

Karandeep Jaswal

4/24/23

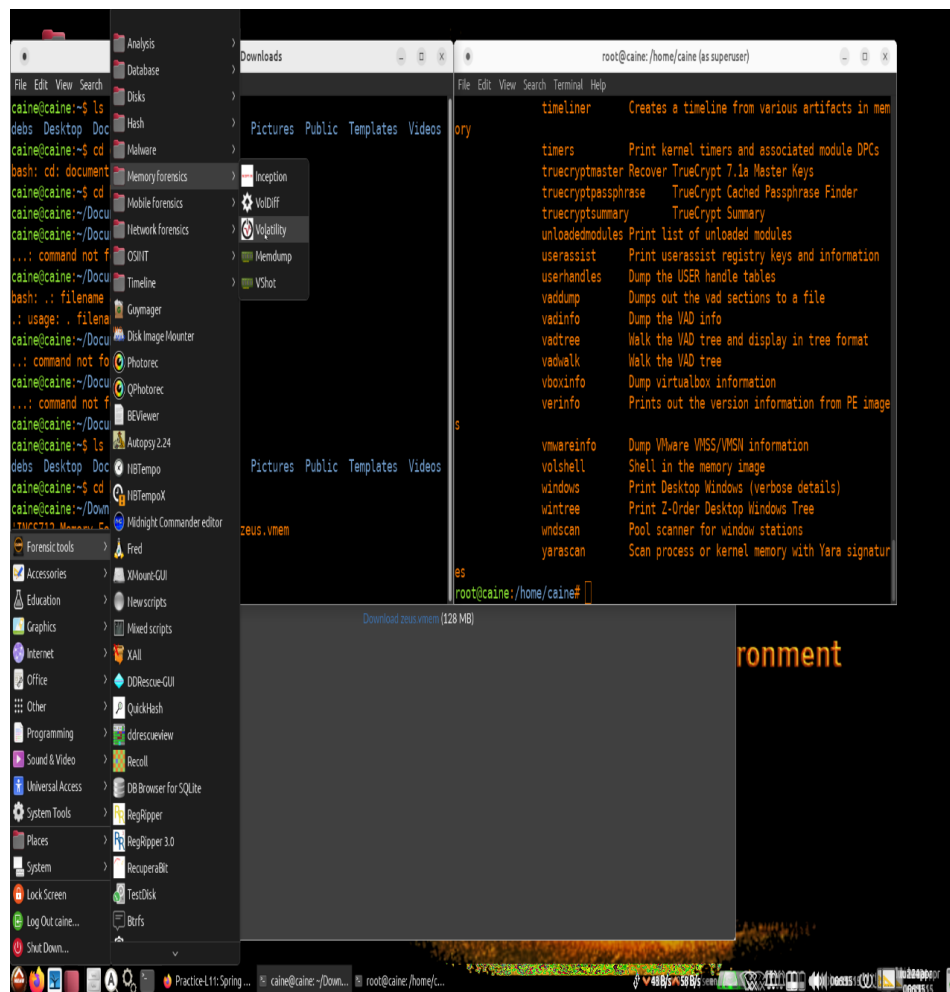
INCS 712

- 1) Download the zeus.vmem file on the Caine system.

```
debs Desktop Documents Downloads Music Pictures Public Templates Videos
caine@caine:~$ cd Downloads
caine@caine:~/Downloads$ ls
'INCS712 Memory Forensics Tutorial.pdf'  zeus.vmem
```

- 2) Run the Volatility tool, which analyzes the extract data from the volatile memory. We will use Volatility to analyze the zeus.vmem file.

Navigate to *Main Menu*> *Forensic tools*> *Memory Forensics*> *Volatility*



### 3) Use **volatility -f /home/caine/Downloads/zeus.vmem imageinfo**

The **-f** is used to specify the path to the memory image. **imageinfo** is used to get information about the memory image.

```
root@caine:/home/caine# volatility -f /home/caine/Downloads/zeus.vmem imageinfo
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.addrspaces.ieee1394 (AttributeError: /usr/local/lib/libforensic1394.so.2: undefined symbol: forensic1394_get_device_nodeid)
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 (/home/caine/Downloads/zeus.vmem)
      PAE type : PAE
      DTB : 0x319000L
      KDBG : 0x80544ce0L
      Number of Processors : 1
      Image Type (Service Pack) : 2
      KPCR for CPU 0 : 0xffdf000L
      KUSER_SHARED_DATA : 0xffdf000L
      Image date and time : 2010-08-15 19:17:56 UTC+0000
      Image local date and time : 2010-08-15 15:17:56 -0400
```

### 4) Set environment variables:

- **export VOLATILITY\_LOCATION=file:///home/caine/Downloads/zeus.vmem** [path to image file]
- **export VOLATILITY\_PROFILE=WinXPSP2x86** [Since the **Service Pack** is **2**, which corresponds to WinXPSP2x86 profile].

```
root@caine:/home/caine# export VOLATILITY_LOCATION=file:///home/caine/Downloads/zeus.vmem
root@caine:/home/caine# export VOLATILITY_PROFILE=WinXPSP2x86
```

