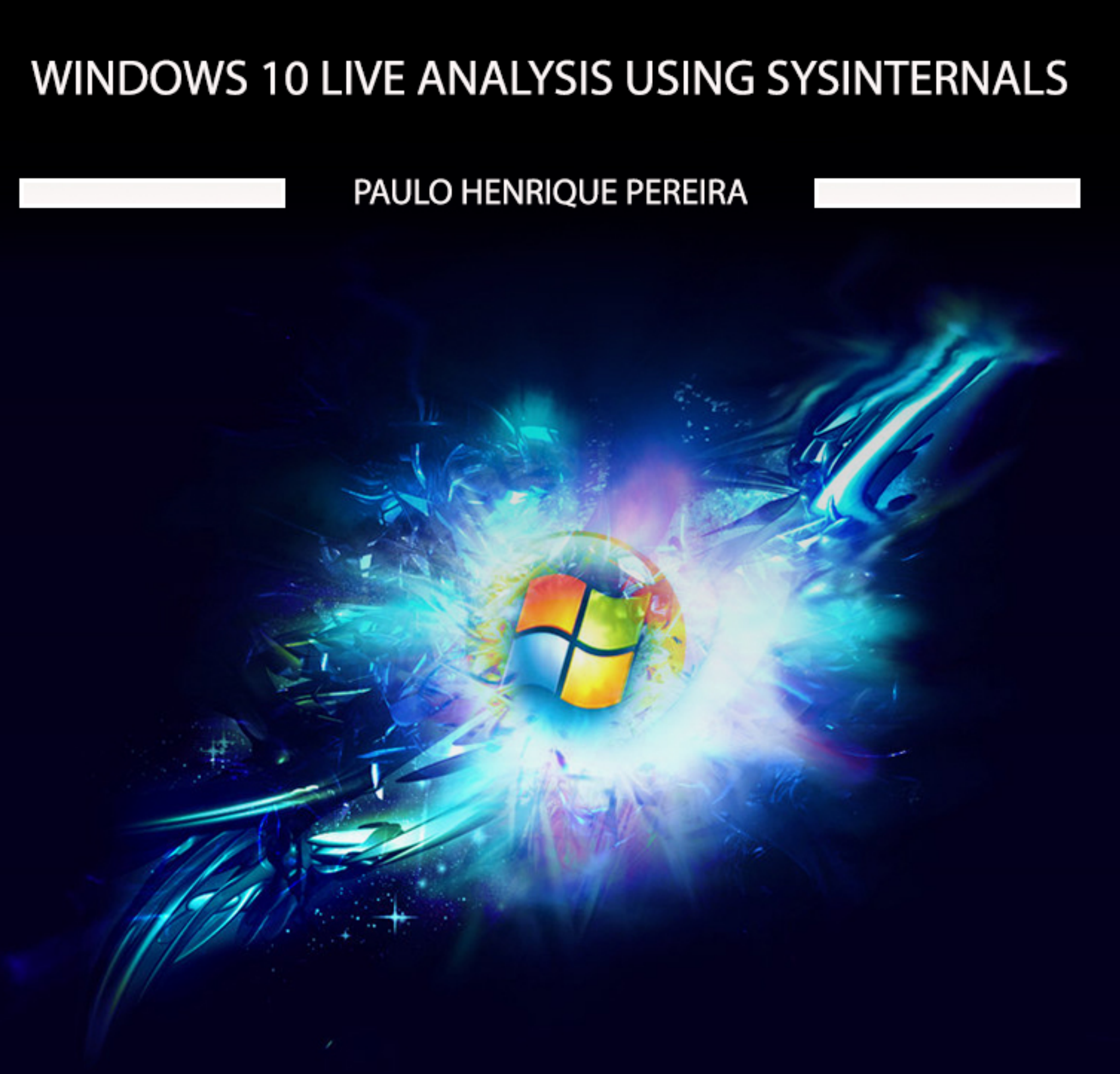
# WINDOWS 10 LIVE ANALYSIS USING SYSINTERNALS

PAULO HENRIQUE PEREIRA



## Introductory Materials

eForensics Magazine

# I. General course instructions (please read carefully)

This course will address forensic problems in *real time*. This implies that the analyzed files, libraries, extensions or packages (among other objects and instances) *do not originate from a captured memory image of a machine*. In other words, the files manipulated in this file *are all files that can cause problems on your machine* if you do not follow these instructions.

**WARNING!**

a) **Keep in mind that this course is a forensic course and for this reason you will be able *to deal with malicious artifacts.***

b) **Do the labs exercises of this course *always using a virtual machine.* Never use your virtual machine with the active internet connection!**

c) ***Disable the internet connection* of the virtual machines that this course will use in the labs!**

d) ***Never share the analyzed files* with your physical machine!**

e) **Do not reproduce laboratories on a machine that you use for personal purposes!**

f) **Do not use the virtual machines of this course to access your emails, pay bills online or use social media to talk with your friends!**

g) **All files used in this course should never be saved to your personal machine!**

After reading all the above warnings, consider yourself warned.

# II. Software used in this course

Since the course proposal is to provide students with a forensic analysis that may be very like what would happen in a real case, we have chosen to indicate that you install the following software **in the virtual machines**:

- Sysinternals Suite
- WDK and Windbg for Windows 10 (https://developer.microsoft.com/en-us/windows/hardware/windows-driver-kit)
- Visual Studio
- About debuggers read instructions in this site: https://msdn.microsoft.com/en-us/library/windows/hardware/ff551063(v=vs.85).aspx
- A Hex editor to analyze data structure of files.

# III. Sysinternals Tools

In this course, we will focus **on some tools** that belong to the Sysinternals suite. Given the large number of tools we will not be able to cover all of them in a four-module course. For this reason, we will highlight the tools that may be most used in a forensic analysis. Sysinternals Suite® is a great conjunction of open tools. The last version was updated in November (2016) with has 69 utilities and can be downloaded in the link: https://technet.microsoft.com/en-us/sysinternals/bb842062.

Suite has not the tools BSOD Screen Saver and NotMyFault. The descriptive of the utilities is found in the index page: https://technet.microsoft.com/en-us/sysinternals/bb545027.

According the last version, the Suite contain the following tools:

| | | |
|---|---|---|
| AccessChk | Hex2dec | PsLogList |
| AccessEnum | Junction | PsPasswd |
| AdExplorer | LDMDump | PsService |
| AdInsight | ListDLLs | PsShutdown |
| AdRestore | LiveKd | PsSuspend |
| Autologon | LoadOrder | RAMMap |
| Autoruns | LogonSessions | RegDelNull |
| BgInfo | MoveFile | Registry Usage (RU) |
| CacheSet | NTFSInfo | RegJump |
| ClockRes | PendMoves | SDelete |
| Contig | PipeList | ShareEnum |
| Coreinfo | PortMon | ShellRunas |
| Ctrl2Cap | ProcDump | Sigcheck |
| DebugView | Process Explorer | Streams |
| Desktops | Process Monitor | Strings |
| Disk2vhd | PsExec | Sync |
| DiskExt | PsFile | Sysmon |
| DiskMon | PsGetSid | TCPView |
| DiskView | PsInfo | VMMap |
| Disk Usage (DU) | PsPing | VolumeID |
| EFSDump | PsKill | WhoIs |
| FindLinks | PsList | WinObj |
| Handle | PsLoggedOn | ZoomIt |

In my opinion, these tools can be classified in four groups. The name of the group is my suggestion based on **Windows Sysinternals Administrator's Reference**:

**a.** Process and System diagnostic

**b.** Security and Network

**c.** Files, Desktop and Disk analysis

**d.** Derivative tools (Miscellaneous)

This classification is just to organize the tools and does not have the perspective of assigning importance to each tool. According site of Sysinternals we have following groups (I regrouping tools for my purposes here):

