Memory Forensics Slayer:101

By WHMIR

FOR CSLU Brunei 2025

$- echo Me

- Cybersecurity graduate
- Security Consultant at Bluesify
- RE:UN10N Member
- Malaysia Cybersecurity Camp Alumni and Agent
- Finalist ACS 2023

Agenda

- Forensics 101
- Memory Forensics
- Volatility & MemProcFS
- Hands-On

Objective

- Understand what memory forensics is
- Learn where to extract information from memory
- Explore how memory analysis is done
- Hands-on: Volatility3 & MemProcFS usage

Forensics

What is Forensics?

- Process of colecting data, analyzing data, investigate data or recovering digital data
- Incident Respond Team or Security Operation Center (SOC) or Threat Hunting or Blue Teams

Forensics in CTF

Steganography (Embedded Image)	Email Analysis	Packet Analysis
Memory Analysis	Malware Analysis	File Cracking

🧠 **Real-World Insight**

- Steganography ≠ Forensics in Real World
- Threat Hunting / Incident Response = Real Forensics

What is Memory Forensics?

- Process of analyzing memory dumps to extract digital evidence (artifacts)
- Used in:
  - Malware analysis
  - Incident response
  - Threat hunting
- Focuses on volatile data (RAM)

Overview

```
├── 1️⃣ Acquisition
│   └── Capture RAM from live system
├── 2️⃣ Validation
│   └── Ensure integrity (hashes, format check)
├── 3️⃣ Analysis
│   ├── Use tools like Volatility / MemProcFS
│   ├── Extract artifacts (processes, connections)
│   └── Detect anomalies (malware, injections)
├── 4️⃣ Documentation
│   └── Record findings step-by-step
└── 5️⃣ Reporting
    └── Summarize conclusions and evidence
```

Where Do We Look?

- Key memory structures:
  - Processes
  - DLLs and Handles
  - Network connections
  - Registry hives
  - Kernel objects
  - Command history

How is it Done?

1. Acquire memory (e.g., with `DumpIt`, `AVML`, etc.)
2. Use forensic tools to analyze (e.g., Volatility3, MemProcFS)
3. Correlate artifacts
4. Report findings

Memory Dump Formats

Type	Format / Extension	Description
Raw Dump	`.raw`, `.bin`	Full byte-for-byte copy of RAM
Crash Dump	`.dmp`	Captured during system crash (Windows)
Hibernation File	`hiberfil.sys`	RAM saved when system hibernates
VMware Dump	`.vmem`	VM snapshot memory
Lime Dump	`.lime`	Linux memory, structured, forensics-friendly
ELF Core Dump	`.core`, `.elf`	Unix/Linux crash dump

Tool 1

Volatility3 Overview

- Python-based memory analysis framework
- Works on Windows, Linux, Mac memory dumps
- Modular plugin system
- Open-source

Demo File

https://shorturl.at/J4cJX

Installation Volatility3

```
mkdir -p envi
python3 -m venv vola
source vola/bin/activate
git clone https://github.com/volatilityfoundation/volatility3
cd volatility3
python3 vol.py -h
```

Optional

Make alias

```
echo "alias vol3='python3 /path/to/volatiltyfile/vol.py'"
vol3 -h
```

Process List

Define

- Snapshot of all process running in the system/host when the memory being capture

Purpose?

- To identify malicious process or root cause
  ** pslist = List all running processes
  ** pstree = Display parent and child relationship
  ** psscan = Identifies hidden or teminated proccess

Process List Command

```
vol3 -f <path/to/memory> windows.pslist
```

```
vol3 -f <path/to/memory> windows.psscan
```

```
vol3 -f <path/to/memory> windows.pstree
```

