

Assignment

Name: Hassan Ahmed

Class: BS DFCS

Section: A

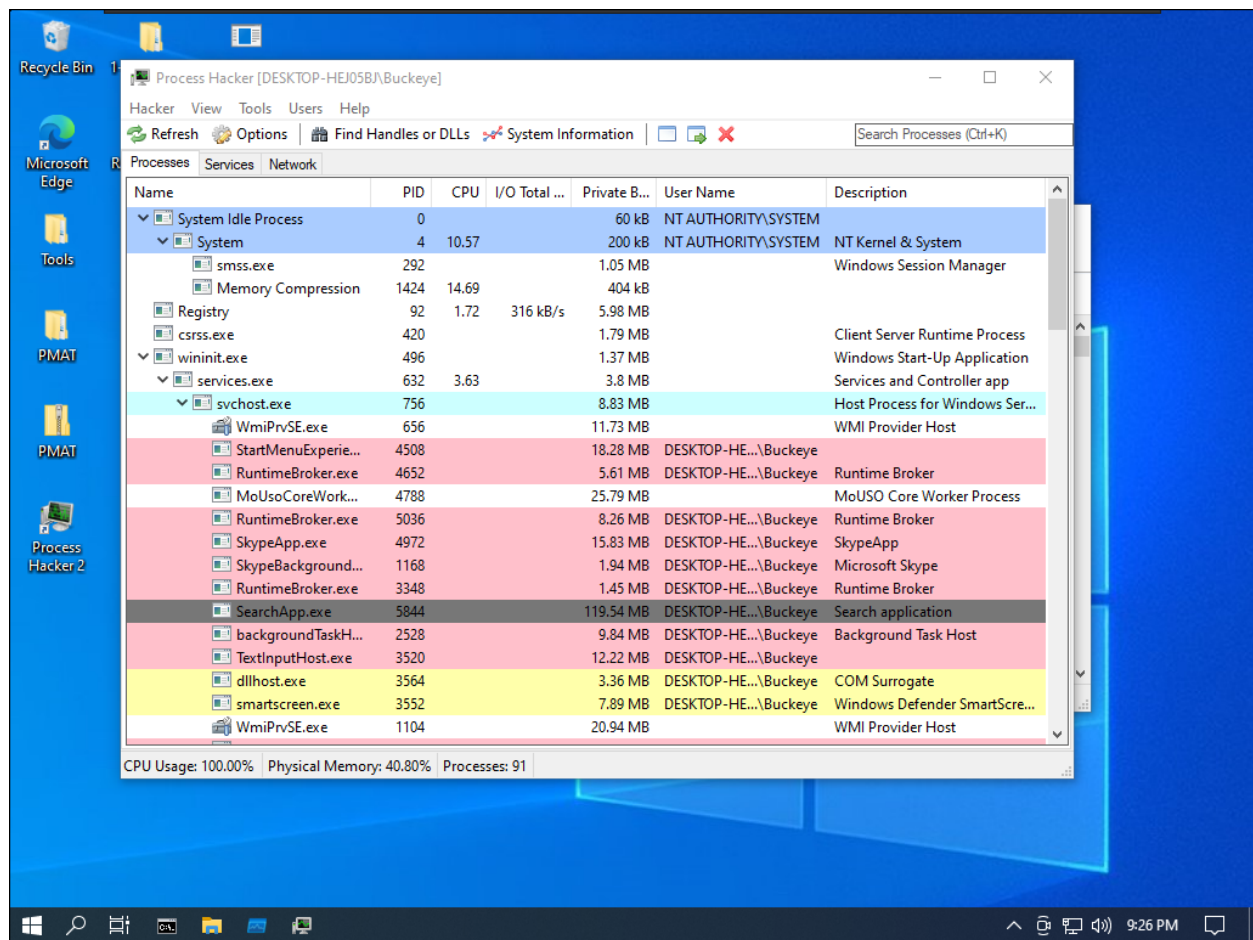
ID: Fa 19/BS DFCS/026

Instructor: Sir Taseer Suleeman

Generate a Procmon-based report. Also write about the details of windows based processes such as explorer.exe, procmon.exe, ntoskrnl.exe.

Process Hacker

Process Hacker is an open-source tool that will allow you to see what processes are running on a device, identify programs that are eating up CPU resources and identify network connections that are associated with a process. These types of features make Process Hacker an ideal tool for monitoring malware on a device.



It runs a process “explorer.exe”

Windows Explorer (Explorer.exe) is the process responsible for starting and displaying most of the user interface (UI), including the desktop, taskbar, Action Center, Start menu, and File Explorer

explorer.exe	1840	5.10		57.8 MB	DESKTOP-HEJ05B\Buckeye	Windows Explorer
SecurityHealthSystray.exe	5068			1.66 MB	DESKTOP-HEJ05B\Buckeye	Windows Security notification...
vmtoolsd.exe	5180	0.24	1.34 kB/s	24.86 MB	DESKTOP-HEJ05B\Buckeye	VMware Tools Core Service
OneDrive.exe	5252			23.11 MB	DESKTOP-HEJ05B\Buckeye	Microsoft OneDrive

