# Analysis and Investigation

Six-step investigative methodology by SANS

1. Identify rogue processes
2. Analyze process DLLs and handles
3. Review network artifacts
4. Look for evidence of code injection
5. Check for signs of rootkit
6. Dump suspicious processes and drivers

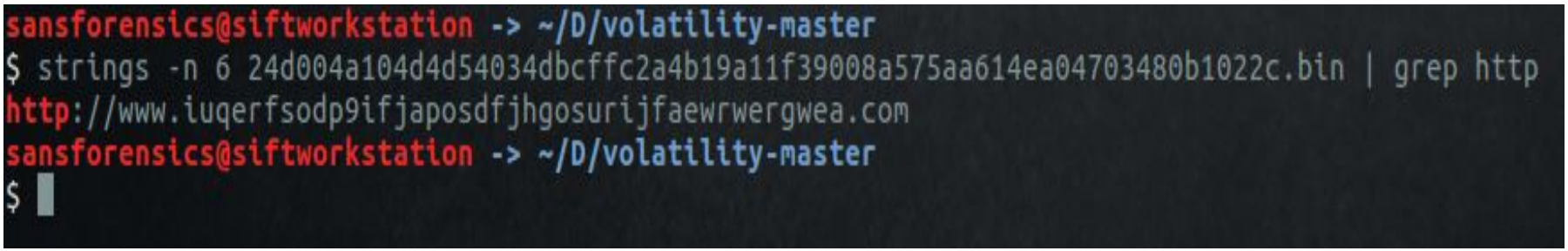
# Main goal is to find Indicators of Compromise

**Volatility , strings, bulk_extractor, Wireshark**

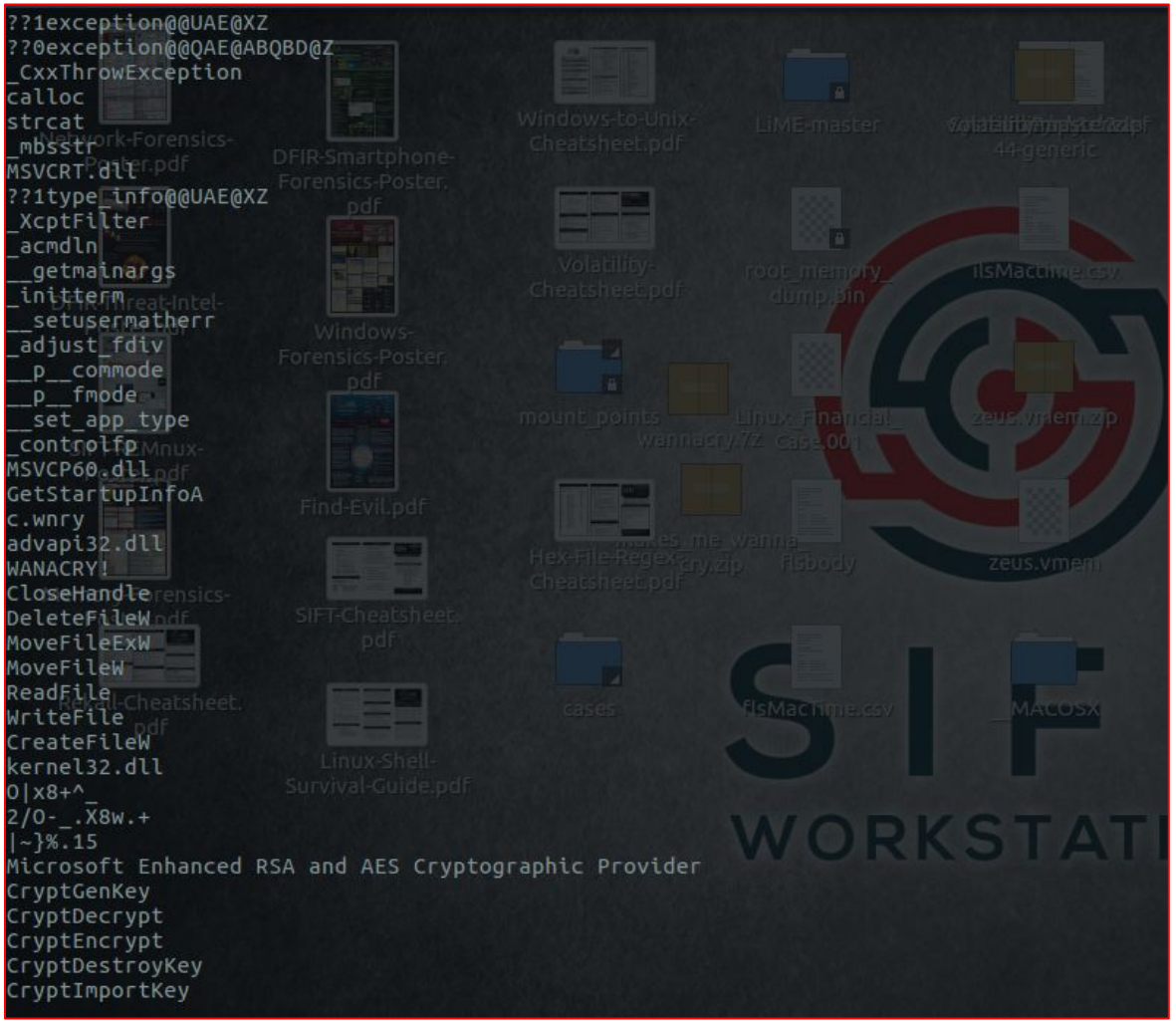
## Step 1 : Using ‘strings’

Strings -n 6 *filename.bin* | grep http

Strings -n 6 *filename.bin* | grep exe

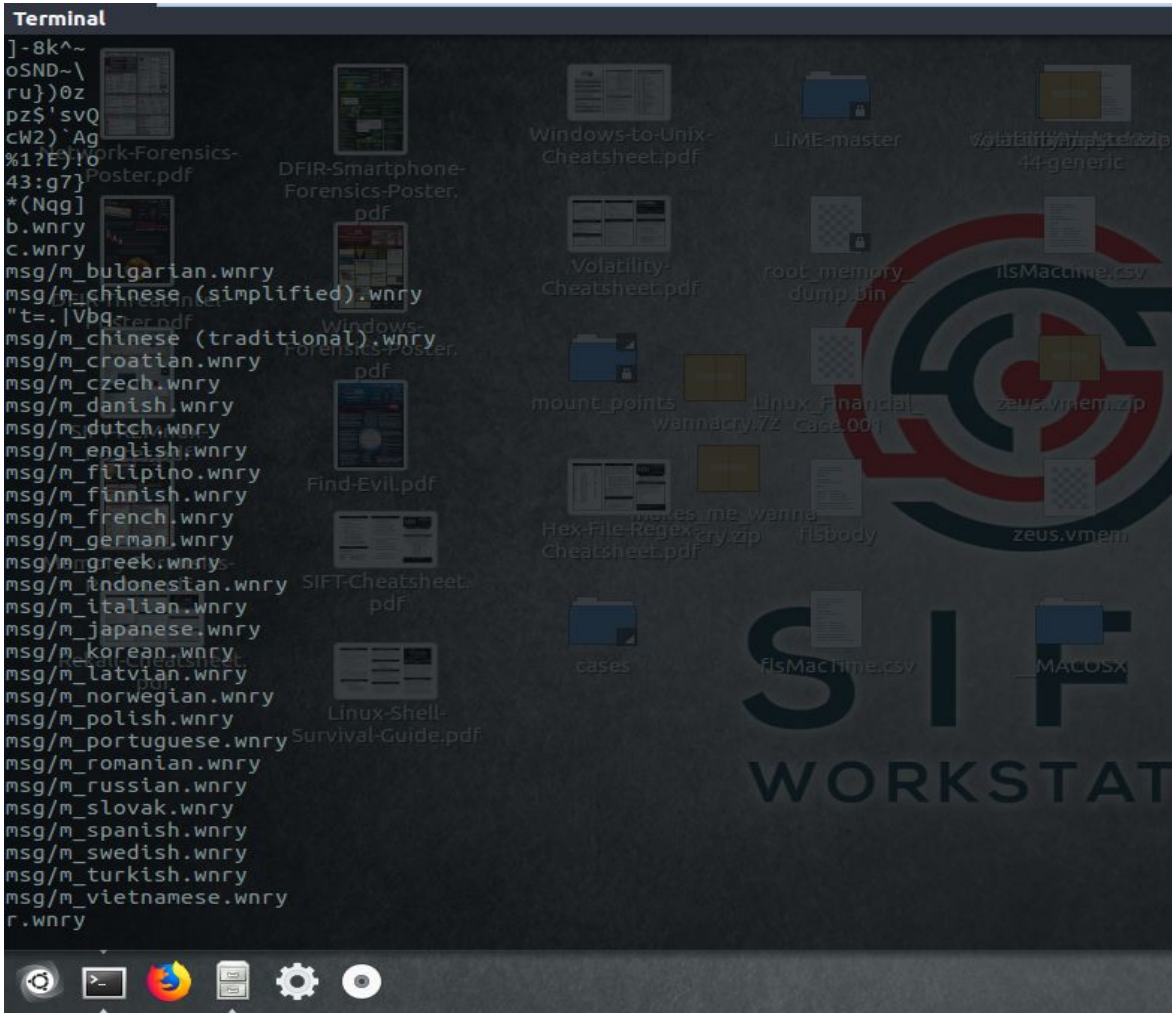

sansforensics@siftworkstation -> ~/D/volatility-master
$ strings -n 6 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c.bin | grep http
http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
sansforensics@siftworkstation -> ~/D/volatility-master
$

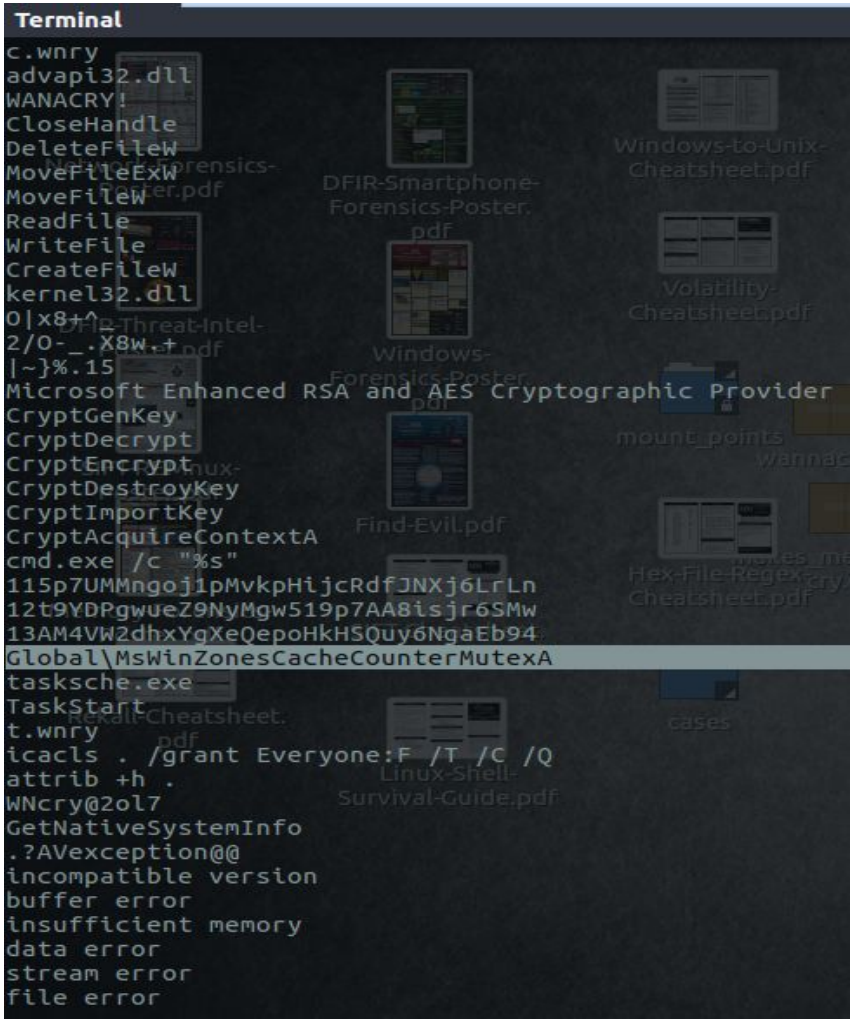

sansforensics@siftworkstation -> ~/D/volatility-master
$ strings -n 6 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c.bin | grep exe
mssecsvc.exe
mssecsvc.exe
tasksche.exe
cmd.exe /c "%s"
tasksche.exe
taskdl.exe
taskse.exed*
taskdl.exe
taskse.exe
sansforensics@siftworkstation -> ~/D/volatility-master
$




WANACRY !

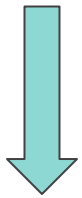
c.wnry


Terminal
]-8k^~
oSND~\
ru})0z
pz$'svQ
cW2)`Ag
%1?E)!o
43:g7}
*(Nqg]
b.wnry
c.wnry
msg/m_bulgarian.wnry
msg/m_chinese (simplified).wnry
"t=.|Vbq-
msg/m_chinese (traditional).wnry
msg/m_croatian.wnry
msg/m_czech.wnry
msg/m_danish.wnry
msg/m_dutch.wnry
msg/m_english.wnry
msg/m_filipino.wnry
msg/m_finnish.wnry
msg/m_french.wnry
msg/m_german.wnry
msg/m_greek.wnry
msg/m_indonesian.wnry
msg/m_italian.wnry
msg/m_japanese.wnry
msg/m_korean.wnry
msg/m_latvian.wnry
msg/m_norwegian.wnry
msg/m_polish.wnry
msg/m_portuguese.wnry
msg/m_romanian.wnry
msg/m_russian.wnry
msg/m_slovak.wnry
msg/m_spanish.wnry
msg/m_swedish.wnry
msg/m_turkish.wnry
msg/m_vietnamese.wnry
r.wnry
DFIR-Smartphone-Forensics-Poster.pdf
Windows-to-Unix-Cheatsheet.pdf
LiME-master
Volatility-Cheatsheet.pdf
root_memory_dump.bin
mount_points
Linux_Financial_Case.001
zeus.vmem.zip
zeus.vmem
Find-Evil.pdf
SIFT-Cheatsheet.pdf
Hex-File-Regex-Cheatsheet.pdf
fls_body
cases
fls_MacTime.csv
__MACOSX
Linux-Shell-Survival-Guide.pdf
SIF
WORKSTAT

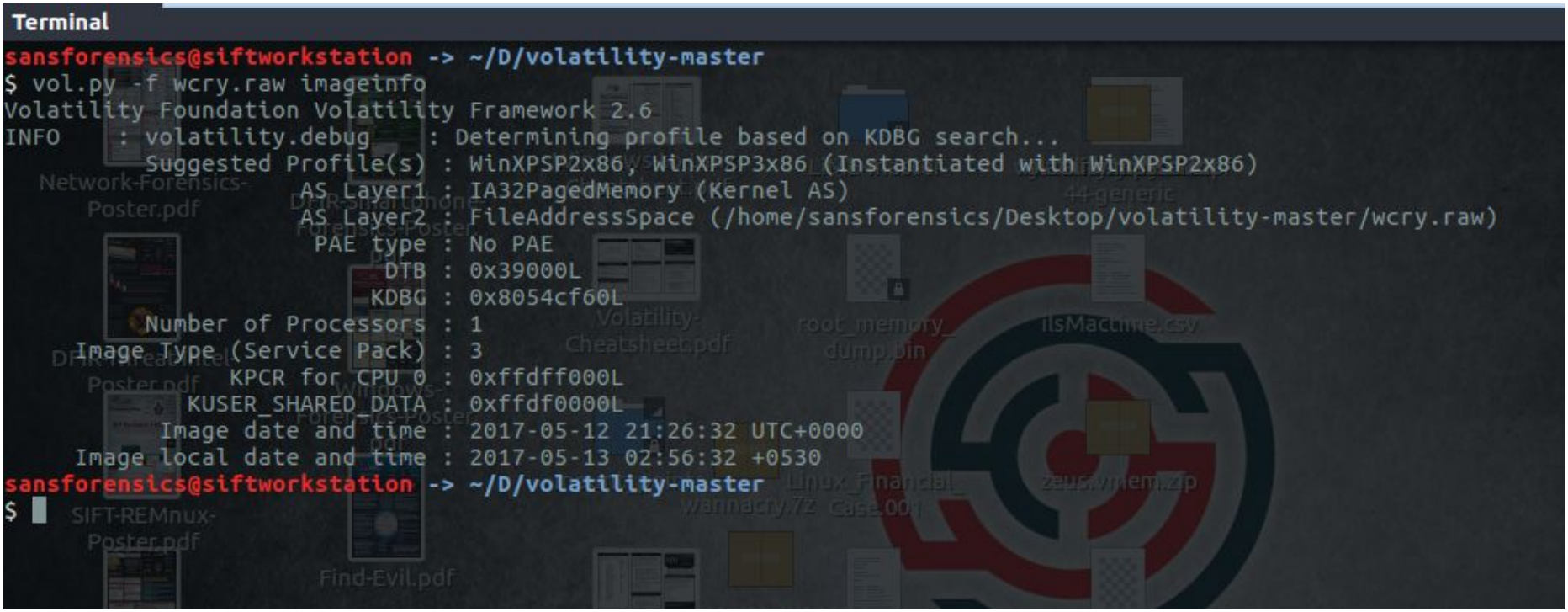

Terminal
c.wnry
advapi32.dll
WANACRY!
CloseHandle
DeleteFileW
MoveFileExW
MoveFileW
ReadFile
WriteFile
CreateFileW
kernel32.dll
O|x8+^
2/O-_.X8w.+
|~}%.15
Microsoft Enhanced RSA and AES Cryptographic Provider
CryptGenKey
CryptDecrypt
CryptEncrypt
CryptDestroyKey
CryptImportKey
CryptAcquireContextA
cmd.exe /c "%s"
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
Global\MsWinZonesCacheCounterMutexA
tasksche.exe
TaskStart
t.wnry
icacls . /grant Everyone:F /T /C /Q
attrib +h .
WNcry@2ol7
GetNativeSystemInfo
.?AVexception@@
incompatible version
buffer error
insufficient memory
data error
stream error
file error

# Using 'imageinfo' plugin

vol.py -f **wcry.raw** imageinfo



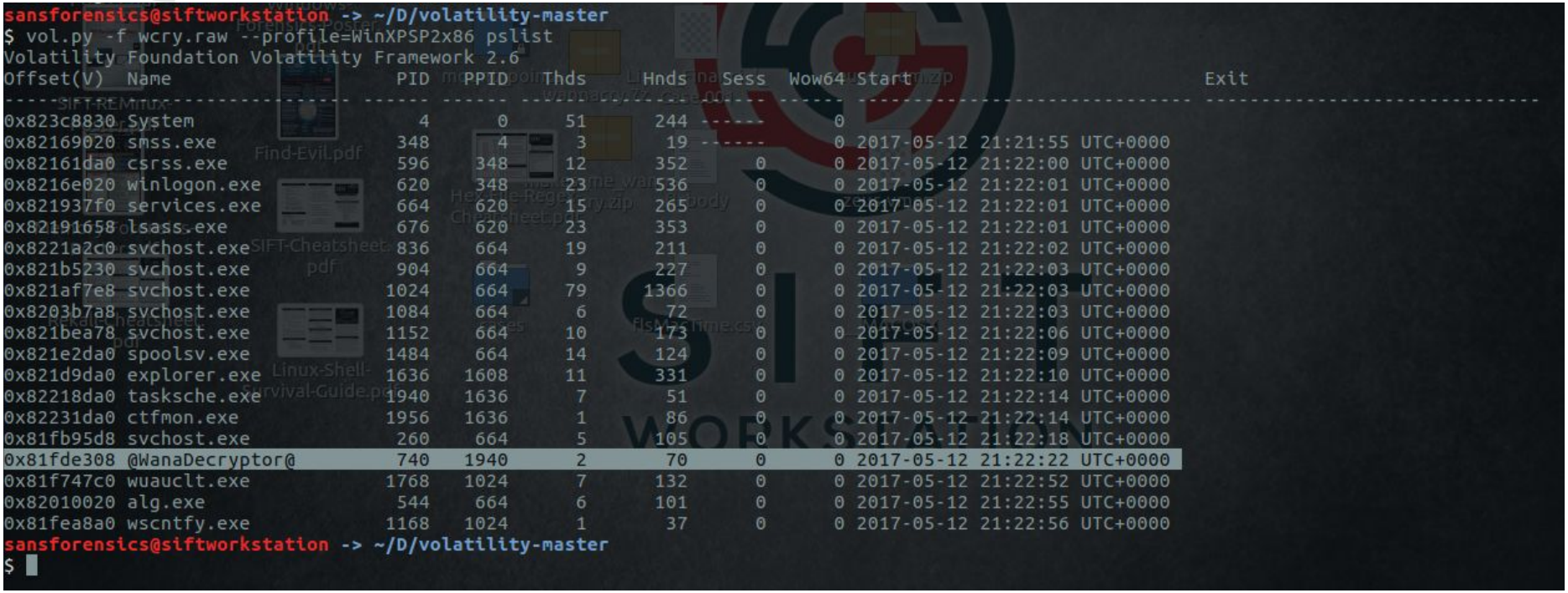
Memory dump

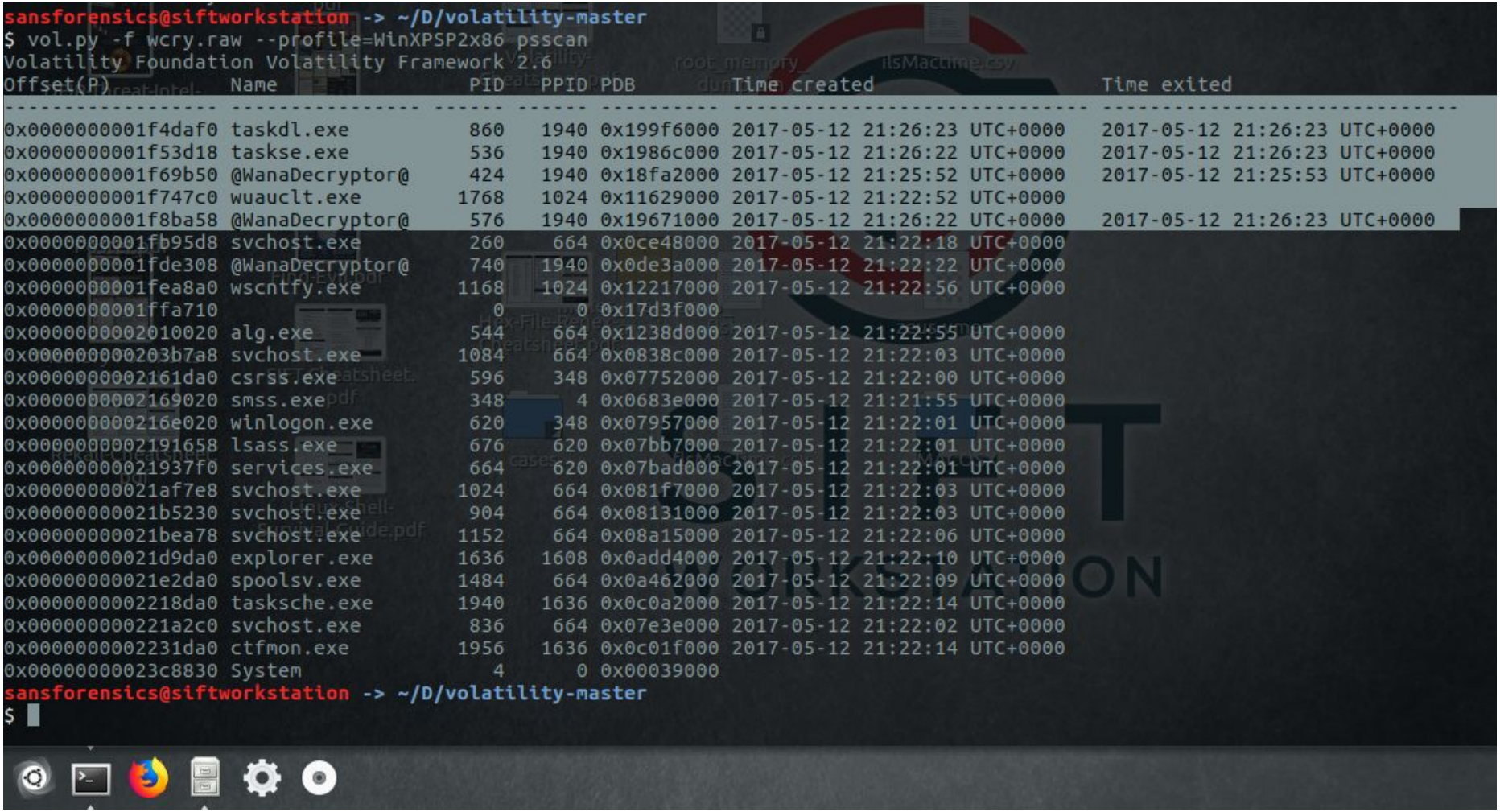

Terminal
sansforensics@siftworkstation -> ~/D/volatility-master
$ vol.py -f wcry.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
AS Layer1 : IA32PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (/home/sansforensics/Desktop/volatility-master/wcry.raw)
PAE type : No PAE
DTB : 0x39000L
KDBG : 0x8054cf60L
Number of Processors : 1
Image Type (Service Pack) : 3
KPCR for CPU 0 : 0xffdff000L
KUSER_SHARED_DATA : 0xffdf0000L
Image date and time : 2017-05-12 21:26:32 UTC+0000
Image local date and time : 2017-05-13 02:56:32 +0530
sansforensics@siftworkstation -> ~/D/volatility-master
$

# Using pslist and psscan plugins

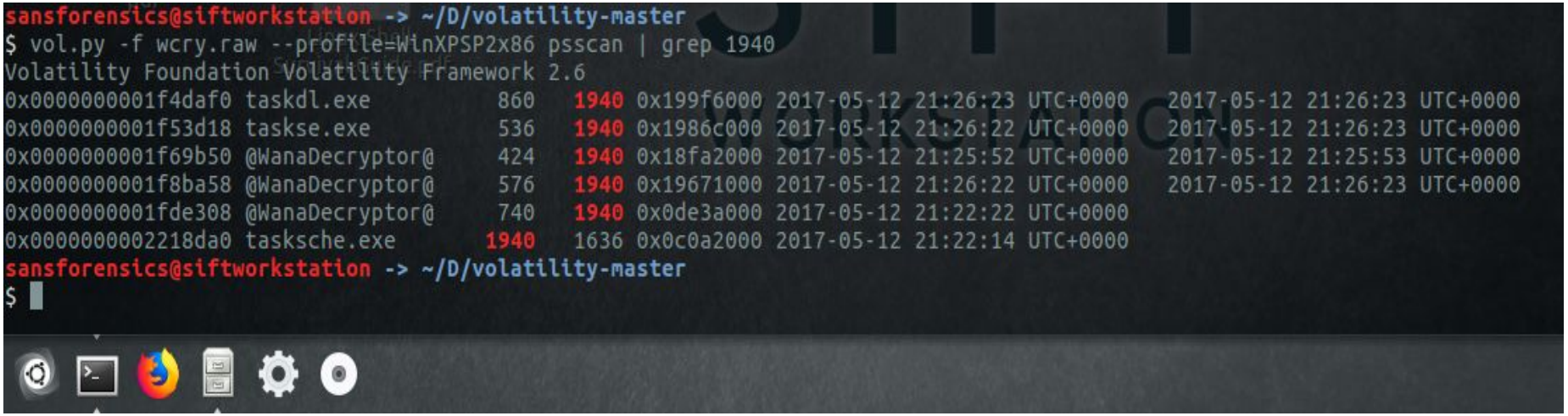
vol.py -f wcry.raw --profile=WinXPSP2x86 pslist

vol.py -f wcry.raw --profile=WinXPSP2x86 psscan


sansforensics@siftworkstation -> ~/D/volatility-master
$ vol.py -f wcry.raw --profile=WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V) Name PID PPID Thds Hnds Sess Wow64 Start Exit
0x823c8830 System 4 0 51 244 ------ 0
0x82169020 smss.exe 348 4 3 19 ------ 0 2017-05-12 21:21:55 UTC+0000
0x82161da0 csrss.exe 596 348 12 352 0 0 2017-05-12 21:22:00 UTC+0000
0x8216e020 winlogon.exe 620 348 23 536 0 0 2017-05-12 21:22:01 UTC+0000
0x821937f0 services.exe 664 620 15 265 0 0 2017-05-12 21:22:01 UTC+0000
0x82191658 lsass.exe 676 620 23 353 0 0 2017-05-12 21:22:01 UTC+0000
0x8221a2c0 svchost.exe 836 664 19 211 0 0 2017-05-12 21:22:02 UTC+0000
0x821b5230 svchost.exe 904 664 9 227 0 0 2017-05-12 21:22:03 UTC+0000
0x821af7e8 svchost.exe 1024 664 79 1366 0 0 2017-05-12 21:22:03 UTC+0000
0x8203b7a8 svchost.exe 1084 664 6 72 0 0 2017-05-12 21:22:03 UTC+0000
0x821bea78 svchost.exe 1152 664 10 173 0 0 2017-05-12 21:22:06 UTC+0000
0x821e2da0 spoolsv.exe 1484 664 14 124 0 0 2017-05-12 21:22:09 UTC+0000
0x821d9da0 explorer.exe 1636 1608 11 331 0 0 2017-05-12 21:22:10 UTC+0000
0x82218da0 tasksche.exe 1940 1636 7 51 0 0 2017-05-12 21:22:14 UTC+0000
0x82231da0 ctfmon.exe 1956 1636 1 86 0 0 2017-05-12 21:22:14 UTC+0000
0x81fb95d8 svchost.exe 260 664 5 105 0 0 2017-05-12 21:22:18 UTC+0000
0x81fde308 @WanaDecryptor@ 740 1940 2 70 0 0 2017-05-12 21:22:22 UTC+0000
0x81f747c0 wuauclt.exe 1768 1024 7 132 0 0 2017-05-12 21:22:52 UTC+0000
0x82010020 alg.exe 544 664 6 101 0 0 2017-05-12 21:22:55 UTC+0000
0x81fea8a0 wscntfy.exe 1168 1024 1 37 0 0 2017-05-12 21:22:56 UTC+0000
sansforensics@siftworkstation -> ~/D/volatility-master
$


sansforensics@siftworkstation -> ~/D/volatility-master
$ vol.py -f wcry.raw --profile=WinXPSP2x86 psscan
Volatility Foundation Volatility Framework 2.6
Offset(P) Name PID PPID PDB Time created Time exited
0x0000000001f4daf0 taskdl.exe 860 1940 0x199f6000 2017-05-12 21:26:23 UTC+0000 2017-05-12 21:26:23 UTC+0000
0x0000000001f53d18 taskse.exe 536 1940 0x1986c000 2017-05-12 21:26:22 UTC+0000 2017-05-12 21:26:23 UTC+0000
0x0000000001f69b50 @WanaDecryptor@ 424 1940 0x18fa2000 2017-05-12 21:25:52 UTC+0000 2017-05-12 21:25:53 UTC+0000
0x0000000001f747c0 wuauclt.exe 1768 1024 0x11629000 2017-05-12 21:22:52 UTC+0000
0x0000000001f8ba58 @WanaDecryptor@ 576 1940 0x19671000 2017-05-12 21:26:22 UTC+0000 2017-05-12 21:26:23 UTC+0000
0x0000000001fb95d8 svchost.exe 260 664 0x0ce48000 2017-05-12 21:22:18 UTC+0000
0x0000000001fde308 @WanaDecryptor@ 740 1940 0x0de3a000 2017-05-12 21:22:22 UTC+0000
0x0000000001fea8a0 wscntfy.exe 1168 1024 0x12217000 2017-05-12 21:22:56 UTC+0000
0x0000000001ffa710 0 0 0x17d3f000
0x0000000002010020 alg.exe 544 664 0x1238d000 2017-05-12 21:22:55 UTC+0000
0x0000000002030b7a8 svchost.exe 1084 664 0x0838c000 2017-05-12 21:22:03 UTC+0000
0x0000000002161da0 csrss.exe 596 348 0x07752000 2017-05-12 21:22:00 UTC+0000
0x0000000002169020 smss.exe 348 4 0x0683e000 2017-05-12 21:21:55 UTC+0000
0x000000002216e020 winlogon.exe 620 348 0x07957000 2017-05-12 21:22:01 UTC+0000
0x0000000002191658 lsass.exe 676 620 0x07bb7000 2017-05-12 21:22:01 UTC+0000
0x00000000021937f0 services.exe 664 620 0x07bad000 2017-05-12 21:22:01 UTC+0000
0x00000000021af7e8 svchost.exe 1024 664 0x081f7000 2017-05-12 21:22:03 UTC+0000
0x00000000021b5230 svchost.exe 904 664 0x08131000 2017-05-12 21:22:03 UTC+0000
0x00000000021bea78 svchost.exe 1152 664 0x08a15000 2017-05-12 21:22:06 UTC+0000
0x00000000021d9da0 explorer.exe 1636 1608 0x0add4000 2017-05-12 21:22:10 UTC+0000
0x00000000021e2da0 spoolsv.exe 1484 664 0x0a462000 2017-05-12 21:22:09 UTC+0000
0x0000000002218da0 tasksche.exe 1940 1636 0x0c0a2000 2017-05-12 21:22:14 UTC+0000
0x000000000221a2c0 svchost.exe 836 664 0x07e3e000 2017-05-12 21:22:02 UTC+0000
0x0000000002231da0 ctfmon.exe 1956 1636 0x0c01f000 2017-05-12 21:22:14 UTC+0000
0x00000000023c8830 System 4 0 0x00039000
sansforensics@siftworkstation -> ~/D/volatility-master
$

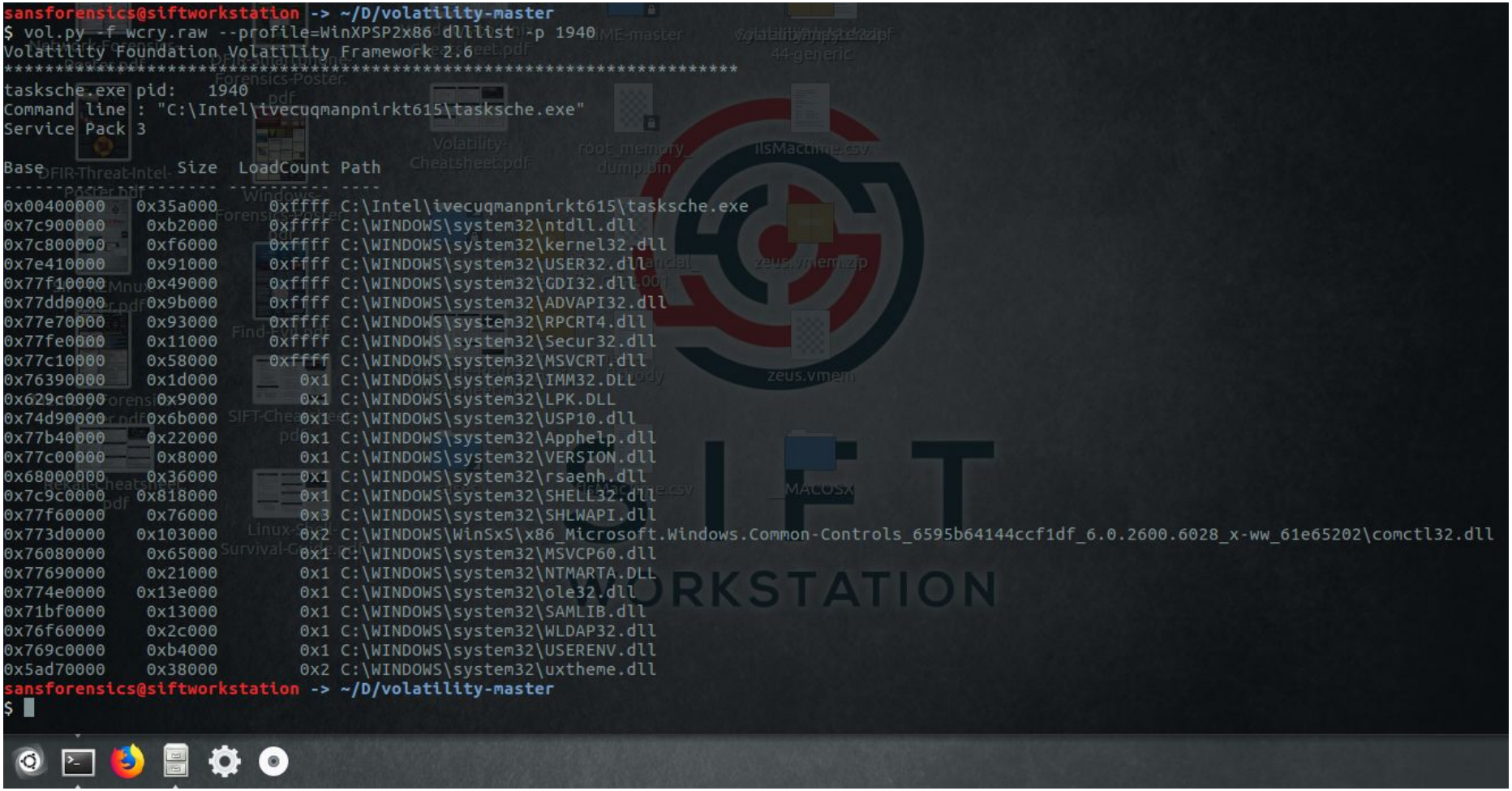
# Using grep for processes 1940 with psscan plugin



# Using dlllist plugin

```
vol.py -f wcry.raw --profile=WinXPSP2x86
dlllist -p 1940

vol.py -f wcry.raw --profile=WinXPSP2x86
dlllist -p 740
```


sansforensics@siftworkstation -> ~/D/volatility-master
$ vol.py -f wcry.raw --profile=WinXPSP2x86 dllist -p 1940
Volatility Foundation Volatility Framework 2.6
**********
tasksche.exe pid: 1940
Command line : "C:\Intel\ivecuqmanpnirkt615\tasksche.exe"
Service Pack 3
Base Size LoadCount Path
0x00400000 0x35a000 0xffff C:\Intel\ivecuqmanpnirkt615\tasksche.exe
0x7c900000 0xb2000 0xffff C:\WINDOWS\system32\ntdll.dll
0x7c800000 0xf6000 0xffff C:\WINDOWS\system32\kernel32.dll
0x7e410000 0x91000 0xffff C:\WINDOWS\system32\USER32.dll
0x77f10000 0x49000 0xffff C:\WINDOWS\system32\GDI32.dll
0x77dd0000 0x9b000 0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000 0x93000 0xffff C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000 0x11000 0xffff C:\WINDOWS\system32\Secur32.dll
0x77c10000 0x58000 0xffff C:\WINDOWS\system32\MSVCRT.dll
0x76390000 0x1d000 0x1 C:\WINDOWS\system32\IMM32.DLL
0x629c0000 0x9000 0x1 C:\WINDOWS\system32\LPK.DLL
0x74d90000 0x6b000 0x1 C:\WINDOWS\system32\USP10.dll
0x77b40000 0x22000 0x1 C:\WINDOWS\system32\Apphelp.dll
0x77c00000 0x8000 0x1 C:\WINDOWS\system32\VERSION.dll
0x68000000 0x36000 0x1 C:\WINDOWS\system32\rsaenh.dll
0x7c9c0000 0x818000 0x1 C:\WINDOWS\system32\SHELL32.dll
0x77f60000 0x76000 0x3 C:\WINDOWS\system32\SHLWAPI.dll
0x773d0000 0x103000 0x2 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.6028_x-ww_61e65202\comctl32.dll
0x76080000 0x65000 0x1 C:\WINDOWS\system32\MSVCP60.dll
0x77690000 0x21000 0x1 C:\WINDOWS\system32\NTMARTA.DLL
0x774e0000 0x13e000 0x1 C:\WINDOWS\system32\ole32.dll
0x71bf0000 0x13000 0x1 C:\WINDOWS\system32\SAMLIB.dll
0x76f60000 0x2c000 0x1 C:\WINDOWS\system32\WLDAP32.dll
0x769c0000 0xb4000 0x1 C:\WINDOWS\system32\USERENV.dll
0x5ad70000 0x38000 0x2 C:\WINDOWS\system32\uxtheme.dll
sansforensics@siftworkstation -> ~/D/volatility-master
$


sansforensics@siftworkstation -> ~/D/volatility-master
$ vol.py -f wcry.raw --profile=WinXPSP2x86 dlllist -p 740
Volatility Foundation Volatility Framework 2.6
**********
@WanaDecryptor@ pid:    740
Command line : @WanaDecryptor@.exe
Service Pack 3
Base  Size  LoadCount Path
0x00400000 0x3d000 0xffff C:\Intel\ivecuqmanpnirkt615\@WanaDecryptor@.exe
0x7c900000 0xb2000 0xffff C:\WINDOWS\system32\ntdll.dll
0x7c800000 0xf6000 0xffff C:\WINDOWS\system32\kernel32.dll
0x73dd0000 0xf2000 0xffff C:\WINDOWS\system32\MFC42.DLL
0x77c10000 0x58000 0xffff C:\WINDOWS\system32\msvcrt.dll
0x77f10000 0x49000 0xffff C:\WINDOWS\system32\GDI32.dll
0x7e410000 0x91000 0xffff C:\WINDOWS\system32\USER32.dll
0x77dd0000 0x9b000 0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000 0x93000 0xffff C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000 0x11000 0xffff C:\WINDOWS\system32\Secur32.dll
0x7c9c0000 0x818000 0xffff C:\WINDOWS\system32\SHELL32.dll
0x77f60000 0x76000 0xffff C:\WINDOWS\system32\SHLWAPI.dll
0x773d0000 0x103000 0xffff C:\WINDOWS\WinSxS\X86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.6028_x-ww_61e65202\COMCTL32.dll
0x77120000 0x8b000 0xffff C:\WINDOWS\system32\OLEAUT32.dll
0x774e0000 0x13e000 0xffff C:\WINDOWS\system32\ole32.dll
0x78130000 0x134000 0xffff C:\WINDOWS\system32\urlmon.dll
0x3dfd0000 0x1ec000 0xffff C:\WINDOWS\system32\iertutil.dll
0x76080000 0x65000 0xffff C:\WINDOWS\system32\MSVCP60.dll
0x71ab0000 0x17000 0xffff C:\WINDOWS\system32\WS2_32.dll
0x71aa0000 0x8000 0xffff C:\WINDOWS\system32\WS2HELP.dll
0x3d930000 0xe7000 0xffff C:\WINDOWS\system32\WININET.dll
0x00340000 0x9000 0xffff C:\WINDOWS\system32\Normaliz.dll
0x76390000 0x1d000 0x4 C:\WINDOWS\system32\IMM32.DLL
0x629c0000 0x9000 0x1 C:\WINDOWS\system32\LPK.DLL
0x74d90000 0x6b000 0x2 C:\WINDOWS\system32\USP10.dll
0x732e0000 0x5000 0x1 C:\WINDOWS\system32\RICHED32.DLL

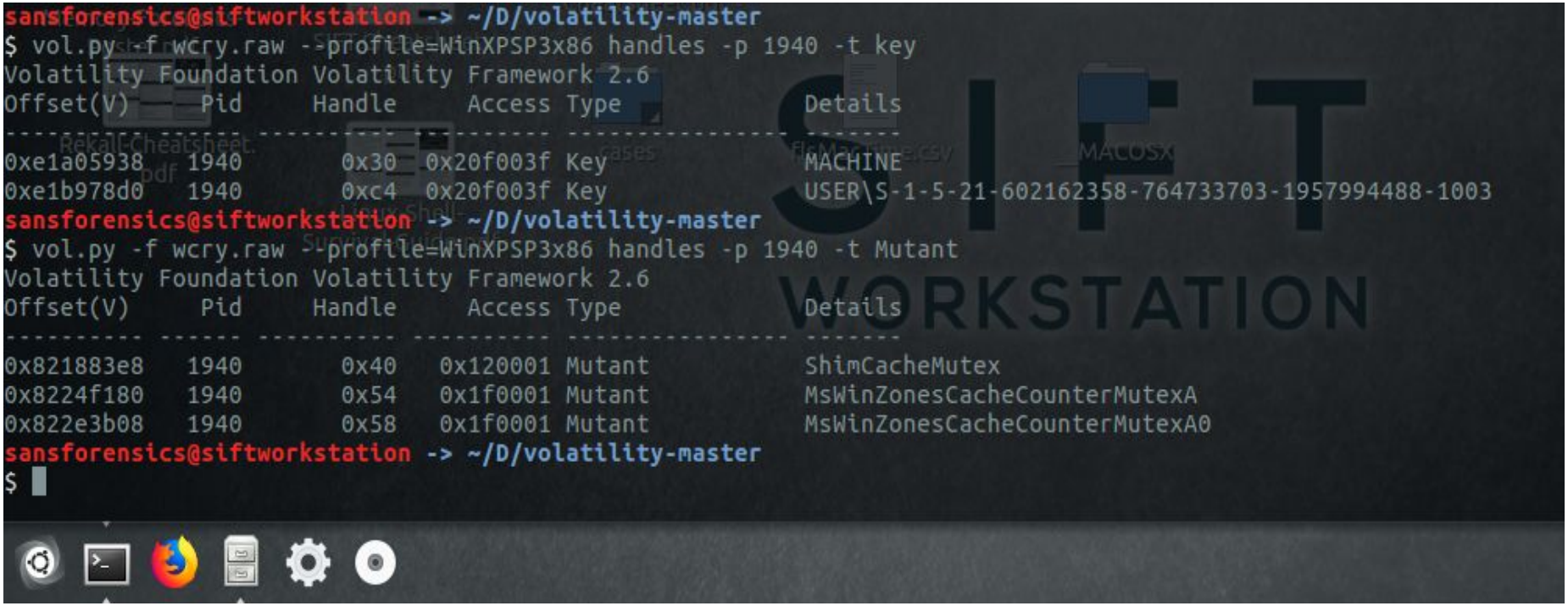
# Using ‘handles’ plugin

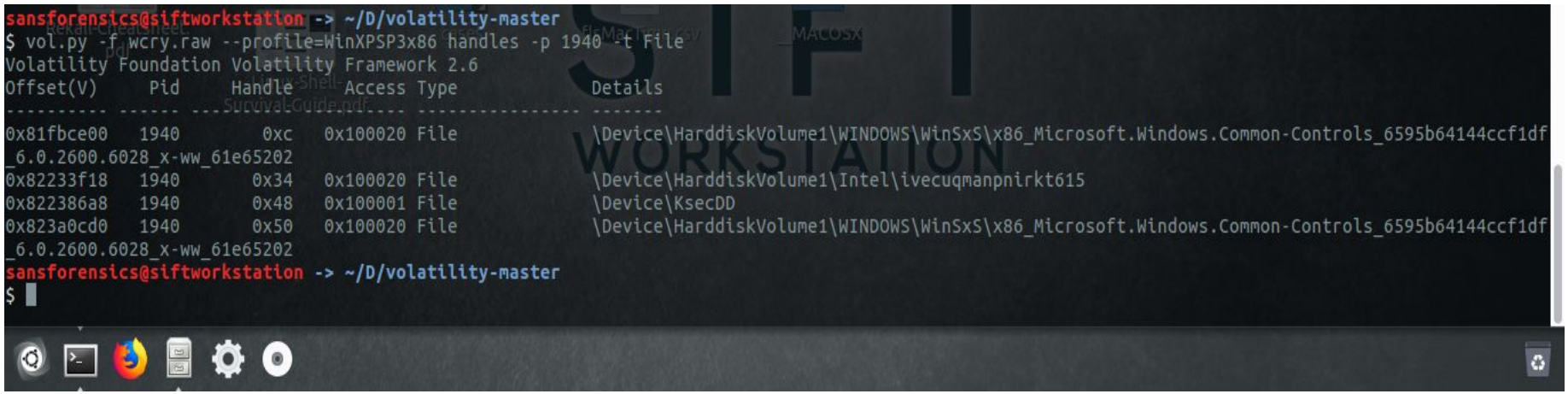
vol.py -f wcry.raw --profile=WinXPSP3x86 handles -p 1940 -t key

vol.py -f wcry.raw --profile=WinXPSP3x86 handles -p 1940 -t Mutant

vol.py -f wcry.raw --profile=WinXPSP3x86 handles -p 1940 -t File

vol.py -f wcry.raw --profile=WinXPSP3x86 handles -p 740 -t key


sansforensics@siftworkstation -> ~/D/volatility-master
$ vol.py -f wcry.raw --profile=WinXPSP3x86 handles -p 1940 -t key
Volatility Foundation Volatility Framework 2.6
Offset(V) Pid Handle Access Type Details
0xe1a05938 1940 0x30 0x20f003f Key MACHINE
0xe1b978d0 1940 0xc4 0x20f003f Key USER\S-1-5-21-602162358-764733703-1957994488-1003
sansforensics@siftworkstation -> ~/D/volatility-master
$ vol.py -f wcry.raw --profile=WinXPSP3x86 handles -p 1940 -t Mutant
Volatility Foundation Volatility Framework 2.6
Offset(V) Pid Handle Access Type Details
0x821883e8 1940 0x40 0x120001 Mutant ShimCacheMutex
0x8224f180 1940 0x54 0x1f0001 Mutant MsWinZonesCacheCounterMutexA
0x822e3b08 1940 0x58 0x1f0001 Mutant MsWinZonesCacheCounterMutexA0
sansforensics@siftworkstation -> ~/D/volatility-master
$

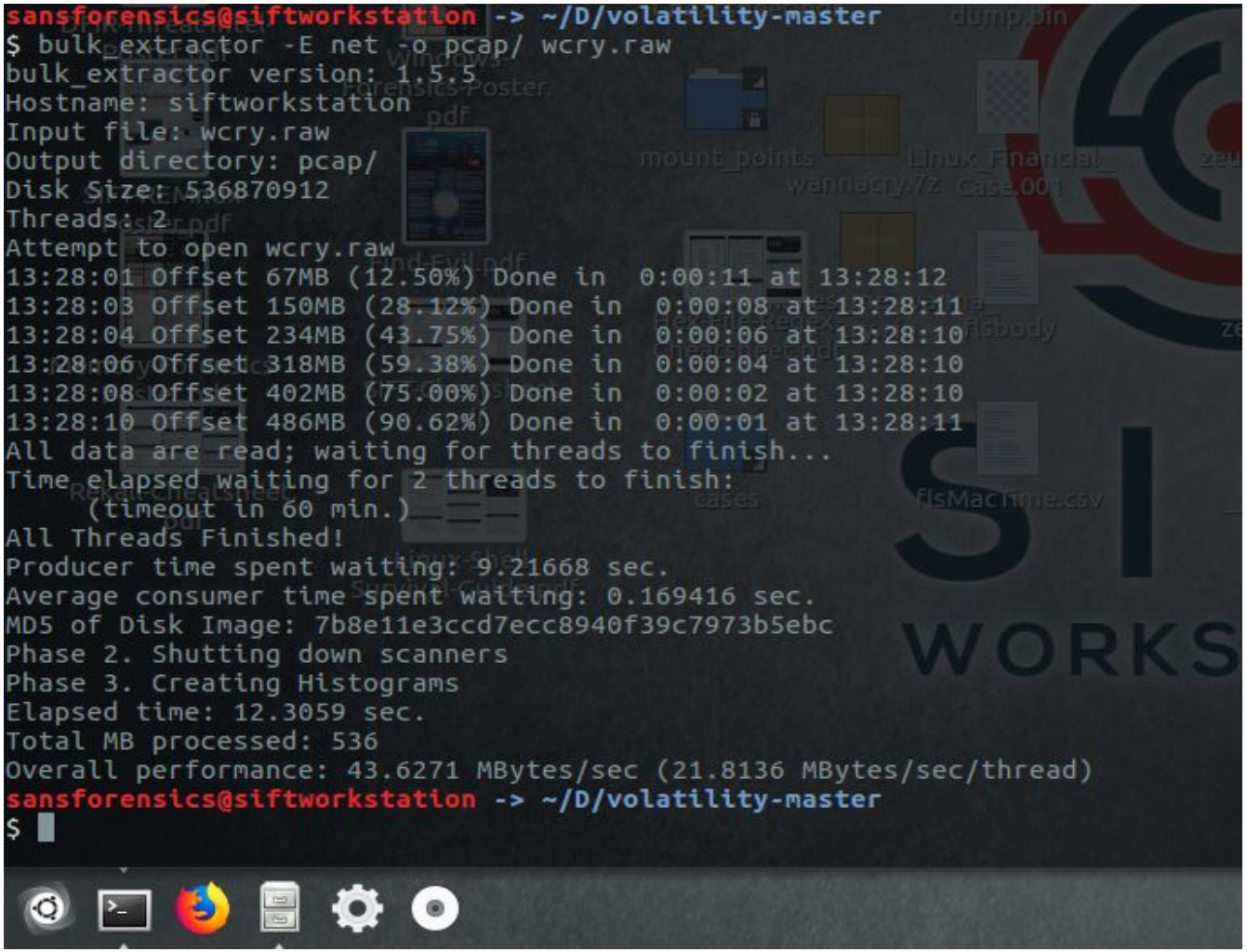

sansforensics@siftworkstation -> ~/D/volatility-master
$ vol.py -f wcry.raw --profile=WinXPSP3x86 handles -p 1940 -t File
Volatility Foundation Volatility Framework 2.6
Offset(V) Pid Handle Access Type Details
0x81fbce00 1940 0xc 0x100020 File \Device\HarddiskVolume1\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.6028_x-ww_61e65202
0x82233f18 1940 0x34 0x100020 File \Device\HarddiskVolume1\Intel\ivecuqmanpnirkt615
0x822386a8 1940 0x48 0x100001 File \Device\KsecDD
0x823a0cd0 1940 0x50 0x100020 File \Device\HarddiskVolume1\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.6028_x-ww_61e65202
sansforensics@siftworkstation -> ~/D/volatility-master
$

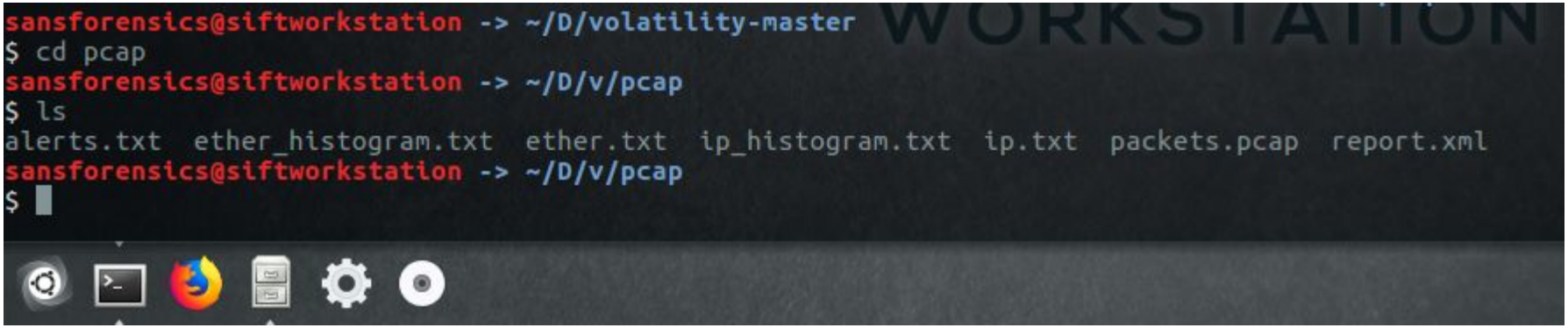
## Using ‘bulk_extractor’ , Wireshark

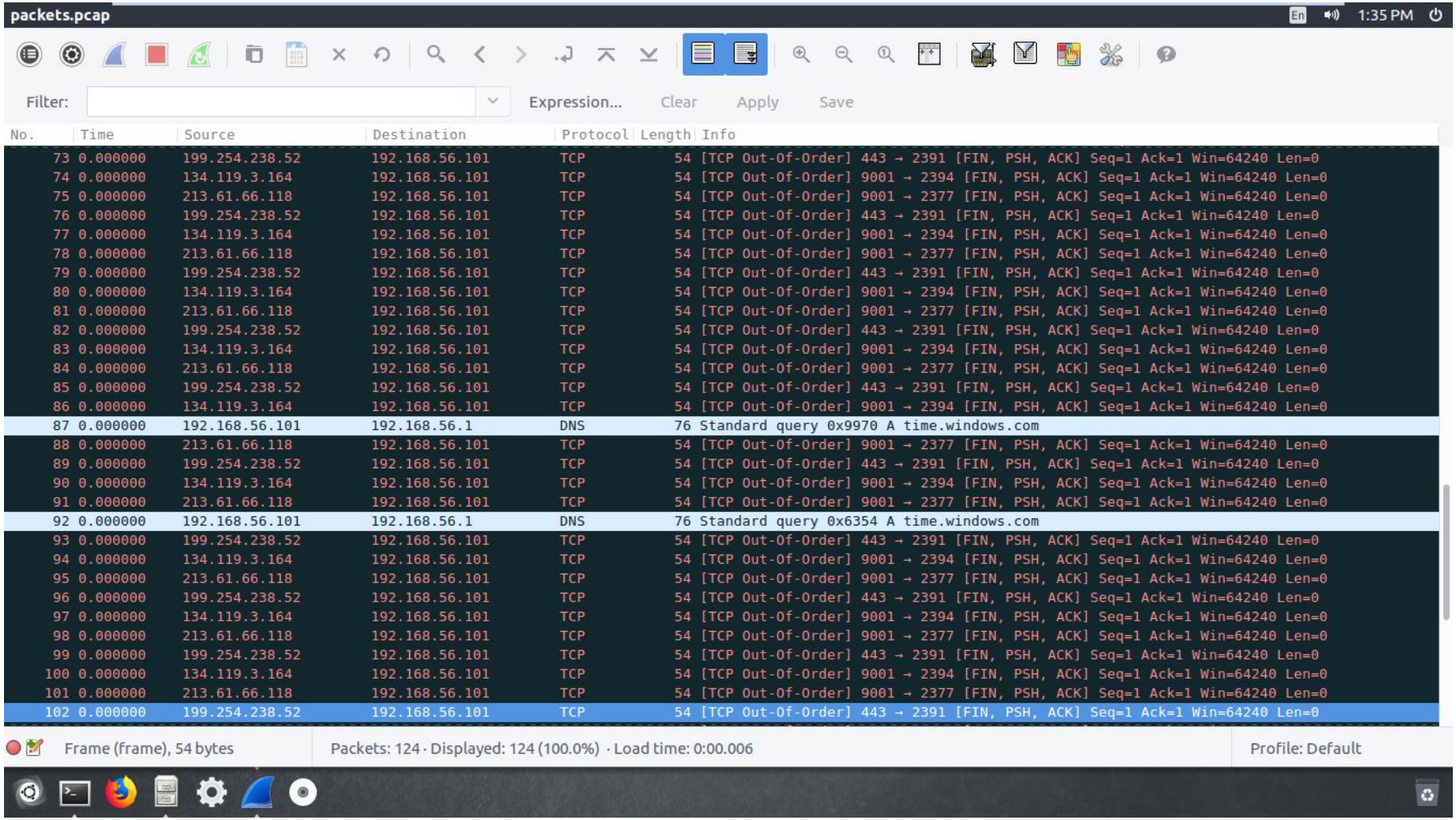
Data carving tool

extract network connections from memory

**bulk_extractor -E net -o pcap/ wcry.raw**

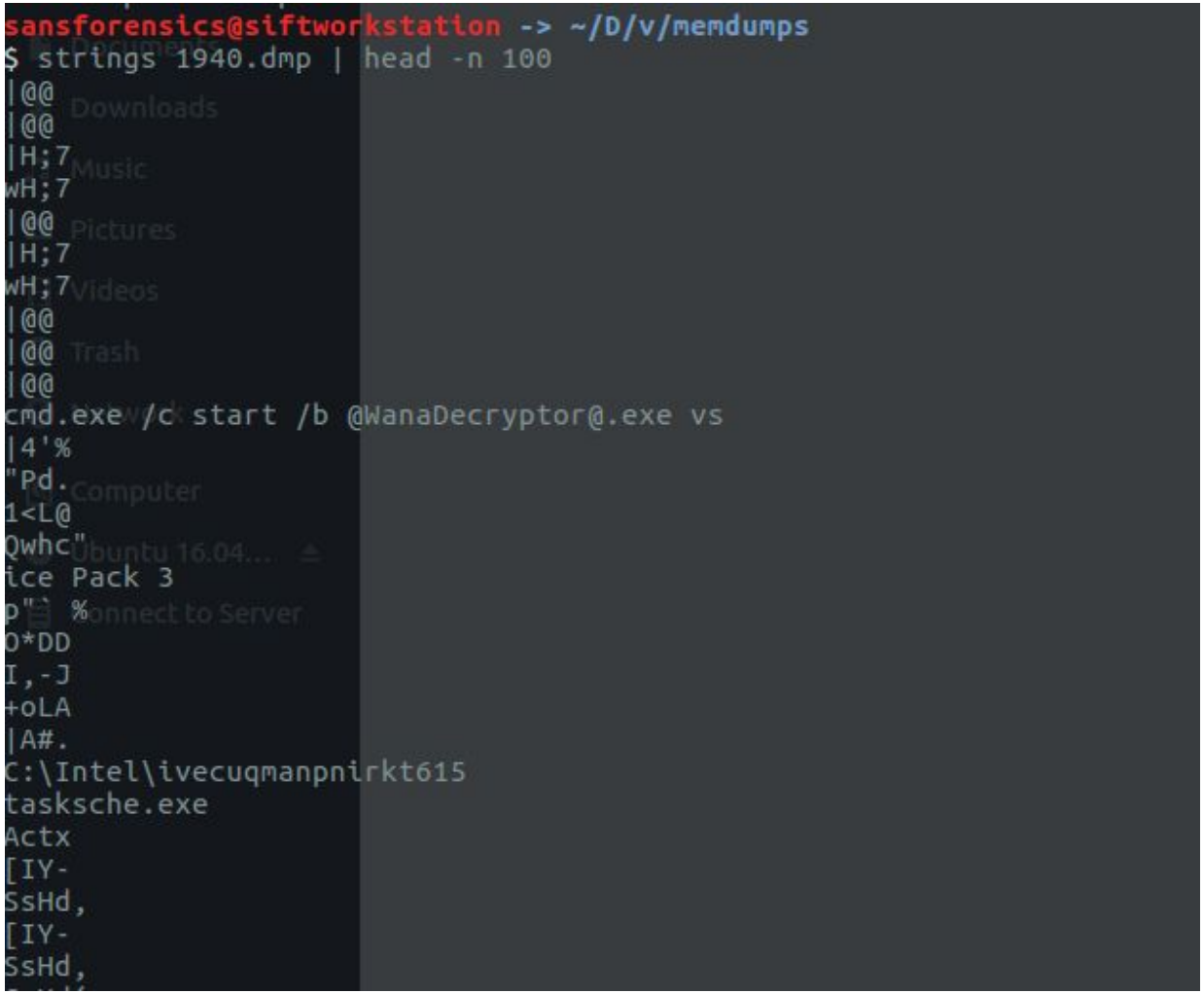

sansforensics@siftworkstation -> ~/D/volatility-master
$ bulk_extractor -E net -o pcap/ wcry.raw
bulk_extractor version: 1.5.5
Hostname: siftworkstation
Input file: wcry.raw
Output directory: pcap/
Disk Size: 536870912
Threads: 2
Attempt to open wcry.raw
13:28:01 Offset 67MB (12.50%) Done in 0:00:11 at 13:28:12
13:28:03 Offset 150MB (28.12%) Done in 0:00:08 at 13:28:11
13:28:04 Offset 234MB (43.75%) Done in 0:00:06 at 13:28:10
13:28:06 Offset 318MB (59.38%) Done in 0:00:04 at 13:28:10
13:28:08 Offset 402MB (75.00%) Done in 0:00:02 at 13:28:10
13:28:10 Offset 486MB (90.62%) Done in 0:00:01 at 13:28:11
All data are read; waiting for threads to finish...
Time elapsed waiting for 2 threads to finish:
(timeout in 60 min.)
All Threads Finished!
Producer time spent waiting: 9.21668 sec.
Average consumer time spent waiting: 0.169416 sec.
MD5 of Disk Image: 7b8e11e3ccd7ecc8940f39c7973b5ebc
Phase 2. Shutting down scanners
Phase 3. Creating Histograms
Elapsed time: 12.3059 sec.
Total MB processed: 536
Overall performance: 43.6271 MBytes/sec (21.8136 MBytes/sec/thread)
sansforensics@siftworkstation -> ~/D/volatility-master
$

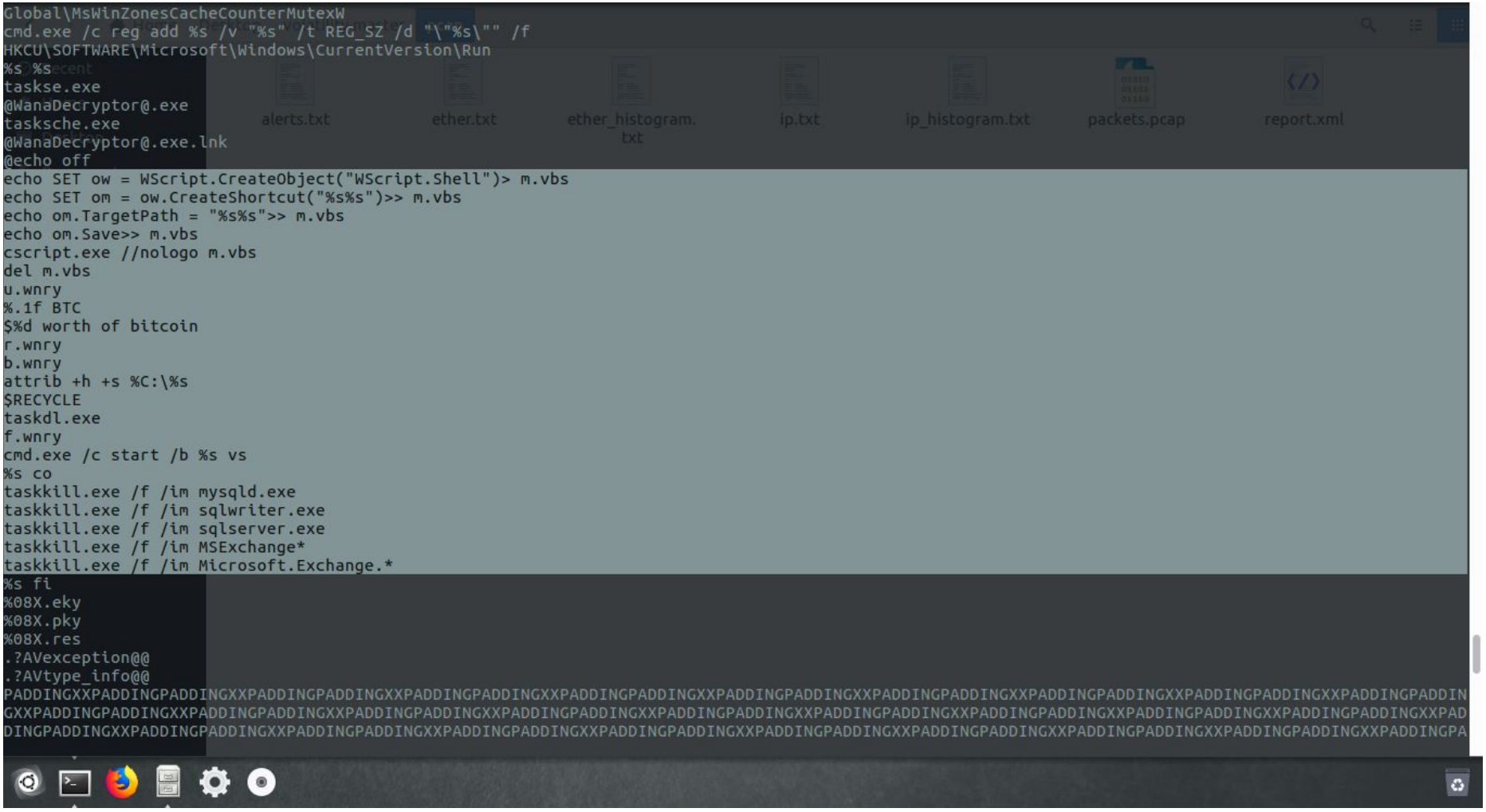

sansforensics@siftworkstation -> ~/D/volatility-master
$ cd pcap
sansforensics@siftworkstation -> ~/D/v/pcap
$ ls
alerts.txt  ether_histogram.txt  ether.txt  ip_histogram.txt  ip.txt  packets.pcap  report.xml
sansforensics@siftworkstation -> ~/D/v/pcap
$

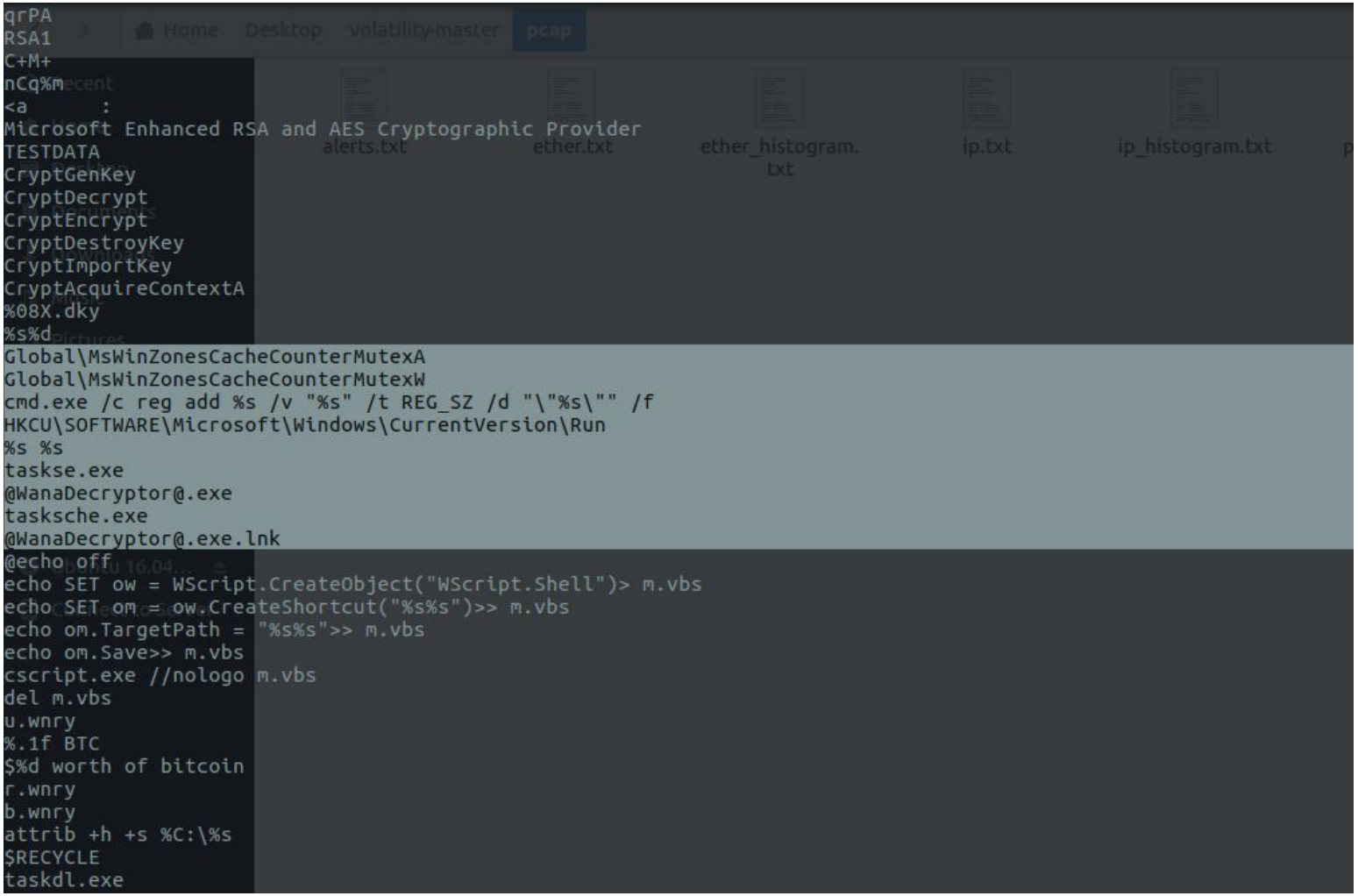

packets.pcap
En
1:35 PM
Filter:
Expression...
Clear
Apply
Save
No. Time Source Destination Protocol Length Info
73 0.000000 199.254.238.52 192.168.56.101 TCP 54 [TCP Out-Of-Order] 443 → 2391 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
74 0.000000 134.119.3.164 192.168.56.101 TCP 54 [TCP Out-Of-Order] 9001 → 2394 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
75 0.000000 213.61.66.118 192.168.56.101 TCP 54 [TCP Out-Of-Order] 9001 → 2377 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
76 0.000000 199.254.238.52 192.168.56.101 TCP 54 [TCP Out-Of-Order] 443 → 2391 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
77 0.000000 134.119.3.164 192.168.56.101 TCP 54 [TCP Out-Of-Order] 9001 → 2394 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
78 0.000000 213.61.66.118 192.168.56.101 TCP 54 [TCP Out-Of-Order] 9001 → 2377 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
79 0.000000 199.254.238.52 192.168.56.101 TCP 54 [TCP Out-Of-Order] 443 → 2391 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
80 0.000000 134.119.3.164 192.168.56.101 TCP 54 [TCP Out-Of-Order] 9001 → 2394 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
81 0.000000 213.61.66.118 192.168.56.101 TCP 54 [TCP Out-Of-Order] 9001 → 2377 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
82 0.000000 199.254.238.52 192.168.56.101 TCP 54 [TCP Out-Of-Order] 443 → 2391 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
83 0.000000 134.119.3.164 192.168.56.101 TCP 54 [TCP Out-Of-Order] 9001 → 2394 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
84 0.000000 213.61.66.118 192.168.56.101 TCP 54 [TCP Out-Of-Order] 9001 → 2377 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
85 0.000000 199.254.238.52 192.168.56.101 TCP 54 [TCP Out-Of-Order] 443 → 2391 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
86 0.000000 134.119.3.164 192.168.56.101 TCP 54 [TCP Out-Of-Order] 9001 → 2394 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
87 0.000000 192.168.56.101 192.168.56.1 DNS 76 Standard query 0x9970 A time.windows.com
88 0.000000 213.61.66.118 192.168.56.101 TCP 54 [TCP Out-Of-Order] 9001 → 2377 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
89 0.000000 199.254.238.52 192.168.56.101 TCP 54 [TCP Out-Of-Order] 443 → 2391 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
90 0.000000 134.119.3.164 192.168.56.101 TCP 54 [TCP Out-Of-Order] 9001 → 2394 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
91 0.000000 213.61.66.118 192.168.56.101 TCP 54 [TCP Out-Of-Order] 9001 → 2377 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
92 0.000000 192.168.56.101 192.168.56.1 DNS 76 Standard query 0x6354 A time.windows.com
93 0.000000 199.254.238.52 192.168.56.101 TCP 54 [TCP Out-Of-Order] 443 → 2391 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
94 0.000000 134.119.3.164 192.168.56.101 TCP 54 [TCP Out-Of-Order] 9001 → 2394 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
95 0.000000 213.61.66.118 192.168.56.101 TCP 54 [TCP Out-Of-Order] 9001 → 2377 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
96 0.000000 199.254.238.52 192.168.56.101 TCP 54 [TCP Out-Of-Order] 443 → 2391 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
97 0.000000 134.119.3.164 192.168.56.101 TCP 54 [TCP Out-Of-Order] 9001 → 2394 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
98 0.000000 213.61.66.118 192.168.56.101 TCP 54 [TCP Out-Of-Order] 9001 → 2377 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
99 0.000000 199.254.238.52 192.168.56.101 TCP 54 [TCP Out-Of-Order] 443 → 2391 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
100 0.000000 134.119.3.164 192.168.56.101 TCP 54 [TCP Out-Of-Order] 9001 → 2394 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
101 0.000000 213.61.66.118 192.168.56.101 TCP 54 [TCP Out-Of-Order] 9001 → 2377 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
102 0.000000 199.254.238.52 192.168.56.101 TCP 54 [TCP Out-Of-Order] 443 → 2391 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
Frame (frame), 54 bytes
Packets: 124 · Displayed: 124 (100.0%) · Load time: 0:00.006
Profile: Default

## *memdump* plugin

vol.py -f wcry.raw --profile=WinXPSP3x86 memdump -p1940,740 -D memdumps/


sansforensics@siftworkstation -> ~/D/v/memdumps
$ strings 1940.dmp | head -n 100
|@@
|@@
|H;7
wH;7
|@@
|H;7
wH;7
|@@
|@@
|@@
cmd.exe /c start /b @WanaDecryptor@.exe vs
|4'%
"Pd.
1<L@
Qwhc"
ice Pack 3
O*DD
I,-J
+oLA
|A#.
C:\Intel\ivecuqmanpnirkt615
tasksche.exe
Actx
[IY-
SsHd,
[IY-
SsHd,


Global\MsWinZonesCacheCounterMutexW
cmd.exe /c reg add %s /v "%s" /t REG_SZ /d "\"%s\"" /f
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
%s %s
taskse.exe
@WanaDecryptor@.exe
tasksche.exe
@WanaDecryptor@.exe.lnk
@echo off
echo SET ow = WScript.CreateObject("WScript.Shell")> m.vbs
echo SET om = ow.CreateShortcut("%s%s")>> m.vbs
echo om.TargetPath = "%s%s">> m.vbs
echo om.Save>> m.vbs
cscript.exe //nologo m.vbs
del m.vbs
u.wnry
%.1f BTC
$%d worth of bitcoin
r.wnry
b.wnry
attrib +h +s %C:\%s
$RECYCLE
taskdl.exe
f.wnry
cmd.exe /c start /b %s vs
%s co
taskkill.exe /f /im mysqld.exe
taskkill.exe /f /im sqlwriter.exe
taskkill.exe /f /im sqlserver.exe
taskkill.exe /f /im MSExchange*
taskkill.exe /f /im Microsoft.Exchange.*
%s fi
%08X.eky
%08X.pky
%08X.res
.?AVexception@@
.?AVtype_info@@
PADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDIN
GXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPAD
DINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPA
alerts.txt
ether.txt
ether_histogram.txt
ip.txt
ip_histogram.txt
packets.pcap
report.xml


qrPA
RSA1
C+M+
nCq%m
<a :
Microsoft Enhanced RSA and AES Cryptographic Provider
TESTDATA
CryptGenKey
CryptDecrypt
CryptEncrypt
CryptDestroyKey
CryptImportKey
CryptAcquireContextA
%08X.dky
%s%d
Global\MsWinZonesCacheCounterMutexA
Global\MsWinZonesCacheCounterMutexW
cmd.exe /c reg add %s /v "%s" /t REG_SZ /d "\"%s\"" /f
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
%s %s
taskse.exe
@WanaDecryptor@.exe
tasksche.exe
@WanaDecryptor@.exe.lnk
@echo off
echo SET ow = WScript.CreateObject("WScript.Shell")> m.vbs
echo SET om = ow.CreateShortcut("%s%s")>> m.vbs
echo om.TargetPath = "%s%s">> m.vbs
echo om.Save>> m.vbs
cscript.exe //nologo m.vbs
del m.vbs
u.wnry
%.1f BTC
$%d worth of bitcoin
r.wnry
b.wnry
attrib +h +s %C:\%s
$RECYCLE
taskdl.exe
Home
Desktop
volatility-master
pcap
alerts.txt
ether.txt
ether_histogram.txt
ip.txt
ip_histogram.txt


sansforensics@siftworkstation -> ~/D/v/memdumps
$ strings 740.dmp | head -n 100
ZhB5
SwrD
SwrD
B~xz
SwrD
SwrD
B~xz
Pvtt
<:v `:v
<:v `:v
<:v5
q\ut
C]ue
A~hPc

# Command and Control Onion Addresses