

Conducting Forensic Investigations on System Memory (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 10

Student:

Imani Williams

Email:

imanilw13@gmail.com

Time on Task:

1 hour, 50 minutes

Progress:

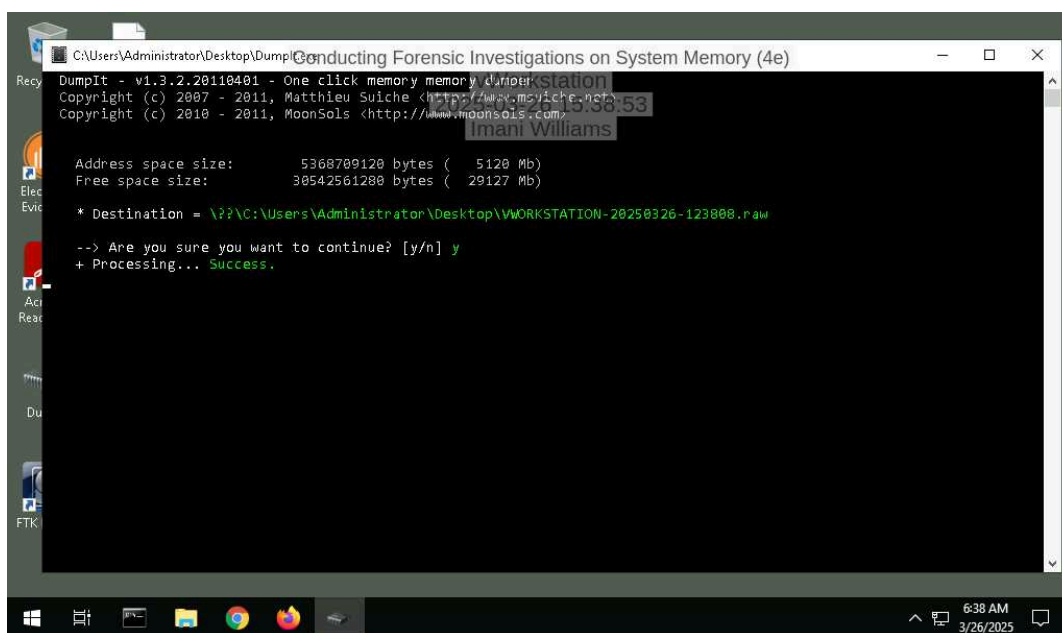
100%

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.

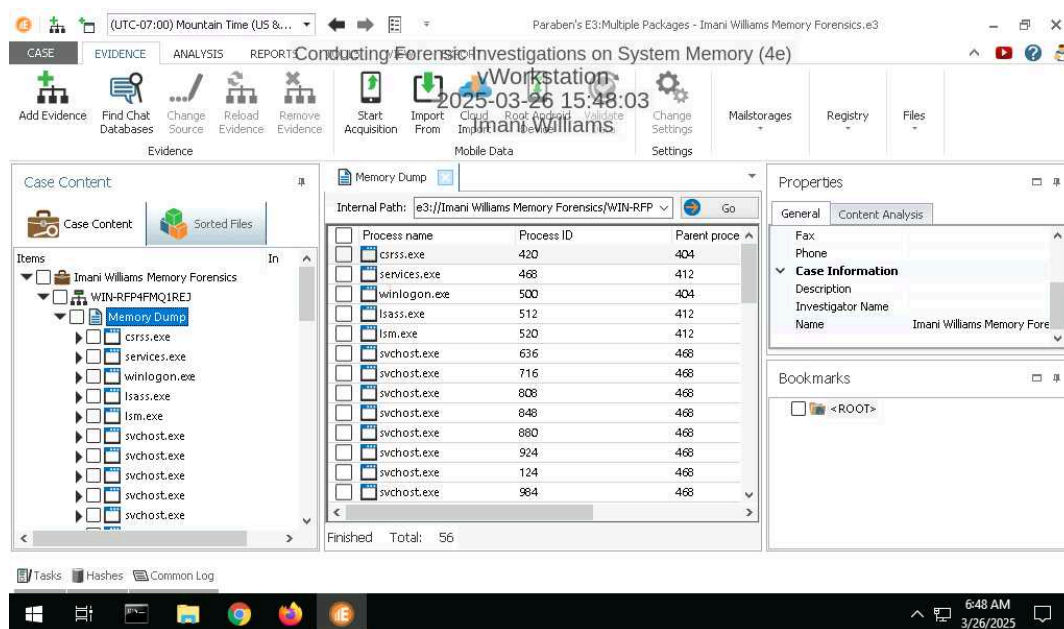


Part 2: Analyze Memory using E3

Conducting Forensic Investigations on System Memory (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 10

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.

