Student:	Email:
Alexis Cherpes	cherpea@ferris.edu

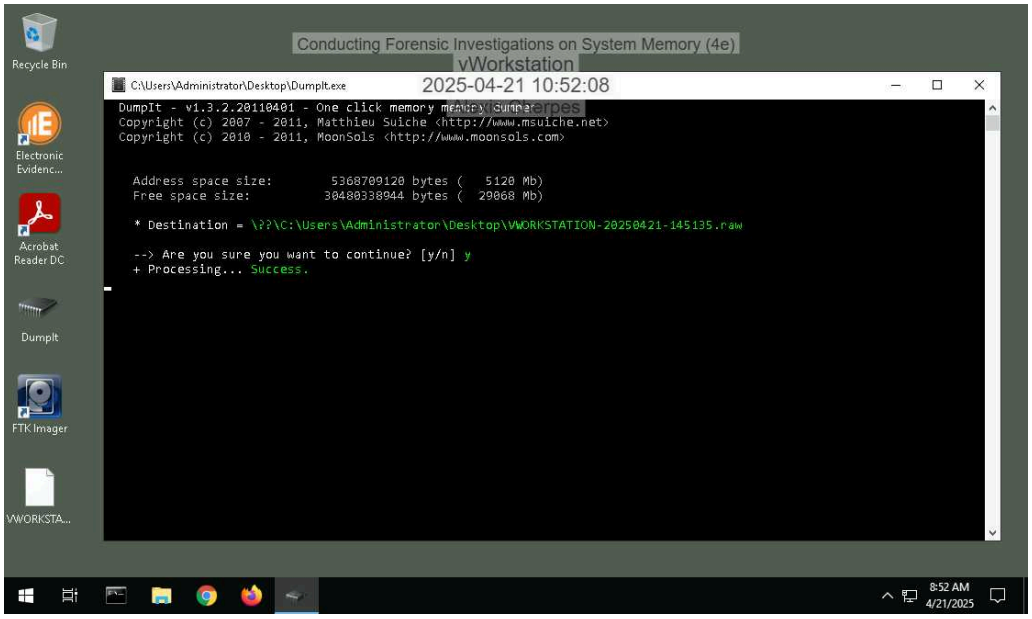
Time on Task:	Progress:
4 hours, 2 minutes	100%

Report Generated: Thursday, May 22, 2025 at 4:51 PM

Section 1: Hands-On Demonstration

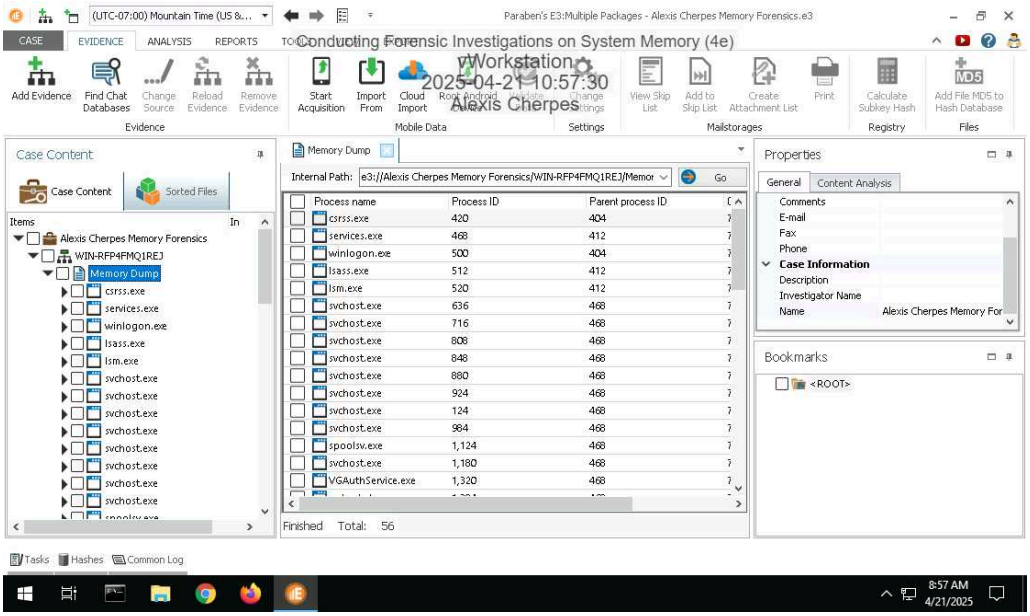
Part 1: Capture Memory using DumpIt

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: System 7/12/2021 4:24:29AM Newest: conhost.exe 7/12/2021 6:42:43AM

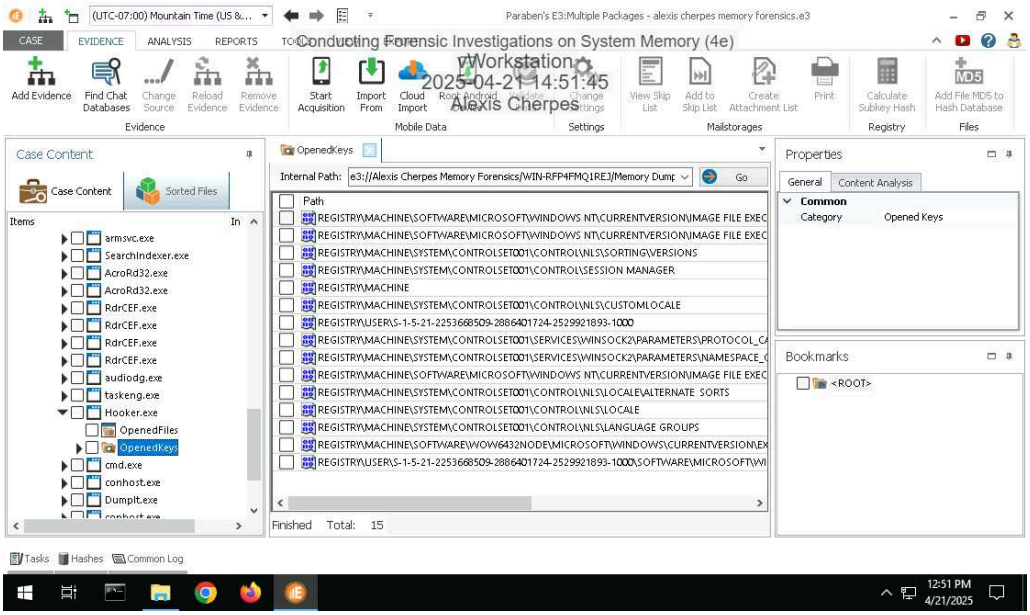
15. **Document** your findings for the conhost.exe process. What is it and what is it used for?

It is a key windows process that helps manage console windows on your computer screen including command prompt and powershell.

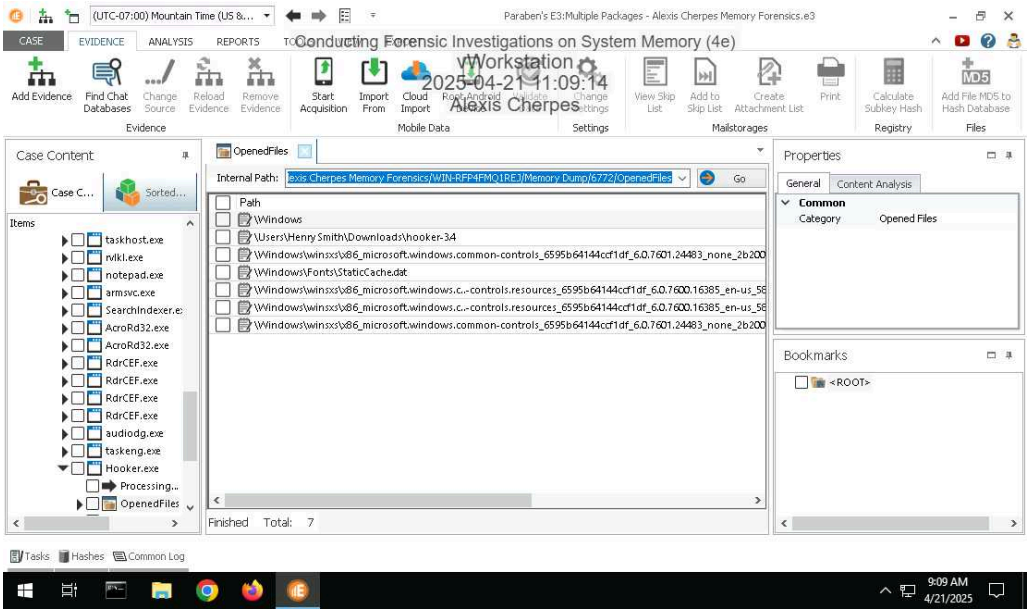
17. **Document** your findings for the hooker.exe process. What is it and what is it used for?

Hooker.exe functions as both a trojan and a keylogger. It is not a legitimate Windows system file. The program can connect to the internet, log keyboard and mouse activity, and monitor running applications. It is considered to pose a maximum-security risk.

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



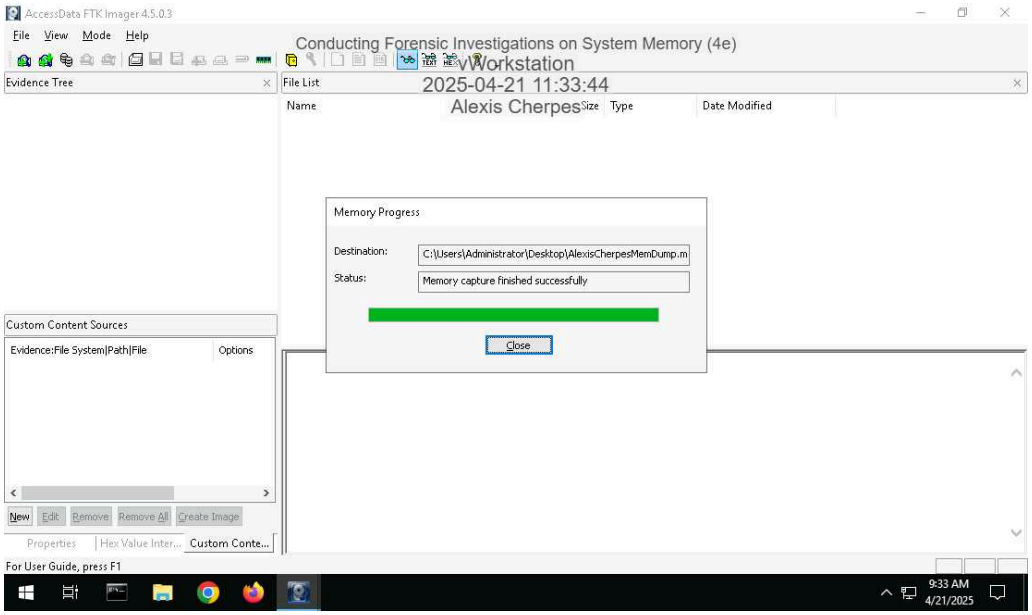
23. **Make a screen capture** showing the **files opened by the hooker.exe process**.



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?

rvlkl.exe is associated with a keylogger and is considered potentially dangerous. It is not a critical Windows component and can often lead to system issues. This process is known as Revealer Keylogger Free and is designed to capture keyboard and mouse input, as well as monitor running applications.

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

There are no hidden processes since pslist flag is not set to false for any process.

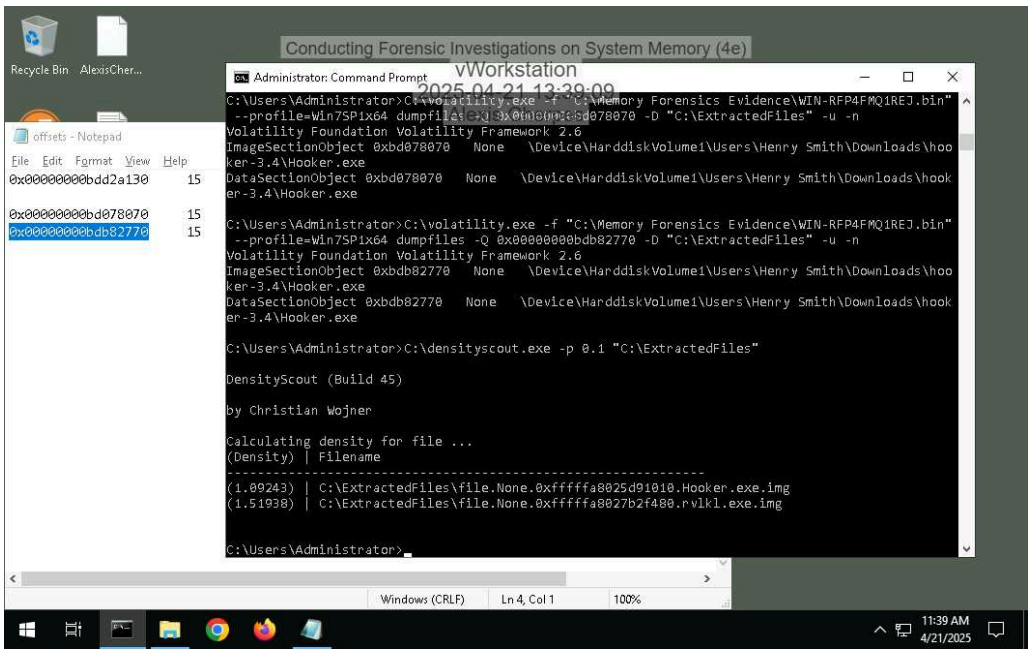
12. **Document** whether the netscan module displays network usage associated with the Hooker.exe or rvlkl.exe processes.

Based on the pid of rvlkl.exe, 4224, and hooker.exe, 6772, there is no indication that these processes were involved in any network activity.

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

Port 56610 is not officially assigned to any specific protocol or service by the IANA. It falls within the dynamic or ephemeral port range (49152–65535), which is typically used for temporary, client-side connections. The actual use of port 56610 depends entirely on the software or process that initiates the connection.