### 5) Run **volatility pslist** to list the process of the system using the **pslist** plugin. Most basic volatility commands are constructed as: **volatility [plugin] -f [image] --profile=[profile]**

Note: We have already specified the **image** and **profile** in step 4).

```
root@caine:/home/caine# volatility pslist
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.addrspaces.ieee1394 (AttributeError: /usr/local/lib/libforensic1394.so.2: undefined symbol: forensic1394_get_device_nodeid)
Offset(V)  Name                PID  PPID  Thds  Hnds  Sess  Wow64  Start                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
0xff218230 vmacthlp.exe        844  676     1    37    0  0  2010-08-11 06:06:24 UTC+0000
0x80ff88d8 svchost.exe       856  676    29   336    0  0  2010-08-11 06:06:24 UTC+0000
0xff217560 svchost.exe       936  676    11   288    0  0  2010-08-11 06:06:24 UTC+0000
0x80fbf910 svchost.exe      1028  676    88  1424    0  0  2010-08-11 06:06:24 UTC+0000
0xff22d558 svchost.exe      1088  676     7    93    0  0  2010-08-11 06:06:25 UTC+0000
0xff203b80 svchost.exe      1148  676    15   217    0  0  2010-08-11 06:06:26 UTC+0000
0xff1d7da0 spoolsv.exe    1432  676    14   145    0  0  2010-08-11 06:06:26 UTC+0000
0xff1b8b28 vmtoolsd.exe     1668  676     5   225    0  0  2010-08-11 06:06:35 UTC+0000
0xff1fdc88 VMwareUpgradeHelper 1788  676     5   112    0  0  2010-08-11 06:06:38 UTC+0000
0xff143b28 TPAAutoConnSvc.e 1968  676     5   186    0  0  2010-08-11 06:06:39 UTC+0000
0xff25a7e0 alg.exe        216  676     8   120    0  0  2010-08-11 06:06:39 UTC+0000
0xff364310 wscntfy.exe       888  1028     1    40    0  0  2010-08-11 06:06:49 UTC+0000
0xff38b5f8 TPAAutoConnect.e 1084  1968     1    68    0  0  2010-08-11 06:06:52 UTC+0000
0x80f60da0 wuauctl.exe      1732  1028     7   189    0  0  2010-08-11 06:07:44 UTC+0000
0xff3865d0 explorer.exe       1724  1708    13   326    0  0  2010-08-11 06:09:29 UTC+0000
0xff3667e8 VMwareTray.exe      432  1724     1    60    0  0  2010-08-11 06:09:31 UTC+0000
0xff374980 VMwareUser.exe     452  1724     8   207    0  0  2010-08-11 06:09:32 UTC+0000
0x80f94588 wuauctl.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
```

- 6) Run **volatility pslist -P**. The **-P** switch gives the physical offset. Without **-P** we see the virtual offset.

```
root@caine:/home/caine# volatility pslist -P
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.addrspaces.iaeel394 (AttributeError: /usr/local/lib/libforensic1394.so.2: undefined symbol: forensic1394_get_device_nodeid)
Offset(P)  Name          PID  PPID  Thds  Hnds  Sess  Wow64  Start          Exit
-----
0x01214680 System          4      0    58   379  -----  0
0x05471020 smss.exe      544     4     3    21  -----  0 2010-08-11 06:06:21 UTC+0000
0x066f0da0 csrss.exe     608    544    10   410    0  0 2010-08-11 06:06:23 UTC+0000
0x066f0978 winlogon.exe  632    544    24   536    0  0 2010-08-11 06:06:23 UTC+0000
0x06015020 services.exe  676    632    16   288    0  0 2010-08-11 06:06:24 UTC+0000
0x05f47020 lsass.exe     688    632    21   405    0  0 2010-08-11 06:06:24 UTC+0000
0x06384230 vmacthlp.exe   844    676     1    37    0  0 2010-08-11 06:06:24 UTC+0000
0x0115b808 svchost.exe   856    676    29   336    0  0 2010-08-11 06:06:24 UTC+0000
0x063c5560 svchost.exe   936    676    11   288    0  0 2010-08-11 06:06:24 UTC+0000
0x01122910 svchost.exe  1028    676    88  1424    0  0 2010-08-11 06:06:24 UTC+0000
0x061ef558 svchost.exe  1088    676     7    93    0  0 2010-08-11 06:06:25 UTC+0000
0x06499b80 svchost.exe  1148    676    15   217    0  0 2010-08-11 06:06:26 UTC+0000
0x06945da0 spoolsv.exe 1432    676    14   145    0  0 2010-08-11 06:06:26 UTC+0000
0x069d5b28 vmtoolsd.exe 1668    676     5   225    0  0 2010-08-11 06:06:35 UTC+0000
0x0655fc08 VMUpgradeHelper 1788    676     5   112    0  0 2010-08-11 06:06:38 UTC+0000
0x0211ab28 TPAutoConnSvc.e 1968    676     5   106    0  0 2010-08-11 06:06:39 UTC+0000
0x05f027e0 alg.exe     216    676     8   120    0  0 2010-08-11 06:06:39 UTC+0000
0x04c2b310 wscntfy.exe   888   1028     1    40    0  0 2010-08-11 06:06:49 UTC+0000
0x049c15f8 TPAutoConnect.e 1084   1968     1    68    0  0 2010-08-11 06:06:52 UTC+0000
0x010c3da0 wuauclt.exe 1732   1028     7   189    0  0 2010-08-11 06:07:44 UTC+0000
0x04a065d0 explorer.exe 1724   1708    13   326    0  0 2010-08-11 06:09:29 UTC+0000
0x04b97e8 VMwareTray.exe  432   1724     1    60    0  0 2010-08-11 06:09:31 UTC+0000
0x04b5a900 VMwareUser.exe  452   1724     8   207    0  0 2010-08-11 06:09:32 UTC+0000
0x010f7588 wuauclt.exe  468   1028     4   142    0  0 2010-08-11 06:09:37 UTC+0000
0x06238020 cmd.exe      124   1668     0  -----  0  0 2010-08-15 19:17:55 UTC+0000 2010-08-15 19:17:56 UTC+0000
```

- 7) Run **volatility pstree** to view the process list in tree form.

```
root@caine:/home/caine# volatility pstree
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.addrspaces.iaeel394 (AttributeError: /usr/local/lib/libforensic1394.so.2: undefined symbol: forensic1394_get_device_nodeid)
Name          Pid  PPID  Thds  Hnds  Time
-----
0x010b1660: System          4      0    58   379  1970-01-01 00:00:00 UTC+0000
. 0xff2ab020: smss.exe      544     4     3    21  2010-08-11 06:06:21 UTC+0000
.. 0xff1ec978: winlogon.exe  632    544    24   536  2010-08-11 06:06:23 UTC+0000
... 0xff255020: lsass.exe     688    632    21   405  2010-08-11 06:06:24 UTC+0000
... 0xff247020: services.exe  676    632    16   288  2010-08-11 06:06:24 UTC+0000
.... 0xff1b8b28: vmtoolsd.exe 1668    676     5   225  2010-08-11 06:06:35 UTC+0000
..... 0xff224020: cmd.exe      124   1668     0  -----  2010-08-15 19:17:55 UTC+0000
.... 0x80ff88d8: svchost.exe   856    676    29   336  2010-08-11 06:06:24 UTC+0000
.... 0xff1d7da0: spoolsv.exe 1432    676    14   145  2010-08-11 06:06:26 UTC+0000
.... 0x80fbf910: svchost.exe  1028    676    88  1424  2010-08-11 06:06:24 UTC+0000
..... 0x80f60da0: wuauclt.exe 1732   1028     7   189  2010-08-11 06:07:44 UTC+0000
..... 0x80f94588: wuauclt.exe  468   1028     4   142  2010-08-11 06:09:37 UTC+0000
..... 0xff364310: wscntfy.exe   888   1028     1    40  2010-08-11 06:06:49 UTC+0000
.... 0xff217560: svchost.exe   936    676    11   288  2010-08-11 06:06:24 UTC+0000
.... 0xff143b28: TPAutoConnSvc.e 1968    676     5   106  2010-08-11 06:06:39 UTC+0000
..... 0xff38b5f8: TPAutoConnect.e 1084   1968     1    68  2010-08-11 06:06:52 UTC+0000
.... 0xff22d558: svchost.exe  1088    676     7    93  2010-08-11 06:06:25 UTC+0000
.... 0xff218230: vmacthlp.exe   844    676     1    37  2010-08-11 06:06:24 UTC+0000
.... 0xff25a7e0: alg.exe     216    676     8   120  2010-08-11 06:06:39 UTC+0000
.... 0xff203b80: svchost.exe  1148    676    15   217  2010-08-11 06:06:26 UTC+0000
.... 0xff1fdc88: VMUpgradeHelper 1788    676     5   112  2010-08-11 06:06:38 UTC+0000
. 0xff1acd80: csrss.exe     608    544    10   410  2010-08-11 06:06:23 UTC+0000
0xff3865d0: explorer.exe 1724   1708    13   326  2010-08-11 06:09:29 UTC+0000
. 0xff374980: VMwareUser.exe  452   1724     8   207  2010-08-11 06:09:32 UTC+0000
. 0xff3667e8: VMwareTray.exe  432   1724     1    60  2010-08-11 06:09:31 UTC+0000
```

## Reviewing Network Artifacts

- 8) Run **volatility connections** to see active network connections (virtual offset).

```
root@caine:/home/caine# volatility connections
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.addrspace.ieee1394 (AttributeError: /usr/local/lib/libforensic1394.so.2: undefined symbol: forensic1394_get_device_nodeid)
Offset(V) Local Address Remote Address Pid
.....
```

- 9) Run **volatility connections -P** to see active network connections on the physical offset.

```
root@caine:/home/caine# volatility connections -P
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.addrspace.ieee1394 (AttributeError: /usr/local/lib/libforensic1394.so.2: undefined symbol: forensic1394_get_device_nodeid)
Offset(P) Local Address Remote Address Pid
.....
```

- 10) Run **volatility connscan** to see recent network connections.

Just because there are no active network connections at the time of capture does not mean no network connections were established.

```
root@caine:/home/caine# volatility connscan
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.addrspace.ieee1394 (AttributeError: /usr/local/lib/libforensic1394.so.2: undefined symbol: forensic1394_get_device_nodeid)
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
```

There seems to be two connections to a remote IP address 193.104.41.75 over port 80 (http). The 2 connections were made by Process ID=856, which matches svchost.exe – this can be observed from process list obtained in 5). This behavior is suspicious and will be analyzed further.

```
root@caine:/home/caine# volatility pslist
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.addrspace.ieee1394 (AttributeError: /usr/local/lib/libforensic1394.so.2: undefined symbol: forensic1394_get_device_nodeid)
Offset(V) Name PID PPID Thds Hnds Sess Wow64 Start Exit
.....
0x010b1660 System 4 0 58 379 ----- 0
0xff2ab020 smss.exe 544 4 3 21 ----- 0 2010-08-11 06:06:21 UTC+0000
0xff1edca0 csrss.exe 608 544 10 410 0 0 2010-08-11 06:06:23 UTC+0000
0xff1ed978 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
0xff218230 vmacthlp.exe 844 676 1 37 0 0 2010-08-11 06:06:24 UTC+0000
0x80f78d08 svchost.exe 856 676 29 336 0 0 2010-08-11 06:06:24 UTC+0000
0xff217560 svchost.exe 936 676 11 288 0 0 2010-08-11 06:06:24 UTC+0000
0x80fb9f10 svchost.exe 1028 676 88 1424 0 0 2010-08-11 06:06:24 UTC+0000
0xff22d558 svchost.exe 1088 676 7 93 0 0 2010-08-11 06:06:25 UTC+0000
0xff203b80 svchost.exe 1148 676 15 217 0 0 2010-08-11 06:06:26 UTC+0000
0xff1d7da0 spoolsv.exe 1432 676 14 145 0 0 2010-08-11 06:06:26 UTC+0000
0xff1b0b28 umtoolld.exe 1668 676 5 225 0 0 2010-08-11 06:06:35 UTC+0000
0xff1fdca8 WUUpgradeHelper 1788 676 5 112 0 0 2010-08-11 06:06:38 UTC+0000
0xff143b28 TPAutoConnSvc.e 1968 676 5 106 0 0 2010-08-11 06:06:39 UTC+0000
0xff25a7e0 alg.exe 216 676 8 120 0 0 2010-08-11 06:06:39 UTC+0000
0xff364310 wscntfy.exe 888 1028 1 40 0 0 2010-08-11 06:06:49 UTC+0000
0xff38b5f8 TPAutoConnect.e 1084 1968 1 68 0 0 2010-08-11 06:06:52 UTC+0000
0x80f60da0 wuauclt.exe 1732 1028 7 189 0 0 2010-08-11 06:07:44 UTC+0000
0xff3865d0 explorer.exe 1724 1708 13 326 0 0 2010-08-11 06:09:29 UTC+0000
0xff3667e8 VMwareTray.exe 432 1724 1 60 0 0 2010-08-11 06:09:31 UTC+0000
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 2010-08-15 19:17:55 UTC+0000 2010-08-15 19:17:56 UTC+0000
```

11) To check open ports/ sockets, run **volatility sockscan**.

```
root@caine:/home/caine# volatility sockscan
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.addrspaces.ieee1394 (AttributeError: /usr/local/lib/libforensic1394.so.2: undefined symbol: forensic1394_get_device_nodeid)
Offset(P)      PID    Port  Proto Protocol      Address      Create Time
-----
0x007c0a20     1148  1900   17 UDP           172.16.176.143 2010-08-15 19:15:43 UTC+0000
0x01120c40         4   445   17 UDP           0.0.0.0 2010-08-11 06:06:17 UTC+0000
0x01131930     1088  1025   17 UDP           0.0.0.0 2010-08-11 06:06:38 UTC+0000
0x01134008         4     0   47 GRE           0.0.0.0 2010-08-11 06:08:00 UTC+0000
0x011568a8         4   138   17 UDP           172.16.176.143 2010-08-15 19:15:43 UTC+0000
0x0115f128     936   135    6 TCP           0.0.0.0 2010-08-11 06:06:24 UTC+0000
0x02dead28     216  1026    6 TCP           127.0.0.1 2010-08-11 06:06:39 UTC+0000
0x04863458         4   139    6 TCP           172.16.176.143 2010-08-15 19:15:43 UTC+0000
0x04864578     1028   68   17 UDP           172.16.176.143 2010-08-15 19:17:26 UTC+0000
0x04864a08         4   137   17 UDP           172.16.176.143 2010-08-15 19:15:43 UTC+0000
0x04a4be98         4  1033    6 TCP           0.0.0.0 2010-08-11 06:08:00 UTC+0000
0x04a51d28     1028  1058    6 TCP           0.0.0.0 2010-08-15 19:17:56 UTC+0000
0x04be7008         4   445    6 TCP           0.0.0.0 2010-08-11 06:06:17 UTC+0000
0x05dee200     1028  123   17 UDP           127.0.0.1 2010-08-15 19:15:43 UTC+0000
0x05e33d68     1148  1900   17 UDP           127.0.0.1 2010-08-15 19:15:43 UTC+0000
0x05f44008     688   500   17 UDP           0.0.0.0 2010-08-11 06:06:35 UTC+0000
0x05f48008     1028  123   17 UDP           127.0.0.1 2010-08-15 19:17:56 UTC+0000
0x06236e98     1028   68   17 UDP           172.16.176.143 2010-08-15 19:17:56 UTC+0000
0x06237b70     688     0  255 Reserved    0.0.0.0 2010-08-11 06:06:35 UTC+0000
0x06450478     856 29220    6 TCP           0.0.0.0 2010-08-15 19:17:27 UTC+0000
0x06496a20     1148  1900   17 UDP           127.0.0.1 2010-08-15 19:17:56 UTC+0000
0x069d5250     688  4500   17 UDP           0.0.0.0 2010-08-11 06:06:35 UTC+0000
```

12) Analyze the malicious IP address – 193.104.41.75 via <https://www.iplocation.net/>

```
root@caine:/home/caine# volatility connscan
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.addrspaces.ieee1394 (AttributeError: /usr/local/lib/libforensic1394.so.2: undefined symbol: forensic1394_get_device_nodeid)
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
```

The IP address is from Czech Republic.

### Geolocation data from IP2Location (Product: DB6, 2023-4-1)



**IP ADDRESS:** 193.104.41.75



**ISP:** ISP Alliance a.s.



**COUNTRY:** Czech Republic



**ORGANIZATION:** Not available



**REGION:** Pardubický kraj



**LATITUDE:** 50.0413



**CITY:** Pardubice




**LONGITUDE:** 15.7725

Use <https://www.ipvoid.com> to check IP blacklist for IP address 193.104.41.75.

193.104.41.75	Check IP Address
---------------	------------------

## IP Address Information

Analysis Date	2023-04-24 02:05:55
Elapsed Time	4 seconds
Detections Count	0/106
IP Address	<b>193.104.41.75</b> <a href="#">Find Sites</a>   <a href="#">IP Whois</a>
Reverse DNS	75.41.104.193.cpsnet.cz
ASN	<a href="#">AS207886</a>
ISP	ISP Alliance a.s.
Continent	Europe
Country Code	 (CZ) Czechia
Latitude / Longitude	<a href="#">Google Map</a>
City	Pardubice
Region	Pardubický kraj

Not blacklisted as of 4/24/23. However, could have been used to run a botnet earlier.

## Dumping Suspicious Processes and Drivers

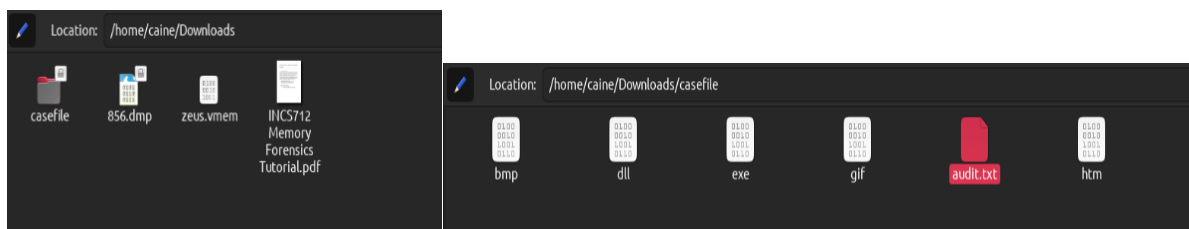
- 13) Run **volatility memdump --dump-dir=/home/caine/Downloads/ -p 856** to get a memory dump for PID=856

```
root@caine:/home/caine# volatility memdump --dump-dir=/home/caine/Downloads/ -p 856
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.addrspace.i386 (AttributeError: /usr/local/lib/libforensic1394.so.2: undefined symbol: forensic1394_get_device_nodeid)
*****
Writing svchost.exe [ 856] to 856.dmp
root@caine:/home/caine#
```

- 14) Run **foremost -i /home/caine/Downloads/856.dmp -o /home/caine/Downloads/casefile** to extract files from the memory dump created in 13).

```
root@caine:/home/caine# foremost -i /home/caine/Downloads/856.dmp -o /home/caine/Downloads/casefile/
Processing: /home/caine/Downloads/856.dmp
|
*|
```

856.dmp is the file created after 13) and the casefile folder is created after running 14).



Contents of audit.txt give the list of 90 extracted files.

```
audit.txt (/home/caine/Downloads/casefile) - Pluma (as supervisor)
File Edit View Search Tools Documents Help
[Icons] Open Save Undo Redo Print
audit.txt
1 Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
2 Audit File
3
4 Foremost started at Mon Apr 24 07:28:20 2023
5 Invocation: foremost -i /home/caine/Downloads/856.dmp -o /home/caine/Downloads/casefile/
6 Output directory: /home/caine/Downloads/casefile
7 Configuration file: /etc/foremost.conf
8
9 File: /home/caine/Downloads/856.dmp
10 Start: Mon Apr 24 07:28:20 2023
11 Length: 60 MB (63823072 bytes)
12
13 Num Name (bs=512) Size File Offset Comment
14
15 0: 00060890.gif 64 B 34862368 (10 x 10)
16 1: 00059408.bmp 27 KB 30417377 (128 x 256)
17 2: 00059630.bmp 21 KB 30530770 (7085304 x 1)
18 3: 00062873.bmp 27 KB 32511185 (128 x 256)
19 4: 00018136.htm 218 B 925845
20 5: 00018144.htm 218 B 9289941
21 6: 00018160.htm 218 B 9298133
22 7: 00018016.htm 218 B 55611805
23 8: 00018024.htm 218 B 55615791
24 9: 00018040.htm 218 B 55623893
25 10: 0001472.dll 202 KB 753664 08/04/2004 07:56:40
26 11: 0004208.dll 773 KB 2154496 08/04/2004 07:56:36
27 12: 0005824.exe 14 KB 2861888 08/04/2004 06:14:46
28 13: 0005976.dll 2 MB 3859712 08/04/2004 07:56:41
29 14: 0001648.dll 60 KB 5963776 08/04/2004 07:56:29
30 15: 0001324.dll 233 KB 6653888 08/04/2004 07:56:25
31 16: 0001228.dll 540 KB 631456 08/04/2004 07:57:39
32 17: 0001384.dll 18 KB 6852608 08/04/2004 07:56:39
33 18: 0001380.dll 126 KB 7084160 08/04/2004 07:59:11
34 19: 0001420.dll 567 KB 7270400 08/04/2004 07:56:30
35 20: 00016328.dll 12 KB 8359936 08/17/2001 20:49:09
36 21: 00016352.exe 9 KB 8372224 08/17/2001 20:57:58
37 22: 00020992.dll 1 MB 10747904 08/04/2004 07:57:38
38 23: 00025056.dll 128 KB 1282672 08/04/2004 05:59:05
39 24: 00031696.exe 1 MB 16228352 08/04/2004 06:17:30
40 25: 00063464.exe 370 KB 42733568 08/04/2004 06:14:22
41 26: 00099304.exe 167 KB 50843648 08/04/2004 06:07:46
42 27: 00010448.exe 81 KB 51429376 08/04/2004 06:15:03
43 28: 00010312.exe 256 KB 51871744 08/04/2004 06:00:09
44 29: 00010208.exe 320 KB 52099136 08/04/2004 06:14:44
45 30: 00010432.exe 135 KB 53428224 08/04/2004 06:14:13
46 31: 00010572.exe 131 KB 54286464 08/04/2004 06:04:48
47 32: 00010600.exe 172 KB 54579200 08/04/2004 06:20:05
48 33: 00010652.exe 135 KB 54759424 08/04/2004 06:14:13
```

```
53: 00115696.exe 51 KB 59236352 08/04/2004 06:14:36
54: 00115832.exe 40 KB 59305984 08/04/2004 06:00:12
55: 00115968.exe 56 KB 59375616 08/04/2004 05:59:34
56: 00116096.exe 39 KB 59441152 07/19/2001 22:28:37
57: 00116224.exe 35 KB 59506688 08/04/2004 05:59:19
58: 00116352.exe 40 KB 59572224 08/04/2004 06:05:06
59: 00116520.exe 34 KB 59658240 08/04/2004 06:04:11
60: 00116616.dll 39 KB 59707392 08/04/2004 05:58:52
61: 00116790.exe 225 KB 59796656 08/04/2004 05:59:25
62: 00117376.dll 35 KB 60096512 08/04/2004 06:08:18
63: 00117472.exe 24 KB 60145664 08/04/2004 05:59:40
64: 00117528.exe 24 KB 60174336 08/04/2004 05:58:32
65: 00117592.exe 26 KB 60207104 08/04/2004 05:59:25
66: 00117672.exe 20 KB 60248064 08/04/2004 06:08:34
67: 00117712.exe 29 KB 60268544 01/23/2009 02:17:16
68: 00117816.exe 18 KB 60321792 08/04/2004 06:07:47
69: 00117856.exe 17 KB 60342272 08/17/2001 20:49:53
70: 00117920.exe 20 KB 60375040 08/04/2004 05:59:24
71: 00117968.exe 30 KB 60399616 08/04/2004 06:00:38
72: 00118064.dll 24 KB 60448768 08/04/2004 06:08:15
73: 00118144.dll 12 KB 60489728 08/17/2001 20:49:09
74: 00118168.exe 9 KB 60502016 08/17/2001 20:57:58
75: 00118200.exe 11 KB 60518400 11/13/2008 02:50:11
76: 00118800.exe 15 KB 60825600 08/04/2004 05:59:06
77: 00118848.exe 9 KB 60850176 08/17/2001 20:55:29
78: 00119008.exe 15 KB 60932096 08/04/2004 06:07:47
79: 00119184.exe 10 KB 61022208 08/17/2001 20:53:19
80: 00119296.dll 6 KB 61079552 08/17/2001 20:49:10
81: 00119312.exe 4 KB 61087744 08/17/2001 21:07:23
82: 00119336.exe 4 KB 61100032 09/29/2008 06:49:38
83: 00119352.dll 4 KB 61108224 08/17/2001 21:02:58
84: 00119368.exe 7 KB 61116416 08/17/2001 20:49:37
85: 00119384.exe 4 KB 61124608 08/17/2001 20:57:28
86: 00119416.exe 7 KB 61140992 02/09/2010 23:19:29
87: 00119616.exe 3 KB 61243392 08/17/2001 20:53:12
88: 00119656.exe 3 KB 61263872 08/17/2001 20:59:40
89: 00120956.exe 328 KB 61468672 08/04/2004 06:14:44
90: Finish: Mon Apr 24 07:28:31 2023
91 90 FILES EXTRACTED
92
93 gif:= 1
94 bmp:= 3
95 htm:= 6
96 exe:= 80
97
98
99 Foremost finished at Mon Apr 24 07:28:31 2023
```



