

Module 3: Redline

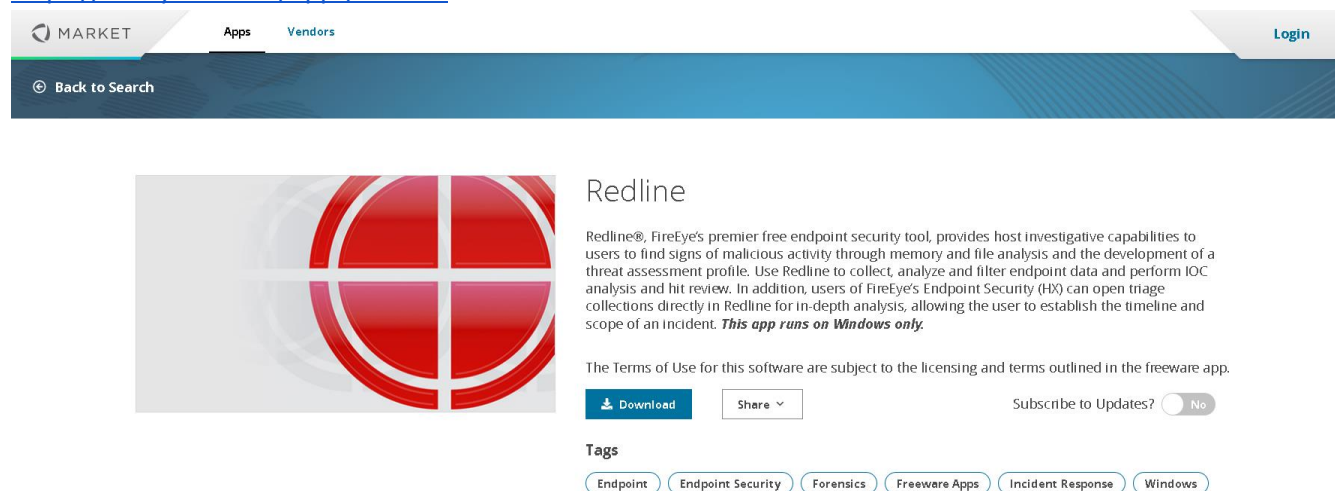
Objectives

- Analyze the same infected memory image from Activity 10-2 to compare Volatility and Redline

Tasks

1. Install Redline (if you are using the prepared Windows 7 virtual machine you can skip this step):

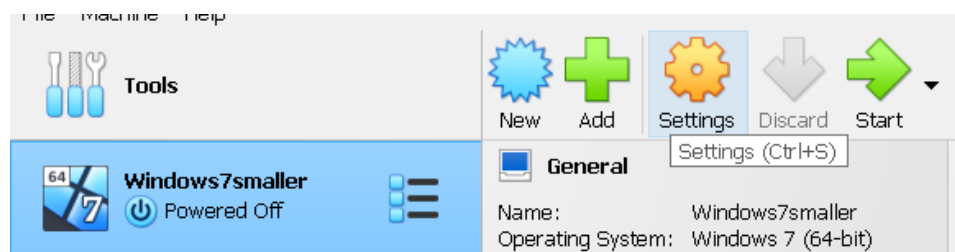
<https://fireeye.market/apps/211364>



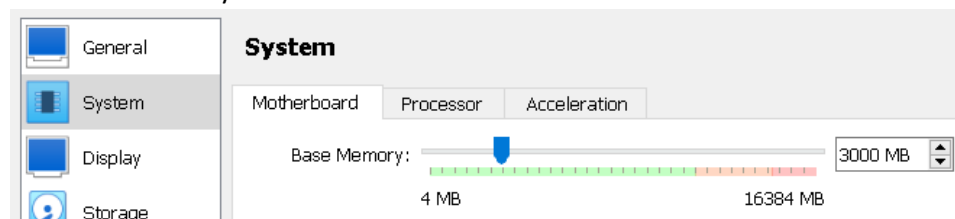
2. Open your infected raw file in Redline:

(NOTE: Redline will load every process in the memory dump and this can take at least 30 minutes. If you would like to speed up the process, you can allocate more ram and processors to your Windows7 machine. This is optional, but highly recommended:

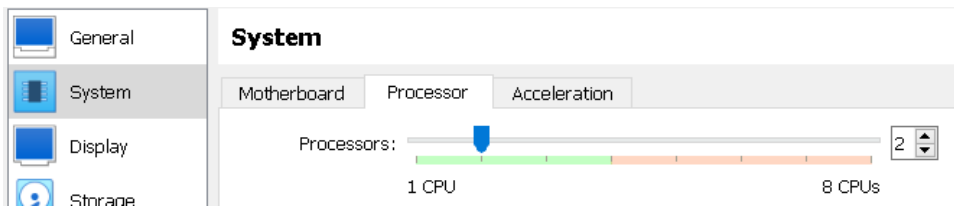
1. Shut down the virtual machine
2. Select your virtual machine and click settings



3. Go to system



As long as the system has already been shut down, you can adjust the base memory. 3000MB should be enough.



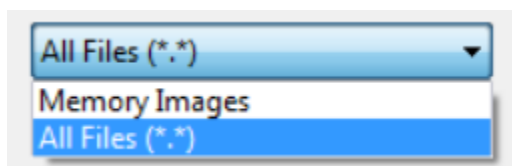
You can also add more processors. 2-4 should be enough.

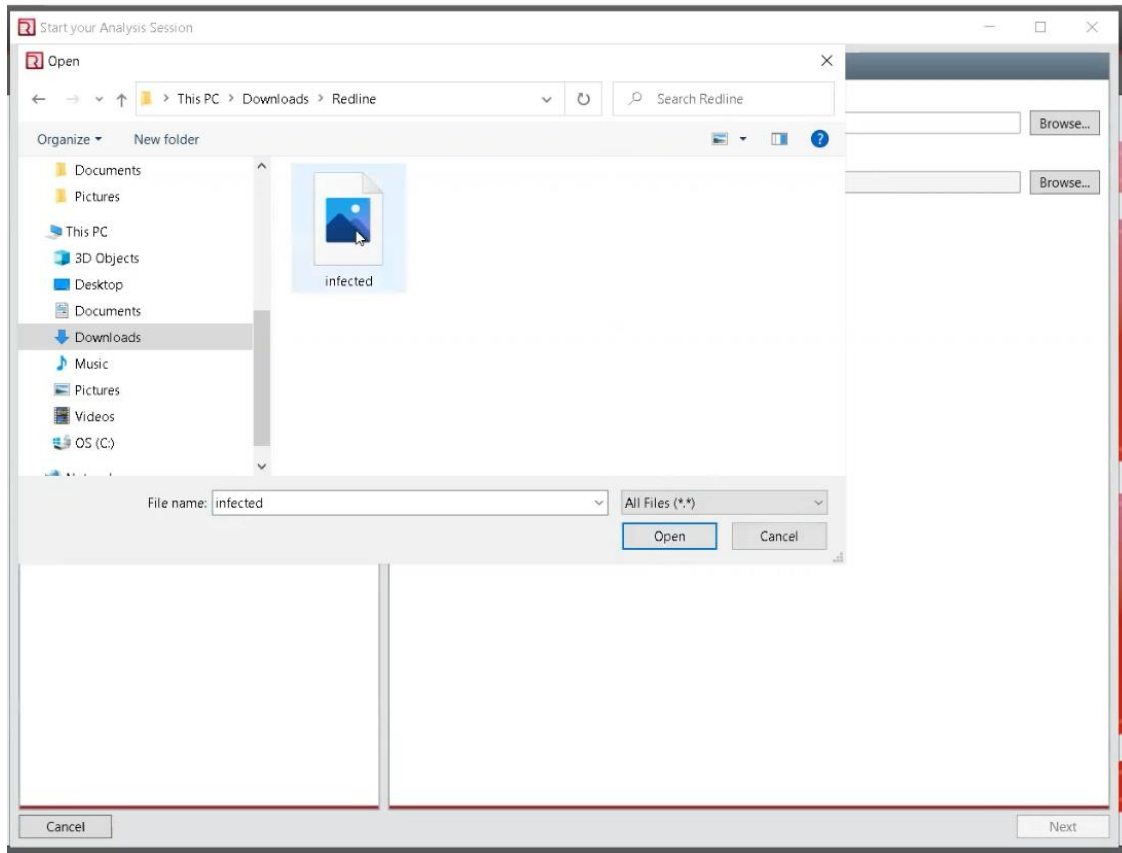
When you are done, you can open your virtual machine back up.

Click Analyze Data > From a Saved Memory File

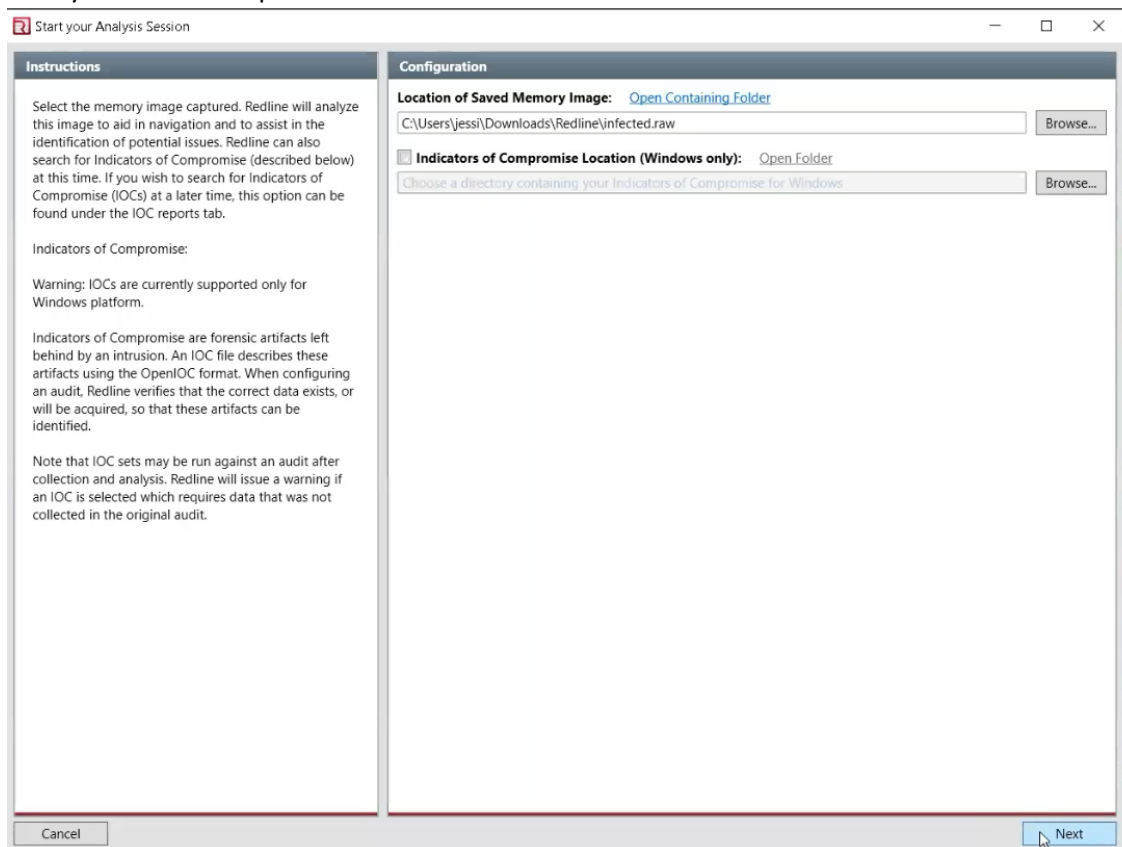


3. Navigate to your raw file by clicking "Browse" and selecting "All files" from the drop down menu next to "File name". Now you should be able to see where your raw file is

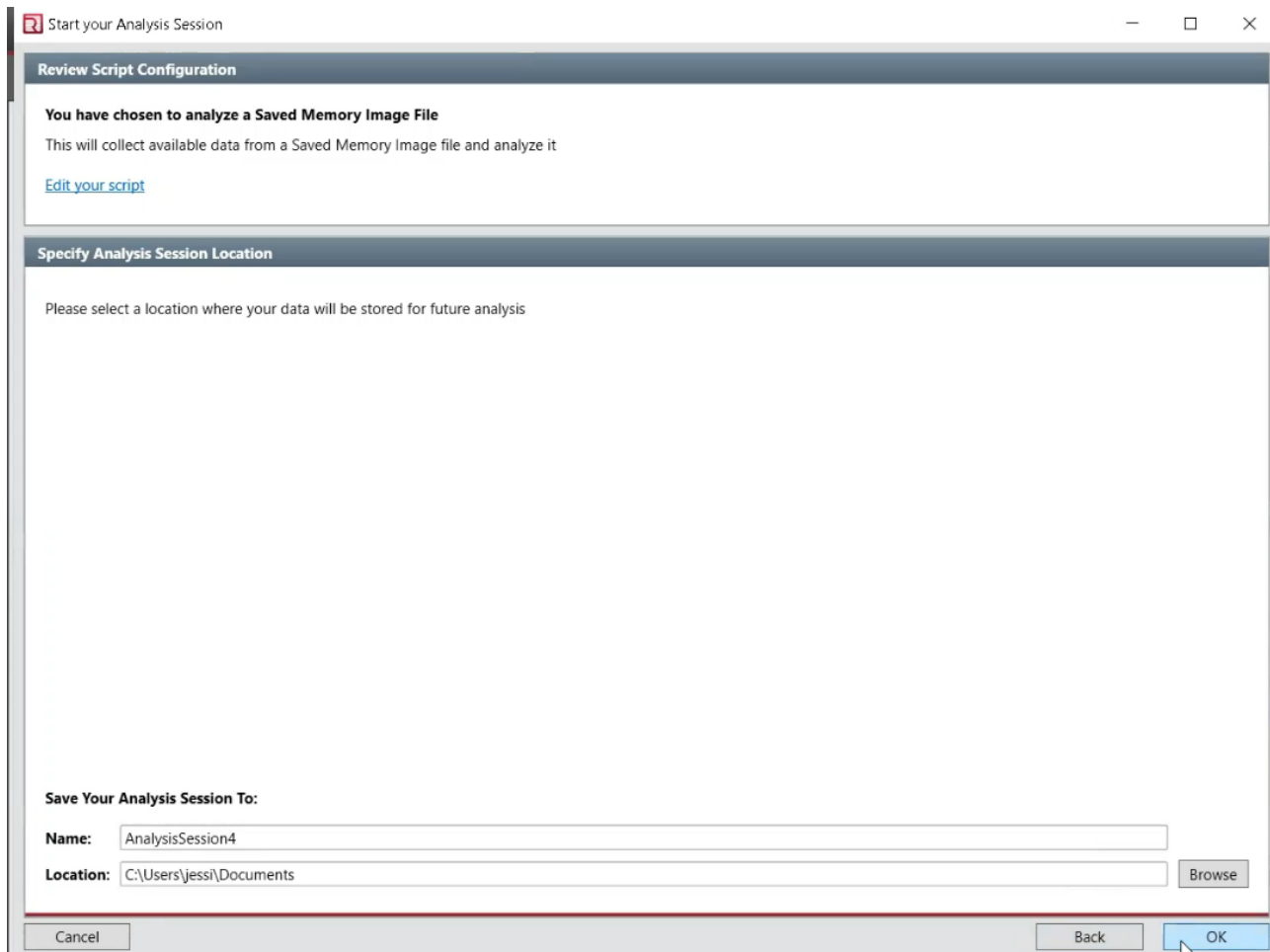




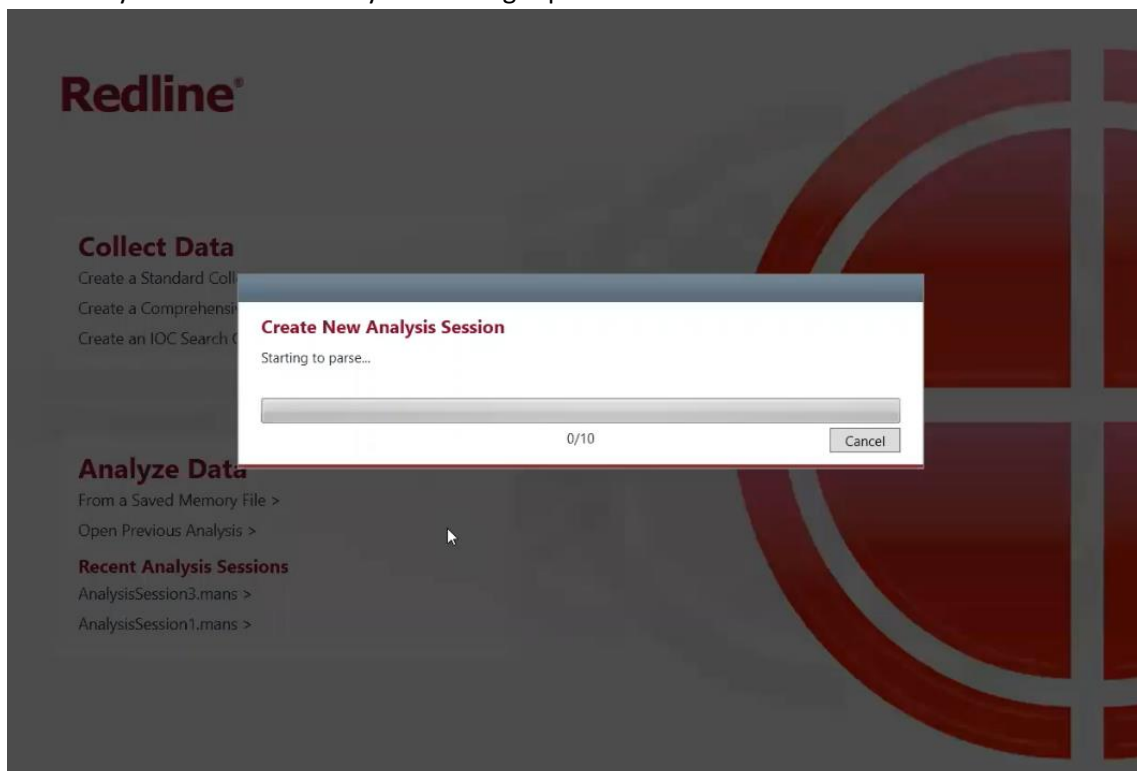
Now you can click “Open” and then “Next”



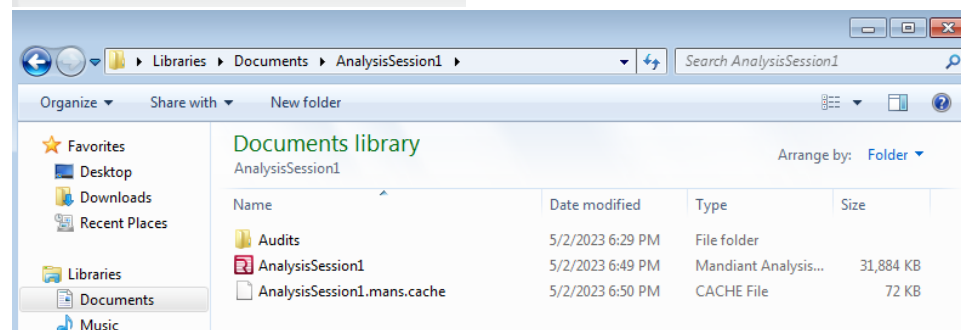
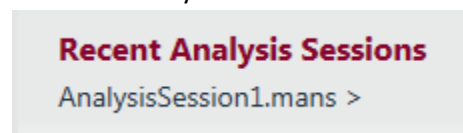
4. On this screen you can name your analysis file and decide where you want to save it by typing where it says “Name” or clicking “Browse”. When you have finished deciding, you can click “Ok”



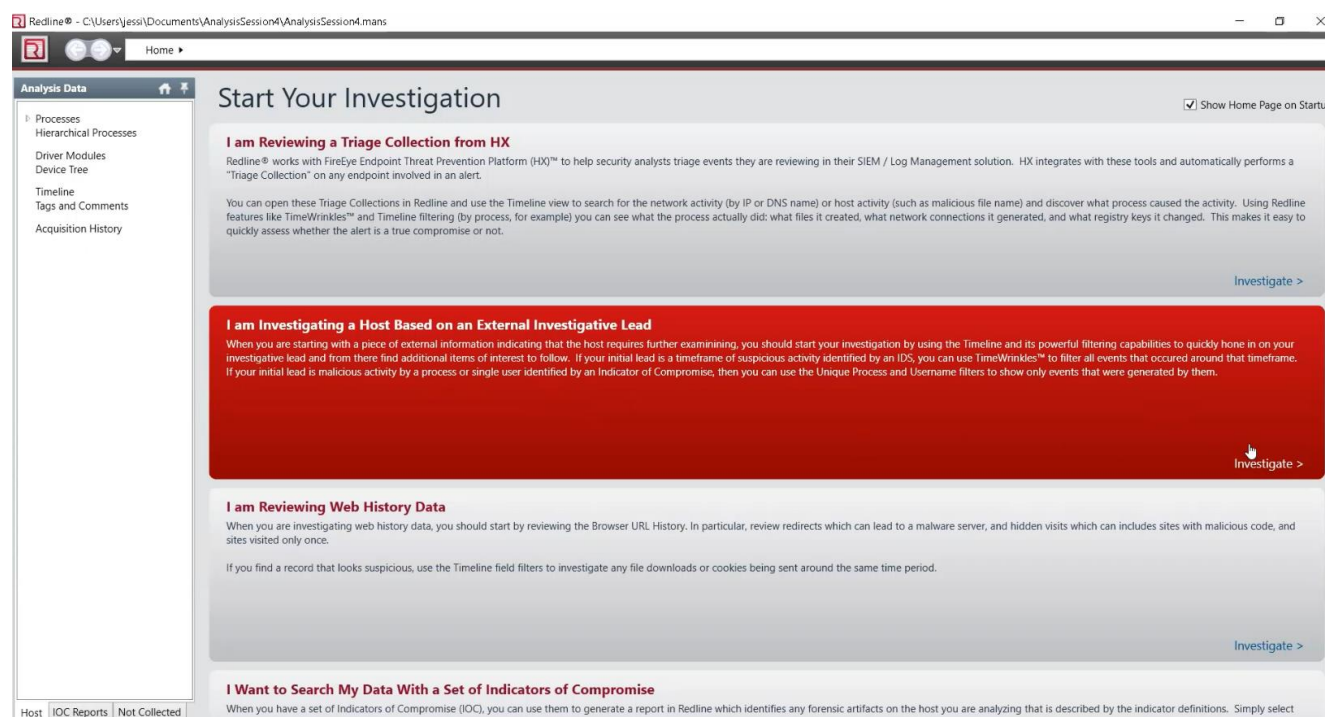
5. If you get a pop up, click "Yes"
6. Now you need to wait for your file to get processed.



- When it's done, open the session. You can open the session either on the home page of redline under "Recent Analysis Sessions" or you can open the file manually wherever you had it saved.

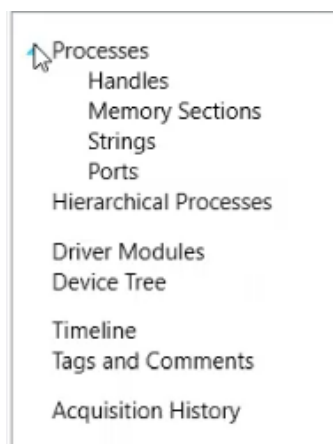


- Click "I am Investigating a Host Based on an External Investigative Lead"



- Click "Processes" on the top left to see all of the processes on the raw file

12. Now click the arrow next to “Processes” to open up the drop down menu and click “Handles”



13. Now you can look through the handles of all of the processes

Filters

Review Handles
These filters allow you to view the different subcategories of Handles in isolation.

Show Named Handles
Display all named handles in the system.

[Show All Handles](#)
Display all handles in the system.

[Show File Handles](#)
Display only Handles to Files.

[Show Directory Handles](#)
Display only Handles to Directories.

[Show Process Handles](#)
Display only Handles to Processes.

[Show Registry Key Handles](#)
Display only Handles to Registry Keys.

[Show Semaphore Handles](#)
Display only Handles to Semaphores.

[Show Mutant Handles](#)
Display only Handles to Mutants.

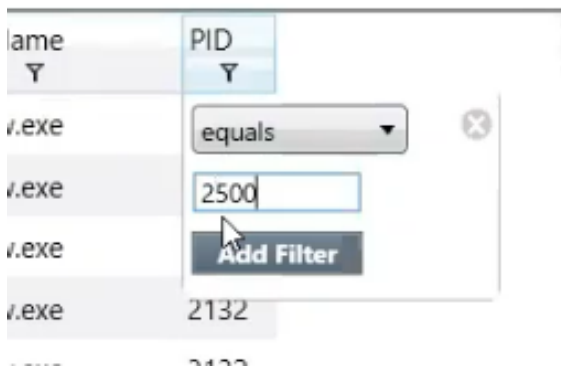
[Show Event Handles](#)
Display only Handles to Events.

[Show Section Handles](#)
Display only Handles to Sections.

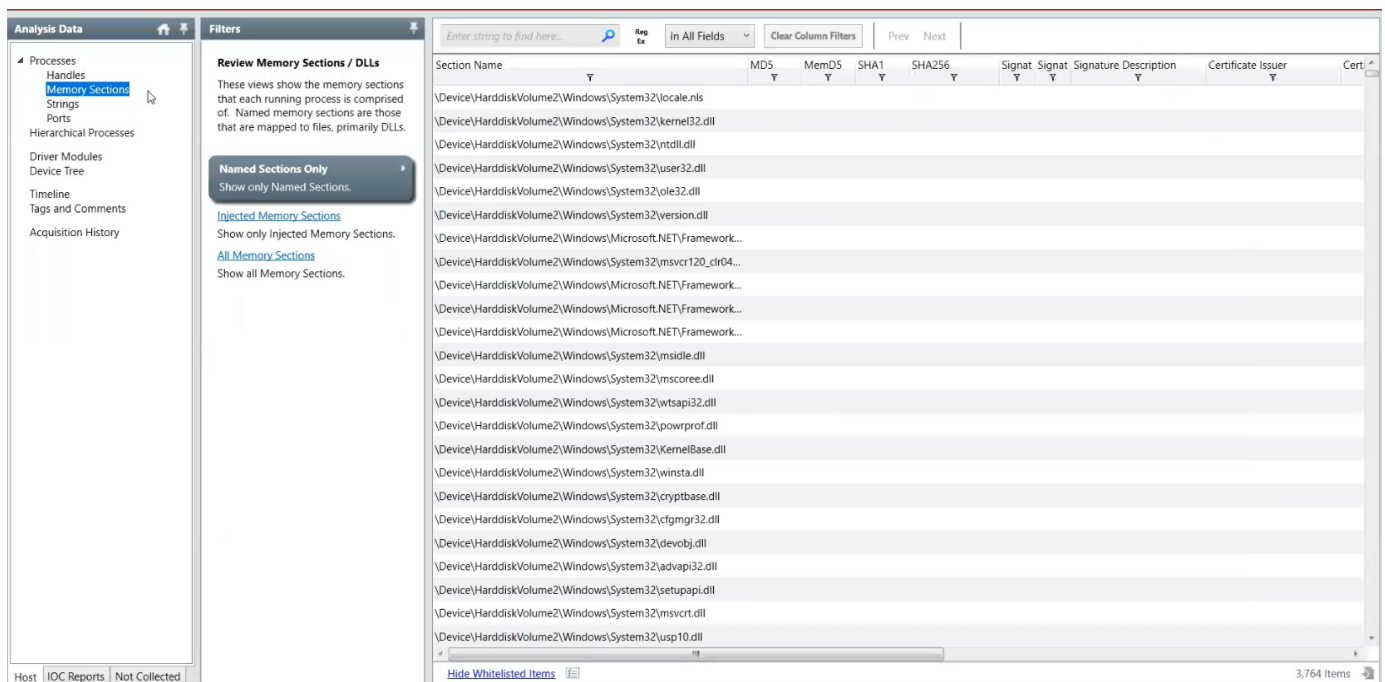
Enter string to find here... **Reg Ex** **In All Fields** **Clear Column Filters** **Prev** **Next**

Handle Name	Handle Type	Handle Index	Access Mask	Object Address	ProcessName	PID
REGISTRY\MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\...	Key	0x00000008	0x00000009	0xfffffa001658...	mscorsvw.exe	2
KnownDlls	Unknown	0x00000010	0x00000003	0xfffffa0007ad...	mscorsvw.exe	2132
\Device\HarddiskVolume2\Windows\System32	File	0x00000018	0x00100020	0xfffffa8004d9...	mscorsvw.exe	2132
REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\NL...	Key	0x00000020	0x00020019	0xfffffa001584...	mscorsvw.exe	2132
REGISTRY\MACHINE\	Key	0x00000040	0x000f003f	0xfffffa00160f...	mscorsvw.exe	2132
REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\SES...	Key	0x00000058	0x00000001	0xfffffa001379...	mscorsvw.exe	2132
Service-0x0-3e7\$	WindowsStation	0x00000070	0x000f016e	0xfffffa800449c...	mscorsvw.exe	2132
Default	Desktop	0x00000078	0x000f00cf	0xfffffa800449ff...	mscorsvw.exe	2132
Service-0x0-3e7\$	WindowsStation	0x00000080	0x000f016e	0xfffffa800449c...	mscorsvw.exe	2132
BaseNamedObjects	Unknown	0x000000c0	0x0000000f	0xfffffa003f37...	mscorsvw.exe	2132
REGISTRY\USER\DEFAULT\	Key	0x000000d0	0x000f003f	0xfffffa001649...	mscorsvw.exe	2132
{790FD7C9-9D97-4B0D-A587-F0F857EDF6F9}	Unknown	0x00000160	0x001f0003	0xfffffa80048c5...	mscorsvw.exe	2132
REGISTRY\MACHINE\SOFTWARE\MICROSOFT\NETFRAMEWO...	Key	0x00000190	0x0002001f	0xfffffa0014c7...	mscorsvw.exe	2132
REGISTRY\MACHINE\SOFTWARE\MICROSOFT\NETFRAMEWO...	Key	0x00000198	0x0002001f	0xfffffa00162d...	mscorsvw.exe	2132
REGISTRY\MACHINE\SOFTWARE\MICROSOFT\NET FRAMEWO...	Key	0x000001d8	0x00000001	0xfffffa00163c...	mscorsvw.exe	2132
TermSrvReadyEvent	Unknown	0x00000210	0x00100000	0xfffffa8004222...	mscorsvw.exe	2132
REGISTRY\MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\...	Key	0x00000004	0x00000009	0xfffffa001090...	taskhost.exe	1876
KnownDlls	Unknown	0x00000008	0x00000003	0xfffffa0007ad...	taskhost.exe	1876
\Device\HarddiskVolume2\Windows\System32	File	0x0000000c	0x00100020	0xfffffa8004a23...	taskhost.exe	1876
REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\NL...	Key	0x00000010	0x00020019	0xfffffa000cd5...	taskhost.exe	1876
REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\SES...	Key	0x00000014	0x00000001	0xfffffa00102f...	taskhost.exe	1876
WinSta0	WindowsStation	0x00000024	0x000f037f	0xfffffa8004207...	taskhost.exe	1876
Default	Desktop	0x00000028	0x000f01ff	0xfffffa8004341...	taskhost.exe	1876
WinSta0	WindowsStation	0x0000002c	0x000f037f	0xfffffa8004207...	taskhost.exe	1876
REGISTRY\MACHINE\	Key	0x00000030	0x00020019	0xfffffa000cd5...	taskhost.exe	1876

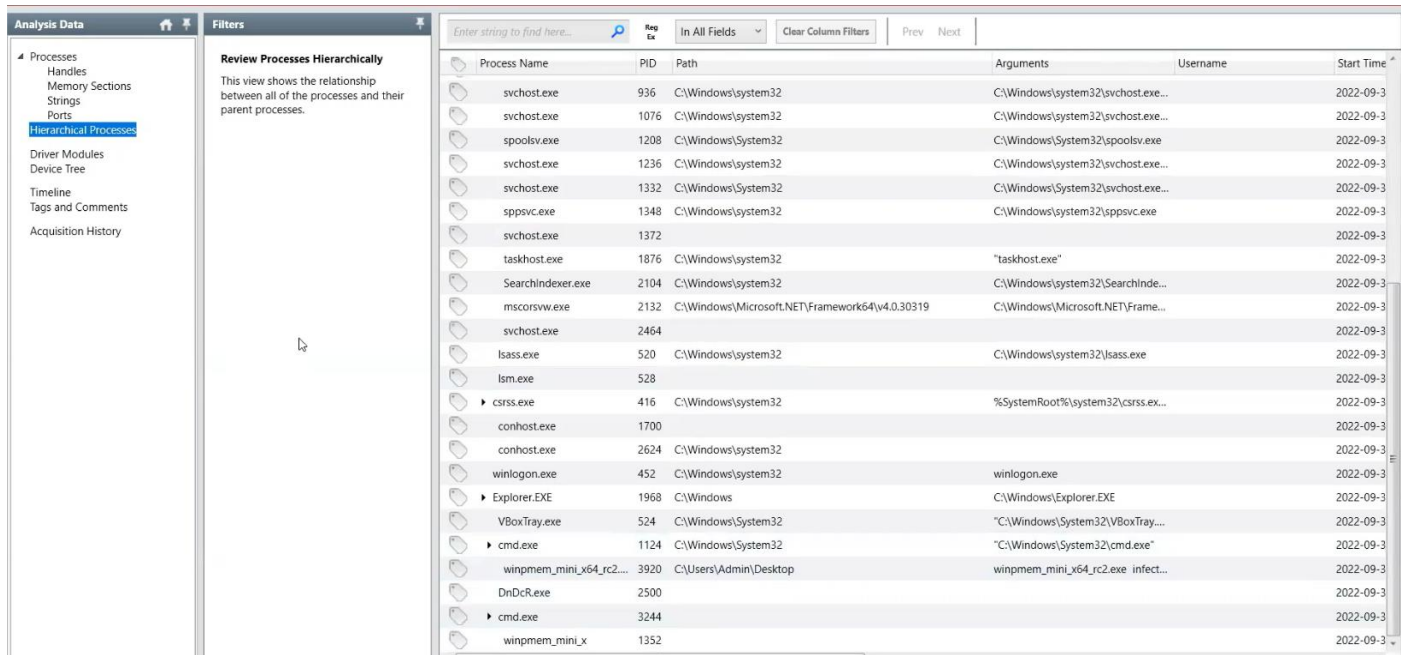
14. Double click on the small filter icon on the tabs to filter out what processes you want to see. Here I am using the PID that my malware’s process had and clicking “Add filter”. Your malware’s PID may be different



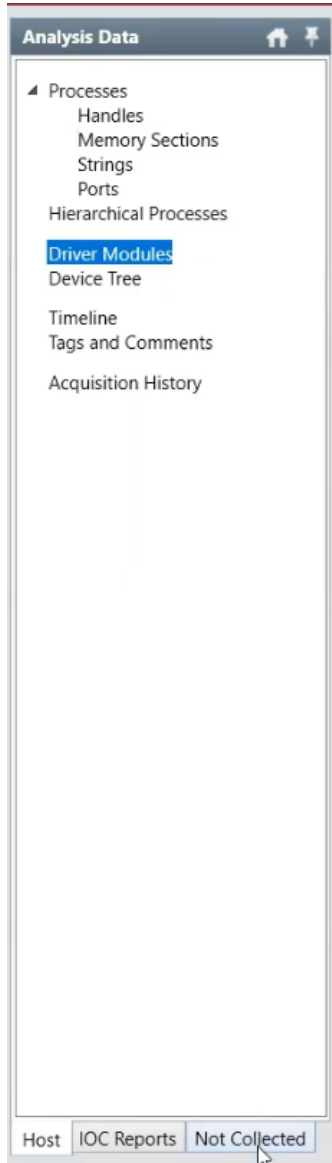
15. Click “memory sections” under processes on the top left to look at memory sections and DLLs



16. Click “Hierarchical Processes” to see the relationships between processes



17. Click “Not collected” on the bottom left to explore what was not recovered by Redline.



Questions:

1. Provide screenshots comparing the process lists acquired from volatility and redline. Use the same memory image file for both programs. Are you able to find a difference?
2. Provide screenshots comparing the data of the process lists (Handles/Memory Sections/Device Processes) acquired from volatility and redline. Use the same image file for both programs. Are you able to find any obvious difference(s)?
3. Explore Redline's page on the Fire Eye website linked in the beginning of this document. What operating system(s) does the app run on?
4. Explore what was not collected by Redline. Is there anything we collected from Volatility that we were not able to with Redline? Provide screenshots.
5. What is an advantage and disadvantage of using Redline?

Deliverable:

Explicitly answer all questions above one by one. Provide screenshots as necessary. You will be evaluated based on the correctness, completeness, clarity and quality of English writing.