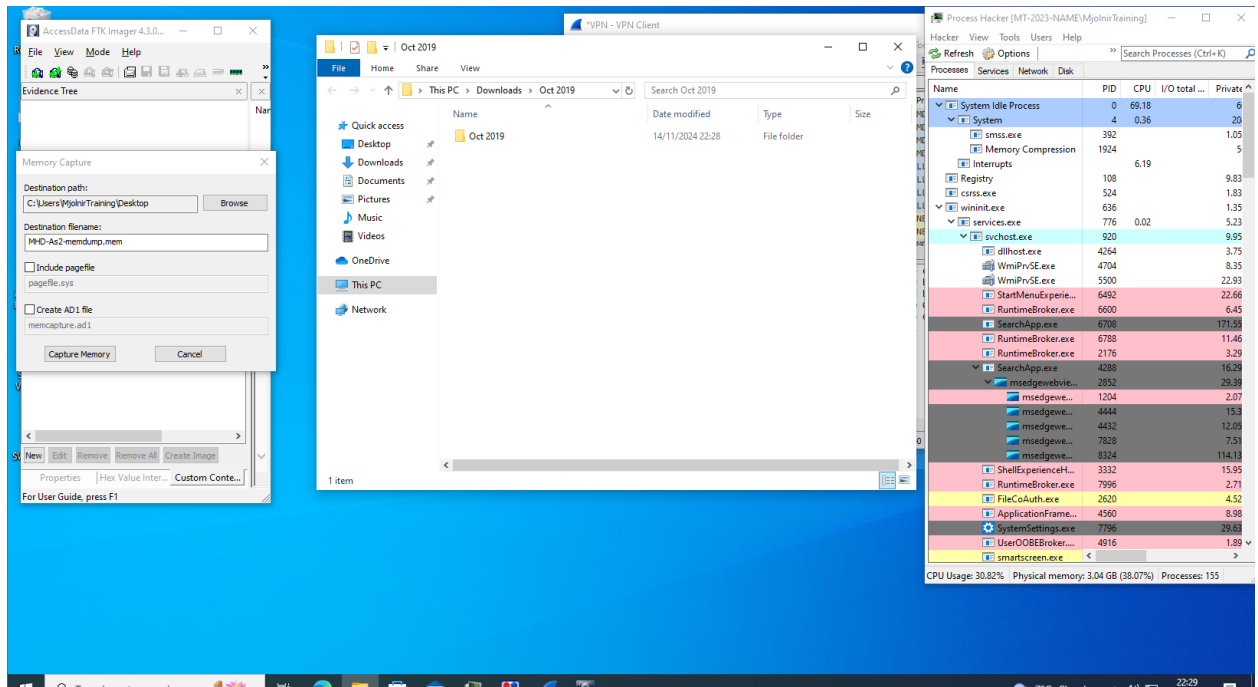
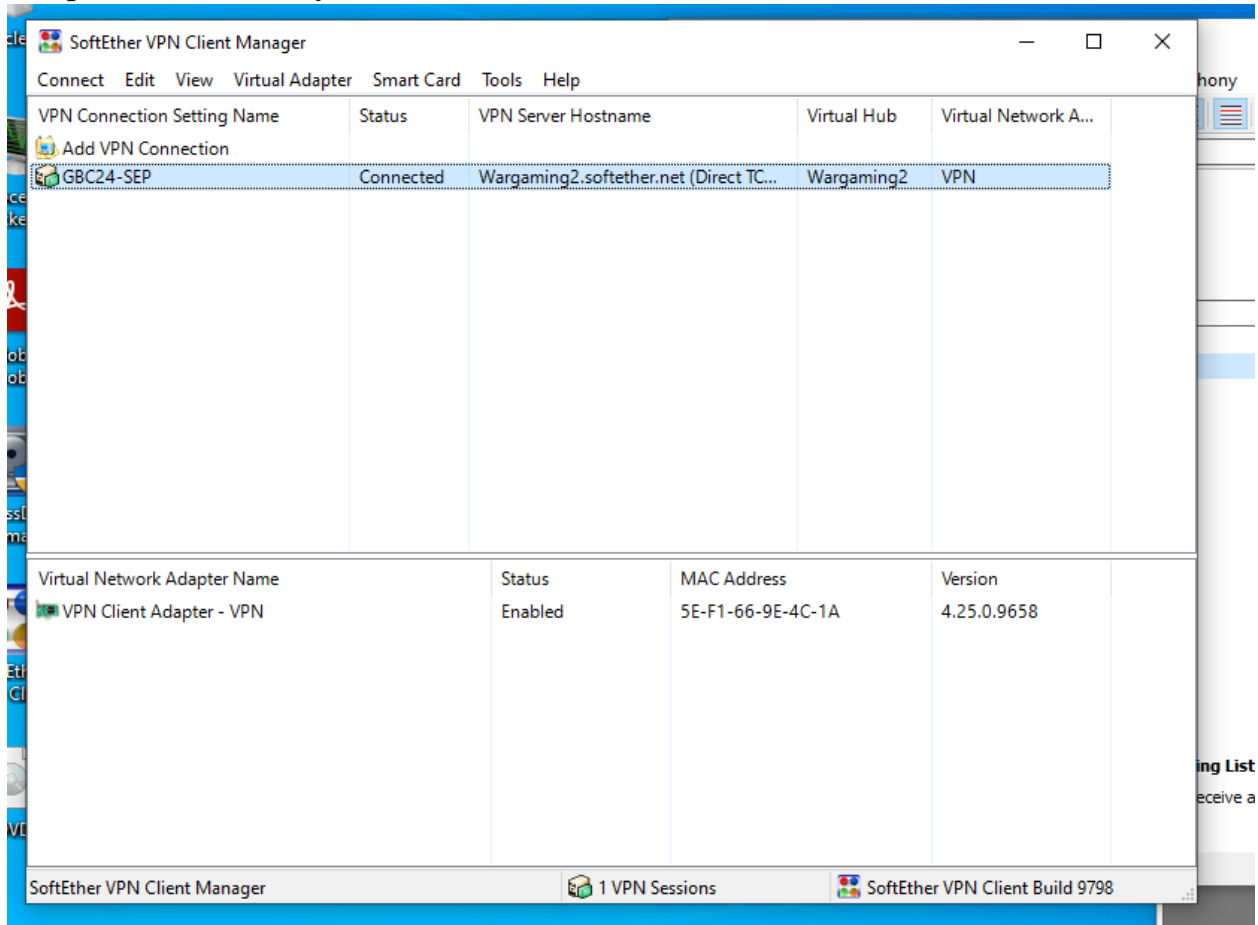


DIGITAL FORENSICS&INCID. RESP - COMP 4071**Assignment 2****Introduction:**

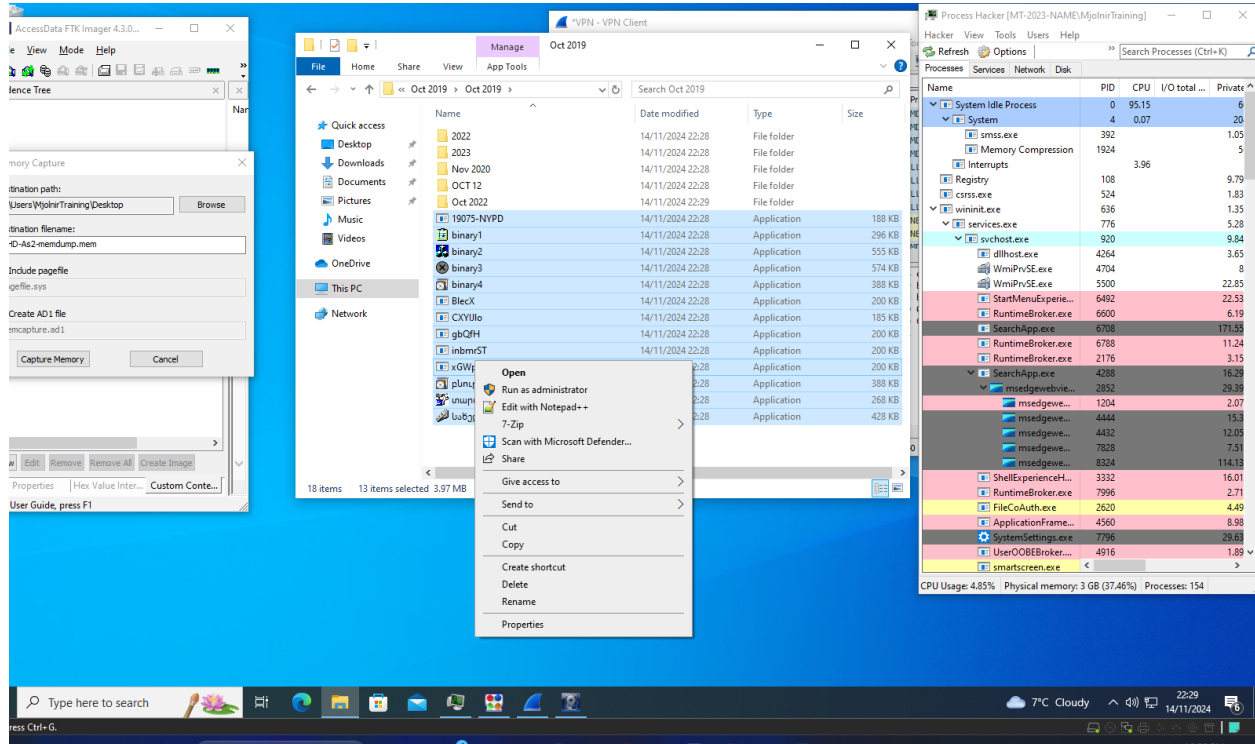
I executed a sample of ransomware in a virtual machine to analyze the sample in this assignment. A range of forensic tools was used in the analysis to identify malicious processes . The focus was on examining memory data, creating YARA rules related to identified ransomware and testing them with the THOR Lite scanner. This report will tell the whole story of how was the evidence collected, what was done with that evidence and finally, analysis of the evidence. Each and everything you will find in this report including a description of the tool which was used and its challenges.

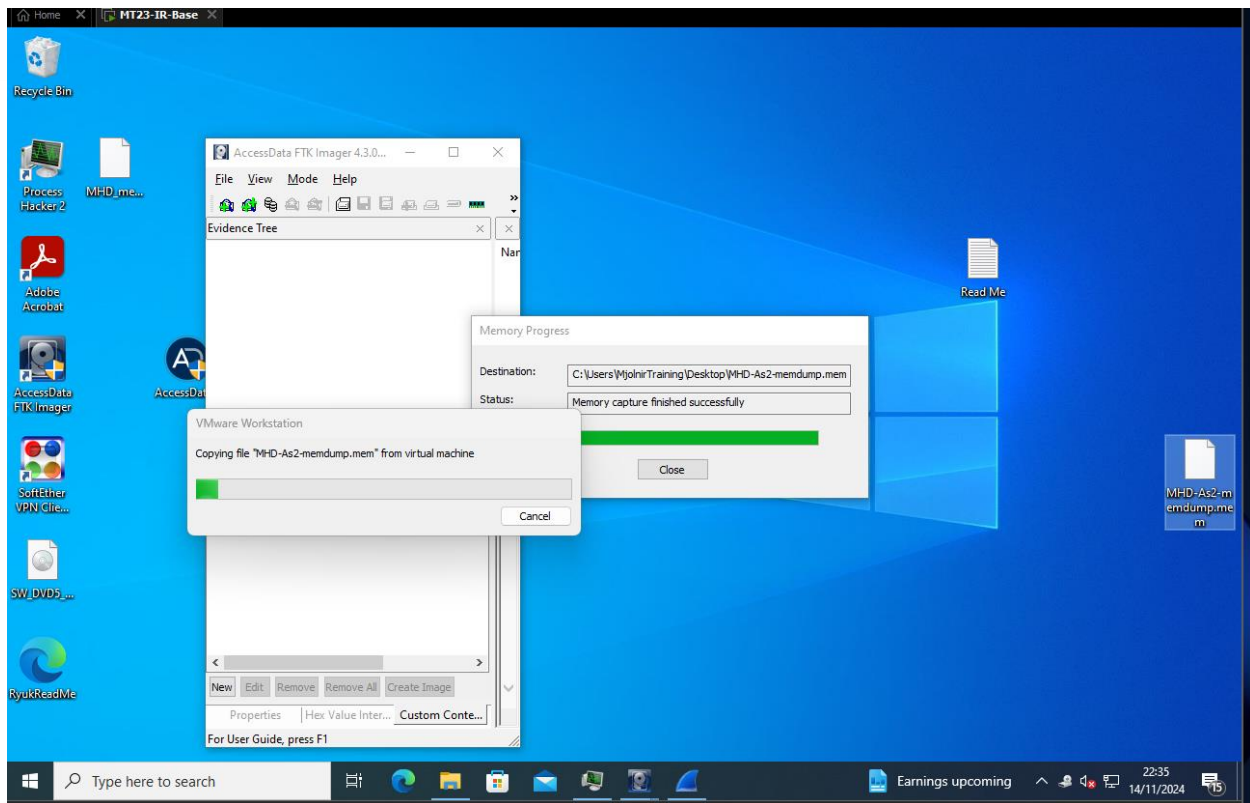
At the start of the process, I prepared my VMware virtual machine and connected to the VPN. After that, I navigated to my system to access the necessary files. I opened the "October 2019" folder, which contained all the ransomware malware

samples for this analysis.

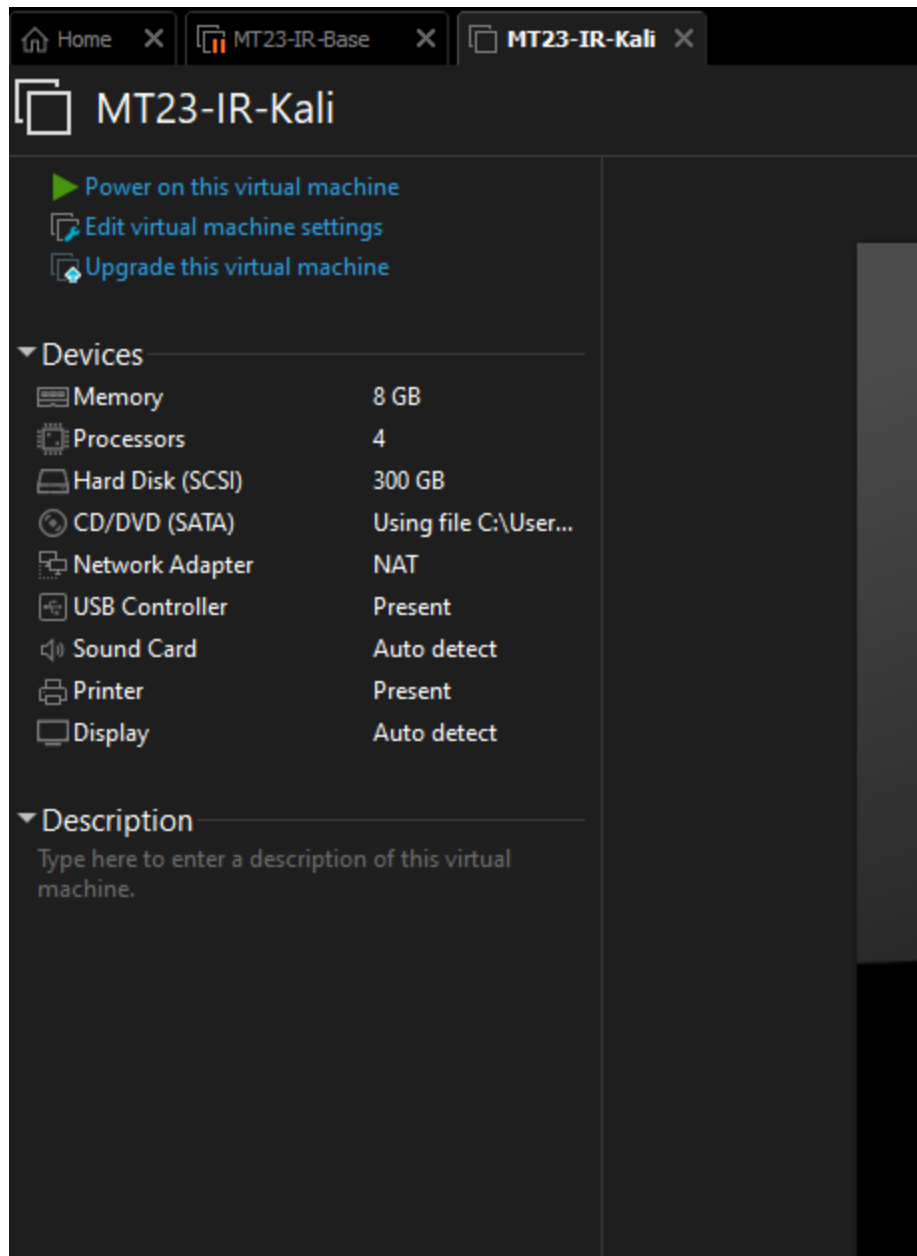


Each ransomware sample was run as an administrator to ensure it executed correctly and fully

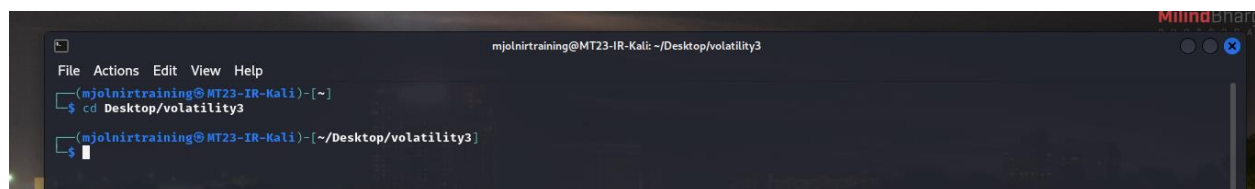




After the memory dump was complete, I copied the file to my Kali machine for analysis. The VM was paused

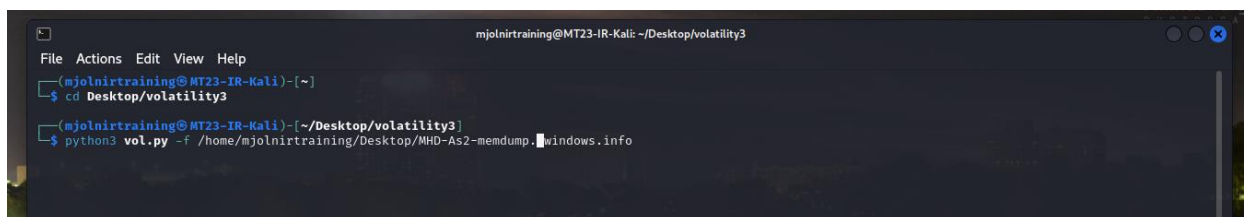


On the Kali VM, I opened the Volatility 3 framework on the terminal to analyze the memory dump.

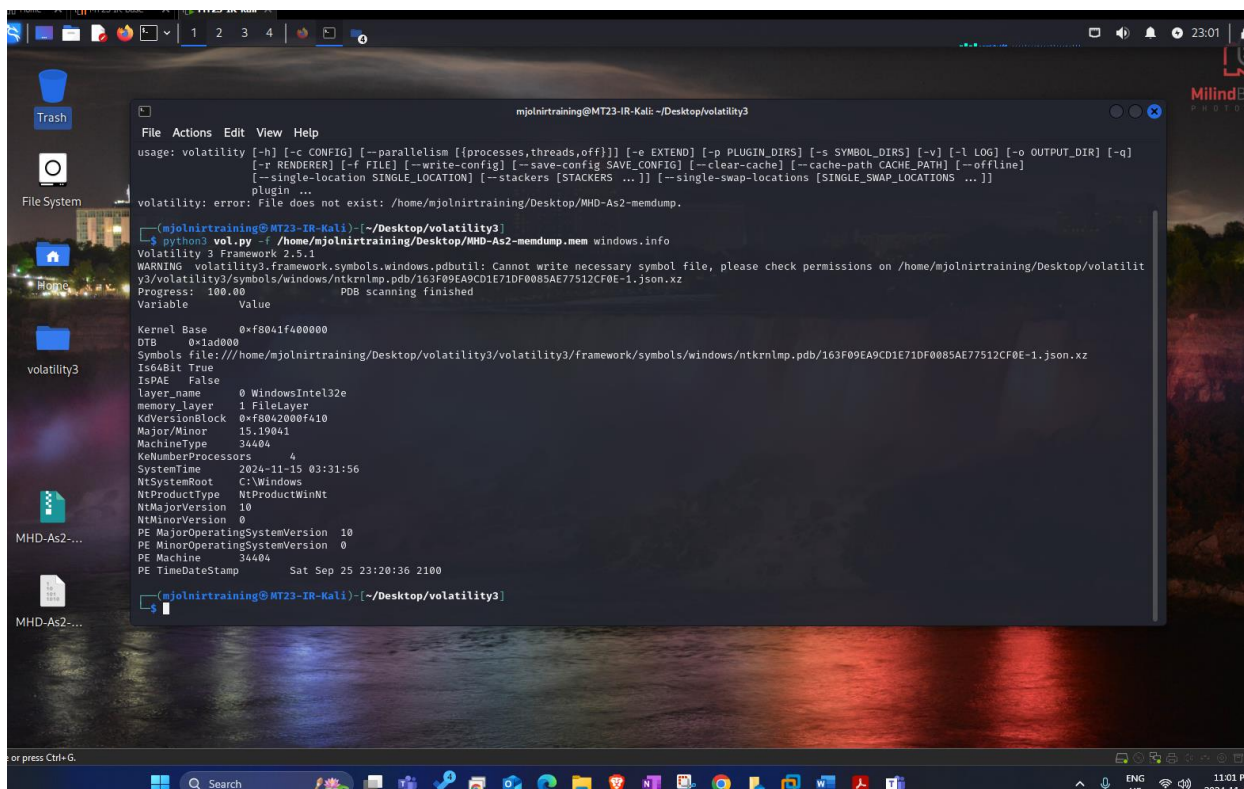


windows.info: This command provided general information about the memory dump, such as the OS version, architecture, and more. It ensures compatibility with subsequent commands.

As you see the screenshot Shows the metadata about the memory dump, validating the environment details.



```
mjolinirtraining@MT23-IR-Kali: ~/Desktop/volatility3
File Actions Edit View Help
(mjolinirtraining@MT23-IR-Kali)-[~]
$ cd Desktop/volatility3
(mjolinirtraining@MT23-IR-Kali)-[~/Desktop/volatility3]
$ python3 vol.py -f /home/mjolinirtraining/Desktop/MHD-As2-memdump. windows.info
```



```
mjolinirtraining@MT23-IR-Kali: ~/Desktop/volatility3
File Actions Edit View Help
usage: volatility [-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]
[--single-location SINGLE_LOCATION] [--stackers [STACKERS ...]] [--single-swap-locations [SINGLE_SWAP_LOCATIONS ...]]
plugin ...
volatility: error: File does not exist: /home/mjolinirtraining/Desktop/MHD-As2-memdump.
(mjolinirtraining@MT23-IR-Kali)-[~/Desktop/volatility3]
$ python3 vol.py -f /home/mjolinirtraining/Desktop/MHD-As2-memdump.mem windows.info
Volatility 3 Framework 2.5.1
WARNING volatility3.framework.symbols.windows.pdbutil: Cannot write necessary symbol file, please check permissions on /home/mjolinirtraining/Desktop/volatility3/volatility3/symbols/windows/ntkrnlmp.pdb/163F09EA9CD1E71DF0085AE77512CF0E-1.json.xz
Progress: 100.00 PDB scanning finished
Variable Value
Kernel Base 0xf8041f400000
DTB 0x1ad000
Symbols file:///home/mjolinirtraining/Desktop/volatility3/volatility3/framework/symbols/windows/ntkrnlmp.pdb/163F09EA9CD1E71DF0085AE77512CF0E-1.json.xz
Is64Bit True
IsPAE False
layer_name 0 WindowsIntel32e
memory_layer 1 FileLayer
KdVersionBlock 0xf8042000f410
Major/Minor 15.19041
MachineType 34404
KeNumberProcessors 4
SystemTime 2024-11-15 03:31:56
NTSystemRoot C:\Windows
NTProductType NTProductWinNT
NTMajorVersion 10
NTMinorVersion 0
PE MajorOperatingSystemVersion 10
PE MinorOperatingSystemVersion 0
PE Machine 34404
PE TimeDateStamp Sat Sep 25 23:20:36 2100
(mjolinirtraining@MT23-IR-Kali)-[~/Desktop/volatility3]
```

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. As you see the screenshot Highlights two processes identified as suspicious. Another two were found in subsequent results.


```
(mjolnirtraining@MT23-IR-Kali)-[~/Desktop/volatility3]
$ python3 vol.py -f /home/mjolnirtraining/Desktop/MHD-As2-memdump.mem windows.dmpfiles.DumpFiles --pid 7580
Volatility 3 Framework 2.5.1
Progress: 100.00 PDB scanning finished
Cache FileObject FileName Result
DataSectionObject 0x9385c5221290 mpr.dll file.0x9385c5221290.0x9385c5415d30.ImageSectionObject.mpr.dll.img
ImageSectionObject 0x9385c5221290 mpr.dll file.0x9385c5221290.0x9385c5415d30.ImageSectionObject.mpr.dll.img
DataSectionObject 0x9385c7db5ae0 xGwpgNo.exe file.0x9385c7db5ae0.0x9385c77aba10.DataSectionObject.xGwpgNo.exe.dat
ImageSectionObject 0x9385c7db5ae0 xGwpgNo.exe file.0x9385c7db5ae0.0x9385c73e1a20.ImageSectionObject.xGwpgNo.exe.img
ImageSectionObject 0x9385c594ecb0 virtdisk.dll file.0x9385c594ecb0.0x9385c59a9050.ImageSectionObject.virtdisk.dll.img
```

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.

```
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 0 Nov 14 23:14 file.0x9385c5221290.0x9385c7744d10.DataSectionObject.mpr.dll.dat
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 127488 Nov 14 23:14 file.0x9385c5946910.0x9385befaaa20.ImageSectionObject.edputil.dll.img
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 57856 Nov 14 23:14 file.0x9385c594ecb0.0x9385c59a9050.ImageSectionObject.virtdisk.dll.img
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 26112 Nov 14 23:14 file.0x9385c59535d0.0x9385c59a6740.ImageSectionObject.fltlib.dll.img
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 462336 Nov 14 23:14 file.0x9385c5f681e0.0x9385c51afa20.ImageSectionObject.OneCoreCommonProxyStub
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 583680 Nov 14 23:14 file.0x9385c6613140.0x9385c1127750.ImageSectionObject.AppResolver.dll.img
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 3398656 Nov 14 23:14 file.0x9385c732ac80.0x9385c63b98a0.ImageSectionObject.OneCoreUAPCommonProxyS
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 206848 Nov 14 23:14 file.0x9385c7db5ae0.0x9385c73e1a20.ImageSectionObject.xGwpgNo.exe.img
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 204800 Nov 14 23:14 file.0x9385c7db5ae0.0x9385c77aba10.DataSectionObject.xGwpgNo.exe.dat
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 79 Sep 13 2023 mypy.ini
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 1854 Sep 13 2023 setup.py
drwxr-xr-x 2 mjolnirtraining mjolnirtraining 4096 Sep 13 2023 test
drwxr-xr-x 2 mjolnirtraining mjolnirtraining 4096 Oct 8 06:26 tools
drwxr-xr-x 1 mjolnirtraining mjolnirtraining 290 Sep 13 2023 vol.py
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 5450 Sep 13 2023 vol.spec
drwxr-xr-x 8 mjolnirtraining mjolnirtraining 4096 Sep 13 2023 volatility3
drwxr-xr-x 2 root root 4096 Sep 13 2023 volatility3.egg-info
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 297 Sep 13 2023 volshell.py
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 2963 Sep 13 2023 volshell.spec
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 206848 Nov 14 23:15 xGwpgNo.exe
(mjolnirtraining@MT23-IR-Kali)-[~/Desktop/volatility3]
$
```

```
(mjolnirtraining@MT23-IR-Kali)-[~/Desktop/volatility3]
$ ls -l
total 232
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 5947 Sep 13 2023 README.md
drwxr-xr-x 4 root root 4096 Sep 13 2023 build
drwxr-xr-x 2 mjolnirtraining mjolnirtraining 4096 Oct 8 06:26 config
drwxr-xr-x 3 mjolnirtraining mjolnirtraining 4096 Sep 13 2023 development
drwxr-xr-x 2 root root 4096 Sep 13 2023 dist
drwxr-xr-x 3 mjolnirtraining mjolnirtraining 4096 Sep 13 2023 doc
drwxr-xr-x 2 mjolnirtraining mjolnirtraining 4096 Oct 8 06:26 docs
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 79 Sep 13 2023 mypy.ini
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 1854 Sep 13 2023 setup.py
drwxr-xr-x 2 mjolnirtraining mjolnirtraining 4096 Sep 13 2023 test
drwxr-xr-x 2 mjolnirtraining mjolnirtraining 4096 Oct 8 06:26 tools
drwxr-xr-x 1 mjolnirtraining mjolnirtraining 290 Sep 13 2023 vol.py
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 5450 Sep 13 2023 vol.spec
drwxr-xr-x 8 mjolnirtraining mjolnirtraining 4096 Sep 13 2023 volatility3
drwxr-xr-x 2 root root 4096 Sep 13 2023 volatility3.egg-info
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 297 Sep 13 2023 volshell.py
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 2963 Sep 13 2023 volshell.spec
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 206848 Nov 14 23:15 xGwpgNo.exe
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 14153 Nov 14 23:17 xGwpgNo.exe.mohamad
(mjolnirtraining@MT23-IR-Kali)-[~/Desktop/volatility3]
$
```

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.

MOHAMAD ALMASR 101167438

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.

```

File Actions Edit View Help
drwxr-xr-x 2 root root 4096 Sep 13 2023 volatility3.egg-info
-rwxr-xr-x 1 mjohnirtraining mjohnirtraining 297 Sep 13 2023 volshell.py
-rw-r--r-- 1 mjohnirtraining mjohnirtraining 2963 Sep 13 2023 volshell.spec
-rw-r--r-- 1 mjohnirtraining mjohnirtraining 206848 Nov 14 23:15 xGwpgNo.exe
-rw-r--r-- 1 mjohnirtraining mjohnirtraining 14153 Nov 14 23:17 xGwpgNo.exe.mohamad

(mjohnirtraining@MT23-IR-Kali)-[~/Desktop/volatility3]
$ cat -n xGwpgNo.exe.mohamad
 1 !This program cannot be run in DOS mode.
 2 { }ux
 3 URich
 4 .text
 5 .rdata
 6 @.data
 7 .pdata
 8 @.gfix
 9 @.reloc
10 H SVWH
11 t$ L
12 0 ^[
13 \AA
14 D$B|
15 D$0L
16 D$0H
17 D$(A
18 \ $ H
19 9/$d
20 H VWAVH
21 D$XL
22 T$Xf
23 D$X3
24 T$Xf
25 D$X3
26 T$Xf
27 T$X3
28 \ $H
29 T$HH

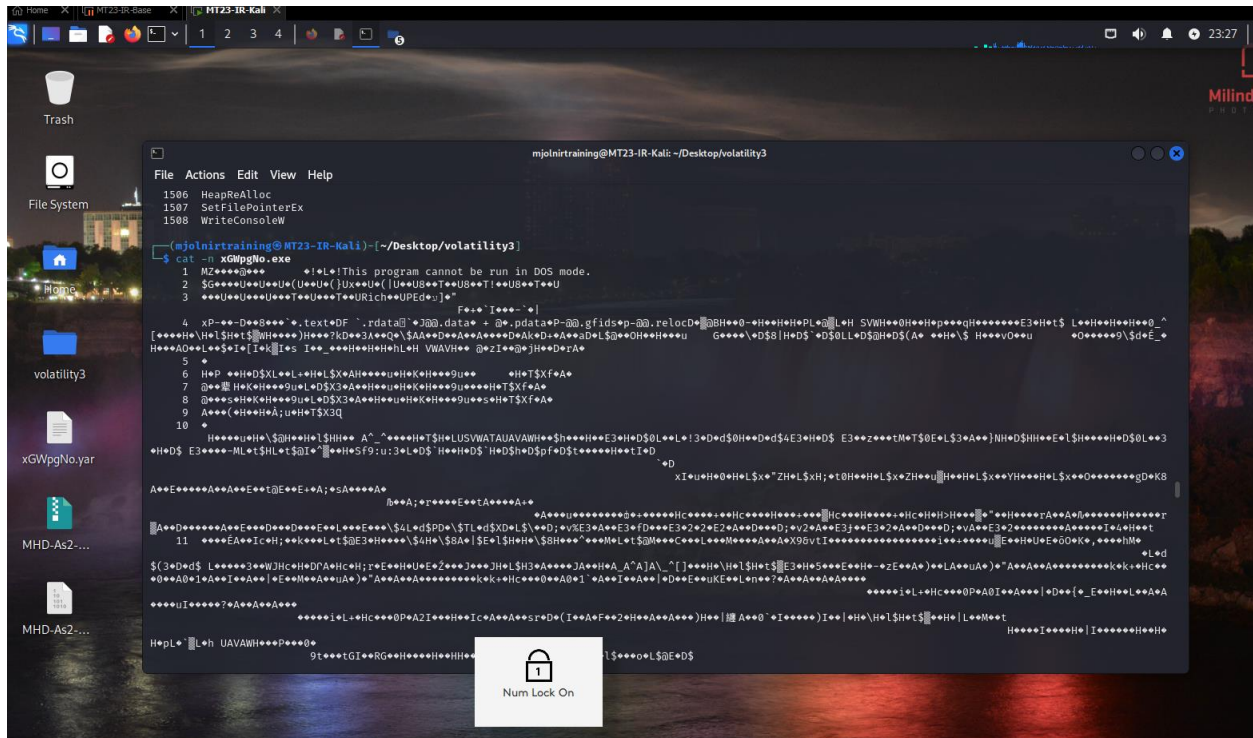
```

```

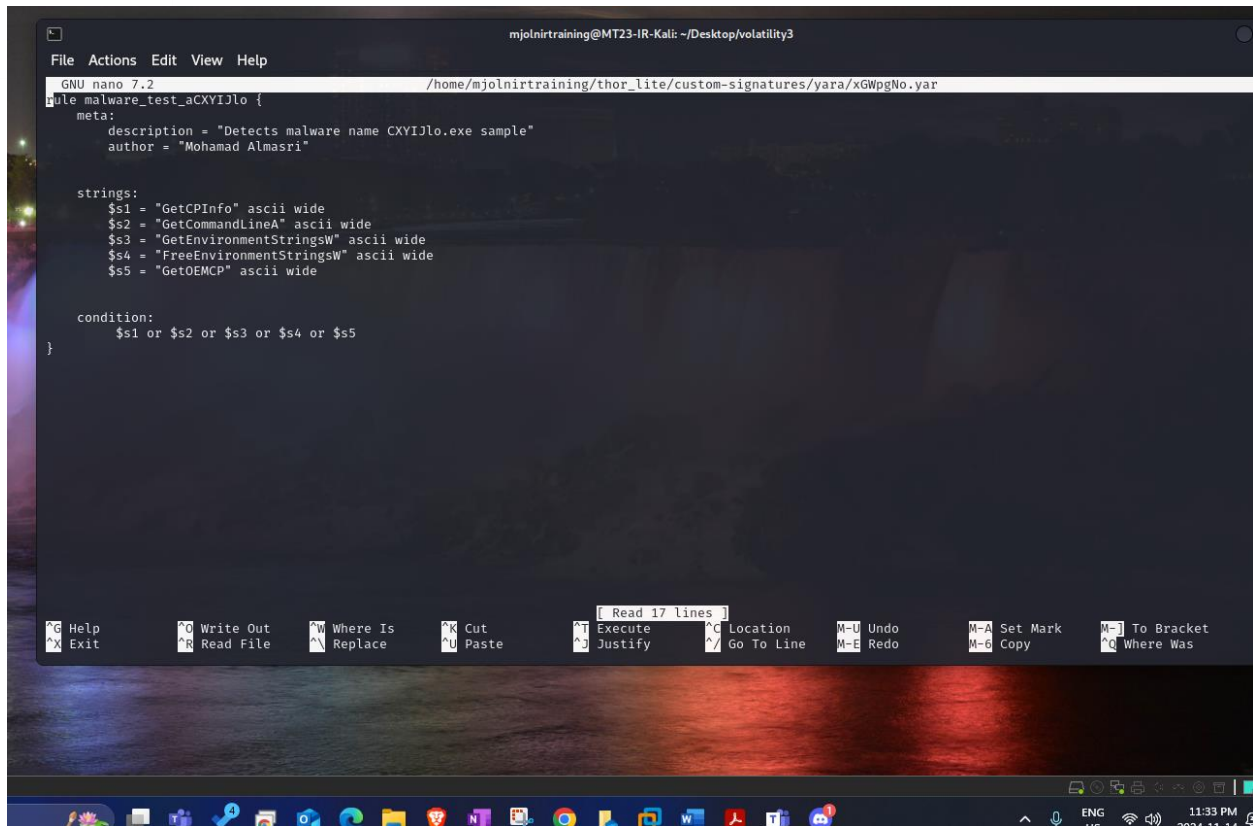
File Actions Edit View Help
1475 DeleteCriticalSection
1476 InitializeCriticalSectionAndSpinCount
1477 TlsAlloc
1478 TlsGetValue
1479 TlsSetValue
1480 TlsFree
1481 LoadLibraryExW
1482 TerminateProcess
1483 GetModuleHandleExW
1484 GetStdHandle
1485 WriteFile
1486 MultiByteToWideChar
1487 WideCharToMultiByte
1488 GetACP
1489 LCMAPStringW
1490 GetStringTypeW
1491 GetFileType
1492 FindClose
1493 FindFirstFileExW
1494 FindNextFileW
1495 IsValidCodePage
1496 GetOEMCP
1497 GetCPInfo
1498 GetCommandLineA
1499 GetEnvironmentStringsW
1500 FreeEnvironmentStringsW
1501 SetStdHandle
1502 FlushFileBuffers
1503 GetConsoleCP
1504 GetConsoleMode
1505 HeapSize
1506 HeapReAlloc
1507 SetFilePointerEx
1508 WriteConsoleW

(mjohnirtraining@MT23-IR-Kali)-[~/Desktop/volatility3]
$ cat -n xGwpgNo.exe.mohamad

```



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.

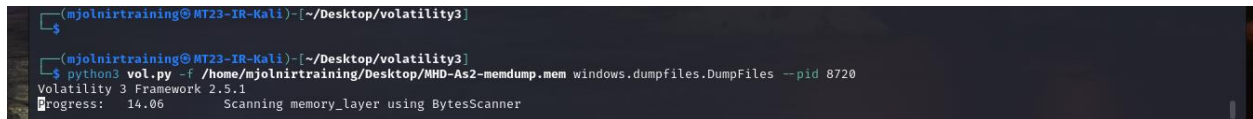


```
mjolinirtraining@MT23-IR-Kali: ~/Desktop/volatility3
GNU nano 7.2 /home/mjolinirtraining/thor_lite/custom-signatures/yara/xGwpgNo.yar
rule malware_test_aCXIJIlo {
  meta:
    description = "Detects malware name CXIJIlo.exe sample"
    author = "Mohamad Almasri"

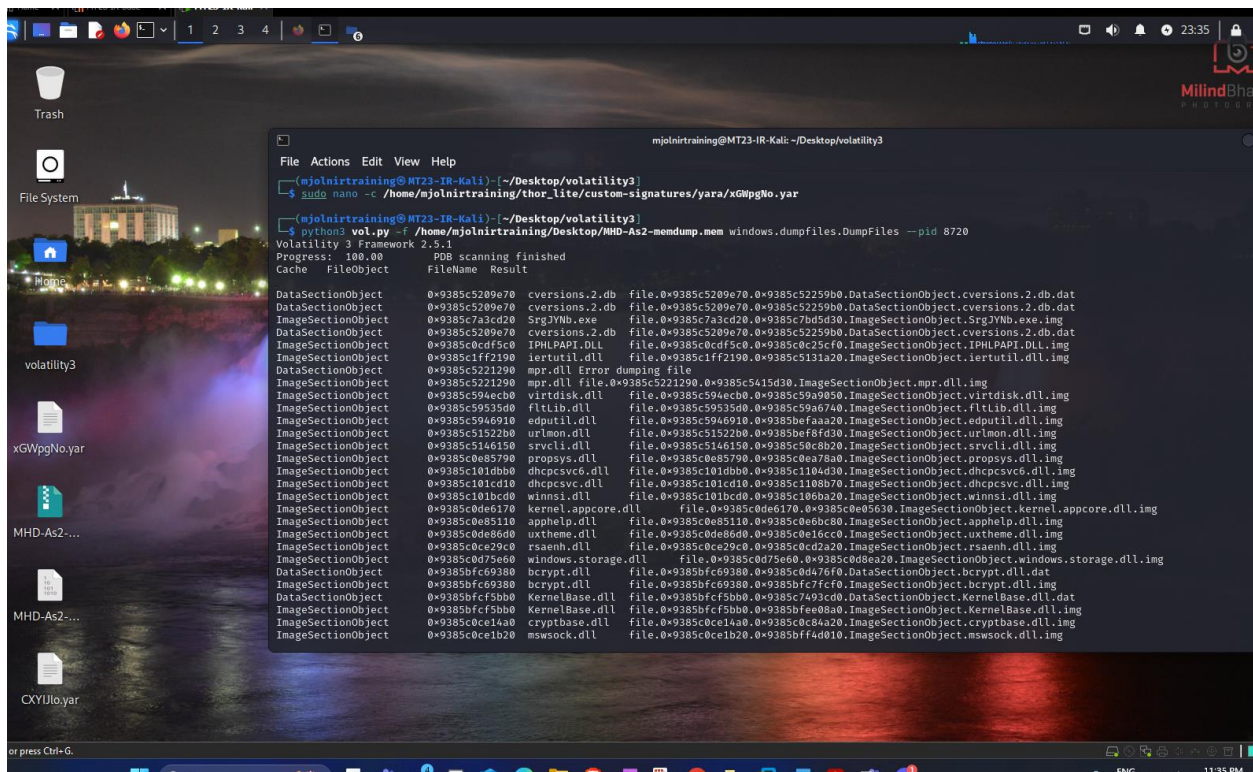
  strings:
    $s1 = "GetCPInfo" ascii wide
    $s2 = "GetCommandLineA" ascii wide
    $s3 = "GetEnvironmentStringsW" ascii wide
    $s4 = "FreeEnvironmentStringsW" ascii wide
    $s5 = "GetOEMCP" ascii wide

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

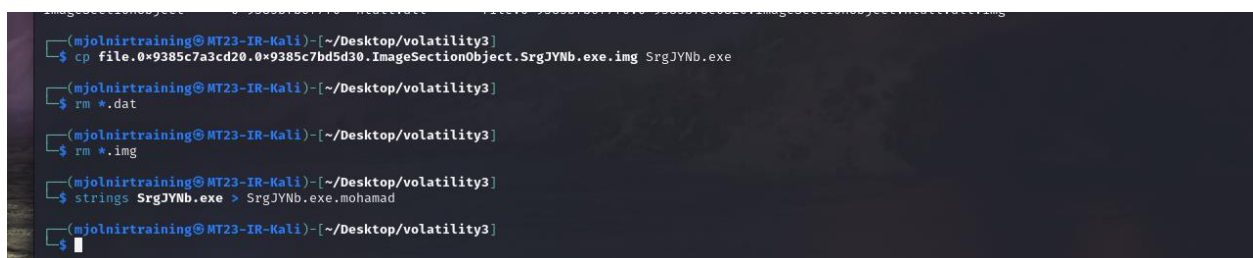
Help Exit Write Out Read File Where Is Replace Cut Paste Read 17 lines Execute Justify Location Go To Line Undo Redo Set Mark Copy To Bracket Where Was



```
(mjolinirtraining@MT23-IR-Kali)-[~/Desktop/volatility3]
(mjolinirtraining@MT23-IR-Kali)-[~/Desktop/volatility3]
$ python3 vol.py -f /home/mjolinirtraining/Desktop/MHD-As2-memdump.mem windows.dumpfiles.DumpFiles --pid 8720
Volatility 3 Framework 2.5.1
Progress: 14.06 Scanning memory_layer using BytesScanner
```



```
DataSectionObject 0x9385c5209e70 cversions.2.db file.0x9385c5209e70.0x9385c52259b0.DataSectionObject.cversions.2.db.dat
ImageSectionObject 0x9385c7a3cd20 SrgJYNb.exe file.0x9385c7a3cd20.0x9385c7bd5d30.ImageSectionObject.SrgJYNb.exe.img
DataSectionObject 0x9385c5209e70 cversions.2.db file.0x9385c5209e70.0x9385c52259b0.DataSectionObject.cversions.2.db.dat
```




```
mjolinirtraining@MT23-IR-Kali: ~/Desktop/volatility3
File Actions Edit View Help
GNU nano 7.2 /home/mjolinirtraining/thor_lite/custom-signatures/yara/SrgJYNb.yar
rule malware_test_SrgJYNb{
  meta:
    description = "Detects malware name SrgJYNb.exe sample"
    author = "Mohamad Almasri"

  strings:
    $s1 = "LCMapStringW" ascii wide
    $s2 = "EnterCriticalSection" ascii wide
    $s3 = "CommandLineToArgvW" ascii wide
    $s4 = "WS2_32.dll" ascii wide
    $s5 = "OpenProcess" ascii wide

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

```
mjolinirtraining@MT23-IR-Kali: ~/Desktop/volatility3
File Actions Edit View Help
1324 TlsGetValue
1325 TlsSetValue
1326 TlsFree
1327 LoadLibraryExW
1328 TerminateProcess
1329 GetModuleHandleExW
1330 GetStdHandle
1331 WriteFile
1332 MultiByteToWideChar
1333 WideCharToMultiByte
1334 GetACP
1335 LCMapStringW
1336 GetStringTypeW
1337 GetFileType
1338 FindClose
1339 FindFirstFileExW
1340 FindNextFileW
1341 IsValidCodePage
1342 GetOEMCP
1343 GetCPInfo
1344 GetCommandLineA
1345 GetEnvironmentStringsW
1346 FreeEnvironmentStringsW
1347 SetStdHandle
1348 FlushFileBuffers
1349 GetConsoleCP
1350 GetConsoleMode
1351 HeapSize
1352 HeapReAlloc
1353 SetFilePointerEx
1354 WriteConsoleW

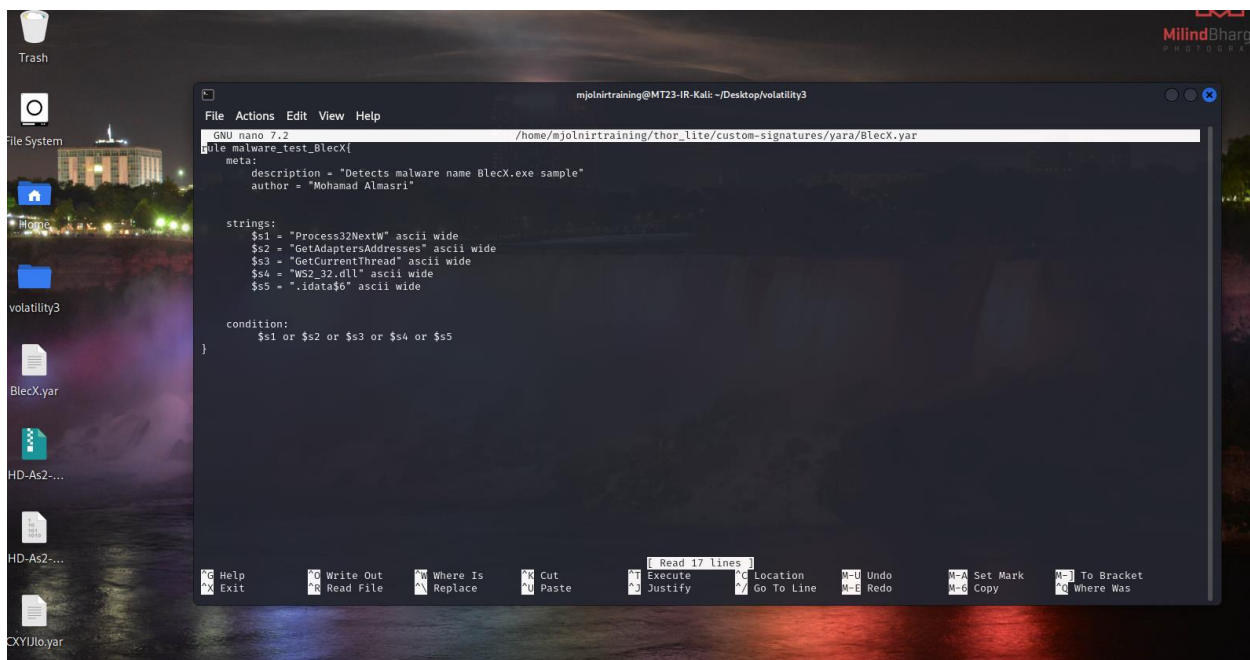
(mjolinirtraining@MT23-IR-Kali)-[~/Desktop/volatility3]
$ sudo nano -c /home/mjolinirtraining/thor_lite/custom-signatures/yara/SrgJYNb.yar
(mjolinirtraining@MT23-IR-Kali)-[~/Desktop/volatility3]
$ cat -n SrgJYNb.exe|moahamad
```



```

mjolnirtraining@MT23-IR-Kali: ~/Desktop/volatility3
File Actions Edit View Help
rm: cannot remove '*.img': No such file or directory
(mjolnirtraining@MT23-IR-Kali)-[~/Desktop/volatility3]
$ rm *.dat
(mjolnirtraining@MT23-IR-Kali)-[~/Desktop/volatility3]
$ strings BlecX.exe > BlecX.exe.mohamad
(mjolnirtraining@MT23-IR-Kali)-[~/Desktop/volatility3]
$ ls -l
total 524
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 206848 Nov 14 23:46 BlecX.exe
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 14153 Nov 14 23:48 BlecX.exe.mohamad
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 5947 Sep 13 2023 README.md
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 205824 Nov 14 23:37 SrgJYNb.exe
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 13069 Nov 14 23:38 SrgJYNb.exe.mohamad
drwxr-xr-x 4 root root 4096 Sep 13 2023 build
drwxr-xr-x 2 mjolnirtraining mjolnirtraining 4096 Oct 8 06:26 config
drwxr-xr-x 3 mjolnirtraining mjolnirtraining 4096 Sep 13 2023 development
drwxr-xr-x 2 root root 4096 Sep 13 2023 dist
drwxr-xr-x 3 mjolnirtraining mjolnirtraining 4096 Sep 13 2023 doc
drwxr-xr-x 2 mjolnirtraining mjolnirtraining 4096 Oct 8 06:26 docs
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 79 Sep 13 2023 mpyy.ini
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 1854 Sep 13 2023 setup.py
drwxr-xr-x 2 mjolnirtraining mjolnirtraining 4096 Sep 13 2023 test
drwxr-xr-x 2 mjolnirtraining mjolnirtraining 4096 Oct 8 06:26 tools
-rwxr-xr-x 1 mjolnirtraining mjolnirtraining 290 Sep 13 2023 vol.py
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 5450 Sep 13 2023 vol.spec
drwxr-xr-x 8 mjolnirtraining mjolnirtraining 4096 Sep 13 2023 volatility3
drwxr-xr-x 2 root root 4096 Sep 13 2023 volatility3.egg-info
-rwxr-xr-x 1 mjolnirtraining mjolnirtraining 297 Sep 13 2023 volshell.py
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 2963 Sep 13 2023 volshell.spec
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 206848 Nov 14 23:15 xGWpgNo.exe
-rw-r--r-- 1 mjolnirtraining mjolnirtraining 14153 Nov 14 23:17 xGWpgNo.exe.mohamad
(mjolnirtraining@MT23-IR-Kali)-[~/Desktop/volatility3]
$

```




```

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-As2-memdump.mem windows.dumpfiles.DumpFiles --pid 83868
Volatility 3 Framework 2.5.1
Progress: 100.00      POB scanning finished
Cache  FileObject      FileName  Result
DataSectionObject  0x9385c5209e70  cversions.2.db  file.0x9385c5209e70.0x9385c52259b0.DataSectionObject.cversions.2.db.dat
DataSectionObject  0x9385c5209e70  cversions.2.db  file.0x9385c5209e70.0x9385c52259b0.DataSectionObject.cversions.2.db.dat
DataSectionObject  0x9385c77366c0  {AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000007.db  Error dumping file

(mjohnirtraining@MT23-IR-Kali)~[~/Desktop/volatility3]
$ python3 vol.py -f /home/mjohnirtraining/Desktop/MHD-As2-memdump.mem windows.dumpfiles.DumpFiles --pid 83868
Volatility 3 Framework 2.5.1
Progress: 100.00      POB scanning finished
Cache  FileObject      FileName  Result
DataSectionObject  0x9385c5209e70  cversions.2.db  file.0x9385c5209e70.0x9385c52259b0.DataSectionObject.cversions.2.db.dat
DataSectionObject  0x9385c5209e70  cversions.2.db  file.0x9385c5209e70.0x9385c52259b0.DataSectionObject.cversions.2.db.dat
DataSectionObject  0x9385c77366c0  {AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000007.db  Error dumping file

(mjohnirtraining@MT23-IR-Kali)~[~/Desktop/volatility3]
$ ls -l /home/mjohnirtraining/thor_lite/custom-signatures/yara/
total 12
-rw-r--r-- 1 mjohnirtraining mjohnirtraining 415 Nov 14 23:52 BlecX.yar
-rw-r--r-- 1 mjohnirtraining mjohnirtraining 422 Nov 14 23:42 SrgJYNb.yar
-rw-r--r-- 1 mjohnirtraining mjohnirtraining 430 Nov 13 15:10 xGwpgNo.yar

(mjohnirtraining@MT23-IR-Kali)~[~/Desktop/volatility3]

```

Transferred the created YARA rules to the **THOR Lite** custom signature folder on the Windows VM.

Downloaded and configured THOR Lite for scanning

```

Administrator: Windows PowerShell
Info Disabling module Mutex due to Lite version
Info Disabling module NetworkShares due to Lite version
Info Disabling module Timestomp due to Lite version
Thor-Lite Disabling module UserDir due to Lite version
Info Disabling module WMISTartup due to Lite version
Info Disabling module AtJobs due to Lite version
Info Disabling module SHIMCache due to Lite version
Info Disabling module HotfixCheck due to Lite version
Info Disabling module Rootkit due to Lite version
Info Disabling module Users due to Lite version
Info Disabling module EnvCheck due to Lite version
Info Disabling module RegistryChecks due to Lite version
Info Disabling module LSASessions due to Lite version
Info Disabling feature ExeDecompress due to Lite version
Info Disabling feature GroupsXML due to Lite version
Info Disabling feature SHIMCache due to Lite version
Info Disabling feature DoublePulsar due to Lite version
Info Disabling feature Eml due to Lite version
Info Disabling feature WMIPersistence due to Lite version
Info Disabling feature EVTX due to Lite version
Info Disabling feature ProgressTracker due to Lite version
md5s.csv Info Disabling feature WebdirScan due to Lite version
2024-11- Info Disabling feature Amcache due to Lite version
Info Disabling feature Bifrost2 due to Lite version
Info Disabling feature Stix due to Lite version
Info Disabling feature WER due to Lite version
Info Disabling feature Auditlog due to Lite version
Info Disabling feature OLE due to Lite version
Info Disabling feature Archive due to Lite version
Info Disabling feature Prefetch due to Lite version
jb8af4-20 Info Disabling feature Sigma due to Lite version
Info Disabling feature SignalHandler due to Lite version
Info Disabling feature ArchiveScan due to Lite version
Info Disabling feature AuthorizedKeys due to Lite version
2024-11- Info Disabling feature TeamViewer due to Lite version
Info Disabling feature MagicHeader due to Lite version
Info Disabling feature RegistryHive due to Lite version
Info Disabling feature Lnk due to Lite version
Info Disabling feature Logger due to Lite version
Info Disabling feature VulnerabilityCheck due to Lite version
Info Disabling feature WorkerProgressTracker due to Lite version
Info Disabling feature AtJobs due to Lite version
Info Disabling feature BulkScan due to Lite version
Info Disabling feature CronParser due to Lite version
Info Disabling feature RecycleBin due to Lite version
Info Disabling feature VirusTotal due to Lite version

> Reading YARA signatures and IOC files ...
Info Adding rule set from thor-lite-all.yas as 'default' type

HIMCache, ScheduledTasks, ServiceCheck, Timestomp, UserDir, Users, WMISTartup
Info Deselected modules: Artifact-Collector, DeepDive, Dropzone, MFT, Thunderstorm
Info Selected features: Amcache, Archive, ArchiveScan, AtJobs, Auditlog, AuthorizedKeys, Bifrost2, BulkScan, C2, CPULimit, CheckString, CronParser, DoublePulsar, ETL, EVTX, Eml, EnrichFileInfo, ExeDecompress, FilenameIOCs, Filescan, GroupsXML, KeywordIOCs, Lnk, LogScan, Logger, MagicHeader, OLE, ParseCobaltStrike, Prefetch, ProcessConnections, ProcessHandles, ProgressTracker, RecycleBin, RegistryHive, Rescontrol, SHIMCache, Sigma, SignalHandler, Stix, TeamViewer, ThorDB, VirusTotal, VulnerabilityCheck, WER, WMIPersistence, WebdirScan, WorkerProgressTracker, Yara
Info Deselected features: AuditTrail, AuditTrailWriter, Bifrost, Dumpscan, ProcessIntegrity
Info System Type: Workstation
Info License file found LICENSE: C:\Users\Mj0inairTraining\Desktop\Thor-Lite\thor-lite-c9688227-870b8af4-20241101-20250504 .lic OWNER: mohamad.almasri@georgebrown.ca TYPE: Lite STARTS: 2024/11/01

```

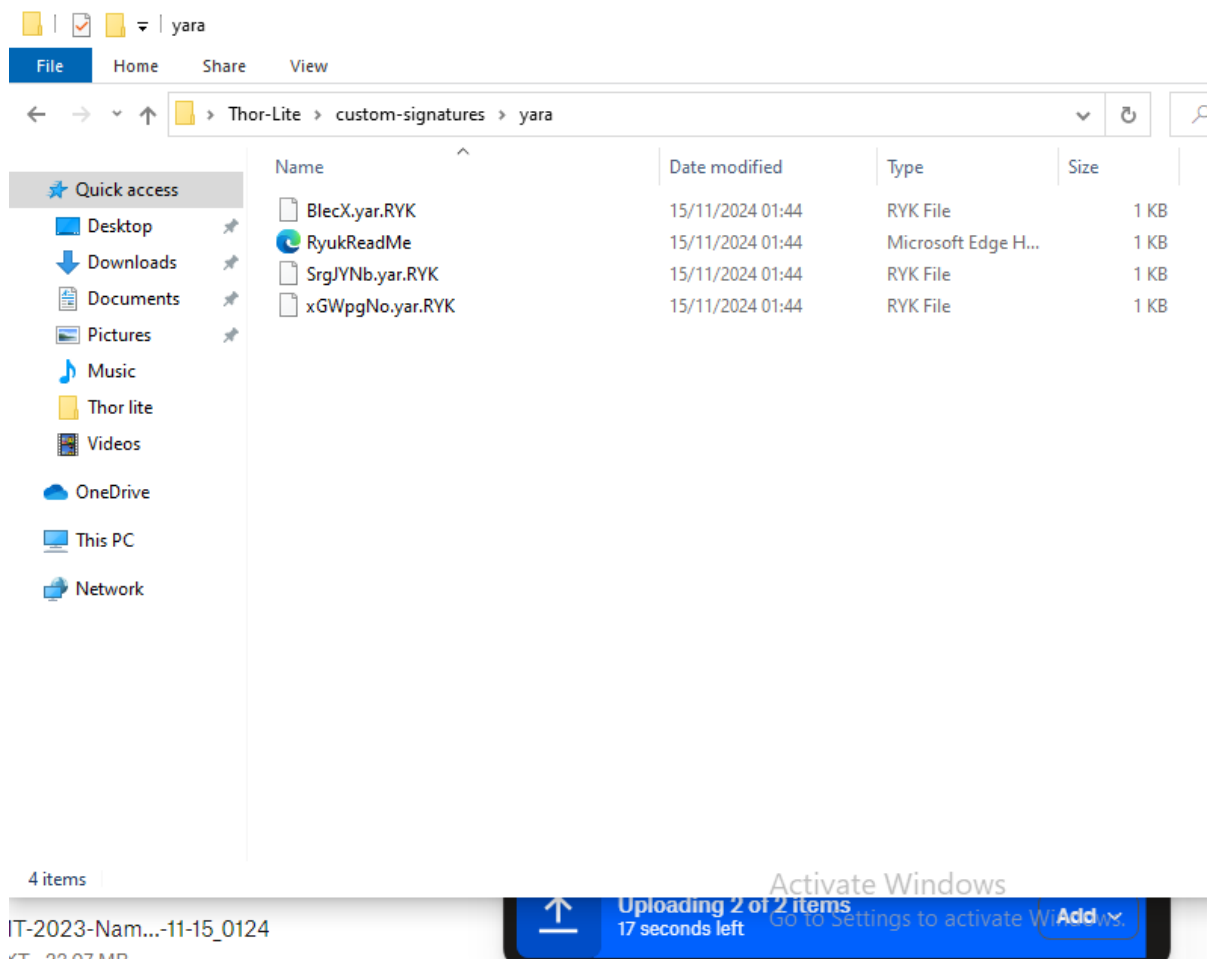


```

Info Successfully compiled 0 malware and 0 false positive hashes TYPE: IOC
Info Successfully compiled 0 file type signatures TYPE: IOC
Info Successfully compiled 0 malware domains TYPE: IOC
Info Successfully compiled 0 named pipe ioc strings and 0 named pipe ioc regexs TYPE: IOC
Info Successfully compiled 0 malicious handles and 0 regex malicious handles TYPE: IOC
Warning No file type signatures compiled, file type detection can't be done. Because of this, many files won't be scanned.
Info No custom directory excludes defined
Info No custom registry excludes defined
Info No custom eventlog excludes defined
Info No custom process excludes defined
Info Successfully compiled 5714 default YARA rules TYPE: YARA
Info Successfully compiled 0 custom default YARA rules TYPE: YARA
Info Successfully compiled 0 meta YARA rules TYPE: YARA
Info Successfully compiled 0 process YARA rules TYPE: YARA
Info Successfully compiled 0 log YARA rules TYPE: YARA
Info Successfully compiled 0 registry YARA rules TYPE:

```

Ran the scanner, but the rules were encrypted during scanning, which resulted in detection failure.



What Evidence I Started With

- 1. Ransomware samples:** October 2019 folder containing multiple ransomware samples. This is performed on a Windows virtual machine (VM).
- 2. Memory dump:** A VM's memory dump, which is performed after executing all ransomware samples. It records the state of the system during malware activity
- 3. Process Monitoring:** Process Hacker Observation is a tool used to monitor the processes running during malware execution. It identifies suspicious processes.
- 4. Screenshots: Screenshots taken during the process, including:**
 - VM state paused
 - Active processes and their relationships.
 - Memory analysis output

What Analysis Was Done

- 1. Memory Dump Analysis:**
 - Transfer the memory dump file from the Windows VM to the Kali Linux machine for analysis
 - Used Volatility 3 to extract forensic data, focusing on processes and their behaviors.
 - Run windows.info, windows.pslist, windows.procdump and other commands to collect details about active processes. Identify malicious processes and delete the executable file
- 2. Process Relationship Examination:**
 - Analyze parent-child relationships between processes using tools such as windows.pstree and windows.cmdline. To follow up on other processes How is it dynamically generated by some malware.
- 3. Executable Extraction:**
 - Extracted malicious executables from memory using the cp command.

- For one malware sample, the executable couldn't be directly extracted as it was dynamically generated by a parent process, a behavior noted in the process tree.

4. String Analysis:

- Conducted string analysis on dumped executables using the strings command.
- Identified unique markers or patterns to create custom YARA rules for each piece of malware.

5. YARA Rule Development:

- Create YARA rules based on findings from string analysis.
- Each rule targets a specific pattern or behavior of the identified malware.

6. THOR Lite Testing:

- Loaded the custom YARA rules into the **THOR Lite** scanner and configured it for testing.
- Ran the scanner on the Windows VM to detect malware using the created rules.
- Observed that some YARA rules failed due to encryption issues during runtime.

Did your yara rules work? If no, why?

One possible reason is that the rules were encoded or changed when I copied them. After running all the ransomware files from the "October 2019 folder on the VM, it is possible that one of the ransomware programs encrypted or modified the YARA rules file.

Details on the Encryption Issue

- File extension changes: YARA rules normally have the extension .yar, but after copying Rules now have the extension .RYK. This suggests that the ransomware encrypted or scrambled the file, converting it from a readable YARA rule into an encrypted format that THOR Lite cannot detect.

- **Impact on THOR Lite:** THOR Lite expects YARA rules to be in a specific format (.yar or .yara). When files are encrypted or modified by ransomware, THOR Lite is unable to detect those threats. causing the scan to fail.

Why did this happen?

Perhaps the ransomware was programmed to encrypt files on the system, including my custom YARA rules. Because I ran the ransomware without restoring the VM, it affected all accessible files. Including my rules.

Conclusion

This work gave me valuable hands-on experience in memory forensics and malware analysis. I learned how to take memory from a virtual machine and analyze it using Volatility 3, an important tool in digital forensics. Using commands such as windows.info, windows.pslist, windows.pstree, and windows.cmdline I can identify suspicious processes, find PIDs, and examine relationships. Understanding the parent and child structure of malware processes helps me understand how some malicious processes replicate other processes. Create relevant threat groups... I also performed string analysis on the discarded files to identify specific patterns and behavior for each malware sample. This analysis is critical in shaping YARA regulations to identify similar hazards in the future. Although I faced challenges such as encoding my YARA rules to prevent ransomware from running on THOR Lite, I gained valuable insight into the risks of running malware in this environment. Undamaged environment.