DIGITAL FORENSICS LAB

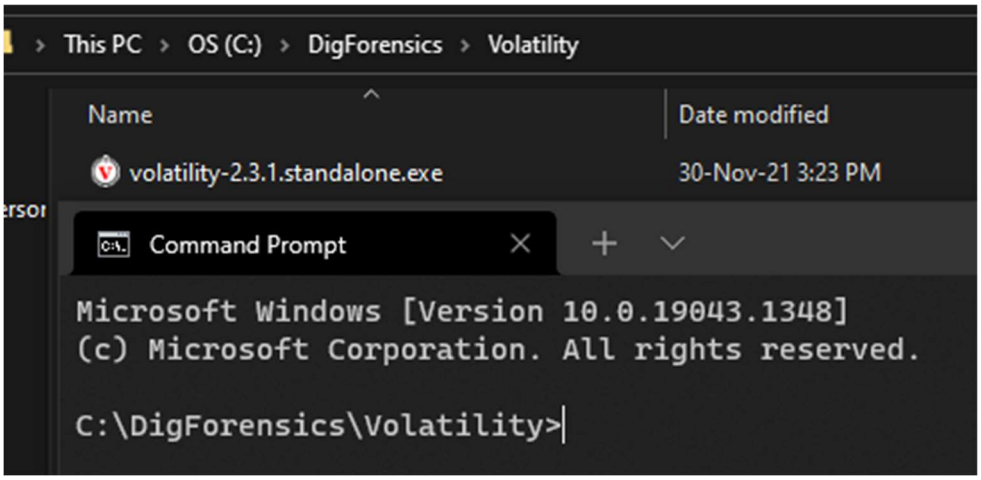
Exercise 14	
Name	S Shyam Sundaram
Registration Number	19BCE1560
Slot	L39+L40
Faculty	Dr. Seshu Babu Pulagara
Date	30th November, 2021

AIM

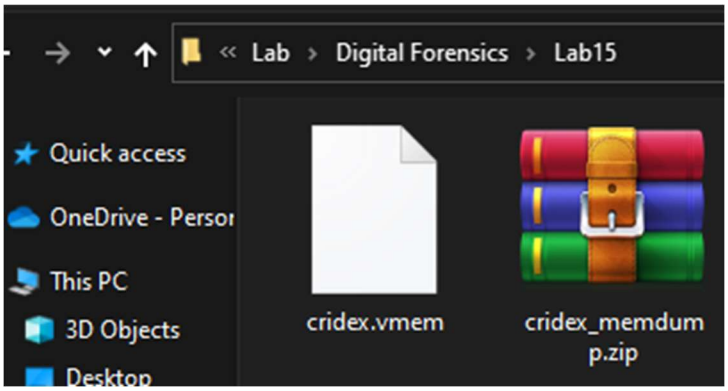
Employing memory forensic tool to analyse a memory dump.

PROCEDRE

1. Go to the folder where Volatility is downloaded and open the terminal there.



2. Download a memory image file or create your own using 'Magnet RAM Capture'. Here I have downloaded a memory file with the Cridex malware.



3. Now run the following command to get more info about the memory file.

```
Command Prompt

C:\DigForensics\Volatility>volatility-2.3.1.standalone.exe -f "C:\Files\Academics\VIT\Lab\Digital Forensics\Lab15\cridex.vmem" imageinfo
Volatility Foundation Volatility Framework 2.3.1
Determining profile based on KDBG search...

          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\Files\Academics\VIT\Lab\Digital Forensics\Lab15\cridex.vmem)
                      PAE type : PAE
                           DTB : 0x2fe000L
                          KDBG : 0x80545ae0L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2012-07-22 02:45:08 UTC+0000
     Image local date and time : 2012-07-21 22:45:08 -0400

C:\DigForensics\Volatility>
```

This gives us a list of suggested profiles to use for the cridex.vmem image.

4. Now we see what were the processes running in the memory with the following command.

```
C:\DigForensics\Volatility>volatility-2.3.1.standalone.exe -f cridex.vmem --profile=WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.3.1
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x823c89c8 System                    4      0     53      240 ------      0
0x822f1020 smss.exe                368      4      3       19 ------      0 2012-07-22 02:42:31 UTC+0000
0x822a0598 csrss.exe               584    368      9      326      0      0 2012-07-22 02:42:32 UTC+0000
0x82298700 winlogon.exe            608    368     23      519      0      0 2012-07-22 02:42:32 UTC+0000
0x81e2ab28 services.exe            652    608     16      243      0      0 2012-07-22 02:42:32 UTC+0000
0x81e2a3b8 lsass.exe               664    608     24      330      0      0 2012-07-22 02:42:32 UTC+0000
0x82311360 svchost.exe             824    652     20      194      0      0 2012-07-22 02:42:33 UTC+0000
0x81e29ab8 svchost.exe             908    652      9      226      0      0 2012-07-22 02:42:33 UTC+0000
0x823001d0 svchost.exe            1004    652     64     1118      0      0 2012-07-22 02:42:33 UTC+0000
0x821dfda0 svchost.exe            1056    652      5       60      0      0 2012-07-22 02:42:33 UTC+0000
0x82295650 svchost.exe            1220    652     15      197      0      0 2012-07-22 02:42:35 UTC+0000
0x821dea70 explorer.exe           1484   1464     17      415      0      0 2012-07-22 02:42:36 UTC+0000
0x81eb17b8 spoolsv.exe            1512    652     14      113      0      0 2012-07-22 02:42:36 UTC+0000
0x81e7bda0 reader_sl.exe          1640   1484      5       39      0      0 2012-07-22 02:42:36 UTC+0000
0x820e8da0 alg.exe                 788    652      7      104      0      0 2012-07-22 02:43:01 UTC+0000
0x821fcda0 wuauclt.exe            1136   1004      8      173      0      0 2012-07-22 02:43:46 UTC+0000
0x8205bda0 wuauclt.exe            1588   1004      5      132      0      0 2012-07-22 02:44:01 UTC+0000

C:\DigForensics\Volatility>
```

5. To see it in another format, we replace pslist with pstree.

```
C:\DigForensics\Volatility>volatility-2.3.1.standalone.exe -f cridex.vmem --profile=WinXPSP2x86 pstree
Volatility Foundation Volatility Framework 2.3.1
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x823c89c8:System                                      4      0     53    240 1970-01-01 00:00:00 UTC+0000
. 0x822f1020:smss.exe                                 368      4      3     19 2012-07-22 02:42:31 UTC+0000
.. 0x82298700:winlogon.exe                            608    368     23    519 2012-07-22 02:42:32 UTC+0000
... 0x81e2ab28:services.exe                           652    608     16    243 2012-07-22 02:42:32 UTC+0000
.... 0x821dfda0:svchost.exe                          1056    652      5     60 2012-07-22 02:42:33 UTC+0000
.... 0x81eb17b8:spoolsv.exe                          1512    652     14    113 2012-07-22 02:42:36 UTC+0000
.... 0x81e29ab8:svchost.exe                           908    652      9    226 2012-07-22 02:42:33 UTC+0000
.... 0x823001d0:svchost.exe                          1004    652     64   1118 2012-07-22 02:42:33 UTC+0000
..... 0x8205bda0:wuauclt.exe                         1588   1004      5    132 2012-07-22 02:44:01 UTC+0000
..... 0x821fcda0:wuauclt.exe                         1136   1004      8    173 2012-07-22 02:43:46 UTC+0000
.... 0x82311360:svchost.exe                           824    652     20    194 2012-07-22 02:42:33 UTC+0000
.... 0x820e8da0:alg.exe                               788    652      7    104 2012-07-22 02:43:01 UTC+0000
.... 0x82295650:svchost.exe                          1220    652     15    197 2012-07-22 02:42:35 UTC+0000
... 0x81e2a3b8:lsass.exe                              664    608     24    330 2012-07-22 02:42:32 UTC+0000
.. 0x822a0598:csrss.exe                               584    368      9    326 2012-07-22 02:42:32 UTC+0000
 0x821dea70:explorer.exe                             1484   1464     17    415 2012-07-22 02:42:36 UTC+0000
. 0x81e7bda0:reader_sl.exe                           1640   1484      5     39 2012-07-22 02:42:36 UTC+0000

C:\DigForensics\Volatility>
```

6. To see more about the tool's options and get some help, we execute this:

```
Command Prompt

C:\DigForensics\Volatility>volatility-2.3.1.standalone.exe -h
Volatility Foundation Volatility Framework 2.3.1
Usage: Volatility - A memory forensics analysis platform.

Options:
  -h, --help            list all available options and their default values.
                        Default values may be set in the configuration file
                        (/etc/volatilityrc)
  --conf-file=.volatilityrc
                        User based configuration file
  -d, --debug           Debug volatility
  --plugins=PLUGINS     Additional plugin directories to use (semi-colon
                        separated)
```

7. To uncover any hidden process, use psxview as below.

```
C:\DigForensics\Volatility>volatility-2.3.1.standalone.exe -f cridex.vmem --profile=WinXPSP2x86 psxview
Volatility Foundation Volatility Framework 2.3.1
Offset(P)  Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd
---------- -------------------- ------ ------ ------ -------- ------ ----- ------- --------
0x02498700 winlogon.exe            608 True   True   True     True   True  True    True
0x02511360 svchost.exe             824 True   True   True     True   True  True    True
0x022e8da0 alg.exe                 788 True   True   True     True   True  True    True
0x020b17b8 spoolsv.exe            1512 True   True   True     True   True  True    True
0x0202ab28 services.exe            652 True   True   True     True   True  True    True
0x02495650 svchost.exe            1220 True   True   True     True   True  True    True
0x0207bda0 reader_sl.exe          1640 True   True   True     True   True  True    True
0x025001d0 svchost.exe            1004 True   True   True     True   True  True    True
0x02029ab8 svchost.exe             908 True   True   True     True   True  True    True
0x023fcda0 wuauclt.exe            1136 True   True   True     True   True  True    True
0x0225bda0 wuauclt.exe            1588 True   True   True     True   True  True    True
0x0202a3b8 lsass.exe               664 True   True   True     True   True  True    True
0x023dea70 explorer.exe           1484 True   True   True     True   True  True    True
0x023dfda0 svchost.exe            1056 True   True   True     True   True  True    True
0x024f1020 smss.exe                368 True   True   True     True   False False   False
0x025c89c8 System                    4 True   True   True     True   False False   False
0x024a0598 csrss.exe               584 True   True   True     True   False True    True
```

8. To check the running open TCP conections, we can use connscan.

```
C:\DigForensics\Volatility>volatility-2.3.1.standalone.exe -f cridex.vmem --profile=WinXPSP2x86 connscan
Volatility Foundation Volatility Framework 2.3.1
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

C:\DigForensics\Volatility>
```

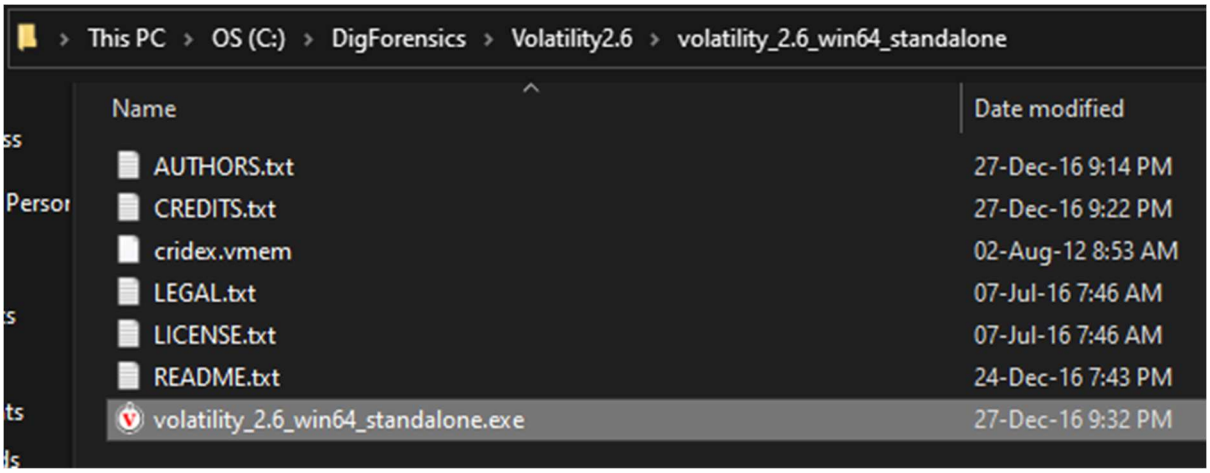
9. To view both TCP and UDP connections, use 'sockets'

```
Command Prompt

C:\DigForensics\Volatility>volatility-2.3.1.standalone.exe -f cridex.vmem --profile=WinXPSP2x86 socket
Volatility Foundation Volatility Framework 2.3.1
Offset(V)       PID   Port  Proto Protocol        Address         Create Time
---------- -------- ------ ------ ---------- ---------- -----------
0x81ddb780      664    500     17 UDP          0.0.0.0         2012-07-22 02:42:53 UTC+0000
0x82240d08     1484   1038      6 TCP          0.0.0.0         2012-07-22 02:44:45 UTC+0000
0x81dd7618     1220   1900     17 UDP          172.16.112.128  2012-07-22 02:43:01 UTC+0000
0x82125610      788   1028      6 TCP          127.0.0.1       2012-07-22 02:43:01 UTC+0000
0x8219cc08        4    445      6 TCP          0.0.0.0         2012-07-22 02:42:31 UTC+0000
0x81ec23b0      908    135      6 TCP          0.0.0.0         2012-07-22 02:42:33 UTC+0000
0x82276878        4    139      6 TCP          172.16.112.128  2012-07-22 02:42:38 UTC+0000
0x82277460        4    137     17 UDP          172.16.112.128  2012-07-22 02:42:38 UTC+0000
0x81e76620     1004    123     17 UDP          127.0.0.1       2012-07-22 02:43:01 UTC+0000
0x82172808      664      0    255 Reserved     0.0.0.0         2012-07-22 02:42:53 UTC+0000
0x81e3f460        4    138     17 UDP          172.16.112.128  2012-07-22 02:42:38 UTC+0000
0x821f0630     1004    123     17 UDP          172.16.112.128  2012-07-22 02:43:01 UTC+0000
0x822cd2b0     1220   1900     17 UDP          127.0.0.1       2012-07-22 02:43:01 UTC+0000
0x82172c50      664   4500     17 UDP          0.0.0.0         2012-07-22 02:42:53 UTC+0000
0x821f0d00        4    445     17 UDP          0.0.0.0         2012-07-22 02:42:31 UTC+0000

C:\DigForensics\Volatility>
```

10. **FOR THE FOLLOWING, USE VOLATILITY 2.6. This was saved in another folder called "Volatility2.6" in "DigForensics" folder.**



To display the commandline arguments of each process, use cmdline:

```
C:\DigForensics\Volatility2.6\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone -f cridex.vmem cmdline
Volatility Foundation Volatility Framework 2.6
**************************************************************************
System pid:      4
**************************************************************************
smss.exe pid:    368
Command line : \SystemRoot\System32\smss.exe
**************************************************************************
csrss.exe pid:    584
Command line : C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072,512 Windows=On SubSystemTy
pe=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitializatio
n,2 ProfileControl=Off MaxRequestThreads=16
**************************************************************************
winlogon.exe pid:    608
```

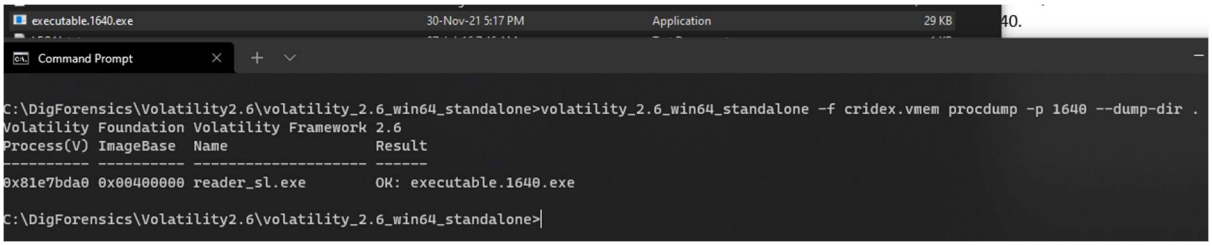
Scolling down we see the command line arguments and the path where reader_sl was stored. It is found using its process id 1640.

```
**************************************************************************
reader_sl.exe pid:    1640
Command line : "C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe"
**************************************************************************
alg.exe pid:     788
```

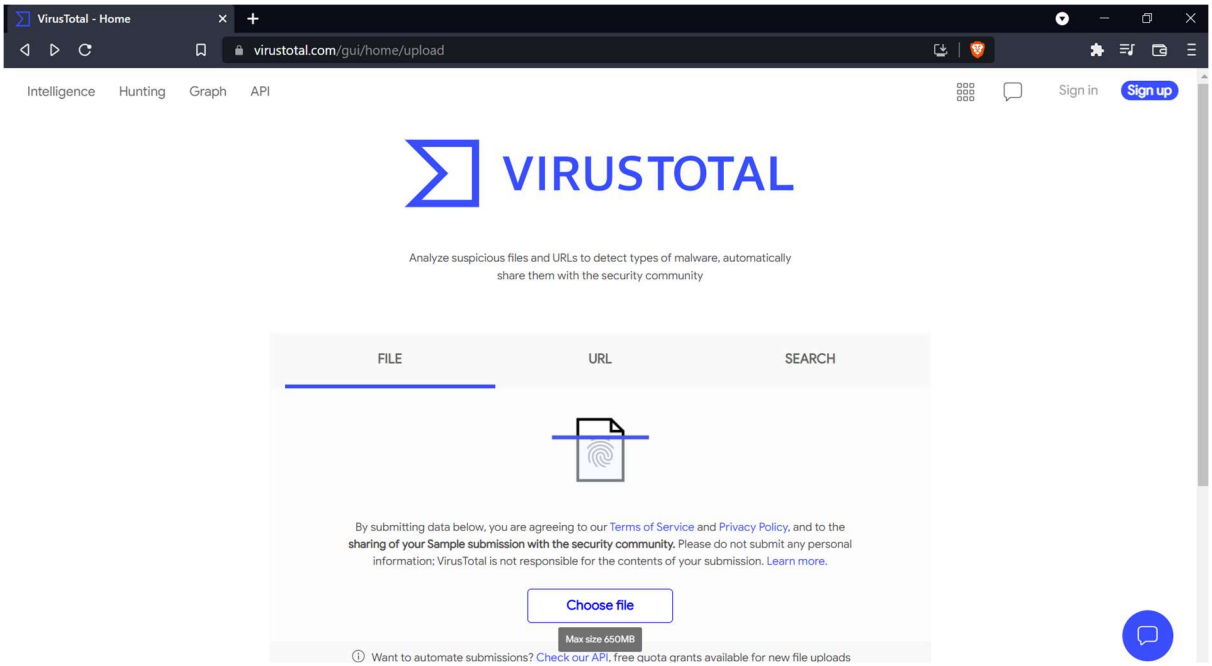
11. We now create a dump of this process and check it out. The command for this is given below using procdump and specifying the PID of the process.

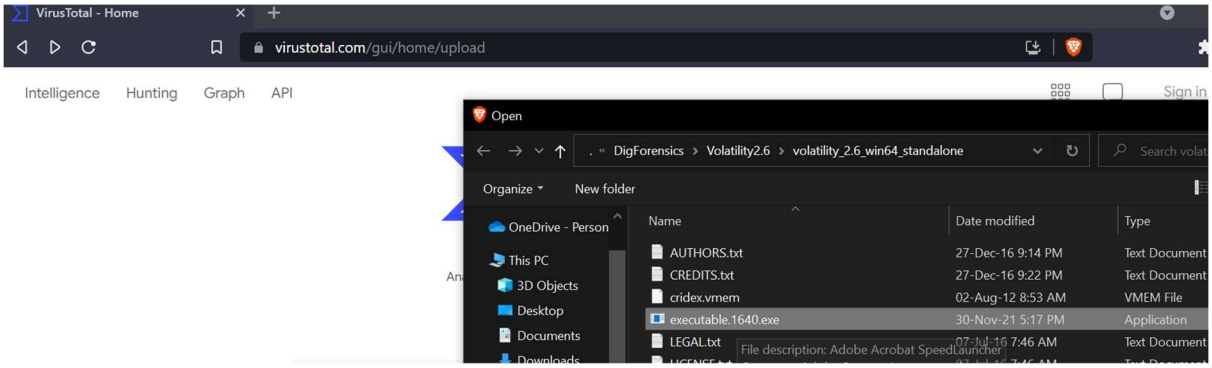
    Command run: volatility_2.6_win64_standalone -f cridex.vmem procdump -p 1640 --dump-dir .

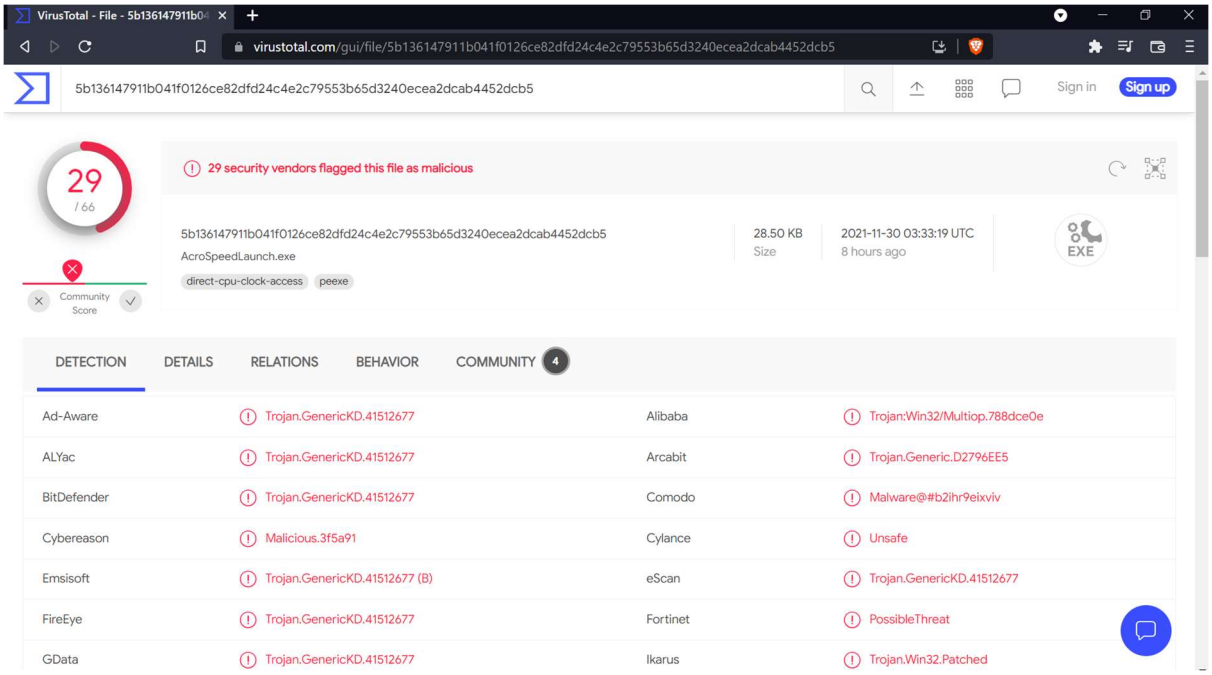
    NOTE: DO NOT DOUBLE CLICK OR RUN THIS NEWLY CREATED EXE/DUMP FILE!



12. Now, go to virustotal.com and upload this newly created exe file.







From the image above, we see that VirusTotal recognized this file as a Trojan malware. Thus, reader_sl.exe is a malware.

OBSERVATIONS

In the fifth image, we see that there is a process named “reader_sl.exe” with “explorer.exe” as its parent process. Upon checking the connections and sockets, we see in image 8 that its parent process 1484 makes a connection to some location with address 41.168.140:8080. This is a bit suspicious as the name says it is a process of Adobe Reader but there is no reason why Adobe reader would have to make a connection to some remote location.

Thus, this process’s dump was made and uploaded to VirusTotal which recognized this file as a malware.

CONCLUSION

We have used a memory image to figure out which process was the malware.