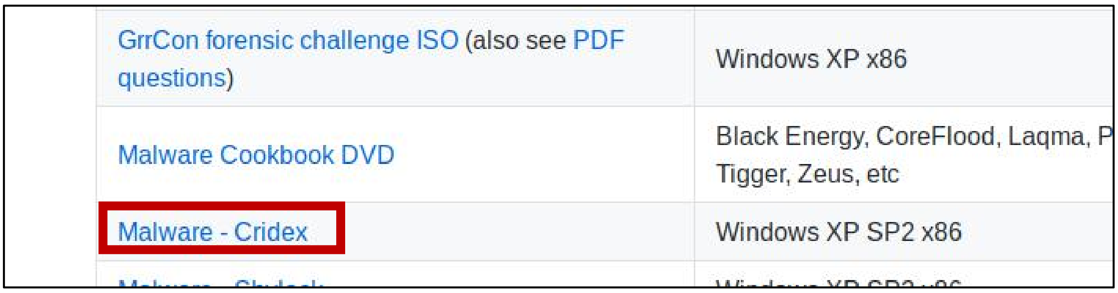
DIGITAL FORENSICS II
EXPERIMENT 7

Submitted to: Mr. Keshav Kaushik
Submitted by: Kashish Srivastava
R134218079
500067405

Aim: Memory Forensics using Volatility tool.

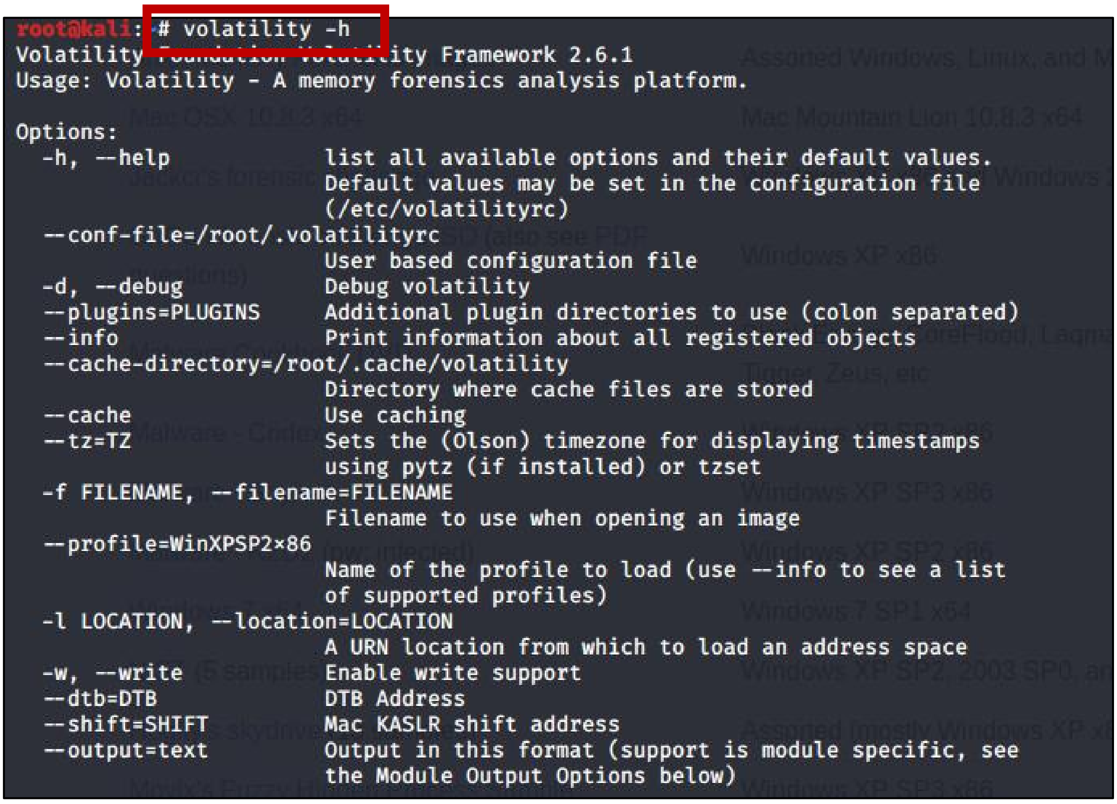
Steps:

Step 1: Using the link provided, we need to use the memory samples from here: https://github.com/volatilityfoundation/volatility/wiki/Memory-Samples



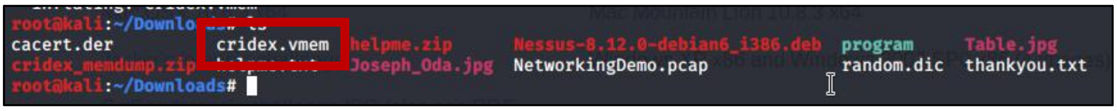
GrrCon forensic challenge ISO (also see PDF questions)	Windows XP x86
Malware Cookbook DVD	Black Energy, CoreFlood, Laqma, P Tigger, Zeus, etc
Malware - Cridex	Windows XP SP2 x86

Step 2: After installing volatility, we use the command ***volatility -h*** for viewing all the options present.



