

Conducting Forensic Investigations on System Memory (4e)

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

Student:

Jake Simpson

Email:

jaksimps@iu.edu

Time on Task:

0 hours, 58 minutes

Progress:

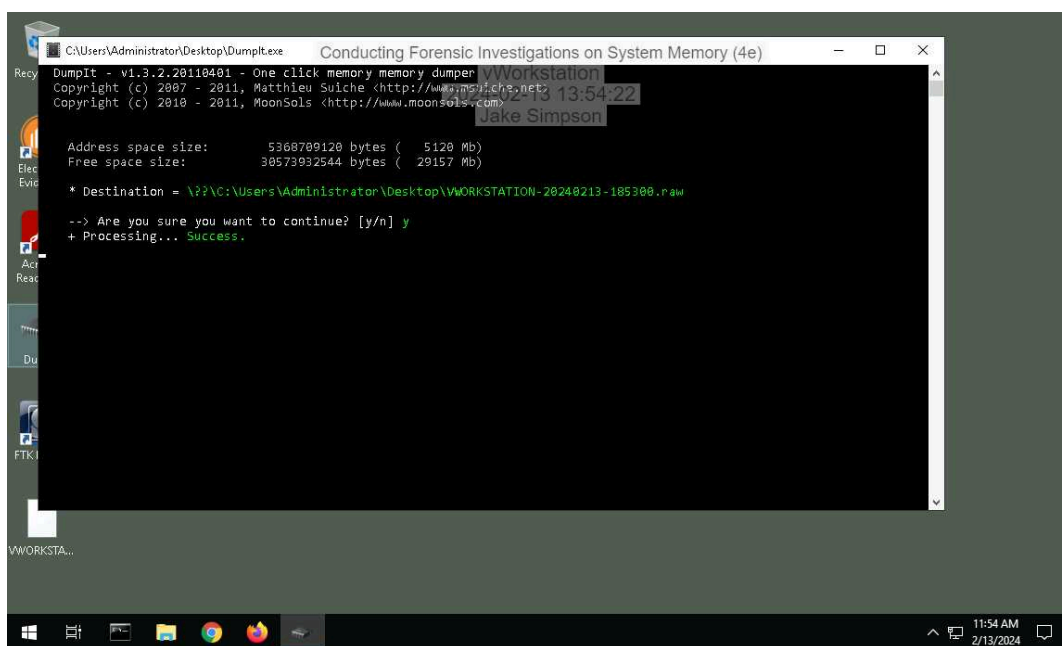
100%

Report Generated: Tuesday, February 13, 2024 at 2:47 PM

Section 1: Hands-On Demonstration

Part 1: Capture Memory using DumpIt

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

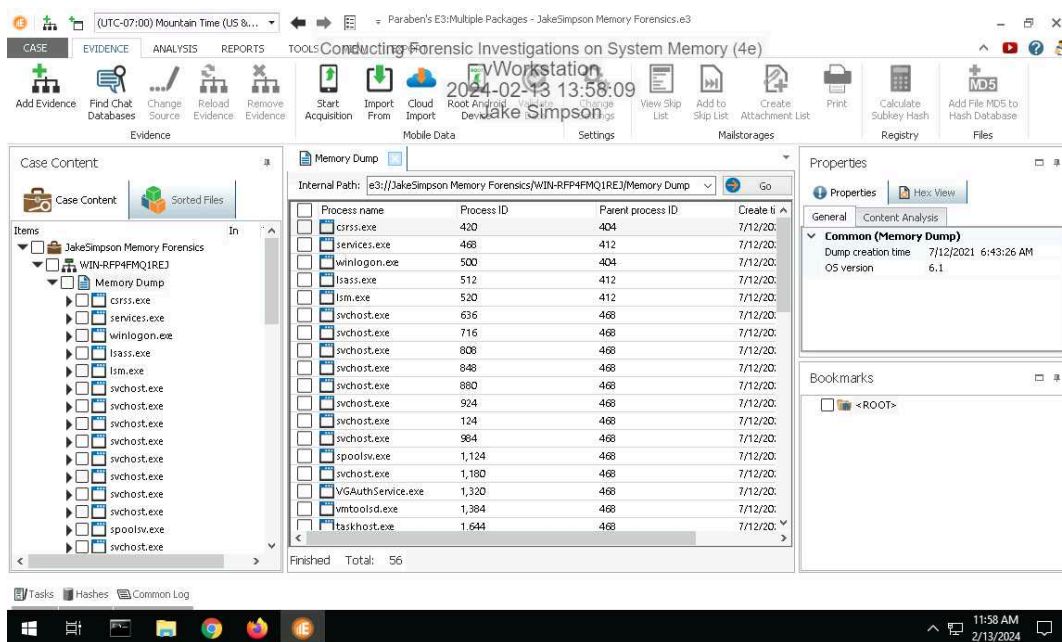


Part 2: Analyze Memory using E3

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 7/12/2021 4:24:49

Newest 7/12/2021 6:42:43

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

It is a legit process used to host the command prompt and powershell sessions.

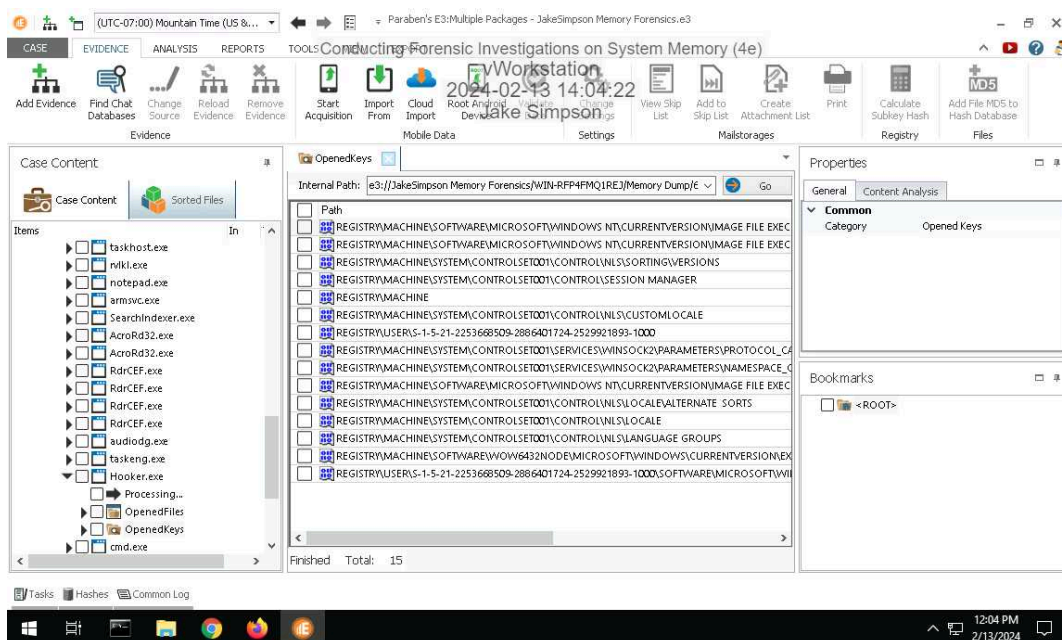
17. Document your findings for the hooker.exe process. What is it and what is it used for?

There is no hooker.exe system process. This could be malware

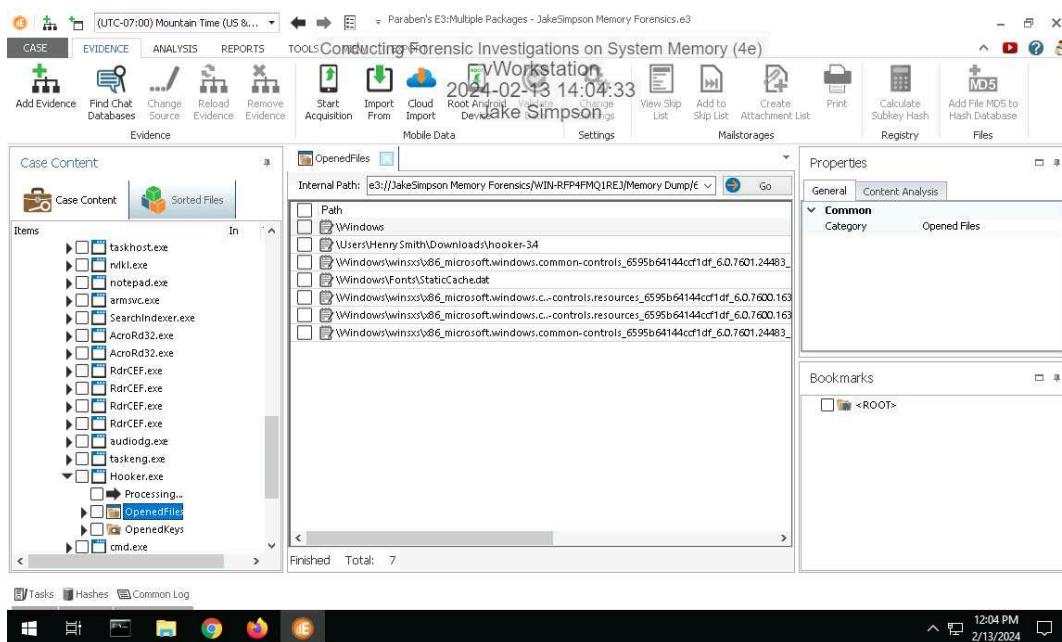
Conducting Forensic Investigations on System Memory (4e)

