CC Terminals, Inc.
Forensic Examination Report:
Examination of a USB Hard Drive

Examination Requestor
Mark Mawer
Security Administrator, CC Terminals, Inc.

Forensic Examiner
Brent C. Duckworth

Examination Date(s)
February 23, 2005 – April 7, 2005

Report Submission Date
April 15, 2005

GIAC Certified Forensic Analyst (GCFA)
Practical Version 2.0
SANS CDI East 2004

Executive Summary

Mark Mawer, security administrator for CC Terminals, Inc., presented a USB hard drive to me for analysis. He explained that the hard drive came from the cubicle of Mr. Robert Lawrence and might contain information supporting a harassment claim made against Mr. Lawrence by Ms. Leila Conlay, both CC Terminals sales representatives. Mr. Mawer requested that I examine the drive and its contents to determine if they support Ms. Conlay's concerns.

Using the computer forensics methodology described in this report, I examined the contents of the USB drive and found evidence that the subject Mr. Lawrence used a software program to intercept Ms. Conlay's electronic communication without Ms. Conlay's consent. By intercepting her communication, Mr. Lawrence was able to discover Ms. Conlay's whereabouts on the evening of October 28, 2004.

The USB hard drive contained three documents that describe encounters with an unnamed individual. The contents of these documents may have been sent to Ms. Conlay via e-mail. Further, I used forensic tools to recover three deleted files from the USB drive. The first file was the software program used by Mr. Lawrence to intercept Ms. Conlay's communications. The second file contained the intercepted communication, and the third file was an image depicting the location of Ms. Conlay's social engagement. The last document, written after Mr. Lawrence's final rejection, alludes to possible bodily harm to Ms. Conlay.

The examination indicates that the following CC Terminals, Inc. policies are implicated:

- CC Terminals User Rules of Behavior, which states that use of information systems equipment owned or operated by the company by an employee, for other than official CC Terminals business or authorized purposes, is prohibited. Mr. Lawrence violated this policy by using a CC Terminals information system for personal business. The penalties for violating this policy are disciplinary action up to and including termination.
- CC Terminals Appropriate Use policy states that the use of restricted software by an unauthorized user is prohibited. Restricted software includes, but is not limited to, network "sniffers", network scanning software, and vulnerability assessment tools. Mr. Lawrence violated this policy by installing and executing restricted software on a CC Terminals information system. The penalties for violating this policy are disciplinary action up to and including termination.

Further, the following U.S. federal statutes may be implicated:

- 18 U.S. Code. Sec. 2511(1)(a), which prohibits the interception and disclosure of wire, oral, or electronic communications, unless an exemption applies, and carries a penalty of a fine or up to five years in prison, or both, if convicted. Mr. Lawrence intercepted Ms. Conlay's communications in real-time, without her consent, and none of the exemptions apply which would support his actions.

- 18 U.S. Code. Sec. 875(c), which prohibits using interstate or foreign commerce to transmit any communication containing any threat to injure another person, and carries a penalty of a fine or up to five years in prison, or both, if convicted. If determined that Mr. Lawrence did send Ms. Conlay the contents of the recovered documents, he would be in violation of this statute.

Mr. Mawer, CC Terminals Security Administrator, is retaining the evidence involved in this incident, which includes a copy of this report, the physical USB hard drive and the products of the forensics examination.

Case Overview

Mr. Robert Lawrence and Ms. Leila Conlay both work as sales representatives for CC Terminals, Inc., a credit card processing firm. Mr. Mark Mawer, the security administrator for CC Terminals, contacted me regarding a complaint filed by Ms. Conlay. She reported that Mr. Lawrence had made numerous attempts to meet her both inside and outside of work and had sent e-mail to her personal e-mail address, becoming increasingly aggressive at her rejections. Then, while on a personal evening engagement with a friend on October 28th, Mr. Lawrence arrived at the same location; Ms. Conlay contacted Mr. Mawer the next day.

Mr. Mawer searched Mr. Lawrence's work area and found a USB hard drive. He imaged the hard drive and provided the image to me along with the following chain of custody information:

- **Tag #:** USBFD-64531026-RL-001
- **Description:** 64M Lexar Media JumpDrive
- **Serial #:** JDSP064-04-5000C
- **Image:** USBFD-64531026-RL-001.img
- **MD5:** 338ecf17b7fc85bbb2d5ae2bbc729dd5

Mr. Mawer requested that I perform a computer forensic examination of the hard drive to determine if the contents supported Ms. Conlay's complaint.

This report is my response to Mark Mawer, Security Administrator for CC Terminals, Inc., who requested the forensic examination. The report describes the methods I used to conduct the examination and my findings.

Methodology

My methodology for performing this computer forensic examination consisted of four phases. During each phase, I collect data that serve as the foundation for the subsequent phases. My process includes:

- **Evidence Collection** – I collect, photograph, and make forensic copies of the physical evidence while ensuring that I protect evidence integrity. I also perform procedures on the forensic copies of the evidence to prepare them for analysis. I collect detailed information on the contents of the forensics copy and the file system(s) it contains.
- **Timeline Creation and Analysis** – By constructing a timeline, I create another view of file system activity that details what occurred on the system. A timeline is a chronology of file timestamps indicating what

happened on the system and when, which I use to identify activity of interest.

- **Media Analysis** – The Media analysis phase contains the majority of my work in this examination. I analyze the forensics copies created during evidence collection. In this phase, I also identify words and phrases of interest for further investigation. I recover any deleted files on the file system of the forensic copy and attempt to determine their type. I then analyze the files I recover and ascertain if they had any role in the incident.
- **Reporting** – My final task is to report my findings and determine any policy or potential legal implications. My goal is to effectively communicate this information and provide recommendations for possible follow-up actions.

In each of the following sections, I describe my work in each of the aforementioned phases to arrive at a conclusion and discuss any CC Terminals policies or laws that are implicated.

Evidence Collection

Forensic Analysis Workstation

To perform my examination, I used a forensics analysis workstation, a computer specifically configured and outfitted with forensic software. I used tools provided on the Helix 1.5 (2004-12-07) bootable CD-ROM distribution to collect and examine the digital evidence. A bootable CDROM (or live CD) distribution enables a workstation to run an operating environment utilizing only the system memory. Helix is a specialized Linux distribution that contains a complete set of forensic analysis and examination tools. e-fense, Inc. developed the Helix distribution and makes it available for download on its website: http://www.e-fense.com/helix.

From the Helix website:

> **"Helix is a customized distribution of the Knoppix Live Linux CD. Helix has more than just a bootable live CD. You can still boot into a customized Linux environment that includes customized linux kernels (2.4.27 & 2.6.7), excellent hardware detection and many applications dedicated to Incident Response and Forensics. Helix has been modified very carefully to NOT touch the host computer in any way and it is forensically sound. Helix wil not auto mount swap space, it will also not auto mount any found devices. Helix also has a special Windows autorun side for Incident Response and Forensics. Helix is used by SANS for training in Track 8: System Forensics, Investigation and Response."[1]**

[1] e-fense, Inc. "Helix Incident Response & Computer Forensics." URL: http://www.e-fense.com/helix/index2.html. (11 Mar 2005)

For the hardware platform, I used a Sony VAIO laptop with the following specifications:

- Intel Pentium® III CPU 596MHz processor
- 128MB of Memory

I installed Windows XP on the laptop and attached a 80GB ACOM Data USB 2.0 hard drive on which I stored the files pertinent to the examination.

Uncompressing the USB Hard Drive Image

After Mr. Mawer gave me a copy of the USB hard drive contents, I copied it onto my workstation. I ran the `file` command on the image file. The `file` command reads a file and attempts to determine its type by comparing the file header with headers of known file types. The output of the `file` command indicated that the file was compressed with `gzip` and that the original file name of the compressed file was *USBFD-64531026-RL-001.img*.

```
$ file GCFAPractical2.0-USBImageAndInfo.zip.gz

GCFAPractical2.0-USBImageAndInfo.zip.gz: gzip compressed data, was
"USBFD-64531026-RL-001.img", from Unix, max compression
```

Mr. Mawer had used the `gzip` program, a file compression program, to make the file smaller and reduce the time it takes to transmit electronically. I needed to uncompress the file to retrieve the original. The file compression is reversible and does not alter the file contents.

To inflate the file, I used the `gunzip` command on *GCFAPractical2.0-USBImageAndInfo.zip.gz.* The `gunzip` command performs the opposite of the `gzip` command and inflates the compressed file. I used the `--name` option so that `gunzip` would restore the original filename.

```
$ gunzip --name GCFAPractical2.0-USBImageAndInfo.zip.gz
```

After running `gunzip`, the resulting file was named *USBFD-64531026-RL-001.img*. I then ran the `file` command on *USBFD-64531026-RL-001.img*, and the output of that command told me that the file started with an x86 boot sector, indicative of a disk image. A boot sector is the first sector on a disk that tells the CPU to process the partition table on the disk and locate the executable code to start the operating system.[2]

```
$ file USBFD-64531026-RL-001.img
```

```
USBFD-64531026-RL-001.img: x86 boot sector
```

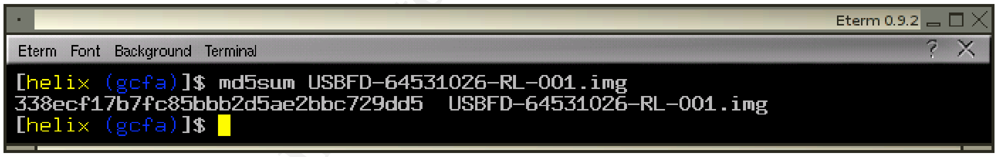
Forensic Image Creation

A forensic image, or copy, of digital evidence is an exact duplicate of the original evidence. Since I did not have access to the physical USB hard drive in this examination, I handled the forensic copy Mr. Mawer provided to me as if it were the original evidence. Therefore, to start my examination, I duplicated the image and verified that the copy I created was identical to the original. I then used the forensic copy I created to perform my examination, which ensured I did not modify the original.

The chain of custody form contained an important detail that assisted in verifying the integrity of the image, the MD5 hash. An MD5 hash is a 128-bit (32-character) "fingerprint" of the input file. According to Ronald Rivest, "it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given prespecified target [hash]."[3] This digital hash, or fingerprint, is so sensitive that if a single character changes in a file, it will produce an entirely different fingerprint. I can use this hash fingerprint to show the data integrity during and after an examination.

I used a tool called `md5sum` to generate the MD5 hash for a file. When I ran the `md5sum` command on the *`USBFD-64531026-RL-001.img`* file Mr. Mawer provided me, the tool generated the same MD5 hash in the chain of custody information (Figure 1), indicating that the file had not been altered.

Figure 1



```
[helix (gcfa)]$ md5sum USBFD-64531026-RL-001.img
338ecf17b7fc85bbb2d5ae2bbc729dd5  USBFD-64531026-RL-001.img
[helix (gcfa)]$
```

With the integrity of the image file verified, I copied the file to read-only media, a CD-ROM. To create my forensic copy of the evidence, I used the `dcfldd` tool, which is an enhanced version of `dd`. This tool reads the first byte of a file, writes that byte to a new file, and then repeats the process until it reaches the end of the file. This operation produces an exact copy of the original.

```
$ dcfldd if=/mnt/cdrom/USBFD-64531026RL-001.img of=/images/gcfa/USBFD-
64531026-RL-001.img bs=512 hashwindow=0
```

[2] Carrier, Brian. File System Forensic Analysis. Crawfordsville: Addison Wesley, 2005. Pg. 28
[3] Rivest, Ronald. "Executive Summary." The MD5 Message-Digest Algorithm. April 1992. URL: http://www.ietf.org/rfc/rfc1321.txt?number=1321. (15 Apr 1992)

I ran md5sum again to ensure the image was not modified during the operation, and the new file produced the same fingerprint as the original. This result verified that I had an identical copy of the original that I could use for the rest of my examination.

My forensic copy contained a raw hard disk image, identical to the physical hard drive. Typically, files are stored on a hard disk using a file system. The file system is an organizational structure that facilitates data location and storage by the operating system.

Hard drives, at their lowest level, store data as groups of one's and zero's. Each one or zero is called a bit, and eight bits are collectively called a byte. The smallest addressable location on a disk is 512 bytes in size and is called a sector. To manage and group data on a disk, the disk can be divided up into one or more logical volumes called partitions. The size and order of these partitions is stored in a partition table, which is part of the first sector of the disk.[4] The file system structure is then overlaid on the partition. To examine the files stored on the forensic copy, I needed to identify, locate, and extract any partitions.

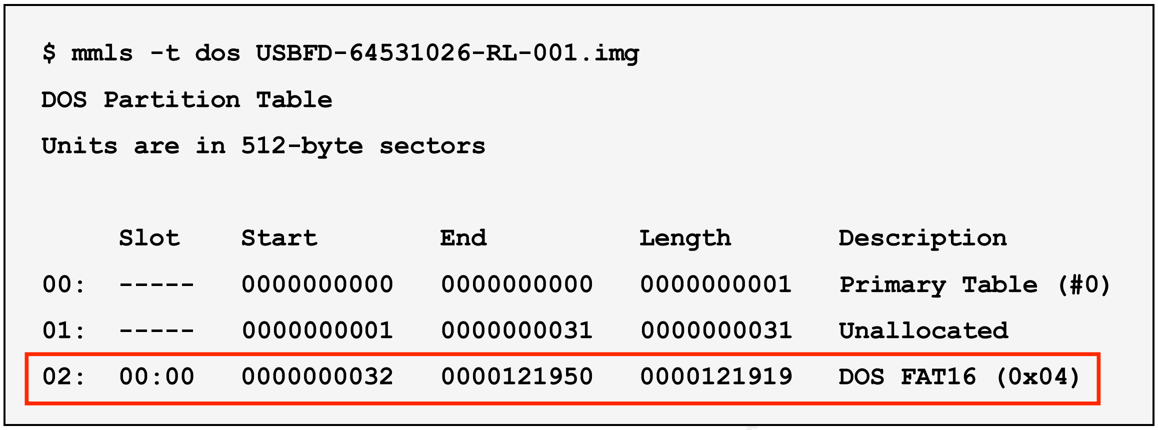
I ran fdisk on the image to view the partition table. The -l option tells fdisk to only list the partition table rather than start an interactive session, which might modify the partitions. The output from the command indicates that the image contains a single FAT16 partition.

```
$ fdisk -l USBFD-64531026-RL-001.img


Disk USBFD-64531026-RL-001.img: 62 MB, 62439424 bytes
17 heads, 32 sectors/track, 224 cylinders
Units = cylinders of 544 * 512 = 278528 bytes


                    Device Boot      Start         End      Blocks
Id  System
USBFD-64531026-RL-001.img1   *           1         225       60959+
4   FAT16 <32M
```

I then ran mmls on the image to determine the starting and ending sectors for the FAT16 partition. The mmls tool is part of The Sleuth Kit, an open-source forensic toolkit developed by Brian Carrier. mmls shows the layout of the partitions[5], which I can use to extract the partition to a new file. The -t option to the mmls command specifies that the image contains a DOS-based (FAT16) partition.

[4] "Unix man pages: fdisk." Linux Programmer's Manual. 11 Jun 1998. URL: http://www.rt.com/man/fdisk.8.html. (2 Apr 2005)
[5] Carrier, Brian. "Tool Details." The Sleuth Kit. 2005. URL: http://www.sleuthkit.org/sleuthkit/tools.php. (2 Apr 2005)

The Sleuth Kit contains a variety of forensic tools for examining and analyzing disk layout in a non-invasive way.[6] Many of the tools I use in the examination are tools from that toolkit.

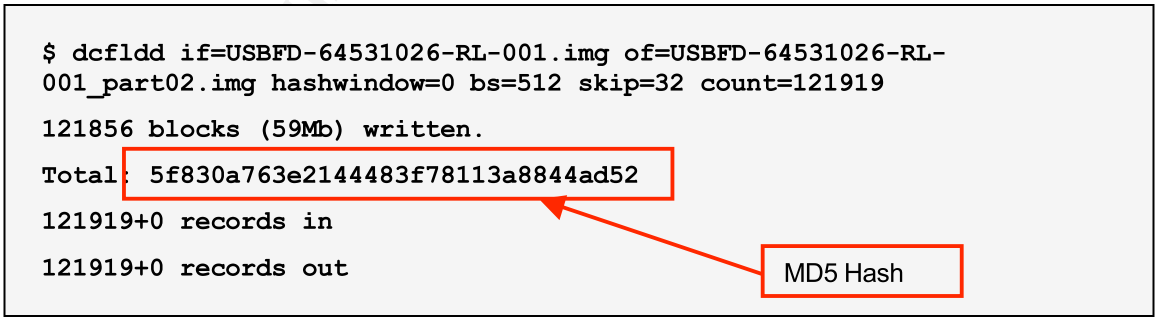


```
$ mmls -t dos USBFD-64531026-RL-001.img
DOS Partition Table
Units are in 512-byte sectors

     Slot    Start        End          Length       Description
00:  -----   0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----   0000000001   0000000031   0000000031   Unallocated
02:  00:00   0000000032   0000121950   0000121919   DOS FAT16 (0x04)
```

The mmls command validated that the partition was FAT16. Further, the mmls output indicated that the first sector of the FAT16 partition was 32, while the last sector was 121950, with an overall partition length of 121919 sectors.

Now that I had the starting sector and the length, I could use dcfldd to create an image file of just the partition. I used the output of the mmls command to determine the options I gave the dcfldd command.

The of=*USBFD-64531026-RL-001_part02.img* option specifies the output file; the skip=32 option tells dcfldd to skip to the 32nd sector from the start of the image; the count=121919 option specifies the number of sectors to include before stopping; the bs=512 option specifies that I want to copy data in blocks 512-byte in size; the hashwindow=0 specifies that I want dcfldd to calculate the MD5 hash fingerprint for the file once it is done copying data. The tool then creates an image file containing only the FAT16 partition.



```
$ dcfldd if=USBFD-64531026-RL-001.img of=USBFD-64531026-RL-
001_part02.img hashwindow=0 bs=512 skip=32 count=121919
121856 blocks (59Mb) written.
Total: 5f830a763e2144483f78113a8844ad52
121919+0 records in
121919+0 records out
```

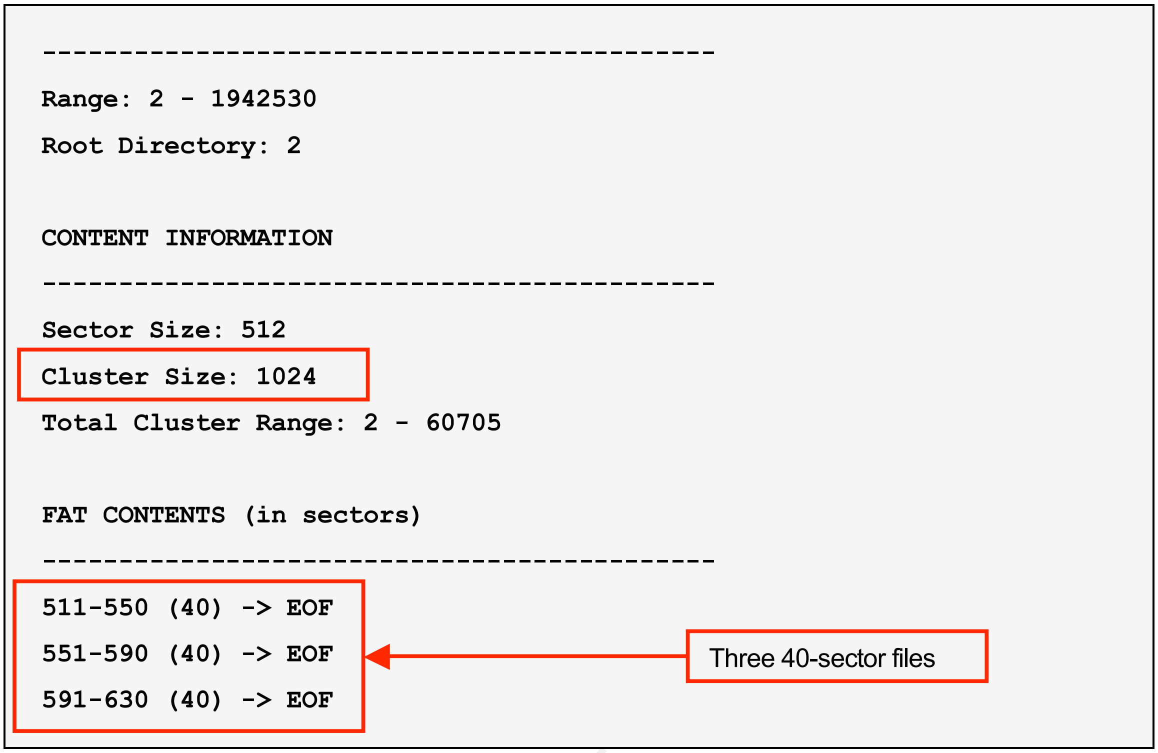
I ran the file command on the resulting image. The file command confirmed the image as a FAT16 partition 121919 sectors in length.

[6] Carrier, Brian. “Description.” The Sleuth Kit. 2005. URL: http://www.sleuthkit.org/sleuthkit/desc.php. (2 Apr 2005)

```
$ file USBFD-64531026-RL-001_part02.img

USBFD-64531026-RL-001_part02.img: x86 boot sector, code offset 0x3c,
OEM-ID "MSWIN4.1", sectors/cluster 2, root entries 512, Media
descriptor 0xf8, sectors/FAT 239, heads 17, hidden sectors 32, sectors
121919 (volumes > 32 MB) , serial number 0x0, unlabeled, FAT (16 bit)
```

The `fsstat` tool is part of The Sleuth Kit and displays "file system details and statistics including layout, sizes, and labels."[7] I ran the `fsstat` command on the FAT 16 file system image. The `fsstat` command provided important information about the image including the cluster size, total cluster range, and the contents of the File Allocation Table.

```
$ fsstat -f fat16 USBFD-64531026-RL-001_part02.img


FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: FAT


OEM Name: MSWIN4.1
Volume ID: 0x0
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory):
File System Type Label: FAT16


Sectors before file system: 32


File System Layout (in sectors)
Total Range: 0 - 121918
* Reserved: 0 - 0
** Boot Sector: 0
* FAT 0: 1 - 239
* FAT 1: 240 - 478
* Data Area: 479 - 121918
** Root Directory: 479 - 510
** Cluster Area: 511 - 121918


METADATA INFORMATION
```



```
-------------------------------------------

Range: 2 - 1942530

Root Directory: 2


CONTENT INFORMATION

-------------------------------------------

Sector Size: 512

Cluster Size: 1024

Total Cluster Range: 2 - 60705


FAT CONTENTS (in sectors)

-------------------------------------------

511-550 (40) -> EOF

551-590 (40) -> EOF

591-630 (40) -> EOF
```

The output of the `fsstat` tool provides a few key pieces of information about the FAT16 file system: the cluster size is 1024 bytes and three files exist in the File Allocation Table (FAT) that are each 40 sectors in length.

Timeline Creation and Analysis

The file system on a disk drive is analogous to a card catalog in a library; each card in the catalog points to a book located on the shelves. By using the card catalog, a librarian can quickly determine the exact location of a book. Similarly, a file system maintains pointers to data stored on the physical disk. These pointers in the FAT16 file system are called directory entries, and the areas on the disk to which they point are called clusters. The File Allocation Table (FAT) keeps track of what clusters are allocated and what clusters belong to which file. Directory entries contain file details such as filename, size, starting cluster, and timestamps.[8] These timestamps are the basis for creating a timeline.

When I create a timeline, I use tools to query the file system directory entries about their contents. Specifically, I am interested in the three times associated with each entry: the last time the file was modified, the time the file was last accessed, and the time the directory entry for that file was updated (changed). These times are called MAC times, which is short for Modified, Accessed, Changed times. My tools collect these timestamps and the file names then organize the files in chronological order.

[7] Carrier, Brian. "Tool Details." The Sleuth Kit. 2005. URL: http://www.sleuthkit.org/sleuthkit/tools.php. (2 Apr 2005)
[8] Carrier, Brian. File System Forensic Analysis. Crawfordsville: Addison Wesley, 2005. Pg. 212

To collect these timestamps and their corresponding files, I query two types of data: the allocated clusters and the unallocated clusters. When files are deleted, their content is not actually erased. The clusters they occupy are simply marked as unallocated, and the last changed timestamp is updated.[9]

To query the allocated clusters, I used the `fls` tool, also part of The Sleuth Kit. This tool recursively reads all directory entries, starting with the topmost entry, and (with the `-m` option) reports their timestamp information.

```
$ fls -f fat16 -m / -r USBFD-64531026-RL-001_part02.img > USBFD-
64531026-RL-001_part02.fls
```

The `-f` option specifies the file system type; the `-m` option tells `fls` to output `mactime` format; the `/` specifies the starting directory; the `-r` option specifies directory recursion. I direct the output of this command to *USBFD-64531026-RL-001_part02.fls*.

To query the unallocated clusters, I used the `ils` tool, also part of The Sleuth Kit.

```
$ ils -f fat16 -r -m USBFD-64531026-RL-001_part02.img > USBFD-
64531026-RL-001_part02.ils
```

The `-r` option tells `ils` to only list removed files; the `-m` option tells `ils` to output `mactime` format.

With the output from both tools, I concatenated the files using the `cat` utility and redirected the output to a new file named *USBFD-64531026-RL-001_part02.mac*.

```
$ cat USBFD-64531026-RL-001_part02.?ls > USBFD-64531026-RL-
001_part02.mac
```

The `mactime` tool is a script that uses the output of the `ils` and `fls` tools to create an ASCII timeline of system activity.[10]

```
$ mactime -b USBFD-64531026-RL-001_part02.mac -d > USBFD-64531026-RL-
001_part02.timeline
```

[9] Carrier, Brian. “File Activity Timelines.” The Sleuth Kit. June 2003. URL: http://www.sleuthkit.org/sleuthkit/docs/ref_timeline.html. (19 Jun 2003)

[10] Carrier, Brian. “mactime.” The Sleuth Kit. URL: http://www.sleuthkit.org/sleuthkit/man/mactime.html. (13 Mar 2005)

The `-b` option identifies the body file (the `.mac` file), and the `-d` option specifies to create comma-separated output, which simplifies importing the data into a spreadsheet for analysis.

A summary of my timeline creation results is listed in Table 1. The entire timeline is located in Appendix A. Table 1 has eight columns. The first column indicates whether the file was deleted; the second column contains the timestamp; the third column contains the directory entry for the file; the fourth column contains the filename; the fifth column contains the file size; columns 6 through 8 indicate to which timestamp attribute the timestamp in column 2 refers.

Table1

Del	Time	Directory Entry	Filename	Size	M	A	C
	10/25/04 0:00	3	her.doc	19968		X	
	10/25/04 8:32	3	her.doc	19968			X
	10/25/04 8:32	3	her.doc	19968	X		
	10/26/04 0:00	4	hey.doc	19968		X	
	10/26/04 8:48	4	hey.doc	19968			X
	10/26/04 8:48	4	hey.doc	19968	X		
X	10/27/04 16:23	10	WinPcap_3_1_beta_3.exe	485810	X		
X	10/27/04 16:23	10	WinPcap_3_1_beta_3.exe	485810			X
X	10/27/04 16:24	14	WinDump.exe	450560	X		
X	10/27/04 16:24	14	WinDump.exe	450560			X
X	10/28/04 0:00	10	WinPcap_3_1_beta_3.exe	485810		X	
X	10/28/04 0:00	14	WinDump.exe	450560		X	
X	10/28/04 0:00	15	_apture	53056		X	
X	10/28/04 0:00	17	_ap.gif	8814		X	
	10/28/04 0:00	18	coffee.doc	19968		X	
X	10/28/04 11:08	15	_apture	53056			X
X	10/28/04 11:11	15	_apture	53056	X		
X	10/28/04 11:17	17	_ap.gif	8814		X	
X	10/28/04 11:17	17	_ap.gif	8814	X		
	10/28/04 19:24	18	coffee.doc	19968			X
	10/28/04 19:24	18	coffee.doc	19968	X		

My timeline showed that the USB drive stored three files that had not been deleted: `her.doc`, `hey.doc`, and `coffee.doc`. The timeline also shows four files were created and deleted between October 26th, when `hey.doc` was created, and October 28th, when *coffee.doc* was last modified: *WinPcap_3_1_beta_3.exe*, *WinDump.exe*, *_apture*, and *_ap.gif*. Also, the last accessed time for every file was midnight the day it was last modified. This may indicate that the last accessed timestamps were modified. The FAT16 file system does not store file ownership information, so I was unable to determine any user or group information regarding these files.

In summary, the File Allocation Table only showed three allocated files on the partition:

- *her.doc* Last modified on Mon, Oct 25, 2004 at 08:32.08
- *hey.doc* Last modified on Tue, Oct 26, 2004 at 08:48:10
- *coffee.doc* Last modified on Thu, Oct 28, 2004 at 19:24:48

The timeline shows additional files that were deleted and residing in unallocated clusters:

- *WinDump.exe* Deleted on Wed, Oct 27, 2004 at 16:24:02
- *WinPcap_3_1_beta_3.exe* Deleted on Wed, Oct 27, 2004 at 16:23:56
- *_apture* Deleted on Wed, Oct 27, 2004 at 11:11:00
- *_ap.gif* Deleted on Wed, Oct 27, 2004 at 11:17:46

Media Analysis and File Recovery

During media analysis, I examine the forensic images and their contents. I mount those images in read-only mode, allowing me to browse the file system without affecting the evidence integrity. When I mount a file system, I essentially graft the file system to a specific directory on my workstation that I can then access as if it were part of my file system.

```
# mount -t vfat -o ro,noatime,loop,uid=helix,gid=helix
/images/gcfa/USBFD-64531026-RL-001_part02.img /fat16
```

The timeline indicated that three files existed on the USB drive that had not been deleted. I started my examination by examining those files. I created MD5 hashes of each file, and then I used the `file` command to help me classify each file's type. I opened each file in Microsoft Word, the word processing program that is part of the Microsoft Office Suite of software, to view its contents.

```
Filename: her.doc

MD5 Hash: 9785a777c5286738f9deb73d8bc57978

File Type: Microsoft Office Document
File Contents:

Hey I saw you the other day.  I tried to say "hi", but you
disappeared???  That was a nice blue dress you were wearing.  I heard
that your car was giving you some trouble.  Maybe I can give you a
ride to work sometime, or maybe we can get dinner sometime?


Have a nice day
```

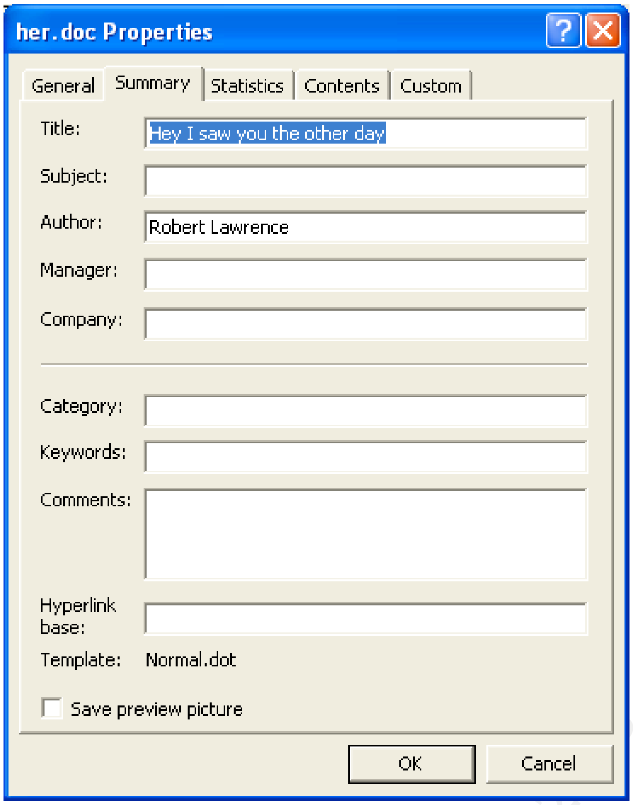
```
Filename: hey.doc

MD5 Hash: ca601d4f8138717dca4de07a8ec19ed1

File Type: Microsoft Office Document

File Contents:

Hey!  Why are you being so mean?  I was just offering to help you out
with your car!  Don't tell me to get lost!  You should give me a
chance.  I'm a nice guy just trying to help you out, just because I
think you're cute doesn't mean I'm weird.  Perhaps coffee would be
better, when would be a good time for you?
```

```
Filename: coffee.doc

MD5 Hash: a833c58689596eda15a27c931e0c76d1

File Contents:

Hey what gives?  I was drinking a coffee on thursday and saw you stop
buy with some guy!  You said you didn't want coffee with me, but
you'll go have it with some random guy???  He looked like a loser!
Guys like that are nothing but trouble.  I can't believe you did this
to me!  You should stick to your word, if you're not interested in
going to coffee with me then you shouldn't be going with anyone!  I
heard rumors about a "bad batch" of coffee, hope you don't get any...
```

The files describe encounters with an unnamed individual. However, `coffee.doc` mentions a meeting involving coffee, and Ms. Conlay stated that she had an encounter with Mr. Lawrence on the evening of October 28th at a coffee house. Still, the files could have been written by anyone. `coffee.doc` is particularly interesting because of its content. The document tone is hostile, and the document suggests a threat of bodily harm.

I viewed the properties for each file and though all the titles were different, they all showed the same Author: Robert Lawrence (see Figure 2).

Figure 2



Title: Hey I saw you the other day

Author: Robert Lawrence

Template: Normal.dot

□ Save preview picture

While the document properties showed Mr. Lawrence as the author of the three documents, that fact alone was not conclusive proof that he wrote the document. However, the fact that he also interacted with Ms. Conlay on the night of October 28th at a coffee house was too much of a coincidence for him not to be the author. So, I had two documents by Mr. Lawrence that indicated interest in Ms. Conlay and one that seemed to indicate he knew the whereabouts of Ms. Conlay that evening. Unfortunately, I still do not know how Mr. Lawrence knew the location of her engagement. I needed to look at the deleted files to see if they were of interest to the examination.

File Recovery

From my timeline, I knew that four deleted files exist on the image of the USB hard drive. I needed to recover the files to examine them. These files were named *WinPcap_3_1_beta_3.exe*, *WinDump.exe*, *_apture*, and *_ap.gif*. I used the `fls` tool to list the directory entries on the image and verify the directory entry that corresponded to each deleted file.

```
$ fls -f fat16 USBFD-64531026-RL-001_part02.img
r/r 3:   her.doc
r/r 4:   hey.doc
```

```
r/r * 7:        WinPcap_3_1_beta_3.exe (_INPCA~1.EXE)
r/r * 10:       WinPcap_3_1_beta_3.exe (_INPCA~1.EXE)
r/r * 12:       WinDump.exe (_INDUMP.EXE)
r/r * 14:       WinDump.exe (_INDUMP.EXE)
r/r * 15:       _apture
r/r * 16:       _ap.gif
r/r * 17:       _ap.gif
r/r 18: coffee.doc
```

The output of the `fls` command shows a list of the directory entry contents for the entire USB image. Each line indicates the directory entry number, the Long File Name (longer than eight characters), and the 8.3 file name (an eight-character filename, a period, and a three-character extension). The entries with an asterisk indicate a deleted file. The first letter of the 8.3 file name is missing because it is used to set the unallocated status of the directory entry.[11]

Remember, the FAT16 file system structure has three main components: directory entries, clusters, and the FAT itself. The `istat` program reads a directory entry and displays details and statistics about that entry, including any allocated data units.[12] The output of the `istat` command contains: the directory entry number, whether the directory entry is allocated, the file attributes associated with the file, the size of the file, the filename, the three timestamps, and any allocated disk sectors.

The output of the `istat` commands is located in Appendix A. However, I have summarized the sector information for each directory entry in Table 2.

Table 2

Directory Entry	Filename	First Sector	Last Sector	File Size
3	her.doc	511	550	19968
4	hey.doc	551	590	19968
7	_INPCA~1.EXE	-	-	0
10	_INPCA~1.EXE	591	630	485810
12	_INDUMP.EXE	-	-	0
14	_INDUMP.EXE	1541	2420	450560
15	_apture	2421	2524	53056
16	_ap.gif	-	-	0
17	_ap.gif	2525	2542	8814
18	coffee.doc	591	630	19968

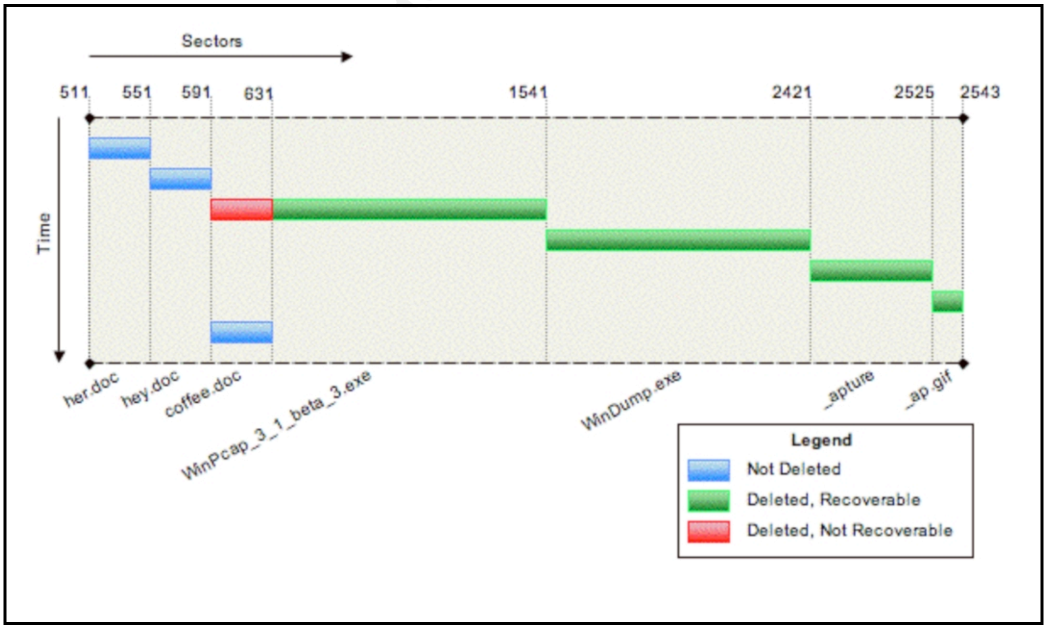
[11] Carrier, Brian. File System Forensic Analysis. Crawfordsville: Addison Wesley, 2005. Pg. 271
[12] Carrier, Brian. “istat.” The Sleuth Kit. URL: http://www.sleuthkit.org/sleuthkit/man/istat.html. (13 Mar 2005)

Directory entries 7, 12, and 16 did not contain any sector information. This could mean that, while the directory entry remained, the sectors were reallocated to another file. The sector numbers for each consecutive directory entry increased except for coffee.doc. coffee.doc has the same first and last sector as directory entry 10 because it was created after the directory entries in red (entries 7-17) were marked as "not allocated". The file system used the next available sector to write coffee.doc: 591.

So, why does directory entry 10 (_INPCA~1.EXE) also say that it occupies sectors 591 – 630 when the file is over 24 times the size of coffee.doc? Essentially, the directory entry only identifies the first cluster of the file. You identify the remaining clusters by using the FAT structure. A group of clusters that store a file on a FAT16 file system is called a cluster chain. Each link in the chain contains the location of the next link until the end of file (EOF) is reached.[13] Both _INPCA~1.EXE and coffee.doc point to FAT entry 591, but coffee.doc has overwritten the cluster chain which started at that entry. As a result, _INPCA~1.EXE now points to the cluster chain for coffee.doc, so querying either directory entry will report the same sectors.

While some files that have been deleted are recoverable, files that have had their data either completely or partially overwritten are not wholly recoverable. Figure 3 illustrates this point by depicting all seven files and their locations by sector on the disk. The blue areas are files that have not been deleted. The green areas are files or parts of files that were deleted but are recoverable. The red area was deleted but is not recoverable because that area has been overwritten by coffee.doc.

Figure 3



[13] Carrier, Brian. File System Forensic Analysis. Crawfordsville: Addison Wesley, 2005. Pg. 228-229

How did this happen? Let's attempt to reconstruct the events in sequence, starting from the top left corner of Figure 3 at sector 511. The system wrote *her.doc* and *hey.doc*. Then, the system wrote *WinPcap_3_1_beta_3.exe*, *WinDump.exe*, *_apture*, and *_ap.gif*. Next, the system deleted all four of the previous files and marked the space they utilized as "not allocated". Lastly, the system wrote *coffee.doc*, beginning at the start of the free space and overwriting the beginning of *WinPcap3_1_beta_3.exe*.

