Volatility Hands-on Activity and Report

Gursimran Singh LNU
Computer and Information Science
Rochester Institute of Technology
Rochester, New York, USA
gl2840 at rit.edu

I. Introduction

The Volatility Framework is an open-source memory forensics tool used to analyze volatile memory (RAM) on a system. It is mainly used for digital forensics, incident response, and malware analysis.

The tool is designed to extract information from memory dumps in a forensically sound manner, allowing us to identify and analyze running processes, network connections, open files, etc. The Volatility Framework supports analyzing memory dumps from a wide range of operating systems, including Windows, Linux, and macOS.

The Volatility Framework uses a plugin-based architecture, where each plugin is responsible for analyzing a specific type of data in memory. The tool provides a command-line interface to interact with the plugins and extract the desired information from the memory dump. The plugins can be used individually or combined to perform a more comprehensive analysis.

Some of the plugins included with the Volatility Framework are:

- **pslist**: lists all running processes in memory.
- **netscan**: lists all open network connections.
- **filescan**: lists all open files in memory.
- **timeliner**: creates a timeline of events based on information extracted from memory.

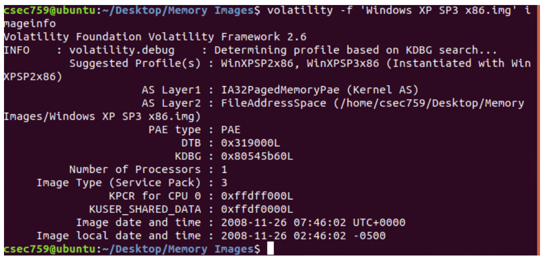
Overall, the Volatility Framework is a powerful tool for digital forensics and incident response teams, allowing them to extract valuable information from volatile memory that would otherwise be lost once the system is powered off or rebooted.

II. Usage of Volatility

We stated by using volatility for by running the *imageinfo* command for an existing memory image, which will return the profile to use with the memory image. Then we used plugins like pslist, psscan, psxview, connscan, dlllist, handles, and impscan. These were the given plugins in the support documentation and their usage is shown from Fig. 1 to Fig. 8, respectively. Next we discuss the additional plugins explored in this study.

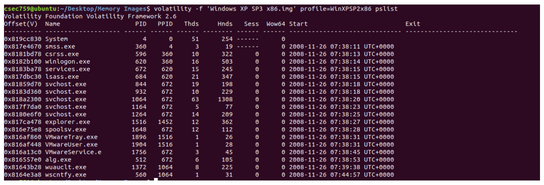
III. Plugin 1 - evtlogs

The evtlogs command in Volatility is a plugin that allows you to extract event logs from a memory dump of a Windows system. Event logs contain important information about system events, such as software installations, logins, and system



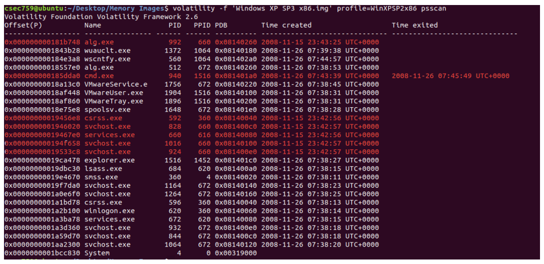
```
csec759@ubuntu:~/Desktop/Memory Images$ volatility -f 'Windows XP SP3 x86.img' i
mageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with Win
XPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/csec759/Desktop/Memory
Images/Windows XP SP3 x86.img)
                      PAE type : PAE
                           DTB : 0x319000L
                          KDBG : 0x80545b60L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2008-11-26 07:46:02 UTC+0000
     Image local date and time : 2008-11-26 02:46:02 -0500
csec759@ubuntu:~/Desktop/Memory Images$
```

Fig. 1. Getting the memory image profile



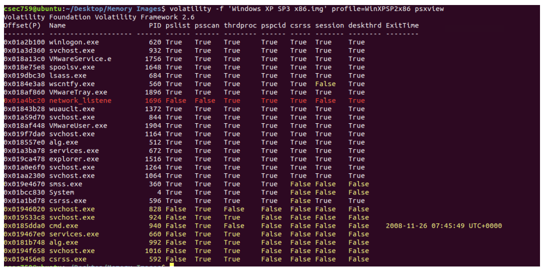
```
csec759@ubuntu:~/Desktop/Memory Images$ volatility -f 'Windows XP SP3 x86.img' profile=WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x819cc830 System                    4      0     51      254 ------      0
0x817e4670 smss.exe                360      4      3       19 ------      0 2008-11-26 07:38:11 UTC+0000
0x8181bd78 csrss.exe               596    360     10      322      0      0 2008-11-26 07:38:13 UTC+0000
0x8182b100 winlogon.exe            620    360     16      503      0      0 2008-11-26 07:38:14 UTC+0000
0x8183ba78 services.exe            672    620     15      245      0      0 2008-11-26 07:38:15 UTC+0000
0x817dbc30 lsass.exe               684    620     21      347      0      0 2008-11-26 07:38:15 UTC+0000
0x81859d70 svchost.exe             844    672     19      198      0      0 2008-11-26 07:38:18 UTC+0000
0x8183d360 svchost.exe             932    672     10      229      0      0 2008-11-26 07:38:18 UTC+0000
0x818a2300 svchost.exe            1064    672     63     1308      0      0 2008-11-26 07:38:20 UTC+0000
0x817f7da0 svchost.exe            1164    672      5       77      0      0 2008-11-26 07:38:23 UTC+0000
0x8180e6f0 svchost.exe            1264    672     14      209      0      0 2008-11-26 07:38:25 UTC+0000
0x817ca478 explorer.exe           1516   1452     12      362      0      0 2008-11-26 07:38:27 UTC+0000
0x816e75e8 spoolsv.exe            1648    672     12      112      0      0 2008-11-26 07:38:28 UTC+0000
0x816af860 VMwareTray.exe         1896   1516      1       26      0      0 2008-11-26 07:38:31 UTC+0000
0x816af448 VMwareUser.exe         1904   1516      1       28      0      0 2008-11-26 07:38:31 UTC+0000
0x816a13c0 VMwareService.e        1756    672      3       45      0      0 2008-11-26 07:38:45 UTC+0000
0x816557e0 alg.exe                 512    672      6      105      0      0 2008-11-26 07:38:53 UTC+0000
0x81643b28 wuauclt.exe            1372   1064      8      225      0      0 2008-11-26 07:39:38 UTC+0000
0x8164e3a8 wscntfy.exe             560   1064      1       31      0      0 2008-11-26 07:44:57 UTC+0000
```

Fig. 2. List of process in EPROCESS list



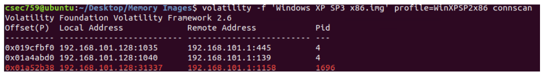
```
csec759@ubuntu:~/Desktop/Memory Images$ volatility -f 'Windows XP SP3 x86.img' profile=WinXPSP2x86 psscan
Volatility Foundation Volatility Framework 2.6
Offset(P)          Name                PID   PPID PDB        Time created                   Time exited
------------------ ---------------- ------ ------ ---------- ------------------------------ ------------------------------
0x000000000181b748 alg.exe             992    660 0x08140260 2008-11-15 23:43:25 UTC+0000
0x0000000001843b28 wuauclt.exe        1372   1064 0x08140180 2008-11-26 07:39:38 UTC+0000
0x000000000184e3a8 wscntfy.exe         560   1064 0x081402a0 2008-11-26 07:44:57 UTC+0000
0x00000000018557e0 alg.exe             512    672 0x08140260 2008-11-26 07:38:53 UTC+0000
0x000000000185dda0 cmd.exe             940   1516 0x081401a0 2008-11-26 07:43:39 UTC+0000   2008-11-26 07:45:49 UTC+0000
0x00000000018a13c0 VMwareService.e    1756    672 0x08140220 2008-11-26 07:38:45 UTC+0000
0x00000000018af448 VMwareUser.exe     1904   1516 0x08140100 2008-11-26 07:38:31 UTC+0000
0x00000000018af860 VMwareTray.exe     1896   1516 0x08140200 2008-11-26 07:38:31 UTC+0000
0x00000000018e75e8 spoolsv.exe        1648    672 0x081401e0 2008-11-26 07:38:28 UTC+0000
0x00000000019456e8 csrss.exe           592    360 0x08140040 2008-11-15 23:42:56 UTC+0000
0x0000000001946020 svchost.exe         828    660 0x081400c0 2008-11-15 23:42:57 UTC+0000
0x00000000019467e0 services.exe        660    616 0x08140080 2008-11-15 23:42:56 UTC+0000
0x000000000194f658 svchost.exe        1016    660 0x08140100 2008-11-15 23:42:57 UTC+0000
0x00000000019533c8 svchost.exe         924    660 0x081400e0 2008-11-15 23:42:57 UTC+0000
0x00000000019ca478 explorer.exe       1516   1452 0x081401c0 2008-11-26 07:38:27 UTC+0000
0x00000000019dbc30 lsass.exe           684    620 0x081400a0 2008-11-26 07:38:15 UTC+0000
0x00000000019e4670 smss.exe            360      4 0x08140020 2008-11-26 07:38:11 UTC+0000
0x00000000019f7da0 svchost.exe        1164    672 0x08140140 2008-11-26 07:38:23 UTC+0000
0x000000001a0e6f0 svchost.exe        1264    672 0x08140160 2008-11-26 07:38:25 UTC+0000
0x000000001a1bd78 csrss.exe           596    360 0x08140040 2008-11-26 07:38:13 UTC+0000
0x000000001a2b100 winlogon.exe        620    360 0x08140060 2008-11-26 07:38:14 UTC+0000
0x000000001a3ba78 services.exe        672    620 0x08140080 2008-11-26 07:38:15 UTC+0000
0x000000001a3d360 svchost.exe         932    672 0x081400e0 2008-11-26 07:38:18 UTC+0000
0x000000001a59d70 svchost.exe         844    672 0x081400c0 2008-11-26 07:38:18 UTC+0000
0x000000001aa2300 svchost.exe        1064    672 0x08140120 2008-11-26 07:38:20 UTC+0000
0x000000001bcc830 System                4      0 0x00319000
```

Fig. 3. Difference in psscan and pslist results



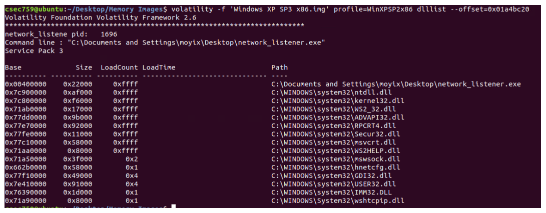
```
csec759@ubuntu:~/Desktop/Memory Images$ volatility -f 'Windows XP SP3 x86.img' profile=WinXPSP2x86 psxview
Volatility Foundation Volatility Framework 2.6
Offset(P)  Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
---------- -------------------- ------ ------ ------ -------- ------ ----- ------- -------- --------
0x01a2b100 winlogon.exe            620 True   True   True     True   True  True    True
0x01a3d360 svchost.exe             932 True   True   True     True   True  True    True
0x018a13c0 VMwareService.e        1756 True   True   True     True   True  True    True
0x018e75e8 spoolsv.exe            1648 True   True   True     True   True  True    True
0x019dbc30 lsass.exe               684 True   True   True     True   True  True    True
0x0184e3a8 wscntfy.exe             560 True   True   True     True   True  False   True
0x018af860 VMwareTray.exe         1896 True   True   True     True   True  True    True
0x01a4bc20 network_listene        1696 False  False  True     True   True  False   True
0x01843b28 wuauclt.exe            1372 True   True   True     True   True  True    True
0x01a59d70 svchost.exe             844 True   True   True     True   True  True    True
0x018af448 VMwareUser.exe         1904 True   True   True     True   True  True    True
0x019f7da0 svchost.exe            1164 True   True   True     True   True  True    True
0x018557e0 alg.exe                 512 True   True   True     True   True  True    True
0x01a3ba78 services.exe            672 True   True   True     True   True  True    True
0x019ca478 explorer.exe           1516 True   True   True     True   True  True    True
0x01a0e6f0 svchost.exe            1264 True   True   True     True   True  True    True
0x01aa2300 svchost.exe            1064 True   True   True     True   True  True    True
0x019e4670 smss.exe                360 True   True   True     True   False False   False
0x01bcc830 System                    4 True   True   True     True   False False   False
0x01a1bd78 csrss.exe               596 True   True   True     True   False True    True
0x01946020 svchost.exe             828 False  True   False    False  False False   False
0x019533c8 svchost.exe             924 False  True   True     False  False False   False
0x0185dda0 cmd.exe                 940 False  True   False    False  False False   False    2008-11-26 07:45:49 UTC+0000
0x019467e0 services.exe            660 False  True   True     False  False False   False
0x0181b748 alg.exe                 992 False  True   True     False  False False   False
0x0194f658 svchost.exe            1016 False  True   True     False  False False   False
0x019456e8 csrss.exe               592 False  True   True     False  False False   False
```