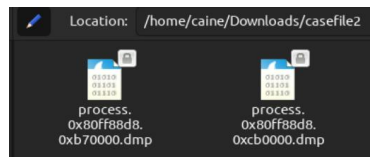
- 15) Run the *malfind* plug-in to find injected code and dumping sections for PID=856:  
**volatility malfind -p 856 --dump-dir /home/caine/Downloads/casefile2**

```
root@caine:/home/caine# volatility malfind -p 856 --dump-dir /home/caine/Downloads/casefile2/
[[AVolatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.addrspaces.linux1394 (AttributeError: /usr/local/lib/libforensic1394.so.2: undefined symbol: forensic1394_get_device_nodeid)
Process: svchost.exe Pid: 856 Address: 0xb70000
Vad Tag: Vad5 Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 38, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x0000000000007000 4d 5a 90 00 03 00 00 04 00 00 ff ff 00 00 HZ.....
0x0000000000007010 58 00 00 00 00 00 00 00 00 00 00 00 00 00 .....0.....
0x0000000000007020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x0000000000007030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

0x0000000000007000 4d      DEC EBP
0x0000000000007001 5a      POP EDX
0x0000000000007002 90      NOP
0x0000000000007003 0003    ADD [EBX], AL
0x0000000000007005 0000    ADD [EAX], AL
0x0000000000007007 000400  ADD [EAX+EAX], AL
0x0000000000007008 0000    ADD [EAX], AL
0x000000000000700c ff      DB 0xff
0x000000000000700d ff00  INC DWORD [EAX]
0x000000000000700f 00b800000000  ADD [EAX+0x0], BH
0x0000000000007015 0000    ADD [EAX], AL
0x0000000000007017 004000  ADD [EAX+0x0], AL
0x0000000000007018 0000    ADD [EAX], AL
0x000000000000701c 0000    ADD [EAX], AL
0x000000000000701e 0000    ADD [EAX], AL
0x0000000000007020 0000    ADD [EAX], AL
0x0000000000007022 0000    ADD [EAX], AL
0x0000000000007024 0000    ADD [EAX], AL
0x0000000000007026 0000    ADD [EAX], AL
0x0000000000007028 0000    ADD [EAX], AL
0x000000000000702a 0000    ADD [EAX], AL
0x000000000000702c 0000    ADD [EAX], AL
0x000000000000702e 0000    ADD [EAX], AL
0x0000000000007030 0000    ADD [EAX], AL
0x0000000000007032 0000    ADD [EAX], AL
0x0000000000007034 0000    ADD [EAX], AL
0x0000000000007036 0000    ADD [EAX], AL
```

The files are extracted to the directory specified (in this case, /home/caine/Downloads/casefile2)



Upload the file on virustotal.com to check if they are malicious. In our case, 62/70 security vendors marked the file as malicious.

VirusTotal - File - 8c3be5dc65aa35d68f2aba1d3d9b0f40d5118f622eb2ec97c9463bd1f1ba1

62 / 70 security vendors and no sandboxes flagged this file as malicious

8c3be5dc65aa35d68f2aba1d3d9b0f40d5118f622eb2ec97c9463bd1f1ba1 152.00 KB 2023-04-12 17:13:58 UTC 11 days ago

process.0xb0ff8bd8.0xb70000.dmp

Popular threat label: Trojan.BotRazy Threat categories: trojan, psn Family labels: zbot, razy, smrf

Security vendors' analysis

Vendor	Detection	Confidence
Acronis (Static ML)	Suspicious	High
Alibaba	Trojan.PSW.Win32.ShellCode.Src75809	High
Antiy-AVL	Trojan(Spy).Win32.Zbot	High
Avast	StCrypt.BT [T]	High
Avira (no cloud)	TR/Patched.Pem.Gen	High
BitDefender Theta	Gen.ML.ZaveF.38132.p2@eq7nHc	High
ClamAV	Win.Malware.Agent.6369795-0	High
Cylance	Unstable	High
Avira (no cloud)	Worm.Win32.IRCBot.C136977	High
Gen Variant	Gen Variant.Razy.447136	High
Trojan.Razy	Trojan.Razy.DIG2A0	High
St.Crypt.BT	St.Crypt.BT [T]	High
Gen Variant	Gen Variant.Razy.447136	High
W32.ADetected	W32.ADetected.01	High
Win.Malicious	Win.Malicious_confidence_100% (W)	High
Malicious (score: 100)	Malicious (score: 100)	High



- 16) Run **strings 856.dmp | grep "http://"** to get a list of URLs from the *856.dmp* that may be malicious and could be analyzed further.

```
root@caine:/home/caine/Downloads# strings /home/caine/Downloads/856.dmp | grep "http://"
http://193.104.41.75/cbd/75.bro
http://www.microsoft.com/provisioning/MsChapV2UserPropertiesV1
http://www.microsoft.com/provisioning/MsPeapUserPropertiesV1
http://www.microsoft.com/provisioning/WirelessProfile
http://%s/%s
Ghttp://crl.microsoft.com/pki/crl/products/MicProSecSerCA_2007-12-04.crl
Ghttp://www.microsoft.com/pki/crl/products/MicProSecSerCA_2007-12-04.crl\
@http://www.microsoft.com/pki/certs/MicProSecSerCA_2007-12-04.crt0
Uhttp://crl.microsoft.com/pki/crl/products/MicrosoftProductSecureCommunicationsPCA.crl
Uhttp://www.microsoft.com/pki/crl/products/MicrosoftProductSecureCommunicationsPCA.crl0j
Nhttp://www.microsoft.com/pki/certs/MicrosoftProductSecureCommunicationsPCA.crt0
?http://crl.microsoft.com/pki/crl/products/microsoftrootcert.crl0T
8http://www.microsoft.com/pki/certs/MicrosoftRootCert.crt0
Ghttp://crl.microsoft.com/pki/crl/products/MicProSecSerCA_2007-12-04.crl
Ghttp://www.microsoft.com/pki/crl/products/MicProSecSerCA_2007-12-04.crl\
@http://www.microsoft.com/pki/certs/MicProSecSerCA_2007-12-04.crt0
Uhttp://crl.microsoft.com/pki/crl/products/MicrosoftProductSecureCommunicationsPCA.crl
Uhttp://www.microsoft.com/pki/crl/products/MicrosoftProductSecureCommunicationsPCA.crl0j
Nhttp://www.microsoft.com/pki/certs/MicrosoftProductSecureCommunicationsPCA.crt0
?http://crl.microsoft.com/pki/crl/products/microsoftrootcert.crl0T
8http://www.microsoft.com/pki/certs/MicrosoftRootCert.crt0
Ghttp://crl.microsoft.com/pki/crl/products/MicProSecSerCA_2007-12-04.crl
Ghttp://www.microsoft.com/pki/crl/products/MicProSecSerCA_2007-12-04.crl\
@http://www.microsoft.com/pki/certs/MicProSecSerCA_2007-12-04.crt0
Uhttp://crl.microsoft.com/pki/crl/products/MicrosoftProductSecureCommunicationsPCA.crl
Uhttp://www.microsoft.com/pki/crl/products/MicrosoftProductSecureCommunicationsPCA.crl0j
Nhttp://www.microsoft.com/pki/certs/MicrosoftProductSecureCommunicationsPCA.crt0
?http://crl.microsoft.com/pki/crl/products/microsoftrootcert.crl0T
8http://www.microsoft.com/pki/certs/MicrosoftRootCert.crt0
```

## Summary

Volatility is a great tool for incidence response to analyze memory dump files to look for suspicious activity or analyze malware.