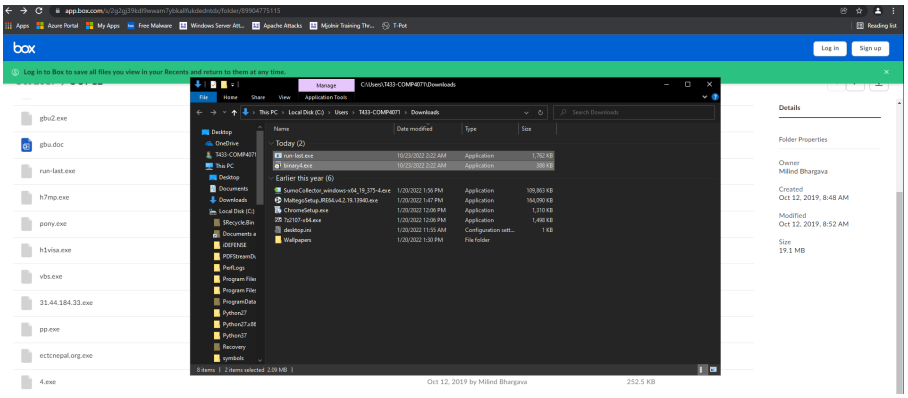
Forensics Lab

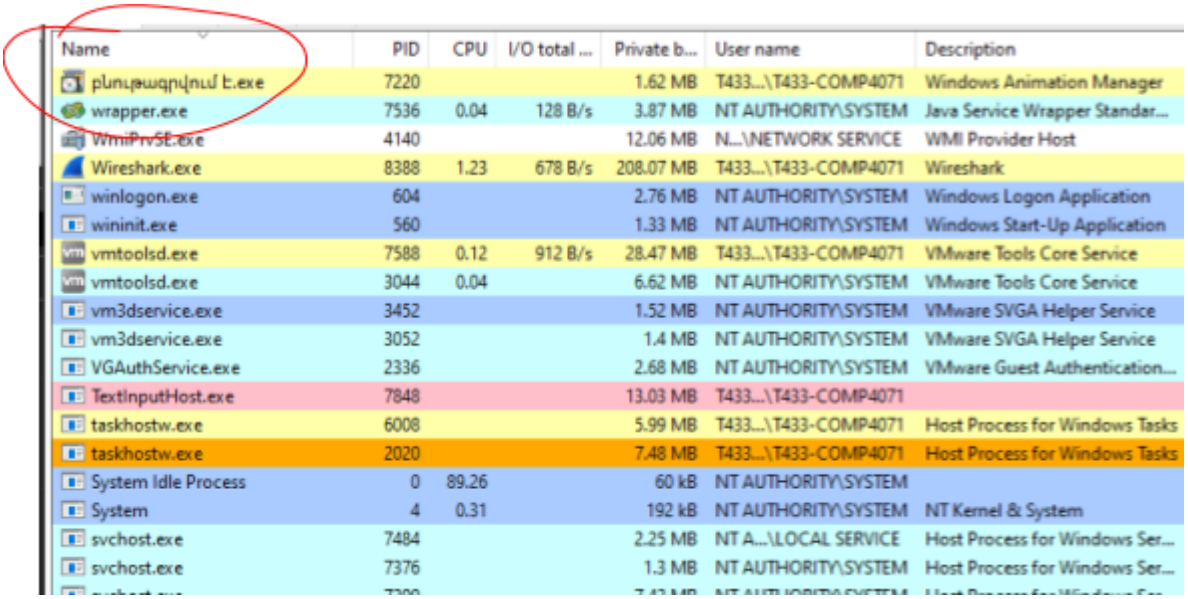
Author Name: Hui Nok Hang

Download and run malwares

The two malwares - binary4.exe and run-last.exe are then downloaded and run in the virtual machine environment.

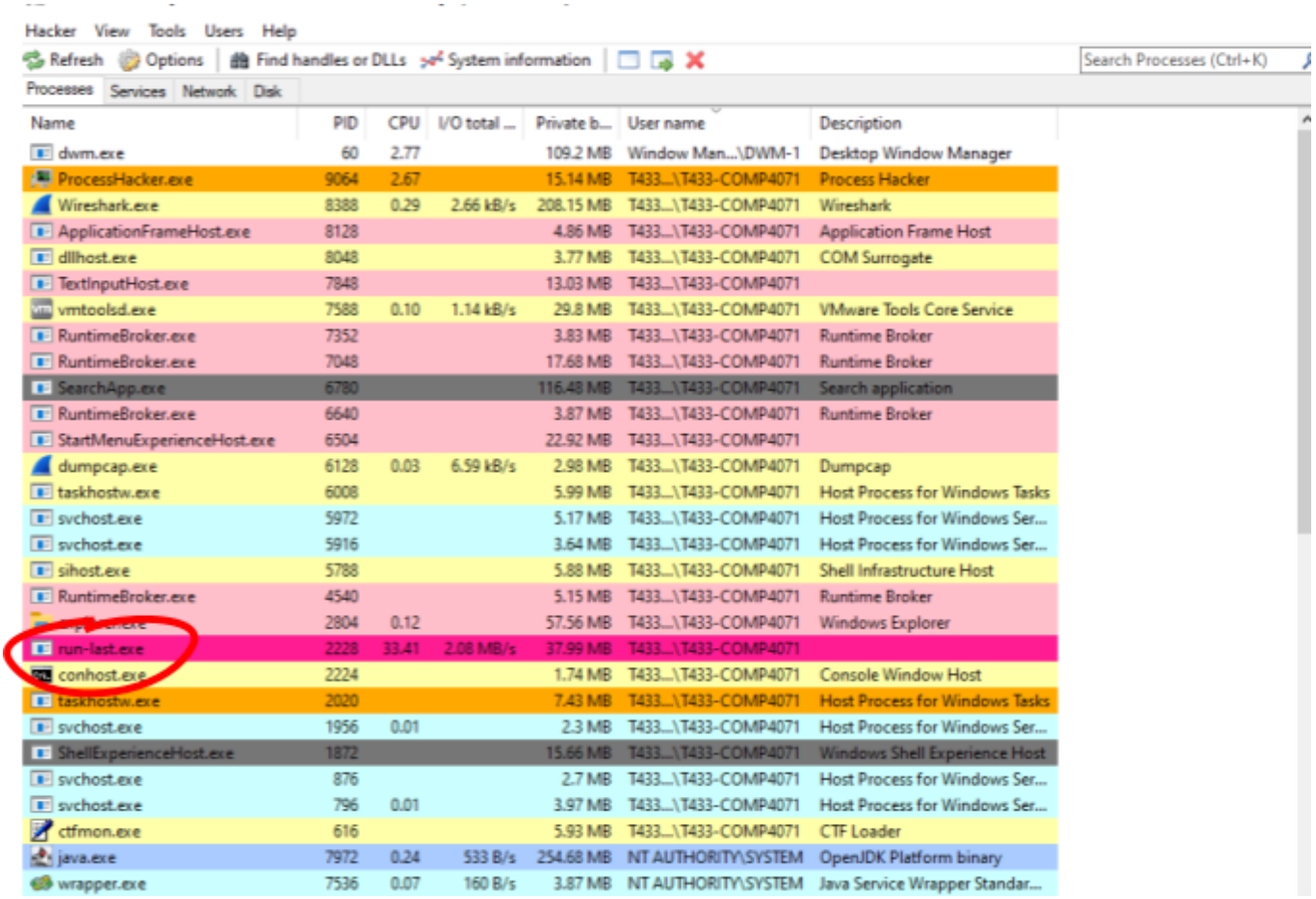


During the process, we can see some malicious activities in Process Hacker. This process with unintelligible text on the top of the process list appears suspicious after the malware binary4.exe is run. However it only lasted for a few seconds before disappearing into thin air.



Name	PID	CPU	I/O total ...	Private b...	User name	Description
pluŋəwqŋvuʌ t.exe	7220			1.62 MB	T433...\T433-COMP4071	Windows Animation Manager
wrapper.exe	7536	0.04	128 B/s	3.87 MB	NT AUTHORITY\SYSTEM	Java Service Wrapper Standar...
WmiPrvSE.exe	4140			12.06 MB	N...\NETWORK SERVICE	WMI Provider Host
Wireshark.exe	8388	1.23	678 B/s	208.07 MB	T433...\T433-COMP4071	Wireshark
winlogon.exe	604			2.76 MB	NT AUTHORITY\SYSTEM	Windows Logon Application
wininit.exe	560			1.33 MB	NT AUTHORITY\SYSTEM	Windows Start-Up Application
vmtoolsd.exe	7588	0.12	912 B/s	28.47 MB	T433...\T433-COMP4071	VMware Tools Core Service
vmtoolsd.exe	3044	0.04		6.62 MB	NT AUTHORITY\SYSTEM	VMware Tools Core Service
vm3dservice.exe	3452			1.52 MB	NT AUTHORITY\SYSTEM	VMware SVGA Helper Service
vm3dservice.exe	3052			1.4 MB	NT AUTHORITY\SYSTEM	VMware SVGA Helper Service
VGAuthService.exe	2336			2.68 MB	NT AUTHORITY\SYSTEM	VMware Guest Authentication...
TextInputHost.exe	7848			13.03 MB	T433...\T433-COMP4071	
taskhostw.exe	6008			5.99 MB	T433...\T433-COMP4071	Host Process for Windows Tasks
taskhostw.exe	2020			7.48 MB	T433...\T433-COMP4071	Host Process for Windows Tasks
System Idle Process	0	89.26		60 kB	NT AUTHORITY\SYSTEM	
System	4	0.31		192 kB	NT AUTHORITY\SYSTEM	NT Kernel & System
svchost.exe	7484			2.25 MB	NT A...\LOCAL SERVICE	Host Process for Windows Ser...
svchost.exe	7376			1.3 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...

And now when the second malware run-last.exe is run, it appears and persists in the process list while seemingly pulling in a high I/O and CPU utilization speed. Knowing that this process is a ransomware that encrypts device files, the phenomenon makes total sense.



Hacker View Tools Users Help

Refresh | Options | Find handles or DLLs | System information | Search Processes (Ctrl+K)

Processes | Services | Network | Disk

Name	PID	CPU	I/O total ...	Private b...	User name	Description
dwm.exe	60	2.77		109.2 MB	Window Man...\DWM-1	Desktop Window Manager
ProcessHacker.exe	9064	2.67		15.14 MB	T433...\T433-COMP4071	Process Hacker
Wireshark.exe	8388	0.29	2.66 kB/s	208.15 MB	T433...\T433-COMP4071	Wireshark
ApplicationFrameHost.exe	8128			4.86 MB	T433...\T433-COMP4071	Application Frame Host
dllhost.exe	8048			3.77 MB	T433...\T433-COMP4071	COM Surrogate
TextInputHost.exe	7848			13.03 MB	T433...\T433-COMP4071	
vmtoolsd.exe	7588	0.10	1.14 kB/s	29.8 MB	T433...\T433-COMP4071	VMware Tools Core Service
RuntimeBroker.exe	7352			3.83 MB	T433...\T433-COMP4071	Runtime Broker
RuntimeBroker.exe	7048			17.68 MB	T433...\T433-COMP4071	Runtime Broker
SearchApp.exe	6780			116.48 MB	T433...\T433-COMP4071	Search application
RuntimeBroker.exe	6640			3.87 MB	T433...\T433-COMP4071	Runtime Broker
StartMenuExperienceHost.exe	6504			22.92 MB	T433...\T433-COMP4071	
dumpcap.exe	6128	0.03	6.59 kB/s	2.98 MB	T433...\T433-COMP4071	Dumpcap
taskhostw.exe	6008			5.99 MB	T433...\T433-COMP4071	Host Process for Windows Tasks
svchost.exe	5972			5.17 MB	T433...\T433-COMP4071	Host Process for Windows Ser...
svchost.exe	5916			3.64 MB	T433...\T433-COMP4071	Host Process for Windows Ser...
sihost.exe	5788			5.88 MB	T433...\T433-COMP4071	Shell Infrastructure Host
RuntimeBroker.exe	4540			5.15 MB	T433...\T433-COMP4071	Runtime Broker
[illegible]	2804	0.12		57.56 MB	T433...\T433-COMP4071	Windows Explorer
run-last.exe	2228	33.41	2.08 MB/s	37.99 MB	T433...\T433-COMP4071	
conhost.exe	2224			1.74 MB	T433...\T433-COMP4071	Console Window Host
taskhostw.exe	2020			7.43 MB	T433...\T433-COMP4071	Host Process for Windows Tasks
svchost.exe	1956	0.01		2.3 MB	T433...\T433-COMP4071	Host Process for Windows Ser...
ShellExperienceHost.exe	1872			15.66 MB	T433...\T433-COMP4071	Windows Shell Experience Host
svchost.exe	876			2.7 MB	T433...\T433-COMP4071	Host Process for Windows Ser...
svchost.exe	796	0.01		3.97 MB	T433...\T433-COMP4071	Host Process for Windows Ser...
ctfmon.exe	616			5.93 MB	T433...\T433-COMP4071	CTF Loader
java.exe	7972	0.24	533 B/s	254.68 MB	NT AUTHORITY\SYSTEM	OpenJDK Platform binary
wrapper.exe	7536	0.07	160 B/s	3.87 MB	NT AUTHORITY\SYSTEM	Java Service Wrapper Standar...

Malware analysis by volatility

After capturing the memory dump via ATK Imager, the dump was imported into Kali for further analysis using volatility 3.

For starters, I decided to use the following plugins to dissect the memory information:
windows.pstree.PsTree
windows.netscan.NetScan
timeliner.Timeliner

First, I saved all the analysis outputs into textfiles.

```
(t433-student㉿T433-HuiNokHang-COMP4071)-[~/Documents/Tools/volatility3]
└─$ sudo python3 vol.py -f memdump.mem windows.pstree.PsTree > pstree.txt

(t433-student㉿T433-HuiNokHang-COMP4071)-[~/Documents/Tools/volatility3]
└─$ sudo python3 vol.py -f memdump.mem windows.netscan.NetScan > netscan.txt

(t433-student㉿T433-HuiNokHang-COMP4071)-[~/Documents/Tools/volatility3]
└─$ sudo python3 vol.py -f memdump.mem timeliner.Timeliner > timeliner.txt

(t433-student㉿T433-HuiNokHang-COMP4071)-[~/Documents/Tools/volatility3]
└─$ ls
API_CHANGES.md  LICENSE.txt  mypy.ini     README.md                requirements.txt  timeliner.txt  volshell.py
development     MANIFEST.in  netscan.txt  requirements-dev.txt     setup.py          volatility3    volshell.spec
doc             memdump.mem  pstree.txt   requirements-minimal.txt test              vol.py         vol.spec

(t433-student㉿T433-HuiNokHang-COMP4071)-[~/Documents/Tools/volatility3]
└─$
```

Pstree

```
** 1516 684     svchost.exe     0x7098e456080  4       -       0       False   2022-10-23 06:15:35.000000      N/A
** 3052 684     vm3dservice.ex  0x7098ea31080  2       -       0       False   2022-10-23 06:15:43.000000      N/A
*** 3452        3052    vm3dservice.ex  0x7098eb40100  2       -       1       False   2022-10-23 06:15:48.000000      N/A
** 5620 684     svchost.exe     0x70991b020c0  1       -       0       False   2022-10-23 06:17:58.000000      N/A
** 6136 684     svchost.exe     0x7098f9990c0  3       -       0       False   2022-10-23 06:16:39.000000      N/A
*** 616 6136    ctfmon.exe      0x7098977e300  9       -       1       False   2022-10-23 06:16:40.000000      N/A
* 860   560     fontdrvhost.ex  0x7098db9a080  5       -       0       False   2022-10-23 06:15:29.000000      N/A
604     532     winlogon.exe    0x7098db05240  4       -       1       False   2022-10-23 06:15:25.000000      N/A
* 6036  604     userinit.exe    0x7098fb1d0c0  0       -       1       False   2022-10-23 06:16:46.000000      2022-10-23 06:17:22.000000
** 2804 6036    explorer.exe    0x7098fb3b080  52      -       1       False   2022-10-23 06:16:47.000000      N/A
*** 7588        2804    vmtoolsd.exe    0x7098f9f4080  7       -       1       False   2022-10-23 06:17:18.000000      N/A
*** 9064        2804    ProcessHacker.  0x70991a57080  7       -       1       False   2022-10-23 06:40:48.000000      N/A
*** 2228        2804    run-last.exe    0x7098eddf080  8       -       1       True    2022-10-23 06:44:19.000000      N/A
**** 632        2228    cmd.exe 0x7098e947080  1       -       1       True    2022-10-23 06:59:36.000000      N/A
***** 2776       632     conhost.exe     0x7098ee5e080  3       -       1       False   2022-10-23 06:59:36.000000      N/A
***** 6960       632     cipher.exe      0x70991e39080  1       -       1       True    2022-10-23 06:59:36.000000      N/A
*** 7800        2804    msedge.exe      0x7098f42f080  0       -       1       False   2022-10-23 06:17:21.000000      2022-10-23 06:17:43.00000
0
*** 7160        2804    FTK Imager.exe  0x7098f237080  12      -       1       False   2022-10-23 07:05:15.000000      N/A
*** 6360        2804    chrome.exe      0x70991ce0340  0       -       1       False   2022-10-23 06:18:53.000000      2022-10-23 06:40:12.00000
0
**** 6712       6360    chrome.exe      0x7099129c080  0       -       1       False   2022-10-23 06:33:59.000000      2022-10-23 06:40:11.00000
0
***** 1144       6712    software_repor  0x7098f30c300  0       -       1       False   2022-10-23 06:19:09.000000      2022-10-23 06:28:02.00000
0
***** 5448       6712    software_repor  0x7098f307080  0       -       1       False   2022-10-23 06:19:10.000000      2022-10-23 06:28:02.00000
0
* 852   604     fontdrvhost.ex  0x7098db9d080  5       -       1       False   2022-10-23 06:15:29.000000      N/A
* 60    604     dwm.exe 0x7098e23a080  15      -       1       False   2022-10-23 06:15:31.000000      N/A
3432    7152    ngen.exe        0x7098fdfa080  0       -       0       False   2022-10-23 06:32:39.000000      2022-10-23 06:33:53.000000
7040    8388    dumpcap.exe     0x70992094080  0       -       1       False   2022-10-23 06:33:22.000000      2022-10-23 06:33:23.000000
5272    7676    svchost.exe     0x7098e919080  4       -       0       False   2022-10-23 06:44:50.000000      N/A

(t433-student㉿T433-HuiNokHang-COMP4071)-[~/Documents/Tools/volatility3]
└─$
```

The first thing I noticed is cipher.exe. Since we know that the malware is a ransomware that encrypts your data, cipher.exe sounds perfectly reasonably like the name of the process responsible for that job.

If we trace cipher.exe (PID 6960) back to its mother process (PID 632), we will find cmd.exe two entries above that. This is another indication that these are likely processes run by malware, since cmd is often used for running commands and accessing or modifying system data.

Tracing back one level, the mother process of cmd.exe (PID 632) is run-last.exe, precisely the malware that we ran.

```
File  Actions  Edit  View  Help
*** 616 6136    ctfmon.exe       0x c7098977e300  9    -    1    False   2022-10-23 06:16:40.000000    N/A
* 860   560     fontdrvhost.ex   0x c7098db9a080  5    -    0    False   2022-10-23 06:15:29.000000    N/A
604     532     winlogon.exe     0x c7098db05240  4    -    1    False   2022-10-23 06:15:25.000000    N/A
* 6036  604     userinit.exe     0x c7098fb1d0c0  0    -    1    False   2022-10-23 06:16:46.000000    2022-10-23 06:17:22.000000
** 2804 6036    explorer.exe     0x c7098fb3b080  52   -    1    False   2022-10-23 06:16:47.000000    N/A
*** 7588        2804    vmtoolsd.exe     0x c7098f9f4080  7    -    1    False   2022-10-23 06:17:18.000000    N/A
*** 9064        2804    ProcessHacker.   0x c70991a57080  7    -    1    False   2022-10-23 06:40:48.000000    N/A
*** 2228        2804    run-last.exe     0x c7098eddf080  8    -    1    True    2022-10-23 06:44:19.000000    N/A
**** 632        2228    cmd.exe 0x c7098e947080  1    -    1    True    2022-10-23 06:59:36.000000    N/A
***** 2776       632     conhost.exe      0x c7098ee5e080  3    -    1    False   2022-10-23 06:59:36.000000    N/A
***** 6960       632     cipher.exe       0x c70991e39080  1    -    1    True    2022-10-23 06:59:36.000000    N/A
*** 7800        2804    msedge.exe       0x c7098f42f080  0    -    1    False   2022-10-23 06:17:21.000000    2022-10-23 06:17:43.00000
0
*** 7160        2804    FTK Imager.exe   0x c7098f237080  12   -    1    False   2022-10-23 07:05:15.000000    N/A
*** 6360        2804    chrome.exe       0x c70991ce0340  0    -    1    False   2022-10-23 06:18:53.000000    2022-10-23 06:40:12.00000
0
**** 6712       6360    chrome.exe       0x c7099129c080  0    -    1    False   2022-10-23 06:33:59.000000    2022-10-23 06:40:11.00000
0
***** 1144       6712    software_repor   0x c7098f30c300  0    -    1    False   2022-10-23 06:19:09.000000    2022-10-23 06:28:02.00000
0
***** 5448       6712    software_repor   0x c7098f307080  0    -    1    False   2022-10-23 06:19:10.000000    2022-10-23 06:28:02.00000
0
* 852   604     fontdrvhost.ex   0x c7098db9d080  5    -    1    False   2022-10-23 06:15:29.000000    N/A
* 60    604     dwm.exe 0x c7098e23a080  15   -    1    False   2022-10-23 06:15:31.000000    N/A
3432    7152    ngen.exe         0x c7098fdfa080  0    -    0    False   2022-10-23 06:32:39.000000    2022-10-23 06:33:53.000000
7040    8388    dumpcap.exe      0x c70992094080  0    -    1    False   2022-10-23 06:33:22.000000    2022-10-23 06:33:23.000000
5272    7676    svchost.exe      0x c7098e919080  4    -    0    False   2022-10-23 06:44:50.000000    N/A

┌──(t433-student㉿T433-HuiNokHang-COMP4071)-[~/Documents/Tools/volatility3]
└─$ cat pstree.txt | grep 2228
*** 2228        2804    run-last.exe     0x c7098eddf080  8    -    1    True    2022-10-23 06:44:19.000000    N/A
**** 632        2228    cmd.exe 0x c7098e947080  1    -    1    True    2022-10-23 06:59:36.000000    N/A

┌──(t433-student㉿T433-HuiNokHang-COMP4071)-[~/Documents/Tools/volatility3]
└─$
```

Netscan

The second step of memory forensics is to investigate what kind of network traffic went through the system during the malware operation.

```
File  Actions  Edit  View  Help

┌──(t433-student㉿T433-HuiNokHang-COMP4071)-[~/Documents/Tools/volatility3]
└─$ cat netscan.txt
Volatility 3 Framework 2.4.0

Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0x9b881c96bb60  TCPv4   192.168.10.151  49920   52.60.149.211   443     ESTABLISHED     7972    java.exe        2022-10-23 06:21:16.000000
0x c7098a808730  TCPv4   169.254.79.144  139     0.0.0.0 0       LISTENING       4       System  2022-10-23 06:15:19.000000
0x c7098a808e10  TCPv4   0.0.0.0 49668   0.0.0.0 0       LISTENING       2144    spoolsv.exe     2022-10-23 06:15:41.000000
0x c7098a808e10  TCPv6   ::      49668   ::      0       LISTENING       2144    spoolsv.exe     2022-10-23 06:15:41.000000
0x c7098a809d30  TCPv4   0.0.0.0 49668   0.0.0.0 0       LISTENING       2144    spoolsv.exe     2022-10-23 06:15:41.000000
0x c7098d03db40  UDPv4   0.0.0.0 63113   *       0               1944    svchost.exe     2022-10-23 07:07:02.000000
0x c7098d03db40  UDPv6   ::      63113   *       0               1944    svchost.exe     2022-10-23 07:07:02.000000
0x c7098d03eae0  UDPv4   0.0.0.0 52761   *       0               1944    svchost.exe     2022-10-23 07:07:02.000000
0x c7098d03eae0  UDPv6   ::      52761   *       0               1944    svchost.exe     2022-10-23 07:07:02.000000
0x c7098d03ee00  UDPv4   0.0.0.0 0       *       0               2976    MsSense.exe     2022-10-23 07:07:02.000000
0x c7098d03ee00  UDPv6   ::      0       *       0               2976    MsSense.exe     2022-10-23 07:07:02.000000
0x c7098d056690  UDPv6   fe80::f9aa:410a:904d:4f90       546     *       0               1440    svchost.exe     2022-10-23 07:05:29.000000
0x c7098d06cae0  UDPv4   0.0.0.0 61773   *       0               -       -       2022-10-23 06:36:18.000000
0x c7098d071370  UDPv4   0.0.0.0 59125   *       0               -       -       2022-10-23 06:36:22.000000
0x c7098d072e00  UDPv4   0.0.0.0 51988   *       0               -       -       2022-10-23 06:35:51.000000
0x c7098d082260  UDPv4   0.0.0.0 56884   *       0               1944    svchost.exe     2022-10-23 06:40:05.000000
0x c7098d082260  UDPv6   ::      56884   *       0               1944    svchost.exe     2022-10-23 06:40:05.000000
0x c7098d0b11f0  UDPv4   0.0.0.0 3702    *       0               2740    svchost.exe     2022-10-23 06:18:45.000000
0x c7098d0b2320  UDPv4   169.254.79.144  137     *       0               4       System  2022-10-23 06:15:19.000000
0x c7098d0b27d0  UDPv4   169.254.79.144  138     *       0               4       System  2022-10-23 06:15:19.000000
0x c7098d15baf0  UDPv4   0.0.0.0 3702    *       0               2740    svchost.exe     2022-10-23 06:18:45.000000
0x c7098d15baf0  UDPv6   ::      3702    *       0               2740    svchost.exe     2022-10-23 06:18:45.000000
0x c7098d1fd050  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       944     svchost.exe     2022-10-23 06:15:30.000000
0x c7098d1fd050  TCPv6   ::      135     ::      0       LISTENING       944     svchost.exe     2022-10-23 06:15:30.000000
0x c7098d1fd310  TCPv4   0.0.0.0 49665   0.0.0.0 0       LISTENING       560     wininit.exe     2022-10-23 06:15:30.000000
0x c7098d1fd310  TCPv6   ::      49665   ::      0       LISTENING       560     wininit.exe     2022-10-23 06:15:30.000000
0x c7098d1fd470  TCPv4   0.0.0.0 49666   0.0.0.0 0       LISTENING       1268    svchost.exe     2022-10-23 06:15:35.000000
0x c7098d1fd5d0  TCPv4   192.168.171.131 139     0.0.0.0 0       LISTENING       4       System  2022-10-23 06:15:38.000000
```

We can see a public IP address at the top of the list: 52.60.149.211. Upon a whois lookup, the IP address is an AWS server so we can presume that the computer was communicating with some services hosted on AWS. The process that established this TCP connection was java.exe. The reason is unknown and it can potentially be a malicious service under a disguise.

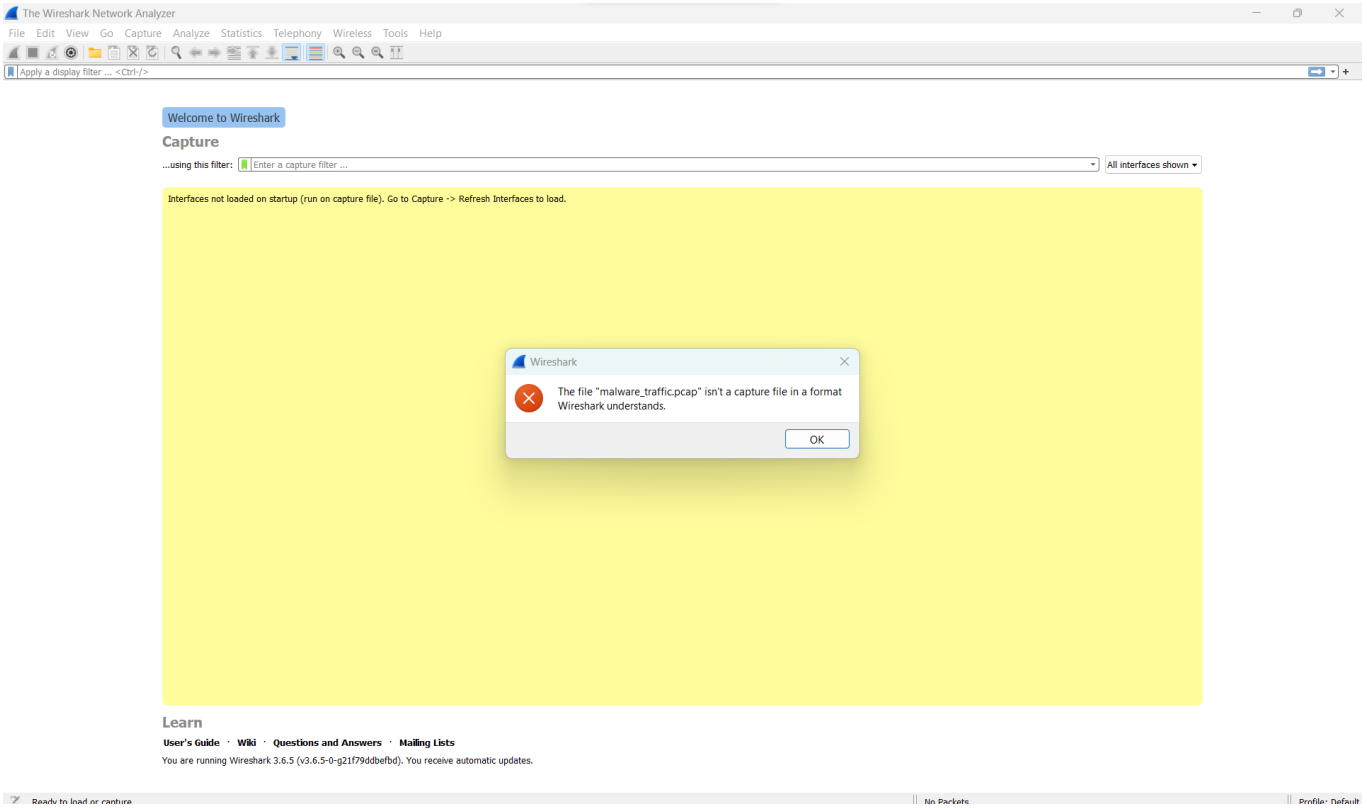
```
File  Actions  Edit  View  Help
0xc7098e5c4470  UDPv4   192.168.171.131 56478   *       0               3748    svchost.exe     2022-10-23 06:18:45.000000
0xc7098e5c4600  UDPv4   192.168.68.131  56479   *       0               3748    svchost.exe     2022-10-23 06:18:45.000000
0xc7098e5c4920  UDPv4   192.168.10.151  56481   *       0               3748    svchost.exe     2022-10-23 06:18:45.000000
0xc7098e5c4dd0  UDPv4   169.254.79.144  56480   *       0               3748    svchost.exe     2022-10-23 06:18:45.000000
0xc7098e5c50f0  UDPv4   127.0.0.1       56482   *       0               3748    svchost.exe     2022-10-23 06:18:45.000000
0xc7098e5c5280  UDPv6   fe80::f9aa:410a:904d:4f90       56476   *       0               3748    svchost.exe     2022-10-23 06:18:45.000000
0xc7098e5c55a0  UDPv4   0.0.0.0 49241   *       0               1944    svchost.exe     2022-10-23 06:44:47.000000
0xc7098e5c55a0  UDPv6   ::      49241   *       0               1944    svchost.exe     2022-10-23 06:44:47.000000
0xc7098e5c5a50  UDPv6   ::1     56477   *       0               3748    svchost.exe     2022-10-23 06:18:45.000000
0xc7098e5c5be0  UDPv4   0.0.0.0 60010   *       0               1944    svchost.exe     2022-10-23 06:57:52.000000
0xc7098e5c5be0  UDPv6   ::      60010   *       0               1944    svchost.exe     2022-10-23 06:57:52.000000
0xc7098e9fe1b0  TCPv4   127.0.0.1       32000   0.0.0.0 0       LISTENING       7536    wrapper.exe     2022-10-23 06:21:09.000000
0xc7098e9fe310  TCPv4   0.0.0.0 5040    0.0.0.0 0       LISTENING       1652    svchost.exe     2022-10-23 06:16:48.000000
0xc7098e9fe5d0  TCPv4   0.0.0.0 49671   0.0.0.0 0       LISTENING       684     services.exe    2022-10-23 06:15:58.000000
0xc7098e9fe890  TCPv4   0.0.0.0 49671   0.0.0.0 0       LISTENING       684     services.exe    2022-10-23 06:15:58.000000
0xc7098e9fe890  TCPv6   ::      49671   ::      0       LISTENING       684     services.exe    2022-10-23 06:15:58.000000
0xc7098e9fee10  TCPv4   0.0.0.0 49670   0.0.0.0 0       LISTENING       2680    svchost.exe     2022-10-23 06:15:55.000000
0xc7098e9ffa70  TCPv4   0.0.0.0 445     0.0.0.0 0       LISTENING       4       System  2022-10-23 06:15:52.000000
0xc7098e9ffa70  TCPv6   ::      445     ::      0       LISTENING       4       System  2022-10-23 06:15:52.000000
0xc7098e9ffd30  TCPv4   0.0.0.0 49670   0.0.0.0 0       LISTENING       2680    svchost.exe     2022-10-23 06:15:55.000000
0xc7098e9ffd30  TCPv6   ::      49670   ::      0       LISTENING       2680    svchost.exe     2022-10-23 06:15:55.000000
0xc7098eb05b60  TCPv4   192.168.10.151  49920   52.60.149.211   443     ESTABLISHED     7972    java.exe        2022-10-23 06:21:16.000000
0xc7098ef08730  TCPv4   192.168.10.151  49841   52.226.139.121  443     ESTABLISHED     2964    svchost.exe     2022-10-23 06:18:48.000000
0xc7099123a460  TCPv4   127.0.0.1       31000   127.0.0.1       32000   ESTABLISHED     7972    java.exe        2022-10-23 06:21:10.000000
0xc7099140db00  TCPv4   192.168.10.151  49845   52.226.139.121  443     ESTABLISHED     2964    svchost.exe     2022-10-23 06:18:53.000000
0xc709914fbbd0  TCPv4   192.168.10.151  139     0.0.0.0 0       LISTENING       4       System  2022-10-23 06:18:45.000000
0xc70991a114b0  TCPv4   192.168.10.151  24977   186.42.98.254   449     CLOSED  5272    svchost.exe     2022-10-23 07:02:25.000000
0xc70991e53010  TCPv4   192.168.10.151  24983   104.46.127.225  443     CLOSED  7576    SenseNdr.exe    2022-10-23 07:04:02.000000
0xc70991e7cb60  TCPv4   192.168.10.151  49919   52.60.149.211   443     ESTABLISHED     7972    java.exe        2022-10-23 06:21:15.000000
0xc70992124b60  TCPv4   127.0.0.1       32000   127.0.0.1       31000   ESTABLISHED     7536    wrapper.exe     2022-10-23 06:21:10.000000
0xc70992140010  TCPv4   192.168.10.151  24951   104.46.127.225  443     CLOSED  2776    conhost.exe     2022-10-23 06:54:00.000000
0xc70992c9daa0  TCPv4   192.168.10.151  24986   181.199.102.179 449     CLOSED  5272    svchost.exe     2022-10-23 07:05:14.000000

┌──(t433-student㉿T433-HuiNokHang-COMP4071)-[~/Documents/Tools/volatility3]
└─$
```

Towards the end of the list, there are also a bunch of public IPs that the computer was trying to establish a TCP connection with. The services involved are java.exe (again), wrapper.exe, conhost.exe, svchost.exe and SenseNdr.exe. Not certain if they are malicious.

In total, the public IP addresses that appeared in the netscan were:

- 52.60.149.211
- 52.226.139.121
- 186.42.98.225
- 104.46.127.225
- 181.199.102.179



Interfaces not loaded on startup (run on capture file). Go to Capture -> Refresh Interfaces to load.

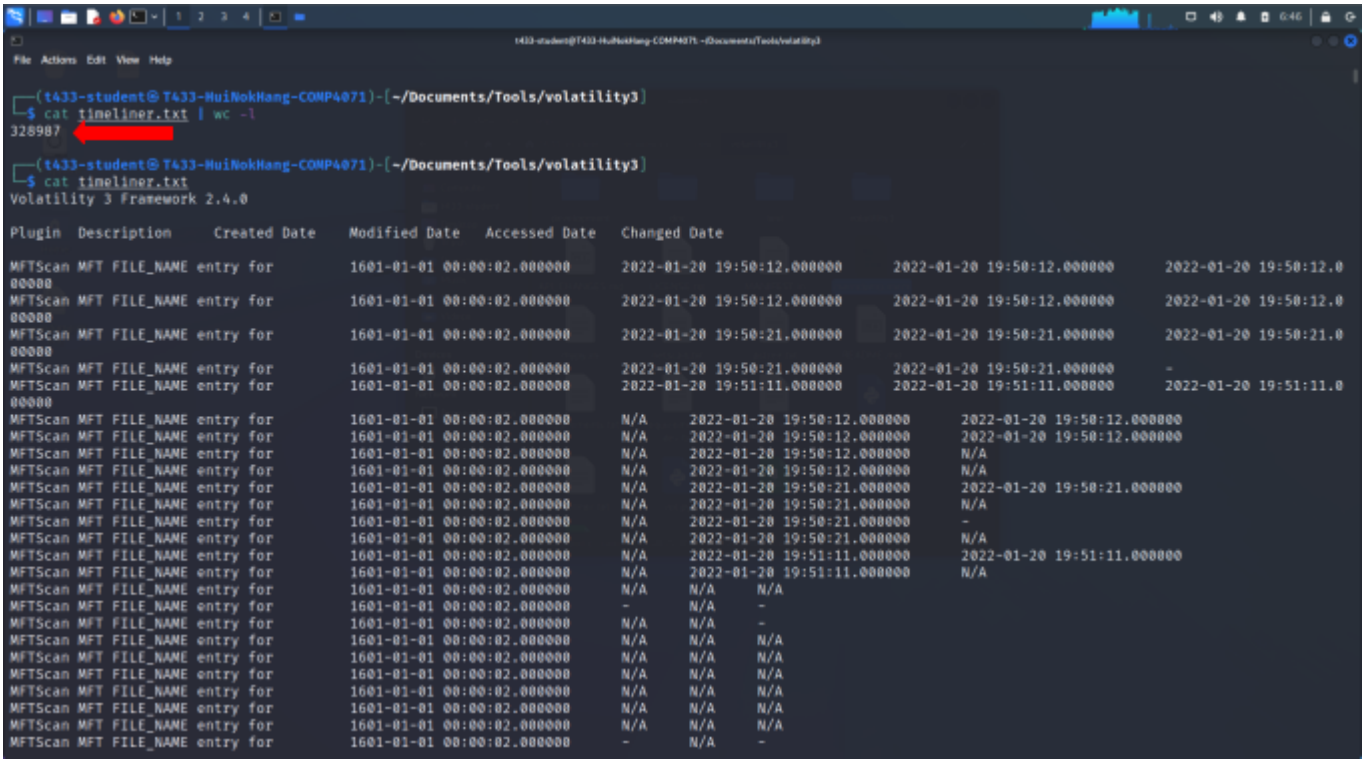
The file "malware_traffic.pcap" isn't a capture file in a format Wireshark understands.

You are running Wireshark 3.6.5 (v3.6.5-0-g21f79ddbefbd). You receive automatic updates.

During the encryption, the ransomware might have corrupted the packet capture file. The file is rendered unreadable by Wireshark.

Treeliner

At last, treeliner will help us digest the information and present events that occurred in the host machine in an orderly and intelligible manner.



```
┌──(t433-student㉿T433-HuiNokHang-COMP4071)-[~/Documents/Tools/volatility3]
└─$ cat timeliner.txt | wc -l
328987

┌──(t433-student㉿T433-HuiNokHang-COMP4071)-[~/Documents/Tools/volatility3]
└─$ cat timeliner.txt
Volatility 3 Framework 2.4.0

Plugin  Description     Created Date     Modified Date    Accessed Date    Changed Date

MFTScan MFT FILE_NAME entry for         1601-01-01 00:00:02.000000      2022-01-20 19:50:12.000000      2022-01-20 19:50:12.000000      2022-01-20 19:50:12.0
00000
MFTScan MFT FILE_NAME entry for         1601-01-01 00:00:02.000000      2022-01-20 19:50:12.000000      2022-01-20 19:50:12.000000      2022-01-20 19:50:12.0
00000
MFTScan MFT FILE_NAME entry for         1601-01-01 00:00:02.000000      2022-01-20 19:50:21.000000      2022-01-20 19:50:21.000000      2022-01-20 19:50:21.0
00000
MFTScan MFT FILE_NAME entry for         1601-01-01 00:00:02.000000      2022-01-20 19:50:21.000000      2022-01-20 19:50:21.000000      -
MFTScan MFT FILE_NAME entry for         1601-01-01 00:00:02.000000      2022-01-20 19:51:11.000000      2022-01-20 19:51:11.000000      2022-01-20 19:51:11.0
00000
MFTScan MFT FILE_NAME entry for         1601-01-01 00:00:02.000000      N/A     2022-01-20 19:50:12.000000      2022-01-20 19:50:12.000000
MFTScan MFT FILE_NAME entry for         1601-01-01 00:00:02.000000      N/A     2022-01-20 19:50:12.000000      2022-01-20 19:50:12.000000
MFTScan MFT FILE_NAME entry for         1601-01-01 00:00:02.000000      N/A     2022-01-20 19:50:12.000000      N/A
MFTScan MFT FILE_NAME entry for         1601-01-01 00:00:02.000000      N/A     2022-01-20 19:50:12.000000      N/A
MFTScan MFT FILE_NAME entry for         1601-01-01 00:00:02.000000      N/A     2022-01-20 19:50:21.000000      2022-01-20 19:50:21.000000
MFTScan MFT FILE_NAME entry for         1601-01-01 00:00:02.000000      N/A     2022-01-20 19:50:21.000000      N/A
MFTScan MFT FILE_NAME entry for         1601-01-01 00:00:02.000000      N/A     2022-01-20 19:50:21.000000      -
MFTScan MFT FILE_NAME entry for         1601-01-01 00:00:02.000000      N/A     2022-01-20 19:50:21.000000      N/A
MFTScan MFT FILE_NAME entry for         1601-01-01 00:00:02.000000      N/A     2022-01-20 19:51:11.000000      2022-01-20 19:51:11.000000
MFTScan MFT FILE_NAME entry for         1601-01-01 00:00:02.000000      N/A     2022-01-20 19:51:11.000000      N/A
MFTScan MFT FILE_NAME entry for         1601-01-01 00:00:02.000000      N/A     N/A     N/A
MFTScan MFT FILE_NAME entry for         1601-01-01 00:00:02.000000      -       N/A     -
MFTScan MFT FILE_NAME entry for         1601-01-01 00:00:02.000000      N/A     N/A     -
MFTScan MFT FILE_NAME entry for         1601-01-01 00:00:02.000000      N/A     N/A     N/A
MFTScan MFT FILE_NAME entry for         1601-01-01 00:00:02.000000      N/A     N/A     N/A
MFTScan MFT FILE_NAME entry for         1601-01-01 00:00:02.000000      N/A     N/A     N/A
MFTScan MFT FILE_NAME entry for         1601-01-01 00:00:02.000000      N/A     N/A     N/A
MFTScan MFT FILE_NAME entry for         1601-01-01 00:00:02.000000      N/A     N/A     N/A
MFTScan MFT FILE_NAME entry for         1601-01-01 00:00:02.000000      N/A     N/A     N/A
MFTScan MFT FILE_NAME entry for         1601-01-01 00:00:02.000000      -       N/A     -
```

Since the file is very long (32k lines), in this section I would occasionally make use of grep to look through the file in an efficient manner.

First, I grepped java.exe, a file that I found previously suspicious in the netscan results as it communicated with the same public address multiple times during the malware process.

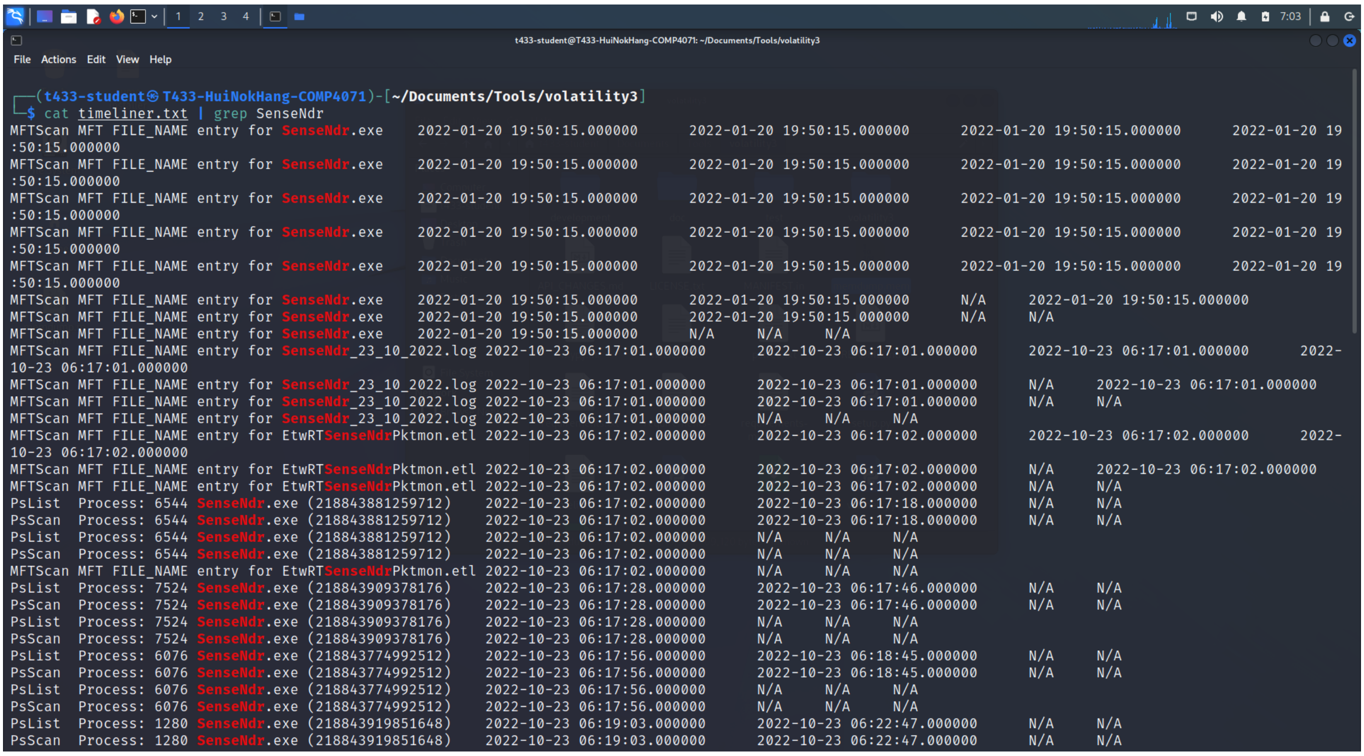
Turns out java.exe loaded multiple dlls into the host machine. This is very suspicious as these are library files that are often used to modify configurations.

```
:20:04.000000
MFTScan MFT FILE_NAME entry for java.exe        2022-10-23 06:20:04.000000      2022-10-23 06:19:27.000000      N/A     2022-10-23 06:20:04.000000
MFTScan MFT FILE_NAME entry for java.exe        2022-10-23 06:20:04.000000      2022-10-23 06:19:27.000000      N/A     N/A
MFTScan MFT FILE_NAME entry for java.exe        2022-10-23 06:20:04.000000      N/A     N/A     N/A
PsList  Process: 7972 java.exe (218843875623616)        2022-10-23 06:21:09.000000      N/A     N/A     N/A
PsList  Process: 7972 java.exe (218843875623616)        2022-10-23 06:21:09.000000      N/A     N/A     N/A
DllList DLL Load: Process 7972 java.exe Loaded java.exe (C:\Program Files\Sumo Logic Collector\jre\bin\java.exe) Size 237568 Offset 140695654694912     2022-
10-23 06:21:09.000000   N/A     N/A     N/A
DllList DLL Load: Process 7972 java.exe Loaded ntdll.dll (C:\Windows\SYSTEM32\ntdll.dll) Size 2052096 Offset 140725041168384    2022-10-23 06:21:09.000000  N
/A      N/A     N/A
DllList DLL Load: Process 7972 java.exe Loaded KERNEL32.DLL (C:\Windows\System32\KERNEL32.DLL) Size 774144 Offset 140725009776640       2022-10-23 06:21:09.0
00000   N/A     N/A     N/A
DllList DLL Load: Process 7972 java.exe Loaded KERNELBASE.dll (C:\Windows\System32\KERNELBASE.dll) Size 2916352 Offset 140724999815168  2022-10-23 06:21:09.0
00000   N/A     N/A     N/A
DllList DLL Load: Process 7972 java.exe Loaded ADVAPI32.dll (C:\Windows\System32\ADVAPI32.dll) Size 704512 Offset 140725040185344       2022-10-23 06:21:09.0
00000   N/A     N/A     N/A
DllList DLL Load: Process 7972 java.exe Loaded msvcrt.dll (C:\Windows\System32\msvcrt.dll) Size 647168 Offset 140725030027264   2022-10-23 06:21:09.000000  N
/A      N/A     N/A
DllList DLL Load: Process 7972 java.exe Loaded sechost.dll (C:\Windows\System32\sechost.dll) Size 634880 Offset 140725036253184 2022-10-23 06:21:09.000000  N
/A      N/A     N/A
DllList DLL Load: Process 7972 java.exe Loaded RPCRT4.dll (C:\Windows\System32\RPCRT4.dll) Size 1224704 Offset 140725037760512  2022-10-23 06:21:09.000000  N
/A      N/A     N/A
DllList DLL Load: Process 7972 java.exe Loaded USER32.dll (C:\Windows\System32\USER32.dll) Size 1703936 Offset 140725019475968  2022-10-23 06:21:09.000000  N
/A      N/A     N/A
DllList DLL Load: Process 7972 java.exe Loaded win32u.dll (C:\Windows\System32\win32u.dll) Size 139264 Offset 140725004533760   2022-10-23 06:21:09.000000  N
/A      N/A     N/A
DllList DLL Load: Process 7972 java.exe Loaded GDI32.dll (C:\Windows\System32\GDI32.dll) Size 172032 Offset 140725023604736     2022-10-23 06:21:09.000000  N
/A      N/A     N/A
DllList DLL Load: Process 7972 java.exe Loaded gdi32full.dll (C:\Windows\System32\gdi32full.dll) Size 1093632 Offset 140725004730368    2022-10-23 06:21:09.0
00000   N/A     N/A     N/A
DllList DLL Load: Process 7972 java.exe Loaded msvcp_win.dll (C:\Windows\System32\msvcp_win.dll) Size 643072 Offset 140724999159808     2022-10-23 06:21:09.0
00000   N/A     N/A     N/A
DllList DLL Load: Process 7972 java.exe Loaded ucrtbase.dll (C:\Windows\System32\ucrtbase.dll) Size 1048576 Offset 140725002764288      2022-10-23 06:21:09.0
00000   N/A     N/A     N/A
DllList DLL Load: Process 7972 java.exe Loaded COMCTL32.dll (C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.19041.844_none_ca
00b6081b84eb1d\COMCTL32.dll) Size 2727936 Offset 140724792524800        2022-10-23 06:21:09.000000      N/A     N/A     N/A
DllList DLL Load: Process 7972 java.exe Loaded msvcr120.dll (C:\Program Files\Sumo Logic Collector\jre\bin\msvcr120.dll) Size 978944 Offset 140724339277824 2
022-10-23 06:21:09.000000       N/A     N/A     N/A
DllList DLL Load: Process 7972 java.exe Loaded msvcp120.dll (C:\Program Files\Sumo Logic Collector\jre\bin\msvcp120.dll) Size 679936 Offset 140724699660288 2
022-10-23 06:21:09.000000       N/A     N/A     N/A
```

Conhosts.exe is also suspected of loading dlls into the system.

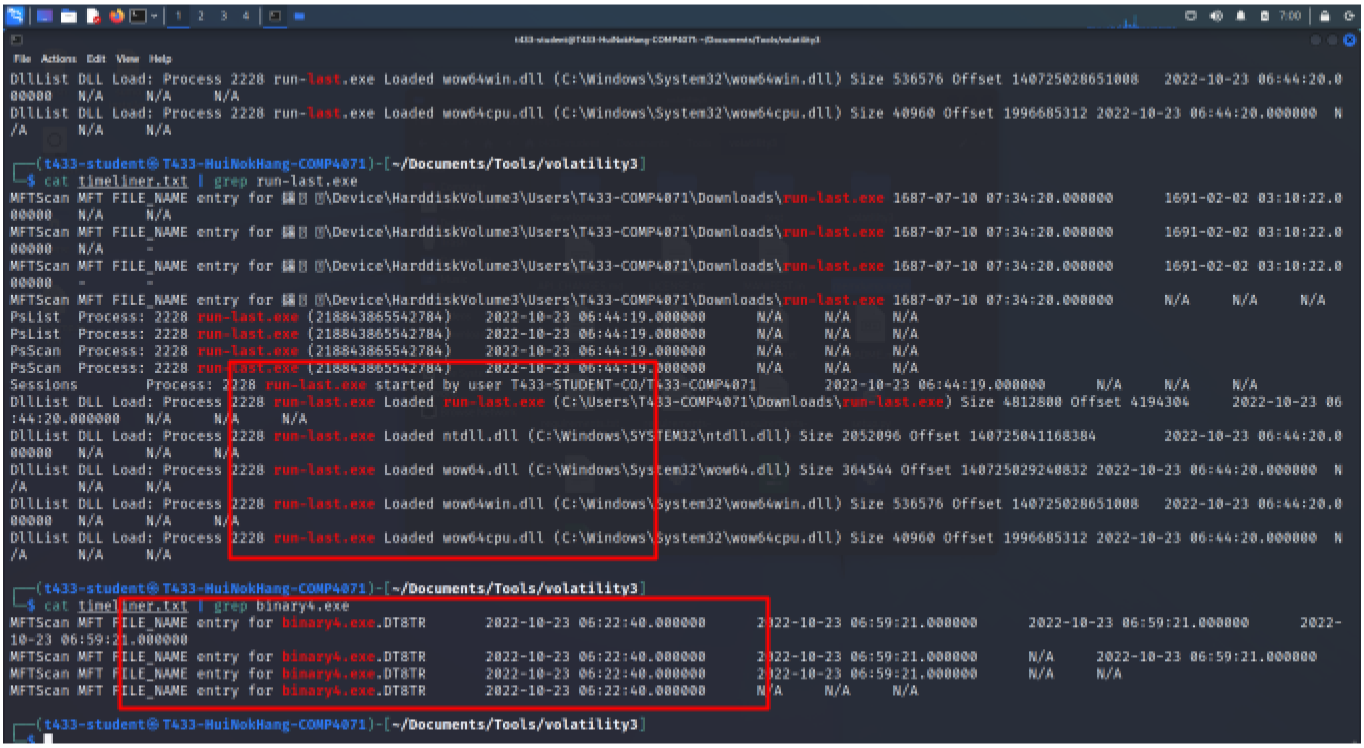
```
┌──(t433-student㉿T433-muiNokHang-COMP4071)-[~/Documents/Tools/volatility3]
└─$ cat timeliner.txt | grep conhost
MFTScan MFT FILE_NAME entry for conhost.exe     2022-01-20 19:50:35.000000      2022-01-20 19:50:35.000000      2022-01-20 19:50:35.000000      2022-01-20 19
:50:35.000000
MFTScan MFT FILE_NAME entry for conhost.exe     2022-01-20 19:50:35.000000      2022-01-20 19:50:35.000000      2022-01-20 19:50:35.000000      2022-01-20 19
:50:35.000000
MFTScan MFT FILE_NAME entry for conhost.exe     2022-01-20 19:50:35.000000      2022-01-20 19:50:35.000000      N/A     2022-01-20 19:50:35.000000
MFTScan MFT FILE_NAME entry for conhost.exe     2022-01-20 19:50:35.000000      2022-01-20 19:50:35.000000      N/A     N/A
MFTScan MFT FILE_NAME entry for conhost.exe     2022-01-20 19:50:35.000000      2022-01-20 19:50:37.000000      2022-01-20 19:50:35.000000      2022-01-20 19
:50:35.000000
MFTScan MFT FILE_NAME entry for conhost.exe     2022-01-20 19:50:35.000000      2022-01-20 19:50:37.000000      2022-01-20 19:50:35.000000      2022-01-20 19
:50:37.000000
MFTScan MFT FILE_NAME entry for conhost.exe     2022-01-20 19:50:35.000000      2022-01-20 19:50:37.000000      2022-01-20 19:50:35.000000      2022-01-20 19
:50:37.000000
MFTScan MFT FILE_NAME entry for conhost.exe     2022-01-20 19:50:35.000000      N/A     N/A     N/A
PsList  Process: 7024 conhost.exe (218843902997248)     2022-10-23 06:17:37.000000      N/A     N/A     N/A
PsList  Process: 7024 conhost.exe (218843902997248)     2022-10-23 06:17:37.000000      N/A     N/A     N/A
DllList DLL Load: Process 7024 conhost.exe Loaded conhost.exe (C:\Windows\system32\conhost.exe) Size 872448 Offset 140699858042880      2022-10-23 06:17:37.0
00000   N/A     N/A     N/A
DllList DLL Load: Process 7024 conhost.exe Loaded ntdll.dll (C:\Windows\SYSTEM32\ntdll.dll) Size 2052096 Offset 140725041168384 2022-10-23 06:17:37.000000  N
/A      N/A     N/A
DllList DLL Load: Process 7024 conhost.exe Loaded KERNEL32.DLL (C:\Windows\System32\KERNEL32.DLL) Size 774144 Offset 140725009776640    2022-10-23 06:17:37.0
00000   N/A     N/A     N/A
DllList DLL Load: Process 7024 conhost.exe Loaded KERNELBASE.dll (C:\Windows\System32\KERNELBASE.dll) Size 2916352 Offset 140724999815168       2022-10-23 06
:17:37.000000   N/A     N/A     N/A
DllList DLL Load: Process 7024 conhost.exe Loaded msvcp_win.dll (C:\Windows\System32\msvcp_win.dll) Size 643072 Offset 140724999159808  2022-10-23 06:17:37.0
00000   N/A     N/A     N/A
DllList DLL Load: Process 7024 conhost.exe Loaded ucrtbase.dll (C:\Windows\System32\ucrtbase.dll) Size 1048576 Offset 140725002764288   2022-10-23 06:17:37.0
00000   N/A     N/A     N/A
DllList DLL Load: Process 7024 conhost.exe Loaded shcore.dll (C:\Windows\System32\shcore.dll) Size 712704 Offset 140725036908544        2022-10-23 06:17:37.0
00000   N/A     N/A     N/A
DllList DLL Load: Process 7024 conhost.exe Loaded msvcrt.dll (C:\Windows\System32\msvcrt.dll) Size 647168 Offset 140725030027264        2022-10-23 06:17:37.0
00000   N/A     N/A     N/A
DllList DLL Load: Process 7024 conhost.exe Loaded combase.dll (C:\Windows\System32\combase.dll) Size 3493888 Offset 140725023801344     2022-10-23 06:17:37.0
00000   N/A     N/A     N/A
DllList DLL Load: Process 7024 conhost.exe Loaded RPCRT4.dll (C:\Windows\System32\RPCRT4.dll) Size 1224704 Offset 140725037760512       2022-10-23 06:17:37.0
00000   N/A     N/A     N/A
DllList DLL Load: Process 7024 conhost.exe Loaded advapi32.dll (C:\Windows\System32\advapi32.dll) Size 704512 Offset 140725040185344    2022-10-23 06:17:37.0
00000   N/A     N/A     N/A
```

However, some previously suspect processes like SenseNdr turns out to look clean.



```
┌──(t433-student㉿T433-HuiNokHang-COMP4071)-[~/Documents/Tools/volatility3]
└─$ cat timeliner.txt | grep SenseNdr
MFTScan MFT FILE_NAME entry for SenseNdr.exe    2022-01-20 19:50:15.000000      2022-01-20 19:50:15.000000      2022-01-20 19:50:15.000000      2022-01-20 19
:50:15.000000
MFTScan MFT FILE_NAME entry for SenseNdr.exe    2022-01-20 19:50:15.000000      2022-01-20 19:50:15.000000      2022-01-20 19:50:15.000000      2022-01-20 19
:50:15.000000
MFTScan MFT FILE_NAME entry for SenseNdr.exe    2022-01-20 19:50:15.000000      2022-01-20 19:50:15.000000      2022-01-20 19:50:15.000000      2022-01-20 19
:50:15.000000
MFTScan MFT FILE_NAME entry for SenseNdr.exe    2022-01-20 19:50:15.000000      2022-01-20 19:50:15.000000      2022-01-20 19:50:15.000000      2022-01-20 19
:50:15.000000
MFTScan MFT FILE_NAME entry for SenseNdr.exe    2022-01-20 19:50:15.000000      2022-01-20 19:50:15.000000      2022-01-20 19:50:15.000000      2022-01-20 19
:50:15.000000
MFTScan MFT FILE_NAME entry for SenseNdr.exe    2022-01-20 19:50:15.000000      2022-01-20 19:50:15.000000      N/A     2022-01-20 19:50:15.000000
MFTScan MFT FILE_NAME entry for SenseNdr.exe    2022-01-20 19:50:15.000000      2022-01-20 19:50:15.000000      N/A     N/A
MFTScan MFT FILE_NAME entry for SenseNdr.exe    2022-01-20 19:50:15.000000      N/A     N/A
MFTScan MFT FILE_NAME entry for SenseNdr_23_10_2022.log 2022-10-23 06:17:01.000000      2022-10-23 06:17:01.000000      2022-10-23 06:17:01.000000      2022-
10-23 06:17:01.000000
MFTScan MFT FILE_NAME entry for SenseNdr_23_10_2022.log 2022-10-23 06:17:01.000000      2022-10-23 06:17:01.000000      N/A     2022-10-23 06:17:01.000000
MFTScan MFT FILE_NAME entry for SenseNdr_23_10_2022.log 2022-10-23 06:17:01.000000      2022-10-23 06:17:01.000000      N/A     N/A
MFTScan MFT FILE_NAME entry for SenseNdr_23_10_2022.log 2022-10-23 06:17:01.000000      N/A     N/A     N/A
MFTScan MFT FILE_NAME entry for EtwRTSenseNdrPktmon.etl 2022-10-23 06:17:02.000000      2022-10-23 06:17:02.000000      2022-10-23 06:17:02.000000      2022-
10-23 06:17:02.000000
MFTScan MFT FILE_NAME entry for EtwRTSenseNdrPktmon.etl 2022-10-23 06:17:02.000000      2022-10-23 06:17:02.000000      N/A     2022-10-23 06:17:02.000000
MFTScan MFT FILE_NAME entry for EtwRTSenseNdrPktmon.etl 2022-10-23 06:17:02.000000      2022-10-23 06:17:02.000000      N/A     N/A
PsList  Process: 6544 SenseNdr.exe (218843881259712)    2022-10-23 06:17:02.000000      2022-10-23 06:17:18.000000      N/A     N/A
PsScan  Process: 6544 SenseNdr.exe (218843881259712)    2022-10-23 06:17:02.000000      2022-10-23 06:17:18.000000      N/A     N/A
PsList  Process: 6544 SenseNdr.exe (218843881259712)    2022-10-23 06:17:02.000000      N/A     N/A     N/A
PsScan  Process: 6544 SenseNdr.exe (218843881259712)    2022-10-23 06:17:02.000000      N/A     N/A     N/A
MFTScan MFT FILE_NAME entry for EtwRTSenseNdrPktmon.etl 2022-10-23 06:17:02.000000      N/A     N/A     N/A
PsList  Process: 7524 SenseNdr.exe (218843909378176)    2022-10-23 06:17:28.000000      2022-10-23 06:17:46.000000      N/A     N/A
PsScan  Process: 7524 SenseNdr.exe (218843909378176)    2022-10-23 06:17:28.000000      2022-10-23 06:17:46.000000      N/A     N/A
PsList  Process: 7524 SenseNdr.exe (218843909378176)    2022-10-23 06:17:28.000000      N/A     N/A     N/A
PsScan  Process: 7524 SenseNdr.exe (218843909378176)    2022-10-23 06:17:28.000000      N/A     N/A     N/A
PsList  Process: 6076 SenseNdr.exe (218843774992512)    2022-10-23 06:17:56.000000      2022-10-23 06:18:45.000000      N/A     N/A
PsScan  Process: 6076 SenseNdr.exe (218843774992512)    2022-10-23 06:17:56.000000      2022-10-23 06:18:45.000000      N/A     N/A
PsList  Process: 6076 SenseNdr.exe (218843774992512)    2022-10-23 06:17:56.000000      N/A     N/A     N/A
PsScan  Process: 6076 SenseNdr.exe (218843774992512)    2022-10-23 06:17:56.000000      N/A     N/A     N/A
PsList  Process: 1280 SenseNdr.exe (218843919851648)    2022-10-23 06:19:03.000000      2022-10-23 06:22:47.000000      N/A     N/A
PsScan  Process: 1280 SenseNdr.exe (218843919851648)    2022-10-23 06:19:03.000000      2022-10-23 06:22:47.000000      N/A     N/A
```

I then searched for run-last.exe and binary4.exe - the two malwares that were executed - and some traces can be found. They are caught loading dlls into the system. However, the list of records does not seem long. It is possible that the majority of their work is done by subsequent child processes rather than the main executable itself.



```
DllList DLL Load: Process 2228 run-last.exe Loaded wow64win.dll (C:\Windows\System32\wow64win.dll) Size 536576 Offset 140725028651008   2022-10-23 06:44:20.0
00000   N/A     N/A     N/A
DllList DLL Load: Process 2228 run-last.exe Loaded wow64cpu.dll (C:\Windows\System32\wow64cpu.dll) Size 40960 Offset 1996685312 2022-10-23 06:44:20.000000  N
/A      N/A     N/A

┌──(t433-student㉿T433-HuiNokHang-COMP4071)-[~/Documents/Tools/volatility3]
└─$ cat timeliner.txt | grep run-last.exe
MFTScan MFT FILE_NAME entry for ▦▯ ▯\Device\HarddiskVolume3\Users\T433-COMP4071\Downloads\run-last.exe 1687-07-10 07:34:20.000000      1691-02-02 03:18:22.0
00000   N/A     N/A
MFTScan MFT FILE_NAME entry for ▦▯ ▯\Device\HarddiskVolume3\Users\T433-COMP4071\Downloads\run-last.exe 1687-07-10 07:34:20.000000      1691-02-02 03:18:22.0
00000   N/A     -
MFTScan MFT FILE_NAME entry for ▦▯ ▯\Device\HarddiskVolume3\Users\T433-COMP4071\Downloads\run-last.exe 1687-07-10 07:34:20.000000      1691-02-02 03:18:22.0
00000   -       -
MFTScan MFT FILE_NAME entry for ▦▯ ▯\Device\HarddiskVolume3\Users\T433-COMP4071\Downloads\run-last.exe 1687-07-10 07:34:20.000000      N/A     N/A     N/A
PsList  Process: 2228 run-last.exe (218843865542784)    2022-10-23 06:44:19.000000      N/A     N/A     N/A
PsList  Process: 2228 run-last.exe (218843865542784)    2022-10-23 06:44:19.000000      N/A     N/A     N/A
PsScan  Process: 2228 run-last.exe (218843865542784)    2022-10-23 06:44:19.000000      N/A     N/A     N/A
PsScan  Process: 2228 run-last.exe (218843865542784)    2022-10-23 06:44:19.000000      N/A     N/A     N/A
Sessions        Process: 2228 run-last.exe started by user T433-STUDENT-CO/T433-COMP4071        2022-10-23 06:44:19.000000      N/A     N/A     N/A
DllList DLL Load: Process 2228 run-last.exe Loaded run-last.exe (C:\Users\T433-COMP4071\Downloads\run-last.exe) Size 4812800 Offset 4194304     2022-10-23 06
:44:20.000000   N/A     N/A     N/A
DllList DLL Load: Process 2228 run-last.exe Loaded ntdll.dll (C:\Windows\SYSTEM32\ntdll.dll) Size 2052096 Offset 140725041168384        2022-10-23 06:44:20.0
00000   N/A     N/A     N/A
DllList DLL Load: Process 2228 run-last.exe Loaded wow64.dll (C:\Windows\System32\wow64.dll) Size 364544 Offset 140725029240832 2022-10-23 06:44:20.000000  N
/A      N/A     N/A
DllList DLL Load: Process 2228 run-last.exe Loaded wow64win.dll (C:\Windows\System32\wow64win.dll) Size 536576 Offset 140725028651008   2022-10-23 06:44:20.0
00000   N/A     N/A     N/A
DllList DLL Load: Process 2228 run-last.exe Loaded wow64cpu.dll (C:\Windows\System32\wow64cpu.dll) Size 40960 Offset 1996685312 2022-10-23 06:44:20.000000  N
/A      N/A     N/A

┌──(t433-student㉿T433-HuiNokHang-COMP4071)-[~/Documents/Tools/volatility3]
└─$ cat timeliner.txt | grep binary4.exe
MFTScan MFT FILE_NAME entry for binary4.exe.DT8TR       2022-10-23 06:22:40.000000      2022-10-23 06:59:21.000000      2022-10-23 06:59:21.000000      2022-
10-23 06:59:21.000000
MFTScan MFT FILE_NAME entry for binary4.exe.DT8TR       2022-10-23 06:22:40.000000      2022-10-23 06:59:21.000000      N/A     2022-10-23 06:59:21.000000
MFTScan MFT FILE_NAME entry for binary4.exe.DT8TR       2022-10-23 06:22:40.000000      2022-10-23 06:59:21.000000      N/A     N/A
MFTScan MFT FILE_NAME entry for binary4.exe.DT8TR       2022-10-23 06:22:40.000000      N/A     N/A     N/A

┌──(t433-student㉿T433-HuiNokHang-COMP4071)-[~/Documents/Tools/volatility3]
└─$ 
```

Here we can see traces of encryption at the tail end of the timeliner result. The file names have been modified to the point of unreadability which is the work of encryption. We can also directly see the CIPHER running.

```
t433-student@T433-HuiNokHang-COMP407t: ~/Documents/Tools/volatility3
File  Actions  Edit  View  Help
MFTScan MFT FILE_NAME entry for 哆□□   -       -       N/A     -
MFTScan MFT FILE_NAME entry for 哆□□   -       -       -       -
MFTScan MFT FILE_NAME entry for 唛□□   -       N/A     N/A     N/A
MFTScan MFT FILE_NAME entry for 唛□□   -       -       N/A     N/A
MFTScan MFT FILE_NAME entry for 唛□□   -       -       N/A     -
MFTScan MFT FILE_NAME entry for 唛□□   -       -       -       -
MFTScan MFT FILE_NAME entry for 瓥□□   -       N/A     N/A     N/A
MFTScan MFT FILE_NAME entry for 瓥□□   -       -       N/A     N/A
MFTScan MFT FILE_NAME entry for 瓥□□   -       -       N/A     -
MFTScan MFT FILE_NAME entry for 瓥□□   -       -       -       -
MFTScan MFT FILE_NAME entry for 喝□□   -       N/A     N/A     N/A
MFTScan MFT FILE_NAME entry for 喝□□   -       -       N/A     N/A
MFTScan MFT FILE_NAME entry for 喝□□   -       -       N/A     -
MFTScan MFT FILE_NAME entry for 喝□□   -       -       -       -
MFTScan MFT FILE_NAME entry for        -       -       -       -
MFTScan MFT FILE_NAME entry for        -       -       N/A     -
MFTScan MFT FILE_NAME entry for 嬢□□   -       N/A     N/A     N/A
MFTScan MFT FILE_NAME entry for 嬢□□   -       -       N/A     N/A
MFTScan MFT FILE_NAME entry for 嬢□□   -       -       N/A     -
MFTScan MFT FILE_NAME entry for 嬢□□   -       -       -       -
MFTScan MFT FILE_NAME entry for 蟋□□   -       N/A     N/A     N/A
MFTScan MFT FILE_NAME entry for 蟋□□   -       -       N/A     N/A
MFTScan MFT FILE_NAME entry for 蟋□□   -       -       N/A     -
MFTScan MFT FILE_NAME entry for 蟋□□   -       -       -       -
MFTScan MFT FILE_NAME entry for 蟋□□   -       N/A     N/A     N/A
MFTScan MFT FILE_NAME entry for 蟋□□   -       -       N/A     N/A
MFTScan MFT FILE_NAME entry for 蟋□□   -       -       N/A     -
MFTScan MFT FILE_NAME entry for 蟋□□   -       -       -       -
MFTScan MFT FILE_NAME entry for 蟋□□   -       -       -       -
MFTScan MFT FILE_NAME entry for 蟋□□   -       -       -       -
MFTScan MFT FILE_NAME entry for 蟋□□   -       -       -       -
MFTScan MFT FILE_NAME entry for 蟋□□   -       -       -       -
MFTScan MFT FILE_NAME entry for 蟋□□   -       -       -       -
MFTScan MFT FILE_NAME entry for 蟋□□   -       -       -       -
MFTScan MFT FILE_NAME entry for        N/A     N/A     N/A     N/A
MFTScan MFT FILE_NAME entry for        N/A     N/A     N/A     N/A
MFTScan MFT FILE_NAME entry for 閘□□□ 閘□□   -       N/A     N/A     N/A
MFTScan MFT FILE_NAME entry for        N/A     N/A     -       N/A
```

```
t433-student@T433-HuiNokHang-COMP407t: ~/Documents/Tools/volatility3
File  Actions  Edit  View  Help
10-23 06:59:46.000000
MFTScan MFT FILE_NAME entry for CIPHER.EXE-362AFD68.pf  2022-10-23 06:59:46.000000  2022-10-23 06:59:46.000000  2022-10-23 06:59:46.000000  2022-
10-23 06:59:46.000000
MFTScan MFT FILE_NAME entry for CIPHER.EXE-362AFD68.pf  2022-10-23 06:59:46.000000  2022-10-23 06:59:46.000000  2022-10-23 06:59:46.000000  2022-
10-23 06:59:46.000000
MFTScan MFT FILE_NAME entry for CIPHER.EXE-362AFD68.pf  2022-10-23 06:59:46.000000  2022-10-23 06:59:46.000000  2022-10-23 06:59:46.000000  2022-
10-23 06:59:46.000000
MFTScan MFT FILE_NAME entry for CIPHER~1.PF  2022-10-23 06:59:46.000000  2022-10-23 06:59:46.000000  2022-10-23 06:59:46.000000  2022-10-23 06
:59:46.000000
MFTScan MFT FILE_NAME entry for CIPHER~1.PF  2022-10-23 06:59:46.000000  2022-10-23 06:59:46.000000  2022-10-23 06:59:46.000000  2022-10-23 06
:59:46.000000
MFTScan MFT FILE_NAME entry for CIPHER~1.PF  2022-10-23 06:59:46.000000  2022-10-23 06:59:46.000000  2022-10-23 06:59:46.000000  2022-10-23 06
:59:46.000000
MFTScan MFT FILE_NAME entry for CIPHER~1.PF  2022-10-23 06:59:46.000000  2022-10-23 06:59:46.000000  2022-10-23 06:59:46.000000  2022-10-23 06
:59:46.000000
MFTScan MFT FILE_NAME entry for CIPHER.EXE-362AFD68.pf  2022-10-23 06:59:46.000000  2022-10-23 06:59:46.000000  2022-10-23 06:59:46.000000  2022-
10-23 06:59:46.000000
MFTScan MFT FILE_NAME entry for CIPHER.EXE-362AFD68.pf  2022-10-23 06:59:46.000000  2022-10-23 06:59:46.000000  2022-10-23 06:59:46.000000  2022-
10-23 06:59:46.000000
MFTScan MFT FILE_NAME entry for CIPHER.EXE-362AFD68.pf  2022-10-23 06:59:46.000000  2022-10-23 06:59:46.000000  2022-10-23 06:59:46.000000  2022-
10-23 06:59:46.000000
MFTScan MFT FILE_NAME entry for CIPHER.EXE-362AFD68.pf  2022-10-23 06:59:46.000000  2022-10-23 06:59:46.000000  2022-10-23 06:59:46.000000  2022-
10-23 06:59:46.000000
MFTScan MFT FILE_NAME entry for CIPHER~1.PF  2022-10-23 06:59:46.000000  2022-10-23 06:59:46.000000  N/A  2022-10-23 06:59:46.000000
MFTScan MFT FILE_NAME entry for CIPHER.EXE-362AFD68.pf  2022-10-23 06:59:46.000000  2022-10-23 06:59:46.000000  N/A  2022-10-23 06:59:46.000000
MFTScan MFT FILE_NAME entry for CIPHER~1.PF  2022-10-23 06:59:46.000000  2022-10-23 06:59:46.000000  N/A  N/A
MFTScan MFT FILE_NAME entry for CIPHER.EXE-362AFD68.pf  2022-10-23 06:59:46.000000  2022-10-23 06:59:46.000000  N/A  N/A
MFTScan MFT FILE_NAME entry for CIPHER~1.PF  2022-10-23 06:59:46.000000  N/A  N/A  N/A
MFTScan MFT FILE_NAME entry for CIPHER.EXE-362AFD68.pf  2022-10-23 06:59:46.000000  N/A  N/A  N/A
MFTScan MFT FILE_NAME entry for fil22F2.tmp  2022-10-23 06:59:56.000000  2022-10-23 06:59:56.000000  2022-10-23 06:59:56.000000  2022-10-23 06
:59:56.000000
MFTScan MFT FILE_NAME entry for 1.E  2022-10-23 06:59:56.000000  2022-10-23 06:59:56.000000  2022-10-23 06:59:56.000000  2022-10-23 06:59:56.0
00000
MFTScan MFT FILE_NAME entry for fil22F2.tmp  2022-10-23 06:59:56.000000  2022-10-23 06:59:56.000000  N/A  2022-10-23 06:59:56.000000
MFTScan MFT FILE_NAME entry for 1.E  2022-10-23 06:59:56.000000  2022-10-23 06:59:56.000000  N/A  2022-10-23 06:59:56.000000
MFTScan MFT FILE_NAME entry for fil22F2.tmp  2022-10-23 06:59:56.000000  2022-10-23 06:59:56.000000  N/A  N/A
MFTScan MFT FILE_NAME entry for 1.E  2022-10-23 06:59:56.000000  2022-10-23 06:59:56.000000  N/A  N/A
MFTScan MFT FILE_NAME entry for fil22F2.tmp  2022-10-23 06:59:56.000000  N/A  N/A  N/A
MFTScan MFT FILE_NAME entry for 1.E  2022-10-23 06:59:56.000000  N/A  N/A  N/A
MFTScan MFT FILE_NAME entry for MALWAR~1.PCA  2022-10-23 07:00:31.000000  2022-10-23 07:00:31.000000  2022-10-23 07:00:31.000000  2022-10-23 07
```

Cmd.exe was called multiple times for various purposes. It is seen that it loads dll into the system32 folder.

```
File  Actions  Edit  View  Help
PsList  Process: 6956 cmd.exe (218843901714560) 2022-10-23 06:17:37.000000      N/A     N/A     N/A
PsList  Process: 6956 cmd.exe (218843901714560) 2022-10-23 06:17:37.000000      N/A     N/A     N/A
DllList DLL Load: Process 6956 cmd.exe Loaded cmd.exe (C:\Windows\system32\cmd.exe) Size 421888 Offset 140696711462912  2022-10-23 06:17:37.000000      N/A N
/A      N/A
DllList DLL Load: Process 6956 cmd.exe Loaded ntdll.dll (C:\Windows\SYSTEM32\ntdll.dll) Size 2052096 Offset 140725041168384     2022-10-23 06:17:37.000000  N
/A      N/A     N/A
DllList DLL Load: Process 6956 cmd.exe Loaded KERNEL32.DLL (C:\Windows\System32\KERNEL32.DLL) Size 774144 Offset 140725009776640        2022-10-23 06:17:37.0
00000   N/A     N/A     N/A
DllList DLL Load: Process 6956 cmd.exe Loaded KERNELBASE.dll (C:\Windows\System32\KERNELBASE.dll) Size 2916352 Offset 140724999815168   2022-10-23 06:17:37.0
00000   N/A     N/A     N/A
DllList DLL Load: Process 6956 cmd.exe Loaded msvcrt.dll (C:\Windows\System32\msvcrt.dll) Size 647168 Offset 140725030027264    2022-10-23 06:17:37.000000  N
/A      N/A     N/A
DllList DLL Load: Process 6956 cmd.exe Loaded combase.dll (C:\Windows\System32\combase.dll) Size 3493888 Offset 140725023801344 2022-10-23 06:17:37.000000  N
/A      N/A     N/A
DllList DLL Load: Process 6956 cmd.exe Loaded ucrtbase.dll (C:\Windows\System32\ucrtbase.dll) Size 1048576 Offset 140725002764288       2022-10-23 06:17:37.0
00000   N/A     N/A     N/A
DllList DLL Load: Process 6956 cmd.exe Loaded RPCRT4.dll (C:\Windows\System32\RPCRT4.dll) Size 1224704 Offset 140725037760512   2022-10-23 06:17:37.000000  N
/A      N/A     N/A
DllList DLL Load: Process 6956 cmd.exe Loaded winbrand.dll (C:\Windows\SYSTEM32\winbrand.dll) Size 217088 Offset 140724723974144        2022-10-23 06:17:37.0
00000   N/A     N/A     N/A
PsScan  Process: 6956 cmd.exe (218843901714560) 2022-10-23 06:17:37.000000      N/A     N/A     N/A
PsScan  Process: 6956 cmd.exe (218843901714560) 2022-10-23 06:17:37.000000      N/A     N/A     N/A
PsList  Process: 632 cmd.exe (218843860725888)  2022-10-23 06:59:36.000000      N/A     N/A     N/A
PsList  Process: 632 cmd.exe (218843860725888)  2022-10-23 06:59:36.000000      N/A     N/A     N/A
DllList DLL Load: Process 632 cmd.exe Loaded cmd.exe (C:\Windows\SysWOW64\cmd.exe) Size 368640 Offset 10682368  2022-10-23 06:59:36.000000      N/A     N/A N
/A
DllList DLL Load: Process 632 cmd.exe Loaded ntdll.dll (C:\Windows\SYSTEM32\ntdll.dll) Size 2052096 Offset 140725041168384      2022-10-23 06:59:36.000000  N
/A      N/A     N/A
DllList DLL Load: Process 632 cmd.exe Loaded wow64.dll (C:\Windows\System32\wow64.dll) Size 364544 Offset 140725029240832       2022-10-23 06:59:36.000000  N
/A      N/A     N/A
DllList DLL Load: Process 632 cmd.exe Loaded wow64win.dll (C:\Windows\System32\wow64win.dll) Size 536576 Offset 140725028651008 2022-10-23 06:59:36.000000  N
/A      N/A     N/A
DllList DLL Load: Process 632 cmd.exe Loaded wow64cpu.dll (C:\Windows\System32\wow64cpu.dll) Size 40960 Offset 1996685312       2022-10-23 06:59:36.000000  N
/A      N/A     N/A
PsScan  Process: 632 cmd.exe (218843860725888)  2022-10-23 06:59:36.000000      N/A     N/A     N/A
PsScan  Process: 632 cmd.exe (218843860725888)  2022-10-23 06:59:36.000000      N/A     N/A     N/A
Sessions        Process: 632 cmd.exe started by user T433-STUDENT-CO/T433-COMP4071      2022-10-23 06:59:36.000000      N/A     N/A     N/A

┌──(t433-student㉿T433-HuiNokHang-COMP4071)-[~/Documents/Tools/volatility3]
└─$
```