**Assignment**

**Name:** Hassan Ahmed

**Class:** BS DFCS

**Section:** A

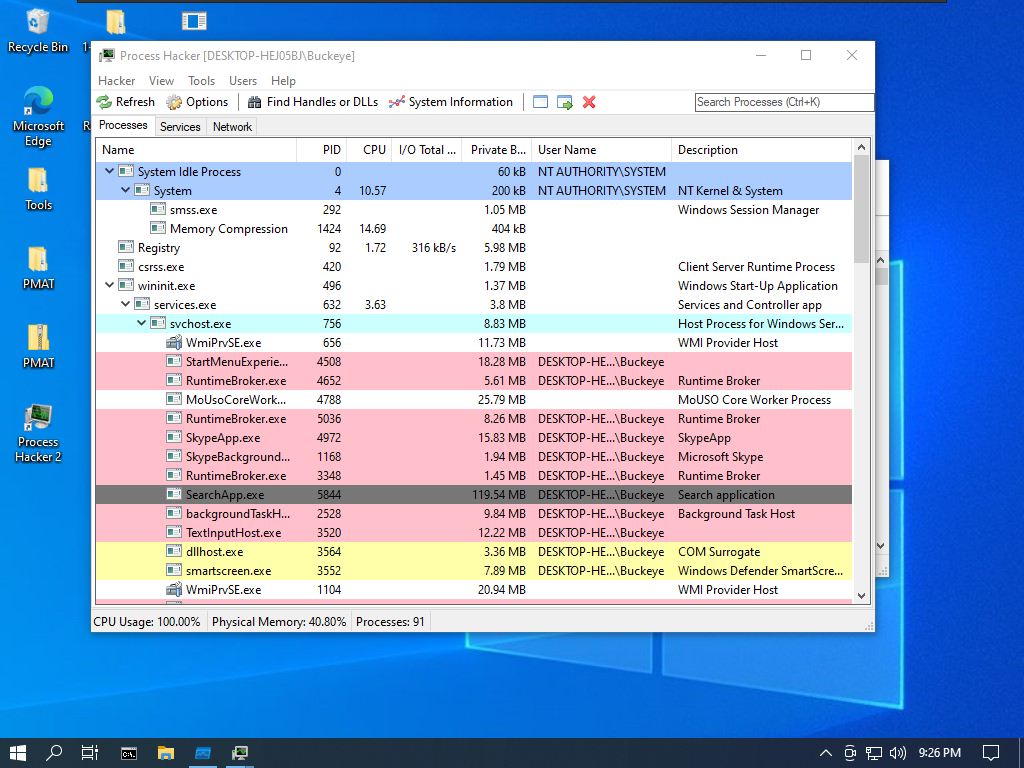
**ID:** Fa 19/BS DFCS/026

**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.

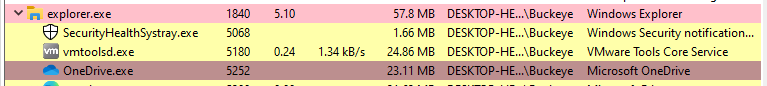
**Process Hacker**

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.

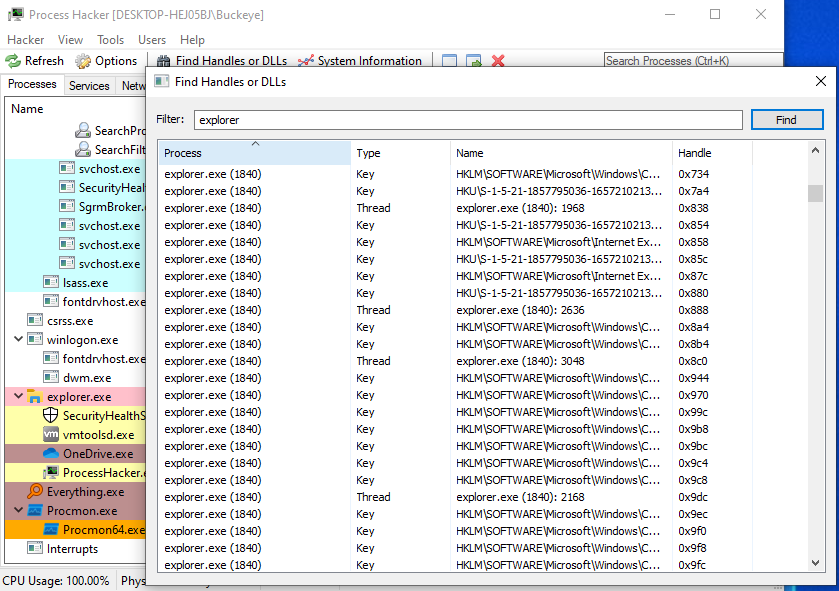


It runs a process “explorer.exe”

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

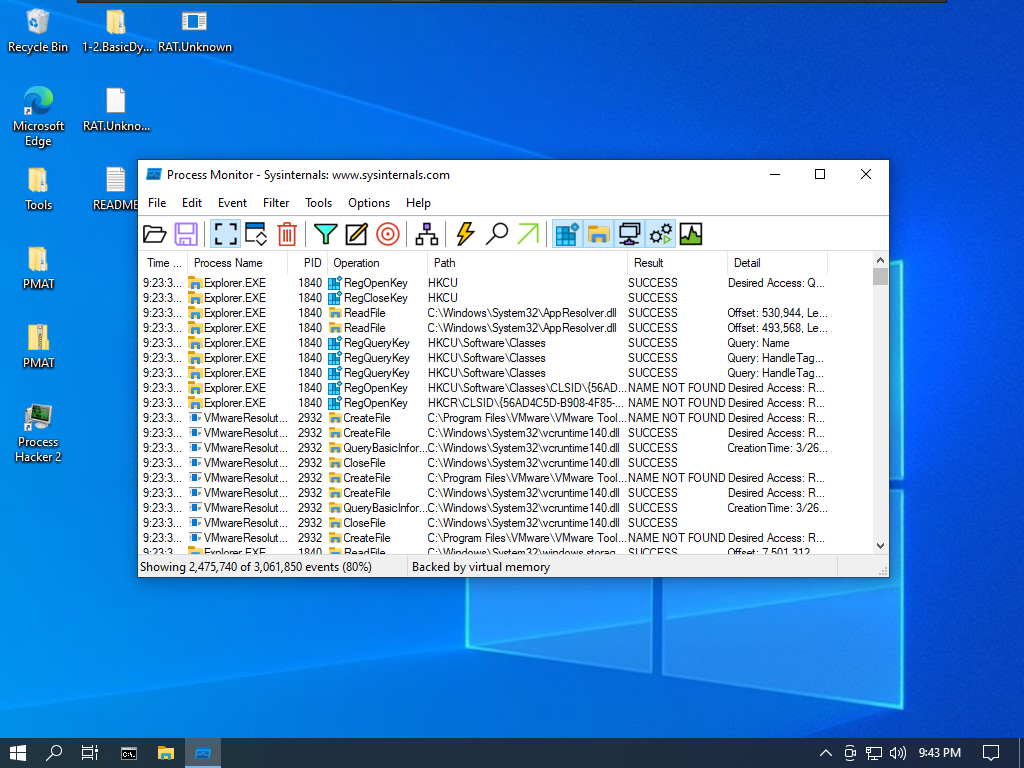


To view dll and threads, we will click on the top “Finds Handles or DLLs”