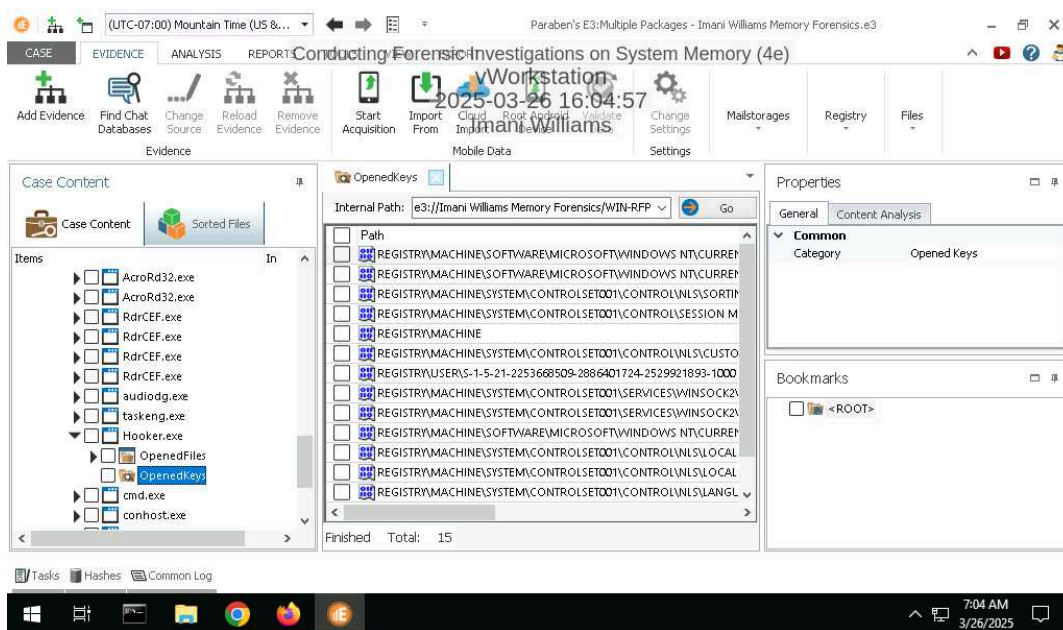
17. Document your findings for the hooker.exe process. What is it and what is it used for?

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.

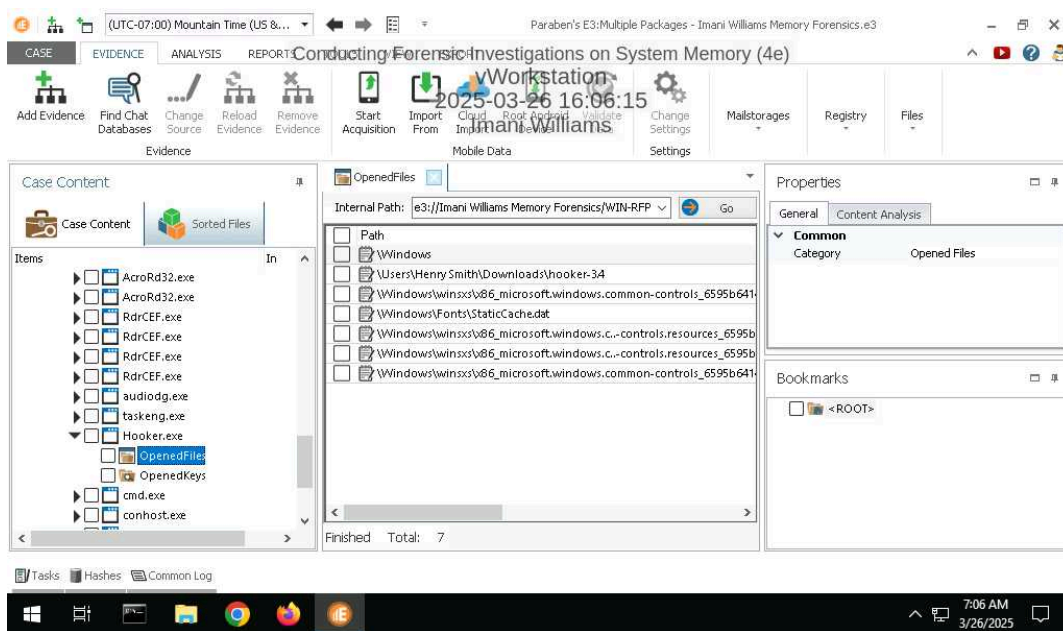
Conducting Forensic Investigations on System Memory (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 10

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



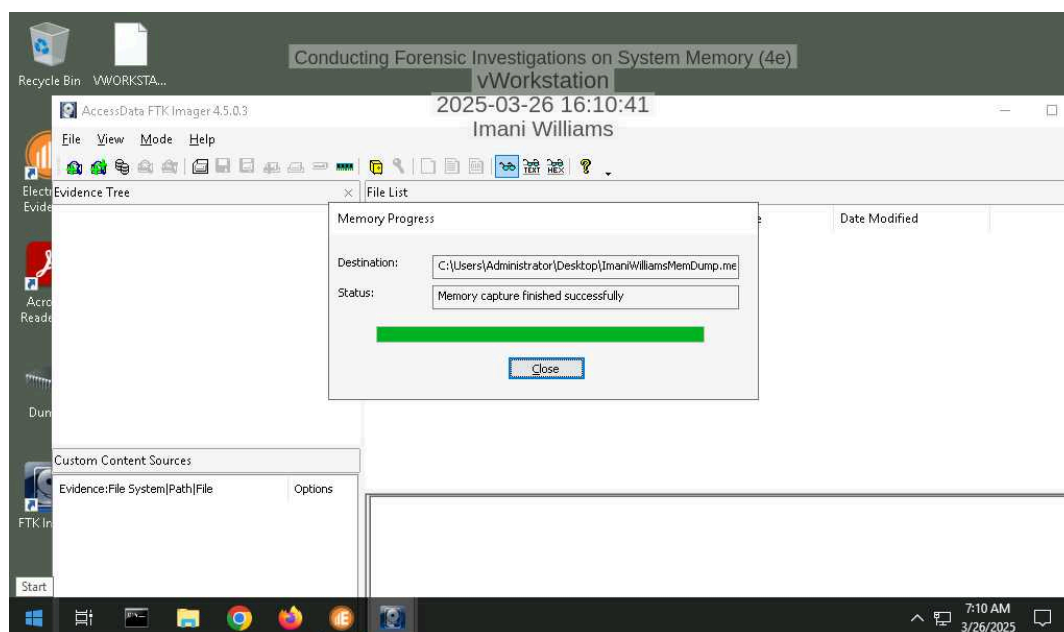
23. Make a screen capture showing the files opened by the hooker.exe process.



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.

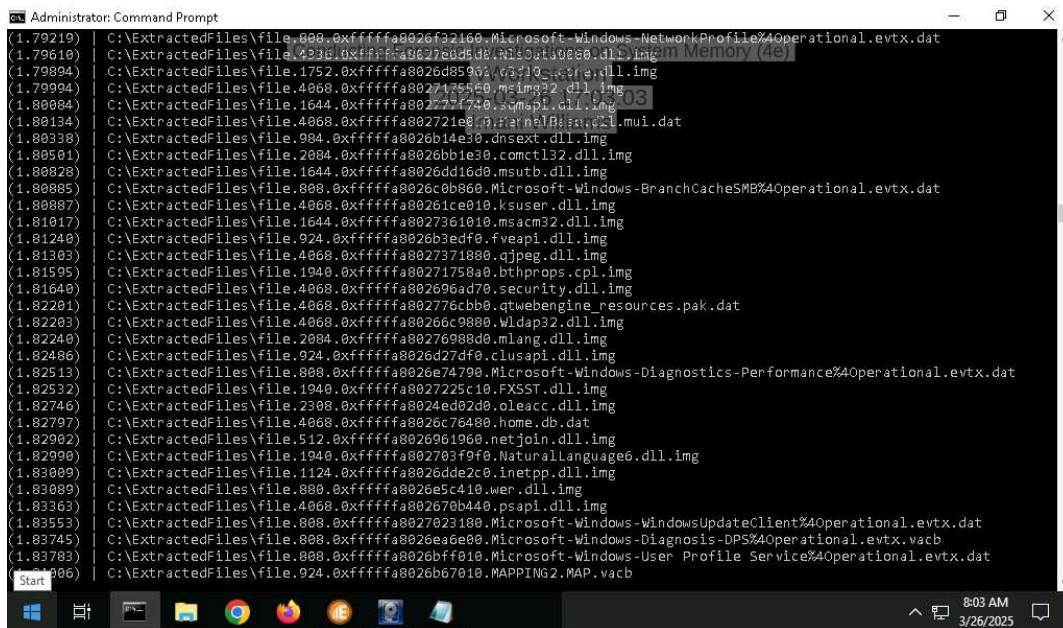
12. **Document** whether the netscan module displays network usage associated with the Hooker.exe or rvlkl.exe processes.

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.

```
Select Administrator: Command Prompt
Conducting Forensic Investigations on System Memory (4e)
vWorkstation
2025-03-26 17:14:43
Imani Williams
0xfffffa8001c1e6f0 firefox.exe 2192 2444 15 288 1 0 2021-08-29 17:48:08 UTC+0000
0xfffffa8001c25360 firefox.exe 1532 2444 17 288 1 0 2021-08-29 17:48:10 UTC+0000
0xfffffa8001cbb30 firefox.exe 2864 2444 2 1 0 2021-08-29 17:48:11 UTC+0000
0xfffffa8001c91440 firefox.exe 1576 2444 16 271 2 1 0 2021-08-29 17:48:23 UTC+0000
0xfffffa8001c0e180 fixtureCompute 2364 2444 3 107 2 0 0 2021-08-29 17:48:54 UTC+0000
0xfffffa8001a29b30 taskhost.exe 2240 448 5 99 2 0 0 2021-08-29 17:50:18 UTC+0000
0xfffffa8001c01b30 whoami.exe 1356 2896 0 ----- 2 0 0 2021-08-29 17:50:43 UTC+0000 2021-08-29
17:50:43 UTC+0000
0xfffffa8001c93b30 whoami.exe 2992 2260 0 ----- 2 0 0 2021-08-29 17:50:43 UTC+0000 2021-08-29
17:50:43 UTC+0000
0xfffffa8001b0a060 tior.exe 2768 924 0 ----- 2 0 0 2021-08-29 17:50:46 UTC+0000 2021-08-29
17:50:48 UTC+0000
0xfffffa8001b1d060 QaNoQBC.exe 2156 2932 4 108 2 0 0 2021-08-29 17:50:46 UTC+0000
0xfffffa8003c9d060 cmd.exe 2392 2156 1 26 2 0 0 2021-08-29 17:57:21 UTC+0000
0xfffffa8001bfc570 conhost.exe 2252 1832 2 48 2 0 0 2021-08-29 17:57:21 UTC+0000
0xfffffa8001a87950 svchost.exe 1952 448 6 78 0 0 0 2021-08-29 17:59:33 UTC+0000
0xfffffa8001d1cab0 DumpIt.exe 2464 2140 2 45 2 1 0 2021-08-29 18:00:16 UTC+0000
0xfffffa8001b04520 conhost.exe 2040 1832 2 49 2 0 0 2021-08-29 18:00:16 UTC+0000
C:\Users\Administrator>
```


Digital Forensics, Investigation, and Response, Fourth Edition - Lab 10

```
Administrator: Command Prompt
0xffffffff8001bfc570 conhost.exe 125 1992 5 13 0 2021-08-20 17:57:21 UTC+0000
0xffffffff8001a87950 svchost.exe 1952 449 1 75 8 0 2021-08-20 17:59:33 UTC+0000
0xffffffff8001dicab0 DumpIt.exe 2464 2140 1 1 2 1 2021-08-20 18:00:16 UTC+0000
0xffffffff8001b04520 conhost.exe 2040 1832 2 49 2 0 2021-08-20 18:00:16 UTC+0000

C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\ALICE-PC-Win7.raw" --profile=Win7SP1x64 yarascan -Y
"tior.exe"
Volatility Foundation Volatility Framework 2.6
Rule: r1
Owner: Process svchost.exe Pid 820
0x05448a30 74 69 6f 72 2e 65 78 65 00 00 00 00 00 00 00 00 tior.exe.....
0x05448a40 11 00 11 00 01 00 01 00 00 00 00 00 00 00 00 00 .....
0x05448a50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x05448a60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x05448a70 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x05448a80 49 42 2f 03 00 00 00 00 c4 49 60 1e 52 9f 4b 89 IB/.....I.R.K.
0x05448a90 e6 0d 00 00 08 00 02 00 70 6f c2 05 00 00 00 00 .....po.....
0x05448aa0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 .....
0x05448ab0 02 00 00 00 bc 09 00 ff fc ac 18 00 00 00 00 00 .....
0x05448ac0 af ed 32 07 7e 66 28 1e 66 69 72 65 66 6f 78 2e ..2..f(.firefox.
0x05448ad0 65 78 65 00 00 00 00 00 16 00 00 00 0c 00 03 00 exe.....
0x05448ae0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x05448af0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x05448b00 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 .....
0x05448b10 cd 07 00 00 00 00 00 00 49 42 2f 03 00 00 00 00 .....IB/.....
0x05448b20 4c 85 b4 6d 3a 8a f0 ba 1e 03 00 00 08 00 00 00 L.m:.....

C:\Users\Administrator>
```

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

The screenshot displays the Windows Task Manager application, specifically the 'Performance' tab. The 'Memory' section is selected, showing a total of 16.0 GB of RAM. The usage is 6.0 GB (38%), leaving 10.0 GB (62%) free. A watermark for 'Conducting Forensic Investigations on System Memory (4e)' is overlaid on the image. The task manager interface includes a top navigation bar with icons for CPU, Memory, Disk, Network, and System. The bottom of the screen shows the Windows taskbar with various application icons and the system clock indicating 8:23 AM on 3/26/2025.