I use the `icat` tool to recover the green files: *WinDump.exe*, *_apture*, and *_ap.gif*. The `icat` tool copies files by directory entry number rather than file name.[14] The `>` option in each command specifies that the system should create a new file with the specified name and write the output of the command to that file.

```
$ icat -r -f fat16 USBFD-64531026-RL-001_part02.img 14 >
recovered/WinDump.exe
```

```
$ icat -r -f fat16 USBFD-64531026-RL-001_part02.img 15 >
recovered/_apture
```

```
$ icat -r -f fat16 USBFD-64531026-RL-001_part02.img 17 >
recovered/_ap.gif
```

For each of the files I recovered with `icat`, I generated a MD5 hash fingerprint and used `file` to determine the file type.

```
File Name: WindDump.exe

MD5 Hash: 79375b77975aa53a1b0507496107bff7

File Type: MS-DOS executable (EXE), OS/2 or MS Windows
```

```
File Name: _apture

MD5 Hash: 2097b7b0a9fedb4238b67e976c4ae1cb

File Type: tcpdump capture file (little-endian) - version 2.4
(Ethernet, capture length 4096)
```

```
File Name: _ap.gif
MD5 Hash: 9bc3923cf8e72fd405d7cea8c8781011
File Type: GIF image data, version 89a, 300 x 200
```

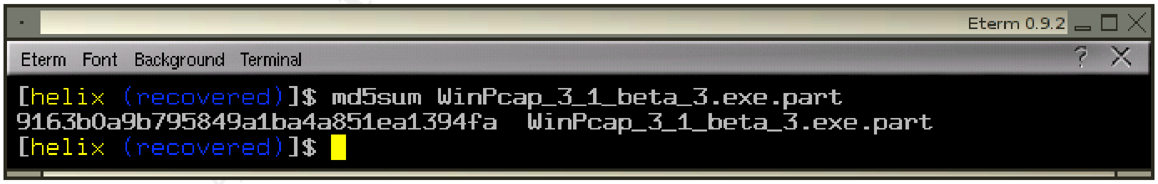
According to the `file` command output, *`WinDump.exe`* is a Windows executable file (a software program), *`_apture`* is a tcpdump capture file (explained in the Recovered File Analysis section), and *`_ap.gif`* is an image file.

I now turned my attention to the partially erased *`WinPcap_3_1_beta_3.exe`*. While the first 19,968 bytes had been overwritten by *`coffee.doc`*, the rest of the file may be intact. I wasn't able to use `icat` to recover the file because `icat` only reads the directory entry, and the directory entry for *`WinPcap_3_1_beta_3.exe`* only pointed to the cluster chain containing *`coffee.doc`*. I needed to read the data straight from the disk sectors. To do this, I used the `dcat` tool, which is also part of The Sleuth Kit. The `dcat` tool displays the contents of disk sectors from a forensic image.[15] I knew that *`coffee.doc`* ended at sector 630, so I used that sector as the starting point for `dcat`. I then specified that `dcat` should read 910 sectors and store the output to a new file named *`WinPcap_3_1_beta.exe.part.`*

```
$ dcat -f fat16 USBFD-64531026-RL-001_part02.img 630 910 >
WinPcap_3_1_beta_3.exe.part
```

I then created an MD5 hash for the partially recovered file.

Figure 4



```
[helix (recovered)]$ md5sum WinPcap_3_1_beta_3.exe.part
9163b0a9b795849a1ba4a851ea1394fa  WinPcap_3_1_beta_3.exe.part
[helix (recovered)]$
```

I now had recovered as many files as possible from the image. My next step was to determine how each file related to the events described by Ms. Conlay.

Program Identification

I found evidence of two executable files on the USB hard drive image: *`WinPcap_3_1_beta_3.exe`* and *`WinDump.exe`*. I was unable to completely recover *`WinPcap_3_1_beta_3.exe`* because the first 19,968 bytes of the file

[14] Carrier, Brian. "icat." The Sleuth Kit. URL: http://www.sleuthkit.org/sleuthkit/man/icat.html. (13 Mar 2005)
[15] Carrier, Brian. "dcat." The Sleuth Kit. URL: http://www.sleuthkit.org/sleuthkit/man/dcat.html. (13 Mar 2005)

had been overwritten by `coffee.doc`. However, I did recover `WinDump.exe` and a portion of `WinDump_3_1_beta_3.exe`. What role did these files have, if any, in Ms. Conlay's complaint?

I started my search on the Internet at the Google[16] website. I entered the search term "windump.exe" into the Google search form. The first page returned was titled "WinDump: tcpdump for Windows" and had an address of http://windump.polito.it/install/default.htm. That website states "WinDump is the porting to the Windows platform of tcpdump, that is a network capture program developed by Network Research Group (NRG) of the Information and Computing Sciences Division (ICSD) at Lawrence Berkeley National Laboratory (LBNL) in Berkeley, California."[17]

Computers communicate with one another via a network. They do so by transmitting small pieces of information called packets. The packet is similar to a letter sent via the postal service. On the outside, the packet identifies the computer it is coming from and where it is destined. On the inside, the packet contains data intended for the other computer. Normally, a computer will discard packets that are not addressed to it. A network packet capture program disables this behavior and allows a system running the software to capture and record all packets it sees rather than discard them. Essentially, this program has the ability to eavesdrop on communications between computers on the network and store them for later viewing. `WinDump.exe` is a network packet capture program.

The file I recovered was named `WinDump.exe` and was executable. However, these two facts do not mean that the file I recovered was actually the WinDump software I located using Google. How could I verify that the file I recovered was WinDump? The WinDump software is freely available from the WinDump website, so I downloaded the latest version of the software, version 3.8.3 beta. When I went to download the software, the download page read that "BEFORE running WinDump 3.8.3 beta you have to download and install WinPcap 3.1 beta2 or beta3."[18] According to the site, WinPcap was a prerequisite to using WinDump. Remember, the other executable file I found was named `WinPcap_3_1_beta_3.exe`. This information supported my hypothesis that the file `WinDump.exe` was the network packet capture software from the WinDump website but did not prove it conclusively.

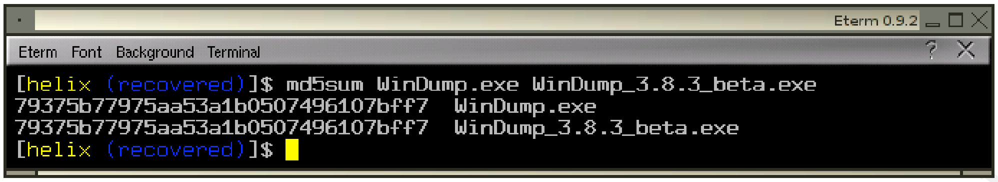
I downloaded the file `WinDump_3_8_3_beta.exe` from the website. I used `md5sum` to create hashes for both the `WinDump.exe` file I recovered and the `WinDump_3_8_3_beta.exe` file that I had downloaded from the WinDump website. The files generated the same hash (see Figure 5), proving conclusively that the files were the same.

[16] Google. "Google Search." URL: http://www.google.com. (2 Apr 2005)

[17] "WinDump: tcpdump for Windows." 3 May 2003. URL: http://windump.polito.it. (3 May 2004)

[18] "WinDump: tcpdump for Windows." 15 May 2004. URL: http://windump.polito.it/install/default.htm. (15 May 2004)

Figure 5



```
[helix (recovered)]$ md5sum WinDump.exe WinDump_3.8.3_beta.exe
79375b77975aa53a1b0507496107bff7  WinDump.exe
79375b77975aa53a1b0507496107bff7  WinDump_3.8.3_beta.exe
[helix (recovered)]$
```

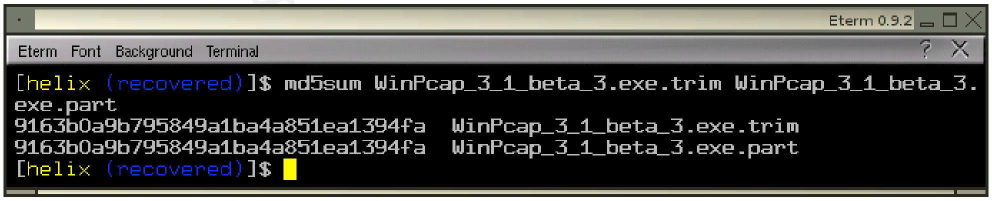
I returned to the Google search page and entered “winpcap_3_1_beta_3.exe” as my search term. One of my search results was a subdirectory off the WinDump website, http://windump.polito.it/misc/bin. The web page contained a directory listing, and *WinPcap_3_1_beta_3.exe* was one of the files listed. I downloaded the file and saved it to my workstation.

While I hadn’t recovered the complete file from the USB hard drive, I did have part of *WinPcap_3_1_beta_3.exe*. Essentially, I wanted to be able to increase my confidence that this program was really WinPcap. And since I didn’t recover a complete file, I planned to compare partial files. Therefore, I needed to remove the same number of bytes from the beginning of my downloaded *WinPcap_3_1_beta_3.exe* as were overwritten by *coffee.doc* in my recovered version. I used `dcfldd` to do this.

```
$ dcfldd if=WinPcap_3_1_beta_3.exe of=WinPcap_3_1_beta_3.exe.trim
ibs=512 skip=39
```

coffee.doc was 19,968 bytes in size, or thirty-nine 512-byte sectors. The `ibs=512` specifies the input block size and the `skip=39` specifies how many blocks to skip before beginning to read and write to the new file. When the command finished, I was left with a file 465,920 bytes in length. I then compared this trimmed file with my recovered file, and the MD5 hashes were identical (see Figure 6).

Figure 6

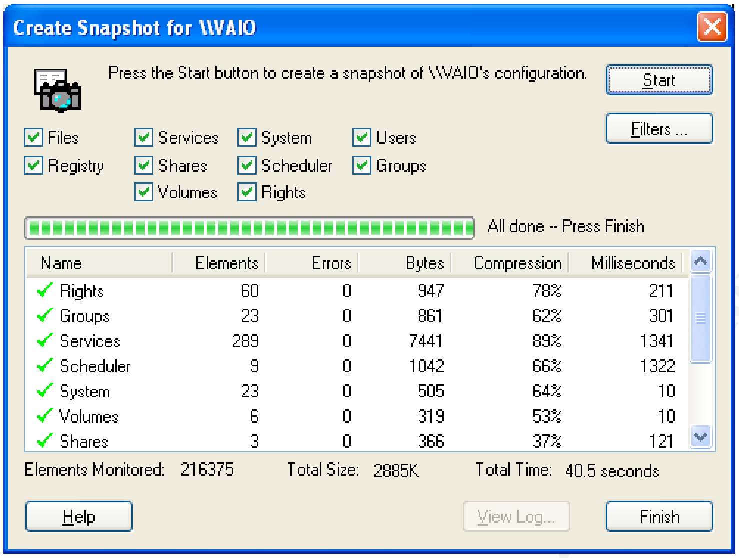


```
[helix (recovered)]$ md5sum WinPcap_3_1_beta_3.exe.trim WinPcap_3_1_beta_3.
exe.part
9163b0a9b795849a1ba4a851ea1394fa  WinPcap_3_1_beta_3.exe.trim
9163b0a9b795849a1ba4a851ea1394fa  WinPcap_3_1_beta_3.exe.part
[helix (recovered)]$
```

While this doesn’t necessarily prove that the file I recovered from the USB drive was identical to the file I downloaded, it dramatically increases my confidence.

So, I knew that *WinDump.exe* required *WinPcap_3_1_beta_3.exe*, but I didn’t know why. How did these two components interact? To attempt to determine their relationship, I analyzed them from on my Windows XP system using two tools. I used `Winalysis` to identify the changes to the system after installing WinPcap, and I used `filemon` from Sysinternals to analyze the running `WinDump.exe` process. The `Winalysis` program can take snapshots of a system and use them to evaluate change on the system including files, registry, users, groups, permissions, and services.[19] I launched `Winalysis`, configured the settings to monitor for all possible changes, and quickly took a photograph of my system (see Figure 7).

Figure 7



Create Snapshot for \\VAIO

Press the Start button to create a snapshot of \\VAIO's configuration.

☑ Files ☑ Services ☑ System ☑ Users
☑ Registry ☑ Shares ☑ Scheduler ☑ Groups
☑ Volumes ☑ Rights

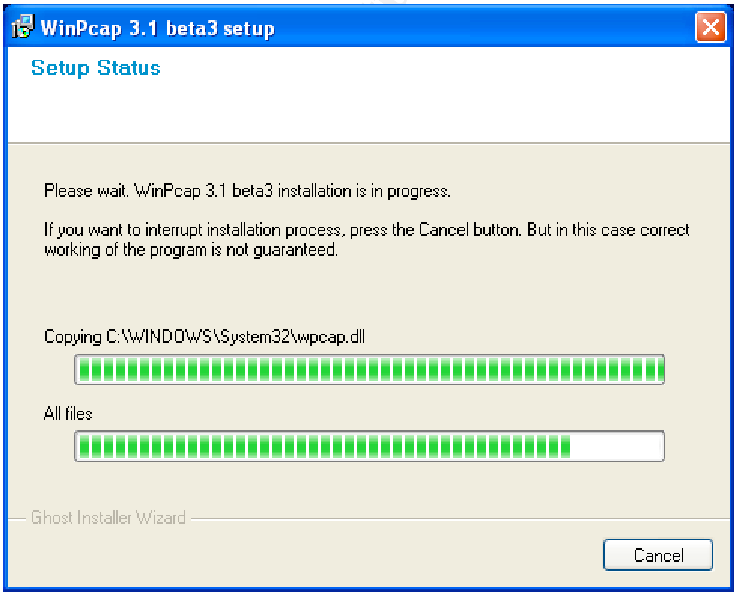
All done -- Press Finish

Name	Elements	Errors	Bytes	Compression	Milliseconds
✓ Rights	60	0	947	78%	211
✓ Groups	23	0	861	62%	301
✓ Services	289	0	7441	89%	1341
✓ Scheduler	9	0	1042	66%	1322
✓ System	23	0	505	64%	10
✓ Volumes	6	0	319	53%	10
✓ Shares	3	0	366	37%	121

Elements Monitored: 216375 Total Size: 2885K Total Time: 40.5 seconds

Once `Winalysis` completed the snapshot, I executed *`WinPcap_3_1_beta_3.exe`*. The file launched an installation program which walked me through installing WinPcap on my system (see Figure 8).

Figure 8



WinPcap 3.1 beta3 setup

Setup Status

Please wait. WinPcap 3.1 beta3 installation is in progress.

If you want to interrupt installation process, press the Cancel button. But in this case correct working of the program is not guaranteed.

Copying C:\WINDOWS\System32\wpcap.dll

All files

[19] "Winalysis Software – Home Page – Security Auditing Solutions." URL: http://www.winalysis.com. (6 May 2003)

With the installation completed, I used the Test function of Winalysis to examine and report the differences found. Winalysis identified 5 new files, 55 new or updated registry keys, and 2 new services.

The new files were:

- C:\WINDOWS\System32\packet.dll
- C:\WINDOWS\System32\pthreadVC.dll
- C:\WINDOWS\System32\wanpacket.dll
- C:\WINDOWS\System32\wpcap.dll
- C:\\WINDOWS\System32\DRIVERS\npf.sys

I now knew what files WinPcap installed, Dynamic Link Library (DLL's) and a system driver. DLL's contain special code that any other program on the system, when executed, can read and utilize to perform special functions.

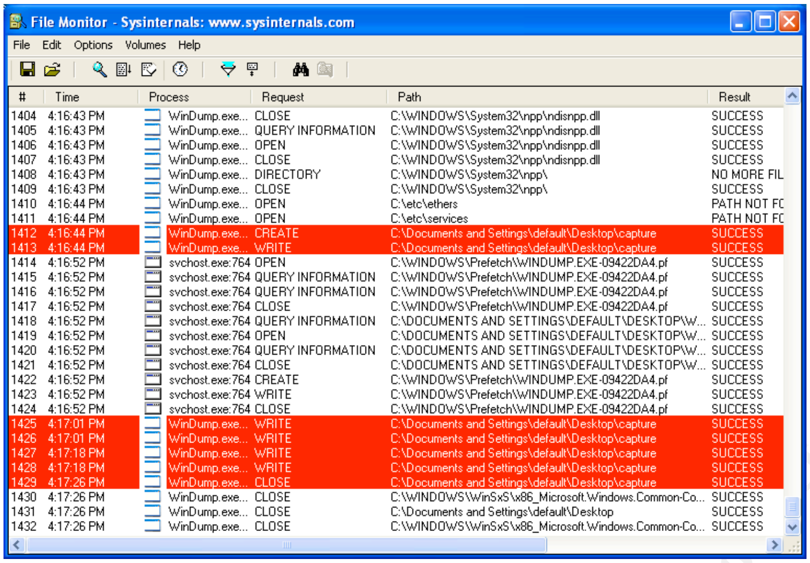
My next step was to execute `WinDump.exe` and "wiretap" it so that I could examine and evaluate its execution. By doing this examination, I hoped to gain a better understanding of how it worked. I used the `filemon` utility from Sysinternals to perform the "tap". The `filemon` utility is a free tool from Sysinternals that "monitors and displays file system activity in real time."[20] I configured the filter within `filemon` to only show activity from `WinDump.exe` and to highlight in red any line with either a WinPcap file or my capture file. I then executed `WinDump.exe` using the command line options specified below.

```
C:\> WinDump.exe –i 2 –w capture –c 2
```

The `-i 2` option specified the network interface to use; the `-w` *`capture`* option identified *`capture`* as the file in which to record all packets; and the `-c 2` option indicated that I only wanted to capture two packets and then exit. Figure 9 shows the `filemon` window after WinDump completed executing. The lines in red are where WinDump created and then wrote to *`capture`* as it received the packets.

[20] "Sysinternals Freeware – Utilities for Windows NT and Windows 2000 – Filemon." URL: www.sysinternals.com/ntw2k/source/filemon.shtml. (5 Apr 2005)

Figure 9



#	Time	Process	Request	Path	Result
1404	4:16:43 PM	WinDump.exe...	CLOSE	C:\WINDOWS\System32\npp\ndisnpp.dll	SUCCESS
1405	4:16:43 PM	WinDump.exe...	QUERY INFORMATION	C:\WINDOWS\System32\npp\ndisnpp.dll	SUCCESS
1406	4:16:43 PM	WinDump.exe...	OPEN	C:\WINDOWS\System32\npp\ndisnpp.dll	SUCCESS
1407	4:16:43 PM	WinDump.exe...	CLOSE	C:\WINDOWS\System32\npp\ndisnpp.dll	SUCCESS
1408	4:16:43 PM	WinDump.exe...	DIRECTORY	C:\WINDOWS\System32\npp\	NO MORE FIL
1409	4:16:43 PM	WinDump.exe...	CLOSE	C:\WINDOWS\System32\npp\	SUCCESS
1410	4:16:44 PM	WinDump.exe...	OPEN	C:\etc\ethers	PATH NOT FC
1411	4:16:44 PM	WinDump.exe...	OPEN	C:\etc\services	PATH NOT FC
1412	4:16:44 PM	WinDump.exe...	CREATE	C:\Documents and Settings\default\Desktop\capture	SUCCESS
1413	4:16:44 PM	WinDump.exe...	WRITE	C:\Documents and Settings\default\Desktop\capture	SUCCESS
1414	4:16:52 PM	svchost.exe:764	OPEN	C:\WINDOWS\Prefetch\WINDUMP.EXE-09422DA4.pf	SUCCESS
1415	4:16:52 PM	svchost.exe:764	QUERY INFORMATION	C:\WINDOWS\Prefetch\WINDUMP.EXE-09422DA4.pf	SUCCESS
1416	4:16:52 PM	svchost.exe:764	QUERY INFORMATION	C:\WINDOWS\Prefetch\WINDUMP.EXE-09422DA4.pf	SUCCESS
1417	4:16:52 PM	svchost.exe:764	CLOSE	C:\WINDOWS\Prefetch\WINDUMP.EXE-09422DA4.pf	SUCCESS
1418	4:16:52 PM	svchost.exe:764	QUERY INFORMATION	C:\DOCUMENTS AND SETTINGS\DEFAULT\DESKTOP\W...	SUCCESS
1419	4:16:52 PM	svchost.exe:764	OPEN	C:\DOCUMENTS AND SETTINGS\DEFAULT\DESKTOP\W...	SUCCESS
1420	4:16:52 PM	svchost.exe:764	QUERY INFORMATION	C:\DOCUMENTS AND SETTINGS\DEFAULT\DESKTOP\W...	SUCCESS
1421	4:16:52 PM	svchost.exe:764	CLOSE	C:\DOCUMENTS AND SETTINGS\DEFAULT\DESKTOP\W...	SUCCESS
1422	4:16:52 PM	svchost.exe:764	CREATE	C:\WINDOWS\Prefetch\WINDUMP.EXE-09422DA4.pf	SUCCESS
1423	4:16:52 PM	svchost.exe:764	WRITE	C:\WINDOWS\Prefetch\WINDUMP.EXE-09422DA4.pf	SUCCESS
1424	4:16:52 PM	svchost.exe:764	CLOSE	C:\WINDOWS\Prefetch\WINDUMP.EXE-09422DA4.pf	SUCCESS
1425	4:17:01 PM	WinDump.exe...	WRITE	C:\Documents and Settings\default\Desktop\capture	SUCCESS
1426	4:17:01 PM	WinDump.exe...	WRITE	C:\Documents and Settings\default\Desktop\capture	SUCCESS
1427	4:17:18 PM	WinDump.exe...	WRITE	C:\Documents and Settings\default\Desktop\capture	SUCCESS
1428	4:17:18 PM	WinDump.exe...	WRITE	C:\Documents and Settings\default\Desktop\capture	SUCCESS
1429	4:17:26 PM	WinDump.exe...	CLOSE	C:\Documents and Settings\default\Desktop\capture	SUCCESS
1430	4:17:26 PM	WinDump.exe...	CLOSE	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Co...	SUCCESS
1431	4:17:26 PM	WinDump.exe...	CLOSE	C:\Documents and Settings\default\Desktop	SUCCESS
1432	4:17:26 PM	WinDump.exe...	CLOSE	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Co...	SUCCESS

