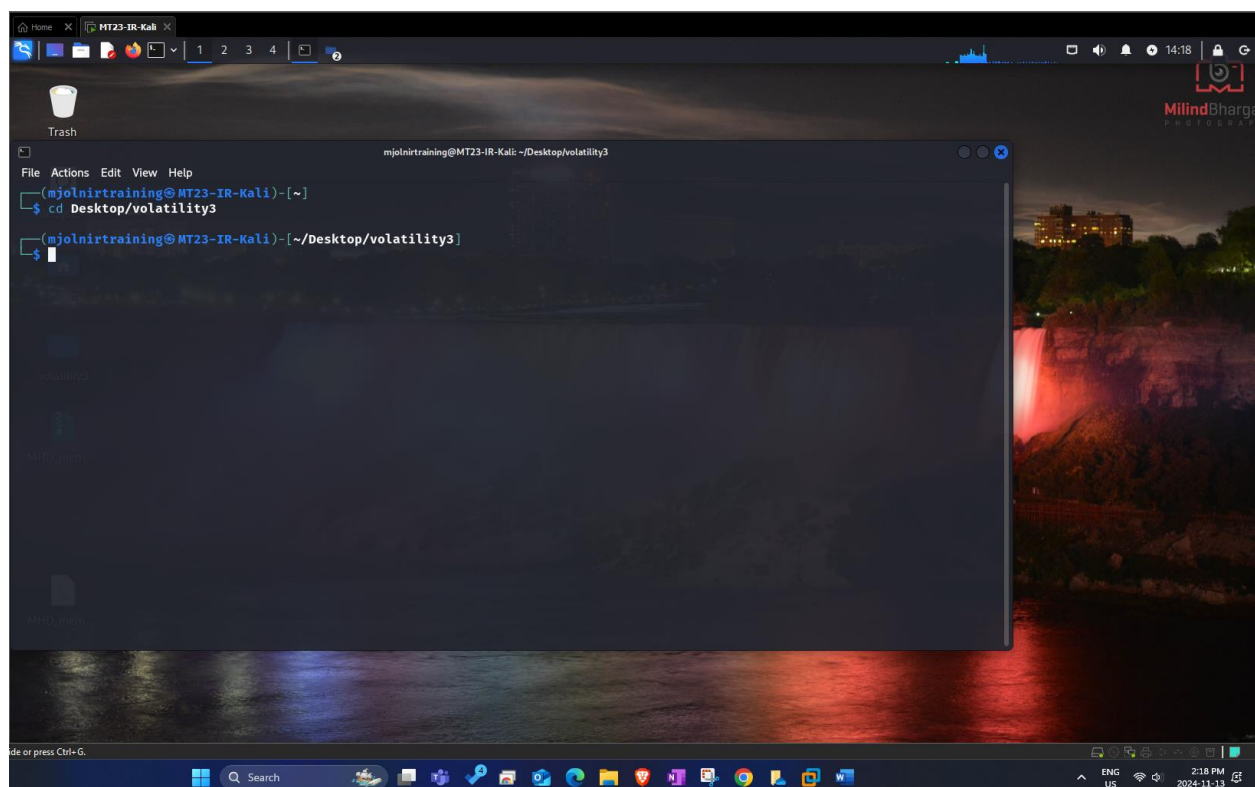
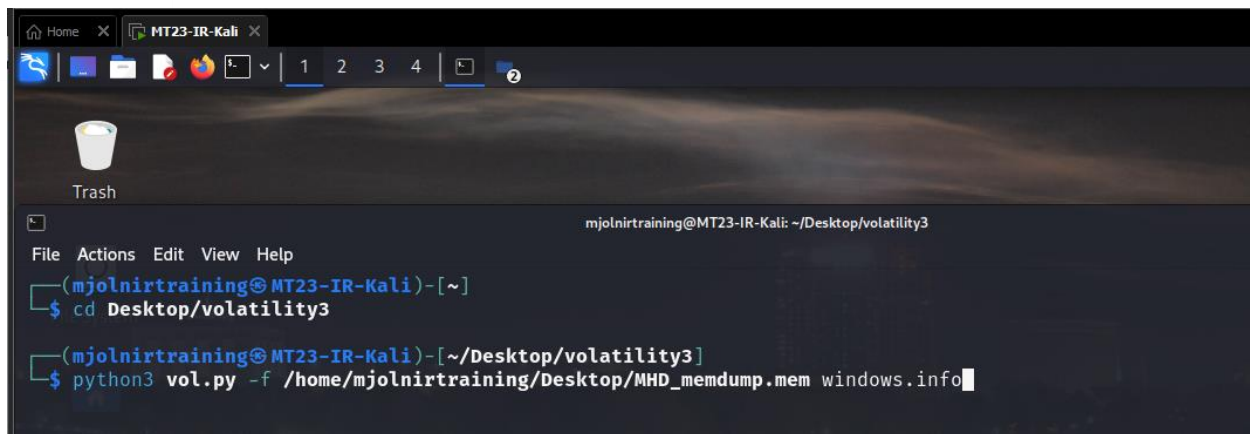


DIGITAL FORENSICS&INCID. RESP - COMP 4071**HOMEWORK LAB 3**

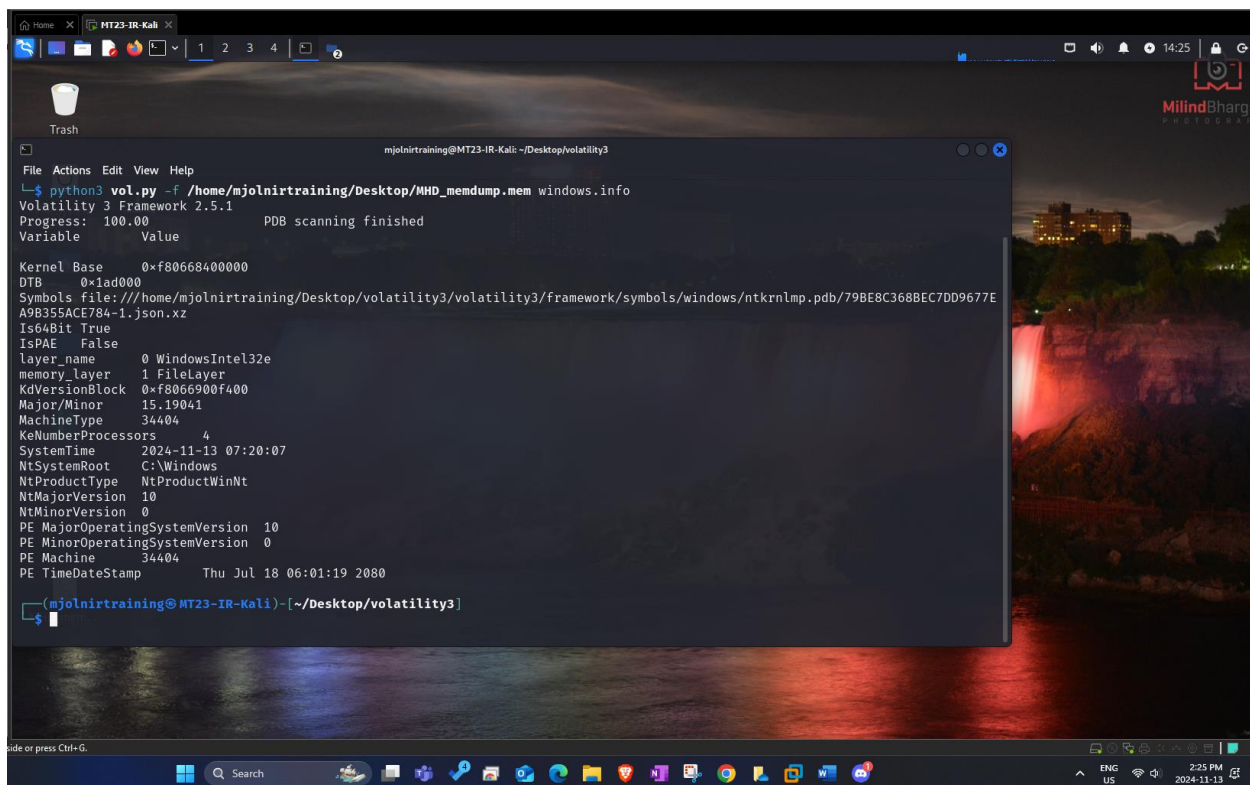
Move the Memory Dump: I started by transferring your memory dump file to Kali Linux, so I could work on it there.

Check the Directory: I navigated to the directory where the memory dump is located to make sure it's ready for analysis.

