

# Report



**Title:** Comparative Memory Forensics: Analyzing Volatile Data Before and After Internet Activity

Riphah International University Islamabad

Name	Sap Id
Saad Naveed	43973
Muhammad Masab Qayyum	46472
Course	Digital Forensics
Course Instructor	Mr. Humayun Raza
Date	5 <sup>th</sup> May 2025

## Contents

Introduction: .....	4
Objective .....	5
Tools Used.....	5
FTK Imager: .....	6
Volatility 3:.....	6
Methodology .....	6
1. Download Windows 11 ISO.....	6
2. Set Up Virtual Machine (VM).....	7
3. Install Tools.....	7
4. Take First Memory Dump (Before Internet) .....	8
5. Use Internet .....	9
6. Take Second Memory Dump (After Internet) .....	9
7. Memory Dump Size .....	9
8. Install Python .....	10
9. Analyze the Memory Dumps .....	10
Phase 1 .....	10
Analysis Phase 1 .....	12
Interpretation Notes.....	14
Interpretation Notes.....	16
Phase 2 .....	17
Analysis Phase 2 .....	18
System Information:.....	19
Interpretation Notes.....	20
Window Services.....	20
Interpretation Notes.....	21
Processes and Threads.....	22
Interpretation Notes.....	23
Interpretation Notes.....	25
Interpretation Notes.....	27
Interpretation Notes.....	31

DLLs and Handles.....	32
Interpretation Notes.....	34
Interpretation Notes.....	37
Registry .....	37
Interpretation Notes.....	40
Interpretation Note .....	43
Interpretation Notes.....	45
Malware Detection .....	45
Interpretation Notes.....	48
Interpretation Notes.....	50
Others Plugins .....	53
Interpretation Notes.....	58
Interpretation Notes.....	62
Interpretation Notes.....	65
Interpretation Notes.....	70
Results and Findings .....	71
Memory Dump 2 (After Internet Activity).....	71
Conclusion.....	73
References .....	74

## Introduction:

Memory forensics is used to see what was happening in a computer's RAM. It helps us find out which programs were running, which websites were visited, and what network connections were active.

In this project, my teacher gave me the task to do memory forensics on **Windows 11**. I downloaded the Windows 11 ISO file and installed it on a **virtual machine (VM)** to do the testing.

I checked the memory in two cases. First, I took a memory dump when the system was clean and not connected to the internet. Then, I connected it to the internet, opened a few websites, and took another memory dump.

I used **FTK Imager** to take the memory dumps and **Volatility 3** to check and analyze them. These tools helped me see what changed in memory before and after using the internet.

This project helped me understand how internet activity changes the data in memory and why memory forensics is useful for finding user activity and digital evidence.

## Objective

The objective of this project was to analyze two memory dumps taken from a Windows 11 system. The first dump was taken when the system was clean and not connected to the internet, while the second dump was taken after connecting to the internet and visiting websites. The goal was to examine both memory dumps and find out what forensic artifacts were present in each dump and how internet usage affected the data stored in memory.

## Tools Used

In this project, I used two main tools to work with memory forensics:

## **FTK Imager:**

FTK Imager is a **GUI-based** (Graphical User Interface) tool. It's easy to use and helps you take memory dumps from the system. The tool lets you create an image of the system's memory (RAM) with just a few clicks. It supports different file formats and is perfect for capturing data from live systems for forensic analysis.

## **Volatility 3:**

Volatility 3 is a **CLI-based** (Command-Line Interface) tool. This one is a bit more advanced, and you have to use commands to run it. It's powerful for analyzing memory dumps and finding important forensic information like running programs, network connections, and other activities. Since it's command-line based, it's better for those who are familiar with using commands in a terminal.

## **Methodology**

### **1. Download Windows 11 ISO**

First, I downloaded the Windows 11 ISO file from the official Microsoft website.

## 2. Set Up Virtual Machine (VM)

Then, I made the ISO bootable using a USB and installed Windows 11 on a virtual machine (VM).

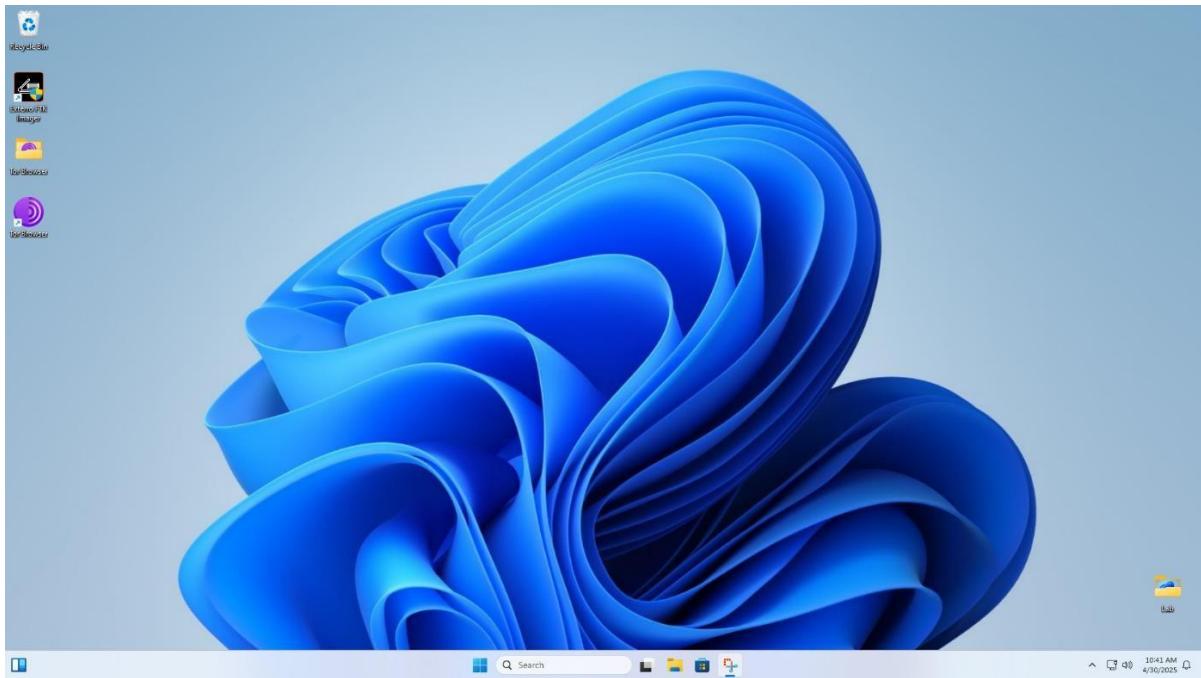


Figure 1 Install Window 11 in VM

## 3. Install Tools

I copied **FTK Imager** and **Volatility 3** from my host system to a USB. Then, I went into the VM and installed both tools there.

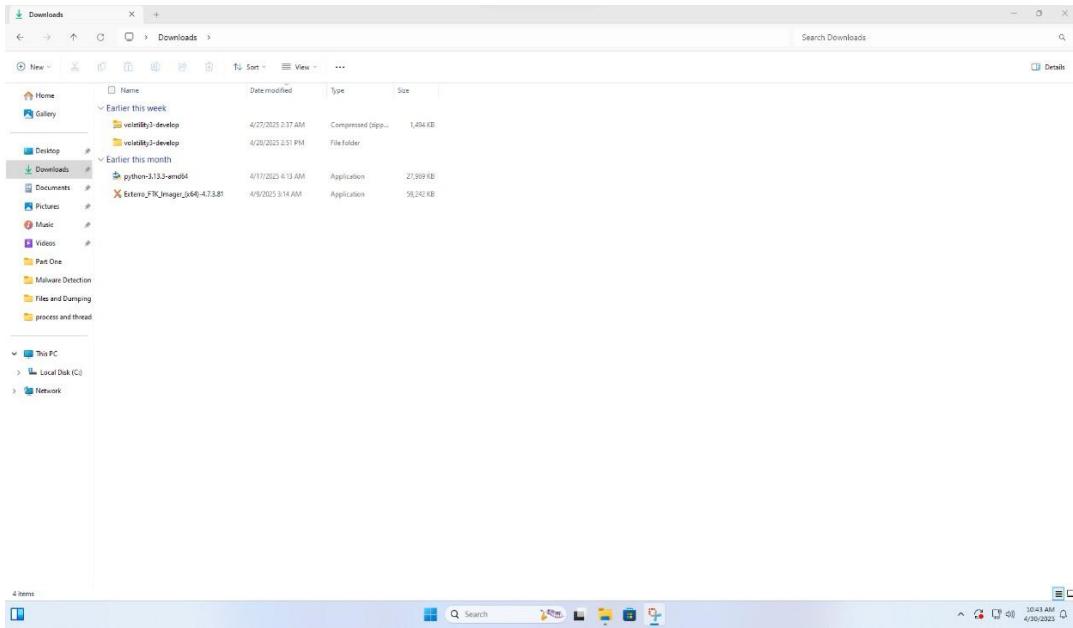


Figure 2 Installs Tools

#### 4. Take First Memory Dump (Before Internet)

I opened FTK Imager and took the first memory dump when the system was not connected to the internet.

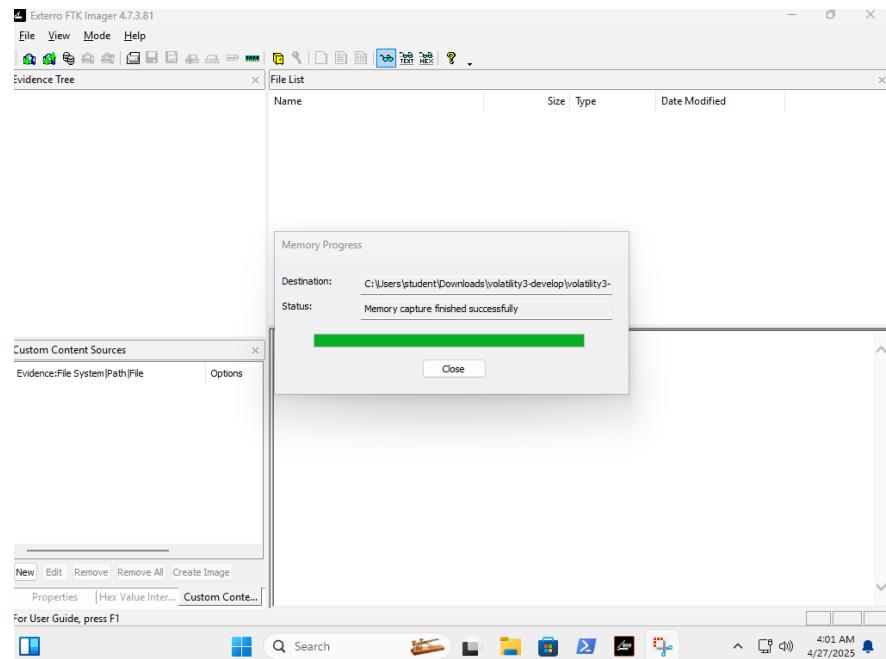


Figure 3 Clean Memory Dump

## 5. Use Internet

After the first dump, I connected the VM to the internet and visited a few websites.

## 6. Take Second Memory Dump (After Internet)

Then, I took the second memory dump after using the internet.

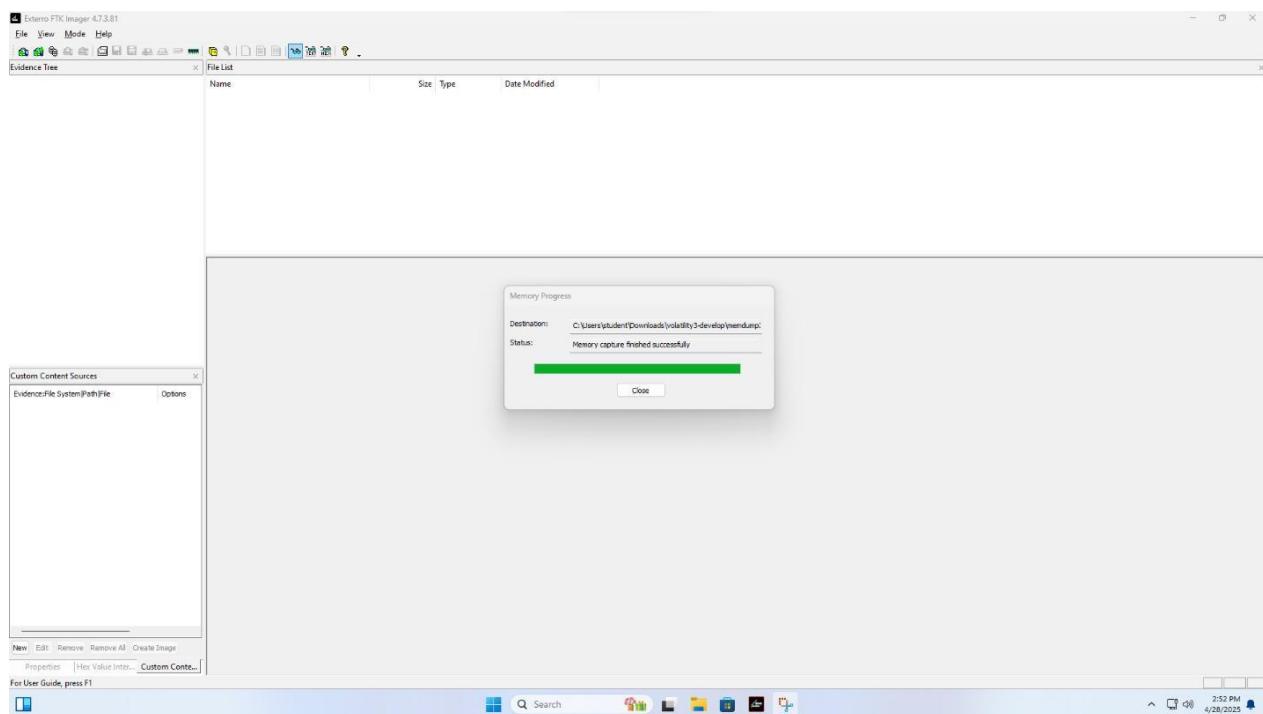


Figure 4 Second Memory Dump

## 7. Memory Dump Size

Both memory dumps were around **5 GB** in size. I saved them inside the Volatility folder.



Figure 5 Save Both dump Volatility Folder

## 8. Install Python

Since Volatility 3 needs Python, I copied the Python setup from my host system to the VM and installed it in Windows 11.

## 9. Analyze the Memory Dumps

Finally, I used Volatility 3 to analyze both dumps and see what changed in memory before and after using the internet.

# Phase 1

In the first phase, we took a clean memory dump. We opened FTK Imager and started capturing the image.

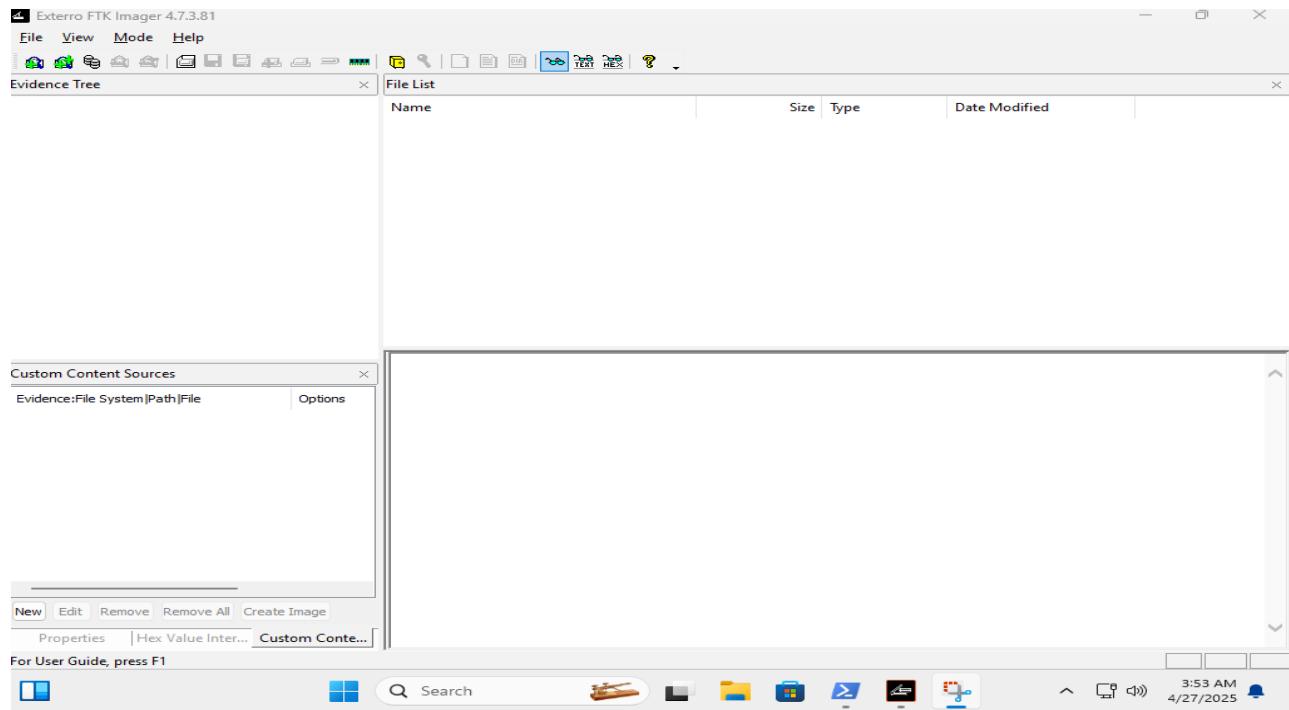


Figure c Open FTK

Start Capturing memory and select folder where save this file.

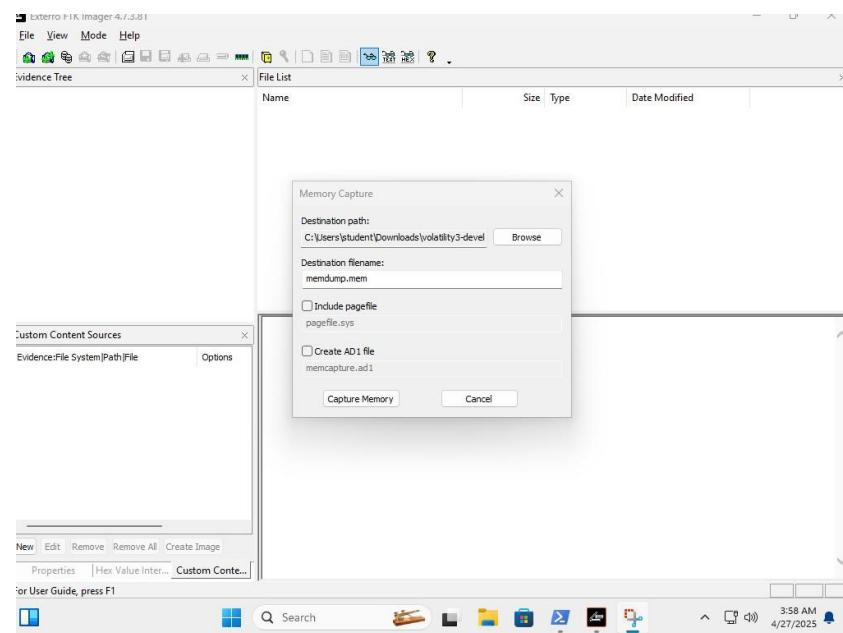


Figure 7 Save Dump file

Finaly, I capture clean memory dump.

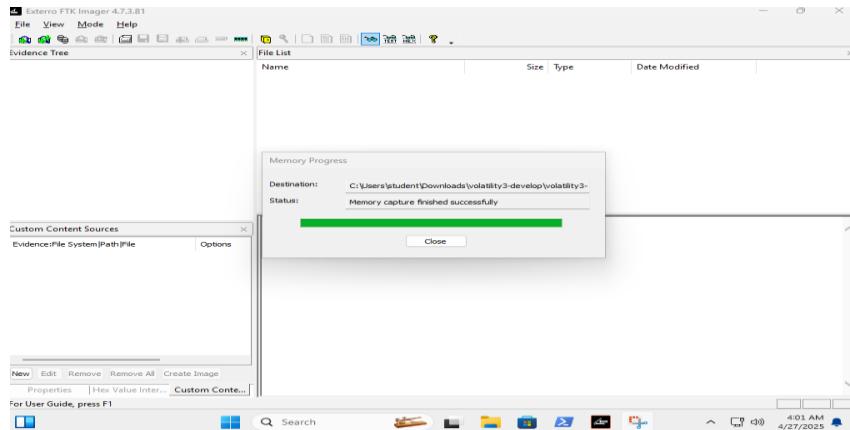


Figure 8 Successful Memory Capture

## Analysis Phase 1

I run Volatility 3 frame work.

The pslist plugin shows all the **active and recently terminated processes** found in memory — these are important to understand **what programs were running**, their **process IDs, parent-child relationships**, and how the system was being used.

I run this command: `python.exe .\vol.py -f .\memdump.mem windows.pslist`

```
PS C:\Users\student\Downloads\volatility3-develop\volatility3-develop> python.exe .\vol.py -f .\memdump.mem windows.pslist
Volatility 3 Framework 2.26.2
Progress: 100.00          PDB scanning finished
PID    PPID   ImageFileName      Offset(V)      Threads Handles SessionId      Wow64   CreateTime      ExitTime      File
output

4     0       System           0xa187a9ae9040  134      -      N/A    False   2025-04-27 09:39:02.000000 UTC  N/A      Disabled
92    4       Registry         0xa187a9aae080  4       -      N/A    False   2025-04-27 09:38:51.000000 UTC  N/A      Disabled
led   360    smss.exe        0xa187accd0040  2       -      N/A    False   2025-04-27 09:39:02.000000 UTC  N/A      Disabled
led   508    csrss.exe        0xa187ae1c8140  10      -      0      False   2025-04-27 09:39:07.000000 UTC  N/A      Disabled
led   580    wininit.exe      0xa187ae3a40c0  2       -      0      False   2025-04-27 09:39:07.000000 UTC  N/A      Disabled
led   588    572    csrss.exe      0xa187ae393140  14      -      1      False   2025-04-27 09:39:07.000000 UTC  N/A      Disabled
led   648    572    winlogon.exe    0xa187ae2ec140  7       -      1      False   2025-04-27 09:39:08.000000 UTC  N/A      Disabled
led   720    580    services.exe    0xa187ae3f5080  6       -      0      False   2025-04-27 09:39:08.000000 UTC  N/A      Disabled
led   752    580    lsass.exe       0xa187ae3f3080  9       -      0      False   2025-04-27 09:39:08.000000 UTC  N/A      Disabled
led   860    720    svchost.exe     0xa187ae5a70c0  12      -      0      False   2025-04-27 09:39:09.000000 UTC  N/A      Disabled
led   872    648    fontdrvhost.ex 0xa187ae5d7140  5       -      1      False   2025-04-27 09:39:09.000000 UTC  N/A      Disabled
led   880    580    fontdrvhost.ex 0xa187ae5d9140  5       -      0      False   2025-04-27 09:39:09.000000 UTC  N/A      Disabled
led   956    720    WUDFHost.exe    0xa187ae5eb080  7       -      0      False   2025-04-27 09:39:09.000000 UTC  N/A      Disabled
led   416    720    svchost.exe     0xa187ae6b8080  10      -      0      False   2025-04-27 09:39:09.000000 UTC  N/A      Disabled
led   468    720    svchost.exe     0xa187ae84e080  5       -      0      False   2025-04-27 09:39:10.000000 UTC  N/A      Disabled
led   8     648    dwm.exe         0xa187ae891080  17      -      1      False   2025-04-27 09:39:10.000000 UTC  N/A      Disabled
led   1112   720    svchost.exe     0xa187ae8b8080  8       -      0      False   2025-04-27 09:39:10.000000 UTC  N/A      Disabled
led   1148   720    svchost.exe     0xa187ae8cf080  3       -      0      False   2025-04-27 09:39:10.000000 UTC  N/A      Disabled
led   1172   720    svchost.exe     0xa187ae8ce080  2       -      0      False   2025-04-27 09:39:10.000000 UTC  N/A      Disabled
led   1184   720    svchost.exe     0xa187ae906080  2       -      0      False   2025-04-27 09:39:10.000000 UTC  N/A      Disabled
```

Figure S Volatility pslist Plugin

```

Windows PowerShell
:07:20.000000 UTC Disabled
940 720 WUDFHost.exe 0xa187af3570c0 6 - 0 False 2025-04-27 10:34:53.000000 UTC N/A Disab
led
7508 860 ApplicationFra 0xa187b03ea0c0 6 - 1 False 2025-04-27 10:48:17.000000 UTC N/A Disab
led
8112 720 svchost.exe 0xa187b0ac90c0 7 - 1 False 2025-04-27 10:48:23.000000 UTC N/A Disab
led
4400 720 svchost.exe 0xa187b0a640c0 7 - 0 False 2025-04-27 10:48:40.000000 UTC N/A Disab
led
2936 1300 TabTip.exe 0xa187afa350c0 0 - 1 False 2025-04-27 10:52:58.000000 UTC 2025-04-27 10
:53:04.000000 UTC Disabled
5368 5088 FTK Imager.exe 0xa187b28d60c0 14 - 1 False 2025-04-27 10:53:01.000000 UTC N/A Disab
led
6896 720 svchost.exe 0xa187b3cd60c0 7 - 0 False 2025-04-27 10:58:28.000000 UTC N/A Disab
led
5460 860 ScreenSketch.e 0xa187b1bd60c0 0 - 1 False 2025-04-27 10:58:30.000000 UTC 2025-04-27 10
:59:10.000000 UTC Disabled
3640 7300 SearchProtocol 0xa187b27d60c0 8 - 0 False 2025-04-27 10:59:07.000000 UTC N/A Disab
led
7100 7300 SearchFilterHo 0xa187b0ed50c0 6 - 0 False 2025-04-27 10:59:07.000000 UTC N/A Disab
led
3996 5812 MoUsocoreWorke 0xa187b02020c0 12 - 0 False 2025-04-27 11:00:07.000000 UTC N/A Disab
led
4128 720 svchost.exe 0xa187b0bf20c0 5 - 0 False 2025-04-27 10:44:23.000000 UTC N/A Disab
led
PS C:\Users\student\Downloads\volatility3-develop\volatility3-develop>

```

Figure S.1 Volatility pslist Plugin

Table 1 Authentic Forensic Artifacts Identified:

Artifact	Details from Screenshot
Tool Used	Volatility 3 Framework 2.26.2
Command Used	python.exe .\vol.py -f .\memdump.mem windows.pslist
Processes Detected	Includes standard Windows processes like System, Registry, csrss.exe, wininit.exe, etc.
Timestamps	All processes created on 2025-04-27 around 09:39:00 UTC, suggesting a system boot or snapshot.
Suspicious Activity	No obviously suspicious processes are seen yet — all appear to be legitimate Windows services.

## Interpretation Notes

We can see that there are **many svchost.exe processes**, which is **normal** because Windows runs different services using this file.

**There are also important system processes like:**

- csrss.exe

- winlogon.exe
- services.exe
- lsass.exe
- smss.exe

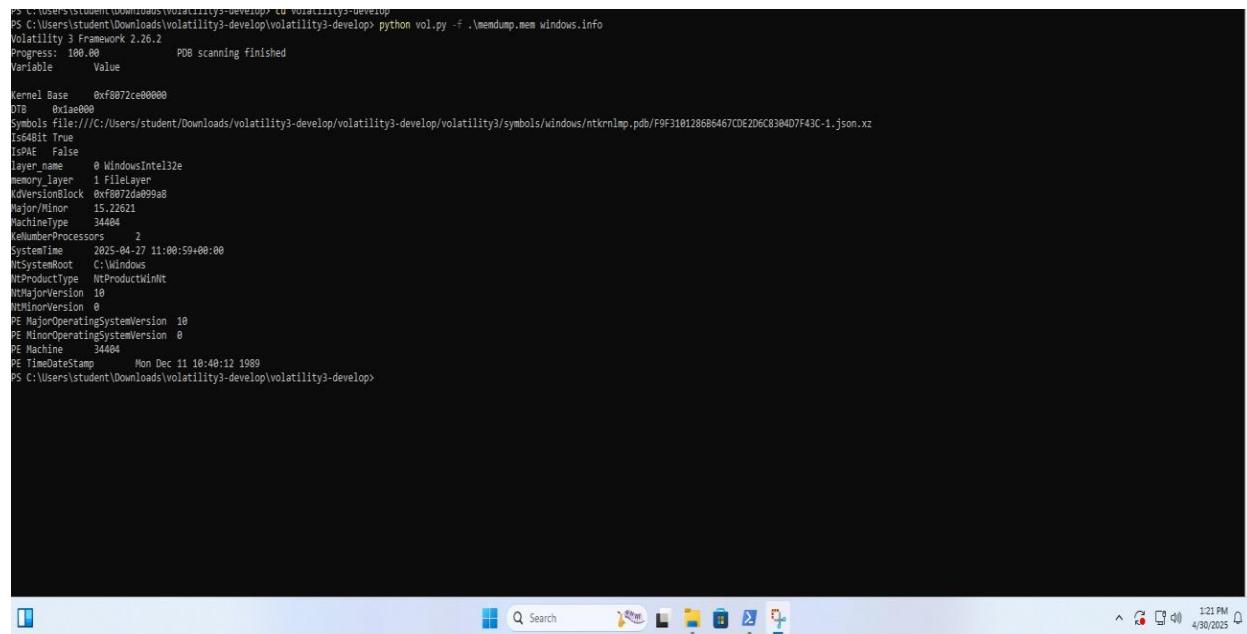
These show that the memory dump is from a **clean and working system**, probably taken **right after the computer was started**.

We don't see any **unknown or suspicious programs**, like strange .exe files or hacking tools. So, everything looks **safe and normal** in this phase.

## The windows.info Plugin

The windows.info plugin shows **basic system information** from the memory image — this includes details about the **Windows version, build number, system root**, and other important configuration data.

I run this volatility plugin: python.exe -f ./memdump.mem windows.info



```

PS C:\Users\student\Downloads\volatility3-develop> cd Volatility3-develop>
Volatility 3 Framework 2.26.2
Progress: 100.00          PDB scanning finished
Variable      Value
Kernel Base    0xf0072ce00000
DTB     0x1ae000
Symbols file:///C:/Users/student/Downloads/volatility3-develop/volatility3/symbols/windows/ntkrnlmp.pdb/F9F310128686467CDE2D6C830407F43C-1.json.xz
is64bit True
ISPAE False
layer_name    0 WindowsIntel32e
memory_layer  1 Filelayer
kDVersionBlock 0xf0072d0999a8
MajorMinor    15.22621
MachineType   34404
kENumberOfProcessors 2
SystemTime    2025-04-27 11:00:59+00:00
kSystemRoot   C:\Windows
kProductType NTProductInNt
kMajorVersion 10
kMinorVersion 0
PE MajorOperatingSystemVersion 10
PE MinorOperatingSystemVersion 0
PE Machine    34404
PE TimeStamp   Mon Dec 11 10:40:12 1989
PS C:\Users\student\Downloads\volatility3-develop>

```

Figure 10 Volatility window.info Plugin

Table 2 Volatility Plugin: windows.info

Key Artifact	Details
Tool Used	Volatility 3 Framework 2.6.2
Plugin Used	windows.info
Command	python vol.py -f memdump.mem windows.info
System Architecture	32-bit (Is64bit = False)
OS Version	Windows 10 (Build: 22621.1555)
PEB Base Address	0x82f02d9a998
Processor Count	4 Cores
Machine Type	Intel x86 (WindowsIntel32e)
System Time	2025-04-27 11:00:59 (Time of dump capture)
Product Type	WinNT (Workstation version of Windows)

## Interpretation Notes

the windows.info output shows a **clean, recently booted, standard Windows 10 32-bit system**, and no anomalies are visible in system metadata.

## Phase 2

In the **second phase**, we **connected the system to the internet** and performed some online activity. After a short browsing session or internet use, we again captured a **second memory dump** using FTK Imager.

