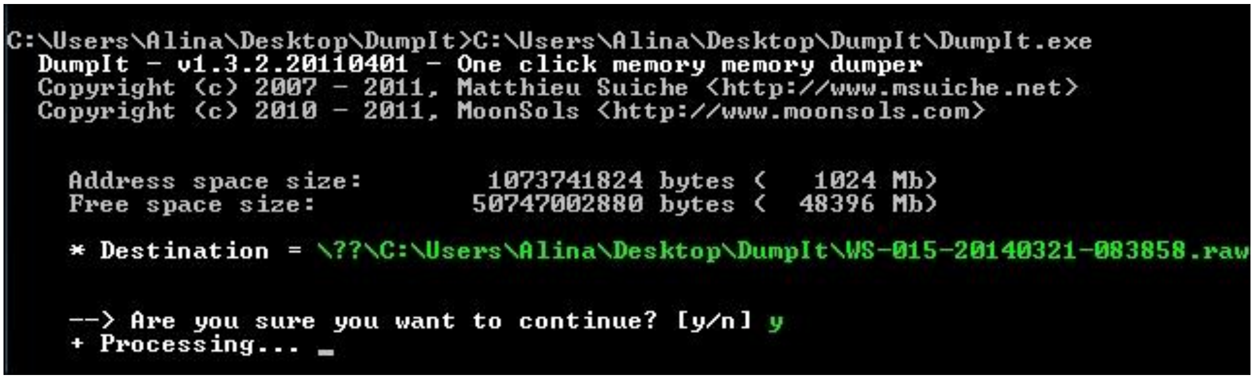
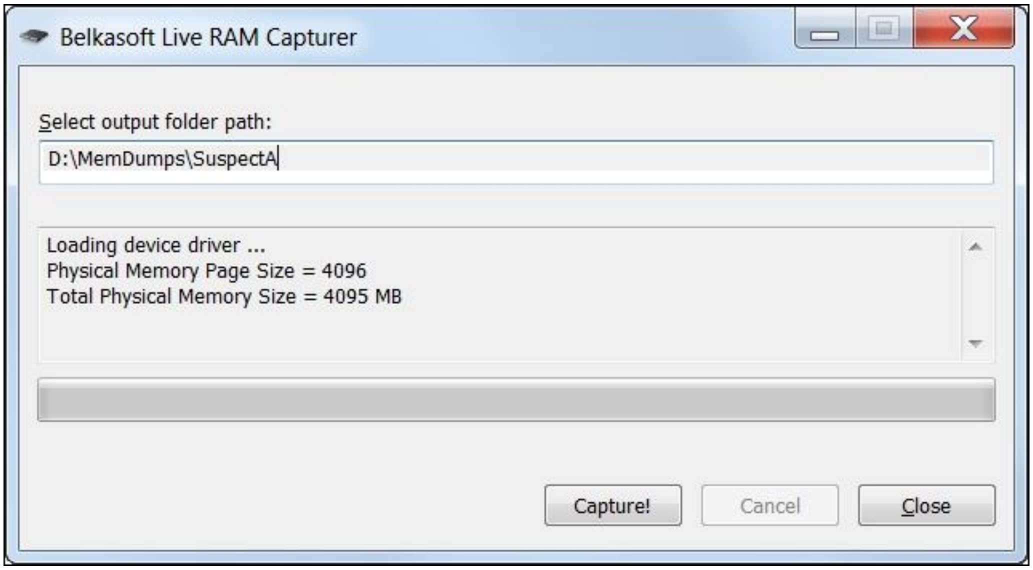
Chapter 2: Incident Response and Live Analysis

Chapter 3: Volatile Data Collection



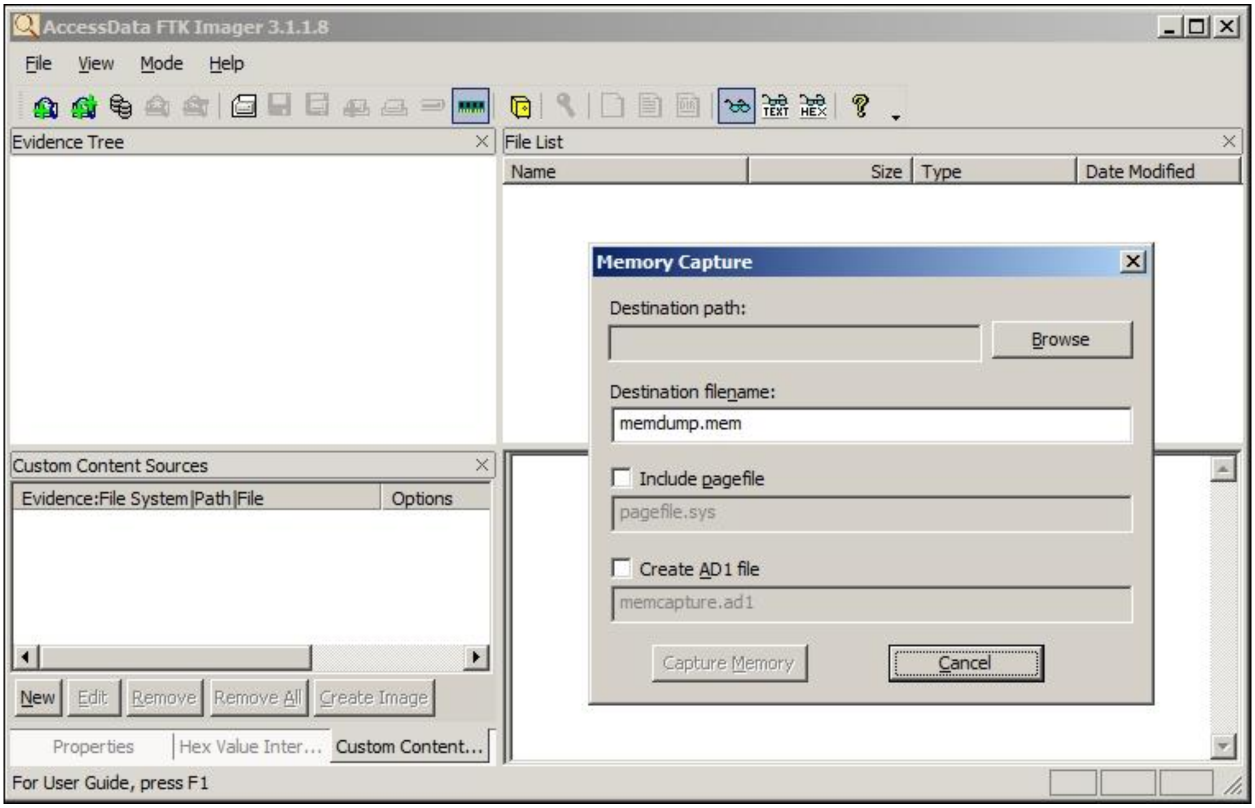
```
C:\Users\Alina\Desktop\DumpIt>C:\Users\Alina\Desktop\DumpIt\DumpIt.exe
  DumpIt - v1.3.2.20110401 - One click memory memory dumper
  Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
  Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>

    Address space size:          1073741824 bytes (   1024 Mb)
    Free space size:            50747002880 bytes (  48396 Mb)

    * Destination = \??\C:\Users\Alina\Desktop\DumpIt\WS-015-20140321-083858.raw

    --> Are you sure you want to continue? [y/n] y
    + Processing... _
```



Select output folder path:

D:\MemDumps\SuspectA

```
Loading device driver ...
Physical Memory Page Size = 4096
Total Physical Memory Size = 4095 MB
```



Memory Capture

Destination path:

Browse

Destination filename: memdump.mem

□ Include pagefile

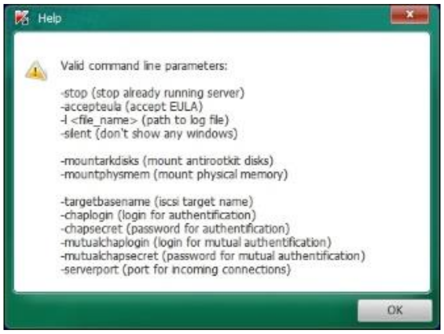
pagefile.sys

□ Create AD1 file

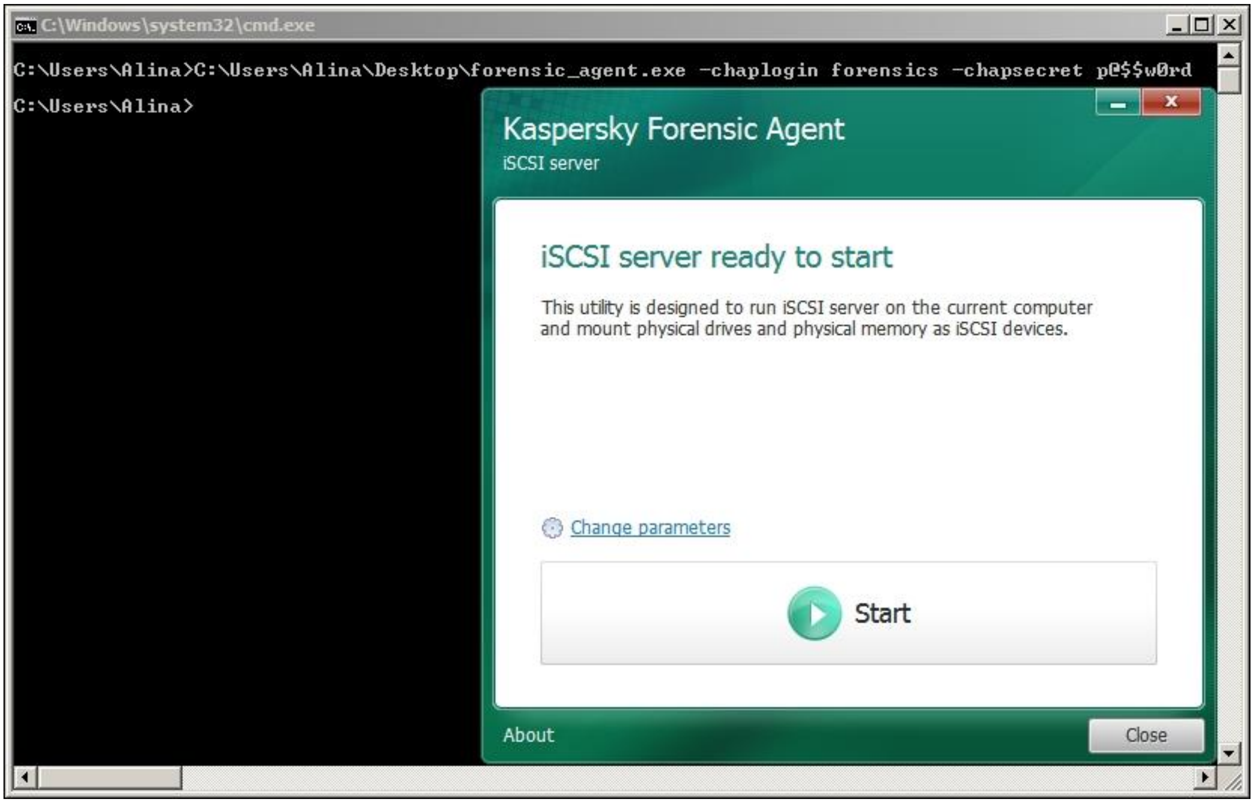
memcapture.ad1

Capture Memory

Cancel



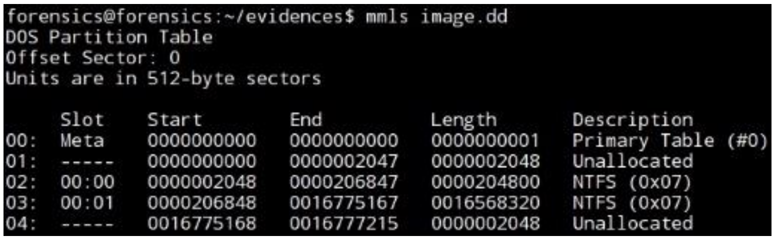
```
Valid command line parameters:

-stop (stop already running server)
-accepteula (accept EULA)
-l <file_name> (path to log file)
-silent (don't show any windows)

-mountarkdisks (mount antirootkit disks)
-mountphysmem (mount physical memory)

-targetbasename (iscsi target name)
-chaplogin (login for authentification)
-chapsecret (password for authentification)
-mutualchaplogin (login for mutual authentification)
-mutualchapsecret (password for mutual authentification)
-serverport (port for incoming connections)
```



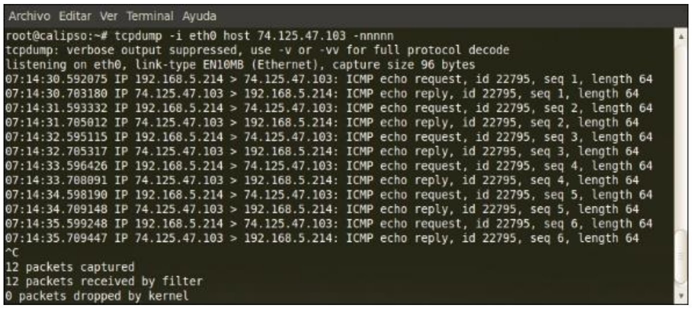
```
C:\Users\Alina>C:\Users\Alina\Desktop\forensic_agent.exe -chaplogin forensics -chapsecret p@$$w0rd

C:\Users\Alina>
```

iSCSI server ready to start

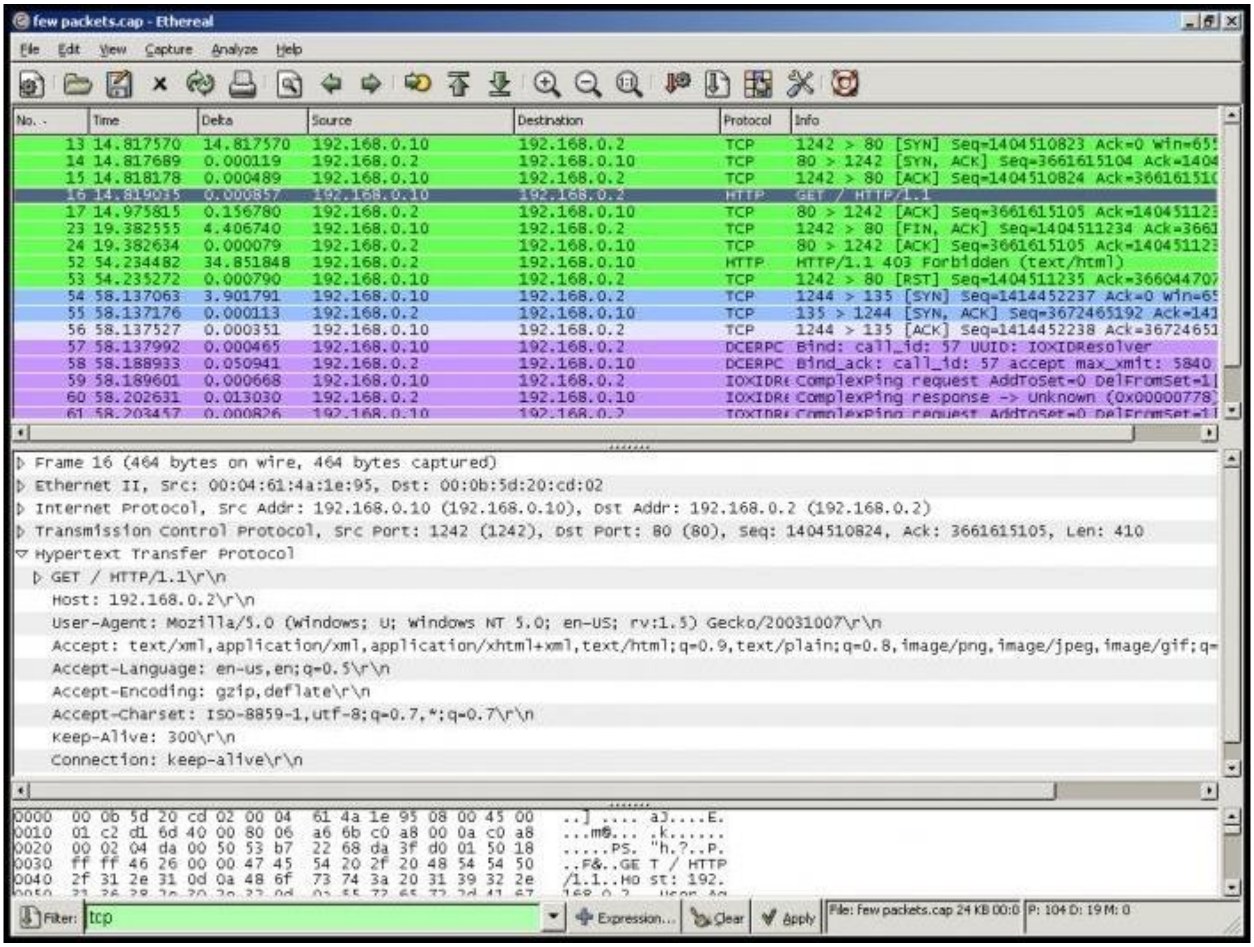
This utility is designed to run iSCSI server on the current computer and mount physical drives and physical memory as iSCSI devices.



```
forensics@forensics:~/evidences$ mmls image.dd
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

     Slot     Start        End          Length       Description
00:  Meta     0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----    0000000000   0000002047   0000002048   Unallocated
02:  00:00    0000002048   0000206847   0000204800   NTFS (0x07)
03:  00:01    0000206848   0016775167   0016568320   NTFS (0x07)
04:  -----    0016775168   0016777215   0000002048   Unallocated
```



```
root@calipso:~# tcpdump -i eth0 host 74.125.47.103 -nnnnn
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
07:14:30.592075 IP 192.168.5.214 > 74.125.47.103: ICMP echo request, id 22795, seq 1, length 64
07:14:30.703180 IP 74.125.47.103 > 192.168.5.214: ICMP echo reply, id 22795, seq 1, length 64
07:14:31.593332 IP 192.168.5.214 > 74.125.47.103: ICMP echo request, id 22795, seq 2, length 64
07:14:31.705012 IP 74.125.47.103 > 192.168.5.214: ICMP echo reply, id 22795, seq 2, length 64
07:14:32.595115 IP 192.168.5.214 > 74.125.47.103: ICMP echo request, id 22795, seq 3, length 64
07:14:32.705317 IP 74.125.47.103 > 192.168.5.214: ICMP echo reply, id 22795, seq 3, length 64
07:14:33.596426 IP 192.168.5.214 > 74.125.47.103: ICMP echo request, id 22795, seq 4, length 64
07:14:33.708091 IP 74.125.47.103 > 192.168.5.214: ICMP echo reply, id 22795, seq 4, length 64
07:14:34.598190 IP 192.168.5.214 > 74.125.47.103: ICMP echo request, id 22795, seq 5, length 64
07:14:34.709148 IP 74.125.47.103 > 192.168.5.214: ICMP echo reply, id 22795, seq 5, length 64
07:14:35.599248 IP 192.168.5.214 > 74.125.47.103: ICMP echo request, id 22795, seq 6, length 64
07:14:35.709447 IP 74.125.47.103 > 192.168.5.214: ICMP echo reply, id 22795, seq 6, length 64
^C
12 packets captured
12 packets received by filter
0 packets dropped by kernel
```



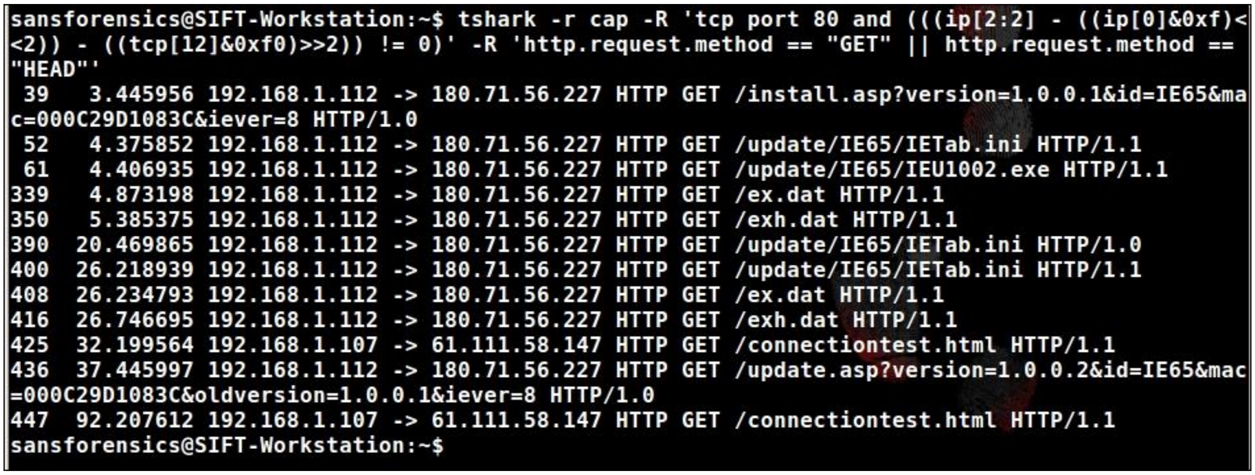
```
No. -  Time       Delta      Source          Destination     Protocol Info
    13 14.817570  14.817570  192.168.0.10    192.168.0.2     TCP      1242 > 80 [SYN] Seq=1404510823 Ack=0 Win=65
    14 14.817689  0.000119   192.168.0.2     192.168.0.10    TCP      80 > 1242 [SYN, ACK] Seq=3661615104 Ack=1404
    15 14.818178  0.000489   192.168.0.10    192.168.0.2     TCP      1242 > 80 [ACK] Seq=1404510824 Ack=36616151(
    16 14.819035  0.000857   192.168.0.10    192.168.0.2     HTTP     GET / HTTP/1.1
    17 14.975815  0.156780   192.168.0.2     192.168.0.10    TCP      80 > 1242 [ACK] Seq=3661615105 Ack=14045112:
    23 19.382555  4.406740   192.168.0.10    192.168.0.2     TCP      1242 > 80 [FIN, ACK] Seq=1404511234 Ack=3661
    24 19.382634  0.000079   192.168.0.2     192.168.0.10    TCP      80 > 1242 [ACK] Seq=3661615105 Ack=14045112:
    52 54.234482  34.851848  192.168.0.2     192.168.0.10    HTTP     HTTP/1.1 403 Forbidden (text/html)
    53 54.235272  0.000790   192.168.0.10    192.168.0.2     TCP      1242 > 80 [RST] Seq=1404511235 Ack=36604470?
    54 58.137063  3.901791   192.168.0.10    192.168.0.2     TCP      1244 > 135 [SYN] Seq=1414452237 Ack=0 Win=65
    55 58.137176  0.000113   192.168.0.2     192.168.0.10    TCP      135 > 1244 [SYN, ACK] Seq=3672465192 Ack=141
    56 58.137527  0.000351   192.168.0.10    192.168.0.2     TCP      1244 > 135 [ACK] Seq=1414452238 Ack=36724651
    57 58.137992  0.000465   192.168.0.10    192.168.0.2     DCERPC   Bind: call_id: 57 UUID: IOXIDResolver
    58 58.188933  0.050941   192.168.0.2     192.168.0.10    DCERPC   Bind_ack: call_id: 57 accept max_xmit: 5840
    59 58.189601  0.000668   192.168.0.10    192.168.0.2     IOXIDR(  ComplexPing request AddToSet=0 DelFromSet=1|
    60 58.202631  0.013030   192.168.0.2     192.168.0.10    IOXIDR(  ComplexPing response -> Unknown (0x00000778)
    61 58.203457  0.000826   192.168.0.10    192.168.0.2     IOXIDR(  ComplexPing request AddToSet=0 DelFromSet=1|
```

```
▷ Frame 16 (464 bytes on wire, 464 bytes captured)
▷ Ethernet II, Src: 00:04:61:4a:1e:95, Dst: 00:0b:5d:20:cd:02
▷ Internet Protocol, Src Addr: 192.168.0.10 (192.168.0.10), Dst Addr: 192.168.0.2 (192.168.0.2)
▷ Transmission Control Protocol, Src Port: 1242 (1242), Dst Port: 80 (80), Seq: 1404510824, Ack: 3661615105, Len: 410
▽ Hypertext Transfer Protocol
  ▷ GET / HTTP/1.1\r\n
    Host: 192.168.0.2\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.5) Gecko/20031007\r\n
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,image/jpeg,image/gif;q=
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
```

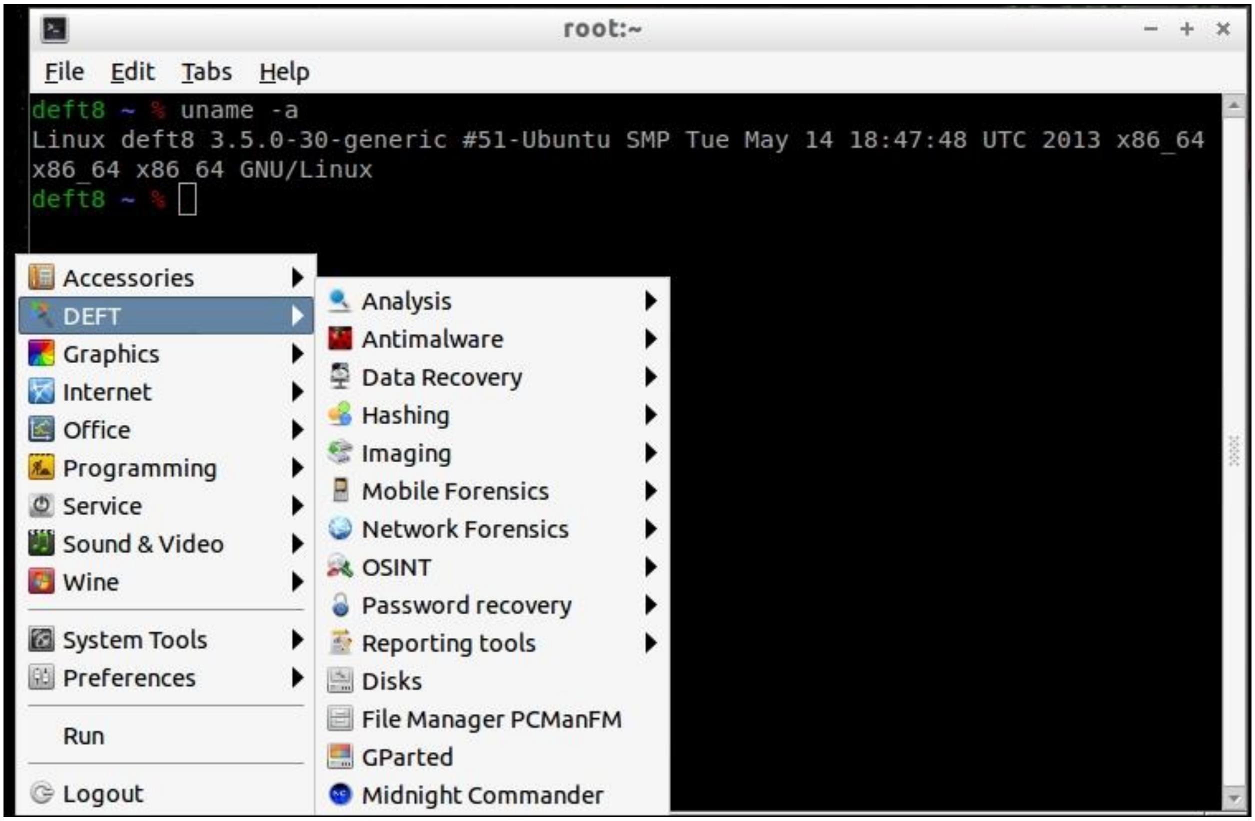
```
0000  00 0b 5d 20 cd 02 00 04  61 4a 1e 95 08 00 45 00   ..] .... aJ....E.
0010  01 c2 d1 6d 40 00 80 06  a6 6b c0 a8 00 0a c0 a8   ...m@... .k......
0020  00 02 04 da 00 50 53 b7  22 68 da 3f d0 01 50 18   .....PS. "h.?..P.
0030  ff ff 46 26 00 00 47 45  54 20 2f 20 48 54 54 50   ..F&..GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 31 39 32 2e   /1.1..Ho st: 192.
```

Filter: tcp

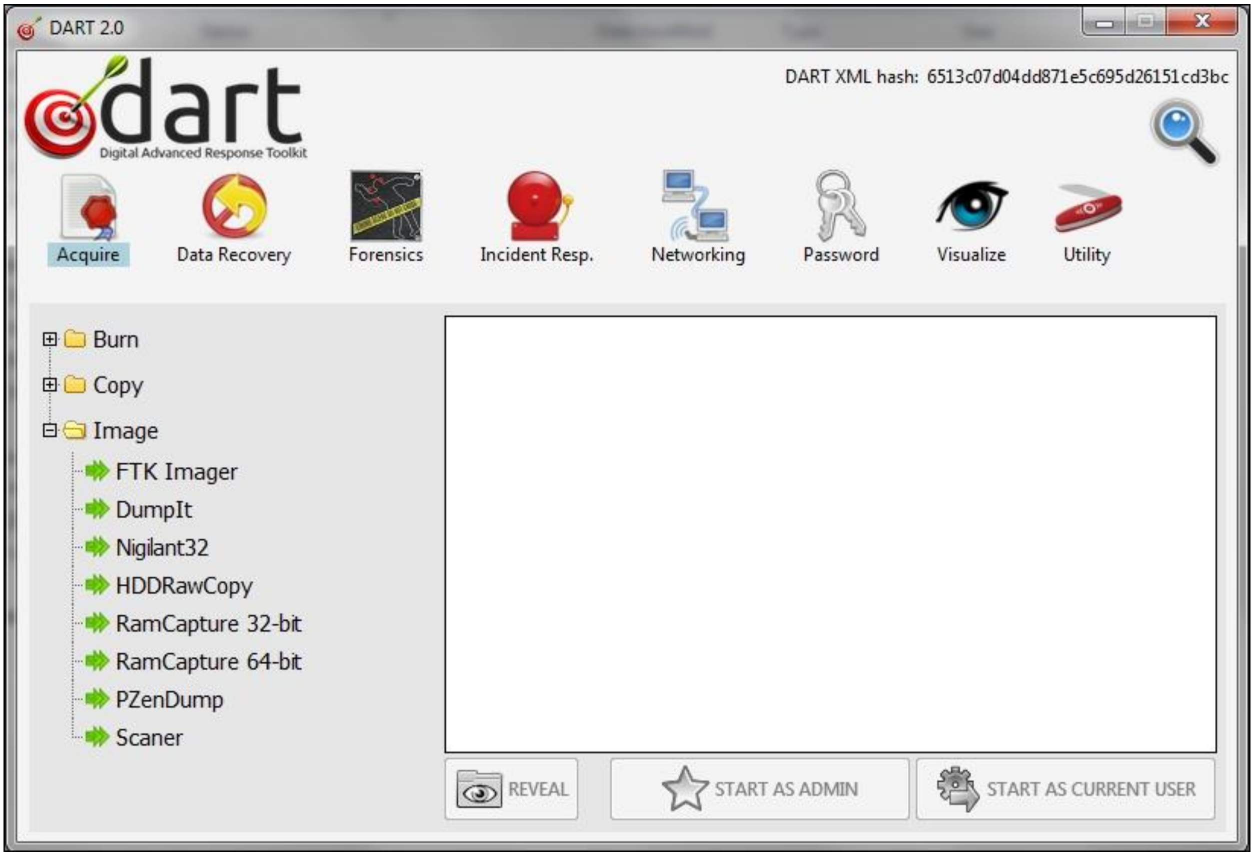
File: Few packets.cap 24 KB 00:0 | P: 104 D: 19 M: 0



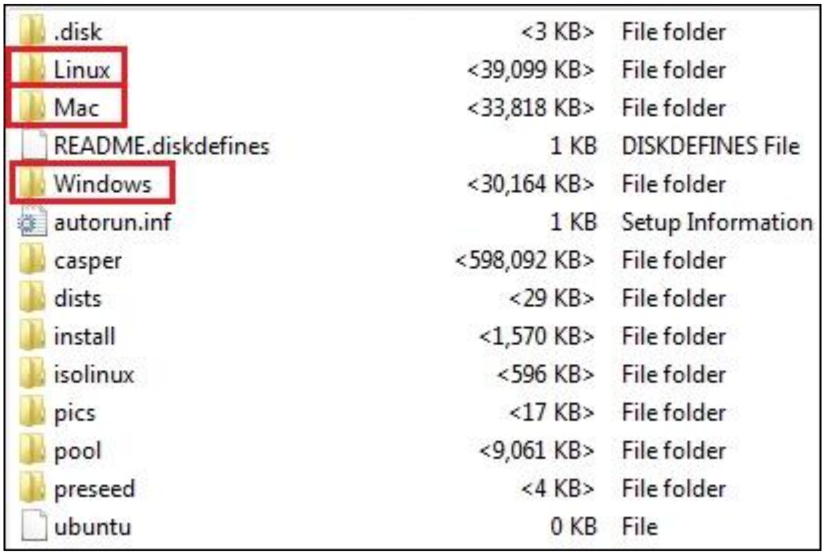
```
sansforensics@SIFT-Workstation:~$ tshark -r cap -R 'tcp port 80 and (((ip[2:2] - ((ip[0]&0xf)<
<2)) - ((tcp[12]&0xf0)>>2)) != 0)' -R 'http.request.method == "GET" || http.request.method ==
"HEAD"'
 39   3.445956 192.168.1.112 -> 180.71.56.227 HTTP GET /install.asp?version=1.0.0.1&id=IE65&ma
c=000C29D1083C&iever=8 HTTP/1.0
 52   4.375852 192.168.1.112 -> 180.71.56.227 HTTP GET /update/IE65/IETab.ini HTTP/1.1
 61   4.406935 192.168.1.112 -> 180.71.56.227 HTTP GET /update/IE65/IEU1002.exe HTTP/1.1
339   4.873198 192.168.1.112 -> 180.71.56.227 HTTP GET /ex.dat HTTP/1.1
350   5.385375 192.168.1.112 -> 180.71.56.227 HTTP GET /exh.dat HTTP/1.1
390  20.469865 192.168.1.112 -> 180.71.56.227 HTTP GET /update/IE65/IETab.ini HTTP/1.0
400  26.218939 192.168.1.112 -> 180.71.56.227 HTTP GET /update/IE65/IETab.ini HTTP/1.1
408  26.234793 192.168.1.112 -> 180.71.56.227 HTTP GET /ex.dat HTTP/1.1
416  26.746695 192.168.1.112 -> 180.71.56.227 HTTP GET /exh.dat HTTP/1.1
425  32.199564 192.168.1.107 -> 61.111.58.147 HTTP GET /connectiontest.html HTTP/1.1
436  37.445997 192.168.1.112 -> 180.71.56.227 HTTP GET /update.asp?version=1.0.0.2&id=IE65&mac
=000C29D1083C&oldversion=1.0.0.1&iever=8 HTTP/1.0
447  92.207612 192.168.1.107 -> 61.111.58.147 HTTP GET /connectiontest.html HTTP/1.1
sansforensics@SIFT-Workstation:~$
```



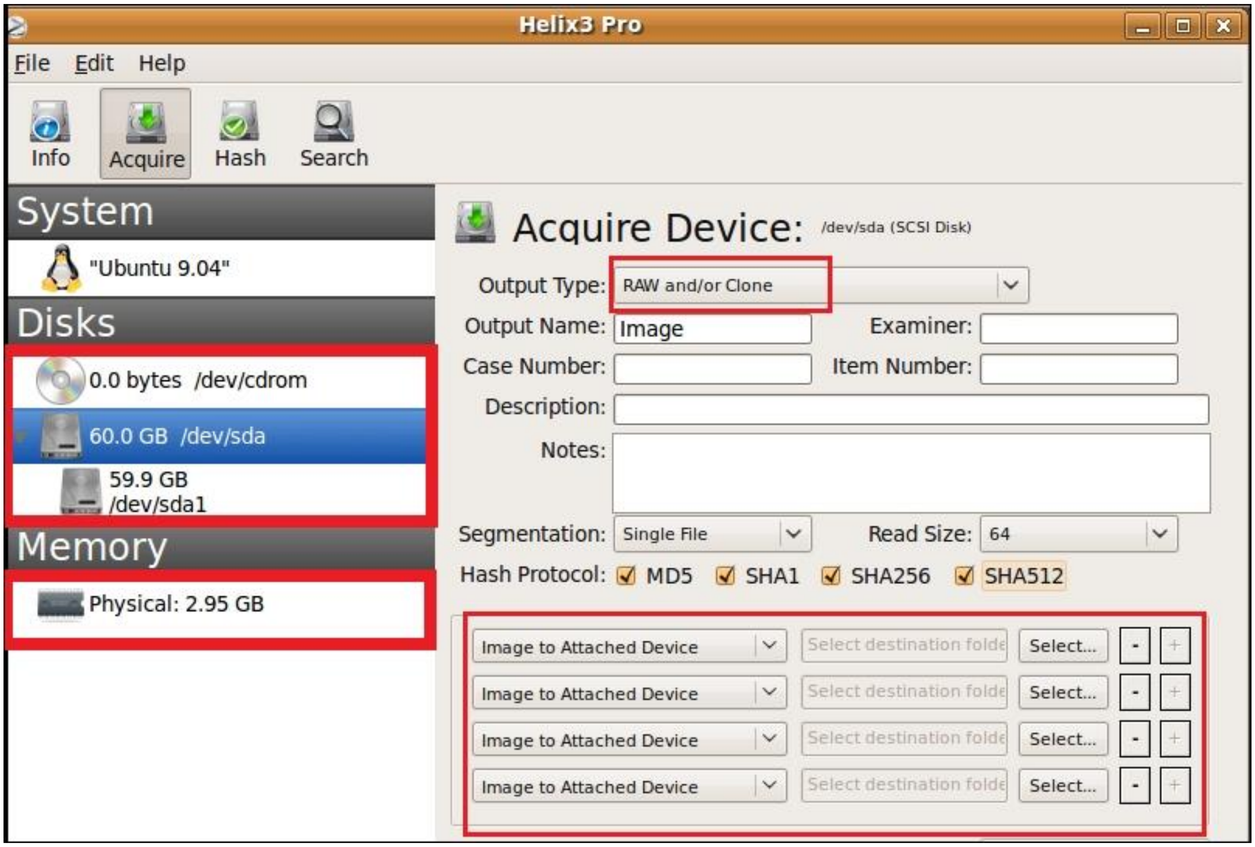
```
deft8 ~ % uname -a
Linux deft8 3.5.0-30-generic #51-Ubuntu SMP Tue May 14 18:47:48 UTC 2013 x86_64
x86_64 x86_64 GNU/Linux
deft8 ~ % 
```



DART XML hash: 6513c07d04dd871e5c695d26151cd3bc



.disk	<3 KB>	File folder
Linux	<39,099 KB>	File folder
Mac	<33,818 KB>	File folder
README.diskdefines	1 KB	DISKDEFINES File
Windows	<30,164 KB>	File folder
autorun.inf	1 KB	Setup Information
casper	<598,092 KB>	File folder
dists	<29 KB>	File folder
install	<1,570 KB>	File folder
isolinux	<596 KB>	File folder
pics	<17 KB>	File folder
pool	<9,061 KB>	File folder
preseed	<4 KB>	File folder
ubuntu	0 KB	File



System

"Ubuntu 9.04"

Disks

0.0 bytes /dev/cdrom

60.0 GB /dev/sda

59.9 GB /dev/sda1

Memory

Physical: 2.95 GB

Acquire Device: /dev/sda (SCSI Disk)

Output Type: RAW and/or Clone

Output Name: Image

Examiner:

Case Number:

Item Number:

Description:

Notes:

Segmentation: Single File

Read Size: 64

Hash Protocol: ☑ MD5 ☑ SHA1 ☑ SHA256 ☑ SHA512

Image to Attached Device	Select destination folde	Select...	-	+
Image to Attached Device	Select destination folde	Select...	-	+
Image to Attached Device	Select destination folde	Select...	-	+
Image to Attached Device	Select destination folde	Select...	-	+

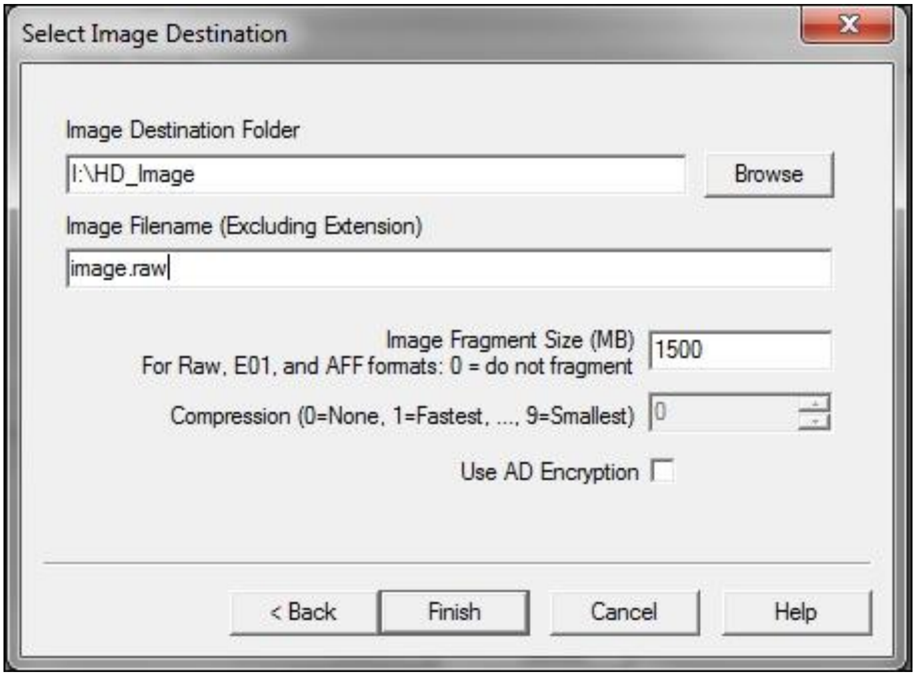


Image Destination Folder

I:\HD_Image

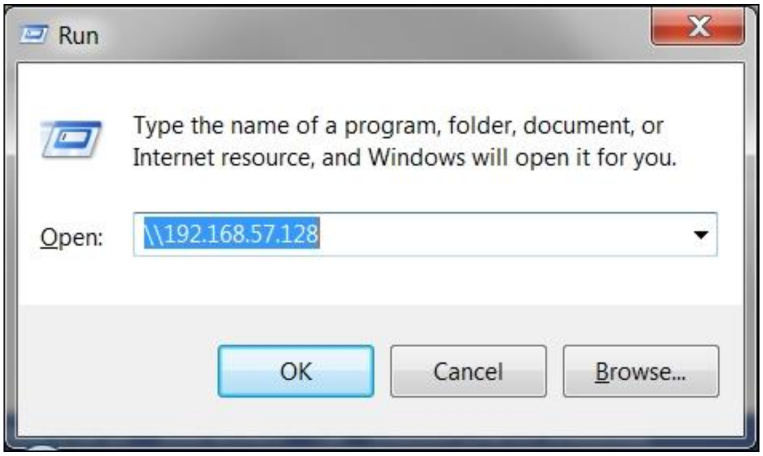
Image Filename (Excluding Extension)

image.raw

Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment 1500

Compression (0=None, 1=Fastest, ..., 9=Smallest) 0

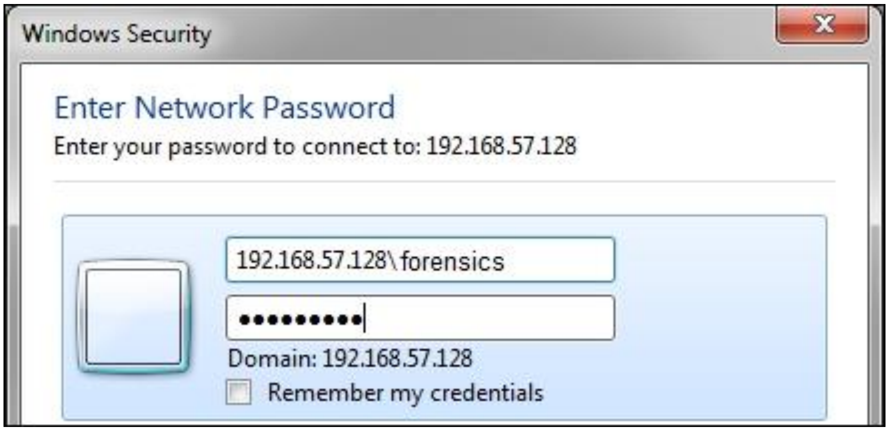
Use AD Encryption □



Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: \\192.168.57.128



Windows Security

Enter Network Password

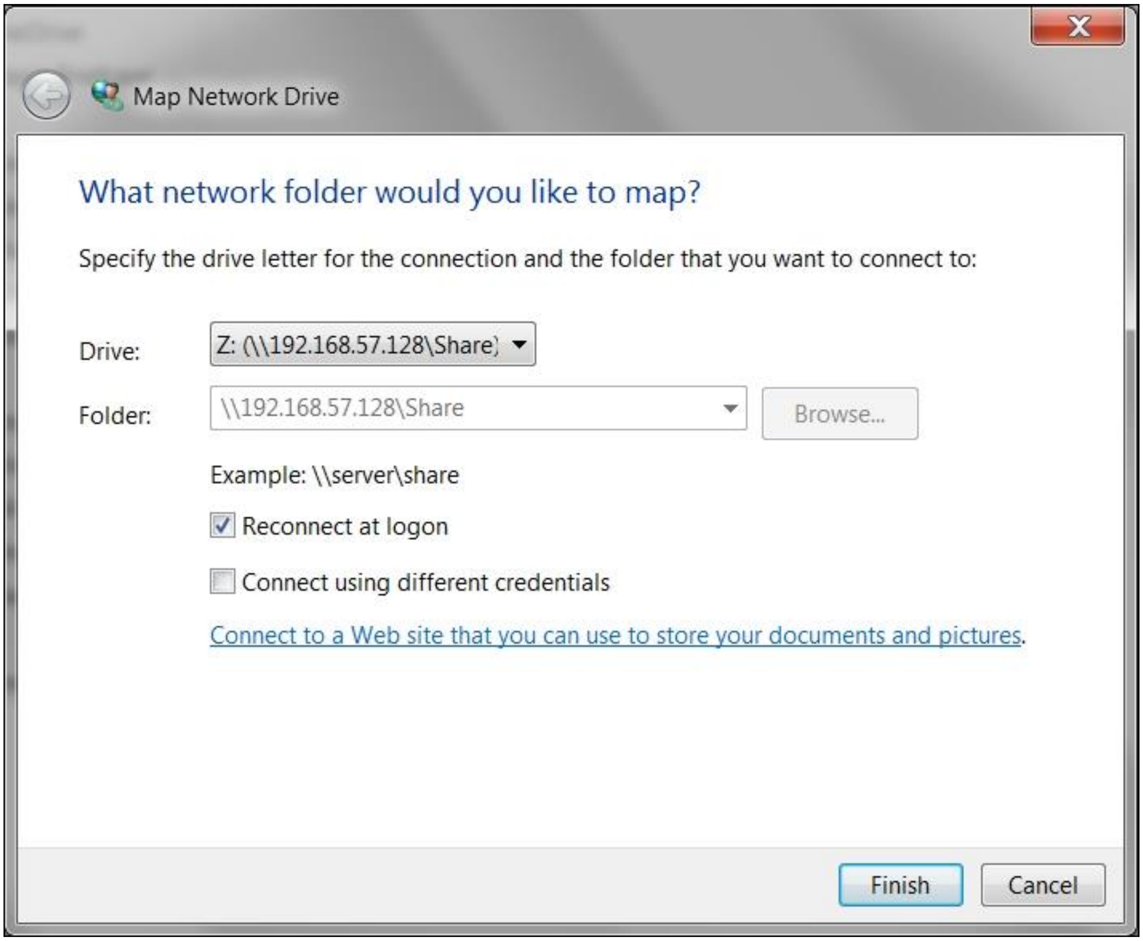
Enter your password to connect to: 192.168.57.128

192.168.57.128\forensics

•••••••••

Domain: 192.168.57.128

□ Remember my credentials



Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z: (\\192.168.57.128\Share)

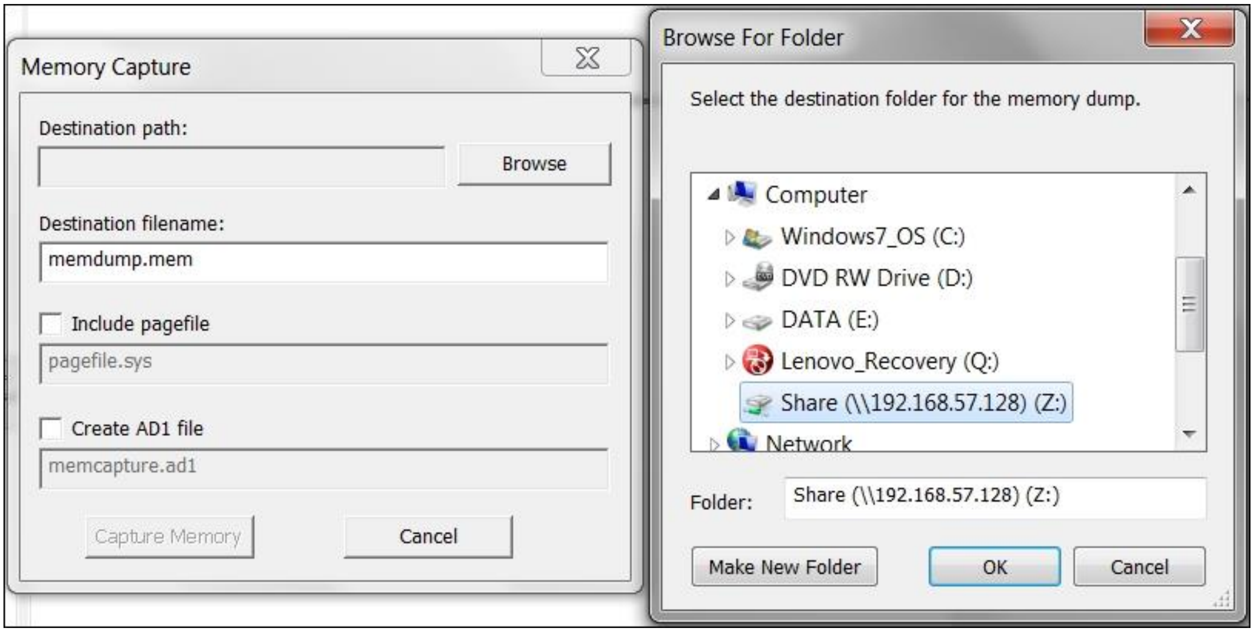
Folder: \\192.168.57.128\Share

Example: \\server\share

☑ Reconnect at logon

□ Connect using different credentials

Connect to a Web site that you can use to store your documents and pictures.



Memory Capture

Destination path:

Destination filename: memdump.mem

□ Include pagefile

pagefile.sys

□ Create AD1 file

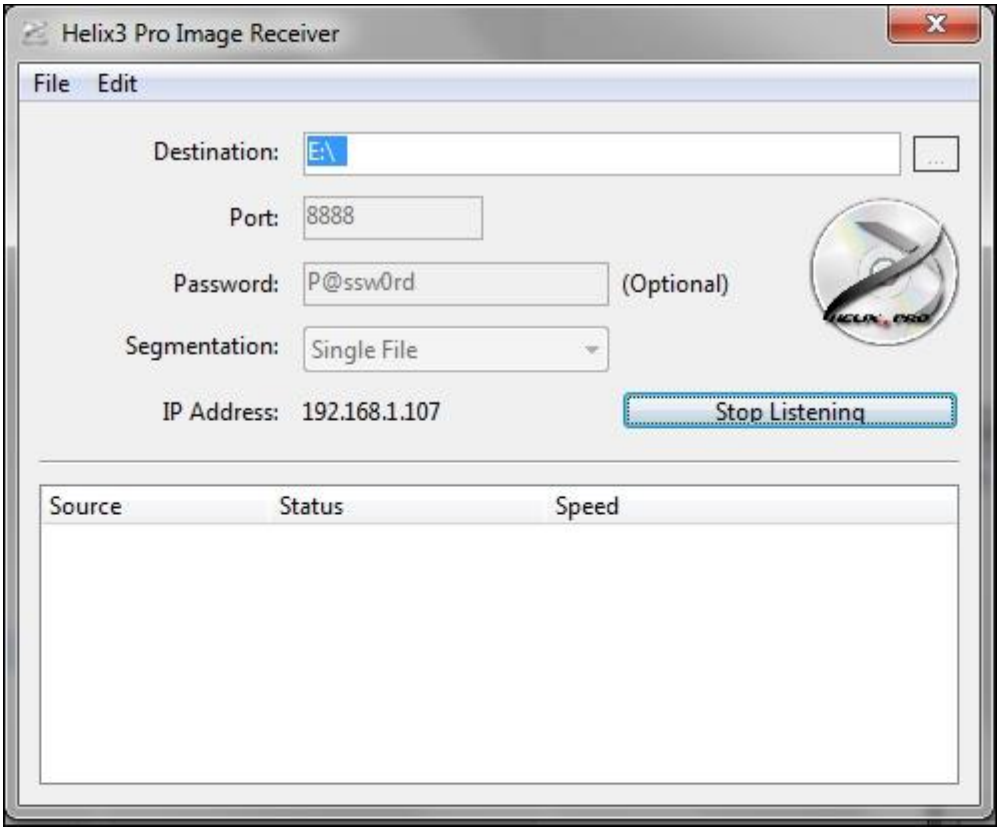
memcapture.ad1

Browse For Folder

Select the destination folder for the memory dump.

- Computer
  - Windows7_OS (C:)
  - DVD RW Drive (D:)
  - DATA (E:)
  - Lenovo_Recovery (Q:)
  - Share (\\192.168.57.128) (Z:)
- Network

Folder: Share (\\192.168.57.128) (Z:)



Destination: E:\

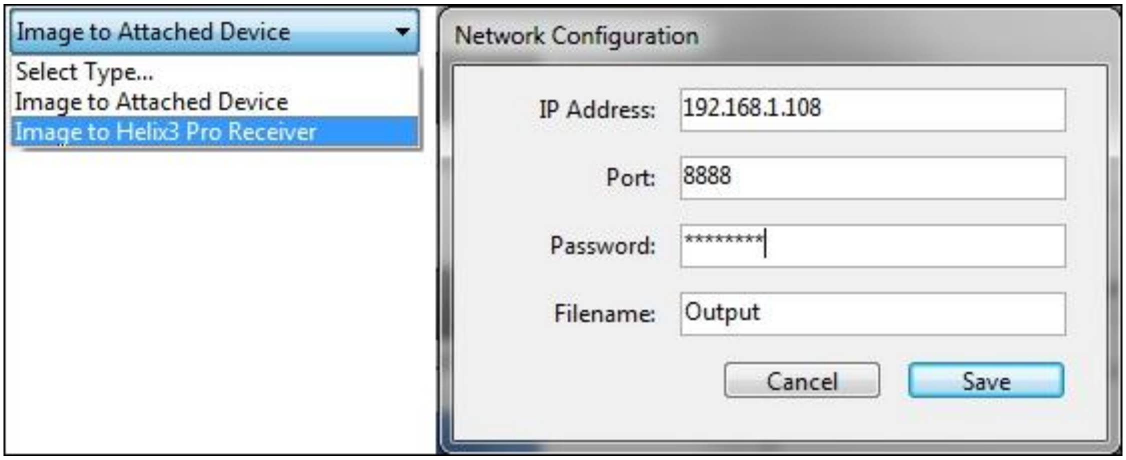
Port: 8888

Password: P@ssw0rd (Optional)

Segmentation: Single File

IP Address: 192.168.1.107

Source	Status	Speed

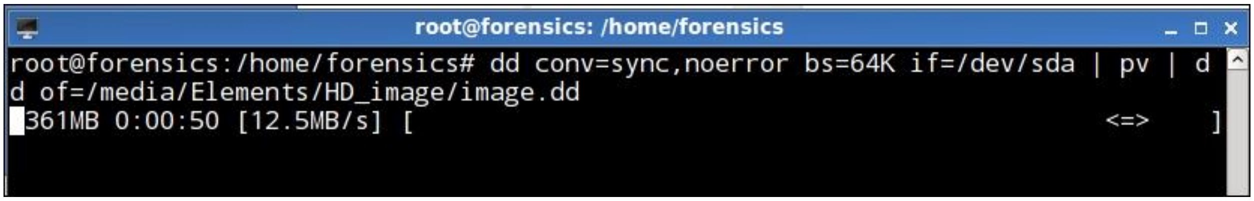


IP Address: 192.168.1.108

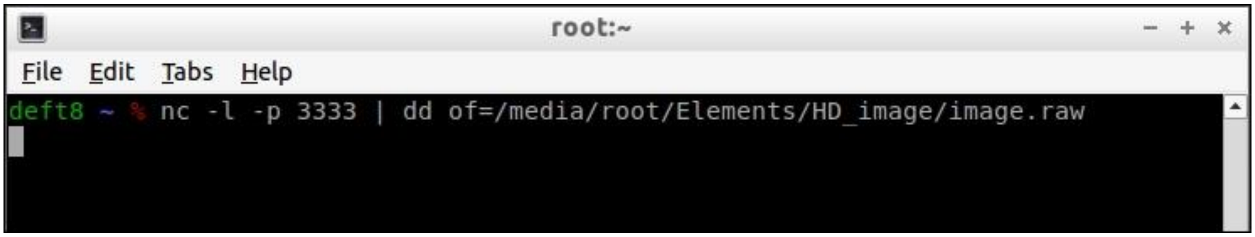
Port: 8888

Password: ********

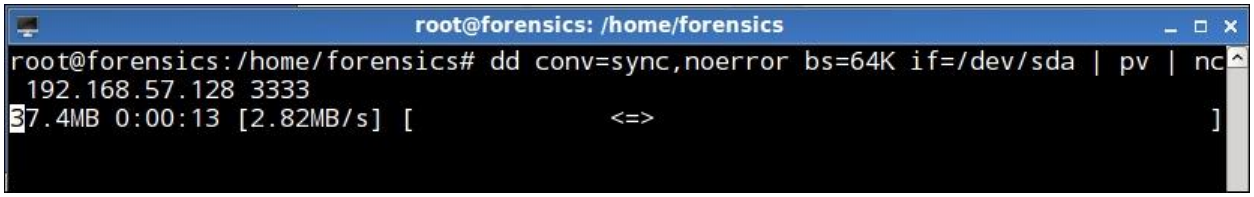
Filename: Output



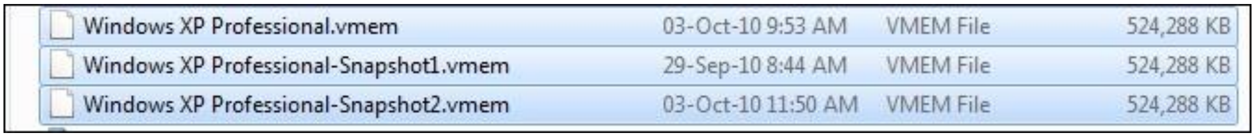
```
root@forensics:/home/forensics# dd conv=sync,noerror bs=64K if=/dev/sda | pv | d
d of=/media/Elements/HD_image/image.dd
█361MB 0:00:50 [12.5MB/s] [                                                 <=>     ]
```



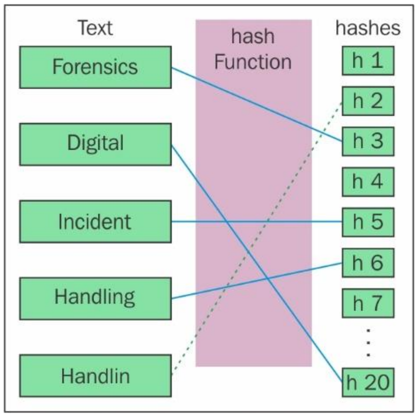
```
deft8 ~ % nc -l -p 3333 | dd of=/media/root/Elements/HD_image/image.raw
```

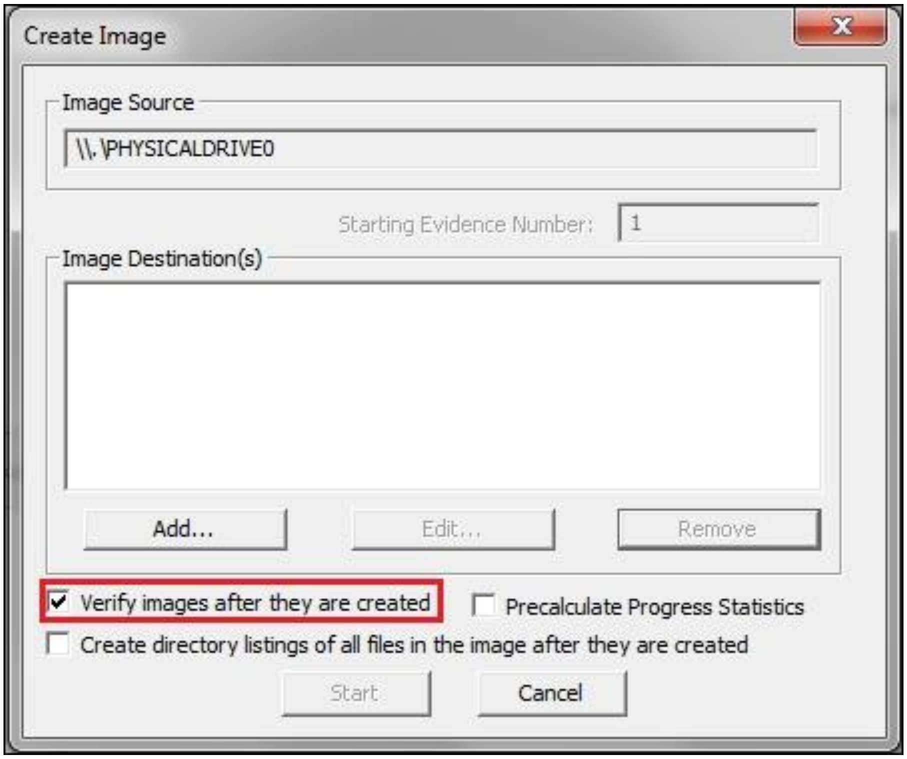


```
root@forensics:/home/forensics# dd conv=sync,noerror bs=64K if=/dev/sda | pv | nc
 192.168.57.128 3333
37.4MB 0:00:13 [2.82MB/s] [          <=>                                      ]
```



Windows XP Professional.vmem	03-Oct-10 9:53 AM	VMEM File	524,288 KB
Windows XP Professional-Snapshot1.vmem	29-Sep-10 8:44 AM	VMEM File	524,288 KB
Windows XP Professional-Snapshot2.vmem	03-Oct-10 11:50 AM	VMEM File	524,288 KB





Create Image

Image Source

\\.\PHYSICALDRIVE0

Starting Evidence Number: 1

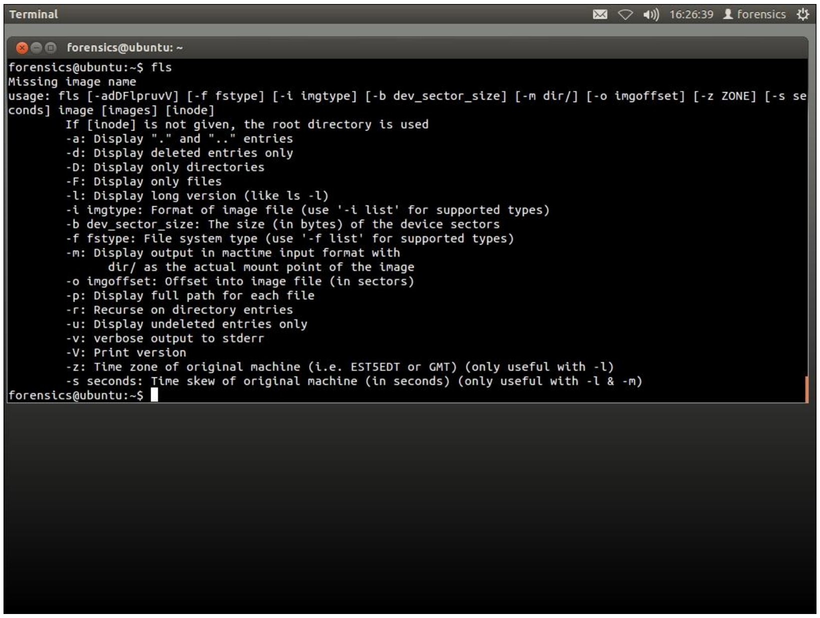
Image Destination(s)

☑ Verify images after they are created

□ Precalculate Progress Statistics

□ Create directory listings of all files in the image after they are created

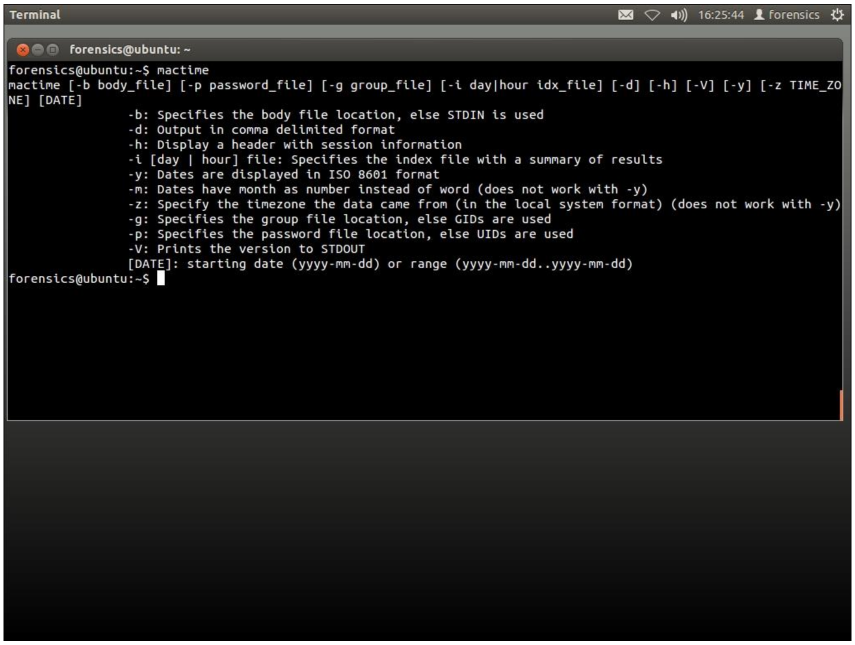
Chapter 5: Timeline



Terminal

forensics@ubuntu: ~

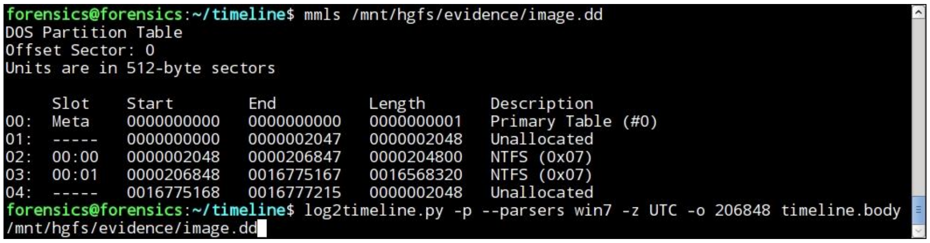
```
forensics@ubuntu:~$ fls
Missing image name
usage: fls [-adDFlpruvV] [-f fstype] [-i imgtype] [-b dev_sector_size] [-m dir/] [-o imgoffset] [-z ZONE] [-s se
conds] image [images] [inode]
        If [inode] is not given, the root directory is used
        -a: Display "." and ".." entries
        -d: Display deleted entries only
        -D: Display only directories
        -F: Display only files
        -l: Display long version (like ls -l)
        -i imgtype: Format of image file (use '-i list' for supported types)
        -b dev_sector_size: The size (in bytes) of the device sectors
        -f fstype: File system type (use '-f list' for supported types)
        -m: Display output in mactime input format with
              dir/ as the actual mount point of the image
        -o imgoffset: Offset into image file (in sectors)
        -p: Display full path for each file
        -r: Recurse on directory entries
        -u: Display undeleted entries only
        -v: verbose output to stderr
        -V: Print version
        -z: Time zone of original machine (i.e. EST5EDT or GMT) (only useful with -l)
        -s seconds: Time skew of original machine (in seconds) (only useful with -l & -m)
forensics@ubuntu:~$ 
```



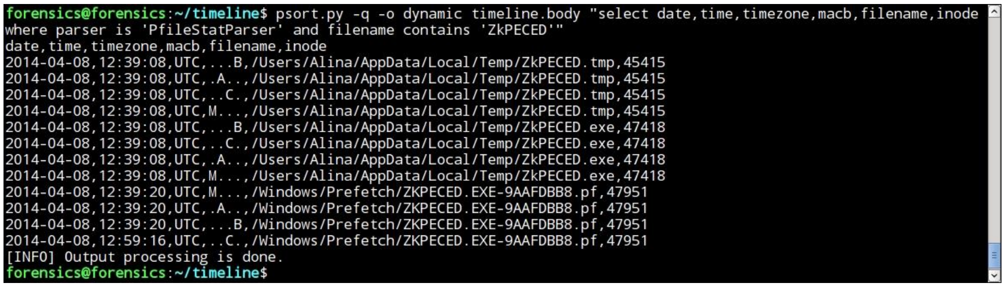
Terminal

forensics@ubuntu: ~

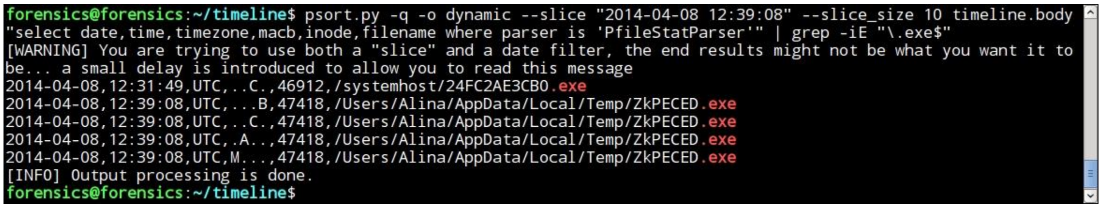
```
forensics@ubuntu:~$ mactime
mactime [-b body_file] [-p password_file] [-g group_file] [-i day|hour idx_file] [-d] [-h] [-V] [-y] [-z TIME_ZO
NE] [DATE]
                -b: Specifies the body file location, else STDIN is used
                -d: Output in comma delimited format
                -h: Display a header with session information
                -i [day | hour] file: Specifies the index file with a summary of results
                -y: Dates are displayed in ISO 8601 format
                -m: Dates have month as number instead of word (does not work with -y)
                -z: Specify the timezone the data came from (in the local system format) (does not work with -y)
                -g: Specifies the group file location, else GIDs are used
                -p: Specifies the password file location, else UIDs are used
                -V: Prints the version to STDOUT
                [DATE]: starting date (yyyy-mm-dd) or range (yyyy-mm-dd..yyyy-mm-dd)
forensics@ubuntu:~$ 
```



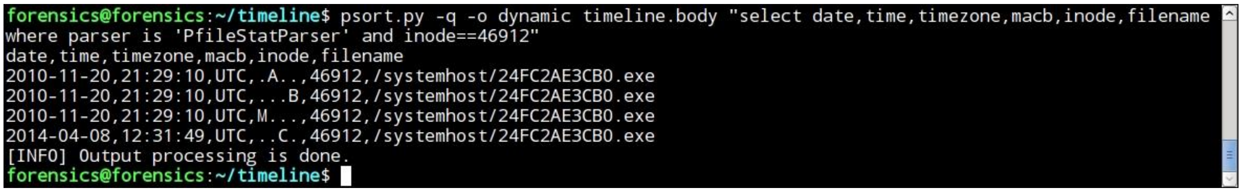
```
forensics@forensics:~/timeline$ mmls /mnt/hgfs/evidence/image.dd
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

     Slot     Start        End          Length       Description
00:  Meta     0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----    0000000000   0000002047   0000002048   Unallocated
02:  00:00    0000002048   0000206847   0000204800   NTFS (0x07)
03:  00:01    0000206848   0016775167   0016568320   NTFS (0x07)
04:  -----    0016775168   0016777215   0000002048   Unallocated
forensics@forensics:~/timeline$ log2timeline.py -p --parsers win7 -z UTC -o 206848 timeline.body
/mnt/hgfs/evidence/image.dd
```



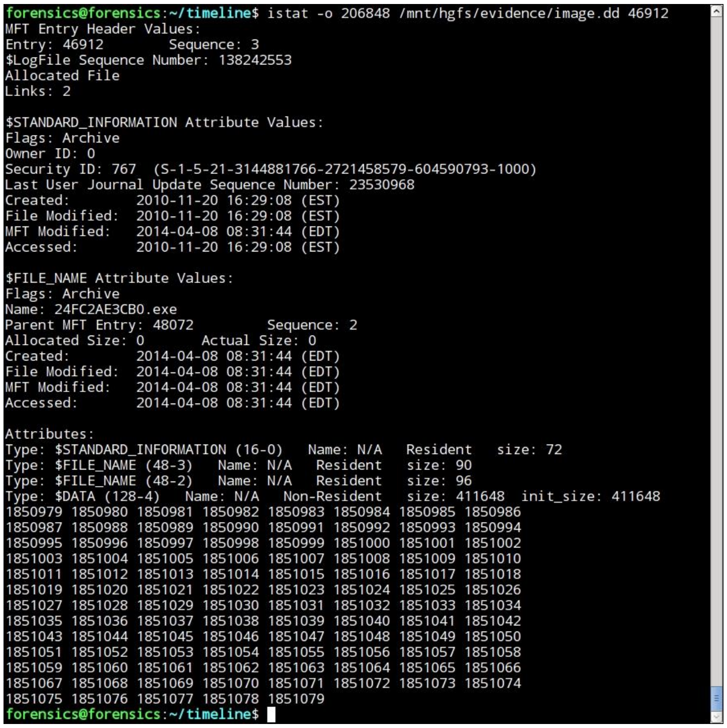
```
forensics@forensics:~/timeline$ psort.py -q -o dynamic timeline.body "select date,time,timezone,macb,filename,inode
where parser is 'PfileStatParser' and filename contains 'ZkPECED'"
date,time,timezone,macb,filename,inode
2014-04-08,12:39:08,UTC,...B,/Users/Alina/AppData/Local/Temp/ZkPECED.tmp,45415
2014-04-08,12:39:08,UTC,.A..,/Users/Alina/AppData/Local/Temp/ZkPECED.tmp,45415
2014-04-08,12:39:08,UTC,..C.,/Users/Alina/AppData/Local/Temp/ZkPECED.tmp,45415
2014-04-08,12:39:08,UTC,M...,/Users/Alina/AppData/Local/Temp/ZkPECED.tmp,45415
2014-04-08,12:39:08,UTC,...B,/Users/Alina/AppData/Local/Temp/ZkPECED.exe,47418
2014-04-08,12:39:08,UTC,..C.,/Users/Alina/AppData/Local/Temp/ZkPECED.exe,47418
2014-04-08,12:39:08,UTC,.A..,/Users/Alina/AppData/Local/Temp/ZkPECED.exe,47418
2014-04-08,12:39:08,UTC,M...,/Users/Alina/AppData/Local/Temp/ZkPECED.exe,47418
2014-04-08,12:39:20,UTC,M...,/Windows/Prefetch/ZKPECED.EXE-9AAFDBB8.pf,47951
2014-04-08,12:39:20,UTC,.A..,/Windows/Prefetch/ZKPECED.EXE-9AAFDBB8.pf,47951
2014-04-08,12:39:20,UTC,...B,/Windows/Prefetch/ZKPECED.EXE-9AAFDBB8.pf,47951
2014-04-08,12:59:16,UTC,..C.,/Windows/Prefetch/ZKPECED.EXE-9AAFDBB8.pf,47951
[INFO] Output processing is done.
forensics@forensics:~/timeline$
```



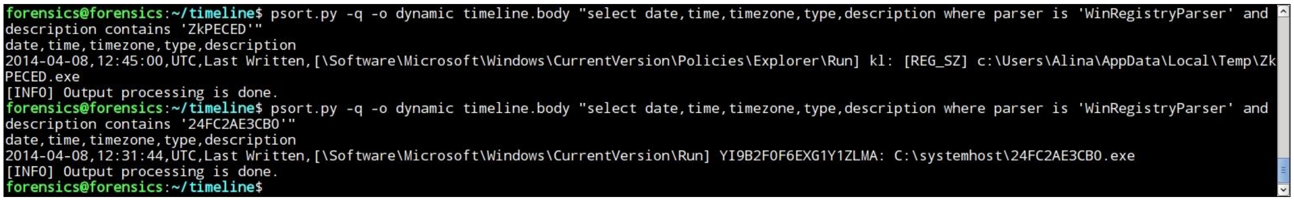
```
forensics@forensics:~/timeline$ psort.py -q -o dynamic --slice "2014-04-08 12:39:08" --slice_size 10 timeline.body
"select date,time,timezone,macb,inode,filename where parser is 'PfileStatParser'" | grep -iE "\.exe$"
[WARNING] You are trying to use both a "slice" and a date filter, the end results might not be what you want it to
be... a small delay is introduced to allow you to read this message
2014-04-08,12:31:49,UTC,..C.,46912,/systemhost/24FC2AE3CB0.exe
2014-04-08,12:39:08,UTC,...B,47418,/Users/Alina/AppData/Local/Temp/ZkPECED.exe
2014-04-08,12:39:08,UTC,..C.,47418,/Users/Alina/AppData/Local/Temp/ZkPECED.exe
2014-04-08,12:39:08,UTC,.A..,47418,/Users/Alina/AppData/Local/Temp/ZkPECED.exe
2014-04-08,12:39:08,UTC,M...,47418,/Users/Alina/AppData/Local/Temp/ZkPECED.exe
[INFO] Output processing is done.
forensics@forensics:~/timeline$
```



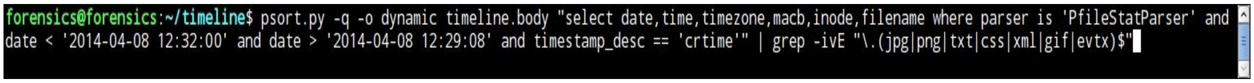
```
forensics@forensics:~/timeline$ psort.py -q -o dynamic timeline.body "select date,time,timezone,macb,inode,filename
where parser is 'PfileStatParser' and inode==46912"
date,time,timezone,macb,inode,filename
2010-11-20,21:29:10,UTC,.A..,46912,/systemhost/24FC2AE3CB0.exe
2010-11-20,21:29:10,UTC,...B,46912,/systemhost/24FC2AE3CB0.exe
2010-11-20,21:29:10,UTC,M...,46912,/systemhost/24FC2AE3CB0.exe
2014-04-08,12:31:49,UTC,..C.,46912,/systemhost/24FC2AE3CB0.exe
[INFO] Output processing is done.
forensics@forensics:~/timeline$
```



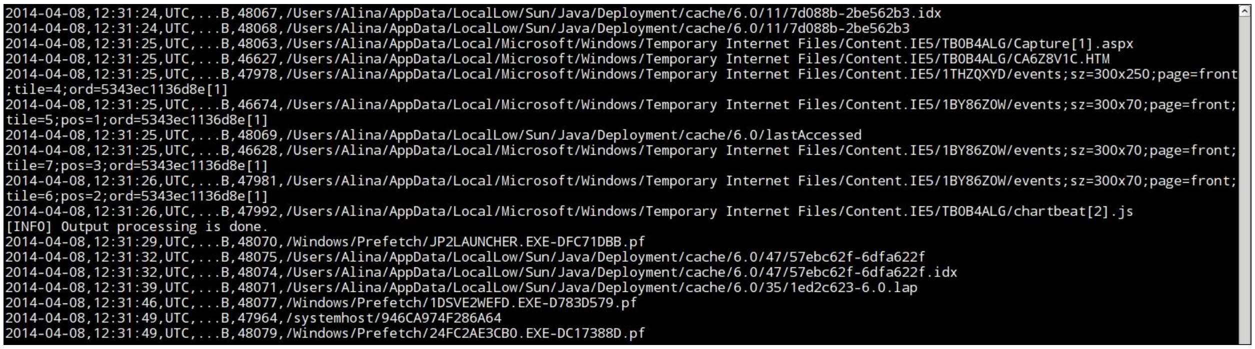
```
forensics@forensics:~/timeline$ istat -o 206848 /mnt/hgfs/evidence/image.dd 46912
MFT Entry Header Values:
Entry: 46912        Sequence: 3
$LogFile Sequence Number: 138242553
Allocated File
Links: 2

$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 767  (S-1-5-21-3144881766-2721458579-604590793-1000)
Last User Journal Update Sequence Number: 23530968
Created:        2010-11-20 16:29:08 (EST)
File Modified:  2010-11-20 16:29:08 (EST)
MFT Modified:   2014-04-08 08:31:44 (EDT)
Accessed:       2010-11-20 16:29:08 (EST)

$FILE_NAME Attribute Values:
Flags: Archive
Name: 24FC2AE3CB0.exe
Parent MFT Entry: 48072         Sequence: 2
Allocated Size: 0       Actual Size: 0
Created:        2014-04-08 08:31:44 (EDT)
File Modified:  2014-04-08 08:31:44 (EDT)
MFT Modified:   2014-04-08 08:31:44 (EDT)
Accessed:       2014-04-08 08:31:44 (EDT)

Attributes:
Type: $STANDARD_INFORMATION (16-0)   Name: N/A   Resident   size: 72
Type: $FILE_NAME (48-3)   Name: N/A   Resident   size: 90
Type: $FILE_NAME (48-2)   Name: N/A   Resident   size: 96
Type: $DATA (128-4)   Name: N/A   Non-Resident   size: 411648  init_size: 411648
1850979 1850980 1850981 1850982 1850983 1850984 1850985 1850986
1850987 1850988 1850989 1850990 1850991 1850992 1850993 1850994
1850995 1850996 1850997 1850998 1850999 1851000 1851001 1851002
1851003 1851004 1851005 1851006 1851007 1851008 1851009 1851010
1851011 1851012 1851013 1851014 1851015 1851016 1851017 1851018
1851019 1851020 1851021 1851022 1851023 1851024 1851025 1851026
1851027 1851028 1851029 1851030 1851031 1851032 1851033 1851034
1851035 1851036 1851037 1851038 1851039 1851040 1851041 1851042
1851043 1851044 1851045 1851046 1851047 1851048 1851049 1851050
1851051 1851052 1851053 1851054 1851055 1851056 1851057 1851058
1851059 1851060 1851061 1851062 1851063 1851064 1851065 1851066
1851067 1851068 1851069 1851070 1851071 1851072 1851073 1851074
1851075 1851076 1851077 1851078 1851079
forensics@forensics:~/timeline$
```



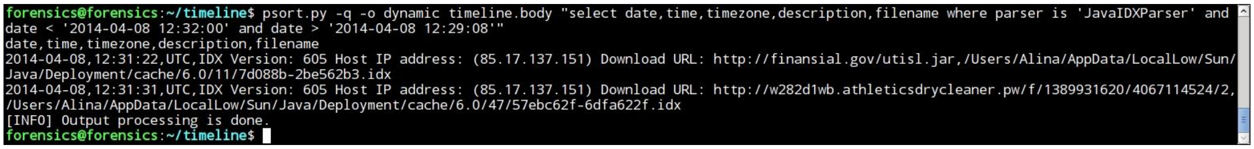
```
forensics@forensics:~/timeline$ psort.py -q -o dynamic timeline.body "select date,time,timezone,type,description where parser is 'WinRegistryParser' and
description contains 'ZkPECED'"
date,time,timezone,type,description
2014-04-08,12:45:00,UTC,Last Written,[\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run] kl: [REG_SZ] c:\Users\Alina\AppData\Local\Temp\Zk
PECED.exe
[INFO] Output processing is done.
forensics@forensics:~/timeline$ psort.py -q -o dynamic timeline.body "select date,time,timezone,type,description where parser is 'WinRegistryParser' and
description contains '24FC2AE3CB0'"
date,time,timezone,type,description
2014-04-08,12:31:44,UTC,Last Written,[\Software\Microsoft\Windows\CurrentVersion\Run] YI9B2F0F6EXG1Y1ZLMA: C:\systemhost\24FC2AE3CB0.exe
[INFO] Output processing is done.
forensics@forensics:~/timeline$
```



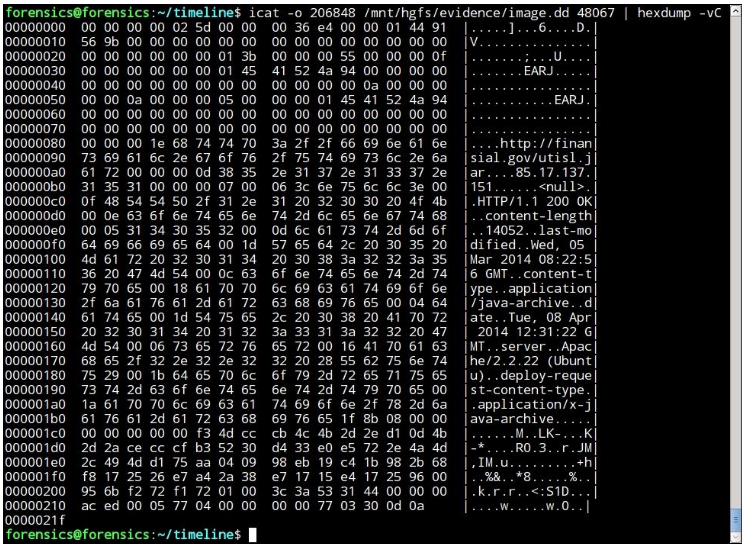
```
forensics@forensics:~/timeline$ psort.py -q -o dynamic timeline.body "select date,time,timezone,macb,inode,filename where parser is 'PfileStatParser' and
date < '2014-04-08 12:32:00' and date > '2014-04-08 12:29:08' and timestamp_desc == 'crtime'" | grep -ivE "\.(jpg|png|txt|css|xml|gif|evtx)$"
```



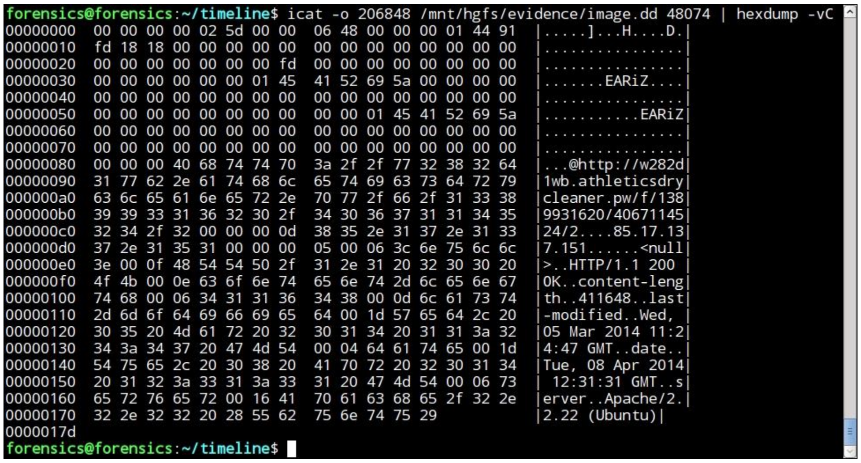
```
2014-04-08,12:31:24,UTC,...B,48067,/Users/Alina/AppData/LocalLow/Sun/Java/Deployment/cache/6.0/11/7d088b-2be562b3.idx
2014-04-08,12:31:24,UTC,...B,48068,/Users/Alina/AppData/LocalLow/Sun/Java/Deployment/cache/6.0/11/7d088b-2be562b3
2014-04-08,12:31:25,UTC,...B,48063,/Users/Alina/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/TB0B4ALG/Capture[1].aspx
2014-04-08,12:31:25,UTC,...B,46627,/Users/Alina/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/TB0B4ALG/CA6Z8V1C.HTM
2014-04-08,12:31:25,UTC,...B,47978,/Users/Alina/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/1THZQXYD/events;sz=300x250;page=front
;tile=4;ord=5343ec1136d8e[1]
2014-04-08,12:31:25,UTC,...B,46674,/Users/Alina/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/1BY86Z0W/events;sz=300x70;page=front;
tile=5;pos=1;ord=5343ec1136d8e[1]
2014-04-08,12:31:25,UTC,...B,48069,/Users/Alina/AppData/LocalLow/Sun/Java/Deployment/cache/6.0/lastAccessed
2014-04-08,12:31:25,UTC,...B,46628,/Users/Alina/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/1BY86Z0W/events;sz=300x70;page=front;
tile=7;pos=3;ord=5343ec1136d8e[1]
2014-04-08,12:31:26,UTC,...B,47981,/Users/Alina/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/1BY86Z0W/events;sz=300x70;page=front;
tile=6;pos=2;ord=5343ec1136d8e[1]
2014-04-08,12:31:26,UTC,...B,47992,/Users/Alina/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/TB0B4ALG/chartbeat[2].js
[INFO] Output processing is done.
2014-04-08,12:31:29,UTC,...B,48070,/Windows/Prefetch/JP2LAUNCHER.EXE-DFC71DBB.pf
2014-04-08,12:31:32,UTC,...B,48075,/Users/Alina/AppData/LocalLow/Sun/Java/Deployment/cache/6.0/47/57ebc62f-6dfa622f
2014-04-08,12:31:32,UTC,...B,48074,/Users/Alina/AppData/LocalLow/Sun/Java/Deployment/cache/6.0/47/57ebc62f-6dfa622f.idx
2014-04-08,12:31:39,UTC,...B,48071,/Users/Alina/AppData/LocalLow/Sun/Java/Deployment/cache/6.0/35/1ed2c623-6.0.lap
2014-04-08,12:31:46,UTC,...B,48077,/Windows/Prefetch/1DSVE2WEFD.EXE-D783D579.pf
2014-04-08,12:31:49,UTC,...B,47964,/systemhost/946CA974F286A64
2014-04-08,12:31:49,UTC,...B,48079,/Windows/Prefetch/24FC2AE3CB0.EXE-DC17388D.pf
```



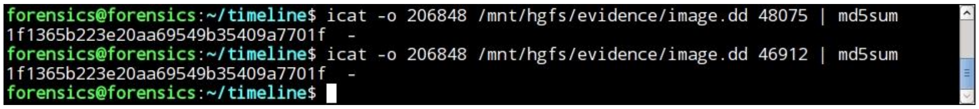
```
forensics@forensics:~/timeline$ psort.py -q -o dynamic timeline.body "select date,time,timezone,description,filename where parser is 'JavaIDXParser' and
date < '2014-04-08 12:32:00' and date > '2014-04-08 12:29:08'"
date,time,timezone,description,filename
2014-04-08,12:31:22,UTC,IDX Version: 605 Host IP address: (85.17.137.151) Download URL: http://finansial.gov/utisl.jar,/Users/Alina/AppData/LocalLow/Sun/
Java/Deployment/cache/6.0/11/7d088b-2be562b3.idx
2014-04-08,12:31:31,UTC,IDX Version: 605 Host IP address: (85.17.137.151) Download URL: http://w282d1wb.athleticsdrycleaner.pw/f/1389931620/4067114524/2,
/Users/Alina/AppData/LocalLow/Sun/Java/Deployment/cache/6.0/47/57ebc62f-6dfa622f.idx
[INFO] Output processing is done.
forensics@forensics:~/timeline$
```



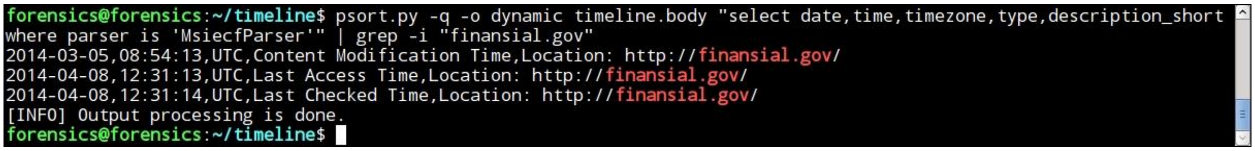
```
forensics@forensics:~/timeline$ icat -o 206848 /mnt/hgfs/evidence/image.dd 48067 | hexdump -vC
00000000  00 00 00 00 02 5d 00 00  00 36 e4 00 00 01 44 91  |.....]...6....D.|
00000010  56 9b 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |V...............|
00000020  00 00 00 00 00 00 01 3b  00 00 00 55 00 00 00 0f  |.......;...U....|
00000030  00 00 00 00 00 00 01 45  41 52 4a 94 00 00 00 00  |.......EARJ.....|
00000040  00 00 00 00 00 00 00 00  00 00 00 00 0a 00 00 00  |................|
00000050  00 00 0a 00 00 00 05 00  00 00 01 45 41 52 4a 94  |...........EARJ.|
00000060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000080  00 00 00 1e 68 74 74 70  3a 2f 2f 66 69 6e 61 6e  |....http://finan|
00000090  73 69 61 6c 2e 67 6f 76  2f 75 74 69 73 6c 2e 6a  |sial.gov/utisl.j|
000000a0  61 72 00 00 00 0d 38 35  2e 31 37 2e 31 33 37 2e  |ar....85.17.137.|
000000b0  31 35 31 00 00 00 07 00  06 3c 6e 75 6c 6c 3e 00  |151......<null>.|
000000c0  0f 48 54 54 50 2f 31 2e  31 20 32 30 30 20 4f 4b  |.HTTP/1.1 200 OK|
000000d0  00 0e 63 6f 6e 74 65 6e  74 2d 6c 65 6e 67 74 68  |..content-length|
000000e0  00 05 31 34 30 35 32 00  0d 6c 61 73 74 2d 6d 6f  |..14052..last-mo|
000000f0  64 69 66 69 65 64 00 1d  57 65 64 2c 20 30 35 20  |dified..Wed, 05 |
00000100  4d 61 72 20 32 30 31 34  20 30 38 3a 32 32 3a 35  |Mar 2014 08:22:5|
00000110  36 20 47 4d 54 00 0c 63  6f 6e 74 65 6e 74 2d 74  |6 GMT..content-t|
00000120  79 70 65 00 18 61 70 70  6c 69 63 61 74 69 6f 6e  |ype..application|
00000130  2f 6a 61 76 61 2d 61 72  63 68 69 76 65 00 04 64  |/java-archive..d|
00000140  61 74 65 00 1d 54 75 65  2c 20 30 38 20 41 70 72  |ate..Tue, 08 Apr|
00000150  20 32 30 31 34 20 31 32  3a 33 31 3a 32 32 20 47  | 2014 12:31:22 G|
00000160  4d 54 00 06 73 65 72 76  65 72 00 16 41 70 61 63  |MT..server..Apac|
00000170  68 65 2f 32 2e 32 2e 32  32 20 28 55 62 75 6e 74  |he/2.2.22 (Ubunt|
00000180  75 29 00 1b 64 65 70 6c  6f 79 2d 72 65 71 75 65  |u)..deploy-reque|
00000190  73 74 2d 63 6f 6e 74 65  6e 74 2d 74 79 70 65 00  |st-content-type.|
000001a0  1a 61 70 70 6c 69 63 61  74 69 6f 6e 2f 78 2d 6a  |.application/x-j|
000001b0  61 76 61 2d 61 72 63 68  69 76 65 1f 8b 08 00 00  |ava-archive.....|
000001c0  00 00 00 00 00 f3 4d cc  cb 4c 4b 2d 2e d1 0d 4b  |......M..LK-...K|
000001d0  2d 2a ce cc cf b3 52 30  d4 33 e0 e5 72 2e 4a 4d  |-*....R0.3..r.JM|
000001e0  2c 49 4d d1 75 aa 04 09  98 eb 19 c4 1b 98 2b 68  |,IM.u.........+h|
000001f0  f8 17 25 26 e7 a4 2a 38  e7 17 15 e4 17 25 96 00  |..%&..*8.....%..|
00000200  95 6b f2 72 f1 72 01 00  3c 3a 53 31 44 00 00 00  |.k.r.r..<:S1D...|
00000210  ac ed 00 05 77 04 00 00  00 00 77 03 30 0d 0a     |....w.....w.0..|
0000021f
forensics@forensics:~/timeline$
```



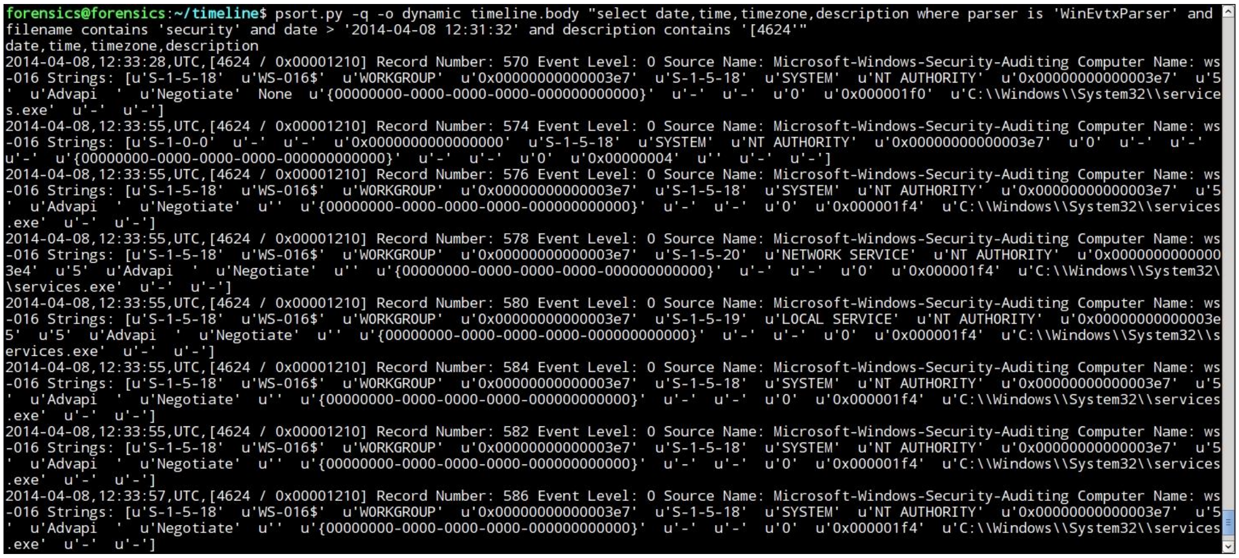
```
forensics@forensics:~/timeline$ icat -o 206848 /mnt/hgfs/evidence/image.dd 48074 | hexdump -vC
00000000  00 00 00 00 02 5d 00 00  06 48 00 00 00 01 44 91  |.....]...H....D.|
00000010  fd 18 18 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000020  00 00 00 00 00 00 00 fd  00 00 00 00 00 00 00 00  |................|
00000030  00 00 00 00 00 00 01 45  41 52 69 5a 00 00 00 00  |.......EARiZ....|
00000040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000050  00 00 00 00 00 00 00 00  00 00 01 45 41 52 69 5a  |...........EARiZ|
00000060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000080  00 00 00 40 68 74 74 70  3a 2f 2f 77 32 38 32 64  |...@http://w282d|
00000090  31 77 62 2e 61 74 68 6c  65 74 69 63 73 64 72 79  |1wb.athleticsdry|
000000a0  63 6c 65 61 6e 65 72 2e  70 77 2f 66 2f 31 33 38  |cleaner.pw/f/138|
000000b0  39 39 33 31 36 32 30 2f  34 30 36 37 31 31 34 35  |9931620/40671145|
000000c0  32 34 2f 32 00 00 00 0d  38 35 2e 31 37 2e 31 33  |24/2....85.17.13|
000000d0  37 2e 31 35 31 00 00 00  05 00 06 3c 6e 75 6c 6c  |7.151......<null|
000000e0  3e 00 0f 48 54 54 50 2f  31 2e 31 20 32 30 30 20  |>..HTTP/1.1 200 |
000000f0  4f 4b 00 0e 63 6f 6e 74  65 6e 74 2d 6c 65 6e 67  |OK..content-leng|
00000100  74 68 00 06 34 31 31 36  34 38 00 0d 6c 61 73 74  |th..411648..last|
00000110  2d 6d 6f 64 69 66 69 65  64 00 1d 57 65 64 2c 20  |-modified..Wed, |
00000120  30 35 20 4d 61 72 20 32  30 31 34 20 31 31 3a 32  |05 Mar 2014 11:2|
00000130  34 3a 34 37 20 47 4d 54  00 04 64 61 74 65 00 1d  |4:47 GMT..date..|
00000140  54 75 65 2c 20 30 38 20  41 70 72 20 32 30 31 34  |Tue, 08 Apr 2014|
00000150  20 31 32 3a 33 31 3a 33  31 20 47 4d 54 00 06 73  | 12:31:31 GMT..s|
00000160  65 72 76 65 72 00 16 41  70 61 63 68 65 2f 32 2e  |erver..Apache/2.|
00000170  32 2e 32 32 20 28 55 62  75 6e 74 75 29           |2.22 (Ubuntu)|
0000017d
forensics@forensics:~/timeline$
```



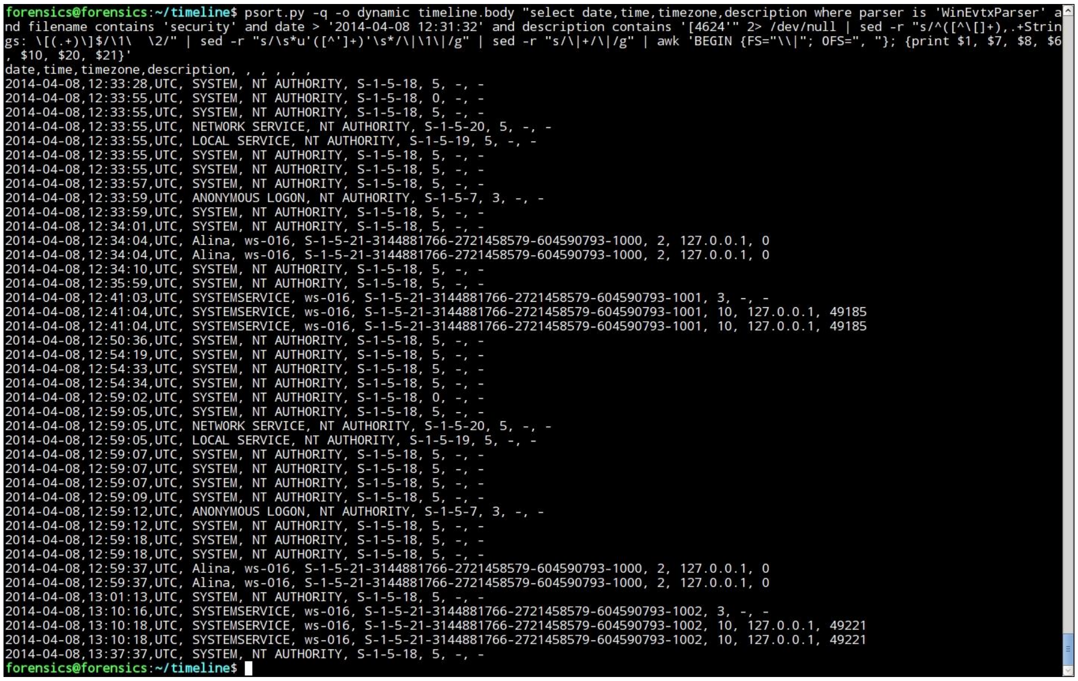
```
forensics@forensics:~/timeline$ icat -o 206848 /mnt/hgfs/evidence/image.dd 48075 | md5sum
1f1365b223e20aa69549b35409a7701f  -
forensics@forensics:~/timeline$ icat -o 206848 /mnt/hgfs/evidence/image.dd 46912 | md5sum
1f1365b223e20aa69549b35409a7701f  -
forensics@forensics:~/timeline$
```



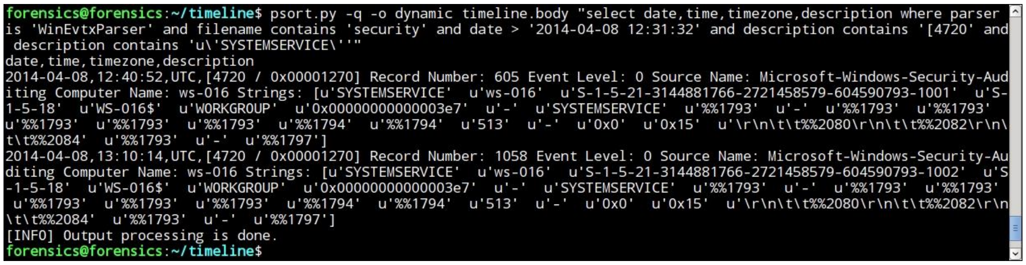
```
forensics@forensics:~/timeline$ psort.py -q -o dynamic timeline.body "select date,time,timezone,type,description_short
where parser is 'MsiecfParser'" | grep -i "finansial.gov"
2014-03-05,08:54:13,UTC,Content Modification Time,Location: http://finansial.gov/
2014-04-08,12:31:13,UTC,Last Access Time,Location: http://finansial.gov/
2014-04-08,12:31:14,UTC,Last Checked Time,Location: http://finansial.gov/
[INFO] Output processing is done.
forensics@forensics:~/timeline$
```



```
forensics@forensics:~/timeline$ psort.py -q -o dynamic timeline.body "select date,time,timezone,description where parser is 'WinEvtxParser' and
filename contains 'security' and date > '2014-04-08 12:31:32' and description contains '[4624'"
date,time,timezone,description
2014-04-08,12:33:28,UTC,[4624 / 0x00001210] Record Number: 570 Event Level: 0 Source Name: Microsoft-Windows-Security-Auditing Computer Name: ws
-016 Strings: [u'S-1-5-18'  u'WS-016$'  u'WORKGROUP'  u'0x00000000000003e7'  u'S-1-5-18'  u'SYSTEM'  u'NT AUTHORITY'  u'0x00000000000003e7'  u'5
'  u'Advapi  '  u'Negotiate'  None  u'{00000000-0000-0000-0000-000000000000}'  u'-'  u'-'  u'0'  u'0x000001f0'  u'C:\\Windows\\System32\\service
s.exe'  u'-'  u'-']
2014-04-08,12:33:55,UTC,[4624 / 0x00001210] Record Number: 574 Event Level: 0 Source Name: Microsoft-Windows-Security-Auditing Computer Name: ws
-016 Strings: [u'S-1-0-0'  u'-'  u'-'  u'0x0000000000000000'  u'S-1-5-18'  u'SYSTEM'  u'NT AUTHORITY'  u'0x00000000000003e7'  u'0'  u'-'  u'-'
u'-'  u'{00000000-0000-0000-0000-000000000000}'  u'-'  u'-'  u'0'  u'0x00000004'  u''  u'-'  u'-']
2014-04-08,12:33:55,UTC,[4624 / 0x00001210] Record Number: 576 Event Level: 0 Source Name: Microsoft-Windows-Security-Auditing Computer Name: ws
-016 Strings: [u'S-1-5-18'  u'WS-016$'  u'WORKGROUP'  u'0x00000000000003e7'  u'S-1-5-18'  u'SYSTEM'  u'NT AUTHORITY'  u'0x00000000000003e7'  u'5
'  u'Advapi  '  u'Negotiate'  u''  u'{00000000-0000-0000-0000-000000000000}'  u'-'  u'-'  u'0'  u'0x000001f4'  u'C:\\Windows\\System32\\services
.exe'  u'-'  u'-']
2014-04-08,12:33:55,UTC,[4624 / 0x00001210] Record Number: 578 Event Level: 0 Source Name: Microsoft-Windows-Security-Auditing Computer Name: ws
-016 Strings: [u'S-1-5-18'  u'WS-016$'  u'WORKGROUP'  u'0x00000000000003e7'  u'S-1-5-20'  u'NETWORK SERVICE'  u'NT AUTHORITY'  u'0x0000000000000
3e4'  u'5'  u'Advapi  '  u'Negotiate'  u''  u'{00000000-0000-0000-0000-000000000000}'  u'-'  u'-'  u'0'  u'0x000001f4'  u'C:\\Windows\\System32\
\services.exe'  u'-'  u'-']
2014-04-08,12:33:55,UTC,[4624 / 0x00001210] Record Number: 580 Event Level: 0 Source Name: Microsoft-Windows-Security-Auditing Computer Name: ws
-016 Strings: [u'S-1-5-18'  u'WS-016$'  u'WORKGROUP'  u'0x00000000000003e7'  u'S-1-5-19'  u'LOCAL SERVICE'  u'NT AUTHORITY'  u'0x00000000000003e
5'  u'5'  u'Advapi  '  u'Negotiate'  u''  u'{00000000-0000-0000-0000-000000000000}'  u'-'  u'-'  u'0'  u'0x000001f4'  u'C:\\Windows\\System32\\s
ervices.exe'  u'-'  u'-']
2014-04-08,12:33:55,UTC,[4624 / 0x00001210] Record Number: 584 Event Level: 0 Source Name: Microsoft-Windows-Security-Auditing Computer Name: ws
-016 Strings: [u'S-1-5-18'  u'WS-016$'  u'WORKGROUP'  u'0x00000000000003e7'  u'S-1-5-18'  u'SYSTEM'  u'NT AUTHORITY'  u'0x00000000000003e7'  u'5
'  u'Advapi  '  u'Negotiate'  u''  u'{00000000-0000-0000-0000-000000000000}'  u'-'  u'-'  u'0'  u'0x000001f4'  u'C:\\Windows\\System32\\services
.exe'  u'-'  u'-']
2014-04-08,12:33:55,UTC,[4624 / 0x00001210] Record Number: 582 Event Level: 0 Source Name: Microsoft-Windows-Security-Auditing Computer Name: ws
-016 Strings: [u'S-1-5-18'  u'WS-016$'  u'WORKGROUP'  u'0x00000000000003e7'  u'S-1-5-18'  u'SYSTEM'  u'NT AUTHORITY'  u'0x00000000000003e7'  u'5
'  u'Advapi  '  u'Negotiate'  u''  u'{00000000-0000-0000-0000-000000000000}'  u'-'  u'-'  u'0'  u'0x000001f4'  u'C:\\Windows\\System32\\services
.exe'  u'-'  u'-']
2014-04-08,12:33:57,UTC,[4624 / 0x00001210] Record Number: 586 Event Level: 0 Source Name: Microsoft-Windows-Security-Auditing Computer Name: ws
-016 Strings: [u'S-1-5-18'  u'WS-016$'  u'WORKGROUP'  u'0x00000000000003e7'  u'S-1-5-18'  u'SYSTEM'  u'NT AUTHORITY'  u'0x00000000000003e7'  u'5
'  u'Advapi  '  u'Negotiate'  u''  u'{00000000-0000-0000-0000-000000000000}'  u'-'  u'-'  u'0'  u'0x000001f4'  u'C:\\Windows\\System32\\services
.exe'  u'-'  u'-']
```

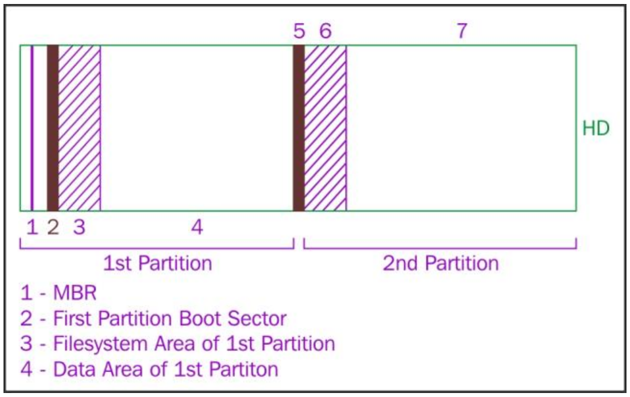


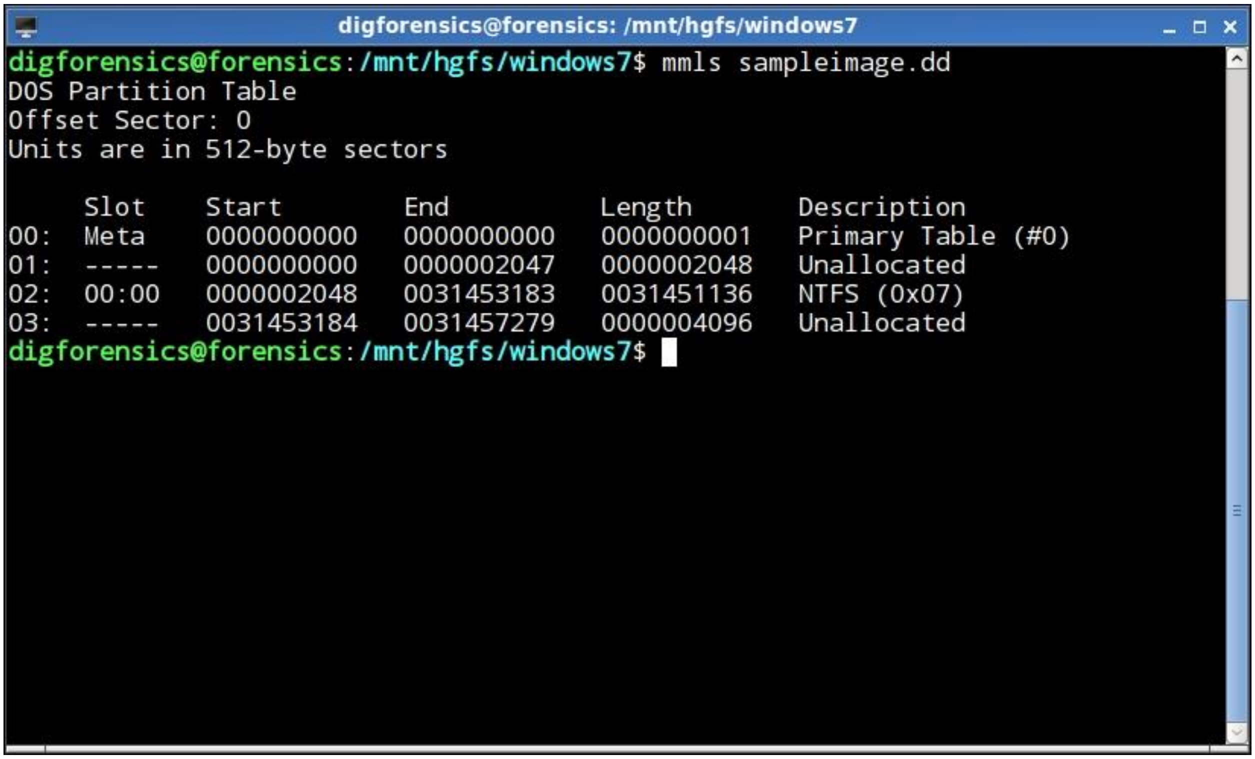
```
forensics@forensics:~/timeline$ psort.py -q -o dynamic timeline.body "select date,time,timezone,description where parser is 'WinEvtxParser' a
nd filename contains 'security' and date > '2014-04-08 12:31:32' and description contains '[4624'" 2> /dev/null | sed -r "s/^([^\[]+),.+Strin
gs: \[(.+)\]$/\1\  \2/" | sed -r "s/\s*u'([^']+)'\s*/\|\1\|/g" | sed -r "s/\|+/\|/g" | awk 'BEGIN {FS="\\|"; OFS=", "}; {print $1, $7, $8, $6
, $10, $20, $21}'
date,time,timezone,description, , , , , ,
2014-04-08,12:33:28,UTC, SYSTEM, NT AUTHORITY, S-1-5-18, 5, -, -
2014-04-08,12:33:55,UTC, SYSTEM, NT AUTHORITY, S-1-5-18, 0, -, -
2014-04-08,12:33:55,UTC, SYSTEM, NT AUTHORITY, S-1-5-18, 5, -, -
2014-04-08,12:33:55,UTC, NETWORK SERVICE, NT AUTHORITY, S-1-5-20, 5, -, -
2014-04-08,12:33:55,UTC, LOCAL SERVICE, NT AUTHORITY, S-1-5-19, 5, -, -
2014-04-08,12:33:55,UTC, SYSTEM, NT AUTHORITY, S-1-5-18, 5, -, -
2014-04-08,12:33:55,UTC, SYSTEM, NT AUTHORITY, S-1-5-18, 5, -, -
2014-04-08,12:33:57,UTC, SYSTEM, NT AUTHORITY, S-1-5-18, 5, -, -
2014-04-08,12:33:59,UTC, ANONYMOUS LOGON, NT AUTHORITY, S-1-5-7, 3, -, -
2014-04-08,12:33:59,UTC, SYSTEM, NT AUTHORITY, S-1-5-18, 5, -, -
2014-04-08,12:34:01,UTC, SYSTEM, NT AUTHORITY, S-1-5-18, 5, -, -
2014-04-08,12:34:04,UTC, Alina, ws-016, S-1-5-21-3144881766-2721458579-604590793-1000, 2, 127.0.0.1, 0
2014-04-08,12:34:04,UTC, Alina, ws-016, S-1-5-21-3144881766-2721458579-604590793-1000, 2, 127.0.0.1, 0
2014-04-08,12:34:10,UTC, SYSTEM, NT AUTHORITY, S-1-5-18, 5, -, -
2014-04-08,12:35:59,UTC, SYSTEM, NT AUTHORITY, S-1-5-18, 5, -, -
2014-04-08,12:41:03,UTC, SYSTEMSERVICE, ws-016, S-1-5-21-3144881766-2721458579-604590793-1001, 3, -, -
2014-04-08,12:41:04,UTC, SYSTEMSERVICE, ws-016, S-1-5-21-3144881766-2721458579-604590793-1001, 10, 127.0.0.1, 49185
2014-04-08,12:41:04,UTC, SYSTEMSERVICE, ws-016, S-1-5-21-3144881766-2721458579-604590793-1001, 10, 127.0.0.1, 49185
2014-04-08,12:50:36,UTC, SYSTEM, NT AUTHORITY, S-1-5-18, 5, -, -
2014-04-08,12:54:19,UTC, SYSTEM, NT AUTHORITY, S-1-5-18, 5, -, -
2014-04-08,12:54:33,UTC, SYSTEM, NT AUTHORITY, S-1-5-18, 5, -, -
2014-04-08,12:54:34,UTC, SYSTEM, NT AUTHORITY, S-1-5-18, 5, -, -
2014-04-08,12:59:02,UTC, SYSTEM, NT AUTHORITY, S-1-5-18, 0, -, -
2014-04-08,12:59:05,UTC, SYSTEM, NT AUTHORITY, S-1-5-18, 5, -, -
2014-04-08,12:59:05,UTC, NETWORK SERVICE, NT AUTHORITY, S-1-5-20, 5, -, -
2014-04-08,12:59:05,UTC, LOCAL SERVICE, NT AUTHORITY, S-1-5-19, 5, -, -
2014-04-08,12:59:07,UTC, SYSTEM, NT AUTHORITY, S-1-5-18, 5, -, -
2014-04-08,12:59:07,UTC, SYSTEM, NT AUTHORITY, S-1-5-18, 5, -, -
2014-04-08,12:59:07,UTC, SYSTEM, NT AUTHORITY, S-1-5-18, 5, -, -
2014-04-08,12:59:09,UTC, SYSTEM, NT AUTHORITY, S-1-5-18, 5, -, -
2014-04-08,12:59:12,UTC, ANONYMOUS LOGON, NT AUTHORITY, S-1-5-7, 3, -, -
2014-04-08,12:59:12,UTC, SYSTEM, NT AUTHORITY, S-1-5-18, 5, -, -
2014-04-08,12:59:18,UTC, SYSTEM, NT AUTHORITY, S-1-5-18, 5, -, -
2014-04-08,12:59:18,UTC, SYSTEM, NT AUTHORITY, S-1-5-18, 5, -, -
2014-04-08,12:59:37,UTC, Alina, ws-016, S-1-5-21-3144881766-2721458579-604590793-1000, 2, 127.0.0.1, 0
2014-04-08,12:59:37,UTC, Alina, ws-016, S-1-5-21-3144881766-2721458579-604590793-1000, 2, 127.0.0.1, 0
2014-04-08,13:01:13,UTC, SYSTEM, NT AUTHORITY, S-1-5-18, 5, -, -
2014-04-08,13:10:16,UTC, SYSTEMSERVICE, ws-016, S-1-5-21-3144881766-2721458579-604590793-1002, 3, -, -
2014-04-08,13:10:18,UTC, SYSTEMSERVICE, ws-016, S-1-5-21-3144881766-2721458579-604590793-1002, 10, 127.0.0.1, 49221
2014-04-08,13:10:18,UTC, SYSTEMSERVICE, ws-016, S-1-5-21-3144881766-2721458579-604590793-1002, 10, 127.0.0.1, 49221
2014-04-08,13:37:37,UTC, SYSTEM, NT AUTHORITY, S-1-5-18, 5, -, -
forensics@forensics:~/timeline$
```



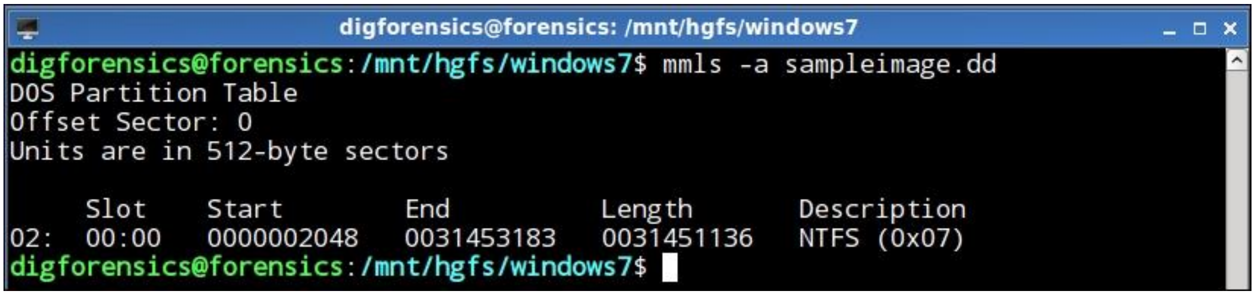
```
forensics@forensics:~/timeline$ psort.py -q -o dynamic timeline.body "select date,time,timezone,description where parser
is 'WinEvtxParser' and filename contains 'security' and date > '2014-04-08 12:31:32' and description contains '[4720' and
 description contains 'u\'SYSTEMSERVICE\''"
date,time,timezone,description
2014-04-08,12:40:52,UTC,[4720 / 0x00001270] Record Number: 605 Event Level: 0 Source Name: Microsoft-Windows-Security-Aud
iting Computer Name: ws-016 Strings: [u'SYSTEMSERVICE'  u'ws-016'  u'S-1-5-21-3144881766-2721458579-604590793-1001'  u'S-
1-5-18'  u'WS-016$'  u'WORKGROUP'  u'0x00000000000003e7'  u'-'  u'SYSTEMSERVICE'  u'%%1793'  u'-'  u'%%1793'  u'%%1793'
u'%%1793'  u'%%1793'  u'%%1793'  u'%%1794'  u'%%1794'  u'513'  u'-'  u'0x0'  u'0x15'  u'\r\n\t\t%%2080\r\n\t\t%%2082\r\n\
t\t%%2084'  u'%%1793'  u'-'  u'%%1797']
2014-04-08,13:10:14,UTC,[4720 / 0x00001270] Record Number: 1058 Event Level: 0 Source Name: Microsoft-Windows-Security-Au
diting Computer Name: ws-016 Strings: [u'SYSTEMSERVICE'  u'ws-016'  u'S-1-5-21-3144881766-2721458579-604590793-1002'  u'S
-1-5-18'  u'WS-016$'  u'WORKGROUP'  u'0x00000000000003e7'  u'-'  u'SYSTEMSERVICE'  u'%%1793'  u'-'  u'%%1793'  u'%%1793'
 u'%%1793'  u'%%1793'  u'%%1793'  u'%%1794'  u'%%1794'  u'513'  u'-'  u'0x0'  u'0x15'  u'\r\n\t\t%%2080\r\n\t\t%%2082\r\n
\t\t%%2084'  u'%%1793'  u'-'  u'%%1797']
[INFO] Output processing is done.
forensics@forensics:~/timeline$
```

Chapter 6: Filesystem Analysis and Data Recovery

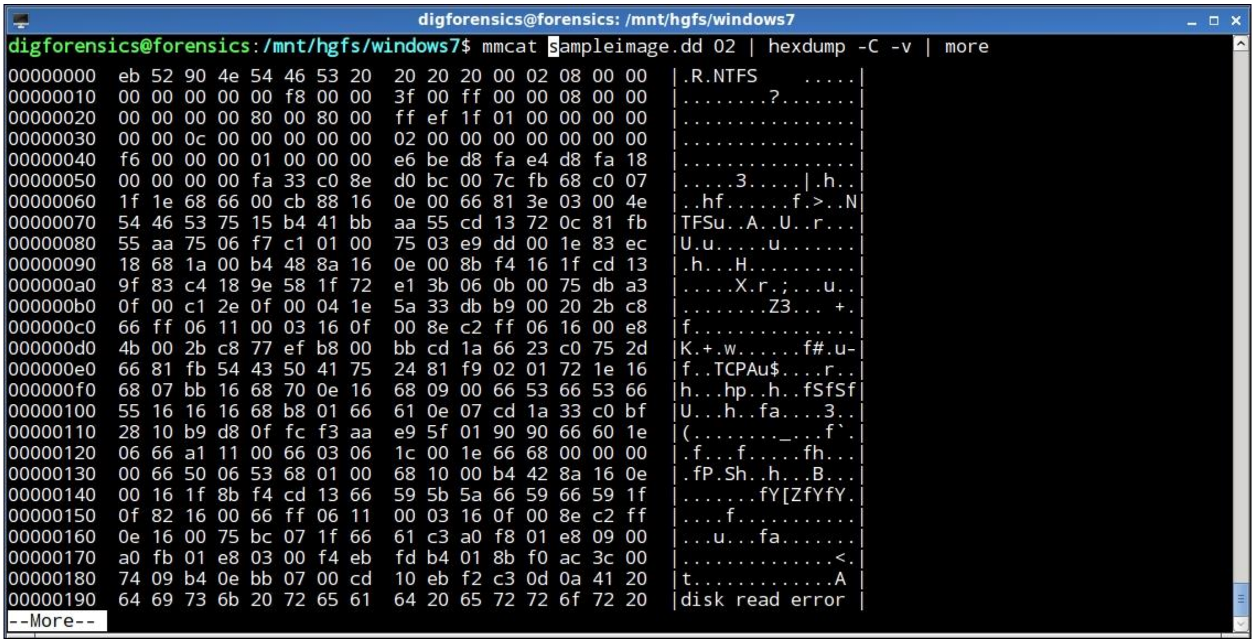

5 6
7
HD
1 2 3
4
1st Partition
2nd Partition
1 - MBR
2 - First Partition Boot Sector
3 - Filesystem Area of 1st Partition
4 - Data Area of 1st Partiton



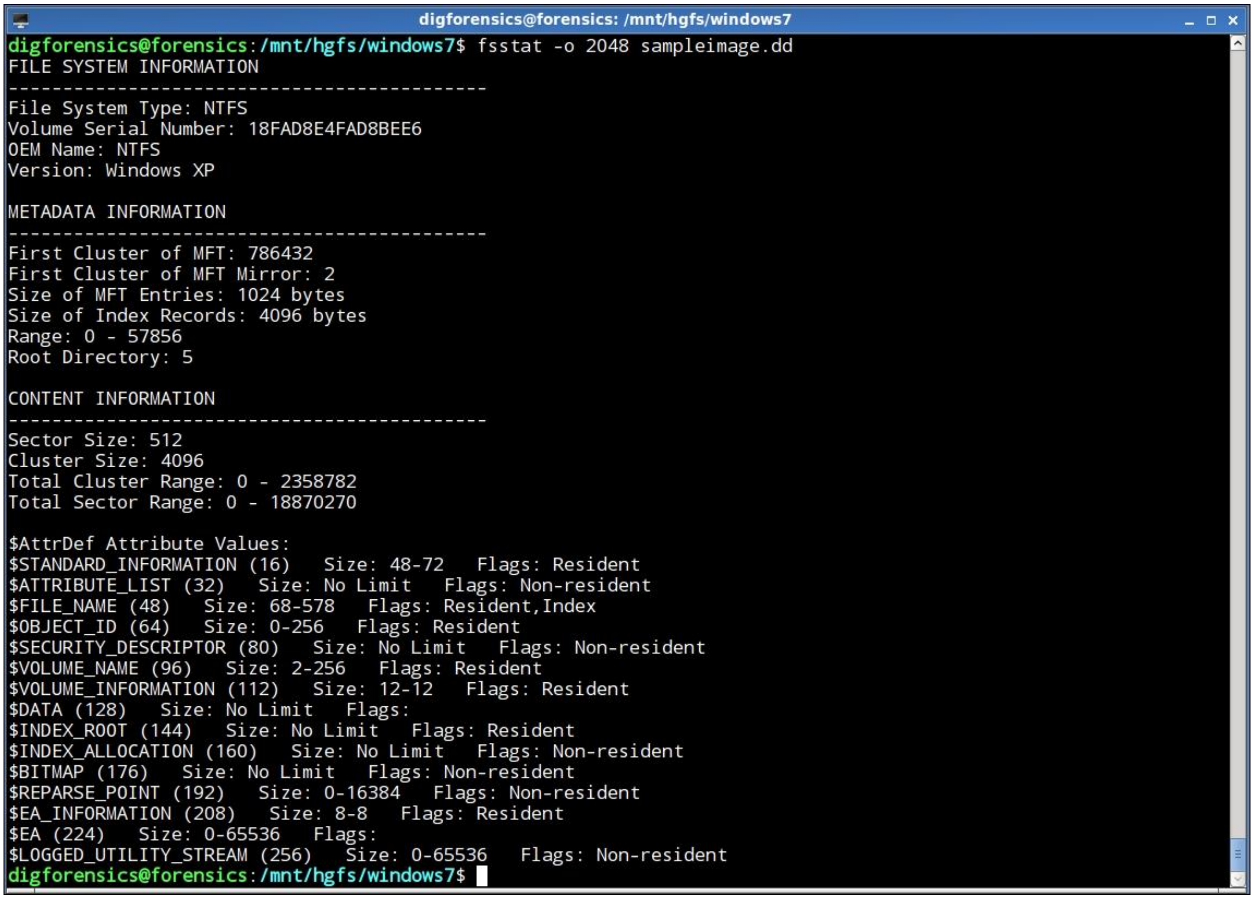
```
digforensics@forensics:/mnt/hgfs/windows7$ mmls sampleimage.dd
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

     Slot     Start        End          Length       Description
00:  Meta     0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----    0000000000   0000002047   0000002048   Unallocated
02:  00:00    0000002048   0031453183   0031451136   NTFS (0x07)
03:  -----    0031453184   0031457279   0000004096   Unallocated
digforensics@forensics:/mnt/hgfs/windows7$
```



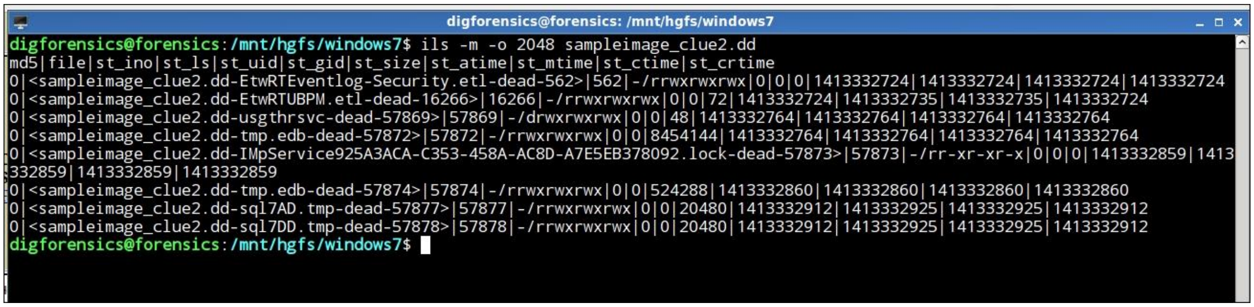
```
digforensics@forensics:/mnt/hgfs/windows7$ mmls -a sampleimage.dd
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

     Slot     Start        End          Length       Description
02:  00:00    0000002048   0031453183   0031451136   NTFS (0x07)
digforensics@forensics:/mnt/hgfs/windows7$
```



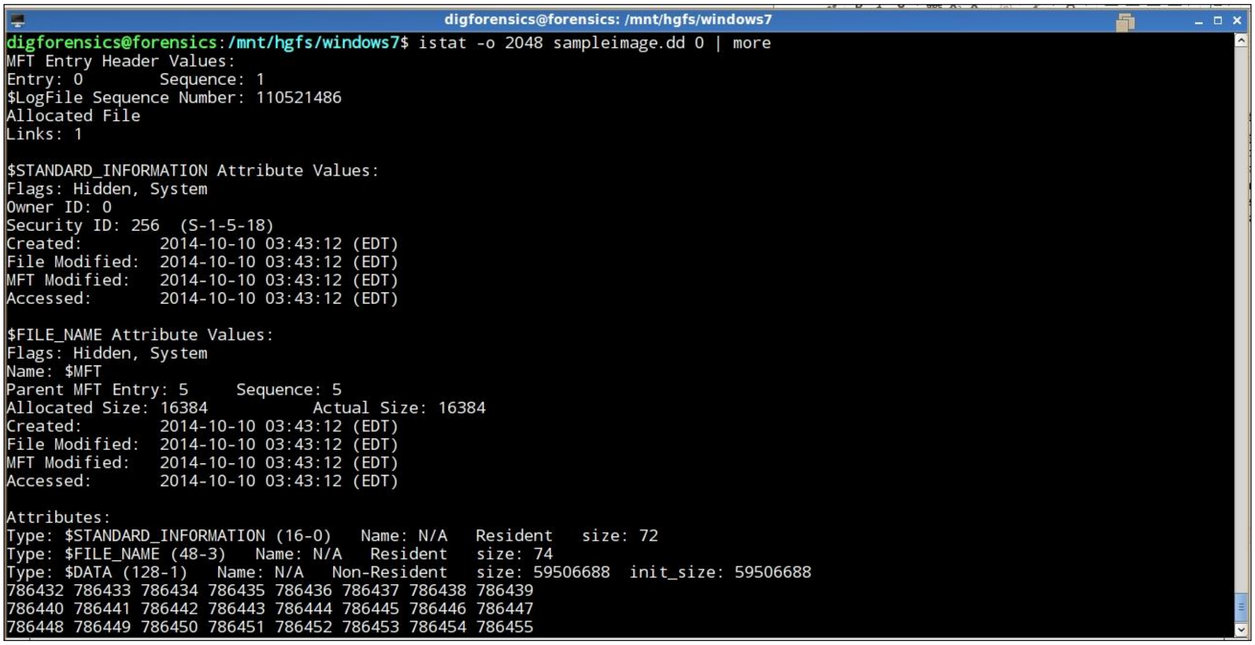
```
digforensics@forensics:/mnt/hgfs/windows7$ mmcat sampleimage.dd 02 | hexdump -C -v | more
00000000  eb 52 90 4e 54 46 53 20  20 20 20 00 02 08 00 00  |.R.NTFS    .....|
00000010  00 00 00 00 00 f8 00 00  3f 00 ff 00 00 08 00 00  |........?.......|
00000020  00 00 00 00 80 00 80 00  ff ef 1f 01 00 00 00 00  |................|
00000030  00 00 0c 00 00 00 00 00  02 00 00 00 00 00 00 00  |................|
00000040  f6 00 00 00 01 00 00 00  e6 be d8 fa e4 d8 fa 18  |................|
00000050  00 00 00 00 fa 33 c0 8e  d0 bc 00 7c fb 68 c0 07  |.....3.....|.h..|
00000060  1f 1e 68 66 00 cb 88 16  0e 00 66 81 3e 03 00 4e  |..hf......f.>..N|
00000070  54 46 53 75 15 b4 41 bb  aa 55 cd 13 72 0c 81 fb  |TFSu..A..U..r...|
00000080  55 aa 75 06 f7 c1 01 00  75 03 e9 dd 00 1e 83 ec  |U.u.....u.......|
00000090  18 68 1a 00 b4 48 8a 16  0e 00 8b f4 16 1f cd 13  |.h...H..........|
000000a0  9f 83 c4 18 9e 58 1f 72  e1 3b 06 0b 00 75 db a3  |.....X.r.;...u..|
000000b0  0f 00 c1 2e 0f 00 04 1e  5a 33 db b9 00 20 2b c8  |........Z3... +.|
000000c0  66 ff 06 11 00 03 16 0f  00 8e c2 ff 06 16 00 e8  |f...............|
000000d0  4b 00 2b c8 77 ef b8 00  bb cd 1a 66 23 c0 75 2d  |K.+.w......f#.u-|
000000e0  66 81 fb 54 43 50 41 75  24 81 f9 02 01 72 1e 16  |f..TCPAu$....r..|
000000f0  68 07 bb 16 68 70 0e 16  68 09 00 66 53 66 53 66  |h...hp..h..fSfSf|
00000100  55 16 16 16 68 b8 01 66  61 0e 07 cd 1a 33 c0 bf  |U...h..fa....3..|
00000110  28 10 b9 d8 0f fc f3 aa  e9 5f 01 90 90 66 60 1e  |(........_...f`.|
00000120  06 66 a1 11 00 66 03 06  1c 00 1e 66 68 00 00 00  |.f...f.....fh...|
00000130  00 66 50 06 53 68 01 00  68 10 00 b4 42 8a 16 0e  |.fP.Sh..h...B...|
00000140  00 16 1f 8b f4 cd 13 66  59 5b 5a 66 59 66 59 1f  |.......fY[ZfYfY.|
00000150  0f 82 16 00 66 ff 06 11  00 03 16 0f 00 8e c2 ff  |....f...........|
00000160  0e 16 00 75 bc 07 1f 66  61 c3 a0 f8 01 e8 09 00  |...u...fa.......|
00000170  a0 fb 01 e8 03 00 f4 eb  fd b4 01 8b f0 ac 3c 00  |..............<.|
00000180  74 09 b4 0e bb 07 00 cd  10 eb f2 c3 0d 0a 41 20  |t.............A |
00000190  64 69 73 6b 20 72 65 61  64 20 65 72 72 6f 72 20  |disk read error |
--More--
```



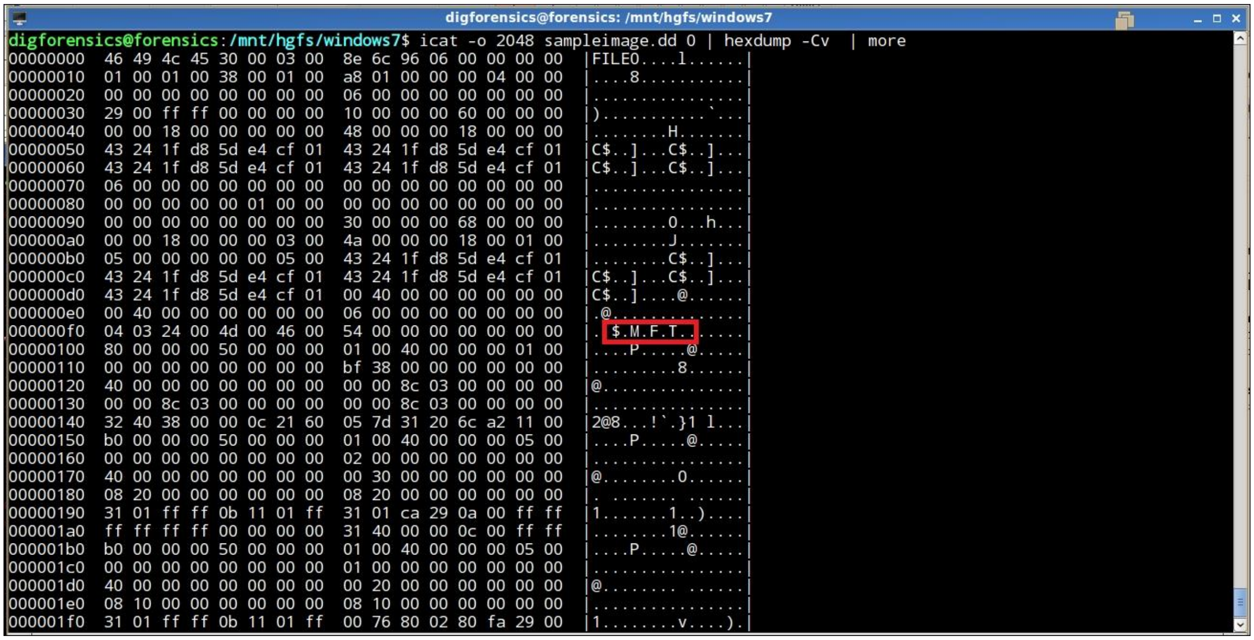
```
digforensics@forensics:/mnt/hgfs/windows7$ fsstat -o 2048 sampleimage.dd
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: NTFS
Volume Serial Number: 18FAD8E4FAD8BEE6
OEM Name: NTFS
Version: Windows XP

METADATA INFORMATION
--------------------------------------------
First Cluster of MFT: 786432
First Cluster of MFT Mirror: 2
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 57856
Root Directory: 5

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 2358782
Total Sector Range: 0 - 18870270

$AttrDef Attribute Values:
$STANDARD_INFORMATION (16)   Size: 48-72   Flags: Resident
$ATTRIBUTE_LIST (32)   Size: No Limit   Flags: Non-resident
$FILE_NAME (48)   Size: 68-578   Flags: Resident,Index
$OBJECT_ID (64)   Size: 0-256   Flags: Resident
$SECURITY_DESCRIPTOR (80)   Size: No Limit   Flags: Non-resident
$VOLUME_NAME (96)   Size: 2-256   Flags: Resident
$VOLUME_INFORMATION (112)   Size: 12-12   Flags: Resident
$DATA (128)   Size: No Limit   Flags:
$INDEX_ROOT (144)   Size: No Limit   Flags: Resident
$INDEX_ALLOCATION (160)   Size: No Limit   Flags: Non-resident
$BITMAP (176)   Size: No Limit   Flags: Non-resident
$REPARSE_POINT (192)   Size: 0-16384   Flags: Non-resident
$EA_INFORMATION (208)   Size: 8-8   Flags: Resident
$EA (224)   Size: 0-65536   Flags:
$LOGGED_UTILITY_STREAM (256)   Size: 0-65536   Flags: Non-resident
digforensics@forensics:/mnt/hgfs/windows7$
```



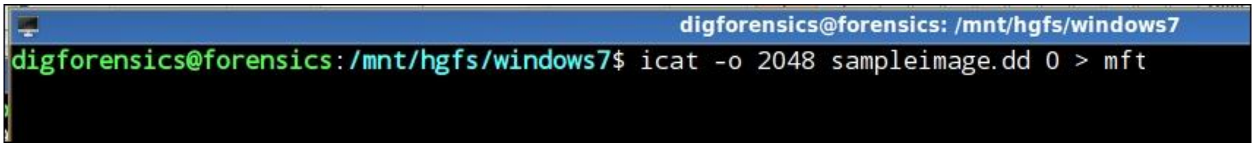
```
digforensics@forensics:/mnt/hgfs/windows7$ ils -m -o 2048 sampleimage_clue2.dd
md5|file|st_ino|st_ls|st_uid|st_gid|st_size|st_atime|st_mtime|st_ctime|st_crtime
0|<sampleimage_clue2.dd-EtwRTEventlog-Security.etl-dead-562>|562|-/rrwxrwxrwx|0|0|0|1413332724|1413332724|1413332724|1413332724
0|<sampleimage_clue2.dd-EtwRTUBPM.etl-dead-16266>|16266|-/rrwxrwxrwx|0|0|72|1413332724|1413332735|1413332735|1413332724
0|<sampleimage_clue2.dd-usgthrsvc-dead-57869>|57869|-/drwxrwxrwx|0|0|48|1413332764|1413332764|1413332764|1413332764
0|<sampleimage_clue2.dd-tmp.edb-dead-57872>|57872|-/rrwxrwxrwx|0|0|8454144|1413332764|1413332764|1413332764|1413332764
0|<sampleimage_clue2.dd-IMpService925A3ACA-C353-458A-AC8D-A7E5EB378092.lock-dead-57873>|57873|-/rr-xr-xr-x|0|0|0|1413332859|1413
332859|1413332859|1413332859
0|<sampleimage_clue2.dd-tmp.edb-dead-57874>|57874|-/rrwxrwxrwx|0|0|524288|1413332860|1413332860|1413332860|1413332860
0|<sampleimage_clue2.dd-sql7AD.tmp-dead-57877>|57877|-/rrwxrwxrwx|0|0|20480|1413332912|1413332925|1413332925|1413332912
0|<sampleimage_clue2.dd-sql7DD.tmp-dead-57878>|57878|-/rrwxrwxrwx|0|0|20480|1413332912|1413332925|1413332925|1413332912
digforensics@forensics:/mnt/hgfs/windows7$
```



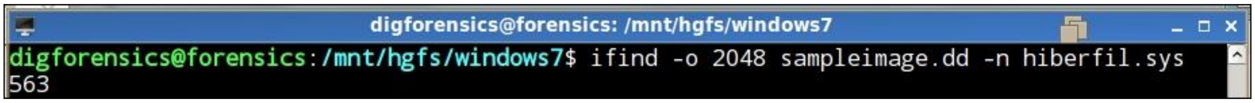
```
digforensics@forensics:/mnt/hgfs/windows7$ istat -o 2048 sampleimage.dd 0 | more
MFT Entry Header Values:
Entry: 0        Sequence: 1
$LogFile Sequence Number: 110521486
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 256  (S-1-5-18)
Created:        2014-10-10 03:43:12 (EDT)
File Modified:  2014-10-10 03:43:12 (EDT)
MFT Modified:   2014-10-10 03:43:12 (EDT)
Accessed:       2014-10-10 03:43:12 (EDT)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $MFT
Parent MFT Entry: 5     Sequence: 5
Allocated Size: 16384          Actual Size: 16384
Created:        2014-10-10 03:43:12 (EDT)
File Modified:  2014-10-10 03:43:12 (EDT)
MFT Modified:   2014-10-10 03:43:12 (EDT)
Accessed:       2014-10-10 03:43:12 (EDT)

Attributes:
Type: $STANDARD_INFORMATION (16-0)   Name: N/A   Resident   size: 72
Type: $FILE_NAME (48-3)   Name: N/A   Resident   size: 74
Type: $DATA (128-1)   Name: N/A   Non-Resident   size: 59506688  init_size: 59506688
786432 786433 786434 786435 786436 786437 786438 786439
786440 786441 786442 786443 786444 786445 786446 786447
786448 786449 786450 786451 786452 786453 786454 786455
```



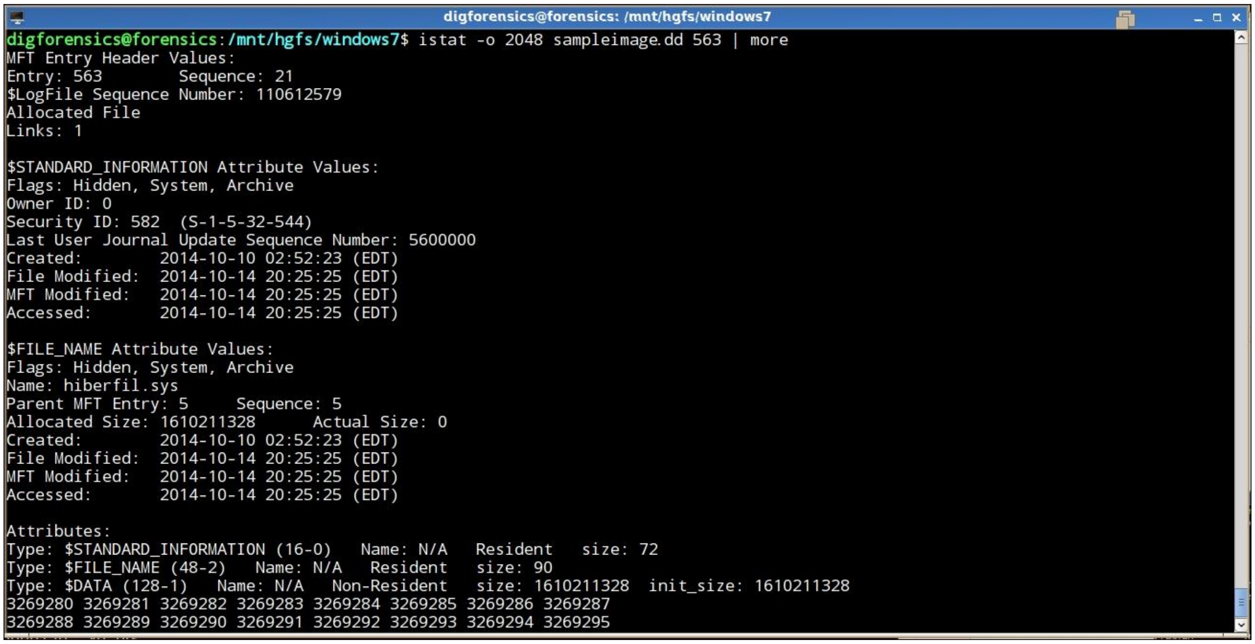
```
digforensics@forensics:/mnt/hgfs/windows7$ icat -o 2048 sampleimage.dd 0 | hexdump -Cv  | more
00000000  46 49 4c 45 30 00 03 00  8e 6c 96 06 00 00 00 00  |FILE0....l......|
00000010  01 00 01 00 38 00 01 00  a8 01 00 00 00 04 00 00  |....8...........|
00000020  00 00 00 00 00 00 00 00  06 00 00 00 00 00 00 00  |................|
00000030  29 00 ff ff 00 00 00 00  10 00 00 00 60 00 00 00  |)...........`...|
00000040  00 00 18 00 00 00 00 00  48 00 00 00 18 00 00 00  |........H.......|
00000050  43 24 1f d8 5d e4 cf 01  43 24 1f d8 5d e4 cf 01  |C$..]...C$..]...|
00000060  43 24 1f d8 5d e4 cf 01  43 24 1f d8 5d e4 cf 01  |C$..]...C$..]...|
00000070  06 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000080  00 00 00 00 00 01 00 00  00 00 00 00 00 00 00 00  |................|
00000090  00 00 00 00 00 00 00 00  30 00 00 00 68 00 00 00  |........0...h...|
000000a0  00 00 18 00 00 00 03 00  4a 00 00 00 18 00 01 00  |........J.......|
000000b0  05 00 00 00 00 00 05 00  43 24 1f d8 5d e4 cf 01  |........C$..]...|
000000c0  43 24 1f d8 5d e4 cf 01  43 24 1f d8 5d e4 cf 01  |C$..]...C$..]...|
000000d0  43 24 1f d8 5d e4 cf 01  00 40 00 00 00 00 00 00  |C$..]....@......|
000000e0  00 40 00 00 00 00 00 00  06 00 00 00 00 00 00 00  |.@..............|
000000f0  04 03 24 00 4d 00 46 00  54 00 00 00 00 00 00 00  |..$.M.F.T.......|
00000100  80 00 00 00 50 00 00 00  01 00 40 00 00 00 01 00  |....P.....@.....|
00000110  00 00 00 00 00 00 00 00  bf 38 00 00 00 00 00 00  |.........8......|
00000120  40 00 00 00 00 00 00 00  00 00 8c 03 00 00 00 00  |@...............|
00000130  00 00 8c 03 00 00 00 00  00 00 8c 03 00 00 00 00  |................|
00000140  32 40 38 00 00 0c 21 60  05 7d 31 20 6c a2 11 00  |2@8...!`.}1 l...|
00000150  b0 00 00 00 50 00 00 00  01 00 40 00 00 00 05 00  |....P.....@.....|
00000160  00 00 00 00 00 00 00 00  02 00 00 00 00 00 00 00  |................|
00000170  40 00 00 00 00 00 00 00  00 30 00 00 00 00 00 00  |@........0......|
00000180  08 20 00 00 00 00 00 00  08 20 00 00 00 00 00 00  |. ....... ......|
00000190  31 01 ff ff 0b 11 01 ff  31 01 ca 29 0a 00 ff ff  |1.......1..)....|
000001a0  ff ff ff ff 00 00 00 00  31 40 00 00 0c 00 ff ff  |........1@......|
000001b0  b0 00 00 00 50 00 00 00  01 00 40 00 00 00 05 00  |....P.....@.....|
000001c0  00 00 00 00 00 00 00 00  01 00 00 00 00 00 00 00  |................|
000001d0  40 00 00 00 00 00 00 00  00 20 00 00 00 00 00 00  |@........ ......|
000001e0  08 10 00 00 00 00 00 00  08 10 00 00 00 00 00 00  |................|
000001f0  31 01 ff ff 0b 11 01 ff  00 76 80 02 80 fa 29 00  |1........v....).|
```



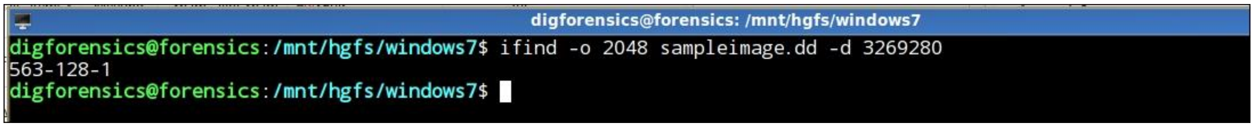
```
digforensics@forensics:/mnt/hgfs/windows7$ icat -o 2048 sampleimage.dd 0 > mft
```



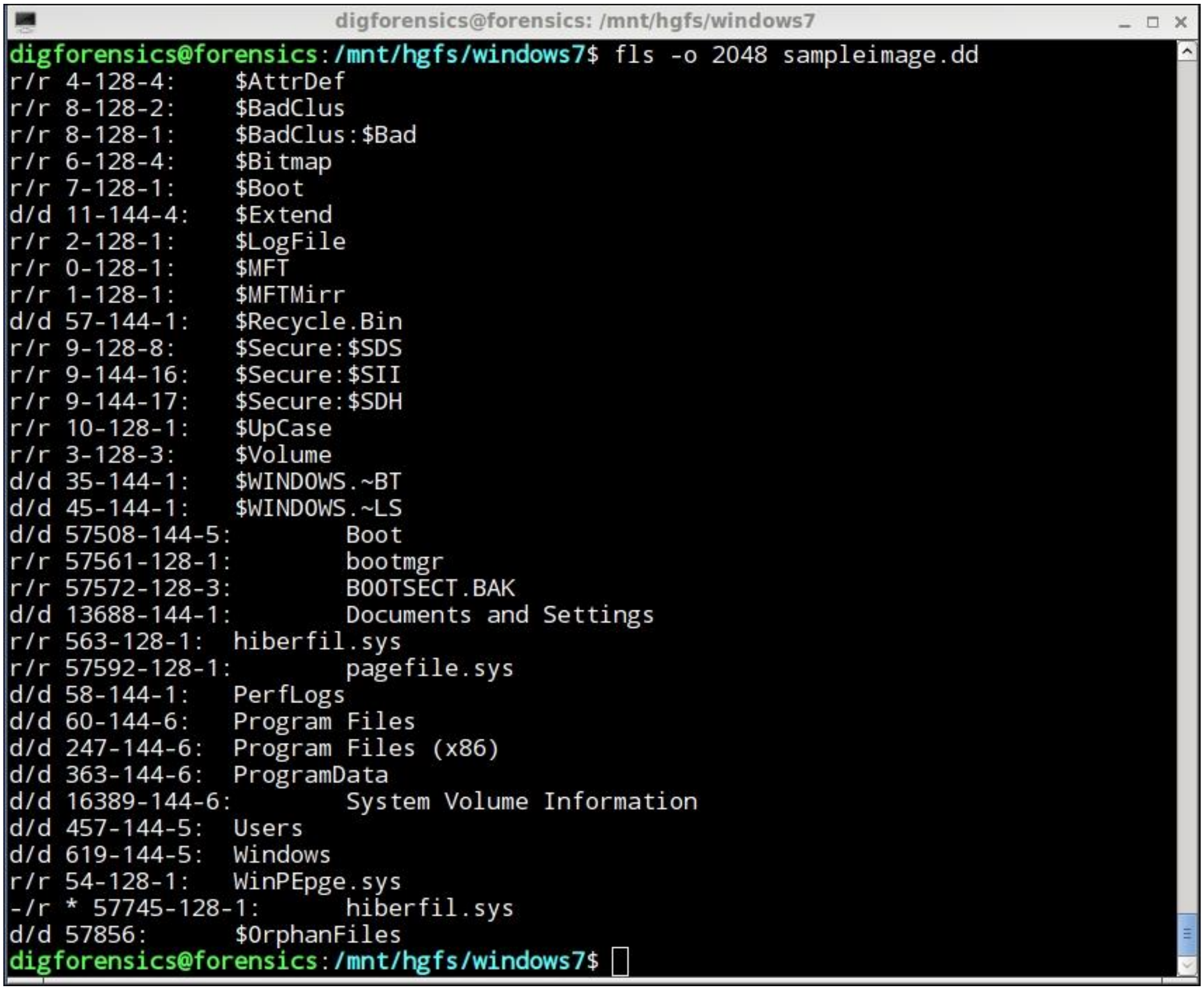
```
digforensics@forensics:/mnt/hgfs/windows7$ ifind -o 2048 sampleimage.dd -n hiberfil.sys
563
```



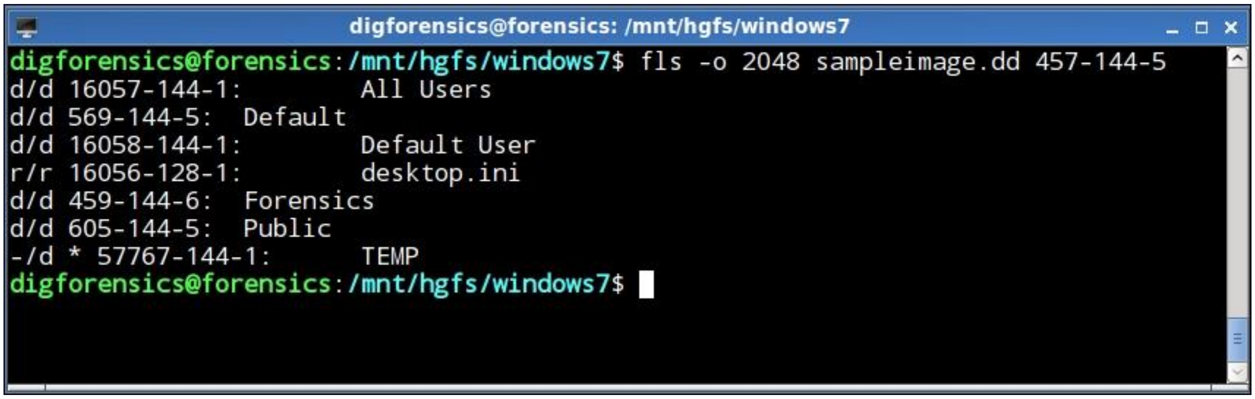
```
digforensics@forensics:/mnt/hgfs/windows7$ istat -o 2048 sampleimage.dd 563 | more
MFT Entry Header Values:
Entry: 563        Sequence: 21
$LogFile Sequence Number: 110612579
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System, Archive
Owner ID: 0
Security ID: 582  (S-1-5-32-544)
Last User Journal Update Sequence Number: 5600000
Created:        2014-10-10 02:52:23 (EDT)
File Modified:  2014-10-14 20:25:25 (EDT)
MFT Modified:   2014-10-14 20:25:25 (EDT)
Accessed:       2014-10-14 20:25:25 (EDT)

$FILE_NAME Attribute Values:
Flags: Hidden, System, Archive
Name: hiberfil.sys
Parent MFT Entry: 5     Sequence: 5
Allocated Size: 1610211328      Actual Size: 0
Created:        2014-10-10 02:52:23 (EDT)
File Modified:  2014-10-14 20:25:25 (EDT)
MFT Modified:   2014-10-14 20:25:25 (EDT)
Accessed:       2014-10-14 20:25:25 (EDT)

Attributes:
Type: $STANDARD_INFORMATION (16-0)   Name: N/A   Resident   size: 72
Type: $FILE_NAME (48-2)   Name: N/A   Resident   size: 90
Type: $DATA (128-1)   Name: N/A   Non-Resident   size: 1610211328  init_size: 1610211328
3269280 3269281 3269282 3269283 3269284 3269285 3269286 3269287
3269288 3269289 3269290 3269291 3269292 3269293 3269294 3269295
```



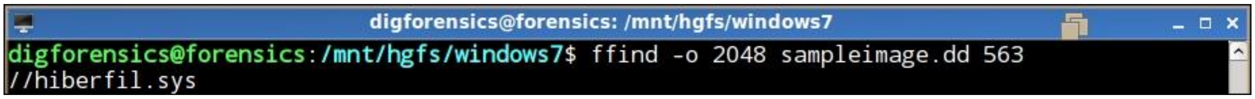
```
digforensics@forensics:/mnt/hgfs/windows7$ ifind -o 2048 sampleimage.dd -d 3269280
563-128-1
digforensics@forensics:/mnt/hgfs/windows7$ 
```



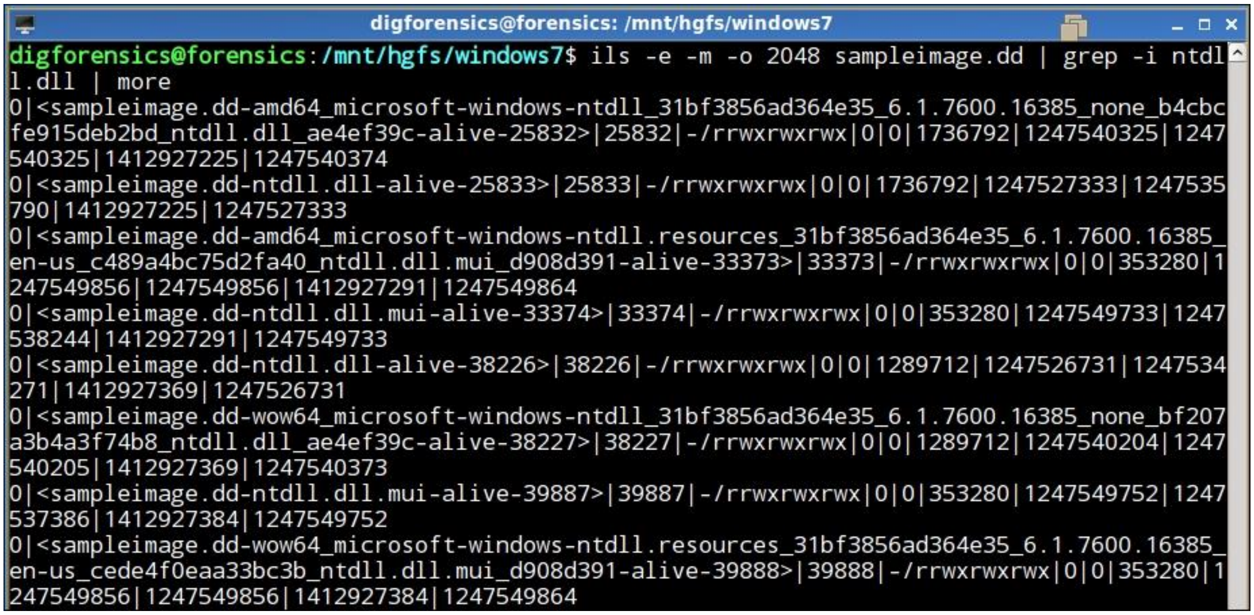
```
digforensics@forensics:/mnt/hgfs/windows7$ fls -o 2048 sampleimage.dd
r/r 4-128-4:    $AttrDef
r/r 8-128-2:    $BadClus
r/r 8-128-1:    $BadClus:$Bad
r/r 6-128-4:    $Bitmap
r/r 7-128-1:    $Boot
d/d 11-144-4:   $Extend
r/r 2-128-1:    $LogFile
r/r 0-128-1:    $MFT
r/r 1-128-1:    $MFTMirr
d/d 57-144-1:   $Recycle.Bin
r/r 9-128-8:    $Secure:$SDS
r/r 9-144-16:   $Secure:$SII
r/r 9-144-17:   $Secure:$SDH
r/r 10-128-1:   $UpCase
r/r 3-128-3:    $Volume
d/d 35-144-1:   $WINDOWS.~BT
d/d 45-144-1:   $WINDOWS.~LS
d/d 57508-144-5:        Boot
r/r 57561-128-1:        bootmgr
r/r 57572-128-3:        BOOTSECT.BAK
d/d 13688-144-1:        Documents and Settings
r/r 563-128-1:  hiberfil.sys
r/r 57592-128-1:        pagefile.sys
d/d 58-144-1:   PerfLogs
d/d 60-144-6:   Program Files
d/d 247-144-6:  Program Files (x86)
d/d 363-144-6:  ProgramData
d/d 16389-144-6:        System Volume Information
d/d 457-144-5:  Users
d/d 619-144-5:  Windows
r/r 54-128-1:   WinPEpge.sys
-/r * 57745-128-1:      hiberfil.sys
d/d 57856:      $OrphanFiles
digforensics@forensics:/mnt/hgfs/windows7$
```



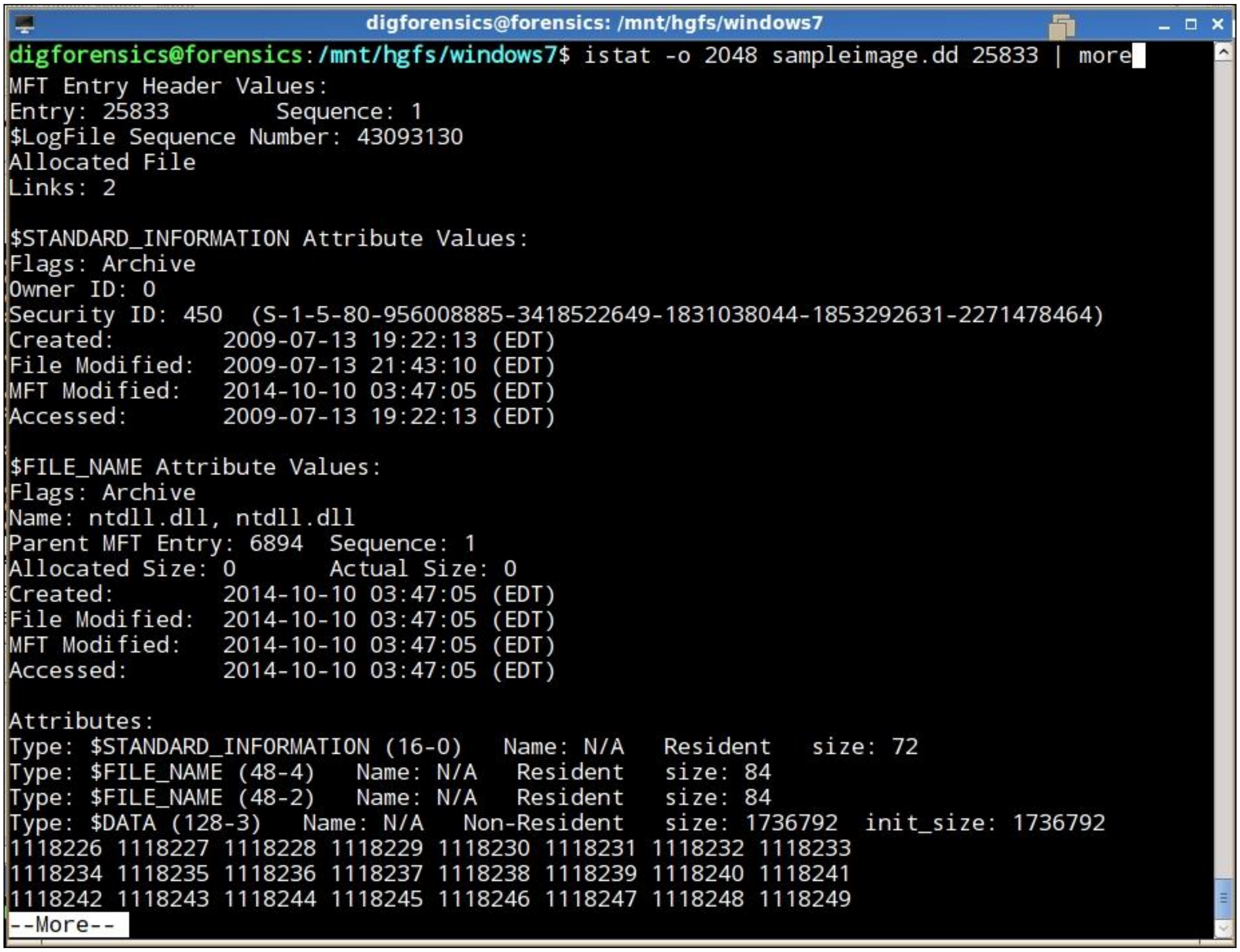
```
digforensics@forensics:/mnt/hgfs/windows7$ fls -o 2048 sampleimage.dd 457-144-5
d/d 16057-144-1:        All Users
d/d 569-144-5:  Default
d/d 16058-144-1:        Default User
r/r 16056-128-1:        desktop.ini
d/d 459-144-6:  Forensics
d/d 605-144-5:  Public
-/d * 57767-144-1:      TEMP
digforensics@forensics:/mnt/hgfs/windows7$
```



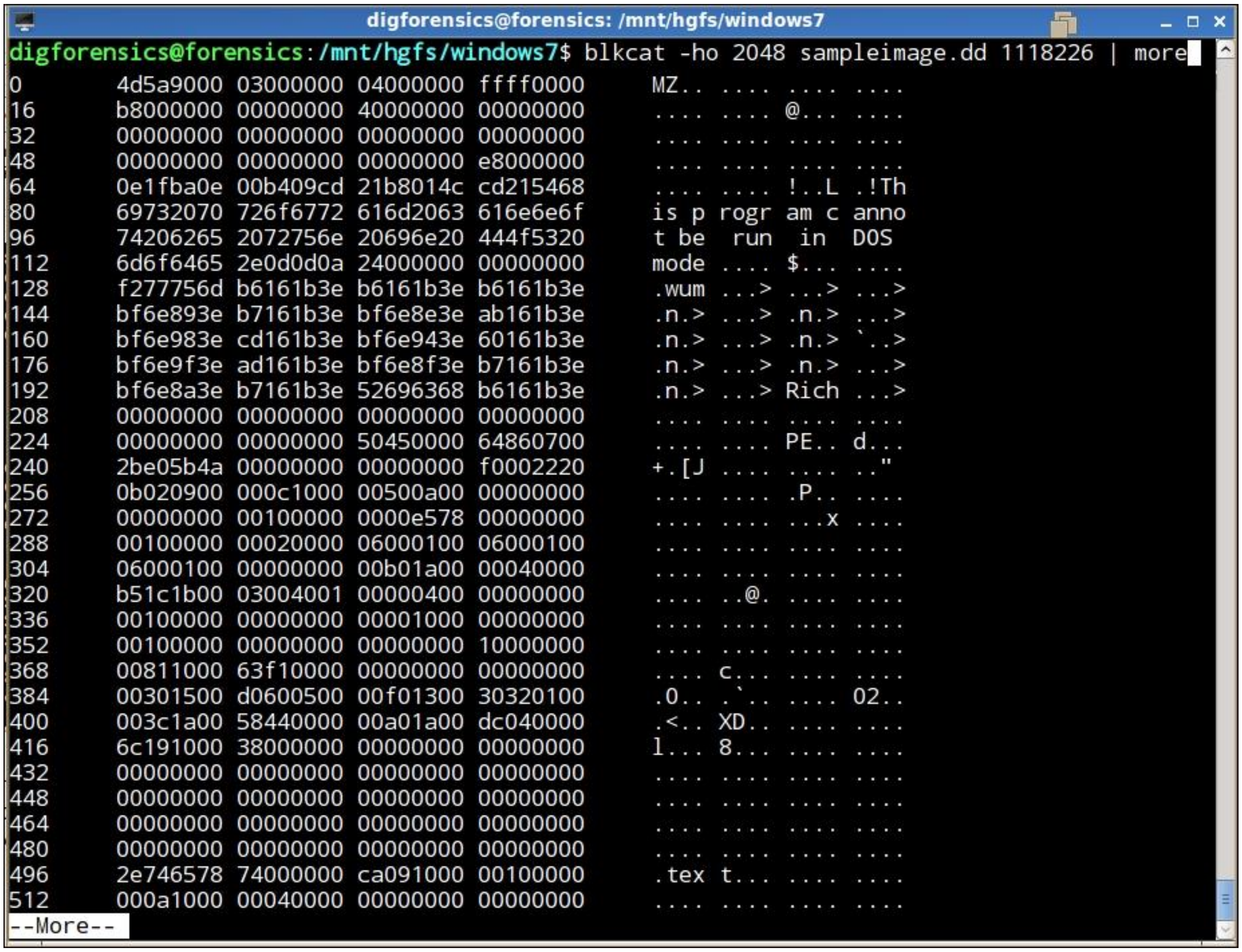
```
digforensics@forensics:/mnt/hgfs/windows7$ ffind -o 2048 sampleimage.dd 563
//hiberfil.sys
```



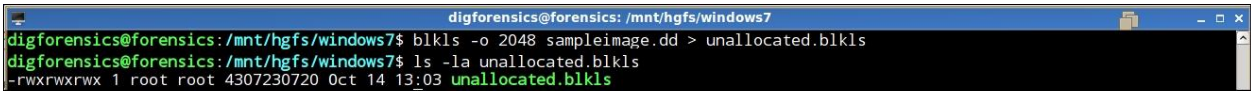
```
digforensics@forensics:/mnt/hgfs/windows7$ ils -e -m -o 2048 sampleimage.dd | grep -i ntdl
l.dll | more
0|<sampleimage.dd-amd64_microsoft-windows-ntdll_31bf3856ad364e35_6.1.7600.16385_none_b4cbc
fe915deb2bd_ntdll.dll_ae4ef39c-alive-25832>|25832|-/rrwxrwxrwx|0|0|1736792|1247540325|1247
540325|1412927225|1247540374
0|<sampleimage.dd-ntdll.dll-alive-25833>|25833|-/rrwxrwxrwx|0|0|1736792|1247527333|1247535
790|1412927225|1247527333
0|<sampleimage.dd-amd64_microsoft-windows-ntdll.resources_31bf3856ad364e35_6.1.7600.16385_
en-us_c489a4bc75d2fa40_ntdll.dll.mui_d908d391-alive-33373>|33373|-/rrwxrwxrwx|0|0|353280|1
247549856|1247549856|1412927291|1247549864
0|<sampleimage.dd-ntdll.dll.mui-alive-33374>|33374|-/rrwxrwxrwx|0|0|353280|1247549733|1247
538244|1412927291|1247549733
0|<sampleimage.dd-ntdll.dll-alive-38226>|38226|-/rrwxrwxrwx|0|0|1289712|1247526731|1247534
271|1412927369|1247526731
0|<sampleimage.dd-wow64_microsoft-windows-ntdll_31bf3856ad364e35_6.1.7600.16385_none_bf207
a3b4a3f74b8_ntdll.dll_ae4ef39c-alive-38227>|38227|-/rrwxrwxrwx|0|0|1289712|1247540204|1247
540205|1412927369|1247540373
0|<sampleimage.dd-ntdll.dll.mui-alive-39887>|39887|-/rrwxrwxrwx|0|0|353280|1247549752|1247
537386|1412927384|1247549752
0|<sampleimage.dd-wow64_microsoft-windows-ntdll.resources_31bf3856ad364e35_6.1.7600.16385_
en-us_cede4f0eaa33bc3b_ntdll.dll.mui_d908d391-alive-39888>|39888|-/rrwxrwxrwx|0|0|353280|1
247549856|1247549856|1412927384|1247549864
```



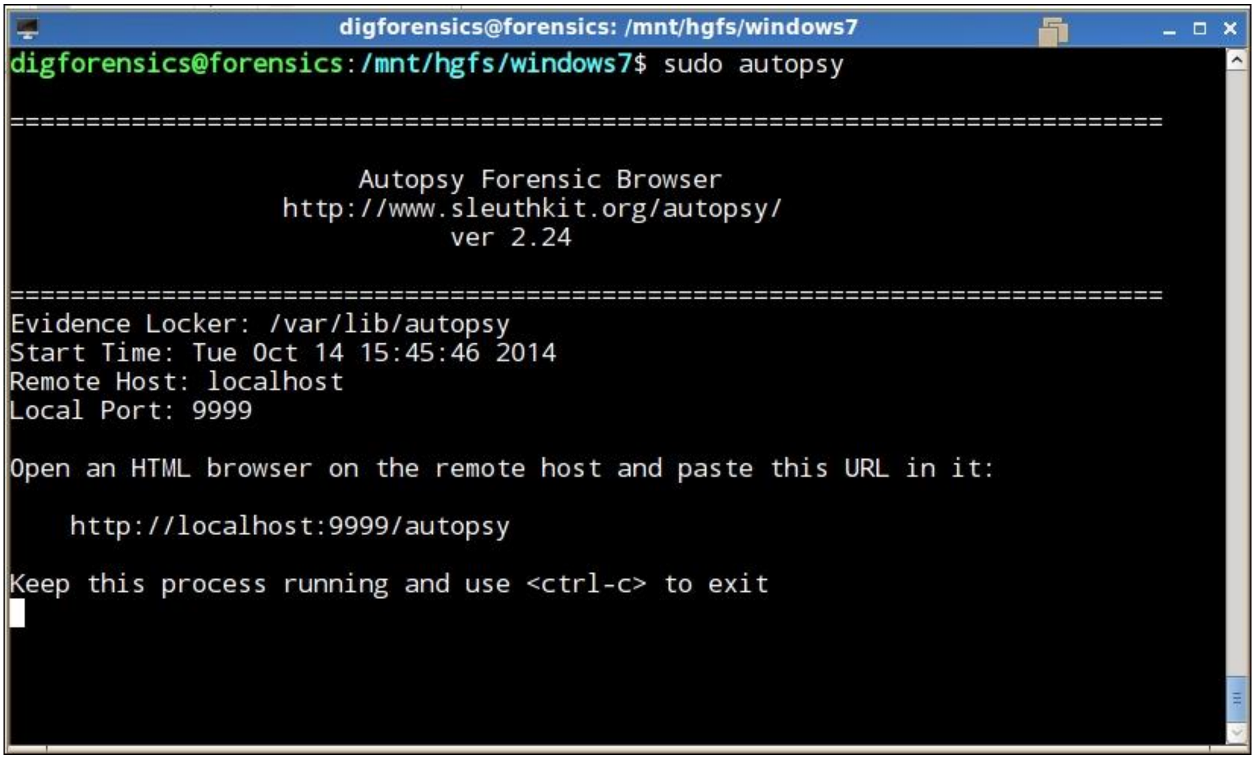
```
digforensics@forensics:/mnt/hgfs/windows7$ istat -o 2048 sampleimage.dd 25833 | more
MFT Entry Header Values:
Entry: 25833        Sequence: 1
$LogFile Sequence Number: 43093130
Allocated File
Links: 2

$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 450  (S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464)
Created:        2009-07-13 19:22:13 (EDT)
File Modified:  2009-07-13 21:43:10 (EDT)
MFT Modified:   2014-10-10 03:47:05 (EDT)
Accessed:       2009-07-13 19:22:13 (EDT)

$FILE_NAME Attribute Values:
Flags: Archive
Name: ntdll.dll, ntdll.dll
Parent MFT Entry: 6894  Sequence: 1
Allocated Size: 0       Actual Size: 0
Created:        2014-10-10 03:47:05 (EDT)
File Modified:  2014-10-10 03:47:05 (EDT)
MFT Modified:   2014-10-10 03:47:05 (EDT)
Accessed:       2014-10-10 03:47:05 (EDT)

Attributes:
Type: $STANDARD_INFORMATION (16-0)   Name: N/A   Resident   size: 72
Type: $FILE_NAME (48-4)   Name: N/A   Resident   size: 84
Type: $FILE_NAME (48-2)   Name: N/A   Resident   size: 84
Type: $DATA (128-3)   Name: N/A   Non-Resident   size: 1736792  init_size: 1736792
1118226 1118227 1118228 1118229 1118230 1118231 1118232 1118233
1118234 1118235 1118236 1118237 1118238 1118239 1118240 1118241
1118242 1118243 1118244 1118245 1118246 1118247 1118248 1118249
--More--
```



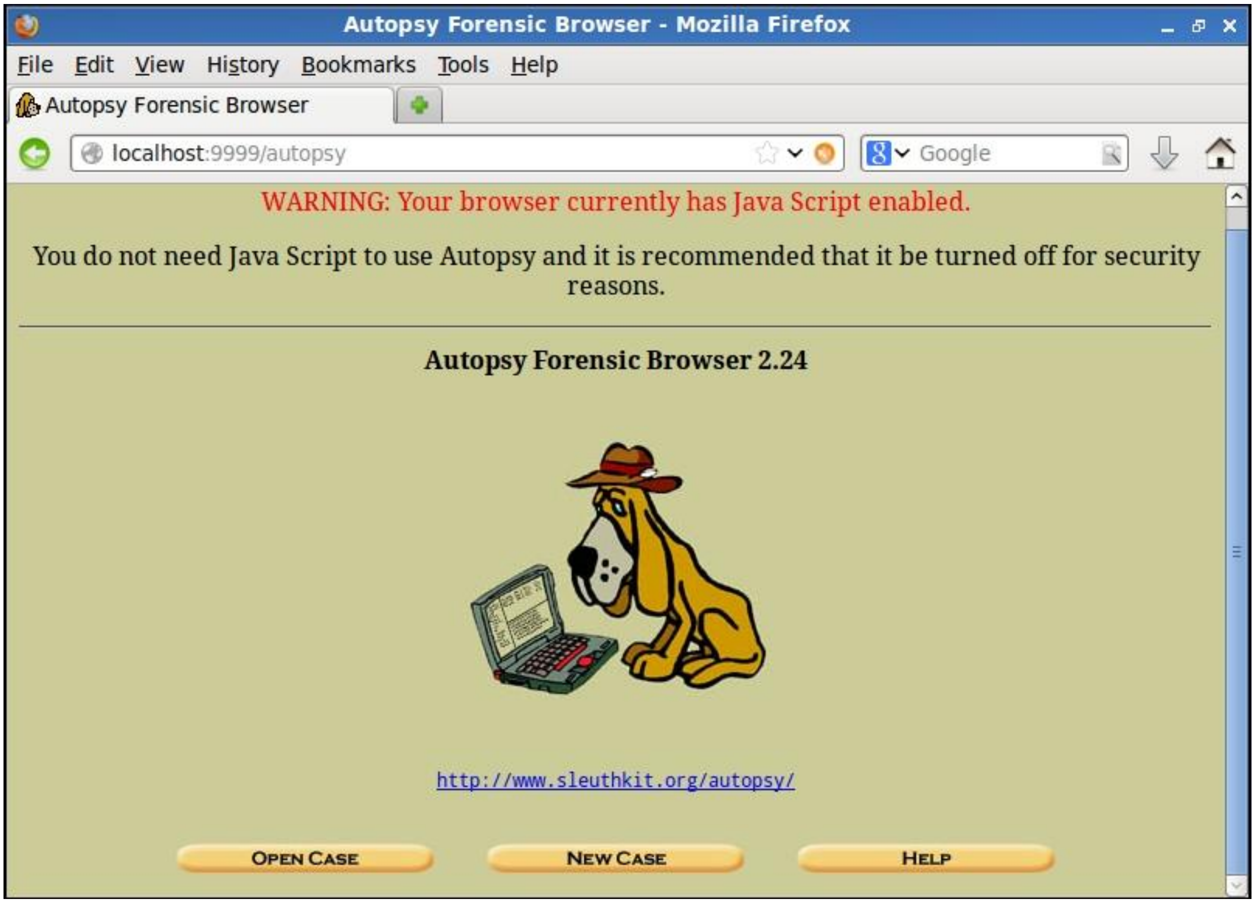
```
digforensics@forensics:/mnt/hgfs/windows7$ blkcat -ho 2048 sampleimage.dd 1118226 | more
0       4d5a9000 03000000 04000000 ffff0000     MZ.. .... .... ....
16      b8000000 00000000 40000000 00000000     .... .... @... ....
32      00000000 00000000 00000000 00000000     .... .... .... ....
48      00000000 00000000 00000000 e8000000     .... .... .... ....
64      0e1fba0e 00b409cd 21b8014c cd215468     .... .... !..L .!Th
80      69732070 726f6772 616d2063 616e6e6f     is p rogr am c anno
96      74206265 2072756e 20696e20 444f5320     t be  run  in  DOS
112     6d6f6465 2e0d0d0a 24000000 00000000     mode .... $... ....
128     f277756d b6161b3e b6161b3e b6161b3e     .wum ...> ...> ...>
144     bf6e893e b7161b3e bf6e8e3e ab161b3e     .n.> ...> .n.> ...>
160     bf6e983e cd161b3e bf6e943e 60161b3e     .n.> ...> .n.> `..>
176     bf6e9f3e ad161b3e bf6e8f3e b7161b3e     .n.> ...> .n.> ...>
192     bf6e8a3e b7161b3e 52696368 b6161b3e     .n.> ...> Rich ...>
208     00000000 00000000 00000000 00000000     .... .... .... ....
224     00000000 00000000 50450000 64860700     .... .... PE.. d...
240     2be05b4a 00000000 00000000 f0002220     +.[J .... .... .."
256     0b020900 000c1000 00500a00 00000000     .... .... .P.. ....
272     00000000 00100000 0000e578 00000000     .... .... ...x ....
288     00100000 00020000 06000100 06000100     .... .... .... ....
304     06000100 00000000 00b01a00 00040000     .... .... .... ....
320     b51c1b00 03004001 00000400 00000000     .... ..@. .... ....
336     00100000 00000000 00001000 00000000     .... .... .... ....
352     00100000 00000000 00000000 10000000     .... .... .... ....
368     00811000 63f10000 00000000 00000000     .... c... .... ....
384     00301500 d0600500 00f01300 30320100     .0.. .`.. .... 02..
400     003c1a00 58440000 00a01a00 dc040000     .<.. XD.. .... ....
416     6c191000 38000000 00000000 00000000     l... 8... .... ....
432     00000000 00000000 00000000 00000000     .... .... .... ....
448     00000000 00000000 00000000 00000000     .... .... .... ....
464     00000000 00000000 00000000 00000000     .... .... .... ....
480     00000000 00000000 00000000 00000000     .... .... .... ....
496     2e746578 74000000 ca091000 00100000     .tex t... .... ....
512     000a1000 00040000 00000000 00000000     .... .... .... ....
--More--
```



```
digforensics@forensics:/mnt/hgfs/windows7$ blkls -o 2048 sampleimage.dd > unallocated.blkls
digforensics@forensics:/mnt/hgfs/windows7$ ls -la unallocated.blkls
-rwxrwxrwx 1 root root 4307230720 Oct 14 13:03 unallocated.blkls
```



```
digforensics@forensics:/mnt/hgfs/windows7$ sudo autopsy

============================================================================

                       Autopsy Forensic Browser
                  http://www.sleuthkit.org/autopsy/
                             ver 2.24

============================================================================
Evidence Locker: /var/lib/autopsy
Start Time: Tue Oct 14 15:45:46 2014
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

    http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
```



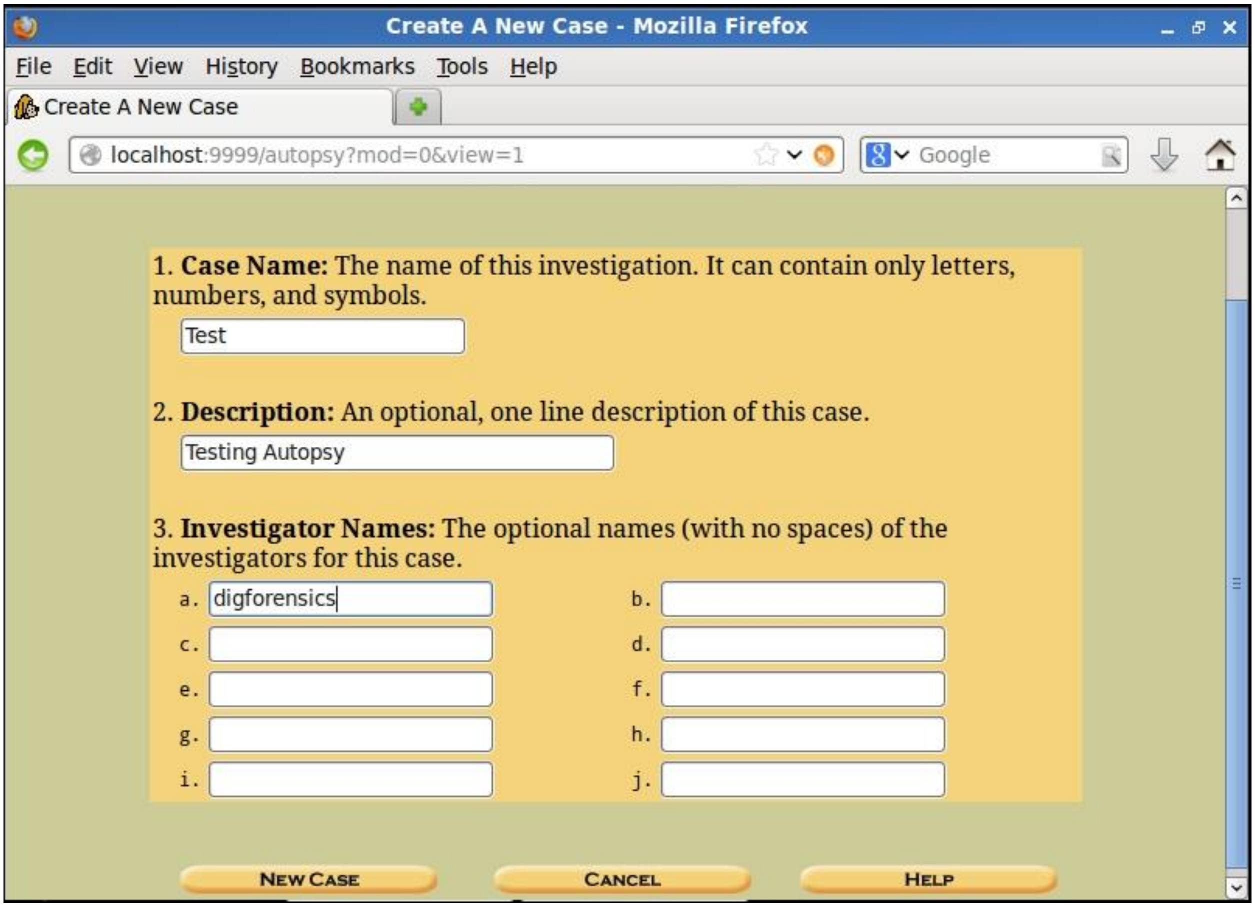
Autopsy Forensic Browser - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Autopsy Forensic Browser
localhost:9999/autopsy
Google

WARNING: Your browser currently has Java Script enabled.

You do not need Java Script to use Autopsy and it is recommended that it be turned off for security reasons.

Autopsy Forensic Browser 2.24

http://www.sleuthkit.org/autopsy/


Create A New Case - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Create A New Case
localhost:9999/autopsy?mod=0&view=1
Google

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

Test

2. **Description:** An optional, one line description of this case.

Testing Autopsy

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

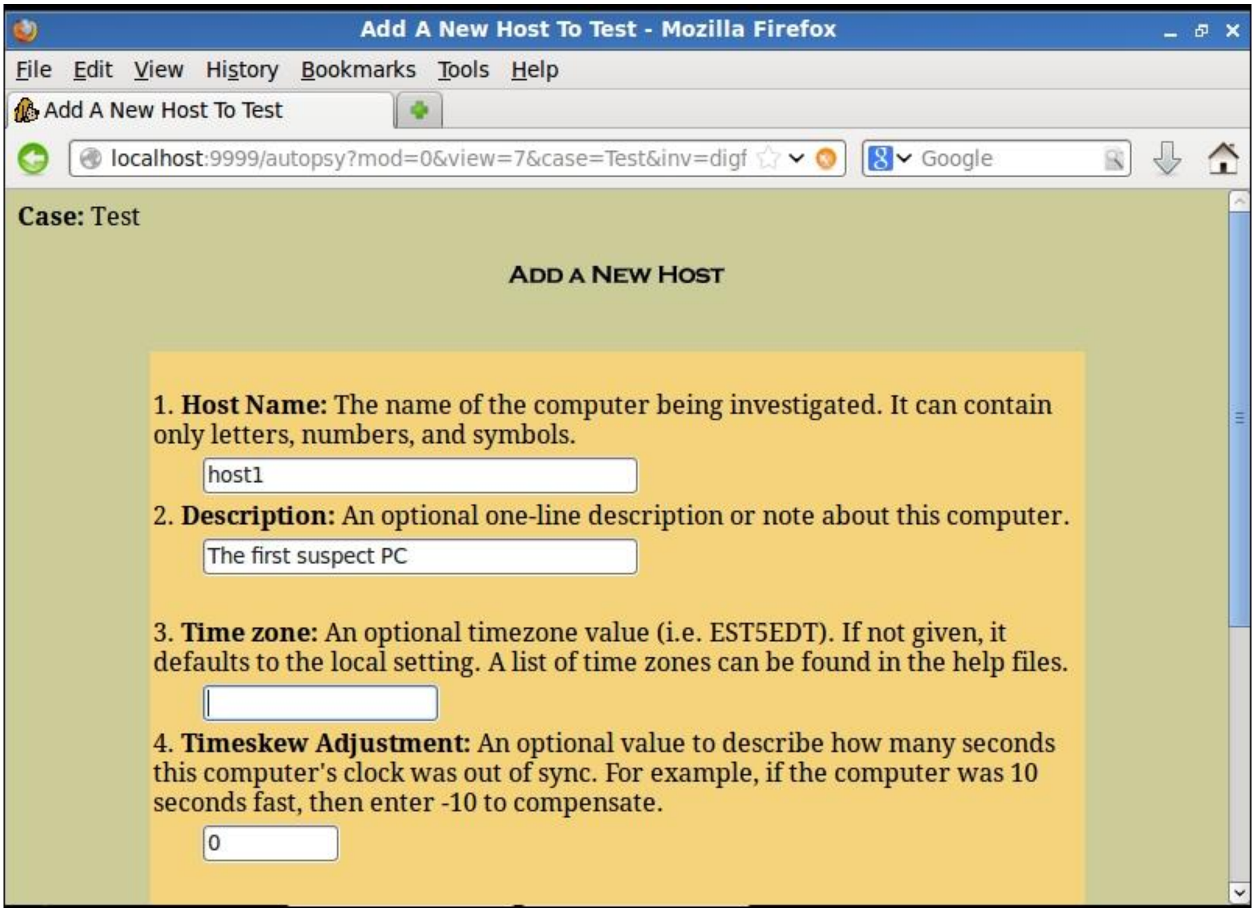
a. digforensics b.

c. d.

e. f.

g. h.

i. j.


Add A New Host To Test - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Add A New Host To Test
localhost:9999/autopsy?mod=0&view=7&case=Test&inv=digf
Google

Case: Test

ADD A NEW HOST

1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.

host1

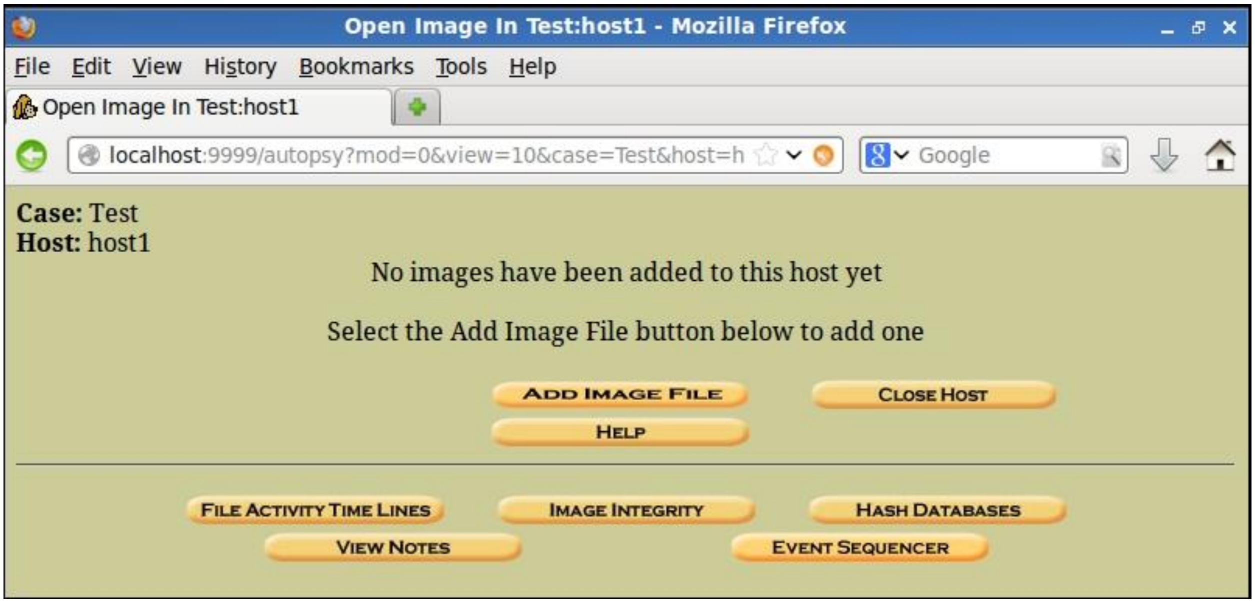
2. **Description:** An optional one-line description or note about this computer.

The first suspect PC

3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.

4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

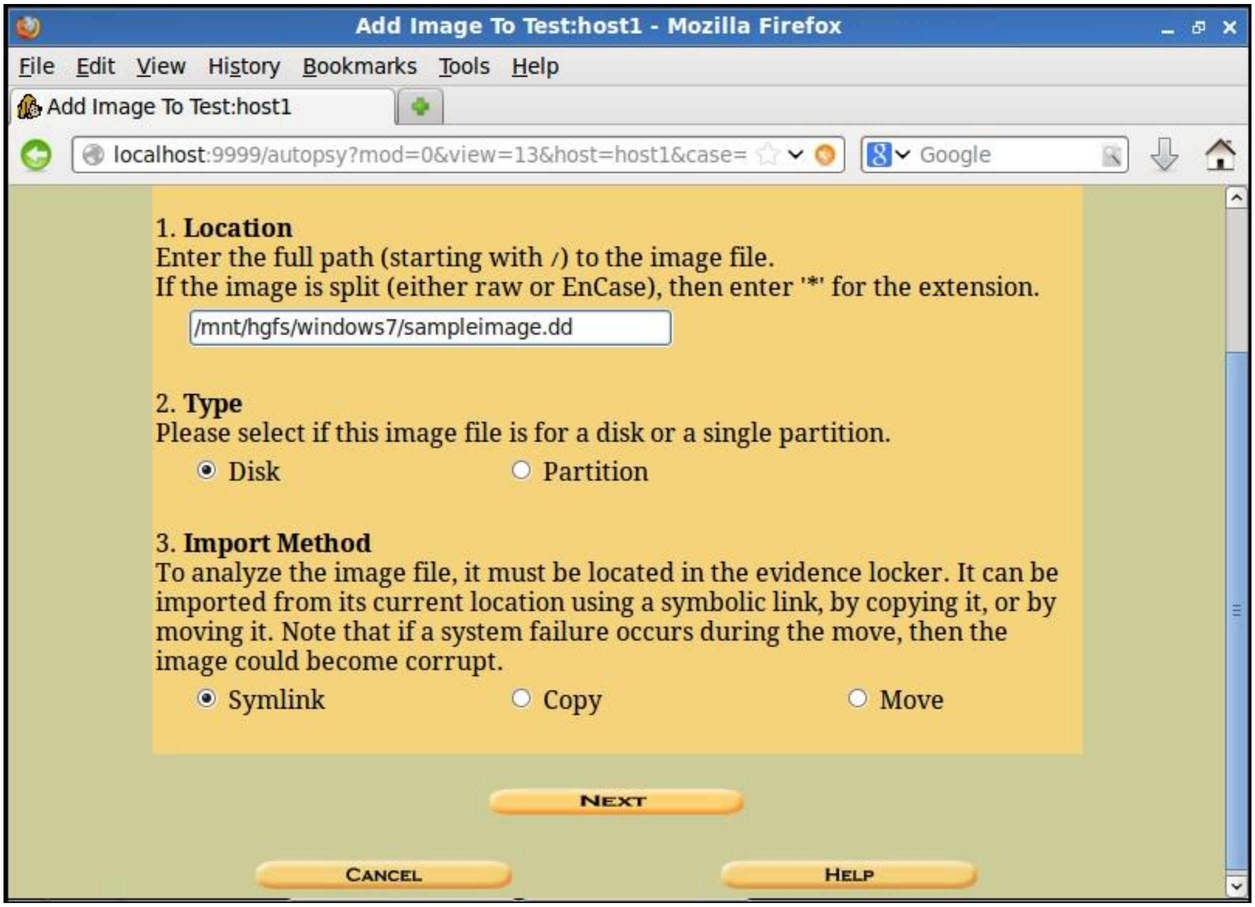
0


Open Image In Test:host1 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Open Image In Test:host1
localhost:9999/autopsy?mod=0&view=10&case=Test&host=h
Google
ADD IMAGE FILE
CLOSE HOST
HELP
FILE ACTIVITY TIME LINES
IMAGE INTEGRITY
HASH DATABASES
VIEW NOTES
EVENT SEQUENCER

Case: Test
Host: host1

No images have been added to this host yet

Select the Add Image File button below to add one



Add Image To Test:host1 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Add Image To Test:host1
localhost:9999/autopsy?mod=0&view=13&host=host1&case=
Google

1. **Location**
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

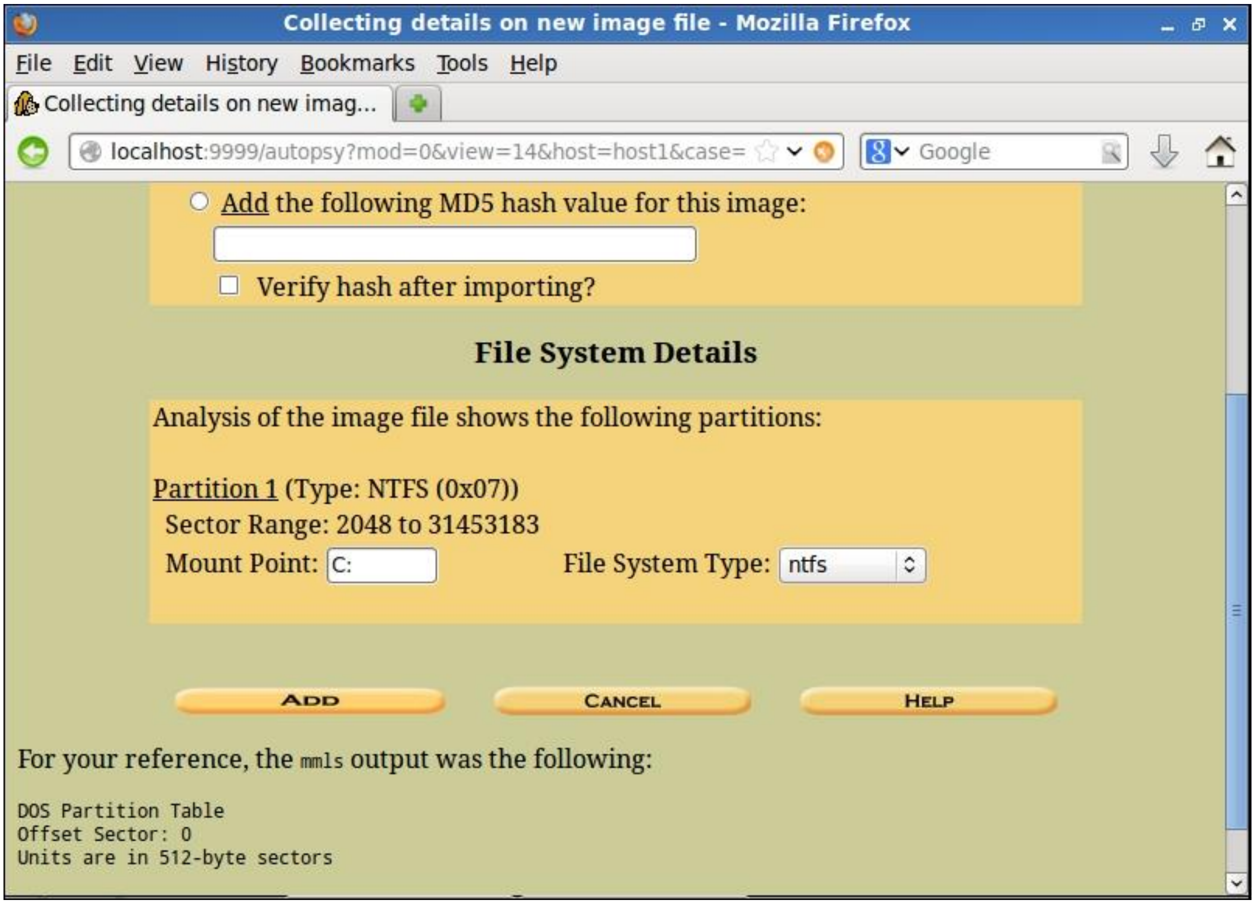
/mnt/hgfs/windows7/sampleimage.dd

2. **Type**
Please select if this image file is for a disk or a single partition.

● Disk ○ Partition

3. **Import Method**
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

● Symlink ○ Copy ○ Move


Collecting details on new image file - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Collecting details on new imag...
localhost:9999/autopsy?mod=0&view=14&host=host1&case=
Google

○ Add the following MD5 hash value for this image:

□ Verify hash after importing?

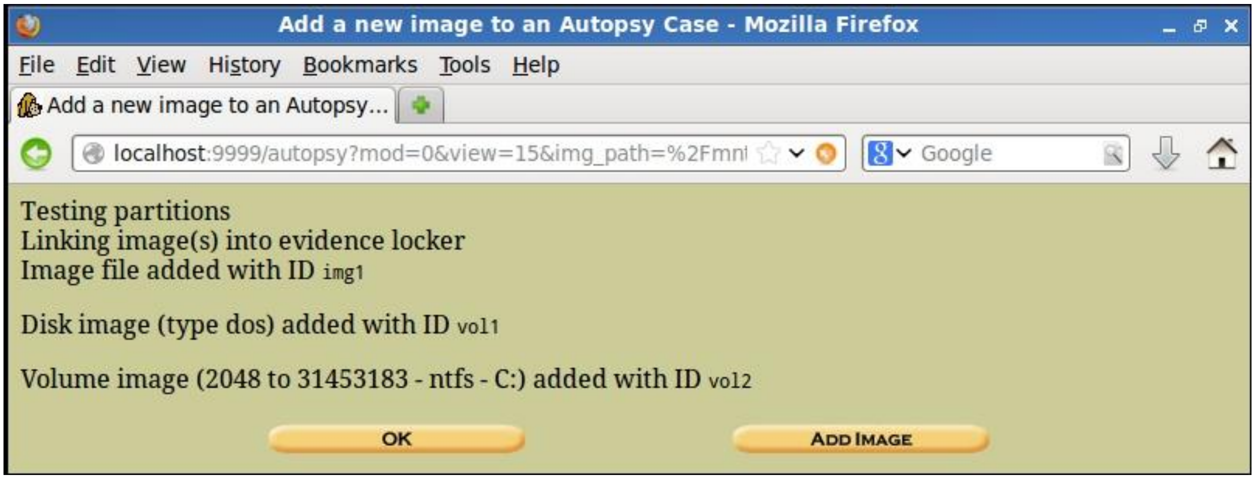
File System Details

Analysis of the image file shows the following partitions:

Partition 1 (Type: NTFS (0x07))
Sector Range: 2048 to 31453183
Mount Point: C: File System Type: ntfs

For your reference, the mmls output was the following:

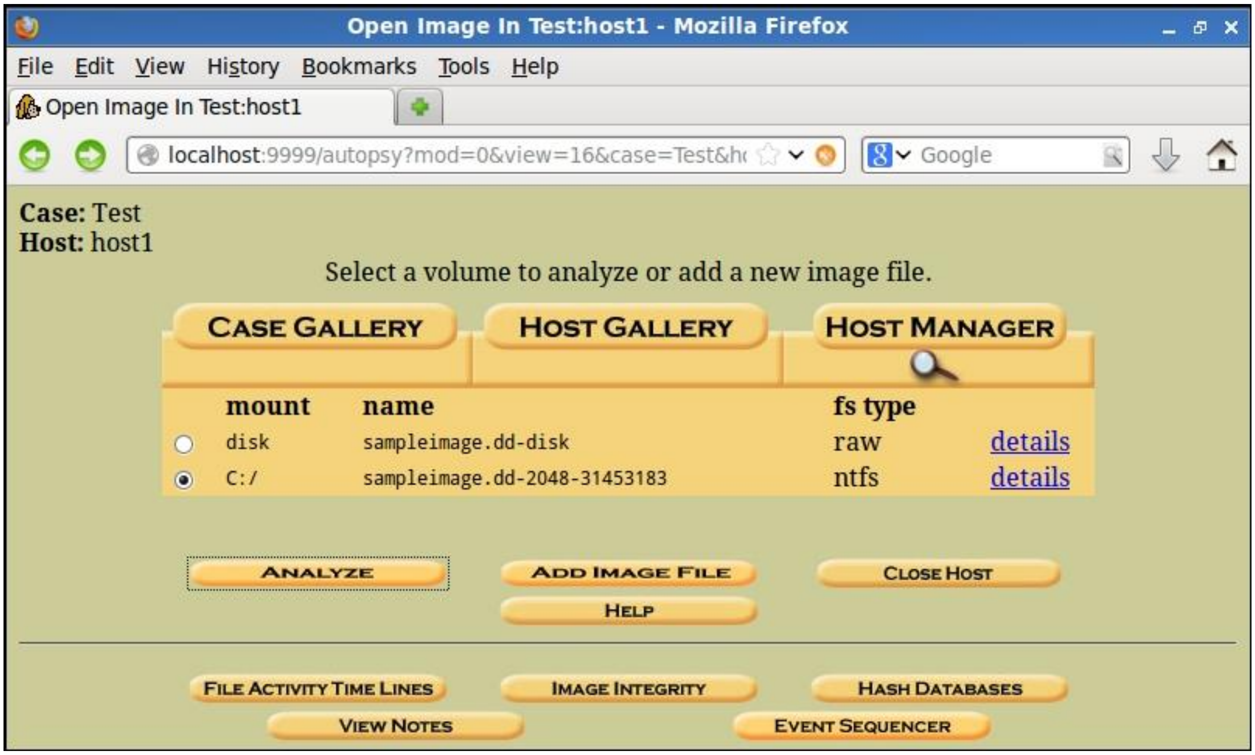
```
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors
```


Add a new image to an Autopsy Case - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Add a new image to an Autopsy...
localhost:9999/autopsy?mod=0&view=15&img_path=%2Fmnt
Google

Testing partitions
Linking image(s) into evidence locker
Image file added with ID img1

Disk image (type dos) added with ID vol1

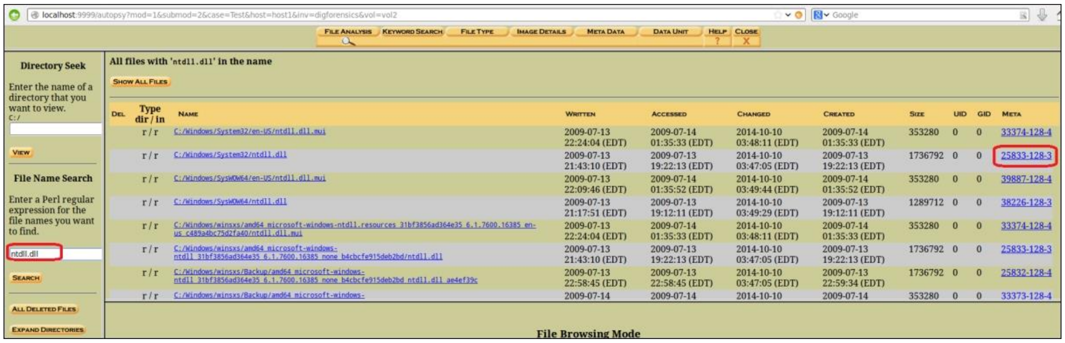
Volume image (2048 to 31453183 - ntfs - C:) added with ID vol2



Case: Test
Host: host1

Select a volume to analyze or add a new image file.

	mount	name	fs type	
○	disk	sampleimage.dd-disk	raw	details
●	C:/	sampleimage.dd-2048-31453183	ntfs	details



Directory Seek

Enter the name of a directory that you want to view.
C:/

File Name Search

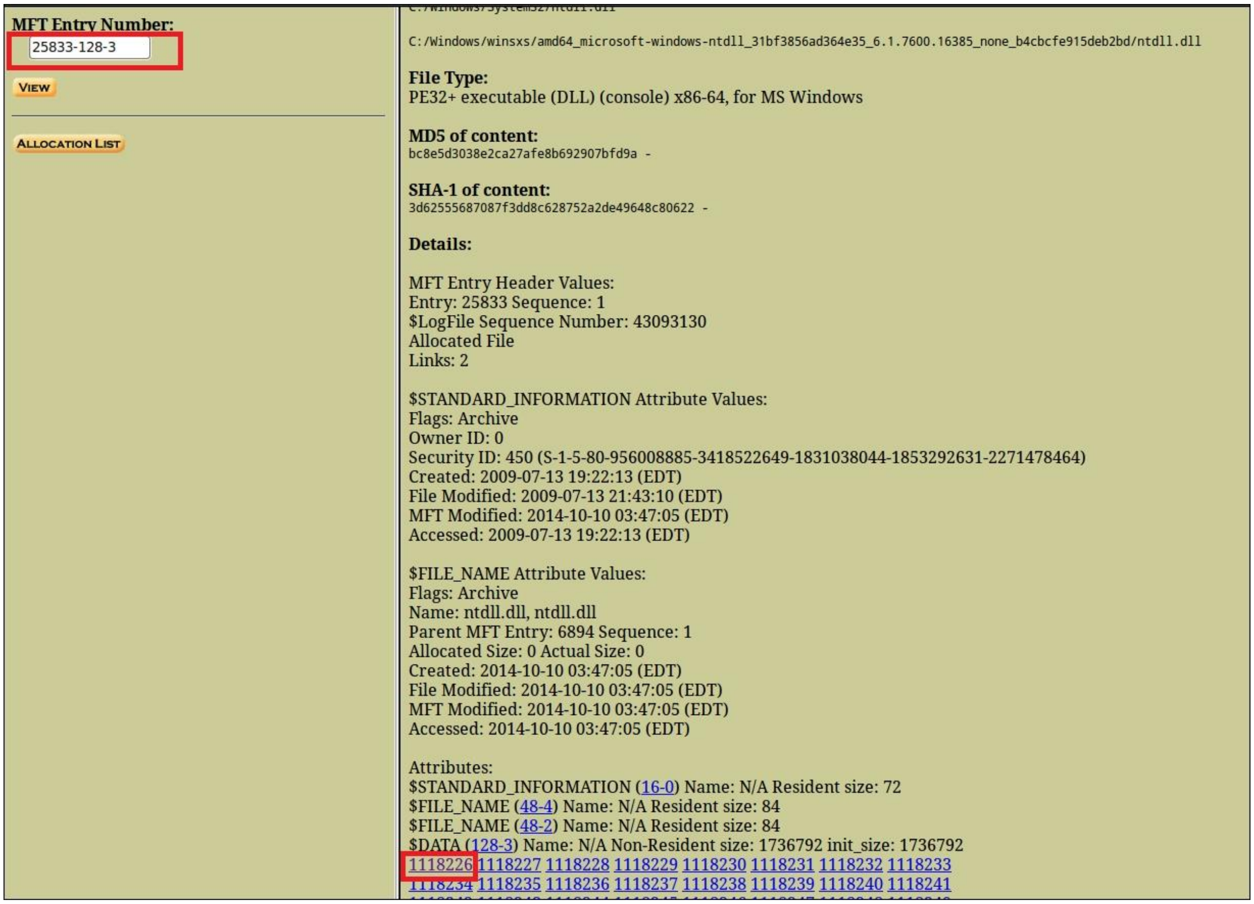
Enter a Perl regular expression for the file names you want to find.

ntdll.dll

All files with 'ntdll.dll' in the name

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	META
	r / r	C:/Windows/System32/en-US/ntdll.dll.mui	2009-07-13 22:24:04 (EDT)	2009-07-14 01:35:33 (EDT)	2014-10-10 03:48:11 (EDT)	2009-07-14 01:35:33 (EDT)	353280	0	0	33374-128-4
	r / r	C:/Windows/System32/ntdll.dll	2009-07-13 21:43:10 (EDT)	2009-07-13 19:22:13 (EDT)	2014-10-10 03:47:05 (EDT)	2009-07-13 19:22:13 (EDT)	1736792	0	0	25833-128-3
	r / r	C:/Windows/SysWOW64/en-US/ntdll.dll.mui	2009-07-13 22:09:46 (EDT)	2009-07-14 01:35:52 (EDT)	2014-10-10 03:49:44 (EDT)	2009-07-14 01:35:52 (EDT)	353280	0	0	39887-128-4
	r / r	C:/Windows/SysWOW64/ntdll.dll	2009-07-13 21:17:51 (EDT)	2009-07-13 19:12:11 (EDT)	2014-10-10 03:49:29 (EDT)	2009-07-13 19:12:11 (EDT)	1289712	0	0	38226-128-3
	r / r	C:/Windows/winsxs/amd64_microsoft-windows-ntdll.resources_31bf3856ad364e35_6.1.7600.16385_en-us_c489a4bc75d2fa40/ntdll.dll.mui	2009-07-13 22:24:04 (EDT)	2009-07-14 01:35:33 (EDT)	2014-10-10 03:48:11 (EDT)	2009-07-14 01:35:33 (EDT)	353280	0	0	33374-128-4
	r / r	C:/Windows/winsxs/amd64_microsoft-windows-ntdll_31bf3856ad364e35_6.1.7600.16385_none_b4cbcfe915deb2bd/ntdll.dll	2009-07-13 21:43:10 (EDT)	2009-07-13 19:22:13 (EDT)	2014-10-10 03:47:05 (EDT)	2009-07-13 19:22:13 (EDT)	1736792	0	0	25833-128-3
	r / r	C:/Windows/winsxs/Backup/amd64_microsoft-windows-ntdll_31bf3856ad364e35_6.1.7600.16385_none_b4cbcfe915deb2bd_ntdll.dll_ae4ef39c	2009-07-13 22:58:45 (EDT)	2009-07-13 22:58:45 (EDT)	2014-10-10 03:47:05 (EDT)	2009-07-13 22:59:34 (EDT)	1736792	0	0	25832-128-4
	r / r	C:/Windows/winsxs/Backup/amd64_microsoft-windows-	2009-07-14	2009-07-14	2014-10-10	2009-07-14	353280	0	0	33373-128-4

File Browsing Mode



MFT Entry Number: 25833-128-3

```
C:/Windows/System32/ntdll.dll

C:/Windows/winsxs/amd64_microsoft-windows-ntdll_31bf3856ad364e35_6.1.7600.16385_none_b4cbcfe915deb2bd/ntdll.dll
```

File Type:
PE32+ executable (DLL) (console) x86-64, for MS Windows

MD5 of content:
`bc8e5d3038e2ca27afe8b692907bfd9a -`

SHA-1 of content:
`3d62555687087f3dd8c628752a2de49648c80622 -`

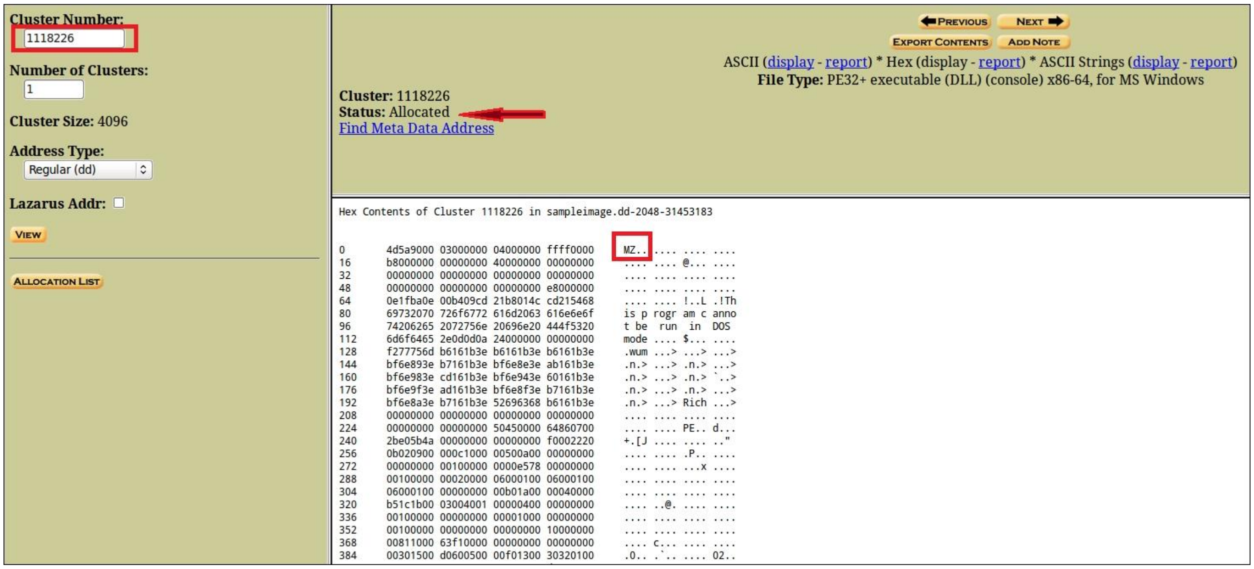
Details:

MFT Entry Header Values:
Entry: 25833 Sequence: 1
$LogFile Sequence Number: 43093130
Allocated File
Links: 2

$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 450 (S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464)
Created: 2009-07-13 19:22:13 (EDT)
File Modified: 2009-07-13 21:43:10 (EDT)
MFT Modified: 2014-10-10 03:47:05 (EDT)
Accessed: 2009-07-13 19:22:13 (EDT)

$FILE_NAME Attribute Values:
Flags: Archive
Name: ntdll.dll, ntdll.dll
Parent MFT Entry: 6894 Sequence: 1
Allocated Size: 0 Actual Size: 0
Created: 2014-10-10 03:47:05 (EDT)
File Modified: 2014-10-10 03:47:05 (EDT)
MFT Modified: 2014-10-10 03:47:05 (EDT)
Accessed: 2014-10-10 03:47:05 (EDT)

Attributes:
$STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
$FILE_NAME (48-4) Name: N/A Resident size: 84
$FILE_NAME (48-2) Name: N/A Resident size: 84
$DATA (128-3) Name: N/A Non-Resident size: 1736792 init_size: 1736792
1118226 1118227 1118228 1118229 1118230 1118231 1118232 1118233
1118234 1118235 1118236 1118237 1118238 1118239 1118240 1118241



Cluster Number: 1118226

Number of Clusters: 1

Cluster Size: 4096

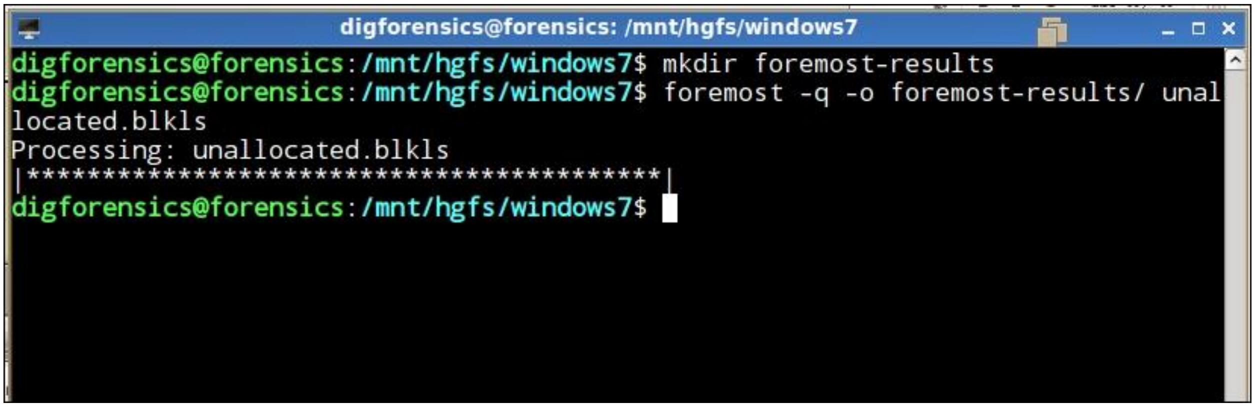
Address Type: Regular (dd)

Lazarus Addr: □

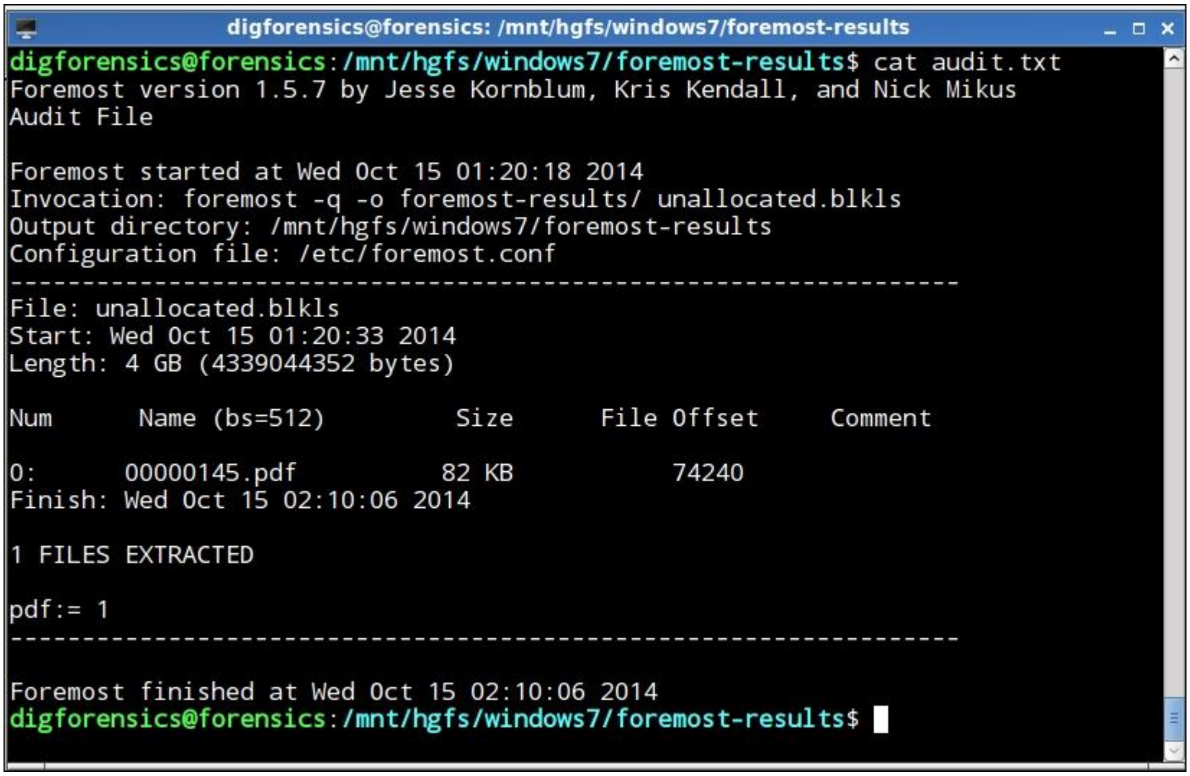
ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report)
File Type: PE32+ executable (DLL) (console) x86-64, for MS Windows

Cluster: 1118226
Status: Allocated
Find Meta Data Address

```
Hex Contents of Cluster 1118226 in sampleimage.dd-2048-31453183


0       4d5a9000 03000000 04000000 ffff0000    MZ.. .... .... ....
16      b8000000 00000000 40000000 00000000    .... .... @... ....
32      00000000 00000000 00000000 00000000    .... .... .... ....
48      00000000 00000000 00000000 e8000000    .... .... .... ....
64      0e1fba0e 00b409cd 21b8014c cd215468    .... .... !..L .!Th
80      69732070 726f6772 616d2063 616e6e6f    is p rogr am c anno
96      74206265 2072756e 20696e20 444f5320    t be  run  in  DOS
112     6d6f6465 2e0d0d0a 24000000 00000000    mode .... $... ....
128     f277756d b6161b3e b6161b3e b6161b3e    .wum ...> ...> ...>
144     bf6e893e b7161b3e bf6e8e3e ab161b3e    .n.> ...> .n.> ...>
160     bf6e983e cd161b3e bf6e943e 60161b3e    .n.> ...> .n.> `..>
176     bf6e9f3e ad161b3e bf6e8f3e b7161b3e    .n.> ...> .n.> ...>
192     bf6e8a3e b7161b3e 52696368 b6161b3e    .n.> ...> Rich ...>
208     00000000 00000000 00000000 00000000    .... .... .... ....
224     00000000 00000000 50450000 64860700    .... .... PE.. d...
240     2be05b4a 00000000 00000000 f0002220    +.[J .... .... .."
256     0b020900 000c1000 00500a00 00000000    .... .... .P.. ....
272     00000000 00100000 0000e578 00000000    .... .... ...x ....
288     00100000 00020000 06000100 06000100    .... .... .... ....
304     06000100 00000000 00b01a00 00040000    .... .... .... ....
320     b51c1b00 03004001 00000400 00000000    .... ..@. .... ....
336     00100000 00000000 00001000 00000000    .... .... .... ....
352     00100000 00000000 00000000 10000000    .... .... .... ....
368     00811000 63f10000 00000000 00000000    .... c... .... ....
384     00301500 d0600500 00f01300 30320100    .0.. .`.. .... 02..
```



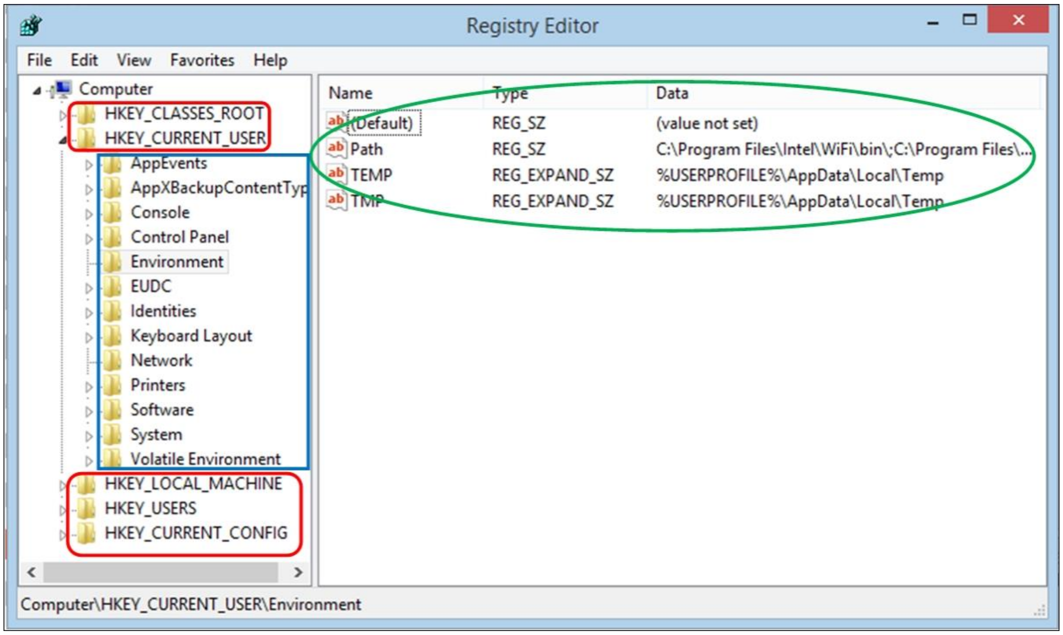
```
digforensics@forensics:/mnt/hgfs/windows7$ mkdir foremost-results
digforensics@forensics:/mnt/hgfs/windows7$ foremost -q -o foremost-results/ unal
located.blkls
Processing: unallocated.blkls
|******************************************|
digforensics@forensics:/mnt/hgfs/windows7$
```



```
digforensics@forensics:/mnt/hgfs/windows7/foremost-results$ cat audit.txt
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Wed Oct 15 01:20:18 2014
Invocation: foremost -q -o foremost-results/ unallocated.blkls
Output directory: /mnt/hgfs/windows7/foremost-results
Configuration file: /etc/foremost.conf
------------------------------------------------------------------
File: unallocated.blkls
Start: Wed Oct 15 01:20:33 2014
Length: 4 GB (4339044352 bytes)

Num      Name (bs=512)          Size      File Offset     Comment

0:      00000145.pdf           82 KB           74240
Finish: Wed Oct 15 02:10:06 2014

1 FILES EXTRACTED

pdf:= 1
------------------------------------------------------------------

Foremost finished at Wed Oct 15 02:10:06 2014
digforensics@forensics:/mnt/hgfs/windows7/foremost-results$
```

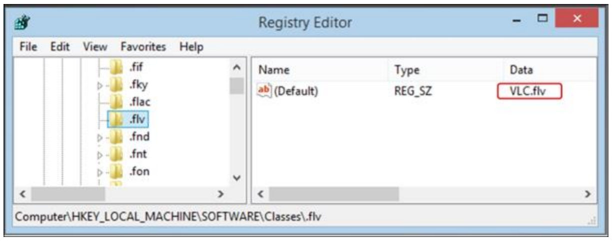
(EVIDENTIAL DATA RELATED TO THE
CASE UNDER INVESTIGATION)

Chapter 7: Registry Analysis



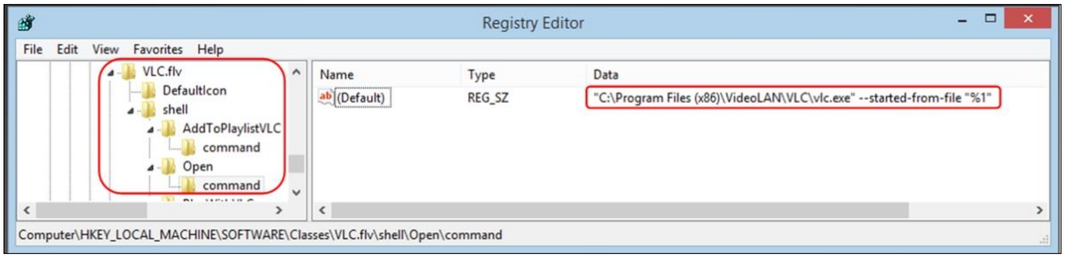
Name	Type	Data
(Default)	REG_SZ	(value not set)
Path	REG_SZ	C:\Program Files\Intel\WiFi\bin\;C:\Program Files\...
TEMP	REG_EXPAND_SZ	%USERPROFILE%\AppData\Local\Temp
TMP	REG_EXPAND_SZ	%USERPROFILE%\AppData\Local\Temp

Computer\HKEY_CURRENT_USER\Environment



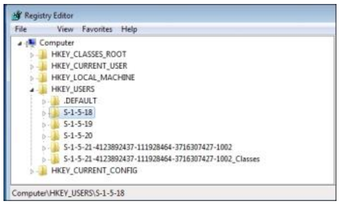
Name	Type	Data
(Default)	REG_SZ	VLC.flv

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.flv



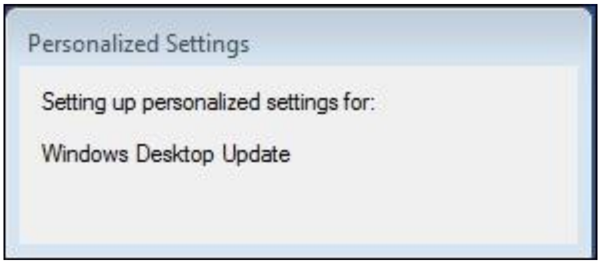
Name	Type	Data
(Default)	REG_SZ	"C:\Program Files (x86)\VideoLAN\VLC\vlc.exe" --started-from-file "%1"

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VLC.flv\shell\Open\command



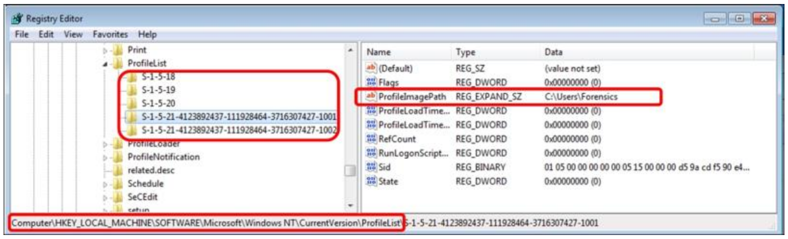
```
Computer
  HKEY_CLASSES_ROOT
  HKEY_CURRENT_USER
  HKEY_LOCAL_MACHINE
  HKEY_USERS
    .DEFAULT
    S-1-5-18
    S-1-5-19
    S-1-5-20
    S-1-5-21-4123892437-111928464-3716307427-1002
    S-1-5-21-4123892437-111928464-3716307427-1002_Classes
  HKEY_CURRENT_CONFIG
```

Computer\HKEY_USERS\S-1-5-18


Personalized Settings

Setting up personalized settings for:

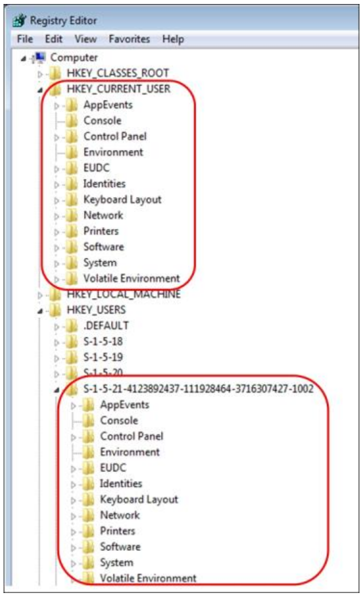
Windows Desktop Update



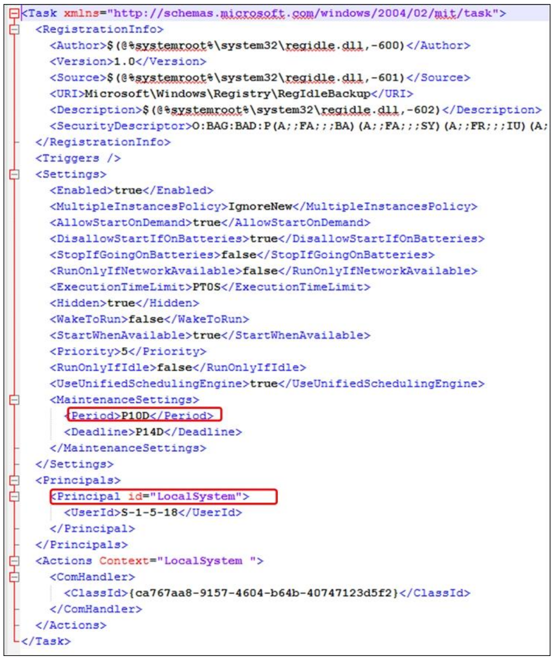
```
Print
ProfileList
  S-1-5-18
  S-1-5-19
  S-1-5-20
  S-1-5-21-4123892437-111928464-3716307427-1001
  S-1-5-21-4123892437-111928464-3716307427-1002
ProfileLoader
ProfileNotification
related.desc
Schedule
SeCEdit
setup
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
Flags	REG_DWORD	0x00000000 (0)
ProfileImagePath	REG_EXPAND_SZ	C:\Users\Forensics
ProfileLoadTime...	REG_DWORD	0x00000000 (0)
ProfileLoadTime...	REG_DWORD	0x00000000 (0)
RefCount	REG_DWORD	0x00000000 (0)
RunLogonScript...	REG_DWORD	0x00000000 (0)
Sid	REG_BINARY	01 05 00 00 00 00 00 05 15 00 00 00 d5 9a cd f5 90 e4...
State	REG_DWORD	0x00000000 (0)

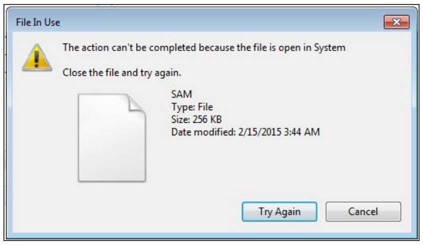
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-4123892437-111928464-3716307427-1001



```
Computer
  HKEY_CLASSES_ROOT
  HKEY_CURRENT_USER
    AppEvents
    Console
    Control Panel
    Environment
    EUDC
    Identities
    Keyboard Layout
    Network
    Printers
    Software
    System
    Volatile Environment
  HKEY_LOCAL_MACHINE
  HKEY_USERS
    .DEFAULT
    S-1-5-18
    S-1-5-19
    S-1-5-20
    S-1-5-21-4123892437-111928464-3716307427-1002
      AppEvents
      Console
      Control Panel
      Environment
      EUDC
      Identities
      Keyboard Layout
      Network
      Printers
      Software
      System
      Volatile Environment
```



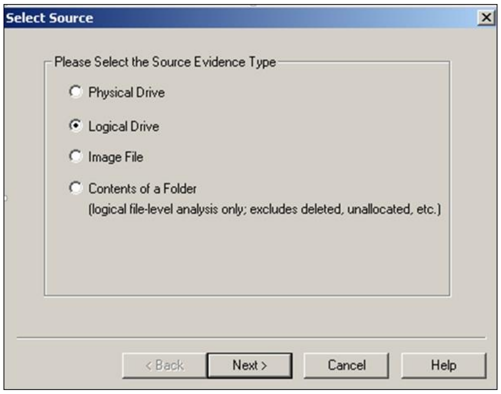
```
<Task xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Author>$(@%systemroot%\system32\regidle.dll,-600)</Author>
    <Version>1.0</Version>
    <Source>$(@%systemroot%\system32\regidle.dll,-601)</Source>
    <URI>Microsoft\Windows\Registry\RegIdleBackup</URI>
    <Description>$(@%systemroot%\system32\regidle.dll,-602)</Description>
    <SecurityDescriptor>O:BAG:BAD:P(A;;FA;;;BA)(A;;FA;;;SY)(A;;FR;;;IU)(A;
  </RegistrationInfo>
  <Triggers />
  <Settings>
    <Enabled>true</Enabled>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <AllowStartOnDemand>true</AllowStartOnDemand>
    <DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>
    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>
    <Hidden>true</Hidden>
    <WakeToRun>false</WakeToRun>
    <StartWhenAvailable>true</StartWhenAvailable>
    <Priority>5</Priority>
    <RunOnlyIfIdle>false</RunOnlyIfIdle>
    <UseUnifiedSchedulingEngine>true</UseUnifiedSchedulingEngine>
    <MaintenanceSettings>
      <Period>P10D</Period>
      <Deadline>P14D</Deadline>
    </MaintenanceSettings>
  </Settings>
  <Principals>
    <Principal id="LocalSystem">
      <UserId>S-1-5-18</UserId>
    </Principal>
  </Principals>
  <Actions Context="LocalSystem ">
    <ComHandler>
      <ClassId>{ca767aa8-9157-4604-b64b-40747123d5f2}</ClassId>
    </ComHandler>
  </Actions>
</Task>
```



The action can't be completed because the file is open in System

Close the file and try again.

SAM
Type: File
Size: 256 KB
Date modified: 2/15/2015 3:44 AM



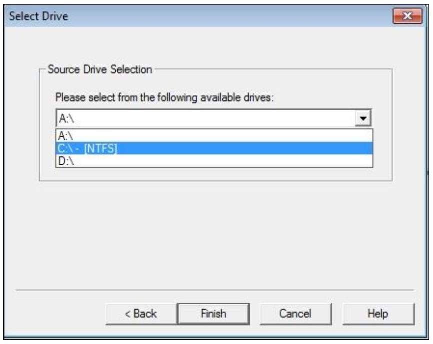
Please Select the Source Evidence Type

○ Physical Drive

● Logical Drive

○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)



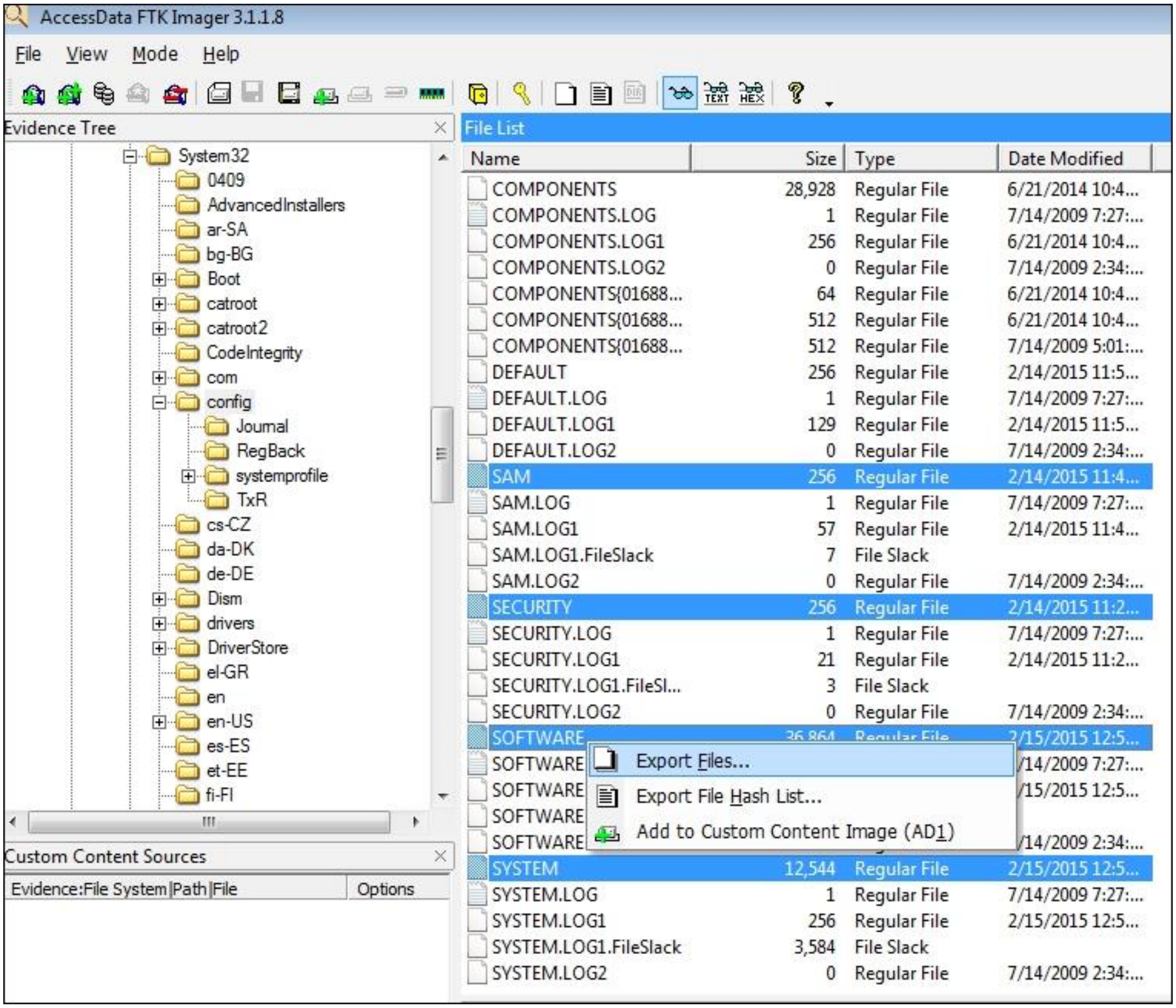
Select Drive

Source Drive Selection

Please select from the following available drives:

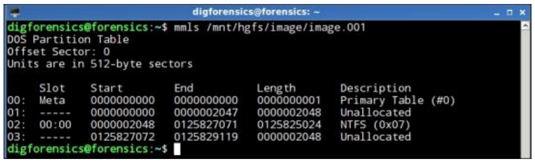
A:\

A:\
C:\ - [NTFS]
D:\

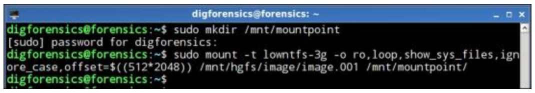


AccessData FTK Imager 3.1.1.8

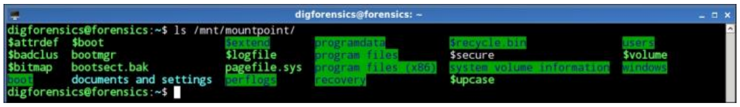
Name	Size	Type	Date Modified
COMPONENTS	28,928	Regular File	6/21/2014 10:4...
COMPONENTS.LOG	1	Regular File	7/14/2009 7:27:...
COMPONENTS.LOG1	256	Regular File	6/21/2014 10:4...
COMPONENTS.LOG2	0	Regular File	7/14/2009 2:34:...
COMPONENTS{01688...	64	Regular File	6/21/2014 10:4...
COMPONENTS{01688...	512	Regular File	6/21/2014 10:4...
COMPONENTS{01688...	512	Regular File	7/14/2009 5:01:...
DEFAULT	256	Regular File	2/14/2015 11:5...
DEFAULT.LOG	1	Regular File	7/14/2009 7:27:...
DEFAULT.LOG1	129	Regular File	2/14/2015 11:5...
DEFAULT.LOG2	0	Regular File	7/14/2009 2:34:...
SAM	256	Regular File	2/14/2015 11:4...
SAM.LOG	1	Regular File	7/14/2009 7:27:...
SAM.LOG1	57	Regular File	2/14/2015 11:4...
SAM.LOG1.FileSlack	7	File Slack	
SAM.LOG2	0	Regular File	7/14/2009 2:34:...
SECURITY	256	Regular File	2/14/2015 11:2...
SECURITY.LOG	1	Regular File	7/14/2009 7:27:...
SECURITY.LOG1	21	Regular File	2/14/2015 11:2...
SECURITY.LOG1.FileSl...	3	File Slack	
SECURITY.LOG2	0	Regular File	7/14/2009 2:34:...
SOFTWARE	36,864	Regular File	2/15/2015 12:5...
SOFTWARE			/14/2009 7:27:...
SOFTWARE			/15/2015 12:5...
SOFTWARE			
SOFTWARE			/14/2009 2:34:...
SYSTEM	12,544	Regular File	2/15/2015 12:5...
SYSTEM.LOG	1	Regular File	7/14/2009 7:27:...
SYSTEM.LOG1	256	Regular File	2/15/2015 12:5...
SYSTEM.LOG1.FileSlack	3,584	File Slack	
SYSTEM.LOG2	0	Regular File	7/14/2009 2:34:...



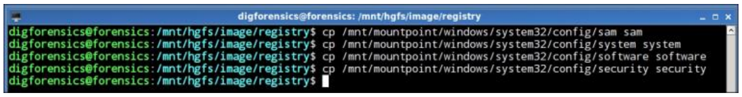
```
digforensics@forensics:~$ mmls /mnt/hgfs/image/image.001
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

     Slot    Start        End          Length       Description
00:  Meta    0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----   0000000000   0000002047   0000002048   Unallocated
02:  00:00   0000002048   0125827071   0125825024   NTFS (0x07)
03:  -----   0125827072   0125829119   0000002048   Unallocated
digforensics@forensics:~$
```



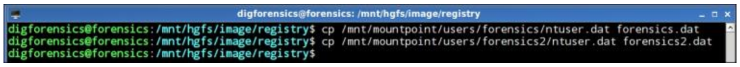
```
digforensics@forensics:~$ sudo mkdir /mnt/mountpoint
[sudo] password for digforensics:
digforensics@forensics:~$ sudo mount -t lowntfs-3g -o ro,loop,show_sys_files,ign
ore_case,offset=$((512*2048)) /mnt/hgfs/image/image.001 /mnt/mountpoint/
digforensics@forensics:~$
```



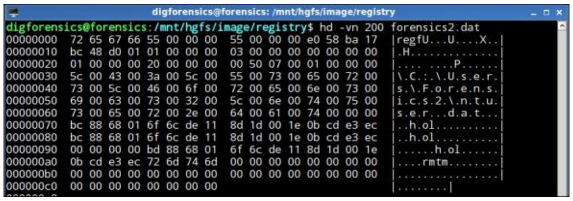
```
digforensics@forensics:~$ ls /mnt/mountpoint/
$attrdef  $boot                 $extend      programdata          $recycle.bin               users
$badclus  bootmgr               $logfile     program files        $secure                    $volume
$bitmap   bootsect.bak          pagefile.sys program files (x86)  system volume information  windows
boot      documents and settings perflogs    recovery             $upcase
digforensics@forensics:~$
```



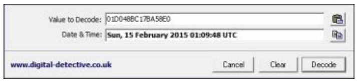
```
digforensics@forensics:/mnt/hgfs/image/registry$ cp /mnt/mountpoint/windows/system32/config/sam sam
digforensics@forensics:/mnt/hgfs/image/registry$ cp /mnt/mountpoint/windows/system32/config/system system
digforensics@forensics:/mnt/hgfs/image/registry$ cp /mnt/mountpoint/windows/system32/config/software software
digforensics@forensics:/mnt/hgfs/image/registry$ cp /mnt/mountpoint/windows/system32/config/security security
digforensics@forensics:/mnt/hgfs/image/registry$
```



```
digforensics@forensics:/mnt/hgfs/image/registry$ cp /mnt/mountpoint/users/forensics/ntuser.dat forensics.dat
digforensics@forensics:/mnt/hgfs/image/registry$ cp /mnt/mountpoint/users/forensics2/ntuser.dat forensics2.dat
digforensics@forensics:/mnt/hgfs/image/registry$
```

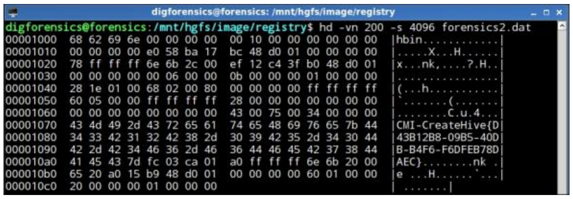


```
digforensics@forensics:/mnt/hgfs/image/registry$ hd -vn 200 forensics2.dat
00000000  72 65 67 66 55 00 00 00  55 00 00 00 e0 58 ba 17  |regfU...U....X..|
00000010  bc 48 d0 01 01 00 00 00  03 00 00 00 00 00 00 00  |.H..............|
00000020  01 00 00 00 20 00 00 00  00 50 07 00 01 00 00 00  |.... ....P......|
00000030  5c 00 43 00 3a 00 5c 00  55 00 73 00 65 00 72 00  |\.C.:.\.U.s.e.r.|
00000040  73 00 5c 00 46 00 6f 00  72 00 65 00 6e 00 73 00  |s.\.F.o.r.e.n.s.|
00000050  69 00 63 00 73 00 32 00  5c 00 6e 00 74 00 75 00  |i.c.s.2.\.n.t.u.|
00000060  73 00 65 00 72 00 2e 00  64 00 61 00 74 00 00 00  |s.e.r...d.a.t...|
00000070  bc 88 68 01 6f 6c de 11  8d 1d 00 1e 0b cd e3 ec  |..h.ol..........|
00000080  bc 88 68 01 6f 6c de 11  8d 1d 00 1e 0b cd e3 ec  |..h.ol..........|
00000090  00 00 00 00 bd 88 68 01  6f 6c de 11 8d 1d 00 1e  |......h.ol......|
000000a0  0b cd e3 ec 72 6d 74 6d  00 00 00 00 00 00 00 00  |....rmtm........|
000000b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
000000c0  00 00 00 00 00 00 00 00                           |........|
```

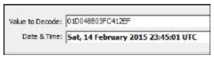


Value to Decode: 01D048BC17BA58E0

Date & Time: Sun, 15 February 2015 01:09:48 UTC

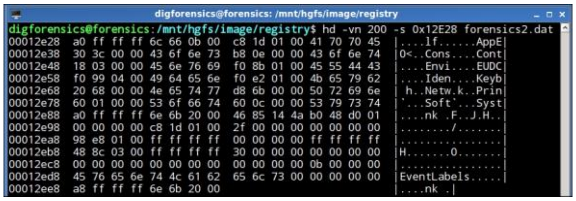


```
digforensics@forensics:/mnt/hgfs/image/registry$ hd -vn 200 -s 4096 forensics2.dat
00001000  68 62 69 6e 00 00 00 00  00 10 00 00 00 00 00 00  |hbin............|
00001010  00 00 00 00 e0 58 ba 17  bc 48 d0 01 00 00 00 00  |.....X...H......|
00001020  78 ff ff ff 6e 6b 2c 00  ef 12 c4 3f b0 48 d0 01  |x...nk,....?.H..|
00001030  00 00 00 00 00 06 00 00  0b 00 00 00 01 00 00 00  |................|
00001040  28 1e 01 00 68 02 00 80  00 00 00 00 ff ff ff ff  |(...h...........|
00001050  60 05 00 00 ff ff ff ff  28 00 00 00 00 00 00 00  |`.......(.......|
00001060  00 00 00 00 00 00 00 00  43 00 75 00 34 00 00 00  |........C.u.4...|
00001070  43 4d 49 2d 43 72 65 61  74 65 48 69 76 65 7b 44  |CMI-CreateHive{D|
00001080  34 33 42 31 32 42 38 2d  30 39 42 35 2d 34 30 44  |43B12B8-09B5-40D|
00001090  42 2d 42 34 46 36 2d 46  36 44 46 45 42 37 38 44  |B-B4F6-F6DFEB78D|
000010a0  41 45 43 7d fc 03 ca 01  a0 ff ff ff 6e 6b 20 00  |AEC}........nk .|
000010b0  65 20 a0 15 b9 48 d0 01  00 00 00 00 60 01 00 00  |e ...H......`...|
000010c0  20 00 00 00 01 00 00 00                           | .......|
```

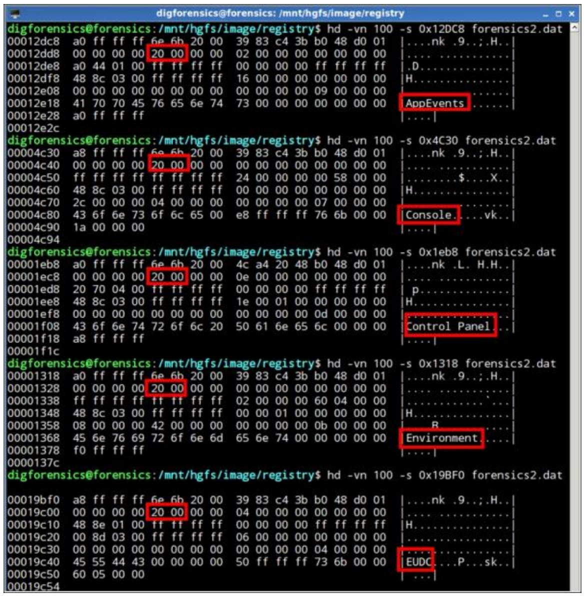


Value to Decode: 01D048B03FC412EF

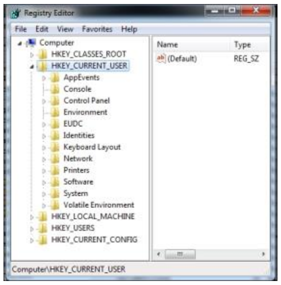
Date & Time: Sat, 14 February 2015 23:45:01 UTC



```
digforensics@forensics:/mnt/hgfs/image/registry$ hd -vn 200 -s 0x12E28 forensics2.dat
00012e28  a0 ff ff ff 6c 66 0b 00  c8 1d 01 00 41 70 70 45  |....lf......AppE|
00012e38  30 3c 00 00 43 6f 6e 73  b8 0e 00 00 43 6f 6e 74  |0<..Cons....Cont|
00012e48  18 03 00 00 45 6e 76 69  f0 8b 01 00 45 55 44 43  |....Envi....EUDC|
00012e58  f0 99 04 00 49 64 65 6e  f0 e2 01 00 4b 65 79 62  |....Iden....Keyb|
00012e68  20 68 00 00 4e 65 74 77  d8 6b 00 00 50 72 69 6e  | h..Netw.k..Prin|
00012e78  60 01 00 00 53 6f 66 74  60 0c 00 00 53 79 73 74  |`...Soft`...Syst|
00012e88  a0 ff ff ff 6e 6b 20 00  46 85 14 4a b0 48 d0 01  |....nk .F..J.H..|
00012e98  00 00 00 00 c8 1d 01 00  2f 00 00 00 00 00 00 00  |......../.......|
00012ea8  98 e8 01 00 ff ff ff ff  00 00 00 00 ff ff ff ff  |................|
00012eb8  48 8c 03 00 ff ff ff ff  30 00 00 00 00 00 00 00  |H.......0.......|
00012ec8  00 00 00 00 00 00 00 00  00 00 00 00 0b 00 00 00  |................|
00012ed8  45 76 65 6e 74 4c 61 62  65 6c 73 00 00 00 00 00  |EventLabels.....|
00012ee8  a8 ff ff ff 6e 6b 20 00                           |....nk .|
```



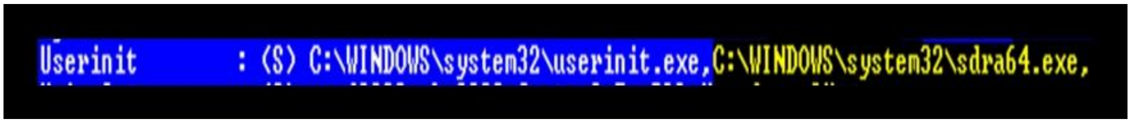
```
digforensics@forensics:/mnt/hgfs/image/registry$ hd -vn 100 -s 0x12DC8 forensics2.dat
00012dc8  a0 ff ff ff 6e 6b 20 00  39 83 c4 3b b0 48 d0 01  |....nk .9..;.H..|
00012dd8  00 00 00 00 20 00 00 00  02 00 00 00 00 00 00 00  |.... ...........|
00012de8  a0 44 01 00 ff ff ff ff  00 00 00 00 ff ff ff ff  |.D..............|
00012df8  48 8c 03 00 ff ff ff ff  16 00 00 00 00 00 00 00  |H...............|
00012e08  00 00 00 00 00 00 00 00  00 00 00 00 09 00 00 00  |................|
00012e18  41 70 70 45 76 65 6e 74  73 00 00 00 00 00 00 00  |AppEvents.......|
00012e28  a0 ff ff ff                                       |....|
00012e2c
digforensics@forensics:/mnt/hgfs/image/registry$ hd -vn 100 -s 0x4C30 forensics2.dat
00004c30  a8 ff ff ff 6e 6b 20 00  39 83 c4 3b b0 48 d0 01  |....nk .9..;.H..|
00004c40  00 00 00 00 20 00 00 00  00 00 00 00 00 00 00 00  |.... ...........|
00004c50  ff ff ff ff ff ff ff ff  24 00 00 00 58 00 00 00  |........$...X...|
00004c60  48 8c 03 00 ff ff ff ff  00 00 00 00 00 00 00 00  |H...............|
00004c70  2c 00 00 00 04 00 00 00  00 00 00 00 07 00 00 00  |,...............|
00004c80  43 6f 6e 73 6f 6c 65 00  e8 ff ff ff 76 6b 00 00  |Console.....vk..|
00004c90  1a 00 00 00                                       |....|
00004c94
digforensics@forensics:/mnt/hgfs/image/registry$ hd -vn 100 -s 0x1eb8 forensics2.dat
00001eb8  a0 ff ff ff 6e 6b 20 00  4c a4 20 48 b0 48 d0 01  |....nk .L. H.H..|
00001ec8  00 00 00 00 20 00 00 00  0e 00 00 00 00 00 00 00  |.... ...........|
00001ed8  20 70 04 00 ff ff ff ff  00 00 00 00 ff ff ff ff  | p..............|
00001ee8  48 8c 03 00 ff ff ff ff  1e 00 01 00 00 00 00 00  |H...............|
00001ef8  00 00 00 00 00 00 00 00  00 00 00 00 0d 00 00 00  |................|
00001f08  43 6f 6e 74 72 6f 6c 20  50 61 6e 65 6c 00 00 00  |Control Panel...|
00001f18  a8 ff ff ff                                       |....|
00001f1c
digforensics@forensics:/mnt/hgfs/image/registry$ hd -vn 100 -s 0x1318 forensics2.dat
00001318  a0 ff ff ff 6e 6b 20 00  39 83 c4 3b b0 48 d0 01  |....nk .9..;.H..|
00001328  00 00 00 00 20 00 00 00  00 00 00 00 00 00 00 00  |.... ...........|
00001338  ff ff ff ff ff ff ff ff  02 00 00 00 60 04 00 00  |............`...|
00001348  48 8c 03 00 ff ff ff ff  00 00 01 00 00 00 00 00  |H...............|
00001358  08 00 00 00 42 00 00 00  00 00 00 00 0b 00 00 00  |....B...........|
00001368  45 6e 76 69 72 6f 6e 6d  65 6e 74 00 00 00 00 00  |Environment.....|
00001378  f0 ff ff ff                                       |....|
0000137c
digforensics@forensics:/mnt/hgfs/image/registry$ hd -vn 100 -s 0x19BF0 forensics2.dat

00019bf0  a8 ff ff ff 6e 6b 20 00  39 83 c4 3b b0 48 d0 01  |....nk .9..;.H..|
00019c00  00 00 00 00 20 00 00 00  04 00 00 00 00 00 00 00  |.... ...........|
00019c10  48 8e 01 00 ff ff ff ff  00 00 00 00 ff ff ff ff  |H...............|
00019c20  00 8d 03 00 ff ff ff ff  06 00 00 00 00 00 00 00  |................|
00019c30  00 00 00 00 00 00 00 00  00 00 00 00 04 00 00 00  |................|
00019c40  45 55 44 43 00 00 00 00  50 ff ff ff 73 6b 00 00  |EUDC....P...sk..|
00019c50  60 05 00 00                                       |`...|
00019c54
```



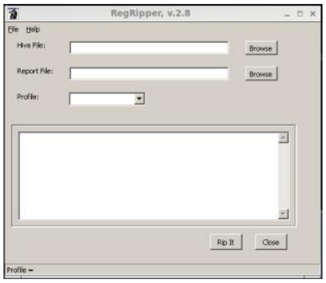
```
Computer
  HKEY_CLASSES_ROOT
  HKEY_CURRENT_USER
    AppEvents
    Console
    Control Panel
    Environment
    EUDC
    Identities
    Keyboard Layout
    Network
    Printers
    Software
    System
    Volatile Environment
  HKEY_LOCAL_MACHINE
  HKEY_USERS
  HKEY_CURRENT_CONFIG
```

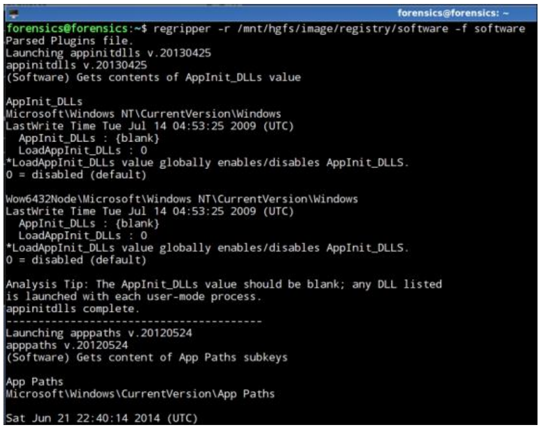
(Default)   REG_SZ

Computer\HKEY_CURRENT_USER

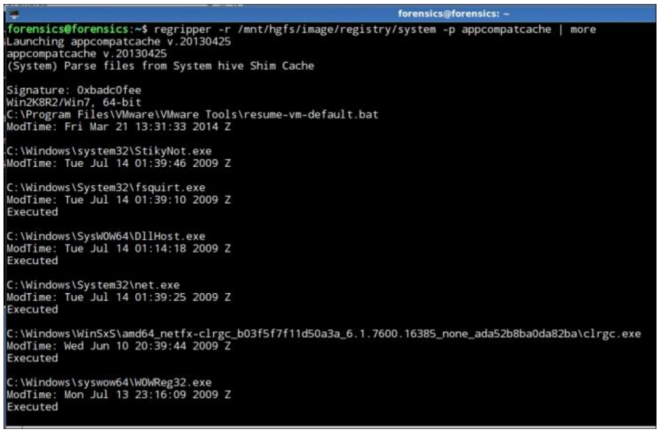


```
Userinit        : (S) C:\WINDOWS\system32\userinit.exe,C:\WINDOWS\system32\sdra64.exe,
```

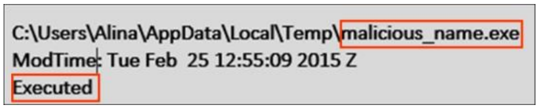




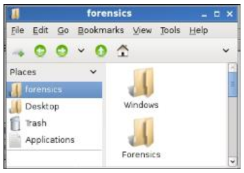
```
forensics@forensics:~$ regripper -r /mnt/hgfs/image/registry/software -f software
Parsed Plugins file.
Launching appinitdlls v.20130425
appinitdlls v.20130425
(Software) Gets contents of AppInit_DLLs value

AppInit_DLLs
Microsoft\Windows NT\CurrentVersion\Windows
LastWrite Time Tue Jul 14 04:53:25 2009 (UTC)
  AppInit_DLLs : {blank}
  LoadAppInit_DLLs : 0
*LoadAppInit_DLLs value globally enables/disables AppInit_DLLS.
0 = disabled (default)

Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows
LastWrite Time Tue Jul 14 04:53:25 2009 (UTC)
  AppInit_DLLs : {blank}
  LoadAppInit_DLLs : 0
*LoadAppInit_DLLs value globally enables/disables AppInit_DLLS.
0 = disabled (default)

Analysis Tip: The AppInit_DLLs value should be blank; any DLL listed
is launched with each user-mode process.
appinitdlls complete.
----------------------------------------
Launching apppaths v.20120524
apppaths v.20120524
(Software) Gets content of App Paths subkeys

App Paths
Microsoft\Windows\CurrentVersion\App Paths

Sat Jun 21 22:40:14 2014 (UTC)
```

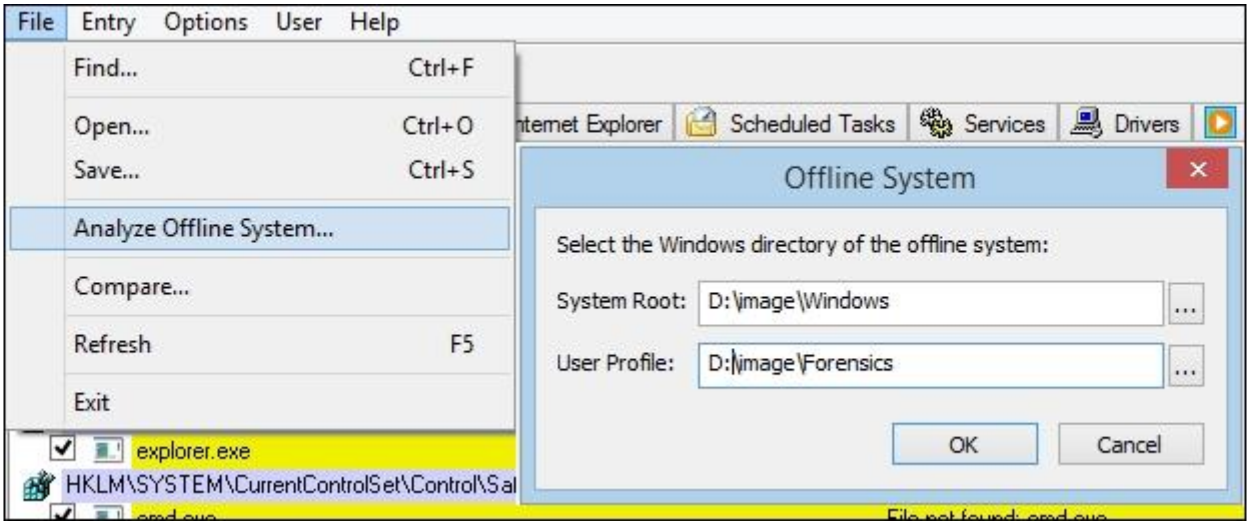


```
forensics@forensics:~$ regripper -r /mnt/hgfs/image/registry/system -p appcompatcache | more
Launching appcompatcache v.20130425
appcompatcache v.20130425
(System) Parse files from System hive Shim Cache

Signature: 0xbadc0fee
Win2K8R2/Win7, 64-bit
C:\Program Files\VMware\VMware Tools\resume-vm-default.bat
ModTime: Fri Mar 21 13:31:33 2014 Z

C:\Windows\system32\StikyNot.exe
ModTime: Tue Jul 14 01:39:46 2009 Z

C:\Windows\System32\fsquirt.exe
ModTime: Tue Jul 14 01:39:10 2009 Z
Executed

C:\Windows\SysWOW64\DllHost.exe
ModTime: Tue Jul 14 01:14:18 2009 Z
Executed

C:\Windows\System32\net.exe
ModTime: Tue Jul 14 01:39:25 2009 Z
Executed

C:\Windows\WinSxS\amd64_netfx-clrgc_b03f5f7f11d50a3a_6.1.7600.16385_none_ada52b8ba0da82ba\clrgc.exe
ModTime: Wed Jun 10 20:39:44 2009 Z
Executed

C:\Windows\syswow64\WOWReg32.exe
ModTime: Mon Jul 13 23:16:09 2009 Z
Executed
```



```
C:\Users\Alina\AppData\Local\Temp\malicious_name.exe
ModTime: Tue Feb  25 12:55:09 2015 Z
Executed
```



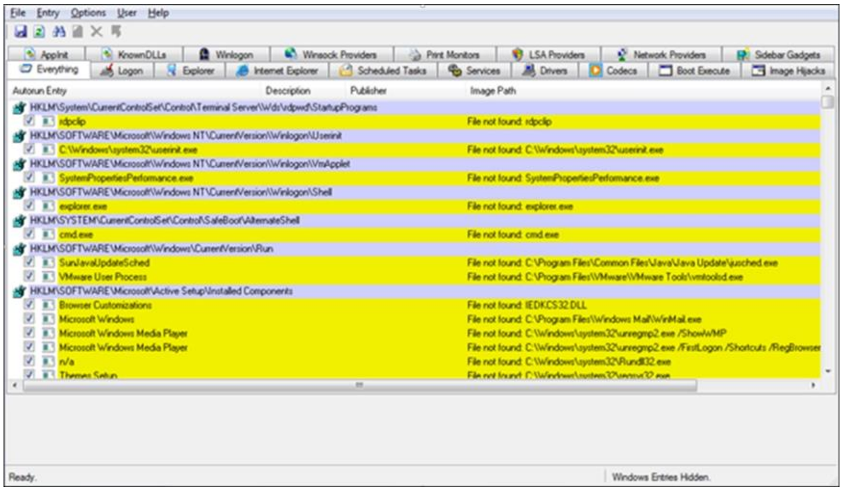


Offline System

Select the Windows directory of the offline system:

System Root: D:\image\Windows

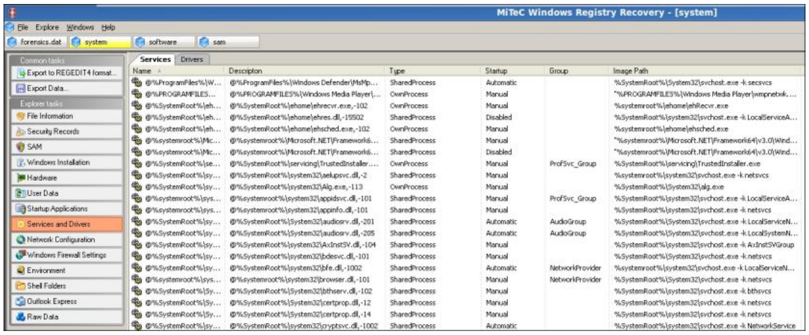
User Profile: D:\image\Forensics



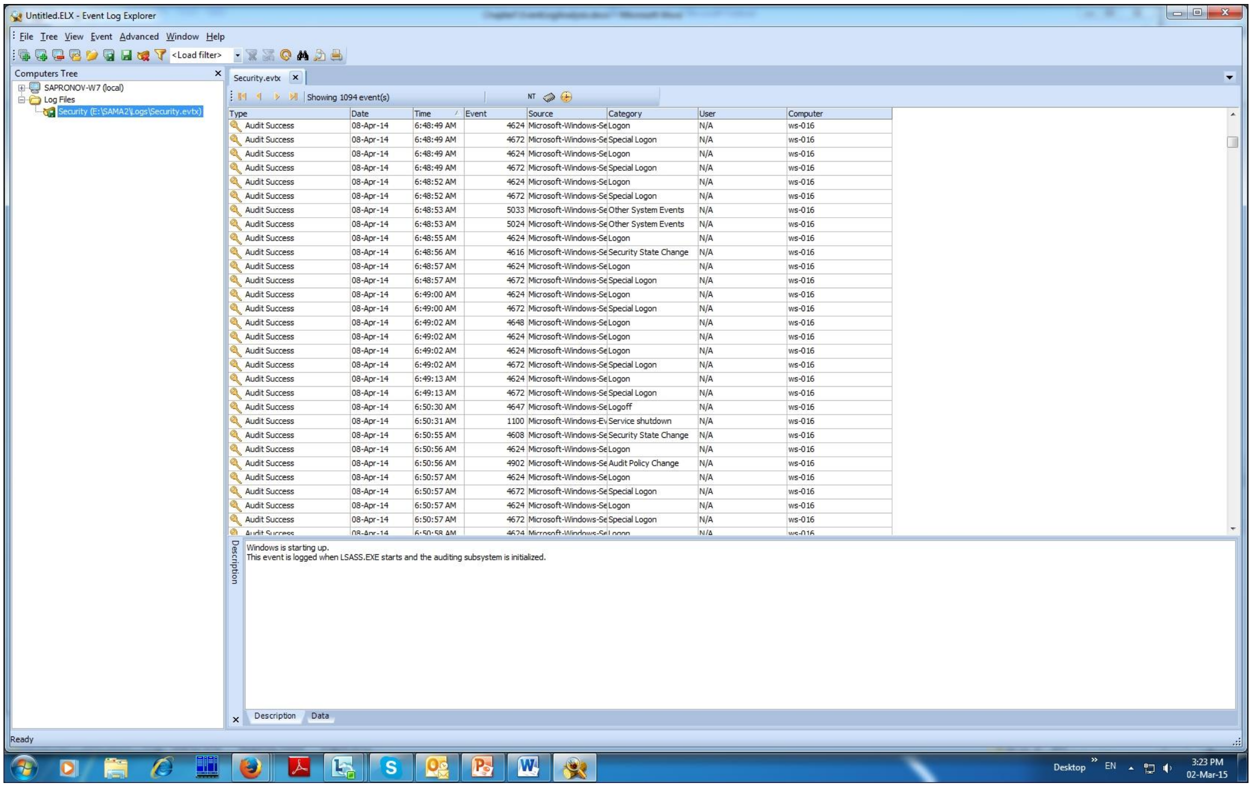
Autorun Entry	Description	Publisher	Image Path
HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\StartupPrograms			
☑ rdpclip			File not found: rdpclip
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit			
☑ C:\Windows\system32\userinit.exe			File not found: C:\Windows\system32\userinit.exe
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\VmApplet			
☑ SystemPropertiesPerformance.exe			File not found: SystemPropertiesPerformance.exe
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell			
☑ explorer.exe			File not found: explorer.exe
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell			
☑ cmd.exe			File not found: cmd.exe
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
☑ SunJavaUpdateSched			File not found: C:\Program Files\Common Files\Java\Java Update\jusched.exe
☑ VMware User Process			File not found: C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components			
☑ Browser Customizations			File not found: IEDKCS32.DLL
☑ Microsoft Windows			File not found: C:\Program Files\Windows Mail\WinMail.exe
☑ Microsoft Windows Media Player			File not found: C:\Windows\system32\unregmp2.exe /ShowWMP
☑ Microsoft Windows Media Player			File not found: C:\Windows\system32\unregmp2.exe /FirstLogon /Shortcuts /RegBrowser
☑ n/a			File not found: C:\Windows\system32\Rundll32.exe
☑ Themes Setup			File not found: C:\Windows\system32\regsvr32.exe

Ready.

Windows Entries Hidden.

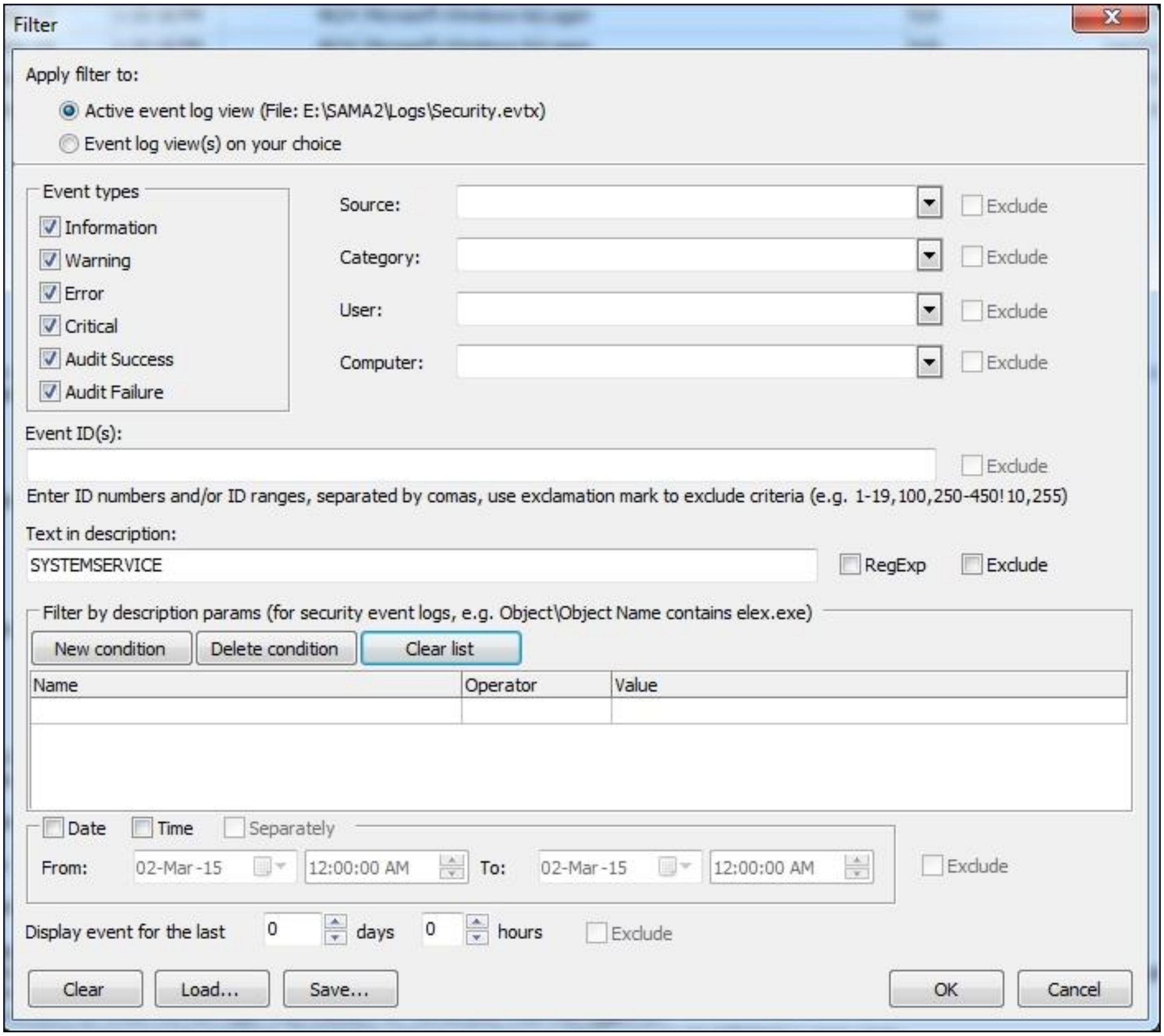


Name	Description	Type	Startup	Group	Image Path
@%ProgramFiles%\W...	@%ProgramFiles%\Windows Defender\MsMp...	SharedProcess	Automatic		%SystemRoot%\System32\svchost.exe -k secsvcs
@%PROGRAMFILES...	@%PROGRAMFILES%\Windows Media Player\...	OwnProcess	Manual		"%PROGRAMFILES%\Windows Media Player\wmpnetwk....
@%SystemRoot%\eh...	@%SystemRoot%\ehome\ehrecvr.exe,-102	OwnProcess	Manual		%systemroot%\ehome\ehRecvr.exe
@%SystemRoot%\eh...	@%SystemRoot%\ehome\ehres.dll,-15502	SharedProcess	Disabled		%SystemRoot%\system32\svchost.exe -k LocalServiceA...
@%SystemRoot%\eh...	@%SystemRoot%\ehome\ehsched.exe,-102	OwnProcess	Manual		%systemroot%\ehome\ehsched.exe
@%systemroot%\Mic...	@%systemroot%\Microsoft.NET\Framework6...	SharedProcess	Manual		"%systemroot%\Microsoft.NET\Framework64\v3.0\Wind...
@%systemroot%\Mic...	@%systemroot%\Microsoft.NET\Framework6...	SharedProcess	Disabled		"%systemroot%\Microsoft.NET\Framework64\v3.0\Wind...
@%SystemRoot%\se...	@%SystemRoot%\servicing\TrustedInstaller....	OwnProcess	Manual	ProfSvc_Group	%SystemRoot%\servicing\TrustedInstaller.exe
@%SystemRoot%\sy...	@%SystemRoot%\system32\aelupsvc.dll,-2	SharedProcess	Manual		%systemroot%\system32\svchost.exe -k netsvcs
@%SystemRoot%\sy...	@%SystemRoot%\system32\Alg.exe,-113	OwnProcess	Manual		%SystemRoot%\System32\alg.exe
@%systemroot%\sys...	@%systemroot%\system32\appidsvc.dll,-101	SharedProcess	Manual	ProfSvc_Group	%SystemRoot%\system32\svchost.exe -k LocalServiceA...
@%systemroot%\sys...	@%systemroot%\system32\appinfo.dll,-101	SharedProcess	Manual		%SystemRoot%\system32\svchost.exe -k netsvcs
@%SystemRoot%\sy...	@%SystemRoot%\System32\audiosrv.dll,-201	SharedProcess	Automatic	AudioGroup	%SystemRoot%\System32\svchost.exe -k LocalServiceN...
@%SystemRoot%\sy...	@%SystemRoot%\System32\audiosrv.dll,-205	SharedProcess	Automatic	AudioGroup	%SystemRoot%\System32\svchost.exe -k LocalSystemN...
@%SystemRoot%\sy...	@%SystemRoot%\system32\AxInstSV.dll,-104	SharedProcess	Manual		%SystemRoot%\system32\svchost.exe -k AxInstSVGroup
@%SystemRoot%\sy...	@%SystemRoot%\system32\bdesvc.dll,-101	SharedProcess	Manual		%SystemRoot%\System32\svchost.exe -k netsvcs
@%SystemRoot%\sy...	@%SystemRoot%\system32\bfe.dll,-1002	SharedProcess	Automatic	NetworkProvider	%systemroot%\system32\svchost.exe -k LocalServiceN...
@%systemroot%\sys...	@%systemroot%\system32\browser.dll,-101	SharedProcess	Manual	NetworkProvider	%SystemRoot%\System32\svchost.exe -k netsvcs
@%SystemRoot%\Sy...	@%SystemRoot%\System32\bthserv.dll,-102	SharedProcess	Manual		%SystemRoot%\system32\svchost.exe -k bthsvcs
@%SystemRoot%\Sy...	@%SystemRoot%\System32\certprop.dll,-12	SharedProcess	Manual		%SystemRoot%\system32\svchost.exe -k netsvcs
@%SystemRoot%\Sy...	@%SystemRoot%\System32\certprop.dll,-14	SharedProcess	Manual		%SystemRoot%\system32\svchost.exe -k netsvcs
@%SystemRoot%\sy...	@%SystemRoot%\system32\cryptsvc.dll,-1002	SharedProcess	Automatic		%SystemRoot%\system32\svchost.exe -k NetworkService



Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	08-Apr-14	6:48:49 AM	4624	Microsoft-Windows-Se	Logon	N/A	ws-016
Audit Success	08-Apr-14	6:48:49 AM	4672	Microsoft-Windows-Se	Special Logon	N/A	ws-016
Audit Success	08-Apr-14	6:48:49 AM	4624	Microsoft-Windows-Se	Logon	N/A	ws-016
Audit Success	08-Apr-14	6:48:49 AM	4672	Microsoft-Windows-Se	Special Logon	N/A	ws-016
Audit Success	08-Apr-14	6:48:52 AM	4624	Microsoft-Windows-Se	Logon	N/A	ws-016
Audit Success	08-Apr-14	6:48:52 AM	4672	Microsoft-Windows-Se	Special Logon	N/A	ws-016
Audit Success	08-Apr-14	6:48:53 AM	5033	Microsoft-Windows-Se	Other System Events	N/A	ws-016
Audit Success	08-Apr-14	6:48:53 AM	5024	Microsoft-Windows-Se	Other System Events	N/A	ws-016
Audit Success	08-Apr-14	6:48:55 AM	4624	Microsoft-Windows-Se	Logon	N/A	ws-016
Audit Success	08-Apr-14	6:48:56 AM	4616	Microsoft-Windows-Se	Security State Change	N/A	ws-016
Audit Success	08-Apr-14	6:48:57 AM	4624	Microsoft-Windows-Se	Logon	N/A	ws-016
Audit Success	08-Apr-14	6:48:57 AM	4672	Microsoft-Windows-Se	Special Logon	N/A	ws-016
Audit Success	08-Apr-14	6:49:00 AM	4624	Microsoft-Windows-Se	Logon	N/A	ws-016
Audit Success	08-Apr-14	6:49:00 AM	4672	Microsoft-Windows-Se	Special Logon	N/A	ws-016
Audit Success	08-Apr-14	6:49:02 AM	4648	Microsoft-Windows-Se	Logon	N/A	ws-016
Audit Success	08-Apr-14	6:49:02 AM	4624	Microsoft-Windows-Se	Logon	N/A	ws-016
Audit Success	08-Apr-14	6:49:02 AM	4624	Microsoft-Windows-Se	Logon	N/A	ws-016
Audit Success	08-Apr-14	6:49:02 AM	4672	Microsoft-Windows-Se	Special Logon	N/A	ws-016
Audit Success	08-Apr-14	6:49:13 AM	4624	Microsoft-Windows-Se	Logon	N/A	ws-016
Audit Success	08-Apr-14	6:49:13 AM	4672	Microsoft-Windows-Se	Special Logon	N/A	ws-016
Audit Success	08-Apr-14	6:50:30 AM	4647	Microsoft-Windows-Se	Logoff	N/A	ws-016
Audit Success	08-Apr-14	6:50:31 AM	1100	Microsoft-Windows-Ev	Service shutdown	N/A	ws-016
Audit Success	08-Apr-14	6:50:55 AM	4608	Microsoft-Windows-Se	Security State Change	N/A	ws-016
Audit Success	08-Apr-14	6:50:56 AM	4624	Microsoft-Windows-Se	Logon	N/A	ws-016
Audit Success	08-Apr-14	6:50:56 AM	4902	Microsoft-Windows-Se	Audit Policy Change	N/A	ws-016
Audit Success	08-Apr-14	6:50:57 AM	4624	Microsoft-Windows-Se	Logon	N/A	ws-016
Audit Success	08-Apr-14	6:50:57 AM	4672	Microsoft-Windows-Se	Special Logon	N/A	ws-016
Audit Success	08-Apr-14	6:50:57 AM	4624	Microsoft-Windows-Se	Logon	N/A	ws-016
Audit Success	08-Apr-14	6:50:57 AM	4672	Microsoft-Windows-Se	Special Logon	N/A	ws-016
Audit Success	08-Apr-14	6:50:58 AM	4624	Microsoft-Windows-Se	Logon	N/A	ws-016

Windows is starting up.
This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.



Filter

Apply filter to:

● Active event log view (File: E:\SAMA2\Logs\Security.evtx)

○ Event log view(s) on your choice

Event types

☑ Information

☑ Warning

☑ Error

☑ Critical

☑ Audit Success

☑ Audit Failure

Source: □ Exclude

Category: □ Exclude

User: □ Exclude

Computer: □ Exclude

Event ID(s): □ Exclude

Enter ID numbers and/or ID ranges, separated by comas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description: SYSTEMSERVICE □ RegExp □ Exclude

Filter by description params (for security event logs, e.g. Object\Object Name contains elex.exe)

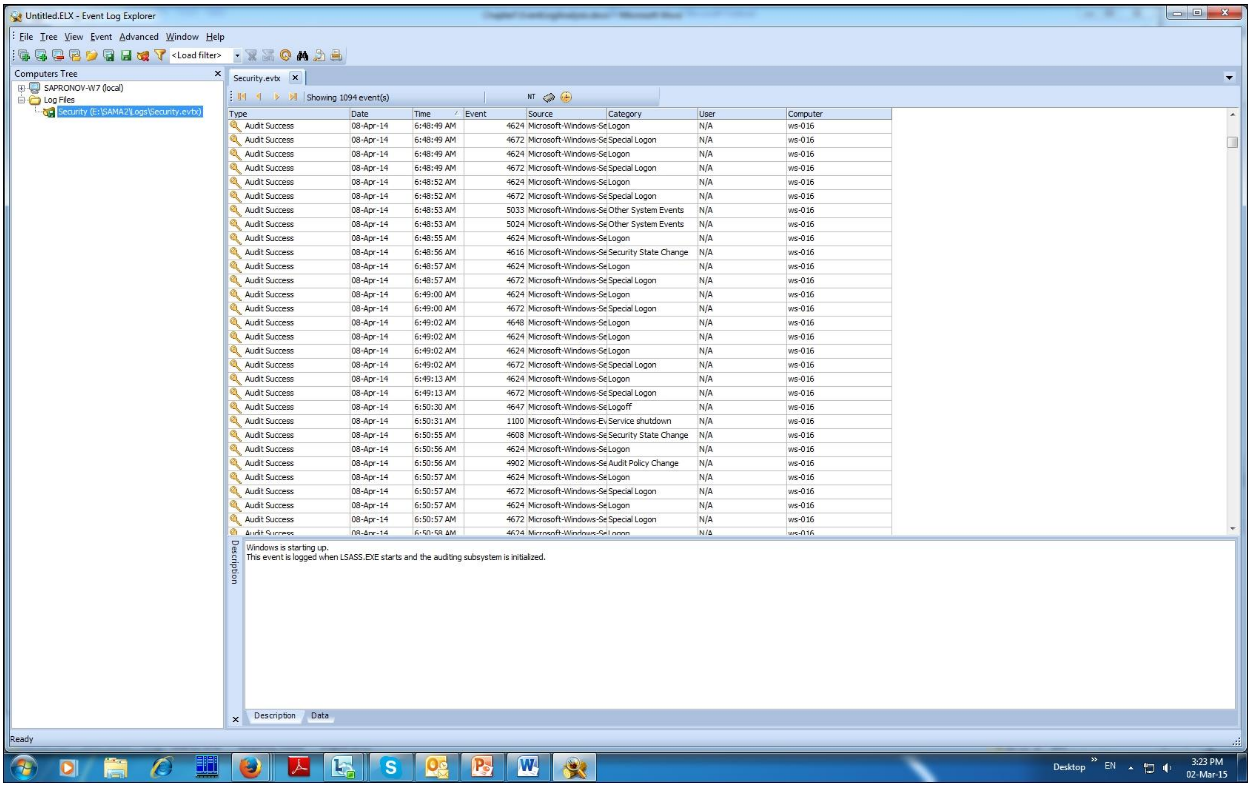
Name	Operator	Value

□ Date □ Time □ Separately

From: 02-Mar-15 12:00:00 AM To: 02-Mar-15 12:00:00 AM □ Exclude

Display event for the last 0 days 0 hours □ Exclude

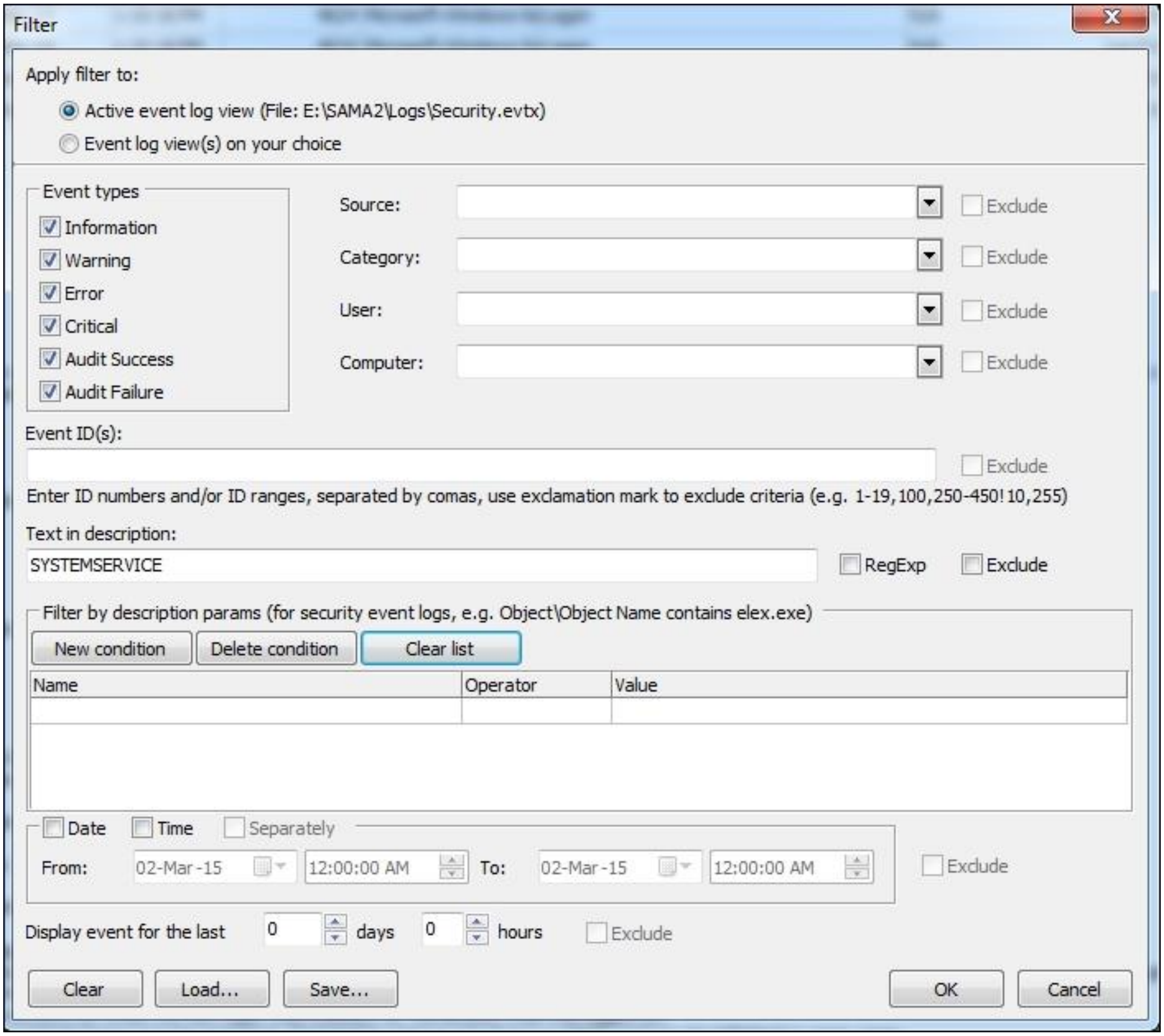
Chapter 8: Event Log Analysis



Showing 1094 event(s)

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	08-Apr-14	6:48:49 AM	4624	Microsoft-Windows-Se	Logon	N/A	ws-016
Audit Success	08-Apr-14	6:48:49 AM	4672	Microsoft-Windows-Se	Special Logon	N/A	ws-016
Audit Success	08-Apr-14	6:48:49 AM	4624	Microsoft-Windows-Se	Logon	N/A	ws-016
Audit Success	08-Apr-14	6:48:49 AM	4672	Microsoft-Windows-Se	Special Logon	N/A	ws-016
Audit Success	08-Apr-14	6:48:52 AM	4624	Microsoft-Windows-Se	Logon	N/A	ws-016
Audit Success	08-Apr-14	6:48:52 AM	4672	Microsoft-Windows-Se	Special Logon	N/A	ws-016
Audit Success	08-Apr-14	6:48:53 AM	5033	Microsoft-Windows-Se	Other System Events	N/A	ws-016
Audit Success	08-Apr-14	6:48:53 AM	5024	Microsoft-Windows-Se	Other System Events	N/A	ws-016
Audit Success	08-Apr-14	6:48:55 AM	4624	Microsoft-Windows-Se	Logon	N/A	ws-016
Audit Success	08-Apr-14	6:48:56 AM	4616	Microsoft-Windows-Se	Security State Change	N/A	ws-016
Audit Success	08-Apr-14	6:48:57 AM	4624	Microsoft-Windows-Se	Logon	N/A	ws-016
Audit Success	08-Apr-14	6:48:57 AM	4672	Microsoft-Windows-Se	Special Logon	N/A	ws-016
Audit Success	08-Apr-14	6:49:00 AM	4624	Microsoft-Windows-Se	Logon	N/A	ws-016
Audit Success	08-Apr-14	6:49:00 AM	4672	Microsoft-Windows-Se	Special Logon	N/A	ws-016
Audit Success	08-Apr-14	6:49:02 AM	4648	Microsoft-Windows-Se	Logon	N/A	ws-016
Audit Success	08-Apr-14	6:49:02 AM	4624	Microsoft-Windows-Se	Logon	N/A	ws-016
Audit Success	08-Apr-14	6:49:02 AM	4624	Microsoft-Windows-Se	Logon	N/A	ws-016
Audit Success	08-Apr-14	6:49:02 AM	4672	Microsoft-Windows-Se	Special Logon	N/A	ws-016
Audit Success	08-Apr-14	6:49:13 AM	4624	Microsoft-Windows-Se	Logon	N/A	ws-016
Audit Success	08-Apr-14	6:49:13 AM	4672	Microsoft-Windows-Se	Special Logon	N/A	ws-016
Audit Success	08-Apr-14	6:50:30 AM	4647	Microsoft-Windows-Se	Logoff	N/A	ws-016
Audit Success	08-Apr-14	6:50:31 AM	1100	Microsoft-Windows-Ev	Service shutdown	N/A	ws-016
Audit Success	08-Apr-14	6:50:55 AM	4608	Microsoft-Windows-Se	Security State Change	N/A	ws-016
Audit Success	08-Apr-14	6:50:56 AM	4624	Microsoft-Windows-Se	Logon	N/A	ws-016
Audit Success	08-Apr-14	6:50:56 AM	4902	Microsoft-Windows-Se	Audit Policy Change	N/A	ws-016
Audit Success	08-Apr-14	6:50:57 AM	4624	Microsoft-Windows-Se	Logon	N/A	ws-016
Audit Success	08-Apr-14	6:50:57 AM	4672	Microsoft-Windows-Se	Special Logon	N/A	ws-016
Audit Success	08-Apr-14	6:50:57 AM	4624	Microsoft-Windows-Se	Logon	N/A	ws-016
Audit Success	08-Apr-14	6:50:57 AM	4672	Microsoft-Windows-Se	Special Logon	N/A	ws-016
Audit Success	08-Apr-14	6:50:58 AM	4624	Microsoft-Windows-Se	Logon	N/A	ws-016

Windows is starting up.
This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.



Filter

Apply filter to:

● Active event log view (File: E:\SAMA2\Logs\Security.evtx)

○ Event log view(s) on your choice

Event types

☑ Information

☑ Warning

☑ Error

☑ Critical

☑ Audit Success

☑ Audit Failure

Source: □ Exclude

Category: □ Exclude

User: □ Exclude

Computer: □ Exclude

Event ID(s): □ Exclude

Enter ID numbers and/or ID ranges, separated by comas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description: SYSTEMSERVICE □ RegExp □ Exclude

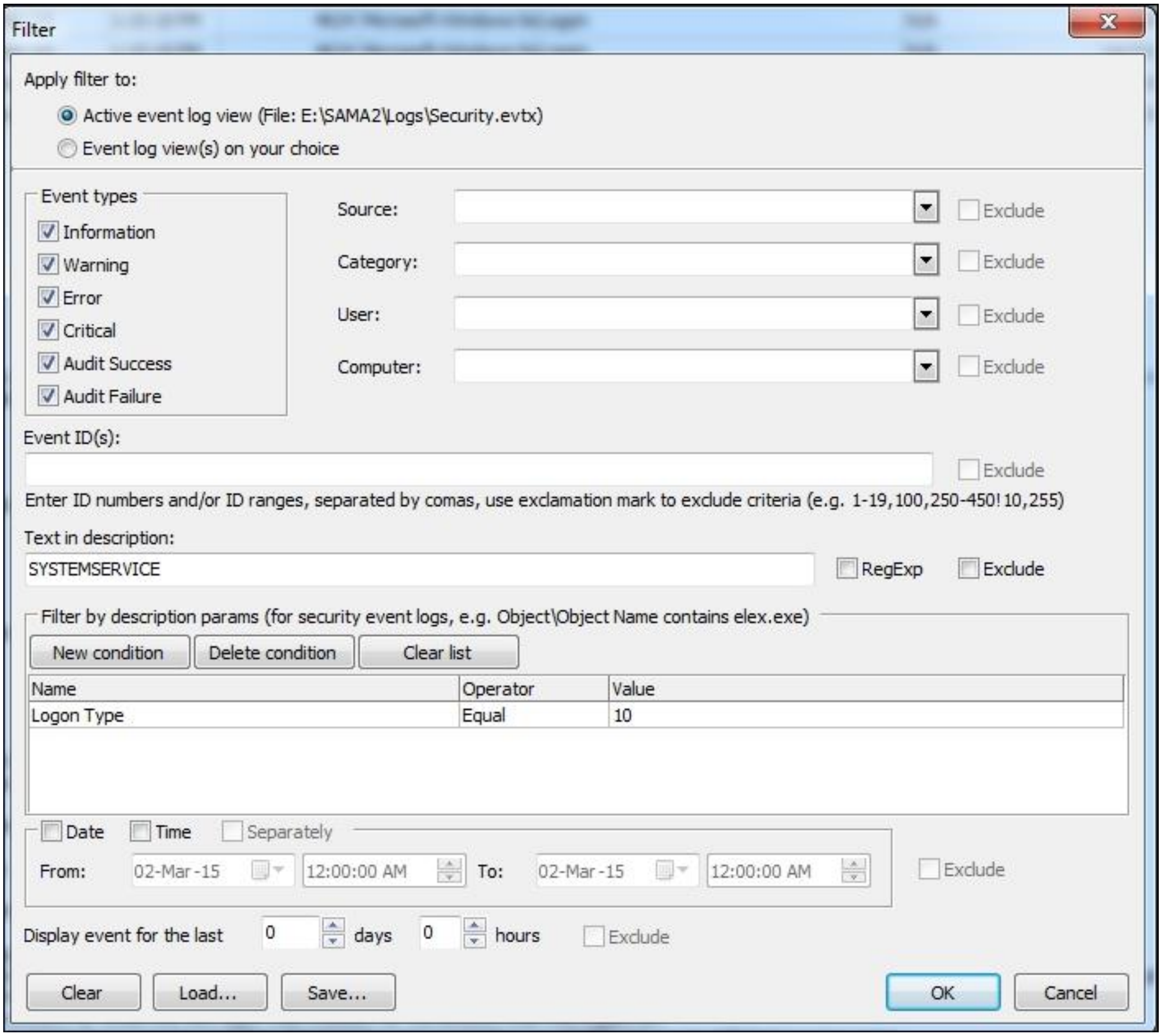
Filter by description params (for security event logs, e.g. Object\Object Name contains elex.exe)

Name	Operator	Value

□ Date □ Time □ Separately

From: 02-Mar-15 12:00:00 AM To: 02-Mar-15 12:00:00 AM □ Exclude

Display event for the last 0 days 0 hours □ Exclude



Filter

Apply filter to:

● Active event log view (File: E:\SAMA2\Logs\Security.evtx)
○ Event log view(s) on your choice

Event types
☑ Information
☑ Warning
☑ Error
☑ Critical
☑ Audit Success
☑ Audit Failure

Source: □ Exclude
Category: □ Exclude
User: □ Exclude
Computer: □ Exclude

Event ID(s): □ Exclude

Enter ID numbers and/or ID ranges, separated by comas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description: SYSTEMSERVICE □ RegExp □ Exclude

Filter by description params (for security event logs, e.g. Object\Object Name contains elex.exe)

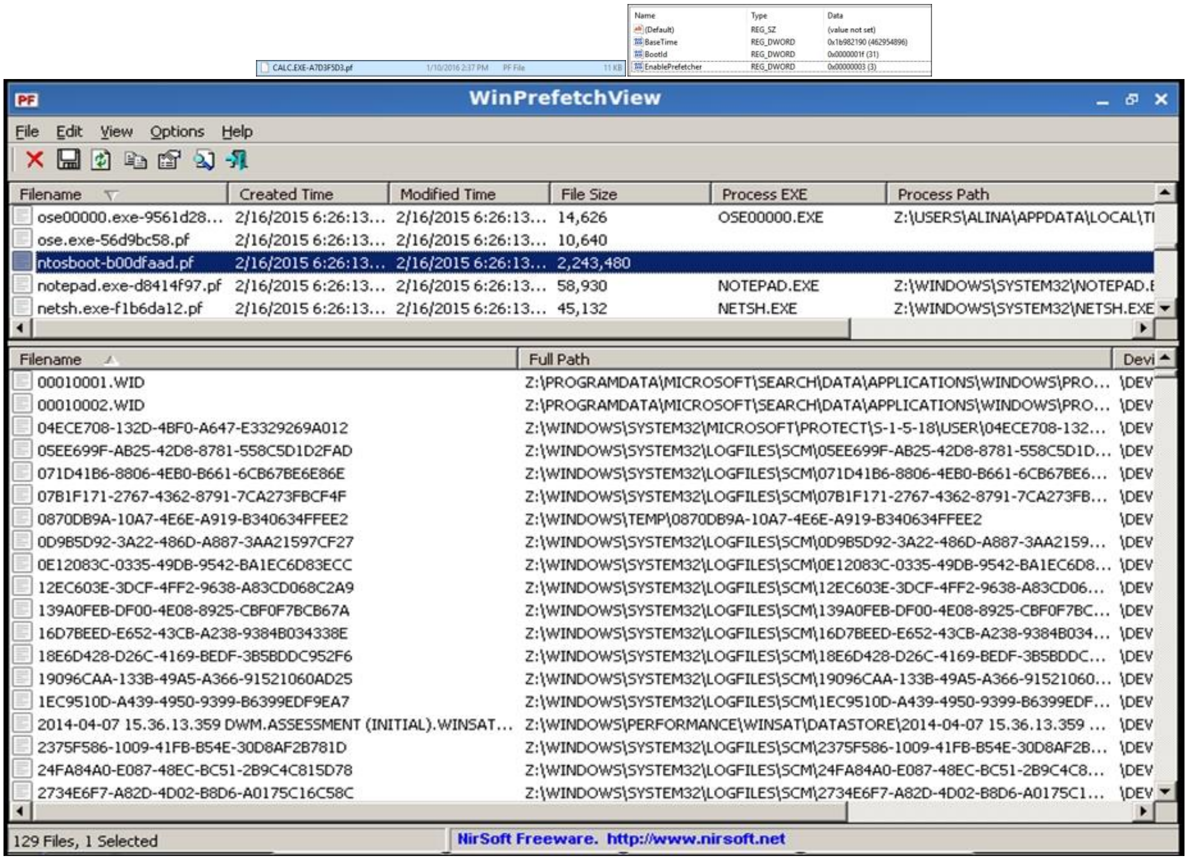
Name	Operator	Value
Logon Type	Equal	10

□ Date □ Time □ Separately

From: 02-Mar-15 12:00:00 AM To: 02-Mar-15 12:00:00 AM □ Exclude

Display event for the last 0 days 0 hours □ Exclude

Chapter 9: Windows Files



CALC.EXE-A7D3F5D3.pf	1/10/2016 2:37 PM	PF File	11 KB

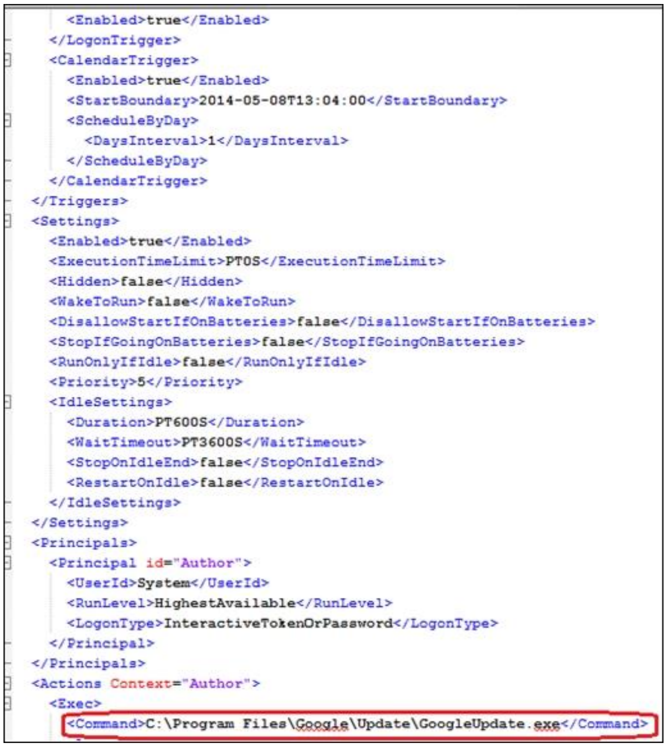
Name	Type	Data
(Default)	REG_SZ	(value not set)
BaseTime	REG_DWORD	0x1b982190 (462954896)
BootId	REG_DWORD	0x0000001f (31)
EnablePrefetcher	REG_DWORD	0x00000003 (3)

Filename	Created Time	Modified Time	File Size	Process EXE	Process Path
ose00000.exe-9561d28...	2/16/2015 6:26:13...	2/16/2015 6:26:13...	14,626	OSE00000.EXE	Z:\USERS\ALINA\APPDATA\LOCAL\TI
ose.exe-56d9bc58.pf	2/16/2015 6:26:13...	2/16/2015 6:26:13...	10,640		
ntosboot-b00dfaad.pf	2/16/2015 6:26:13...	2/16/2015 6:26:13...	2,243,480		
notepad.exe-d8414f97.pf	2/16/2015 6:26:13...	2/16/2015 6:26:13...	58,930	NOTEPAD.EXE	Z:\WINDOWS\SYSTEM32\NOTEPAD.E
netsh.exe-f1b6da12.pf	2/16/2015 6:26:13...	2/16/2015 6:26:13...	45,132	NETSH.EXE	Z:\WINDOWS\SYSTEM32\NETSH.EXE

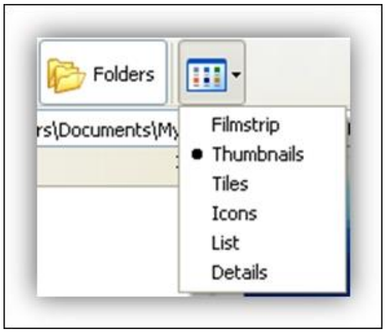
Filename	Full Path	Devi
00010001.WID	Z:\PROGRAMDATA\MICROSOFT\SEARCH\DATA\APPLICATIONS\WINDOWS\PRO...	\DEV
00010002.WID	Z:\PROGRAMDATA\MICROSOFT\SEARCH\DATA\APPLICATIONS\WINDOWS\PRO...	\DEV
04ECE708-132D-4BF0-A647-E3329269A012	Z:\WINDOWS\SYSTEM32\MICROSOFT\PROTECT\S-1-5-18\USER\04ECE708-132...	\DEV
05EE699F-AB25-42D8-8781-558C5D1D2FAD	Z:\WINDOWS\SYSTEM32\LOGFILES\SCM\05EE699F-AB25-42D8-8781-558C5D1D...	\DEV
071D41B6-8806-4EB0-B661-6CB67BE6E86E	Z:\WINDOWS\SYSTEM32\LOGFILES\SCM\071D41B6-8806-4EB0-B661-6CB67BE6...	\DEV
07B1F171-2767-4362-8791-7CA273FBCF4F	Z:\WINDOWS\SYSTEM32\LOGFILES\SCM\07B1F171-2767-4362-8791-7CA273FB...	\DEV
0870DB9A-10A7-4E6E-A919-B340634FFEE2	Z:\WINDOWS\TEMP\0870DB9A-10A7-4E6E-A919-B340634FFEE2	\DEV
0D9B5D92-3A22-486D-A887-3AA21597CF27	Z:\WINDOWS\SYSTEM32\LOGFILES\SCM\0D9B5D92-3A22-486D-A887-3AA2159...	\DEV
0E12083C-0335-49DB-9542-BA1EC6D83ECC	Z:\WINDOWS\SYSTEM32\LOGFILES\SCM\0E12083C-0335-49DB-9542-BA1EC6D8...	\DEV
12EC603E-3DCF-4FF2-9638-A83CD068C2A9	Z:\WINDOWS\SYSTEM32\LOGFILES\SCM\12EC603E-3DCF-4FF2-9638-A83CD06...	\DEV
139A0FEB-DF00-4E08-8925-CBF0F7BCB67A	Z:\WINDOWS\SYSTEM32\LOGFILES\SCM\139A0FEB-DF00-4E08-8925-CBF0F7BC...	\DEV
16D7BEED-E652-43CB-A238-9384B034338E	Z:\WINDOWS\SYSTEM32\LOGFILES\SCM\16D7BEED-E652-43CB-A238-9384B034...	\DEV
18E6D428-D26C-4169-BEDF-3B5BDDC952F6	Z:\WINDOWS\SYSTEM32\LOGFILES\SCM\18E6D428-D26C-4169-BEDF-3B5BDDC...	\DEV
19096CAA-133B-49A5-A366-91521060AD25	Z:\WINDOWS\SYSTEM32\LOGFILES\SCM\19096CAA-133B-49A5-A366-91521060...	\DEV
1EC9510D-A439-4950-9399-B6399EDF9EA7	Z:\WINDOWS\SYSTEM32\LOGFILES\SCM\1EC9510D-A439-4950-9399-B6399EDF...	\DEV
2014-04-07 15.36.13.359 DWM.ASSESSMENT (INITIAL).WINSAT...	Z:\WINDOWS\PERFORMANCE\WINSAT\DATASTORE\2014-04-07 15.36.13.359 ...	\DEV
2375F586-1009-41FB-B54E-30D8AF2B781D	Z:\WINDOWS\SYSTEM32\LOGFILES\SCM\2375F586-1009-41FB-B54E-30D8AF2B...	\DEV
24FA84A0-E087-48EC-BC51-2B9C4C815D78	Z:\WINDOWS\SYSTEM32\LOGFILES\SCM\24FA84A0-E087-48EC-BC51-2B9C4C8...	\DEV
2734E6F7-A82D-4D02-B8D6-A0175C16C58C	Z:\WINDOWS\SYSTEM32\LOGFILES\SCM\2734E6F7-A82D-4D02-B8D6-A0175C1...	\DEV

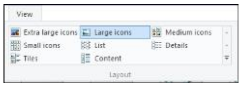
129 Files, 1 Selected

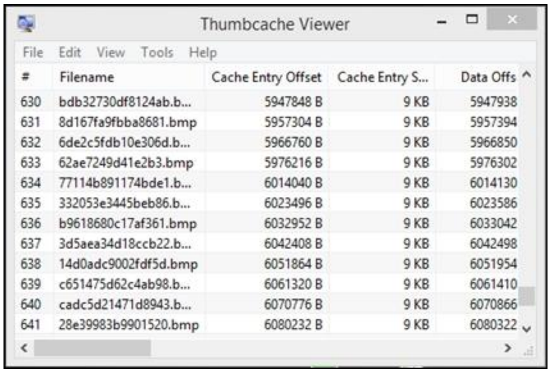
NirSoft Freeware. http://www.nirsoft.net



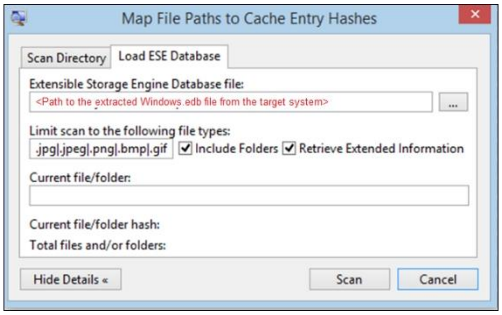
```
      <Enabled>true</Enabled>
    </LogonTrigger>
    <CalendarTrigger>
      <Enabled>true</Enabled>
      <StartBoundary>2014-05-08T13:04:00</StartBoundary>
      <ScheduleByDay>
        <DaysInterval>1</DaysInterval>
      </ScheduleByDay>
    </CalendarTrigger>
  </Triggers>
  <Settings>
    <Enabled>true</Enabled>
    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>
    <Hidden>false</Hidden>
    <WakeToRun>false</WakeToRun>
    <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>
    <RunOnlyIfIdle>false</RunOnlyIfIdle>
    <Priority>5</Priority>
    <IdleSettings>
      <Duration>PT600S</Duration>
      <WaitTimeout>PT3600S</WaitTimeout>
      <StopOnIdleEnd>false</StopOnIdleEnd>
      <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
  </Settings>
  <Principals>
    <Principal id="Author">
      <UserId>System</UserId>
      <RunLevel>HighestAvailable</RunLevel>
      <LogonType>InteractiveTokenOrPassword</LogonType>
    </Principal>
  </Principals>
  <Actions Context="Author">
    <Exec>
      <Command>C:\Program Files\Google\Update\GoogleUpdate.exe</Command>
```







#	Filename	Cache Entry Offset	Cache Entry S...	Data Offs
630	bdb32730df8124ab.b...	5947848 B	9 KB	5947938
631	8d167fa9fbba8681.bmp	5957304 B	9 KB	5957394
632	6de2c5fdb10e306d.b...	5966760 B	9 KB	5966850
633	62ae7249d41e2b3.bmp	5976216 B	9 KB	5976302
634	77114b891174bde1.b...	6014040 B	9 KB	6014130
635	332053e3445beb86.b...	6023496 B	9 KB	6023586
636	b9618680c17af361.bmp	6032952 B	9 KB	6033042
637	3d5aea34d18ccb22.b...	6042408 B	9 KB	6042498
638	14d0adc9002fdf5d.bmp	6051864 B	9 KB	6051954
639	c651475d62c4ab98.b...	6061320 B	9 KB	6061410
640	cadc5d21471d8943.b...	6070776 B	9 KB	6070866
641	28e39983b9901520.bmp	6080232 B	9 KB	6080322



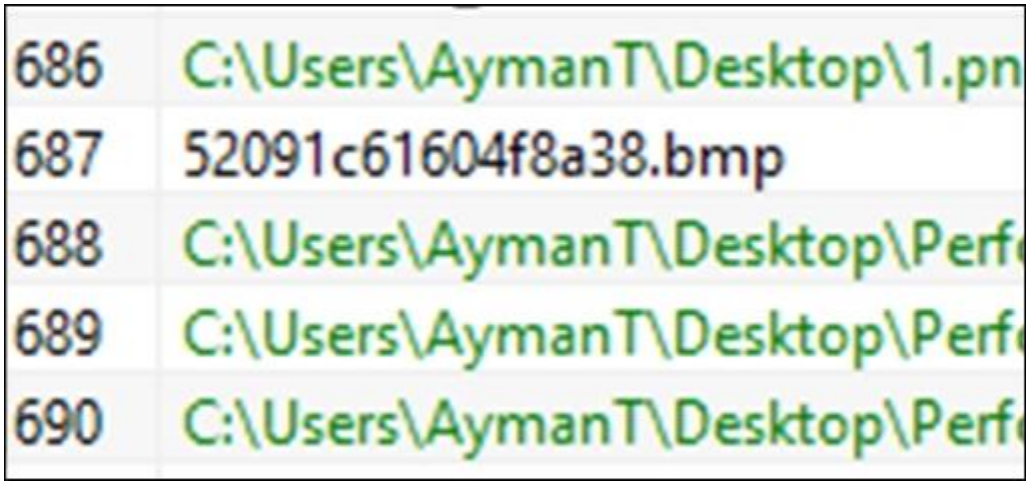
Extensible Storage Engine Database file:
<Path to the extracted Windows.edb file from the target system>

Limit scan to the following file types:
.jpg|.jpeg|.png|.bmp|.gif ☑ Include Folders ☑ Retrieve Extended Information

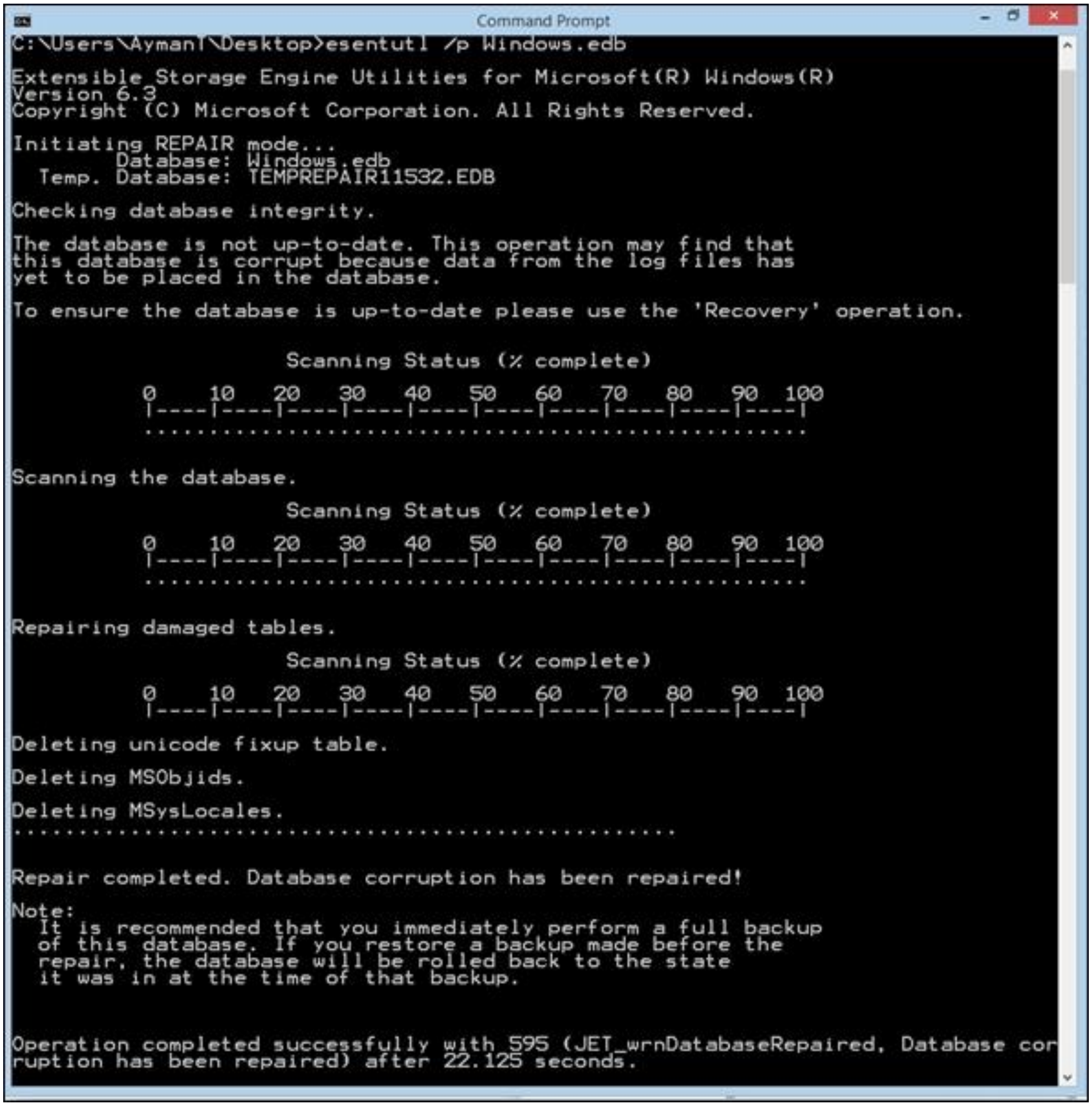
Current file/folder:

Current file/folder hash:

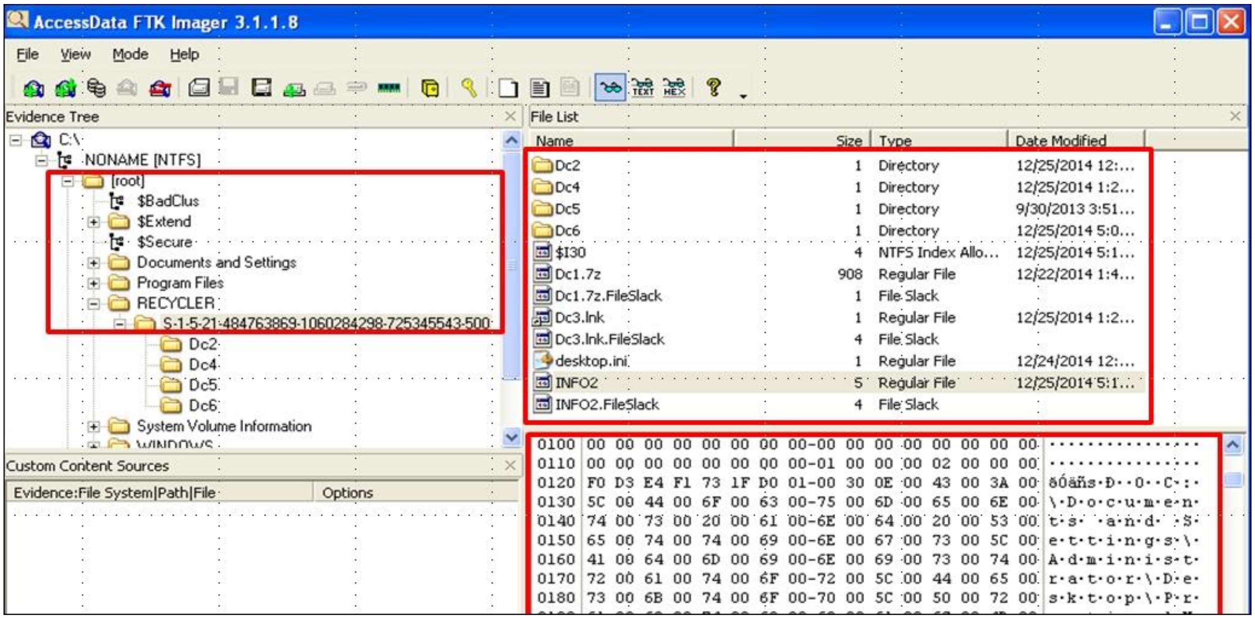
Total files and/or folders:



686	C:\Users\AymanT\Desktop\1.pn
687	52091c61604f8a38.bmp
688	C:\Users\AymanT\Desktop\Perf
689	C:\Users\AymanT\Desktop\Perf
690	C:\Users\AymanT\Desktop\Perf



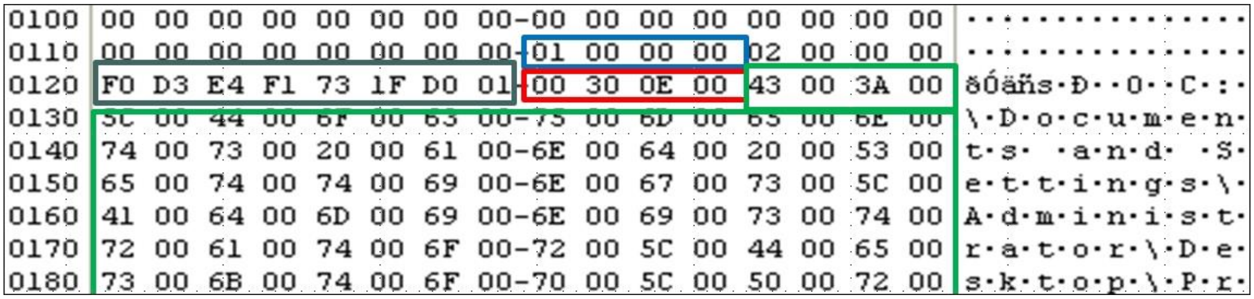
```
C:\Users\AymanT\Desktop>esentutl /p Windows.edb

Extensible Storage Engine Utilities for Microsoft(R) Windows(R)
Version 6.3
Copyright (C) Microsoft Corporation. All Rights Reserved.

Initiating REPAIR mode...
        Database: Windows.edb
  Temp. Database: TEMPREPAIR11532.EDB

Checking database integrity.

The database is not up-to-date. This operation may find that
this database is corrupt because data from the log files has
yet to be placed in the database.

To ensure the database is up-to-date please use the 'Recovery' operation.


                     Scanning Status (% complete)

          0    10   20   30   40   50   60   70   80   90  100
          |----|----|----|----|----|----|----|----|----|----|
          ...................................................


Scanning the database.

                     Scanning Status (% complete)

          0    10   20   30   40   50   60   70   80   90  100
          |----|----|----|----|----|----|----|----|----|----|
          ...................................................


Repairing damaged tables.

                     Scanning Status (% complete)

          0    10   20   30   40   50   60   70   80   90  100
          |----|----|----|----|----|----|----|----|----|----|

Deleting unicode fixup table.

Deleting MSObjids.

Deleting MSysLocales.
...................................................


Repair completed. Database corruption has been repaired!

Note:
  It is recommended that you immediately perform a full backup
  of this database. If you restore a backup made before the
  repair, the database will be rolled back to the state
  it was in at the time of that backup.



Operation completed successfully with 595 (JET_wrnDatabaseRepaired, Database cor
ruption has been repaired) after 22.125 seconds.
```



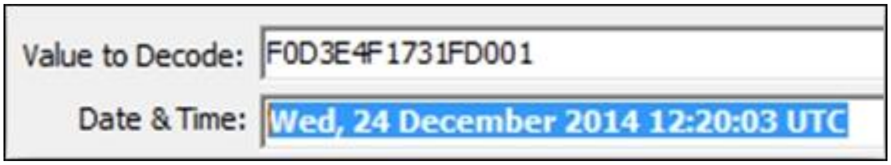
```
C:\
  NONAME [NTFS]
    [root]
      $BadClus
      $Extend
      $Secure
      Documents and Settings
      Program Files
      RECYCLER
        S-1-5-21-484763869-1060284298-725345543-500
          Dc2
          Dc4
          Dc5
          Dc6
      System Volume Information
      WINDOWS
```

Name	Size	Type	Date Modified
Dc2	1	Directory	12/25/2014 12:...
Dc4	1	Directory	12/25/2014 1:2...
Dc5	1	Directory	9/30/2013 3:51...
Dc6	1	Directory	12/25/2014 5:0...
$I30	4	NTFS Index Allo...	12/25/2014 5:1...
Dc1.7z	908	Regular File	12/22/2014 1:4...
Dc1.7z.FileSlack	1	File Slack	
Dc3.lnk	1	Regular File	12/25/2014 1:2...
Dc3.lnk.FileSlack	4	File Slack	
desktop.ini	1	Regular File	12/24/2014 12:...
INFO2	5	Regular File	12/25/2014 5:1...
INFO2.FileSlack	4	File Slack	

```
0100 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0110 00 00 00 00 00 00 00 00-01 00 00 00 02 00 00 00 ................
0120 F0 D3 E4 F1 73 1F D0 01-00 30 0E 00 43 00 3A 00 ðÓäñs·Ð··0··C·:·
0130 5C 00 44 00 6F 00 63 00-75 00 6D 00 65 00 6E 00 \·D·o·c·u·m·e·n·
0140 74 00 73 00 20 00 61 00-6E 00 64 00 20 00 53 00 t·s· ·a·n·d· ·S·
0150 65 00 74 00 74 00 69 00-6E 00 67 00 73 00 5C 00 e·t·t·i·n·g·s·\·
0160 41 00 64 00 6D 00 69 00-6E 00 69 00 73 00 74 00 A·d·m·i·n·i·s·t·
0170 72 00 61 00 74 00 6F 00-72 00 5C 00 44 00 65 00 r·a·t·o·r·\·D·e·
0180 73 00 6B 00 74 00 6F 00-70 00 5C 00 50 00 72 00 s·k·t·o·p·\·P·r·
```

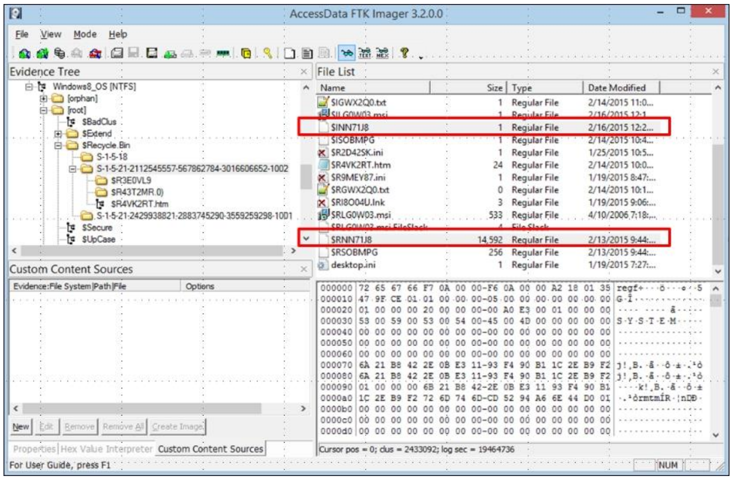


```
0100 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0110 00 00 00 00 00 00 00 00-01 00 00 00 02 00 00 00 ................
0120 F0 D3 E4 F1 73 1F D0 01-00 30 0E 00 43 00 3A 00 ðÓäñs·Ð··0··C·:·
0130 5C 00 44 00 6F 00 63 00-75 00 6D 00 65 00 6E 00 \·D·o·c·u·m·e·n·
0140 74 00 73 00 20 00 61 00-6E 00 64 00 20 00 53 00 t·s· ·a·n·d· ·S·
0150 65 00 74 00 74 00 69 00-6E 00 67 00 73 00 5C 00 e·t·t·i·n·g·s·\·
0160 41 00 64 00 6D 00 69 00-6E 00 69 00 73 00 74 00 A·d·m·i·n·i·s·t·
0170 72 00 61 00 74 00 6F 00-72 00 5C 00 44 00 65 00 r·a·t·o·r·\·D·e·
0180 73 00 6B 00 74 00 6F 00-70 00 5C 00 50 00 72 00 s·k·t·o·p·\·P·r·
```



Value to Decode: F0D3E4F1731FD001

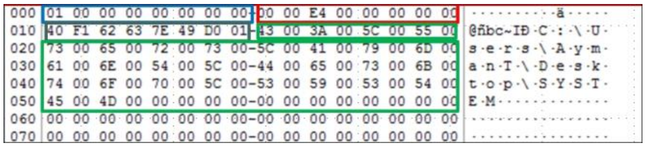
Date & Time: Wed, 24 December 2014 12:20:03 UTC



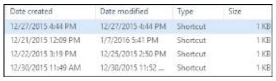
Name	Size	Type	Date Modified
$IGWX2Q0.txt	1	Regular File	2/14/2015 11:0...
$ILG0W03.msi	1	Regular File	2/16/2015 12:1...
$INN71J8	1	Regular File	2/16/2015 12:2...
$ISOBMPG	1	Regular File	2/14/2015 10:4...
$R2D42SK.ini	1	Regular File	1/25/2015 10:5...
$R4VK2RT.htm	24	Regular File	2/14/2015 10:0...
$R9MEY87.ini	1	Regular File	1/19/2015 8:47:...
$RGWX2Q0.txt	0	Regular File	2/14/2015 10:1...
$RI8O04U.lnk	3	Regular File	1/19/2015 9:06:...
$RLG0W03.msi	533	Regular File	4/10/2006 7:18:...
$RLG0W03.msi.FileSlack	4	File Slack	
$RNN71J8	14,592	Regular File	2/13/2015 9:44:...
$RSOBMPG	256	Regular File	2/13/2015 9:44:...
desktop.ini	1	Regular File	1/19/2015 7:27:...

```
000000 72 65 67 66 F7 0A 00 00-F6 0A 00 00 A2 18 01 35 regf÷···ö···¢··5
000010 47 9F CE 01 01 00 00 00-05 00 00 00 00 00 00 00 G·Î·············
000020 01 00 00 00 20 00 00 00-00 A0 E3 00 01 00 00 00 ····  ··· ã·····
000030 53 00 59 00 53 00 54 00-45 00 4D 00 00 00 00 00 S·Y·S·T·E·M·····
000040 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000050 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000060 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000070 6A 21 B8 42 2E 0B E3 11-93 F4 90 B1 1C 2E B9 F2 j!¸B.·ã··ô·±·.¹ò
000080 6A 21 B8 42 2E 0B E3 11-93 F4 90 B1 1C 2E B9 F2 j!¸B.·ã··ô·±·.¹ò
000090 01 00 00 00 6B 21 B8 42-2E 0B E3 11 93 F4 90 B1 ····k!¸B.·ã··ô·±
0000a0 1C 2E B9 F2 72 6D 74 6D-CD 52 94 A6 6E 44 D0 01 ·.¹òrmtmÍR·¦nDÐ·
0000b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000c0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
```

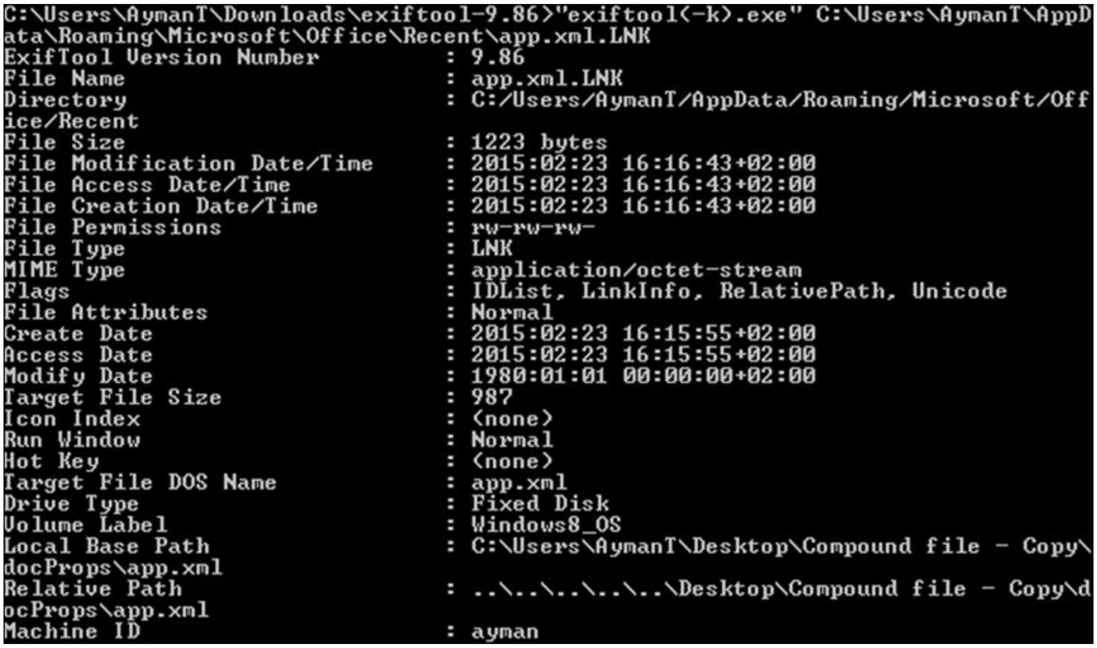
Cursor pos = 0; clus = 2433092; log sec = 19464736



```
000 01 00 00 00 00 00 00 00-00 00 E4 00 00 00 00 00 ··········ä·····
010 40 F1 62 63 7E 49 D0 01-43 00 3A 00 5C 00 55 00 @ñbc~IÐ·C·:·\·U·
020 73 00 65 00 72 00 73 00-5C 00 41 00 79 00 6D 00 s·e·r·s·\·A·y·m·
030 61 00 6E 00 54 00 5C 00-44 00 65 00 73 00 6B 00 a·n·T·\·D·e·s·k·
040 74 00 6F 00 70 00 5C 00-53 00 59 00 53 00 54 00 t·o·p·\·S·Y·S·T·
050 45 00 4D 00 00 00 00 00-00 00 00 00 00 00 00 00 E·M·············
060 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
070 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
```

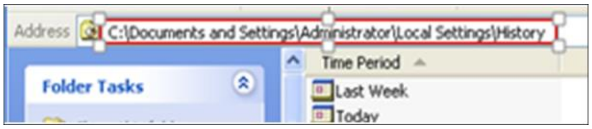


Date created	Date modified	Type	Size
12/27/2015 4:44 PM	12/27/2015 4:44 PM	Shortcut	1 KB
12/21/2015 12:09 PM	1/7/2016 5:41 PM	Shortcut	1 KB
12/22/2015 3:19 PM	12/25/2015 2:50 PM	Shortcut	1 KB
12/30/2015 11:49 AM	12/30/2015 11:52 ...	Shortcut	1 KB

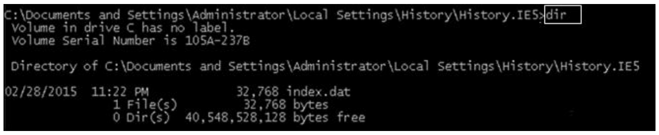


```
C:\Users\AymanT\Downloads\exiftool-9.86>"exiftool(-k).exe" C:\Users\AymanT\AppD
ata\Roaming\Microsoft\Office\Recent\app.xml.LNK
ExifTool Version Number         : 9.86
File Name                       : app.xml.LNK
Directory                       : C:/Users/AymanT/AppData/Roaming/Microsoft/Off
ice/Recent
File Size                       : 1223 bytes
File Modification Date/Time     : 2015:02:23 16:16:43+02:00
File Access Date/Time           : 2015:02:23 16:16:43+02:00
File Creation Date/Time         : 2015:02:23 16:16:43+02:00
File Permissions                : rw-rw-rw-
File Type                       : LNK
MIME Type                       : application/octet-stream
Flags                           : IDList, LinkInfo, RelativePath, Unicode
File Attributes                 : Normal
Create Date                     : 2015:02:23 16:15:55+02:00
Access Date                     : 2015:02:23 16:15:55+02:00
Modify Date                     : 1980:01:01 00:00:00+02:00
Target File Size                : 987
Icon Index                      : (none)
Run Window                      : Normal
Hot Key                         : (none)
Target File DOS Name            : app.xml
Drive Type                      : Fixed Disk
Volume Label                    : Windows8_OS
Local Base Path                 : C:\Users\AymanT\Desktop\Compound file - Copy\
docProps\app.xml
Relative Path                   : ..\..\..\..\..\Desktop\Compound file - Copy\d
ocProps\app.xml
Machine ID                      : ayman
```

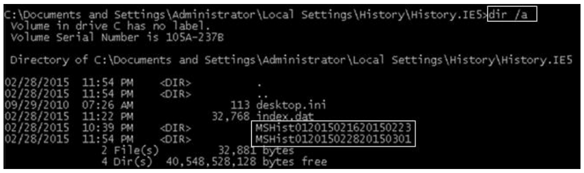
Chapter 10: Browser and E-mail Investigation



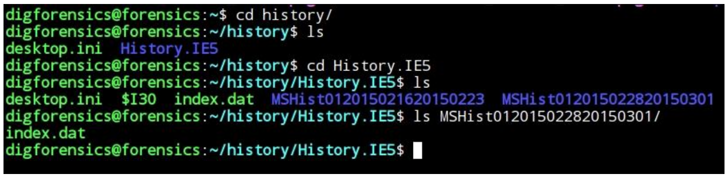
Address C:\Documents and Settings\Administrator\Local Settings\History



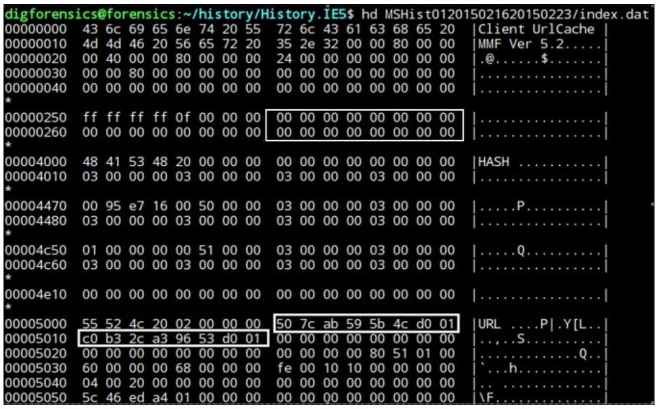
```
C:\Documents and Settings\Administrator\Local Settings\History\History.IE5>dir
 Volume in drive C has no label.
 Volume Serial Number is 105A-237B

 Directory of C:\Documents and Settings\Administrator\Local Settings\History\History.IE5

02/28/2015  11:22 PM            32,768 index.dat
               1 File(s)         32,768 bytes
               0 Dir(s)  40,548,528,128 bytes free
```



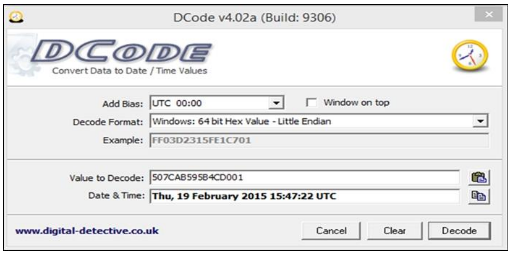
```
C:\Documents and Settings\Administrator\Local Settings\History\History.IE5>dir /a
 Volume in drive C has no label.
 Volume Serial Number is 105A-237B

 Directory of C:\Documents and Settings\Administrator\Local Settings\History\History.IE5

02/28/2015  11:54 PM    <DIR>          .
02/28/2015  11:54 PM    <DIR>          ..
09/29/2010  07:26 AM               113 desktop.ini
02/28/2015  11:22 PM            32,768 index.dat
02/28/2015  10:39 PM    <DIR>          MSHist012015021620150223
02/28/2015  11:54 PM    <DIR>          MSHist012015022820150301
               2 File(s)         32,881 bytes
               4 Dir(s)  40,548,528,128 bytes free
```



```
digforensics@forensics:~$ cd history/
digforensics@forensics:~/history$ ls
desktop.ini  History.IE5
digforensics@forensics:~/history$ cd History.IE5
digforensics@forensics:~/history/History.IE5$ ls
desktop.ini  $I30  index.dat  MSHist012015021620150223  MSHist012015022820150301
digforensics@forensics:~/history/History.IE5$ ls MSHist012015022820150301/
index.dat
digforensics@forensics:~/history/History.IE5$ 
```



```
digforensics@forensics:~/history/History.IE5$ hd MSHist012015021620150223/index.dat
00000000  43 6c 69 65 6e 74 20 55  72 6c 43 61 63 68 65 20  |Client UrlCache |
00000010  4d 4d 46 20 56 65 72 20  35 2e 32 00 00 80 00 00  |MMF Ver 5.2.....|
00000020  00 40 00 00 80 00 00 00  24 00 00 00 00 00 00 00  |.@......$.......|
00000030  00 00 80 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000250  ff ff ff ff 0f 00 00 00  00 00 00 00 00 00 00 00  |................|
00000260  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00004000  48 41 53 48 20 00 00 00  00 00 00 00 00 00 00 00  |HASH ...........|
00004010  03 00 00 00 03 00 00 00  03 00 00 00 03 00 00 00  |................|
*
00004470  00 95 e7 16 00 50 00 00  03 00 00 00 03 00 00 00  |.....P..........|
00004480  03 00 00 00 03 00 00 00  03 00 00 00 03 00 00 00  |................|
*
00004c50  01 00 00 00 00 51 00 00  03 00 00 00 03 00 00 00  |.....Q..........|
00004c60  03 00 00 00 03 00 00 00  03 00 00 00 03 00 00 00  |................|
*
00004e10  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00005000  55 52 4c 20 02 00 00 00  50 7c ab 59 5b 4c d0 01  |URL ....P|.Y[L..|
00005010  c0 b3 2c a3 96 53 d0 01  00 00 00 00 00 00 00 00  |..,..S..........|
00005020  00 00 00 00 00 00 00 00  00 00 00 00 80 51 01 00  |.............Q..|
00005030  60 00 00 00 68 00 00 00  fe 00 10 10 00 00 00 00  |`...h...........|
00005040  04 00 20 00 00 00 00 00  00 00 00 00 00 00 00 00  |.. .............|
00005050  5c 46 ed a4 01 00 00 00  00 00 00 00 00 00 00 00  |\F..............|
```


DCode v4.02a (Build: 9306)
DCode
Convert Data to Date / Time Values
Cancel
Clear
Decode

Add Bias: UTC 00:00

□ Window on top

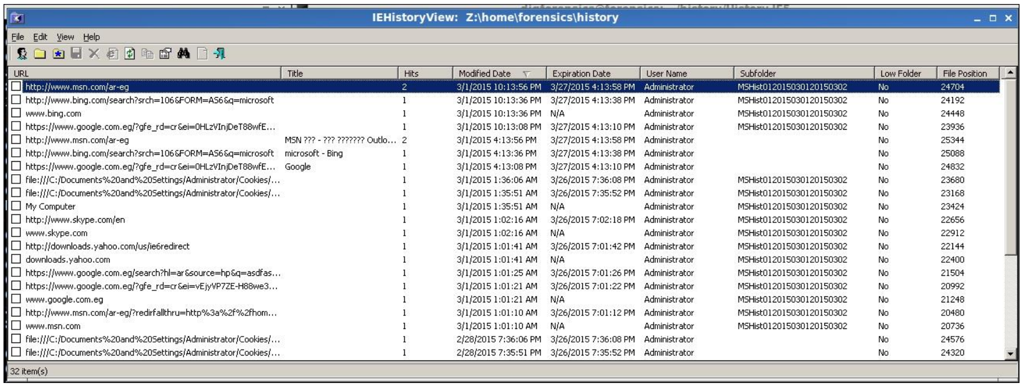
Decode Format: Windows: 64 bit Hex Value - Little Endian

Example: FF03D2315FE1C701

Value to Decode: 507CAB595B4CD001

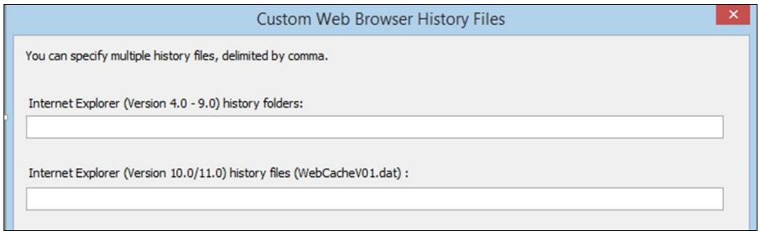
Date & Time: Thu, 19 February 2015 15:47:22 UTC

www.digital-detective.co.uk



URL	Title	Hits	Modified Date	Expiration Date	User Name	Subfolder	Low Folder	File Position
□ http://www.msn.com/ar-eg		2	3/1/2015 10:13:56 PM	3/27/2015 4:13:58 PM	Administrator	MSHist012015030120150302	No	24704
□ http://www.bing.com/search?srch=106&FORM=AS6&q=microsoft		1	3/1/2015 10:13:36 PM	3/27/2015 4:13:38 PM	Administrator	MSHist012015030120150302	No	24192
□ www.bing.com		1	3/1/2015 10:13:36 PM	N/A	Administrator	MSHist012015030120150302	No	24448
□ https://www.google.com.eg/?gfe_rd=cr&ei=0HLzVInjDeT88wfE…		1	3/1/2015 10:13:08 PM	3/27/2015 4:13:10 PM	Administrator	MSHist012015030120150302	No	23936
□ http://www.msn.com/ar-eg	MSN ??? - ??? ??????? Outlo…	2	3/1/2015 4:13:56 PM	3/27/2015 4:13:58 PM	Administrator		No	25344
□ http://www.bing.com/search?srch=106&FORM=AS6&q=microsoft	microsoft - Bing	1	3/1/2015 4:13:36 PM	3/27/2015 4:13:38 PM	Administrator		No	25088
□ https://www.google.com.eg/?gfe_rd=cr&ei=0HLzVInjDeT88wfE…	Google	1	3/1/2015 4:13:08 PM	3/27/2015 4:13:10 PM	Administrator		No	24832
□ file:///C:/Documents%20and%20Settings/Administrator/Cookies/…		1	3/1/2015 1:36:06 AM	3/26/2015 7:36:08 PM	Administrator	MSHist012015030120150302	No	23680
□ file:///C:/Documents%20and%20Settings/Administrator/Cookies/…		1	3/1/2015 1:35:51 AM	3/26/2015 7:35:52 PM	Administrator	MSHist012015030120150302	No	23168
□ My Computer		1	3/1/2015 1:35:51 AM	N/A	Administrator	MSHist012015030120150302	No	23424
□ http://www.skype.com/en		1	3/1/2015 1:02:16 AM	3/26/2015 7:02:18 PM	Administrator	MSHist012015030120150302	No	22656
□ www.skype.com		1	3/1/2015 1:02:16 AM	N/A	Administrator	MSHist012015030120150302	No	22912
□ http://downloads.yahoo.com/us/ie6redirect		1	3/1/2015 1:01:41 AM	3/26/2015 7:01:42 PM	Administrator	MSHist012015030120150302	No	22144
□ downloads.yahoo.com		1	3/1/2015 1:01:41 AM	N/A	Administrator	MSHist012015030120150302	No	22400
□ https://www.google.com.eg/search?hl=ar&source=hp&q=asdfas…		1	3/1/2015 1:01:25 AM	3/26/2015 7:01:26 PM	Administrator	MSHist012015030120150302	No	21504
□ https://www.google.com.eg/?gfe_rd=cr&ei=vEjyVP7ZE-H88we3…		1	3/1/2015 1:01:21 AM	3/26/2015 7:01:22 PM	Administrator	MSHist012015030120150302	No	20992
□ www.google.com.eg		1	3/1/2015 1:01:21 AM	N/A	Administrator	MSHist012015030120150302	No	21248
□ http://www.msn.com/ar-eg/?redirfallthru=http%3a%2f%2fhom…		1	3/1/2015 1:01:10 AM	3/26/2015 7:01:12 PM	Administrator	MSHist012015030120150302	No	20480
□ www.msn.com		1	3/1/2015 1:01:10 AM	N/A	Administrator	MSHist012015030120150302	No	20736
□ file:///C:/Documents%20and%20Settings/Administrator/Cookies/…		1	2/28/2015 7:36:06 PM	3/26/2015 7:36:08 PM	Administrator		No	24576
□ file:///C:/Documents%20and%20Settings/Administrator/Cookies/…		1	2/28/2015 7:35:51 PM	3/26/2015 7:35:52 PM	Administrator		No	24320

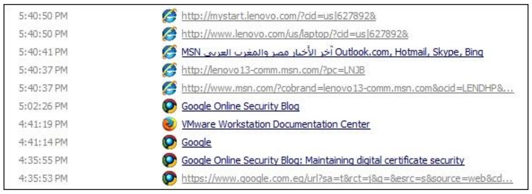
32 item(s)



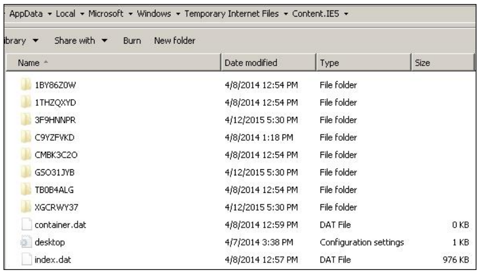
You can specify multiple history files, delimited by comma.

Internet Explorer (Version 4.0 - 9.0) history folders:

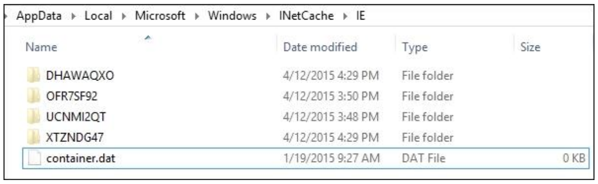
Internet Explorer (Version 10.0/11.0) history files (WebCacheV01.dat) :



5:40:50 PM	http://mystart.lenovo.com/?cid=us|627892&
5:40:50 PM	http://www.lenovo.com/us/laptop/?cid=us|627892&
5:40:41 PM	MSN آخر الأخبار مصر والمغرب العربي Outlook.com, Hotmail, Skype, Bing
5:40:37 PM	http://lenovo13-comm.msn.com/?pc=LNJB
5:40:37 PM	http://www.msn.com/?cobrand=lenovo13-comm.msn.com&ocid=LENDHP&…
5:02:26 PM	Google Online Security Blog
4:41:19 PM	VMware Workstation Documentation Center
4:41:14 PM	Google
4:35:55 PM	Google Online Security Blog: Maintaining digital certificate security
4:35:53 PM	https://www.google.com.eg/url?sa=t&rct=j&q=&esrc=s&source=web&cd…

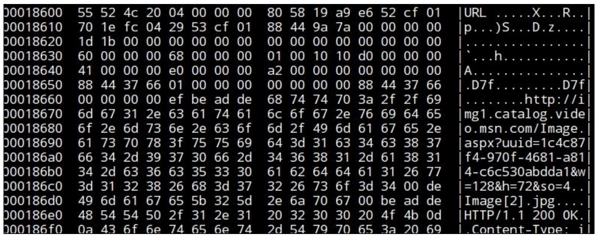

AppData ▾ Local ▾ Microsoft ▾ Windows ▾ Temporary Internet Files ▾ Content.IE5 ▾
ibrary ▾ Share with ▾ Burn New folder

Name	Date modified	Type	Size
1BY86Z0W	4/8/2014 12:54 PM	File folder	
1THZQXYD	4/8/2014 12:54 PM	File folder	
3F9HNNPR	4/12/2015 5:30 PM	File folder	
C9YZFVKD	4/8/2014 1:18 PM	File folder	
CMBK3C2O	4/8/2014 12:54 PM	File folder	
GSO31JYB	4/12/2015 5:30 PM	File folder	
TB0B4ALG	4/8/2014 12:54 PM	File folder	
XGCRWY37	4/12/2015 5:30 PM	File folder	
container.dat	4/8/2014 12:59 PM	DAT File	0 KB
desktop	4/7/2014 3:38 PM	Configuration settings	1 KB
index.dat	4/8/2014 12:57 PM	DAT File	976 KB

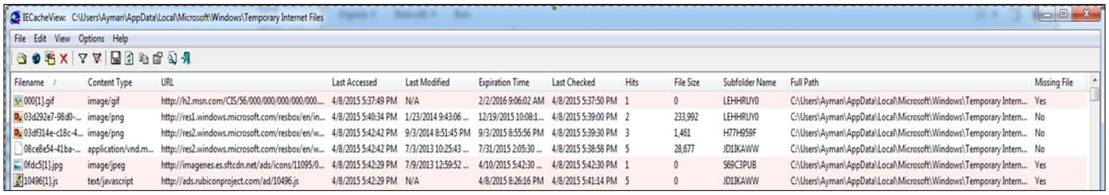


AppData ▸ Local ▸ Microsoft ▸ Windows ▸ INetCache ▸ IE

Name	Date modified	Type	Size
DHAWAQXO	4/12/2015 4:29 PM	File folder	
OFR7SF92	4/12/2015 3:50 PM	File folder	
UCNMI2QT	4/12/2015 3:48 PM	File folder	
XTZNDG47	4/12/2015 4:29 PM	File folder	
container.dat	1/19/2015 9:27 AM	DAT File	0 KB

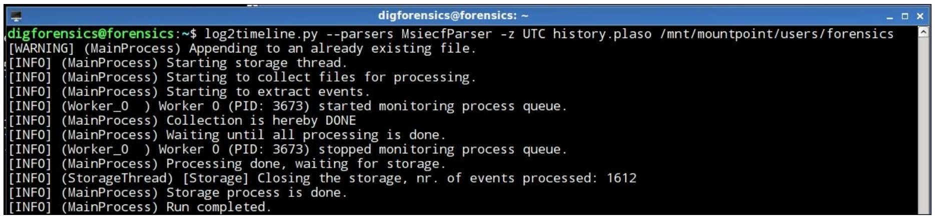


```
00018600  55 52 4c 20 04 00 00 00  80 58 19 a9 e6 52 cf 01  |URL .....X...R..|
00018610  70 1e fc 04 29 53 cf 01  88 44 9a 7a 00 00 00 00  |p...)S...D.z....|
00018620  1d 1b 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00018630  60 00 00 00 68 00 00 00  01 00 10 10 d0 00 00 00  |`...h...........|
00018640  41 00 00 00 e0 00 00 00  a2 00 00 00 00 00 00 00  |A...............|
00018650  88 44 37 66 01 00 00 00  00 00 00 00 88 44 37 66  |.D7f.........D7f|
00018660  00 00 00 00 ef be ad de  68 74 74 70 3a 2f 2f 69  |........http://i|
00018670  6d 67 31 2e 63 61 74 61  6c 6f 67 2e 76 69 64 65  |mg1.catalog.vide|
00018680  6f 2e 6d 73 6e 2e 63 6f  6d 2f 49 6d 61 67 65 2e  |o.msn.com/Image.|
00018690  61 73 70 78 3f 75 75 69  64 3d 31 63 34 63 38 37  |aspx?uuid=1c4c87|
000186a0  66 34 2d 39 37 30 66 2d  34 36 38 31 2d 61 38 31  |f4-970f-4681-a81|
000186b0  34 2d 63 36 63 35 33 30  61 62 64 64 61 31 26 77  |4-c6c530abdda1&w|
000186c0  3d 31 32 38 26 68 3d 37  32 26 73 6f 3d 34 00 de  |=128&h=72&so=4..|
000186d0  49 6d 61 67 65 5b 32 5d  2e 6a 70 67 00 be ad de  |Image[2].jpg....|
000186e0  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d  |HTTP/1.1 200 OK.|
000186f0  0a 43 6f 6e 74 65 6e 74  2d 54 79 70 65 3a 20 69  |.Content-Type: i|
```



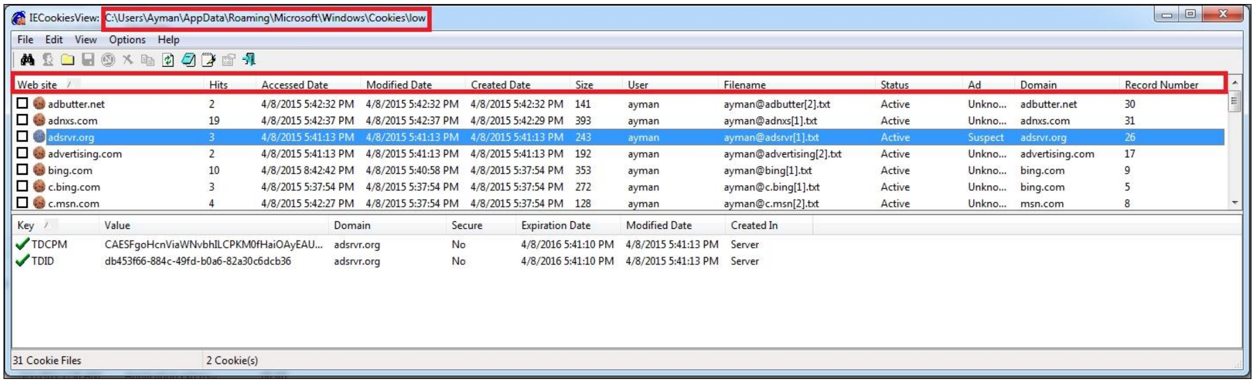
IECacheView: C:\Users\Ayman\AppData\Local\Microsoft\Windows\Temporary Internet Files

Filename	Content Type	URL	Last Accessed	Last Modified	Expiration Time	Last Checked	Hits	File Size	Subfolder Name	Full Path	Missing File
000[1].gif	image/gif	http://h2.msn.com/CIS/56/000/000/000/000/000....	4/8/2015 5:37:49 PM	N/A	2/2/2016 9:06:02 AM	4/8/2015 5:37:50 PM	1	0	LEHHRUY0	C:\Users\Ayman\AppData\Local\Microsoft\Windows\Temporary Intern...	Yes
03d292e7-98d0-...	image/png	http://res1.windows.microsoft.com/resbox/en/in...	4/8/2015 5:40:34 PM	1/23/2014 9:43:06 ...	12/19/2015 10:08:1...	4/8/2015 5:39:00 PM	2	233,992	LEHHRUY0	C:\Users\Ayman\AppData\Local\Microsoft\Windows\Temporary Intern...	No
03df314e-c18c-4...	image/png	http://res2.windows.microsoft.com/resbox/en/w...	4/8/2015 5:42:42 PM	9/3/2014 8:51:45 PM	9/3/2015 8:55:56 PM	4/8/2015 5:39:30 PM	3	1,461	H77H959F	C:\Users\Ayman\AppData\Local\Microsoft\Windows\Temporary Intern...	No
08ce8e54-41ba-...	application/vnd.m...	http://res2.windows.microsoft.com/resbox/en/w...	4/8/2015 5:42:42 PM	7/3/2013 10:25:43 ...	7/31/2015 2:05:30 ...	4/8/2015 5:38:58 PM	5	28,677	JD1IKAWW	C:\Users\Ayman\AppData\Local\Microsoft\Windows\Temporary Intern...	No
0fdc5[1].jpg	image/jpeg	http://imagenes.es.sftcdn.net/ads/icons/11095/0...	4/8/2015 5:42:29 PM	7/9/2013 12:59:52 ...	4/10/2015 5:42:30 ...	4/8/2015 5:42:30 PM	1	0	S69C3PUB	C:\Users\Ayman\AppData\Local\Microsoft\Windows\Temporary Intern...	Yes
10496[1].js	text/javascript	http://ads.rubiconproject.com/ad/10496.js	4/8/2015 5:42:29 PM	N/A	4/8/2015 8:26:16 PM	4/8/2015 5:41:14 PM	5	0	JD1IKAWW	C:\Users\Ayman\AppData\Local\Microsoft\Windows\Temporary Intern...	Yes



digforensics@forensics: ~

```
digforensics@forensics:~$ log2timeline.py --parsers MsiecfParser -z UTC history.plaso /mnt/mountpoint/users/forensics
[WARNING] (MainProcess) Appending to an already existing file.
[INFO] (MainProcess) Starting storage thread.
[INFO] (MainProcess) Starting to collect files for processing.
[INFO] (MainProcess) Starting to extract events.
[INFO] (Worker_0  ) Worker 0 (PID: 3673) started monitoring process queue.
[INFO] (MainProcess) Collection is hereby DONE
[INFO] (MainProcess) Waiting until all processing is done.
[INFO] (Worker_0  ) Worker 0 (PID: 3673) stopped monitoring process queue.
[INFO] (MainProcess) Processing done, waiting for storage.
[INFO] (StorageThread) [Storage] Closing the storage, nr. of events processed: 1612
[INFO] (MainProcess) Storage process is done.
[INFO] (MainProcess) Run completed.
```

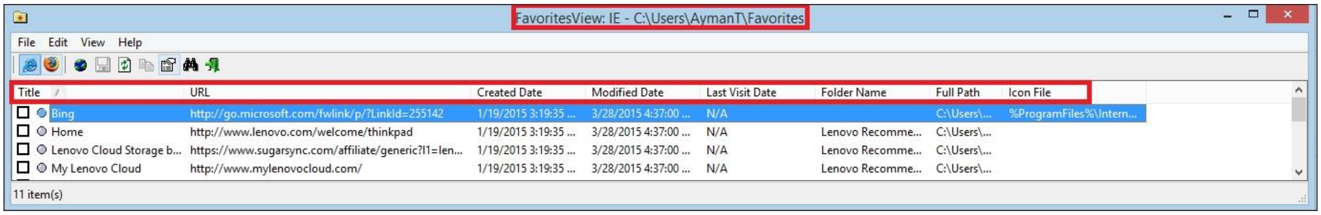


IECookiesView: C:\Users\Ayman\AppData\Roaming\Microsoft\Windows\Cookies\low

Web site	Hits	Accessed Date	Modified Date	Created Date	Size	User	Filename	Status	Ad	Domain	Record Number
□ adbutter.net	2	4/8/2015 5:42:32 PM	4/8/2015 5:42:32 PM	4/8/2015 5:42:32 PM	141	ayman	ayman@adbutter[2].txt	Active	Unkno...	adbutter.net	30
□ adnxs.com	19	4/8/2015 5:42:37 PM	4/8/2015 5:42:37 PM	4/8/2015 5:42:29 PM	393	ayman	ayman@adnxs[1].txt	Active	Unkno...	adnxs.com	31
□ adsrvr.org	3	4/8/2015 5:41:13 PM	4/8/2015 5:41:13 PM	4/8/2015 5:41:13 PM	243	ayman	ayman@adsrvr[1].txt	Active	Suspect	adsrvr.org	26
□ advertising.com	2	4/8/2015 5:41:13 PM	4/8/2015 5:41:13 PM	4/8/2015 5:41:13 PM	192	ayman	ayman@advertising[2].txt	Active	Unkno...	advertising.com	17
□ bing.com	10	4/8/2015 8:42:42 PM	4/8/2015 5:40:58 PM	4/8/2015 5:37:54 PM	353	ayman	ayman@bing[1].txt	Active	Unkno...	bing.com	9
□ c.bing.com	3	4/8/2015 5:37:54 PM	4/8/2015 5:37:54 PM	4/8/2015 5:37:54 PM	272	ayman	ayman@c.bing[1].txt	Active	Unkno...	bing.com	5
□ c.msn.com	4	4/8/2015 5:42:27 PM	4/8/2015 5:37:54 PM	4/8/2015 5:37:54 PM	128	ayman	ayman@c.msn[2].txt	Active	Unkno...	msn.com	8

Key	Value	Domain	Secure	Expiration Date	Modified Date	Created In
✓ TDCPM	CAESFgoHcnViaWNvbhILCPKM0fHaiOAyEAU...	adsrvr.org	No	4/8/2016 5:41:10 PM	4/8/2015 5:41:13 PM	Server
✓ TDID	db453f66-884c-49fd-b0a6-82a30c6dcb36	adsrvr.org	No	4/8/2016 5:41:10 PM	4/8/2015 5:41:13 PM	Server

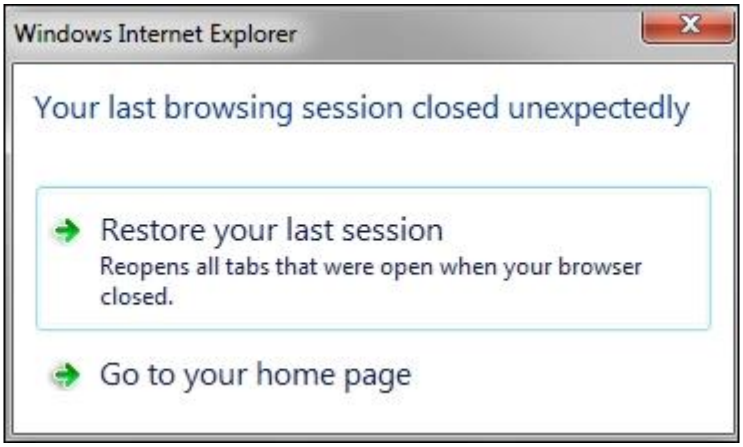
31 Cookie Files   2 Cookie(s)



FavoritesView: IE - C:\Users\AymanT\Favorites

Title	URL	Created Date	Modified Date	Last Visit Date	Folder Name	Full Path	Icon File
□ Bing	http://go.microsoft.com/fwlink/p/?LinkId=255142	1/19/2015 3:19:35 ...	3/28/2015 4:37:00 ...	N/A		C:\Users\...	%ProgramFiles%\Intern...
□ Home	http://www.lenovo.com/welcome/thinkpad	1/19/2015 3:19:35 ...	3/28/2015 4:37:00 ...	N/A	Lenovo Recomme...	C:\Users\...	
□ Lenovo Cloud Storage b...	https://www.sugarsync.com/affiliate/generic?l1=len...	1/19/2015 3:19:35 ...	3/28/2015 4:37:00 ...	N/A	Lenovo Recomme...	C:\Users\...	
□ My Lenovo Cloud	http://www.mylenovocloud.com/	1/19/2015 3:19:35 ...	3/28/2015 4:37:00 ...	N/A	Lenovo Recomme...	C:\Users\...	

11 item(s)

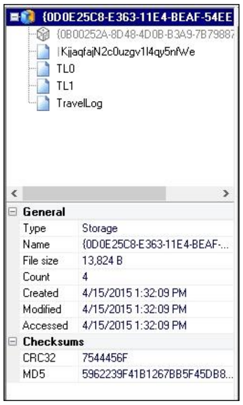


Windows Internet Explorer

Your last browsing session closed unexpectedly

Restore your last session
Reopens all tabs that were open when your browser closed.

Go to your home page



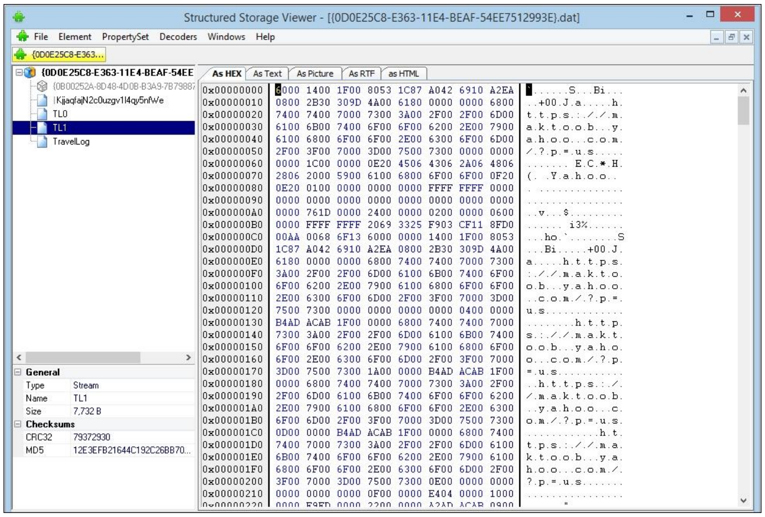
```
{0D0E25C8-E363-11E4-BEAF-54EE
    {0B00252A-8D48-4D0B-B3A9-7B79887
    |KjjaqfajN2c0uzgv1l4qy5nfWe
    TL0
    TL1
    TravelLog
```

General

Type	Storage
Name	{0D0E25C8-E363-11E4-BEAF-...
File size	13,824 B
Count	4
Created	4/15/2015 1:32:09 PM
Modified	4/15/2015 1:32:09 PM
Accessed	4/15/2015 1:32:09 PM

Checksums

CRC32	7544456F
MD5	5962239F41B1267BB5F45DB8...



Structured Storage Viewer - [{0D0E25C8-E363-11E4-BEAF-54EE7512993E}.dat]

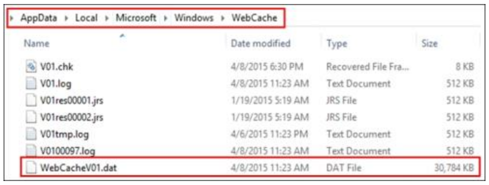
General

Type	Stream
Name	TL1
Size	7,732 B

Checksums

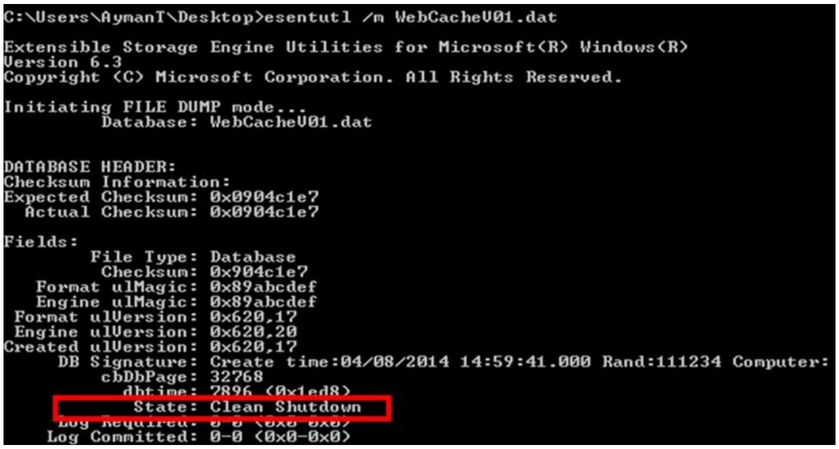
CRC32	79372930
MD5	12E3EFB21644C192C26BB70...

```
0x00000000  6000 1400 1F00 8053 1C87 A042 6910 A2EA  `......S...Bi...
0x00000010  0800 2B30 309D 4A00 6180 0000 0000 6800  ..+00.J.a.....h.
0x00000020  7400 7400 7000 7300 3A00 2F00 2F00 6D00  t.t.p.s.:././.m.
0x00000030  6100 6B00 7400 6F00 6F00 6200 2E00 7900  a.k.t.o.o.b...y.
0x00000040  6100 6800 6F00 6F00 2E00 6300 6F00 6D00  a.h.o.o...c.o.m.
0x00000050  2F00 3F00 7000 3D00 7500 7300 0000 0000  /.?.p.=.u.s.....
0x00000060  0000 1C00 0000 0E20 4506 4306 2A06 4806  ....... E.C.*.H.
0x00000070  2806 2000 5900 6100 6800 6F00 6F00 0F20  (. .Y.a.h.o.o..
0x00000080  0E20 0100 0000 0000 0000 FFFF FFFF 0000  . ..............
0x00000090  0000 0000 0000 0000 0000 0000 0000 0000  ................
0x000000A0  0000 761D 0000 2400 0000 0200 0000 0600  ..v...$.........
0x000000B0  0000 FFFF FFFF 2069 3325 F903 CF11 8FD0  ...... i3%......
0x000000C0  00AA 0068 6F13 6000 0000 1400 1F00 8053  ...ho.`........S
0x000000D0  1C87 A042 6910 A2EA 0800 2B30 309D 4A00  ...Bi.....+00.J.
0x000000E0  6180 0000 0000 6800 7400 7400 7000 7300  a.....h.t.t.p.s.
0x000000F0  3A00 2F00 2F00 6D00 6100 6B00 7400 6F00  :././.m.a.k.t.o.
0x00000100  6F00 6200 2E00 7900 6100 6800 6F00 6F00  o.b...y.a.h.o.o.
0x00000110  2E00 6300 6F00 6D00 2F00 3F00 7000 3D00  ..c.o.m./.?.p.=.
0x00000120  7500 7300 0000 0000 0000 0000 0400 0000  u.s.............
0x00000130  B4AD ACAB 1F00 0000 6800 7400 7400 7000  ........h.t.t.p.
0x00000140  7300 3A00 2F00 2F00 6D00 6100 6B00 7400  s.:././.m.a.k.t.
0x00000150  6F00 6F00 6200 2E00 7900 6100 6800 6F00  o.o.b...y.a.h.o.
0x00000160  6F00 2E00 6300 6F00 6D00 2F00 3F00 7000  o...c.o.m./.?.p.
0x00000170  3D00 7500 7300 1A00 0000 B4AD ACAB 1F00  =.u.s...........
0x00000180  0000 6800 7400 7400 7000 7300 3A00 2F00  ..h.t.t.p.s.:./.
0x00000190  2F00 6D00 6100 6B00 7400 6F00 6F00 6200  /.m.a.k.t.o.o.b.
0x000001A0  2E00 7900 6100 6800 6F00 6F00 2E00 6300  ..y.a.h.o.o...c.
0x000001B0  6F00 6D00 2F00 3F00 7000 3D00 7500 7300  o.m./.?.p.=.u.s.
0x000001C0  0D00 0000 B4AD ACAB 1F00 0000 6800 7400  ............h.t.
0x000001D0  7400 7000 7300 3A00 2F00 2F00 6D00 6100  t.p.s.:././.m.a.
0x000001E0  6B00 7400 6F00 6F00 6200 2E00 7900 6100  k.t.o.o.b...y.a.
0x000001F0  6800 6F00 6F00 2E00 6300 6F00 6D00 2F00  h.o.o...c.o.m./.
0x00000200  3F00 7000 3D00 7500 7300 0E00 0000 0000  ?.p.=.u.s.......
0x00000210  0000 0000 0000 0F00 0000 E404 0000 1000  ................
0x00000220  0000 F9FD 0000 2200 0000 A2AD ACAB 0900  ......"
```

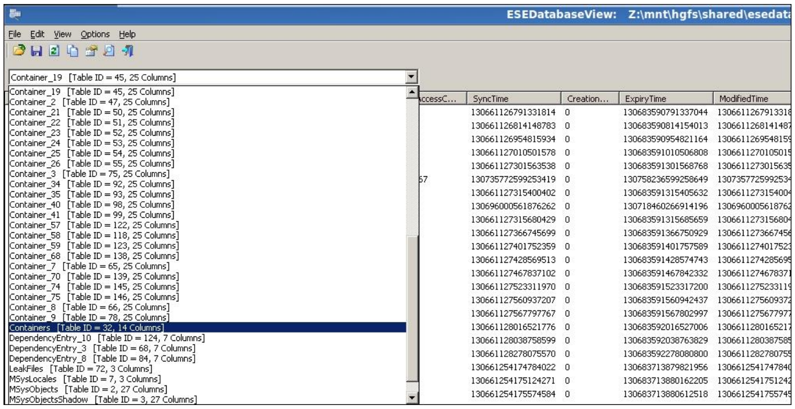


AppData ▸ Local ▸ Microsoft ▸ Windows ▸ WebCache

Name	Date modified	Type	Size
V01.chk	4/8/2015 6:30 PM	Recovered File Fra...	8 KB
V01.log	4/8/2015 11:23 AM	Text Document	512 KB
V01res00001.jrs	1/19/2015 5:19 AM	JRS File	512 KB
V01res00002.jrs	1/19/2015 5:19 AM	JRS File	512 KB
V01tmp.log	4/6/2015 11:23 PM	Text Document	512 KB
V0100097.log	4/8/2015 11:23 AM	Text Document	512 KB
WebCacheV01.dat	4/8/2015 11:23 AM	DAT File	30,784 KB



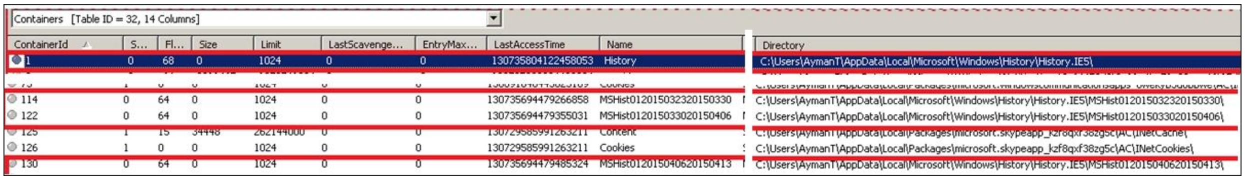
```
C:\Users\AymanT\Desktop>esentutl /m WebCacheV01.dat

Extensible Storage Engine Utilities for Microsoft(R) Windows(R)
Version 6.3
Copyright (C) Microsoft Corporation. All Rights Reserved.

Initiating FILE DUMP mode...
         Database: WebCacheV01.dat


DATABASE HEADER:
Checksum Information:
Expected Checksum: 0x0904c1e7
  Actual Checksum: 0x0904c1e7

Fields:
        File Type: Database
         Checksum: 0x904c1e7
   Format ulMagic: 0x89abcdef
   Engine ulMagic: 0x89abcdef
 Format ulVersion: 0x620,17
 Engine ulVersion: 0x620,20
Created ulVersion: 0x620,17
     DB Signature: Create time:04/08/2014 14:59:41.000 Rand:111234 Computer:
         cbDbPage: 32768
           dbtime: 7896 (0x1ed8)
            State: Clean Shutdown
     Log Required: 0-0 (0x0-0x0)
    Log Committed: 0-0 (0x0-0x0)
```



Container_19   [Table ID = 45, 25 Columns]

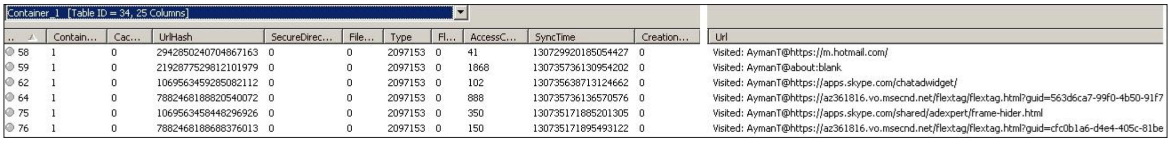
Container_19   [Table ID = 45, 25 Columns]
Container_2   [Table ID = 47, 25 Columns]
Container_21   [Table ID = 50, 25 Columns]
Container_22   [Table ID = 51, 25 Columns]
Container_23   [Table ID = 52, 25 Columns]
Container_24   [Table ID = 53, 25 Columns]
Container_25   [Table ID = 54, 25 Columns]
Container_26   [Table ID = 55, 25 Columns]
Container_3   [Table ID = 75, 25 Columns]
Container_34   [Table ID = 92, 25 Columns]
Container_35   [Table ID = 93, 25 Columns]
Container_40   [Table ID = 98, 25 Columns]
Container_41   [Table ID = 99, 25 Columns]
Container_57   [Table ID = 122, 25 Columns]
Container_58   [Table ID = 118, 25 Columns]
Container_59   [Table ID = 123, 25 Columns]
Container_68   [Table ID = 138, 25 Columns]
Container_7   [Table ID = 65, 25 Columns]
Container_70   [Table ID = 139, 25 Columns]
Container_74   [Table ID = 145, 25 Columns]
Container_75   [Table ID = 146, 25 Columns]
Container_8   [Table ID = 66, 25 Columns]
Container_9   [Table ID = 78, 25 Columns]
Containers   [Table ID = 32, 14 Columns]
DependencyEntry_10   [Table ID = 124, 7 Columns]
DependencyEntry_3   [Table ID = 68, 7 Columns]
DependencyEntry_8   [Table ID = 84, 7 Columns]
LeakFiles   [Table ID = 72, 3 Columns]
MSysLocales   [Table ID = 7, 3 Columns]
MSysObjects   [Table ID = 2, 27 Columns]
MSysObjectsShadow   [Table ID = 3, 27 Columns]

AccessC...	SyncTime	Creation...	ExpiryTime	ModifiedTime
	130661126791331814	0	130683590791337044	130661126791331
	130661126814148783	0	130683590814154013	13066112681414
	130661126954815934	0	130683590954821164	13066112695481
	130661127010501578	0	130683591010506808	13066112701050
	130661127301563538	0	130683591301568768	13066112730156
67	130735772599253419	0	130758236599258649	13073577259925
	130661127315400402	0	130683591315405632	13066112731540
	130696000561876262	0	130718460266914196	13069600056187
	130661127315680429	0	130683591315685659	13066112731568
	130661127366745699	0	130683591366750929	13066112736674
	130661127401752359	0	130683591401757589	13066112740175
	130661127428569513	0	130683591428574743	13066112742856
	130661127467837102	0	130683591467842332	13066112746783
	130661127523311970	0	130683591523317200	13066112752331
	130661127560937207	0	130683591560942437	13066112756093
	130661127567797767	0	130683591567802997	13066112756779
	130661128016521776	0	130683592016527006	13066112801652
	130661128038758599	0	130683592038763829	13066112803875
	130661128278075570	0	130683592278080800	13066112827807
	130661254174784022	0	130683713879821956	13066125417478
	130661254175124271	0	130683713880162205	13066125417512
	130661254175574584	0	130683713880612518	13066125417557



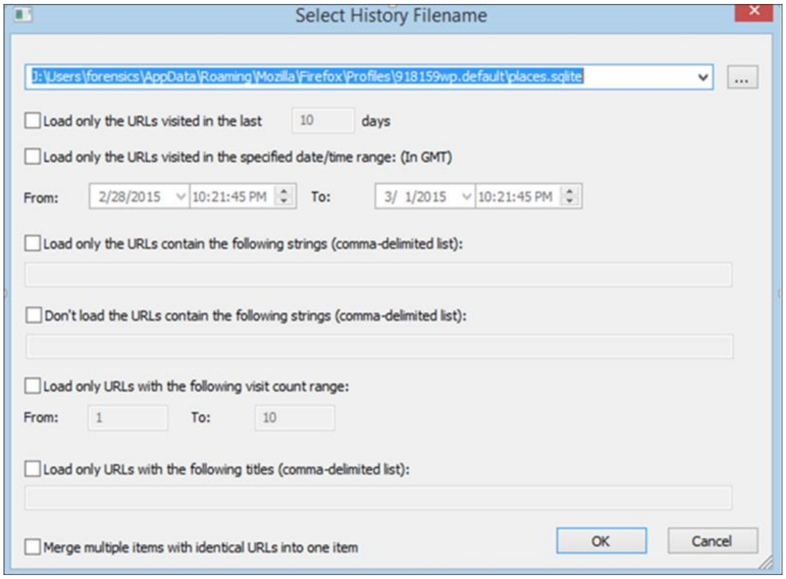
Containers   [Table ID = 32, 14 Columns]

ContainerId	S...	Fl...	Size	Limit	LastScavenge...	EntryMax...	LastAccessTime	Name	Directory
1	0	68	0	1024	0	0	130735804122458053	History	C:\Users\AymanT\AppData\Local\Microsoft\Windows\History\History.IE5\
75	1	0	0	1024	0	0	[illegible]	Cookies	C:\Users\AymanT\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\AC\I
114	0	64	0	1024	0	0	130735694479266858	MSHist012015032320150330	C:\Users\AymanT\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012015032320150330\
122	0	64	0	1024	0	0	130735694479355031	MSHist012015033020150406	C:\Users\AymanT\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012015033020150406\
125	1	15	34448	262144000	0	0	130729585991263211	Content	C:\Users\AymanT\AppData\Local\Packages\microsoft.skypeapp_kzf8qxf38zg5c\AC\INetCache\
126	1	0	0	1024	0	0	130729585991263211	Cookies	C:\Users\AymanT\AppData\Local\Packages\microsoft.skypeapp_kzf8qxf38zg5c\AC\INetCookies\
130	0	64	0	1024	0	0	130735694479485324	MSHist012015040620150413	C:\Users\AymanT\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012015040620150413\



Container_1   [Table ID = 34, 25 Columns]

..	Contain...	Cac...	UrlHash	SecureDirec...	File...	Type	Fl...	AccessC...	SyncTime	Creation...	Url
58	1	0	2942850240704867163	0	0	2097153	0	41	130729920185054427	0	Visited: AymanT@https://m.hotmail.com/
59	1	0	2192877529812101979	0	0	2097153	0	1868	130735736130954202	0	Visited: AymanT@about:blank
62	1	0	1069563459285082112	0	0	2097153	0	102	130735638713124662	0	Visited: AymanT@https://apps.skype.com/chatadwidget/
64	1	0	7882468188820540072	0	0	2097153	0	888	130735736136570576	0	Visited: AymanT@https://az361816.vo.msecnd.net/flextag/flextag.html?guid=563d6ca7-99f0-4b50-91f7
75	1	0	1069563458448296926	0	0	2097153	0	350	130735171885201305	0	Visited: AymanT@https://apps.skype.com/shared/adexpert/frame-hider.html
76	1	0	7882468188688376013	0	0	2097153	0	150	130735171895493122	0	Visited: AymanT@https://az361816.vo.msecnd.net/flextag/flextag.html?guid=cfc0b1a6-d4e4-405c-81be



Select History Filename

D:\Users\forensics\AppData\Roaming\Mozilla\Firefox\Profiles\918159wp.default\places.sqlite

☐ Load only the URLs visited in the last 10 days

☐ Load only the URLs visited in the specified date/time range: (In GMT)

From: 2/28/2015 10:21:45 PM   To: 3/ 1/2015 10:21:45 PM

☐ Load only the URLs contain the following strings (comma-delimited list):

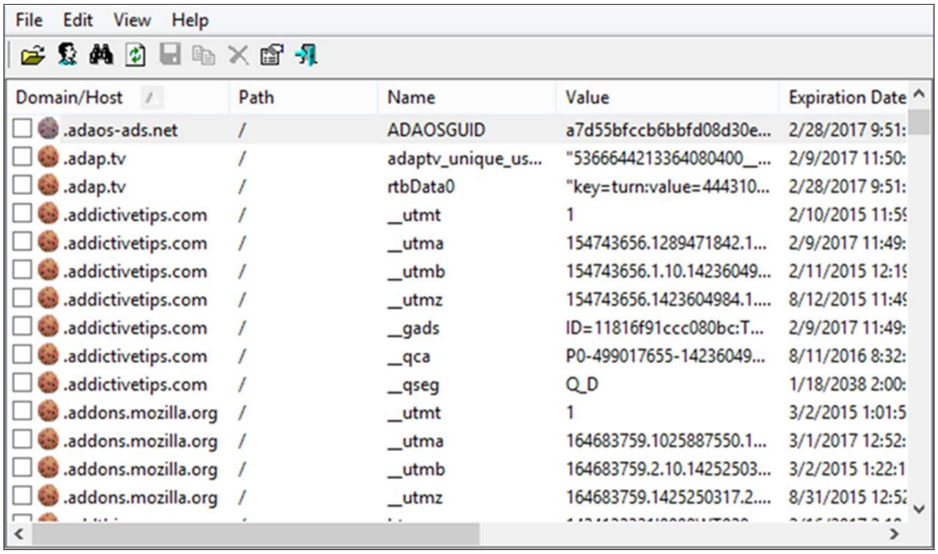
☐ Don't load the URLs contain the following strings (comma-delimited list):

☐ Load only URLs with the following visit count range:

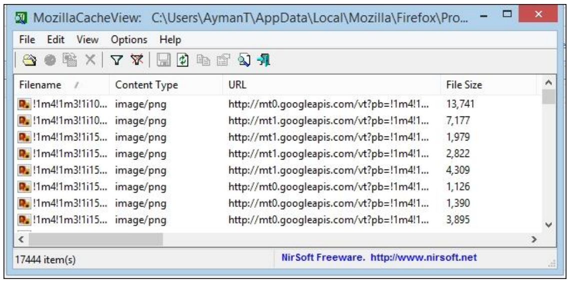
From: 1   To: 10

☐ Load only URLs with the following titles (comma-delimited list):

☐ Merge multiple items with identical URLs into one item



Domain/Host	Path	Name	Value	Expiration Date
□ .adaos-ads.net	/	ADAOSGUID	a7d55bfccb6bbfd08d30e...	2/28/2017 9:51:
□ .adap.tv	/	adaptv_unique_us...	"5366644213364080400__...	2/9/2017 11:50:
□ .adap.tv	/	rtbData0	"key=turn:value=444310...	2/28/2017 9:51:
□ .addictivetips.com	/	__utmt	1	2/10/2015 11:5
□ .addictivetips.com	/	__utma	154743656.1289471842.1...	2/9/2017 11:49:
□ .addictivetips.com	/	__utmb	154743656.1.10.14236049...	2/11/2015 12:1
□ .addictivetips.com	/	__utmz	154743656.1423604984.1....	8/12/2015 11:4
□ .addictivetips.com	/	__gads	ID=11816f91ccc080bc:T...	2/9/2017 11:49:
□ .addictivetips.com	/	__qca	P0-499017655-14236049...	8/11/2016 8:32:
□ .addictivetips.com	/	__qseg	Q_D	1/18/2038 2:00:
□ .addons.mozilla.org	/	__utmt	1	3/2/2015 1:01:5
□ .addons.mozilla.org	/	__utma	164683759.1025887550.1...	3/1/2017 12:52:
□ .addons.mozilla.org	/	__utmb	164683759.2.10.14252503...	3/2/2015 1:22:1
□ .addons.mozilla.org	/	__utmz	164683759.1425250317.2....	8/31/2015 12:5

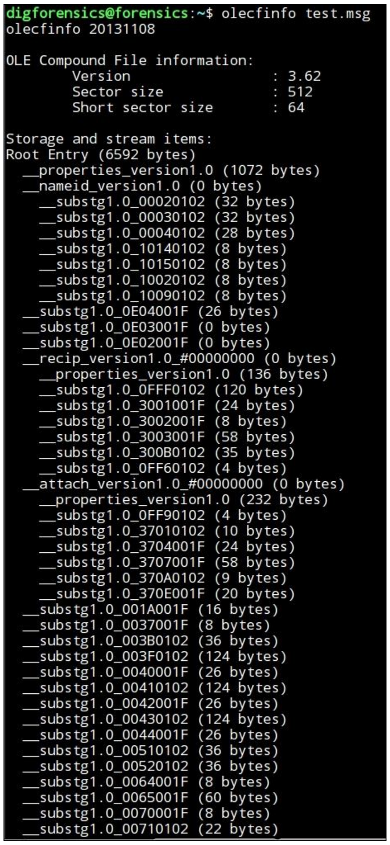


MozillaCacheView: C:\Users\AymanT\AppData\Local\Mozilla\Firefox\Pro...

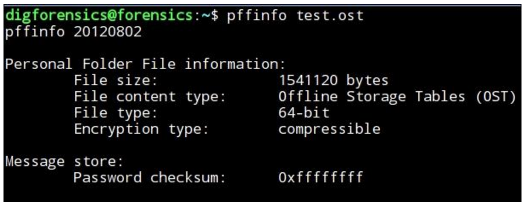
Filename	Content Type	URL	File Size
!1m4!1m3!1i10...	image/png	http://mt0.googleapis.com/vt?pb=!1m4!1...	13,741
!1m4!1m3!1i10...	image/png	http://mt1.googleapis.com/vt?pb=!1m4!1...	7,177
!1m4!1m3!1i15...	image/png	http://mt1.googleapis.com/vt?pb=!1m4!1...	1,979
!1m4!1m3!1i15...	image/png	http://mt1.googleapis.com/vt?pb=!1m4!1...	2,822
!1m4!1m3!1i15...	image/png	http://mt1.googleapis.com/vt?pb=!1m4!1...	4,309
!1m4!1m3!1i15...	image/png	http://mt0.googleapis.com/vt?pb=!1m4!1...	1,126
!1m4!1m3!1i15...	image/png	http://mt0.googleapis.com/vt?pb=!1m4!1...	1,390
!1m4!1m3!1i15...	image/png	http://mt0.googleapis.com/vt?pb=!1m4!1...	3,895

17444 item(s)

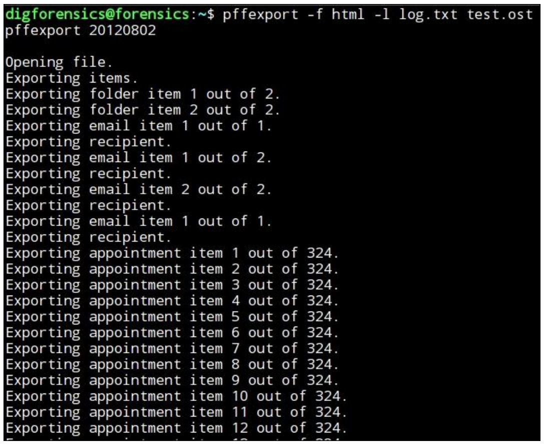
NirSoft Freeware. http://www.nirsoft.net



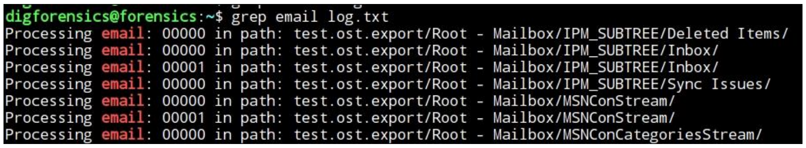
```
digforensics@forensics:~$ olecfinfo test.msg
olecfinfo 20131108

OLE Compound File information:
        Version                 : 3.62
        Sector size             : 512
        Short sector size       : 64

Storage and stream items:
Root Entry (6592 bytes)
  __properties_version1.0 (1072 bytes)
  __nameid_version1.0 (0 bytes)
    __substg1.0_00020102 (32 bytes)
    __substg1.0_00030102 (32 bytes)
    __substg1.0_00040102 (28 bytes)
    __substg1.0_10140102 (8 bytes)
    __substg1.0_10150102 (8 bytes)
    __substg1.0_10020102 (8 bytes)
    __substg1.0_10090102 (8 bytes)
  __substg1.0_0E04001F (26 bytes)
  __substg1.0_0E03001F (0 bytes)
  __substg1.0_0E02001F (0 bytes)
  __recip_version1.0_#00000000 (0 bytes)
    __properties_version1.0 (136 bytes)
    __substg1.0_0FFF0102 (120 bytes)
    __substg1.0_3001001F (24 bytes)
    __substg1.0_3002001F (8 bytes)
    __substg1.0_3003001F (58 bytes)
    __substg1.0_300B0102 (35 bytes)
    __substg1.0_0FF60102 (4 bytes)
  __attach_version1.0_#00000000 (0 bytes)
    __properties_version1.0 (232 bytes)
    __substg1.0_0FF90102 (4 bytes)
    __substg1.0_37010102 (10 bytes)
    __substg1.0_3704001F (24 bytes)
    __substg1.0_3707001F (58 bytes)
    __substg1.0_370A0102 (9 bytes)
    __substg1.0_370E001F (20 bytes)
  __substg1.0_001A001F (16 bytes)
  __substg1.0_0037001F (8 bytes)
  __substg1.0_003B0102 (36 bytes)
  __substg1.0_003F0102 (124 bytes)
  __substg1.0_0040001F (26 bytes)
  __substg1.0_00410102 (124 bytes)
  __substg1.0_0042001F (26 bytes)
  __substg1.0_00430102 (124 bytes)
  __substg1.0_0044001F (26 bytes)
  __substg1.0_00510102 (36 bytes)
  __substg1.0_00520102 (36 bytes)
  __substg1.0_0064001F (8 bytes)
  __substg1.0_0065001F (60 bytes)
  __substg1.0_0070001F (8 bytes)
  __substg1.0_00710102 (22 bytes)
```



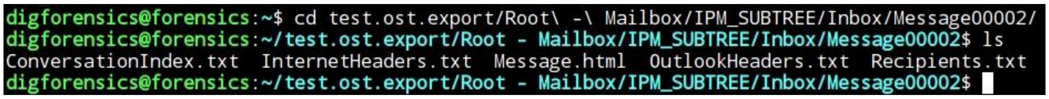
```
digforensics@forensics:~$ pffinfo test.ost
pffinfo 20120802

Personal Folder File information:
        File size:              1541120 bytes
        File content type:      Offline Storage Tables (OST)
        File type:              64-bit
        Encryption type:        compressible

Message store:
        Password checksum:      0xffffffff
```



```
digforensics@forensics:~$ pffexport -f html -l log.txt test.ost
pffexport 20120802

Opening file.
Exporting items.
Exporting folder item 1 out of 2.
Exporting folder item 2 out of 2.
Exporting email item 1 out of 1.
Exporting recipient.
Exporting email item 1 out of 2.
Exporting recipient.
Exporting email item 2 out of 2.
Exporting recipient.
Exporting email item 1 out of 1.
Exporting recipient.
Exporting appointment item 1 out of 324.
Exporting appointment item 2 out of 324.
Exporting appointment item 3 out of 324.
Exporting appointment item 4 out of 324.
Exporting appointment item 5 out of 324.
Exporting appointment item 6 out of 324.
Exporting appointment item 7 out of 324.
Exporting appointment item 8 out of 324.
Exporting appointment item 9 out of 324.
Exporting appointment item 10 out of 324.
Exporting appointment item 11 out of 324.
Exporting appointment item 12 out of 324.
```

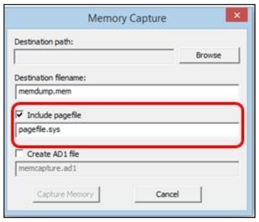


```
digforensics@forensics:~$ grep email log.txt
Processing email: 00000 in path: test.ost.export/Root - Mailbox/IPM_SUBTREE/Deleted Items/
Processing email: 00000 in path: test.ost.export/Root - Mailbox/IPM_SUBTREE/Inbox/
Processing email: 00001 in path: test.ost.export/Root - Mailbox/IPM_SUBTREE/Inbox/
Processing email: 00000 in path: test.ost.export/Root - Mailbox/IPM_SUBTREE/Sync Issues/
Processing email: 00000 in path: test.ost.export/Root - Mailbox/MSNConStream/
Processing email: 00001 in path: test.ost.export/Root - Mailbox/MSNConStream/
Processing email: 00000 in path: test.ost.export/Root - Mailbox/MSNConCategoriesStream/
```



```
digforensics@forensics:~$ cd test.ost.export/Root\ -\ Mailbox/IPM_SUBTREE/Inbox/Message00002/
digforensics@forensics:~/test.ost.export/Root - Mailbox/IPM_SUBTREE/Inbox/Message00002$ ls
ConversationIndex.txt  InternetHeaders.txt  Message.html  OutlookHeaders.txt  Recipients.txt
digforensics@forensics:~/test.ost.export/Root - Mailbox/IPM_SUBTREE/Inbox/Message00002$ 
```

Chapter 11: Memory Forensics



Memory Capture

Destination path:

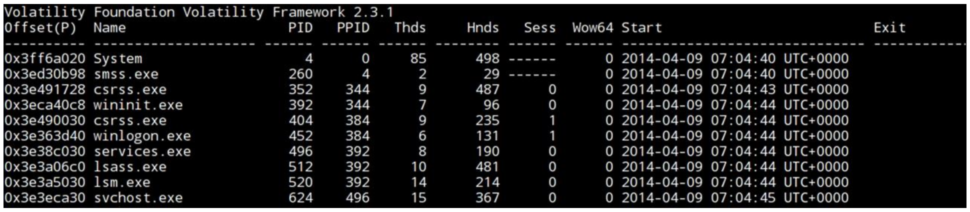
Destination filename: memdump.mem

☑ Include pagefile

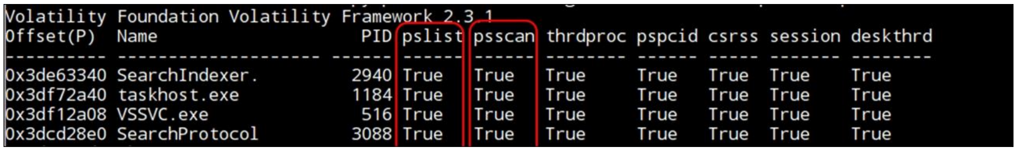
pagefile.sys

□ Create AD1 file

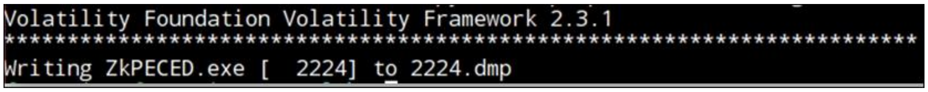
memcapture.ad1



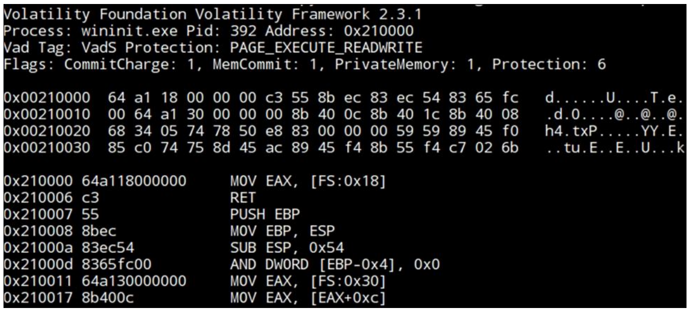
```
Volatility Foundation Volatility Framework 2.3.1
Offset(P)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ -----------
0x3ff6a020 System                    4      0     85      498 ------      0 2014-04-09 07:04:40 UTC+0000
0x3ed30b98 smss.exe                260      4      2       29 ------      0 2014-04-09 07:04:40 UTC+0000
0x3e491728 csrss.exe               352    344      9      487      0      0 2014-04-09 07:04:43 UTC+0000
0x3eca40c8 wininit.exe             392    344      7       96      0      0 2014-04-09 07:04:44 UTC+0000
0x3e490030 csrss.exe               404    384      9      235      1      0 2014-04-09 07:04:44 UTC+0000
0x3e363d40 winlogon.exe            452    384      6      131      1      0 2014-04-09 07:04:44 UTC+0000
0x3e38c030 services.exe            496    392      8      190      0      0 2014-04-09 07:04:44 UTC+0000
0x3e3a06c0 lsass.exe               512    392     10      481      0      0 2014-04-09 07:04:44 UTC+0000
0x3e3a5030 lsm.exe                 520    392     14      214      0      0 2014-04-09 07:04:44 UTC+0000
0x3e3eca30 svchost.exe             624    496     15      367      0      0 2014-04-09 07:04:45 UTC+0000
```



```
Volatility Foundation Volatility Framework 2.3.1
Offset(P)  Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd
---------- -------------------- ------ ------ ------ -------- ------ ----- ------- --------
0x3de63340 SearchIndexer.         2940 True   True   True     True   True  True    True
0x3df72a40 taskhost.exe           1184 True   True   True     True   True  True    True
0x3df12a08 VSSVC.exe               516 True   True   True     True   True  True    True
0x3dcd28e0 SearchProtocol         3088 True   True   True     True   True  True    True
```

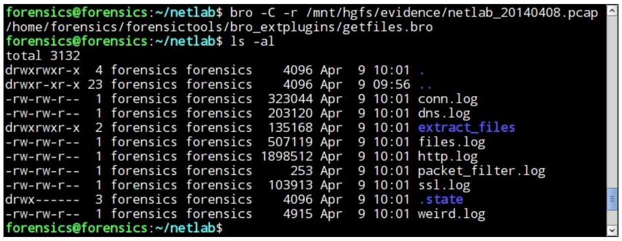


```
Volatility Foundation Volatility Framework 2.3.1
**************************************************************************
Writing ZkPECED.exe [   2224] to 2224.dmp
```

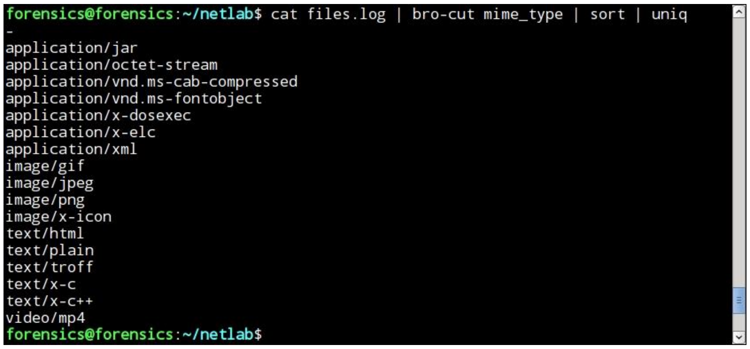


```
Volatility Foundation Volatility Framework 2.3.1
Process: wininit.exe Pid: 392 Address: 0x210000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00210000  64 a1 18 00 00 00 c3 55 8b ec 83 ec 54 83 65 fc   d......U....T.e.
0x00210010  00 64 a1 30 00 00 00 8b 40 0c 8b 40 1c 8b 40 08   .d.0....@..@..@.
0x00210020  68 34 05 74 78 50 e8 83 00 00 00 59 59 89 45 f0   h4.txP.....YY.E.
0x00210030  85 c0 74 75 8d 45 ac 89 45 f4 8b 55 f4 c7 02 6b   ..tu.E..E..U...k

0x210000 64a118000000          MOV EAX, [FS:0x18]
0x210006 c3                    RET
0x210007 55                    PUSH EBP
0x210008 8bec                  MOV EBP, ESP
0x21000a 83ec54                SUB ESP, 0x54
0x21000d 8365fc00              AND DWORD [EBP-0x4], 0x0
0x210011 64a130000000          MOV EAX, [FS:0x30]
0x210017 8b400c                MOV EAX, [EAX+0xc]
```

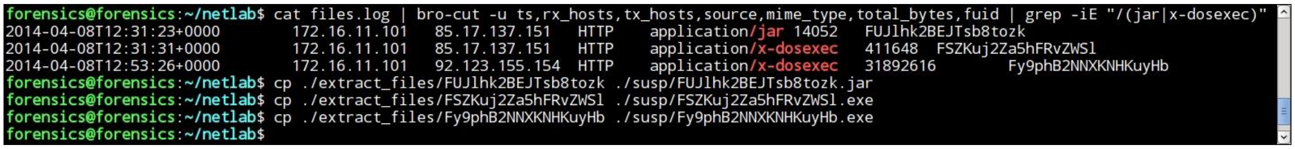
Chapter 12: Network Forensics



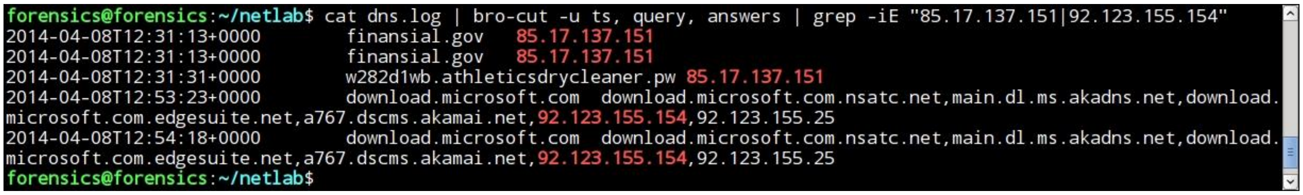
```
forensics@forensics:~/netlab$ bro -C -r /mnt/hgfs/evidence/netlab_20140408.pcap
/home/forensics/forensictools/bro_extplugins/getfiles.bro
forensics@forensics:~/netlab$ ls -al
total 3132
drwxrwxr-x  4 forensics forensics    4096 Apr  9 10:01 .
drwxr-xr-x 23 forensics forensics    4096 Apr  9 09:56 ..
-rw-rw-r--  1 forensics forensics  323044 Apr  9 10:01 conn.log
-rw-rw-r--  1 forensics forensics  203120 Apr  9 10:01 dns.log
drwxrwxr-x  2 forensics forensics  135168 Apr  9 10:01 extract_files
-rw-rw-r--  1 forensics forensics  507119 Apr  9 10:01 files.log
-rw-rw-r--  1 forensics forensics 1898512 Apr  9 10:01 http.log
-rw-rw-r--  1 forensics forensics     253 Apr  9 10:01 packet_filter.log
-rw-rw-r--  1 forensics forensics  103913 Apr  9 10:01 ssl.log
drwx------  3 forensics forensics    4096 Apr  9 10:01 .state
-rw-rw-r--  1 forensics forensics    4915 Apr  9 10:01 weird.log
forensics@forensics:~/netlab$
```



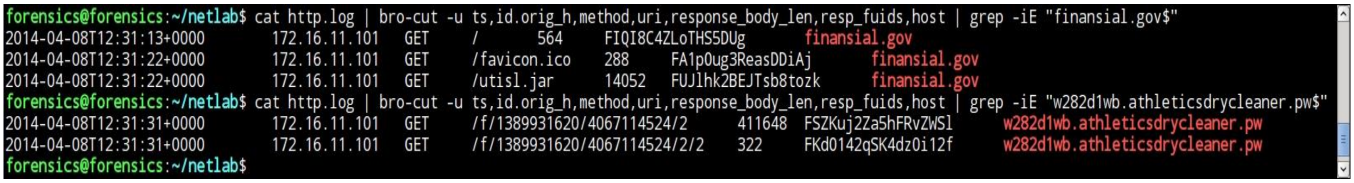
```
forensics@forensics:~/netlab$ cat files.log | bro-cut mime_type | sort | uniq
-
application/jar
application/octet-stream
application/vnd.ms-cab-compressed
application/vnd.ms-fontobject
application/x-dosexec
application/x-elc
application/xml
image/gif
image/jpeg
image/png
image/x-icon
text/html
text/plain
text/troff
text/x-c
text/x-c++
video/mp4
forensics@forensics:~/netlab$
```



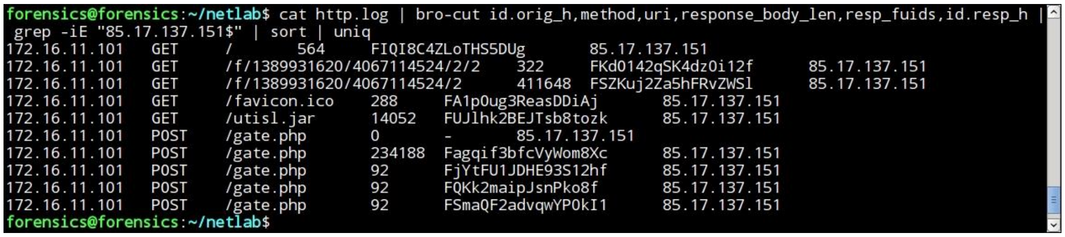
```
forensics@forensics:~/netlab$ cat files.log | bro-cut -u ts,rx_hosts,tx_hosts,source,mime_type,total_bytes,fuid | grep -iE "/(jar|x-dosexec)"
2014-04-08T12:31:23+0000        172.16.11.101   85.17.137.151   HTTP    application/jar 14052   FUJlhk2BEJTsb8tozk
2014-04-08T12:31:31+0000        172.16.11.101   85.17.137.151   HTTP    application/x-dosexec   411648  FSZKuj2Za5hFRvZWSl
2014-04-08T12:53:26+0000        172.16.11.101   92.123.155.154  HTTP    application/x-dosexec   31892616        Fy9phB2NNXKNHKuyHb
forensics@forensics:~/netlab$ cp ./extract_files/FUJlhk2BEJTsb8tozk ./susp/FUJlhk2BEJTsb8tozk.jar
forensics@forensics:~/netlab$ cp ./extract_files/FSZKuj2Za5hFRvZWSl ./susp/FSZKuj2Za5hFRvZWSl.exe
forensics@forensics:~/netlab$ cp ./extract_files/Fy9phB2NNXKNHKuyHb ./susp/Fy9phB2NNXKNHKuyHb.exe
forensics@forensics:~/netlab$
```



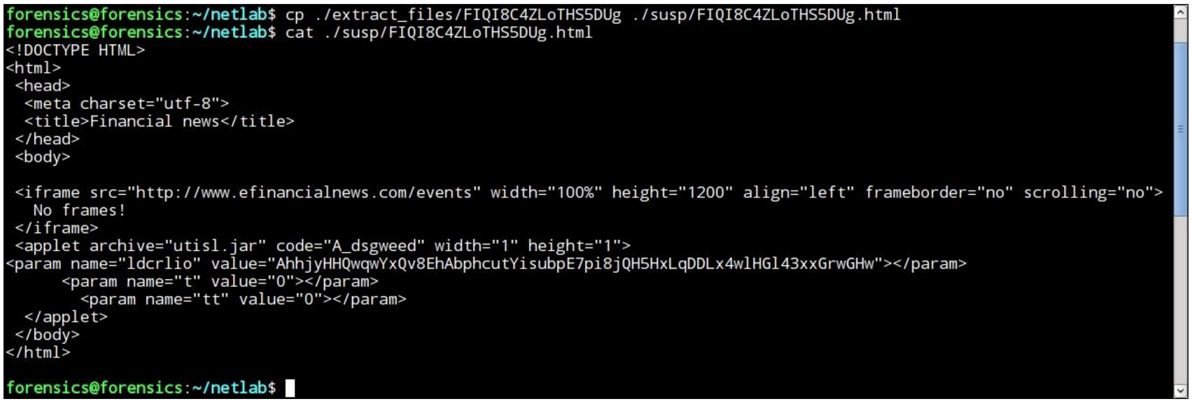
```
forensics@forensics:~/netlab$ cat dns.log | bro-cut -u ts, query, answers | grep -iE "85.17.137.151|92.123.155.154"
2014-04-08T12:31:13+0000        finansial.gov   85.17.137.151
2014-04-08T12:31:13+0000        finansial.gov   85.17.137.151
2014-04-08T12:31:31+0000        w282d1wb.athleticsdrycleaner.pw 85.17.137.151
2014-04-08T12:53:23+0000        download.microsoft.com  download.microsoft.com.nsatc.net,main.dl.ms.akadns.net,download.
microsoft.com.edgesuite.net,a767.dscms.akamai.net,92.123.155.154,92.123.155.25
2014-04-08T12:54:18+0000        download.microsoft.com  download.microsoft.com.nsatc.net,main.dl.ms.akadns.net,download.
microsoft.com.edgesuite.net,a767.dscms.akamai.net,92.123.155.154,92.123.155.25
forensics@forensics:~/netlab$
```



```
forensics@forensics:~/netlab$ cat http.log | bro-cut -u ts,id.orig_h,method,uri,response_body_len,resp_fuids,host | grep -iE "finansial.gov$"
2014-04-08T12:31:13+0000        172.16.11.101   GET     /       564     FIQI8C4ZLoTHS5DUg       finansial.gov
2014-04-08T12:31:22+0000        172.16.11.101   GET     /favicon.ico    288     FA1p0ug3ReasDDiAj       finansial.gov
2014-04-08T12:31:22+0000        172.16.11.101   GET     /utisl.jar      14052   FUJlhk2BEJTsb8tozk      finansial.gov
forensics@forensics:~/netlab$ cat http.log | bro-cut -u ts,id.orig_h,method,uri,response_body_len,resp_fuids,host | grep -iE "w282d1wb.athleticsdrycleaner.pw$"
2014-04-08T12:31:31+0000        172.16.11.101   GET     /f/1389931620/4067114524/2      411648  FSZKuj2Za5hFRvZWSl      w282d1wb.athleticsdrycleaner.pw
2014-04-08T12:31:31+0000        172.16.11.101   GET     /f/1389931620/4067114524/2/2    322     FKd0142qSK4dz0i12f      w282d1wb.athleticsdrycleaner.pw
forensics@forensics:~/netlab$
```

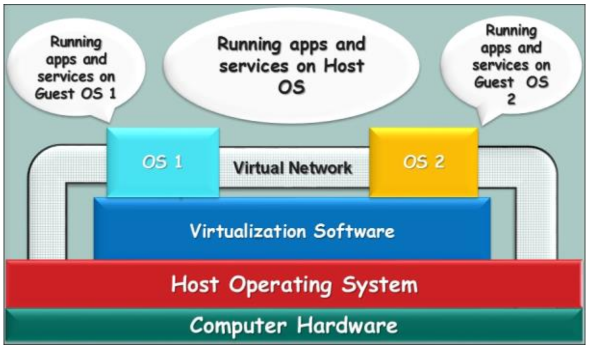


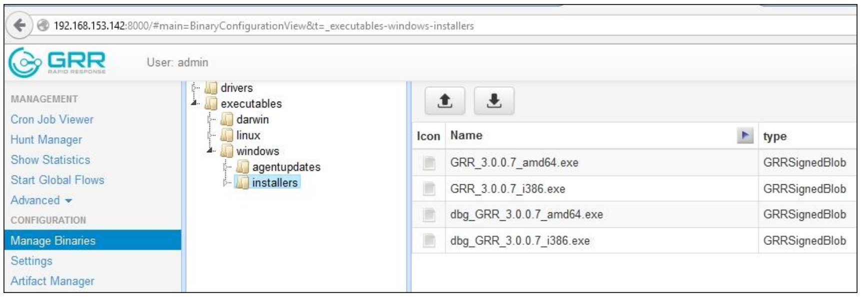
```
forensics@forensics:~/netlab$ cat http.log | bro-cut id.orig_h,method,uri,response_body_len,resp_fuids,id.resp_h |
 grep -iE "85.17.137.151$" | sort | uniq
172.16.11.101   GET     /       564     FIQI8C4ZLoTHS5DUg       85.17.137.151
172.16.11.101   GET     /f/1389931620/4067114524/2/2    322     FKd0142qSK4dz0i12f      85.17.137.151
172.16.11.101   GET     /f/1389931620/4067114524/2      411648  FSZKuj2Za5hFRvZWSl      85.17.137.151
172.16.11.101   GET     /favicon.ico    288     FA1p0ug3ReasDDiAj       85.17.137.151
172.16.11.101   GET     /utisl.jar      14052   FUJlhk2BEJTsb8tozk      85.17.137.151
172.16.11.101   POST    /gate.php       0       -       85.17.137.151
172.16.11.101   POST    /gate.php       234188  Fagqif3bfcVyWom8Xc      85.17.137.151
172.16.11.101   POST    /gate.php       92      FjYtFU1JDHE93S12hf      85.17.137.151
172.16.11.101   POST    /gate.php       92      FQKk2maipJsnPko8f       85.17.137.151
172.16.11.101   POST    /gate.php       92      FSmaQF2advqwYP0kI1      85.17.137.151
forensics@forensics:~/netlab$
```



```
forensics@forensics:~/netlab$ cp ./extract_files/FIQI8C4ZLoTHS5DUg ./susp/FIQI8C4ZLoTHS5DUg.html
forensics@forensics:~/netlab$ cat ./susp/FIQI8C4ZLoTHS5DUg.html
<!DOCTYPE HTML>
<html>
 <head>
  <meta charset="utf-8">
  <title>Financial news</title>
 </head>
 <body>

 <iframe src="http://www.efinancialnews.com/events" width="100%" height="1200" align="left" frameborder="no" scrolling="no">
   No frames!
 </iframe>
 <applet archive="utisl.jar" code="A_dsgweed" width="1" height="1">
<param name="ldcrlio" value="AhhjyHHQwqwYxQv8EhAbphcutYisubpE7pi8jQH5HxLqDDLx4wlHGl43xxGrwGHw"></param>
      <param name="t" value="0"></param>
        <param name="tt" value="0"></param>
  </applet>
 </body>
</html>

forensics@forensics:~/netlab$
```

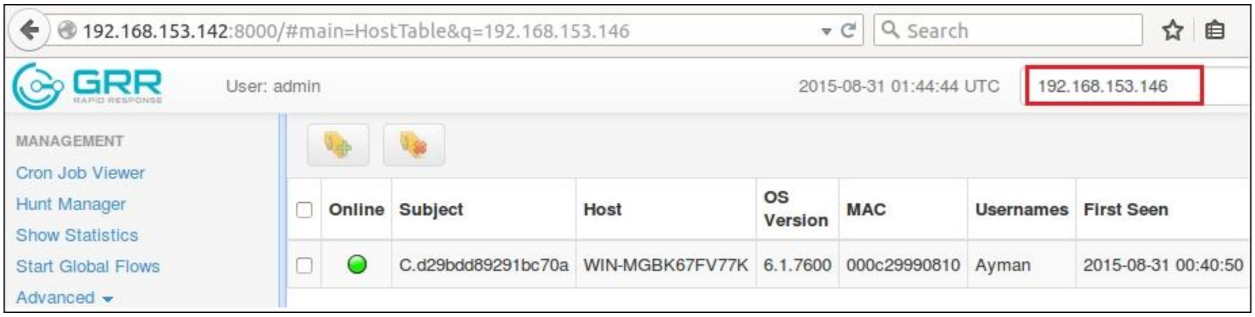
Appendix A: Building a Forensic Analysis Environment


Running apps and services on Guest OS 1
Running apps and services on Host OS
Running apps and services on Guest OS 2
OS 1
Virtual Network
OS 2
Virtualization Software
Host Operating System
Computer Hardware



192.168.153.142:8000/#main=BinaryConfigurationView&t=_executables-windows-installers

Icon	Name	type
	GRR_3.0.0.7_amd64.exe	GRRSignedBlob
	GRR_3.0.0.7_i386.exe	GRRSignedBlob
	dbg_GRR_3.0.0.7_amd64.exe	GRRSignedBlob
	dbg_GRR_3.0.0.7_i386.exe	GRRSignedBlob

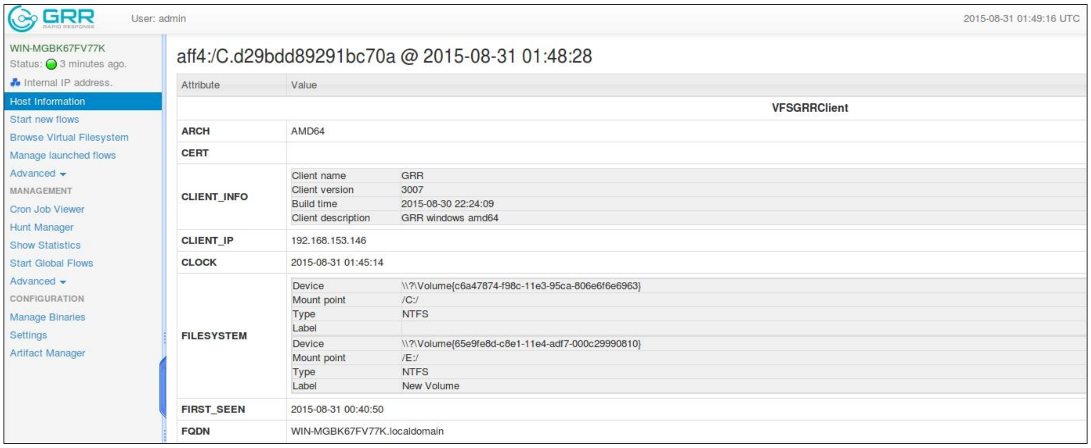


192.168.153.142:8000/#main=HostTable&q=192.168.153.146

2015-08-31 01:44:44 UTC

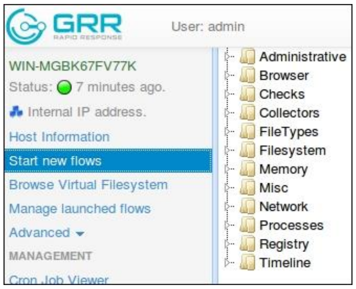
192.168.153.146

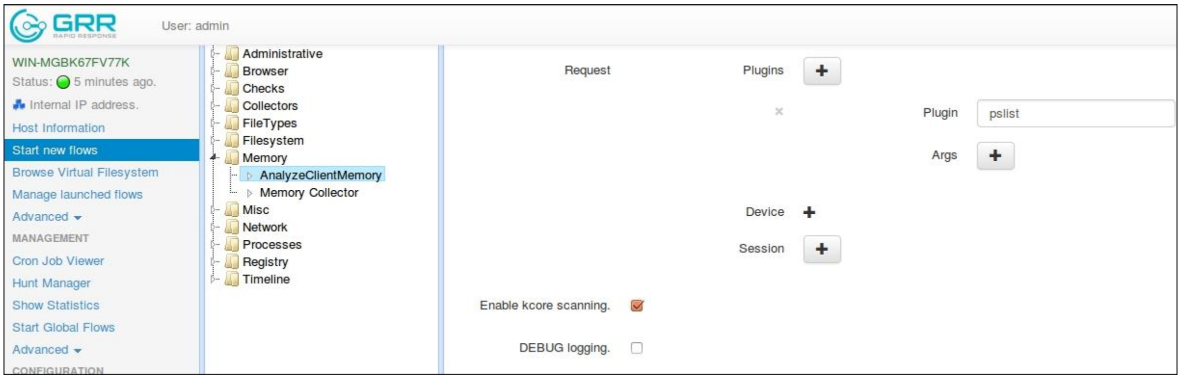
□	Online	Subject	Host	OS Version	MAC	Usernames	First Seen
□	●	C.d29bdd89291bc70a	WIN-MGBK67FV77K	6.1.7600	000c29990810	Ayman	2015-08-31 00:40:50



aff4:/C.d29bdd89291bc70a @ 2015-08-31 01:48:28

Attribute	Value
	VFSGRRClient
ARCH	AMD64
CERT	
CLIENT_INFO	Client name GRR Client version 3007 Build time 2015-08-30 22:24:09 Client description GRR windows amd64
CLIENT_IP	192.168.153.146
CLOCK	2015-08-31 01:45:14
FILESYSTEM	Device \\?\Volume{c6a47874-f98c-11e3-95ca-806e6f6e6963} Mount point /C:/ Type NTFS Label Device \\?\Volume{65e9fe8d-c8e1-11e4-adf7-000c29990810} Mount point /E:/ Type NTFS Label New Volume
FIRST_SEEN	2015-08-31 00:40:50
FQDN	WIN-MGBK67FV77K.localdomain

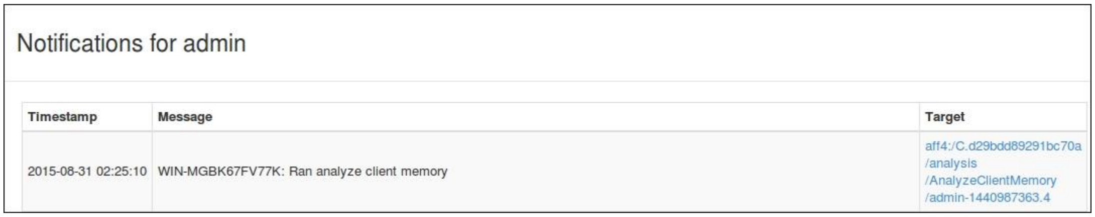




Plugin: pslist

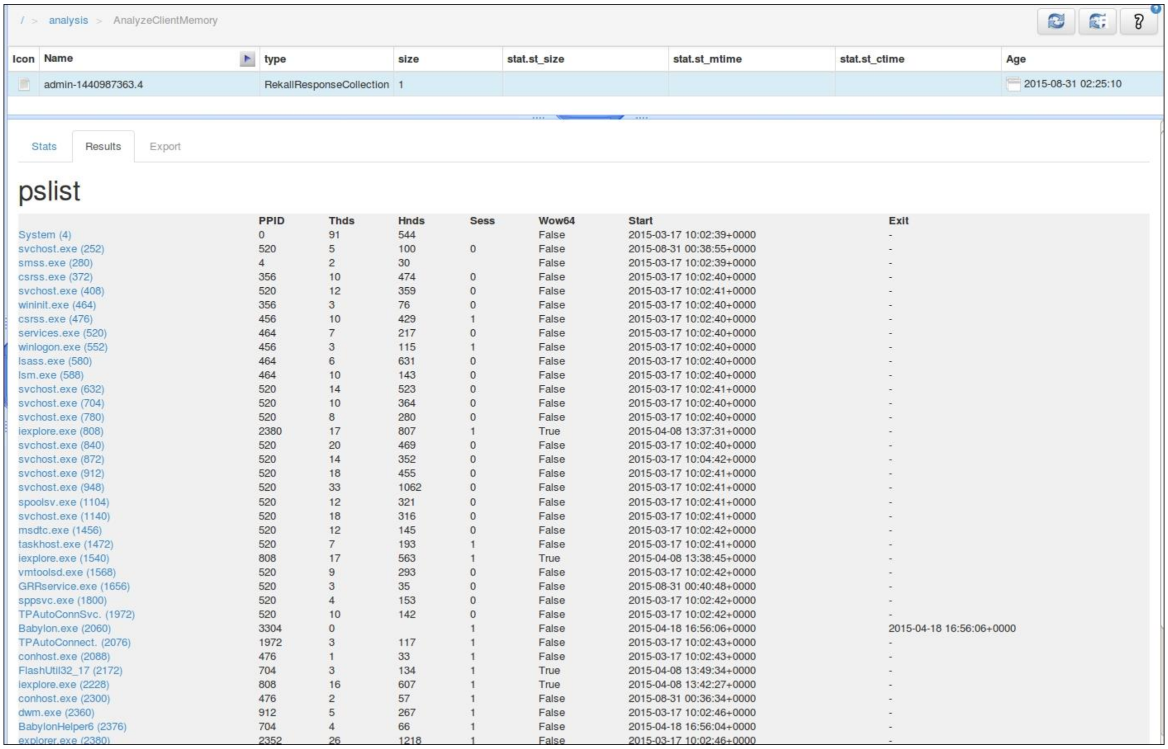
Enable kcore scanning. ☑

DEBUG logging. ☐



Notifications for admin

Timestamp	Message	Target
2015-08-31 02:25:10	WIN-MGBK67FV77K: Ran analyze client memory	aff4:/C.d29bdd89291bc70a /analysis /AnalyzeClientMemory /admin-1440987363.4

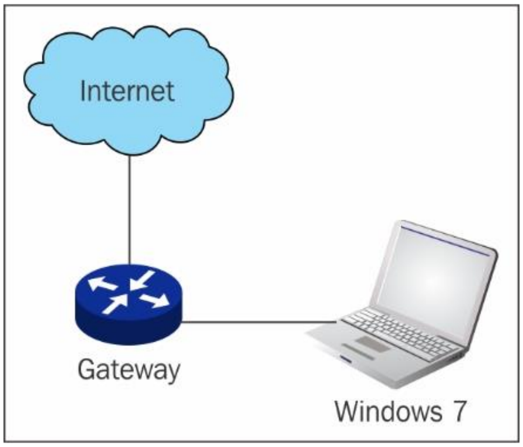


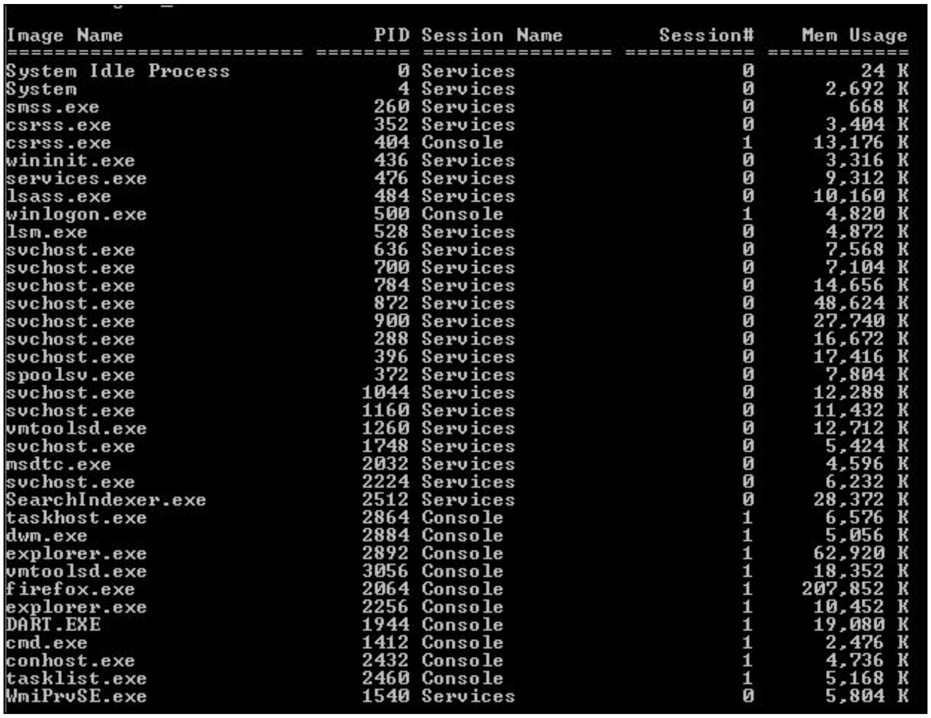
Icon	Name	type	size	stat.st_size	stat.st_mtime	stat.st_ctime	Age
	admin-1440987363.4	RekallResponseCollection	1				2015-08-31 02:25:10

pslist

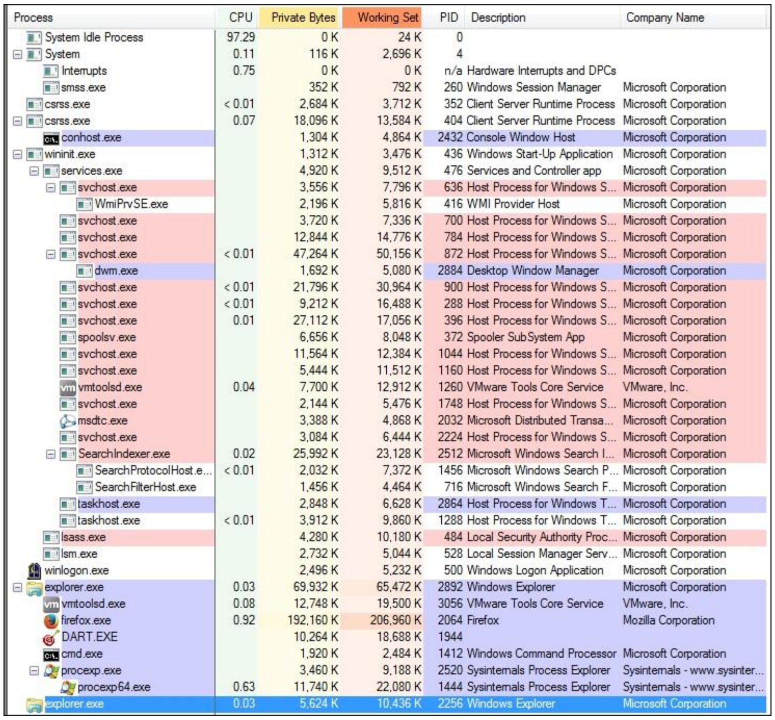
	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
System (4)	0	91	544		False	2015-03-17 10:02:39+0000	-
svchost.exe (252)	520	5	100	0	False	2015-08-31 00:38:55+0000	-
smss.exe (280)	4	2	30		False	2015-03-17 10:02:39+0000	-
csrss.exe (372)	356	10	474	0	False	2015-03-17 10:02:40+0000	-
svchost.exe (408)	520	12	359	0	False	2015-03-17 10:02:41+0000	-
wininit.exe (464)	356	3	76	0	False	2015-03-17 10:02:40+0000	-
csrss.exe (476)	456	10	429	1	False	2015-03-17 10:02:40+0000	-
services.exe (520)	464	7	217	0	False	2015-03-17 10:02:40+0000	-
winlogon.exe (552)	456	3	115	1	False	2015-03-17 10:02:40+0000	-
lsass.exe (580)	464	6	631	0	False	2015-03-17 10:02:40+0000	-
lsm.exe (588)	464	10	143	0	False	2015-03-17 10:02:40+0000	-
svchost.exe (632)	520	14	523	0	False	2015-03-17 10:02:41+0000	-
svchost.exe (704)	520	10	364	0	False	2015-03-17 10:02:40+0000	-
svchost.exe (780)	520	8	280	0	False	2015-03-17 10:02:40+0000	-
iexplore.exe (808)	2380	17	807	1	True	2015-04-08 13:37:31+0000	-
svchost.exe (840)	520	20	469	0	False	2015-03-17 10:02:40+0000	-
svchost.exe (872)	520	14	352	0	False	2015-03-17 10:04:42+0000	-
svchost.exe (912)	520	18	455	0	False	2015-03-17 10:02:41+0000	-
svchost.exe (948)	520	33	1062	0	False	2015-03-17 10:02:41+0000	-
spoolsv.exe (1104)	520	12	321	0	False	2015-03-17 10:02:41+0000	-
svchost.exe (1140)	520	18	316	0	False	2015-03-17 10:02:41+0000	-
msdtc.exe (1456)	520	12	145	0	False	2015-03-17 10:02:42+0000	-
taskhost.exe (1472)	520	7	193	1	False	2015-03-17 10:02:41+0000	-
iexplore.exe (1540)	808	17	563	1	True	2015-04-08 13:38:45+0000	-
vmtoolsd.exe (1568)	520	9	293	0	False	2015-03-17 10:02:42+0000	-
GRRservice.exe (1656)	520	3	35	0	False	2015-08-31 00:40:48+0000	-
sppsvc.exe (1800)	520	4	153	0	False	2015-03-17 10:02:42+0000	-
TPAutoConnSvc. (1972)	520	10	142	0	False	2015-03-17 10:02:42+0000	-
Babylon.exe (2060)	3304	0		1	False	2015-04-18 16:56:06+0000	2015-04-18 16:56:06+0000
TPAutoConnect. (2076)	1972	3	117	1	False	2015-03-17 10:02:43+0000	-
conhost.exe (2088)	476	1	33	1	False	2015-03-17 10:02:43+0000	-
FlashUtil32_17 (2172)	704	3	134	1	True	2015-04-08 13:49:34+0000	-
iexplore.exe (2228)	808	16	607	1	True	2015-04-08 13:42:27+0000	-
conhost.exe (2300)	476	2	57	1	False	2015-08-31 00:36:34+0000	-
dwm.exe (2360)	912	5	267	1	False	2015-03-17 10:02:46+0000	-
BabylonHelper6 (2376)	704	4	66	1	False	2015-04-18 16:56:04+0000	-
explorer.exe (2380)	2352	26	1218	1	False	2015-03-17 10:02:46+0000	-

Appendix B: Case Study

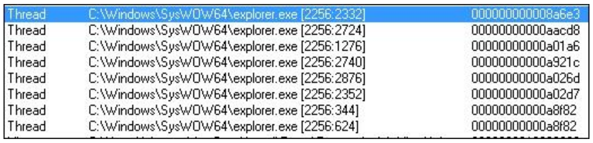




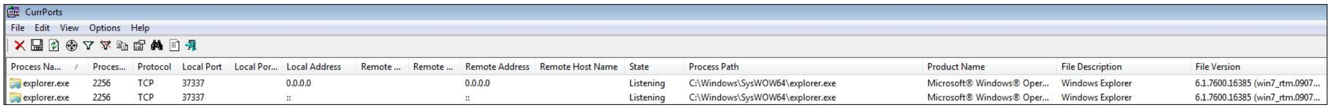
```
Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0         24 K
System                           4 Services                   0      2,692 K
smss.exe                       260 Services                   0        668 K
csrss.exe                      352 Services                   0      3,404 K
csrss.exe                      404 Console                    1     13,176 K
wininit.exe                    436 Services                   0      3,316 K
services.exe                   476 Services                   0      9,312 K
lsass.exe                      484 Services                   0     10,160 K
winlogon.exe                   500 Console                    1      4,820 K
lsm.exe                        528 Services                   0      4,872 K
svchost.exe                    636 Services                   0      7,568 K
svchost.exe                    700 Services                   0      7,104 K
svchost.exe                    784 Services                   0     14,656 K
svchost.exe                    872 Services                   0     48,624 K
svchost.exe                    900 Services                   0     27,740 K
svchost.exe                    288 Services                   0     16,672 K
svchost.exe                    396 Services                   0     17,416 K
spoolsv.exe                    372 Services                   0      7,804 K
svchost.exe                   1044 Services                   0     12,288 K
svchost.exe                   1160 Services                   0     11,432 K
vmtoolsd.exe                  1260 Services                   0     12,712 K
svchost.exe                   1748 Services                   0      5,424 K
msdtc.exe                     2032 Services                   0      4,596 K
svchost.exe                   2224 Services                   0      6,232 K
SearchIndexer.exe             2512 Services                   0     28,372 K
taskhost.exe                  2864 Console                    1      6,576 K
dwm.exe                       2884 Console                    1      5,056 K
explorer.exe                  2892 Console                    1     62,920 K
vmtoolsd.exe                  3056 Console                    1     18,352 K
firefox.exe                   2064 Console                    1    207,852 K
explorer.exe                  2256 Console                    1     10,452 K
DART.EXE                      1944 Console                    1     19,080 K
cmd.exe                       1412 Console                    1      2,476 K
conhost.exe                   2432 Console                    1      4,736 K
tasklist.exe                  2460 Console                    1      5,168 K
WmiPrvSE.exe                  1540 Services                   0      5,804 K
```



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	97.29	0 K	24 K	0		
System	0.11	116 K	2,696 K	4		
Interrupts	0.75	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		352 K	792 K	260	Windows Session Manager	Microsoft Corporation
csrss.exe	< 0.01	2,684 K	3,712 K	352	Client Server Runtime Process	Microsoft Corporation
csrss.exe	0.07	18,096 K	13,584 K	404	Client Server Runtime Process	Microsoft Corporation
conhost.exe		1,304 K	4,864 K	2432	Console Window Host	Microsoft Corporation
wininit.exe		1,312 K	3,476 K	436	Windows Start-Up Application	Microsoft Corporation
services.exe		4,920 K	9,512 K	476	Services and Controller app	Microsoft Corporation
svchost.exe		3,556 K	7,796 K	636	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe		2,196 K	5,816 K	416	WMI Provider Host	Microsoft Corporation
svchost.exe		3,720 K	7,336 K	700	Host Process for Windows S...	Microsoft Corporation
svchost.exe		12,844 K	14,776 K	784	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	47,264 K	50,156 K	872	Host Process for Windows S...	Microsoft Corporation
dwm.exe		1,692 K	5,080 K	2884	Desktop Window Manager	Microsoft Corporation
svchost.exe	< 0.01	21,796 K	30,964 K	900	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	9,212 K	16,488 K	288	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.01	27,112 K	17,056 K	396	Host Process for Windows S...	Microsoft Corporation
spoolsv.exe		6,656 K	8,048 K	372	Spooler SubSystem App	Microsoft Corporation
svchost.exe		11,564 K	12,384 K	1044	Host Process for Windows S...	Microsoft Corporation
svchost.exe		5,444 K	11,512 K	1160	Host Process for Windows S...	Microsoft Corporation
vmtoolsd.exe	0.04	7,700 K	12,912 K	1260	VMware Tools Core Service	VMware, Inc.
svchost.exe		2,144 K	5,476 K	1748	Host Process for Windows S...	Microsoft Corporation
msdtc.exe		3,388 K	4,868 K	2032	Microsoft Distributed Transa...	Microsoft Corporation
svchost.exe		3,084 K	6,444 K	2224	Host Process for Windows S...	Microsoft Corporation
SearchIndexer.exe	0.02	25,992 K	23,128 K	2512	Microsoft Windows Search I...	Microsoft Corporation
SearchProtocolHost.e...	< 0.01	2,032 K	7,372 K	1456	Microsoft Windows Search P...	Microsoft Corporation
SearchFilterHost.exe		1,456 K	4,464 K	716	Microsoft Windows Search F...	Microsoft Corporation
taskhost.exe		2,848 K	6,628 K	2864	Host Process for Windows T...	Microsoft Corporation
taskhost.exe	< 0.01	3,912 K	9,860 K	1288	Host Process for Windows T...	Microsoft Corporation
lsass.exe		4,280 K	10,180 K	484	Local Security Authority Proc...	Microsoft Corporation
lsm.exe		2,732 K	5,044 K	528	Local Session Manager Serv...	Microsoft Corporation
winlogon.exe		2,496 K	5,232 K	500	Windows Logon Application	Microsoft Corporation
explorer.exe	0.03	69,932 K	65,472 K	2892	Windows Explorer	Microsoft Corporation
vmtoolsd.exe	0.08	12,748 K	19,500 K	3056	VMware Tools Core Service	VMware, Inc.
firefox.exe	0.92	192,160 K	206,960 K	2064	Firefox	Mozilla Corporation
DART.EXE		10,264 K	18,688 K	1944		
cmd.exe		1,920 K	2,484 K	1412	Windows Command Processor	Microsoft Corporation
procexp.exe		3,460 K	9,188 K	2520	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	0.63	11,740 K	22,080 K	1444	Sysinternals Process Explorer	Sysinternals - www.sysinter...
explorer.exe	0.03	5,624 K	10,436 K	2256	Windows Explorer	Microsoft Corporation

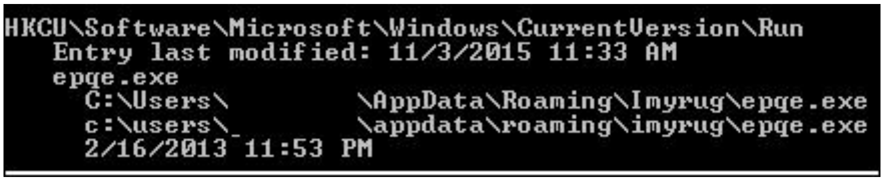


Thread	C:\Windows\SysWOW64\explorer.exe [2256:2332]	00000000008a6e3
Thread	C:\Windows\SysWOW64\explorer.exe [2256:2724]	00000000000aacd8
Thread	C:\Windows\SysWOW64\explorer.exe [2256:1276]	00000000000a01a6
Thread	C:\Windows\SysWOW64\explorer.exe [2256:2740]	00000000000a921c
Thread	C:\Windows\SysWOW64\explorer.exe [2256:2876]	00000000000a026d
Thread	C:\Windows\SysWOW64\explorer.exe [2256:2352]	00000000000a02d7
Thread	C:\Windows\SysWOW64\explorer.exe [2256:344]	00000000000a8f82
Thread	C:\Windows\SysWOW64\explorer.exe [2256:624]	00000000000a8f82

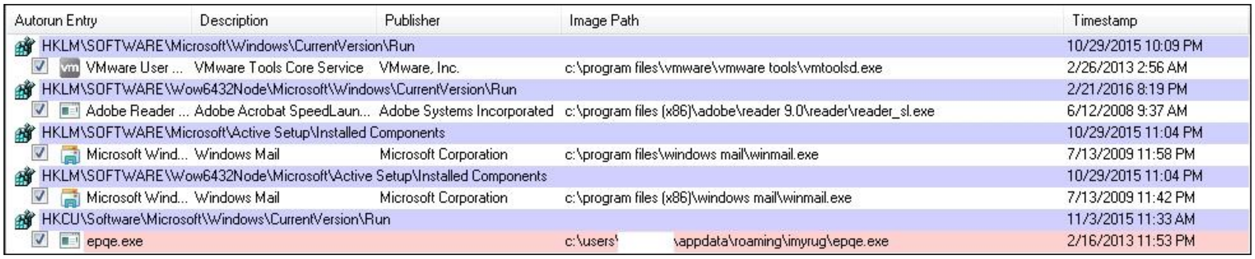


CurrPorts

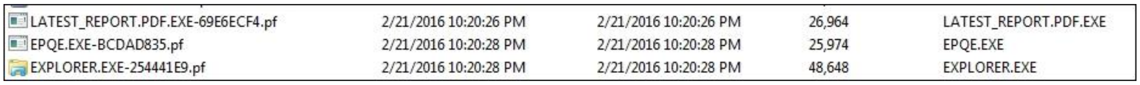
Process Na...	Proces...	Protocol	Local Port	Local Por...	Local Address	Remote ...	Remote ...	Remote Address	Remote Host Name	State	Process Path	Product Name	File Description	File Version
explorer.exe	2256	TCP	37337		0.0.0.0			0.0.0.0		Listening	C:\Windows\SysWOW64\explorer.exe	Microsoft® Windows® Oper...	Windows Explorer	6.1.7600.16385 (win7_rtm.0907...
explorer.exe	2256	TCP	37337		::			::		Listening	C:\Windows\SysWOW64\explorer.exe	Microsoft® Windows® Oper...	Windows Explorer	6.1.7600.16385 (win7_rtm.0907...



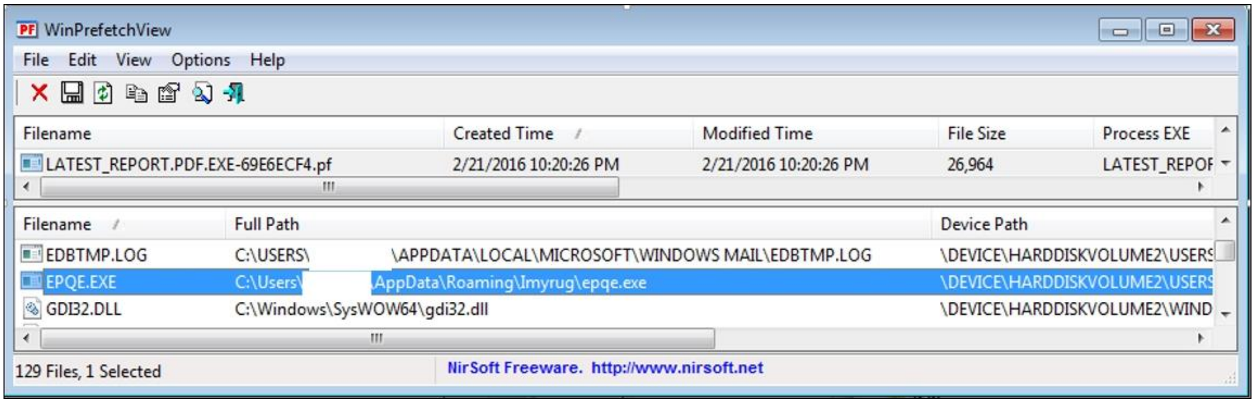
```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
   Entry last modified: 11/3/2015 11:33 AM
   epqe.exe
     C:\Users\[redacted]\AppData\Roaming\Imyrug\epqe.exe
     c:\users\[redacted]\appdata\roaming\imyrug\epqe.exe
     2/16/2013 11:53 PM
```



Autorun Entry	Description	Publisher	Image Path	Timestamp
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				10/29/2015 10:09 PM
☑ VMware User ...	VMware Tools Core Service	VMware, Inc.	c:\program files\vmware\vmware tools\vmtoolsd.exe	2/26/2013 2:56 AM
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				2/21/2016 8:19 PM
☑ Adobe Reader ...	Adobe Acrobat SpeedLaun...	Adobe Systems Incorporated	c:\program files (x86)\adobe\reader 9.0\reader\reader_sl.exe	6/12/2008 9:37 AM
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				10/29/2015 11:04 PM
☑ Microsoft Wind...	Windows Mail	Microsoft Corporation	c:\program files\windows mail\winmail.exe	7/13/2009 11:58 PM
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				10/29/2015 11:04 PM
☑ Microsoft Wind...	Windows Mail	Microsoft Corporation	c:\program files (x86)\windows mail\winmail.exe	7/13/2009 11:42 PM
HKCU\Software\Microsoft\Windows\CurrentVersion\Run				11/3/2015 11:33 AM
☑ epqe.exe			c:\users\[redacted]\appdata\roaming\imyrug\epqe.exe	2/16/2013 11:53 PM



LATEST_REPORT.PDF.EXE-69E6ECF4.pf	2/21/2016 10:20:26 PM	2/21/2016 10:20:26 PM	26,964	LATEST_REPORT.PDF.EXE
EPQE.EXE-BCDAD835.pf	2/21/2016 10:20:28 PM	2/21/2016 10:20:28 PM	25,974	EPQE.EXE
EXPLORER.EXE-254441E9.pf	2/21/2016 10:20:28 PM	2/21/2016 10:20:28 PM	48,648	EXPLORER.EXE

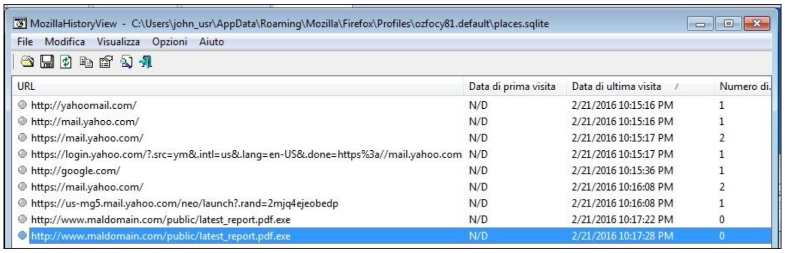


Filename	Created Time	Modified Time	File Size	Process EXE
LATEST_REPORT.PDF.EXE-69E6ECF4.pf	2/21/2016 10:20:26 PM	2/21/2016 10:20:26 PM	26,964	LATEST_REPOF

Filename	Full Path	Device Path
EDBTMP.LOG	C:\USERS\ \APPDATA\LOCAL\MICROSOFT\WINDOWS MAIL\EDBTMP.LOG	\DEVICE\HARDDISKVOLUME2\USERS
EPQE.EXE	C:\Users\ \AppData\Roaming\Imyrug\epqe.exe	\DEVICE\HARDDISKVOLUME2\USERS
GDI32.DLL	C:\Windows\SysWOW64\gdi32.dll	\DEVICE\HARDDISKVOLUME2\WIND

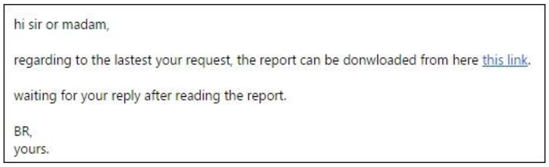
129 Files, 1 Selected

NirSoft Freeware. http://www.nirsoft.net



MozillaHistoryView - C:\Users\john_usr\AppData\Roaming\Mozilla\Firefox\Profiles\ozfocy81.default\places.sqlite
File Modifica Visualizza Opzioni Aiuto

URL	Data di prima visita	Data di ultima visita	Numero di.
http://yahoomail.com/	N/D	2/21/2016 10:15:16 PM	1
http://mail.yahoo.com/	N/D	2/21/2016 10:15:16 PM	1
https://mail.yahoo.com/	N/D	2/21/2016 10:15:17 PM	2
https://login.yahoo.com/?.src=ym&.intl=us&.lang=en-US&.done=https%3a//mail.yahoo.com	N/D	2/21/2016 10:15:17 PM	1
http://google.com/	N/D	2/21/2016 10:15:36 PM	1
https://mail.yahoo.com/	N/D	2/21/2016 10:16:08 PM	2
https://us-mg5.mail.yahoo.com/neo/launch?.rand=2mjq4ejeobedp	N/D	2/21/2016 10:16:08 PM	1
http://www.maldomain.com/public/latest_report.pdf.exe	N/D	2/21/2016 10:17:22 PM	0
http://www.maldomain.com/public/latest_report.pdf.exe	N/D	2/21/2016 10:17:28 PM	0

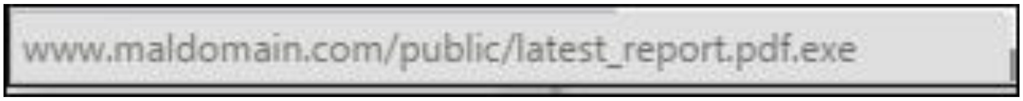


hi sir or madam,

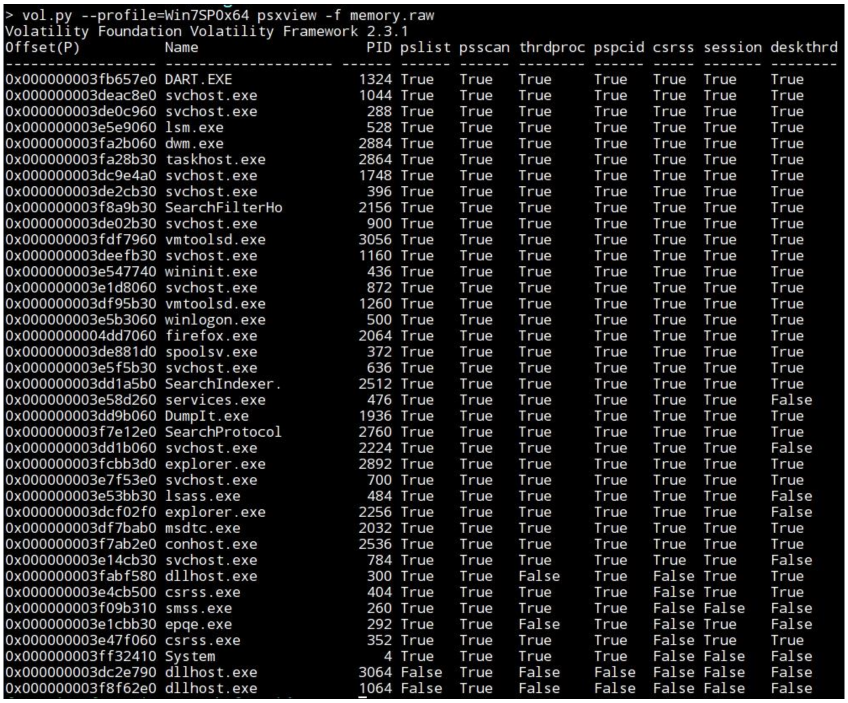
regarding to the lastest your request, the report can be donwloaded from here this link.

waiting for your reply after reading the report.

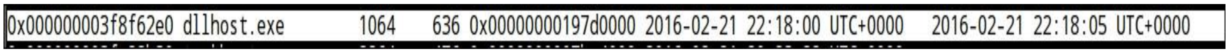
BR,
yours.



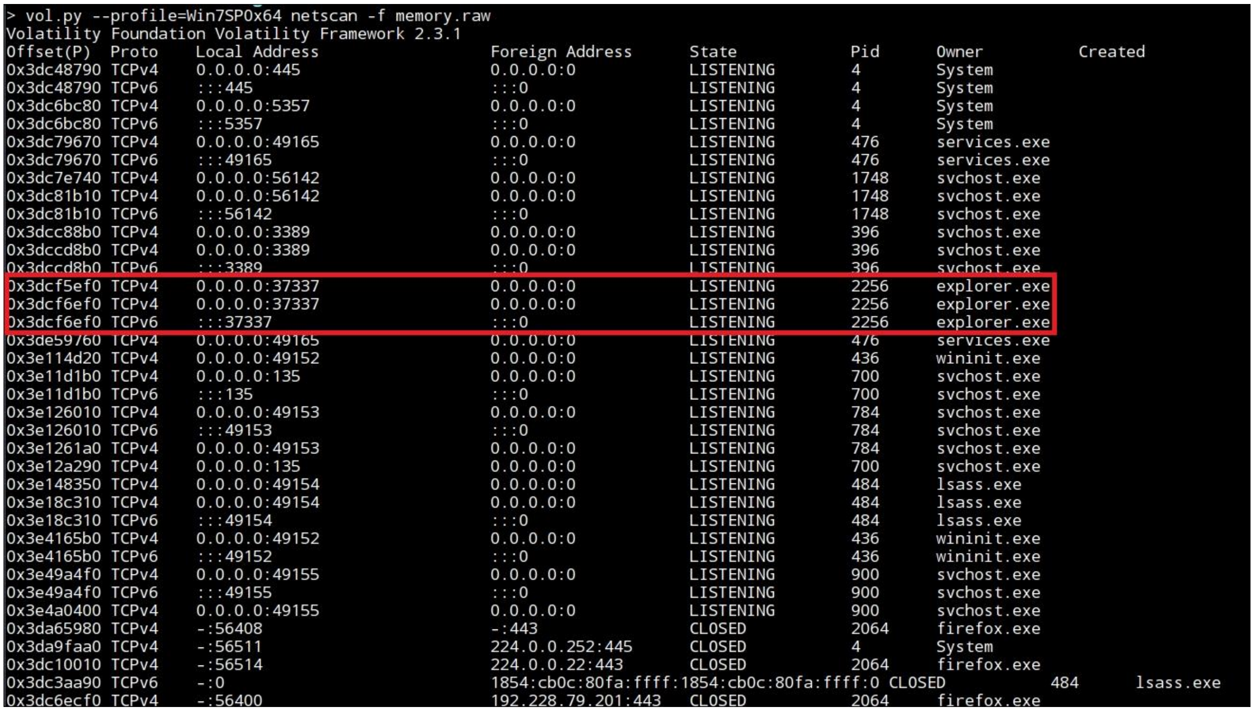
www.maldomain.com/public/latest_report.pdf.exe



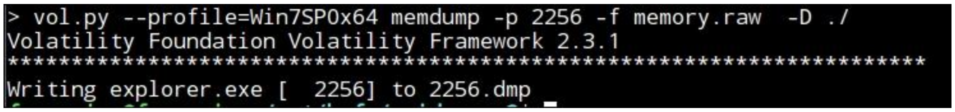
```
> vol.py --profile=Win7SP0x64 psxview -f memory.raw
Volatility Foundation Volatility Framework 2.3.1
Offset(P)          Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd
------------------ -------------------- ------ ------ ------ -------- ------ ----- ------- --------
0x000000003fb657e0 DART.EXE               1324 True   True   True     True   True  True    True
0x000000003deac8e0 svchost.exe            1044 True   True   True     True   True  True    True
0x000000003de0c960 svchost.exe             288 True   True   True     True   True  True    True
0x000000003e5e9060 lsm.exe                 528 True   True   True     True   True  True    True
0x000000003fa2b060 dwm.exe                2884 True   True   True     True   True  True    True
0x000000003fa28b30 taskhost.exe           2864 True   True   True     True   True  True    True
0x000000003dc9e4a0 svchost.exe            1748 True   True   True     True   True  True    True
0x000000003de2cb30 svchost.exe             396 True   True   True     True   True  True    True
0x000000003f8a9b30 SearchFilterHo         2156 True   True   True     True   True  True    True
0x000000003de02b30 svchost.exe             900 True   True   True     True   True  True    True
0x000000003fdf7960 vmtoolsd.exe           3056 True   True   True     True   True  True    True
0x000000003deefb30 svchost.exe            1160 True   True   True     True   True  True    True
0x000000003e547740 wininit.exe             436 True   True   True     True   True  True    True
0x000000003e1d8060 svchost.exe             872 True   True   True     True   True  True    True
0x000000003df95b30 vmtoolsd.exe           1260 True   True   True     True   True  True    True
0x000000003e5b3060 winlogon.exe            500 True   True   True     True   True  True    True
0x000000004dd7060 firefox.exe            2064 True   True   True     True   True  True    True
0x000000003de881d0 spoolsv.exe             372 True   True   True     True   True  True    True
0x000000003e5f5b30 svchost.exe             636 True   True   True     True   True  True    True
0x000000003dd1a5b0 SearchIndexer.         2512 True   True   True     True   True  True    True
0x000000003e58d260 services.exe            476 True   True   True     True   True  True    False
0x000000003dd9b060 DumpIt.exe             1936 True   True   True     True   True  True    True
0x000000003f7e12e0 SearchProtocol         2760 True   True   True     True   True  True    True
0x000000003dd1b060 svchost.exe            2224 True   True   True     True   True  True    False
0x000000003fcbb3d0 explorer.exe           2892 True   True   True     True   True  True    True
0x000000003e7f53e0 svchost.exe             700 True   True   True     True   True  True    True
0x000000003e53bb30 lsass.exe               484 True   True   True     True   True  True    False
0x000000003dcf02f0 explorer.exe           2256 True   True   True     True   True  True    False
0x000000003df7bab0 msdtc.exe              2032 True   True   True     True   True  True    True
0x000000003f7ab2e0 conhost.exe            2536 True   True   True     True   True  True    True
0x000000003e14cb30 svchost.exe             784 True   True   True     True   True  True    False
0x000000003fabf580 dllhost.exe             300 True   True   False    True   False True    True
0x000000003e4cb500 csrss.exe               404 True   True   True     True   False True    True
0x000000003f09b310 smss.exe                260 True   True   True     True   False False   False
0x000000003e1cbb30 epqe.exe                292 True   True   False    True   False True    False
0x000000003e47f060 csrss.exe               352 True   True   True     True   False True    True
0x000000003ff32410 System                    4 True   True   True     True   False False   False
0x000000003dc2e790 dllhost.exe            3064 False  True   False    False  False False   False
0x000000003f8f62e0 dllhost.exe            1064 False  True   False    False  False False   False
```



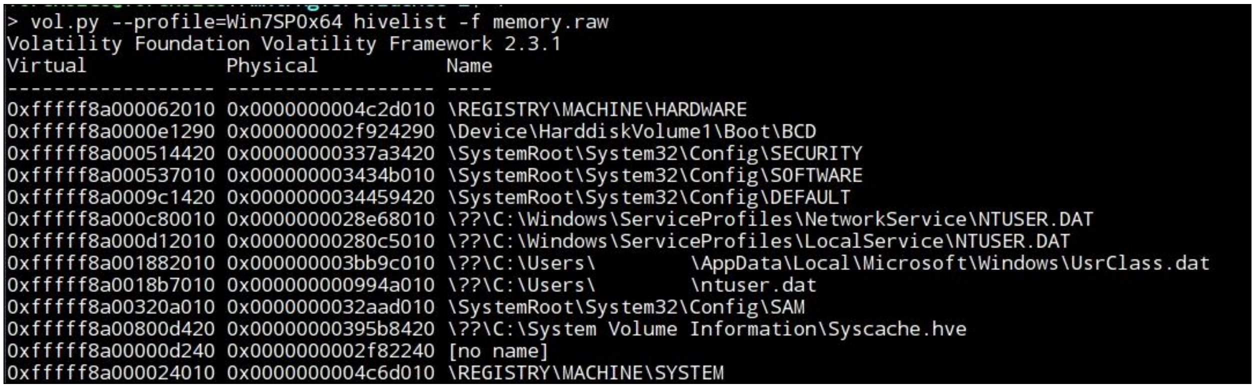
```
0x000000003f8f62e0 dllhost.exe          1064    636 0x00000000197d0000 2016-02-21 22:18:00 UTC+0000    2016-02-21 22:18:05 UTC+0000
```



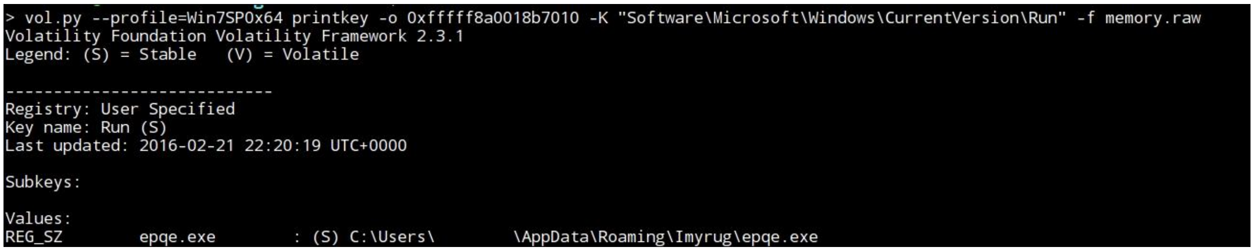
```
> vol.py --profile=Win7SP0x64 netscan -f memory.raw
Volatility Foundation Volatility Framework 2.3.1
Offset(P)  Proto    Local Address                  Foreign Address      State            Pid      Owner          Created
0x3dc48790 TCPv4    0.0.0.0:445                    0.0.0.0:0            LISTENING        4        System
0x3dc48790 TCPv6    :::445                         :::0                 LISTENING        4        System
0x3dc6bc80 TCPv4    0.0.0.0:5357                   0.0.0.0:0            LISTENING        4        System
0x3dc6bc80 TCPv6    :::5357                        :::0                 LISTENING        4        System
0x3dc79670 TCPv4    0.0.0.0:49165                  0.0.0.0:0            LISTENING        476      services.exe
0x3dc79670 TCPv6    :::49165                       :::0                 LISTENING        476      services.exe
0x3dc7e740 TCPv4    0.0.0.0:56142                  0.0.0.0:0            LISTENING        1748     svchost.exe
0x3dc81b10 TCPv4    0.0.0.0:56142                  0.0.0.0:0            LISTENING        1748     svchost.exe
0x3dc81b10 TCPv6    :::56142                       :::0                 LISTENING        1748     svchost.exe
0x3dcc88b0 TCPv4    0.0.0.0:3389                   0.0.0.0:0            LISTENING        396      svchost.exe
0x3dccd8b0 TCPv4    0.0.0.0:3389                   0.0.0.0:0            LISTENING        396      svchost.exe
0x3dccd8b0 TCPv6    :::3389                        :::0                 LISTENING        396      svchost.exe
0x3dcf5ef0 TCPv4    0.0.0.0:37337                  0.0.0.0:0            LISTENING        2256     explorer.exe
0x3dcf6ef0 TCPv4    0.0.0.0:37337                  0.0.0.0:0            LISTENING        2256     explorer.exe
0x3dcf6ef0 TCPv6    :::37337                       :::0                 LISTENING        2256     explorer.exe
0x3de59760 TCPv4    0.0.0.0:49165                  0.0.0.0:0            LISTENING        476      services.exe
0x3e114d20 TCPv4    0.0.0.0:49152                  0.0.0.0:0            LISTENING        436      wininit.exe
0x3e11d1b0 TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING        700      svchost.exe
0x3e11d1b0 TCPv6    :::135                         :::0                 LISTENING        700      svchost.exe
0x3e126010 TCPv4    0.0.0.0:49153                  0.0.0.0:0            LISTENING        784      svchost.exe
0x3e126010 TCPv6    :::49153                       :::0                 LISTENING        784      svchost.exe
0x3e1261a0 TCPv4    0.0.0.0:49153                  0.0.0.0:0            LISTENING        784      svchost.exe
0x3e12a290 TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING        700      svchost.exe
0x3e148350 TCPv4    0.0.0.0:49154                  0.0.0.0:0            LISTENING        484      lsass.exe
0x3e18c310 TCPv4    0.0.0.0:49154                  0.0.0.0:0            LISTENING        484      lsass.exe
0x3e18c310 TCPv6    :::49154                       :::0                 LISTENING        484      lsass.exe
0x3e4165b0 TCPv4    0.0.0.0:49152                  0.0.0.0:0            LISTENING        436      wininit.exe
0x3e4165b0 TCPv6    :::49152                       :::0                 LISTENING        436      wininit.exe
0x3e49a4f0 TCPv4    0.0.0.0:49155                  0.0.0.0:0            LISTENING        900      svchost.exe
0x3e49a4f0 TCPv6    :::49155                       :::0                 LISTENING        900      svchost.exe
0x3e4a0400 TCPv4    0.0.0.0:49155                  0.0.0.0:0            LISTENING        900      svchost.exe
0x3da65980 TCPv4    -:56408                        -:443                CLOSED           2064     firefox.exe
0x3da9faa0 TCPv4    -:56511                        224.0.0.252:445      CLOSED           4        System
0x3dc10010 TCPv4    -:56514                        224.0.0.22:443       CLOSED           2064     firefox.exe
0x3dc3aa90 TCPv6    -:0                            1854:cb0c:80fa:ffff:1854:cb0c:80fa:ffff:0 CLOSED           484      lsass.exe
0x3dc6ecf0 TCPv4    -:56400                        192.228.79.201:443   CLOSED           2064     firefox.exe
```



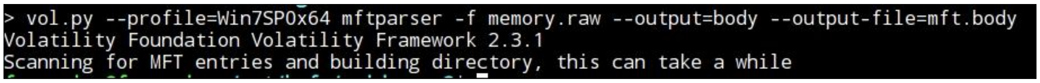
```
> vol.py --profile=Win7SP0x64 memdump -p 2256 -f memory.raw  -D ./
Volatility Foundation Volatility Framework 2.3.1
************************************************************************
Writing explorer.exe [  2256] to 2256.dmp
```



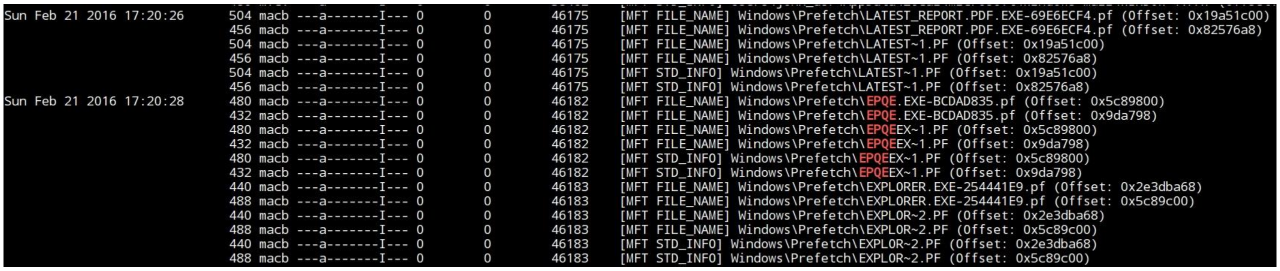
```
> vol.py --profile=Win7SP0x64 hivelist -f memory.raw
Volatility Foundation Volatility Framework 2.3.1
Virtual            Physical           Name
------------------ ------------------ ----
0xfffff8a000062010 0x000000004c2d010 \REGISTRY\MACHINE\HARDWARE
0xfffff8a0000e1290 0x000000002f924290 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a000514420 0x00000000337a3420 \SystemRoot\System32\Config\SECURITY
0xfffff8a000537010 0x000000003434b010 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a0009c1420 0x0000000034459420 \SystemRoot\System32\Config\DEFAULT
0xfffff8a000c80010 0x0000000028e68010 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a000d12010 0x00000000280c5010 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a001882010 0x000000003bb9c010 \??\C:\Users\         \AppData\Local\Microsoft\Windows\UsrClass.dat
0xfffff8a0018b7010 0x000000000994a010 \??\C:\Users\         \ntuser.dat
0xfffff8a00320a010 0x0000000032aad010 \SystemRoot\System32\Config\SAM
0xfffff8a00800d420 0x00000000395b8420 \??\C:\System Volume Information\Syscache.hve
0xfffff8a00000d240 0x0000000002f82240 [no name]
0xfffff8a000024010 0x0000000004c6d010 \REGISTRY\MACHINE\SYSTEM
```



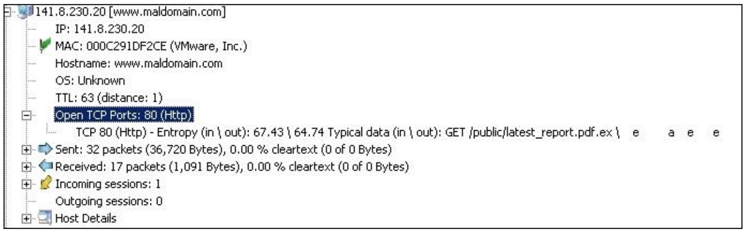
```
> vol.py --profile=Win7SP0x64 printkey -o 0xfffff8a0018b7010 -K "Software\Microsoft\Windows\CurrentVersion\Run" -f memory.raw
Volatility Foundation Volatility Framework 2.3.1
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: User Specified
Key name: Run (S)
Last updated: 2016-02-21 22:20:19 UTC+0000

Subkeys:

Values:
REG_SZ        epqe.exe        : (S) C:\Users\        \AppData\Roaming\Imyrug\epqe.exe
```



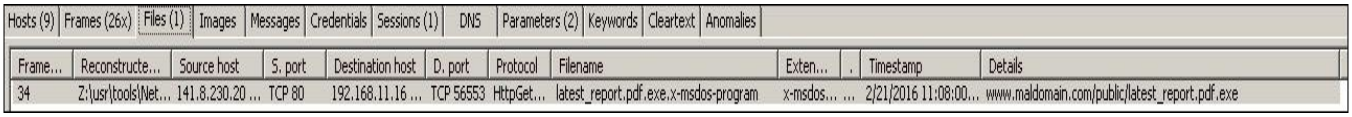
```
> vol.py --profile=Win7SP0x64 mftparser -f memory.raw --output=body --output-file=mft.body
Volatility Foundation Volatility Framework 2.3.1
Scanning for MFT entries and building directory, this can take a while
```



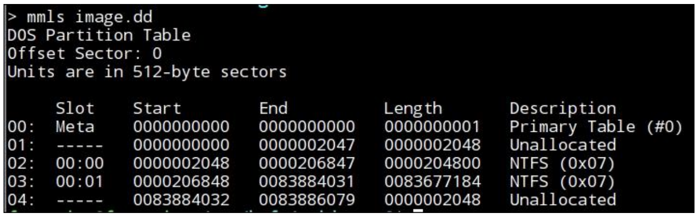
```
Sun Feb 21 2016 17:20:26     504 macb ---a-------I--- 0      0      46175     [MFT FILE_NAME] Windows\Prefetch\LATEST_REPORT.PDF.EXE-69E6ECF4.pf (Offset: 0x19a51c00)
                             456 macb ---a-------I--- 0      0      46175     [MFT FILE_NAME] Windows\Prefetch\LATEST_REPORT.PDF.EXE-69E6ECF4.pf (Offset: 0x82576a8)
                             504 macb ---a-------I--- 0      0      46175     [MFT FILE_NAME] Windows\Prefetch\LATEST~1.PF (Offset: 0x19a51c00)
                             456 macb ---a-------I--- 0      0      46175     [MFT FILE_NAME] Windows\Prefetch\LATEST~1.PF (Offset: 0x82576a8)
                             504 macb ---a-------I--- 0      0      46175     [MFT STD_INFO] Windows\Prefetch\LATEST~1.PF (Offset: 0x19a51c00)
                             456 macb ---a-------I--- 0      0      46175     [MFT STD_INFO] Windows\Prefetch\LATEST~1.PF (Offset: 0x82576a8)
Sun Feb 21 2016 17:20:28     480 macb ---a-------I--- 0      0      46182     [MFT FILE_NAME] Windows\Prefetch\EPQE.EXE-BCDAD835.pf (Offset: 0x5c89800)
                             432 macb ---a-------I--- 0      0      46182     [MFT FILE_NAME] Windows\Prefetch\EPQE.EXE-BCDAD835.pf (Offset: 0x9da798)
                             480 macb ---a-------I--- 0      0      46182     [MFT FILE_NAME] Windows\Prefetch\EPQEEX~1.PF (Offset: 0x5c89800)
                             432 macb ---a-------I--- 0      0      46182     [MFT FILE_NAME] Windows\Prefetch\EPQEEX~1.PF (Offset: 0x9da798)
                             480 macb ---a-------I--- 0      0      46182     [MFT STD_INFO] Windows\Prefetch\EPQEEX~1.PF (Offset: 0x5c89800)
                             432 macb ---a-------I--- 0      0      46182     [MFT STD_INFO] Windows\Prefetch\EPQEEX~1.PF (Offset: 0x9da798)
                             440 macb ---a-------I--- 0      0      46183     [MFT FILE_NAME] Windows\Prefetch\EXPLORER.EXE-254441E9.pf (Offset: 0x2e3dba68)
                             488 macb ---a-------I--- 0      0      46183     [MFT FILE_NAME] Windows\Prefetch\EXPLORER.EXE-254441E9.pf (Offset: 0x5c89c00)
                             440 macb ---a-------I--- 0      0      46183     [MFT FILE_NAME] Windows\Prefetch\EXPLOR~2.PF (Offset: 0x2e3dba68)
                             488 macb ---a-------I--- 0      0      46183     [MFT FILE_NAME] Windows\Prefetch\EXPLOR~2.PF (Offset: 0x5c89c00)
                             440 macb ---a-------I--- 0      0      46183     [MFT STD_INFO] Windows\Prefetch\EXPLOR~2.PF (Offset: 0x2e3dba68)
                             488 macb ---a-------I--- 0      0      46183     [MFT STD_INFO] Windows\Prefetch\EXPLOR~2.PF (Offset: 0x5c89c00)
```



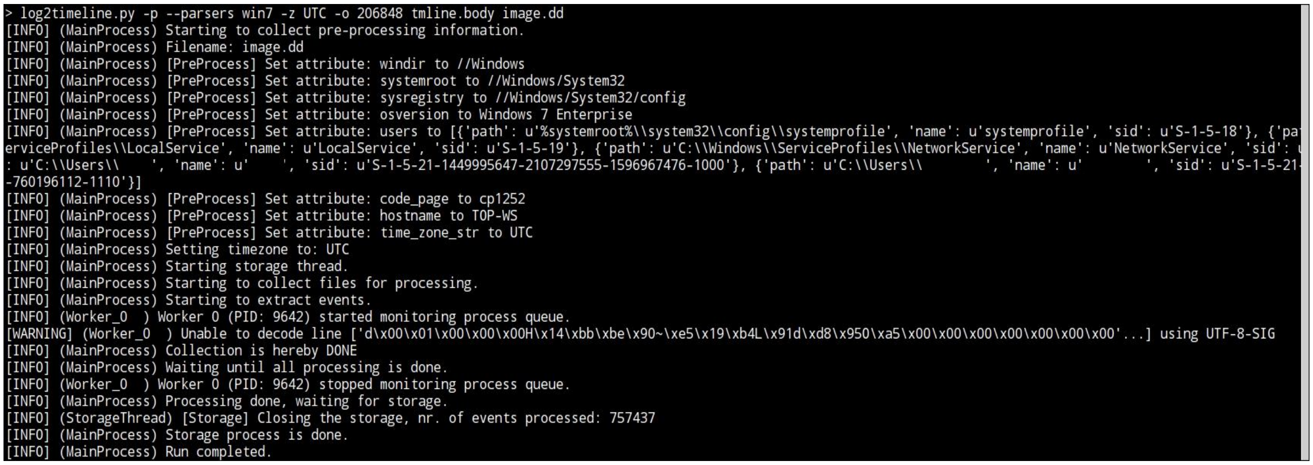
```
⊟ 141.8.230.20 [www.maldomain.com]
     IP: 141.8.230.20
     MAC: 000C291DF2CE (VMware, Inc.)
     Hostname: www.maldomain.com
     OS: Unknown
     TTL: 63 (distance: 1)
  ⊟  Open TCP Ports: 80 (Http)
        TCP 80 (Http) - Entropy (in \ out): 67.43 \ 64.74 Typical data (in \ out): GET /public/latest_report.pdf.ex \  e     a  e   e
  ⊞  Sent: 32 packets (36,720 Bytes), 0.00 % cleartext (0 of 0 Bytes)
  ⊞  Received: 17 packets (1,091 Bytes), 0.00 % cleartext (0 of 0 Bytes)
  ⊞  Incoming sessions: 1
     Outgoing sessions: 0
  ⊞  Host Details
```



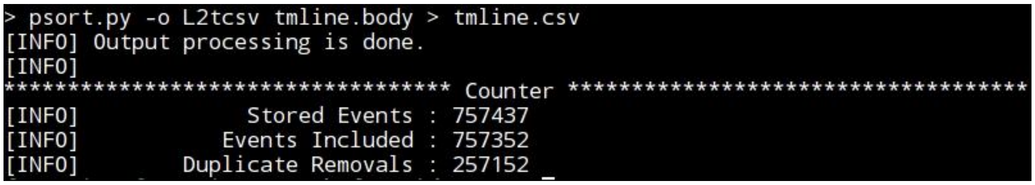
Frame...	Reconstructe...	Source host	S. port	Destination host	D. port	Protocol	Filename	Exten...	.	Timestamp	Details
34	Z:\usr\tools\Net...	141.8.230.20 ...	TCP 80	192.168.11.16 ...	TCP 56553	HttpGet...	latest_report.pdf.exe.x-msdos-program	x-msdos...	...	2/21/2016 11:08:00...	www.maldomain.com/public/latest_report.pdf.exe



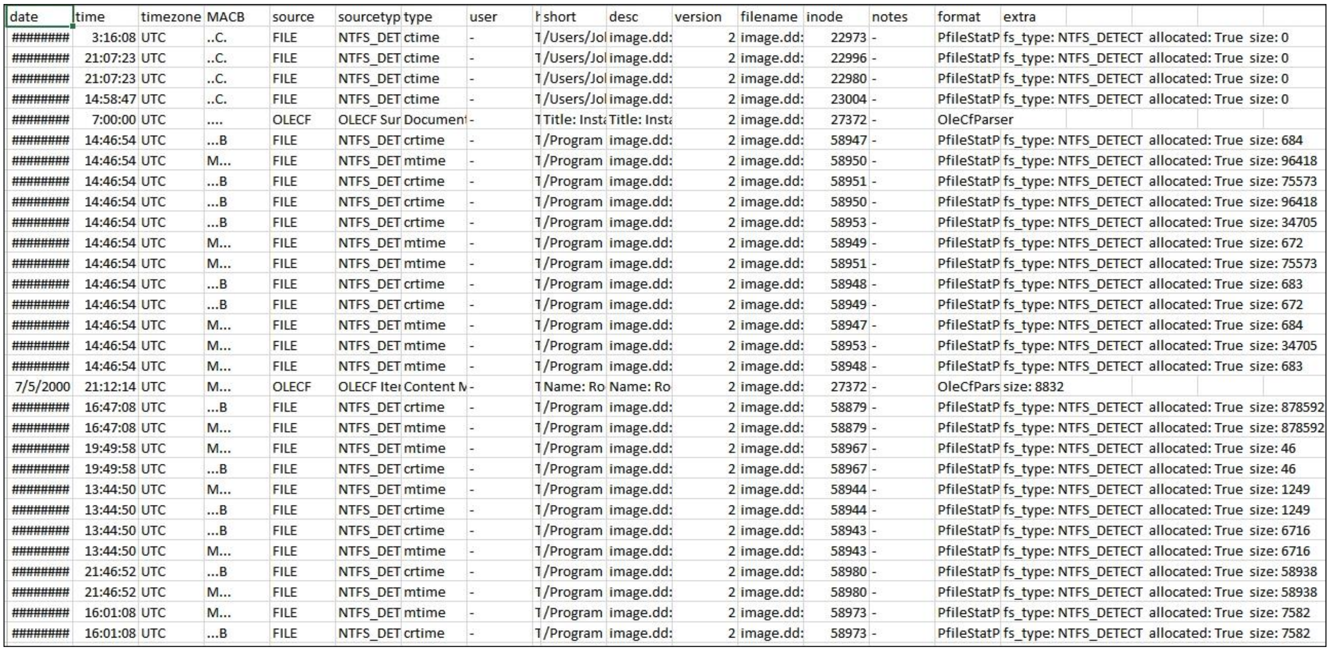
```
> mmls image.dd
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

     Slot      Start        End          Length       Description
00:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----     0000000000   0000002047   0000002048   Unallocated
02:  00:00     0000002048   0000206847   0000204800   NTFS (0x07)
03:  00:01     0000206848   0083884031   0083677184   NTFS (0x07)
04:  -----     0083884032   0083886079   0000002048   Unallocated
```



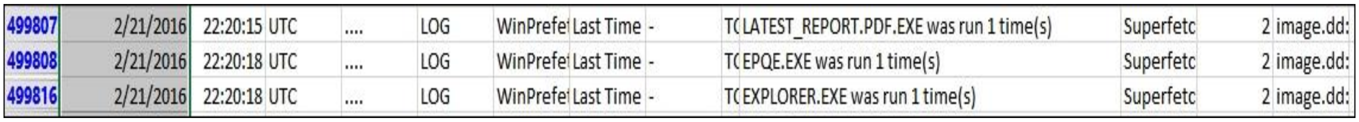
```
> log2timeline.py -p --parsers win7 -z UTC -o 206848 tmline.body image.dd
[INFO] (MainProcess) Starting to collect pre-processing information.
[INFO] (MainProcess) Filename: image.dd
[INFO] (MainProcess) [PreProcess] Set attribute: windir to //Windows
[INFO] (MainProcess) [PreProcess] Set attribute: systemroot to //Windows/System32
[INFO] (MainProcess) [PreProcess] Set attribute: sysregistry to //Windows/System32/config
[INFO] (MainProcess) [PreProcess] Set attribute: osversion to Windows 7 Enterprise
[INFO] (MainProcess) [PreProcess] Set attribute: users to [{'path': u'%systemroot%\\system32\\config\\systemprofile', 'name': u'systemprofile', 'sid': u'S-1-5-18'}, {'pa
erviceProfiles\\LocalService', 'name': u'LocalService', 'sid': u'S-1-5-19'}, {'path': u'C:\\Windows\\ServiceProfiles\\NetworkService', 'name': u'NetworkService', 'sid': u
: u'C:\\Users\\    ', 'name': u'    ', 'sid': u'S-1-5-21-1449995647-2107297555-1596967476-1000'}, {'path': u'C:\\Users\\        ', 'name': u'        ', 'sid': u'S-1-5-21-
-760196112-1110'}]
[INFO] (MainProcess) [PreProcess] Set attribute: code_page to cp1252
[INFO] (MainProcess) [PreProcess] Set attribute: hostname to TOP-WS
[INFO] (MainProcess) [PreProcess] Set attribute: time_zone_str to UTC
[INFO] (MainProcess) Setting timezone to: UTC
[INFO] (MainProcess) Starting storage thread.
[INFO] (MainProcess) Starting to collect files for processing.
[INFO] (MainProcess) Starting to extract events.
[INFO] (Worker_0  ) Worker 0 (PID: 9642) started monitoring process queue.
[WARNING] (Worker_0  ) Unable to decode line ['d\x00\x01\x00\x00\x00H\x14\xbb\xbe\x90~\xe5\x19\xb4L\x91d\xd8\x950\xa5\x00\x00\x00\x00\x00\x00\x00'...] using UTF-8-SIG
[INFO] (MainProcess) Collection is hereby DONE
[INFO] (MainProcess) Waiting until all processing is done.
[INFO] (Worker_0  ) Worker 0 (PID: 9642) stopped monitoring process queue.
[INFO] (MainProcess) Processing done, waiting for storage.
[INFO] (StorageThread) [Storage] Closing the storage, nr. of events processed: 757437
[INFO] (MainProcess) Storage process is done.
[INFO] (MainProcess) Run completed.
```



```
> psort.py -o L2tcsv tmline.body > tmline.csv
[INFO] Output processing is done.
[INFO]
********************************** Counter ***************************************
[INFO]             Stored Events : 757437
[INFO]           Events Included : 757352
[INFO]        Duplicate Removals : 257152 _
```



date	time	timezone	MACB	source	sourcetyp	type	user	h	short	desc	version	filename	inode	notes	format	extra
#########	3:16:08	UTC	..C.	FILE	NTFS_DET	ctime	-	T	/Users/Jo	image.dd:	2	image.dd:	22973	-	PfileStatP	fs_type: NTFS_DETECT allocated: True size: 0
#########	21:07:23	UTC	..C.	FILE	NTFS_DET	ctime	-	T	/Users/Jo	image.dd:	2	image.dd:	22996	-	PfileStatP	fs_type: NTFS_DETECT allocated: True size: 0
#########	21:07:23	UTC	..C.	FILE	NTFS_DET	ctime	-	T	/Users/Jo	image.dd:	2	image.dd:	22980	-	PfileStatP	fs_type: NTFS_DETECT allocated: True size: 0
#########	14:58:47	UTC	..C.	FILE	NTFS_DET	ctime	-	T	/Users/Jo	image.dd:	2	image.dd:	23004	-	PfileStatP	fs_type: NTFS_DETECT allocated: True size: 0
#########	7:00:00	UTC	....	OLECF	OLECF Sur	Document	-	T	Title: Insta	Title: Insta	2	image.dd:	27372	-	OleCfParser	
#########	14:46:54	UTC	...B	FILE	NTFS_DET	crtime	-	T	/Program	image.dd:	2	image.dd:	58947	-	PfileStatP	fs_type: NTFS_DETECT allocated: True size: 684
#########	14:46:54	UTC	M...	FILE	NTFS_DET	mtime	-	T	/Program	image.dd:	2	image.dd:	58950	-	PfileStatP	fs_type: NTFS_DETECT allocated: True size: 96418
#########	14:46:54	UTC	...B	FILE	NTFS_DET	crtime	-	T	/Program	image.dd:	2	image.dd:	58951	-	PfileStatP	fs_type: NTFS_DETECT allocated: True size: 75573
#########	14:46:54	UTC	...B	FILE	NTFS_DET	crtime	-	T	/Program	image.dd:	2	image.dd:	58950	-	PfileStatP	fs_type: NTFS_DETECT allocated: True size: 96418
#########	14:46:54	UTC	...B	FILE	NTFS_DET	crtime	-	T	/Program	image.dd:	2	image.dd:	58953	-	PfileStatP	fs_type: NTFS_DETECT allocated: True size: 34705
#########	14:46:54	UTC	M...	FILE	NTFS_DET	mtime	-	T	/Program	image.dd:	2	image.dd:	58949	-	PfileStatP	fs_type: NTFS_DETECT allocated: True size: 672
#########	14:46:54	UTC	M...	FILE	NTFS_DET	mtime	-	T	/Program	image.dd:	2	image.dd:	58951	-	PfileStatP	fs_type: NTFS_DETECT allocated: True size: 75573
#########	14:46:54	UTC	...B	FILE	NTFS_DET	crtime	-	T	/Program	image.dd:	2	image.dd:	58948	-	PfileStatP	fs_type: NTFS_DETECT allocated: True size: 683
#########	14:46:54	UTC	...B	FILE	NTFS_DET	crtime	-	T	/Program	image.dd:	2	image.dd:	58949	-	PfileStatP	fs_type: NTFS_DETECT allocated: True size: 672
#########	14:46:54	UTC	M...	FILE	NTFS_DET	mtime	-	T	/Program	image.dd:	2	image.dd:	58947	-	PfileStatP	fs_type: NTFS_DETECT allocated: True size: 684
#########	14:46:54	UTC	M...	FILE	NTFS_DET	mtime	-	T	/Program	image.dd:	2	image.dd:	58953	-	PfileStatP	fs_type: NTFS_DETECT allocated: True size: 34705
#########	14:46:54	UTC	M...	FILE	NTFS_DET	mtime	-	T	/Program	image.dd:	2	image.dd:	58948	-	PfileStatP	fs_type: NTFS_DETECT allocated: True size: 683
7/5/2000	21:12:14	UTC	M...	OLECF	OLECF Ite	Content N	-	T	Name: Ro	Name: Ro	2	image.dd:	27372	-	OleCfPars	size: 8832
#########	16:47:08	UTC	...B	FILE	NTFS_DET	crtime	-	T	/Program	image.dd:	2	image.dd:	58879	-	PfileStatP	fs_type: NTFS_DETECT allocated: True size: 878592
#########	16:47:08	UTC	M...	FILE	NTFS_DET	mtime	-	T	/Program	image.dd:	2	image.dd:	58879	-	PfileStatP	fs_type: NTFS_DETECT allocated: True size: 878592
#########	19:49:58	UTC	M...	FILE	NTFS_DET	mtime	-	T	/Program	image.dd:	2	image.dd:	58967	-	PfileStatP	fs_type: NTFS_DETECT allocated: True size: 46
#########	19:49:58	UTC	...B	FILE	NTFS_DET	crtime	-	T	/Program	image.dd:	2	image.dd:	58967	-	PfileStatP	fs_type: NTFS_DETECT allocated: True size: 46
#########	13:44:50	UTC	M...	FILE	NTFS_DET	mtime	-	T	/Program	image.dd:	2	image.dd:	58944	-	PfileStatP	fs_type: NTFS_DETECT allocated: True size: 1249
#########	13:44:50	UTC	...B	FILE	NTFS_DET	crtime	-	T	/Program	image.dd:	2	image.dd:	58944	-	PfileStatP	fs_type: NTFS_DETECT allocated: True size: 1249
#########	13:44:50	UTC	...B	FILE	NTFS_DET	crtime	-	T	/Program	image.dd:	2	image.dd:	58943	-	PfileStatP	fs_type: NTFS_DETECT allocated: True size: 6716
#########	13:44:50	UTC	M...	FILE	NTFS_DET	mtime	-	T	/Program	image.dd:	2	image.dd:	58943	-	PfileStatP	fs_type: NTFS_DETECT allocated: True size: 6716
#########	21:46:52	UTC	...B	FILE	NTFS_DET	crtime	-	T	/Program	image.dd:	2	image.dd:	58980	-	PfileStatP	fs_type: NTFS_DETECT allocated: True size: 58938
#########	21:46:52	UTC	M...	FILE	NTFS_DET	mtime	-	T	/Program	image.dd:	2	image.dd:	58980	-	PfileStatP	fs_type: NTFS_DETECT allocated: True size: 58938
#########	16:01:08	UTC	M...	FILE	NTFS_DET	mtime	-	T	/Program	image.dd:	2	image.dd:	58973	-	PfileStatP	fs_type: NTFS_DETECT allocated: True size: 7582
#########	16:01:08	UTC	...B	FILE	NTFS_DET	crtime	-	T	/Program	image.dd:	2	image.dd:	58973	-	PfileStatP	fs_type: NTFS_DETECT allocated: True size: 7582



499807	2/21/2016	22:20:15	UTC	....	LOG	WinPrefe	Last Time	-	TC	LATEST_REPORT.PDF.EXE was run 1 time(s)	Superfetc	2	image.dd:
499808	2/21/2016	22:20:18	UTC	....	LOG	WinPrefe	Last Time	-	TC	EPQE.EXE was run 1 time(s)	Superfetc	2	image.dd:
499816	2/21/2016	22:20:18	UTC	....	LOG	WinPrefe	Last Time	-	TC	EXPLORER.EXE was run 1 time(s)	Superfetc	2	image.dd: