Student:	Email:
Imani Williams	imanilw13@gmail.com

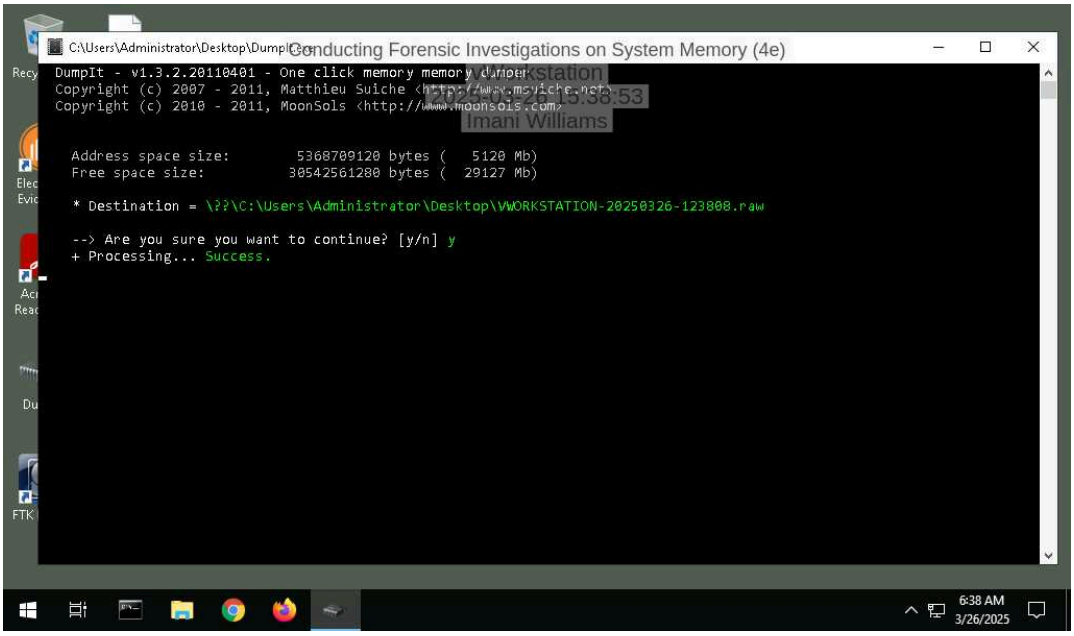
Time on Task:	Progress:
1 hour, 50 minutes	100%

Report Generated: Wednesday, March 26, 2025 at 10:23 AM

Section 1: Hands-On Demonstration

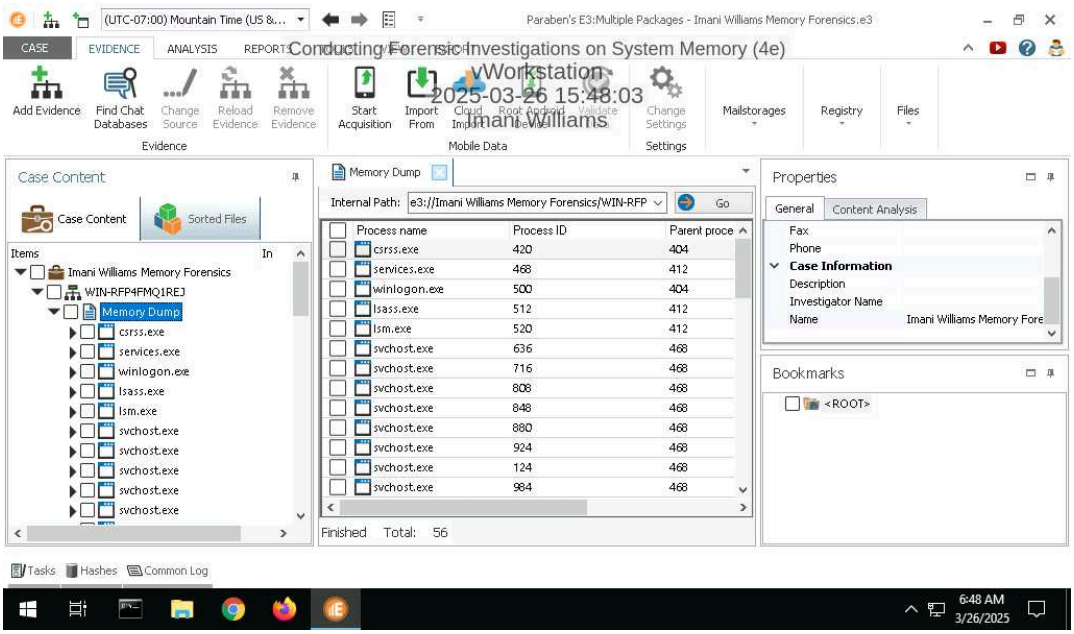
Part 1: Capture Memory using DumpIt

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.

The oldest process running on the system is System, which was created on July 12, 2021, at 4:24:49 AM. The newest process is conhost.exe, created on July 12, 2021, at 6:42:43 AM.

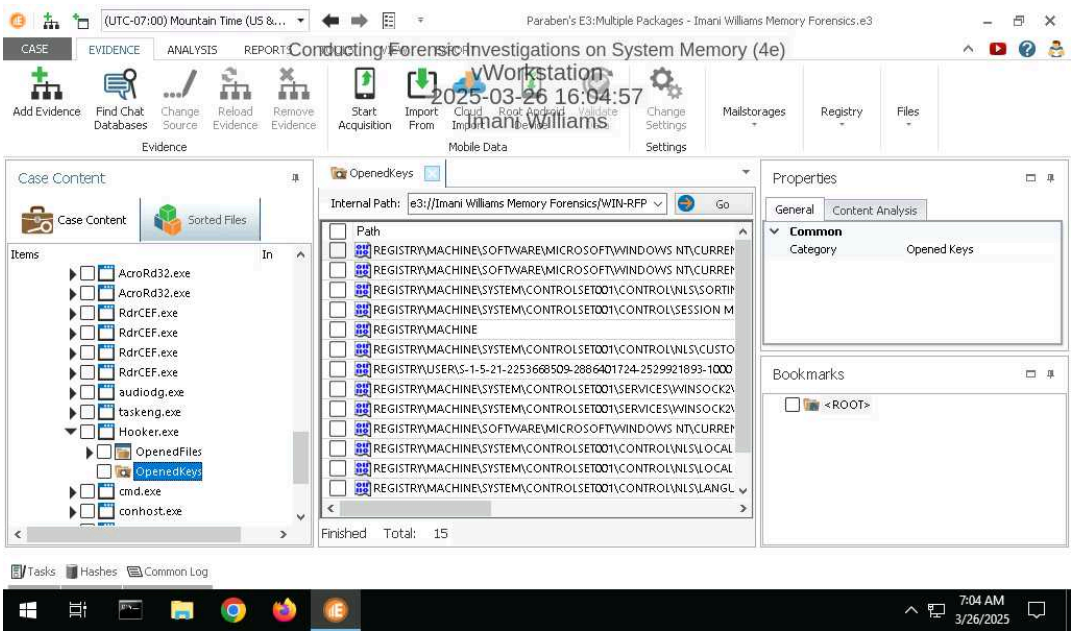
15. **Document** your findings for the conhost.exe process. What is it and what is it used for?

The conhost.exe (Console Window Host) process is a legitimate Windows system process that manages command-line interface windows, such as Command Prompt (cmd.exe) and PowerShell. It acts as a bridge between the command-line applications and the Windows graphical interface to ensure compatibility and security.

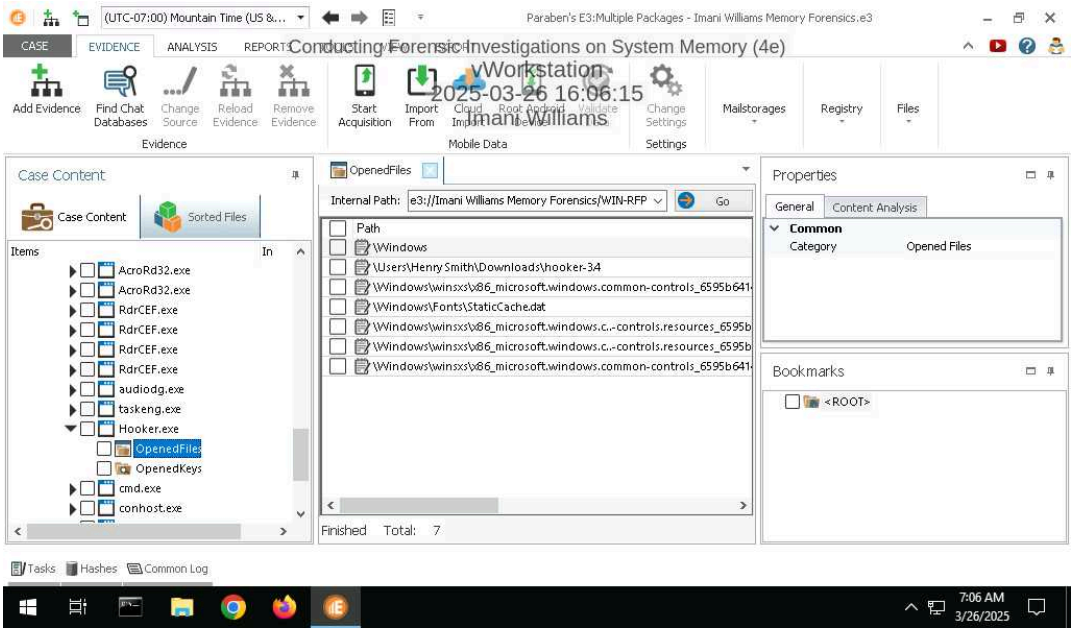
17. **Document** your findings for the hooker.exe process. What is it and what is it used for?

hooker.exe is an illegitimate Windows system file and can be considered as an evidence of malicious usage. It typically accompanies keyloggers or spyware for tracking and logging the user input like keystrokes and using it in unauthorized manners or stealing data.

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



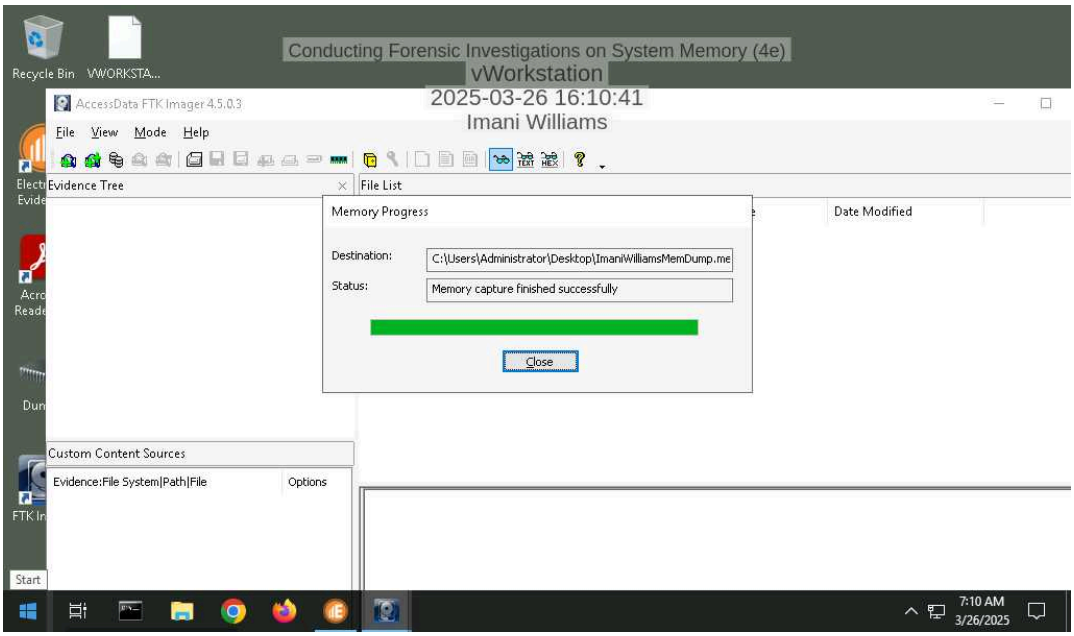
23. **Make a screen capture** showing the **files opened by the hooker.exe process**.



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?

The rvlkl.exe process is associated with Revealer Keylogger by Logixoft, a monitoring program for keystroke logging and activity of the user. It is normally utilized for parental control, employee monitoring, and security. The basic version is free, while the Complete paid version has additional features like screenshot capture and log delivery through remote. It is located in "C:\\Windows\\System32\\rvlkl.exe" by default, while the paid version is concealed.

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

No processes were identified as hidden when they were analyzed. All processes that were being executed were visible and listed in the system task manager and forensic utilities without any indication of stealth or hidden processes reflecting malicious purposes.

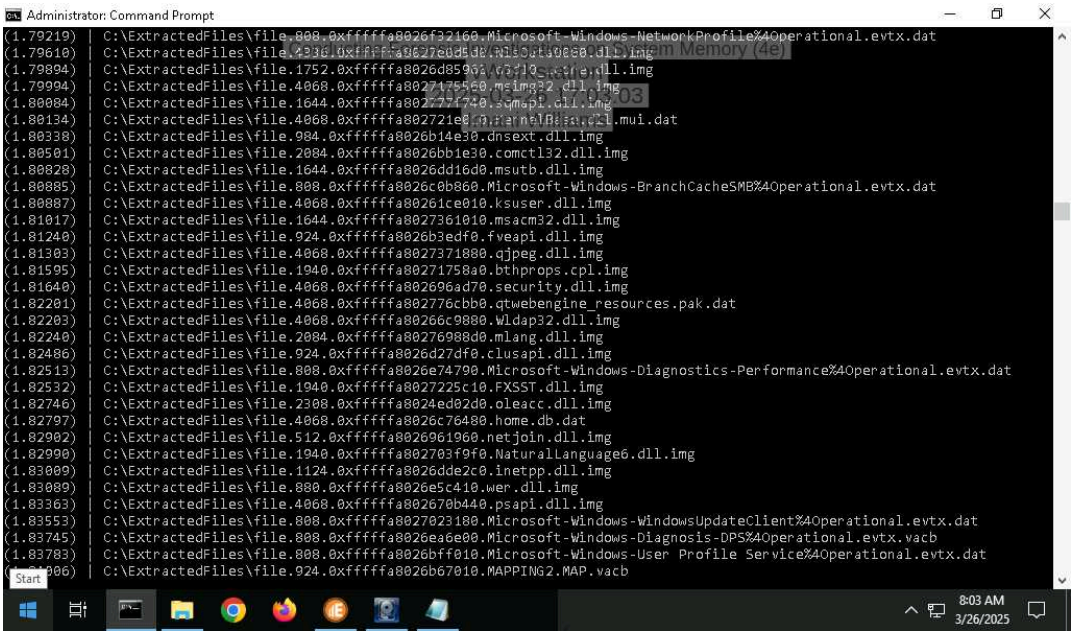
12. **Document** whether the netscan module displays network usage associated with the Hooker.exe or rvlkl.exe processes.

The netscan module checks network traffic concerning both the hooker.exe and rvlkl.exe processes. This implies that these programs are presently exchanging information over the network, perhaps sending logged data or receiving remote commands.

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

Port 56610 is a dynamic (transient) port that uses the Transmission Control Protocol (TCP), which is one of TCP/IP networks' main protocols. It is typically allocated temporarily for outgoing network communication and allows user data to be sent bi-directionally on the connection. While it is not associated with any known services, it may be used by programs for data transfer, remote sessions, or potential malware activity.

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.