**Tools marked with (*) will be used in the labs in this course.**

| Sysinternals Security tools (*) | Specification |
|---|---|
| AccessChk | This tool shows you the accesses the user or group you specify has to files, Registry keys or Windows services. |
| AccessEnum | This simple yet powerful security tool shows you who has what access to directories, files and Registry keys on your systems. Use it to find holes in your permissions. |
| Autologon | Bypass password screen during logon. |
| Autoruns (*) | **See what programs are configured to startup automatically when your system boots and you log in. Autoruns also shows you the full list of Registry and file locations where applications can configure auto-start settings.** |
| LogonSessions | List active logon sessions |
| Process Explorer (*) | **Find out what files, registry keys and other objects processes have open, which DLLs they have loaded, and more. This uniquely powerful utility will even show you who owns each process.** |
| PsExec | Execute processes with limited-user rights. |
| PsLoggedOn | Show users logged on to a system. |
| PsLogList | The PsTools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more. |
| PsTools * | **The PsTools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more.** |
| SDelete | Securely overwrite your sensitive files and cleanse your free space of previously deleted files using this DoD-compliant secure delete program. |
| ShareEnum | Scan file shares on your network and view their security settings to close security holes. |
| ShellRunas | Launch programs as a different user via a convenient shell context-menu entry. |
| Sigcheck (*) | **Dump file version information and verify that images on your system are digitally signed.** |
| Sysmon (*) | **Monitors and reports key system activity via the Windows event log.** |

https://technet.microsoft.com/en-us/sysinternals/bb795534

| Sysinternals Process tools (*) | Specification |
|---|---|
| Handle | This handy command-line utility will show you what files are open by which processes, and much more. |
| Autoruns (*) | **See what programs are configured to startup automatically when your system boots and you log in. Autoruns also shows you the full list of Registry and file locations where applications can configure auto-start settings.** |
| Process Explorer (*) | **Find out what files, registry keys and other objects processes have open, which DLLs they have loaded, and more. This uniquely powerful utility will even show you who owns each process.** |
| PsExec | Execute processes with limited-user rights. |
| PsLoggedOn | Show users logged on to a system. |
| PsLogList | The PsTools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more. |
| ListDLLs | List all the DLLs that are currently loaded, including where they are loaded and their version numbers. Version 2.0 prints the full path names of loaded modules. |
| PortMon | Monitor serial and parallel port activity with this advanced monitoring tool. It knows about all standard serial and parallel IOCTLs and even shows you a portion of the data being sent and received. Version 3.x has powerful new UI enhancements and advanced filtering capabilities. |
| ProcDump (*) | **This new command-line utility is aimed at capturing process dumps of otherwise difficult to isolate and reproduce CPU spikes. It also serves as a general process dump creation utility and can also monitor and generate process dumps when a process has a hung window or unhandled exception.** |
| Process Monitor | Monitor file system, Registry, process, thread and DLL activity in real-time. |
| PsExec | Execute processes remotely. |
| PsGetSid | Displays the SID of a computer or a user. |
| PsKill | Terminate local or remote processes. |
| PsList | Show information about processes and threads. |
| PsSuspend | Suspend and resume processes. |
| ShellRunas | Launch programs as a different user via a convenient shell context-menu entry. |
| PsTools | The PsTools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more. |
| PsService | View and control services. |
| VMMap (*) | **See a breakdown of a process's committed virtual memory types as well as the amount of physical memory (working set) assigned by the operating system to those types. Identify the sources of process memory usage and the memory cost of application features.** |

https://technet.microsoft.com/en-us/sysinternals/bb795533

| Sysinternals System tools (*) | Specification |
|---|---|
| Handle | This handy command-line utility will show you what files are open by which processes, and much more. |
| Autoruns (*) | **See what programs are configured to startup automatically when your system boots and you log in. Autoruns also shows you the full list of Registry and file locations where applications can configure auto-start settings.** |
| Process Explorer (*) | **Find out what files, registry keys and other objects processes have open, which DLLs they have loaded, and more. This uniquely powerful utility will even show you who owns each process.** |
| Process Monitor (*) | **Monitor file system, Registry, process, thread and DLL activity in real-time.** |
| PsList | Show information about processes and threads. |
| PsTools | The PsTools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more. |
| ClockRes | View the resolution of the system clock, which is also the maximum timer resolution. |
| Coreinfo | Coreinfo is a command-line utility that shows you the mapping between logical processors and the physical processor, NUMA node, and socket on which they reside, as well as the cache's assigned to each logical processor. |
| LiveKd (*) | **Use Microsoft kernel debuggers to examine a live system.** |
| LoadOrder | See the order in which devices are loaded on your WinNT/2K system. |
| LogonSessions | List the active logon sessions on a system. |
| PendMoves | Enumerate the list of file rename and delete commands that will be executed the next boot. |
| ProcFeatures | This applet reports processor and Windows support for Physical Address Extensions and No Execute buffer overflow protection. |
| RAMMap (*) | **An advanced physical memory usage analysis utility that presents usage information in different ways on its several different tabs.** |
| WinObj | The ultimate Object Manager namespace viewer is here. |
| PsLoggedOn | Show users logged on to a system |

