TUTORIAL On How To Use Process Explorer

This information was adapted from the help file for the program.

Process Explorer is an advanced process management utility is very similar to Task Manager. Process Manager picks up where Task Manager leaves off. It allows you to see detailed information about a process such as what icon it uses , command-line, full image path, memory statistics, user account, security attributes, and more so much more. When you zoom in on a particular process you can list the DLLs that has been loaded or the operating system

resource handles it has open. A search capability enables you to track down a process that has a resource opened, such as a file, directory or Registry key, or to view the list of processes that have a DLL loaded.

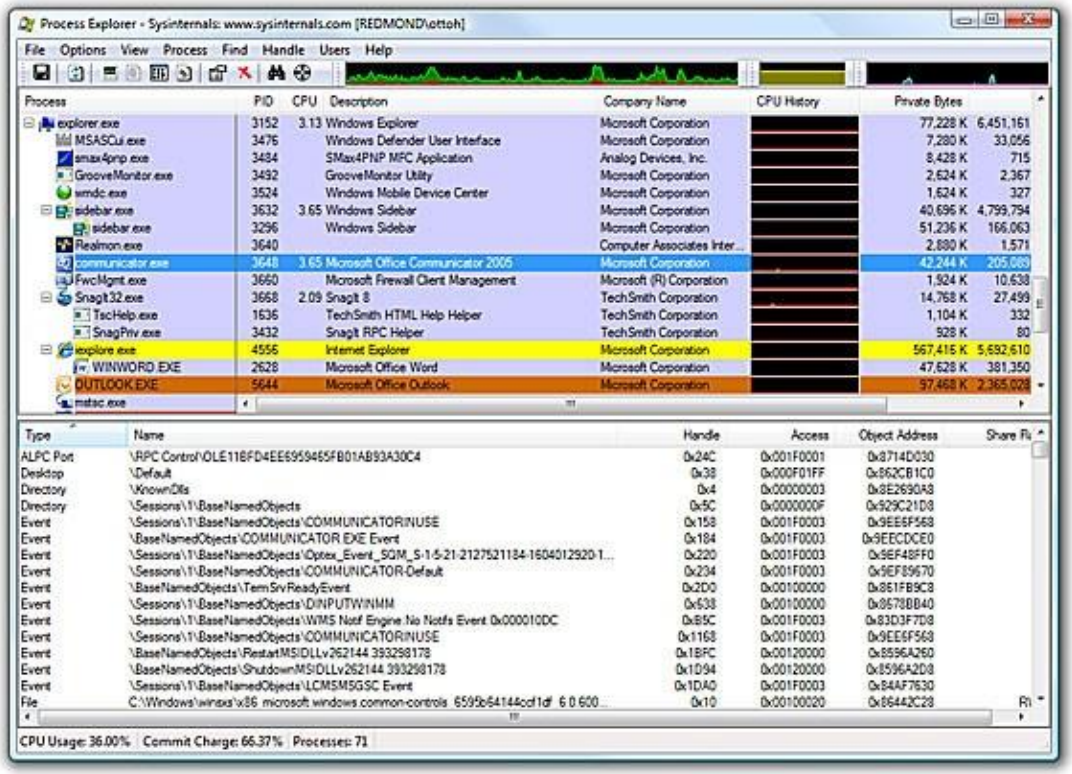
The Process Explorer display uses two sub-windows. The top always shows a list of the currently active processes, including the names of their owning accounts, whereas the information displayed in the bottom window, which you can close, depends on the mode that Process Explorer is in: if it is in handle mode you will see the handles that the process selected in the top window has opened; if Process Explorer is in DLL mode you will see the DLLs and memory-mapped files that the process has loaded.

Process Explorer also has a powerful search capability that will quickly show you which processes have particular handles opened or DLLs loaded. The unique capabilities of Process Explorer make it useful for tracking down DLL-version problems or handle leaks, and provide insight into the way Windows and applications work.

You can obtain equivalent command-line tools, Handle and ListDLLs, at the Sysinternals Web site.

Process Explorer does not require administrative privileges to run and works on Windows 9x/Me, Windows NT 4.0, Windows 2000, Windows XP, Server 2003, Windows Vista, Windows Server 2008 and on the x64 version of 64-bit Windows XP, Windows Vista, Windows Server 2003, and Windows Server 2008.

The Main Window (Here is the Main Menu for Process Explorer.



Views

The Process Explorer window shows by default two panes: the upper pane is always a process list and the bottom either shows the list of DLLs loaded into the process selected in the upper pane, or the list of operating system resource handles (files, Registry keys, synchronization objects) the process has open; the view mode determines which information is shown in the bottom pane. To switch the view, use the **View|Lower Pane View** menu item, the corresponding toolbar button (which toggles), or the Ctrl+D (DLL view) and Ctrl-H (handle view) accelerator keys.