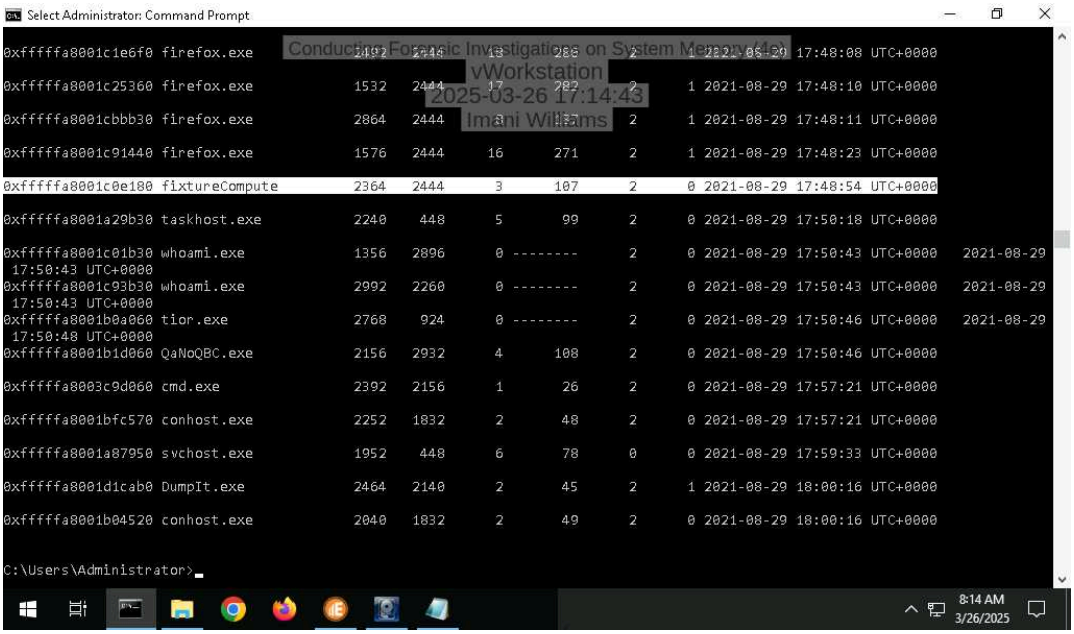
The analysis identified three processes: dllhost.exe, QaNoQBC.exe, and fixtureCompute, that established a connection to the IP address 205.134.253.10 on port 4444

Document the name and purpose of the software you discovered.

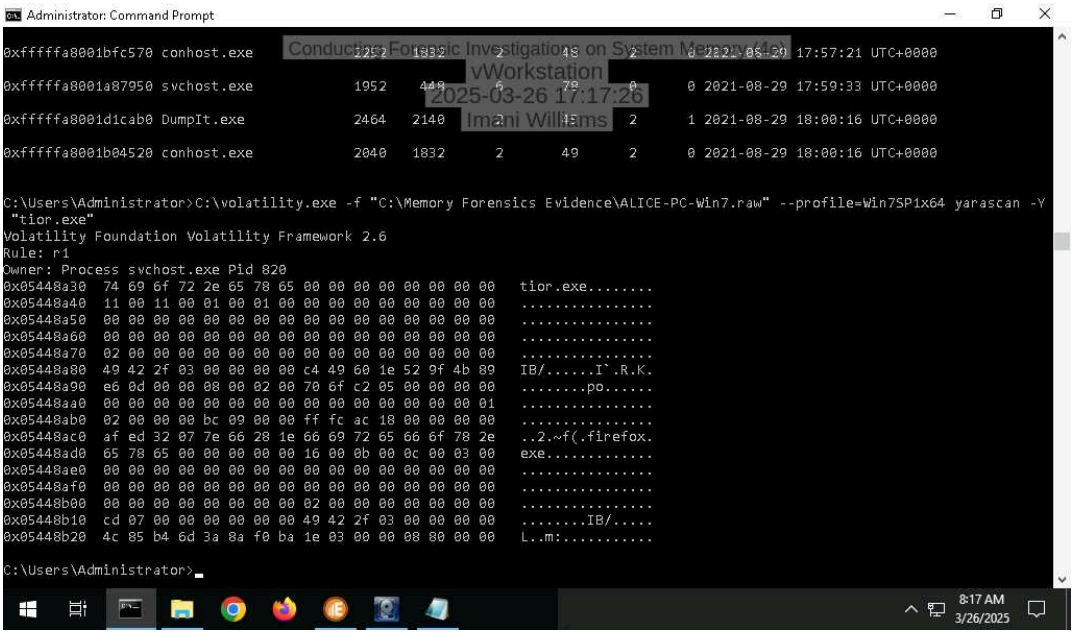
The analysis revealed that port 4444 is commonly associated with Metasploit, a penetration testing framework often used for exploits, payload delivery, and establishing reverse shells. The connection to 205.134.253.10:4444 suggests that the system may have been compromised.

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**.