Dynamic Malware Analysis

Running and observing malware in a controlled environment to study its behavior in real-time.
=> File Changes, Registry Changes, Network Connections, Processes

Process Monitor : [Download and Unzip]

https://download.sysinternals.com/files/ProcessMonitor.zip

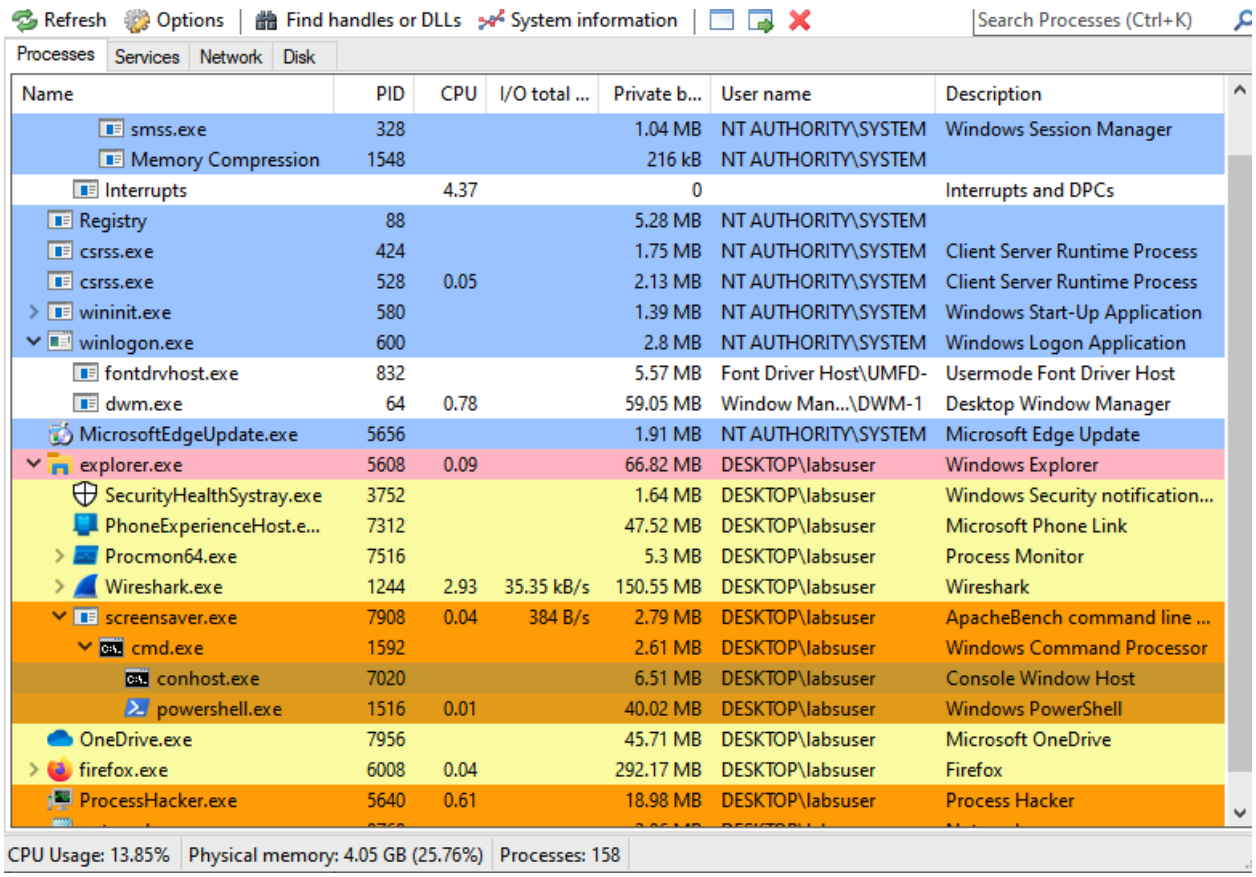
Process Hacker :[Download and Install]
https://sourceforge.net/projects/processhacker/files/processhacker2/processhacker-2.39-setup.exe/download

Graphviz : [Download and Install]
https://gitlab.com/api/v4/projects/4207231/packages/generic/graphviz-releases/8.1.0/windows_10_cmake_Release_graphviz-install-8.1.0-win64.exe

WireShark : [Download and Install]
https://2.na.dl.wireshark.org/win64/Wireshark-4.4.0-x64.exe

Proc Dot: [Download and Install]
https://www.procdot.com/download/procdot/binaries/procdot_1_22_57_windows.zip

RegShot : [Download and Unzip]
https://sourceforge.net/projects/regshot/files/latest/download


Refresh
Options
Find handles or DLLs
System information
Search Processes (Ctrl+K)
Processes
Services
Network
Disk
Name
PID
CPU
I/O total ...
Private b...
User name
Description
smss.exe 328 1.04 MB NT AUTHORITY\SYSTEM Windows Session Manager
Memory Compression 1548 216 kB NT AUTHORITY\SYSTEM
Interrupts 4.37 0 Interrupts and DPCs
Registry 88 5.28 MB NT AUTHORITY\SYSTEM
csrss.exe 424 1.75 MB NT AUTHORITY\SYSTEM Client Server Runtime Process
csrss.exe 528 0.05 2.13 MB NT AUTHORITY\SYSTEM Client Server Runtime Process
wininit.exe 580 1.39 MB NT AUTHORITY\SYSTEM Windows Start-Up Application
winlogon.exe 600 2.8 MB NT AUTHORITY\SYSTEM Windows Logon Application
fontdrvhost.exe 832 5.57 MB Font Driver Host\UMFD- Usermode Font Driver Host
dwm.exe 64 0.78 59.05 MB Window Man...\DWM-1 Desktop Window Manager
MicrosoftEdgeUpdate.exe 5656 1.91 MB NT AUTHORITY\SYSTEM Microsoft Edge Update
explorer.exe 5608 0.09 66.82 MB DESKTOP\labsuser Windows Explorer
SecurityHealthSystray.exe 3752 1.64 MB DESKTOP\labsuser Windows Security notification...
PhoneExperienceHost.e... 7312 47.52 MB DESKTOP\labsuser Microsoft Phone Link
Procmon64.exe 7516 5.3 MB DESKTOP\labsuser Process Monitor
Wireshark.exe 1244 2.93 35.35 kB/s 150.55 MB DESKTOP\labsuser Wireshark
screensaver.exe 7908 0.04 384 B/s 2.79 MB DESKTOP\labsuser ApacheBench command line ...
cmd.exe 1592 2.61 MB DESKTOP\labsuser Windows Command Processor
conhost.exe 7020 6.51 MB DESKTOP\labsuser Console Window Host
powershell.exe 1516 0.01 40.02 MB DESKTOP\labsuser Windows PowerShell
OneDrive.exe 7956 45.71 MB DESKTOP\labsuser Microsoft OneDrive
firefox.exe 6008 0.04 292.17 MB DESKTOP\labsuser Firefox
ProcessHacker.exe 5640 0.61 18.98 MB DESKTOP\labsuser Process Hacker
CPU Usage: 13.85%
Physical memory: 4.05 GB (25.76%)
Processes: 158