Process List Anatomy

```
┌──(vol3)─(kali㉿kali)-[~/Desktop/CSLU/tools]
└─$  python3 volatility3/vol.py -f ~/Desktop/CSLU/challenge/MemoryDump_Lab1.raw windows.pslist
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0xfa8000ca0040  80      570     N/A     False   2019-12-11 13:41:25.000000 UTC  N/A     Disabled
248     4       smss.exe        0xfa800148f040  3       37      N/A     False   2019-12-11 13:41:25.000000 UTC  N/A     Disabled
320     312     csrss.exe       0xfa800154f740  9       457     0       False   2019-12-11 13:41:32.000000 UTC  N/A     Disabled
368     360     csrss.exe       0xfa8000ca81e0  7       199     1       False   2019-12-11 13:41:33.000000 UTC  N/A     Disabled
376     248     psxss.exe       0xfa8001c45060  18      786     0       False   2019-12-11 13:41:33.000000 UTC  N/A     Disabled
416     360     winlogon.exe    0xfa8001c5f060  4       118     1       False   2019-12-11 13:41:34.000000 UTC  N/A     Disabled
424     312     wininit.exe     0xfa8001c5f630  3       75      0       False   2019-12-11 13:41:34.000000 UTC  N/A     Disabled
484     424     services.exe    0xfa8001c98530  13      219     0       False   2019-12-11 13:41:35.000000 UTC  N/A     Disabled
492     424     lsass.exe       0xfa8001ca0580  9       764     0       False   2019-12-11 13:41:35.000000 UTC  N/A     Disabled
500     424     lsm.exe 0xfa8001ca4b30  11      185     0       False   2019-12-11 13:41:35.000000 UTC  N/A     Disabled
```

PID: Process ID (unique identifier).

PPID: Parent Process ID (shows hierarchy).

Name: Executable name of the process.

Start Time: When the process started

Network List

Purpose?

- Identify active connection during memory capture
- Detect inbound/outbound connection

netstat = Equivalent to the netstat command on a live system.

netscan = Detects listening ports, remote IPs, PIDs.

Network List Command

```
vol3 -f <path/to/memory> windows.netstat
```

```
vol3 -f <path/to/memory> windows.netscan
```

```
└$ python3 tools/volatility3/vol.py -f challenge/MemoryDump_Lab1.raw windows.netstat
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
Offset  Proto    LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID

0×fa8001fe86e0  TCPv4   0.0.0.0 7       0.0.0.0 0       LISTENING       1416    TCPSVCS.EXE
0×fa8001fe86e0  TCPv6   ::      7       ::      0       LISTENING       1416    TCPSVCS.EXE
0×fa8001fe8010  TCPv4   0.0.0.0 7       0.0.0.0 0       LISTENING       1416    TCPSVCS.EXE
0×fa8001fe4ef0  TCPv4   0.0.0.0 9       0.0.0.0 0       LISTENING       1416    TCPSVCS.EXE
```

CommandLine History

Detect all commands being used by an attacker.
Understand the sequence of events (especialy for automation/scripting)
cmdline = command were passed to executed process when it execute.

CommandLine Command

```
vol3 -f <path/to/memory> windows.cmdline
```

- Alternative way to read what command being execute in console/terminal

  ```
  vol3 -f <path/to/memory> windows.cmdline | grep "cmd.exe"
  ```

```
└─$ python3 tools/volatility3/vol.py -f  challenge/MemoryDump_Lab1.raw windows.cmdline | grep cmd.exe
1984ressCmd.exe "C:\Windows\system32\cmd.exe"

┌──(vol3)─(kali㉿kali)-[~/Desktop/CSLU]
└─$ python3 tools/volatility3/vol.py -f  challenge/MemoryDump_Lab1.raw windows.handles --pid 1984
Volatility 3 Framework 2.26.2
```

```
vol3 -f <path/to/memory> windows.handles --pid 1984
vol3 -f <path/to/memory> windows.memmap --pid 1984 --dump
strings pid.1984.dump > cmd.txt
strings cmd.txt | grep SmartNet
```

```
└─$ strings cmd.txt -a 100 | grep "SmartNet"
APPDATA=C:\Users\SmartNet\AppData\Roaming
HOMEPATH=\Users\SmartNet
LOCALAPPDATA=C:\Users\SmartNet\AppData\Local
TEMP=C:\Users\SmartNet\AppData\Local\Temp
TMP=C:\Users\SmartNet\AppData\Local\Temp
USERDOMAIN=SmartNet-PC
USERNAME=SmartNet
USERPROFILE=C:\Users\SmartNet
C:\Users\SmartNet\Desktop\St4G3$1.bat
```

> Next step on next slide.

File List

DEFINE

Investigating files and file-related artifacts stored in memory.

PURPOSE

Detect suspicious or malicious files in memory.

Recover files loaded by processes or mapped to disk.

File List Command

```
vol3 -f <path/to/memory> windows.filescan
```

```
└─$ python3 tools/volatility3/vol.py -f  challenge/MemoryDump_Lab1.raw windows.filescan | grep St4G3
0×3edcfc20 100.0\Windows\System32\St4G3$1.bat
```

```
vol3 -f <path/to/memory> -o "/path/to/dir"  windows.dumpfiles --physaddr <offset>
```

```
└─$ python3 tools/volatility3/vol.py -f  challenge/MemoryDump_Lab1.raw -o .  windows.dumpfile --physadd 0×3edcfc20
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
Cache   FileObject      FileName        Result

DataSectionObject       0×3edcfc20      St4G3$1.bat     file.0×3edcfc20.0×fa8000e9ac40.DataSectionObject.St4G3$1.bat.dat

┌──(vol3)─(kali㉿kali)-[~/Desktop/CSLU]
└─$ ls
 challenge   cmd.txt  'file.0×3edcfc20.0×fa8000e9ac40.DataSectionObject.St4G3$1.bat.dat'   mem   pid.1984-1.dmp   pid.1984.dmp   tools

┌──(vol3)─(kali㉿kali)-[~/Desktop/CSLU]
└─$ strings file.0×3edcfc20.0×fa8000e9ac40.DataSectionObject.St4G3\$1.bat.dat
@ECHO OFF
ECHO ZmxhZ3t0aDFzXzFzX3RoM18xc3Rfc3Q0ZzMhIX0=
PAUSE
```

Registry Key

logical group of keys, subkeys, and values in the registry.

- Sometimes being use as persistence.
- SYSTEM: Stores system-wide configuration like services, drivers, and control sets.
- SOFTWARE: Stores software-specific settings, including installed applications and system configuration.

```
\SystemRoot\System32\Config\SYSTEM

\SystemRoot\System32\Config\SOFTWARE
```

Registry Key Command

registry.hivelist = to list al key.

registry.printkey = print specific key (SOFTWARE/SYSTEM)

```
python3 vol.py -f memdump.raw windows.registry.hivelist
```

```
—$ python3 tools/volatility3/vol.py -f  challenge/MemoryDump_Lab1.raw windows.registry.hivelist
olatility 3 Framework 2.26.2
rogress:  100.00               PDB scanning finished
ffset  FileFullPath    File output

×f8a00000d010          Disabled
×f8a000024010  \REGISTRY\MACHINE\SYSTEM        Disabled
×f8a00004e010  \REGISTRY\MACHINE\HARDWARE      Disabled
×f8a0000b9010  \??\C:\Users\SmartNet\AppData\Local\Microsoft\Windows\UsrClass.dat      Disabled
×f8a0000c1010  \??\C:\Users\SmartNet\ntuser.dat        Disabled
×f8a000264010  \Device\HarddiskVolume1\Boot\BCD        Disabled
×f8a001032010  \SystemRoot\System32\Config\SOFTWARE    Disabled
×f8a0012ff300  \SystemRoot\System32\Config\DEFAULT     Disabled
×f8a001491010  \SystemRoot\System32\Config\SECURITY    Disabled
```

From previous image we can't get credentials from SAM and SYTEM.

To done this, can use `hashdump`

```
python3 vol.py -f memdump.raw windows.hashdump
```

```
Administrator   500     aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
Guest   501     aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
SmartNet        1001    aad3b435b51404eeaad3b435b51404ee        4943abb39473a6f32c11301f4987e7e0
HomeGroupUser$  1002    aad3b435b51404eeaad3b435b51404ee        f0fc3d257814e08fea06e63c5762ebd5
Alissa Simpson  1003    aad3b435b51404eeaad3b435b51404ee        f4ff64c8baac57d22f22edc681055ba6
```

This hash can be crack using John the Ripper or Hashcat.

Environment (Envars/Env)

- Key-value pairs used by the OS and applications
- Define runtime environment (e.g., `PATH`, `TEMP`, `USERNAME`)
- Can reveal:
  - Usernames
  - Installed software paths
  - Malware persistences

Envars Command

```
python3 vol.py -f memdump.raw windows.envars
```

```
└─$ python3 tools/volatility3/vol.py -f  challenge/MemoryDump_Lab1.raw windows.envars
2260ressconhost.exe     0×3518f0PDB scanProgramW6432d   C:\Program Files
2260    conhost.exe     0×3518f0        PSModulePath    C:\Windows\system32\WindowsPow
2260    conhost.exe     0×3518f0        SystemDrive     C:
2260    conhost.exe     0×3518f0        SystemRoot      C:\Windows
2260    conhost.exe     0×3518f0        TEMP    C:\Windows\TEMP
2260    conhost.exe     0×3518f0        TMP     C:\Windows\TEMP
```

HANDS-ON

https://shorturl.at/9B4jG

>cslUPM

Challenge

1. What was the local IP address of the victim's machine?
2. What was the OS environment variable's value?
3. What was the Administrator's password?
4. Which process was most likely responsible for the initial exploit?
5. Suspicious processes opened network connections to external IPs. One of them starts with "2". Provide the ful IP.
6. A suspicious URL was present in process svchost.exe memory. Provide the ful URL that points to a PHP page hosted over a public IP (no FQDN).
7. Extract files from the initial process. One file has an MD5 hash ending with "528afe08e437765cc". When was this file first submitted for analysis on VirusTotal?

8. What is the name of the malicious executable referenced in registry hive '\WINDOWS\system32\config\software', and is a variant of ZeuS trojan?
9. The shelcode for Acrobat v7 downloads a file named e.exe from a specific URL. Provide the URL.

Answer

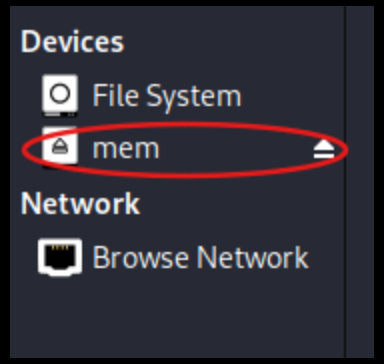
1. 192.168.0.176
2. Windows_NT
3. password
4. AcroRd32.exe
5. 193.104.22.71,212.150.164.203
6. http://193.104.22.71/~produkt/9j856f_4m9y8urb.php
7. f32aa81676c7391528afe08e437765cc
8. sdra64.exe
9. http://search-network-plus.com/load.php?a=a&st=Internet Explorer 6.0&e=2

BREAK Time!

Tool 2

MemProcFS Overview

- Mount the Artifact (Memory) Images into machine
- Ease analyse and finding evidence in File Exploreer and Notepad.
- MemProcFS will create VIRTUAL File System/Network File Explorer



MemProcFS Command

- For windows

```
memprocfs.exe -device <artifact.raw> -forensic 1”
```

```
C:\Windows\System32\cmd.exe - MemProcFS.exe -device ..\For-Challenge\Slide\sunsun.raw -forensic 1

C:\Users\playerz\Desktop\MemprocFS>MemProcFS.exe -device ..\For-Challenge\Slide\sunsun.raw -forensic 1
Initialized 64-bit Windows 10.0.19041
[FORENSIC] Built-in Yara rules from Elastic are disabled. Enable with: -license-accept-elastic-license-2-0
[PLUGIN]   Python initialization failed. Python 3.6 or later not found.
```

- For Linux

```
./memprocfs -device <artifact.raw> -mount /mnt/
```

```
└─$ ./memprocfs -device ../../challenge/MemoryDump_Lab1.raw -mount ../../mem
Initialized 64-bit Windows 6.1.7601

================================ MemProcFS ================================
```

How Does It Work?

- Uses **FUSE** (Filesystem in Userspace) to mount memory
- Memory dump becomes browsable: `/memprocfs/`
- Each process has a folder:
  - `/proc/<PID>/`
- Also exposes:
  - Kernel memory
  - DLLs
  - Handles
  - Network connections
  - Environment variables
  - Command lines

Sys

- System Information

Sys/proc Folder

- Process List of computer being capture during memory acquisation
- Similar to pslist and pstree in volatility.

sys > proc > proc.txt

```
Process                    Pid Parent   Flag User            Create Time              Exit Time
-----------------------------------------------------------------------------------------------------
- System                     4      0        SYSTEM          2019-12-11 13:41:25 UTC                  ***
-- smss.exe                 248      4        SYSTEM          2019-12-11 13:41:25 UTC                  ***
--- psxss.exe               376    248        SYSTEM          2019-12-11 13:41:33 UTC                  ***
- csrss.exe                 320    312        SYSTEM          2019-12-11 13:41:32 UTC                  ***
- wininit.exe               424    312        SYSTEM          2019-12-11 13:41:34 UTC                  ***
-- services.exe             484    424        SYSTEM          2019-12-11 13:41:35 UTC                  ***
--- taskhost.exe            296    484     U  SmartNet        2019-12-11 14:32:24 UTC                  ***
--- svchost.exe             472    484        LOCAL SERVICE   2019-12-11 13:41:47 UTC                  ***
--- SearchIndexer.          480    484        SYSTEM          2019-12-11 14:16:09 UTC                  ***
---- SearchFilterHo        1720    480        SYSTEM          2019-12-11 14:37:21 UTC                  ***
---- SearchProtocol        2524    480     U  Alissa Simpson  2019-12-11 14:37:21 UTC                  ***
---- SearchProtocol        2868    480        SYSTEM          2019-12-11 14:37:23 UTC                  ***
--- svchost.exe             588    484        SYSTEM          2019-12-11 13:41:39 UTC                  ***
```

