How To establish a clean environment for Malware monitoring, reverse engineering, and removal purposes

NOTE: a PE environment does not mean that it can't be infected, nor does a VM client, as sophisticated Malware is now capable of escaping
sandboxed environments (Boo!) It is critical that you are either working from a WRITE PROTECTED environment, or simply have no HD in the
lab pc(no HD, nothing but RAM to infect, and that's erased when you cut power...usually :P)

Run your process monitoring tool of choice, and a process viewing tool as well.
I prefer to run these a system start-up, before attaching the infected HD. This enables you to start catching Malware traces the moment they
attempt to inject themselves into your VM, or even PE environment.

Develop a log that contains information about the Malware, by allowing the Malware to infect the host system (VM, or PE RAM environment).
Dumpster Dive, I mean search the log for clue's to identify the Malware.
Flag the Malware for your removal process.
Identify MBR infections, Bootloader infections, Hidden Partitions, etc.

MBR infections can be isolated using software like MBRCheck, aswMBR, GMER, etc.
Use tools like Partition Magic, diskpart, etc., to mount and unmount hidden partitions.

Mount the hidden partition if there is one, and inspect the files for Malware. My suggestion, if you find Malware on the partition, format the partition completely.
You can always clone partition's like this to another storage media device for future analysis.

NOTE: some hidden partitions are simply encrypted, hence why they do not mount. I'm not going to expand on breaking into encrypted environments...

Remove the Malware from the HD.
Repair the MBR if an Unknown MBR record is detected using MBRCheck, aswMBR, etc.
Run your Rootkit removal tools; TDSSKiller, etc.
Run your Malware Removal tools; Malwarebytes, Hitman, Superantispyware, etc.
Run your Anti-Virus programs; AVG, Norton, etc.
Isolate and remove remaining infected files⁄partitions manually using your Malware log created previously, and a Explorer tool⁄partition editing application.
Enjoy your hopefully clean system.

These are some basic steps I employ to remove troublesome Malware. It is not fool proof, and I am in no way a Malware Analysis Pro, so please do your
own research, (Nick's Quote) as your mileage may vary.

More advise...
Never attach an infected HD to a clean system without having first removed your systems HD, or ensured that it is write-protected.
Purchase a write-protected USB drive...they are cheap, and you can load your PE environment onto it providing you with a write-protected forensic lab in
your POCKET!!