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.

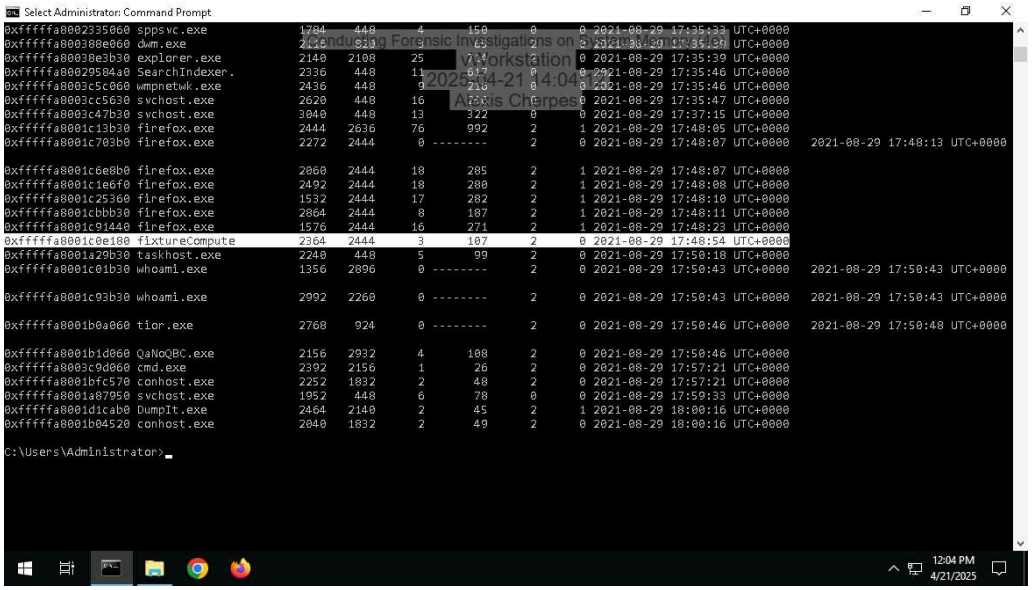
1. dlhost.exe 2. QaNoQBC.exe 3. fixtureCompute

Document the name and purpose of the software you discovered.

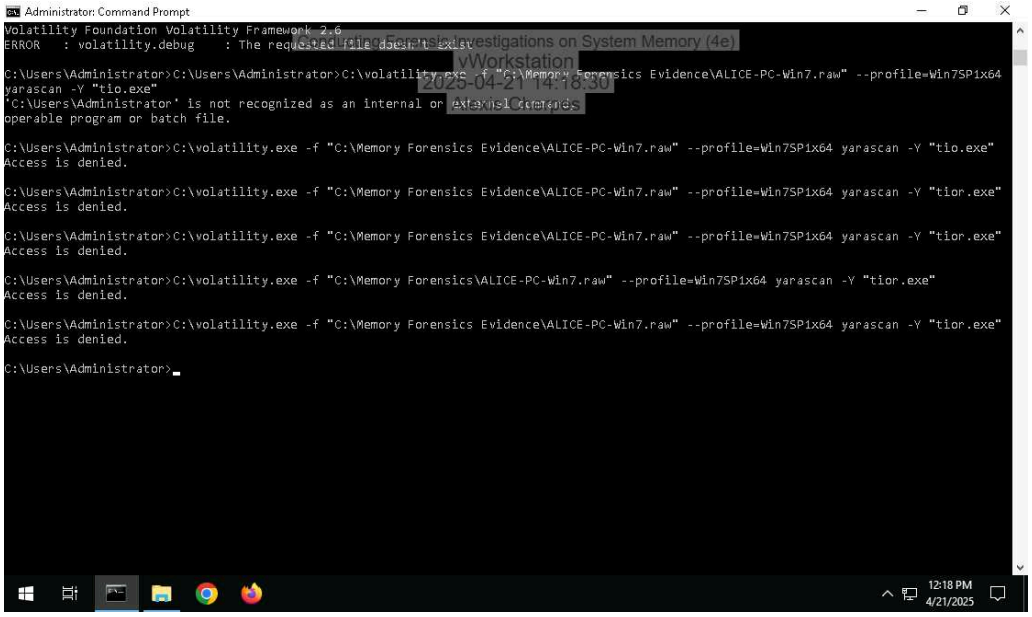
Port 4444 is often associated with malicious activity. It has been used by various rootkits, trojans, and backdoors to facilitate unauthorized access. Attackers may leverage this port to intercept communication or maintain persistent control over compromised systems. Malware such as Blaster worm and its variants used port 4444 to create backdoors.https://isc.sans.edu/diary/RPC+DCOM+WORM+MSBLASTER/25 https://www.sciencedirect.com/topics/computer-science/blaster-worm?

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**.