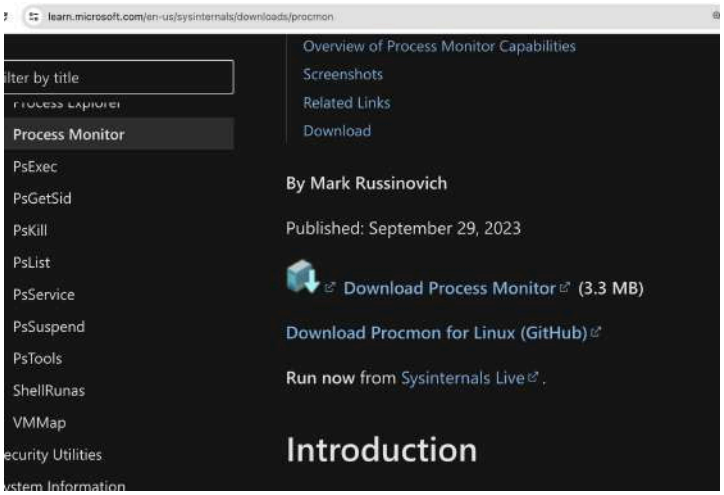
In Enterprise and Infrastructure Module => Launch the Labs

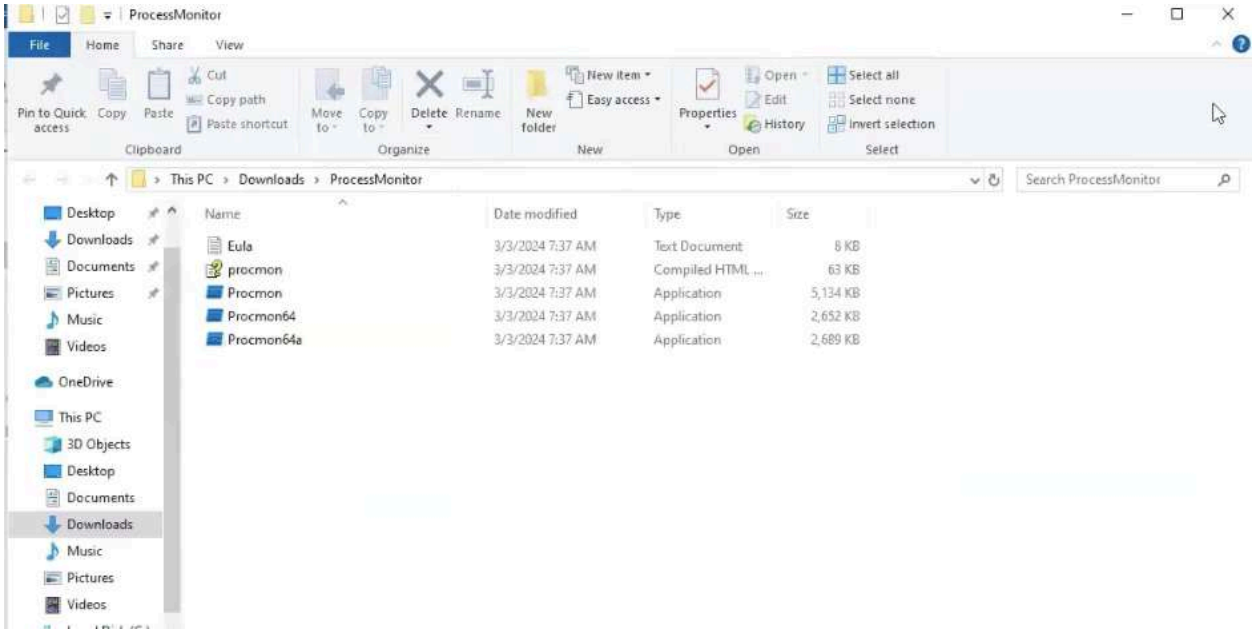
Step 1: Windows 10 PC and ensure you have already turned off the Virus Protection Settings and ensure the download folder is already excluded in Virus Protection Settings

Step 2:
Download the following tools in Windows 10 Machine

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

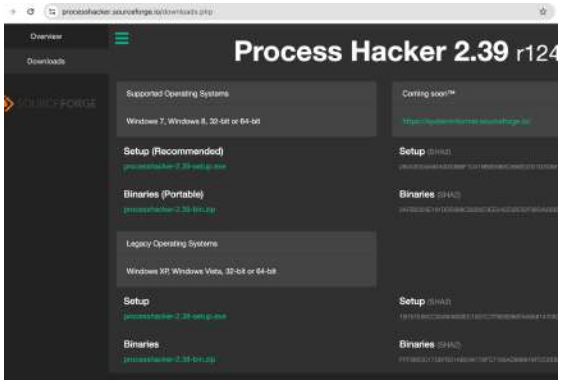
1. Just extract this folder of ZIP file [We are ready to use Process Monitor 64 Bit]





Process Hacker:
https://sourceforge.net/projects/processhacker/files/processhacker2/processhacker-2.39-setup.exe/download

2. Now install the Process Hacker tool in Windows 10 with just NEXT steps



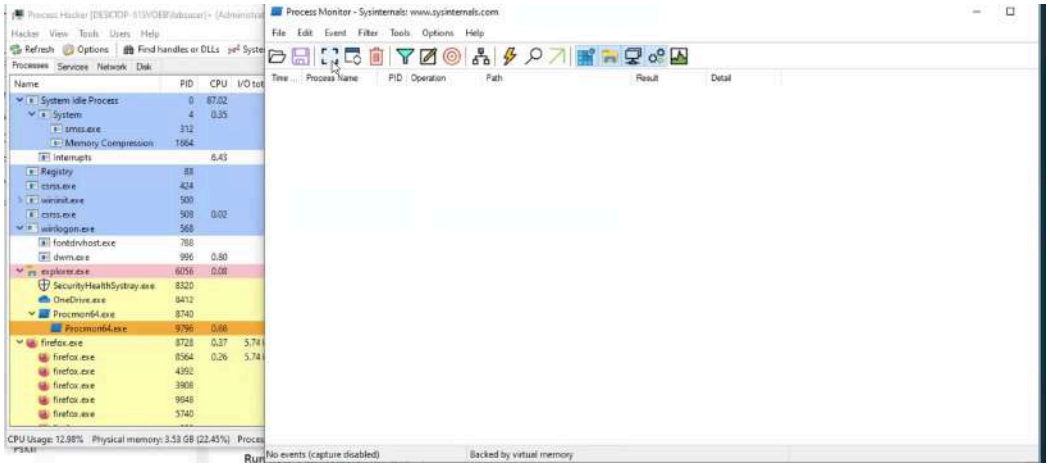
Step 3:

3. Generate the Screensaver.exe malware and keep it ready in Windows 10 PC [Do NOT Run now at this step but just keep it ready]
4. Go to your Kali Linux and open the Terminal and launch the msfconsole and set the payloads and just run the exploit step in msfconsole [You should refer previous lab document which is provided to reach this step]