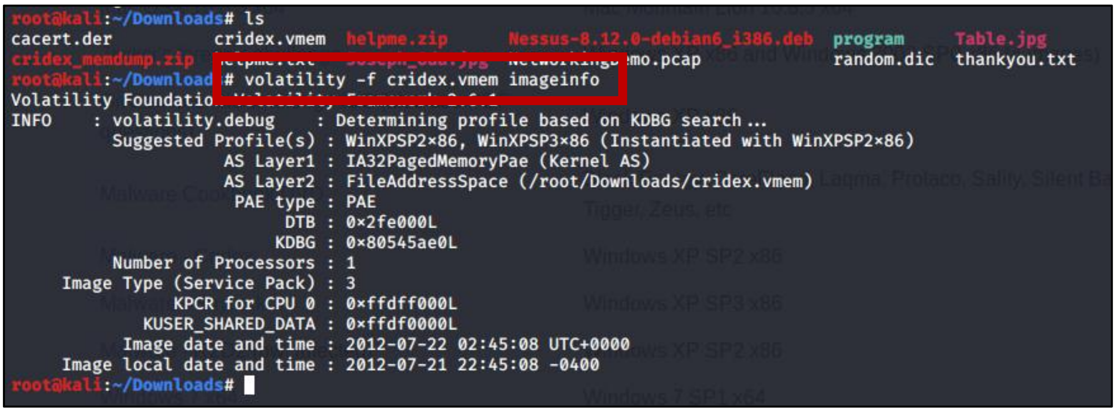
```
root@kali:~# volatility -h
Volatility Foundation Volatility Framework 2.6.1
Usage: Volatility - A memory forensics analysis platform.

Options:
  -h, --help            list all available options and their default values.
                        Default values may be set in the configuration file
                        (/etc/volatilityrc)
  --conf-file=/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
                        the Module Output Options below)
```

Step 3: After downloading ***malware - Cridex***, we extract the files present and find the extracted file named as ***cridex.vmem***



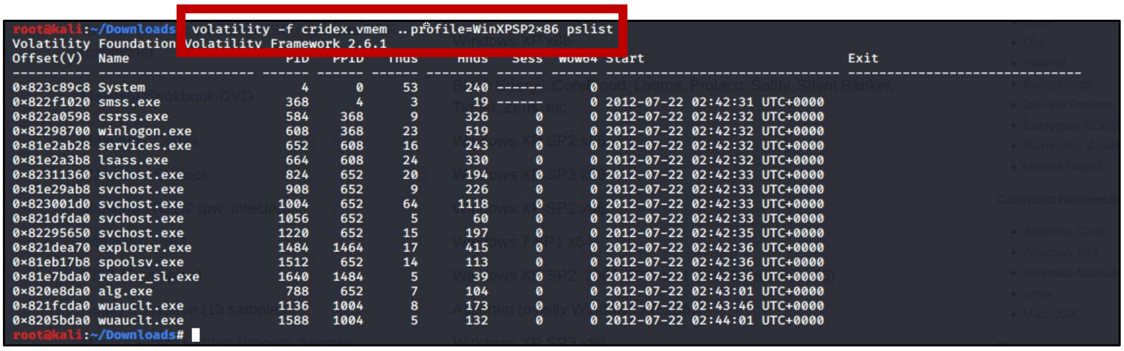
```
root@kali:~/Downlo    ls
cacert.der          cridex.vmem    helpme.zip      Nessus-8.12.0-debian6_i386.deb  program     Table.jpg
cridex_memdump.zip  helpme.txt     Joseph_Oda.jpg  NetworkingDemo.pcap             random.dic  thankyou.txt
root@kali:~/Downloads# █
```

Step 4 : We use ***imageinfo command*** to view the details of this image. The most important yet interesting thing here is ***Profile(s)*** that have been suggested



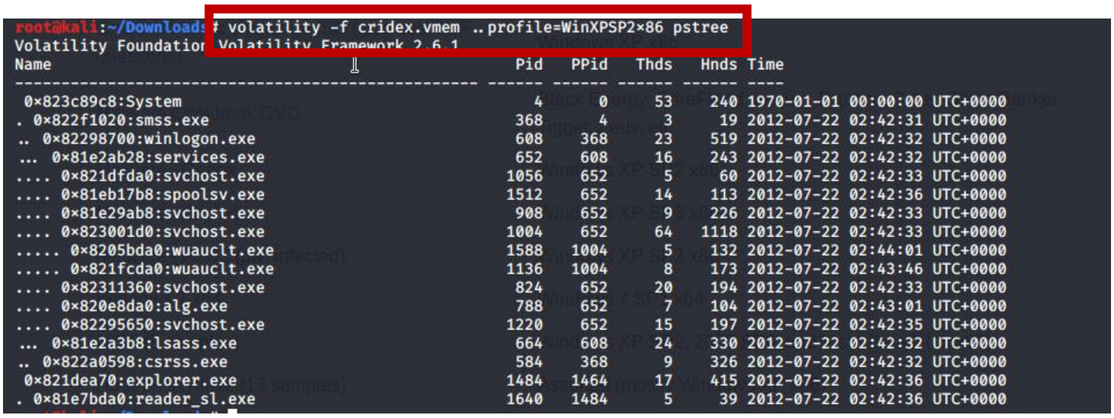
```
root@kali:~/Downloads# ls
cacert.der          cridex.vmem  helpme.zip      Nessus-8.12.0-debian6_i386.deb  program     Table.jpg
cridex_memdump.zip  helpme.txt   Joseph_Oda.jpg  NetworkingDemo.pcap             random.dic  thankyou.txt
root@kali:~/Download # volatility -f cridex.vmem imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search ...
          Suggested Profile(s) : WinXPSP2×86, WinXPSP3×86 (Instantiated with WinXPSP2×86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/root/Downloads/cridex.vmem)
                      PAE type : PAE
                           DTB : 0×2fe000L
                          KDBG : 0×80545ae0L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0×ffdff000L
             KUSER_SHARED_DATA : 0×ffdf0000L
           Image date and time : 2012-07-22 02:45:08 UTC+0000
     Image local date and time : 2012-07-21 22:45:08 -0400
root@kali:~/Downloads# █
```

Step 5: Selecting the profile ***(WinXPSP2x86)*** and getting the list of all the process that were available in this memory dump, through the module ***'pslist'***.



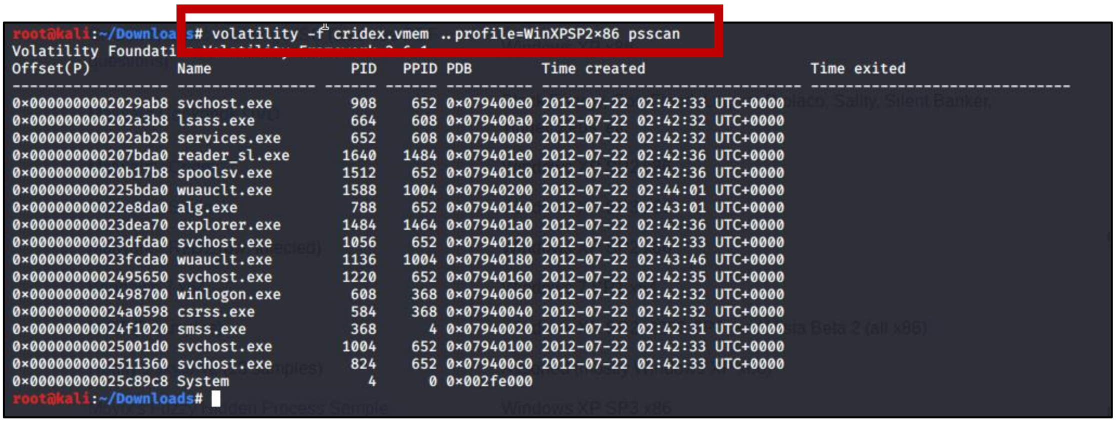
```
root@kali:~/Downloads volatility -f cridex.vmem ..profile=WinXPSP2×86 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0×823c89c8 System                    4      0     53      240 ------      0
0×822f1020 smss.exe                368      4      3       19 ------      0 2012-07-22 02:42:31 UTC+0000
0×822a0598 csrss.exe               584    368      9      326      0      0 2012-07-22 02:42:32 UTC+0000
0×82298700 winlogon.exe            608    368     23      519      0      0 2012-07-22 02:42:32 UTC+0000
0×81e2ab28 services.exe            652    608     16      243      0      0 2012-07-22 02:42:32 UTC+0000
0×81e2a3b8 lsass.exe               664    608     24      330      0      0 2012-07-22 02:42:32 UTC+0000
0×82311360 svchost.exe             824    652     20      194      0      0 2012-07-22 02:42:33 UTC+0000
0×81e29ab8 svchost.exe             908    652      9      226      0      0 2012-07-22 02:42:33 UTC+0000
0×823001d0 svchost.exe            1004    652     64     1118      0      0 2012-07-22 02:42:33 UTC+0000
0×821dfda0 svchost.exe            1056    652      5       60      0      0 2012-07-22 02:42:33 UTC+0000
0×82295650 svchost.exe            1220    652     15      197      0      0 2012-07-22 02:42:35 UTC+0000
0×821dea70 explorer.exe           1484   1464     17      415      0      0 2012-07-22 02:42:36 UTC+0000
0×81eb17b8 spoolsv.exe            1512    652     14      113      0      0 2012-07-22 02:42:36 UTC+0000
0×81e7bda0 reader_sl.exe          1640   1484      5       39      0      0 2012-07-22 02:42:36 UTC+0000
0×820e8da0 alg.exe                 788    652      7      104      0      0 2012-07-22 02:43:01 UTC+0000
0×821fcda0 wuauclt.exe            1136   1004      8      173      0      0 2012-07-22 02:43:46 UTC+0000
0×8205bda0 wuauclt.exe            1588   1004      5      132      0      0 2012-07-22 02:44:01 UTC+0000
root@kali:~/Downloads# █
```

There are various columns present here, as the metadata for the processes of this image. (process ID, Parent Process ID, threads, handles, Timestamp etc.) Parent process of all the services is services.exe, as you can see the services mentioned in the list contain the same PPID as the PID of services.exe. We can also confirm this in a later command ***'pstree'***. To understand the process hierarchy clearly in visuals.



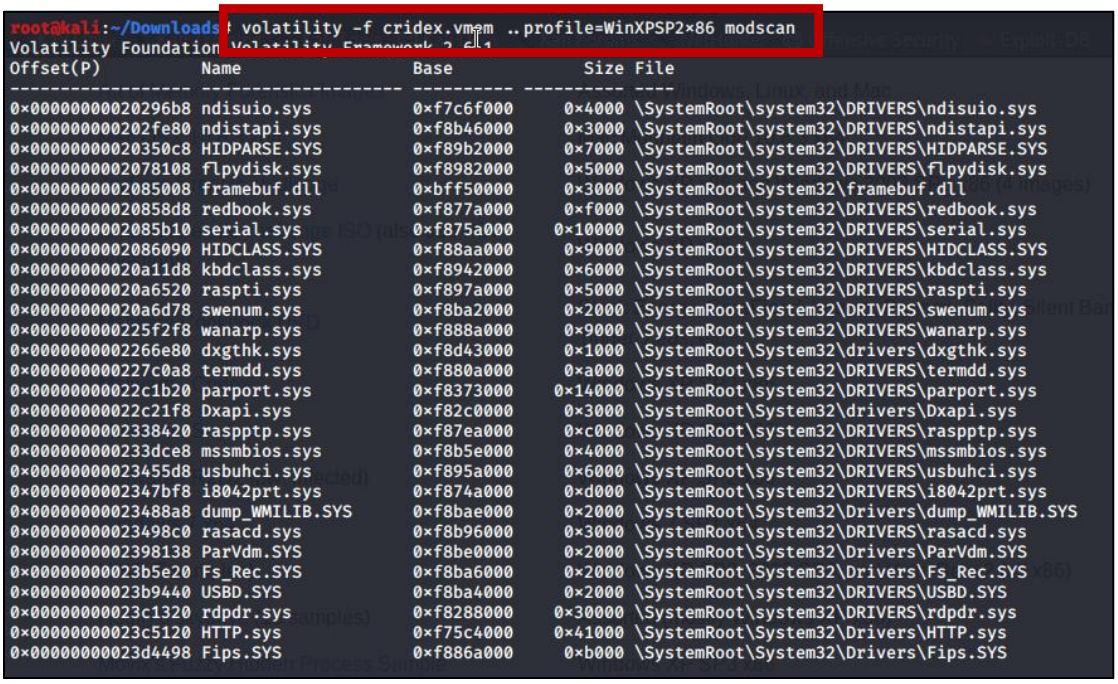
```
root@kali:~/Downloads# volatility -f cridex.vmem ..profile=WinXPSP2×86 pstree
Volatility Foundation Volatility Framework 2.6.1
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0×823c89c8:System                                      4      0     53    240 1970-01-01 00:00:00 UTC+0000
. 0×822f1020:smss.exe                                 368      4      3     19 2012-07-22 02:42:31 UTC+0000
.. 0×82298700:winlogon.exe                            608    368     23    519 2012-07-22 02:42:32 UTC+0000
... 0×81e2ab28:services.exe                           652    608     16    243 2012-07-22 02:42:32 UTC+0000
.... 0×821dfda0:svchost.exe                          1056    652      5     60 2012-07-22 02:42:33 UTC+0000
.... 0×81eb17b8:spoolsv.exe                          1512    652     14    113 2012-07-22 02:42:36 UTC+0000
.... 0×81e29ab8:svchost.exe                           908    652      9    226 2012-07-22 02:42:33 UTC+0000
.... 0×823001d0:svchost.exe                          1004    652     64   1118 2012-07-22 02:42:33 UTC+0000
..... 0×8205bda0:wuauclt.exe                         1588   1004      5    132 2012-07-22 02:44:01 UTC+0000
..... 0×821fcda0:wuauclt.exe                         1136   1004      8    173 2012-07-22 02:43:46 UTC+0000
.... 0×82311360:svchost.exe                           824    652     20    194 2012-07-22 02:42:33 UTC+0000
.... 0×820e8da0:alg.exe                               788    652      7    104 2012-07-22 02:43:01 UTC+0000
.... 0×82295650:svchost.exe                          1220    652     15    197 2012-07-22 02:42:35 UTC+0000
... 0×81e2a3b8:lsass.exe                              664    608     24    330 2012-07-22 02:42:32 UTC+0000
.. 0×822a0598:csrss.exe                               584    368      9    326 2012-07-22 02:42:32 UTC+0000
 0×821dea70:explorer.exe                             1484   1464     17    415 2012-07-22 02:42:36 UTC+0000
. 0×81e7bda0:reader_sl.exe                           1640   1484      5     39 2012-07-22 02:42:36 UTC+0000
```

Step 6: For more details about it we can also perform using ***'psscan'*** module.



```
root@kali:~/Downloads# volatility -f cridex.vmem --profile=WinXPSP2x86 psscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)          Name             PID    PPID PDB        Time created                   Time exited
------------------ ---------------- ------ ------ ---------- ------------------------------ ------------------------------
0x0000000002029ab8 svchost.exe         908    652 0x079400e0 2012-07-22 02:42:33 UTC+0000
0x000000000202a3b8 lsass.exe           664    608 0x079400a0 2012-07-22 02:42:32 UTC+0000
0x000000000202ab28 services.exe        652    608 0x07940080 2012-07-22 02:42:32 UTC+0000
0x000000000207bda0 reader_sl.exe      1640   1484 0x079401e0 2012-07-22 02:42:36 UTC+0000
0x00000000020b17b8 spoolsv.exe        1512    652 0x079401c0 2012-07-22 02:42:36 UTC+0000
0x000000000225bda0 wuauclt.exe        1588   1004 0x07940200 2012-07-22 02:44:01 UTC+0000
0x00000000022e8da0 alg.exe             788    652 0x07940140 2012-07-22 02:43:01 UTC+0000
0x00000000023dea70 explorer.exe       1484   1464 0x079401a0 2012-07-22 02:42:36 UTC+0000
0x00000000023dfda0 svchost.exe        1056    652 0x07940120 2012-07-22 02:42:33 UTC+0000
0x00000000023fcda0 wuauclt.exe        1136   1004 0x07940180 2012-07-22 02:43:46 UTC+0000
0x0000000002495650 svchost.exe        1220    652 0x07940160 2012-07-22 02:42:35 UTC+0000
0x0000000002498700 winlogon.exe        608    368 0x07940060 2012-07-22 02:42:32 UTC+0000
0x00000000024a0598 csrss.exe           584    368 0x07940040 2012-07-22 02:42:32 UTC+0000
0x00000000024f1020 smss.exe            368      4 0x07940020 2012-07-22 02:42:31 UTC+0000
0x00000000025001d0 svchost.exe        1004    652 0x07940100 2012-07-22 02:42:33 UTC+0000
0x0000000002511360 svchost.exe         824    652 0x079400c0 2012-07-22 02:42:33 UTC+0000
0x00000000025c89c8 System                4      0 0x002fe000
root@kali:~/Downloads#
```

Step 7: All the List of processes in kernel module can be reviewed with the module ***'modscan'.***

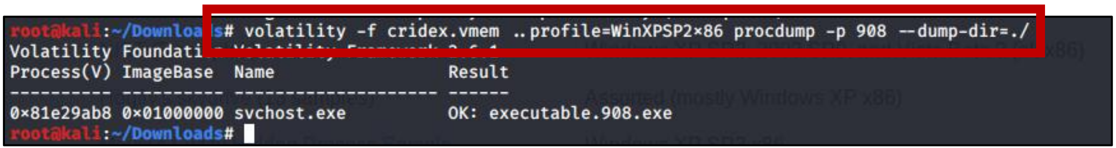


```
root@kali:~/Downloads# volatility -f cridex.vmem --profile=WinXPSP2x86 modscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)          Name                 Base             Size File
------------------ -------------------- ---------- ---------- ----
0x00000000020296b8 ndisuio.sys          0xf7c6f000     0x4000 \SystemRoot\system32\DRIVERS\ndisuio.sys
0x000000000202fe80 ndistapi.sys         0xf8b46000     0x3000 \SystemRoot\system32\DRIVERS\ndistapi.sys
0x00000000020350c8 HIDPARSE.SYS         0xf89b2000     0x7000 \SystemRoot\system32\DRIVERS\HIDPARSE.SYS
0x0000000002078108 flpydisk.sys         0xf8982000     0x5000 \SystemRoot\system32\DRIVERS\flpydisk.sys
0x0000000002085008 framebuf.dll         0xbff50000     0x3000 \SystemRoot\System32\framebuf.dll
0x00000000020858d8 redbook.sys          0xf877a000     0xf000 \SystemRoot\system32\DRIVERS\redbook.sys
0x0000000002085b10 serial.sys           0xf875a000    0x10000 \SystemRoot\system32\DRIVERS\serial.sys
0x0000000002086090 HIDCLASS.SYS         0xf88aa000     0x9000 \SystemRoot\system32\DRIVERS\HIDCLASS.SYS
0x00000000020a11d8 kbdclass.sys         0xf8942000     0x6000 \SystemRoot\system32\DRIVERS\kbdclass.sys
0x00000000020a6520 raspti.sys           0xf897a000     0x5000 \SystemRoot\system32\DRIVERS\raspti.sys
0x00000000020a6d78 swenum.sys           0xf8ba2000     0x2000 \SystemRoot\system32\DRIVERS\swenum.sys
0x000000000225f2f8 wanarp.sys           0xf888a000     0x9000 \SystemRoot\system32\DRIVERS\wanarp.sys
0x0000000002266e80 dxgthk.sys           0xf8d43000     0x1000 \SystemRoot\System32\drivers\dxgthk.sys
0x000000000227c0a8 termdd.sys           0xf880a000     0xa000 \SystemRoot\system32\DRIVERS\termdd.sys
0x00000000022c1b20 parport.sys          0xf8373000    0x14000 \SystemRoot\system32\DRIVERS\parport.sys
0x00000000022c21f8 Dxapi.sys            0xf82c0000     0x3000 \SystemRoot\System32\drivers\Dxapi.sys
0x0000000002338420 raspptp.sys          0xf87ea000     0xc000 \SystemRoot\system32\DRIVERS\raspptp.sys
0x000000000233dce8 mssmbios.sys         0xf8b5e000     0x4000 \SystemRoot\system32\DRIVERS\mssmbios.sys
0x00000000023455d8 usbuhci.sys          0xf895a000     0x6000 \SystemRoot\system32\DRIVERS\usbuhci.sys
0x0000000002347bf8 i8042prt.sys         0xf874a000     0xd000 \SystemRoot\system32\DRIVERS\i8042prt.sys
0x00000000023488a8 dump_WMILIB.SYS      0xf8bae000     0x2000 \SystemRoot\System32\Drivers\dump_WMILIB.SYS
0x00000000023498c0 rasacd.sys           0xf8b96000     0x3000 \SystemRoot\system32\DRIVERS\rasacd.sys
0x0000000002398138 ParVdm.SYS           0xf8be0000     0x2000 \SystemRoot\System32\Drivers\ParVdm.SYS
0x00000000023b5e20 Fs_Rec.SYS           0xf8ba6000     0x2000 \SystemRoot\System32\Drivers\Fs_Rec.SYS
0x00000000023b9440 USBD.SYS             0xf8ba4000     0x2000 \SystemRoot\system32\DRIVERS\USBD.SYS
0x00000000023c1320 rdpdr.sys            0xf8288000    0x30000 \SystemRoot\system32\DRIVERS\rdpdr.sys
0x00000000023c5120 HTTP.sys             0xf75c4000    0x41000 \SystemRoot\System32\Drivers\HTTP.sys
0x00000000023d4498 Fips.SYS             0xf886a000     0xb000 \SystemRoot\System32\Drivers\Fips.SYS
```

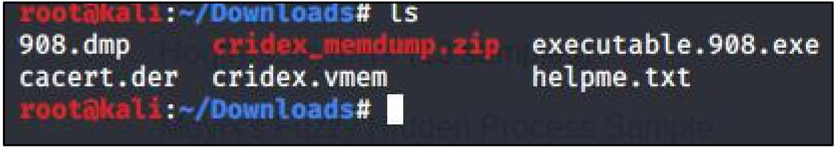
Step 8: Now, we run two modules and save their output as a file in the current directory.

'procdump' - created the process in executable format (.exe),

'Memdump' - the memory present for that process at the time of its execution is stored in the **.dmp** file

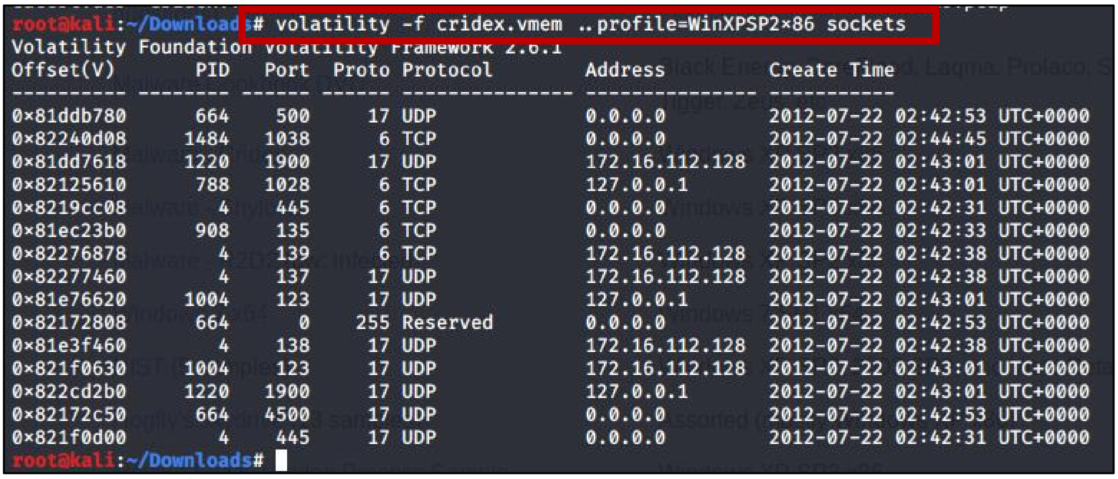


```
root@kali:~/Downloads# volatility -f cridex.vmem --profile=WinXPSP2x86 procdump -p 908 --dump-dir=./
Volatility Foundation Volatility Framework 2.6.1
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x81e29ab8 0x01000000 svchost.exe          OK: executable.908.exe
root@kali:~/Downloads#
```

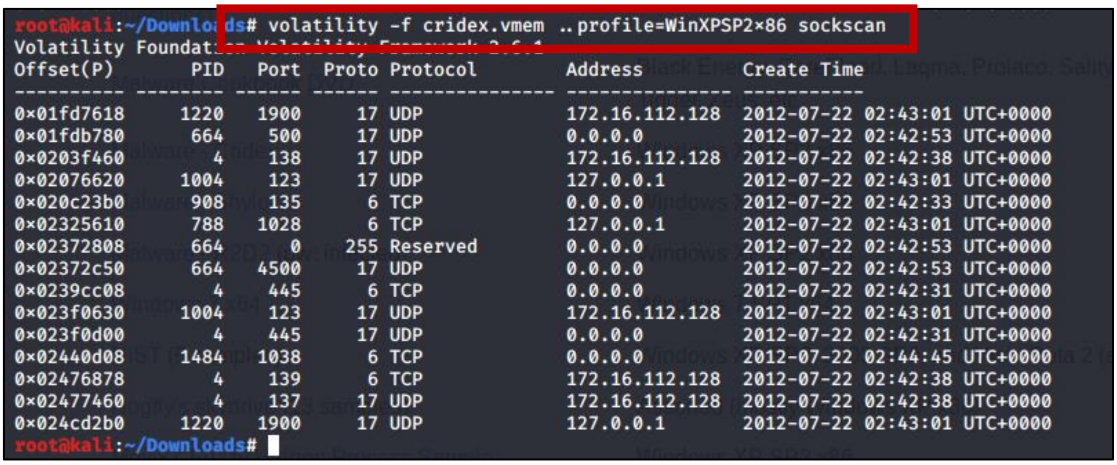


```
root@kali:~/Downloads# ls
908.dmp     cridex_memdump.zip  executable.908.exe
cacert.der  cridex.vmem         helpme.txt
root@kali:~/Downloads#
```

Step 9: Now, to explore about the sockets of the machine, we used ***'sockets'*** module to view the list of open sockets
And to scan for TCP socket objects we used ***'sockscan'***

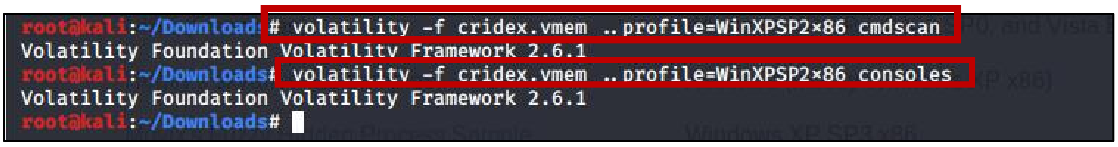


```
root@kali:~/Downloads# volatility -f cridex.vmem ..profile=WinXPSP2x86 sockets
Volatility Foundation Volatility Framework 2.6.1
Offset(V)       PID   Port  Proto Protocol        Address         Create Time
---------- -------- ------ ------ --------------- --------------- -----------
0x81ddb780      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
root@kali:~/Downloads#
```



```
root@kali:~/Downloads# volatility -f cridex.vmem ..profile=WinXPSP2x86 sockscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)       PID   Port  Proto Protocol        Address         Create Time
---------- -------- ------ ------ --------------- --------------- -----------
0x01fd7618     1220   1900     17 UDP             172.16.112.128  2012-07-22 02:43:01 UTC+0000
0x01fdb780      664    500     17 UDP             0.0.0.0         2012-07-22 02:42:53 UTC+0000
0x0203f460        4    138     17 UDP             172.16.112.128  2012-07-22 02:42:38 UTC+0000
0x02076620     1004    123     17 UDP             127.0.0.1       2012-07-22 02:43:01 UTC+0000
0x020c23b0      908    135      6 TCP             0.0.0.0         2012-07-22 02:42:33 UTC+0000
0x02325610      788   1028      6 TCP             127.0.0.1       2012-07-22 02:43:01 UTC+0000
0x02372808      664      0    255 Reserved        0.0.0.0         2012-07-22 02:42:53 UTC+0000
0x02372c50      664   4500     17 UDP             0.0.0.0         2012-07-22 02:42:53 UTC+0000
0x0239cc08        4    445      6 TCP             0.0.0.0         2012-07-22 02:42:31 UTC+0000
0x023f0630     1004    123     17 UDP             172.16.112.128  2012-07-22 02:43:01 UTC+0000
0x023f0d00        4    445     17 UDP             0.0.0.0         2012-07-22 02:42:31 UTC+0000
0x02440d08     1484   1038      6 TCP             0.0.0.0         2012-07-22 02:44:45 UTC+0000
0x02476878        4    139      6 TCP             172.16.112.128  2012-07-22 02:42:38 UTC+0000
0x02477460        4    137     17 UDP             172.16.112.128  2012-07-22 02:42:38 UTC+0000
0x024cd2b0     1220   1900     17 UDP             127.0.0.1       2012-07-22 02:43:01 UTC+0000
root@kali:~/Downloads#
```

Step 10: Further, we explored for commands, we used ***'cmdscan'*** to extract command history by scanning for _COMMAND_HISTORY, and ***'consoles'*** module to extract command history for _CONSOLE_INFORMATION
Here, there were no commands to be found by both of these modules



```
root@kali:~/Downloads# volatility -f cridex.vmem ..profile=WinXPSP2x86 cmdscan
Volatility Foundation Volatility Framework 2.6.1
root@kali:~/Downloads# volatility -f cridex.vmem ..profile=WinXPSP2x86 consoles
Volatility Foundation Volatility Framework 2.6.1
root@kali:~/Downloads#
```