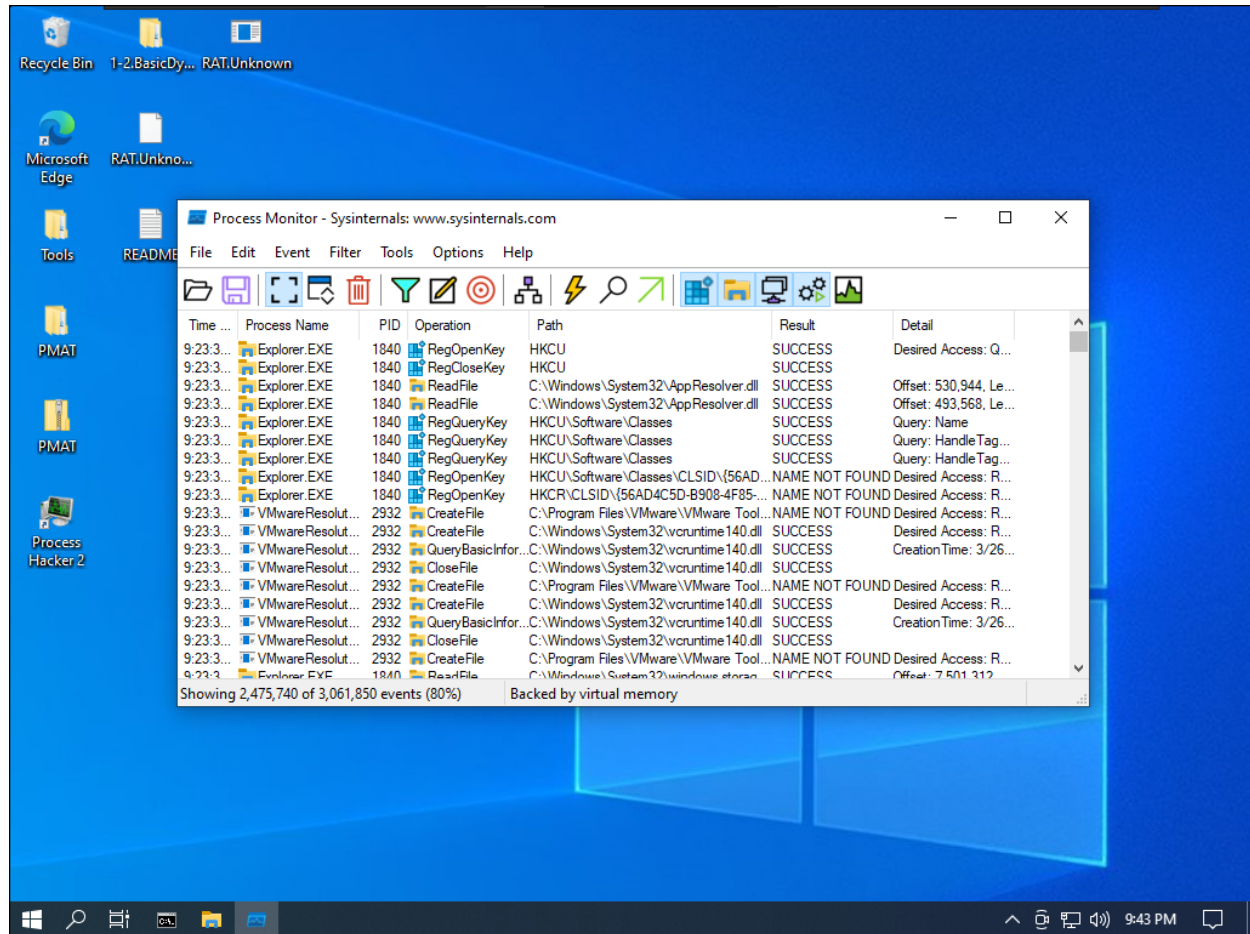
To view dll and threads, we will click on the top “Finds Handles or DLLs”

The screenshot shows the Process Hacker application window. The 'Find Handles or DLLs' window is open, displaying a list of handles for the selected process, explorer.exe (PID 1840). The list is filtered by 'explorer' and shows various registry keys and threads. The CPU usage is 100.00%.

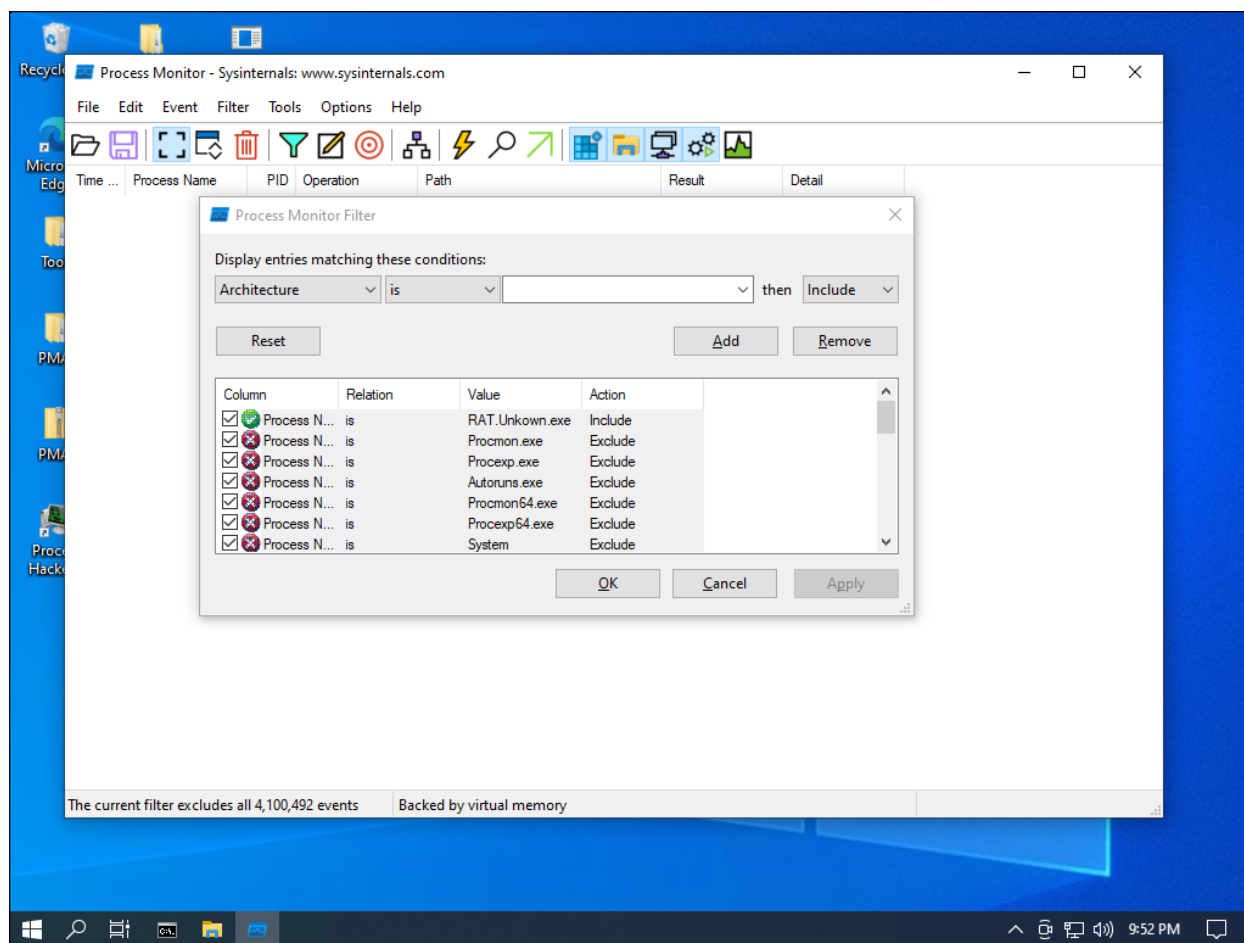
Process	Type	Name	Handle
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Windows\C...	0x734
explorer.exe (1840)	Key	HKU\S-1-5-21-1857795036-1657210213...	0x7a4
explorer.exe (1840)	Thread	explorer.exe (1840): 1968	0x838
explorer.exe (1840)	Key	HKU\S-1-5-21-1857795036-1657210213...	0x854
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Internet Ex...	0x858
explorer.exe (1840)	Key	HKU\S-1-5-21-1857795036-1657210213...	0x85c
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Internet Ex...	0x87c
explorer.exe (1840)	Key	HKU\S-1-5-21-1857795036-1657210213...	0x880
explorer.exe (1840)	Thread	explorer.exe (1840): 2636	0x888
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Windows\C...	0x8a4
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Windows\C...	0x8b4
explorer.exe (1840)	Thread	explorer.exe (1840): 3048	0x8c0
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Windows\C...	0x944
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Windows\C...	0x970
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Windows\C...	0x99c
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Windows\C...	0x9b8
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Windows\C...	0x9bc
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Windows\C...	0x9c4
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Windows\C...	0x9c8
explorer.exe (1840)	Thread	explorer.exe (1840): 2168	0x9dc
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Windows\C...	0x9ec
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Windows\C...	0x9f0
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Windows\C...	0x9f8
explorer.exe (1840)	Key	HKLM\SOFTWARE\Microsoft\Windows\C...	0x9fc

