Global Information Assurance Certification Paper

Forensic Image Analysis of a USB Flashdrive

Howard Heerwagen
February 10th, 2005

GIAC Certified Forensic Analyst (GCFA)
Version 2.0 – Option 1

Abstract

This practical was done to obtain the GIAC GCFA certification. Option 1 from the GCFA 2.0 track was selected, and the results of the analysis are outlined in this document. The document steps through several areas of forensic analysis, from analyzing the image to choose the best course of action, to doing the actual forensic investigation of files and binaries, to making recommendation to a course of action for affected parties.

Executive Summary

Robert Lawrence, an employee of CC Terminals is suspected of having harassed a fellow employee, Leila Conlay. Mr. Lawrence has been accused of making several unwanted romantic advances towards Ms. Conlay, and Ms. Conlay feels that Mr. Lawrence's advances have become increasingly aggressive. He has even come so far as to have obtained her personal e-mail address, and follow her to a local coffee shop where she was meeting a friend. In the report below, evidence will be presented as to how Mr. Lawrence did indeed craft letters to Ms. Conlay that are threatening in nature, how Mr. Lawrence obtained Ms. Conlay's personal e-mail address, and how Mr. Lawrence obtained the information required to gain the knowledge of Ms. Conlay's whereabouts on the evening of Thursday, October 29th 2004.

Mr. Lawrence was found to be in possession a USB Flashdrive, which was seized from his cubicle at CC Terminals. Discovered on this device were three letters that are presumed to be destined for Ms. Conlay, which were created on a PC belonging to Mr. Lawrence. It is also believed that Mr. Lawrence captured data from a wireless network (possibly at CC Terminals) for the purpose of obtaining information about Ms. Conlay's e-mail address and behaviors. A deleted capture of network traffic was also found on the Flashdrive, as well as utilities that would have enabled Mr. Lawrence to capture or “sniff” the data from the wireless network. Contained in the network capture was Ms. Conlay’s e-mail address, as well as the address of a male friend of Ms. Conlay, a Mr. Sam Guarillo. The content of the e-mail referred to Ms. Conlay meeting Mr. Guarillo at a coffee shop on the corner of Hollywood and McCadden. Also found on the Flashdrive was a .GIF file containing a map to the Hollywood area, with a location marker indicating a destination of Hollywood at McCadden. I believe that all of the above information is compelling enough to prove that Mr. Lawrence did illegally obtain information about Ms. Conlay, and used this information for the purpose of determining Ms. Conlay whereabouts for the sole purpose of harassing her.

Tools Used

During the course of the analysis of this image and any discovered files and binaries, several tools were used which the reader may or may not be familiar with. In order to allow these results to be duplicated, and to preserve the integrity of this investigation, I will outline the tools used, along with descriptions of them and link to where they may be found.

1. md5sum – (coreutils) – 5.2.1 – Included with Fedora Core 2 – Computes the MD5 hash of a specified file.

2. The Sleuth Kit – 1.73 – http://www.sleuthkit.org/ - A collection of UNIX-based command line file system and media management forensic analysis tools.

3. Autopsy Forensic Browser – 2.03 - http://www.sleuthkit.org/ - A graphical interface to the command line digital forensic analysis tools in The Sleuth Kit.

4. mmls – Included in The Sleuth Kit version 1.73 - Displays the layout of a disk, including the unallocated spaces. The output identifies the type of partition and its length, which makes it easy to use 'dd' to extract the partitions.

5. fsstat - Included in The Sleuth Kit version 1.73 - Shows file system details and statistics including layout, sizes, and labels.

6. fls - Included in The Sleuth Kit version 1.73 - Lists file and directory names in a forensic image.

7. ils - Included in The Sleuth Kit version 1.73 - Lists the meta data structures and their contents in a pipe delimited format.

8. dls - Included in The Sleuth Kit version 1.73 - Lists the details about data units and can extract the unallocated space of the file system.

9. strings – (binutils) – 2.15.90.03 - Included with Fedora Core 2

10. KhexEdit – 0.8.5 – Included with KDE 3.3.2 – http://home.online.no/~espensa/khexedit - A KDE based hex viewer and editor.

11. VMWare – 4.5.2.build 8848 – www.vmware.com – Allows for the creation of virtual machines on a host system that are capable of running a variety of operating systems. Virtual Machines used in this analysis are as

follows: Windows XP Professional with Service Pack 2.

12. Ethereal – 10.0.9 – www.ethereal.com – A network protocol analyzer.

13. X-Ways Forensics – 12.0 SR17 – www.x-ways.com – Windows based forensic analysis software.

14. file – 4.07 - Included with Fedora Core 2

15. dcfldd – 1.0 - Enhanced dd with md5 checksums

Image Details

The machine used to do the analysis of this image was a clone-type PC of x86 architecture running Linux Fedora Core 2 with kernel 2.6.9-1.6_FC2. This machine was not connected to any network while the image was being analyzed to prevent malicious activity from any binaries contained in the image.

