



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Advanced Incident Response, Threat Hunting, and Digital Forensics (Forensics
at <http://www.giac.org/registration/gcfa>



Forensic with Open-Source Tools and Platform:
USB Flash Drive Image Forensic Analysis

GIAC Certified Forensic Analyst
(GCFA)

Practical Assignment
Version 2.0
Option 1

SANS CDI East 2004
Washington, D.C.

Leonard Ong
GCIH, GAWN, CISM, CISA,
CISSP [ISSMP, ISSAP], PMP
March 20, 2005

Table of Contents

Abstract	3
Document Conventions	3
Executive Summary	4
Examination Detail	6
File Recovery	14
_ap.gif	15
_apture	15
Windump.exe	15
WinPcap 3 1 beta 3.exe	15
Image Details	16
Listing of all the files in the image	16
True name of programs/files used by Mr. Lawrence	16
MAC Time for files in the image	17
File Owners	17
File Sizes	17
MD5 Hash of Recovered Files	18
Keywords	18
Forensic Details	19
Windump.exe	19
WinPcap 3 1 beta 3.exe	19
Microsoft Word 10	19
_apture (Network capture) analysis	20
Microsoft MapPoint	22
Timeline	23
Program Identification	25
Windump.exe	25
WinPcap 3 1 beta 3.exe	25
Legal Implications	28
Law	28
Computer Misuse Act	28
Miscellaneous Offences (Public Order and Nuisance) Act	29
Penal code (Chapter 224)	29
Company Policies	29
Acceptable Use Policy	30
Ethics Policy	30
Email Policy	30
Recommendations	31
Additional Information	32
References	33
Appendix 1 – Investigation Time Line	34
Appendix 2 – File Recovery Flowchart	35
Appendix 3 – Step by Step Activities	36
Appendix 4 – MAC Timeline	43

List of Figures

Figure 1 Verifying image integrity	7
Figure 2 mmls output from image file	8
Figure 3 Using dcfldd to seperate each segment	8
Figure 4 Segments of image file	9
Figure 5 'file' command applied to image parts	10
Figure 6 Partition 1 in Hex Editor view	10
Figure 7 Partition 2 in Hex-editor view	10
Figure 8 Partition 3 in Hex-editor view	11
Figure 9 Files on file system	11
Figure 10 Robert's first email on Oct, 25 2004	12
Figure 11 Robert's second email dated Oct 26 2004	12
Figure 12 Robert's third email dated Oct 28	13
Figure 13 Retrieving Files from disk image	14
Figure 14 Comparing Retrieve files from file system and disk image	14
Figure 15 Recovered Image File	15
Figure 16 Metadata Information for Word Documents	16
Figure 17 Creating MAC time line	17
Figure 18 Recovered files size in bytes	17
Figure 19 MD5 hash of Recovered Files	18
Figure 20 Map generated from Microsoft MapPoint (left) and recovered Map (right)	22
Figure 21 Removing slack space	25
Figure 22 Both files have same data at end after recovered file removing slack	26
Figure 23 Differences before offset 19968	27
Figure 24 Common pattern	27
Figure 25 File Recovery Flowchart	35

Abstract

This paper is written to fulfill practical assignment version 2.0 (November 19, 2004) for GIAC Certified Forensic Analyst (GCFA). The first option from the assignment is selected, that is to analyze a USB flash drive image and report the findings.

The paper is structured according to recommended outline from practical assignment. Executive summary will be the first part of the report that will provide concise, clear, yet easy to understand findings of the investigation. The following sections will be examination details, image details, forensics details, program identification, and legal implications to Singapore laws. The concluding parts include recommendations and additional information.

The paper will use freely available tools and command line utilities. Therefore, it offers benefits to reader for their forensic efforts. The use of command line is to illustrate the function of tools rather than automated-GUI.

Document Conventions

When you read this practical assignment, you will see that certain words are represented in different fonts and typefaces. The types of words that are represented this way include the following:

<code>command</code>	Operating system commands are represented in this font style. This style indicates a command that is entered at a command prompt or shell.
<code>filename</code>	Filenames, paths, and directory names are represented in this style.
<code>computer output</code>	The results of a command and other computer output are in this style
<code>URL</code>	Web URL's are shown in this style.
<i>Qu ota tio n</i>	A citation or quotation from a book or web site is in this style.

Executive Summary

On October 29th 2004, Leila Conlay reported that she has been harassed by Robert Lawrence. Leila and Robert works at the same company, CC Terminals. She has been contacted by Mr. Lawrence through her personal email and the messages have been increasingly aggressive. Mr. Lawrence was reported to follow her on her personal appointment with a friend. Mark Mawer from corporate security requested a forensic investigation from an image derived from USB flash drive seized on after-hour search in Mr. Lawrence's cubicle.

From forensic investigation, it is gathered that there are three documents written by Mr. Lawrence directed to Ms. Conlay. The documents showed that Mr. Lawrence has been making advances to Ms. Conlay and got disappointed when his advances rejected. In increasing aggressiveness, he violated her privacy, local laws and company's policies by gaining information through unauthorized network sniffer. The information was used to follow her without consent.

The image contains three documents and several deleted files. The deleted files have been retrieved to find out the programs Mr. Lawrence used, and information that described unlawful activities. The existence of network sniffer application and required libraries, together with network capture, proved that Mr. Lawrence has been listening to Ms. Conlay's private communication. He derived the location of appointment that Ms. Conlay made with Mr. Guarillo, and generated an online map of the location. The last letter sent to Ms. Conlay stated that Mr. Lawrence was happened to be on the same coffee shop and he was very disappointed to see her met her friend.

The investigation has verified Ms. Conlay allegations against Mr. Lawrence. The paper will provide forensic analysis taken to arrive at the conclusion. Relevant organization policies and government statutes will also be discussed. The outcome of the case will depend on company's human resources department for disciplinary actions and/or offences if reported to enforcement agencies.

This case has also shown the company network is not secured and prone to information disclosure. The company should secure their network especially when it is wireless network with over-the-air communication.

Open source tools and platform is used in the investigation with detailed step-by-step analysis to provide high-confidence of the result with lowest possible cost.

© SANS Institute 2000 - 2005, Author retains full rights.

Examination Detail

Mark Mawer, Security Administrator, briefed me on Leila Conlay's report against Robert Lawrence. Leila made a report on October 29th to corporate security that she has been harassed by Robert. Robert has tried numerous attempts to meet her. He has also tried to contact Leila by her personal email address with increasing aggressiveness. One night before filing the report, Robert showed up while Leila was having a coffee with her friend.

Mark provided an image file, taken from Robert's USB flash drive, and asked for my assistance to analyze the image. A chain of custody was provided with the following information:

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

USB image available at:
<https://www.giac.org/GCFAPractical2.0-USBImageAndInfo.zip.gz>

Before forensic activities can be started, a suitable environment for forensic is needed. For this purpose, a secured room with biometric authentication is used. Access to the room is limited to investigator on the case, therefore eliminating any possible physical tampering from unauthorized parties. A laptop with clean hard drive was acquired along with supporting DVDs and CDs.

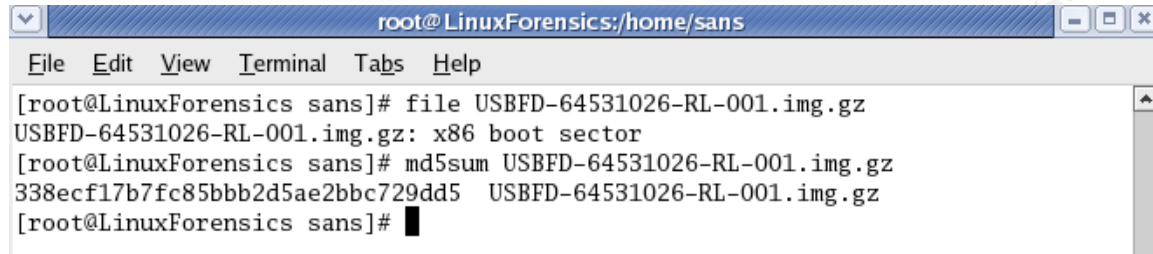
Chronological setup of forensic laptop is described at appendix 1. The principle is that the forensic laptop should have a high-confidence for its integrity. To achieve this purpose, cautious efforts are taken to ensure integrity of operating system media, forensics tools, and installations. The laptop is not connected with any networks. Operating System media was acquired from official mirror and verified against published MD5 hash. Media check is conducted before operating system installation started.

Acer TravelMate 803LCi with Fedora Core 3 operating system will be used for this investigation. Operating system was installed according the guide provided to prepare laptops for SANS Track 8 version 3.0¹.

The image is acquired by downloading from the URL given above to an empty USB drive using a different workstation. The drive later is used to transfer the image into a working folder in forensic workstation. One note to be taken into

¹ Forensics Installation Guide for Track 8 Student, Version 3.0. SANS. Online. Available from: http://www.sans.org/conference/forensic_install.pdf . Accessed on March 19, 2005

consideration, although the URL was accessible, the resulting download was 'USBFD-64531026-RL-001.img.gz' instead of 'GCFAPractical2.0-USBImageAndInfo.zip.gz'. The first action is to verify if the image has not been modified in anyway and still have the same checksum as chain of custody form.



```

root@LinuxForensics:/home/sans
File Edit View Terminal Tabs Help
[root@LinuxForensics sans]# file USBFD-64531026-RL-001.img.gz
USBFD-64531026-RL-001.img.gz: x86 boot sector
[root@LinuxForensics sans]# md5sum USBFD-64531026-RL-001.img.gz
338ecf17b7fc85bbb2d5ae2bbc729dd5  USBFD-64531026-RL-001.img.gz
[root@LinuxForensics sans]#

```

Figure 1 Verifying image integrity

The two commands above shows that the file has x86 boot sector signature, which mean the file is an image file and is not compressed, despite the filename extension. A MD5 checksum test verifies that the file has the same hash provided by Mark in chain of custody form. By comparing MD5 checksum, we have a high-level confidence that the two files are identical and not tampered with.

Tools used based on the order of usage:

No.	Tool Name	Version	Description
1.	file*	4.10	Describes type of a file based on "magic" signature file.
2.	md5sum*	5.2.1	Calculates MD5 hash from an input
3.	The Sleuth Kit (TSK)	1.72	Collection of forensic tools
4.	mmls	1.72	Part of TSK. Reads primary and extended partition table.
5.	dcfldd	1.0	Improved version of 'dd'. A versatile tool to create bit-image, split, truncate data from disk blocks
6.	fsstat	1.72	Part of TSK. Provides information on file system
7.	kHexEdit*	0.8.5	Part of KDE 3.3.0-5. GUI-based Hex Editor
8.	mount*	2.12a	Mount an image file/file system into a folder
9.	OpenOffice.org Writer*	1.1.2	Part of OpenOffice suite. Word processor that is compatible with Microsoft Word.
10.	fls	1.72	Part of TSK. Displays file entries in a directory inode.
11.	istat	1.72	Part of TSK. Displays information about a specific node
12.	Eye of Gnome	2.8.0	Part of GNOME. Image viewer
13	mactime	N/A	Script that will generate MAC timeline

(* included in Fedora Core 3 OS)

As we have established the integrity of image file, the next step is to start looking inside the image. The image contains one or more file system, and to find out partition tables in the image, 'mmls' tool will be used.

```

root@LinuxForensics:/home/sans
File Edit View Terminal Tabs Help
[root@LinuxForensics sans]# mmls -t dos USBFD-64531026-RL-001.img.gz
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)
[root@LinuxForensics sans]#

```

Figure 2 mmls output from image file

```

root@LinuxForensics:/home/sans
File Edit View Terminal Tabs Help
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)
[root@LinuxForensics sans]# dcfldd count=1 hashwindow=0 if=USBFD-64531026-RL-001
.img.gz of=USBFD-64531026-RL-001.img.part1

Total: 5bf1cea807dec8655ed18b9bbf2ee918
1+0 records in
1+0 records out
[root@LinuxForensics sans]# dcfldd skip=1 count=31 hashwindow=0 if=USBFD-6453102
6-RL-001.img.gz of=USBFD-64531026-RL-001.img.part2

Total: 51596dda30fc38f0df3556d6f115256d
31+0 records in
31+0 records out
[root@LinuxForensics sans]# dcfldd skip=32 count=121950 hashwindow=0 if=USBFD-64
531026-RL-001.img.gz of=USBFD-64531026-RL-001.img.part3
121856 blocks (59Mb) written.
Total: ac666df2072927fb9b0047886f0e2385
121920+0 records in
121920+0 records out

```

Figure 3 Using dcfldd to separate each segment

Based on 'mmls' result, there are three distinct segments. From the information, we could break the image into three different files using dcfldd. dcfldd is an improved 'dd' that allows us to grab data from disk image. Breaking a full image into several smaller images will help to break forensic work into manageable pieces, especially in a very large image with many partitions.

No.	File name	Size (bytes)	Hash and Segment Type
1.	USBFD-64531026-RL-001.img.gz	62,439,424	338ecf17b7fc85bbb2d5ae2bbc729dd5 (Main Image)
2.	USBFD-64531026-RL-001.img.part1	512	5bf1cea807dec8655ed18b9bbf2ee918 (Primary table #0)
3.	USBFD-64531026-RL-001.img.part2	15,872	51596dda30fc38f0df3556d6f115256d (Unallocated)
4.	USBFD-64531026-RL-001.img.part3	62,423,040	ac666df2072927fb9b0047886f0e2385 (DOS FAT16)

Figure 4 Segments of image file

fsstat tool is used to gain more information on the partition of last image part. From this output alone there, we can get many information such as: no label on the drive, FAT area, root area, data area, sectors and clusters information. There are also 3 files that is currently listed in FAT occupying 40 sectors or about 20 Kbytes each. The tool does not list file that has been deleted. The command is

```
[root@LinuxForensics sans]# fsstat -f fat16 USBFD-64531026-RL-001.img.part3 > USBFD-64531026-RL-001.img.part3.fsstat
```