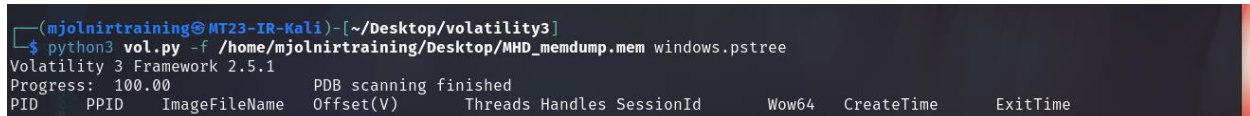




```
mjолnirtraining@MT23-IR-Kali: ~/Desktop/volatility3
File Actions Edit View Help
(mjолnirtraining@MT23-IR-Kali)-[~]
$ cd Desktop/volatility3
(mjолnirtraining@MT23-IR-Kali)-[~/Desktop/volatility3]
$ python3 vol.py -f /home/mjолnirtraining/Desktop/MHD_memdump.mem windows.info
```



```
mjолnirtraining@MT23-IR-Kali: ~/Desktop/volatility3
File Actions Edit View Help
$ python3 vol.py -f /home/mjолnirtraining/Desktop/MHD_memdump.mem windows.info
Volatility 3 Framework 2.5.1
Progress: 100.00 PDB scanning finished
Variable Value
Kernel Base 0xf80668400000
DTB 0x1ad000
Symbols file: ///home/mjолnirtraining/Desktop/volatility3/volatility3/framework/symbols/windows/ntkrnlmp.pdb/79BE8C368BEC7DD9677E
A9B3F5ACF784-1.json.xz
Is64Bit True
IsPAE False
layer_name 0 WindowsIntel32e
memory_layer 1 FileLayer
KdVersionBlock 0xf8066900f400
Major/Minor 15.19041
MachineType 34404
KeNumberProcessors 4
SystemTime 2024-11-13 07:20:07
NtSystemRoot C:\Windows
NtProductType NtProductWinNt
NtMajorVersion 10
NtMinorVersion 0
PE MajorOperatingSystemVersion 10
PE MinorOperatingSystemVersion 0
PE Machine 34404
PE TimeDateStamp Thu Jul 18 06:01:19 2080
(mjолnirtraining@MT23-IR-Kali)-[~/Desktop/volatility3]
$
```



```
(mjолnirtraining@MT23-IR-Kali)-[~/Desktop/volatility3]
$ python3 vol.py -f /home/mjолnirtraining/Desktop/MHD_memdump.mem windows.pstree
Volatility 3 Framework 2.5.1
Progress: 100.00 PDB scanning finished
PID PPID ImageFileName Offset(V) Threads Handles SessionId Wow64 CreateTime ExitTime
```

```

(mjolinirtraining@MT23-IR-Kali) ~/Desktop/volatility3
**** 5996      10816      msedgeview2      0xe30dbffac080      0      -      1      False      2024-11-13 07:17:27.000000      2024-11-
13 07:17:34.000000
**** 10748     10816      dumpcap.exe      0xe30dbf8e70c0      1      -      1      False      2024-11-13 07:18:38.000000      N/A
**** 6104     10748      conhost.exe      0xe30dc61e60c0      5      -      1      False      2024-11-13 07:18:38.000000      N/A
** 12644      5948      4.exe            0xe30dc092d080      6      -      1      True       2024-11-13 07:19:51.000000      N/A
** 7720       5948      SecurityHealth   0xe30dbba51080      1      -      1      False      2024-11-13 06:40:40.000000      N/A
** 6792       5948      ProcessHacker.   0xe30dc5fe60c0      8      -      1      False      2024-11-13 07:18:29.000000      N/A
** 2856       5948      CXVIjlo.exe      0xe30dbf193080      7      -      1      True       2024-11-13 07:19:42.000000      N/A
**** 11252    2856      gnVEJcw.exe      0xe30dc54c7080      8      -      1      True       2024-11-13 07:19:43.000000      N/A
** 652 5948   vmtoolsd.exe     0xe30dbba57080      7      -      1      False      2024-11-13 06:40:41.000000      N/A
** 9396       5948      FTK Imager.exe   0xe30dbb48b080      12     -      1      False      2024-11-13 07:16:45.000000      N/A
** 5144       5948      vncmgr_x64.ex    0xe30dbbdf2080      13     -      1      False      2024-11-13 07:07:31.000000      N/A
** 4252       5948      msedge.exe       0xe30dbba56300      0      -      1      False      2024-11-13 06:40:45.000000      2024-11-
13 06:41:56.000000
** 5304       5948      19075-NYPD.exe   0xe30dbb5c50c0      19     -      1      True       2024-11-13 07:19:34.000000      N/A
**** 7340     5304      eJLMBW.exe       0xe30dc4674080      10     -      1      True       2024-11-13 07:19:35.000000      N/A
* 964 732     fontdrvhost.ex   0xe30dc53e0140      5      -      1      False      2024-11-13 06:39:59.000000      N/A
4588 3220     wvututil.exe     0xe30dbb493080      0      -      0      False      2024-11-13 06:40:11.000000      2024-11-13 06:40
:11.000000
5020 5040     msedge.exe       0xe30dbb6c30c0      0      -      1      False      2024-11-13 06:41:54.000000      2024-11-13 06:41
:54.000000
4572 1080     OneDrive.exe     0xe30dc55d2080      23     -      1      False      2024-11-13 06:43:23.000000      N/A
8588 4560     MicrosoftEdgeU   0xe30dbb62b080      4      -      0      True       2024-11-13 06:44:08.000000      N/A
4100 10612     FTK Imager.exe   0xe30dc03dc080      9      -      1      False      2024-11-13 06:51:20.000000      N/A
7676 5148     vpnclient_x64.   0xe30dc47b8080      8      -      1      False      2024-11-13 06:53:46.000000      N/A
24964830102440 0      0xe30dc64d2080      0      -      N/A      1600-11-25 03:55:32.000000      N/A

(mjolinirtraining@MT23-IR-Kali) ~/Desktop/volatility3
$

```

```

**** 5996      10816      msedgeview2      0xe30dbffac080      0      -      1      False      2024-11-13 07:17:27.000000      2024-11-
13 07:17:34.000000
**** 10748     10816      dumpcap.exe      0xe30dbf8e70c0      1      -      1      False      2024-11-13 07:18:38.000000      N/A
**** 6104     10748      conhost.exe      0xe30dc61e60c0      5      -      1      False      2024-11-13 07:18:38.000000      N/A
** 12644      5948      4.exe            0xe30dc092d080      6      -      1      True       2024-11-13 07:19:51.000000      N/A
** 7720       5948      SecurityHealth   0xe30dbba51080      1      -      1      False      2024-11-13 06:40:40.000000      N/A
** 6792       5948      ProcessHacker.   0xe30dc5fe60c0      8      -      1      False      2024-11-13 07:18:29.000000      N/A
** 2856       5948      CXVIjlo.exe      0xe30dbf193080      7      -      1      True       2024-11-13 07:19:42.000000      N/A
**** 11252    2856      gnVEJcw.exe      0xe30dc54c7080      8      -      1      True       2024-11-13 07:19:43.000000      N/A
** 652 5948   vmtoolsd.exe     0xe30dbba57080      7      -      1      False      2024-11-13 06:40:41.000000      N/A
** 9396       5948      FTK Imager.exe   0xe30dbb48b080      12     -      1      False      2024-11-13 07:16:45.000000      N/A
** 5144       5948      vncmgr_x64.ex    0xe30dbbdf2080      13     -      1      False      2024-11-13 07:07:31.000000      N/A
** 4252       5948      msedge.exe       0xe30dbba56300      0      -      1      False      2024-11-13 06:40:45.000000      2024-11-
13 06:41:56.000000
** 5304       5948      19075-NYPD.exe   0xe30dbb5c50c0      19     -      1      True       2024-11-13 07:19:34.000000      N/A
**** 7340     5304      eJLMBW.exe       0xe30dc4674080      10     -      1      True       2024-11-13 07:19:35.000000      N/A
* 964 732     fontdrvhost.ex   0xe30dc53e0140      5      -      1      False      2024-11-13 06:39:59.000000      N/A
4588 3220     wvututil.exe     0xe30dbb493080      0      -      0      False      2024-11-13 06:40:11.000000      2024-11-13 06:40
:11.000000
5020 5040     msedge.exe       0xe30dbb6c30c0      0      -      1      False      2024-11-13 06:41:54.000000      2024-11-13 06:41
:54.000000
4572 1080     OneDrive.exe     0xe30dc55d2080      23     -      1      False      2024-11-13 06:43:23.000000      N/A
8588 4560     MicrosoftEdgeU   0xe30dbb62b080      4      -      0      True       2024-11-13 06:44:08.000000      N/A
4100 10612     FTK Imager.exe   0xe30dc03dc080      9      -      1      False      2024-11-13 06:51:20.000000      N/A
7676 5148     vpnclient_x64.   0xe30dc47b8080      8      -      1      False      2024-11-13 06:53:46.000000      N/A
24964830102440 0      0xe30dc64d2080      0      -      N/A      1600-11-25 03:55:32.000000      N/A

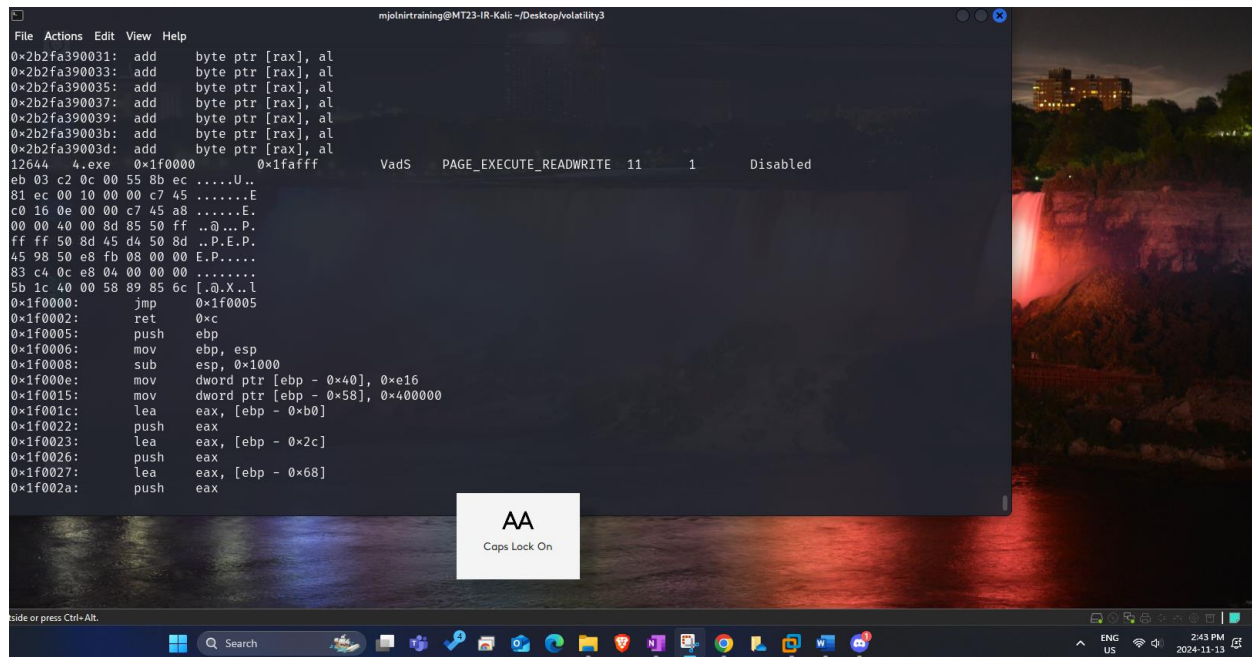
```

Runs the malfind plugin, which is used to detect injected code in memory

```

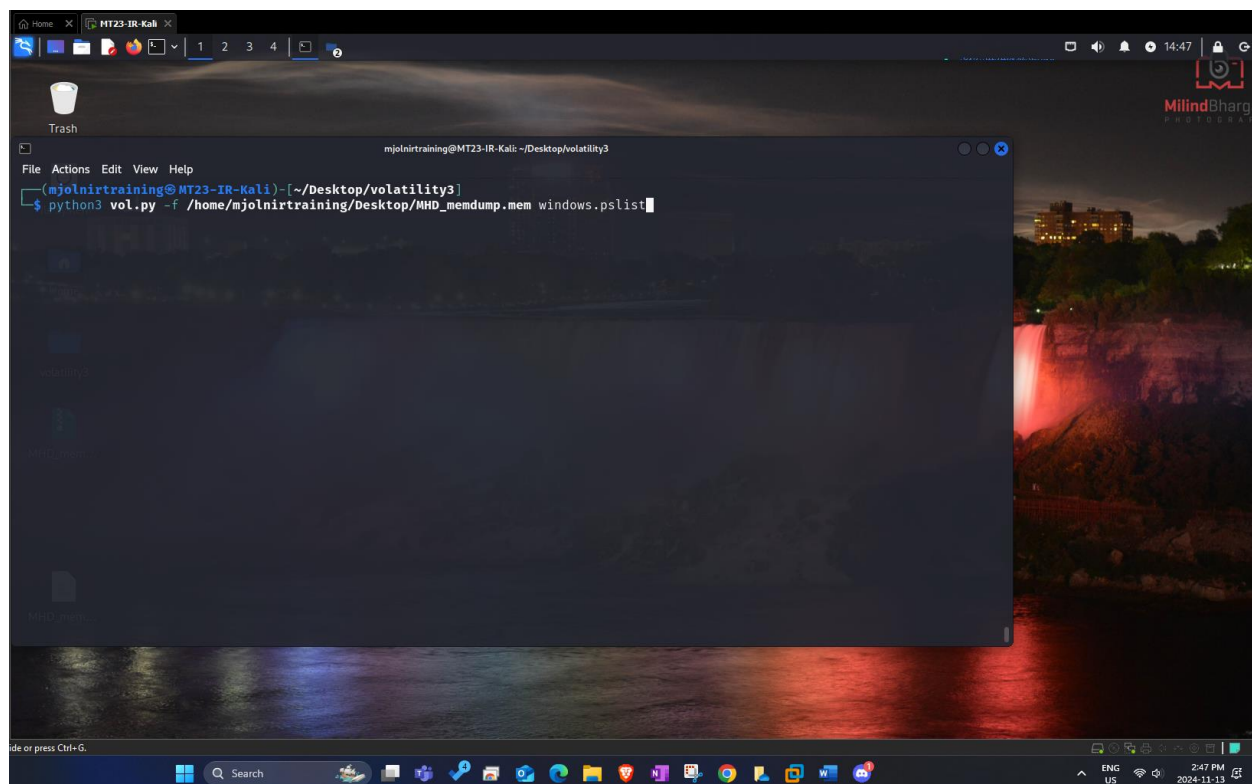
(mjolinirtraining@MT23-IR-Kali) ~/Desktop/volatility3
$ python3 vol.py -f /home/mjolinirtraining/Desktop/MHD_memdump.mem windows.malfind
Volatility 3 Framework 2.5.1
Progress: 100.00
PDB scanning finished
PID Process Start VPN End VPN Tag Protection CommitCharge PrivateMemory File output Hexdump Disasm
5172 sihost.exe 0x30000000 0x3008bfff VadS PAGE_EXECUTE_READWRITE 140 1 Disabled
4d 5a 90 00 03 00 00 00 MZ

```



```
mjolintraining@MT23-IR-Kali: ~/Desktop/volatility3
File Actions Edit View Help
0x2b2fa390031: add byte ptr [rax], al
0x2b2fa390033: add byte ptr [rax], al
0x2b2fa390035: add byte ptr [rax], al
0x2b2fa390037: add byte ptr [rax], al
0x2b2fa390039: add byte ptr [rax], al
0x2b2fa39003b: add byte ptr [rax], al
0x2b2fa39003d: add byte ptr [rax], al
12644 4.exe 0x1f0000 0x1fafff VadS PAGE_EXECUTE_READWRITE 11 1 Disabled
eb 03 c2 0c 00 55 8b ec .....U..
81 ec 00 10 00 00 c7 45 .....E
c0 16 0e 00 00 c7 45 a8 .....E.
00 00 40 00 8d 85 50 ff ..@...P.
ff ff 50 8d 45 d4 50 8d ..P.E.P.
45 98 50 e8 fb 08 00 00 E.P.....
83 c4 0c e8 04 00 00 00 .....
5b 1c 40 00 58 89 85 6c [.@.X..l
0x1f0000: jmp 0x1f0005
0x1f0002: ret 0xc
0x1f0005: push ebp
0x1f0006: mov ebp, esp
0x1f0008: sub esp, 0x1000
0x1f000e: mov dword ptr [ebp - 0x40], 0xe16
0x1f0015: mov dword ptr [ebp - 0x58], 0x400000
0x1f001c: lea eax, [ebp - 0xb0]
0x1f0022: push eax
0x1f0023: lea eax, [ebp - 0x2c]
0x1f0026: push eax
0x1f0027: lea eax, [ebp - 0x68]
0x1f002a: push eax

AA
Caps Lock On
```



```
mjolintraining@MT23-IR-Kali: ~/Desktop/volatility3
File Actions Edit View Help
(mjolintraining@MT23-IR-Kali)~-[~/Desktop/volatility3]
$ python3 vol.py -f /home/mjolintraining/Desktop/MHD_memdump.mem windows.pslist
```

```

mjohnirtraining@MT23-IR-Kali: ~/Desktop/volatility3
File Actions Edit View Help
(mjohnirtraining@MT23-IR-Kali)-[~/Desktop/volatility3]
$ python3 vol.py -f /home/mjohnirtraining/Desktop/MHD_memdump.mem windows.pslist
Volatility 3 Framework 2.5.1
Progress: 67.88      Scanning memory_layer using BytesScanner

```

Run Volatility for System Info: Using the Volatility tool, I ran the windows.info command to gather basic information about the system in the memory dump. This gave US a quick overview of the operating system and version.

List Processes pslist: Next, I used Volatility's windows.pslist to list all active processes in the memory dump. This helped US decide which process (PID) to analyze.

```

0104 10748 ComHost.exe 0xe30dc61e00c0 5 - 1 False 2024-11-13 07:18:38.000000 N/A Disabled
5304 5948 19075-NYPD.exe 0xe30dbb5c50c0 19 - 1 True 2024-11-13 07:19:34.000000 N/A Disabled
7340 5304 eJLGMbW.exe 0xe30dc4674080 10 - 1 True 2024-11-13 07:19:35.000000 N/A Disabled
2856 5948 CXVIJlo.exe 0xe30dbf193080 7 - 1 True 2024-11-13 07:19:42.000000 N/A Disabled
11252 2856 gnVEJcw.exe 0xe30dc54c7080 8 - 1 True 2024-11-13 07:19:43.000000 N/A Disabled
12644 5948 4.exe 0xe30dc092d080 6 - 1 True 2024-11-13 07:19:51.000000 N/A Disabled
18296 3116 SenseIR.exe 0xe30dc5bea0c0 13 - 0 False 2024-11-13 07:19:58.000000 N/A Disabled
22488 928 WmiPrvSE.exe 0xe30dc65f3280 7 - 0 True 2024-11-13 07:20:08.000000 N/A Disabled
249648301024440 0 0xe30dc64d2080 0 - N/A False 1600-11-25 03:55:32.000000 N/A Disabled

(mjohnirtraining@MT23-IR-Kali)-[~/Desktop/volatility3]
$ python3 vol.py -f /home/mjohnirtraining/Desktop/MHD_memdump.mem windows.dumpfiles.DumpFiles --pid 2856

```

```

(mjolinrtraining@MT23-IR-Kali)~/Desktop/volatility3
$ python3 vol.py -f /home/mjolinrtraining/Desktop/MHD_memdump.mem windows.dumpfiles.DumpFiles --pid 12644
Volatility 3 Framework 2.5.1
Progress: 100.00
PDB scanning finished
Cache FileObject FileName Result
ImageSectionObject 0xe30dc52bb220 apphelp.dll file.0xe30dc52bb220.0xe30dbb83a850.ImageSectionObject.apphelp.dll.img
ImageSectionObject 0xe30dc5b448a0 4.exe file.0xe30dc5b448a0.0xe30dbba63aa0.ImageSectionObject.4.exe.img
ImageSectionObject 0xe30dbf554480 dnsapi.dll file.0xe30dbf554480.0xe30dbba59a10.ImageSectionObject.dnsapi.dll.img
ImageSectionObject 0xe30dbf76fce0 sxs.dll file.0xe30dbf76fce0.0xe30dbba58270.ImageSectionObject.sxs.dll.img
ImageSectionObject 0xe30dc5d80760 msimg32.dll file.0xe30dc5d80760.0xe30dc14d0dc0.ImageSectionObject.msimg32.dll.img
ImageSectionObject 0xe30dbf576ea0 winhttp.dll file.0xe30dbf576ea0.0xe30dc32df460.ImageSectionObject.winhttp.dll.img
ImageSectionObject 0xe30dbf576d00 mswsock.dll file.0xe30dbf576d00.0xe30dbb83a2e0.ImageSectionObject.mswsock.dll.img
ImageSectionObject 0xe30dc138b6e0 MpOAV.dll file.0xe30dc138b6e0.0xe30dc404bb80.ImageSectionObject.MpOAV.dll.img
ImageSectionObject 0xe30dbf570ec0 userenv.dll file.0xe30dbf570ec0.0xe30dbba52aa0.ImageSectionObject.userenv.dll.img
ImageSectionObject 0xe30dc5b65c00 fastprox.dll file.0xe30dc5b65c00.0xe30dc48d8c80.ImageSectionObject.fastprox.dll.img
ImageSectionObject 0xe30db9840470 ntdll.dll file.0xe30db9840470.0xe30db981cd00.ImageSectionObject.ntdll.dll.img
ImageSectionObject 0xe30db9b77b00 gdi32full.dll file.0xe30db9b77b00.0xe30db9b54010.ImageSectionObject.gdi32full.dll.img
ImageSectionObject 0xe30db9b7f3f0 combase.dll file.0xe30db9b7f3f0.0xe30db9b51c50.ImageSectionObject.combase.dll.img
ImageSectionObject 0xe30db94c0760 amsi.dll file.0xe30db94c0760.0xe30dbfecdd20.ImageSectionObject.amsi.dll.img
ImageSectionObject 0xe30dc0e13e40 wbemprox.dll file.0xe30dc0e13e40.0xe30dc0397d30.ImageSectionObject.wbemprox.dll.img
ImageSectionObject 0xe30dc0e12c60 wbemcomn.dll file.0xe30dc0e12c60.0xe30dc4a03d10.ImageSectionObject.wbemcomn.dll.img
ImageSectionObject 0xe30dbf575b20 IPHLPAPI.DLL file.0xe30dbf575b20.0xe30dbb85c8a0.ImageSectionObject.IPHLPAPI.DLL.img
ImageSectionObject 0xe30dc4942b00 profapi.dll file.0xe30dc4942b00.0xe30dc320b4d0.ImageSectionObject.profapi.dll.img
ImageSectionObject 0xe30dc3f61600 version.dll file.0xe30dc3f61600.0xe30dc54ca470.ImageSectionObject.version.dll.img
ImageSectionObject 0xe30dc4d6e8c0 sspicli.dll file.0xe30dc4d6e8c0.0xe30dbb878b20.ImageSectionObject.sspicli.dll.img
ImageSectionObject 0xe30dc0568160 uxtheme.dll file.0xe30dc0568160.0xe30dbb845b70.ImageSectionObject.uxtheme.dll.img

```

```

(mjolinrtraining@MT23-IR-Kali)~/Desktop/volatility3
$ python3 vol.py -f /home/mjolinrtraining/Desktop/MHD_memdump.mem windows.dumpfiles.DumpFiles --pid 5304

```

Next, I used Volatility's windows.pslist to list all active processes in the memory dump. This helped US decide which process PID to analyze.

```

(mjolinrtraining@MT23-IR-Kali)~/Desktop/volatility3
$ python3 vol.py -f /home/mjolinrtraining/Desktop/MHD_memdump.mem windows.dumpfiles.DumpFiles --pid 2856

```

Process ID	Process Name	Process Path	Process Type	Process Status	Process Time	Process User	Process Group	Process Session	Process Window	Process Title
5144	vpcnmg_r64.exe	0xe30dbbdf2080	13	-	1	False	2024-11-13 07:07:31.000000	N/A	Disabled	
7160	svchost.exe	0xe30dc09c9240	0	-	0	False	2024-11-13 07:10:51.000000	2024-11-13 07:14		
29.000000	Disabled									
2368	svchost.exe	0xe30dbfba240	5	-	0	False	2024-11-13 07:11:32.000000	N/A	Disabled	
4384	SenseNdr.exe	0xe30dc2ff3080	19	-	0	False	2024-11-13 07:11:39.000000	N/A	Disabled	
3844	taskhostw.exe	0xe30dbb5cc340	2	-	1	False	2024-11-13 07:11:39.000000	N/A	Disabled	
7056	svchost.exe	0xe30dc46ad080	0	-	0	False	2024-11-13 07:13:24.000000	2024-11-13 07:26		
407.000000	Disabled									
9396	FTK Imager.exe	0xe30dbb48b080	12	-	1	False	2024-11-13 07:16:45.000000	N/A	Disabled	
10816	Wireshark.exe	0xe30dc4203080	10	-	1	False	2024-11-13 07:16:59.000000	N/A	Disabled	
3724	svchost.exe	0xe30dc4a04080	1	-	0	False	2024-11-13 07:17:26.000000	N/A	Disabled	
5996	msedgewebview2.exe	0xe30dbffac080	0	-	1	False	2024-11-13 07:17:27.000000	2024-11-13 07:17		
34.000000	Disabled									
1448	dumpcap.exe	0xe30dc40780c0	0	-	1	False	2024-11-13 07:17:44.000000	2024-11-13 07:17		
47.000000	Disabled									
6792	ProcessHacker.exe	0xe30dc5fe60c0	8	-	1	False	2024-11-13 07:18:29.000000	N/A	Disabled	
10748	dumpcap.exe	0xe30dbf8e70c0	1	-	1	False	2024-11-13 07:18:38.000000	N/A	Disabled	
6104	conhost.exe	0xe30dc61e60c0	5	-	1	False	2024-11-13 07:18:38.000000	N/A	Disabled	
5304	19075-NYPD.exe	0xe30dbb5c50c0	19	-	1	True	2024-11-13 07:19:34.000000	N/A	Disabled	
7340	eJLGMbW.exe	0xe30dc4674080	10	-	1	True	2024-11-13 07:19:35.000000	N/A	Disabled	
2856	CXVIJlo.exe	0xe30dbf193080	7	-	1	True	2024-11-13 07:19:42.000000	N/A	Disabled	
11252	gnVEJcw.exe	0xe30dc54c7080	8	-	1	True	2024-11-13 07:19:43.000000	N/A	Disabled	
12644	4.exe	0xe30dc092d080	6	-	1	True	2024-11-13 07:19:51.000000	N/A	Disabled	
18296	SenseIR.exe	0xe30dc5bea0c0	13	-	0	False	2024-11-13 07:19:58.000000	N/A	Disabled	
22488	WmiPrvSE.exe	0xe30dc65f3280	7	-	0	True	2024-11-13 07:20:08.000000	N/A	Disabled	
249648301024440	0	0xe30dc64d2080	0	-	N/A	False	1600-11-25 03:55:32.000000	N/A	Disabled	

Select and Dump Process: With a specific PID chosen, I used windows.dumpfiles to extract the file associated with that process. This step gave US a copy of the file in memory

The screenshot shows a Kali Linux desktop environment. A terminal window titled 'mjolnirtraining@MT23-IR-Kali: ~/Desktop/volatility3' is open. It displays the output of the 'volatility3 --pid 2856' command, which lists running processes. The process 'CXVIJlo.exe' with PID 2856 is highlighted. Below the process list, the terminal shows the execution of 'python3 vol.py -f /home/mjolnirtraining/Desktop/MHD_memdump.mem windows.dumpfiles.DumpFiles --pid 2856'. The output indicates that the PDB scanning is finished and the file 'CXVIJlo.exe' has been successfully dumped to the file 'CXVIJlo.exe.dat'.

File	Actions	Edit	View	Help
6104	10748	conhost.exe	0xe30dc61e60c0	5
5304	5948	19075-NYPD.exe	0xe30dbb5c50c0	19
7340	5304	eJLGMbW.exe	0xe30dc4674080	10
2856	5948	CXVIJlo.exe	0xe30dbf193080	7
11252	2856	gnVEJcw.exe	0xe30dc54c7080	8
12644	5948	4.exe	0xe30dc092d080	6
18296	3116	SenseIR.exe	0xe30dc5bea0c0	13
22488	928	WmiPrvSE.exe	0xe30dc65f3280	7
249648301024440	0		0xe30dc64d2080	0

```

(mjolnirtraining@MT23-IR-Kali)~[/Desktop/volatility3]
$ python3 vol.py -f /home/mjolnirtraining/Desktop/MHD_memdump.mem windows.dumpfiles.DumpFiles --pid 2856
Volatility 3 Framework 2.5.1
Progress: 100.00
Cache FileObject FileName Result
DataSectionObject 0xe30dc4571710 cversions.2.db file.0xe30dc4571710.0xe30dbbfa9c70.DataSectionObject.cversions.2.db.dat
DataSectionObject 0xe30dc4571710 cversions.2.db file.0xe30dc4571710.0xe30dbbfa9c70.DataSectionObject.cversions.2.db.dat
ImageSectionObject 0xe30db9b75580 kernel32.dll file.0xe30db9b75580.0xe30db9b55010.ImageSectionObject.kernel32.dll.img
ImageSectionObject 0xe30dc52bb220 apphelp.dll file.0xe30dc52bb220.0xe30db883a850.ImageSectionObject.apphelp.dll.img
DataSectionObject 0xe30dc5b63840 CXVIJlo.exe file.0xe30dc5b63840.0xe30db9507550.DataSectionObject.CXVIJlo.exe.dat
ImageSectionObject 0xe30dc5b63840 CXVIJlo.exe file.0xe30dc5b63840.0xe30dc3aa88b0.ImageSectionObject.CXVIJlo.exe.img
DataSectionObject 0xe30dc4571710 cversions.2.db file.0xe30dc4571710.0xe30dbbfa9c70.DataSectionObject.cversions.2.db.dat
ImageSectionObject 0xe30dc230f6c0 iertutil.dll file.0xe30dc230f6c0.0xe30dbba59770.ImageSectionObject.iertutil.dll.img
ImageSectionObject 0xe30dbf570ec0 userenv.dll file.0xe30dbf570ec0.0xe30dbba52aa0.ImageSectionObject.userenv.dll.img
ImageSectionObject 0xe30dc1d22ec0 mpr.dll file.0xe30dc1d22ec0.0xe30dbba59270.ImageSectionObject.mpr.dll.img
DataSectionObject 0xe30dc52c9c20 rsaenh.dll Error dumping file
ImageSectionObject 0xe30dc52c9c20 rsaenh.dll file.0xe30dc52c9c20.0xe30dbb9a1a20.ImageSectionObject.rsaenh.dll.img
ImageSectionObject 0xe30dbf6d8580 AppResolver.dll file.0xe30dbf6d8580.0xe30db899cda0.ImageSectionObject.AppResolver.dll.im
  
```

Copy and Extract Dumped File: I copied the dumped file and saved it in a new location. This made it easier to manage and examine the file separately.

```

ImageSectionObject 0xe30db983ad70 ntdll.dll file.0xe30db983ad70.0xe30db8f1a560.ImageSectionObject.ntdll.dll.img
ImageSectionObject 0xe30db9b416a0 wow64win.dll file.0xe30db9b416a0.0xe30db9abbd90.ImageSectionObject.wow64win.dll.img

(mjолnirtraining@MT23-IR-Kali) [~/Desktop/volatility3]
$ cp file.0xe30dc5b63840.0xe30dc3aa88b0.ImageSectionObject.CXYIJlo.exe.img CXYIJlo.exe
(mjолnirtraining@MT23-IR-Kali) [~/Desktop/volatility3]
$

```

```

(mjолnirtraining@MT23-IR-Kali) [~/Desktop/volatility3]
$ cp file.0xe30dc5b63840.0xe30dc3aa88b0.ImageSectionObject.CXYIJlo.exe.img CXYIJlo.exe
(mjолnirtraining@MT23-IR-Kali) [~/Desktop/volatility3]
$ rm *.img
(mjолnirtraining@MT23-IR-Kali) [~/Desktop/volatility3]
$ rm *.dat
(mjолnirtraining@MT23-IR-Kali) [~/Desktop/volatility3]
$

```

```

-rw-r--r-- 1 mjолnirtraining mjолnirtraining 2963 Sep 13 2023 volshell.spec

(mjолnirtraining@MT23-IR-Kali) [~/Desktop/volatility3]
$ strings CXYIJlo.exe > CXYIJlo.exe.mohamad
(mjолnirtraining@MT23-IR-Kali) [~/Desktop/volatility3]
$ cat -n CXYIJlo.exe.mohamad

```

```

(mjолnirtraining@MT23-IR-Kali) [~/Desktop/volatility3]
$ ls -l
total 9550220
-rw-r--r-- 1 mjолnirtraining mjолnirtraining 192512 Nov 13 14:54 CXYIJlo.exe
-rw-r--r-- 1 mjолnirtraining mjолnirtraining 4946 Nov 13 02:56 CXYIJlo.exe.mohamad
-rw-r--r-- 1 mjолnirtraining mjолnirtraining 201 Sep 13 2023 MANIFEST.in
-rw-r--r-- 1 mjолnirtraining mjолnirtraining 232596 Nov 13 03:23 MT23-IR-Kali_files_md5s.csv
-rw-r--r-- 1 mjолnirtraining mjолnirtraining 19964399 Nov 13 03:23 MT23-IR-Kali_thor_2024-11-13_0301.h
-rw-r--r-- 1 mjолnirtraining mjолnirtraining 4776082 Nov 13 03:23 MT23-IR-Kali_thor_2024-11-13_0301.t
-rw-r--r-- 1 mjолnirtraining mjолnirtraining 9663676416 Sep 13 2023 Oct17memdump.mem
-rw-r--r-- 1 mjолnirtraining mjолnirtraining 5947 Sep 13 2023 README.md
drwxr-xr-x 4 root root 4096 Sep 13 2023 build
drwxr-xr-x 2 mjолnirtraining mjолnirtraining 4096 Oct 8 06:26 config
drwxr-xr-x 6 mjолnirtraining mjолnirtraining 4096 Oct 8 06:26 custom-signatures
drwxr-xr-x 3 mjолnirtraining mjолnirtraining 4096 Sep 13 2023 development
drwxr-xr-x 2 root root 4096 Sep 13 2023 dist
drwxr-xr-x 3 mjолnirtraining mjолnirtraining 4096 Sep 13 2023 doc

```

```

File Actions Edit View Help
itives.dll.img 0xe30db9b73a20 KernelBase.dll file.0xe30db9b73a20.0xe30db9b50c90.ImageSectionObject.KernelBase.dll.img
ImageSectionObject 0xe30db9b73700 ucrtbase.dll file.0xe30db9b73700.0xe30db9a85010.ImageSectionObject.ucrtbase.dll.img
ImageSectionObject 0xe30db9b74ce0 ws2_32.dll file.0xe30db9b74ce0.0xe30db93e7c40.ImageSectionObject.ws2_32.dll.img
ImageSectionObject 0xe30db9b733e0 SHCore.dll file.0xe30db9b733e0.0xe30db9703870.ImageSectionObject.SHCore.dll.img
ImageSectionObject 0xe30db9b74510 advapi32.dll file.0xe30db9b74510.0xe30db9b174e0.ImageSectionObject.advapi32.dll.img
ImageSectionObject 0xe30db9b629c0 clbcatq.dll file.0xe30db9b629c0.0xe30db9b39d90.ImageSectionObject.clbcatq.dll.img
ImageSectionObject 0xe30db9b62510 msvcrt.dll file.0xe30db9b62510.0xe30db9a858d0.ImageSectionObject.msvcrt.dll.img
ImageSectionObject 0xe30db9b3e890 wow64cpu.dll file.0xe30db9b3e890.0xe30db9b1f260.ImageSectionObject.wow64cpu.dll.img
ImageSectionObject 0xe30db9b4f510 wow64.dll file.0xe30db9b4f510.0xe30db9b3ad30.ImageSectionObject.wow64.dll.img
ImageSectionObject 0xe30db983ed70 ntdll.dll file.0xe30db983ed70.0xe30db8f1a560.ImageSectionObject.ntdll.dll.img
ImageSectionObject 0xe30db9b416a0 wow64win.dll file.0xe30db9b416a0.0xe30db9abb90.ImageSectionObject.wow64win.dll.img

(mjolinrtraining@MT23-IR-Kali)-[~/Desktop/volatiliy3]
$ cp file.0xe30dc5b448a0.0xe30dbba63aa0.ImageSectionObject.4.exe 4.exe
(mjolinrtraining@MT23-IR-Kali)-[~/Desktop/volatiliy3]
$ strings 4.exe > 4.exe.mohamad
(mjolinrtraining@MT23-IR-Kali)-[~/Desktop/volatiliy3]
$ cat -n 4.exe | less
zsh: suspended cat -n 4.exe | less
(mjolinrtraining@MT23-IR-Kali)-[~/Desktop/volatiliy3]
$ cat -n 4.exe.mohamad

```

Analyze with Strings Command: To look for readable text within the dumped file, I used the strings command. This helped US identify any suspicious patterns, keywords, or clues within the file.

Save Strings Output: I saved the strings output with my name filename . This way, I could keep track of it and refer back to it later.

Open File with cat Command: Using cat, I viewed the contents of the saved strings output file. This allowed us to review the extracted text from the dumped file easily.

```

(mjolinrtraining@MT23-IR-Kali)-[~/Desktop/volatiliy3]
$ cat -n CXYIJlo.exe | less

```

cat this to chose strings for yara rules

Review Output with cat:



```

$ grep -a \".*ryk\" vpncmgr_x64.exe.mohamad
(mjolinrtraining@ MT23-IR-Kali)-[~/Desktop/volatility3]
$

```

Create YARA Rules: After analyzing the file, I created YARA rules that would help detect patterns or behaviors identified in the memory dump. These rules are tailored to look for specific types of malware.



The screenshot shows a Kali Linux desktop environment. A terminal window is open, displaying the GNU nano 7.2 editor. The editor is editing a file named 'CXVIJlo.yar'. The content of the file is a YARA rule named 'malware_test_aCXVIJlo'. The rule has a meta section with a description 'Detects malware name CXVIJlo.exe sample' and an author 'Mohamad Almasri'. It has a strings section with five strings: '\$s1 = "GetCPInfo" ascii wide', '\$s2 = "GetCommandLineA" ascii wide', '\$s3 = "GetEnvironmentStringsW" ascii wide', '\$s4 = "FreeEnvironmentStringsW" ascii wide', and '\$s5 = "GetOEMCP" ascii wide'. The condition is '\$s1 or \$s2 or \$s3 or \$s4 or \$s5'. The status bar at the bottom of the editor shows 'line 17/18 (94%), col 2/ 2 (100%), char 429/430 (99%)'. The desktop background is a dark image with a cityscape. There are icons for 'Trash', 'File System', 'Home', 'volatility3', and 'MHD_mem...' on the left side. A lock icon is visible at the bottom center of the desktop.

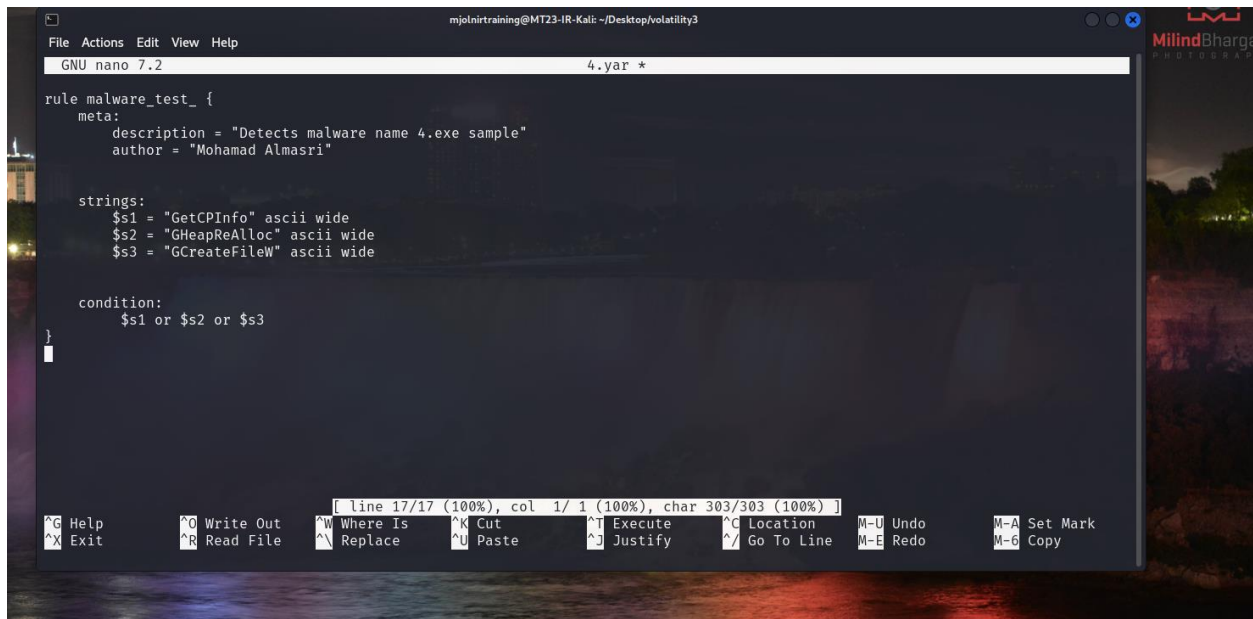
```
File Actions Edit View Help
GNU nano 7.2 CXVIJlo.yar *
rule malware_test_aCXVIJlo {
  meta:
    description = "Detects malware name CXVIJlo.exe sample"
    author = "Mohamad Almasri"

  strings:
    $s1 = "GetCPInfo" ascii wide
    $s2 = "GetCommandLineA" ascii wide
    $s3 = "GetEnvironmentStringsW" ascii wide
    $s4 = "FreeEnvironmentStringsW" ascii wide
    $s5 = "GetOEMCP" ascii wide

  condition:
    $s1 or $s2 or $s3 or $s4 or $s5
}
```

[line 17/18 (94%), col 2/ 2 (100%), char 429/430 (99%)]

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark
^X Exit ^R Read File ^M Replace ^U Paste ^J Justify ^_ Go To Line M-E Redo M-6 Copy



The screenshot shows a Kali Linux desktop environment. A terminal window is open, displaying the GNU nano 7.2 editor. The editor is editing a file named '4.yar'. The content of the file is a YARA rule named 'malware_test_'. The rule has a meta section with a description 'Detects malware name 4.exe sample' and an author 'Mohamad Almasri'. It has a strings section with three strings: '\$s1 = "GetCPInfo" ascii wide', '\$s2 = "GHeapReAlloc" ascii wide', and '\$s3 = "GCreateFileW" ascii wide'. The condition is '\$s1 or \$s2 or \$s3'. The status bar at the bottom of the editor shows 'line 17/17 (100%), col 1/ 1 (100%), char 303/303 (100%)'. The desktop background is a dark image with a cityscape. There are icons for 'Trash', 'File System', 'Home', 'volatility3', and 'MHD_mem...' on the left side. A lock icon is visible at the bottom center of the desktop.

```
File Actions Edit View Help
GNU nano 7.2 4.yar *
rule malware_test_ {
  meta:
    description = "Detects malware name 4.exe sample"
    author = "Mohamad Almasri"

  strings:
    $s1 = "GetCPInfo" ascii wide
    $s2 = "GHeapReAlloc" ascii wide
    $s3 = "GCreateFileW" ascii wide

  condition:
    $s1 or $s2 or $s3
}
```

[line 17/17 (100%), col 1/ 1 (100%), char 303/303 (100%)]

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark
^X Exit ^R Read File ^M Replace ^U Paste ^J Justify ^_ Go To Line M-E Redo M-6 Copy

```

mjolnirtraining@MT23-IR-Kali: ~/Desktop/volatility3
File Actions Edit View Help
[mjolnirtraining@MT23-IR-Kali]~$ cd Desktop/volatility3
[mjolnirtraining@MT23-IR-Kali]~/Desktop/volatility3$ ls -l ./../home/mjolnirtraining/Desktop/volatility3/custom-signatures'
ls: cannot access './../home/mjolnirtraining/Desktop/volatility3/custom-signatures': No such file or directory

[mjolnirtraining@MT23-IR-Kali]~/Desktop/volatility3$ ls -l ../home/mjolnirtraining/Desktop/volatility3/custom-signatures'
total 16
drwxr-xr-x 3 mjolnirtraining mjolnirtraining 4096 Oct  8 06:26 iocs
drwxr-xr-x 2 mjolnirtraining mjolnirtraining 4096 Oct  8 06:26 misc
drwxr-xr-x 2 mjolnirtraining mjolnirtraining 4096 Oct  8 06:26 sigma
drwxr-xr-x 2 mjolnirtraining mjolnirtraining 4096 Nov 13 15:25 yara

[mjolnirtraining@MT23-IR-Kali]~/Desktop/volatility3$ ls -l ../home/mjolnirtraining/Desktop/volatility3/custom-signatures/yara'
total 8
-rw-rw-r-- 1 mjolnirtraining mjolnirtraining 302 Nov 13 15:25 4.yar
-rw-rw-r-- 1 mjolnirtraining mjolnirtraining 430 Nov 13 15:10 CKYIJlo.yar

[mjolnirtraining@MT23-IR-Kali]~/Desktop/volatility3$

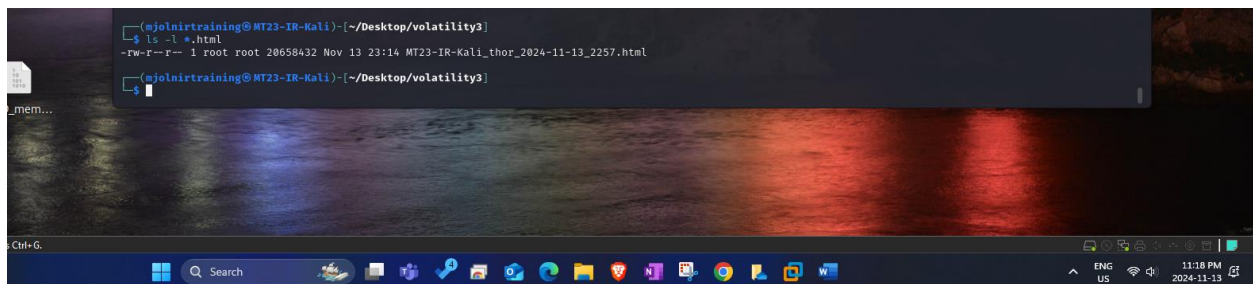
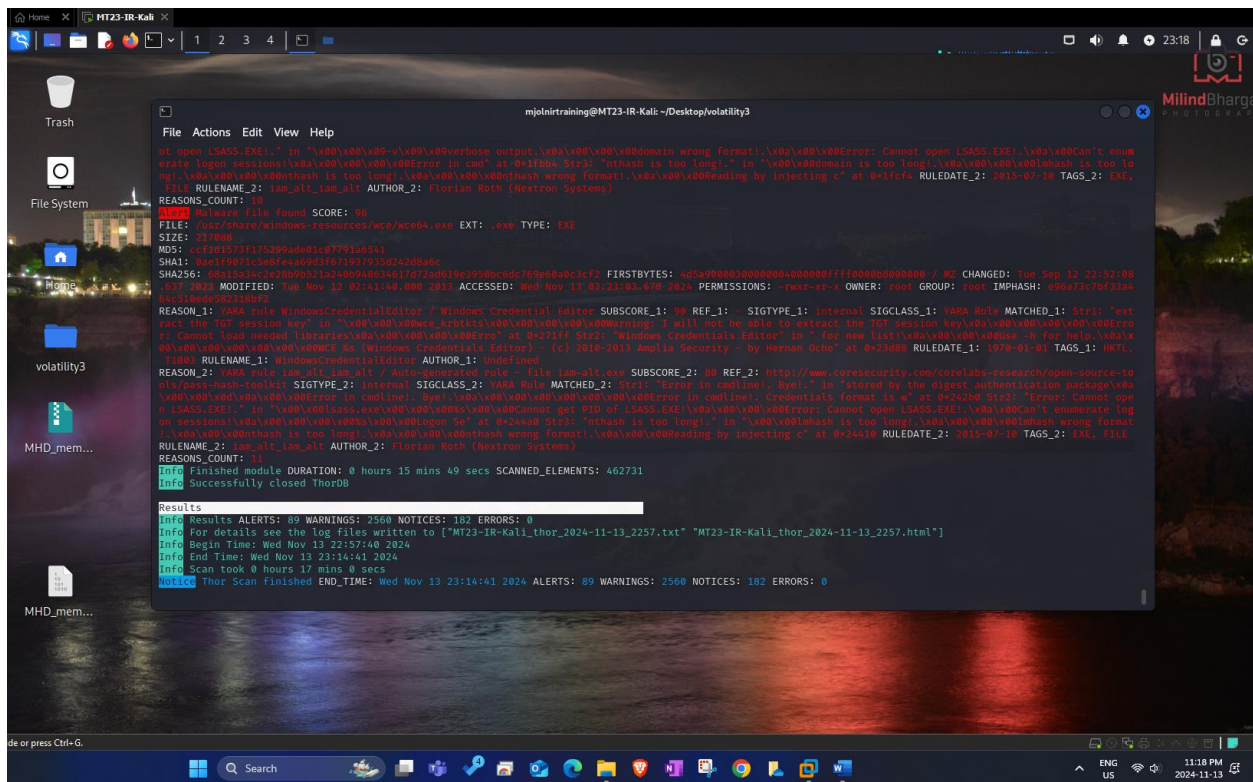
```

I downloaded THOR Lite a scanning tool which allowed US to use it for checking the memory dump

```

mjolnirtraining@MT23-IR-Kali: ~/Desktop/volatility3
File Actions Edit View Help
[mjolnirtraining@MT23-IR-Kali]~/Desktop/volatility3$ unzip /home/mjolnirtraining/Downloads/thor10.7lite-linux-pack.zip
Archive: /home/mjolnirtraining/Downloads/thor10.7lite-linux-pack.zip
  creating: signatures/
    creating: signatures/sigma/
      inflating: signatures/sigma/thor.yml
    creating: signatures/sigma/category/
      inflating: signatures/sigma/category/antivirus/
        inflating: signatures/sigma/category/antivirus/av_relevant_files.yml
        inflating: signatures/sigma/category/antivirus/av_webshell.yml
        inflating: signatures/sigma/category/antivirus/av_pansomware.yml
        inflating: signatures/sigma/category/antivirus/av_exploiting.yml
        inflating: signatures/sigma/category/antivirus/av_password_dumper.yml
        inflating: signatures/sigma/category/antivirus/av_hacktool.yml
      creating: signatures/sigma/windows/
        inflating: signatures/sigma/windows/sysmon/
          inflating: signatures/sigma/windows/sysmon/sysmon_file_executable_detected.yml
          inflating: signatures/sigma/windows/sysmon/sysmon_config_modification_status.yml
          inflating: signatures/sigma/windows/sysmon/sysmon_file_block_executable.yml
          inflating: signatures/sigma/windows/sysmon/sysmon_config_modification_error.yml
          inflating: signatures/sigma/windows/sysmon/sysmon_file_block_shredding.yml
        creating: signatures/sigma/windows/create_stream_hash/
          inflating: signatures/sigma/windows/create_stream_hash/create_stream_hash_file_sharing_domains_download_susp_extension.yml
          inflating: signatures/sigma/windows/create_stream_hash/create_stream_hash_hkml_generic_download.yml
          inflating: signatures/sigma/windows/create_stream_hash/create_stream_hash_file_sharing_domains_download_unusual_extension.yml
          inflating: signatures/sigma/windows/create_stream_hash/create_stream_hash_susp_ip_domains.yml
          inflating: signatures/sigma/windows/create_stream_hash/create_stream_hash_ads_executable.yml
          inflating: signatures/sigma/windows/create_stream_hash/create_stream_hash_creation_internet_file.yml
          inflating: signatures/sigma/windows/create_stream_hash/create_stream_hash_zip_tld_download.yml
          inflating: signatures/sigma/windows/create_stream_hash/create_stream_hash_winget_susp_package_source.yml
          inflating: signatures/sigma/windows/create_stream_hash/create_stream_hash_regedit_export_to_ads.yml
        creating: signatures/sigma/windows/powershell/
          creating: signatures/sigma/windows/powershell/powershell_module/
            inflating: signatures/sigma/windows/powershell/powershell_module/posh_pm_syncappypublishingserver_exe.yml
            inflating: signatures/sigma/windows/powershell/powershell_module/posh_pm_remote_powershell_session.yml
            inflating: signatures/sigma/windows/powershell/powershell_module/posh_pm_malicious_commandlets.yml

```

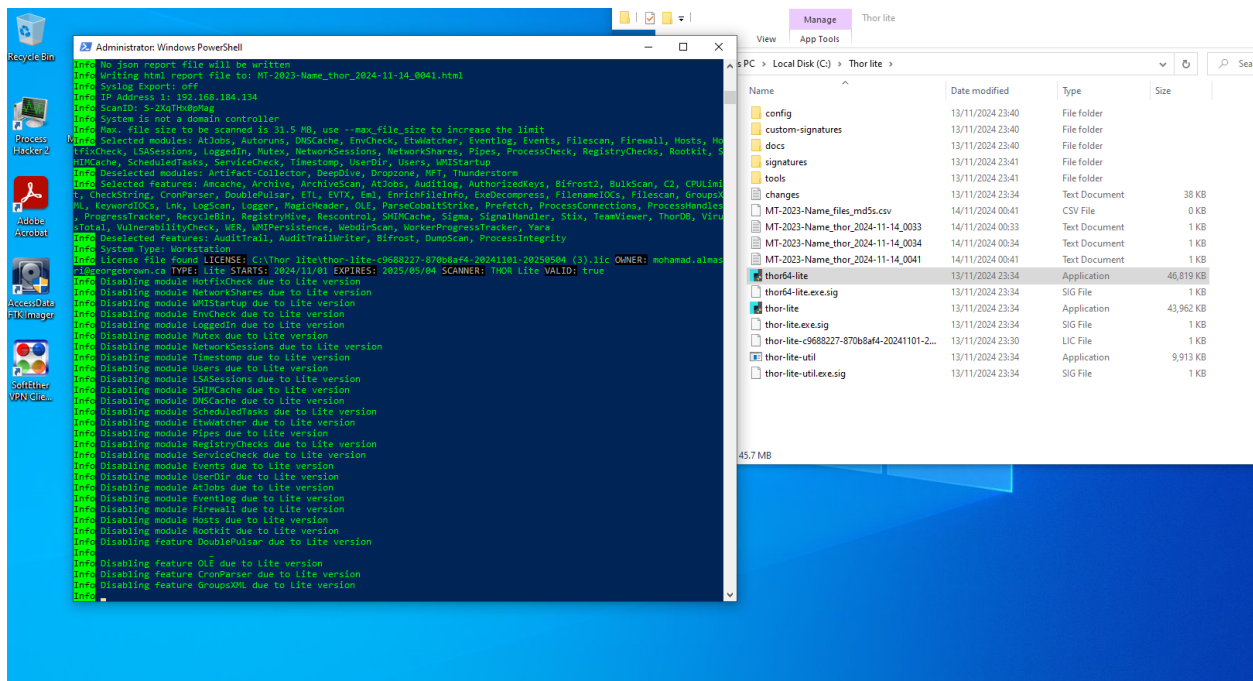



Run THOR Lite and Generate a Report: Finally, I ran THOR Lite with thor-lite-linux-64 and generated a report to see any detections.

THOR Lite produced an HTML report showing any detections.

ON WINDOWS:

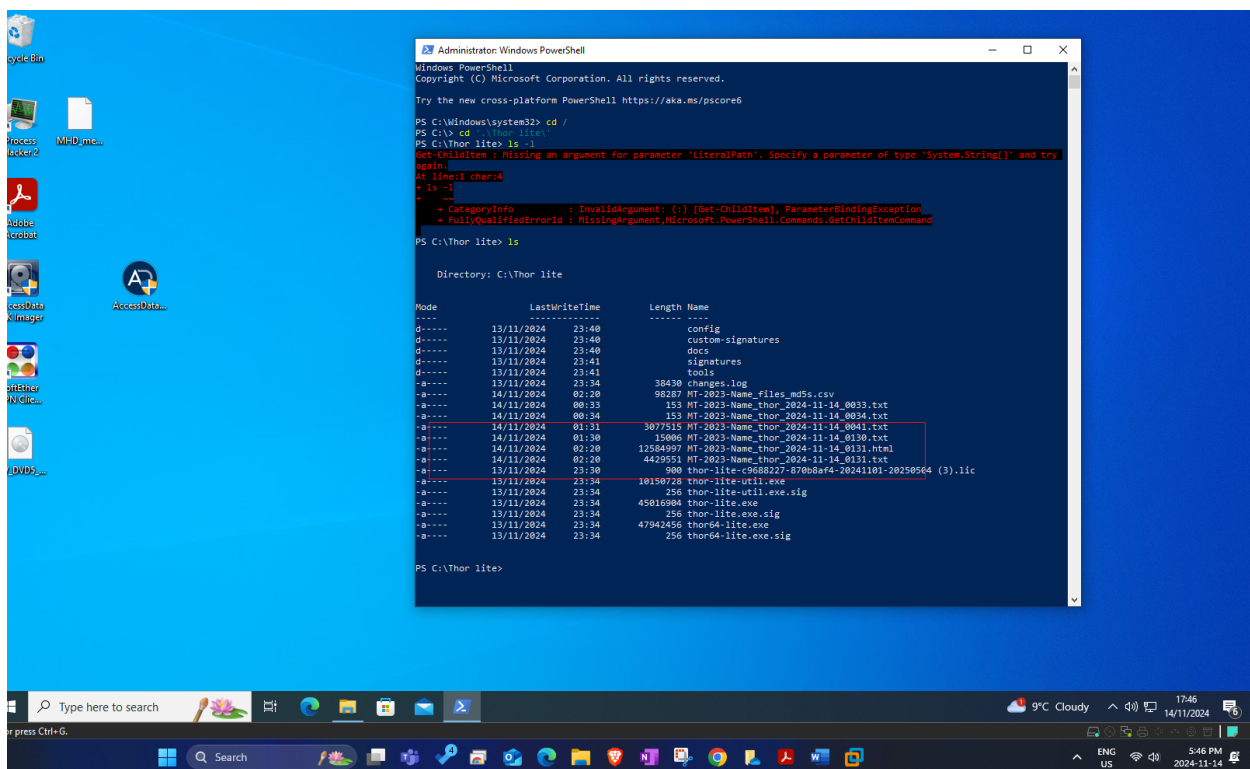
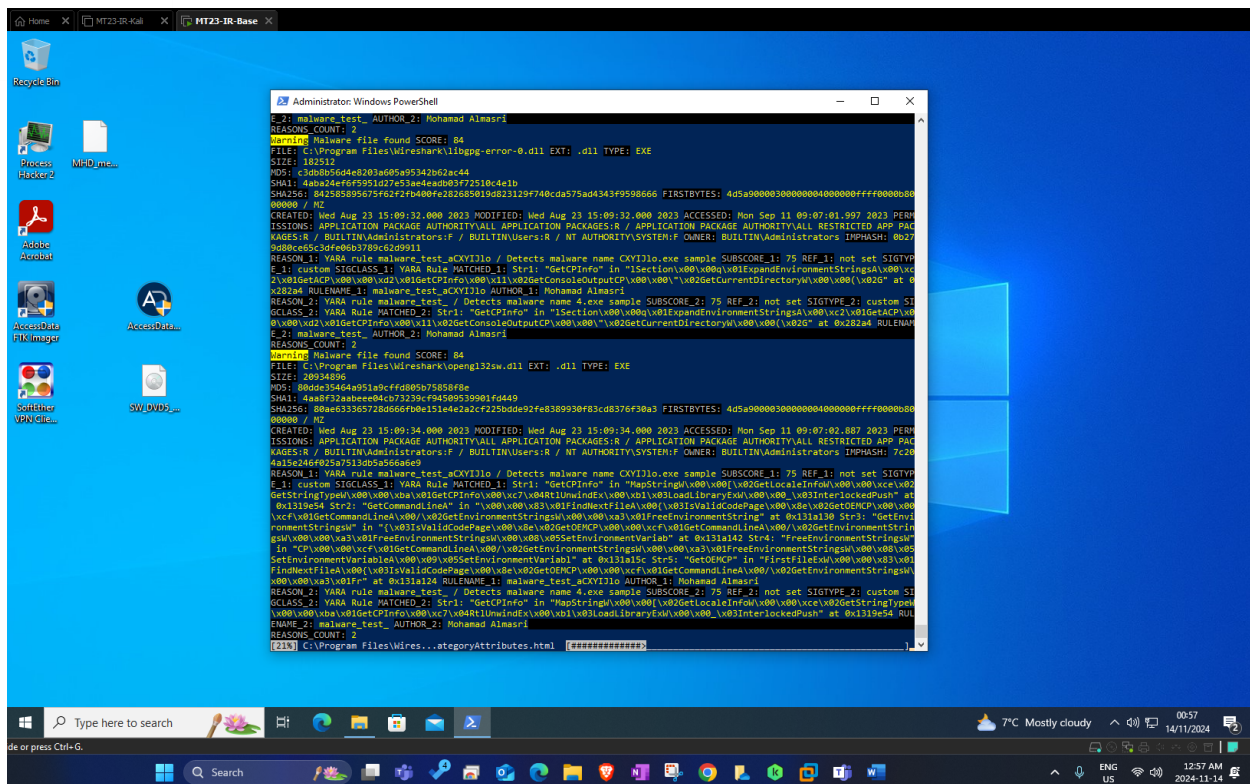
DOWNLOAD Thor lite and extract it then copy the license



THOR Lite is scanning the system files and registry entries

THOR Lite is applying YARA rules, identifying the files as potentially suspicious, and giving them scores based on the findings.

Detailed information about the file's location, creation date, and matching YARA rule is displayed.



MOHAMAD ALMASR 101167438

```
-a--- 14/11/2024 02:20 12584997 MT-2023-Name_thor_2024-11-14_0131.html
-a--- 14/11/2024 02:20 4429551 MT-2023-Name_thor_2024-11-14_0131.txt
```

[illegible][illegible]