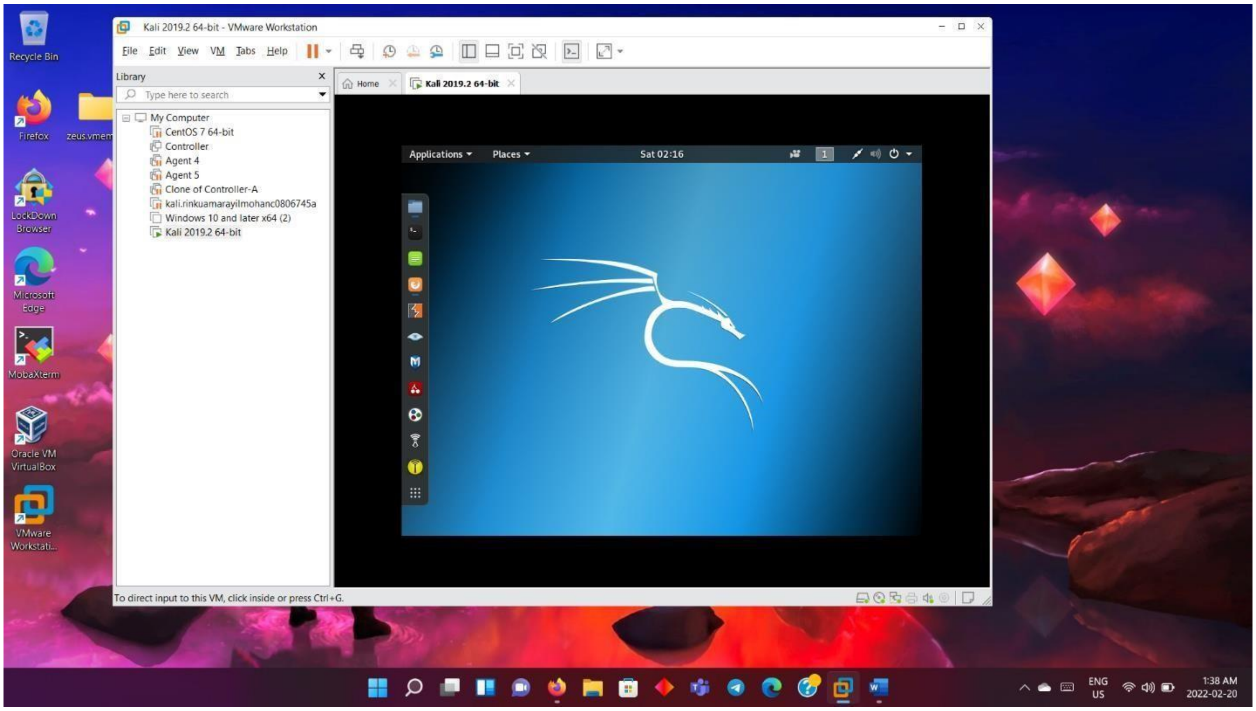
Table of Contents

Abstract

Volatility is an open-source memory forensics framework for incident response and malware analysis. It is used to analyze crash dumps, raw dumps, number of processes, process id's running. Volatility is a powerful tool and can be used to get a load of information regarding DLL files. In this activity we'll utilize volatility and its different commands to understand more about these files.

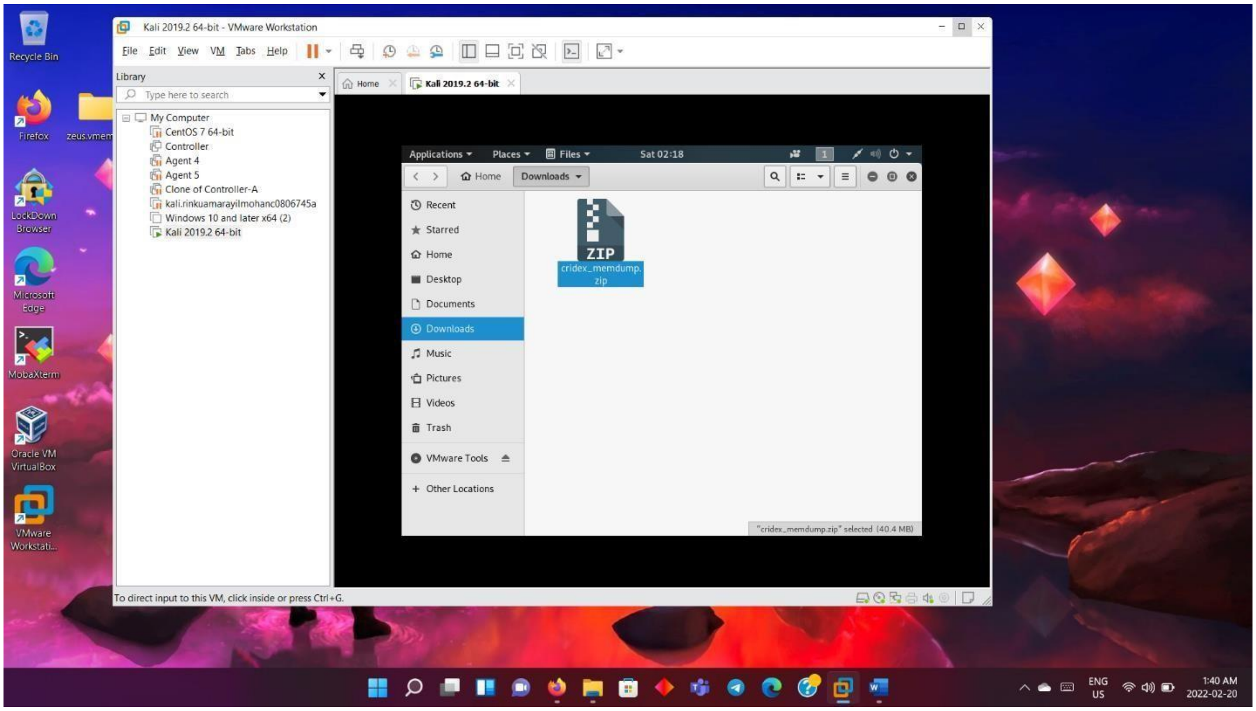
Part 1

Volatility Linux



To direct input to this VM, click inside or press Ctrl+G.

Installed and configured Kali linux 2019.2

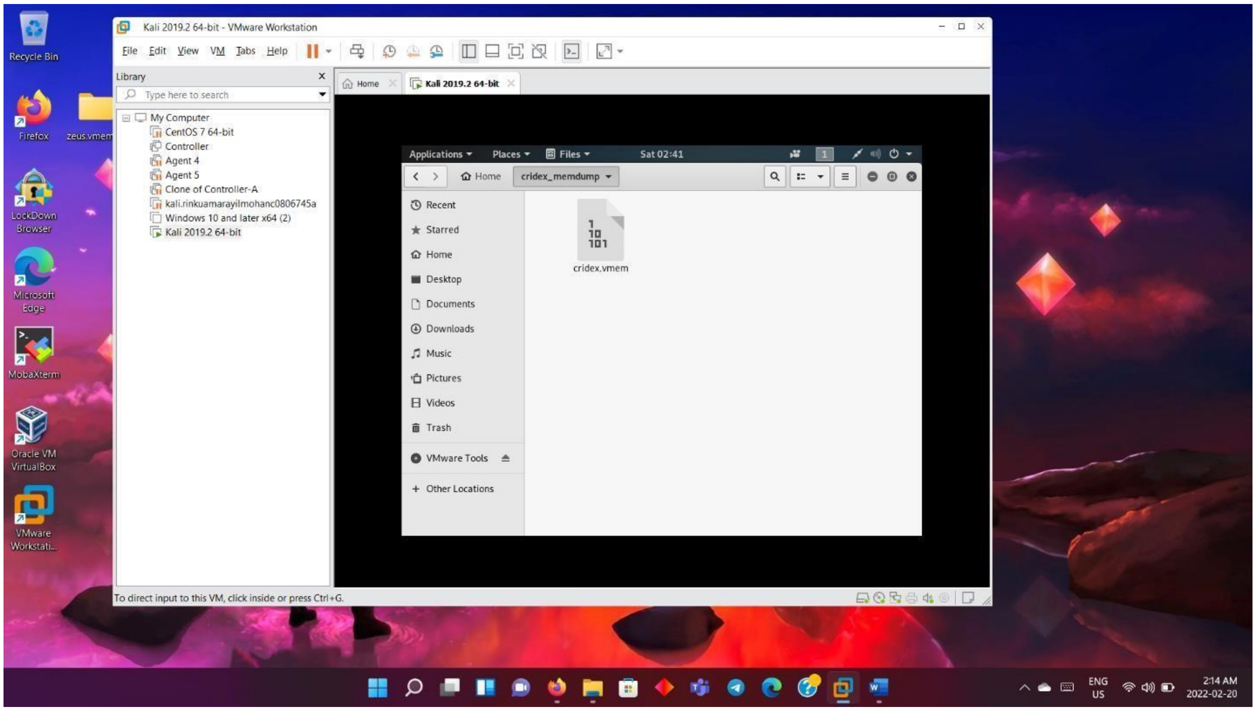


"cridex_memdump.zip" selected (40.4 MB)

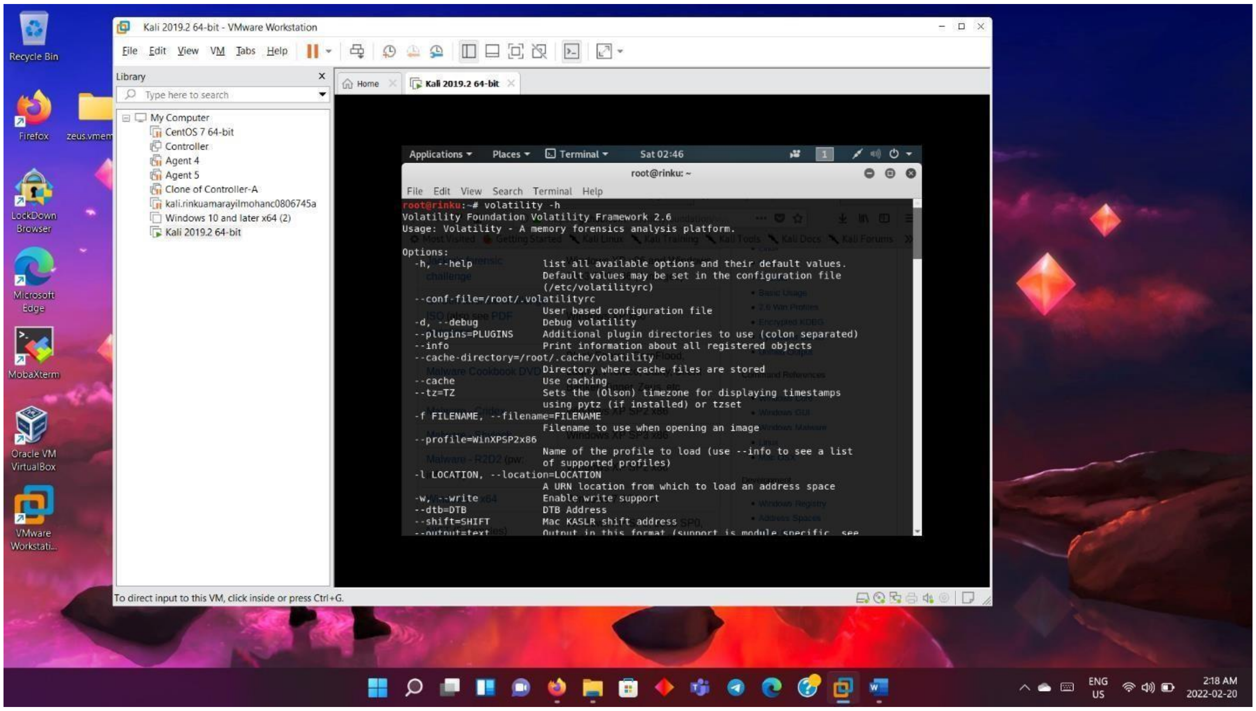
To direct input to this VM, click inside or press Ctrl+G.

Download the Cridex_memdump file on to the virtual machine.

Now move this file from downloads to the home folder and then extract to the same home folder.



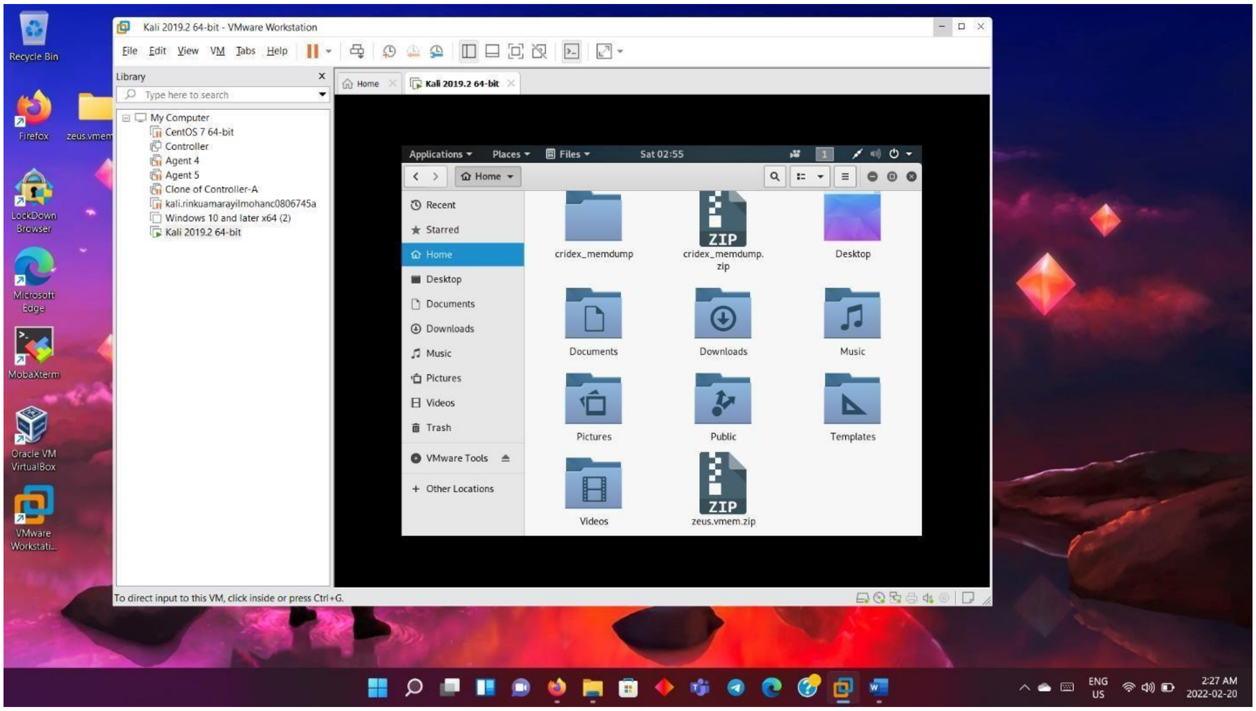
We can use the above tool to analyze.


Kali 2019.2 64-bit - VMware Workstation
Applications
Places
Terminal
Sat 02:46
root@rinku: ~
File Edit View Search Terminal Help
To direct input to this VM, click inside or press Ctrl+G.
2:18 AM
2022-02-20

```
root@rinku:~# volatility -h
Volatility Foundation Volatility Framework 2.6
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=/root/.volatilityrc
                        User based configuration file
  -d, --debug           Debug volatility
  --plugins=PLUGINS     Additional plugin directories to use (colon separated)
  --info                Print information about all registered objects
  --cache-directory=/root/.cache/volatility
                        Directory where cache files are stored
  --cache               Use caching
  --tz=TZ               Sets the (Olson) timezone for displaying timestamps
                        using pytz (if installed) or tzset
  -f FILENAME, --filename=FILENAME
                        Filename to use when opening an image
  --profile=WinXPSP2x86
                        Name of the profile to load (use --info to see a list
                        of supported profiles)
  -l LOCATION, --location=LOCATION
                        A URN location from which to load an address space
  -w, --write           Enable write support
  --dtb=DTB             DTB Address
  --shift=SHIFT         Mac KASLR shift address
  --output=text         Output in this format (support is module specific, see
```

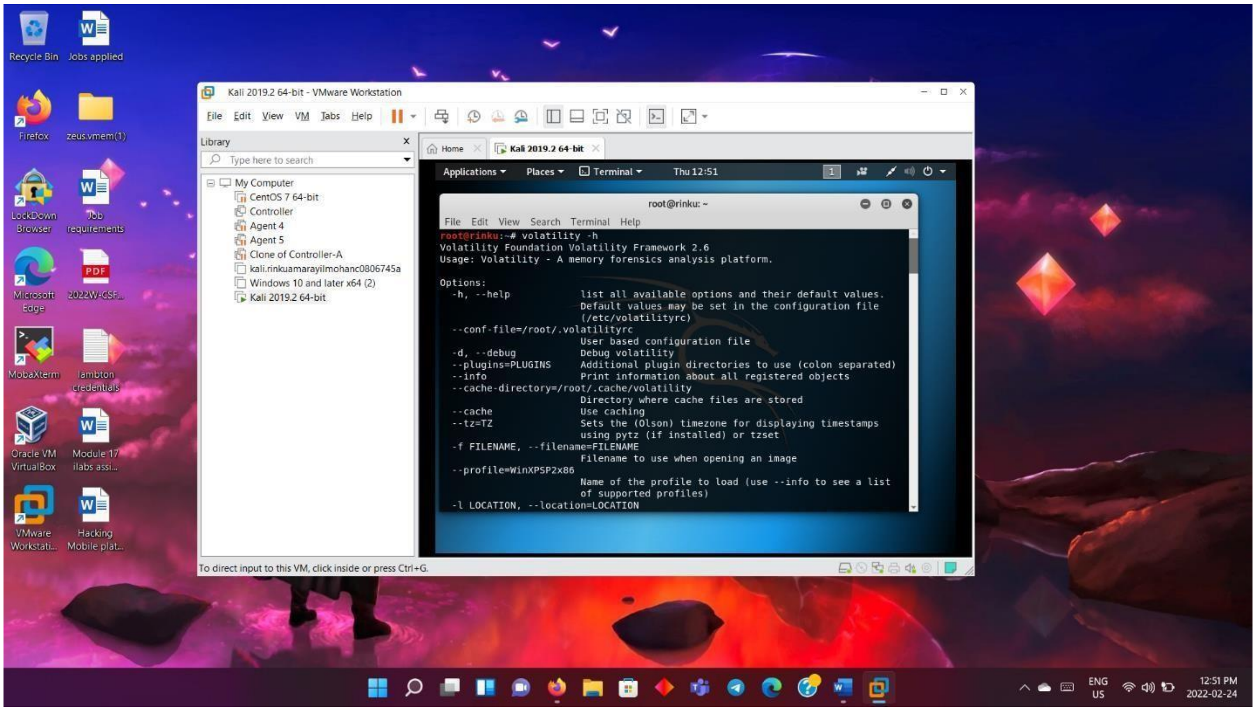
This is to check if the tool is up and running.

H gives detail of the image downloaded.



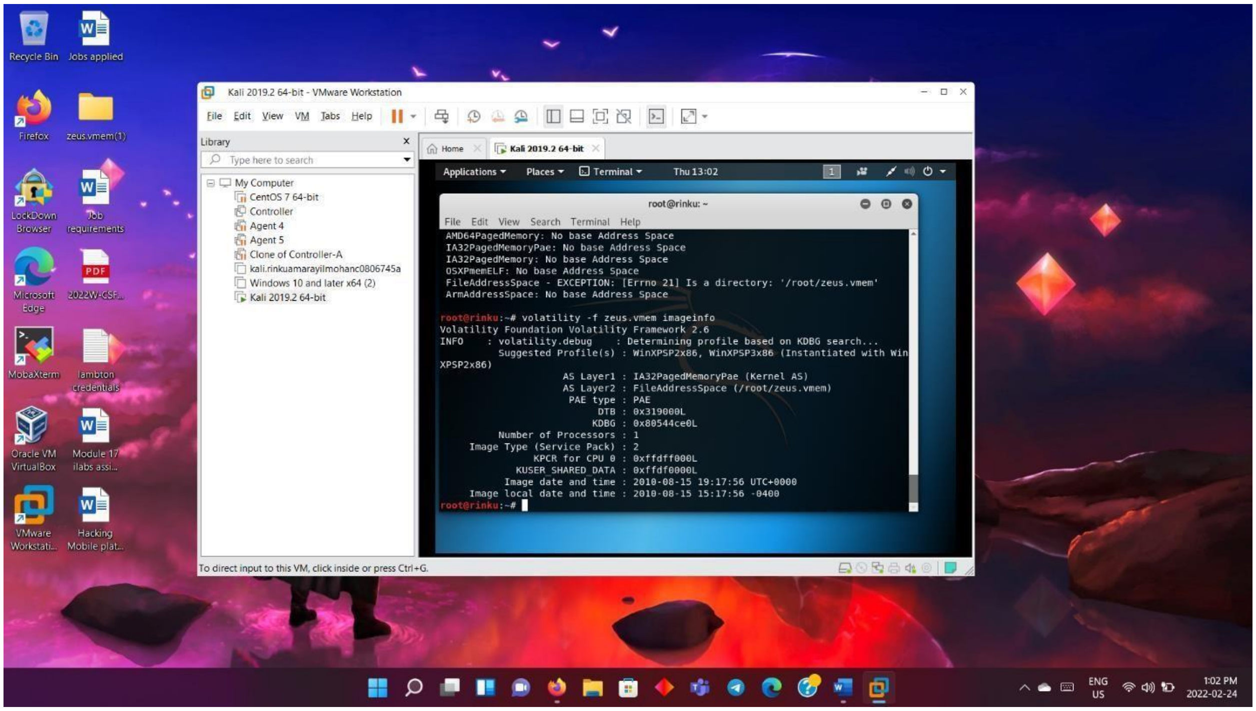
Downloaded zeus emem and stored under home folder.

Run **volatility -h** in the terminal.


```
root@rinku:~# volatility -h
Volatility Foundation Volatility Framework 2.6
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=/root/.volatilityrc
                        User based configuration file
  -d, --debug           Debug volatility
  --plugins=PLUGINS     Additional plugin directories to use (colon separated)
  --info                Print information about all registered objects
  --cache-directory=/root/.cache/volatility
                        Directory where cache files are stored
  --cache               Use caching
  --tz=TZ               Sets the (Olson) timezone for displaying timestamps
                        using pytz (if installed) or tzset
  -f FILENAME, --filename=FILENAME
                        Filename to use when opening an image
  --profile=WinXPSP2x86
                        Name of the profile to load (use --info to see a list
                        of supported profiles)
  -l LOCATION, --location=LOCATION
```
Kali 2019.2 64-bit - VMware Workstation
Applications
Places
Terminal
Thu 12:51
root@rinku: ~
File Edit View Search Terminal Help
To direct input to this VM, click inside or press Ctrl+G.
12:51 PM
2022-02-24

Run **volatility**

-f zeus.vmem imageinfo

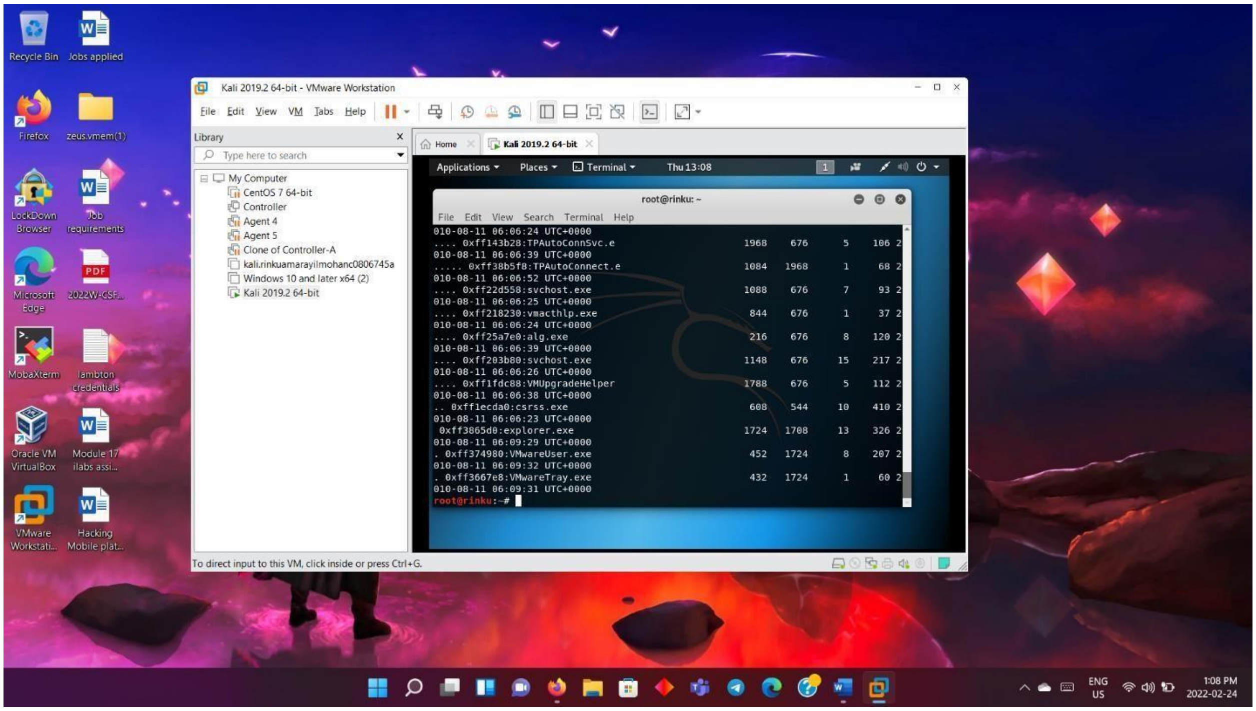


```
 AMD64PagedMemory: No base Address Space
 IA32PagedMemoryPae: No base Address Space
 IA32PagedMemory: No base Address Space
 OSXPmemELF: No base Address Space
 FileAddressSpace - EXCEPTION: [Errno 21] Is a directory: '/root/zeus.vmem'
 ArmAddressSpace: No base Address Space

root@rinku:~# volatility -f zeus.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with Win
XPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/root/zeus.vmem)
                      PAE type : PAE
                           DTB : 0x319000L
                          KDBG : 0x80544ce0L
          Number of Processors : 1
     Image Type (Service Pack) : 2
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2010-08-15 19:17:56 UTC+0000
     Image local date and time : 2010-08-15 15:17:56 -0400
root@rinku:~# 
```

This displays the information about the image.

Run **volatility Foundation volatility Framework 2.6**

Run **volatility**

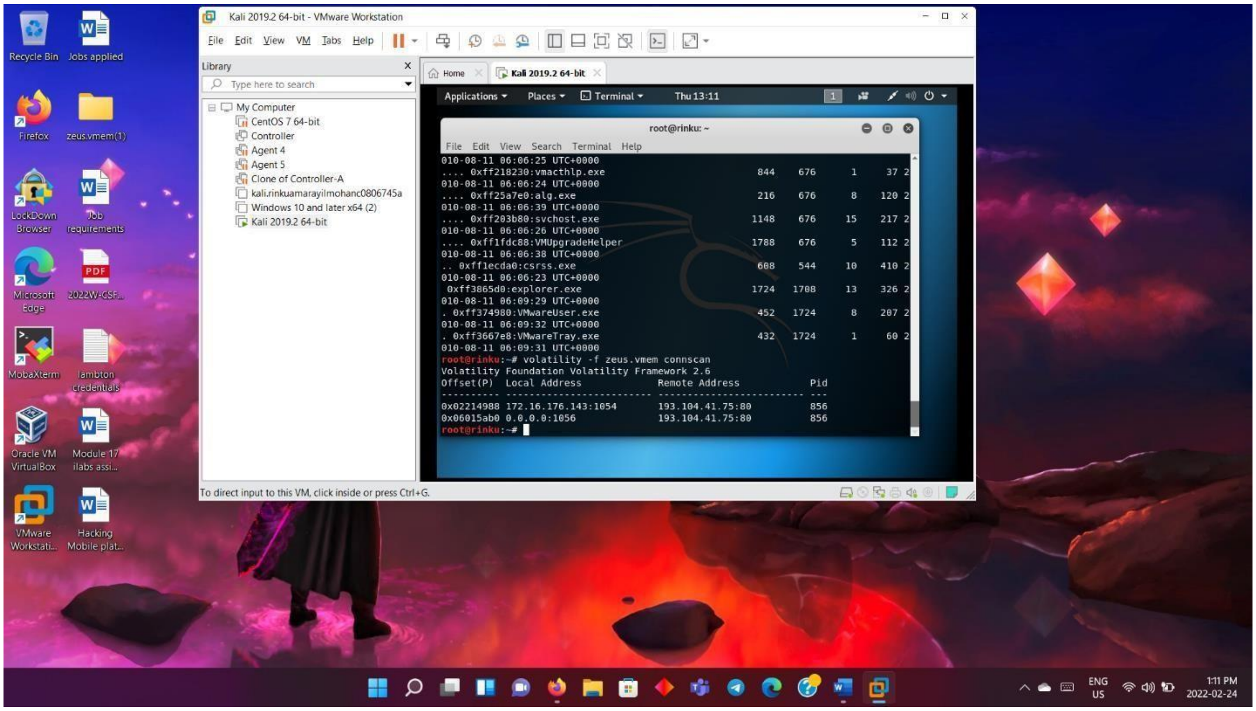

Kali 2019.2 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
CentOS 7 64-bit
Controller
Agent 4
Agent 5
Clone of Controller-A
kali.rinkuamarayilmohanc0806745a
Windows 10 and later x64 (2)
Kali 2019.2 64-bit
Home
Kali 2019.2 64-bit
Applications
Places
Terminal
Thu 13:08
root@rinku: ~
File Edit View Search Terminal Help
To direct input to this VM, click inside or press Ctrl+G.

```
010-08-11 06:06:24 UTC+0000
.... 0xff143b28:TPAutoConnSvc.e                    1968    676      5    106 2
010-08-11 06:06:39 UTC+0000
..... 0xff38b5f8:TPAutoConnect.e                   1084   1968      1     68 2
010-08-11 06:06:52 UTC+0000
.... 0xff22d558:svchost.exe                        1088    676      7     93 2
010-08-11 06:06:25 UTC+0000
.... 0xff218230:vmacthlp.exe                        844    676      1     37 2
010-08-11 06:06:24 UTC+0000
.... 0xff25a7e0:alg.exe                             216    676      8    120 2
010-08-11 06:06:39 UTC+0000
.... 0xff203b80:svchost.exe                        1148    676     15    217 2
010-08-11 06:06:26 UTC+0000
.... 0xff1fdc88:VMUpgradeHelper                    1788    676      5    112 2
010-08-11 06:06:38 UTC+0000
.. 0xff1ecda0:csrss.exe                             608    544     10    410 2
010-08-11 06:06:23 UTC+0000
 0xff3865d0:explorer.exe                           1724   1708     13    326 2
010-08-11 06:09:29 UTC+0000
. 0xff374980:VMwareUser.exe                         452   1724      8    207 2
010-08-11 06:09:32 UTC+0000
. 0xff3667e8:VMwareTray.exe                         432   1724      1     60 2
010-08-11 06:09:31 UTC+0000
root@rinku:~#
```

Gives the details of all process, process name pid, time, relation between child and parent, parent and child details.

-f zeus.vmem connscan

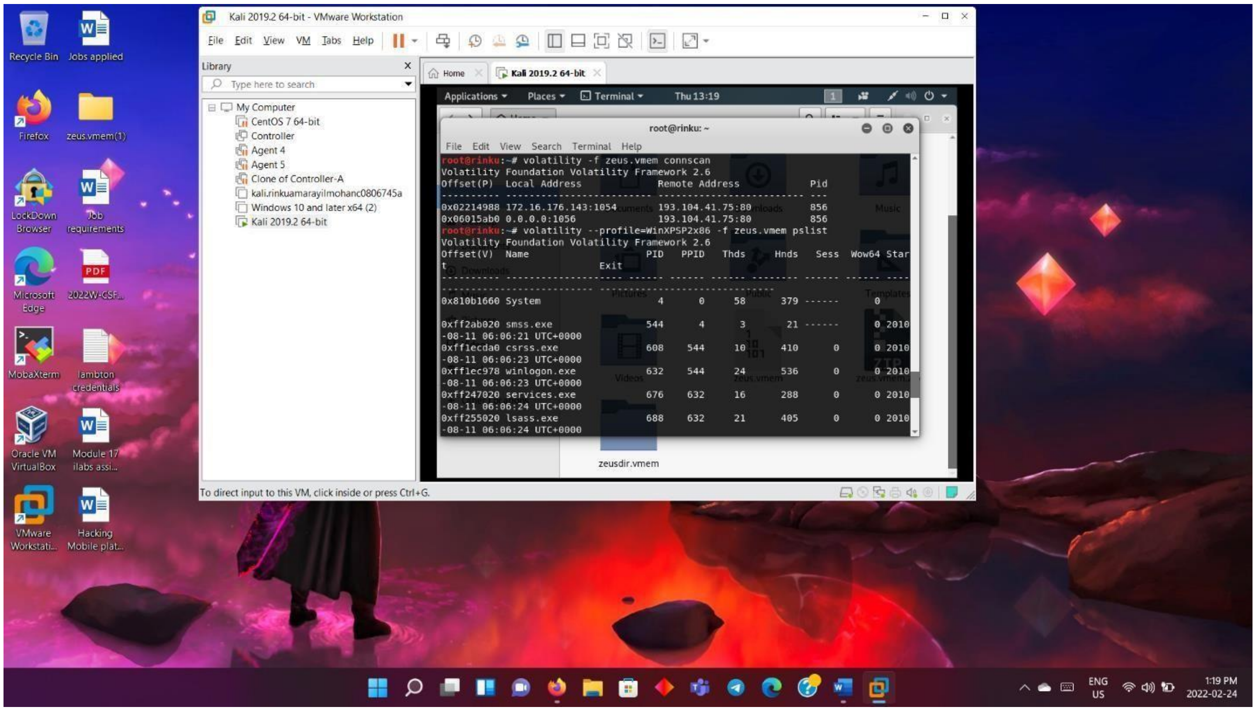
Run **volatility**



```
010-08-11 06:06:25 UTC+0000
.... 0xff218230:vmacthlp.exe                         844    676      1     37 2
010-08-11 06:06:24 UTC+0000
.... 0xff25a7e0:alg.exe                              216    676      8    120 2
010-08-11 06:06:39 UTC+0000
.... 0xff203b80:svchost.exe                         1148    676     15    217 2
010-08-11 06:06:26 UTC+0000
.... 0xff1fdc88:VMUpgradeHelper                     1788    676      5    112 2
010-08-11 06:06:38 UTC+0000
.. 0xff1ecda0:csrss.exe                              608    544     10    410 2
010-08-11 06:06:23 UTC+0000
 0xff3865d0:explorer.exe                            1724   1708     13    326 2
010-08-11 06:09:29 UTC+0000
. 0xff374980:VMwareUser.exe                          452   1724      8    207 2
010-08-11 06:09:32 UTC+0000
. 0xff3667e8:VMwareTray.exe                          432   1724      1     60 2
010-08-11 06:09:31 UTC+0000
root@rinku:~# volatility -f zeus.vmem connscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x02214988 172.16.176.143:1054       193.104.41.75:80          856
0x06015ab0 0.0.0.0:1056              193.104.41.75:80          856
root@rinku:~# 
```

This is to understand the remote connection between the host machines. It also provides the process ID.

Run **volatility –profile=WinXPSP2x86 -f zeus.vmem pslist**

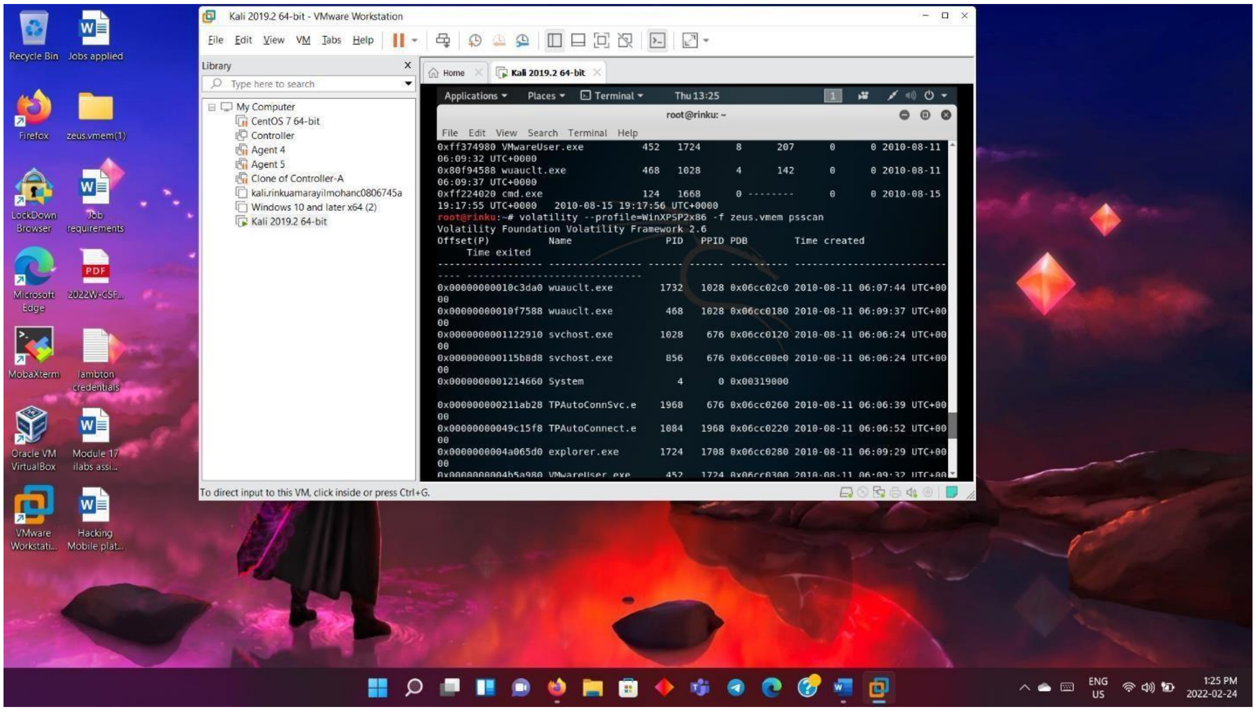


```
root@rinku:~# volatility -f zeus.vmem connscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x02214988 172.16.176.143:1054       193.104.41.75:80          856
0x06015ab0 0.0.0.0:1056              193.104.41.75:80          856
root@rinku:~# volatility --profile=WinXPSP2x86 -f zeus.vmem pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Star
t                           Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ----
------------------------------ ------------------------------
0x810b1660 System                    4      0     58      379 ------      0

0xff2ab020 smss.exe                544      4      3       21 ------      0 2010
-08-11 06:06:21 UTC+0000
0xff1ecda0 csrss.exe               608    544     10      410      0      0 2010
-08-11 06:06:23 UTC+0000
0xff1ec978 winlogon.exe            632    544     24      536      0      0 2010
-08-11 06:06:23 UTC+0000
0xff247020 services.exe            676    632     16      288      0      0 2010
-08-11 06:06:24 UTC+0000
0xff255020 lsass.exe               688    632     21      405      0      0 2010
-08-11 06:06:24 UTC+0000
```

Gives list of all running processes, parent process ID, also provides details of when the process started. **–profile=WinXPSP2x86 -f zeus.vmem psscan**