Fig. 4. psxview results from seven different lists



```
csec759@ubuntu:~/Desktop/Memory Images$ volatility -f 'Windows XP SP3 x86.img' profile=WinXPSP2x86 connscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x019cfbf0 192.168.101.128:1035      192.168.101.1:445         4
0x01a4abd0 192.168.101.128:1040      192.168.101.1:139         4
0x01a52b38 192.168.101.128:31337     192.168.101.1:1158        1696
```

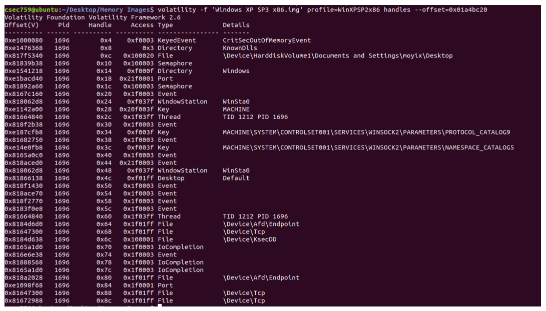
Fig. 5. Looking for suspicious connections



```
csec759@ubuntu:~/Desktop/Memory Images$ volatility -f 'Windows XP SP3 x86.img' profile=WinXPSP2x86 dlllist --offset=0x01a4bc20
Volatility Foundation Volatility Framework 2.6
************************************************************************
network_listene pid:   1696
Command line : "C:\Documents and Settings\moyix\Desktop\network_listener.exe"
Service Pack 3

Base             Size  LoadCount LoadTime                       Path
---------- ---------- ---------- ------------------------------ ----
0x00400000    0x22000     0xffff                                C:\Documents and Settings\moyix\Desktop\network_listener.exe
0x7c900000    0xaf000     0xffff                                C:\WINDOWS\system32\ntdll.dll
0x7c800000    0xf6000     0xffff                                C:\WINDOWS\system32\kernel32.dll
0x71ab0000    0x17000     0xffff                                C:\WINDOWS\system32\WS2_32.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
0x77c10000    0x58000     0xffff                                C:\WINDOWS\system32\msvcrt.dll
0x71aa0000     0x8000     0xffff                                C:\WINDOWS\system32\WS2HELP.dll
0x71a50000    0x3f000        0x2                                C:\WINDOWS\system32\mswsock.dll
0x662b0000    0x58000        0x1                                C:\WINDOWS\system32\hnetcfg.dll
0x77f10000    0x49000        0x4                                C:\WINDOWS\system32\GDI32.dll
0x7e410000    0x91000        0x4                                C:\WINDOWS\system32\USER32.dll
0x76390000    0x1d000        0x1                                C:\WINDOWS\system32\IMM32.DLL
0x71a90000     0x8000        0x1                                C:\WINDOWS\System32\wshtcpip.dll
```

Fig. 6. DLLs used by suspicious process



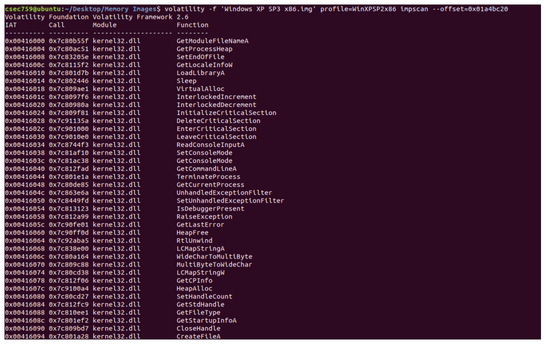
```
csec759@ubuntu:~/Desktop/Memory Images$ volatility -f 'Windows XP SP3 x86.img' profile=WinXPSP2x86 handles --offset=0x01a4bc20
Volatility Foundation Volatility Framework 2.6
Offset(V)     Pid     Handle     Access Type             Details
---------- ------ ---------- ---------- ---------------- -------
0xe1000080   1696        0x4    0xf0003 KeyedEvent       CritSecOutOfMemoryEvent
0xe1476368   1696        0x8        0x3 Directory        KnownDlls
0x817f5340   1696        0xc   0x100020 File             \Device\HarddiskVolume1\Documents and Settings\moyix\Desktop
0x81839b38   1696       0x10   0x100003 Semaphore
0xe1541218   1696       0x14    0xf000f Directory        Windows
0xe1bacd40   1696       0x18  0x21f0001 Port
0x81892a60   1696       0x1c   0x100003 Semaphore
0x8167c160   1696       0x20   0x1f0003 Event
0x818062d8   1696       0x24    0xf037f WindowStation    WinSta0
0xe1142a00   1696       0x28  0x20f003f Key              MACHINE
0x81664840   1696       0x2c   0x1f03ff Thread           TID 1212 PID 1696
0x818f2b38   1696       0x30   0x1f0003 Event
0xe187cfb8   1696       0x34    0xf003f Key              MACHINE\SYSTEM\CONTROLSET001\SERVICES\WINSOCK2\PARAMETERS\PROTOCOL_CATALOG9
0x81682750   1696       0x38   0x1f0003 Event
0xe14e0fb8   1696       0x3c    0xf003f Key              MACHINE\SYSTEM\CONTROLSET001\SERVICES\WINSOCK2\PARAMETERS\NAMESPACE_CATALOG5
0x8165a0c0   1696       0x40   0x1f0003 Event
0x818aced0   1696       0x44  0x21f0003 Event
0x818062d8   1696       0x48    0xf037f WindowStation    WinSta0
0x81866138   1696       0x4c    0xf01ff Desktop          Default
0x818f1430   1696       0x50   0x1f0003 Event
0x818ace70   1696       0x54   0x1f0003 Event
0x818f2770   1696       0x58   0x1f0003 Event
0x8183f0e8   1696       0x5c   0x1f0003 Event
0x81664840   1696       0x60   0x1f03ff Thread           TID 1212 PID 1696
0x8184d6d0   1696       0x64   0x1f01ff File             \Device\Afd\Endpoint
0x81647300   1696       0x68   0x1f01ff File             \Device\Tcp
0x8184d638   1696       0x6c   0x100001 File             \Device\KsecDD
0x8165a1d0   1696       0x70   0x1f0003 IoCompletion
0x816e6e38   1696       0x74   0x1f0003 Event
0x81888568   1696       0x78   0x1f0003 IoCompletion
0x8165a1d0   1696       0x7c   0x1f0003 IoCompletion
0x818a2028   1696       0x80   0x1f01ff File             \Device\Afd\Endpoint
0xe1098f68   1696       0x84   0x1f0001 Port
0x81647300   1696       0x88   0x1f01ff File             \Device\Tcp
0x81672988   1696       0x8c   0x1f01ff File             \Device\Tcp
```

Fig. 7. Handles used by suspicious process

errors. By analyzing event logs, digital forensic investigators can reconstruct the activities that occurred on a system and identify potential security incidents.

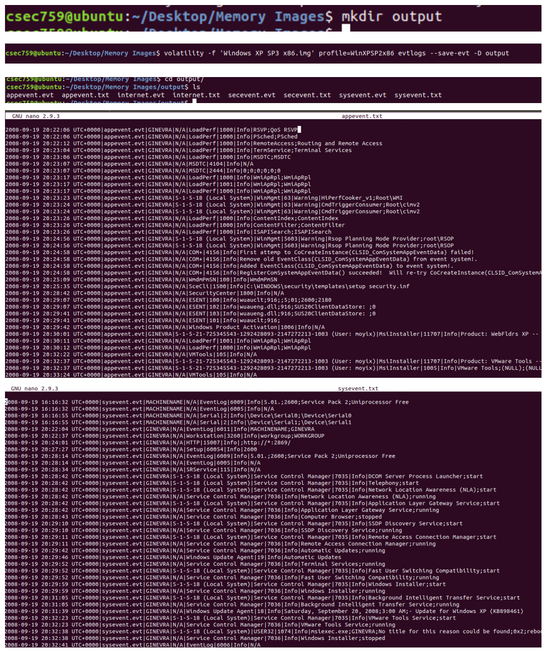
The evtlogs command supports the analysis of event logs from Windows XP through Windows 10. It can extract logs from both the Security and System channels and can also filter logs based on specific event IDs or time ranges.

We can use the tool as shown in Fig. 9. After generating the logs we can then use this information to further investigate the system and identify potential security incidents.



```
csec759@ubuntu:~/Desktop/Memory Images$ volatility -f 'Windows XP SP3 x86.img' profile=WinXPSP2x86 impscan --offset=0x01a4bc20
Volatility Foundation Volatility Framework 2.6
IAT        Call       Module               Function
---------- ---------- -------------------- --------
0x00416000 0x7c80b55f kernel32.dll         GetModuleFileNameA
0x00416004 0x7c80ac51 kernel32.dll         GetProcessHeap
0x00416008 0x7c83205e kernel32.dll         SetEndOfFile
0x0041600c 0x7c8115f2 kernel32.dll         GetLocaleInfoW
0x00416010 0x7c801d7b kernel32.dll         LoadLibraryA
0x00416014 0x7c802446 kernel32.dll         Sleep
0x00416018 0x7c809ae1 kernel32.dll         VirtualAlloc
0x0041601c 0x7c8097f6 kernel32.dll         InterlockedIncrement
0x00416020 0x7c80980a kernel32.dll         InterlockedDecrement
0x00416024 0x7c809f81 kernel32.dll         InitializeCriticalSection
0x00416028 0x7c91135a kernel32.dll         DeleteCriticalSection
0x0041602c 0x7c901000 kernel32.dll         EnterCriticalSection
0x00416030 0x7c9010e0 kernel32.dll         LeaveCriticalSection
0x00416034 0x7c8744f3 kernel32.dll         ReadConsoleInputA
0x00416038 0x7c81af10 kernel32.dll         SetConsoleMode
0x0041603c 0x7c81ac38 kernel32.dll         GetConsoleMode
0x00416040 0x7c812fad kernel32.dll         GetCommandLineA
0x00416044 0x7c801e1a kernel32.dll         TerminateProcess
0x00416048 0x7c80de85 kernel32.dll         GetCurrentProcess
0x0041604c 0x7c863e6a kernel32.dll         UnhandledExceptionFilter
0x00416050 0x7c8449fd kernel32.dll         SetUnhandledExceptionFilter
0x00416054 0x7c813123 kernel32.dll         IsDebuggerPresent
0x00416058 0x7c812a99 kernel32.dll         RaiseException
0x0041605c 0x7c90fe01 kernel32.dll         GetLastError
0x00416060 0x7c90ff0d kernel32.dll         HeapFree
0x00416064 0x7c92aba5 kernel32.dll         RtlUnwind
0x00416068 0x7c838e00 kernel32.dll         LCMapStringA
0x0041606c 0x7c80a164 kernel32.dll         WideCharToMultiByte
0x00416070 0x7c809c88 kernel32.dll         MultiByteToWideChar
0x00416074 0x7c80cd38 kernel32.dll         LCMapStringW
0x00416078 0x7c812f06 kernel32.dll         GetCPInfo
0x0041607c 0x7c9100a4 kernel32.dll         HeapAlloc
0x00416080 0x7c80cd27 kernel32.dll         SetHandleCount
0x00416084 0x7c812fc9 kernel32.dll         GetStdHandle
0x00416088 0x7c810ee1 kernel32.dll         GetFileType
0x0041608c 0x7c801ef2 kernel32.dll         GetStartupInfoA
0x00416090 0x7c809bd7 kernel32.dll         CloseHandle
0x00416094 0x7c801a28 kernel32.dll         CreateFileA
```

Fig. 8. Some of the API calls imported by suspicious process



```
csec759@ubuntu:~/Desktop/Memory Images$ mkdir output
```

```
csec759@ubuntu:~/Desktop/Memory Images$ volatility -f 'Windows XP SP3 x86.img' profile=WinXPSP2x86 evtlogs --save-evt -D output
```

```
csec759@ubuntu:~/Desktop/Memory Images$ cd output/
csec759@ubuntu:~/Desktop/Memory Images/output$ ls
appevent.evt  appevent.txt  internet.evt  internet.txt  secevent.evt  secevent.txt  sysevent.evt  sysevent.txt
```

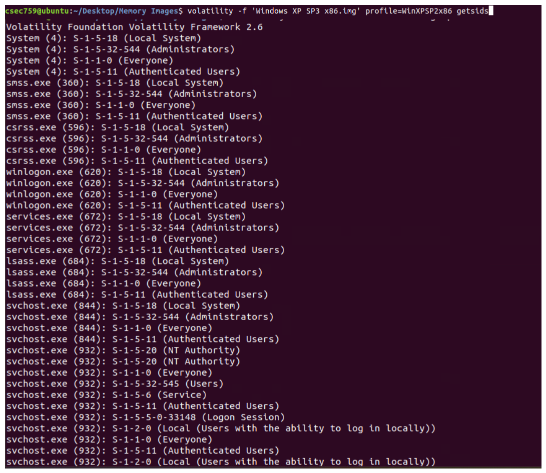
```
  GNU nano 2.9.3                                         appevent.txt

2008-09-19 20:22:06 UTC+0000|appevent.evt|GINEVRA|N/A|LoadPerf|1000|Info|RSVP;QoS RSVP
2008-09-19 20:22:06 UTC+0000|appevent.evt|GINEVRA|N/A|LoadPerf|1000|Info|PSched;PSched
2008-09-19 20:22:12 UTC+0000|appevent.evt|GINEVRA|N/A|LoadPerf|1000|Info|RemoteAccess;Routing and Remote Access
2008-09-19 20:23:04 UTC+0000|appevent.evt|GINEVRA|N/A|LoadPerf|1000|Info|TermService;Terminal Services
2008-09-19 20:23:06 UTC+0000|appevent.evt|GINEVRA|N/A|LoadPerf|1000|Info|MSDTC;MSDTC
2008-09-19 20:23:07 UTC+0000|appevent.evt|GINEVRA|N/A|MSDTC|4104|Info|N/A
2008-09-19 20:23:07 UTC+0000|appevent.evt|GINEVRA|N/A|MSDTC|2444|Info|0;0;0;0;0;0
2008-09-19 20:23:17 UTC+0000|appevent.evt|GINEVRA|N/A|LoadPerf|1000|Info|WmiApRpl;WmiApRpl
2008-09-19 20:23:17 UTC+0000|appevent.evt|GINEVRA|N/A|LoadPerf|1001|Info|WmiApRpl;WmiApRpl
2008-09-19 20:23:17 UTC+0000|appevent.evt|GINEVRA|N/A|LoadPerf|1000|Info|WmiApRpl;WmiApRpl
2008-09-19 20:23:23 UTC+0000|appevent.evt|GINEVRA|S-1-5-18 (Local System)|WinMgmt|63|Warning|HiPerfCooker_v1;Root\WMI
2008-09-19 20:23:24 UTC+0000|appevent.evt|GINEVRA|S-1-5-18 (Local System)|WinMgmt|63|Warning|CmdTriggerConsumer;Root\cimv2
2008-09-19 20:23:24 UTC+0000|appevent.evt|GINEVRA|S-1-5-18 (Local System)|WinMgmt|63|Warning|CmdTriggerConsumer;Root\cimv2
2008-09-19 20:23:26 UTC+0000|appevent.evt|GINEVRA|N/A|LoadPerf|1000|Info|ContentIndex;ContentIndex
2008-09-19 20:23:26 UTC+0000|appevent.evt|GINEVRA|N/A|LoadPerf|1000|Info|ContentFilter;ContentFilter
2008-09-19 20:23:26 UTC+0000|appevent.evt|GINEVRA|N/A|LoadPerf|1000|Info|ISAPISearch;ISAPISearch
2008-09-19 20:24:56 UTC+0000|appevent.evt|GINEVRA|S-1-5-18 (Local System)|WinMgmt|5603|Warning|Rsop Planning Mode Provider;root\RSOP
2008-09-19 20:24:56 UTC+0000|appevent.evt|GINEVRA|S-1-5-18 (Local System)|WinMgmt|5603|Warning|Rsop Planning Mode Provider;root\RSOP
2008-09-19 20:24:58 UTC+0000|appevent.evt|GINEVRA|N/A|COM+|4156|Info|First attemp to CoCreateInstance(CLSID_ComSystemAppEventData) failed!
2008-09-19 20:24:58 UTC+0000|appevent.evt|GINEVRA|N/A|COM+|4156|Info|Remove old EventClass(CLSID_ComSystemAppEventData) from event system!.
2008-09-19 20:24:58 UTC+0000|appevent.evt|GINEVRA|N/A|COM+|4156|Info|Added EventClass(CLSID_ComSystemAppEventData) to event system!.
2008-09-19 20:24:58 UTC+0000|appevent.evt|GINEVRA|N/A|COM+|4156|Info|RegisterComSystemAppEventData() succeeded!  Will re-try CoCreateInstance(CLSID_ComSystemA
2008-09-19 20:25:09 UTC+0000|appevent.evt|GINEVRA|N/A|WmdmPmSN|100|Info|WmdmPmSN
2008-09-19 20:25:35 UTC+0000|appevent.evt|GINEVRA|N/A|SceCli|1500|Info|C:\WINDOWS\security\templates\setup security.inf
2008-09-19 20:28:42 UTC+0000|appevent.evt|GINEVRA|N/A|SecurityCenter|1800|Info|N/A
2008-09-19 20:29:07 UTC+0000|appevent.evt|GINEVRA|N/A|ESENT|100|Info|wuauclt;916;;5;01;2600;2180
2008-09-19 20:29:07 UTC+0000|appevent.evt|GINEVRA|N/A|ESENT|102|Info|wuaueng.dll;916;SUS20ClientDataStore: ;0
2008-09-19 20:29:41 UTC+0000|appevent.evt|GINEVRA|N/A|ESENT|103|Info|wuaueng.dll;916;SUS20ClientDataStore: ;0
2008-09-19 20:29:41 UTC+0000|appevent.evt|GINEVRA|N/A|ESENT|101|Info|wuauclt;916;
2008-09-19 20:29:42 UTC+0000|appevent.evt|GINEVRA|N/A|Windows Product Activation|1006|Info|N/A
2008-09-19 20:30:01 UTC+0000|appevent.evt|GINEVRA|S-1-5-21-725345543-1292428093-2147272213-1003 (User: moyix)|MsiInstaller|11707|Info|Product: WebFldrs XP --
2008-09-19 20:30:11 UTC+0000|appevent.evt|GINEVRA|N/A|LoadPerf|1001|Info|WmiApRpl;WmiApRpl
2008-09-19 20:30:12 UTC+0000|appevent.evt|GINEVRA|N/A|LoadPerf|1000|Info|WmiApRpl;WmiApRpl
2008-09-19 20:32:22 UTC+0000|appevent.evt|GINEVRA|N/A|VMTools|105|Info|N/A
2008-09-19 20:32:37 UTC+0000|appevent.evt|GINEVRA|S-1-5-21-725345543-1292428093-2147272213-1003 (User: moyix)|MsiInstaller|11707|Info|Product: VMware Tools --
2008-09-19 20:32:37 UTC+0000|appevent.evt|GINEVRA|S-1-5-21-725345543-1292428093-2147272213-1003 (User: moyix)|MsiInstaller|1005|Info|VMware Tools;(NULL);(NULL
2008-09-19 20:33:24 UTC+0000|appevent.evt|GINEVRA|N/A|VMTools|105|Info|N/A
```

```
  GNU nano 2.9.3                                         sysevent.txt

2008-09-19 16:16:32 UTC+0000|sysevent.evt|MACHINENAME|N/A|EventLog|6009|Info|5.01.;2600;Service Pack 2;Uniprocessor Free
2008-09-19 16:16:32 UTC+0000|sysevent.evt|MACHINENAME|N/A|EventLog|6005|Info|N/A
2008-09-19 16:16:55 UTC+0000|sysevent.evt|MACHINENAME|N/A|Serial|2|Info|\Device\Serial0;\Device\Serial0
2008-09-19 16:16:55 UTC+0000|sysevent.evt|MACHINENAME|N/A|Serial|2|Info|\Device\Serial1;\Device\Serial1
2008-09-19 20:22:04 UTC+0000|sysevent.evt|GINEVRA|N/A|EventLog|6011|Info|MACHINENAME;GINEVRA
2008-09-19 20:22:37 UTC+0000|sysevent.evt|GINEVRA|N/A|Workstation|3260|Info|workgroup;WORKGROUP
2008-09-19 20:24:01 UTC+0000|sysevent.evt|GINEVRA|N/A|HTTP|15007|Info|;http://*:2869/
2008-09-19 20:27:27 UTC+0000|sysevent.evt|GINEVRA|N/A|Setup|60054|Info|2600
2008-09-19 20:28:14 UTC+0000|sysevent.evt|GINEVRA|N/A|EventLog|6009|Info|5.01.;2600;Service Pack 2;Uniprocessor Free
2008-09-19 20:28:14 UTC+0000|sysevent.evt|GINEVRA|N/A|EventLog|6005|Info|N/A
2008-09-19 20:28:34 UTC+0000|sysevent.evt|GINEVRA|N/A|SRService|115|Info|N/A
2008-09-19 20:28:42 UTC+0000|sysevent.evt|GINEVRA|S-1-5-18 (Local System)|Service Control Manager|7035|Info|DCOM Server Process Launcher;start
2008-09-19 20:28:42 UTC+0000|sysevent.evt|GINEVRA|S-1-5-18 (Local System)|Service Control Manager|7035|Info|Telephony;start
2008-09-19 20:28:42 UTC+0000|sysevent.evt|GINEVRA|S-1-5-18 (Local System)|Service Control Manager|7035|Info|Network Location Awareness (NLA);start
2008-09-19 20:28:42 UTC+0000|sysevent.evt|GINEVRA|N/A|Service Control Manager|7036|Info|Network Location Awareness (NLA);running
2008-09-19 20:28:42 UTC+0000|sysevent.evt|GINEVRA|S-1-5-18 (Local System)|Service Control Manager|7035|Info|Application Layer Gateway Service;start
2008-09-19 20:28:42 UTC+0000|sysevent.evt|GINEVRA|N/A|Service Control Manager|7036|Info|Application Layer Gateway Service;running
2008-09-19 20:28:43 UTC+0000|sysevent.evt|GINEVRA|N/A|Service Control Manager|7036|Info|Computer Browser;stopped
2008-09-19 20:29:10 UTC+0000|sysevent.evt|GINEVRA|S-1-5-18 (Local System)|Service Control Manager|7035|Info|SSDP Discovery Service;start
2008-09-19 20:29:10 UTC+0000|sysevent.evt|GINEVRA|N/A|Service Control Manager|7036|Info|SSDP Discovery Service;running
2008-09-19 20:29:11 UTC+0000|sysevent.evt|GINEVRA|S-1-5-18 (Local System)|Service Control Manager|7035|Info|Remote Access Connection Manager;start
2008-09-19 20:29:11 UTC+0000|sysevent.evt|GINEVRA|N/A|Service Control Manager|7036|Info|Remote Access Connection Manager;running
2008-09-19 20:29:42 UTC+0000|sysevent.evt|GINEVRA|N/A|Service Control Manager|7036|Info|Automatic Updates;running
2008-09-19 20:29:46 UTC+0000|sysevent.evt|GINEVRA|N/A|Windows Update Agent|19|Info|Automatic Updates
2008-09-19 20:29:52 UTC+0000|sysevent.evt|GINEVRA|N/A|Service Control Manager|7036|Info|Terminal Services;running
2008-09-19 20:29:52 UTC+0000|sysevent.evt|GINEVRA|S-1-5-18 (Local System)|Service Control Manager|7035|Info|Fast User Switching Compatibility;start
2008-09-19 20:29:52 UTC+0000|sysevent.evt|GINEVRA|N/A|Service Control Manager|7036|Info|Fast User Switching Compatibility;running
2008-09-19 20:29:59 UTC+0000|sysevent.evt|GINEVRA|S-1-5-18 (Local System)|Service Control Manager|7035|Info|Windows Installer;start
2008-09-19 20:29:59 UTC+0000|sysevent.evt|GINEVRA|N/A|Service Control Manager|7036|Info|Windows Installer;running
2008-09-19 20:31:05 UTC+0000|sysevent.evt|GINEVRA|S-1-5-18 (Local System)|Service Control Manager|7035|Info|Background Intelligent Transfer Service;start
2008-09-19 20:31:05 UTC+0000|sysevent.evt|GINEVRA|N/A|Service Control Manager|7036|Info|Background Intelligent Transfer Service;running
2008-09-19 20:31:39 UTC+0000|sysevent.evt|GINEVRA|N/A|Windows Update Agent|18|Info|Saturday, September 20, 2008;3:00 AM;- Update for Windows XP (KB898461)
2008-09-19 20:32:23 UTC+0000|sysevent.evt|GINEVRA|S-1-5-18 (Local System)|Service Control Manager|7035|Info|VMware Tools Service;start
2008-09-19 20:32:23 UTC+0000|sysevent.evt|GINEVRA|N/A|Service Control Manager|7036|Info|VMware Tools Service;running
2008-09-19 20:32:38 UTC+0000|sysevent.evt|GINEVRA|S-1-5-18 (Local System)|USER32|1074|Info|msiexec.exe;GINEVRA;No title for this reason could be found;0x2;reboo
2008-09-19 20:32:38 UTC+0000|sysevent.evt|GINEVRA|N/A|Service Control Manager|7036|Info|Windows Installer;stopped
2008-09-19 20:32:41 UTC+0000|sysevent.evt|GINEVRA|N/A|EventLog|6006|Info|N/A
```

Fig. 9. Setting up the evtlogs



```
csec759@ubuntu:~/Desktop/Memory Images$ volatility -f 'Windows XP SP3 x86.img' profile=WinXPSP2x86 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 (360): S-1-5-18 (Local System)
smss.exe (360): S-1-5-32-544 (Administrators)
smss.exe (360): S-1-1-0 (Everyone)
smss.exe (360): S-1-5-11 (Authenticated Users)
csrss.exe (596): S-1-5-18 (Local System)
csrss.exe (596): S-1-5-32-544 (Administrators)
csrss.exe (596): S-1-1-0 (Everyone)
csrss.exe (596): S-1-5-11 (Authenticated Users)
winlogon.exe (620): S-1-5-18 (Local System)
winlogon.exe (620): S-1-5-32-544 (Administrators)
winlogon.exe (620): S-1-1-0 (Everyone)
winlogon.exe (620): S-1-5-11 (Authenticated Users)
services.exe (672): S-1-5-18 (Local System)
services.exe (672): S-1-5-32-544 (Administrators)
services.exe (672): S-1-1-0 (Everyone)
services.exe (672): S-1-5-11 (Authenticated Users)
lsass.exe (684): S-1-5-18 (Local System)
lsass.exe (684): S-1-5-32-544 (Administrators)
lsass.exe (684): S-1-1-0 (Everyone)
lsass.exe (684): S-1-5-11 (Authenticated Users)
svchost.exe (844): S-1-5-18 (Local System)
svchost.exe (844): S-1-5-32-544 (Administrators)
svchost.exe (844): S-1-1-0 (Everyone)
svchost.exe (844): S-1-5-11 (Authenticated Users)
svchost.exe (932): S-1-5-20 (NT Authority)
svchost.exe (932): S-1-5-20 (NT Authority)
svchost.exe (932): S-1-1-0 (Everyone)
svchost.exe (932): S-1-5-32-545 (Users)
svchost.exe (932): S-1-5-6 (Service)
svchost.exe (932): S-1-5-11 (Authenticated Users)
svchost.exe (932): S-1-5-5-0-33148 (Logon Session)
svchost.exe (932): S-1-2-0 (Local (Users with the ability to log in locally))
svchost.exe (932): S-1-1-0 (Everyone)
svchost.exe (932): S-1-5-11 (Authenticated Users)
svchost.exe (932): S-1-2-0 (Local (Users with the ability to log in locally))
```

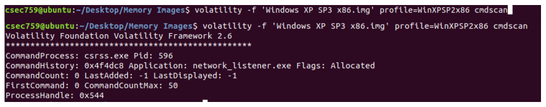
Fig. 10. Using getsids to get SIDs

IV. PLUGIN 2 - GETSIDS

The getsids command is a plugin in Volatility, this command is used to extract the Security Identifiers (SIDs) from a Windows memory dump.

Security Identifiers (SIDs) are unique identifiers assigned to user accounts, groups, and other security principals in Windows systems. By analyzing SIDs, we can determine the user account or group associated with a particular action or event in the system.

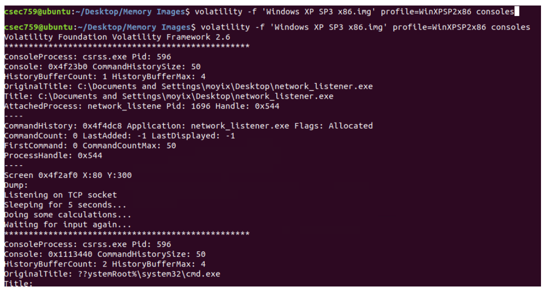
The getsids command in Volatility extracts the SIDs from the memory dump and displays them in a readable format as shown in Fig. 10. It can also filter the output to display only the SIDs associated with a particular process or thread.



```
csec759@ubuntu:~/Desktop/Memory Images$ volatility -f 'Windows XP SP3 x86.img' profile=WinXPSP2x86 cmdscan

csec759@ubuntu:~/Desktop/Memory Images$ volatility -f 'Windows XP SP3 x86.img' profile=WinXPSP2x86 cmdscan
Volatility Foundation Volatility Framework 2.6
**************************************************
CommandProcess: csrss.exe Pid: 596
CommandHistory: 0x4f4dc8 Application: network_listener.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x544
```

Fig. 11. Trying to list all commands used using cmdscan



```
csec759@ubuntu:~/Desktop/Memory Images$ volatility -f 'Windows XP SP3 x86.img' profile=WinXPSP2x86 consoles

csec759@ubuntu:~/Desktop/Memory Images$ volatility -f 'Windows XP SP3 x86.img' profile=WinXPSP2x86 consoles
Volatility Foundation Volatility Framework 2.6
**************************************************
ConsoleProcess: csrss.exe Pid: 596
Console: 0x4f23b0 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: C:\Documents and Settings\moyix\Desktop\network_listener.exe
Title: C:\Documents and Settings\moyix\Desktop\network_listener.exe
AttachedProcess: network_listene Pid: 1696 Handle: 0x544
----
CommandHistory: 0x4f4dc8 Application: network_listener.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x544
----
Screen 0x4f2af0 X:80 Y:300
Dump:
Listening on TCP socket
Sleeping for 5 seconds...
Doing some calculations...
Waiting for input again...
**************************************************
ConsoleProcess: csrss.exe Pid: 596
Console: 0x1113440 CommandHistorySize: 50
HistoryBufferCount: 2 HistoryBufferMax: 4
OriginalTitle: ??ystemRoot%\system32\cmd.exe
Title:
```

Fig. 12. Result of consoles plugin

V. Plugin 3 - cmdscan

The cmdscan command is a plugin in Volatility, this command is used to extract command histories from a Windows memory dump.

Command histories can be a valuable source of information for forensic investigators, as they can provide insight into the activities performed on the system. By analyzing command histories, investigators can determine what commands were executed, when they were executed, and by whom they were executed. It can also filter the output to display only the command histories associated with a particular process.

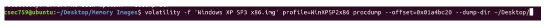
The cmdscan command in Volatility extracts the command histories from the memory dump and displays them in a readable format as shown in Fig. 11. However, we didn't find any commands during out investigation.

VI. Plugin 4 - consoles

The consoles command is a plugin in Volatility, this command is used to extract information about command prompt windows from a Windows memory dump.

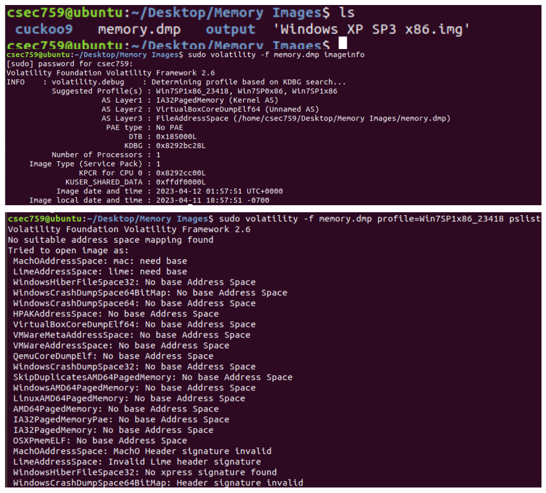
Command prompt windows can be a valuable source of information for us, as they can provide insight into the activities performed on the system. By analyzing command prompt windows, we can determine what commands were executed, when they were executed, and by whom they were executed.

The consoles command in Volatility extracts information about command prompt windows from the memory dump and displays it in a readable format. It can also filter the output to display only the command prompt windows associated with a particular process.



```
csec759@ubuntu:~/Desktop/Memory Images$ volatility -f 'Windows XP SP3 x86.img' profile=WinXPSP2x86 procdump --offset=0x01a4bc20 --dump-dir ~/Desktop/
```

Fig. 13. Dumping out an executable



```
csec759@ubuntu:~/Desktop/Memory Images$ ls
 cuckoo9   memory.dmp   output  'Windows XP SP3 x86.img'
csec759@ubuntu:~/Desktop/Memory Images$
csec759@ubuntu:~/Desktop/Memory Images$ sudo volatility -f memory.dmp imageinfo
[sudo] password for csec759:
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86
                     AS Layer1 : IA32PagedMemory (Kernel AS)
                     AS Layer2 : VirtualBoxCoreDumpElf64 (Unnamed AS)
                     AS Layer3 : FileAddressSpace (/home/csec759/Desktop/Memory Images/memory.dmp)
                      PAE type : No PAE
                           DTB : 0x185000L
                          KDBG : 0x8292bc28L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x8292cc00L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2023-04-12 01:57:51 UTC+0000
     Image local date and time : 2023-04-11 18:57:51 -0700

csec759@ubuntu:~/Desktop/Memory Images$ sudo volatility -f memory.dmp profile=Win7SP1x86_23418 pslist
Volatility Foundation Volatility Framework 2.6
No suitable address space mapping found
Tried to open image as:
 MachOAddressSpace: mac: need base
 LimeAddressSpace: lime: need base
 WindowsHiberFileSpace32: No base Address Space
 WindowsCrashDumpSpace64BitMap: No base Address Space
 WindowsCrashDumpSpace64: No base Address Space
 HPAKAddressSpace: No base Address Space
 VirtualBoxCoreDumpElf64: No base Address Space
 VMWareMetaAddressSpace: No base Address Space
 VMWareAddressSpace: No base Address Space
 QemuCoreDumpElf: No base Address Space
 WindowsCrashDumpSpace32: No base Address Space
 SkipDuplicatesAMD64PagedMemory: No base Address Space
 WindowsAMD64PagedMemory: No base Address Space
 LinuxAMD64PagedMemory: No base Address Space
 AMD64PagedMemory: No base Address Space
 IA32PagedMemoryPae: No base Address Space
 IA32PagedMemory: No base Address Space
 OSXPmemELF: No base Address Space
 MachOAddressSpace: MachO Header signature invalid
 LimeAddressSpace: Invalid Lime header signature
 WindowsHiberFileSpace32: No xpress signature found
 WindowsCrashDumpSpace64BitMap: Header signature invalid
```

Fig. 14. Issue with profile of cuckoo memdump

VII. Conclusion

During our study, we used a number of volatility plugins to analyze the given memory dump. In our investigation, we found a suspicious process, which we dumped that executable from memory using procdump as shown in Fig. 13 and this can be used further for static analysis using tools like IDApro or ghidra. We also tried to replicate this process using a process dump generted by cuckoo sandbox, but unfortunately, we faced an issue with the profile of memory dump generated by cuckoo as shown in Fig. 14(issue also raised by others). Overall, I think that volatility is very useful tool to study memory of machines which are suspected to be infected and can be a pre-step before doing advanced static analysis.

References

[1] https://github.com/volatilityfoundation/volatility/wiki/Command-Reference