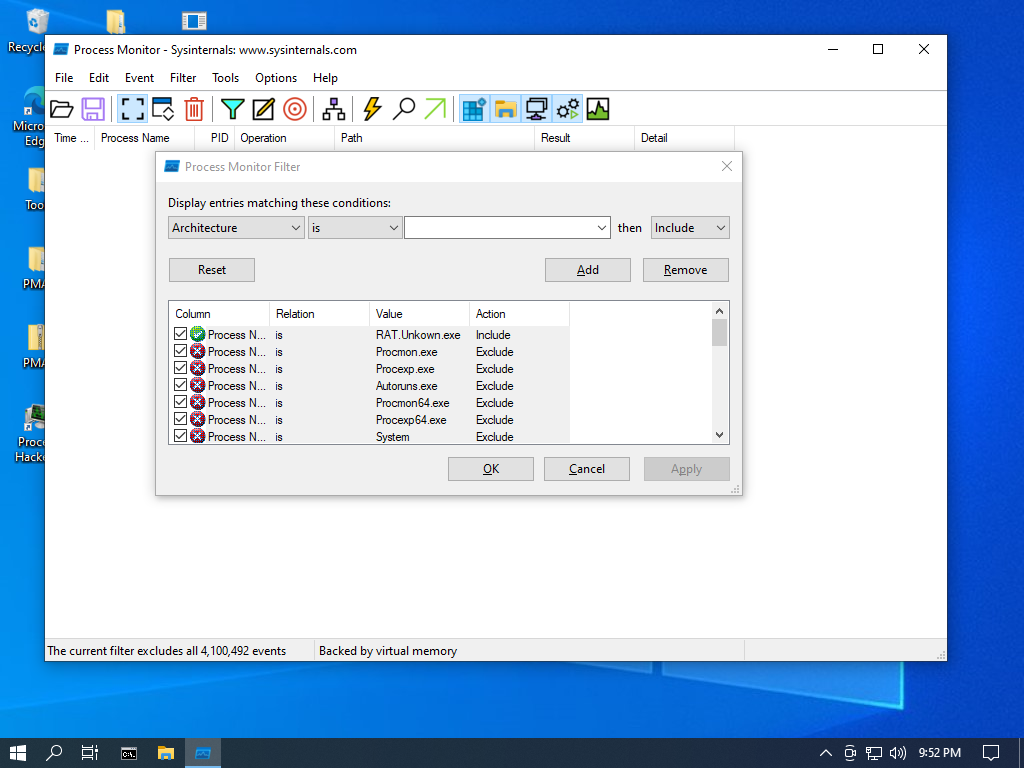


**Procmon(Process Monitor)**

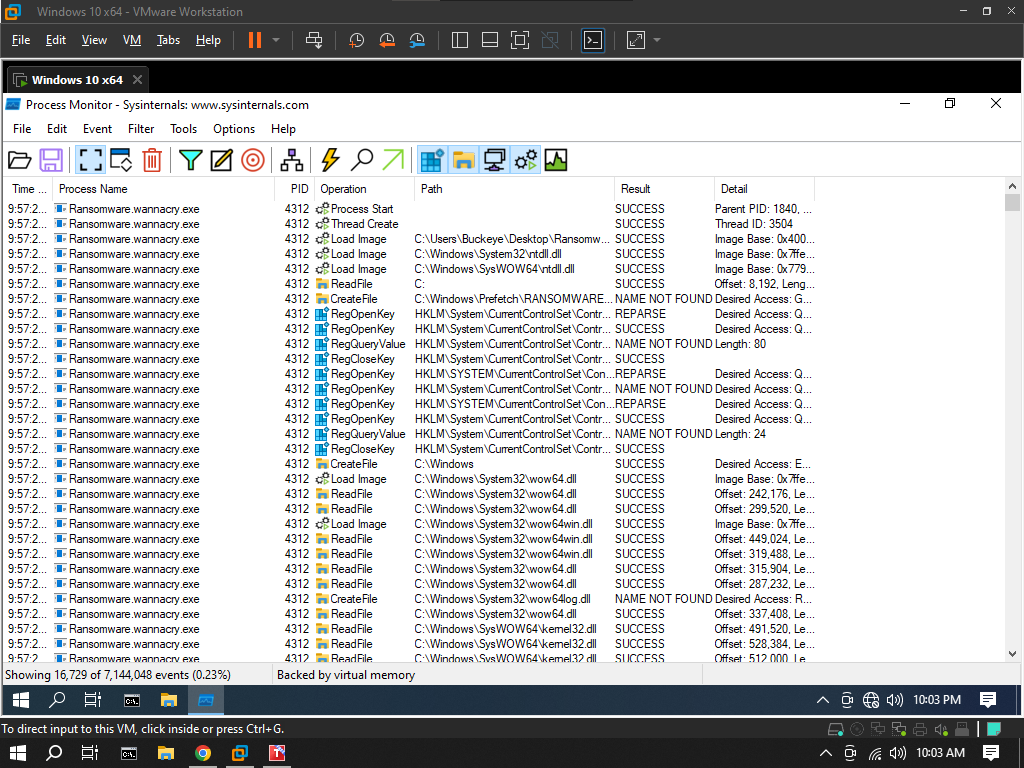
Process Monitor is a tool from Windows Sysinternals, part of the Microsoft TechNet website. The tool monitors and displays in real-time all file system activity on a Microsoft Windows or Unix-like operating system.



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

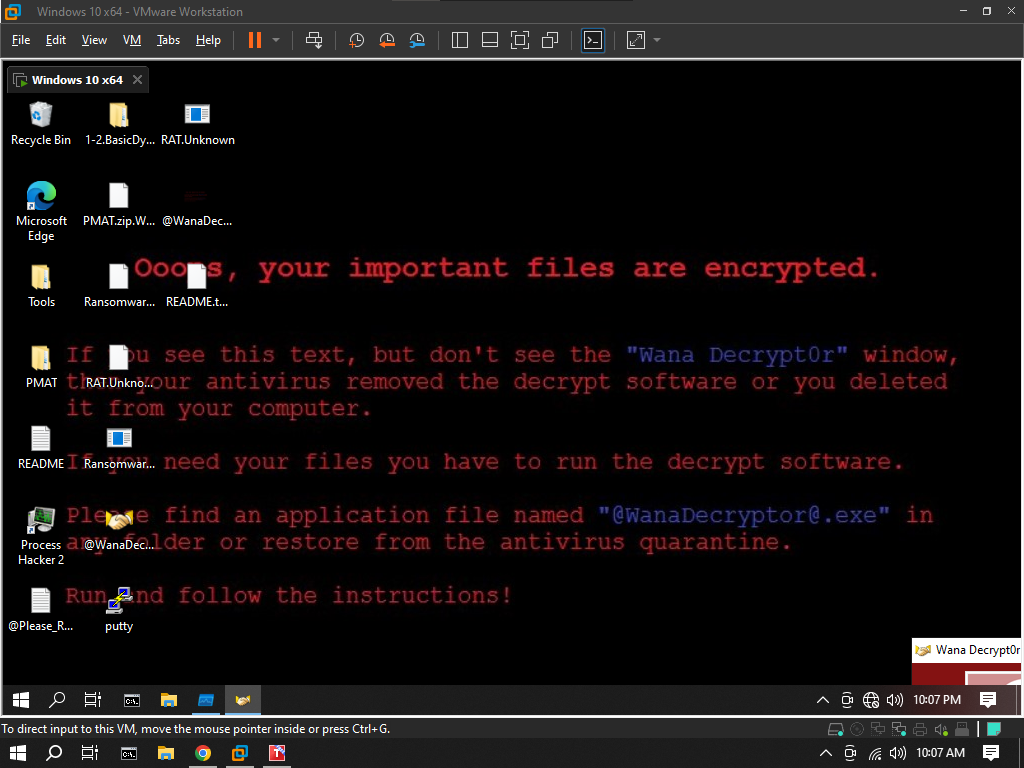


Now Running the one of known malware “Wannacry.exe”



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:





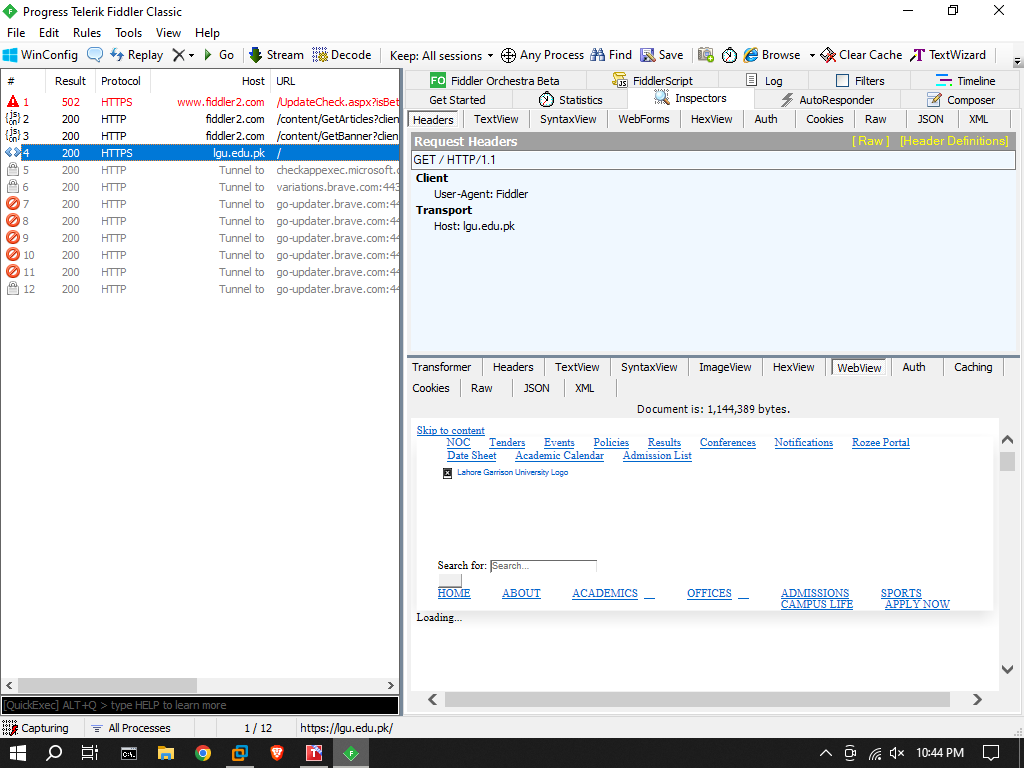
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**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**

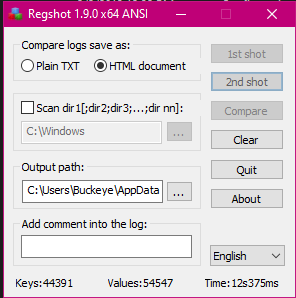
Fiddler is web debugging proxy tool. It allows developers to capture, analyze, and modify HTTP and HTTPS traffic between a client and server. Fiddler is widely used for web development, testing, and troubleshooting purposes. With Fiddler, you can monitor network traffic, inspect and modify requests and 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**

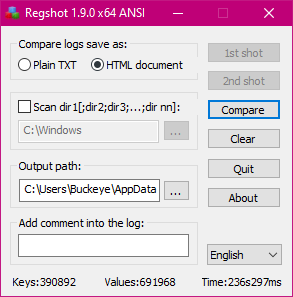
Regshot is a free and open-source utility that helps in comparing the changes made to the Windows registry before and after a specific event or action. It allows you to take snapshots of the registry at different points in time and then compare those snapshots to identify any modifications.

Take 1st Shot:

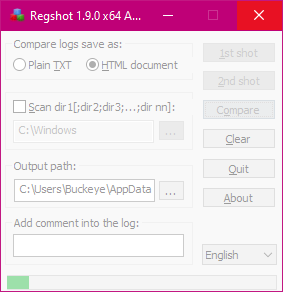


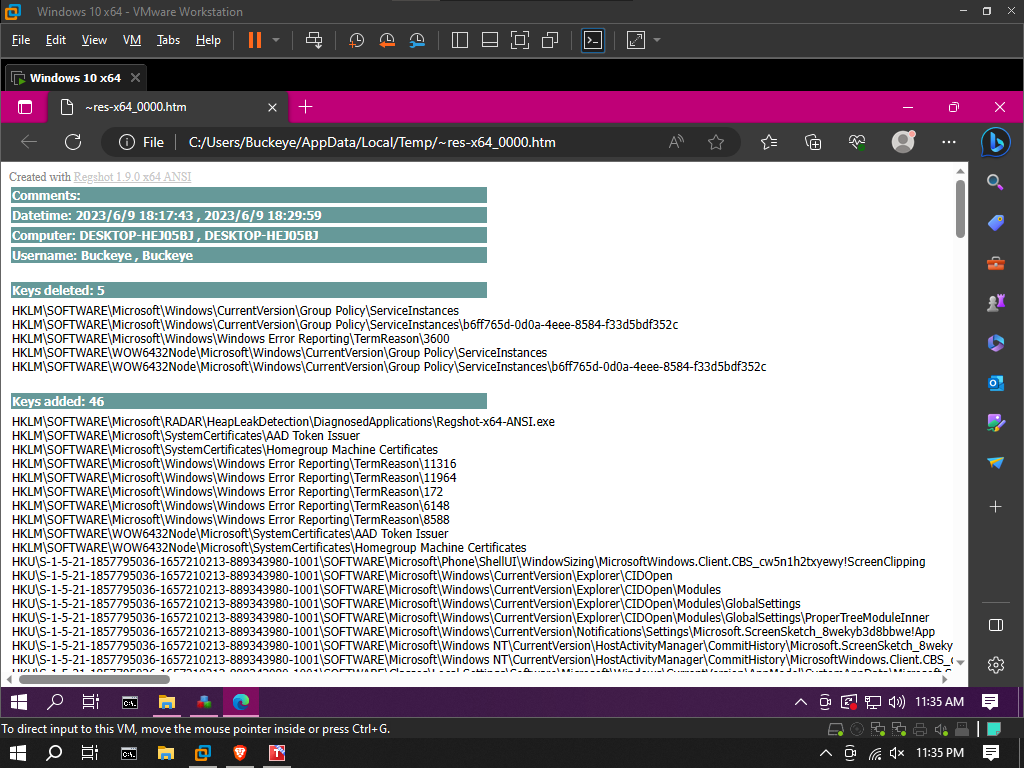
(do some activity / execute Malware)

Take 2nd Shot:



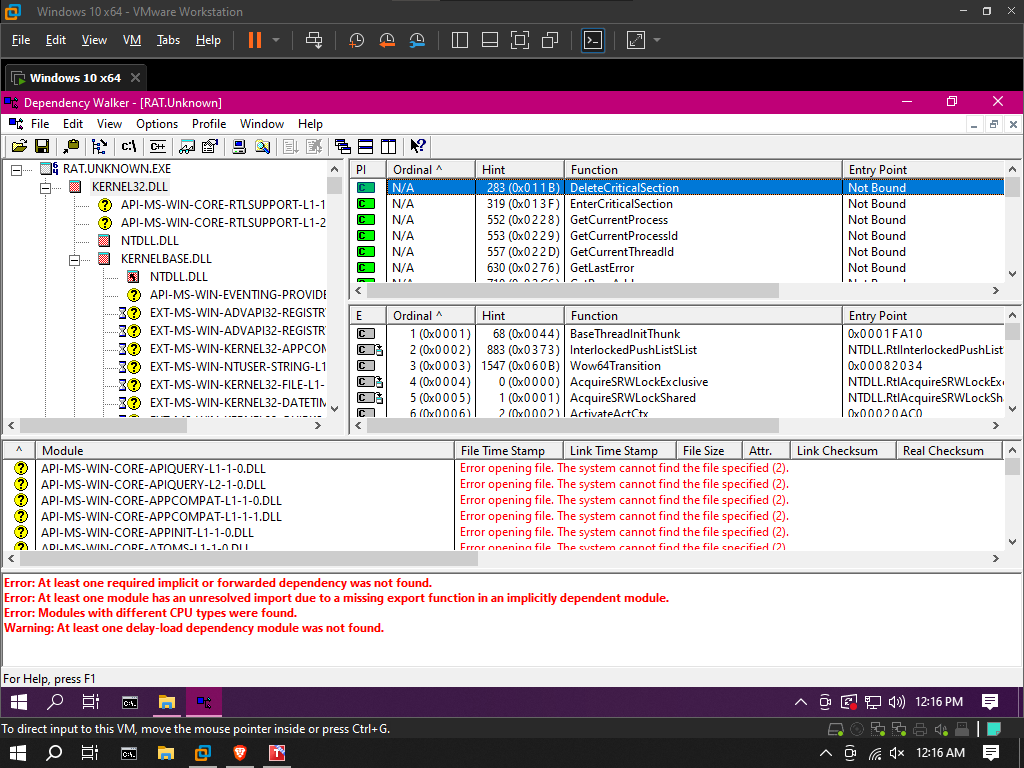
Now Compare:





**Dependency Walker**

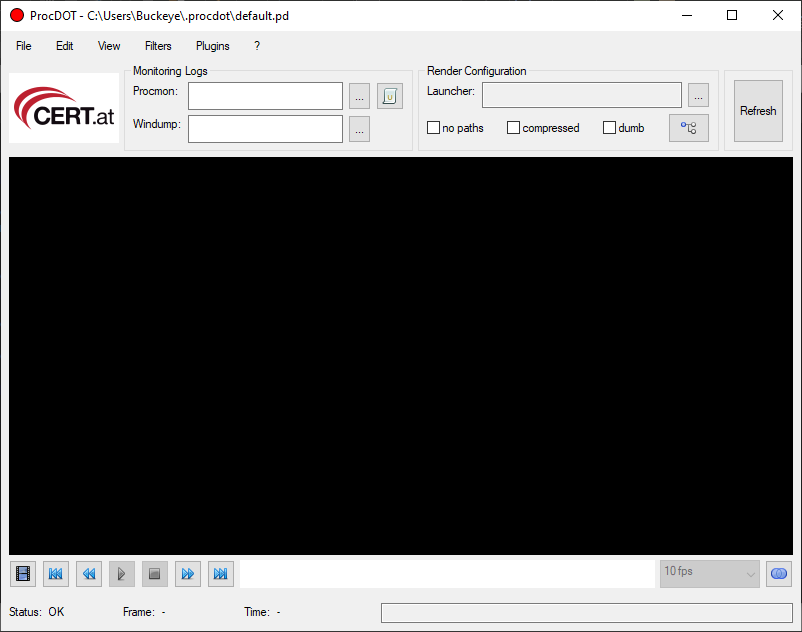
The main purpose of Dependency Walker is to help identify missing or mismatched dependencies that can cause errors or prevent an executable file from running correctly. It can be particularly useful in diagnosing "DLL not found" or "entry point not found" errors.



**ProcDot**

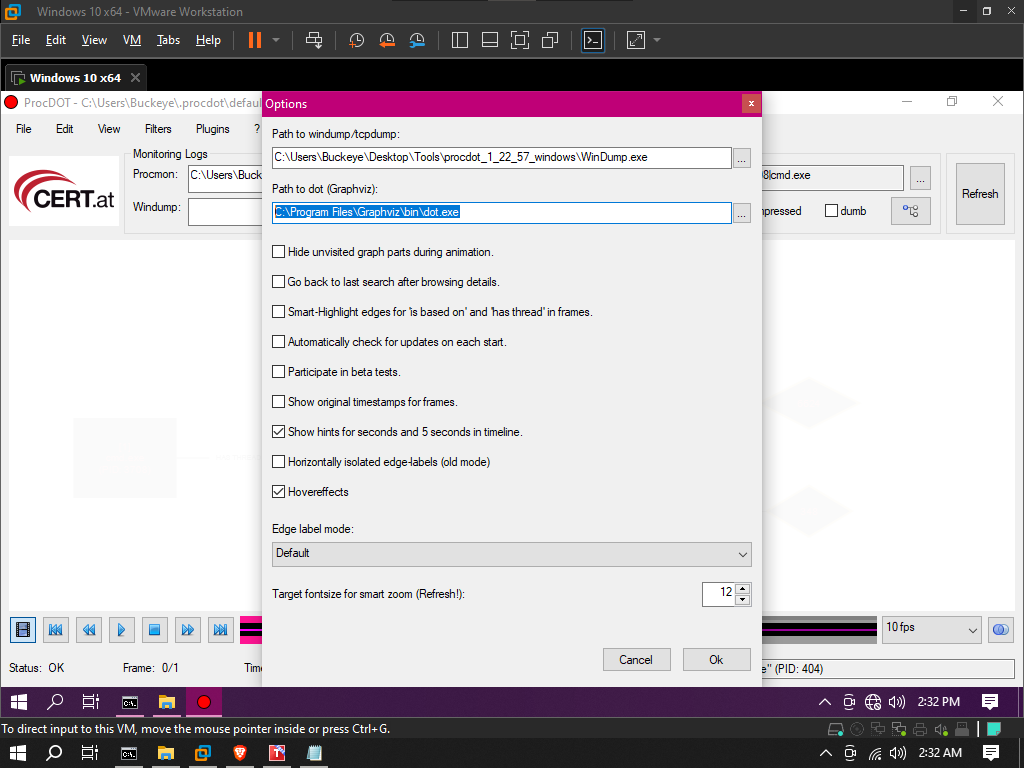
ProcDOT allows analysts to load Process Monitor log files and provides an interactive graphical representation of the captured events. It can help in understanding the behavior of malicious processes, identifying suspicious activities, and visualizing the relationships between different processes, files,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



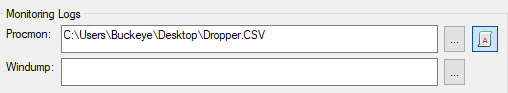
Update Procmon Configuration :

| \* 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 |
| --- |

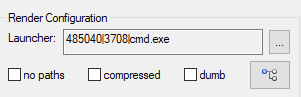
Now, Starting Procmon, and Wireshark.

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

Start procdot > add log file



Render Configuration:



Refresh:

