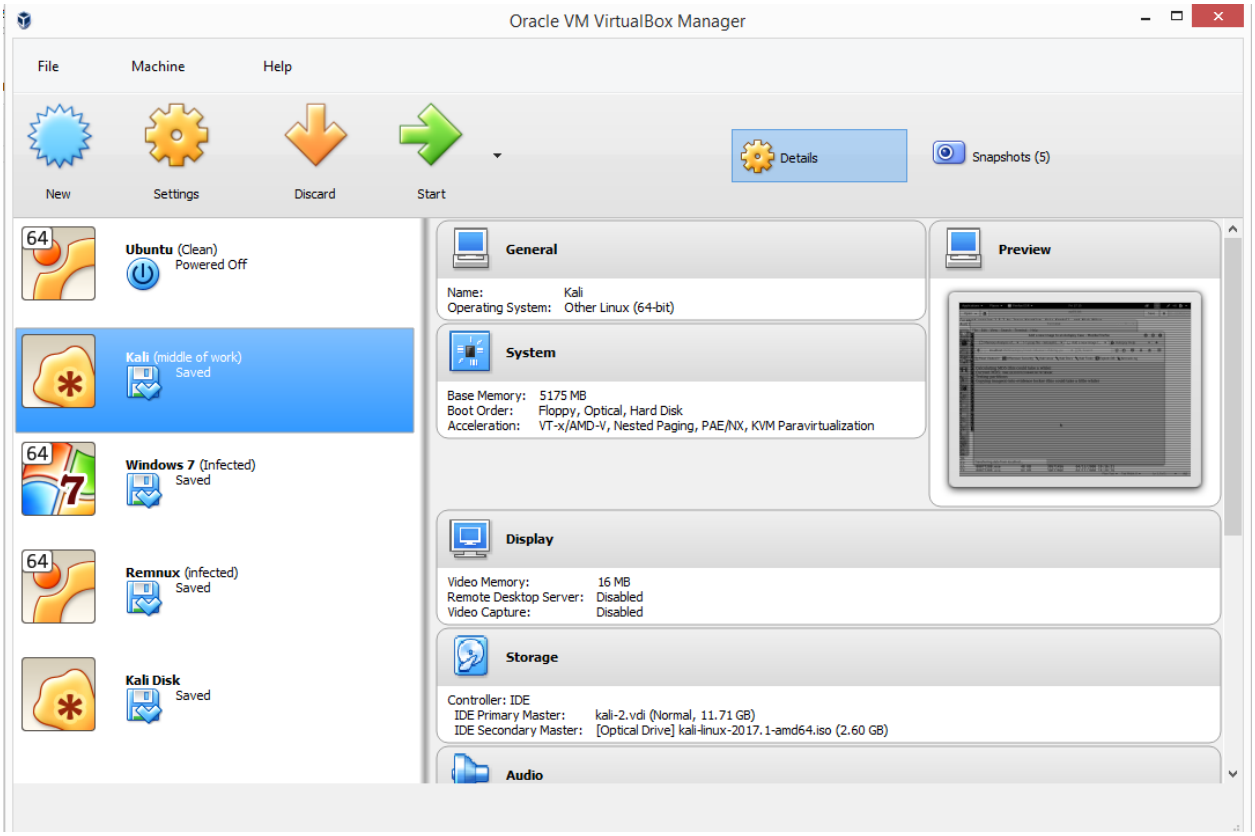
Analyzing the Memory Dump of WannaCry Ransomware

Background:

Setup:

Open the Kali Virtual Machine



If you see the login page and do not know the password try the default: toor

Evidence

wcry.raw memory sample

Learning objectives:

1. Use common Volatility plugins to follow the six step SANS memory analysis framework:
2. Identify rogue processes
3. Analyze process DLLs and handles
4. Review network artifacts
5. Look for evidence of code injection
6. Check for signs of a Rootkit
7. Dump suspicious processes and drivers

- Getting started with Volatility

```
root@kali:~# volatility -f ~/Documents/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 Win
XPSP2x86)
                     AS Layer1 : IA32PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/root/Documents/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
root@kali:~#
```

- Identify rogue processes

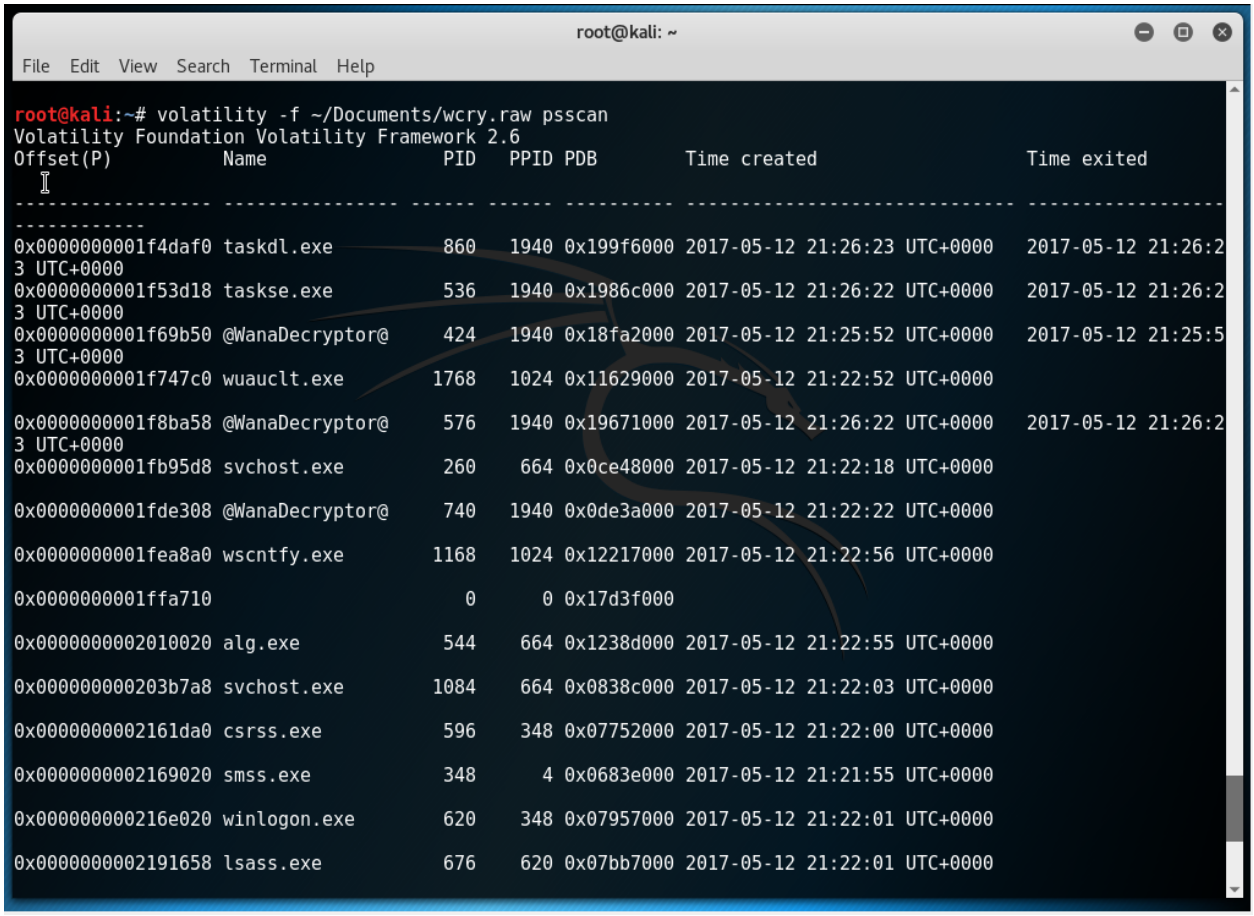
Volatility plugins

Pslist - view running processes

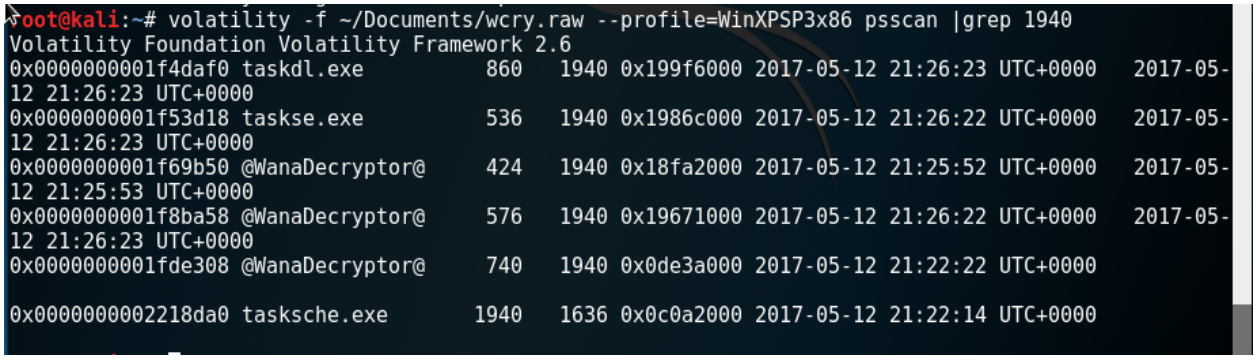
Psscan - scan memory for process blocks

Pstree - display process relationships

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# volatility -f ~/Documents/wcry.raw pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exi
t
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ---
--------------------------
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
```



Detailed psscan to identify odd processes that were exited (@wanaDecryptor@):



- Analyze process dlls and handles

Plugins

Dlllist - list of loaded dll by process with process ids

Handles - list of open handles for each process

Filescan - scan memory for FILE_OBJECT handles

```
root@kali:~# volatility -f ~/Documents/wcry.raw --profile=WinXPSP3x86 dlllist -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_6.0.2
600.6028_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
```

```
root@kali:~# volatility -f ~/Documents/wcry.raw --profile=WinXPSP3x86 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-w
w_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
0x74e30000    0x6d000        0x1 C:\WINDOWS\system32\RICHED20.dll
0x5ad70000    0x38000        0x3 C:\WINDOWS\system32\uxtheme.dll
0x74720000    0x4c000        0x1 C:\WINDOWS\system32\MSCTF.dll
0x755c0000    0x2e000        0x2 C:\WINDOWS\system32\msctfime.ime
0x769c0000    0xb4000        0x1 C:\WINDOWS\system32\USERENV.dll
0x00ea0000    0x29000        0x1 C:\WINDOWS\system32\msls31.dll
root@kali:~#
```

Handles:

```
root@kali:~# volatility -f ~/Documents/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
root@kali:~# volatility -f ~/Documents/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
root@kali:~# volatility -f ~/Documents/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.Commo
n-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.Commo
n-Controls_6595b64144ccf1df_6.0.2600.6028_x-ww_61e65202
```

Filescan:

```
root@kali:~# volatility -f ~/Documents/wcry.raw --profile=WinXPSP3x86 filescan | grep ivecuqmanpnirkt615
Volatility Foundation Volatility Framework 2.6
0x0000000001f871a0      1      0 R--rw- \Device\HarddiskVolume1\Intel\ivecuqmanpnirkt615\@WanaDecryptor@.exe
0x0000000001fb17a8      1      0 R--r-d \Device\HarddiskVolume1\Intel\ivecuqmanpnirkt615\@WanaDecryptor@.exe
0x0000000001fb2278      1      0 R--r-d \Device\HarddiskVolume1\Intel\ivecuqmanpnirkt615\taskse.exe
0x0000000001fbcef8      1      0 -W---- \Device\HarddiskVolume1\Intel\ivecuqmanpnirkt615\u.wnry
0x000000000209dbe8      1      0 -W-r-- \Device\HarddiskVolume1\Intel\ivecuqmanpnirkt615\00000000.res
0x000000000209de48      1      0 R--r-- \Device\HarddiskVolume1\Intel\ivecuqmanpnirkt615\b.wnry
0x00000000021d8ac0      1      0 -W---- \Device\HarddiskVolume1\Intel\ivecuqmanpnirkt615\s.wnry
0x00000000021dc028      1      0 R--r-d \Device\HarddiskVolume1\Intel\ivecuqmanpnirkt615\taskdl.exe
0x00000000021f3870      1      0 R--rw- \Device\HarddiskVolume1\Intel\ivecuqmanpnirkt615\tasksche.exe
0x000000000220ec40      1      0 -W---- \Device\HarddiskVolume1\Intel\ivecuqmanpnirkt615\msg\m_turkish.wnry
0x0000000002212028      1      0 -W---- \Device\HarddiskVolume1\Intel\ivecuqmanpnirkt615\msg\m_russian.wnry
0x0000000002217528      1      0 -W---- \Device\HarddiskVolume1\Intel\ivecuqmanpnirkt615\msg\m_spanish.wnry
0x0000000002219b30      1      0 -W---- \Device\HarddiskVolume1\Intel\ivecuqmanpnirkt615\msg\m_slovak.wnry
0x0000000002229748      1      0 -W---- \Device\HarddiskVolume1\Intel\ivecuqmanpnirkt615\msg\m_vietnamese.wnry
0x0000000002232418      1      0 -W---- \Device\HarddiskVolume1\Intel\ivecuqmanpnirkt615\msg\m_swedish.wnry
0x0000000002233f18      1      1 R--rw- \Device\HarddiskVolume1\Intel\ivecuqmanpnirkt615
0x0000000022456e0       1      1 R--rw- \Device\HarddiskVolume1\Intel\ivecuqmanpnirkt615
0x0000000002256c88      1      0 -W---- \Device\HarddiskVolume1\Intel\ivecuqmanpnirkt615\t.wnry
0x00000000022bb7f8      1      0 R--r-- \Device\HarddiskVolume1\Intel\ivecuqmanpnirkt615\00000000.pky
0x00000000022c72b0      1      0 R----- \Device\HarddiskVolume1\Intel\ivecuqmanpnirkt615\msg\m_english.wnry
0x00000000022d2f28      1      0 R--r-d \Device\HarddiskVolume1\Intel\ivecuqmanpnirkt615\tasksche.exe
0x00000000022ec718      1      0 R--rw- \Device\HarddiskVolume1\Intel\ivecuqmanpnirkt615\c.wnry
0x00000000022f06f8      1      0 -W---- \Device\HarddiskVolume1\Intel\ivecuqmanpnirkt615\msg\m_romanian.wnry
root@kali:~#
```

- Review network artifacts

Volatility plugins:
Connections - list of open TCP connections
Connscan - ID TCP connections (including closed)
Sockets - find listening sockets
Additional tools:
Bulk_extractor
tshark

Ideally a pcap file will be available for analysis. However, if a pcap file does not exist it is possible to extract some network traffic from the memory dump using bulk_extractor

```
root@kali:~# bulk_extractor -E net -o pcap/ ~/Documents/wcry.raw
bulk_extractor version: 1.6.0-dev
Hostname: kali
Input file: /root/Documents/wcry.raw
Output directory: pcap/
Disk Size: 536870912
Threads: 1
Attempt to open /root/Documents/wcry.raw
15:12:32 Offset 67MB (12.50%) Done in  0:00:15 at 15:12:47
15:12:34 Offset 150MB (28.12%) Done in  0:00:11 at 15:12:45
15:12:37 Offset 234MB (43.75%) Done in  0:00:08 at 15:12:45
15:12:39 Offset 318MB (59.38%) Done in  0:00:06 at 15:12:45
15:12:42 Offset 402MB (75.00%) Done in  0:00:04 at 15:12:46
15:12:46 Offset 486MB (90.62%) Done in  0:00:01 at 15:12:47
All data are read; waiting for threads to finish...
Time elapsed waiting for 1 thread to finish:
     (timeout in 60 min.)
All Threads Finished!
Producer time spent waiting: 14.4656 sec.
Average consumer time spent waiting: 0.080741 sec.
****************************************
** bulk_extractor is probably CPU bound. **
**    Run on a computer with more cores  **
**      to get better performance.       **
****************************************
MD5 of Disk Image: 7b8e11e3ccd7ecc8940f39c7973b5ebc
Phase 2. Shutting down scanners
Phase 3. Creating Histograms
Elapsed time: 17.9119 sec.
Total MB processed: 536
Overall performance: 29.9729 MBytes/sec (29.9729 MBytes/sec/thread)
```

In this particular case the none of the traditional volatility plugins provided much information to work with:

```
root@kali:~# volatility -f ~/Documents/wcry.raw --profile=WinXPSP3x86 connections
Volatility Foundation Volatility Framework 2.6
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------ ---
root@kali:~# volatility -f ~/Documents/wcry.raw --profile=WinXPSP3x86 connscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------ ---
root@kali:~# volatility -f ~/Documents/wcry.raw --profile=WinXPSP3x86 sockets
Volatility Foundation Volatility Framework 2.6
Offset(V)       PID   Port  Proto Protocol        Address         Create Time
---------- -------- ------ ------ --------------- --------------- -----------
0x8223d3b8        4    138     17 UDP             192.168.56.101  2017-05-12 21:21:56 UTC+0000
0x81fb4890        4      0     47 GRE             0.0.0.0         2017-05-12 21:22:55 UTC+0000
0x81f707c0     1024   1025     17 UDP             127.0.0.1       2017-05-12 21:22:53 UTC+0000
0x81f74c18      676    500     17 UDP             0.0.0.0         2017-05-12 21:22:53 UTC+0000
0x82188658     1024    123     17 UDP             192.168.56.101  2017-05-12 21:22:53 UTC+0000
0x8219b3b8        4    445      6 TCP             0.0.0.0         2017-05-12 21:21:55 UTC+0000
0x821824b0      904    135      6 TCP             0.0.0.0         2017-05-12 21:22:03 UTC+0000
0x81ffb890        4   1027      6 TCP             0.0.0.0         2017-05-12 21:22:55 UTC+0000
0x81f6a360     1024    123     17 UDP             127.0.0.1       2017-05-12 21:22:53 UTC+0000
0x81f7fe98      676      0    255 Reserved        0.0.0.0         2017-05-12 21:22:53 UTC+0000
0x81fb42a0     1152   1900     17 UDP             192.168.56.101  2017-05-12 21:22:55 UTC+0000
0x821617e0        4    139      6 TCP             192.168.56.101  2017-05-12 21:21:56 UTC+0000
0x81f97320      544   1026      6 TCP             127.0.0.1       2017-05-12 21:22:55 UTC+0000
0x82165e98        4    137     17 UDP             192.168.56.101  2017-05-12 21:21:56 UTC+0000
0x81f86008     1152   1900     17 UDP             127.0.0.1       2017-05-12 21:22:55 UTC+0000
0x81f6ae98      676   4500     17 UDP             0.0.0.0         2017-05-12 21:22:53 UTC+0000
0x8219b7e0        4    445     17 UDP             0.0.0.0         2017-05-12 21:21:55 UTC+0000
```

To identify ip addresses in the extracted pcap file we can use tshark. Note the directory change.

```
root@kali:~# cd pcap
root@kali:~/pcap# tshark -T fields -e ip.src -r packets.pcap | sort -u
Running as user "root" and group "root". This could be dangerous.
tshark: Lua: Error during loading:
 [string "/usr/share/wireshark/init.lua"]:44: dofile has been disabled due to running Wireshark as superuser. See https://w
iki.wireshark.org/CaptureSetup/CapturePrivileges for help in running Wireshark as an unprivileged user.
134.119.3.164
192.168.56.101
199.254.238.52
213.61.66.118
root@kali:~/pcap#
```

For further analysis we can create a dumpfile with all of the potentially bad ips using the following tshark command:

```
> tshark -T fields -e ip.src -r dump.pcap | sort -u
```

- Look for evidence of code injection

Volatility plugins:

Malfind - find injected code and dump sections

Ldrmodules - detect unlinked dlls

```
root@kali:~# volatility -f ~/Documents/wcry.raw --profile=WinXPSP3x86 malfind -p 836,904
Volatility Foundation Volatility Framework 2.6
root@kali:~#
root@kali:~#
```

```
root@kali:~# volatility -f ~/Documents/wcry.raw --profile=WinXPSP3x86 ldrmodules -p 676
Volatility Foundation Volatility Framework 2.6
Pid      Process            Base       InLoad InInit InMem MappedPath
-------- ------------------ ---------- ------ ------ ----- ----------
     676 lsass.exe          0x01000000 True   False  True  \WINDOWS\system32\lsass.exe
     676 lsass.exe          0x7c800000 True   True   True  \WINDOWS\system32\kernel32.dll
     676 lsass.exe          0x769c0000 True   True   True  \WINDOWS\system32\userenv.dll
     676 lsass.exe          0x76b40000 True   True   True  \WINDOWS\system32\winmm.dll
     676 lsass.exe          0x75730000 True   True   True  \WINDOWS\system32\lsasrv.dll
     676 lsass.exe          0x76360000 True   True   True  \WINDOWS\system32\winsta.dll
     676 lsass.exe          0x77c00000 True   True   True  \WINDOWS\system32\version.dll
     676 lsass.exe          0x5ad70000 True   True   True  \WINDOWS\system32\uxtheme.dll
     676 lsass.exe          0x77be0000 True   True   True  \WINDOWS\system32\msacm32.dll
     676 lsass.exe          0x774e0000 True   True   True  \WINDOWS\system32\ole32.dll
     676 lsass.exe          0x74d90000 True   True   True  \WINDOWS\system32\usp10.dll
     676 lsass.exe          0x77c70000 True   True   True  \WINDOWS\system32\msv1_0.dll
     676 lsass.exe          0x723a0000 True   True   True  \WINDOWS\system32\tspkg.dll
     676 lsass.exe          0x743a0000 True   True   True  \WINDOWS\system32\pstorsvc.dll
     676 lsass.exe          0x77dd0000 True   True   True  \WINDOWS\system32\advapi32.dll
     676 lsass.exe          0x77a80000 True   True   True  \WINDOWS\system32\crypt32.dll
     676 lsass.exe          0x743e0000 True   True   True  \WINDOWS\system32\ipsecsvc.dll
     676 lsass.exe          0x68000000 True   True   True  \WINDOWS\system32\rsaenh.dll
     676 lsass.exe          0x5b860000 True   True   True  \WINDOWS\system32\netapi32.dll
     676 lsass.exe          0x773d0000 True   True   True  \WINDOWS\WinSxS\x86_Microsoft.Windows.C
ommon-Controls_6595b64144ccf1df_6.0.2600.6028_x-ww_61e65202\comctl32.dll
     676 lsass.exe          0x74440000 True   True   True  \WINDOWS\system32\samsrv.dll
     676 lsass.exe          0x71a50000 True   True   True  \WINDOWS\system32\mswsock.dll
     676 lsass.exe          0x743c0000 True   True   True  \WINDOWS\system32\psbase.dll
     676 lsass.exe          0x59c00000 True   True   True  \WINDOWS\system32\credssp.dll
     676 lsass.exe          0x767f0000 True   True   True  \WINDOWS\system32\schannel.dll
     676 lsass.exe          0x6f880000 True   True   True  \WINDOWS\AppPatch\AcGenral.dll
     676 lsass.exe          0x71a90000 True   True   True  \WINDOWS\system32\wshtcpip.dll
     676 lsass.exe          0x71ab0000 True   True   True  \WINDOWS\system32\ws2_32.dll
```

- Check for signs of a rootkit
- Dump suspicious processes and drivers