Student:	Email:
Jake Simpson	jaksimps@iu.edu

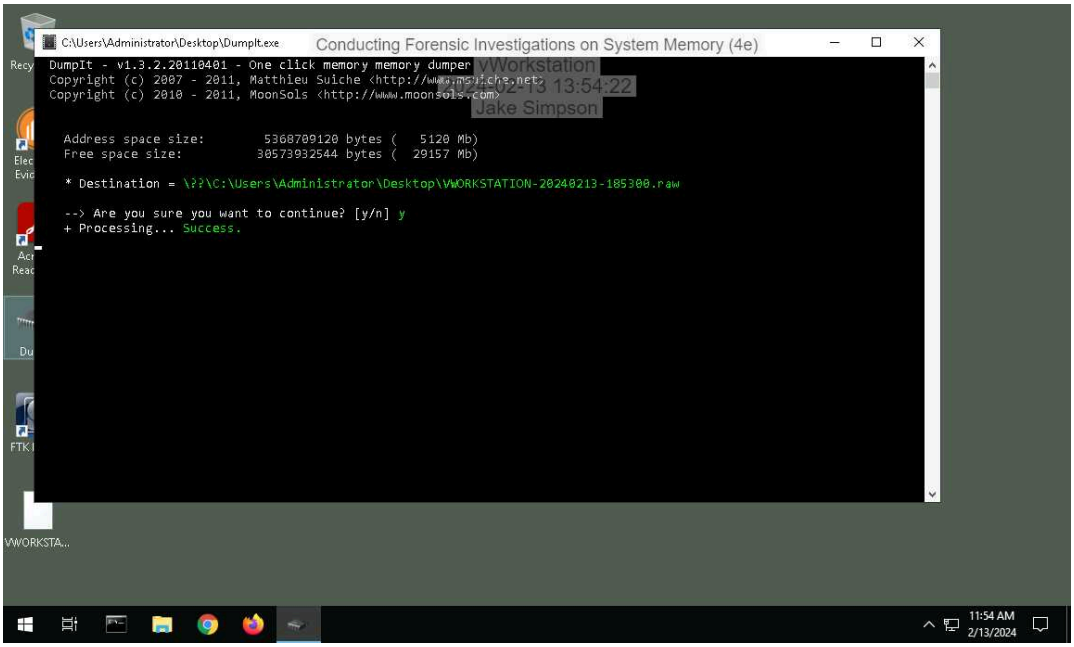
Time on Task:	Progress:
0 hours, 58 minutes	100%

Report Generated: Tuesday, February 13, 2024 at 2:47 PM

Section 1: Hands-On Demonstration

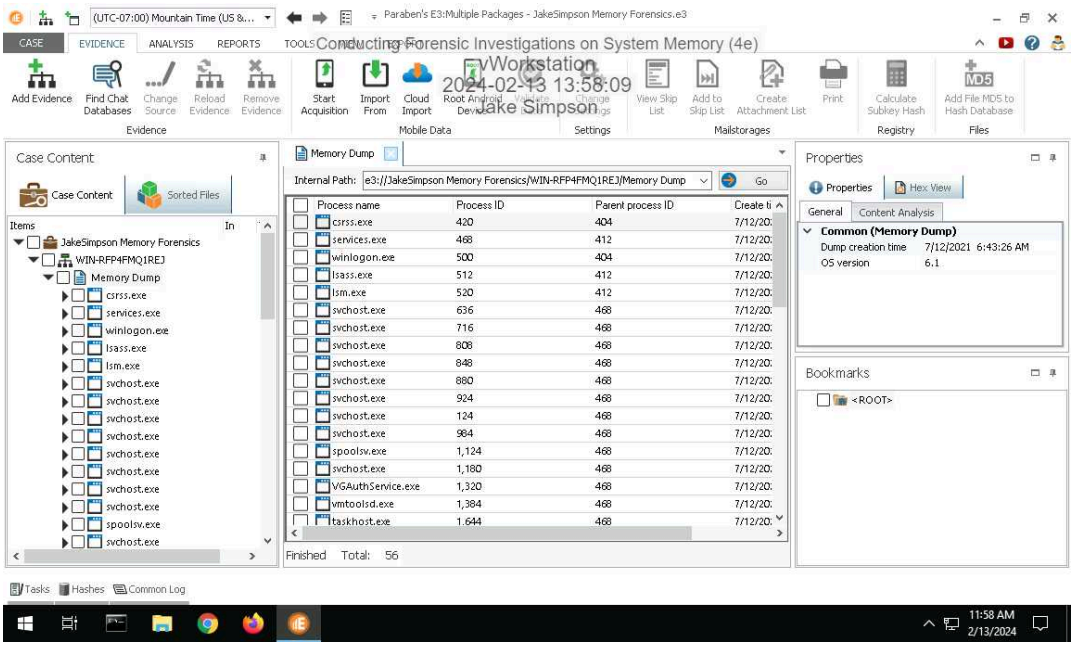
Part 1: Capture Memory using DumpIt

3. **Make a screen capture** showing the **DumpIt success notification**.



Part 2: Analyze Memory using E3

8. **Make a screen capture** showing the **list of processes in the memory dump**.



10. **Record** the start times for the oldest process and the newest process.

Oldest 7/12/2021 4:24:49
Newest 7/12/2021 6:42:43

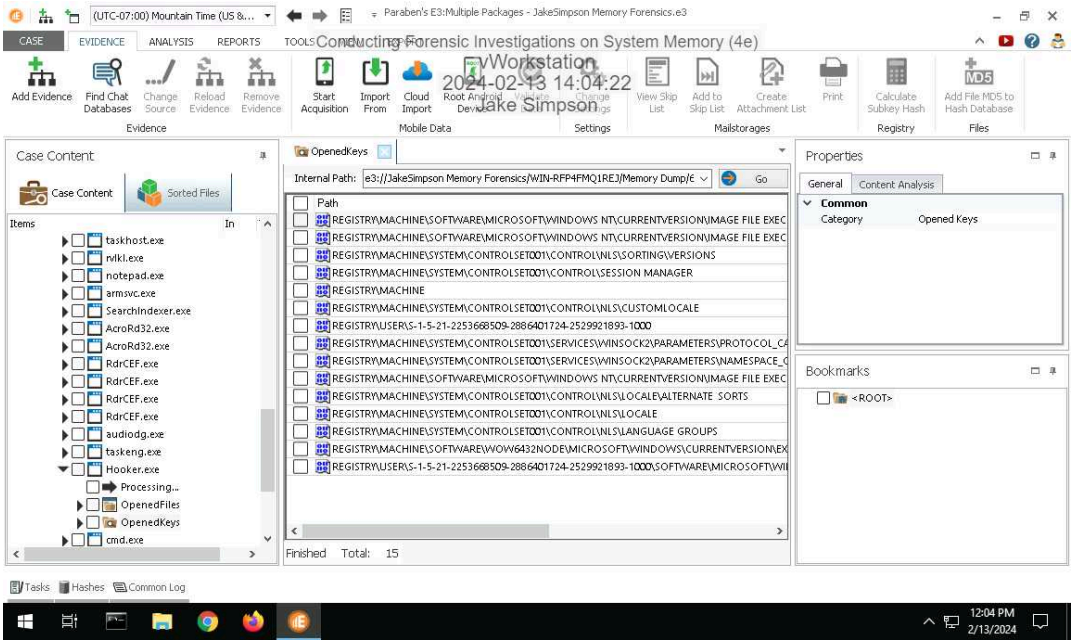
15. **Document** your findings for the conhost.exe process. What is it and what is it used for?

It is a legit process used to host the command prompt and powershell sessions.

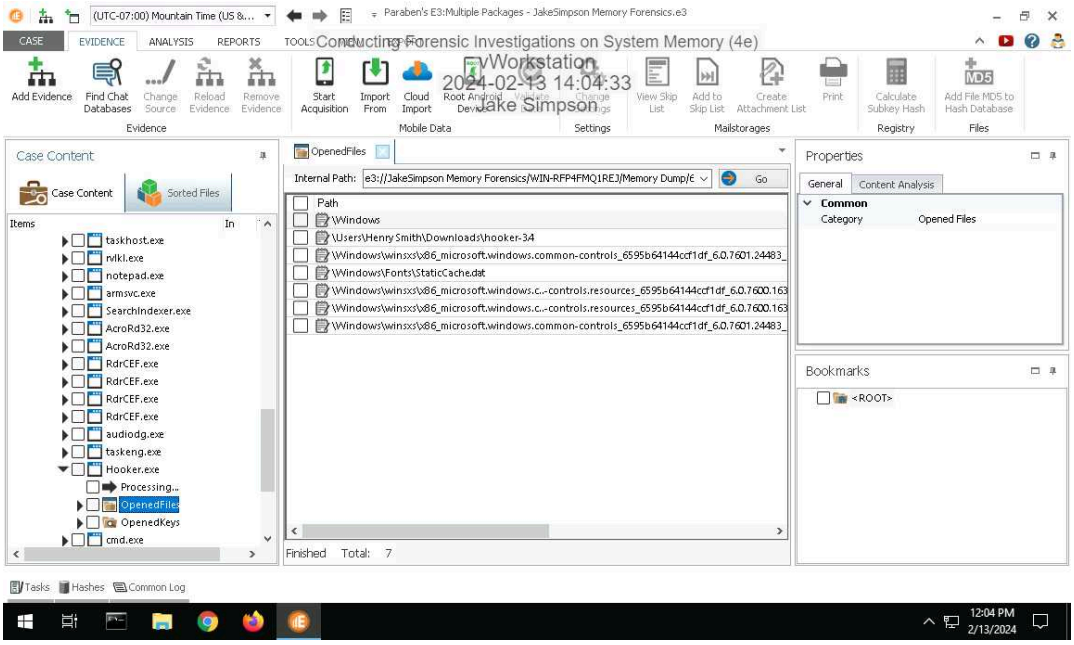
17. **Document** your findings for the hooker.exe process. What is it and what is it used for?

There is no hooker.exe system process. This could be malware

21. **Make a screen capture** showing the **registry keys opened by the Hooker.exe process**.



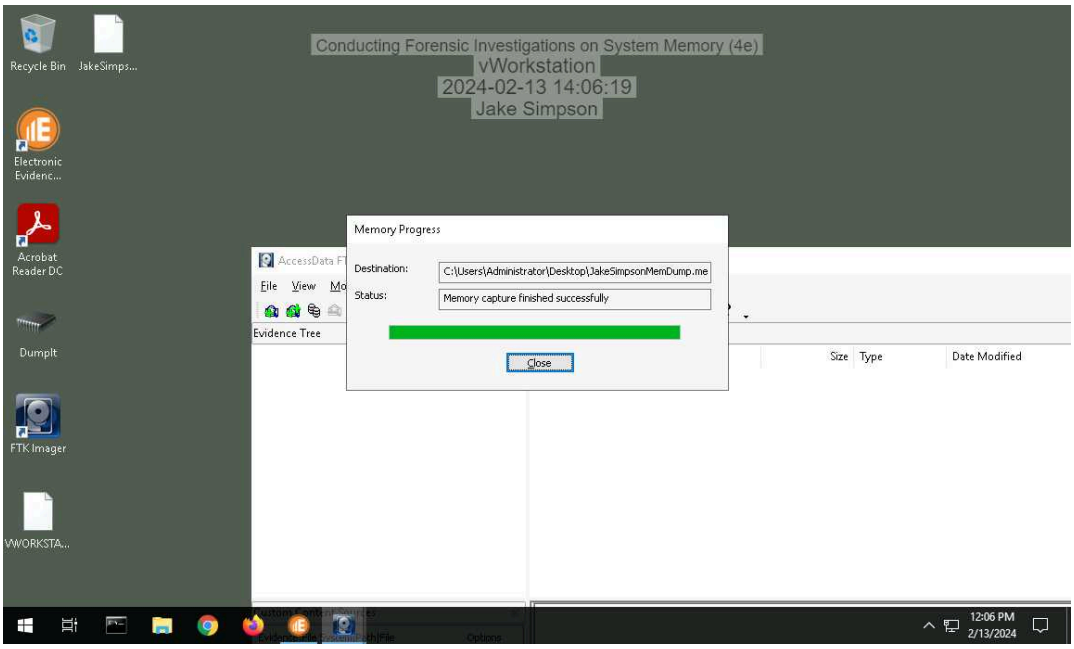
23. **Make a screen capture** showing the **files opened by the hooker.exe process**.



Section 2: Applied Learning

Part 1: Capture Memory using FTK Imager

6. **Make a screen capture** showing the ***Memory capture finished successfully*** **confirmation.**



Part 2: Analyze Memory using Volatility

7. **Document** your findings for the rvlkl.exe process. What is it and what is it used for?

PID: 4224 PPID: 1940 Threads: 2

It is the executable file associated with Kapersky Anti-Virus software

9. **Document** whether any processes are flagged as hidden.

None are flagged as hidden they all have the True value

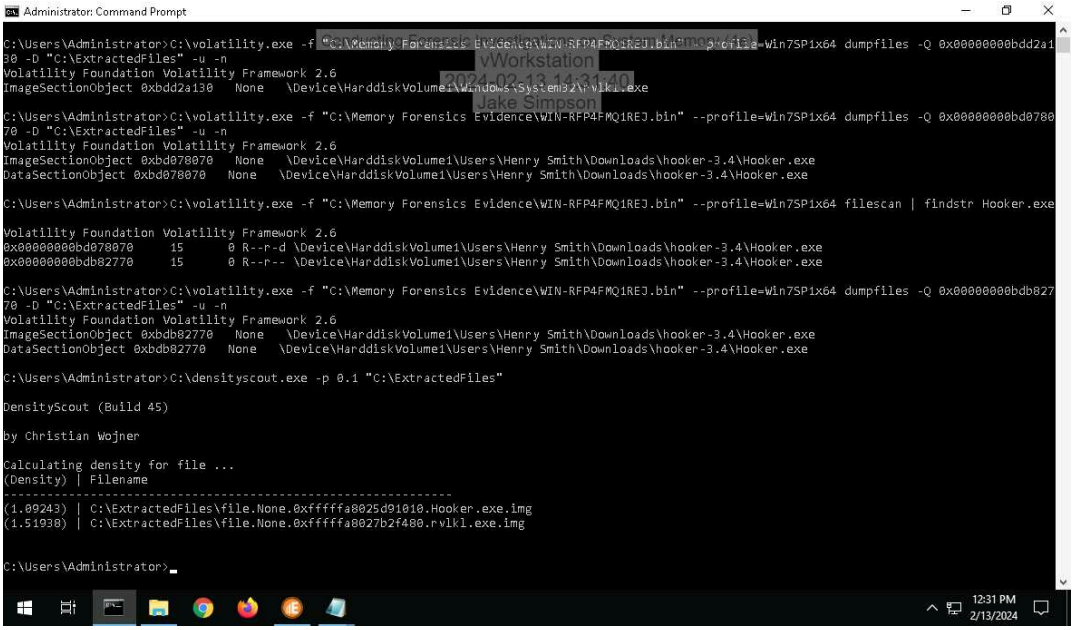
12. **Document** whether the netscan module displays network usage associated with the Hooker.exe or rvlkl.exe processes.

It does not

15. **Document** any information you were able to gather about port 56610.

Ports 49151 and above are typically used for private services. So it is being used by a custom application.

26. **Make a screen capture** showing the **DensityScout results**.



Section 3: Challenge and Analysis

Part 1: Identify Malicious Connections

Document the three processes that connected to 205.134.253.10:4444.

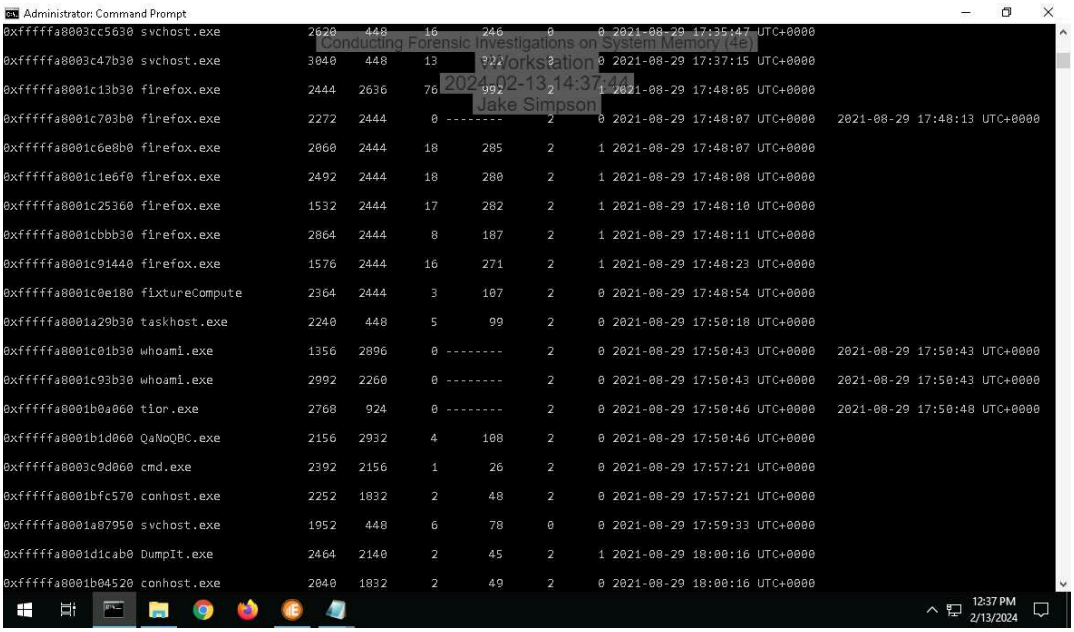
The processes that connected are 0x7fa9a3d0, 0x7fd01010, 0x7fd01a30

Document the name and purpose of the software you discovered.

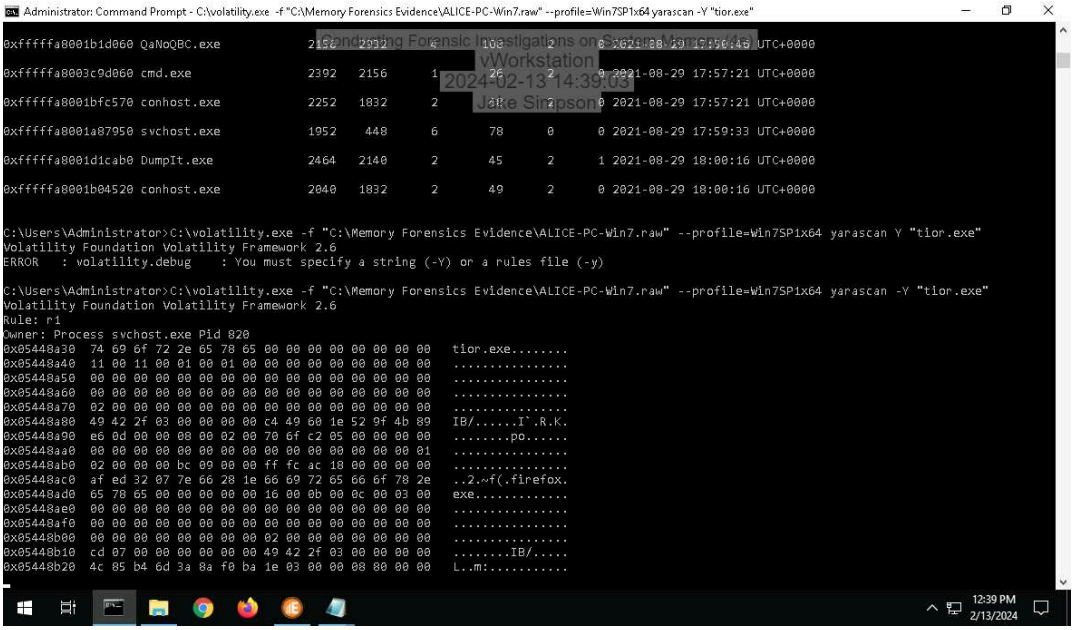
Metasploit Framework will often use port 4444

Part 2: Identify Malicious Processes

Make a screen capture showing the **fixtureComputer.exe process, and all those below it, in the pslist output.**



Make a screen capture showing the **output of the yarascan**.



Part 3: Identify Privilege Escalation

Make a screen capture showing the **output of your privilege comparison**.