The compressed image of the flashdrive was downloaded to the analysis workstation via a USB flashdrive. The image was then decompressed. A MD5SUM was taken of the extracted file was taken.

```
[root@LinuxForensics extract]# gunzip -N GCFAPractical2.0-
USBImageAndInfo.zip.gz
[root@LinuxForensics extract]# ls
USBFD-64531026-RL-001.img
[root@LinuxForensics extract]# md5sum USBFD-64531026-RL-001.img
338ecf17b7fc85bbb2d5ae2bbc729dd5  USBFD-64531026-RL-001.img
```

The MD5 hash of the extracted file matched the MD5 hash of the file provided from the GIAC site.

From the GIAC site:

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

This was encouraging since that it is mathematically improbable to create two different files with the same MD5 hash value. The hash value was also concatenated to a file for future reference.

The image provided is a physical image of the USB Flashdrive described above. Before this physical image can be properly analyzed, it must first be separated into its logical components. In order to accomplish this, the *mmls* program is run. *Mmls* analyzes a physical drive image and determines the start and end sectors of its logical components.

[*root@LinuxForensics images]# 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)*

Notice that there are three distinct areas of the physical image that warrant attention: 1) the primary table, 2) unallocated space, and 3) a DOS FAT16 partition. It is also noted at this point that the sector size is 512-bytes. This will be useful information later on in the process. The results of the *mmls* tool were concatenated to a file for future reference. In order to break the physical image, the tool *dcfldd* was used. The results from *mmls* were entered into *dcfldd* in order to extract the three logical areas of interest.

[*root@LinuxForensics images]# dcfldd skip=0 count=1 hashwindow=0*
if=USBFD-64531026-RL-001.img of=pri_usb.img
Total: 5bf1cea807dec8655ed18b9bbf2ee918
1+0 records in
1+0 records out

[root@LinuxForensics images]# dcfldd skip=1 count=31 hashwindow=0
if=USBFD-64531026-RL-001.img of=unal_usb.img
Total: 51596dda30fc38f0df3556d6f115256d
31+0 records in
31+0 records out

[root@LinuxForensics images]# dcfldd skip=32 count=121950 hashwindow=0
if=USBFD-64531026-RL-001.img of=sda0.img
121856 blocks (59Mb) written.
Total: ac666df2072927fb9b0047886f0e2385
121920+0 records in
121920+0 records out

MD5 hashes were taken at the time of extraction by specifying the hashwindow=0 option. The file command was run against each extracted partition to verify that they had been extracted correctly and completely. The

results were concatenated to a file.

The *fsstat* tool was also run against the FAT16 image and the results recorded. The *fsstat* tool shows information about the logical image against which it was ran. It shows information such as the file system's last mount time, the volume type, the volume label, and the file system structure.

[root@LinuxForensics images]# fsstat -f fat16 sda0.img > sda0.fsstat
[root@LinuxForensics images]# cat sda0.fsstat

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

At this point, nothing has been done to the images that could potentially alter any data contained in them. Before the images can be mounted and analyzed, information must be extracted from them to re-created a MAC (modified, accessed, changed) timeline. This is accomplished with the *fls* and *ils* tools. *Fls* parses through the image, and reports information on file and directory names in the image, and lists the output in a data file format. *Ils* parses through the image and reports information on removed files that still have inode entries, and lists the output in a data file.

[root@LinuxForensics images]# fls -f fat16 -m / -r sda0.img > sda0.fls

[root@LinuxForensics images]# ils -f fat16 -m sda0.img > sda0.ils

These two output files are concatenated together into one file to facilitate the execution of the *mactime* tool. *Mactime* is a perl script that takes a data file in the proper format, and converts it into a human readable sequence of events.

[root@LinuxForensics images]# cat sda0.?ls > sda0.mac

Mactime was run against the above file, and the results were recorded in sda0.all

[root@LinuxForensics images]# mactime –b sda0.mac > sda0.all

The results can be viewed in Appendix A

Next, the *strings* program was run against the FAT16 image to extract all strings of 4 characters or more. The command was ran win the –radix=d option to display the offset where the particular strings were found. The results are concatenated to a file to be queried for string searches in the future.

[root@LinuxForensics images]# strings --radix=d sda0.img > sda0.str

The tool *dls* was also ran to extract all of the unallocated data from the image.

[root@LinuxForensics images]# dls -f fat16 sda0.img > sda0.dls

At this point, the image that was provided has been broken up into the basic components required to perform a thorough analysis.

Examination Details

As stated previously, the physical image was broken down into three logical images; the primary table, some unallocated space, and a FAT16 partition. First, the primary table and unallocated space are analyzed to determine if any hidden data is residing within them. The primary table was opened in *khexedit*. It contained no hidden data, files, or code. The unallocated space was then opened in *khexedit*. The contents of this extracted region consisted of all 0's. This means that there was no data stored, nor had data recently been deleted from here or was left over from a previous partition. After viewing these files in hex, it was determined that their contents are irrelevant in the terms of this investigation. This conclusion is supported by the fact that previously, the FSSTAT tool had reported that there were 32 sectors present before the file system. The MMLS output also showed that the FAT16 file system began with sector number 32.

Next, the FAT16 partition is analyzed. The logical partition was mounted on the forensic analysis workstation so that its contents could be viewed as it existed on the last system that it was mounted on. The *mount* program was issued certain commands to ensure that the integrity of the image was not altered. The options ro (read-only), noatime (do not update inode access time), loop (mount using the loopback device), and noexec (prevent executable files from being run) were given.

[root@LinuxForensics images]# mount -t vfat -o,ro,loop,noatime,noexec sda0.img /mnt/winfornensics/

The output of *mount* was grep'd for the image name to confirm that it was mounted with the appropriate options.

[root@LinuxForensics images]# mount | grep sda0.img
/forensics/images/sda0.img on /mnt/winfornensics type vfat (ro,noexec,noatime,loop=/dev/loop0)

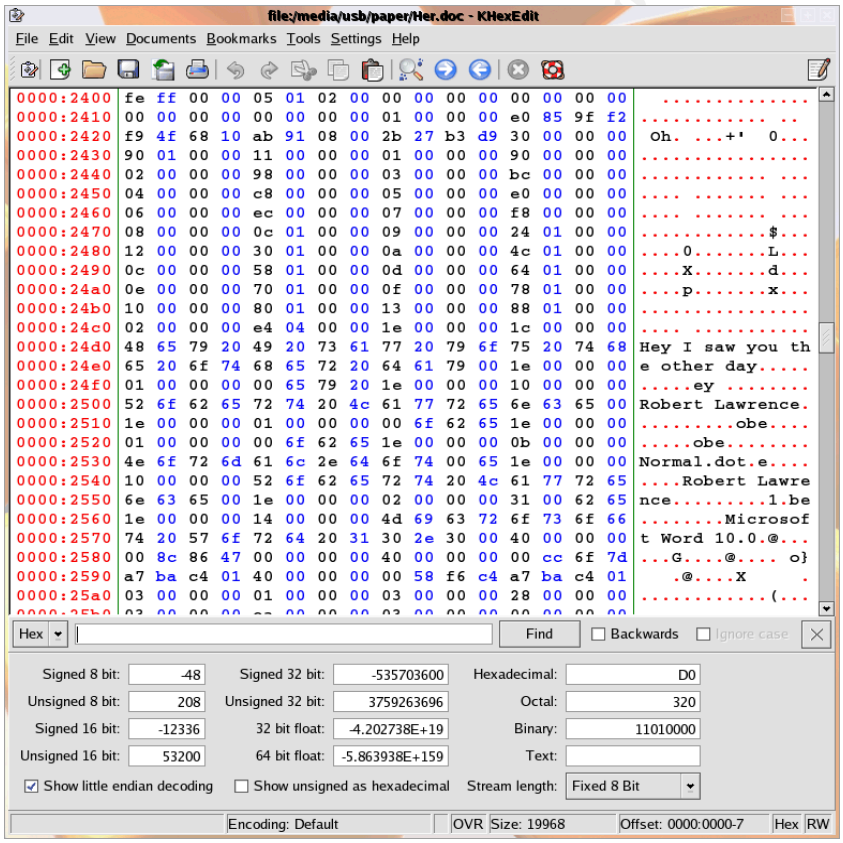
The image of the FAT16 partition is now available for analysis. The directory was changed to /mnt/winforensics. The command *ls* with the -lit switches is used to list the files in the root directory of the image.

[root@LinuxForensics winfornensics]# ls -lit
total 60
7 -rwxr-xr-x 1 root root 19968 Oct 28 20:24 coffee.doc
6 -rwxr-xr-x 1 root root 19968 Oct 26 09:48 hey.doc
5 -rwxr-xr-x 1 root root 19968 Oct 25 09:32 her.doc

The *file* program was run against each of the file found in the root directory, and the output was recorded:

[*root@LinuxForensics winfornensics]# file coffee.doc hey.doc her.doc*
coffee.doc: Microsoft Office Document
hey.doc: Microsoft Office Document
her.doc: Microsoft Office Document

Some very important information is reported back from the file command. The output shows that all three of the documents present were created with Microsoft Office. This exposes a new area to be examined, as Microsoft Office is known to hide information pertaining to the document owner/creator in the metadata of the saved files. The files were then examined in *khexedit* to look for information hidden in the metadata of the files. In all three files, the name "Robert Lawrence" appeared numerous times, indicating that he was probably the creator of these three files. No other names were found present in the metadata of the three files.
Other pertinent information is hidden in the metadata of these files as well. The files were created with Microsoft Word version 10.0.



File Content

The actual contents of the files are as follows:

her.doc

```
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
```

hey.doc

```
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?
```

coffee.doc

```
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...
```

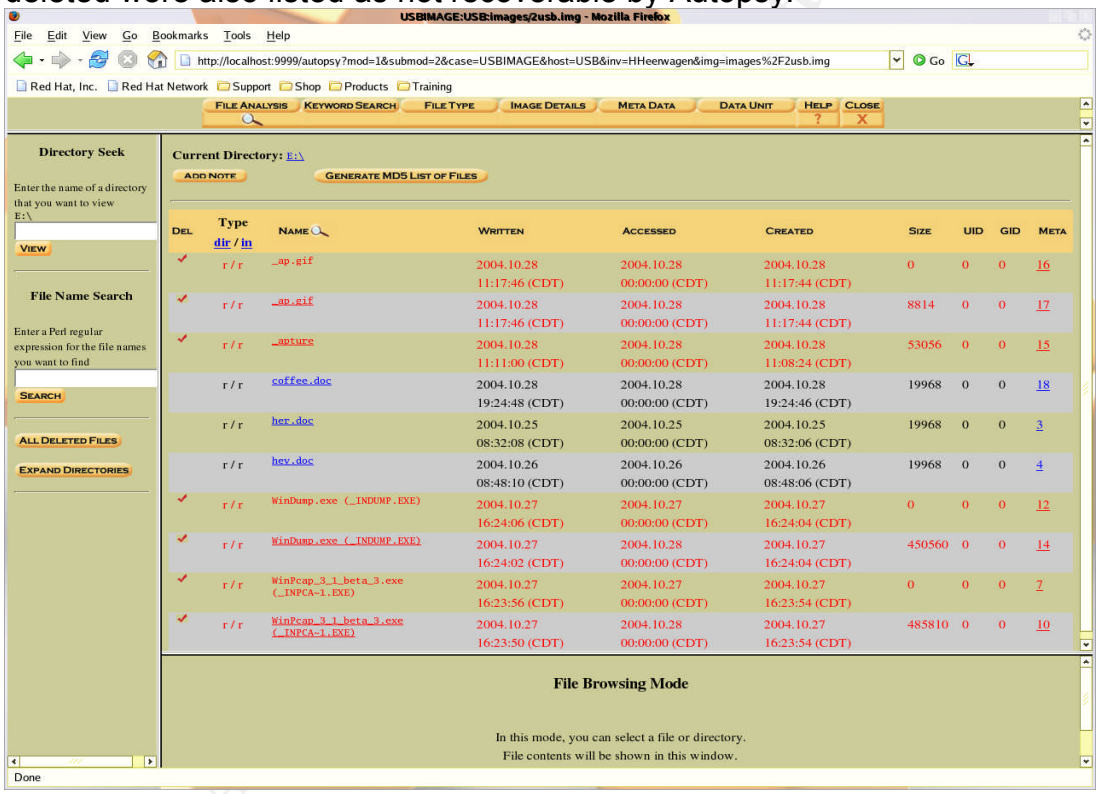
The tone of these writings devolves from one of innocent friendship, to one of anger, to one of obsession. In the last file, coffee.doc, he alludes that physical harm may come to Ms. Conlay via a “bad batch” of coffee. It appears that Mr. Lawrence was obsessed with the victim, and became increasingly more threatening in his communications with here when his advances were ignored.

File Recovery

At this point, the image was analyzed to determine if there were any deleted files present on the drive that were recoverable. The software used to perform this analysis is Autopsy. Autopsy is a graphical interface to the tools contained in The SleuthKit, and the Coroner's Toolkit. In Autopsy, a new case was created, and the image file “sda0.img” was added to the case. Before any analysis was performed, a file activity timeline was extracted so that events and

file content could be correlated to file MAC times. After the file timeline is extracted, it is viewed to verify integrity. Notice that the access times all read 00:00:00. This is due to the fact that the FAT16 file system does not log access times, only the access dates. Explanation of the FAT file structure can be found at http://home.freeuk.net/foxy2k/disk/disk6.htm.

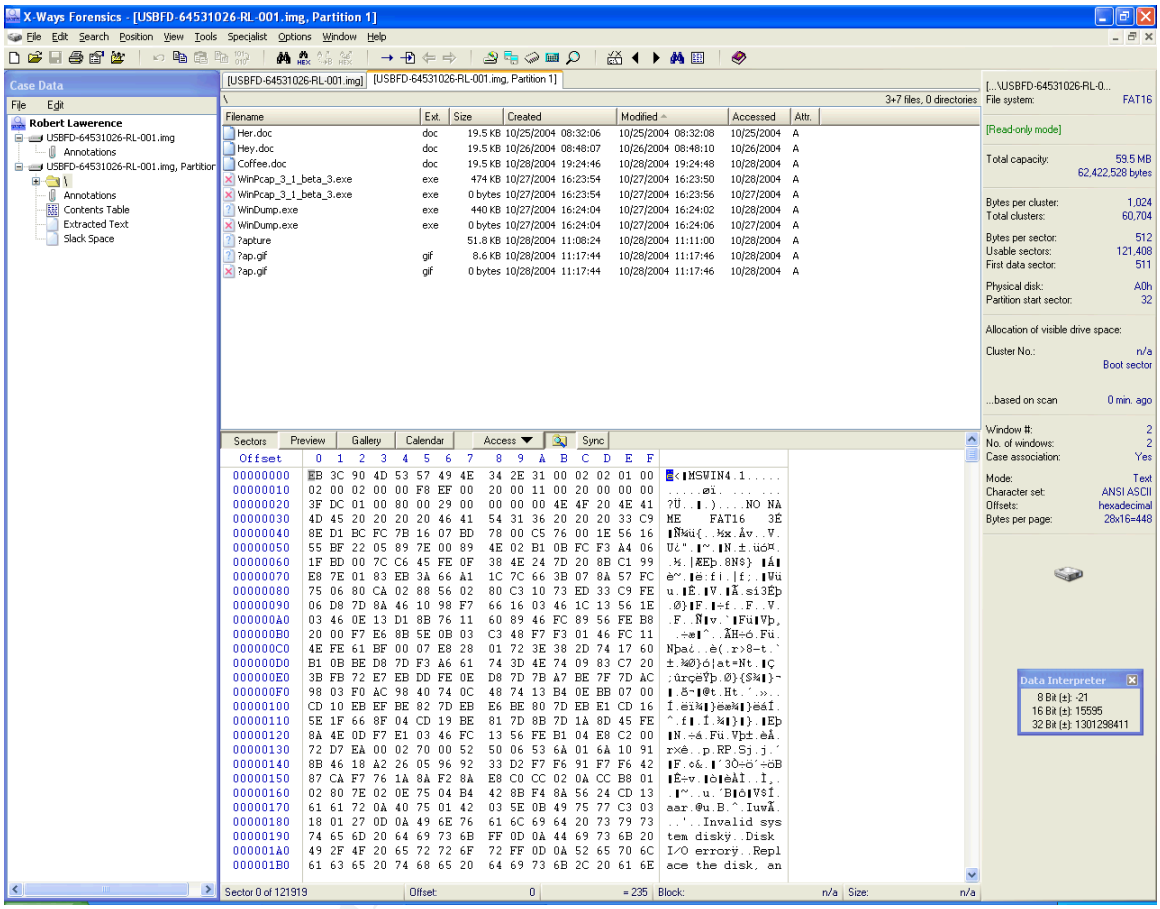
The scripts in Autopsy and mactime that generate the timeline are file system independent, and a missing value is substituted as 00:00:00. After the timeline was created, the analysis of files contained within the image begins. Several files are visible in File Browsing mode. The three files listed previously are displayed here as current files. Several files are listed as deleted files, meaning that the data exists on the disk, but the files have been deleted (the space has been marked as unallocated by the file system). One of these files listed as deleted were also listed as not recoverable by Autopsy.



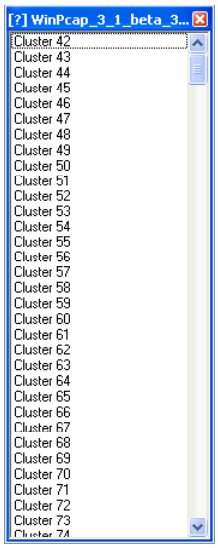
WinPcap_3_1_beta_3.exe

The first file encountered is named “WinPcap_3_1_beta_3.exe (_INPCA~1.EXE). It is identified by inode entry 10, and is contained in sectors 591-630. Autopsy has also marked this file as unrecoverable. Some further investigation reveals why - the file coffee.doc, which was created on a later date, is also assigned the same area on the disk. The most likely reason for this is that the file WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) was probably deleted on or about 10-28-2004. The file coffee.doc was created shortly thereafter, and

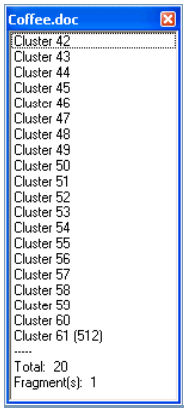
was allocated the disk space that the file WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) previously occupied. To facilitate in the recovery of this file, the Windows based tool, X-Ways Forensics will be used. After this image file is loaded into X-Ways, X-Ways is told to treat the image file as a disk. Partition 1 was then opened for analysis.



By right-clicking on the file “WinPcap_3_1_beta_3.exe”, the clusters that contain the file can be viewed. X-Ways shows that WinPcap is contained in clusters XX-XX. From our previous investigation with Autopsy, it was determined that some of the disk space that was at one time allocated to the file “WinPcap_3_1_beta_3.exe” is now allocated to the file Coffee.doc.



By following the same process for Coffee.doc, it was discovered that the first 19 clusters of both files are overlapping.



At this point WinPcap_3_1_beta_3.exe was recovered from the image by right-clicking, as selecting Recover/Copy. The file was saved to the hard drive of the analysis workstation.

WinDump.exe

Next is WinDump.exe (_INDUMP.EXE). This file is identified by inode entry 14, and is contained in sectors 1541 through 2420. The inode entry shows that currently this space is marked as “Not Allocated”, meaning that the sectors allocated have been marked as overwritable. In other words, the file has been deleted. The file is displayed in the file browser window, and exported to the analysis workstation as WinDump.exe. The file command was run against this file, and it was identified as an MS-DOS executable (EXE), OS/2 or MS Windows.

_apture

The file _apture is encountered next. It is identified by inode entry 15, and is contained in sectors 2421 through 2524. The file is displayed in the file browser window, and exported to the analysis workstation as “_apture”. The FILE command was ran against this file, and it was identified as a “tcpdump capture file (little-endian) - version 2.4 (Ethernet, capture length 4096)”. This is important information, as it shows which program that might be used to analyze the contents of this file.
The last deleted file discovered is named “_ap.gif”. This file is identified by inode entry 17, and is contained in sectors 2525 through 2542. The inode entry shows that this space is currently marked as Not Allocated. The file is displayed in the file browser window, and exported to the analysis workstation as “_ap.gif”. he file command was run against this file, and it was identified as “GIF image data, version 89a, 300 x 200”.

