Conducting Forensic Investigations on System Memory (4e)

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

Student:	Email:
noble antwi	nantwi@hawk.iit.edu

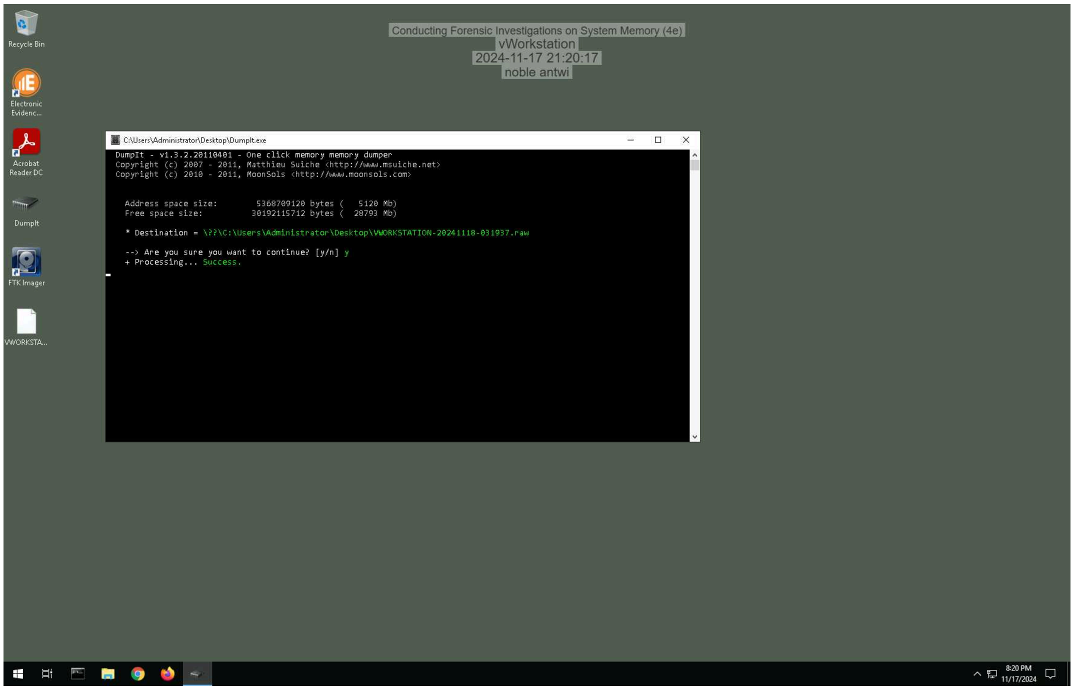
Time on Task:	Progress:
3 hours, 4 minutes	100%

Report Generated: Monday, November 18, 2024 at 1:03 AM

Section 1: Hands-On Demonstration

Part 1: Capture Memory using DumpIt

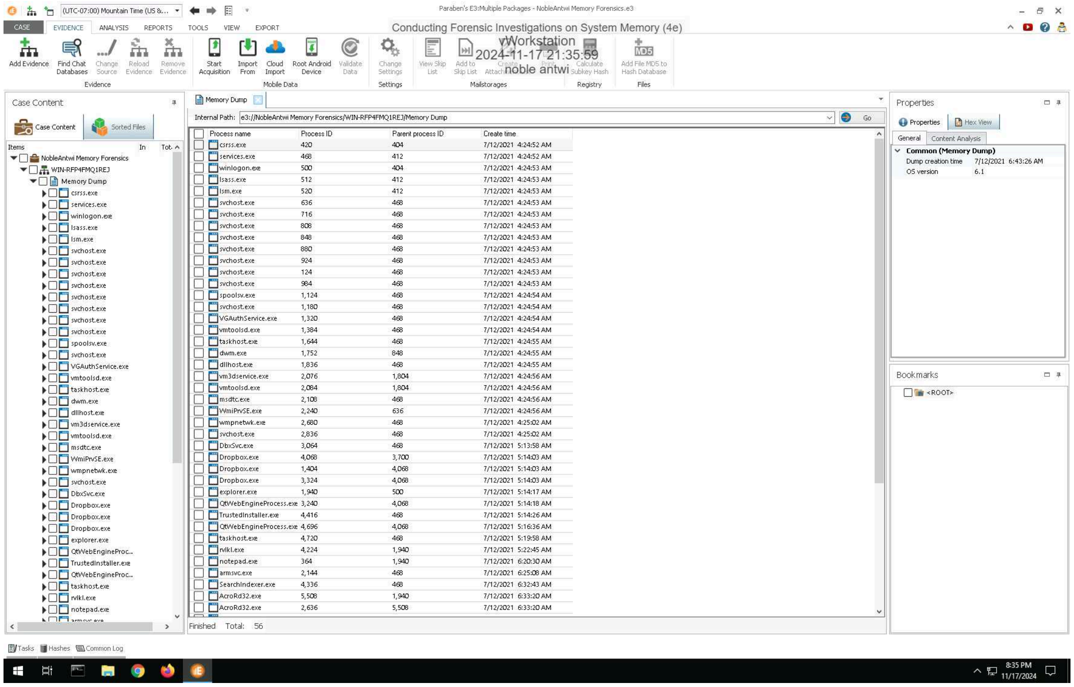
3. **Make a screen capture** showing the **DumpIt success notification**.



```
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:          30192115712 bytes (  28793 Mb)

  * Destination = \??\C:\Users\Administrator\Desktop\VWORKSTATION-20241118-031937.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**.


Paraben's E3:Multiple Packages - NobleAntwi Memory Forensics.e3
Conducting Forensic Investigations on System Memory (4e)
vWorkstation
2024-11-17 21:35:59
noble antwi
Memory Dump
8:35 PM
11/17/2024

Internal Path: e3://NobleAntwi Memory Forensics/WIN-RFP4FMQ1REJ/Memory Dump

Process name	Process ID	Parent process ID	Create time
csrss.exe	420	404	7/12/2021 4:24:52 AM
services.exe	468	412	7/12/2021 4:24:52 AM
winlogon.exe	500	404	7/12/2021 4:24:53 AM
lsass.exe	512	412	7/12/2021 4:24:53 AM
lsm.exe	520	412	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
wmpnetwk.exe	2,680	468	7/12/2021 4:25:02 AM
svchost.exe	2,836	468	7/12/2021 4:25:02 AM
DbxSvc.exe	3,064	468	7/12/2021 5:13:58 AM
Dropbox.exe	4,068	3,700	7/12/2021 5:14:03 AM
Dropbox.exe	1,404	4,068	7/12/2021 5:14:03 AM
Dropbox.exe	3,324	4,068	7/12/2021 5:14:03 AM
explorer.exe	1,940	500	7/12/2021 5:14:17 AM
QtWebEngineProcess.exe	3,240	4,068	7/12/2021 5:14:18 AM
TrustedInstaller.exe	4,416	468	7/12/2021 5:14:26 AM
QtWebEngineProcess.exe	4,696	4,068	7/12/2021 5:16:36 AM
taskhost.exe	4,720	468	7/12/2021 5:19:58 AM
rvlkl.exe	4,224	1,940	7/12/2021 5:22:45 AM
notepad.exe	364	1,940	7/12/2021 6:20:30 AM
armsvc.exe	2,144	468	7/12/2021 6:25:08 AM
SearchIndexer.exe	4,336	468	7/12/2021 6:32:43 AM
AcroRd32.exe	5,508	1,940	7/12/2021 6:33:20 AM
AcroRd32.exe	2,636	5,508	7/12/2021 6:33:20 AM

Finished Total: 56

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 is System and its start time is 4:24:49 AM The Newest Process is the conhost.exe which was started at 6:42:43 AM

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

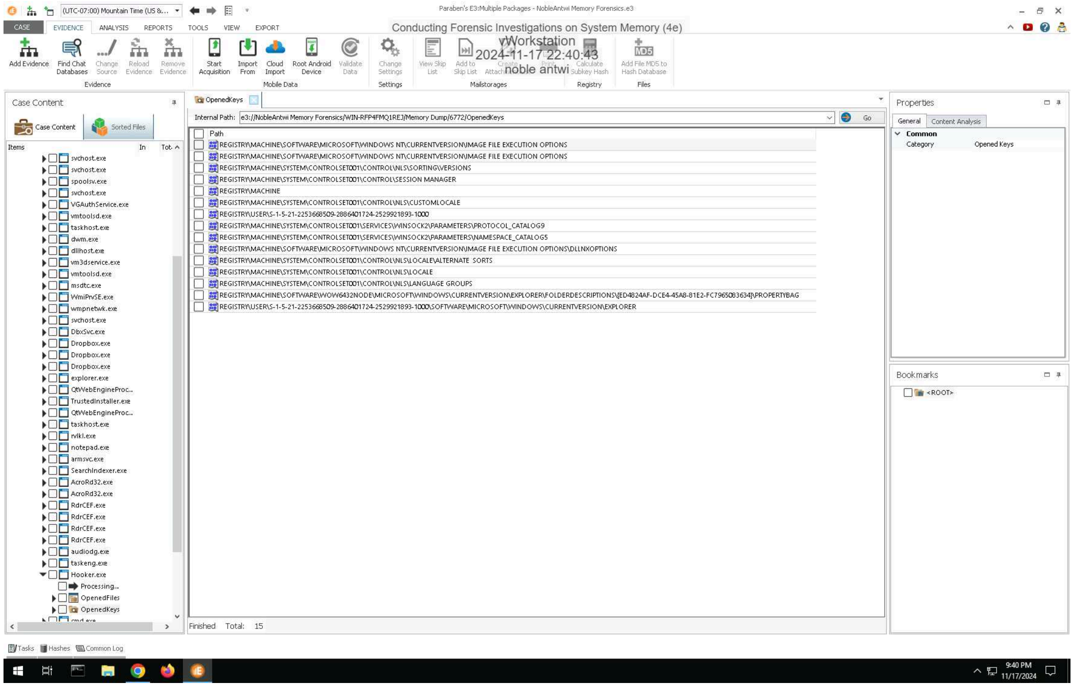
Conhost.exe, short for Console Host Window Process, also referred to as the Console Application Host, is a legitimate software component of Microsoft Windows and Microsoft Server operating systems, developed by Microsoft Corporation. It plays a crucial role in managing console windows for command-line applications such as the Command Prompt (cmd.exe) or PowerShell. Introduced to enhance the user experience, conhost.exe provides improved text rendering, drag-and-drop functionality for files into command-line interfaces, and better integration between the graphical user interface and command-line tools.

As a trusted component, conhost.exe resides in the C:\Windows\System32 directory and ensures the stability and security of console applications by isolating their processes from the main Windows shell. While conhost.exe is typically safe, it can be exploited by malicious actors who may create harmful software disguised with the same name. To verify its legitimacy, users can check the file's location and monitor its behavior using system tools or antivirus software, especially if unusual activity, such as excessive resource usage, is observed.

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

Hooker.exe is an executable file associated with software called Hooker, developed by Ayuda Soft. It is not an essential component of the Windows operating system and is generally regarded as unsafe. Depending on its location and behavior, it poses varying security risks.
Typically found in a subfolder of **C:**, hooker.exe is known for its ability to record keyboard and mouse inputs, monitor applications, and connect to the internet. In these cases, it has been assigned a security rating of 100% dangerous due to its potential use for malicious purposes. If located in C:\Program Files, the security risk is lower, rated at 54% dangerous, and the file may feature a visible program window. If found in a subfolder of the user's profile folder, the risk increases to 78% dangerous, and similar keylogging capabilities are present.
Hooker.exe is not a core Windows file and does not have a clear description or legitimate use associated with the operating system. It is often loaded during the Windows boot process, which further raises concerns about its behavior. Moreover, malware such as Generic PUP.z (detected by McAfee) or not-a-virus.Win32.Hooker.n (detected by Kaspersky) may disguise itself using the name hooker.exe.
Given these risks, it is essential to verify the legitimacy of hooker.exe on your system. Using tools like Security Task Manager is recommended to determine if it is a threat and to take appropriate action if necessary.

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



Paraben's E3:Multiple Packages - NobleAntwi Memory Forensics.e3

Conducting Forensic Investigations on System Memory (4e)
vWorkstation
2024-11-17 22:40:43
noble antwi

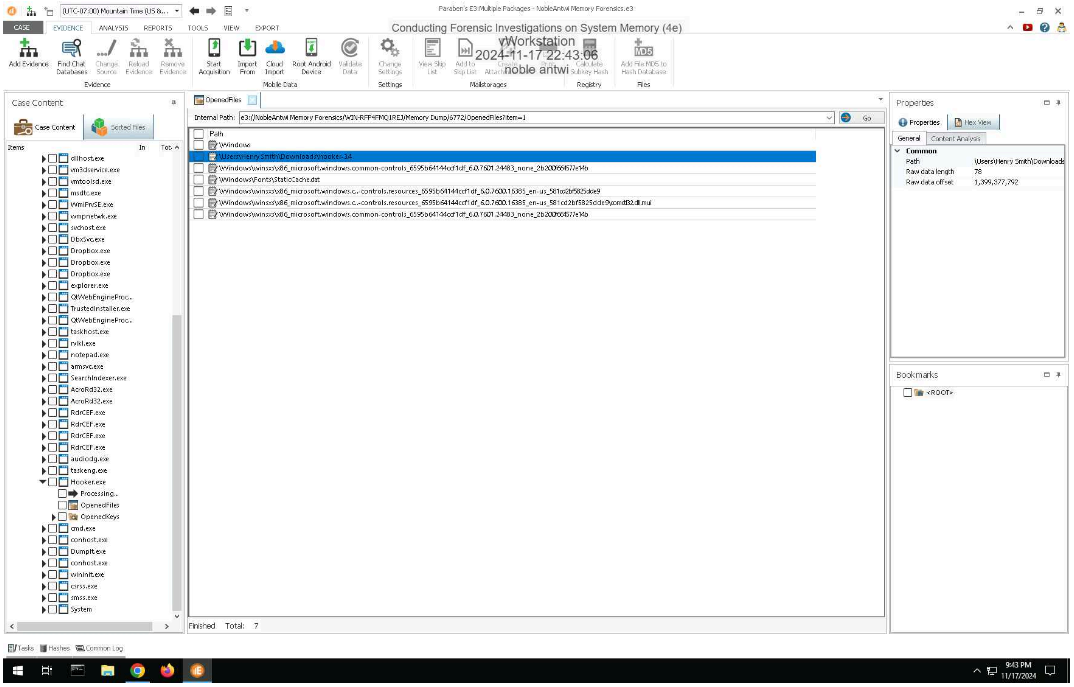
Internal Path: e3://NobleAntwi Memory Forensics/WIN-RFP4FMQ1REJ/Memory Dump/6772/OpenedKeys

```
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-DCE4-45A8-81E2-FC7965083634}\PROPERTYBAG
REGISTRY\USER\S-1-5-21-2253668509-2886401724-2529921893-1000\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER
```

Finished Total: 15

Properties — Common: Category: Opened Keys

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



Internal Path: e3://NobleAntwi Memory Forensics/WIN-RFP4FMQ1REJ/Memory Dump/6772/OpenedFiles?item=1

```
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

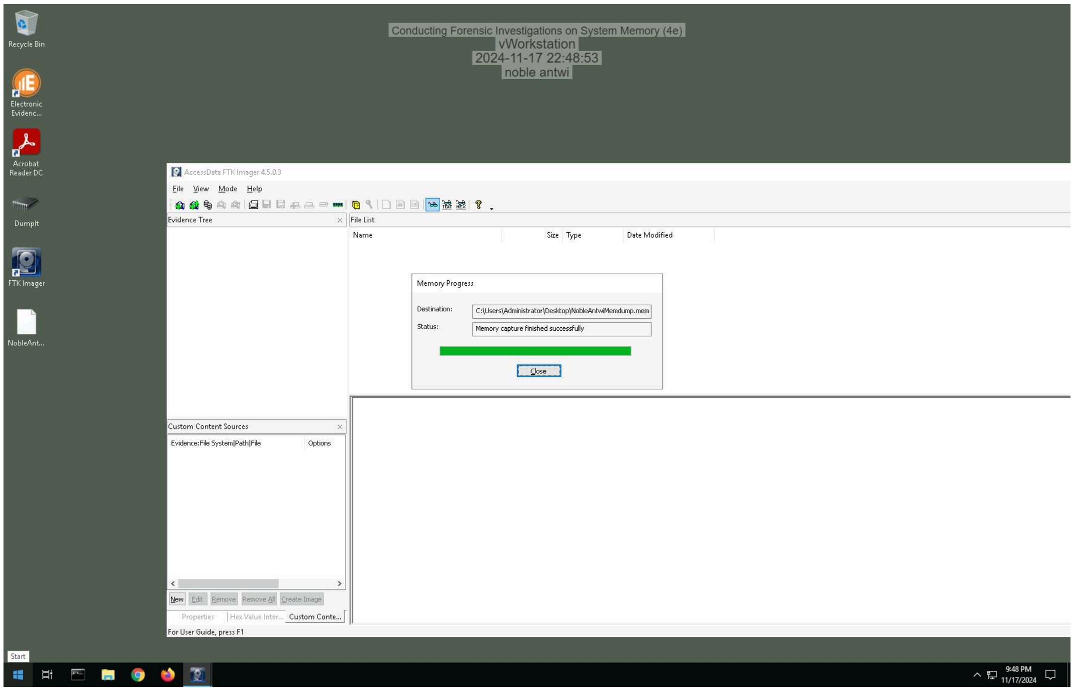
Common

Path	\Users\Henry Smith\Downloads
Raw data length	78
Raw data offset	1,399,377,792

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
2024-11-17 22:48:53
noble antwi

AccessData FTK Imager 4.5.0.3

Memory Progress

Destination: C:\Users\Administrator\Desktop\NobleAntwiMemdump.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?

Rvlkl.exe is the executable file for Revealer Keylogger, a software developed by Logixoft. This keylogger is designed to monitor and log user activity, making it popular for parental monitoring and security purposes. It is available in a free Basic version and a paid Complete version, which offers additional features such as multi-PC licensing, remote log delivery, and screenshots of activity.
The default location of the file is C:\Windows\System32\rvlkl.exe, and in its Complete version, the process can be hidden both on disk and in Task Manager for discreet operation. Uninstallation can be done through the program’s "Help" interface or by re-running its setup program. A version of the rvlkl.exe process is also used in Geometrix architectural training AI software, which can be updated or removed via the Control Panel.
Although Revealer Keylogger is legitimate software and widely used in Europe, especially in France, it can raise security concerns due to its ability to record user activity and potentially sensitive data. As with any executable file, rvlkl.exe could be exploited by malicious actors, so it is important to confirm its legitimacy. If unauthorized, the file should be removed using antivirus or monitoring tools.

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

the pslist column has not no process flagged as hidden. All values of pslist is true.

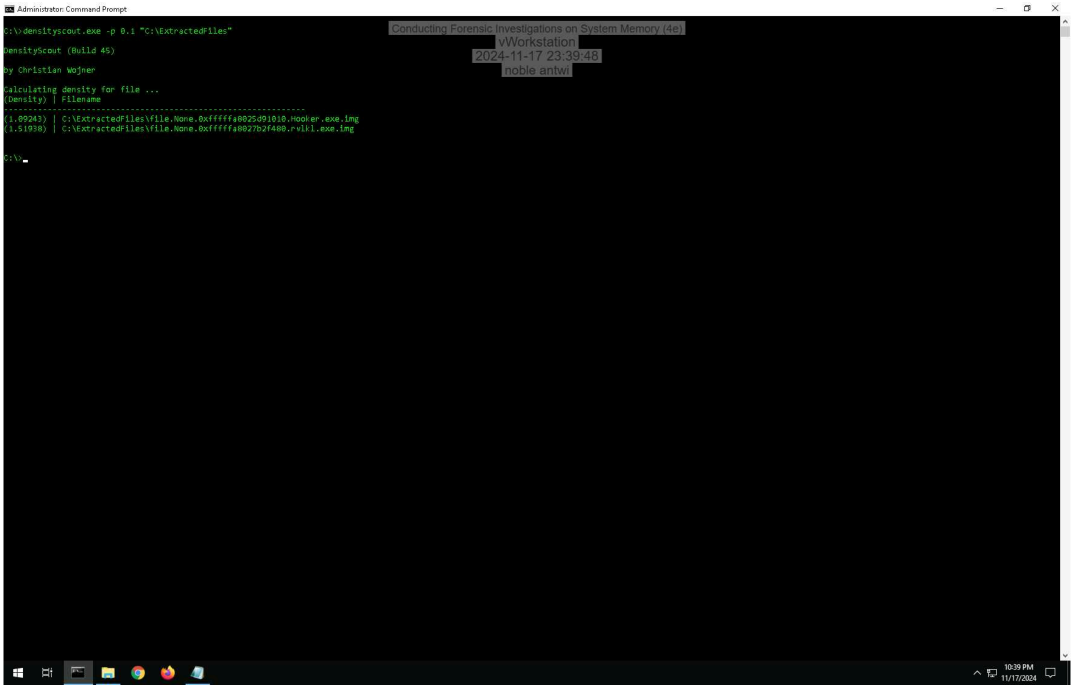
12. **Document** whether the netscan module displays network usage associated with the Hooker.exe or rvlkl.exe processes.

There was no network usage or connection associated with either Hooker.exe or rvlkl.exe

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

Port 56610 is commonly used as a temporary or local "ephemeral" port in network communications. It acts as a scratch port for client-side applications, such as web browsers, email clients, or news readers, to establish connections with remote servers' service ports. Both TCP and UDP protocols utilize this port, with TCP providing reliable, connection-oriented communication and UDP offering faster, connectionless data transfer. These ephemeral ports are dynamically assigned by the operating system when an application initiates communication with a remote server.
While Port 56610 is not associated with any specific service or application, its dynamic use is part of the standard network operation to manage client-server connections. Proper firewall and security configurations are crucial, as open ephemeral ports can sometimes be exploited by attackers

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


Administrator: Command Prompt
Conducting Forensic Investigations on System Memory (4e)
vWorkstation
2024-11-17 23:39:48
noble antwi
10:39 PM
11/17/2024

```
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:\>
```

Section 3: Challenge and Analysis

Part 1: Identify Malicious Connections

Document the three processes that connected to 205.134.253.10:4444.

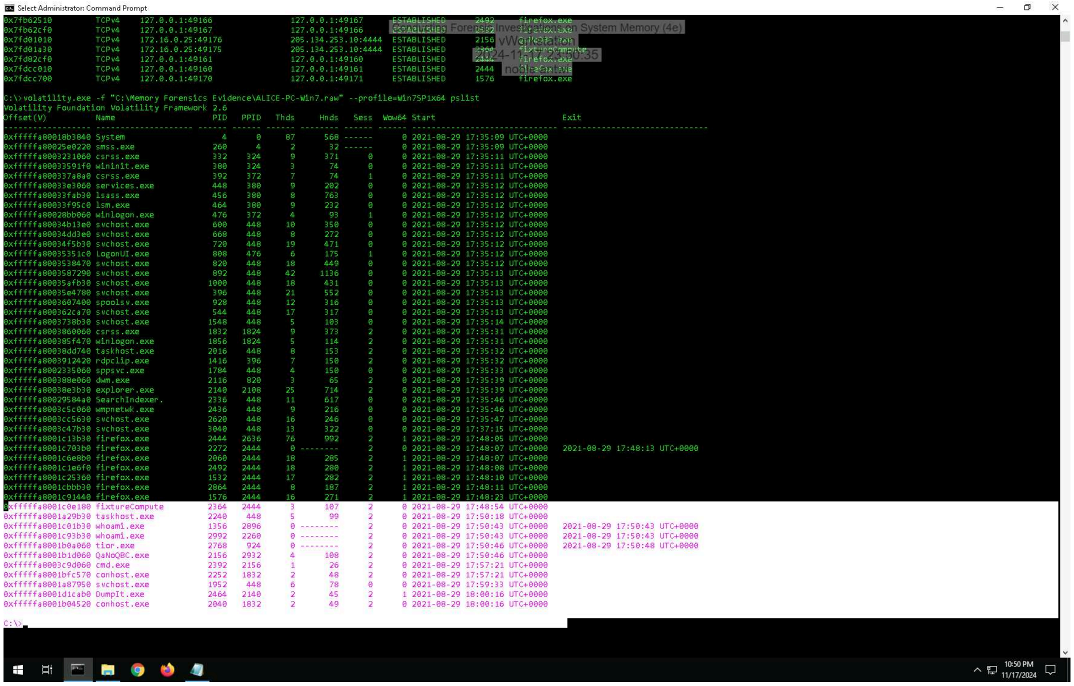
The three processes are QaNoQBC.exe, fistureCompute and dllhost.exe

Document the name and purpose of the software you discovered.

Several types of software and tools use port 4444 as their default listener port: 1. Metasploit Framework: This is one of the most well-known tools that uses port 4444 by default. Metasploit is a penetration testing framework that allows security professionals to test the security of systems by simulating attacks. The default port for reverse shells and payload handlers in Metasploit is often set to 4444.
2. Netcat: Often referred to as the "Swiss Army knife" of networking, Netcat can be used to open TCP or UDP connections, including listening on port 4444. It's commonly used for debugging and network exploration.
3. Malware and Backdoors: Unfortunately, port 4444 is also commonly used by various types of malware, including rootkits, backdoors, and Trojan horses. These malicious programs use the port to listen for incoming connections, exfiltrate data, or receive commands from an attacker.

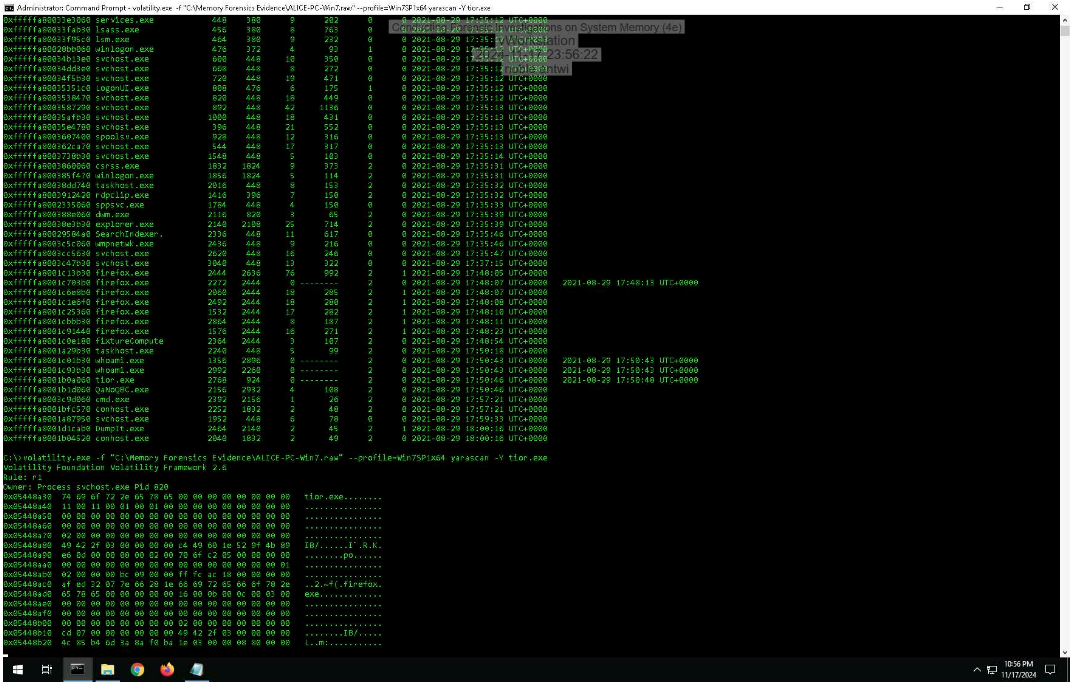
Part 2: Identify Malicious Processes

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



```
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:\>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
0xfffffa80035afb30 svchost.exe            1000    448     18      431      0      0 2021-08-29 17:35:13 UTC+0000
0xfffffa80035e4780 svchost.exe             396    448     21      552      0      0 2021-08-29 17:35:13 UTC+0000
0xfffffa8003607400 spoolsv.exe             928    448     12      316      0      0 2021-08-29 17:35:13 UTC+0000
0xfffffa800362ca70 svchost.exe             544    448     17      317      0      0 2021-08-29 17:35:13 UTC+0000
0xfffffa8003738b30 svchost.exe            1548    448      5      103      0      0 2021-08-29 17:35:14 UTC+0000
0xfffffa8003860060 csrss.exe              1832   1824      9      373      2      0 2021-08-29 17:35:31 UTC+0000
0xfffffa800385f470 winlogon.exe           1856   1824      5      114      2      0 2021-08-29 17:35:31 UTC+0000
0xfffffa80038dd740 taskhost.exe           2016    448      8      153      2      0 2021-08-29 17:35:32 UTC+0000
0xfffffa8003912420 rdpclip.exe            1416    396      7      150      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:\>
```

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

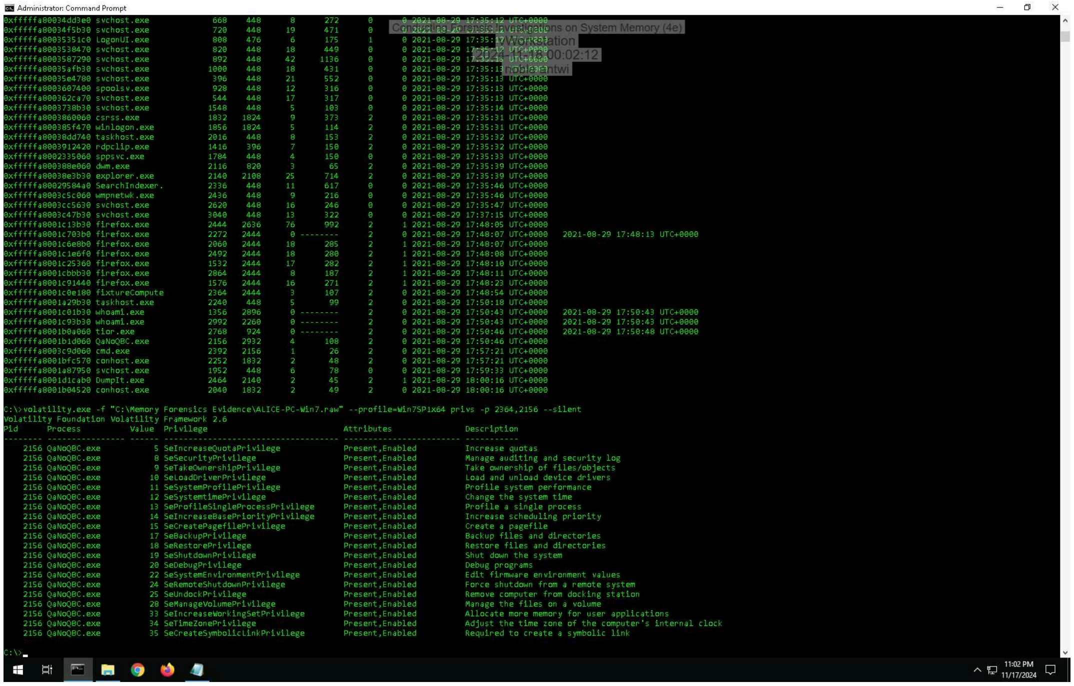


Administrator: Command Prompt - volatility.exe -f "C:\Memory Forensics Evidence\ALICE-PC-Win7.raw" --profile=Win7SP1x64 yarascan -Y tior.exe
10:56 PM
11/17/2024

```
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
0xfffffa80035afb30 svchost.exe            1000    448     18      431      0      0 2021-08-29 17:35:13 UTC+0000
0xfffffa80035e4780 svchost.exe             396    448     21      552      0      0 2021-08-29 17:35:13 UTC+0000
0xfffffa8003607400 spoolsv.exe             928    448     12      316      0      0 2021-08-29 17:35:13 UTC+0000
0xfffffa800362ca70 svchost.exe             544    448     17      317      0      0 2021-08-29 17:35:13 UTC+0000
0xfffffa8003738b30 svchost.exe            1548    448      5      103      0      0 2021-08-29 17:35:14 UTC+0000
0xfffffa8003860060 csrss.exe              1832   1824      9      373      2      0 2021-08-29 17:35:31 UTC+0000
0xfffffa800385f470 winlogon.exe           1856   1824      5      114      2      0 2021-08-29 17:35:31 UTC+0000
0xfffffa80038dd740 taskhost.exe           2016    448      8      153      2      0 2021-08-29 17:35:32 UTC+0000
0xfffffa8003912420 rdpclip.exe            1416    396      7      150      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:\>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**.


Administrator: Command Prompt
Conducting Forensic Investigations on System Memory (4e)
Workstation
2024-11-18 00:02:12
noblecntwi
11:02 PM
11/17/2024

```
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
0xfffffa80035afb30 svchost.exe           1000    448     18      431      0      0 2021-08-29 17:35:13 UTC+0000
0xfffffa80035e4780 svchost.exe            396    448     21      552      0      0 2021-08-29 17:35:13 UTC+0000
0xfffffa8003607400 spoolsv.exe            928    448     12      316      0      0 2021-08-29 17:35:13 UTC+0000
0xfffffa800362ca70 svchost.exe            544    448     17      317      0      0 2021-08-29 17:35:13 UTC+0000
0xfffffa8003738b30 svchost.exe           1548    448      5      103      0      0 2021-08-29 17:35:14 UTC+0000
0xfffffa8003860060 csrss.exe             1832   1824      9      373      2      0 2021-08-29 17:35:31 UTC+0000
0xfffffa800385f470 winlogon.exe          1856   1824      5      114      2      0 2021-08-29 17:35:31 UTC+0000
0xfffffa80038dd740 taskhost.exe          2016    448      8      153      2      0 2021-08-29 17:35:32 UTC+0000
0xfffffa8003912420 rdpclip.exe           1416    396      7      150      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:\>volatility.exe -f "C:\Memory Forensics Evidence\ALICE-PC-Win7.raw" --profile=Win7SP1x64 privs -p 2364,2156 --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:\>_
```