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

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



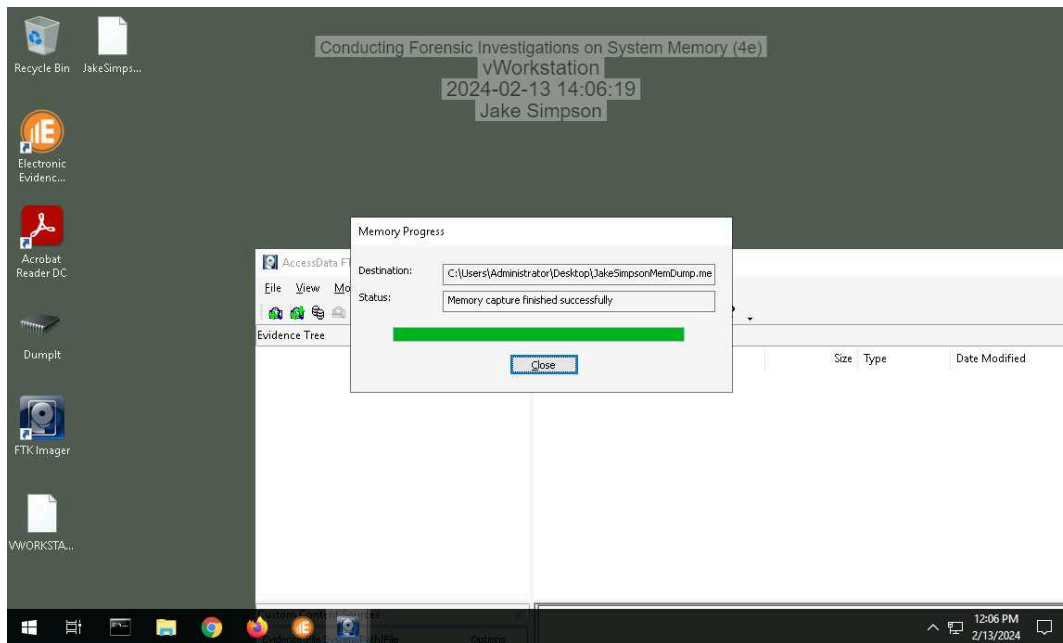
23. Make a screen capture showing the files opened by the hooker.exe process.



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?

PID: 4224 PPID: 1940 Threads: 2

It is the executable file associated with Kaspersky Anti-Virus software

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

None are flagged as hidden they all have the True value

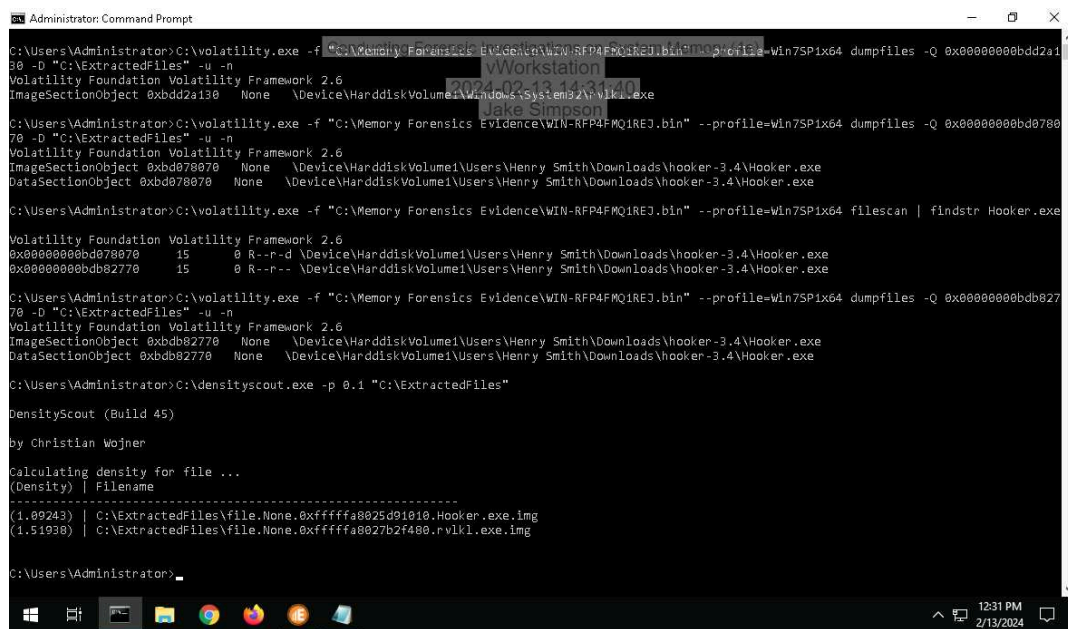
12. **Document** whether the netscan module displays network usage associated with the Hooker.exe or rvkl.exe processes.

It does not

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

Ports 49151 and above are typically used for private services. So it is being used by a custom application.

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



```
Administrator: Command Prompt
C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\WIN-RFP4FQ1REJ.bin" --profile=Win7SP1x64 dumpfiles -Q 0x00000000bdd2a130 -D "C:\ExtractedFiles" -u -n
Volatility Foundation Volatility Framework 2.6
ImageSectionObject 0xbdd2a130 None \Device\HarddiskVolume1\Users\Henry Smith\Downloads\hooker-3.4\Hooker.exe
DataSectionObject 0xbdd2a130 None \Device\HarddiskVolume1\Users\Henry Smith\Downloads\hooker-3.4\Hooker.exe

C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\WIN-RFP4FQ1REJ.bin" --profile=Win7SP1x64 dumpfiles -Q 0x00000000bd078070 -D "C:\ExtractedFiles" -u -n
Volatility Foundation Volatility Framework 2.6
ImageSectionObject 0xbdd078070 None \Device\HarddiskVolume1\Users\Henry Smith\Downloads\hooker-3.4\Hooker.exe
DataSectionObject 0xbdd078070 None \Device\HarddiskVolume1\Users\Henry Smith\Downloads\hooker-3.4\Hooker.exe

C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\WIN-RFP4FQ1REJ.bin" --profile=Win7SP1x64 filescan | findstr Hooker.exe
Volatility Foundation Volatility Framework 2.6
0x00000000bd078070 15 0 R--d \Device\HarddiskVolume1\Users\Henry Smith\Downloads\hooker-3.4\Hooker.exe
0x00000000bd82770 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-RFP4FQ1REJ.bin" --profile=Win7SP1x64 dumpfiles -Q 0x00000000bd82770 -D "C:\ExtractedFiles" -u -n
Volatility Foundation Volatility Framework 2.6
ImageSectionObject 0xbdd82770 None \Device\HarddiskVolume1\Users\Henry Smith\Downloads\hooker-3.4\Hooker.exe
DataSectionObject 0xbdd82770 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.0xffffffff8025d01010.Hooker.exe.img
(1.51930) | C:\ExtractedFiles\file.None.0xffffffff8027b2f400.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.

The processes that connected are 0x7fa9a3d0, 0x7fd01010, 0x7fd01a30

Document the name and purpose of the software you discovered.

Metasploit Framework will often use port 4444

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
0xfffffa8003cc5030 svchost.exe 2620 448 16 246 0 0 2021-08-29 17:35:47 UTC+0000
0xfffffa8003c47b30 svchost.exe 3040 448 13 322 0 0 2021-08-29 17:37:15 UTC+0000
0xfffffa8001c13b30 firefox.exe 2444 2636 76 862 0 0 2021-08-29 17:48:05 UTC+0000
0xfffffa8001c703b0 firefox.exe 2272 2444 0 0 2 0 2021-08-29 17:48:07 UTC+0000
0xfffffa8001c6e8b0 firefox.exe 2060 2444 18 285 2 1 2021-08-29 17:48:07 UTC+0000
0xfffffa8001c1e6f0 firefox.exe 2492 2444 18 280 2 1 2021-08-29 17:48:08 UTC+0000
0xfffffa8001c25360 firefox.exe 1532 2444 17 282 2 1 2021-08-29 17:48:10 UTC+0000
0xfffffa8001cbb30 firefox.exe 2864 2444 8 187 2 1 2021-08-29 17:48:11 UTC+0000
0xfffffa8001c91440 firefox.exe 1576 2444 16 271 2 1 2021-08-29 17:48:23 UTC+0000
0xfffffa8001c0e180 fixtureCompute 2364 2444 3 107 2 0 2021-08-29 17:48:54 UTC+0000
0xfffffa8001a29b30 taskhost.exe 2240 448 5 99 2 0 2021-08-29 17:50:18 UTC+0000
0xfffffa8001c01b30 whoamI.exe 1356 2896 0 0 2 0 2021-08-29 17:50:43 UTC+0000
0xfffffa8001c93b30 whoamI.exe 2992 2260 0 0 2 0 2021-08-29 17:50:43 UTC+0000
0xfffffa8001b0a060 tlor.exe 2768 924 0 0 2 0 2021-08-29 17:50:46 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
```


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

```

Administrator: Command Prompt - C:\Memory Forensics Evidence\ALICE-PC-Win7.raw --profile=Win7SP1x64 yarascan -Y "tior.exe"
0xffffffffb1d060e QaNoQBC.exe 2150 2156 1 26 0 0 2021-08-29 17:57:15 UTC+0000
0xffffffffb003c9d060e cmd.exe 2392 2156 1 26 0 0 2021-08-29 17:57:21 UTC+0000
0xffffffffb001bfc570e conhost.exe 2252 1832 2 49 2 0 2021-08-29 17:57:21 UTC+0000
0xffffffffb001a87950e svchost.exe 1052 448 6 78 0 0 2021-08-29 17:59:33 UTC+0000
0xffffffffb001dicab0e DumpIt.exe 2464 2140 2 45 2 1 2021-08-29 18:00:16 UTC+0000
0xffffffffb001b04520e conhost.exe 2048 1832 2 49 2 0 2021-08-29 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
ERROR : volatility.debug : You must specify a string (-Y) or a rules file (-y)

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 c2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x05448a80 40 42 2f 03 00 00 00 c4 49 60 1e 52 9f 4b 00 .....T.R.K.
0x05448a90 e6 00 00 00 00 00 02 70 6f c2 05 00 00 00 00 ..... po.....
0x05448aa0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 .....
0x05448ab0 02 00 00 00 bc 00 00 ff fc ac 18 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 0b 0c 0c 00 03 00 exe.....
0x05448ae0 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 .....
0x05448b00 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 .....
0x05448b10 cd 07 00 00 00 00 00 40 42 2f 03 00 00 00 00 .....IB.....
0x05448b20 4c 85 b4 6d 3a 8a fa b0 1e 03 00 00 00 00 00 .....L.m.....

```

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

```
C:\Users\Administrator>cmd
Volatility Foundation Volatility Framework 2.6
ERROR : volatility.debug : Invalid PID 7, Producing Forensic Investigations on System Memory (4e)
C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\ALICE-PC-Win7.raw" --profile=win7SP1x64 privs -p 2364, 2156 --silent
Volatility Foundation Volatility Framework 2.6
ERROR : volatility.debug : Invalid PID 2364,
C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\ALICE-PC-Win7.raw" --profile=win7SP1x64 privs -p 2364 --silent
Volatility Foundation Volatility Framework 2.6
Pid Process Value Privilege Attributes Description
-----
C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\ALICE-PC-Win7.raw" --profile=win7SP1x64 privs -p 2156 --silent
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 internal clock
2156 QaNoQBC.exe 35 SeCreateSymbolicLinkPrivilege Present,Enabled Required to create a symbolic link
C:\Users\Administrator>
```