Run **volatility**

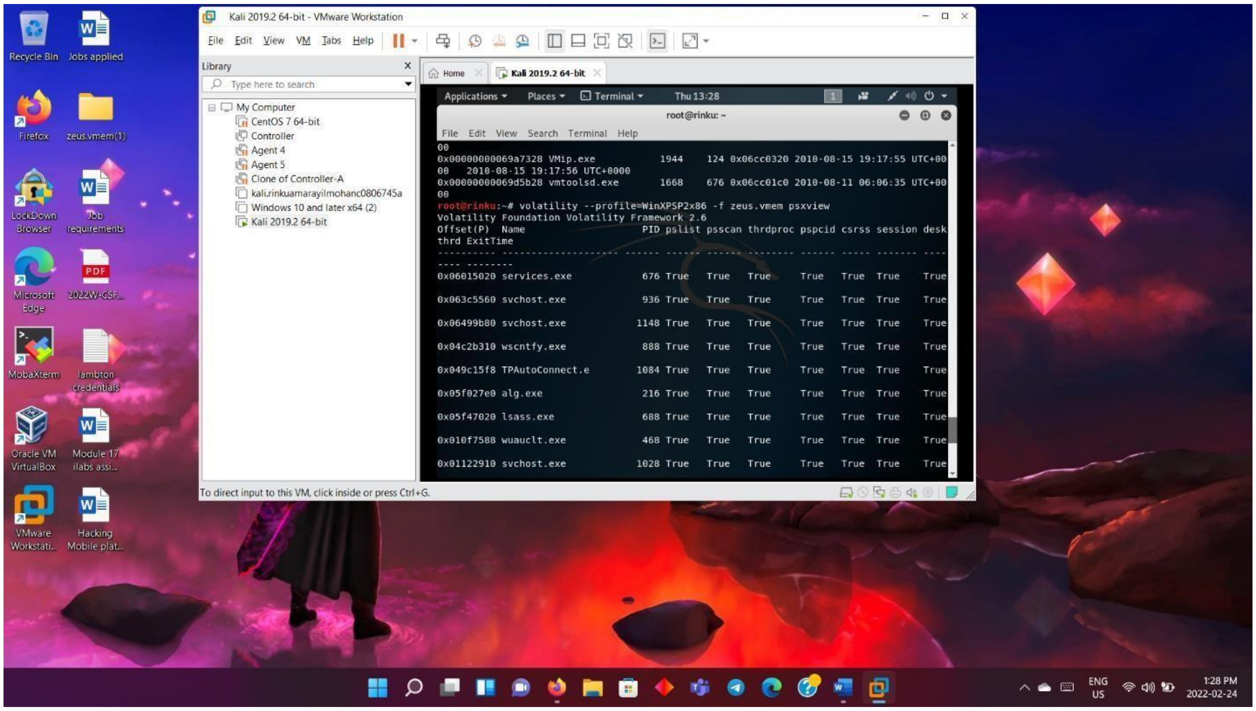
Provides details of hidden process, inactive process caused by malware like rootkit. By running this command, we get the mentioned details.



```
0xff374980 VMwareUser.exe         452   1724      8      207      0      0 2010-08-11
06:09:32 UTC+0000
0x80f94588 wuauclt.exe            468   1028      4      142      0      0 2010-08-11
06:09:37 UTC+0000
0xff224020 cmd.exe                124   1668      0 --------      0      0 2010-08-15
19:17:55 UTC+0000   2010-08-15 19:17:56 UTC+0000
root@rinku:~# volatility --profile=WinXPSP2x86 -f zeus.vmem psscan
Volatility Foundation Volatility Framework 2.6
Offset(P)          Name                PID   PPID PDB        Time created
     Time exited
------------------ ---------------- ------ ------ ---------- ------------------------
---- ------------------------------
0x00000000010c3da0 wuauclt.exe        1732   1028 0x06cc02c0 2010-08-11 06:07:44 UTC+00
00
0x00000000010f7588 wuauclt.exe         468   1028 0x06cc0180 2010-08-11 06:09:37 UTC+00
00
0x0000000001122910 svchost.exe        1028    676 0x06cc0120 2010-08-11 06:06:24 UTC+00
00
0x000000000115b8d8 svchost.exe         856    676 0x06cc00e0 2010-08-11 06:06:24 UTC+00
00
0x0000000001214660 System                4      0 0x00319000

0x000000000211ab28 TPAutoConnSvc.e    1968    676 0x06cc0260 2010-08-11 06:06:39 UTC+00
00
0x00000000049c15f8 TPAutoConnect.e    1084   1968 0x06cc0220 2010-08-11 06:06:52 UTC+00
00
0x0000000004a065d0 explorer.exe       1724   1708 0x06cc0280 2010-08-11 06:09:29 UTC+00
00
0x0000000004b5a980 VMwareUser.exe      452   1724 0x06cc0300 2010-08-11 06:09:32 UTC+00
```

Run **volatility –profile=WinXPSP2x86 -f zeus.vmem psxview**

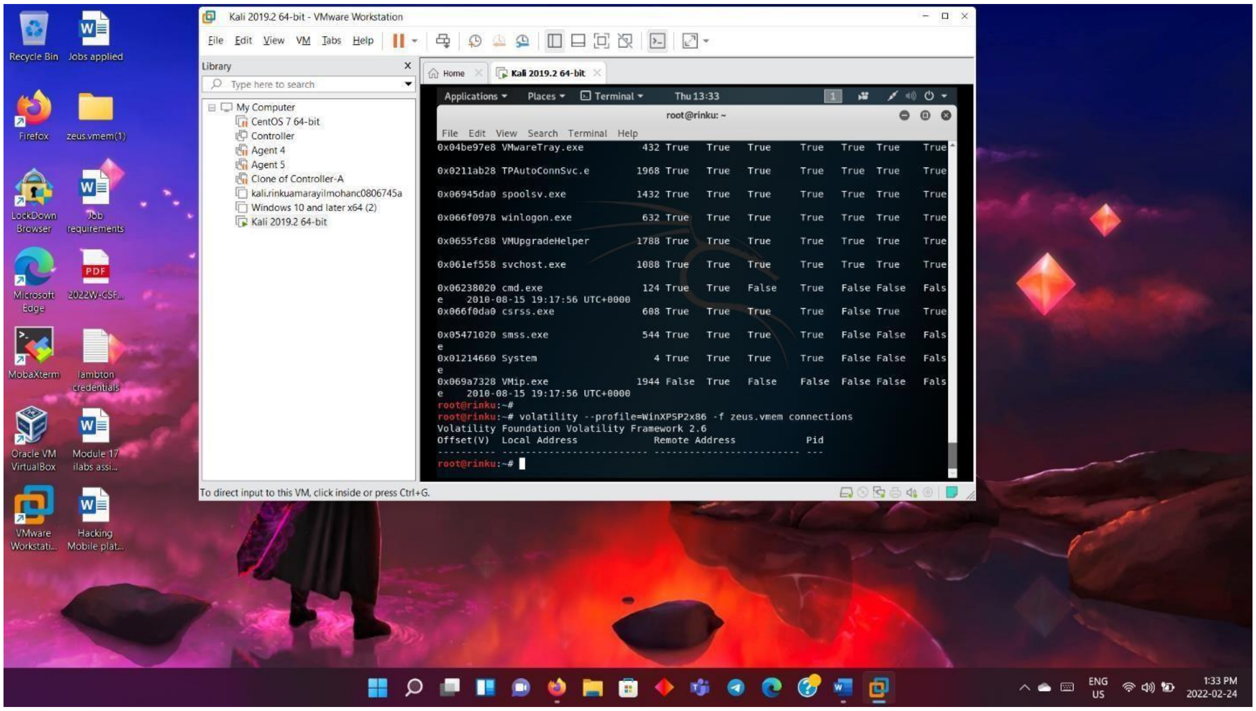
Run **volatility**



```
00
0x00000000069a7328 VMip.exe           1944    124 0x06cc0320 2010-08-15 19:17:55 UTC+00
00   2010-08-15 19:17:56 UTC+0000
0x00000000069d5b28 vmtoolsd.exe       1668    676 0x06cc01c0 2010-08-11 06:06:35 UTC+00
00
root@rinku:~# volatility --profile=WinXPSP2x86 -f zeus.vmem psxview
Volatility Foundation Volatility Framework 2.6
Offset(P)  Name                    PID pslist psscan thrdproc pspcid csrss session desk
thrd ExitTime
---------- -------------------- ------ ------ ------ -------- ------ ----- ------- ----
---- --------
0x06015020 services.exe            676 True   True   True     True   True  True    True

0x063c5560 svchost.exe             936 True   True   True     True   True  True    True

0x06499b80 svchost.exe            1148 True   True   True     True   True  True    True

0x04c2b310 wscntfy.exe             888 True   True   True     True   True  True    True

0x049c15f8 TPAutoConnect.e        1084 True   True   True     True   True  True    True

0x05f027e0 alg.exe                 216 True   True   True     True   True  True    True

0x05f47020 lsass.exe               688 True   True   True     True   True  True    True

0x010f7588 wuauclt.exe             468 True   True   True     True   True  True    True

0x01122910 svchost.exe            1028 True   True   True     True   True  True    True
```

It gives true and false value; false value gives attention of malware or possibility.

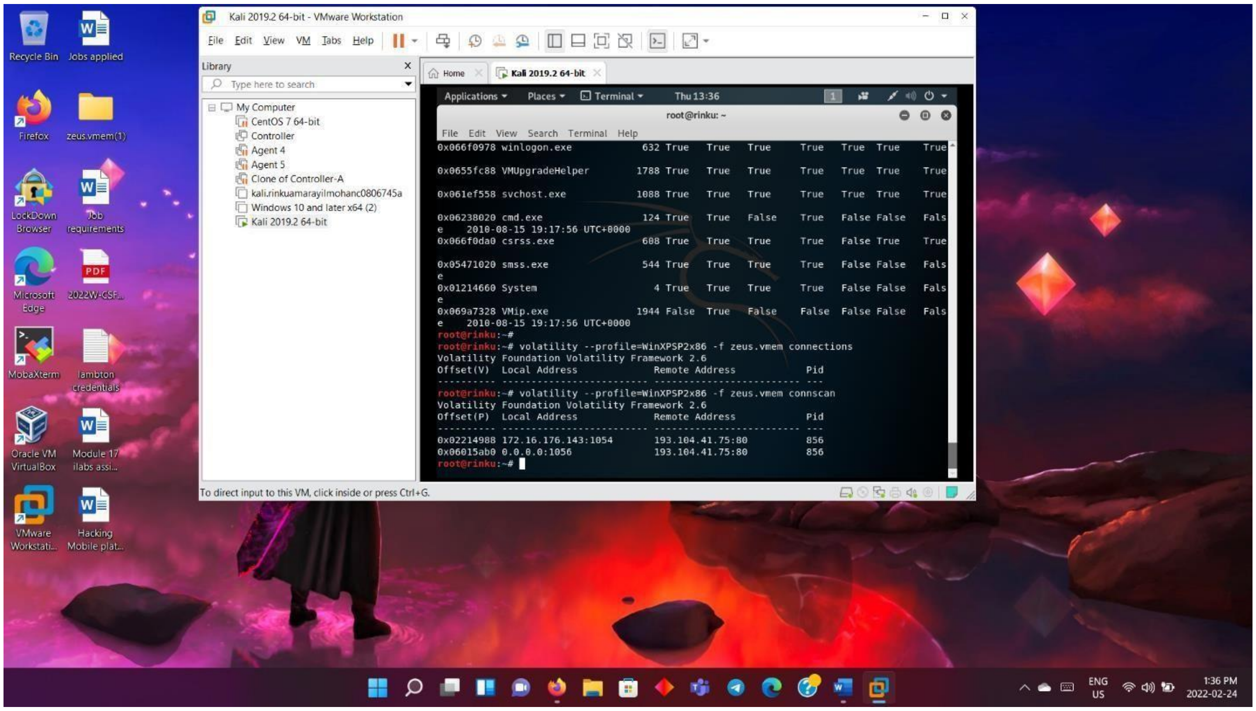
Now run **volatility –profile=WinXPSP2x86 -f zeus.vmem connections**



```
0x04be97e8 VMwareTray.exe          432 True   True   True    True   True  True    True

0x0211ab28 TPAutoConnSvc.e        1968 True   True   True    True   True  True    True

0x06945da0 spoolsv.exe            1432 True   True   True    True   True  True    True

0x066f0978 winlogon.exe            632 True   True   True    True   True  True    True

0x0655fc88 VMUpgradeHelper        1788 True   True   True    True   True  True    True

0x061ef558 svchost.exe            1088 True   True   True    True   True  True    True

0x06238020 cmd.exe                 124 True   True   False   True   False False   Fals
e    2010-08-15 19:17:56 UTC+0000
0x066f0da0 csrss.exe               608 True   True   True    True   False True    True

0x05471020 smss.exe                544 True   True   True    True   False False   Fals
e
0x01214660 System                    4 True   True   True    True   False False   Fals
e
0x069a7328 VMip.exe               1944 False  True   False   False  False False   Fals
e    2010-08-15 19:17:56 UTC+0000
root@rinku:~#
root@rinku:~# volatility --profile=WinXPSP2x86 -f zeus.vmem connections
Volatility Foundation Volatility Framework 2.6
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
root@rinku:~# 
```

It provides active connections during memory dump.

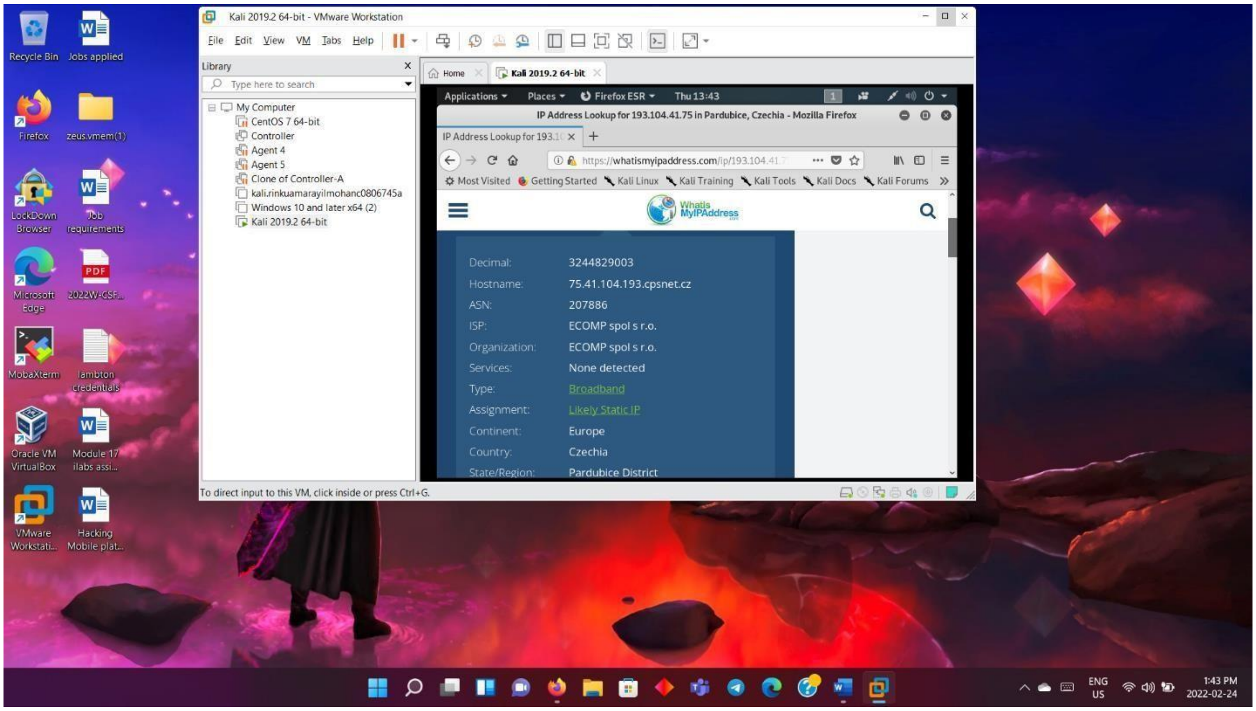
Run **volatility –profile=WinXPSP2x86 -f zeus.vmem connscan**



```
0x066f0978 winlogon.exe            632 True   True   True    True   True  True    True

0x0655fc88 VMUpgradeHelper        1788 True   True   True    True   True  True    True

0x061ef558 svchost.exe            1088 True   True   True    True   True  True    True

0x06238020 cmd.exe                 124 True   True   False   True   False False   Fals
e    2010-08-15 19:17:56 UTC+0000
0x066f0da0 csrss.exe               608 True   True   True    True   False True    True

0x05471020 smss.exe                544 True   True   True    True   False False   Fals
e
0x01214660 System                    4 True   True   True    True   False False   Fals
e
0x069a7328 VMip.exe               1944 False  True   False   False  False False   Fals
e    2010-08-15 19:17:56 UTC+0000
root@rinku:~#
root@rinku:~# volatility --profile=WinXPSP2x86 -f zeus.vmem connections
Volatility Foundation Volatility Framework 2.6
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
root@rinku:~# volatility --profile=WinXPSP2x86 -f zeus.vmem connscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x02214988 172.16.176.143:1054       193.104.41.75:80          856
0x06015ab0 0.0.0.0:1056              193.104.41.75:80          856
root@rinku:~# 
```

It provides IP and local address, along with the process id, to prove that the connection was successfully established.

We can get the details of this IP by looking into the website https://whatismyipaddress.com We get the below details.



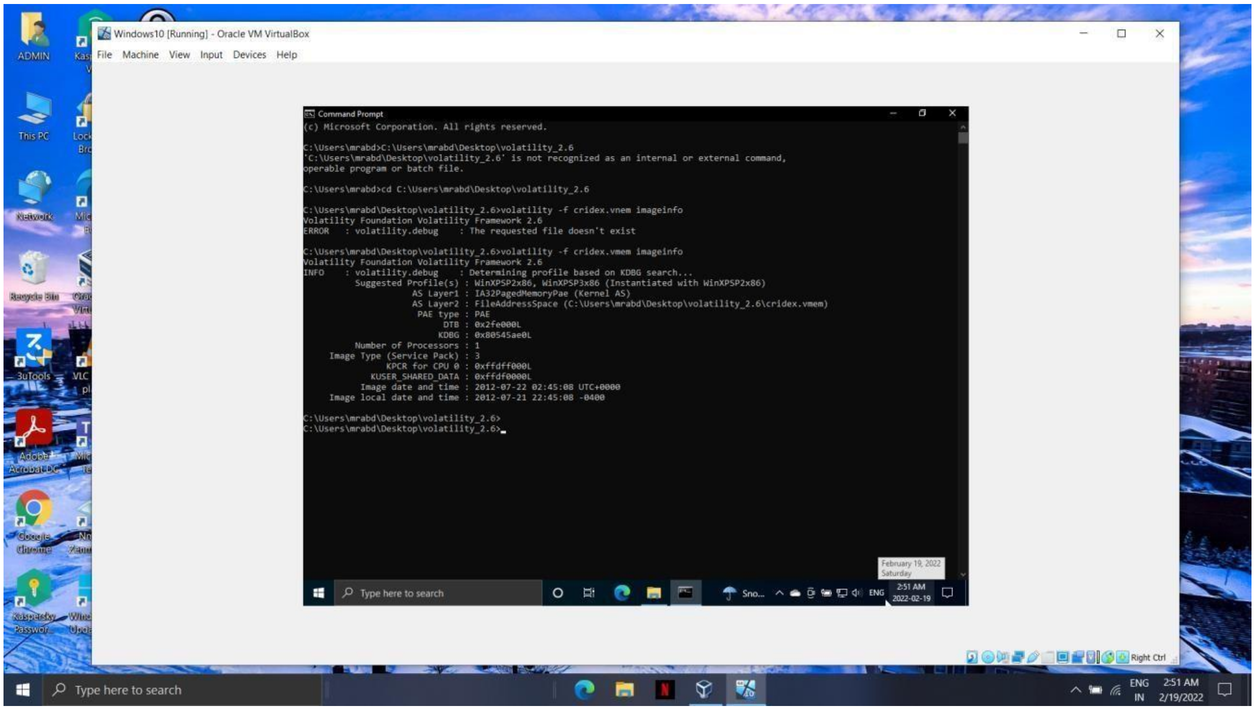
Decimal: 3244829003
Hostname: 75.41.104.193.cpsnet.cz
ASN: 207886
ISP: ECOMP spol s r.o.
Organization: ECOMP spol s r.o.
Services: None detected
Type: Broadband
Assignment: Likely Static IP
Continent: Europe
Country: Czechia
State/Region: Pardubice District

It gives the host name, country, location information, broadband. Map.

Part 2

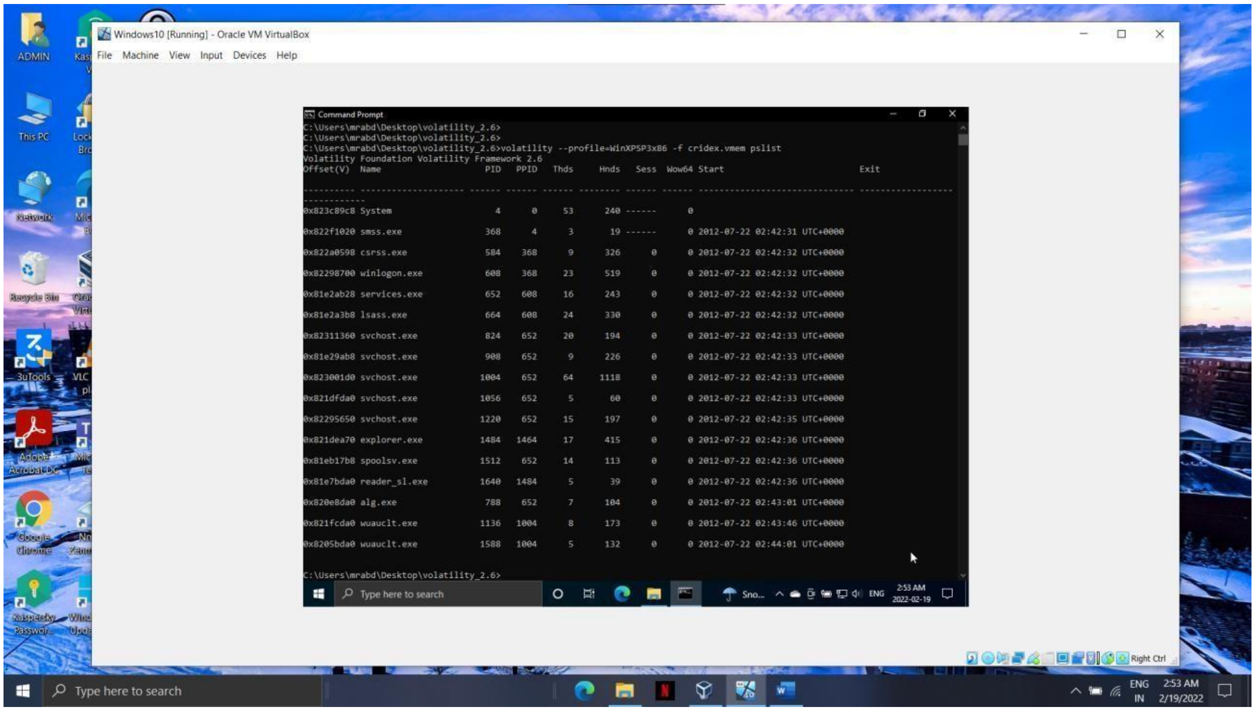
Volatility Windows

To view image information



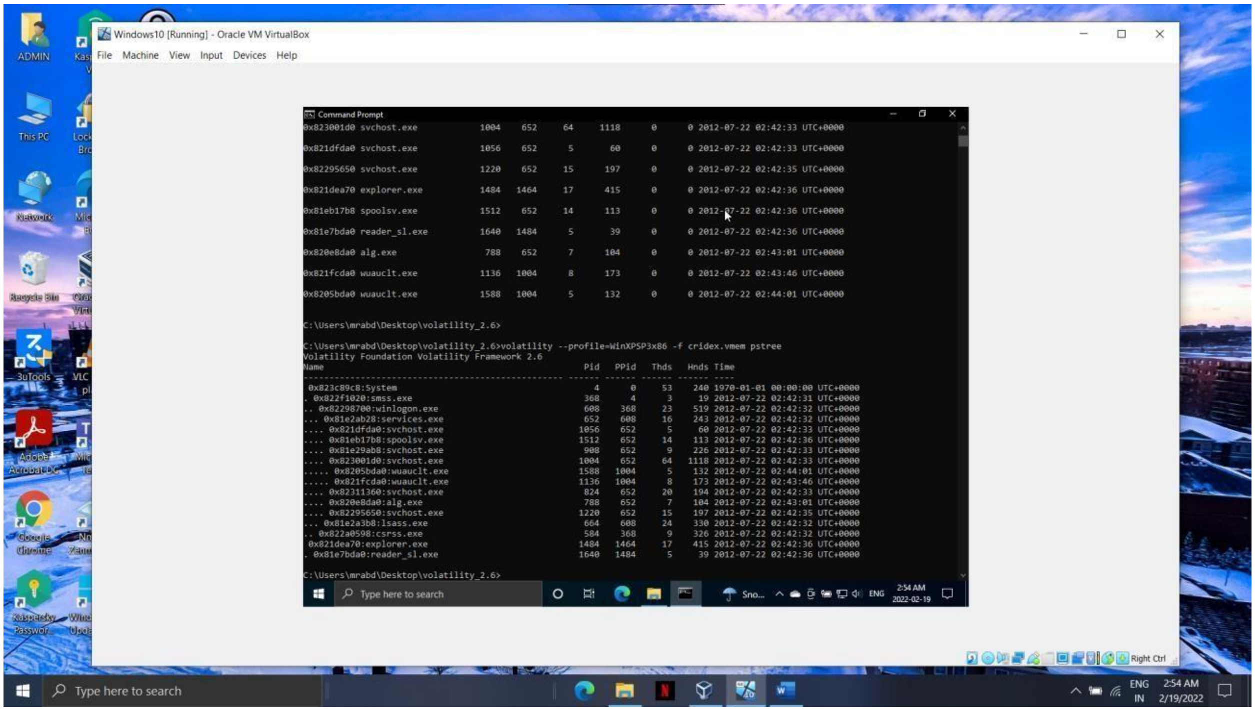
```
(c) Microsoft Corporation. All rights reserved.

C:\Users\mrabd>C:\Users\mrabd\Desktop\volatility_2.6
'C:\Users\mrabd\Desktop\volatility_2.6' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\mrabd>cd C:\Users\mrabd\Desktop\volatility_2.6

C:\Users\mrabd\Desktop\volatility_2.6>volatility -f cridex.vnem imageinfo
Volatility Foundation Volatility Framework 2.6
ERROR   : volatility.debug    : The requested file doesn't exist

C:\Users\mrabd\Desktop\volatility_2.6>volatility -f cridex.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\Users\mrabd\Desktop\volatility_2.6\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:\Users\mrabd\Desktop\volatility_2.6>
C:\Users\mrabd\Desktop\volatility_2.6>
```

To view process list


Windows10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Command Prompt
Type here to search
2:53 AM
2022-02-19
2:53 AM
2/19/2022

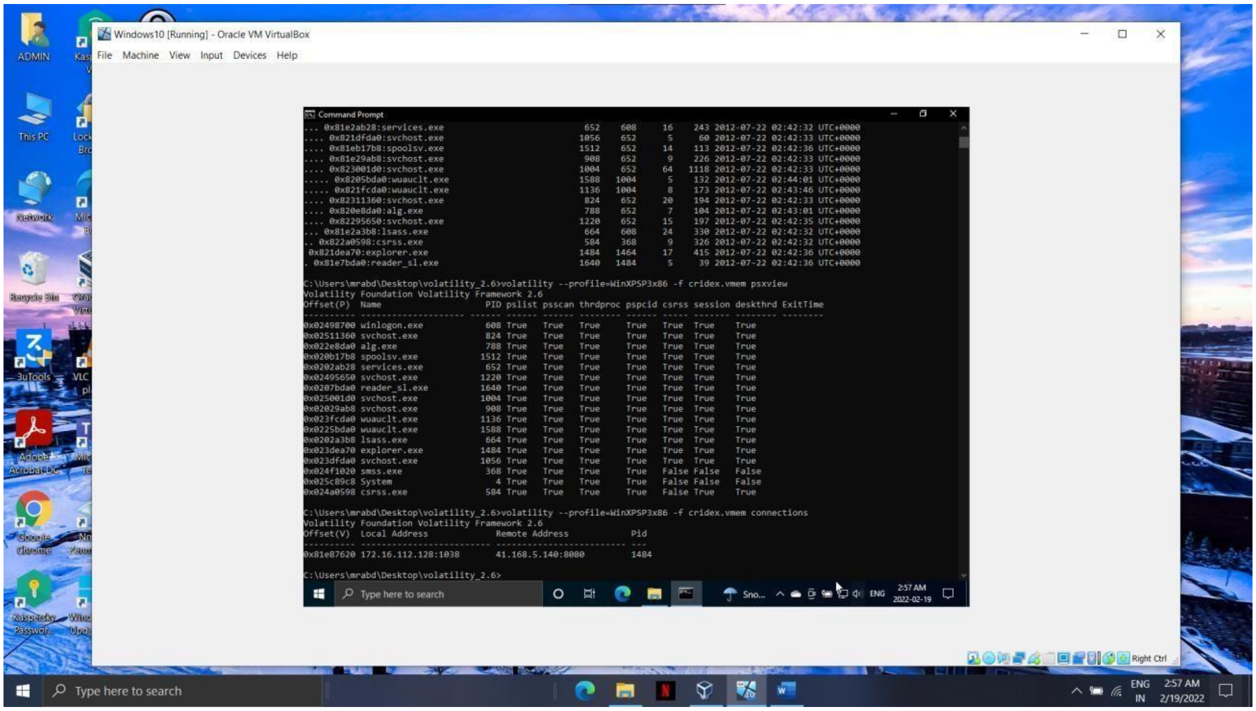
```
C:\Users\mrabd\Desktop\volatility_2.6>
C:\Users\mrabd\Desktop\volatility_2.6>
C:\Users\mrabd\Desktop\volatility_2.6>volatility --profile=WinXPSP3x86 -f cridex.vmem pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          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:\Users\mrabd\Desktop\volatility_2.6>
```

To check process legitimacy


Windows10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Command Prompt
Type here to search
2:54 AM
2022-02-19
2/19/2022
Right Ctrl

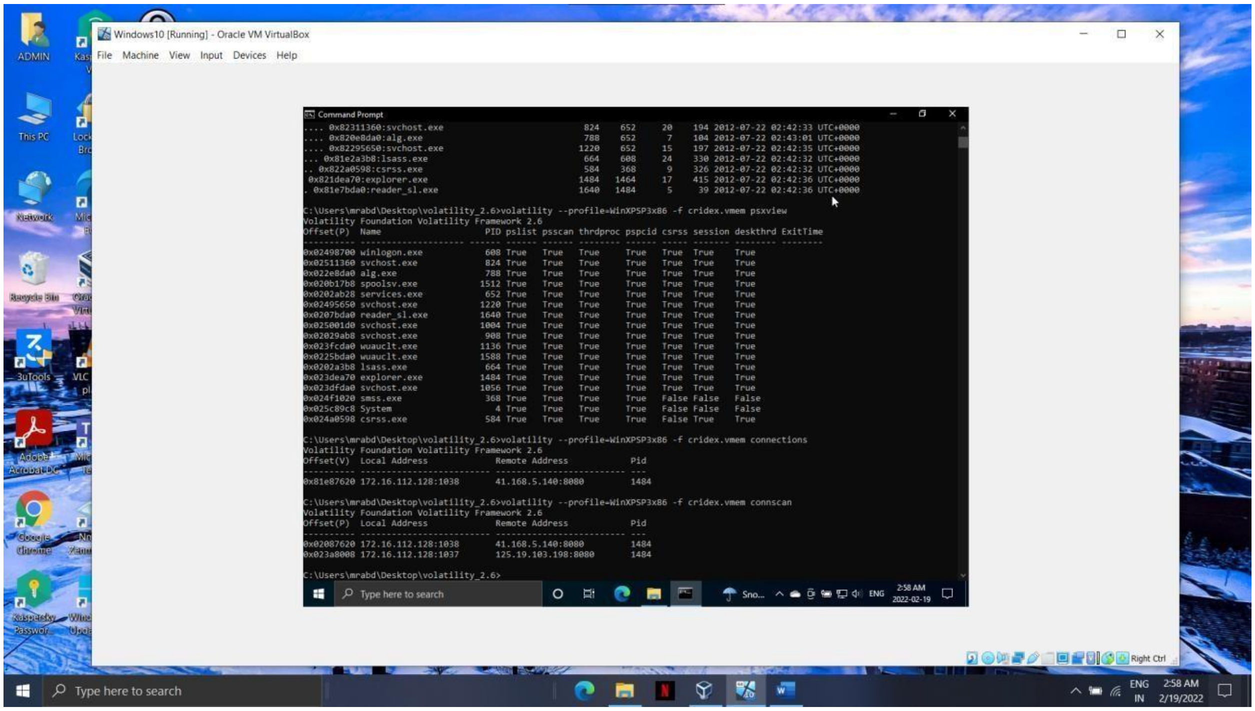
```
0x823001d0 svchost.exe           1004    652     64     1118      0      0 2012-07-22 02:42:33 UTC+0000

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:\Users\mrabd\Desktop\volatility_2.6>

C:\Users\mrabd\Desktop\volatility_2.6>volatility --profile=WinXPSP3x86 -f cridex.vmem pstree
Volatility Foundation Volatility Framework 2.6
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:\Users\mrabd\Desktop\volatility_2.6>
```

To view connections


Windows10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Command Prompt
Type here to search
2:57 AM
2022-02-19
2/19/2022
Right Ctrl

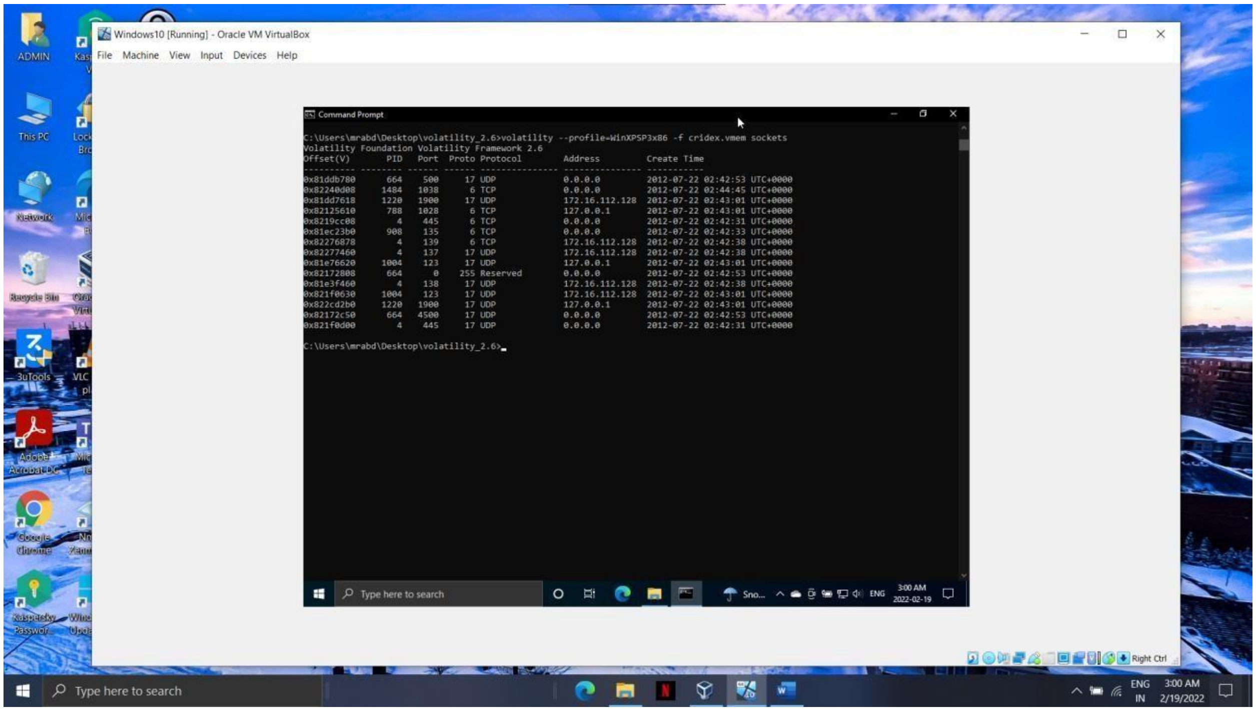
```
... 0x81e2ab28:services.exe                           652    608     16    243 2012-07-22 02:42:32 UTC+0000
.... 0x821dfda0:svchost.exe                          1056    652      5     60 2012-07-22 02:42:33 UTC+0000
.... 0x81eb17b8:spoolsv.exe                          1512    652     14    113 2012-07-22 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:\Users\mrabd\Desktop\volatility_2.6>volatility --profile=WinXPSP3x86 -f cridex.vmem psxview
Volatility Foundation Volatility Framework 2.6
Offset(P)  Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
---------- -------------------- ------ ------ ------ -------- ------ ----- ------- -------- --------
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

C:\Users\mrabd\Desktop\volatility_2.6>volatility --profile=WinXPSP3x86 -f cridex.vmem connections
Volatility Foundation Volatility Framework 2.6
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x81e87620 172.16.112.128:1038       41.168.5.140:8080         1484

C:\Users\mrabd\Desktop\volatility_2.6>
```

To view remote connections



```
.... 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:\Users\mrabd\Desktop\volatility_2.6>volatility --profile=WinXPSP3x86 -f cridex.vmem psxview
Volatility Foundation Volatility Framework 2.6
Offset(P)  Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
---------- -------------------- ------ ------ ------ -------- ------ ----- ------- -------- --------
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

C:\Users\mrabd\Desktop\volatility_2.6>volatility --profile=WinXPSP3x86 -f cridex.vmem connections
Volatility Foundation Volatility Framework 2.6
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x81e87620 172.16.112.128:1038       41.168.5.140:8080         1484

C:\Users\mrabd\Desktop\volatility_2.6>volatility --profile=WinXPSP3x86 -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

C:\Users\mrabd\Desktop\volatility_2.6>
```

To view protocols



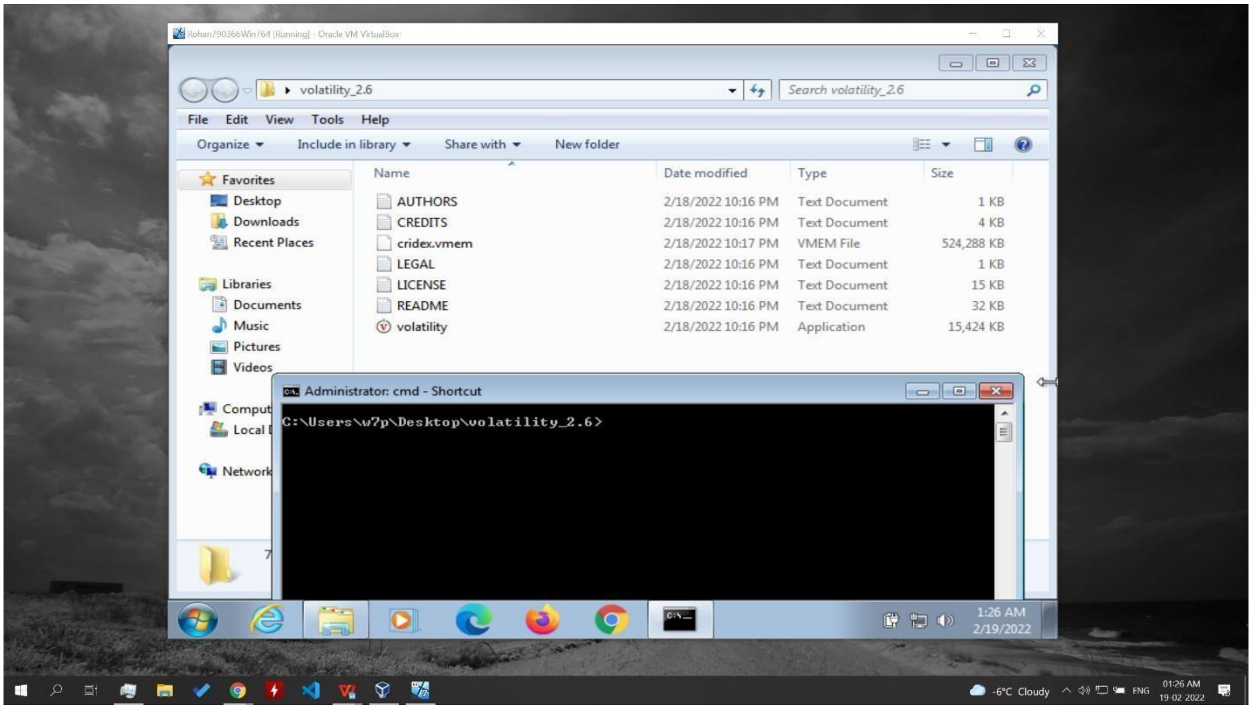
```
C:\Users\mrabd\Desktop\volatility_2.6>volatility --profile=WinXPSP3x86 -f cridex.vmem sockets
Volatility Foundation Volatility Framework 2.6
Offset(V)       PID   Port  Proto Protocol        Address         Create Time
---------- -------- ------ ------ --------------- --------------- -----------
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:\Users\mrabd\Desktop\volatility_2.6>
```

Part 3

Dll Volatility

DLL (Dynamic-link Library) is a file that contains code which is used by multiple programs simultaneously.