Procmon(Process Monitor)

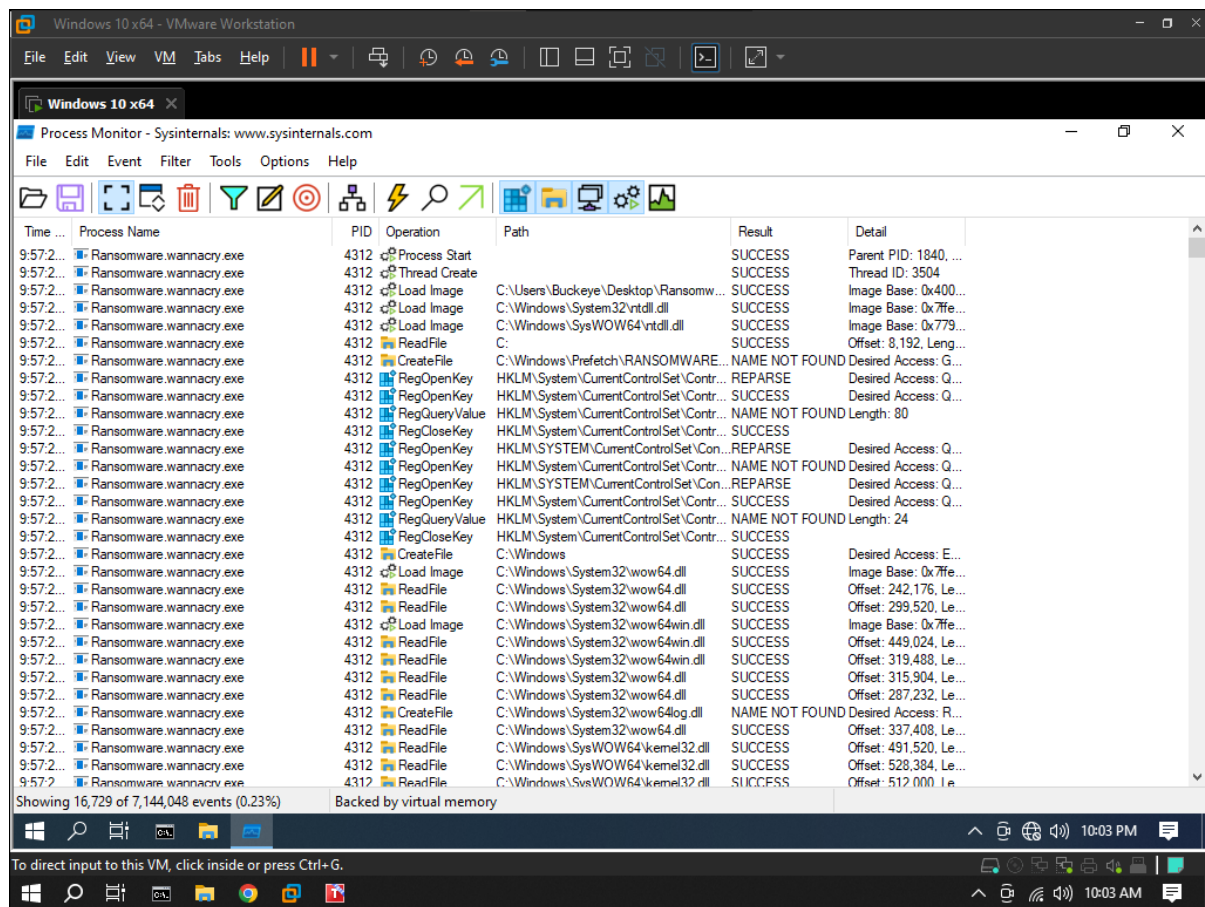
Process Monitor is a tool from Windows Sysinternals, part of the Microsoft TechNet website. The tool monitors and displays in real-time all file system activity on a Microsoft Windows or Unix-like operating system.



