

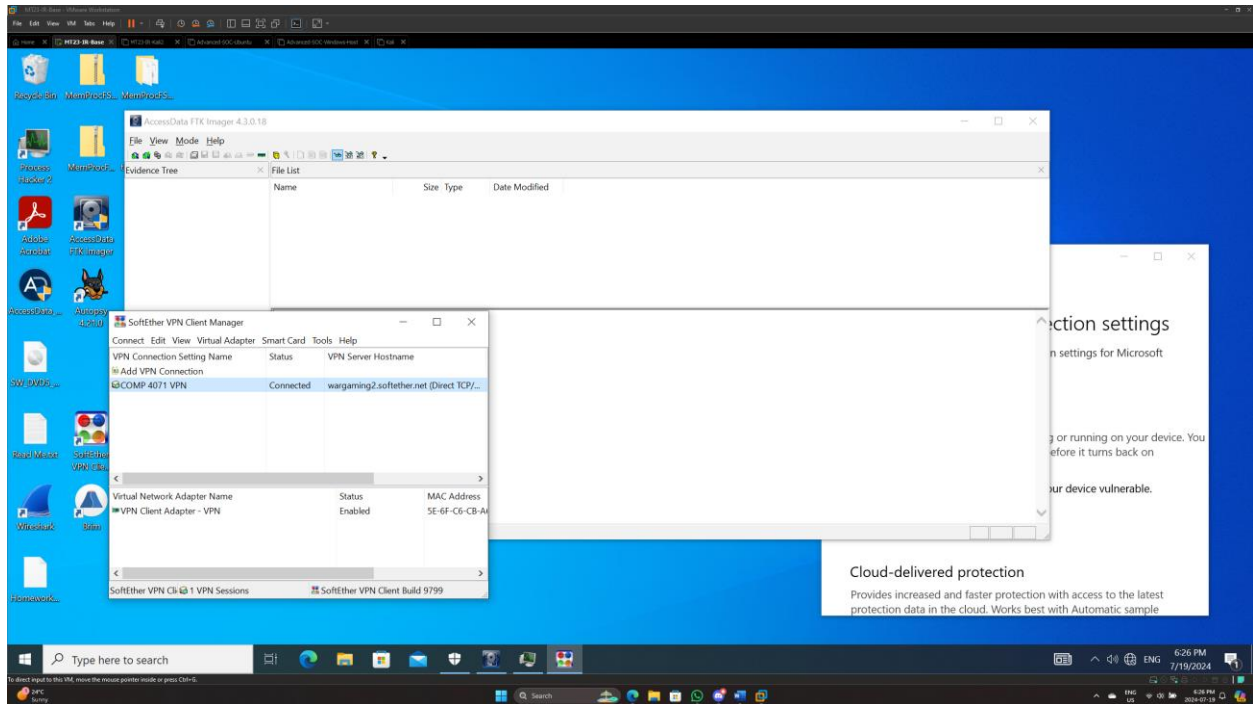
EXTRACT MALWARE STRINGS FROM A MEMORY DUMP AND CREATE YARA RULES

Jordan Patterson
2024

Goals of this Lab:

- Generate a memdump file after successfully executing all ransomware in the Oct 2019 folder on your vm
 - do not revert the vm, just pause it
 - Copy memdump to Kali VM
 - Run volatility
 - Dump malicious processes (screenshot for each)
 - String analysis to create yara rule for each process
 - Put the rule in thor lite custom signature folder
 - download the scanner for thor lite to windows, unpause the vm and run the thor lite scanner for custom signature
 - collect report
 - The word report for this activity must contain:
 - What evidence you started with
 - What analysis was done
 - What were the findings
 - Did your yara rules work? If no, why?
 - Final analysis in 2000 words. This must include a flow of thoughts, have an opening, a body, screenshots with explanations and conclusion.
 - **Submission items:**
 - Word report
 - Thorlite Output HTML report
-

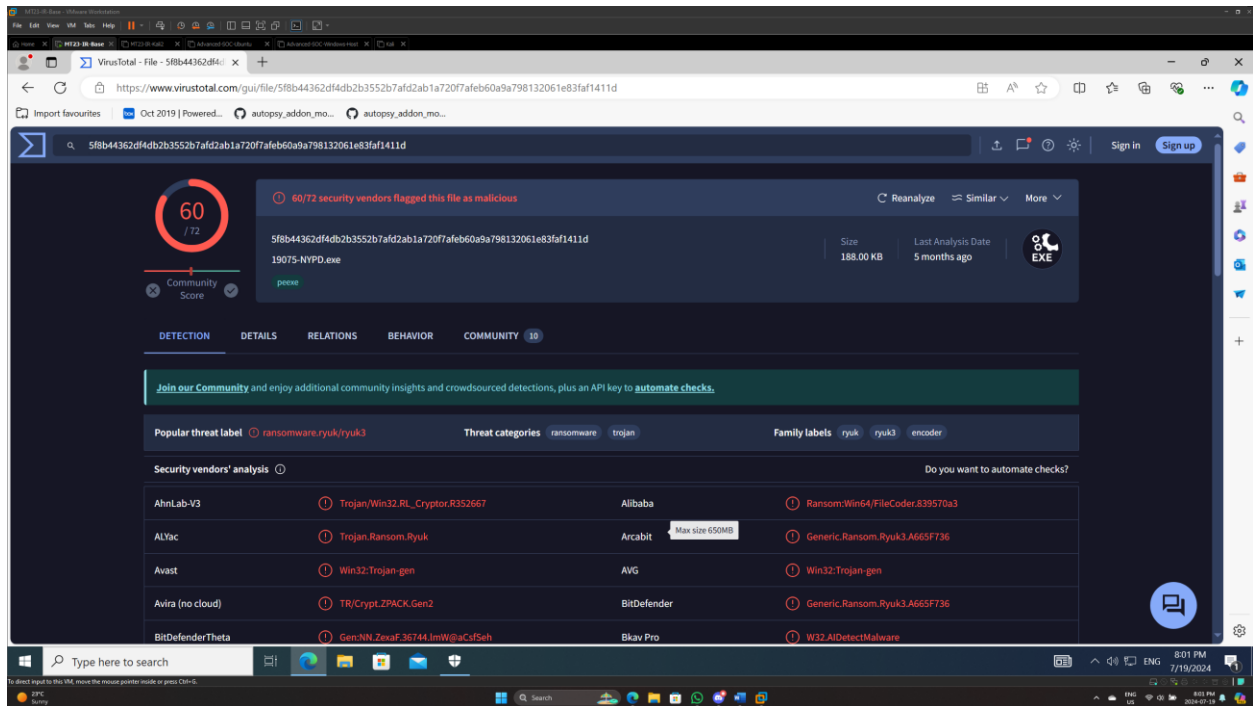
I began this lab with my Windows VM. I took a snapshot before beginning. I downloaded the required malware, connected to the VPN, ensured that real-time protection was off, and ensured that FTK Imager was open and ready to capture the memory of the system after the ransomware had been run.



I then gathered all of the malware in the Oct 2019 folder and compared them with VirusTotal to determine which of them were ransomware. I identified 4 of the executables as ransomware.

The identified Ransomware were:

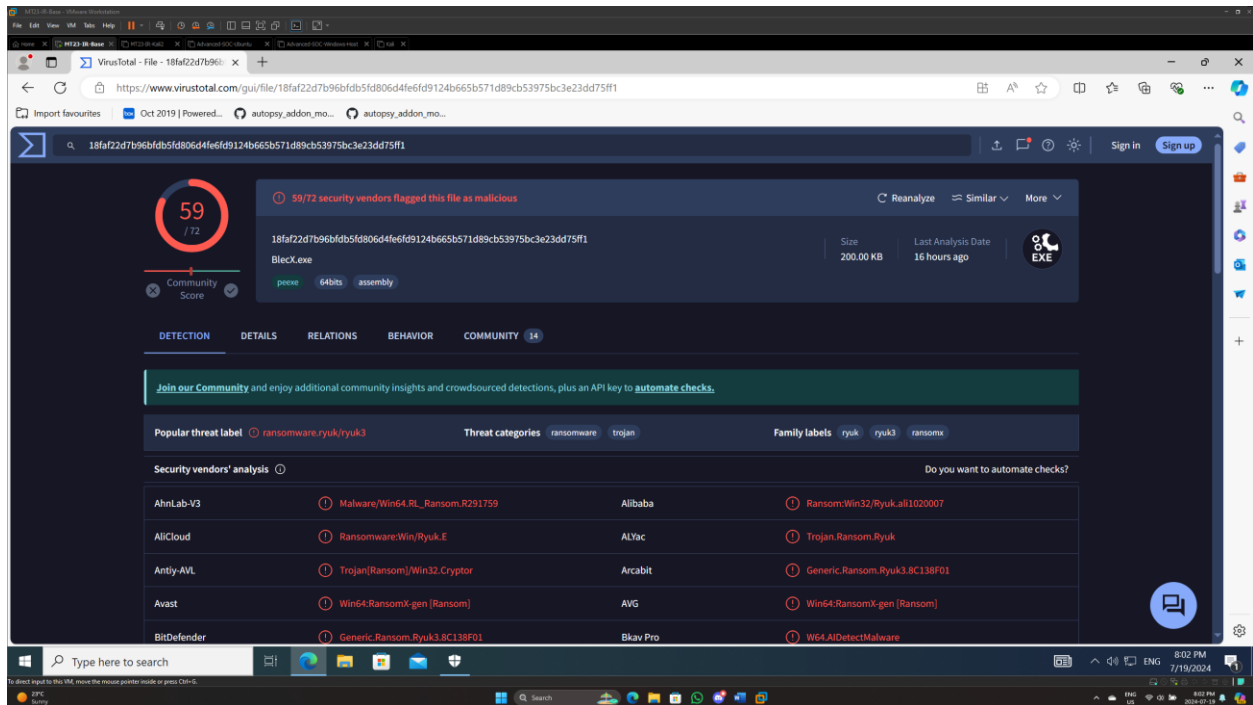
19075-NYPD.exe



The screenshot shows the VirusTotal web interface for the file 19075-NYPD.exe. The file's SHA-256 hash is 5f8b44362df4db2b3552b7afd2ab1a7207afeb60a9a798132061e83faf1411d. The file is 188.00 KB in size and was last analyzed 5 months ago. It has a community score of 60/72, with 60 security vendors flagging it as malicious. The file is identified as a ransomware, specifically a variant of Ryuk. The security vendors' analysis table shows the following results:

Vendor	Detection	Category	Family
AhnLab-V3	Trojan.Win32.RL_Cryptor.R352667	Ransomware	Ransom:Win64/FileCoder.839570a3
ALYac	Trojan.Ransom.Ryuk	Ransomware	Generic.Ransom.Ryuk3.A665F736
Avast	Win32:Trojan-gen	Trojan	Win32:Trojan-gen
Avira (no cloud)	TR/Crypt.ZPACK.Gen2	Trojan	Generic.Ransom.Ryuk3.A665F736
BitDefender Theta	Gem.NM.Zexaf.36744.lmW@aCfSeh	Trojan	W32.AIDetect!Malware

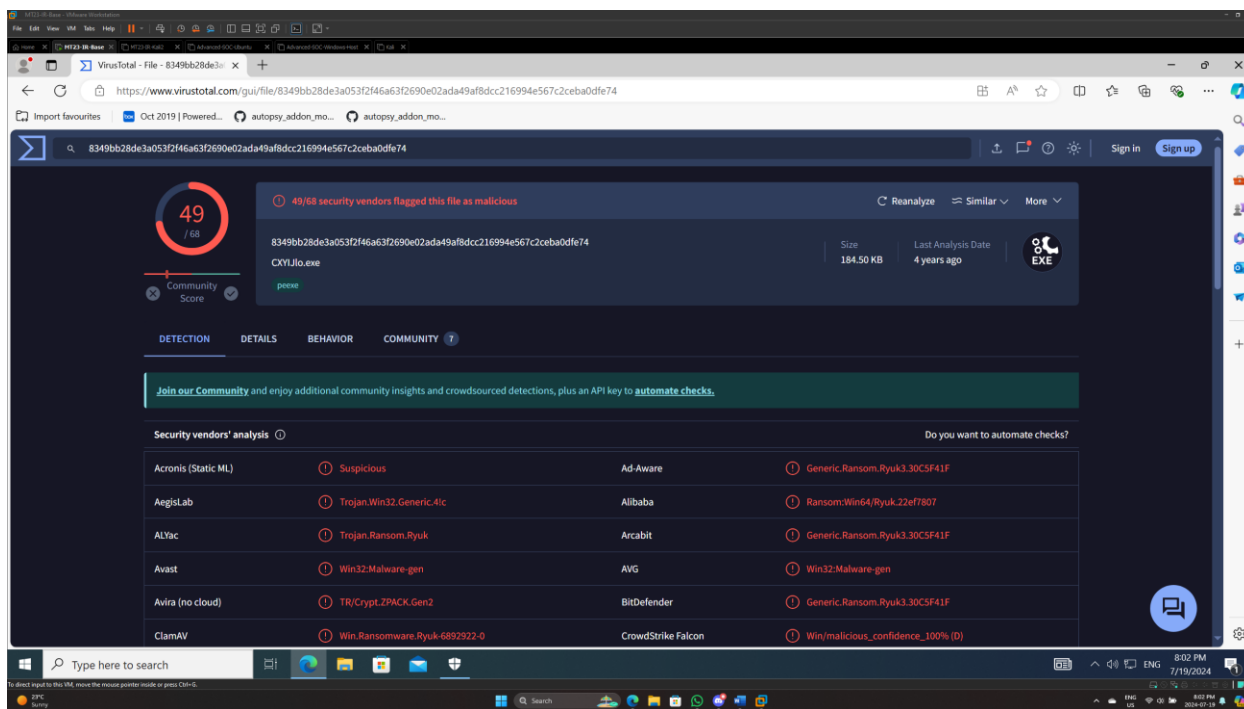
BlecX.exe



The screenshot shows the VirusTotal web interface for the file BlecX.exe. The file's SHA-256 hash is 18fa22d7b96bdfb5d806d4fe6d9124b665b571d89cb53975bc3e23dd75f1. The file is 200.00 KB in size and was last analyzed 16 hours ago. It has a community score of 59/72, with 59 security vendors flagging it as malicious. The file is identified as a ransomware, specifically a variant of Ryuk. The security vendors' analysis table shows the following results:

Vendor	Detection	Category	Family
AhnLab-V3	Malware.Win64.RL_Ransom.R291759	Ransomware	Ransom:Win32/Ryuk.ali1020007
AliCloud	Ransomware.Win/Ryuk.E	Ransomware	Trojan.Ransom.Ryuk
Antiy-AVL	Trojan(Ransom)/Win32.Cryptor	Trojan	Generic.Ransom.Ryuk3.8C138F01
Avast	Win64.RansomX-gen [Ransom]	Ransomware	Win64.RansomX-gen [Ransom]
BitDefender	Generic.Ransom.Ryuk3.8C138F01	Ransomware	W64.AIDetect!Malware

CXYIJlo.exe

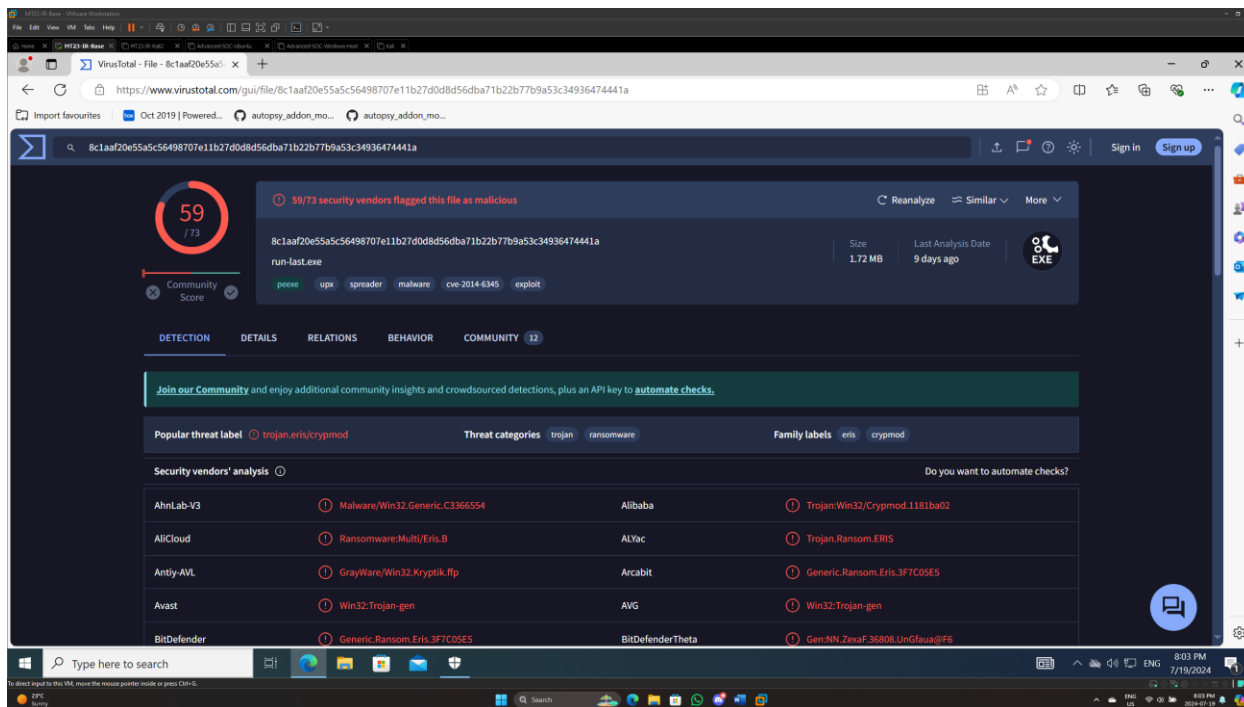


The screenshot shows the VirusTotal web interface for the file CXYIJlo.exe. The file's SHA-256 hash is 8349bb28de3a053f2f46a63f2690e02ada49af8dcc216994e567c2ceba0dfe74. The community score is 49/68, and it is flagged as malicious by 49/68 security vendors. The file size is 184.50 KB, and it was last analyzed 4 years ago. The file type is EXE.

Security vendors' analysis

Vendor	Detection	Vendor	Detection
Acronis (Static ML)	Suspicious	Ad-Aware	Generic.Ransom.Ryuk3.30CSF41F
AegisLab	Trojan.Win32.Generic.4tc	Alibaba	Ransom:Win64/Ryuk.22ef7807
ALYac	Trojan.Ransom.Ryuk	Arcabit	Generic.Ransom.Ryuk3.30CSF41F
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira (no cloud)	TR/Crypt.ZPACK.Gen2	BitDefender	Generic.Ransom.Ryuk3.30CSF41F
ClamAV	Win.Ransomware.Ryuk-6892922-0	CrowdStrike Falcon	Win/malicious_confidence_100% (D)

Run-last.exe

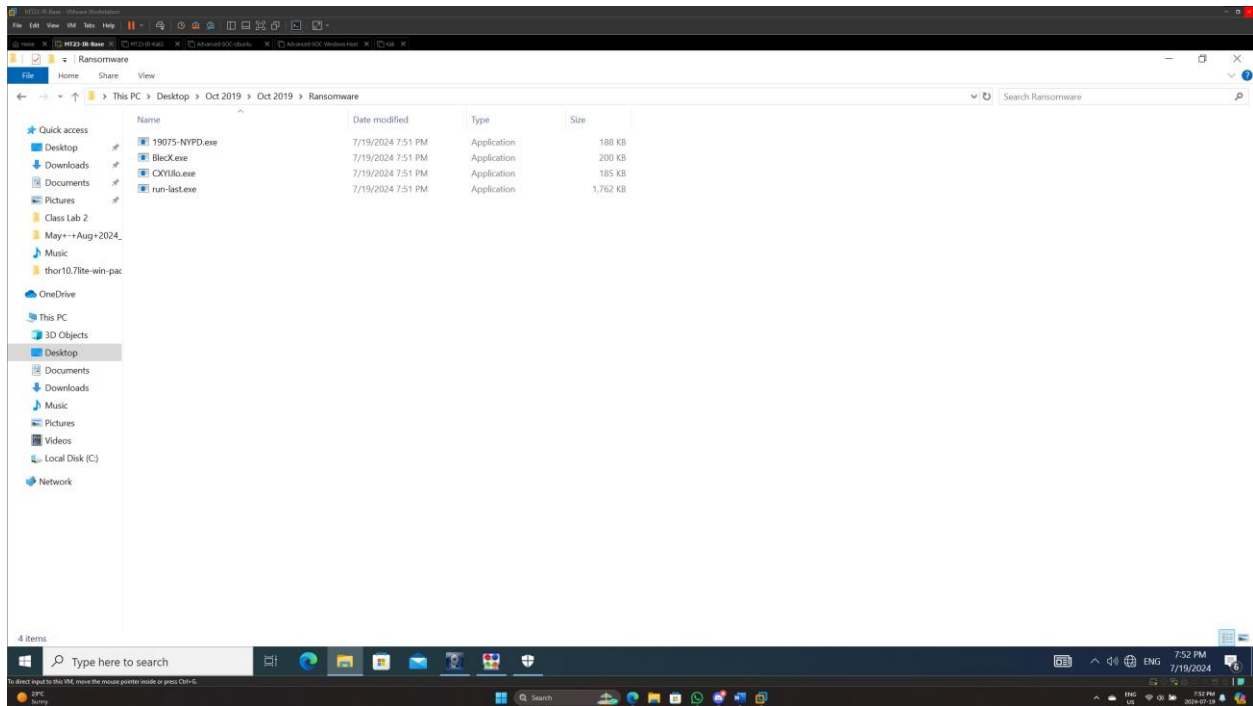


The screenshot shows the VirusTotal web interface for the file Run-last.exe. The file's SHA-256 hash is 8c1aaf20e55a5c56498707e11b27d0d8d56dba71b22b77b9a53c34936474441a. The community score is 59/73, and it is flagged as malicious by 59/73 security vendors. The file size is 1.72 MB, and it was last analyzed 9 days ago. The file type is EXE.

Security vendors' analysis

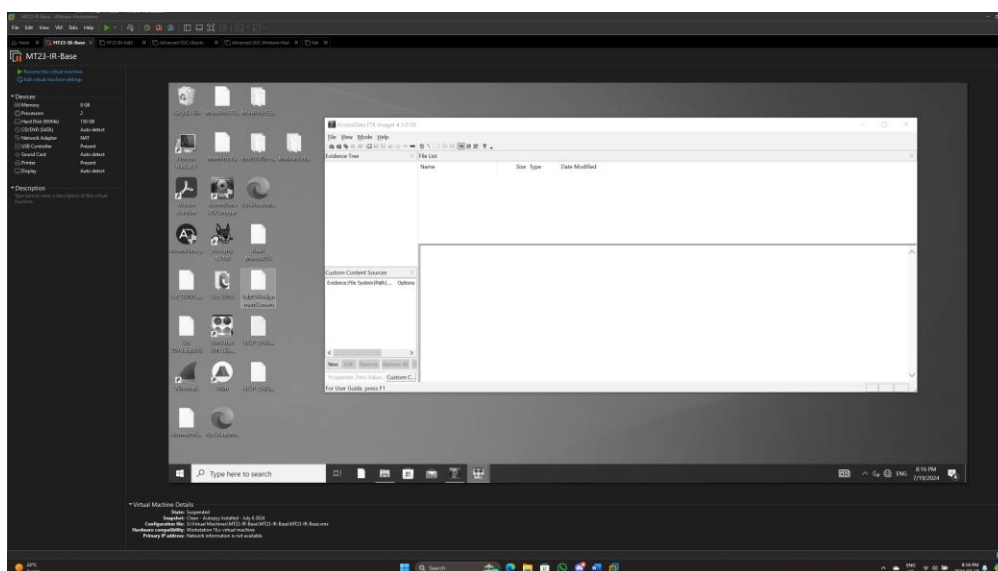
Vendor	Detection	Vendor	Detection
AhnLab-V3	Malware/Win32.Generic.C3366554	Alibaba	Trojan:Win32/Crypm0d.1181ba02
AliCloud	Ransomware:Multi/Eris.B	ALYac	Trojan.Ransom.ERIS
Antiy-AVL	GrayWare/Win32.Kryptik.flp	Arcabit	Generic.Ransom.Eris.3F7C09E5
Avast	Win32:Trojan-gen	AVG	Win32:Trojan-gen
BitDefender	Generic.Ransom.Eris.3F7C09E5	BitDefender Theta	Gen:NN.Zenaf.36808.LinGava@FG

I then ran all identified ransomware from the Oct 2019 folder as administrator and allowed them time to run properly.

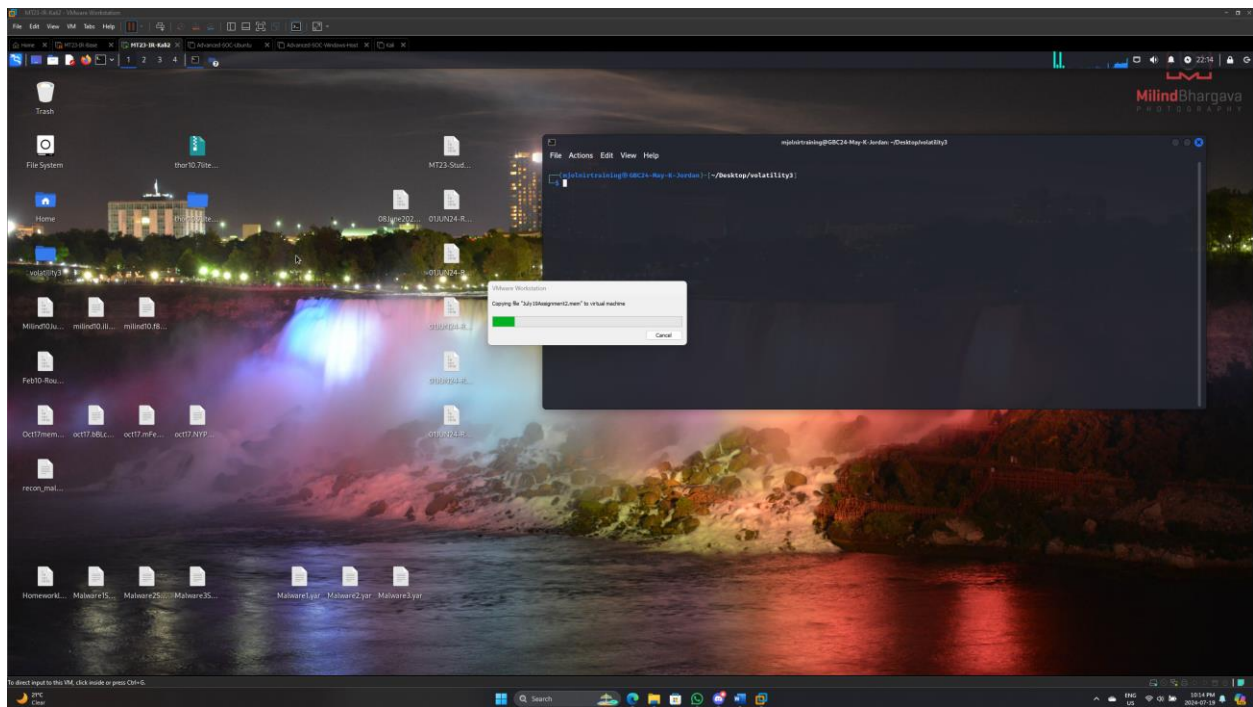


After all Ransomware had been run, I captured the systems memory using FTK Imager and successfully copied it out of the VM before it became encrypted.

I then paused the Windows VM in its current state.

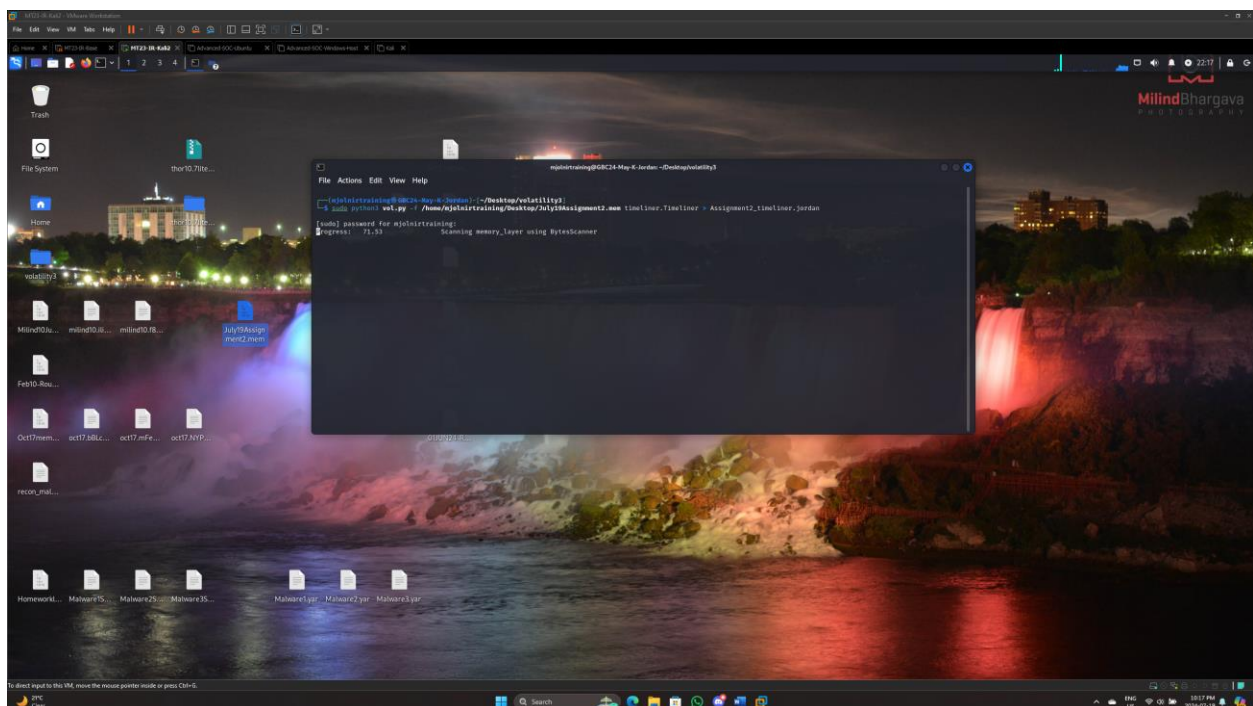


I turned on the Kali VM, transferred the memory dump, and opened Volatility.

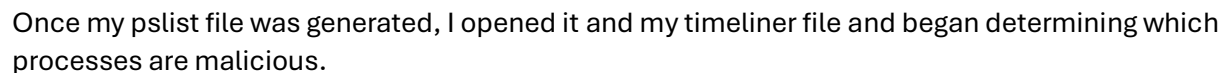


I used the following command to run Timeliner and output the results to a separate file.

```
sudo python3 vol.py -f /home/mjohnirtraining/Desktop/July19Assignment2.mem  
timeliner.Timeliner > Assignment2_timeliner.jordan
```




```
sudo python3 vol.py -f /home/mjolinrtraining/Desktop/July19assignment2.mem  
windows.pslist.PsList > Assignment2_pslist.jordan
```

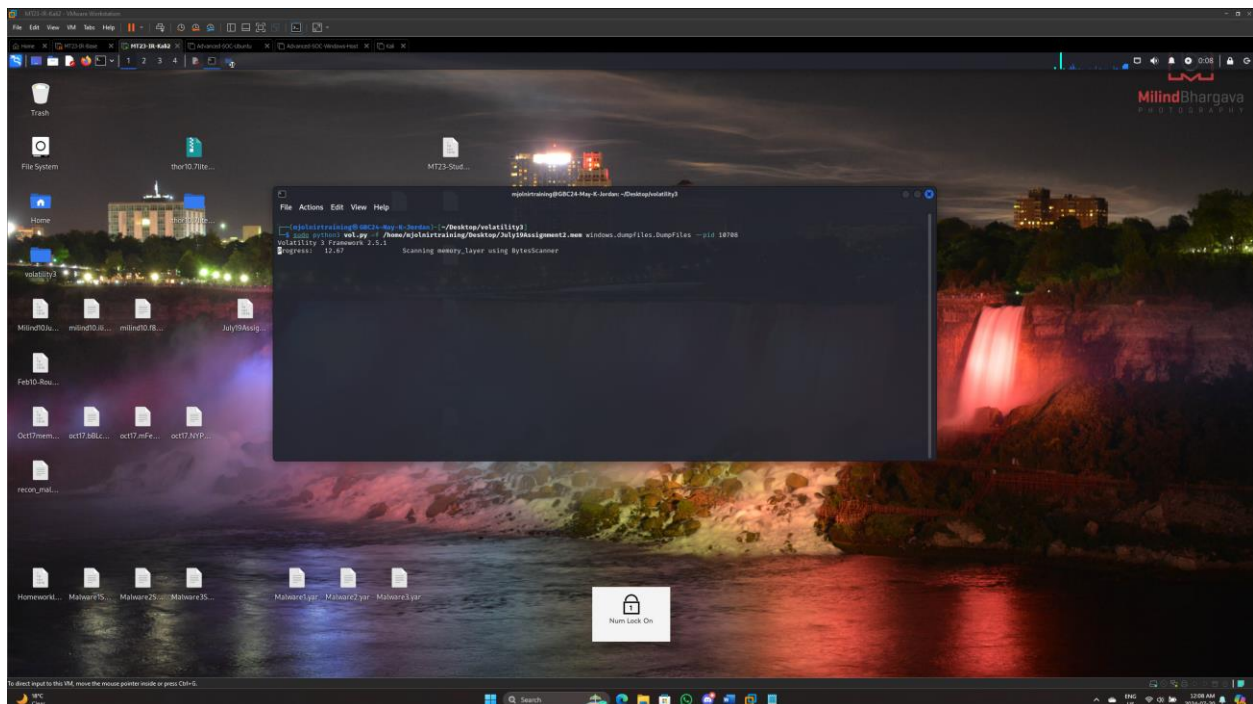
[illegible]

I identified the following process ID's:

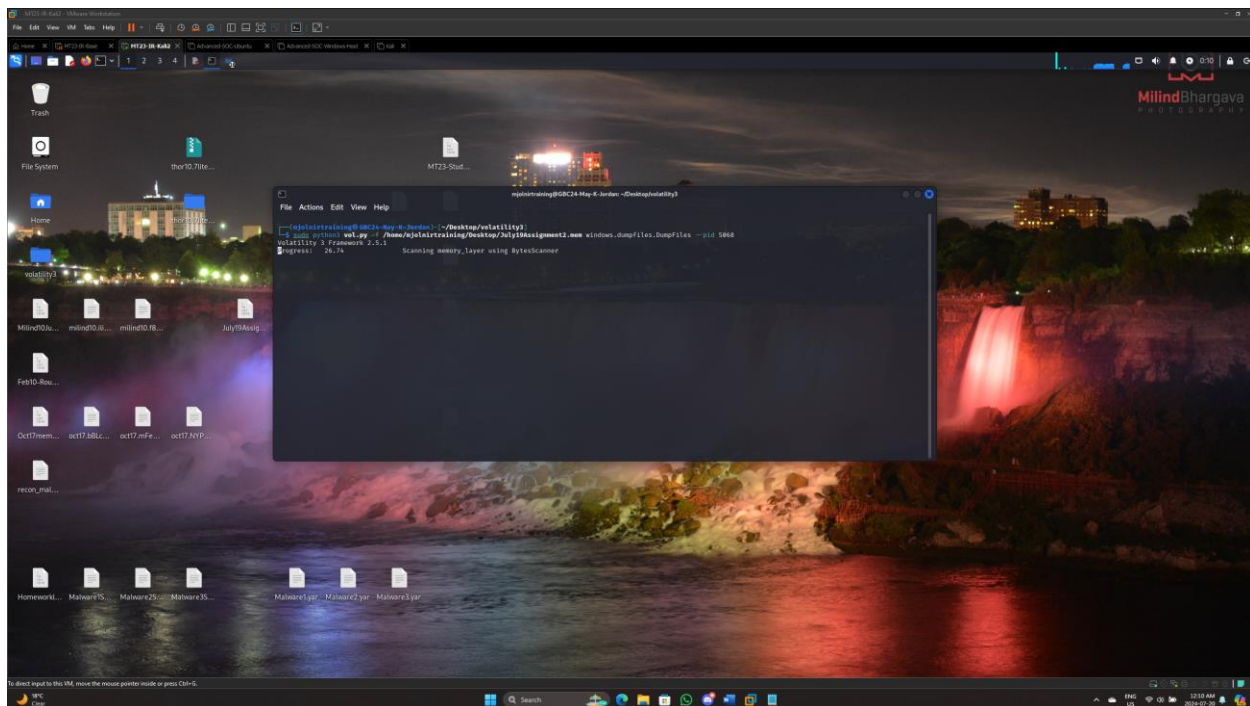
- **PID: 10708**
 - **Process: 19075-NYPD.exe**
- **PID: 5068**
 - **Process: BlecX.exe**
- **PID: 536208**
 - **Process: CXYIJlo.exe**
- **PID: 600084**
 - **Process: run-last.exe**

I used the following command to dump the executable for the 19075-NYPD.exe ransomware. I then repeated these steps, changing the PID, to dump the executables for the other ransomware as well.

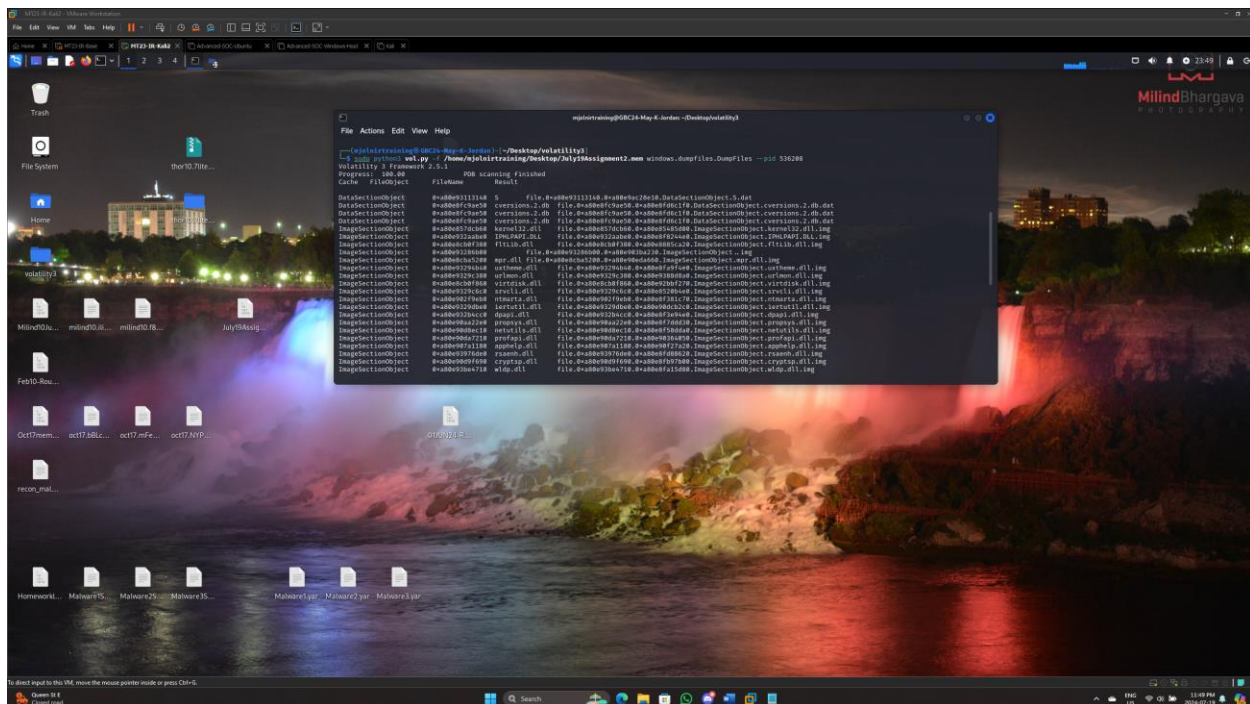
```
sudo python3 vol.py -f /home/mjolnirtraining/Desktop/July19Assignment2.mem  
windows.dumpfiles.DumpFiles --pid 10708
```



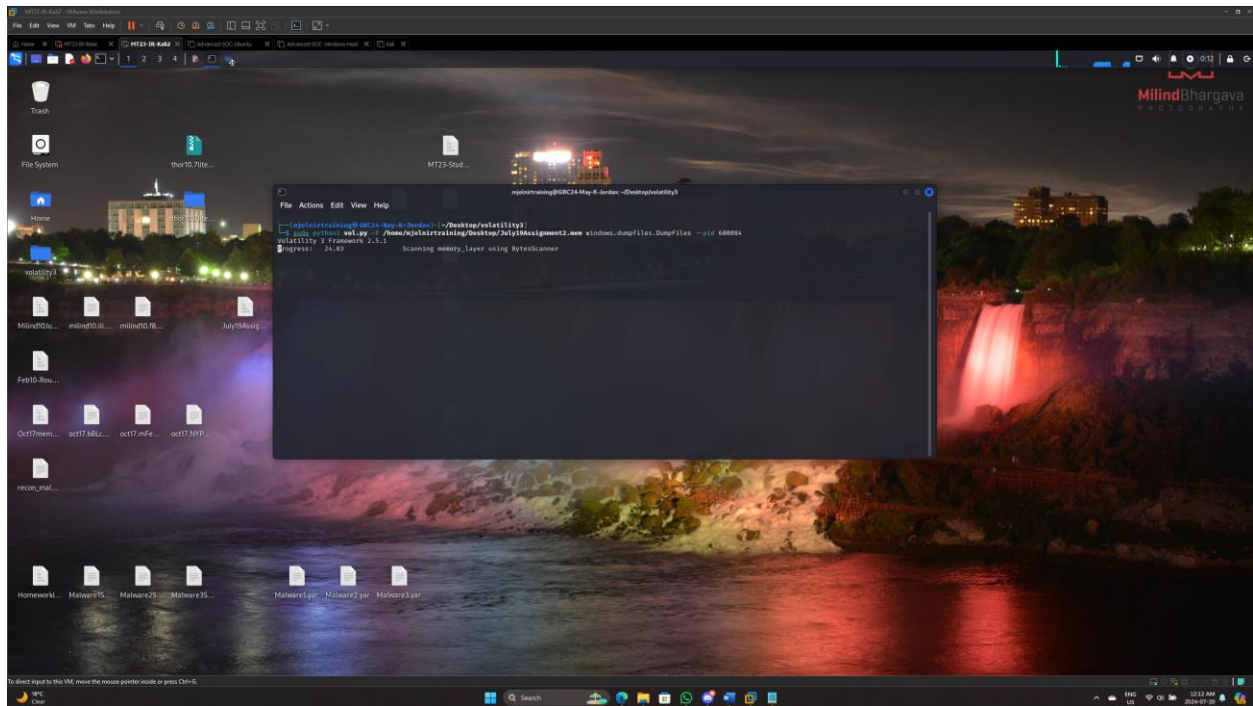
**sudo python3 vol.py -f /home/mjolinrtraining/Desktop/July19Assignment2.mem
windows.dumptfiles.DumpFiles --pid 5068**



**sudo python3 vol.py -f /home/mjolinrtraining/Desktop/July19Assignment2.mem
windows.dumptfiles.DumpFiles --pid 536208**



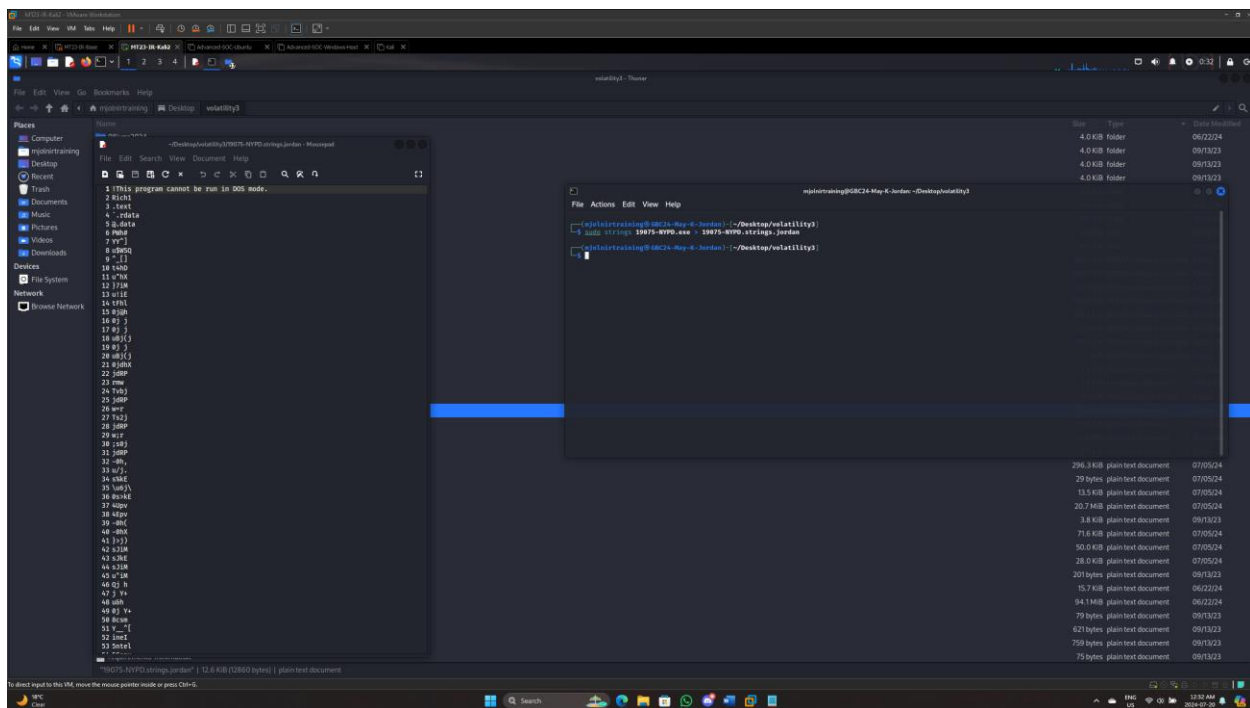
```
sudo python3 vol.py -f /home/mjolinrtraining/Desktop/July19Assignment2.mem  
windows.dumpfiles.DumpFiles --pid 600084
```



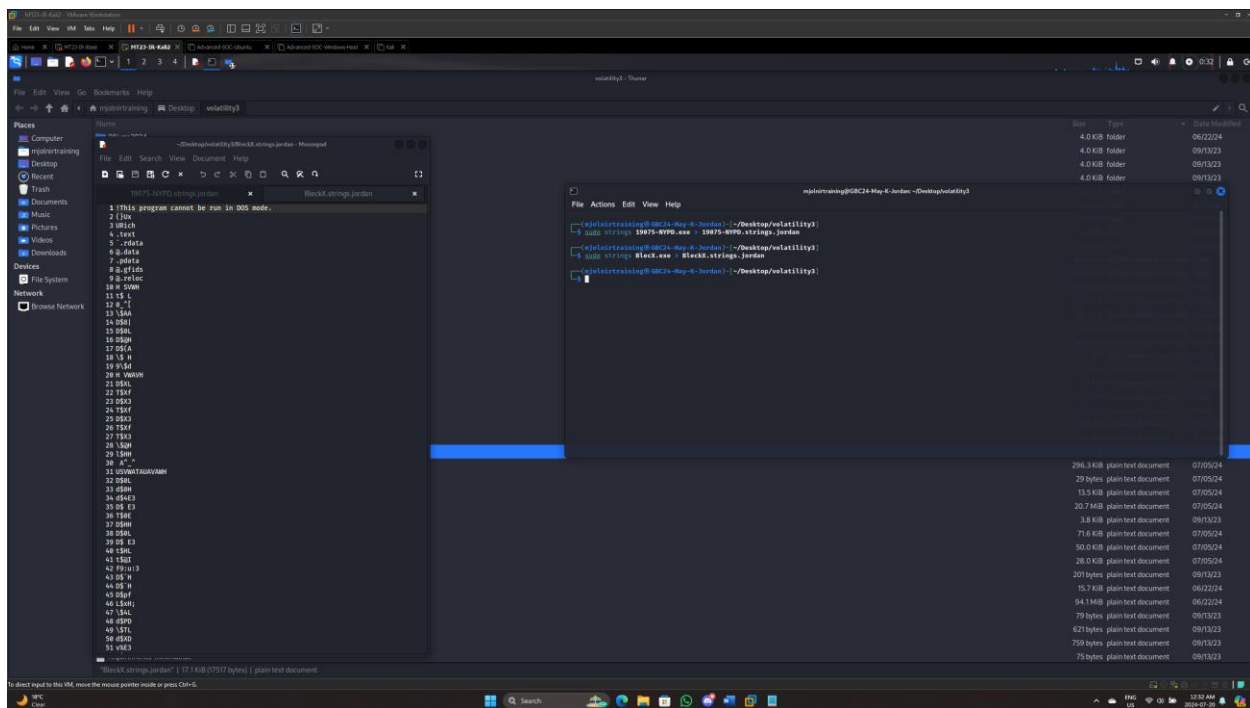
Once this was complete, I duplicated the ransomware files and renamed them so that I had the executables. I then removed .img and .dat files.

I then ran the strings command for each executable in my possession using the following commands:

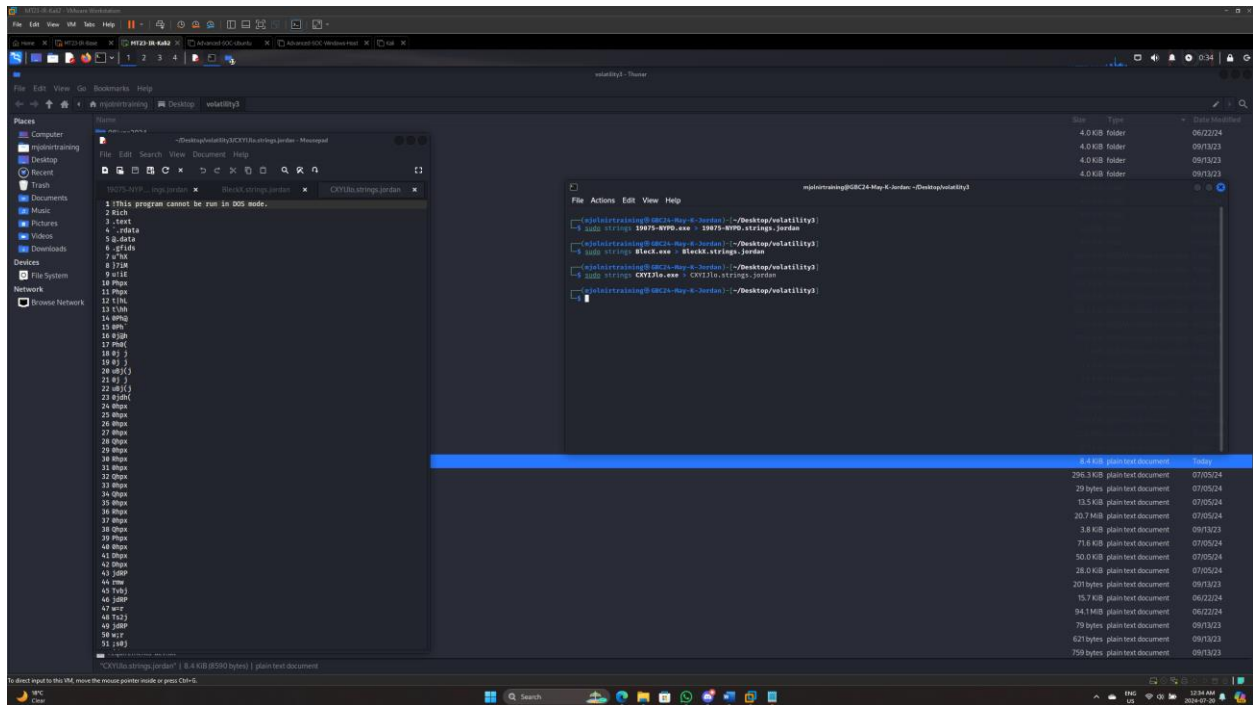
sudo strings 19075-NYPD.exe > 19075-NYPD.strings.jordan



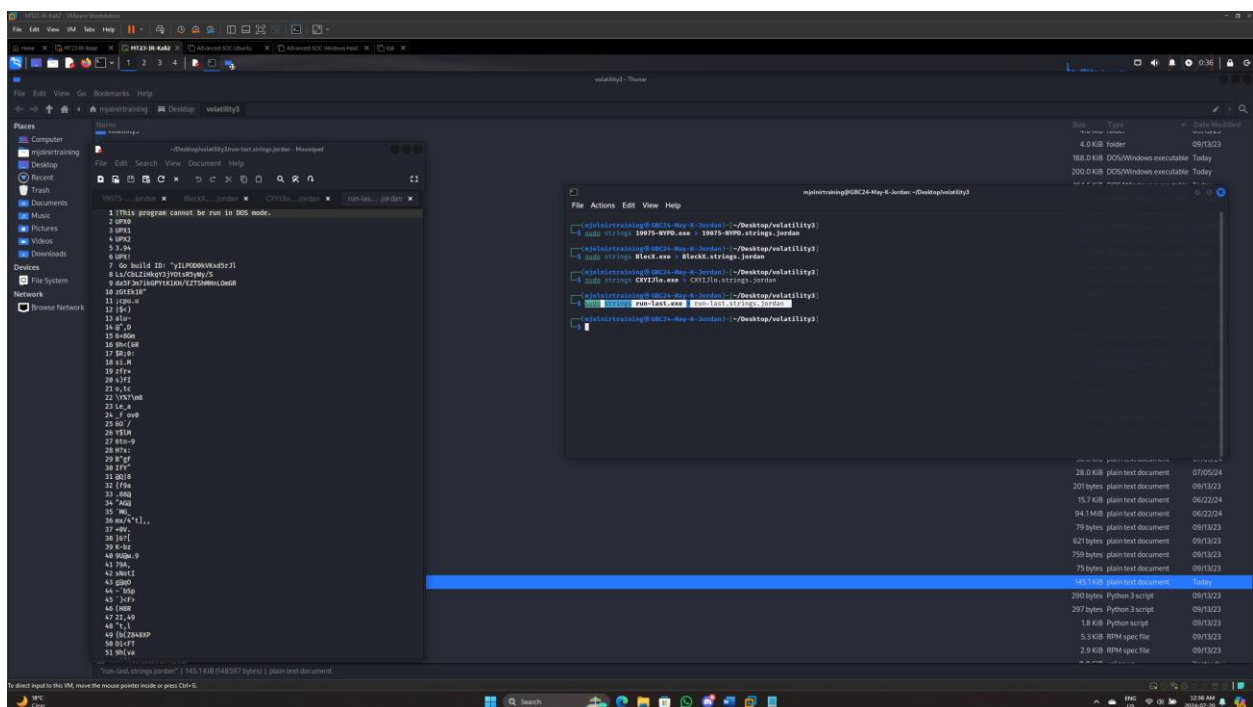
sudo strings BleckX.exe > BleckX.strings.jordan



sudo strings CXYIJlo.exe > CXYIJlo.strings.jordan

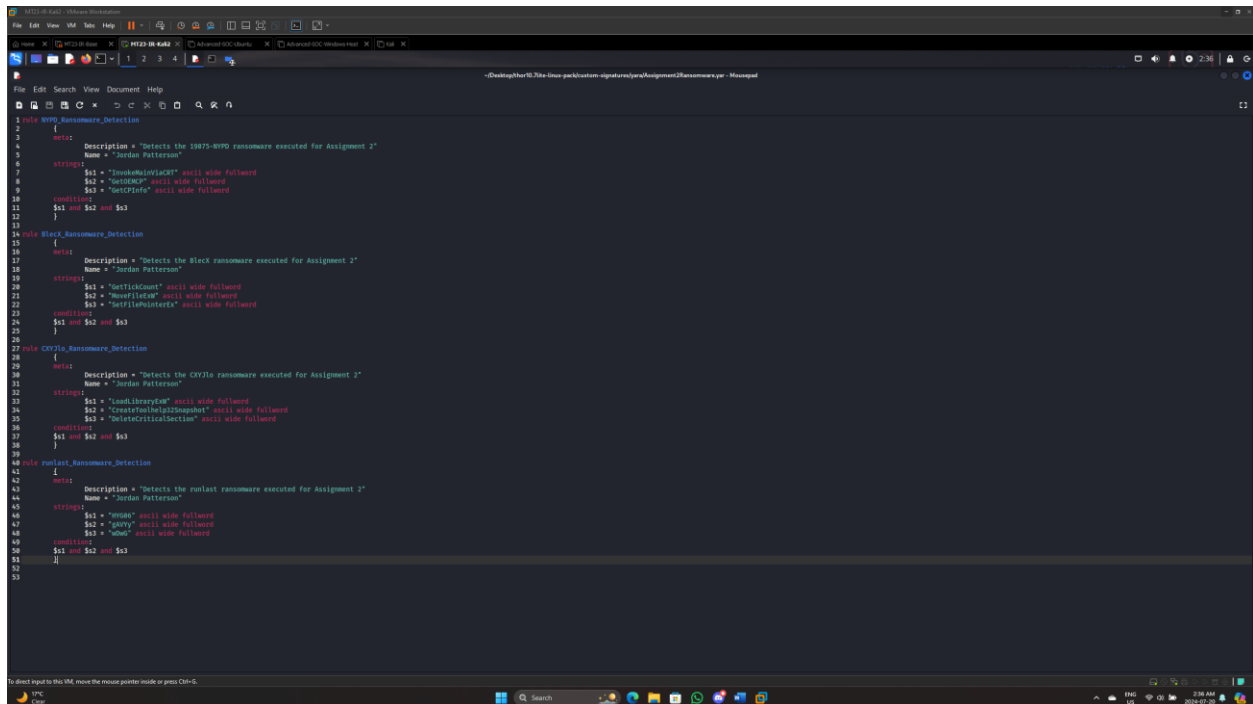


sudo strings run-last.exe > run-last.strings.jordan



Now that we have the strings for all the ransomware, we can begin creating YARA rules.

I created the following YARA rules for each ransomware:



```
1 rule NYPD_Ransomware_Detection
2 {
3     meta:
4         Description = "Detects the 19075-NYPD ransomware executed for Assignment 1"
5         Name = "Jordan Patterson"
6     strings:
7         $s1 = "InvokeMainViaCRT" ascii wide fullword
8         $s2 = "GetOEMCP" ascii wide fullword
9         $s3 = "GetCPInfo" ascii wide fullword
10    condition:
11        $s1 and $s2 and $s3
12 }
13
14 rule Black_Ransomware_Detection
15 {
16     meta:
17         Description = "Detects the Black ransomware executed for Assignment 1"
18         Name = "Jordan Patterson"
19     strings:
20         $s1 = "GetTickCount" ascii wide fullword
21         $s2 = "MoveFileEx" ascii wide fullword
22         $s3 = "SetFilePointer" ascii wide fullword
23    condition:
24        $s1 and $s2 and $s3
25 }
26
27 rule CRYLO_Ransomware_Detection
28 {
29     meta:
30         Description = "Detects the CRYLO ransomware executed for Assignment 1"
31         Name = "Jordan Patterson"
32     strings:
33         $s1 = "LoadLibrary" ascii wide fullword
34         $s2 = "CreateFileW" ascii wide fullword
35         $s3 = "DeleteCriticalSection" ascii wide fullword
36    condition:
37        $s1 and $s2 and $s3
38 }
39
40 rule ru1ast_Ransomware_Detection
41 {
42     meta:
43         Description = "Detects the ru1ast ransomware executed for Assignment 1"
44         Name = "Jordan Patterson"
45     strings:
46         $s1 = "rmcmd" ascii wide fullword
47         $s2 = "rmcmd" ascii wide fullword
48         $s3 = "rmcmd" ascii wide fullword
49    condition:
50        $s1 and $s2 and $s3
51 }
52
53 }
```

rule NYPD_Ransomware_Detection

{

meta:

Description = "Detects the 19075-NYPD ransomware executed for Assignment 2"

Name = "Jordan Patterson"

strings:

\$s1 = "InvokeMainViaCRT" ascii wide fullword

\$s2 = "GetOEMCP" ascii wide fullword

\$s3 = "GetCPInfo" ascii wide fullword

condition:

\$s1 and \$s2 and \$s3

}

rule BlecX_Ransomware_Detection

```
{  
  meta:  
    Description = "Detects the BlecX ransomware executed for Assignment 2"  
    Name = "Jordan Patterson"  
  
  strings:  
    $s1 = "GetTickCount" ascii wide fullword  
    $s2 = "MoveFileExW" ascii wide fullword  
    $s3 = "SetFilePointerEx" ascii wide fullword  
  
  condition:  
    $s1 and $s2 and $s3  
}
```

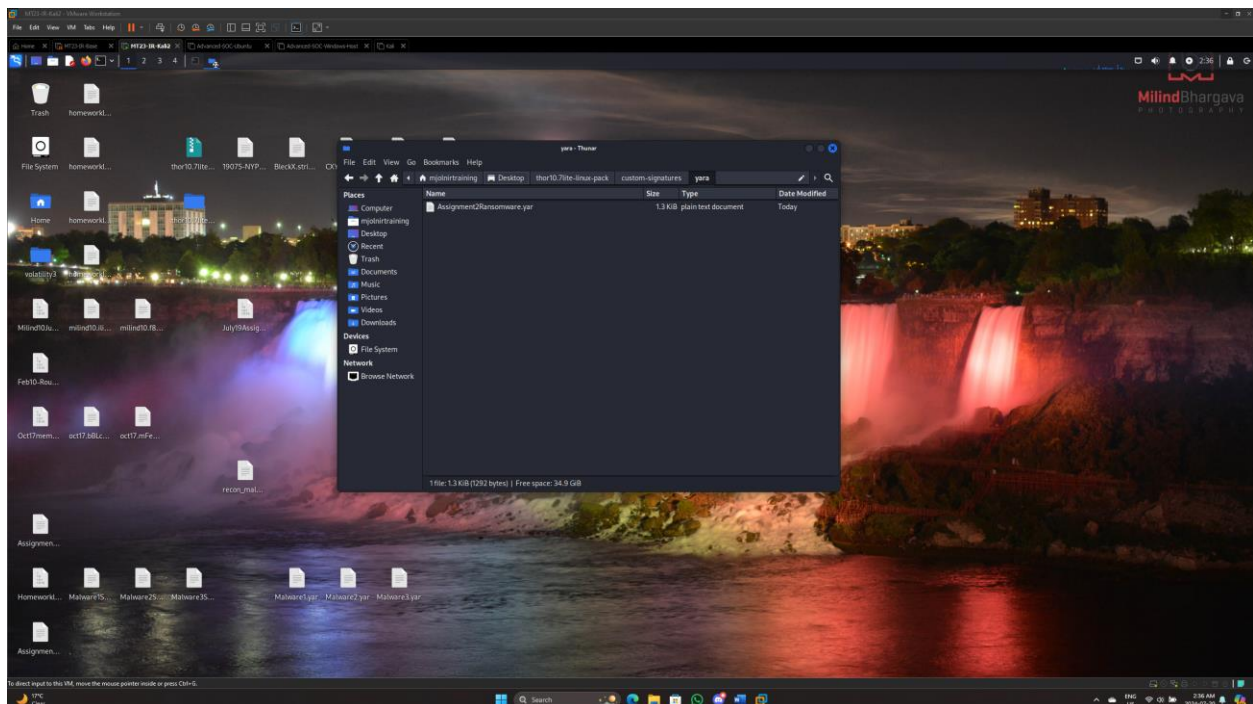
rule CXYJlo_Ransomware_Detection

```
{  
  meta:  
    Description = "Detects the CXYJlo ransomware executed for Assignment 2"  
    Name = "Jordan Patterson"  
  
  strings:  
    $s1 = "LoadLibraryExW" ascii wide fullword  
    $s2 = "CreateToolhelp32Snapshot" ascii wide fullword  
    $s3 = "DeleteCriticalSection" ascii wide fullword  
  
  condition:  
    $s1 and $s2 and $s3  
}
```

rule runlast_Ransomware_Detection

```
{  
  meta:  
    Description = "Detects the runlast ransomware executed for Assignment 2"  
    Name = "Jordan Patterson"  
  
  strings:  
    $s1 = "HYG06" ascii wide fullword  
    $s2 = "gAVYy" ascii wide fullword  
    $s3 = "wDwG" ascii wide fullword  
  
  condition:  
    $s1 and $s2 and $s3  
}
```

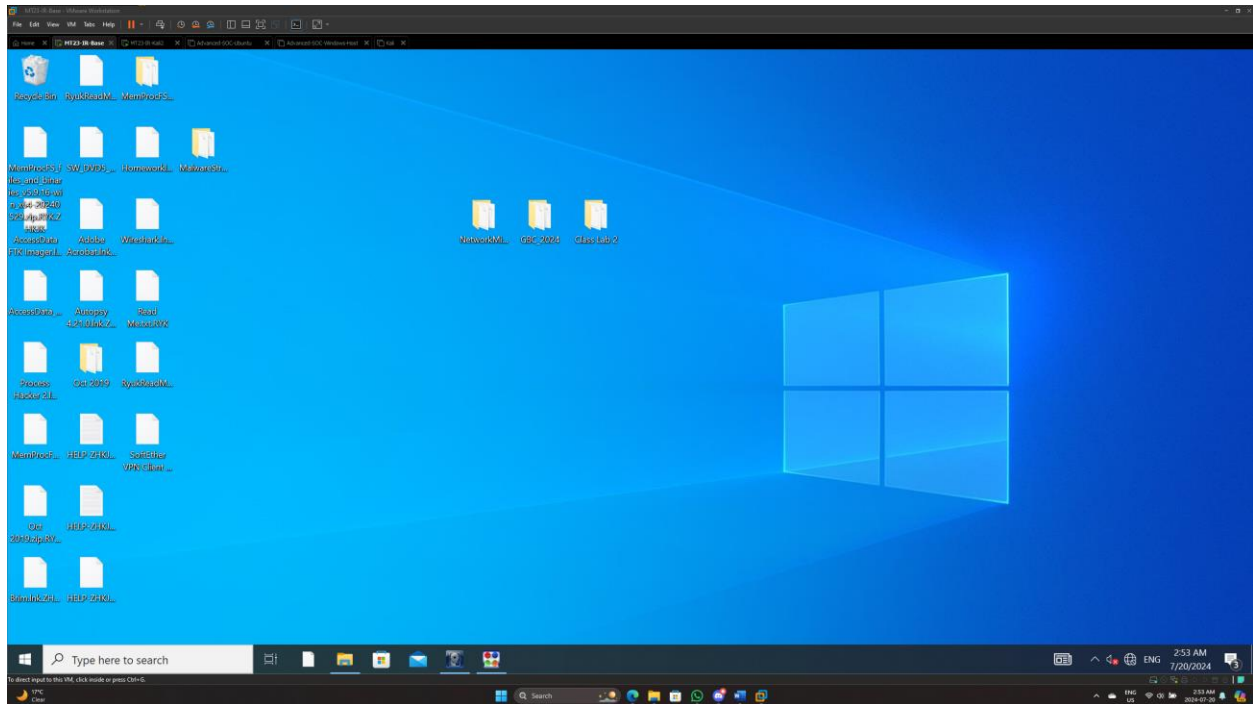
I then placed my custom rules file in Thor Lite's custom signatures folder



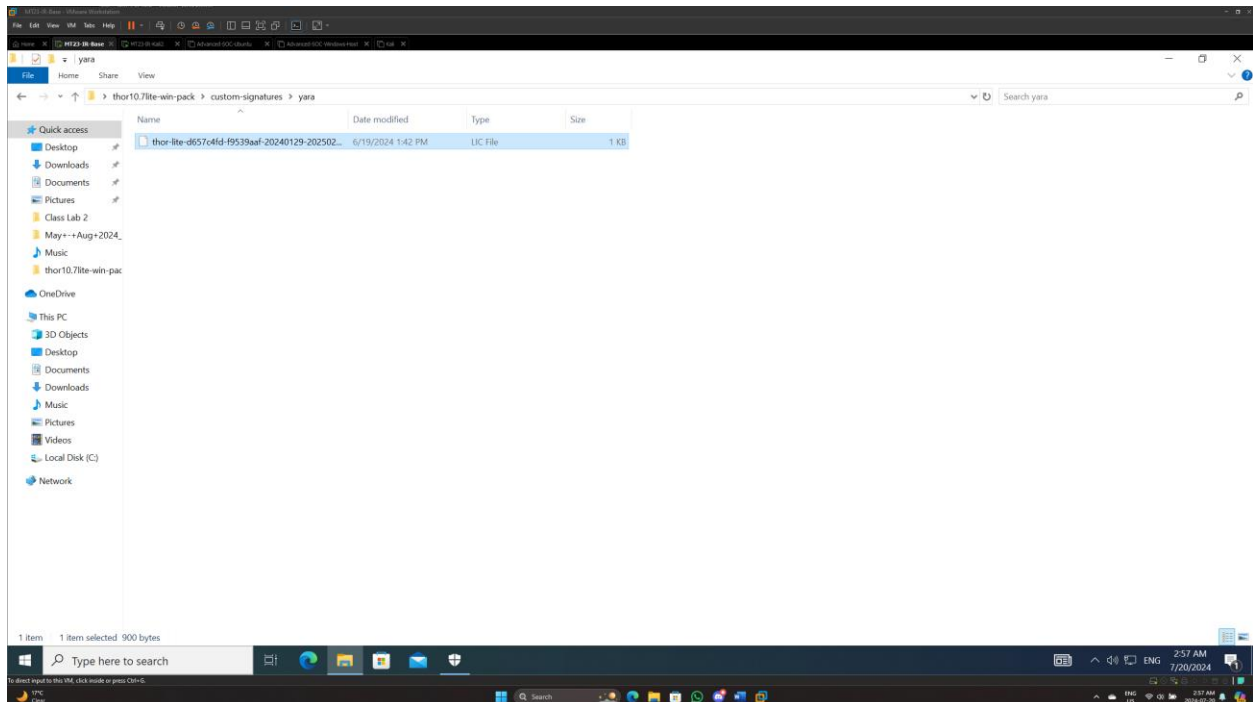
```
sudo ./thor-lite-linux-64 --path /home/mjolinrtraining/Desktop/volatility3 --quick --customonly
```

[illegible]

I returned to my Windows VM and un-paused it but within moments the remainder of my files were encrypted including VMware tools, preventing me from transferring over my custom Yara Signatures.

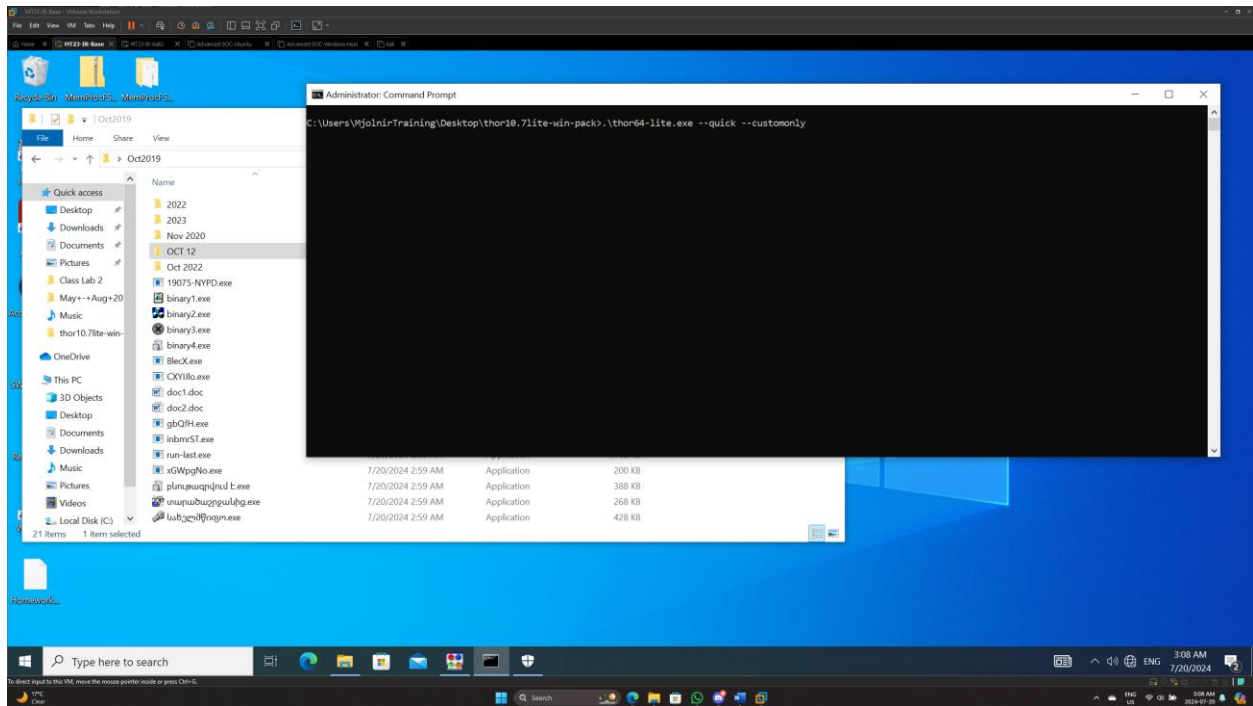


I reloaded the VM and transferred over my custom Yara Signatures.

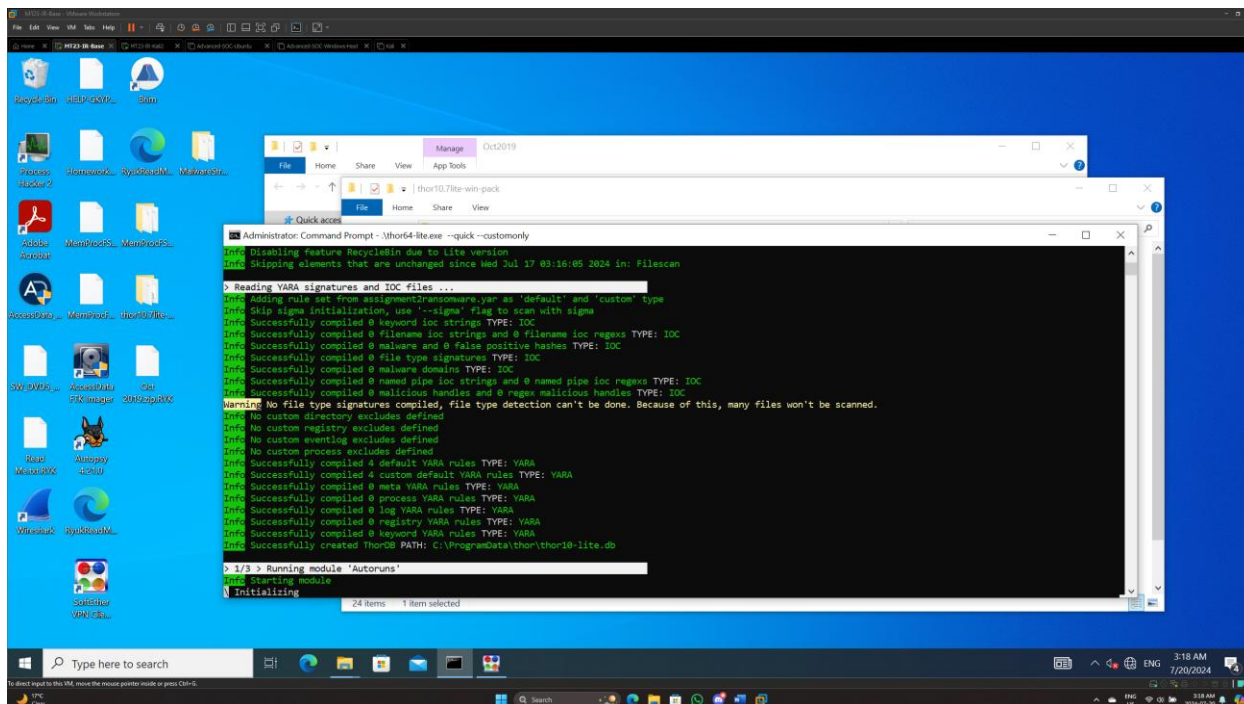


I prepared the following command so that I could run it as soon as the ransomware was ran.

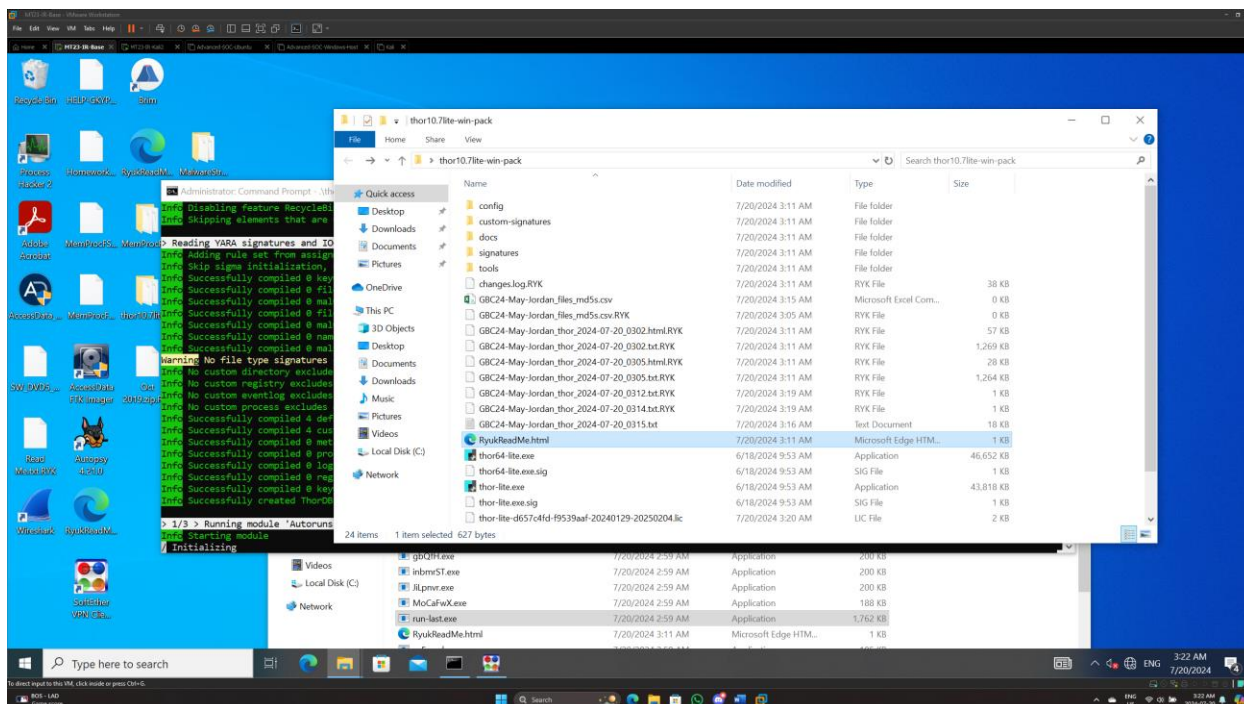
.\thor64-lite.exe --quick --customonly



I turned on my VPN, turned off smartscreen, and re-ran all of the ransomware. I quickly ran a Thor Lite scan before the tool could become encrypted.

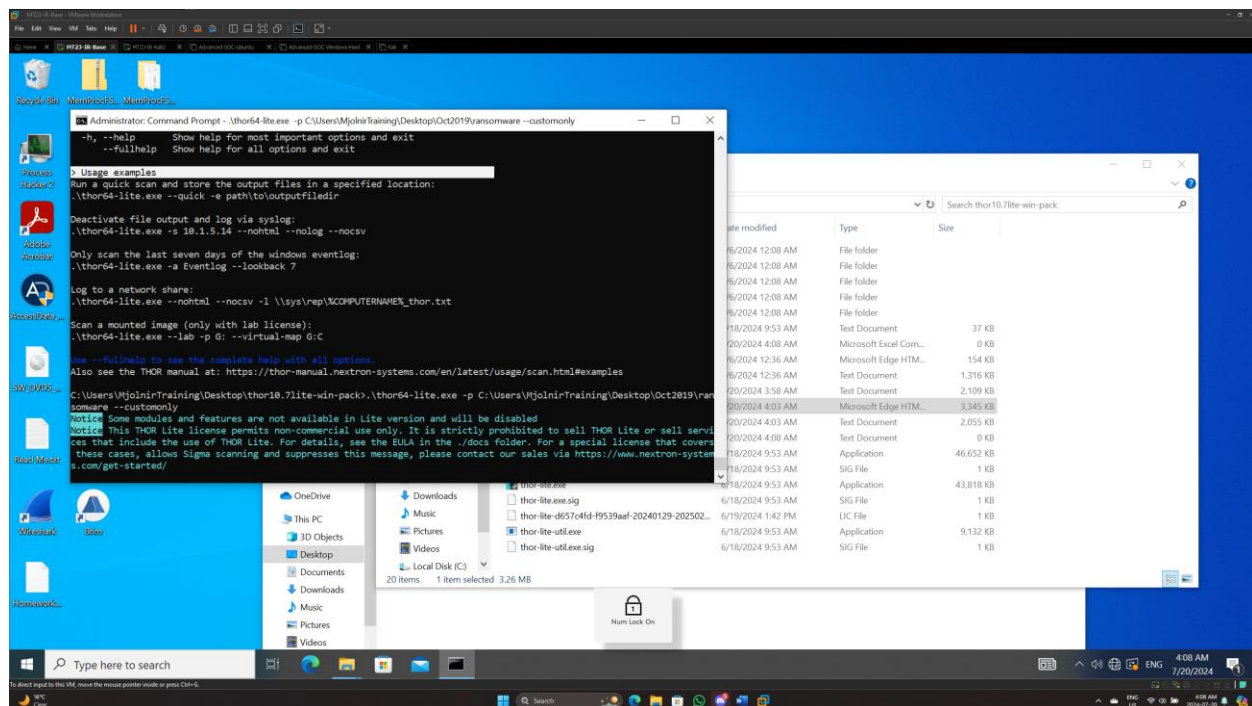


Unfortunately, the tool and my custom signatures became encrypted during the scan, causing the scan to hang.



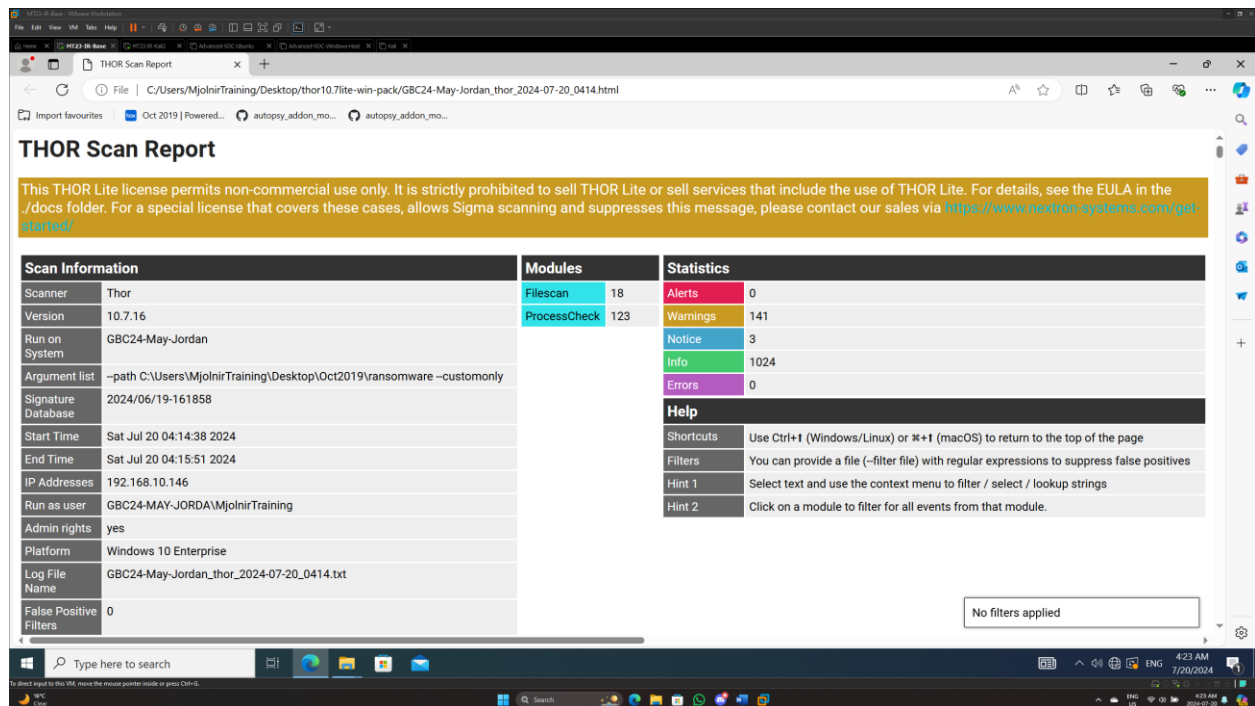
I restarted the VM and reverted to a clean state. I re-ran the scan pointing Thor Lite directly to a directory containing the Ransomware files using the following command.

.\thor64-lite.exe -p C:\Users\MjolinrTraining\Desktop\Oct2019\ransomware --customonly



Despite my specifying the path the scan kept going out of scope and detecting false positives. I tried multiple iterations of the command and tried tweaking my YARA rules but with no change in the result of the scan.

At this stage in the lab I am unsure what's gone wrong with my YARA rules and Thor Lite scan on Windows as they seemed to work perfectly in KALI.



THOR Scan Report

This THOR Lite license permits non-commercial use only. It is strictly prohibited to sell THOR Lite or sell services that include the use of THOR Lite. For details, see the EULA in the ./docs folder. For a special license that covers these cases, allows Sigma scanning and suppresses this message, please contact our sales via <https://www.hextron-systems.com/get-started/>.

Scan Information		Modules		Statistics	
Scanner	Thor	Filescan	18	Alerts	0
Version	10.7.16	ProcessCheck	123	Warnings	141
Run on System	GBC24-May-Jordan			Notice	3
Argument list	-path C:\Users\MjolnirTraining\Desktop\Oct2019\ransomware --customonly			Info	1024
Signature Database	2024/06/19-161858			Errors	0
Start Time	Sat Jul 20 04:14:38 2024			Help	
End Time	Sat Jul 20 04:15:51 2024			Shortcuts	Use Ctrl+T (Windows/Linux) or ⌘+T (macOS) to return to the top of the page
IP Addresses	192.168.10.146			Filters	You can provide a file (-filter file) with regular expressions to suppress false positives
Run as user	GBC24-MAY-JORDA\MjolnirTraining			Hint 1	Select text and use the context menu to filter / select / lookup strings
Admin rights	yes			Hint 2	Click on a module to filter for all events from that module.
Platform	Windows 10 Enterprise				
Log File Name	GBC24-May-Jordan_thor_2024-07-20_0414.txt				
False Positive Filters	0				

No filters applied

Conclusion:

In conclusion, while I was able to successfully complete the necessary steps to get to the point of running my YARA rules on Windows, including getting my YARA rules working in Kali, I was unable to get my Yara rules working properly in Windows and I was unable to run the scan live while the malware was running.