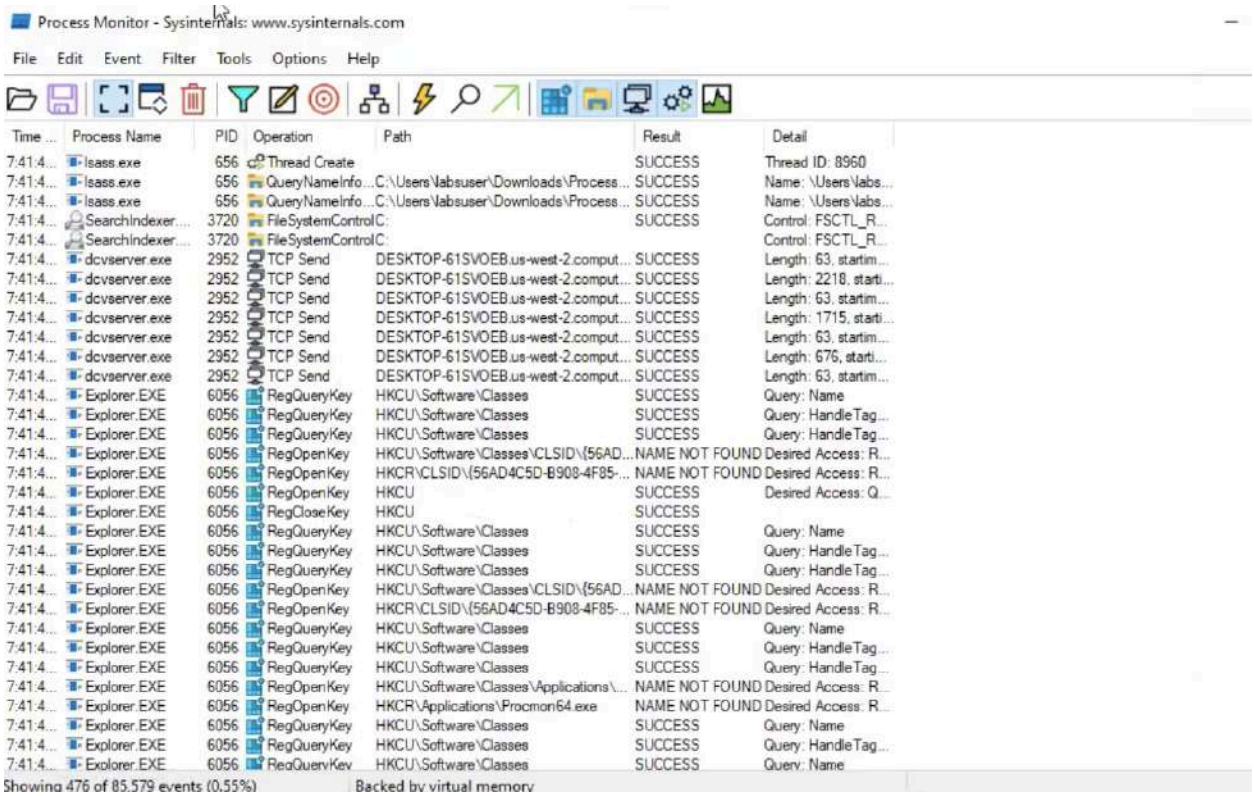
```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 172.31.34.220:4444
```

5. Now Go to Windows 10 Machine and ensure the following Process Hacker and Process Monitor tools are run or open this tools
6. In Process Monitor Click the Capture button to stop the event collection and Delete button to clear the already captured events from screen.



7. Again In Process Monitor Click the Capture button to start collecting the events freshly.



Time ...	Process Name	PID	Operation	Path	Result	Detail
7:41:4...	lsass.exe	656	Thread Create		SUCCESS	Thread ID: 8960
7:41:4...	lsass.exe	656	QueryNameInfo...	C:\Users\labsuser\Downloads\Process...	SUCCESS	Name: \Users\labs...
7:41:4...	lsass.exe	656	QueryNameInfo...	C:\Users\labsuser\Downloads\Process...	SUCCESS	Name: \Users\labs...
7:41:4...	SearchIndexer....	3720	FileSystemControl	C:	SUCCESS	Control: FSCTL_R...
7:41:4...	SearchIndexer....	3720	FileSystemControl	C:		Control: FSCTL_R...
7:41:4...	dcvserver.exe	2952	TCP Send	DESKTOP-61SVOEB.us-west-2.comput...	SUCCESS	Length: 63, startim...
7:41:4...	dcvserver.exe	2952	TCP Send	DESKTOP-61SVOEB.us-west-2.comput...	SUCCESS	Length: 2218, starti...
7:41:4...	dcvserver.exe	2952	TCP Send	DESKTOP-61SVOEB.us-west-2.comput...	SUCCESS	Length: 63, startim...
7:41:4...	dcvserver.exe	2952	TCP Send	DESKTOP-61SVOEB.us-west-2.comput...	SUCCESS	Length: 1715, starti...
7:41:4...	dcvserver.exe	2952	TCP Send	DESKTOP-61SVOEB.us-west-2.comput...	SUCCESS	Length: 63, startim...
7:41:4...	dcvserver.exe	2952	TCP Send	DESKTOP-61SVOEB.us-west-2.comput...	SUCCESS	Length: 676, starti...
7:41:4...	dcvserver.exe	2952	TCP Send	DESKTOP-61SVOEB.us-west-2.comput...	SUCCESS	Length: 63, startim...
7:41:4...	Explorer.EXE	6056	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
7:41:4...	Explorer.EXE	6056	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
7:41:4...	Explorer.EXE	6056	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
7:41:4...	Explorer.EXE	6056	RegOpenKey	HKCU\Software\Classes\CLSID\{56AD...	NAME NOT FOUND	Desired Access: R...
7:41:4...	Explorer.EXE	6056	RegOpenKey	HKCR\CLSID\{56AD4C5D-B908-4F85-...	NAME NOT FOUND	Desired Access: R...
7:41:4...	Explorer.EXE	6056	RegOpenKey	HKCU	SUCCESS	Desired Access: Q...
7:41:4...	Explorer.EXE	6056	RegCloseKey	HKCU	SUCCESS	
7:41:4...	Explorer.EXE	6056	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
7:41:4...	Explorer.EXE	6056	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
7:41:4...	Explorer.EXE	6056	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
7:41:4...	Explorer.EXE	6056	RegOpenKey	HKCU\Software\Classes\CLSID\{56AD...	NAME NOT FOUND	Desired Access: R...
7:41:4...	Explorer.EXE	6056	RegOpenKey	HKCR\CLSID\{56AD4C5D-B908-4F85-...	NAME NOT FOUND	Desired Access: R...
7:41:4...	Explorer.EXE	6056	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
7:41:4...	Explorer.EXE	6056	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
7:41:4...	Explorer.EXE	6056	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
7:41:4...	Explorer.EXE	6056	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: R...
7:41:4...	Explorer.EXE	6056	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
7:41:4...	Explorer.EXE	6056	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
7:41:4...	Explorer.EXE	6056	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
7:41:4...	Explorer.EXE	6056	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name

8. Now go to Windows10 Machine and run the screensaver.exe malware as Administrator by right click
9. Now go to Kali Linux you will find meterpreter session is successful [as usual to get the shell ⇒ Powershell ⇒ Start notepad Process]
10. And observe the Process Hacker tool as shown below and you will find the malware process named “screensaver.exe” is running and associated child processes as well triggered through the malware

Process Hacker [DESKTOP-61SVOEB\labsuser]+ (Administrator)

Hacker View Tools Users Help

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
System Idle Process	0	78.46		60 kB	NT AUTHORITY\SYSTEM	
System	4	0.95		196 kB	NT AUTHORITY\SYSTEM	NT Kernel & System
smss.exe	312			1.07 MB	NT AUTHORITY\SYSTEM	Windows Session Manager
Memory Compression	1664			56 kB	NT AUTHORITY\SYSTEM	
Interrupts		6.56		0		Interrupts and DPCs
Registry	88			4.12 MB	NT AUTHORITY\SYSTEM	
csrss.exe	424			1.76 MB	NT AUTHORITY\SYSTEM	Client Server Runtime Process
wininit.exe	500			1.35 MB	NT AUTHORITY\SYSTEM	Windows Start-Up Application
csrss.exe	508	0.04		2.16 MB	NT AUTHORITY\SYSTEM	Client Server Runtime Process
winlogon.exe	568			2.53 MB	NT AUTHORITY\SYSTEM	Windows Logon Application
fontdrvhost.exe	788			3.59 MB	Font Driver Host\UMFD-	Usermode Font Driver Host
dwm.exe	996	1.95		46.29 MB	Window Man...\DWM-1	Desktop Window Manager
explorer.exe	6056	0.09		55.6 MB	DESKTOP-61S...\labsuser	Windows Explorer
SecurityHealthSystray.exe	8320			1.7 MB	DESKTOP-61S...\labsuser	Windows Security notification...
OneDrive.exe	8412			46.12 MB	DESKTOP-61S...\labsuser	Microsoft OneDrive
Procmon64.exe	8740			5.2 MB	DESKTOP-61S...\labsuser	Process Monitor
Procmon64.exe	9796	0.95	299.95 kB...	76.64 MB	DESKTOP-61S...\labsuser	Process Monitor
screensaver_newapp.exe	5588	0.04	400 B/s	2.7 MB	DESKTOP-61S...\labsuser	ApacheBench command line ...
cmd.exe	3160			2.64 MB	DESKTOP-61S...\labsuser	Windows Command Processor
conhost.exe	9208			6.52 MB	DESKTOP-61S...\labsuser	Console Window Host
powershell.exe	8104			39.43 MB	DESKTOP-61S...\labsuser	Windows PowerShell
notepad.exe	4712			3.5 MB	DESKTOP-61S...\labsuser	Notepad
firefox.exe	8728	0.34	6.22 kB/s	364.14 MB	DESKTOP-61S...\labsuser	Firefox

CPU Usage: 21.54% Physical memory: 3.87 GB (24.63%) Processes: 155

Process Hacker [DESKTOP-61SVOEB\labsuser]+ (Administrator)

Hacker View Tools Users Help

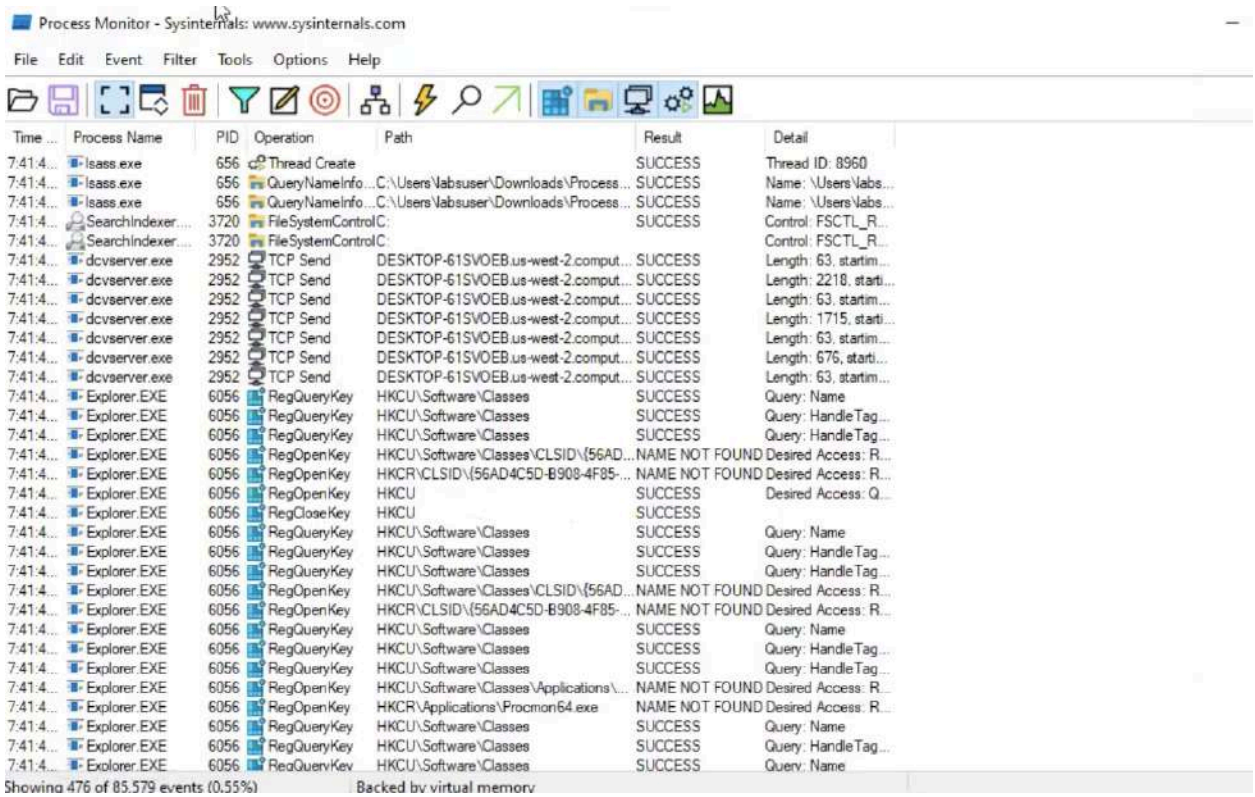
Refresh Options Find handles or DLLs System information Search Network (Ctrl+K)

Processes Services Network Disk

Name	Local address	Local...	Remote address	Rem...	Prot...	State	Owner
firefox.exe ...	DESKTOP-61SVOEB	49928	DESKTOP-61SVOEB	49929	TCP	Establish...	
firefox.exe ...	DESKTOP-61SVOEB	49929	DESKTOP-61SVOEB	49928	TCP	Establish...	
lsass.exe (6...	DESKTOP-61SVOEB	49664			TCP	Listen	
lsass.exe (6...	DESKTOP-61SVOEB	49664			TCP6	Listen	
screensave...	DESKTOP-61SVOE...	51221	ip-172-31-46-73.us-west-2.compute.internal			lish...	
services.ex...	DESKTOP-61SVOEB	49684			TCP	Listen	
services.ex...	DESKTOP-61SVOEB	49684			TCP6	Listen	
spoolsv.ex...	DESKTOP-61SVOEB	49669			TCP	Listen	Spooler
spoolsv.ex...	DESKTOP-61SVOEB	49669			TCP6	Listen	Spooler
ssm-agent...	DESKTOP-61SVOE...	49719	52.94.177.19	443	TCP	Establish...	
ssm-agent...	DESKTOP-61SVOE...	51234	52.94.177.134	443	TCP	Establish...	
svchost.ex...	DESKTOP-61SVOEB	49666			TCP	Listen	EventLog
svchost.ex...	DESKTOP-61SVOEB	49666			TCP6	Listen	EventLog
svchost.ex...	DESKTOP-61SVOEB	123			UDP		W32Time
svchost.ex...	DESKTOP-61SVOEB	123			UDP6		W32Time
svchost.ex...	DESKTOP-61SVOEB	49667			TCP	Listen	Schedule
svchost.ex...	DESKTOP-61SVOEB	49667			TCP6	Listen	Schedule
svchost.ex...	DESKTOP-61SVOEB	5040			TCP	Listen	CDPSvc
svchost.ex...	DESKTOP-61SVOEB	5050			UDP		CDPSvc
svchost.ex...	DESKTOP-61SVOEB	7680			TCP	Listen	DoSvc
svchost.ex...	DESKTOP-61SVOEB	7680			TCP6	Listen	DoSvc
svchost.ex...	DESKTOP-61SVOEB	5353			UDP		Dnscache
svchost.ex...	DESKTOP-61SVOEB	5355			UDP		Dnscache

CPU Usage: 19.63% Physical memory: 3.87 GB (24.66%) Processes: 155

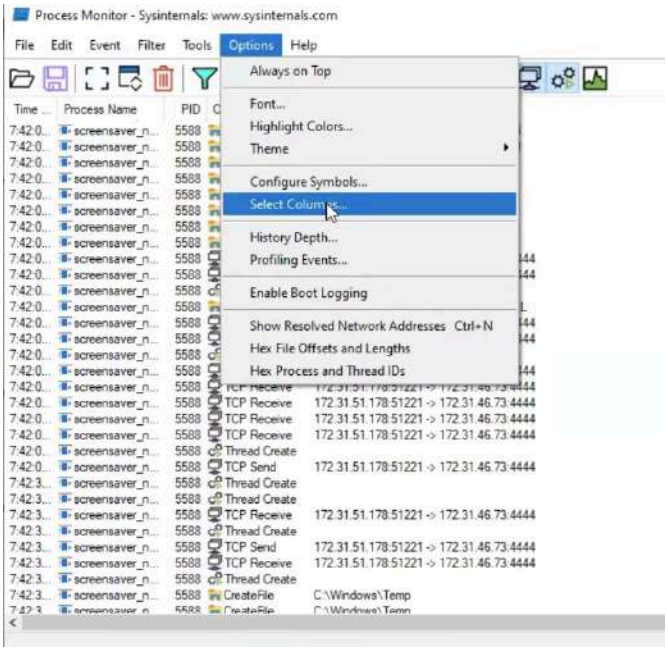
11. Now go to the Process Monitor tool and stop the capture button to stop collecting events



