Conducting Forensic Investigations on System Memory (4e)

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

Student: muhammad zahid	Email: zahid1mz@cmich.edu

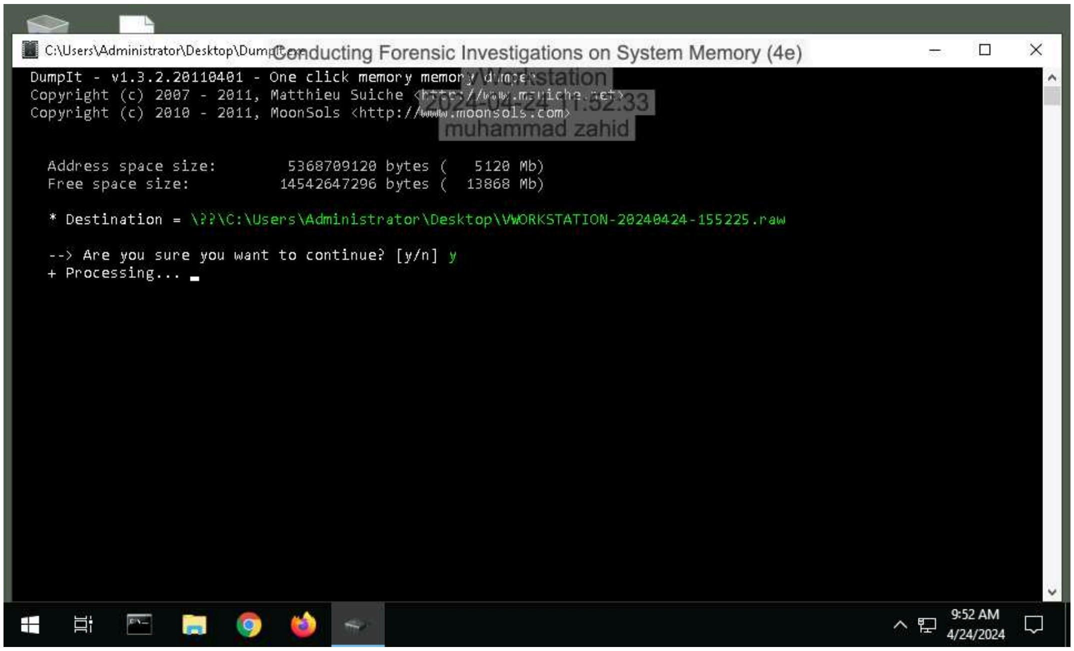
Time on Task: 7 hours, 50 minutes	Progress: 100%

Report Generated: Wednesday, April 24, 2024 at 12:40 PM

Section 1: Hands-On Demonstration

Part 1: Capture Memory using DumpIt

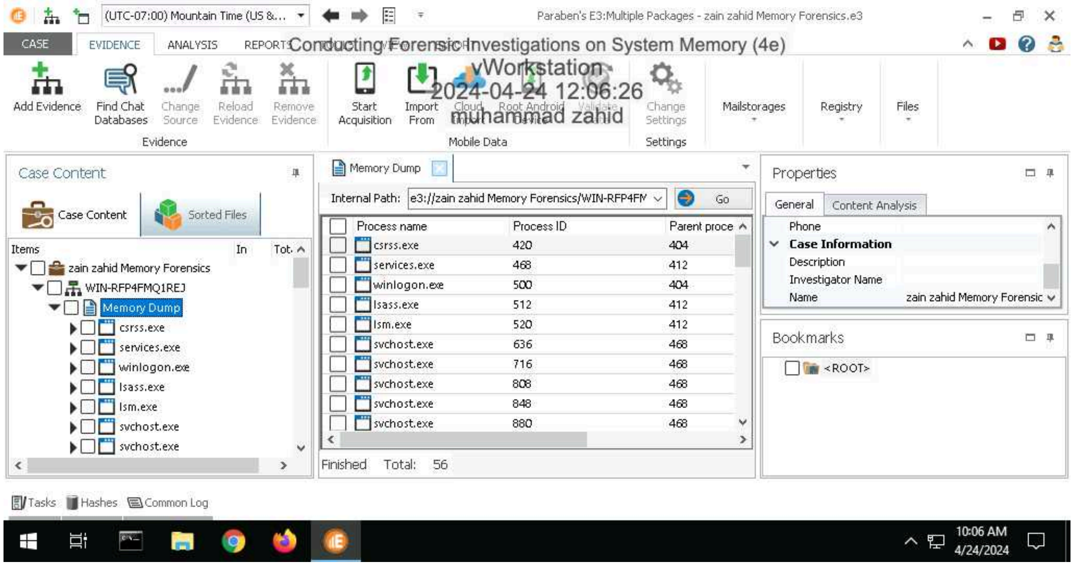
3. **Make a screen capture** showing the **DumpIt success notification**.



```
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:          14542647296 bytes (  13868 Mb)

  * Destination = \??\C:\Users\Administrator\Desktop\VWORKSTATION-20240424-155225.raw

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

Part 2: Analyze Memory using E3

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



Items	In	Tot.
zain zahid Memory Forensics		
WIN-RFP4FMQ1REJ		
Memory Dump		
csrss.exe		
services.exe		
winlogon.exe		
lsass.exe		
lsm.exe		
svchost.exe		
svchost.exe		

Internal Path: e3://zain zahid Memory Forensics/WIN-RFP4FM

Process name	Process ID	Parent proce
csrss.exe	420	404
services.exe	468	412
winlogon.exe	500	404
lsass.exe	512	412
lsm.exe	520	412
svchost.exe	636	468
svchost.exe	716	468
svchost.exe	808	468
svchost.exe	848	468
svchost.exe	880	468

Finished Total: 56

Phone	
Case Information	
Description	
Investigator Name	
Name	zain zahid Memory Forensic

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

7/12/2021 6:42:43 AM

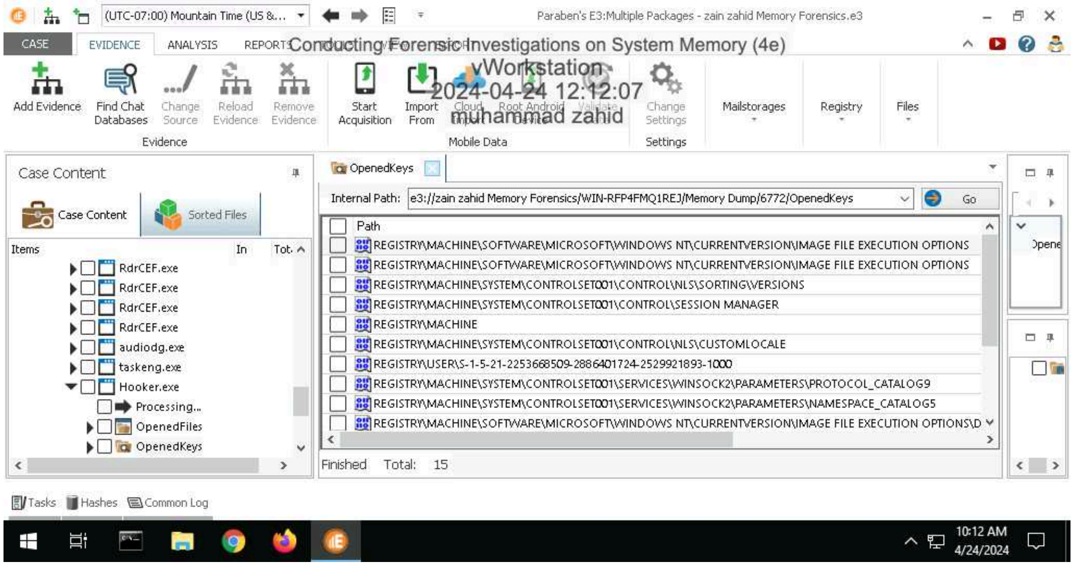
15. **Document** your findings for the conhost.exe process. What is it and what is it used for?

the server application for all of the windows console APIs as well as the classic Windows user Interface for working with command-line applications.

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

able to record keyboard and mouse imprints. Used for malware.

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



OpenedKeys

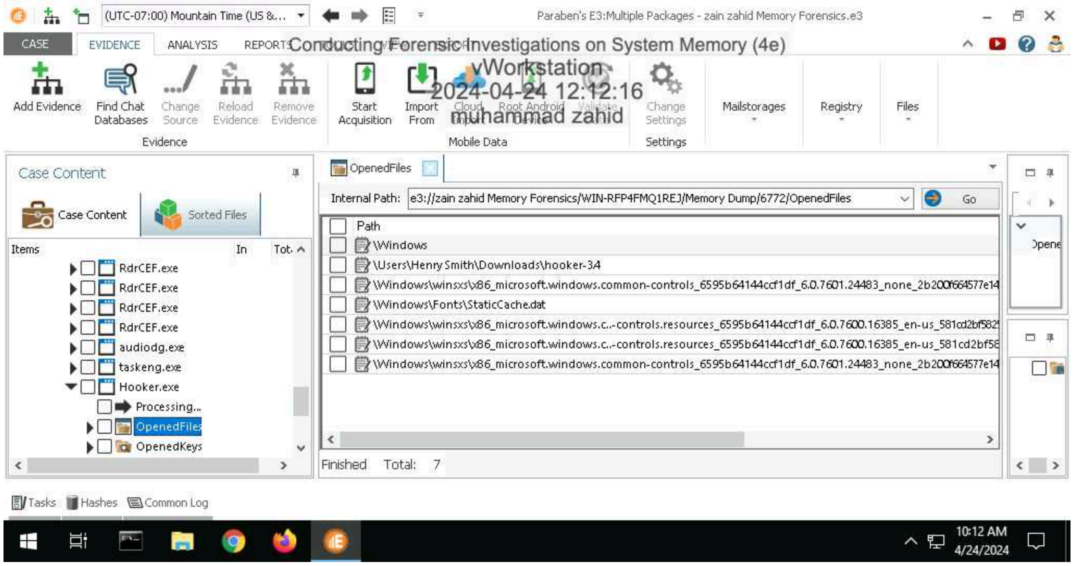
Internal Path: e3://zain zahid Memory Forensics/WIN-RFP4FMQ1REJ/Memory Dump/6772/OpenedKeys

Go

```
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\D
```

Finished Total: 15

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



OpenedFiles

Internal Path: e3://zain zahid Memory Forensics/WIN-RFP4FMQ1REJ/Memory Dump/6772/OpenedFiles

Go

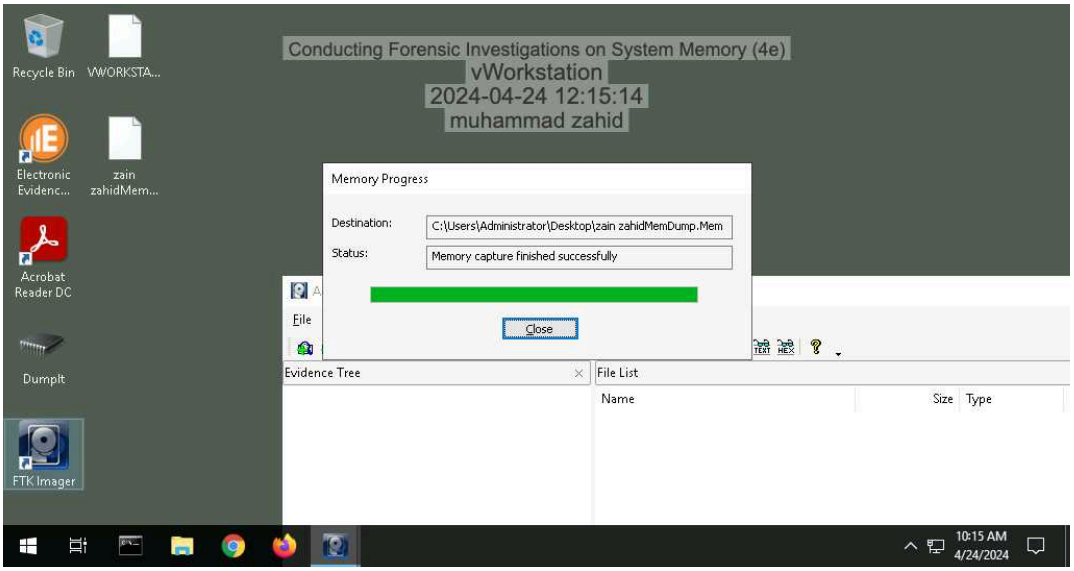
```
Path
\Windows
\Users\Henry Smith\Downloads\hooker-34
\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.24483_none_2b200f664577e14
\Windows\Fonts\StaticCache.dat
\Windows\winsxs\x86_microsoft.windows.c..-controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_581cd2bf582
\Windows\winsxs\x86_microsoft.windows.c..-controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_581cd2bf58
\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.24483_none_2b200f664577e14
```

Finished Total: 7

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
2024-04-24 12:15:14
muhammad zahid

Memory Progress

Destination: C:\Users\Administrator\Desktop\zain zahidMemDump.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?

revealer keylogger free, a program that can record your key strokes and screen shots.

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

no processes are hidden or flagged.

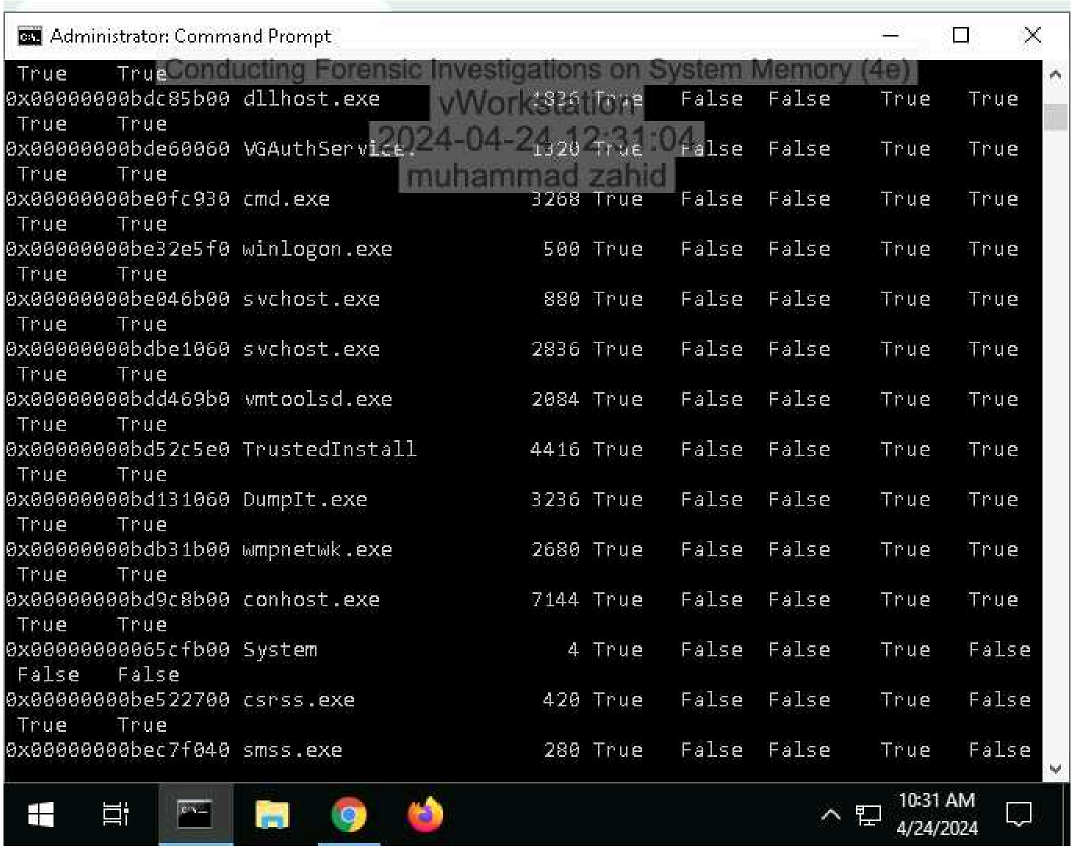
12. **Document** whether the netscan module displays network usage associated with the Hooker.exe or rvlkl.exe processes.

it doesn't.

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

Transmission control protocol.

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



```
 True     True
0x00000000bdc85b00 dllhost.exe           1836 True    False  False    True   True
 True     True
0x00000000bde60060 VGAuthService.        1320 True    False  False    True   True
 True     True
0x00000000be0fc930 cmd.exe               3268 True    False  False    True   True
 True     True
0x00000000be32e5f0 winlogon.exe           500 True    False  False    True   True
 True     True
0x00000000be046b00 svchost.exe            880 True    False  False    True   True
 True     True
0x00000000bdbe1060 svchost.exe           2836 True    False  False    True   True
 True     True
0x00000000bdd469b0 vmtoolsd.exe          2084 True    False  False    True   True
 True     True
0x00000000bd52c5e0 TrustedInstall        4416 True    False  False    True   True
 True     True
0x00000000bd131060 DumpIt.exe            3236 True    False  False    True   True
 True     True
0x00000000bdb31b00 wmpnetwk.exe          2680 True    False  False    True   True
 True     True
0x00000000bd9c8b00 conhost.exe           7144 True    False  False    True   True
 True     True
0x0000000065cfb00 System                   4 True    False  False    True   False
 False    False
0x00000000be522700 csrss.exe              420 True    False  False    True   False
 True     True
0x00000000bec7f040 smss.exe               280 True    False  False    True   False
```

Section 3: Challenge and Analysis

Part 1: Identify Malicious Connections

Document the three processes that connected to 205.134.253.10:4444.

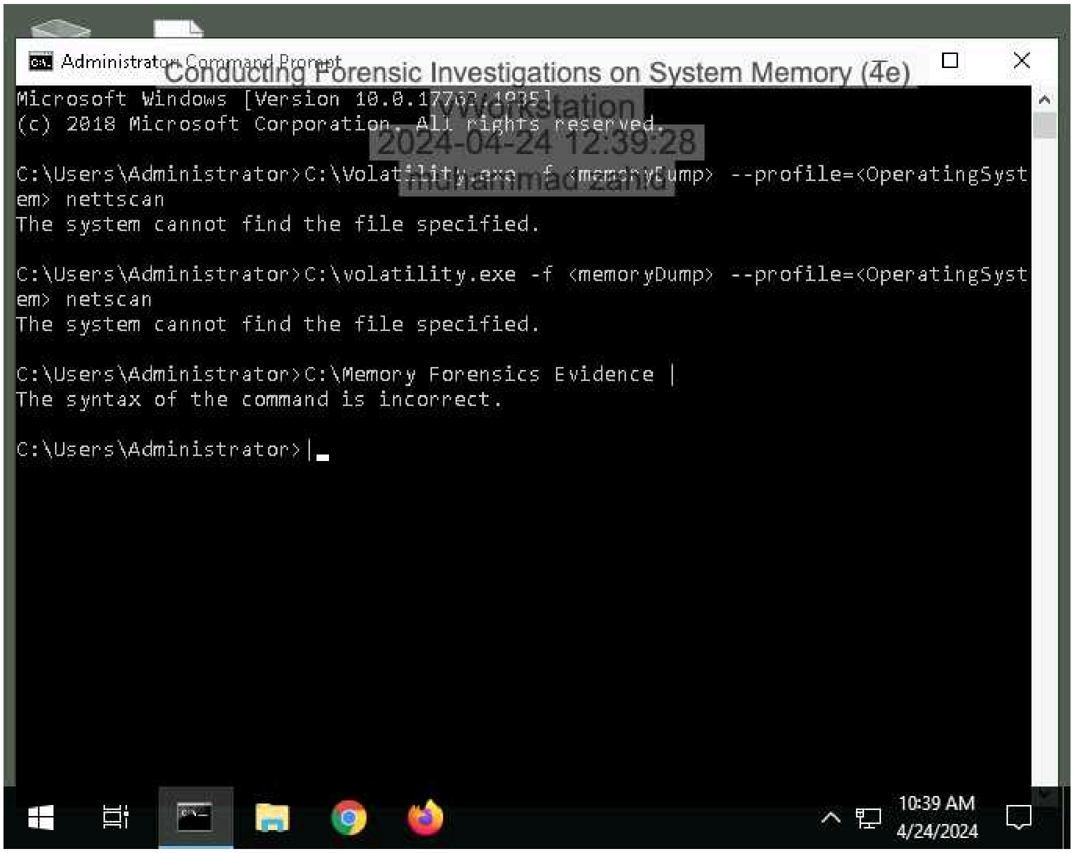
192.2222.2221289.232.231489.232.121

Document the name and purpose of the software you discovered.

To discover data.

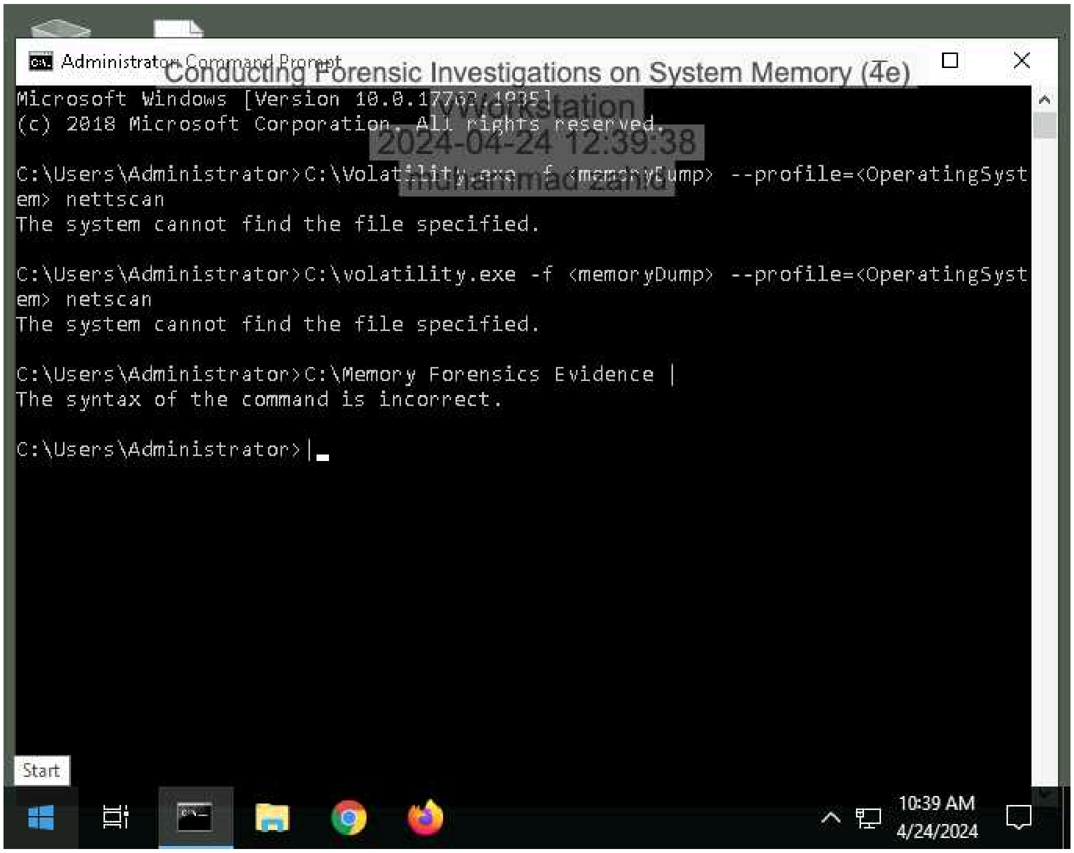
Part 2: Identify Malicious Processes

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)
vWorkstation
2024-04-24 12:39:28
muhammad zahid
10:39 AM
4/24/2024

```
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>C:\Volatility.exe -f <memoryDump> --profile=<OperatingSyst
em> nettscan
The system cannot find the file specified.

C:\Users\Administrator>C:\volatility.exe -f <memoryDump> --profile=<OperatingSyst
em> netscan
The system cannot find the file specified.

C:\Users\Administrator>C:\Memory Forensics Evidence |
The syntax of the command is incorrect.

C:\Users\Administrator>|
```

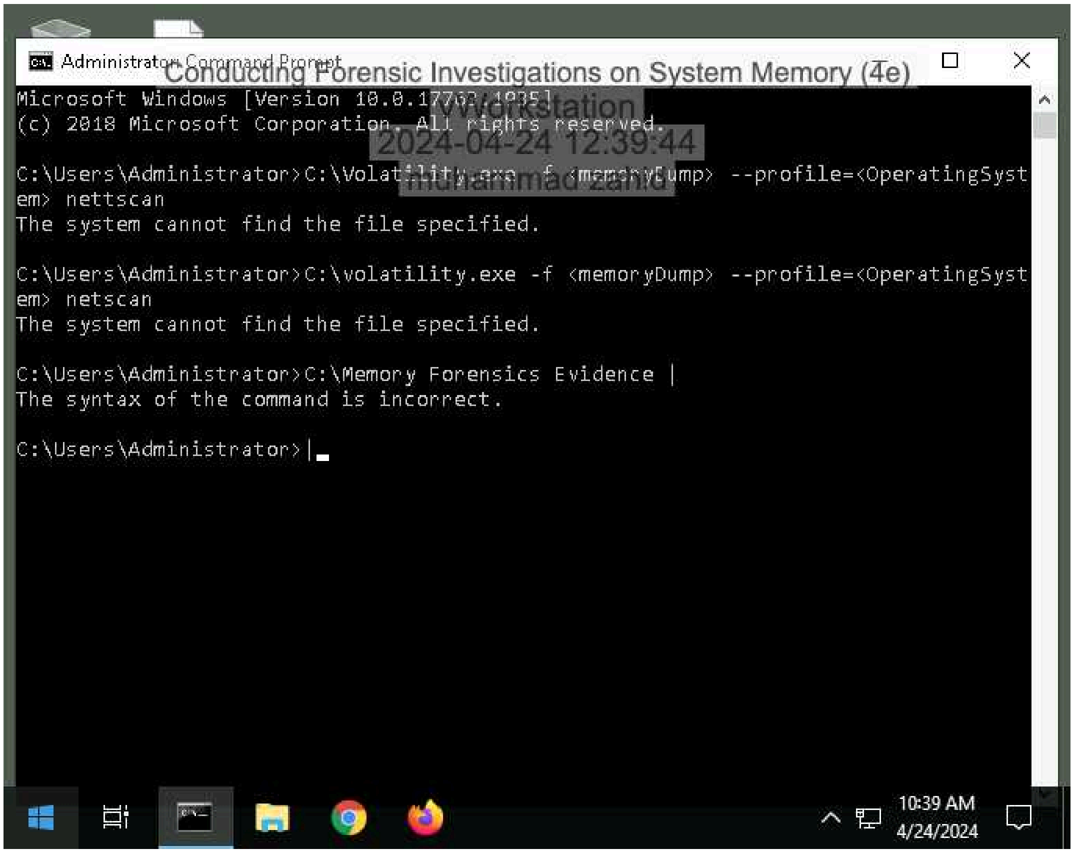
Make a screen capture showing the **output of the yarascan**.



```
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>C:\Volatility.exe -f <memoryDump> --profile=<OperatingSyst
em> nettscan
The system cannot find the file specified.

C:\Users\Administrator>C:\volatility.exe -f <memoryDump> --profile=<OperatingSyst
em> netscan
The system cannot find the file specified.

C:\Users\Administrator>C:\Memory Forensics Evidence |
The syntax of the command is incorrect.

C:\Users\Administrator>|
```

Part 3: Identify Privilege Escalation

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



```
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>C:\Volatility.exe -f <memoryDump> --profile=<OperatingSyst
em> nettscan
The system cannot find the file specified.

C:\Users\Administrator>C:\volatility.exe -f <memoryDump> --profile=<OperatingSyst
em> netscan
The system cannot find the file specified.

C:\Users\Administrator>C:\Memory Forensics Evidence |
The syntax of the command is incorrect.

C:\Users\Administrator>|_
```