Sys/Proc Folder

- View in command line/consoles

sys > proc > proc-v.txt

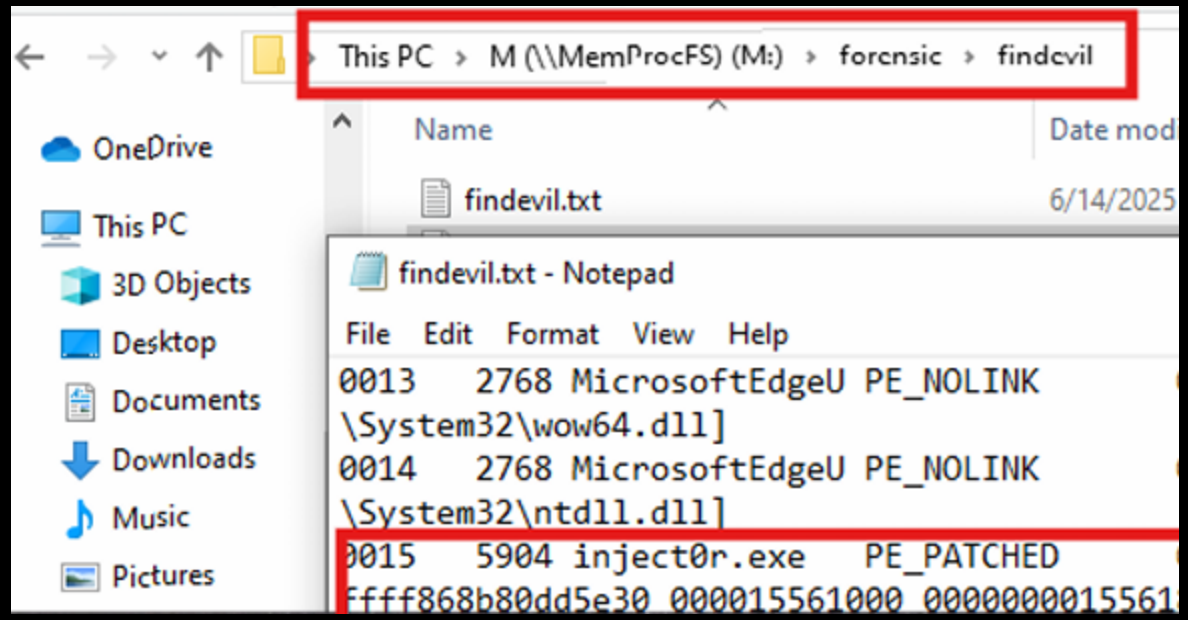
```
                                                                                "C:\Windows\System32\VBoxTray.exe"
                                                                                2019-12-11 14:32:35 UTC ->                    ***
                                                                                Medium

 -- cmd.exe                    1984    604     U  SmartNet        \Device\HarddiskVolume2\Windows\System32\cmd.exe
                                                                   C:\Windows\system32\cmd.exe
                                                                   "C:\Windows\system32\cmd.exe"
                                                                   2019-12-11 14:34:54 UTC ->                    ***
                                                                   Medium

 -- mspaint.exe                2424    604     U  SmartNet        \Device\HarddiskVolume2\Windows\System32\mspaint.exe
                                                                   C:\Windows\system32\mspaint.exe
                                                                   "C:\Windows\system32\mspaint.exe"
                                                                   2019-12-11 14:35:14 UTC ->                    ***
                                                                   Medium
```

