

# Conducting Forensic Investigations on System Memory (4e)

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

Student:

Karan Atul Vora

Email:

kxv230021@utdallas.edu

Time on Task:

1 hour, 41 minutes

Progress:

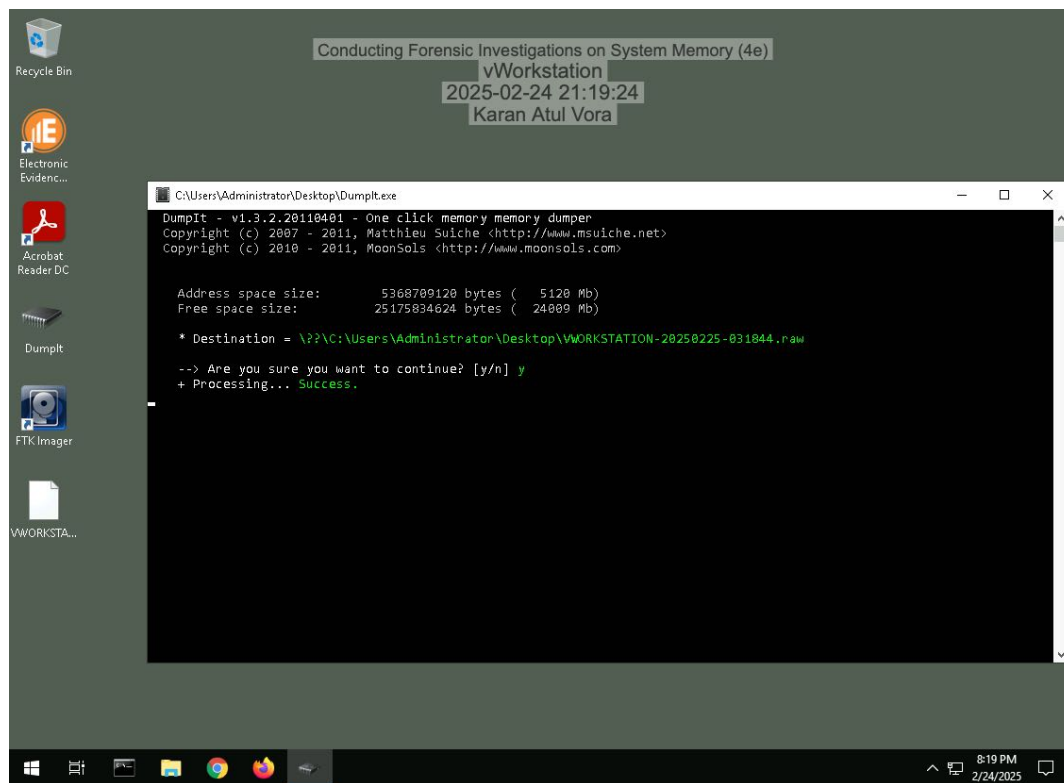
100%

Report Generated: Monday, February 24, 2025 at 11:57 PM

## Section 1: Hands-On Demonstration

### Part 1: Capture Memory using DumpIt

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

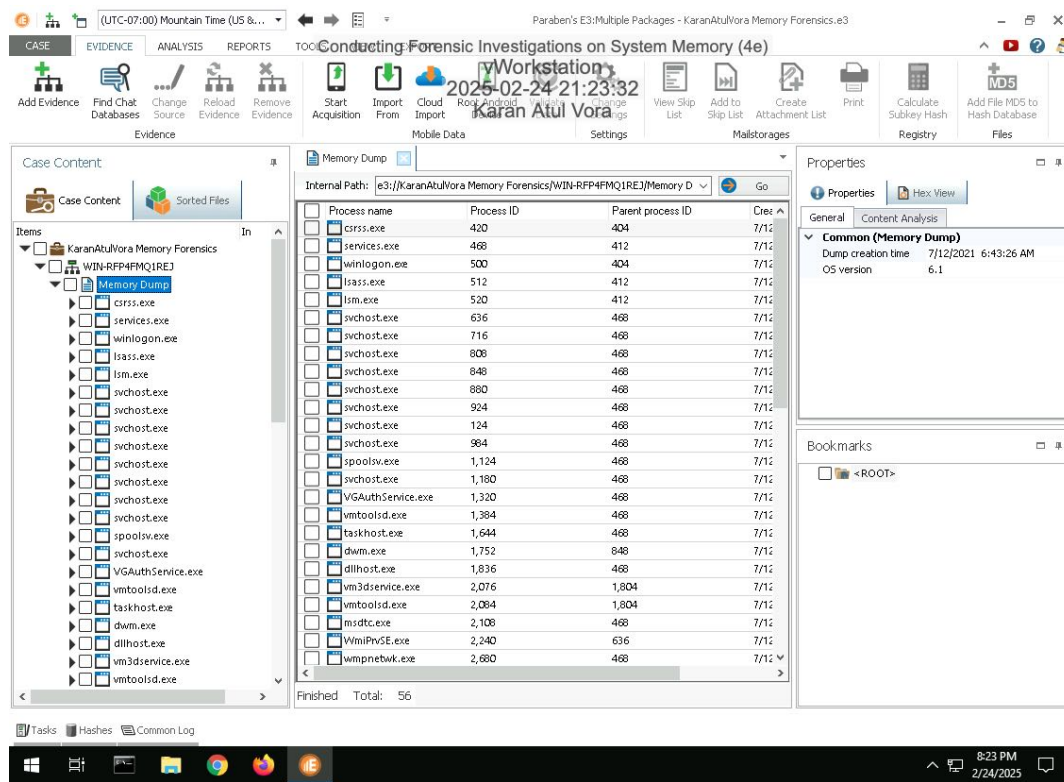


### Part 2: Analyze Memory using E3

# 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.

4:24:49 AM, 6:42.43 AM

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

contest.exe - Windows Console Host - It is a application for all the windows Console APIs as well as the classic Windows User Interface for working with command-line application

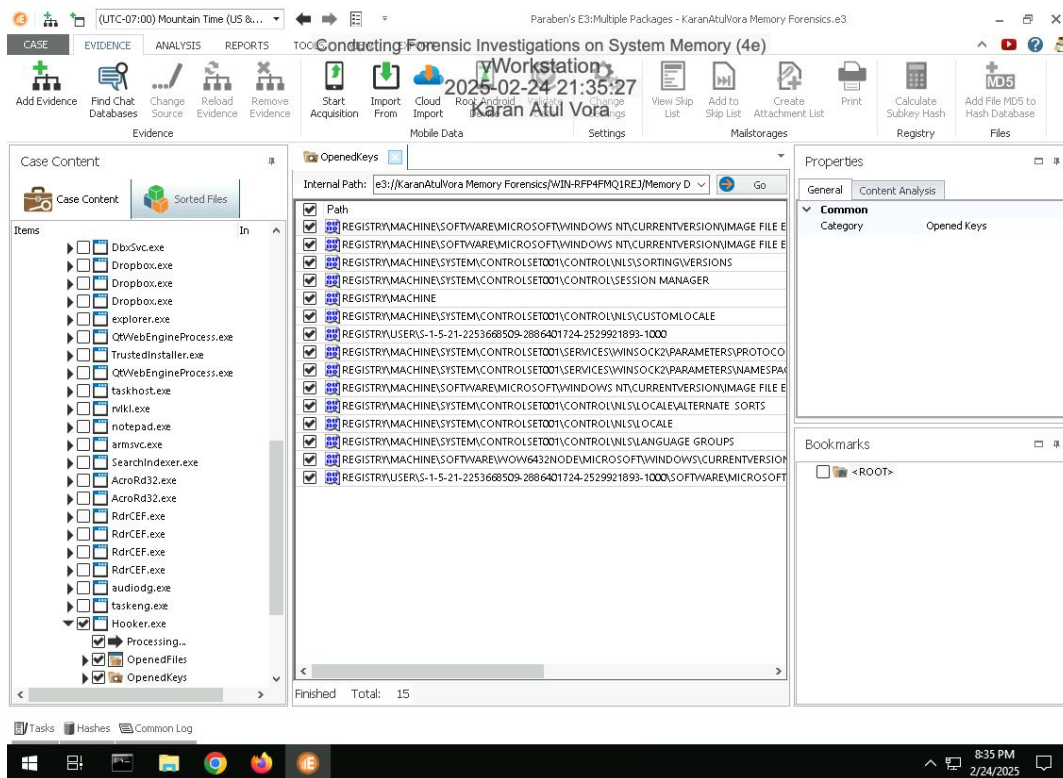
## 17. Document your findings for the hooker.exe process. What is it and what is it used for?

hooker.exe - is a password and data stealing trojan/ Malware

# Conducting Forensic Investigations on System Memory (4e)

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

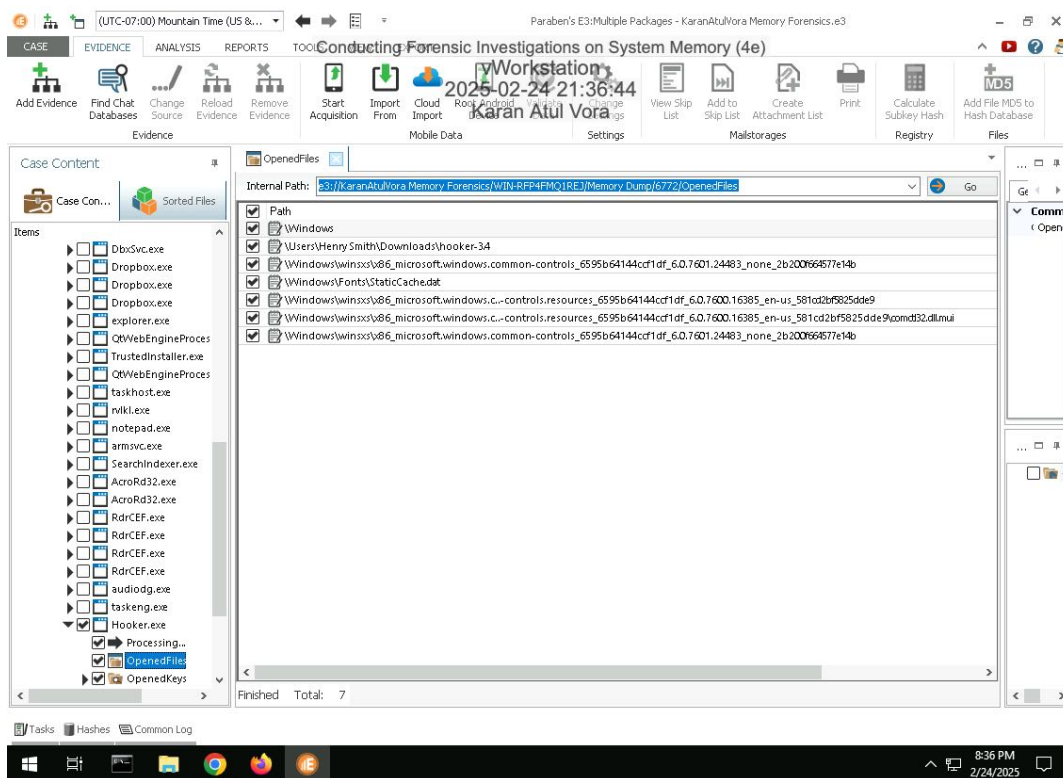
21. Make a screen capture showing the registry keys opened by the Hooker.exe process.



# Conducting Forensic Investigations on System Memory (4e)

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

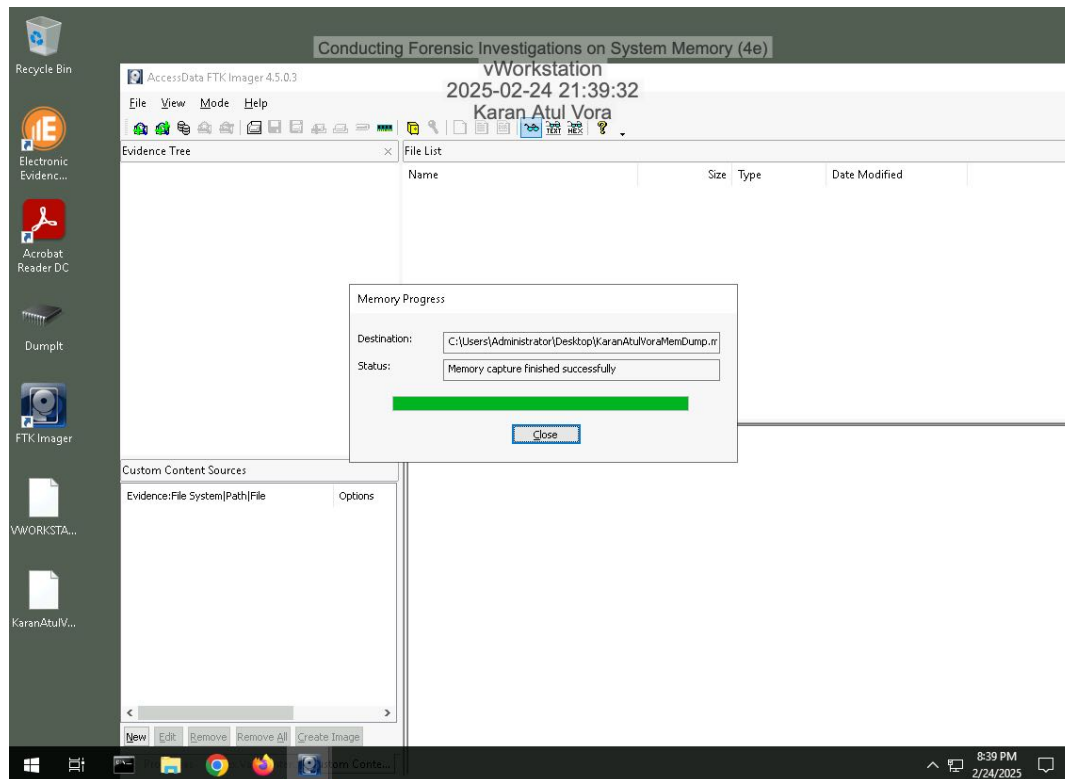
## 23. Make a screen capture showing the files opened by the hooker.exe process.



## 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 - This is a monitoring tool. It monitors what you do on your PC.

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

None

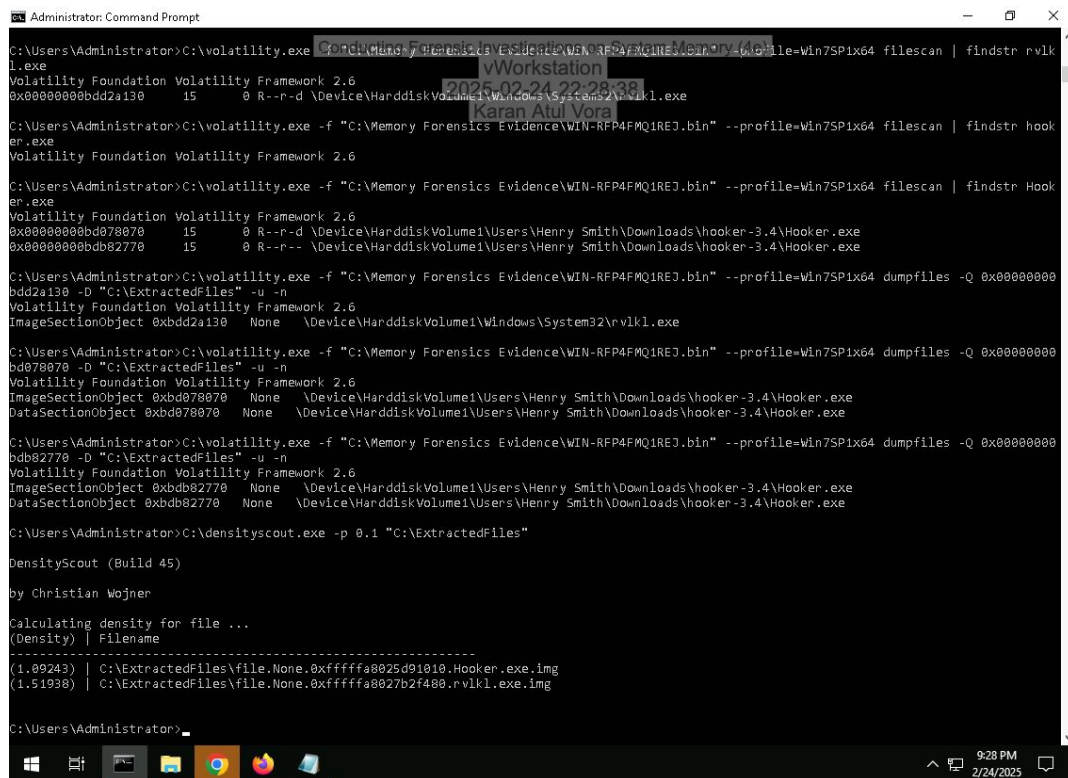
12. **Document** whether the netscan module displays network usage associated with the Hooker.exe or rvkl.exe processes.

NoneBut there are services with PID of -1

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

Port 56610 is primarily used for accessing the Xsan file system, a storage area network (SAN) developed by Apple, specifically on the TCP protocol; it is considered a "dynamic and/or private port" which means it can be used for temporary or private purposes by various applications depending on the network configuration.

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



```
Administrator: Command Prompt
C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\WIN-RFP4FWQ1REJ.bin" --profile=Win7SP1x64 filescan | findstr rvkl
.exe
Volatility Foundation Volatility Framework 2.6
0x0000000bdd2a130 15 0 R--r-d \Device\HarddiskVolume1\Windows\System32\rvkl.exe

C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\WIN-RFP4FWQ1REJ.bin" --profile=Win7SP1x64 filescan | findstr hook
er.exe
Volatility Foundation Volatility Framework 2.6

C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\WIN-RFP4FWQ1REJ.bin" --profile=Win7SP1x64 filescan | findstr Hook
er.exe
Volatility Foundation Volatility Framework 2.6
0x0000000bd078070 15 0 R--r-d \Device\HarddiskVolume1\Users\Henry Smith\Downloads\hooker-3.4\Hooker.exe
0x0000000bd078070 15 0 R--r-- \Device\HarddiskVolume1\Users\Henry Smith\Downloads\hooker-3.4\Hooker.exe

C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\WIN-RFP4FWQ1REJ.bin" --profile=Win7SP1x64 dumpfiles -Q 0x0000000
bdd2a130 -D "C:\ExtractedFiles" -u -n
Volatility Foundation Volatility Framework 2.6
ImageSectionObject 0xbdd2a130 None \Device\HarddiskVolume1\Windows\System32\rvkl.exe

C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\WIN-RFP4FWQ1REJ.bin" --profile=Win7SP1x64 dumpfiles -Q 0x0000000
bd078070 -D "C:\ExtractedFiles" -u -n
Volatility Foundation Volatility Framework 2.6
ImageSectionObject 0xbd078070 None \Device\HarddiskVolume1\Users\Henry Smith\Downloads\hooker-3.4\Hooker.exe
DataSectionObject 0xbd078070 None \Device\HarddiskVolume1\Users\Henry Smith\Downloads\hooker-3.4\Hooker.exe

C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\WIN-RFP4FWQ1REJ.bin" --profile=Win7SP1x64 dumpfiles -Q 0x0000000
bdb82770 -D "C:\ExtractedFiles" -u -n
Volatility Foundation Volatility Framework 2.6
ImageSectionObject 0xbdb82770 None \Device\HarddiskVolume1\Users\Henry Smith\Downloads\hooker-3.4\Hooker.exe
DataSectionObject 0xbdb82770 None \Device\HarddiskVolume1\Users\Henry Smith\Downloads\hooker-3.4\Hooker.exe

C:\Users\Administrator>C:\densityscout.exe -p 0.1 "C:\ExtractedFiles"

DensityScout (Build 45)

by Christian Wojner

Calculating density for file ...
(Density) | Filename
-----
(1.09243) | C:\ExtractedFiles\file.None.0xfffffa8025d91010.Hooker.exe.img
(1.51938) | C:\ExtractedFiles\file.None.0xfffffa8027b2f480.rvkl.exe.img

C:\Users\Administrator>
```

### Section 3: Challenge and Analysis

#### Part 1: Identify Malicious Connections

**Document** the three processes that connected to 205.134.253.10:4444.

QaNoQBC.exe, fixtureCompute, dllhost.exe

**Document** the name and purpose of the software you discovered.

The port 4444 is used by the OpenAM as the administration port, OpenAM (Open Access Management) is an open-source platform that manages access to applications, web services, and other resources.

#### Part 2: Identify Malicious Processes

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

```
Administrator: Command Prompt
pslist
1576 2444 16 271 2 1 2021-08-29 17:48:23 UTC+0000
0xfffffa8001c91440 firefox.exe
2364 2444 3 0 0 0 2021-08-29 17:48:54 UTC+0000
0xfffffa8001c0e180 fixtureCompute
2240 448 2 0 0 0 2021-08-29 17:50:18 UTC+0000
0xfffffa8001a29b30 taskhost.exe
1356 2896 0 ----- 2 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 2021-08-29 17:50:43 UTC+0000 2021-08-29 17:50:43 UTC+
0000
0xfffffa8001b0a060 tior.exe
2768 924 0 ----- 2 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 2021-08-29 17:50:46 UTC+0000
0xfffffa8003c9d060 cmd.exe
2392 2156 1 26 2 0 2021-08-29 17:57:21 UTC+0000
0xfffffa8001bfc570 conhost.exe
2252 1832 2 48 2 0 2021-08-29 17:57:21 UTC+0000
0xfffffa8001a87950 svchost.exe
1952 448 6 78 0 0 2021-08-29 17:59:33 UTC+0000
0xfffffa8001d1cab0 DumpIt.exe
2464 2140 2 45 2 1 2021-08-29 18:00:16 UTC+0000
0xfffffa8001b04520 conhost.exe
2040 1832 2 49 2 0 2021-08-29 18:00:16 UTC+0000

C:\Users\Administrator>
```

