

Conducting Forensic Investigations on System Memory (4e)

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

Student:

Alexis Cherpes

Email:

cherpea@ferris.edu

Time on Task:

4 hours, 2 minutes

Progress:

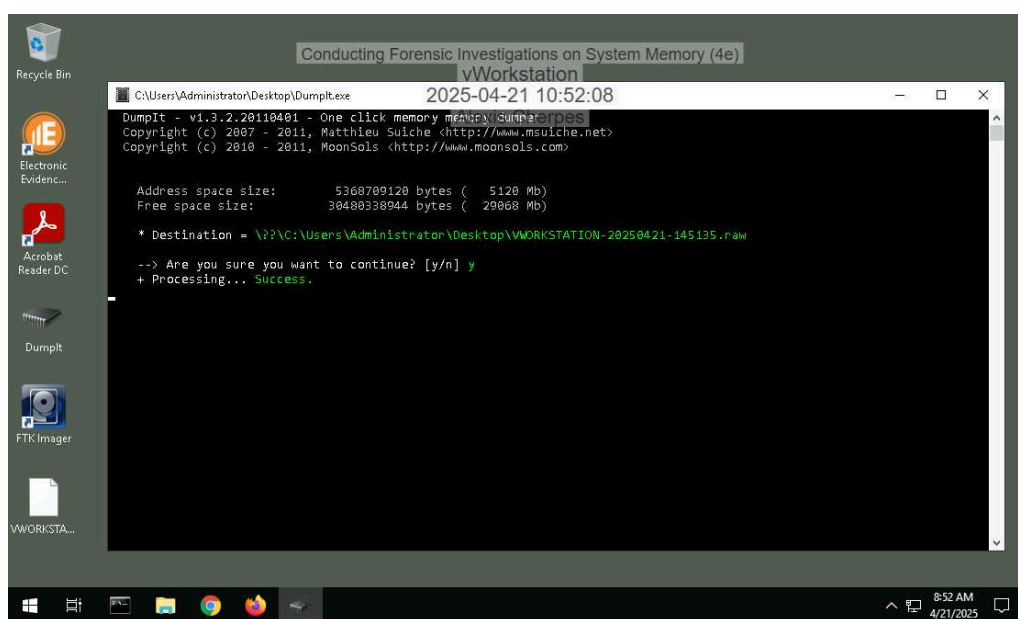
100%

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 **Dumplt success notification**.

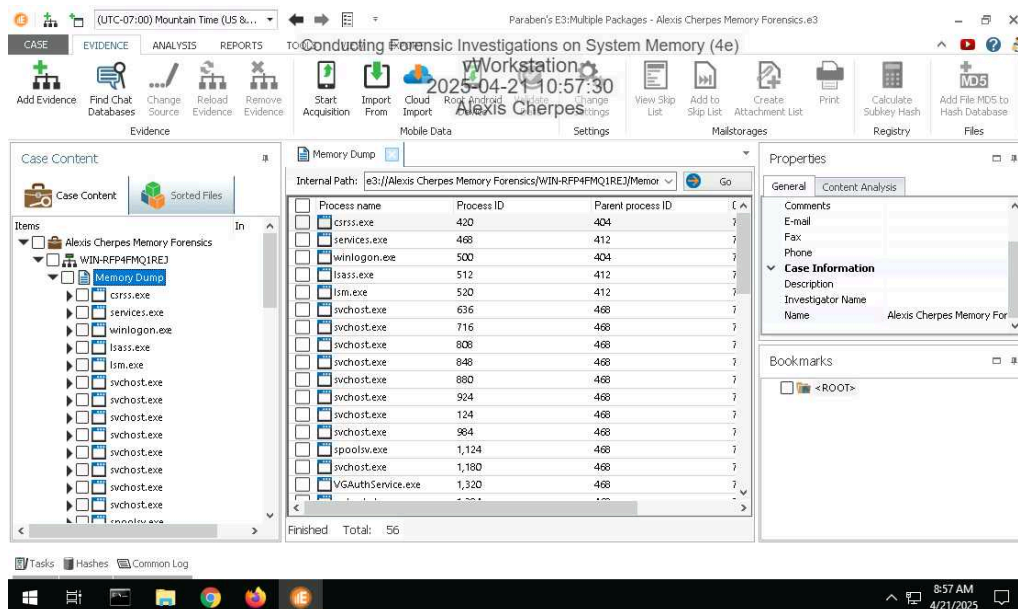


Part 2: Analyze Memory using E3

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.

