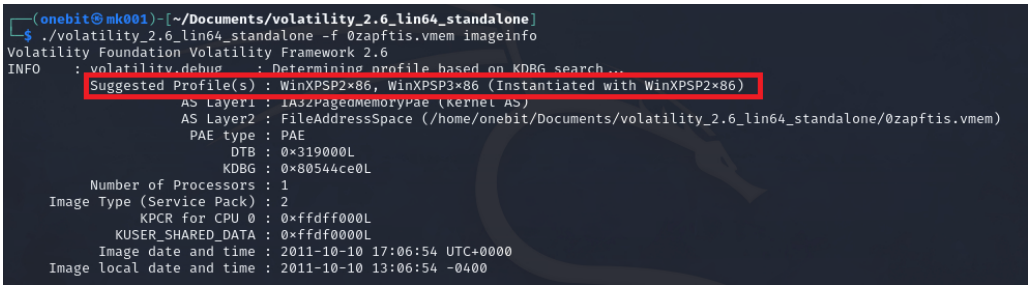
Matthew Kurniawan - 2540124702

Benedicto Marvelous - 2540125384

John Orlond - 2540118933

Step 1

Command	./volatility -f [file name] imageinfo
Image	
Output	 From the output we can conclude that the memory is a Windows XP sample with profile **WinXPSP2x*6, WinXPSP3x86**

After finding out the image info of the memory, we continue our investigation by checking all the active processes while the dump was captured.

Step 2

Command	python3 vol.py -f ../0zapftis.vmem windows.pslist

Image	

```
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0x819cc830      55      162     N/A     False   N/A     N/A     Disabled
536     4       smss.exe        0x81945020      3       21      N/A     False   2011-10-10 17:03:56.000000      N/A     Disabled
608     536     csrss.exe       0x816c6020      11      355     0       False   2011-10-10 17:03:58.000000      N/A     Disabled
632     536     winlogon.exe    0x813a9020      24      533     0       False   2011-10-10 17:03:58.000000      N/A     Disabled
676     632     services.exe    0x816da020      16      261     0       False   2011-10-10 17:03:58.000000      N/A     Disabled
688     632     lsass.exe       0x813c4020      23      336     0       False   2011-10-10 17:03:58.000000      N/A     Disabled
832     676     vmacthlp.exe    0x81772ca8      1       24      0       False   2011-10-10 17:03:59.000000      N/A     Disabled
848     676     svchost.exe     0x8167e9d0      20      194     0       False   2011-10-10 17:03:59.000000      N/A     Disabled
916     676     svchost.exe     0x817757f0      9       217     0       False   2011-10-10 17:03:59.000000      N/A     Disabled
964     676     svchost.exe     0x816c6da0      63      1058    0       False   2011-10-10 17:03:59.000000      N/A     Disabled
1020    676     svchost.exe     0x815daca8      5       58      0       False   2011-10-10 17:03:59.000000      N/A     Disabled
1148    676     svchost.exe     0x813aeda0      12      187     0       False   2011-10-10 17:04:00.000000      N/A     Disabled
1260    676     spoolsv.exe     0x817937e0      13      140     0       False   2011-10-10 17:04:00.000000      N/A     Disabled
1444    676     VMwareService.e 0x81754990      3       145     0       False   2011-10-10 17:04:00.000000      N/A     Disabled
1616    676     alg.exe 0x8136c5a0      7       99      0       False   2011-10-10 17:04:01.000000      N/A     Disabled
1920    964     wscntfy.exe     0x815c4da0      1       27      0       False   2011-10-10 17:04:39.000000      N/A     Disabled
1956    1884    explorer.exe    0x813bcda0      18      322     0       False   2011-10-10 17:04:39.000000      N/A     Disabled
184     1956    VMwareTray.exe  0x816d63d0      1       28      0       False   2011-10-10 17:04:41.000000      N/A     Disabled
192     1956    VMwareUser.exe  0x8180b478      6       83      0       False   2011-10-10 17:04:41.000000      N/A     Disabled
228     1956    reader_sl.exe   0x818233c8      2       26      0       False   2011-10-10 17:04:41.000000      N/A     Disabled
400     964     wuauclt.exe     0x815e7be0      8       173     0       False   2011-10-10 17:04:46.000000      N/A     Disabled
544     1956    cmd.exe 0x817a34b0      1       30      0       False   2011-10-10 17:06:42.000000      N/A     Disabled
```

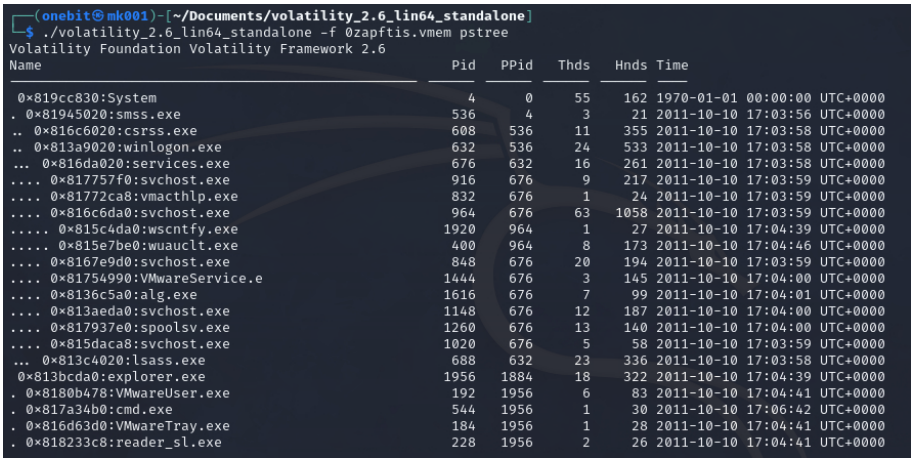
Output	With this command we are able to see many active processes along with their PID, PPID, their start time, and so on.

After finding out all the active processes, we decided to look at all the parent-child processes by using “pstree”

Step 3

Command	./volatility -f [file name] pstree
Image	

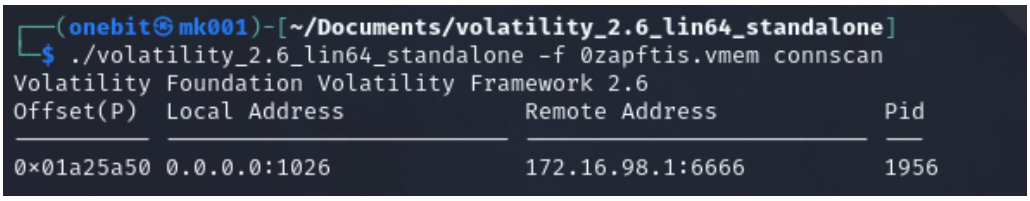
```
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime

4       0       System  0x819cc830      55      162     N/A     False   N/A     N/A
* 536   4       smss.exe        0x81945020      3       21      N/A     False   2011-10-10 17:03:56.000000      N/A
** 608  536     csrss.exe       0x816c6020      11      355     0       False   2011-10-10 17:03:58.000000      N/A
** 632  536     winlogon.exe    0x813a9020      24      533     0       False   2011-10-10 17:03:58.000000      N/A
*** 688 632     lsass.exe       0x813c4020      23      336     0       False   2011-10-10 17:03:58.000000      N/A
*** 676 632     services.exe    0x816da020      16      261     0       False   2011-10-10 17:03:58.000000      N/A
**** 832        676     vmacthlp.exe    0x81772ca8      1       24      0       False   2011-10-10 17:03:59.000000      N/A
**** 964        676     svchost.exe     0x816c6da0      63      1058    0       False   2011-10-10 17:03:59.000000      N/A
***** 1920       964     wscntfy.exe     0x815c4da0      1       27      0       False   2011-10-10 17:04:39.000000      N/A
***** 400        964     wuauclt.exe     0x815e7be0      8       173     0       False   2011-10-10 17:04:46.000000      N/A
**** 1444       676     VMwareService.e 0x81754990      3       145     0       False   2011-10-10 17:04:00.000000      N/A
**** 1260       676     spoolsv.exe     0x817937e0      13      140     0       False   2011-10-10 17:04:00.000000      N/A
**** 848        676     svchost.exe     0x8167e9d0      20      194     0       False   2011-10-10 17:03:59.000000      N/A
**** 1148       676     svchost.exe     0x813aeda0      12      187     0       False   2011-10-10 17:04:00.000000      N/A
**** 1616       676     alg.exe 0x8136c5a0      7       99      0       False   2011-10-10 17:04:01.000000      N/A
**** 916        676     svchost.exe     0x817757f0      9       217     0       False   2011-10-10 17:03:59.000000      N/A
**** 1020       676     svchost.exe     0x815daca8      5       58      0       False   2011-10-10 17:03:59.000000      N/A
1956    1884    explorer.exe    0x813bcda0      18      322     0       False   2011-10-10 17:04:39.000000      N/A
* 184   1956    VMwareTray.exe  0x816d63d0      1       28      0       False   2011-10-10 17:04:41.000000      N/A
* 544   1956    cmd.exe 0x817a34b0      1       30      0       False   2011-10-10 17:06:42.000000      N/A
* 228   1956    reader_sl.exe   0x818233c8      2       26      0       False   2011-10-10 17:04:41.000000      N/A
* 192   1956    VMwareUser.exe  0x8180b478      6       83      0       False   2011-10-10 17:04:41.000000      N/A
```

Output	 By looking at the output, we are able to see some suspicion based on the PPid of explorer.exe processes like cmd.exe, VMwareUser.exe, VMwareTray.exe and reader_sl.exe.

```
┌──(onebit㉿mk001)-[~/Documents/volatility_2.6_lin64_standalone]
└─$ ./volatility_2.6_lin64_standalone -f 0zapftis.vmem pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x819cc830:System                                      4      0     55    162 1970-01-01 00:00:00 UTC+0000
. 0x81945020:smss.exe                                 536      4      3     21 2011-10-10 17:03:56 UTC+0000
.. 0x816c6020:csrss.exe                               608    536     11    355 2011-10-10 17:03:58 UTC+0000
.. 0x813a9020:winlogon.exe                            632    536     24    533 2011-10-10 17:03:58 UTC+0000
... 0x816da020:services.exe                           676    632     16    261 2011-10-10 17:03:58 UTC+0000
.... 0x817757f0:svchost.exe                           916    676      9    217 2011-10-10 17:03:59 UTC+0000
.... 0x81772ca8:vmacthlp.exe                          832    676      1     24 2011-10-10 17:03:59 UTC+0000
.... 0x816c6da0:svchost.exe                           964    676     63   1058 2011-10-10 17:03:59 UTC+0000
..... 0x815c4da0:wscntfy.exe                         1920    964      1     27 2011-10-10 17:04:39 UTC+0000
..... 0x815e7be0:wuauclt.exe                          400    964      8    173 2011-10-10 17:04:46 UTC+0000
.... 0x8167e9d0:svchost.exe                           848    676     20    194 2011-10-10 17:03:59 UTC+0000
.... 0x81754990:VMwareService.e                      1444    676      3    145 2011-10-10 17:04:00 UTC+0000
.... 0x8136c5a0:alg.exe                              1616    676      7     99 2011-10-10 17:04:01 UTC+0000
.... 0x813aeda0:svchost.exe                          1148    676     12    187 2011-10-10 17:04:00 UTC+0000
.... 0x817937e0:spoolsv.exe                          1260    676     13    140 2011-10-10 17:04:00 UTC+0000
.... 0x815daca8:svchost.exe                          1020    676      5     58 2011-10-10 17:03:59 UTC+0000
... 0x813c4020:lsass.exe                              688    632     23    336 2011-10-10 17:03:58 UTC+0000
 0x813bcda0:explorer.exe                             1956   1884     18    322 2011-10-10 17:04:39 UTC+0000
. 0x8180b478:VMwareUser.exe                           192   1956      6     83 2011-10-10 17:04:41 UTC+0000
. 0x817a34b0:cmd.exe                                  544   1956      1     30 2011-10-10 17:06:42 UTC+0000
. 0x816d63d0:VMwareTray.exe                           184   1956      1     28 2011-10-10 17:04:41 UTC+0000
. 0x818233c8:reader_sl.exe                            228   1956      2     26 2011-10-10 17:04:41 UTC+0000
```

After that we decided to look at the connection dump to see if there is any connection made

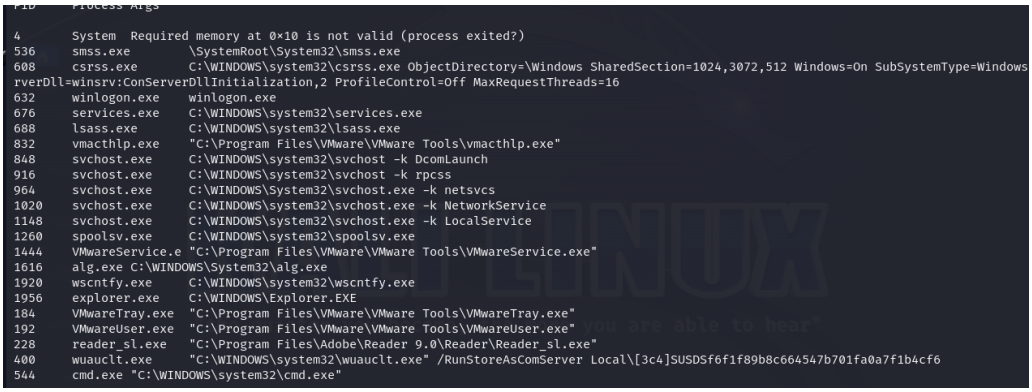
Step 4

Command	./volatility -f [file name] connscan
Image	
Description	The command ***./volatility -f [file name] connscan*** is used to scan for network connections in a memory dump file. The benefit of this command is it can help identify any potential security threats or malware on the system.
Output	We can see that there are some connection processes made, and the prosces with Pid 1956 made some connection outside

```
┌──(onebit㉿mk001)-[~/Documents/volatility_2.6_lin64_standalone]
└─$ ./volatility_2.6_lin64_standalone -f 0zapftis.vmem connscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- -------------------------- -------------------------- ---
0x01a25a50 0.0.0.0:1026              172.16.98.1:6666          1956
```

After this we decided to see the command line argument from the memory dump file by using cmdscan