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

```
Administrator: Command Prompt
C:\Users\Administrator>C:\volatility.exe -f "C:\Memorv Forensics Evidence\ALICE-PC-Win7.rar" --profile=win7SP1x64 yarascan -Y "tior.exe"
Volatility Foundation Volatility Framework 2.10.0
Rule: p1
Owner: Process svchost.exe Pid 020
0x05448a30 74 69 6f 72 2e 65 78 65 00 00 00 00 00 00 00 00 .....vWorkstation
0x05448a40 11 00 11 00 01 00 01 00 00 00 00 00 00 00 00 00 .....2025-02-24 22:49:52
0x05448a50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....Karan Atul Vora
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 c4 49 00 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 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.exe.....
0x05448ad0 65 78 65 00 00 00 00 16 00 00 00 00 00 00 00 00 .....
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 49 42 2f 03 00 00 00 00 .....IB/.....
0x05448b20 4c 85 b4 6d 3a 8a f0 ba 1e 03 00 00 00 00 00 00 L.m:.....
Interrupted

C:\Users\Administrator>
```

## Page 8 of 9



# Conducting Forensic Investigations on System Memory (4e)

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

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

```
Select Administrator: Command Prompt
C:\Users\Administrator>C:\volatility.exe --profile=Win7SP1x64 privs -p 2364,2156 --sile
nt
Volatility Foundation Volatility Framework 2.6
-----
Pid      Process      Value      Privilege      Attributes      Description
-----
2156     QaNoQBC.exe      5      SeIncreaseQuotaPrivilege      Present,Enabled      Increase quotas
2156     QaNoQBC.exe      8      SeSecurityPrivilege      Present,Enabled      Manage auditing and security log
2156     QaNoQBC.exe      9      SeTakeOwnershipPrivilege      Present,Enabled      Take ownership of files/objects
2156     QaNoQBC.exe      10     SeLoadDriverPrivilege      Present,Enabled      Load and unload device drivers
2156     QaNoQBC.exe      11     SeSystemProfilePrivilege      Present,Enabled      Profile system performance
2156     QaNoQBC.exe      12     SeSystemTimePrivilege      Present,Enabled      Change the system time
2156     QaNoQBC.exe      13     SeProfileSingleProcessPrivilege      Present,Enabled      Profile a single process
2156     QaNoQBC.exe      14     SeIncreaseBasePriorityPrivilege      Present,Enabled      Increase scheduling priority
2156     QaNoQBC.exe      15     SeCreatePagefilePrivilege      Present,Enabled      Create a pagefile
2156     QaNoQBC.exe      17     SeBackupPrivilege      Present,Enabled      Backup files and directories
2156     QaNoQBC.exe      18     SeRestorePrivilege      Present,Enabled      Restore files and directories
2156     QaNoQBC.exe      19     SeShutdownPrivilege      Present,Enabled      Shut down the system
2156     QaNoQBC.exe      20     SeDebugPrivilege      Present,Enabled      Debug programs
2156     QaNoQBC.exe      22     SeSystemEnvironmentPrivilege      Present,Enabled      Edit firmware environment values
2156     QaNoQBC.exe      24     SeRemoteShutdownPrivilege      Present,Enabled      Force shutdown from a remote system
2156     QaNoQBC.exe      25     SeUndockPrivilege      Present,Enabled      Remove computer from docking station
2156     QaNoQBC.exe      28     SeManageVolumePrivilege      Present,Enabled      Manage the files on a volume
2156     QaNoQBC.exe      33     SeIncreaseWorkingSetPrivilege      Present,Enabled      Allocate more memory for user applications
2156     QaNoQBC.exe      34     SeTimeZonePrivilege      Present,Enabled      Adjust the time zone of the computer's inter
nal clock
2156     QaNoQBC.exe      35     SeCreateSymbolicLinkPrivilege      Present,Enabled      Required to create a symbolic link
C:\Users\Administrator>
```