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.

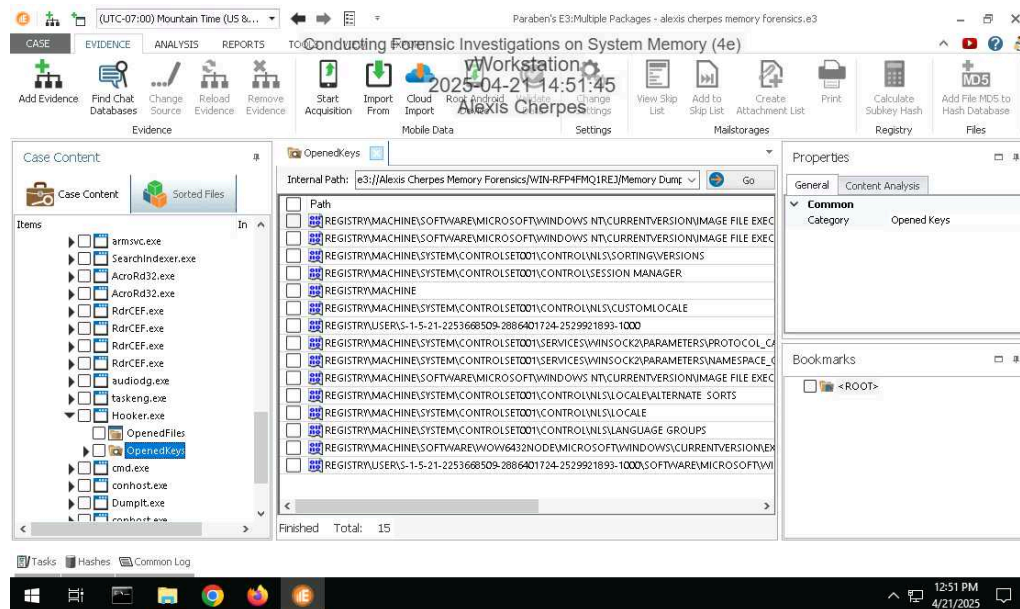
17. Document your findings for the hooker.exe process. What is it and what is it used for?

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.

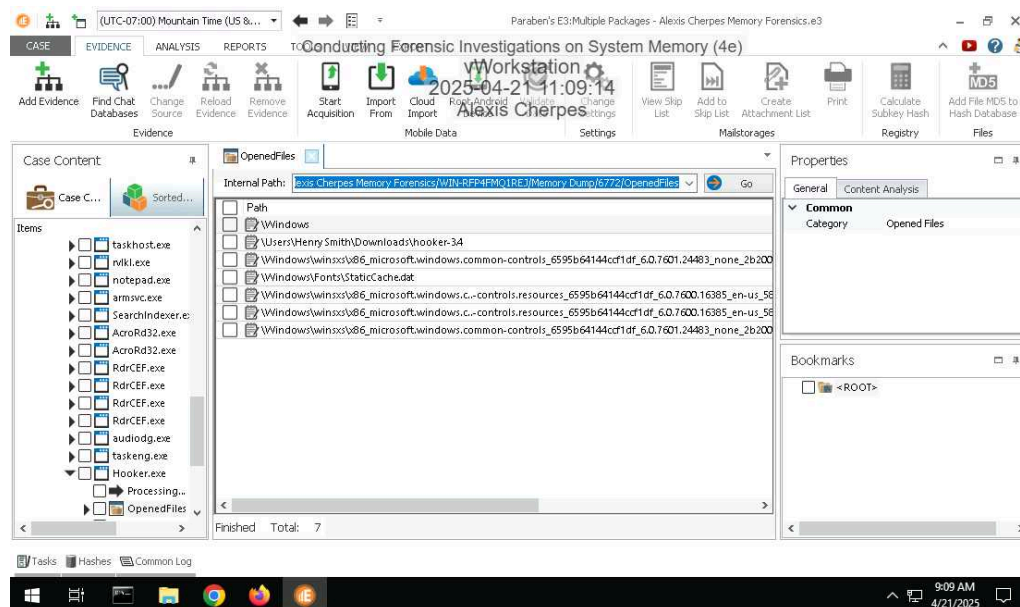
Digital Forensics, Investigation, and Response, Fourth Edition - Lab 10

