Conducting Forensic Investigations on System Memory (4e)

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

Student:	Email:
Samman Chouhan	schouhan1@hawk.iit.edu

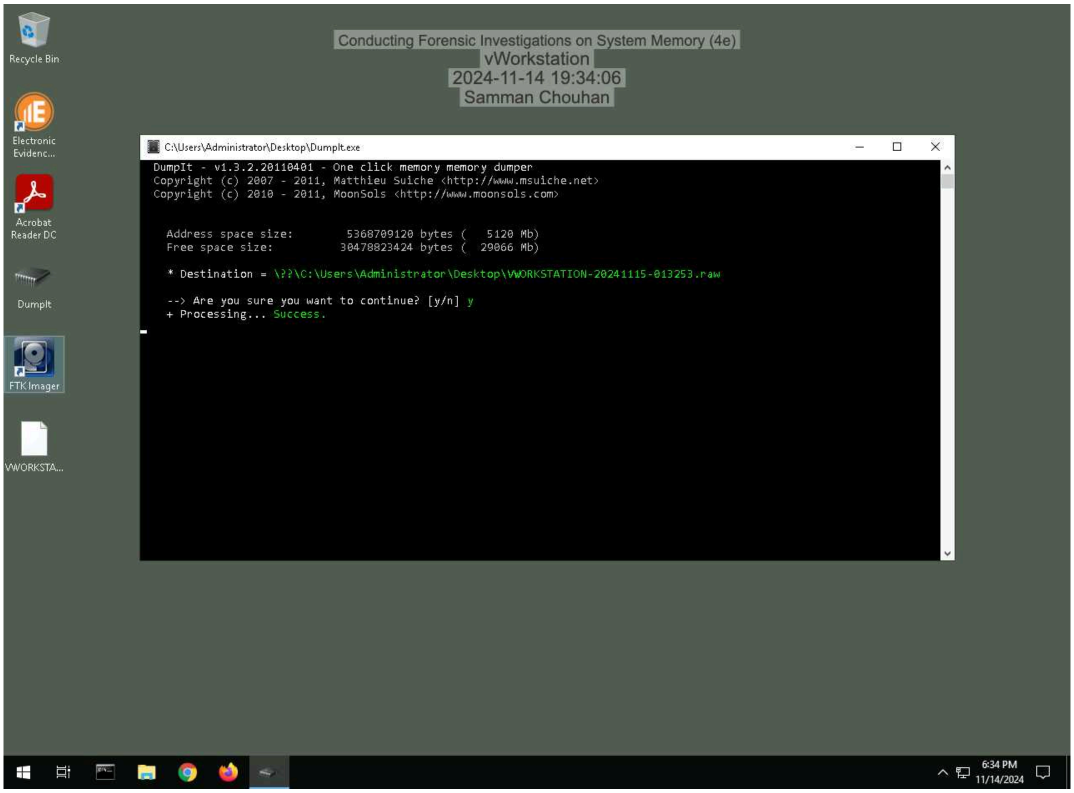
Time on Task:	Progress:
1 hour, 33 minutes	100%

Report Generated: Saturday, November 23, 2024 at 5:08 PM

Section 1: Hands-On Demonstration

Part 1: Capture Memory using DumpIt

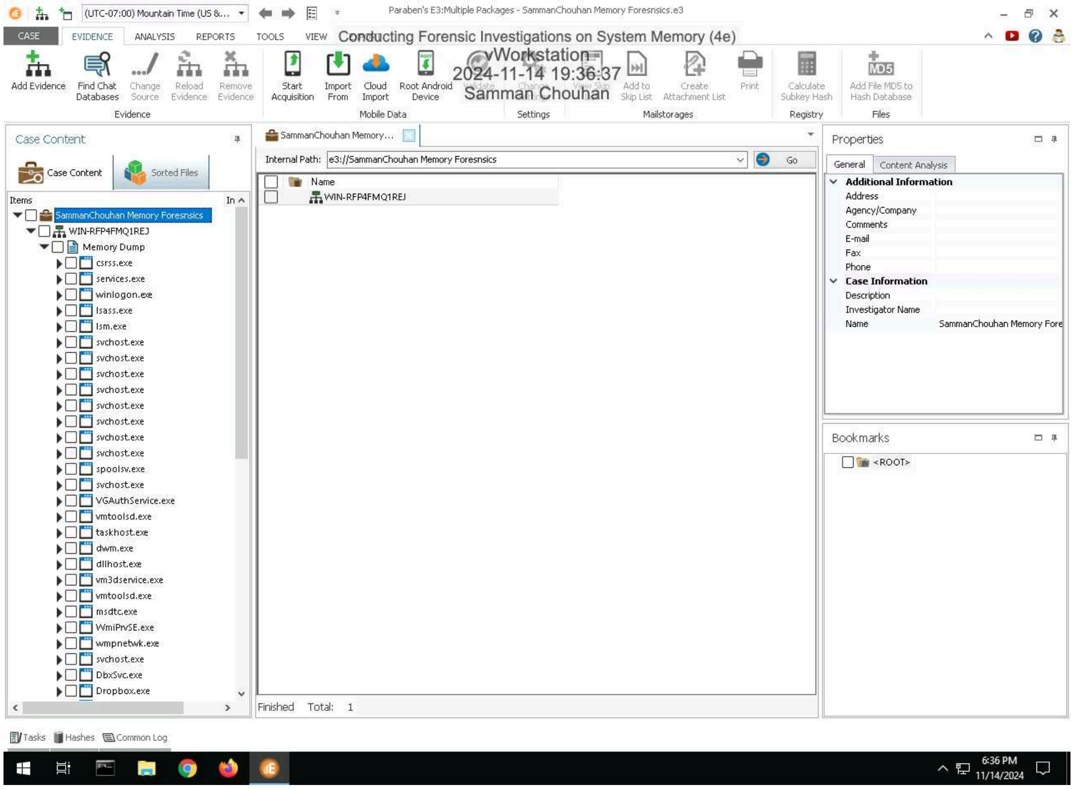
3. **Make a screen capture** showing the **DumpIt success notification**.



```
DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>


  Address space size:        5368709120 bytes (   5120 Mb)
  Free space size:          30478823424 bytes (  29066 Mb)

  * Destination = \??\C:\Users\Administrator\Desktop\VWORKSTATION-20241115-013253.raw

  --> Are you sure you want to continue? [y/n] y
  + Processing... Success.
```

Part 2: Analyze Memory using E3

8. **Make a screen capture** showing the **list of processes in the memory dump**.



```
Items
▼ □ SammanChouhan Memory Foresnsics
  ▼ □ WIN-RFP4FMQ1REJ
    ▼ □ Memory Dump
      ▶ □ csrss.exe
      ▶ □ services.exe
      ▶ □ winlogon.exe
      ▶ □ lsass.exe
      ▶ □ lsm.exe
      ▶ □ svchost.exe
      ▶ □ svchost.exe
      ▶ □ svchost.exe
      ▶ □ svchost.exe
      ▶ □ svchost.exe
      ▶ □ svchost.exe
      ▶ □ svchost.exe
      ▶ □ svchost.exe
      ▶ □ spoolsv.exe
      ▶ □ svchost.exe
      ▶ □ VGAuthService.exe
      ▶ □ vmtoolsd.exe
      ▶ □ taskhost.exe
      ▶ □ dwm.exe
      ▶ □ dllhost.exe
      ▶ □ vm3dservice.exe
      ▶ □ vmtoolsd.exe
      ▶ □ msdtc.exe
      ▶ □ WmiPrvSE.exe
      ▶ □ wmpnetwk.exe
      ▶ □ svchost.exe
      ▶ □ DbxSvc.exe
      ▶ □ Dropbox.exe
```

SammanChouhan Memory...

Internal Path: e3://SammanChouhan Memory Foresnsics

□	Name
□	WIN-RFP4FMQ1REJ

Finished Total: 1

Additional Information
- Address
- Agency/Company
- Comments
- E-mail
- Fax
- Phone

Case Information
- Description
- Investigator Name
- Name: SammanChouhan Memory Fore

10. **Record** the start times for the oldest process and the newest process.

The First process system was started at 7/12/2021 at 4:24:29 AM , and the last process was started at 7/12/2021 6:42:43AM

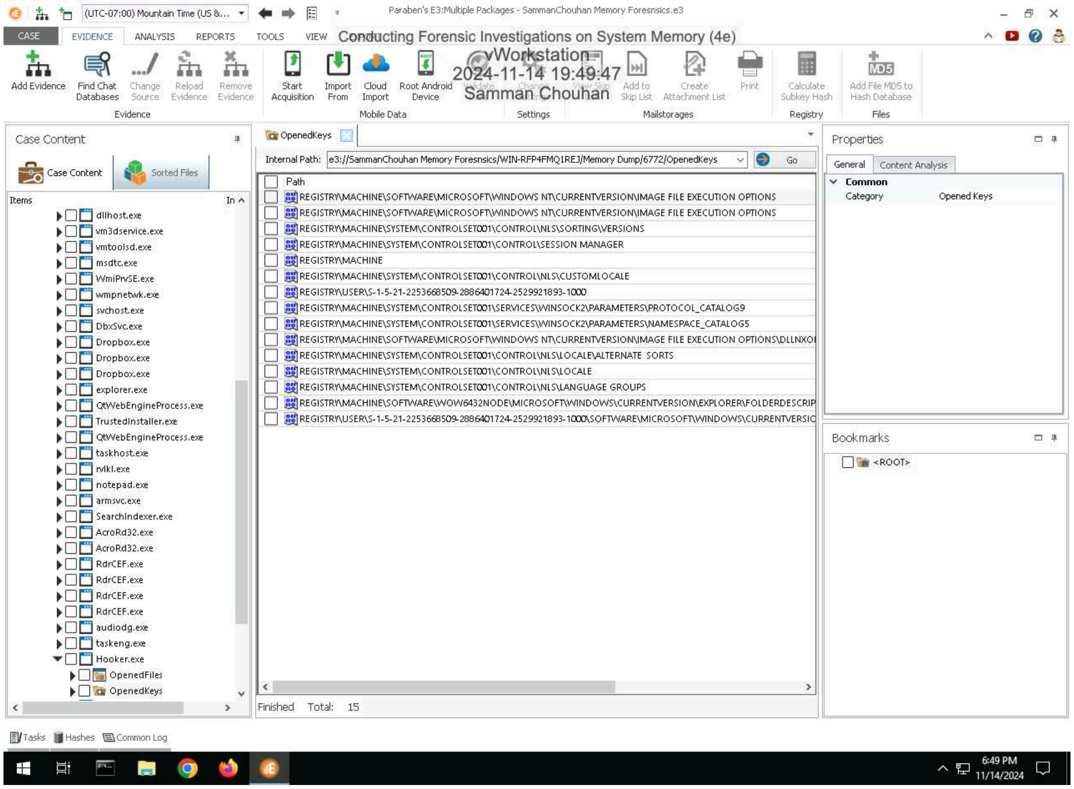
15. **Document** your findings for the conhost.exe process. What is it and what is it used for?

The conhost.exe (Console Windows Host) file is provided by Microsoft.Conhost.exe needs to run for Command Prompt to interface with File Explorer. One of its duties is to provide the ability to drag and drop files/folders directly into Command Prompt. Even third-party programs can use conhost.exe if they need access to the command line.

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

Hooker is a password and data stealing trojan. Being run it installs itself as KERN32.EXE (name may differ in different versions) into \Windows\System\ directory and modifies RunOnce key in the Registry to be run during next Windows session. When activated next time the trojan renews the RunOnce key, so it becomes active during all Windows sessions.

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



Items

- dllhost.exe
- vm3dservice.exe
- vmtoolsd.exe
- msdtc.exe
- WmiPrvSE.exe
- wmpnetwk.exe
- svchost.exe
- DbxSvc.exe
- Dropbox.exe
- Dropbox.exe
- Dropbox.exe
- explorer.exe
- QtWebEngineProcess.exe
- TrustedInstaller.exe
- QtWebEngineProcess.exe
- taskhost.exe
- rvlkl.exe
- notepad.exe
- armsvc.exe
- SearchIndexer.exe
- AcroRd32.exe
- AcroRd32.exe
- RdrCEF.exe
- RdrCEF.exe
- RdrCEF.exe
- RdrCEF.exe
- audiodg.exe
- taskeng.exe
- Hooker.exe
  - OpenedFiles
  - OpenedKeys