When I executed `WinDump.exe` with the above command, the system performed the following high-level operations on the system:

- Opened `WinDump.exe`
- Opened a large number of Dynamic Link Libraries (DLL's) including *wpcap.dll*, *packet.dll*, and *wanpacket.dll*
- Opened the *npf.sys* driver
- Created the *capture* file
- Wrote two times the *capture* file
- Closed the *capture* file

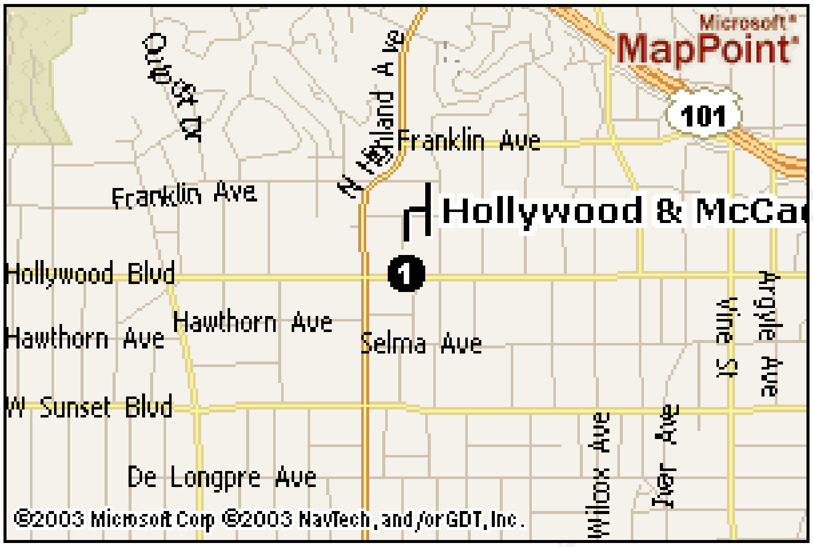
From my evaluation of the two software programs, I verified that *WinDump.exe* does require files provided by the installation of *WinPcap_3_1_beta_3.exe*. Those installed files were a driver file and four dynamic link library files, which included additional functionality and code required by WinDump.

So, I had verified that `Windump.exe`, the network packet capture software, was stored on the USB hard drive and was deleted. I also knew that the recovered *WinPcap_3_1_beta_3.exe* file was most likely the prerequisite file required to make *WinDump.exe* function and I had a good idea about what *WinDump.exe* did during execution. However, I still did not know if and how this software might have been used in the events on October 28th. I needed to continue my examination and analysis of the other two recovered files.

Recovered File Analysis

I first need to verify that the `file` program correctly identified each file type. The file program identified the `_ap.gif` file as a GIF image file. I opened the image using the `kview` image viewer. The image is shown in Figure 10 and is a street map of an area of Los Angeles, CA.

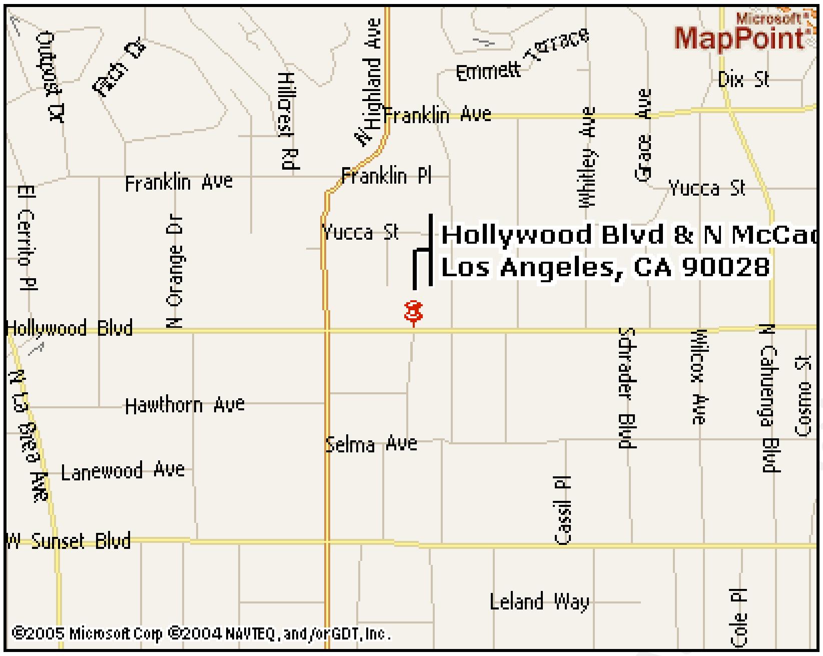
Figure 10



From the image, I could tell that Microsoft MapPoint generated the map. Again, I used Google and entered my search term "Microsoft MapPoint". The first page of my search results was titled "MSN Maps and Directions" and had an address of http://www.mapblast.com. I used my web browser to navigate to that address. I entered in the address "Hollywood & McCadden" as the Street Address and "Los Angeles, CA" as the city and state in the search form on the Map and Directions page[21]. MapPoint returned the following street map of Hollywood Blvd & N. McCadden Pl., Los Angeles, CA 90028. The street map depicted in the image I recovered from the USB drive was very similar to the image I viewed on the MapPoint web site (see Figure 11).

[21] "MSN Maps & Directions." URL: http://www.mapblast.com. (2 Apr 2005)

Figure 11



The `file` program identified the `_apture` file as a `tcpdump` capture file. Remember, the `WinDump.exe` program I recovered was essentially `tcpdump` for Microsoft Windows. `tcpdump` is a network packet capture program which reads network packets seen by a computer and writes them to a file. The most reasonable hypothesis is that the `WinDump.exe` program was executed and stored the packets it captured in the `_apture` file. However, I needed to examine the `_apture` file and determine if it contained packets with content relating to Ms. Conlay.

I used `ethereal` to view the `_apture` file. The `ethereal` program is similar to `tcpdump`; it is able to capture network packets as well as to decode network packets from an existing packet capture file.[22] I successfully opened the `_apture` file, and `ethereal` indicated that the file contained 113 packets captured over a period of .935 seconds starting at 14:10:54 and ending at 14:10:55 on October 28, 2004.

After opening the `_apture` file in `ethereal`, I began my analysis of the packet capture. The IP address `192.168.2.104` initiated the only TCP conversations. During the brief duration of the capture, this source address had nine conversations with six unique hosts on port 80, which is the standard port for web communications. I have listed the statistics relating to each conversation in Table 3, ordered by total packets sent during the conversation.

[22] "Ethereal: Introduction." 5 Apr 2005. URL: http://www.ethereal.com/introduction.html. (5 Apr 2005)

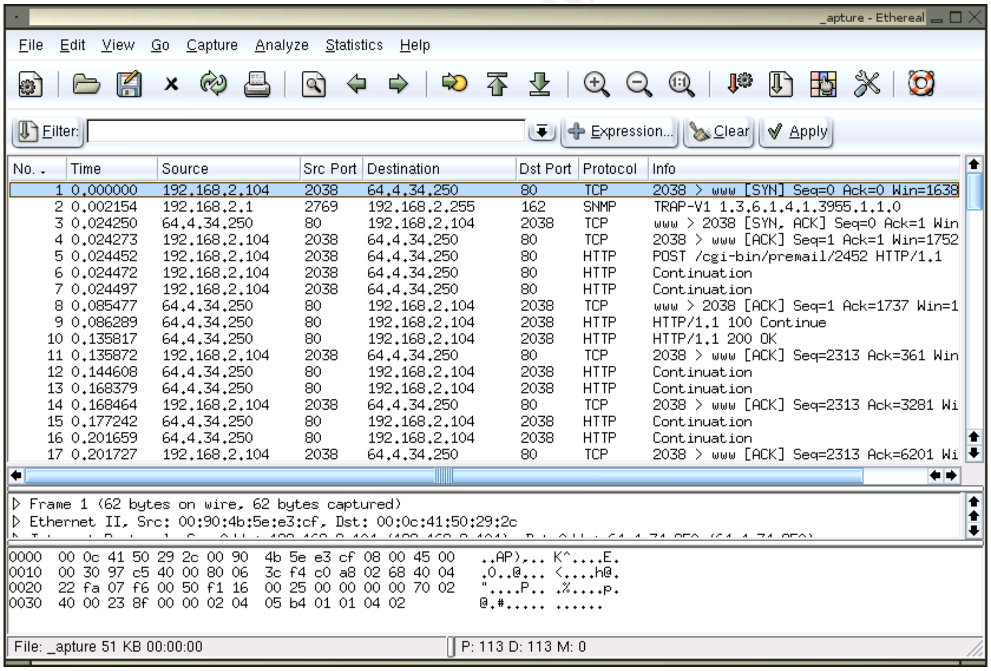
Table 3

Source Port	Destination Address	Dest. Port	Pkts	Bytes	Packets Sent	Bytes Sent	Packets Received	Bytes Received
2038	64.4.34.250	80	34	22578	16	3232	18	19346
2039	207.68.178.16	80	18	7764	8	4013	10	3751
2040	207.68.178.16	80	13	5365	6	2716	7	2649
2042	63.209.188.62	80	12	5055	6	1281	6	3774
2045	216.73.86.40	80	11	5396	6	985	5	4411
2041	207.68.177.124	80	8	1886	5	1326	3	560
2043	63.209.188.62	80	7	2006	4	699	3	1307
2044	216.73.86.40	80	3	178	2	116	1	62
2046	63.166.13.75	80	1	62	1	62	0	0

From the table, the conversation with the most activity and data was between `192.168.2.104` and `64.4.34.250`. I performed a DNS lookup on `64.4.34.250`, and that address resolved to www.bay12.hotmail.com. Hotmail is part of the MSN network and is Microsoft's free e-mail service provider that allows its users to send and receive e-mail using a web browser.[23]

I selected packet number 1 in the capture file, which was the first packet in the most active Hotmail conversation (see Figure 12).

Figure 12



```
No. .  Time      Source          Src Port Destination     Dst Port Protocol Info
     1 0.000000  192.168.2.104   2038     64.4.34.250     80       TCP      2038 > www [SYN] Seq=0 Ack=0 Win=1638
     2 0.002154  192.168.2.1     2769     192.168.2.255   162      SNMP     TRAP-V1 1.3.6.1.4.1.3955.1.1.0
     3 0.024250  64.4.34.250     80       192.168.2.104   2038     TCP      www > 2038 [SYN, ACK] Seq=0 Ack=1 Win
     4 0.024273  192.168.2.104   2038     64.4.34.250     80       TCP      2038 > www [ACK] Seq=1 Ack=1 Win=1752
     5 0.024452  192.168.2.104   2038     64.4.34.250     80       HTTP     POST /cgi-bin/premail/2452 HTTP/1.1
     6 0.024472  192.168.2.104   2038     64.4.34.250     80       HTTP     Continuation
     7 0.024497  192.168.2.104   2038     64.4.34.250     80       HTTP     Continuation
     8 0.085477  64.4.34.250     80       192.168.2.104   2038     TCP      www > 2038 [ACK] Seq=1 Ack=1737 Win=1
     9 0.086289  64.4.34.250     80       192.168.2.104   2038     HTTP     HTTP/1.1 100 Continue
    10 0.135817  64.4.34.250     80       192.168.2.104   2038     HTTP     HTTP/1.1 200 OK
    11 0.135872  192.168.2.104   2038     64.4.34.250     80       TCP      2038 > www [ACK] Seq=2313 Ack=361 Win
    12 0.144608  64.4.34.250     80       192.168.2.104   2038     HTTP     Continuation
    13 0.168379  64.4.34.250     80       192.168.2.104   2038     HTTP     Continuation
    14 0.168464  192.168.2.104   2038     64.4.34.250     80       TCP      2038 > www [ACK] Seq=2313 Ack=3281 Wi
    15 0.177242  64.4.34.250     80       192.168.2.104   2038     HTTP     Continuation
    16 0.201659  64.4.34.250     80       192.168.2.104   2038     HTTP     Continuation
    17 0.201727  192.168.2.104   2038     64.4.34.250     80       TCP      2038 > www [ACK] Seq=2313 Ack=6201 Wi
```

```
▷ Frame 1 (62 bytes on wire, 62 bytes captured)
▷ Ethernet II, Src: 00:90:4b:5e:e3:cf, Dst: 00:0c:41:50:29:2c
```

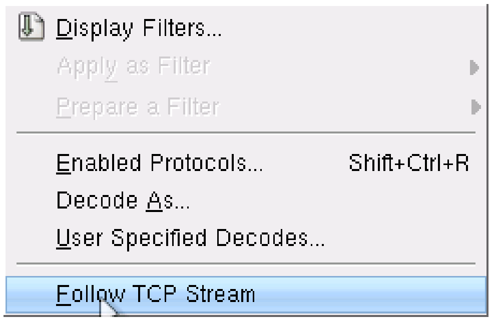
```
0000  00 0c 41 50 29 2c 00 90  4b 5e e3 cf 08 00 45 00   ..AP),.. K^....E.
0010  00 30 97 c5 40 00 80 06  3c f4 c0 a8 02 68 40 04   .0..@... <....h@.
0020  22 fa 07 f6 00 50 f1 16  00 25 00 00 00 00 70 02   "....P.. .%....p.
0030  40 00 23 8f 00 00 02 04  05 b4 01 01 04 02         @.#..... ......
```

File: _apture 51 KB 00:00:00 | P: 113 D: 113 M: 0

I then went to `ethereal`'s `Analyze` menu and selected `Follow TCP Stream`, as shown in Figure 13.

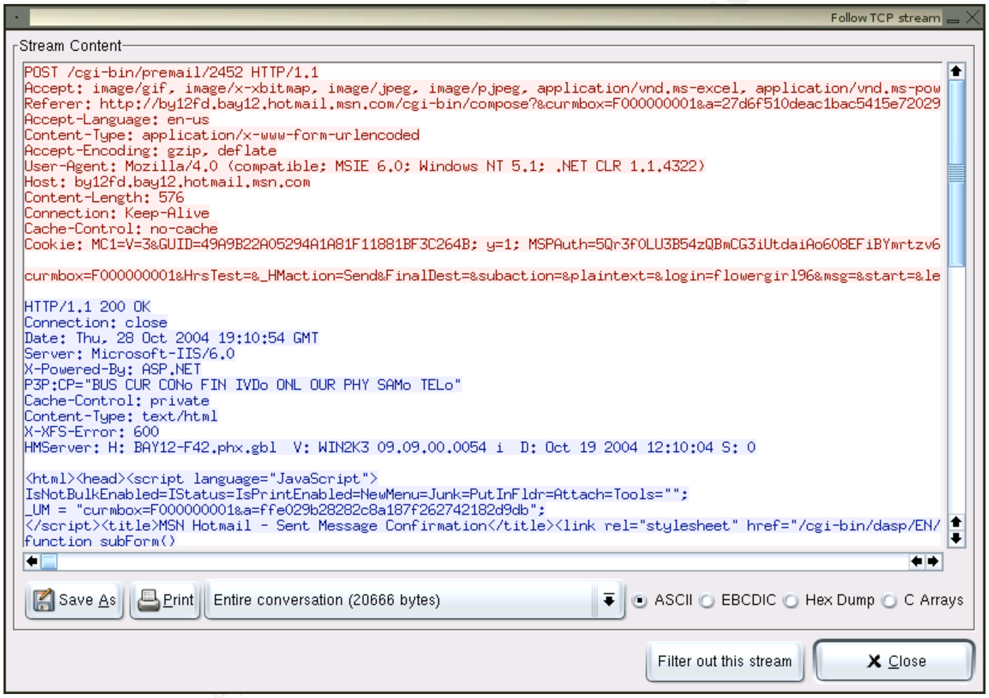
[23] "MSN Hotmail." URL: http://www.hotmail.com. (5 Apr 2005)

Figure 13



The Follow TCP Stream option takes a specific conversation and aggregates all the content from that conversation into one window where it identifies each side of the conversation by color. Figure 14 shows a portion of the content of the conversation between `192.168.2.104` and the Hotmail server.

Figure 14



```
POST /cgi-bin/premail/2452 HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/vnd.ms-pow
Referer: http://by12fd.bay12.hotmail.msn.com/cgi-bin/compose?&curmbox=F000000001&a=27d6f510deac1bac5415e72029
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)
Host: by12fd.bay12.hotmail.msn.com
Content-Length: 576
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: MC1=V=3&GUID=49A9B22A05294A1A81F11881BF3C264B; y=1; MSPAuth=5Qr3f0LU3B54zQBmCG3iUtdaiAo608EFiBYmrtzv6

curmbox=F000000001&HrsTest=&_HMaction=Send&FinalDest=&subaction=&plaintext=&login=flowergirl96&msg=&start=&le

HTTP/1.1 200 OK
Connection: close
Date: Thu, 28 Oct 2004 19:10:54 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
P3P:CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo"
Cache-Control: private
Content-Type: text/html
X-XFS-Error: 600
HMServer: H: BAY12-F42.phx.gbl  V: WIN2K3 09.09.00.0054 i  D: Oct 19 2004 12:10:04 S: 0

<html><head><script language="JavaScript">
IsNotBulkEnabled=IStatus=IsPrintEnabled=NewMenu=Junk=PutInFldr=Attach=Tools="";
_UM = "curmbox=F000000001&a=ffe029b28282c8a187f262742182d9db";
</script><title>MSN Hotmail - Sent Message Confirmation</title><link rel="stylesheet" href="/cgi-bin/dasp/EN/
function subForm()
```

Save As
Print
Entire conversation (20666 bytes)
● ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays
Filter out this stream
Close

I have highlighted the data of interest contained in the conversation.

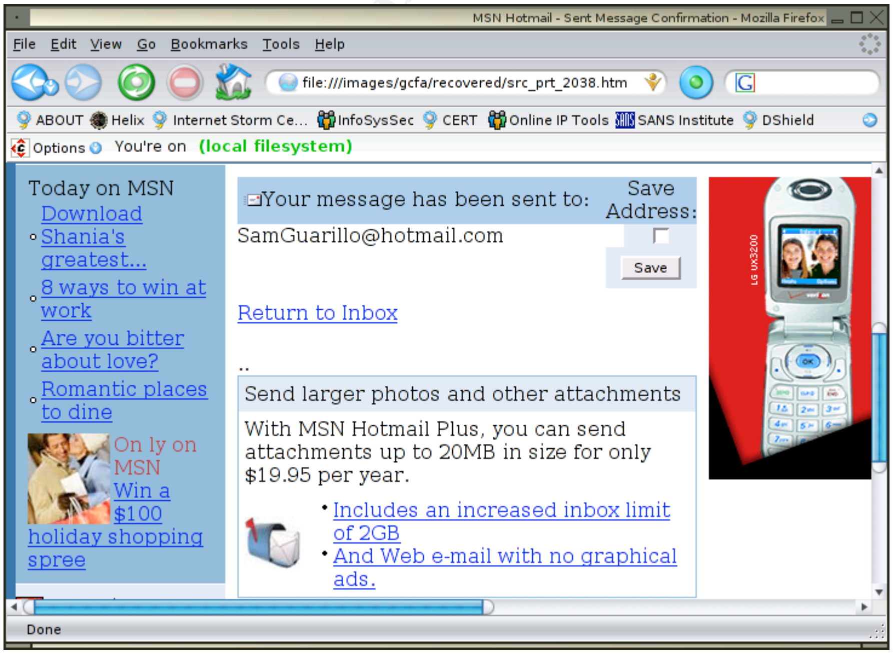
```
curmbox=F000000001&HrsTest=&_HMaction=Send&FinalDest=&subaction=&plain
text=&login=flowergirl96&msg=&start=&len=&attfile=&attlistfile=&eurl=&
type=&src=&ref=&ru=&msghdrid=b16479b18beec291196189c78555223c_10986924
52&RTEbgcolor=&encodedto=SamGuarillo@hotmail.com&encodedcc=&encodedbcc
=&deleteUponSend=0&importance=&sigflag=&newmail=new&to=SamGuarillo@hot
mail.com&cc=&bcc=&subject=RE%3A+coffee&body=Sure%2C+coffee+sounds+grea
t.++Let%27s+meet+at+the+coffee+shop+on+the+corner+Hollywood+and+McCadd
en.++It%27s+a+nice+out+of+the+way+spot.%0D%0A%0D%0ASee+you+at+7pm%21%0
D%0A%0D%0A-Leila
```

The string contains a login ID (`flowergirl96`) and, what appears to be, the content of an e-mail message. Remember, Hotmail provides web access to a user's e-mail account. In order to send the content to the server, the browser encoded all the special characters (such as spaces, carriage returns, and punctuation) to ensure that the server did not misinterpret them. To decode the message, I converted all the '%XX' characters from hexadecimal to their character equivalent. For example, %27 is 91 in decimal, which equates to an apostrophe in ASCII. When I decoded the entire message using this method, the message read (I formatted the "To" line and the "Subject" line for clarity):

```
To: SamGuarillo@hotmail.com

Subject: RE: coffee

Sure, coffee sounds great.  Let's meet at the
coffee shop on the corner Hollywood and McCadden.
It's a nice out of the way spot.


See you at 7pm.


-Leila
```

The Hotmail server sent back an HTML page (in blue) in response to the e-mail submission. I saved the HTML page and viewed it in my web browser and was presented with the page shown in Figure 14, confirming that the Ms. Conlay sent an e-mail message to the SamGuarillo@hotmail.com e-mail address. The contents of that e-mail message provided a meeting time and a location.

Figure 15



MSN Hotmail - Sent Message Confirmation - Mozilla Firefox

file:///images/gcfa/recovered/src_prt_2038.htm

You're on (local filesystem)

Your message has been sent to: SamGuarillo@hotmail.com

Save Address: □ Save

Return to Inbox

Send larger photos and other attachments

With MSN Hotmail Plus, you can send attachments up to 20MB in size for only $19.95 per year.

- Includes an increased inbox limit of 2GB
- And Web e-mail with no graphical ads.

From the contents of the packet capture file `_apture`, I determined that Mr. Lawrence executed the `WinDump.exe` program at 11:10 and used that program to intercept communications between Ms. Conlay and the Hotmail server. The communication informed Mr. Lawrence of the whereabouts of Ms. Conlay on the evening of October 28, 2004. The recovered map image, `_ap.gif`, indicated that Mr. Lawrence attempted to geographically find the location of Ms. Conlay's meeting and subsequently appeared at that location. Further, after this encounter, Mr. Lawrence may have sent a threat to Ms. Conlay.

Legal and Policy Implications

From the information I collected, the following organizational policies and federal laws were implicated by Mr. Lawrence's actions.

The examination indicates that the following CC Terminals, Inc. policies are implicated:

- CC Terminals User Rules of Behavior, which states that use of information systems equipment owned or operated by the company by an employee, for other than official CC Terminals business or authorized purposes, is prohibited. Mr. Lawrence violated this policy by using a CC Terminals information system for personal business. The penalties for violating this policy are disciplinary action up to and including termination.
- CC Terminals Appropriate Use policy states that the use of restricted software by an unauthorized user is prohibited. Restricted software includes, but is not limited to, network "sniffers", network scanning software, and vulnerability assessment tools. Mr. Lawrence violated this policy by installing and executing restricted software on a CC Terminals information system. The penalties for violating this policy are disciplinary action up to and including termination.

Further, the following federal U.S. statutes may be implicated:

- 18 U.S. Code. Sec. 2511(1)(a), which prohibits the interception and disclosure of wire, oral, or electronic communications, unless an exemption applies, and carries a penalty of a fine or up to five years in prison, or both, if convicted. Mr. Lawrence intercepted Ms. Conlay's communications in real-time, without her consent, and none of the exemptions apply which would support his actions.[24]
- 18 U.S. Code. Sec. 875(c), which prohibits using interstate or foreign commerce to transmit any communication containing any threat to injure another person, and carries a penalty of a fine or up to five years in prison, or both, if convicted. If it is determined that Mr. Lawrence did

[24] 18 U.S. Code. Sec. 2511(1)(a)

send Ms. Conlay the contents of the recovered documents, he would be in violation of this statute.[25]

Recommendations

The evidence I collected from the USB drive image showed that Mr. Lawrence used `WinDump` to intercept Ms. Conlay's electronic communications. In addition to the CC Terminals policy violations, Mr. Lawrence could be facing criminal charges. Since federal statutes are implicated, I recommend that CC Terminals immediately report the incident to the FBI and that Mr. Lawrence be placed on unpaid leave pending the outcome of a full investigation, including examination of his workstation and e-mail. Ms. Conlay's e-mail should also be examined to determine if the documents recovered from Mr. Lawrence's USB hard drive were ever sent to her.

Additional Information

- **File System Forensic Analysis**, Brian Carrier. 2005. Brian Carrier has written the quintessential reference for understanding the most popular file system formats. This book contains details on the FAT16 file system that I encountered on the USB hard drive image, and Mr. Carrier explains how to analyze this type of file system.
- "**The Sleuth Kit**", Brian Carrier: http://www.sleuthkit.org/sleuthkit. I predominantly used The Sleuth Kit for my analysis. The website provides information on all the tools contained in the tool kit.
- ***Wire and Electronic Communications Interception and Interception of Oral Communications***, U.S. Department of Justice http://www.cybercrime.gov/wiretap2510_2522.htm. I used this document to understand the nuances and exemptions pertinent to the wiretap statutes. The document does a reasonable job explaining the law and penalties if convicted.
- ***Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations***, Computer Crime and Intellectual Property Section, Criminal Division, U.S. Department of Justice http://www.cybercrime.gov/criminal/cybercrime/s&smanual2002.pdf. This document contains case law and background information to understand the correct methods to collect and handle digital evidence. It is written to law enforcement. However, the document describes key information necessary for any digital investigation.

[25] 18 U.S. Code. Sec. 875(c)

References

18 U.S. Code. Sec. 2511(1)(a)

18 U.S. Code. Sec. 875(c)

Carrier, Brian (2005). “dcat.” The Sleuth Kit. http://www.sleuthkit.org/sleuthkit/man/dcat.html. (13 Mar 2005)

Carrier, Brian (2005) “Description.” The Sleuth Kit. http://www.sleuthkit.org/sleuthkit/desc.php. (2 Apr 2005)

Carrier, Brian (2003) “File Activity Timelines.” The Sleuth Kit. http://www.sleuthkit.org/sleuthkit/docs/ref_timeline.html. (19 Jun 2003)

Carrier, Brian (2005). File System Forensic Analysis. Crawfordsville: Addison Wesley.

Carrier, Brian (2005). “icat.” The Sleuth Kit. http://www.sleuthkit.org/sleuthkit/man/icat.html. (13 Mar 2005)

Carrier, Brian (2005). “mactime.” The Sleuth Kit. http://www.sleuthkit.org/sleuthkit/man/mactime.html. (13 Mar 2005)

Carrier, Brian (2005). “Tool Details.” The Sleuth Kit. 2005. http://www.sleuthkit.org/sleuthkit/tools.php. (2 Apr 2005)

e-fense, Inc. (2005). “Helix Incident Response & Computer Forensics.” http://www.e-fense.com/helix/index2.html. (11 Mar 2005)

“Ethereal: Introduction.” http://www.ethereal.com/introduction.html. (5 Apr 2005)

Google. “Google Search.” http://www.google.com. (2 Apr 2005)

“MSN Hotmail.” http://www.hotmail.com. (5 Apr 2005)

“MSN Maps & Directions.” URL: http://www.mapblast.com. (2 Apr 2005)

Rivest, Ronald (1992). “Executive Summary.” The MD5 Message-Digest Algorithm. http://www.ietf.org/rfc/rfc1321.txt?number=1321. (15 Apr 1992)

“Sysinternals Freeware – Utilities for Windows NT and Windows 2000 – Filemon.” www.sysinternals.com/ntw2k/source/filemon.shtml. (5 Apr 2005)

“Unix man pages: fdisk.” Linux Programmer’s Manual (1998). http://www.rt.com/man/fdisk.8.html. (2 Apr 2005)

"Winalysis Software – Home Page – Security Auditing Solutions." http://www.winalysis.com. (6 May 2003)

"WinDump: tcpdump for Windows." http://windump.polito.it. (3 May 2004)

"WinDump: tcpdump for Windows." http://windump.polito.it/install/default.htm. (15 May 2004)

Appendix A – Command Summary

Output: mactime

Date	Size	Type	Meta	File Name
Mon Oct 25 2004 00:00:00	19968	.a.	3	/her.doc
Mon Oct 25 2004 08:32:06	19968	..c	3	/her.doc
Mon Oct 25 2004 08:32:08	19968	m..	3	/her.doc
Tue Oct 26 2004 00:00:00	19968	.a.	4	/hey.doc
Tue Oct 26 2004 08:48:06	19968	..c	4	/hey.doc
Tue Oct 26 2004 08:48:10	19968	m..	4	/hey.doc
Wed Oct 27 2004 00:00:00	485810	.a.	7	/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)
Wed Oct 27 2004 00:00:00	450560	.a.	12	/WinDump.exe (_INDUMP.EXE) (deleted)
Wed Oct 27 2004 00:00:00	0	.a.	7	<USBFD-64531026-RL-001_part02.img-_INPCA~1.EXE-dead-7>
Wed Oct 27 2004 00:00:00	0	.a.	12	<USBFD-64531026-RL-001_part02.img-_INDUMP.EXE-dead-12>
Wed Oct 27 2004 16:23:50	485810	m..	10	<USBFD-64531026-RL-001_part02.img-_INPCA~1.EXE-dead-10>
Wed Oct 27 2004 16:23:50	485810	m..	10	/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)
Wed Oct 27 2004 16:23:54	485810	..c	10	<USBFD-64531026-RL-001_part02.img-_INPCA~1.EXE-dead-10>
Wed Oct 27 2004 16:23:54	485810	..c	10	/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)
Wed Oct 27 2004 16:23:54	0	..c	7	<USBFD-64531026-RL-001_part02.img-_INPCA~1.EXE-dead-7>

Wed Oct 27 2004 16:23:54	485810	..c	7	/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)
Wed Oct 27 2004 16:23:56	0	m..	7	<USBFD-64531026-RL-001_part02.img-_INPCA~1.EXE-dead-7>
Wed Oct 27 2004 16:23:56	485810	m..	7	/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)
Wed Oct 27 2004 16:24:02	450560	m..	14	/WinDump.exe (_INDUMP.EXE) (deleted)
Wed Oct 27 2004 16:24:02	450560	m..	14	<USBFD-64531026-RL-001_part02.img-_INDUMP.EXE-dead-14>
Wed Oct 27 2004 16:24:04	0	..c	12	<USBFD-64531026-RL-001_part02.img-_INDUMP.EXE-dead-12>
Wed Oct 27 2004 16:24:04	450560	..c	12	/WinDump.exe (_INDUMP.EXE) (deleted)
Wed Oct 27 2004 16:24:04	450560	..c	14	/WinDump.exe (_INDUMP.EXE) (deleted)
Wed Oct 27 2004 16:24:04	450560	..c	14	<USBFD-64531026-RL-001_part02.img-_INDUMP.EXE-dead-14>
Wed Oct 27 2004 16:24:06	450560	m..	12	/WinDump.exe (_INDUMP.EXE) (deleted)
Wed Oct 27 2004 16:24:06	0	m..	12	<USBFD-64531026-RL-001_part02.img-_INDUMP.EXE-dead-12>
Thu Oct 28 2004 00:00:00	53056	.a.	15	/_apture (deleted)
Thu Oct 28 2004 00:00:00	8814	.a.	17	<USBFD-64531026-RL-001_part02.img-_ap.gif-dead-17>
Thu Oct 28 2004 00:00:00	8814	.a.	16	/_ap.gif (deleted)
Thu Oct 28 2004 00:00:00	450560	.a.	14	/WinDump.exe (_INDUMP.EXE) (deleted)
Thu Oct 28 2004 00:00:00	19968	.a.	18	/coffee.doc
Thu Oct 28 2004 00:00:00	53056	.a.	15	<USBFD-64531026-RL-001_part02.img-_apture-dead-15>

Thu Oct 28 2004 00:00:00	8814	.a.	17	/_ap.gif (deleted)
Thu Oct 28 2004 00:00:00	0	.a.	16	<USBFD-64531026-RL-001_part02.img-_ap.gif-dead-16>
Thu Oct 28 2004 00:00:00	485810	.a.	10	<USBFD-64531026-RL-001_part02.img-_INPCA~1.EXE-dead-10>
Thu Oct 28 2004 00:00:00	450560	.a.	14	<USBFD-64531026-RL-001_part02.img-_INDUMP.EXE-dead-14>
Thu Oct 28 2004 00:00:00	485810	.a.	10	/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)
Thu Oct 28 2004 11:08:24	53056	..c	15	/_apture (deleted)
Thu Oct 28 2004 11:08:24	53056	..c	15	<USBFD-64531026-RL-001_part02.img-_apture-dead-15>
Thu Oct 28 2004 11:11:00	53056	m..	15	/_apture (deleted)
Thu Oct 28 2004 11:11:00	53056	m..	15	<USBFD-64531026-RL-001_part02.img-_apture-dead-15>
Thu Oct 28 2004 11:17:44	8814	..c	16	/_ap.gif (deleted)
Thu Oct 28 2004 11:17:44	8814	..c	17	/_ap.gif (deleted)
Thu Oct 28 2004 11:17:44	0	..c	16	<USBFD-64531026-RL-001_part02.img-_ap.gif-dead-16>
Thu Oct 28 2004 11:17:44	8814	..c	17	<USBFD-64531026-RL-001_part02.img-_ap.gif-dead-17>
Thu Oct 28 2004 11:17:46	8814	m..	17	<USBFD-64531026-RL-001_part02.img-_ap.gif-dead-17>
Thu Oct 28 2004 11:17:46	0	m..	16	<USBFD-64531026-RL-001_part02.img-_ap.gif-dead-16>
Thu Oct 28 2004 11:17:46	8814	m..	16	/_ap.gif (deleted)
Thu Oct 28 2004	8814	m..	17	/_ap.gif (deleted)

11:17:46				
Thu Oct 28 2004 19:24:46	19968	..c	18	/coffee.doc
Thu Oct 28 2004 19:24:48	19968	m..	18	/coffee.doc

Output: istat

```
$ istat -f fat16 USBFD-64531026-RL-001_part02.img 3
Directory Entry: 3
Allocated
File Attributes: File, Archive
Size: 19968
Name: her.doc

Directory Entry Times:
Written:        Mon Oct 25 08:32:08 2004
Accessed:       Mon Oct 25 00:00:00 2004
Created:        Mon Oct 25 08:32:06 2004

Sectors:
511 512 513 514 515 516 517 518
519 520 521 522 523 524 525 526
527 528 529 530 531 532 533 534
535 536 537 538 539 540 541 542
543 544 545 546 547 548 549 550
```

```
$ istat -f fat16 USBFD-64531026-RL-001_part02.img 4
Directory Entry: 4
Allocated
File Attributes: File, Archive
Size: 19968
Name: hey.doc
```

```
Directory Entry Times:
Written:        Tue Oct 26 08:48:10 2004
Accessed:       Tue Oct 26 00:00:00 2004
Created:        Tue Oct 26 08:48:06 2004

Sectors:
551 552 553 554 555 556 557 558
559 560 561 562 563 564 565 566
567 568 569 570 571 572 573 574
575 576 577 578 579 580 581 582
583 584 585 586 587 588 589 590
```

```
$ istat -f fat16 USBFD-64531026-RL-001_part02.img 7
Directory Entry: 7
Not Allocated
File Attributes: File, Archive
Size: 0
Name: _INPCA~1.EXE

Directory Entry Times:
Written:        Wed Oct 27 16:23:56 2004
Accessed:       Wed Oct 27 00:00:00 2004
Created:        Wed Oct 27 16:23:54 2004

Sectors:

Recovery:
File recovery not possible
```

```
$ istat -f fat16 USBFD-64531026-RL-001_part02.img 10
Directory Entry: 10
Not Allocated
File Attributes: File, Archive
```

```
Size: 485810
Name: _INPCA~1.EXE

Directory Entry Times:
Written:        Wed Oct 27 16:23:50 2004
Accessed:       Thu Oct 28 00:00:00 2004
Created:        Wed Oct 27 16:23:54 2004

Sectors:
591 592 593 594 595 596 597 598
599 600 601 602 603 604 605 606
607 608 609 610 611 612 613 614
615 616 617 618 619 620 621 622
623 624 625 626 627 628 629 630

Recovery:
File recovery not possible
```

```
$ istat -f fat16 USBFD-64531026-RL-001_part02.img 12
Directory Entry: 12
Not Allocated
File Attributes: File, Archive
Size: 0
Name: _INDUMP.EXE

Directory Entry Times:
Written:        Wed Oct 27 16:24:06 2004
Accessed:       Wed Oct 27 00:00:00 2004
Created:        Wed Oct 27 16:24:04 2004

Sectors:

Recovery:
File recovery not possible
```

```
$ istat -f fat16 USBFD-64531026-RL-001_part02.img 14
Directory Entry: 14
Not Allocated
File Attributes: File, Archive
Size: 450560
Name: _INDUMP.EXE

Directory Entry Times:
Written:        Wed Oct 27 16:24:02 2004
Accessed:       Thu Oct 28 00:00:00 2004
Created:        Wed Oct 27 16:24:04 2004

Sectors:
1541 1542

Recovery:
1541 1542 1543 1544 1545 1546 1547 1548
<REMOVED FOR BREVITY>
2413 2414 2415 2416 2417 2418 2419 2420
```

```
$ istat -f fat16 USBFD-64531026-RL-001_part02.img 15
Directory Entry: 15
Not Allocated
File Attributes: File, Archive
Size: 53056
Name: _apture

Directory Entry Times:
Written:        Thu Oct 28 11:11:00 2004
Accessed:       Thu Oct 28 00:00:00 2004
Created:        Thu Oct 28 11:08:24 2004

Sectors:
```

```
2421 2422

Recovery:
2421 2422 2423 2424 2425 2426 2427 2428
<REMOVED FOR BREVITY>
2517 2518 2519 2520 2521 2522 2523 2524
```

```
$ istat -f fat16 USBFD-64531026-RL-001_part02.img 16
Directory Entry: 16
Not Allocated
File Attributes: File, Archive
Size: 0
Name: _ap.gif

Directory Entry Times:
Written:        Thu Oct 28 11:17:46 2004
Accessed:       Thu Oct 28 00:00:00 2004
Created:        Thu Oct 28 11:17:44 2004

Sectors:

Recovery:
File recovery not possible
```

```
$ istat -f fat16 USBFD-64531026-RL-001_part02.img 17
Directory Entry: 17
Not Allocated
File Attributes: File, Archive
Size: 8814
Name: _ap.gif

Directory Entry Times:
Written:        Thu Oct 28 11:17:46 2004
```

```
Accessed:       Thu Oct 28 00:00:00 2004
Created:        Thu Oct 28 11:17:44 2004

Sectors:
2525 2526

Recovery:
2525 2526 2527 2528 2529 2530 2531 2532
2533 2534 2535 2536 2537 2538 2539 2540
2541 2542
```

```
$ istat -f fat16 USBFD-64531026-RL-001_part02.img 18
Directory Entry: 18
Allocated
File Attributes: File, Archive
Size: 19968
Name: coffee.doc

Directory Entry Times:
Written:        Thu Oct 28 19:24:48 2004
Accessed:       Thu Oct 28 00:00:00 2004
Created:        Thu Oct 28 19:24:46 2004

Sectors:
591 592 593 594 595 596 597 598
599 600 601 602 603 604 605 606
607 608 609 610 611 612 613 614
615 616 617 618 619 620 621 622
623 624 625 626 627 628 629 630
```

Output: filemon

```
880   4:16:42 PM  cmd.exe:856  QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS      Attributes: A
```

```
881   4:16:42 PM   cmd.exe:856  DIRECTORY    C:\Documents and
Settings\default\Desktop\SUCCESS      FileBothDirectoryInformation:
WinDump.exe

882   4:16:42 PM   cmd.exe:856  OPEN  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS      Options: Open  Access:
All

883   4:16:42 PM   cmd.exe:856  QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS      Attributes: A

884   4:16:42 PM   cmd.exe:856  QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS      Length: 450560

885   4:16:42 PM   cmd.exe:856  QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS      FileNameInformation

886   4:16:42 PM   cmd.exe:856  QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS      Attributes: A

887   4:16:42 PM   cmd.exe:856  DIRECTORY    C:\Documents and
Settings\default\Desktop\SUCCESS      FileBothDirectoryInformation:
WinDump.exe

888   4:16:42 PM   cmd.exe:856  OPEN  C:\Documents and
Settings\default\Desktop\WinDump.exe.Manifest     NOT FOUND    Options:
Open  Access: All

889   4:16:42 PM   cmd.exe:856  CLOSE C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS

890   4:16:42 PM   WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS      FileNameInformation

891   4:16:42 PM   WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS      FileNameInformation

892   4:16:42 PM   WinDump.exe:1912   OPEN
      C:\WINDOWS\Prefetch\WINDUMP.EXE-09422DA4.pf SUCCESS      Options:
Open  Access: All

893   4:16:42 PM   WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\Prefetch\WINDUMP.EXE-09422DA4.pf SUCCESS      Length:
39232

894   4:16:42 PM   WinDump.exe:1912   READ
      C:\WINDOWS\Prefetch\WINDUMP.EXE-09422DA4.pf SUCCESS      Offset: 0
Length: 39232

895   4:16:42 PM   WinDump.exe:1912   OPEN  C:    SUCCESS      Options:
Open  Access: All

896   4:16:42 PM   WinDump.exe:1912   QUERY INFORMATION  C:    SUCCESS
      FileFsVolumeInformation

897   4:16:42 PM   WinDump.exe:1912   OPEN  C:\   SUCCESS      Options:
Open Directory  Access: All
```

```
898   4:16:42 PM  WinDump.exe:1912  DIRECTORY   C:\   SUCCESS
      FileNamesInformation

899   4:16:42 PM  WinDump.exe:1912  DIRECTORY   C:\   NO MORE FILES
      FileNamesInformation

900   4:16:42 PM  WinDump.exe:1912  OPEN  C:\DOCUMENTS AND SETTINGS\
      SUCCESS     Options: Open Directory  Access: All

901   4:16:42 PM  WinDump.exe:1912  DIRECTORY   C:\DOCUMENTS AND
SETTINGS\   SUCCESS     FileNamesInformation

902   4:16:42 PM  WinDump.exe:1912  DIRECTORY   C:\DOCUMENTS AND
SETTINGS\   NO MORE FILES     FileNamesInformation

903   4:16:42 PM  WinDump.exe:1912  OPEN  C:\DOCUMENTS AND
SETTINGS\DEFAULT\  SUCCESS     Options: Open Directory  Access: All

904   4:16:42 PM  WinDump.exe:1912  DIRECTORY   C:\DOCUMENTS AND
SETTINGS\DEFAULT\  SUCCESS     FileNamesInformation

905   4:16:42 PM  WinDump.exe:1912  DIRECTORY   C:\DOCUMENTS AND
SETTINGS\DEFAULT\  NO MORE FILES     FileNamesInformation

906   4:16:42 PM  WinDump.exe:1912  OPEN  C:\DOCUMENTS AND
SETTINGS\DEFAULT\DESKTOP\SUCCESS     Options: Open Directory  Access: All

907   4:16:42 PM  WinDump.exe:1912  DIRECTORY   C:\DOCUMENTS AND
SETTINGS\DEFAULT\DESKTOP\SUCCESS     FileNamesInformation

908   4:16:42 PM  WinDump.exe:1912  DIRECTORY   C:\DOCUMENTS AND
SETTINGS\DEFAULT\DESKTOP\NO MORE FILES     FileNamesInformation

909   4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\  SUCCESS
      Options: Open Directory  Access: All

910   4:16:42 PM  WinDump.exe:1912  DIRECTORY   C:\WINDOWS\  SUCCESS
      FileNamesInformation

911   4:16:42 PM  WinDump.exe:1912  DIRECTORY   C:\WINDOWS\  SUCCESS
      FileNamesInformation

912   4:16:42 PM  WinDump.exe:1912  DIRECTORY   C:\WINDOWS\  NO MORE
FILES FileNamesInformation

913   4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\SYSTEM32\
      SUCCESS     Options: Open Directory  Access: All

914   4:16:42 PM  WinDump.exe:1912  DIRECTORY   C:\WINDOWS\SYSTEM32\
      SUCCESS     FileNamesInformation

915   4:16:42 PM  WinDump.exe:1912  DIRECTORY   C:\WINDOWS\SYSTEM32\
      SUCCESS     FileNamesInformation

916   4:16:42 PM  WinDump.exe:1912  DIRECTORY   C:\WINDOWS\SYSTEM32\
      SUCCESS     FileNamesInformation
```

```
917   4:16:42 PM  WinDump.exe:1912   DIRECTORY    C:\WINDOWS\SYSTEM32\
      SUCCESS     FileNamesInformation

918   4:16:42 PM  WinDump.exe:1912   DIRECTORY    C:\WINDOWS\SYSTEM32\
      SUCCESS     FileNamesInformation

919   4:16:42 PM  WinDump.exe:1912   DIRECTORY    C:\WINDOWS\SYSTEM32\
      NO MORE FILES      FileNamesInformation

920   4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\DRIVERS\
      SUCCESS     Options: Open Directory  Access: All

921   4:16:42 PM  WinDump.exe:1912   DIRECTORY
      C:\WINDOWS\SYSTEM32\DRIVERS\   SUCCESS     FileNamesInformation

922   4:16:42 PM  WinDump.exe:1912   DIRECTORY
      C:\WINDOWS\SYSTEM32\DRIVERS\   NO MORE FILES
      FileNamesInformation

923   4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\NPP\
      SUCCESS     Options: Open Directory  Access: All

924   4:16:42 PM  WinDump.exe:1912   DIRECTORY    C:\WINDOWS\SYSTEM32\NPP\
      SUCCESS     FileNamesInformation

925   4:16:42 PM  WinDump.exe:1912   DIRECTORY    C:\WINDOWS\SYSTEM32\NPP\
      NO MORE FILES      FileNamesInformation

926   4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\WINSXS\ SUCCESS
      Options: Open Directory  Access: All

927   4:16:42 PM  WinDump.exe:1912   DIRECTORY    C:\WINDOWS\WINSXS\
      SUCCESS     FileNamesInformation

928   4:16:42 PM  WinDump.exe:1912   DIRECTORY    C:\WINDOWS\WINSXS\ NO
MORE FILES   FileNamesInformation

929   4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\WINSXS\X86_MICROSOFT.WINDOWS.COMMON-
CONTROLS_6595B64144CCF1DF_6.0.0.0_X-WW_1382D70A\  SUCCESS      Options:
Open Directory  Access: All

930   4:16:42 PM  WinDump.exe:1912   DIRECTORY
      C:\WINDOWS\WINSXS\X86_MICROSOFT.WINDOWS.COMMON-
CONTROLS_6595B64144CCF1DF_6.0.0.0_X-WW_1382D70A\  SUCCESS
      FileNamesInformation

931   4:16:42 PM  WinDump.exe:1912   DIRECTORY
      C:\WINDOWS\WINSXS\X86_MICROSOFT.WINDOWS.COMMON-
CONTROLS_6595B64144CCF1DF_6.0.0.0_X-WW_1382D70A\  NO MORE FILES
      FileNamesInformation

932   4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\NTDLL.DLL
      SUCCESS     Options: Open  Access: All
```

```
933   4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\NTDLL.DLL  SUCCESS     Length: 651264

934   4:16:42 PM  WinDump.exe:1912  OPEN
      C:\WINDOWS\SYSTEM32\KERNEL32.DLL     SUCCESS     Options: Open
Access: All

935   4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\KERNEL32.DLL     SUCCESS     Length: 898048

936   4:16:42 PM  WinDump.exe:1912  OPEN  C:\DOCUMENTS AND
SETTINGS\DEFAULT\DESKTOP\WINDUMP.EXE  SUCCESS     Options: Open  Access:
All

937   4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION  C:\DOCUMENTS AND
SETTINGS\DEFAULT\DESKTOP\WINDUMP.EXE  SUCCESS     Length: 450560

938   4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\SYSTEM32\UNICODE.NLS
      SUCCESS     Options: Open  Access: All

939   4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\UNICODE.NLS SUCCESS     Length: 89588

940   4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\SYSTEM32\LOCALE.NLS
      SUCCESS     Options: Open  Access: All

941   4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\LOCALE.NLS  SUCCESS     Length: 209012

942   4:16:42 PM  WinDump.exe:1912  OPEN
      C:\WINDOWS\SYSTEM32\SORTTBLS.NLS     SUCCESS     Options: Open
Access: All

943   4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\SORTTBLS.NLS     SUCCESS     Length: 21116

944   4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\SYSTEM32\WSOCK32.DLL
      SUCCESS     Options: Open  Access: All

945   4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\WSOCK32.DLL SUCCESS     Length: 21504

946   4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\SYSTEM32\WS2_32.DLL
      SUCCESS     Options: Open  Access: All

947   4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\WS2_32.DLL  SUCCESS     Length: 75264

948   4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\SYSTEM32\MSVCRT.DLL
      SUCCESS     Options: Open  Access: All

949   4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\MSVCRT.DLL  SUCCESS     Length: 322560

950   4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\SYSTEM32\WS2HELP.DLL
      SUCCESS     Options: Open  Access: All
```

```
951   4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\WS2HELP.DLL SUCCESS     Length: 18944

952   4:16:42 PM  WinDump.exe:1912  OPEN
      C:\WINDOWS\SYSTEM32\ADVAPI32.DLL     SUCCESS     Options: Open
Access: All

953   4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\ADVAPI32.DLL     SUCCESS     Length: 549888

954   4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\SYSTEM32\RPCRT4.DLL
      SUCCESS     Options: Open  Access: All

955   4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\RPCRT4.DLL SUCCESS     Length: 442880

956   4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\SYSTEM32\WPCAP.DLL
      SUCCESS     Options: Open  Access: All

957   4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\WPCAP.DLL  SUCCESS     Length: 225280

958   4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\SYSTEM32\PACKET.DLL
      SUCCESS     Options: Open  Access: All

959   4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\PACKET.DLL SUCCESS     Length: 81920

960   4:16:42 PM  WinDump.exe:1912  OPEN
      C:\WINDOWS\SYSTEM32\WANPACKET.DLL    SUCCESS     Options: Open
Access: All

961   4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\WANPACKET.DLL    SUCCESS     Length: 61440

962   4:16:42 PM  WinDump.exe:1912  OPEN
      C:\WINDOWS\SYSTEM32\NPPTOOLS.DLL     SUCCESS     Options: Open
Access: All

963   4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\NPPTOOLS.DLL     SUCCESS     Length: 49152

964   4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\SYSTEM32\MFC42U.DLL
      SUCCESS     Options: Open  Access: All

965   4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\MFC42U.DLL SUCCESS     Length: 995384

966   4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\SYSTEM32\GDI32.DLL
      SUCCESS     Options: Open  Access: All

967   4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\GDI32.DLL  SUCCESS     Length: 241664

968   4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\SYSTEM32\USER32.DLL
      SUCCESS     Options: Open  Access: All
```

```
969   4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\USER32.DLL SUCCESS     Length: 528896

970   4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\SYSTEM32\OLE32.DLL
      SUCCESS     Options: Open  Access: All

971   4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\OLE32.DLL  SUCCESS     Length: 1105408

972   4:16:42 PM  WinDump.exe:1912  OPEN
      C:\WINDOWS\SYSTEM32\OLEAUT32.DLL     SUCCESS     Options: Open
Access: All

973   4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\OLEAUT32.DLL     SUCCESS     Length: 569344

974   4:16:42 PM  WinDump.exe:1912  OPEN
      C:\WINDOWS\SYSTEM32\IPHLPAPI.DLL     SUCCESS     Options: Open
Access: All

975   4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\IPHLPAPI.DLL     SUCCESS     Length: 77312

976   4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\SYSTEM32\NETMAN.DLL
      SUCCESS     Options: Open  Access: All

977   4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\NETMAN.DLL SUCCESS     Length: 147968

978   4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\SYSTEM32\MPRAPI.DLL
      SUCCESS     Options: Open  Access: All

979   4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\MPRAPI.DLL SUCCESS     Length: 79360

980   4:16:42 PM  WinDump.exe:1912  OPEN
      C:\WINDOWS\SYSTEM32\ACTIVEDS.DLL     SUCCESS     Options: Open
Access: All

981   4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\ACTIVEDS.DLL     SUCCESS     Length: 181760

982   4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\SYSTEM32\ADSLDPC.DLL
      SUCCESS     Options: Open  Access: All

983   4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\ADSLDPC.DLL SUCCESS     Length: 139264

984   4:16:42 PM  WinDump.exe:1912  OPEN
      C:\WINDOWS\SYSTEM32\NETAPI32.DLL     SUCCESS     Options: Open
Access: All

985   4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\NETAPI32.DLL     SUCCESS     Length: 301568

986   4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\SYSTEM32\WLDAP32.DLL
      SUCCESS     Options: Open  Access: All
```

```
987   4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\WLDAP32.DLL SUCCESS     Length: 167936

988   4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\ATL.DLL
      SUCCESS     Options: Open  Access: All

989   4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\ATL.DLL     SUCCESS     Length: 74802

990   4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\RTUTILS.DLL
      SUCCESS     Options: Open  Access: All

991   4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\RTUTILS.DLL SUCCESS     Length: 39936

992   4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\SAMLIB.DLL
      SUCCESS     Options: Open  Access: All

993   4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\SAMLIB.DLL  SUCCESS     Length: 54784

994   4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\SYSTEM32\SETUPAPI.DLL      SUCCESS     Options: Open
Access: All

995   4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\SETUPAPI.DLL      SUCCESS     Length: 922624

996   4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\SYSTEM32\RASAPI32.DLL      SUCCESS     Options: Open
Access: All

997   4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\RASAPI32.DLL      SUCCESS     Length: 218112

998   4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\RASMAN.DLL
      SUCCESS     Options: Open  Access: All

999   4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\RASMAN.DLL  SUCCESS     Length: 55808

1000  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\TAPI32.DLL
      SUCCESS     Options: Open  Access: All

1001  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\TAPI32.DLL  SUCCESS     Length: 163328

1002  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\SHLWAPI.DLL
      SUCCESS     Options: Open  Access: All

1003  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\SHLWAPI.DLL SUCCESS     Length: 393728

1004  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\WINMM.DLL
      SUCCESS     Options: Open  Access: All
```

```
1005  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\WINMM.DLL  SUCCESS     Length: 170496

1006  4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\SYSTEM32\SHELL32.DLL
      SUCCESS     Options: Open  Access: All

1007  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\SHELL32.DLL SUCCESS     Length: 8227840

1008  4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\SYSTEM32\SECUR32.DLL
      SUCCESS     Options: Open  Access: All

1009  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\SECUR32.DLL SUCCESS     Length: 52224

1010  4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\SYSTEM32\WZCSVC.DLL
      SUCCESS     Options: Open  Access: All

1011  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\WZCSVC.DLL SUCCESS     Length: 184320

1012  4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\SYSTEM32\WMI.DLL
      SUCCESS     Options: Open  Access: All

1013  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\WMI.DLL    SUCCESS     Length: 5632

1014  4:16:42 PM  WinDump.exe:1912  OPEN
      C:\WINDOWS\SYSTEM32\DHCPCSVC.DLL     SUCCESS     Options: Open
Access: All

1015  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\DHCPCSVC.DLL     SUCCESS     Length: 98816

1016  4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\SYSTEM32\DNSAPI.DLL
      SUCCESS     Options: Open  Access: All

1017  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\DNSAPI.DLL SUCCESS     Length: 139264

1018  4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\SYSTEM32\CRYPT32.DLL
      SUCCESS     Options: Open  Access: All

1019  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\CRYPT32.DLL SUCCESS     Length: 544256

1020  4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\SYSTEM32\MSASN1.DLL
      SUCCESS     Options: Open  Access: All

1021  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\MSASN1.DLL SUCCESS     Length: 51712

1022  4:16:42 PM  WinDump.exe:1912  OPEN
      C:\WINDOWS\SYSTEM32\WTSAPI32.DLL     SUCCESS     Options: Open
Access: All
```

```
1023  4:16:42 PM   WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\WTSAPI32.DLL      SUCCESS      Length: 16896

1024  4:16:42 PM   WinDump.exe:1912   OPEN   C:\WINDOWS\SYSTEM32\WINSTA.DLL
      SUCCESS      Options: Open  Access: All

1025  4:16:42 PM   WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\WINSTA.DLL  SUCCESS      Length: 47104

1026  4:16:42 PM   WinDump.exe:1912   OPEN   C:\WINDOWS\SYSTEM32\VERSION.DLL
      SUCCESS      Options: Open  Access: All

1027  4:16:42 PM   WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\VERSION.DLL SUCCESS      Length: 16384

1028  4:16:42 PM   WinDump.exe:1912   OPEN   C:\WINDOWS\SYSTEM32\CTYPE.NLS
      SUCCESS      Options: Open  Access: All

1029  4:16:42 PM   WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\CTYPE.NLS   SUCCESS      Length: 8386

1030  4:16:42 PM   WinDump.exe:1912   OPEN
      C:\WINDOWS\SYSTEM32\MFC42LOC.DLL      SUCCESS      Options: Open
Access: All

1031  4:16:42 PM   WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\MFC42LOC.DLL      SUCCESS      Length: 53248

1032  4:16:42 PM   WinDump.exe:1912   OPEN   C:\WINDOWS\SYSTEM32\SORTKEY.NLS
      SUCCESS      Options: Open  Access: All

1033  4:16:42 PM   WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\SORTKEY.NLS SUCCESS      Length: 262148

1034  4:16:42 PM   WinDump.exe:1912   OPEN
      C:\WINDOWS\WINSXS\X86_MICROSOFT.WINDOWS.COMMON-
CONTROLS_6595B64144CCF1DF_6.0.0.0_X-WW_1382D70A\COMCTL32.DLL   SUCCESS
      Options: Open  Access: All

1035  4:16:42 PM   WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\WINSXS\X86_MICROSOFT.WINDOWS.COMMON-
CONTROLS_6595B64144CCF1DF_6.0.0.0_X-WW_1382D70A\COMCTL32.DLL   SUCCESS
      Length: 921088

1036  4:16:42 PM   WinDump.exe:1912   OPEN
      C:\WINDOWS\WINDOWSSHELL.MANIFEST      SUCCESS      Options: Open
Access: All

1037  4:16:42 PM   WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\WINDOWSSHELL.MANIFEST      SUCCESS      Length: 749

1038  4:16:42 PM   WinDump.exe:1912   OPEN
      C:\WINDOWS\SYSTEM32\COMCTL32.DLL      SUCCESS      Options: Open
Access: All

1039  4:16:42 PM   WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\COMCTL32.DLL      SUCCESS      Length: 557568
```

```
1040  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\SYSTEM32\DRIVERS\NPF.SYS   SUCCESS     Options: Open
Access: All

1041  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\DRIVERS\NPF.SYS   SUCCESS     Length: 32896

1042  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\SYSTEM32\NPP\NDISNPP.DLL   SUCCESS     Options: Open
Access: All

1043  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\SYSTEM32\NPP\NDISNPP.DLL   SUCCESS     Length: 55808

1044  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\NTDLL.DLL
      SUCCESS     Options: Open  Access: Execute

1045  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\SYSTEM32\KERNEL32.DLL      SUCCESS     Options: Open
Access: Execute

1046  4:16:42 PM  WinDump.exe:1912   OPEN  C:\DOCUMENTS AND
SETTINGS\DEFAULT\DESKTOP\WINDUMP.EXE  SUCCESS     Options: Open  Access:
Execute

1047  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\WSOCK32.DLL
      SUCCESS     Options: Open  Access: Execute

1048  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\WS2_32.DLL
      SUCCESS     Options: Open  Access: Execute

1049  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\MSVCRT.DLL
      SUCCESS     Options: Open  Access: Execute

1050  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\WS2HELP.DLL
      SUCCESS     Options: Open  Access: Execute

1051  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\SYSTEM32\ADVAPI32.DLL      SUCCESS     Options: Open
Access: Execute

1052  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\RPCRT4.DLL
      SUCCESS     Options: Open  Access: Execute

1053  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\WPCAP.DLL
      SUCCESS     Options: Open  Access: Execute

1054  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\PACKET.DLL
      SUCCESS     Options: Open  Access: Execute

1055  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\SYSTEM32\WANPACKET.DLL     SUCCESS     Options: Open
Access: Execute
```

```
1056  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\SYSTEM32\NPPTOOLS.DLL      SUCCESS      Options: Open
Access: Execute

1057  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\MFC42U.DLL
      SUCCESS      Options: Open  Access: Execute

1058  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\GDI32.DLL
      SUCCESS      Options: Open  Access: Execute

1059  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\USER32.DLL
      SUCCESS      Options: Open  Access: Execute

1060  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\OLE32.DLL
      SUCCESS      Options: Open  Access: Execute

1061  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\SYSTEM32\OLEAUT32.DLL      SUCCESS      Options: Open
Access: Execute

1062  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\SYSTEM32\IPHLPAPI.DLL      SUCCESS      Options: Open
Access: Execute

1063  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\NETMAN.DLL
      SUCCESS      Options: Open  Access: Execute

1064  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\MPRAPI.DLL
      SUCCESS      Options: Open  Access: Execute

1065  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\SYSTEM32\ACTIVEDS.DLL      SUCCESS      Options: Open
Access: Execute

1066  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\ADSLDPC.DLL
      SUCCESS      Options: Open  Access: Execute

1067  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\SYSTEM32\NETAPI32.DLL      SUCCESS      Options: Open
Access: Execute

1068  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\WLDAP32.DLL
      SUCCESS      Options: Open  Access: Execute

1069  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\ATL.DLL
      SUCCESS      Options: Open  Access: Execute

1070  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\RTUTILS.DLL
      SUCCESS      Options: Open  Access: Execute

1071  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\SAMLIB.DLL
      SUCCESS      Options: Open  Access: Execute

1072  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\SYSTEM32\SETUPAPI.DLL      SUCCESS      Options: Open
Access: Execute
```

```
1073  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\SYSTEM32\RASAPI32.DLL      SUCCESS      Options: Open
Access: Execute

1074  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\RASMAN.DLL
      SUCCESS      Options: Open  Access: Execute

1075  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\TAPI32.DLL
      SUCCESS      Options: Open  Access: Execute

1076  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\SHLWAPI.DLL
      SUCCESS      Options: Open  Access: Execute

1077  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\WINMM.DLL
      SUCCESS      Options: Open  Access: Execute

1078  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\SHELL32.DLL
      SUCCESS      Options: Open  Access: Execute

1079  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\SECUR32.DLL
      SUCCESS      Options: Open  Access: Execute

1080  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\WZCSVC.DLL
      SUCCESS      Options: Open  Access: Execute

1081  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\WMI.DLL
      SUCCESS      Options: Open  Access: Execute

1082  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\SYSTEM32\DHCPCSVC.DLL      SUCCESS      Options: Open
Access: Execute

1083  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\DNSAPI.DLL
      SUCCESS      Options: Open  Access: Execute

1084  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\CRYPT32.DLL
      SUCCESS      Options: Open  Access: Execute

1085  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\MSASN1.DLL
      SUCCESS      Options: Open  Access: Execute

1086  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\SYSTEM32\WTSAPI32.DLL      SUCCESS      Options: Open
Access: Execute

1087  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\WINSTA.DLL
      SUCCESS      Options: Open  Access: Execute

1088  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\SYSTEM32\VERSION.DLL
      SUCCESS      Options: Open  Access: Execute

1089  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\SYSTEM32\MFC42LOC.DLL      SUCCESS      Options: Open
Access: Execute

1090  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\WINSXS\X86_MICROSOFT.WINDOWS.COMMON-
```

```
CONTROLS_6595B64144CCF1DF_6.0.0.0_X-WW_1382D70A\COMCTL32.DLL   SUCCESS
      Options: Open  Access: Execute

1091  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\SYSTEM32\COMCTL32.DLL      SUCCESS      Options: Open
Access: Execute

1092  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\SYSTEM32\DRIVERS\NPF.SYS   SUCCESS      Options: Open
Access: Execute

1093  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\SYSTEM32\NPP\NDISNPP.DLL   SUCCESS      Options: Open
Access: Execute

1094  4:16:42 PM  WinDump.exe:1912   OPEN  C:\Documents and
Settings\default\Desktop SUCCESS      Options: Open Directory  Access:
Traverse

1095  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WinDump.exe.Local  NOT FOUND   Attributes: Error

1096  4:16:42 PM  vsmon.exe:1432     OPEN  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS      Options: Open  Access:
All

1097  4:16:42 PM  vsmon.exe:1432     CLOSE C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS

1098  4:16:42 PM  vsmon.exe:1432     OPEN  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS      Options: Open  Access:
All

1099  4:16:42 PM  vsmon.exe:1432     QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS      Attributes: A

1100  4:16:42 PM  vsmon.exe:1432     SET INFORMATION    C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS      FileBasicInformation

1101  4:16:42 PM  vsmon.exe:1432     READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS      Offset: 0 Length: 64

1102  4:16:42 PM  vsmon.exe:1432     READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS      Offset: 224 Length: 64

1103  4:16:42 PM  vsmon.exe:1432     READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS      Offset: 296 Length: 4

1104  4:16:42 PM  vsmon.exe:1432     READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS      Offset: 316 Length: 4

1105  4:16:42 PM  vsmon.exe:1432     CLOSE C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS

1106  4:16:42 PM  vsmon.exe:1432     OPEN  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS      Options: Open  Access:
All
```

```
1107  4:16:42 PM  vsmon.exe:1432     CLOSE C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS

1108  4:16:42 PM  vsmon.exe:1432     QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Attributes: A

1109  4:16:42 PM  vsmon.exe:1432     OPEN  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Options: Open  Access:
Execute

1110  4:16:42 PM  vsmon.exe:1432     QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Length: 450560

1111  4:16:42 PM  vsmon.exe:1432     CLOSE C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS

1112  4:16:42 PM  vsmon.exe:1432     QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Attributes: A

1113  4:16:42 PM  vsmon.exe:1432     OPEN  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Options: Open  Access:
All

1114  4:16:42 PM  vsmon.exe:1432     QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Length: 450560

1115  4:16:42 PM  vsmon.exe:1432     CLOSE C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS

1116  4:16:42 PM  vsmon.exe:1432     OPEN  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Options: Open Sequential
Access: All

1117  4:16:42 PM  vsmon.exe:1432     QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Length: 450560

1118  4:16:42 PM  vsmon.exe:1432     QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Length: 450560

1119  4:16:42 PM  vsmon.exe:1432     READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Offset: 0 Length: 32768

1120  4:16:42 PM  vsmon.exe:1432     READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Offset: 32768 Length:
32768

1121  4:16:42 PM  vsmon.exe:1432     READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Offset: 65536 Length:
32768

1122  4:16:42 PM  vsmon.exe:1432     READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Offset: 98304 Length:
32768
```

```
1123  4:16:42 PM  vsmon.exe:1432    READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Offset: 131072 Length:
32768

1124  4:16:42 PM  vsmon.exe:1432    READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Offset: 163840 Length:
32768

1125  4:16:42 PM  vsmon.exe:1432    READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Offset: 196608 Length:
32768

1126  4:16:42 PM  vsmon.exe:1432    READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Offset: 229376 Length:
32768

1127  4:16:42 PM  vsmon.exe:1432    READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Offset: 262144 Length:
32768

1128  4:16:42 PM  vsmon.exe:1432    READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Offset: 294912 Length:
32768

1129  4:16:42 PM  vsmon.exe:1432    READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Offset: 327680 Length:
32768

1130  4:16:42 PM  vsmon.exe:1432    READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Offset: 360448 Length:
32768

1131  4:16:42 PM  vsmon.exe:1432    READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Offset: 393216 Length:
32768

1132  4:16:42 PM  vsmon.exe:1432    READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Offset: 425984 Length:
32768

1133  4:16:42 PM  vsmon.exe:1432    CLOSE C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS

1134  4:16:42 PM  vsmon.exe:1432    OPEN  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Options: Open  Access:
All

1135  4:16:42 PM  vsmon.exe:1432    READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Offset: 0 Length: 32768

1136  4:16:42 PM  vsmon.exe:1432    READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Offset: 32768 Length:
32768

1137  4:16:42 PM  vsmon.exe:1432    READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Offset: 65536 Length:
32768
```

```
1138  4:16:42 PM  vsmon.exe:1432     READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Offset: 98304 Length:
32768

1139  4:16:42 PM  vsmon.exe:1432     READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Offset: 131072 Length:
32768

1140  4:16:42 PM  vsmon.exe:1432     READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Offset: 163840 Length:
32768

1141  4:16:42 PM  vsmon.exe:1432     READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Offset: 196608 Length:
32768

1142  4:16:42 PM  vsmon.exe:1432     READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Offset: 229376 Length:
32768

1143  4:16:42 PM  vsmon.exe:1432     READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Offset: 262144 Length:
32768

1144  4:16:42 PM  vsmon.exe:1432     READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Offset: 294912 Length:
32768

1145  4:16:42 PM  vsmon.exe:1432     READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Offset: 327680 Length:
32768

1146  4:16:42 PM  vsmon.exe:1432     READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Offset: 360448 Length:
32768

1147  4:16:42 PM  vsmon.exe:1432     READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Offset: 393216 Length:
32768

1148  4:16:42 PM  vsmon.exe:1432     READ  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Offset: 425984 Length:
32768

1149  4:16:42 PM  vsmon.exe:1432     CLOSE C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS

1150  4:16:42 PM  vsmon.exe:1432     DIRECTORY   C:\Documents and
Settings\default\Desktop\SUCCESS     FileBothDirectoryInformation:
WinDump.exe

1151  4:16:42 PM  vsmon.exe:1432     OPEN  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Options: Open  Access:
All
```

```
1152  4:16:42 PM  vsmon.exe:1432     QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Length: 450560

1153  4:16:42 PM  vsmon.exe:1432     QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     Length: 450560

1154  4:16:42 PM  vsmon.exe:1432     CLOSE C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS

1155  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WSOCK32.dll  NOT FOUND   Attributes: Error

1156  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WSOCK32.dll  NOT FOUND   Attributes: Error

1157  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\WSOCK32.dll SUCCESS     Attributes: A

1158  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\System32\WSOCK32.dll
      SUCCESS     Options: Open  Access: Execute

1159  4:16:42 PM  WinDump.exe:1912   CLOSE C:\WINDOWS\System32\WSOCK32.dll
      SUCCESS

1160  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WS2_32.dll   NOT FOUND   Attributes: Error

1161  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WS2_32.dll   NOT FOUND   Attributes: Error

1162  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\WS2_32.dll  SUCCESS     Attributes: A

1163  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\System32\WS2_32.dll
      SUCCESS     Options: Open  Access: Execute

1164  4:16:42 PM  WinDump.exe:1912   CLOSE C:\WINDOWS\System32\WS2_32.dll
      SUCCESS

1165  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WS2HELP.dll  NOT FOUND   Attributes: Error

1166  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WS2HELP.dll  NOT FOUND   Attributes: Error

1167  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\WS2HELP.dll SUCCESS     Attributes: A

1168  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\System32\WS2HELP.dll
      SUCCESS     Options: Open  Access: Execute

1169  4:16:42 PM  WinDump.exe:1912   CLOSE C:\WINDOWS\System32\WS2HELP.dll
      SUCCESS

1170  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\wpcap.dll    NOT FOUND   Attributes: Error
```

```
1171  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\wpcap.dll    NOT FOUND    Attributes: Error

1172  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\wpcap.dll   SUCCESS      Attributes: A

1173  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\System32\wpcap.dll
      SUCCESS      Options: Open  Access: Execute

1174  4:16:42 PM  WinDump.exe:1912   CLOSE C:\WINDOWS\System32\wpcap.dll
      SUCCESS

1175  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\packet.dll   NOT FOUND    Attributes: Error

1176  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\packet.dll   NOT FOUND    Attributes: Error

1177  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\packet.dll  SUCCESS      Attributes: A

1178  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\System32\packet.dll
      SUCCESS      Options: Open  Access: Execute

1179  4:16:42 PM  WinDump.exe:1912   CLOSE C:\WINDOWS\System32\packet.dll
      SUCCESS

1180  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WanPacket.dll      NOT FOUND    Attributes: Error

1181  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WanPacket.dll      NOT FOUND    Attributes: Error

1182  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\WanPacket.dll     SUCCESS      Attributes: A

1183  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\System32\WanPacket.dll     SUCCESS      Options: Open
Access: Execute

1184  4:16:42 PM  WinDump.exe:1912   CLOSE
      C:\WINDOWS\System32\WanPacket.dll     SUCCESS

1185  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\NPPTools.dll NOT FOUND    Attributes: Error

1186  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\NPPTools.dll NOT FOUND    Attributes: Error

1187  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\NPPTools.dll      SUCCESS      Attributes: A

1188  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\System32\NPPTools.dll      SUCCESS      Options: Open
Access: Execute
```

```
1189  4:16:42 PM   WinDump.exe:1912   CLOSE
      C:\WINDOWS\System32\NPPTools.dll      SUCCESS

1190  4:16:42 PM   WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\MFC42u.DLL   NOT FOUND    Attributes: Error

1191  4:16:42 PM   WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\MFC42u.DLL   NOT FOUND    Attributes: Error

1192  4:16:42 PM   WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\MFC42u.DLL SUCCESS      Attributes: A

1193  4:16:42 PM   WinDump.exe:1912   OPEN  C:\WINDOWS\System32\MFC42u.DLL
      SUCCESS      Options: Open  Access: Execute

1194  4:16:42 PM   WinDump.exe:1912   CLOSE C:\WINDOWS\System32\MFC42u.DLL
      SUCCESS

1195  4:16:42 PM   WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\iphlpapi.dll NOT FOUND    Attributes: Error

1196  4:16:42 PM   WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\iphlpapi.dll NOT FOUND    Attributes: Error

1197  4:16:42 PM   WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\iphlpapi.dll      SUCCESS      Attributes: A

1198  4:16:42 PM   WinDump.exe:1912   OPEN
      C:\WINDOWS\System32\iphlpapi.dll      SUCCESS      Options: Open
Access: Execute

1199  4:16:42 PM   WinDump.exe:1912   CLOSE
      C:\WINDOWS\System32\iphlpapi.dll      SUCCESS

1200  4:16:42 PM   WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\netman.dll   NOT FOUND    Attributes: Error

1201  4:16:42 PM   WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\netman.dll   NOT FOUND    Attributes: Error

1202  4:16:42 PM   WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\netman.dll SUCCESS      Attributes: A

1203  4:16:42 PM   WinDump.exe:1912   OPEN  C:\WINDOWS\System32\netman.dll
      SUCCESS      Options: Open  Access: Execute

1204  4:16:42 PM   WinDump.exe:1912   CLOSE C:\WINDOWS\System32\netman.dll
      SUCCESS

1205  4:16:42 PM   WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\MPRAPI.dll   NOT FOUND    Attributes: Error

1206  4:16:42 PM   WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\MPRAPI.dll   NOT FOUND    Attributes: Error

1207  4:16:42 PM   WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\MPRAPI.dll SUCCESS      Attributes: A
```

```
1208  4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\System32\MPRAPI.dll
      SUCCESS     Options: Open  Access: Execute

1209  4:16:42 PM  WinDump.exe:1912  CLOSE C:\WINDOWS\System32\MPRAPI.dll
      SUCCESS

1210  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\ACTIVEDS.dll NOT FOUND   Attributes: Error

1211  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\ACTIVEDS.dll NOT FOUND   Attributes: Error

1212  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\System32\ACTIVEDS.dll      SUCCESS     Attributes: A

1213  4:16:42 PM  WinDump.exe:1912  OPEN
      C:\WINDOWS\System32\ACTIVEDS.dll      SUCCESS     Options: Open
Access: Execute

1214  4:16:42 PM  WinDump.exe:1912  CLOSE
      C:\WINDOWS\System32\ACTIVEDS.dll      SUCCESS

1215  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\adsldpc.dll  NOT FOUND   Attributes: Error

1216  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\adsldpc.dll  NOT FOUND   Attributes: Error

1217  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\System32\adsldpc.dll SUCCESS     Attributes: A

1218  4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\System32\adsldpc.dll
      SUCCESS     Options: Open  Access: Execute

1219  4:16:42 PM  WinDump.exe:1912  CLOSE C:\WINDOWS\System32\adsldpc.dll
      SUCCESS

1220  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\NETAPI32.dll NOT FOUND   Attributes: Error

1221  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\NETAPI32.dll NOT FOUND   Attributes: Error

1222  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\System32\NETAPI32.dll      SUCCESS     Attributes: A

1223  4:16:42 PM  WinDump.exe:1912  OPEN
      C:\WINDOWS\System32\NETAPI32.dll      SUCCESS     Options: Open
Access: Execute

1224  4:16:42 PM  WinDump.exe:1912  CLOSE
      C:\WINDOWS\System32\NETAPI32.dll      SUCCESS

1225  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\ATL.DLL      NOT FOUND   Attributes: Error
```

```
1226  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\ATL.DLL      NOT FOUND   Attributes: Error

1227  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\ATL.DLL     SUCCESS     Attributes: A

1228  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\System32\ATL.DLL
      SUCCESS     Options: Open  Access: Execute

1229  4:16:42 PM  WinDump.exe:1912   CLOSE C:\WINDOWS\System32\ATL.DLL
      SUCCESS

1230  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\rtutils.dll  NOT FOUND   Attributes: Error

1231  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\rtutils.dll  NOT FOUND   Attributes: Error

1232  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\rtutils.dll SUCCESS     Attributes: A

1233  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\System32\rtutils.dll
      SUCCESS     Options: Open  Access: Execute

1234  4:16:42 PM  WinDump.exe:1912   CLOSE C:\WINDOWS\System32\rtutils.dll
      SUCCESS

1235  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\SAMLIB.dll   NOT FOUND   Attributes: Error

1236  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\SAMLIB.dll   NOT FOUND   Attributes: Error

1237  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\SAMLIB.dll  SUCCESS     Attributes: A

1238  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\System32\SAMLIB.dll
      SUCCESS     Options: Open  Access: Execute

1239  4:16:42 PM  WinDump.exe:1912   CLOSE C:\WINDOWS\System32\SAMLIB.dll
      SUCCESS

1240  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\SETUPAPI.dll NOT FOUND   Attributes: Error

1241  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\SETUPAPI.dll NOT FOUND   Attributes: Error

1242  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\SETUPAPI.dll      SUCCESS     Attributes: A

1243  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\System32\SETUPAPI.dll      SUCCESS     Options: Open
Access: Execute

1244  4:16:42 PM  WinDump.exe:1912   CLOSE
      C:\WINDOWS\System32\SETUPAPI.dll      SUCCESS
```

```
1245  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\RASAPI32.dll NOT FOUND   Attributes: Error

1246  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\RASAPI32.dll NOT FOUND   Attributes: Error

1247  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\System32\RASAPI32.dll     SUCCESS     Attributes: A

1248  4:16:42 PM  WinDump.exe:1912  OPEN
      C:\WINDOWS\System32\RASAPI32.dll     SUCCESS     Options: Open
Access: Execute

1249  4:16:42 PM  WinDump.exe:1912  CLOSE
      C:\WINDOWS\System32\RASAPI32.dll     SUCCESS

1250  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\rasman.dll  NOT FOUND   Attributes: Error

1251  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\rasman.dll  NOT FOUND   Attributes: Error

1252  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\System32\rasman.dll SUCCESS     Attributes: A

1253  4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\System32\rasman.dll
      SUCCESS     Options: Open  Access: Execute

1254  4:16:42 PM  WinDump.exe:1912  CLOSE C:\WINDOWS\System32\rasman.dll
      SUCCESS

1255  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\TAPI32.dll  NOT FOUND   Attributes: Error

1256  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\TAPI32.dll  NOT FOUND   Attributes: Error

1257  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\System32\TAPI32.dll SUCCESS     Attributes: A

1258  4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\System32\TAPI32.dll
      SUCCESS     Options: Open  Access: Execute

1259  4:16:42 PM  WinDump.exe:1912  CLOSE C:\WINDOWS\System32\TAPI32.dll
      SUCCESS

1260  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WINMM.dll   NOT FOUND   Attributes: Error

1261  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WINMM.dll   NOT FOUND   Attributes: Error

1262  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\System32\WINMM.dll  SUCCESS     Attributes: A
```

```
1263  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\System32\WINMM.dll
      SUCCESS     Options: Open  Access: Execute

1264  4:16:42 PM  WinDump.exe:1912   CLOSE C:\WINDOWS\System32\WINMM.dll
      SUCCESS

1265  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\Secur32.dll  NOT FOUND   Attributes: Error

1266  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\Secur32.dll  NOT FOUND   Attributes: Error

1267  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\Secur32.dll SUCCESS     Attributes: A

1268  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\System32\Secur32.dll
      SUCCESS     Options: Open  Access: Execute

1269  4:16:42 PM  WinDump.exe:1912   CLOSE C:\WINDOWS\System32\Secur32.dll
      SUCCESS

1270  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WZCSvc.DLL   NOT FOUND   Attributes: Error

1271  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WZCSvc.DLL   NOT FOUND   Attributes: Error

1272  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\WZCSvc.DLL  SUCCESS     Attributes: A

1273  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\System32\WZCSvc.DLL
      SUCCESS     Options: Open  Access: Execute

1274  4:16:42 PM  WinDump.exe:1912   CLOSE C:\WINDOWS\System32\WZCSvc.DLL
      SUCCESS

1275  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WMI.dll      NOT FOUND   Attributes: Error

1276  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WMI.dll      NOT FOUND   Attributes: Error

1277  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\WMI.dll     SUCCESS     Attributes: A

1278  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\System32\WMI.dll
      SUCCESS     Options: Open  Access: Execute

1279  4:16:42 PM  WinDump.exe:1912   CLOSE C:\WINDOWS\System32\WMI.dll
      SUCCESS

1280  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\DHCPCSVC.DLL NOT FOUND   Attributes: Error

1281  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\DHCPCSVC.DLL NOT FOUND   Attributes: Error
```

```
1282  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\DHCPCSVC.DLL     SUCCESS     Attributes: A

1283  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\System32\DHCPCSVC.DLL     SUCCESS     Options: Open
Access: Execute

1284  4:16:42 PM  WinDump.exe:1912   CLOSE
      C:\WINDOWS\System32\DHCPCSVC.DLL     SUCCESS

1285  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\DNSAPI.dll   NOT FOUND   Attributes: Error

1286  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\DNSAPI.dll   NOT FOUND   Attributes: Error

1287  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\DNSAPI.dll  SUCCESS     Attributes: A

1288  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\System32\DNSAPI.dll
      SUCCESS     Options: Open  Access: Execute

1289  4:16:42 PM  WinDump.exe:1912   CLOSE C:\WINDOWS\System32\DNSAPI.dll
      SUCCESS

1290  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WTSAPI32.dll NOT FOUND   Attributes: Error

1291  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WTSAPI32.dll NOT FOUND   Attributes: Error

1292  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\WTSAPI32.dll     SUCCESS     Attributes: A

1293  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\System32\WTSAPI32.dll     SUCCESS     Options: Open
Access: Execute

1294  4:16:42 PM  WinDump.exe:1912   CLOSE
      C:\WINDOWS\System32\WTSAPI32.dll     SUCCESS

1295  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WINSTA.dll   NOT FOUND   Attributes: Error

1296  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WINSTA.dll   NOT FOUND   Attributes: Error

1297  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\WINSTA.dll  SUCCESS     Attributes: A

1298  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\System32\WINSTA.dll
      SUCCESS     Options: Open  Access: Execute

1299  4:16:42 PM  WinDump.exe:1912   CLOSE C:\WINDOWS\System32\WINSTA.dll
      SUCCESS
```

```
1300  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\System32\MFC42LOC.DLL     SUCCESS     Attributes: A

1301  4:16:42 PM  WinDump.exe:1912  OPEN
      C:\WINDOWS\System32\MFC42LOC.DLL     SUCCESS     Options: Open
Access: Execute

1302  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\System32\MFC42LOC.DLL     SUCCESS     Length: 53248

1303  4:16:42 PM  WinDump.exe:1912  CLOSE
      C:\WINDOWS\System32\MFC42LOC.DLL     SUCCESS

1304  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\System32\MFC42LOC.DLL     SUCCESS     Attributes: A

1305  4:16:42 PM  WinDump.exe:1912  OPEN
      C:\WINDOWS\System32\MFC42LOC.DLL     SUCCESS     Options: Open
Access: Execute

1306  4:16:42 PM  WinDump.exe:1912  CLOSE
      C:\WINDOWS\System32\MFC42LOC.DLL     SUCCESS

1307  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WinDump.exe  BUFFER OVERFLOW
      FileNameInformation

1308  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WinDump.exe  SUCCESS     FileNameInformation

1309  4:16:42 PM  WinDump.exe:1912  SET INFORMATION
      C:\WINDOWS\SYSTEM32\config\software.LOG     SUCCESS     Length:
12288

1310  4:16:42 PM  WinDump.exe:1912  SET INFORMATION
      C:\WINDOWS\SYSTEM32\config\software.LOG     SUCCESS     Length:
12288

1311  4:16:42 PM  WinDump.exe:1912  SET INFORMATION
      C:\WINDOWS\SYSTEM32\config\software.LOG     SUCCESS     Length:
20480

1312  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION  C:\WINDOWS\
      SUCCESS     Attributes: D

1313  4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\System32\TAPI32.dll
      SUCCESS     Options: Open  Access: All

1314  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\System32\TAPI32.dll  SUCCESS     Length: 163328

1315  4:16:42 PM  WinDump.exe:1912  OPEN
      C:\WINDOWS\System32\TAPI32.dll.124.Manifest NOT FOUND   Options:
Open  Access: All
```

```
1316  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\System32\TAPI32.dll.124.Config   NOT FOUND    Options:
Open  Access: All

1317  4:16:42 PM  WinDump.exe:1912   CLOSE C:\WINDOWS\System32\TAPI32.dll
      SUCCESS

1318  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WinDump.exe.Local\ NOT FOUND    Attributes: Error

1319  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.0.0_x-ww_1382d70a   SUCCESS      Attributes:
D

1320  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.0.0_x-ww_1382d70a   SUCCESS      Options:
Open Directory  Access: Traverse

1321  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.0.0_x-ww_1382d70a\comctl32.dll   SUCCESS
      Options: Open  Access: Execute

1322  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.0.0_x-ww_1382d70a\comctl32.dll   SUCCESS
      Length: 921088

1323  4:16:42 PM  WinDump.exe:1912   CLOSE
      C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.0.0_x-ww_1382d70a\comctl32.dll   SUCCESS


1324  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.0.0_x-ww_1382d70a\comctl32.dll   SUCCESS
      Options: Open  Access: Execute

1325  4:16:42 PM  WinDump.exe:1912   CLOSE
      C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.0.0_x-ww_1382d70a\comctl32.dll   SUCCESS


1326  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\WindowsShell.Manifest      SUCCESS      Attributes: RHA

1327  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\WindowsShell.Manifest      SUCCESS      Options: Open
Access: Execute

1328  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\WindowsShell.Manifest      SUCCESS      Length: 749

1329  4:16:42 PM  WinDump.exe:1912   CLOSE
      C:\WINDOWS\WindowsShell.Manifest      SUCCESS
```

```
1330  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\WindowsShell.Manifest      SUCCESS      Attributes: RHA

1331  4:16:42 PM  WinDump.exe:1912  OPEN
      C:\WINDOWS\WindowsShell.Manifest      SUCCESS      Options: Open
Access: All

1332  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\WindowsShell.Manifest      SUCCESS      Length: 749

1333  4:16:42 PM  WinDump.exe:1912  CLOSE
      C:\WINDOWS\WindowsShell.Manifest      SUCCESS

1334  4:16:42 PM  WinDump.exe:1912  OPEN
      C:\WINDOWS\WindowsShell.Manifest      SUCCESS      Options: Open
Access: All

1335  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\WindowsShell.Manifest      SUCCESS      Length: 749

1336  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\WindowsShell.Manifest      SUCCESS      Length: 749

1337  4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\WindowsShell.Config
      NOT FOUND    Options: Open  Access: All

1338  4:16:42 PM  WinDump.exe:1912  CLOSE
      C:\WINDOWS\WindowsShell.Manifest      SUCCESS

1339  4:16:42 PM  WinDump.exe:1912  OPEN  C:\WINDOWS\system32\SHELL32.dll
      SUCCESS      Options: Open  Access: All

1340  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\system32\SHELL32.dll SUCCESS      Length: 8227840

1341  4:16:42 PM  WinDump.exe:1912  OPEN
      C:\WINDOWS\system32\SHELL32.dll.124.Manifest      NOT FOUND
      Options: Open  Access: All

1342  4:16:42 PM  WinDump.exe:1912  OPEN
      C:\WINDOWS\system32\SHELL32.dll.124.Config  NOT FOUND    Options:
Open  Access: All

1343  4:16:42 PM  WinDump.exe:1912  CLOSE C:\WINDOWS\system32\SHELL32.dll
      SUCCESS

1344  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\WinDump.exe.Local\ NOT FOUND    Attributes: Error

1345  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.0.0_x-ww_1382d70a   SUCCESS      Attributes:
D

1346  4:16:42 PM  WinDump.exe:1912  OPEN
      C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
```

```
Controls_6595b64144ccf1df_6.0.0.0_x-ww_1382d70a   SUCCESS     Options:
Open Directory  Access: Traverse

1347  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\drivers\npf.sys    PATH NOT FOUND    Attributes:
Error

1348  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\drivers\npf.sys    PATH NOT FOUND    Attributes:
Error

1349  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\System32\drivers\npf.sys  SUCCESS     Attributes: A

1350  4:16:42 PM  WinDump.exe:1912  OPEN
      C:\WINDOWS\System32\drivers\npf.sys  SUCCESS     Options: Open
Access: Execute

1351  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\System32\drivers\npf.sys  SUCCESS     Length: 32896

1352  4:16:42 PM  WinDump.exe:1912  CLOSE
      C:\WINDOWS\System32\drivers\npf.sys  SUCCESS

1353  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\drivers\npf.sys    PATH NOT FOUND    Attributes:
Error

1354  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\drivers\npf.sys    PATH NOT FOUND    Attributes:
Error

1355  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\System32\drivers\npf.sys  SUCCESS     Attributes: A

1356  4:16:42 PM  WinDump.exe:1912  OPEN
      C:\WINDOWS\System32\drivers\npf.sys  SUCCESS     Options: Open
Access: All

1357  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\System32\drivers\npf.sys  SUCCESS     Length: 32896

1358  4:16:42 PM  WinDump.exe:1912  CLOSE
      C:\WINDOWS\System32\drivers\npf.sys  SUCCESS

1359  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\drivers\npf.sys    PATH NOT FOUND    Attributes:
Error

1360  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\drivers\npf.sys    PATH NOT FOUND    Attributes:
Error

1361  4:16:42 PM  WinDump.exe:1912  QUERY INFORMATION
      C:\WINDOWS\System32\drivers\npf.sys  SUCCESS     Attributes: A
```

```
1362  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\System32\drivers\npf.sys  SUCCESS     Options: Open
Access: Execute

1363  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\drivers\npf.sys  SUCCESS     Length: 32896

1364  4:16:42 PM  WinDump.exe:1912   CLOSE
      C:\WINDOWS\System32\drivers\npf.sys  SUCCESS

1365  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\drivers\npf.sys    PATH NOT FOUND    Attributes:
Error

1366  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\drivers\npf.sys    PATH NOT FOUND    Attributes:
Error

1367  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\drivers\npf.sys  SUCCESS     Attributes: A

1368  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\System32\drivers\npf.sys  SUCCESS     Options: Open
Access: All

1369  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\drivers\npf.sys  SUCCESS     Length: 32896

1370  4:16:42 PM  WinDump.exe:1912   CLOSE
      C:\WINDOWS\System32\drivers\npf.sys  SUCCESS

1371  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\dagc.dll     NOT FOUND   Attributes: Error

1372  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION  C:\Documents and
Settings\default\Desktop\dagc.dll     NOT FOUND   Attributes: Error

1373  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\dagc.dll    NOT FOUND   Attributes: Error

1374  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\system\dagc.dll      NOT FOUND   Attributes: Error

1375  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\dagc.dll      NOT FOUND   Attributes: Error

1376  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\system32\dagc.dll    NOT FOUND   Attributes: Error

1377  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\dagc.dll      NOT FOUND   Attributes: Error

1378  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\COMMAND\dagc.dll     NOT FOUND   Attributes: Error

1379  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\system32\WBEM\dagc.dll     NOT FOUND    Attributes: Error
```

```
1380  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\System32\npp\
      SUCCESS     Options: Open Directory  Access: All

1381  4:16:42 PM  WinDump.exe:1912   DIRECTORY   C:\WINDOWS\System32\npp\
      SUCCESS     FileBothDirectoryInformation: *.dll

1382  4:16:42 PM  WinDump.exe:1912   DIRECTORY   C:\WINDOWS\System32\npp\
      NO MORE FILES     FileBothDirectoryInformation

1383  4:16:42 PM  WinDump.exe:1912   CLOSE C:\WINDOWS\System32\npp\
      SUCCESS

1384  4:16:42 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\System32\npp\
      SUCCESS     Options: Open Directory  Access: All

1385  4:16:42 PM  WinDump.exe:1912   DIRECTORY   C:\WINDOWS\System32\npp\
      SUCCESS     FileBothDirectoryInformation: *.dll

1386  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\npp\ndisnpp.dll  SUCCESS     Attributes: A

1387  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\System32\npp\ndisnpp.dll  SUCCESS     Options: Open
Access: Execute

1388  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\npp\ndisnpp.dll  SUCCESS     Length: 55808

1389  4:16:42 PM  WinDump.exe:1912   CLOSE
      C:\WINDOWS\System32\npp\ndisnpp.dll  SUCCESS

1390  4:16:42 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\npp\ndisnpp.dll  SUCCESS     Attributes: A

1391  4:16:42 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\System32\npp\ndisnpp.dll  SUCCESS     Options: Open
Access: Execute
1392  4:16:42 PM  WinDump.exe:1912   CLOSE
      C:\WINDOWS\System32\npp\ndisnpp.dll  SUCCESS
1393  4:16:42 PM  WinDump.exe:1912   DIRECTORY   C:\WINDOWS\System32\npp\
      NO MORE FILES     FileBothDirectoryInformation
1394  4:16:42 PM  WinDump.exe:1912   CLOSE C:\WINDOWS\System32\npp\
      SUCCESS
1395  4:16:43 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\System32\npp\
      SUCCESS     Options: Open Directory  Access: All
1396  4:16:43 PM  WinDump.exe:1912   DIRECTORY   C:\WINDOWS\System32\npp\
      SUCCESS     FileBothDirectoryInformation: *.dll
1397  4:16:43 PM  WinDump.exe:1912   DIRECTORY   C:\WINDOWS\System32\npp\
      NO MORE FILES     FileBothDirectoryInformation
1398  4:16:43 PM  WinDump.exe:1912   CLOSE C:\WINDOWS\System32\npp\
      SUCCESS
1399  4:16:43 PM  WinDump.exe:1912   OPEN  C:\WINDOWS\System32\npp\
      SUCCESS     Options: Open Directory  Access: All
1400  4:16:43 PM  WinDump.exe:1912   DIRECTORY   C:\WINDOWS\System32\npp\
      SUCCESS     FileBothDirectoryInformation: *.dll
```

```
1401  4:16:43 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\npp\ndisnpp.dll   SUCCESS     Attributes: A
1402  4:16:43 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\System32\npp\ndisnpp.dll   SUCCESS     Options: Open
Access: Execute
1403  4:16:43 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\npp\ndisnpp.dll   SUCCESS     Length: 55808
1404  4:16:43 PM  WinDump.exe:1912   CLOSE
      C:\WINDOWS\System32\npp\ndisnpp.dll   SUCCESS
1405  4:16:43 PM  WinDump.exe:1912   QUERY INFORMATION
      C:\WINDOWS\System32\npp\ndisnpp.dll   SUCCESS     Attributes: A
1406  4:16:43 PM  WinDump.exe:1912   OPEN
      C:\WINDOWS\System32\npp\ndisnpp.dll   SUCCESS     Options: Open
Access: Execute
1407  4:16:43 PM  WinDump.exe:1912   CLOSE
      C:\WINDOWS\System32\npp\ndisnpp.dll   SUCCESS
1408  4:16:43 PM  WinDump.exe:1912   DIRECTORY   C:\WINDOWS\System32\npp\
      NO MORE FILES      FileBothDirectoryInformation
1409  4:16:43 PM  WinDump.exe:1912   CLOSE C:\WINDOWS\System32\npp\
      SUCCESS
1410  4:16:44 PM  WinDump.exe:1912   OPEN  C:\etc\ethers      PATH NOT
FOUND Options: Open  Access: All
1411  4:16:44 PM  WinDump.exe:1912   OPEN  C:\etc\services    PATH NOT
FOUND Options: Open  Access: All
1412  4:16:44 PM  WinDump.exe:1912   CREATEC:\Documents and
Settings\default\Desktop\capture      SUCCESS     Options: OverwriteIf
Access: All
1413  4:16:44 PM  WinDump.exe:1912   WRITE C:\Documents and
Settings\default\Desktop\capture      SUCCESS     Offset: 0 Length: 24
1414  4:16:52 PM  svchost.exe:764    OPEN
      C:\WINDOWS\Prefetch\WINDUMP.EXE-09422DA4.pf SUCCESS      Options:
Open  Access: All
1415  4:16:52 PM  svchost.exe:764    QUERY INFORMATION
      C:\WINDOWS\Prefetch\WINDUMP.EXE-09422DA4.pf SUCCESS      Length:
39232
1416  4:16:52 PM  svchost.exe:764    QUERY INFORMATION
      C:\WINDOWS\Prefetch\WINDUMP.EXE-09422DA4.pf SUCCESS      Length:
39232
1417  4:16:52 PM  svchost.exe:764    CLOSE
      C:\WINDOWS\Prefetch\WINDUMP.EXE-09422DA4.pf SUCCESS
1418  4:16:52 PM  svchost.exe:764    QUERY INFORMATION  C:\DOCUMENTS AND
SETTINGS\DEFAULT\DESKTOP\WINDUMP.EXE  SUCCESS     Attributes: A
1419  4:16:52 PM  svchost.exe:764    OPEN  C:\DOCUMENTS AND
SETTINGS\DEFAULT\DESKTOP\WINDUMP.EXE  SUCCESS     Options: Open  Access:
All
1420  4:16:52 PM  svchost.exe:764    QUERY INFORMATION  C:\DOCUMENTS AND
SETTINGS\DEFAULT\DESKTOP\WINDUMP.EXE  SUCCESS     FileInternalInformation
1421  4:16:52 PM  svchost.exe:764    CLOSE C:\DOCUMENTS AND
SETTINGS\DEFAULT\DESKTOP\WINDUMP.EXE  SUCCESS
1422  4:16:52 PM  svchost.exe:764    CREATE
      C:\WINDOWS\Prefetch\WINDUMP.EXE-09422DA4.pf SUCCESS      Options:
OverwriteIf  Access: All
1423  4:16:52 PM  svchost.exe:764    WRITE
      C:\WINDOWS\Prefetch\WINDUMP.EXE-09422DA4.pf SUCCESS      Offset: 0
Length: 39244
1424  4:16:52 PM  svchost.exe:764    CLOSE
      C:\WINDOWS\Prefetch\WINDUMP.EXE-09422DA4.pf SUCCESS
```

```
1425  4:17:01 PM  WinDump.exe:1912  WRITE C:\Documents and
Settings\default\Desktop\capture     SUCCESS     Offset: 24 Length: 16
1426  4:17:01 PM  WinDump.exe:1912  WRITE C:\Documents and
Settings\default\Desktop\capture     SUCCESS     Offset: 40 Length: 96
1427  4:17:18 PM  WinDump.exe:1912  WRITE C:\Documents and
Settings\default\Desktop\capture     SUCCESS     Offset: 136 Length: 16
1428  4:17:18 PM  WinDump.exe:1912  WRITE C:\Documents and
Settings\default\Desktop\capture     SUCCESS     Offset: 152 Length: 96
1429  4:17:26 PM  WinDump.exe:1912  CLOSE C:\Documents and
Settings\default\Desktop\capture     SUCCESS
1430  4:17:26 PM  WinDump.exe:1912  CLOSE
      C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.0.0_x-ww_1382d70a   SUCCESS
1431  4:17:26 PM  WinDump.exe:1912  CLOSE C:\Documents and
Settings\default\Desktop SUCCESS
1432  4:17:26 PM  WinDump.exe:1912  CLOSE
      C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.0.0_x-ww_1382d70a   SUCCESS
```