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

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



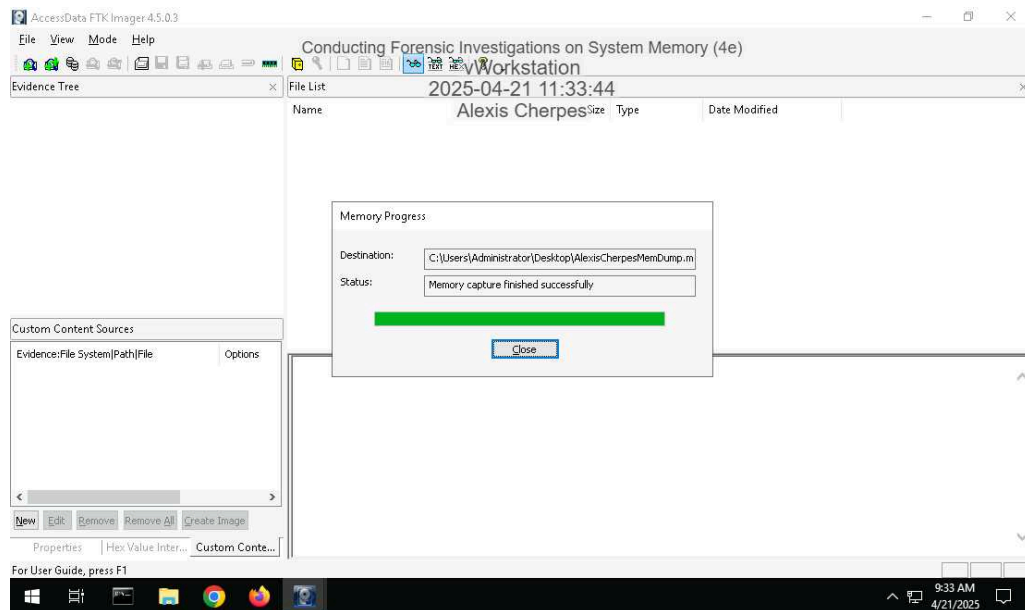
23. **Make a screen capture** showing the **files opened** by the **hooker.exe** process.



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 rvkl.exe process. What is it and what is it used for?

rvkl.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.

Conducting Forensic Investigations on System Memory (4e)

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

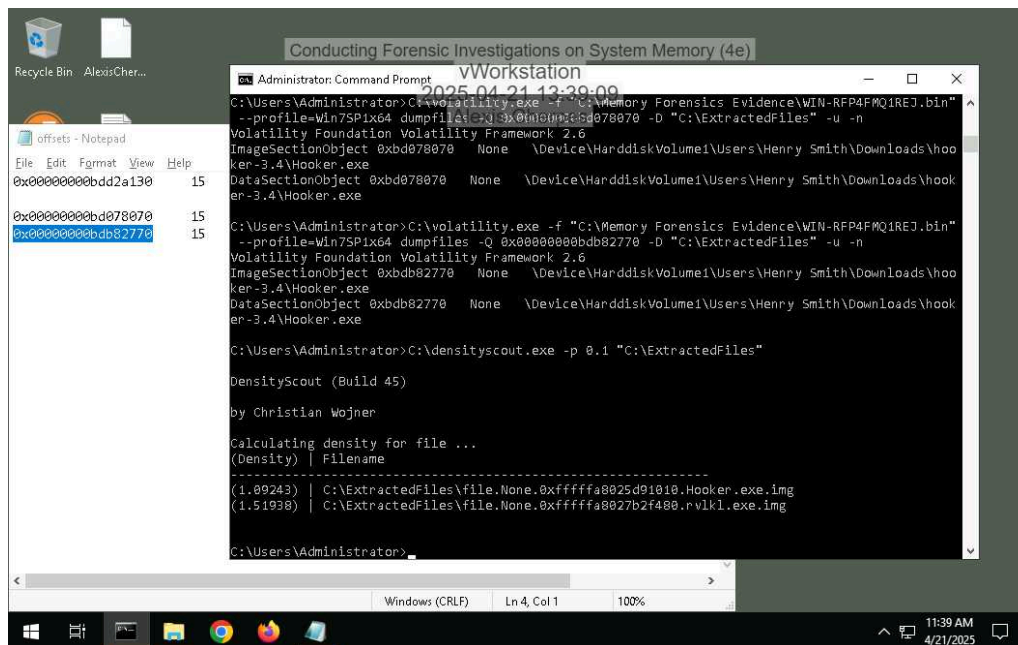
12. **Document** whether the netscan module displays network usage associated with the Hooker.exe or rvlkl.exe processes.