Sys/Net Folder

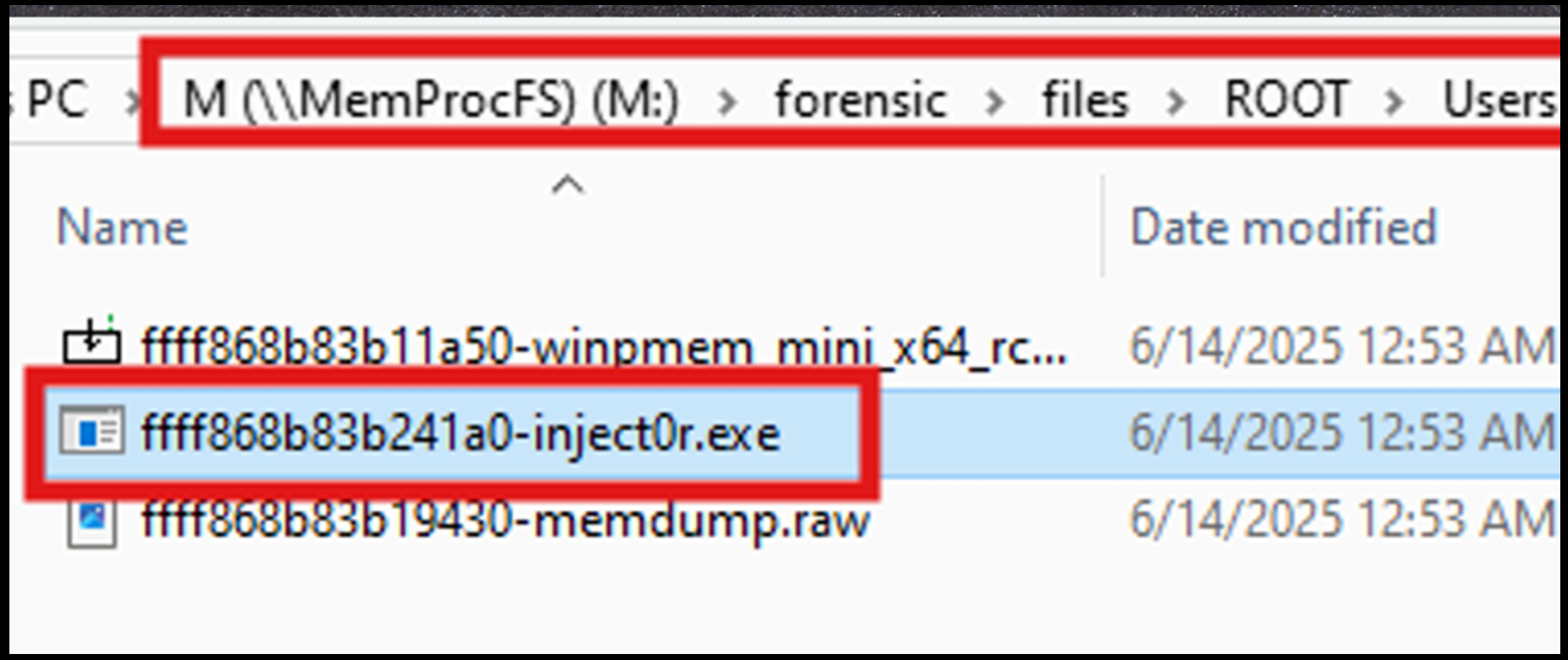
- Network status from captured host.
- Similar to netstat output
- In volatility, netscan
- sys > net > netstat.txt

```
#     PID Proto  State        Src                        Dst                        Process
-----------------------------------------------------------------------------------------------
0000      4 TCPv6  LISTENING    [::]:445                   ***                        System
0001      4 TCPv6  LISTENING    [::]:2869                  ***                        System
0002      4 TCPv6  LISTENING    [::]:5357                  ***                        System
0003      4 TCPv6  LISTENING    [::]:10243                 ***                        System
0004      4 TCPv4  LISTENING    10.0.2.15:139              ***                        System
```

FindEvil Folder

- To find any Read, Write and Execute permission.
- 

Locate the Evil

- Find where file location and dump it.
- Similar to Real File System
- 


```
forensics>files>ROOT>Users>username>Downloads
```

Hand-On

-https://shorturl.at/KTESM

% in venv install this tools

```
sudo -H pip install -U oletools[full]
```

Challenge

The victim kept his study notes somewhere in the machine. Can you recover his study notes and analyze it to make sure it is safe before handing it to him.

> sunctf{vba_macros_are_dangerous}

Q & A

🙏 Thank You!

Feel free to connect with me or explore more of my work:

🔗 https://www.linkedin.com/in/ymiir

📝 https://ymiir.gitbook.io/nota/

-
-
-

Prepared for CSLU Brunei 2025