Files Recovered

[root@LinuxForensics recovered]# ls -al
total 580
drwxr-xr-x 2 root root   4096 Feb 9 23:01 .
drwxr-xr-x 4 root root   4096 Feb 9 23:00 ..
-rw-r--r-- 1 root root   8814 Feb 5 00:20 _ap.gif
-rw-r--r-- 1 root root 53056 Feb 5 00:16 _apture
-rwxr-xr-x 1 root root 19968 Feb 5 00:12 coffee.doc
-rwxr-xr-x 1 root root 19968 Feb 5 00:12 her.doc
-rwxr-xr-x 1 root root 19968 Feb 5 00:12 hey.doc
-rw-r--r-- 1 root root 450560 Feb 5 00:11 WinDump.exe
-rw-r-r-- 1 root root 485810 Feb 5 00:11 WinPcap_3_1_beta_3.exe

Forensic Details

WinPcap_3_1_beta_3.exe

WinPcap is an application that was written to give Win32 applications raw access to network hardware, without the interference of protocol stacks. Is was designed to let the used capture raw packets, filter those packets, transmit raw packets, and gather network statistics. It has no direct user interface, but is used by programs such as network and protocol analyzers, traffic loggers, and network scanners. WinPcap simply sniffs the packets that are transmitted on the wire.
Details of WinPcap's functionality are thoroughly documented at http://winpcap.polito.it/docs/man/html/index.html.

WinDump.exe

Windump is a Windows port of tcpdump, a packet sniffing application coded for the UNIX platform. Windump interfaces with the WinPcap libraries to gain access to the network harware of a Windows based system, and record packets seen by that particular physical interface.
(http://windump.polito.it/docs/manual.htm)

To verify the functionality of WinDump, the recovered WinDump binary was transferred to a Virtual Machine running Windows XP Pro under VMWare Workstation version 4.52.

From a command prompt, WinDump.exe was run, specifying the -D option to list all available network adapters in the system. WinDump.exe was then run with the -s , -n and -w options as specified in the manual available at http://windump.polito.it/docs/manual.htm. The resulting capture file was

analyzed in Ethereal, and determined to indeed be a packet capture of the specified interface, demonstrating that the function of the discovered binary is identical to the known binary obtained from the internet.

_apture

The file _apture was identified previously as a tcpdump capture file (little-endian) - version 2.4 (Ethernet, capture length 4096). This type of file is one that may have been created by intercepting data transferred over a network and intercepted by WinDump. (The file name "_apture" was probably "capture" before it was deleted. The file _apture was analyzed with Ethereal version 0.10.9. After the file was loaded into Ethereal for analysis, the Time of Day Format in Ethereal was changed from the default of Settings -> Since Beginning of Capture, to Date and Time of Day. This will assist in correlating the information contained within the file to other timeline evidence that was gathered previously.

First, the content of the file is analyzed to determine what was obtained with the WinDump.exe program. The file contains TCP/IP conversations between several different hosts:

192.168.2.1	Presumed to be the network gateway
192.168.2.104	Presumed to be the victim's computer
192.168.2.255	Network Broadcast Address
207.68.177.124	h.msn.com
216.73.86.40	annyadvip2.doubleclick.net
63.166.13.75	Not Found in DNS
63.209.188.62	unknown.Level3.net
64.4.34.250	www.bay12.hotmail.com

MAC address hosts on the network local to the machine capturing the data are also logged in the file. There are some interesting things about the MAC addresses that may explain how the data was captured. The MAC address if the gateway device is 00:0c:41:50:29:2c. Ethereal reports that MAC addresses beginning with the string "00:0c:41" are allocated to Linksys, a manufactures of broadband gateway devices. The MAC address of the computer presumed to be the victim's computer is 00:90:4b:5e:e3:cf. MAC addresses beginning with "00:90:4b" are allocated to the manufacturer Gemtek. A visit to Gemtek's website (http://www.gemtek-systems.com.tw) reveals that they are a manufacturer of wireless networking equipment.

It is also noted that in the captured data, there are SNMP packets which

originate from the Linksys gateway to the broadcast address of the local network. Contained within these SNMP packets is data about every connection that the victim's computer made through the Linksys gateway. While the default behavior of the Linksys gateway is to send SNMP traps to the broadcast address of the local network, to report data on one specific machine is not. Linksys gateways with the model number beginning in "BEF", are vulnerable to several exploits, some of which can let a malicious user gain access to the device, or manipulate the contents of SNMP traps. SNMP traps can be manipulated to report network access activity about a specific machine, and send that data to the broadcast address of the local network, or to a specific host (http://www.securiteam.com/securitynews/5AP0G0A61Y.html). Based on the network sniff, there is no direct evidence to prove that Mr. Lawrence manipulated the device in this manner, but the data that is being broadcast to the network about the victim's computer is definitely not the default behavior.

The first TCP/IP conversation which was captured and evidenced in the file is between the victim's computer and 64.4.34.250, www.bay12.hotmail.com. The data conversation is re-created in Ethereal by selecting any packet in the conversation, and choosing "Follow TCP Stream" from the "Analyze" menu. The stream content shows a POST transaction from the victim's computer to www.bay12.hotmail.com. (A POST transaction is the uploading of content to an http server). An analysis of the stream shows that a message was successfully uploaded to Hotmail, and the actual content is shown as well.

Content:

curmbox=F000000001&HrsTest=&_HMaction=Send&FinalDest=&subaction=&plaintext=&login=flowergirl96&msg=&start=&len=&attfile=&attlistfile=&eurl=&type=&src=&ref=&ru=&msghdrid=b16479b18beec291196189c78555223c_1098692452&RTEbgcolor=&encodedto=SamGuarillo@hotmail.com&encodedcc=&encodedbcc=&deleteUponSend=0&importance=&sigflag=&newmail=new&to=SamGuarillo@hotmail.com&cc=&bcc=&subject=RE%3A+coffee&body=Sure%2C+coffee+sounds+great.++Let%27s+meet+at+the+coffee+shop+on+the+corner+Hollywood+and+McCadden.++It%27s+a+nice+out+of+the+way+spot.%0D%0A%0D%0ASee+you+at+7pm%21%0D%0A%0D%0A-Leila

Confirmation:

<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

Not only is the content of the message revealed, but other key items such as the victim's hotmail account name, as well as the e-mail recipient's e-mail address.

Victim's Hotmail Account Name: flowergirl96@hotmail.com

Recipient's e-mail address: SamGuarillo@hotmail.com

Content of e-mail:

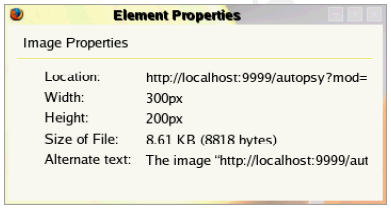
> Sure%2C+coffee+sounds+great.++Let%27s+meet+at+the+coffee
> +shop+on+the+corner+Hollywood+and+McCadden.++It%27s+a+n
> ice+out+of+the+way+spot.%0D%0A%0D%0ASee+you+at+7pm%2
> 1%0D%0A%0D%0A-Leila

By obtaining this information, Mr. Lawrence had acquired all of the information necessary to determine where Ms. Conlay would be at 7pm on the evening of Thursday, October 29th 2004. The address that was stated in the e-mail that Ms. Conlay had sent to Mr. Guarillo was also the same address that was indicated in the _ap.gif file that was found on Mr. Lawrence's USB Flashdrive.

The other TCP/IP conversations contained within the capture are connections spawned by the connection described above. They pull graphics, banners, and content from other web sites, and were not intentionally visited by Ms. Conlay (she would not have had time to manually initiate the connections, since the entire packet capture spans less than one second in length).

_ap.gif

_ap.gif was identified as a "GIF image data, version 89a, 300 x 200" by the program file. The recovered file was opened in through the Autopsy browser in Firefox for analysis. The file _ap.gif is a GIF (Graphics Interchange Format) file with a resolution of 300 x 200 pixels.



Based on the content of the image, it appears to have been acquired with the Microsoft MapPoint application. It is a map to the intersection of Hollywood and McCadden, as annotated by a point labeled "1" in the image. It is believed that this is the same intersection which is referred to in the data that was intercepted by the suspect and recorded in the file "_apture".

Timeline

The contents of the MAC time analysis are shown in Appendix A.

Based on the analysis described above, the picture of Mr. Lawrence's actions become clearer:

On Monday, October 25th, 2004, at 08:32:08, Mr. Lawrence created a Microsoft Word document named "her.doc". The text contained in this file detailed how Mr. Lawrence had seen Ms. Conlay on a previous day, and suspected that she was having car trouble. The letter went with Mr. Lawrence offering her a ride to work sometime, and even offering to take her out for dinner. It is assumed that this document was eventually delivered to Ms. Conlay as described in her original complaint.

On Tuesday, October 26th, 2004, at 08:48:10 Mr. Lawrence created a Microsoft Word document named "hey.doc". In this document, Mr. Lawrence proceeds to express his dissatisfaction with Ms. Conlay's ignorance of his feelings and advances towards her. He concludes the document with another attempt to ask her out, this time for coffee.

On Wednesday, October 27th, 2004, at 16:23:56, the program WinPcap_3_1_beta_3.exe was downloaded to Mr. Lawrence's USB Flashdrive. At 16:24:06, the program WinDump.exe was downloaded to the USB Flashdrive.

On Thursday, October 28th 2004, the programs WinPcap_3_1_beta_3.exe and WinDump.exe were executed. The output file of WinDump, _apture was created at 11:11:00. It is believed that sometime between 11:11:00 and 11:17:44, the data in _apture was analyzed by Mr. Lawrence. At 11:17:44, the file _ap.gif was downloaded to Mr. Lawrence's USB Flashdrive. It is believed that Mr. Lawrence intercepted Ms. Conlay at the location described in the file _ap.gif, as outlined in the original complaint. At 19:24:48, Mr. Lawrence created a Microsoft Word document named "coffee.doc". In this document, Mr.

Lawrence attempts to explain that he just happened to be at the same coffee shop as Ms. Conlay at the same time that she was visiting with a friend. He goes on to express disdain with her actions, and even goes so far at to hint that physical harm might come to her.

On Friday, October 29th, 2004, Ms. Conlay contacted corporate security at CC Terminals. Later that day, a search of Mr. Lawrence's cubicle produced a USB Flashdrive, which was analyzed, and the findings reported in this document.

Program Identification

WinPcap_3_1_beta_3.exe

"WinPcap is an open source library for packet capture and network analysis for the Win32 platforms. It includes a kernel-level packet filter, a low-level dynamic link library (packet.dll), and a high-level and system-independent library (wpcap.dll, based on libpcap version 0.6.2).