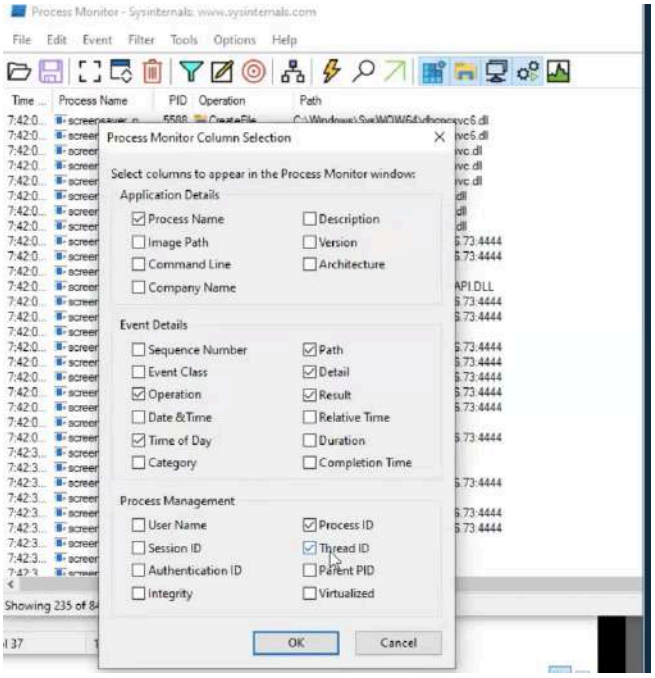
Time ...	Process Name	PID	Operation	Path	Result	Detail
7:41:4...	lsass.exe	656	Thread Create		SUCCESS	Thread ID: 8960
7:41:4...	lsass.exe	656	QueryNameInfo...	C:\Users\labsuser\Downloads\Process...	SUCCESS	Name: \Users\labs...
7:41:4...	lsass.exe	656	QueryNameInfo...	C:\Users\labsuser\Downloads\Process...	SUCCESS	Name: \Users\labs...
7:41:4...	SearchIndexer....	3720	FileSystemControl	C:	SUCCESS	Control: FSCTL_R...
7:41:4...	SearchIndexer....	3720	FileSystemControl	C:		Control: FSCTL_R...
7:41:4...	dcvserver.exe	2952	TCP Send	DESKTOP-61SVOEB.us-west-2.comput...	SUCCESS	Length: 63, startim...
7:41:4...	dcvserver.exe	2952	TCP Send	DESKTOP-61SVOEB.us-west-2.comput...	SUCCESS	Length: 2218, starti...
7:41:4...	dcvserver.exe	2952	TCP Send	DESKTOP-61SVOEB.us-west-2.comput...	SUCCESS	Length: 63, startim...
7:41:4...	dcvserver.exe	2952	TCP Send	DESKTOP-61SVOEB.us-west-2.comput...	SUCCESS	Length: 1715, starti...
7:41:4...	dcvserver.exe	2952	TCP Send	DESKTOP-61SVOEB.us-west-2.comput...	SUCCESS	Length: 63, startim...
7:41:4...	dcvserver.exe	2952	TCP Send	DESKTOP-61SVOEB.us-west-2.comput...	SUCCESS	Length: 676, starti...
7:41:4...	dcvserver.exe	2952	TCP Send	DESKTOP-61SVOEB.us-west-2.comput...	SUCCESS	Length: 63, startim...
7:41:4...	Explorer.EXE	6056	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
7:41:4...	Explorer.EXE	6056	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
7:41:4...	Explorer.EXE	6056	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
7:41:4...	Explorer.EXE	6056	RegOpenKey	HKCU\Software\Classes\CLSID\{56AD...	NAME NOT FOUND	Desired Access: R...
7:41:4...	Explorer.EXE	6056	RegOpenKey	HKCR\CLSID\{56AD4C5D-B908-4F85-...	NAME NOT FOUND	Desired Access: R...
7:41:4...	Explorer.EXE	6056	RegOpenKey	HKCU	SUCCESS	Desired Access: Q...
7:41:4...	Explorer.EXE	6056	RegCloseKey	HKCU	SUCCESS	
7:41:4...	Explorer.EXE	6056	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
7:41:4...	Explorer.EXE	6056	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
7:41:4...	Explorer.EXE	6056	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
7:41:4...	Explorer.EXE	6056	RegOpenKey	HKCU\Software\Classes\CLSID\{56AD...	NAME NOT FOUND	Desired Access: R...
7:41:4...	Explorer.EXE	6056	RegOpenKey	HKCR\CLSID\{56AD4C5D-B908-4F85-...	NAME NOT FOUND	Desired Access: R...
7:41:4...	Explorer.EXE	6056	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
7:41:4...	Explorer.EXE	6056	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
7:41:4...	Explorer.EXE	6056	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
7:41:4...	Explorer.EXE	6056	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: R...
7:41:4...	Explorer.EXE	6056	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
7:41:4...	Explorer.EXE	6056	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
7:41:4...	Explorer.EXE	6056	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
7:41:4...	Explorer.EXE	6056	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name

12. In Options Tab uncheck the “Show Resolved Network Address” if it’s already there unchecked or not enabled leave this settings do no change

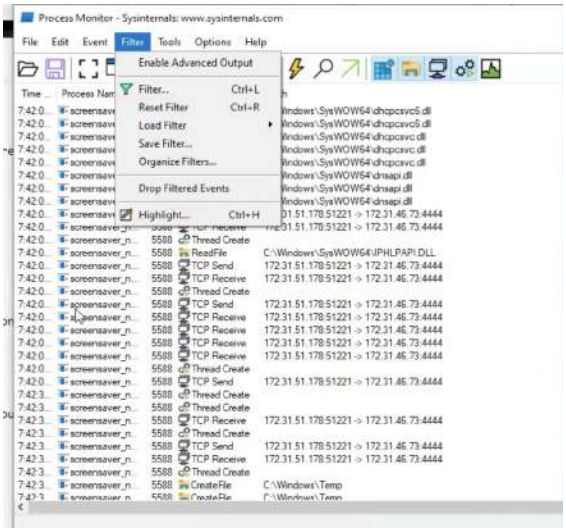
13. Now ensure following settings are turned off in Process Monitor tool
    Go to “Select Columns”



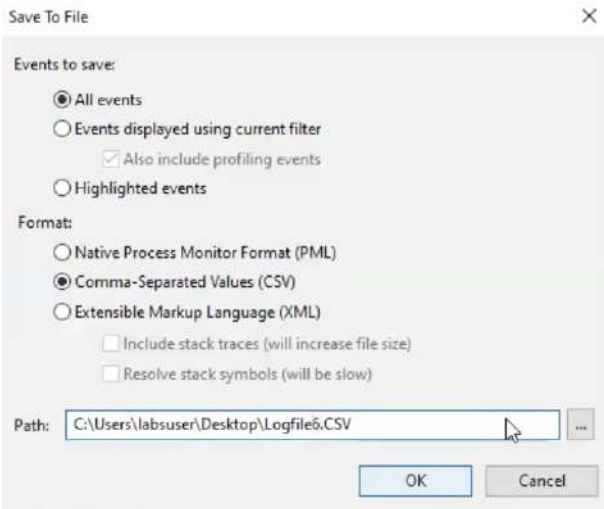
Do not select “Sequence Number” and “select the “Thread ID” as shown below Click Ok



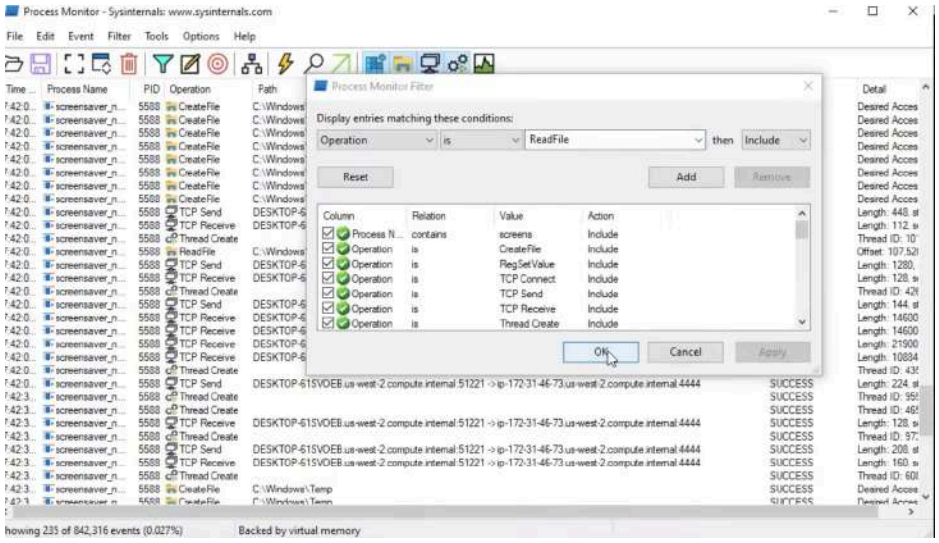
In Filter option uncheck the “Enable Advanced Output” if it’s already there unchecked or not enabled leave this settings do no change



14. Click on Save button in Process Monitor and ensure you have selected “All Events” and “CSV” format and save to desktop in Windows 10



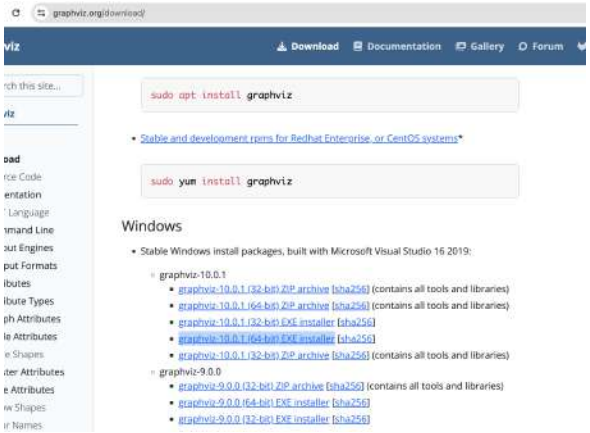
Step 4:
Now you can also investigate the events in Process Monitor specific to malware by applying following filters



Step 5:
Now it's time to generate a report with Graph analysis of malware behavior based on the process events we collected in CSV format in Process Monitor tool

In order to do that we need to install the tool called ProcDot [but procdoc requires dependency as GraphViz to run the machine hence we will proceed with following steps of installing]

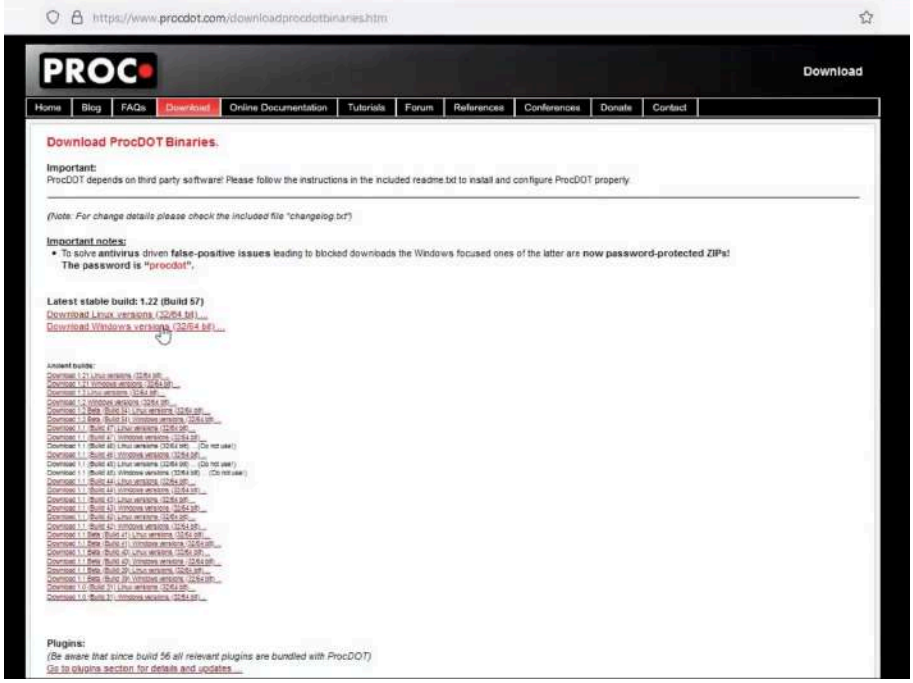
https://gitlab.com/api/v4/projects/4207231/packages/generic/graphviz-releases/10.0.1/windows_10_cmake_Release_graphviz-install-10.0.1-win64.exe

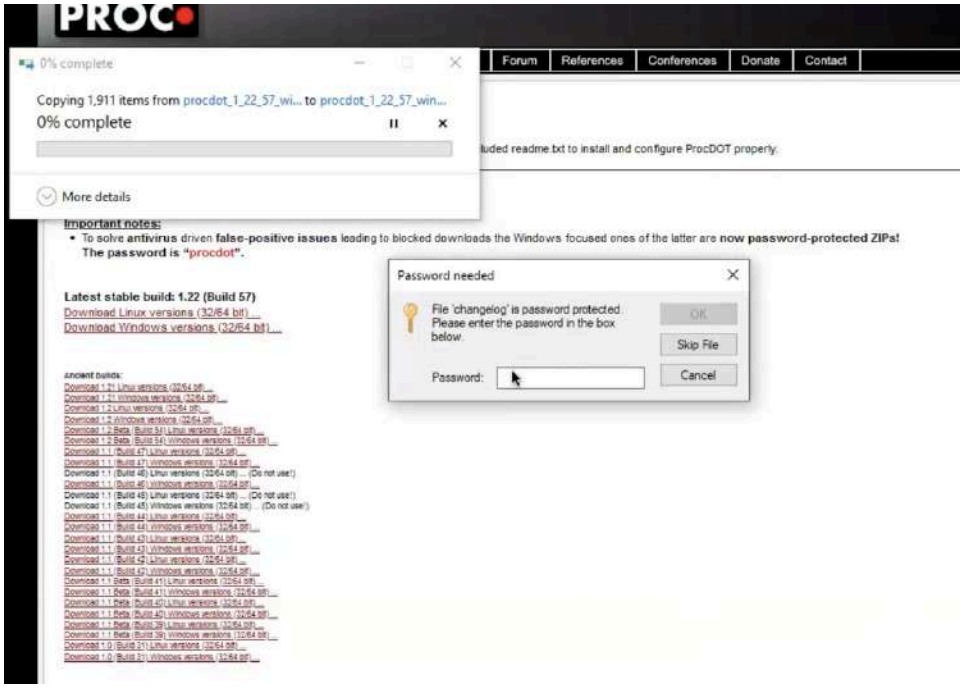


Install the Graphviz by following Next as shown below however ensure the following option is selected during the installation of this "Add GraphViz to the system PATH for all users"

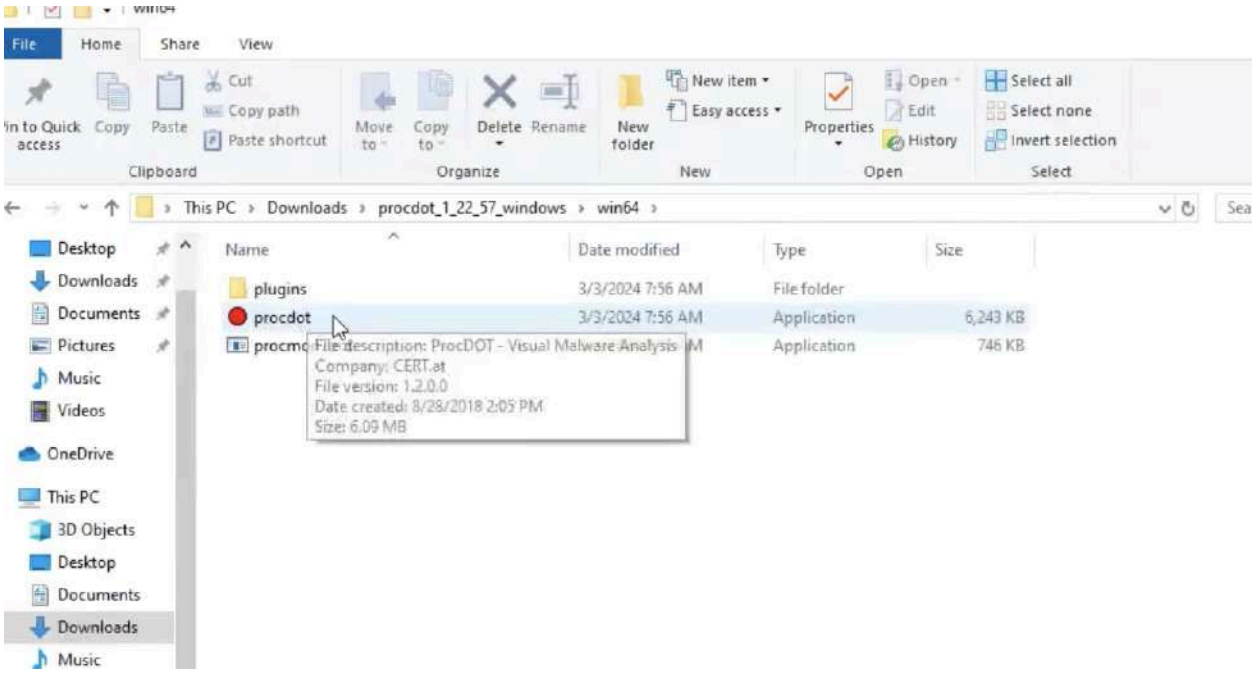
Now Download the Procdot tool using the link below and extract zip .
ProcDot have password protection while extracting with 7Zip and The password is “procdot”

https://www.procdot.com/download/procdot/binaries/procdot_1_22_57_windows.zip

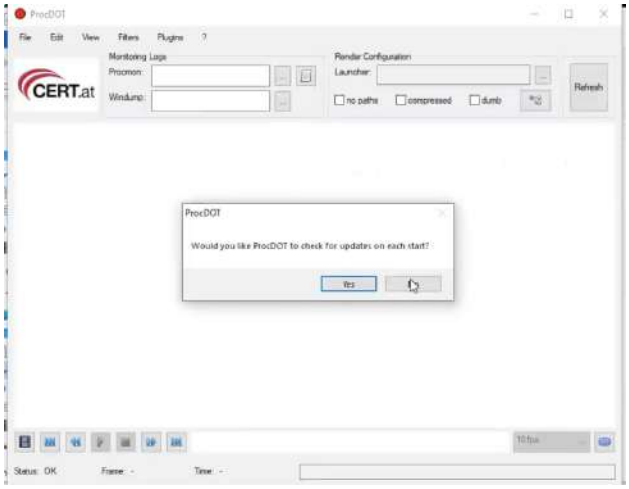


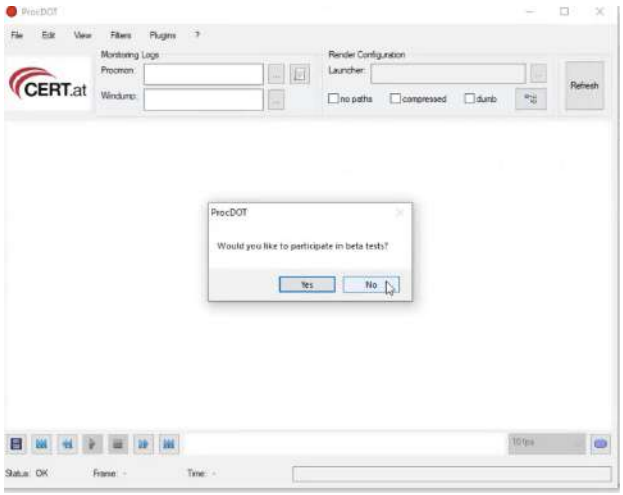


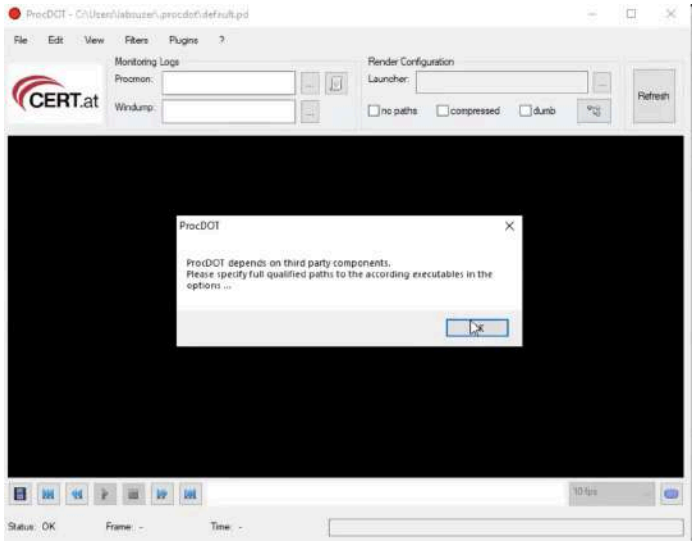
Step 6:
Configure and the ProcDot tool



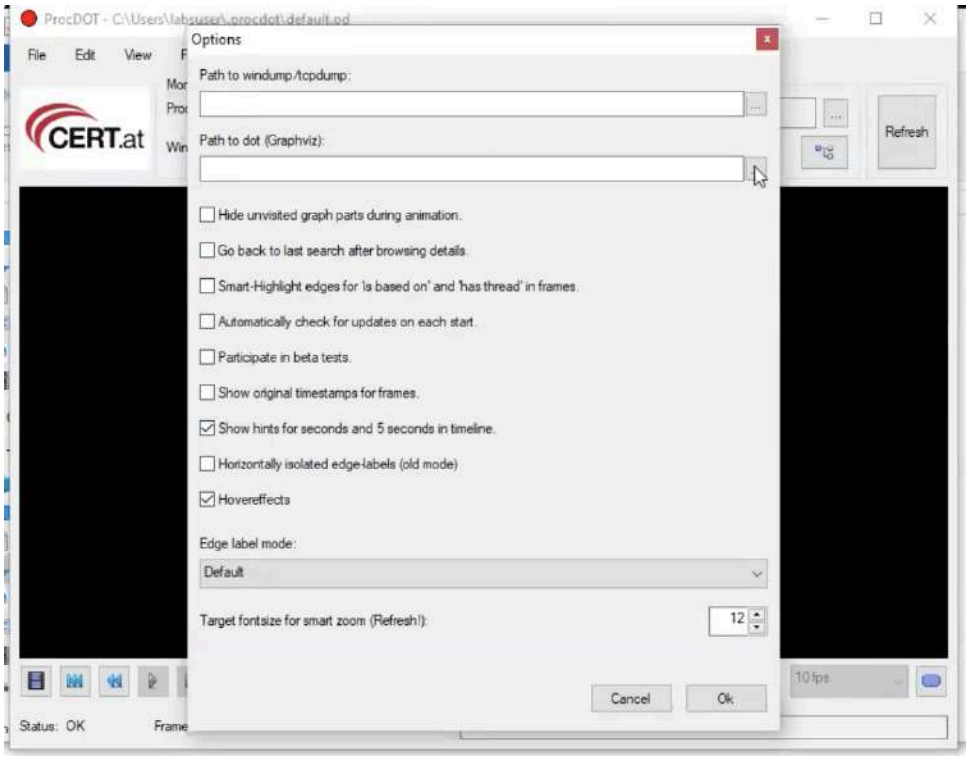
Click on “No” if its ask for updates

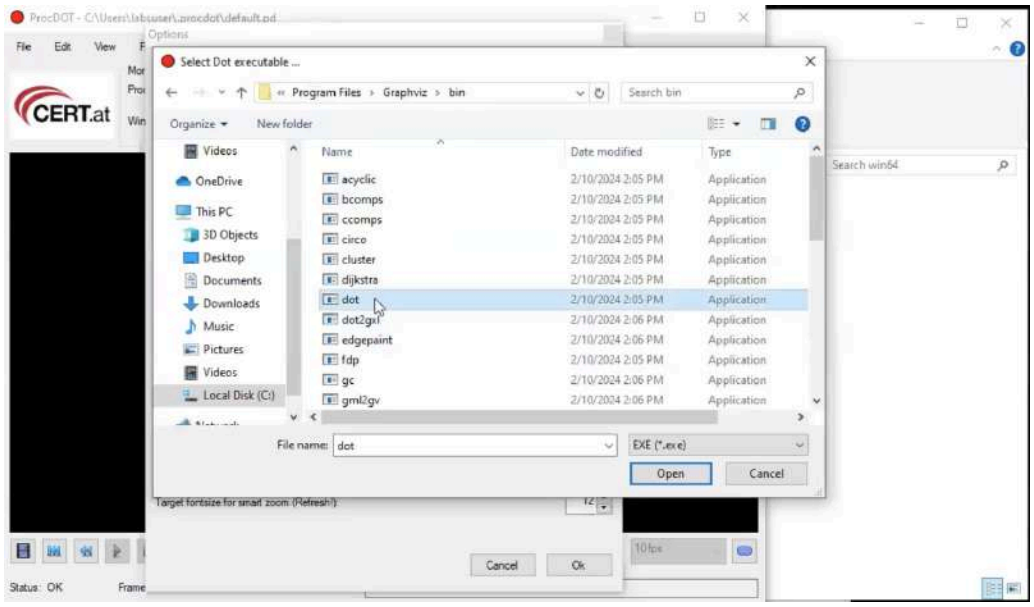


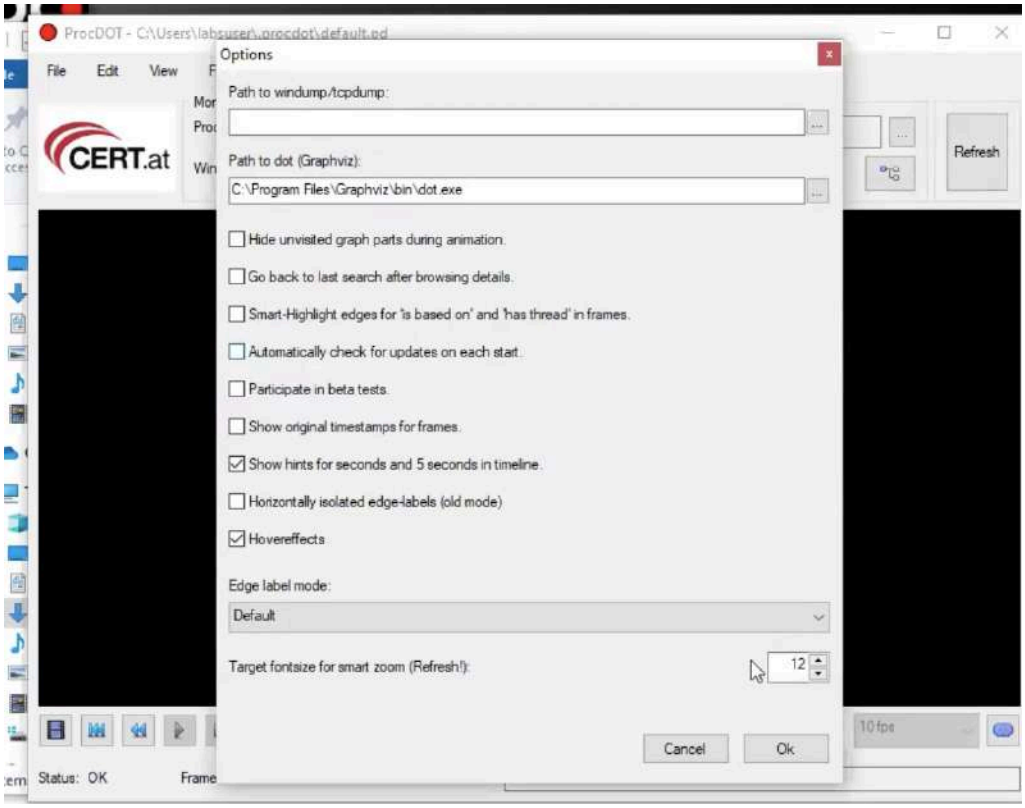




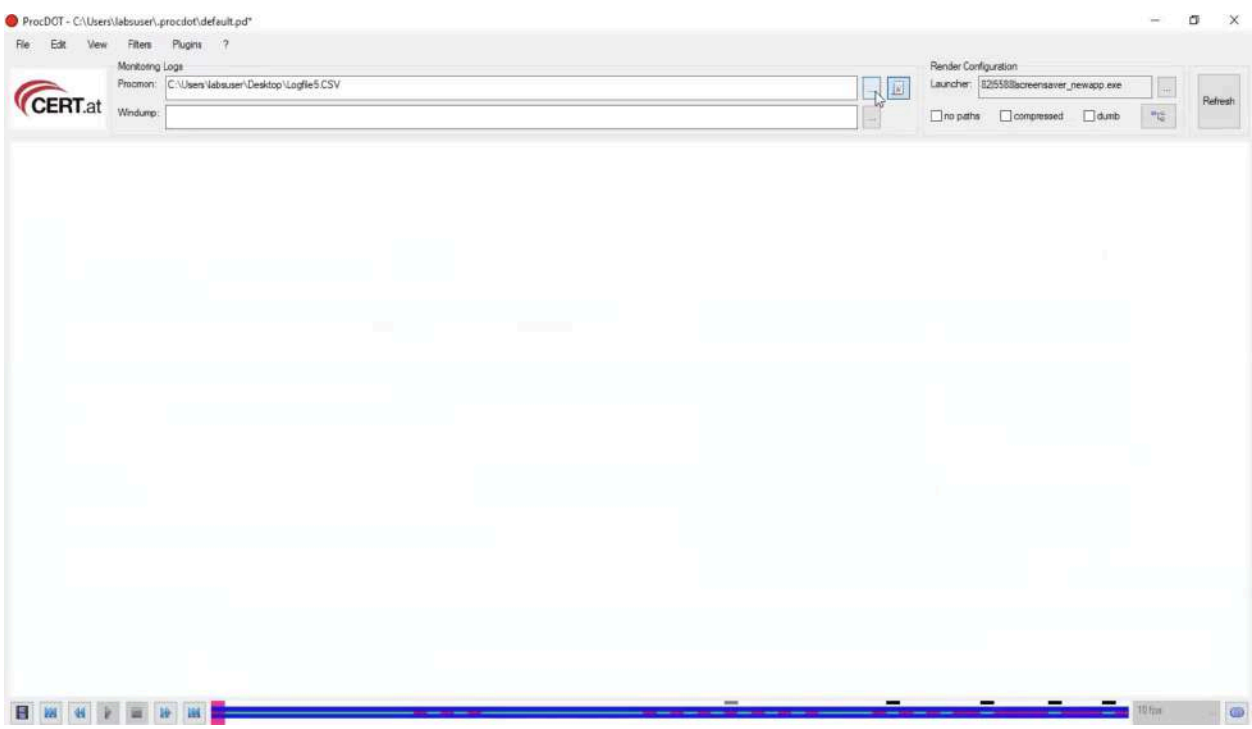
Now you need to load the “Path to Dot” for (Graphiviz} as dependency for this ProcDot tool



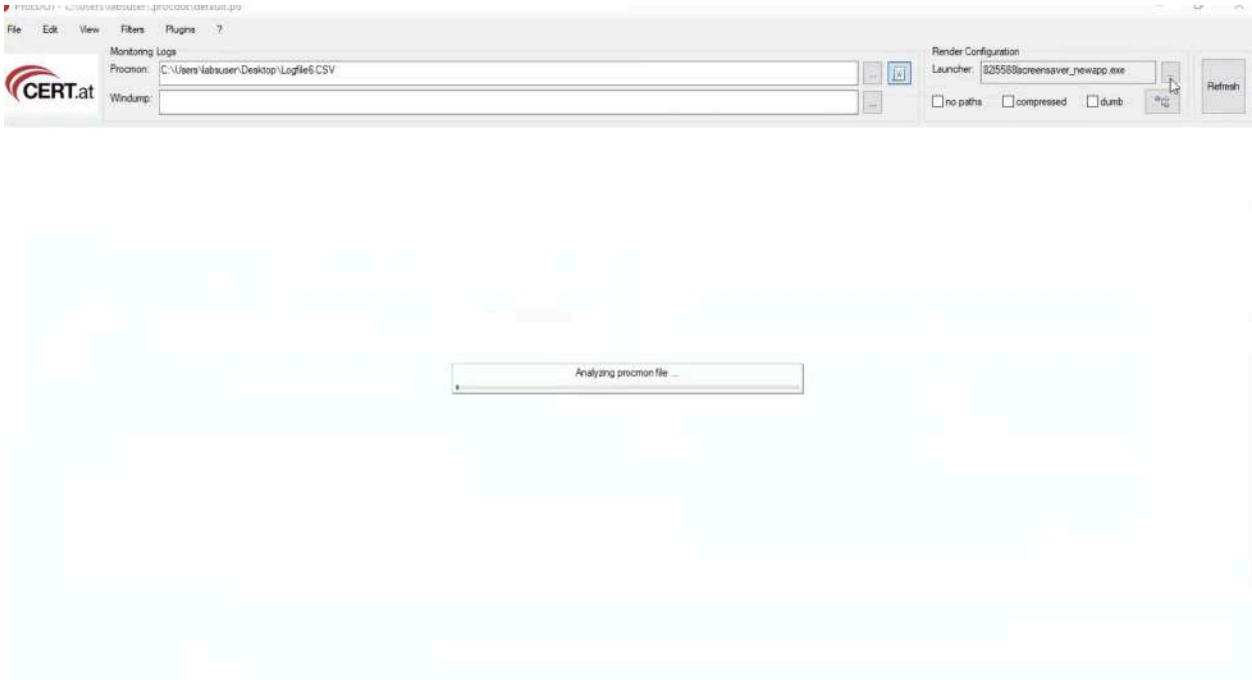




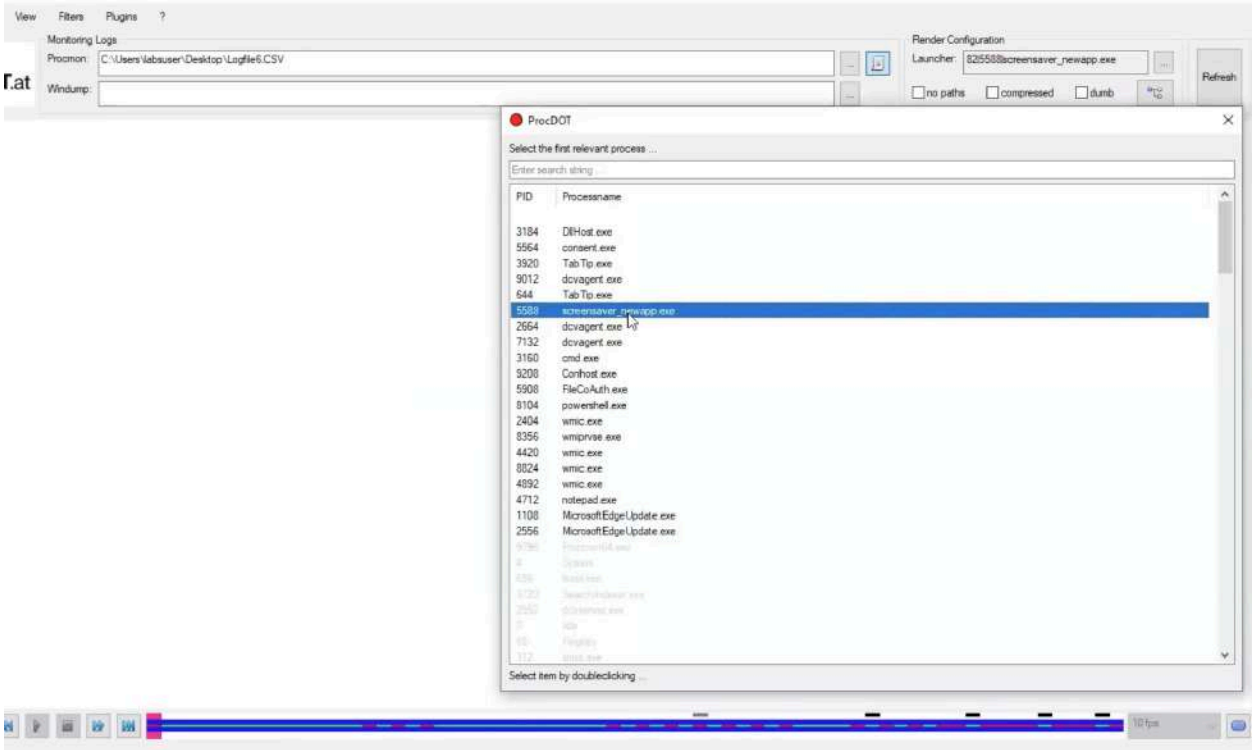
Now load the CSV file generated from Process Monitor tool in to ProDot as shown below



Now click on Launcher button to start Analyzing the Procmon file

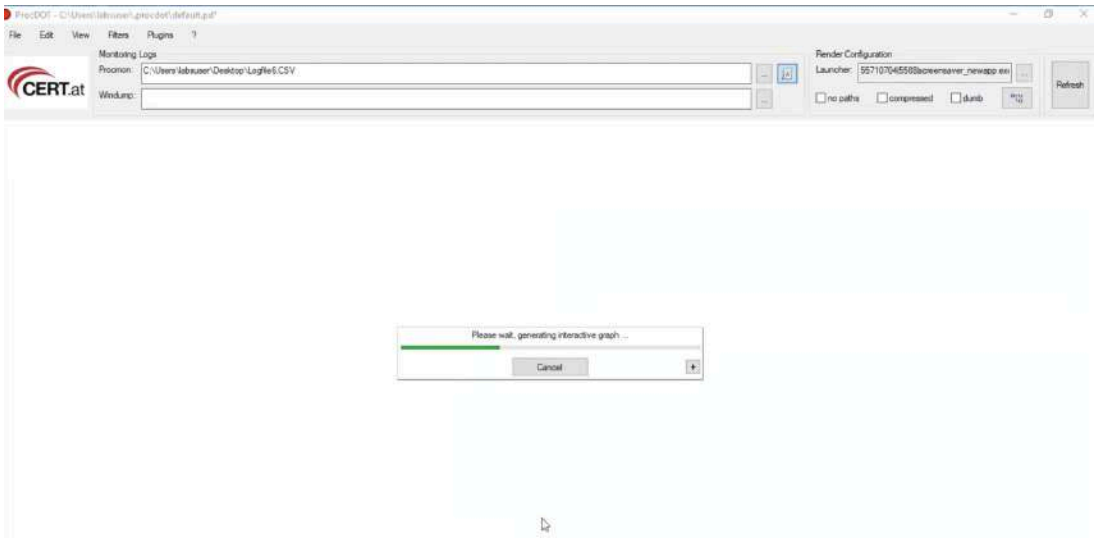


Then you will find the below windows loaded with all the processes however we need to select the processes relevant to our malware "screensaver.exe"



Once selected click on “**Refresh**” tab

Then you will find the graph will be loaded to generate



Finally graph is generated [Investigate the Processes and child processes created from malware]