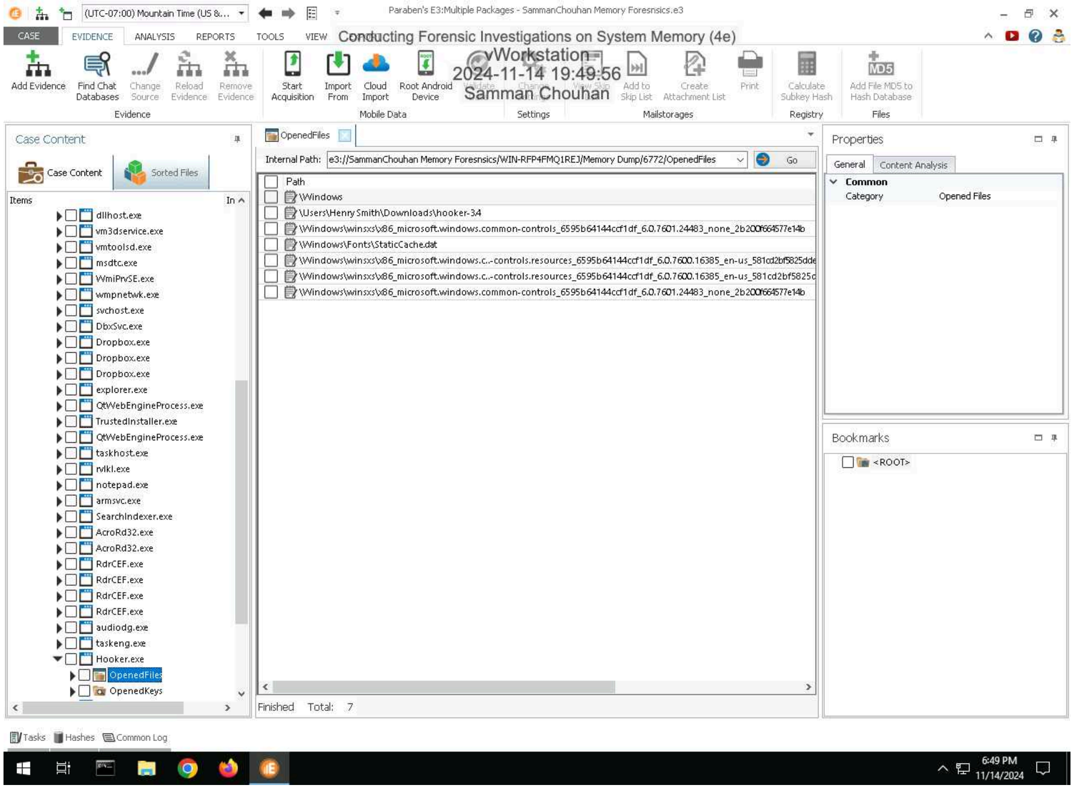
Internal Path: e3://SammanChouhan Memory Foresnsics/WIN-RFP4FMQ1REJ/Memory Dump/6772/OpenedKeys

```
Path
REGISTRY\MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\IMAGE FILE EXECUTION OPTIONS
REGISTRY\MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\IMAGE FILE EXECUTION OPTIONS
REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\SORTING\VERSIONS
REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\SESSION MANAGER
REGISTRY\MACHINE
REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\CUSTOMLOCALE
REGISTRY\USER\S-1-5-21-2253668509-2886401724-2529921893-1000
REGISTRY\MACHINE\SYSTEM\CONTROLSET001\SERVICES\WINSOCK2\PARAMETERS\PROTOCOL_CATALOG9
REGISTRY\MACHINE\SYSTEM\CONTROLSET001\SERVICES\WINSOCK2\PARAMETERS\NAMESPACE_CATALOG5
REGISTRY\MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\IMAGE FILE EXECUTION OPTIONS\DLLNXOI
REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\LOCALE\ALTERNATE SORTS
REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\LOCALE
REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\LANGUAGE GROUPS
REGISTRY\MACHINE\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\FOLDERDESCRIP
REGISTRY\USER\S-1-5-21-2253668509-2886401724-2529921893-1000\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSIC
```

Finished Total: 15

Properties: Common — Category: Opened Keys

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



Conducting Forensic Investigations on System Memory (4e)
vWorkstation
2024-11-14 19:49:56
Samman Chouhan

dllhost.exe
vm3dservice.exe
vmtoolsd.exe
msdtc.exe
WmiPrvSE.exe
wmpnetwk.exe
svchost.exe
DbxSvc.exe
Dropbox.exe
Dropbox.exe
Dropbox.exe
explorer.exe
QtWebEngineProcess.exe
TrustedInstaller.exe
QtWebEngineProcess.exe
taskhost.exe
rvlkl.exe
notepad.exe
armsvc.exe
SearchIndexer.exe
AcroRd32.exe
AcroRd32.exe
RdrCEF.exe
RdrCEF.exe
RdrCEF.exe
RdrCEF.exe
audiodg.exe
taskeng.exe
Hooker.exe
OpenedFiles
OpenedKeys

OpenedFiles

Internal Path: e3://SammanChouhan Memory Foresnsics/WIN-RFP4FMQ1REJ/Memory Dump/6772/OpenedFiles Go

Path
\Windows
\Users\Henry Smith\Downloads\hooker-3.4
\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.24483_none_2b200f664577e14b
\Windows\Fonts\StaticCache.dat
\Windows\winsxs\x86_microsoft.windows.c..-controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_581cd2bf5825dde
\Windows\winsxs\x86_microsoft.windows.c..-controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_581cd2bf5825c
\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.24483_none_2b200f664577e14b

Finished Total: 7

Properties

General Content Analysis

Common
Category Opened Files

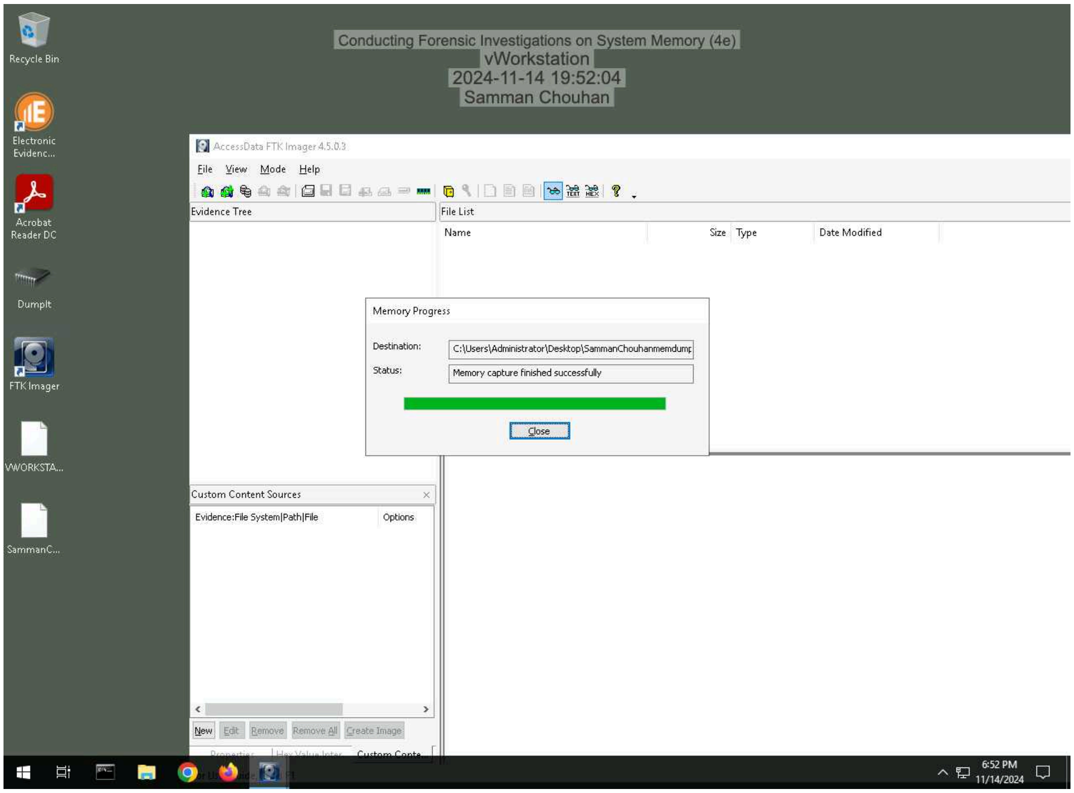
Bookmarks

□ <ROOT>

Section 2: Applied Learning

Part 1: Capture Memory using FTK Imager

6. **Make a screen capture** showing the ***Memory capture finished successfully* confirmation.**


Conducting Forensic Investigations on System Memory (4e)
vWorkstation
2024-11-14 19:52:04
Samman Chouhan

AccessData FTK Imager 4.5.0.3

Memory Progress

Destination: C:\Users\Administrator\Desktop\SammanChouhanmemdump

Status: Memory capture finished successfully

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 file rvlkl.exe is associated with Revealer Keylogger, a software developed by Logixoft designed to monitor and record keystrokes on a computer. This tool is often used for legitimate purposes, such as parental monitoring or employee activity tracking, but it can also be misused for malicious intent, such as unauthorized data collection or spying.

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

the process hooker.exe seems to be hidden and is found malicious

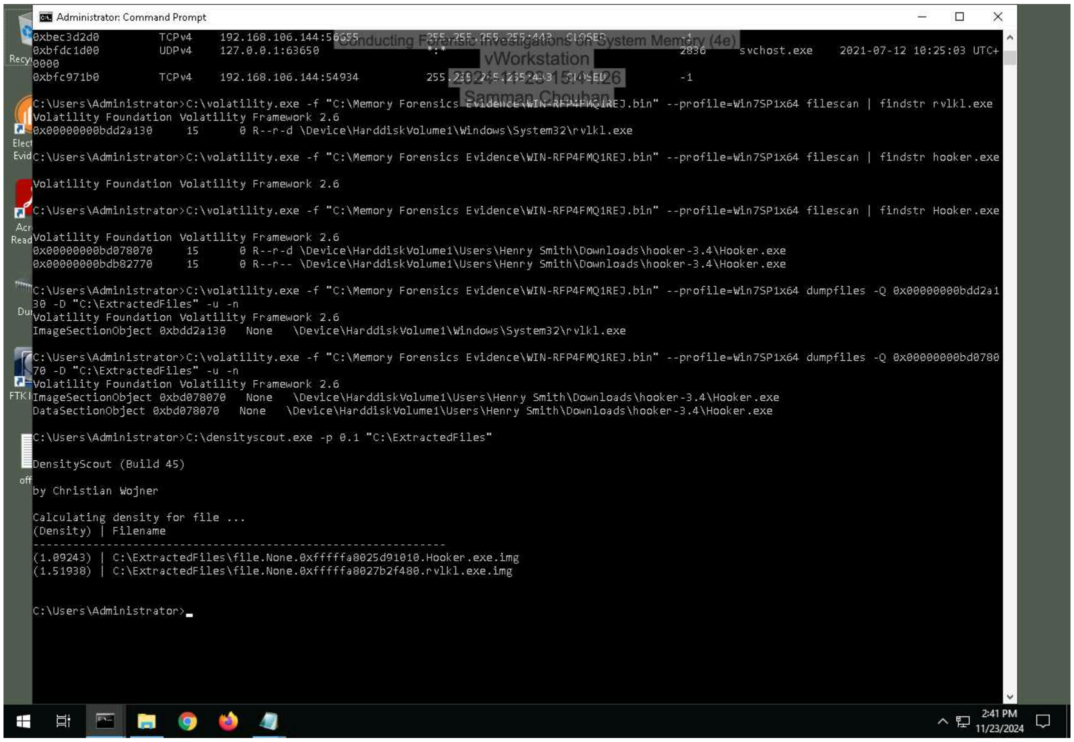
12. **Document** whether the netscan module displays network usage associated with the Hooker.exe or rvlkl.exe processes.

no the netscan module doesn't show any direct reference to the hooker.exe or rvlkl.exe module, even after searching with the same pid , i do not see anything , although i see -1 as a pid which is usually used foe undefined slots ,which i will investigate further

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

Port 56610 is not assigned a specific purpose or service by the Internet Assigned Numbers Authority (IANA), which maintains a registry of officially recognized ports and their uses. Instead, it is part of the ephemeral port range, which typically spans ports 49152 through 65535. If you notice unusual activity involving port 56610, it could indicate malware, unauthorized access, or misconfigured software.Such ports are dynamically assigned by the operating system and used for private communication between software processes.

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


Administrator: Command Prompt
Conducting Forensic Investigations on System Memory (4e)
vWorkstation
2024-11-23 15:41:26
Samman Chouhan
2:41 PM
11/23/2024

```
0xbec3d2d0         TCPv4    192.168.106.144:56655          255.255.255.255:443  CLOSED          -1
0xbfdc1d00         UDPv4    127.0.0.1:63650                *:*                                  2836     svchost.exe    2021-07-12 10:25:03 UTC+
0000
0xbfc971b0         TCPv4    192.168.106.144:54934          255.255.255.255:443  CLOSED          -1

C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\WIN-RFP4FMQ1REJ.bin" --profile=Win7SP1x64 filescan | findstr rvlkl.exe
Volatility Foundation Volatility Framework 2.6
0x00000000bdd2a130     15      0 R--r-d \Device\HarddiskVolume1\Windows\System32\rvlkl.exe

C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\WIN-RFP4FMQ1REJ.bin" --profile=Win7SP1x64 filescan | findstr hooker.exe

Volatility Foundation Volatility Framework 2.6

C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\WIN-RFP4FMQ1REJ.bin" --profile=Win7SP1x64 filescan | findstr Hooker.exe

Volatility Foundation Volatility Framework 2.6
0x00000000bd078070     15      0 R--r-d \Device\HarddiskVolume1\Users\Henry Smith\Downloads\hooker-3.4\Hooker.exe
0x00000000bdb82770     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-RFP4FMQ1REJ.bin" --profile=Win7SP1x64 dumpfiles -Q 0x00000000bdd2a1
30 -D "C:\ExtractedFiles" -u -n
Volatility Foundation Volatility Framework 2.6
ImageSectionObject 0xbdd2a130   None   \Device\HarddiskVolume1\Windows\System32\rvlkl.exe

C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\WIN-RFP4FMQ1REJ.bin" --profile=Win7SP1x64 dumpfiles -Q 0x00000000bd0780
70 -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:\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.rvlkl.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.

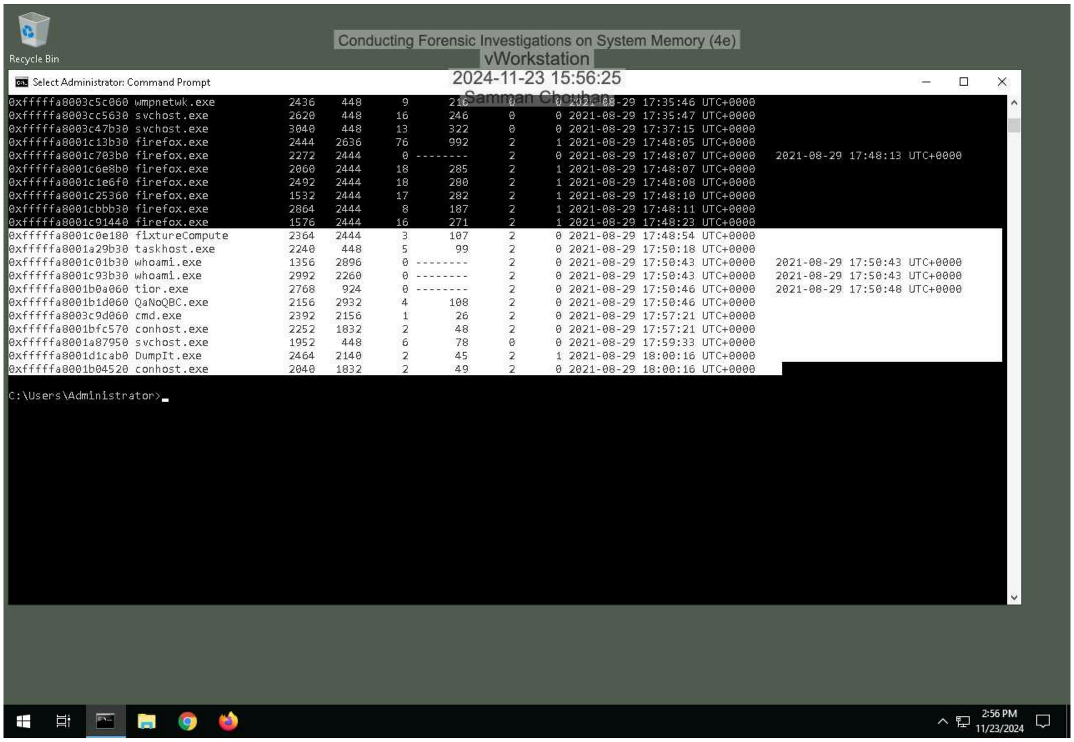
The three process that were found to be connected on 205.134.253.10:4444 , were dllhost.exe ,QaNoQBC.exe and fixturecompute

Document the name and purpose of the software you discovered.

dllhost.exe is a legitimate Windows process, known as the COM Surrogate, that handles COM objects to ensure system stability, like generating thumbnails in Explorer. QaNoQBC.exe is not a recognized system file and likely indicates a custom application or potential malware requiring investigation. Similarly, fixturecompute appears to be an uncommon term or file, possibly related to computational or testing tasks, though it might also signify malicious activity.

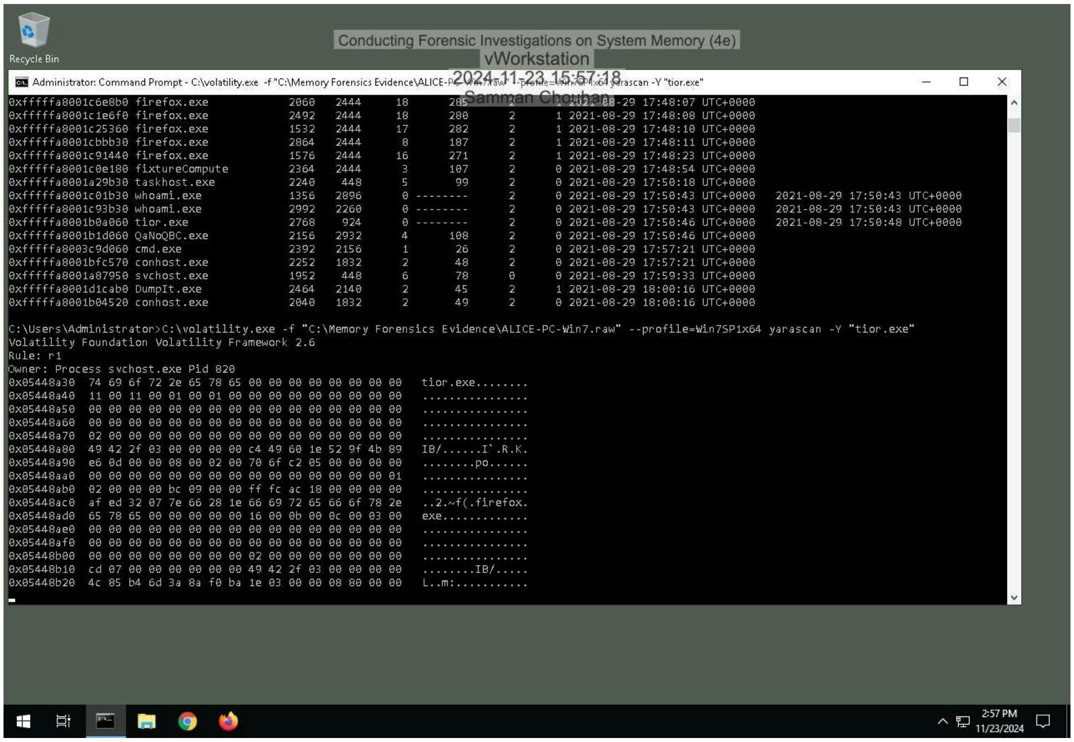
Part 2: Identify Malicious Processes

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


Recycle Bin
Conducting Forensic Investigations on System Memory (4e)
vWorkstation
2024-11-23 15:56:25
Samman Chouhan
Select Administrator: Command Prompt
2:56 PM
11/23/2024

```
0xfffffa8003c5c060 wmpnetwk.exe           2436    448      9      216      0      0 2021-08-29 17:35:46 UTC+0000
0xfffffa8003cc5630 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      992      2      1 2021-08-29 17:48:05 UTC+0000
0xfffffa8001c703b0 firefox.exe            2272   2444      0 --------      2      0 2021-08-29 17:48:07 UTC+0000   2021-08-29 17:48:13 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
0xfffffa8001cbbb30 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 --------      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>
```

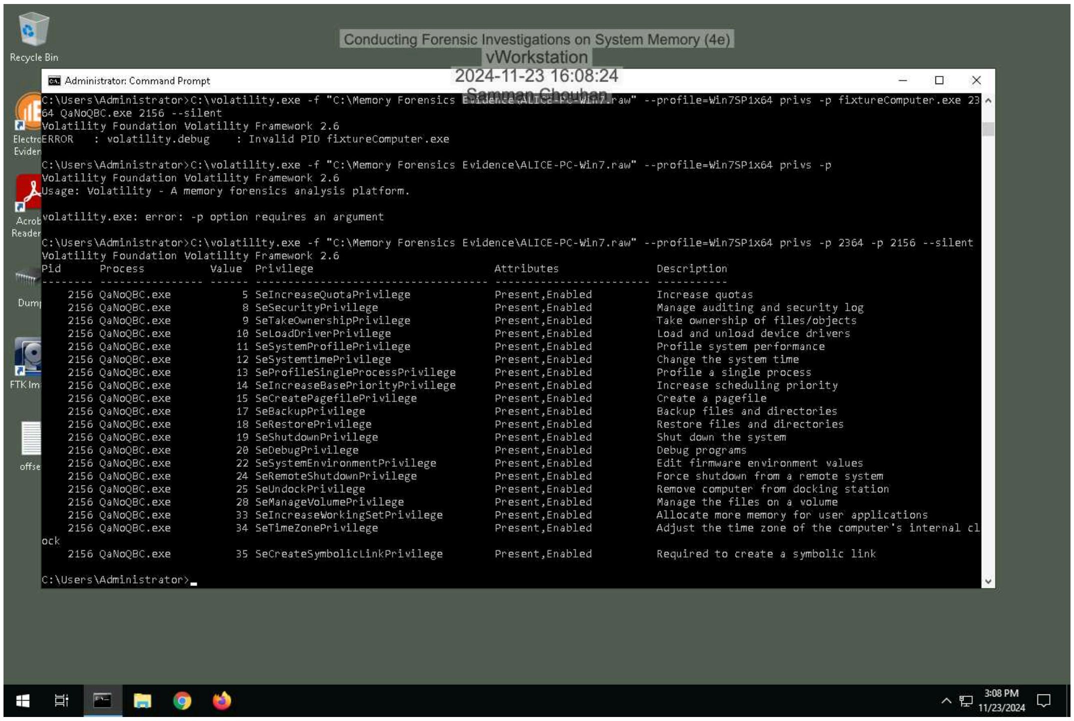
Make a screen capture showing the **output of the yarascan**.


Recycle Bin
Conducting Forensic Investigations on System Memory (4e)
vWorkstation
2024-11-23 15:57:18
Samman Chouhan
Administrator: Command Prompt - C:\volatility.exe -f "C:\Memory Forensics Evidence\ALICE-PC-Win7.raw" --profile=Win7SP1x64 yarascan -Y "tior.exe"
2:57 PM
11/23/2024

```
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
0xfffffa8001cbbb30 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 --------      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>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 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 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 80 00 00   L..m:...........
```

Part 3: Identify Privilege Escalation

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



```
C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\ALICE-PC-Win7.raw" --profile=Win7SP1x64 privs -p fixtureComputer.exe 23
64 QaNoQBC.exe 2156 --silent
Volatility Foundation Volatility Framework 2.6
ERROR   : volatility.debug    : Invalid PID fixtureComputer.exe

C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\ALICE-PC-Win7.raw" --profile=Win7SP1x64 privs -p
Volatility Foundation Volatility Framework 2.6
Usage: Volatility - A memory forensics analysis platform.

volatility.exe: error: -p option requires an argument

C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\ALICE-PC-Win7.raw" --profile=Win7SP1x64 privs -p 2364 -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 cl
ock
    2156 QaNoQBC.exe          35 SeCreateSymbolicLinkPrivilege        Present,Enabled          Required to create a symbolic link

C:\Users\Administrator>
```