It show all process currently running on the system. If we want to check specific malware process then we have to make filer on it and run the process

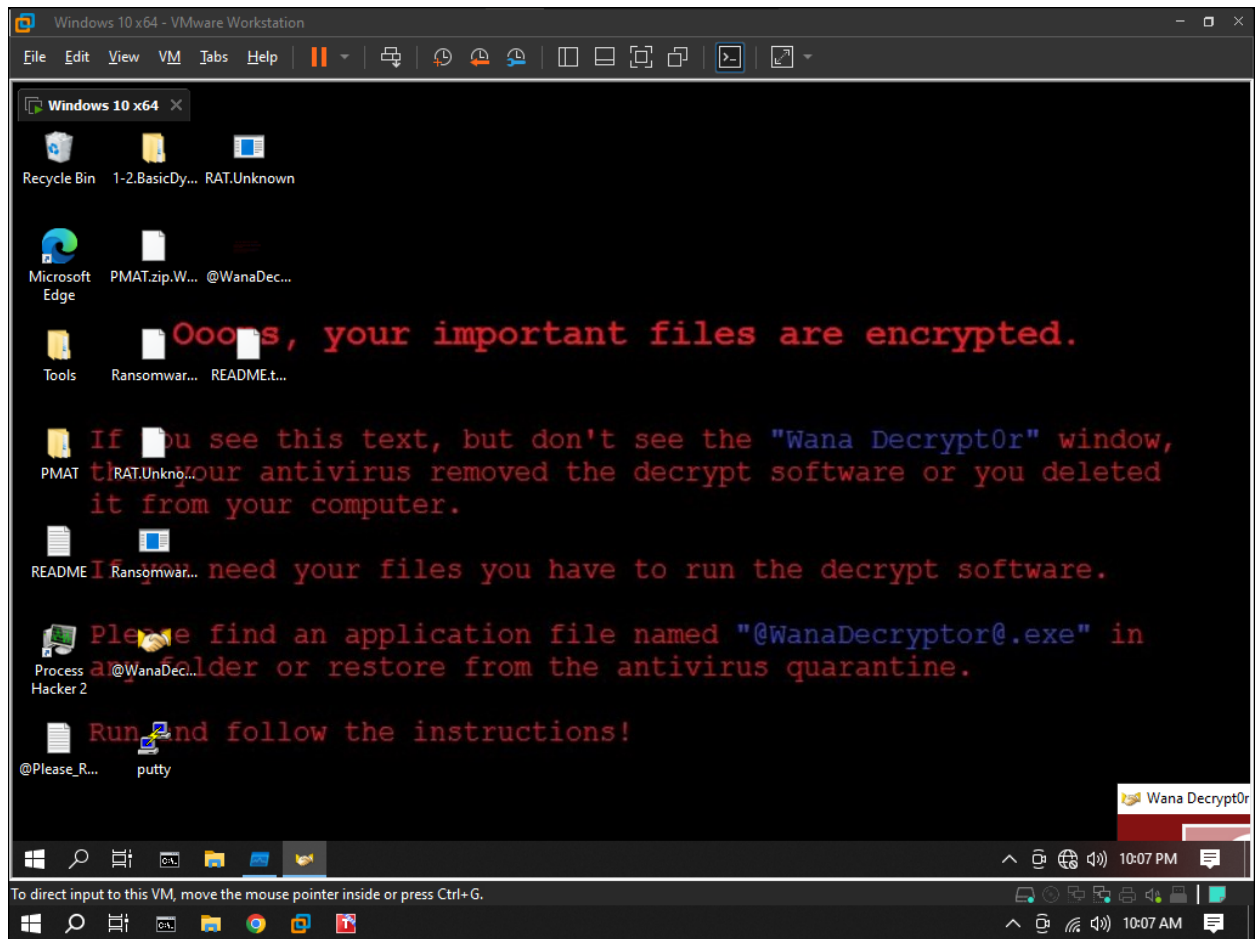


Now Running the one of known malware "Wannacry.exe"



So here are the process load by the WannaCry.exe

Because of not setting the network and domain used by this ransomware, it didn't proceed , as it need to request a domain first but it execute some host based process:



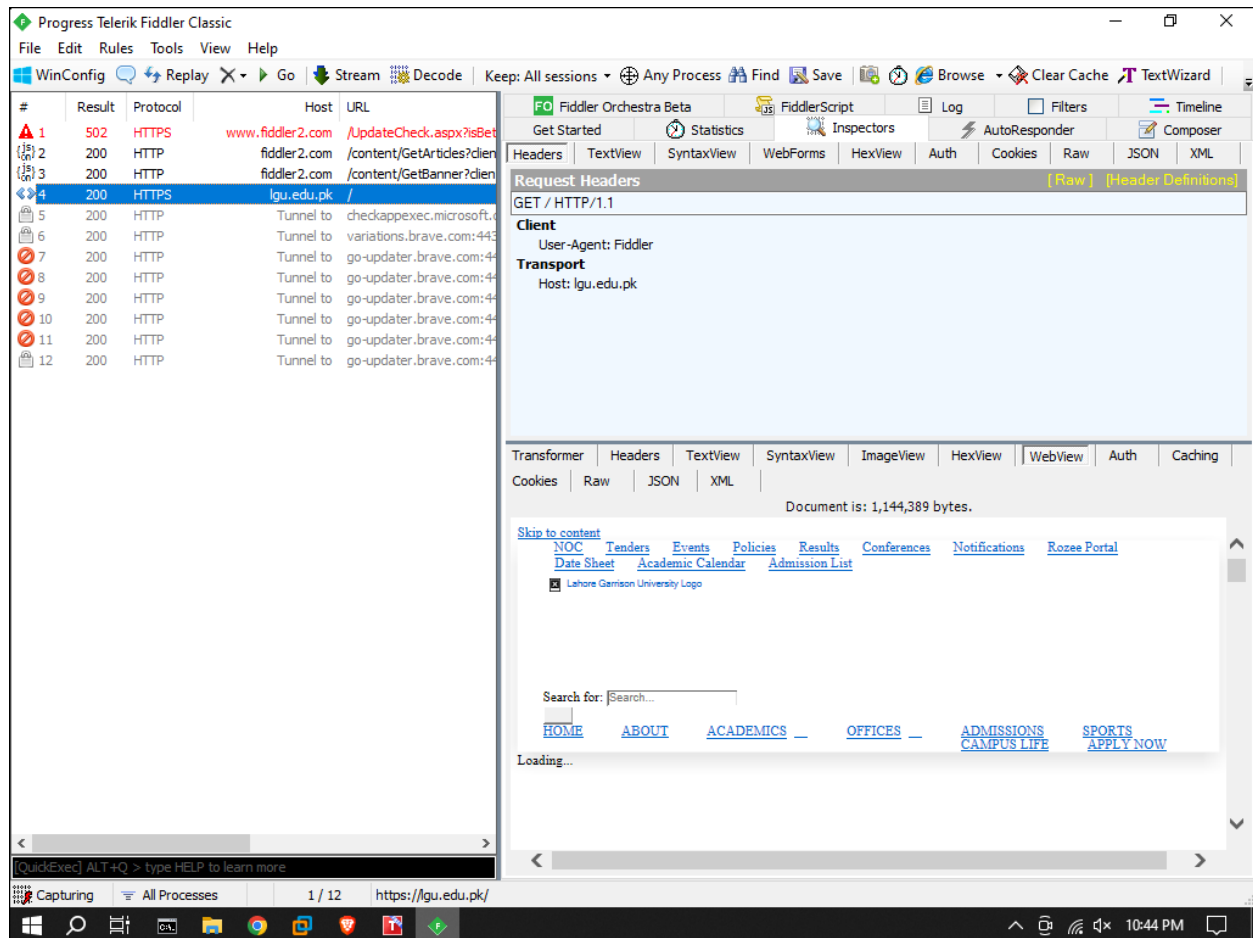


ntoskrnl.exe

ntoskrnl.exe (short for Windows NT operating system kernel executable), also known as the kernel image, contains the kernel and executive layers of the Microsoft Windows NT kernel, and is responsible for hardware abstraction, process handling, and memory management. In addition to the kernel and executive mentioned earlier, it contains the cache manager, security reference monitor, memory manager, scheduler (Dispatcher), and blue screen of death (the prose and portions of the code).

Fiddler

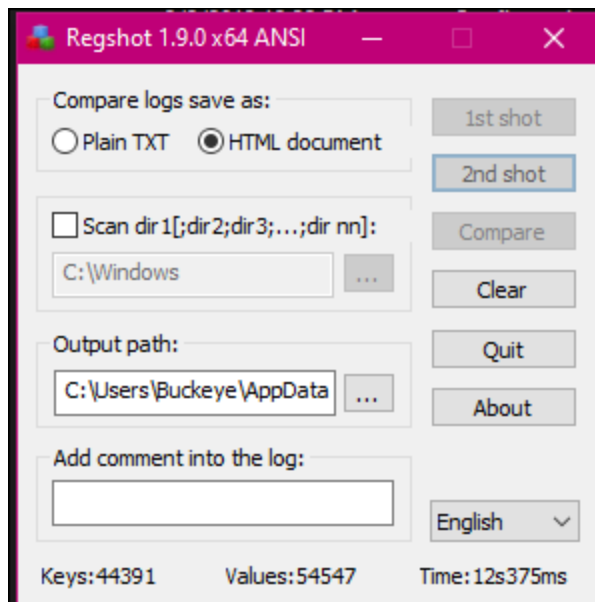
Fiddler is web debugging proxy tool. It allows developers to capture, analyze, and modify HTTP and HTTPS traffic between a client and server. Fiddler is widely used for web development, testing, and troubleshooting purposes. With Fiddler, you can monitor network traffic, inspect and modify requests and responses, simulate various network conditions, and debug web applications. It provides a user-friendly interface that displays the details of each HTTP request and response, including headers, cookies, and content.



RegShot

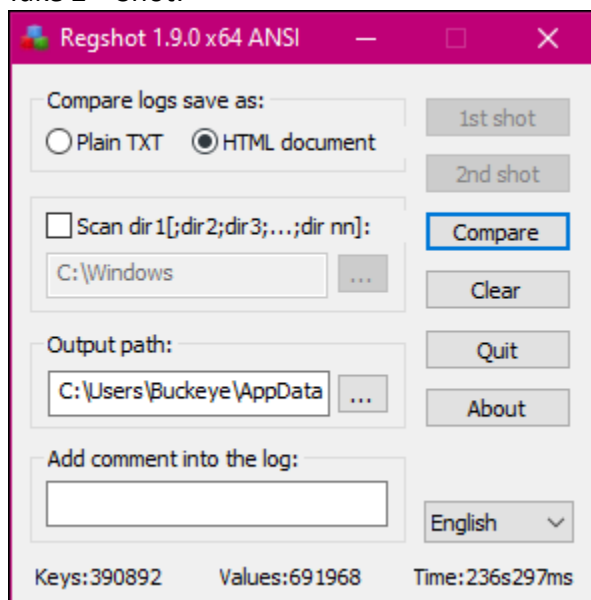
Regshot is a free and open-source utility that helps in comparing the changes made to the Windows registry before and after a specific event or action. It allows you to take snapshots of the registry at different points in time and then compare those snapshots to identify any modifications.

Take 1st Shot:

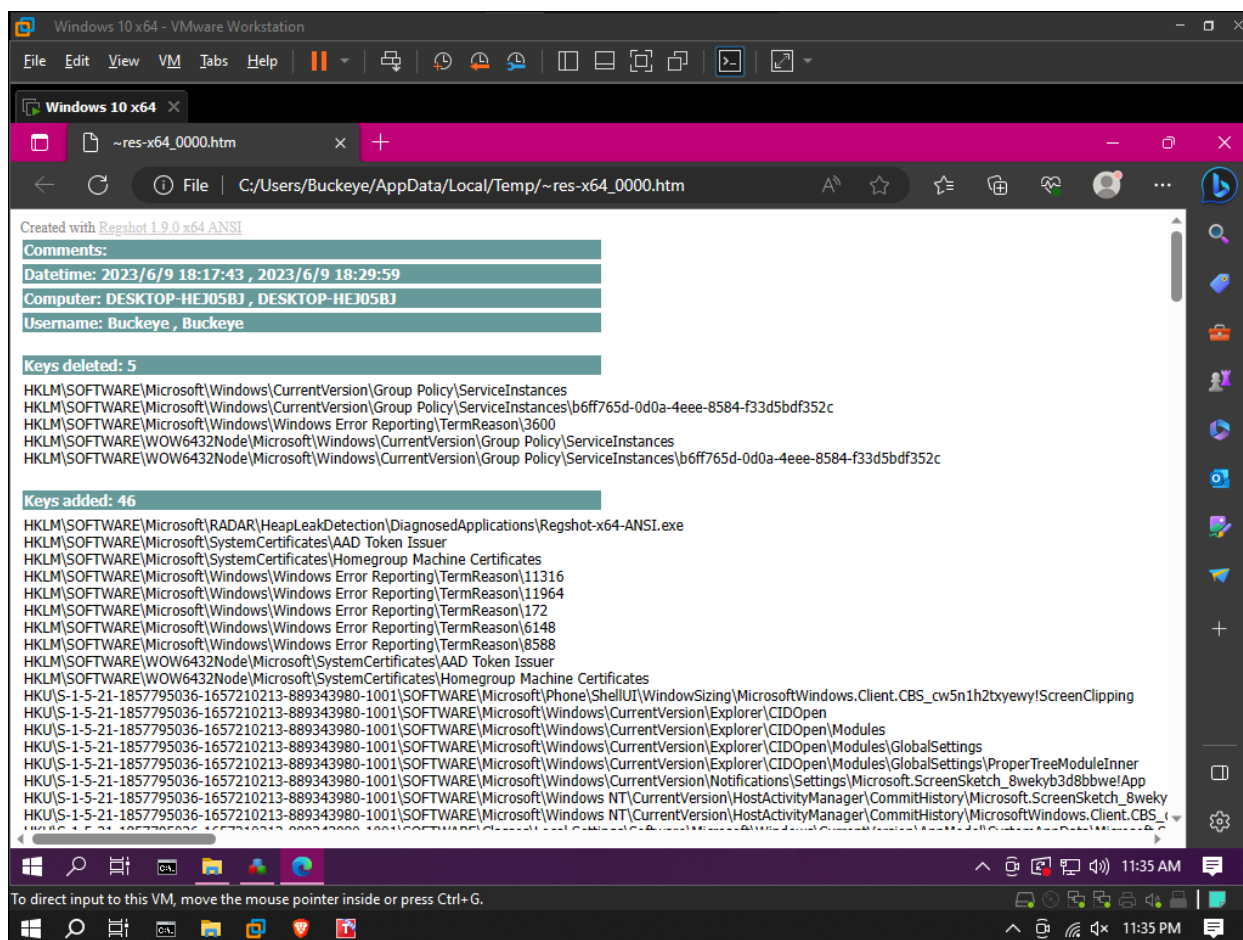
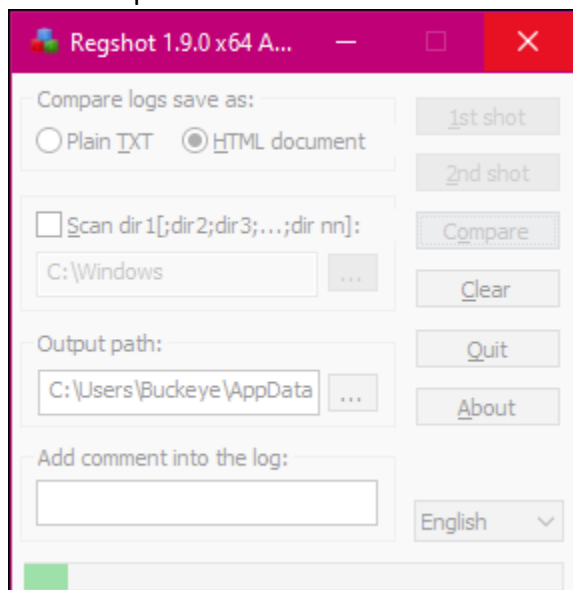


(do some activity / execute Malware)

Take 2nd Shot:

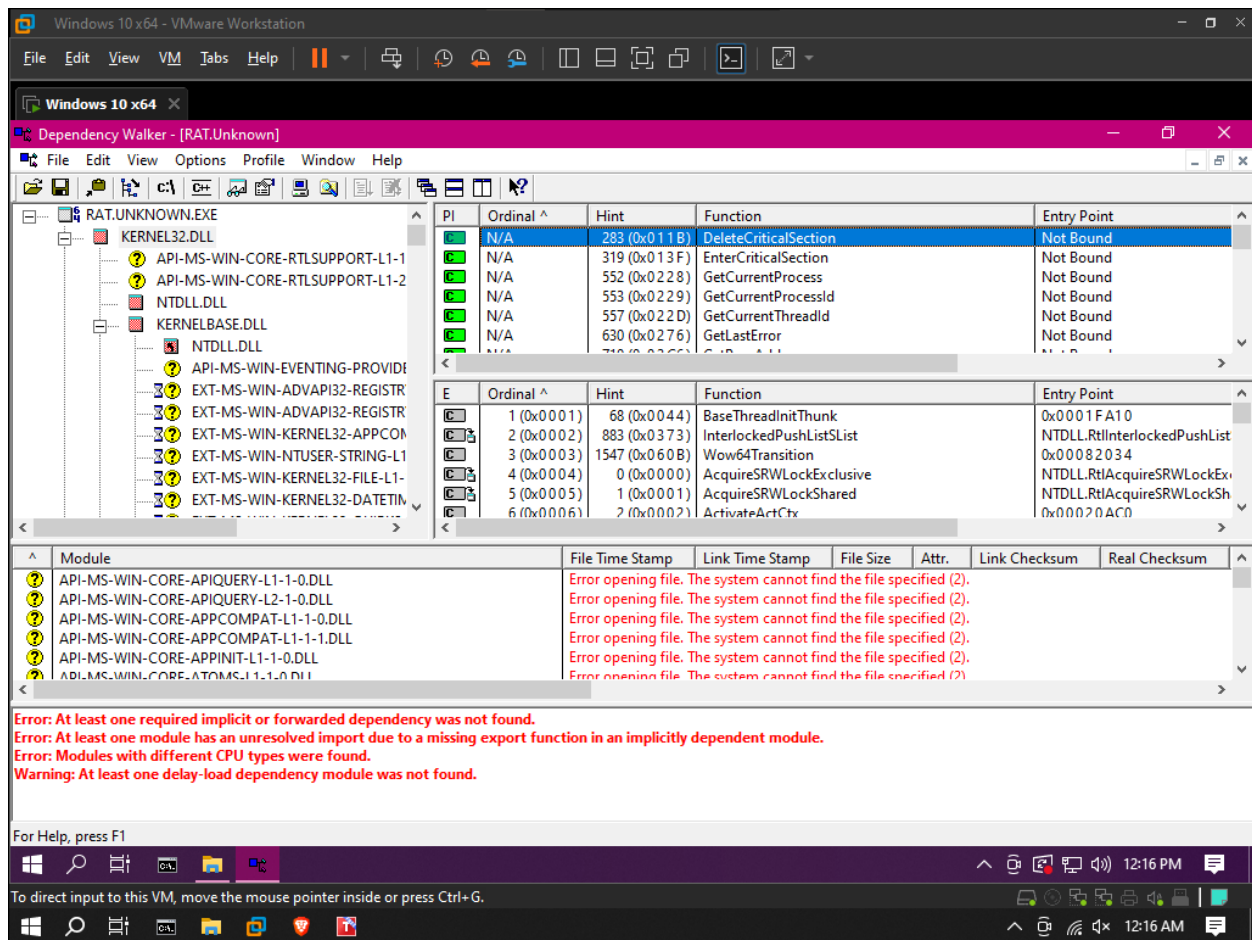


Now Compare:



Dependency Walker

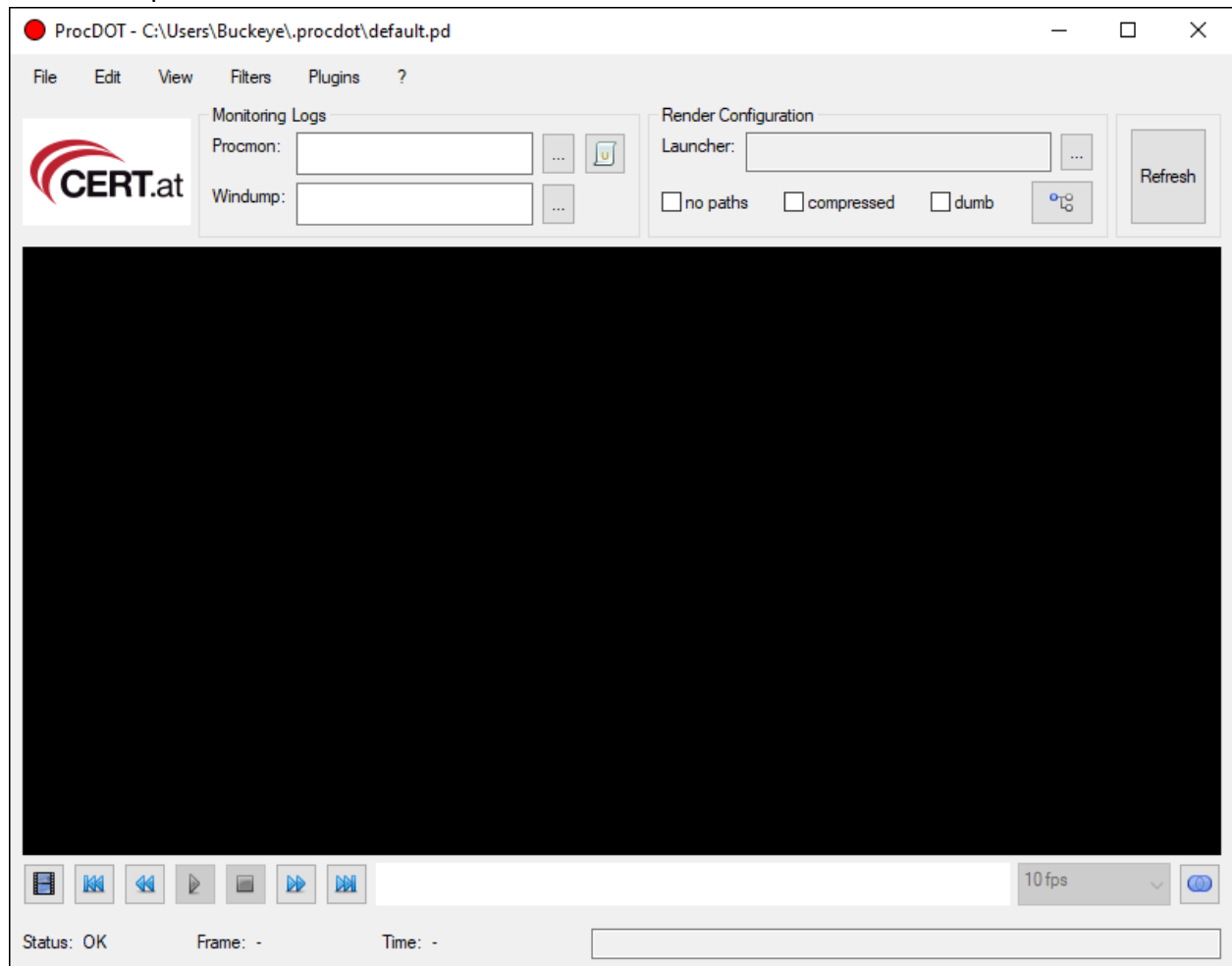
The main purpose of Dependency Walker is to help identify missing or mismatched dependencies that can cause errors or prevent an executable file from running correctly. It can be particularly useful in diagnosing "DLL not found" or "entry point not found" errors.



ProcDot

ProcDOT allows analysts to load Process Monitor log files and provides an interactive graphical representation of the captured events. It can help in understanding the behavior of malicious processes, identifying suspicious activities, and visualizing the relationships between different processes, files, registry keys, and network connections.

First Install procdot



Prerequisites

=====

ProcDOT depends on third party software and therefore needs the following software pre-installed to work properly:

* Graphviz-Suite

Windows: Get the installer and run it.