https://technet.microsoft.com/en-us/sysinternals/bb795535

| Sysinternals File and Disk tools (*) | Specification |
|---|---|
| AccessChk | This tool shows you the accesses the user or group you specify has to files, Registry keys or Windows services. |
| AccessEnum | This simple yet powerful security tool shows you who has what access to directories, files and Registry keys on your systems. Use it to find holes in your permissions. |
| CacheSet | CacheSet is a program that allows you to control the Cache Manager's working set size using functions provided by NT. It's compatible with all versions of NT. |
| Contig | Wish you could quickly defragment your frequently used files? Use Contig to optimize individual files, or to create new files that are contiguous. |
| Disk2vhd | Disk2vhd simplifies the migration of physical systems into virtual machines (p2v). |
| DiskExt | Display volume disk-mappings. |
| DiskMon | This utility captures all hard disk activity or acts like a software disk activity light in your system tray. |
| DiskView | Graphical disk sector utility. |
| Disk Usage (DU) | View disk usage by directory. |
| EFSDump (*) | **View information for encrypted files.** |
| FindLinks | FindLinks reports the file index and any hard links (alternate file paths on the same volume) that exist for the specified file. A file's data remains allocated so long as at it has at least one file name referencing it. |
| Junction | Create Win2K NTFS symbolic links. |
| LDMDump | Dump the contents of the Logical Disk Manager"s on-disk database, which describes the partitioning of Windows 2000 Dynamic disks. |
| MoveFile | Schedule file rename and delete commands for the next reboot. This can be useful for cleaning stubborn or in-use malware files. |
| NTFSInfo (*) | **Use NTFSInfo to see detailed information about NTFS volumes, including the size and location of the Master File Table (MFT) and MFT-zone, as well as the sizes of the NTFS meta-data files.** |
| PsFile | See what files are opened remotely. |
| SDelete | Securely overwrite your sensitive files and cleanse your free space of previously deleted files using this DoD-compliant secure delete program. |
| ShareEnum | Scan file shares on your network and view their security settings to close security holes. |
| Sigcheck (*) | **Dump file version information and verify that images on your system are digitally signed.** |
| Streams | Reveal NTFS alternate streams. |
| Sync | Flush cached data to disk. |
| VolumeID | Set Volume ID of FAT or NTFS drives. |
| Process Monitor (*) | **Monitor file system, Registry, process, thread and DLL activity in real-time.** |
| PsTools (*) | **The PsTools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more.** |
| PendMoves | Enumerate the list of file rename and delete commands that will be executed the next boot. |
| PsFile | See what files are opened remotely. |

https://technet.microsoft.com/en-us/sysinternals/bb545046

| Sysinternals Network tools (*) | Specification |
|---|---|
| AD Explorer | Active Directory Explorer is an advanced Active Directory (AD) viewer and editor. |
| AD Insight | AD Insight is an LDAP (Light-weight Directory Access Protocol) real-time monitoring tool aimed at troubleshooting Active Directory client applications. |
| AdRestore | Undelete Server 2003 Active Directory objects. |
| PipeList | Displays the named pipes on your system, including the number of maximum instances and active instances for each pipe. |
| PsFile | See what files are opened remotely. |
| PsPing | Measures network performance. |
| PsTools (*) | **The PsTools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more.** |
| ShareEnum (*) | **Scan file shares on your network and view their security settings to close security holes.** |
| TCPView (*) | **Active socket command-line viewer.** |
| Whois (*) | **See who owns an Internet address.** |

https://technet.microsoft.com/en-us/sysinternals/bb795532

I'll add here the **Strings** tool (Miscellaneous group) because in a forensic investigation of an malicious artifact we will need discovery the strings associated with an malware (for example).