Worcester Polytechnic Institute
Department of Computer Science

Module 3: Redline

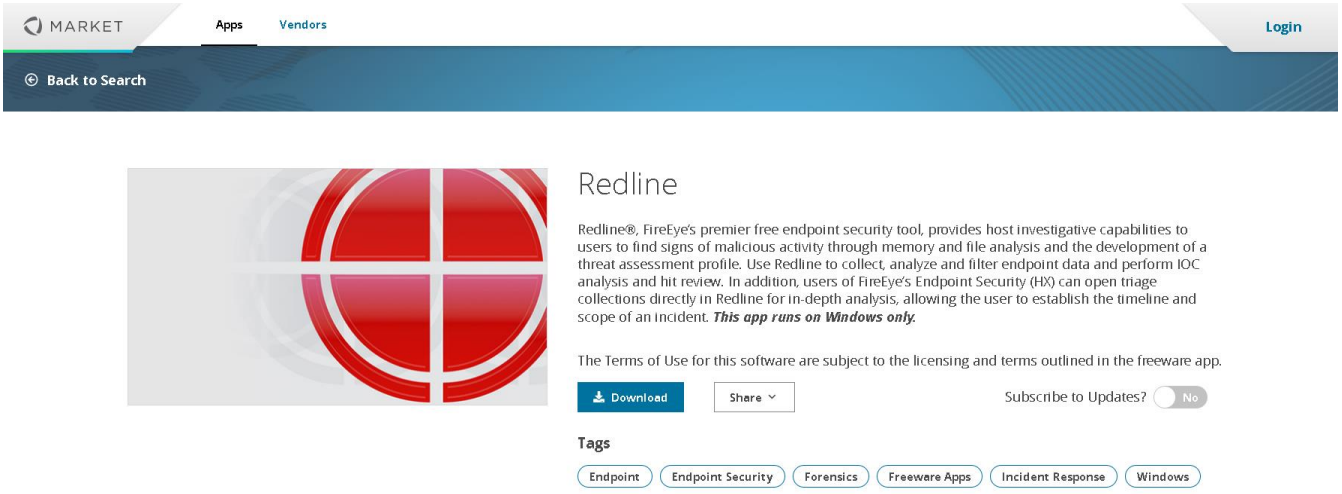
Objectives

- 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):

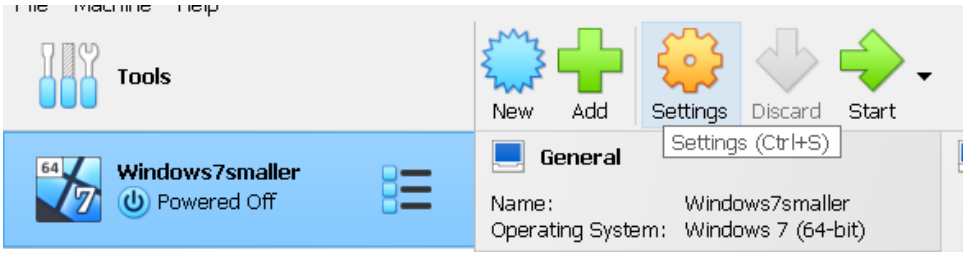
https://fireeye.market/apps/211364



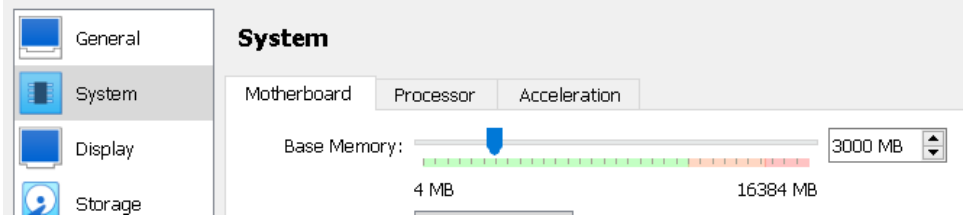
2. Open your infected raw file in Redline:

(**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:

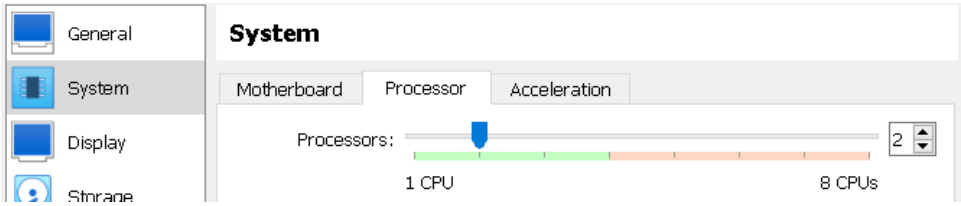
1. Shut down the virtual machine
2. Select your virtual machine and click settings



3. Go to system



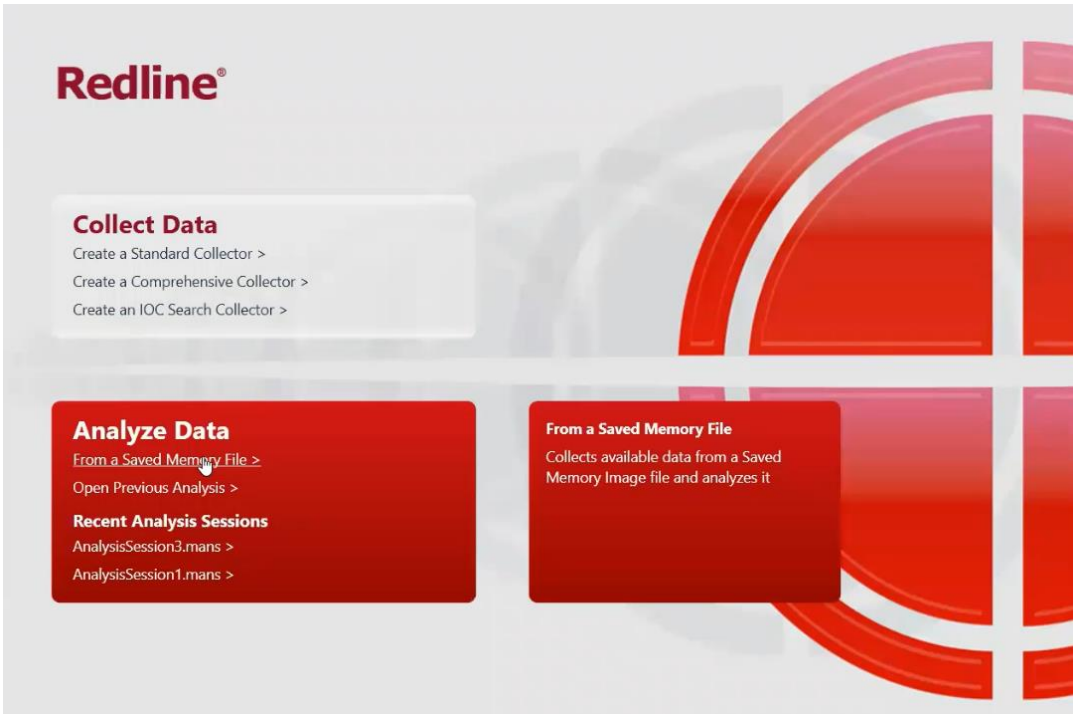
As long as the system has already been shut down, you can adjust the base memory. 3000MB should be enough.



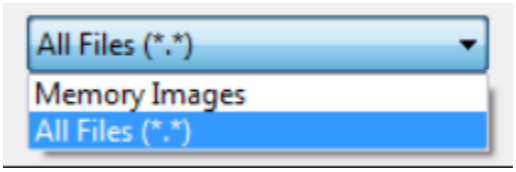
You can also add more processors. 2-4 should be enough.

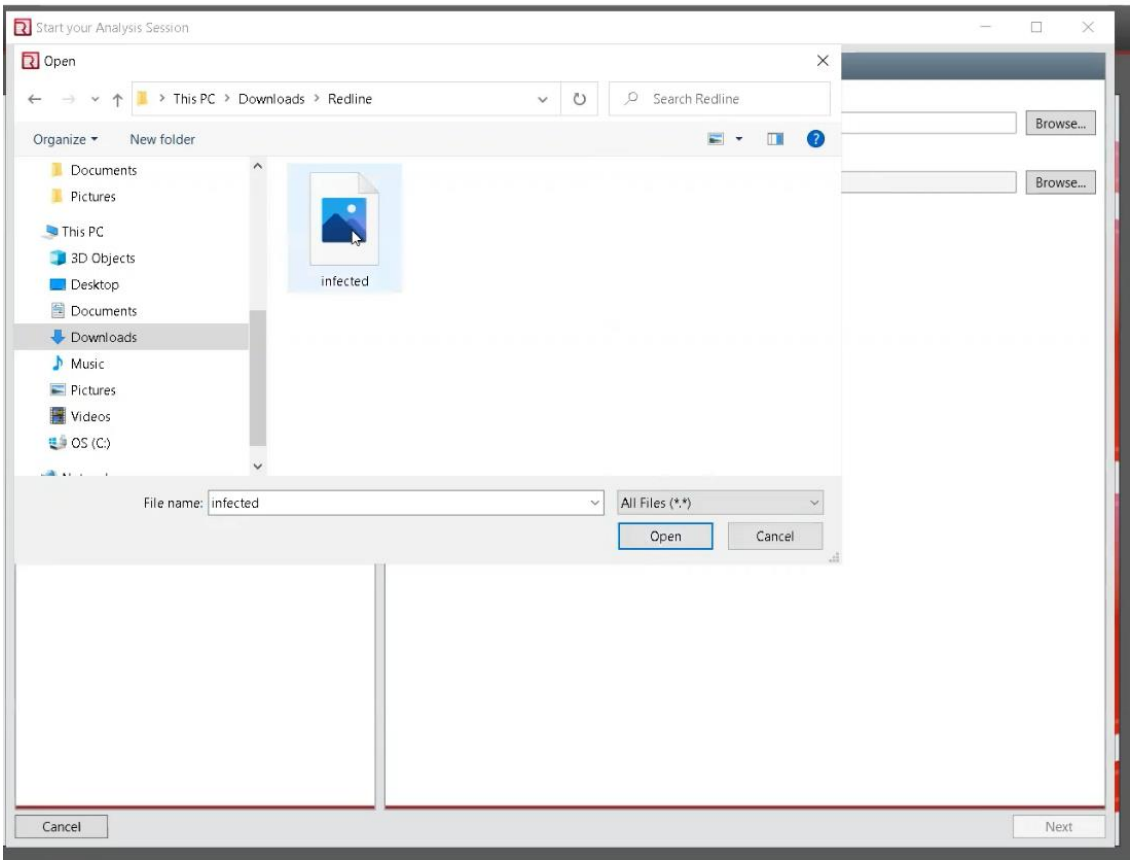
When you are done, you can open your virtual machine back up.

Click Analyze Data > From a Saved Memory File

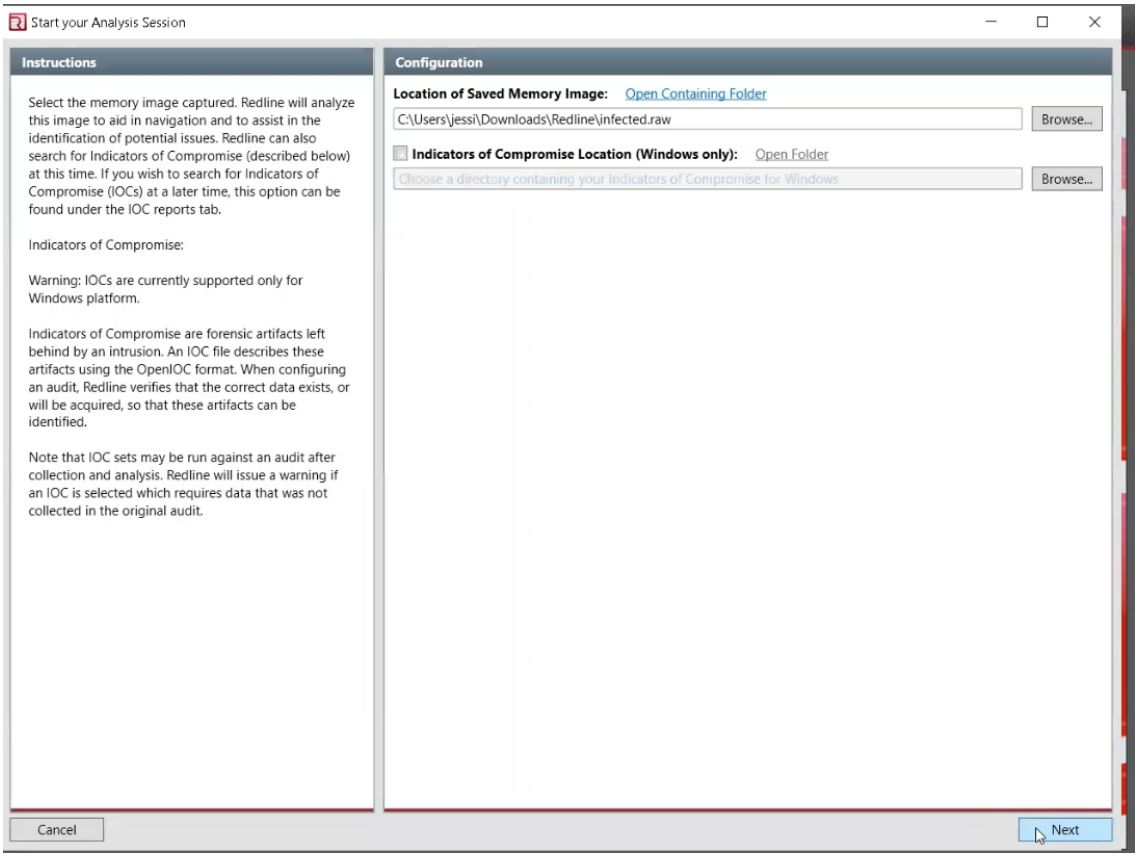


3. Navigate to your raw file by clicking “Browse” and selecting “All files” from the drop down menu next to “File name”. Now you should be able to see where your raw file is

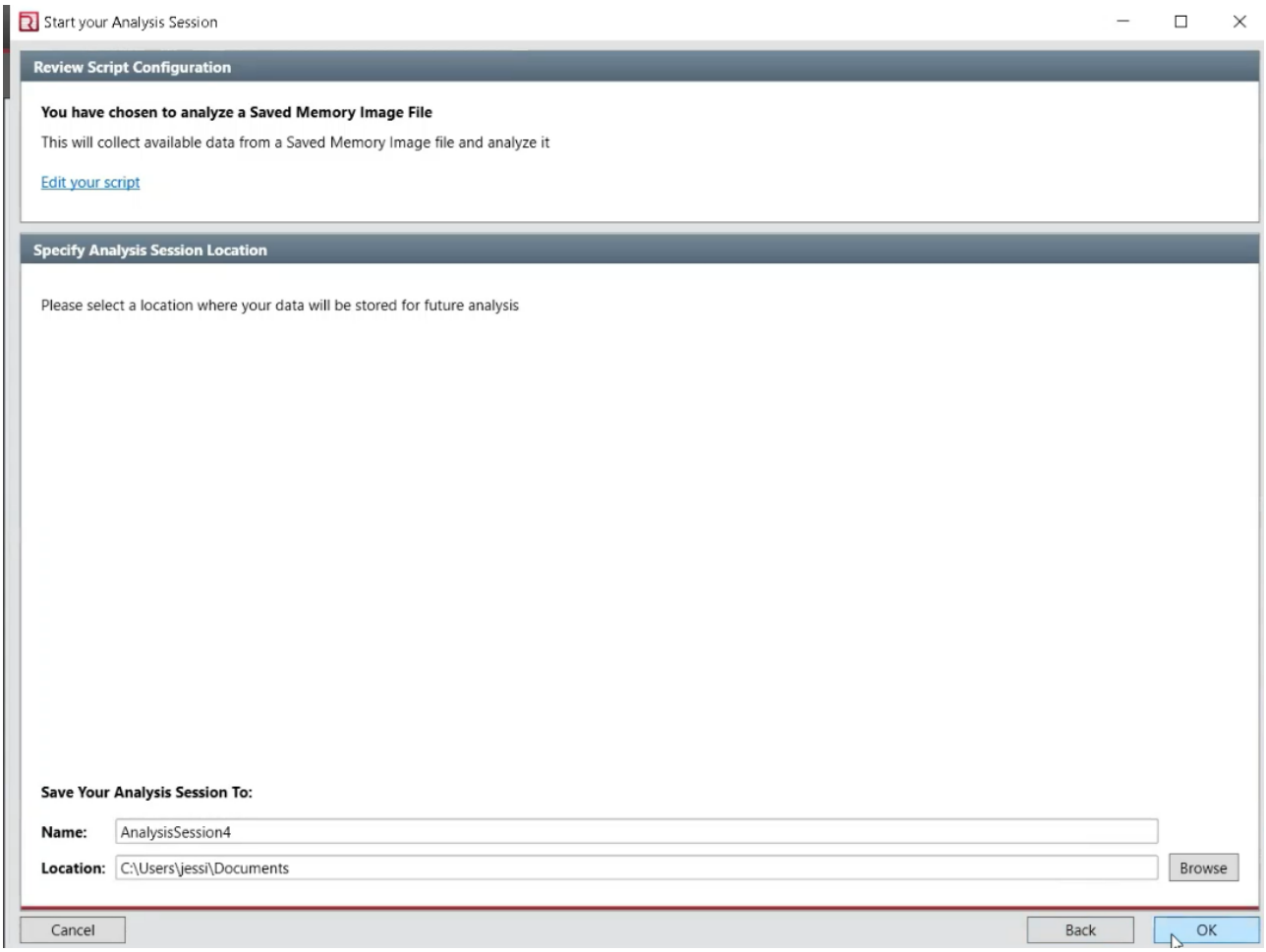




Now you can click “Open” and then “Next”

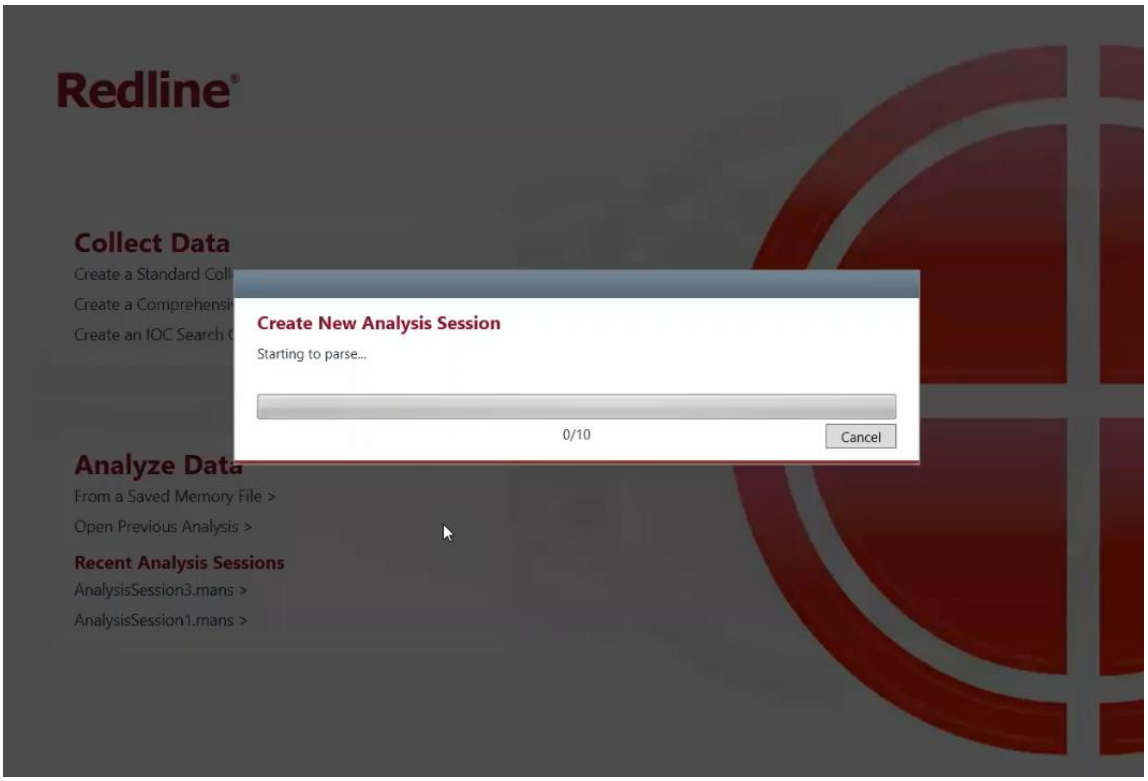


4. On this screen you can name your analysis file and decide where you want to save it by typing where it says “Name” or clicking “Browse”. When you have finished deciding, you can click “Ok”

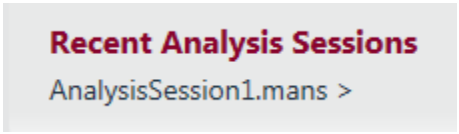


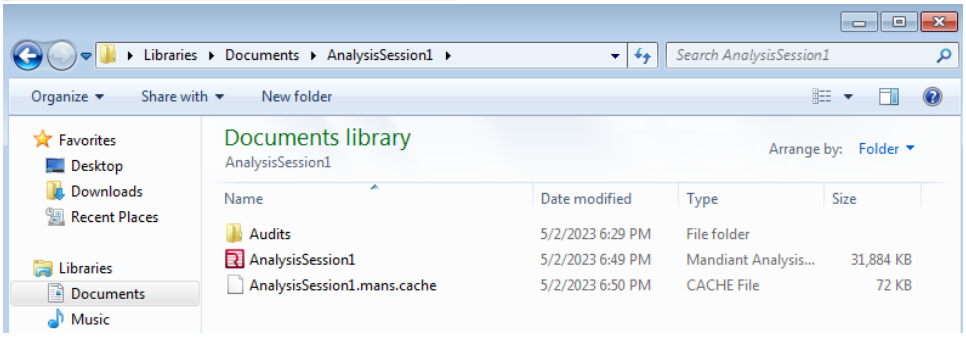
5. If you get a pop up, click “Yes”

6. Now you need to wait for your file to get processed.

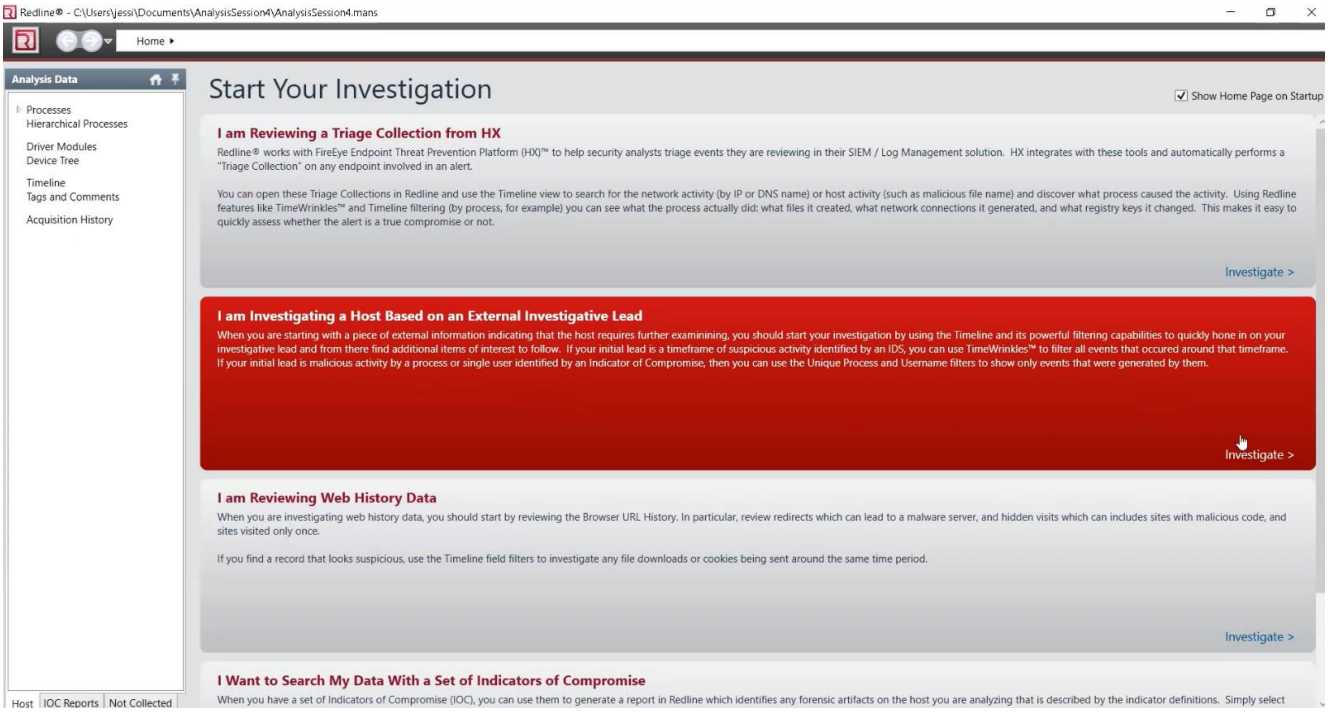


7. When it's done, open the session. You can open the session either on the home page of redline under "Recent Analysis Sessions" or you can open the file manually wherever you had it saved.

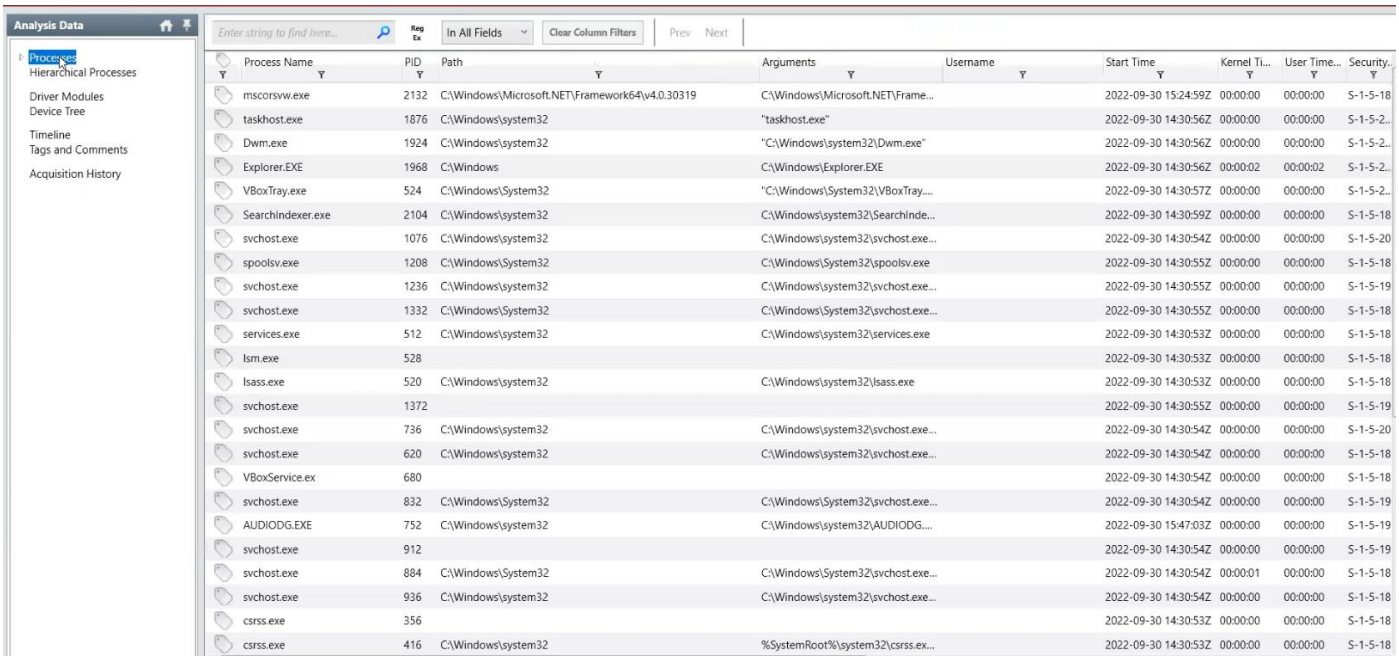




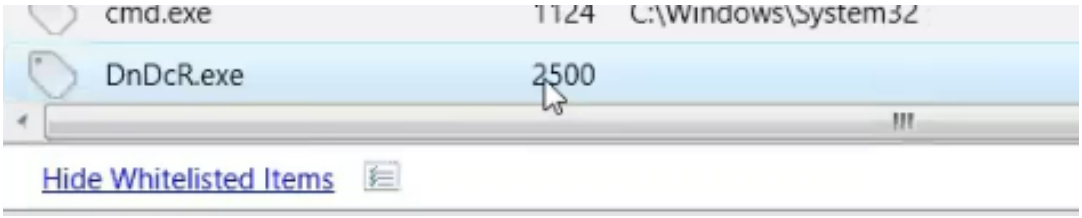
8. Click "I am Investigating a Host Based on an External Investigative Lead"



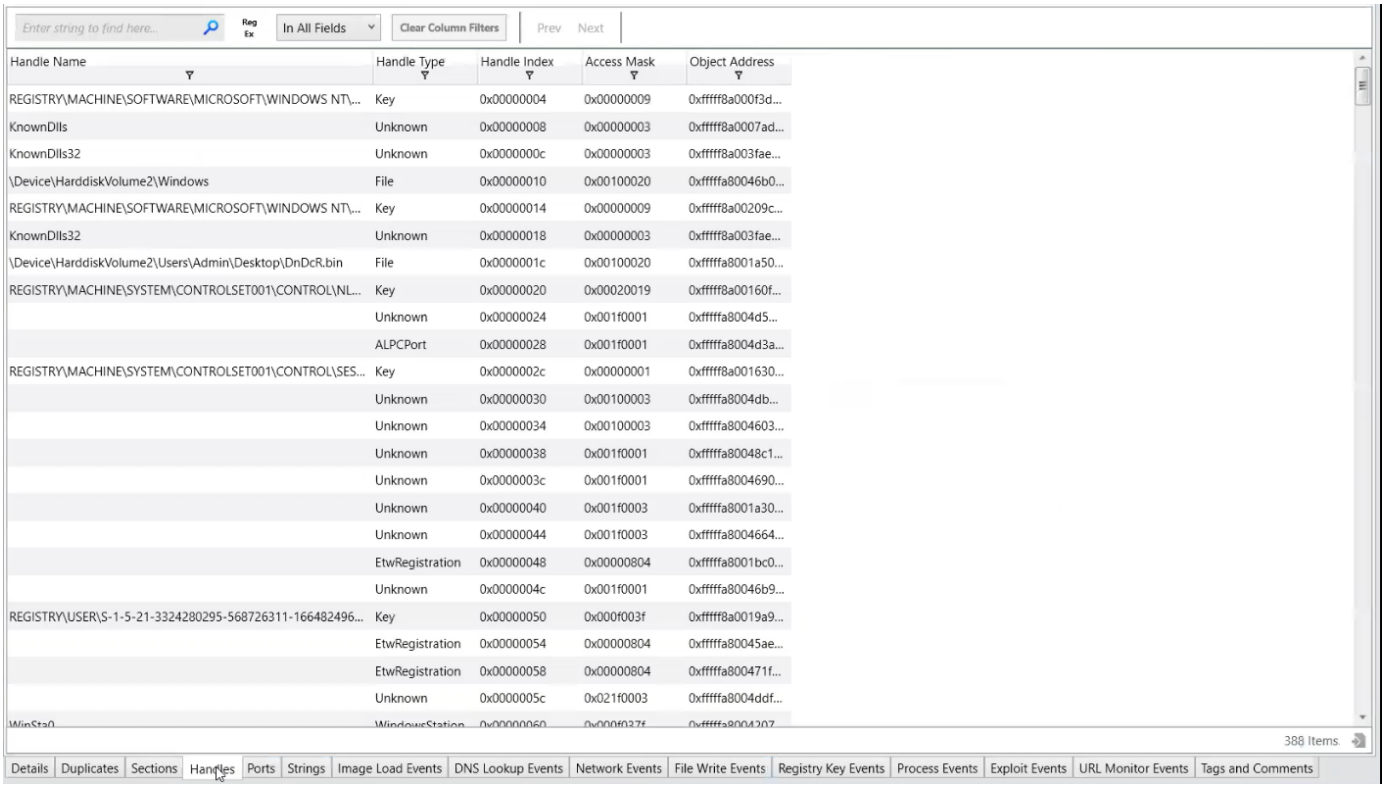
9. Click "Processes" on the top left to see all of the processes on the raw file



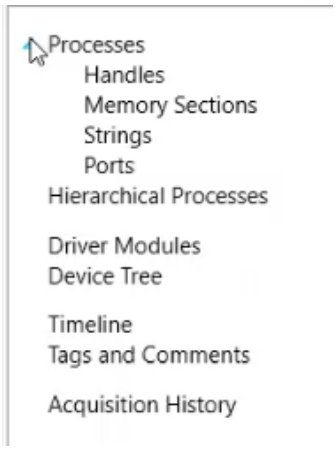
10. Double click the suspicious process



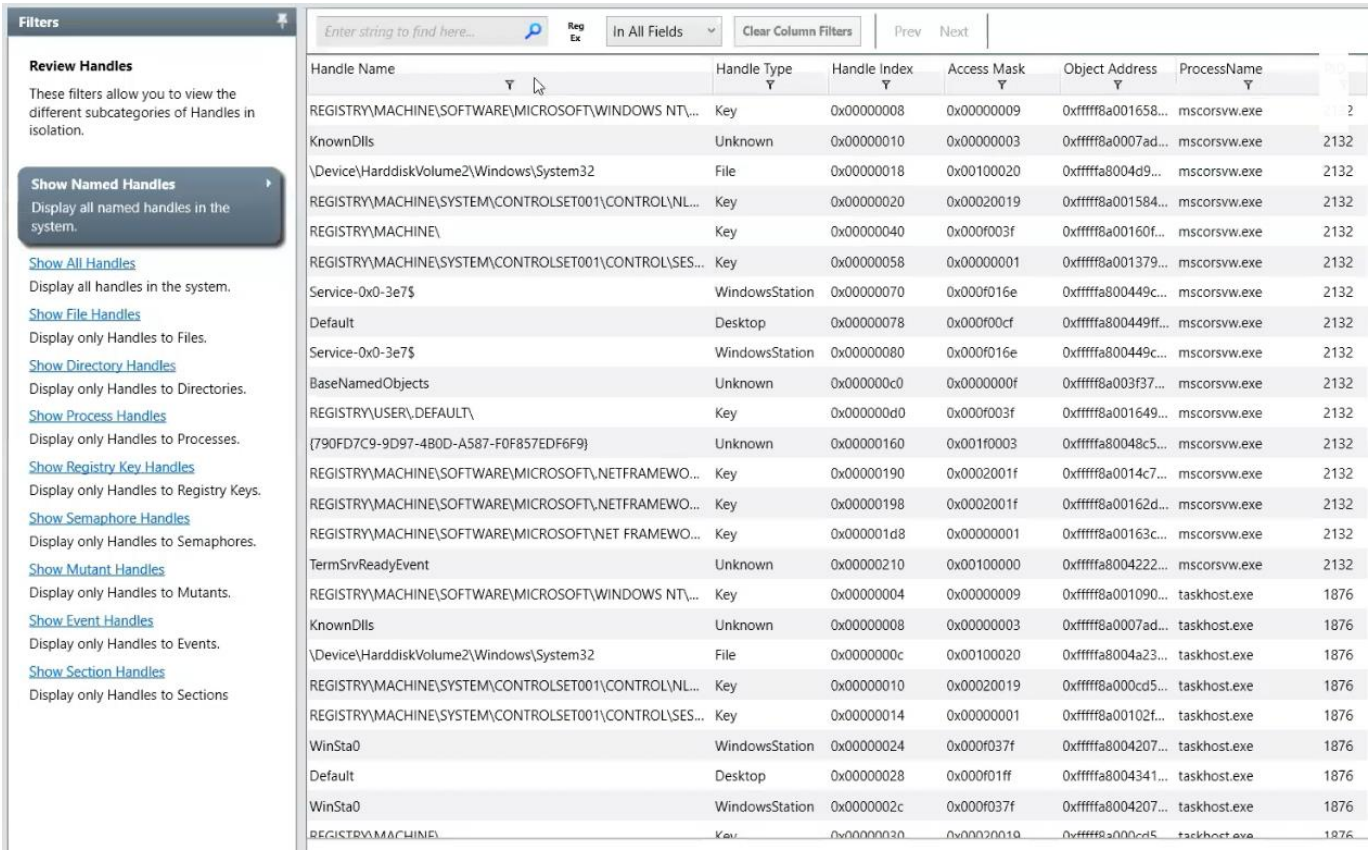
11. You can navigate through information on the process by clicking the tabs on the bottom



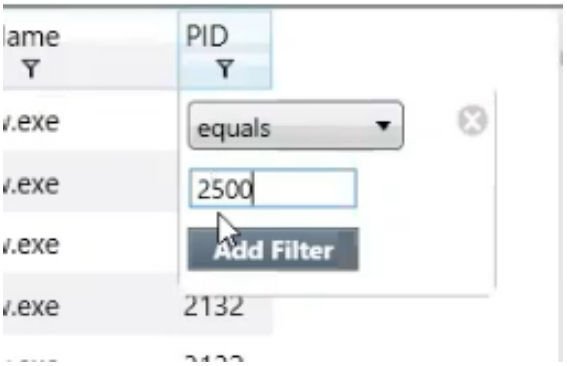
12. Now click the arrow next to “Processes” to open up the drop down menu and click “Handles”



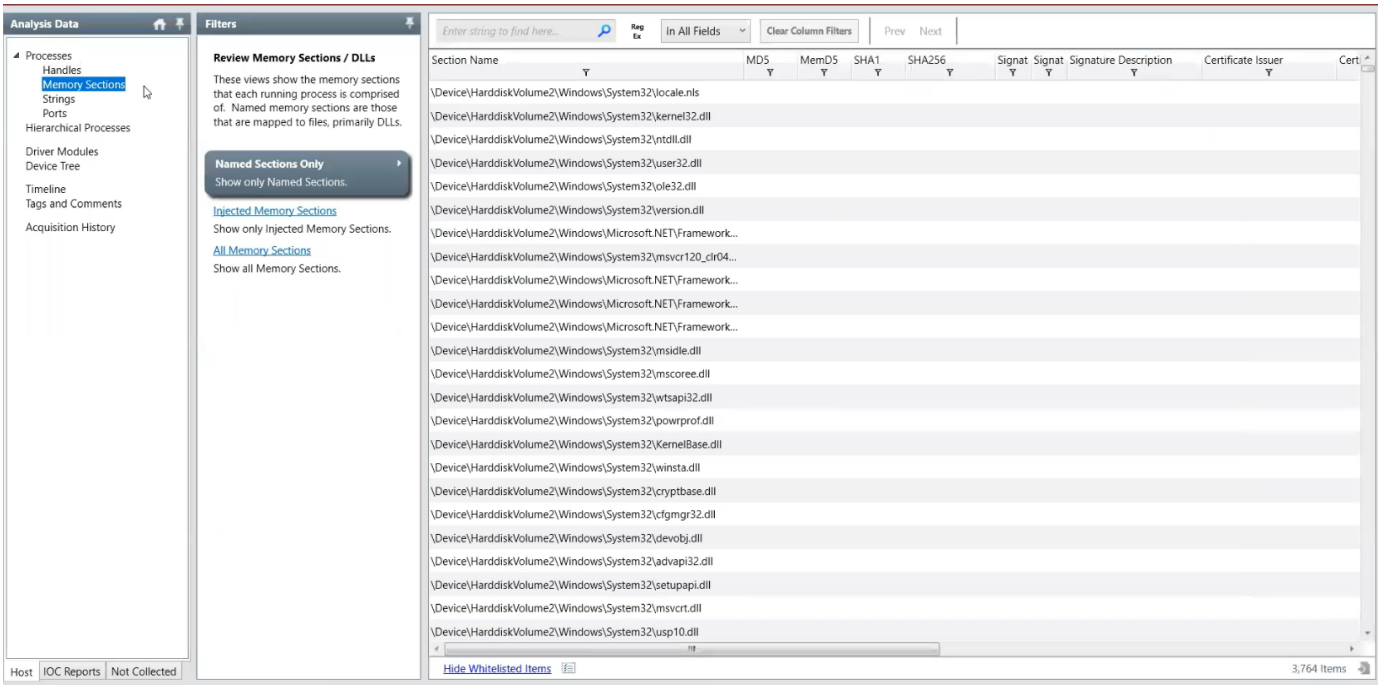
13. Now you can look through the handles of all of the processes



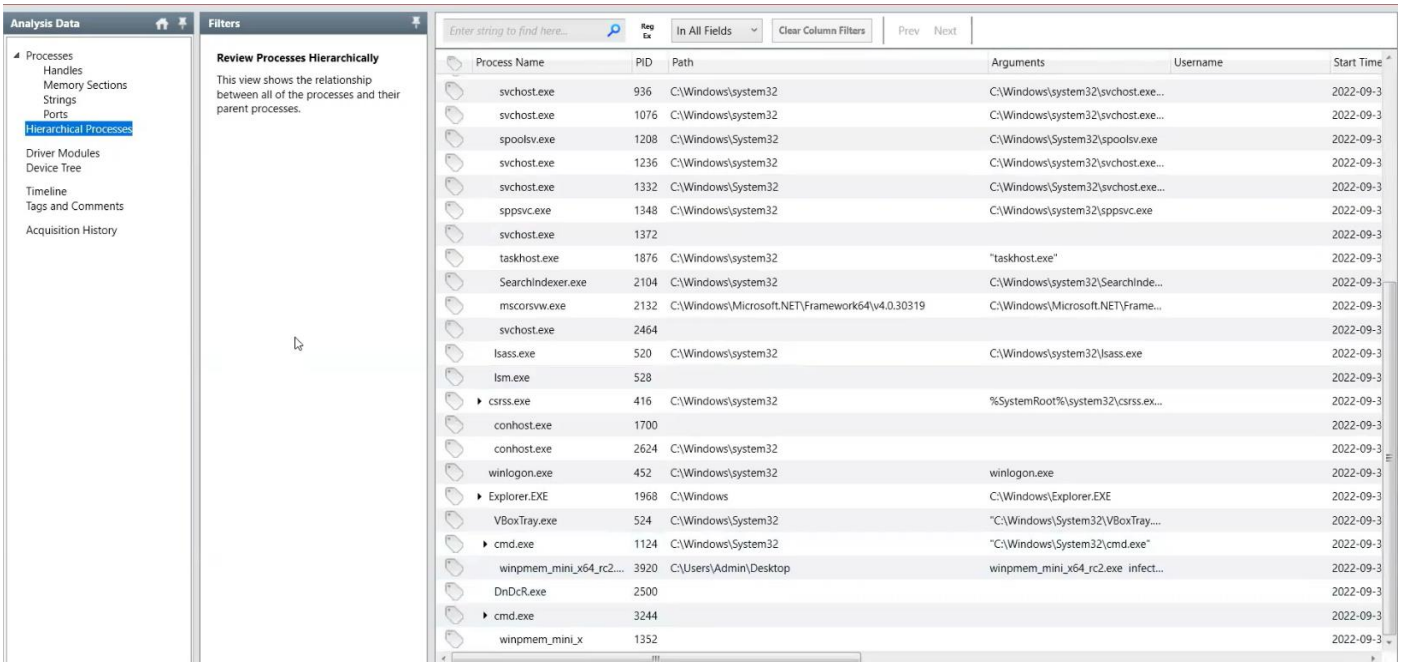
14. Double click on the small filter icon on the tabs to filter out what processes you want to see. Here I am using the PID that my malware’s process had and clicking “Add filter”. Your malware’s PID may be different



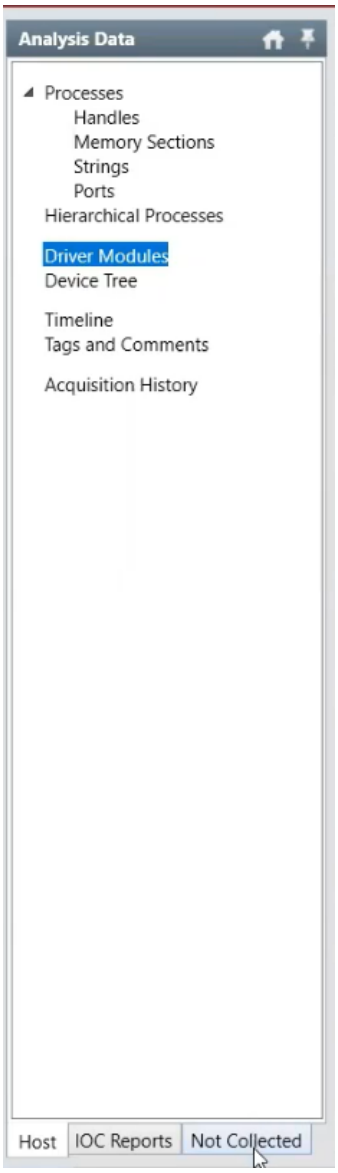
15. Click “memory sections” under processes on the top left to look at memory sections and DLLs



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.