If you are only interested in seeing the processes running on your system You can hide the lower pane by selecting **View|Hide Lower Pane**, the corresponding toolbar button, the Ctrl+L accelerator, or by dragging the pane divider to the bottom of the Process Explorer window. You can bring back the lower pane by selecting **View|Show Lower Pane**, typing Ctrl+L or selecting the toolbar button again.

Mini Graphs

Process Explorer includes a toolbar and mini graphs for CPU, memory, and if on Windows 2000 or higher, I/O history, at the top of the main window. They can be resized with respect to one another or dragged such that each is on a separate row. The mini-graphs show history of

system activity and hovering the mouse over a point on a graph displays in a tooltip the associated time and the process information for point in time. For example, the tooltip for the mini-CPU graph shows the process that was the largest consumer of CPU. Clicking on any of the mini-graphs opens the System Information dialog.

Refresh Rate and Difference Highlighting

Configure the rate at which Process Explorer refreshes its window by using the **View|Update Speed** menu item. You can refresh the view manually at any time with **View|Refresh**, the refresh toolbar button, or by pressing F5. Some checks, such as whether a process is part of a Job object or uses the .NET runtime, only occur during process startup. Press F5 to have Process Explorer recheck the status of all processes.

Process Explorer uses difference highlighting to help you see what items change between refreshes. Items, including processes, DLLs, and handles, that exit or are closed show in red and new items show in green. If the refresh rate is not paused the highlighting remains in effect for the interval specified by the **Options|Difference Highlight Duration** dialog, which has a default value of 1 second. If you pause the display the difference highlighting is in effect only until the next time you manually refresh.

Opacity

You can make the Process Explorer window partially transparent so that windows beneath it show through on systems that support it by making a selection under the **View|Opacity** menu item.

Saving

When you choose **File|Save** Process Explorer saves the contents of the Process and lower pane, if it is showing, as a tab-delimited text file.

Shutting Down or Logging Off
Use the **File|Shutdown** menu items to shutdown, reboot, lock or logoff the system. When available, the menu also offers options for hibernating and suspending the system.

Run
Use this option to run other applications from Process Explorer using the standard Windows Run dialog.

Runas
This variant on the Run command allows you to enter alternate credentials for the launching application. Process Explorer leverages the same Windows functionality as the Runas Windows command to provide this support. The Runas menu item is not present on Windows 9x.

Run as Limited User
This variant on the Run command runs the application you specify in the same account as that of Process Explorer, but without administrative privileges or membership in the local administrators group. This option restricts the exposure of your system from applications, such as Internet Explorer, that might be compromised through access of untrusted data.

Columns and Column Sets

Column Selection

The information Process Explorer displays in its main window is fully configurable. You can reorder columns by dragging them to their new position. To select which columns of data you want visible in each of the views and the status bar, choose View|Select Columns or right-click on a column header and use Select Columns from the resulting context menu. A column selection editor opens that lets you pick the columns you want to enable for the Process, DLL, handle panes, and status bar.

Column Sets
You can save a column configuration and its associated sort settings by choosing View|Save Column Set. Process Explorer will prompt you to name the column set. You can load a saved column set by selecting it in the View|Load Column Set menu or by entering its associated accelerator keys. To reorder or rename existing column sets go to View|Organize Column Sets to open the column set organizer.

General Options

Command-Line Usage: Process Explorer takes two options that modify its behavior:

/e	Prompt for UAC elevation to restart with administrative rights if launched without administrative rights.
/s:<pid>	Select the process having the specified process ID after starting.
/t	Start Process Explorer minimized in the tray.
/p:[r|h|n|l]	Set Process Explorer's priority to realtime (r), high (h), normal (n), or low (l).

(Taken From Wikipedia)

Always on Top: Choose this option to have Process Explorer's window remain above other windows.

Replace Task Manager: Select the Replace Task Manager entry under the Options menu to have Process Explorer execute instead of Task Manager when you launch Task Manager. Note that this is a global setting that affects all users regardless of how they start Task Manager. After replacing Task Manager the menu item renames to **Restore Task Manager** and selecting it removes Process Explorer's association.

Confirm Kill: uncheck this if you do not want Process Explorer to prompt you for confirmation before terminating a process you've directed it to kill.
CPU History in Tray: this option toggles Process Explorer's tray icon between a standard chart representation of the current CPU usage and a miniature version of the CPU history graph.

Verify Image Signatures: if this is checked then images corresponding to processes are checked for trusted signatures automatically when you view a process properties and the result is shown next to the company field in the process properties dialog. "(Verified)" next a company name means the file is signed by a trusted root certificate authority and "(Unable to Verify)" means the file is either unsigned or signed by an untrusted authority. Uncheck this option to speed performance when viewing process image properties.

Configure Symbols: on Windows NT and higher, if you want Process Explorer to resolve addresses for thread start addresses in the threads tab of the process properties dialog and the thread stack window then configure symbols by first downloading the Debugging Tools for Windows package from Microsoft's web site and installing it in its default directory. Open the Configure Symbols dialog and specify the path to the dbghelp.dll that's in the Debugging Tools directory and have the symbol engine download symbols on demand from Microsoft to a directory on your disk by entering a symbol server string for the symbol path. For example, to have symbols download to the c:\symbols directory you would enter this string:

srv*c:\symbols*http://msdl.microsoft.com/download/symbols

Process Explorer sorts processes into the system process tree. The process tree reflects the parent-child relationship between processes where child processes are shown directly beneath their parent and right-indented. Processes that are left-justified are orphans; their parent has exited and is no longer being
used. To change the sort order simply click on a the column by which you wish to sort. To return the sort to the process tree select **View|Show Process Tree**, click the process tree toolbar button, or type Ctrl+T.

Interrupts and DPCs

On Windows NT-based systems Process Explorer shows two artificial processes: Interrupts and DPCs. These processes reflect the amount of time the system spends servicing hardware interrupts and Deferred Procedure Calls (DPCs), respectively. High CPU consumption by these activities can indicate a hardware problem or device driver bug. To see the total number of interrupts and DPCs executed since the system booted add the Context Switch column. Another sometimes useful metric is the number of interrupts and DPCs generated per refresh interval, which you see when you add the CSwitches Delta column.

Find Window's Process

You can highlight the process that owns a window visible on the desktop by dragging the target-like toolbar button over the window in question. Process Explorer will select the owning process entry in the process view.
Enter a comment for a process in the Comment field. Comments are visible in the process view in the Comment column, or if you do not have the comment column selected, in the tool tip that displays when you hover the mouse over a process. Comments apply to all processes with the same path and are remembered from execution to execution.

On systems that support Data Execution Protection (DEP), Process Explorer shows the DEP

status of the selected process as either "on" or "off". Software DEP is currently supported by Windows XP SP2 and higher on 32-bit x86 systems whereas hardware DEP is available only on 64-bit versions of Windows. You can also view DEP status by adding the corresponding DEP Status column to the process view.

Malware, including viruses, spyware, and adware is often stored in a packed encrypted form on disk in order to attempt to hide the code it contains from antispyware and antivirus. Process Explorer uses a heuristic to determine if an image is packed and if it is changes the text above the full path display field to include "(Image is probably packed)".

Performance:

Memory and CPU performance data displays on this page, including physical and virtual memory, and CPU usage. The data refreshes at the same interval that the main display does.

Performance Graph:

A history of a process' CPU usage and its private bytes allocation shows as in Task Manager-like graphs on this page. Red in the CPU usage graph indicates CPU usage in kernel-mode whereas green is the sum of kernel-mode and user-mode execution. Private Bytes represents the

amount of private virtual memory a process has allocated and is the value that will rise of a process exhibiting a memory leak bug. Note that while the System Information performance graphs update while Process Explorer is minimized to the tray, these graphs do not. The private bytes usage graphs are scaled against the peak amount of private bytes the process has allocated; if the peak grows the graphs recalculate their scales. In the I/O graph the blue line indicates total I/O traffic, which is the sum of all process I/O reads and writes, between refreshes and the pink line shows write traffic. The I/O graph is scaled against the peak I/O traffic the process has generated since the start of monitoring.

Moving the mouse over part of a graph results in the time of the corresponding data point being shown in the graph as a popup either on the far left or right.

Threads:

The list of the threads running in the process shows on this tab. The thread list shows start address information that's provided by the Windows symbol engine. If you want to see accurate names for start addresses then follow the directions for configuring symbols.

The Module button on the threads page launches Explorer's file properties dialog box for the image file that contains the start address of the currently selected thread. The Stack button shows the current stack of the selected thread. Stack information is unreliable unless symbol files are available for process and DLLs referenced in the stack.

Use the Kill button to terminate a thread. Note that terminating a thread may lead to a crash or erratic behavior of the process.

Use the Suspend button to suspend a thread. Note that suspending threads may cause its process to stop executing.

TCP/IP:

Any active TCP and UDP endpoints owned by the process are shown on this page.
On Windows XP SP2 and higher this page includes a Stack button that opens a dialog that shows the stack of the thread that opened the selected endpoint at the time of the open. This is useful for identifying the purpose of endpoints in the System process and Svchost processes because the stack will include the name of the driver or service that is responsible for the endpoint.

Security:

Process Explorer reports the list of groups and privileges listed in the security token of the process on this page. Privileges shown in grey are disabled. The permissions button opens a permissions editor that shows the access permissions assigned to the process.

Job:

This tab is present only for processes that are part of a Win32 Job. The Job page shows the list of processes that are part of the same job and the limits that are applied to the job.

Services:

This tab is present only for processes that are executing Win32 services, and lists the services running within the process. Process Explorer shows a service's name and display name, and on Windows 2000 and higher, if available, the service's description. The permissions button opens a permissions editor that shows the access permissions assigned to the service.

Environment:

The environment variables associated with the process show on this page.

Strings:

All printable strings of at least 3 characters in length display on this page. Image strings are read from the process image file on disk whereas Memory strings are read from the image's in-memory storage. Memory strings may be different than on-disk strings when an image uses a decompresses or decrypts when it loads into memory.

The DLL View

The DLL Context Menu

The DLL view shows the image file, DLLs, and data files mapped into the address space of the selected process. When you click the properties toolbar button or select **Properties** from the DLL menu Process Explorer opens a properties dialog for the DLL or mapped file that contains two tabs:

Image:

This page shows version information extracted from the image file and the full path of the image file.

Process Explorer checks for whether or not an image has been digitally signed by a certificate root authority trusted by the computer and displays the status of the check, which is either "Trusted" (signed), "Unsigned", or "Not Verified" (signature has not been checked). You can press the **Verify** button to have Process Explorer check the signature of an image that has not been verified. Note that the verification operation can result in Process Explorer contacting web sites to check for certificate validity. See the **Verify Image Signatures** option.

Malware, including viruses, spyware, and adware is often stored in a packed encrypted form on disk in order to attempt to hide the code it contains from antispyware and antivirus. Process Explorer uses a heuristic to determine if an image is packed and if it is changes the text above the full path display field to include "**(Image is probably packed)**".

Strings:

All printable strings of at least 3 characters in length display on this page. Image strings are read from the process image file on disk whereas Memory strings are read from the image's in-memory storage. Memory strings may be different than on-disk strings when an image uses a decompresses or decrypts when it loads into memory.

Highlight Relocated DLLs

When you select the **Relocated DLLs** entry in the **Options|Configure Highlighting** dialog any DLLs that are not loaded at their programmed base address show in yellow. DLLs that cannot load at their base address because other files are already mapped there are relocated by the loader, which consumes CPU and makes parts of the DLL that are modified as part of the relocation un-sharable.

Search Online
Selecting this entry will result in Process Explorer launching the system's configured Internet browser and initiating an Internet search for the selected DLL's name.

The Handle View

The Handle Context Menu

Two items appear under the Handle menu or when you right-click to show the Handle context menu:

Close Handle: choose this item to force closed a handle. Use this at your own risk: because the process that owns the handle is not aware that its handle has been closed, using this feature can lead to a crash of the application or data corruption; closing a handle in the System process can lead to a system crash.

Properties: when you select this item Process Explorer opens a handle properties dialog that shows you the total number of handles open to the object, as well as kernel references to the object. It also shows information specific to the type of object you are viewing. For example, when you view the properties of a mutant object Process Explorer reports whether or not the mutant is held, and if so, by which thread.

The **Security** tab on the handle properties dialog shows the security that's applied to the object the handle references.

The Users Menu

On systems that include Terminal Services Process Explorer displays a Users menu that lists the currently connected sessions. Process Explorer creates a menu entry for each session that's name includes the session's session ID and the user logged into the session. Each entry opens a sub menu that has options for disconnecting, logging off, and sending a message to the session's user. In addition, a Properties menu for each session entry opens a dialog box that lists detailed information about the session, including the IP address and name of the client connected to the session.

The contents of the Users menu are updated each time you open the menu to reflect current session information.

Searching

One of the common problems Process Explorer solves with ease is the question: what process has this file or directory open, or which processes have a particular DLL loaded?

You can perform a handle and DLL search by selecting **Find|Find Handle or DLL** or by typing Ctrl+F. Searches are case insensitive substring searches of all of the handles opened and DLLs loaded on the system with the text you enter. Thus, to search for the process or processes that have c:\directory\somefile.txt open enter enough text to make the search find only the results you are interested in e.g. "somefile".

The search dialog populates with the list of results indexed by process. Select lines in the results to have Process Explorer select the reported process and DLL or handle, and double-click on a line to have it do the same and dismiss the Search dialog.