Conducting Forensic Investigations on System Memory (4e)

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

Student:	Email:
Matias Kun	rvh4zx@virginia.edu

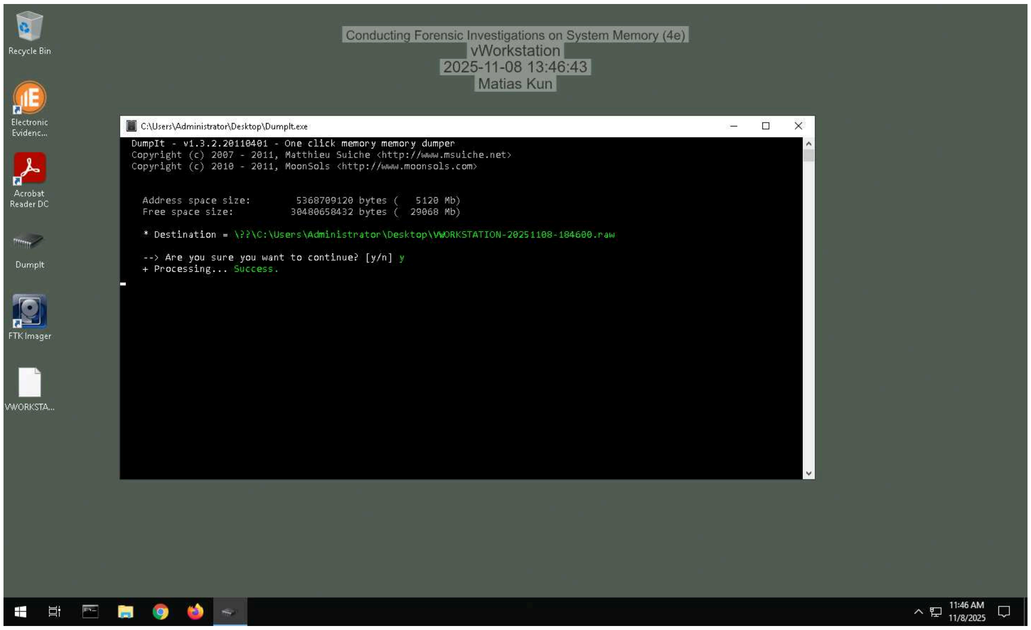
Time on Task:	Progress:
6 hours, 4 minutes	100%

Report Generated: Saturday, November 8, 2025 at 3:54 PM

Section 1: Hands-On Demonstration

Part 1: Capture Memory using DumpIt

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



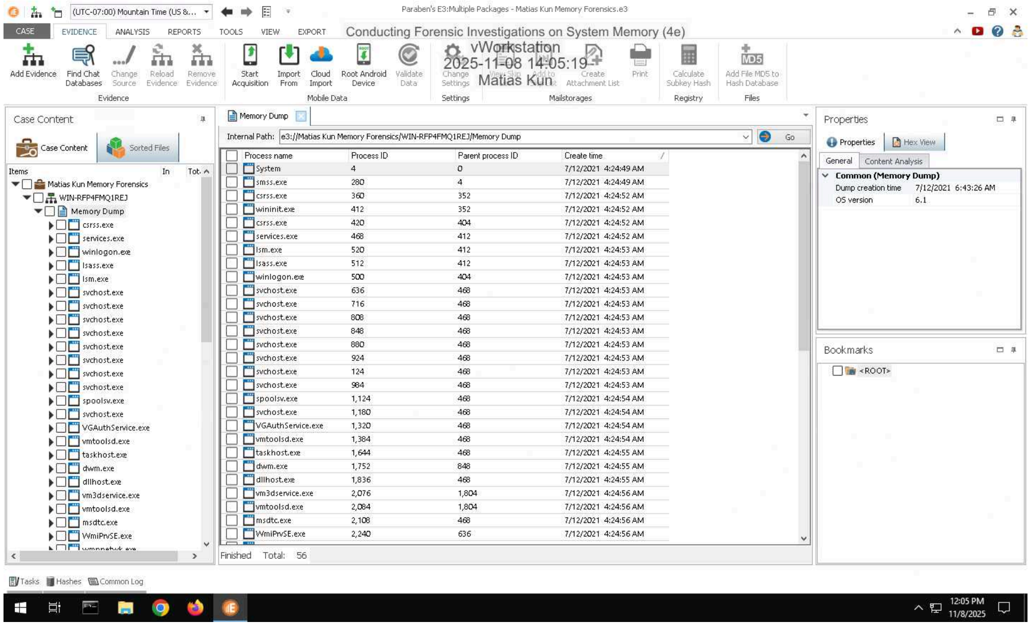
Conducting Forensic Investigations on System Memory (4e)
vWorkstation
2025-11-08 13:46:43
Matias Kun

C:\Users\Administrator\Desktop\DumpIt.exe

```
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:          30480658432 bytes (  29068 Mb)

  * Destination = \??\C:\Users\Administrator\Desktop\VWORKSTATION-20251108-184600.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**.



Case Content

Items / In / Tot.
- Matias Kun Memory Forensics
  - 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

Memory Dump

Internal Path: e3://Matias Kun Memory Forensics/WIN-RFP4FMQ1REJ/Memory Dump

Process name	Process ID	Parent process ID	Create time
System	4	0	7/12/2021 4:24:49 AM
smss.exe	280	4	7/12/2021 4:24:49 AM
csrss.exe	360	352	7/12/2021 4:24:52 AM
wininit.exe	412	352	7/12/2021 4:24:52 AM
csrss.exe	420	404	7/12/2021 4:24:52 AM
services.exe	468	412	7/12/2021 4:24:52 AM
lsm.exe	520	412	7/12/2021 4:24:53 AM
lsass.exe	512	412	7/12/2021 4:24:53 AM
winlogon.exe	500	404	7/12/2021 4:24:53 AM
svchost.exe	636	468	7/12/2021 4:24:53 AM
svchost.exe	716	468	7/12/2021 4:24:53 AM
svchost.exe	808	468	7/12/2021 4:24:53 AM
svchost.exe	848	468	7/12/2021 4:24:53 AM
svchost.exe	880	468	7/12/2021 4:24:53 AM
svchost.exe	924	468	7/12/2021 4:24:53 AM
svchost.exe	124	468	7/12/2021 4:24:53 AM
svchost.exe	984	468	7/12/2021 4:24:53 AM
spoolsv.exe	1,124	468	7/12/2021 4:24:54 AM
svchost.exe	1,180	468	7/12/2021 4:24:54 AM
VGAuthService.exe	1,320	468	7/12/2021 4:24:54 AM
vmtoolsd.exe	1,384	468	7/12/2021 4:24:54 AM
taskhost.exe	1,644	468	7/12/2021 4:24:55 AM
dwm.exe	1,752	848	7/12/2021 4:24:55 AM
dllhost.exe	1,836	468	7/12/2021 4:24:55 AM
vm3dservice.exe	2,076	1,804	7/12/2021 4:24:56 AM
vmtoolsd.exe	2,084	1,804	7/12/2021 4:24:56 AM
msdtc.exe	2,108	468	7/12/2021 4:24:56 AM
WmiPrvSE.exe	2,240	636	7/12/2021 4:24:56 AM

Finished Total: 56

Properties

General | Content Analysis

Common (Memory Dump)	
Dump creation time	7/12/2021 6:43:26 AM
OS version	6.1

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

Oldest process start time was July 12, 2021 at 4:24:49 AM. Newest process start time was 6:42:43 AM on July 12, 2021

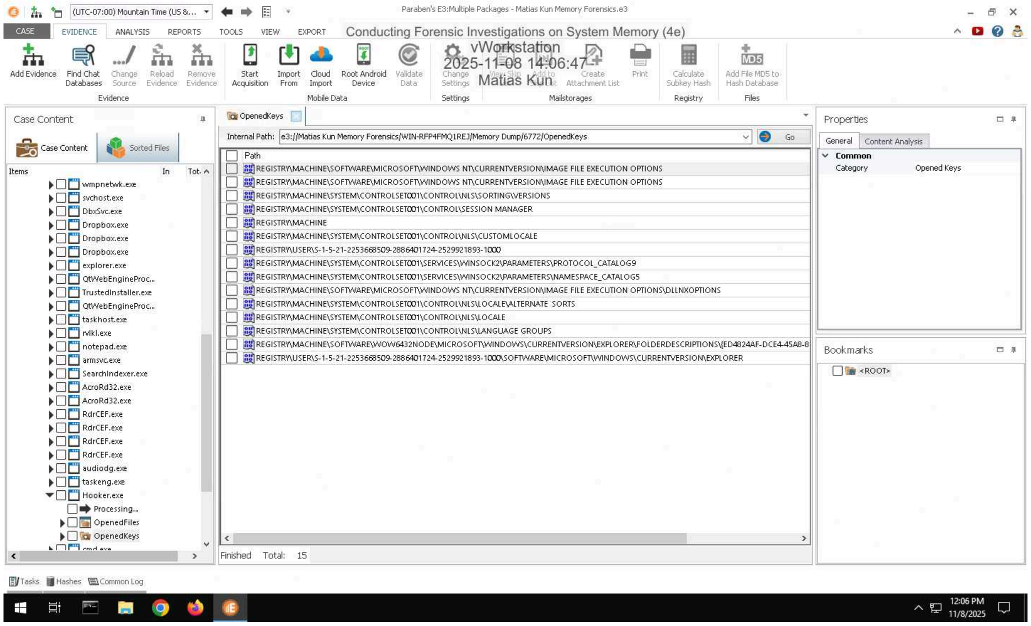
15. **Document** your findings for the conhost.exe process. What is it and what is it used for?

The Conhost.exe process is used for core services to the Command Prompt. It is used for features allowing the Command Prompt to function with Windows Explorer to drag and drop files and folders to the terminal window. It stands for "Console Window Host" and it is a legitimate program. However, it can be susceptible to vulnerabilities caused by hackers.

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

The Hooker.exe process is not a Windows system file. But rather, a program used to record keyboard shortcuts as well as connect to the internet, record keyboard and mouse inputs, and monitor applications. In other words, it is a keylogger process. It is considered a malicious application and is vulnerable to attacks.

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



Conducting Forensic Investigations on System Memory (4e)
vWorkstation
2025-11-08 14:06:47
Matias Kun

OpenedKeys

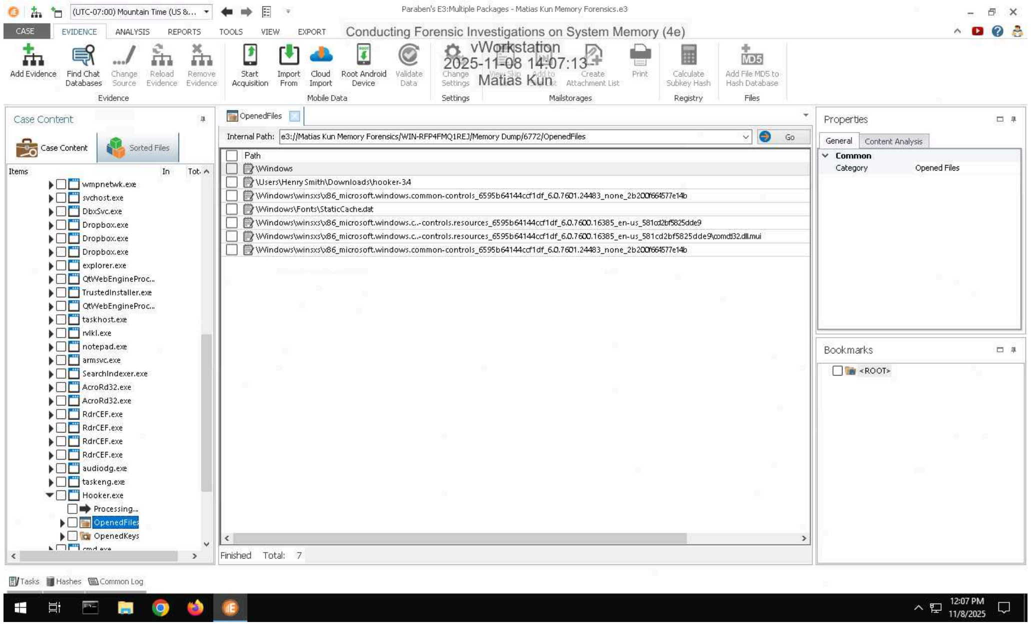
Internal Path: e3://Matias Kun Memory Forensics/WIN-RFP4FMQ1REJ/Memory Dump/6772/OpenedKeys

```
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\DLLNXOPTIONS
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\FOLDERDESCRIPTIONS\{ED4824AF-DCE4-45A8-8
REGISTRY\USER\S-1-5-21-2253668509-2886401724-2529921893-1000\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER
```

Finished Total: 15

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
2025-11-08 14:07:13
Matias Kun

OpenedFiles

Internal Path: e3://Matias Kun Memory Forensics/WIN-RFP4FMQ1REJ/Memory Dump/6772/OpenedFiles

```
Path
\Windows
\Users\Henry Smith\Downloads\hooker-34
\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_581cd2bf5825dde9
\Windows\winsxs\x86_microsoft.windows.c..-controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_581cd2bf5825dde9\comctl32.dll.mui
\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.24483_none_2b200f664577e14b
```

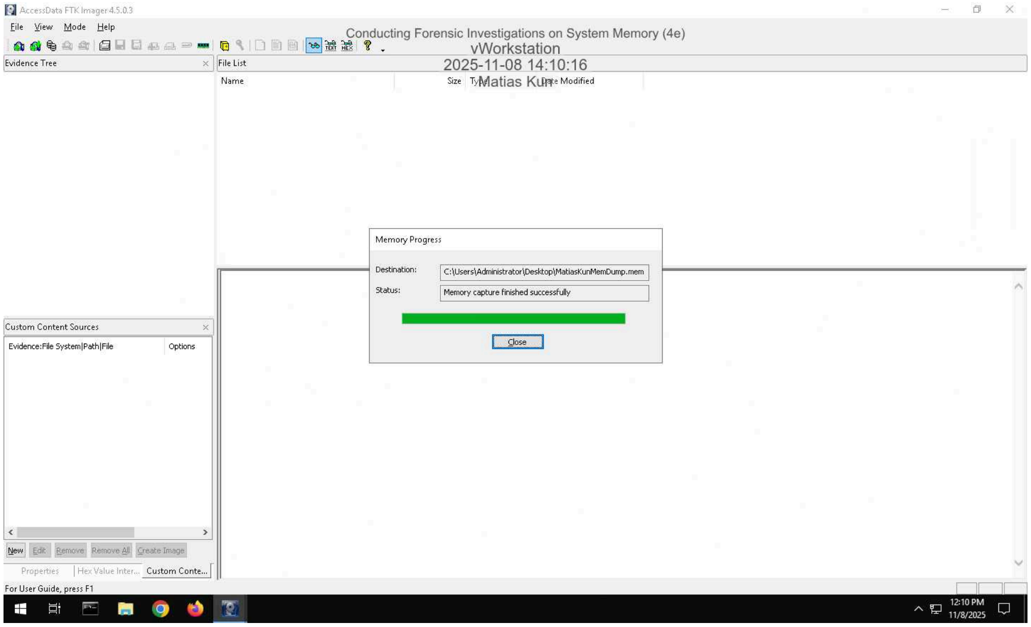
Finished Total: 7

Common
Category: Opened Files

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
2025-11-08 14:10:16
Matias Kun

Memory Progress

Destination: C:\Users\Administrator\Desktop\MatiasKunMemDump.mem

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 rvlkl.exe process is a security and monitoring software tool which is named "Logixoft's Revealer Keylogger." The tool creates log files of all usage, including screenshots and logs, that can be remotely sent to the customer. This program is invisible. The program also has a digital signature and is able to record keyboard and mouse inputs, as well as monitor inputs. It is not considered fully safe to use and may not work properly with some layouts.

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

There are three different processes that are flagged as hidden.
One is services.exe. The other two are lsass.exe and lsm.exe.

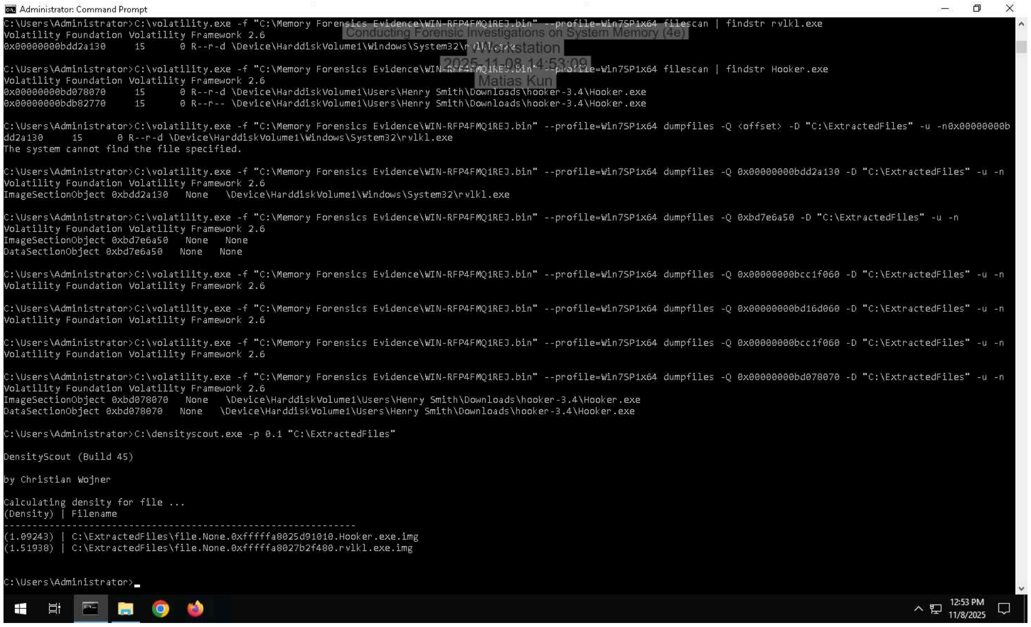
12. **Document** whether the netscan module displays network usage associated with the Hooker.exe or rvlkl.exe processes.

The netscan module displays that there are network usages associated with the Hooker.exe and rvlkl.exe processes through the Chrome Browser and Dropbox applications.

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

The information I discovered regarding port 56610 was that it is a dynamic and private port that is used for accessing files on the system. The program name for the filesystem access tools is Xsan, also konwn as Xsan Filesystem Access.

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


Administrator: Command Prompt
Conducting Forensic Investigations on System Memory (4e)
Workstation
2025-11-08 14:53:09
Matias Kun
12:53 PM
11/8/2025

```
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
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 <offset> -D "C:\ExtractedFiles" -u -n0x00000000b
dd2a130     15      0 R--r-d \Device\HarddiskVolume1\Windows\System32\rvlkl.exe
The system cannot find the file specified.

C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\WIN-RFP4FMQ1REJ.bin" --profile=Win7SP1x64 dumpfiles -Q 0x00000000bdd2a130 -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 0xbd7e6a50 -D "C:\ExtractedFiles" -u -n
Volatility Foundation Volatility Framework 2.6
ImageSectionObject 0xbd7e6a50   None   None
DataSectionObject 0xbd7e6a50   None   None

C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\WIN-RFP4FMQ1REJ.bin" --profile=Win7SP1x64 dumpfiles -Q 0x00000000bcc1f060 -D "C:\ExtractedFiles" -u -n
Volatility Foundation Volatility Framework 2.6

C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\WIN-RFP4FMQ1REJ.bin" --profile=Win7SP1x64 dumpfiles -Q 0x00000000bd16d060 -D "C:\ExtractedFiles" -u -n
Volatility Foundation Volatility Framework 2.6

C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\WIN-RFP4FMQ1REJ.bin" --profile=Win7SP1x64 dumpfiles -Q 0x00000000bcc1f060 -D "C:\ExtractedFiles" -u -n
Volatility Foundation Volatility Framework 2.6

C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\WIN-RFP4FMQ1REJ.bin" --profile=Win7SP1x64 dumpfiles -Q 0x00000000bd078070 -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.

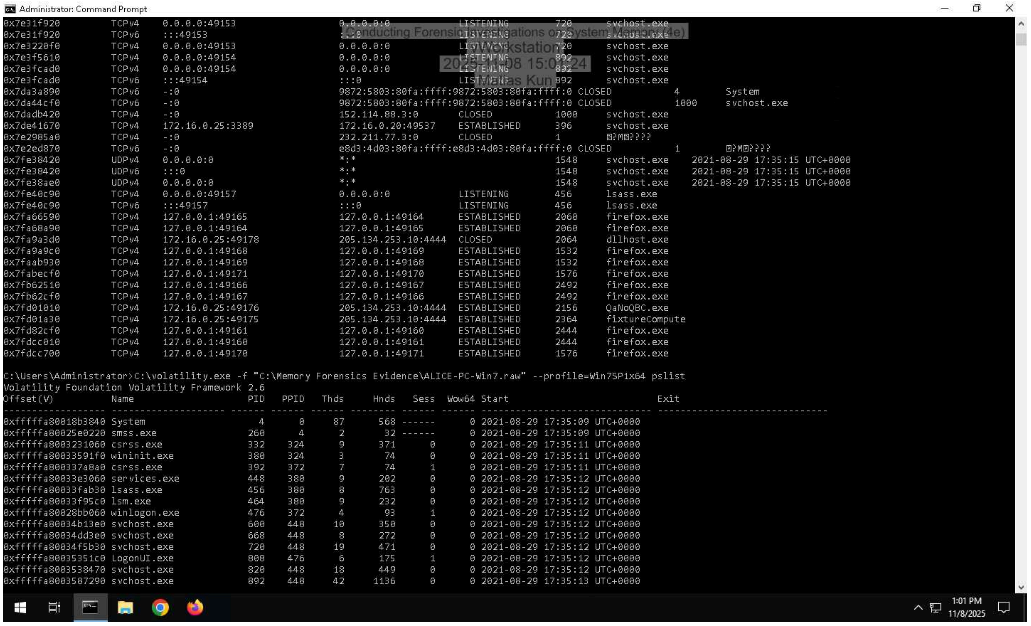
The three processes that connected to 205.134.253.10:4444 are "fixtureCompute," "QaNoQBC.exe," and "dllhost.exe."

Document the name and purpose of the software you discovered.

The software that commonly uses port 4444 is Metasploit by default. It also contains a proxy named 12P HTTP/S. Metasploit is a security software programming tool used to provide data about vulnerabilities and assists in the penetration testing setting.

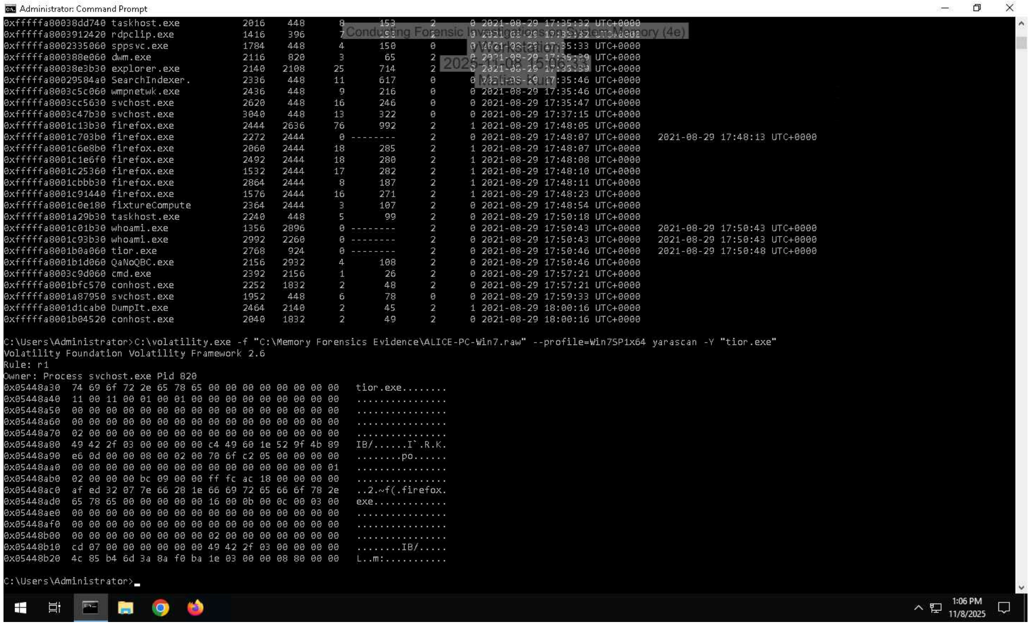
Part 2: Identify Malicious Processes

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


Administrator: Command Prompt
Conducting Forensic Investigations on System Memory (4e)
Workstation
2025-11-08 15:01:24
Matias Kun
1:01 PM
11/8/2025

```
0x7e31f920         TCPv4    0.0.0.0:49153                  0.0.0.0:0            LISTENING        720      svchost.exe
0x7e31f920         TCPv6    :::49153                       :::0                 LISTENING        720      svchost.exe
0x7e3220f0         TCPv4    0.0.0.0:49153                  0.0.0.0:0            LISTENING        720      svchost.exe
0x7e3f5610         TCPv4    0.0.0.0:49154                  0.0.0.0:0            LISTENING        892      svchost.exe
0x7e3fcad0         TCPv4    0.0.0.0:49154                  0.0.0.0:0            LISTENING        892      svchost.exe
0x7e3fcad0         TCPv6    :::49154                       :::0                 LISTENING        892      svchost.exe
0x7da3a890         TCPv6    -:0                            9872:5803:80fa:ffff:9872:5803:80fa:ffff:0 CLOSED           4        System
0x7da44cf0         TCPv6    -:0                            9872:5803:80fa:ffff:9872:5803:80fa:ffff:0 CLOSED           1000     svchost.exe
0x7dadb420         TCPv4    -:0                            152.114.88.3:0       CLOSED           1000     svchost.exe
0x7de41670         TCPv4    172.16.0.25:3389               172.16.0.20:49537    ESTABLISHED      396      svchost.exe
0x7e2985a0         TCPv4    -:0                            232.211.77.3:0       CLOSED           1        ⊡?M⊡????
0x7e2ed870         TCPv6    -:0                            e8d3:4d03:80fa:ffff:e8d3:4d03:80fa:ffff:0 CLOSED           1        ⊡?M⊡????
0x7fe38420         UDPv4    0.0.0.0:0                      *:*                                   1548     svchost.exe    2021-08-29 17:35:15 UTC+0000
0x7fe38420         UDPv6    :::0                           *:*                                   1548     svchost.exe    2021-08-29 17:35:15 UTC+0000
0x7fe38ae0         UDPv4    0.0.0.0:0                      *:*                                   1548     svchost.exe    2021-08-29 17:35:15 UTC+0000
0x7fe40c90         TCPv4    0.0.0.0:49157                  0.0.0.0:0            LISTENING        456      lsass.exe
0x7fe40c90         TCPv6    :::49157                       :::0                 LISTENING        456      lsass.exe
0x7fa66590         TCPv4    127.0.0.1:49165                127.0.0.1:49164      ESTABLISHED      2060     firefox.exe
0x7fa68a90         TCPv4    127.0.0.1:49164                127.0.0.1:49165      ESTABLISHED      2060     firefox.exe
0x7fa9a3d0         TCPv4    172.16.0.25:49178              205.134.253.10:4444  CLOSED           2064     dllhost.exe
0x7fa9a9c0         TCPv4    127.0.0.1:49168                127.0.0.1:49169      ESTABLISHED      1532     firefox.exe
0x7faab930         TCPv4    127.0.0.1:49169                127.0.0.1:49168      ESTABLISHED      1532     firefox.exe
0x7fabecf0         TCPv4    127.0.0.1:49171                127.0.0.1:49170      ESTABLISHED      1576     firefox.exe
0x7fb62510         TCPv4    127.0.0.1:49166                127.0.0.1:49167      ESTABLISHED      2492     firefox.exe
0x7fb62cf0         TCPv4    127.0.0.1:49167                127.0.0.1:49166      ESTABLISHED      2492     firefox.exe
0x7fd01010         TCPv4    172.16.0.25:49176              205.134.253.10:4444  ESTABLISHED      2156     QaNoQBC.exe
0x7fd01a30         TCPv4    172.16.0.25:49175              205.134.253.10:4444  ESTABLISHED      2364     fixtureCompute
0x7fd82cf0         TCPv4    127.0.0.1:49161                127.0.0.1:49160      ESTABLISHED      2444     firefox.exe
0x7fdcc010         TCPv4    127.0.0.1:49160                127.0.0.1:49161      ESTABLISHED      2444     firefox.exe
0x7fdcc700         TCPv4    127.0.0.1:49170                127.0.0.1:49171      ESTABLISHED      1576     firefox.exe

C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\ALICE-PC-Win7.raw" --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xfffffa80018b3840 System                    4      0     87      568 ------      0 2021-08-29 17:35:09 UTC+0000
0xfffffa80025e0220 smss.exe                260      4      2       32 ------      0 2021-08-29 17:35:09 UTC+0000
0xfffffa8003231060 csrss.exe               332    324      9      371      0      0 2021-08-29 17:35:11 UTC+0000
0xfffffa80033591f0 wininit.exe             380    324      3       74      0      0 2021-08-29 17:35:11 UTC+0000
0xfffffa800337a8a0 csrss.exe               392    372      7       74      1      0 2021-08-29 17:35:11 UTC+0000
0xfffffa80033e3060 services.exe            448    380      9      202      0      0 2021-08-29 17:35:12 UTC+0000
0xfffffa80033fab30 lsass.exe               456    380      8      763      0      0 2021-08-29 17:35:12 UTC+0000
0xfffffa80033f95c0 lsm.exe                 464    380      9      232      0      0 2021-08-29 17:35:12 UTC+0000
0xfffffa80028bb060 winlogon.exe            476    372      4       93      1      0 2021-08-29 17:35:12 UTC+0000
0xfffffa80034b13e0 svchost.exe             600    448     10      350      0      0 2021-08-29 17:35:12 UTC+0000
0xfffffa80034dd3e0 svchost.exe             668    448      8      272      0      0 2021-08-29 17:35:12 UTC+0000
0xfffffa80034f5b30 svchost.exe             720    448     19      471      0      0 2021-08-29 17:35:12 UTC+0000
0xfffffa80035351c0 LogonUI.exe             808    476      6      175      1      0 2021-08-29 17:35:12 UTC+0000
0xfffffa8003538470 svchost.exe             820    448     18      449      0      0 2021-08-29 17:35:12 UTC+0000
0xfffffa8003587290 svchost.exe             892    448     42     1136      0      0 2021-08-29 17:35:13 UTC+0000
```

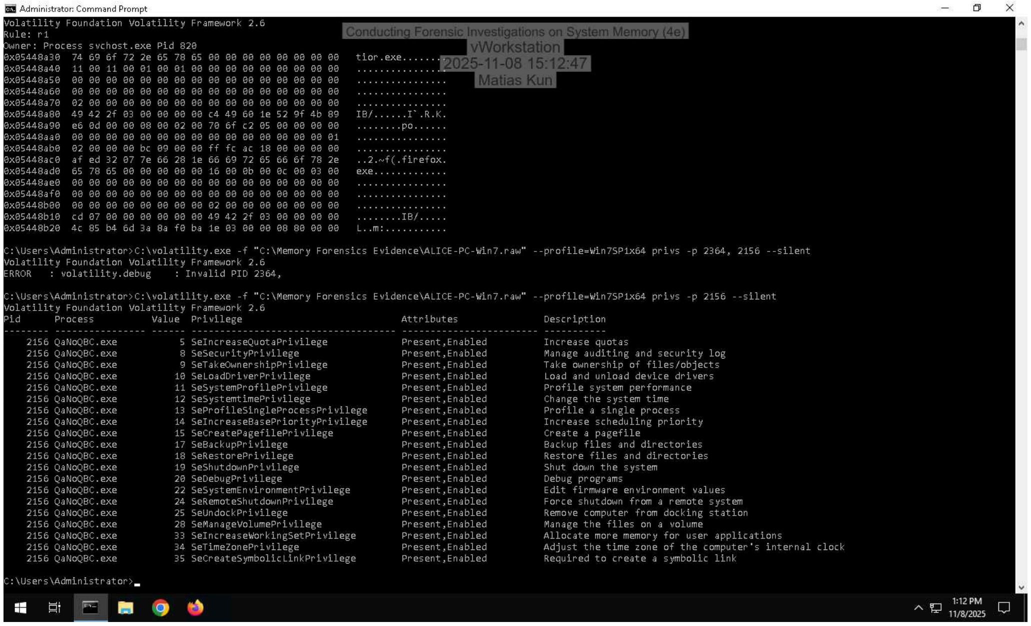
Make a screen capture showing the **output of the yarascan**.



```
0xfffffa80038dd740 taskhost.exe           2016    448      8      153      2      0 2021-08-29 17:35:32 UTC+0000
0xfffffa8003912420 rdpclip.exe            1416    396      7 [illegible]   2      0 2021-08-29 17:35:32 UTC+0000
0xfffffa8002335060 sppsvc.exe             1784    448      4      150      0      0 2021-08-29 17:35:33 UTC+0000
0xfffffa800388e060 dwm.exe                2116    820      3       65      2      0 2021-08-29 17:35:39 UTC+0000
0xfffffa80038e3b30 explorer.exe           2140   2108     25      714      2      0 2021-08-29 17:35:39 UTC+0000
0xfffffa80029584a0 SearchIndexer.         2336    448     11      617      0      0 2021-08-29 17:35:46 UTC+0000
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>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:...........

C:\Users\Administrator>_
```

Part 3: Identify Privilege Escalation

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



```
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:...........

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 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>_
```