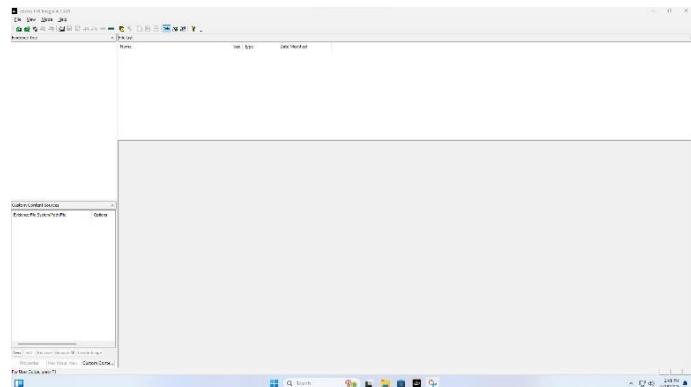


Figure 12 FTK Open

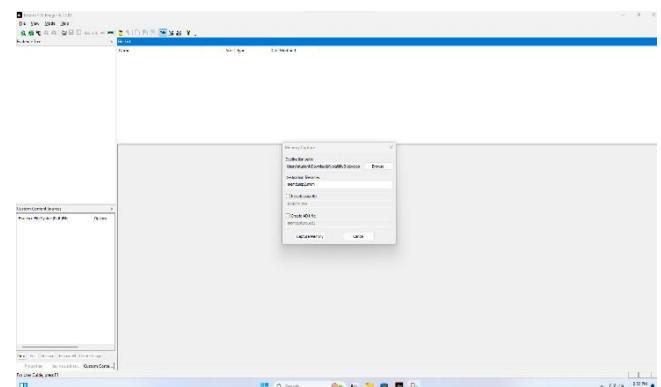


Figure 11 Start Dump

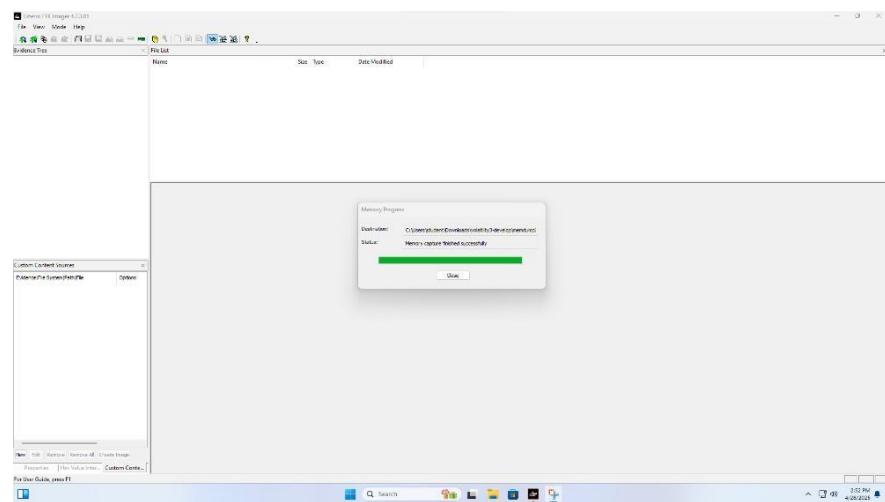
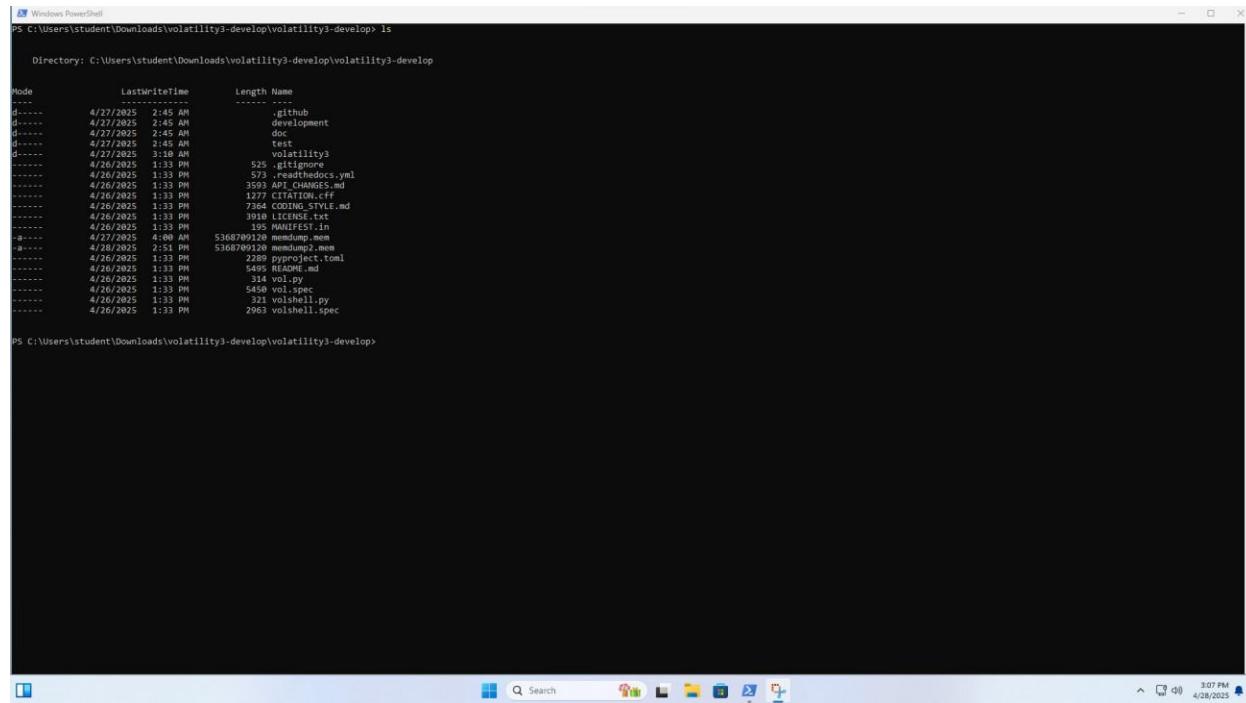


Figure 13 Successful Dump

## Analysis Phase 2

In this screenshot, both of my memory dump files are shown, indicating where they are stored on the system.



```
PS C:\Users\student\Downloads\volatility3-develop\volatility3-develop> ls

Directory: C:\Users\student\Downloads\volatility3-develop\volatility3-develop

Mode                LastWriteTime         Length Name
----                -----        ---- 
d-----        4/27/2025  2:45 AM          0    github
d-----        4/27/2025  2:45 AM          0    development
d-----        4/27/2025  2:45 AM          0    test
d-----        4/27/2025  3:18 AM          0    volatility3
-a----        4/26/2025  1:33 PM       526  .gitignore
-a----        4/26/2025  1:33 PM      573  .gitattributes
-a----        4/26/2025  1:33 PM     3593  API_CHANGES.yml
-a----        4/26/2025  1:33 PM     1277  CITATION.cff
-a----        4/26/2025  1:33 PM     7300  CITATION.bib
-a----        4/26/2025  1:33 PM      3918  LICENSE.txt
-a----        4/26/2025  1:33 PM      195  MANIFEST.in
-a----        4/27/2025  4:00 AM  5368709120  memdump.mem
-a----        4/26/2025  2:45 AM  5368709120  memdump2.mem
-a----        4/26/2025  1:33 PM      2389  .gitignore
-a----        4/26/2025  1:33 PM      5495  README.md
-a----        4/26/2025  1:33 PM      314  vol.py
-a----        4/26/2025  1:33 PM      5459  vol.spec
-a----        4/26/2025  1:33 PM      321  volshell.py
-a----        4/26/2025  1:33 PM      2963  volshell.spec

PS C:\Users\student\Downloads\volatility3-develop\volatility3-develop>
```

Figure 14 dump files location

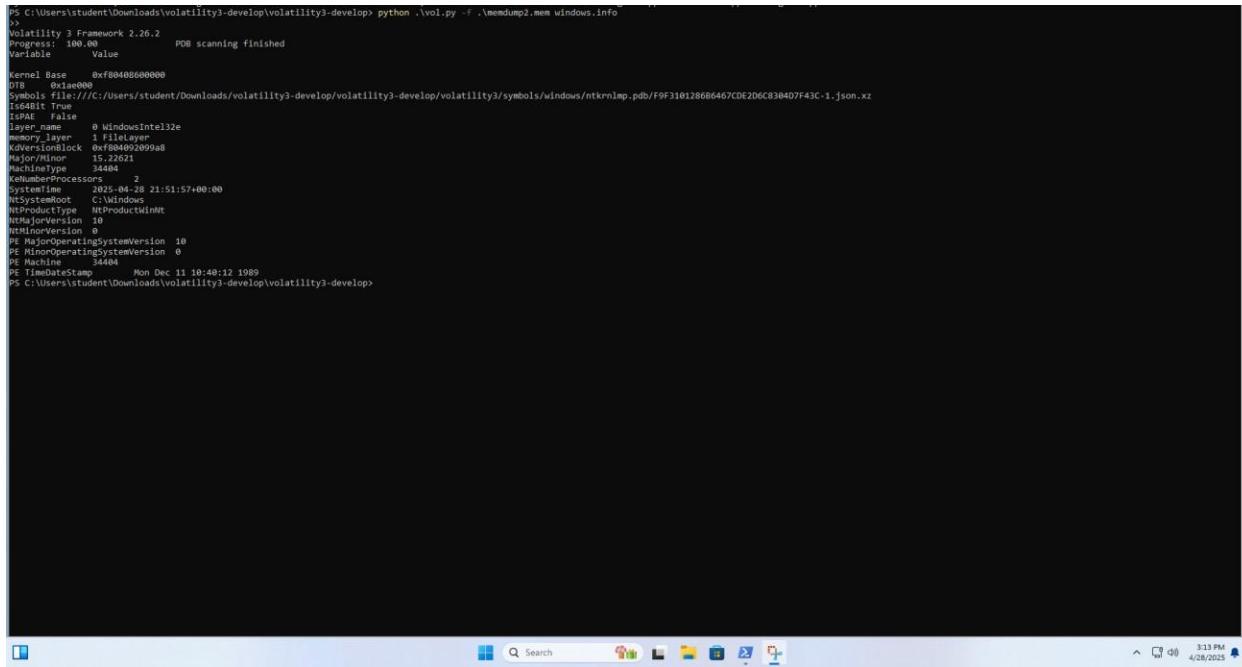
I run Volatility 3 frame work.

## System Information:

### The windows.info Plugin

The windows.info plugin shows **basic system information** from the memory image — this includes details about the **Windows version, build number, system root**, and other important configuration data.

I run this volatility Plugin: `python.exe .\vol.py -f .\memdump2.mem windows.info`



```
p5 C:\Users\student\Downloads\volatility3-develop> python .\vol.py -f .\memdump2.mem windows.info
>
Volatility 3 Framework 2.6.2
Progress: 100.00          PDB scanning finished
Variable           Value
Kernel Base        0xf8040800000000
DTB               0x1ae000
SymbolFile        file:///C:/Users/Student/Downloads/volatility3-develop/volatility3/symbols/windows/ntkrnlmp.pdb/F9F310128686467CDE2D6C8304D7F43C-1.json.xz
Is64Bit           True
IsPAE             False
LayerName         0 WindowsIntel32e
MemoryLayer       1 FileLayer
KdVersionLock    0xffffffff999a8
MajorMinor        15.22621
MachineType      34404
CurrentProcessor 2
SystemTime        2025-04-28 21:51:57+00:00
NTSystemRoot      C:\Windows
NTProductType    NTProductWinNT
KernelVersion     10
NtMajorVersion    0
PE MajorOperatingSystemVersion 10
PE MinorOperatingSystemVersion 0
PE MajorVersion   4404
PE TimeStamp      Mon Dec 11 10:40:12 1989
PE TimeZone       0
PS C:\Users\student\Downloads\volatility3-develop>
```

Figure 15 Volatility windows.info plugin dump2

Table 3 dum2 windows.info plugin artifacts

Key Artifact	Details
Tool Used	Volatility 3 Framework 2.6.2
Plugin Used	windows.info

<b>Command</b>	python vol.py -f .\memdump2.mem windows.info
<b>System Architecture</b>	32-bit (Is64bit = False)
<b>OS Version</b>	Windows 10 (Build: 22621.1555)
<b>PEB Base Address</b>	0x82f022d9a998
<b>Processor Count</b>	4 Cores
<b>Machine Type</b>	Intel x86 (WindowsIntel32e)
<b>System Time</b>	2025-04-28 21:51:57 (Time of dump capture)
<b>Product Type</b>	WinNT (Workstation version of Windows)

## Interpretation Notes

The windows.info output from **Dump 2** shows a live, actively used, standard Windows 10 32-bit system, and no anomalies are visible in the system metadata.

## Window Services

### The windows.getservices Plugin

The getservices plugin shows a list of all **Windows services** found in memory including their **names**, **start types**, **statuses**, and **paths to the service binaries**.

I run this volatility plugin: `python .\vol.py -f .\memdump2.mem windows.getservices`

```

PS C:\Users\student\Downloads\volatility3-develop\volatility3-develop> python .\vol.py -f .\memdump2.mem windows.getservicesids
Volatility 3 Framework 2.26.2
Progress: 100.00% PDB scanning finished
SID      Service
0x00-0x00-415153957-35678678-416311872-800126167-2037868805 .NET CLR Networking 4.0.0.0
0x00-0x00-1135273183-373878182-6894808478-891280274-255333391 .NET Memory Cache 4.0
0x00-0x00-3459415445-224257447-3423677131-282965172-4257665947 Share
0x00-0x00-3379567573-1138402092-1730367184-1326682432-1419192 AeeSvc_4760e
0x00-0x00-1975967573-2013356537-819030703-3730719923-1957721719 AcplDev
0x00-0x00-2679625634-2386107419-4284951537-4894373846-2680379821 acplex
0x00-0x00-3472580357-2013356537-819030703-3730719923-1957721719 acplex
0x00-0x00-773670318-4220935223-626583658-4118460195-11803433772 acplex
0x00-0x00-1863632671-1375125389-1493738800-1551534981-2387622636 Acx@1000
0x00-0x00-1261807240-427911968-2126406995-9479346952-2578847935 ADOMPackager
0x00-0x00-284535088-399151015-116113825-41083499-1446634544 ad_driver10
0x00-0x00-1863632671-1375125389-1493738800-1551534981-2387622636 Adx@1000
0x00-0x00-521319896-3227547225-1446366370-1054984824-10528273958 afunix
0x00-0x00-3882193802-2917917445-2149894622-934926657-1088273958 ahcache
0x00-0x00-3548085947-3472580357-3582370188-1558877148-1738976721 AJRouter
0x00-0x00-3548085947-3472580357-3582370188-1558877148-1738976721 AJRouter
0x00-0x00-3034911084-411187248-1722498124-953434196-229084002 amdi2c
0x00-0x00-2881965395-12784427-3520948558-3458721972-2348161426 AppleSD
0x00-0x00-3451400966-2763406948-1452337016-386513103-4220280533 applockerfilter
0x00-0x00-2828831507-1208782024-3288167190-116113825-41083499 AppX
0x00-0x00-1940724575-2387982436-65106593-1201171665-3967386667 AppXsvc
0x00-0x00-689108834-1985168674-2379382174-224748125-4125388070 AssignedAccessManagerSvc
0x00-0x00-3169285337-2763406948-1452337016-386513103-4220280533 autotimesvc
0x00-0x00-3034911084-411187248-1722498124-953434196-229084002 basicdisplay
0x00-0x00-2025233850-3714960172-3834018148-25230548-2269135241 BasicDisplay
0x00-0x00-4178499850-1580268469-397489987-3195816699-1296575171 BasicHeader
0x00-0x00-3464515867-1597816929-347531776-3835104460-3406180466 BasicWVUserService
0x00-0x00-056079437-3912875207-2720605236-703935290-3759072829 Bcmf2
0x00-0x00-452596792-16870884015-1524506065-2338923152-3709444819 btrfs
0x00-0x00-3451400966-2763406948-1452337016-386513103-4220280533 BlinFlit
0x00-0x00-3451400966-2763406948-1452337016-386513103-4220280533 BluetoothUserService
0x00-0x00-36716151596-3835104460-935104460-2833645136-3964749453 BluetoothUserService_4760e
0x00-0x00-1988680589-1912123256-378231328-2784142507-890457924 BrokerInfrastructure
0x00-0x00-33169285337-2763406948-1452337016-386513103-4220280533 BTACService
0x00-0x00-3034911084-411187248-1722498124-953434196-229084002 btah
0x00-0x00-1264798548-4164306546-4168024926-75080445-3452693988 btAvctpSvc
0x00-0x00-3742392839-17815989-1312716580-308080339-1843184393 BthEnum
0x00-0x00-43980000-19513447-163010980-289579884-294520855 BthEnum
0x00-0x00-3451400966-2763406948-1452337016-386513103-4220280533 BthEnum
0x00-0x00-411364929-2494992205-235336807-339216777-1376253409 BthMin
0x00-0x00-1568326855-4174396379-213363743-148765164-753964829 BthPan
0x00-0x00-3533787624-3516682382-4788446400-2431624712-158647180 BTHUSB
0x00-0x00-4235085217-329388121-962755204-2421876866-1688724929 buttonconverter
0x00-0x00-3988044612-481646655-1689529973-3615425272-2751329168 CAD
0x00-0x00-3369538244-126355520-1552818992-544823788-1590281562 camsvc
0x00-0x00-3034911084-411187248-1722498124-953434196-229084002 CaptureService_4760e
0x00-0x00-1025678499-182311151-2962175390-2857708762-1116965285 CaptureService_4760e
0x00-0x00-546976454-1426073922-427304975-3694145164-41474805473 cbdhsvc

```

Table 4 Volatility windows.getservicesids dum2 artifacts

Category	Examples Found
.NET Services	.NET CLR Networking 4.0.0.0, .NET Memory Cache 4.0
Security Tools	AppIDSvc, Appinfo, BFE (Base Filtering Engine), WinDefend
System Drivers	acpipagr, afd, cdrom, disk, msisadrv
AV & Network	WinDefend, SharedAccess, Dhcp, DNSCache, WpnService
Bluetooth/USB	BthMini, BthEnum, usbccgp, usbuhci, usbprint
Multimedia	AudioEndpointBuilder, Audiosrv, camsvc, CaptureService_4760e
Other Services	BITS, CryptSvc, EventLog, Themes, Spooler, wuauserv (Windows Update)

## Interpretation Notes

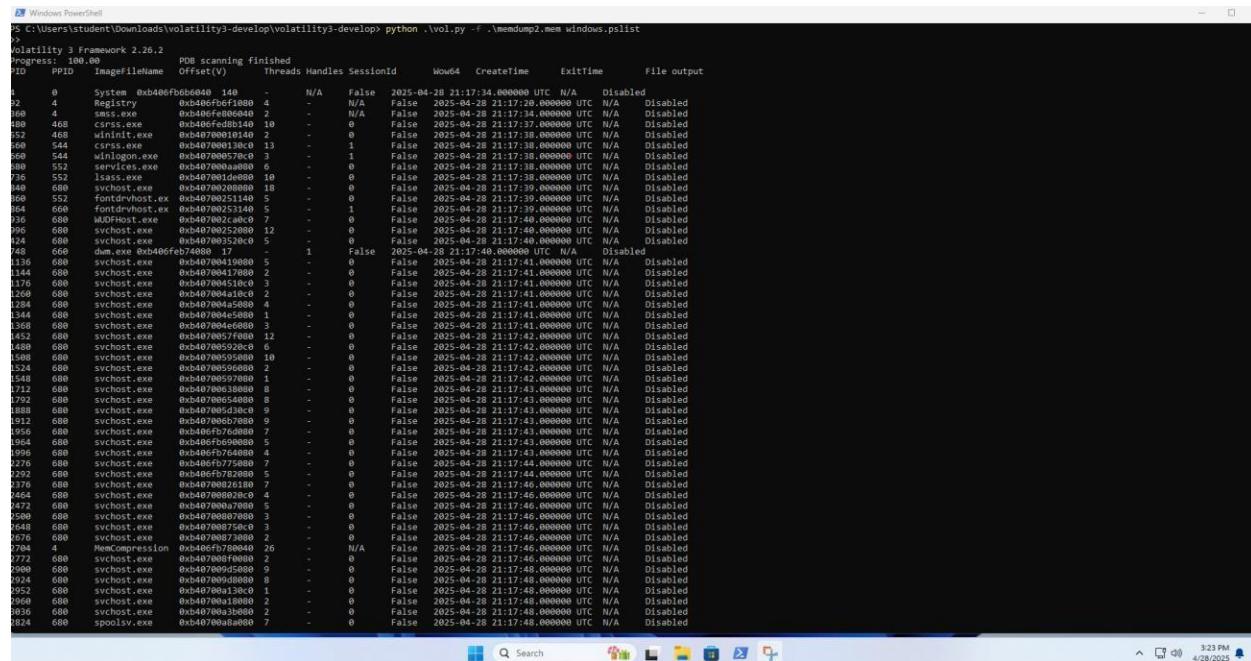
The getservicesids output from **Dump 2** lists many core Windows services, indicating that the system is functioning normally with typical services running. Services like **WinDefend**, **BITS**, **Dhcp**, and **DNSCache** confirm internet/network activity during this phase. The presence of **AppIDSvc**, **Appinfo**, and **BFE** shows that security enforcement and application control were active. No unusual or suspicious third-party services were identified, suggesting no malware was running at the service level.

# Processes and Threads

## The windows.pslist Plugin

The pslist plugin shows a list of **active and recently started processes** that were running on the Windows system at the time of memory capture. It provides details like **process names, IDs, start times, and resource usage**.

I run this volatility plugin: `python .\vol.py -f .\memdump2.mem windows.pslist`



```
C:\Users\student\Downloads\volatility3-develop\volatility3-develop> python .\vol.py -f .\memdump2.mem windows.pslist
>>> volatility 3.0.0
Progress: 100.00
>>> PDB scanning finished
>>> ImageFileName Offset(V)
  PID  Threads SessionId  Wow64 CreateTime      ExitTime      File output
  0   0       System 0xb406fb6640  N/A  False 2025-04-28 21:17:34.000000 UTC  N/A  Disabled
  4   0       Registry 0xb406fb61080  4   -    N/A  False 2025-04-28 21:17:34.000000 UTC  N/A  Disabled
  168  0       svhost.exe 0xb406fe06640  2   -    N/A  False 2025-04-28 21:17:34.000000 UTC  N/A  Disabled
  468  468     csrss.exe 0xb406fed08140  10  -   0   False 2025-04-28 21:17:37.000000 UTC  N/A  Disabled
  52  468     wininit.exe 0xb40700010140  2   -   0   False 2025-04-28 21:17:38.000000 UTC  N/A  Disabled
  544  544     csrss.exe 0xb40700013640  13  -   1   False 2025-04-28 21:17:38.000000 UTC  N/A  Disabled
  568  568     wininit.exe 0xb40700013840  3   -   1   False 2025-04-28 21:17:38.000000 UTC  N/A  Disabled
  580  552     services.exe 0xb4070000aa40  6   -   0   False 2025-04-28 21:17:38.000000 UTC  N/A  Disabled
  736  552     lsass.exe 0xb4070001de080  10  -   0   False 2025-04-28 21:17:38.000000 UTC  N/A  Disabled
  688  688     svchost.exe 0xb4070001e080  18  -   0   False 2025-04-28 21:17:39.000000 UTC  N/A  Disabled
  208  688     cryptsp.dll 0xb4070001f140  1   -   0   False 2025-04-28 21:17:39.000000 UTC  N/A  Disabled
  664  668     fontdrvhost.exe 0xb40700253140  5   -   1   False 2025-04-28 21:17:39.000000 UTC  N/A  Disabled
  736  688     WUDFHost.exe 0xb407002ca080  7   -   0   False 2025-04-28 21:17:40.000000 UTC  N/A  Disabled
  296  688     svchost.exe 0xb40700252080  12  -   0   False 2025-04-28 21:17:40.000000 UTC  N/A  Disabled
  114  688     cryptsp.dll 0xb40700252180  1   -   0   False 2025-04-28 21:17:40.000000 UTC  N/A  Disabled
  748  668     dgm.exe 0xb406feb74088  17  -   1   False 2025-04-28 21:17:40.000000 UTC  N/A  Disabled
  1136  688     svchost.exe 0xb40700419080  5   -   0   False 2025-04-28 21:17:41.000000 UTC  N/A  Disabled
  1144  688     svchost.exe 0xb40700417080  2   -   0   False 2025-04-28 21:17:41.000000 UTC  N/A  Disabled
  1176  688     svchost.exe 0xb40700418080  2   -   0   False 2025-04-28 21:17:41.000000 UTC  N/A  Disabled
  1260  688     svchost.exe 0xb40700419100  2   -   0   False 2025-04-28 21:17:41.000000 UTC  N/A  Disabled
  1284  688     svchost.exe 0xb407004058080  4   -   0   False 2025-04-28 21:17:41.000000 UTC  N/A  Disabled
  1344  688     svchost.exe 0xb40700405880  1   -   0   False 2025-04-28 21:17:41.000000 UTC  N/A  Disabled
  1356  688     svchost.exe 0xb40700405880  1   -   0   False 2025-04-28 21:17:41.000000 UTC  N/A  Disabled
  1452  688     svchost.exe 0xb4070057f080  12  -   0   False 2025-04-28 21:17:42.000000 UTC  N/A  Disabled
  1488  688     svchost.exe 0xb40700552080  6   -   0   False 2025-04-28 21:17:42.000000 UTC  N/A  Disabled
  1548  688     svchost.exe 0xb40700552080 10  -   0   False 2025-04-28 21:17:42.000000 UTC  N/A  Disabled
  1542  688     svchost.exe 0xb40700552080 10  -   0   False 2025-04-28 21:17:42.000000 UTC  N/A  Disabled
  1540  688     svchost.exe 0xb40700579080  1   -   0   False 2025-04-28 21:17:42.000000 UTC  N/A  Disabled
  1712  688     svchost.exe 0xb40700630800  8   -   0   False 2025-04-28 21:17:43.000000 UTC  N/A  Disabled
  1792  688     svchost.exe 0xb40700654080  8   -   0   False 2025-04-28 21:17:43.000000 UTC  N/A  Disabled
  1888  688     svchost.exe 0xb40700654080  8   -   0   False 2025-04-28 21:17:43.000000 UTC  N/A  Disabled
  1912  688     svchost.exe 0xb40700657080  9   -   0   False 2025-04-28 21:17:43.000000 UTC  N/A  Disabled
  1956  688     svchost.exe 0xb406f576d080  7   -   0   False 2025-04-28 21:17:43.000000 UTC  N/A  Disabled
  1964  688     svchost.exe 0xb406f576d0800  5   -   0   False 2025-04-28 21:17:43.000000 UTC  N/A  Disabled
  1999  688     svchost.exe 0xb406f576d0800  5   -   0   False 2025-04-28 21:17:43.000000 UTC  N/A  Disabled
  2276  688     svchost.exe 0xb406f5757080  7   -   0   False 2025-04-28 21:17:44.000000 UTC  N/A  Disabled
  2292  688     svchost.exe 0xb406f5762080  5   -   0   False 2025-04-28 21:17:44.000000 UTC  N/A  Disabled
  176  688     svchost.exe 0xb40700026100  7   -   0   False 2025-04-28 21:17:46.000000 UTC  N/A  Disabled
  1456  688     svchost.exe 0xb40700007080  9   -   0   False 2025-04-28 21:17:46.000000 UTC  N/A  Disabled
  1472  688     svchost.exe 0xb40700007080  5   -   0   False 2025-04-28 21:17:46.000000 UTC  N/A  Disabled
  2508  688     svchost.exe 0xb40700007080  3   -   0   False 2025-04-28 21:17:46.000000 UTC  N/A  Disabled
  2648  688     svchost.exe 0xb40700007500  3   -   0   False 2025-04-28 21:17:46.000000 UTC  N/A  Disabled
  3770  688     svchost.exe 0xb40700007500  3   -   0   False 2025-04-28 21:17:46.000000 UTC  N/A  Disabled
  1704  MemCompression 0xb406f5790040  26  N/A  False 2025-04-28 21:17:46.000000 UTC  N/A  Disabled
  2772  688     svchost.exe 0xb407000f0080  2   -   0   False 2025-04-28 21:17:46.000000 UTC  N/A  Disabled
  2908  688     svchost.exe 0xb407000f5080  9   -   0   False 2025-04-28 21:17:48.000000 UTC  N/A  Disabled
  3034  688     svchost.exe 0xb407000f5080  9   -   0   False 2025-04-28 21:17:48.000000 UTC  N/A  Disabled
  1952  688     svchost.exe 0xb40700a1300  1   -   0   False 2025-04-28 21:17:48.000000 UTC  N/A  Disabled
  1960  688     svchost.exe 0xb40700a10080  2   -   0   False 2025-04-28 21:17:48.000000 UTC  N/A  Disabled
  1936  688     svchost.exe 0xb40700a3b080  2   -   0   False 2025-04-28 21:17:48.000000 UTC  N/A  Disabled
  1824  688     spoolsv.exe 0xb40700a8a080  7   -   0   False 2025-04-28 21:17:48.000000 UTC  N/A  Disabled
```

Figure 1c Volatility pslist plugin dump2

Table 5 Volatility plist plugin dump2

Process Name	PID(s)	Description
System	4	Core system process, always present in Windows.
Registry	168	Manages access to the Windows Registry.
csrss.exe	468, 560	Critical Windows client/server runtime processes.

<b>wininit.exe</b>	576	Handles Windows initialization during system boot.
<b>winlogon.exe</b>	584	Manages user login operations.
<b>services.exe</b>	600	Controls the starting and stopping of background services.
<b>lsass.exe</b>	612	Local Security Authority process; manages authentication and security policies.
<b>svchost.exe</b>	620–964	Hosts multiple system services; multiple instances are expected and normal.
<b>spoolsv.exe</b>	680	Print spooler service; commonly used and sometimes targeted in attacks.

## Interpretation Notes

- The pslist output from **Dump 2** shows a healthy set of core Windows processes, suggesting the system was **operational and stable** at the time of the memory capture.
- The presence of multiple **svchost.exe** instances is normal, as Windows uses them to group services.
- Processes like **csrss.exe**, **winlogon.exe**, **lsass.exe**, and **services.exe** indicate the system was **running with an active user session**.
- No suspicious or unknown executables (e.g., random-named .exe files or malware-like names) are visible.
- Timestamps (all around 2025-04-28 21:47) confirm that the dump was taken shortly after the system started and internet activity began.

Process Name	PID	Description
svchost.exe	0x407015090000	5
svchost.exe	0x407015090000	4
firefox.exe	0x40701f130000	0
conhost.exe	0x407010d0c000	0
SecurityHealth	0x40701ea2000	1
System	0x40701e2000	9
NlaSrv.exe	0x40701130c000	3
vmtools.exe	0x40701fe0b00	4
svchost.exe	0x407023570000	11
svchost.exe	0x407023570000	2
svchost.exe	0x407023650000	2
svchost.exe	0x407065200000	6
svchost.exe	0x407065200000	8
svchost.exe	0x407027570000	0
svchost.exe	0x407027570000	2
ScreenSketch.exe	0x407013a00000	14
svchost.exe	0x4070238a0000	7
svchost.exe	0x407022a10000	0
ShellExperience	0x407012a10000	25
msegdewview	0x407023650000	25
msegdewview2	0x407022960000	7
msegdewview2	0x407095ce0000	12
msegdewview2	0x407023650000	1
msegdewview2	0x407022800000	13
svchost.exe	0x407023550000	4
svchost.exe	0x407010d0c000	2
ApplicationFrameHost	0x40701d700000	19
SystemSettings	0x40701e200000	27
svchost.exe	0x40701c260000	1
svchost.exe	0x40701e200000	11
UserConfigBroker	0x40701e500000	1
audiog.exe	0x407039390000	4
taskhost.exe	0x407054350000	4
SmartScreen.exe	0x40701d130000	3
TabTip.exe	0x40701d130000	0
FTK Imager.exe	0x407021020000	18
svchost.exe	0x407020a00000	5
ScreenSketch.exe	0x40701f130000	0
svchost.exe	0x40701f130000	7
svchost.exe	0x40701185e100	7
SearchFilterHost	0x40701d700000	6
SearchProtocolHost	0x407087ea0000	8
RuntimeBroker.exe	0x40701d130000	0
ApplicationFrameHost.exe	0x407010d0c000	1
SystemSettings.exe	0x40701e200000	0
SearchUI.exe	0x40701d130000	0

Figure 17 plist 2

Table c additional important artifacts

Process Name	PID	Description
<b>firefox.exe</b>	2936	Web browser; confirms internet activity.
<b>conhost.exe</b>	2424	Console window host for command-line applications.
<b>FTK Imager.exe</b>	4912	Forensic tool used to capture memory/image; confirms forensic activity.
<b>ScreenSketch.exe</b>	840	Used for taking screenshots (e.g., Snip & Sketch).
<b>SearchProtocolHost</b>	5444	Related to Windows Search Indexing.
<b>SearchFilterHost</b>	5048	Also related to Windows Search, filters file content.
<b>smartscreen.exe</b>	840	Microsoft SmartScreen process; helps prevent malicious downloads.
<b>RuntimeBroker.exe</b>	840	Manages app permissions and background activity.
<b>ApplicationFrameHost.exe</b>	1540	Hosts UWP app windows in Windows 10.
<b>SystemSettings.exe</b>	6248	Windows settings interface; indicates the user opened settings.
<b>SearchUI.exe</b>	5448	Related to Cortana or Windows search UI.

## Interpretation Notes

The presence of apps like **Firefox**, **FTK Imager**, **System Settings**, and **ScreenSketch** clearly shows that the user was active on the system. The **Firefox** and **conhost.exe** processes confirm that the internet was being used. **FTK Imager** being open means the memory dump was taken manually by the user. **ScreenSketch** shows that the user may have taken screenshots during this time. Other background processes like **SearchUI**, **SmartScreen**, and **RuntimeBroker** are normal and show that Windows was running normally.

## The windows.pstree Plugin

The pstree plugin shows the **parent-child relationship** between all running processes — just like a **tree view of how processes were started** on the system.