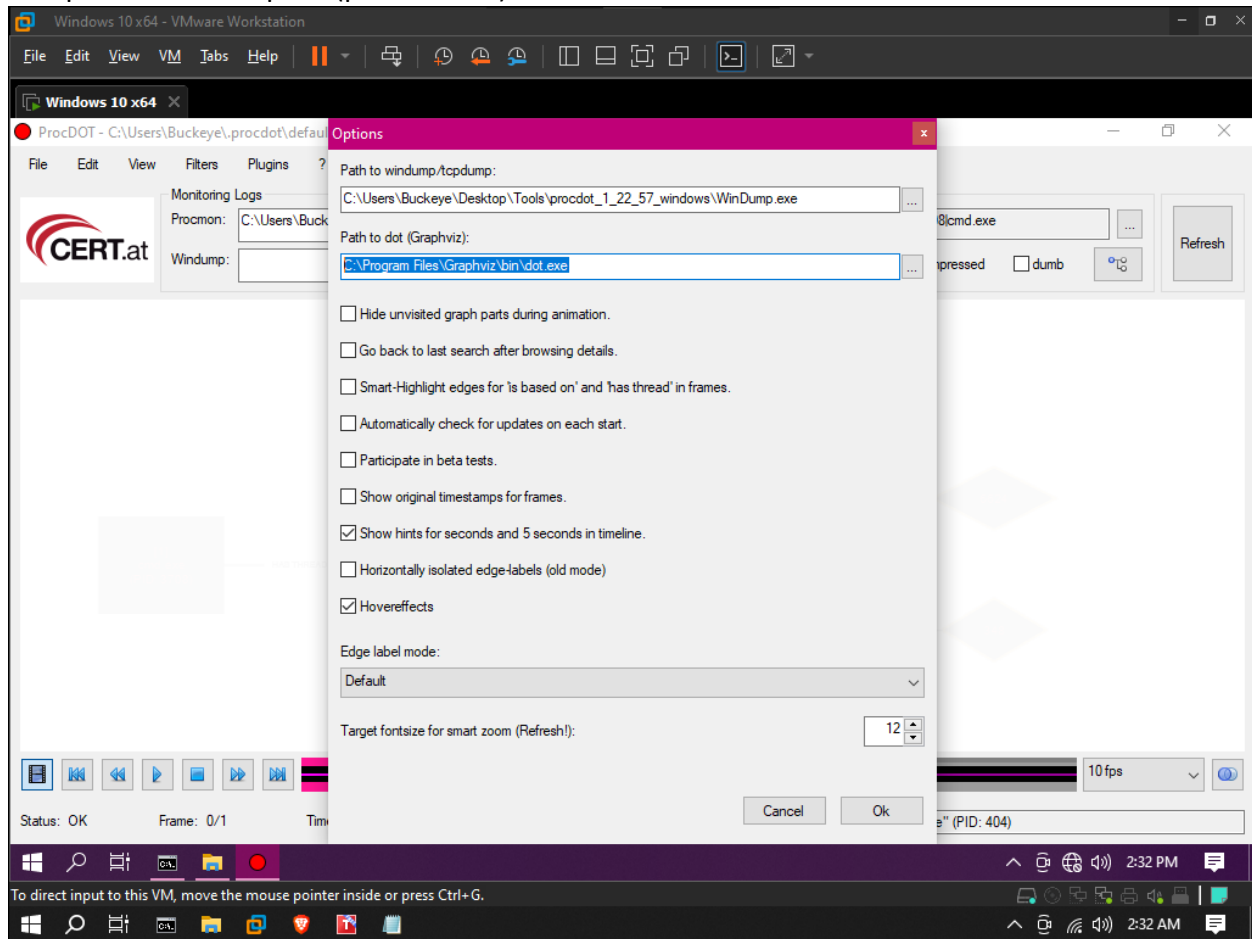
(<http://www.graphviz.org/pub/graphviz/stable/windows/graphviz-2.28.0.msi>)

* Windump/Tcpdump

Windows: Get the executable and put it in any location.

(http://www.winpcap.org/windump/install/bin/windump_3_9_5/WinDump.exe)

Add paths to Edit>Option(prcodot.exe):



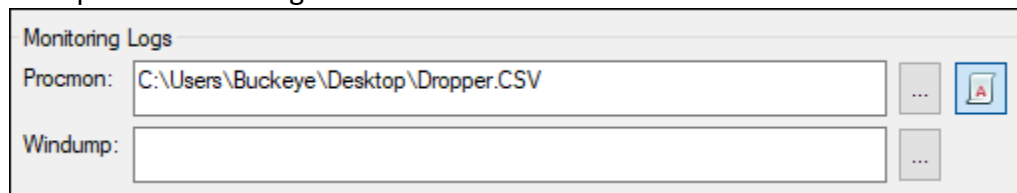
Update Procmon Configuration :

- * disable (uncheck) "Show Resolved Network Addresses" (Options)
- * disable (uncheck) "Enable Advanced Output" (Filter)
- * adjust the displayed columns (Options > Select Columns ...)
 - * to not show the "Sequence" column
 - * to show the "Thread ID" column

Now, Starting Procmon, and Wireshark.

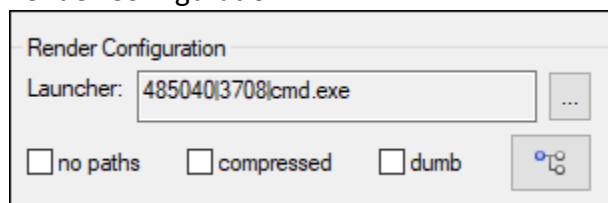
Procmon > clearing logs >	> save log > .CSV format
[execute malware]	
Wireshark > start capturing >	> save log > .TXT format

Start procdot > add log file



The 'Monitoring Logs' dialog box contains two text input fields. The first field, labeled 'Procmon:', contains the path 'C:\Users\Buckeye\Desktop\Dropper.CSV'. To its right is a button with three dots and a file icon. The second field, labeled 'Windump:', is empty. To its right is a button with three dots.

Render Configuration:



The 'Render Configuration' dialog box features a 'Launcher:' label followed by a text box containing '485040|3708|cmd.exe' and a button with three dots. Below this are three checkboxes labeled 'no paths', 'compressed', and 'dumb', all of which are currently unchecked. To the right of these checkboxes is a button with a circular arrow icon.

Refresh:


Windows 10 x64 - VMware Workstation

File Edit View VM Tabs Help

Windows 10 x64

ProcDOT - C:\Users\Buckeye\procdot\default.pd*

File Edit View Filters Plugins ?

 Monitoring Logs

Procmon: C:\Users\Buckeye\Desktop\Dropper.CSV

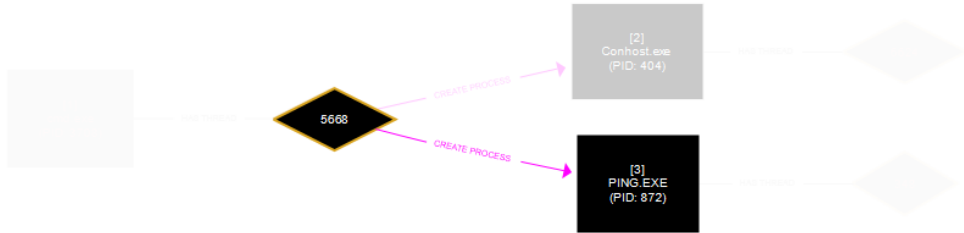
Windump:

Render Configuration

Launcher: 485040\3708\cmd.exe

☐ no paths ☐ compressed ☐ dumb

Refresh



Status: OK Frame: 1/1 Time: 00:00:02.7573189 Thread 5668-n2 of process "cmd.exe" (PID: 3708) creates process "PING.EXE" (PID: 872)

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

2:46 PM 2:46 AM