Step 6

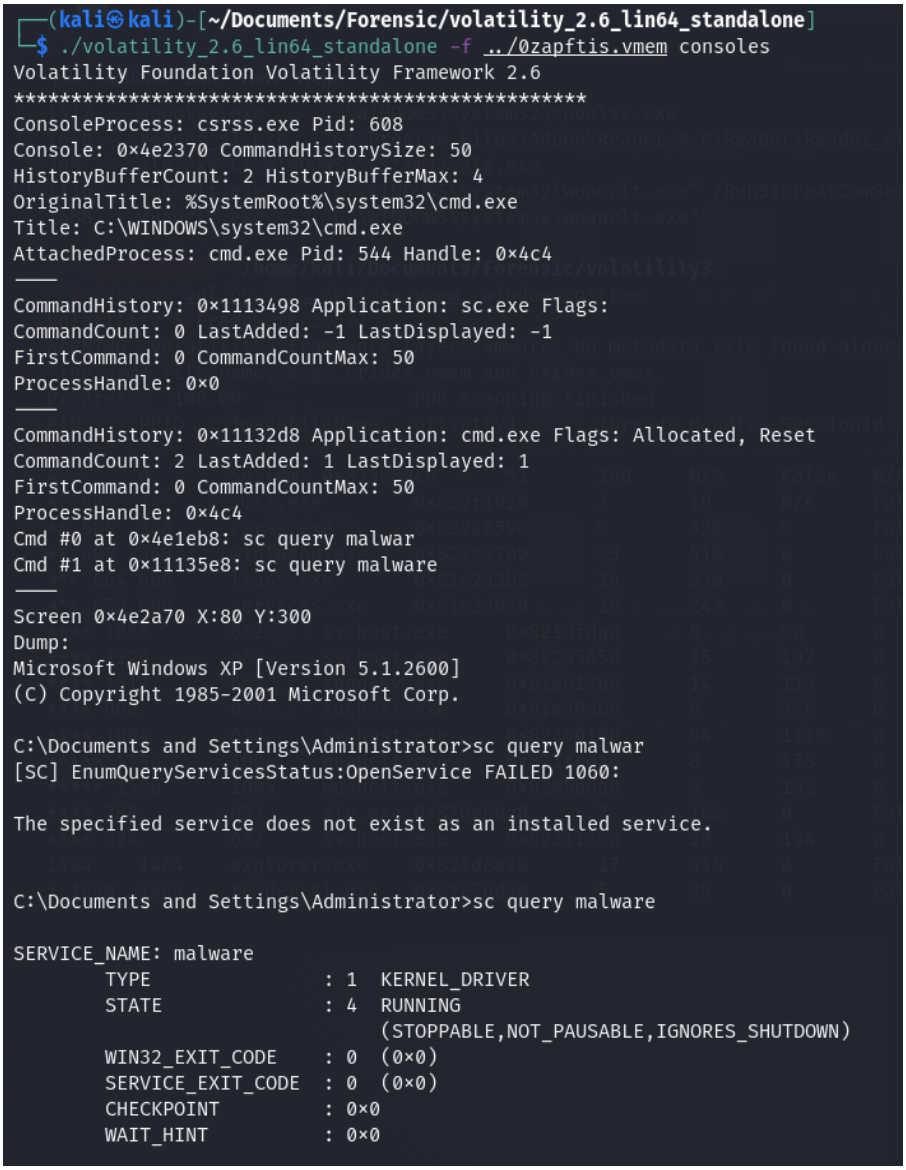
Command	./volatility -f [file name] cmdscan
Image	
Output	e are able to see that the process csrss.exe ran some commands on the cmd

```
PID     Process Args

4       System  Required memory at 0×10 is not valid (process exited?)
536     smss.exe        \SystemRoot\System32\smss.exe
608     csrss.exe       C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072,512 Windows=On SubSystemType=Windows
rverDll=winsrv:ConServerDllInitialization,2 ProfileControl=Off MaxRequestThreads=16
632     winlogon.exe    winlogon.exe
676     services.exe    C:\WINDOWS\system32\services.exe
688     lsass.exe       C:\WINDOWS\system32\lsass.exe
832     vmacthlp.exe    "C:\Program Files\VMware\VMware Tools\vmacthlp.exe"
848     svchost.exe     C:\WINDOWS\system32\svchost -k DcomLaunch
916     svchost.exe     C:\WINDOWS\system32\svchost -k rpcss
964     svchost.exe     C:\WINDOWS\System32\svchost.exe -k netsvcs
1020    svchost.exe     C:\WINDOWS\system32\svchost.exe -k NetworkService
1148    svchost.exe     C:\WINDOWS\system32\svchost.exe -k LocalService
1260    spoolsv.exe     C:\WINDOWS\system32\spoolsv.exe
1444    VMwareService.e "C:\Program Files\VMware\VMware Tools\VMwareService.exe"
1616    alg.exe C:\WINDOWS\System32\alg.exe
1920    wscntfy.exe     C:\WINDOWS\system32\wscntfy.exe
1956    explorer.exe    C:\WINDOWS\Explorer.EXE
184     VMwareTray.exe  "C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
192     VMwareUser.exe  "C:\Program Files\VMware\VMware Tools\VMwareUser.exe"
228     reader_sl.exe   "C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe"
400     wuauclt.exe     "C:\WINDOWS\system32\wuauclt.exe" /RunStoreAsComServer Local\[3c4]SUSDSf6f1f89b8c664547b701fa0a7f1b4cf6
544     cmd.exe "C:\WINDOWS\system32\cmd.exe"
```

After this we decided to run the command consoles to gain more information.

Step 7

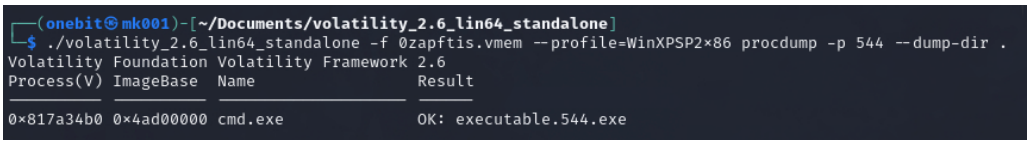
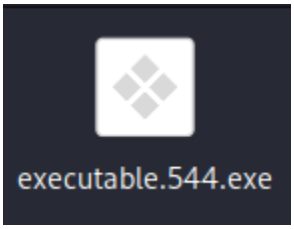
Command	./volatility -f [file name] consoles

Image	 (kali㉿kali)-[~/Documents/Forensic/volatility_2.6_lin64_standalone] $ ./volatility_2.6_lin64_standalone -f ../0zapftis.vmem consoles Volatility Foundation Volatility Framework 2.6 ********** ConsoleProcess: csrss.exe Pid: 608 Console: 0×4e2370 CommandHistorySize: 50 HistoryBufferCount: 2 HistoryBufferMax: 4 OriginalTitle: %SystemRoot%\system32\cmd.exe Title: C:\WINDOWS\system32\cmd.exe AttachedProcess: cmd.exe Pid: 544 Handle: 0×4c4 ---- CommandHistory: 0×1113498 Application: sc.exe Flags: CommandCount: 0 LastAdded: -1 LastDisplayed: -1 FirstCommand: 0 CommandCountMax: 50 ProcessHandle: 0×0 ---- CommandHistory: 0×11132d8 Application: cmd.exe Flags: Allocated, Reset CommandCount: 2 LastAdded: 1 LastDisplayed: 1 FirstCommand: 0 CommandCountMax: 50 ProcessHandle: 0×4c4 Cmd #0 at 0×4e1eb8: sc query malwar Cmd #1 at 0×11135e8: sc query malware ---- Screen 0×4e2a70 X:80 Y:300 Dump: Microsoft Windows XP [Version 5.1.2600] (C) Copyright 1985-2001 Microsoft Corp. C:\Documents and Settings\Administrator>sc query malwar [SC] EnumQueryServicesStatus:OpenService FAILED 1060: The specified service does not exist as an installed service. C:\Documents and Settings\Administrator>sc query malware SERVICE_NAME: malware TYPE : 1 KERNEL_DRIVER STATE : 4 RUNNING (STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN) WIN32_EXIT_CODE : 0 (0×0) SERVICE_EXIT_CODE : 0 (0×0) CHECKPOINT : 0×0 WAIT_HINT : 0×0
Output	We are able to see that the “sc query malware” command was executed. This confirm that cmd.exe and csrss.exe are used for malicious activities

All we have to do now is to take the process dump of the activities and convert it into an .exe file. The first one is cmd.exe with PID 544.

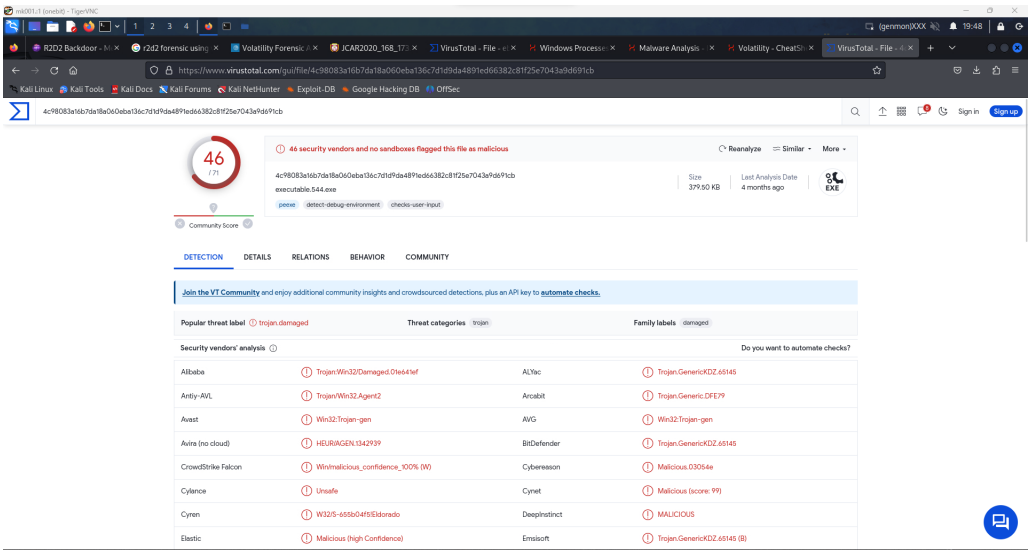
Step 8

Command	./volatility -f [file name] –profile=WinXPSP2x86 procdump -p 544 –dump-dir .

Image	
Output	 We are able to take the process dump and convert it to an exe

After we got the .exe file we use a website www.virustotal.com to scan the virus.

Step 9

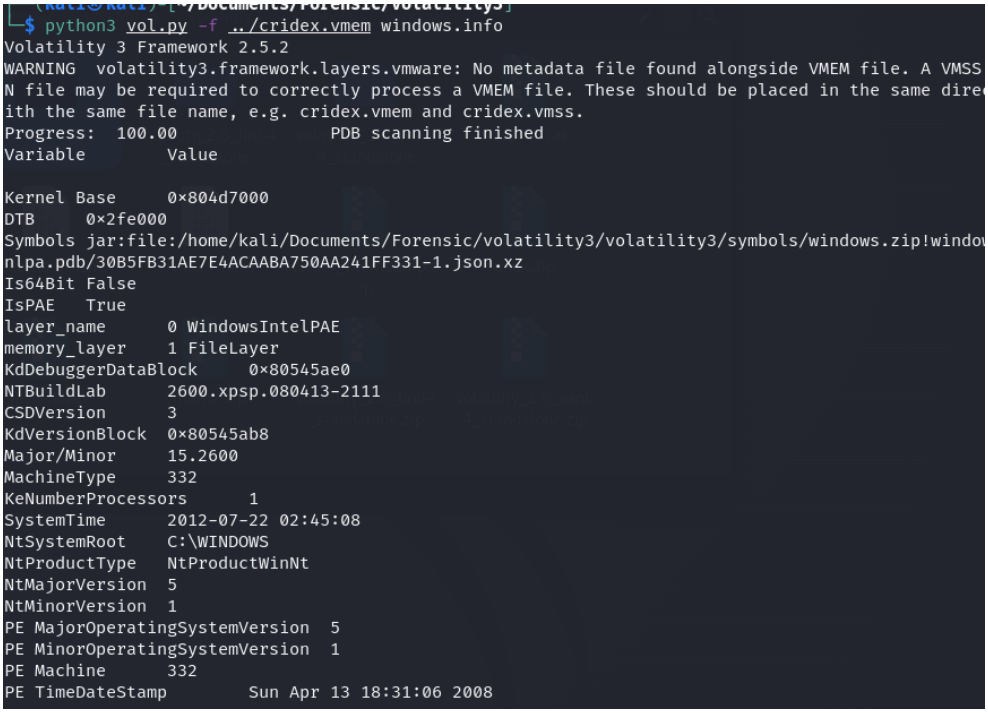
Command	Check the .exe files on browser using virustotal.com
Image	

Output	

Security vendors' analysis	Do you want to automate checks?
Alibaba	Trojan:Win32/Damaged.01e641ef
ALYac	Trojan.GenericKDZ.65145
Antiy-AVL	Trojan/Win32.Agent2
Arcabit	Trojan.Generic.DFE79
Avast	Win32:Trojan-gen
AVG	Win32:Trojan-gen
Avira (no cloud)	HEUR/AGEN.1342939
BitDefender	Trojan.GenericKDZ.65145
CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.03054e
Cylance	Unsafe
Cynet	Malicious (score: 99)
Cyren	W32/S-655b04f5!Eldorado
DeepInstinct	MALICIOUS
Elastic	Malicious (high Confidence)
Emsisoft	Trojan.GenericKDZ.65145 (B)
eScan	Trojan.GenericKDZ.65145
ESET-NOD32	A Variant Of Generik.FZHQXLK
F-Secure	Heuristic.HEUR/AGEN.1342939
Fortinet	W32/Generic.KDZ!tr

We are able to see that this exe file is a trojan malware

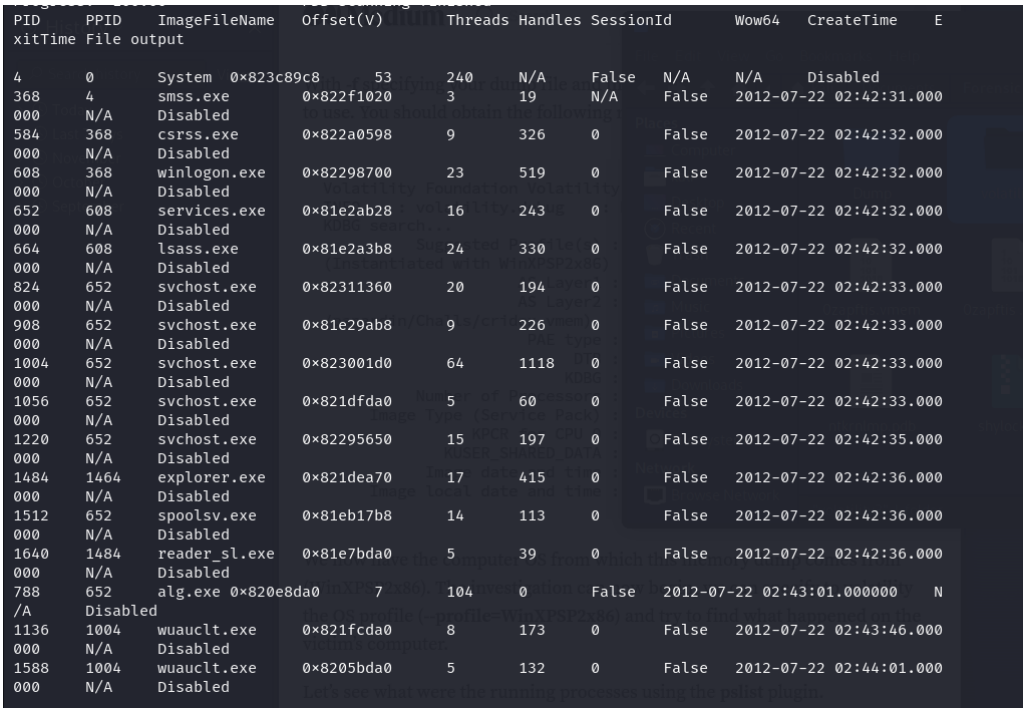
Cridex :

Command	python3 vol.py -f ../cridex.vmem windows.info
Image	
Output	The output shows info about its OS

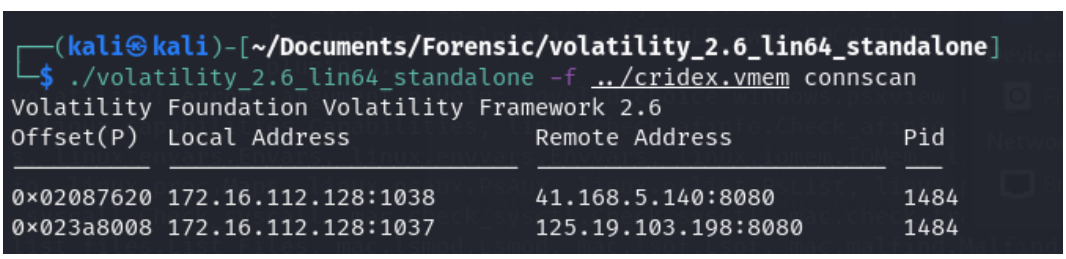
```
└─$ python3 vol.py -f ../cridex.vmem windows.info
Volatility 3 Framework 2.5.2
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS
N file may be required to correctly process a VMEM file. These should be placed in the same direc
ith the same file name, e.g. cridex.vmem and cridex.vmss.
Progress:  100.00               PDB scanning finished
Variable        Value

Kernel Base     0x804d7000
DTB     0x2fe000
Symbols jar:file:/home/kali/Documents/Forensic/volatility3/volatility3/symbols/windows.zip!window
nlpa.pdb/30B5FB31AE7E4ACAABA750AA241FF331-1.json.xz
Is64Bit False
IsPAE   True
layer_name      0 WindowsIntelPAE
memory_layer    1 FileLayer
KdDebuggerDataBlock     0x80545ae0
NTBuildLab      2600.xpsp.080413-2111
CSDVersion      3
KdVersionBlock  0x80545ab8
Major/Minor     15.2600
MachineType     332
KeNumberProcessors      1
SystemTime      2012-07-22 02:45:08
NtSystemRoot    C:\WINDOWS
NtProductType   NtProductWinNt
NtMajorVersion  5
NtMinorVersion  1
PE MajorOperatingSystemVersion  5
PE MinorOperatingSystemVersion  1
PE Machine      332
PE TimeDateStamp        Sun Apr 13 18:31:06 2008
```

Command	python3 vol.py -f ../cridex.vmem windows.pslist
Image	
Output	The output all of the proses that was runned.

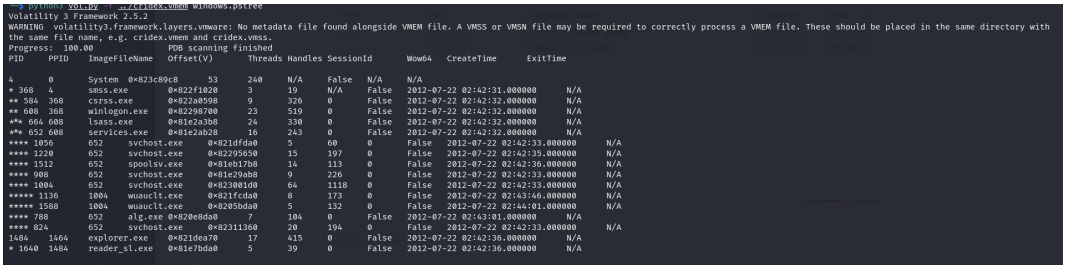
```
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime    E
xitTime File output

4       0       System  0x823c89c8      53      240     N/A     False   N/A     N/A     Disabled
368     4       smss.exe        0x822f1020      3       19      N/A     False   2012-07-22 02:42:31.000
000     N/A     Disabled
584     368     csrss.exe       0x822a0598      9       326     0       False   2012-07-22 02:42:32.000
000     N/A     Disabled
608     368     winlogon.exe    0x82298700      23      519     0       False   2012-07-22 02:42:32.000
000     N/A     Disabled
652     608     services.exe    0x81e2ab28      16      243     0       False   2012-07-22 02:42:32.000
000     N/A     Disabled
664     608     lsass.exe       0x81e2a3b8      24      330     0       False   2012-07-22 02:42:32.000
000     N/A     Disabled
824     652     svchost.exe     0x82311360      20      194     0       False   2012-07-22 02:42:33.000
000     N/A     Disabled
908     652     svchost.exe     0x81e29ab8      9       226     0       False   2012-07-22 02:42:33.000
000     N/A     Disabled
1004    652     svchost.exe     0x823001d0      64      1118    0       False   2012-07-22 02:42:33.000
000     N/A     Disabled
1056    652     svchost.exe     0x821dfda0      5       60      0       False   2012-07-22 02:42:33.000
000     N/A     Disabled
1220    652     svchost.exe     0x82295650      15      197     0       False   2012-07-22 02:42:35.000
000     N/A     Disabled
1484    1464    explorer.exe    0x821dea70      17      415     0       False   2012-07-22 02:42:36.000
000     N/A     Disabled
1512    652     spoolsv.exe     0x81eb17b8      14      113     0       False   2012-07-22 02:42:36.000
000     N/A     Disabled
1640    1484    reader_sl.exe   0x81e7bda0      5       39      0       False   2012-07-22 02:42:36.000
000     N/A     Disabled
788     652     alg.exe 0x820e8da0      7       104     0       False   2012-07-22 02:43:01.000000    N
/A      Disabled
1136    1004    wuauclt.exe     0x821fcda0      8       173     0       False   2012-07-22 02:43:46.000
000     N/A     Disabled
1588    1004    wuauclt.exe     0x8205bda0      5       132     0       False   2012-07-22 02:44:01.000
000     N/A     Disabled
```

Command	python3 vol.py -f ../cridex.vmem windows.pslist
Image	
Output	The output all of the proses that was runned.

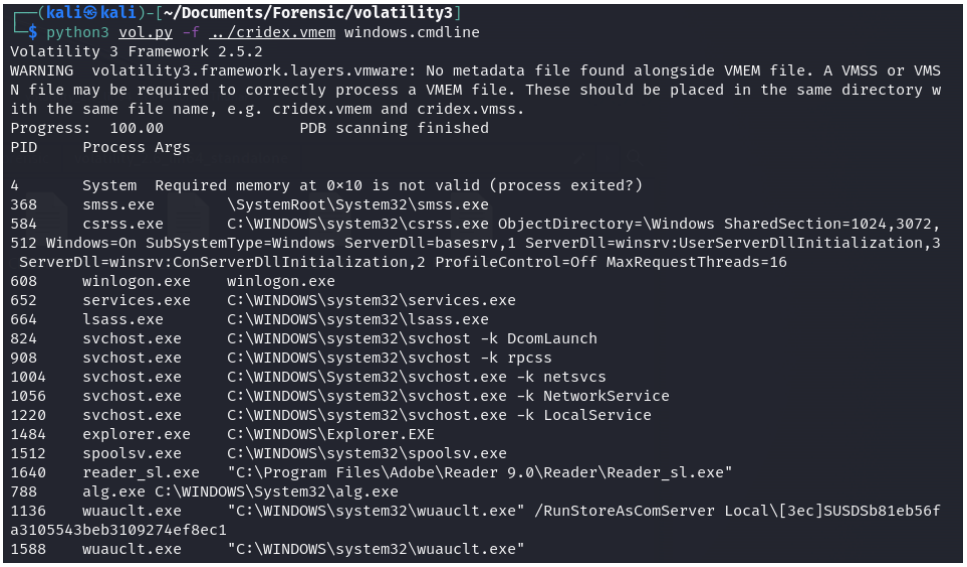
```
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime    E
xitTime File output

4       0       System  0x823c89c8      53      240     N/A     False   N/A     N/A     Disabled
368     4       smss.exe        0x822f1020      3       19      N/A     False   2012-07-22 02:42:31.000
000     N/A     Disabled
584     368     csrss.exe       0x822a0598      9       326     0       False   2012-07-22 02:42:32.000
000     N/A     Disabled
608     368     winlogon.exe    0x82298700      23      519     0       False   2012-07-22 02:42:32.000
000     N/A     Disabled
652     608     services.exe    0x81e2ab28      16      243     0       False   2012-07-22 02:42:32.000
000     N/A     Disabled
664     608     lsass.exe       0x81e2a3b8      24      330     0       False   2012-07-22 02:42:32.000
000     N/A     Disabled
824     652     svchost.exe     0x82311360      20      194     0       False   2012-07-22 02:42:33.000
000     N/A     Disabled
908     652     svchost.exe     0x81e29ab8      9       226     0       False   2012-07-22 02:42:33.000
000     N/A     Disabled
1004    652     svchost.exe     0x823001d0      64      1118    0       False   2012-07-22 02:42:33.000
000     N/A     Disabled
1056    652     svchost.exe     0x821dfda0      5       60      0       False   2012-07-22 02:42:33.000
000     N/A     Disabled
1220    652     svchost.exe     0x82295650      15      197     0       False   2012-07-22 02:42:35.000
000     N/A     Disabled
1484    1464    explorer.exe    0x821dea70      17      415     0       False   2012-07-22 02:42:36.000
000     N/A     Disabled
1512    652     spoolsv.exe     0x81eb17b8      14      113     0       False   2012-07-22 02:42:36.000
000     N/A     Disabled
1640    1484    reader_sl.exe   0x81e7bda0      5       39      0       False   2012-07-22 02:42:36.000
000     N/A     Disabled
788     652     alg.exe 0x820e8da0      7       104     0       False   2012-07-22 02:43:01.000000    N
/A      Disabled
1136    1004    wuauclt.exe     0x821fcda0      8       173     0       False   2012-07-22 02:43:46.000
000     N/A     Disabled
1588    1004    wuauclt.exe     0x8205bda0      5       132     0       False   2012-07-22 02:44:01.000
000     N/A     Disabled
```

Command	./volatility_2.6_lin64_standalone -f ../cridex.vmem connscan
Image	
Output	We are able to see that Pid 1484 made a connection outside

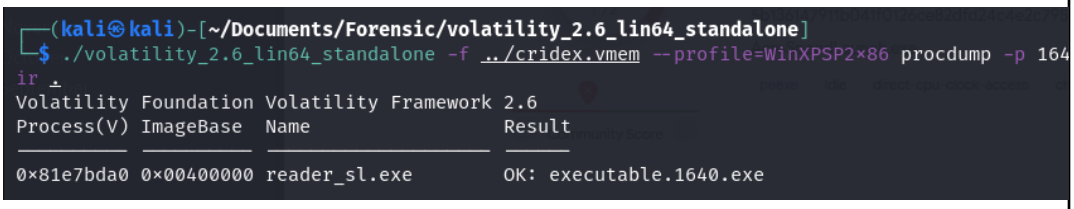
```
┌──(kali㉿kali)-[~/Documents/Forensic/volatility_2.6_lin64_standalone]
└─$ ./volatility_2.6_lin64_standalone -f ../cridex.vmem connscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- -------------------------- --------------------------- ---
0x02087620 172.16.112.128:1038        41.168.5.140:8080         1484
0x023a8008 172.16.112.128:1037        125.19.103.198:8080       1484
```

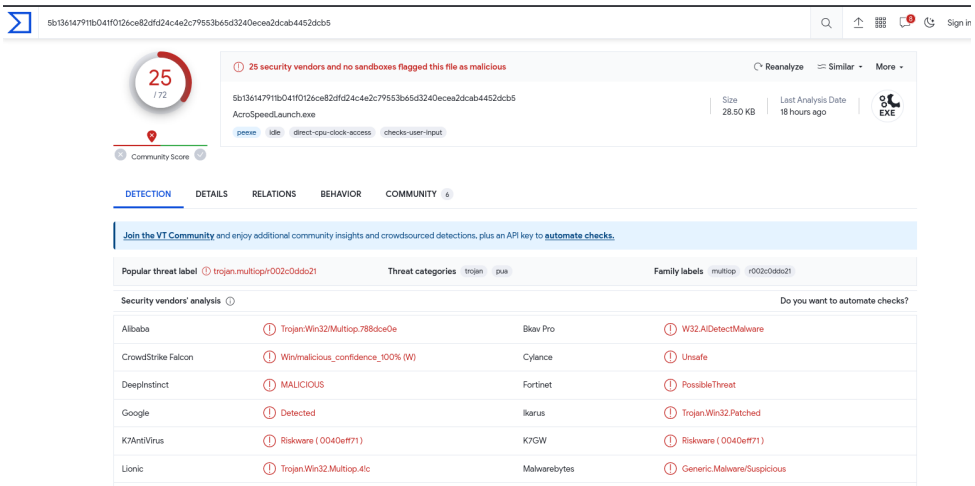
Command	python3 vol.py -f ../cridex.vmem windows.pstree
Image	
Output	We are able to see that PID 1484 has a child process : 1640

```
~$ python3 vol.py -f ../cridex.vmem windows.pstree
Volatility 3 Framework 2.5.2
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file. These should be placed in the same directory with
the same file name, e.g. cridex.vmem and cridex.vmss.
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime

4       0       System  0×823c89c8      53      240     N/A     False   N/A     N/A
* 368   4       smss.exe        0×822f1020      3       19      N/A     False   2012-07-22 02:42:31.000000      N/A
** 584  368     csrss.exe       0×822a0598      9       326     0       False   2012-07-22 02:42:32.000000      N/A
** 608  368     winlogon.exe    0×82298700      23      519     0       False   2012-07-22 02:42:32.000000      N/A
*** 664 608     lsass.exe       0×81e2a3b8      24      330     0       False   2012-07-22 02:42:32.000000      N/A
*** 652 608     services.exe    0×81e2ab28      16      243     0       False   2012-07-22 02:42:32.000000      N/A
**** 1056       652     svchost.exe     0×821dfda0      5       60      0       False   2012-07-22 02:42:33.000000      N/A
**** 1220       652     svchost.exe     0×82295650      15      197     0       False   2012-07-22 02:42:35.000000      N/A
**** 1512       652     spoolsv.exe     0×81e917b8      14      113     0       False   2012-07-22 02:42:36.000000      N/A
**** 908        652     svchost.exe     0×81e29ab8      9       226     0       False   2012-07-22 02:42:33.000000      N/A
**** 1004       652     svchost.exe     0×823001d0      64      1118    0       False   2012-07-22 02:42:33.000000      N/A
***** 1136       1004    wuauclt.exe     0×821fcda0      8       173     0       False   2012-07-22 02:43:46.000000      N/A
***** 1588       1004    wuauclt.exe     0×82805da0      5       132     0       False   2012-07-22 02:44:01.000000      N/A
**** 788        652     alg.exe 0×820e8da0      7       104     0       False   2012-07-22 02:43:01.000000      N/A
**** 824        652     svchost.exe     0×82311360      20      194     0       False   2012-07-22 02:42:33.000000      N/A
1484    1464    explorer.exe    0×821dea70      17      415     0       False   2012-07-22 02:42:36.000000      N/A
* 1640  1484    reader_sl.exe   0×81e7bda0      5       39      0       False   2012-07-22 02:42:36.000000      N/A
```

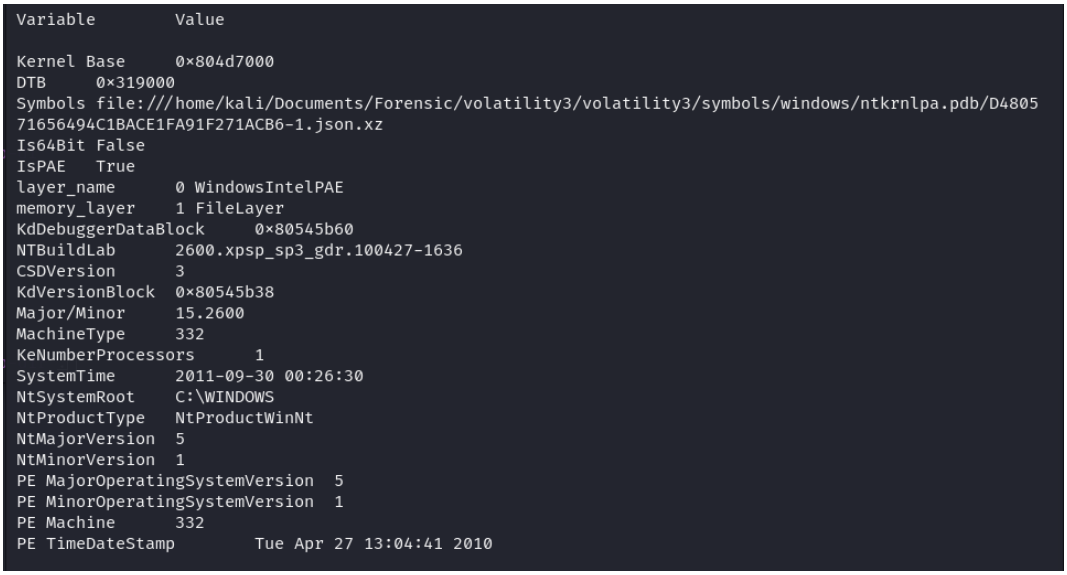
Command	python3 vol.py -f ../cridex.vmem windows.cmdline
Image	
Output	We can see that PID 1640 ran reader_sl.exe

```
┌──(kali㉿kali)-[~/Documents/Forensic/volatility3]
└─$ python3 vol.py -f ../cridex.vmem windows.cmdline
Volatility 3 Framework 2.5.2
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMS
N file may be required to correctly process a VMEM file. These should be placed in the same directory w
ith the same file name, e.g. cridex.vmem and cridex.vmss.
Progress:  100.00               PDB scanning finished
PID     Process Args

4       System  Required memory at 0×10 is not valid (process exited?)
368     smss.exe        \SystemRoot\System32\smss.exe
584     csrss.exe       C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072,
512 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3
 ServerDll=winsrv:ConServerDllInitialization,2 ProfileControl=Off MaxRequestThreads=16
608     winlogon.exe    winlogon.exe
652     services.exe    C:\WINDOWS\system32\services.exe
664     lsass.exe       C:\WINDOWS\system32\lsass.exe
824     svchost.exe     C:\WINDOWS\system32\svchost -k DcomLaunch
908     svchost.exe     C:\WINDOWS\system32\svchost -k rpcss
1004    svchost.exe     C:\WINDOWS\System32\svchost.exe -k netsvcs
1056    svchost.exe     C:\WINDOWS\system32\svchost.exe -k NetworkService
1220    svchost.exe     C:\WINDOWS\system32\svchost.exe -k LocalService
1484    explorer.exe    C:\WINDOWS\Explorer.EXE
1512    spoolsv.exe     C:\WINDOWS\system32\spoolsv.exe
1640    reader_sl.exe   "C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe"
788     alg.exe C:\WINDOWS\System32\alg.exe
1136    wuauclt.exe     "C:\WINDOWS\system32\wuauclt.exe" /RunStoreAsComServer Local\[3ec]SUSDSb81eb56f
a3105543beb3109274ef8ec1
1588    wuauclt.exe     "C:\WINDOWS\system32\wuauclt.exe"
```

Command	./volatility_2.6_lin64_standalone -f ../cridex.vmem --profile=WinXPSP2x86 procdump -p 1640 --dump-dir .
Image	
Output	We are now going to proc dump the pid and convert it to exe file

Command	Visit virus total to check the exe for malware
Image	
Output	There are many virus detected on this exe

SHYLOCK :

Command	python3 vol.py -f ../Windows\ XP\ Professional.vmem -vvv windows.info
Image	
Output	This output display info about the vmem

Command	python3 vol.py -f ../Windows\ XP\ Professional.vmem -vvv windows.pslist

Image	

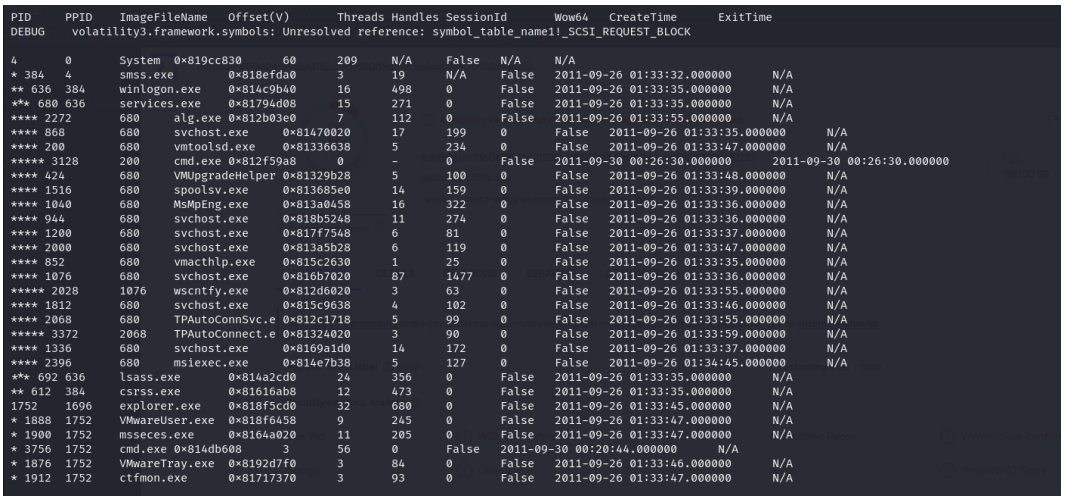
```
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime    E
xitTime File output
DEBUG    volatility3.framework.symbols: Unresolved reference: symbol_table_name1!_SCSI_REQUEST_BLOCK

4       0       System  0x819cc830      60      209     N/A     False   N/A     N/A     Disabled
384     4       smss.exe        0x818efda0      3       19      N/A     False   2011-09-26 01:33:32.000
000     N/A     Disabled
612     384     csrss.exe       0x81616ab8      12      473     0       False   2011-09-26 01:33:35.000
000     N/A     Disabled
636     384     winlogon.exe    0x814c9b40      16      498     0       False   2011-09-26 01:33:35.000
000     N/A     Disabled
680     636     services.exe    0x81794d08      15      271     0       False   2011-09-26 01:33:35.000
000     N/A     Disabled
692     636     lsass.exe       0x814a2cd0      24      356     0       False   2011-09-26 01:33:35.000
000     N/A     Disabled
852     680     vmacthlp.exe    0x815c2630      1       25      0       False   2011-09-26 01:33:35.000
000     N/A     Disabled
868     680     svchost.exe     0x81470020      17      199     0       False   2011-09-26 01:33:35.000
000     N/A     Disabled
944     680     svchost.exe     0x818b5248      11      274     0       False   2011-09-26 01:33:36.000
000     N/A     Disabled
1040    680     MsMpEng.exe     0x813a0458      16      322     0       False   2011-09-26 01:33:36.000
000     N/A     Disabled
1076    680     svchost.exe     0x816b7020      87      1477    0       False   2011-09-26 01:33:36.000
000     N/A     Disabled
1200    680     svchost.exe     0x817f7548      6       81      0       False   2011-09-26 01:33:37.000
000     N/A     Disabled
1336    680     svchost.exe     0x8169a1d0      14      172     0       False   2011-09-26 01:33:37.000
000     N/A     Disabled
1516    680     spoolsv.exe     0x813685e0      14      159     0       False   2011-09-26 01:33:39.000
000     N/A     Disabled
1752    1696    explorer.exe    0x818f5cd0      32      680     0       False   2011-09-26 01:33:45.000
000     N/A     Disabled
1812    680     svchost.exe     0x815c9638      4       102     0       False   2011-09-26 01:33:46.000
000     N/A     Disabled
1876    1752    VMwareTray.exe  0x8192d7f0      3       84      0       False   2011-09-26 01:33:46.000
```

Output	This command shows all the processes that runned

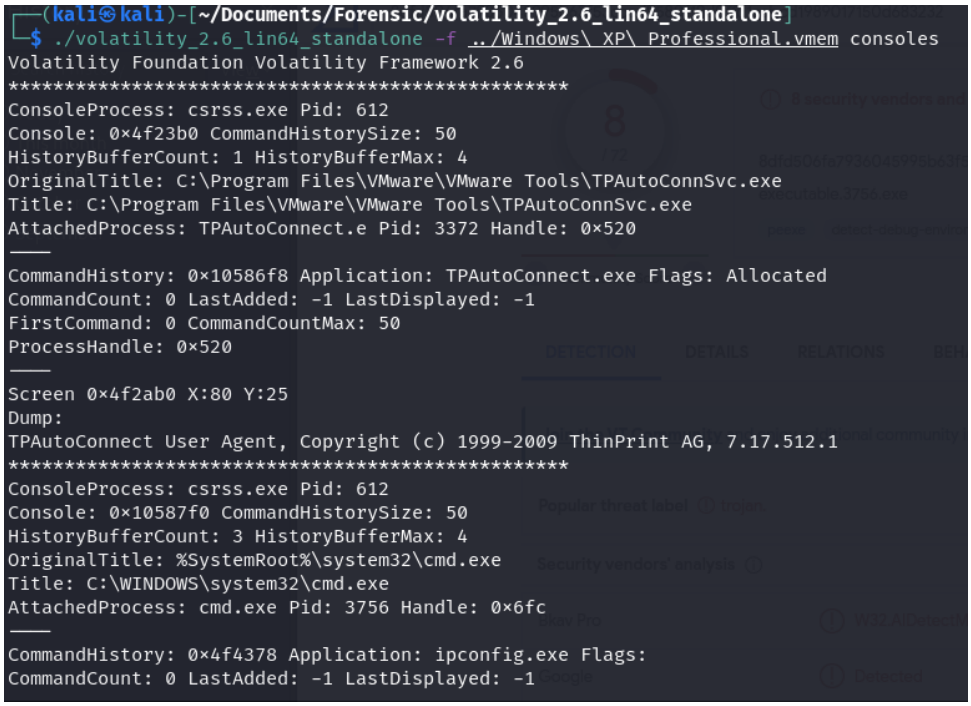
Command	./volatility_2.6_lin64_standalone -f ../Windows\ XP\ Professional.vmem connscan
Image	

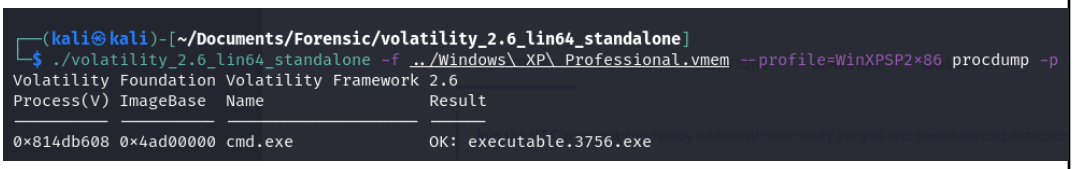
```
┌──(kali㉿kali)-[~/Documents/Forensic/volatility_2.6_lin64_standalone]
└─$ ./volatility_2.6_lin64_standalone -f ../Windows\ XP\ Professional.vmem
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x014f6ab0 10.0.0.109:1072           209.190.4.84:443          1752
0x01507380 10.0.0.109:1073           209.190.4.84:443          1752
0x016c2b00 10.0.0.109:1065           184.173.252.227:443       1752
0x017028a0 10.0.0.109:1067           184.173.252.227:443       1752
0x01858cb0 10.0.0.109:1068           209.190.4.84:443          1752
```

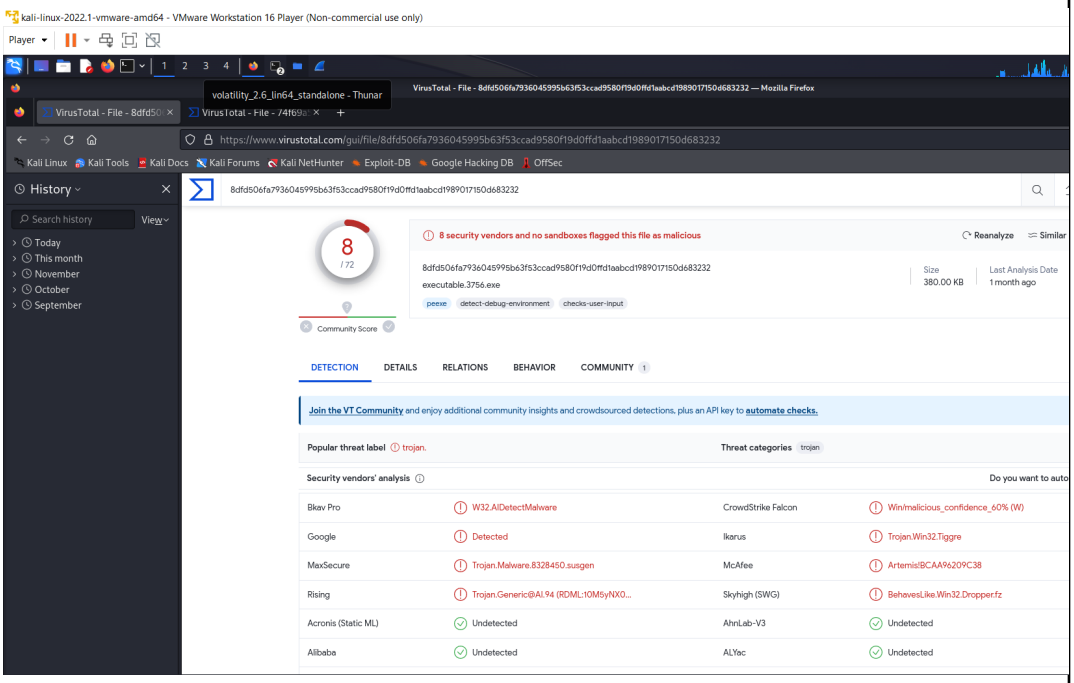
Output	This output shows that Pid 1752 made some connections

Command	python3 vol.py -f ../Windows\ XP\ Professional.vmem -vvv windows.pstree
Image	
Output	We are able too see that there are many child processes that are made.

```
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime
DEBUG    volatility3.framework.symbols: Unresolved reference: symbol_table_name1!_SCSI_REQUEST_BLOCK

4       0       System  0x819cc830      60      209     N/A     False   N/A     N/A
* 384   4       smss.exe        0x818efda0      3       19      N/A     False   2011-09-26 01:33:32.000000      N/A
** 636  384     winlogon.exe    0x814c9b40      16      498     0       False   2011-09-26 01:33:35.000000      N/A
*** 680 636     services.exe    0x81794d08      15      271     0       False   2011-09-26 01:33:35.000000      N/A
**** 2272       680     alg.exe 0x812b03e0      7       112     0       False   2011-09-26 01:33:55.000000      N/A
**** 868        680     svchost.exe     0x81470020      17      199     0       False   2011-09-26 01:33:35.000000      N/A
**** 200        680     vmtoolsd.exe    0x81336638      5       234     0       False   2011-09-26 01:33:47.000000      N/A
***** 3128       200     cmd.exe 0x812f59a8      0       -       0       False   2011-09-30 00:26:30.000000      2011-09-30 00:26:30.000000
**** 424        680     VMUpgradeHelper 0x81329b28      5       100     0       False   2011-09-26 01:33:48.000000      N/A
**** 1516       680     spoolsv.exe     0x813685e0      14      159     0       False   2011-09-26 01:33:39.000000      N/A
**** 1040       680     MsMpEng.exe     0x813a0458      16      322     0       False   2011-09-26 01:33:36.000000      N/A
**** 944        680     svchost.exe     0x818b5248      11      274     0       False   2011-09-26 01:33:36.000000      N/A
**** 1200       680     svchost.exe     0x817f7548      6       81      0       False   2011-09-26 01:33:37.000000      N/A
**** 2000       680     svchost.exe     0x813a5b28      6       119     0       False   2011-09-26 01:33:47.000000      N/A
**** 852        680     vmacthlp.exe    0x815c2630      1       25      0       False   2011-09-26 01:33:35.000000      N/A
**** 1076       680     svchost.exe     0x816b7020      87      1477    0       False   2011-09-26 01:33:36.000000      N/A
***** 2028       1076    wscntfy.exe     0x812d6020      3       63      0       False   2011-09-26 01:33:55.000000      N/A
**** 1812       680     svchost.exe     0x815c9638      4       102     0       False   2011-09-26 01:33:46.000000      N/A
**** 2068       680     TPAutoConnSvc.e 0x812c1718      5       99      0       False   2011-09-26 01:33:55.000000      N/A
***** 3372       2068    TPAutoConnect.e 0x81324020      3       90      0       False   2011-09-26 01:33:59.000000      N/A
**** 1336       680     svchost.exe     0x8169a1d0      14      172     0       False   2011-09-26 01:33:37.000000      N/A
**** 2396       680     msiexec.exe     0x814e7b38      5       127     0       False   2011-09-26 01:34:45.000000      N/A
*** 692 636     lsass.exe       0x814a2cd0      24      356     0       False   2011-09-26 01:33:35.000000      N/A
** 612  384     csrss.exe       0x81616ab8      12      473     0       False   2011-09-26 01:33:35.000000      N/A
1752    1696    explorer.exe    0x818f5cd0      32      680     0       False   2011-09-26 01:33:45.000000      N/A
* 1888  1752    VMwareUser.exe  0x818f6458      9       245     0       False   2011-09-26 01:33:47.000000      N/A
* 1900  1752    msseces.exe     0x8164a020      11      205     0       False   2011-09-26 01:33:47.000000      N/A
* 3756  1752    cmd.exe 0x814db608      3       56      0       False   2011-09-30 00:20:44.000000      N/A
* 1876  1752    VMwareTray.exe  0x8192d7f0      3       84      0       False   2011-09-26 01:33:46.000000      N/A
* 1912  1752    ctfmon.exe      0x81717370      3       93      0       False   2011-09-26 01:33:47.000000      N/A
```

Command	./volatility_2.6_lin64_standalone -f ../Windows\ XP\ Professional.vmem consoles
Image	 (kali㉿kali)-[~/Documents/Forensic/volatility_2.6_lin64_standalone] $ ./volatility_2.6_lin64_standalone -f ../Windows\ XP\ Professional.vmem consoles Volatility Foundation Volatility Framework 2.6 ********** ConsoleProcess: csrss.exe Pid: 612 Console: 0×4f23b0 CommandHistorySize: 50 HistoryBufferCount: 1 HistoryBufferMax: 4 OriginalTitle: C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe Title: C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe AttachedProcess: TPAutoConnect.e Pid: 3372 Handle: 0×520 ——— CommandHistory: 0×10586f8 Application: TPAutoConnect.exe Flags: Allocated CommandCount: 0 LastAdded: -1 LastDisplayed: -1 FirstCommand: 0 CommandCountMax: 50 ProcessHandle: 0×520 ——— Screen 0×4f2ab0 X:80 Y:25 Dump: TPAutoConnect User Agent, Copyright (c) 1999-2009 ThinPrint AG, 7.17.512.1 ********** ConsoleProcess: csrss.exe Pid: 612 Console: 0×10587f0 CommandHistorySize: 50 HistoryBufferCount: 3 HistoryBufferMax: 4 OriginalTitle: %SystemRoot%\system32\cmd.exe Title: C:\WINDOWS\system32\cmd.exe AttachedProcess: cmd.exe Pid: 3756 Handle: 0×6fc ——— CommandHistory: 0×4f4378 Application: ipconfig.exe Flags: CommandCount: 0 LastAdded: -1 LastDisplayed: -1
Output	We are able too see that the pid 3756 runned cmd.exe

Command	./volatility_2.6_lin64_standalone -f ../Windows\ XP\ Professional.vmem --profile=WinXPSP2x86 procdump -p 3756 --dump-dir .
Image	 (kali㉿kali)-[~/Documents/Forensic/volatility_2.6_lin64_standalone] $ ./volatility_2.6_lin64_standalone -f ../Windows\ XP\ Professional.vmem --profile=WinXPSP2×86 procdump -p Volatility Foundation Volatility Framework 2.6 Process(V) ImageBase Name Result ———— ———— ———— ———— 0×814db608 0×4ad00000 cmd.exe OK: executable.3756.exe
Output	We are now going to proc dump the pid and convert it to exe file

Command	Taking the exe file to virus total to detect malware
Image	
Output	We are able to see that the file contains some malware.