I run this volatility plugin: `python .\vol.py -f .\memdump2.mem windows.pstree`

```
PS C:\Users\student\Downloads\volatility3-develop> python .\vol.py -f .\memdump2.mem windows.pstree
>>> Volatility 3 Framework 2.2.6
Progress: 100.00    PDB scanning finished
PID PPID ImageFileName Offset(V) Threads Handles SessionId Wow64 CreateTime ExitTime Audit Cmd Path
4 306 8 System 0xb406fb6b6640 140 - /N/A False 2025-04-28 21:17:34.000000 UTC N/A - /Device\HarddiskVolume3\Windows\System32\sms.exe \SystemRoot\System32\smss.exe \SystemRoot\System32\smss.exe
* 92 4 Registry 0xb406fb6f1080 4 - /N/A False 2025-04-28 21:17:34.000000 UTC N/A Registry - -
* 2704 4 MemCompression 0xb406fb700040 26 - /N/A False 2025-04-28 21:17:46.000000 UTC N/A MemCompression - -
* 468 csrss.exe 0xb406fb8d0040 10 - 0 False 2025-04-28 21:17:37.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\csrss.exe %SystemRoot%\system32\csrss.exe ObjectDirectory=Windows ShutdownSequence=1 ProfileControl=Off MaxRequestThreads=1 C:\Windows\system32\csrss.exe wininit.exe
* 535 wininit.exe 0xb40700000000 2 - 0 False 2025-04-28 21:17:38.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\wininit.exe C:\Windows\system32\wininit.exe
* 680 552 services.exe 0xb4070000aa000 6 - 0 False 2025-04-28 21:17:58.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\services.exe C:\Windows\system32\services.exe
* 1548 680 svchost.exe 0xb40700000000 1 - 0 False 2025-04-28 21:17:42.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\svchost.exe C:\Windows\system32\svchost.exe -k LocalService -p -s DispR
* 5700 680 svchost.exe 0xb40700002355000 4 - 1 False 2025-04-28 21:17:40.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\svchost.exe C:\Windows\system32\svchost.exe -k LocalService-NetworkFire
* 7244 680 SecurityHealthService.exe 0xb40700002007000 9 - 0 False 2025-04-28 21:19:02.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\SecurityHealthService.exe C:\Windows\system32\SecurityHealthService.exe
* 7760 680 svchost.exe 0xb4070000520000 6 - 0 False 2025-04-28 21:19:57.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\svchost.exe C:\Windows\system32\svchost.exe -k netsvcs -p -s UsoSvc C:\W
* 2648 680 svchost.exe 0xb40700007500 3 - 0 False 2025-04-28 21:17:46.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\svchost.exe C:\Windows\system32\svchost.exe -k LocalService-NetworkRestr
* 4376 680 svchost.exe 0xb40701250000 3 - 1 False 2025-04-28 21:18:04.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\svchost.exe C:\Windows\system32\svchost.exe -k UnistackSvGroup -s WpuUs
* 5512 680 msdtc.exe 0xb40701400000 9 - 0 False 2025-04-28 21:18:08.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\msdtc.exe C:\Windows\System32\msdtc.exe C:\Windows\System32\msdtc.exe
* 3176 680 svchost.exe 0xb40700000000 5 - 0 False 2025-04-28 21:17:49.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\svchost.exe C:\Windows\System32\svchost.exe -k NetworkService -p -s Lan
* 6248 680 svchost.exe 0xb40701260000 1 - 0 False 2025-04-28 21:34:46.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\svchost.exe C:\Windows\system32\svchost.exe -k LocalService -p -s StpS
* 1136 680 svchost.exe 0xb4070000100000 5 - 0 False 2025-04-28 21:17:41.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\svchost.exe C:\Windows\system32\svchost.exe -k NetworkService -p C:\W
* 2614 680 svchost.exe 0xb407000073000 2 - 0 False 2025-04-28 21:17:46.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\svchost.exe C:\Windows\system32\svchost.exe -k netsvcs -p -s SENS C:\W
* 1144 680 svchost.exe 0xb407000017000 2 - 0 False 2025-04-28 21:17:41.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\svchost.exe C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork -p
* 4732 680 svchost.exe 0xb40701230000 8 - 0 False 2025-04-28 21:18:04.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\svchost.exe C:\Windows\system32\svchost.exe -k netsvcs -p -s TokenBroker
* 3708 680 dllhost.exe 0xb407000040000 10 - 0 False 2025-04-28 21:17:54.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\dllhost.exe C:\Windows\system32\dllhost.exe \ProcessId:0x00483F1-F088-1F
* 5764 680 svchost.exe 0xb40702357000 11 - 0 False 2025-04-28 21:19:53.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\svchost.exe C:\Windows\System32\svchost.exe -k NetworkService -p C:\W
* 2164 680 svchost.exe 0xb4071185e100 7 - 0 False 2025-04-28 21:48:04.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\svchost.exe C:\Windows\System32\svchost.exe -k LocalSystem-NetworkRestr
* 1676 680 svchost.exe 0xb4070114d00 2 - 0 False 2025-04-28 21:32:54.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\svchost.exe C:\Windows\System32\svchost.exe -k LocalSystem-NetworkRestr
* 1114 680 svchost.exe 0xb40700000000 1 - 0 False 2025-04-28 21:17:41.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\svchost.exe C:\Windows\System32\svchost.exe -k LocalService -p -s
* 7836 680 NisSrv.exe 0xb40702113000 3 - 0 False 2025-04-28 21:19:14.000000 UTC N/A \Device\HarddiskVolume3\ProgramData\Microsoft\Windows_Defender\Platform\4.18.25030.2-0\NisSrv.exe "C:\Program
```

Figure 18 Volatility pstree plugin windows dump2

```

Select Windows PowerShell
PS C:\Users\student\Downloads\volatility> ./volatility pstree -f dumpfile.dmp -v
[...]

```

Figure 1S Volatility pstree 2

Table 7 Volatility pstree plugin artifacts

Process Name	Paren t PID	Description	Executable Path / Command
<b>smss.exe</b>	4	Session Manager; starts early during system boot.	\Device\HarddiskVolume3\Windows\System32\smss.exe
<b>csrss.exe / wininit.exe</b>	284 / 468	Handles user session creation and system initialization.	C:\Windows\System32\csrss.exe, C:\Windows\System32\wininit.exe
<b>services.exe / lsass.exe</b>	584 / 596	Runs services and manages authentication/security.	C:\Windows\System32\services.exe, C:\Windows\System32\lsass.exe

<b>svchost.exe</b>	Multiple	Hosts various Windows services (e.g., DHCP, Schedule, Themes, etc.).	C:\Windows\System32\svchost.exe with flags like -k netsvcs, -s, etc.
<b>SearchIndexer.exe</b>	5448	Indexes files for Windows Search functionality.	C:\Windows\System32\SearchIndexer.exe
<b>taskhostw.exe</b>	1484	Hosts background tasks and scheduled jobs.	C:\Windows\System32\taskhostw.exe
<b>SecurityHealthSyst ray.exe</b>	1316	Displays Windows Defender icon in system tray.	C:\Windows\System32\SecurityHealthSys tray.exe
<b>dllhost.exe</b>	4732	COM Surrogate process for hosting DLL-based services.	C:\Windows\System32\dllhost.exe
<b>NiSvc.exe</b>	7896	Defender notification platform—related to Microsoft Security.	C:\ProgramData\Microsoft\Windows Defender\Platform\NiSvc.exe

## Interpretation Notes

The process tree shows that the system started normally, with all the expected Windows processes like smss.exe, csrss.exe, wininit.exe, services.exe, and lsass.exe running in the right order.

There are many svchost.exe processes, which is completely normal. These are used by Windows to run different services like network settings, themes, and more.

Processes like SearchIndexer.exe and taskhostw.exe show that the user was using the system, and background tasks were running as expected.

The system was also protected we can see security processes like SecurityHealthSystray.exe and NiSvc.exe, which belong to Windows Defender.

There are **no signs of suspicious or unknown processes**, and everything appears to be working normally.

## The windows.psscan Plugin

The psscan plugin scans raw memory to find **all process structures**, including **hidden or previously terminated processes** — even if they were not listed by normal tools like pslist.

I run this volatility plugin: python .\vol.py -f .\memdump2.mem windows.psscan

```

PS C:\Users\student\Downloads\volatility3-develop\volatility3-develop> python .\vol.py -f .\memdump2.mem windows.psscan
>>>
Volatility 3 Framework 2.26.2
Progress: 100.00
PID    PDB ImageFileName      PDB scanning finished      Threads Handles SessionId      Wow64      CreateTime      ExitTime      File output
PID   Offset(V)
1964   680 svchost.exe 0xb46fbd90000 5 - 0 False 2025-04-28 21:17:43.000000 UTC N/A Disabled
92     4 Registry 0xb46f5f10000 4 - 0 False 2025-04-28 21:17:20.000000 UTC N/A Disabled
1996   680 svchost.exe 0xb46f5f10000 5 - 0 False 2025-04-28 21:17:20.000000 UTC N/A Disabled
1956   680 svchost.exe 0xb46f5f760000 7 - 0 False 2025-04-28 21:17:43.000000 UTC N/A Disabled
2278   680 svchost.exe 0xb46f5f760000 7 - 0 False 2025-04-28 21:17:44.000000 UTC N/A Disabled
2704   4 MemCompression 0xb46f5f780040 26 - 0 N/A False 2025-04-28 21:17:46.000000 UTC N/A Disabled
2392   4 svchost.exe 0xb46f5f780040 2 - 0 N/A False 2025-04-28 21:17:46.000000 UTC N/A Disabled
168   4 smst.exe 0xb46fe86e000 2 - 0 N/A False 2025-04-28 21:17:34.000000 UTC N/A Disabled
748   680 dsm.exe 0xb46fe86f74000 17 - 1 False 2025-04-28 21:17:48.000000 UTC N/A Disabled
488   468 csrss.exe 0xb46ffed8b100 10 - 0 False 2025-04-28 21:17:37.000000 UTC N/A Disabled
322   488 csrss.exe 0xb46ffed8b100 10 - 0 False 2025-04-28 21:17:37.000000 UTC N/A Disabled
568   544 csrss.exe 0xb47000001200 13 - 1 False 2025-04-28 21:17:38.000000 UTC N/A Disabled
668   544 winlogon.exe 0xb4700005700 3 - 1 False 2025-04-28 21:17:38.000000 UTC N/A Disabled
2472   688 svchost.exe 0xb47000077000 5 - 0 False 2025-04-28 21:17:46.000000 UTC N/A Disabled
400   52 svchost.exe 0xb47000077000 5 - 0 False 2025-04-28 21:17:46.000000 UTC N/A Disabled
736   552 lsass.exe 0xb470001d0000 10 - 0 False 2025-04-28 21:17:38.000000 UTC N/A Disabled
849   688 svchost.exe 0xb4700020000 18 - 0 False 2025-04-28 21:17:39.000000 UTC N/A Disabled
868   552 fontdrvhost.exe 0xb47000251140 5 - 0 False 2025-04-28 21:17:39.000000 UTC N/A Disabled
869   500 svchost.exe 0xb47000251140 12 - 0 False 2025-04-28 21:17:39.000000 UTC N/A Disabled
964   680 csndrvhost.exe 0xb47000251140 5 - 1 False 2025-04-28 21:17:39.000000 UTC N/A Disabled
936   688 WUDHost.exe 0xb470002c000 7 - 0 False 2025-04-28 21:17:49.000000 UTC N/A Disabled
424   688 svchost.exe 0xb4700035200 5 - 0 False 2025-04-28 21:17:40.000000 UTC N/A Disabled
3088   688 svchost.exe 0xb4700035200 5 - 1 False 2025-04-28 21:17:40.000000 UTC N/A Disabled
1144   688 svchost.exe 0xb47000417000 2 - 0 False 2025-04-28 21:17:41.000000 UTC N/A Disabled
1136   688 svchost.exe 0xb47000419000 5 - 0 False 2025-04-28 21:17:41.000000 UTC N/A Disabled
1178   688 svchost.exe 0xb47000451000 3 - 0 False 2025-04-28 21:17:41.000000 UTC N/A Disabled
1260   688 svchost.exe 0xb47000451000 3 - 0 False 2025-04-28 21:17:41.000000 UTC N/A Disabled
1284   688 svchost.exe 0xb47000450000 4 - 0 False 2025-04-28 21:17:41.000000 UTC N/A Disabled
1344   688 svchost.exe 0xb47000450000 1 - 0 False 2025-04-28 21:17:41.000000 UTC N/A Disabled
1368   688 svchost.exe 0xb47000460000 3 - 0 False 2025-04-28 21:17:41.000000 UTC N/A Disabled
1432   688 svchost.exe 0xb4700052000 62 - 0 False 2025-04-28 21:17:42.000000 UTC N/A Disabled
1480   688 svchost.exe 0xb4700052000 6 - 0 False 2025-04-28 21:17:42.000000 UTC N/A Disabled
1508   688 svchost.exe 0xb4700059000 10 - 0 False 2025-04-28 21:17:42.000000 UTC N/A Disabled
1524   688 svchost.exe 0xb4700059000 2 - 0 False 2025-04-28 21:17:42.000000 UTC N/A Disabled
1545   688 svchost.exe 0xb4700059000 3 - 0 False 2025-04-28 21:17:42.000000 UTC N/A Disabled
1888   688 svchost.exe 0xb47000d1000 9 - 0 False 2025-04-28 21:17:43.000000 UTC N/A Disabled
1712   688 svchost.exe 0xb47000638000 8 - 0 False 2025-04-28 21:17:43.000000 UTC N/A Disabled
1792   688 svchost.exe 0xb47000654000 8 - 0 False 2025-04-28 21:17:43.000000 UTC N/A Disabled
1932   688 svchost.exe 0xb47000654000 8 - 0 False 2025-04-28 21:17:43.000000 UTC N/A Disabled
1664   688 svchost.exe 0xb47000802000 4 - 0 False 2025-04-28 21:17:46.000000 UTC N/A Disabled
2508   688 svchost.exe 0xb47000802000 3 - 0 False 2025-04-28 21:17:46.000000 UTC N/A Disabled
2376   688 svchost.exe 0xb47000826100 7 - 0 False 2025-04-28 21:17:46.000000 UTC N/A Disabled
2071   688 svchost.exe 0xb47000826100 7 - 0 False 2025-04-28 21:17:46.000000 UTC N/A Disabled
2640   688 svchost.exe 0xb47000875000 3 - 0 False 2025-04-28 21:17:46.000000 UTC N/A Disabled
2777   688 svchost.exe 0xb470008f0000 2 - 0 False 2025-04-28 21:17:46.000000 UTC N/A Disabled
2980   688 svchost.exe 0xb47000915000 9 - 0 False 2025-04-28 21:17:48.000000 UTC N/A Disabled
3000   688 svchost.exe 0xb47000915000 9 - 0 False 2025-04-28 21:17:48.000000 UTC N/A Disabled
2952   688 svchost.exe 0xb47000915000 1 - 0 False 2025-04-28 21:17:48.000000 UTC N/A Disabled
2960   688 svchost.exe 0xb47000a18000 2 - 0 False 2025-04-28 21:17:48.000000 UTC N/A Disabled
3036   688 svchost.exe 0xb47000a3b000 2 - 0 False 2025-04-28 21:17:48.000000 UTC N/A Disabled
3096   688 svchost.exe 0xb47000a3c000 10 - 0 False 2025-04-28 21:17:48.000000 UTC N/A Disabled

```

Figure 20 Volatility psscan plugin

```

Windows PowerShell
PS C:\Users\student\Downloads\volatility3-devel\volatility> psscan

```

Process Name	Paren t PID	Description	Executable Path / Command
smss.exe	4	Session Manager, starts system processes.	\Device\HarddiskVolume3\Windows\System32\smss.exe
csrss.exe / wininit.exe	284 / 468	Responsible for user session and system startup.	C:\Windows\System32\csrss.exe, wininit.exe
services.exe / lsass.exe	584 / 596	Run services and handle system security/login.	C:\Windows\System32\services.exe, lsass.exe

Figure 21 Volatility psscan plugin

Figure 22 Volatility psscan plugin artifacts

Process Name	Paren t PID	Description	Executable Path / Command
smss.exe	4	Session Manager, starts system processes.	\Device\HarddiskVolume3\Windows\System32\smss.exe
csrss.exe / wininit.exe	284 / 468	Responsible for user session and system startup.	C:\Windows\System32\csrss.exe, wininit.exe
services.exe / lsass.exe	584 / 596	Run services and handle system security/login.	C:\Windows\System32\services.exe, lsass.exe

<b>svchost.exe</b>	Multip le	Runs many built-in Windows services.	C:\Windows\System32\svchost.exe with various flags like -k, -s
<b>SecurityHealthSystr a.exe</b>	1316	Part of Windows Defender, shows icon in system tray.	C:\Windows\System32\SecurityHealthSystr a.exe
<b>SearchIndexer.exe</b>	5448	Indexes files so they can be searched faster.	C:\Windows\System32\SearchIndexer.exe
<b>taskhostw.exe</b>	1484	Runs background tasks and scheduled tasks.	C:\Windows\System32\taskhostw.exe
<b>dllhost.exe</b>	4732	Hosts DLL files used by other applications (COM surrogate).	C:\Windows\System32\dllhost.exe
<b>NiSvc.exe</b>	7896	Defender-related service for notifications.	C:\ProgramData\Microsoft\Windows Defender\Platform\NiSvc.exe
<b>explorer.exe</b>	1568	Windows desktop and start menu — user was actively	C:\Windows\explorer.exe

		using the GUI.	
<b>firefox.exe (Tor)</b>	2936	User launched Firefox from the Tor Browser folder — internet activity confirmed.	C:\Users\student\Desktop\Tor Browser\Browser\firefox.exe
<b>FTK Imager.exe</b>	4912	Forensic imaging tool — shows memory was dumped manually by the user.	C:\Program Files\AccessData\FTK Imager\FTK Imager.exe
<b>vmtoolsd.exe</b>	2788	Part of VMware tools — confirms system is running in a virtual machine.	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe

## Interpretation Notes

- The process tree looks normal and complete, showing that the system started properly with all Windows processes in place.

- The presence of explorer.exe, firefox.exe, and FTK Imager.exe shows that the **user was actively using the system**, browsing the internet (via Tor Browser) and capturing memory manually.
- Processes like SearchIndexer.exe and taskhostw.exe show that background tasks and file indexing were also running normally.
- Windows Defender was active**, as seen from processes like SecurityHealthSystray.exe and NiSvc.exe.
- The process tree shows **no suspicious processes**, and all process names, paths, and parent-child relationships appear **normal and clean**.
- The presence of vmtoolsd.exe confirms that this analysis was done inside a **virtual machine**

## DLLs and Handles

### The windows.dlllist Plugin

The dlllist plugin shows all the **DLL (Dynamic Link Library)** files loaded by each process it helps you see **what code is being used by running programs**.

I run this volatility plugin: `python .\vol.py -f \memdump2.mem windows.dlllist`

```

PS C:\Users\student\Downloads\volatility3-develop\volatility3-develop> python .\vol.py -f \memdump2.mem windows.dlllist
Volatility 3 Framework 2.26.2
Progress: 100.00
PID Process Base Size PDB Name Path Loadtime File output
560 smss.exe 0x7ff6c46b0000 0x2b000 smss.exe \SystemRoot\System32\smss.exe 2025-04-28 21:17:34.000000 UTC Disabled
560 smss.exe 0x7ff724790000 0x217000 ntdll.dll C:\Windows\SYSTEM32\ntdll.dll 2025-04-28 21:17:34.000000 UTC Disabled
400 csrss.exe 0x7ff724780000 0x217000 csrss.exe C:\Windows\SYSTEM32\csrss.exe 2025-04-28 21:17:37.000000 UTC Disabled
400 csrss.exe 0x7ff724790000 0x217000 ntdll.dll C:\Windows\SYSTEM32\ntdll.dll 2025-04-28 21:17:37.000000 UTC Disabled
400 csrss.exe 0x7ff7247e0000 0x190000 CSRSRV.dll C:\Windows\SYSTEM32\CSRSRV.dll 2025-04-28 21:17:37.000000 UTC Disabled
400 csrss.exe 0x7ff7247e0000 0x16000 basesrv.DLL C:\Windows\system32\basesrv.DLL 2025-04-28 21:17:37.000000 UTC Disabled
400 csrss.exe 0x7ff7247e0000 0x16000 cryptbase.dll C:\Windows\system32\cryptbase.dll 2025-04-28 21:17:37.000000 UTC Disabled
400 csrss.exe 0x7ff724b00000 0x3a5000 kernelbase.dll C:\Windows\SYSTEM32\kernelbase.dll 2025-04-28 21:17:37.000000 UTC Disabled
400 csrss.exe 0x7ff724b00000 0xc40000 kernel32.dll C:\Windows\SYSTEM32\kernel32.dll 2025-04-28 21:17:37.000000 UTC Disabled
400 csrss.exe 0x7ff724770000 0x23000 win32kext.dll C:\Windows\SYSTEM32\win32kext.dll 2025-04-28 21:17:37.000000 UTC Disabled
400 csrss.exe 0x7ff724770000 0x17000 win32k.dll C:\Windows\SYSTEM32\win32k.dll 2025-04-28 21:17:37.000000 UTC Disabled
400 csrss.exe 0x7ff724760000 0x29000 GDID32.dll C:\Windows\system32\GDID32.dll 2025-04-28 21:17:37.000000 UTC Disabled
400 csrss.exe 0x7ff724b00000 0x119000 gdi32full.dll C:\Windows\SYSTEM32\gdi32full.dll 2025-04-28 21:17:37.000000 UTC Disabled
400 csrss.exe 0x7ff725140000 0x94000 msvcv_win.dll C:\Windows\system32\msvcv_win.dll 2025-04-28 21:17:37.000000 UTC Disabled
400 csrss.exe 0x7ff725140000 0x16000 msvcv_common.dll C:\Windows\system32\msvcv_common.dll 2025-04-28 21:17:37.000000 UTC Disabled
400 csrss.exe 0x7ff726920000 0x1ae000 cryptbase.dll C:\Windows\system32\cryptbase.dll 2025-04-28 21:17:37.000000 UTC Disabled
400 csrss.exe 0x7ff726920000 0x1ae000 USER32.dll C:\Windows\system32\USER32.dll 2025-04-28 21:17:37.000000 UTC Disabled
400 csrss.exe 0x7ff724760000 0x3a5000 sssrvr.DLL C:\Windows\system32\ssssrvr.DLL 2025-04-28 21:17:38.000000 UTC Disabled
400 csrss.exe 0x7ff726130000 0xb1000 ADVAPI32.dll C:\Windows\system32\ADVAPI32.dll 2025-04-28 21:17:38.000000 UTC Disabled
400 csrss.exe 0x7ff727330000 0x17000 sechost.dll C:\Windows\SYSTEM32\sechost.dll 2025-04-28 21:17:38.000000 UTC Disabled
400 csrss.exe 0x7ff724440000 0x17000 RPCRT4.dll C:\Windows\system32\RPCRT4.dll 2025-04-28 21:17:38.000000 UTC Disabled
400 csrss.exe 0x7ff724440000 0x17000 servicing.dll C:\Windows\SYSTEM32\servicing.dll 2025-04-28 21:17:38.000000 UTC Disabled
400 csrss.exe 0x7ff724920000 0x7a0000 cryptbase.dll C:\Windows\SYSTEM32\cryptbase.dll 2025-04-28 21:17:38.000000 UTC Disabled
400 csrss.exe 0x7ff724920000 0x7a0000 cryptPrimitives.dll C:\Windows\SYSTEM32\cryptPrimitives.dll 2025-04-28 21:17:38.000000 UTC Disabled
552 wininit.exe 0x7ff724730000 0x200000 wininit.exe C:\Windows\system32\wininit.exe 2025-04-28 21:17:38.000000 UTC Disabled
552 wininit.exe 0x7ff724730000 0x16000 cryptbase.dll C:\Windows\SYSTEM32\cryptbase.dll 2025-04-28 21:17:38.000000 UTC Disabled
552 wininit.exe 0x7ff726430000 0x1ae000 KERNEL32.DLL C:\Windows\SYSTEM32\KERNEL32.DLL 2025-04-28 21:17:38.000000 UTC Disabled
552 wininit.exe 0x7ff726430000 0x1ae000 USER32.dll C:\Windows\SYSTEM32\USER32.dll 2025-04-28 21:17:38.000000 UTC Disabled
552 wininit.exe 0x7ff724b00000 0x3a5000 ucrtbase.dll C:\Windows\SYSTEM32\ucrtbase.dll 2025-04-28 21:17:38.000000 UTC Disabled
552 wininit.exe 0x7ff724b00000 0x3a5000 ucrtbase.dll C:\Windows\SYSTEM32\ucrtbase.dll 2025-04-28 21:17:38.000000 UTC Disabled
552 wininit.exe 0x7ff727330000 0x9a0000 sechost.dll C:\Windows\SYSTEM32\sechost.dll 2025-04-28 21:17:39.000000 UTC Disabled
552 wininit.exe 0x7ff727330000 0x16000 CRVPI32.dll C:\Windows\SYSTEM32\CRVPI32.dll 2025-04-28 21:17:39.000000 UTC Disabled
552 wininit.exe 0x7ff724730000 0x26000 profapi.dll C:\Windows\SYSTEM32\profapi.dll 2025-04-28 21:17:39.000000 UTC Disabled
552 wininit.exe 0x7ff724730000 0x26000 cryptui.dll C:\Windows\SYSTEM32\cryptui.dll 2025-04-28 21:17:39.000000 UTC Disabled
552 wininit.exe 0x7ff725450000 0x7a0000 msver.dll C:\Windows\SYSTEM32\msver.dll 2025-04-28 21:17:39.000000 UTC Disabled
552 wininit.exe 0x7ff726920000 0x1ae000 USER32.dll C:\Windows\system32\USER32.dll 2025-04-28 21:17:39.000000 UTC Disabled
552 wininit.exe 0x7ff724710000 0x200000 win32u.dll C:\Windows\SYSTEM32\win32u.dll 2025-04-28 21:17:39.000000 UTC Disabled
552 wininit.exe 0x7ff724710000 0x200000 win32kfull.dll C:\Windows\SYSTEM32\win32kfull.dll 2025-04-28 21:17:39.000000 UTC Disabled
552 wininit.exe 0x7ff724b00000 0x119000 gdi32full.dll C:\Windows\SYSTEM32\gdi32full.dll 2025-04-28 21:17:39.000000 UTC Disabled
552 wininit.exe 0x7ff725140000 0x94000 msvcv_win.dll C:\Windows\system32\msvcv_win.dll 2025-04-28 21:17:39.000000 UTC Disabled
552 wininit.exe 0x7ff726130000 0xb1000 ADVAPI32.dll C:\Windows\SYSTEM32\ADVAPI32.dll 2025-04-28 21:17:39.000000 UTC Disabled
552 wininit.exe 0x7ff724730000 0x17000 cryptbase.dll C:\Windows\SYSTEM32\cryptbase.dll 2025-04-28 21:17:39.000000 UTC Disabled
552 wininit.exe 0x7ff724730000 0x17000 cryptPrimitives.dll C:\Windows\SYSTEM32\cryptPrimitives.dll 2025-04-28 21:17:39.000000 UTC Disabled
552 wininit.exe 0x7ff723100000 0xa70000 firewallapi.dll C:\Windows\SYSTEM32\firewallapi.dll 2025-04-28 21:17:39.000000 UTC Disabled
552 wininit.exe 0x7ff723100000 0x460000福音.dll C:\Windows\SYSTEM32\福音.dll 2025-04-28 21:17:39.000000 UTC Disabled
552 wininit.exe 0x7ff724230000 0x690000 msasn1.dll C:\Windows\SYSTEM32\msasn1.dll 2025-04-28 21:17:40.000000 UTC Disabled
552 wininit.exe 0x7ff724230000 0x690000 msasn1ock.dll C:\Windows\SYSTEM32\msasn1ock.dll 2025-04-28 21:17:40.000000 UTC Disabled
560 csrss.exe 0x7ff7b80e0000 0x78000 csrss.exe C:\Windows\system32\csrss.exe 2025-04-28 21:17:39.000000 UTC Disabled

```

Figure 23 Volatility dlllist plugin

```

Windows Power Shell
Process          Loaded DLLs                               Path
smss.exe          smss.exe.ni.dll, ntdll.dll           C:\Windows\System32\smss.exe
csrss.exe         CSRSRV.dll, basesrv.dll, winsrv.dll, user32.dll, kernel32.dll   C:\Windows\System32\csrss.exe
wininit.exe       kernel32.dll, advapi32.dll, gdi32.dll, rpcrt4.dll, user32.dll   C:\Windows\System32\wininit.exe
vmtoolsd.exe     guestInfo.dll, vmstatsProvider.dll, libcrypto-3-x64.dll   C:\Program Files\VMware\VMware Tools\plugins
FTK Imager.exe   Qt5Core.dll, Qt5Gui.dll, ntdll.dll, KERNEL32.dll, ucrtbase.dll   C:\Program Files\AccessData\FTK Imager\

File: C:\Windows\Temp\student\Downloads\volatility3-develop\vol.py, line 11, in <module>
      volatility.cli.main()

```

Figure 24 Volatility dlllist plugin

Table 8 Volatility dllslist artifacts

Process	Loaded DLLs (Examples)	Path
smss.exe	smss.exe.ni.dll, ntdll.dll	C:\Windows\System32\smss.exe
csrss.exe	CSRSRV.dll, basesrv.dll, winsrv.dll, user32.dll, kernel32.dll	C:\Windows\System32\csrss.exe
wininit.exe	kernel32.dll, advapi32.dll, gdi32.dll, rpcrt4.dll, user32.dll	C:\Windows\System32\wininit.exe
vmtoolsd.exe	guestInfo.dll, vmstatsProvider.dll, libcrypto-3-x64.dll	C:\Program Files\VMware\VMware Tools\plugins
FTK Imager.exe	Qt5Core.dll, Qt5Gui.dll, ntdll.dll, KERNEL32.dll, ucrtbase.dll	C:\Program Files\AccessData\FTK Imager\

<b>firefox.exe</b>	xul.dll, nss3.dll, mozglue.dll, user32.dll, WS2_32.dll	C:\Users\student\Desktop\Tor Browser\Browser\firefox.exe
<b>MsMpEng.exe</b>	mpengine.dll, mpclient.dll, MpSvc.dll	C:\ProgramData\Microsoft\Windows Defender\
<b>SearchIndexer.exe</b>	searchutil.dll, mssprxy.dll, SearchFilterHost.dll	C:\Windows\System32\SearchIndexer.exe

## Interpretation Notes

- The DLL list shows that **every major Windows process** has **normal system DLLs loaded**, like kernel32.dll, user32.dll, and advapi32.dll. This means the system is **stable and unmodified**.
- firefox.exe is using **Mozilla and networking DLLs**, which confirms that the browser was used and internet communication likely occurred.
- FTK Imager.exe is loaded with **Qt libraries**, showing that the forensic imaging tool was actively being used by the user.
- MsMpEng.exe, the **Windows Defender engine**, is loaded with its protection modules (mpengine.dll, mpclient.dll) — this confirms **real-time antivirus protection** was running.
- **No unknown, injected, or suspicious DLLs** are observed, and all are loaded from **expected locations**, which suggests no signs of malware or tampering.

## The windows.handles Plugin

The handles plugin lists all **open handles** for each process — these are like **pointers to files, registry keys, threads, events, ports, and more** that the process is using.

I run this volatility plugin: python .\vol.py -f .\memdump2.mem windows.handles

```
PS C:\Users\student\Downloads\volatility3-develop\volatility3-develop> python .\vol.py -f .\memdump2.mem windows.handles
>>>
Volatility 3 Framework 2.26.2
Progress: 100.00          PDB scanning finished
PID  Process Offset HandleValue Type GrantedAccess Name
4   System 0xb406fb5b6040 0x4  Process 0xffffffff System Pid 4
4   System 0xd406fb5f35080 0x8  Thread 0xffffffff System Tid 4
4   System 0xa406fb5f35080 0x10  Event 0xffffffff 0x1fffff&0x1
4   System 0xa40c24428010 0x18  Directory 0xf000f CpuPartitions
4   System 0xa40c2442fa40 0x14  Directory 0xf000f GLOBAL?
4   System 0xa40c2442fa40 0x10  Partition 0x1ffff03 MemoryPartition0
4   System 0xa40c2442fa40 0x1c  Directory 0xf000f
4   System 0xa40c2442fa40 0x20  Directory 0xf000f KernelObjects
4   System 0xb406fb5b7040 0x24  Event 0xffffffff LowPagePoolCondition
4   System 0xb406fb5b7040 0x28  Event 0xffffffff HighPagePoolCondition
4   System 0xb406fb5b7040 0x2c  Event 0xffffffff LowMemoryPoolCondition
4   System 0xb406fb5b7040 0x34  Event 0xffffffff HighMemoryCondition
4   System 0xb406fb5b7040 0x38  Event 0xffffffff HighMemoryCondition
4   System 0xb406fb5b7040 0x3c  Event 0xffffffff LowMemoryCondition
4   System 0xb406fb5b7040 0x44  Event 0xffffffff MaximumCommitCondition
4   System 0xb406fb5b7040 0x48  Event 0xffffffff MemoryErrors
4   System 0xb406fb5b7040 0x4c  Event 0xffffffff PhysicalMemoryChange
4   System 0xb406fb5b7040 0x50  Event 0xffffffff RegistryValue92
4   System 0xb406fb5b7040 0x54  Thread 0xffffffff Tid 80 Pid 4
4   System 0xa40c24538070 0x58  Key 0x2001f MACHINE\SYSTEM\CONTROLSET001\CONTROL\HIVELIST
4   System 0xa40c24538070 0x5c  Process 0xffffffff smss.exe Pid 360
4   System 0xa40c24538070 0x60  Key 0x1fffff SYSTEM\SECURITY\SECURITY
4   System 0xa40c24538070 0x64  Key 0x11 MACHINE\SYSTEM\CONTROLSET001\CONTROL\POWER
4   System 0xa40c24538070 0x68  Key 0x20019 MACHINE\SYSTEM\CONTROLSET001\CONTROL\LEAPSECONFORMATION
4   System 0xa40c24538070 0x6c  Key 0x20015 MACHINE\SYSTEM\SETUP
4   System 0xa40c24538070 0x70  Key 0x20019 MACHINE\SYSTEM\CONTROLSET001\CONTROL\SESSIONMANAGERMEMORYMANAGEMENT\PREFETCHPARAMETERS
4   System 0xa40c24537400 0x74  Key 0x20019 MACHINE\SYSTEM\CONTROLSET001\CONTROL\NOTIFICATIONS
4   System 0xa40c244290d0 0x78  SymbolicLink 0x0f001 DriversStores
4   System 0xa40c244290d0 0x7c  Key 0x20019 MACHINE\SYSTEM\CONTROLSET001\CONTROL\POWERMONITORPORT
4   System 0xb406fb5b7040 0x80  ALPC Port 0xffffffff PowerMonitorPort
4   System 0xb406fb5b7040 0x84  IoCompletionReserve 0x0f003
4   System 0xb406fb5b7040 0x88  ALPC Port 0xffffffff SleepStudyControlPort
4   System 0xb406fb5b7040 0x8c  ALPC Port 0xffffffff PowerPort
4   System 0xa40c24545040 0x90  Key 0x0f003
4   System 0xa40c24545040 0x94  Key 0x0f003f MACHINE\SYSTEM\CONTROLSET001
4   System 0xa40c24543a20 0x98  Key 0x0f003f MACHINE\SYSTEM\ORIVEDATABASE
4   System 0xa40c24543a20 0x9c  Key 0x0f003f MACHINE\SYSTEM\ORIVEDATABASE
4   System 0xb406fb5b7040 0x98  Event 0xffffffff -
4   System 0xa40c24544a00 0x9c  Key 0x0f003f MACHINE\SYSTEM\CONTROLSET001\ENUM
4   System 0xa40c24545040 0x9d  Key 0x0f003f MACHINE\SYSTEM\CONTROLSET001\CONTROL\DEVICECLASSES
4   System 0xa40c24545040 0x9e  Key 0x0f003f MACHINE\SYSTEM\CONTROLSET001\CONTROL\DEVICECLASSES
4   System 0xa40c24545040 0x9f  Key 0x0f003f MACHINE\SYSTEM\CONTROLSET001\CONTROL\DEVICECONTAINERS
4   System 0xa40c24545020 0x94  Key 0x0f003f MACHINE\SYSTEM\CONTROLSET001\CONTROL\CLASS
4   System 0xa40c24545020 0x98  Key 0x0f003f MACHINE\SYSTEM\CONTROLSET001\CONTROL\DEVICEPANELS
4   System 0xa40c24545020 0x9c  Key 0x0f003f MACHINE\SYSTEM\CONTROLSET001\CONTROL\DRIVER
4   System 0xa40c2480e0c0 0x9c  Key 0x0f003f MACHINE\SYSTEM\CONTROLSET001\SERVICES
4   System 0xa40c2480e030 0x9c  Key 0x0f003f MACHINE\SYSTEM\HARDWARECONFIG
4   System 0xb406fb5f10e0 0x98  Event 0xffffffff HwMthdNotAllowed
4   System 0xb406fb5f10e0 0x9c  Event 0xffffffff HwMthdNotAllowed
4   System 0xb406fb5f10e0 0x9d  Thread 0xffffffff Tid 348 Pid 4
4   System 0xa40c2480b140 0xd4  SymbolicLink 0x0f001 API_HAL#MPICOB#0!{1c5e253-bbc4-452e-99df-461d0ff5078c8}
```

Figure 25 Volatility handles plugin

```
PS C:\Users\student\Downloads\volatility3-develop\volatility3-develop> python .\vol.py -f .\memdump2.mem windows.handles
>>>
Volatility 3 Framework 2.26.2
Progress: 100.00          PDB scanning finished
588 services.exe 0xb407000c38000 0x458  Process 0xffffffff svchost.exe Pid 1712
588 services.exe 0xb407000d0000 0x49c  Event 0x1ffff03 -
588 services.exe 0xa40c288705f0 0x4a0  Key 0x2001f USER\5-1-5-19
588 services.exe 0xb407004e6080 0x4a4  Process 0xffffffff 0x1ffff01 -
588 services.exe 0xb407004e6080 0x4a8  Thread 0xffffffff svchost.exe Pid 1368
588 services.exe 0xb407004e6080 0x4ac  Event 0xffffffff -
588 services.exe 0xb407004e6080 0x4b0  ALPC Port 0xffffffff -
588 services.exe 0xb407004e6080 0x4b4  WaitCompletionPacket 0x1 -
588 services.exe 0xb40700513500 0x4b8  WaitCompletionPacket 0x1 -
588 services.exe 0xb40700515040 0x4bc  WaitCompletionPacket 0x1 -
588 services.exe 0xb40700515040 0x4c0  ALPC Port 0xffffffff -
588 services.exe 0xb40c28d57730 0x4cc  Token 0x0f0ff -
588 services.exe 0xb407005920c 0x4cc  Process 0xffffffff svchost.exe Pid 1800
588 services.exe 0xb407005920c 0x4dc  ALPC Port 0xffffffff -
588 services.exe 0xb40700575000 0x4dc  Process 0xffffffff svchost.exe Pid 2276
588 services.exe 0xb40700575000 0x4d8  WaitCompletionPacket 0x1 -
588 services.exe 0xb40700595000 0x4dc  Process 0xffffffff svchost.exe Pid 1508
588 services.exe 0xb406ffef4d700 0x4ec  ALPC Port 0xffffffff -
588 services.exe 0xb40700833100 0x4f0  Event 0x1ffff03 -
588 services.exe 0xb40700833100 0x4fc  Event 0x1ffff03 -
588 services.exe 0xb40700833100 0x504  Process 0xffffffff svchost.exe Pid 1524
588 services.exe 0xb40700833100 0x508  WaitCompletionPacket 0x1 -
588 services.exe 0xb40700515700 0x4fc  WaitCompletionPacket 0x1 -
588 services.exe 0xb40700570000 0x500  Process 0xffffffff svchost.exe Pid 1548
588 services.exe 0xb40700570000 0x504  WaitCompletionPacket 0x1 -
588 services.exe 0xb40700450000 0x508  Event 0x1ffff03 -
588 services.exe 0xb40700051000 0x508  ALPC Port 0xffffffff -
588 services.exe 0xb40700051000 0x512  Process 0xffffffff svchost.exe Pid 1792
588 services.exe 0xb40700051000 0x516  Thread 0xffffffff -
588 services.exe 0xb40700450000 0x518  ALPC Port 0xffffffff -
588 services.exe 0xa40c28b96050 0x518  Key 0x2001f USER\5-1-5-20
588 services.exe 0xb40700450000 0x520  Key 0x2001f USER\5-1-5-19
588 services.exe 0xb40c28d57730 0x524  Thread 0xffffffff -
588 services.exe 0xb40700450000 0x528  Key 0x2001f USER\5-1-5-19
588 services.exe 0xb40700450000 0x52c  WaitCompletionPacket 0x1 -
588 services.exe 0xb40700450000 0x530  Token 0x0f0ff -
588 services.exe 0xb40700450000 0x534  Process 0xffffffff svchost.exe Pid 1888
588 services.exe 0xb40700450000 0x538  ALPC Port 0xffffffff -
588 services.exe 0xb40700450000 0x540  Event 0x1ffff01 -
588 services.exe 0xb40700450000 0x544  Event 0x1ffff01 -
588 services.exe 0xb40700450000 0x548  Token 0x0f0ff -
588 services.exe 0xb40700450000 0x552  Process 0xffffffff svchost.exe Pid 1912
588 services.exe 0xb40700450000 0x556  Thread 0xffffffff -
588 services.exe 0xb40700450000 0x560  Key 0x2001f USER\5-1-5-19
588 services.exe 0xb40700450000 0x564  WaitCompletionPacket 0x1 -
588 services.exe 0xb40700450000 0x568  ALPC Port 0xffffffff -
588 services.exe 0xb40700532400 0x568  WaitCompletionPacket 0x1 -
588 services.exe 0xb40700532400 0x572  Process 0x20010 MACHINE\SYSTEM\CONTROLSET001\SERVICES\SAMSS
588 services.exe 0xb40700532400 0x574  Token 0x0f0ff -
588 services.exe 0xa40c28bedf0 0x578  Key 0x2001f USER\5-1-5-19
```

Figure 2c Volatility handles plugin

```

000 services.exe 0xb40700ab2580 0x6ec ALPC Port 0x1f0001 -
000 services.exe 0xb4070091d150 0x6f0 WaitCompletionPacket 0x1 -
000 services.exe 0xa40c298c9b50 0x6f4 Key 0xf003f MACHINE\SYSTEM\CONTROLSET001\SERVICES\WINSOCK2\PARAMETERS\NAMESPACE_CATALOGS
000 services.exe 0xb4070084e600 0x6f8 Process 0xfffff svchost.exe Pid 2966
000 services.exe 0xb4070084e600 0x700 Event 0x1f0003 -
000 services.exe 0xb4070084e600 0x704 ALPC Port 0x1f0001 -
000 services.exe 0xb4070084e600 0x710 WaitCompletionPacket 0x1 -
000 services.exe 0xb4070084e600 0x714 Event 0x1f0003 -
000 services.exe 0xb4070084e600 0x718 ALPC Port 0x1f0001 -
000 services.exe 0xb4070084e600 0x71c WaitCompletionPacket 0x1 -
000 services.exe 0xb4070084e600 0x724 ALPC Port 0x1f0001 -
000 services.exe 0xb4070084e600 0x728 ALPC Port 0x1f0001 -
000 services.exe 0xb4070084e600 0x72c Event 0x1f0003 -
000 services.exe 0xb4070084e600 0x730 WaitCompletionPacket 0x1 -
000 services.exe 0xb4070084e600 0x734 Process 0xfffff svchost.exe Pid 3096
000 services.exe 0xb4070084e600 0x740 Process 0xfffff svchost.exe Pid 3096
000 services.exe 0xb4070084e600 0x744 Event 0x1f0003 -
000 services.exe 0xb4070084e600 0x748 Token 0x0fffff 0x1f0001 -
000 services.exe 0xa40c28ae0600 0x750 Token 0x0fffff 0x1f0001 -
000 services.exe 0xa40c29370590 0x754 Key 0x2001f USERIS-1-5-20
000 services.exe 0xb4070084e600 0x758 Event 0x1f0003 -
000 services.exe 0xb4070084e600 0x75c Event 0x1f0003 -
000 services.exe 0xb4070084e600 0x760 Process 0xfffff svchost.exe Pid 3176
000 services.exe 0xb4070084e600 0x764 ALPC Port 0x1f0001 -
000 services.exe 0xb4070084e600 0x768 Event 0x1f0003 -
000 services.exe 0xb4070084e600 0x772 Key 0xf003f svchost.exe Pid 4796
000 services.exe 0xb4070084e600 0x774 ALPC Port 0x1f0001 -
000 services.exe 0xb4070084e600 0x778 Event 0x1f0003 -
000 services.exe 0xb4070084e600 0x780 File 0x100001 \Device\HarddiskVolume3\Windows\System32\en-US\combase.dll.mui
000 services.exe 0xb4070084e600 0x784 Event 0x1f0003 -
000 services.exe 0xb4070084e600 0x788 Event 0x1f0003 -
000 services.exe 0xb4070084e600 0x792 Event 0x1f0003 -
000 services.exe 0xb4070084e600 0x796 Event 0x1f0003 -
000 services.exe 0xb4070084e600 0x79c Event 0x1f0003 -
000 services.exe 0xb4070084e600 0x7a0 WaitCompletionPacket 0x1 -
000 services.exe 0xb4070084e600 0x7a4 Event 0x1f0003 -
000 services.exe 0xb4070084e600 0x7a8 Event 0x1f0003 -
000 services.exe 0xb4070084e600 0x7ac Event 0x1f0003 -
000 services.exe 0xb4070084e600 0x7b0 Event 0x1f0003 -
000 services.exe 0xb4070084e600 0x7b4 Event 0x1f0003 -
000 services.exe 0xb4070084e600 0x7bc Event 0x1f0003 -
000 services.exe 0xb4070084e600 0x7c0 Event 0x1f0003 -
000 services.exe 0xb4070084e600 0x7c4 Key 0x2001f USERIS-1-5-20
000 services.exe 0xb4070084e600 0x7c8 Event 0x1f0003 -
000 services.exe 0xb4070084e600 0x7cc Token 0x0fffff 0x1f0001 -
000 services.exe 0xa40c2937e120 0x7d0 Key 0x2001f USERIS-1-5-19
000 services.exe 0xb4070124b00 0x7d4 ALPC Port 0x1f0001 -
000 services.exe 0xb4070084e600 0x7dc Event 0x1f0003 -
000 services.exe 0xb4070084e600 0x7e0 WaitCompletionPacket 0x1 -
000 services.exe 0xb4070084e600 0x7e4 Token 0x0fffff 0x1f0001 -
000 services.exe 0xb4070084e600 0x7e8 Process 0xfffff svchost.exe Pid 3332

```

Figure 27 Volatility handles plugin

Table S Volatility handles artifacts

Process	Type of Object / Description Handle
<b>System (PID 4)</b>	Key, Thread, Event, Port
	Access to critical system components like \Registry\Machine\SYSTEM, PowerPort, etc.
<b>services.exe (PID 600)</b>	Process
	Handles linked to various child processes, e.g., svchost.exe, spoolsv.exe, etc.
<b>services.exe</b>	ALPC Port
	Advanced Local Procedure Call ports — used for service communication.
<b>services.exe</b>	Registry Keys
	Handles to registry paths like SERVICES\SAMSS, PROTOCOL_CATALOG9, etc.
<b>services.exe</b>	Event / Mutant / Token
	Normal Windows service sync and permission-related handles.

<b>services.exe</b>	DLL Path	Refers to loaded file: \Device\HarddiskVolume3\...\combase.dll.mui — language UI file.
<b>spoolsv.exe</b>	Process	Shows that spooler service is active and being monitored.
<b>svchost.exe</b>	Multiple	Referenced in almost all system handles — hosting many Windows services.

## Interpretation Notes

- The system was running normally, with the System and services.exe processes holding many **key handles to threads, registry, ports, and services** — all expected for a Windows system.
- The presence of **ALPC ports, event, and mutant objects** under services.exe shows **inter-process communication** and system syncing, which is standard.
- Several handles point to **registry locations** like SERVICES\SAMSS and WINSOCK2\CATALOGS, confirming that **network services and security subsystems** were active.
- A handle to **combase.dll.mui** (Microsoft UI language component) shows legitimate use of Windows system libraries.
- Many svchost.exe and spoolsv.exe processes are shown as being **accessed and managed**, which confirms **system-level activity was normal**.
- There are **no signs of suspicious handles**, injected DLLs, or access to unusual files or registry entries.

## Registry

### The windows.registry.printkey Plugin

The printkey plugin shows the **contents of a specific Windows registry key** from memory this includes the **key name, subkeys, and values** stored inside it.



```

0925-04-26 16:57:00.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat .spl N/A False appinstaller.oauth2 N/A False
0925-04-26 16:58:53.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat Applications N/A False
0925-04-26 16:59:05.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserModelId N/A False
0925-04-26 17:13:16.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserModelName N/A False
0925-04-26 16:57:06.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserModelToken N/A False
0925-04-27 13:57:04.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64 N/A False
0925-04-26 16:57:08.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64Install N/A False
0925-04-26 17:13:46.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPath N/A False
0925-04-26 16:57:04.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathN N/A False
0925-04-26 17:13:17.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNN N/A False
0925-04-26 16:57:02.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNN N/A False
0925-04-26 16:57:02.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNNN N/A False
0925-04-26 16:57:04.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNNNN N/A False
0925-04-27 13:57:04.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNNNNN N/A False
0925-04-26 17:13:30.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNNNNNN N/A False
0925-04-26 16:57:06.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNNNNNNN N/A False
0925-04-26 16:57:04.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNNNNNNNN N/A False
0925-04-26 17:13:46.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNNNNNNNNN N/A False
0925-04-26 16:57:04.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNNNNNNNNNN N/A False
0925-04-26 17:13:45.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNNNNNNNNNNN N/A False
0925-04-26 16:58:47.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNNNNNNNNNNNN N/A False
0925-04-26 16:58:52.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNNNNNNNNNNNNN N/A False
0925-04-26 17:13:38.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNNNNNNNNNNNNNN N/A False
0925-04-27 13:57:04.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNNNNNNNNNNNNNNN N/A False
0925-04-26 16:57:47.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNNNNNNNNNNNNNNNN N/A False
0925-04-26 16:57:47.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNNNNNNNNNNNNNNNNN N/A False
0925-04-27 14:00:14.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNNNNNNNNNNNNNNNNNN N/A False
0925-04-26 16:57:04.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNNNNNNNNNNNNNNNNNNN N/A False
0925-04-26 16:58:47.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNNNNNNNNNNNNNNNNNNNN N/A False
0925-04-26 17:13:38.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNNNNNNNNNNNNNNNNNNNN N/A False
0925-04-26 16:57:08.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNNNNNNNNNNNNNNNNNNNNN N/A False
0925-04-26 17:13:19.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNNNNNNNNNNNNNNNNNNNNNN N/A False
0925-04-26 16:58:54.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNNNNNNNNNNNNNNNNNNNNNNN N/A False
0925-04-26 17:13:34.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNNNNNNNNNNNNNNNNNNNNNNNN N/A False
0925-04-26 16:57:04.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNNNNNNNNNNNNNNNNNNNNNNNNN N/A False
0925-04-26 16:58:47.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNNNNNNNNNNNNNNNNNNNNNNNNNN N/A False
0925-04-26 16:58:47.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNNNNNNNNNNNNNNNNNNNNNNNNNNN N/A False
0925-04-26 16:57:08.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNNNNNNNNNNNNNNNNNNNNNNNNNNN N/A False
0925-04-26 17:13:18.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNNNNNNNNNNNNNNNNNNNNNNNNNNN N/A False
0925-04-26 16:57:28.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNNNNNNNNNNNNNNNNNNNNNNNNNNN N/A False
0925-04-26 16:57:28.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64InstallPathNNNNNNNNNNNNNNNNNNNNNNNNNNNN N/A False
0925-04-26 16:57:00.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserX64Holographic N/A False
0925-04-26 16:57:14.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat AppUserVideo N/A False
0925-04-26 16:57:03.000000 UTC 0xa40c2a0e3000 Key \?C:\Users\student\AppData\Local\Microsoft\Windows\UsrClass.dat ms-aad-brokerplugin N/A False

```

Figure 30 Volatility windows.registry.printkey plugin 3

Table 10 Volatility windows.registry.printkey plugin artifacts

Key Path	What It Means	Why It's Important
<b>SYSTEM\Setup</b>	Tells us how the system was set up	Shows if the system was in a special mode like test or setup
<b>W32Time</b>	Windows Time Service	Used to keep system time correct – time changes can hide hacker actions
<b>Tcpip</b>	Network settings	Shows how the system connects to the internet or network
<b>USBSTOR</b>	USB storage settings	Shows if USB drives are allowed or blocked – helps track USB use
<b>LanmanWorkstation</b>	File sharing service	Can be used by attackers to move files or spread malware
<b>MountedDevices</b>	Shows which drives were plugged in	Helps find USBs or external devices that were used

Table 11 Volatility windows.registry.printkey artifacts 2

Key Path	What It Means	Why It's Important
<b>LocalService, NetworkService</b>	Special Windows accounts	Used to run background system services
<b>AppRepository\Packages</b>	App installation records	Shows which apps were installed – malware can hide here
<b>SYSTEM\Select</b>	Boot config settings	Can show changes to startup settings – attackers may change it

Table 12 Volatility windows.registry.printkey artifacts 3

Key Path	What It Means	Why It's Important
<b>UsrClass.dat</b>	User activity data	Shows which apps and files were opened by the user
<b>File types like .mp4, .jpg, .cur</b>	File types used	Tells what kind of files the user worked with (images, videos, etc.)
<b>AppX entries</b>	Modern app packages	Some apps may be suspicious or fake (used by hackers)
<b>MicrosoftEdge, aad-BrokerPlugin</b>	Browser & Microsoft login info	Shows browsing activity and Microsoft account use (e.g., for school or work)

## Interpretation Notes

**System Boot Looks Clean:** No signs of setup or test mode – system booted normally.

**USB Activity Found:** USBs were connected. Can help investigate file copying or data theft.

**Network Services Active:** System was connected to network/internet.

**User Was Active:** User used apps, opened files, and browsed internet.

**App Installs Detected:** Many apps were installed. Some might need checking to ensure they're safe.

*Table 13 Summary*

Area	What We Saw	Should You Worry?	What To Do
<b>USB Devices</b>	USBSTOR and MountedDevices present	Medium	Check if any unknown USB was used
<b>Internet &amp; Network</b>	Valid keys for networking and time	Low	Confirm no weird DNS or time change
<b>App Installs</b>	AppX and Edge data found	Medium	Look for fake or unknown apps
<b>User Activity</b>	UsrClass.dat shows files and apps used	Low	Use to build timeline of what happened
<b>Boot Info</b>	System booted normally	Low	Just confirm no tampering

## The Windows Registry hives plugin

The hivelist plugin shows all the **Windows Registry hives** found in memory — these are important files that store system, user, and app settings.

I run this volatility plugin: `python .\vol.py -f .\memdump2.mem windows.registry.hivelist`

```

PS C:\Users\student\Downloads\volatility3-develop\volatility3-develop> python .\vol.py -f .\memdump2.mem windows.registry.hivelist
Volatility Framework 3.2.6.2
Progress: 100.00% PDB scanning finished
Offset FileFullPath File output
0x40c24426000 \REGISTRY\MACHINE\SYSTEM Disabled
0x40c24426000 \REGISTRY\MACHINE\SYSTEM Disabled
0x40c24426000 \REGISTRY\MACHINE\SYSTEM Disabled
0x40c24426000 \SystemRoot\System32\Config\SECURITY Disabled
0x40c271a0e00 \SystemRoot\System32\Config\DEFAULT Disabled
0x40c271a0e00 \SystemRoot\System32\Config\SAM Disabled
0x40c271a0e00 \SystemRoot\System32\Config\LOGONMAN Disabled
0x40c271a0e00 \SystemRoot\System32\Config\LOGONMAN Disabled
0x40c28613000 !?\?C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT Disabled
0x40c28803000 !?\?C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT Disabled
0x40c2a0e00 \SystemRoot\System32\UsrClass.dat Disabled
0x40c2a0e00 !?\?C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Client.FileExp_1000_22651_1000_0_x64_cw5nh2txyew\ActivationStore.dat Disabled
0x40c2a0e00 !?\?C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Client.Core_1000_22643_1000_0_x64_cw5nh2txyew\ActivationStore.dat Disabled
0x40c2a0e00 !?\?C:\Users\student\user.dat Disabled
0x40c2a0e00 !?\?C:\ProgramData\Microsoft\Windows\UsrClass.dat Disabled
0x40c2a0e00 !?\?C:\ProgramData\Microsoft\Windows\UsrClass\Amcache.hve Disabled
0x40c2a0e00 !?\?C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Client.CBS_1000_22677_1000_0_x64_cw5nh2txyew\ActivationStore.dat Disabled
0x40c2a0e00 !?\?C:\ProgramData\Microsoft\Windows\StartMenu\ExperienceHost_10_0_22621_2506_neutral_neutral_cw5nh2txyew\ActivationStore.dat Disabled
0x40c2a0e00 !?\?C:\ProgramData\Microsoft\Windows\StartMenu\ExperienceHost_10_0_22621_2506_neutral_neutral_cw5nh2txyew\Settings\ValueIndex.dat Disabled
0x40c2a0e00 !?\?C:\ProgramData\Microsoft\Windows\StartMenu\ExperienceHost_10_0_22621_2506_neutral_neutral_cw5nh2txyew\Settings\ValueIndex_105_0_x64_cw5nh2txyew\ActivationStore.dat Disabled
0x40c2a0e00 !?\?C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Client.WebXperience_cw5nh2txyew\ActivationStore.dat Disabled
0x40c2a0e00 !?\?C:\ProgramData\Microsoft\Windows\UI_Xaml_CBS_8_2305_1000_0_x64_Bmekyld3db0bwe\ActivationStore.dat Disabled
0x40c2a0e00 !?\?C:\ProgramData\Microsoft\Windows\Client.WebXperience_cw5nh2txyew\S-1-5-21-496136692-271927161_3940787789_1001\SystemAppData\Helium\Cache\ebb45e04fb183500.dat Disabled
0x40c2a0e00 !?\?C:\ProgramData\Microsoft\Windows\Client.WebXperience_cw5nh2txyew\S-1-5-21-496136692-271927161_3940787789_1001\SystemAppData\Helium\Cache\ebb45e04fb183500_COM15.dat Disabled
0x40c2a0e00 !?\?C:\ProgramData\Microsoft\Windows\Client.WebXperience_cw5nh2txyew\S-1-5-21-496136692-271927161_3940787789_1001\SystemAppData\Helium\Cache\ebb45e04fb183500_dat Disabled
0x40c2a0e00 !?\?C:\ProgramData\Microsoft\Windows\Background_CBS_4000_1027_2341_0_x64_Bmekyld3db0bwe\ActivationStore.dat Disabled
0x40c2a0e00 !?\?C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.DeliveryOptimizationState\dosvcState.dat Disabled
0x40c2a0e00 !?\?C:\Windows\ServiceProfile\NetworkService\ApdData\local\Microsoft.Windows.ShellExperienceHost_10_0_22621_2506_neutral_neutral_cw5nh2txyew\ActivationStore.dat Disabled
0x40c2a0e00 !?\?C:\ProgramData\Microsoft\Windows\DeliveryOptimizationState\dosvcState.dat Disabled
PS C:\Users\student\Downloads\volatility3-develop\volatility3-develop>

```

Figure 31 Volatility windows.registry.hivelist plugin

Table 14 Volatility windows.registry.hivelist plugin artifacts

Hive / File	What It Is	Why It's Important
\REGISTRY\MACHINE\SYSTEM	System settings	Stores driver info, services, and boot data
\REGISTRY\MACHINE\SOFTWARE	Software settings	Lists installed software and configuration
\REGISTRY\MACHINE\SECURITY	Security policies	Shows local security settings (accounts, groups)
\REGISTRY\MACHINE\SAM	User account data	Holds usernames and password hashes (very sensitive)
\Device\HarddiskVolumeX\...NTUSER.DAT	User registry file	Stores user activity like apps used, files opened, etc.
UsrClass.dat	GUI and shell settings	Shows which programs and file types were used
AppRepository\Packages	Windows Store app data	Shows which UWP apps are installed

<b>ActivationStore.dat</b>	Activation records	Tells if the apps are activated and legit
<b>Cache\WebCacheV01.dat</b>	Browser cache	Stores visited websites and browsing info (Edge/Internet Explorer)

### Interpretation Note

**System registry hives** (SYSTEM, SOFTWARE, SAM, SECURITY) were present this is good, we can extract a lot of forensic data from them.

**User hives** (NTUSER.DAT, UsrClass.dat) also present these tell us what the user was doing.

**App data and browser cache** were found useful for knowing what apps were used and websites were visited.

**All hives marked as “Disabled”** just means they weren’t actively in use during memory capture, **no sign of tampering**.

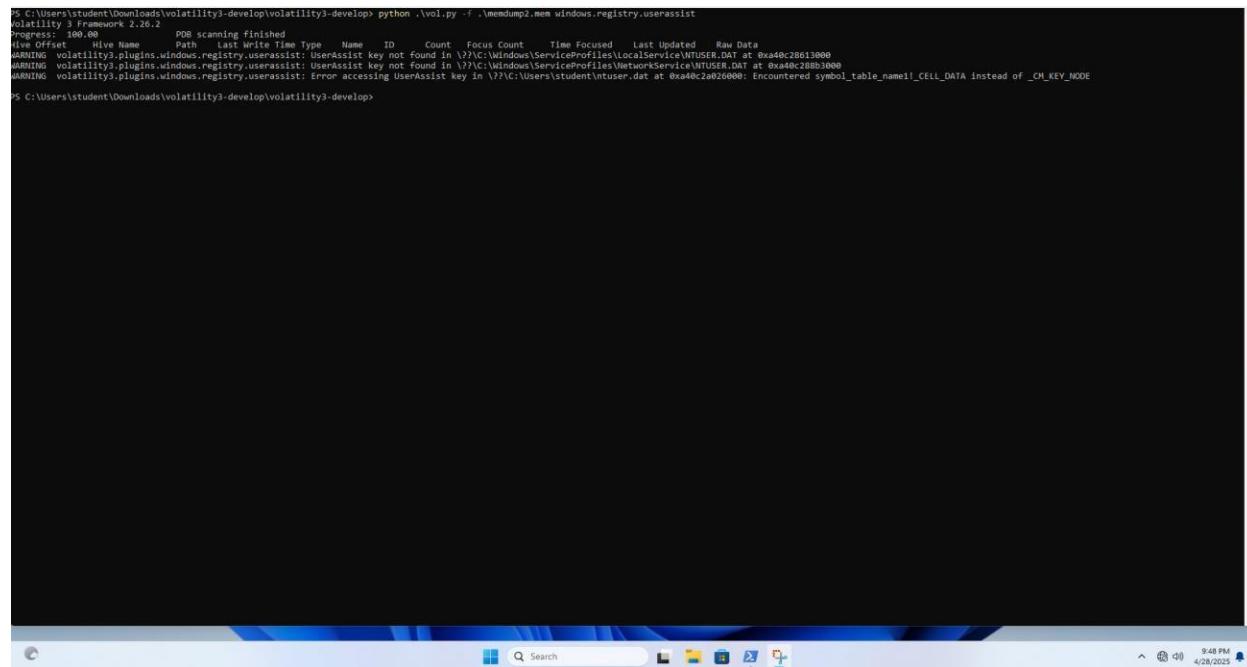
*Table 15 Summary*

Category	Found?	Why It Matters
<b>System settings</b>	SYSTEM, SOFTWARE	Driver, service, and software info
<b>User activity</b>	NTUSER.DAT, UsrClass.dat	File, app, and desktop usage
<b>App installs</b>	AppRepository	Shows installed UWP apps
<b>Browser history</b>	WebCacheV01.dat	Web usage, site visits
<b>Security/account data</b>	SAM, SECURITY	User accounts, policies
<b>Hive Status</b>	Disabled	Normal – not being used when memory was captured

## The windows.registry.userassist Plugin

The userassist plugin shows a list of **programs and files that the user interacted with through the GUI (like clicking icons or opening apps)**. This data comes from the **UserAssist registry key**, which stores usage details in a hidden/encoded format.

I run this volatility plugin: `python .\vol.py -f .\memdump2.mem windows.registry.userassist`



```
PS C:\Users\student\Downloads\volatility3-develop\volatility3-develop> python .\vol.py -f .\memdump2.mem windows.registry.userassist
Volatility 3 Framework 2.26.2
Progress: 100.00%    PDB scanning finished
Hive:          Hive Name      Path      Last Write Time Type   Name     ID   Count  Focus Count  Time Focused  Last Updated  Raw Data
WARNING: volatility3.plugins.windows.registry.userassist: UserAssist key not found in \?\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT at 0xa40c28613000
WARNING: volatility3.plugins.windows.registry.userassist: UserAssist key not found in \?\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT at 0xa40c288b3000
WARNING: volatility3.plugins.windows.registry.userassist: Error accessing UserAssist key in \?\C:\Users\student\ntuser.dat at 0xa00c2a026000: Encountered symbol_table_name!_CELL_DATA instead of _CH_KEY_NODE
PS C:\Users\student\Downloads\volatility3-develop\volatility3-develop>
```

Figure 32 Volatility windows.registry.userassist

Table 1c Volatility windows.registry.userassist plugin artifacts

Artifact / Hive Path	Description	Status / Result
C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT	UserAssist key in LocalService profile	Not found
C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT	UserAssist key in NetworkService profile	Not found
C:\Users\student\ntuser.dat	UserAssist key for actual logged-in user	Failed to access wrong

		symbol structure
<b>_CELL_DATA instead of _CM_KEY_NODE</b>	Memory parsing issue	Plugin failed to interpret registry key
<b>Focus Count, Last Updated, Raw Data</b>	Normally shows user GUI activity	No data returned

## Interpretation Notes

- The plugin **couldn't extract UserAssist data** due to format or memory issues.
- This doesn't mean the user didn't open any apps — just that **Volatility couldn't read the data** from the memory dump.
- You can still try tools like **RegRipper** or **RECcmd** on the extracted NTUSER.DAT file to view the same info.
- The error shows Volatility expected a certain **registry structure**, but **found something else**, likely due to:
  - New Windows version (structure changed)
  - Damaged registry hive
  - Memory capture issues

## Malware Detection

### The windows.malfind Plugin

The malfind plugin looks for **suspicious code or hidden malware** injected into the memory of running processes — especially useful for finding **code injections, shellcode, and memory-resident malware**.

I run this volatility plugin: `python .\vol.py -f .\memdump2.mem windows.malfind`



Table 17 Volatility windows.malfind plugin artifacts

Process Name	PID	Start - End Memory Address	Protection	Memo ry Type	Suspicio us?	Notes
MsMpEng.e xe (Windows Defender)	348 8	Multiple addresses (e.g., 0x1b8bc6a0 000)	PAGE_EXECUTE_READWRITE	VADs	Highly suspicious	Defender normally doesn't use this type of memory
SearchHost.exe	580 0	0x2d88a132 0000 → 0x2d88a133 efff	PAGE_EXECUTE_READWRITE	VADs	Suspicious	Could be shellcode
SearchHCI.exe	580 0	Multiple memory blocks	PAGE_EXECUTE_READWRITE	VADs	Suspicious	Contains long sequences of cc and jump instructions
Hex Dump	All above	Starts with cc cc cc... then e9 db... (JMP)	Executable memory	Typical shellcode behavior	Could be part of injected malware or loader	

## Interpretation Notes

**MsMpEng.exe (Defender)**: Normally safe, but multiple memory blocks with PAGE\_EXECUTE\_READWRITE protection and suspicious shellcode-like patterns could mean:

- **Malware is injecting code into Defender** to avoid detection
- **OR Defender is analyzing/containing malware** in memory needs further check

## SearchHost.exe and SearchHCI.exe:

- Contain **jump instructions (e9 ...)** and large blocks of cc cc cc bytes (padding or overwritten memory)
- This strongly points to **code injection or shellcode**

**PAGE\_EXECUTE\_READWRITE**: This memory permission is **very unusual for clean processes**. It allows code to be written and executed perfect for malware.