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.

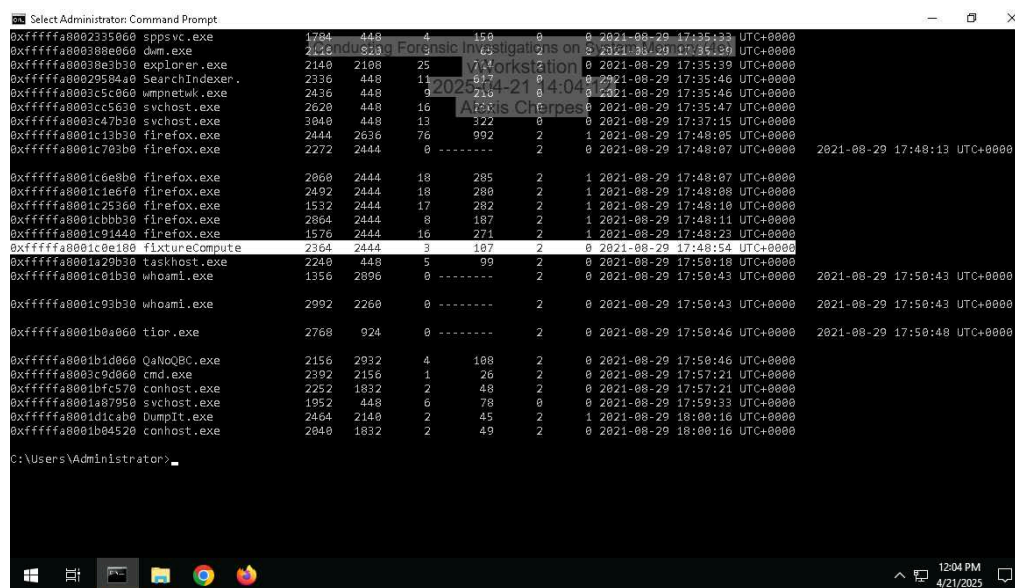
1. dlhost.exe 2. QaNoQBC.exe 3. fixtureCompute

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.



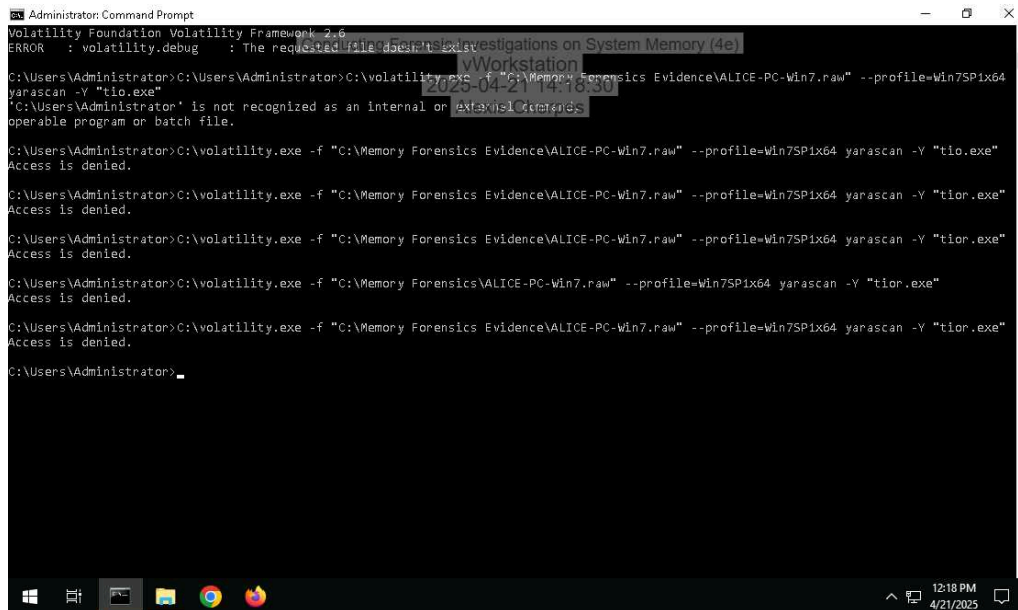
```
Select Administrator: Command Prompt
pslist
0xffffffff800235000 sppsvc.exe 1784 448 4 150 0 0 2021-08-29 17:35:33 UTC+0000
0xffffffff800380e00 dm.exe 2140 2108 25 0 0 0 2021-08-29 17:35:33 UTC+0000
0xffffffff800380b30 explorer.exe 2336 448 11 0 0 0 2021-08-29 17:35:46 UTC+0000
0xffffffff8003c5c00 wmpnetwk.exe 2636 448 9 0 0 0 2021-08-29 17:35:46 UTC+0000
0xffffffff8003c5b30 svchost.exe 2620 448 16 0 0 0 2021-08-29 17:35:47 UTC+0000
0xffffffff8003c47b30 svchost.exe 3040 448 13 122 0 0 2021-08-29 17:37:15 UTC+0000
0xffffffff8001c13b30 firefox.exe 2444 2636 76 992 2 1 2021-08-29 17:48:05 UTC+0000
0xffffffff8001c703b0 firefox.exe 2272 2444 0 ----- 2 0 2021-08-29 17:48:07 UTC+0000
0xffffffff8001c0e8b0 firefox.exe 2060 2444 18 285 2 1 2021-08-29 17:48:07 UTC+0000
0xffffffff8001c1e0f0 firefox.exe 2402 2444 18 288 2 1 2021-08-29 17:48:08 UTC+0000
0xffffffff8001c25300 firefox.exe 1532 2444 17 282 2 1 2021-08-29 17:48:10 UTC+0000
0xffffffff8001cbb30 firefox.exe 2864 2444 8 187 2 1 2021-08-29 17:48:11 UTC+0000
0xffffffff8001c91440 firefox.exe 1576 2444 16 271 2 1 2021-08-29 17:48:23 UTC+0000
0xffffffff8001c0e180 fixtureCompute 2364 2444 3 107 2 0 2021-08-29 17:48:54 UTC+0000
0xffffffff8001a29b30 taskhost.exe 2240 448 5 99 2 0 2021-08-29 17:50:18 UTC+0000
0xffffffff8001c01b30 whoami.exe 1356 2896 0 ----- 2 0 2021-08-29 17:50:43 UTC+0000
0xffffffff8001c93b30 whoami.exe 2902 2260 0 ----- 2 0 2021-08-29 17:50:43 UTC+0000
0xffffffff8001b0a060 tior.exe 2768 924 0 ----- 2 0 2021-08-29 17:50:46 UTC+0000
0xffffffff8001b1d060 QaNoQBC.exe 2156 2932 4 108 2 0 2021-08-29 17:50:46 UTC+0000
0xffffffff8003c9d060 cmd.exe 2392 2156 1 26 2 0 2021-08-29 17:57:21 UTC+0000
0xffffffff8001bfcc570 conhost.exe 2252 1832 2 48 2 0 2021-08-29 17:57:21 UTC+0000
0xffffffff8001a87950 svchost.exe 1952 448 6 78 0 0 2021-08-29 17:59:33 UTC+0000
0xffffffff8001dicab0 DumpIt.exe 2464 2140 2 45 2 1 2021-08-29 18:00:16 UTC+0000
0xffffffff8001b04520 conhost.exe 2040 1832 2 49 2 0 2021-08-29 18:00:16 UTC+0000

C:\Users\Administrator>
```


Conducting Forensic Investigations on System Memory (4e)

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

Make a screen capture showing the output of the yarascan.



```
Administrator: Command Prompt
Volatility Foundation Volatility Framework 2.6
ERROR : volatility.debug : The requested file does not exist.

C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\ALICE-PC-Win7.raw" --profile=Win7SP1x64
yarascan -Y "tio.exe"
'C:\Users\Administrator' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\ALICE-PC-Win7.raw" --profile=Win7SP1x64
yarascan -Y "tio.exe"
Access is denied.

C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\ALICE-PC-Win7.raw" --profile=Win7SP1x64
yarascan -Y "tior.exe"
Access is denied.

C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\ALICE-PC-Win7.raw" --profile=Win7SP1x64
yarascan -Y "tior.exe"
Access is denied.

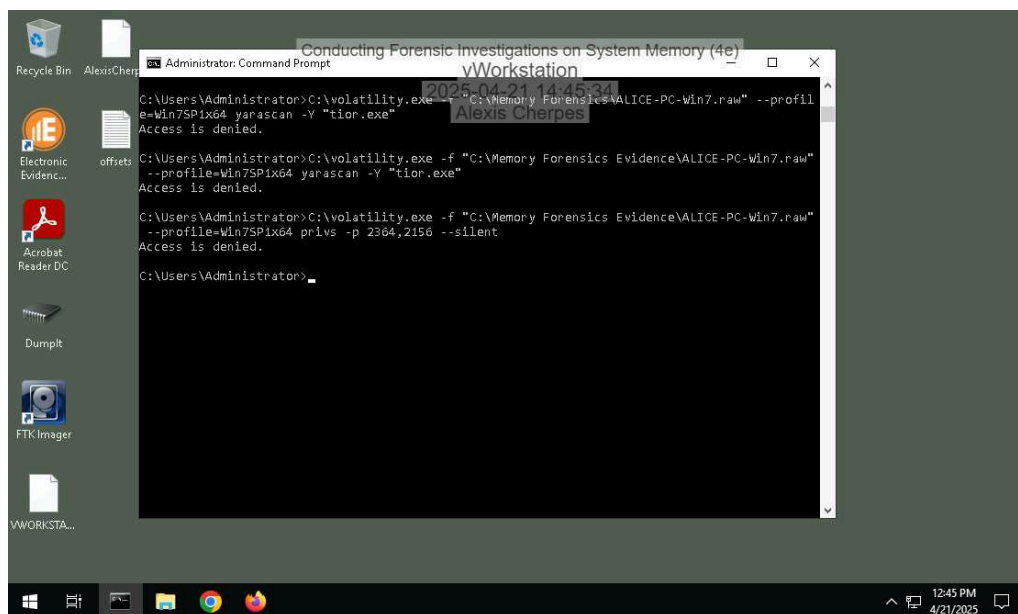
C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\ALICE-PC-Win7.raw" --profile=Win7SP1x64
yarascan -Y "tior.exe"
Access is denied.

C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\ALICE-PC-Win7.raw" --profile=Win7SP1x64
yarascan -Y "tior.exe"
Access is denied.

C:\Users\Administrator>
```

Part 3: Identify Privilege Escalation

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



```
Administrator: Command Prompt
Conducting Forensic Investigations on System Memory (4e)
vWorkstation
2025-04-21 14:45:34
Alexis Cherpes

C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\ALICE-PC-Win7.raw" --profil
e=Win7SP1x64 yarascan -Y "tior.exe"
Access is denied.

C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\ALICE-PC-Win7.raw"
--profile=Win7SP1x64 yarascan -Y "tior.exe"
Access is denied.

C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\ALICE-PC-Win7.raw"
--profile=Win7SP1x64 privs -p 2364,2156 --silent
Access is denied.

C:\Users\Administrator>
```