The packet filter is a device driver that adds to Windows 95, 98, ME, NT, 2000, XP and 2003 the ability to capture and send raw data from a network card, with the possibility to filter and store in a buffer the captured packets." (http://winpcap.polito.it/)

A copy of WinPcap_3_1_beta_3.exe was obtained from http://winpcap.polito.it/ for comparison to the recovered binary. A MD5SUM was taken of this file and recorded for future reference.

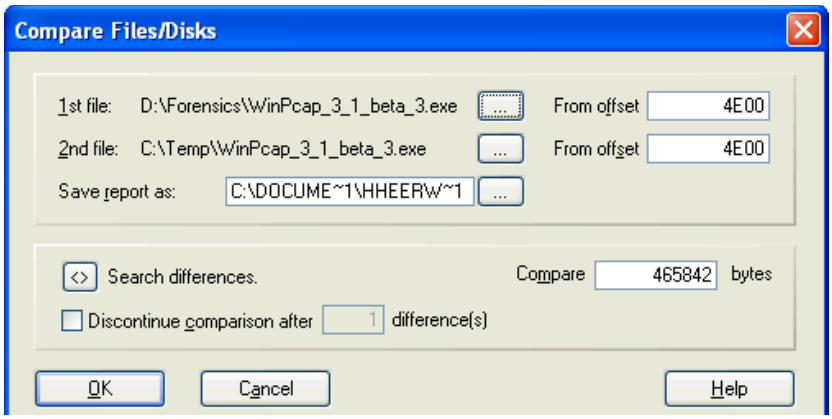
```
[root@LinuxForensics winfiles]# md5sum WinPcap_3_1_beta_3.exe
4511ee3b4e5d8150c035a140dfba72c0  WinPcap_3_1_beta_3.exe
```

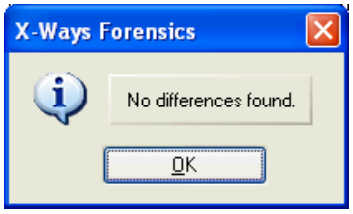
The analysis of the recovered file was started by running the file command against the file.

[root@HH-LIN-X paper]# file WinPcap_3_1_beta_3.exe

WinPcap_3_1_beta_3.exe: Microsoft Office Document

Next, the WinPcap_3_1_beta_3.exe file was compared to the known good binary of WinPcap_3_1_beta_3.exe. This was done by using the compare utility in X-Ways. The files were compared for differences, and were found to be different up to offset 4E00.





Everything past offset 4E00 was found to be identical. To verify as accurately as possible that the two files were identical, both files were copied from byte 4E00 to the end of the file. MD5 hashes were then taken of both files and compared.

[root@LinuxForensics forensics]# md5sum /forensics/images/recovered/Suspect_WinPcap_3_1_beta_3.exe.chopped
39bcc3387dca158dd850fae6f9410405 /forensics/images/recovered/Suspect_WinPcap_3_1_beta_3.exe.chopped

[root@LinuxForensics forensics]# md5sum /forensics/winfiles/WinPcap_3_1_beta_3.exe.Chopped
39bcc3387dca158dd850fae6f9410405 /forensics/winfiles/WinPcap_3_1_beta_3.exe.Chopped

This at the very least proves that 95.79% of both the recovered file and the known copy of WinPcap_3_1_beta_3.exe are identical.

WinDump.exe

"WinDump is the porting to the Windows platform of tcpdump, the most used network sniffer/analyzer for UNIX. WinDump is fully compatible with tcpdump and can be used to watch and diagnose network traffic according to various complex rules. It can run under Windows 95/98/ME, and under Windows NT/2000/XP.

WinDump uses a libpcap-compatible library for Windows, WinPcap, which is freely downloadable from the WinPcap site. (http://windump.polito.it/)"

A copy of WinDump.exe was obtained from http://windump.polito.it/install/bin/windump_3_8_3_beta/WinDump.exe. A MD5SUM was taken of this file and recorded for future reference.

[*root@LinuxForensics winfiles]# md5sum WinDump.exe*
79375b77975aa53a1b0507496107bff7 WinDump.exe

The recovered file is then compared to the original binary. A MD5 hash was taken if the two files and compared:

[root@LinuxForensics recovered]# pwd
/forensics/images/recovered
[root@LinuxForensics recovered]# md5sum WinDump.exe
79375b77975aa53a1b0507496107bff7 WinDump.exe

The MD5SUMs of both files are identical.

Based on these results, it can be said with a degree of certainty that both files are identical.

Legal Implications

During the course of this investigation, evidence was uncovered that Mr. Lawrence has violated several laws and statutes in his pursuit of Ms. Conlay's affection. He not only harassed Ms. Conlay, but illegally obtained her private electronic transmissions, and used this data to ascertain here whereabouts on the evening of October 28th, 2004. This is evidenced by the presence of known packet capture software (WInDump), as well as a packet capture (_apture) that was found to be in the possession of Mr. Lawrence, as well as a map to Ms. Conlay's location (_ap.gif), with evidence of this location being present in the illegally obtained packet capture. The applicable laws that Mr. Lawrence has broken are as follows: