TWEAKING COMPANION

for Windows Vista™

KOROUSH GHAZI
WWW.TWEAKGUIDES.COM

[Version 3.0]

TABLE OF CONTENTS

Table of Contents 2
Copyright & Credits 11
Introduction 12
Before Using this Book 13
Basic Requirements 13
Different Versions of Windows 13
Where are the Pictures? 13
Why is the Book So Long? 13
Where Do I Start? 14
Recommended Software 14
Problems with the Book 14
Your Responsibilities 14
Vista Usage Notes 15
Search Box 15
User Account Control 15
Administrator Command Prompt 16
Windows Explorer 16
Notification Area 16
Windows Aero Interface 16
Program Compatibility 16
Driver Compatibility 17
Basic PC Terminology 18
Bits & Bytes 18
Data 19
PC 19
CPU 19
Motherboard 19
Memory 19
Storage Drives 20
Graphics Card 21
Display Device 21
Sound Card 22
Speakers 22
Power Supply Unit 22
Cooling Devices 22
Case 23
Peripheral 23
Operating System and Software 23
System Specifications 24
System Information Tools 24
Windows System Information Tool 24
Performance & Information Tools 24
Device Manager 25
DirectX Diagnostics 25
3DMark 25
SIW 25
Sandra 26
CPU-Z 26
GPU-Z 26
HD Tune 26
Providing System Specifications 27
Backup & Recovery 28
Backup and Restore Center 28
Backing up Files 28
Restoring Files 29
Backing Up the Entire Computer 30

Copyright © 2010 Koroush Ghazi

Restoring the Entire Computer ... 31
System Protection ... 31
System Restore ... 31
Previous Versions ... 32
Resizing System Protection's Reserved Drive Space ... 33
Other Automated Backup Methods ... 34
Third Party Drive Imaging Software ... 34
Online Backup ... 34
Manual Backup ... 35
Backing Up the Windows Registry ... 36
Backing Up & Restoring Passwords ... 37
Backing Up Login Password ... 37
Restoring Login Password ... 37
Recovering Login Password ... 37
Storing Passwords ... 38
Recovering Other Passwords ... 38
File Deletion and Recovery ... 39
Recovering Deleted Files ... 39
Permanently Deleting Files ... 40
Low Level Format and Zero Fill ... 40
System Recovery ... 41
System File Checker ... 42
Advanced Boot Options ... 42
Windows Recovery Environment ... 43
Startup Repair ... 44
System Restore ... 44
Windows Complete PC Restore ... 44
Windows Memory Diagnostic Tool ... 44
Command Prompt ... 44
BIOS & Hardware Management ... 46
The BIOS ... 46
Post Screen ... 46
BIOS Settings ... 47
BIOS Updates ... 47
Firmware Updates ... 47
Hardware Maintenance ... 48
Hardware Handling Tips ... 48
Surge Protectors ... 49
Power Supply Unit ... 49
Cooling ... 50
Device Manager ... 53
ACPI Resource Allocation ... 53
Interrupt Requests (IRQs) ... 54
Device Power Management ... 55
Transient Multimon Manager ... 55
Remove Unused Devices ... 56
Windows Installation ... 57
Prior to Installation ... 57
Check your Hardware for Compatibility ... 57
Disable Unused Resources in the BIOS ... 57
Scan for Malware and Prepare Backups ... 57
Migrating Files and Settings or Upgrade Install ... 58
Modifying The Windows Installation Disc ... 58
Preparing the Drive(s) ... 59
Dual Boot or Multibooting ... 60
Partitioning ... 60
RAID Configuration ... 62
File Systems ... 63
32-bit vs. 64-bit ... 63
Installing Windows ... 64
Step 1 - Start the Install ... 65
Step 2 - Install Now ... 65
Step 3 - Get Important Updates ... 65
Step 4 - Enter Product Key ... 66

Copyright © 2010 Koroush Ghazi

Step 5 - Upgrade or Custom Install ... 66
Step 6 - Set Target Drive ... 66
Step 7 - Automated Installation ... 67
Step 8 - Basic User Setup ... 67
Step 9 - Windows Experience Index & Startup ... 68

Boot Configuration ... 69
BCDEdit ... 69
Startup and Recovery ... 69
MSConfig ... 69
Third Party Tools ... 70
VistaBoot Pro ... 70
EasyBCD ... 71
Bootdisks ... 72

Windows Product Activation & Validation ... 73
Licensing Agreement ... 73
OEM vs. Upgrade vs. Retail Editions ... 73
General Conditions of Use ... 74
Activation ... 74
Product Key ... 74
Activation ... 75
Reduced Functionality Mode ... 76
Validation ... 76

Windows Explorer ... 77
Basic Features ... 77
Folder Options ... 79
General ... 79
View ... 80
Search ... 81
Personal Folders ... 81
Directory Junctions and Symbolic Links ... 82
Advanced Features ... 83
Manipulate Multiple Files at once ... 83
Directory Shortcuts ... 84
Set Windows Explorer Default Startup Folder ... 84
Expanded Context Menus ... 84
Edit Context Menus ... 84
Add 'Copy To' and 'Move To' Context Menu Items ... 86
Add 'Open with Notepad' Context Menu Item ... 86
Edit 'Open With' Context Menu ... 87
Edit 'Send To' Context Menu ... 87
Fix Incorrect Folder Views ... 87
Show Super Hidden Files ... 89
Explorer Restart substitute for Reboot ... 89
Keyboard Shortcuts ... 89
Keyboard and Mouse Substitutes ... 90

Windows Drivers ... 91
Signed vs. Unsigned Drivers ... 91
Vista 32-bit ... 91
Vista 64-bit ... 92
Signature Verification ... 92
Driver Installation ... 92
Step 1 - Service Packs ... 93
Step 2 - DirectX ... 93
Step 3 - Windows Update (Important Updates) ... 93
Step 4 - Motherboard Drivers ... 94
Step 5 - Graphics Drivers ... 95
Step 6 - Sound Drivers ... 95
Step 7 - Peripheral Drivers ... 96
Step 8 - Windows Update (Driver Updates) ... 96
Viewing, Updating or Uninstalling Drivers ... 97
Viewing Driver Details ... 97
Manually Updating Drivers ... 97
Rolling Back to an Earlier Version of Drivers ... 98
Uninstalling Drivers ... 99

Copyright © 2010 Koroush Ghazi

Driver File Repository ... *100*
Driver Verifier ... 101
General Driver Tips ... 102
PC Security ... 104
Security Threats ... 104
Viruses & Worms ... *104*
Trojan Horses ... *105*
Spyware ... *105*
Adware ... *105*
Rootkits ... *105*
Phishing ... *105*
Windows Security Center ... 106
User Account Control ... 107
File System and Registry Virtualization ... *109*
Customizing UAC ... *109*
UAC and the Language Bar ... *112*
Disabling UAC ... *112*
Access Control ... 113
Windows Defender ... 114
Configuring Windows Defender ... *114*
Windows Firewall ... 116
Basic Configuration ... *116*
Advanced Configuration ... *117*
Local Security Policy ... 118
Account Policies ... *119*
Local Policies ... *119*
Data Execution Prevention ... 120
Structured Exception Handling Overwrite Protection ... 120
Kernel Patch Protection ... 121
Encrypting File System ... 121
BitLocker Drive Encryption ... 122
Essential Additional Security ... 122
Malicious Software Removal Tool ... *123*
Microsoft Security Essentials ... *123*
A-Squared Free ... *126*
Spybot Search & Destroy ... *127*
Phishing Protection ... *128*
Firewalls ... *128*
Important Security Tips ... 129
Malware Avoidance Methods ... *129*
Balancing Security vs. Convenience ... *133*
Memory Optimization ... 134
Memory Hardware ... 134
CPU Cache ... *134*
Physical RAM ... *134*
Video RAM ... *135*
Windows Memory Management ... 136
Maximum Supported RAM ... *136*
SuperFetch ... *137*
ReadyBoost ... *138*
ReadyBoot ... *138*
Resource Exhaustion Prevention ... *139*
Virtual Memory ... *139*
Upgrading Memory ... 142
Drive Optimization ... 143
Windows I/O Management ... 143
ReadyDrive ... *144*
Disk Diagnostics ... *144*
Check Disk ... *145*
Drive Controllers ... 145
Master File Table ... 147
Windows Disk Defragmenter ... 148
Advanced Defragmentation ... 149

Copyright © 2010 Koroush Ghazi

The Control Panel 151
Customizing Windows Control Panel 151
Add Hardware 152
Administrative Tools 152
Computer Management *152*
Data Sources (ODBC) *153*
Event Viewer *153*
iSCSI Initiator *153*
Local Security Policy *153*
Memory Diagnostics Tool *153*
Print Management *153*
Reliability and Performance Monitor *154*
Services *154*
System Configuration *154*
Task Scheduler *154*
Windows Firewall with Advanced Security *154*
AutoPlay 155
Backup and Restore Center 155
BitLocker Drive Encryption 155
Color Management 155
Date and Time 155
Date and Time *155*
Additional Clocks *156*
Internet Time *156*
Default Programs 156
Set Your Default Programs *156*
Associate a File Type or Protocol with a Program *156*
Change AutoPlay Settings *157*
Set Program Access and Computer Defaults *157*
Device Manager 157
Ease of Access Center 157
Folder Options 158
Fonts 158
Game Controllers 158
Indexing Options 158
Internet Options 158
iSCSI Initiator 158
Keyboard 158
Mouse 159
Buttons *159*
Pointer Options *159*
Wheel *159*
Network and Sharing Center 159
Offline Files 160
Parental Controls 161
Pen and Input Devices 161
People Near Me 161
Performance Information and Tools 161
Personalization 161
Window Color and Appearance *161*
Desktop Background *162*
Screen Saver *162*
Sounds *163*
Mouse Pointers *163*
Theme *163*
Display Settings *163*
Phone and Modem 164
Power Options 164
Power Plan *164*
Printers 167
Problem Reports and Solutions 168
Programs and Features 168
Regional and Language Options 170
Formats *170*
Location *170*

Copyright © 2010 Koroush Ghazi

Keyboards and Languages ... *170*
Administrative ... *170*
Scanners and Cameras ... 171
Security Center ... 171
Sound ... 171
Volume Mixer ... *172*
Playback ... *172*
Recording ... *173*
Sounds ... *173*
Speech Recognition ... 174
Sync Center ... 174
System ... 174
Computer Name ... *175*
Hardware ... *175*
Advanced ... *175*
System Protection ... *176*
Remote ... *176*
Tablet PC Settings ... 176
Taskbar and Start Menu ... 176
Taskbar ... *176*
Start Menu ... *177*
Notification Area ... *180*
Toolbars ... *180*
Text to Speech ... 181
User Accounts ... 181
User Account Scenarios ... *182*
Managing Accounts ... *183*
Parental Controls ... *184*
Advanced User Account Properties ... *185*
Welcome Center ... 186
Windows CardSpace ... 186
Windows Defender ... 186
Windows Firewall ... 186
Windows Sidebar ... 186
Windows Sideshow ... 187
Windows Update ... 187

Startup Programs ... 189
Finding Startup Programs ... 189
Software Explorer ... *189*
Microsoft System Configuration Utility ... *189*
Registry Editor ... *190*
Autoruns ... *190*
Identifying Startup Programs ... 191
Removing Startup Programs ... 192
Startup Problems ... 192
Regular Maintenance ... 193

Services ... 194
Services Utility ... 194
Default Services ... *194*
Customizing Services ... *195*
Restarting a Service ... *199*
Non-Microsoft Services ... *199*
Change Service Status via Command Line ... *200*
Permanently Deleting Services ... *200*

Windows Registry ... 202
Registry Editor ... 202
Editing Registry Entries ... *203*
Creating New Registry Entries ... *203*
Backing up and Restoring Portions of the Registry ... *203*
Miscellaneous Registry Tweaks ... 204
Customize Shutdown Speeds ... *204*
Increase NTFS System Performance ... *205*
Turn Off System Beeps ... *205*
Disable Windows Key ... *205*

Copyright © 2010 Koroush Ghazi

Maintaining the Registry 206
Group Policy 208
Prevent Automatic Restore Point During Driver Installation 208
Prevent Windows Media DRM Internet Access 208
Prevent Windows Media Player Automatic Updates 208
Hide Specific Control Panel Items 209
Turn off Thumbnails 209
Remove 'Map Network Drive' and 'Disconnect Network Drive' context Menu Items 209
Remove All Right-Click Context Menus 209
Remove Clock From Notification Area 209
Remove Balloon Tips 209
Handling of Windows Mail Attachments 210
Modify CTRL+ALT+DEL Screen 210
Windows Search 211
Search Indexing 211
Performance Impact 212
Customizing the Index 212
Indexing and File Properties 214
Disabling the Index 214
Search Methods 215
Instant Search 215
Search Explorer 215
Customizing Search 216
Internet Explorer 217
Basic Settings 217
General 217
Security 219
Privacy 220
Content 221
Connections 221
Programs 221
Advanced 222
InPrivate Browsing 225
InPrivate Filtering 225
Accelerators 226
Advanced Settings 226
Customize Internet Explorer 8's Appearance 226
Change or Disable Click Sound 227
Change Default Download Directory 227
Start with InPrivate Browsing Mode Enabled 228
Start with InPrivate Filtering Mode Enabled 228
Customize IE Title Bar 228
Built-In Flash Blocking 228
Fix Internet Explorer 8 229
Increase Maximum Simultaneous Connections 229
DNS Cache Issues 230
Advanced Customization 230
Other Internet Browsers 231
Windows Mail 232
Basic Settings 232
General 232
Read 232
Receipts 232
Send 233
Compose, Signatures, Spelling 233
Security 233
Connection 234
Advanced 234
Windows Contacts 234
Junk Email Options 235
Advanced Settings 237
Backing Up and Restoring Emails and Accounts 237
Disable Windows Mail Splash Screen 237
Other EMail Clients 238

Copyright © 2010 Koroush Ghazi

Windows Media Player **239**
Basic Settings 239
Player *239*
Rip Music *239*
Devices *240*
Burn *240*
Performance *241*
Library *242*
Plug-ins *242*
Privacy *243*
Security *243*
DVD *243*
Network *243*
Graphic Equalizer *243*
Skins *244*
Mini Player Mode *244*
Audio & Video Codecs 244
Digital Rights Management 246
Other Media Players 247
Graphics & Interface **248**
Windows Aero Interface 249
Requirements *249*
Performance *250*
Desktop Background 250
Static Backgrounds *250*
Additional Vista Static Backgrounds *251*
Animated Backgrounds *251*
Windows Photo Gallery 251
Windows Sidebar 252
Desktop Fonts 253
Interface Font Size *254*
Custom Fonts *254*
Desktop Icons 254
Resize Desktop Icons *254*
Remove text from desktop icons *255*
Remove Shortcut Arrows from Icons *255*
Create desktop icons for Shutdown or Restart *255*
Save desktop icon positions *256*
Set spacing between desktop icons *256*
Remove '- Shortcut' from new shortcuts *257*
Advanced Icon Customization *257*
Repair Incorrectly Displayed Icons *257*
General Interface Customization 257
Increase Menu Display Speed *257*
Customize Vista Boot Screen *258*
Create Custom Desktop Toolbar *258*
Slow Down Vista Animations *258*
Customize 3D Task Switching *258*
Customize Other Interface Components *259*
Multi Monitor Customization *259*
DirectX 10 & DirectX 11 259
Gaming in Vista 261
Games Explorer *261*
Problems Launching Games *263*
Overclocking **264**
Benefits and Drawbacks 264
Benefits *264*
Drawbacks *265*
Methodology 266
CPU Overclocking *266*
RAM Overclocking *266*
Graphics Card Overclocking *267*
Voltage Adjustment *267*
Stability 268

Copyright © 2010 Koroush Ghazi

Power Supply Unit ... 269
Cooling ... 269
Comparing Overclocks ... 269
Researching Overclocking ... 270
Performance Measurement & Diagnostics ... 271
Windows Experience Index ... 271
Windows System Assessment Tool ... 273
Event Viewer ... 275
Performance Measurement ... 275
Troubleshooting ... 275
Reliability and Performance Monitor ... 277
Performance Measurement ... 277
Troubleshooting ... 278
Task Manager ... 278
Performance Measurement ... 278
Troubleshooting ... 280
Multi-Core CPUs ... 282
Process Explorer ... 283
System Health Report ... 283
Network Diagnostics Tool ... 284
Memory Diagnostic Tool ... 284
Problem Reports and Solutions ... 285
Windows Errors ... 286
Third Party Tools ... 287
3DMark ... 287
Unigine Heaven ... 287
RTHDRIBL ... 287
Lightsmark ... 288
FurMark ... 288
Game Benchmarks ... 288
PCMark ... 288
Sandra ... 288
Prime95 ... 289
Super PI ... 289
HD Tune ... 290
MemTest ... 290
Memtest86+ ... 290
Cleaning Windows ... 291
Disk Cleanup ... 291
Advanced Disk Cleanup ... 292
Service Pack Cleanup Tool ... 293
Recycle Bin ... 294
CCleaner ... 294
Manual Cleaning ... 296
Deleting 'In Use' Files ... 297
Regular Maintenance ... 299
Step 1 - Maintain Security ... 299
Step 2 - Check Startup Programs & Services ... 299
Step 3 - Backup ... 299
Step 4 - Clean Windows ... 300
Step 5 - Check Disk ... 300
Step 6 - Defragment ... 300
Scheduled Maintenance ... 300
Conclusion ... 301
Version History ... 301

Copyright © 2010 Koroush Ghazi

COPYRIGHT & CREDITS

The contents of this book are Copyright © Koroush Ghazi and protected under US, Australian and International Copyright laws. No unauthorized reproduction, alteration or distribution of the book, in part or in whole, in any language, is permitted. All Trademarks used in this publication are the property of their respective owners.

HOSTING, DISTRIBUTION AND TRANSLATIONS OF THIS BOOK

Reproducing, altering, hosting, or mass distributing this book in any way is not permitted. The latest version is always available from TweakGuides.com.

Translations of this book are not permitted, as I have absolutely no way to determine the quality and accuracy of any translations, particularly given the somewhat complex and often delicate procedures in this book. Professional translations of this 175,000 word book into the multiple languages required would cost a great deal, and amateur translations are unacceptably shoddy.

If you wish to spread the word regarding the book, please link to the TweakGuides Tweaking Companion download page.

I've invested a huge amount of time and effort into creating this book, and I also provide a free version of this book which is easily accessible so that the widest possible audience can benefit from its contents. There is no reason for anyone to publicly reproduce or distribute this book when the latest version is always available for free from my site. People who host this book or portions of it are usually doing so to generate easy traffic, income or credit for themselves using my hard work, which is not acceptable. Appropriate action will be taken against any such individuals who do not respect the concept of author rights.

For those who do not understand the strictness of these conditions, please see the TweakGuides FAQ.

CREDITS

This book is a reference compilation borne out of a great deal of testing, research, reading and personal experience. I give full credit to any websites and authors linked in this book, as well as all the software developers whose excellent tools I recommend in this book, especially those who provide their software for free. It is amazing that they invest so much time and effort into developing and testing their software and then provide it free to all PC users. I encourage you to support their work with donations and purchases where relevant, because giving is a two way street.

Thank you to my readers who, since TweakGuides began in April 2004, have provided a great deal of support. From those who support the site by linking to it on various websites and forums, to those who take the time to write to me with thoughtful and constructive contributions, and in particular to those who donate to the site or purchase the Deluxe Edition of the TGTC - I truly appreciate it. The only thing which motivates me to keep writing guides is the fact that I know there are intelligent people out there who are patient enough to take the time to read them, and to use the material in the spirit in which it is intended: to learn more about their PCs, and to think for themselves and resolve their own problems.

Copyright © 2010 Koroush Ghazi

INTRODUCTION

After years of development and anticipation, Windows Vista was released on January 30, 2007 amidst a great deal of hype and confusion, as well as liberal amounts of misleading information across the Internet. With its predecessor Windows XP having been the dominant operating system for over five years, most people are unfamiliar with, wary of, even hostile towards Vista. The vague and often incorrect advice on Vista's features that has been proliferating around the Internet only makes things worse.

Having written computer guides since 2002, and running a site well known for providing comprehensive guides like the original *TweakGuides Tweaking Companion* for Windows XP, I realized that it would be expected of me to provide at the very least a basic guide that discusses how to optimize and customize Vista. But I wanted to do much more than that, so I set about the task of writing a truly comprehensive Vista book. Initially I, like many others, underestimated the sheer number of changes and new features in Vista. However after several hundred hours of research, experimentation, writing and editing, the *TweakGuides Tweaking Companion for Windows Vista* was completed and sits before you today.

The length of this book will no doubt frustrate people who are looking for a handful of tweaks or quick fixes to 'make Vista faster'. Clearly that is not the sole aim of this book. My goal is to explain how things work in simple but sufficient detail so that readers can customize and optimize their machines appropriately while learning more about them. Computers are now integral to many aspects of our lives, so it is simply not possible to pretend that it is not important to know how they work. The book is long because I make sure that whether novice or advanced, you are given enough details to actually understand the logic behind Windows functionality as well as any recommendations I provide, rather than being treated like a small child who is simply told to do something without a second thought.

I promise you that if you patiently work your way through this book over the course of several days, that you will come out at the other end with not only a better performing, more stable and better customized PC, you will also be much more comfortable with using Windows Vista on a daily basis; the mystery will disappear. More importantly, you will be able to better diagnose, indeed prevent, any problems on your PC in the future. In any case, the choice as to how best to use the book is left up to you.

In closing, if you find the book useful, I ask that you consider making a donation or purchasing the enhanced Deluxe Edition of this book at www.TweakGuides.com. This support will allow me to continue releasing a free version of this book, and to also continue creating new works in the future.

Cheers,

Koroush Ghazi
Owner/Author
TweakGuides.com

In honor of 2,500 years of Persian Culture
Dedicated to the noble ideals of Cyrus the Great

Copyright © 2010 Koroush Ghazi

BEFORE USING THIS BOOK

BASIC REQUIREMENTS

There are three key requirements you must meet to use this book successfully:

- You will need access to an Administrator level user account to make many of the changes in this book. The default account created during Windows installation is one such account. See User Accounts under the Control Panel chapter for more details.
- You should prepare backups of all your important data prior to undertaking any of the changes detailed in this book. See the Backup & Recovery chapter for details.
- You should have a Windows Vista DVD. Do not undertake the tweaks in this book if you don't have a Vista DVD as you may not be able to reverse certain changes or fix any problems which may occur.

I do not recommend applying any of the changes covered in this book unless you meet all three of the requirements above, however the bare minimum requirement is that you must have Administrator access.

DIFFERENT VERSIONS OF WINDOWS

This book is designed only for Windows Vista - there are separate TweakGuides Tweaking Companion books for Windows 7 and Windows XP, to which users of those operating systems should refer. The major content differences between the various editions of Vista are covered in this Microsoft Article. However there are no content differences between the OEM, Academic, MSDN, TechNet, Upgrade and Retail editions of Windows Vista - these are all identical in terms of performance and content. The actual difference is that certain licensing and usage conditions apply to each of them - see the Windows Product Activation & Validation chapter for details.

WHERE ARE THE PICTURES?

There is a distinct lack of pictures in this version of the book. The Deluxe Edition of this book does contain detailed screenshots and illustrative images, as well as other useful features which make using this book much more convenient, such as high quality text resolution for better print quality, full bookmarks for quicker chapter and section access, and the ability to copy text which is handy for purposes such as correctly assigning Registry values or entering complex Command Prompt commands. If you want the book with these features, and more importantly want to show your support, please consider purchasing a Deluxe Edition from the link above, the electronic version of which is only a few dollars.

WHY IS THE BOOK SO LONG?

This book is intended primarily as an educational and reference source. It is not intended for people seeking quick fixes. I provide explanations for a wide range of features and procedures for a relatively broad audience so that anyone can gain a good understanding of what they're doing, and make up their own mind, rather than just taking my word for it. I firmly believe in the old saying: *Give a man a fish and he will eat for a day; Teach a man to fish and he will eat for a lifetime*. To find information on any topic in the book at any time, you can use the Table of Contents or press CTRL+F to bring up the PDF search functionality. I will not be releasing a cut-down version of this book; there are no '10 best tweaks' or a handful of changes which magically speed up or fix Windows. It is a complex interrelationship of hardware and software settings which determine how fast and how stable your PC runs, and it requires understanding and thought to correctly optimize and customize a system.

Copyright © 2010 Koroush Ghazi

WHERE DO I START?

This book has been designed to cater to both those who are doing a new installation of Windows Vista and those who are using an existing installation of Windows Vista. The chapters follow a roughly sequential order as to the types of things I would personally configure before and after doing a new installation. However any chapter or even any section can be read in any order you wish, because where any procedures or details from other chapters are required, they are referenced accordingly. If you don't wish to read the book sequentially, I strongly recommend reading the Basic PC Terminology and Vista Usage Notes chapters before reading anything else. Then I suggest becoming familiar with the contents of the Windows Explorer, Windows Drivers, PC Security and Graphics & Interface chapters as soon as possible, as these cover the most important interface, functionality and security-related topics.

RECOMMENDED SOFTWARE

Listed throughout this book is a range of software which I recommend to enable you to carry out some of the procedures in the book or to provide additional functionality in Windows. If you do not feel comfortable in downloading or installing this software for whatever reason, you should ignore those procedures which rely upon it, as none of them are critical to the functioning of Windows. Furthermore, at no point do you have to purchase any software. I am not paid or sponsored by any software or hardware company, so I generally recommend the best free software available to do the job. In a few cases the software may require purchase, but usually the trial version of it retains enough functionality to complete the job for which I have recommended it. Of course if you do find any of the software useful I encourage you to purchase it or donate to the software's author. Not everything on the Internet is free, nor should it be.

PROBLEMS WITH THE BOOK

While I have made every effort to ensure that this book is as clear and accurate as it can be, I hope you can appreciate the fact that I cannot possibly test the information and recommendations in this book on every potential combination of PC hardware and software available. If there is anything in the book which you believe is genuinely inaccurate or misleading, or if you just want to report a broken link, please Email Me with specific details and if appropriate I will rectify it in the next version of the book. You can also email me if you wish to share any general feedback or thoughts you have about the book.

However I must stress that the book is provided 'as is', and I cannot provide technical support of any kind. It simply isn't viable or appropriate for me to do so, so under no circumstances will I provide personalized optimization, customization or purchasing advice/feedback, or any other form of technical support related to the information in this book. The whole reason for writing this book is to give each and every reader a thorough rundown on all the steps necessary to customize and optimize their system. As such, there are sufficient resources and links in this book to help anyone learn more about their system and solve most any problem when combined with additional research and thought.

YOUR RESPONSIBILITIES

The basic theme throughout this book is that as long as you read and consider the advice given carefully and use common sense when applying any changes, you will remain problem-free. I have made every reasonable effort to ensure that the contents of this book are completely accurate to the best of my knowledge, and that the sites and utilities linked to in the book are free from any malware or deceptive practices at the time of writing. In all respects the book is safe to use if followed correctly, with careful consideration and taking appropriate precautions. However for legal reasons I cannot take any responsibility for any damage or loss incurred through the use of this book. **It is a condition of use for this book that you agree to take full responsibility for any of your actions resulting from reading this book**. If you do not wish to take full responsibility for using this book and any resulting impacts, then do not proceed any further - close the book immediately.

Copyright © 2010 Koroush Ghazi

VISTA USAGE NOTES

This chapter briefly highlights important changes in Windows Vista compared to Windows XP, as well as covering the most frequently used Vista features. Do not skip this chapter - read through it quickly now, then refer back here as necessary when you go through the book.

SEARCH BOX

Throughout this book you will see me refer to Start>Search Box as a place to input particular text, often to launch a program or Windows feature. This Search Box is actually an Instant Search box which appears (among other places) at the bottom of the Start Menu when you click the Start button. Strictly speaking it is not a command line interface like the Windows Run box - which you can access by pressing WINDOWS+R or using the Run item on the Start Menu (when configured appropriately). However it is much quicker to use than going through menus to find a shortcut, or typing an exact executable or command name in the Run box, so I refer to it constantly in the book.

More details of this Search Box and how the search functionality works in Vista are in the Windows Search chapter.

USER ACCOUNT CONTROL

Vista has changed the way users are allowed to make major changes to the system. To start with you will need to be using (or have access to) an Administrator-level user account if you want to implement most of the changes in this book. The default account that you create when first installing Vista is one such Administrator-level account, so start by logging into that account when using this book.

When User Account Control (UAC) is enabled, you will be prompted to Continue prior to making any system-level changes; this is normal. Click the Details button on the UAC prompt to ensure you will be running the program you expect to be running. In some cases older programs not designed specifically for Vista may not launch properly or have full functionality when UAC is enabled, because they don't ask for Administrative access to the system even when it is required. In such cases, launch the program by right-clicking on its executable or launch icon and select 'Run as Administrator' to ensure it will have full functionality.

Importantly: Even if you find it annoying, do not disable UAC to start with because aside from security issues, if you choose to enable it again in the future, due to file and registry virtualization your settings for any currently-installed programs may be lost. The reason for this is explained more clearly in the PC Security chapter. Keep UAC enabled initially both for security and consistency purposes, and once you've finished reading this book you will have enough information to properly consider whether to keep it enabled or not and the impact that this choice will have.

These changes are all detailed under the User Account Control section of the PC Security chapter, and the User Accounts section of the Control Panel chapter.

Copyright © 2010 Koroush Ghazi

ADMINISTRATOR COMMAND PROMPT

Related to UAC is the fact that if using an MS-DOS Command Prompt to make command-line based changes, you will often require what is known as an 'Administrator Command Prompt' to successfully use certain system commands. There are several ways to access an Administrator Command Prompt.

- § Go to Start>Search Box, type *cmd* then right-click on the 'cmd.exe' item which appears at the top of the Start Menu and select 'Run as Administrator'.
- § Go to Start>Search Box, type *cmd* then press CTRL+SHIFT+ENTER.
- § Go to Start>Search Box, type *cmd* then right-click on the 'cmd.exe' item, select 'Send To>Desktop' to create a shortcut on your Desktop. Right-click on this shortcut, select Properties, click the Advanced button and tick 'Run as Administrator'. You can now use this shortcut to always launch an Administrator Command Prompt as required.

If ever a particular command line option is not executing properly or appears to have no impact, it is most likely because you need to use it in an Administrator Command Prompt. Note that you can also run any program or Vista feature from an Administrator Command Prompt without requiring a re-confirmation through UAC, because it already has elevated privileges.

WINDOWS EXPLORER

Most users will need to start using the Windows Explorer and Explorer-based windows and features relatively early in their experience with Vista, typically to manipulate files, so the Windows Explorer chapter has been moved closer to the start of this book. I encourage you to refer to that chapter as early as possible, and as often as necessary to understand how the Explorer interface works in Vista since it is a key tool. The Windows Explorer chapter also contains a list of keyboard shortcuts which may come in handy as you use this book, so again it may be worth perhaps skipping to early on to see the changes and new features.

NOTIFICATION AREA

This is a relatively insignificant change, but it should be noted that Microsoft now refers to the area at the bottom right of the screen in the Taskbar (next to the clock) as the Notification Area, not the System Tray area. All references in this book to the Notification Area refer to that location.

WINDOWS AERO INTERFACE

An obvious new feature introduced in Vista is the Windows Aero glass-like interface. The Windows Desktop is no longer simply a 2D environment, under Vista the Desktop always runs in Direct3D mode, so it can have both 2D and 3D elements at the same time. To see if you are running Aero, and to demonstrate its 3D capabilities, press WINDOWS+TAB to trigger Vista's 'Windows Flip 3D' task switching interface.

For details of how to enable and use the new interface features see the Graphics & Interface chapter.

PROGRAM COMPATIBILITY

While Vista is quite different to older versions of Windows such XP or 2000, most programs which ran under those platforms will usually run on Vista without problems. If in doubt, check this Windows Vista Software Compatibility List to see if your program has any known issues. Newer programs are of course quite compatible with Windows Vista, particularly as Vista shares the bulk of its underpinnings with Windows 7.

If you are having problems running an old program, right-click on the program executable or launch icon, select Properties and under the Compatibility tab tick the 'Run this program in compatibility mode' and select the appropriate OS - Windows XP Service Pack 2 is the most compatible configuration. Also make sure to try running the program as an Administrator (see User Account Control further above), as some older programs do not inform Vista that they need full Admin access to the system, and hence will abort during

Copyright © 2010 Koroush Ghazi

launch or give errors during installation or usage unless you right-click on them and select 'Run as Administrator'.

DRIVER COMPATIBILITY

Windows Vista introduced a new driver model designed to make the system more stable, but this meant that most older drivers designed for Windows XP did not work in Vista. In some cases, older peripheral drivers such as those for printers do work on Vista, but for the most part only drivers specifically designed for Vista can be used. Initially there were some teething problems as a result of this major change, as hardware manufacturers were slow to support Vista and this is one of the main reasons why Vista unfairly gained a poor reputation. Fortunately the driver compatibility issues rapidly disappeared and this is no longer an issue whatsoever.

Windows Vista 64-bit users should note that under normal circumstances you cannot run drivers which are unsigned under Vista 64-bit, nor can you use drivers designed for Vista 32-bit. See the Windows Drivers chapter for more details of drivers under Vista, as well as the Sound section under the Control Panel chapter, and the start of the Graphics & Interface chapter for important details on audio and video driver-related changes introduced in Vista.

These are just some of the more important areas which may confuse new users of Vista. Vista has a vast range of changes, some large and some small, for which you must steadily read through this entire book to learn more about and understand the rationale behind them. The one thing I can guarantee you is that Windows Vista is not just Windows XP with a new interface and annoying prompts. It has introduced a large number of changes both above and beneath the hood, and contains greatly improved built-in utilities, enhanced security and many new features which are all covered in this book.

Copyright © 2010 Koroush Ghazi

BASIC PC TERMINOLOGY

This chapter explains in layman's terms commonly used technical terminology. All of the major hardware components found in a modern PC are also covered. While advanced users may want to skip this chapter, everyone should read the Bits & Bytes section below to clarify a common point of confusion.

BITS & BYTES

You will often see the terms Bits, Bytes, Kilobytes, Megabytes and Gigabytes (or their abbreviations) being thrown around. Understanding these is very important to learning more about PC usage. To start with, a Bit (Binary Digit) is the lowest form of computer information, and can take the value 0 or 1 (i.e. Off or On). All computer functionality is derived from the behavior of bits. For the purposes of this book, the most common units of measurement are:

8 bits (b) = 1 Byte (B)
1,024 Bytes = 1 Kilobyte (KB)
1,024 Kilobytes = 1 Megabyte (MB)
1,024 Megabytes = 1 Gigabyte (GB)

Note that bits are shown as a small 'b', and Bytes are shown as a capital B - this is an important distinction. For example 512kbps is 512 kilo*bits* per second, which converts to 64KB/s (Kilob*ytes* per second).

For most users, knowing the above conversion factors is sufficient for understanding the terminology used in this book and around the Internet, as well as for general PC usage. However strictly speaking, the values shown above are not correct, as explained in this article. The discrepancy stems from the fact that the commonly used metric prefixes Kilo, Mega, Giga and so forth are based on the decimal (base ten) system, while as noted, computers are based on the behavior of bits, which is a binary (two digit) system. Therefore while 8 bits still equals 1 Byte under either system, the correct prefixes to use in other cases are:

1,024 Bytes = 1 *Kibi*byte (KiB)
1,024 Kibibytes = 1 *Mebi*byte (MiB)
1,024 Mebibytes = 1 *Gibi*byte (GiB)

1,000 Bytes = 1 Kilobyte (KB)
1,000 Kilobytes = 1 Megabyte (MB)
1,000 Megabytes = 1 Gigabyte (GB)

What's the difference? Well one Kilobyte (KB) actually equals 1,000 bytes, since 'kilo' is a decimal prefix meaning 'thousand'. Yet one Kilobyte as interpreted by a computer is actually 1,024 bytes, so 'kilo' is not the appropriate prefix to use, Kibibyte (KiB) is the correct term referring to multiples of 1,024 bytes. This discrepancy may seem minor at first - only 24 bytes difference between 1KB and 1KiB - but as the values grow, it becomes more significant, so it is important to understand the difference. This is particularly true because hardware and software manufacturers often use these prefixes differently, causing PC users a great deal of confusion.

The best practical example of this discrepancy is drive capacity. A drive advertised as having 150GB of storage space is a technically correct use of the term Gigabyte, because it holds 150,000,000,000 Bytes of storage. However purchasers of the drive soon become confused when they see that Windows typically reports the drive as having only 139GB of usable space. This is because 150,000,000,000 Bytes translates to 139GiB in the binary system the computer uses, as opposed to 150GB in the decimal system, but Windows incorrectly shows GB instead of GiB. This results in many users feeling ripped off because their usable drive space does not match the advertised storage capacity. As drive capacities grow, the discrepancy between advertised and reported space becomes much larger, causing even greater concern among consumers.

Copyright © 2010 Koroush Ghazi

In any case, to avoid further confusion, throughout this book I will continue to refer to values based on the accepted (but technically inaccurate) common usage, i.e. the way in which hardware manufacturers report them, and the way in which Windows reports them, despite the discrepancy. Eventually however widespread adoption of the correct terms will be necessary to prevent growing consumer confusion.

DATA

In the context of PCs and technology, Data is a general term referring to any amount or type of information which is stored and used by a computer.

PC

A Personal Computer (PC), also referred to as a System, Machine, Rig or Box, is a collection of hardware (electronic components) which function as a unified system through the use of software (programmed instructions).

CPU

The Central Processing Unit (CPU), also referred to as the Processor, is the single most important component of a PC. The CPU chip is typically a small thin square chip which is seated firmly on your Motherboard, and usually covered by a large metal heatsink and fan to cool it. The CPU controls and co-ordinates the actions of the entire PC under instruction from software. It has the role of determining which hardware component does what, assigning tasks and undertaking complex calculations which are then fed through the various relevant components and back.

MOTHERBOARD

The Motherboard, also called a Mainboard or Mobo, is the large rectangular Printed Circuit Board (PCB) into which all of the electronic components are connected in a PC. The motherboard is typically firmly attached to the inside of a PC Case. The motherboard provides a network of pathways for the CPU to communicate with the various hardware components, and a range of ports for standard peripherals and other devices to plug into the PC.

MEMORY

A PC uses several different types of Computer Memory to store data, whether temporarily or permanently, for the purposes of speeding up processing performance. Memory chips are fast because unlike other forms of data storage, such as physical Hard Drives or Optical Drives, they have no moving parts. The main types of PC memory are covered below:

Random Access Memory (RAM), also called System RAM or simply just Memory, is the most common form of hardware used by a PC. RAM usually comes in the form of a long thin PCB stick (a DIMM) that plugs into the motherboard and through it provides a place for the CPU and other components to temporarily store any data which the system needs to rapidly access. RAM only holds data while it has a source of power; if a PC is rebooted or switched off, any data in RAM is instantly lost. For this reason, this type of memory is referred to as Volatile Memory.

Read Only Memory (ROM) is a more permanent form of memory, and works similar to RAM, however unlike RAM it can only be read from and not written to under normal circumstances. Furthermore it will not clear when it has no source of power; that is, when the system is rebooted or switched off it does not lose its contents. For this reason, this type of memory is referred to as Non-Volatile Memory. ROM is primarily used to hold smaller amounts of important data, such as the Basic Input Output System (BIOS) - the program which tells the computer how to function when it is first switched on - stored on the ROM chip in the motherboard. Certain ROMs can be written to by use of a process called Flashing, such as when the BIOS is flashed with a newer version of its programming.

Copyright © 2010 Koroush Ghazi

The CPU and other hardware such as hard drives often have small memory chips of their own called Caches to temporarily hold data. This memory is typically a smaller RAM chip and is used as another point of temporary storage to further speed up data transfers.

STORAGE DRIVES

As noted under Memory above, RAM is only a temporary form of storage, and while able to store data permanently in the absence of power, ROM has typically been too small to store large volumes of data, and is also not designed for being frequently written to. Therefore modern computers employ one or more of several forms of storage drives designed to permanently hold data in large quantities and with varying degrees of portability. Storage drives plug into one of four main types of drive controllers found on the motherboard, listed from slowest to fastest below:

§ Floppy Disk Controller (FDC);
§ Integrated Drive Electronics (IDE) / Parallel ATA (PATA);
§ Serial ATA (SATA); or
§ Small Computer System Interface (SCSI), including Serial Attached SCSI (SAS).

The controller available for any particular drive to use depends on both the drive type and the motherboard type. Some storage drives can also plug into the Universal Serial Bus (USB) port of a PC, however this is a multi-purpose port and not a dedicated drive controller, so it is not listed above.

The various types of drive hardware are covered below:

A Hard Disk Drive (HDD) is a magnetic storage device that acts like Memory, except it is semi-permanent, slower and far larger in capacity. The hard drive is a rectangular metallic box inside which is a stack of round platters and a read/write head. Whenever the PC requires data, it must first be read from the hard drive, usually into RAM, from where it is then accessed by the CPU and other devices. Data written to the hard drive will remain on the drive regardless of whether the system is rebooted or switched off. Because a hard drive has moving physical components, such as the read/write head and a spinning disk, it can never be as fast as memory chips - which have no moving parts - in providing data. As a result, a system may slow down or stutter while waiting for more data to be loaded up from or written to a hard drive. The amount of data stored on the hard drive itself usually has no significant impact on its performance, however if the data on the drive becomes fragmented, this will reduce performance.

A Solid State Drive (SSD) is a memory-based storage device which combines the advantages of the speed of computer memory with the more permanent nature and larger capacities of hard disk drives. By using a type of Non-Volatile memory called Flash Memory, which is similar to ROM as covered under the Memory section above, an SSD can store data even when the PC is rebooted or switched off. Unlike a hard drive, an SSD has no mechanical moving parts, and as such is much faster in accessing its stored data. As SSDs become cheaper, faster and more reliable, they are steadily replacing hard disk drives for consumer PC usage.

An Optical Disc Drive is a disc-based data storage device that reads from and sometimes writes data onto CD, DVD or Blu-Ray discs via laser or other light-based methods, hence the use of the term 'optical'. These portable discs permanently hold this data until overwritten or deleted. Optical drives usually come in plastic rectangular boxes with a loading slot or extendable tray in the front. While much slower than hard drives or SSDs due to physical limitations, the main advantage of optical drives is the portability and relatively low cost of their media, along with the fact that such media can also be played on a variety of non-PC devices, such as standalone DVD or Blu-Ray players. Note that the term *disk* usually refers to magnetic media, like a floppy disk, while the term *disc* refers to optical media, such as a DVD disc.

Copyright © 2010 Koroush Ghazi

A Floppy Disk Drive (FDD) is a magnetic storage device which reads and writes data on thin plastic 3.5" Floppy Disks. The floppy drive comes in a rectangular plastic box with a loading slot at the front and a manual ejection button. Floppy drives are extremely slow compared to any other form of drive, and also hold very little data (around 1.44MB), and hence are a legacy device no longer used on most modern PCs. Some PC users retain a floppy drive for Windows recovery purposes, or to flash the BIOS, however this is no longer necessary as most modern PCs now fully support the use of optical discs or USB drives for these purposes instead. In fact the only major advantage of floppy drives - the relative portability of their 3.5" disk media - has been completely superseded by USB drives which are much smaller, faster, sturdier and more reliable, and can hold several GB of data as opposed to just 1.44MB.

A USB Flash Drive is extremely similar to an SSD, in that it also uses Non-Volatile Flash memory to store data. However USB drives are typically much smaller in capacity and physical size, and offer much slower performance and reliability than an SSD. Their main advantage is that of low cost and portability due to their very small size, which is why they are also known as thumb or key drives. They plug into a standard external USB port on a PC, making them much easier to use for connecting to and transferring data between different PCs, since unlike a standard drive they do not need to be connected to a motherboard drive controller found inside a PC.

GRAPHICS CARD

The Graphics Card, also called the Video Card, GPU, Graphics Adapter or VGA Adapter, is a miniature computer of its own dedicated solely to processing complex graphics-related data. It is a thin rectangular plastic PCB with a Graphics Processing Unit (GPU), also known as the Core, and Video RAM (VRAM), also known as Video Memory. The GPU and VRAM are the graphics-specific equivalents of the CPU and System RAM on a PC, and the graphics card itself has Pipelines for transferring data internally, similar to the data pathways on a motherboard. The graphics card plugs into the motherboard through one of the following interfaces, sorted from slowest to fastest:

- Peripheral Component Interconnect (PCI);
- Accelerated Graphics Port (AGP); or
- Peripheral Component Interconnect Express (PCI-E).

Graphics cards typically come with some form of cooling enclosure built around them, to ensure that the GPU and the VRAM remain cool enough to operate correctly. The graphics card undertakes the majority of 2D and 3D graphics calculations under Windows, and also sends data directly to a Display Device. Some motherboards have built-in graphics functionality that works in much the same way as a plug-in graphics card, but is referred to as Onboard or Integrated Graphics. PCs with such graphics functionality typically process graphics-related data far less quickly than those with plug-in graphics cards.

DISPLAY DEVICE

A Display Device, more commonly referred to as the Monitor, is the device through which the PC's data output is displayed graphically. This graphical data typically comes directly from the graphics card, and a display device must be plugged into the graphics card to facilitate this. Some computers still have a traditional Cathode Ray Tube (CRT) monitor as their primary display device, however most modern PC monitors now utilize Liquid Crystal Display (LCD) technology. Furthermore a modern PC can also be plugged into a television set of any type, such as CRT, LCD, Plasma, Rear or Front Projector, and other similar technology sets if the user desires, or even a combination of multiple displays at once if the graphics card supports such functionality.

Display devices have the ability to display graphics at various Display Resolutions, typically expressed in number of Pixels wide by number of Pixels high (e.g. 1920 x 1200). A Pixel is the smallest component of a digital image, thus the higher the resolution, the more pixels are displayed on the display device and the

Copyright © 2010 Koroush Ghazi

clearer the image. At each resolution a display device can also redraw the image a number of times per second, referred to as the Refresh Rate which is expressed in hertz (Hz). Refresh rate is not to be confused with Frame Rate, which is expressed in Frames Per Second (FPS). Refresh rate is a physical limitation of a display device in refreshing the image on the screen a certain number of times per second. Frame rate on the other hand is the number of times per second that the software and graphics device can provide a whole new frame of imagery.

Sound Card

The Sound Card, also called the Audio Card or Audio Device, is a thin PCB that acts as a dedicated CPU for calculation of audio data. It typically plugs into the motherboard, and usually has no form of cooling enclosure around it. Some motherboards have built-in audio functionality that works in much the same way as a sound card, but is referred to as Onboard or Integrated Sound. PCs with such audio functionality may process audio-related data less quickly or with less additional functionality than those using plug-in sound cards.

Speakers

A PC usually comes with some form of sound output device, typically a built-in PC speaker to provide audible warnings in the form of beeps or tones. Users with a Sound Card or Integrated Sound can attach more functional sound output devices, such as Speakers or Headphones, directly into the sound card or integrated sound device through the back of the PC. The addition of speakers or headphones allows the user to experience higher quality sound and also a potentially higher number of discrete Audio Channels which can increase the realism of sound reproduction.

Power Supply Unit

The Power Supply Unit (PSU) is a square metal box which is connected to mains power from the back of the PC, and inside the PC is cabled to several major components, as well as to the motherboard which regulates this power to the remaining components. Thus the PSU is the primary source of power which allows the PC to function; if the PSU cannot provide sufficient stable power to the hardware components of a PC, it can cause erratic behavior or even a failure to start up.

Cooling Devices

Electronic components can generate a great deal of heat, especially when under heavy load. The hardware components in a PC most susceptible to heat buildup, such as the CPU and GPU, come with cooling solutions designed to dissipate the heat into the surrounding air. The two most common types of PC Cooling solutions used are:

A Heatsink is a square or rectangular solid metal object typically with a perfectly flat surface on one side, and multiple spines, fins or rods on the other side(s). The role of a heatsink is to sit on top of the component to be cooled, and draw out the heat from the component through conduction. This heat then travels along the heatsink until cooler air and a large surface area help in accelerating the dissipation of the heat.

A Fan is designed to draw in cold air or expel hot air. Fans can either be employed on their own, such as case fans which simply suck in or blow out air from a PC case; or they can be mounted on or near heatsinks to assist in more rapidly removing the heat drawn out from hardware components. The larger the fan and/or the faster it rotates, the greater the volume of air it can move, hence the greater the potential cooling, at the cost of additional noise.

Other forms of cooling, such as Watercooling, are much less common due to their additional cost, risk and complexity.

Copyright © 2010 Koroush Ghazi

CASE

The PC Case is a hardened structure, usually made of thin but strong metal and/or plastic, which encloses all the PC components and onto which the motherboard is firmly attached. The case provides the basic framework required for holding together and protecting all the components of a modern PC. However a case also increases the potential for heat buildup around components, and can also trap dust which can cause hardware to overheat and malfunction if not cleaned out regularly.

PERIPHERAL

Peripheral is a general term referring to any device attached or used externally to a PC, such as a mouse, keyboard or printer for example. The term specifically indicates that the device tends to lie on the periphery - that is, the outside - of the PC case. The only thing peripherals have in common with each other is that they provide additional input and output capabilities to a PC.

OPERATING SYSTEM AND SOFTWARE

The Operating System (OS), such as Windows Vista, is a vital piece of software - a compilation of instructions that tells all the hardware and software components in a PC how to function to achieve particular outcomes in a unified manner. An OS is a necessity on all modern PCs since without an overarching program to provide core functionality, all the computer components would not be able to function as a single machine. The OS also provides the main interface for users to interact with the PC hardware and software.

Software is a more general term, referring to a collection of programmed instructions which through interaction with hardware provide various functionality on a PC. While the OS itself is part of the software on a PC, and provides a great deal of functionality, additionally installed software provides further functionality to perform more specialized tasks, such as word processing or gaming.

Hopefully the information in this chapter has helped you to better understand common technical terminology used throughout this book. I encourage you to research further about any particular concept or component which may confuse or intrigue you, as it is important to have a solid grounding in the basic concepts and terms before moving on to more advanced material. The better you understand the basics, the more readily you will grasp the more complex topics covered in this book.

Copyright © 2010 Koroush Ghazi

SYSTEM SPECIFICATIONS

The first step in optimizing or customizing your PC is to find out precisely what hardware components you have, and what their various capabilities are. This is known as your System Specifications, and to find out the specific details of your hardware you will require an appropriate set of tools. Information about your system specifications is vital both for using this book and for general PC usage and maintenance in the future. For example you must know the model and chipset type of your motherboard before you can upgrade your BIOS or install the correct motherboard drivers; you must know the full capabilities of your graphics card if you want to know if it can run Aero, to update its drivers, or to see whether it can run the latest games; or you may have a complex problem which you wish to resolve yourself, or provide details of to a Technical Support person. This chapter covers the tools you need and the methods you can use to obtain all the relevant system information.

< SYSTEM INFORMATION TOOLS

There are a range of good free system information utilities to choose from, including some comprehensive ones built into Windows. A combination of these programs will tell you everything you need to know about your system specifications and capabilities:

WINDOWS SYSTEM INFORMATION TOOL

You can access the Windows System Information Tool by going to Start>Search Box, typing *msinfo32* and pressing Enter. The Windows System Information Tool presents a range of basic information about your system. Some of its more useful functionality includes:

§ A listing of your hardware components by type under the Components section.
§ All the system driver files and their current status under Software Environment>System Drivers.
§ IRQ allocations under Hardware Resources>IRQs.
§ Check for shared IRQs and other potential conflicts under Hardware Resources>Conflicts/Sharing.
§ Recent Windows errors are found under Software Environment>Windows Error Reporting.

In general the System Information Tool is best used by medium to advanced users who can comprehend the more complex interface and detailed information much more easily than a beginner. Its main advantage is that it is a free built-in utility that anyone can easily access.

PERFORMANCE & INFORMATION TOOLS

Windows Vista contains several tools which provide performance and diagnostic information about your system. These can be found under Control Panel>Performance Information and Tools>Advanced Tools and include the Task Manager, the Reliability and Performance Monitor, the Windows Memory Diagnostics and the Generate System Health Report items. These tools are very useful in both providing more detailed information about your system, and more importantly for allowing you to undertake troubleshooting/diagnostics. They are covered in detail under the Performance Measurement & Diagnostics chapter.

Copyright © 2010 Koroush Ghazi

DEVICE MANAGER

You can access Device Manager under the Windows Control Panel, or by going to Start>Search Box, typing *device manager* and then pressing Enter. As a built-in Windows utility you can gain a great deal of useful information about your hardware and associated drivers from this tool. Your major devices are displayed under various categories, and you can even choose to update individual device drivers or uninstall a device altogether should you wish. The Device Manager has several important roles and is covered in more detail under the BIOS & Hardware Management chapter.

DIRECTX DIAGNOSTICS

You can access the DirectX Diagnostic Utility (DXDiag) by going to Start>Search Box, typing *dxdiag* and pressing Enter. DXDiag is another built-in Windows Diagnostic/System Information tool that is part of the DirectX API (See the Graphics & Interface chapter). The main tab of DXDiag, called System, displays basic information about your system such as your Processor (CPU) type and speed, amount of Memory (physical RAM) and the Pagefile (Virtual Memory) usage among other things. Under the Display, Sound and Input tabs you can find more information about the particular hardware you are running for each of these functions. In particular you should ensure that all the DirectX Features listed are Enabled. If they are not, they can't be changed here however this indicates that there may be an issue with your hardware or drivers - see the Windows Drivers chapter for more details.

The most useful function for DXDiag is its ability to generate a detailed text file with all your major system information, including your main hardware specifications, driver files, and environmental settings. To create this text file click the 'Save All Information' button found at the bottom of the main DXDiag screen. You will be prompted to save this report somewhere, and the default of the Windows Desktop is fine. You can now double-click this *DXDiag.txt* file to read through its contents. It can also be attached to an email you can send to a technical support person, or its contents can be copied and pasted onto an online forum to allow others to help you with any problems you may be experiencing. It doesn't contain any information such as serial numbers or passwords, so it is safe to post publicly.

3DMARK

You can download the latest version of 3DMark from the Futuremark Website, and you can read more about its main functionality under the Performance Measurement & Diagnostics chapter. 3DMark is primarily designed as a graphics benchmarking utility, however it has a system information section that gives you a brief snapshot of major system information. Make sure to select the Custom installation option and untick all unnecessary components except the 'Shortcut on Desktop' option. You will also need to obtain a free registration key via email to use this program. Start 3DMark and on the main screen click the System Info tab, then click the 'View System Info' button and a browser window will open with a range of information about your system. Generally it is best to go to the trouble of setting up 3DMark if you are also considering using it as a 3D benchmark - as covered in the Performance Measurement & Diagnostics chapter.

SIW

SIW is the System Information for Windows tool which can be downloaded from the SIW Website. Once you've downloaded the standalone version of the program, you can simply run it from the file - there's no need to install anything. The interface is intuitive; click items in the left pane to see more details about them. For example, to find out more about your motherboard, click the Motherboard item under the Hardware section, and the details will be shown in the right pane. Alternatively, you can access each item by going to the Software or Hardware menus at the top of the screen. Note that SIW also has a range of other tools built into it, but I don't recommending changing anything using them - the best use for this utility is simply for viewing system information.

Copyright © 2010 Koroush Ghazi

SANDRA

Sandra stands for System ANalyser, Diagnostic and Reporting Assistant. You can download Sandra from the SiSoftware Website - the Lite version is free, and once installed, you will see a wide selection of information and benchmarking modules to choose from. Note that during installation of Sandra, you can disable the Remote Network Services, Price Engines and Rank Engines as they are not critical, however the Rank Engines option does allow Sandra to display a comparison of your score with others who have run the benchmark, which can be useful. If you've enabled the Rank Engine, after installation you can customize it so that your results aren't made public for example. Note that Sandra installs a new Service for itself called the 'SiSoftware Deployment Agent Service' which you should leave at its default of Manual.

Sandra Lite has many inactive (grayed out) modules, however the main ones we need have sufficient functionality for our purposes. For example, if you want to know more about your system, double-click the Hardware icon (or select the Hardware tab) and then double-click on the Computer Overview module. It will display a range of useful information about your system, such as the CPU speed and type, your motherboard Chipset, and your Memory Module brand and speed. If you then want to know more about your motherboard in particular for example, open the Mainboard module, and it will display more detailed information. Sandra also has several useful benchmarking and stress testing features that are covered in more detail in the Performance Measurement & Diagnostics chapter.

CPU-Z

A highly recommended tool, you can download CPU-Z from the CPU-Z Website. Run the program and it will provide you with all the major information you require about your hardware. It has highly detailed information about your processor under the CPU and Caches tabs, such as the CPU brand, socket type, speeds and voltage, and the various cache sizes. It also provides key motherboard details under the Mainboard tab, and your RAM's complete details under the Memory and SPD tabs, although note that for information to appear under the SPD tab you must first select the slot(s) on the motherboard that your RAM stick(s) occupy. CPU-Z even provides details about your graphics card under the Graphics tab, as well as PCI-E link speeds under the Graphics Interface section of the Mainboard tab.

GPU-Z

Another highly recommended tool, you can download GPU-Z from the GPU-Z Website. Note that GPU-Z is distinct from the CPU-Z utility covered above; it relates to your GPU (Graphics Processing Unit), which is typically your graphics card. Run the *GPU-Z.exe* file, and much like CPU-Z, it will provide you with all the information you need to know about your graphics card. Under the main Graphics Card tab you will see all the specifications for your graphics hardware, including the amount and type of Video RAM, the level of Direct X support, the BIOS version and the clock speeds. Under the Sensors tab you will find your current clock speeds, temperatures, fan speed and so forth. Finally, note that the Validation tab is there only if you want to submit your specs to the GPU-Z Statistics Database, which is not essential.

HD TUNE

HD Tune is a tool for quickly gaining an insight into your drive details and current capabilities. The free (non-Pro) version has sufficient functionality to provide important drive details including a list of supported features, the drive standard, firmware version, serial number, as well as the current temperature of the drive and the health of the drive. It even includes a benchmark, which is covered under the Performance Measurement & Diagnostics chapter.

There are many other system information tools which are available, some of which are not free. However a combination of the tools in this section should be more than enough to give you all the details you need for every aspect of the hardware that is in your PC. I strongly encourage you to make sure that you are fully

Copyright © 2010 Koroush Ghazi

aware of your hardware specifications and capabilities, as incorrect knowledge can cause major problems when you try to install drivers or make changes in software or the BIOS for example. Also make sure you are familiar with the contents of the Basic PC Terminology chapter in this book.

< PROVIDING SYSTEM SPECIFICATIONS

If you ever require technical assistance for a computer-related problem, you will inevitably have to provide your system specifications. Whether to a qualified technical support person, or for computer enthusiasts on an online forum, you should provide your specifications in an appropriate format. Simply copying the entire contents of a DXDiag text file for example might be quick and easy, but few people have the patience to wade through it, so I recommend using the format shown below unless instructed otherwise.

Also bear in mind that no-one can magically solve a problem simply by looking at your system specifications, no matter how detailed. There is no real substitute for becoming extremely familiar with your own system, for a range of reasons beyond simply troubleshooting problems.

Use several of the system information tools covered above to fill in the appropriate details in the categories shown below. The more detail you can provide, the better - the bare minimum is the brand and model number of your major components, but you should add in details like whether any of the components are overclocked or physically modified in any way. I have filled in some sample information from my own system in italics:

CPU:	*Intel Core i7 920 CPU @ 2.66GHz, stock speed, stock cooling*
Motherboard:	*Asus P6T Deluxe X58*
Graphics card:	*Leadtek Nvidia GeForce GTX 285 1GB, stock speed*
Monitor:	*24" Samsung 2443BW LCD*
Sound Card:	*Onboard ADI AD2000B HD Audio Chipset*
RAM:	*6GB (3 x 2GB) G.Skill 1333MHz DDR3*
Storage Drive(s):	*Western Digital 150GB VelociRaptor SATA2* *Western Digital 74GB Raptor SATA*
Optical Drive(s):	*Pioneer DVD-RW 216BK SATA*
Power Supply:	*Seasonic 700W M12*
Operating System:	*Windows Vista Ultimate 64-bit, including latest Windows Updates*
Other Details:	*195.55 Nvidia Forceware graphics driver* *6.10.0002.6585 SoundMax HD Audio sound driver* *System not overclocked, not physically modified*

You can also provide details of your other hardware, such as the keyboard, mouse, speakers/headphones and case, however these are usually not critical to solving most PC problems, at least not in the first instance.

I must stress again that it is an extremely important element of PC optimization and customization that you have more than just a passing acquaintance with your hardware components. Becoming familiar with hardware specifications and what they mean not only allows you to discover areas of potential optimization on your system and assist with troubleshooting problems, it also gives you the ability to make better purchasing decisions when buying a system or upgrading any hardware components in the future.

Copyright © 2010 Koroush Ghazi

BACKUP & RECOVERY

Computers can store a great deal of valuable information. Over time your PC may come to hold a lot of important, private, irreplaceable data such as digital photographs, home movies, financial documents, emails, bookmarks and login details. It is of critical importance that you establish an appropriate method for regularly backing up this information, so that if your PC is stolen, damaged, or its data is corrupted or accidentally overwritten, that you do not lose all this valuable data permanently. Hence backing up is a vital and unavoidable part of sensible computing.

This chapter not only covers various backup strategies and tools, it also details a range of useful data recovery methods you can use to regain valuable information which has been lost through forgetting passwords, accidental deletion of files, data corruption or damage to your Windows installation. You should have at least one backup copy of all your important and irreplaceable data proceeding any further with this book. If you already have a recent backup of all your important data, you can skip to the next chapter and return to this chapter at a later point.

< BACKUP AND RESTORE CENTER

Windows Vista's Backup and Restore Center allows you to either create backups of particular files, or create a complete backup image of your system drive(s), as well as a means of restoring these backups at a later date. To access the Backup and Restore Center, go to Start>All Programs>Maintenance, or to Start>Search Box and type *backup restore* and press Enter. The Backup and Restore Center dialog box will open, giving you two main options for backing up (or restoring) your data: either as a range of files, or as an entire image of your system drive(s). Each option is covered below:

BACKING UP FILES

This option backs up only particular files from your system. This takes up far less space than the 'Back Up Computer' option, and also allows you to selectively back up and restore certain file types. However it is still much less precise than a manual backup, typically including a lot of files you don't wish to back up. This is because Vista does not allow you to select the specific files and folders you want to back up, only files of a certain type. For example, if you want to back up all Pictures and Music and select these categories, then aside from any pictures and music you've created, saved or downloaded, it will also back up all image and music files from other folders such as those under the *\Program Files* directory (e.g. game music and image files). This can obviously take up a great deal of additional space to backup, so I only recommend using this option if you prefer its automated nature and don't mind its lack of control. A manual backup is the preferred method of backing up specific files/folders in a more efficient manner (see further below).

When you select the 'Back Up Files' button, Vista first asks you where you wish to backup the files to, either a CD, DVD or another drive, or to another Network location if applicable. I recommend that you back up your files to rewriteable DVD regularly, even if you also backup to another drive as well. I don't recommend only backing up the files to a partition on your main Vista drive for example, because for example if your main Vista drive fails, all partitions on it will also be lost. So on balance a combination of another drive and also DVDs is recommended for total safety.

Once you've made your selection, you will be prompted as to which drive(s) you wish to backup files from. Your current Vista system drive will be selected automatically and cannot be unselected; select other drives if you wish. The next screen shows the specific types of files you may want to back up. As noted, a major drawback is that Vista does not allow you to select specific directories or files to backup, merely the broad category of files. By clicking on the name of each file type here you can see the kinds of files which will be

Copyright © 2010 Koroush Ghazi

backed up from your chosen drive(s). Files which will not be backed up regardless of the categories you choose include:

- System files - The files that Windows needs to run.
- Program files - Mainly .EXE and .DLL files; other portions of program files will be backed up depending on their type.
- Files stored on disks that are formatted using the FAT file system.
- Web-based e-mail that is not stored on your drive.
- Files that are in the Recycle Bin.
- Temporary files.
- User profile settings.
- Files that have been encrypted using the Encrypting File System (EFS).

Once you've selected the file types you want to back up, Vista will assume you want to automatically do this on a recurring basis, and asks you to schedule a regular time for automatic backups each day, week or month. Note that scheduling automatic backups is not possible in Vista Home Basic, though it will periodically remind you to back up manually. To turn off automatic backups, or indeed alter any backup files settings, open the Backup and Restore Center, click the 'Change settings' link below the 'Back up files' button. Then you can click the 'Turn Off' button at the bottom of the next screen to disable automatic backups, and/or if you want to change the backup settings you can click the 'Change Backup Settings' option. Note, to get back to this configuration screen quickly at any time, you can type *backup status* in the Start>Search Box and press Enter. If you want to permanently disable scheduled backups altogether, see Task Scheduler under the Administrative Tools section of the Control Panel chapter.

Once done with the configuration, the 'Create a new, full backup' option should be ticked, now click the 'Save settings and start backup' button. You will be prompted to insert/format any disks required until the backup is completed. If you need to manually format a DVD or hard drive at this point, open Windows Explorer, right click on the relevant drive letter, and select Format or 'Erase this Disk' as applicable. If you attempt to create a backup which requires more space than you have available on your target drive (e.g. the backup requires 5 DVDs and you only have 4), then you can resume the backup process at a later date by running the 'Back up files' option and it will continue from where it left off. If an automatic backup fails due to lack of disc(s), it too can be resumed the same way.

The first time the Backup Files function runs, it automatically creates a full backup of all your selected file categories, this may time quite some time. Vista then starts keeping track of which of your selected file types across your chosen drive(s) have been modified or newly created, and in future when you return to the 'Back up files' option you will be given the option of creating another full backup, or simply creating an incremental backup of new/modified files only. You can also choose this by clicking on the 'Change settings' link, and either selecting 'Back Up Now' to find new/updated files to add to your backup, or 'Change backup settings' to alter the settings and/or create a new full backup. Using the incremental method makes backing up much faster and easier, so it is recommended.

When using Windows backup features, backup files are saved in a special format on your target drive/disk, in the form *Drive Letter:\<computer name>\Backup Set <year-month-day> <time>\Backup Files <year-month-day> <time>.* The actual files themselves are stored in a set of archived .ZIP files, which you can open and view/extract the contents of with an archival utility like WinZip or 7-Zip. However to properly view and restore these backed up files you should use the option below.

RESTORING FILES

If at any time you want to restore or simply view any files and folders backed up via the 'Back up files' option, then you should go to the Backup and Restore Center and click the 'Restore Files' button. You can then select to restore the file(s) from the latest backup you made, or from an older backup. I recommend

Copyright © 2010 Koroush Ghazi

clicking the 'Advanced restore' link instead as this provides additional options, including the ability to restore a backup of files made on another PC. On the next screen, click the 'Advanced Restore' option. If your backups were made on another PC, select the 'Files from a backup made on a different computer' item; if you've made several backups of the files on this PC but you want to restore an older version of a file, select the 'Files from an older backup...' option. Finally the most common option is to restore the latest version of the files which you've backed up by selecting the 'Files from the latest backup...' item. Click Next when done.

On the next screen, if you chose to restore an older backup you can select the date of the backup made and insert the appropriate disk if required before proceeding. If the files were backed up on a different computer, connect or insert the disk(s) required and then continue. If you're using the latest backup, make sure you insert the appropriate disk(s) if required.

To restore particular files or folders, select the 'Add Files' or 'Add Folders' option as appropriate and browse to the 'Backup' folder in the file browser on the left side of the dialog box. You should see the backed up drive letter shown with a listing of the files and folders which have been backed up onto this particular drive or disc. Highlight each of the particular files/folders you want to restore and click the Add button at the bottom of the box. If you want to restore the entire backup, tick the 'Restore everything in this backup' box at the top of the screen instead. Once done, click the Next button and nominate a location to restore the file to. You can either have the backed up version of the file overwrite the current version on your Vista drive (not recommended), or you can restore it to another location to prevent it overwriting the existing version - this is the option I recommend just to play it safe, in case you restore the wrong backup, or the backup itself is somehow corrupt or infected. Restore it to another location, delete your current version to the Recycle Bin, then move the newly restored files to their original location and see if they are fine.

BACKING UP THE ENTIRE COMPUTER

Backing up specific file types is a useful but not foolproof way of making sure you don't lose valuable documents in case of a drive failure or severe malware infestation for example. It prevents total data loss but it is still time consuming to have to reinstall Windows and reconfigure everything back to the way you want it after a major problem. Therefore Vista allows you to make a backup image of your entire system drive, backing up every file and detail such that you can restore your PC to the exact same state at any time. Unfortunately this method does not allow you to selectively choose particular files or folders to backup or restore - you will be backing up/restoring your entire PC in every way. If you have a dual boot arrangement, this also includes the other version of Windows you're using as well, which can take up quite a bit of space. Note that this function is not available in Vista Home Basic or Vista Home Premium - for alternatives to Vista's drive imaging method, see further below.

To start the process click the 'Back up Computer' button in the Backup and Restore Center, and as recommended, select another drive/partition to back up to. If you don't have any other drives, you can select DVDs though this obviously requires quite a number of them. Regardless of where you choose, on the next screen you will be given a rough estimate of the amount of space required, the drive(s) which are to be backed up, and you can then commence the process by clicking 'Start Backup'. Depending on the size of your current Window installation(s) and all programs installed, this could take quite a while.

This method is only recommended in conjunction with other automatic or manual backups of your specific valuable files. This is because if you wish to restore your computer backup, it will completely overwrite your current Vista install, and if you have a dual boot, it will also completely overwrite your other version of Windows as well, with the version you backed up earlier. Clearly this is overkill just to restore a single lost file for example, and also may mean you lose other data which was created or modified after your previous entire computer backup. So on balance this method is recommended more for recovering from a catastrophic failure like a total drive failure/corruption, or a severe malware infestation, and also requires that you regularly maintain the entire computer backup to keep it up to date.

Copyright © 2010 Koroush Ghazi

RESTORING THE ENTIRE COMPUTER

If you want to restore an entire computer backup image, click the 'Restore Computer' button and you will be given the instructions on how to do this. Basically restoring a computer image cannot be done while you are already running Vista or another version of Windows, so it needs to be done prior to the OS starting up. It requires that you reboot, enter the recovery options and select the 'Windows Complete PC Restore' option. For full details of how to access your recovery options and how to use them, see the System Recovery section further below.

Remember, you cannot restore particular files or folders using this type of a backup, it only allows you to restore your entire computer setup to the state it was in when you last backed it up using the 'Back up computer' option. All the drives you made a backup of will be completely reformatted, losing all existing data on them, and the backups are then restored over them. If you had a dual boot arrangement, this will be restored, however once again that means that any other operating system you were using along with Vista will also be deleted and returned to the state it was in when you last backed up your entire computer.

Clearly this method is only recommended if you either have no other backups of important information, you have suffered a catastrophic failure such as total drive corruption or a severe malware infestation which has compromised a great deal of your current data. If this not the case then I recommend attempting other forms of system repair or recovery first, as covered further below.

< SYSTEM PROTECTION

Windows Vista attempts to ensure that you don't accidentally delete your files or have them unintentionally altered without some form of backup. To that end, Vista's System Protection features, enabled by default, automatically back up previous versions of your files regularly. These backups are known as Shadow Copies, and they are automatically created on a daily basis for files which have been altered, as well as being created whenever you use the System Restore feature to create restore points, or when you use the automated Backup features of the Backup and Restore Center. To access the System Protection settings, go to Control Panel>System and click the System Protection link in the left pane, or go to Start>Search Box, type *systempropertiesprotection* and press Enter.

I recommend that all of these functions be enabled initially until you can get a better idea of the types of backup strategies you wish to use for your system. The use of these features primarily impacts on drive space and does not have any significant performance impact. Given it may help prevent the loss of important documents and/or get you out of trouble if you have system issues, I believe on balance this makes them worth keeping enabled. There is some scope to customize these features, and we look at the various specific features of System Protection below.

SYSTEM RESTORE

System Restore is not a general backup and restore utility, and should not be mistaken as one. It does not back up or maintain any copies of your personal files, such as your emails, pictures, documents or music. Instead it tries to track and save information specifically related to system-level changes, such as Windows system files which are changed due to driver installations, and alterations made to the Windows Registry by programs. It is thus useful as a general system state backup and recovery tool. Enabled by default, System Restore relies on 'Restore Points' which are a snapshot of your system state at a point in time. Restore points can be created manually by you at any time, as well as being created automatically on a daily basis and also just prior to major system events like the installation of drivers or Windows Update patches.

To open System Restore, go to System Protection and click the 'System Restore' button, or go to Start>Search Box, type *rstrui* and press Enter. On the main dialog box for the utility, you will be presented with a link to go to the System Protection screen if you want to manually create a restore point. I strongly recommend manually creating at least one restore point after you have installed Vista and prior to conducting any

Copyright © 2010 Koroush Ghazi

detailed tweaking. Go to System Protection and click the Create button, then give the restore point a suitable name and click Create.

To use a restore point to return your system state to the way it was when that point was created, follow these steps:

1. Open System Restore, and if any restore points exist, you will be able view the last restore point, and the date it was created. If you just want to see all available restore points, select the 'Choose a different restore point' option and click Next.
2. To restore a specific restore point, highlight that restore point and click Next. You will be shown the drive(s) to which the restore point applies, and you can then click Next, and on the next screen confirm that you wish to use that restore point.
3. Your system will restart and your system files will revert to the way they were at the time of the restore point. You will be notified if the restore was successful. Your personal files will not be altered.
4. If you find that using the restore point was no help at all, or made things even worse, you can undo the use of the restore point by opening System Restore again, clicking Next to view the list of restore points, and selecting the 'Undo: Restore Operation' item, click Next and follow the prompts. Note that this option is not available if you use System Restore in safe mode.

If you wish to turn off System Restore, go to the System Protection screen and untick all the available drive(s) you wish to disable this functionality for, then click Apply. Note however that this also removes all existing restore points and turns off the general System Protection functionality. This is not recommended unless you are genuinely a very advanced user who does not experience system issues often and you also regularly create backups of all important files.

System Restore uses up to 15% of drive space on each drive on which it is enabled, and requires a minimum of 300MB of free space to work properly. Over time System Restore will delete older restore points automatically so as not to exceed its size limit. However if you want to save disk space, you can manually delete all older restore points except the very latest one at any time by using the Disk Cleanup utility - see the Cleaning Windows chapter for details.

PREVIOUS VERSIONS

Although System Restore does not restore copies of your personal files as part of a restore point, the System Protection feature ensures that Shadow Copies, also known as Previous Versions, are automatically created for most non-system files during the creation of restore points. As long as you keep System Protection enabled on a particular drive, then shadow copies will also be made of relevant files whenever they are altered. While shadow copies are not a substitute for taking proper backups of your important files, this is one of the added safety features in Vista to help prevent accidental deletion or alteration of important files of all types, which is why it is again recommended that you do not disable System Protection on your main Vista drive.

Just to be clear: the main difference between System Restore and Previous Versions is that System Restore is used for backing up and restoring system-related files, while Previous Versions is for backing up and restoring personal and other non-system files. Previous Versions of Windows system files (e.g. those under the *\Windows* directories) are not kept.

Copyright © 2010 Koroush Ghazi

To view and/or restore the existing Previous Versions of any file, do the following:

1. Open Windows Explorer and browse to the selected file.
2. Right-click on the file and select 'Restore previous versions', or alternatively right-click on the file, select Properties and click on the 'Previous Versions' tab - both have the same effect.
3. Under the Previous Versions tab you will see all available previous versions listed in order of the date upon which the file was last modified, not the date it was saved. Note the Location field - if the file has been saved as part of a Shadow Copy on your drive, it will be listed as such; if it was backed up using the Backup and Restore Center, it will be listed as a Backup.
4. To restore a previous version, highlight the version you wish to restore and click the Restore button. Shadow copies are stored on your main Vista drive and will be restored immediately, whereas Backup copies will be stored on another medium such as another hard drive and require you to have that particular medium connected or inserted before the restore can be completed.
5. If restoration is possible you will be asked to confirm the task, and if you agree, the file will be overwritten with the earlier version.

Note that on Vista Home Premium and Basic editions, Shadow Copies are made but the Previous Versions interface is not available. To access Shadow Copies in these versions of Vista, you will need a third party tool like ShadowExplorer.

Again, while Previous Versions is a very useful Vista function, it is not a substitute for taking proper backups regularly of your irreplaceable personal files. Depending on the amount of drive space you have available and the number of files on your system, over time you will lose older previous versions.

RESIZING SYSTEM PROTECTION'S RESERVED DRIVE SPACE

As noted previously, the System Protection functionality requires at least 300MB of drive space, and can use up to 15% of your total drive space on your Vista system drive. If you wish to manually alter the amount of drive space used by System Protection and its associated features including System Restore and Previous Versions, you can do so as follows, though this is only recommended for advanced users:

1. Open an Administrator Command Prompt.
2. In the command prompt that opens, to see how much space is currently being used by System Protection, type the following and press Enter:

   ```
   vssadmin List ShadowStorage
   ```

3. Now to resize the amount of space allocated to System Protection, type the following command, changing the main parameters to suit your specific needs:

   ```
   vssadmin Resize ShadowStorage /For=C: /On=C: /MaxSize=900MB
   ```

   Where:
   /For= The drive letter for your main Vista drive;
   /On= The drive letter where the relevant System Protection backups are held, usually the same drive;
   /MaxSize= Specifies the maximum amount (preferably in MegaBytes (MB)) allowed to be allocated to System Protection, with the minimum allowable value being 300MB.

4. Once you've used the appropriate parameters for your own system and typed up the command, press Enter and the amount of space used will be immediately resized as requested.

Note that by reducing the maximum amount of space usable by System Protection, you may lose older restore points and shadow copies, and if set too low this may make System Protection effectively useless by not being able to protect all your important system files and provide sufficient previous versions of all your

Copyright © 2010 Koroush Ghazi

files. I would recommend you set at least 2GB of drive space, preferably more if you have more files on the drive and/or you've nominated more than one drive to be protected. If in doubt, do not alter this setting. In the end if you really resent the space taken up by System Protection features, or just don't have the space to spare on your drive, then it may be best to simply disable System Protection for that drive altogether. This is not recommended of course, but if you do decide to do this then you must make sure to regularly backup all your files often.

< OTHER AUTOMATED BACKUP METHODS

Aside from the automated backup methods built into Windows Vista, there are other ways you can create and maintain backups in a relatively automated manner.

THIRD PARTY DRIVE IMAGING SOFTWARE

There are third party programs available which can provide features similar to the 'Back Up Computer' imaging option in Vista. The two major software packages for imaging drives quickly and easily are Norton Ghost and Acronis TrueImage. However neither is free, so they will not be covered here in any detail - refer to the relevant Norton Ghost Manual or the Acronis TrueImage User Guide for more details. The main benefit of third party imaging utilities over Vista's built-in system imaging option is that firstly the Vista utility is not available on Vista Home Basic or Vista Home Premium, and secondly because Vista's built-in drive imaging program does not allow selective backup and restoration - it backs up and restores everything. Therefore you may consider one of the utilities above as a valuable investment, as they allow greater flexibility in choosing what to backup and restore.

ONLINE BACKUP

Online backup services allow you to back up data to a secure location, typically a remote data center. This ensures that your data is encrypted and stored safely, but this not a free service, so it is only recommended if you genuinely need that level of protection against data loss or theft. This form of backup is not absolutely necessary for the average user, but it provides additional security and peace of mind, particularly in the event of fire or theft, whereby your PC and your onsite backups may all be destroyed or stolen, leaving you with nothing to rely on for restoring your data. For the average user however there are several ways of using free online services to provide added security against such data loss:

ISP Storage: Many Internet Service Providers (ISPs) provide their customers with a basic web space to which you can upload personal data. This is a relatively secure and typically free method of storing your data offsite - check your ISP's website or contact them directly for further details. Even if a small fee is involved in obtaining such a facility, it can be worthwhile given the added protection it provides you as another location to store your backups.

Email Storage: Free email services such as Gmail provide extremely large amounts of storage space - in the order of several Gigabytes. While I do not recommend uploading/emailing any sensitive data to these locations, as they are not completely secure, they do serve as good holding spots for additional backups of digital photos and other important irreplaceable files. In fact you can use free utilities such as GSpace or Gmail Drive to make storage of data on a Gmail account much easier to manage, though bear in mind that Gmail and other free email providers may take steps to prevent this practice if it becomes widespread.

Photo Storage: There are a range of free photo album providers which will allow you to upload and keep a large library of digital photos, which is extremely useful again as yet another place to store photos which are otherwise irreplaceable in case your originals are ever lost. The most popular free photo gallery providers are Flickr, Photobucket and Picasa. Make sure to read the instructions for the gallery and enable all the privacy features so that members of the public cannot view your gallery contents without your permission. Regardless of such features, a direct link to a particular photo can often be publicly discovered, so I do not recommend uploading sensitive photos to such galleries.

Copyright © 2010 Koroush Ghazi

Ultimately, if you believe your data is worth preserving against all eventualities, or you need to store it with maximum security, it is necessary that you consider a professional remote data storage service to hold your backups. The free options while convenient do not provide sufficient security against unauthorized access. Of course most Windows users do not require this level of protection; regularly taking backups and also keeping a copy of your backups in a fireproof safe for example is sufficient protection.

< MANUAL BACKUP

The following is a list of tips for creating a manual backup of your data and settings in Windows Vista. There are methods that can be used to create automated backups of your system which are covered above, however I personally use the manual method regularly to ensure I have a 'clean' backup copy of all my important files, especially if I am going to do a reinstallation of Windows. Any automated backup utility you use may inevitably backup the problematic or sub-optimal settings you were trying to escape in the first place, or back up a range of additional files you don't need, so a manual backup is strongly recommended especially if you are experiencing problems. You can combine this with an automatic backup as well if required, especially since Vista has a good built-in backup utility.

How precisely you do a manual backup is up to you; below are my personal methods for preparing data and manually backing up your important files regularly:

Directory Structure: Windows Vista has a much cleaner and more logical directory structure than Windows XP by default, with a set of personal folders named after each user account, found under your *\Users* directory. Under here are several clearly-named subdirectories: *Contacts*, *Documents*, *Downloads*, *Favorites*, *Music*, *Pictures*, *Saved Games*, *Search* and *Videos*. You are strongly encouraged to take advantage of this structure for a range of reasons as covered later in this book. Make sure you get in the habit of placing all your relevant files in the appropriate folders, creating sub-folders under them as necessary. Then any time you want to make a manual backup, all you need to do is backup your entire personal folder and all its subfolders. If you wish, you can create or use another partition or separate drive to store your files, or even move your personal folders there (see the Windows Explorer chapter), however again this still doesn't negate the need to regularly back them up to another medium in case of drive failure.

Internet Bookmarks: Your Internet Explorer bookmarks are automatically saved under the *\Users\[username]\Favorites* directory, and as long as you back this directory up as part of your manual backup strategy, they will be backed up as well. If at any time you want to export your IE bookmarks, you can do so by opening IE, going to the File menu>Import and Export>Export Favorites and select the appropriate folders - usually the top folder is best. Follow the prompts to export your Favorites to a suitable location under the default name *Bookmark.htm*. To import the Favorites back into Internet Explorer at any time go back to the Import and Export function and choose 'Import Favorites'. If you use a browser like Mozilla Firefox, you can backup your bookmarks by going to the Bookmarks menu, selecting 'Organize Bookmarks', then clicking the 'Import and Backup' button and choosing either the Backup or 'Export HTML' options.

Program Directories: Don't attempt to backup an entire program or game directory, as you cannot restore/reinstall a game or program in this manner - these will not run properly if they are copied back onto another installation of Vista due to the lack of appropriate registry entries and files spread throughout various other directories. You must use the original installation files/discs to reinstall a program or game correctly.

Saved Games: If you want to backup any saved games or game configuration files, these are typically held under the game's main directory in one of the subdirectories name *Saves*, *Savegames* or *Profilename*, and/or under your *\Users\[username]\Documents* directory, often under a directory with the name of the game. If

Copyright © 2010 Koroush Ghazi

you are having problems with a game, I don't recommend backing up the game's configuration files as it may just pass the problem onto your new install of Windows.

Usernames/Passwords: You can store all your usernames and passwords securely electronically - see the Backing Up & Restoring System Passwords section further below. If you have no interest in electronic storage systems then compile a written list/printout of the major usernames and passwords on your system. However you must then store this list safely in a physically secure place like a safe, and keep in mind that any time you write down or store your passwords in unencrypted format in any location you are facing a security risk if it falls into the wrong hands, particularly if you share your PC with other users.

Backup to Disk or Drive: Once you have determined the files to backup, you should regularly backup your important files/programs to another medium, such as another hard drive, a USB flash drive, or to DVDs. I certainly don't recommend backing up your files to another partition on your main system drive. I recommend rewriteable DVDs or a USB flash drive in particular simply because aside from ease of storage, it is easier to transfer data to any other PC via these mediums. When selecting which files to regularly back up, give top priority to files that are genuinely irreplaceable, such as digital photos and financial documents. Anything that has a high sentimental or monetary value should be backed up often, ideally to more than one location. Data which changes frequently should also be backed up more often.

Remember that the Previous Versions option does provide some level of protection against accidental deletion or modification of your personal files, and System Restore also allows you to undo the general system damage caused by other mishaps, but neither of these should be relied upon solely as your only backup procedure because they provide no protection against drive failure. Furthermore Vista's 'Back up files' option is quite imprecise in backing up your personal files and folders, so I recommend manually backing up the specific files which are important to you on a regular basis. Ideally you should use both Vista's automated backup features *and* manual backing up together, not just one or the other, but manual backups should be your first priority.

< BACKING UP THE WINDOWS REGISTRY

The Windows Registry is a critical component of Windows Vista, and any problems you experience with it can make Windows unbootable, or result in a variety of errors or strange behavior - see the Windows Registry chapter. For this reason it is important to have a backup of the Registry before undertaking any system changes. Specifically, prior to editing the registry manually at any time, you should make a backup of that portion of the registry - this is covered under the Windows Registry chapter. However you should also make full backups of the registry regularly to allow you to undo any recent changes which can cause problems with Windows. By default System Restore already maintains a snapshot of your registry at each restore point, and this is one of the main reasons why you should keep System Protection enabled on your system drive and create a restore point before editing the registry for example. However this is not a foolproof way of preventing registry corruption or unintended alteration.

To provide a layer of added protection, ideally you should regularly back up your entire registry manually as well. You cannot do this using the Export function in Registry Editor as that method is only handy for saving individual branches of the registry; unfortunately full registry backups made by Registry Editor will not restore correctly if your registry becomes corrupted.

Instead, I recommend you use a free utility called Erunt (Emergency Recovery Utility for NT). Download this program and install it with full Administrative privileges (or disable UAC). Note that during the installation of Erunt you should answer 'No' if asked whether you want Erunt to be placed in the startup folder, as this is unnecessary. To make a backup of the Windows Registry using Erunt, launch the program again with full Administrative privileges or with UAC disabled. You will be prompted to backup your registry to a folder, which you should accept by clicking Ok until the backup has been made. If you want to

Copyright © 2010 Koroush Ghazi

restore this backup at any point, simply go to the directory where the backup was made, typically *\Windows\ERDNT\[Date of backup]*, and launch the *ERDNT.exe* file there to restore that backup.

< BACKING UP & RESTORING PASSWORDS

One of the biggest headaches when running Windows would be losing your main login password, particularly if you're the Administrator on your machine. With the NTFS file system it is quite difficult to access the data on your drive without the correct login password (there is a method to reset this password - see further below). Clearly the best thing to do is back up your password now before anything happens, so that if necessary you can restore it without any difficulties. The recommended way to securely back it up is as follows, though note you will require a floppy drive or USB flash drive for this to work:

BACKING UP LOGIN PASSWORD

1. Go to Control Panel>User Accounts and click on your User Account.
2. Click on 'Create a Password Reset Disk' in the left pane. The Forgotten Password Wizard will open up. Click Next.
3. Insert a blank formatted 3.5" floppy disk into your A:\ drive or attach a USB flash drive and click Next. If you need to format the drive first, insert the floppy disk or USB drive, open Windows Explorer, right-click on the relevant drive letter and select Format.
4. Type your current User Password in the box and click Next. Once the disk has been created, click Next and select Finish. Store this disk/stick somewhere safe, as anyone can use it to access your account.

Note that some people may use any old 3.5" floppy disk they find to backup their password and often these disks are quite old. A floppy disk has an error-free life of 10 years on average, so I urge you to buy a small USB flash drive just for this purpose.

RESTORING LOGIN PASSWORD

If you ever need to restore your password from the backup created above, follow these steps:

1. Boot your PC as normal, and on the Windows Login screen select your User Name.
2. Try entering your password (or just press Enter), and if it's incorrect you'll get a message saying the Username or Password is incorrect. Click OK and then select 'Reset Password', inserting the password reset disk or USB flash drive you created earlier.
3. Follow the Password Reset Wizard to set a new password and log back into your system.

Note that the password reset disk needs to be write-enabled so that Windows can update it with the new password automatically during this procedure. When done, you should once again put it away in a physically secure place. Note further that if you have another user who is an Administrator on your PC, they can log in and change the password for your account. However this method will prevent you from accessing any existing encrypted files or folders for your account, so it is strongly recommended that you use the password reset disk method above instead. It is the best precaution against a lost account password.

RECOVERING LOGIN PASSWORD

If you've completely lost your login password, you don't have a password reset disk, and you don't have any other Administrator who can reset it for you then generally you're in a lot of trouble. Usually you will have to simply reformat and reinstall Windows.

However if you are really desperate to regain access to your user account and you have the time, you can try the Offline NT Password & Registry Editor for cracking your Windows account password. I am providing this information in good faith for users who want to restore their own account, not to attempt to hack other accounts. If you are alarmed at the existence of cracking tools and methods for getting account passwords in

Copyright © 2010 Koroush Ghazi

Windows then I strongly recommend that firstly you set your user account password to something strong such as a 12 character (or more) base64 or base95 random password. For example, you can use this online Password Generator to generate one. These complex passwords are extremely difficult to crack, especially the more characters you use. Secondly and most importantly, I recommend that you restrict physical access to your machine to only those people you absolutely trust, and if in doubt, make sure to observe the use of your PC by others to ensure they don't use a tool like the one above to compromise your account's security.

Storing Passwords

If you simply want to hold all your usernames and passwords in a relatively straightforward central database protected by high level encryption, which also provides the ability to securely export and store the database for backup purposes, use the free KeePass Password Safe utility. There is both a Classic Edition and a newer version available to download. The differences in features are spelled out in this table, but for the most part all the functionality required, in addition to portability and smaller footprint, can be found in the Classic Edition (ZIP Package) version of this software, which is the one I recommend and describe below.

To use KeePass, launch *KeePass.exe* and select New under the File menu, then enter a Master Password and/or select a Key File. These measures are used to secure the password list, and while the key file is not essential, make sure to enter a master password which has a high bit-rate by using a combination of letters both lowercase and uppercase, as well as numbers, and not just a common word or name. This master password is a critical component - if you forget it, there is no way to unlock your password list. Once the database is created, you can populate it. The database is sorted by groups, which are simply categories of passwords. You can right-click in the left pane and add new groups, or add sub-groups under the existing groups, or remove any group or sub-group as you wish. Highlight the group which you believe your username/password combination is best stored under, and in the right pane right-click and select 'Add Entry' to create a new entry containing your username and password combination for a particular Windows feature, other software, or a website. Do this as many times as required to populate the database with all the username and password combinations you wish to store.

You can backup this password database to any location you wish by using the 'Export To' feature under the File menu. I strongly recommend exporting the database as a KeePass Database .KDB file. This database can then be stored or backed up wherever you wish, and its contents can only be successfully viewed by using KeePass to open the file and entering the correct master password. Because the database is encrypted, it is virtually impossible to access the database contents without the right password/key file.

There is also a built-in Vista Key Manager which you can access by going to Start>Search Box, typing *control userpasswords2* then pressing Enter. This opens the User Accounts Advanced screen - see User Accounts under the Control Panel chapter for more details. Under the Advanced tab click the 'Manage Passwords' button and you can then add login and password details for particular programs, websites or servers here, and they will be saved and used whenever you launch the relevant program, site or server. You can even backup and restore these credentials to another location. The Vista Key Manager is less secure though because unlike KeePass above there is no master password which blocks access to this utility.

Recovering Other Passwords

If you haven't properly stored your passwords and you've managed to forget or lose an important password which you can't simply reset, such as your Windows login password, there are utilities you can use to recover or crack these passwords. The best free tool which works in Windows Vista is Ophcrack, though you can also try the free Cain & Abel. However I cannot go into detail regarding these tools, as it is beyond the scope of this book. The presence of these types of tools should again let you see that nothing is completely safe on your machine, so it is very important to always restrict physical access to your machine only to those people you trust, and always follow the tips provided in the PC Security chapter, as well as the User Accounts section of the Control Panel chapter.

Copyright © 2010 Koroush Ghazi

< FILE DELETION AND RECOVERY

Accidental deletion of files is one of the most common ways in which files are lost. By default Windows Vista has some protection against this with its built-in backup features (see further above), and also not being able to easily delete a file for which you are not the owner (See the PC Security chapter). Furthermore, it's obviously wise to not only backup often but to also leave System Protection enabled, so that you have several different Previous Versions of a file to choose from in case the file is damaged (again see further above). You should also leave the Recycle Bin enabled and make sure that files are moved to the Recycle Bin when deleted - see the Cleaning Windows chapter for the details.

However in the end for one reason or another you may still wind up permanently deleting a necessary file, and have no previous backup, restore point or previous version available. Fortunately, when you delete a file from your system the file is removed from view and you regain the space on your drive, however it is not actually permanently deleted from your drive. In fact, nothing on your drive is permanently removed when you delete it. Whenever you delete a file Windows simply marks it for deletion. The entire file is still sitting on your drive, but is not visible. Windows then allows other files to write over the space where it resides if required, but the file is not completely gone from your drive until it is fully overwritten at some point. This means that you can sometimes recover files that have been 'permanently' deleted, but you need to act quickly and will require special software to do so.

RECOVERING DELETED FILES

Recuva: To use Recuva, after installing it you can simply follow the wizard which appears. For more options, click the 'Switch to advanced mode' button in the main Recuva window, or disable and exit the wizard at startup. Essentially once you specify the particular drive to scan, or all available drives if you so wish, you then specify the file type you're looking for - whether by using the drop-down list, or entering a portion of the filename (or leave the box blank for all files), and then click the Scan button. One of the benefits of Recuva is that it provides a preview of the recovered files wherever possible, making it easier to determine which may be the suitable one to restore. Another benefit is that Recuva can find and restore deleted emails. If nothing is found after a basic scan, you can opt for an in-depth scan if prompted, or click the Options button and under the Actions tab tick the 'Deep Scan' box and scan again, but bear in mind this could take quite a while.

Restoration: To use Restoration first download the file and run it to extract the contents to an empty directory, preferably on a USB flash drive or another drive. Then run the *Restoration.exe* file as an Administrator and either enter a filename in the search box, or a file extension (e.g. JPG, DOC, TXT), or leave the box blank (to find all recoverable deleted files) and click the 'Search Deleted Files' button. Restoration will scan your drive for files which can be restored and list them. Once done, you can highlight a file and click 'Restore by Copying' to recover it.

IsoBuster: If you want to recover deleted or damaged files on a CD or DVD disc, you will have to use a more specialized utility such as IsoBuster. While it can be downloaded for free, IsoBuster requires paid registration for full functionality. However you can use the free version to first check to see if there is any recoverable data on your particular disc. There is no guarantee that any usable data can be recovered from a damaged or deleted disc - particularly if it has been overwritten.

Regardless of which tool you use, the more activity there is on the medium where the deleted files reside, the less chance you can fully recover them, since portions of it may have been overwritten by new data. This is why the files recovered by any tool are often not complete since portions of them have already been overwritten, so there is no guarantee you can recover a usable file this way. For this reason, if you have accidentally deleted an important file, try and minimize any further activity before running a data recovery utility. If you can't run a recovery utility straight away it is best to shut down Windows immediately to

Copyright © 2010 Koroush Ghazi

prevent a background task from commencing (e.g. a scheduled defragmentation) as these will potentially overwrite the areas where deleted file portions are sitting. Furthermore it is best to install on and run a recovery utility from another drive, again to prevent overwriting data on the drive where the deleted files reside.

Permanently Deleting Files

As you may have noticed, it is entirely possible to recover some or all of a file after it has been 'permanently' deleted in Windows. If you ever want to truly permanently delete a file so that others can't recover it in any practical sense, you can use the Recuva, Restoration or CCleaner programs to do this - see the CCleaner section of the Cleaning Windows chapter for details of this functionality in CCleaner.

To securely permanently delete a file, first delete the file as normal in Windows - i.e. highlight it in Windows Explorer, press Delete, then empty the Recycle Bin.

Next, if using Recuva, launch it and do a scan for that filename (or all files) as normal, and it should show up in the list of recoverable files. Right-click on the file and select 'Secure Overwrite Highlighted'. This will overwrite all areas of that file with data such that it can't be recovered. If you want to adjust how secure the overwriting is, click the Options button and under the General tab, select the desired level of overwriting for the 'Secure overwriting' option; the more passes the more secure it will be.

If using Restoration, then launch it and enter the name of the file (or leave blank for all files) and click 'Search Deleted Files'. When Restoration finds the file and lists it, highlight the file and go to the Others file menu in Restoration and select 'Delete Completely'.

These methods will permanently delete a file so that it is effectively unrecoverable by virtually any program or method. However there always remains the possibility that the file may still be recoverable by law enforcement agencies using specialized methods, although it is highly unlikely that anyone could recover the bulk of this data regardless of the methods used.

Low Level Format and Zero Fill

People might suggest that you Low Level Format your drive to permanently remove data or fix a drive problem. This is not recommended unless you are experiencing severe hard drive problems, and even then it is not possible on most modern hard drives due to the complexity involved. Modern hard drives are low-level formatted at the factory to create tracks and sectors and do not need to have it done again. The correct course of action is to Zero Fill your drive, which people often confuse for a low-level format. This method overwrites the entire hard drive with blank data, ensuring that everything is deleted permanently for most intents and purposes, but it is not as intensive or potentially disk-damaging as a low-level format. A zero fill is your best bet in getting back to a 'good as new' hard drive.

A quick and easy way to zero fill a hard drive and error check it at the same time is to use the built-in formatting functionality of Windows itself to do a full format - see the Windows Installation chapter for more details. If however you insist on low level formatting a hard drive and/or using a custom diagnostic program to error check it and ensure that it is wiped absolutely clean, then check your hard drive make and model and consult your manufacturer's website for an appropriate utility such as: Seagate DiskWizard & SeaTools for both Seagate and Maxtor drives, Western Digital Data LifeGuard, or Hitachi Drive Fitness.

If you are using an SSD, you will need to use a custom utility to erase the drive, which should be available from your SSD manufacturer's website.

Copyright © 2010 Koroush Ghazi

< SYSTEM RECOVERY

This section covers all the main methods of recovering data and/or control of Windows after a major system error or crash. Also refer to the Performance Measurement & Diagnostics chapter for more details of ways to troubleshoot the potential source of such problems. If after any changes you make to Windows Vista your system starts crashing or behaving oddly, or you are having major problems booting into Windows, it may be because the Windows Registry or Windows system files have been corrupted or perhaps contains conflicting or bad data of some kind. The most common reasons for system file issues or data corruption are:

§ Overheating and/or Overclocking - See the Overclocking and BIOS & Hardware Management chapters for details. An overheating or overclocked component can malfunction, often in subtle ways, leading to data corruption over time or within a short space of time.
§ Faulty hardware - If a component is faulty, such as your RAM or CPU, it can corrupt data and cause a range of problems.
§ A bad shutdown - Can occur if your system suddenly reboots or Blue Screens, or if the power is lost to your PC while it is on. This prevents Windows from properly closing down.
§ Bad driver or faulty program installation - A faulty driver or program, including possible malware infestation, can cause data corruption.

The very first thing is to try and undo what you last did which you suspect caused this problem, such as uninstalling any recently installed drivers or programs. However if this is not possible or does not work, then try one of the following:

If you can boot into Windows:

§ You should run a range of malware scanners to make sure your system is free of any malware which may be causing the corruption or crashes/odd behavior - see the PC Security chapter.
§ You should run System Restore and revert to the most recent Restore Point available - see System Restore earlier in this chapter. This is the easiest and safest method for undoing harmful changes to system files. Remember, System Restore doesn't overwrite or alter your personal files, it only undoes system file changes.
§ If System Restore doesn't work or you don't have any recent Restore Points, you should then try to restore an Erunt Registry backup and reboot to see if this resolves your problem.
§ If you don't have a registry backup, try using the System File Checker as detailed further below.

If none of these options work or are not available to you, then try the options in the Windows Recovery Environment section further below.

If you can't boot into Windows:

If you simply can't boot into Windows, then you will have to use the Advanced Boot Options at Windows startup to attempt to fix the issue or attempt further system recovery procedures, such as running System Restore in Safe Mode. If these don't work or you don't have the expertise to troubleshoot the problem then you will need to use the automated Startup Repair tool in Vista. See the Windows Recovery Environment section further below for details of the above procedures.

If you can't switch on your PC or the problem occurs immediately after the PC is switched on:

If your problem is with a PC that won't turn on properly, or which crashes or shows screen corruption immediately after you switch the PC on and during the POST sequence, prior to the Windows startup screen, then the issue is definitely with your hardware, not Windows or your software settings. This can include problems like a bad BIOS setting, overheating, bad connections or a faulty piece of hardware - see the BIOS & Hardware Management chapter for details of things to try.

Copyright © 2010 Koroush Ghazi

System File Checker

The System File Checker is a built-in function of Windows that allows the system to go through and check all the major protected Windows system files against the original versions stored on a valid Microsoft Windows Vista DVD. This is extremely handy if you suspect corrupted/tampered system files that are leading to unusual Windows behavior.

To access the System File Checker follow this procedure:

1. Open an Administrator Command Prompt.
2. Type `sfc /scannow` then press Enter to start an immediate scan of your system files.
3. The System File Checker will go through all your important system files and make sure they have not been altered in any way. Where major system files are corrupted or shown to be different from original, they will be replaced with cached originals and/or your Windows Vista DVD.
4. If prompted reboot your PC as required.

Full usage options for the System File Checker can found in this Microsoft Article. The System File Checker does not repair general system issues such as registry corruption or faulty drivers or conflicting startup programs, so it may not resolve your problems, in which case check the options below.

Advanced Boot Options

To access a range of more advanced startup options for Windows Vista, reboot your PC and keep pressing the F8 key during startup - you will come to a screen with the heading Advanced Boot Options, providing a range of options, the most useful of which are covered below in more detail. Importantly, these options are listed in the order in which you should use them when trying to resolve a problem.

Last Known Good Configuration: This mode is the first thing you should select if trying to resolve problems with Windows not booting up or acting strangely. This mode uses the most recent system and registry settings which were in effect the last time you successfully booted up Windows. It will not alter or revert your personal files to an earlier state, only relevant system files/settings and the Windows Registry.

Safe Mode: Safe Mode is an important Windows mode which only loads up the bare essentials required for Windows to function. Third party drivers, graphical enhancements, startup programs, unnecessary processes etc. are all skipped and only the minimum required to display and use Windows and access your drives is provided. Safe Mode is provided precisely for troubleshooting purposes and not for general usage. The idea is that by reducing the number of software variables involved in the Windows environment, it becomes easier to identify the cause of a problem. You can read the details of the specific devices, drivers and services which are loaded up in Safe Mode in this Microsoft Article.

There are three types of Safe Mode you can launch:

- Safe Mode - This is the basic Safe Mode and is usually the option you should select.
- Safe Mode with Networking - Loads up Safe Mode with network drivers, allowing Internet access. You should not select this mode to start with if your issue is potentially connected with networking device drivers or a malware infestation.
- Safe Mode with Command Prompt - Loads up Safe Mode with a DOS command prompt interface instead of a graphical user interface - use this if you have problems entering normal Safe Mode. Note this is not the same as DOS mode.

When you enter Safe Mode you will see the Windows Desktop, typically shown at lower resolution, and with no graphical enhancements such as Vista Aero or even the background wallpaper. The words 'Safe

Copyright © 2010 Koroush Ghazi

Mode' appear around the edges of the screen to inform you that you are running a cut-down version of Windows Vista. The main use for Safe Mode is to determine whether your device drivers or recently installed software are the source of a problem you are currently experiencing, and allow you to uninstall them or alter your system as necessary to be able to restart normally. Because Safe Mode does not load any of your installed third party device drivers - instead using the default versions built into Windows - and because Safe Mode does not load up any startup programs or non-essential services into the background, this gives you the opportunity to determine whether your software or one (or more) of your startup programs is causing problems.

If you couldn't boot into Windows normally, but you can in Safe Mode for example, that is a clear sign that one of your recently installed drivers or programs is the likely cause of the problem. You can choose to permanently remove/roll back or temporarily disable the relevant programs or drivers by using Device Manager, Software Explorer or MSConfig. Furthermore if you made a change to a system setting or the Windows Registry that may have caused the problem, you can undo the setting in Safe Mode, or use System Restore to revert to an earlier Restore Point, or restore a Registry backup here.

Finally, a major use for Safe Mode is the removal of malicious software such as viruses, trojans or spyware. Many of these will load into the memory areas of Windows that cannot be unloaded during normal Windows operation, preventing proper removal. However in Safe Mode there are no such protected memory areas, and no startup programs or services are loaded with Windows, so this is the best way to remove such troublesome software. Enter Safe Mode and find and delete the problematic file(s), edit your startup items or Services to remove unusual or harmful entries (See the Startup Programs and Services chapters), or run a suitable scanner in Safe Mode to find and remove any malicious software (See the PC Security chapter).

In extreme cases where you cannot resolve your problem using Safe Mode, then at the very least Safe Mode provides you with the opportunity to access and backup your important personal files before reinstalling Windows or restoring a system image for example.

If you find that you cannot boot into Safe Mode, or are having similar problems in Safe Mode as you are in normal Windows - for example your graphics are garbled or show glitches - then the problem is likely hardware-based such as overclocking, excess heat, permanent damage to a component/faulty component(s), or a bad BIOS setting or incompatibility. See the BIOS & Hardware Management chapter for further details.

< WINDOWS RECOVERY ENVIRONMENT

Windows Recovery Environment is Windows Vista's replacement for Windows XP's Recovery Console. It attempts as much as possible to automate the process of recovering from any major system issues preventing you from booting up successfully into Windows. If all of the methods above have failed to work, or you simply don't feel you have the expertise to apply the above methods, then you should use these options to try to fix your issue. There are two main ways to access the Recovery Environment options:

§ Booting Off the Windows Vista DVD - All Vista Installation DVDs come with the Windows Recovery Environment tools. To access these tools, insert your original Vista DVD and restart your PC. Your computer should boot from the Vista DVD, but if it doesn't, go into your BIOS and set your optical drive as the first boot device then reboot again, and if prompted, press any key to boot from the disc. Once you reach the main Vista installation screen, select your language and keyboard layout, then click Next. On the next screen click the 'Repair your computer' link at the bottom of the box.
§ Recovery Partition - If purchased pre-built and with Vista already installed, your PC may come with a Recovery Partition which contains the information required by the Recovery Environment tools. To see if this is the case, as you're booting up your PC keep pressing the F8 key to reach the Advanced Boot Options. If you see a 'Repair your computer' option in the list of advanced boot options, then you should

Copyright © 2010 Koroush Ghazi

highlight it and press Enter to launch the Windows Recovery Environment. If your PC doesn't have a Recovery Partition, you can install it on your system drive at any time using these instructions.

Once you've launched the Recovery Environment using one of the methods above, you will be presented with the list of detected Windows Vista installation(s) on your drive(s). Select the one you want to fix and click Next. If you don't see any or all of your drives containing Windows, then you will need to insert a driver disk containing your SATA/RAID/SCSI drivers, click the 'Load drivers' button and browse to the driver disk and load up the relevant driver files before the drives are correctly detected.

The main Recovery Environment options are covered below:

STARTUP REPAIR

Startup Repair is quite possibly the most important feature of Windows Vista's Recovery Environment. It is the primary tool you can use to diagnose and automatically fix any issues which are preventing you from booting up properly into Windows Vista. Click this option and allow it to scan your system for any potential problems. If it can resolve the issues, it will do so automatically, rebooting as often as required, and will provide links at the end of the process which you can click to see precisely what issues have been found and resolved. Note that Startup Repair cannot recover your Windows under certain circumstances, including problems due to hardware failure, or certain types of virus attacks, or if your drive(s) are not being correctly detected. If Startup Repair cannot detect or repair the problem, you can try using the manual commands which are listed further below under the Command Prompt option.

SYSTEM RESTORE

This utility has been covered in detail under the System Restore section further above. This option allows you to launch System Restore and use a previous Restore Point in case you can't access System Restore from within Windows or Safe Mode. Obviously this requires that a suitable Restore Point be present and able to be used. This is yet another reason why I recommend that you keep System Restore enabled.

WINDOWS COMPLETE PC RESTORE

This utility has been covered in detail under the Backup and Restore Center section further above. If your PC is not recoverable, this option allows you to restore a full backup you made earlier with the 'Back up Computer' option in the Backup and Restore Center. It requires that you insert or attach the relevant drive or disc which contain the backup. If you haven't made any such backup then this option will not work, it cannot operate on partial backups of files for example.

WINDOWS MEMORY DIAGNOSTIC TOOL

The Windows Memory Diagnostic Tool is covered in further detail in the Performance Measurement & Diagnostics chapter. This option allows you to run the tool immediately by clicking the 'Restart now and check for problems' link, or 'Check for problems the next time I start my computer'. The first option should be fine unless you have other things you still wish to finalize in the Recovery Environment, in which case choose the second option.

COMMAND PROMPT

This option allows you to open a DOS Command Prompt window to enter a range of commands. This is useful if you want to access specific DOS commands or attempt to browse for particular files or directories on the stricken drive(s) and try to copy them to another drive.

Furthermore even though the Windows Recovery Environment replaces the XP Recovery Console, most of the Recovery Console commands have been kept and can still be used if required. Here is the full list of

Copyright © 2010 Koroush Ghazi

legacy Recovery Console Commands, and a list of those which have changed or no longer work in Vista. For example, the following commands may be of some use:

- Use the `CHKDSK /R` command to do a drive check and fix any errors if possible. If chdsk says the drive is unreadable or there are too many errors, make sure that if you have a SATA/RAID setup, you loaded the appropriate SATA/RAID drivers on the Recovery Environment main screen.
- Use the `BOOTREC /FIXBOOT` command to repair the boot sector of the drive.
- Use the `BOOTREC /FIXMBR` command to repair the Master Boot Record of the drive.

If none of the options above work in repairing or restoring your Windows installation, then it is highly likely that your drive has experienced too much data corruption and/or the drive or other hardware has actual physical faults which prevent proper startup. In the first instance you should make sure your system is not overclocked, and then try to run some disk diagnostics on it using the tools covered under the Low Level Format and Zero Fill section further above. If the drive appears sound you should consider doing a clean reformat and reinstall of Windows on it. After that you should run a range of performance and diagnostic tools to ensure that the system is working correctly and that no other hardware components - particularly your motherboard, CPU and RAM - are faulty in any way, as otherwise you may experience data corruption and the same problems all over again.

Copyright © 2010 Koroush Ghazi

BIOS & HARDWARE MANAGEMENT

Before delving any further into Windows optimization or customization, it is very important to first ensure that your hardware and connected devices are correctly configured for optimal operation. Regardless of any changes you make in Windows or your software, if your hardware is not configured properly its capabilities will not be correctly utilized, indeed serious problems such as random crashes or data corruption may occur. Whether you've built a PC or purchased a pre-built machine, you should make certain that all of the settings in the BIOS are correct, that the hardware is properly cooled, and that all of your devices are configured to function optimally in Windows. This chapter covers all of these topics in detail.

Note that this chapter does not provide information on how to select and purchase a PC from new, however if you are interested in that type of information, see my Hardware Confusion article for general guidance.

< THE BIOS

The BIOS (Basic Input/Output System) is a program held on a small ROM chip on your motherboard. It provides the instructions for what your PC should do as soon as it turns on. Your BIOS is independent of your Operating System, which means it is not directly affected by the operating system you use, or which driver version you've installed, or what your settings are in Windows for example. The BIOS supersedes all of that, and your drivers and operating system will load after the BIOS has loaded up. The BIOS controls a range of hardware-related features and is the middle-man between your CPU and other devices.

If there is an incorrect setting in your BIOS - that is a setting which is not optimal or correct for your hardware configuration - then you will have problems regardless of what setting you change in Windows, or which driver versions you install. Importantly, the BIOS is best configured correctly before installing Windows, as this reduces the number of unnecessary services and drivers which Windows may install, and helps reduce the potential for device conflicts.

Note that some of the latest motherboards may have a different type of BIOS-like interface called UEFI (Unified Extensible Firmware Interface). UEFI is a new form of software interface between your hardware and the Operating System. While UEFI brings with it a range of changes as covered in this Intel Article, in practice you will still need to configure all your hardware settings in much the same way as a BIOS, so the information in this chapter still applies in much the same way.

POST SCREEN

As your BIOS starts to load, the first thing it does is the Power-On Self Test (POST), a diagnostic program which quickly checks your components and makes sure everything is present and working OK. The POST sequence is usually extremely fast; you will only really notice it if it stops when encountering an error. POST error messages can be a bit obscure, but usually give you a lead as to where to look in your BIOS settings. A quick general guide to what the startup error beeps may mean is this POST Error Codes, but a more accurate description specific to your hardware is usually found in your motherboard's manual.

If you have no initial POST errors you will then see your PC's startup screen, which shows such information as your BIOS type (e.g. American Megatrends), the key to press to access your BIOS settings (e.g. DEL, F1 or ESC), the type of processor and its speed, RAM amount and RAM test results, drive information, and so forth. Note that if any of this information is incorrect, it may be that your hardware is extremely new and hence not recognized correctly by the current BIOS version; you've overclocked your PC too far; or you have bad hardware or incorrect BIOS settings.

Copyright © 2010 Koroush Ghazi

BIOS Settings

To access the detailed settings in your BIOS, you typically need to press a particular key (e.g. the Delete key) repeatedly as your system is booting up - check your motherboard manual. If your BIOS also has a password then you'll need to enter it first to access your BIOS settings; if you've forgotten the password, then try this BIOS Password Site. Once in your BIOS screen you will see a multitude of settings. The layout of the BIOS, and the names of the various settings vary greatly depending on the particular motherboard brand and model you own, so I cannot possibly cover them all here. The best reference source is this Definitive BIOS Optimization Guide - scroll down that page to find the 'Free Access' link to the guide. It covers all the common BIOS settings, and combined with your motherboard's manual and Google, you can understand what all of your BIOS settings do and thus undertake the very important task of optimizing your BIOS before doing any Windows tweaking.

I cannot stress the importance of making sure all the major settings in your BIOS are correct for your particular hardware setup and importantly that you've disabled all unnecessary devices and options. It may take some time and some research, but it ensures maximum performance and stability. No amount of Windows customization can overcome a badly set up BIOS.

BIOS Updates

The BIOS is written on a rewriteable ROM chip, which means that it can be updated (or 'flashed') with new information. Motherboard manufacturers release new BIOS versions that can improve performance, stability and compatibility, add new features or modify existing features, and fix known bugs. These new BIOS versions are available for download on the manufacturer's website. I can't list all the manufacturer websites here, as there are far too many, however if you have a look through your motherboard manual you should see a link to the appropriate website. Download the latest BIOS for your exact motherboard brand and model number and follow the instructions on the site to Flash (reprogram) the BIOS chip on your motherboard with this new BIOS version. A word of warning: flashing the BIOS is not to be taken lightly. If something does go wrong then your PC may not boot up and you may have to take your motherboard to a dealer to have the BIOS chip replaced or reprogrammed. While this is rare, when updating your BIOS make sure you follow the instructions provided to the letter.

Note that most modern motherboards allow flashing the BIOS from a CD/DVD or USB flash drive, so installing a floppy disk drive on your PC is no longer necessary.

Firmware Updates

Your motherboard is not the only device which has a BIOS. Many components, indeed most major electronic equipment like TVs, DVD players and mobile phones have their own inbuilt BIOS chips. The software on these chips is typically referred to as Firmware, and all firmware can be updated using the correct equipment and software. This firmware can usually be upgraded in much the same way as flashing your BIOS - check your hardware manufacturer's website for recent versions of the BIOS/firmware you require, and any specific instructions or software necessary. The most common firmware updates are for optical drives. If you want to find out more about these updates, check your hardware manufacturer's website, and see this Firmware Database in particular for optical drives. A firmware upgrade can help resolve problems like difficulties reading from a particular disc type, 'disc not detected' errors, and other issues. Just like BIOS flashing it involves an element of risk, so please read any instructions carefully before proceeding.

The motherboard BIOS is a critical component of the PC which is often overlooked, so I urge you to take the time to become more familiar with your own BIOS, and to configure it correctly. Of course if you are not sure what a setting in the BIOS does, do not change it from its default. If necessary check your hardware manufacturer's website for more details, or do a thorough search on Google. It might be tedious at first, but

Copyright © 2010 Koroush Ghazi

it's typically a once-only job - once you've done it, you don't need to go back and customize the BIOS settings again, you can reap the benefits of an optimal BIOS from that point onward.

< HARDWARE MAINTENANCE

It is important to properly maintain your hardware, to ensure it remains in good operation. The information below will help you understand how to handle, clean and keep your components operating smoothly.

HARDWARE HANDLING TIPS

If you have to physically handle the hardware components in your system at any time, such as removing or installing a component, checking component connections, or cleaning components, you should make sure to follow these tips to prevent any permanent damage to the components through mishandling:

- Before opening your case and/or handling any of your components, always shut down your PC and turn off the power directly at the wall socket - the electricity in your PC can kill or injure you, especially the dangerous voltages contained in your Power Supply. Even when switched off at the wall, the PSU can retain a lethal charge for quite some time, so on no account should you ever open your PSU or insert any metal objects into its casing.
- Once you've turned off your system at the wall, press and hold the PC power button for several seconds to discharge any residual charge in the motherboard's capacitors.
- While handling computer components, make sure you regularly discharge any static electricity in your body by touching any 'earthed' object - that is any object that can harmlessly dissipate static electricity. Typically if you leave your Power Supply Unit plugged into the wall socket (but switched off) then periodically touching the side of the metal PSU case will harmlessly discharge any static electricity. You can also purchase an anti-static wrist strap if you handle components regularly. If you are going to handle components try to minimize how much artificial fabrics and materials you are wearing as these can help to build up a significant electrostatic charge in your body. An electrostatic discharge from your body can damage or kill an electronic component, so do not take this lightly as it can actually happen.
- Do not use a vacuum cleaner to clean the inside of your computer and its components, precisely because vacuum cleaner nozzles can discharge static electricity and zap your components. Use a clean barely damp lint-free cloth or barely damp q-tips to wipe dust from most surfaces, making sure you don't scrape the Printed Circuit Board (PCB). Don't use any detergents and most certainly don't spray anything onto the components. Ideally if it is available to you, use a can of compressed air (or an air compressor) to blow dust from hard-to-reach or sensitive surfaces as this is much safer and far more effective.
- If blowing dust from a fan, especially if using a high pressure source like compressed air, insert and hold something like a pen in the fan's spokes to prevent it from suddenly spinning rapidly as this can damage the fan's bearings
- Do not force any plugs, cables or components into sockets that do not appear to be accepting them. Even if the two ends appear to be matched, the pin arrangements may be slightly different or out of alignment and hence forcing a fit may actually bend or break some of the pins and make the connection useless or permanently damaged. Computer hardware interfaces are designed to fit together with firm but not excessive force. This includes components like the CPU chip which fits into the appropriate socket on the motherboard - align all the pins perfectly and press evenly but not too hard and they will mate safely. Force the fit and you may just end up making your CPU unusable.
- Most devices in your PC require a source of power, however the voltage they require is very specific. If you connect the wrong plug to the component (which is hard to do), or forget to attach a necessary power connector (which is quite common), then the component will appear to be dead or may malfunction. You will have to check your component documentation and especially the motherboard manual to ensure that all components are plugged in correctly and firmly to receive sufficient power.

Copyright © 2010 Koroush Ghazi

- Most hardware components are sensitive to physical impact and strong vibrations. Avoid situations which result in the bumping or banging of these components, or for example mounting heavy fans onto them insecurely which can pass vibrations to these components or warp them under the weight.
- Do not handle liquids around electronic components. Any spillage can result in disastrous short-circuiting.
- Do not place excessive weights on PCBs as this can crack or warp them such that they will be permanently damaged. Don't even rest a large object temporarily on the motherboard or a component for example, put them on another surface until you need to use them.

Electronic components these days are quite hardy, and can withstand some abuse, but given how valuable they are I suggest that you don't take any risks when handling them and in their general usage, so the tips above are best observed if you want to maintain your PC and your electronic components in good condition.

SURGE PROTECTORS

Make sure you invest in a good quality Surge Protector for your PC and all your other sensitive electronic devices. Aside from typically letting you plug in multiple devices into one outlet, surge protectors serve an important function: they prevent spikes in voltage - which can occur for a range of reasons - from harming your components. Voltage surges needn't be sudden or catastrophic; even minor increases in voltage can reduce your component's lifespan over a period of time. Note that most surge protectors will not protect your equipment from the surge generated by a direct lightning strike on or near your house, so during heavy thunderstorms it is recommended that you turn off your PC and any other expensive electronic equipment and disconnect their power plugs from the wall socket to provide foolproof protection against any surge. This also includes any phone lines used for DSL for example.

POWER SUPPLY UNIT

Your Power Supply Unit (PSU) is an essential part of your system, and one that is often ignored. It is critical to system stability, and if after reading the information below you feel that there may be cause for doubting the quality or capability of your existing PSU to service your PC properly, you may wish to purchase a new and more adequate unit before investing too much time into optimizing your Windows installation. This is because no amount of customization or optimization can overcome the problems caused by a poor quality PSU, and it also jeopardizes your other components, potentially damaging them over time. A more efficient PSU can also save you money by using less electricity.

For basic details regarding PSUs see this PSU FAQ which talks about the common output specifications for PSUs and what they mean. In particular you should consider three key factors when determining the quality and adequacy of a PSU for your system: Wattage, PSU efficiency, and total amps delivered on the +12V rail. These figures should be readily available from the PSU's specifications.

Wattage: To work out a rough estimate of the PSU Wattage which is sufficient for a particular system, use this Interactive PSU Calculator. It is fairly straightforward to use, however note that there are some traps you can easily fall into which will result in overestimating your power usage. For example under the 'System Type' box, you should always select 'Single Socket' unless you actually have multiple CPU sockets on your motherboard. A Core i7 CPU for example has four cores, but it is still a single socket CPU; virtually no desktop system has more than one CPU socket on the motherboard, so pay careful attention to the descriptions while going through the calculator.

Efficiency: This doesn't represent how much of a PSU's power is usable - all good PSUs should provide up to their maximum rated wattage with stability if required. Furthermore, contrary to popular belief, whether a high or low wattage PSU, the PSU only provides the amount of power the system needs, so buying a larger PSU than you require won't result in extra power usage all by itself. PSU efficiency is the proportion of the power the PSU draws from your power socket that is relayed to your system. For example a PSU with 80%

Copyright © 2010 Koroush Ghazi

efficiency providing 400W of power to your system will actually draw 500W from the power socket on your wall while doing so. In practice efficiency will differ at different levels of load on different PSUs, and it's an important figure to look out for. Ideally you want 80% efficiency or higher at your expected load level on the PSU - the higher the efficiency, the more money you save in electricity bills.

Amperage: The Amperage on the +12V rail, a key factor in system stability. For example if you look at the specifications of some graphics cards, they will say that they require a current of a certain number of amps on the +12V rail (e.g. 40A on +12V for an Nvidia GeForce GTX 285). You should refer to the specifications of the PSU to see if the +12V rail(s) provide that much amperage in total. Note that some PSUs may have multiple 12V rails - this is technically a safety requirement to prevent potential overload on a single 12V rail, but is not a necessity, and some even consider it undesirable. In practice as long as the amps and total wattage supplied along the 12V rail(s) are solid and sufficient for the job required, it shouldn't make a huge difference whether you have single or multiple 12V rails.

The problem is that beyond trying to take note of the key factors above, an accurate review is required to tell you whether a PSU is genuinely good quality or not. As this article points out, specialized measurement instruments are necessary to determine this, not just measuring voltages with a multimeter. Hence most PSU reviews are inaccurate and effectively useless. Accurate PSU reviews can be found at sites like SilentPCReview and JonnyGuru, so start there if you want to know more about a particular PSU.

As a final note, if you live in an area where the mains power supply is not stable or you can suffer periodic outages, I strongly recommend investing in a good quality Uninterruptible Power Supply. This will increase the life of your components, and is important in preventing potential data loss resulting from a power outage, such as when you enable the performance features covered under the Drive Optimization chapter.

COOLING

One of the most common reasons for a range of problems in Windows has nothing to do with Windows or software; it is actually the hardware-related phenomenon of overheating. Overheating hardware can cause all sorts of strange errors, crashes and problems, and is often misdiagnosed as being a software or driver problem. Most computer hardware generates heat due to the power it consumes, and this heat needs to be dissipated somewhere. A typical computer case is designed such that it traps heat, and hence as heat builds up in a PC case, it will cause components to malfunction and even become permanently damaged over time. Overheating can occur in both stock systems and overclocked systems; it all depends on a range of factors we look at below. Before spending time optimizing your Windows, you must make sure your system is properly cooled.

Measuring Temperatures: The first step in determining whether a component is running too hot is to measure its temperature. On modern PCs the CPU, graphics card and motherboard all have built-in diodes that measure the temperature for these components. The CPU temperature monitor is a reasonably accurate measure of the temperature at or near the core of the CPU; the graphics card temperature monitor provides an indication of the temperature near the GPU core; while the motherboard temperature monitor is a good measure of the general temperature within the PC case, otherwise known as the ambient temperature. Some other hardware components such as power supply units and hard drives may also come with temperature measurement devices you can access.

To actually see the temperature readings from your components, you can check the key readings in your BIOS settings screens, typically under a Hardware Monitor section or similar. This gives you the CPU and motherboard temperatures, perhaps also the PSU temperatures as well. Clearly you need a more convenient method of checking temperatures under Windows, especially when running system intensive applications or games. Most motherboards already come with such software, so check your motherboard manual and driver disc, or the motherboard manufacturer's website for an appropriate monitoring utility. However for

Copyright © 2010 Koroush Ghazi

the most accurate and consistent temperature readings I recommend one of the following free utilities which work on almost any system:

Real Temp - Primarily for measuring CPU temperatures, particularly across the individual cores of a multi-core CPU. Also provides a basic GPU temperature reading.
Core Temp - Similar to Real Temp, is designed to measure CPU temperatures.
GPU-Z - Covered under the System Specifications chapter, GPU-Z has a range of GPU temperature monitoring capabilities found under its Sensors tab. It also has basic CPU and motherboard temperature monitoring.
HWMonitor - Can monitor a range of system temperatures as well as system voltages and fan speeds.
HD Tune - Covered under the System Specifications chapter, the free version of HD Tune provides a temperature readout towards the top of the HD Tune window, showing the current temperature of the selected drive.
SpeedFan - A more general temperature monitoring utility which can provide CPU, motherboard and hard drive temperature readouts, as well as allowing manual fan speed adjustment.

Once you have the appropriate utilities, monitor your component temperatures at both idle and when your system is under heavy load. If particular components reach what appear to be very high temperatures when under load, then those components may malfunction while undertaking strenuous activities on your PC for a sustained period of time, such as playing games. However even when idle, your PC may begin to malfunction if heat steadily builds up in your PC case and is not cleared fast enough.

Safe Temperatures: Most people will want to know what the 'safe' temperature is for a particular component in their system. Unfortunately there is no easy answer - safe temperatures differ based on different hardware architectures, as some are designed to run hotter than others. However you can ascertain a reasonably normal temperature range for your component by searching Google using the specific brand and model of the component along with the word 'temperature' to see if any user feedback or reviews of your hardware states what temperature ranges are normal. As a very general rule of thumb, at the time of writing, both the current generation of CPUs and GPUs should not exceed 90-100C under 100% load; and for hard drives, no more than 50-60C is normal when under maximum sustained load.

The best way to tell if your component is overheating is to watch for potential symptoms:

CPUs - An overheating CPU will usually throttle down its speed when under increasingly heavier loads, resulting in noticeably reduced performance. Use a utility like CPU-Z (See the System Specifications chapter) to monitor your CPU frequencies and run a CPU-intensive program such as Prime95 (See the Performance Measurement & Diagnostics chapter). If under 90 - 100% load you find that the CPU is not reaching its full advertised frequency then there is a strong likelihood it is overheating, especially if temperature monitoring also reveals a very high temperature under full load.

GPUs - An overheating GPU will result in graphical corruption and/or crashes, whether on the Windows Desktop or within graphically intensive applications like 3D games. Using GPU-Z, under the Sensors tab tick the 'Continue refreshing this screen while GPU-Z is in the background', then launch a modern game or stressful 3D application - see the Performance Measurement & Diagnostics chapter for some free ones you can obtain. Watch for any noticeable anomalies in the graphics, such as flickering textures, dots, or strange colors, and then after a few minutes quit the game and click the 'GPU temperature' line of GPU-Z, select 'Show Highest Reading' to see what the highest temperature was. A moderately high temperature combined with signs of graphical anomalies or corruption is almost always a clear sign of an overheating graphics card.

HDDs - An overheating hard drive is less common, and also harder to spot, however any strange noises from the drive, any signs of data corruption, or any problems or long delays in accessing the drive tend to

Copyright © 2010 Koroush Ghazi

indicate a problem which may be caused by overheating. Note that SSDs are not the same as HDDs and are unlikely to suffer from heat-related issues because they have no moving parts.

If you believe you're experiencing any heat-related issues in your system, see the tips below.

Cooling Tips: If you are experiencing problems with heat in your system, or more importantly if you want to prevent any heat-related problems from occurring in your system, the following basic cooling tips should be observed. This applies equally to overclocked and non-overclocked systems:

- Remove any obstructions from around your case. For example don't obscure any of your case grills/air holes, such as having them pressed against a wall, blocked by dust etc. Insufficient flow of air into and out of the case is the number one cause of heat buildup and heat-related problems. No matter how much cooling you have inside a case, if air can't easily get into and out of the case then your system will overheat.
- If you have few or no major case fans drawing in cool air and expelling hot air, remove the sides of your case so that the fans on the CPU, graphics card and Power Supply can get a fresh supply of cooler air, and can expel hot air outside the case.
- If you do have several case fans, arrange them so that some are to the front and low in the case, sucking air into the case (as the air near the floor is cooler) and some are to the rear and/or the top of the case, blowing hot air out of the case (where the hot air expelled will rise away from the case). In this situation make sure to keep the sides of your case closed so that the fans have more pressure to suck/blow air through the case's contents like a wind tunnel.
- Don't position a sucking and a blowing fan too close together as they will 'short circuit' each other - that is they will pass air through the shortest line between the two, bypassing your components and hence not cooling them as efficiently. Again, fans sucking air into your case should be low and on the furthest side of the case from the blowing fans that expel heat from the case.
- If one component is shedding a lot of heat, pay extra attention to perhaps providing greater cooling to the components immediately around it. Often the excess heat from one component can cause another nearby component to overheat.
- Tidy the internal components of your case. This means all ribbon cables, power cables, etc. should be clipped or twisty-tied to be as neatly arranged as possible, primarily to avoid blocking the flow of free air around components, especially near the CPU and graphics card which are the two hottest components in most cases. Secured cabling and snug plug connections also means you can be sure nothing becomes accidentally unplugged or short-circuited over time and hence cause mysterious hardware-based errors that will confuse you in the future.
- If using additional internal cooling like larger heatsinks or fans, make sure they are not too heavy for the surface they are mounted on. For example, using extremely large heatsinks on a graphics card can result in the card actually bending under the weight and hence becoming permanently damaged. Even a large heatsink mounted on a motherboard can cause it to warp or crack, once again damaging the motherboard PCB beyond repair. If you feel you require such hefty cooling you should consider instead buying a larger case that has better airflow properties.
- Make sure your drive(s) are not smothered by cabling or crammed into a stuffy area of the case with no nearby cooling or fresh air. Higher speed hard drives in particular (i.e. 10,000 RPM or faster) can heat up quite a bit. Hard drives are often overlooked in cooling, and yet they are a vital system component, and as such you should make sure they aren't confined to an extremely hot section of your case.
- Make sure that any heatsinks or heatpipes on the motherboard itself are not covered or blocked by other components or cables, or covered in dust. There is a reason why these heatsinks are there: because the chips on a motherboard often require cooling otherwise they can malfunction due to excessive heat just like any other major component. Don't assume a heatsink or heatpipe without a fan implies the component requires minimal cooling, as sometimes manufacturers skimp on putting a fan on these components, which simply means the heatsinks have to do more work, so keep them well exposed to cool air. You may even consider positioning a fan near them if you wish to aid in system stability.

Copyright © 2010 Koroush Ghazi

While non-overclocked components can overheat, overclocked components heat up much faster and are a very common cause of system instability and a range of problems. If experiencing problems on your system make absolutely certain that as part of your initial troubleshooting you return all your components to their default settings to see if this removes or reduces the severity of the problem - see the Overclocking chapter for more details.

It should be noted that a common cause for component overheating is the incorrect application of thermal compound by the user. Too much or too little thermal compound can cause a component to overheat dramatically, so always follow the application instructions to the letter and don't improvise unless you are highly experienced. You may also wish to consider purchasing better quality thermal compound for use on your components.

The most simple of all of these tips which anyone can undertake is to provide greater access to fresh cool air for the case's contents and regularly clean the case to remove dust buildup. Dust in particular can reduce airflow significantly, so keep your case and your components dust-free using a barely damp cloth, q-tip or compressed air. Furthermore the next time you go to upgrade your PC, consider buying a larger case with plenty of ventilation as the single best investment in cooling and hence general system stability.

< DEVICE MANAGER

Once you have set up your hardware and BIOS correctly, the Device Manager in Windows is the central location for viewing and configuring connected hardware on your system. To access Device Manager, you can find it under the Control Panel, or go to Start>Search Box, type *device manager* and press Enter. The main Device Manager window lists all your detected hardware grouped by category, and you can expand particular categories to see individual devices. Double-click on any particular device to see more details of it.

Devices with a question mark or exclamation mark next to them will need further troubleshooting to correctly identify and install, as by default Windows is unable to use the Plug and Play system to identify what they are. Until Windows can identify a device properly, it cannot be used even if it is correctly connected to your system and identified by your BIOS for example. You can use the Add Hardware component of the Control Panel to add older devices which don't support Plug and Play (See the Add Hardware section of the Control Panel chapter) and/or you may have to install an appropriate device driver for Windows to detect and use the device properly - see the Windows Drivers chapter.

If you aren't using certain devices, you can also safely disable them here by right-clicking on the device and selecting Disable. This is generally only recommended for more advanced users, as disabling necessary devices can cause a lot of problems. The main aim of disabling unused devices is to speed up startup time, and also free up system resources. In practice however it is best to disable unused devices in your BIOS wherever possible, and preferably before installing Windows - see the IRQ section below for the explanation.

ACPI RESOURCE ALLOCATION

ACPI is the Advanced Configuration and Power Interface standard, and is an important part of the way Windows Vista and drivers communicate with your hardware. In previous versions of Windows you could run hardware which didn't support ACPI, or even disable ACPI if you wanted to attempt manual resource allocation. However this is no longer possible in Windows Vista - Vista requires ACPI for it to function. That means that you cannot disable ACPI, and older hardware which is not properly ACPI-Compliant will not run Vista. In fact Vista only supports systems based on motherboards whose BIOS is ACPI Compliant and dated 1 January 1999 or newer. If you're running older hardware that means you should update to the latest available BIOS for your motherboard and also ensure that any ACPI options are enabled for Vista to install and run without problems.

Copyright © 2010 Koroush Ghazi

Windows Vista does not fundamentally change the way resources are handled compared to previous versions of Windows. Since Windows Vista only accepts ACPI-compliant systems, and because most recent hardware supports Plug and Play functionality, resource allocation is handled automatically and quite efficiently and should not be a major issue. However one practical aspect of ACPI is covered below.

INTERRUPT REQUESTS (IRQS)

Interrupt Requests (IRQs) are the way in which all of your major system devices get the CPU's attention for instructions/interaction as often as necessary. There are usually 16 - 24 main hardware IRQs in a modern PC. To view your current IRQ allocation go to Control Panel>Device Manager and under the View menu select 'Resources by Type', then expand the 'Interrupt Request (IRQ)' item. You will see all the devices currently active on your PC arranged by IRQ number, starting at 0 [System Timer]. Under Vista you may see IRQs numbered up to 190 or more, but all of the IRQ numbers above 24 appear to be for legacy Industry Standard Architecture (ISA) or non-Plug and Play devices, not for your main system hardware.

Window Vista allows several devices to share an IRQ without any major issues, and in general this is fine. In any case you can't alter the IRQ allocations from within Windows, as they are automatically handled by ACPI. Only legacy devices will have the option to attempt manual alteration of their resources under the Resources tab of the relevant device Properties; most other devices do not allow the 'Use automatic settings' option to be unticked. However you may have problems or reduced performance if two or more major devices (such as the sound card and graphics card) share the same IRQ, so you should try to minimize IRQ sharing.

To first check to see if any of your major hardware is sharing IRQs, you can go to each hardware device in Device Manager, and see if any yellow exclamation marks appear for the device, indicating problems. Open the Device Properties box (double-click the device or right-click and select Properties), then click the Resources tab and see if any conflicts are listed under the 'Conflicting device list' box.

For an easier method of viewing IRQs and checking for potential IRQ conflicts, use the built-in System Information tool (see the System Specifications chapter). To access it go to Start>Search Box, type *system information* and press Enter. Expand the 'Hardware Resources' item in the left pane, and click the IRQs item to see IRQs listed in order from 0 upwards. Click the 'Conflicts/Sharing' item to see a summary of sharing conflicts. Don't panic if you see conflicts, this doesn't mean your system is unstable or configured incorrectly. In many cases some hardware will be sharing a single IRQ or resource and there's not much you can do to prevent or alter this, it is normal behavior. The only ways to prevent or minimize the impact of IRQ sharing are:

Disable Unused Devices: IRQs and other system resources are typically assigned by your BIOS and set by Windows Vista during the installation process. Usually they are next to impossible to alter in any significant way, so the best way to ensure that you are less likely to end up with shared IRQs (and potential problems) is to disable any unused devices in the BIOS before installing Windows Vista. However it is still useful to disable these devices even after Vista is installed. Some examples of common devices that can be disabled - if you're not going to use them - are:

- Unused IDE Channels
- Unused SATA Channels
- RAID options
- Onboard Audio
- Onboard Video
- Game Port
- Midi Port

Copyright © 2010 Koroush Ghazi

Disabling unused devices not only frees up unreserved IRQs and reduces the chances of sharing, it can also speed up bootup time noticeably because Windows won't load up drivers for these devices. Clearly if you already have, or plan to have, a piece of hardware connected to any of these Ports, or need to use a particular device, then you should not disable them. For example if you one or more IDE-based drives which connect to an IDE channel, then you cannot disable that IDE channel and expect the drives to work. You can always re-enable these devices in the BIOS at any time, so this is by no means a permanent disabling of particular devices. However you should only disable devices in the BIOS that you are certain will not be used during your normal Windows usage.

Move Conflicting Devices: If you are using an existing installation of Windows Vista you can attempt to reduce IRQ sharing by physically moving a device. Note however that on certain motherboards particular IRQs are shared by default and cannot be changed. For example on many systems the USB Host Controller (for USB peripherals) is often on an IRQ shared by another fixed system device, such as your Serial ATA Controller - this is unavoidable and usually does not result in any problems. In such cases where you feel there may be a conflict or reduced performance, your only course of action is to physically move one of the items to another location on your system if possible. For example, if your sound card is sharing an IRQ with your graphics card, physically shift the sound card from one PCI/PCI-E slot to another free one; if the USB Host Controller is sharing with another device, avoid using the particular USB hub that controller relates to. If neither of the shared devices can be physically moved then you will have to accept the situation. Remember that Windows can share IRQs without major problems in most cases, and Vista is quite refined in this respect.

If after the above procedures you still have major difficulties which you feel are attributable to IRQ sharing, the final option is to reformat and reinstall Windows Vista, making sure of course to first correctly configure your BIOS and disable all unnecessary devices. Even then there is no guarantee that major devices won't wind up being shared again. Unlike previous versions of Windows, you cannot disable ACPI to force manual IRQ allocation, as Vista must have ACPI enabled to work.

DEVICE POWER MANAGEMENT

Aside from the global Power Options available under Control Panel and covered under the relevant section of the Control Panel chapter, you can access individual device-specific power management settings in Device Manager for certain types of devices (e.g. Keyboards, Mice and USB devices). To do so, open the Properties of any specific device and if there is a Power Management tab, click on it and you will typically see two options, one or both of which are available:

Allow the computer to turn off this device to save power: This option lets Windows power management disable a device if it considers it idle. However unfortunately USB devices in particular seem to have performance issues if this option is ticked, so I recommend unticking it. If you're having problems unticking this option, see this Microsoft Article.

Allow this device to wake up the computer: If selected, this allow the device to wake the computer up from Sleep mode. It should be only enabled if you want that to occur, otherwise untick it. Note that if you are having problems with a device waking the computer, see this Microsoft Article.

In most cases both boxes should be unticked if you want to minimize problems with a device, particularly USB devices.

TRANSIENT MULTIMON MANAGER

Unlike earlier versions of Windows, Vista is designed to search for any recently attached monitors and automatically enable them - it does this using the Transient Multimon Manager. This means that if you connect (or disconnect) any display device Vista will now automatically handle this just like any other Plug and Play device covered in this chapter.

Copyright © 2010 Koroush Ghazi

However if you only have a single display device connected to your desktop PC and do not regularly connect other display devices, are not running a mobile PC, or do not run a multi-monitor setup, then you can safely disable the Transient Multimon Manager and thus save several seconds at each bootup. To do this, you need to open Task Scheduler - go to Start>Search Box, type *taskschd.msc* and press Enter. In the left pane of Task Scheduler expand the directory tree until you reach Microsoft>Windows>MobilePC. Click on the MobilePC item in the left pane and in the right pane right-click on the TMM task and select Disable. The next time you boot up Windows it will not be enabled.

Once again, this is only recommended for users with a single display device connected to a desktop PC, as those with multiple monitors, mobile PC users and people who switch displays often will actually benefit from the Transient Multimon Manager.

REMOVE UNUSED DEVICES

For each device that has ever been connected to your system, Device Manager will retain a range of entries in the Windows Registry relating to the device type, and the drivers and settings it used. That way if it is ever reconnected it can be quickly recognized again. However there are times when you have permanently discontinued the use of a device, or want the device to re-initialize, and you want to clean out the Device Manager of any traces of it. To firstly view unused devices in Device Manager, do the following:

1. Open an Administrative Command Prompt.
2. Type the following lines exactly as shown, pressing Enter after each one:

```
Set devmgr_show_nonpresent_devices=1

Devmgmt.msc
```

3. In the Device Manager window that opens go to the View menu and select 'Show Hidden Devices'. Now expand all the categories and start looking through all the devices. Devices in gray are usually for old/unused/disconnected devices and safe to remove by right clicking on each one and selecting 'Uninstall'. However don't uninstall a device you know you will be reconnecting to Windows soon.
4. In particular, you might find several entries under the Monitors and Display Adapters sections from previous graphics driver or graphics card installations. You should delete all of these grayed out entries, but at least one un-grayed entry should remain. You may also find grayed entries for drive controllers you no longer use, and these should be safe to remove.
5. Do not remove any Microsoft devices such as those under the 'Sound, video and game controllers', or those under 'Storage volume shadow copies'. If in doubt, do not remove an item, gray or otherwise.
6. Once done, you can close Device Manager the usual way and the next time you open it up it will not show unused devices until you again use this method to do so.

Use this method with caution. In many cases if you accidentally uninstall a hardware device which is currently connected to or required by your system, you can simply disconnect and reconnect the device, or reboot Windows, and it will be redetected by Windows and the appropriate drivers installed again - so this method doesn't permanently remove any device such that it prevents it from being detected or used again in the future usage. In some cases however removing important devices may prevent Windows from booting up, which is where an appropriate restore point comes in handy to undo the damage.

In general I recommend making sure that your hardware and BIOS is correctly configured, clean and well maintained otherwise no amount of software tweaking will resolve odd problems in Windows if they are hardware based. The single most common reason for Windows problems is lack of adequate cooling, so if you only do one thing, it should be to ensure your components are clean and cooled properly.

Copyright © 2010 Koroush Ghazi

WINDOWS INSTALLATION

The methodology behind the installation of Windows Vista has changed from previous versions of Windows. Vista uses an image-based installation method which is covered in this Microsoft Article. Your Windows Vista installation DVD contains all the different Vista editions, and at the start of installation, the Product Key you enter identifies the specific edition you've purchased and will be installing. Then as installation begins, instead of selectively copying across a large number of individual files as XP did, a complete compressed 'hardware neutral' image of a standard Vista installation is copied across to the target drive, is uncompressed and overwrites the drive contents. As the installation continues, Vista then identifies your hardware and configures itself accordingly. This change in the underlying installation method has a range of practical impacts which are discussed further below, and also in Microsoft Article.

This chapter covers a series of important things you should consider prior to installation, as well as all the steps involved during the actual installation of Vista and immediately afterwards.

< PRIOR TO INSTALLATION

Before we move onto the Windows installation process, we first look at the various preparations you should make and the issues you should consider prior to starting installation. Even if you've already installed Vista some of the information in the chapter is still applicable and worth reading through.

CHECK YOUR HARDWARE FOR COMPATIBILITY

Just to be safe, before purchasing and installing Windows Vista, you should make sure that all your hardware components are compatible with Vista and will run it reasonably well. To do so, check the Vista Minimum Requirements and also use the Windows Vista Upgrade Advisor if you believe your system to be borderline compatible. The Advisor scans your PC and will tell you if you will have any issues, and can also help choose the version of Vista which suits you best. Also check this Vista Hardware Compatibility List to see if your hardware is listed as having any issues or being incompatible with Vista.

DISABLE UNUSED RESOURCES IN THE BIOS

As covered in the BIOS & Hardware Management chapter, it is important to turn off any options and resources in the BIOS which you will not be using prior to installing Windows Vista. This will ensure that you minimize any shared resources in Vista, prevent the installation of unnecessary drivers, and help minimize potential problems. Remember, you cannot manually reallocate IRQs and other system resources to your hardware once Vista is installed, so don't skip this step.

SCAN FOR MALWARE AND PREPARE BACKUPS

If you are going to transfer any data or personal files from an existing installation of Windows to your new installation of Windows Vista, it is strongly recommended that you do a complete malware scan of your existing Windows installation. This ensures that you don't wind up copying across infected files which ruin your new installation of Windows. See the PC Security chapter of this book for full details. Importantly, if you plan to run the Windows Vista installation DVD from within your current install of Windows, make sure to completely disable any anti-malware program(s) after your scan, as they can interfere with the proper installation of Windows.

Once you're sure that your files are clear of any malware, the next step is to prepare complete backups of all your important information. This is covered under the Backup & Recovery chapter of this book. Regardless of which type of install you're going to undertake, even if you choose an Upgrade install for example, I still

Copyright © 2010 Koroush Ghazi

strongly recommend having backups of your irreplaceable data on disc or another drive prior to installation of Windows, just in case anything goes wrong and you lose all the existing data on your drive. It is genuinely much better to be safe than sorry.

I also recommend preparing a separate disc or USB flash drive with a copy of the latest appropriate Windows Vista device drivers for all your key hardware. Installing the correct drivers as soon as possible after installing Windows ensures optimal stability, compatibility and performance, and can prevent major problems. You may even need certain drivers - especially SATA, RAID or other drive-related drivers - for correct detection of your drives during the Windows installation process. Prepare these in advance and store them on a DVD, USB flash drive or external drive so that you can load them if necessary during the step where you choose the target drive for Windows installation. Check the Windows Drivers chapter for more details of where to obtain these drivers.

Migrating Files and Settings or Upgrade Install

If you just want to move user accounts, data and settings from a Windows XP or Windows 2000 machine to your current Windows Vista installation in an automated manner, you can use the Windows Easy Transfer utility. To access Windows Easy Transfer, go to Start>All Programs>Accessories>System Tools, or go to your Start>Search Box, type *windows easy* and press Enter. You will enter a migration wizard which will take you through the steps required to carry out the migration. For full details of how to handle the migration, see this Microsoft Article. To successfully migrate between two machines you will need either a removable hard drive, a USB 'Easy Transfer' Cable, be connected to the same network (not counting the Internet), or use CDs/DVDs. The categories of things you can migrate are:

- Files and folders
- E-mail settings, contacts, and messages
- Program settings
- User accounts and settings
- Internet settings and favorites
- Music
- Pictures and video

If you don't want to transfer settings and files between two different machines, and instead you want to install Windows Vista over the top of an existing installation of Windows while maintaining all your files and settings, you will need to commence installation of Vista from within your current version of Windows as detailed under the Installing Windows section further below. Then when you reach Step 5 below select the Upgrade option and continue from there.

For home users I don't recommend migrating or doing an upgrade install and transferring user accounts, files and settings in this manner. Vista's image-based installation method is quite sound compared to prior versions of Windows, and hence an upgrade install is not likely to cause problems. However to ensure that you have a clean slate to begin with, I recommend that you start with a full clean install of Vista on a freshly formatted drive, and then manually copy across only the files you need. If you insist on using the transfer tool or doing an upgrade install, I strongly recommend only transferring personal files, not any settings or user accounts.

Modifying The Windows Installation Disc

Vista's image-based installation system allows easier creation of a modified installation disc. The tools you need to do this are in the Windows Automated Installation Kit and combined with these ImageX commands you can generate and alter a new Windows Vista image which may incorporate the latest device drivers or other updated components, or remove unnecessary components, for use in future installations.

Copyright © 2010 Koroush Ghazi

Note however that there is no simple way to incorporate ('slipstream') Vista Service Pack 1 (SP1) into a pre-SP1 install image of Vista - the reasons for this are explained here; Vista SP2 similarly requires a lot more work to slipstream. If you wish to undertake this procedure refer to these Create a Vista SP1 Slipstream and Create a Vista SP2 Slipstream tutorials for more details. In general it is best to either obtain an official ISO image of Vista with SP2 incorporated, or buy a Vista SP2 disc if you must use a slipstreamed image. It should be noted however that slipstreaming is in no way a necessary step, nor does it provide any performance benefits - it is simply more convenient, especially if you frequently (re)install Vista.

For general alterations to your Vista installation image, the easiest method is to use vLite. vLite is a free automated utility for creating a custom Windows Vista disk image for use in installation. It allows you to select the components you wish to remove from Windows, as well as things you might like to add, such as particular Windows Updates, the latest drivers and so on. Once you have integrated the relevant components and/or removed the components you don't need, vLite generates an ISO file which you can burn onto disc and use as your Windows Vista installation disk.

I encourage you to experiment with vLite, however I strongly recommend that you research what you are doing before using this tool. Don't simply remove something from the Vista installation disk because you think that it somehow 'speeds up' your PC. Removing most components simply reduces disk space, it doesn't increase speed in the majority of cases. Removing Internet Explorer 7 for example is more likely to cause problems in the future and doesn't speed up your PC in any significant way at all. Removing certain other features may appear intuitive at first, but may have unintended results. For example removing the TabletPC features of Vista also winds up removing the very useful Snipping Tool (see the Control Panel chapter), while removing Windows Defender also removes access to Software Explorer (see the Startup Programs chapter). Don't fall into the trap of thinking that it is cool to strip out virtually every component of Windows and replace it with a third-party alternative - you are more likely to cripple desired functionality in Vista inadvertently or cause other problems for yourself down the track which only a reinstall of Vista can fix.

I recommend instead that you use vLite mainly to add useful components to the Vista installation disk if so desired, then later you can remove particular Windows components using the built-in Programs and Features utility in Vista (See the Control Panel chapter) as well as the other methods covered throughout this book as required. That way if you want any component back at any time, you can simply re-enable it again quite easily, whereas removing something permanently during installation can make things very difficult.

Importantly: Installing Vista SP1 from an image modified by vLite can prevent Vista SP2 from installing correctly. More details are in this Microsoft Article. This is yet another reason why you should be extremely careful in how you use a tool like vLite. Despite popular belief, slipstreaming of service packs and modification of installation disks are not a performance tweak, and can often cause more problems than any marginal benefits they may provide.

Also be aware that Vista's image-based installation system means that you face greater exposure to malware if you use a downloaded Vista installation image which you yourself have not created. Do not download or use any untrusted installation images as aside from legal issues, you could be installing serious malware on your system in the process, bypassing all security measures and rendering them useless.

< PREPARING THE DRIVE(S)

Before you can install Windows, you need to think about how best to configure your drive(s) for optimal performance and the functionality to properly meet your needs. This includes considering whether you want to (re)format or partition any of the drives, whether you want to use a RAID configuration, and whether you want to dual boot Vista with another OS. It is also much easier to partition and format drives prior to Windows installation, though you can still do it after you install Vista. Make absolutely certain to read the following information before proceeding with Windows installation.

Copyright © 2010 Koroush Ghazi

DUAL BOOT OR MULTIBOOTING

You might want to consider a dual boot configuration of Windows Vista along with your existing version of Windows such as XP or 2000, or another operating system altogether. This will allow you to use both operating systems on one machine, with a Boot Menu letting you select which to boot into each time your PC starts up. Such a configuration does not provide any performance benefits, it is simply designed to allow two or more different operating systems to reside on the same machine, totally isolated from each other. If you only want Windows Vista on your PC, you can skip this procedure.

The instructions for creating a dual boot/multiboot system in Vista are in this Microsoft Article, and more specific details and tips are in this Multi Boot Configuration article. To begin with you need to have at least two or more partitions on your current drive and/or have two or more drives - see further below for partitioning information. You should then boot up into your existing version of Windows and insert the Windows Vista DVD and run Vista setup from there. This ensures that Vista will correctly detect your existing Windows installation and configure the boot menu properly to give you the choice of booting into either OS - see the Boot Configuration chapter. Importantly, if you run SATA or RAID drives, for Vista to correctly identify all of your drives prior to installation and correctly configure the dual boot, you must have appropriate SATA/RAID drivers on a floppy disk, USB flash drive or CD/DVD and insert them during the drive identification stage of Windows Setup.

In general I recommend having Vista and an older version of Windows on completely separate drives, as this causes the least number of problems, particularly if you want to remove the older version of Windows eventually. If using a hard drive, performance is also improved if each OS resides on the first primary partition of a different hard drive, so for optimal performance in Vista, do not install it on a secondary partition of any hard drive - SSDs show no performance difference across partitions.

Some important things to note about dual boot setups:

- It is strongly recommended that you install the older version of Windows first (or it must already exist) before installing Vista. It is possible to install Vista first and then install an older version of Windows afterwards, but this requires more risky boot configuration editing - see the Boot Configuration chapter.
- If your older version of Windows is the active partition on the first boot drive (the drive or partition which is first booted up by your BIOS), then it will be altered to include Vista's boot manager files. If you delete or damage these boot files, or you reformat the older OS or disconnect its drive, then you will need to boot from the Vista DVD and run Startup Repair to fix Vista's boot configuration, otherwise it will not bootup properly - see the Backup and Recovery and Boot Configuration chapters.
- If you want to remove Vista from a dual boot arrangement and return the boot record of your earlier version of Windows to its normal state, see the Boot Configuration chapter for details.

PARTITIONING

Before formatting a drive you must first Partition it. Partitions are fenced-off portions of a drive, and there must be at least one on a drive before it can be used. You can instead create multiple partitions, effectively dividing a single drive into several smaller logical drives of varying size, each with their own drive letter. There are various advantages and disadvantages to partitioning a drive, but it is important to understand that you should never create multiple partitions under the false impression that this improves performance. On a hard drive, the first (Primary) partition is always the fastest, and subsequent partitions are not as fast. On an SSD, partitioning makes no difference to performance as all partitions can be sought out with equal speed.

In any case, whether SSD or HDD, partitioning does not replicate the performance benefits of having multiple separate drives, such as in a RAID configuration (see further below). On a single hard drive in

Copyright © 2010 Koroush Ghazi

particular, performance is still limited by how fast the single drive head can seek (move around to read or write) information. It can't be in two places at once, whereas with two physically separate hard drives, each hard drive's head can seek information independently, such as one drive reading game information while the other concurrently reads/writes Virtual Memory information in the Pagefile. Therefore partitioning is not a true substitute for having two or more drives, it is most useful as an organizational tool. For example one of the major reasons you may wish to create multiple partitions is to allow you to dual boot with Windows XP and Windows Vista, as discussed further above. This allows you to run Vista along with XP on the same hard drive for example, but completely separated from each other.

It is ideal to format and partition a drive prior to starting Windows installation, and you can do this either using a third party tool as covered further below, or you can use the built-in formatting and partitioning functionality of XP or Vista under the Administrative Tools>Computer Management>Disk Management utility. The instructions for can be found in this Microsoft Article and also under the Computer Management section of the Control Panel chapter in this book.

Furthermore in Windows Vista, you can not only create partitions during the normal formatting process (see further below), you can also repartition a disk on an existing installation of Vista. To add partitions in Vista follow these instructions:

1. Go to Control Panel>Administrative Tools>Computer Management or go to Start>Search Box, type *computer management* then press Enter.
2. In the Computer Management box, click the 'Disk Management' item in the left pane.
3. Select the drive for which you want to alter a partition from the list at the top of the screen.
4. Right-click on the drive and select 'Shrink Volume' - this will reduce the size of the existing partition, freeing up space for a new partition(s) to be made.
5. In the next dialog box enter the amount in MB you want to use for the new partition; the maximum amount available is the amount of free space left on the drive.
6. When done, click the Shrink button and the existing partition will be reduced by the amount you chose above.

You can now create a new partition in this freed up space. There are a range of other functions possible under Disk Management, but these are covered in more detail under the Control Panel Chapter.

If you want to undertake more complex partitioning of your drive, you can use the free GParted tool instead. It is not a Windows-specific tool, however it supports all Windows file systems and works with Windows Vista. It won't be covered here as it is quite detailed in functionality, and recommended for more advanced users, however refer to its documentation if you wish to learn more.

It is worth noting that there is a partitioning procedure which may improve performance on a hard drive (but not an SSD). It is referred to as Short Stroking, and essentially involves restricting the drive such that the head movements on the hard drive are kept only to the outer sectors of each platter in the drive, which are the quickest to access. The problem with short stroking is that it significantly reduces the usable storage capacity of the hard drive, although given the lower cost of large hard drives, and when combined in a RAID configuration (see below), you can still generate a reasonably large amount of storage using multiple short-stroked hard drives, albeit at a higher cost. Short stroking can also reduce the lifespan of the hard drive.

In any case, the easiest way to achieve the short stroke effect on a hard drive is to create only a single small partition (i.e. around 10% of the total drive capacity or less in size), which is automatically placed at the outer edge of the drive, and this may improve performance for the drive. Note that the real-world performance benefits of short stroking are somewhat dubious, because the benefits are mostly seen in synthetic benchmarks. On balance this is not a procedure I would recommend for most people - if you value performance over drive space, then consider purchasing an SSD instead as they will provide a range of

Copyright © 2010 Koroush Ghazi

benefits including much greater real-world performance gains than any short stroking ever could, as well as quieter operation and lower heat, at a cost that is rapidly declining.

Finally, keep in mind that using multiple partitions on the same drive for backup purposes is not a good substitute for having backups of your important data on disc or another drive. Drives can and do become physically corrupted and this affects data on all partitions of a drive, so backing up from one partition to another on the same drive as your main backup strategy is not appropriate. However partitioning a single drive to create a recovery partition for Startup Repair for example can provide useful additional protection. See the Backup and Recovery chapter for more details on these topics.

RAID CONFIGURATION

RAID (Redundant Array of Independent Disks) is a common method of configuring multiple drives to perform better and/or provide protection against data loss. The various RAID levels are best demonstrated in this RAID Article - click the numbers at the top right of the article to see the various RAID levels demonstrated graphically, including the common RAID 0, RAID 1, RAID 5, RAID 10 and RAID 0+1 configurations.

To set up a RAID array you need two or more drives, whether HDD or SSD, preferably of the same size and speed, and a motherboard with RAID support. You will then need to install the drives as normal and configure the appropriate RAID options in your motherboard's BIOS - see your motherboard manual for instructions. If your motherboard supports RAID, and most motherboards do, then there is no additional hardware required, it is all driven by Windows and the motherboard. Once configured correctly, the RAID configuration of multiple drives will be seen as a single drive by Windows, and treated as such.

To determine which RAID configuration best suits your needs if any, you will need to read the articles linked above and consider your most common PC tasks. For the average user the most commonly used RAID array is a pair of similar drives in RAID 0 formation, which provides the best all-round performance at minimal cost. RAID 0 usually beats a single drive configuration in terms of speed, particularly for large file movements, due to there being two independent drives seeking data in place of one. However RAID 0 also provides absolutely no fault tolerance at all, and in fact doubles the chance for data loss. If one of the drives suffers a serious error or is damaged, you lose all the data on both drives since the data is split evenly ('striped') across both drives. Therefore if you require proper protection against data loss, combined with good desktop performance, you should consider a RAID 5 or RAID 10 configuration which is more costly, but far safer.

While setting up striped RAID arrays - that is, RAID arrays which split data evenly across two or more drives (such as RAID 0 or RAID 5), you will need to determine a Stripe Size - the smallest unit of data allocation - to be used in your RAID BIOS. In general, if you are uncertain of the size to choose, use the Auto setting (if available) or a 64kb stripe. If you use the drives primarily for gaming I suggest a smaller stripe size such as 16kb, as this can assist in reducing stuttering in games.

In any case once you have connected your drives and set up your RAID array using the options in the motherboard's BIOS, you may need to have a disc or USB flash drive handy with the correct RAID drivers prior to starting the Windows installation procedure. Then during Windows installation, on the screen where you select which drive to install Windows onto, if your RAID drives are not shown as a single logical drive with the correct size and volume name, you will need to click the 'Load driver' link, insert a disc or connect a device with the appropriate SATA/RAID driver, load up the relevant drivers, then click Refresh on the drive selection screen. If you miss this step, the RAID drives may not be correctly detected by Windows as one large drive, and you will not be able to install Windows on them properly or you will break the RAID array and lose the benefits of RAID.

Copyright © 2010 Koroush Ghazi

Once Windows Vista is successfully installed on your RAID drives, from that point onwards there are no special considerations as such; the drives are treated as one large normal drive for all intents and purposes, though remember that under certain RAID configurations such as RAID 0, a single faulty drive can see the loss of all your data on the RAID drives.

File Systems

During the formatting of your hard drive and/or its partitions, you can choose to format using the NTFS (NT File System) or FAT32 (File Allocation Table) File System. The file system used on a drive determines how the drive will store and organize data, so it is an important choice. You can see a comparison of the two file systems in this Microsoft Article. Windows Vista actually uses an enhanced version of NTFS called Transactional NTFS which allows Vista to perform single and multiple file operations more securely and with greater data integrity. This newer version of NTFS also allows other changes, such as Directory Junctions and improved searching - see the Windows Explorer and Windows Search chapters for details.

In general your drive(s) should be formatted in NTFS only. The only possible reason for using the earlier FAT32 file system on a drive or partition would be for compatibility purposes, such as when considering installing an older version of Windows. If you want to convert an existing FAT32 drive or partition to NTFS, it is strongly recommended that you reformat the drive in NTFS. However if that is not possible or not desirable, you can convert the FAT32 drive to NTFS using the instructions in this Microsoft Article.

32-bit vs. 64-bit

The final choice to make is whether you install Windows Vista 32-bit (also called x86) or 64-bit (also called x64). For more details of 64-bit computing see this Wikipedia Article, and also see this Microsoft Article. Most editions of Windows Vista do not come with a 64-bit Vista DVD; only Vista Ultimate contains the 64-bit DVD along with the regular 32-bit DVD. For other editions of Vista you will need to either specifically purchase the 64-bit version of a particular edition of Vista, or order a 64-bit installation DVD as detailed in this Microsoft Article. In any case the following things should be considered when deciding whether to install 32-bit or 64-bit Vista:

- Vista 64-bit only runs on 64-bit Processors. Fortunately all recent CPUs are 64-bit, but specifically all Intel Pentium D, Xeon, Core 2, Core i5, i7, i9 and Extreme Edition based CPUs or newer, and all AMD Turion, Opteron, Athlon64, X2 and Phenom or newer CPUs support 64-bit computing. See the System Specifications chapter for details of how to determine your CPU's specifications and abilities. For example, using CPU-Z and checking under the Instructions section of the main CPU tab, you should see a 64-bit related instruction set such as EM64T or AMD64 listed if your CPU supports 64-bit. A quicker way to check is to use the free SecurAble utility which does not require installation - simply download and run the small file and you will see in the 'Maximum Bit Length' field whether your CPU supports 32 or 64 bits.
- Vista 64-bit requires that all device drivers be designed specifically for 64-bit and that they be signed. Vista 64-bit cannot use 32-bit drivers, and can only use unsigned drivers with a tedious workaround at each bootup (pressing F8 at each startup and selecting 'Disable Driver Signature Enforcement'). This can mean that some older or less popular hardware may never receive Vista 64-bit signed drivers, or not get updates to them as frequently, because of the extra costs to the hardware manufacturer of development and having them signed. This is only a major concern if you have older hardware, as almost all recent hardware receives good Vista 64-bit support. See the Windows Drivers chapter for more details.
- Vista 64-bit can use 4GB or more of RAM efficiently, whereas Vista 32-bit cannot - the 4GB RAM limit is a technical limitation of the 32-bit architecture. See the Boot Configuration chapter for more details.
- Vista 64-bit does not support 16-bit programs, and while it can use all 32-bit programs, there are usually no performance benefits when doing so. However programs designed specifically for 64-bit computing will have improved performance and/or stability under Vista 64-bit.

Copyright © 2010 Koroush Ghazi

In general, it is recommended that anyone with a modern PC choose Windows Vista 64-bit. Unless you have specific hardware for which appropriate 64-bit drivers are not available, or you use programs which you know are not supported under 64-bit, the choice of 64-bit Windows is optimal. In fact if you have 4GB of RAM or more, there is no reason to use Windows Vista 32-bit, since doing so will result in much of the memory effectively being wasted. The level of support for 64-bit Windows has grown dramatically in the past few years, and this is primarily because of the fact that 64-bit computing is a logical and inevitable evolution of 32-bit computing, and must occur as programs become increasingly more complex and data-intensive, especially games. Rapid adoption of 64-bit Windows starting with Windows Vista has ensured that driver and program support is now excellent.

Note that once you install Vista 64-bit, there will be few if any noticeable differences between it and the 32-bit version on the surface - most of the differences are not obvious to users. The most prominent differences users will notice are as follows:

§ In Windows Explorer you will see both the *\Program Files* directory and a new *\Program Files (x86)* directory. The main Program Files directory is for native 64-bit programs, while the (x86) version of the directory is for 32-bit programs - Windows will usually determine which directory to install a program in automatically. In fact it makes no practical difference which directory a program is installed to, it will work regardless, so if given the choice, and you're not clear on whether a program is a native 64-bit application, simply choose the *\Program Files (x86)* directory.
§ In Windows Explorer you will see a *\Windows\SysWOW64* directory under the *\Windows* directory. WOW64 stands for Windows 32-bit on Windows 64-bit, and it handles the emulation of a 32-bit environment for non-64-bit applications. You do not need to manually install anything in this directory nor do anything for this emulation to function correctly.
§ If you use the Windows Registry Editor, you will see an option to create `QWORD (64-bit)` keys. In practice it is not necessary to use this feature unless specifically instructed to.
§ In the Windows Control Panel you will see that certain items have the (32-bit) suffix. This has no practical impact on the functionality of these items.

For all intents and purposes 64-bit Windows Vista looks and feels precisely the same as 32-bit Windows Vista, so you should not be concerned about any major changes in functionality or usability if you are switching to 64-bit Windows for the first time. The most important changes are under the hood, and provide the potential for greater performance, security and stability. Only very old or low-end systems should use Windows Vista 32-bit.

< INSTALLING WINDOWS

At this point you are ready to begin the actual format and installation process for Windows Vista. This section details the procedures required to install Vista, but it also assumes that you have read all of the sections above and considered which options suit you best. It is strongly recommended that you take the time to research and consider factors such as whether you want a dual boot configuration, the number of partitions you have on your drive(s) and/or whether you wish to use a RAID configuration prior to starting the installation process. There is no point rushing the installation, only to have to go through it again soon afterwards because you overlooked something.

The official Vista installation options are covered in this Microsoft Article. You can also see more detailed instructions of how to install Windows complete with screenshots using one of these guides:

Vista Upgrade Install Guide
Vista Clean Install Guide
Vista Dual Boot Install Guide

Copyright © 2010 Koroush Ghazi

I will still run through the installation procedures step by step below, noting the various options available depending on what particular type of installation you wish to do, and include any recommendations I have:

STEP 1 - START THE INSTALL

There are two main ways to start Windows Vista installation depending on the type of install you want:

Upgrade Install or Dual Boot

An Upgrade Install or Dual Boot installation of Vista will require that you first load up your existing version of Windows and then insert your Vista DVD and run *setup.exe* on the disk if Setup doesn't run automatically. This is necessary for Vista to correctly identify your existing version of Windows. If you are going to do an Upgrade Install of Vista over an existing installation of Windows XP or Windows 2000 (not recommended), first check this table of qualifying versions as some editions of XP/2000 cannot be upgraded to certain editions of Vista in this manner.

Clean Install

A Clean Install of Windows Vista will erase all data on the target drive/partition - it will not keep any existing files or settings on that drive. Make sure you have backed up all your data appropriately. To start a Clean Install, go into your BIOS and set your DVD drive as the first boot device, and make sure all your hard drives are correctly connected, configured and detected in the BIOS. Then insert your Vista DVD in the optical drive and reboot your system, pressing any key when prompted on the screen to boot up via the optical drive.

Note: If you are using an Upgrade Edition DVD of Vista, normally you can only do a clean install of Vista by first booting into an existing qualifying version of Windows, then selecting either an Upgrade Install or a Clean Install as above. However there is a method which allows you to do a clean install by booting up from your Vista DVD on a newly formatted drive. Refer to this article for details and note that it is legal only if you actually qualify to install an Upgrade Edition by owning the correct previous version of Windows.

STEP 2 - INSTALL NOW

On the first Vista Installation screen, if you booted from the Vista DVD you will be asked to select your Language, Time & Currency Format and Keyboard method. Set these correctly and click Next.

Once you've done this, or if you started Vista installation from within an existing version of Windows, the next screen you will see should have a large 'Install Now' button. Click this to start installation.

Note: If you aren't certain of your hardware compatibility with Vista or you want to migrate your settings from your current install of Windows to Vista (See Migrating Files and Settings further above), then click the relevant link. The migration link only appears if you launch the Vista setup from within an existing install of Windows. Alternatively if you booted up from the Vista DVD, the 'Repair your computer' link will be shown instead, and its functionality is covered under the Backup and Recovery chapter.

STEP 3 - GET IMPORTANT UPDATES

You will be prompted to check for important updates prior to installation. If you are connected to the Internet, it is recommended that you get the latest updates now, but this can be done later manually so it is not critical.

Copyright © 2010 Koroush Ghazi

STEP 4 - ENTER PRODUCT KEY

You will be prompted to enter your 25 character Vista Product Key. This Product Key identifies the edition of Vista you purchased. If you don't enter your key, you will be able to choose any version of Vista to install, and there is also a method for extending your Activation grace period to 120 days from within Vista such that you can test these other editions - see the Windows Product Activation & Validation chapter. Unless you want to undertake such a trial, or you still expect to make changes to your hardware configuration, I recommend entering your key now and ticking the 'Automatically activate Windows when I'm online' box.

STEP 5 - UPGRADE OR CUSTOM INSTALL

You will then be prompted to accept the End User License Agreement (EULA), which you should read and accept if you wish to continue installation. More details of the EULA conditions are in the Windows Product Activation & Validation chapter.

At this point, you will get the choice to do an Upgrade install or a Custom (Advanced) install which translates to a clean installation. The Upgrade installation option should only be chosen if you want to do an Upgrade install; all other configurations including dual boot should choose the Custom option.

If you do choose an Upgrade install, you will be given a Compatibility Report indicating which of your currently installed programs and drivers may be problematic under Vista, and you can stop installation at this point without any problems or changes to your existing Windows install if you feel there are too many issues identified. If you choose to proceed with the Upgrade installation, the procedure will be similar to that outlined in the steps below, but not exactly the same, since for starters the target drive has to be the one on which your current install of Windows is sitting. Once again, an Upgrade installation is not recommended.

STEP 6 - SET TARGET DRIVE

The next screen is an important one, as it allows you to choose the logical drive where Vista will be installed. You should see a list of all the existing drive(s) correctly displayed in the format: *Disk [No.] Partition [No.] [volumename] [driveletter].* If the drive(s) are not correctly identified, or are unformatted, then you will see something like 'Disk 0 Unallocated Space' as the title.

If you have SATA or RAID configured drives, to ensure that they are correctly identified, you will need to click the 'Load driver' link at the bottom of this box, and then insert an appropriate floppy disk, CD/DVD or USB flash drive containing your SATA/RAID drivers and load all the relevant controller drivers needed. Once done, click the Refresh link at the bottom of the screen and your drives should be shown correctly. If they still aren't then you may have to abort installation (click the red X button at the top right of the screen) and either get more appropriate drivers from your motherboard manufacturer's website and/or check your BIOS to see if the drives are configured correctly. If Vista does not detect your drives properly at this stage you will either be unable to install Windows, or the installation will not work as intended especially if you are attempting a dual boot configuration or using a RAID configuration.

If you booted up with the Vista DVD you can choose to format or partition any drives here by highlighting the relevant drive and clicking the 'Drive options (advanced)' link at the bottom right of the screen. Note that this option is not available if you started setup from within Windows, so if necessary abort installation and follow the steps under the Partitioning section further above if you want to partition your drives.

If your drives are partitioned and formatted the way you want them and are detected correctly, highlight the relevant drive or partition to which you want to install Windows Vista. Remember that if you want to create a dual boot configuration, your existing version of Windows and Vista must be on separate partitions or drives, so select the drive/partition on which your current install of Windows is not resident otherwise you will simply wind up overwriting (deleting) your existing Windows install.

Copyright © 2010 Koroush Ghazi

Once the suitable logical drive is selected, and you are certain you want the installation to proceed, click the Next button. Any existing contents of the target drive or partition will be lost as Vista installs over it. Note that Vista allows resizing and repartitioning from within Windows, so you can alter your partitions to some extent in the future without having to reinstall - see the Computer Management section of the Control Panel chapter.

STEP 7 - AUTOMATED INSTALLATION

From this point on, no user interaction is required for some time as Vista begins to copy across the compressed image of itself to your target drive, expands it and configures the required features and updates. Your PC will then restart and will complete installation before rebooting again.

STEP 8 - BASIC USER SETUP

Vista will then commence on the final phase of the installation which requires your input. Each section is covered below:

User Account details: This is quite important. You will be asked to enter your preferred Username and Password for the first User Account on this system. This User Account will have Administrator privileges - see the User Accounts section of the Control Panel chapter and the User Account Control section of the PC Security chapter for details. The User Account Username will also be used to label the base directory of your personal folders, so choose something relatively simple but descriptive, like your first name. If you share this PC with others, want to have multiple user accounts, if the PC is physically accessible by others you don't trust, or you simply have security concerns, then enter a password. If this is not the case, for convenience's sake I recommend not entering a password (leave the Password fields blank and click Next) for the moment. You can always change these settings later. Select a user picture, and note that this too can be easily customized to any image of your own choice later. These details are covered under the User Account section of the Control Panel chapter.

Computer Name & Wallpaper: The computer name is primarily for identifying the PC in a network of computers. As such you should not need to change this, the default of *[Username]-PC* should be fine for a home PC. You can also select a background wallpaper for your Windows Desktop here. Once again this can be easily customized to any image of your choice later as covered under the Graphics & Interface chapter.

Important Updates: You will be asked to configure Vista's basic security and online update settings. To maintain good security during the initial startup period I recommend clicking the 'Use recommended settings' option at the top, as we will modify all these options later in the book anyway.

Time and Date: Set your correct time zone, time and date, and also I recommend ticking the 'Automatically adjust clock for Daylight Saving Time'.

Computer's Current Location: This screen asks you to set your location for networking/Internet connectivity purposes. The options are Home, Work or Public Location. Ironically, for the average standalone home PC connected to the Internet the best choice is actually 'Public Location' not Home, as this allows you to connect to the Internet with full functionality but maintains tighter security. You can customize these settings later as covered under the Network & Sharing Center section of the Control Panel chapter.

Copyright © 2010 Koroush Ghazi

STEP 9 - WINDOWS EXPERIENCE INDEX & STARTUP

Vista then launches into its final setup phase, which may take a while, during which your system performance is measured by the Windows System Assessment Tool to determine your hardware's Windows Experience Index, and hence whether certain features will be enabled or not - see the Performance Measurement & Diagnostics chapter for details. You will eventually reach the Welcome Center, which you can browse or close immediately as it is not a particularly necessary feature. You will be able to disable the Welcome Center from running at startup each time by unticking the small 'Run at startup' box at the bottom left of the Welcome. If the box is unavailable it should be there upon the next bootup.

At this point you can continue with the rest of the book, but a few things to keep in mind:

- Make sure to go into your BIOS and reset your system drive(s) as the first boot device if you had set your optical drive as the first boot device for Windows installation purposes.
- Make sure to remove the Vista DVD and any floppy disks from your drives before rebooting.
- Limit any Internet browsing or other online activities until you've gone through the PC Security chapter.
- Don't Activate your PC straight away if you plan on making any major physical changes to the hardware configuration of your PC, or if you believe you'll be reinstalling Vista again within the next 30 days; wait until you've bedded down your configuration before activating. This is because multiple activations within a short period of time are viewed as suspicious by Microsoft - see the Windows Product Activation & Validation chapter for details.

Since this book has been designed to cater to both those who are doing a new installation of Vista, and those who are using an existing installation of Vista, it follows a roughly sequential order as to the types of things I would recommend configuring after doing a new installation, but any chapter can also be read by itself if you want to focus on a particular topic first. I would however strongly recommend becoming familiar with the contents of the Windows Explorer and PC Security chapters as soon as possible, along with (re)reading the Vista Usage Notes chapter at the start of this book.

Copyright © 2010 Koroush Ghazi

BOOT CONFIGURATION

Windows Vista has a different bootup configuration than earlier versions of Windows. Instead of using a simple *Boot.ini* file as in Windows XP, Vista has a special Boot Configuration Data (BCD) database to hold all the relevant bootup parameters, and to allow compatibility with new bootup methods. However this change also makes boot configuration and editing much more tricky. Editing the boot configuration is particularly important if you've installed a dual boot setup of Vista as covered in the previous chapter. For the most part, you should not need to edit or alter the Vista boot configuration unless you're troubleshooting a system problem, attempting to use more than 4GB of RAM on 32-bit Windows, or you want to repair the boot configuration. There are several ways you can view and modify your Vista boot configuration, and each is covered in more detail below.

< BCDEDIT

BCDEdit is a built-in command line tool for altering the boot configuration in Vista. It must be used from an Administrator Command Prompt. The full list of BCDEdit command line options is in this Microsoft Article. Given it is a complex tool to use, it is not recommended that you edit the boot configuration this way - I recommend using the tools below instead, at least to start with.

< STARTUP AND RECOVERY

The easiest method to alter your basic bootup options is to go to Control Panel>System>Advanced System Settings, or go to Start>Search Box, type *systempropertiesadvanced* and press Enter. Then click the Settings button under the 'Startup and Recovery' section of the Advanced tab.

In the Startup and Recovery box, under System Startup if you want a Boot Menu to be shown when your PC first loads with a list of all installed Operating Systems, tick the 'Time to display list of operating systems' box and in the box next to it choose how many seconds you want the Boot Menu to remain on screen before it automatically loads up the default OS. If on the other hand you don't want a boot menu to be shown at all, and want the default OS to load up straight away, untick the box.

The 'Time to display recovery options when needed' box should be ticked, and a reasonable amount of time entered, such as 15 seconds or more. The recovery options menu will only appear if you run into problems with Vista, and its features (such as Safe Mode) are covered under the Backup & Recovery chapter.

< MSCONFIG

Another way to alter the boot configuration is to use the Microsoft System Configuration utility (MSConfig). Go to Start>Search Box, type *msconfig* then press Enter. Go to the Boot tab of MSConfig and you will see under the 'Boot Options' section there are several options for altering the way your PC boots up. These are primarily used for troubleshooting purposes. Highlight the install of Windows Vista you wish to alter then you can select one of these options to apply to it:

Safe Boot: If selected, the next boot will be into Safe Mode, as detailed under the Backup & Recovery chapter. Default Safe Mode is called Minimal; 'Alternate Shell' is Safe Mode with Command Prompt instead of GUI; 'Active Directory repair' is Safe Mode with GUI and Active Directory; Network is Safe Mode with GUI and Networking features enabled.

Copyright © 2010 Koroush Ghazi

No GUI boot: Removes the default Windows Vista 'scrolling bars' startup screen when booting up, replaces it with the Aurora image. See the Graphics & Interface chapter for more details on how to customize the boot screen.

Boot log: Records all bootup information in a *Ntbtlog.txt* logfile stored under your *\Windows* directory.

Base video: Boots up Windows using the default Windows graphics driver rather than the specific graphics driver for your graphics hardware. Useful if a recent graphics driver installation is preventing you from booting up.

OS boot information: Shows the names of all the drivers as they're being loaded during bootup.

The Timeout value in the box on the right is the same as the 'Time to display a list of operating systems' setting covered under 'Startup and Recovery' further above - it controls how long the boot menu for multiboot systems is shown.

If you click the 'Advanced Options' button you will see more advanced bootup options for troubleshooting:

Number of processors: If you have a multi-core CPU, ticking this option allows you to manually force some or only one of the processors (cores) on the CPU be detected and used by Windows during bootup. However, this is not a performance option, it is only related to troubleshooting by artificially limiting the number of cores on your CPU being used to determine if there is a fault with one of them. The default setting of having this box unticked is optimal and results in the best bootup time.

Maximum Memory: Allows you to manually force Windows to only use a certain amount of RAM on your system, up to and including your full physical RAM amount, for troubleshooting purposes. Amount entered is in Kilobytes (KB).

PCI Lock: Stops Windows from dynamically assigning system resources to PCI devices. The devices will use the BIOS configuration instead. Of no practical use to most users.

Detect HAL: Forces Windows to redetect the Hardware Abstraction Layer (HAL) in case your hardware is incorrectly being detected/reported.

Debug: Starts Windows in debugging mode, with a range of options as to where to write the debug output. Again, of no practical use to most users.

Once done selecting which bootup options you wish to apply to the boot configuration, click the Apply button then OK, and these option(s) will come into effect on next boot. Should you wish to apply any permanently, you can tick the 'Make all boot settings permanent' box. Generally I recommend using MSConfig to test a boot option, and then using BCDEdit or VistaBoot Pro to make it permanent.

< THIRD PARTY TOOLS

Aside from the built-in tools above, there are a range of third party tools you can use to do what is covered above more easily and more safely.

VISTABOOT PRO

VistaBoot Pro is a tool for editing the boot configuration in Vista using a graphical interface and does not require detailed knowledge of how the BCD works. Upon installation you will be prompted to make a backup of your BCD database, which is strongly recommended before you do anything else. Should

Copyright © 2010 Koroush Ghazi

anything undesirable occur with the BCD, you can click the 'Backup/Restore Center' button and restore your original backed up BCD files.

VistaBoot Pro has a range of functions, but we'll cover only the major ones here. On the main 'View Settings' screen in VistaBoot Pro you can see a summary of the data held in the BCD. If you have a dual or multiboot setup, you should see all the operating systems listed with the correct drives shown. You can expand this display by clicking the Detailed or All buttons at the top of the text display area. The information here is useful for troubleshooting, and also gives you an idea of the kind of data held in the BCD.

If you want to alter these entries, click the 'Manage OS Entries' button. Here you can set the default OS and the timeout, though these are best altered using the normal Vista Startup and Recovery options as covered further above. Of use for multibooters, you can rename the OS entries which show up in the Boot Menu. By default, Vista insists on calling your older Windows operating system 'Earlier version of Windows' in the Boot Menu, and it calls Vista simply 'Microsoft Windows'. To help prevent confusion and make things neater, click on each OS listed and tick the 'Rename selected operating system' checkbox - new options will appear allowing you to provide a new name and also change the drive letter if necessary. You can also add a new (Windows) OS listing here by ticking the 'Add new operating system entry' option and filling in the details. Finally, you can change the order in which the OSes are listed by highlighting the relevant OS and using the up or down arrows to the right.

The 'Advanced Settings' include various advanced features which the MSConfig utility can also accomplish, and these are described further above. Some additional useful features you can use VistaBoot Pro for are:

Disable Vista Driver Signing: By default the 64-bit version of Vista only allows signed drivers to be installed and loaded up. Ticking this option attempts to override that limitation - has no impact on 32-bit Vista editions. Note that this method has been disabled by Microsoft in recent updates, so this option is unlikely to work if selected.

Physical Address Extension: If ticked, this option enables Physical Address Extension (PAE) in Vista. This is necessary for correct memory detection if you have more than 4GB of RAM in Windows Vista 32-bit.

Data Execution Prevention: Data Execution Prevention (DEP) is on by default, but can be turned off by unticking this option. DEP is covered in detail in the PC Security chapter and usually should not be disabled.

Finally, the 'System Bootloader' section of VistaBoot Pro allows you to attempt to fix any problems with the Vista bootloader, or to uninstall it if you've removed Vista or the other OS from a dual boot system. By default, simply deleting/reformatting/removing one of the OS drives or partitions in a dual boot configuration will cause startup problems since the bootloaders are interdependent. This option lets you to remove the relevant bootloader before deleting that OS so that you can boot into the other OS as normal.

VistaBoot Pro is a very useful tool for easy BCD editing, however if in doubt do not alter any settings, and if you wind up seriously damaging your BCD or any other Vista boot files, use the Startup Repair functionality of Vista to fix the problem (See the Backup & Recovery chapter), or see the instructions here.

EASYBCD

EasyBCD is another free automated utility which makes editing the Vista boot configuration much easier. However it is virtually identical to VistaBoot Pro in terms of its major features and functions, so it will not be covered in detail here. You can use either utility to achieve much the same results.

Copyright © 2010 Koroush Ghazi

< BOOTDISKS

As mentioned in this Microsoft Article, Windows Vista does not use Boot Disks any more; the original Vista DVD is effectively a boot disk. If you're having problems booting up Windows, you can boot up using the original Vista DVD then use Startup Repair to automatically detect and repair any issue preventing proper Windows startup. You can also access the DOS Command Prompt in the Vista Recovery Tools if necessary. Details of these functions are covered under the Backup & Recovery chapter.

If you still want to create a Vista bootup disk, you can do so according to the details here. If you want to start up your PC in very basic DOS mode and the Command Prompt mode of the Vista Recovery Environment is not appropriate since it only provides an emulated DOS-like Command Prompt interface, then you must use the instructions and tools provided at BootDisks or the Ultimate Boot CD utility to create a bootable floppy or CD. Alternatively, you can use the instructions provided here to make your USB flash drive bootable into DOS mode, but bear in mind that you also need to alter your BIOS options to allow correct bootup from a removable device like a USB flash drive.

On balance there aren't many reasons to manually alter your boot configuration under normal circumstances, so approach the use of the tools and methods in this chapter with caution rather than any desire to experiment.

Copyright © 2010 Koroush Ghazi

WINDOWS PRODUCT ACTIVATION & VALIDATION

To confirm that you are running a legitimately purchased copy of Windows Vista in accordance with the terms of the End User License Agreement (EULA), Microsoft relies on Windows Product Activation, a process which verifies your Product Key and hardware configuration online or over the phone. While activation has been around since it was introduced in Windows XP, some of the measures surrounding it have been tightened as part of the new Microsoft Software Protection Platform. This chapter looks at how Activation and Validation work, though note that I don't cover any illegal methods of bypassing these systems.

< LICENSING AGREEMENT

The End User License Agreement (EULA) for Windows Vista contains the terms and conditions of acceptable usage for the OS. This section attempts to provide the most important practical considerations which arise from the standard user license in plain English. Importantly however, what follow are my interpretations of the license terms based on research, but for legal reasons this should not be considered a replacement for actually reading the license yourself, as your license terms and conditions may differ for a range of reasons.

The reason you require a license for Windows Vista is that, as with previous versions of Windows, and indeed most modern software, you do not actually own the software outright. Microsoft gives you permission (a license) to use a copy of their software as long as you operate it in accordance with certain terms and conditions, to which you explicitly agree during the installation of Windows. The key points are explained below.

OEM VS. UPGRADE VS. RETAIL EDITIONS

While their contents do not differ, there are some notable differences between the license conditions for OEM (Original Equipment Manufacturer) editions of Vista - sometimes called 'System Builder' editions - versus the Upgrade editions vs. the Retail editions:

OEM: An OEM edition of Windows Vista usually comes pre-installed on, or accompanying, a new PC or the purchase of one or more major hardware components. The license is bound specifically to the first PC on which it is installed. If you substantially alter that PC's hardware, or you attempt to reinstall the OEM copy on a different PC, you may fail activation since you have technically breached the licensing conditions. There are other limitations applying to OEM versions, including limited or no technical support from Microsoft. This is why OEM copies are the cheapest editions to purchase.

Upgrade: An Upgrade Edition requires that you already own a qualifying previous full version of Windows XP or Windows 2000. However in terms of upgrading your PC or transferring Vista to a new PC, there are no specific limitations on the number of times you can do this.

Retail: The full Retail Edition does not require the ownership of any other version of Windows, and can be installed on any PC, and allows unlimited upgrades or moves to another PC. This is why it is the most expensive edition.

However all editions of Vista must adhere to the following general conditions of use.

Copyright © 2010 Koroush Ghazi

GENERAL CONDITIONS OF USE

Some important conditions of use you should consider from the EULA for the average home PC user are spelled out in plain English below:

§ The OS is licensed to one specific device at any time, namely the PC on which it is installed. You can't install the same copy of Vista on multiple PCs unless you have specifically purchased multiple licenses - one for each PC.
§ If the edition includes both the 32-bit and 64-bit version of Vista, you can use one or the other, but not both at the same time. Even if you order a 64-bit version of your edition, you cannot install and use both 32-bit and 64-bit editions at the same time, whether on the same machine or separate machines.
§ You can transfer Vista from one PC to another as many times as you want, as long as it is not installed on more than one machine at a time. However this does not apply to the OEM version which is always bound to the first PC on which it was installed.
§ You can upgrade or alter the hardware in the PC on which Vista is installed as often as you wish. This does not apply to the OEM version, for which any major system upgrades may invalidate the license.
§ You must Activate your copy of Windows within 30 days of installation, and you must allow it to periodically connect to the Internet to Validate - see further below for details. Some OEM versions of Vista come pre-installed and already activated, so manual activation is not required.
§ You are allowed to make one backup copy of the Vista DVD for your own use.

The above has been provided for information purposes only and cannot be the sole basis for any actions you take - you must read the specific EULA which accompanies your particular edition of Windows carefully to ensure you understand all the licensing terms and conditions as applicable to you in your country and based on your particular circumstances. For example, if you have purchased a PC with Windows Vista pre-installed from a certain hardware manufacturer, your OEM copy of Windows Vista may have different or additional terms and conditions than those specified here or elsewhere.

< ACTIVATION

This section goes through the procedure for activation, and also addresses any common issues you may experience.

PRODUCT KEY

When you first install Vista, you will be prompted to enter your Product Key, which appears as a series of 25 letters or numbers separated by dashes in the format: xxxxx-xxxxx-xxxxx-xxxxx-xxxxx. This key can be found on a sticker on your computer if you purchased the PC with Vista pre-installed, on the installation disk holder of your Vista retail package, or on the Vista manual. The Product Key is very important for two reasons:

§ The Vista installation DVD contains all versions of Windows Vista, from Home Basic through to Ultimate - it is only the Product Key which tells Vista the correct version which you are licensed to install.
§ The Product Key is integral to validating and activating your copy of Windows Vista. If the key is used by anyone else at the same time as you, or on another one of your PCs, this will invalidate your key.

Make sure you keep your Product Key in a safe place, do not share it with anyone else and if your PC or copy of Vista did not come with a Product Key then contact your retailer or the person from whom you purchased the Vista DVD and ask them to give you one as it is absolutely necessary - unless you are in a corporate or business environment. If you wish at any time to alter your Product Key while using Vista, you can do so by going to Control Panel>System and clicking the 'Change product key' link at the bottom of the box. Entering a new key will require you to reactivate. If you want to look at options for purchasing additional Product Key(s) online from Microsoft see here.

Copyright © 2010 Koroush Ghazi

ACTIVATION

Once you have installed Windows Vista, you will have exactly 30 days within which to activate Windows. During this time you can use Windows Vista as normal, but you will regularly be prompted to activate. To see how many days you have left before your activation grace period runs out, either click the prompt which appears in the Notification Area, or go to Control Panel>System and click the link at the bottom of the box, or go to the Start>Search Box, type *slui* and press Enter.

If you are aware that your PC may undergo some further changes shortly, such as the installation or removal of key pieces of hardware it is recommended that you do not activate Windows right away. You have 30 days within which to bed down your final hardware configuration and I suggest you use it. Activating before your hardware setup is finalized could see you having to re-activate repeatedly, including having to call Microsoft to complete Activation or running into other potential complications. Microsoft generally views multiple activations in a short space of time as quite suspicious.

There is a legal method by which you can attempt to extend the grace period before Activation by another 30 days, up to a maximum of 120 days in total, before you must Activate. Follow these steps to do so:

1. Open an Administrator Command Prompt.
2. In the Command Prompt type `slmgr -rearm` and press Enter.
3. Reboot your PC and you should now have an additional 30 days before Activation.
4. You can repeat Steps 1 - 3 above to give you a total of 120 days maximum before Activation is required.

This is useful if you want to bed down your hardware prior to final activation, or if you want to try out one of the different editions of Vista, by not entering a Product Key during installation and extending the Activation period. However at some point you will have to Activate for your copy of Vista to be legal.

Once you are ready to activate, use one of the means further above to access the activation application and click the 'Activate Windows online now' button. When activation commences, you will automatically connect to a Microsoft server and send several pieces of information specific to your system including:

§ The version of the OS and the version of the activation software.
§ Your language.
§ Your Product Key.
§ The Internet Protocol (IP) address of your PC.
§ A set of non-unique hardware hashes generated based on your hardware configuration. These hashes don't have any personal information, nor can they be used to determine the make/model of your PC.

If automatic activation fails or you are not connected to the Internet, you will be given instructions on how to activate Vista by contacting Microsoft over the phone. If Activation succeeds you will not be required to reactivate Windows Vista again unless:

§ You substantially alter the PC's main hardware components, or possibly if a driver update makes your hardware appear to be different.
§ Your Product Key is found to be in use by another system and/or turns out to be an illegally obtained one.
§ There are signs of tampering with Windows to circumvent Activation.

For more details of exactly what Activation entails, and under what circumstances you may need to do it, see this Activation FAQ.

Copyright © 2010 Koroush Ghazi

REDUCED FUNCTIONALITY MODE

Prior to Vista SP1, if you had not activated successfully within 30 days, or if you did not reactivate within 3 days after any major hardware changes, or were found to be running a non-genuine version of Windows, you would enter Reduced Functionality mode. This meant that certain features and capabilities of Vista were disabled as detailed in this Microsoft Article. However as of Vista SP1, Microsoft formally removed Reduced Functionality Mode. Non-genuine copies of Vista will not have any reduced functionality - the user will only experience the following:

§ A prompt at every logon requesting activation.
§ The Desktop Wallpaper will turn black and a flashing activation dialog will appear every hour. Even if you reset the wallpaper to something else, it will again turn black within an hour.
§ A 'This copy of Vista is not genuine' stamp will be placed at the bottom right hand corner of the screen.

You will need to successfully activate your copy of Vista with a valid product key to get back to normal. If you were lead to believe your copy of Vista was genuine when you purchased it, contact Microsoft and report the details of where and how you purchased this copy of Vista.

< VALIDATION

Alongside Product Activation, Microsoft has implemented an additional anti-piracy feature into Windows called Windows Genuine Advantage (WGA) Validation, or just Validation for short. Windows Vista will periodically connect to Microsoft servers to validate itself, sending similar information to that sent under Activation (see further above). This validation may also occur when you connect to Windows Update or download certain Microsoft updates. If Validation fails, the user will not be able to download updates from Microsoft, and can only download critical security updates through the Microsoft Download Center or through Windows Update set to automatically update (See the Control Panel chapter). The OS may also exhibit the symptoms described under the Reduced Functionality Mode section above.

If you are having problems with WGA on a legitimate installation of Windows, visit the Windows Genuine Advantage Diagnostic Site. If you use Firefox as your main browser, Microsoft has released a Firefox plugin to allow WGA to work on this popular browser.

If you are still having problems with Activation or Validation, the only correct course of action is to contact Microsoft Technical Support for your particular country.

Copyright © 2010 Koroush Ghazi

WINDOWS EXPLORER

Windows Vista uses the Explorer interface as the primary means for manipulating files and folders in Windows. This interface appears in Windows Explorer as well as in many applications which prompt you to open or save files, and of course in most standard Desktop windows. Windows Explorer can be accessed in several ways, including by going to Start>All Programs>Accessories, or by going to Start>Search Box, typing *windows explorer* and pressing Enter, or by clicking on the Computer link in the Start Menu, or by pressing WINDOWS+E at any time. The interface is familiar to any Windows user and the basics have remained the same, however there are important changes and handy new features which are explained in more detail in this chapter.

< BASIC FEATURES

Instant Search: The Instant Search box is present in all Explorer interfaces, shown at the top right of the window. This is a very useful feature which allows you to quickly refine what is displayed in the current window by typing in a search term or even partial characters. This feature is covered in detail in the Windows Search chapter.

Address Bar: At the top of each Explorer-based window is an Internet Explorer-like Address Bar which has back and forward arrows at the left, a refresh button at the right, and the path to the currently displayed directory in the address box. Useful aspects of the Address Bar include:

§ You can view/jump to any subdirectories under each branch of the displayed path by clicking the small black arrow next to that particular directory branch.
§ You can type in a specific directory path by left-clicking on an empty space in the navigation pane.
§ You can click on the small arrow between the box and the arrows on the left and select a recently viewed directory to go to.
§ You can view recently opened directories by clicking the small down arrow next to the Refresh button at the far right of the box.
§ You can copy the current directory path by right-clicking in the box and selecting 'Copy address as text'.

Navigation Pane: This is the area to the left of Windows Explorer which lists quick links to your favorite folders at the top left, and below that is the normal Folders listing of all the directories and subdirectories on your drive(s).

Command Bar: Beneath the Address Bar at the top of Windows Explorer is the Command Bar which contains a range of buttons. These buttons will change depending on the particular file(s) or folder(s) you are viewing or have highlighted. For example if you highlight an .MP3 file, the command bar will display a Play button. You may also see a Burn, Share, Email, Open, Preview, Print, or Slideshow button depending on the specific file highlighted or folder type.

You will always see Organize and Views buttons on the command bar; these allow you to access a range of useful functions that let you customize the Explorer interface. Under the Organize button, aside from common tasks such as Copy, Rename and New Folder are the following features:

§ Under the Layout item you can select whether to display the Menu bar at the top of the screen - if selected the Menu Bar will be enabled permanently in Explorer and Explorer-based interfaces. If you don't wish for it to be permanently displayed, you can toggle it on or off at any time by pressing the ALT key while in an Explorer-based window.

Copyright © 2010 Koroush Ghazi

§ Under the Layout item you can select whether to enable or disable the Details, Preview and Navigation panes. The Navigation Pane is covered above, the Details and Preview panes are covered further below.
§ The 'Folder and Search Options' link opens Folder Options, covered in detail under the Folder Options section below. Importantly, you can set each folder type's view more quickly by using this option.

You can use the Views button to change the way folder contents are shown. By clicking the button you can cycle through the various available options, including Tiles, Details, Lists and Icon views. You can also use these features instead:

§ You can click on the drop arrow next to the button and manually select the view by clicking on it, or using the slider. This is particularly useful if you want to select a particular icon size for Icon view.
§ You can hold down the CTRL key and use your mouse scroll wheel to cycle through the various views.

Preview Pane: The Preview Pane if enabled sits at the right side of the Explorer window, and is usually blank if no file is highlighted. Once you highlight a particular file, a preview of the contents will be displayed where possible. Since this can increase file browsing time, disable it if you don't need this functionality.

Details Pane: The Details Pane if enabled sits at the bottom of the Explorer window, and displays details about the highlighted file or folder, including information from its Properties tab, as well as any preview of its contents if possible. Note that you can edit the properties for a file by clicking on customizable fields in the Details Pane and entering new information (if the file is not write-protected). You should disable this option if you don't need or use this functionality, as it can affect file browsing time. You can always right-click on a file and select Properties then look under the Details tab to see the same information.

Live Icons: The contents of some folders are shown as Live Icons, which are icons that show a preview of the actual current contents of the particular file - e.g. the Pictures folder. You can disable this for specific folders by switching to Details or List view for example, which helps speed up browsing such folders.

Note that if you've enabled Live Icons but they are not being displayed correctly, then you need to consider several things. Under Windows Vista 64-bit, even though 32-bit applications can run without any issues, when it comes to Windows Explorer, it runs as a 64-bit application by default, and requires that all the shell extensions (extra interface features) it uses are also compiled as native 64-bit applications for full functionality. In plain English this means under Windows Vista 64-bit the default program/codec/plugin associated with viewing particular content needs to also be a 64-bit application or the Live Icon will not be correctly generated. So for file types which are being handled by 32-bit applications, you need to install and/or associate a 64-bit application or media handler with that file type. Note that in the case of documents saved using Microsoft Office 2007 which is a 32-bit-only application, or the 32-bit version of Office 2010, Live Icons for documents won't be shown in 64-bit Windows. There is a way around this: when saving a document, select the 'Save As' option and the tick the 'Save Thumbnail' box, then save the document. It will now be saved with the equivalent of a Live Icon thumbnail preview, which can be seen in Icon View in Windows Explorer for example.

Sort By: The contents of any folder displayed can be sorted by a range of properties. By default the contents are automatically sorted in Ascending order by Name (file name), and the sorting is dynamic; that is, there is no need to refresh the screen whenever new files are added, Vista will automatically resort everything instantly to maintain appropriate order. To sort by something other than file name, right-click on a blank spot in the content area and select 'Sort By', and you will see the common properties such as Date Modified, Type and Size on which you can sort the contents, either in Ascending or Descending order. You can click the More option and select any one of a larger range of properties upon which to sort the current view of contents.

Copyright © 2010 Koroush Ghazi

Group By: You can create subcategories within a content view by right-clicking on a blank spot in the content area and selecting 'Group By', then selecting the particular property by which you wish to group the contents. This will arrange the contents under headings for each subcategory. Once again you can select the More item to see additional properties for use in grouping contents. If you wish to remove grouped view, right-click, select 'Group By' then choose the (none) item.

Stack By: Instead of grouping contents with headings, you can 'stack' files into smaller folders within the current folder. These Stacked Folders are clickable, and when opened their contents are displayed. The folders are also able to be manipulated like a normal folder, such as moving them to other subdirectories. However they are only virtual folders and their main purpose is to help you organize directory contents.

Filter By: If you only want to view a certain subset of the contents in a folder, aside from using the Instant Search box (see above), move your mouse over a column header and click on the small black arrow which appears at the right side of the header. Here you will be able to select a check box to filter the contents by a particular category. If the category you wish to use for filtering isn't available, you can add more column types by right-clicking on a column header, selecting the More item and selecting which additional columns to add.

To further customize Windows Explorer and folder appearances, you need to use the Folder Options component of the Control Panel, as covered further below.

< FOLDER OPTIONS

Folder Options can be found under the Control Panel, or by pressing the Organize button in the Command Bar of Windows Explorer and selecting 'Folder and Search Options'. As the name suggests, Folder Options has a range of options which affect the way folders are viewed, but it also has important Search-related options. Each tab of the Folder Options box is covered separately below:

GENERAL

Tasks: If the 'Show preview and filters' option is chosen, all Windows Explorer-based windows will have a Details pane at the bottom of the screen, a Preview pane at right hand side, and filter options at the top of the screen. To turn these added features off select the 'Use Windows classic folders' instead. Choose whichever one suits your taste. Note that you can manually turn off the Details or Preview panes individually in Windows Explorer - see further above. In general disabling the Preview pane improves responsiveness in Explorer.

Browse Folders: If 'Open each folder in the same window' is chosen, then launching a Windows option or utility from a window will mean that it opens in the existing window. If 'Open each folder in its own window' is chosen, a new window will open for each utility or option launched from within an existing window. I recommend the first option, as this reduces the number of open windows which in turn reduces memory usage and Desktop clutter.

Click items as follows: The 'Double-click to open an item (single-click to select)' is the default behavior most Windows users are familiar with, and the one which is assumed when providing descriptions in this book, and most places on the Internet. If you prefer a more web-like behavior, you can select the 'Single-click to open an item (point to select)', and further choose whether to have selectable items and icons underlined all the time, or only when you hover your mouse over them. In general the double-click method is most familiar and prevents accidental launching of programs or options from errant mouse clicks, so it is recommended.

Copyright © 2010 Koroush Ghazi

VIEW

Folder views: When you change the look and layout of a particular folder in Windows Explorer, such as column widths, whether files are show in List, Details or Thumbnail view and so forth, to apply your changes to all folders of that same type, click the 'Apply to Folders' button here. However you must do this for each type of folder separately; for example, the layout you choose for a music folder will not apply to anything other than other music folders. So you should take the time to set up one of each general type of folder the way you want it in Windows Explorer, then in each case open Folder Options>View, or click the Organize button in the Command Bar area of Explorer and select 'Folder and Search Options' then click the View tab, then click 'Apply to Folders' to make those changes apply to all folders of that type. Note that if you still find your folder view options are not 'sticking', see Fix Incorrect Folder Views further below in this chapter.

Advanced Settings: Most of the options in this section of Folder Options are dependent on your own particular tastes in functionality and appearance. However certain settings are important and I provide my recommendations for these below.

It is recommended that you tick the following options:

§ Display simple folder view in Navigation pane - Removes the dotted lines in the Windows Explorer folder Navigation Pane, which I believe looks better. The dotted lines can however help in quickly identifying parent directories if you have complex layers of folders and sub-folders.
§ Show hidden files and folders - Shows hidden system files and folders. It is important to have this option ticked if you want to see all the files and folders on your system, especially when using this book, but also for any future tweaking.
§ Hide protected operating system files - Shows a range of additional hidden system files and folders which under normal circumstances should be not be changed or deleted. If unticked, you will see these files and folders (such as Directory Junctions - see below), but this adds to clutter and is generally not necessary unless you're conducting advanced tweaking or troubleshooting a system problem.
§ Remember each folder's view settings - Makes sure that Windows remembers your specific folder settings for each folder. Remember though that different folder types require individual configuration as noted further above.
§ Show drive letters - Important in knowing which specific drive you're viewing (e.g. C:, D:, E: etc.).
§ Show encrypted or compressed NTFS files in color - Highlights files which have been encrypted or compressed in a different color.

It is recommended that the following are unticked:

§ Display file size information in folder tips - If enabled, holding your mouse over a file or folder will show further information; this can cause small delays while navigating so is best switched off.
§ Hide extensions for known file types - Needs to be disabled to correctly see and when necessary change the file extensions for various files, especially when undertaking tweaking.
§ Show popup description for folder and desktop items - Switching this off removes the popup information boxes which appear whenever you hover the mouse over a folder or desktop item. These are unnecessary and can also cause slight pauses while navigating folders or the desktop.

The options not mentioned above can be ticked or unticked according to your tastes, and their individual functionality is covered in this Microsoft Article.

Copyright © 2010 Koroush Ghazi

SEARCH

These options relate to the Instant Search box found at the top of every folder window in Vista, as well as the Instant Search box found on the main Start menu. This functionality allows you to find a file within the current folder, and is covered in detail in the Windows Search chapter. If you use search indexing or just want the fastest results I recommend that you enable (tick) the following settings:

§ In indexed locations, search filenames and contents.
§ Include subfolders when typing in the Search box.
§ Find partial matches.
§ Include system directories.

If you start to notice that you're often not finding what you're after, or if you've disabled search indexing, I recommend enabling the following settings instead which are slower but more thorough:

§ Always search file names and contents.
§ Include subfolders when typing in the Search box.
§ Find partial matches.
§ Don't use the index when searching the file system.
§ Include system directories.
§ Include compressed files.

Be careful as the second set of options though quite thorough may be much slower, and can tie up a great deal of system resources when searching for a non-indexed file. This may make using the Instant Search box in the Start menu in particular a pain if you just want to quickly launch common Windows programs from it, so on balance I recommend the first set of options further above for most everyone. The time difference depends on how many files and sub-folders are in the particular folder in which you've commenced a search. For a small folder, it shouldn't make a huge difference; for a system-wide search it may take quite a long time. Again, more details on optimal searching strategies are in the Windows Search chapter, and remember that search functionality isn't so much about finding lost files, it's more about making access to common files and programs much quicker.

< PERSONAL FOLDERS

Every User Account has a set of Personal Folders created for that account. They can be found under your *\Users\[username]* directory, and contain such subfolders as *Documents*, *Pictures*, *Music* and *Videos*. Note that you depending on your folder view options you may also see the legacy personal folders from Windows XP (such as *My Documents*) showing up under your main personal folder directory, but these are Directory Junctions not actual folders - see further below for more details on those.

While your first temptation may be to ignore these personal folders and create your own ones, I recommend against doing so. Aside from already being quite convenient for holding various file types, these folders are also linked to particular features in Vista, such as the User Account security features, and the Documents, Pictures and Music items you can enable on your Start Menu. Furthermore by default certain applications will initially start looking for the appropriate file types in those folders, e.g. Windows Media Player will initially open its file browser in the Music folder. So while you can place your files wherever you wish, I would strongly suggest taking advantage of this directory structure and if necessary create subdirectories under the existing folders if you want to further categorize your material - or you can use Windows Explorer's Grouping and/or Stacking features (covered further above) to sort things virtually under each folder.

Copyright © 2010 Koroush Ghazi

Fortunately the location of these personal folders is not fixed; you can move them around to another place on the same drive, or to another drive if you want to, without losing their link to key Vista features. To do so follow these steps:

1. Go to the relevant folder under your personal folders.
2. Right-click on it and select Properties, then go to the Location tab.
3. Click the Move button and specify a new folder and/or drive to move the current folder to. Alternatively you can just type the new path in the Target box.

When you're done, Windows will move the folder(s) and its contents, and now recognize the new location as the home of your present folder, and all references to it throughout Vista should point correctly to this new location automatically.

It is important to note that if you try to alter any files or folders outside your own personal folders, you will often be faced with a UAC prompt. This is due to Access Control, and the reasons behind this are detailed under the Access Control and User Account Control sections of the PC Security chapter. The bottom line is that it would be wise to take advantage of your personal folders, given they are tied in to several useful features in Vista and also require the least security credentials to alter.

< DIRECTORY JUNCTIONS AND SYMBOLIC LINKS

If you disable (untick) the 'Hide Protected Operating System Files' option under the View tab in Folder Options, you will notice that a range of new directories become visible among your personal folders. That is, under the *\Users\[username]* directory you will see additional sub-directories such as *\Cookies*, *\Local Settings*, *\My Documents*, and *\Recent*. Yet when you click on them, you will get an access error. This is because they are not actual directories and don't contain anything, they're Directory Junctions - redirection links which point to another directory, and this is also why they are denoted with a shortcut icon.

Directory Junctions exist for compatibility purposes, so that when an application originally designed for Windows XP attempts to put files or folders under the *\My Documents* directory for example (which doesn't exist in Vista), the *\My Documents* junction in Vista redirects the program to place its files/folders under the correct new *\Documents* directory. Meanwhile the application's requirements are satisfied, because it sees the directory junction as though it were a real directory of the same name, so it doesn't report any errors or problems.

Under Windows Vista the following junctions redirect to the following real directories:

Windows XP Directory / Junction	Corresponding Windows Vista Directory
Application Data	\AppData\Roaming
Cookies	\AppData\Roaming\Microsoft\Windows\Cookies
Local Settings	\AppData\Local
My Documents	\Documents
NetHood	\AppData\Roaming\Microsoft\Windows\Network Shortcuts
PrintHood	\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
Recent	\AppData\Roaming\Microsoft\Windows\Recent
SendTo	\AppData\Roaming\Microsoft\Windows\SendTo
Start Menu	\AppData\Roaming\Microsoft\Windows\Start Menu
Templates	\AppData\Roaming\Microsoft\Windows\Templates

Along with Directory Junctions, Vista also supports a similar feature called Symbolic Links. A Symbolic Link is like a shortcut, except a shortcut is actually a type of file (.LNK), whereas a Symbolic Link is not a file; it exists at the file system level. It can point to anywhere, whether a file, a directory, or even another drive.

Copyright © 2010 Koroush Ghazi

If you wish to create a Directory Junction or Symbolic Link of your own, you can do so by opening an Administrator Command Prompt and then use the `MKLink` command. For example to create a link simply called *ReadMe* in your current directory, linking to the file *Text.doc* under C:*Users**User1**Documents*\, the following command can be used:

```
MKLink ReadMe C:\Users\User1\Documents\Text.doc
```

The link *ReadMe* will be created, denoted with a shortcut icon when viewed in Windows Explorer. If you want to see where this link points to, right-click on it, select Properties and under the Shortcut tab click the 'Open folder location' button. You can use either the `/J` or `/D` switches for the MKLink command to specify whether you wish to create a Directory Junction or Symbolic Directory Link (to link to a directory as opposed to the default Symbolic file link) respectively.

These features are not really designed for the average user, they are more for maintaining compatibility for older applications and games, and generally speaking you should not need to ever create or alter Directory Junctions or Symbolic Links. If however after upgrading from Windows XP to Vista you have problems with the default Vista junctions not redirecting properly, see this Microsoft Article.

< ADVANCED FEATURES

The following are some slightly more advanced features of Windows Explorer, including tips and tweaks for making Explorer easier to use.

MANIPULATE MULTIPLE FILES AT ONCE

If you have a range of files you want to manipulate together - e.g. move, copy, rename, change the properties of all of them - you can do so rapidly in Windows Explorer by doing the following:

Highlight the group of files you want to manipulate in one of three ways:

- Hold down the SHIFT key and click on the first file in the group, then while still holding down SHIFT, click on the last file in the group and everything in between will also be highlighted.
- Hold down the CTRL key and click on any individual files you want to select until all the files you want to select are highlighted.
- Under the Folder Options component of Windows Control Panel enable the 'Use check boxes to select items' option under the View tab, then select files using the check boxes which appear when you hover your mouse cursor over them, or all files in a column by ticking the check box at the top of the column.

You can also combine these methods, e.g. SHIFT select a large range of files, then use CTRL or the check box method to add or remove individual files to or from the already highlighted ones.

Without clicking anywhere else, you can now:

- Drag and drop these files to move them.
- Hold down CTRL while dragging and dropping to copy them.
- Hold down ALT while dragging and dropping to create shortcut links to them.
- Right-click on the first file you want to manipulate and select Rename, Copy, Delete, Properties or any other available options.

If you choose to rename the files, all the highlighted files will be renamed with the same name you gave the first file, however they will also be automatically assigned a number in brackets at the end of their filename. For example, if you rename the first in a series of highlighted photo files *SummerHoliday.jpg*, the remaining highlighted files will automatically be renamed *SummerHoliday (1).jpg*, *SummerHoliday (2).jpg,* and so on.

Copyright © 2010 Koroush Ghazi

DIRECTORY SHORTCUTS

If you want to open a Windows Explorer window at a particular folder quickly, there are two main ways to do this:

§ Go to Start>Run or Start>Search Box and type the path of the folder then press Enter. If you don't specify the full path, Windows Explorer will open up at the first incidence of that directory. E.g. enter only the word 'Downloads' in the Search Box and press Enter, and a Windows Explorer window will open at the *\User\[username]\Downloads* directory by default.
§ Right-click on an empty spot in Windows Explorer or your Desktop, select New>Shortcut, then enter the full directory path to the folder of your choice. When done this shortcut will now open Windows Explorer at the folder you specified whenever it is launched.

SET WINDOWS EXPLORER DEFAULT STARTUP FOLDER

If you usually open Windows Explorer from a shortcut, this procedure allows you to set which directory it will start in by default when launched from that shortcut:

1. Right-click on the shortcut icon you use to launch Windows Explorer and select Properties. Note that by default there is a shortcut for Windows Explorer under Start>All Programs>Accessories.
2. In the Target box replace the existing text with the following:

   ```
   %SystemRoot%\Explorer.exe /e, path
   ```

   In place of `path` above you should enter the actual path to the directory you want open by default. For example *C:\Users\User1\Pictures*. The path does not require quote marks around it. Make sure not to forget the comma and single blank space after the `/e` switch and before the `path`. E.g.:

   ```
   %SystemRoot%\Explorer.exe /e, C:\Users\User1\Pictures
   ```

3. Click OK, and now using this shortcut will always open a Windows Explorer window in the directory specified.

EXPANDED CONTEXT MENUS

A context menu is the small menu which pops up when you right-click on various Windows components, such as a file, folder or icon, whether in Explorer-based views or on your Desktop. If you want to view an 'expanded' context menu for a particular file or icon, hold down the SHIFT button while right-clicking on them. You'll see additional options such as 'Pin to Start Menu', 'Add to Quick Launch' and 'Copy as Path', or other options depending on the particular file or icon.

EDIT CONTEXT MENUS

When you right-click your mouse button on any location you will see a range of context menu entries. As the name implies, the entries are dependent on the context in which the right-click was used, whether it was on a file, folder, an empty location on the Desktop, and so forth. Unfortunately some of the entries in the context menu have been unnecessarily inserted by programs you have installed, and you may wish to remove these.

The first step in getting rid of any unwanted entries involves opening the programs to which the entries relate and looking through the program's options to see if you can unselect any 'shell integration' or 'context menu' settings they have. If that doesn't work or is not possible, you can use several other methods to find and remove these entries. Before making any changes to your context menus, make sure to use System Restore to create a new restore point, as some of these changes cannot be easily undone.

Copyright © 2010 Koroush Ghazi

Autoruns

The free Autoruns startup identification utility can be used in a relatively straightforward manner to temporarily disable or permanently remove context menu entries. For our purposes look under the Explorer tab of Autoruns - the majority of the entries will be context menu entries of one type or another. The Description, Publisher and Image Path columns should provide sufficient information to identify which Autorun entries relate to which particular context menu items. Untick any you wish to temporarily disable, then close Autoruns, reboot and check to see if the undesirable context menu entries are gone. To permanently remove an item, right-click on it and select Delete. For full details of how to use Autoruns, see the Startup Programs chapter.

ShellMenuView

The free ShellMenuView utility is an automated tool which displays all static context menu items. Download and run the *shmnview.exe* file to launch the utility - no installation is required. The interface is confusing at first, but keep in mind that most standard Windows entries are not being displayed as long as the 'Hide standard menu items' option is ticked under the Options menu, so the bulk of these entries relate to third party programs.

Each entry under the 'Menu Name' column is precisely that, the name of a menu entry in one of the context menus on your system. To determine which entries apply to which particular applications, expand the columns and look under the 'File Type' column - the associated applications for each menu entry are shown. Highlight the entries you believe you wish to remove, right-click and select 'Disable selected items', and check to see if this removes the relevant entries from your context menu. If not, you can easily undo this by highlighting the same entries, right-clicking and selecting 'Enable selected items'. Note also that if you can't disable an item properly, close the program, right-click on the *shmnview.exe* file and select 'Run as Administrator' to launch it again with full Administrator privileges.

ShellExView

Some context menu entries are not static, they enable additional functionality which makes them a shell extension. You can use the free ShellExView utility, which is similar to ShellMenuView, to view and adjust these. Download and run the *shexview.exe* file to launch the utility - no installation is required. The interface is once again slightly confusing at first, however non-Windows shell extensions are highlighted in pink by default, as long as the 'Mark non-Microsoft extensions' option is ticked under the Options menu. Right-click on any extension you wish to disable and select 'Disable selected items'. Test to see if this disables the item, however you will likely have to reboot to see the impact of the changes. Note also that if you can't disable an item properly, close the program, right-click on the *shexview.exe* file and select 'Run as Administrator' to launch it again with full Administrator privileges.

Windows Registry

The utilities above are recommended for most users as they are automated and provide safeguards to more easily undo changes. However if you wish to manually (and hence permanently) remove context menu entries via the Windows Registry, look under the following locations using the Registry Editor:

Copyright © 2010 Koroush Ghazi

```
[HKEY_CLASSES_ROOT\*\shellex\ContextMenuHandlers]
[HKEY_CLASSES_ROOT\AllFilesystemObjects\shellex\ContextMenuHandlers]
[HKEY_CLASSES_ROOT\Directory\shellex\ContextMenuHandlers]
[HKEY_CLASSES_ROOT\Directory\Background\shellex\ContextMenuHandlers]
[HKEY_CLASSES_ROOT\Drive\shell]
[HKEY_CLASSES_ROOT\Drive\shellex\ContextMenuHandlers]
[HKEY_CLASSES_ROOT\Folder\shell]
[HKEY_CLASSES_ROOT\Folder\shellex\ContextMenuHandlers]
```

The subfolders above are locations which hold most context menu entries in Windows. Under each, aside from standard Windows items such as `Sharing` or `Offline Files`, you may find keys or values which relate to particular third party programs. Right-clicking on the relevant program key and selecting Delete will remove its context menu entries. In most cases as you remove unwanted program entries, you can test the effects immediately by checking to see if the relevant entry was removed from the context menu. In some cases - mainly with shell extensions - you may need to reboot to see the effects. There is no undo function in Registry Editor, so make sure to back up the relevant branch before editing it. See the Windows Registry chapter for full details of registry editing.

ADD 'COPY TO' AND 'MOVE TO' CONTEXT MENU ITEMS

If you want to add two useful commands to your context menus - namely 'Copy To' and 'Move To', follow the steps below:

```
[HKEY_CLASSES_ROOT\AllFileSystemObjects\shellex\ContextMenuHandlers]

Copy To= {C2FBB630-2971-11d1-A18C-00C04FD75D13}
Move To= {C2FBB631-2971-11d1-A18C-00C04FD75D13}
```

To add one or both of these items to your context menu, create a new key under the `ContextMenuHandlers` folder - that is, right-click on the `ContextMenuHandlers` subfolder, select New>Key, and name it `Copy To` or `Move To` as desired. Then left-click once on this new key, go to the right pane in Registry Editor and double-click on the `(Default)` entry and assign the appropriate value data as shown above, including the parentheses around the numbers. This will create a new context menu entry that allows you to select either 'Copy To Folder...' or 'Move To Folder...' in the context menu for a particular file or folder and then specify the location to copy or move them to. Repeat these steps to create the other entry if you wish to have both on your context menu. To remove either of these entries simply delete the relevant subfolder in Registry Editor.

ADD 'OPEN WITH NOTEPAD' CONTEXT MENU ITEM

If you want to quickly open any file using Notepad, you can add a new 'Open with Notepad' context menu item by going to the following location in the Registry:

```
[HKEY_CLASSES_ROOT\*\shell\]
```

Right-click on the subfolder above, select New>Key and call it `Open with Notepad.` Then right-click on this new key, select New>Key again to create a new key under it called `command,` with the final result looking like this:

```
[HKEY_CLASSES_ROOT\*\shell\Open with Notepad\command]
```

Select the `command` subfolder and in the right pane, double-click on the `(Default)` entry and enter the following value data exactly as shown:

```
notepad.exe %1
```

Copyright © 2010 Koroush Ghazi

Now whenever you right-click on any file it will have a new context menu entry called 'Open with Notepad', which when selected opens that file instantly in Notepad. To remove this context menu entry simply delete the `Open with Notepad` subfolder.

Edit 'Open With' Context Menu

Whenever you open a file with a particular program, it will usually be added to the 'Open With' context menu for that file type. To edit the programs which are included in this list for a particular file extension, first go to the following location in your Registry:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts]
```

Here you can select the relevant file extension from the list of keys shown. For example to edit the *.AVI* file extension (for videos), go to the `.avi` key. Then select the `OpenWithList` key under it, and in the right pane you will see a list of STRING entries such as the ones below:

```
a=wmplayer.exe
b=VirtualDub.exe
```

Each value corresponds with a particular program which is shown as an entry in the 'Open With' context menu for that particular file extension. Right-click on values for the program(s) you wish to remove and select Delete, and they will be immediately removed from the relevant 'Open With' context menu.

Edit 'Send To' Context Menu

When you right-click on most files or icons, you will see a 'Send To' context menu item, which has further options to select. Typically you will see options like sending the file to the desktop (as an icon), or sending the file to a compressed folder, etc. You can edit the options which appear in the 'Send To' context menu by going to the following folder:

\Users\[username]\AppData\Roaming\Microsoft\Windows\SendTo

To remove any item from the 'Send To' context menu, simply delete it from this folder, or preferably move it to another folder to keep as a backup. To add a new 'Send To' item, such as a new folder or program, simply copy its shortcut into this folder.

Fix Incorrect Folder Views

If your folder views in Explorer-based interfaces are constantly being shown incorrectly, or being reset by Vista, even after you have followed the instructions earlier in this chapter to set individual folder view types, then follow these instructions to fix this issue permanently. First go to the following registry keys:

```
[HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\
Windows\Shell\Bags]

[HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\
Windows\Shell\BagMRU]
```

Right-click on the `Bags` key in the left pane and select Delete, then do the same thing for `BagMRU`. This will remove most existing customizations for things like window sizes, positions and views. While still in the same place in the Registry Editor, you will need to manually recreate one of these keys with a new setting. Right-click on the following key in the left pane:

```
[HKEY_CURRENT_USER\Software\Classes\Local
Settings\Software\Microsoft\Windows\Shell]
```

Copyright © 2010 Koroush Ghazi

Create a new key called `Bags` to replace the one you just deleted. Right-click on `Bags`, select New>Key and name this new key `AllFolders`. Right-click on `AllFolders`, select New>Key and name this new key `Shell`. The end result should look like this in Registry Editor:

```
[HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\
Windows\Shell\Bags\AllFolders\Shell]
```

Now left-click on the last `Shell` key and in the right pane right-click in an empty area and select New>String Value. Name this new string `FolderType` and once created, double-click on it and in the Value Data box you can set the default view which all folders will initially take (unless otherwise specified) by entering one of the following values:

- NotSpecified
- Contacts
- Documents
- Music
- Pictures

For example if you enter Documents in the `FolderType` Value Data box (which I recommend), then all folders for which you do not manually set a view will default to the standard Documents folder view as you set it.

Now in Windows Explorer go to your *\Users\[username]* directory and for each of the main folder types under there (Documents, Pictures, Music, Videos), make sure that you set the view you wish, including things like choosing which columns to show and how wide they each are, the size of any icons/thumbnails, the way in which they are sorted, etc. As you make the changes, for each folder click the Organize button at the top of Windows Explorer, select 'Folder and Search Options', go to the View tab and click the 'Apply to Folders' button. This will set this view for all folders of that same type, and this method also means that should you copy files of any other type into a folder, it will not alter that folder's view settings - from now on the settings should remain exactly as you leave them.

There is one last step which can help ensure these settings remain fixed. Go to the following key:

```
[HKEY_CURRENT_USER\Software\Classes\Local
Settings\Software\Microsoft\Windows\Shell]
```

Left-click on the `Shell` key and in the right pane, if you can see `BagMRU Size` then there is no need to undertake this step. If it isn't there however, right-click and select New>DWORD 32-bit Value and name it `BagMRU Size`. Now set this value to 10000 in Decimal view (or 2710 in Hexadecimal view).

The above steps should ensure that your folder views don't change again without you changing them manually. However if you still find your folder views resetting or changing every once in a while even after following the steps above, it indicates that you may have data corruption issues (e.g. faulty or overclocked RAM or CPU), or a particular program you have installed is constantly interfering with Explorer-based views in the Windows interface.

Copyright © 2010 Koroush Ghazi

SHOW SUPER HIDDEN FILES

If you've selected 'Show hidden files and folders' and unticked 'Hide protected operating system files' in Folder Options as covered further above, you will see most every hidden file and folder on your system. However there are a class of 'super hidden' system files which still won't show up, and to see them you will need to change the following setting:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]

SuperHidden=1
```

Setting the DWORD above to =1 will allow you to view all hidden files after you reboot. Obviously it is not recommended that you alter these files unless there is a specific need; they're hidden for a reason, and you generally don't need to see them unless troubleshooting a system problem.

EXPLORER RESTART SUBSTITUTE FOR REBOOT

There is a method of doing a reboot of the Explorer process as a substitute for having to do a full restart of Windows under certain circumstances. This is done as follows:

1. Open Task Manager - see the Performance Measurement & Diagnostics chapter
2. Under the Processes tab right-click on the *Explorer.exe* process and select 'End Process'. Confirm the End Process prompt which comes up. The Taskbar and parts of the screen will go blank.
3. Still in Task Manager, go to the File menu and select 'New Task (Run)'.
4. Type *explorer* in the box which opens and press Enter. Explorer will be reloaded and the interface should return to normal.

This method can help resolve problems with the Vista interface showing glitches or being unresponsive, or if a particular file or program is not responding. Furthermore if you've implemented a registry change then restarting Explorer will often implement the change without having to reboot. This method does not replace the need to reboot in most other circumstances such as during the installation of drivers, or after serious errors.

< KEYBOARD SHORTCUTS

Most people know that you can use the keyboard to speed up access to common commands and functions in Windows. A list of them can be found in this Microsoft Article, a range of these are already mentioned throughout this book, however on the next page is a consolidated table of all the major common keyboard shortcuts you can use to quickly access useful functions in Vista:

Copyright © 2010 Koroush Ghazi

Keyboard Combination	Function
CTRL + C	Copy selected item(s)
CTRL + X	Cut selected item(s)
CTRL + V	Paste copied/cut item(s)
CTRL + Z	Undo last action
CTRL + Y	Redo last action
CTRL+ +	Force all columns to be shown in Explorer interfaces
SHIFT + DEL	Delete highlighted item, bypassing Recycle Bin
WINDOWS	Open Start Menu
WINDOWS + D	Minimize/Restore all Windows
WINDOWS + E	Open Windows Explorer
WINDOWS + F	Open Windows Search
WINDOWS + L	Lock Workstation
WINDOWS + R	Open Start>Run box
WINDOWS + F1	Open Help & Support
WINDOWS + Number	Open Quick Bar item - number corresponds to order of item on Quick Bar
WINDOWS + TAB	Switches between active programs in 3D Flip mode. CTRL + WINDOWS + TAB opens 3D Flip permanently, TAB or arrow keys to cycle elements, ESC to exit
ALT + TAB	Switch between active programs in 2D Task Switcher. CTRL + ALT + TAB opens Task Switcher permanently, TAB or arrow keys to cycle elements, ESC to exit
CTRL + SHIFT + ESC	Open Task Manager
ALT + F4	Close highlighted program Show PC Shutdown options if Desktop or Taskbar highlighted
SHIFT + LEFT CLICK	Select multiple items within a range
CTRL + LEFT CLICK	Select multiple non-sequential items individually
TAB	Step forward through screen elements
SHIFT + TAB	Step backward through screen elements
F2	Rename/Enter text for item
F5	Update/Refresh active window
SHIFT + F10	Open Context Menu for highlighted item

KEYBOARD AND MOUSE SUBSTITUTES

If you're having problems using your keyboard or mouse, either because one or the other is broken, or you are differently abled, there are two substitute methods you can use in Windows:

Microsoft Onscreen Keyboard: This utility can be accessed by going to Control Panel>Ease of Access Center and selecting it, or go to Start>Search Box, type *osk* then press Enter. A virtual keyboard will be displayed, allowing you to use your mouse to click on virtual keys as though you were using a keyboard. To make things easier, position it somewhere convenient and then select 'Always on Top' under the Settings menu so you don't constantly have to switch back and forward between tasks to use it. If you can't click the left mouse button to select keys, or just want a quicker way of selecting keys, under the Settings menu select 'Typing Mode' and then 'Hover to Select', then set the length of time needed to hover over a key before it registers as an entry (values in seconds between 0.00 and 1.00 second). Now you can rapidly move your mouse cursor over keys on the Onscreen Keyboard and it will register as a keystroke.

Mouse Keys: If instead of your keyboard you're having problems using the mouse, you can enable the Windows MouseKeys functionality by going to Control Panel>Ease of Access and select 'Make the mouse easier to use' and then tick the 'Turn on Mouse Keys' option. MouseKeys allows you to use the Numpad keys - the numerical keys on the far right of your keyboard - to move the mouse cursor around on screen. You can configure these keys further by clicking the 'Set up Mouse Keys'.

Copyright © 2010 Koroush Ghazi

WINDOWS DRIVERS

Device drivers are the software that is necessary to give instructions to your hardware. Graphics drivers for example tell your graphics hardware what to do in various situations, such as during 3D games or when displaying the Windows Desktop. Windows Vista comes with built-in driver support for virtually any type of common computer hardware, and hence most of your hardware will operate in Windows even without installing additional drivers. However the built-in Windows drivers are not optimal and do not guarantee that you will get full efficient functionality out of your hardware. Thus wherever possible you need to download, install and configure the latest available Vista-specific device drivers for your hardware to make sure your entire system performs optimally, with full functionality and maximum stability.

Windows Vista is based on the new Windows Driver Model which attempts to make the creation, installation and usage of device drivers much simpler, more secure and less likely to cause critical system-wide instability. This is because much of the driver is now not involved with the Kernel - the core software of Vista - and thus if a device or driver malfunctions then usually the system state can be restored by restarting the driver rather than rebooting the entire system. This model also allows better sharing of resources, making it easier to genuinely multitask without running into serious problems. However the new driver model also requires drivers specifically written for Vista, and in turn Vista 32-bit and Vista 64-bit have different driver requirements. This chapter runs through these issues and details how to install, view, uninstall and troubleshoot device drivers in Windows.

< SIGNED VS. UNSIGNED DRIVERS

When a device driver is installed, it effectively becomes a part of the operating system and has unrestricted access to much of the computer. This means it's important to only install drivers you are familiar with and which are from a reputable source, such as directly from the company which manufactured the hardware for which the driver is intended. To ensure that the drivers you are installing are legitimate and have not been tampered with to include malware for example, Windows Vista prefers the installation of Signed Drivers. A signed driver has a digital signature which indicates who created the driver and whether its contents have been altered in any way after the drivers were packaged. The treatment of unsigned drivers is different under Vista 64-bit as compared to Vista 32-bit:

VISTA 32-BIT

In Vista 32-bit you can still install unsigned drivers but you must have Administrator access and you will be warned first:

§ *Windows can't verify the publisher of this driver software:* This means the driver is unsigned or the signature cannot be verified. You should only install such drivers if you have obtained them from a trusted source. In most cases this should be direct from the hardware manufacturer's site. If you are not completely sure of the trustworthiness of the source, do further research before installing the driver.

§ *This driver software has been altered:* This means the driver has been altered after being signed. It could be a 'modded' driver, in which case if you are aware of the risks and are downloading it from a site you trust, you can proceed. If you downloaded it from an untrusted or unfamiliar source, such as peer to peer or a file sharing site, then do not install the driver as there's a reasonable chance it could contain malware or be problematic. If you downloaded it from a hardware manufacturer, it is best to do further research and seek user feedback before installing this driver.

Copyright © 2010 Koroush Ghazi

VISTA 64-BIT

In Vista 64-bit if you see either of the warnings above you will not be allowed to install the driver. This is because it contains a feature called PatchGuard which is designed to protect the system Kernel even further - see the PC Security chapter for details. This is the reason why Vista 64-bit is not recommended for users with old hardware, because some manufacturers may not be able to afford to release updated signed drivers for such hardware on a consistent basis, and obviously this could then be problematic.

However there is a way around this limitation of Vista 64-bit if you absolutely must install an unsigned driver. It is detailed in this Microsoft Article and involves restarting your PC and during bootup continually pressing the F8 key. You will come to the Advanced Boot Options screen and can select the 'Disable Driver Signature Enforcement' option to prevent signature checks throughout the current session. You will need to do this at every restart though, otherwise the unsigned driver(s) will not load up. Various other workarounds and utilities have been released to allow the loading of unsigned drivers in Vista 64-bit, however Microsoft has consistently patched Vista to disable or prevent these methods because they are seen as security holes.

SIGNATURE VERIFICATION

If your system is suffering from problems and general instability, it might be a good idea to check to see precisely how many unsigned drivers you have on your system, and perhaps uninstall the ones which are least trustworthy for troubleshooting purposes. The File Signature Verification utility in Vista is a simple tool for quickly checking the status of drivers. Go to Start>Search Box, type *sigverif* and press Enter. In the dialog box which opens, click the Start button and it will scan your system and display all the currently installed unsigned drivers. You can click the Advanced button in the utility and also tell it to save the results as a log file, as well as being able to view the current log file.

Some hardware manufacturers have released unsigned drivers which are perfectly safe and functional, but you should still try to minimize the number of unsigned drivers on your system. Installing unsigned drivers in either version of Vista is not recommended unless you are certain of the trustworthiness and reputation of the source of the drivers. This usually means they should be direct from the hardware manufacturer's website. By installing unsigned drivers you are defeating a major security feature of Vista, and potentially allowing malicious or problematic software direct access to your machine. It's a question of system security, not just system stability, so it is not to be taken lightly.

< DRIVER INSTALLATION

All of your major hardware devices require the latest available Vista-compatible drivers and related updates to function correctly, and indeed many problems in recent applications and games often result from a lack of the latest drivers. It is important therefore to check for and install all the relevant drivers as soon as possible after installing Vista.

Note that during the installation of a driver, if you are prompted to reboot at any time, you must do so to allow proper driver installation. Even though Vista has a new Restart Manager which is designed to automatically attempt to close down all non-critical processes and hence allow them to be updated without a full system reboot, many major device drivers still typically need a reboot in order to continue. Hence it is recommended that you reboot as often as required and not do anything else on your system while installing a driver.

The specific updates and drivers you should install, and their preferred order, is provided below in a series of steps you should follow:

Copyright © 2010 Koroush Ghazi

Step 1 - Service Packs

A Service Pack is a compilation of important security, stability and performance updates for Windows. The latest service pack for Windows Vista is Service Pack 2 (SP2). However if you did not use a Vista install DVD which incorporates SP1, then first install the full standalone version of Service Pack 1 (SP1) for Windows Vista - either Vista SP1 32-bit or Vista SP1 64-bit as relevant. You can see a full list of the individual updates contained in SP1 in this Microsoft Article. If your Vista installation DVD is clearly marked to indicate that it already has SP1 incorporated into it, then you will not need to manually install SP1 - skip this step.

Next, install Vista SP2 - either Vista SP2 32-bit or Vista SP2 64-bit as relevant. The list of changes in SP2 are provided in this Microsoft Article. Note that SP2 requires that Vista SP1 be installed first. Once again, if you are using a Vista installation disc which already incorporates SP2, then you can skip this step. If you experience an error during the installation of SP2 and you have used the vLite utility to modify your current installation of Vista, see the vLite section under the Windows Installation chapter for more details.

Note that although you can download and install both SP1 and SP2 through Windows Update, I recommend downloading and manually installing the full standalone versions of each of the required service packs as linked above because this method is the least likely to cause problems, and also ensures that you install the service pack(s) first and foremost before any other updates or drivers can be installed automatically by Windows.

Once you have installed SP2, keep in mind that you can remove the unnecessary backup files and the redundant previous versions of system files left over from the service pack process by using the appropriate Service Pack Cleanup Utility - see the Cleaning Windows chapter for details. Furthermore, if you have SuperFetch enabled, you should allow Vista at least a week after the installation of SP2 to get back to full speed. Finally, since a service pack patches or replaces a wide range of system files, it is strongly recommended that you make sure to run a disk defragmenter at some point after installing a service pack.

Step 2 - DirectX

Install the latest version of Microsoft DirectX. As covered under the Graphics & Interface chapter, DirectX is an important component of Windows which allows advanced multimedia functionality. Windows Vista already comes with both DirectX 10 and DirectX 9EX installed, however from time to time Microsoft releases updates for DirectX, and the latest of these should always be installed to ensure the best performance and stability.

You can also enable DirectX 11 capability on Windows Vista by installing the Platform Update. The relevant components of the update are available for download in 32-bit or 64-bit versions. For more details of DirectX see the Graphics & Interface chapter.

Step 3 - Windows Update (Important Updates)

It is imperative for security purposes that you run Windows Update to check for and install all important updates to the core Vista software. To do this, go to Control Panel>Windows Update, click 'Change Settings' in the left pane and I recommend selecting 'Check for updates but let me choose whether to download and install them'. To begin with I recommend unticking the 'Include recommended updates' option so as to prevent Vista from installing any updated generic Windows device drivers for your hardware components - we will revisit this option again in Step 8 below.

Click OK to close the settings and then click the 'Check for updates' link in the left pane and allow Vista to search for all the relevant updates online. Once done, you will see precisely how many updates there are and the total combined size of these updates. You should then click the 'Install Updates' button and allow Vista to download and install them all. See the Windows Update section of the Control Panel chapter for more details of the Windows Update functionality and how best to configure it and use it in the future.

Copyright © 2010 Koroush Ghazi

STEP 4 - MOTHERBOARD DRIVERS

Install your motherboard drivers. The motherboard is the hardware foundation of your entire system, so using the latest drivers for it is important in achieving optimal, trouble-free performance for your entire system, as well as providing additional motherboard-specific functionality such as onboard audio, onboard network adapter, RAID, and so forth.

Finding all the correct motherboard drivers is not necessarily a straightforward task. To start with, it's important to understand that the motherboard chipset type is not the same as the motherboard brand or model number. The chipset type is based on the company that manufactures the actual chipset architecture used in the motherboard. The motherboard's brand is based on the company that buys this chipset, packages it with certain features and sells it under its own brand name with a specific model number. For example, an *ASUS P6T Deluxe* motherboard is manufactured by a company called ASUS, it uses an Intel X58 Express chipset and it has the specific model name P6T Deluxe. All of these details are important when determining the correct driver to use. A combination of the utilities covered in the System Specifications chapter, along with your motherboard manual and Google will give you all of these details about your motherboard.

Your motherboard usually comes with a driver disc which contains the relevant drivers, however these are usually well out of date. The first place you should look for the latest version of these drivers is on your motherboard manufacturer's website - there are too many to list here, so check your motherboard manual for a link. Once at the site, under the Support or Downloads section you will usually find several different types of updates for your particular motherboard model. These are broken down by category below:

BIOS - These are not drivers, they are BIOS updates for which you should refer to the BIOS & Hardware Management chapter for more details.
Chipset - These are the core drivers which control your motherboard's key functionality. All systems require these for optimal performance and functionality.
IDE, SATA, RAID - These drivers are required for correct operation of your motherboard's drive controllers. You may also require these drivers for correct detection of your drives during the installation of Windows - see the Windows Installation chapter.
Video - If you are using your motherboard's onboard or integrated graphics capabilities, then these drivers are necessary. If you are using a separate graphics card, these are not necessary. Refer to Step 5 below.
Audio - If you are using your motherboard's onboard or integrated audio capabilities, then these drivers are necessary. If you are using a separate sound card, these are not necessary. Refer to Step 6 below.
USB - If you are using the USB ports on your motherboard, you may require separate USB drivers for correct functionality, although typically this feature is already incorporated into the Chipset driver.
LAN - If you are using your motherboard's onboard network/Ethernet controller, whether for an Internet connection or a connection to a network of computers, then these drivers are necessary.

There may be additional drivers for other specific functionality on your motherboard, but the ones above are the most important, particularly the Chipset and IDE/SATA/RAID drivers.

If you're not using a particular function on your motherboard, I strongly recommend disabling it in your BIOS as detailed in the BIOS & Hardware Management chapter. This will prevent Windows from automatically detecting them and installing drivers for them, and in turn this can reduce resource usage and speed up Windows startup.

If there are no appropriate drivers on your motherboard manufacturer's site, or they appear to be fairly old, you can download the latest drivers directly from one of the major chipset manufacturers:

Copyright © 2010 Koroush Ghazi

§ For **Intel** motherboards, download and install the latest Intel Chipset Software.
If you also have a RAID or AHCI setup install the Intel Rapid Storage Technology Driver.
§ For **Nvidia** motherboards, download and install the latest nForce Drivers.
§ For **VIA** motherboards, download and install the latest VIA Hyperion Drivers.
§ For **SiS** motherboards, download and install the latest SiS Chipset Software.

Note that some of these drivers may contain a mix of driver components, including chipset, SATA/RAID and LAN drivers all in one package. Read the driver notes on the site for more details.

STEP 5 - GRAPHICS DRIVERS

Install your graphics card video drivers. Just as with motherboards, graphics chipsets are developed by one company and then sold to different manufacturers who then package them together with certain features and capabilities and market them under their own brand name. The important thing to know is the manufacturer of the chipset on which your graphics card is based - for most graphics cards this will be either Nvidia or ATI. For example, an *EVGA GeForce GTX 285* graphics card uses an Nvidia GeForce 200 series chipset, packaged and sold by the company EVGA under its own brand. The chipset is the determinant of which driver to use, not the company selling the card. Determine your chipset and model name using the utilities in the System Specifications chapter, then download and install the relevant package:

§ For **Nvidia** graphics cards, download and install the latest Forceware Graphics Drivers.
For details on how to install and set these up correctly read the Nvidia Forceware Tweak Guide.
§ For **ATI** graphics cards, download and install the latest ATI Catalyst Drivers.
For details on how to install and set these up correctly read the ATI Catalyst Tweak Guide.
§ For **Intel** graphics cards, download and install the latest Intel Graphics Drivers.
§ For **SiS** graphics cards, download and install the latest SiS Graphics Drivers.
§ For **S3** graphics cards, download and install the latest S3 Graphics Drivers.
§ For **Matrox** graphics cards, download and install the latest Matrox Graphics Drivers.
§ For motherboards with onboard graphics, check your motherboard manufacturer's website first (See Step 4), then check one of the sites above for Integrated or Onboard Graphics drivers.

Note that unlike motherboards, you do not need to download your graphics drivers from your hardware manufacturer's website. Installing the latest 'reference' chipset drivers shown above is the best method as they are typically much newer.

STEP 6 - SOUND DRIVERS

Install your Sound card audio drivers. These vary depending on the brand of the sound card you are running. Only the major brands are covered below:

§ For **Creative** sound cards, download and install the latest Creative Audio Drivers.
§ For **ASUS** sound cards, download and install the latest ASUS Audio Drivers.
§ For **Auzentech** sound cards, download and install the latest Auzentech Drivers.
§ For **Turtle Beach** sound cards, download and install the latest Turtle Beach Audio Drivers.
§ For **Hercules** sound cards, download and install the latest Hercules Audio Drivers.
§ For **AOpen** sound cards, download and install the latest AOpen Audio Drivers.
§ For motherboards with onboard audio, check your motherboard manufacturer's website first (See Step 4), then check your onboard audio chipset manufacturer's website such as Realtek.

Importantly under Windows Vista there have been major changes in the way sound is handled compared to Windows XP - see the Sound section under the Control Panel chapter for full details. The result is that sound cards no longer have as much importance or control over the sound functionality in Windows. There are many benefits to this sound management method, but one problem it causes is that in old games which use

Copyright © 2010 Koroush Ghazi

the DirectSound/DirectSound3D API, your sound card's hardware capabilities for enhanced audio effects (such as EAX) will not be used. Games which use OpenAL are not affected. If you have a game which has an option to use OpenAL mode, I recommend selecting it if you want extra sound features offered by your sound card. If you own a Creative Audigy or X-Fi sound card, there is another solution for running older games which involves using the Creative ALchemy Patch as a workaround. If you have Realtek onboard sound, you can use the Realtek SoundBack utility as a workaround.

If after updating to the latest audio drivers you find you are having strange performance issues in games, or audio problems such as crackling, distortion or disconnected sound, then I recommend that pending newer drivers for your sound card, you consider disabling or physically removing the card and reverting to the onboard sound functionality which most recent motherboards have. Onboard audio is designed for software-driven sound which is what Vista and Windows 7 now use, and hence it is likely to have few problems and probably offer the same audio quality under Vista. The performance difference should not be significant. Again, refer to the Sound section of the Control Panel chapter for more details.

STEP 7 - PERIPHERAL DRIVERS

Before installing any peripheral drivers, connect these devices (e.g. Mouse, Printer, Digital Camera) to your system and test their functionality. If they appear to work fine and all the major functions which you would use are intact, then do not install a new driver for them. For example, if you connect an optical mouse and it appears to have sufficient functionality, do not then install the drivers that come on the disc with the mouse, or download and install new drivers from the manufacturer's website. The reason for this is that such drivers typically need to load into the background at Windows startup and usually add to overall resource usage, increase boot times, and quite often don't add anything of real value to the device's function. Vista should already support the important basic functionality of your major peripherals without the need for additional drivers.

However obviously should your device not function correctly, or a feature that you need to use appears disabled, you will then need to install the latest Vista-compatible driver for that device. In that case I recommend you go to the device manufacturer's website and download the latest available drivers rather than using the older drivers that come on the disk with the device. There are far too many device manufacturers to list here, but the website address is usually prominently listed on the device's box and/or in the manual. Where possible follow the device installation instructions in the device's manual (or on its website) for the best method of installation. Typically this involves connecting the devices to your machine one by one, and when Windows Vista detects them and prompts for drivers, insert the appropriate driver disk or point Windows to the directory where you have downloaded the latest driver files for the device and continue from there.

If you have an older device which is not compatible with Plug and Play, or your device isn't being detected correctly, see the Add Hardware section under the Control Panel chapter for more details of how to manually install such a device under Vista.

STEP 8 - WINDOWS UPDATE (DRIVER UPDATES)

Now that you've installed all the latest Vista-compatible drivers for your hardware, you should run Windows Update again to see if any newer drivers can be found for your devices. Go to Control Panel>Windows Update, click 'Change Settings' in the left pane, and make sure the 'Include recommended updates when downloading, installing or notifying me of updates' option is ticked. Click OK and then click the 'Check for updates' link in the left pane and allow Vista to search for any newer drivers. If any are found, these drivers should be completely safe to install as they've been tested by MS before being included in Windows Update, and they will only be detected and shown if they are appropriate for your hardware and newer than the driver versions you are currently using.

Copyright © 2010 Koroush Ghazi

Once you've completed all the steps above, your Vista will be up to date and your major devices should all have appropriate drivers to allow full and optimal functionality. If there are any devices which are not being detected correctly, or which have impaired functionality, then you may have to wait for updated drivers to be released by your hardware manufacturer. Although Vista now has greatly improved driver support, some hardware manufacturers may neglect older or lower-end hardware, or have yet to fix specific bugs in their drivers, and only newer versions of drivers can resolve these issues.

< VIEWING, UPDATING OR UNINSTALLING DRIVERS

To view the current version of a driver for a particular hardware component, or to update or uninstall a driver, you can use Device Manager. To access Device Manager, go to Control Panel>Device Manager or go to Start>Search Box, type *device manager* and press Enter. Note that the general hardware functionality of Device Manager is already covered under the BIOS & Hardware Management chapter.

VIEWING DRIVER DETAILS

To view the current version of the drivers installed for particular hardware component in detail follow the steps below:

1. Open Device Manager and expand the category under which your particular hardware device is placed. For example to view your monitor drivers, expand the Monitor category and your monitor(s) will be listed underneath.
2. Double-click on the device or right-click on it and select Properties.
3. Under the Driver tab you will see the specific driver version, date and provider. If the device is using a default Windows driver the Driver Provider will usually be listed as Microsoft.
4. Click the 'Driver Details' button and you will see the specific driver files associated with that device. You can then click on each individual file shown, and the provider and version of that file will also be displayed just below it.

For a more user-friendly display of driver detail for your major components, use the tools under the System Specifications chapter.

MANUALLY UPDATING DRIVERS

Normally, when you wish to update a device driver, the best course of action is to download the new driver package and run it. It should automatically execute and walk you through the steps necessary to update the device. However in some cases you may need to manually update a driver - for example if a driver does not come in an executable (.EXE) package, but rather as a set of files, perhaps within a .ZIP or .RAR archive. Follow the steps below to manually search for and update a device driver:

1. Open Device Manager and expand the category under which your particular hardware device is placed, then double-click on the device or right-click on it and select Properties.
2. Under the Driver tab click the 'Update Driver' button.
3. You will have two options; you can either allow Vista to 'Search automatically for updated driver software', or if you know where the driver files are stored click the 'Browse my computer for driver software' option. The first option is recommended only if you do not already have the new driver files, or if you are a novice user - if you choose this option see Steps 4 - 5 below. If you have the relevant driver files, or if you feel you are more advanced, choose the second option and go directly to Step 6.
4. You may be presented with three options: 'Yes, always search online'; 'Yes, search online this time only'; and 'Don't search online'. If you have the new driver files already on your system I recommend clicking the 'Don't search online' option as this should detect and install the local version. If you don't know whether newer drivers are available and/or you don't have them downloaded on your system, then I

Copyright © 2010 Koroush Ghazi

suggest the second option, that is to allow Vista to search online, but not to make this the default behavior.

5. Once Vista has searched it will either ask you to install newly found drivers, or tell you that your current version is the latest. Proceed as appropriate. If you know there are newer drivers on your system and they're not being detected, go back to Step 3 and select 'Browse my computer for driver software' then follow Step 6 onwards.
6. Depending on where the newer driver files are held, insert the appropriate disc and/or browse to that directory/drive - make sure the 'Include subfolders' option is ticked. Click Next and Vista should detect and ask you to install the newer driver version.
7. If the above steps fail and you are certain you have newer driver files for the device, then follow Steps 1 - 3, selecting 'Browse my computer for driver software', then select 'Let me pick from a list of device drivers on my computer'.
8. Click the 'Have disk' button and insert or browse to the place where the newer drivers reside. If an appropriate .INF file is found, click on it and click Open. If your hardware is supported by that driver file you can select the specific driver to install.
9. If nothing else works and you wish to install another driver for a device similar to yours, then follow Steps 1 - 3 above, then Step 7. Then untick the 'Show compatible hardware' box and you will see a much wider range of drivers. Select one which you believe would be most compatible with your device, though clearly if you select a driver not meant for your specific device, you may not be allowed to install it, or it may result in a lack of correct functionality or major problems. This is only a last resort option.

Rolling Back to an Earlier Version of Drivers

If you have recently installed a driver set which you believe is causing you problems, then you may wish to go back to the previous drivers you were using. To do this follow these steps:

1. Open Device Manager and expand the category under which your particular hardware device is placed, then double-click on the device or right-click on it and select Properties.
2. Under the Driver tab click the 'Roll Back Driver' button. If it is not available then you do not have any earlier driver versions installed, or they may not be detected - see the manual instructions further below.
3. Confirm whether you want to do this, and your current drivers will be replaced with the previously installed version.

The above is the quickest way to go back to a previously installed version, however it may not resolve your problems, or you may wish to go back to a specific driver version, in which case you will have to do things manually. To manually go back to an earlier driver version which was installed on your system, or if you wish to revert to the standard Windows driver for a device for some reason (e.g. to troubleshoot a driver-related issue), then follow these steps:

1. Open Device Manager and expand the category under which your particular hardware device is placed, then double-click on the device or right-click on it and select Properties.
2. Under the Driver tab click the 'Update Driver' button.
3. Click the 'Browse my computer for driver software' option.
4. Select 'Let me pick from a list of device drivers on my computer'.
5. Make sure the 'Show compatible hardware' box is ticked, and you will see all the previous versions of compatible drivers which are available on your system for this device, along with their version number and date where applicable. Select the earlier version you want and click Next to install it. Note that the latest version of the drivers may have no date or version number.
6. Alternatively, if you wish to go back to the default Windows driver for this device, select the driver with the word Standard or Microsoft in it and click Next.
7. If instead of the options above you want to choose the most basic driver for that class of device, you should look for a driver starting with the name Generic. You may have to untick the 'Show compatible

Copyright © 2010 Koroush Ghazi

hardware' box to see it. This provides very limited functionality and should only be used for troubleshooting or if no other driver works on your system.

If you're having continual problems and suspect a driver is the cause then I recommend cleaning out your drivers and installing only the latest version or the version which you know works best on your system.

UNINSTALLING DRIVERS

In general it is recommended that you do not maintain multiple versions of the same driver on your system, as these leave various bits and pieces - known as driver residue - on your system. This increases the potential for driver-related problems, especially if you ever go backwards in driver version, since components of driver files with varying versions may inadvertently be used together by Vista and this can cause problems.

To correctly uninstall a driver through Windows you should go to Control Panel>Programs and Features and on the main screen you should see most if not all the programs, updates and drivers currently installed on your system. Look for the driver manufacturer or relevant device name in the list, and if found highlight the item (or right-click on it) and select Uninstall, thus removing it.

However if a driver is not listed in the Programs and Features list there is another way you can uninstall it:

1. Open Device Manager and expand the category under which your particular hardware device is placed, then double-click on the device or right-click on it and select Properties.
2. Under the Driver tab click the Uninstall button.
3. Make sure to tick the 'Delete the driver software for this device' check box. If this option is not available, it means you are already using the default Windows driver for the device, in which case you should not continue attempting to uninstall the device unless you want the default driver to reinstall for some reason.
4. Click OK and the device will be uninstalled from your system, and its currently-used driver will be removed from your system as well. Restart your PC as prompted to complete the process. Importantly, uninstalling certain devices such as your graphics card or monitor may cause your system display to go black. In this case simply wait a few moments, then press the power or restart button on your PC to tell Vista to shut down and/or restart the PC.
5. Once your system restarts, your device will be redetected by Vista and the next available drivers will be installed for it automatically, or you will be prompted to provide new drivers.

Driver Sweeper

If after using the above methods you feel there is still some driver residue left on your system, you can use the free Driver Sweeper utility to attempt to remove any remaining traces of the more common drivers. Follow these steps:

1. Launch Driver Sweeper and make sure it has Administrator privileges.
2. Tick the driver(s) you wish to remove from the list provided, and click the Analyze button first to see what will be removed. You can manually untick any components you wish to keep.
3. If you wish to continue, click the Clean button and reboot your PC to make sure all driver files and related Registry entries are removed.
4. If you find certain driver elements are still not being removed, reboot into Safe Mode and follow Steps 1 - 3 above again. Under Safe Mode no third party drivers are in use by Windows, so none of them should be locked against deletion as long as you have Administrator access to the system. See the Backup & Recovery chapter for details of using Safe Mode.

Driver Sweeper only allows the removal of the specific drivers in the list it provides. Furthermore newer versions of these drivers may install additional files and registry entries which an existing version of Driver

Copyright © 2010 Koroush Ghazi

Sweeper cannot find, so check for updates to Driver Sweeper and remember that no automated method is foolproof in finding all aspects of driver residue, since drivers are constantly changing.

Autoruns

You can use the free Autoruns utility covered under the Startup Programs chapter to identify, disable or permanently remove any driver files which are loading up with Windows. Follow these steps:

1. Uninstall any programs or drivers you do not wish to use as normal, then reboot your system when finished.
2. Launch Autoruns and go to the Drivers tab. Under the Options menu, untick 'Hide Microsoft and Windows Entries' and 'Hide Windows Entries', but make sure the 'Verify Code Signatures' item is ticked. Press F5 or select Refresh under the File menu.
3. In the list which appears, most of the entries are Microsoft drivers for Windows and should not be unticked or deleted. However under the Publisher column you should check every entry for which the provider is not 'Microsoft Corporation', as most of these are third party drivers installed on your system - though note that some are still generic Windows drivers provided by other companies. Check the Description column to see which application or device the driver relates to. Highlight the file and look at the details pane at the bottom of Autoruns to see the date and version number for the driver file.
4. For any drivers you wish to remove, first untick entry in Autoruns, and when finished close Autoruns and reboot Windows. After a period of time if you believe there are no adverse impacts on your system, and required functionality is not affected, you can repeat Steps 1 - 3 above, but this time right-click on a driver and select Delete to remove it.
5. Reboot Windows and the driver file will no longer be loaded or resident on your system.

The Autoruns method only removes specific driver files, usually .SYS files, and not entire driver packages, nor a range of registry entries which a driver may have created, so this method does not remove all driver residue, only the files which load up with Windows.

DRIVER FILE REPOSITORY

If you are still struggling to find and remove certain drivers, or you just want to see the contents of the drivers Vista is installing, then you should note that Vista holds all the driver packages it has downloaded or uses for standard installation under the *\Windows\System32\DriverStore\FileRepository* directory. These are not the actual driver files actually in use by the system, as those are held under the *\Windows\System32* directory. Each separate driver package is a subdirectory with the name of the .INF file for the package. For example the Nvidia nForce RAID drivers can be found in a subdirectory starting with *nvraid* and ending with a string of numbers.

You can use this driver repository for three things:

§ Remove traces of a faulty or undesirable driver.
§ Manually direct Vista to a particular driver package if it does not detect it automatically.
§ Find and manually modify the driver package so that when Vista detects your device it uses the modified contents to install the driver.

In each case you must first identify which folder under the *\Windows\System32\DriverStore\FileRepository* directory relates to the driver package you are seeking. To do this follow these steps:

1. Download the latest version of the driver and manually open the package in an archiving utility like WinZip or 7-Zip to view its contents, even if it is an .EXE file.
2. Open Windows Search and do an Advanced Search for a specific driver file you know to be unique to that particular driver package (preferably an .INF file), as identified in Step 1.

Copyright © 2010 Koroush Ghazi

3. Match the driver filename and date with one under the relevant subdirectory of *\Windows\System32\DriverStore\FileRepository*.

In most cases you will find that these are mainly the default Microsoft drivers built into Vista, and hence you should not delete them. However if you find the driver package you are looking for then you can delete it and if you uninstall and reinstall your hardware device in Device Manager, Vista will use the next recent driver package when it detects the device. Alternatively you can modify the folder contents with portions of other driver packages, and Vista will attempt to install them when it redetects your device. Or you can simply point Vista to this folder when manually updating drivers as detailed further above.

Obviously these methods are really only for advanced users, as in all other respects you should be able to install or uninstall drivers using the normal methods covered earlier in this chapter. Messing with the driver repository could have serious unintended consequences, so it is generally not recommended.

< DRIVER VERIFIER

If you believe you're having driver-related problems, you can use an advanced tool which comes with Vista called the Driver Verifier. To run it, go to Start>Search Box, type *verifier* and press Enter. It is a complex tool, so read the detailed instructions for its usage in this Microsoft Article. I'll cover its basic usage details below:

1. Once Verifier starts, after a moment you will see a dialog box open - leave the options at their default and click Next.
2. On the next screen, you can either let the Verifier test all the drivers it deems fit, or (as I recommend), select the 'Select driver names from a list' option to pick specific drivers you suspect to be problematic, and click Next.
3. Place a tick against all the driver files you believe need to be checked. To make things simpler, click the Provider column header so that the list is sorted by the providing company, that way if you want to choose your graphics drivers for example you can tick all the boxes for the files provided by Nvidia or ATI. Note that only drivers which are loaded up by Vista are shown; if for some reason you want to add drivers which are not currently loaded, click the 'Add currently not loaded driver(s) to the list' button and select the additional files. Once all the relevant boxes are ticked, click Finish.
4. You will have to reboot your system, at which point during or soon after your PC starts up again you may see a Blue Screen error (BSOD) if the driver file(s) you chose are potentially problematic. If Windows starts up normally and you see no BSOD after a while then the file(s) have been verified as being fine.

Importantly, you will need to disable Verifier once you've finished with it, otherwise it will continue to verify the files at each loadup. To do this, open Verifier again and select 'Delete existing settings' then click Finish. If you cannot access the Verifier user interface to turn it off, open an Administrator Command Prompt, or use the Windows Recovery Environment Command Prompt and type `verifier /reset` and press Enter. You can also uninstall the driver which is causing problems in Safe Mode - see the Backup & Recovery chapter.

Having an error in Driver Verifier is not indicative that a driver is the primary source of your problems. However it is one more way of seeing if it is indeed a driver file which may be contributing to a problem or the source of a problem, or something else altogether. Bear in mind that the majority of system issues are the result of factors completely unrelated to drivers, such as overheating, overclocking, bad BIOS settings, faulty hardware, one or more installed programs causing conflicts, etc. Just because an error points to a driver file in its message, that doesn't mean the file itself is the cause of the problem - drivers often crash when a system is unstable for a range of reasons, and not because they are buggy or unstable themselves. See the Performance Measurement & Diagnostics chapter for more ways of troubleshooting a system issue, including the use of Event Viewer to see specific error logs.

Copyright © 2010 Koroush Ghazi

< GENERAL DRIVER TIPS

The following is some general information and advice regarding all device drivers:

Source of Drivers - Only download and use drivers directly from your hardware manufacturer's website, Windows Update, or from a reputable and well established third-party source which you know and trust. This does not guarantee their stability, but it does help ensure that they do not contain malware. While many people think nothing of downloading drivers from file sharing sites for example, you are essentially putting your trust in people you don't know, and who may even be infected with malware without knowing it. Then of course there are people who are deliberately malicious and will use any opportunity to spread malware through drivers. The hardware manufacturer's site should always be your first choice for obtaining drivers.

User Feedback - Be wary of general user feedback on drivers on places like public forums and in blog comments. In recent years more and more users have turned to blaming drivers (or Windows itself) for various problems on their system, when the problems are often actually the result of factors resulting from general user ignorance or lack of system maintenance, such as overclocking, overheating, conflicting software, or excessive driver residue. This is particularly true for graphics and audio drivers, with any audio or graphics-related problem automatically being attributed to the drivers by the average user, when indeed many other factors can cause these issues. User feedback is useful, but should not be the sole or even the primary basis for determining which driver to install.

Beta Drivers - Beta drivers are pre-final drivers which carry the risk of causing additional system problems because they have not necessarily undergone thorough testing, thus the hardware manufacturer provides no support to users of beta drivers. Generally speaking though, beta drivers downloaded directly from your hardware manufacturer should be relatively stable and safe to use, but best installed only if you are having problems with your current driver and/or only if the release notes and the consensus of user feedback clearly indicate that they provide some significant benefit.

Alpha Drivers - Alpha drivers are even less polished than beta drivers and their use can lead to serious problems such as major instability and even data loss. They are only recommended for advanced users who wish to experiment, or for users who have absolutely no other available option for obtaining a working driver for their hardware. Make certain you prepare a full backup before installing an alpha driver.

Leaked Drivers - Leaked drivers may be alpha, beta or final versions, but they have been unofficially released to the public, often against the wishes of the hardware manufacturer. They may be modified and/or not digitally signed, which only increases the risk that they contain malware and/or may not provide stable functionality for your device and result in data loss. As with alpha drivers, I do not recommend using leaked drivers unless you have absolutely no other option, and only after making proper backups beforehand. Aside from putting your data at risk of being lost, you are also putting your security at risk.

Modified ('modded') Drivers - Current modified drivers do not provide any genuine benefit over the standard drivers from your hardware manufacturer. Don't be fooled by promises of large performance gains or magic fixes - these are almost always unfounded or exaggerated claims designed to entice people into using the driver. The only time I would recommend a modified driver is if they have been .INF modified to allow them to be installed and used on hardware they were not originally intended for. This is a simple text file modification done primarily to provide drivers for hardware which may otherwise not have frequent driver support, such as laptop graphics chipsets. Obviously .INF modification can result in unexpected behavior because the driver is being used on hardware it was not designed for, but it may be the only option available to people with certain hardware. In all other cases I recommend against using modified drivers for safety and stability reasons. If a manufacturer has disabled a particular feature in a driver, it is for a good reason.

Copyright © 2010 Koroush Ghazi

Drivers are a critical component of the way your hardware interacts with Windows, and have a significant impact on performance and stability, so it is best to make sure they are kept up to date, and that you do not experiment unnecessarily with them. Regularly refer to the front page of TweakGuides.com for the latest news on official driver updates.

Copyright © 2010 Koroush Ghazi

PC SECURITY

Over the past few years PC security has become a major issue of concern due to the increase in the number of ways in which the security of the average home PC user can be compromised. Accordingly, Windows Vista has seen a marked improvement in security features over Windows XP. You may find some of these features annoying or confusing, however I strongly advise you not to take the topic of PC security lightly or ignore it. It is extremely important that you become acquainted with both the types of threats to the integrity and privacy of your PC, as well as how the Windows security-related features actually work to counter them.

It is incorrect to suggest that only the very careless or novice user will succumb to a security-related problem or Malware (malicious software) infestation. Even if you consider yourself an advanced user, you need to bear in mind that malware threats these days are becoming increasingly complex and dangerous. In the past a malware infestation would usually result in little to no real harm; you'd have to delete a few files or at worst reinstall Windows or restore a backup. Now however, malware development and distribution is often coordinated by organized crime groups for financial gain, so even a single incidence of malware infestation can potentially result in the loss of money, software serial numbers, email account details, and other sensitive personal information. Having a carefree attitude towards PC security is a thing of the past.

This chapter starts by explaining the types of threats to PC security, then looks at the built-in features and tools in Windows Vista which deal with these threats, and then at recommended third party tools and applications to supplement Vista's security measures, as well as general tips for maintaining a secure PC.

< SECURITY THREATS

There are a wide range of security threats which Windows users face, particularly from various types of malicious software. Malware can enter your system and cause problems ranging from the very minor to the very serious. Malware can remain hidden for long periods and have subtle effects, or its impact can be immediate and blatant. However it is important to understand that malware does not damage your computer hardware directly nor does it actually physically 'infect' the hardware. Malware is software-based, and its threat is to the integrity of your data, your privacy and your finances.

There are different types of malware and security threats, and the major categories of these are covered below:

VIRUSES & WORMS

Viruses are small programs that load onto your computer without your permission and without your knowledge of their real function. They are called viruses because just like a human virus they are designed to self-replicate, attaching themselves to normal programs and files and spreading to other computers through exchange of these infected files, where they repeat the same process once on the new computer. Viruses range from the mischievous to the truly harmful, destroying valuable information through data corruption and causing a range of strange system behaviors.

Worms are similar to viruses, however they generally do not attach to other files, they can spread independently.

Copyright © 2010 Koroush Ghazi

TROJAN HORSES

A Trojan, short for Trojan Horse, is a malicious program that is often installed on your system under the guise of being another, often useful, program. Trojans differ from viruses in that they are used to provide an outside attacker with access to your system. This may be for the purposes of stealing valuable information, installing other forms of malware, or using your system as part of an illegal network such as a botnet.

SPYWARE

Spyware is similar to a Trojan, in that it is software that is usually installed on your system purporting to have different functionality, or as a component of a useful program. Spyware does not allow an outside attacker to take control of your system, but it does transmit information about you and your system, such as your passwords, keystrokes or Internet usage behavior to the distributor of the spyware.

ADWARE

Adware is similar to spyware, but is not necessarily malicious, as it is mainly used to target online advertising or create popup ads or redirect/force your browser to view pages with advertising. However again it is usually installed without your full knowledge or permission. Despite it's relatively less malicious nature, this software is usually undesirable, breaches your privacy and uses system resources and bandwidth for no genuinely useful purpose.

ROOTKITS

A Rootkit is a form of malware deliberately designed to mask the fact that your machine has been compromised and is now open to unauthorized usage by an outside attacker. The rootkit will prevent traces of itself or any associated malicious activity from being detected by usual detection methods such as running an anti-virus program or examining the Windows Task Manager for unusual processes. At the same time, a remote attacker can take advantage of the rootkit to access your machine for malicious purposes.

PHISHING

While not a form of malicious software, Phishing is fast becoming a common and significant security threat. Typically it involves fooling unsuspecting users into revealing important personal information such as credit card numbers or passwords. For example a phishing attempt may involve getting you to click a login link in a fake email from your bank, which then takes you to a fraudulent imitation of the user's bank login page, whereupon you enter your login details, giving the perpetrator all the details they need to then login to your real bank account and rob it. Phishing is not malware as such, since it does not usually involve software infection, it uses social engineering techniques instead to trick and defraud its targets.

The categories above are in no way conclusive or all-encompassing. There are many variants and combinations of the above security threat categories, and more are emerging every day. Over the past few years these types of threats have become ever-more sophisticated, intrusive and malicious. Even relatively tech-savvy users face the risk of picking up a serious piece of malware or even accidentally falling prey to phishing. It may not happen often, but it only takes one serious security breach to result in financial loss or data loss and the subsequent major hassles of having to obtain new credit cards, proving your case to a bank or financial institution, changing all your passwords, contacting software manufacturers for new serial numbers, and so forth. The people behind the creation of these security threats are making large sums of money from doing this, so they have the resources and the incentive to constantly adapt to existing malware defenses and innovate new and ever-more-intrusive forms of malware and online scams.

Protecting yourself against these security threats is not as simple as installing lots of malware scanners and turning them all on. Aside from draining performance, causing software conflicts and other system issues, malware scanners often lag behind in the detection of new security vulnerabilities and exploits. The best

Copyright © 2010 Koroush Ghazi

defense against malware is a combination of correctly configuring built-in Windows security features, using appropriate third party security software, and most importantly, being educated and vigilant, and understanding your own system. This is one of the reasons I urge users to learn about how Windows and their PC works, because people who gain an intuitive understanding of the fundamentals stand a much greater chance of avoiding a security breach.

The rest of this chapter contains the tools and methods you can use to counter a wide range of security threats, starting with the security features built into Windows Vista.

< WINDOWS SECURITY CENTER

The Windows Security Center is designed to consolidate the main Windows security-related information in a central location, issuing alerts to users if it believes any of your security settings are insecure, or if there are any problems with any of your installed security software. The Vista version of the Security Center is much more refined and better integrated than the XP version. It now allows installed security software such as third-party antivirus or firewall packages to use the Security Center to both warn users if something is wrong, as well as provide users with useful steps for how to rectify the problem - this is detailed in this Microsoft Article.

While all this sounds good in theory, and is certainly useful for novice users, in practice the Security Center makes itself an unnecessary annoyance. Once you've established optimal security settings based on your own preferences and having read through this book, unfortunately the Security Center will continue to sit in the Notification Area and regularly nag you with Windows Security Alerts if your settings don't match what it considers optimal. If Windows Security Center detects an issue, it will place a small red shield icon with a cross in the middle of it in your Notification Area, at the bottom right corner of the screen. Just after you start a Windows session it will warn you about any issues, and also when launching the offending program(s) it will again provide details of the potential problems it's detected. Clicking the shield or prompt will take you to the Security Center.

By default Security Center has four categories of security features it monitors: Firewall, Automatic Updating, Malware Protection and Other Security Settings. Each section is color-coded as either Green (good), Yellow (potential problems) or Red (bad). The sections are described in more detail below:

Firewall: This area monitors whether the Windows Firewall is turned on or off. Fortunately, the Security Center can detect some (but not all) third-party firewalls which are installed on your system, and as it recommends, it is not wise to run both the Windows Firewall and another software firewall together. It won't red light as long as a valid firewall is detected and on. See the Windows Firewall section further below for firewall configuration details - I generally recommend running the Windows Firewall as it is perfectly adequate, unless you have a specific third-party firewall you want to use instead.

Automatic Updating: This area monitors whether you have the Windows Updates feature set to allow automatic updating. As recommended under the Windows Updates section of the Control Panel chapter, you do not need to have automatic updates enabled for your system to remain secure; preferably you should select the 'Check for updates but let me choose whether to download and install them' so that you are still alerted when an update is available, but you can choose if and when you want to download and install it. Unfortunately Security Center considers anything other than full automatic updating as insecure and flags it as a yellow or red light.

Malware Protection: This area monitors your main antivirus scanner, as well as Windows Defender. It does not necessarily detect all anti-malware programs such as those covered later in this chapter, but it does seem to detect the major antivirus packages. If you don't have a recognized malware scanner, click the 'Show me available options' link and select 'I have an antivirus program that I'll monitor myself' though this still throws up a yellow light. If it detects your anti-malware package you can even update it through the

Copyright © 2010 Koroush Ghazi

Security Center, however it seems to insist on the background scanning features of the anti-malware software being enabled otherwise it throws up a red light. Of course if Windows Defender is disabled at any time then that too gets a red light, even if you're using other anti-malware scanners which may be more effective. See the Windows Defender section below for more advice.

Other Security Settings: The last category monitors Internet Explorer's security settings and User Account Control. If IE's security-related features, such as Protected Mode, the Phishing Filter and general Security Level are not enabled or high enough then Vista will warn you and allow you to reset them to secure levels - see the Internet Explorer chapter for details of these features. If User Account Control is disabled, this too raises a red light - see UAC further below.

While the idea behind the Security Center is a noble one, and indeed is useful to novice or very forgetful home PC users, unfortunately the Security Center is more of an annoyance to medium or advanced users, particularly those who have decided on a different security strategy than the one the Security Center considers optimal. Using certain perfectly good anti-malware programs such as those covered later in this chapter will protect you extremely well, yet because some of them are not detected by the Security Center or because it believes that all the features of an anti-malware program need to be enabled for it to be effective, you will constantly get false warnings. Fortunately you can turn off the Security Center's incessant prompts by clicking the 'Change the way the Security Center alerts me' link in the left pane of the Security Center. You can select the default of 'Yes, notify me and display the icon' which is only recommended for novice users; 'Don't notify me, but display the icon' which is only recommended if all your security software is totally compliant with the Security Center; or 'Don't notify me and don't display the icon' which is recommended for everyone else who has read this book.

If you do disable the Security Center prompts, this will not disable the software the Security Center monitors, only the Center's own prompting behavior. Make sure to go through the rest of this chapter and configure your security properly.

< USER ACCOUNT CONTROL

The most fundamental layer of improved security in Windows Vista is the restriction of Administrator level access to the system by default. This is because a user logged in with a full Administrator-level User Account can do pretty much anything to the system, from altering the registry to installing any software to creating or deleting other User Accounts. An Administrator User Account therefore provides the greatest power and flexibility, and hence is the preferred choice for most users, as opposed to the 'Standard User' account. For more details of User Accounts, see the section of the same name under the Control Panel chapter, however for the purposes of this discussion you should keep in mind:

§ Administrator User Accounts can make any type of changes to the system without restriction, including altering other User Accounts.
§ Standard User Accounts are restricted to installing most non-intrusive software and making changes as relevant to their own account such as changing display or power settings. They cannot make a range of system-wide changes nor changes which affect other users.

Unfortunately malware capitalizes on the fact that most people run Administrator-level User Accounts, tricking users into installing malware, often quietly in the background while the user is unaware of what's happened, hence gaining total access to your system. Obviously running an Administrator-level User Account as your normal account has a great deal of risk attached to it, but it is also extremely convenient and often necessary for undertaking tweaking, driver updates and other advanced functionality. So in an attempt to balance convenience and security, Vista has changed the way it manages User Account access to a method called User Account Control (UAC) which is enabled by default.

Copyright © 2010 Koroush Ghazi

The process of how User Account Control works is detailed as follows:

1. Regardless of whether you're logged in as a Standard User or Administrator level User Account, you are initially restricted to making changes to the files and folders you own, installing basic programs and other non-intrusive functions. Basically you have Standard User privileges even if logged on as an Administrator.
2. As soon as you try to make a system-level change such as installing a driver, editing the registry, launching or installing system-intrusive software or altering or deleting another user's files, you will be prompted to confirm your action. When UAC is launched, there are two important things to note:

    § Your screen will change as you are placed in a sort of 'limbo' called Secure Desktop mode whereby no other program can execute itself except for important System processes. This Secure Desktop is an important layer of protection and prevents malware programs from doing things like faking the file details on a UAC prompt or automatically accepting a UAC prompt;
    § You can't just press Enter to continue - by default the UAC prompt's focus is on the Cancel button, so pressing Enter will abort execution of the program or change. This helps ensure that people don't just get into the habit of quickly pressing Enter whenever they see a UAC prompt without paying attention.

3. If you're running an Administrator level User Account, the prompt simply requires that you click the Continue button to continue the task; if you're running a Standard User level User Account, you will also need to enter the password for an Administrator level account to continue. If you don't have the password, or you're not familiar with the program being launched, then click Cancel.

In the past, if a Windows user wanted optimal security they would have to run two separate accounts, one an Administrator and the other a Standard account, and switch between them whenever they wanted to install any software, or play certain games. The end result was that most people simply did not bother with this and just used their Administrator account all the time, creating unnecessary risks. UAC combines security with relative convenience: you can use one account all the time, whether a Standard user or Administrator, and only elevate privileges to Administrator level when you actually need it. UAC effectively provides a barrier against malware quietly executing itself and/or making any system changes at any time in the background without your knowledge.

Even if a program or file has no malicious intentions whatsoever, you are still giving it unrestricted access to your system should you accept a UAC prompt. This means the program may make system-intrusive alterations which can destabilize your system or make undesirable changes to it. Consider whether you really need to install or launch the program, as the more of these types of programs you have on your system, the greater the potential for problems regardless of security concerns.

If you did not specifically initiate the program or procedure, then you should view the UAC prompt with great suspicion, click the Details link, note the path and filename of the program that wants to execute, Cancel the UAC prompt and investigate further. At the very least run several malware scanners on the program in question.

Copyright © 2010 Koroush Ghazi

File System and Registry Virtualization

In order to provide compatibility with older applications not built with UAC in mind, UAC incorporates File System and Registry Virtualization. It comes into effect if a program is not given full Administrator privileges while attempting to make changes to the following folders or registry locations:

- *ProgramFiles*
- *Windows*
- *Windows**System32*
- `[HKEY_LOCAL_MACHINE\SOFTWARE\]`

Any files, folders or registry changes the program needs to make are redirected to local copies stored under the current user's profile. This prevents users with insufficient privileges from harming the system, but still allows them to install and use most types of software.

However this is not a foolproof solution. Some older applications and games can only function if they have full Administrator access, but may not ask for such privileges, and hence there will be no UAC prompt to escalate their privileges during installation or at launch time. Virtualization will allow them to install, but they will not install properly and/or will fail to launch or function properly.

The best way to address the issue of certain trusted applications failing to install or launch properly when UAC is enabled is to go to the main setup executable or launch icon for the program, right click on it and select 'Run as Administrator'. This will raise a UAC prompt to elevate privileges each time the program is launched, which you will need to successfully accept to continue. The program will then launch or install as normal, having been given full Administrator access. To set this behavior permanently, right-click on the main executable or launch icon, select Properties and under the Compatibility tab tick the 'Run this program as an administrator' box and click OK. Alternatively if that option is not available, go to the main Shortcut tab for the program's launch icon and under the Shortcut tab click the Advanced button, then place a tick in the 'Run as Administrator' box. Only do this if you know and completely trust the application, having obtained it from a reputable and trusted source.

Importantly, because of File System and Registry Virtualization, if you install an application under a Standard User Account and/or don't accept an elevation prompt from UAC, your settings for particular applications may be stored under your local profile. If you then switch to another User Account, or run that same application with full Administrator privileges later on, your settings may be appear to have reset to the defaults as the program switches to using another set of folders or another area of the Registry for its saved settings. In simple terms this means that it is not wise to enable or disable UAC constantly. For common solutions to Virtualization issues, see this Microsoft Article.

Customizing UAC

Instead of turning it off, you may wish to customize UAC so that some of its behavior is changed. This is not to be taken lightly, since changing some of the features of UAC, such as turning off the Secure Desktop function, can in effect completely undermine the effectiveness of UAC, in which case you'd just be better off turning it off altogether; crippling UAC is in some ways worse than just turning it off because it gives you a false sense of security.

To customize UAC you will need to use the Local Security Policy Editor - note that if you run Vista Home Basic or Vista Home Premium, this is not available so see further below for an alternate method. To launch Local Security Policy go to Start>All Programs>Administrative Tools>Local Security Policy, or go to Start>Search Box, type *secpol.msc* and press Enter. In the window which opens, double-click on the 'Local Policies' item in the left pane, then select the 'Security Options' item. In the right pane scroll down and you'll see a range of options starting with 'User Account Control'. Each is covered in more detail below, but you

Copyright © 2010 Koroush Ghazi

can also double-click on any option and click the Explain tab to see more details including the default settings which are different depending on which edition of Vista you're using:

Admin Approval Mode for the Built-in Administrator account: This setting determines whether the built-in Administrator account in Vista is affected by UAC - by default it is not. This account is not the same as the Administrator level account you create when installing Vista, this setting refers to the hidden built-in Administrator account in Vista - see the User Accounts section of the Control Panel chapter for details.

Allow UIAccess applications to prompt for elevation without using the secure desktop: This setting determines whether User Interface Accessibility (UIAccess) programs, such as Windows Remote Assistance, can automatically disable the Secure Desktop feature when providing UAC elevation prompts. Disabled is fine for most people, unless you are in an environment where you're likely to need remote assistance and are using a Standard User Account.

Behavior of the elevation prompt for administrators in Admin Approval mode: Normally the UAC prompt will ask Administrators to simply click Continue to proceed. This is equivalent to the 'Prompt for Consent' option and is recommended. You can however select 'Prompt for Credentials' if you want even tighter security, so that even Administrators have to enter their password each time they face a UAC prompt; or you can select 'Elevate without Prompting' which is not recommended, as it effectively turns off UAC by removing all UAC for Administrator level User Accounts.

Behavior of the elevation prompt for standard users: This option is similar to the one above, however it controls the behavior of UAC for Standard Users not Administrators. The default is 'Prompt for Credentials', but you can change this to 'Automatically deny elevation requests' if you want tighter security, so that Standard Users won't see a UAC prompt; they won't be able to undertake any task which triggers a UAC prompt.

Detect application installations and prompt for elevation: If Enabled, Vista will attempt to detect an application installation and UAC will kick in to ensure the application gets Administrative access if it requests it; if Disabled, any program can be installed without UAC prompt, but this is not wise as programs which need Administrator access but don't request it and hence don't get it will not install properly.

Only elevate executables that are signed and validated: If Enabled forces Public Key Infrastructure (PKI) certificate validation before an executable can be run. In other words only signed, validated and therefore trusted executables can be given full Administrator access to the system. Disabled is recommended for home users unless you require absolute maximum security; some legitimate programs will fail this test.

Only elevate UIAccess applications that are installed in secure locations: If Enabled only UIAccess applications which reside in a secure location, namely under the *\Program Files*, *\Program Files (x86)* or *\Windows\System32* directories will run with UIAccess level integrity; if Disabled any UIAccess program can run with UIAccess integrity from any location. There is no reason to Disable this as it provides an extra layer of security against malware.

Run all administrators in Admin Approval Mode: This option provides the core functionality of UAC. If Enabled all Administrator level User Accounts will operate as described further above in this section. If Disabled then UAC is effectively disabled for Administrator level User Accounts, so it is not recommended unless you perhaps want to disable UAC for Administrators and leave it functional for Standard Users.

Switch to the secure desktop when prompting for elevation: Secure Desktop mode has been described further above and is a critical component of UAC. It prevents tampering or execution of programs in the background when UAC is running. You can Disable it here but it is strongly not recommended except perhaps briefly for troubleshooting purposes.

Copyright © 2010 Koroush Ghazi

Virtualize file and registry write failures to per-user locations: As discussed under the File System and Registry Virtualization section above, when Enabled (by default), this option ensures that Standard User level User Accounts can still install pre-Vista applications which require traditional full Administrator access; the system locations usually written to by the program will be 'virtualized' by redirecting them to locations within the Standard User's personal folders.

You should ensure that you do not change any of the above options unless you have good reason to do so. Most of the options above are necessary for UAC to work effectively.

If you run Vista Home Basic or Vista Home Premium, there is no Local Security Policy editor, so you will instead need to access the Windows Registry directly if you want to customize UAC as covered above. All the main UAC settings are held under the following location when using Registry Editor:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]
```

The following settings may not exist, so you will have to create each of them as a new DWORD as required. The names of the settings covered further above are reproduced below along with the relevant registry entries and the valid values that can be assigned to them:

Admin Approval Mode for the Built-in Administrator account:

```
FilterAdministratorToken=0
```

Set to 1 to enable, 0 to disable.

Allow UIAccess applications to prompt for elevation without using the secure desktop:

```
EnableUIADesktopToggle=0
```

Set to 1 to enable, 0 to disable.

Behavior of the elevation prompt for administrators in Admin Approval mode:

```
ConsentPromptBehaviorAdmin=2
```

Set to 0 to elevate without prompting, 1 to prompt for credentials, 2 to prompt for consent.

Behavior of the elevation prompt for standard users:

```
ConsentPromptBehaviorUser=1
```

Set to 0 to automatically deny elevation requests, 1 to prompt for credentials.

Detect application installations and prompt for elevation:

```
EnableInstallerDetection=1
```

Set to 1 to enable, 0 to disable.

Copyright © 2010 Koroush Ghazi

Only elevate executables that are signed and validated:

```
ValidateAdminCodeSignatures=0
```

Set to 1 to enable, 0 to disable.

Only elevate UIAccess applications that are installed in secure locations:

```
EnableSecureUIAPaths=1
```

Set to 1 to enable, 0 to disable.

Run all administrators in Admin Approval Mode:

```
EnableLUA=1
```

Set to 1 to enable, 0 to disable.

Switch to the secure desktop when prompting for elevation:

```
PromptOnSecureDesktop=1
```

Set to 1 to enable, 0 to disable.

Virtualize file and registry write failures to per-user locations:

```
EnableVirtualization=1
```

Set to 1 to enable, 0 to disable.

UAC and the Language Bar

In some instances when a UAC prompt appears, the Language Bar will also appear at the top of the screen for no apparent reason. If you do not need to switch languages, this is an unnecessary addition, and can be disabled by opening the Registry Editor and going to the following location:

```
[HKEY_USERS\.DEFAULT\Software\Microsoft\CTF\LangBar]
```

```
ShowStatus=3
```

The DWORD above may not exist in your registry, so create it as shown above. Setting it to a value of 3 will prevent the language bar from appearing whenever a UAC prompt appears. If for any reason you want to reverse this, set the above entry to a value of 0.

Disabling UAC

I strongly recommend that if you have access to an Administrator level User Account that you leave UAC enabled. Malware is becoming increasingly more common, insidious and malicious. Simply using a few malware scanners and 'being careful' is no longer enough to safeguard your system. As security measures become more complex, so too is malware. It is not an exaggeration to say that all it takes is one incidence of a malware infection and your login passwords and credit card details could be compromised and sent across the Internet within hours. Hackers don't have to specifically target you or your machine, there are automated scripts and software which do the work for malware creators and hence can compromise thousands of machines with little effort if they sit unprotected.

Copyright © 2010 Koroush Ghazi

UAC is an inconvenience when compared to not having any prompting behavior, and it can indeed seem excessive at times. However UAC has no performance impact so disabling it will not make your system any faster. Like most people I started off absolutely hating UAC and its continual prompting, but after a while of using it I've found that I've become used to it and the extra layer of security is actually welcome now; it only requires one or two extra mouse clicks to accept a UAC prompt which is hardly a major sacrifice. By itself UAC is not designed to be a perfect form of protection against malware, but it does give you greater control and knowledge of exactly what is running on your system and what changes are being made to the system at any time. Ironically this is precisely what a more advanced user should desire - more control and knowledge, not less.

If you still wish to turn off UAC, the process is relatively straightforward. Go to Control Panel>User Accounts and click the 'Turn User Account Control on or off' link. On the next screen, untick the 'Use User Account Control (UAC) to help protect your computer' and click OK. You will then have to reboot for the change to come into effect. Remember that whenever you enable or disable UAC, due to Virtualization (see further above), you may lose your settings for particular programs if they were not installed with full Administrator privileges, or were installed under a different User Account.

Some final thoughts on UAC:

- § UAC has no performance impact, compared to the performance impact that background malware scanners have in slowing down reads and writes to your drive and causing potential conflicts.
- § UAC tries to provide a compromise between the convenience of running an Administrator account all the time with the security of running a Standard Account.
- § UAC is perfect for people wanting to have multiple accounts on the same PC. By setting these accounts as Standard Users and enabling UAC, they each cannot install harmful software or change system settings, but due to Virtualization can still install and use most non-intrusive software normally and without impact on the other users.

Make sure to read the User Accounts section of the Control Panel chapter for more details relevant to understanding UAC.

< ACCESS CONTROL

Windows assigns every item on the system a security descriptor which describes which users or groups are allowed access to them, and what that level of access is. This is designed to prevent unauthorized access or harmful changes. To view these Permissions for any file or folder, right-click on it and select Properties, then under the Security tab you can see the groups or usernames currently assigned to that object. Left-click on a particular group or username and you will see in the box below it the types of things they are allowed to do to that file.

If you are an Administrator or have appropriate permission you can alter the permissions for the file by clicking the Edit button and either Add or Remove other users or groups, or alter the specific things they are permitted to do, such as making a file read only for particularly users or groups. Alternatively you can click the Advanced button if you wish to get even more specific about permissions. One important feature is that any time a user creates a file or folder, they are the Owner of that file and can always change the permissions of the object. Note that in general given the system has to check permissions for every file and folder, it is better for system performance purposes to assign permissions to groups rather than specific users wherever possible.

Copyright © 2010 Koroush Ghazi

If as the Administrator you find a file or folder which you are not the owner of and hence may not be able to access or alter, you can use the `Takeown` command to reclaim ownership of it. Open an Administrator Command Prompt, type `takeown /?` and press Enter for details of how to use the command.

While users don't have to worry about Access Control for the most part, it's important to understand that this is one reason why you may see several prompts if you go to alter a file on another drive or outside your own personal folders. Standard User privileges are generally not sufficient to alter most files except your own, so Administrator credentials need to be shown, even for something as simple as renaming a file you don't own. For more details of Access Control and related security features see this Microsoft Article.

< WINDOWS DEFENDER

Another layer of protection included in Vista is Windows Defender. The primary aim of this program is to provide basic protection against spyware, as this is the most common type of malware on the average PC, and hence the most dangerous in terms of compromising personal details such as online banking login passwords or credit card numbers. Windows Defender can also find other common forms of malware including adware and rootkits, but it is not completely effective in finding all types of malware so it should definitely not be relied upon as the sole anti-malware scanner on your system.

Windows Defender is on and running in the background by default, but to access its user interface, go to Start>All Programs>Windows Defender, or go to Control Panel>Windows Defender, or go to Start>Search Box, type *defender* and press Enter. I recommend that you leave Windows Defender enabled, but configure it to be less intrusive as detailed below. Even when you use other spyware scanners (which you must do), Windows Defender needs to remain enabled to provide access to the important Software Explorer feature covered under the Startup Programs chapter, so that's at least one reason to not disable it outright. If you are going to disable it altogether, make absolutely certain that you are using a combination of UAC and good anti-malware scanners including at least one dedicated spyware scanner.

Note that if you are going to install Microsoft Security Essentials as recommended later in this chapter, then you can skip the entire Windows Defender section because Windows Defender is automatically disabled and replaced by Microsoft Security Essentials. Only follow the instructions below if you wish to leave Defender enabled alongside other third party malware scanners:

CONFIGURING WINDOWS DEFENDER

Below are details on the range of options and features in Windows Defender, including recommendations:

Home: Takes you to the main Windows Defender screen where you can see the current status of your machine, whether any scan is running, and when the last and next scans are scheduled to be undertaken. Note the Definition version is important - do not allow the Windows Defender definition file to be too old, regularly update the definition file through Windows Update - see Windows Update under the Control Panel chapter for details.

Scan: When clicked, this option starts a Quick Scan of your system by default, going through your important system files, folders and the Windows Registry to look for traces of spyware. By clicking the small down arrow next to the Scan button, you can manually choose to do a Quick Scan, Full Scan or Custom Scan. As noted, a Quick Scan focuses on your system files and folders, taking the least amount of time to complete, but also providing the least security. A Full Scan goes through your entire PC to look for malware, which is more secure but can take quite a bit longer. A Custom Scan allows you to select the specific drive(s) and/or folder(s) you wish to scan. You should run a Full Scan of Windows Defender in conjunction with other scanners every week or so, and also if you suspect you've actually been infected. A custom scan of any downloaded files is also recommended as required.

Copyright © 2010 Koroush Ghazi

History: This section displays a history of any recent actions you've taken in response to Windows Defender notifications. You can click on each item to see more details of the exact file(s) involved.

Tools: This section contains several important settings and tools:

§ *Options:* Used to configure how Windows Defender actually works. I recommend disabling Defender's automatic scans of your PC. If you wish to leave this enabled, a daily scan using Quick Scan should be sufficient as this usually only takes a few minutes at most and is useful if you forget to manually run any malware scanners often. If you wish to leave automatic scanning enabled, then I recommend ticking the 'Check for updated definitions before scanning' so that it uses the latest definition file, as without the latest definition file it's pointless to scan your system regularly; I also recommend ticking the 'Apply default action to items detected during scanning' box and configuring them as covered below.

The default actions listed allow you to specify what you want Windows Defender to do when it finds potentially malicious software in one of three categories: Low, Medium and High risk; the fourth category Severe is automatically acted upon. The default actions are explained in detail in this Microsoft Article, and they seem reasonable, so select 'Default Action' for all three alert levels. You will be notified immediately of most actions Windows Defender undertakes, unless they are extremely insignificant.

The Real-time Protection options allow you to determine which types of activities and areas Windows Defender monitors to prevent spyware from installing or executing. These options are explained in detail in this Microsoft Article. There have been accounts of Windows Defender causing system slowdowns when using these options, and Windows and application startup being slightly longer, however the precise performance impacts are not clear. They are best left enabled for more novice users, but advanced users can disable them if you regularly scan your system with other malware scanners (which is of course recommended) and importantly if you have UAC enabled.

When asked to select when Windows Defender notifies you, it should be safe to untick both boxes to reduce annoyance. Once again this is particularly true if you have UAC enabled.

To remove the Windows Defender icon from the Notification Area select 'Only if Windows Defender detects an action to take'. That way you'll only see the Windows Defender icon if action is required.

The three Advanced Options here should all be enabled if you use Windows Defender. They increase the effectiveness of Windows Defender in finding new or more deeply hidden spyware. Note however that the 'Use heuristics to detect potentially harmful or unwanted behavior by software that hasn't been analyzed for risks' option could marginally decrease system performance. The 'Scan the contents of archived files and folders for potential threats' will also add to scanning time if enabled. The 'Create a restore point before applying actions to detected items' should be ticked for added protection.

You can manually specify any particular files or folders you wish to exclude from Windows Defender's scanning, however this is only recommended if you know for certain that a particular file or location is safe but will provide a false positive. Also remember that definition file updates may resolve false positives.

Finally, the Administrator options allow you to completely turn off Windows Defender - which is not recommended, particularly given the Software Explorer function is tied to Windows Defender being enabled. Click the Save button when finished here, and you will be taken back to the Tools screen.

Copyright © 2010 Koroush Ghazi

§ *Quarantined Items:* Shows any items which have been caught as suspected spyware and allows you to determine what to do with them.
§ *Allowed Items:* Lists the items which have been flagged by Windows Defender but you have manually chosen to allow to keep on your system.
§ *Software Explorer:* This is a useful utility for monitoring and enabling/disabling/removing startup programs, background programs and network connected programs. More details of this utility's functionality can be found under the Startup Programs chapter.

Windows Defender must be viewed in the context that it is there to provide basic protection against harmful spyware in Windows Vista out of the box. Many users of Windows will never be fully aware of the danger of malware nor use appropriate precautions, so Windows Defender by default gives a good level of protection to these users.

< WINDOWS FIREWALL

To help protect your system against intrusions through your network connection, Vista provides a built-in Windows Firewall. The major role for a firewall is to prevent unauthorized or malicious data from being sent into your machine over the Internet, or being sent from your machine via the Internet connection. For example once a spyware or trojan program installs on your system, it needs to send information out of your machine back to its originator. A firewall can serve to block this type of unauthorized data transfer, thwarting the main aim of the malware which is to steal your sensitive information. Some hackers run automated programs looking all over the Internet for entry points (called Ports) into unprotected PCs, and once again this can only be blocked through the use of a firewall.

To access the Windows Firewall go to Control Panel>Windows Firewall, or go to Start>Search Box, type *windows firewall* and you can either choose the basic Windows Firewall or the Windows Firewall with Advanced Security - both are covered below. Importantly, Vista's firewall allows users to block both incoming and outgoing network traffic, whereas Windows XP's firewall could only block incoming traffic. For more details see this Microsoft Article.

BASIC CONFIGURATION

On the main Windows Firewall screen you will see the status of the firewall - whether it is on or off, and details of the security and notification settings. By default the Windows Firewall is on and already blocks all unauthorized incoming connections, but it doesn't block any unauthorized outgoing connections. The reason for this is that blocking incoming connections causes few problems, but blocking outgoing connections can prevent normal Internet functionality in a range of circumstances, so it requires specific configuration which may be beyond the average user - see Advanced Configuration further below.

To change the specific settings for the Windows Firewall, click the 'Change settings' link and a new dialog box will open, the details of each tab are covered below:

General: Here you can turn the firewall On or Off, or choose additionally to 'Block all incoming connections'. I strongly recommend that you keep the Windows Firewall set to On at all times unless you have another software firewall installed and enabled, in which case you should disable the Windows Firewall, as two or more software firewalls working together can cause problems. A firewall has no performance impact on your system as such, it is a barrier against inappropriate or malicious network activity and without it you greatly increase the risk of having your machine compromised and even used by hackers to distribute spam for example.

Copyright © 2010 Koroush Ghazi

Note that it is not recommended that you tick the 'Block all incoming connections' unless you want the tightest possible security, as although this will allow you to browse most of the Internet and send and receive emails, it will impair necessary Internet functionality like online gaming and Internet communications by legitimate applications, since all Exceptions are ignored.

Exceptions: With the Windows Firewall enabled, Vista recognizes that legitimate programs will need to send and receive information via your Internet connection. When you first run a program that requires such access to the Internet through the Windows Firewall, you will receive a notification informing you that the Windows Firewall has blocked some features of the program (namely those requiring Internet access), and that you can either 'Keep Blocking' it or Unblock it. If you didn't initiate the program, or it appears suspicious, select 'Keep Blocking' and investigate further. By selecting Unblock you have created an Exception which tells the firewall to always allow this program access to the Internet through the Windows Firewall when it starts running. The problem is that the more Exceptions you create, the more open Ports there will be while these programs are running, and hence the greater the chance that a hacker scanning across the Internet for open ports will find yours and use it. Fortunately the required Ports are only opened when the program launches and are closed as soon as the program is closed, so the risk is minimized.

The Exceptions list shows all programs which may require access through the Windows Firewall, but only those which have a tick next to them are currently not blocked by the firewall. Try to keep the number of programs with ticks on this list to a minimum To see more details about a program on the list, highlight it and click the Properties button. Should you wish to manually add a new program to the list, click the 'Add Program' button and select the program - obviously it is imperative that you don't add a program to the list unless you're 100% sure it is a safe and necessary program. You can also manually add a Port to open by clicking the 'Add port' button, but this is not advisable as an open Port configured this way stays open until you manually close it again, whereas an Exception only opens a Port when a program begins to run, and closes it again when it exits, which is much safer.

Finally, make sure you place a tick in the 'Notify me when Windows Firewall blocks a new program' box at the bottom, otherwise you will receive no warning that a new program you are attempting to run is being blocked by the Firewall and hence may not function properly.

Advanced: This tab merely allows you to select specific connections for which these Windows Firewall settings apply. All your connections should be listed and ticked unless it is a connection to a totally trusted network such as another PC you own or a network within an already-firewalled business environment. If you feel you've messed up your Windows Firewall settings and/or you're having network or Internet connectivity issues, click the 'Restore Defaults' button. The actual advanced settings have moved from here and are covered below.

ADVANCED CONFIGURATION

To access the true Windows Firewall advanced settings, you will need to go to Start>Search Box and type *windows firewall* and select the 'Windows Firewall with Advanced Security' item, or in Start>Search Box type *wf.msc* and press Enter. A new box will open which allows much greater customization and monitoring of the Windows Firewall, including allowing you to configure the blocking of outgoing network traffic.

Covering all the functionality of the Advanced Windows Firewall settings is beyond the scope of this book, as it is quite detailed. Fortunately you can get detailed instructions by scrolling down the main screen of the Windows Firewall Advanced box and clicking the links under the Resources section. Below we will only look at how to enable the blocking of outbound network traffic, which is generally not required for the average user, but might be desirable for people wanting tighter security.

Copyright © 2010 Koroush Ghazi

In the main Overview box, you will see three profiles: Domain Profile, Private Profile and Public Profile. These profile types are covered in more detail under the Network & Sharing Center section of the Control Panel chapter. As recommended there, most PC users with a standard connection to the Internet should select the Public Profile for maximum security while still retaining normal functionality. Regardless, the profile you are using now for your connection should show the words 'is Active' after it in this box. You will see whether the Windows Firewall is On, and the fact that the inbound connections that do not match a rule are blocked, meaning inbound network traffic is only allowed for Exceptions as covered further above.

To block outbound network connections, click the 'Windows Firewall Properties' link in the Overview section and a new dialog box will open. It has four tabs: one for each type of profile, and the last for IPsec Settings. Go to the tab for your active profile (e.g. the Public Profile tab), and there are two settings of particular interest to us which are not available in the basic Windows Firewall settings:

Outbound Connections: The Windows Firewall blocks inbound connections by default, only allowing programs on the Exceptions list to go through. All outbound connections are allowed by default, however here you can also block them from your PC by selecting Block from the drop down list and clicking the Apply button at the bottom of the screen. I don't recommend doing this unless you genuinely feel at risk and want tight security.

Logging: By default the Windows Firewall does not keep a log of successful or denied connection attempts through the Firewall. If you wish to enable logging, for example to troubleshoot a problem or to see if there is any suspicious activity, then click the Customize button next to the Logging option and set the details of where and what to log here.

Importantly, if outbound connections blocking is enabled, you will not be able to access the Internet or another Network through your browser or most any other means as any connection attempts you make will be blocked without warning. This is why Vista does not have outbound connection blocking on by default, as it requires additional configuration to work. To allow an Exception to outbound connections, you will need to go to the main 'Windows Firewall with Advanced Security' screen and click the 'Outbound Rules' link in the left pane. Now click the 'New Rule' link in the right pane and a Rule Wizard will open, walking you through the steps necessary to add a particular program or port to the Exceptions list for example, and hence allow it to send data through the Windows Firewall. For example you may wish to add your Internet browser to the exceptions, as well as any online games, and any malware scanners which update via an Internet connection.

Again, it is not recommended that the average user block outbound connections under normal circumstances. It should only be enabled if you are willing to spend the time configuring it, and you genuinely feel you need this level of security. It might be useful however to temporarily block all outbound connections for example if you believe you are already infected with a serious piece of spyware or trojan, as this will prevent it from sending any information out of your machine until you can find and remove all traces of it.

< LOCAL SECURITY POLICY

One of the Administrative Tools provided to customize general Windows Vista security settings is the Local Security Policy tool. This can be accessed by going to Start>All Programs>Administrative Tools>Local Security Policy, or go to Start>Search Box, typing *secpol.msc* and pressing Enter. Note that this tool is not available in Vista Home Basic or Vista Home Premium. The main purpose for this tool is to allow Administrators to be able to impose certain limitations on other users of the same machine or network, so many of the settings are not relevant to the average home PC user and won't be covered here. Furthermore some options have already been covered - namely the Advanced Firewall settings and the User Account Control-related settings under the relevant sections above.

Copyright © 2010 Koroush Ghazi

For our purposes though, the Account Policies and Local Policies categories contain several settings which are useful in customizing the level of security on your system. To access and change a setting, click on the relevant category in the left pane, then find the setting in the right pane and double-click on it to alter it, or to see a more detailed explanation. Below are a range of useful settings you can alter, but please exercise caution and do not change anything if in doubt. To see the default option for each setting, click the Explain tab:

ACCOUNT POLICIES

Password Policy settings: These settings allow you to force passwords for User Accounts to be a certain length, age and complexity. In general you should not alter these settings unless you want tighter security, as they will create extra requirements for User Account passwords. For example by enabling the 'Passwords must meet complexity requirements' option, you will force all user passwords to meet the requirements detailed under the Explain tab whenever they change or create a password. This can cause problems with users remembering their own passwords. Importantly, you should not enable the 'Store passwords using reversible encryption' as it makes passwords easy to find since they will not be encrypted.

Account Lockout Policy settings: These settings control what happens when a user is locked out of their User Account for failing to enter a correct password. By default they can't be locked out, but if you wish you can set the number of times a user can try to login and fail before being locked out for a certain duration from using the account. This provides tighter security against users attempting to crack a User Account through repeated login attempts, and these settings should only be changed if you are in a less physically secure environment and untrusted individuals have access to your PC.

LOCAL POLICIES

Audit Policy settings: These settings allow you to enable a range of options for logging various events, viewable under Event Viewer - see the Performance Measurement & Diagnostics chapter. For example you can log the number of successful and failed logon attempts. These are useful for both troubleshooting purposes, and also if you suspect any unauthorized or unusual activity on your system.

User Rights Assignment settings: These settings determine the default user rights for system tasks such as creating a pagefile, or backup files and directories. These should not be altered unless you have an explicit need, as in every case there is a reason why particular users are restricted from conducting these tasks, namely to prevent a security breach or to prevent system instability or harm.

Security Options settings: These settings are the most useful in customizing Vista's security for the average home user. We've already looked at the User Account Control-related settings in the UAC section further above, so we will look at the rest of the more useful settings below:

- *Accounts: Administrator account status:* If Enabled, this option turns on the built-in Administrator account in Vista. This is the global Administrator account with the username 'Administrator' which is not obstructed by UAC and is not the same as the Administrator level account you created when first installing Vista. For more details see the User Accounts section of the Control Panel chapter.
- *Accounts: Guest account status:* Allows you to enable or disable the Guest account. For security reasons the Guest account should be kept disabled unless explicitly needed, such as when giving a person temporary restricted access to your PC.
- *Accounts: Rename Guest account:* If you've enabled the Guest account, this option allows you to rename the account to something other than 'Guest'. This is useful in making the Guest account more secure, as it is harder for others to guess the username for the account if it is not set to the default of 'Guest'.
- *Interactive Logon: Do not require CTRL+ALT+DEL:* If you disable this option it will require that a user press CTRL+ALT+DEL before being able to logon. This can increase security because it will mean

Copyright © 2010 Koroush Ghazi

users are entering their password in Secure Desktop mode, where no malware can interfere with or record their keystrokes.

§ *Shutdown: Clear virtual memory pagefile:* If enabled this option clears the virtual memory (stored in *pagefile.sys* - see the Memory Optimization chapter) each and every time you shut down the PC. While this can increase security since the pagefile may contain fragments of personal information, it can noticeably slow down shutdown time and is generally not recommended.

As noted several times before, be very careful with what you change here, as in general the defaults are perfectly fine for the average PC user, and some of the settings can cause problems for yourself or other users if changed. Think carefully about appropriately balancing security vs. convenience before enabling or disabling a setting.

< DATA EXECUTION PREVENTION

Data Execution Prevention (DEP) is a method that uses software and (where supported) hardware detection of programs that try to access and run code from designated 'non-executable' memory areas. In practice DEP protects against viruses that have become resident on the system and which then try running malicious code from such areas. When it detects an attempt to launch an executable from a non-executable memory area it will shut the program down and provide a notification that it has done so.

You can access the DEP settings by going to Control Panel>System and clicking the 'Advanced system settings' link in the left pane, or by going to Start>Search Box, typing *systempropertiesadvanced* and pressing Enter. Click the Settings button under the Performance section, and go to the 'Data Execution Prevention' tab.

By default when 'Turn on DEP for essential Windows programs and services only' is selected, DEP protection is only enabled for programs that choose to work with DEP, along with Windows system files. This is the minimum form of DEP protection and the one I recommend. For greater protection you can choose to extend DEP to all programs by selecting 'Turn on DEP for all programs and services except those I select' and then select which programs to manually exclude from DEP by using the Add or Remove buttons.

DEP is a valuable form of additional protection, and I strongly recommend that it be left enabled on its default setting. If for some reason you wish to completely disable DEP, such as to temporarily troubleshoot a problem to see if it is DEP-related, you can force DEP off in your boot options by using the BCDEdit command as follows:

1. Open an Administrator Command Prompt.
2. Type the following and press Enter:

```
bcdedit /set {current} nx AlwaysOff
```

3. You should see a confirmation that the operation was successful.
4. Reboot your system to implement the change.

Alternatively you can use a tool like VistaBoot Pro to toggle this option on or off more easily - see the Boot Configuration chapter for more details.

< STRUCTURED EXCEPTION HANDLING OVERWRITE PROTECTION

Structured Exception Handling Overwrite Protection (SEHOP) is a Vista feature introduced as of SP1, designed to protect applications from being exposed to exploits using the Structured Exception Handler overwrite technique. By default this feature is disabled, however Microsoft recommends that users enable it

Copyright © 2010 Koroush Ghazi

to provide enhanced security. The method for enabling this feature requires that you go to the following location in the Windows Registry:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\kernel]

DisableExceptionChainValidation=0
```

The DWORD above controls whether this feature is enabled or not. If it doesn't exist, create it, and set it =0 to enable SEHOP. If at any time you want to disable SEHOP again, you can set this value to =1.

Enabling SEHOP should have a negligible impact on performance, however it is known to cause issues with software that is based on Cygwin, Skype or Armadillo. If you experience any issues which you think are related to SEHOP, disable it, reboot and check your application(s) again to confirm whether SEHOP is the cause.

< KERNEL PATCH PROTECTION

Kernel Patch Protection, also known as PatchGuard, is a feature unique to recent 64-bit versions of Windows, including Windows Server 2003 SP1 x64, Windows XP x64, Windows 7 64-bit and Windows Vista 64-bit. This feature is not available under the 32-bit architecture at the moment, but it is possible to implement it for 32-bit operating systems in the future. Basically the feature protects the system Kernel - the core of the operating system - such that only Microsoft-certified changes can directly be made to memory locations holding the Kernel. This provides excellent protection against malware or any other software making unauthorized changes to the Kernel which can destabilize or compromise Windows. More details are provided in this Microsoft Article.

However Kernel Patch Protection requires that software developers ensure compatibility of their software with this feature. For this reason some older security or system-intrusive programs, as well as unsigned drivers will not work on Vista 64-bit.

You cannot disable PatchGuard, however you can manually override one of its key components - the check for digitally signed drivers during Windows bootup. A method to temporarily disable this check is under the Windows Drivers chapter, but there is no permanent way to disable it, as that would be a security hole and Microsoft frequently patches Windows to prevent any applications from doing so.

< ENCRYPTING FILE SYSTEM

The Encrypting File System (EFS) is the built-in file encryption protection method for Vista. It allows you to encrypt a file or folder such that it cannot be opened by anyone else unless they have the appropriate encryption key. To enable EFS for a file, follow these steps:

1. Open Windows Explorer and go to the file or folder you wish to encrypt.
2. Right-click on it and select Properties, and under the General tab click the Advanced button.
3. Tick the 'Encrypt contents to secure data' box and click OK, then click OK, and then click Apply.
4. You will be prompted firstly whether you want to apply the encryption to the file itself, or to its parent folder. It is best to encrypt an entire folder, so if necessary move all the files you wish to encrypt to a new folder and encrypt both the files and folders; otherwise just encrypt the file if you don't wish to move it.
5. The file will be shown in green text by default in Windows Explorer to indicate that it is encrypted.
6. You can remove encryption for your own files at any time by following the steps above and unticking the 'Encrypt contents to secure data' box instead, then clicking OK and Apply.

Copyright © 2010 Koroush Ghazi

To view details of the encryption, allow other users to use the file/folder, and more importantly to backup the encryption key for this file/folder, follow Steps 1 - 2 above, then click the Details button. Whenever you aren't using the file, it will be encrypted and thus secure against access by anyone else.

Note that EFS encryption is not available on Vista Home Basic or Home Premium editions - you can only decrypt encrypted files in those editions if firstly you have the encryption key for the file or folder, and then use the `Cipher` command - type `cipher /?` in a command prompt to see more details of this command. In general you shouldn't need to use encryption, and encryption is not a substitute for using secure passwords, UAC and other security-related measures. If someone logs in under your User Account they can access all encrypted material normally for example, so it is only one extra layer of protection.

< BITLOCKER DRIVE ENCRYPTION

BitLocker is an add-on feature of Windows Vista Ultimate and Enterprise editions. It is a drive encryption technology which secures an entire drive against unauthorized access, as opposed to the Encrypting File System (see above) which is used on a per-file or per-folder basis. However BitLocker can be used in conjunction with EFS, so the two are not mutually exclusive.

BitLocker is aimed primarily at providing protection in case of physical theft, using the Trusted Platform Module standard which requires hardware support. For the average home PC user I do not believe it is a necessary feature, and I will not go into detail about its functionality here. If you want more details of how to use this feature, see this Microsoft Article.

< ESSENTIAL ADDITIONAL SECURITY

Having examined Windows Vista's major built-in security features, it is obvious that security is very important in Vista. However Vista's security features, though more formidable than Windows XP, are still not sufficient on their own to protect you against all malware, nor do they pretend to be. They are important layers of defense against most of the common security threats, and provide the average user with a good starting point in preventing harm to their system. Yet there is more that needs to be done to provide genuinely good security. It is important to have additional layers of different types of protection so that even if several defenses are defeated, other layers exist to prevent or detect the malware before it does any serious harm. That's where the use of selected third party anti-malware scanners is absolutely critical to ensuring that your system is clean of malware and remains so, but I urge you to use them in conjunction with Windows security features, not instead of them, or vice versa.

In this section I provide detailed configuration advice for the recommended malware scanners which I personally use on my system. This will help give you a balance between security and convenience, with minimal performance impact. You may notice that I recommend disabling certain real-time protection and/or background functionality - this may seem risky at first glance, however there are two very important reasons for this:

§ Background functionality typically involves constantly scanning your data in an attempt to detect patterns which may indicate the presence of malware. This not only uses system resources such as CPU and memory, of greater significance is the fact that it can induce stuttering and reduce performance in a range of scenarios, particularly during gaming or when running drive-intensive applications.
§ Having background scanning/real-time protection functionality active on malware scanners can cause software conflicts which can result in the incorrect installation of software, as well as general system instability and crashes while running software. This is a known issue which many software developers specifically warn against in the documentation for their programs.

I strongly believe that there is no reason to slow down a system with intrusive malware scanning features when the best protection comes from a combination of a range of built-in Windows security features, user

Copyright © 2010 Koroush Ghazi

vigilance, and regular manual scans of your system. See the advice throughout this chapter, and the tips at the end of this chapter for more details.

If you disagree with my security philosophy, particularly if you are a user who feels that the trade-off between security and performance should favor security in your own circumstances then ignore my advice and use the default settings for each of these software packages. Just keep in mind that installing and enabling any malware scanning package on your system does not automatically mean that you are protected against malware. There is no simple automated fix to the problem of malware, otherwise it would have been defeated by now; instead malware is a bigger problem than ever. This is because prevention is always better than any potential cure, and that comes from user education and awareness, not a reliance on a range of automated tools. Unfortunately user education requires user effort, whereas the relatively ignorance of total reliance on automated tools requires minimal user effort, so obviously most users opt for the easy way out. I encourage you not to be such a user if you genuinely value your security.

Below is the essential free security software I recommend that you install and use in conjunction with the Windows features and advice covered in this chapter:

MALICIOUS SOFTWARE REMOVAL TOOL

To start with, regularly download and use the Malicious Software Removal Tool. This is a free Microsoft tool provided monthly through Windows Update, so as long as you keep up to date with Windows Update, it will automatically install and run itself when a new version is available. You can also download it from the link above and run it manually at any time, if you suspect an infection for example. Once it is downloaded and installed you can choose to do a Quick Scan or a Full Scan of your system for the most common viruses - a Quick Scan is sufficient if you also use another virus scanner. Note that the Malicious Software Removal Tool does not install itself permanently on your system and does not stay resident on your system, it simply runs a single scan each time it is downloaded from Windows Update, or if you manually download it and use it.

The tool is designed to detect the most common malware threats, but as the tool itself recommends, you will need dedicated anti-malware scanning software which can perform regular full scans of your system for a wide range of viruses, worms and other types of malware.

MICROSOFT SECURITY ESSENTIALS

I personally use and recommend Microsoft Security Essentials (MSE) as a dedicated all-purpose anti-malware scanner. It is a free and lightweight malware scanner which is very similar to Windows Defender, however it contains a much more powerful engine designed to scan for viruses, worms, trojans, adware and spyware, as well are other types of security threats. After you install MSE, it is recommended that you allow it to download the latest definitions through the Microsoft Update Center. One of the benefits of MSE is that it integrates neatly into Windows and upon installation the Windows Defender scanning functionality will automatically be disabled, so there is no duplication involved.

There are four main tabs under the main MSE window, and each is covered below:

Home: Displays your current security status:

- Green - Everything is fine, and MSE is using its recommended settings.
- Yellow - There may be a problem, usually due to outdated definition file, so you should go to the Update tab and allow MSE to update over the Internet.
- Red - A potential threat has been detected, or you have disabled one or more of the real-time protection components.

Copyright © 2010 Koroush Ghazi

Seeing a red status indicator simply because you have disabled one of the real-time protection components can be misleading, since this does not mean you are at any significant risk as long as you follow the rest of the advice in this chapter. However look closely, because if the red status indicator is accompanied by details of a potential threat being found, and the red button on the home page says 'Clean computer', then malware has been detected. Click the 'Clean computer' button to have MSE undertake the default action for that risk type. Remember that the default action for severe and high risk levels is deletion of the suspected infected file, so check first before clicking 'Clean computer' - see Default Actions below.

Also available here are the manual scanning options. You can select from a Quick scan, a Full scan, or a Custom scan. The Quick scan is the fastest, going through your important system files, folders and the Windows Registry to look for traces of malware. A Full scan goes through all your files and folders looking for malware, and hence takes longer and provides greater security. A Custom Scan allows you to select the specific drive(s) and/or folder(s) you wish to scan. I recommend running a Custom scan on any file you download or consider suspicious at any time. I also recommend running a Full scan at least once a week - whether scheduled or not is up to you - to ensure your system remains free from malware.

Update: Shows the current version and date for definition files. These files are what allow MSE to more accurately detect new malware, so you must keep MSE up to date by regularly clicking the Update button here, or by checking Windows Update for updates to MSE. I strongly recommend updating the definitions prior to launching a manual scan.

History: Shows any malware detected by MSE, as well as any programs or file types you have manually excluded from scanning in MSE. Note that if the 'Allow all users to view the full History results' is not ticked in the Advanced section of the Settings tab, each user will not be able to see results from other users, which can protect privacy. The Administrator can click the 'View details' button to see all details regardless.

Settings: MSE comes with a good default configuration, so beginner users in particular do not need to alter anything here. However I provide my recommendations for particular options below:

- Scheduled Scan - The default is a Quick scan 2:00am every Sunday, but I recommend changing this to a Full scan instead for greater security. Also make sure the 'Start the scheduled scan only when my computer is on but not in use' and the 'Check for the latest virus and spyware definitions before running a scheduled scan' boxes are both ticked.
- Default Actions - The default actions listed are essentially identical to those listed for Windows Defender, and are also described in this Microsoft Article. In short the 'Recommended Action' option is fine for each of these. However if the 'Apply recommended actions' box is ticked, MSE will automatically apply its recommended actions to your software - I strongly recommend against ticking this box to avoid seeing your software removed without your consent. For example, should a false positive occur and it is rated as a Severe risk, MSE will automatically delete the particular file(s). Alternatively, you can leave this box ticked, but for the Severe and High alert levels, you can change the default action to Quarantine to ensure there is no automatic file/program deletion.
- Real-time Protection - The options here allow you to determine which types of activities and areas MSE constantly monitors in the background to prevent malware from installing or executing on your system. The performance impact of having full real-time protection in MSE is minimal, and hence for novice users all these options are best left enabled. However for intermediate and advanced users I recommend leaving real-time protection enabled, but unticking the 'Scan programs that run on my computer' box, leaving the 'Scan downloaded files and attachments' box ticked. This should minimize the potential for performance issues and conflicts, because MSE will only scan a file or attachment which is downloaded, and will not constantly scan in the background during normal system usage. Note however that this setting will cause the MSE status to go red, which is no cause for alarm.
- Excluded Files and Folders, Excluded File Types - These two sections allow you to specify particular files, folders or file types which you don't want MSE to include as part of its scans. It is not

Copyright © 2010 Koroush Ghazi

recommended that you exclude anything from MSE's scans, as this may allow malware to slip past. However if you know for certain that a particular file, folder or file type is going to be picked up as a false positive (i.e. falsely detected as malware when it is not), then you can include it here.

§ Advanced - There several options here to further customize MSE's behavior. 'Scan archive files' if ticked allows MSE to scan inside archived files such as .ZIP, .CAB and .RAR archives - I recommend ticking this as malware can easily hide inside such files. 'Scan removable drives', if ticked, scans any removable drives such as USB flash drives when they are attached to the system - an extra form of protection, however ticking this may cause additional delays when you attach such drives, so untick it if this bothers you, but leave it ticked if you often connect removable drives from dubious sources. 'Create a system restore point' if ticked does precisely what it says: creates a new restore point for System Restore (if enabled) before taking any action against detected malware - I strongly recommend ticking this because it allows you to easily undo any system changes MSE makes which are undesirable. 'Allow all users to view the full History results' - I recommend ticking this, as it saves you having to click the 'View Details' button in the History section of MSE to see full details. You can untick this box if there are multiple users and you wish to protect each user's privacy, since infected filenames shown here may be something a user doesn't wish to have revealed.

§ Microsoft SpyNet - MSE uses anonymous information collected from your machine as part of the Basic Membership status for Microsoft SpyNet. If you have concerns, see the Privacy Statement for more details. It is precisely because of this information from such a large user base that MSE can provide such powerful malware detection functionality without resorting to more intrusive measures that other scanners do. An example of the type of information collected can be found in this Microsoft Article. If you wish to provide more advanced information, including some potentially personally identifiable information, select the 'Advanced Membership'. Microsoft has proven in the past that it takes the protection of user information very seriously, so the risk to users is not great, but ultimately if privacy is a concern, the Basic Membership option is fine. If you still have privacy concerns, then you may wish to use another anti-malware package altogether.

Click the 'Save changes' button when finished here.

Note that MSE also installs a new service called 'Microsoft Antimalware Service' (*MsMpEng.exe*) which is set to Automatic, and needs to remain that way for MSE to work properly. MSE also installs a new startup program 'Microsoft Security Essentials Interface' (*msseces.exe*) which triggers the launch of MSE at startup. You can disable this item however it will disable all real-time protection features until you manually launch MSE in a session, so it is best left to load at startup. Once running, MSE also places an icon in your Notification Area which you can click to quickly open MSE at any time.

Microsoft Security Essentials is a powerful anti-malware package which detects a range of malware, not just viruses. It provides a good balance between security and convenience, and integrates well into Windows Vista. It is extremely tempting to allow MSE to replace all the other anti-malware packages on your system. However this is not recommended for a single reason: should MSE not detect a piece of malware, or provide what might be a suspected false positive, the only way you can be certain is to run a scan using one or more other anti-malware package(s). For this reason, I recommend installing at least one dedicated trojan scanner, as well as a dedicated spyware scanner on your system, though the background functionality of neither should be enabled. See further below for details.

In any case MSE is not the only decent all-round anti-malware package. There is no consensus of opinion among security experts as to which particular package is the absolute best, but there are several other reputable scanners which are compatible with Windows Vista and which you can use instead, though some of them are only free for a trial period, or may take quite a bit of work in reining in their intrusiveness:

Copyright © 2010 Koroush Ghazi

AVG
Avast
Kaspersky
NOD32
Trend Micro AV

A-SQUARED FREE

Trojans differ from viruses in many ways, and are increasingly becoming more of a threat than viruses. Some trojans are not detected by all-purpose virus scanners, so you need a dedicated trojan scanner as well, if only to provide a second opinion. The built-in Windows Defender in Windows Vista does pick up some of the more common trojans, and Microsoft Security Essentials provides even greater defense against trojans. However I strongly advise installing a dedicated trojan scanner. I personally use and recommend A-Squared Free - it is one of the best free trojan scanners while also being the least intrusive. The following is information on how to set up the recommended A-Squared Free trojan scanner.

After installation of A-Squared Free, as long as you're running it under an Administrator account with full access privileges, you can set the new 'A-Squared Free Service' it installs to Disabled as it is not needed. If you then have any problems, you can set it to Manual if necessary.

On the main Security Status screen, click the 'Update Now' button to allow the program to download all the latest updates it requires - I recommend doing this each time before you do a manual scan. Fortunately the more intrusive aspects of A-Squared, such as 'Background Guard' background scanning, are not available in the free edition, so we do not need to configure/disable them. To set the depth of scanning used, click the 'Scan PC' option on the left of the main screen, and for normal usage select either Smart Scan or Deep Scan - I recommend Deep Scan which is longer but much more thorough. For more control over the scanning, select Custom Scan and click the Scan button - you will be taken to a screen which allows you to configure individual scanning options. I recommend all options be ticked, with the exception of 'use extension filter' - unless you wish to manually exclude or include certain file types. Once you've set your chosen scanning method, whenever you want to run a scan using A-Squared, you need only click the 'Scan Now' button on the program's main screen.

Note that from time to time A-Squared may find software which it classifies as Riskware, but is not actually malware. Such software is not necessarily malicious, it just carries greater risk in usage if your system is compromised by malicious software. I recommend investigating cases of Riskware by scanning with other malware scanners first, then doing some research on Google. To disable detection of Riskware, go to the Scan PC screen, select 'Custom Scan' and you can untick the 'Alert Riskware that is often used by Malware' option.

A-Squared is best used as follows:

- To run a full scan of your system at least once a week.
- To run a quick Custom Scan of a particular folder whenever you download a file or save an email attachment.
- To run a full system scan if another malware scanner shows possible infection - this helps provide a valuable second opinion.

In most respects A-Squared is ideal because it doesn't use any system resources or need to run in the background, so you can launch it whenever it is required and conduct scans when necessary.

Copyright © 2010 Koroush Ghazi

SPYBOT SEARCH & DESTROY

A spyware/adware scanner will find and remove this common type of malware from your system. Windows Defender is the basic built-in Windows spyware scanner, and it will protect you against most forms of common spyware. If you've installed Microsoft Security Essentials, that takes over the role of Windows Defender to a greater extent. However for even greater security you can install and use at least one additional third party spyware/adware scanner. There are two main alternatives: Ad-Aware and Spybot Search & Destroy. Both are powerful, and both are nominally free. However Spybot is completely free and does not contain any prompts to upgrade to a paid version. Furthermore while both require some modification to reduce their intrusiveness, Spybot is much easier to configure to remove its intrusive aspects, so on balance I recommend Spybot. The following are my recommended settings for Spybot:

The most important configuration options for Spybot actually occur during the installation process. During installation of Spybot, you will be given the option to select the components it installs. I strongly recommend unticking everything that is available. If you wish to customize Spybot's appearance, the 'Skins to change appearance' option can also be ticked, and if you require multiple languages, the 'Additional languages' option should also be ticked. Otherwise everything else is unnecessary to the core functionality of Spybot, and will only increase its resource usage if selected.

Furthermore, a few steps later in the installation procedure you will be asked to select common tasks for Spybot. Under the 'permanent protection' section I strongly recommend unticking the 'Use Internet Explorer protection (SDHelper)' option, which is a form of additional protection Spybot integrates into Internet Explorer and hence a level of undesirable intrusiveness and a background process which is unnecessary. Similarly, the 'Use system settings protection (Tea Timer)' option is a real-time protection functionality which always runs in the background if enabled, and as discussed earlier, is not desirable.

As long as you follow all of the steps above, Spybot will not install any additional services or startup items.

Once Spybot commences, you will be given a message regarding advertisement robots - this is simply a warning that if you use Spybot to remove certain advertising features from specific programs, the programs may not function correctly. You will then be prompted to backup your registry. You can do this if you wish, but it is not necessary and best done later as covered in the Backup & Recovery and Windows Registry chapters. Click the green next arrow to skip this step, and click the 'Start using this program' button.

To start with, click the Update button, select an update server closest to you, then I recommend making sure that you deselect any updates relating to disabled functionality, like the TeaTimer. Click Download and Spybot will update its definitions, then Exit the update box when done. Make sure to update Spybot before every manual scan.

To run a full manual scan, click the 'Search & Destroy' button in the left pane, and in the right pane select the 'Check for problems' button - if necessary click the 'Hide permanently' button to remove the tips box and allow you to see the list of potential problems found. If problem(s) are found and listed, you can highlight a particular item and select the 'Fix selected problem' button - red entries are relatively important spyware issues that should be fixed, while green problems are less harmful, although they can be fixed if desired. Check the additional information and/or search Google if you aren't certain. If anything is removed and later you wish to undo the change, you can click the Recovery item in the left pane.

To access the advanced and more detailed settings in Spybot, under the Mode menu select 'Advanced mode', however there are too many settings to cover here, and for most users there is no need to alter them unless you have specific requirements. Furthermore, I do not recommend the Immunize function, which attempts to block certain sites using your Hosts file. This function has caused conflicts and false positives in the past, and is unnecessary.

Copyright © 2010 Koroush Ghazi

Spybot is best used as follows:

§ To run a full scan of your system at least once a week.
§ To run a full system scan if another malware scanner shows possible infection - this helps provide a valuable second opinion.
§ Conversely, make sure to run another malware scanner if Spybot detects a problem, because spyware and adware detection can often exaggerate or misreport the level of potential threat.

Importantly there are a wide range of spyware, adware and other malware scanners which purport to remove malicious software, but ironically contain malware themselves, or are bad knock-offs of good scanners. Consult the lists below if you plan on installing any malware scanners other than the ones recommended in this book:

Spyware Warrior Suspect List
2-Spyware Corrupt List

Also conduct a thorough Google search to read user feedback and as many reviews as you can find on your chosen anti-malware package, as there are far too many new packages coming onto the market which are not just useless and intrusive, but deliberately malicious or designed to hold your system hostage with dubious reports of malware infection and then constantly prompt you to purchase the paid version to remove such non-existent infections. In other words a great deal of alleged anti-malware software is now being created with exactly the same aims as malware itself: for financial gain through malicious or fraudulent means.

PHISHING PROTECTION

Phishing is a form of deception which does not necessarily rely on any malicious software. Simply by tricking unsuspecting users into entering personal information into fake websites and falsified login screens, the originators of this form of online fraud obtain exactly the information they need to steal your money without having to go through any of the defenses built into Windows. Phishing is the age-old method of conning people taken to a new level through the use of technology. The main method for combating phishing is user vigilance. Fortunately there is some assistance, as the most popular Internet browsers - Internet Explorer, Firefox, Chrome and Opera - all have some form of phishing protection built into them, detecting reported phishing sites and warning users of the potential dangers of visiting such sites.

In Internet Explorer the Phishing Filter is enabled by default and will warn you if it suspects that a site you are about to visit is fraudulent. I do not recommend disabling it - see the Internet Explorer chapter for more details. The Phishing Protection feature in Firefox is covered in more detail in the Firefox Tweak Guide, and once again it is strongly recommended that you do not disable this functionality. Chrome's anti-Phishing features are detailed in Chrome Help, and protect against phishing and malware, thus should be kept enabled. More details of Opera's Fraud Protection features are in this Opera FAQ and it too is best kept enabled.

Even the most advanced user can fall prey to phishing, either due to laziness or simply because some fraudulent sites and techniques are becoming so realistic that they can fool almost anyone. For various practices designed to prevent falling victim to phishing and malware see the Important Security Tips section at the end of this chapter.

FIREWALLS

The built-in Windows Firewall is completely sufficient in protecting against network intrusion. By default it prevents external intruders from accessing your system, as long as you do not manually open lots of Ports and/or have lots of program Exceptions. It can also be configured further if required, but this functionality is

Copyright © 2010 Koroush Ghazi

best suited to more advanced users. In short the Windows Firewall provides a good balance of security and convenience, while still providing full customization options for advanced purposes should they be needed.

However you do have other options if you want greater security. There are several commercial Firewall packages you can turn to. For free alternatives, ZoneAlarm and Comodo provide two popular software firewalls for those who want to use a third party package. Note that your network device, such as a router or modem, may come with a hardware firewall which you can configure - see your manufacturer's site or your product's packaging for documentation. A combination of a software firewall like Windows Firewall, and the hardware firewall capabilities of most routers and modems, is totally sufficient to prevent the majority of unauthorized intrusions into your system, without crippling normal functionality on your system.

< IMPORTANT SECURITY TIPS

All of Windows Vista's built-in security features, and all the malware scanners and phishing protection in the world are no substitute for learning how to prevent malware infestation, and how to detect and avoid phishing and other forms of online fraud. Prevention is indeed much better than the cure, especially in the case of malware, because once your system is infected, and once your credit card details, login passwords, software serial numbers, personal documents and so forth have been compromised, then it is usually too late. Often times the infection may quietly spread to your backups as well, rendering them useless, so a simple reformat and reinstall of Windows may not rid you of the malware. Furthermore certain malware and exploits are so new that no malware scanner or known method can detect or block them, at least for a period of time, so you must learn other ways of preventing their entry into your system, and detecting their possible presence.

This is why it is so important that you read and understand the information in this chapter, and throughout this book. In particular, the tips I provide below are lengthy, but can be just as valuable as any anti-malware feature or software. This advice has stood me in good stead for many years, steering me clear of malware infection and the loss of personal data or money, while at the same time allowing me to enjoy all the features of my PC and full use of the Internet without reducing my system performance in any way.

MALWARE AVOIDANCE METHODS

Below are a range of general rules for helping you avoid becoming victim to malware and online fraud. Of course I could write a thousand rules, and none of them could cover every single type of circumstance. But the rules below do provide a strong basis for warding off the bulk of malware, and set you on the right course for coming to intuitively understand how malware works:

Address Book/Contacts: Don't keep any contacts in your email address book/contacts list. If you are infected with malware, this is one of the first methods it will use to distribute itself to all of your contacts, and since the email comes from someone they know, they are more likely to click a link or open an infected attachment. Instead save at least one email you receive from people you wish to contact regularly in a separate mail folder. Then whenever you want to email someone, open this folder and reply to their last email, clearing the existing contents and subject line before entering your text.

Stay Up to Date: Regularly keep your system up-to-date in terms of Windows patches and security updates, definition files for malware scanners, and the latest versions of your installed programs. These updates often contain fixes for known security exploits and vulnerabilities, and are a simple but effective way to prevent infection. Don't wait until you suspect infection before updating your system, as by then it may be too late, since some malware deliberately blocks the use of certain updating features.

Attachments and Downloads: A common methods for spreading malware is through infected email attachments and file downloads. Different file types can hold or trigger malware on your system depending on your settings. Any email attachment or download link should be viewed as a potential source of

Copyright © 2010 Koroush Ghazi

malware, even if it is from a known source, because even if the sender/host is not deliberately malicious, they could be infected themselves and hence accidentally spreading infected files. Only save attachments from trusted people, and always scan any saved attachments with malware scanners.

Patches & Security Updates: If you receive an email with an update or security patch for a software package or Windows attached, do not use it. Furthermore any links to such updates or patches are likely also fraudulent. No reputable software company publicly distributes updates or patches via email, they are always hosted on the company's site. If unsure, use a bookmark or manually type the legitimate company's web address into your browser and check for any updates or patches that way.

Unknown Sender: If you receive an email or message from someone you don't know, this is instant cause for suspicion. The vast majority of message from unknown individuals are spam, malicious and/or fraudulent.

Too Good to be True: If you receive a message or see an online offer which seems too good to be true, then almost without exception, it is likely to be a scam or a form of malware. It may not be malicious, it might simply be a hoax or a chain letter, but in virtually every case, it is worth deleting.

Spelling and Grammar Oddities: A dead giveaway that something is potentially malicious or spam/scam is the presence of bad spelling/grammar. This is not necessarily due to the author being foreign; the use of misspellings of common words, or symbols and other characters in place of standard letters, is a tactic designed to circumvent keywords in spam filters.

Replying or Unsubscribing: There is a large online market for email lists used by spammers and malware distributors. These people place a particularly high value on email addresses where the recipient is known to still check their email, as opposed to a false or long-dead email account. One way they verify an email address is with a phony 'Click here to unsubscribe' or similar link. Worse still, some of these links take you to a phishing site or download malware when clicked. For similar reasons never reply to any such emails - spammers know full-well that they cause annoyance, so abusing them is pointless; replying simply lets them know your account is active.

IP Addresses: Any link starting with a series of numbers instead of a domain name should be viewed with extreme suspicion. For example http://74.125.45.100/ tells you absolutely nothing about the site (actually it's Google). In most cases the IP address is used instead of a domain name precisely to hide the true nature of the site.

Backups: The need for regular backups has been covered in detail in the Backup & Recovery chapter. However malware also provides another important aspect to consider - you should always do a full malware scan of your system before creating any backups, and never backup if you suspect you are infected, otherwise you may wind up infecting your backups and rendering them useless.

File Sharing: One of the biggest sources of malware infestation in recent times is file sharing, such as via torrents, usenet, FTP, IRC or web-based file sharing services. Many shared files are fakes containing malware, but equally, genuine files can also contain malware, especially in any 'key generators' or associated utilities or links allegedly designed to unlock the shared files. Legality aside, file sharing is very risky and one of the easiest ways of being infected with malware. Malware distributors are increasingly innovating in this area due to the surging popularity of file sharing.

Address Check: If a particular email or website appears suspicious, check the address closely. Often times the address of an apparently well-known site can be easily spotted as false if you pay attention. For example the addresses http://www.amazon.shop.com and http://webstore.us/amazon.com/ have nothing to do with the reputable online store http://www.amazon.com. Similarly, the address http://www.facebook.com.users.org has no relationship with the social networking site http://www.facebook.com A domain name is always read

Copyright © 2010 Koroush Ghazi

from right to left before the first single slash (/) mark. The first component of an address when read from right to left is the Top Level Domain (TLD) found in the main site name, such as .com, .net, .co.uk and so forth. The real site name always appears just after the first incidence of a TLD when read from right to left. So in the example http://www.amazon.shop.com, the amazon portion of the address is just a sub-location of the website Shop.com. Scammers and even advertisers are very inventive, and create all sorts of variations on legitimate site names, sometimes with only a letter or two out of place, so in reality the only true way to be completely sure you are going to a correct site is to open a new tab or window in your browser and manually enter a known and trusted site address. You can also use your bookmarks, but always check the address of the site which opens.

Browser Security Check: For any secure transaction, the link which appears in your address bar must contain *https://* at the start, not just *http://* - note the addition of the 's' in the first link, which indicates it is a secure web link. Do not enter any financial information on a site which doesn't start with https://. However the level of security provided by a secure https:// link can vary, so by itself this is not a guarantee that your transaction is completely secure. Your browser will usually give you some indication or warning about the level of security, and this should be combined with research on the site in question.

Link Check: Even if a link on a web page or email appears completely legitimate and correct, spoofing links is extremely easy. For example this link: http://www.google.com/ actually goes to my website www.tweakguides.com, not Google. The only way to safely tell where a link actually goes to, whether it is provided in an email or on a website, is to right-click on the link and select 'Copy shortcut' (or similar), and then paste it somewhere harmless (i.e. not in your browser address bar). For example you can paste it into a plain text document, or the search box of a web search engine like Google. Then look closely at the link to (a) see if it matches the original displayed text for the link - if it doesn't this instantly proves that the link was attempting to be deceptive and hence is untrustworthy; and (b) to see the actual site it links to, which you can research further as covered below. With the rise of services such as Twitter, it has become fashionable for people to use short link services to generate URLs which are short but completely non-descriptive and hence potentially unsafe. For example this link http://bit.ly/dxdpT should point to www.tweakguides.com, but there is no possible way to determine that using any of the methods above. The only way to check such links is to use a service such as ExpandMyURL which allows you to paste in a short link and see where it goes.

Domain Check: If you believe a particular website may be untrustworthy, you can check to see who owns it and where they are located. A Google search on the site name is a start, but for more details, enter the domain name in a WHOIS lookup box at a domain registrar, such as the one provided here. In most cases this will provide sufficient details regarding the owner of the domain to help determine whether it is reputable or possibly malicious. Any site where the owner and/or administrator details are deliberately protected tends to greatly reduce its trustworthiness.

Financial Statement Check: If malware perpetrators gain access to your finances, they can sometimes be very cautious not to trigger any preset alarm points. Instead of withdrawing large sums of money which can arouse suspicion on both your part and the bank's, they can instead withdraw smaller irregular sums, or purchase normal goods and services online in an unpredictable and thus seemingly normal manner. The only way to detect this is if you regularly check your financial statements closely, making sure you can account for every transaction.

Browser Tools: If an untrusted website prompts you to install a particular plugin, program or toolbar to view or download their content, chances are this is malicious or at the very least undesirable. Cancel all such attempts. The most common software you require for full Internet multimedia functionality are the Flash, Shockwave and Silverlight players, as well as Java. You can install these safely by downloading the latest versions directly from their respective websites: ShockWave Player, Flash Player, SilverLight and Java. Only if a completely trusted and reputable website, such as Microsoft.com for example, asks you to install a

Copyright © 2010 Koroush Ghazi

browser plugin or download manager should you consider accepting, and if in any doubt, cancel and research further.

Intimate System Knowledge: One of the many benefits of becoming closely acquainted with your PC and the workings of Windows is that it allows you to spot odd behavior and unusual files and processes which most other users dismiss as normal. When properly configured and maintained, contrary to popular belief, Windows does not behave in an unpredictable manner, and your programs and games will not randomly crash. Therefore when strange things do begin to happen, such as unexpected program crashes or changes, your browser redirecting in odd ways, the system slowing down at times, or other unusual activity, you can spot it almost straight away and investigate. Using a range of tools, such as those covered throughout this book, you can then determine which processes and files are not normal for your system, and hence detect malware which may otherwise elude less knowledgeable users. Unfortunately there is no simple way to gain such knowledge, it takes time and patience, but there are many rewards for being familiar with the fundamentals of Windows and PCs.

Block Internet Access: If you strongly suspect a malware infection on your system, disable your Internet connection as soon as possible - if necessary update your malware scanner definition files first and run Windows Update before doing this. The quickest and most foolproof way to disable your Internet connection is to turn off your router/modem and/or unplug your cable or DSL line. The main reasons to do this is (a) to prevent the malware from spreading; (b) to prevent it from sending out any of your personal information; and (c) to prevent any hacker from accessing your system using any newly opened exploits or vulnerabilities. You can then use the Scan and Research methods below to track down the malware and remove it, and once you're confident your system is malware-free, reconnect to the Internet.

Scan for Malware: This is a somewhat obvious but necessary step. If you suspect a downloaded file or attachment of containing malware, or you believe your system is already infected with malware, then you must run a full manual scan using the scanners recommended earlier in this chapter. This is one of the reasons why I recommend several separate scanners, as running each one, one after the other, greatly increases your chances of successfully finding a variety of different malware types. Importantly, if you find your malware scanners are not launching or behaving oddly, or can't remove detected malware, then this is a sure sign that malware is resident on your system and blocking attempts to remove it. Reboot your system into Safe Mode and run your scans from there - see the Backup & Recovery chapter for details.

Common Sense: The simple application of common sense can provide an excellent method for detecting the validity of many forms of fraud or malware. For example if you receive an offer from a foreign king to place $18m into your bank account, but he needs your details first, then common sense would tell you it is ridiculous and highly risky. Similarly, a beautiful woman you don't know contacts you out of the blue to become friends with you. Or a close friend sends you an odd email with an uncharacteristic request and/or a suspicious attachment. All of these threats can be easily countered with the application of common sense, as none of them remotely pass even a simple sanity check. Yet every year, thousands of people fall victim to these scams. Don't allow your curiosity or base desires to overwhelm your common sense. At the same time, you cannot live in a constant state of complete paranoia - there are reputable sites and individuals whom you know you can trust, and cases where a quick rudimentary check is sufficient. Still, the adage *If there is doubt, there is no doubt* rings true: if you have even the slightest bit of suspicion, act on it by conducting further checks; don't take silly risks.

Research, Research, Research: This is the Golden Rule. You are not the only person in the world using the Internet or receiving emails, thus it is highly likely that you are not the first person to encounter a particular form of malware, fraud or related problem. This means that somewhere someone is quite likely to have posted about your problem, or similar symptoms, and furthermore, detailed sources of knowledge may already exist to help you determine the best course of action in an almost limitless range of scenarios. Everything from researching whether a particular website is potentially malicious, to the true nature and

Copyright © 2010 Koroush Ghazi

purpose of strange files on your system, to working out if a particular browser plugin is safe and actually necessary for certain functionality - the information is already there, you simply need to make use of it. Almost without fail I have always found sufficient information to determine virtually anything I need to know simply by using Google. Remember that knowledge is power.

BALANCING SECURITY VS. CONVENIENCE

In the past the balancing act between adequate security and convenience tended more towards convenience, since security threats were not as prominent, and even if you caught a virus, it was often just a harmless prank or at worst it ruined a few of your files. Unfortunately in the past few years there has been a significant rise in genuinely malicious software; namely software designed solely to do harm to your system and/or compromise your personal information. This coincides with the rise in the number of people who are using the Internet to pay bills, do their banking and go online shopping.

The stakes are much higher now, so no matter how advanced a user you believe yourself to be, it is incredibly important to pay attention to the security of your PC, and it will continue to become even more important in years to come as the malware creators and online fraudsters find increasingly more complex and intrusive ways of getting into your system. They make millions of dollars from undertaking this sort of activity, so they have every incentive to innovate. This is why Windows Vista's security features, which at first appear to be annoying - especially User Account Control - are actually very necessary and should not be disabled without careful consideration. You will most definitely need to do more than just install and enable a few anti-malware packages on your system to keep it secure.

The balancing act between security and convenience has now swung more towards security than purely convenience, so you must make some effort to keep your system secure, even if this can be a bit of a pain at times; it's simply unavoidable now. In this chapter I've provided what I believe is a good balance, especially for more performance-minded users. Rather than just suggest the use of background malware scanners which can hurt performance, I have recommended a combination of Windows' own built-in features and several trusted free third party tools used in minimalist but effective manner to create an excellent layer of defense with no real performance impact. Of course the most important theme throughout this entire chapter has been the need for user education and research, which as I've repeatedly stated, is the only genuine defense against malware and online fraud.

Copyright © 2010 Koroush Ghazi

MEMORY OPTIMIZATION

This chapter looks at the configuration and optimization of memory-related functionality on your system. It is very important to understand the basics of how your computer uses the various forms of memory on your system, including the way the Windows Memory Management system works. Memory-related hardware and software settings have a significant influence on your system's responsiveness and stability, not to mention your data integrity. A system with poorly configured memory-related settings risks slowing down, stuttering, becoming unstable, experiencing errors and sudden reboots, and ultimately causes data corruption.

< MEMORY HARDWARE

The following are the common forms of memory hardware used on most modern PCs:

CPU CACHE

The CPU Caches are small fast memory chips that cache (buffer) information for faster usage by the CPU, since the CPU is the central component of your system. They assist in temporarily storing the information in anticipation of reading/writing by the CPU, preventing any bottlenecks or slowdowns. There are usually several levels of CPU caches, Level 1 (L1), Level 2 (L2), Level 3 (L3) and so forth. The cache chips themselves vary in storage capacity depending on your CPU, but essentially they are physical chips that you should not have to worry about. Windows and your associated hardware are designed to automatically detect the size of these caches and use them optimally as long as you have them enabled in your BIOS. That is, if options relating to the use of CPU L1/L2/L3 Cache(s) are present in your BIOS, never disable them unless troubleshooting. Aside from BIOS settings, there is a `SecondLevelDataCache` Registry setting for attempting to manually adjusting your CPU's L2 Cache setting. However as with Windows XP, altering this setting is not necessary, as the default value of 0 already allows Windows Vista to automatically identify and use the correct L2 Cache size from the Hardware Abstraction Layer (HAL). This setting is therefore for older CPUs, such as pre-Pentium II models, which use direct-mapped L2 caches.

In general since the user has no control over the CPU's caches aside from ensuring that they are enabled in the BIOS, this is one area of the memory subset you should not worry about unless you are troubleshooting a memory-related problem. For example, a CPU with a faulty cache may exhibit strange behavior such as constantly returning data errors and CRC errors. In these cases you can try temporarily disabling the caches in the BIOS to see if this reduces or resolves errors.

PHYSICAL RAM

This is probably the most well-known and most important form of memory. RAM (Random Access Memory) is a temporary data storage area covered under the Memory section of the Basic PC Terminology chapter. The primary advantage of RAM over other forms of storage such as your hard drive is that it is much, much faster to access, so optimal RAM usage means smoother performance for your system. There are three main factors affecting RAM performance: RAM size, RAM speed and RAM timings, each covered below:

RAM Size: This is the actual storage capacity of the RAM in Megabytes (MB) or Gigabytes (GB). The main impact of having more RAM is that - when combined with appropriate Windows Memory Management settings - your system will perform more smoothly. This is because data has to be loaded less often from your drive, as more of it is stored in RAM, making it easier to access rapidly by your CPU and the rest of

Copyright © 2010 Koroush Ghazi

your system when required. RAM size is important in Windows because of the way it can utilize physical memory to speed up your system.

Vista Home Basic has a minimum RAM requirement of 512MB, and the higher versions of Vista require 1GB of RAM as a minimum. Furthermore many recent games and applications require 2GB or more of RAM to perform without stuttering or displaying frequent loading pauses. There are no RAM size tweaks; essentially if you have a low level of RAM (e.g. 512MB) then it is strongly recommended that you consider getting more RAM, especially if you constantly experience stuttering and long pauses in games or the Desktop for example. Bear in mind however that Vista 32-bit cannot practically use more than 4GB of RAM; only the 64-bit version can do that. So any more than 4GB of RAM is usually wasted in Vista 32-bit - see the Windows Memory Management section further below for details.

RAM Speed: This is the frequency at which RAM operates (in MHz), much like the speed at which a CPU operates. The higher the RAM's speed, the faster it can undertake the operations it needs to perform. Each stick of RAM has a speed rating, which is the speed up to which a stick of RAM is certified to safely operate. However the actual speed a RAM module is currently running at on a particular system varies depending on how fast it is set to operate in the BIOS. It is possible to adjust your BIOS such that the RAM can operate at a higher or lower speed in practice. The bottom line is, the faster the RAM's actual speed in MHz, the faster it reads and writes information and the better your performance. Remember though that the more the RAM's actual speed surpasses its advertised speed rating, the greater the chance for instability, so ideally you should keep the RAM at or below its rated speed for maximum stability and data integrity.

RAM Timings: These are composed of several variables, set in your BIOS, which determine not the frequency of the RAM module (i.e. the RAM speed), but the Latency of the RAM - that is, the amount of time it waits between updating various signals. For example the RAS (Row Access Strobe) and CAS (Column Access Strobe) latency settings measure in clock cycles the delay in sending signals which specify firstly the row in which a particular memory cell is located, and then the column. The lower the RAM timings, the less time the RAM rests between these operations, and hence the faster it performs, but the greater the chance for errors and instability. Just like speed ratings, RAM modules come with recommended timings already encoded in their Serial Presence Detect (SPD) on a special chip. These SPD settings are used by default by your system unless manually changed in the BIOS, and when used with the recommended speed rating (see above) ensure maximum stability.

To view all the details of your RAM, including current and maximum rated speeds and timings, use a utility like CPU-Z and check under its Memory and SPD tabs - see the System Specifications chapter for details. Also see the Overclocking chapter for more details on adjusting RAM speed and/or timings and the impacts this has. If you want to test your RAM for stability, see the Windows Memory Diagnostic Tool under the Performance Measurement & Diagnostics chapter.

VIDEO RAM

Video RAM (VRAM) is the physical memory built into a graphics card, and the size of this is usually quoted in MB or GB as part of the graphics card's specifications (e.g. GeForce GTX 285 1GB). This RAM acts as a temporary storage location to hold graphics data for faster access by your graphics card, much the same as system RAM does for general data. For this reason the VRAM is also called the Frame Buffer, in that it holds (buffers) individual graphics 'frames' ready to send to your monitor one by one. Just like physical RAM, VRAM has a speed in MHz, and latency in clock cycles, with the higher the speed and the lower the latency the better the graphics performance. Unlike physical RAM, altering the latency of your VRAM is tricky and not recommended, though still possible. The speed in MHz can be easily altered up or down using an overclocking utility, with the faster the speed the higher the performance, but once again the greater the chance of graphical glitches and freezes. See the Overclocking chapter for more details.

Copyright © 2010 Koroush Ghazi

If you're interested in a plain English step-by-step overview of how the memory features of your system are utilized for a system-intensive task like gaming, check the Graphics Process section of the Gamer's Graphics & Display Settings Guide for details.

< WINDOWS MEMORY MANAGEMENT

Windows Vista has implemented a different and improved form of memory management over Windows XP, and the results have caused some confusion. People look at their Vista memory usage statistics in Task Manager and are surprised to find that Vista is using a great deal of their system RAM, even immediately after system startup. The reason for this change is simple: Vista's is deliberately trying to make sure that as much of your RAM as is practically possible is utilized effectively via a feature called SuperFetch. There are many improvements to Windows Memory Management in Vista, and you can see a summary of them in this Wikipedia Article, but to summarize in plain English the changes include:

§ New features including SuperFetch which attempts to anticipate and preload information for quick access, and ReadyBoost which uses a connected USB flash drive to provide additional memory resources. Both are user-configurable and both are designed to increase system responsiveness.
§ Improved performance on 64-bit capable CPUs and multi-core CPUs.
§ Increased security to maintain data integrity and prevent memory exploits.
§ Registry virtualization to prevent system harm, and optimizations to prevent registry corruption.
§ Removal of various limitations which affected performance under Windows XP.
§ General performance improvements through optimizations in the way the memory management algorithms work.

Below we look at the important aspects of Vista's Memory Management system in more detail.

MAXIMUM SUPPORTED RAM

Before examining Vista's memory management features, it's important to understand that under Windows Vista 32-bit, any PC can normally only effectively use a maximum of 4GB of RAM; any higher won't be detected or used by default. In fact even with 4GB of RAM you may only see around 3GB of that displayed, because some of the 4GB of address space will be reserved by the system for certain hardware requirements, which in turn limits how much system RAM can be used at any time. However as of Vista SP1 if you have 4GB of RAM installed you should see this correctly reported in a range of areas within Vista, as explained in this Microsoft Article.

The 4GB memory barrier itself is a normal limitation of the 32-bit architecture, not just Vista, and is detailed in this Microsoft Article. To force Windows Vista 32-bit to use 4GB or more of RAM, you need to enable a feature called Physical Address Extension (PAE), which can be done by opening an Administrator Command Prompt and typing the following:

```
BCDEdit /set PAE forceenable
```

Alternatively you can enable PAE using a utility like VistaBoot Pro - see the Boot Configuration chapter.

In general under the 32-bit platform there is not much to be gained by having more than 4GB of RAM, as it cannot be used as efficiently. Any single application or process under a 32-bit environment can't address more than 3GB, so for gaming purposes for example, more than 4GB is a waste. If you use or require larger amounts of RAM then the correct course of action is to install the 64-bit version of Windows Vista. Under Windows Vista 64-bit, the maximum supported RAM is 8GB for Vista Home Basic, 16GB for Vista Home Premium and 128GB for the Vista Business, Vista Enterprise and Vista Ultimate editions. This is because the 64-bit architecture is specifically designed to natively support such higher amounts of RAM without sacrificing efficiency.

Copyright © 2010 Koroush Ghazi

SUPERFETCH

SuperFetch is a cornerstone of Vista's memory management system, and is an evolution of the Windows Prefetcher in XP. It functions on the principle that 'Free RAM is wasted RAM', which is true in theory. For example if you have 2GB of physical RAM, and your system only uses 512MB of that at any time, rather than being efficient this is actually quite wasteful of the other 75% of your RAM which sits idle, drawing power but not helping to speed up the system in any way when it could otherwise do so. Rather than waiting for you to launch common tasks and programs and then loading the data into RAM, SuperFetch uses an intelligent prioritization scheme which over time tries to work out your usage patterns and anticipates what you will need and when. It will load portions of your most commonly used programs into and out of memory in advance, making the system feel more responsive on average. In effect this turns your RAM into one big cache to improve speed and responsiveness in Windows.

However this doesn't mean that SuperFetch will keep filling RAM until you run out of memory and slow the whole system down. For starters Vista has a feature called Resource Exhaustion Prevention (covered further below) which specifically attempts to prevent the system from becoming slow due to a lack of memory resources, with or without SuperFetch. Secondly, SuperFetch's caching method is designed to be adaptive, so programs you use less often or which are a lower priority than those you are currently using will be shifted out of RAM to make room for whatever the current top priority program is, allowing your system to remain responsive. For example if you suddenly launch a program which requires most of the memory, such as a game, SuperFetch will instantly free up as much memory as is required. For the most part this actually works well in practice, with no noticeable performance impact as SuperFetch reallocates resources almost instantly. Any program which needs memory gets it; SuperFetch does not prevent that.

The most noticeable negative impact of SuperFetch occurs right after Vista has booted up - you may notice a fair bit of additional drive activity as SuperFetch begins to cache as much information as it can into RAM. In fact any time you free up memory resources, either by removing unnecessary background programs, or by closing an open application for example, SuperFetch will immediately attempt to cache more into memory and this can churn the drive for a short while. Rarely does this impact on performance, but it is wise not to launch a game or major application immediately after system startup - allow a minute or two for SuperFetch to do its job. As a tradeoff for this wait your most commonly used applications and games will load much faster and usually have less stuttering, because major portions of them have already been preloaded into memory.

You can see how much RAM is being used as a cache by SuperFetch at any time by opening Task Manager and under the Performance tab looking at the Cached and Free lines under the Physical Memory section; the main Memory graph display in Task Manager is actually the sum of memory resources used by running processes which is not the same as total RAM used. When SuperFetch is enabled your Free RAM will be minimal, often close to 0 as SuperFetch uses as much of it as is not directly in use by open processes for the Cached component. This is not something to be alarmed about - see the Task Manager section under the Performance Measurement & Diagnostics chapter for a full description of how to use Task Manager and understand what all of its components mean.

SuperFetch does a good job of handling memory in day-to-day situations, and can noticeably improve responsiveness in Vista. Application launch times can literally drop from a few seconds to a second or less, opening almost instantaneously in some cases, making your common tasks feel very snappy. SuperFetch needs time to analyze your usage patterns and adapt to them, and improves over time, so I recommend that you leave SuperFetch enabled for at least two weeks of daily Vista usage before judging the impact it can have on your machine.

If you still want to disable SuperFetch, to do so open the Services utility, double-click on the SuperFetch service and select Disabled - see the Services chapter for more details. Then you will also need to delete the contents of the *\Windows\Prefetch* directory. After a reboot SuperFetch will no longer be in use. Disabling

Copyright © 2010 Koroush Ghazi

SuperFetch may be the best course of action for those with 1GB or less of RAM. Note that if you do disable it, and then want to re-enable it, remember that it will take SuperFetch a while to get back up to speed in analyzing your usage patterns. Importantly, don't regularly 'clean out' the *\Windows\Prefetch* folder as this ruins SuperFetch's performance.

If you want to customize SuperFetch's behavior you can do so in the Windows Registry:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\
Memory Management\PrefetchParameters]

EnableSuperfetch=3
```

This DWORD value can be changed to a value of 0 to disable; 1 to prefetch boot processes; 2 to prefetch applications; and 3 for both. The default of 3 is recommended and generally should not be changed.

READYBOOST

Another feature introduced in Vista is ReadyBoost, which allows you to use external memory devices to speed your PC in conjunction with SuperFetch. You will require a USB flash drive or similarly fast removable media with 256MB of space or more. Connecting this device to your system will bring up a prompt asking if you want to 'Speed up my system'. Note that the prompt will not come up if you've disabled Autoplay for this type of device - see Autoplay under the Control Panel chapter. If you select this option, the device will now be configured for use by SuperFetch to hold information which would otherwise be cached out to your system drive; by placing it on the much faster flash drive, SuperFetch can access it much more quickly thus further improving system performance. The less RAM you have, the more you will see a benefit from ReadyBoost; however ReadyBoost is not a direct replacement for RAM, and any improvements may not be significant. It is best used by people who cannot upgrade their system RAM.

In the ReadyBoost dialog box which opens - or which can be accessed by going to Windows Explorer, right-clicking on the device, selecting Properties and then clicking the ReadyBoost tab - you can configure ReadyBoost. You can set the amount of the device's RAM ReadyBoost uses under the 'Space to reserve for system speed'. Windows will provide a recommendation of how much you should use as a minimum, and the general recommendation is based on around one to three times the amount of physical RAM on your PC. Note that the information on the ReadyBoost device is compressed and encrypted using 128-bit AES encryption, so if you misplace the device or it is stolen, others will not be able to access your information.

If you don't wish to use the device for ReadyBoost or wish to stop at any time, select ' Do not use this device' in the ReadyBoost box. Note that if you've disabled SuperFetch then ReadyBoost will have no impact.

READYBOOT

Not to be confused with ReadyBoost, ReadyBoot is another feature designed to use memory to optimize the boot process, but ReadyBoot uses normal system RAM to do this rather than an external device. After every bootup, ReadyBoot calculates a caching plan for the next boot and stores part of this information under the *\Windows\Prefetch\ReadyBoot* folder, and part in the Windows Registry. The end result is that each time you boot up Vista, ReadyBoot can improve boot times through use of this cache. After bootup the memory used for caching is automatically freed up after 90 seconds, or sooner if required.

Importantly, ReadyBoot relies on the ReadyBoost Service to function, so you should not disable this service even if you don't use ReadyBoost; it should be left at Automatic - see the Services chapter for details.

Copyright © 2010 Koroush Ghazi

RESOURCE EXHAUSTION PREVENTION

Part of Vista's built-in diagnostic features is Resource Exhaustion Prevention which automatically detects if any particular processes are consuming most of your memory resources. As resources come close to being depleted Vista may present a warning to the user indicating the particular program that is using too much memory, and provide the user with an option to close the program to prevent data loss through forced shutdown of processes. You can cancel out of this prompt if you know the program is supposed to take up all available memory, such as using a benchmarking utility that uses all available RAM by design.

The prompt usually appears when a program has a memory leak - that is, it is using ever-increasing amounts of memory resources as part of a fault within the program. Check for an update to the program in question which may fix this bug. If there is no such update or the program is not faulty, you should: reduce unnecessary background programs - see the Startup Programs and Services chapters; increase your Virtual Memory amount (see below); use ReadyBoost to add to the system's memory resources; or if all else fails then consider purchasing more RAM.

VIRTUAL MEMORY

Virtual Memory refers to a memory management technique used in several generations of Windows. During normal operation, system RAM is the best place to store information for fast access by your CPU and other components, since it has no moving parts and information in it can be accessed at many times the speed of any drive. So ideally Windows likes to keep a portion of all of your most commonly used programs in RAM, as well as most of your currently used application(s). There are also other memory requirements for the hardware and software on your system which all require some portion of memory resources.

When RAM starts to run low, or if Windows determines that a particular application is no longer a high enough priority, it breaks up some of the portions of memory (called 'pages') and temporarily swaps them out from your RAM to your drive. The 'swap file' where the memory pages are held on your drive is called *pagefile.sys*, and resides in the base directory on your drive. That's why you will often see the terms Virtual Memory, Pagefile and Swapfile being used interchangeably to refer to the same thing. Note you can only see the *pagefile.sys* file if the 'Hide Protected Operating System Files' option is unticked under Folder Options - see the Windows Explorer chapter.

Windows Memory Management techniques try to minimize reliance on your physical drive, since using it can cause stuttering or small delays and hence reduce responsiveness. However a Pagefile is still very important to Windows Memory Management and even with a great deal of RAM, is not something you should disable or consider redundant, as paging portions of processes to Virtual Memory is a necessary part of normal memory management. In the absence of Virtual Memory, your system may use more system RAM than is necessary.

Adjusting the Pagefile

To access your Virtual Memory settings, go to Control Panel>System and click the 'Advanced system settings' link. Alternatively go to Start>Search Box, type *systempropertiesadvanced* and press Enter. Under the main Advanced tab click the Settings button under Performance, and select the Advanced tab in the new box which opens. Click the Change button. Untick the 'Automatically manage paging file size for all drives' and you can now alter the physical location and size of the pagefile. Read the advice below before making any changes however:

Clearing the Pagefile: Before setting a new Pagefile size or location, you need to first clear your existing Pagefile. To do this select each relevant drive, choose the 'No paging file' option and click the Set button, then you need to reboot your system. This step does two things: first it clears the Pagefile, fixing any potential Pagefile corruption which can occur after a bad shutdown; and secondly it ensures that any new

Copyright © 2010 Koroush Ghazi

Pagefile you create will start off as a single unfragmented contiguous block on your drive for optimal performance, and should remain unfragmented in the future. Note that if you have any problems booting back up into Windows due to a lack of a Pagefile during this step, enter Windows in Safe Mode and continue the setup procedures for Virtual Memory from there - see the Backup & Recovery chapter.

Location of the Pagefile: Highlight the logical drive where you want the pagefile to be placed under the Drive window. Which drive(s) or partition(s) the pagefile should be located on is based loosely on the following scenarios:

- 1 Drive with 1 Partition - The pagefile can only be located on the first primary partition of your drive, which provides optimal performance. Do not create a new partition for the Pagefile.
- 1 Drive with 2 or more Partitions - Make sure the Pagefile is placed on the first primary partition as this is the fastest partition on hard drives; on SSDs it makes no difference which partition is chosen. Placing the Pagefile on another partition of the same drive does not provide any performance benefits.
- 2 Drives or more (similar speeds) - If all your drives are similar in terms of their rated speed, you should put the main portion of the Pagefile on the drive that doesn't contain your Windows installation and applications/games, e.g. put it on a general data drive. If you've already separated your Windows installation from your applications/games, then place the Pagefile on the drive which doesn't contain your applications/games, even if this is the Windows drive. Alternatively you can experiment with splitting the Pagefile evenly by creating multiple smaller Pagefiles, one on each drive and this may improve overall performance.
- 2 Drives or more (different speeds) - If one drive is notably faster than the others (e.g. an SSD), you should put the main Pagefile on that drive, regardless of whether it is the system drive or not. This is particularly important if you have low system RAM, since the Pagefile will be accessed more often, and thus needs to be on the fastest drive. Note that for the purposes of creating a memory dump, you may need to retain a small Pagefile on your system drive regardless of where the main Pagefile is located.
- RAID Configuration - For striped RAID configurations such as RAID 0 or RAID 5, Windows sees these as a single large drive, hence you cannot actually choose which drive to place the Pagefile on; it will be split evenly across the drives, which is optimal. If you have a separate faster drive outside the RAID configuration, such as an SSD vs. a pair of RAID hard drives, you may choose to shift the Pagefile there.

Microsoft does not recommend disabling the Pagefile if you have an SSD, indeed it is recommended that if you have the choice, you should place the pagefile on an SSD if available. Pagefile access primarily consists of reads, which will not have a significant detrimental impact on SSD lifespan, and the same rules to determining the Pagefile size as covered below apply to SSDs.

Pagefile Size: After selecting the location for the Pagefile, you can then determine its total size in MB. In the Virtual Memory settings screen select the 'Custom size' option. Although there are many differing opinions as to how big the Pagefile should be, it is important not to disable your Pagefile regardless of how much RAM you have. Windows need a Pagefile in order to operate correctly and efficiently. Setting the Pagefile to zero results in less efficient use of System RAM, and it also restricts the amount of memory resources your system can allocate should a program require more memory than you have in the form of available RAM. It also prevents memory dumps being created for debugging purposes after a crash.

By default Windows Vista sets your pagefile with a minimum size equal to System RAM + 300MB, and the maximum size at 3 times System RAM. So if you have 2GB of RAM, Vista will set a dynamic pagefile which starts off at 2.3GB and can go up to a maximum of 6GB. This default pagefile size is reasonable but not optimal. The correct size of the Pagefile is often debated, and there are many conflicting accounts of the optimal size. In the past I have provided what I have personally tested and found to be completely safe recommendations for the Pagefile size. However to remove all doubt and provide a concrete recommendation for this important system file, I now rely on the advice of the person best positioned on this

Copyright © 2010 Koroush Ghazi

topic with both practical and theoretical experience on the matter: Microsoft technical guru Mark Russinovich, as covered in this Microsoft Article.

Essentially, the correct method to determine the optimal Pagefile size for your particular system is to examine the maximum Commit Charge value for the combination of programs you frequently run at the same time. The Commit Charge is the amount of Virtual Memory reserved for a particular process. Compare this value to the current Commit Limit on your system, which is the sum of your system RAM + Pagefile. If the sum of Commit Charge for all your processes attempts to exceed the Commit Limit, then there will be memory allocation problems, potentially leading to crashes and even system failure. So the aim is to ensure that the peak value achieved for Commit Charge never exceeds the Commit Limit, which in turn tells us how big the Pagefile must be.

The way to determine your Peak Commit Charge and also see the Commit Limit is as follows:

1. Download and launch the free Process Explorer utility and keep it running in the background.
2. Use your system normally for a lengthy period, including loading up any and all programs you would normally use in a session, as well as any additional data. For example, load up your most strenuous games one by one and play them for a while. Or load up your largest applications and load any custom data you may be working on within those applications. The aim is to see the maximum amount of memory resources you might potentially use in any session in the future. Don't artificially load up a dozen applications at once if that's not what you would normally do.
3. Without restarting your system, after a period of time go to the View menu in Process Explorer and select System Information - a new window will open.
4. In the System Information window, examine the Commit Charge section - the Peak Commit Charge is shown, as well as the Commit Charge Limit. The Peak/Limit section also shows you how large a proportion of the Commit Limit the Peak Commit Charge came to being.

Using this data, you should then set the pagefile minimum size according to this formula:

Pagefile Minimum Size = Peak Commit Charge - Total System RAM

If the value for this is negative (i.e. you have more RAM than the Peak Commit Charge), this does not mean you should set a 0 Pagefile minimum size. Remember that a Pagefile is required for a range of reasons, so as a safe value for the Pagefile Minimum Size I recommend at least 1GB or the result of the formula above, whichever is higher.

The pagefile maximum size is then calculated as:

Pagefile Maximum Size = Up to 2 x Pagefile Minimum Size

Given your Commit Limit has already been set such that it meets your most strenuous requirements as per the Pagefile minimum, you should already have plenty of headroom even if you set your Pagefile Maximum Size to equal that of the Pagefile Minimum Size. However I recommend being safe and setting the maximum up to twice the minimum to provide even greater headroom, especially in case of unforeseen usage patterns, and to future-proof against upcoming applications and games which may use more memory. Note that there is a 4GB limit for maximum Pagefile size if running a 32-bit version of Windows Vista. You need to enable Physical Address Extension to remove this limit - see further above.

If you've spread the Pagefile over multiple drives, ensure that the sum of the Pagefile sizes equals the values above, or that the main Pagefile follows the above rules, and the other Pagefiles are all very small.

Once you've adjusted your Virtual Memory size settings click the Set button and reboot if required.

Copyright © 2010 Koroush Ghazi

A common point of confusion regarding Pagefile usage is the Paged and Nonpaged memory items in Kernel Memory section under the Performance tab of the Task Manager - these do not monitor Pagefile usage, they monitor areas of core Windows memory usage which can be paged if necessary or must remain unpaged. This is not the same as actual data in the Pagefile.

If you still insist on setting an extremely small or zero Pagefile, keep in mind that in some circumstances you may lose any unsaved work if Windows runs out of memory and does not have access to sufficient Virtual Memory.

The method for determining the Pagefile size in this section may seem tedious or confusing at first, in which case I strongly advise that you use the 'System managed size' option until you have the time to get a better understanding of it by reading the associated articles. As noted, the recommendation is fairly broad but it comes from one of the most reputable Microsoft experts available, so any other recommendations you find are unlikely to be as accurate. However keep in mind that the recommendation hinges solely on proper analysis of your Peak Commit Charge at a point in time. If over time you install and launch new programs and games which use much greater amounts of memory and/or you multitask with more programs than you originally envisioned, or load up data for your programs which are very large, then obviously there is greater likelihood that your Peak Commit Charge will rise, and you must therefore revisit your Pagefile size and go through the steps above again with more recent data.

If at any time the Resource Exhaustion Prevention prompt comes up, you should consider increasing your maximum Pagefile size. Having a larger Pagefile size does not hurt performance as such; it mainly takes up additional drive space, so if in doubt play it safe, or just revert back to the System Managed setting.

Note that you can set the Pagefile to be automatically erased each time you shutdown Windows if you have security concerns regarding the fragments of user information which may be stored there. This is an unnecessary measure for most users as it can slow down shutdown times noticeably, but if you require this level of security, see the Local Security Policy section of the PC Security chapter for details.

< UPGRADING MEMORY

There is no real substitute for having a decent amount of physical RAM installed on your system. All the advanced memory management features in Windows ultimately can't truly compensate for having too little RAM for the programs you choose to run. This is particularly true for gamers, as complex 3D games sometimes require large amounts of RAM to operate smoothly. Although the minimum requirement for RAM in Vista is 512MB for Home Basic, and 1GB for the other versions, I suggest a practical minimum of 2GB as a more realistic minimum for Vista. There's only so much Windows Memory Management can do when it's managing a scarce resource in such high demand.

Fortunately RAM is relatively cheap. A combination of purchasing more RAM and switching to using the 64-bit version of Windows Vista provides the simplest method of attaining smooth and responsive performance on your system. With increasing support from developers for 64-bit Windows, and with Vista's Windows Memory Management features, the RAM will be used efficiently to improve your Windows experience noticeably.

Copyright © 2010 Koroush Ghazi

DRIVE OPTIMIZATION

Windows Memory Management is intimately related to the way your drive(s) are used in Windows. Your drive is one of the relatively slower components of your system - even the fastest Hard Disk Drive (HDD) or Solid State Drive (SDD) cannot access, read or write data as quickly as RAM. So when one of your components such as the CPU or graphics card needs information, to prevent pauses, stuttering or slowdowns, Windows attempts to hold as much of the information as possible in RAM for fast access. However regardless of how much RAM you have, or how efficient Windows is with memory management, at the end of the day RAM is only a temporary form of storage which is cleared each time your PC shuts down. Therefore it is the physical drive(s) where all your information is permanently held, and your system must regularly access the drive for data. This chapter looks at how the how drives are used in Windows, and examines how you can make sure that this usage is optimal for your particular hardware configuration.

< WINDOWS I/O MANAGEMENT

To deal with the potential bottleneck that the drive represents on modern systems, Vista has an improved Input/Output (I/O) System. Windows prioritizes the allocation of drive read and write tasks by your various programs. Multiple applications running on a system at the same time can put great demands on your drive, which may struggle to smoothly supply all the data required. For example you may be using Windows Media Player to listen to music or watch a movie while a malware scanner is doing a full scan; or you may be playing a game while a disk defragmenter attempts to run a scheduled job in the background; or you may be downloading a file from the Internet while your system is encoding a large video file. If multiple tasks like these are not handled properly by Windows, the end result is significant stuttering, long pauses or freezes and even data errors.

When you run multiple applications at once - called multitasking - Vista initially prioritizes applications based on how much CPU time they need. This is not I/O prioritization, this is the management of separate program 'threads' which are competing to get access to the CPU so they can complete their tasks. Vista prioritizes these threads such that the important ones receive more overall CPU time if they require it. The six broad priority categories for CPU Priority from highest to lowest are: Real Time, High, Above Normal, Normal, Below Normal and Low. They can be viewed and manually altered using Task Manager - see the Task Manager section of the Performance Measurement & Diagnostics chapter for details. Note also that multitasking is where having a multi-core CPU is of most benefit, as any time you run multiple programs at once, the separate threads are split across your CPU cores and thus completed faster.

Having allocated a priority for CPU time, Vista then determines the relative priority of applications for drive time, or in other words I/O Prioritization. Vista bases I/O Priority on four broad categories: Critical, High, Normal and Low. You cannot manually alter these, as they are determined by the application itself combined with Vista and how a user is currently using the system. The bottom line is that certain tasks will run at reduced speed or even cease altogether if the I/O resources are required by more important tasks; this is particularly important for gamers since games require total control of I/O resources for smooth gaming.

The practical impacts of this I/O Prioritization scheme are that firstly less critical tasks such as scheduled Windows Defender scans, the Windows Disk Defragmenter or SuperFetch will not cause the system to become unresponsive. In fact Vista will suspend certain tasks altogether if a more important task is being undertaken, like playing a game or using a program. So the background Search Indexer function for example will not suddenly conflict with whatever else you are doing; it will only run when the system is relatively idle, and the speed with which it runs will vary to maintain system responsiveness at all times. Vista also specifically reserves drive bandwidth for certain tasks which specifically need a consistent flow of data,

Copyright © 2010 Koroush Ghazi

especially multimedia applications, so that these are not disrupted. Thus it is possible to run the Disk Defragmenter while also listening to music on Windows Media Player without glitches occurring for example.

However the actual impact of multiple tasks running at once on your system will vary depending on a range of factors, particularly your drive speed and the amount of RAM you have. The slower your drive and/or the less RAM you have and/or the more applications you try to run at once, the greater the likelihood that no matter how hard Windows tries, it won't be able to prevent some slowdowns or stuttering. In that case clearly you should try to reduce the number of things you're doing at once. Windows I/O prioritization cannot work miracles, so to minimize stuttering issues when running system-intensive programs such as games, I recommend that you still close down all other open applications.

As a final note related to I/O Prioritization, Vista also ensures that when you want to undertake a file copy or move, such as moving several large files from one drive to another, it checks first to ensure the resources are available and the task can be completed without problems before it undertakes the actual drive-intensive job of moving files. This prevents the situation where you reach halfway through a file copy or move only to have the task exit due to an error of some kind.

READYDRIVE

ReadyDrive is a feature of Vista specifically designed to take advantage of a Hybrid Hard Disk Drive (H-HDD) when combined with SuperFetch. Hybrid hard drives are composed of a traditional hard drive combined with onboard flash memory which acts as a high-performance cache for the drive. This cache reduces the actual usage of the drive mechanism itself, in turn saving power and increasing read and write speeds for common tasks. The larger the cache size, the greater the benefit, with the minimum supported size being 50MB, but a recommended minimum of at least 128MB is required for any noticeable advantage, and preferably 256MB - 1GB for a genuine performance advantage. The maximum cache possible for ReadyDrive is 2TB (TeraBytes), so it is not really limited in that respect.

Unless you have a Hybrid Drive connected to your system you will not be able to use this technology, and the most common use for this technology would be in notebook computers which would benefit the most from the reduction in power consumption. Note that if you disable SuperFetch you may reduce some of the speed benefits of ReadyDrive.

DISK DIAGNOSTICS

By hourly checking data from the your hard drives' Self Monitoring, Analysis, Reporting Technology (SMART) feature, Vista's built-in Disk Diagnostics can detect if there are going to be potential disk errors or a disk failure in the near future, and either take steps to rectify it or warn the user in advance, providing a set of steps to undertake to backup your data before it is potentially lost. Note that SMART must be enabled in your BIOS for this functionality to work, so if your drive(s) don't support SMART or it is disabled, Vista won't be able to check for disk problems automatically in this way. Note further that some drive setups such as RAID configurations may not allow SMART functionality.

If you want to manually check the SMART information yourself at any time to see your drive's health, use one of the methods below:

HD Tune: The free version of HD Tune has a Health tab under which you can see whether your drive has any problems.

PassMark: The free PassMark Disk Checkup utility shows SMART information for a drive by selecting that drive under the Physical Devices list in the tool, then checking under the SMART Info tab and looking at the Status column where everything should read OK.

Copyright © 2010 Koroush Ghazi

This feature is extremely useful, however you may not get sufficient warning of drive failure and/or the failure may be catastrophic enough to render some of your data unreadable when it first occurs, so Disk Diagnostics is not a replacement for making regular backups as covered in the Backup & Recovery chapter.

CHECK DISK

To check your drive for errors, such as bad sectors or corrupted indexes, you can run the Windows Check Disk utility. To access it follow these steps:

1. Go to the Computer category in Windows Explorer, or click on the Computer item in Start Menu.
2. Right-click on your drive name and select Properties.
3. Under the Tools tab, click the 'Check Now' button to launch Windows Check Disk.
4. To run a quick and basic error scan with Windows, untick both boxes and click the Start button.
5. To run a longer scan of the drive to find any bad sectors within Windows, tick only the 'Scan for and attempt recovery of bad sectors' box and click Start. This can take a while.
6. To run a thorough check and automatic repair procedure which requires restarting Windows, tick both boxes and click Start. Click the 'Schedule disk check' button and the next time you reboot Check Disk will run at startup. If it finds any problems it will try to fix them automatically.

I recommend you do a thorough check whenever you suspect drive-related problems as per Step 6, but even if you don't suspect any major problems, a periodic run of Check Disk using only the 'Automatically fix file system errors' option is relatively quick and detects and fixes any small errors before they develop into anything more serious.

< DRIVE CONTROLLERS

One of the key determinants of your drive performance is the type of drive controller it is using. The most common drive controllers are for the IDE and SATA interfaces, including the newer SATA II standard - see the Basic PC Terminology chapter for more details. To ensure that your controllers are set up correctly and configured for optimal performance in Windows, follow the steps below:

Make sure that you have installed the latest and correct motherboard drivers for your particular motherboard, as the drive controllers on your motherboard require these for optimal operation, as well as special functions like RAID - see the Driver Installation section of the Windows Drivers chapter for more details. Open Device Manager in the Windows Control Panel, and expand the Disk Drives section. Your drive(s) should all be listed here and correctly identified. If they are not, check your BIOS to ensure that you have enabled the relevant controllers and that the drives are being detected in the BIOS - see the BIOS & Hardware Management chapter. Now right-click on each drive and select Properties. Under the Policies tab, you will see some or all of the following options:

Optimize for: The 'Optimize for performance' option should be selected for maximum performance, unless you actually need to 'hot swap' drives regularly, that is to remove them quickly. Most desktop PC users will not remove their internal drives often. Note that if you see a 'Safely Remove Hardware' icon in your Notification Area, you should click it before disconnecting your drive. Furthermore this icon cannot be removed and is normal; you can only hide it - see the Taskbar and Start Menu section of the Control Panel chapter for details.

Enable Write Caching on the Disk: Write caching temporarily uses the drive cache to store writes to your drive before they are actually written to the drive. This allows the drive to write faster, since writing to cache is quicker than writing directly to the drive. However if there's a power failure, any data in the cache is lost before being committed to the drive. The risks are quite remote, so this option should be ticked for maximum performance.

Copyright © 2010 Koroush Ghazi

Enable Advanced Performance: This option further relies on the drive cache for reads and writes to improve performance, and again the risk is that if any there is any interruption to the power supply to your drive, or any hardware issues, you may lose or corrupt data. I believe the risk to be low, so I recommend ticking this option. If you don't have a steady power supply or a reliable drive then you may untick this just to be safe.

Next, go to the 'IDE ATA/ATAPI Controllers' or 'SCSI and RAID Controllers' section in Device Manager and expand it. Right-click on any sub-controllers listed, select Properties for each and see the relevant section below where applicable. The information below covers the most common options, however what you see on your system may vary depending on your motherboard drivers and hardware configuration - in some cases some of the options below may not be available:

IDE Channel / ATA Channel: This controller affects all PATA drives which use the IDE interface - typically this is older hard drives and optical drives, or SATA drives specifically configured to run in 'legacy' IDE emulation mode in the BIOS. Go to the 'Advanced Settings' tab and at the bottom make sure 'Enable DMA' is ticked for optimal performance. In the Devices box you will also see what mode any attached IDE drive(s) are running under. The maximum speeds which can be shown here are Ultra DMA Mode 4 for optical drives, and Ultra DMA Mode 6 for IDE drives. However your actual speeds may be even higher due to newer technology, so use a tool like HD Tune to check your actual drive mode under its Info tab.

You cannot alter the drive speed under the controller section here, but if it is below the maximum then it may be due to one or more of the following factors which you should troubleshoot:

- Check your motherboard manual for the various drive configuration details, and also make sure you have installed the correct drivers for this motherboard - see the Windows Drivers chapter.
- Your BIOS is not configured correctly to enable the highest speed - see the BIOS & Hardware Management chapter.
- You are sharing a hard drive or SSD with an optical drive on the same channel - move any optical drive(s) to a separate channel of their own.
- Your hardware doesn't physically support the highest transfer mode available. This should only be the case if the motherboard and/or the drive are quite old.
- No drive should be running in PIO or Multi-word DMA mode as these provide poor performance, so if this is the case, check your BIOS and any switches on the back of the drive(s).

Serial ATA Controller: This affects all drives connected to the SATA controllers on your motherboard. Right-click on this controller, select Properties, then go to the 'Primary Channel' and 'Secondary Channel' (or 'Port 0' and 'Port 1') tabs. If a drive is connected to these channels, the 'Transfer Mode' should show the correct maximum speed for the drive - 1.5GB/s for SATA I, or 3.0GB/s for SATA II. Alternatively click the 'Speed Test' button to do an actual quick benchmark of the drive's speed and see the speed rating. The 'Let BIOS select transfer mode' box should be ticked unless you are troubleshooting, or you see 'PIO Mode' for your hard drive, which is sub-optimal; in that case untick the box and manually attempt to switch to 'DMA Mode'.

Selecting IDE mode under the drive configuration in your BIOS is generally the best choice for most users, as it is the most compatible mode for SATA hard drives and SSDs while also providing excellent performance. However AHCI mode is native to SATA drives, and is covered below:

AHCI Mode: If you run a SATA-based drive, you can try enabling Advanced Host Controller Interface (AHCI) mode on your SATA controller in your BIOS. This mode has a range of benefits, especially on SATA II hard drives with NCQ support - this includes quieter operation and better multi-tasking capabilities. However it may or may not result in a speed boost. Furthermore it requires appropriate drivers from your motherboard manufacturer to function properly. Most importantly, if you do not enable this mode in your

Copyright © 2010 Koroush Ghazi

BIOS prior to installing Windows, you may experience an error and may not be able to boot back into your system if you switch to AHCI from IDE mode or vice versa on an existing install of Windows - see this Microsoft Article for details.

Note that some SSDs may not properly support AHCI, and indeed some SSD manufacturers do not recommend using AHCI mode due to potential performance issues, since NCQ is designed for drives with a physical drive head, not SSDs which are memory-based. However some users report increased speeds with AHCI enabled on their SSD, so it can still provide performance benefits if you are willing to experiment.

You can also select RAID mode in the BIOS, but this is only necessary if you have a RAID drive configuration - see the Windows Installation chapter for more details on RAID.

To test your drive's actual speeds at any time, you can run a drive benchmark such as HD Tune, or the drive benchmarking component of Sandra, or simply the built-in Windows Experience Index. Drive benchmarks can be quite artificial and not necessarily indicative of real-world performance, so they are best used simply to determine if your performance has improved or degraded, or to compare with other users of the same drive to check in case your performance is significantly lower and hence indicative of a potential problem. See the Performance Measurement & Diagnostics chapter for more details.

< MASTER FILE TABLE

The Master File Table is a system area of Windows which contains an entry for every file and directory on your drive with information on its size, attributes, permissions, timestamps and so forth. In a way, it is like a table of contents for your drive, and as such serves a very important function. Windows automatically manages the MFT, increasing its size as necessary. It initially reserves around 200 MB in drive space for the MFT to prevent fragmentation, and this allocation grows as required. If your drive is full, Windows allows your data to overwrite any reserved MFT space which is not actually being used by the MFT, so the space is not wasted.

If you want to manually control the amount of space Windows reserves for the MFT as it grows you can do so by going to the following location in the Registry:

```
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem]

NtfsMftZoneReservation=0
```

The DWORD above is set to 0 by default, which means it is automatically managed and will increase as required - this is recommended. However you can change the value above to be between 1 and 4 inclusive, which implements a multiplier for the MFT reservation, with 1=200MB, 2=400MB, 3=600MB, and 4=800MB. For example, if the above value is set to 4, the MFT reserved zone will rise in 800MB increments as required.

In Windows Vista the MFT is automatically managed and never needs any user input or adjustment. However it is important to regularly defragment hard drives (not SSDs) to ensure the MFT doesn't become fragmented over time and thus degrade drive performance.

Copyright © 2010 Koroush Ghazi

< WINDOWS DISK DEFRAGMENTER

As data is written to or deleted from your drive, portions of individual files will become fragmented and physically spread out all over the drive. This happens because as Windows starts writing the data for a file onto the drive, when it reaches an occupied portion of the drive it jumps to the next available empty spot and continues writing from there. So a single large file may actually be in several separate chunks in various locations on your drive. The more the files on your system are fragmented, and in particular the smaller the fragments, the more time your drive takes to find all these fragments and access all the information it needs at any time. It's like trying to read a book with the pages out of order. This can clearly reduce drive performance and increase the potential for stuttering and loading pauses on hard drives.

Windows Disk Defragmenter (Defrag) is a built-in utility that performs a very important function: it finds all these file fragments and puts them back together in the same location on the disk, preventing the degradation of your hard drive's performance. To access the Windows Defrag utility, go to Start>All Programs>Accessories>System Tools, or go to Start>Search Box, type *dfrgui* and press Enter. In Windows Vista the Defrag interface and functionality has changed from that under XP. Defrag is now designed primarily to be automated and by default runs on a weekly schedule, defragmenting your drive in the background at a low priority hence causing minimal disruption to system responsiveness. It does a good job of this, however unlike previous versions of the Defrag utility, there is no graphical progress indicator or otherwise, showing you how fragmented your drive is or how long the process may take. Microsoft claims that this is both because an accurate graphical representation of fragmentation, and progress towards completion of defragmentation, is difficult to provide, and that users do not understand or want to see such a display. If this aspect of the Windows Defrag tool bothers you, then see the Advanced Defragmentation section further below.

If you wish to change the scheduled times or frequency with which the automatic defragmentation occurs, click the 'Modify schedule' box and you can specify how often, on which particular day and at what time the process is initiated. If you wish to disable this scheduled defragmentation altogether then untick the 'Run on a schedule' box. Importantly, do not use a defragmenter on an SSD, because an SSD's random read times are extremely fast, counteracting any performance decreases due to fragmentation, not to mention that the act of defragmenting an SSD can reduce the lifespan of the drive. Disable scheduled defragmentation for your SSD and do not run Defrag on it.

For hard drive users you can leave the automated defragmentation schedule to run once a week, preferably at a time when you will not be playing a game or doing any other drive-intensive activity. Note that if you miss the scheduled time, such as your PC being off at that time, Vista will do it when next possible.

In practice however, defragmentation is best done immediately after you make major file changes to the drive, so I strongly recommend that you also do a manual defrag immediately after any of the following events:

§ Installation of any program, especially games or any drive-intensive applications such as benchmarks.
§ Patching any program or running Windows Update.
§ Installation of any drivers.
§ Adding or deleting large file(s) or folder(s) of any type.

Defragmentation is particularly necessary for gamers, since games are already quite prone to stuttering and longer loading times due to their data-intensive nature, so by defragmenting your drive after a game installation or after patching a game, you can significantly reduce any stuttering while playing the game.

To initiate a manual disk defragmentation at any time, first close as many applications as possible, then open Defrag and wait for it to analyze your hard drive if necessary. When complete click the 'Defragment now' button and it will start the defragmentation process straight away. Note that as of Vista SP1, the Windows

Copyright © 2010 Koroush Ghazi

Defrag utility also allows you to select specific drives to include or exclude for defragmentation by clicking the 'Select Volumes' button. Once defragmentation starts, as mentioned before, no indication will be given on how long it will take or how far it has progressed - it will continue until it indicates that it has finished. If you run any other program during this process, Vista will reduce the priority given to Defrag, which in turn will increase the time taken for process to complete, so try not to do anything else while Defrag is running.

If you want greater control and feedback from the Windows Disk Defragmenter, you can use the `Defrag` command line option in Vista. Start an Administrator Command Prompt and then type `Defrag /?` for a list of commands. Common commands are shown below:

```
Defrag [driveletter:] -a
```

e.g. `Defrag C: -a`

This will run an analysis and provide more detailed information on how fragmented your drive really is. To run a defrag on the specific drive with more detailed feedback, type:

```
Defrag [driveletter:] -v
```

By default the Defrag utility will not defragment file fragments larger than 64MB. If you want to do a more thorough defragmentation job for all sizes of file fragments, type:

```
Defrag [driveletter:] -v -w
```

Note that for defragmentation to work, you must have a reasonable amount of free space on the drive, preferably 15% or more. If you find that the Windows Disk Defragmenter does not provide you with sufficient control or feedback, then you will need to consider a third party disk defragmenter - these are covered below.

< ADVANCED DEFRAGMENTATION

If you want a graphical interface for your defragmentation utility, and also want it to do a more thorough defragmentation and maintenance of your hard drive you will have to look beyond the built-in Windows Disk Defragmenter. There are several applications which can defragment a disk in more efficient ways, and also defragment files which the Windows Defragmenter cannot move, such as system files. Note that the Windows pagefile will not become fragmented if configured correctly as detailed in this book - see the Memory Optimization chapter.

For utilities which are free, I recommend the following:

MyDefrag
Auslogics Disk Defrag

There are several commercial defragmentation packages which all have a free trial version you can use for a limited period, but ultimately require purchase for use beyond this period. Of these, I recommend:

Diskeeper
PerfectDisk
O&O Defrag

In general I don't see a pressing need to use a third party defragmentation tool in Windows Vista. The third party defragmentation packages above may provide marginally improved drive performance as a result of more advanced defragmentation or additional features, but this has to be balanced with the fact that the Windows Disk Defragmenter is free, fully integrated into Windows, and gives you the majority of the

Copyright © 2010 Koroush Ghazi

benefits of defragmentation. Furthermore, as traditional hard drives are being phased out in favor of much faster solutions like SSDs which don't require the use of a defragmentation utility, I don't believe it is a wise investment to purchase a third party defragmentation tool now. The money is better put towards eventually upgrading to an SSD instead.

In any case, regardless of whether you use the built-in defragmenter or a third party utility, make sure to defragment your hard drives regularly as it is essential to smooth hard drive performance.

Copyright © 2010 Koroush Ghazi

THE CONTROL PANEL

This section covers all the general options available under the default Windows Vista Control Panel, which is an important central location for accessing many of Vista's settings. I cannot go into each section of the Control Panel in great detail due to space considerations however all the important settings which are relevant to the average home PC user are covered here and where necessary you will be referred to the various relevant chapters of this book for more details. My recommendations for each option are safe to use on most systems unless you have special requirements. In any case, take the time to go through this section carefully as although it is long, it is very important for Vista's performance and functionality.

Importantly, it is assumed throughout this book that Windows Control Panel is being viewed using the 'Classic view' option, as this provides the most detail of all the different utilities and options available. Furthermore you may have additional items showing in your Control Panel, as some third-party programs will automatically insert shortcuts into the Control Panel, however only the default Windows Vista items are covered below. Only the default Windows Vista Control Panel components are covered in this chapter, though some editions of Vista may not have all the Control Panel items because particular features are not available in certain editions.

< CUSTOMIZING WINDOWS CONTROL PANEL

Third party applications can install Windows Control Panel items which may be undesirable, particularly as they can add clutter to the Control Panel. This section provides methods for finding and removing these components. These methods do not uninstall or otherwise harm the functionality associated with the components, they simply prevent the relevant components from being displayed in the Control Panel.

The easiest method to hide any Windows Control Panel item, whether a default Windows component or one installed by a third party program, is to use the Local Group Policy Editor - see the Hide Specific Control Panel Items tip in the Group Policy chapter.

However Local Group Policy Editor is only available in all versions of Vista, so if you do not have access to it, there are other methods for removing Control Panel items. Many third party applications install .CPL files which are small applications designed to run in the Windows Control Panel. Removing the relevant .CPL file will remove that component from Windows Control Panel. You can see a list of common third party .CPL files in this Wikipedia Article. You can find these .CPL files typically stored under the *\Windows\System32* folder, or in the program's own directories, or you can initiate a system-wide search for all .CPL files. Once the file is found, close the Windows Control Panel, temporarily delete the suspected .CPL file to the Recycle Bin, reopen Control Panel and if you removed the correct file the component should no longer be visible.

You can also check the Windows Registry for Windows Control Panel components. Go to the following locations in the registry:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Control
Panel\Cpls]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ControlPa
nel\NameSpace]
```

The keys and values located beneath the subfolders above contain entries which relate to Windows Control Panel components, both third party and default Windows components. However remember that deleting an entry in Registry Editor cannot be undone, so make sure you create a backup of the relevant branch and/or

Copyright © 2010 Koroush Ghazi

the entire registry as covered in the Backup & Restore and Windows Registry chapters before deleting anything. You may have to restart Windows or logoff and logon to see the changes made in the registry in the Windows Control Panel.

The remainder of this chapter covers the individual default Windows Control Panel components.

< ADD HARDWARE

This utility allows you to go through a set of procedures for adding a new piece of hardware to your system. In most cases though, since Windows Vista is a 'Plug and Play' operating system, and as long as you have 'Plug and Play' enabled in your BIOS and the 'Plug and Play' service set to Automatic, all you need to do to add any new hardware is to connect it to your system and Vista will automatically detect it and either install basic drivers for it, or if it can't determine the type of hardware, request that you insert a driver disk. See the BIOS & Hardware Management chapter for more details.

The main use for the Add Hardware function therefore is for adding non-Plug and Play hardware to the system. In these cases, Windows may not detect the device automatically, so firstly before adding any new piece of hardware, spend some time reading through the installation instructions which come with the hardware, as some have unique requirements for optimal installation which may be different to what you might expect, such as requiring special drivers to be installed first before connecting the device.

If there are no specific instructions, then connect the device and click Next in the Add Hardware Wizard, and first select the 'Search for and install the hardware automatically' then click Next. If the device isn't found and/or is not identified correctly, click Next and attempt to choose it from the list provided, or try to find a similar device from the same manufacturer.

< ADMINISTRATIVE TOOLS

The Administrative Tools are a range of utilities for advanced configuration and monitoring of the system. As their name suggests, they are designed for Administrators, so some of the utilities and functions are not useful to the average home PC user. However I provide details of the main Administrative Tools and point out their most useful aspects for the average user below:

COMPUTER MANAGEMENT

This utility provides access to a combination of several Administrative and system tools which are covered in other sections, including Event Viewer, Task Scheduler, Device Manager, Reliability and Performance and Services - see the relevant chapters of this book for more details on each of these.

The main use for the Computer Management tool is the Disk Management sub-component, which you can find under the Storage section in the left pane of Computer Management. Once you click on it you will then see your drive(s) listed in the top right pane, with all your available drives (including optical drives) listed in the bottom right pane. Some common tasks you can do with Disk Management include:

Changing Drive Letters: If you want to change any of the drive letters on your system - for example if you want to alter your DVD-ROM drive from being called D: to F: or change a hard drive letter from C: to J: you can do so here by right-clicking on the drive letter in the bottom right pane and selecting 'Change Drive Letter and Paths', then highlight the drive letter which appears, click the Change button and assign a new drive letter. Note that you cannot change system drive letters under some circumstances.

Partitioning: Vista allows more comprehensive partitioning options for drives. A Partition is a logical subdivision of your drive. To create a new partition on your current drive(s), you will need to have some Unallocated Space (which is not the same as free drive space). In most cases there will not be any since your

Copyright © 2010 Koroush Ghazi

existing partition(s) are likely taking up all allocated space. You can however create unallocated space by using the Shrink function which reduces one of your partitions and in return creates unallocated space. Once you have some unallocated space, you can right-click on it and select 'New Simple Volume' to create a new partition, and follow the Wizard to choose a size for it. You can also format an existing partition, which destroys all data currently on it and prepares it for use. If you want to create more than three partitions, you will have to create an Extended partition within an existing partition. For more details on partitions see the Partitioning section under the Windows Installation chapter.

Basic and Dynamic Disks: All your drives are formatted as a Basic disk with partition(s) as necessary. However if you wish, you can format them as a Dynamic Disk by right-clicking on the relevant drive and selecting 'Convert to Dynamic Disk'. Dynamic disks can emulate a RAID array - that is they can span multiple drives as though they are one large drive, and they do not use partitions. The features of Dynamic Disks are discussed in this Microsoft Article. It is generally not necessary nor recommended that you convert your disk from Basic to Dynamic for the average home PC user, and note that you cannot reverse the process without losing all your data, so it is not worth experimenting with. You should only use this option if you have specific needs which you know will require a Dynamic Disk, such as for holding very large databases. Note that this function is only available on Vista Ultimate and Enterprise editions.

DATA SOURCES (ODBC)

This tool lets you add and configure drivers for managing access to data on various database management systems. Unless you use databases extensively on your machine, you can ignore this tool as it is not relevant to the average home PC user, and won't be covered in this book.

EVENT VIEWER

The Event Viewer is a useful troubleshooting tool which shows a list of system events. These events are recorded by Windows over time, and reflect information alerts, warnings and errors that have occurred to date. Details of Event Viewer usage are provided in the relevant section of the Performance Measurement & Diagnostics chapter.

ISCSI INITIATOR

The iSCSI Initiator is a management interface for iSCSI devices. These devices can be disks, tapes or other storage components which are connected to your network. The iSCSI Initiator handles the connection and control of these target devices, thus is not relevant to the average home PC user as it is mainly used for remote storage over a network, and won't be covered in this book.

LOCAL SECURITY POLICY

This tool allows you to establish and alter security-related settings. The main purpose is to allow an Administrator to limit or control the usage rights of other user accounts on the system or a network. For more details see the relevant section of the PC Security chapter.

MEMORY DIAGNOSTICS TOOL

The Memory Diagnostics Tool is a troubleshooting utility designed to determine if your system memory (RAM) has any physical problems. Its functionality is covered in detail under the Performance Measurement & Diagnostics chapter.

PRINT MANAGEMENT

This tool allows you to manager print servers and printers connected to the PC. Full details of its usage are in this Microsoft Article.

Copyright © 2010 Koroush Ghazi

Reliability and Performance Monitor

This tool allows you to monitor the usage of major system resources, as well as seeing a graphical representation of system errors and failures. It is covered in detail under the Performance Measurement & Diagnostics chapter.

Services

This tool is extremely useful in configuring service usage under Windows Vista. See the Services chapter which explains its features in detail.

System Configuration

The Microsoft System Configuration tool is also known as MSConfig for short, and is covered in greater detail under the Boot Configuration, Startup Programs and Services chapters.

Task Scheduler

The Task Scheduler maintains all the existing scheduled tasks on the system, and also allows users to add custom tasks for future execution on a defined schedule. You can also access the Task Scheduler at any time by going to Start>Search Box, typing *taskschd.msc* and pressing Enter.

In the center of the main screen, you can view the recently executed tasks under the 'Task Status' box. You can choose the time period over which the tasks were performed in the box at the top right - the default is 'Last 24 hours'. Each listed task can be expanded to show when it was last run, and whether it was successful or not.

To view all currently running tasks, first go to the View option in the right pane, click it and select 'Show Hidden Tasks'. Then click the 'Display all running tasks' link in the right pane, and a box will open with the tasks listed - you can manually force any of these to end if you wish, though this is not recommended unless you are troubleshooting. You can customize the system tasks currently queued for execution by looking under the 'Active Tasks' section at the bottom of the main window. Double-clicking on a task provides a range of additional options for customizing the tasks. In general you should not alter tasks in this way, it is best to alter them through the actual program or Windows function first, and only come here if you need additional ways of customizing the task.

If you are looking for a particular task, such as the Windows Backup task, use the directory tree in the left pane, expand the top item and look under the Microsoft>Windows branch to see all the various applications and features. For Windows Backup the relevant subfolder is labeled WindowsBackup - click on it and all relevant tasks are shown in the middle box.

To add your own custom task, click the 'Create Basic Task' link in the right pane, and you will be presented with an automated Wizard which will step you through the process.

Task Scheduler can be turned off altogether by forcing the 'Task Scheduler' service in the Services utility to Disabled - see the Services chapter. This is not recommended as Task Scheduler is an important component and disabling it prevents any scheduled tasks from running, some of which have important diagnostic or system maintenance functions.

Windows Firewall with Advanced Security

This tool allows you to configure the Windows Firewall in much more detail. It is covered under the PC Security chapter.

Copyright © 2010 Koroush Ghazi

< AUTOPLAY

Whenever you insert a particular type of media such as an audio CD or a movie DVD, or connect a device such as a portable media player or digital camera, Vista detects the type of device or media and can automatically take specific action, such as opening a movie in Windows Media Player. This functionality is called AutoPlay, and while it can be very handy in some instances, it can also be highly annoying in others. By default the first time you connect a particular device or insert a new type of media Vista will ask you what to do, and whether you want this to be the default action from now on. However under the Autoplay component of Control Panel you can manually adjust Vista's default behavior for each and every particular type of media or device. For example if you insert an audio CD into your optical drive, you can tell Vista to automatically start playing the music, to prepare to rip the music, to take no action at all, or to prompt you to decide each time.

I recommend going through and selecting the default action for all of your common media types. I also recommend connecting any devices you wish to use with Vista if they are not already listed here and telling Vista what to do in each case. If for some reason you do not want AutoPlay to be used for any of your devices or media, untick the 'Use AutoPlay for all media and devices' box at the top of the screen. In fact you may wish to do this for security reasons, as some malware can use AutoPlay functionality to launch itself when an infected disc/device is inserted/connected - although UAC will help prevent this if it is enabled and you are vigilant.

< BACKUP AND RESTORE CENTER

The Backup and Restore Center provides access to a range of functionality which is covered in full detail in the Backup & Recovery chapter.

< BITLOCKER DRIVE ENCRYPTION

BitLocker Drive Encryption is a drive security feature available only to Vista Ultimate and Vista Enterprise owners. It is covered in more detail under the relevant section of the PC Security chapter.

< COLOR MANAGEMENT

Windows Color Management is a tool which allows users to ensure that the colors displayed on their screen are accurate and will be reproduced faithfully across a range of devices. For accurate color reproduction it is very important that your monitor have proper drivers loaded in Vista - see the Windows Driver chapter for details of how to check and update device drivers as necessary. More details of how the Color Management functionality works is in this Microsoft Article, but for the average home PC user you should not change these settings as they require specialist knowledge.

< DATE AND TIME

Although relatively straightforward, it is important that you have the correct system date and time. Some software and some Internet sites will not function properly unless these are set and maintained correctly. There are also additional features you may wish to configure here.

DATE AND TIME

Make sure the date and time are set correctly here. Click the 'Change data and time' button if necessary and manually set the current date and time, though the quickest and most accurate method is to update via the Internet - see Internet Time below. Make sure to set the correct Time Zone for your region by clicking the 'Change Time Zone' button, as this will affect the way changes like Daylight Savings will impact on your system. I strongly recommend ticking the 'Automatically adjust clock for Daylight Savings Time' so that your clock is automatically adjusted back or forward when Daylight Savings occurs in your area. If

Copyright © 2010 Koroush Ghazi

necessary also tick the 'Remind me one week before the change occurs' box on the main screen, though this is not vital.

ADDITIONAL CLOCKS

Under Windows Vista you can select to maintain and show up to two additional clocks in different time zones from your main system clock. Click the 'Show this clock' box above each of the clocks you wish to show, set the time zone for the clock(s), and I recommend naming the clock(s) with suitable names such as 'London Time'. The clock name(s) and the time for each clock will then appear whenever you hover your mouse over the time display in the Notification Area on the lower right corner of the Taskbar at any time.

INTERNET TIME

By default Vista connects to the Internet once a week to update your system clock and ensure its accuracy. If you wish to disable this option or manually update your clock at any time, click the 'Change settings' button. To update manually immediately, click the 'Update now' button. To disable the automatic update functionality, untick the 'Synchronize with an Internet time server' option. If for some reason the system time is not updating or is inaccurate, click the drop down box and select another time server for Vista to connect to for this purpose. In general I recommend allowing Vista to update the clock automatically, as it has no performance impact and helps prevent the clock from slowly becoming more and more inaccurate over time for a variety of reasons.

< DEFAULT PROGRAMS

This option has a range of sub-options which allow you to set the default programs your system uses for a range of functions and importantly the file associations Vista users when launching certain file types. Each of the other sub-options are covered in detail below:

SET YOUR DEFAULT PROGRAMS

This option only allows you to control the files which the main built-in Windows programs handle by default. Select a listed program, and in the right pane you will see that you can either 'Set this program as default' which basically sets the program as the default one for all the file types it can open; or you can manually choose which file types it can open by clicking the 'Choose defaults for this program'. For example if you select Windows Media Player, you can either let it automatically become the default for all the relevant media types it can support, or see details of the specific file types and choose from them manually.

In general I recommend that you do not alter these settings unless you have specific strong preferences, or you know a certain program is problematic with certain file types. If you do want to manually assign a default program to a particular file type, it is quicker and more thorough to use the 'Associate a file type or protocol with a program' option below.

ASSOCIATE A FILE TYPE OR PROTOCOL WITH A PROGRAM

This option allows you to manually view and set the default program to be used when opening a file with a particular type of extension. For example you can choose the program which will open all .MP3 files, or all .TXT files on your system by default. It doesn't prevent other programs from opening these files, it just chooses the default program. Note, if you can't see file extensions for your files in Windows Explorer then make sure the 'Hide extensions for known file types' option is unticked in Folder Options - see Folder Options under the Windows Explorer chapter.

When you first open this tool, it will take a moment for it to populate the list of all known file types on your system and their associated default programs. You can then scroll down the list to view the associations, and note that where 'Unknown application' is listed, that means there is no default for that file type. To change

Copyright © 2010 Koroush Ghazi

the association for a particular file extension, highlight it and click the 'Change program' button at the top right of the box. If it already has a default program, it will be shown and recommended. To add a new program to the list, click the Browse button and go to the specific program file which you wish to use.

Don't change a program association unless you want that program to become the default for an entire file type. If you have problems with an association changing suddenly, remember that when installing certain programs, they will automatically make themselves the default program for particular file types, often without asking your permission. Your best bet is to go into the options for the particular program which is currently associated with a file and check for any settings or file associations there, and alter them first before coming here and changing file associations manually, otherwise the program may override the association again.

You can even associate protocols like HTTP with a particular program here at the bottom of the list. For example you can associate FTP with your own FTP client instead of Internet Explorer which is the default. Note that as of Vista SP1, a new Search protocol has been added, allowing Windows to use a third-party search provider in place of many built-in search functions - see the Windows Search chapter for details.

CHANGE AUTOPLAY SETTINGS

The AutoPlay settings here are already covered in full detail under the AutoPlay section further above in this chapter.

SET PROGRAM ACCESS AND COMPUTER DEFAULTS

This section allows you to set the general defaults for your Internet browser, media player, instant messaging, Java virtual machine and email program. It also allows you to prevent access to particular built-in Vista programs, effectively blocking them. The main reason for the existence of these options is that Microsoft has been charged with monopolistic behavior and as part of the terms of settlement of a case against them, they are required to provide users with the option to disable certain built-in programs such as Internet Explorer, Windows Media Player and Windows Mail which cannot otherwise be uninstalled.

To start with you should select the Custom option and a drop-down box will appear with further options you can customize. Choose your default programs, and I strongly recommend that you do not untick the 'Enable access to this program' option for Internet Explorer or Windows Media Player, as both of these may be required to view certain web pages or play certain media sources.

If you really want to remove certain built-in features completely from Windows Vista, see the Modifying the Windows Installation Disk section under Windows Installation chapter. Note that it is generally not wise to strip out important Vista components because you may need them one day, and some of them cannot just be reinstalled as standalone components.

< DEVICE MANAGER

The Device Manager is an important hardware management tool which is covered in detail under the BIOS & Hardware Management and Drive Optimization chapters.

< EASE OF ACCESS CENTER

There are a range of features here that can be used to accommodate different keyboard usage styles, make Windows easier to see on screen, or provide audible notification of events for example. Quite obviously which settings you choose will depend on your individual requirements. If you want to find out more about these options go to the Windows Vista Accessibility Page. The majority of users will not need to enable or use these settings, and can leave them at their defaults. Some of the more useful functions such as Speech Recognition are also covered further below in this chapter.

Copyright © 2010 Koroush Ghazi

< FOLDER OPTIONS

The Folder Options are often overlooked, but are actually very important to the look and feel of Windows, especially when using any Windows Explorer-based interfaces as well as the general Windows Desktop. It also has specific settings for the Search functionality in Vista. Folder Options is covered in more detail under the Windows Explorer chapter.

< FONTS

This item displays the contents of your *\Windows\Fonts* folder, which contains all your currently installed system fonts. Fonts are the various types of text styles used by a variety of programs such as word processors, paint programs and the Windows WordPad for example. You can install a new font simply by copying its .FON or .TTF files into this folder, or by going to the File menu and selecting 'Install New Font' and pointing to the directory where the new font file(s) reside. Note that TrueType is a font technology that ensures good scaling and that what is displayed on your screen should come out exactly the same on your printer; other types of fonts may look slightly different in different applications and/or when printed and/or when using different font sizes. To find out more about fonts, go to the Microsoft Typography Website. A good site that contains additional fonts you can download and install for free is Simply The Best Fonts. Also see the Graphics & Interface chapter of this book for more details on how to make fonts look better in Vista.

< GAME CONTROLLERS

This tool allows you to configure game-specific controllers detected by Vista to be connected to your system. This typically includes gamepads, joysticks and game simulation hardware. If your device is not being detected by Vista then follow the procedures for installing and setting up the device which come with it, and also see the Add Hardware section further above. Note that although often used in PC games, the mouse and keyboard are not classed as 'game controllers' here - they have their own separate setup tools in the Control Panel (see Keyboard and Mouse below). Further note that if you play certain games only using the keyboard and mouse combination, and you find your character is displaying strange movement behavior (e.g. constantly moving with no user input), then physically disconnect all game controllers from your system (excluding the keyboard and mouse), reboot then relaunch the game.

< INDEXING OPTIONS

This tool displays and controls the indexing of files and folders for the Windows Search functionality. This is covered in more detail under the Windows Search chapter.

< INTERNET OPTIONS

This setting in the Control Panel simply brings up the Internet Explorer 'Internet Properties' box. There is no difference between accessing it here and accessing from within Internet Explorer, so see the Internet Explorer chapter for full details of how to configure these options. Note if you are using another browser as the system default browser then clicking this item will still bring up the Internet Explorer 'Internet Properties' box, not the one for your other browser - this is normal and cannot be changed.

< ISCSI INITIATOR

The iSCSI Initiator is a management interface for controlling iSCSI storage devices connected via a network. This functionality is not relevant to home PC users and is not covered here.

< KEYBOARD

Under the Speed tab, I recommend you set the 'Repeat Delay' slider to the far right (Short) and also set the 'Repeat Rate' slider to the far right (Fast). This will provide maximum responsiveness for your keyboard

Copyright © 2010 Koroush Ghazi

under Windows Vista. You can test these settings by holding down a key in the box provided to see if they suit you. Note that there may also be keyboard-related options in your BIOS that affect the speed with which the keyboard responds, so check there if you find your keyboard still feels sluggish - see the BIOS & Hardware Management chapter.

You can also adjust the 'Cursor Blink Rate' to your taste, and then click OK to apply.

< MOUSE

I only cover the performance-related mouse settings below, as the other mouse settings can be adjusted according to your taste. If you've installed a special mouse driver for your mouse, you may see different settings available under this screen, however the settings below should still be available on most systems.

BUTTONS

Adjust the double-click speed to the rate which suits your usage patterns, and test it on the image of the folder provided. I generally recommend setting a slower double-click speed so that you can open files and folders more comfortably.

POINTER OPTIONS

I recommend ticking the 'Enhance pointer precision' option before you adjust your pointer speed. This option enhances the acceleration/deceleration of your mouse to provide for larger movements when you move the mouse fast, and finer movements when you move the mouse more slowly, allowing more precision while also allowing you greater coverage of your Desktop with the mouse.

WHEEL

If your mouse has a mousewheel, you can increase the wheel's responsiveness by increasing the number of lines it will scroll on each turn of the wheel. Even an increase from the default of 3 to 4 will make a subtle, but noticeable difference if you previously found the mousewheel relatively unresponsive.

< NETWORK AND SHARING CENTER

The Network and Sharing Center provides a visual representation of your current network setup and allows you to further customize and troubleshoot your connection settings. Note that detailed network setting configuration advice is beyond the scope of this book, as it is a very complex topic which varies based on the type of connection and hardware involved. In general Vista detects and sets up your network/Internet connection automatically and does a good job of it. Changing your network settings beyond what is covered below can cause problems including being unable to connect to the network/Internet, which is not worth risking. The main settings and functionality of the Network and Sharing Center are covered below:

Network: When you first installed Vista, you were prompted to choose your Network Type, however you can change it again by clicking the Customize link here. In the 'Customize Network settings' box which opens, you can choose to make the location type Public or Private with the difference described in this Microsoft Article. For the average home PC user with a connection to the Internet, I strongly recommend Public, which ironically is more private and secure than the Private location, because it means that you are connecting to a Public Network (the Internet) and hence require more protection than if you were connecting to a Private network (e.g. at work). Only choose Private if you're connected to a trusted network of other PCs. In any case you can customize the details of this network type further below. Once done click Next then Close.

Importantly, remember that the Network Type you choose also affects the profile used in the Windows Firewall Advanced Settings, so if you set up specific firewall settings for a Network Type there, then altered

Copyright © 2010 Koroush Ghazi

your Network Type afterwards, go back and change the firewall settings to apply to the new Network Type as well - see the PC Security chapter for details.

Connection: Here you will see your current connection type. This is usually set automatically based on the type of network device you have connected or installed on your PC. Click 'View Status' to see more details on the device, and click the Details button to see even more details. If you're having problems with your connection, click the Diagnose button. If no problem is found, you can either send a report to Microsoft for further help, or reset the connection which may resolve the issue. Generally as long as you use the latest drivers for the device then there shouldn't be any problems or any need to alter the device settings.

For advanced configuration, click the Properties button. Here you can see the various clients, services and protocols the connection uses, which again should not be altered unless you know what you are doing. Below are my recommendations for a standard Internet connection via a modem or router on a home PC not connected to a network of other PCs:

You can untick the following items (but don't Uninstall them):

§ Client for Microsoft Networks
§ QoS Packet Scheduler
§ File and Printer Sharing for Microsoft Networks
§ Link-Layer Topology Discovery Mapper I/O Driver
§ Link-Layer Topology Discovery Responder

The above protocols, clients and services are intended primarily for PCs connected to a network, and hence are not needed by the average non-networked home PC for normal Internet access. However if at any point you experience reduced functionality or problems, re-tick them all again and restart your PC.

Importantly, you may experience issues with general Internet browsing when using the newer IPv6 protocol enabled by default in Vista as detailed in this Microsoft Article. You can try to resolve this by temporarily disabling the 'Internet Protocol Version 6 (TCP/IPv6)' item. Alternatively you can highlight it, select Properties and try to configure it manually using the details in this Microsoft Article. In general though this should not be necessary nor is it recommended as Vista is designed to automatically fall back to IPv4 if IPv6 starts experiencing issues on your system. And again, if in doubt do not alter any settings here as there is more potential to do harm than good.

Sharing and Discovery: These options relate to the way in which your PC interacts with other PCs on a network of computers. For the average home PC connected to the Internet, most if not all of these options should be turned Off - except 'Password protected sharing' which should be On. If you're on a network then make sure that at least the 'Network discovery' option is On, and configure the other options as advised by your Network Administrator or leave them at their default.

Set up a Connection or Network: Should you wish to add a new connection type, click this link in the left pane and follow the Wizard. Again, Vista does a good job of detecting your existing networking device(s) and configuring them properly, as long as you have the right drivers installed, so you should not need to use this under normal circumstances. You may need to follow the manufacturer's instructions and/or download the most recent drivers if your network device is not being detected.

< OFFLINE FILES

Offline Files allow users connected to a network of PCs to be able to store copies of particular network files on their own PC. That way you can work with these files even when you are not connected to the network. When you reconnect to the network Vista will sync the files between your PC and the network. The average home PC user should not need to enable this functionality.

Copyright © 2010 Koroush Ghazi

< PARENTAL CONTROLS

The Parental Controls option is designed to let an Administrator set particular limitations on specific User Accounts. You will need to create Standard User Accounts for each person you wish to control using these features, and you will need to have an Administrator User Account with a password. See the User Accounts later in this chapter for details of how to enable and configure Parental Controls.

< PEN AND INPUT DEVICES

This option allows you to configure pen-based or similar input devices connected to your system. Go through and adjust these as necessary, and obviously none of the settings impact on standard input devices such as keyboard or mouse.

< PEOPLE NEAR ME

People Near Me is a feature which allows you to invite other users on the same network to engage in a shared task. The average home PC user will not need to use this function, so make sure to untick the 'Sign me in automatically when Windows starts' box here, and under the 'Sign in' tab make sure the 'Sign out of People Near Me' option is selected.

< PERFORMANCE INFORMATION AND TOOLS

This option takes you to a range of tools which are useful in troubleshooting and benchmarking your system. Full details of these tools can be found under the Performance Measurement & Diagnostics chapter.

< PERSONALIZATION

This option provides a range of features designed to allow you to alter the appearance and sound of Windows Vista. To start with, note that you can click the 'Change desktop icons' link in the left pane if you wish to add, remove or change the appearance of several of Vista's standard desktop icons including the Recycle Bin. Importantly, if you wish to change the general size of all text in the Windows interface, you can click the 'Adjust font size (DPI)' link in the left pane. Below are the general settings for this feature:

WINDOW COLOR AND APPEARANCE

Here you can adjust the color of the general Windows interface, including the level of transparency used for Vista's Aero Glass see-through effects. If you don't like the sample colors shown, click the 'Show color mixer' option at the bottom of the box and you can create your own custom color using the Hue, Saturation and Brightness sliders which appear.

If your graphics card supports the Vista Aero interface, and you have it selected, you can use the Color Intensity slider to adjust the level of transparency - at far right the see-through effect is disabled, at far left it is as transparent as possible. You can turn off transparency altogether by unticking the 'Enable transparency' box. As discussed under the Graphics & Interface chapter, for most systems Aero has no real impact on Desktop performance, and your Desktop configuration in general has no impact at all on gaming performance, because it is suspended when a 3D game is running.

You can customize the settings further however - click the 'Open classic appearance properties for more color options' link and you will see more options, some of which are quite important and covered below:

Color Scheme: If your graphics card can support it, you can select the 'Windows Aero' transparency-based effects for the Vista interface. If your graphics card doesn't support this feature, or you have Vista Home Basic then you can select 'Windows Vista Basic' for a similar interface with no 3D or transparency effects. If

Copyright © 2010 Koroush Ghazi

you wish to return to a Windows 98/2000 style interface, select 'Windows Standard' or 'Windows Classic'. The 'High Contrast' options are primarily for the visually impaired - see the Ease of Access section above.

Windows Aero is actually designed to be smoother in transitions and screen updates, such as moving an open window around the screen. However it can also be slower on some systems which have older/slower graphics cards, so if you feel the interface is sluggish then select the Vista Basic option, though note that various advanced features such as transparency effects and 3D Flip will be disabled. If you want to further increase interface responsiveness then switch to 'Windows Standard'. Note that if you believe your system supports the Aero interface but the option is unavailable here, see the Graphics & Interface chapter for details of how to check for and if necessary forcibly enable Aero compatibility.

Effects: Click this button and you will see several additional effects which you can alter. In the 'Use the following method to smooth edges of screen fonts' box you can choose ClearType or Standard font smoothing. Either method reduces the jaggedness of text on the screen and is best left enabled. I recommend you select ClearType if you have an LCD or Plasma display, but for more details see the Graphics & Interface chapter.

You can also choose whether to have a shadow show under the menus, and whether to display the contents of a dialog box or window while it is being moved around. Both can be left enabled unless you don't like them, or you want to improve your desktop responsiveness if it seems slow, particularly while dragging around windows.

Advanced: If you really want to customize your Windows Desktop appearance, clicking the Advanced button takes you to a screen where you can select the various components of the desktop, such as window borders, window titles, icons and so forth, and manually adjust their size, color and font type and size if applicable.

DESKTOP BACKGROUND

Here you can select the type of image you wish to use as the background wallpaper on your Windows Desktop. More details of this feature are covered under the Graphics & Interface chapter.

SCREEN SAVER

Here you can set whether a screen saver becomes enabled after a period of inactivity. A screen saver is not necessary on modern CRT or LCD displays, so if you don't wish to use one simply set this option to None. However a screen saver is useful in preventing temporary image retention on LCD monitors, and also to prevent image retention and permanent burn-in on Plasma displays. It can also be useful in saving energy, or improving security by preventing others from seeing what is on your desktop when you are away from the PC. In fact to further bolster security you can tick the 'On resume, display logon screen' box to force a logon prompt whenever the screen saver is exited. Of course this has no impact if the User Account does not use a password.

Go through and preview the screen savers, then select one. I recommend the Blank screen saver as this will use less energy, provide the most security and privacy, and prevent any potential image retention. Note that some screen savers can be configured further by clicking the Settings button; e.g. the Photos screensaver requires you to tell it where your desired photos are stored. Choose how long a period of inactivity is required before the screensaver kicks in by entering an amount in minutes in the Wait box. An idle period of 5 - 10 minutes is usually sufficient for the screen saver to kick in during genuine idle periods without interrupting you while you work. Note that the screen saver will not interfere with games or 3D applications.

Finally, the settings found when clicking the 'Change power settings' link here are covered in detail further below under the Power Options section.

Copyright © 2010 Koroush Ghazi

SOUNDS

These options are covered under the Sound section of this chapter further below.

MOUSE POINTERS

These options are covered under the Mouse section of this chapter further above.

THEME

When you have configured the various personalized Windows appearance and sound settings the way you want them, you can come to this section and save this collection of customized settings as a Theme. Click the 'Save As' button and specify a location and name for your theme. This is important because sometimes unintended system changes can alter various aspects of your current theme and to get it all back without a lot of tedious work you can come back here and reload it all at once.

DISPLAY SETTINGS

This option allows you to configure the Windows Desktop resolution and color depth, as well as your monitor configuration, as covered below. Note that you may need updated graphics and/or monitor drivers for the functionality below to work properly:

Monitor: This should be automatically configured and does not need to be changed if you have a single monitor setup. If you have two or more monitors you can use the drop box to select which monitor to add/extend your Windows Desktop to, or set as your main monitor. Clicking the 'Identify Monitors' button will briefly display a large white numeral on the screen to show which is the primary monitor (denoted by the number 1) and which the secondary (number 2) and so forth.

Resolution: When selecting your desktop Resolution, if you have an LCD or Plasma monitor then try to match the desktop resolution with the monitor's 'native' resolution - this is usually the maximum possible resolution available on the slider. More details can be found under the Resolution section of the Gamer's Graphics & Display Settings guide. This setting only affects your resolution when using the Windows Desktop, it has no impact on games and other 3D programs which have their own independent resolution settings.

Colors: Under this option select 'Highest (32 bit)' as this provides the most accurate representation of colors; the 'Medium (16-bit)' option will reduce color complexity and hence not look as good. There should be no reason why any Vista-compatible graphics card would struggle with 32-bit color on the Windows Desktop as there is negligible performance impact - but if you absolutely need more desktop responsiveness select the Medium option. Note however that Windows Aero will not be available unless you set 32-bit here.

If you click the 'Advanced Settings' button under the Settings tab, you will be taken to the advanced control panel for your graphics card. While many sections of this screen differ based on your particular graphics card, all graphics cards share the following common elements, which are described below:

Adapter: Here you will find the details of your current graphics adapter (i.e. your graphics card). If the details are incorrect, this could indicate a poorly installed or incorrect graphics and/or motherboard driver, or modified hardware.

Monitor: You can set the Refresh rate used by your monitor for the current screen resolution. I strongly recommend that you first tick the 'Hide modes that this monitor cannot display' box, then select the highest refresh rate listed. The refresh rate determines how many times per second the image onscreen is redrawn. The higher the setting, the more times the screen is 'refreshed', and the less strain there is on your eyes - see

Copyright © 2010 Koroush Ghazi

the Refresh Rate section of the Gamer's Graphics & Display Settings Guide for full details. If you cannot see your monitor's known maximum supported refresh rate in this box, then you can either wait for updated graphics drivers, or you can untick the 'Hide modes...' box and manually select the closest refresh rate which is still lower than your maximum. Most refresh rate issues in Vista are due to drivers, so install the very latest ones for your graphics card and also your monitor if possible.

Troubleshoot: You can click the 'Change settings' button (if available) to access the 'Graphics Hardware Acceleration' slider. Normally this slider should be at the far right for full graphics functionality. However if you are troubleshooting a graphics-related issue, lower this slider and test to see if this resolves the problem. If the problem is resolved when the slider is at None or Basic, then the issue is likely with your graphics drivers as these control the more advanced graphics functionality.

Color Management: These settings are already covered under the Color Management section in this chapter.

Graphics Card Name: The tab bearing your graphics card name contains the means by which you can access further graphics-card specific settings. It is important that you set these up correctly as they control the bulk of your graphics card's advanced 3D functionality, particularly in games. See my Nvidia Forceware Tweak Guide or ATI Catalyst Tweak Guide as relevant for more details.

Once again remember that all of the major graphics and display settings on your system are heavily dependent on your graphics driver, especially if you're using Vista Aero. Any glitches or problems you experience are generally due to driver-related issues, and are often fixed by updating to the latest drivers and/or removing traces of previously installed drivers - see the Windows Drivers chapter for details.

< PHONE AND MODEM

This option lets you configure any connected phone or modem devices. Details are provided in this Microsoft Article, and won't be covered in any more detail here.

< POWER OPTIONS

These options impact on the power consumption and idle behavior of Windows Vista. They also allow you to change the behavior of the Power, Reset and Sleep buttons on your PC.

POWER PLAN

There are three preset levels of power management, called Power Plans: Balanced, Power Saver and High Performance. These are described further in this Microsoft Article. I strongly recommend that you individually customize the settings rather than relying on any of the presets, since none of them is exactly right for most systems. To customize your own settings, follow these steps:

1. Click the 'Create a power plan' link in the left pane.
2. I suggest choosing 'High Performance' as the basis for your changes, as the other schemes can result in reduced performance.
3. You can give the plan a descriptive name, or use the default which is fine.
4. I recommend turning off the display after a set period of system inactivity, as this has no performance impact and does not harm the monitor, but prevents energy waste and potential image retention on LCD or Plasma displays. Around 15 - 20 minutes should be reasonable.
5. I don't recommend enabling the Sleep functionality (select Never), see further below for details.
6. Importantly, click the 'Change advanced power settings' link to access the more detailed settings.
7. Click the small plus sign next to each and every setting to fully expand them one by one, changing them as covered below. Note that if any settings are unable to be changed, click the 'Change settings that are currently unavailable' link then go back and change them.

Copyright © 2010 Koroush Ghazi

The advanced power settings are covered below, with my recommendations. Note that Mobile PC users will have two sets of options to configure: 'On battery' for when using battery power; and 'Plugged in' for when connected to mains power - configure the 'On battery' setting differently than below. Below are my recommendations for a standard desktop home PC not on battery power:

Additional Settings - Require a password on wakeup: When waking up from sleep mode, if set to Yes this option forces you to reenter the password (if one exists) for the current User Account to unlock the PC. Set to suit your security needs.

Hard Disk - Turn off hard disk after: Set this to the number of minutes of inactivity before your hard drive is turned off. I recommend selecting Never to maintain maximum responsiveness; hard drives are best not switched on and off constantly.

Wireless Adapter Settings - Power Saving Mode: If you have a wireless network adapter connected to your system, select the power saving mode. Again for maximum responsiveness select 'Maximum Performance'.

Sleep - Sleep after: This option lets you choose how long a period of inactivity is required before your system goes to Sleep. Sleep is a power-saving mode designed as a compromise between totally switching off your PC and leaving it running at full functionality. It is primarily intended for mobile PC users who need to conserve power but maintain responsiveness. In Sleep mode your PC turns off most of its components and saves your documents to RAM. Thus it uses minimal power and appears to be inactive, but it can be 'woken up' almost instantly by pressing the Power button. Sleep replaces the Standby mode of previous Windows versions as detailed in this Microsoft Article, though Hibernate is still available and covered further below.

The problem with Sleep mode is that firstly it can potentially cause system instability or strange behavior after recovering from sleep, sometimes due to driver incompatibilities. Secondly, of concern is that in Sleep mode your open documents, programs and general system state are saved to RAM and the RAM is kept on, which means your system is susceptible to data loss should there be power loss or RAM failure. So generally speaking I don't recommend using Sleep mode - set this option to Never. However if you still wish to use something similar, I recommend Hybrid Sleep as covered below.

Sleep - Allow Hybrid Sleep: In this section you can choose whether to enable Hybrid Sleep mode or not. If you can't see the Hybrid Sleep or Hibernate settings here you need to open an Administrator Command Prompt, then type:

```
Powercfg /hibernate on
```

This will re-enable the display of these options in the advanced power options.

Hybrid Sleep mode is the same as Sleep mode covered above, however instead of saving your open documents, programs and system state to RAM, it saves them to a *Hiberfil.sys* file in your system drive's base directory, providing added security against potential data loss. This file is exactly the same size as your system RAM and the act of writing to it when entering Hybrid Sleep and reading from it during waking up will make your system take longer to shutdown and startup than Sleep mode. The key benefit is that unlike Sleep mode, Hybrid Sleep keeps your data safe by recording it to your drive rather than simply storing it in RAM.

Sleep - Hibernate after: This option allows you to configure Hibernation, which is the same as Hybrid Sleep in that it will write your open documents, programs and system state to the *Hiberfil.sys* file after a period of inactivity as specified here. However unlike Sleep or Hybrid Sleep, rather than putting your system into a power-saving mode, it allows you to turn off the entire PC and leave it that way for as long as you like. You

Copyright © 2010 Koroush Ghazi

can then turn the system back on in the future to find that your previous session is restored exactly as you left it. This mode is generally not recommended to anyone but mobile PC users who plan on not using their mobile PC for several days or more but still want to quickly get back to where they were. I do not recommend Hibernation for the standard desktop home PC user due to the potential for additional problems. It is much wiser to start with a 'clean' session each time you boot your PC. Note that just as with Hybrid Sleep, if you cannot see the Hibernation options under the advanced power options, you will need to execute the `Powercfg` command as shown further above.

Importantly, whether for Hybrid Sleep or Hibernate, if you have disabled these options and do not plan on using them, you should also delete the *Hiberfil.sys* file on your system drive as it can be quite large. However you cannot do so by just highlighting and deleting it. You must go to Disk Cleanup (See the Cleaning Windows chapter) and on the main screen select 'Hibernation File Cleaner' as one of the items to remove, then click OK, and it will be deleted. Note that this will also remove the Hibernate and Hybrid Sleep options from your Power Options as well. They can be restored using the `Powercfg` command as shown further above.

USB settings - USB selective suspend setting: This option controls whether the system will selectively suspend individual USB devices which do not require power. In general this should be left at Disabled to prevent potential problems with USB devices, unless you run a mobile PC where power savings are more important.

Power buttons and lid - Power button action: This is actually quite an important setting as it determines what happens when you press the Power button on your PC. I strongly recommend setting this to 'Shut Down' which is the normal expected behavior for a power button.

Power buttons and lid - Sleep button action: This setting determines what happens when you press the Sleep button - if one exists - on your PC. Set to suit your taste, though generally it would make sense to set the Sleep button to match the Sleep function. Again I don't recommend using Sleep under normal desktop conditions, so if you're certain you won't use sleep, set this option to 'Do nothing' instead.

Power buttons and lid - Start menu power button: This setting determines what the red power button (next to the Search box) on the Windows Start Menu does by default. I recommend setting it to 'Shut Down' as that is the expected behavior for this button. Note that you can access all the power options by clicking the small white triangle to the far right of the red power button on the start menu. Of annoyance is the fact that there is no restart button, however this is addressed under the Graphics & Interface chapter where you can create your own custom Shutdown and Restart desktop icons for quicker access.

PCI Express - Link state power management: This setting will allow an idle PCI-E connection to reduce power consumption depending on the option chosen here. Since PCI-E is most commonly used for graphics cards on higher-end systems at the moment, I would strongly recommend against anything other than Off for this setting to prevent slowdowns or crashes.

Search and Indexing - Power savings mode: If search indexing is enabled (See the Windows Search chapter), this option determines whether to allow background disk indexing to use more or less power by updating the index more or less frequently. For the average home PC user there is no reason to attempt to save a small amount of power by setting this option to anything other than 'High Performance'. Any power savings you might make by lowering this setting will mean that your index will be less up to date and hence less useful in return.

Display - Turn off display after: This setting lets you select the amount of inactivity before your monitor is switched off. It will instantly switch on again as soon as you press a key or move the mouse. Since displays use a fair bit of power, and since LCD and Plasma displays in particular can suffer from temporary image retention (LCD) or permanent burn-in (Plasma) if displaying a static image for too long, it makes sense to

Copyright © 2010 Koroush Ghazi

enable this option and set it to something like 15 or 20 minutes of inactivity. That way when you're away from your PC for longer periods your monitor switches off, protecting the display and having no impact on your PC's performance or your hardware longevity since monitors are designed to turn off and on frequently. If you're not sure of how long to set this, use the setting below.

Display - Adaptive display: If you enable this setting, in conjunction with the setting above it will monitor to see how often you actually wake up your display with the mouse or keyboard. If it finds you're waking up the display shortly after it has turned itself off, it may automatically extend the inactive time period for the 'Turn off display after' setting above, to both suit your usage pattern and optimize energy savings.

Windows DreamScene settings - Power Saving Mode: This option only appears if you have Windows DreamScene, which is a Vista Ultimate Extra. You can choose whether to enable Power Saver mode, such that DreamScene will stop playing to conserve energy, or High Performance mode which leaves DreamScene to run without interruption regardless of the power status.

Multimedia settings - When sharing media: Determines your PC's behavior when your PC is sharing or playing back media from your PC via a connected device or other computer(s). I recommend selecting 'Prevent idling to sleep' so that your PC doesn't enter Sleep mode, disrupting the media stream, unless you manually select to put it to Sleep.

Battery: These settings can be configured to determine what your mobile PC does under various custom battery levels.

There may be additional settings, or options missing, compared to those listed above. This depends on your actual hardware and its capabilities. Once done with these settings click the Apply button and your scheme will now be configured and put into effect. You can see this under the main Power Options screen. Note that other plans which may not be in use will be under the 'Show additional plans' line; click it once to expand it and show the other available plans.

In general while there are valid concerns about Global Warming and the wasteful use of energy and resources, I believe it is false economy to enable too many power saving features as you may reduce the functionality of your PC, increase instability and also lose data if you go overboard. For gamers and other high-end users I certainly don't recommend that most power saving options be used aside from those recommended above. For mobile PC and casual desktop PC users however the options require personal choice and thought based on individual usage patterns and battery life. Regardless, if you experience any system instability or strange system behavior, I recommend using the 'High Performance' preset for troubleshooting purposes to see if power-based settings are the cause of your problems.

< PRINTERS

This section allows you to view all connected printers, and add, remove or configure such devices. It is recommended that you refer to the particular device's instructions for optimal setup information as each will differ. Right-click on each printer and select Properties for more detailed configuration options. Importantly, note that if you have disabled the 'Print Spooler' service then any printer on your system will not function, so make sure the 'Print Spooler' service is set to Automatic in the Services utility if you want to use a printer. This also includes virtual printers, such as PDF makers, which require this service to be on. Finally, if you are connected to a network printer and you have followed my configuration recommendations in this book - which as noted repeatedly are not intended for networked computers - then your network printer may not be detected by Windows. Go back and change your settings to default, especially the Services and Network and Sharing Center settings.

Copyright © 2010 Koroush Ghazi

< PROBLEM REPORTS AND SOLUTIONS

This tool provides a means by which you can view recorded system problems, and also check for possible solutions. Usage details are covered in detail under the Performance Measurement & Diagnostics chapter.

< PROGRAMS AND FEATURES

Programs and Features is an essential tool which can be used to view or uninstall the programs and drivers currently installed on your system. It provides useful details such as when a program was installed under the 'Installed On' column, the total size of the program on disk under the Size column, and even the version number in some cases in the Details pane at the bottom when a program is highlighted. Unfortunately some programs and drivers installed on the system will not appear in this list, possibly because of non-compliant installers; this situation should improve - for now see the Windows Drivers chapter for information on how to manually find and remove installed drivers.

The main functionality for Programs and Features is covered below:

Uninstalling Programs: Highlight the program you wish to uninstall, right-click on it and select Uninstall to commence removal of it. If the program allows you to alter its installation, a Change option will also be available, or you may see Uninstall/Change, meaning you will have to choose which you prefer in the wizard which launches.

Get New Programs Online at Windows Marketplace: This option shown in the left pane allows you to go to the Windows Marketplace site and purchase a range of software made or approved by Microsoft.

View Purchased Software (Digital Locker): This option shown in the left pane launches the Digital Locker Assistant. The main purpose for Digital Locker is to complete an online purchase at Windows Marketplace, allowing you to securely download and install your purchased software.

Turn Windows Features On or Off: This option is shown in the left pane, and when launched opens a new box displaying a list of all the built-in Windows features which you can individually install or uninstall. By making sure you have only the features you need, you can save a bit of disk space, but by the same token if you strip out functionality from Windows which you may need later, it can be an inconvenience. You will need to take your time going through these features and carefully deciding if you really need them. If in doubt, do not remove or alter a feature as it is not necessary and could cause more problems than any benefits you experience. A detailed listing of features which you can use to help you decide what to keep and what to remove is this Vista Feature Guide. Below are my own brief descriptions and recommendations, intended for a standard home PC connected to the Internet but not to a network. Note that some editions of Vista will not contain all of these features:

Copyright © 2010 Koroush Ghazi

Feature	Recommend	Details
ActiveX Installer Service	Untick	ActiveX is not necessary and carries a security risk.
Games	Tick	There is no harm in keeping all the standard Vista games such as Solitaire and Chess Titans. If necessary uninstall the specific games you don't play.
Indexing Service	Untick	This is not the same as the Vista search indexing service; it's for legacy applications and may cause issues if left enabled.
Internet Information Service	Untick	These are all designed for users running a Web or FTP server.
Microsoft .NET Framework 3.0	Tick	Required for applications programmed using .NET.
Microsoft Message Queue (MSMQ) Server	Untick	Not necessary unless you want run an MSMQ server.
Print Services	Untick	Not needed for standard home printers, only required if you use or provide remote (networked or web-based) printers.
Remote Differential Compression	Untick	Only tick if connected to a network at any time.
Removable Storage Management	Untick	Only tick if you use removal storage media.
RIP Listener	Untick	Only tick if on a network which uses the RIPv1 protocol.
Services for NFS	Untick	Not required, NFS Protocol is for networks.
Simple TCPIP Services	Untick	Not required, installs services such as echo, daytime, etc.
SNMP Feature	Untick	Simple Network Management Protocol is for networks.
Subsystem for UNIX-based Applications	Untick	Only tick if running Unix-based applications, which home users don't normally do.
Tablet PC Optional Components	Untick/Tick	This component is required for access to the Snipping Tool covered in the Tablet PC section of this chapter. Tick if you want to use that tool or have a Tablet PC, untick if you don't.
Telnet Client	Untick	Only tick if you plan to use Telnet features to connect to a server.
Telnet Server	Untick	Lets others connect to your machine via Telnet, which is a security risk unless you need this functionality.
TFTP Client	Untick	Only tick if you want to use TFTP to connect to TFTP server, which normal Internet usage does not require.
Windows DFS Replication Service	Untick	Only tick if connected to a network at any time.
Windows Fax and Scan	Untick	Only needed if you want to use connected fax devices.
Windows Meeting Space	Untick	Only tick if you use the Windows Meeting Space functionality, see the People Near Me section of the Control Panel chapter.
Windows Process Activation Service	Untick	Nothing to do with Product Activation, required for some applications to be able to transfer information. Usually not needed.
Windows Ultimate Extras	Tick	Allows Vista Ultimate owners access to any Ultimate Extras they've installed.

After changing these settings and clicking OK you may need to reboot and/or insert your original Vista DVD as required. If you experience any odd behavior, reduced functionality or other problems then come back to this area and reset the features back to their defaults - see the guide linked further above for a detailed list of the default values for every feature and sub-feature.

Copyright © 2010 Koroush Ghazi

< REGIONAL AND LANGUAGE OPTIONS

The basic region and language options should have already been chosen during the installation process, however here you can change or refine these settings. It's important to select the correct location in particular, as this determines things like daylight savings adjustments to the system clock.

FORMATS

Select the language format that suits your particular region of the world. This is important for making sure that tools such as spell checkers can operate correctly, and that your currency and time are appropriately displayed. If you want to alter the way these things are displayed, click the 'Customize this format' button and manually edit the way numbers, dates, times and currency is shown.

LOCATION

Set your current physical location from the list.

KEYBOARDS AND LANGUAGES

Click the 'Change keyboards' button to access the advanced settings here. Each tab is covered below:

General: The default input language used for your keyboard should be chosen correctly based on your location and hardware. In many countries using the western alphabet the keyboard used is a standard QWERTY US keyboard. However if you have a different type of keyboard and/or you want to set a different language from the location you are in, click the Add button, select the language you wish to use, then tick the box for the actual keyboard hardware you're using. To see a graphical representation of what the keyboard layout looks like, highlight the keyboard type and select Properties or Preview. If you are not going to use a particular location or keyboard layout, then highlight it on the list and click Remove. If your keyboard hardware is not being detected correctly you may have to install specific drivers for the keyboard.

Language Bar: The Language Bar is a small icon or floating bar which only appears if you have two or more keyboard languages installed. It is used to provide easy access for switching between languages. To alter where the Language Bar is shown, select whether to have it as a floating rectangular box on the desktop or whether it will sit in the Taskbar at the bottom of the screen. To alter the appearance of the language bar use the three checkboxes on this page to suit your tastes. If you want to get rid of the Language Bar then either select Hidden or go and delete all additional languages from under the General tab above.

Advanced Key Settings: Here you can set the keyboard shortcut method to switch between languages. The default for switching between input languages is Left ALT+SHIFT to switch language, and CTRL+SHIFT to switch keyboard layouts. You can change this sequence by highlighting the 'Between input languages' item and select 'Change key sequence', and you can also assign a key shortcut combination to switch directly to a specific language by highlighting the language in the list and once again clicking the 'Change key sequence' button.

ADMINISTRATIVE

Language for non-Unicode programs: The Unicode system basically allows most modern programs to adapt their menus and dialogs to your system's default language, so this setting only applies to older non-unicode programs. For these older (non-unicode) programs you can set the locale which they will use in case the program's text is not being displayed correctly. In most cases the system locale and non-Unicode locale should be the same.

Reserved Accounts: You have the option of copying your Regional and Language settings to the default template used to create new User Accounts in the future. To do this, click the 'Copy to reserved accounts'

Copyright © 2010 Koroush Ghazi

button and tick the 'Default user account' option. If you also want to copy these settings across and make them the default for the system (aside from existing User Accounts), then also tick the 'System Accounts' option as well, then click OK and click Apply.

< SCANNERS AND CAMERAS

This section will allow you to install and manage any digital image devices such as scanners or digital cameras you've connected to your machine. Typically you only need to attach your device to the PC and Windows will detect it and install drivers. For unrecognized devices first refer to your device's manual for specific setup recommendations, and if necessary attach the device to the PC, come to this utility, click Refresh and if that fails click the 'Add Device' button and follow the Wizard.

< SECURITY CENTER

The Windows Security Center unifies access to and monitoring of major security-related Windows settings on your system. It is not a security utility in itself, as it does nothing but warn you about certain security features. It is covered in detail in the PC Security chapter.

< SOUND

One of the major changes in Windows Vista is the way in which it handles sound. These changes have been made to both increase the stability and performance of audio, as well as its compatibility with a range of audio devices, plus provide additional audio functionality at the system level. The changes are detailed in this Microsoft Article as well as this OpenAL Article and this Creative Article.

In plain English, the changes mean that:

§ There is much less potential for system instability, since the drivers are not entangled with the Kernel of the OS. This means a sound-related problem is less likely to slow down or crash the entire system.
§ The Vista audio engine runs faster and with greater accuracy than the XP audio engine.
§ You can now independently set the volume level for different devices or applications using the Volume Control. This means that you can have your media player at full volume for example, but at the same time a Windows sound like a warning prompt from UAC can be played at a lower volume if you wish.
§ Increased configuration options for different speaker setups, including headphones, and more options for genuine home theater usage.
§ Most users now have access to a range of audio enhancements which do not require high-end sound hardware or specialized software.

There is however a drawback to the way in which Vista forces most audio through software mode, and that is any older programs or games using the DirectSound/DirectSound3D API will not be able to use hardware-accelerated functionality like Creative's EAX audio effects, since under Vista this runs only in software mode. More details of this, including a patch for Audigy and X-Fi sound cards is at the Creative ALchemy Project site as well as the links further above. Fortunately most games and applications now run OpenAL-based audio and are not affected; they can use hardware acceleration since they bypass the software mode emulation. For users who are having major audio problems, it may be wise to remove or disable any plugin sound cards and revert to onboard audio functionality, since this is designed for software mode and is likely to be less troublesome under Vista. The performance difference should be minimal and you may even gain access to additional features as covered below.

Below we look at the new sound features, beginning with the Volume Mixer found in the Notification Area:

Copyright © 2010 Koroush Ghazi

VOLUME MIXER

Shown as a small speaker icon in the Notification Area at the bottom right corner of the screen, the Volume Mixer allows you to adjust the master volume level for the current sound output device. When you hover your mouse over it, it will show the current master volume level as a number between 1 and 100, the current output device, as well as the sound hardware being used. If you click once on it you can adjust the master volume level using a slider. If you want to mute or unmute all sound, click the small blue speaker icon to toggle this.

To open the full Volume Mixer, left click on the Volume Mixer icon in the Notification Area and select the Mixer link. The Volume Mixer lists the separate sound output device(s) supported and enabled, as well as the application(s) supporting sound input/output currently running, including Windows itself. You can independently adjust Windows and application volumes to suit your taste or mute them individually. I recommend firstly setting a master volume for the sound output device quite high (e.g. at 75%), then adjust other devices accordingly.

Below are the features of the Sound component found in the Control Panel:

PLAYBACK

This tab lists all the available sound playback devices on your system. This includes devices such as speakers or headphones. To select which will be the default playback device (denoted by a small green tick next to its icon), highlight the device and click the 'Set Default' button.

Certain devices allow additional configuration, so highlight the device and if the Configure button is available, click it and follow the Wizard to correctly configure the device. Most commonly this involves configuring a set of speakers for the correct number and type of speakers used.

Each sound playback device can be configured in more detail, including access to a range of new functions, by highlighting it and clicking the Properties button. While I can't detail every feature for all types of playback devices, below are the common features for speaker output. Importantly, some of these features depend on specific types of hardware and/or drivers and hence may not be available on every system:

Tone: This option allows you to set the Bass and Treble level for all sound playback. I recommend playing some music or a movie on a media player with a neutral or disabled graphic equalizer and adjust these settings appropriately. Judicious use of this feature can make a real difference to sound quality.

Levels: The sliders under this section allow you to adjust the volume levels for each of your various output and input types, such as CD audio, microphone, Line In, etc. I recommend muting (clicking on the blue speaker icon) each input/output type you don't use, as this helps reduce background hissing. You can also set the Balance for each one by clicking its Balance button; you will be able to set the relative volume level for every channel possible on that output type.

Enhancements: This is an important set of features now included with Vista, and is covered in detail in this Microsoft Article. It is only available on certain types of sound hardware, so you may not see this tab. The full set of enhancements are summarized below:

- Bass Management - Controls Bass for home theater particularly when a subwoofer is missing.
- Speaker Phantoming - When using a multi-channel source, compensates for an incomplete multi-channel speaker setup.
- Speaker Fill - The reverse of Speaker Phantoming, takes a two-channel source and spreads it over more channels.
- Virtual Surround - Converts multi-channel sound to two-channel, and back again if required.

Copyright © 2010 Koroush Ghazi

§ Loudness Equalization - Attempts to maintain a more constant sound level across a range of sources.
§ Room Correction - Through the use of a microphone Vista can automatically calibrate a multi-channel home theater setup.
§ Headphone Virtualization - Creates a 3D sound environment for headphones.
§ Bass Boost - Boosts the Bass response on smaller speakers such as mobile PC speakers.

The availability of any of these options is dependent on the sound hardware and drivers you are using, as well as the playback device chosen.

Advanced: The 'Default Format' option shown here is the number of channels, the sample rate and the bit depth generally used to play back all audio (i.e. the normal 'shared mode' Vista uses) through this playback device. This is very important to the overall quality of sound you will experience in Vista. You can try various options and click the Test button to hear the difference in audio quality. I recommend that you select at least 16-bit 44,100Hz sample rate or the default already chosen by Vista, whichever is higher. You can then set this even higher if you want. The higher this is set the greater the clarity and quality of most sound, however some audio is encoded at a relatively low sample rate or bit rate, so raising this setting won't magically make a bad audio source better. Also remember that setting this to an extremely high rate can also cause sound glitches on some hardware, and may also reduce performance depending on your CPU since the sample rate conversion is a done by Vista, not your sound hardware - except in OpenAL and ASIO environments (see further above for details).

I recommend ticking the 'Allow applications to take exclusive control of this device' and 'Give exclusive mode applications priority'. These will ensure that a program or game using the sound output device in Vista can bypass the Windows audio engine if it needs to. If you run into problems with your sound output in particular applications, untick the first option as it may cause compatibility problems with older programs under certain circumstances.

RECORDING

This tab lists all the available sound recording devices on your system. This includes devices such as a microphone. To select which will be the default recording device (denoted by a small green tick on its icon), highlight the device and click the 'Set Default' button. Just like playback devices, recording devices have advanced options which can be configured. When you highlight the recording device and click the Configure button, this will take you to the advanced configuration options. For microphones in particular, the options are covered under the Speech Recognition section further below in this chapter. When you click the Properties button for the recording device, you are taken to a set of tabs similar to those shown under the Playback section discussed above. The descriptions and recommendations are much the same.

SOUNDS

You can assign different sounds to particular system events in this section. Each system event is listed under the main Program box, and to hear the current sound assigned to it (if it has a speaker icon), highlight the item and click the Test button. To assign another sound to the event, choose from the list available under the Sounds box, or click the Browse button and find a .WAV sound file which you can use instead, then click the Apply button and it will now be used for this event.

While system sounds are important in warning you about various things that may be occurring at any time, they take up memory because they are loaded into RAM at Windows startup and stay there most of the time. Therefore I recommend disabling as many unnecessary sounds as you can - highlight the item and select None under the Sounds list then click Apply when done. Unnecessary sounds can include sound prompts for obvious things like the Windows Logon or Logoff sounds, or the sound prompts for features you don't have or don't use, such as the Battery-related, Fax-related or Windows Speech Recognition-related events on PCs which don't use these features. You can even disable the Windows Startup sound by

Copyright © 2010 Koroush Ghazi

unticking the relevant box, and this can help speed up system startup slightly; similarly, I recommend disabling the sound for the Windows Exit event to speed up exiting.

Furthermore, for the sound events you do wish to keep I suggest assigning the same sound to several types of warnings - for example, assign the 'Windows User Account Control' sound to all the other types of system warning sounds including Asterisk, Critical Stop, Default Beep and Exclamation. By assigning the same sound to multiple events you will still get audible alerts of certain events, but you save memory since only one sound has to be loaded into memory, regardless of how many uses it may have.

As you install new programs or features they may add new system events and sounds, so make sure to go through this list every once in a while to refine it and remove unnecessary sounds, and as recommended, try to use the same sound for as many events as possible. Once you've set up the sounds the way you like them, click the 'Save As' button at the top of the box and save your new sound scheme under a suitable name; any changes you make in the future will be saved automatically to this scheme. If you just want to quickly disable all system event sounds select the 'No Sounds' option under the sound scheme area, but note that this doesn't turn off all sound on your system, it simply removes sounds effects from all the system events.

< SPEECH RECOGNITION

This component allows you to configure the Speech Recognition functionality of Windows Vista, which will let you control the computer using voice commands. To use speech recognition, you will require a microphone connected to your system, preferably a good quality one. The Speech Recognition feature is quite specialized, and fortunately Microsoft has provided a lot of resources to both configure and learn more about this functionality, so it won't be detailed here. More details can be found in this Microsoft Document and also by clicking the 'Take Speech Tutorial' link in the Speech Recognition Options box. Most problems experienced with Speech Recognition are due to either using a poor quality microphone and/or being in a noisy environment. For those who don't use Speech Recognition functionality, click the 'Advanced speech options' link in the left pane and make sure the 'Run Speech Recognition at startup' box is unticked.

< SYNC CENTER

The Sync Center is a feature for people working on two or more copies of the same file across different devices or a network. Note that synchronizing across network folders is only possible under Vista Ultimate, Vista Business and Vista Enterprise Editions, and if synchronizing across two computers, both need to be running Windows Vista or newer. When a compatible device is detected, Vista will show it under the list of available Sync Partnerships you can use in the Sync Center. Then when a file is stored on both your PC and the device with which you have a partnership, if one version of the file is changed, Sync Center allows you to synchronize the files, such that the newest version is always maintained in both locations. If there is any doubt - for example if both file locations show a changed version, then Vista will ask you which version to keep. I won't go into more detailed description of the Sync Center functionality here, but bear in mind that synchronization can sometimes take quite a while if you have a lot of shared or offline files.

< SYSTEM

The System component of Control Panel provides central access to a range of functionality, as well as an overview of the system on the main page, showing the details of your CPU and RAM, as well as the specific edition of Vista you are currently running, including whether you have the latest Service Pack installed (which you should - see the Windows Drivers chapter). The actual functions found here are covered in full detail under other chapters. In particular see the BIOS & Hardware Management chapter for Device Manager, Backup & Recovery chapter for System Protection, and Performance Measurement & Diagnostics for the Windows Experience Index.

Copyright © 2010 Koroush Ghazi

The main functionality unique to this area is access to the System Properties box which contains advanced configuration options, and this is covered below. Note that you do not need to open the System component in Control Panel to gain access to the System Properties box; you can access it directly at any time by going to Start>Search Box, typing *systempropertiesadvanced* and pressing Enter. Below are the details of the System Properties box:

COMPUTER NAME

The Computer Name tab is only really useful for PCs connected to a network, since these details are used to make it easier to identify this PC and connect to a network properly. For the average home PC user you can skip this tab; do not alter any of these details.

HARDWARE

You can access Device Manager here. Importantly, you can also set Windows Vista's behavior when a new device is connected and detected. Click the 'Windows Update Driver Settings' button and you will be able to choose whether to allow Vista to 'Check for drivers automatically'; 'Ask me each time I connect a new device before checking for drivers'; or 'Never check for drivers when I connect a device'. As covered under the Windows Drivers chapter, I recommend that you set this to the middle option, namely to force Vista to ask you before checking for new drivers. This gives you more control in case you wish to install an older driver rather than the latest one, or if the latest drivers are known to be problematic for example.

ADVANCED

This section has four main sub-sections, covered below:

Performance Settings: Clicking this button takes you to a set of performance options. Under the 'Visual Effects' tab you can select a range of graphical effects you can enable or disable within Windows, depending on your graphics card's capabilities. In general the fewer of these are ticked, the more responsive Windows usage will feel. Refer to the Graphics & Interface chapter for more details. Under the Advanced tab you can select whether Vista allocates more CPU resources towards the Programs you run, or for 'Background Services' such as the Search Indexer or other scheduled/background tasks. It is strongly recommended that you leave this set to Programs for optimal performance in Vista; only if your system is used primarily for very basic tasks and has a lot of background tasks constantly running should you consider selecting the other option. The Virtual Memory settings accessed here are covered in detail under the Memory Optimization chapter. Finally, Data Execution Prevention is a security feature covered in more detail in the PC Security chapter.

User Profiles Settings: This area allows you to view and if necessary change User Profiles, i.e. the profiles which hold all the Windows Desktop and User Account-related settings for each user. There should be at least one User Profile here for you, and one for every other user. You can Delete or Copy a profile if you wish, though this should be done with caution. Clicking 'Change Type' allows you switch between a Roaming and Local profile if on a network, but for the average home PC user you cannot do this.

Startup and Recovery Settings: These settings control the display of the Windows Boot Menu and Advanced Recovery Options menu when applicable, and they are covered under the Boot Configuration and Backup & Recovery chapters respectively. The System Failure functionality is covered under the Performance Measurement & Diagnostics chapter.

Environment Variables: This button accesses a set of variables which are all configured by Windows Vista when it first installs, and for the most part are always set appropriately. You should not change these unless you have specific knowledge of what it is you are about to change. Many of them can be changed using the MSConfig utility - see the Boot Configuration chapter.

Copyright © 2010 Koroush Ghazi

SYSTEM PROTECTION

The features here are covered under the Backup & Recovery chapter. I strongly recommend keeping System Protection enabled on your main Vista drive.

REMOTE

This tab allows you to configure how a remote (outside) connection to your PC is controlled. The main purpose for remote connections is when someone in another location on the same network wants to control your PC, for the purpose of troubleshooting a problem you're having for example, or to access resources on your machine directly as though they were sitting in front of your machine. While this is an extremely useful feature when you're on a trusted network (e.g. your work network), it is a security risk for home PCs or when you are on an untrusted network. I strongly recommend that you disable (untick) the 'Allow Remote Assistance connections to this computer' option and only enable it when prompted by a technical support person from a trusted company (e.g. Microsoft or your hardware manufacturer). I also recommend setting the Remote Desktop option to 'Don't allow connections to this computer', and only manually configure this to allow particular users - click the 'Select Users' button - if once again you are dealing with a trusted individual. Leaving these features enabled when you don't use them is a security risk. There are also relevant services you can disable, so see the Services chapter.

< TABLET PC SETTINGS

This component of the Control Panel allows you to configure a Tablet PC. Such functionality will not be covered in this book.

However there is one component of the Tablet PC functionality which all Vista users may benefit from: it is called the Snipping Tool, and if you haven't uninstalled the Tablet PC component from Windows - see the Programs & Features section further above for details - then you can access it by going to Start>All Programs>Accessories, or by going to Start>Search Box, typing *snipping* and pressing Enter. The Snipping Tool allows you to take a screenshot of whatever portion of the screen you select, and you can then edit the image immediately, email it to someone or save it as a normal .JPG image.

< TASKBAR AND START MENU

The Taskbar is the bar which sits at the bottom of the Windows screen by default, and the Start Menu is the main menu which opens when you click on the circular Start button with the Vista logo on it at the far left of the Taskbar. There are a range of features which can be customized here, and they are detailed as follows:

TASKBAR

The Taskbar contains the Start button, Quick Launch area, buttons for any open programs, and the Notification Area at the far right. Below are brief descriptions of what each of the functions in this tab do, along with recommendations:

Lock the taskbar: When ticked it prevents accidental resizing or movement of the Taskbar. When unticked, you can left-click and hold on the Taskbar and drag it to reposition where it sits, you can resize it to make it thicker or wider, and you can also resize the components on it such as the Quick Launch bar. Once you're done customizing the Taskbar, make sure to tick this option again for normal daily use to prevent accidental resizing or movement. Note, you can also lock or unlock the Taskbar quickly at any time by right-clicking on the Taskbar and ticking or unticking 'Lock the Taskbar' from there.

Auto-hide the taskbar: When ticked the Taskbar is automatically hidden whenever your mouse is elsewhere on the screen, and only shown when you move your mouse to the bottom of the screen. Set to suit your taste.

Copyright © 2010 Koroush Ghazi

Keep the taskbar on top of other windows: If ticked, the Taskbar is always displayed on top of all open Windows for easy access; it can never be obscured. If unticked you may have to go back to your Desktop at any time to regain access to the Taskbar. For that reason I recommend keeping this option ticked.

Group similar taskbar buttons: If ticked, multiple buttons from the same or similar applications will be grouped together into one button. For example multiple open documents in a word processor will show up as only one button with a number indicating how many of that type the button contains. This can help reduce clutter but it can also reduce speed of access to individual documents or applications. Set to suit your taste.

Show Quick Launch: The Quick Launch bar is the section on the Taskbar where small shortcut icons representing various applications can be placed. These allow you to quickly launch particular programs by clicking the relevant icon, or by pressing the WINDOWS key and a numerical key corresponding to the order of the item on the Quick Launch bar (e.g. press WINDOWS+2 to launch the second application from the left on the bar). In general you should keep the Quick Launch bar enabled, but if you want to remove it, untick this option. If you want to resize or reposition the Quick Launch bar, make sure the 'Lock the taskbar' option is unticked then move the Quick Launch bar left or right, and you can also drag its small 'grip' area to widen or shorten its length. To remove a component from the Quick Launch bar, left-click and hold down on the component, then drag it off the bar. To add a component, drag a shortcut onto the Quick Launch bar. You can also rearrange the order of the icons shown in the Quick Launch bar by moving them around as required. Note that you can add other toolbars to the Taskbar aside from the Quick Launch bar - see Toolbars further below.

Show window previews (thumbnails): If ticked, shows small preview images of what each button on the taskbar represents when your mouse hovers over them. While this can be handy, they can also get in the way at times, and in general the title on the Taskbar open application buttons should be sufficient to tell you what each one is.

START MENU

The Start Menu is an important component of Windows, and is accessed very often so you need to make sure it is configured correctly. To begin with, you have two choices - whether to use the Vista Start Menu, or to use a Classic Start Menu which looks the same as under Windows XP. I strongly recommend the Vista Start Menu as it has very useful features such as the Search Box. Throughout this book and in this section it is assumed that this is the version of the Start Menu being used.

At the bottom of this box you can choose two options:

Store and display a list of recently opened files: If this option is ticked, the 'Recent Items' menu in the Start Menu will display all your recently opened files (documents, music files, pictures etc.). If unticked, nothing will be shown under Recent Items. Set to suit your taste.

Store and display a list of recently opened programs: If this option is ticked then your most recently opened programs will be shown in the main Start Menu area. The number of these displayed depends on the 'Number of recent programs to display' setting found further below.

By default the Start Menu may not contain all the items you want, and usually contains far too many items you don't want which makes it large and unwieldy. So once you've selected the Start Menu type, click the Customize button and examine the details and recommendations below. Note that some items have the option of 'Display as a link' which means the item will be displayed as a clickable link on the Start Menu; 'Display as a menu' which means that clicking the item on the Start Menu opens up a sub-menu of options instead; or 'Don't display this item' which completely removes it from the Start Menu. Any changes you

Copyright © 2010 Koroush Ghazi

make will only come into effect if you click OK then click Apply. Below are option descriptions and recommendations:

Computer: This option controls whether the Computer item appears on the Start Menu. Clicking this option or menu opens Windows Explorer, and generally this isn't a necessary item. You can open Windows Explorer much more quickly using a Quick Launch icon or by pressing WINDOWS+E at any time for example.

Connect To: If ticked this option places a 'Connect To' link on the Start Menu which when clicked allows you to choose a network to connect to. If you're not connected to a network of PCs, untick this option.

Control Panel: This item allows quick access to the Control Panel, either as a menu or a link. I recommend selecting 'Display as a link', since the menu version can be quite large.

Default Programs: If ticked places a 'Default Programs' link on the Start Menu which accesses the Default Programs options - not necessary for daily usage, and can be readily accessed from Control Panel when needed anyway so untick.

Documents: This option places a Documents item on the Start Menu which links to your *\Users\[username]\Documents* folder. I recommend selecting 'Display as a link' so that you can quickly navigate to the particular documents under it when required.

Enable context menus and dragging and dropping: I strongly recommend that this option be ticked, as it allows you to move around and add or remove items from the Start Menu just as you would in Windows Explorer. It also allows you to use the right-click context menu on the Start Menu items, which is important if you want to rename icons, pin/unpin items or run them as Administrator from the Start Menu easily.

Favorites Menu: If this option is ticked, your Internet Explorer Favorites menu will be displayed on the Start Menu as a menu. If you don't use Internet Explorer as your default browser you may want to untick this.

Games: This item will take you to the contents of Games Explorer which shows installed games on your system, both the default Windows games as well as third-party games you have installed yourself. Set to suit your taste.

Help: If ticked, the 'Help and Support' link is shown on the Start Menu. I strongly recommend ticking this option and making use of the help functionality when you have a question about a feature. Alternatively if you disable this, you can bring up Help and Support at any time by pressing WINDOWS+F1.

Highlight newly installed programs: If ticked this option will highlight in orange the directory and launch icon for recently installed program(s) on the Start Menu. This generally isn't necessary but set to suit your taste.

Music: Determines whether a menu or link is shown to your *\Users\[username]\Music* folder or not. Set to suit your taste.

Network: If ticked displays a Network item on the Start Menu which when clicked takes you to a list of available network drives. Untick unless you are on a network.

Open submenus when I pause on them with the mouse pointer: I recommend that this option be ticked, as it allows you to open a submenu or directory link in the Start Menu just by hovering your mouse over it; otherwise you will have to click on the item to open the menu.

Copyright © 2010 Koroush Ghazi

Personal Folder: This displays an item or menu on the Start Menu with your username as its title. When clicked on or hovered over, it opens up the contents of your entire *\Users\[username]* directory. Generally not necessary if you already have the relevant subfolders (i.e. Documents, Music, Pictures) as items on the Start Menu.

Pictures: Determines whether a menu or link is shown to your *\Users\[username]\Pictures* folder or not. Set to suit your taste.

Printers: If ticked a Printers item will be placed on the Start Menu, which when clicked launches the Printers component which allows management of printers and print jobs. Untick if you don't have a printer.

Run Command: If ticked this places a 'Run...' item on the Start Menu, which when clicked opens a Run box for entering command line commands. This item is very useful, although note that you can bring up a Run box at any time by pressing WINDOWS+R. Note further that the default Search Box in the Start Menu can also execute commands in a similar manner to the Run box.

Search options: The following items all control the default search behavior of the Search Box in the Start Menu. Depending on which of the below are ticked, a particular search phrase will be searched for and presented under certain category headings:

§ Search communications - Searches through communications-related files, namely email.
§ Search favorites and history - Searches through Internet Explorer Favorites and History.
§ Search files - The sub-options here allow you to not search through files; search the entire Search Index; or only search through the current user's personal folders.
§ Search programs - Searches through installed program names.

In general you should at least tick Search Programs, and for Search Files set it to search the entire index. If you haven't enabled the Search Index or restricted the index in some way this will result in not finding all relevant files - see the Windows Search chapter for details.

Sort All Programs menu by name: If ticked, your All Programs menu in the Start Menu will have all the items automatically arranged in alphabetical order. This is recommended, however if you wish to rearrange things manually untick this. Note that when this option is selected, the 'Sort by name' context menu item will not appear when you right-click on any item in All Programs; with it disabled, the context menu entry will reappear, allowing you to manually force a sort by name whenever you wish.

System Administrative Tools: The Administrative Tools covered earlier in this chapter can be displayed or removed here. Generally it is not necessary to display them here, as they aren't used all that often and can be easily accessed through shortcuts to individual components, or via the Control Panel.

Use large icons: If ticked, the main items in the Start Menu will use the default larger icons. Unless you're running a very high screen resolution, I recommend unticking this option to force Vista to use smaller icons. In return you can fit more items in the Start Menu and in my opinion makes it easier to navigate.

Number of recent programs to display: If you have ticked the 'Store and display a list of recently opened programs' item, then this determines how many recently opened programs will be shown in the main Start Menu area. Set to suit your taste.

Show on Start Menu: These two options, namely 'Internet Link' and 'Email Link' pin the relevant programs chosen in the drop boxes at the top of your Start Menu. The default programs are Internet Explorer and Windows Mail, but you can set other programs by making sure they're available under the Default Programs area of the Control Panel (see further above in this chapter). If you don't want one or either of these links

Copyright © 2010 Koroush Ghazi

automatically shown on the Start Menu (e.g. if your default browser is still not showing up in the list) then untick the relevant boxes.

Once you've made all your changes, click OK then make sure to click the Apply button on the main Start Menu tab otherwise you will not see your changes applied to the Start Menu. Note that you can manually reorganize or change the shortcuts and folders shown in the Start Menu by going to the following directories:

\Users\[username]\AppData\Roaming\Microsoft\Windows\Start Menu
\Users\All Users\Microsoft\Windows\Start Menu

Any changes you make to the second directory will affect all users on the machine.

NOTIFICATION AREA

The Notification Area was previously known as the System Tray in earlier versions of Windows. It contains icons from some of the currently running programs, warnings or notifications from programs and Windows, and the System Clock, Network indicator and Volume Mixer icons.

Hide Inactive Icons: When ticked the Notification Area hides icons for particular programs or notifications which are not urgent or necessary to draw attention to, both to reduce annoyance and make sure Taskbar space is not unnecessarily taken up. When holding hidden icons, the Notification Area will show a small white arrow which you can click to show all hidden icons. It is wise to minimize how many background programs and hence icons in the Notification Area there will be. Some icons can also be removed by configuring the relevant program or utility, and looking for a 'System Tray' or Notification option to turn off, such as those for Windows Defender or the Security Center discussed under the PC Security chapter.

Regardless of how many programs you have running in the background, there may still be some icons shown here which you may wish to hide (or show). For example some types of hardware will place a 'Safely Remove Hardware' icon in the Notification Area. This icon is not always needed but cannot be removed, so you can hide it instead. The same with the Windows Sidebar icon which is not really necessary, since you can always access Sidebar options by right-clicking on the Sidebar area itself. I recommend ticking this option and clicking the Customize button to manually adjust which icons are always shown, which are always hidden, and which are hidden after a period of inactivity. If in doubt, leave an item at its default which is usually 'Hide when inactive'. Again, hiding an icon does not remove the program from memory, so as recommended in the Startup Programs chapter, make sure to remove unnecessary startup programs and also go through existing programs to remove unnecessary Notification Area/System Tray icons properly.

System Icons: Here you can select which of the four types of permanent system icons usually shown in the Notification are displayed or removed. This includes the System Clock, the Volume Mixer icon, the Network Animation icon and the Power icon for mobile PCs. I generally recommend all available options here being enabled as they provide valuable information on core Windows features.

TOOLBARS

A Toolbar is a portion of the Taskbar which contains specific functionality. By default the Quick Launch toolbar is enabled, and is discussed further above. It is quite handy for quickly launching commonly used programs, or even commonly used files or folders. You can however add several additional built-in Toolbars, including:

Address: If ticked this places an Internet Explorer address box on the Taskbar, and any text you enter will be launched as a URL in a new browser window.

Copyright © 2010 Koroush Ghazi

Windows Media Player: When ticked, this allows Windows Media Player to sit in 'Mini Player' mode when it is open and minimized to the Taskbar, which is recommended. See the Windows Media Player chapter for more details.

Links: This item places a Links box on the Taskbar if ticked, allowing you to select any custom Internet links you've placed there. Any links you select will be launched in an Internet Explorer window.

Tablet PC Input Panel: If ticked this places an icon on the Taskbar which when clicked opens the Tablet PC Input Panel.

Desktop: If selected, when clicked this item opens a list of Desktop icons you can select to launch, as well as links to common resources including the Control Panel and your user folders.

Quick Launch: This item is covered in more detail under the Taskbar section further above.

Note that at any time you can quickly add or remove Toolbar items by right-clicking on the Taskbar and select the Toolbars menu item. You can also create your own custom Toolbar by clicking the 'New Toolbar' item and selecting a program, file or folder to link to.

< TEXT TO SPEECH

Text to Speech is a function which allows Windows Vista to use a synthesized voice to read text on the screen out aloud through speakers or a headphone. To change the voice used for Text to Speech, select a voice under the Voice selection box. The default Microsoft Anna is the best choice as it uses a more natural sounding voice than the older voice engines. To preview the selected voice enter some text in the box below then click the Preview Voice button - don't just press the Enter key after entering the text as this will exit the program. You can adjust the voice speed using the slider further below.

By itself the Text to Speech component does not allow you to enable the functionality required to actually read out any text on the screen under normal circumstances. To actually have Vista read out portions of the screen aloud using the Text to Speech voice, you will need to enable the Narrator, found under Control Panel>Ease of Access Center, or by going to Start>Search Box, typing *narrator* and hitting Enter. Basic details of how to use Narrator are in this Microsoft Article.

More details of this functionality and for additional voices you can download see the Microsoft Speech Site. Additional voices are available at places like ByteCool.

< USER ACCOUNTS

User Accounts are a way of allowing more than one person to use the same PC in isolation of one another. Thus two or more people can have different background wallpapers, different mouse settings, and different files and documents all stored on the same machine, separate from each other (under their own *\Users\[username]* directory) and without impact on, and without access to, each other. However User Accounts are not solely designed for sharing purposes; even if there is only ever one user of the PC, you will still need to have at least one User Account. When you first install Vista, a default User Account with Administrator privileges is created with the username and password (optional) you choose just prior to finalizing installation. Every time you start using Vista from then on, this User Account is used by default unless you create others.

It's important to understand the privilege levels given to User Accounts. In Vista there are three main types of User Accounts: Guest, Standard and Administrator. Each has different privileges - when using a Guest or Standard account, by default various actions are initially blocked by the system due to insufficient privileges. This is done to prevent these users from viewing or deleting each others' files for example, or

Copyright © 2010 Koroush Ghazi

installing or running certain programs or making system-wide changes that can destabilize or harm the entire system. An Administrator level account on the other hand can undertake a full range of actions, from installing any program and making system-level changes, to viewing the files and folders of other User Accounts on the system (if they are not password-protected accounts). Administrators can also create, change or delete new or existing User Accounts. While some systems may not have any Standard User Accounts, there must always be at least one Administrator User Account on the system to be able to manage it - which is why Vista creates one by default immediately at the end of Windows installation. There is also another built-in Administrator account which is disabled and hidden by default and discussed under the Advanced section further below.

The problem is that an Administrator level account is so powerful, it also poses a security risk if used on a day-to-day basis as the default account. If the system is compromised by malware, or physically accessed by another person, they can do anything they want while logged in under an Administrator-level account. So for security purposes, it has long been recommended by Microsoft that even sole users of a PC create two accounts; one Administrator and one Standard, and use the Standard account for day-to-day purposes, and then login to the Administrator account only to do more system-intensive tasks. Unfortunately this has usually been such an inconvenience that most people run as Administrator users the whole time.

Vista's solution to this dilemma is called User Account Control (UAC), and is covered in more detail under the PC Security chapter. Basically it means that whether you're logged in with an Administrator or Standard User Account, you are actually running with only Standard account privileges. Then, whenever you do something which requires Administrator-level privileges, a UAC prompt appears asking you to either click the Continue button (if you're an Administrator) or enter the Administrator password (if you're a Standard user) to elevate your privileges in order to complete the task. Thus Administrator privileges are only granted on an as-needs basis, helping to prevent malware programs launching or making changes in the background without your knowledge, and also preventing other inadvertent or unauthorized system changes.

While many people hate UAC and its incessant prompting, the benefits of UAC - and I strongly recommend that you keep it enabled - are that you don't need to create additional User Accounts and switch back and forth for optimal security, nor do you need to expose yourself to the major security risks of running the Administrator account on a regular basis as has been in the past; you can now run an Administrator account as your main account, and through UAC, benefit from having tighter security as well.

What follows is my advice on how to set up User Accounts on your system based on four common scenarios.

USER ACCOUNT SCENARIOS

When you are setting up User Accounts in Vista, you must first decide on how many people you want to provide access to your machine, and also consider whether the PC is readily accessible by others or is relatively isolated from physical access. The number of users is an obvious factor, but the second variable has to do with the fact that a PC which can be physically accessed by other people you don't necessarily trust requires much tighter security than one which is physically isolated. Below are my recommendations for the various general scenarios and the best way to configure one or more User Accounts to suit:

Single user, isolated machine: If the PC only has one main user and is not accessible by untrusted individuals then the default User Account created by Vista during installation is sufficient. For maximum convenience this Administrator level account can also do without a password, which provides the fastest startup into Vista as you won't see a login screen.

Single user, accessible machine: If the PC has only one main user, but other people who are not necessarily trustworthy can physically access it, or you are worried about sensitive information and potential theft, then the default User Account created by Vista is sufficient but you must assign a strong password to the account - see the Backup & Recovery Chapter for details. The password will need to be entered at the login screen

Copyright © 2010 Koroush Ghazi

each time you start up Vista, and as long as the password is quite strong, this will prevent others from gaining access. You may also wish to use EFS Encryption and/or BitLocker if the data is valuable and/or the threat of physical access or theft is quite high - see the PC Security chapter.

Multiple users, isolated machine: If the PC has more than one user but is only physically accessed by trusted people such as close family members, then I recommend creating a Standard User Account for each of the additional people who will be using the machine, and keeping the Administrator account for yourself to use. However importantly you must now use a password for your Administrator account and you must also enable UAC. Aside from malware risks, a password and UAC are required to prevent the other User Accounts from making system-wide changes which may destabilize or harm the PC, and it also allows you to use the Parental Control features detailed further below. Note that the Standard accounts themselves don't have to have passwords, but it is recommended that they do in case one user accidentally (or purposely) logs in under another user's account and makes undesired changes. Keep in mind that Standard accounts which don't have passwords can have the contents of their personal folders viewed by Administrators; if password protected, personal folders cannot be viewed by anyone else.

Multiple users, accessible machine: If the PC has more than one user, but is also physically accessible by a range of people who you may not completely trust, or there is greater risk of theft, then I recommend the same procedures as the scenario above, however the Administrator password must be made very strong, and the Standard account passwords should also be made quite strong. Individual users may also wish to use EFS Encryption for sensitive files or folders. In addition, if you want to allow an untrusted person limited access to your machine (e.g. for basic web browsing), then turn the Guest account on as well and ask them to use that - they won't be able to change any settings or access your personal files using the Guest account, as it is extremely limited. UAC must be enabled at all times in this scenario for maximum protection against unauthorized changes to your system and to help prevent accidental or deliberate installation of malware.

Note that on a PC with multiple user accounts, you can quickly switch between accounts without restarting the machine by pressing CTRL+ALT+DEL and selecting 'Switch User'. You can also go back to the main logon screen by selecting 'Log Off' instead of rebooting. Once again, if you aren't clear on how UAC works, or want to know about additional ways you can customize both UAC and User Account-related security to suit your specific needs, see the User Account Control and Local Security Policy sections of the PC Security chapter for more details and tips.

MANAGING ACCOUNTS

Once you've decided on the best strategy, you will need to create, delete or modify existing User Accounts to suit your needs. This is done by first logging in as an Administrator, then going to the main User Accounts screen. Here you can either edit your own account, or by clicking the 'Manage another account' link, you can edit the details of any other accounts on the system. Below are the typical range of options shown when managing an account:

Create a new account: This allows an Administrator to create a new account, assigning it a name and an account type. I strongly suggest only creating as many additional Standard accounts as you actually need. Unused accounts will simply take up drive space for no purpose, as each account automatically has a set of personal folders created for it. Remember also that the more Administrator accounts you have, the more likelihood there is that a user can cause unintended harm to the system, or inadvertently allow malware onto the system. For that reason if you do wish to have more than one Administrator I strongly recommend enabling UAC and having strong passwords on all Administrator accounts. Generally it is best to only have one Administrator account - the default one created by Vista. For power users there is also a hidden Administrator account which is discussed further below.

Delete the account: You can delete any account except your own. This is obviously something that should done with caution, since deleting an account not only deletes all that account's saved preferences, it can also

Copyright © 2010 Koroush Ghazi

delete all their personal files and folders. For this reason you will be asked whether you wish to save the account's personal files to a new directory before deletion, but you will not be able to save their emails and personal settings.

Create a password: If the account doesn't have a password and and you need to create one, then click this link and enter an appropriate password. Importantly, if you lose or forget the password for an Administrator account you will need someone with another Administrator account on the same machine to help you - if another Administrator doesn't exist you will be in serious trouble - see the Backup & Recovery Chapter for recovery options. If a Standard User Account forgets their password, an Administrator can click the 'Change the password' or 'Remove the password' link as appropriate to fix this. To change your own password at any time press CTRL+ALT+DEL and select 'Change a password'.

Change the picture: By default each User Account has a small picture attached to it to make quick identification of different accounts easier on the login screen and at the top of the Start Menu among other places. Select one from the list shown, or to use your own custom picture click the 'Browse for more pictures' link at the bottom of the images and find an appropriate image to use. Note that you can access the User Account properties window by going to Start Menu and clicking your User Account picture at the top.

Change the account name: You can change an account name, including your own, at any time if you are an Administrator. However aside from causing confusion at login time, it also causes further confusion because the actual name of the personal folder for the relevant user found under the *\Users* directory will not be changed; it will remain as originally set, while the version of it shown under My Computer will change to the new name. For this reason it's not recommended that you change account names unless absolutely necessary.

Change the account type: An account can be changed from Administrator to Standard user and vice versa, though this is obviously something which should be done with caution. I don't recommend changing the first default account created under Vista to a Standard user as this can cause major problems.

Guest account: You can select whether to turn the Guest account on or off, and in general it should remain off. It is only to be used if you wish to give temporary access to a user who will then be able to use your machine in a very limited capacity, unable to access or alter any personal files, nor able to change any system settings or install software or hardware. It is still a security risk when left on, and also forces the logon screen to appear unnecessarily even if you only have one other account, so turn it off until it is truly needed.

PARENTAL CONTROLS

One of the options under the account management section (as well as in the Control Panel) which an Administrator can use is 'Set up Parental Controls'. Since one of the most common uses of User Accounts is by parents who wish to restrict their kids from making a big mess of the family computer, this set of controls is extremely handy - but it is not just for managing kids. Parental Controls allows you to lay down certain additional limitations on any Standard User Account, and these are described below:

Activity Reporting: If enabled, the user's activity will be logged. You can view these logs here by clicking the 'View activity reports' link at the right of the screen. You can see more details by browsing the log categories in the left pane.

Windows Vista Web Filter: The web filter allows you to manually allow or block specific websites by address, as well as setting a general restriction level of None, Medium or High. To specify the exact type of content you want to block, click the Custom option and select the categories to be blocked. Keep in mind that the rating system is not perfect, it is based on the Windows Live Family Safety service, so material which you may find offensive may still slip through if you rely solely on the rating system; it is not foolproof, but it

Copyright © 2010 Koroush Ghazi

should be quite robust. You can even tick the 'Block file downloads' option to prevent any files being downloaded to the machine.

Time limits: You can specify the time of day in one hour blocks that this user is not allowed to logon to the PC, for every day of the week. Any areas shaded with a color block mean the user will not be able to use the machine at that time.

Games: This area lets you select firstly whether the user can play any games at all, and then you can block games with particular ratings - these should be set to match your local region's rating scheme. You can choose either to allow or block unrated games, but note that some (mainly older) games may be unrated regardless of their content type. You can then manually specify the games you wish to block or allow, in the case of exceptions which aren't handled appropriately by the ratings scheme for example.

Allow and block specific programs: If you wish to block the user from being able to run particular programs, click the '[user] can only use the programs I allow' and then select from the list of all installed programs shown. If a program file is missing from the list, click Browse and go to its directory then select it.

As you can see, these controls can be used not just for kids but also to prevent certain users from running specific programs or accessing certain websites which may be harmful, or even if you just wish to monitor a particular user's activities.

ADVANCED USER ACCOUNT PROPERTIES

There is another area of User Account options which you can access by going to Start>Search Box, typing *control userpasswords2* and pressing Enter. The options provided here are more advanced than those provided under the normal User Accounts area, and require much more caution as you can easily delete or ruin a User Account or create a major security risk if you're not careful. If in doubt do not alter anything here. Below are the descriptions for these settings:

Users must enter a user name and password to use this computer: If your system is only using one account - the default one created at Vista startup - and you have not set a password, then in effect you won't have to enter a username or password at any time regardless. However if you have two or more User Accounts then unticking this option means that the account which is shown highlighted (and which you can select while the box is ticked) will become the default account. This account will then automatically login each time you start Vista. This is a major security risk and is not recommended unless you are the sole user of the machine and the machine is in a physically secure environment.

Users for this computer: This area lists all the User Accounts on this PC. You can add or remove accounts here, though it is not recommended. Highlight an account and click Properties; aside from letting you change the name and description of the account, under the 'Group Membership' tab you can not only select whether to set this as an Administrator or Standard account, you can select one of the other more specialized sub groups which have specific limitations. For example you can select the 'Power User' group which provides more privileges than a Standard User and less than an Administrator. To add these groups to the list of selectable account types in the main User Accounts box, see the Advanced user management option below.

Reset Password: Allows you to set a new password for the highlighted User Account (if it has one), but to change your own password press CTRL+ALT+DEL and select 'Change a password'.

The following options are under the Advanced tab:

Manage Passwords: This option allows you store and backup various passwords - see the Backup and Recovery chapter for more details.

Copyright © 2010 Koroush Ghazi

Advanced user management: Clicking the Advanced button opens the Local User Management box. Click the Users or Groups item in the left pane and you will see list of current users on the system, as well as the available group types.

Importantly, you will see under Users that aside from your own User Account and any you've created, there is also an account with the username 'Administrator' - this is the built-in Administrator account in Vista, and is different to the one created during Vista's installation. This Administrator account is not available by default and is very powerful, since it has no password, allows complete access to the system and is not affected by UAC - which is precisely why it's hidden by default. Double-click the account and you can untick the 'disabled' box to enable it and it will now be available for login and configuration as a normal User Account. I must stress that you should not use this account regularly as it is a major security risk, since it is not protected by a password, nor is it affected by UAC. A user logging in under this default Administrator account is leaving a major security hole open. The primary use for this account would be for troubleshooting purposes, or to more easily perform a large number of system intrusive tasks which would otherwise result in lots of prompts and file permission/ownership alterations.

Secure Logon: If you wish to have added security, you can tick the 'Require users to press CTRL+ALT+DELETE' box, and thus whenever anyone tries to logon on this PC, they will first have to press the CTRL, ALT and DEL keys together to bring up the logon screen; it will not display automatically. This increases security because it places the logon screen in Secure Desktop mode (See User Account Control in the PC Security Chapter), meaning that the logon screen cannot be faked by malware to capture your login details for example. This level of security is not necessary for the average home PC user.

< WELCOME CENTER

The Welcome Center is a central location showing the exact edition of Vista you are using, a brief snapshot of your PC's basic system specifications, as well as a range of Vista options and Microsoft offers. It is shown by default the first time you start Windows Vista and every time after that, and in general it is not necessary at all since all of the information and utilities it contains are available from various places in Vista. I recommend disabling the Welcome Center to speed up Windows startup - untick the 'Run at startup' box at the bottom of the Welcome Center then close it.

< WINDOWS CARDSPACE

Windows CardSpace is form of digital identity verification 'Card' which you can use online rather than a username and password combination. You can create a Personal Card or a Managed Card, with Personal Cards being less reliable and less likely to be accepted for important transactions since they rely on you to enter and store all the details on your own PC (though the data is encrypted); Managed Cards on the other hand are created by a third-party provider who manages the card for you and thus verifies who you are. Full details of how CardSpace works are in this Microsoft Article. Whether you use CardSpace is up to you. To start with you should have no need to set this system up until you encounter a site which uses it; you can then decide whether to proceed, and whether to only use Personal Cards or set up a Managed Card as well.

< WINDOWS DEFENDER

Windows Defender is a security feature which is covered in detail in the PC Security chapter.

< WINDOWS FIREWALL

The Windows Firewall is a security feature which is covered in detail in the PC Security chapter.

< WINDOWS SIDEBAR

The Windows Sidebar is a visual feature and is covered in detail in the Graphics & Interface chapter.

Copyright © 2010 Koroush Ghazi

< WINDOWS SIDESHOW

Windows Sideshow is a feature only available in Vista Ultimate, Vista Home Premium and Vista Business. It allows a user who has connected an external device with a display to show a range of information on this device without turning the PC on. This feature is not covered in the book.

< WINDOWS UPDATE

Windows Update is the main tool used to obtain security patches, as well as driver and feature updates in Windows Vista. Unlike Windows XP, Vista users do not need to access the Windows Update website for this functionality. By default Windows Update prompts you to allow a scheduled check of the Microsoft site for updates every day, and to download and install them automatically as required.

The information Windows Update sends to the MS site during an update is as follows:

§ Computer make and model
§ Version information for the operating system, browser, and any other Microsoft software for which updates might be available
§ Plug and Play ID numbers of hardware devices
§ Region and language setting
§ Globally unique identifier (GUID)
§ Product ID and product key
§ BIOS name, revision number, and revision date
§ Your Internet Protocol (IP) address

Full details of what information is collected and how it is used are in this Microsoft Article.

To customize the Windows Update settings, click the 'Change settings' link in the left pane. The main choice is under the 'Choose how Windows can install updates' section. If the 'Install updates automatically' option is enabled, set it to check for updates 'Every day' at the time when you are most likely to be connected to the Internet. This allows Windows Update to check for updates and download and install important updates such as security patches and fixes. If you also want Windows Update to download and install 'recommended' updates, which includes driver updates and compatibility patches, tick the 'Include recommended updates' link at the bottom of the screen. Configuring Windows Update to undertake automatic updates in this way is recommended for those who are more forgetful, or who are less experienced and want to remain up to date and secure.

For medium to advanced users I recommend selecting the 'Check for updates but let me choose whether to install them' option instead. This includes ticking the 'Include recommended updates' box. The reason for this is that it provides the best of both worlds: Vista will check for updates daily so that you don't have to remember to do so manually, but it will not download or install anything without your permission - instead you will see a small Windows Update globe in the Notification Area at the bottom right of the screen. You can then click it to open Windows Update and then click the 'View available updates' link to see the details of updates, and select which update(s) you want to install. Then simply click the Install button and they will be downloaded and installed. If you've unticked an individual update component and don't want to see it again, right-click on it and select 'Hide update'. This gives you greater control over what you are installing on your system. Obviously all important updates should be installed, and if you do see any optional updates of interest, they are usually safe and worth installing (e.g. driver updates).

I do not recommend selecting 'Never check for updates'. Windows Update is a very important part of keeping Vista up to date and secure, and as such should never be completely disabled. If you are in an environment where you need to control access to the Internet, then read this Microsoft Article. If you do

Copyright © 2010 Koroush Ghazi

insist on disabling update checking, then you must check Windows Updates manually every couple of days by opening it and clicking the 'Check for updates' link in the left pane; clearly this requires a lot of discipline. Failing to check Windows Updates regularly opens your system up to recent security exploits and vulnerabilities, which nowadays can quickly circulate around the Internet within days or even hours. For maximum security you must always install the latest important updates - see the PC Security chapter for more details of the importance of PC security.

To view the updates already installed on your system via Windows Update at any time, click the 'View update history'. To view further details of each update installed, right-click on it and select 'View details'. To remove an installed update, you can click the 'Installed updates' link at the top of the detail update history box.

If you want to download updates for other Microsoft products, click the 'Get updates for more products', but this is not necessary unless you have specific Microsoft products which need regular updating, such as Microsoft Office. You will not get general updates for your installed programs this way; there is no reliable automated method of keeping all your installed programs and drivers up to date, it requires that you keep an eye out for update notifications on various websites, such as the front page of TweakGuides.com.

If you are using Windows Vista Ultimate Edition, you can also select the available list of Ultimate Extras to download here. This includes extras such as BitLocker and EFS Enhancements, Hold 'Em Poker and DreamScene as detailed in this Microsoft Article, as well as under the PC Security and Graphics & Interface chapters.

If you are receiving an error when using Windows Update, check this Microsoft Article. If you cannot get Windows Update to work then in the interim I strongly recommend monitoring the updates on the Windows Security Updates site, and manually downloading and installing any important Windows updates as often as necessary so that the security and stability of your machine is not compromised while you try to resolve this particular problem. The above site is also useful if for some reason you want to download specific Windows update(s) and store or transfer them to another machine.

Finally, by default Windows Update creates a Restore Point prior to installing new updates, so I strongly recommend leaving System Protection enabled to allow this to happen, as it provides an extra layer of protection in case an update goes wrong and you want to put your system back to the way it was before it.

Copyright © 2010 Koroush Ghazi

STARTUP PROGRAMS

Windows loads up a range of programs into memory during its startup procedure, including drivers and programs needed to provide the main functionality in Vista just prior to showing the Windows Desktop or the logon screen. Unlike Windows XP, Vista is designed to try get the user to the Windows Desktop as fast as possible. It does this through the use of features such as ReadyBoot, as well as by loading certain programs, scripts and services in the background with a lower priority and/or loading them after the Windows Desktop has appeared.

Regardless of the improvements in Windows Vista's boot time, removing unnecessary startup programs, services and tasks is still strongly recommended, as it helps to further reduce excessive loading both during and immediately after Windows startup, and more importantly, will reduce unnecessary background resource usage, which in turn improves overall responsiveness, reduces stuttering, and prevents program conflicts and crashes.

In this chapter we look at the correct way to find, identify and properly remove unnecessary startup programs. Details of how Windows Vista's startup behavior is optimized, as well as information on post-startup processes, are provided in the Memory Optimization, Drive Optimization and Services chapters.

< FINDING STARTUP PROGRAMS

The first step in the process is to find the names of all the programs and files which are running at startup on your system. To do this you will need to use one or more of the several tools covered below:

SOFTWARE EXPLORER

Windows Vista has a built-in utility which among other things allows you to view and if necessary disable the main startup programs on your systems. It is available from within Windows Defender, and if Windows Defender is disabled that prevents access to this useful tool - see the PC Security chapter. To access Software Explorer open Windows Defender and click the Tools link, then select 'Software Explorer'.

On the main page of Software Explorer you can select which types of programs to view in the Category box: 'Startup Programs'; 'Currently Running Programs'; 'Network Connected Programs'; and 'Winsock Service Providers'. Regardless of which you choose, make sure to click the 'Show for all users' button so you can see everything and importantly this also allows you to change their status from Enabled to Disabled and vice versa, or to Remove them if applicable. To see further details for any program on the list, click once on the program item and in the right pane its details will be shown. In particular note the 'File Name' field as this is important in correctly identifying the program, and also note the 'Ships with Operating System' field as this tells you whether it was installed as part of Vista, or if it's been installed by a third-party program.

MICROSOFT SYSTEM CONFIGURATION UTILITY

Another built-in Windows utility for additional tweaking and troubleshooting of your system is the Microsoft System Configuration Utility (MSConfig). To access it, go to Start>Search Box, type *msconfig* and press Enter. Its main use is to provide a brief snapshot of key system variables, and provide a means for troubleshooting Windows boot and startup problems. The options under the Boot tab of MSConfig are covered in more detail under the Boot Configuration chapter, the options under the Services tab are covered in more detail in the Services chapter, and the options under the Tools tab are merely shortcuts to other features of Vista covered throughout this book. So below we examine the General and Startup tabs of this utility.

Copyright © 2010 Koroush Ghazi

General: By default when your system is running at full functionality, MSConfig will show the 'Normal startup' item selected. This means all programs, drivers and features are loading up as normal. If you wish to boot up into Safe Mode (See Backup & Recovery chapter) you can select the 'Diagnostic startup' item instead. To perform a quick temporary check to see the impact on functionality and performance of your startup items, you can set a 'Selective Startup' and untick the 'Load startup items' box then click Apply. When you next reboot your system, Vista will start up without loading any of the additional programs it would usually load at startup - only the core Vista features, device drivers and services. You will then be able to see firstly how much of an impact your startup programs are having on startup time, and more importantly on post-startup drive usage. You will also be able to see the types of functionality which is no longer available as a result of these items being removed. This can range from not being able to open certain programs or use certain features of these programs, through to certain Windows features not being available, like the Sidebar.

Make sure to run MSConfig again and reset it back to 'Normal startup' under the General tab, then examine the details below to see how to correctly identify unnecessary startup items using MSConfig.

Startup: This tab under MSConfig shows all the current programs which load into memory at Windows startup. You should note the file path and filename shown under the Command column. The Location column shows where in the Windows Registry the command to run this particular file resides. Any item here can be temporarily disabled by unticking the box next to its name, however this should only be done for testing purposes; MSConfig is not the correct place to permanently disable or remove a startup program.

REGISTRY EDITOR

The Registry Editor is detailed under the Windows Registry chapter. To launch the Registry Editor go to Start>Search Box, type *regedit* and press Enter. Below is a brief run-down of where in the startup items are held in the Registry and how to remove them. The Windows Registry holds a record of the programs to launch at startup, contained in four separate areas:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce]
```

If you find any items listed under any of these keys, it means they are set to run at Vista startup, with those under the `Run` keys being permanent items, and those under `RunOnce` being temporary items which only run for the next bootup. You cannot temporarily disable a startup item here, however to permanently delete any of these items, right-click on it and select Delete. Since there is no undo functionality in Registry Editor, you should consider doing a backup of the registry in part or in full, as detailed under the Backup & Recovery chapter, before deleting any items.

AUTORUNS

Autoruns is an advanced and highly useful free startup file identification and removal utility with unique features not available in the utilities covered above. It also serves a range of other purposes covered throughout this book, so it is a highly recommended program. Download it, extract its contents to an empty folder and run the *Autoruns.exe* file. Under the 'Everything' tab you will see a large number of items which are loaded up with Windows - far more than most other utilities will ever show; this is what makes Autoruns so valuable for a range of purposes. Most of the entries shown are required for various programs to run, and the vast majority are Microsoft items which Windows absolutely needs to function correctly.

Correctly identifying and removing the truly unnecessary items using Autoruns is more complex precisely because it shows so much detail. To narrow down the list to remove core Windows items, go to the Options menu and tick the 'Hide Windows Entries' item, and also make sure there is a tick against the 'Verify Code

Copyright © 2010 Koroush Ghazi

Signatures' item. Then click the Refresh icon on the taskbar or press F5 to update the list under the Everything tab. The list of items shown will be reduced, with only items primarily relating to third party programs showing, making it easier to spot unnecessary items.

One of the key benefits of Autoruns is that it allows you to temporarily disable any item, as well as choosing to permanently remove it. This means that similar to MSConfig, you can temporarily disable specific items to see what impact this has on the functionality for that particular program, as well as on Windows in general. Remember however that Autoruns is listing not only startup programs, but also various components related to a range of programs, including context menu entries, Services, and third party Gadgets. Click on each suspicious item and look in the Details Pane at the bottom of the program for more information, then right-click on it and select Properties and look under the Details tab for yet more details. If still unclear, right-click on the item and select 'Search Online' to initiate a Google search on the item's name in your default browser. A combination of the displayed information plus any additional information on the Internet should allow you to accurately identify what functionality the component relates to.

You can then disable any suspected unnecessary item temporarily by unticking its entry, and Autoruns will prevent that item from loading up the next time Windows starts up. Reboot and test to see the impacts of disabling such items.

< IDENTIFYING STARTUP PROGRAMS

Once you have noted the names of all the startup programs and files using one or more of the utilities above, and you have a reasonable suspicion as to which are unnecessary, the next step is to make sure you correctly identify their functionality and determine whether they are truly necessary. Some features require that a program or certain component(s) load into memory at Windows startup otherwise they may not function correctly or at all. Other times a startup component is not necessary for a program to function properly, or provides optional functionality for particular features you may not use. Some startup items may even be part of malware or other undesirable software and hence must be removed.

Follow the steps below to try to correctly identify all of your startup programs:

1. Some filenames will tell you quite clearly what the startup program relates to. If in doubt, also check the directory path of the file and see if there are any other indications as to which program it relates to. It's important to know the actual program the file is for, firstly so you can tell what functionality may be affected for testing purposes, and secondly for the purpose covered in the next step below.
2. Launch the program which the file relates to and look through its options for settings like 'Load with Windows', 'Load at startup', 'Enable System Tray', 'Enable Shell Integration', and so on. In many cases you will be given the option to disable any such settings, and you may also see text or a warning which explains whether doing so will affect the program's functionality in any major way. Typically disabling a program component from loading at startup means it won't be running in the background after Windows loads; you will have to manually open it yourself. For some programs this is not an issue, and in fact is desirable; for others it can prevent them from working automatically in the background or even from being able to be launched. For our purposes, we want to minimize the number of programs and components running in the background at all times, but not damage the functionality for necessary programs.
3. If the filename still isn't clear, and you can't determine from its directory path which program it relates to (e.g. it resides in the *\Windows\System32* directory) then you will have to do some online research to find out more details. Start by searching one of the following online resources using the exact filename:

   Google
   SysInfo Definitive Startup List
   ProcessLibrary
   Security Task Manager List

Copyright © 2010 Koroush Ghazi

Some of the more obscure or new Windows Vista system files may not be listed in the sources above, or typically have ambiguous or even false information regarding potential malware, so reading through a large number of Google search results is the best method for finding the truth.

4. Run the malware scanners recommended in the PC Security chapter to ensure that none of the startup files relate to malicious software. If any such files are flagged as malware by your scanner, you can usually click on their names or a provided link to find out more details from the scanner's own database.
5. Use MSConfig or Autoruns to temporarily disable the startup item(s) in question - that is, untick it in Autoruns or MSConfig - then reboot Windows and test to see over a period of several days whether any of your regular program or Windows functionality is impaired. If still in doubt, leave the item temporarily disabled for an even longer period, and you should be able to categorically determine after a few weeks whether it is truly necessary.

< REMOVING STARTUP PROGRAMS

Once you've followed all the steps above, and you're confident that you've found a truly unnecessary startup item, the final step involves permanent removal. You can do this in several ways:

§ Go to the program in question and make sure there are no options to disable it from running at Windows startup. As noted further above, if any options such as 'Load with Windows', 'Load at startup' or similar exist, disable them otherwise if you just manually delete the item it may simply be recreated each time you boot into Windows or start that program.
§ Go to Software Explorer>Startup Programs, make to press the 'Show for all users' button and if the item is listed there, highlight it and click the Remove button.
§ Go to Autoruns, right-click on the item and select Delete.
§ Go to the Registry Editor, find the item under the relevant key, highlight it in the right pane and select Delete. Registry Editor does not have any undo capabilities, so it is best used as a last resort, or only if you are completely certain.

Once the item is removed from your startup, you should reboot Windows and re-check to see if it is indeed gone. In a worst case scenario, if at any point any of your programs start to behave strangely or do not function at all, then uninstall and reinstall that particular program and its relevant startup items will be recreated. In general it's also wise not to permanently remove any Microsoft startup programs unless you're completely certain you will never use such functionality.

< STARTUP PROBLEMS

As noted at the start of this chapter, Vista is designed to prioritize boot programs, services and drivers such that the system reaches the Desktop as quickly as possible, and if necessary continues loading programs as required. This means that the removal of startup programs may not visibly improve system startup time. The best way to measure startup time is not to count the number of times the bar scrolls on the bootup screen, as these can vary for any number of reasons; rather you should time the overall Windows startup process. If you want an objective measure of your startup time and/or if you believe you are having startup problems then you can see specific statistics on this in Event Viewer. To view your startup and shutdown times and any associated problems follow these steps:

1. Open Event Viewer.
2. In the left pane go to Applications and Services Logs>Microsoft>Windows>Diagnostics-Performance.
3. Click on the Operational log shown underneath the above folder, and in the centre of the screen you will see a range of events.
4. Typically there will be items with the Task Category 'Boot Performance Monitoring' or 'Shutdown Performance Monitoring' (Event IDs of 100, 200 or similar). Click on the more recent of these to see details - you can click the 'Date and Time' column to sort by date if necessary.

Copyright © 2010 Koroush Ghazi

5. In the Details box the precise startup time (Boot Duration) or shutdown time (Shutdown Duration) is shown in milliseconds (ms), which you can divide by 1000 to get seconds. You may also see which particular program or driver may be slowing down performance, though obviously many of them are necessary and can't be disabled.

For more details about Event Viewer usage see the Performance Measurement & Diagnostics chapter.

< REGULAR MAINTENANCE

Removing startup items is far more important than most people believe. It is not a case of simply boosting your startup time, though it can help to do that. It is actually a critical step in ensuring overall system responsiveness, preventing stuttering and slowdowns, and also preventing potential crashes and conflicts which can otherwise be very difficult to resolve and are often incorrectly blamed on Windows, drivers or the program which is crashing.

It is perfectly normal for almost all systems to have at least a few startup items which need to be kept enabled and serve a useful purpose. However any system which has a long list of startup items is at risk of experiencing performance and stability issues. Remember that the software you use on your system may not have been tested in combination with all the various other background programs you are currently using, so the results can be unexpected. Certainly people using system-intensive applications and games will be the first to trigger any potential conflicts or performance issues in such scenarios, so if you belong in this category, then make absolutely sure you follow the procedures in this chapter and remove all unnecessary startup items and minimize what runs at startup.

Importantly, in the future as you install new programs you should continue to regularly examine and identify new startup items which are being added and remove those which are not needed. I generally recommend that after each installation of any new program you open MSConfig and quickly look under the Startup and Services tabs to see whether new item(s) have been added, and take the time to determine whether these are really needed or not. Though tedious, this is an essential part of regular maintenance on a PC.

Copyright © 2010 Koroush Ghazi

SERVICES

Services are programs that run in the background and support specific functionality in Windows Vista. They can be initiated by Windows itself, or they can be installed and initiated by third party programs. They may start automatically during or immediately after Windows startup, they may be triggered to start or stop by the launching of certain programs or functionality, or they can be blocked from running altogether. Aside from the addition of several new services, the main changes to services under Windows Vista include the ability to specify a delayed start to a service, preventing it from conflicting with Windows startup, as well as security and stability enhancements to isolate services such that they cannot be as easily compromised by outside attackers, nor can then be as easily destabilized by running programs.

Services are user-configurable under Windows Vista, just as they were in Windows XP. This means that there is scope to improve system resource usage and startup time by disabling unnecessary services, and also by setting certain Automatic services to the new 'Automatic (Delayed Start)' setting such that they load immediately after Windows startup, not during. As before, it is wise to learn more about what a particular service does before considering altering its default status. In this chapter we look at customizing services, and I provide safe recommendations for service configuration for the average home PC user.

< SERVICES UTILITY

The built-in Services utility gives you the ability to view and edit your Service configuration. To access the Services Utility, you can either go to Control Panel>Administrative Tools, or go to Start>Search Box, typing *services* and pressing Enter. This opens the Services utility, displaying all installed services by name, showing you whether they are currently running or not under the Status column, and whether they're set for Automatic, Automatic (Delayed Start), Manual or Disabled under the 'Startup type' column.

You can see the details of each service by left-clicking on it and the default Extended view will show the description to the left of the service. To see more details and configure a service, either double-click on the service, or right-click on it and select Properties. Here you can where the actual program file resides for the service, and you can also manually Start, Stop or Pause/Resume a service as applicable. Importantly, you can change its startup type here - the startup type of a service is defined as follows:

- *Automatic:* This service is automatically started during the Vista boot process.
- *Automatic (Delayed Start):* This service begins loading automatically after Vista has reached the Windows Desktop.
- *Manual:* This service must be started manually by the user, or typically as requested by a program when needed. It does not reside in memory nor load at startup otherwise.
- *Disabled:* This service is blocked from running and does not load into memory at any point, even if a program requires it. It can only be started by manually setting it one of the above startup types then clicking the Start button.

DEFAULT SERVICES

Before we move on to service customization, it is important to backup your default service configuration in Vista in case you have any problems and need to return any of your services to their default state. Services may be configured differently on various machines based on the particular features and programs you are using, as well as your specific hardware configuration, so the best thing to do is save your current service configuration. To do this, open the Services utility, then right-click on the 'Services (Local)' item in the left pane and select 'Export List'. In the box which opens, enter a name for the list and save it as the default 'Text

Copyright © 2010 Koroush Ghazi

(tab delimited) (*.txt)' option. This file will then save with all the details of your services as they currently stand, and can then be viewed with correct formatting in a program like Microsoft Excel.

For convenience sake, I have also listed my default Windows Vista Ultimate service configuration in the table further below under the column labeled 'Startup Type (Default)', but again, remember that this will vary from system to system so as a precaution take the steps above before altering your own services.

CUSTOMIZING SERVICES

The Vista Services Control Manager has configured services to ensure full functionality for all the programs and features you use in Windows Vista, including any third-party programs you have installed. While we can customize these further, it is important to note that by setting a service to Disabled you may cause a particular function or feature(s) of Windows or your programs to stop working without warning. If you change several services at once in particular, it can sometimes be extremely difficult to track back your problems to a particular service - not all services are obvious in what they affect. The main aim of customizing services is to:

§ Help speed up Windows startup time especially on systems with slower hard drives.
§ Help reduce post-startup drive activity since Windows relegates some services and programs to loading in the background well after startup.
§ Reduce RAM and CPU usage by preventing unwanted services from running in the background.
§ Prevent program conflicts, instability and even security risks by removing unwanted services.

Keep in mind that altering the service configuration will not increase your framerate in games (though it may reduce stuttering), it will not have a significant visible impact on visible RAM usage because SuperFetch takes up any slack, and it can impair your functionality if not done carefully. It is not something to be taken lightly - it does have benefits, but they won't necessarily be dramatic. Windows Vista's default service configuration is already quite good; most unnecessary services are set to Manual, meaning they already don't use up any extra resources and will only start if required.

With all of the above in mind, on the next few pages are a list of the services in Windows Vista, the defaults for Vista Ultimate and my recommendations for any services that can be changed on an average standalone home PC not connected to a network of other PCs, but retaining full Internet functionality. This configuration should be safe on most PCs, however if your system is unique in some way, or is on a network of PCs, make sure to read the descriptions for any service in the Services utility before altering it.

Important: There are some unnecessary services which are already set to Manual, and hence don't need to be altered, and there are some which are set to Automatic which I recommend setting to Manual. Most services do not need to be set to Disabled as that has no benefit whatsoever - a service set to Manual is not taking up any resources nor will it load up unless it is needed, yet provides a safeguard because if it is truly needed it can be restarted by Windows or a program. Only disable a service if it keeps restarting and you are 100% certain that it is not needed on your system. Some services can be very tricky in the impact they have - for example disabling the 'Server' service winds up turning off the display of Previous Versions for files, despite no indication that it will do so from its name or description. I urge you not to consider the disabling of services as some sort of major performance tweak and go crazy turning everything off.

The following pages contain my Windows service recommendations.

Copyright © 2010 Koroush Ghazi

Service Name	Startup Type (Default)	Recommended Change	Notes
Application Experience	Automatic		
Application Information	Manual		
Application Layer Gateway Service	Manual		
Application Management	Manual		
Background Intelligent Transfer Service	Automatic (Delayed Start)		
Base Filtering Engine	Automatic		
Block Level Backup Engine Service	Manual		
Certificate Propagation	Manual		
CNG Key Isolation	Manual		
COM+ Event System	Automatic		
COM+ System Application	Manual		
Computer Browser	Automatic	Disabled	Network-related
Cryptographic Services	Automatic		
DCOM Server Process Launcher	Automatic		
Desktop Window Manager Session Manager	Automatic		
DFS Replication	Manual		
DHCP Client	Automatic		
Diagnostic Policy Service	Automatic		
Diagnostic Service Host	Manual		
Diagnostic System Host	Manual		
Distributed Link Tracking Client	Automatic		
Distributed Transaction Coordinator	Manual		
DNS Client	Automatic		
Extensible Authentication Protocol	Manual		
Fax	Manual		
Function Discovery Provider Host	Manual		
Function Discovery Resource Publication	Automatic	Disabled	Network-related
Group Policy Client	Automatic		
Health Key and Certificate Management	Manual		
Human Interface Device Access	Manual		
IKE and AuthIP IPsec Keying Modules	Automatic	Manual	Network-related
Infrared Monitor Service	Automatic	Disabled	If not using infrared devices
Interactive Services Detection	Manual		
Internet Connection Sharing (ICS)	Disabled		
IP Helper	Automatic		
IPsec Policy Agent	Automatic	Disabled	Network-related
KtmRm for Distributed Transaction Coordinator	Automatic (Delayed Start)	Disabled	Network-related
Link-Layer Topology Discovery Mapper	Manual		
Microsoft .NET Framework NGEN v2.0.50727_X86	Manual		
Microsoft iSCSI Initiator Service	Manual		
Microsoft Software Shadow Copy Provider	Manual		
Multimedia Class Scheduler	Automatic		
Net.Tcp Port Sharing Service	Disabled		
Netlogon	Manual		
Network Access Protection Agent	Manual		
Network Connections	Manual		
Network List Service	Automatic		
Network Location Awareness	Automatic		
Network Store Interface Service	Automatic		
Offline Files	Automatic	Disabled	If not using Offline Files
Parental Controls	Manual		
Peer Name Resolution Protocol	Manual		
Peer Networking Grouping	Manual		

Copyright © 2010 Koroush Ghazi

Service Name	Startup Type (Default)	Recommended Change	Notes
Continued...			
Peer Networking Identity Manager	Manual		
Performance Logs & Alerts	Manual		
Plug and Play	Automatic		
PnP-X IP Bus Enumerator	Manual		
PNRP Machine Name Publication Service	Manual		
Portable Device Enumerator Service	Automatic	Manual	If not regularly using portable devices
Print Spooler	Automatic	Disabled	If not using a printer, incl. virtual printers (e.g. PDF maker)
Problem Reports and Solutions Control Panel Support	Manual		
Program Compatibility Assistant Service	Automatic		
Protected Storage	Manual		
Quality Windows Audio Video Experience	Manual		
ReadyBoost	Automatic		Required for ReadyBoot, even if not using ReadyBoost
Remote Access Auto Connection Manager	Manual		
Remote Access Connection Manager	Manual		
Remote Procedure Call (RPC)	Automatic		
Remote Procedure Call (RPC) Locator	Manual		
Remote Registry	Manual	Disabled	Security Risk
Routing and Remote Access	Disabled		
Secondary Logon	Automatic	Manual	If only using one User Account at a time
Secure Socket Tunneling Protocol Service	Manual		Added in SP1
Security Accounts Manager	Automatic		
Security Center	Automatic (Delayed Start)	Manual	If not using the Security Center
Server	Automatic		
Shell Hardware Detection	Automatic		
SL UI Notification Service	Manual		
Smart Card	Manual		
Smart Card Removal Policy	Manual		
SNMP Trap	Manual		
Software Licensing	Automatic		
SSDP Discovery	Manual		
Superfetch	Automatic		
System Event Notification Service	Automatic		
Tablet PC Input Service	Automatic	Disabled	If not using a Tablet PC
Task Scheduler	Automatic		
TCP/IP NetBIOS Helper	Automatic	Disabled	Network-related
Telephony	Manual		
Terminal Services	Automatic	Disabled	Network-related Security risk
Terminal Services Configuration	Manual		
Terminal Services UserMode Port Redirector	Manual		
Themes	Automatic		
Thread Ordering Server	Manual		
TPM Base Services	Manual		
UPnP Device Host	Automatic		
User Profile Service	Automatic		
Virtual Disk	Manual		
Volume Shadow Copy	Manual		
WebClient	Automatic	Disabled	Network-related
Windows Audio	Automatic		

Copyright © 2010 Koroush Ghazi

Service Name	Startup Type (Default)	Recommended Change	Notes
Continued...			
Windows Audio Endpoint Builder	Automatic		
Windows Backup	Manual		
Windows CardSpace	Manual		
Windows Color System	Manual		
Windows Connect Now - Config Registrar	Manual		
Windows Defender	Automatic	Manual	If Windows Defender is disabled
Windows Driver Foundation - User-mode Driver Framework	Manual		
Windows Error Reporting Service	Automatic		
Windows Event Collector	Manual		
Windows Event Log	Automatic		
Windows Firewall	Automatic		
Windows Image Acquisition (WIA)	Manual		
Windows Installer	Manual		
Windows Management Instrumentation	Automatic		
Windows Media Center Extender Service	Disabled		
Windows Media Center Receiver Service	Manual		
Windows Media Center Scheduler Service	Manual		
Windows Media Center Service Launcher	Automatic (Delayed Start)	Manual	If not using Media Center functions
Windows Media Player Network Sharing Service	Manual		
Windows Modules Installer	Manual		
Windows Presentation Foundation Font Cache 3.0.0.0	Manual		
Windows Process Activation Service	Manual		
Windows Remote Management (WS-Management)	Manual		
Windows Search	Automatic		
Windows Time	Automatic		
Windows Update	Automatic (Delayed Start)		
WinHTTP Web Proxy Auto-Discovery Service	Manual		
Wired AutoConfig	Manual		
WLAN AutoConfig	Manual		
WMI Performance Adapter	Manual		
Workstation	Automatic		

Copyright © 2010 Koroush Ghazi

RESTARTING A SERVICE

If for some reason you find that a Disabled or Manual service is required for certain functionality you want to use, but is not starting up, then you can simply go to the General tab for that service, change the Startup Type back to Automatic or Manual, and then click the Start button. If the Start button is greyed out or the service fails to restart, it is because it is dependent on another service which is currently disabled or stopped. Go to the Dependencies tab for the service and under the first box you will see the other services it relies on - go to those services and set them to Manual or Automatic as required and start them. The bottom box displays the services which depend on this service to function, so also keep that in mind when disabling a service, as other dependent services will also stop working.

NON-MICROSOFT SERVICES

You may notice that your services list has several additional services that are not in the list above. This is because particular programs and drivers, such as graphics drivers, malware scanners and system utilities, can install their own unique services. These services are not part of Windows by default, but may be required for some of the specialized functionality of the programs you have installed. However often due to poor programming practices, the software developer may set a service to run automatically at launch and hence always be running in the background, when this is neither required nor desirable. As such, in many cases these third party services can be set to Manual or even Disabled to speed up startup time, reduce background resource usage and prevent conflicts without affecting the program's functionality in any significant way.

The quickest and easiest method of displaying all third party services is to run MSConfig (See the Startup Programs chapter), go to the Services tab and tick the 'Hide All Microsoft Services' box at the bottom. The only services which will then be shown are those that have been installed by third party software. To determine which of these are truly unnecessary, you will have to work out which software package has installed the service - in most cases it is fairly obvious because of the service name, however some services are not clear, or may even be part of malware and hence difficult to identify.

To correctly identify which program a service relates to, and in particular which file is launching it, follow these steps:

1. In MSConfig, having ticked the 'Hide All Microsoft Services' box, write down the exact name of each non-Microsoft service.
2. Open the Services utility and find the same service name in the listing.
3. Double-click the service and under the General tab for that service, look under the 'Path to executable' item, noting both the filename and its directory path.
4. If the service is currently running, open Task Manager, click the 'Show Processes from all users' button, then under the Services tab see if you can find the filename. Right-click on this filename and select 'Go to Process'. This may show you the program which is running it, though often it's just the generic Service Host process *svchost.exe*.
5. Search Google or one of the databases shown under the Startup Programs chapter for this particular filename. This should give you an indication of what its functionality is related to. If necessary you can temporarily Stop the service, or set it to Disabled and reboot to see what functionality it impacts on.

As with Microsoft Services, you should be able to Disable a range of these third-party services as they are not necessary. In some cases, Manual is the correct choice, and in other cases Automatic must be chosen otherwise the relevant program will not launch or will have problematic functionality. I cannot provide guidance in this respect as it depends on the program and the functionality you wish to use. If in doubt, leave a non-Microsoft service on its default setting.

Copyright © 2010 Koroush Ghazi

Change Service Status via Command Line

If you wish to change the status of a service without opening the Services Utility, you can do so by using a Command Prompt. This is useful if you have changed a critical service such that you cannot successfully boot back into Windows to change it back, or if you want to compile a batch file to start or stop a range of services at any time.

To alter a service via the command line you will need to know the name of the service, either its short name or full name. For example the full name for the Windows Defender service is 'Windows Defender', while its short name is WinDefend. You can find these details in the Services utility by double-clicking on a service and looking at the 'Service Name' field, or by looking at the subfolders under the following key in the registry:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services]
```

To start or stop a service via command line, open an Administrator Command Prompt and use the form:

```
Net [Start/Stop] "servicename"
```

Note, if using the short name for a service, quotes are not necessary, but if using the service's full name, quotes must be used around the name. For example to start the Application Layer Gateway Service, you can use either command below to achieve the same result:

```
Net start alg
Net start "application layer gateway service"
```

You will receive a confirmation that the service has been started or stopped if successful.

Permanently Deleting Services

There are times when a particular third party program or malware installs a custom service and then does not completely remove it upon being uninstalled or forcibly removed. If you wish to delete a service from your system - and obviously this must only be done if you are certain the service is unnecessary and not related to default Windows functionality - then follow the steps below:

1. Open an Administrative Command Prompt.
2. Determine the correct name of the service which you wish to remove - see earlier sections above for instructions on how to do this.
3. Type the following:

   ```
   sc delete servicename
   ```

4. You will see a message indicating that the process is successful, and you will no longer see that service displayed in the Services utility.

Note that if you do not feel comfortable using the command line method, then you can use the free Total Service and Driver Control (TDSC) utility. Run the program, let it enumerate your drivers and services, then click OK. Select the service you wish to delete from the list and click Remove, then reboot.

Once again, use caution permanently deleting a service. Deleting a necessary service can cause major problems and will usually require the reinstallation of the program to get it back. The situation will be made even worse if you manage to delete a default Windows service, so at the very least only attempt deletion of known third party services.

Copyright © 2010 Koroush Ghazi

Service editing is an area of ongoing debate. Some people suggest that altering services from their default is completely pointless and unnecessary and should not be done due to the potential problems it can cause; others will argue that many services should be disabled to 'increase performance'. I tend to be in the middle - there is certainly a case for disabling genuinely unnecessary services for functions you will never use, but this must be done with a bit of thought and research: only disable services if you are absolutely certain of their functionality and that you don't need them, and if in doubt, leave the services set at their defaults. This is particularly true of Manual services which do not need to be set to Disabled in most cases as this has no impact on resource usage whatsoever.

Just as we removed unnecessary startup items under the Startup Programs chapter, there is still a genuine need for all users to identify and if necessary alter the configuration of unnecessary services installed by third party programs. Due to poor and sometimes deliberately deceptive programming practices these services often launch when they are not required and sit in the background, adding to startup time and background resource usage, increasing the security risk and greatly increasing the potential for system instability or conflicts on your system. Remember that not all software developers are particularly interested in fast Windows performance, nor do they care about instigating inconvenience or additional resource usage on your system as long as it benefits them. This is why editing services is still essential - for removing these unnecessary third party impositions.

Copyright © 2010 Koroush Ghazi

WINDOWS REGISTRY

The Windows Registry is a central database for holding a range of important system and program-related data. Whenever you change certain Windows settings, install new programs, or even move or resize open windows for example, the registry will be updated with key pieces of information recording these changes

Under Windows Vista, the registry remains much the same as before, however there have been some improvements to decrease the possibility of registry corruption, and notably there has been the addition of Virtualization support as part of the User Account Control feature. This allows the installation of applications which usually require Administrator privileges under a Standard account - see the UAC section of the PC Security chapter for more details.

< REGISTRY EDITOR

The Windows Registry Editor is the primary built-in Windows tool used to view and edit the Windows Registry. To access it go to Start>Search Box, type *regedit* then press Enter. The Registry Editor displays a Windows Explorer-like view of the database as a range of folders and subfolders which can be navigated just like any other Explorer-based interface.

For our purposes, the main reason for editing the registry is to alter settings that cannot otherwise be changed using the normal Windows interface. Learning to use the Registry Editor is important because it is a powerful tool, and unlike any third-party utility designed to edit the registry, using Registry Editor provides the most direct access to the entire Windows Registry and ensures that you are aware of precisely what has been changed each time, and where it originally resides should you need to change it back. I recommend you take the time to learn more about using this important tool.

To use the Registry Editor correctly, open it and you will see what looks like a directory listing under Computer, with five folders starting with 'HKEY_', e.g. `[HKEY_CURRENT_USER]`. Under these Root Keys are a series of sub-folders called Keys. Within each key there is at least one Value called `(Default)`, visible in the right pane of the Registry Editor window when you click on the key name. Typically there are several other values underneath the Default entry. These values can be of several types, including STRING, DWORD and BINARY values.

The most common form of registry editing involves changing the contents of values, or adding new values under certain keys. Note that in this book the key name and location is provided in square brackets [ ], and the name of the value to be edited is shown underneath. The data to be entered into the value is given after the '=' (equals) sign. An example is provided below.

Copyright © 2010 Koroush Ghazi

Editing Registry Entries

To edit an existing registry entry follow the example below to see the correct procedure:

```
[HKEY_CURRENT_USER\Control Panel\Desktop]

CursorBlinkRate=530
```

The text above indicates that to make this registry change, you should open Registry Editor and then:

1. Double-click on the `HKEY_CURRENT_USER` root key or click the small '+' sign next to it in the left pane of the Registry Editor window. This will show every subfolder sitting directly under it.
2. Next, you must double-click on the `Control Panel` sub-key.
3. Left-click once on the `Desktop` sub-key to select it.
4. In the right pane of the Registry Editor window, look for a value called `CursorBlinkRate`.
5. Double-click on this item and in the box that opens, click in the Value Data box, note that it says `600`.
6. You can edit this value data by entering a new value if you wish.
7. As soon as you click OK the change has automatically been saved to the registry.

You can close Registry Editor if you wish.

Creating New Registry Entries

You may need to create a new key or value if it does not exist by default in your registry. To create a new entry from scratch correctly, follow this procedure:

1. Go to the particular subfolder under which you need to create a new key.
2. Right-click on the relevant sub-key and select New>Key to create a new subfolder beneath it; alternatively, select New> and the correct value type to create a new value (entry in the right pane).
3. Enter the name for the new key or value and press Enter.
4. To confirm that the new key or value is in the correct location, left-click on it and look at the bottom of the Registry Editor to see if the full path matches that which you desire.

Note that you will not see any confirmation or sign that you've entered a valid key or value. Further note that DWORD (32-bit) is the type you should use for 32-bit Vista if prompted to create a DWORD.

A more detailed guide to editing the Registry is in this Microsoft Article. Just remember that the Windows Registry is very important, and editing it is not to be taken lightly, so if in doubt, don't edit the registry unless you absolutely have to.

Backing up and Restoring Portions of the Registry

Restoring a full registry backup or using a previous restore point can be considered overkill if you simply want to undo a single change to the registry. Since most users typically make a range of minor individual changes to the registry, a more practical precaution is to make a backup of the particular branch of the registry you are about to edit, especially if you don't feel confident about making the change, or aren't sure how the change will impact on your system. That way if anything goes wrong you don't have to go through a lengthy recovery process which may also undo other changes you wish to keep - you can simply restore the individual branch that you have changed quickly and easily.

Copyright © 2010 Koroush Ghazi

The steps to backing up a specific registry branch or key are as follows:

1. Open the Registry Editor.
2. In the left pane of the Registry Editor window, right-click on the name of the key that holds the settings you wish to edit.
3. Select the Export option, and choose a suitably descriptive name and appropriate location for the file. Make sure that the 'Selected Branch' option is ticked at the very bottom of the box, so that only that particular branch and all its sub-components are saved, not the entire registry. Click the Save button and the file will be saved with a .REG extension.
4. Once the relevant section of the registry has been saved, you can go ahead and make the desired changes to this branch of the registry.

If you experience any undesirable behavior after your registry changes - and remember that some registry changes require a reboot or logoff and logon before their effects can be seen - then you can restore this backup of your registry by going to the place where you saved the .REG file and double-clicking on it to upload it to your registry. This will overwrite the existing sections of the registry with the backed up version, effectively undoing your changes quickly and easily. Reboot or logoff and logon again if necessary to implement the change.

If you want to backup the entire registry, see the Backup & Recovery chapter for more details on how to make proper full registry backups, as well as other forms of protection against unintended registry changes.

< MISCELLANEOUS REGISTRY TWEAKS

Once you've learned how to edit the registry, you can use a range of tweaks to customize your system using the Registry Editor. This section covers the miscellaneous tweaks; most registry tweaks are actually covered under the chapter relevant to the specific area of Windows they relate to. For example, registry tweaks relevant to Internet Explorer are covered in the Internet Explorer chapter.

Remember that some registry changes require a reboot or logoff/logon before they come into effect, though you can also use the Explorer Reboot trick covered in the Windows Explorer chapter in many cases. Importantly, don't forget to backup your registry properly before changing anything in it.

CUSTOMIZE SHUTDOWN SPEEDS

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control]

WaitToKillServiceTimeout=20000
```

By default Vista can wait up to 20000 milliseconds (20 seconds) for some running services to end as shown in the STRING above. However you can edit this to a lower amount, such as 8000 (8 seconds) to speed up shutdown speed. Note that often services may be doing necessary tasks and terminating them sooner may cause problems, so I recommend caution in lowering this too much. If you notice that Windows is behaving strangely or your Windows or application settings are not being saved properly from each session, raise the value again.

Copyright © 2010 Koroush Ghazi

INCREASE NTFS SYSTEM PERFORMANCE

These tweaks can improve the performance of Windows systems that use the NTFS File System. See the Windows Installation chapter for more details of NTFS.

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem]

NTFSDisableLastAccessUpdate=1
```

This DWORD disables the constant updating of dates a file/folder was last accessed if set to 1. It should be disabled by default in Vista, but if not then set it =1 here.

```
NTFSDisable8Dot3NameCreation=1
```

This DWORD disables support for old MSDOS 8-character filenames if set to 1. It should not cause any problems except with very old programs.

TURN OFF SYSTEM BEEPS

By default Windows makes beeping noises under certain situations, regardless of your Windows sound settings. To alter this behavior, go to the following registry entry:

```
[HKEY_CURRENT_USER\Control Panel\Sound]

Beep=Yes
```

Set this STRING to =No to disable any system beeps that occur during Windows usage. Note that to disable other Windows event-based sounds you will still need to go into Control Panel>Sound.

DISABLE WINDOWS KEY

If you want to disable the Windows Keys on your keyboard (usually found between the CTRL and ALT keys), perhaps because they are interfering in a game you are playing, do the following:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layout]

Scancode Map=
```

Under the `Keyboard Layout` key above (not *Keyboard Layouts*) create a new BINARY value called `Scancode Map` and then double-click on it and click once in the top right hand side of the value data box. Manually type in the following values in the exact order as shown (note all the 0's are zeros, and no spaces are necessary):

```
00 00 00 00 00 00 00 00 03 00 00 00 00 00 5B E0 00 00 5C E0 00 00 00 00
```

You will need to reboot for this change to come into effect. If you want to reverse this tweak, delete the above key and reboot. The Windows key is very useful for a range of reasons, so generally it should not be disabled.

While you will find a range of registry changes throughout this book, I don't recommend implementing a large number of registry changes at once, as this makes troubleshooting any subsequent problems difficult. Select the ones that you feel are the most necessary for performance and convenience sake, implement them individually if possible and reboot. If your system remains stable and trouble-free, implement another one and repeat. Remember, there is no undo function for the Registry Editor, so take the appropriate backup precautions as spelt out earlier.

Copyright © 2010 Koroush Ghazi

< MAINTAINING THE REGISTRY

The Windows Registry has thousands of entries, and just like any large database, over time some of these entries can become obsolete due to changes in hardware and software, and some entries can even become corrupted due to bad shutdowns, overclocking or faulty software or hardware for example. For the most part the Windows Registry is self-maintaining, and given the improvements to the registry made in Windows Vista, on balance I recommend that you do not attempt to run any utilities which attempt to optimize the registry by cleaning it. There are more risks involved and more likelihood of unintended consequences than any marginal benefits.

However for the sake of completeness, and also for more advanced users who feel ready to accept the risks, and want to use a registry cleaner to assist in removing debris left over from bad driver or program uninstalls for example, then this section briefly covers this topic.

The programs you can use for this functionality are the free CCleaner utility, which has a registry cleaning capability, or the JV16 PowerTools utility which requires purchase after a trial period. I recommend and cover the CCleaner Registry-related functionality below, as it is more than sufficient for our purposes:

1. Open CCleaner and click the Options button on the left side.
2. Click the Advanced button and make sure there is a tick against the 'Show prompt to backup registry issues' box.
3. Click the Registry button on the left side.
4. I recommend ticking everything under the Registry Integrity section except 'Unused File Extensions', 'Start Menu Ordering' and 'MUI Cache'.
5. Click the 'Scan for Issues' button and wait for the scan to complete - nothing will be altered.
6. Examine the list carefully, focusing on any entries related to programs or drivers which are no longer installed on your system - leave a tick next to these entries.
7. Untick any others unless you are absolutely sure they are safe to remove.
8. Click the 'Fix selected issues' button to commence removal of the ticked Registry entries.
9. When prompted, click Yes to backup Registry changes and save the backup to an appropriate location.
10. Click the 'Fix All Selected Issues' button then click OK to remove all ticked items from the registry.

Over a period of several days, if Windows features or any of your programs start acting strangely, you can undo the changes caused by registry cleaning by double-clicking the backed-up .REG file you saved in Step 9 above and rebooting. Note that CCleaner's primary functionality is covered under the Cleaning Windows chapter.

The NTRegOpt utility, by the same author as the Erunt utility covered in the Backup & Recovery chapter, does not clean or alter the Registry, but instead can compress it to take up less space. Similar to Erunt, it requires that you install and launch it with full Administrator privileges, or disable UAC, for it to work properly. Registry compression is not of major importance anymore, given the saving of a few Megabytes of memory are tiny in proportion to the total installed RAM on most modern systems.

Once again, for general users I recommend against using any registry cleaning tools due to the substantial risks compared with the marginal benefits which come from using these utilities in Windows. Any form of automated change to the registry can result in a range of problems and unusual behavior in Windows.

The Windows Registry is a vitally important component of Windows, a central database holding a range of critical information. If it is damaged or if parts of it are altered or removed without adequate knowledge, you may run into major problems, which in the worst case scenario could require the full reinstallation of Windows. For this reason I urge you to become familiar with the registry as covered in this chapter, and

Copyright © 2010 Koroush Ghazi

importantly, check the Backup & Recovery chapter both to read details of how to protect yourself against, and if necessary recover from, any catastrophic changes to the registry.

Finally, it is strongly recommended that if you have doubts about altering the registry in any way, it is best to leave it alone. None of the registry changes listed throughout this book can be considered absolutely necessary, and if you don't feel comfortable editing the registry at the moment, skip all registry-related steps, and come back to them when you feel more confident and have more knowledge about the registry.

Copyright © 2010 Koroush Ghazi

GROUP POLICY

The Group Policy Editor is an Administrative Tool designed primarily for Administrators to alter the way in which Windows behaves for groups of users on their network. It is only available in Windows Vista Business, Vista Enterprise and Vista Ultimate editions. To access the Group Policy Editor go to Start>Search Box, type *gpedit.msc* and press Enter. This will open the Group Policy Editor, which shows two main branches: 'Computer Configuration' and 'User Configuration'. Changes made under the 'User Configuration' sections only affect the current user; changes made under the 'Computer Configuration' section apply to the entire machine and affect all users on that machine. Note that the Security Settings found under the Computer Configuration branch are the same as those covered in detail under the Local Security Policy section of the PC Security chapter and won't be covered again here.

The Group Policy Editor can be useful if you wish to prevent users on your system accessing specific features, because it allows you to remove access to virtually any component of Vista. In terms of changing various settings, many of the options in Group Policy Editor can be applied using the various normal Vista settings and options. Furthermore some of the settings are legacy options left over from previous versions of Windows and have no impact on Vista, so only those that work are covered below.

To change a setting, go to the sub-folder shown and double-click on the setting in the right pane then choose Enabled, Disabled or 'Not Configured' as required and click Apply. The default for each setting is usually 'Not Configured' unless otherwise noted. Before changing a setting left-click on it and in the Extended view you can see a brief description of the setting to the left of it. If in doubt, do not alter a setting; none of these are necessarily recommended, they are provided in case you require this functionality. For more details of common usage scenarios for Group Policy Editor see this Microsoft Article.

PREVENT AUTOMATIC RESTORE POINT DURING DRIVER INSTALLATION

Folder: Computer Configuration\Administrative Templates\System\Device Installation
Setting: Do not create system restore point when new device driver installed

If Enabled prevents Vista from automatically creating a Restore Point during installation of new drivers. This can speed up driver installation but obviously provides less protection against potential problems.

PREVENT WINDOWS MEDIA DRM INTERNET ACCESS

Folder: Computer Configuration\Administrative Templates\Windows Components\Windows Media Digital Rights Management
Setting: Prevent Windows Media DRM internet access

If Enabled prevents Vista from automatically connecting to the Internet to check for Windows Media Digital Rights Management (DRM) licenses or upgrades. Existing DRM protected material with proper licenses will still play as normal.

PREVENT WINDOWS MEDIA PLAYER AUTOMATIC UPDATES

Folder: Computer Configuration\Administrative Templates\Windows Components\Windows Media Player
Setting: Prevent Automatic Updates

If Enabled prevents Windows Media Player from automatically downloading updates of itself.

Copyright © 2010 Koroush Ghazi

HIDE SPECIFIC CONTROL PANEL ITEMS

Folder: User Configuration \ Administrative Templates \ Control Panel
Setting: Hide Specified Control Panel Items

If Enabled, allows you to choose which components of the Control Panel you wish to hide. Click the Show button, then click the Add button in the box which opens. You will have to manually type in the full correct name of the Control Panel component - for example to hide the 'Pen and Input Devices' component in Control Panel, type *Pen and Input Devices* and click OK. When finished adding components to the list, click OK and then click Apply, and when you next open the Control Panel the relevant component(s) will be missing. Disable this option or remove the items from the list to show them again.

TURN OFF THUMBNAILS

Folder: User Configuration \ Administrative Templates \ Windows Components \ Windows Explorer \
Setting: Turn off the display of thumbnails and only display icons

If Enabled prevents any folder from displaying Thumbnail view. This can increase the speed with which you can browse such folders, but obviously removes thumbnail previews from such folders and replaces them with a standard icon.

REMOVE 'MAP NETWORK DRIVE' AND 'DISCONNECT NETWORK DRIVE' CONTEXT MENU ITEMS

Folder: User Configuration \ Administrative Templates \ Windows Components \ Windows Explorer \
Setting: Remove 'Map Network Drive' and 'Disconnect Network Drive'

If Enabled removes the 'Map Network Drive' and 'Disconnect Network Drive' items which appear on the right-click context menu in certain circumstances. These are unnecessary on PCs not connected to a network.

REMOVE ALL RIGHT-CLICK CONTEXT MENUS

Folder: User Configuration \ Administrative Templates \ Windows Components \ Windows Explorer \
Setting: Remove Windows Explorer's default context menu

If Enabled removes all right-click context menus from Windows Explorer-based interfaces, including within Windows Explorer itself and on the Desktop.

REMOVE CLOCK FROM NOTIFICATION AREA

Folder: User Configuration \ Administrative Templates \ Start Menu and Taskbar
Setting: Remove clock from the system notification area

If Enabled removes the main clock displayed in the Notification Area at the bottom right corner.

REMOVE BALLOON TIPS

Folder: User Configuration \ Administrative Templates \ Start Menu and Taskbar
Setting: Turn off all balloon notifications

If Enabled removes the small popup 'balloon tips' shown around various places in the interface when the mouse is hovered over them.

Copyright © 2010 Koroush Ghazi

HANDLING OF WINDOWS MAIL ATTACHMENTS

Folder: User Configuration \ Administrative Templates \ Windows Components \ Attachment Manager
Setting: Inclusion list for ...

Here you can specify precisely what file types (entered as a list of extensions, such as .EXE) the Attachment Manager in Windows Mail determines to be High, Medium and Low risk attachments. By moving certain file types into the Medium or Low category you can access them more easily in Windows Mail, though obviously this presents a greater security risk.

MODIFY CTRL+ALT+DEL SCREEN

Folder: User Configuration \ Administrative Templates \ System \ CTRL+ALT+DEL Options
Setting: Remove...

Here you can specify which components to remove from the screen which appears when you press CTRL+ALT+DEL. Set the specific components you want to remove to Enabled.

There are a wide range of things you can do in Group Editor, and you can browse to see all the available functionality, but bear in mind that most of what can be done in Group Editor is already possible using the normal Vista settings. It is not wise to force things off in Group Editor if you can change them in Vista via other means, especially those under the 'Computer Configuration' branch, because in the future if you or another user forgets about the changes you made here, it will cause confusion when you find you can't re-enable or use certain functionality - remember, Group Policy overrides the ability to adjust the features anywhere else within Vista, so use it only when required.

Copyright © 2010 Koroush Ghazi

WINDOWS SEARCH

One of the major changes in Windows Vista is the enhanced Windows Search functionality. Microsoft has integrated the Windows Desktop Search engine into Vista such that there are now many ways of quickly finding the files, folders, emails and even programs that you are after. The most fundamental change is that searching is no longer about knowing specific details like filename, creation date, location or file extension. By typing in a partial or whole word or sentence, the Windows search engine can display the most likely targets almost instantly. In this way Vista's search is much more like Internet searching, and hence is much easier and more useful in day-to-day situations for the average user.

However Windows Search is more than a search tool. People may claim that they already know where all the files on their PC are, and so search isn't necessary. This is not true - Windows Search functionality speeds up access to all programs, files and features. For example to open a particular picture or song quickly, instead of navigating to it in Windows Explorer you can click the Start button, type part of its name or related information in the Search Box, and it will be instantly displayed in the Start Menu, ready for launching. You can also remove many of your Desktop, Start Menu and Quick Launch icons because you can now rapidly access those same programs by simply entering their name in the Search Box instead. So Windows Search is no longer just about finding 'lost' files; it's about making access to the files and programs on your drive quicker in every way.

Before we examine how to use the Search functionality, it's important to understand the way in which Vista searches for files and how to configure this behavior, as this has a significant impact on how quickly Vista finds what you want, how successful more thorough searches are, and what sort of performance impacts you may experience.

< SEARCH INDEXING

In previous versions of Windows, searching for files generally required that you knew some precise details about the file (e.g. its filename, date of creation, or file type), and even with specific details it could still take quite a while to perform a search, even for a commonly-used file. To facilitate faster searching, the core of Vista's search engine is the Search Index. This index is a pre-built file similar to the index of a book, and it stores a range of details about files on your system, updated regularly by Vista. So when you launch a search in Vista, it will look at this index first rather than searching across your drive(s), with the result being a more thorough search done much faster than before.

However to start with, the search indexer does not index your entire drive, nor all the details of your files, as this would take a long time to regularly update, and reduce search performance and the quality of search results. By default the indexer only indexes the following information to begin with:

- All files and folders under the Personal folders - i.e. everything under the *\Users* directory.
- Email.
- Offline Files.
- Only certain more commonly-used file types are indexed; some with the contents of their Properties tab only and some with their entire file contents indexed as well. E.g. .DOC files have their properties and contents indexed; .EXE files only have their properties indexed; .BIN files are not indexed at all.

The actual index files used by the Search Indexer to store this information are held under the *\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex* directory which is usually hidden. The index files don't usually take up much drive space, and you should not delete them manually.

Copyright © 2010 Koroush Ghazi

Furthermore, for indexed searching to work properly the Windows Search service must be running (See the Services chapter), and indexing must be enabled under your drive properties - that is, go to Windows Explorer, right-click on the relevant drive and select Properties; the 'Index this drive for faster searching' box must be ticked for indexing to be enabled on that drive.

PERFORMANCE IMPACT

The search indexer is a very useful feature given the significant integration of search functionality in Vista. It makes searching much faster especially when using the Instant Search feature. However the index is really only useful if it is constantly kept up to date by the system, otherwise your searches may exclude more recently added files, or show results for files which have since been deleted, moved or altered. By default Vista runs the search indexer in the background as a low priority process. This means that only during periods when your system is idle, the indexer may spring to life and update the index for any changes to the contents of indexed folders. This usually happens at least once a session on average, but it really depends on how often you alter the contents of indexed folders.

Indexing is a drive and CPU intensive task, and if your system is idle the indexer may use up all of your spare CPU resources and churn the drive noticeably for a short period of time. This shouldn't be cause for alarm, because as covered under the Drive Optimization and Memory Optimization chapters, as soon as you launch a program or do something on your Desktop which requires resources, Vista will automatically throttle back or even stop the indexer immediately to provide all the resources the other task or program needs. This prevents the indexer getting in the way of major programs and games, and even during normal Desktop usage the indexer will run at greatly reduced speed to maintain system responsiveness. The time taken to maintain the index depends on how many folders you have indexed, how many files you have under those folders, how often these change and how many other tasks you do in Vista while the indexer is running.

To see the progress of the indexer when it is running, you can go to Control Panel>Indexing Options and at the top of the main screen you will see how many files it has indexed so far, and you may see something like 'Indexing speed is reduced due to user activity', which means it is taking a back seat to some other task, even if it's something as simple as you accessing a Control Panel option. Again, the indexer is not going to impact on system responsiveness in any noticeable way. For this reason, and given how useful the Search features can be, I strongly recommend against disabling Windows Search, even if you have an SSD for example. However if you still wish to disable Search, see further below for details on how to do so.

CUSTOMIZING THE INDEX

If you wish to improve the speed and accuracy of your search results and streamline the indexer's resource usage, you can customize precisely what Vista includes in its Search Index. Go to the Windows Control Panel and select the Indexing Options component. The main screen shows the folders which are currently indexed and at the top of the box displays how many actual files are in the index. To add or remove indexed locations, click the Modify button, then click the 'Show all locations' button. Expand the directory listing for the drive you wish to index. As mentioned, by default Windows Vista already indexes the files in several folders including the *\Users* folder and some of its sub-folders, however you can choose to remove these if you wish, or add other folders and their contents by browsing to them and ticking the boxes for each folder and/or sub-folder you wish to add (or remove). I recommend that you untick any folders/subfolders you know are never going to contain files you wish to search for or regularly access. When finished, click OK and there will be a wait as Windows adds or removes these folders and their contents in the index.

If you wish to further customize the search index, click the Advanced button. There are some important functions here, and these are covered below:

Copyright © 2010 Koroush Ghazi

Index encrypted files: If this option is ticked, encrypted files will be included in the index. However because the indexer cannot access the contents of EFS encrypted user files, this option really only indexes encrypted Offline Files (if any). Hence it is best left unticked.

Treat similar words with diacritics as different words: Diacritics are accent marks used in different languages and even for certain words in English, such as *touché* vs. *touche*. Ticking this option tells the indexer to treat the words as different if there is a difference in accent marks. Best left unticked unless you specifically remember to include diacritics when searching.

Re-Index selected locations: The indexed folders selected can have their index rebuilt at any time by clicking the Rebuild button. The process can be quite lengthy, especially if you have a lot of files and folders indexed, however this may be necessary if you experience problems with search results not finding indexed files. It is recommended that if you choose to rebuild, that you shut down all other programs and leave the system idle for a while otherwise it may take even longer to complete.

Restore your index to its original settings: Click the 'Restore Defaults' button if you wish to return the indexer to its default folders and settings at any time.

Index Location: As mentioned further above, the actual files for the index are held in a particular location by default. If you wish to move these files to another directory/drive you can do so by clicking the 'Select new' button and browsing to the new location. The main reason you would want to change this is if you wish to move the index contents to a faster drive for example, as this helps speed up both use of the index in searches, and more importantly allows faster updating/rebuilding of the index by Vista without interfering with your current system drive usage.

File Types: Under the 'File Types' tab of the Indexing Options you will be able to see the types of files the indexer can currently include in the index, listed by file extension. Any extensions which are ticked are included in the search index, and you can tick or untick any of these extensions as you wish. By default all the major and indeed many less common file extensions are already indexed so you should not need to change the indexed file types. If you have an extension which is not listed, you can add it manually by clicking in the text area at the bottom left of the box, typing the extension and pressing the 'Add new extension' button which will become ungrayed.

Importantly, here you can change whether a file type only has the contents of its Properties tab indexed ('Index Properties Only'), or whether all of that file's contents are also indexed ('Index Properties and File Contents'). For example highlight the .DOC extension and you will see that it has both its Properties tab and its contents indexed. So if you enter a sentence in the search box, if it exists within one of your indexed .DOC files the document will be included in the search results shown. It is generally pointless to index the contents of files which only have computer code as their content, so for many file types such as .EXE or .JPG files, the contents are not indexed and should not be; they don't have any useful plain English text in them. Certain types of files can have their contents 'translated' into something intelligible by Windows Search with the use of Filters. For example .PDF files can use an Adobe PDF IFilter (now built into the latest version of Adobe Reader) to allow their contents to become searchable by Vista's search engine. You will see if any filters are used for each file type under the 'Filter Description' column; since most files don't have their contents indexed they will have 'Null Filter' listed.

Whether a file type has its properties, or both the properties and contents indexed has an impact on maintaining the index, because the more files with complex contents are indexed, the more work the indexer has to do to maintain the index if these contents change regularly and/or significantly. I recommend only indexing the contents of file types for which you actually wish to initiate a content search.

Copyright © 2010 Koroush Ghazi

If you've changed the index settings I strongly recommend that when finished you click the Rebuild button to do a total rebuild of the index data using the latest settings, though note that this may take quite some time to complete. This will help prevent the index file retaining older entries and also make sure all your search results will be completely up-to-date and accurate.

Indexing and File Properties

As discussed above, the search indexer will index most files by what is in their Properties, as well as their content in some instances. So one of the ways in which you can further influence search indexing is by configuring the Details tab of a file under its Properties. You will notice there are a range of fields here that are either empty or already filled in with certain details about the file, such as its Size, Date Created, Title, and so forth. This is referred to as Metadata and provides additional information which the indexer can use to identify the file. If you want to make it easier to access or group a particular file(s) in the future, it is wise to add some metadata to it. For example you may wish to tag all your Jazz songs with the word 'Jazz' in the Genre field under the Details tab of their Properties. Then when you type the word Jazz in the Start Menu Search Box all these songs will be instantly listed for you to choose from.

To edit a file's details, first right-click on it in Windows Explorer and select Properties. Make sure it is not write protected (if it is, untick the 'Read Only' box, click Apply then reopen the file), and it is not currently in use. Then click the Details tab and move your mouse cursor over the fields under that tab, and you will see that many of these fields can be edited. Edit the field(s) appropriately and when you click OK, that information is saved along with the file. You can now search for that file using any one of the pieces of metadata entered into the Details tab of the file's properties - see the Search section below for details.

There is another useful function you can perform when in the file properties. Right-click on a file, select Properties and under the main General tab, click the Advanced button at the bottom. In the box which opens you can untick the 'Index this file for faster searching' box, and now the file will no longer be included in the indexer. In this way you can exclude any private files, or individual files which may be useless for indexing, from being included in indexed search results.

Disabling the Index

The indexer does not have a major performance impact because it only uses idle resources which would otherwise go wasted. The benefits of indexing are much more tangible in Vista because of the way the search resembles web search functionality and hence improves speed of access to commonly used files and programs. However if after reading this chapter - especially the Search section further below - you still feel you won't use the search features often and you want to disable indexing completely, follow these steps:

1. Remove all indexed folders from the indexer. This may take a few moments.
2. Go to Windows Explorer, right-click on your drive(s), select Properties and untick the 'Index this drive for faster searching' box, then click Apply. Choose to apply this to the drive and all subfolders, and click 'Ignore all' to ignore any errors for system files which can't have their properties changed (this is normal). The process may take quite some time to complete.
3. Set the Windows Search service to Disabled and Stop the service.
4. To confirm that indexing is disabled, go to Control Panel>Indexing Options and it should now say 'Indexing is not running'.

You can enable indexing again at any time by reversing the steps above, however it may take Vista some time to again apply indexing to your files and folders and rebuild the index so be patient.

Note that this procedure does not completely disable searching in Vista, but it does make Instant Search relatively useless, and it will also make general searches much longer and more system intensive, because they can't rely on the index. Importantly, you must configure your searches correctly if you've disable

Copyright © 2010 Koroush Ghazi

indexing, otherwise by default the search functionality looks in the index and without one it may incorrectly report that it cannot find certain files or folders even if they exist - details are below.

< SEARCH METHODS

Having covered the way in which Vista actually indexes and maintains files for quick searches, we now look at the ways in which you can undertake searching in Vista. Even though the search indexer is used by default, it does not necessarily mean that you are restricted to searching in indexed files. Furthermore there are many uses to search, beyond simply finding hard-to-locate files. While you may put your most commonly-accessed files and programs as icons on the Windows Desktop or in the Quick Launch bar for example, there are still many files on your system which you might want to access as quickly as possible, and the search functionality can help in that regard.

INSTANT SEARCH

Possibly the most useful new feature of Vista in my opinion is the Instant Search box which you can find at the top right of most any window, and of course most handily at the bottom of the Start Menu when you click the Start button. Extensive use of this search box is already made throughout this book to quickly find and launch particular Vista programs, such as typing *Services* and pressing Enter to quickly launch the Services Utility in less time than it would take to open the Control Panel, double-click on the Administrative Tools component then double-click on the Services item for example. Or if you want to launch the Windows Calculator utility, you can simply type *calc* and press Enter in less time than it would take to click All Programs, then Accessories then Calculator on the Start Menu. If you've added TweakGuides.com to your Internet Explorer favorites, then any time you want to visit the site, just type *tweakguides* in the search box and press Enter; a new browser window opens and loads the site straight away.

This search box is powered primarily by the indexing functionality described earlier in this chapter, and is one of the main reasons I strongly recommend keeping indexing enabled. You may even find over time that you get used to launching most of your programs using this box as opposed to any other method, as I have.

The Instant Search box has certain features which make it even more useful. To start with, it will provide rapid matches for incomplete text, so you can start by typing the first few characters of what you're looking for, and you will be presented with a list of applicable files. In a normal window, using the Instant Search box this way refines the available contents of that particular window to the files which contain the search term or letters; in the Start Menu Search Box using incomplete text will provide you with a list of all relevant files, programs, emails and so forth shown under appropriate category headings (Files, Programs, Communications, Favorites & History). Note that how the Start Menu search box functions and precisely what it searches for and shows when doing searches is actually configured under Control Panel>Taskbar and Start Menu>Start Menu>Customize - see the Taskbar and Start Menu section of the Control Panel chapter for details. Note that as of SP1, the Search item has been removed from the Start Menu itself - that is, when you open the Start Menu and look at the right side, it is no longer there and cannot be added via the Taskbar and Start Menu options.

If you cannot find what you are looking for by using the search box, or if there are too many results, you can click the 'Search Everywhere' link. If you want to narrow it to an Internet-only search, click the 'Search the Internet' link. When clicking 'Search Everywhere', the Search Explorer window will open, and this is covered below. Note that as of Vista SP1, the link was renamed from 'See All Results' to 'Search Everywhere' - the reasons for this and more details are provided further below.

SEARCH EXPLORER

When Instant Search doesn't provide useful results, or to do a more thorough search of all files and folders on your drive(s), you will need to use the Search Explorer. If you don't have a third party search program

Copyright © 2010 Koroush Ghazi

installed, you can access Search Explorer by entering search text in the Start Menu search box then clicking the 'Search Everywhere' link which appears, or directly at any time by pressing WINDOWS+F.

The Search Explorer interface is minimal to begin with, and you can enter your search term in the Instant Search box in the right top corner as normal. You can refine the search location in the location box to the left of the search box, and under it you can choose which category to limit the instant search to, i.e. E-Mail, Document, Picture, Music, Other. However to genuinely make use of Search Explorer, click the 'Advanced Search' option at the top right and a set of fields is revealed - you can now use the search functionality in the more traditional method as done in previous versions of Windows.

You can search for a file using a combination of its file type, its metadata such as date modified, name, or any major tag, and importantly you can specify a particular drive and then tick the 'Include non-indexed, hidden, and system files' box, then click the Search button to do a thorough and complete search on that entire drive for the search phrase. This will bypass the index and hence may take a while to conduct the search, but the results are complete and not restricted in any way aside from the parameters you specify here. The green progress bar in the Address Bar at the top will show you how far the search has progressed, and this can be quite CPU and drive-intensive, so let it complete without initiating any other major tasks or programs. If you wish to stop the search at any time click the red X next to the progress bar; merely closing the search box will not end the search.

Note that if you wish to set this type of advanced search behavior permanently, either click the 'Search Tools' button on the command bar in Search Explorer and select 'Search Options', or go to the Control Panel>Folder Options>Search tab. There you can specify the option 'Don't use the index when searching the file system', along with other customizations to make searching more thorough, albeit also much slower - see the Folder Options section under the Control Panel chapter for details. To save your search for future use, click the 'Save Search' button in Search Explorer and it will be saved under the *\Users\[username]\Searches* directory.

CUSTOMIZING SEARCH

As of Vista Service Pack 1, if you install a third party search utility which is compatible with Vista's search protocol, it will be better integrated into the existing Windows Search features, such as being launched when you click the 'Search Everywhere' link in the Start Menu. Details of these changes are in this Microsoft Article. I don't believe there is any need to install any third party software to replace or duplicate Windows Search, as Vista's default search features are already quite good. If you wish, you can install the latest version of Windows Search which will improve the search engine's performance, although if you have already installed SP2 - which is strongly recommended - then this newer version of Windows Search is already installed on your system.

A useful tool which is more of an enhancement rather than a replacement for Windows Search is Start++. The utility lets you specify aliases which will assist in further automating actions based on search results. You can even export and share these small macros as Startlets. It demonstrates one more reason why Search should not be disabled or ignored in Vista.

The search functionality in Windows Vista has been enhanced over previous versions of Windows and forms an integral part of Windows usage. The average user who may never have needed to use the Search function in Windows XP for example may now find themselves using it in Vista many times a day, and not even thinking about is as being a 'search'. Given the way in which the search indexer is genuinely non-intrusive, and given the many benefits of search, I strongly encourage you to leave indexing enabled and configure search in Vista for maximum functionality to begin with, then as you refine your usage patterns over time, disable the components you don't need and change the indexer to only index folders you really wish to access regularly. I do not recommend simply turning off the indexer or avoiding the use of search-related features, as there are no real performance benefits - the search indexer will not run while a game is running for example.

Copyright © 2010 Koroush Ghazi

INTERNET EXPLORER

Internet Explorer (IE) is the most used Internet browser in the world, and most Windows users are comfortable and familiar with it. While I recommend that you begin trialing alternatives to Internet Explorer to see if they can provide you with additional functionality you may like, Internet Explorer is a fast, functional browser, and has a range of security benefits - you should not feel you have to use another browser if you are happy with it.

Vista comes with Internet Explorer 7, however Internet Explorer 8 is now the latest official version of IE and the one I would strongly recommend all IE users upgrade to for security, performance, stability and compatibility reasons. Accordingly, the advice in this chapter now relates solely to IE8. You can download Internet Explorer 8 from here.

< BASIC SETTINGS

To configure Internet Explorer, open the browser, go to the Tools menu and select 'Internet Options' - note this is the same as if you go to Control Panel and choose 'Internet Options'. Below are the descriptions and my recommendations for the important settings under each tab of Internet Options in IE:

GENERAL

Home Page: Here you can set the page that opens by default whenever you start Internet Explorer. If you don't want any homepage to start when IE is opened, click the 'Use blank' button; if you want to set the website you are currently viewing as your homepage, click the 'Use current' button; clicking 'Use default' will restore IE's default homepage which is a Microsoft site such as MSN (depending on your location). If you are using tabbed browsing (see further below), then you can enter multiple website addresses in the box, one on each line. Then whenever you open IE, all of these pages will open at the same time, as separate tabs.

Browsing History: As you browse the Internet, certain files and settings are stored on your hard drive (cached) by IE to make your browsing faster in the future. Click the Settings button and you can select how IE uses this cache to speed up your browsing. Under the 'Check for newer versions of stored pages' you can tell IE how often to check to see if a web page has been updated; any parts of a site which don't appear to be updated will be loaded from your cache rather than site, and this can increase page load times especially for sites which have a lot of items to load up. I recommend selecting 'Automatically' as this allows IE to detect updated content and reload from the site only when it believes it is necessary. However this does not guarantee that you will always see the very latest content on the sites you visit, so if you want to see the absolute latest version of every page you visit select 'Every time I visit a webpage', though note this may increase page loading times. If you only want to view the latest version of certain pages at any time, press CTRL + F5 when on that page and this forces IE to reload the entire page from the site rather than from its own cache. Importantly, do not select the Never option here as that will mean IE will not update web pages you commonly view; it will always rely on the cached version which always results in out-of-date web pages.

If for privacy purposes you wish at any point to delete any components of your browsing history from the cache, click the Delete button back under the General tab - see further below for details. If you just wish to browse privately from time to time, see the InPrivate Browsing feature covered in the section of the same name further below.

Copyright © 2010 Koroush Ghazi

Disk space to use: You specify the maximum amount of space IE uses for its Temporary Internet Files cache in Megabytes in the box provided. If the cache is too small, it will generally result in longer page loading times; if the cache is too large then depending on your Internet connection speed and your drive speed, you may still get longer page loading times as IE has to search its cache to find the components of a web page to load, when it may actually be faster just to reload them from the original site. Therefore I recommend 150MB of disk space for the cache as a balance of size and speed. If you have a faster drive and view more complex sites with lots of large images or scripts you may wish to increase this cache to 300MB or even larger if desired. The maximum is 1024MB (1GB).

Current Location: Internet Explorer lists the current location of its cache - this is where all of IE's cached content is actually stored on your drive. You can view the files already there by clicking the 'View files' button, and you can view any downloaded programs or configuration files necessary for certain sites to run by clicking the 'View objects' button. If you wish to move the cache, to a faster drive for example, click the 'Move folder' button. To delete cache contents, it is recommended that you follow the instructions further below rather than manually deleting any files here.

History: Internet Explorer can keep a record of the addresses of all the websites you have viewed for a certain number of days. Here you can select how many days worth of recently viewed websites IE keeps. If you don't want a history of visited sites to be kept at all enter 0 in the box. Alternatively, see the InPrivate Browsing section if you just want to disable the storage of browsing history at particular times.

Delete Browsing History: By clicking the Delete button under Browsing History, you will open a new box which contains a range of options. These options list the individual components of your browsing history, giving you greater control over the specific elements you can delete. If you don't wish to leave any trace of your browsing history for each and every session, you can use the InPrivate Browsing feature of IE, which is covered later in this chapter. In general it is completely safe to tick all of these boxes and click the Delete button to remove all traces of browsing, however doing so too often will also decrease the efficiency of your browsing. For this reason, there is an option entitled 'Preserve Favorites website data' which if ticked (recommended) will keep your preferences and cached files for any sites you have in your Favorites. This increases convenience and speed when accessing your favorite sites, without retaining date for non-favorite sites. However if you want to remove all stored content then untick this box as well. In any case once you've selected which components you want to remove, click the Delete button at the bottom and they'll be removed immediately.

Search: The Search Box at the top right of Internet Explorer allows you to quickly initiate a web search using the search engine of your choice, the results of which are displayed on the main IE screen. By default it is set to use Bing, however if you wish to set it to another engine such as Google, click the Settings button and select a new engine under the Search Providers section. If you want to use a search engine not listed here, click the 'Find more search providers' link at the bottom of the window. If you don't want sites or programs to suggest changes to your default search provider, then tick the relevant box at the bottom of the window as well. If you want to use a different provider for particular searches, then in the main IE window click on the small arrow to the right of the Search box, select a provider from the list, enter your search query and press Enter - that search provider will be used only for that search, it will not change your default provider.

Tabs: Tabbed browsing means that new web pages launched from clicked links or via other methods will be opened as tabbed pages within the current browser window by default, rather than opening an entirely new browser window. This helps reduce resource usage and it is also much easier to manage multiple open pages this way. To configure tabbed browser, click the Settings button. In the box which opens you can select whether to enable or disable tabbed browsing altogether, and set the behavior of it if enabled. Briefly, I recommend ticking the following settings:

Copyright © 2010 Koroush Ghazi

- *Enable Tabbed Browsing* - As mentioned above, tabbed browsing reduces resource usage by only keeping one IE window open; each new tab takes up far less memory than additional entirely new IE windows.
- *Enable Quick Tabs* - Quick Tabs places a small box at the far left of your tabs when you have multiple open tabs. Clicking it opens a page which contains previews of the content of every open tab.
- *Enable Tab Groups* - Tab Groups allows IE to group together tabs which are related. Tabs originating from the same source page are grouped next to each other and use the same color.
- *When a pop-up is encountered - Always open popups in a new tab* - This prevents popup windows from attempting to hide by forcing them to open in a new tab instead of a new window.
- *Open links from other programs in - A new tab in the current window* - When a program launches a web page, this option forces it to open a tab in any existing IE window rather than open a new IE window, again conserving resources.

You can select any other options if you wish, but the main aim of tabbed browsing is to make viewing multiple web pages more manageable and prevent having lots of separate open IE windows which can use resources and space for no good reason. Some tips you can use to make tabbed browsing easier in IE include:

- Clicking on any hyperlink with the middle mouse button opens that link in a new tab.
- Clicking on any tab with the middle mouse button closes that tab.
- Holding down SHIFT and left-clicking on any link forces it to open in a new IE window.
- Holding down CTRL and left-clicking on any link forces it to open in a new tab.
- Use CTRL+TAB to quickly switch from tab to tab.
- You can reopen a recently closed tab by pressing CTRL+SHIFT+T.
- Left-click and hold on any tab and you can then drag and drop it to rearrange tab order.
- Right-click on any tab to bring up a tab-specific context menu.
- If you want to save a set of tabs as a single bookmark folder, click the 'Add to Favorites' icon (the star with a green plus sign under the main Favorites star), select 'Add to Favorites' and select 'Add Current Tabs to Favorites'.
- To open the contents of an entire Favorites folder in a series of tabs, right-click on the folder under Favorites and select 'Open in Tab Group'.
- To manage Tab Groups, right-click on a tab within the group and you can close the entire group for example by selecting 'Close This Group'.

Appearance: These options allow you to change the appearance of web pages, customizing colors, fonts and even forcing particular style sheets. You shouldn't alter these options unless you have specific needs.

SECURITY

Security level for this zone: You can set the level of security Internet Explorer uses on the main slider here, from Medium to Medium-High, to High. I recommend the default Medium-High level of security as it designed to allow most normal Internet functionality without being overly restrictive nor too relaxed. However if you constantly browse unsafe or untrusted websites, you may wish instead to set the High security level, though this will impact on Internet functionality. If you want to be even more selective, click the 'Custom level' button and manually select each security function; clearly though this is for more advanced users - the preset levels are fine for most users.

Enable Protected Mode: One of the most important security features in Internet Explorer - and this is only available in the Windows Vista and 7 versions of IE, not in XP - is Protected Mode. This feature works for browsing much like User Account Control does for general system usage: by default it restricts websites and online programs from accessing system areas and launching or installing malicious or undesirable software. Protected Mode has been further improved in IE8. While it is not foolproof, it is an important level of protection and I strongly recommend that it be left enabled.

Copyright © 2010 Koroush Ghazi

PRIVACY

Settings: The slider here controls the level of privacy in IE, which for the most part pertains to Cookies - small files stored on your machine designed to hold your preferences for particular websites. Cookies are not usually malicious or dangerous, as they cannot read or delete data on your computer, and can be very useful. Some cookies may attempt to track your online behavior for advertising purposes for example, and for this reason, the 'Medium High' level is recommended as it provides the best security/functionality compromise and should not prevent legitimate cookies from being placed on your machine while still protecting your privacy. However to be even more selective, you can click the Advanced button and tick 'Override automatic cookie handling'. Third-party Cookies can usually be Blocked without any major issues, as these are mainly from advertisers. First-party Cookies on the other hand are often useful (e.g. for holding your login details for forums, or recording visual settings for particular sites), and blocking them can impair a site's functionality. If you do decide to block all first party cookies, and/or if you select a higher Privacy setting on the slider, click the Sites button and here you can manually allow or block specific website's cookies. I recommend adding your trusted favorite sites to this list and allowing them to prevent any problems with functionality. For example, if you set a High or Very High privacy setting this will block almost all cookies, making some sites non-functional, but you can still allow specific sites' cookies by making sure they're in the list of allowed sites. For broader blocking of third party content see the InPrivate Filtering section further below.

Pop-up Blocker: A 'popup' is a new window or tab which opens when you visit particular sites and/or click on particular links or areas of a site. They are most commonly used for advertising, and hence the option here to block them. I recommend ticking the 'Turn on Pop-up Blocker' box, but you should also click the Settings button and manually add the names of websites you trust which have legitimate popups that would otherwise be blocked. For example you may wish to add your Internet banking site to the list, or Microsoft.com, as these are trusted sites which may launch legitimate popups that would otherwise be blocked. By default when a popup is blocked by IE, a small yellow warning bar will appear at the top of the page to inform you of this, and you may also hear a sound. If you want to disable either or both of these visual warnings, untick the relevant boxes here. Bear in mind that this may mean you will not be aware that a legitimate site is trying to open a necessary popup box, and thus you may run into problems on some sites - again make sure to add trusted sites to the list if you want them to function properly. Finally, you can choose the blocking level as either Low, Medium or High. The default of Medium is recommended as it captures most illegitimate popups without blocking legitimate ones, however you can choose High to block most popups - once again I strongly recommend manually adding desirable sites to the allowed list if you do this, as otherwise legitimate popups will also be blocked.

InPrivate: InPrivate Browsing is a new feature of IE which allows you to surf the web without leaving any trace of your activities on the PC. This is covered in more detail in the InPrivate Browsing section further below. The options here relate to the way in which the InPrivate Browsing and InPrivate Filtering features operate when enabled. By default IE keeps a record of the sites you visit for the purposes of determining what data to automatically block from third party providers. If you tick the 'Do not collect data for use by InPrivate Filtering' box, IE will not record any such data. This will impact on how effective InPrivate Filtering is at automatically blocking third party content, but start off by ticking this box and if you find problems on particular sites, make manual adjustments in the InPrivate Filtering settings box - see the InPrivate Filtering section further below.

When using InPrivate Browsing, ticking the 'Disable toolbars and extensions when InPrivate Browsing starts' box will disable all such toolbars and extensions to prevent them from saving any private data during an InPrivate session. This is recommended for maximum privacy, however if you absolutely require their functionality during InPrivate Browsing then untick this box, but make sure to research your installed toolbars and extensions to ensure they do not breach your privacy, as otherwise it will defeat much of the purpose of using InPrivate Browsing in the first place. Note that in general I strongly recommend against

Copyright © 2010 Koroush Ghazi

installing many (if any) toolbars and extensions wherever possible, for both security, stability and performance reasons, regardless of whether you use InPrivate Browsing or not.

CONTENT

Parental Controls: Clicking the 'Parental Controls' button opens the Parental Controls section of the User Accounts screen, allowing you to set specific parameters for Internet surfing for particular accounts. This is covered in detail under the User Accounts section of the Control Panel chapter.

Content Advisor: If enabled, the Content Advisor allows you to attempt to filter out and control access to websites that contain offensive or inappropriate material. Go through each category of content and use the slider below the box to set the restrictions on that category. Once done, click OK and you will be prompted to set a Password, as well as a Hint in case you forget that password. IE will now attempt to restrict content based on content advice from ICRA (Internet Content Rating Association), so this is not a fool-proof method.

Certificates: Certificates are a form of electronic authentication method to verify that a particular website or individual is what/who it/they claim to be. Certificates are described in more detail in this Microsoft Article, and it is beyond the scope of this book in detailing their functions. I don't recommend altering any of the settings in this section unless you are acting under advice from a trusted tech support person. If a particular site displays a certificate error or warning, I recommend pursuing this further with the site owner or researching via Google before conducting any financial transactions with the site, as advised in this Microsoft Article.

AutoComplete: AutoComplete can save any website address you have typed into the address bar (or have already stored in your History), any text you've entered into online forms, and any usernames and/or passwords you've entered on a web page. The aim is that next time you start to type a URL, or visit a site, AutoComplete will automatically complete or restore your typed text, speeding up logging in or filling out details, or typing URLs into the address bar. Click the Settings button to configure which particular aspects of a web page AutoComplete will function for, but in general for security purposes I don't recommend enabling any of these options unless you have strong protection on your User Account and the PC is physically isolated from anyone else.

Note that ticking the 'Use Windows Search for better results' box will mean that an item called 'Internet Explorer History' will be added to the Indexing Options used by Windows Search. This item cannot be removed from within the Indexing Options; to remove it, untick the box here and click OK.

Feeds and Web Slices: If a website you're viewing has RSS or Web Slice capability, you will see the orange RSS or green Web Slice icon. You can then click the relevant icon to view the feed or to preview relevant slice information. Clicking the Settings button here allows you to configure how often such feeds and slices are updated, how they're read, and how IE warns you about capable websites. If you don't use these features, untick all the boxes on the Settings page.

CONNECTIONS

You should set up and customize the details of your Internet connection under the Network and Sharing Center in the Control Panel - see Network and Sharing Center under the Control Panel chapter.

PROGRAMS

Default web browser: If you have installed any other browsers, you can choose to set or reset IE as your default browser by clicking the 'Make default' button. Unless you are worried about another browser taking over this default association, you needn't tick the 'Tell me if Internet Explorer is not the default web browser' box for optimal startup speed. If you wish to make another web browser your default, see the Default Programs component under the Control Panel chapter for details.

Copyright © 2010 Koroush Ghazi

Manage Add-ons: Clicking this button allows you to configure Add-ons in IE. Any small program installed for use within Internet Explorer is an add-on, and generally you will be aware that a site is installing an IE add-on through prompts. However you can view all the main add-ons here by selecting the relevant category and making sure that the Show drop down box under the Toolbars and Extensions category says 'All add-ons'. For example Adobe Flash Player is a common add-on which allows flash-based content to play on web pages, such as YouTube videos. When you first visit a web page with a flash animation, IE will prompt you with a yellow warning bar that 'This website wants to install the following add-on:' and mentions the name of the add-on, in this case 'Adobe Flash Player from Adobe Systems Incorporated'. If you wish to continue then click the warning bar and follow the prompts.

For the most part some add-ons are legitimate, such as allowing you to view PDF files from within Internet Explorer, or running free browser games. You can also download a Range of Add-Ons which provide useful additional functionality for Internet Explorer, such as spell checking. Many of these add-ons are free and operate similar to Extensions for Firefox, making Internet Explorer more functional and customizable.

The problem is that some sites try to install add-ons which contain potentially harmful or intrusive scripts designed to alter Internet Explorer's settings to suit their purposes. Furthermore some sites and programs will insist on installing useless toolbars in IE which take up space, collect data on your browsing behavior, and add to resource usage unnecessary. For this reason it's extremely important that you don't just automatically accept the installation of any add-on; only install add-ons from trusted websites and only if absolutely necessary. In general the less add-ons the better, both for security and performance purposes. Even legitimate add-ons can potentially slow down the launch and browsing speeds of Internet Explorer. Regularly check the list of add-ons in this section and disable those you don't trust; do a Google search if the name does not seem familiar.

The Search Providers category in the Manage Add-ons box is covered under the General section further above; the Accelerators category is covered under the Accelerators section later on in this chapter, as is the InPrivate Filtering category.

HTML Editing: Here you can set the program IE uses for editing the HTML code of web pages when you select the 'Edit with *[program name]*' option under the Page menu.

Internet Programs: Clicking the 'Set Programs' button here simply opens the Default Programs component of Control Panel, covered in full detail under the Default Programs section of the Control Panel chapter.

ADVANCED

This section contains important settings for Internet Explorer's functionality, security and general behavior. There are too many settings to be able to describe each one of them in full here, however I want to discuss a few important options in more detail before going into the recommended settings:

Phishing Filter/SmartScreen Filter: As discussed under the PC Security chapter, Phishing is a form of deception designed to illegally secure your personal details, such as logon, password and credit card numbers. It is usually done for financial gain, and is becoming an increasingly significant threat. Internet Explorer 7 introduced the built-in Phishing Filter which warns you if a particular site seems to be deceptive or a known phishing perpetrator. Internet Explorer 8 has changed the name of this option to the SmartScreen Filter. More than just a name change, the way in which the filter works has also changed. The filter now works much more efficiently, has new features to detect and block potential malware downloads, and in general it is strongly recommended that you leave the 'Enable SmartScreen Filter' box ticked under the Security section of the Advanced tab. If you visit a potentially unsafe site, the prompts you will receive are quite intuitive. If you still wish to continue visiting the reported site, click the 'More Information' link at the bottom of the warning, or click 'Disregard and download unsafe file' to continue downloading an allegedly unsafe file

Copyright © 2010 Koroush Ghazi

download. Obviously in both cases this is not recommended unless you are certain the report is false - remember that even trusted websites can unintentionally host malware without their owner's knowledge.

To manually check a particular site using the SmartScreen Filter, go to the Safety menu in IE, select the 'SmartScreen Filter' menu and click 'Check this Website'. To report a website as being unsafe, go to the same menu and this time select 'Report Unsafe Website' - however bear in mind this doesn't automatically add the site to the list of unsafe websites, it only reports it for further examination by Microsoft. Finally, you can disable SmartScreen Filter by selecting the 'Turn Off SmartScreen Filter' option here, but this is not recommended.

Zoom: Different web pages have different sized text and pictures. Internet Explorer allows you to zoom in/out of any page at any time simply by selecting the zoom level using the Zoom box at the bottom right of the screen - click on it and select the desired zoom level. However a quicker method is to hold down the CTRL button and scroll up or down with your mousewheel. Alternatively you can use CTRL + (plus key) or CTRL - (minus key) to zoom in and out respectively, and to reset the page to its default size, press CTRL 0 (zero). Under the Accessibility section of the Advanced options tab you can alter how this behavior works - if you tick the 'Reset zoom level for new windows and tabs', regardless of how zoomed in or out you are on your current tab, opening a new tab will mean the page will open at the default zoom level; if unticked, the new tab will open at the same zoom level as your current page. You can also experiment with the 'Reset text size to medium while zooming' option to see if it suits your tastes.

Compatibility View: Internet Explorer 8 introduces Compatibility View which helps correctly render web pages that use code designed for older browsers. You can switch to Compatibility View at any time by selecting the option under the Page menu, or by clicking the small 'broken page' icon to the right of the Address Bar. This essentially changes IE8 into IE7 for the purposes of rendering the page. You should only use this option if you believe a web page is being shown incorrectly, typically when elements on the page are out of alignment, obscured by other elements, glitchy or missing objects/text is visible, and so forth. Most sites will render correctly in IE8, so this is not a common problem. To manually force any page to permanently show itself in Compatibility View, select the 'Compatibility View Settings' option under the Page menu and add it to the list. You can also tick the 'Include updated websites lists from Microsoft' to use a pre-compiled list held by Microsoft which determines which sites require Compatibility View to automatically be enabled - more details can be found in this Microsoft Article. Of relevance to this section, under the Advanced tab in the main IE Internet Options, there is an option entitled 'Automatically recover from page layout errors with Compatibility View' - if ticked, as the option implies, page layout rendering errors will result in the page being shown in Compatibility View. You can leave this option ticked, however if you notice a site you regularly visit triggering this option, it is better to add it to the list under Compatibility View Settings for faster rendering.

The rest of my recommendations for the more important Advanced settings in IE are provided below.

I recommend that the following options be ticked for maximum performance, stability and convenience:

- Disable script debugging (Internet Explorer)
- Disable script debugging (Other)
- Enable automatic crash recovery
- Enable third-party browser extensions
- Enable visual styles on buttons and controls in webpages
- Show friendly HTTP error messages
- Use Passive FTP
- Use smooth scrolling
- Use HTTP 1.1
- Use HTTP 1.1 through proxy connections

Copyright © 2010 Koroush Ghazi

- Always use ClearType for HTML
- Enable automatic image resizing
- Show pictures
- Check for publisher's certificate revocation
- Check for server certificate revocation
- Check for signatures on downloaded programs
- Do not save encrypted pages to disk
- Enable DOM storage
- Enable Integrated Windows Authentication
- Enable native XMLHTTP support
- Enable SmartScreen Filter
- Use SSL 3.0
- Use TLS 1.0
- Warn about certificate address mismatch
- Warn if POST submittal is redirected to a zone that does not permit posts

I recommend the following be unticked, again for maximum performance, stability and convenience:

- Display a notification about every script error
- Enable Suggested Sites
- Allow active content to run in files on My Computer
- Allow software to run or install even if the signature is invalid

Settings for which I have no specific recommendation, but which are noteworthy:

Display Accelerator Button on selection: Accelerators are covered in more detail in the section of the same name further below. If ticked, this option brings up the blue Accelerators button whenever you highlight a selection on a page for example. This may be annoying for some people, especially if they keep accidentally clicking the button. Unticking this option removes the button.

Enable memory protection to help mitigate online attacks: Firstly to be able to change this option you will need to start Internet Explorer by right-clicking on the IE8 icon and selecting 'Run as Administrator'. If ticked, this option enables Data Execution Prevention (DEP) specifically for IE, which although more secure may cause problems with some older IE plugins and add-ons. You can try enabling it first and then disable it if it causes problems.

Do not submit unknown addresses to your auto-search provider: If selected, this option prevents the search functionality of the Address Bar. Given IE already provides an Instant Search box at the top right of the screen, this functionality appears superfluous. If you wish to retain it, select 'Just display the results in the main window', then whenever you enter some plain text in the Address Bar it will initiate a search using the default search engine used for the Instant Search box.

Empty Temporary Internet Files folder when browser is closed: As discussed under the General section above, the use of the browser cache speeds up browsing in IE. However if for privacy and/or security purposes you want the cache cleared every time you close IE, tick this option. This may result in slower browsing each time you start a new session of IE. A better alternative might be to browse with InPrivate Browsing automatically enabled - see the relevant section later in this chapter.

The remaining settings not covered above can be set to suit your taste, or simply left at their default. If any setting is greyed out then make sure to launch IE with full Administrator privileges; i.e. right-click on the IE launch icon and selecting 'Run as Administrator'. Some settings may only work after being changed by closing all instances of Internet Explorer and reopening it again.

Copyright © 2010 Koroush Ghazi

INPRIVATE BROWSING

InPrivate Browsing is a feature of Internet Explorer 8 designed to allow you to surf the Internet without leaving any trace on the PC you are using. To access this feature, select the 'InPrivate Browsing' option under the Safety menu, or press CTRL+SHIFT+P - a new browser window will open, clearly marked as 'InPrivate'. Any browsing done using this InPrivate session will not store data on your drive. This is ideal for people who browse the Internet using publicly shared machines, but it is also useful if you simply want to ensure that there is no potentially embarrassing Internet-related material stored on your PC via normal browsing.

While using an InPrivate session, IE will generate and store several temporary pieces of information, mainly to ensure that website functionality is maintained. Cookies and cached internet files will be stored temporarily for example, but as soon as you close the InPrivate browser window, these are all automatically removed. Importantly however, there are a range of caveats to keep in mind when using InPrivate Browsing:

- If you add any Favorites, RSS Feeds or Web Slices while using InPrivate, or you install any software, or add a new home page, then such changes will be saved and kept permanently even after you close it.
- If you don't close the InPrivate window then others may be able to view your browsing history and temporary files on the same PC.
- InPrivate functionality does not extend to protecting your anonymity when surfing - your IP address for example will still be visible and stored on various sites as you browse the Internet.
- An InPrivate session does not offer any greater security than using the standard IE mode. Do not mistake InPrivate as a form of protection against malware or phishing for example.

Note also that if you have installed any third party toolbars or extensions in IE, then unless you tick the 'Disable toolbars and extensions when InPrivate Browsing starts' box as covered under the Privacy section further above, these toolbars and extensions may be saving and transmitting private data regardless. For that reason, I recommend ticking this box, but more importantly, resisting the urge to install additional software for IE as much as possible unless absolutely necessary.

While InPrivate Browsing is a useful feature, especially for those using shared machines, it is not a substitute for correctly configuring all of IE's options (see the rest of this chapter), and also exercising common sense as to general browsing. InPrivate does not guarantee that others will not find out about your browsing habits through other techniques, so minimize the extent to which you undertake potentially embarrassing or secure browsing on shared PCs for example.

You can configure Internet Explorer to always open in InPrivate Browsing mode by default - see the Advanced Settings section later in this chapter.

INPRIVATE FILTERING

InPrivate Filtering is an additional Internet Explorer 8 feature which goes hand-in-hand with InPrivate Browsing. As noted above, InPrivate Browsing is designed to remove traces of your activity from the PC, but it does not protect your privacy when online. InPrivate Filtering attempts to do just that, to a reasonable extent, by preventing your private data from being broadcast unnecessarily to third party sites which are displaying content on the page you are viewing. For example, when you visit a trusted site, it may have content such as an interactive map or advertising which is drawn from another provider. You may wish to block data regarding your current actions on the trusted site from being transmitted to these third party providers.

To turn on InPrivate Filtering, go to the Safety menu in IE and select the 'InPrivate Filtering' option to enable it; this must be done each time you start IE, although there is a advanced tweak to overcome this covered later in this chapter. Once enabled, you can then refine the way in which it works by selecting the 'InPrivate

Copyright © 2010 Koroush Ghazi

Filtering Settings' option under the Safety menu. Alternatively, you can access these options by clicking the small lock icon in the Status Bar at the bottom of the screen.

You have three main options for InPrivate Filtering: Automatically Block; Choose Content to Block or Allow; or Off. When 'Automatically Block' is chosen, if the same third party content appears frequently across a range of sites it will be tracked and eventually blocked by IE to protect your privacy. However you can manually choose to block or allow content yourself if you're not satisfied with the automated results. At the bottom of the Settings box there is a small box which allows you to change how many websites need to be visited with the same third party content before it appears on the list of Content Providers in the Settings screen at the bottom of the screen. The default is 10, but you can lower it to 3 or raise it to 30; the lower the number the more third content will be blocked and hence also appear for you to choose to block or allow in the list.

Alternatively, click the 'Advanced Settings' link at the bottom of the Settings box and you will be taken to the Manage Add-Ons box which then allows you to import pre-made filters for InPrivate Filtering. One example is this list which a user has compiled, mimicking the filter list from Adblock plus, a popular ad-blocking extension for Firefox. Save the list and use the Import feature in the InPrivate Filtering category of Manage Add-Ons to apply it to IE.

Remember however that InPrivate Filtering is not specifically designed to block advertising as such, it is a general tool to limit the amount of data you send to third party providers. Enabling InPrivate Filtering can result in some sites not displaying correctly, or missing importantly functionality. However more importantly, constantly using InPrivate Filtering to block advertising can and will affect the viability of many sites on the Internet which rely on third party advertising income to remain free to view. If you block the ads on sites you enjoy, consider donating to them directly if you wish to see them remain open and free.

ACCELERATORS

Accelerators are browser-based tools which provide additional functionality for a site. You can access an Accelerator by highlighting a portion of a site and clicking the blue Accelerators button which appears. To access a list of Accelerators currently installed on your IE, right-click the blue button and select 'All Accelerators', or go to the Tools menu in IE, select 'Manage Add-Ons' and then select the Accelerators category. There are a range of additional free Accelerators you can download, you can view the full list by right-clicking on the Accelerators button and selecting 'All Accelerators'>'Find More Accelerators', or by clicking the 'Find More Accelerators' link in the 'Manage Add-Ons' screen. While they provide useful functionality, I recommend exercising constraint in how many you add to IE and keep active at any time to reduce resource usage.

If you find the Accelerators functionality unnecessary, then disable all the available Accelerators in the 'Manage Add-Ons' box, and also disable the blue Accelerators button - see the Advanced settings section just below for details.

< ADVANCED SETTINGS

The following are some more advanced customizations to make IE easier to use:

CUSTOMIZE INTERNET EXPLORER 8'S APPEARANCE

Internet Explorer 8 does allow customization of its interface, although in practice there isn't a great deal of scope for changing the way IE8 looks. To streamline IE8's appearance, try the following changes:

Copyright © 2010 Koroush Ghazi

1. Right-click on an empty area of the main IE toolbar (e.g. in the blank area to the right of any open tabs) to access the customization options.
2. Untick any components you do not wish to view. For example the Favorites Bar, Menu Bar and the Compatibility View button are prime candidates for removal, as they are not frequently used by most people and their functionality is duplicated in a range of other places.
3. Select the 'Lock All Toolbars' option to turn it off, and you can now move the Command Bar - the icon bar on the right side of the screen holding your main IE options. Grab the dotted line to the left of the Command Bar and you can move it up slightly to sit on a new line above your Favorites button and tabs for example; this might make access to it quicker for some people. Regardless of whether you do move the Command Bar, make sure the 'Lock All Toolbars' option is ticked at this point to prevent accidental movement of any toolbars.
4. Select the Customize option and tick or untick the 'Use Large Icons' option to toggle the size of the icons to suit your taste, and also tick or untick the 'Show Stop and Refresh Buttons Before Address Bar' option if you wish to move the location of the Stop and Refresh buttons accordingly.
5. Select the Customize option and then select whether you wish to display any text next to icons or not - selecting 'Show Only Icons' will reduce the space they take up and is recommended.
6. Select the Customize option and then select 'Add or Remove Commands'.
7. Highlight the commands you wish to add or remove to/from the Command Bar and use the Add and Remove arrows to make the appropriate changes in the box on the right. For example you may wish to remove the Read Mail and Help buttons, and instead add a 'Delete Browsing History' button to the Command Bar. Once done, click Close to see the changes.

Unfortunately there isn't much more that can be done to truly customize IE8's appearance. Fortunately, for the most part IE8's interface is reasonably streamlined.

CHANGE OR DISABLE CLICK SOUND

Every time you navigate anywhere using Internet Explorer, or for that matter in Windows Explorer, you will hear a 'click' sound. To disable this clicking sound, or to change it to another sound follow these steps:

1. Go to Control Panel>Sound.
2. Go to the Sounds tab.
3. Scroll down the list of event sounds and left-click on 'Start Navigation' to highlight it.
4. To disable the sound completely go to the Sounds list below it and select (None) at the very top of the list, then click Apply; or
5. To change the sound, which is *Windows Navigation Start.wav* by default, pick another more suitable sound from the list, or click the Browse button to find another sound file on your drive to use - remember, the larger the sound file the more memory is used. Click Apply when done.

Note that changing or disabling this sound will affect both Internet Explorer and Windows Explorer equally.

CHANGE DEFAULT DOWNLOAD DIRECTORY

By default Internet Explorer uses the same directory path to save files whenever you download a file from the Internet. You can change this default path at any time by opening the Registry Editor and going to:

```
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer]

Download Directory=C:\Users\User1\Downloads
```

This STRING specifies the default directory where IE will save downloaded files. Enter the path to wherever you want the new default to be.

Copyright © 2010 Koroush Ghazi

START WITH INPRIVATE BROWSING MODE ENABLED

By default the InPrivate Browsing mode in IE8 requires that you start up IE normally, then select the 'InPrivate Browsing' option under the Safety menu (or press CTRL+SHIFT+P) to open a new browser window which specifically uses InPrivate. To avoid all this, you can create a shortcut which opens IE already in InPrivate Browsing mode, ready to go at the start of every session. To do this, follow these instructions:

1. Go to Start>Search Box and type *Internet Explorer*.
2. Right-click on the Internet Explorer item which appears and select Send to>Desktop.
3. Right-click on this new icon and select Properties.
4. In the Target box, go to the very end of the existing text, insert one blank space and then add the *-private* switch, and click Apply then OK to close the box.

Now whenever IE is launched from this modified icon, it will automatically open with InPrivate Browsing mode already activated every time.

START WITH INPRIVATE FILTERING MODE ENABLED

By default InPrivate Filtering needs to be enabled each and every time you start a new session of IE if you wish to use it. If you want InPrivate Filtering to be on by default all the time, then go to the following location in the registry:

```
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Safety\PrivacIE]

StartMode=1
```

The DWORD above needs to be created. When set =1 it forces IE8 to automatically begin with InPrivate Filtering mode enabled with each session. Delete it if you wish to undo this option.

CUSTOMIZE IE TITLE BAR

If you want to customize what is displayed at the top of each Internet Explorer window (typically the name of the site followed by *Windows Internet Explorer*), go to:

```
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main]

Window Title=Windows Internet Explorer
```

Create a new STRING called `Window Title` (there is one space between the two words), and assign whatever text you wish to use. The next time you launch a new Internet Explorer window this text will be displayed at the top of IE. Delete the entry if you wish to return to the default.

BUILT-IN FLASH BLOCKING

If you want to block Flash-based content on any web page, you can use the functionality in the 'Manage Add-Ons' screen in IE8 which allows greater control of ActiveX content, as described in this Microsoft Article. Follow these steps to customize how Flash content is allowed/blocked on a per-site basis:

1. Go to the Tools menu in IE, select 'Manage Add-Ons'.
2. Highlight the 'Toolbars and Extensions' category and make sure the 'All add-ons' option is selected under the Show drop-down box.
3. Left-click on the Flash-related entry (e.g. Shockwave Flash Object), and at the bottom of the screen select the 'More Information' link, or simply double-click on the entry.
4. In the box which opens, at the very bottom you will see a section where you can manually enter the names of sites which are allowed to use Flash-based content. By default it says * (asterisk) which means

Copyright © 2010 Koroush Ghazi

all sites. Remove the *, or click the 'Remove All Sites' button and click Close to disallow all Flash-based content on all sites. Alternatively, remove the * and then manually enter only the names of specific sites for which you wish to allow Flash functionality.

5. With Flash functionality disabled for sites, you will see a yellow information bar when a site requires flash for full functionality. You can either ignore this bar, or if you wish to add the site to your allow list, click on the bar and select the 'Run Add-On' option and follow the prompts.

As noted earlier, be aware that blocking flash-based content not only affects the functionality on certain sites, but it may also affect their viability if you block all their advertising as well.

Fix Internet Explorer 8

Many users have reported that this tweak has improved IE8's speed and/or stability, and in general it should be quite harmless either way, so it is included here for the sake of completeness. If you believe IE8 is running slowly on your machine, or you are experiencing problems with the browser, open an Administrator Command Prompt, type the following and press Enter:

```
regsvr32 actxprxy.dll
```

Reboot your system and open IE8 to see if there is any difference.

If you are having problems with Internet Explorer, you can browse through this Microsoft Fixit Site. In particular, to attempt to automatically diagnose and repair an Internet Explorer issue, you can run through this Microsoft Interactive Support Wizard.

Furthermore, you can first attempt to reset all of Internet Explorer 8's settings to their defaults by opening Internet Options - via the Windows Control Panel if you can't access it from within Internet Explorer itself - then under the Advanced tab, click the Reset button and follow the prompts.

Increase Maximum Simultaneous Connections

By default Internet Explorer 7 only allowed two items to be downloaded at a time from a server, but Internet Explorer 8 has raised this limit to 6. This can still be slow for sites which have multiple items that need to be downloaded before the page can be displayed. You can increase the value beyond 6 by going to the following location in the Registry:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet
Explorer\MAIN\FeatureControl\FEATURE_MAXCONNECTIONSPERSERVER]

iexplore.exe=10
```

The value above doesn't exist, so create it as a new DWORD and in Decimal view assign the maximum number of connections you wish to have (e.g. 10 as shown above). You must also change the value at the key below:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet
Explorer\MAIN\FeatureControl\FEATURE_MAXCONNECTIONSPER1_0SERVER]

iexplore.exe=10
```

The value above doesn't exist, so create it as a new DWORD and in Decimal view assign the maximum number of connections you wish to have (e.g. 10 as shown above).

Restart Windows or logoff and logon to implement this change. You can experiment with higher values if you wish, but note that increasing the maximum number of simultaneous connections to a very high value

Copyright © 2010 Koroush Ghazi

may technically be a breach of Internet Standards, or result in your connection being refused, so if you experience any problems reset these values to 6 or simply delete these values altogether.

DNS Cache Issues

Whenever your browser tries to load up a page on the Internet, it has to access a Domain Name System (DNS) server to resolve or translate the text address you use (e.g. www.google.com) into the actual IP address for the website (e.g.: 74.125.67.100). Since your browser needs to check DNS addresses each time it loads any web pages, the browser speeds up this process by locally storing the DNS addresses you use for a period of time so that next time you try to go to the same address it uses the IP address it has cached rather than looking it up again on a DNS Server. Unfortunately if a site is down temporarily, or has recently moved, then your DNS cache may store the site as being inaccessible for a while even if it comes back online shortly afterwards, and therefore every time you try to connect to it for a while you will get an error.

To resolve any DNS problems with web pages not loading up at all or loading up with outdated information, open an Administrator Command Prompt and type `ipconfig /flushdns` and press Enter. This will clear your DNS cache. Furthermore, to make sure that your browser never stores a negative DNS cache entry - i.e. one which says a site is inaccessible - then go to the following location in the registry:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters]

MaxNegativeCacheTtl=0
```

If the value above doesn't exist, create it as a new DWORD and assign it a value of 0 so that no negative DNS entries can be kept in the DNS cache. You can also set the length of time in 'Time To Live' (TTL) for a 'positive' (or working) DNS cache entry to remain active before being updated. To do this, add the following DWORD in the same location:

```
MaxCacheTtl=10800
```

Assign it a value which measures (in seconds) the total Time To Live for the positive cache entry. Make sure to enter the amount of seconds in Decimal view. Do not set this value too low as your DNS cache will effectively become useless and browsing will take longer. A value of between 3 and 6 hours (10800 - 21600 seconds) should be fine.

Advanced Customization

While Internet Explorer is a good browser in many respects, it is very limited in the extent to which it can be truly customized using relatively simple methods. This is one of the reasons why, if you are interested in undertaking more advanced customization of browser functionality and appearance, you may wish to explore the option of using one of the other free web browsers covered at the end of this chapter.

However if you still wish to try advanced customization of IE, you can use the free IE7Pro add-on which despite its name also works with IE8. Download and install IE7Pro, but during installation make sure the 'Enable Userscripts Plugin' option is ticked, and then select the 'Do not install ProgSense' option. Once installed, to access the new features which IE7Pro enables, go to the Tools menu in IE and select 'IE7Pro Preferences'. In the window which opens you will see a range of options which you can use to alter the appearance and behavior of Internet Explorer.

For example, using the 'User Scripts' component in the IE7Pro preferences box, you can load up a range of user-made scripts, such as those freely available at UserScripts.org, to achieve a range of customizations - though be aware that some user scripts can be deliberately malicious or annoying, so research a script carefully before enabling it.

Copyright © 2010 Koroush Ghazi

The various other functionality of IE7Pro won't be covered here, but clearly this add-on provides users with a great many options for further customization of Internet Explorer if used wisely. Note that if at any time you wish to disable the additional toolbar IE7Pro installs, right-click on the toolbar area and untick the new 'Grab Pro' item. This will also remove the 'IE7Pro Preferences' item in the Tools menu. You can re-enable these again by right-clicking on the toolbar area and reticking the 'Grab Pro' item.

< OTHER INTERNET BROWSERS

You may be wondering if there are other reputable browsers you can try if you are not happy with Internet Explorer. Fortunately there are at least three other major free browsers which are a viable and secure alternative to IE: Mozilla Firefox, Google Chrome and Opera.

My personal preference is for Firefox. It is an excellent browser which is free and well-supported and runs without any problems alongside Internet Explorer, giving you the opportunity to try it out to see if you prefer it. The main advantage of Firefox over Internet Explorer and many other browsers is that Firefox is much more customizable through a range of Extensions and Themes. If you want to find out more about Firefox I recommend you read my Firefox Tweak Guide which covers all aspects of Firefox from the basic to the advanced.

You have nothing to lose by trying other browsers out. All of the major browsers, including Internet Explorer, have the essential features required for fast, secure browsing. It all depends on which browser best meets your needs, as there is no outright best browser.

Copyright © 2010 Koroush Ghazi

WINDOWS MAIL

Windows Mail is the Vista replacement for Outlook Express, the built-in mail client for Windows users. It looks and behaves similar to Outlook Express in most respects, so OE users should be quite familiar with most of its functionality, however it does contain some important new features. For starters all stored emails are held as individual files, not in a single database as in Outlook Express. These emails are indexed and hence easier to rapidly search through using the Instant Search box at the top right of Windows Mail or in Vista's Start Menu. Furthermore your email account(s) and emails are more secure and more reliable, with less chance of any data corruption, and easier to move around. Importantly, there is phishing protection and a Junk Email filter built into Windows Mail. All of these features are examined in this chapter.

< BASIC SETTINGS

To configure Windows Mail, open the program and go to the Tools menu and select Options. Each section of the tabs under the Options box is covered below. Note that the options under most tabs can be set to suit your personal tastes, so I only cover recommendations for some of the more important or confusing settings:

GENERAL

Check for new messages every: If ticked, Windows Mail will automatically check for new messages at set intervals which you specify. If you are not connected to the Internet when it tries to do this, you can tell it to connect automatically or to remain disconnected. In general I strongly recommend this option be ticked, and that you set the interval fairly short (e.g. 5 or 10 minutes). That way if you leave Windows Mail open in the background while doing other things, it will inform you much earlier about any new emails you have received. However if you plan to play an online game make sure to close Windows Mail first if this option is enabled, as the act of checking for mail may disrupt your game.

Default Messaging Programs: This area tells you if Windows Mail is your default mail or news handler. If you want to use another application to handle your mail and/or newsgroups, see the Default Programs section of the Control Panel chapter for details of how to make them the default instead.

READ

Automatically download message when viewing in the preview pane: If ticked, Windows Mail will automatically download and show a preview of the contents of any highlighted email in the Preview Pane at the bottom of the Windows Mail window. I recommend unticking this option, otherwise any highlighted spam or malware emails will be downloaded and opened in the Preview Pane as well. In fact it is recommended that you disable the Preview Pane by going to the View menu, selecting Layout and unticking the 'Show preview pane' box.

RECEIPTS

Read receipts tell the sender of a message whether a message has been opened by the recipient. If you want to use them it is up to you, however keep in mind that many people find them annoying. Under the 'Returning Read Receipts' section I recommend selecting 'Notify me for each read receipt request'. That way you know when someone has sent an email to you with a receipt request, and you can choose whether to accept or deny the request to send a receipt when you open the email.

Secure receipts are useful if you are sending a very important message and you want to make sure that the recipient has opened the message and/or that the message arrived at the other end unaltered. Otherwise the same settings apply.

Copyright © 2010 Koroush Ghazi

SEND

Automatically put people I reply to in my Contacts list: I generally recommend unticking this option, as otherwise every person you reply to will go into your Contacts list, and hence if you are infected with any malware it may automatically send out infected emails to all your Contacts as well. Ideally I recommend not having anyone in your Windows Contacts list, however this is up to you - see the Windows Contacts section further below for more details and tips in relation to this.

COMPOSE, SIGNATURES, SPELLING

Everything under these tabs should be quite clear and can be set to suit your tastes.

SECURITY

Security is an important consideration in Windows Mail, since a lot of malware and phishing attacks are initiated through emails:

Virus Protection: Here you can select either the 'Internet zone' or 'Restricted sites zone' for your default email behavior. When in Internet Zone mode, HTML-based emails with active content will display their content just like a web page in Internet Explorer. In fact the security settings you choose under the Security tab in Internet Explorer Options also apply to Internet Zone email content. When in Restricted Sites Zone mode on the other hand, Windows Mail will disable active content from HTML-based emails, which is much more secure, but may reduce email functionality for HTML formatted emails. I strongly recommend running in Restricted Sites Zone mode, as most HTML-based emails are spam or malicious. For the most part legitimate emails come with plain text or minimal formatting, so this should have little visible impact on everyday email usage for most people.

Warn me when other applications try to send email as me: I recommend ticking this option as it provides a warning when an application initiates an email with your email address as the sender. This helps prevent any unauthorized emails going out under your name, though this setting does not stop most malware which sends out email such as spam from your account, as that works differently.

Do not allow attachments to be saved or opened that could potentially be a virus: This option will attempt to protect you from malware in email attachments. When this option is enabled, Windows Mail's Attachment Manager will analyze the attachment and the email it is part of to determine whether the attachment is likely to contain malware. By default if this option is ticked you will not be able to download attachments which are flagged as malware. Note however that just because an attachment is not blocked, doesn't mean that it is safe to open - you should still consider the source of the email as to whether it is trustworthy, and then save it (by default it is saved under your *\Documents* folder) and scan it for malware. If an attachment you trust is blocked, untick this option temporarily, view the email again, save the attachment then retick this option. Regardless of whether you trust the sender of an email or not, I strongly recommend scanning attachments you receive just in case the person sending it to you is unknowingly infected with malware themselves. See the PC Security chapter for details. For details on how to adjust the Attachment Manager's behavior, see the Group Policy chapter.

Block images and other external content in HTML email: If enabled this option blocks certain images and content in HTML email which may be exploited by malware to infect your system. I recommend ticking this option as generally most legitimate emails are not in HTML format, so it should have minimal practical impact.

You should not alter the remainder of the settings here, as doing things like encrypting your emails or digitally signing messages can cause problems for the people who receive your emails. Only alter these settings if you know what you are doing, otherwise they are not needed for the average home PC user.

Copyright © 2010 Koroush Ghazi

CONNECTION

The first set of options here apply to dialup users only, so only change if needed. When you click the Change button it will open the Internet Explorer Connections tab - see the Internet Explorer chapter for details.

ADVANCED

Contact Attachment Conversion: This option allows you to change any file attachments which is in the newer Contacts format to the vCard format used in previous versions of Windows.

IMAP: If this option is ticked, when using an IMAP email folder, if you delete a message it also removes the message from your message list at the same time.

Compose reply at the bottom of the original message: If ticked, when you reply to a message your reply will begin at the bottom of the original message text, as opposed to the default of the top.

Insert signature at the bottom of a reply: If ticked this option automatically inserts the default signature you have created under the Signature tab for every reply you make; normally a signature is only inserted for new emails you initiate.

Windows Contacts: These settings determine the pictures used to graphically represent your contacts on your Windows Contacts list, and are not significant as such.

When you click the Maintenance button you will see additional options. The most significant of these are:

Compact database on shutdown every: This option determines how often Windows Mail compacts your stored email messages to save space. You can set the number of times Windows Mail shuts down between each compacting. Since the process can take a bit of time, particularly if you have a lot of stored emails, I recommend something like 30 or 50 shutdowns, which should equate to roughly once every few weeks. If you open and close Windows Mail many times a day, increase this limit accordingly.

Store Folder: Clicking this button shows you where your emails are actually stored on your drive. By default it is normally under the *\Users\[username]\AppData\Local/Microsoft\Windows Mail* directory, however you can change the location if you wish. If you're after a method of exporting or backing up your messages instead of just moving their currently stored location, see further below for details.

Once you've adjusted all the settings you wish to change, click the Apply button and exit the settings screen. You may need to close and reopen Windows Mail for some of the settings to come into effect.

WINDOWS CONTACTS

Windows Contacts is the central location in Vista for storing contact details for people you know, replacing the Address Book in previous versions of mail such as Outlook Express. However Windows Contacts is not restricted to being a feature of Windows Mail; you can open it separately at any time by going to Start>All Programs, or going to Start>Search Box, typing *contacts* and pressing Enter, as well as under the Tools menu in Windows Mail. To add a contact to your list, you can do so in four main ways:

- If you ticked the 'Automatically put people I reply to in my Contacts list' option under the Send section of Windows Mail options, then each time you send an email reply to someone, they will automatically be added to your contacts.
- You can right-click on any email address in any email message and select 'Add to contacts'; alternatively you can just right-click on an email message and select 'Add sender to contacts'
- You can click the 'New Contact' button in Windows Contacts to create a new contact.

Copyright © 2010 Koroush Ghazi

§ You can click the Import button and import an existing file with contact details, such as your Address Book from Outlook Express.

Once a contact is added to the list you can view and edit their details by double-clicking on their contact item. This allows you to enter a range of personal and/or professional details as necessary. You can even add photos of these people to be the default display picture for each contact, making them easier to identify. You can export contacts to any application which supports the .contact file format, and you can also use contacts for other Windows features like People Near Me.

While this is a handy feature, particularly for corporate users on a network, for the average home PC user I consider it a risk to hold detailed information about yourself and/or other people here. To start with, if your PC becomes infected with malware, it may attempt to use the Contacts list to send itself out to all the other people you know, proliferating the malware. If someone compromises your account then they can see personal details of not only you, but all your friends and acquaintances as well, and this can be very useful in successfully undertaking identity theft. Instead I recommend keeping emails from all the people you wish to regularly contact under a general folder in Windows Mail. That way if you want to contact someone you can simply do a reply to their last email. Malware cannot use these stored emails to send itself out, and if someone compromises your machine it will take a lot more effort to work out personal details and the relationship between you and the senders of all the emails you've stored.

JUNK EMAIL OPTIONS

One of the important features of Windows Mail is the additional Junk Email Options it provides in protecting you against unsolicited email, or Spam. This type of email usually contains malware, or at best is simply an annoyance. The options here allow you to tell Windows Mail how to deal with emails it suspects to be spam. Windows Mail uses a special junk email filter called Microsoft SmartScreen to detect and flag email as spam. This filter is enabled by default and often updated through Windows Updates, so make sure to download relevant updates as they are available. Unfortunately no spam filter is 100% successful because spammers are constantly finding new ways of fooling automated spam filters.

Options: Here you can choose the level of spam protection, and this is a very important setting so it must be set knowing the possible problems it may cause. By default Windows Mail is set to Low junk email protection. This means that only very obvious email emails are flagged as spam and moved into your 'Junk E-mail' folder, and most if not all legitimate email will get through to your inbox. I don't recommend selecting the lower 'No Automatic Filtering' option, as there is no real benefit to turning off the spam filter. The only reason you might do this is if you regularly receive a lot of legitimate unsolicited emails and you need to respond to them in a timely manner. If you're worried about legitimate emails being caught up in the spam filter, simply remember to check the Junk Email folder regularly and sift through it for legitimate emails; with the default Low filter setting few if any real emails should ever be caught up in there.

If you want strong protection against spam, select the High filter setting, but keep in mind that at some point some legitimate email will almost certainly be mistakenly classified as junk email and moved to the Junk Email folder, so you will have to regularly check your Junk Email folder for these, which can be difficult if there are hundreds of spam emails in there as well. High is not recommended for most people.

If you only communicate with a set few people, and you want almost total protection against spam, you can select the 'Safe list only' option, and make sure to add all the email addresses of the people you communicate with under the 'Safe Senders' tab. Clearly this is only viable if you know exactly whom to expect emails from, as everyone else who sends you email will wind up in the Junk Email folder.

Regardless of which option you choose I strongly recommend not ticking the 'Permanently delete suspected junk email instead of moving it to the junk email folder' box. If this option is ticked, you stand a very good chance of automatically deleting legitimate emails without ever seeing them, and this could cause you

Copyright © 2010 Koroush Ghazi

confusion and problems if the emails were important. As noted earlier no automated spam filter is 100% accurate.

Safe Senders: To ensure that emails from people you know and trust do not ever get caught up in the Junk Email folder, you can manually enter the email addresses or domains of trusted people/sites here. For example you can enter *user1@tweakguides.com* to mark a single address as safe, or you can enter t*weakguides.com* to allow any email address from the domain TweakGuides.com to send you email without any problems. It is recommended that you also tick the 'Automatically add people I email to the Safe Senders list' as this automates the process of making sure the people you email are not blocked in future by the spam filter when they attempt to reply. Importantly, remember that some spammers 'spoof' email addresses or domains; that is they can make the email appear to be coming from t*weakguides.com* for example, when in reality it's coming from another address altogether. This feature does not guarantee that you won't receive spam, but it does help ensure that legitimate emails are not blocked, so on balance it is still useful to flag particular addresses/domains in this way.

Blocked Senders: If you know particular individuals or domains are only ever going to send you spam, enter their address or domain here to block them. Again, bear in mind that spam email spoofing may mean you might block a legitimate domain or address, so be careful what you add here.

International: These options allow you to block emails which are from a domain indicating another country (e.g. domains ending in .au are Australian, .ca for Canadian, .ru for Russian, etc). You can also block emails encoded in particular character sets indicative of certain languages (e.g. block all emails which contain characters specific to Turkish). Once again these tools must be used with caution. It is generally safe to block domains from which you know you would never receive an legitimate email, but bear in mind most spammers use email spoofing to fake common US email addresses ending in .com so this is only useful if you are getting a lot of spam from a particular country address, or filled with characters from a particular language.

Phishing: Enabled by default, this option uses Internet Explorer's Phishing Filter technology for checking emails - see the Internet Explorer chapter for details. By default any emails which are known to have fraudulent phishing-based content are flagged as such and you may not be able to access the links within them. If the 'Move phishing email to the junk email folder' option is ticked as well, these emails will be moved to the Junk Emails folder when received, which can provide added security. Not many legitimate emails should ever get caught by the Phishing Filter, so it should be safe to tick both options. I recommend enabling the phishing filter at all times.

If you wish to set up additional filters to send certain types of mail to the Junk Email folder - or any other folder for that matter - you can do so by going to the Tools menu, selecting Message Rules>Mail. This opens a box where you can set up custom filters as you wish, containing specific conditions such as if the Subject line of an email contains a particular phrase that you specify, it can be deleted from the server without downloading it, or moved to a particular folder you specify, or have an automatic reply sent to it. You can even set up multiple layers of filters if desired to truly refine the types of emails for which particular actions are applied. This gives you more control over not only spam but other emails as well, but obviously requires a bit more time and effort to setup, whereas the built-in spam filter in Windows Mail is totally automated.

Copyright © 2010 Koroush Ghazi

< ADVANCED SETTINGS

This section contains more advanced setting and tips for Windows Mail users:

BACKING UP AND RESTORING EMAILS AND ACCOUNTS

If you want to back up the emails you've saved in Windows Mail, follow these procedures:

1. Open Windows Mail, go to File>Export and select Messages.
2. Select the format for the emails to be saved in - Microsoft Windows Mail is recommended as this is compatible with newer versions of Windows such as Windows 7. Click Next.
3. Click Browse and specify the folder location to export these emails and click Next.
4. Choose the specific email folders you wish to export. Select All Folders if in doubt. Click Next.
5. Your messages will be saved to your specified location as a series of folders which contain the email messages in .EML files. You can then back these folders up, perhaps by archiving them first into a single .ZIP file.

To restore these emails back into Windows Mail at any point, say after a reformat of Windows, follow these steps:

1. Open Windows Mail, go to File>Import and select Messages.
2. Select Microsoft Windows Mail, or if importing from a previous version such as Outlook Express, select that and click Next.
3. Click Browse and select the location of the backup files you wish to restore, then click Next.
4. Your emails will be restored in Windows Mail.

To back up your mail user accounts, follow these steps:

1. Open Windows Mail, go to Tools>Accounts.
2. Highlight the account you wish to export and click the Export button.
3. Choose a location for the .IAF file and click Save.
4. The account and all its relevant details will be saved with your account email address as the filename. These can be imported into Windows Vista or Windows 7.

To restore your mail user accounts, follow these steps:

1. Open Windows Mail, go to Tools>Accounts.
2. Click the Import button.
3. Browse to where the saved .IAF file(s), highlight it and click OK.
4. The account is added into Windows Mail, complete with email address, passwords and any associated settings.

DISABLE WINDOWS MAIL SPLASH SCREEN

By default when Windows Mail launches, a small 'splash screen' is shown each time. To remove this permanently, go to the Windows Registry as below:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows Mail]

NoSplash=1
```

Create this new DWORD value and set it to =1, and it will remove the splash screen. Removing the splash screen doesn't necessarily make Windows Mail load up any quicker, but it can remove the annoyance. If you want to regain the splash screen at any time, just delete the above entry.

Copyright © 2010 Koroush Ghazi

< OTHER EMAIL CLIENTS

Windows Mail should be more than adequate for the average PC user. If you're not happy with Windows Mail for any reason, there are a range of viable alternatives. The most full-featured of these is Microsoft Outlook, which is included with the Microsoft Office suite. This is an email client which is highly customizable and has a range of additional features. If you own a copy of Microsoft Office then Outlook is available to you - perhaps you can install and use it for a period of time to see if you prefer it.
If you want a more advanced free email client, you can try Microsoft's Windows Live Mail which is a newer version of Windows Mail, but requires some customization - detailed configuration advice for Windows Live Mail is covered in the Windows 7 version of the TweakGuides Tweaking Companion.

If you want to try other free email clients, see this Wikipedia Article which lists and compares a range of email clients, providing feature details and relevant download links. Or you can simply use an online web client, such as Yahoo, Hotmail or GMail. These sites not only provide free email accounts and comprehensive web-based interfaces, they also provide plenty of storage space. However obviously they cannot be accessed in offline mode, and in general I don't recommend relying solely on an online provider, because if your email account is hijacked for example, you lose access to both your account and any stored emails.

Finally, I strongly suggest that you examine the tips provided in the PC Security chapter of this book for ways you can protect yourself from Email-related security risks while also preventing the spread of spam and malicious software.

Copyright © 2010 Koroush Ghazi

WINDOWS MEDIA PLAYER

Windows Media Player (WMP) is the built-in Windows utility for playing multimedia files. It has many useful features and is actually a very efficient, feature-packed media player, but is often mistakenly dismissed as being bloated. If configured correctly, WMP provides excellent audio quality and all the functionality that most users require for playing movies and music.

This chapter contains configuration advice and details on all of WMP's features. If you don't like Windows Media Player, alternative free media players are covered at the end of this chapter, as well as a discussion of a range of media-related issues relevant to all media players, including Codecs and DRM.

Note that I do not cover Windows Media Center configuration as it is too specialized and too varied based on different home theatre setups to be explained adequately in this book. However some of the information in this chapter also applies to Windows Media Center and many other media players.

< BASIC SETTINGS

To access Windows Media Player, go to Start Menu>All Programs or go to Start>Search Box, type *windows media player* and press Enter. You can also launch Windows Media Player by going to Start>Search Box and typing the name of a song or movie stored in your personal folders then selecting it.

To access Windows Media Player's menus, in Full View mode right-click on an empty spot on the black command bar, or just press the ALT key. To configure Windows Media Player as covered below, select Tools>Options:

PLAYER

Automatic Updates: WMP can automatically check for updates to itself at set intervals. Since it is not updated all that often, the 'Once a month' option should be fine. If you tick 'Download codecs automatically', whenever you attempt to play a media file for which you don't have the correct codec, Windows Media Player will automatically try to find and download the required codec and install it so you can play the file. This is recommended, and see the Audio and Video Codecs section below for more information.

Player settings: You can set these to suit your taste, however note that the 'connect to the Internet' option determines if Windows Media Player is allowed to connect to the Internet to update various information. If selected, it can override your other Internet-related settings as covered further below, so I recommend unticking it and manually configuring each individual option separately, then only coming back and ticking this option should you need to ensure Internet connectivity for a particular online-based feature that is otherwise not working properly.

Start the mini player for file names that contain this text: This option allows you to tell WMP to automatically launch into Mini Player mode (see further below) for files containing the specified text in their filename.

RIP MUSIC

Rip music to this location: Ripping music is the process of copying it from an audio CD to a media file on your computer. Click the Change button and select the directory where any ripped music or media is placed; by default it will be placed under the *\Users\[username]\Music* directory. Click the 'File Name' button to specify the particular attributes of the CD which will be used to compose the ripped music track's filename. Check the preview at the bottom of the box to see how this will look.

Copyright © 2010 Koroush Ghazi

Rip Settings: I strongly recommend you untick the 'Copy protect music' option as otherwise each track you rip will become DRM protected and this cannot be changed - see the DRM section further below. On the slider below, choose the audio quality you prefer for ripped music - 160Kbps or above is recommended for good quality audio, 128Kbps is the minimum recommended. The higher the quality the larger the file size of the ripped file however.

To use WMP to convert any audio tracks you want from a non-protected Audio CD to .WMA or .MP3 format do the following:

1. Insert the Audio CD in your drive.
2. Close and restart Windows Media Player to make sure it detects the CD.
3. Maximize WMP so you can see the track listing.
4. Click the Rip button at the top of the screen.
5. Put a tick against the track(s) you wish to rip
6. Click the arrow under the Rip button and you can select the specific Format you wish to use - .MP3 is recommended as a good balance between quality, size and compatibility with a wide range of media players, Windows Media Audio (.WMA) is good but less compatible, and .WAV provides the best quality but is usually too large because it doesn't compress the audio information.

There are various third party ripping tools available, however Windows Media Player is free, quick and easy to use, and the audio tracks it produces will not contain any copy protection as long as you use the relevant options covered above, so it is well worth using.

DEVICES

The devices listed under this tab are capable of media playback, whether video or audio or both. Select each playback device and click the Properties button. Adjust settings as appropriate, and if in doubt leave at their defaults which are fine for most purposes. Note that for your Display properties, you can alter the aspect ratio for video/DVD playback if it appears to be too wide or too narrow; the circle shown should be perfectly round on your screen.

I recommend that you untick the 'When deleting playlists from devices, also remove their contents' option to prevent undesired file deletion.

Click the Advanced button to alter the settings for audio and video file conversions when being transferred to/from multimedia devices and set to suit your tastes.

BURN

Windows Media Player allows you to also burn music or media files to a CD or DVD. Music can be burnt as an audio CD, but other media can only be burnt to CD or DVD as data files. If you want to burn pictures or movies to DVD for playback on an actual DVD player, you can use the Windows DVD Maker instead, accessible by going to Start>Search Box, typing *windows dvd* and pressing Enter. Its features are fairly self-explanatory and won't be covered in this book. Note that for general burning purposes a full-featured burning program called Nero Burning ROM is recommended, but the full version is not free. A useful free burning program compatible with Vista is Deep Burner.

Burn Speed: Select the burning speed, keeping in mind that if you are continually having errors with burnt discs, you should reduce the speed to Medium or even Low to ensure accurate burning. If you want the disc automatically ejected after the burn is complete, tick the box.

Copyright © 2010 Koroush Ghazi

Apply volume leveling across tracks on the CD: If burning an audio CD, you can tick this option to have WMP attempt to set a common volume level for all audio tracks. This can help prevent some tracks from being overly loud or soft relative to others.

Use media information to arrange files in folders on the disk: If you are burning a data disk and this option is ticked, WMP will sort your media into separate folders using *\Music\Artist\Album*, *\TV*, *\Video* and *\Picture* folders. If unticked, WMP will burn all tracks to the base directory of the disc without sorting.

Conversion: If you select the 'Convert to' option here, you will be able to use a slider which determines how the various music files will be resampled for burning to audio CD. I strongly recommended against allowing conversion, as most music files will lose quality if converted, especially if it's to 128Kbps or below, and more importantly, WMP automatically converts all files to .WMA format during conversion which is not necessarily desirable.

To burn a disk, open WMP in full view, click the Burn button at the top of the screen, and an interface for arranging files for burning appears. Click the small arrow under the Burn button to select whether to burn an audio CD or a data CD/DVD. You can then drag and drop files into the right-hand pane to add them to the list of media to be burnt to disk, and when finished clicked the 'Start Burn' button at the bottom.

PERFORMANCE

Connection Speed: This setting controls the speed with which Windows Media Player can download streaming media. I recommend the 'Detect connection speed' option, however if WMP consistently has problems detecting your connection speed and it seems to be too low, then set it manually here.

Network Buffering: This setting controls the amount of data to be buffered (stored in advance of playing), to help prevent stutters and skipping in streaming media playback. The 'Use default buffering' option is usually fine to use, but if you find streaming videos are constantly disjointed, then experiment with increasing the buffer size.

DVD and video playback: These options affect all DVD and video playback, and can be used to help resolve issues with particular videos or DVDs. If your video goes out of sync - sometimes due to lack of sufficient bandwidth - tick the 'Drop frames to keep audio and video synchronized' option. Tick the 'Use video smoothing' option if playing back video with low framerate, as WMP will try to interpolate frames (fill in the blanks) to provide the appearance of smoother video playback.

When playing fullscreen video, if the 'Display full screen controls' option is ticked, a set of controls will be shown at the bottom of the screen. If you want these removed, untick this box for true fullscreen video playback. You can then control playback at any time using your mouse and the following keyboard/mouse commands:

- Play or Pause - Left-click.
- Change Volume - Use the mouse wheel to increase or decrease volume.
- Mute Volume - Press the middle mouse button.
- Fast Forward/Rewind - Press and hold the front and back thumb buttons (if any) for Fast Forward/Rewind.
- Skip Forward/Back - Click the front or back thumb buttons to Skip Forward/Skip Back.
- Command Menu - Right-click.
- Return to Full Mode - Press ESC.

If you have a standalone graphics card, tick the 'Turn on DirectX Video Acceleration for WMV Files' option to allow your graphics hardware to provide better video playback performance for .WMV video. Finally, for videos which don't fill the entire screen due to their aspect ratio being different to your monitor shape, you

Copyright © 2010 Koroush Ghazi

can set the color used to display the surrounding area. For example for playback on a Plasma TV to prevent burn-in or uneven phosphor aging, you can set a white background by clicking the Change button.

LIBRARY

Sharing: If you wish to share the media on your current PC with other machines or devices on the same network, click the 'Configure Sharing' button. For instructions on how to configure this, click the 'Learn about sharing Online'. It won't be covered here as it's not a feature for the average home PC user.

Update Library: By default when Windows Media Player is first run it checks your personal folders to find any media files it can use, and adds them to your Library - a listing of all the media files on your PC. Windows Media Player will keep monitoring your personal folders to add or delete listings from the library as you add or delete your media files. You can access the Library listings by category at any time by going to WMP and clicking the Library tab. Here you can view the media files in various ways, sorted by categories such as Album, Genre, even Rating. You can create specific Playlists from the listings, and you can use the Instant Search bar to search through your media files as described in the Windows Search chapter.

If you want to alter the automatic updating of files to the Library, click the 'Monitor Folders' button, then on the next screen click the 'Advanced Options' button. You can now add further folders to monitor if you wish, but you cannot remove the default folders WMP monitors; you can only choose to Ignore certain folders. If you want to prevent WMP from adding any more files to the Library, enter the maximum values of 9999 for the 'Skip files smaller than' boxes at the right side, so that any file smaller than 10MB is not automatically added to the Library. When done click OK and WMP will scan for any changes it needs to make to the Library. Finally, back under the main Library tab I strongly recommend unticking the 'Delete files from computer when deleted from library' box to prevent accidental deletion of files. This allows you to edit or delete items in your Library listing without deleting the corresponding media files.

Automatic Media Information: If you want WMP to retrieve information about the particular media you are playing from the Internet - such as the name of the Album or Artist for a track - then tick the 'Retrieve additional information from the Internet box'; you can then choose to have it fill in the gaps or overwrite all existing information for the media. This information can be useful in making searches much easier, since the more details there are about a particular file, the more efficiently you can search for it (again see the Windows Search chapter). You can also manually force Windows Media Player to fill in missing information for particular files by clicking the Library button in WMP, then right-clicking on a particular track which isn't fully identified and select the 'Find Album Info' option - a new box will open which loads up the possible matches for this track and you can select the appropriate one, or enter the media information manually.

The remaining options here determine how WMP behaves when a track is ripped - see the Rip Music section further above.

PLUG-INS

Plug-ins are various modules which add functionality to Windows Media Player such as Visualizations or Digital Signal Processing (DSP) effects. These can be added, removed or configured here. To find more plugins to add, click the 'Look for plug-ins on the web' link, and for more visualizations, click the 'look for visualizations on the web' link - you will be taken to relevant Microsoft sites where you can download useful plugins or visualizations which should be safe to use with WMP. You can remove any added plugin by highlighting it and selecting the Remove button, and you can configure any settings they may have by selecting the Properties button. Bear in mind that the more plugins you use in WMP, the more resources the player may take up, and also the greater the chance for potential problems, so only install plugins you feel are genuinely necessary.

Copyright © 2010 Koroush Ghazi

PRIVACY

This is an important area of Windows Media Player which causes users a lot of concern. There is a common fear that by using Windows Media Player, Microsoft is spying on your media usage behaviors. This is not true, however to ensure that none of the media on your drive is altered, or any information about it reported back to Microsoft, follow the recommended settings in this section. To begin with untick every option on this page. None of them are necessary for normal media playback. If you use DRM-protected media, you may want to tick the 'Download usage rights automatically when I play or sync a file' and 'Automatically check if protected files need to be refreshed' options to prevent problems, but best to do so only if you run into a problem playing back such files.

If you don't want your media files altered in any way without your permission, I suggest that you make all of your media files (e.g. .MP3, .MPG, .WMV and .AVI files) write protected. To do this, in Windows Explorer go to the folders where your media files are stored and highlight all of them, right-click on them, select Properties and place a tick in the 'Read Only' box. By write-protecting all your media, Windows Media Player can't alter them or add any additional identifying information without your permission.

Finally, see the Windows Media Digital Rights Management (DRM) option under the Group Policy chapter of this book and enable it if you want to prevent Windows DRM from accessing the Internet when you use Windows Media Player. In the end though, at no point does Microsoft truly 'spy' on you; there are no real privacy risks to using Windows Media Player.

SECURITY

Your Internet Explorer security settings will be used when Windows Media Player is browsing any web content, so see the Internet Explorer chapter for details. For the remaining boxes here, I recommend you set them to suit your taste. You can start off by having them all unticked for maximum security, then if you encounter a legitimate website with multimedia content that doesn't function correctly, you can tick these options to allow it to do so. None of these options should be necessary to view most online media.

DVD

If you have a DVD-ROM drive on your system and use Windows Media Player to play DVD movies, you can adjust the settings in this section to suit your particular tastes and needs.

NETWORK

Configure this section according to your needs - the defaults should be fine.

GRAPHIC EQUALIZER

Windows Media Player comes with a fairly decent graphic equalizer which can noticeably enhance audio quality if set up correctly. To alter it, go to Full View mode and under the View menu select Enhancements>Graphic Equalizer. While you can use a range of presets, I recommend selecting the individual slider movement option - the top option on the far left - and then customizing the settings to suit your tastes. For reference, my personal settings from left to right for each slider are: 3 6 4 0 0 2 2 5 6 9. Your settings will vary both based on your playback device, as well as your any adjustments you may have made to the Tone settings for your playback device - see the Sound section of the Control Panel chapter.

Other options found under the Enhancements section include enabling SRS WOW effects, as well as Video Settings to alter the Brightness, Contrast, Hue and Saturation of video, and Crossfading and Auto Volume Leveling. You can close the Enhancements box at any time by clicking the small red 'x' at the far right of the Enhancements area.

Copyright © 2010 Koroush Ghazi

SKINS

You can customize the way Windows Media Player looks through the use of skins. These skins can change the appearance and visible functionality of Windows Media Player. There are some skins which already come with the player, and you can view them by opening Windows Media Player, and under the View menu select 'Skin Chooser'. In the Skin Chooser box you can click on a skin to see a preview of it in the right pane. If you want to try a skin out, click the 'Apply Skin' button. If you want to get new skins online click the 'More Skins' button, or go to a site such as The Skins Factory to download more free skins. Some skins will install automatically when you download them, but if you download a skin file in .WMZ format you can manually install it so that it appears in the Skin Chooser by putting the .WMZ file into your *\Program Files\Windows Media Player\Skins* directory. Note that using more complex skins can take up slightly more memory and possible use extra CPU power when you run Windows Media Player, so if you want to ensure the fastest performance and least resource usage simply use the default WMP appearance - that is, under the View Menu select 'Full Mode'.

In fact my preferred look for WMP is to switch to Full Mode and then simply use the resizing button at the bottom right of the player to shrink it down to the Compact Mode. In 'Mini Player' mode WMP uses even less resources - see below.

MINI PLAYER MODE

One of the neat features of Windows Media Player which sets it apart from many other media players is the ability to shrink it down into a 'Mini Player' interface which sits in the Windows Taskbar. To activate this, right-click on an empty area of your Windows Taskbar and under the Toolbars menu select the 'Windows Media Player' option so a tick appears next to it. Now open Windows Media Player and click the Minimize button on the top right of the player window. The player will minimize and sit in your Taskbar with a handy interface that allows access to all the major functions of the player, and whenever you want to maximize it again click the Maximize button on the bottom right of the mini player. Not only is this a neat feature, but more importantly while sitting in the Taskbar the player also uses less resources. You can also access WMP's seek functionality by hovering your mouse over the mini player, and using the slider bar which appears.

Finally, if you are having problems running Windows Media Player, or any other media-related features in Windows Vista, check the Windows Media Knowledge Center for help resolving it.

< AUDIO & VIDEO CODECS

A Codec (Compressor Decompressor) is a program which allows audio or video to be compressed and decompressed to or from its original format. Compressed files use special algorithms to achieve their size reductions, and it is the codec which can encode/decode these algorithms. Note that a Codec is not the same as a file format - a file format is simply a container type, while a Codec relates to the actual encoding of the media held in the container. For the most part you don't need to worry about this, because if you can play or record audio/video in a particular format, you have a Codec for that format already installed on your system. More details about Codecs in WMP can be found in this Microsoft Article.

To view the codecs already installed on your system, do the following:

1. Open Windows Media Player.
2. Go to the Help menu and select 'About Windows Media Player'.
3. Click the 'Technical Support Information' link at the bottom of the box.
4. A new browser window will open and towards the bottom is a list of all the audio and video codecs installed on your system, the files which relate to these codecs, and their version numbers.

To view Codec information for any file or your system in more detail, and to also attempt to adjust the priorities Windows assigns to individual Codecs - for example to force Windows to use one codec of the

Copyright © 2010 Koroush Ghazi

same type over another - you can use the free GSpot utility. Install GSpot and launch it, then under the System menu select the 'List Codecs and Other Filters' option. In the box which appears, you can sort Codecs by general type, name, driver filename, etc. - I recommend sorting by the first Type column to start with. Double-click on any particular codec for more information. To set the priority for a Codec, right-click on the relevant Codec and select 'Set Filter Merit'. Raising the slider will give this Codec higher priority over other Codecs of its type; lowering the slider will lessen the possibility that it will be used. Use this feature with great care, and be sure to note the original merit value for any codec you change.

If you want to uninstall a non-standard or problematic codec, the best way to remove it is to go to the Programs and Features component of the Windows Control Panel and look for the codec name in the list shown. If it's not listed there, then you can use GSpot to manually remove it. Follow the instructions above to get to the complete list of Codecs on your system, and then right-click on the relevant one and select 'Un-Register Filter', then you can try to manually delete the relevant file(s), usually found under your *\Windows\System32* directory.

If you need to download a new Codec because a particular media file is not playing back correctly, first determine what Codec(s) a particular file uses. Use GSpot to load the file and the relevant Codec information will be displayed on the main page. If you then want to then manually find the required Codec, search Google for the Codec name to find the original author's site. The most common third party codec required to play back video found on the web is DivX. You can also download FFDShow which is a filter that decodes most common video and audio formats, including DivX, XviD, AC3, FLAC and OGG. If you simply want FLAC and OGG support, install the Xiph Directshow Filters. For FLAC only, install the FLAC codec.

There are also certain types of media which won't normally play back on Windows Media Player or other common media players due to proprietary issues. The QuickTime .MOV and the RealPlayer .RM formats are two types of files which require special codecs and are usually viewable using their respective players: QuickTime Player and RealPlayer. If you don't want to install these players and instead want to view these audio/video files on Windows Media Player, or other players, you should install the Real Alternative and QuickTime Alternative codecs. Usually a Google search for any codec you require should find you a place to download it, but very old or proprietary codecs may be difficult to find or may cost money to obtain.

Codec Packs: I strongly advise against installing any general Codec Packs. These packs are tempting as they typically advertise themselves as containing all the Codecs you'll ever need in one simple package. However they are known to cause conflicts which result in a range of problems, from reduced performance, glitches and crashes in games and multimedia playback, to the complete loss of audio in certain applications. Even Microsoft warns against the installation of Codec Packs, so this is not a warning to be taken lightly, especially as the thorough removal of Codecs can be extremely difficult, and in some cases, a full reinstall of Windows may be required to undo the damage caused by a Codec Pack.

64-bit Codecs: Under Windows Vista 64-bit, normal 32-bit Codecs will work, however some native 64-bit software and some Windows features may exhibit minor issues. For example, videos may not correctly display a content thumbnail in Icon view in Windows Explorer. You can resolve this by installing the 64-bit version of the Codec instead. Some 64-bit applications may not detect 32-bit Codecs; for example the 64-bit version of the free video editing software VirtualDub works perfectly well on Windows Vista 64-bit, but it may require 64-bit Codecs like Lame64 for full MP3 encoding support. You will have to check and resolve these issues for any third party media players and encoders.

Copyright © 2010 Koroush Ghazi

< DIGITAL RIGHTS MANAGEMENT

A major issue of concern for people playing back media in Windows is Digital Rights Management (DRM). This is a form of protection applied to media content to prevent it from being copied or used beyond the scope of its original licensing terms, similar to the way Activation is used in Windows.

To see if a media file you are trying to play back is protected by DRM, open Windows Media Player in Library view, right-click on the Title of the file and select Properties. Under the 'Media Usage Rights' tab you will see if the file has any protection, and what conditions if any there are to its usage, such as number of times you can play it back, or when the file usage rights expire. In general you cannot remove or alter DRM legally, so it will not be covered here. If you have a file protected by DRM, comply with the terms it requires and see further below for some DRM tips.

An additional form of DRM has been integrated into Windows Vista. It is designed to provide protection for High Definition (HD) video content, such as that provided on the Blu-Ray disc format. This format allow resolutions of 720p and 1080p (i.e. 720 or 1080 vertical lines in Progressive format), whereas standard DVD for example is 480p (NTSC) or 576p (PAL). To ensure that content from an HD format is not being copied, altered, or coming from an unauthorized copy, Windows requires that all of the following conditions be satisfied for protected HD content:

§ The TV or monitor is connected via a pure digital DVI or HDMI cable.
§ The TV or monitor supports the High Bandwidth Digital Content Protection (HDCP) format.
§ An original HD-DVD or Blu-Ray disc is being used.
§ An activated and valid copy of Windows Vista is being used.
§ A signed WDDM graphics driver is being used.

Windows will check at startup to ensure that your hardware and system drivers support the conditions above, and if satisfied will enter Protected Environment such that you can play back any HD-DVD or Blu-Ray content without any problems. Note that any standalone HD-DVD/Blu-Ray playback device requires the first three conditions above to be met as well for the playback of commercial content, so this is not a Windows-specific requirement. More details of the specific requirements and impacts are in this Microsoft Article.

If you don't meet any of the requirements above, and thus don't enter Protected Environment, the content provider, that is the company which produced the actual HD material you are trying to view, can implement a degradation in the quality of the video to that of a regular 480p DVD, or prevent playback altogether. This is left up to the provider to decide; Windows has no involvement in this process, it simply tells the media that it is not running on a Protected Media Path.

There is also the Protected User Mode Audio function, which has been introduced in Vista, providing the ability to protect audio content from being unlawfully copied, similar to the protection provided to HD video content.

A key point to note is that none of the above information applies to HD content or audio which is not DRM protected. Furthermore even DRM protected content may not enforce any or all of the possible restrictions, this is left up to each content provider to determine. So in practice, for the average user, the DRM present in Windows Vista and Windows Media Player has no noticeable impact since it is all being handled behind the scenes by Windows without any need for user input, and typically has no practical impact.

However if you want to minimize the impact of DRM protection on your system I recommend purchasing your media and games on physical CDs, DVDs and Blu-Ray discs, rather than through digital channels. The physical versions of this media have the following benefits:

Copyright © 2010 Koroush Ghazi

- Fewer restrictions - You can rip an audio CD as often as you like for example, and to any particular quality you prefer, whereas digital copies are locked at a particular bitrate and have transfer restrictions.
- Greater security against accidental deletion - If you accidentally delete a digital copy, you may not be able to simply redownload it from the online store where you purchased it. A physical copy is generally more secure against accidental loss and hence rarely needs to be repurchased.
- Potential resale value - In most cases, digital copies of music, movies and games cannot be legally resold; legitimate physical copies can be resold whenever and however you wish.
- Protection against DRM changes - Some DRM protection systems may be phased out or altered in such a way as to cause problems with existing protected content, even locking you out of such content. Physical copies are effectively immune from changes in DRM, since they don't require updates to continue working, and most standalone players and software are backward compatible.

While somewhat old-fashioned, legitimate physical media copies provide a reasonable balance of cost, convenience, protection, the ability to transfer the media between machines, as well as rewarding the creators of the content. Digital downloads may be cheaper and more convenient, but they carry more restrictions and risks.

< OTHER MEDIA PLAYERS

If you don't wish to use Windows Media Player to view multimedia content, there are a range of alternatives including the following popular free players:

VLC
WinAmp
DivX Player
QuickTime Player
iTunes

I can't go into detail about each of these players in this chapter, however they are each good players, depending on your personal preference and specific needs. One specific media player worth noting further however is Media Player Classic. There is a free generic media player which can play back most formats, including proprietary formats, and is also both easy to use and utilizes very little system resources. Download and launch the *mplayerc* package - it requires no installation because it is in a single .EXE file which contains the player. It also requires no reconfiguration as such, it is ready to be used immediately without any issues.

Copyright © 2010 Koroush Ghazi

GRAPHICS & INTERFACE

One of the most talked-about changes to Windows Vista is the way it handles graphics under DirectX 10, and its glass-like Windows Aero interface. These changes both rely on the Windows Display Driver Model (WDDM) introduced in Vista, as well as the Windows Presentation Foundation (WPF). Much the same as the changes undertaken for other types of drivers under Vista, WDDM 1.0 ensures that the graphics driver does not have direct access to the software Kernel. All Desktop rendering, whether 2D or 3D is now done through Direct3D, a component of DirectX which is integrated into Vista. WDDM also provides advanced graphics card memory management and scheduling to allow better use of graphics hardware, which can further improve performance and stability.

In plain English, the changes mean that:

- There is much less potential for system instability, since the graphics driver is not directly entangled with the software core of Vista. A graphics-related issue is less likely to slow down or crash the entire system. For example, if Vista detects that the system is frozen it can restart the display driver without requiring a system reboot.
- Vista utilizes the graphics hardware on your system for everything from rendering the Desktop to 3D games, freeing up the CPU and making better use of the GPU when it would otherwise be relatively idle.
- Advanced graphical effects are possible on the Windows Desktop, including a combination of 2D and 3D effects, in an efficient manner. This is what allows the glass-like transparencies of the Aero interface, as well as features like Windows 3D Flip.
- Graphics card memory and resources are better managed than under Windows XP. The graphics card can be properly multitasked, so that switching between multiple 3D applications or games (or the Desktop) won't result in system instability. For example, when running a game, Vista's Aero interface has no impact on performance because it is suspended when the game enters Exclusive Mode; thus you can enable a range of advanced Desktop features without worrying about any negative impact on games. This is only possible because of the improved resource management.
- Video playback is improved under Vista, due in part to the new video memory management features which allow smoother playback and help in maintaining audio and video sync.
- Both gaming performance and eye candy can be increased under DirectX 10 (and DirectX 11), as DirectX 10 was a ground-up rebuild of DirectX designed to improve functionality and remove some of the limits on programming a graphics card which developers faced in past versions of DirectX.

The major drawback to Vista's driver model is that it is dependent on graphics card companies providing good WDDM graphics drivers to allow the correct functionality. This is something which proved difficult even for major graphics companies like ATI and Nvidia, resulting in a range of initial problems. However these have all been resolved and Vista now performs extremely well due to solid driver support.

Note that you can now also enable DirectX 11 capability on Windows Vista by installing a Platform Update - see the DirectX section of the Windows Drivers chapter for more details. DirectX 11 functionality enhances existing DirectX 10 features, but is most useful for those who have a DirectX 11-capable graphics card and undertake gaming in Vista. See the end of this chapter for more information.

Below we look at the major graphics-based components of Vista, starting with its interface.

Copyright © 2010 Koroush Ghazi

< WINDOWS AERO INTERFACE

Windows Aero is the Graphical User Interface (GUI) first introduced in Windows Vista. It is a mix of two dimensional and three dimensional components, and thus it requires Vista's Windows Display Driver Model to operate. Some of the prominent features of Aero include:

§ Glass-like transparencies on window borders and buttons and Desktop elements like the Sidebar.
§ Thumbnail previews of the contents of currently running applications by hovering your mouse over their Taskbar button or when accessing Task Switcher by pressing ALT+TAB.
§ Animated 3D previews of running applications while using the Windows 3D Flip task switcher accessed by pressing WINDOWS+TAB.
§ Animated 3D transition effects when minimizing or maximizing windows.

REQUIREMENTS

Aero is not automatically available to all users of Vista. If you do not see all the features above keep in mind that you must meet all of the following conditions to run full Aero mode:

§ You must have Windows Vista Business, Vista Enterprise, Vista Home Premium or Vista Ultimate. You cannot access full Windows Aero mode in Vista Home Basic.
§ You must have the appropriate settings enabled in Vista. Under Control Panel, open Personalization. Click the 'Display Settings' link and make sure your Colors setting is set to 32-bit. Click the 'Windows Colors and Appearance' link and make sure 'Enable Transparency' is ticked, then click the 'Open classic appearance properties for more color options' link and set the Color Scheme to 'Windows Aero'.
§ You must have a supported DX9-capable graphics card with 64MB of Video RAM or higher, and the card must have hardware support for Pixel Shader 2.0 or above. Specifically this means a Radeon 9500, GeForce FX 5200 or Intel 945G/GM or newer graphics solution.
§ You must be using a proper WDDM graphics driver for Vista.
§ You must have more than 512MB of System RAM.
§ The monitor must have a refresh rate of more than 10Hz.

If you do not meet all of the requirements above, you cannot run the Aero interface simply because it requires a minimum combination of hardware DX9 functionality with proper driver support for Direct3D under Vista, and sufficient power and memory to allow Aero to perform with reasonable smoothness and to full effect. For example, Vista uses the pixel shader pipeline on a graphics card to achieve the glass-like transparency effect, so cards that don't provide hardware support for Pixel Shader 2.0 cannot undertake this effect in real-time. See the System Specifications and Performance Measurement & Diagnostics chapters for details of how to find out if your hardware meets these requirements.

Additional points to consider when attempting to use Aero:

§ You will need a Windows Experience Index score of 3.0 on the Graphics component for Aero to be enabled automatically. If you've installed a new graphics card or drivers and you lose Vista Aero, or it still doesn't show up despite having appropriate hardware, drivers and settings as above, go to Control Panel>System and update your Windows Experience Index score. Vista should detect the new hardware capabilities properly and enable Aero. See the Performance Measurement & Diagnostics chapter for more details of what the Windows Experience Index calculates and how to troubleshoot it.
§ If running a very high resolution and/or multiple monitors the minimum requirements for graphics card memory will rise. Typically anything above 1280x1024 resolution requires 128MB of Video RAM, and dual monitors running 1920x1200 require 256MB of Video RAM as a minimum for full Aero effects.
§ If you are using a Mobile PC set to a Power Saver power plan, Vista may automatically exit the Aero interface at any time to save power. To prevent this, go to Control Panel>Power Options and change the plan from Power Saver to Balanced or High Performance.

Copyright © 2010 Koroush Ghazi

If after all of the above Aero is still not working for you and you have appropriate hardware, try the following changes to the Windows Registry:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\DWM]

Composition=1
CompositionPolicy=2
```

Find and change the DWORDs above to the values shown. Then open the Services Utility (see the Services chapter), go to the 'Desktop Window Manager Session Manager' service, double-click on it, select Stop and then select Start to restart it. Aero should now be available to choose and enable. If it is not then your graphics hardware and/or drivers do not meet the minimum requirements for Aero. There was a tweak available to force Aero for non-compliant hardware, but it only worked in the pre-final versions of Vista and has been disabled since then.

PERFORMANCE

Vista's WDDM framework means that as soon as you start Vista, the Desktop Window Manager starts running and uses Direct3D to compose the desktop image in a back buffer, a process similar to the one described under Step 8 on this page of the Gamer's Graphics & Display Settings Guide. This process makes the Desktop smooth to view and reduces or removes any 'tearing' or visual glitches. When you then launch a full-screen 3D application such as a game, it is launched in Exclusive Mode, and Vista suspends any rendering for the Desktop. This means that there is no performance impact on games or fullscreen 3D applications from using Aero or additional Desktop features.

Most systems with supported graphics cards should be able to support full Windows Aero functionality without problems. However if your Desktop starts to become sluggish or less responsive at times, to customize the effects used for the interface go to Start>Control Panel and open the System component. Then click the 'Advanced System Settings' link, or go to Start>Search Box, type *systempropertiesadvanced* and press Enter. Under the Advanced tab, click the first Settings button and you will see a range of options under the Visual Effects tab. Here you can customize precisely which effects are activated and which are disabled for the Windows interface. For example to turn off the animation effects in Aero, untick the 'Animate windows when minimizing and maximizing'; if your desktop windows are behaving sluggishly when being moved around, untick the 'Show windows contents while dragging', and so forth. You shouldn't have to disable many, if any, of these options unless they're not to your liking. Obviously though if your Desktop is filled with gadgets, windows and 3D items then at some point your system will become more sluggish depending on your graphics card's capabilities.

< DESKTOP BACKGROUND

You can set an image for your Desktop background by going to the Control Panel, opening Personalization and clicking the 'Desktop Background' link.

STATIC BACKGROUNDS

By default you will see a range of Vista background wallpapers held under the *\Windows\Web\Wallpaper* directory. When you click on any image it is instantly shown as a 'wallpaper' on the Desktop, so you can preview as many desktop backgrounds as you like in real-time to see how they'll look. At the bottom of the box you will notice there are five options as to how the wallpaper is displayed. They are covered below in order from left to right:

Copyright © 2010 Koroush Ghazi

1. This option stretches or shrinks the wallpaper to fill your entire Desktop, in the process the image may become distorted depending on its original aspect ratio and size compared to your screen ratio and size.
2. This option tiles the image repeatedly across the entire Desktop.
3. This option shows the image in its full resolution, and this may be too small or too large to fit exactly on your Desktop so there may be colored border(s) shown - you can change the color of the border(s) by clicking the 'Change background color' link.
4. This option stretches or shrinks the wallpaper to fit your screen similar to the first option, however it maintains the correct aspect ratio so there may be borders shown.
5. This option stretches or shrinks the wallpaper to fit the entire screen, however it maintains the aspect ratio of the image but crops the image in places.

If you want to use your own images for the Desktop background, click the Browse button and go to the directory which holds your preferred image. The image needs to be in .JPG or .BMP format to be used, and ideally for optimal quality I recommend making sure that it is the same resolution as your Desktop so that Windows doesn't have to rescale it. If necessary manually rescale the image to exactly match your screen resolution using a paint program, as this provides the best image quality.

ADDITIONAL VISTA STATIC BACKGROUNDS

The photographer who took a range of photos for the default Vista backgrounds has placed a range of the photos which did not get included in the final version of Vista on his site. You can view and download them here: Hamad Darwish. You can also download a wide range of great free wallpapers at InterfaceLift. Another method to find wallpapers of a specific size is to use Google Image Search, enter a search term for your generally desired wallpaper image (e.g. *sky*), then using the sidebar options to the left, click the Exactly link, and enter a Width and Height in pixels to match your current screen resolution (e.g. Width 1920 Height 1200) then click Search.

ANIMATED BACKGROUNDS

One of the Extras that Windows Vista Ultimate owners can access for free is Windows DreamScene which allows an animated desktop background to be set using a video loop. For example a looping video of raindrops hitting a puddle of water can be set as the Desktop background. The Windows DreamScene feature can be downloaded by Vista Ultimate owners under Windows Update in the Control Panel, and comes with eight video backgrounds - you can select these under Control Panel>Personalization>Desktop Background by selecting the 'Windows DreamScene Content' item from the Location drop box at the top.

You can download additional videos for DreamScene from WinCustomize or you can use your own custom-made videos in .MPG or .WMV formats, such as the ones you can download from SkyTimeLapse for example.

The Desktop background you choose may have an impact on memory usage since it is loaded into memory at Windows startup, though this shouldn't be of any real concern. Because Vista suspends the Desktop (and thus pauses a DreamScene video) while a game or any fullscreen application is running, having a fancy desktop background or animated desktop is not going to have any impact on gaming performance. If however you find an animated background impacts on Desktop performance and responsiveness, it is recommended you use a simpler video loop or failing that, just disable it.

< WINDOWS PHOTO GALLERY

Windows Photo Gallery is the default image viewer in Windows Vista. However there is an enhanced version of it which I recommend that you install, called Windows Live Photo Gallery. This version has additional image editing features among other things, and integrates into Vista without any problems, replacing the default Photo Gallery seamlessly.

Copyright © 2010 Koroush Ghazi

< WINDOWS SIDEBAR

The Windows Sidebar is a utility which runs on the right-hand side of the screen by default, providing a place to hold Sidebar Gadgets - small programs which provide custom Windows Desktop-based functionality. By default the Sidebar comes with a range of Gadgets you can try, including a clock, calendar and live weather forecast. When you hover your mouse over the right-hand side of the screen the Sidebar becomes visible as a translucent strip. A small Sidebar icon is also displayed in the Notification Area in the bottom right hand corner of the screen. To access the Sidebar options, right-click on the Sidebar area or the Sidebar icon and select Properties, or go to Control Panel and select the Windows Sidebar Properties component. In the box which opens, you can select from the following options covered below:

Start Sidebar when Windows starts: Even if the Sidebar itself is not being displayed (see further below), to display and access Gadgets on your Desktop, the Sidebar process needs to start at Windows Startup, so this box should be ticked. Alternatively you can manually start the Sidebar at any time by going to Start>Search Box, typing *sidebar* and pressing Enter. If you wish to disable the Sidebar and Gadgets altogether untick this box.

Sidebar is always on top of other windows: This option forces the Sidebar to remain on top of all other open windows. This is not recommended as it can get in the way. Ticking this option does not force all floating Gadgets to remain on top of open windows; only those which are docked onto the Sidebar. To force a single Gadget to remain on top of all open windows see further below.

Display Sidebar on this side of the screen: Choose whether to have the Sidebar on the left or right side of the screen. Set to suit your taste.

View list of running gadgets: Clicking this button shows all the currently active Gadgets.

Gadgets: These are the individual small programs which can either sit on the Sidebar, or can be dragged and dropped anywhere to 'float' on your Desktop. Almost every Gadget has options which can be customized, so right-click on the Gadget and select Options to see its individual options, or left-click on the small wrench which appears at the top right when you hover over the Gadget. When you right-click on a Gadget you can also determine how transparent it is by selecting the Opacity item and choosing a percentage; you can select whether the individual Gadget remains on top of all open windows by ticking 'Always on top'; or you can 'Attach it to Sidebar' to remove it from floating mode. Note that you can temporarily bring all Gadgets to the top of all open windows by pressing WINDOWS+SPACEBAR.

Gadgets can be detached or attached to the Sidebar as you wish just by dragging and dropping them. In fact if you detach all the Gadgets from the Sidebar, you can remove the Sidebar from view altogether if you wish by right-clicking on the Sidebar area and selecting 'Close Sidebar'. Aside from the default Gadgets already provided which you can choose from - right-click on the Sidebar or a Gadget and select 'Add Gadgets' - you can download and add new ones by going to the Windows Live Gallery. You can also download and use the Amnesty Generator to allow you to make custom Gadgets out of a range of existing small programs from around the web, or use the Windows Sidebar Styler to make custom Gadgets.

In general Gadgets usually have a relatively insignificant impact on Desktop performance, and of course no impact on gaming performance since everything on the Desktop is suspended. Far from being just a gimmick they can actually become very useful as informational tools and even help in troubleshooting problems - for example you can use the CPU Meter Gadget to display and monitor real-time CPU or memory usage while using certain programs. See if you can find Gadgets to suit your needs.

Copyright © 2010 Koroush Ghazi

< DESKTOP FONTS

Windows Vista contains several new fonts, including Segoe UI, Constantia, Cambria, Corbel, Candara, Calibri, and Consolas. These give Vista its distinctive look, however if for any reason you wish to change the font type, size and general clarity of the user interface, the first place to look is under the Personalization component of the Control Panel. Select 'Windows Color and Appearance', then click the 'open classic appearance properties for more color options' link. Here you can adjust some important settings related to the appearance of fonts in Vista:

Effects: Click this button and you can choose whether to use font smoothing (recommended), and whether you use ClearType or not. ClearType is a particular type of technology designed to make text clearer, particularly on fixed pixel displays such as LCD or Plasma, so I recommend that if you run such a display that you tick the box and set this option to ClearType. If you run a CRT, or just want to see what text looks like without ClearType, set this option to Standard, click OK then click Apply - now check to see whether text quality has improved (you may have to press F5 to refresh the screen). If you want to adjust the appearance of ClearType text you can use the ClearType Tuner.

If instead of installing the program above you want to manually customize ClearType text appearance then go to the following key in the registry:

```
[HKEY_CURRENT_USER\Control Panel\Desktop]

FontSmoothingGamma=0
FontSmoothingOrientation=1
```

The first DWORD above determines how bright or dark the text will be. The default is fine, however you can increase it up to a maximum of 2200 (in Decimal view) to customize the appearance of ClearType text; the higher the value, the lighter and thinner text will be. The second DWORD above determines the type of display used, with 0=CRT, 1=Standard fixed-pixel RGB display, and 2=fixed pixel display using non-standard BGR arrangement.

Advanced: If you wish to change the actual fonts and font sizes used for particular interface elements, click the Advanced button and you can now select a particular component of the interface in the Item box, and not only customize its size and color, but for relevant elements, you can also change the font and font size used. If you don't wish to make this change manually, and want to apply a global change to all the fonts used for the interface, you can access the specific font types and settings under the following registry keys:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Fonts]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
FontSubstitutes]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\FontMapper\FamilyDefaults]

[HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]
```

By specifying different font names and filenames in the relevant keys above, you can change the appearance of the entire Vista interface. For example, changing the line in the registry under the following key:

Copyright © 2010 Koroush Ghazi

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Fonts]

Times New Roman (TrueType)=times.ttf
```

to

```
Times New Roman (TrueType)=segoeui.ttf
```

Will tell Vista to use the Segoe UI TrueType font in all places where Times New Roman would normally be used in the Vista interface. All the font names can be found under the Fonts component in the Control Panel - right click on a font there, select Properties and you will see its real filename. Make sure to backup the registry and set a Restore Point first as this cannot be undone any other way. For a simpler but less thorough method of changing the size of fonts displayed see below.

INTERFACE FONT SIZE

If you find that Vista's screen fonts are generally too small especially at higher resolutions, you can easily change the Dots Per Inch (DPI) Scaling setting which will resolve this issue. Go to the Control Panel, open Personalization and click the 'Adjust font size (DPI)' link in the left pane. Here you can adjust the DPI font scaling to a larger number than the default of 96, thereby increasing text size without altering any other aspect of the interface. To scale the text to suit your needs, click the 'Custom DPI' button at the bottom right of the DPI Scaling box, and either enter a percentage of the normal size you wish to scale to, or drag the ruler with your mouse. The 'Use Windows XP style DPI Scaling' box should be ticked to prevent some programs which were not originally designed to work with Vista's DPI scaling from showing blurry fonts. Once done, click OK then click Apply and the changes should come into effect.

CUSTOM FONTS

Vista has a built-in font editing utility called Private Character Editor which you can access by going to Start>Search Box, typing *eudcedit* and pressing Enter. It allows you to create custom fonts which you can then insert into documents using the Character Map utility. For more details see this Microsoft Article.

< DESKTOP ICONS

Vista uses a new icon system which results in smoothly scalable icons: all system icons in Vista can be smoothly resized using a slider from within Windows Explorer, and most any program or file icon can be rescaled or set to display as a Live Icons; thumbnails of the actual contents of a file - see the Windows Explorer chapter for details.

To adjust the appearance of Desktop icons, you can right-click on an empty space on the Desktop and under the View menu select either Classic, Medium or Large icon size; whether to let Vista 'Auto Arrange' the icon layout; or 'Align to Grid' to place an invisible grid on the Desktop that icons will 'snap' to when moved. You can even disable Desktop icons if you so wish, though this is not recommended. Fortunately there is much more that can be done to customize the Desktop icon size, layout and appearance, and these tips are covered below:

RESIZE DESKTOP ICONS

You can manually resize the Desktop icons beyond the three fixed sizes already available. To do so click once on an empty spot on the Desktop, then hold down the CTRL button while using the scrollwheel on your mouse to gradually increase (scroll up) or decrease (scroll down) the size of the icons to suit your taste. This works much like the resizing slider in Windows Explorer. Note that icons not designed for Vista will not scale well, and beyond a certain size cannot be made any larger; default system icons and program icons designed for Vista will scale smoothly due to the new icon system.

Copyright © 2010 Koroush Ghazi

REMOVE TEXT FROM DESKTOP ICONS

To remove the text beneath any icon on your Desktop, follow these steps:

1. Right-click on the icon whose title you want to remove and select Rename.
2. Instead of entering any characters in the text box, hold down the ALT key and type 255 (ALT + 2 + 5 + 5). Note that you need to use the NUMPAD number keys for this to work, that is the numbers to the right of your arrow keys, not the ones at the top of the keyboard.
3. When you release the ALT key the title will be blank, and you can press Enter to accept this. Blank titles are usually denied under Windows, but not when done this way as it inserts a special blank character.
4. For every icon whose title you wish to remove, do the same as above. However since no two icons can have the same name, for each subsequent icon you'll have to add an additional ALT 255 to the end of the string you enter. E.g. to blank a second icon name you'll need to hold down ALT and type 255, release, then hold ALT and type 255 again, then release and press Enter. For a third, you'll have to type ALT 255, ALT 255, ALT 255, Enter and so on.

If you want to regain the icon names you will have to manually edit each icon's name.

REMOVE SHORTCUT ARROWS FROM ICONS

The small Shortcut Arrows which display at the bottom left of any shortcut icon are associated with the following Registry entry:

```
[HKEY_CLASSES_ROOT\lnkfile]

IsShortcut=
```

The STRING entry above can be deleted to remove shortcuts, however this will cause a range of problems, such as being unable to launch certain links (e.g. Games Explorer game links). Therefore the best way to actually remove shortcut arrows is to use a free utility called Vista Shortcut Overlay Remover. Download and install the FxVisor program, then launch it and select the type of shortcut arrow appearance you like, and once your session is restarted the change should be applied. If it doesn't work for you, try the older versions of the FXVisor program - download either the FXVisor 32-bit or FXVisor 64-bit version as relevant.

CREATE DESKTOP ICONS FOR SHUTDOWN OR RESTART

Instead of using the Shutdown or Restart options available from the Start Menu, you can create icons which automatically perform the same functions with just a double-click. These icons can then be placed on the Desktop for your convenience, or pinned to Quick Launch bar for quick access. Follow these instructions

Shutdown Icon:

1. Right click on an empty area on your desktop.
2. Select New>Shortcut.
3. In the first box of the Create Shortcut Wizard, type the following and click Next:

   ```
   shutdown /s /t 00
   ```

4. Call the shortcut something descriptive like Shutdown and click Finish. Alternatively you can remove its name altogether using the Remove Text from Desktop Icons tip further above.
5. Right click on this new icon, select Properties, click the Change Icon button and select an appropriate icon and click Apply.

Copyright © 2010 Koroush Ghazi

Reboot Icon:

To create a Reboot icon, follow the same steps as above, but substitute the following steps in place of the corresponding ones above:

3. In the first box of the Create Shortcut Wizard, type the following and click Next:

```
shutdown /r /t 00
```

4. Call the shortcut something descriptive like Restart and click Finish.

Double-clicking any of these icons will commence shutdown or restart straight away without any warning. If you want a countdown before shutdown or restart, substitute an amount of time in seconds in place of the '00' entries in the shortcut properties above (e.g. `shutdown /s /t 10` gives 10 seconds warning before shutting down). Also note that once these processes begin they can't be aborted. If you want more command line switches which can be used with the shutdown command, open a command prompt and type `shutdown /?` and press Enter.

SAVE DESKTOP ICON POSITIONS

This tweak allows you to save the current positions of your desktop icons so that if the icons are rearranged or moved you can quickly restore them back to their saved positions at any time. To give you this added functionality do the following on Windows Vista 32-bit:

1. Download the file Layout.zip (mirror) and extract the contents to an empty directory.
2. Copy the *Layout.dll* file to your *\Windows\System32* directory.
3. Double-click on the *Layout.reg* file to automatically make the appropriate changes to your Registry.
4. Go to your Desktop and arrange all your icons as you would like them to be saved.
5. Once done, right-click on the Recycle Bin and select the new 'Save Desktop Icon Layout' option. The positions of all the icons are now saved.
6. You can move the icons around freely and whenever you want them restored to their original saved positions, right-click on Recycle Bin again and select 'Restore Desktop Icon Layout'.

If you're using Windows Vista 64-bit, the above method won't work. You must use the Dips64 utility instead. Install Dips64, then to save or restore the desktop icon position at any time, left-click on an empty area of your Desktop to make sure no icon is highlighted. Now hold down the SHIFT key while right-clicking on the empty spot to access the relevant 'Save icon positions' and 'Restore icon positions' context menu items.

SET SPACING BETWEEN DESKTOP ICONS

To adjust the spaces between your desktop icons, you can manually move them. However if you've chosen automatic spacing - that is, right-click on the Desktop and select Arrange Icons by>Auto Arrange - then you can still adjust the fixed vertical and horizontal spaces placed between each icon by doing the following:

1. Right-click on the Desktop and choose Personalization.
2. Select the 'Window Colors and Appearance' item.
3. Click the 'Open classic appearance properties for more color options'.
4. Click the Advanced button, and under Items select 'Icon Spacing (Horizontal)' and 'Icon Spacing (Vertical)' and edit their values to determine how many pixels are placed between the icons. The defaults are 43 pixels between icons. Smaller values squeeze them closer together, higher values spread them further apart. Click Ok then click Apply and the changes should immediately impact on the Desktop.

Copyright © 2010 Koroush Ghazi

Note that by changing these icon spacing values, you will also change the spacing between all icons in windows as well, such as in the Control Panel window for example.

REMOVE '- SHORTCUT' FROM NEW SHORTCUTS

Whenever you create a new shortcut, the words '- Shortcut' appear at the end of the shortcut's name. To remove this default suffix for new shortcuts, open Registry Editor and change the following:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer]

Link=1E 00 00 00
```

Create this BINARY value if it doesn't exist and set it equal to 00 00 00 00 to remove the '- Shortcut' suffix on new shortcuts. Reboot Windows to implement the change.

ADVANCED ICON CUSTOMIZATION

You can use the free Iconoid utility to further customize the appearance of your desktop icons, such as whether they have a transparent background or a solid color, the color of the text used for icon titles, whether icons are automatically hidden until you move your mouse over them, and so forth. For the most part the utility is fairly straightforward to use, however click the Help button if you need further instructions.

If you wish to create or edit Windows Vista scalable icons, you can use the free Paint.NET program combined with this free Icon/Cursor Plugin. Alternatively, you can use the RealWorld Icon Editor, though it is only free for a trial period. Using original .PNG images for best results, you will be able to create a high quality .ICO file for use as a replacement for any program or folder icon. To change any program file icon, simply right-click on it, select Properties, click the 'Change icon' button and browse to your custom .ICO file and select it, then click Apply. Or you can browse to the *Imageres.dll* or *Shell32.dll* files, both found under the *\Windows\System32* directory, to view a range of built-in Windows icons.

REPAIR INCORRECTLY DISPLAYED ICONS

By default Windows stores a range of commonly used icons in a cache to speed up their display on the Windows Desktop for example. If you are experiencing problems with your icons displaying incorrectly, go to the *\Users\[username]\AppData\Local* directory under your personal folders and delete the file *IconCache.db*. Reboot Windows and this file will be recreated afresh, resolving any incorrectly displayed icons.

< GENERAL INTERFACE CUSTOMIZATION

The following are some general interface customizations that most users should find handy:

INCREASE MENU DISPLAY SPEED

Whenever you open a menu in Vista, the speed with which it opens might seem a bit slow. This is not necessarily due to any performance issues, it has to do with the fact that by default Vista waits a fraction of a second before opening a menu. You can adjust this delay under the following registry key:

```
[HKEY_CURRENT_USER\Control Panel\Desktop]

MenuShowDelay=400
```

The default delay is 400 milliseconds, which is just less than half a second. You can lower this value to increase menu responsiveness - try a value of 80 for example and see how it feels.

Copyright © 2010 Koroush Ghazi

Customize Vista Boot Screen

Already covered under the Boot Configuration chapter is the 'No GUI Boot' option which you can easily enable under the Boot tab of the MSConfig utility. This replaces the 'scrolling green bar' Vista boot screen with the Aurora desktop image. However you can further customize Vista's boot screen by using the Vista Boot Logo Generator. This free utility allows you to turn any 24-bit .BMP file into a boot screen image for Vista, which you should then copy into your *\Windows\System32\en-US* (or relevant language) directory, and then enable the No GUI Boot option in MSConfig for it to work.

Create Custom Desktop Toolbar

If you want to create a full length separate customized toolbar on your Desktop, follow these steps:

1. Go to the Windows Desktop.
2. Right-click on an empty area and select New>Folder.
3. Give the new folder a name, then double-click on it to open it.
4. Drag and drop any files, folders or shortcuts you wish into this folder, then close it.
5. Drag the folder icon to the very edge of your screen and drop it.

The custom folder you created will suddenly turn into a full-length toolbar complete with all your files, folders and shortcuts each shown as an icon on the toolbar. You can resize the toolbar's width, and by right-clicking on it you can access further options such as being able to enable or disable its title, any text shown, and whether it shows small or large icons. To close it simply right-click on it and select 'Close toolbar'.

Slow Down Vista Animations

If you want to enable the ability to slow down Vista Desktop animations, such as when maximizing or minimizing windows, go to the following registry key:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\DWM]

AnimationsShiftKey=1
```

Add the DWORD shown above and set it to =1. Reboot your system, and now whenever you hold down the SHIFT key while an animation is playing, it will slow down so you can see precisely what it's doing. This is more of a novelty than something to permanently enable, so delete the entry above if you want to remove it.

Customize 3D Task Switching

By default, pressing WINDOWS+TAB brings up the Windows 3D Flip task switcher. If you want to have 3D Flip remain in 3D mode without having to hold down WINDOWS+TAB, use CTRL+WINDOWS+TAB instead; now 3D Flip will remain as such when you let go, and you can use the TAB key or the arrow keys to cycle through open windows and press ESC to return to normal 2D mode.

If you want to change the number of windows that 3D Flip shows at any one time (the default is ten), then go to the following registry entry:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\DWM]

Max3DWindows=5
```

Create the DWORD above and assign it a number in Decimal view to match how many open windows you want 3D Flip to show at any one time, though note that higher values may reduce the responsiveness of 3D Flip on some systems. Reboot for the change to come into effect.

Copyright © 2010 Koroush Ghazi

If instead of the default Windows 3D Flip you want another neat way of flipping through open tasks, you can use the free SmartFlip utility. This tool allows you to cycle open windows in a 2D/3D rotational manner and is customizable.

If you simply want to disable the 3D Flip functionality altogether, go to the follow registry entry:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DWM]

DisallowFlip3d=1
```

Right-click on the `Windows` key in the left pane and create a new key called `DWM` under it. Then click on `DWM`, and in the right pane create a new DWORD as shown above and assign it a value of 1, and reboot - Flip 3D will no longer work. If you want to regain this functionality, simply delete the key above.

CUSTOMIZE OTHER INTERFACE COMPONENTS

There are several other aspects of the Vista interface you can customize using Ave's Vista Apps. These useful free customizations include a 3D User Account picture on the Start Menu, Glass Toasts-style balloon notifications, Thumbnail Resizer for Taskbar thumbnails, an Active Desktop replacement, a utility to add custom Folder Background images, and a Desktop Effects dynamic desktop add-on.

MULTI MONITOR CUSTOMIZATION

If you run a dual or multi-monitor setup with Vista, there are a range of additional features you can customize using the tool UltraMon. The tool is free for a trial period if you wish to see if provides features you need.

< DIRECTX 10 & DIRECTX 11

With Vista Microsoft introduced a new foundation for multimedia called DirectX 10 (DX10). DirectX is a collection of Application Programming Interfaces (APIs) which include Direct3D for advanced graphics, and DirectSound and Direct3DSound for advanced sound. Version 10 of DirectX was rebuilt from the ground up, removing a great deal of legacy support and sub-optimal features found in earlier DirectX releases. This means that DirectX 10 and the newer DirectX 11 are not backward compatible with Windows XP or older graphics hardware. More details can found in this Microsoft Article and this Microsoft Article. However DirectX is not the only API which can be used under Vista - OpenGL (for graphics) and OpenAL (for sound) are third party open-source alternatives which are supported and fully functional under Windows Vista.

The potential benefits of DX10 are demonstrated in this Microsoft Article, and in plain English include:

- Unified Shaders, which mean more efficient use of graphics hardware for complex shader effects.
- The addition of a new Geometry Shader to add to Pixel and Vertex shaders. This shader type allows a range of 'organic' special effects without reliance on the CPU.
- Paging of graphics memory, allowing Video RAM to page data to the System RAM and back. This allows games to use much larger textures for example.
- Texture arrays allow texture swapping to occur without CPU intervention. In fact due to a range of CPU/GPU resource balance improvements such as the Geometry Shader further above, the CPU is much less likely to bottleneck the GPU.
- Removal of the limits on the number of objects rendered.
- Improved Instancing which allows multiple objects of the same type (e.g. multiple trees, grass or people) to be rendered much more quickly.

Copyright © 2010 Koroush Ghazi

§ Removal of backward compatibility with DX9 means the potential for improved performance. Because DX10 has been built from scratch it isn't constrained by the usual compromises needed to run legacy hardware.

While the changes in DirectX 10 are designed to make it easier for programmers to develop advanced games, the choice of which API to use for particular games for example still depends on the software developer. Many current games are still programmed for use primarily under DirectX 9.0 (DX9), so Vista also contains a version of DirectX 9.0 called DirectX 9.0EX (Extended). This version of DX9 was introduced in Vista and is based on the Windows Display Driver Model, so it cannot be used under Windows XP.

As of Vista SP1, the DirectX version in Windows Vista has been upgraded to DirectX 10.1. This is simply an incremental update of the base DirectX 10.0, and contains more improvements and higher standards for game developers to follow.

Furthermore, a Platform Update has been released for Vista which allows it to use the newer DirectX 11 found in Windows 7. Unlike the transition from DirectX 9 to DirectX 10, DirectX 11 is an extension of the features of DirectX 10, not a re-write, and as such, some of the features of DirectX 11, such as multithreaded rendering improvements, can also be utilized on existing DirectX 10-capable graphics cards. Tessellation and other Shader Model 5.0 features on the other hand require dedicated DirectX 11-capable graphics cards.

The changes in DirectX 10 and DirectX 11 are of greatest benefit to gamers. However the important thing to note if you want to undertake gaming using these newer versions of DirectX is that it will require three things:

§ Games written to take advantage of DX10 or DX11 - Most existing and upcoming PC games are actually developed using DirectX 9, because the games were originally made for the popular consoles which have ageing hardware that only supports DX9. These games are then ported across to the PC and in the process they may, in a few cases, have some DX10 or DX11 features tacked on. This means that in practice, most games do not truly take advantage of the features in these newer DirectX versions. A list of games which support DirectX 10 can be found here, and a similar list of games supporting DirectX 11 can be found here.
§ DX10 or DX11 Capable Graphics Hardware - You must have a graphics card specifically designed to provide hardware support for DirectX 10 or DirectX 11 to be able to utilize these newer versions of DirectX. For DirectX 10 capability this means an Nvidia GeForce 8000 series or ATI HD 2000 series or newer graphics card. For DirectX 11 capability this means a GeForce GTX 400 or ATI HD 5000 series or newer graphics card. If you do not have a full DX10 or DX11-capable graphics card then you cannot run a game in DX10 or DX11 mode as relevant; there is no way around this.
§ WDDM Graphics Drivers - You must have the latest WDDM graphics drivers to run DX10 or DX11 in Windows Vista with optimal performance and with access to full functionality.

It does bear noting that most games which are capable of rendering in DX9, DX10 and/or DX11 usually perform noticeably better under DX9 mode in Vista. DX10 or DX11 modes may have improved image quality, but this usually comes at the cost of a drop in performance. In theory the newer DirectX versions provide the potential for both better performance and better graphics than DX9, but in practice because games are currently being developed for ageing console platforms using DX9, the full advantages of newer DirectX versions are not being programmed into games from the ground up, resulting in minimal benefits and sub-optimal performance.

In any case, regardless of which version of DirectX you are using, make sure it is always kept up to date by installing the latest DirectX update - details are in the Windows Drivers chapter.

Copyright © 2010 Koroush Ghazi

< GAMING IN VISTA

This book has already been written with gamers in mind, so there are no specific performance tips or changes in this section for gamers - follow the recommendations throughout this book to get improved performance in both games and general Windows usage. However I cover a specific game-related Windows feature below.

GAMES EXPLORER

Games Explorer is a central location for games in Vista, both the standard Windows games built into Vista such as Hearts and Solitaire, as well as any games you have installed yourself. You can access it by opening the Games item on the Start Menu, or by going to Start>Search Box, typing *games explorer* and pressing Enter. By default the Games Explorer contains all the built-in Windows games, and also any 'Games for Windows' branded games you've installed on your system - these are automatically added to Games Explorer upon installation. For any games which are missing from Games Explorer, simply drag and drop their launch icon into the Games Explorer window and they'll be added instantly. If you want easier access to Games Explorer, drag and drop the Games item from your Start Menu onto your desktop. This allows easy access to all your games from a single place, reducing desktop clutter by replacing all the individual game icons.

To configure Games Explorer, aside from the usual Windows Explorer-related choices such as the View type, click the Options button in the green Command Bar area and choose whether to allow Games Explorer to download game-related information, and whether to list the recently played games. I recommend that you enable both these options to make Games Explorer much more useful.

The main features are covered below:

Game Details: If you have the Details pane enabled in Windows Explorer - see the Windows Explorer chapter - when you click on a game icon you will see in the Details pane at the bottom some useful information about the game's release date, version number, publisher and developer, and you can click on the links in this pane to take you to the game's home page.

If you have the Preview Pane enabled as well, a preview of the game's box cover is also shown in the right hand pane, and for games which support it, a listing of your current Windows Experience Index (WEI) performance rating, and the game's required and recommended WEI performance ratings. The WEI is covered in more detail under the Performance Measurement & Diagnostics chapter. It is a good indicator of the strengths and weaknesses of your system, so do not ignore it - check the detailed breakdown of your WEI score to see which areas need improvement. In particular if your system does not meet the recommended WEI score, then you may not experience a satisfactory level of image quality and performance from the game. Games developers can even customize games such that they automatically disable or reduce certain features if your WEI score is not sufficient for full functionality, but for the majority of games, even if you don't meet the minimum WEI score, Games Explorer does not prevent you from launching the game.

Tools Button: In the green Command Bar area of the Games Explorer you can click on the Tools button and you will see shortcuts to games-related functionality in Vista, including Audio Devices, Display Devices, Input Devices and Performance Information and Tools. These are all covered throughout various chapters in this book, however having them all under one button here allows quicker access.

Community & Support Button: If a game supports it, when highlighted you can click on the 'Community and Support' button in the Command Bar area to see links to the game's home page, support page, forums and so forth.

Note that you can also access many of the features above simply by right-clicking on the selected game.

Copyright © 2010 Koroush Ghazi

Adding Missing Games: If an installed game on your system is missing from Games Explorer, you can still add it by dragging and dropping a game icon or game executable into the Games Explorer window. However this doesn't necessarily create the full details Games Explorer needs to define things like box art, support links and so forth. These details will either be downloaded by Games Explorer from the Internet if the 'Download Information about installed games' item is ticked under the Options button, or are provided in an appropriate .XML file along with the game.

If neither is working, or if you want to manually edit game details for a game in Games Explorer, they are held under the following area of the Windows Registry:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\GameUX]
```

For games which support Games Explorer, you will find their entries as a string of numbers under the `Games` key (each one refers to a different game), and look in the right pane for the `Title` entry which shows which game it is. For games which don't natively support Games Explorer, you will find their entries under the key which is a string of numbers itself (it corresponds with a user account). Once the correct folder has been found, you can edit entries, and if you have another game with full details, click on its key and you can replicate similar entries in the key for the games which lack them. However manually editing game entries is generally not recommended.

Instead of editing registry entries, the best path to take if you want to add correct details, a proper box cover image and so forth is to use the free Game Explorer Editor utility. This utility provides a graphical interface for properly editing and configuring games in Games Explorer. Its usage is relatively straightforward, however if you want more instructions click the Tutorial link on the right side of the utility's website. Note that if you manually want to find boxart for any game, go to AllGame, and note further that you cannot edit ESRB Ratings for games, as these must be digitally signed to work.

Some additional useful functionality in Games Explorer includes:

§ Playing in DX9 Mode - By default most DX10-capable games will launch in DX10 mode whenever you start them in Vista, whether from Games Explorer or a desktop icon. To actually choose which mode to start a game in, right-click on it in Games Explorer and select 'Play - DX9' or 'Play - DX10' (or similar) as appropriate, launching the game in that mode. This is a handy choice to have because DX9 mode is usually faster than DX10 or DX11 modes in most games, with minimal image quality difference. Note that if you want to make DX9 mode the default mode for launching a game in Games Explorer, right-click on the game, select Customize, highlight the 'Play - DX9' (or similar) item and click the 'Move Up' button until it sits at the top of the list.

§ Custom Launch Commands - If you want to customize precisely what command(s) is executed when you launch a game from Games Explorer, right-click on the game and select the Customize option. In the box which opens highlight the first Play option and click Edit. You can add custom switches here which vary by game. For example, for some games to skip the startup movies you can add a *-nointro* command switch. The precise switches to use are different for most games, so you will need a reference source for the correct commands to use. See my Game Guides for example.

§ Hiding Unused Games - Instead of uninstalling a game or deleting it from Games Explorer, you can simply hide its icon. This is useful if you don't want to see particular games which you rarely (or never) play, especially some of the built-in Windows games. Right-click on the relevant game icon, select 'Hide This Game', and its icon will be removed. To regain this icon at any time click the Options button at the top of Games Explorer and click the 'Unhide Games' button.

§ Finding Saved Games - To find the saved games for any game, instead of looking around your drive, you can simply right-click on a game in Games Explorer and if a 'Saved Games' option exists, click it and you will be taken straight to the directory on your drive where the relevant saved games are held. This is useful if you want to back them up prior to reformatting your drive, or reinstalling the game for

Copyright © 2010 Koroush Ghazi

example, and they can then be restored afterwards in the same folder on your new installation so that you can resume play from the same spot.

As you can see, Games Explorer is actually a very useful feature for gaming in Vista. Almost all modern games support its core features, so it should be the central place for you to organize, customize and launch your games.

Problems Launching Games

If you are having problems launching or running games under Vista, you can try resolving it by one or all of the following methods:

- If UAC is enabled, make sure the game is being run in Administrator mode. Some games - particularly older games - will not request Admin access even if they require it, and hence will not run properly. Right-click on the game's launch icon and select 'Run as Administrator', or right-click on it, select Properties and under the Compatibility tab select 'Run this program as an administrator', or click Advanced under the Shortcut tab and tick the 'Run as Administrator' box. See the UAC section under the PC Security chapter for details.
- Make sure that you are using the latest Vista-compatible graphics drivers. See the Windows Drivers chapter for links to the relevant graphics hardware manufacturers.
- Make sure you have updated to the latest version of DirectX as covered in the Windows Drivers chapter. Updating DirectX this way is a necessity for newer games to function properly.
- If all else fails, run the game in Windows XP compatibility mode. Right-click on the game's launch icon, select Properties and under the Compatibility tab, tick the 'Run this program in compatibility mode' box and select 'Windows XP (Service Pack 2)' - which is the most compatible option - then click OK.

Make sure to also refer to the Performance Measurement & Diagnostics chapter if you are having problems with games. It bears noting that Windows Vista performs much the same as Windows 7 when it comes to gaming, so there is no reason to blame Vista for your gaming problems; most gaming problems are due to general system issues such as overheating hardware or overclocking; sub-optimal or incorrect settings in the BIOS; outdated or badly installed driver(s); conflicting background programs; misconfiguration of game settings, etc. Vista may have improved stability and performance, but all of the above issues (and more) will still cause problems - no OS can overcome these types of things, it is up to the user to understand how their system works and best configure their machine for optimal usage, which is precisely what this book is about.

Copyright © 2010 Koroush Ghazi

OVERCLOCKING

When people want additional performance from their machines, they may undertake a procedure called Overclocking. This is the process of increasing the clock speed of a component in your PC above its normal specifications, hence the term 'over clocking'. The clock referred to is a specialized oscillator pulsing with a frequency that determines the rate at which a data processor can perform instructions. The theory of overclocking is simple: increase this clock speed and you will increase the rate at which instructions are performed, leading to a faster PC. Overclocking is possible on a range of hardware components including CPUs, Graphics cards, Motherboards and RAM.

Another method of overclocking which doesn't involve increasing the clock rate is by altering timings. Memory-based components such as system RAM and Video RAM have latency timings - rest periods between operations measured in clock cycles. By decreasing the latency time, a memory component can be made to wait less between completing specific operations and hence function faster.

So why are these methods possible? Why aren't the hardware components you buy not already performing to their peak potential? The reason for this is that hardware components are expected to work in diverse environmental conditions and be put to vastly different tasks. Hardware manufacturers ensure safe headroom is provided so that in adverse conditions the component can still operate safely and with stability. Overclocking takes up this slack by pushing the component beyond manufacturers' specifications.

Of course when you push a component beyond its recommended specifications the component requires ideal conditions to continue operating with stability. That usually means more cooling on/around the component, since any cooling device it already uses is only really designed to deal with stock operation. The component also requires stable voltage from the Power Supply either directly or through the motherboard. Often to achieve a stable overclock the component may also require additional voltage, which in turn can add to heat and hence raise the cooling requirements even further. Furthermore, the additional heat being dissipated from one component may cause other nearby components to overheat. As you can see overclocking is not as simple as it first appears, and there are often complex interactions involved both at the hardware and software level which must be taken into account to achieve proper stability. This chapter examines the general theory and operation of overclocking, and is a starting point for people interested in this topic.

< BENEFITS AND DRAWBACKS

Before going into any more detail about overclocking it is important to discuss the advantages and disadvantages of overclocking objectively, so you don't undertake it without knowing what you're getting yourself into:

BENEFITS

§ Increased performance - this is of course the primary reason why people overclock. The degree to which performance improves depends on the component(s) being overclocked, how far they are overclocked, and whether they are the hardware most relied upon by particular games and applications. The performance difference can be anywhere from negligible to quite significant.

§ Bragging rights or 'coolness factor' attached to overclocking - some people gain a great deal of satisfaction and prestige in having the fastest machine, or the highest overclocked component, or the highest benchmark score. Or they may simply feel they are extracting the most out of their hardware by overclocking it. Some people also enjoy the tinkering and hobbyist aspect of overclocking and hardware modification.

Copyright © 2010 Koroush Ghazi

DRAWBACKS

- There will be costs in providing improved cooling - in almost all cases you will have to purchase more effective and/or additional cooling for your system in the form of more efficient heatsinks and/or more fans, a case with more space or better airflow, or specialized equipment like a water cooling setup. Of course if you start out by planning your system purchase carefully, you can minimize the additional costs to some extent by beginning with the right components.
- The overclocked component, and therefore your entire system, may become unstable and crash randomly - without a doubt the number one cause of problems in games and applications is overclocking. People often refuse to acknowledge that their overclocking is the cause of the problem, and mistakenly blame Windows, their drivers or the game or application instead. Different programs react differently to overclocking. Some can tolerate much higher levels of overclocking on particular components, some cannot tolerate any overclocking at all; it all depends on how stressful the game or program is, and how stable or unstable the overclock actually is in your particular setup.
- Potential data corruption if certain components are pushed beyond their limits - pushing components like the CPU or RAM beyond their limits on your system can result in instability leading to data corruption, up to and including the loss of all your data. Often this data corruption can occur subtly over time without any indication or warning.
- Excessive heat can damage or permanently kill a component - since computer hardware is based on sensitive electronic equipment, if a hardware component is not kept adequately cool (and even in some cases if it is) it can be permanently damaged or destroyed through overclocking. It happens quite often, especially with graphics cards, so it is not as rare as might be thought.
- Overclocking automatically voids the warranty on the component - most hardware manufacturers make it clear that overclocking beyond recommended clock speeds or timings will instantly void your warranty. This also goes for any physical modifications to the hardware such as changing its cooling. Unless explicitly stated otherwise, a warranty is only designed to cover unmodified hardware operating within specifications.
- Overclocking reduces the life span of the component - since the component is working beyond specification and working hotter and faster than it was designed to handle, most components will have reduced life spans. This can reduce the useful life of a component sometimes negligibly or sometimes noticeably, depending on the extremity of the overclock, the quality of the components, and how well the components are kept cool and powered. A mild overclock typically has little or no practical impact on the life expectancy of a component; an extreme overclock can drastically reduce the error-free life of a component.

So far the disadvantages appear to far outweigh the advantages of overclocking. This is not strictly true, it all depends on how far you overclock a component and how much performance you can gain in return, as well as the quality of the hardware itself. It's important to point out that it overclocking is not a simple or even beneficial procedure at all times. Despite everyone urging you to overclock your system you should weigh up the options rationally and either choose to avoid overclocking due to the additional expense and the potentially modest performance gains and/or the strong likelihood of instability/damage; or alternatively research the topic thoroughly and invest the time and money required to achieve a good balance of performance and stability.

The bottom line is if you don't have much time or patience, or you can't afford to replace a vital system component should it get damaged, do not overclock. If your CPU or graphics card dies for example and you can't replace it, your entire computer becomes unusable, so it is not something to be taken lightly simply because people flippantly encourage you to do it.

Copyright © 2010 Koroush Ghazi

< METHODOLOGY

The precise details of how to overclock vary depending on your particular hardware configuration and BIOS options. The information below is only indicative and designed to give you a broad idea of the types of steps involved in overclocking; for more detailed information see the guides linked to at the end of this chapter. Importantly, before commencing any type of overclocking you must make sure you are totally familiar with the exact brand, model and default specifications of your major hardware components. If necessary refer to any packaging or manuals which came with your system, and more importantly see the System Specifications chapter for links to tools which can help you identify your components and their precise capabilities in detail.

Also make sure that before changing any BIOS settings for the purposes of overclocking that you record your existing BIOS settings. This is because in some cases when overclocking beyond the point of stability, you will have to reset your BIOS (or it may reset automatically) back to its factory default settings, losing any customized settings you've put in. So make sure you document what the major BIOS settings are which you've altered through any general BIOS customization.

CPU OVERCLOCKING

Overclocking a CPU on most systems involves entering the BIOS and increasing the speed of the Front Side Bus (FSB) or QuickPath Interconnect (QPI) for Intel CPUs, or HyperTransport (HTT) for AMD CPUs. The FSB/QPI/HTT is the main pathway (Bus or Interconnect) between your major system components, and as its speed increases, information is transferred back and forth more rapidly between all your major components working off this bus speed. There are various settings in the BIOS which alter the speed of these buses or interconnects, however depending on the setting used, you may also be increasing the speed of other components, such as your system RAM. Check the relevant settings in your motherboard manual.

Your CPU also has a Multiplier, which as the name suggests sets the overall CPU speed in MHz as a multiple of the main Bus/Interconnect speed. For example on a system with an effective Bus of 200MHz and a CPU that has a multiplier of 20 gives you a CPU speed of 20x200 = 4000MHz = 4GHz. Note that some CPUs have their multiplier locked at the hardware level, which means you can't actually change it.

RAM OVERCLOCKING

Increasing the speed of your RAM is dependent on a number of factors. Overclocking refers to the process of increasing the clock speed of a component; in the case of system RAM this involves raising the main system Bus/Interconnect frequency and/or simply raising the RAM's Frequency directly to alter the RAM's speed in MHz - depending on your available BIOS options. However you can also alter the Timings (Latency) of a memory chip such that it refreshes faster between operations, meaning less waiting time between each operation and hence faster performance.

Whether increasing RAM speed or lowering latency is the better option is not clear. There is no set answer - it all depends on your particular hardware and the applications you most commonly run as to the precise combination of RAM speed and RAM latency which will perform best and with greatest stability, so you will have to experiment. Generally speaking, applications or games which have large amounts of non-graphics information to transfer to the CPU and back will benefit more from greater RAM speed, which provides more bandwidth. On the other hand applications and particularly games which primarily require very complex calculations with repeated access to information in memory will benefit more from lower RAM latency. Obviously some applications and games require both, so again, there is no clear-cut answer.

RAM overclocking also depends a great deal on how many sticks of RAM you have, their quality, and how similar they are. Because your RAM DIMMs (Dual Inline Memory Modules, also referred to as 'sticks') have to work together in your system, if you have two or more sticks of RAM in your system, you must try and ensure that firstly they are all equally matched in terms of rated speed and timings, and secondly that they

Copyright © 2010 Koroush Ghazi

should ideally be from the same brand and model of RAM. RAM chips can vary in quality and performance, so having mixed brands or types of RAM can lead to a variety of problems - even when running at default speeds.

Graphics Card Overclocking

The following is a modified summary from the overclocking section of the ATI Catalyst Tweak Guide and Nvidia Forceware Tweak Guide. It applies to all graphics cards regardless of brand, however if you are an ATI or Nvidia graphics card user please read through the relevant guide above for full details.

The modern graphics card is a lot like a small computer by itself. It has a Graphics Processing Unit (GPU) which is the graphics equivalent of the CPU, it sits on a motherboard-like Printed Circuit Board (PCB), and has its own Video RAM (VRAM). And just like a computer system, the components on a video card can be overclocked to increase performance. Overclocking a graphics card involves increasing the frequency of the GPU (also called the Engine or Core) and/or the Video RAM (also called VRAM or Graphics Memory). You can overclock one or both of these components, with varying results based on a number of factors, but generally resulting in an increase in performance the higher you overclock each component. To overclock your video card, ideally you'll need a tool which allows you to change the clock speeds of the Core and the VRAM - you can use RivaTuner or ATI Tray Tools for these purposes.

Overclocking your video card is similar to CPU overclocking and RAM overclocking combined - simply increase the clock speed of the Core/Engine, and/or the clock speed of the Graphics Memory, both of which are measured in MHz. The Core generates graphics data, and depending on your CPU and the rest of your system specifications, increasing the core speed can result in a small or large overall performance improvement. The Video Memory transfers information to/from the Core, and increasing its speed can once again improve performance either slightly or significantly, in conjunction with your Core speed and the speed of the rest of your system.

All other things being equal, the higher the resolution being used for a 3D application or game and the higher the graphics settings, and the more recent the game, the greater the potential for graphics card overclocking to yield bigger improvements in performance. This is because newer and more graphically intensive games running at higher resolutions rely heavily on the GPU for their performance.

Remember however that if you have an old or low-end graphics card then overclocking is unlikely to improve performance dramatically. The reason for this is that lower end graphics cards simply do not have hardware support for the advanced functionality demanded by recent games, such as the latest Pixel Shaders and Vertex Shaders. If your card does not have hardware support for a required advanced function, such as a new DirectX 11 feature for example, then overclocking cannot surmount this handicap.

Voltage Adjustment

As components are pushed outside specifications with overclocking, they will do more work. Often they can accommodate this extra work within their current voltage, however sometimes to gain stability and/or to push a component further, you will have to increase the voltage to these components. The three main components that can benefit from voltage tweaking are the CPU, the graphics card and RAM. The two main voltage adjustments you will find in almost any BIOS are CPU Voltage and RAM Voltage, and these are explained below.

CPU Voltage: This is the amount of voltage applied to the CPU. The base voltage will vary depending on the CPU architecture, however make sure to note what your CPU's default voltage is before raising it. The only reason to alter the CPU voltage from its default is that when overclocking your CPU you may notice that you cannot overclock it beyond a certain point, or that you experience a lot of instability at higher clock speeds. Raising the CPU voltage by a small increment in your BIOS may allow the CPU to regain stability and/or

Copyright © 2010 Koroush Ghazi

allow you to push the CPU further. The theory behind raising the CPU voltage is more complex than just supplying more juice to the CPU, and you can read about it in this Wikipedia Article. The most important thing to understand is that upping the voltage beyond a certain point can result in permanent damage to your CPU, and strictly speaking any increase in the voltage can further shorten the life span of a CPU. However for the most part a small bump in voltage can help stabilize an overclocked CPU that is acting slightly unstable. Just remember that more voltage always equals more heat, which requires greater cooling to maintain safe temperatures.

RAM Voltage: Sometimes called DRAM Voltage, this is the amount of voltage for the RAM DIMMs. Just like CPU voltage, increasing RAM voltage can improve stability at higher clock speeds. This is particularly true if you're experiencing random reboots or sudden crashes to desktop, as these are almost always RAM related in some way. Once again, increasing the voltage to your RAM can result in permanent damage so do not overvolt by a substantial amount without first consulting with your motherboard manual to determine the maximum safe voltage level. Implement any increase in RAM voltage in very small increments, and provide additional cooling to prevent heat building in the area surrounding the RAM.

You can view your existing system voltages in the BIOS, however if you want a utility to monitor system voltages from within Windows, use the free CPU-Z or HWMonitor utilities. See the System Specifications and BIOS & Hardware Management chapters for other utilities which may be useful.

There may be additional voltage settings in your BIOS, and unless you have full knowledge of what they do, and what a safe adjustment is, do not alter them as you can permanently damage your components this way.

< STABILITY

Overclocking is pointless if it leads to instability or other problems. The Golden Rule for troubleshooting any problem on an overclocked system is:

Always start by assuming your overclock is the primary source of any problem

Begin the investigation of any problem or strange behavior on your PC by suspecting your overclock as the source of that problem. Reset your entire system to its default speeds and see if the problem persists or is as severe. If the problem goes away, or doesn't happen as often, you can be certain your overclocking is contributing in some way to it, or is the sole cause of it. You will have to lower or remove your overclock and/or increase your cooling. Details on how to correctly test your system for stability are covered in the Performance Measurement & Diagnostics chapter, but bear in mind that even if your system can run every artificial test and benchmark there is for hours on end without a problem, the real test is having complete stability day-in, day-out, even when running stressful games and programs during hot summer days for example. If your system starts behaving strangely, or you are having crashes and problems, don't persist in maintaining your overclock.

Electronic hardware components are highly accurate devices, and forcing them to run outside their normal operating speeds can increase the potential for small errors to creep into their operation. Manufacturers often push a particular component close to its limits by default from the factory, so even a small amount of overclocking can be enough to cause problems. If you're going to overclock, don't do it at the cost of system stability. At the first sign of strange behavior, don't be quick to blame everything else - suspect your overclock first and foremost. Make sure you have optimized and maintained your entire system as covered in this book. Then, and only then, if the problem persists to the same degree, and even after further online research, you still find no solution, you can consider the actual program or game to be buggy in some way. Unfortunately many people start this process the other way around.

Copyright © 2010 Koroush Ghazi

POWER SUPPLY UNIT

See the Hardware Management section of the BIOS & Hardware Management chapter for details on how to determine if your Power Supply Unit (PSU) is appropriate, and whether you need to purchase a new one to ensure stable and optimal performance. Successful overclocking requires a stable source of power, and a poor quality PSU will mean that you experience instability regardless of any other settings you alter. Invest in a good PSU before considering overclocking your system.

COOLING

If you are overclocking, you need to know what the safe temperature range is for all of your major components. There is no single answer, as each different component, indeed different architectures and brands of components, have different safe temperature ranges. Some components such as the CPU and graphics card have built-in thermal throttling which automatically reduces the speed of the hardware if it reaches a preset temperature, however the temperature limits are different for various hardware, and in any case you should never let your component become hot enough to get close to these limits, since prolonged operation at such temperatures reduces the lifespan and increases potential instability. See the BIOS & Hardware Management chapter for more details. Just like a good PSU, if your system does not have decent cooling, then overclocking is a waste of time as it will simply result in system instability and eventual damage to your components.

COMPARING OVERCLOCKS

One of the most common statements heard when people compare overclocks or are told that their overclock is unstable is: "But someone else who has the exact same system can overclock it much higher than me and their games don't crash - it must be a game bug!". A comment like that demonstrates a complete lack of understanding of some fundamental principles of overclocking:

- No two components are exactly the same. Even if the two components being compared are an identical brand, model and speed, they may have very different tolerances to overclocking depending on which factory they were produced in and which revision they are; that is, how early/late into the production run they were produced - for CPUs this is called Stepping.
- No two people have the exact same conditions for their overclocking. Your computer room may be hotter or cooler, your case may provide better or worse cooling, your combination of components may include a different PSU or different brand or speed of RAM, your system may be clogged with more dust, etc.
- Your Windows settings and software environment will not be identical to anyone else's. You may have sub-optimal software settings, background programs that are the source of conflicts, or malware causing problems, or you may even have data corruption.
- No two games are identical in the way they use resources and stress components on your machine, and hence if all of your other games work absolutely fine at a certain level of overclock, it may well be that the latest game you are playing has a completely different tolerance to your overclock and will crash most of the time.

Copyright © 2010 Koroush Ghazi

RESEARCHING OVERCLOCKING

Having stressed the importance of researching overclocking before you dive into it, I recommend that you start by referring to the following guides as relevant for more details. This is obviously not a definitive list of places to research, nor have I personally tested out all the procedures in these guides - they are simply a good starting point, and provide an indication of the types of practical procedures involved in overclocking particular hardware:

General Overclocking Guide 1
General Overclocking Guide 2
Core2Duo Overclocking Guide
Core i7 Overclocking Guide
Core i5 Overclocking Guide
AMD CPU Overclocking Guide
GeForce GTX 275 Overclocking Guide
AMD HD 5750 Overclocking Guide

This chapter has been just a taste of the information available on overclocking. Don't rush into overclocking, do it slowly and methodically, and take the time to search Google and various tech forums for peoples' experiences with overclocking hardware similar to your own. More often than not you will find someone who has a similar setup and who has overclocked it with reasonable success, so look out for such information as it can save you some time in your own experimentation. However be aware that people often have different definitions of 'stable' when it comes to overclocking, or may even outright lie when asked if their system is stable. Also as noted further above, no two systems are identical so don't just automatically assume you can reach the same results as someone else using similar hardware. Take the time to research, read and think about overclocking and make sure you have the right tools and knowledge to undertake it properly, and if in doubt, don't overclock. It is not a necessary procedure and in my opinion, carries more risks than benefits, especially if you value genuine stability and data integrity.

Copyright © 2010 Koroush Ghazi

PERFORMANCE MEASUREMENT & DIAGNOSTICS

Whenever you change various settings on your PC, or install and use particular programs, or alter your hardware in some way, it is difficult to tell whether your overall performance or system stability has improved or decreased. While you can get a general feel for whether things have improved, it is often best to gauge performance and stability changes objectively by using a range of performance measurement tools. By the same token, you may be trying to resolve a problem which is showing up in the form of poor performance, strange behavior or an error message. Through the use of appropriate diagnostic tools and troubleshooting methodology, you can resolve a problem more efficiently.

Fortunately Windows Vista contains a range of handy tools which you can use to both monitor and measure your performance, as well as accurately troubleshoot and diagnose problems. Furthermore, as part of the Windows Diagnostic Infrastructure, Vista can automatically identify and point out potential causes of problems. In addition to Vista's tools there are a range of third party programs which will help you benchmark performance and further assist in isolating the cause of a problem, and these are all covered in this chapter.

The central location for many of Vista's built-in performance and diagnostic tools is the Performance Information and Tools component under the Control Panel. This is an important area of Vista which contains access to a range of tools, and we examine the main ones below.

< WINDOWS EXPERIENCE INDEX

One of the first things Vista does after you have installed Windows is to examine your system with the Windows System Assessment Tool (WinSAT), running a series of tests to calculate the Windows Experience Index (WEI) for your system. This is an important process, and the results are shown as a series of five sub-scores, culminating in a single base score shown as the large number at the right of the sub-scores. The base score is determined by the lowest of your five individual sub-scores; it is not an average or cumulative score.

Windows Vista actually uses this base score and sub-scores to determine a range of things, such as whether your system can display Windows Aero, so the score is quite important and you should investigate areas where you score relatively lowly. From the article linked above, below is a summary of how WinSAT calculates your Windows Experience Index number for each sub-score:

Processor: The results of this score are calculated as a weighted average of the following tests:

- Compression and decompression using the LZW compression algorithm.
- Compression and decompression using the Windows Vista compression algorithm used for hibernation files, ReadyBoost and other features.
- Encryption and decryption assessment.
- Computing hashes.
- Encoding of video.

Memory (RAM): The results of this score are calculated based on the amount of bandwidth (in MB/s) that the memory can move within a certain period. However the highest score attainable is constrained by the amount of system RAM (minus any memory reserved for graphics). This is shown in the table below - e.g. if you have 640MB of system RAM, the highest you can score regardless of RAM speed is 3.5:

Copyright © 2010 Koroush Ghazi

- Less than 256 MB - 1.0
- Less than 500 MB - 2.0
- 512 MB or less - 2.9
- Less than 704 MB - 3.5
- Less than 960 MB - 3.9
- Less than 1.5 GB - 4.5

Graphics: This score is mainly used to determine how your system will run Windows Aero and play back Windows Media Video. It measures video memory bandwidth (in MB/s). Note the following restrictions:

- If your graphics card does not support DX9 then it can only score a maximum of 1.0.
- If the system supports DX9 or higher, but does not have a proper WDDM driver installed than it can only score a maximum of 1.9.

Gaming Graphics: This score is calculated based on how many Frames Per Second (FPS) your graphics card can display for various textures. Note the following restrictions:

- If the graphics card does not support D3D 9 then it can only score a maximum of 1.0.
- If the system supports D3D 9, is DX9 capable and has a WDDM driver, it will score at least 2.0.
- If the score is greater than or equal to 5.0 but the graphics card doesn't support Shader Model 3.0 then the maximum score possible is 4.9.

Primary Hard Disk: This score is calculated based on your primary drive's bandwidth measured in MB/s. All modern hard drives will score a 2.0 or above.

The scoring system has been set up so that at the moment the highest score that any system can attain for any component is 5.9. In the future Microsoft will update Vista to allow for scores higher than this. When looking at your base score, the breakdown of what to expect in Vista is as follows:

- *Base Score 1.0* - This is the absolute minimum specifications needed to run Vista, but without Windows Aero and with a range of general performance problems. Best used only for things like email, Internet browsing, and Solitaire.
- *Base Score 2.0* - This is the recommended minimum specification to run Vista, and may be able to run Windows Aero but with some performance issues. Similar recommended usage scenario as with a Base Score of 1.0, but with greater responsiveness.
- *Base Score 3.0* - This is the 'average' Vista system which can run Windows Aero and perform reasonably well in normal applications, and provide basic performance in games.
- *Base Score 4.0* - This machine will run Vista well and be quite responsive, even in multitasking. Runs most applications and games quite well.
- *Base Score 5.0* - This machine is a high-end machine suitable for excellent performance in gaming, multimedia and multitasking. Some very high-end 5.0 machines may be reclassified as 6.0 when the scoring system is updated.

These scores are not the ultimate test of what a machine is capable of, as clearly different applications and games will rely more on different components. However because of the way the base score is shown not as an average - which would be misleading (e.g. a 1.0 and a 5.0 average out to be 3.0) - but as the lowest of your individual sub-scores, it is very useful for gauging the general performance level of a PC, and its existing bottlenecks. The idea is that it highlights the weakest link of the main hardware components of your system, and there is good reason for this; your system is only as fast as its weakest link.

For instance on a PC which scores a 5.9 on its Gaming Graphics sub-score, you would expect excellent gaming performance, but this is not necessarily so. If the same system scores lowly on other areas then it is

Copyright © 2010 Koroush Ghazi

likely you will run into problems with gaming. Let's say the Memory or Primary Hard Disk score is below 3.0 - this means that while your graphics card can easily handle intensive 3D rendering for a game, your hard drive and/or memory may simply not be fast enough to continually supply the graphics card with the information it needs, and the end result will be major stuttering or frequent loading pauses, or indeed you may not be able to run some games at all due to insufficient RAM. Ideally your scores should be very close to each other, and if you are looking to upgrade your system, then it would be wise to pay attention to which components are scoring lowly. If you want to view other peoples' scores, check on your favorite online forum, or at a site like ShareYourScore

If you're buying a pre-built system then make sure it has a good base score, and don't accept any statements that the Windows Experience Index is not important. A low WEI is an indication of potentially low performance and can also result in certain features being disabled in Windows.

WINDOWS SYSTEM ASSESSMENT TOOL

Windows Vista takes the performance information it obtains from the Windows System Assessment Tool (WinSAT) to calculate the Windows Experience Index (WEI) quite seriously. For example if you don't score 3.0 or higher in the Graphics component, then Vista will not enable Windows Aero by default. Some applications and games make use of WinSAT's ability to provide performance information and thus automatically customize or disable certain settings based on your scores, in order to provide better performance - see the Games Explorer section under the Graphics & Interface chapter for details. So the score is important, and not just haphazardly put together.

Therefore one of the first things you should do is to make sure that you keep the performance scores accurate and up to date. Whenever you change your hardware, update your graphics drivers, alter relevant BIOS settings, or overclock your system you may be prompted to update the WEI, and I strongly recommend that you do so straight away. You can also manually update these scores at any time by being to go to Control Panel>Performance Information and Tools and click the 'Update my score' link on the main page. I encourage you to do this as often as necessary, and be sure not to do anything while your score is being updated if you want the best results.

To update individual scores for a particular component, and to also see more details of the actual tests being undertaken and the results, you can access WinSAT directly through a command line interface. Open an Administrator Command Prompt and type `WinSAT features` then press Enter. This will list the details about your system as identified by WinSAT. To do a full test and update your scores, type `WinSAT formal` and press Enter. You can also run specific tests on individual components, with the results being shown in more detail. This is useful to see precisely what is going on in each test and view the actual results in detail. WinSAT can be used to run a variety of complex specific tests - see this detailed WinSAT Command List. Below are basic WinSAT commands to run the default WEI tests:

```
Winsat cpu
```

Runs the Processor test. Add the -encryption or -compression switch to specify which type of test to run.

```
Winsat mem
```

Runs the Memory test. Shows memory bandwidth in MB/s.

```
Winsat dwm
```

Runs the Graphics (Desktop Window Manager in Direct3D) test. Shows graphics performance and memory throughput in MB/s. You can also get a similar test by using the command AURORA. Press ESC to exit the aurora screen.

Copyright © 2010 Koroush Ghazi

```
Winsat media
```

Runs the Graphics (Media) test. Must specify a media file in .WMV format to test. The default test file is under *\Windows\Performance\WinSAT* and is called *Winsat.wmv*, so for example you can type `Winsat media -input c:\windows\performance\winsat\winsat.wmv` to have it run the test.

```
Winsat mfmedia
```

Runs the Media Foundation-based test. Requires an input file similar to the media command above.

```
Winsat d3d
```

Runs the Gaming Graphics (Direct3D) test. Runs a texture test on screen, press ESC to exit and see result.

```
Winsat disk -drive
```

Runs the Primary Hard Disk test on the drive specified. For example type `Winsat disk -drive c` to have it run the test on C: drive.

WinSAT can be used to help both measure performance and to troubleshoot a problem with a specific component, so it is well worth becoming familiar with it. Each time a full WEI test is run, the results from WinSAT are stored in your *\Windows\Performance\WinSAT\DataStore* directory in an .XML file which you can open and view to see the details if you wish. If you are having problems with WEI or WinSAT, you can delete or move these files to another location to clear the results and then rerun the WEI tests.

In particular if you are having problems with WEI/WinSAT correctly identifying your graphics card's capabilities, consider the following causes of problems:

- Some older graphics drivers have bugs that prevent WinSAT from correctly assessing the full capabilities of the graphics card.
- At times a graphics driver may cause a crash or freeze during the graphics card's setup. If the system is restarted this means the card may not be detected properly.
- Graphics driver bugs may cause problems in correctly identifying the amount of Video RAM on the card.

The main solution to this problem is to download and cleanly install the latest version of the graphics drivers - see the Windows Drivers chapter. If this doesn't resolve the problem, you can go to the Windows Registry and manually check and alter the following areas:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winsat\]

DedicatedVideoMemory=
SharedVideoMemory=
VideoMemoryBandwidth=
VideoMemorySize=
```

These DWORD values should all exist in the registry; if any are missing then this indicates a fault or problem, and you can manually insert them. The values shown should be viewed in Decimal format and represent an amount in Bytes. To see what it is in MB, divide the number by 1,048,576 (i.e. divide by 1,024 then 1,024 again). The `VideoMemorySize` value is calculated as the sum of `DedicatedSystemMemory` + `DedicatedVideoMemory`, which should be equivalent to your onboard Video RAM amount for standalone graphics cards. It may not match exactly the amount of actual Video Memory you have on your graphics card, but it should be quite close. Make sure to backup your registry before making any changes here. You

Copyright © 2010 Koroush Ghazi

may also be able to manipulate your score by changing the values in this section of the registry but that is not recommended.

< EVENT VIEWER

An important place to view details of any performance impediments or potential problems is the Event Viewer. Though complex, learning how to use the Event Viewer can greatly improve your chances of finding the cause of any problems or performance issues. Aside from going to Start>Search Box, typing *eventvwr* and pressing Enter, there are two other ways to directly access specific Event Viewer functionality, depending on your primary purpose:

PERFORMANCE MEASUREMENT

If you are trying to improve performance, then to access the performance-specific logs in Event Viewer go to Control Panel>Performance Information and Tools, click the 'Advanced tools' link in the left pane, then click the 'View performance details in Event log' link. This will take you to the Operation log under the Applications and Services Logs>Microsoft>Windows>Diagnostics-Performance area of Event Viewer. Here you can see individual events which describe potential performance issues, as identified by the Windows Diagnostic Infrastructure which automatically monitors a range of events, including Windows startup, shutdown, Desktop performance and a range of other system events. For example if you have a 'Boot Performance Monitoring' warning here, it is because Vista thinks your boot time may be too long. It will provide details such as how many seconds boot time is taking up (e.g. 38000ms = 38 seconds). Go through these warnings or errors and see if there are any which specify things you can do to rectify them. Note that as discussed under the Startup Programs chapter, these logs are also very useful if you want an objective measure of exactly how long your bootup or shutdown times have been.

Fortunately, Vista reports the most significant of these performance issues in more intelligible form - when you open the Advanced Tools area of the Performance Information and Tools box, you may see listed at the very top of the box under 'Performance issues' a series of links, which are the results of Window's diagnostic analysis. For example you may see a 'Startup programs are causing Windows to start slowly' link, which is connected to the log warning mentioned above. Clicking this link however gives you very clear details as to what Windows thinks is the problem - in some cases even a specific file or setting you should investigate. Of course it's not as simple as removing or disabling the component(s) Vista thinks is the problem, as they may be necessary, and Vista sometimes may be hasty in identifying something as a problem when it isn't. But this form of automated diagnostic still provides information which is much easier to understand than the raw Event Viewer logs.

TROUBLESHOOTING

If you are trying to do some general troubleshooting, you can access Event Viewer either under the Administrative Tools (see the relevant section of the Control Panel chapter), or via the method above, but you should then click on the main 'Event Viewer' item at the very top the left pane. This brings up the Overview and Summary screen, showing the major events and warnings summarized and ranked from Critical events, Errors, Warnings, Information down to Audit Success and Audit Failure.

To run through an example of how to use Event Viewer to find system problems, in the Overview and Summary page follow these steps:

1. Click on the '+' sign next to Error to expand it. You will see all Errors listed in order of Event ID number, with the number of errors in the last hour, 24 hours, 7 days and Total shown to the right (expand the Event Viewer box if necessary to see these).
2. Double-click on the Event ID which has had the most number of errors in the last 24 hours. You will see a listing of all the individual event logs, sort from latest to oldest.

Copyright © 2010 Koroush Ghazi

3. Click once (or double-click) on the first Error listed at the top of the table, and look at the pane below (or the box which opens), under the General tab. You will see a general description of the error. The information under the Details tab is usually not easy to comprehend, but you can view that also if you wish.
4. Under the General tab, click the 'Event Log Online Help' link and click Yes. A new browser window will open and you may be able to see helpful additional advice on what the actual problem is.

Often times you won't be able to find much helpful advice about a particular Event ID, so instead you can firstly try searching the official Microsoft Events and Errors Message Center, and if you have no luck there or need further clarification try Google or this Event ID Site for more details.

If instead of viewing the logs by type, you wish to view them for a specific category or component of Windows, go to the left pane of Event Viewer and browse down to the log file type you wish to view. For example to view all User Account Control-related logs, go to Applications and Services Logs>Microsoft>Windows>UAC and click the log file(s) under it to see the details.

Some important things to note in general about event logs:

§ To troubleshoot an issue, focus on Critical events to start with, followed by Errors. Warning and Information events are useful mainly for performance optimization rather than troubleshooting.
§ Look at how recent the event was. It may be that it occurred a while ago and is no longer occurring, so it may be a one-off or could have been resolved through some other action such as a recent Windows Update. Focus on issues which occur often and more recently. If the error is very recent, such as during your latest session, consider what you have done recently that may have triggered it. For example if you started a particular program or disabled a particular Service.
§ Remember that a log of 100 events may be the same issue which has occurred every time you start your PC. That is, seeing 100 errors may just mean that you had the same error twice a day over the past 50 days, not 100 different errors. You can sort events by the Event ID column, so do so to see how many unique events there are.

If you want to customize the type of event logs which are presented to you in Event Viewer, click the 'Create a custom view' link in the right pane, and then specify the types of event levels to be shown and the time period over which they have been logged among other things. You can then view this custom view by clicking it under 'Custom Views' folder in the left pane. If you want a graphical representation of more important events, see the Reliability Monitor functionality below.

You can even configure Vista to actually alert you immediately of a specific Event, via Email if you even want. Highlight a particular Event - I recommend an Error event which is likely to be important and infrequent - and then in the right pane you can select 'Attach Task to this Event'. In the Wizard which opens you can specify in the Action section to 'Send an email' or 'Display a message' and then fill in the details as to the specific email address you want it sent to, or the message which appears. In this way any events you consider significant can come to your attention immediately.

Ultimately the Event Viewer is generally more suited to advanced troubleshooting, not for beginners. However it has a wealth of information which can help you refine where a problem is occurring if you take some time to go through it. Fortunately Vista does extract what it believes to be performance issues or errors worthy of attention and shows you more details automatically, so even relatively novice users can have some idea of what is causing a slowdown or problem. There are several other automated methods of determining problems in Vista which are much easier for everyone to understand and use and they are detailed below.

Copyright © 2010 Koroush Ghazi

< RELIABILITY AND PERFORMANCE MONITOR

The Reliability and Performance Monitor can be accessed in a number of ways, either through the Performance Information and Tools>Advanced Tools area by clicking the 'Open Reliability and Performance Monitor' link, or by going to Start>Search Box, typing *perfmon* and pressing Enter. You can also access just the Resource Usage section of this utility by clicking the 'Resource Monitor' button under the Performance tab of Task Manager. The Reliability and Performance Monitor is an important tool for monitoring and measuring system performance in Vista, and can again be used to troubleshoot problems as well as improve performance.

PERFORMANCE MEASUREMENT

One of the ways to determine how to improve your performance is to monitor your system resources and determine firstly if any programs are using too many resources when they shouldn't be; and secondly to observe and see just what type of resources your more resource-hungry applications and games need - this can help identify any bottlenecks.

To begin monitoring resource usage, open the Reliability and Performance Monitor, and on the main Resource Overview screen you will see four graphs which immediately commence displaying CPU, Hard Drive, Network and Memory (RAM) usage. You can leave the monitor open as you undertake a task or start a program to see its impact on the four areas of resource usage. Clicking on any graph will open the relevant sub-component underneath the graph area, displaying the details of specific programs or processes and how much of that particular resource they are consuming at the moment. You may even like to briefly run a game or strenuous application and see which resources are pushed to their limits.

However as the name suggests, Resource Overview is just a real-time overview of system resource usage. If you want to actually conduct a proper performance analysis over time, you will need to click the Performance Monitor item in the left pane, which opens up a large single graph. You can now add components for this graph to map over time by clicking the green '+' button at the top, or right-clicking on the graph itself and selecting 'Add Counters'. For example to add a counter measuring hard drive usage, double-click on the Logical Disk item in the list, then select the specific variable you wish to measure (e.g. Disk Write Bytes/Sec) and click the Add button. You can add as many components as you like, though obviously it is wise to limit this to make the graph readable. Click OK when done.

The graph will now update to start mapping all the variables you've added, and you can see in the legend at the bottom of the graph the components being mapped, the color for each component and you can tick or untick particular ones if you wish to temporarily show or hide them. Remember that since the Y (vertical) axis scale is fixed, some components will not display in any meaningful way when using a common scale. However you can change the type of data display used in two ways:

- The simple method involves clicking the 'Change graph type' button at the top and selecting either Histogram or Report view which may be much more meaningful - or you can press CTRL+G to cycle display types.
- The more detailed method involves right-clicking on the graph and selecting Properties. Then under the Graph tab you can adjust the vertical scale manually by entering a maximum and minimum, and under the View box you can select Histogram or Report view instead of Line for example. Under the Appearance and General tabs you can also further customize the display appearance and sample rate as well, and importantly you can set the duration for the graph (default is 100 seconds).

Data Collector Sets can be created to allow you to schedule performance monitoring. To begin this process, right-click on the 'Performance Monitor' item in the left pane and select New>Data Collector Set. This will open the Create New Data Collector Set Wizard. Follow the prompts to define where the set will be held (typically under the *\perflogs* directory). You can start the collection straight away and to stop it, right-click

Copyright © 2010 Koroush Ghazi

on the name of the new Collector Set you've created in the left pane and select Stop. To view the results at any time, go to where the log is stored and double-click on it to open it in the Performance Monitor, or find it under the Reports>User Defined area in the left pane of Performance Monitor. To schedule performance monitoring using a Data Collector Set, right-click on it and select Properties. Then under the Schedule tab click the Add button and you can set the time and day the task will begin, and over what period of time it will occur.

TROUBLESHOOTING

While you can use the Performance Monitor as above to assist in troubleshooting and diagnosing a performance problem, to quickly identify individual issues affecting your system's stability, you can use the Reliability Monitor found under the left pane of the Reliability and Performance Monitor window. The main feature of the Reliability Monitor is a System Stability chart which attempts to graph just how stable your system is over time. The closer you are to 10 on the System Stability Index scale of 0 - 10, the more stable your system is deemed to be. The reliability monitor begins graphing your system in the first 24 hours after you install Vista, so use the scroll bar at the bottom to view the full length of the graph.

At the bottom of the graph you can see Errors (red X), Warnings (yellow exclamation) or Information (white i) events in the five categories of Software (Un)installs, Application Failures, Hardware Failures, Windows Failures and Miscellaneous Failures. Click on any event and at the bottom of the screen you will see the details of the particular process, program or hardware component that is related to the issue.

This is a useful method of quickly seeing when your system has been at its least stable, and the types of issues which may have caused this - though note that some of the identified issues are not serious in any way, and can be the result of deliberate user customization (e.g. disabling certain Services).

The Reliability and Performance Monitor generally requires a bit more effort to use, but rewards those who are patient and who compile appropriate logs with valuable information on the types of things which may be causing system issues or performance bottlenecks.

< TASK MANAGER

The Windows Task Manager is a key Windows utility that allows you to view real-time information about which applications, processes and services are running on your system, as well as a range of performance and system information. There are several ways of accessing Task Manager, some quicker than others:

§ Press CTRL+ALT+DEL together and then select 'Start Task Manager'.
§ Go to Start>Search Box, type *taskmgr* and press Enter.
§ Right-click on the Taskbar and select the 'Task Manager' item.
§ Press CTRL+SHIFT+ESC to bring up Task Manager.

By default Task Manager only shows the running processes for your particular User Account. If you want to see all processes, including System and Network processes, click the 'Show processes from all users' button under the Processes tab. This will provide the most detailed view of what is running on your PC at the moment, and is always the recommended view.

Task Manager has a range of performance and troubleshooting uses, and we look at the main ones below:

PERFORMANCE MEASUREMENT

To use Task Manager for performance monitoring, the place to start is under the Performance tab which, similar to the Performance Monitor Resource Overview section, has graphs which display CPU and Memory usage in real time. The 'CPU Usage History' graph(s) at the top show the percentage of CPU used for each core on your CPU; so for dual core CPUs there will be two graphs, for quad core CPUs four graphs, and if

Copyright © 2010 Koroush Ghazi

the CPU has HyperThreading enabled, then there will be one graph for each 'virtual' core as well. Note that if you only want a single graph for all CPU cores, go to the View menu and select CPU History>'One graph, All CPUs'. Under the View menu you can also tick the 'Show Kernel Times' to display the amount of CPU resources used by the Kernel (core Vista software) as a red line.

Next to the graphs, the CPU Usage scale shows the actual percentage of total CPU resources used. It is important to understand that the total CPU usage figure is an average of the combination of all CPU cores, so if you have a dual core CPU with both cores working at around 50% each for example, the total CPU usage shown is 50%, which is the average, not the sum of the two CPU cores.

CPU usage should be relatively low during idle periods (i.e. 1- 10% at most), though remember that your system may launch a CPU-intensive task such as the Search Indexer when idle, so if the CPU usage is high go to the Processes tab, click the CPU column to sort processes in order of highest to lowest CPU usage, and see what is taking up CPU time (aside from 'System Idle Process'). See Troubleshooting further below.

The box below CPU Usage shows the amount of memory (RAM) being used by the system at present for all your running processes. It is not however the total amount of RAM used by the system, as the system also uses RAM for caching by SuperFetch. Next to this figure is the graphed history of recent memory usage. To see the actual details of the way memory is being used by Vista at the moment, the text below these graphs tells the full story, as covered below:

Physical Memory (MB)

§ Total - Total amount of physical RAM installed in your system.
§ Cached - Amount of RAM recently used by the system for holding a range of data for quick access, typically related to SuperFetch.
§ Free - Unused RAM; not cached nor in use by any process.

Kernel Memory (MB)

§ Total - Total amount of memory used by data for the Kernel (the core software of Vista) on your system.
§ Paged - The portion of the data which can be safely paged out to disk at any time.
§ Non-Paged - The portion of the core Windows data which can't be paged out to disk as this might cause problems under certain circumstances.

The important thing to understand here is that when SuperFetch is enabled, Vista actively attempts to put as much data as it can into the system memory in the form of cached data. It doesn't matter how many programs, services or processes are currently running; that only affects the main Memory Usage figure shown on the graph. The Cached figure shows the true story of what SuperFetch is doing, and that is to cache as much information in RAM as possible in anticipation of its usage, and this in turn should make Windows more responsive. This is why the Free figure under Physical Memory is usually very low, sometimes even 0. The rationale behind this is that any truly free RAM is wasted - if it holds no information, it does nothing to assist in speeding up the system, and thus sits idle and consumes power for no productive purpose.

As soon as you run a relatively memory-intensive program, SuperFetch will give up this cache almost instantly. For example while keeping Task Manager open on this pane, run a Blend test in Prime95 (see the Prime95 section further below) and you will see the Cached figure suddenly drop to almost nothing as all of it goes towards the main Memory Usage figure shown in the Memory graph. Then when you exit the program, SuperFetch will begin steadily recaching information again and you will notice drive activity while it does this. See the SuperFetch section of the Memory Optimization chapter for more details.

Copyright © 2010 Koroush Ghazi

Under the System area to the right you can see the following components:

§ Handles - The number of unique object identifiers in use by processes.
§ Threads - The number of objects or processes running within larger processes or programs.
§ Processes - The number of individual processes running (as listed under the Processes tab).
§ Up Time - The number of minutes since the PC was last started.
§ Page File - The amount of virtual memory in use (left of slash); the sum of system RAM + virtual memory (right of slash) - see the Memory Optimization chapter.

If you click the 'Resource Monitor' button it will take you to the Resource Overview screen of the Reliability and Performance Monitor - see the section further above for more details.

Once you've had a look at the Performance tab, go to the Processes tab and while this is mostly useful for troubleshooting - as covered below - there is still some useful performance-relevant information here. For example you can go to the Applications tab, right-click on a program and select 'Go to Process' to see precisely which main process is running for that application. You can then see how much CPU it is using under the CPU column (shown as a % of total CPU resources), and the amount of memory it is currently using under the 'Memory (Private Working Set)' column. If you want to see the most resource-intensive processes, click on the CPU or Memory column header to sort it such that the processes are sorted with the highest usage ones shown at the top. You can also see their associated Service(s) (if any) by right-clicking on a process and selecting 'Go to Service'. See the Services chapter for more details.

In fact under the Processes tab you can specify a range of information to be shown. Go to the View menu and choose the 'Select Columns' item. You will be presented with a list of details you can display for processes as separate columns, and you can tick those you wish to show. For example if you want to see the drive usage statistics for running processes, tick the 'IO Read Bytes' to see how many bytes of data each process has read from the drive this session.

TROUBLESHOOTING

The most common use for Task Manager is typically to allow a user to close a problematic program/process. Whenever a program stops responding or you can't close it any other way, open Task Manager and under the Applications or Processes tab you can highlight the offending task or process and select 'End Task' or 'End Process' as relevant. Given Vista's methods of isolating the core of the operating system (the Kernel) from being corrupted, this is not necessary most of the time, since by default Vista will prevent the entire system from becoming unstable, detecting a frozen or non-responsive application or process and after a short period will terminate it automatically or present you with a list of options as to how to proceed. You can still terminate a program or process manually with Task Manager if you don't want to wait for Vista to detect its state.

Many of the performance-related uses for Task Manager further above can also assist in troubleshooting program problems as well. For example if your CPU usage is consistently at or close to 100%, then you can investigate under the Processes tab to see which particular process is using so much resources. Make sure though that you are viewing processes for all users in Task Manager (see further above) otherwise this exercise can be pointless. In some cases a program can become caught in a loop or have some other kind of error which causes it to use up all available CPU resources. You can manually end the process causing problems, restart the program and see if it happens again - if so then the program bears further investigation. Some programs require or specifically attempt to use full CPU resources, such as games or intensive benchmarking programs. Even some background Windows tasks such as the Search Indexer can monopolize the CPU when they consider it is idle, but because of the way Vista prioritizes CPU and I/O resources (see the Drive Optimization chapter), no background task should use large amounts of CPU resources when Vista detects that you are trying to undertake another task which requires those resources.

Copyright © 2010 Koroush Ghazi

If your system is consistently showing signs of being sluggish and/or you see a lot of drive activity, check the memory usage figures under the Processes tab. The Memory (Private Working Set) column shows specifically the amount of memory in use by a process which cannot be shared by other processes. Bear in mind that as mentioned further above you can also place additional columns in the Processes tab, so go to View>Select Columns and chose some more metrics which may reveal system issues. In particular the other Memory-related columns are described below:

§ Memory (Working Set) - The sum of Memory (Private Working Set) + memory which can be shared.
§ Memory (Peak Working Set) - The maximum amount of Memory (Working Set) used by the process.
§ Memory (Working Set Delta) - The change in Memory (Working Set) used by the process.
§ Memory (Commit Size) - The amount of virtual memory that is reserved for use by a process.
§ Memory (Paged Pool) - The amount of committed memory for a process that can be written (paged) to the hard disk.
§ Memory (Non-paged Pool) - The amount of committed memory for a process that can't be paged out to disk.

The descriptions for all the Task Manager columns can be seen in this Microsoft Article.

One very useful column which you can enable under the Processes tab is 'Image Path Name'. When displayed, it shows the exact file locations for every running process, so for example if you believe the process is related to malware, you will be able to see precisely where its file is hidden or which program it relates to.

Another useful column you can add is Virtualization, which displays whether file and registry virtualization has been enabled for the process - see the User Account Control section of the PC Security chapter for details.

For the *svchost.exe* (Service Host) processes or any other process you believe is related to a Windows service, right-click on it and select 'Go to Service(s)' and the relevant service(s) will be highlighted under the Services tab of Task Manager. If the process is not related to a service, no service will be highlighted. Conversely you can right-click on a service under the Services tab and click 'Go to Process' to see its relevant process under the Processes tab highlighted. This is particularly useful when determining service resource usage.

If you can't resolve a process-related issue yourself, then you can create a special file which contains debugging information for use by a technical support person. Right-click on the relevant process you believe to be problematic or suspicious and select 'Create Dump File'. A .DMP file with the name of the process will be created under your *\Users\[username]\AppData\Local\Temp* directory. While you can't open this file and view its contents normally, you can use the Windows Debugging Tools to view and troubleshoot the contents, or allow someone with more expertise to do so for you.

At any time if you wish to view or manually adjust the CPU priority with which a process runs, you can right-click on it and select 'Set Priority'. Each process has a level of priority as to how much CPU time it is allowed when multiple applications are running together. This is described in more detail under the Drive Optimization chapter. You can force a particular process to have higher (or lower) priority if you wish to either experiment to see if a particular process is the source of resource-based problems (like stuttering), or if you want to guarantee that a particular process gets top priority when multitasking. Right-click on the process and select 'Set Priority' then select the relevant level.

If you wish to permanently apply this priority change to a particular program, so that it automatically occurs each time the program starts, go to the program's launch icon, right-click on it and select Properties. In the Target box enter the following text exactly as shown in front of the text already there, making sure there is one blank space between the end of /high and the existing text in the Target box:

Copyright © 2010 Koroush Ghazi

```
%windir%\system32\cmd.exe /c start "" /high
```

Note that manually changing process priorities can destabilize the system, and furthermore major programs such as games will already get the highest priority for resource usage. If altering the priority helps improve performance then this means you should focus on removing a range of background programs - see the Startup Programs chapter. Forcing priority is not the appropriate way to resolve this issue in the long term.

MULTI-CORE CPUS

Most desktop PCs now contain a CPU with two or more cores - that is, a single CPU which is actually made up of two (or more) separate CPU chips. Furthermore some Intel CPUs have a technology called HyperThreading which in effect emulates two physical cores on each single core of a CPU. For a program to truly take advantage of multiple cores on a CPU, it needs to be multi-threaded. That means several program 'threads' will run in parallel, with each thread assigned to a particular core to handle. Alternatively, multiple separate programs can be run together much more smoothly on a multi-core system, as each program can be run on a separate core. However some older programs and games are not multi-threaded, and hence show no real benefits when run individually on a dual core system. In fact some programs exhibit problems, such as stuttering, skipping or incorrect speeds when run on a multi-core CPU.

To use Task Manager to troubleshoot multi-core CPU related problems you can manually force the main process for a program to temporarily run on only one specified CPU core. Do this as follows:

- Launch the program in question, and as soon as it appears to be loading, or immediately after it has loaded up, open the Task Manager.
- Under the Processes tab, find the game/program's main process; if necessary go to the Applications tab, right-click on the program and select 'Go to Process'.
- Right-click on the relevant process and select 'Set Affinity'.
- In the box which appears, untick 'CPU 1' (and any other available CPUs), so that only 'CPU 0' is ticked. If you're troubleshooting problems you suspect on one particular core, you can do the opposite - disable all cores except CPU 1 (or CPU 2 or CPU 3 etc.). The aim is to restrict the program to run on only one specific core.

The program is now forced to run on only one CPU core, which should resolve any problems if they were genuinely related to the multi-core setup. If this works, there is a way of permanently forcing the affinity change on a program each time it loads. Before undertaking it, be aware that it modifies the executable file to which it is applied, so backup that file first before using this method:

1. Download the file *imagecfg.exe* from this page and put it into your *\Windows\System32* directory. The file is safe to use, as it was originally a Windows NT system file.
2. Identify the problematic program's main executable. To do this go to the program's launch icon, right-click on it, select Properties and highlight and copy the text in the Target box.
3. Make a backup copy of this executable first and put it somewhere safe.
4. Open an Administrator Command Prompt.
5. In the command prompt window type: `imagecfg -a 0x1` followed by the text you copied from step 1 above (right-click in the command prompt box and select Paste) then press Enter. Make sure to put quote marks around the path if it's not already there. E.g.:

   ```
   imagecfg -a 0x1 "c:/program files/RegCleaner/RegCleanr.exe"
   ```

6. Windows will now only allow that program to see and use the specified CPU core each and every time it is launched by using that particular executable.

Copyright © 2010 Koroush Ghazi

Alternatively if you're having problems with imagecfg, you can use this small SetAffinity program instead. Download and extract the contents to an empty folder, and run the *setaffinity.exe* file. This will bring up the interface where you can select to run a particular process or executable with only one CPU core, either temporarily or permanently.

For all other intents and purposes a multi-core CPU-based system will behave the same way as a single core system. You should only use the steps above if you run into a problems with a particular program which you genuinely believe is associated solely with multi-core CPU usage - usually the program will be an old one; recent programs are designed to take into account the existence of multi-core CPUs.

As you can see, the Task Manager has multiple functions as detailed above. Familiarizing yourself with its various uses will help give you a good idea of what is happening on your system at any time, both for troubleshooting and general performance and maintenance purposes. For example, regularly checking active processes and memory usage will give you early warning of things such as malware infections, since they often cannot be hidden from the Task Manager's Processes list or memory usage statistics.

PROCESS EXPLORER

Similar to the Task Manager in many ways, Process Explorer is a free utility which provides far greater ability to analyze system resource usage. It is far too comprehensive to be covered here in detail, however several features are worth noting. For example, if you right-click on a particular process in Process Explorer and select the Properties item, it opens a window with a range of tabs providing detailed information, such as the individual performance, security and thread data for this process. Under the main Image tab of the properties, you can click the Verify button to determine whether the file is a verified signature.

In the main Process Explorer window, under the View menu you can select 'System Information' to open a new window with a data display similar to that under the Performance tab of Task Manager. However here you can see a range of additional data in more detail, such as the actual Commit Limit and Peak Commit Charge - both critical for determining the correct Pagefile size, as covered under the Memory Optimization chapter. Importantly, you can also see actual Pagefile and drive behavior here, under the Paging section. Page Fault Delta for example displays drive usage when Windows can't find the required information in memory, while the Paging File Write Delta shows how much is being written to the Pagefile at the moment. These are real-time displays, so to actually track these values over time and get an indication of how much is being written to the Pagefile and how often, you would need to use Performance Monitor to log these types of variables over time - add the 'Paging File Usage %' item to the counters in Performance Monitor for example.

< SYSTEM HEALTH REPORT

One of Vista's built-in diagnostic routines is the System Health Report, which is actually a preset Data Collector Set that runs using Performance Monitor, and provides user-friendly output. To access System Health Report, go to Control Panel>Performance Information and Tools>Advanced Tools and click the 'Generate a system health report' link, or go to Start>Search Box, type *perfmon /report* and press Enter.

As soon as it launches, the System Health Report starts gathering information for 60 seconds. When complete, the report highlights any Errors, Warnings or Critical issues at the top of the report, with details of possible methods for rectifying them. Note that some errors and warnings are completely normal; for example if you have purposely disabled a hardware device on your system, or disabled some of Vista's security features, the report will highlight these. Ideally you should run several System Health Reports, firstly under normal (relatively idle) conditions, and then subsequently if you wish to troubleshoot a particular application or game, launch the report then launch the relevant program and exit it after a minute to see what the System Health Report says.

Copyright © 2010 Koroush Ghazi

Under the Basic System Checks section of the report, you can see the areas in which there may be potential issues, though again these are usually highlighted in the section above, so you can browse them for more detailed information. The Resource Overview section shows the status of system resources during the 60-second period the report was run, and is not indicative of your general system resource usage. This is why it's useful to run a System Health Report several times under various system conditions, so you can better see what type of bottlenecks your system may be facing under particular circumstances.

You can see detailed information under the various categories at the bottom of the report by clicking the small triangle at the far right of a particular category, or you can jump directly to specific areas of the report by left-clicking once on the report icon in the middle of any of the category toolbars, then choosing the sub-category link to investigate.

You can save each report by going to the File menu and selecting 'Save As'. The report is saved in .HTML format and can be viewed in your browser. Since this is a system snapshot, as mentioned it is recommended to run multiple reports under various circumstances and then view the results and compare to see if there are common issues with a particular resource, or specific errors which occur under certain circumstances.

< NETWORK DIAGNOSTICS TOOL

The Network Diagnostic Tool is designed to help troubleshoot network and Internet connection-related problems. To access it, go to Control Panel>Network and Sharing Center and click the 'Diagnose and repair' link in the left pane. The tool will launch and do an automatic scan of your connection to see if there are any connectivity problems. If a problem is found Windows will then either automatically resolve it, or present you with options or advice on how to fix the issue. More complex problems are generally not solvable this way, but for simple connectivity issues you should first run this tool. You can also see a graphical representation of your network connection setup in the Network and Sharing Center, and if there are any problems it will be displayed in the diagram.

For further diagnosis of any potential issues on your Internet connection, you can also use Microsoft's online Internet Connectivity Evaluation Tool. Launch the link in Internet Explorer and follow the prompts. Once the test has been completed, you will be given a range of results to examine. To see more information, click the 'View Detailed Report' link at the bottom.

< MEMORY DIAGNOSTIC TOOL

The Windows Memory Diagnostic Tool is another built-in Vista diagnostic that is usually triggered when Vista detects that a problem may be caused by your physical memory (RAM) chips. It is similar to the MemTest86 utility covered further below, and needs to run at startup because that is the optimal time when your RAM is free of any operating system or other software components residing in it. You can also opt to manually run the tool at any time if you suspect memory-related problems with your RAM or CPU memory caches, by going to Control Panel>Administrative Tools and selecting the Memory Diagnostics Tool there, or by going to Start>Search Box, typing *memory* and pressing Enter.

The tool will run at the next reboot, doing a series of tests to determine whether your memory subset is faulty. You can choose which tests to run if you wish by pressing F1 as soon as the tool starts, and selecting from the following options, pressing TAB to move between option categories:

§ Test mix - Select the type of test you want to run, whether Basic, Standard or Extended. Standard is recommended to begin with, and Extended is recommended if you want to do more strenuous testing of your RAM but is very lengthy.
§ Cache - Select whether to have the CPU caches Enabled, Disabled or Default (depends on the test). I recommend having the cache Enabled to start with, then Disable it if you wish to isolate whether it is a RAM-related error, or a CPU cache-related error.

Copyright © 2010 Koroush Ghazi

§ Pass count - The number of times you want to repeat the test, with 0 being infinite. I recommend 2 passes to start with, more if you really want to stress test your memory.

Press F10 to confirm your choices and start the test, progress will be shown both for each test and the overall progress for all tests. This may take some time to complete depending on the options you've chosen. If you suspect a memory-related problem, the longer and more strenuous the testing, the better (e.g. 2-3 hours of testing). This will bring out any latent instabilities in your RAM or CPU caches. You will be told if an error is found, and what it may be related to, however if your memory subset is clear of problems then no issues should occur. If errors are found you can try the following:

§ Reduce or remove any overclocking on your motherboard, RAM or CPU, including any RAM timing changes, then rerun the tests. If the problems don't occur then clearly the issue is with your components being pushed too far by overclocking or reducing the RAM latencies too much. See the Overclocking chapter.
§ Rerun the tests with only one stick of RAM. Vista may even tell you which particular memory stick is potentially faulty, so remove it and rerun the tests.
§ Increase the cooling in your case and make sure to remove any clutter or dust around your CPU and RAM in particular, and anything blocking the free flow of air into and out of your case. If running in a hotter environment you may need additional case cooling. See the Cooling section under the BIOS & Hardware Management chapter for more details.

The Windows Memory Diagnostic Tool while thorough can't detect all memory-related errors, so see the other tools you can use later in this chapter. If it does detect a problem however it is very likely that your RAM is physically faulty or misconfigured in your BIOS, and if ignored will lead to data corruption.

< PROBLEM REPORTS AND SOLUTIONS

Microsoft now consolidates program error reports in a central location under the Problem Reports and Solutions automated utility, found under Control Panel, or by going to Start>Search Box, typing *problem* and pressing Enter. On the main screen of Problem Reports and Solutions you will see the last known solutions to the problems identified on your system - clicking each link gives you more details. To view a list of the individual problems Windows has detected on your system, click the 'View problem history' link in the left pane, and each problem or error is listed under the relevant program which has triggered it. You can double-click on a specific problem to see the technical details of it.

When Windows detects an error, the way it checks for a solution is by sending a report to Microsoft, containing your Product ID, and a minidump file (in the format *Mini[date].dmp*) which includes exception information, system information, a list of all the modules that are currently loaded and their version information, and a list of all the threads that are currently running.

To change this behavior, click the 'Change Settings' link in the left pane and select 'Ask me to check if a problem occurs', and then click the 'Advanced Settings' link below this and choose whether to turn on problem reporting for all programs (recommended), whether you wish to change settings for any other users on the system (best set to 'Allow each user to choose settings'), and whether to 'Automatically send more information if it is needed to help solve problems' (recommended). If necessary click the Add button if you wish to exempt particular programs from having their problems reported in this way, in case you are worried about privacy issues for example.

Having viewed your problem history, if you want to manually check to see if there are any solutions to your problems, click the 'Check for new solutions' link in the left pane, and after a while you will see on the main screen if any solutions or further information is available. Click the links shown to either resolve the issue, or to find out more about it. If prompted to provide additional information I recommend that you allow this, however the choice is yours. Submitting errors and additional information to Microsoft allows them to

Copyright © 2010 Koroush Ghazi

compile a better database of the types of issues which occur, what sort of circumstances trigger them, and hence how best to release fixes for them.

This method of checking for and resolving problems is by no means complete, nor will you solve all problems this way, but it provides a relatively easy to understand interface for viewing and attempting to resolve program and Windows-related problems. Most of the time you will have to do further investigation on your own to work out the source of a problem. Even if you find no solution, at least Microsoft will be aware of this problem and if it is due to a valid bug or error, they can work to resolve it in a patch or update or inform the relevant program developers of the issue.

< WINDOWS ERRORS

Regardless of how many automated tools and diagnostics Windows Vista contains, you may still experience a range of error messages or problems which cannot easily be resolved. Some problems are caused by faulty hardware or adverse conditions (e.g. overheating), or by incompatible software or problematic drivers, and these are virtually impossible for Vista to self-diagnose. However you can investigate these issues further by yourself to work out what the problem may be related to.

For most major errors you will receive a Blue Screen of Death error, often listing an error message and an error code. By default Vista is set to automatically reboot when it experiences a serious error, so you will have to go to Control Panel>System>Advanced System Settings, or go to Start>Search Box, type *systempropertiesadvanced* and press Enter. Then under the Advanced tab, click the Settings button under the 'Startup and Recovery' section, and untick the 'Automatically restart' box. Now when a major error occurs your system will freeze and show details of the error, and I recommend you make a note of the exact error message and any error number(s) provided. If the problem you're experiencing doesn't have a specific error message or number, then note down the application or procedure involved when you triggered the error.

Then using this information search through the following official Microsoft resources for solutions:

Microsoft Fix It Solution Center
Microsoft Knowledgebase
Microsoft TechNet
Microsoft Windows Vista Support Center
Microsoft Events & Errors Message Center

If nothing is found in the resources above, search Google using the error number or exact error phrase, or keywords from a layman's description of the error. This often provides excellent leads for finding out more information from others with the same problem, and what they've attempted to do to resolve it, at the very least saving you time and effort in otherwise chasing false solutions.

Most any problem can be resolved if researched using the links above as well as the tools in this chapter. It may not be quick or easy, but often it is the only way.

Copyright © 2010 Koroush Ghazi

< THIRD PARTY TOOLS

Although Windows contains a range of performance measurement and diagnostic tools, there are several third party tools which can be just as valuable in helping you to measure the performance of various aspects of your PC, and also assist you further in troubleshooting problems. These are covered in this section.

3DMARK

3DMark is a 3D graphics benchmarking utility which primarily utilizes your graphics card, and to a lesser extent the CPU and memory. 3DMark provides you with a good indication of advanced 3D gaming performance on your machine. It also allows you to compare your system's gaming graphics performance with other systems, and broadly speaking the system with a higher 3DMark score is generally better for gaming purposes.

The latest version of 3DMark is called 3DMark Vantage, and runs only on DirectX 10-capable or newer hardware. The Trial version is free, but can only be run once. When you start 3DMark and run the benchmark, you will see a series of tests running. These use various graphical techniques, some of which may not be supported by your graphics card, and some of which are only available in the purchased version of 3DMark. At the end of the run the benchmark will present a final score. You can then use this score to compare with other people who have run the benchmark and this will tell you whether your system is relatively faster or slower, and if compared with others who have very similar system specifications, it will also tell you whether you have room to improve on your particular system. Note however that some systems with the same specifications may be heavily overclocked just to get a high 3DMark score and are not particularly stable for day-to-day use.

UNIGINE HEAVEN

Heaven is a free DirectX 11 benchmark which also supports DirectX 9, DirectX 10 and OpenGL graphics functionality. To run the benchmark, launch Heaven and adjust the settings as desired, then click the Run button. The Heaven demo will begin, but to commence an actual benchmark run you will need to press the F9 key. Once completed you will see a result in both FPS and numerical Score - compare this with others who have run Heaven with the same settings as you to gauge your relative performance. Note there are also Tropics and Sanctuary benchmarks available from the link above, which both support DirectX 10 and DirectX 9 as well as OpenGL.

RTHDRIBL

RTHDribl (Real Time High Dynamic Range Image-Based Lighting) is an older DirectX 9 tech demo and not specifically designed as a benchmark or stress tester. It does not have a series of tests to run, so simply start up the program and observe your framerates in the top left corner. You can turn off the text shown on the screen at any time by pressing F1 and F3. You can also cycle through a range of object shown (Press O), the materials used on their surfaces (Press M), and the backgrounds used (Press L). You can change the display resolution or increase the size of the program's window, either of which will increase the load on your graphics card.

To use it as a stress tester, go to the File menu and select 'Config Display'. In the Direct3D Settings window which opens, select the 'Fullscreen' option, then select the highest available resolution. You don't need to alter any of the other options on this screen unless you know what you're doing. Click Ok and the changes will be implemented. Now start the Auto Demo mode by pressing F5, or select Enter Planet Demo' under the Demo menu, and let the program run for a while. Any graphics instabilities will soon become apparent through crashes, artifacts or glitches. You can put further stress on the graphics card by changing the Multisample setting under the Options menu to progressively higher values.

Copyright © 2010 Koroush Ghazi

LIGHTSMARK

Many graphical benchmarking utilities are based on Direct3D, because this is the most common API used for developing games for Windows. However Lightsmark is an advanced OpenGL-based utility which is free and easy to use. Simply launch the program, select your screen resolution and then click the 'Start Benchmark' button to begin an automated benchmark sequence. At the end of the run you will be given an average framerate for the run which you can compare to other machines running Lightsmark at the same resolution.

FURMARK

FurMark is an intensive OpenGL-based benchmark, which also doubles as a stress tester. As with most benchmarks, installing and running the program results in a run through a series of tests, with results provided at the end. You can upload and compare these results online with other FurMark users. If you experience any graphical glitches or problems while running FurMark, this is a sign that your graphics card is not being cooled sufficiently and/or is overclocked too far.

GAME BENCHMARKS

The graphical benchmarks above are all very useful, however they are all entirely synthetic. The most realistic form of graphical benchmarking and stress testing is through the use of the benchmarking features recent games. Modern PC games are the most system intensive benchmarks you can use, because they stress almost all areas of your system - the CPU, the graphics card, your memory and your drive(s), as well as general Windows stability.

If you can't find an automated or built-in benchmarking feature for a game, simply select the most strenuous game you have - that is, the one with the most graphical detail, best artificial intelligence and physics, and preferably the most recent - and use the FRAPS utility to measure performance over a set period of time. You can assign a key which starts and stops the benchmarking process in FRAPS, or you can tell FRAPS to stop benchmarking automatically after a period of time. You can specify the benchmarking stats to save, such as minimum, maximum and average frames per second. These results can then be compared with others to give you a general idea of your overall performance.

To use any strenuous game as a stress tester, play it continuously for a sustained period of time at very high settings, such as two or three hours. If the game crashes at any point then this is usually a very good indication that your system is not completely stable. Contrary to popular belief, it is not normal for games to crash regularly, and you should not fall into the trap of blaming everything but your own system and its configuration for any problems. The vast majority of game-related problems are due to individual systems, not the game.

PCMARK

PCMark is a general benchmarking utility from the makers of 3DMark. It runs a series of tests based on such things as file encoding, disk reads/writes and basic graphics display. To use PCMark run the program and click the 'Run PCMark' button on the main screen. After several tests it arrives at a score you can compare with others. Note that PCMark results are recorded separately from 3DMark results and are not comparable.

SANDRA

Sandra is discussed under the System Specifications chapter, however in this chapter we look at the modules designed to test certain components of your system, such as the CPU, RAM, or drives. The free version of Sandra is limited in the particular modules you can access and hence the tests you can run, however there are sufficient benchmarks for our purposes in the free version.

Copyright © 2010 Koroush Ghazi

To see the modules of Sandra which have benchmarking functionality, click the Benchmarks tab and you will see modules such as Processor Arithmetic, Physical Disks and Cache and Memory. To run a benchmark, open the appropriate module and press F5 or click the blue arrows (Refresh) icon at the bottom of the module. This will begin a benchmarking run, after which you will eventually see the results displayed at the top of the module. You might want to record the score(s) somewhere. You can put the benchmarking results in context by looking at the results for other reference systems also provided. You can also change the reference data to reflect a variety of hardware to compare against, by clicking the relevant drop down boxes.

Sandra also has a role as a diagnostic tool. To use it as a stress tester of specific components on your system, use the relevant modules under the Benchmarking tab. However instead of simply running them once, if you want to stress test the relevant component simply refresh the benchmark repeatedly (by pressing F5) whenever it completes each run. Alternatively, if you want to automate the process, Sandra has a Burn-in Computer module under the Tools tab which will undertake more thorough stress testing of your machine. Start the wizard, tick the components you want to continually stress test, set the number of times for them to loop, or the period over which you want to perform these test, make sure the 'Monitor your computer's health' and 'Terminate on overheat/failure' boxes are ticked to be safe, and then commence the stress testing.

PRIME95

Prime95 is a small mathematics program which will effectively stress test only your CPU and memory. Once you've downloaded the application, run *Prime95.exe* and click the 'Just Stress Testing' button. Next, you should automatically be prompted to select a test, but if not, under the Options menu select 'Torture Test' to start stress testing. Select the test type based on the particular components you want to focus on testing:

§ Small FFTs - Select if you want to primarily test your CPU.
§ In-place Large FFTs - Select if you want to test your CPU for stability under high heat and voltage usage.
§ Blend - Select if you want a more general 'real word' test which tests both the CPU and plenty of RAM.

Once you click OK the testing will begin and Prime95 will open multiple threads to ensure all your CPU cores are being fully utilized. If at any point you want to stop the test, go to the Test menu and select Stop. If the program aborts with an error at any time, this indicates system instability. In general if your PC can run the test for over one or two continuous hours it shows that the CPU and memory subset are quite stable. However Prime95 is still just a synthetic test which only stresses your CPU and RAM, and regardless of how long you can run it without errors, it is not indicative of a completely stable system. Only real-world applications and games running without problems indicate this.

SUPER PI

Super PI is a small utility similar to Prime95, in that it stress tests your CPU and memory subset by calculating the mathematical number PI to a certain number of places. Download it and run the *super_pi_mod.exe* file. Click the Calculate menu item at the top, and select the number of places to calculate PI to, ranking from 16 thousand (16k) to 32 million (32M) places - the larger the number of places, the longer it will take.

For a speed test of your CPU, select the 1M option and once the calculation is done, note the time in seconds taken. You can then compare this figure to other people to see how fast your CPU is in raw calculation power relative to theirs. If you want to stress test your CPU, run the full 32M calculation which will take longer, and hence is a better stress test of your CPU. Once again you can also compare the time taken to complete this with other users.

Copyright © 2010 Koroush Ghazi

HD TUNE

HD Tune is a drive information and benchmarking utility which has been covered in various chapters of this book, including the System Specifications and Drive Optimization chapters. You can run a drive benchmark in HD Tune by clicking the Start button on the main Benchmark tab. The test will run, providing a real-time mapping of drive performance, and the final results will be displayed for use in online comparisons.

MEMTEST

MemTest is a Windows-based memory test which will help in stress testing your Windows memory configuration and RAM to detect any potential problems. Memory-related errors are one of the primary causes of system instability and data corruption, so a system memory tester is a necessity. To use MemTest simply launch the program, and I recommend manually entering the amount of RAM you wish to test - e.g. enter 512 to test 512MB of RAM, 1024 for 1GB of RAM or 2048 to test 2GB of RAM. You may need to run multiple instances of MemTest to use up all your system RAM. Click the 'Start Testing' button to begin RAM testing and allow the test to run until it has reached 100%. Ideally you should run the test for at least an hour or more. If running the test triggers any errors, Windows-related warnings or prompts, then you have potentially faulty RAM and/or mis-configured BIOS or Windows memory settings, which can lead to many types of system problems. To refine the test solely to your physical RAM, run the Windows Memory Diagnostic Tool as covered earlier in this chapter.

MEMTEST86+

Memtest86+ is similar to the Windows Memory Diagnostic Tool in that it tests your memory before Windows loads into memory. This is a much more accurate way to test your physical RAM and memory subset free of any memory spaces taken up by the operating system. The version of Memtest86+ you download is based on which device you use at bootup, whether CD, Floppy or USB flash drive. Once booted on this device, your system will launch Memtest86+ and test your RAM. Any errors indicate BIOS or physical RAM problems.

That covers the main performance measurement and diagnostic tools you can use to troubleshooting and optimize your system. Importantly, despite promises you may read to the contrary, there are no tools which automatically diagnose and fix all your problems. Many tools are advertised as being able to do this, but no such tool actually exists. The causes of PC problems are often very complex and inter-related, and can be a combination of hardware problems along with incorrect settings and/or driver problems. Furthermore every system is unique in terms of the hardware it contains, the software installed on it, the configuration of that software and the interactions between the software, and even the physical environment in which your PC sits. All of these variables can individually or collectively have a tangible impact on system stability and performance. The best way to diagnose any issue and optimize your system correctly is to understand how your system works combined with research and thought. If there really was an easier way or automated utility to resolve problems, everyone would be using it by now, and similarly Microsoft would have purchased the rights to it and incorporated it into Windows, rather than providing so many different diagnostic and performance measurement tools.

Copyright © 2010 Koroush Ghazi

CLEANING WINDOWS

As you use your system in day-to-day activities, a range of unnecessary temporary, backup and log files can build up on your drive. Many of these files are automatically deleted whenever you close an application, or whenever you shut down Windows. Unfortunately some of them aren't, and over time they can build up, taking up disk space and cluttering your directories. This chapter looks at the tools and methods required to safely clean out unnecessary files from Windows.

< DISK CLEANUP

The built-in Disk Cleanup utility provides the ability to automatically find and remove a range of unnecessary files. To access the Disk Cleanup utility go to your Start>All Programs>Accessories>System Tools menu, or go to Start>Search Box, type *cleanup* and press Enter. You will be asked whether you want to clean up just your own files, or files from all users on this computer, and the specific drive to clean. If there are other users on this machine, I recommend considering the impact on them - cleaning up some components such as Temporary Internet Files, Error Reports or older Restore Points could adversely impact them, but of course at no point will personal files or folders be removed.

To remove unnecessary Windows files at any time, under the Disk Cleanup utility you can select any of the following components. Some of these items may not appear if they have nothing to clean. Furthermore, for some of these options you can click the 'View Files' button to see precisely what files will be affected:

Downloaded Program Files: Ticking this item removes all the files held under *\Windows\Downloaded Program Files* directory, usually small ActiveX and Java programs which you may have downloaded while browsing certain web pages. This option does not delete any other files you have downloaded anywhere else on your system. This setting is best left unticked, especially if you often visit trusted pages which need these program files, since they will need to be redownloaded.

Temporary Internet Files: Ticking this item clears your Internet Explorer browser cache, held under *Users\[username]\AppData\Local\Microsoft\Windows\Temporary Internet Files*. It does not affect the browser cache of your other browsers. In general this is best left unticked as constantly clearing your browser cache can slow down browsing on IE - only clear the cache periodically (See the Internet Explorer chapter).

Hibernation File Cleaner: Ticking this option has two important effects: Firstly it removes the system file *Hiberfil.sys* found under your system drive's base directory. This file is for the Hibernation feature covered under the Power Options section of the Control Panel chapter. It is a large file, equal in size to your system RAM, so removing it can save quite a bit of drive space. However if you use the Hibernation or Hybrid Sleep feature you should not tick this item, as the file needs to stay. Secondly, by removing this file you also disable access to the Hibernation feature, which can only be regained by following the instructions in this Microsoft Article. Therefore only tick this option if you do not currently use, and do not wish to use, Hibernation or Hybrid Sleep. If the option doesn't appear it means you don't have this file on your system.

Offline Webpages: Ticking this item clears any offline web pages stored under the *\Windows\Offline Web Pages* directory. This item is fine to tick unless you wish to keep these pages.

Recycle Bin: Ticking this item removes all the files and folders currently in the Recycle Bin. Tick this item only if you're sure that you no longer need any for them.

Copyright © 2010 Koroush Ghazi

System error memory dump files: Ticking this item removes all memory dump files, such as *Memory.dmp* usually found under your *\Windows* directory. These dump files can help when reporting an error - see the Performance Measurement & Diagnostics chapter. If you aren't having any problems or don't need to troubleshoot your system this way, you can delete these.

System error minidump files: Similar to the above option, ticking this item removes all minidump files, for example *Mini020407-01.dmp*, found under the *\Windows\Minidump* directory among other places. Only tick if you don't have any system issues.

Temporary Files: Ticking this item removes any temporary files created by various programs and Windows. These files are usually cleaned out by the program or Windows itself after a restart, but this does not happen at times due to a bad shutdown or program crash. This item should be ticked.

Thumbnails: Ticking this item removes the cached thumbnails which Vista creates for viewing files, folders and particularly pictures in Icon or Tile view. In general you should not tick this item unless you have most of your folders set for Details or List view instead. Deleting thumbnails only increases the time it takes for Vista to regenerate thumbnails for folders which use this view.

Per user archived Windows Error Reports
Per user queued Windows Error Reports
System archived Windows Error Reports
System queued Windows Error Reports

The four options above refer to error reports generated by Vista and covered under the Performance Measurement & Diagnostics chapter. If your system is free of errors or problems, then you can safely remove these, otherwise they may be useful for troubleshooting purposes so don't remove them.

More options: Under this tab you will be able to access the Programs and Features area of Vista by clicking the first 'Clean up' button. See the Programs and Features section under the Control Panel chapter for more details. The second option here is more important, as clicking the 'Clean up' button under the 'System Restore and Shadow Copies' area will bring up a prompt asking you if you wish to Delete all of your System Restore points except for the most recent, also removing any older Shadow Copies as part of this process. These are covered in more detail under the Backup & Recovery chapter. If your system is performing without any problems and you also don't wish to restore any recent Previous Versions then it is usually fine to click this option, as older Restore Points can often take up a fair bit of disk space.

ADVANCED DISK CLEANUP

There is a more advanced form of disk cleanup which provides a few additional options you can select for cleanup along with the original options covered above. To activate it, you must type the following in an Administrator Command Prompt or at the Start>Search Box:

```
Cleanmgr /sageset:1
```

The number after the `/sageset` switch can be anything from 0 to 65535, it doesn't matter - it's simply the specific place in the registry that your options will be saved. You cannot specify a drive or user to clean files for, this applies to all drives and partitions, so use cautiously if you have other users and/or drives on the machine. The following additional options will be available using this advanced cleanup method:

Debug Dump Files: Ticking this option removes any general .DMP files which are usually not needed unless you are trying to troubleshoot a problem.

Copyright © 2010 Koroush Ghazi

Old Chkdsk Files: If you have run the `chkdsk` command or any automated recovery method in Windows Recovery Environment then it may have found portions of damaged or lost files which it has saved with the .CHK extension in your base directory. Unless you are still in the process of recovering these files, they are safe to delete.

Previous Windows installation(s): If Vista found any files or folders which were not compatible when doing an Upgrade over a previous version of Windows, it will store them in a series of folders called *Windows.old*. You can view their contents to see if there's anything you want to keep.

Setup Log Files: Ticking this option removes any log files created during Windows installation. These are not normally needed, and best removed if your system is not showing signs of any installation-related problems.

Temporary Windows installation files: Ticking this option removes a range of temporary installation files created during Windows installation. These files can be removed without any problems.

Files discarded by Windows Upgrade: During an Upgrade install of Vista, any non-system files which Vista cannot move across, it will keep backed up just in case. If none of your personal files are missing after an Upgrade install, you can tick this option.

Once you have selected the relevant options, click OK. Nothing will be deleted just yet - your settings are saved and you can now run advanced Disk Cleanup with these options at any time by typing the following in a Command Prompt or in Start>Search Box:

```
Cleanmgr /sagerun:1
```

Press Enter and the cleanup process will begin immediately. Note that the number after `/sagerun` must match the number used in the `/sageset` switch further above for the same options to execute. In general this advanced method need not be used very often; once after you have installed Windows and then infrequently after that is sufficient. The regular Disk Cleanup method further above is safer and more configurable, making sure it doesn't have inadvertent impacts on other users or other drives on your system.

< SERVICE PACK CLEANUP TOOL

If you have installed a Service Pack on an existing installation of Windows Vista, it will create a range of backup files which allow you to uninstall the service pack if necessary. However for all intents and purposes, once you've installed SP1 and/or SP2 there should never be any need to uninstall them again, so to delete the unnecessary backup files and redundant versions of system files, you can use the Windows Component Clean Tool, which is effectively a Service Pack Cleanup Tool by any other name.

This is a command-line only tool which is installed along with SP2, so to run it you will need to go to the Start>Search Box, or open a Command Prompt, type `compcln` and press Enter. You will be presented with a prompt indicating that Windows is ready to commence removal of unnecessary service pack and other package-related files - press Y to continue or N to abort. If you proceed then Vista will remove the files and thus free up additional disk space. Note that this tool supersedes the Vista SP1 Cleanup Tool, which could be accessed after installing SP1 by typing `vsp1cln` at a Command Prompt. That tool is not necessary nor available once SP2 is installed, as compcln will remove all redundant files from SP2 and SP1.

Once the cleanup process is complete, you will no longer be able to uninstall SP1 or SP2, but as noted this is something that is not recommended anyway. If you are having major issues with your system after installing a service pack then it is strongly recommended that you reinstall Vista and then apply the service pack(s) immediately after a fresh installation.

Copyright © 2010 Koroush Ghazi

< RECYCLE BIN

The Recycle Bin provides a storage area for deleted files and acts as an additional layer of protection against permanently deleting files on your system. To access the Recycle Bin configuration options, right-click on the Recycle Bin icon on your Windows Desktop and select Properties. Note, if you can't see the Recycle Bin anywhere on the Desktop, see further below.

Custom Size: This option sets the maximum amount of drive space allocated to the Recycle Bin should it need it. Highlight the logical drive you wish to set the space for, and then enter an amount in MegaBytes (MB), with the minimum amount being 1MB. I recommend allocating a decent amount of space here, at least as large as the largest files you are likely to delete (e.g. 4000MB which is roughly 4GB). If the Recycle Bin is not large enough for a file you're deleting, it will be permanently deleted instead, so don't skimp on the Recycle Bin size.

Do not move files to the Recycle Bin: If this option is ticked, all files will be deleted permanently instead of being moved to the Recycle Bin first. I do not recommend ticking this option, as the Recycle Bin gives an added level of protection against accidental deletion of important files. If you wish to permanently delete individual files at any time, simply hold down the SHIFT button at the same time as pressing Delete or choosing the Delete option to bypass the Recycle Bin.

Display delete confirmation dialog: If ticked, every time you choose to delete a file, you will be asked if you wish to continue. As long as you have the Recycle Bin enabled, then I recommend unticking this option as it is an unnecessary annoyance.

Note that no file is actually permanently deleted when it is deleted 'permanently' from your drive. It is simply marked for deletion and hidden by the file system, but it can be overwritten at any time. For details of how to recover a file which has been 'permanently' deleted from Windows or the Recycle Bin, see the Backup & Recovery chapter.

By default, when you right-click on the Recycle Bin, there is a Delete option which if selected will actually delete the Recycle Bin itself from the desktop, not the contents of the Recycle Bin. Be careful not to choose this option unless you really want to remove the Recycle Bin. If you do this accidentally, then you can re-enable the Recycle Bin icon by right-clicking on an empty spot on your Desktop, selecting Personalize, then clicking the 'Change desktop icons' link in the left pane. Here you can tick or untick the 'Recycle Bin' item to show or hide this component on the Desktop. You can also change the icon used for the Recycle Bin if you wish - highlight the Recycle Bin (full) and/or Recycle Bin (empty) icons here, click the 'Change icon' box, then select a new icon to use, or click Browse to find and select additional icons aside from the system default icons.

< CCLEANER

CCleaner is a free utility which can automatically find and remove a wide variety of potentially useless files from your system. CCleaner automates a task that you can perform manually to some extent (see further below), but which takes longer to do by hand; CCleaner finds and removes a range of files with common extensions or locations which can indicate that they are unnecessary. If used with caution it is usually quite safe in removing only unnecessary files.

Run the program and click the Options button, and adjust the following settings:

Copyright © 2010 Koroush Ghazi

1. Under the Settings section, all available boxes can be unticked if desired, as none are vital to running CCleaner correctly. Selecting the 'Normal file deletion' option is recommended, as secure deletion can make it virtually impossible to recover accidentally deleted files.
2. Under the Cookies section, in the left pane are a list of cookies CCleaner will automatically delete if the Cookies option(s) are ticked under the main Cleaner portion of the program. If you have ticked any of the Cookies boxes in the Cleaner portion, select any cookies you would like to keep from the list.
3. Under the Include and Exclude sections you can manually add particular files or folders which you would specifically like CCleaner to scan for deletion or exclude from deletion. This is only recommended if you know categorically that the contents of these files or folders are safe to delete.
4. Under the Advanced section I recommend ticking the 'Show prompt to backup registry issues' box as a safety mechanism if you use the Registry cleaning functionality; and the 'Only delete files in Windows Temp folders older than 24 hours' to prevent deletion of temporary files which are required for the current session.

To start the cleaning process, first make sure you close all open applications to prevent conflicts if CCleaner tries to delete actively used files. Then launch CCleaner and under the Windows tab of the Cleaner function, take the time to go through and select or unselect particular options. As a general balance between safety and removing all unnecessary files, I recommend the following configuration for each category:

§ Internet Explorer - If you don't use Internet Explorer as your main browser, all options here can be ticked. If you do use Internet Explorer, I don't recommend ticking any options here as it can reduce performance and functionality in IE. Proper configuration of IE is covered under the Internet Explorer chapter will ensure the necessary files are kept or removed by IE itself during normal operation.
§ Windows Explorer - All options can be ticked, however I recommend unticking the 'Thumbnail Cache' option as it means any folders in which you use Icon views will need to regenerate their thumbnails, slowing down browsing of those folders. I also recommend unticking the 'Taskbar Jump Lists' functions unless you don't use the Recent functionality of Jump Lists. See the Taskbar section of the Graphics & Sound chapter for details.
§ System - All options can be ticked, but bear in mind that ticking items like 'Windows Log Files', 'Memory Dumps' and 'Windows Error Reporting' can make troubleshooting much more difficult, so only select these if you are having no problems on your system. See the Performance Measurement & Diagnostics chapter for details. I also don't recommend ticking the 'Empty Recycle Bin' option here for the reason covered at the end of this chapter.
§ Advanced - I recommend against ticking any of the options here, as most of the options here will result in deletion of files which are self-maintained by Windows. For example, 'Old Prefetch data' is unnecessary, as Windows automatically purges the Prefetch folder periodically to maintain a list of the most commonly used programs based on its analysis. Various caches are also necessary to speed up normal Windows functionality, so regularly deleting them simply works against this. For security purposes you can tick the 'Wipe Free Space' option, but I recommend against this, as it prevents you from recovering any accidentally deleted files and also makes cleaning very lengthy.

Under the Applications tab I recommend unticking all available options. This is because in the vast majority of cases removing application-specific files in this manner can remove desirable functionality from such applications and introduce unexpected behavior - deletion of application-specific files can result in the loss certain custom preferences for example. Also be aware that CCleaner may add and automatically tick new options here when you install new applications, so check under this tab regularly.

Once you have ticked all the relevant options, click the Analyze button and after a while CCleaner will come up with a list of files it wants to delete. However the results are shown in summary form, which can make it difficult to determine what will be deleted. Right-click in the analysis window and select 'View detailed results' to see precisely which files are going to be deleted, and scroll through the list to make sure no desirable files are here. If in doubt, go back and untick any options, then click the Analyze button again.

Copyright © 2010 Koroush Ghazi

When you are satisfied that the files to be deleted are truly unnecessary, click the 'Run Cleaner' button and the files will all be permanently deleted.

There are two more useful functions of CCleaner covered in this book:

Registry: The Registry function in CCleaner attempts to find redundant Registry entries, and is relatively safe to use if configured correctly. This functionality is covered under the Maintaining the Registry section of the Windows Registry chapter.

Uninstall: The Uninstall function found under the Tools section of CCleaner can be used to remove faulty entries from the Programs and Features list. This functionality is covered under the Programs and Features section of the Windows Control Panel chapter.

CCleaner is a useful tool in removing a range of unnecessary files, but caution is required, as Windows Vista is already quite good at maintaining itself and thus does not need to have a range of files deleted by this or any other utility. Many files will simply recreate themselves the next time you start Windows or use a program, so in many ways all you are doing by deleting them with CCleaner is actually slowing down normal Windows and application functionality. The recommendations in this section try to limit CCleaner to deletion of genuinely unnecessary files.

< MANUAL CLEANING

Below is a basic method for manually finding and removing the more obvious redundant files in your system. If you don't trust an automated cleaner, or just want to be certain of what it is you are deleting, read the following. However this method is not recommended for beginners as it requires a reasonable level of knowledge and personal judgment in determining which files to delete and which to keep.

Before manually cleaning out any files, first close all open applications and games as some of these may have created temporary files that cannot be deleted because they are in use, and would be pointless to delete. Then restart your system just to be certain, as Windows will remove many unnecessary temporary files upon shutdown. Now make sure that the option to move files to the Recycle Bin is enabled. This will provide protection against accidentally deleting a necessary file.

To begin with, it is safe to delete any files or folders beneath the *\Users\[username]\AppData\Local\Temp* directory. These are temporary files specific to your User Account.

Next, go to the Programs and Features component under the Windows Control Panel and uninstall any programs you do not wish to keep. Then go to the following folders and manually delete any subfolders for programs you are certain you have uninstalled from your system:

\Program Files
\Program Files\Common Files
\Program Files (x86) - for 64-bit users
\Program Files (x86)\Common Files
\ProgramData
\Users\[username]\AppData\Local
\Users\[username]\AppData\LocalLow
\Users\[username]\AppData\Roaming

In some cases the folders may be named after the company which has created the software rather than the software itself - a quick check on Google should help you remember which programs the folders relate to if

Copyright © 2010 Koroush Ghazi

in doubt. Certain programs may have files which are 'in use' and can't be deleted - see the section further below for details.

Next, if you have no major issues on your system and you are not trying to troubleshoot a problem or recover any files, it is possible to delete a range of files with particular extensions identifying them as potentially redundant. Press WINDOWS+F to open the advanced Windows Search functionality, and find all files with the following extensions:

.DMP files are Dump Files created by Windows after crashes and errors.
.OLD files are generally backup copies of files.
.BAK files are generally backup copies of files.
.LOG files are files containing logged data, either by Windows or a program.
.WER is for files related to the Windows Error Reporting function.
.LNK is for shortcut files, including links to recently opened files in programs.

I do not recommend simply deleting all the results you discover for each of the searches above. You must exercise your judgment in most cases - for example many .LNK files are valid and necessary shortcuts and links; you must only find and remove links to programs or files which you know no longer exist on your system.

As noted in the CCleaner section, do not regularly clean out the contents of Windows directories such as *\Windows\Prefetch*. These directories are self-maintaining and there is greater potential for harm than good in removing these files unless you are a very advanced user.

The key thing to understand is that, aside from deleting certain Windows or program files or folders for troubleshooting purposes, there are no performance benefits to be had by deleting unnecessary files. This is only done primarily to reduce clutter and free up disk space. Given most of these potentially unnecessary files are very small, and often hidden from view, there is no need to risk a loss in functionality or performance by deleting lots of 'unnecessary' files as some sort of optimization procedure.

DELETING 'IN USE' FILES

If during manual file cleaning you find that you cannot delete an unnecessary file because Vista claims that it is 'in use' by another person or program, or simply denies you access to the file or folder, then reboot your system and try again. If that doesn't work, then it is usually either a driver or some other system-level file which is loading up during bootup, or a file required for an active program. Go through and close all active programs, particularly ones which load at startup and try again. If necessary, temporarily disable the suspected startup program(s) using MSConfig, reboot and try again. Alternatively use AutoRuns and see if the file is shown there, and untick it to prevent it being loaded up at startup, then reboot and try again. See the Startup Programs chapter for more details of how to use both these programs.

Ultimately however some files will refuse to be deleted no matter what you try, in which case you should try the free Unlocker utility. To use the program, right-click on the relevant file or folder and select Unlocker, then click the 'Unlock All' button to unlock the file. Alternatively choose from the list of actions at the bottom left of the box shown, and reboot if necessary for the action to complete.

Be warned however that in general Vista locks files or prevents deletion for a reason, so only use Unlocker if you're absolutely certain that that file in question is genuinely no longer required.

Copyright © 2010 Koroush Ghazi

After deleting all files you consider unnecessary via any of the methods above, importantly you should not empty your Recycle Bin. Reboot your system and use it normally for a few days just to be sure the files you have deleted are genuinely no longer needed. In general the use of CCleaner - if enabled with sensible options - is the safest method for conducting regular cleaning of your system, however manual cleaning is also necessary at times, particularly after uninstalling a program which does not correctly remove all portions of itself from your system. Again, cleaning Windows is not a performance boosting method, it is primarily for reducing clutter and freeing up disk space, and even then it is not to be done without some thought as to what precisely it is you are removing.

Copyright © 2010 Koroush Ghazi

REGULAR MAINTENANCE

Keeping Windows and your PC in optimal working order requires regular system maintenance. Any operating system will degrade over time if not properly maintained, particularly as you install and uninstall a range of programs and drivers. Even though Windows Vista has improved its self-maintenance procedures, and by default schedules a range of important tasks to run on a weekly basis, such as defragmenting the system and scanning it for malware, this is not a replacement for proper system maintenance.

The best method of conducting system maintenance is to get into a routine, so that it becomes a matter of habit. This prevents you from forgetting to conduct system maintenance. However it cannot be done on a completely rigid schedule; certain maintenance tasks should only be done under certain circumstances, their frequency depending on how you are using your PC.

For the reasons above, I can't provide an all-encompassing maintenance schedule which everyone should follow. This entire book contains a wealth of information and recommendations designed to help you understand how best to maintain your PC. By having appropriate knowledge of the various functions in Windows, you will come to know how to configure Windows automated maintenance tools, and when to manually intervene as necessary. For the purposes of providing some basic guidelines however, I provide a list of maintenance tasks I regularly perform on my own PC to maintain it in peak condition. This is only an example and should not be followed blindly - for example the Defragment step doesn't apply to people using SSDs, as explained under the Drive Optimization chapter.

STEP 1 - MAINTAIN SECURITY

Action: Run Windows Update, then update malware scanners and run a full manual scan of all drives.
Frequency: Once a week at least, and also scan individual downloaded files before use with MSE.

See the PC Security chapter for details.

STEP 2 - CHECK STARTUP PROGRAMS & SERVICES

Action: Use MSConfig to quickly check under the Startup and Services tabs for any newly installed startup programs or non-Microsoft services. Identify any new or unfamiliar entries and disable unnecessary ones as required, first by checking the program's own options, then using Registry Editor or Autoruns as necessary.
Frequency: After every new program or game install.

See the Startup Programs and Services chapters for details.

STEP 3 - BACKUP

Action: Create a new restore point using System Restore, and then run the automated Backup utility to create/update a full system image backup stored on a separate drive. Also make a separate manual backup of important personal files to DVDs for secure and portable storage.
Frequency: Once a week at least.

See the Backup & Recovery chapter.

Copyright © 2010 Koroush Ghazi

STEP 4 - CLEAN WINDOWS

Action: Run the Disk Cleanup utility, then CCleaner. Do a manual clean out of remaining unnecessary files.
Frequency: Once a week at least, and also after major updates or program uninstalls.

See the Cleaning Windows chapter for details.

STEP 5 - CHECK DISK

Action: Use the Check Disk utility to do a full disk scan and automatic repair of the primary system drive.
Frequency: Once every month at least.

See the Drive Optimization chapter for details.

STEP 6 - DEFRAGMENT

Action: Use the Windows Disk Defragmenter to run a full defragmentation of the drive.
Frequency: Once a week at least. Also after every major program or game install/uninstall, or any manual game or Windows patching, such as after Windows Update or driver installation.

See the Drive Optimization chapter for details.

Some of the steps above may seem somewhat tedious to run through on a frequent basis, but in practice it is precisely what has ensured that my system always remains problem-free. Proper maintenance is important in ensuring that your data remains secure, your system remains as responsive as when you first installed Windows Vista, and you don't keep running into 'mysterious' crashes and problems. Of course proper system knowledge and prevention are also two key aspects of system maintenance.

SCHEDULED MAINTENANCE

Windows Vista's Task Scheduler allows you to create and customize a range of automated tasks for maintaining your PC. For example if you leave your machine on overnight, you can schedule certain utilities to run at that time, especially for lengthier tasks such as full manual malware scans or disk defragmenting. Even without appropriate options in a program, you can use Task Scheduler to launch tasks at particular times in case you forget to do so manually. See the Task Scheduler section of the Control Panel chapter.

A critical part of proper maintenance is prevention, and this involves making sure that you do not constantly install a range of unnecessary programs on your system. Codec packs, various dubious tweaking utilities, piracy tools and pirated software, constant upgrades/downgrades of leaked drivers, etc. are one of the major reasons why many systems are so unstable and insecure, beyond Windows Vista's capabilities of managing the mess of program conflicts and detritus that such systems have accumulated. Treat your PC as a complex and finely-tuned electronic machine, not a dumping ground for everything you find on the Internet, and you will find that it remains stable and performs well for a very long time.

Copyright © 2010 Koroush Ghazi

CONCLUSION

That brings *The TweakGuides Tweaking Companion for Windows Vista* to a close. I hope you've found the information in this book valuable as a reference source.

Cheers,
Koroush Ghazi

< VERSION HISTORY

The table below shows all the major revisions made to this book since first released.

Version	Release Date	Pages Revised
1.0	1 March 2007	Nil - First Release.
1.1	1 July 2007	All pages - Several typographical/grammatical errors fixed. All pages - Fixed any dead or inaccurate hyperlinks. pp.79,140 - ALchemy for X-Fi now also for Audigy. pp.102 - Updated A-Squared Free advice. pp.103 - Added info on Ad-Aware 2007. pp.189 - Expanded and clarified DEP for IE7 option. pp.213 - Added details of new DX10 games and benchmarks/demos.
1.2	22 September 2007	All pages - Fixed any dead or inaccurate hyperlinks. pp.103 - Updated Ad-Aware advice. pp.171-172 - Updated RegSupreme advice. pp.184 - Added IE7 Security Guide link. pp.205 - Added InterfaceLift wallpapers link. pp.211 - Added Ave's Vista Apps for interface customization. pp.238 - Added Rightmark3D benchmark. pp.244 - Updated CCleaner advice.
2.0	19 March 2008	This is a major revision of the guide. It has been thoroughly revised throughout, not just for SP1. There are a large number of changes, but only the more significant ones are listed below: All pages - Fixed any dead or inaccurate hyperlinks. All pages - Fixed a large number of typographical/grammatical errors. pp.24 - Added GPU-Z utility. pp.31 - Fixed VSSAdmin command advice. pp.49 - Added Transient Multimon Manager section. pp.52 - Updated installation image / vLite advice for SP1. pp.62-63 - Updated VistaBootPro advice. pp.66 - Updated Reduced Functionality Mode section for SP1. pp.71 - Updated and corrected Folder Options advice. pp.76 - Added Edit 'Open With' Context Menu section. pp.76 - Added Edit 'Send To' Context Menu section. pp.77 - Updated & expanded Incorrect Folder Views section. pp.81 - Updated Vista 64-bit advice. pp.81-82 - Added Vista SP1 installation instructions and advice. pp.82 - Added DirectX installation advice. pp.82 - Updated & clarified motherboard drivers advice. pp.83 - Updated & clarified graphics driver advice. pp.87 - Updated driver uninstall advice, added Driver Sweeper utility. pp.95 - Added new UAC customization option for UIAccess prompts elevation due to SP1. pp.106-107 - Updated AVG Anti-virus advice. pp.109 - Added AVG Anti-Rootkit Free link. pp.116 - Updated 4GB RAM display change due to SP1. pp.118 - Added ReadyBoot section. pp.125 - Updated Drive Controllers section. pp.125-126 - Added Master File Table section. pp.128-129 - Updated Diskeeper advice. pp.135 - Added new Search protocol due to SP1. *Continued on Next Page...*

Copyright © 2010 Koroush Ghazi

Version	Release Date	Pages Revised
		Continued... pp.143-144 - Updated Power Plan section, added USB Settings. pp.166 - Updated Windows Update advice, added MS Download Site link. pp.175 - **Important:** Changed ReadyBoost Service advice from Disabled to Automatic due to ReadyBoot. pp.185 - Added Hide Specific Control Panel Items tip. pp.191-192 - Updated Search options for changes due to SP1. pp.208 - Added Windows Live Mail link. pp.214 - Added GSpot utility link. pp.215-216 - Updated Blu-Ray and HD-DVD advice. pp.219 - Updated & expanded options for wallpaper display. pp.221 - Added ClearType XP Powertoy link and advice. pp.225 - Added Advanced Icon Customization section with Iconoid utility. pp.227 - Updated & expanded Customize 3D Task Switching tips. pp.228-229 - Updated DirectX 10 advice for changes in SP1 and the latest games. pp.229-231 - Updated & expanded Games Explorer tips. pp.252 - Added Internet Connectivity Evaluation Tool link and advice. pp.255 - Added Lightsmark OpenGL benchmark. pp.261 - Added SP1 Cleanup Tool section. pp.264 - Added Deleting 'In Use' Files section with Unlocker utility.
2.1	1 July 2008	All pages - Fixed any dead or inaccurate hyperlinks. All pages - Fixed some typographical/grammatical errors. pp.23, 254-255 - Updated 3DMark advice to include 3DMark Vantage. pp.87 - Updated Driver Sweeper instructions. pp.106-108 - Updated AVG Free Edition 8.0 advice. pp.109-110 - Updated Ad-aware 2008 advice. pp.192 - Added Windows Search 4.0 link.
2.2	2 October 2008	All pages - Fixed any dead or inaccurate hyperlinks. All pages - Fixed some typographical/grammatical errors. pp.23,259 - Update advice for Sandra 2009. pp.31 - Added ShadowExplorer link. pp.56-57 - Revised 64-bit advice. pp.77-78 - Updated & expanded Incorrect Folder Views section. pp.84 - Added ASUS Audio Drivers link. pp.96-97 - Expanded Customizing UAC section. pp.97 - Added UAC and the Language Bar section. pp.106 - Added Structured Exception Handling Overwrite Protection section. pp.108-110 - Updated AVG Free Edition 8.0 advice. pp.203 - Added Google Chrome link. pp.218 - Added VLC link. pp.222 - Added Windows Photo Gallery section.
2.3	6 April 2009	All pages - Fixed any dead or inaccurate hyperlinks. All pages - Fixed some typographical/grammatical errors. pp.13 - Added Windows 7 note. pp.45 - Revised Cooling section. pp.56-57 - Expanded 32-bit vs. 64-bit details. pp.84 - Added AHCI reference. pp.85 - Added Auzentech audio driver link. pp.85 - Added Realtek Soundback link. pp.109-111 - Updated AVG Free Edition 8.5 advice. pp.112 - Updated Ad-Aware advice. pp.128 - Added AHCI Mode details. pp.185-186 - Added JV16 PowerTools section, replacing RegSupreme. pp.197-210 - Revised Internet Explorer chapter for IE8. pp.223-224 - Updated and expanded Codecs section. pp.234 - Added Dips64 utility. pp.242-249 - Revised Overclocking chapter with updated information. pp.267 - Added FurMark benchmark.
2.4	28 May 2009	All pages - Fixed any dead or inaccurate hyperlinks. pp.52-53 - Updated slipstreaming and vLite advice for SP2. pp.82-83 - Updated Service Packs installation step for SP2. pp.196 - Noted the inclusion of Windows Search 4.0 in SP2. pp.272 - Updated/renamed Service Pack Cleanup Tool section for SP2.

Copyright © 2010 Koroush Ghazi

Version	Release Date	Pages Revised
3.0	23 June 2010	This is a relatively major revision in terms of a combination of numerous minor changes as well as updating the layout of the book. All pages - Fixed any dead or inaccurate hyperlinks. All pages - Fixed any typographical/grammatical errors. All pages - Updated layout. All pages - Various minor edits and updates throughout to improve readability and accuracy. pp.15-17 - Vista Usage Notes chapter revised. pp.18-23 - Revised Basic PC Terminology chapter with updated/additional information. pp.25-26 - Sandra usage information updated, added SIW and HD Tune utilities. pp.34-35 - Expanded online backup advice. pp.38 - Updated KeePass usage information. pp.39 - Added Recuva utility. pp.46 - Added UEFI details. pp.48-53 - Expanded Hardware Maintenance section. pp.58-59 - Revised SP1 and SP2 slipstreaming advice, added tutorial links. pp.61 - Removed Partition Magic utility and replaced with GParted utility. pp.61-62 - Added short stroking advice. pp.63-64 - Updated 32-bit vs. 64-bit advice. pp.78 - Expanded Live Icon details. pp.84-86 - Revised Edit Context Menus section; added Autoruns, ShellMenuView, ShellExView instructions. pp.93,248,260 - Added Platform Update for DirectX 11 functionality details. pp.93,248,250-260 - Added/revised DirectX information for DirectX 11. pp.94-95 - Revised Motherboard and Graphics Drivers information. pp.99-100 - Expanded Uninstalling Drivers section. pp.102-103 - General Driver Tips section revised/expanded. pp.104-133 - Revised PC Security chapter Microsoft Security Essentials replaces AVG; Spybot replaces Ad-aware. pp.139-142 - Revised Virtual Memory configuration advice. pp.147 - Corrected Master File Table description. pp.148-150 - Revised Windows Disk Defragmenter and Advanced Defragmentation sections; Diskeeper configuration details removed. pp.151-152 - Added Customizing the Windows Control Panel section. pp.200 - Added TDSC utility. pp.206-207 - Expanded/revised the Maintaining the Registry section. pp.229-230 - Corrected Increase Maximum Simultaneous Connections tip. pp.230-231 - Added IE7Pro utility instructions. pp.244-247 - Revised the Audio & Video Codecs and Digital Rights Management sections. pp.257 - Expanded Advanced Icon Customization section. pp.264-270 - Revised Overclocking chapter with updated/additional information. pp.287-290 - Added Heaven, Lightsmark, HD Tune utilities; updated Prime95 instructions. pp.294-296 - Updated/expanded CCleaner usage information. pp.296-297 - Revised Manual Cleaning section. pp.299-300 - Revised and reordered Regular Maintenance chapter instructions.

Copyright © 2010 Koroush Ghazi