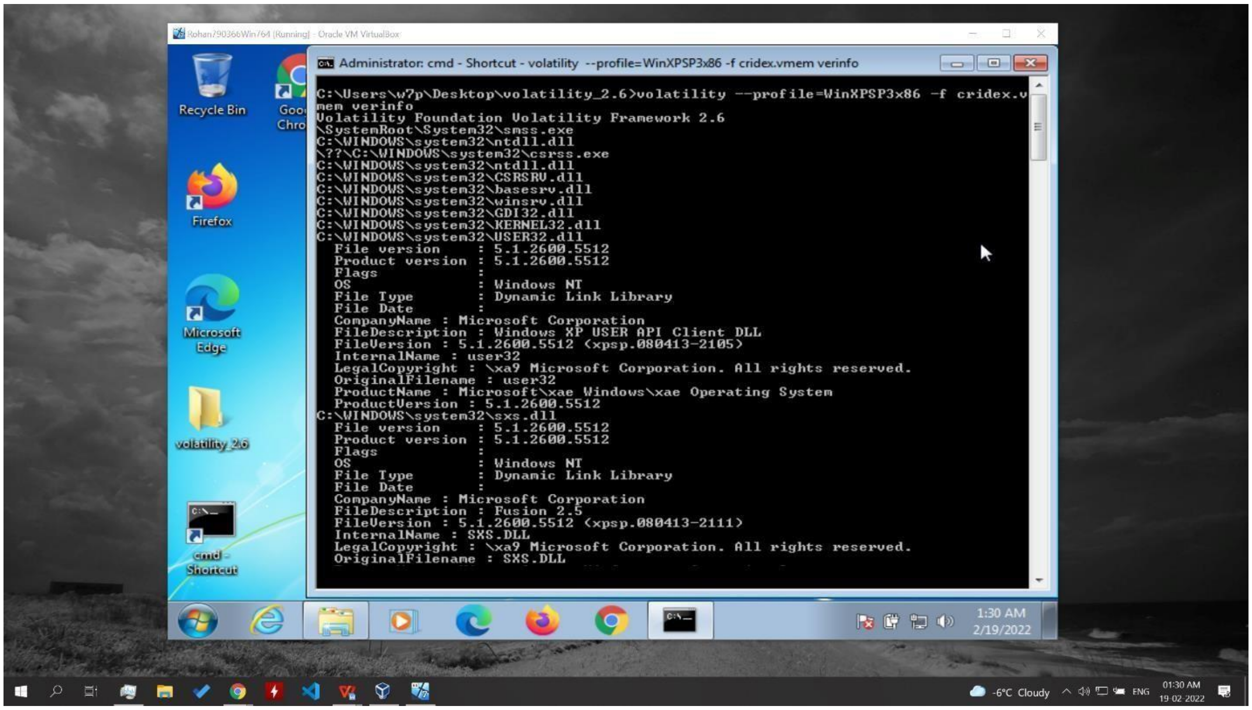
Step 1 : Extract volatility in Windows 7 VM



Name	Date modified	Type	Size
AUTHORS	2/18/2022 10:16 PM	Text Document	1 KB
CREDITS	2/18/2022 10:16 PM	Text Document	4 KB
cridex.vmem	2/18/2022 10:17 PM	VMEM File	524,288 KB
LEGAL	2/18/2022 10:16 PM	Text Document	1 KB
LICENSE	2/18/2022 10:16 PM	Text Document	15 KB
README	2/18/2022 10:16 PM	Text Document	32 KB
volatility	2/18/2022 10:16 PM	Application	15,424 KB

```
C:\Users\w7p\Desktop\volatility_2.6>
```

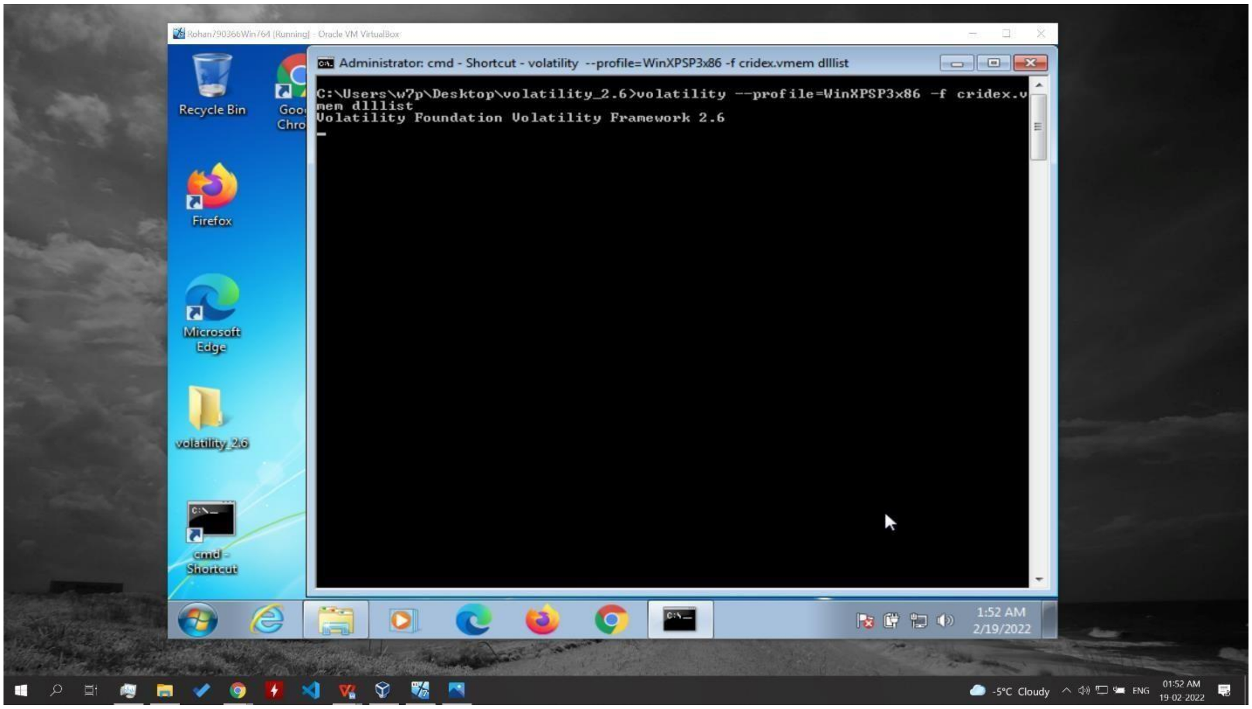
Step 2 : Run the *volatility --profile=WinXPSP3x86 -f cridex.vmem verinfo* command to display information about the .dll files, such as their version, creator company, OS, etc.



Administrator: cmd - Shortcut - volatility --profile=WinXPSP3x86 -f cridex.vmem verinfo

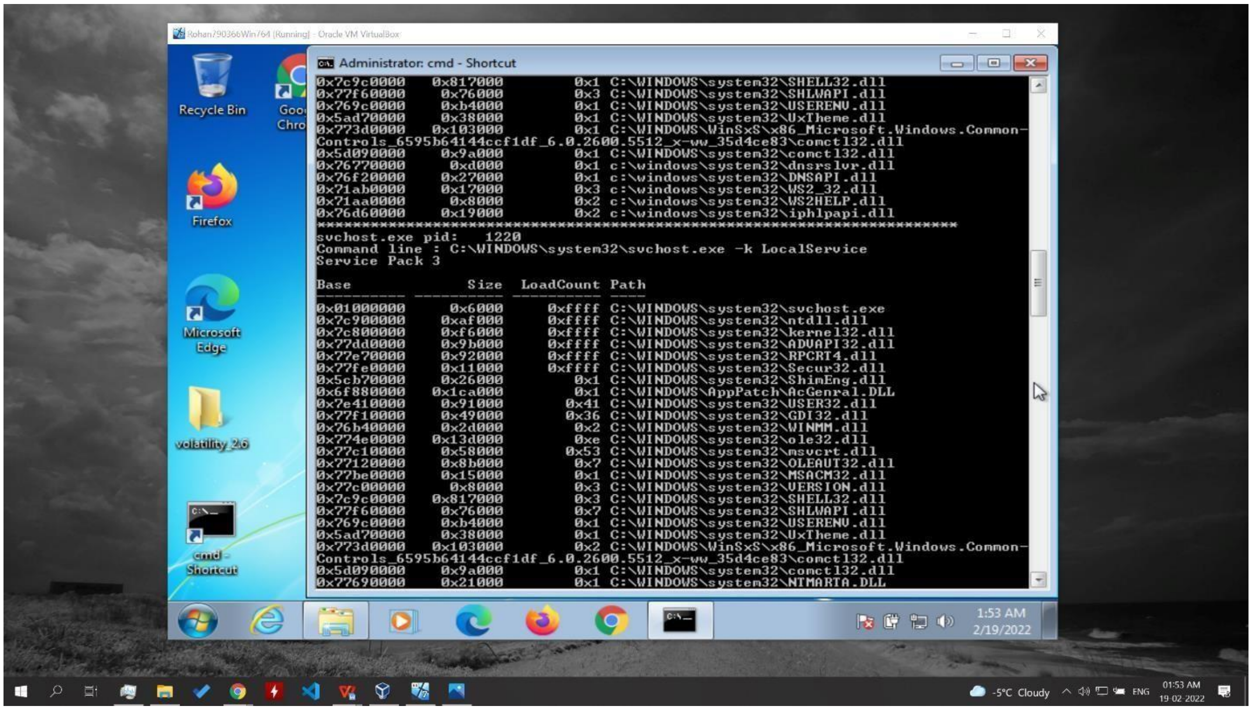
```
C:\Users\w7p\Desktop\volatility_2.6>volatility --profile=WinXPSP3x86 -f cridex.v
mem verinfo
Volatility Foundation Volatility Framework 2.6
\SystemRoot\System32\smss.exe
C:\WINDOWS\system32\ntdll.dll
\??\C:\WINDOWS\system32\csrss.exe
C:\WINDOWS\system32\ntdll.dll
C:\WINDOWS\system32\CSRSRV.dll
C:\WINDOWS\system32\basesrv.dll
C:\WINDOWS\system32\winsrv.dll
C:\WINDOWS\system32\GDI32.dll
C:\WINDOWS\system32\KERNEL32.dll
C:\WINDOWS\system32\USER32.dll
  File version    : 5.1.2600.5512
  Product version : 5.1.2600.5512
  Flags           :
  OS              : Windows NT
  File Type       : Dynamic Link Library
  File Date       :
  CompanyName : Microsoft Corporation
  FileDescription : Windows XP USER API Client DLL
  FileVersion : 5.1.2600.5512 (xpsp.080413-2105)
  InternalName : user32
  LegalCopyright : \xa9 Microsoft Corporation. All rights reserved.
  OriginalFilename : user32
  ProductName : Microsoft\xae Windows\xae Operating System
  ProductVersion : 5.1.2600.5512
C:\WINDOWS\system32\sxs.dll
  File version    : 5.1.2600.5512
  Product version : 5.1.2600.5512
  Flags           :
  OS              : Windows NT
  File Type       : Dynamic Link Library
  File Date       :
  CompanyName : Microsoft Corporation
  FileDescription : Fusion 2.5
  FileVersion : 5.1.2600.5512 (xpsp.080413-2111)
  InternalName : SXS.DLL
  LegalCopyright : \xa9 Microsoft Corporation. All rights reserved.
  OriginalFilename : SXS.DLL
```

Step 3 : Run the *dlllist* command to list all the process names and their ids along with the current DLLs being utilized by them.



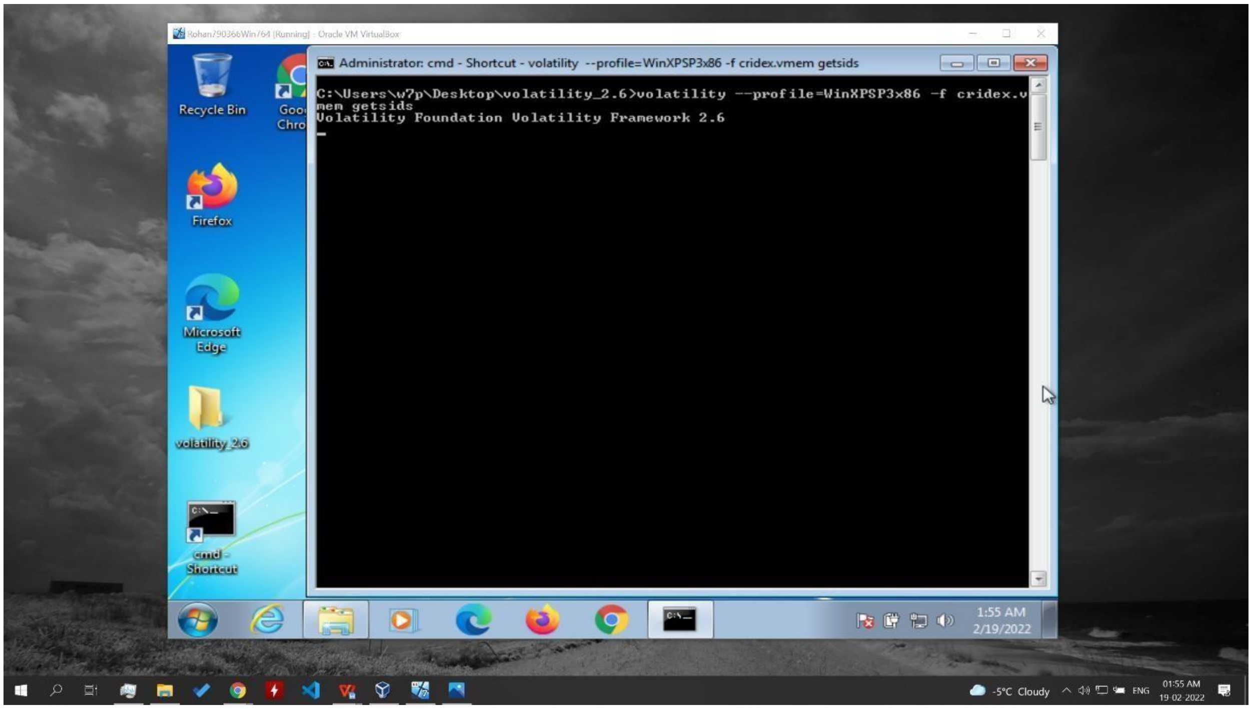
Administrator: cmd - Shortcut - volatility --profile=WinXPSP3x86 -f cridex.vmem dlllist

```
C:\Users\w7p\Desktop\volatility_2.6>volatility --profile=WinXPSP3x86 -f cridex.v
mem dlllist
Volatility Foundation Volatility Framework 2.6
_
```

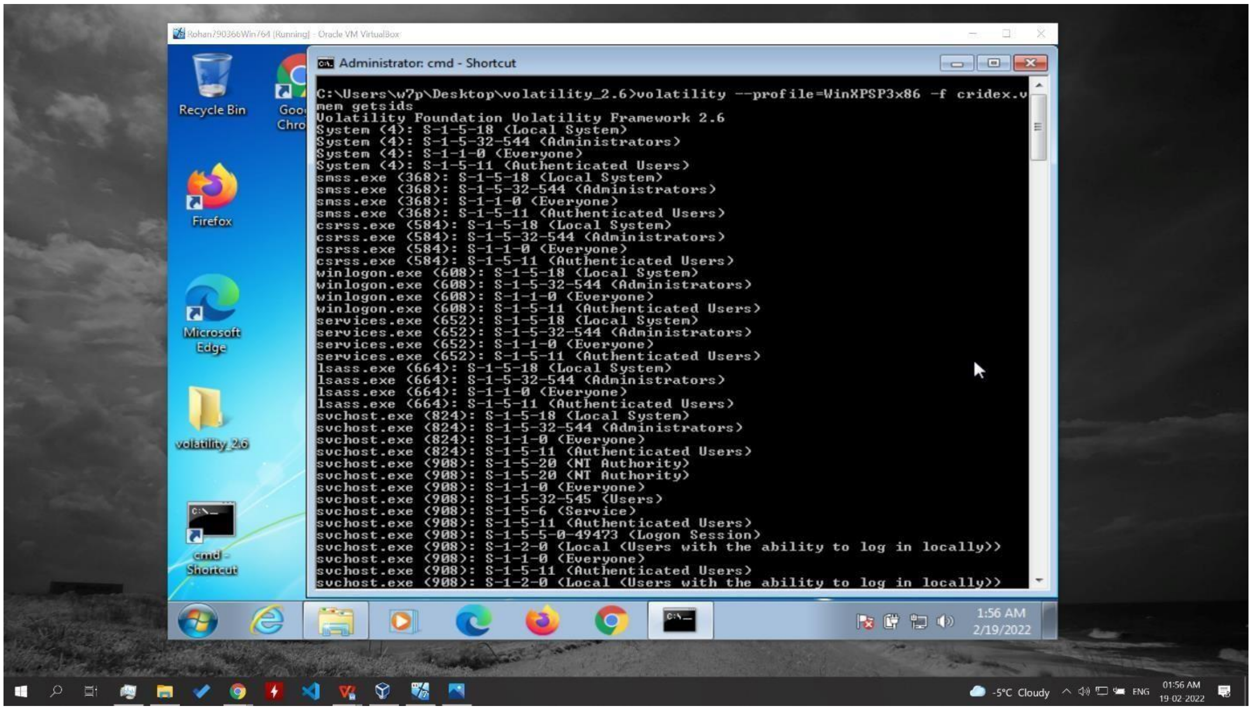


```
0x7c9c0000   0x817000        0x1 C:\WINDOWS\system32\SHELL32.dll
0x77f60000    0x76000        0x3 C:\WINDOWS\system32\SHLWAPI.dll
0x769c0000    0xb4000        0x1 C:\WINDOWS\system32\USERENV.dll
0x5ad70000    0x38000        0x1 C:\WINDOWS\system32\UxTheme.dll
0x773d0000   0x103000        0x1 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
0x5d090000    0x9a000        0x1 C:\WINDOWS\system32\comctl32.dll
0x76770000     0xd000        0x1 c:\windows\system32\dnsrslvr.dll
0x76f20000    0x27000        0x1 c:\windows\system32\DNSAPI.dll
0x71ab0000    0x17000        0x3 c:\windows\system32\WS2_32.dll
0x71aa0000     0x8000        0x2 c:\windows\system32\WS2HELP.dll
0x76d60000    0x19000        0x2 c:\windows\system32\iphlpapi.dll
************************************************************************
svchost.exe pid:   1220
Command line : C:\WINDOWS\system32\svchost.exe -k LocalService
Service Pack 3

Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x01000000     0x6000     0xffff C:\WINDOWS\system32\svchost.exe
0x7c900000    0xaf000     0xffff C:\WINDOWS\system32\ntdll.dll
0x7c800000    0xf6000     0xffff C:\WINDOWS\system32\kernel32.dll
0x77dd0000    0x9b000     0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000    0x92000     0xffff C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000    0x11000     0xffff C:\WINDOWS\system32\Secur32.dll
0x5cb70000    0x26000        0x1 C:\WINDOWS\system32\ShimEng.dll
0x6f880000   0x1ca000        0x1 C:\WINDOWS\AppPatch\AcGenral.DLL
0x7e410000    0x91000       0x41 C:\WINDOWS\system32\USER32.dll
0x77f10000    0x49000       0x36 C:\WINDOWS\system32\GDI32.dll
0x76b40000    0x2d000        0x2 C:\WINDOWS\system32\WINMM.dll
0x774e0000   0x13d000        0xe C:\WINDOWS\system32\ole32.dll
0x77c10000    0x58000       0x53 C:\WINDOWS\system32\msvcrt.dll
0x77120000    0x8b000        0x7 C:\WINDOWS\system32\OLEAUT32.dll
0x77be0000    0x15000        0x1 C:\WINDOWS\system32\MSACM32.dll
0x77c00000     0x8000        0x3 C:\WINDOWS\system32\VERSION.dll
0x7c9c0000   0x817000        0x3 C:\WINDOWS\system32\SHELL32.dll
0x77f60000    0x76000        0x7 C:\WINDOWS\system32\SHLWAPI.dll
0x769c0000    0xb4000        0x1 C:\WINDOWS\system32\USERENV.dll
0x5ad70000    0x38000        0x1 C:\WINDOWS\system32\UxTheme.dll
0x773d0000   0x103000        0x2 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
0x5d090000    0x9a000        0x1 C:\WINDOWS\system32\comctl32.dll
0x77690000    0x21000        0x1 C:\WINDOWS\system32\NTMARTA.DLL
```

Step 4 : Run the *getsids* command to get information about process name, process id user and their system privileges


Administrator: cmd - Shortcut - volatility --profile=WinXPSP3x86 -f cridex.vmem getsids

```
C:\Users\w7p\Desktop\volatility_2.6>volatility --profile=WinXPSP3x86 -f cridex.v
mem getsids
Volatility Foundation Volatility Framework 2.6
```



```
C:\Users\w7p\Desktop\volatility_2.6>volatility --profile=WinXPSP3x86 -f cridex.v
mem getsids
Volatility Foundation Volatility Framework 2.6
System (4): S-1-5-18 (Local System)
System (4): S-1-5-32-544 (Administrators)
System (4): S-1-1-0 (Everyone)
System (4): S-1-5-11 (Authenticated Users)
smss.exe (368): S-1-5-18 (Local System)
smss.exe (368): S-1-5-32-544 (Administrators)
smss.exe (368): S-1-1-0 (Everyone)
smss.exe (368): S-1-5-11 (Authenticated Users)
csrss.exe (584): S-1-5-18 (Local System)
csrss.exe (584): S-1-5-32-544 (Administrators)
csrss.exe (584): S-1-1-0 (Everyone)
csrss.exe (584): S-1-5-11 (Authenticated Users)
winlogon.exe (608): S-1-5-18 (Local System)
winlogon.exe (608): S-1-5-32-544 (Administrators)
winlogon.exe (608): S-1-1-0 (Everyone)
winlogon.exe (608): S-1-5-11 (Authenticated Users)
services.exe (652): S-1-5-18 (Local System)
services.exe (652): S-1-5-32-544 (Administrators)
services.exe (652): S-1-1-0 (Everyone)
services.exe (652): S-1-5-11 (Authenticated Users)
lsass.exe (664): S-1-5-18 (Local System)
lsass.exe (664): S-1-5-32-544 (Administrators)
lsass.exe (664): S-1-1-0 (Everyone)
lsass.exe (664): S-1-5-11 (Authenticated Users)
svchost.exe (824): S-1-5-18 (Local System)
svchost.exe (824): S-1-5-32-544 (Administrators)
svchost.exe (824): S-1-1-0 (Everyone)
svchost.exe (824): S-1-5-11 (Authenticated Users)
svchost.exe (908): S-1-5-20 (NT Authority)
svchost.exe (908): S-1-5-20 (NT Authority)
svchost.exe (908): S-1-1-0 (Everyone)
svchost.exe (908): S-1-5-32-545 (Users)
svchost.exe (908): S-1-5-6 (Service)
svchost.exe (908): S-1-5-11 (Authenticated Users)
svchost.exe (908): S-1-5-5-0-49473 (Logon Session)
svchost.exe (908): S-1-2-0 (Local (Users with the ability to log in locally))
svchost.exe (908): S-1-1-0 (Everyone)
svchost.exe (908): S-1-5-11 (Authenticated Users)
svchost.exe (908): S-1-2-0 (Local (Users with the ability to log in locally))
```

Conclusion

We used volatility to successfully capture a lot of information about these DLL files which are essential to the operation of the system. The information we got also included the currently running DLL files and the process using them at the time along with the username.

Achievement

We get to understand in dept about all the active connections established during the memory dump, also the Ip address along with the location details, map, internet service provider details, location, organization, and the location map. We used three different commands which helped us in analysing the DLL files in a much different manner. We got to see how many of these files were being used simultaneously by different processes, we also got to know each file's location, their version and creator organization.

References

1. *Host and Memory Forensics* – Google Drive. (n.d.). Google Drive. Retrieved February

18, 2022, from https://drive.google.com/drive/folders/19BcrG1-57OMdlylRyPi_35kpCffFyQYv?usp=sharing

2. *Private video on Vimeo.* (n.d.-a). Vimeo. Retrieved February 18, 2022, from https://vimeo.com/629598156
3. *Private video on Vimeo.* (n.d.-b). Vimeo. Retrieved February 18, 2022, from https://vimeo.com/625511507
4. *Private video on Vimeo.* (n.d.-c). Vimeo. Retrieved February 18, 2022, from https://vimeo.com/625524276

Name of students who has not participated in the assignment.
Student name:
Student name:
Student name:
Student name:
Student name:

Everyone has participated in this activity