**No file output**: Means the plugin didn't automatically dump the memory contents to a file you can manually extract those pages if needed.

## The windows.ssdt Plugin

The ssdt plugin shows the **System Service Descriptor Table (SSDT)** a list of **system calls (kernel functions)** used by Windows to handle low-level operations like reading files, creating processes, and accessing memory.

I run this volatility plugin: `python .\vol.py -f .\memdump2.mem windows.ssdt`

```

5 C:\Users\student\Downloads\volatility3-develop\volatility3-develop> python .\vol.py -f .\Memdump2.mem windows.ssdt
volatility: 3 Framework 2.26.2
Progress: 100.00          PDB scanning finished
Index  Address Module Symbol
1   0x0f80408885810 ntoskrnl  NtAccessCheck
2   0x0f80408951020 ntoskrnl  NtWorkerFactoryWorkerReady
3   0x0f80408d61b50 ntoskrnl  NtAcceptConnectPort
4   0x0f80408d61c50 ntoskrnl  NtAllocateVirtualMemory
5   0x0f80408d3f6e0 ntoskrnl  NtWaitForSingleObject
6   0x0f80408a1b500 ntoskrnl  NtCallbackReturn
7   0x0f80408d82300 ntoskrnl  NtReadFile
8   0x0f80408d21140 ntoskrnl  NtReadFileControlFile
9   0x0f80408d20600 ntoskrnl  NtWriteFile
10  0x0f80408d2f540 ntoskrnl  NtRemoveIoCompletion
11  0x0f80408d4c900 ntoskrnl  NtReleaseSemaphore
12  0x0f80408d2f2e0 ntoskrnl  NtReplyWaitReceivePort
13  0x0f80408d68d6c ntoskrnl  NtSetInformationThread
14  0x0f80408d92320 ntoskrnl  NtSetEvent
15  0x0f80408d41000 ntoskrnl  NtClose
16  0x0f80408d5d610 ntoskrnl  NtQueryObject
17  0x0f80408d5a910 ntoskrnl  NtQueryInformationFile
18  0x0f80408d5a910 ntoskrnl  NtOpenKey
19  0x0f80408d21b00 ntoskrnl  NtOpenValueKey
20  0x0f80408d5b590 ntoskrnl  NtFindAtom
21  0x0f80408d70600 ntoskrnl  NtQueryDefaultLocale
22  0x0f80408d5a910 ntoskrnl  NtQueryPerformanceCounter
23  0x0f80408d5d610 ntoskrnl  NtQueryValueKey
24  0x0f80408d5a8910 ntoskrnl  NtAllocateVirtualMemory
25  0x0f80408d5d610 ntoskrnl  NtQueryInformationProcess
26  0x0f80408d5d610 ntoskrnl  NtQueryObject
27  0x0f80408d5d610 ntoskrnl  NtWriteFileGather
28  0x0f80408d8c7350 ntoskrnl  NtSetInformationProcess
29  0x0f80408d5d610 ntoskrnl  NtCreateKey
30  0x0f80408d5d610 ntoskrnl  NtDeleteValueKey
31  0x0f80408d765a0 ntoskrnl  NtImpersonateClientOfPort
32  0x0f80408d5a910 ntoskrnl  NtReleaseMutant
33  0x0f80408d5d610 ntoskrnl  NtQueryInformationToken
34  0x0f80408d2f2e0 ntoskrnl  NtReplyWaitReceivePortEx
35  0x0f80408d68d6c ntoskrnl  NtTerminateProcess
36  0x0f80408d69d60 ntoskrnl  NtQueryVirtualMemory
37  0x0f80408d9f900 ntoskrnl  NtOpenThreadToken
38  0x0f80408d70600 ntoskrnl  NtQueryInformationThread
39  0x0f80408d5d610 ntoskrnl  NtMapViewOfFile
40  0x0f80408d5c340 ntoskrnl  NtSetInformationSection
41  0x0f80408d5d610 ntoskrnl  NtUnmapViewOfFile
42  0x0f80408d5d610 ntoskrnl  NtAcquireExclusiveResource
43  0x0f80408d2f420 ntoskrnl  NtReplyWaitReceivePortEx
44  0x0f80408d21c10 ntoskrnl  NtTerminateProcess
45  0x0f80408d5d610 ntoskrnl  NtWaitForSectionExclusivePriority
46  0x0f80408d5d610 ntoskrnl  NtReadFileScatter
47  0x0f80408d5d610 ntoskrnl  NtOpenThreadTokenEx
48  0x0f80408d5d610 ntoskrnl  NtOpenProcessTokenEx
49  0x0f80408d5d610 ntoskrnl  NtQueryPerformanceCounter
50  0x0f80408d5d610 ntoskrnl  NtEnumerateKey
51  0x0f80408d5d610 ntoskrnl  NtOpenFile
52  0x0f80408d5d610 ntoskrnl  NtDelayExecution
53  0x0f80408d5d610 ntoskrnl  NtQueryDirectoryFile

```

Figure 35 Volatility windows.ssdt plugin

```

57  0x0f804088314e00 ntoskrnl  NtCancelTimer
58  0x0f804089a14a0 ntoskrnl  NtSetTimer
59  0x0f80408952a50 ntoskrnl  NtAccessCheckByType
60  0x0f80408855f50 ntoskrnl  NtAccessCheckByTypeResultList
61  0x0f80408d5d610 ntoskrnl  NtAccessCheckByTypeResultListAndAuditAlarm
62  0x0f80408d5d610 ntoskrnl  NtAccessCheckByTypeResultListAndAuditAlarmByHandle
63  0x0f80409003590 ntoskrnl  NtAcquireCrossVmMutant
64  0x0f80408d5d610 ntoskrnl  NtAcquireProcessActivityReference
65  0x0f80408d5d610 ntoskrnl  NtAddBootEntry
66  0x0f80408d5d610 ntoskrnl  NtAddDriveEntry
67  0x0f80408d5d610 ntoskrnl  NtAdjustGroupsToken
68  0x0f80408d5d610 ntoskrnl  KFDRIVELETTERNAMEW DISK@EAA1PEAXPEAPEX@Z
69  0x0f80408d5d610 ntoskrnl  NtAdjustTokenClaimAndDeviceGroups
70  0x0f80408d5d610 ntoskrnl  NtCreateEventPair
71  0x0f80408d5d610 ntoskrnl  NtDeleteEventPair
72  0x0f80408d5d610 ntoskrnl  NtFilterTokenEx
73  0x0f80408d5d610 ntoskrnl  NtOpenEventPair
74  0x0f80408d5d610 ntoskrnl  NtSetHighEventPair
75  0x0f80408d5d610 ntoskrnl  NtSetLowEventPair
76  0x0f80408d5d610 ntoskrnl  NtSetWaitHighEventPair
77  0x0f80408d5d610 ntoskrnl  NtSetWaitLowEventPair
78  0x0f80408d5d610 ntoskrnl  NtVmControl
79  0x0f80408d5d610 ntoskrnl  NtWaitHighEventPair
80  0x0f80408d5d610 ntoskrnl  NtWaitLowEventPair
81  0x0f80408d5d610 ntoskrnl  PsNotifyJobToExecutableMemory
82  0x0f80408d5d610 ntoskrnl  SeAdjustObjectSecurity
83  0x0f80408d5d610 ntoskrnl  XhalAllocatePages
84  0x0f80408d5d610 ntoskrnl  XhalLoadMicrocode
85  0x0f80408d5d610 ntoskrnl  XhalPostMicrocodeUpdate
86  0x0f80408d5d610 ntoskrnl  XhalUnloadMicrocode
87  0x0f80408d5d610 ntoskrnl  XhalWaitThread
88  0x0f80408d3e020 ntoskrnl  NtAlertThreadByThreadId
89  0x0f80408d74100 ntoskrnl  NtLocateLocallyUniqueId
90  0x0f80408d5d610 ntoskrnl  NtAllocateVirtualMemory
91  0x0f80409004000 ntoskrnl  NtAllocateUserPhysicalPages
92  0x0f80409004010 ntoskrnl  NtAllocateUserPhysicalPagesNx
93  0x0f80408d5d610 ntoskrnl  NtLocateVuids
94  0x0f80408d5d610 ntoskrnl  NtLocateVirtualMemoryNx
95  0x0f80408d2a6c0 ntoskrnl  NtAcceptConnectPort
96  0x0f80408d5d610 ntoskrnl  NtAcceptConnectPortEx
97  0x0f80408d5d610 ntoskrnl  NtAcceptConnectPortRx
98  0x0f80408d5d610 ntoskrnl  NtAcceptCreatePort
99  0x0f80408d16200 ntoskrnl  NtAcceptCreatePortSection
100 0x0f80408d5d610 ntoskrnl  NtAcceptCreateSectionReserve
101 0x0f80408d16420 ntoskrnl  NtAcceptCreateSectionView
102 0x0f80408d17290 ntoskrnl  NtAcceptCreateSecurityContext
103 0x0f80408d16190 ntoskrnl  NtAcceptDeletePortSection
104 0x0f80408d5d610 ntoskrnl  NtAcceptDeleteSection
105 0x0f80408d15f50 ntoskrnl  NtAcceptDeleteSectionView
106 0x0f80408d17090 ntoskrnl  NtAcceptDeleteSecurityContext
107 0x0f80408d5d610 ntoskrnl  NtAcceptDisconnectPort
108 0x0f80408d5d610 ntoskrnl  NtAcceptImpersonateClientContainerOfPort
109 0x0f80408d2c2f0 ntoskrnl  NtAcceptOpenSenderProcess
110 0x0f80408d5d610 ntoskrnl  NtAcceptOpenSenderThread
111 0x0f80408d5d610 ntoskrnl  NtAcceptQueryInformation

```

Figure 3c Volatility windows.ssdt plugin

```

179 0xf8048d8f6760 ntoskrnl NtDirectGraphicsCall
179 0xf8048d8f6760 ntoskrnl NtFilterTokenEx
179 0xf8048d8f6760 ntoskrnl NtOpenEventPair
179 0xf8048d8f6760 ntoskrnl NtSetHighEventPair
179 0xf8048d8f6760 ntoskrnl NtSetLowEventPair
179 0xf8048d8f6760 ntoskrnl NtSetLowWithHighEventPair
179 0xf8048d8f6760 ntoskrnl NtVmControl
179 0xf8048d8f6760 ntoskrnl NtWaitForEventPair
179 0xf8048d8f6760 ntoskrnl NtWaitForEventPair
179 0xf8048d8f6760 ntoskrnl PsNotifyWriteToExecutableMemory
179 0xf8048d8f6760 ntoskrnl SeAdjustObjectSecurity
179 0xf8048d8f6760 ntoskrnl xHalLoadMicrocode
179 0xf8048d8f6760 ntoskrnl xHalPostMicrocodeUpdate
179 0xf8048d8f6760 ntoskrnl xHalReadMicrocode
180 0xf8048d8f6728 ntoskrnl NtWaitForThreadId
181 0xf8048d8f6f728 ntoskrnl NtWaitForDebugEvent
182 0xf8048d8f6250 ntoskrnl NtWaitForKeyedEvent
183 0xf8048d8f6250 ntoskrnl NtWaitForWorkViaWorkerFactory
184 0xf8048d8f6250 ntoskrnl PsNotifyWriteToDisk@0EAA3PEAXPEAPEAX@Z
184 0xf8048d8f6760 ntoskrnl NtAdjustTokenClaimsAndDeviceGroups
184 0xf8048d8f6760 ntoskrnl NtCreateEventPair
184 0xf8048d8f6760 ntoskrnl NtDirectGraphicsCall
184 0xf8048d8f6760 ntoskrnl NtFilterTokenEx
184 0xf8048d8f6760 ntoskrnl NtOpenEventPair
184 0xf8048d8f6760 ntoskrnl NtSetHighEventPair
184 0xf8048d8f6760 ntoskrnl NtSetLowEventPair
184 0xf8048d8f6760 ntoskrnl NtSetLowWithHighEventPair
184 0xf8048d8f6760 ntoskrnl NtVmControl
184 0xf8048d8f6760 ntoskrnl NtWaitForEventPair
184 0xf8048d8f6760 ntoskrnl NtWaitForEventPair
184 0xf8048d8f6760 ntoskrnl PsNotifyWriteToExecutableMemory
184 0xf8048d8f6760 ntoskrnl SeAdjustObjectSecurity
184 0xf8048d8f6760 ntoskrnl xHalLoadMicrocode
184 0xf8048d8f6760 ntoskrnl xHalPostMicrocodeUpdate
184 0xf8048d8f6760 ntoskrnl xHalReadMicrocode
185 0xf8048d8f6760 ntoskrnl PsNotifyWriteToDisk@0EAA3PEAXPEAPEAX@Z
185 0xf8048d8f6760 ntoskrnl NtAdjustTokenClaimsAndDeviceGroups
185 0xf8048d8f6760 ntoskrnl NtCreateEventPair
185 0xf8048d8f6760 ntoskrnl NtDirectGraphicsCall
185 0xf8048d8f6760 ntoskrnl NtFilterTokenEx
185 0xf8048d8f6760 ntoskrnl NtOpenEventPair
185 0xf8048d8f6760 ntoskrnl NtSetHighEventPair
185 0xf8048d8f6760 ntoskrnl NtSetLowEventPair
185 0xf8048d8f6760 ntoskrnl NtSetLowWithHighEventPair
185 0xf8048d8f6760 ntoskrnl NtVmControl
185 0xf8048d8f6760 ntoskrnl NtWaitForEventPair
185 0xf8048d8f6760 ntoskrnl PsNotifyWriteToExecutableMemory
185 0xf8048d8f6760 ntoskrnl SeAdjustObjectSecurity
185 0xf8048d8f6760 ntoskrnl xHalLoadMicrocode
185 0xf8048d8f6760 ntoskrnl xHalPostMicrocodeUpdate
185 0xf8048d8f6760 ntoskrnl xHalUnloadMicrocode
185 0xf8048d8f6760 ntoskrnl xHalUnloadMicrocode
$ C:\Users\student\Downloads\volatility3-develop\volatility3-develop>

```

Figure 37 Volatility windows.ssdt plugin

Table 18 Volatility windows.ssdt plugin artifacts

Index	Function Name	Module	Memory Address	Comment
0–136	Multiple like NtReadFile, NtOpenProcess, NtQueryInfo, etc.	ntoskrnl	All valid kernel addresses	All appear to be standard Windows kernel system calls
137–485	Many repeat entries like NtCreateEventPair, NtOpenThread, xHal functions	ntoskrnl	All return same address 0xf8048d8f6760	<b>Suspicious</b> – multiple entries mapped to same address repeatedly

## Interpretation Notes

- **Early entries look normal:** Common Windows system calls like NtReadFile, NtOpenProcess, and others are pointing to ntoskrnl, which is expected.
- **Suspicious Behavior Detected:**
  - Many later functions (over 100+) point to the **same memory address** 0xf8048d8f6760

- Repeated function names like NtCreateEventPair, NtWaitForSingleObject, etc.
- This behavior suggests **potential SSDT hooking** often used by **rootkits or stealthy malware** to:
  - Hijack system calls
  - Hide files/processes from forensic tools
  - Bypass antivirus

## The windows.modules Plugin

The windows.modules plugin lists all **loaded kernel modules (drivers)** found in memory. These modules are .sys files that control hardware or system-level functions in Windows.

I run this volatility plugin: python .\vol.py -f .\memdump2.mem windows.modules

```
% C:\Users\Student\Downloads\volatility3-develop\volatility3-develop> python .\vol.py -f .\memdump2.mem windows.modules
Volatility Framework 2.26.1
Progress: 100.00    PDB scanning finished
Offset Base Size Name Path File output

0xb406fb65c3b0 0xf80404860000 0x1047000 ntoskrnl.exe \SystemRoot\system32\ntoskrnl.exe    Disabled
0xb406fb65d3b0 0xf8040479f0000 0x60000 hal.dll \SystemRoot\system32\hal.dll    Disabled
0xb406fb65c6b0 0xf80404ce0000 0xb2000 kcdcm.dll \SystemRoot\system32\kcd.dll    Disabled
0xb406fb65c9b0 0xf80404760000 0x383000 mupadat.dll \SystemRoot\system32\mupadat.GenuineIntel.dll Disabled
0xb406fb65d6b0 0xf80404c10000 0x290000 tms.sys \SystemRoot\system32\drivers\tms.sys    Disabled
0xb406fb65d6f10 0xf80404ce10000 0x1b0000 PSHED.dll \SystemRoot\system32\PSHED.dll    Disabled
0xb406fb65d6f20 0xf80404c10000 0x100000 BOOTVID.dll \SystemRoot\system32\BOOTVID.dll    Disabled
0xb406fb65d6f30 0xf80404c10000 0x100000 cryptui.dll \SystemRoot\system32\cryptui.dll    Disabled
0xb406fb65d6f50 0xf80404d00000 0x63000 msrpc.sys \SystemRoot\system32\drivers\msnspc.sys Disabled
0xb406fb65d6f70 0xf80404d00000 0x2c000 ksecdd.sys \SystemRoot\system32\drivers\ksecdd.dll Disabled
0xb406fb65d6f90 0xf80404d10000 0xf0000 clipplp.sys \SystemRoot\system32\drivers\clipplp.sys Disabled
0xb406fb65d6f90 0xf80404d10000 0x16000 cmimexv.sys \SystemRoot\system32\drivers\cmimexv.sys Disabled
0xb406fb65d6f90 0xf80404d10000 0x16000 werkernel.sys \SystemRoot\system32\drivers\werkernel.sys Disabled
0xb406fb65e010 0xf80404d10000 0xc800 ntosext.sys \SystemRoot\system32\drivers\ntosext.sys Disabled
0xb406fb65e010 0xf80404d20000 0x100000 vsm.sys \SystemRoot\system32\drivers\vsm.dll Disabled
0xb406fb65e010 0xf80404d20000 0x100000 vsmc.sys \SystemRoot\system32\drivers\vsmc.dll Disabled
0xb406fb65e010 0xf80404d20000 0x70000 wdf01000.sys \SystemRoot\system32\drivers\wdf01000.sys Disabled
0xb406fb65e010 0xf80404d10000 0x13000 wpfrecoorder.sys \SystemRoot\system32\drivers\wpfrecoorder.sys Disabled
0xb406fb65e010 0xf80404d10000 0x12000 wdf01000.dll \SystemRoot\system32\drivers\wdf01000.dll Disabled
0xb406fb65e010 0xf80404d10000 0x100000 wfdm.sys \SystemRoot\system32\drivers\wfdm.sys Disabled
0xb406fb65e010 0xf80404d440000 0x27000 acpix.sys \SystemRoot\system32\drivers\acpix.sys Disabled
0xb406fb65e010 0xf80404d47000 0xf0000 mssecore.sys \SystemRoot\system32\drivers\mssecore.sys Disabled
0xb406fb65e010 0xf80404d47000 0x16000 mssecore.dll \SystemRoot\system32\drivers\mssecore.dll Disabled
0xb406fb65e010 0xf80404d540000 0xc800 WMILIB.SYS \SystemRoot\system32\drivers\WMILIB.SYS Disabled
0xb406fb65e010 0xf80404d540000 0x86000 intelpep.sys \SystemRoot\system32\drivers\intelpep.sys Disabled
0xb406fb65e010 0xf80404d70000 0x18000 WindowsTrustedRt.sys \SystemRoot\system32\drivers\WindowsTrustedRt.sys Disabled
0xb406fb65e010 0xf80404d70000 0x16000 WindowsTrustedRtProxy.sys \SystemRoot\system32\drivers\WindowsTrustedRtProxy.sys Disabled
0xb406fb65e020 0xf80404d60000 0x16000 pcv.sys \SystemRoot\system32\drivers\pcv.sys Disabled
0xb406fb65e020 0xf80404d60000 0x16000 Wmssd.sys \SystemRoot\system32\drivers\wmssd.sys Disabled
0xb406fb65e020 0xf80404d60000 0x14000 msfilter.sys \SystemRoot\system32\drivers\msfilter.sys Disabled
0xb406fb65e020 0xf80404d60000 0x13000 vdrvrroot.sys \SystemRoot\system32\drivers\vdrvrroot.sys Disabled
0xb406fb65e020 0xf80404d72000 0x13000 pdc.sys \SystemRoot\system32\drivers\pdऍ.sys Disabled
0xb406fb65e020 0xf80404d72000 0x13000 CEA.sys \SystemRoot\system32\drivers\CEA.sys Disabled
0xb406fb65e020 0xf80404d72000 0x13000 VOLUME.sys \SystemRoot\system32\drivers\volume.sys Disabled
0xb406fb65e020 0xf80404d72000 0x13000 spaceport.sys \SystemRoot\system32\drivers\spaceport.sys Disabled
0xb406fb65e020 0xf80404d80000 0x13000 volmgr.sys \SystemRoot\system32\drivers\volmgr.sys Disabled
0xb406fb65e020 0xf80404d80000 0x13000 VIDEOPORT.sys \SystemRoot\system32\drivers\videoport.sys Disabled
0xb406fb65e020 0xf80404d90000 0x13000 PCITDDEX.SYS \SystemRoot\system32\drivers\pcitdex.sys Disabled
0xb406fb65e020 0xf80404d90000 0x13000 vlmgr.sys \SystemRoot\system32\drivers\vlmgr.sys Disabled
0xb406fb65e020 0xf80404d90000 0x14000 vsmock.sys \SystemRoot\system32\drivers\vsdock.sys Disabled
0xb406fb65e020 0xf80404d90000 0x18000 vsmock.sys \SystemRoot\system32\drivers\vsmock.sys Disabled
0xb406fb65e020 0xf80404d90000 0x11000 vsmc.sys \SystemRoot\system32\drivers\vsdock.sys Disabled
0xb406fb65e020 0xf80404d90000 0x11000 atapi.sys \SystemRoot\system32\drivers\atapi.sys Disabled
0xb406fb65e020 0xf80404d90000 0x13000 ataport.sys \SystemRoot\system32\drivers\ataport.sys Disabled
0xb406fb65e020 0xf80404d90000 0x12000 atapiport.sys \SystemRoot\system32\drivers\atapiport.sys Disabled
0xb406fb65e020 0xf80404d90000 0x11000 atapiport.sys \SystemRoot\system32\drivers\atapiport.sys Disabled
0xb406fb65e020 0xf80404d90000 0x11000 stport.sys \SystemRoot\system32\drivers\stport.sys Disabled
0xb406fb65f20 0xf80404df0000 0x3b000 stormvme.sys \SystemRoot\system32\drivers\stormvme.sys Disabled
0xb406fb65f30 0xf80404df1000 0x24000 EhStorClass.sys \SystemRoot\system32\drivers\ehstorclass.sys Disabled
0xb406fb65f40 0xf80404df1000 0x23000 ehstorfilter.sys \SystemRoot\system32\drivers\ehstorfilter.sys Disabled
0xb406fb65f50 0xf80404df1000 0x45000 Wcf.sys \SystemRoot\system32\drivers\wcf.sys Disabled
0xb406fb65f50 0xf80404df0000 0x94000 wdffilter.sys \SystemRoot\system32\drivers\wdffilter.sys Disabled
0xb406fb65f50 0xf80404df0000 0x334000 Ntfs.sys \SystemRoot\system32\drivers\ntfs.sys Disabled
```

Figure 38 Volatility windows.modules plugin

```

0xb406f9ecdd10 0x8f80417480000 0x13000 hidusb.sys | \SystemRoot\system32\drivers\hidusb.sys Disabled
0xb406fe8e51900 0x8f80417460000 0x44000 HIDCLASS.SYS | \SystemRoot\system32\drivers\HIDCLASS.SYS Disabled
0xb406ffecfb10 0x8f80417450000 0x16000 HIDPARSE.SYS | \SystemRoot\system32\drivers\HIDPARSE.SYS Disabled
0xb406ffed74c10 0x8f80417440000 0x11000 hiduid.sys | \SystemRoot\system32\drivers\hiduid.sys Disabled
0xb406ffed74d10 0x8f80417430000 0x11000 hiduid.sys | \SystemRoot\system32\drivers\hiduid.sys Disabled
0xb406ffed74e10 0x8f80417420000 0x11000 win32k.sys | \SystemRoot\system32\drivers\win32k.sys Disabled
0xb406ffed74f10 0x8f80417410000 0x11000 win32k.sys | \SystemRoot\system32\drivers\win32k.sys Disabled
0xb406ffed74f90 0x8f80417500000 0x80000 WIN32KSGD.SYS | \SystemRoot\system32\WIN32KSGD.SYS Disabled
0xb406ffed75010 0x8f80417510000 0x315000 win32kbase.sys | \SystemRoot\system32\win32kbase.sys Disabled
0xb406ffed75020 0x8f80417520000 0x16000 win32kfull.sys | \SystemRoot\system32\win32kfull.sys Disabled
0xb406ffed75030 0x8f80417530000 0x88000 dxgms1.sys | \SystemRoot\system32\drivers\dxgms1.sys Disabled
0xb406ffdff6310 0x8f80417540000 0x116000 dxgms2.sys | \SystemRoot\system32\drivers\dxgms2.sys Disabled
0xb406ffdff6410 0x8f80417550000 0x470000 dd.dll | \SystemRoot\system32\drivers\dd.dll Disabled
0xb406ffdff6510 0x8f80417560000 0x1000 monitor.sys | \SystemRoot\system32\drivers\monitor.sys Disabled
0xb406ffdff6550 0x8f80417570000 0x11000 dump_storport.sys | \SystemRoot\system32\drivers\dump_storport.sys Disabled
0xb406ffdff6590 0x8f80417770000 0x3b000 dump_stormme.sys | \SystemRoot\system32\drivers\dump_stormme.sys Disabled
0xb406ffdff6610 0x8f80417780000 0x16000 dumpdrive.sys | \SystemRoot\system32\drivers\dumpdrive.sys Disabled
0xb406ffdff6710 0x8f80417840000 0x157000 WdFilter.sys | \SystemRoot\system32\drivers\WdFilter.sys Disabled
0xb406ffdff6810 0x8f80417850000 0x3a000 apfilter.sys | \SystemRoot\system32\drivers\apfilter.sys Disabled
0xb406ffdff6820 0x8f80417860000 0x3a000 applockerfltr.sys | \SystemRoot\system32\drivers\applockerfltr.sys Disabled
0xb406ffdff6830 0x8f80417870000 0x16000 bfr.sys | \SystemRoot\system32\drivers\bfr.sys Disabled
0xb406ffdff6840 0x8f80417910000 0x24000 wanarp.sys | \SystemRoot\system32\drivers\wanarp.sys Disabled
0xb406ffdff6950 0x8f80417940000 0x13000 wcfif.sys | \SystemRoot\system32\drivers\wcfif.sys Disabled
0xb406ffdff6a50 0x8f80417950000 0x16000 cldfit.sys | \SystemRoot\system32\drivers\cldfit.sys Disabled
0xb406ffdff6b50 0x8f80417960000 0x16000 dppif.sys | \SystemRoot\system32\drivers\dppif.sys Disabled
0xb406ffdff6c50 0x8f80417970000 0x28000 bindflt.sys | \SystemRoot\system32\drivers\bindflt.sys Disabled
0xb406ffdff6e10 0x8f80417980000 0x19000 lltdio.sys | \SystemRoot\system32\drivers\lltdio.sys Disabled
0xb406ffdff6e20 0x8f80417990000 0x19000 msldp.sys | \SystemRoot\system32\drivers\msldp.sys Disabled
0xb406ffdff6e30 0x8f804179a0000 0x16000 msldp.sys | \SystemRoot\system32\drivers\msldp.sys Disabled
0xb406ffdff6e50 0x8f804179b0000 0x16000 wanarp.sys | \SystemRoot\system32\DRIVERS\wanarp.sys Disabled
0xb406ffdff6e60 0x8f804d7420000 0x5d000 msquic.sys | \SystemRoot\system32\drivers\msquic.sys Disabled
0xb406ffdff6e70 0x8f804d7430000 0x16000 mncss.sys | \SystemRoot\system32\drivers\mncss.sys Enabled
0xb406ffdff6e80 0x8f804d7440000 0x16000 msdp.sys | \SystemRoot\system32\drivers\msdp.sys Enabled
0xb406ffdff6e90 0x8f804d7450000 0x16000 msdp.sys | \SystemRoot\system32\drivers\msdp.sys Enabled
0xb406ffdff6fa10 0x8f804d7460000 0x16000 vmmemt1.sys | \SystemRoot\system32\DRIVERS\vmmemt1.sys Disabled
0xb406ffdff6fa20 0x8f804d7470000 0x5b000 svmet.sys | \SystemRoot\system32\DRIVERS\svmet.sys Disabled
0xb406ffdff6fa30 0x8f804d7480000 0x16000 sv2.sys | \SystemRoot\system32\DRIVERS\sv2.sys Disabled
0xb406ffdff6fa40 0x8f804d7490000 0x16000 sv3.sys | \SystemRoot\system32\DRIVERS\sv3.sys Disabled
0xb406ffdff6fa50 0x8f804d74a0000 0x16000 peauth.sys | \SystemRoot\system32\drivers\peauth.sys Disabled
0xb406ffdff6fa60 0x8f804d74b0000 0x16000 tcipreg.sys | \SystemRoot\system32\drivers\tcipreg.sys Disabled
0xb406ffdff6fa70 0x8f804d74c0000 0x15800 vtd.sys | \SystemRoot\system32\DRIVERS\vtd.sys Disabled
0xb406ffdff6fa80 0x8f804d74d0000 0x16000 vtd.sys | \SystemRoot\system32\DRIVERS\vtd.sys Disabled
0xb406ffdff6fa90 0x8f804d74e0000 0x12000 condrv.sys | \SystemRoot\system32\drivers\condrv.sys Disabled
0xb406ffdff6fa90 0x8f804d74f0000 0x13000 k1d.sys | \SystemRoot\system32\drivers\k1d.sys Disabled
0xb406ffdff6fa90 0x8f804d7500000 0x16000 k1d.sys | \SystemRoot\system32\drivers\k1d.sys Disabled
0xb406ffdff6fa90 0x8f804d7510000 0x16000 rassstsp.sys | \SystemRoot\system32\drivers\rassstsp.sys Disabled
0xb406ffdff6fa90 0x8f804d7520000 0x16000 RDPProxy.sys | \SystemRoot\system32\DRIVERS\RDPProxy.sys Disabled
0xb406ffdff6fa90 0x8f804d7530000 0x16000 AglAvn.sys | \SystemRoot\system32\drivers\AglAvn.sys Disabled
0xb406ffdff6fa90 0x8f804d7540000 0x16000 AglAvn.sys | \SystemRoot\system32\drivers\AglAvn.sys Disabled
0xb406ffdff6fa90 0x8f804d7550000 0x16000 raspppt.sys | \SystemRoot\system32\drivers\raspppt.sys Disabled
0xb406ffdff6fa90 0x8f804d7560000 0x16000 rasppop.sys | \SystemRoot\system32\DRIVERS\rasppop.sys Disabled
0xb406ffdff6fa90 0x8f804d7570000 0x16000 ndistapi.sys | \SystemRoot\system32\drivers\ndistapi.sys Disabled
0xb406ffdff6fa90 0x8f804d7580000 0x16000 vtd.sys | \SystemRoot\system32\DRIVERS\vtd.sys Disabled
0xb406ffdff6fa90 0x8f804d7590000 0x16000 vtd.sys | \SystemRoot\system32\DRIVERS\vtd.sys Disabled
0xb406ffdff6fa90 0x8f804d75a0000 0x16000 ad_driver.10.sys | \V7C\Users\student\Downloads\volatility-develop\Windows\Temp\ad_driver.10.sys Disabled
PS C:\Users\student\Downloads\volatility-develop>

```

Figure 35 Volatility windows.modules plugin

Module Name	Path	Comment / Status
<b>ntoskrnl.exe</b>	\SystemRoot\system32\ntoskrnl.exe	Windows kernel — expected
<b>hal.dll</b>	\SystemRoot\system32\hal.dll	Hardware Abstraction Layer
<b>mcupdate.dll</b>	\System32\mcupdate_GenuineIntel.dll	CPU microcode update
<b>MsMpEng.sys</b>	\System32\drivers\MsMpEng.sys	Microsoft Defender (safe)
<b>WdFilter.sys, WdNisDrv.sys</b>	Windows Defender drivers	Clean system drivers

AppData\Local\Temp\ad_driver-10.sys	Suspicious temp path	Potential malicious driver
-------------------------------------	----------------------	----------------------------

## Others Plugins

The windows.filescan plugin scans **physical memory** to find file objects in memory including deleted or hidden files that may not appear in standard file listings. It helps detect malicious files, dropped payloads, unusual DLLs, and forensic artifacts **not visible via normal tools**.

I run this volatility plugin: python .\vol.py -f .\memdump2.mem windows.filescan

```

# C:\Users\student\Downloads\volatility3-develop\volatility3-develop> python .\vol.py -f .\memdump2.mem windows.filescan
volatility 3 Framework 2.26.2
Progress: 100.00          P08 scanning finished
Offset  Name
0xb406fb0c2c50 \Windows\system32\svchost.exe
0xb406fd8fe3e0 \Windows\system32\psapi.dll
0xb406fdaf5b50 \Windows\system32\userenv.dll.mui
0xb406fdaf5b60 \Windows\system32\cssrss.exe
0xb406fdaf5b60 \Windows\system32\wlnsrsv.dll
0xb406fdaf5b60 \Windows\system32\drivers\dxgmm61.sys
0xb406fdaf2300 \Windows\system32\kernel32.dll
0xb406fdaf2300 \Windows\system32\ole32.dll
0xb406fdaf2300 \Windows\system32\shaserv.dll
0xb406fdaf2300 \Sessions\1\AppContainerNamedObjects
0xb406fdaf2340 \Windows\system32\wlnsrsvext.dll
0xb406fdaf2340 \Windows\system32\ole32.dll
0xb406fdaf2360 \Windows\system32\ssssrv.dll
0xb406fdaf2380 \Windows\system32\en-US\cssrss.exe.mui
0xb406fdaf2d30 \Windows\system32\drivers\dxgmm62.sys
0xb406fdaf2d30 \Windows\system32\kernel32.dll
0xb406fdaf2d30 \Windows\system32\wlninit.exe
0xb406fdaf2d70 \Windows\system32
0xb406fdaf2d70 \Sessions\1\AppContainerNamedObjects
0xb406fdaf2d80 \Windows\system32\profapi.dll
0xb406fdaf2d80 \Windows\system32\ole32.dll
0xb406fdaf4e00 \SDIRECTORY
0xb406fdaf5e00 \Windows\system32\en-US\user32.dll.mui
0xb406fdaf6e10 \Windows\system32\cdll.dll
0xb406fdaf6e10 \Windows\system32\kernel32.dll
0xb406fdaf6e10 \Windows\system32\user32.dll
0xb406fdaf6e10 \Windows\system32\VB005.DLL
0xb406fdaf6e10 \SBitmap
0xb406fdaf6e10 \����්ති:INDEX_ALLOCATION
0xb406fdaf6e10 \��ක්ද:INDEX_ALLOCATION
0xb406fdaf6e10 \Extend\$RmMetadata\$Repair
0xb406fdaf6e20 \Extend\$RmMetadata\$Repair:$Corrupt:$DATA
0xb406fdaf6e20 \Extend\$RmMetadata\$Repair:$DATA
0xb406fdaf6e40 \Vigil
0xb406fdaf6e40 \Secure:$S05:$DATA
0xb406fdaf6f30 \SDIRECTORY
0xb406fdaf730 \SHFILE
0xb406fdff60 \Windows\system32\drivers\filecrypt.sys
0xb406fe68800 \Windows\system32\1252.NLS
0xb406fe68800 \Windows\system32\1252_C_437.NLS
0xb406fe68400 \SDIRECTORY
0xb406fe68600 \Windows\system32\drivers\lbase.sys
0xb406fe69400 \Windows\system32\drivers\vhache.sys
0xb406fe69400 \SDIRECTORY
0xb406fe69a00 \Windows\system32\intnl.nls
0xb406fe6a5e0 \Windows\bootstat.dat
0xb406fe6a6e0 \Windows\system32\DriverStore\FileRepository\compositebus.inf_amd64_2e50c98177d0a40\CompositeBus.sys
0xb406fe6a6e0 \Windows\system32\drivers\wlan.sys
0xb406fe7a0b0 \Windows\System32\drivers\Ucx@01000.sys
0xb406fe7a170 \Windows\system32\drivers\vmgencounter.sys
0xb406fe7a180 \Windows\system32\drivers\cmdbatt.sys
0xb406fe7a180 \Windows\system32\drivers\cmdbatt.sys
0xb406fe7a2340 \Windows\system32\drivers\babttc.sys
0xb406fe7a42e0 \Windows\System32\drivers\rdpbus.sys
0xb406fe7a4450 \Windows\System32\drivers\WdiVirtualBus.sys
0xb406fe7a52b0 \Windows\System32\DriverStore\FileRepository\svenum.inf_amd64_d84a235075a8ff73\svenum.sys

```

Figure 40 Volatility windows.filescan plugin



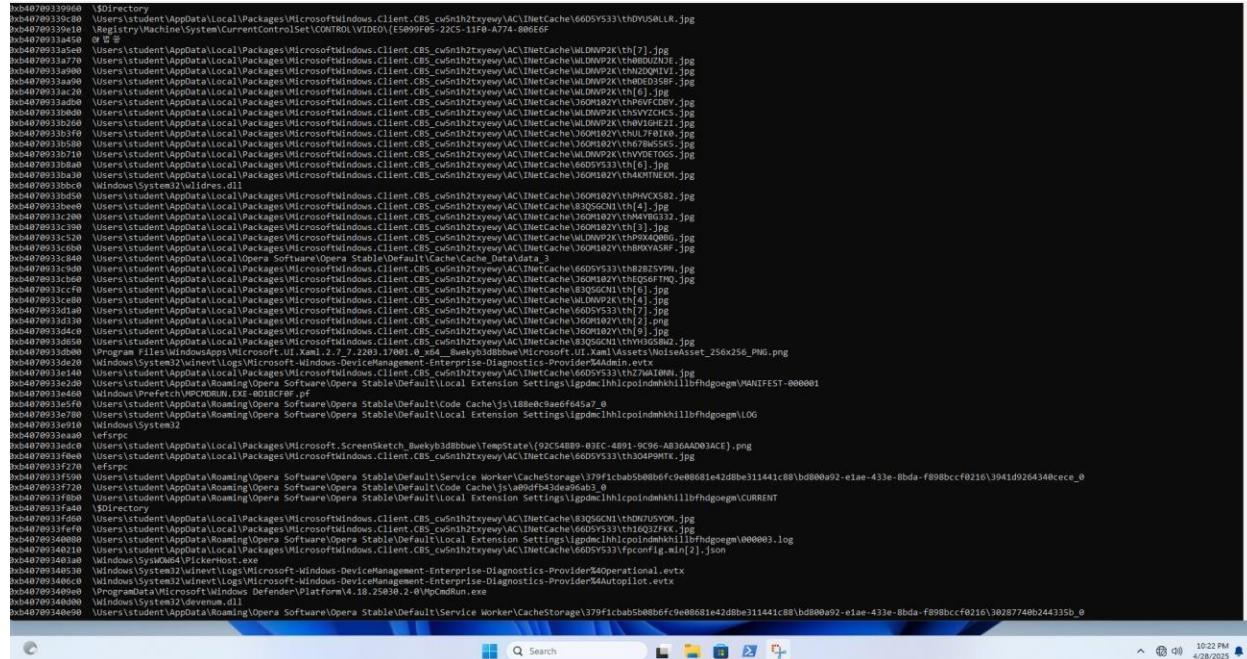


Figure 43 Volatility windows.filescan plugin

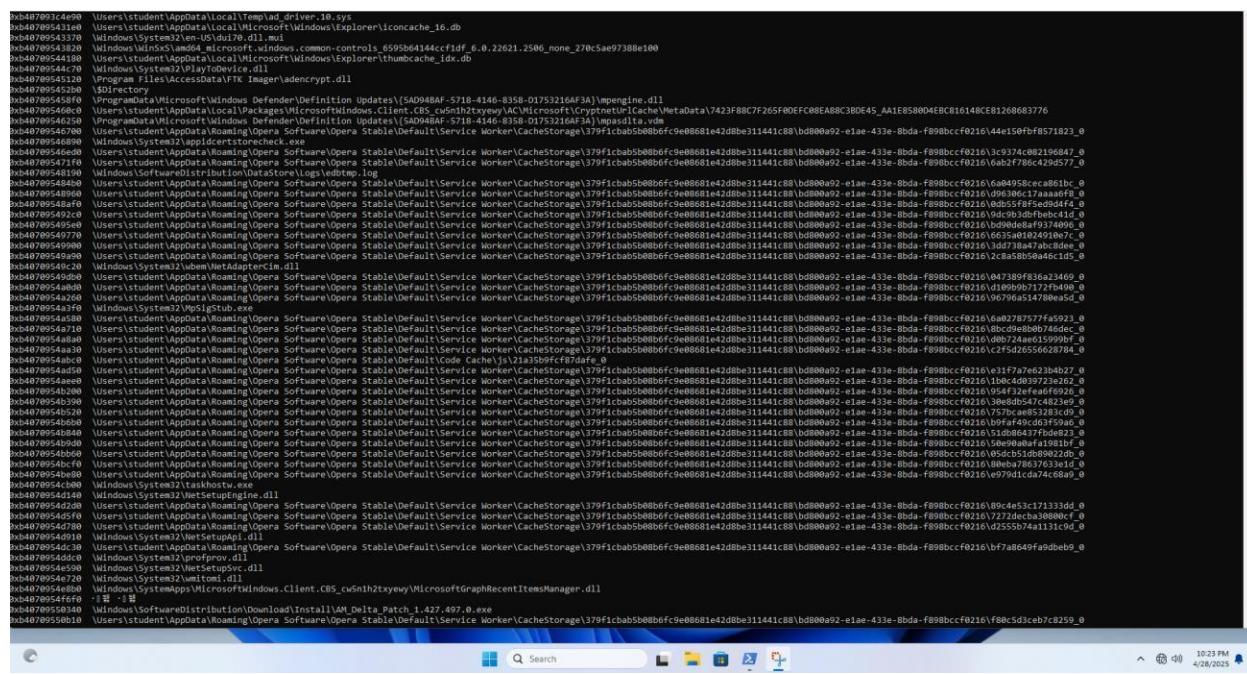


Figure 44 Volatility windows.filescan plugin

```

0xb4079056ba50 \Users\student\AppData\Roaming\Opera Software\Opera Stable\Default\Code Cache\js\fef2d07fd2fec14b_0
0xb4079056c540 \Users\student\AppData\Roaming\Opera Software\Opera Stable\Default\Code Cache\js\1117b796dc2edbbf_0
0xb4079056db00 \Program Files\AccessData\FTK Imager\MS.dll
0xb4079056e200 \Program Files\AccessData\FTK Imager\adshared.dll
0xb4079056e500 \Program Files\AccessData\FTK Imager\adshared.dll
0xb4079056f460 \Program Files\AccessData\FTK Imager\efdecrypter.dll
0xb4079056fd080 \Program Files\AccessData\FTK Imager\efconnect22.dll
0xb407905708a0 \Users\student\AppData\Roaming\Opera Software\Opera Stable\Default\Code Cache\js\bbedb31e7dfb3d52_0
0xb40790571100 \Program Files\AccessData\FTK Imager\efsconnect24.dll
0xb40790571500 \Program Files\AccessData\FTK Imager\efsconnect24_mt_159.dll
0xb407905783c0 \Program Files\AccessData\FTK Imager\libvshadow.dll
0xb40790578500 \Program File (x64)\Internet Explorer\flexproxy.exe
0xb40790578520 \Users\student\AppData\Roaming\Opera Software\Opera Stable\Default\Code Cache\js\3ef0970e66ffea7ff_0
0xb40790578640 \Users\student\AppData\Roaming\Opera Software\Opera Stable\Default\Code Cache\js\4ef7e784cb7cfdf_0
0xb40790571100 \!Directory:
0xb40790571c0 \Program Files\AccessData\FTK Imager\adsharedfrfs.dll
0xb4079057210 \Program Files\AccessData\FTK Imager\wincms\frfs\client.CBS_cwNlh2txyew\Ac\IMfrcache\0001B2V\th[1].png
0xb40790572400 \Users\student\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessibility\On-Screen Keyboard.lnk
0xb40790572620 \Program Files\AccessData\Local\Packages\Microsoft.Windows.Client.CBS_cwNlh2txyew\CacheStorage\Files4\52MMWQ31_1\JB24vBFP_2\KVCM4813O_49
0xb40790572840 \Windows\Fonts\seguisb.ttf
0xb40790572a00 \Program Files\AccessData\FTK Imager\libvshadow.dll
0xb40790572680 \Users\student\AppData\Roaming\Opera Software\Opera Stable\Default\Code Cache\js\186da218c48b0586_0
0xb40790572d00 \Windows\System Apps\Microsoft.Windows.Client.CBS_cwNlh2txyew\Cortana.Settings.winmd
0xb40790573000 \Windows\System32\WinMetadata\Windows.Foundation.winmd
0xb40790573100 \Windows\System32\WinMetadata\Windows\KernelBase.dll
0xb40790573400 \Windows\Fonts\seguief.ttf
0xb40790574240 \Windows\Fonts\seguilem.ttf
0xb40790574600 \Users\student\AppData\Local\Packages\Microsoft\Windows\Explorer\thumbcache_16.db
0xb40790574800 \Windows\System32\WinMetadata\Local\Opera\Software\Opera Stable\Default\Cache\Cache_Data_F_0000be
0xb40790574d00 \Windows\System32\en-US\combase.dll.mui
0xb40790575100 \Program Data\Microsoft\Windows Defender\Definition Updates\5AD04BAF-5718-4146-8358-D1753216AF3A\mpasdlta.vdm
0xb40790575200 \Windows\System32\WinMetadata\Windows\Definitions\en-US\af.dll
0xb40790575300 \!Directory:
0xb40790575600 \Windows\System32\en-US\DFrgUI.exe.mui
0xb40790575800 \Windows\SystemResources\DFrgui.exe.mun
0xb40790575700 \Users\student\AppData\Local\Packages\MicrosoftWindows.Client.CBS_cwNlh2txyew\appdata\CacheStorage\Files4\52MMWQ31_1\JB24vBFP_2\WMR6C19SW_12
0xb40790576400 \Windows\System32\en-US\Font\en-US\prinr.dll
0xb40790577600 \Program Data\Microsoft\Windows Defender\Definition Updates\5AD04BAF-5718-4146-8358-D1753216AF3A\mpavbase.vdm
0xb40790577800 \Windows\ImmersiveControlPanel\prinr.dll
0xb40790577940 \Users\student\AppData\Local\Packages\MicrosoftWindows.Client.CBS_cwNlh2txyew\appdata\CacheStorage\Files4\52MMWQ31_1\JB24vBFP_2\IRNEIQ0Q5P_10
0xb407905778f0 \Windows\ImmersiveControlPanel\images\logo_targetsize-32_aflorm-unplated.png
0xb40790579140 \Program Data\Microsoft\Windows Defender\Definition Updates\5AD04BAF-5718-4146-8358-D1753216AF3A\mpavdata.vdm
0xb40790579300 \Users\student\AppData\Local\Packages\MicrosoftWindows.Client.CBS_cwNlh2txyew\appdata\CacheStorage\Files4\52MMWQ31_1\JB24vBFP_2\I3L1FD63Y8_41
0xb40790579510 \Users\student\AppData\Local\Packages\MicrosoftWindows.Client.CBS_cwNlh2txyew\appdata\CacheStorage\Files4\52MMWQ31_1\JB24vBFP_2\3I79TY0VWX_65
0xb40790579910 \Windows\System32\en-US\shell32.dll
0xb40790579940 \!Directory:
0xb40790579970 \Program Data\Microsoft\Windows Defender\Definition Updates\5AD04BAF-5718-4146-8358-D1753216AF3A\mpavbase.vdm
0xb4079057a200 \Users\student\AppData\Local\Packages\Microsoft\Windows.Client.CBS_cwNlh2txyew\appdata\CacheStorage\Files4\52MMWQ31_1\JB24vBFP_2\60906D0M2_61
0xb4079057a400 \Users\student\AppData\Local\Packages\Microsoft\ScreenSketch\8weky3d8bhw\Temp\state\09AC1613-35B2-4000-AE01-F110c8898497.png
0xb40790579d00 \Program Data\Microsoft\Windows Defender\Definition Updates\5AD04BAF-5718-4146-8358-D1753216AF3A\mpavdata.vdm
0xb4079057a800 \Program Files\WindowsApps\Microsoft.VCLibs.140_0.33519.0_x64_8weky3d8bhw\vccon11140_app.dll
0xb4079057a820 \Windows\System32\Windows\Microsoft\Windows.Client.CBS_cwNlh2txyew\appdata\CacheStorage\Files4\52MMWQ31_1\JB24vBFP_2\MS0H2R24NX6_46
0xb4079057b2c0 \Users\student\AppData\Local\Microsoft\Internet Explorer\cacheStorage\editmap.asp
0xb4079057b500 \Windows\System32\GraphicsCapture.dll
0xb4079057b900 \!Directory:\faceback (most recent call last)
File "C:\Users\student\Downloads\volatility3-develop\vol.py", line 11, in <module>

```

Figure 45 Volatility windows.filescan plugin

Figure 4c Volatility windows.filescan plugin artifacts

File Path / Name	Description	Suspicious / Noteworthy
Windows\System32\svchost.exe	Core Windows service host process	Expected
Windows\System32\dxgmms1.dll	Graphics memory manager	Normal
Windows\System32\filecrypt.sys	File encryption driver	System driver
Windows\System32\config\systemprofile\AppData\Local\Temp\ad_driver-10.sys	Unknown .sys driver in	Suspicious — could

	Temp folder	be a dropped malicious driver
<b>Opera\Software\Opera Stable\CacheStorage\*.log</b>	Logs from the Opera browser	Useful for browser activity tracking
<b>Program Files\AccessData\FTK Imager\*</b>	Forensic tools present	Analyst - installed tools
<b>ChromeUnpacker_BeginUnzipping*.manifest.json</b>	Chrome extension install trace	Review for malicious extensions
<b>Windows\Prefetch\CHROME.EXE.*</b>	Prefetch file for Chrome	Useful for timeline analysis
<b>Windows\System32\Drivers\bam.sys</b>	Background activity manager	Normal
<b>Microsoft.Client.CBS_ *CacheStorageFiles\*</b>	AppX/Morden UI app data	Might hide sideloaded malware

<b>Windows\System32\config\SystemProfile\AppData\Local\Microsoft\Windows\Explorer\IconCache.db</b>	Tracks desktop icons and file usage	Useful for user interaction tracking
<b>Windows\System32\Tasks\Microsoft\Windows\UpdateOrchestrator</b>	Task Scheduler trace	System behavior trace
<b>Users\student\AppData\Roaming\Opera\Software\...</b>	<b>Opera cache logs and service worker files</b>	Useful for web activity and plugin analysis
<b>Windows\System32\LogFiles\WMI\RtBackup</b>	Windows Management Instrumentation logs	Normal logging area
<b>Windows\WinSxS\...</b>	Windows Side-by-Side assembly	Normal unless modified

## Interpretation Notes

### User Activity Evidence:

- Files from Opera and Chrome show that the user actively browsed the internet.
- Prefetch, cache, and .log files confirm usage of browsers, downloads, and possibly Chrome extensions.

### Suspicious Finding:

- ad\_driver-10.sys in the **Temp directory** is very suspicious. Legitimate drivers are not stored there. This could be:

- A dropped rootkit
- Part of malware that loads a kernel driver

### **Useful Forensic Evidence:**

- .db files like IconCache.db, .dat files from AppData, and cache storage  
JSONs help in reconstructing user sessions and behavior.
- Manifest and extension files (e.g., ChromeUnpacker, Opera Logs) should be examined for signs of malicious code or unauthorized extensions.

### **System & App Logs:**

- Windows update logs, task scheduler traces, and AppX app cache paths are useful for understanding:
  - App installation timelines
  - Update behavior
  - Background task activity (possibly abused by malware)

### **Plugin Definition: windows.dumpfiles**

The windows.dumpfiles plugin is used to extract and list memory-resident file objects (like registry hives, logs, executables, DLLs, app data) from a Windows memory dump.

I run this volatility plugin: python .\vol.py -f .\memdump2.mem  
windows.dumpfiles



```

ImageSectionObject 0xb4d70716083c0 networkexplorer.dll file.0xb4d70716083c0.0xb4d7071529080.ImageSectionObject.networkexplorer.dll.img
ImageSectionObject 0xb4d70803126d0 IconCodecsService.dll file.0xb4d70803126d0.0xb4d70803126d0.ImageSectionObject.IconCodecsService.dll.img
DataSectionObject 0xb4d70555150 MSOTC.LOG Error dumping file
ImageSectionObject 0xb4d70713c4e80 cryptui.dll file.0xb4d70713c4e80.0xb4d70713c4e80.ImageSectionObject.cryptui.dll.img
ImageSectionObject 0xb4d70713c4e90 cryptui.dll file.0xb4d70713c4e90.0xb4d70713c4e90.ImageSectionObject.cryptui.dll.img
ImageSectionObject 0xb4d70713c4e70 mtxoc1.dll file.0xb4d70713c4e70.0xb4d70713c4e70.ImageSectionObject.mtxoc1.dll.img
ImageSectionObject 0xb4d70713b0b0 msdtc.exe file.0xb4d70713b0b0.0xb4d70713b0b0.ImageSectionObject.msdtc.exe.img
ImageSectionObject 0xb4d70713b0f0 msdtc.exe file.0xb4d70713b0f0.0xb4d70713b0f0.ImageSectionObject.msdtc.exe.img
ImageSectionObject 0xb4d70713b0e0 msdtc.exe file.0xb4d70713b0e0.0xb4d70713b0e0.ImageSectionObject.msdtc.exe.img
ImageSectionObject 0xb4d70713b0f1 msdtc.exe file.0xb4d70713b0f1.0xb4d70713b0f1.ImageSectionObject.msdtc.exe.img
ImageSectionObject 0xb4d70713351b0 SmartActionPlatform.dll file.0xb4d70713351b0.0xb4d70713351b0.ImageSectionObject.SmartActionPlatform.dll.img
ImageSectionObject 0xb4d707133518b0 SmartActionPlatform.dll file.0xb4d707133518b0.0xb4d707133518b0.ImageSectionObject.SmartActionPlatform.dll.img
ImageSectionObject 0xb4d70713351890 SmartActionPlatform.dll file.0xb4d70713351890.0xb4d70713351890.ImageSectionObject.SmartActionPlatform.dll.img
ImageSectionObject 0xb4d70713b748 windows.applicationmodel.datatransfer.dll file.0xb4d70713b748.0xb4d70713b748.ImageSectionObject.windows.applicationmodel.datatransfer.dll.img
ImageSectionObject 0xb4d707155a8d0 appinfo.dll file.0xb4d707155a8d0.0xb4d707155a8d0.ImageSectionObject.appinfo.dll.img
ImageSectionObject 0xb4d707155a8b0 appinfo.dll file.0xb4d707155a8b0.0xb4d707155a8b0.ImageSectionObject.appinfo.dll.img
ImageSectionObject 0xb4d7071455a80 Windows.UI.wimnd file.0xb4d7071455a80.0xb4d7071455a80.ImageSectionObject.Windows.UI.wimnd.img
ImageSectionObject 0xb4d7071565450 Windows.Foundation.wimnd file.0xb4d7071565450.0xb4d7071565450.ImageSectionObject.Windows.Foundation.wimnd.img
ImageSectionObject 0xb4d7071458260 Cortana.Search.wimnd file.0xb4d7071458260.0xb4d7071458260.ImageSectionObject.Cortana.Search.wimnd.img
ImageSectionObject 0xb4d7071458261 Cortana.Settings.wimnd file.0xb4d7071458261.0xb4d7071458261.ImageSectionObject.Cortana.Settings.wimnd.img
DataSectionObject 0xb4d7071842550 AppsIndex.db file.0xb4d7071842550.0xb4d7071842550.DataSectionObject.AppsIndex.db.dat
sharedCacheMap 0xb4d7071842550 AppsIndex.db file.0xb4d7071842550.0xb4d7071842550.ShareCacheMap.AppsIndex.db.vacb
DataSectionObject 0xb4d7071842560 AppsIndex.db file.0xb4d7071842560.0xb4d7071842560.DataSectionObject.AppsIndex.db.vacb
DataSectionObject 0xb4d7071842561 AppsIndex.db file.0xb4d7071842561.0xb4d7071842561.DataSectionObject.AppsIndex.db.vacb
ImageSectionObject 0xb4d7071455a8d0 Cortana.Internal.Search.wimnd file.0xb4d7071455a8d0.0xb4d7071455a8d0.ImageSectionObject.Cortana.Internal.Search.wimnd.img
ImageSectionObject 0xb4d7071455a8b0 Windows.Storage.wimnd file.0xb4d7071455a8b0.0xb4d7071455a8b0.ImageSectionObject.Windows.Storage.wimnd.img
ImageSectionObject 0xb4d70714d7670 Windows.System.wimnd file.0xb4d70714d7670.0xb4d70714d7670.ImageSectionObject.Windows.System.wimnd.img
ImageSectionObject 0xb4d70714d7671 ChatUI.wimnd file.0xb4d70714d7671.0xb4d70714d7671.ImageSectionObject.ChatUI.wimnd.img
DataSectionObject 0xb4d70714d7672 Cryptoki.dll file.0xb4d70714d7672.0xb4d70714d7672.DataSectionObject.Cryptoki.dll.dat
ImageSectionObject 0xb4d70715d9880 Windows.ApplicationModel.wimnd file.0xb4d70715d9880.0xb4d70715d9880.ImageSectionObject.Windows.ApplicationModel.wimnd.img
DataSectionObject 0xb4d70715d9881 settings.db file.0xb4d70715d9881.0xb4d70715d9881.DataSectionObject.settings.db.dat
ImageSectionObject 0xb4d70715d9882 settings.db file.0xb4d70715d9882.0xb4d70715d9882.DataSectionObject.settings.db.wimnd
DataSectionObject 0xb4d70715d9883 settings.db.wimnd file.0xb4d70715d9883.0xb4d70715d9883.DataSectionObject.settings.db.wimnd
ImageSectionObject 0xb4d70715d770 Cortana.Settings.wimnd file.0xb4d70715d770.0xb4d70715d770.ImageSectionObject.Cortana.Settings.wimnd.img
DataSectionObject 0xb4d70715d33e6b0 IconCache.db file.0xb4d70715d33e6b0.0xb4d70715d33e6b0.DataSectionObject.IconCache.db.vacb
ImageSectionObject 0xb4d70715d724f0 TileCache_100_4_PNGEncoded_Data.bin file.0xb4d70715d724f0.0xb4d70715d724f0.ImageSectionObject.TileCache_100_4_PNGEncoded_Data.bin.vacb
ImageSectionObject 0xb4d7071836840 ole32.dll file.0xb4d7071836840.0xb4d7071836840.ImageSectionObject.ole32.dll.img
DataSectionObject 0xb4d70715t3530 netmsg.dll file.0xb4d70715t3530.0xb4d70715t3530.DataSectionObject.netmsg.dll.dat
ImageSectionObject 0xb4d70715t3540 Windows.Foundation.wimnd file.0xb4d70715t3540.0xb4d70715t3540.ImageSectionObject.Windows.Foundation.wimnd.img
ImageSectionObject 0xb4d7071827930 SearchUI.UI.dll file.0xb4d7071827930.0xb4d7071827930.ImageSectionObject.SearchUI.UI.dll.img
ImageSectionObject 0xb4d7071827931 EdgeManager.dll file.0xb4d7071827931.0xb4d7071827931.ImageSectionObject.EdgeManager.dll.img
ImageSectionObject 0xb4d7071827932 EdgeManager.dll file.0xb4d7071827932.0xb4d7071827932.ImageSectionObject.EdgeManager.dll.img
ImageSectionObject 0xb4d7071827933 EdgeManager.dll file.0xb4d7071827933.0xb4d7071827933.ImageSectionObject.EdgeManager.dll.img
ImageSectionObject 0xb4d7071828420 SearchHost.exe file.0xb4d7071828420.0xb4d7071828420.ImageSectionObject.SearchHost.exe.img
ImageSectionObject 0xb4d7071820404 ntoskrnl.exe file.0xb4d7071820404.0xb4d7071820404.ImageSectionObject.ntoskrnl.exe.img
ImageSectionObject 0xb4d70718134960 SearchChk.Model.dll file.0xb4d70718134960.0xb4d70718134960.ImageSectionObject.SearchChk.Model.dll.img
ImageSectionObject 0xb4d70718135050 cryptoki.dll file.0xb4d70718135050.0xb4d70718135050.ImageSectionObject.Cryptoki.dll.dat
ImageSectionObject 0xb4d707181350490 edgeiso.dll file.0xb4d707181350490.0xb4d707181350490.ImageSectionObject.edgeiso.dll.img
ImageSectionObject 0xb4d707181350540 CryptOInMt.dll file.0xb4d707181350540.0xb4d707181350540.ImageSectionObject.CryptOInMt.dll.img
ImageSectionObject 0xb4d7071813505410 ChatUI.dll file.0xb4d7071813505410.0xb4d7071813505410.ImageSectionObject.ChatUI.dll.img
ImageSectionObject 0xb4d7071813505420 CryptOInMt.dll file.0xb4d7071813505420.0xb4d7071813505420.ImageSectionObject.CryptOInMt.dll.img
ImageSectionObject 0xb4d707155f6f0 edgethtml.dll file.0xb4d707155f6f0.0xb4d707155f6f0.ImageSectionObject.edgethtml.dll.img
ImageSectionObject 0xb4d7071562620 Windows.UI.Input.Inking.dll file.0xb4d7071562620.0xb4d7071562620.ImageSectionObject.Windows.UI.Input.Inking.dll.img
ImageSectionObject 0xb4d70718137970 corral12.dll file.0xb4d70718137970.0xb4d70718137970.ImageSectionObject.corral12.dll.img
ImageSectionObject 0xb4d70718137980 corral12.dll file.0xb4d70718137980.0xb4d70718137980.ImageSectionObject.corral12.dll.img
ImageSectionObject 0xb4d707182c5c8 ole3d32.dll file.0xb4d707182c5c8.0xb4d707182c5c8.ImageSectionObject.ole3d32.dll.img
ImageSectionObject 0xb4d707182c2a0 Windows.Storage.ApplicationData.dll file.0xb4d707182c2a0.0xb4d707182c2a0.ImageSectionObject.Windows.Storage.ApplicationData.dll.img
ImageSectionObject 0xb4d7071600860 Windows.Storage.OneCore.dll file.0xb4d7071600860.0xb4d7071600860.ImageSectionObject.Windows.Storage.OneCore.dll.img

```

Figure 4S Volatility windows.dumpfiles plugin

Table 1S Volatility windows.dumpfiles plugin

File Name / Type	Artifact Description	Suspicious/Important Reason
<b>NTUSER.DAT, SAM, SECURITY, SOFTWARE, SYSTEM</b>	Registry hives	Store critical info about users, system config, passwords
<b>UsrClass.dat</b>	Tracks user GUI activity	Good for reconstructing user behavior
<b>ActivationStore.dat, BCD.LOG, DEFAULT.LOG2</b>	System state info	Used in boot analysis and anti-forensics checks
<b>amsi.dll, amstream.dll, AppResolver.dll, etc.</b>	System DLLs	Validate for tampering or injection
<b>vcruntime140.dll, msvcp140.dll</b>	Runtime dependencies	Malware may sideload fake DLLs with same name
<b>vmware-vmsvc.log, vmtoolsd.exe</b>	Virtualization logs	Confirms analysis/test environment (VM-aware malware alert)
<b>IconCache.db, TileCache.bin</b>	GUI traces	Shows what user recently opened or viewed

<b>ad_driver.10.sys</b>	TEMP driver file	Suspicious, should be verified (may indicate dropped driver/malware)
<b>SearchUI.exe, SearchProtocolHost.exe</b>	Cortana/Search services	Check for abuse of search-related binaries
<b>Opera Stable Cache, Opera Software folders</b>	Browser cache traces	Can reveal recent visited sites or downloaded files
<b>boost_thread-vc140-mt-1_59.dll, ads_shared.dll, etc.</b>	Custom/lib DLLs	May be part of forensic tools or injected libraries
<b>.img and .dat files for dlls, drivers, services</b>	Raw memory-mapped files	Can be checked for code injection or anomalies

## Interpretation Notes

### Registry Hives (NTUSER.DAT, SAM, SYSTEM, etc.):

These files hold user accounts, passwords, installed apps, and system settings.

Good for forensic timeline and malware persistence analysis.

### UsrClass.dat & IconCache.db:

Show which apps the user interacted with and recently accessed icons helps build user activity timeline.

### DLLs like vcruntime140.dll, amstream.dll:

These are often **replaced or sideloaded** by malware. Their presence is normal, but they should be hash-checked against clean versions.

### Temporary/Unknown Drivers like ad\_driver.10.sys:

Drivers in Temp folder are highly suspicious. Could indicate rootkit or stealth malware was active.

### Opera and Cortana Data:

Browsing traces (Opera) and Windows Search service activity (SearchUI) can reveal what the user was doing before memory was captured.

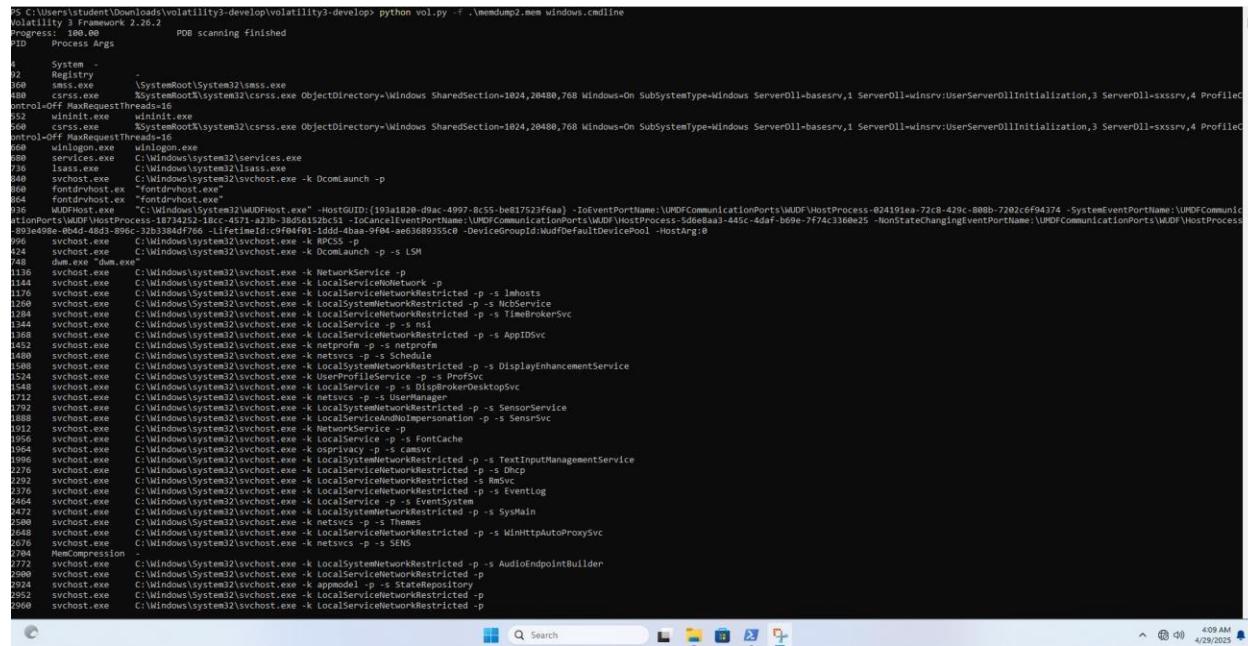
### VMware/VM logs:

Confirms the machine is running in a **virtual environment** some malware behaves differently or avoids execution if it detects this.

## Plugin Name: windows.cmdline

windows.cmdline plugin in Volatility 3 extracts the **command-line arguments** used to launch each process from memory. It helps forensic analysts understand **what commands were executed**, which is crucial in **identifying malware behavior, scripts, or attack vectors like persistence mechanisms, backdoors, or unauthorized tools.**

I run this volatility plugin: `python .\vol.py -f .\memdump2.mem windows.cmdline`



```
PS C:\Users\student\Downloads\volatility3-develop\volatility3-develop> python vol.py -f .\memdump2.mem windows.cmdline
Progress: 100.00          PDB scanning finished
PID  Process Args
0  System -
02 Registry -
060 smss.exe  \SystemRoot\System32\smss.exe
088 csrss.exe  %SystemRoot%\System32\csrss.exe ObjectDirectory=>Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows Server0!l=base!rv,1 Server0!l=win!rv:UserServer0!lInitialization,3 Server0!l=sxssrv,4 ProfileC
controlOfFileAndThread=16
052 wininit.exe  wininit.exe
056 csrss.exe  %SystemRoot%\System32\csrss.exe ObjectDirectory=>Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows Server0!l=base!rv,1 Server0!l=win!rv:UserServer0!lInitialization,3 Server0!l=sxssrv,4 ProfileC
controlOfFileAndThread=16
058 winlogon.exe  winlogon.exe
088 services.exe  C:\Windows\system32\services.exe
100 lsass.exe  C:\Windows\system32\lsass.exe
124 svchost.exe  C:\Windows\system32\svchost.exe -k DcomLaunch -p
148 svchost.exe  C:\Windows\system32\svchost.exe -k fontdvrhost -p
164 fontdrvhost.exe  "fontdrvhost.exe"
176 MUDFHost.exe  "C:\Windows\System32\MUDFHost.exe" -IDevPortName:UMDFCommunicationPorts\UMDF\HostProcess-024191ea-72c8-429c-808b-7202c0f94374 -SystemEventPortName:UMDFCommunicationPort-00000000-0000-0000-0000-000000000000 -LifetimemId:c9f04f01-1ddd-4baa-9f4a-aed3680935c0 -DeviceGroupid:UmdfDefaultDevicePool -HostArg:0
188 svchost.exe  C:\Windows\system32\svchost.exe -k RPCSrv -p
198 svchost.exe  C:\Windows\system32\svchost.exe -k DcomLaunch -s LS
1136 svchost.exe  C:\Windows\system32\svchost.exe -k NetworkService -p
1144 svchost.exe  C:\Windows\system32\svchost.exe -k localServiceNetwork -p
1176 svchost.exe  C:\Windows\system32\svchost.exe -k localServiceNetwork&Restricted -p -s lmhosts
1200 svchost.exe  C:\Windows\system32\svchost.exe -k localServiceNetwork&Restricted -p -s NtbtService
1284 svchost.exe  C:\Windows\system32\svchost.exe -k localServiceNetwork&Restricted -p -s TimeBrokerSv
1344 svchost.exe  C:\Windows\system32\svchost.exe -k localService -p -s nsi
1388 svchost.exe  C:\Windows\system32\svchost.exe -k localServiceNetwork&Restricted -p -s AppIDSvc
1452 svchost.exe  C:\Windows\system32\svchost.exe -k localServiceNetwork&Restricted -p -s netlogon
1480 svchost.exe  C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
1508 svchost.exe  C:\Windows\system32\svchost.exe -k localSystemNetwork&Restricted -p -s DisplayEnhancementService
1524 svchost.exe  C:\Windows\system32\svchost.exe -k UserFileSystemService -p -s ProfSvc
1540 svchost.exe  C:\Windows\system32\svchost.exe -k localSystemNetwork&Restricted -p -s DispenserDesktopSv
1712 svchost.exe  C:\Windows\system32\svchost.exe -k netsvcs -p -s UserManager
1792 svchost.exe  C:\Windows\system32\svchost.exe -k localSystemNetwork&Restricted -p -s SensorService
1888 svchost.exe  C:\Windows\system32\svchost.exe -k localSystemNetwork&Restricted -p -s Sensorsvc
1912 svchost.exe  C:\Windows\system32\svchost.exe -k NetworkService -p
1956 svchost.exe  C:\Windows\system32\svchost.exe -k localService -p -s FontCache
1964 svchost.exe  C:\Windows\system32\svchost.exe -k osprivacy -p -s cmsvc
1992 svchost.exe  C:\Windows\system32\svchost.exe -k localServiceNetwork&Restricted -p -s TextInputManagementService
2276 svchost.exe  C:\Windows\system32\svchost.exe -k localServiceNetwork&Restricted -p -s Dhcp
2292 svchost.exe  C:\Windows\System32\svchost.exe -k localServiceNetwork&Restricted -p -s RmSvc
2376 svchost.exe  C:\Windows\System32\svchost.exe -k localServiceNetwork&Restricted -p -s EventLog
2454 svchost.exe  C:\Windows\System32\svchost.exe -k localServiceNetwork&Restricted -p -s EventSystem
2472 svchost.exe  C:\Windows\System32\svchost.exe -k localSystemNetwork&Restricted -p -s SysMain
2508 svchost.exe  C:\Windows\System32\svchost.exe -k netsvcs -p -s Themes
2524 svchost.exe  C:\Windows\System32\svchost.exe -k localServiceNetwork&Restricted -p -s WinHttpAutoProxySvc
2576 svchost.exe  C:\Windows\System32\svchost.exe -k netsvcs -p -s SENS
2704 MemCompression
2722 svchost.exe  C:\Windows\System32\svchost.exe -k localSystemNetwork&Restricted -p -s AudioEndpointBuilder
2780 svchost.exe  C:\Windows\System32\svchost.exe -k localServiceNetwork&Restricted -p -s StateMonitor
2824 svchost.exe  C:\Windows\System32\svchost.exe -k localServiceNetwork&Restricted -p -s StateMonitor
2952 svchost.exe  C:\Windows\System32\svchost.exe -k localServiceNetwork&Restricted -p
2968 svchost.exe  C:\Windows\system32\svchost.exe -k localServiceNetwork&Restricted -p
```

Figure 50 Volatility windows.cmdline plugin



Table 20 Volatility windows.cmdline plugin artifacts

PID	Process Name	Command Line Argument
340	csrss.exe	\SystemRoot\System32\csrss.exe SharedSection=1024,20480,768 ... ObjectDirectory=Windows
648	wininit.exe	wininit.exe
736	services.exe	C:\Windows\system32\services.exe
748	lsass.exe	C:\Windows\system32\lsass.exe
1000	svchost.exe	C:\Windows\system32\svchost.exe -k DcomLaunch -p
1140	svchost.exe	C:\Windows\system32\svchost.exe -k RPCSS -p
1576	svchost.exe	C:\Windows\system32\svchost.exe-k LocalServiceNoNetwork -p -s AppIDSvc
6464	FTK Imager.exe	"C:\Program Files\AccessData\FTK Imager\FTK Imager.exe"
5856	firefox.exe	Not fully shown, but evidence of web usage
7688	SearchHost.exe	"C:\Windows\system32\SearchHost.exe" Global\UsGthrCtrlFltPipeMssGthrPipe4 ...

## Interpretation Notes

**System Processes:** Standard processes like csrss.exe, services.exe, lsass.exe, and multiple instances of svchost.exe are running with typical arguments indicating legitimate service initialization.

### Suspicious Clues:

svchost.exe is launched with multiple services, which is normal, but if any unknown or unauthorized service name is attached, it could indicate service abuse for persistence.

The presence of **FTK Imager** confirms forensic tooling is actively running on this system, possibly for evidence acquisition.

SearchHost.exe is seen with unusual command-line flags (Global\UsGthrCtrlFltPipe...), often observed in telemetry/data-gathering services.

msedgewebview2.exe shows embedded webview usage — legitimate in many applications but can also be **used in Electron-based malware** if launched from suspicious paths.

**No obvious malware yet,**

## Plugin: windows.envars

Extracts environment variables of processes from memory useful for identifying user context, runtime paths, and potential malicious temp usage.

I run this volatility plugin: python .\vol.py -f .\memdump2.mem windows.envars

```
15 C:\Users\student\Downloads\volatility3-develop\volatility3-develop> python vol.py -f .\memdump2.mem windows.envars
volatility 3 Framework 2.26.2
Progress: 100.00      POB scanning finished
ID  Process Block  Variable          Value
060  smss.exe    0x23e59a02df0  Path   C:\Windows\System32
060  smss.exe    0x23e59a02df0  SystemDrive  C:
060  smss.exe    0x180c7f603610  SystemRoot  C:\Windows
060  csrss.exe   0x180c7f603610  DriverData C:\Windows\System32\cmd.exe
060  csrss.exe   0x180c7f603610  Processor  Intel64 Family 6 Model 142 Stepping 12, GenuineIntel
060  csrss.exe   0x180c7f603610  NUMBER_OF_PROCESSORS 2
060  csrss.exe   0x180c7f603610  OS       Windows NT
060  csrss.exe   0x180c7f603610  Path   C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0;C:\Windows\System32\OpenSSH\
060  csrss.exe   0x180c7f603610  PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
060  csrss.exe   0x180c7f603610  PROCESSOR_ARCHITECTURE AMD64
060  csrss.exe   0x180c7f603610  PROCESSOR_IDENTIFIER Intel64 Family 6 Model 142 Stepping 12, GenuineIntel
060  csrss.exe   0x180c7f603610  PROCESSOR_LEVEL 6
060  csrss.exe   0x180c7f603610  PROCESSOR_REVISION 800c
060  csrss.exe   0x180c7f603610  PSModulePath $ProgramFiles\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules
060  csrss.exe   0x180c7f603610  SystemRoot C:\Windows
060  csrss.exe   0x180c7f603610  TEMP   C:\Windows\TEMP
060  csrss.exe   0x180c7f603610  TMP    C:\Windows\TEMP
060  csrss.exe   0x180c7f603610  USERPROFILE C:\Windows\user
060  csrss.exe   0x180c7f603610  WinDir C:\Windows
060  csrss.exe   0x228a003610  ComSpec C:\Windows\system32\cmd.exe
060  csrss.exe   0x228a003610  DriverData C:\Windows\System32\Drivers\DriverData
060  csrss.exe   0x228a003610  NUMBER_OF_PROCESSORS 2
060  csrss.exe   0x228a003610  OS     Windows NT
060  csrss.exe   0x228a003610  Path   C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0;C:\Windows\System32\OpenSSH\
060  csrss.exe   0x228a003610  PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
060  csrss.exe   0x228a003610  PROCESSOR_ARCHITECTURE AMD64
060  csrss.exe   0x228a003610  PROCESSOR_IDENTIFIER Intel64 Family 6 Model 142 Stepping 12, GenuineIntel
060  csrss.exe   0x228a003610  PROCESSOR_LEVEL 6
060  csrss.exe   0x228a003610  PROCESSOR_REVISION 800c
060  csrss.exe   0x228a003610  PSModulePath $ProgramFiles\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules
060  csrss.exe   0x228a003610  SystemDrive C:
060  csrss.exe   0x228a003610  SystemRoot C:\Windows
060  csrss.exe   0x228a003610  TEMP   C:\Windows\TEMP
060  csrss.exe   0x228a003610  TMP    C:\Windows\TEMP
060  csrss.exe   0x228a003610  USERNAME SYSTEM
060  csrss.exe   0x228a003610  WinDir C:\Windows
060  csrss.exe   0x2d06a03610  CurrentSPProfile C:\ProgramData
060  winlogon.exe 0x1d06a03610  CommonProgramFiles C:\Program Files\Common Files
060  winlogon.exe 0x1d06a03610  CommonProgramFiles(x86) C:\Program Files (x86)\Common Files
060  winlogon.exe 0x1d06a03610  CommonProgramFiles(x64) C:\Program Files\Program Files
060  winlogon.exe 0x1d06a03610  DESKTOP_47A94090 C:\Program Files\Program Files
060  winlogon.exe 0x1d06a03610  ComSpec C:\Windows\system32\cmd.exe
060  winlogon.exe 0x1d06a03610  DriverData C:\Windows\System32\Drivers\DriverData
060  winlogon.exe 0x1d06a03610  NUMBER_OF_PROCESSORS 2
060  winlogon.exe 0x1d06a03610  OS     Windows NT
060  winlogon.exe 0x1d06a03610  Path   C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0;C:\Windows\System32\OpenSSH\
060  winlogon.exe 0x1d06a03610  PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
060  winlogon.exe 0x1d06a03610  PROCESSOR_ARCHITECTURE AMD64
060  winlogon.exe 0x1d06a03610  PROCESSOR_IDENTIFIER Intel64 Family 6 Model 142 Stepping 12, GenuineIntel
060  winlogon.exe 0x1d06a03610  PROCESSOR_LEVEL 6
060  winlogon.exe 0x1d06a03610  PROCESSOR_REVISION 800c
060  winlogon.exe 0x1d06a03610  ProgramData C:\ProgramData
```

Figure 52 Volatility windows.envars plugin

```

668 winlogon.exe 0x1dc60003610 Path C:\Windows\System32;C:\Windows\System32\wbem;C:\Windows\System32\WindowsPowerShell\v1.0;C:\Windows\System32\OpenSSH
668 winlogon.exe 0x1dc60003610 PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
668 winlogon.exe 0x1dc60003610 PROCESSOR ARCHITECTURE AMD64
668 winlogon.exe 0x1dc60003610 PROCESSOR LEVEL 6
668 winlogon.exe 0x1dc60003610 PROCESSOR REVISION 80c
668 winlogon.exe 0x1dc60003610 ProgramData C:\ProgramData
668 winlogon.exe 0x1dc60003610 ProgramFiles C:\Program Files
668 winlogon.exe 0x1dc60003610 ProgramFiles(x86) C:\Program Files (x86)
668 winlogon.exe 0x1dc60003610 ProgramFiles64 C:\Program Files
668 winlogon.exe 0x1dc60003610 PSModulePath %ProgramFiles%\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules
668 winlogon.exe 0x1dc60003610 PUBLIC C:\Users\Public
668 winlogon.exe 0x1dc60003610 SystemRoot C:\Windows
668 winlogon.exe 0x1dc60003610 TEMP C:\Windows\TEMP
668 winlogon.exe 0x1dc60003610 TMP C:\Windows\Temp
668 winlogon.exe 0x1dc60003610 USERNAME SYSTEM
668 winlogon.exe 0x1dc60003610 winder C:\Windows
668 services.exe 0x1fe4b0003550 ALLUSERSPROFILE C:\ProgramData
668 services.exe 0x1fe4b0003550 COMPUTERNAME DESKTOP-54K7QV1S
668 services.exe 0x1fe4b0003550 CommonProgramFiles(x86) C:\Program Files (x86)\Common Files
668 services.exe 0x1fe4b0003550 CommonProgramFiles(x86) C:\Program Files (x86)\Common Files
668 services.exe 0x1fe4b0003550 CommonProgramFiles(x86) C:\Program Files (x86)\Common Files
668 services.exe 0x1fe4b0003550 ComputerName DESKTOP-54K7QV1S
668 services.exe 0x1fe4b0003550 COMSPEC C:\Windows\system32\cmd.exe
668 services.exe 0x1fe4b0003550 DriverData C:\Windows\System32\Drivers\DriverData
668 services.exe 0x1fe4b0003550 NUMBER_OF_PROCESSORS 2
668 services.exe 0x1fe4b0003550 OS C:\Windows
668 services.exe 0x1fe4b0003550 Path C:\Windows\System32\WindowsPowerShell\v1.0;C:\Windows\System32\OpenSSH
668 services.exe 0x1fe4b0003550 PROCESSOR ARCHITECTURE AMD64
668 services.exe 0x1fe4b0003550 PROCESSOR LEVEL 6
668 services.exe 0x1fe4b0003550 PROCESSOR REVISION 80c
668 services.exe 0x1fe4b0003550 ProgramData C:\ProgramData
668 services.exe 0x1fe4b0003550 ProgramFiles C:\Program Files
668 services.exe 0x1fe4b0003550 ProgramFiles(x86) C:\Program Files (x86)
668 services.exe 0x1fe4b0003550 ProgramFiles64 C:\Program Files
668 services.exe 0x1fe4b0003550 PSModulePath %ProgramFiles%\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules
668 services.exe 0x1fe4b0003550 PUBLIC C:\Windows\System32\WindowsPowerShell\v1.0\Modules
668 services.exe 0x1fe4b0003550 SystemDrive C:
668 services.exe 0x1fe4b0003550 SystemRoot C:\Windows
668 services.exe 0x1fe4b0003550 TEMP C:\Windows\TEMP
668 services.exe 0x1fe4b0003550 TMP C:\Windows\Temp
668 services.exe 0x1fe4b0003550 USERNAME SYSTEM
668 services.exe 0x1fe4b0003550 UserProfile C:\Windows\system32\config\systemprofile
668 services.exe 0x1fe4b0003550 Windows NT
668 lsass.exe 0x251bc403550 ALLUSERSPROFILE C:\ProgramData
668 lsass.exe 0x251bc403550 CommonProgramFiles C:\Program Files\Common Files
668 lsass.exe 0x251bc403550 CommonProgramFiles(x86) C:\Program Files (x86)\Common Files
668 lsass.exe 0x251bc403550 ComputerName DESKTOP-54K7QV1S
668 lsass.exe 0x251bc403550 ComSpec C:\Windows\system32\cmd.exe
668 lsass.exe 0x251bc403550 DriverData C:\Windows\System32\Drivers\DriverData
668 lsass.exe 0x251bc403550 NUMBER_OF_PROCESSORS 2
668 lsass.exe 0x251bc403550 OS C:\Windows NT
668 lsass.exe 0x251bc403550 Path C:\Windows\System32
668 lsass.exe 0x251bc403550 PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC

```

Figure 53 Volatility windows.envars plugin

```

648 svchost.exe 0x1fc3c4403740 Path C:\Windows\System32;C:\Windows;C:\Windows\System32\wbem;C:\Windows\System32\WindowsPowerShell\v1.0;C:\Windows\System32\OpenSSH;C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\FontCache
648 svchost.exe 0x1fc3c4403740 PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
648 svchost.exe 0x1fc3c4403740 PROCESSOR ARCHITECTURE AMD64
648 svchost.exe 0x1fc3c4403740 PROCESSOR IDENTIFIER Intel64 Family 6 Model 142 Stepping 12, GenuineIntel
648 svchost.exe 0x1fc3c4403740 PROCESSOR LEVEL 6
648 svchost.exe 0x1fc3c4403740 PROCESSOR REVISION 80c
648 svchost.exe 0x1fc3c4403740 ProgramData C:\ProgramData
648 svchost.exe 0x1fc3c4403740 ProgramFiles C:\Program Files
648 svchost.exe 0x1fc3c4403740 ProgramFiles(x86) C:\Program Files (x86)
648 svchost.exe 0x1fc3c4403740 PSModulePath %ProgramFiles%\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules
648 svchost.exe 0x1fc3c4403740 PUBLIC C:\Users\Public
648 svchost.exe 0x1fc3c4403740 SystemDrive C:
648 svchost.exe 0x1fc3c4403740 SystemRoot C:\Windows
648 svchost.exe 0x1fc3c4403740 TEMP C:\Windows\TEMP
648 svchost.exe 0x1fc3c4403740 TMP C:\Windows\Temp
648 svchost.exe 0x1fc3c4403740 WINDIR C:\Windows
648 svchost.exe 0x1fc3c4403740 USERNAME DESKTOP-54K7QV1S
648 svchost.exe 0x1fc3c4403740 UserProfile C:\Windows\system32\config\systemprofile
648 svchost.exe 0x1fc3c4403740 winder C:\Windows
648 fontdrvhost.exe 0x1790c655370 ALLUSERSPROFILE C:\ProgramData
648 fontdrvhost.exe 0x1790c655370 CommonProgramFiles C:\Program Files\Common Files
648 fontdrvhost.exe 0x1790c655370 CommonProgramFiles(x86) C:\Program Files (x86)\Common Files
648 fontdrvhost.exe 0x1790c655370 ComputerName DESKTOP-54K7QV1S
648 fontdrvhost.exe 0x1790c655370 ComSpec C:\Windows\system32\cmd.exe
648 fontdrvhost.exe 0x1790c655370 DriverData C:\Windows\System32\Drivers\DriverData
648 fontdrvhost.exe 0x1790c655370 LOCALAPDATA %TEMP%\Packages\microsoft.windows.Fontdrvhost\AC
648 fontdrvhost.exe 0x1790c655370 NUMBER_OF_PROCESSORS 2
648 fontdrvhost.exe 0x1790c655370 OS C:\Windows NT
648 fontdrvhost.exe 0x1790c655370 Path C:\Windows\System32;C:\Windows\System32\wbem;C:\Windows\System32\WindowsPowerShell\v1.0;C:\Windows\System32\OpenSSH
648 fontdrvhost.exe 0x1790c655370 PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
648 fontdrvhost.exe 0x1790c655370 PROCESSOR ARCHITECTURE AMD64
648 fontdrvhost.exe 0x1790c655370 PROCESSOR IDENTIFIER Intel64 Family 6 Model 142 Stepping 12, GenuineIntel
648 fontdrvhost.exe 0x1790c655370 PROCESSOR LEVEL 6
648 fontdrvhost.exe 0x1790c655370 PROCESSOR REVISION 80c
648 fontdrvhost.exe 0x1790c655370 ProgramData C:\ProgramData
648 fontdrvhost.exe 0x1790c655370 ProgramFiles C:\Program Files
648 fontdrvhost.exe 0x1790c655370 ProgramFiles(x86) C:\Program Files (x86)
648 fontdrvhost.exe 0x1790c655370 PSModulePath %ProgramFiles%\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules
648 fontdrvhost.exe 0x1790c655370 PUBLIC C:\Users\Public
648 fontdrvhost.exe 0x1790c655370 SystemDrive C:
648 fontdrvhost.exe 0x1790c655370 SystemRoot C:\Windows
648 fontdrvhost.exe 0x1790c655370 TEMP %TEMP%\Packages\microsoft.windows.Fontdrvhost\AC\Temp
648 fontdrvhost.exe 0x1790c655370 TMP %TEMP%\Packages\microsoft.windows.Fontdrvhost\AC\Temp
648 fontdrvhost.exe 0x1790c655370 USERDOMAIN Font Driver Host
648 fontdrvhost.exe 0x1790c655370 WERD_E
648 fontdrvhost.exe 0x1790c655370 UserProfile C:\Users\Default
648 fontdrvhost.exe 0x1790c655370 winder C:\Windows
648 fontdrvhost.exe 0x1fce4a8370 ALLUSERSPROFILE C:\ProgramData
648 fontdrvhost.exe 0x1fce4a8370 CommonProgramFiles C:\Program Files\Common Files
648 fontdrvhost.exe 0x1fce4a8370 CommonProgramFiles(x86) C:\Program Files (x86)\Common Files
648 fontdrvhost.exe 0x1fce4a8370 CommonProgramFiles64 C:\Program Files\Common Files
648 fontdrvhost.exe 0x1fce4a8370 ComputerName DESKTOP-54K7QV1S
648 fontdrvhost.exe 0x1fce4a8370 ComSpec C:\Windows\system32\cmd.exe
648 fontdrvhost.exe 0x1fce4a8370 DriverData C:\Windows\System32\Drivers\DriverData

```

Figure 54 Volatility windows.envars plugin

```
1136 svchost.exe 0x23ee0207c0 PROCESSOR_LEVEL 6
1136 svchost.exe 0x23ee0207c0 PROCESSOR_REVISION 8e0c
1136 svchost.exe 0x23ee0207c0 ProgramFiles C:\Program Files
1136 svchost.exe 0x23ee0207c0 ProgramFiles C:\Program Files
1136 svchost.exe 0x23ee0207c0 ProgramFiles(x86) C:\Program Files (x86)
1136 svchost.exe 0x23ee0207c0 ProgramFiles(x86) C:\Program Files (x86)\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules
1136 svchost.exe 0x23ee0207c0 PUBLIC C:\Users\Public
1136 svchost.exe 0x23ee0207c0 SystemDrive C:
1136 svchost.exe 0x23ee0207c0 SystemRoot C:\Windows
1136 svchost.exe 0x23ee0207c0 Tmp :\\Windows\TEMP;\\Windows\TEMP\NETBIOS-1\Temp
1136 svchost.exe 0x23ee0207c0 USERDOMAIN WORKGROUP
1136 svchost.exe 0x23ee0207c0 USERNAME DESKTOP-S4K7QV18
1136 svchost.exe 0x23ee0207c0 Win32ServiceProfile C:\Windows\ServiceProfiles\NetworkService
1136 svchost.exe 0x23ee0207c0 windir C:\Windows
1136 svchost.exe 0x23ee0207c0 :\\Windows\ServiceProfiles\NetworkService :\\Windows\ServiceProfiles\NetworkService
1136 svchost.exe 0x23ee0207c0 windir C:\Windows
1136 svchost.exe 0x23ee0207c0 svchost C:\Windows\NetworkService
1136 svchost.exe 0x23ee0207c0 windir C:\Windows
1136 svchost.exe 0x23ee0207c0 OMAIN WORKGROUP
1136 svchost.exe 0x23ee0207c0 SYSTEM DESKTOP-S4K7QV18
1136 svchost.exe 0x23ee0207c0 USERPROFILE C:\\Windows\ServiceProfiles\\NetworkService
1136 svchost.exe 0x23ee0207c0 windir C:\Windows
1136 svchost.exe 0x23ee0207c0 RPPROFILE C:\\Windows\ServiceProfiles\\NetworkService
1136 svchost.exe 0x23ee0207c0 svchost C:\\Windows\\System32\\cmd.exe
1136 svchost.exe 0x23ee0207c0 KTOP-S4K7QV1 KTOP-S4K7QV18
1136 svchost.exe 0x23ee0207c0 USERPROFILE C:\\Windows\ServiceProfiles\\NetworkService
1136 svchost.exe 0x23ee0207c0 windir C:\\Windows
1136 svchost.exe 0x23ee0207c0 :\\Windows\\System32\\es\\esNetworkService
1136 svchost.exe 0x23ee0207c0 windir C:\\Windows
1144 svchost.exe 0x20ae0f037b0 ALLUSERSPROFILE C:\\ProgramData
1144 svchost.exe 0x20ae0f037b0 COMMONAPPDATA C:\\Windows\\ServiceProfiles\\VirtualUser\\VirtualRoaming
1144 svchost.exe 0x20ae0f037b0 CommonProgramFiles C:\\Windows\\Common Files
1144 svchost.exe 0x20ae0f037b0 CommonProgramFiles(x86) C:\\Program Files (x86)\\Common Files
1144 svchost.exe 0x20ae0f037b0 CommonProgramFiles(x86) C:\\Program Files\\Common Files
1144 svchost.exe 0x20ae0f037b0 CommonProgramFiles(x86) C:\\Program Files\\Common Files
1144 svchost.exe 0x20ae0f037b0 C:\\Windows\\System32\\cmd.exe
1144 svchost.exe 0x20ae0f037b0 DriverData C:\\Windows\\System32\\Drivers\\DriverData
1144 svchost.exe 0x20ae0f037b0 LOCALAPPDATA C:\\Windows\\ServiceProfiles\\LocalService\\AppData\\Local
1144 svchost.exe 0x20ae0f037b0 NUMBER_OF_PROCESSORS 2
1144 svchost.exe 0x20ae0f037b0 OS\\Windows_NT
1144 svchost.exe 0x20ae0f037b0 Path C:\\Windows\\system32;C:\\Windows;C:\\Windows\\System32\\Wbm;C:\\Windows\\System32\\WindowsPowerShell\\v1.0;C:\\Windows\\System32\\OpenSSH;C:\\Windows\\ServiceProfiles\\LocalService\\AppData\\Local\\Micros
1144 svchost.exe 0x20ae0f037b0 PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.HSC
1144 svchost.exe 0x20ae0f037b0 PROCESSOR_ARCHITECTURE AMD64
1144 svchost.exe 0x20ae0f037b0 PROCESSOR_IDENTIFIER Intel64 Family 6 Model 142 Stepping 12, GenuineIntel
1144 svchost.exe 0x20ae0f037b0 PROCESSOR_LEVEL 6
1144 svchost.exe 0x20ae0f037b0 PROCESSOR_REVISION 8e0c
1144 svchost.exe 0x20ae0f037b0 ProgramData C:\\ProgramData
1144 svchost.exe 0x20ae0f037b0 ProgramFiles C:\\Program Files
1144 svchost.exe 0x20ae0f037b0 ProgramFiles(x86) C:\\Program Files (x86)
1144 svchost.exe 0x20ae0f037b0 ProgramFiles(x86) C:\\Program Files (x86)\\WindowsPowerShell\\Modules
1144 svchost.exe 0x20ae0f037b0 PModulePath %ProgramFiles%\\WindowsPowerShell\\Modules;C:\\Windows\\system32\\WindowsPowerShell\\v1.0\\Modules
1144 svchost.exe 0x20ae0f037b0 PUBLIC C:\\Users\\Public
1144 svchost.exe 0x20ae0f037b0 SystemDrive C:
1144 svchost.exe 0x20ae0f037b0 SystemRoot C:\\Windows
1144 svchost.exe 0x20ae0f037b0 TEMP C:\\Windows\\SERVIC=1\\LOCALS=1\\AppData\\local\\Temp
```

*Figure 55 Volatility windows.envars plugin*

```
1884 svchost.exe 0x27c4fc03700 Path C:\Windows\system32;C:\Windows;C:\Windows\System32\WBem;C:\Windows\System32\WindowsPowerShell\v1.0;C:\Windows\System32\OpenSSH;C:\Windows\ServiceProfiles\LocalService\AppData\Local\Microsoft\Windows\DeliveryOptimization
1284 svchost.exe 0x27c4fc03700 PATHTEXT _COM_,EXE_,BAT_,CMD_,VBS_,VBE_,JS_,JSE_,WSF_,WSH_,MSC
1284 svchost.exe 0x27c4fc03700 PROCESSOR_ARCHITECTURE AMD64
1284 svchost.exe 0x27c4fc03700 PROCESSOR_IDENTIFIER Intel64 Family 6 Model 142 Stepping 12, GenuineIntel
1284 svchost.exe 0x27c4fc03700 PROCESSOR_LEVEL 6
1284 svchost.exe 0x27c4fc03700 PROCESSOR_REVISION B6C
1284 svchost.exe 0x27c4fc03700 ProgramData C:\ProgramData
1284 svchost.exe 0x27c4fc03700 ProgramFiles(x86) C:\Program Files (x86)
1284 svchost.exe 0x27c4fc03700 ProgramFiles C:\Program Files
1284 svchost.exe 0x27c4fc03700 ProgramFilesCommon(x86) C:\Program Files\Common Files
1284 svchost.exe 0x27c4fc03700 ProgramFilesCommon C:\Program Files\Common Files
1284 svchost.exe 0x27c4fc03700 SystemRoot C:\Windows
1284 svchost.exe 0x27c4fc03700 TEMP C:\Windows\TEMP;C:\Windows\TEMP\LOCALS-1\AppData\Local\Temp
1284 svchost.exe 0x27c4fc03700 TMP C:\Windows\TEMP;C:\Windows\TEMP\LOCALS-1\AppData\Local\Temp
1284 svchost.exe 0x27c4fc03700 USERDOMAIN NT AUTHORITY
1284 svchost.exe 0x27c4fc03700 USERNAME LOCAL SERVICE
1284 svchost.exe 0x27c4fc03700 USERPROFILE C:\Windows\ServiceProfiles\LocalService
1284 svchost.exe 0x21f1f303700 AllUsersProfile C:\Windows\AllUsersProfile
1284 svchost.exe 0x21f1f303700 APPDATA C:\Windows\ServiceProfiles\LocalService\AppData\Roaming
1344 svchost.exe 0x21f1f303700 CommonProgramFiles C:\Program Files\Common Files
1344 svchost.exe 0x21f1f303700 CommonProgramFiles(x86) C:\Program Files (x86)\Common Files
1344 svchost.exe 0x21f1f303700 CommonProgramFiles6432 C:\Program Files\Common Files
1344 svchost.exe 0x21f1f303700 COMPUTERNAME DESKTOP-S4X7V6I
1344 svchost.exe 0x21f1f303700 ComSpec C:\Windows\system32\cmd.exe
1344 svchost.exe 0x21f1f303700 DriverData C:\Windows\system32\Drivers\DriverData
1344 svchost.exe 0x21f1f303700 LOCALAPPDATA C:\Windows\ServiceProfiles\LocalService\AppData\Local
1344 svchost.exe 0x21f1f303700 NUMBER_OF_PROCESSORS 2
1344 svchost.exe 0x21f1f303700 OS Windows_NT
1344 svchost.exe 0x21f1f303700 Path C:\Windows\system32;C:\Windows;C:\Windows\System32\WBem;C:\Windows\System32\WindowsPowerShell\v1.0;C:\Windows\System32\OpenSSH;C:\Windows\ServiceProfiles\LocalService\AppData\Local\Microsoft\Windows\DeliveryOptimization
1344 svchost.exe 0x21f1f303700 PATHTEXT _COM_,EXE_,BAT_,CMD_,VBS_,VBE_,JS_,JSE_,WSF_,WSH_,MSC
1344 svchost.exe 0x21f1f303700 PROCESSOR_ARCHITECTURE AMD64
1344 svchost.exe 0x21f1f303700 PROCESSOR_IDENTIFIER Intel64 Family 6 Model 142 Stepping 12, GenuineIntel
1344 svchost.exe 0x21f1f303700 PROCESSOR_LEVEL 6
1344 svchost.exe 0x21f1f303700 PROCESSOR_REVISION B6C
1344 svchost.exe 0x21f1f303700 ProgramData C:\ProgramData
1344 svchost.exe 0x21f1f303700 ProgramFiles(x86) C:\Program Files (x86)
1344 svchost.exe 0x21f1f303700 ProgramFiles C:\Program Files
1344 svchost.exe 0x21f1f303700 ProgramFilesCommon(x86) C:\Program Files\Common Files
1344 svchost.exe 0x21f1f303700 ProgramFilesCommon C:\Program Files\Common Files
1344 svchost.exe 0x21f1f303700 SystemRoot C:\Windows
1344 svchost.exe 0x21f1f303700 TEMP C:\Windows\TEMP;C:\Windows\TEMP\LOCALS-1\AppData\Local\Temp
1344 svchost.exe 0x21f1f303700 TMP C:\Windows\TEMP;C:\Windows\TEMP\LOCALS-1\AppData\Local\Temp
1344 svchost.exe 0x21f1f303700 USERDOMAIN NT AUTHORITY
1344 svchost.exe 0x21f1f303700 USERNAME LOCAL SERVICE
1344 svchost.exe 0x21f1f303700 USERPROFILE C:\Windows\ServiceProfiles\LocalService
1344 svchost.exe 0x21f1f303700 AllUsersProfile C:\Windows\AllUsersProfile
1344 svchost.exe 0x21f1f303700 APPDATA C:\Windows\ServiceProfiles\LocalService\AppData\Roaming
1344 svchost.exe 0x21f1f303700 CommonProgramFiles C:\Program Files\Common Files
1344 svchost.exe 0x21f1f303700 CommonProgramFiles(x86) C:\Program Files (x86)\Common Files
1344 svchost.exe 0x21f1f303700 CommonProgramFiles6432 C:\Program Files\Common Files
1368 svchost.exe 0x2a061c03700 AllUsersProfile C:\ProgramData
1368 svchost.exe 0x2a061c03700 APPDATA C:\Windows\ServiceProfiles\LocalService\AppData\Roaming
1368 svchost.exe 0x2a061c03700 CommonProgramFiles C:\Program Files\Common Files
1368 svchost.exe 0x2a061c03700 CommonProgramFiles(x86) C:\Program Files (x86)\Common Files
1368 svchost.exe 0x2a061c03700 CommonProgramFiles6432 C:\Program Files\Common Files
```

*Figure 5c Volatility windows.envars plugin*

```

1488 svchost.exe 0x27346808740 CommonProgramFiles(x86) C:\Program Files (x86)\Common Files
1488 svchost.exe 0x27446808740 CommonProgram6432 C:\Program Files\Common Files
1488 svchost.exe 0x27446808740 COMPUTERNAME DESKTOP-54K76V1
1488 svchost.exe 0x27446808740 DrvData C:\Windows\System32\Drivers\DriverData
1488 svchost.exe 0x27446808740 DriverData C:\Windows\System32\Drivers\DriverData
1488 svchost.exe 0x27446808740 LOCALAPDATA C:\Windows\system32\config\systemprofile\AppData\Local
1488 svchost.exe 0x27446808740 NUMBER_OF_PROCESSORS 2
1488 svchost.exe 0x27446808740 OS Windows_NT
1488 svchost.exe 0x27446808740 Path C:\Windows\system32;c:\Windows;c:\Windows\System32\WindowsPowerShell\v1.0;c:\Windows\System32\OpenSSH;c:\Windows\system32\config\systemprofile\AppData\Local\Microsoft\WindowsApps
1488 svchost.exe 0x27446808740 PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
1488 svchost.exe 0x27446808740 PROCESSOR_ARCHITECTURE AMD64
1488 svchost.exe 0x27446808740 PROCESSOR_IDENTIFIER Intel64 Family 6 Model 142 Stepping 12, GenuineIntel
1488 svchost.exe 0x27446808740 PROCESSOR_LEVEL 6
1488 svchost.exe 0x27446808740 PROCESSOR_REVISION 8e0c
1488 svchost.exe 0x27446808740 ProgramData C:\Program Files
1488 svchost.exe 0x27446808740 ProgramFiles(x86) C:\Program Files (x86)
1488 svchost.exe 0x27446808740 ProgramFiles6432 C:\Program Files
1488 svchost.exe 0x27446808740 PUBLIC C:\Users\Public
1488 svchost.exe 0x27446808740 SystemDrive C:
1488 svchost.exe 0x27446808740 SystemRoot C:\Windows
1488 svchost.exe 0x27446808740 TMP C:\Windows\TEMP
1488 svchost.exe 0x27446808740 USERDOMAIN C:\Windows
1488 svchost.exe 0x27446808740 WORKGROUP
1488 svchost.exe 0x27446808740 USERNAME DESKTOP-54K76V1
1488 svchost.exe 0x27446808740 WORKERNAME C:\Windows\system32\config\systemprofile
1488 svchost.exe 0x27446808740 windir C:\Windows
1488 svchost.exe 0x27446808740 wkdir C:\Windows
1508 svchost.exe 0x1178f8c8740 ALLUSERSPROFILE C:\ProgramData
1508 svchost.exe 0x1178f8c8740 APPDATA C:\Windows\System32\config\systemprofile\TempData\Roaming
1508 svchost.exe 0x1178f8c8740 COMPUTERNAME DESKTOP-54K76V1
1508 svchost.exe 0x1178f8c8740 DrvData C:\Windows\System32\Drivers\DriverData
1508 svchost.exe 0x1178f8c8740 LOCALAPDATA C:\Windows\system32\config\systemprofile\AppData\Local
1508 svchost.exe 0x1178f8c8740 NUMBER_OF_PROCESSORS 2
1508 svchost.exe 0x1178f8c8740 OS Windows_NT
1508 svchost.exe 0x1178f8c8740 Path C:\Windows\System32;c:\Windows;c:\Windows\System32\WindowsPowerShell\v1.0;c:\Windows\System32\OpenSSH;c:\Windows\system32\config\systemprofile\AppData\Local\Microsoft\WindowsApps
1508 svchost.exe 0x1178f8c8740 PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
1508 svchost.exe 0x1178f8c8740 PROCESSOR_ARCHITECTURE AMD64
1508 svchost.exe 0x1178f8c8740 PROCESSOR_IDENTIFIER Intel64 Family 6 Model 142 Stepping 12, GenuineIntel
1508 svchost.exe 0x1178f8c8740 PROCESSOR_LEVEL 6
1508 svchost.exe 0x1178f8c8740 PROCESSOR_REVISION 8e0c
1508 svchost.exe 0x1178f8c8740 ProgramData C:\Program Data
1508 svchost.exe 0x1178f8c8740 ProgramFiles(x86) C:\Program Files (x86)
1508 svchost.exe 0x1178f8c8740 ProgramFiles6432 C:\Program Files
1508 svchost.exe 0x1178f8c8740 PSModulePath %ProgramFiles%\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules
1508 svchost.exe 0x1178f8c8740 PUBLIC C:\Users\Public
1508 svchost.exe 0x1178f8c8740 SystemDrive C:
1508 svchost.exe 0x1178f8c8740 SystemRoot C:\Windows
1508 svchost.exe 0x1178f8c8740 TMP C:\Windows\TEMP
1508 svchost.exe 0x1178f8c8740 USERDOMAIN C:\Windows
1508 svchost.exe 0x1178f8c8740 WORKGROUP

```

Figure 57 Volatility windows.envars plugin

```

2292 svchost.exe 0x1b158a03780 USERPROFILE C:\Windows\ServiceProfiles\localService
2292 svchost.exe 0x1b158a03780 windir C:\Windows
2376 svchost.exe 0x2544f603780 AppData C:\Windows\ServiceProfiles\localService\AppData\Roaming
2376 svchost.exe 0x2544f603780 APPDATA C:\Windows\System32\config\systemprofile\AppData\Roaming
2376 svchost.exe 0x2544f603780 CommonProgramFiles C:\Program Files\Common Files
2376 svchost.exe 0x2544f603780 CommonProgramFiles(x86) C:\Program Files (x86)\Common Files
2376 svchost.exe 0x2544f603780 ComputerName DESKTOP-54K76V1
2376 svchost.exe 0x2544f603780 ComSpec C:\Windows\system32\cmd.exe
2376 svchost.exe 0x2544f603780 DrvData C:\Windows\System32\Drivers\DriverData
2376 svchost.exe 0x2544f603780 LOCALAPDATA C:\Windows\ServiceProfiles\localService\AppData\Local
2376 svchost.exe 0x2544f603780 NUMBER_OF_PROCESSORS 2
2376 svchost.exe 0x2544f603780 OS Windows_NT
2376 svchost.exe 0x2544f603780 Path C:\Windows\System32;c:\Windows;c:\Windows\System32\WindowsPowerShell\v1.0;c:\Windows\System32\OpenSSH;c:\Windows\ServiceProfiles\localService\AppData\Local\Microsoft\WindowsApps
2376 svchost.exe 0x2544f603780 PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
2376 svchost.exe 0x2544f603780 PROCESSOR_ARCHITECTURE AMD64
2376 svchost.exe 0x2544f603780 PROCESSOR_IDENTIFIER Intel64 Family 6 Model 142 Stepping 12, GenuineIntel
2376 svchost.exe 0x2544f603780 PROCESSOR_LEVEL 6
2376 svchost.exe 0x2544f603780 PROCESSOR_REVISION 8e0c
2376 svchost.exe 0x2544f603780 ProgramData C:\Program Data
2376 svchost.exe 0x2544f603780 ProgramFiles(x86) C:\Program Files (x86)
2376 svchost.exe 0x2544f603780 ProgramFiles6432 C:\Program Files
2376 svchost.exe 0x2544f603780 PSModulePath %ProgramFiles%\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules
2376 svchost.exe 0x2544f603780 PUBLIC C:\Users\Public
2376 svchost.exe 0x2544f603780 SystemDrive C:
2376 svchost.exe 0x2544f603780 SystemRoot C:\Windows
2376 svchost.exe 0x2544f603780 TEMP C:\Windows\TEMP
2376 svchost.exe 0x2544f603780 USERDOMAIN C:\Windows\TEMP
2376 svchost.exe 0x2544f603780 WORKGROUP
2464 svchost.exe 0x208a1803780 LOCALAPDATA C:\Windows\LocalService\AppData\Local
2464 svchost.exe 0x208a1803780 ALLUSERSPROFILE C:\ProgramData
2464 svchost.exe 0x208a1803780 APPDATA C:\Windows\ServiceProfiles\LocalService\AppData\Roaming
2464 svchost.exe 0x208a1803780 COMPUTERNAME DESKTOP-54K76V1
2464 svchost.exe 0x208a1803780 DrvData C:\Windows\System32\Drivers\DriverData
2464 svchost.exe 0x208a1803780 LOCALAPDATA C:\Windows\ServiceProfiles\localService\AppData\Local
2464 svchost.exe 0x208a1803780 NUMBER_OF_PROCESSORS 2
2464 svchost.exe 0x208a1803780 OS Windows_NT
2464 svchost.exe 0x208a1803780 Path C:\Windows\System32;c:\Windows;c:\Windows\System32\WindowsPowerShell\v1.0;c:\Windows\System32\OpenSSH;c:\Windows\ServiceProfiles\localService\AppData\Local\Microsoft\WindowsApps
2464 svchost.exe 0x208a1803780 PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
2464 svchost.exe 0x208a1803780 PROCESSOR_ARCHITECTURE AMD64
2464 svchost.exe 0x208a1803780 PROCESSOR_IDENTIFIER Intel64 Family 6 Model 142 Stepping 12, GenuineIntel
2464 svchost.exe 0x208a1803780 PROCESSOR_LEVEL 6
2464 svchost.exe 0x208a1803780 PROCESSOR_REVISION 8e0c
2464 svchost.exe 0x208a1803780 ProgramData C:\Program Data
2464 svchost.exe 0x208a1803780 ProgramFiles(x86) C:\Program Files (x86)
2464 svchost.exe 0x208a1803780 ProgramFiles6432 C:\Program Files
2464 svchost.exe 0x208a1803780 PSModulePath %ProgramFiles%\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules
2464 svchost.exe 0x208a1803780 PUBLIC C:\Users\Public

```

Figure 58 Volatility windows.envars plugin

```
0x00 TextInputHost 0x1007ab5f800 USERPROFILE C:\Users\student
0x00 TextInputHost 0x1907ba03900 windir C:\Windows
0x00 svchost.exe 0x27558003700 ALLUSERSPROFILE C:\ProgramData
0x00 svchost.exe 0x27558003700 APPDATA C:\Windows\ServiceProfiles\LocalService\AppData\Roaming
0x00 svchost.exe 0x27558003700 CommonProgramWFiles C:\Program Files\Common Files
0x00 svchost.exe 0x27558003700 CommonProgramFiles(x86) C:\Program Files (x86)\Common Files
0x00 svchost.exe 0x27558003700 COMPUTERNAME DESKTOP-54K70V1
0x00 svchost.exe 0x27558003700 DEPAGEDATA C:\Windows\System32\Drivers\DriverData
0x00 svchost.exe 0x27558003700 DriverData C:\Windows\System32\Drivers\DriverData
0x00 svchost.exe 0x27558003700 LOCALAPOLTA C:\Windows\ServiceProfiles\LocalService\AppData\Local
0x00 svchost.exe 0x27558003700 NUMBER_OF_PROCESSORS 2
0x00 svchost.exe 0x27558003700 PWD C:\Windows\System32\WindowsPowerShell\v1.0;C:\Windows\System32\OpenSSH;C:\Windows\ServiceProfiles\LocalService\AppData\Local\Microsoft\WindowsApps
0x00 svchost.exe 0x27558003700 Path C:\Windows\system32\WindowsPowerShell\v1.0;C:\Windows\System32\WindowsPowerShell\v1.0\Modules;C:\Windows\System32\WindowsPowerShell\v1.0\Modules;C:\Windows\System32\OpenSSH;C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\WindowsApps
0x00 svchost.exe 0x27558003700 PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
0x00 svchost.exe 0x27558003700 PROCESSOR_ARCHITECTURE AMD64
0x00 svchost.exe 0x27558003700 PROCESSOR_IDENTIFIER Intel64 Family 6 Model 142 Stepping 12, GenuineIntel
0x00 svchost.exe 0x27558003700 PROCESSOR_LEVEL 6
0x00 svchost.exe 0x27558003700 PROCESSOR_REVISION 8e0c
0x00 svchost.exe 0x27558003700 ProgramData C:\ProgramData
0x00 svchost.exe 0x27558003700 ProgramFiles C:\Program Files
0x00 svchost.exe 0x27558003700 ProgramFiles(x86) C:\Program Files (x86)
0x00 svchost.exe 0x27558003700 ProgramFiles(x86)\Common Files C:\Program Files (x86)\Common Files
0x00 svchost.exe 0x27558003700 ProgramFiles(x86)\System C:\Program Files (x86)\System
0x00 svchost.exe 0x27558003700 PUBLIC C:\Users\Public
0x00 svchost.exe 0x27558003700 SystemDrive C:
0x00 svchost.exe 0x27558003700 SystemRoot C:\Windows
0x00 svchost.exe 0x27558003700 TEMP C:\ProgramData\Microsoft\Search\Temp\usgrhsrvc
0x00 svchost.exe 0x27558003700 TMP C:\ProgramData\Microsoft\Search\Temp\usgrhsrvc
0x00 svchost.exe 0x27558003700 USERDOMAIN WORKGROUP
0x00 svchost.exe 0x27558003700 USERNAME DESKTOP-54K70V1
0x00 svchost.exe 0x27558003700 USERPROFILE C:\Windows\system32\config\systemprofile
0x00 svchost.exe 0x27558003700 windir C:\Windows
0x00 svchost.exe 0x1e04e203740 ALLUSERSPROFILE C:\ProgramData
0x00 svchost.exe 0x1e04e203740 APPDATA C:\Windows\ServiceProfiles\LocalService\AppData\Roaming
0x00 svchost.exe 0x1e04e203740 CommonProgramWFiles C:\Program Files\Common Files
0x00 svchost.exe 0x1e04e203740 CommonProgramFiles(x86) C:\Program Files (x86)\Common Files
0x00 svchost.exe 0x1e04e203740 CommonProgramFiles(x86)\Common Files C:\Program Files (x86)\Common Files
0x00 svchost.exe 0x1e04e203740 ComSpec C:\Windows\system32\cmd.exe
0x00 svchost.exe 0x1e04e203740 DriverData C:\Windows\System32\Drivers\DriverData
0x00 svchost.exe 0x1e04e203740 LOCALAPOLTA C:\Windows\System32\Config\SystemProfile\AppData\Local
0x00 svchost.exe 0x1e04e203740 NUMBER_OF_PROCESSORS 2
0x00 svchost.exe 0x1e04e203740 OS Windows_NT
0x00 svchost.exe 0x1e04e203740 Path C:\Windows\system32\WindowsPowerShell\v1.0\Modules;C:\Windows\System32\WindowsPowerShell\v1.0\Modules
0x00 svchost.exe 0x1e04e203740 PUBLIC C:\Users\Public
0x00 svchost.exe 0x1e04e203740 SystemDrive C:
0x00 svchost.exe 0x1e04e203740 SystemRoot C:\Windows
0x00 svchost.exe 0x1e04e203740 TEMP C:\ProgramData\Microsoft\Search\Temp\usgrhsrvc
0x00 svchost.exe 0x1e04e203740 TMP C:\ProgramData\Microsoft\Search\Temp\usgrhsrvc
0x00 svchost.exe 0x1e04e203740 USERDOMAIN WORKGROUP
0x00 svchost.exe 0x1e04e203740 USERNAME DESKTOP-54K70V1
0x00 svchost.exe 0x1e04e203740 USERPROFILE C:\Windows\system32\config\systemprofile
0x00 svchost.exe 0x1e04e203740 windir C:\Windows
0x00 SearchProtocol 0x2a09b0d45f80 ComSpec C:\Windows\System32\cmd.exe
0x00 SearchProtocol 0x2a09b0d45f80 DriveData C:\Windows\System32\Drivers\DriverData
0x00 SearchProtocol 0x2a09b0d45f80 LOCALAPOLTA C:\Windows\system32\Config\SystemProfile\AppData\Local
0x00 SearchProtocol 0x2a09b0d45f80 NUMBER_OF_PROCESSORS 2
0x00 SearchProtocol 0x2a09b0d45f80 PWD C:\Windows\System32\WindowsPowerShell\v1.0;C:\Windows\System32\OpenSSH;C:\Windows\System32\Config\SystemProfile\AppData\Local\Microsoft\WindowsApps
0x00 SearchProtocol 0x2a09b0d45f80 Path C:\Windows\system32\WindowsPowerShell\v1.0\Modules;C:\Windows\System32\WindowsPowerShell\v1.0\Modules;C:\Windows\System32\OpenSSH;C:\Windows\System32\Config\SystemProfile\AppData\Local\Microsoft\WindowsApps
0x00 SearchProtocol 0x2a09b0d45f80 PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
0x00 SearchProtocol 0x2a09b0d45f80 PROCESSOR_ARCHITECTURE AMD64
0x00 SearchProtocol 0x2a09b0d45f80 PROCESSOR_IDENTIFIER Intel64 Family 6 Model 142 Stepping 12, GenuineIntel
0x00 SearchProtocol 0x2a09b0d45f80 PROCESSOR_LEVEL 6
0x00 SearchProtocol 0x2a09b0d45f80 PROCESSOR_REVISION 8e0c
0x00 SearchProtocol 0x2a09b0d45f80 ProgramData C:\ProgramData
0x00 SearchProtocol 0x2a09b0d45f80 ProgramFiles C:\Program Files
0x00 SearchProtocol 0x2a09b0d45f80 ProgramFiles(x86) C:\Program Files (x86)
0x00 SearchProtocol 0x2a09b0d45f80 ProgramFiles(x86)\Common Files C:\Program Files (x86)\Common Files
0x00 SearchProtocol 0x2a09b0d45f80 ProgramFiles(x86)\System C:\Program Files (x86)\System
0x00 SearchProtocol 0x2a09b0d45f80 PUBLIC C:\Users\Public
0x00 SearchProtocol 0x2a09b0d45f80 SystemDrive C:
0x00 SearchProtocol 0x2a09b0d45f80 SystemRoot C:\Windows
0x00 SearchProtocol 0x2a09b0d45f80 TEMP C:\ProgramData\Microsoft\Search\Temp\usgrhsrvc
0x00 SearchProtocol 0x2a09b0d45f80 TMP C:\ProgramData\Microsoft\Search\Temp\usgrhsrvc
0x00 SearchProtocol 0x2a09b0d45f80 USERDOMAIN WORKGROUP
0x00 SearchProtocol 0x2a09b0d45f80 USERNAME DESKTOP-54K70V1
0x00 SearchProtocol 0x2a09b0d45f80 USERPROFILE C:\Windows\system32\config\systemprofile
0x00 SearchProtocol 0x2a09b0d45f80 windir C:\Windows
0x00 SearchProtocol 0x2a6d24f6f500 ALLUSERSPROFILE C:\ProgramData
0x00 SearchProtocol 0x2a6d24f6f500 APPDATA C:\Windows\System32\Config\SystemProfile\AppData\Roaming
0x00 SearchProtocol 0x2a6d24f6f500 CommonProgramWFiles C:\Program Files\Common Files
0x00 SearchProtocol 0x2a6d24f6f500 CommonProgramFiles(x86) C:\Program Files (x86)\Common Files
0x00 SearchProtocol 0x2a6d24f6f500 ComSpec C:\Windows\system32\cmd.exe
0x00 SearchProtocol 0x2a6d24f6f500 DriverData C:\Windows\System32\Drivers\DriverData
0x00 SearchProtocol 0x2a6d24f6f500 LOCALAPOLTA C:\Windows\system32\Config\SystemProfile\AppData\Local
0x00 SearchProtocol 0x2a6d24f6f500 NUMBER_OF_PROCESSORS 2
0x00 SearchProtocol 0x2a6d24f6f500 OS Windows_NT
0x00 SearchProtocol 0x2a6d24f6f500 Path C:\Windows\system32\WindowsPowerShell\v1.0;C:\Windows\System32\OpenSSH;C:\Windows\System32\Config\SystemProfile\AppData\Local\Microsoft\WindowsApps
0x00 SearchProtocol 0x2a6d24f6f500 PUBLIC C:\Users\Public
0x00 SearchProtocol 0x2a6d24f6f500 SystemDrive C:
0x00 SearchProtocol 0x2a6d24f6f500 SystemRoot C:\Windows
0x00 SearchProtocol 0x2a6d24f6f500 TEMP C:\ProgramData\Microsoft\Search\Temp\usgrhsrvc
0x00 SearchProtocol 0x2a6d24f6f500 TMP C:\ProgramData\Microsoft\Search\Temp\usgrhsrvc
0x00 SearchProtocol 0x2a6d24f6f500 USERDOMAIN WORKGROUP
0x00 SearchProtocol 0x2a6d24f6f500 USERNAME DESKTOP-54K70V1
0x00 SearchProtocol 0x2a6d24f6f500 USERPROFILE C:\Windows\system32\config\systemprofile
0x00 SearchProtocol 0x2a6d24f6f500 windir C:\Windows
```

Figure 55 Volatility windows.envars plugin

```
0x00 SearchProtocol 0x2a09b0d45f80 ComSpec C:\Windows\System32\cmd.exe
0x00 SearchProtocol 0x2a09b0d45f80 DriveData C:\Windows\System32\Drivers\DriverData
0x00 SearchProtocol 0x2a09b0d45f80 LOCALAPOLTA C:\Windows\system32\Config\SystemProfile\AppData\Local
0x00 SearchProtocol 0x2a09b0d45f80 NUMBER_OF_PROCESSORS 2
0x00 SearchProtocol 0x2a09b0d45f80 PWD C:\Windows\System32\WindowsPowerShell\v1.0;C:\Windows\System32\OpenSSH;C:\Windows\System32\Config\SystemProfile\AppData\Local\Microsoft\WindowsApps
0x00 SearchProtocol 0x2a09b0d45f80 Path C:\Windows\system32\WindowsPowerShell\v1.0\Modules;C:\Windows\System32\WindowsPowerShell\v1.0\Modules;C:\Windows\System32\OpenSSH;C:\Windows\System32\Config\SystemProfile\AppData\Local\Microsoft\WindowsApps
0x00 SearchProtocol 0x2a09b0d45f80 PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
0x00 SearchProtocol 0x2a09b0d45f80 PROCESSOR_ARCHITECTURE AMD64
0x00 SearchProtocol 0x2a09b0d45f80 PROCESSOR_IDENTIFIER Intel64 Family 6 Model 142 Stepping 12, GenuineIntel
0x00 SearchProtocol 0x2a09b0d45f80 PROCESSOR_LEVEL 6
0x00 SearchProtocol 0x2a09b0d45f80 PROCESSOR_REVISION 8e0c
0x00 SearchProtocol 0x2a09b0d45f80 ProgramData C:\ProgramData
0x00 SearchProtocol 0x2a09b0d45f80 ProgramFiles C:\Program Files
0x00 SearchProtocol 0x2a09b0d45f80 ProgramFiles(x86) C:\Program Files (x86)
0x00 SearchProtocol 0x2a09b0d45f80 ProgramFiles(x86)\Common Files C:\Program Files (x86)\Common Files
0x00 SearchProtocol 0x2a09b0d45f80 ProgramFiles(x86)\System C:\Program Files (x86)\System
0x00 SearchProtocol 0x2a09b0d45f80 PUBLIC C:\Users\Public
0x00 SearchProtocol 0x2a09b0d45f80 SystemDrive C:
0x00 SearchProtocol 0x2a09b0d45f80 SystemRoot C:\Windows
0x00 SearchProtocol 0x2a09b0d45f80 TEMP C:\ProgramData\Microsoft\Search\Temp\usgrhsrvc
0x00 SearchProtocol 0x2a09b0d45f80 TMP C:\ProgramData\Microsoft\Search\Temp\usgrhsrvc
0x00 SearchProtocol 0x2a09b0d45f80 USERDOMAIN WORKGROUP
0x00 SearchProtocol 0x2a09b0d45f80 USERNAME DESKTOP-54K70V1
0x00 SearchProtocol 0x2a09b0d45f80 USERPROFILE C:\Windows\system32\config\systemprofile
0x00 SearchProtocol 0x2a09b0d45f80 windir C:\Windows
0x00 SearchProtocol 0x2a6d24f6f500 ALLUSERSPROFILE C:\ProgramData
0x00 SearchProtocol 0x2a6d24f6f500 APPDATA C:\Windows\System32\Config\SystemProfile\AppData\Roaming
0x00 SearchProtocol 0x2a6d24f6f500 CommonProgramWFiles C:\Program Files\Common Files
0x00 SearchProtocol 0x2a6d24f6f500 CommonProgramFiles(x86) C:\Program Files (x86)\Common Files
0x00 SearchProtocol 0x2a6d24f6f500 ComSpec C:\Windows\system32\cmd.exe
0x00 SearchProtocol 0x2a6d24f6f500 DriverData C:\Windows\System32\Drivers\DriverData
0x00 SearchProtocol 0x2a6d24f6f500 LOCALAPOLTA C:\Windows\system32\Config\SystemProfile\AppData\Local
0x00 SearchProtocol 0x2a6d24f6f500 NUMBER_OF_PROCESSORS 2
0x00 SearchProtocol 0x2a6d24f6f500 OS Windows_NT
0x00 SearchProtocol 0x2a6d24f6f500 Path C:\Windows\system32\WindowsPowerShell\v1.0;C:\Windows\System32\OpenSSH;C:\Windows\System32\Config\SystemProfile\AppData\Local\Microsoft\WindowsApps
0x00 SearchProtocol 0x2a6d24f6f500 PUBLIC C:\Users\Public
0x00 SearchProtocol 0x2a6d24f6f500 SystemDrive C:
0x00 SearchProtocol 0x2a6d24f6f500 SystemRoot C:\Windows
0x00 SearchProtocol 0x2a6d24f6f500 TEMP C:\ProgramData\Microsoft\Search\Temp\usgrhsrvc
0x00 SearchProtocol 0x2a6d24f6f500 TMP C:\ProgramData\Microsoft\Search\Temp\usgrhsrvc
0x00 SearchProtocol 0x2a6d24f6f500 USERDOMAIN WORKGROUP
0x00 SearchProtocol 0x2a6d24f6f500 USERNAME DESKTOP-54K70V1
0x00 SearchProtocol 0x2a6d24f6f500 USERPROFILE C:\Windows\system32\config\systemprofile
0x00 SearchProtocol 0x2a6d24f6f500 windir C:\Windows
```

Figure c0 Volatility windows.envars plugin

## Interpretation Notes

**Multiple users:** SYSTEM, LOCAL SERVICE, student, Font Driver Host.

**Temp directories:** Vary per user; important for tracing malware or dropped executables.

**Script execution paths:** Paths include PowerShell and CMD — possible script-based activity.

**User focus:** student session is the active interactive user — important for tracing inputs or attacks.

## Results and Findings

- Only **core system processes** were running: System, winlogon.exe, services.exe, csrss.exe, svchost.exe, etc.
- No third-party or internet-related applications detected.
- No suspicious or unknown processes in pslist, pstree, or psscan.
- The system appeared **freshly booted**, based on process start times and registry keys.
- **No malware indicators** found: malfind, ssdt, and modules were clean.
- **USB and network services were configured**, but not active — shows no external activity had taken place.
- No browser history, cached files, or temporary data.

## Memory Dump 2 (After Internet Activity)

- New processes observed: firefox.exe, FTK Imager.exe, SearchUI.exe, ScreenSketch.exe, confirming **active user session**.
- Network services like DNSCache, WinDefend, WpnService, and SharedAccess were running, proving **internet use**.
- Registry keys like USBSTOR, Tcpip, LanmanWorkstation, and MountedDevices confirmed:
  - USB devices were used.
  - Networking and file sharing were active.
- **DLL analysis** revealed browser-related and forensic tool libraries:
  - Mozilla libraries loaded in firefox.exe.
  - Qt5 libraries in FTK Imager.exe.

- **Filescan** revealed:
  - Logs and cache from Opera and Chrome.
  - Suspicious driver ad\_driver-10.sys in the Temp folder.
- cmdline plugin confirmed FTK Imager and Firefox were run manually.
- envars revealed active student user, temporary folders in use, and potential scripting capability (PowerShell, CMD in PATH).
- malfind detected:
  - Suspicious code injection in MsMpEng.exe and SearchHost.exe.
  - Presence of **shellcode patterns** and memory marked as PAGE\_EXECUTE\_READWRITE.
- ssdt showed **potential rootkit behavior**: multiple system calls mapped to the same memory address.
- Registry hives like NTUSER.DAT, UsrClass.dat, AppRepository, and WebCacheV01.dat confirmed:
  - App usage
  - File interaction
  - Internet browsing
- UserAssist plugin failed due to registry parsing issue, but activity was proven through other artifacts.
- Virtualization confirmed with vmtoolsd.exe.

## Conclusion

This digital forensics investigation was performed on two memory dumps captured from a **Windows 11 system** using industry-standard forensic tools: **FTK Imager** (for memory acquisition) and **Volatility 3** (for in-depth memory analysis). One memory image was collected in a clean, unused state, and the second after active internet use.

The **first memory dump** reflected a clean environment with only default system processes running. No user interaction, network activity, or third-party applications were present. Memory analysis showed no signs of tampering, malware, or code injection, confirming a stable system state after boot.

The **second memory dump**, taken after browsing and user interaction, revealed multiple layers of activity:

- Applications such as **Firefox** and **FTK Imager** were actively executed.
- Browser caches, session logs, registry entries, and user profile artifacts confirmed extensive system use.
- Suspicious evidence such as the unsigned driver ad\_driver-10.sys in the Temp folder was discovered.
- malfind and ssdt plugins identified signs of memory injection and possible rootkit hooks — indicative of **stealthy or fileless malware behavior**.
- The student user account was verified as the active session through environment variables and command-line traces.

This investigation proves the effectiveness of **memory forensics** in detecting volatile evidence that may never reach the hard drive. The combination of **FTK Imager** for acquisition and **Volatility 3** for plugin-based artifact extraction allowed detailed observation of system behavior before and after activity. This approach is essential in modern threat hunting and incident response, especially on platforms like **Windows 11** where attackers may hide in memory without leaving disk traces.

## References

Tool	Official Download Link
<b>FTK Imager</b>	<a href="https://accessdata.com/product-download/ftk-imager">https://accessdata.com/product-download/ftk-imager</a>
<b>Volatility 3</b>	<a href="https://github.com/volatilityfoundation/volatility3">https://github.com/volatilityfoundation/volatility3</a>
<b>Windows 11 ISO</b>	<a href="https://www.microsoft.com/software-download/windows11">https://www.microsoft.com/software-download/windows11</a>