<p>FILE SYSTEM INFORMATION</p> <p>-----</p> <p>File System Type: FAT</p> <p>OEM Name: MSWIN4.1</p> <p>Volume ID: 0x0</p> <p>Volume Label (Boot Sector): NO NAME</p> <p>Volume Label (Root Directory):</p> <p>File System Type Label: FAT16</p> <p>Sectors before file system: 32</p> <p>File System Layout (in sectors)</p> <p>Total Range: 0 - 121918</p> <p>* Reserved: 0 - 0</p> <p>** Boot Sector: 0</p> <p>* FAT 0: 1 - 239</p> <p>* FAT 1: 240 - 478</p> <p>* Data Area: 479 - 121918</p> <p>** Root Directory: 479 - 510</p> <p>** Cluster Area: 511 - 121918</p>	<p><i>(Continued)</i></p> <p>METADATA INFORMATION</p> <p>-----</p> <p>Range: 2 - 1942530</p> <p>Root Directory: 2</p> <p>CONTENT INFORMATION</p> <p>-----</p> <p>Sector Size: 512</p> <p>Cluster Size: 1024</p> <p>Total Cluster Range: 2 - 60705</p> <p>FAT CONTENTS (in sectors)</p> <p>-----</p> <p>511-550 (40) -> EOF</p> <p>551-590 (40) -> EOF</p> <p>591-630 (40) -> EOF</p>
---	--

Running 'file' command to the three segments shows that the first segment most likely does not contain anything of interest, while second and third segment worth looking.

```

root@LinuxForensics:/home/sans
File Edit View Terminal Tabs Help

[root@LinuxForensics sans]# file USBFD-64531026-RL-001.img.part1
USBFD-64531026-RL-001.img.part1: x86 boot sector
[root@LinuxForensics sans]# file USBFD-64531026-RL-001.img.part2
USBFD-64531026-RL-001.img.part2: data
[root@LinuxForensics sans]# file USBFD-64531026-RL-001.img.part3
USBFD-64531026-RL-001.img.part3: x86 boot sector, code offset 0x3c, OEM-ID "MSWI
N4.1", sectors/cluster 2, root entries 512, Media descriptor 0xf8, sectors/FAT 2
39, heads 17, hidden sectors 32, sectors 121919 (volumes > 32 MB) , serial numbe
r 0x0, unlabeled, FAT (16 bit)
[root@LinuxForensics sans]#

```

Figure 5 'file' command applied to image parts

A quick look in hex editor (kHexEdit) shows that the first segment is just a boot sector. Second segment contains '00' and nothing else, which mean this is really unallocated data, and never been used before. Therefore, the second segment is not interesting for us to continue investigating. The last one is full of interesting texts.

```

file:/home/sans/USBFD-64531026-RL-001.img.part1 - KHexEdit
File Edit View Documents Bookmarks Tools Settings Help

0000:0000  3Ä.Ð¼. |ûP.P.û¼. |¿..PW¹ä.ó¼½¼. ±.8n. |.u..Ä.äóÍ..ö.Æ.It.8,tô µ.´..
0000:0040  ð¬<.tü»... Í.ëò.N.èF.s*þF...~.t...~.t. ¶.uò.F...F...V..è!.s. ¶.ë
0000:0080  ¼.>þ}U*t...~.tÈ .ë©.û.W.ðÈ¿...V.´.Í.r#.Ä$?...þ.ûC÷ä.Ñ.Ö±.òìB÷â9V
0000:00c0  .w#r.9F.s.,...|.N..V.Í.sQotN2ä.V.Í.ëä.V.´»ªU´AÍ.r6.ûUªu0öÄ.t+a`
0000:0100  j.j.ÿv.ÿv.j.h.|j.j.´B.ôÍ.aas.Ot.2ä.V.Í.ëöauÄInvalid partition ta
0000:0140  ble.Error loading operating system.Missing operating system.....
0000:0180  .....Dc...Ä...
0000:01c0  .... ù ...?Ü.....Uª
0000:0200

Hex  Find  Backwards  Ignore case

```

Figure 6 Partition 1 in Hex Editor view

```

file:/home/sans/USBFD-64531026-RL-001.img.part2 - KHexEdit
File Edit View Documents Bookmarks Tools Settings Help

0000:0000  .....
0000:0040  .....
0000:0080  .....
0000:00c0  .....
0000:0100  .....
0000:0140  .....
0000:0180  .....
0000:01c0  .....
0000:0200  .....
0000:0240  .....
0000:0280  .....
0000:02c0  .....
0000:0300  .....

Hex  Find  Backwards  Ignore case

```

Figure 7 Partition 2 in Hex-editor view

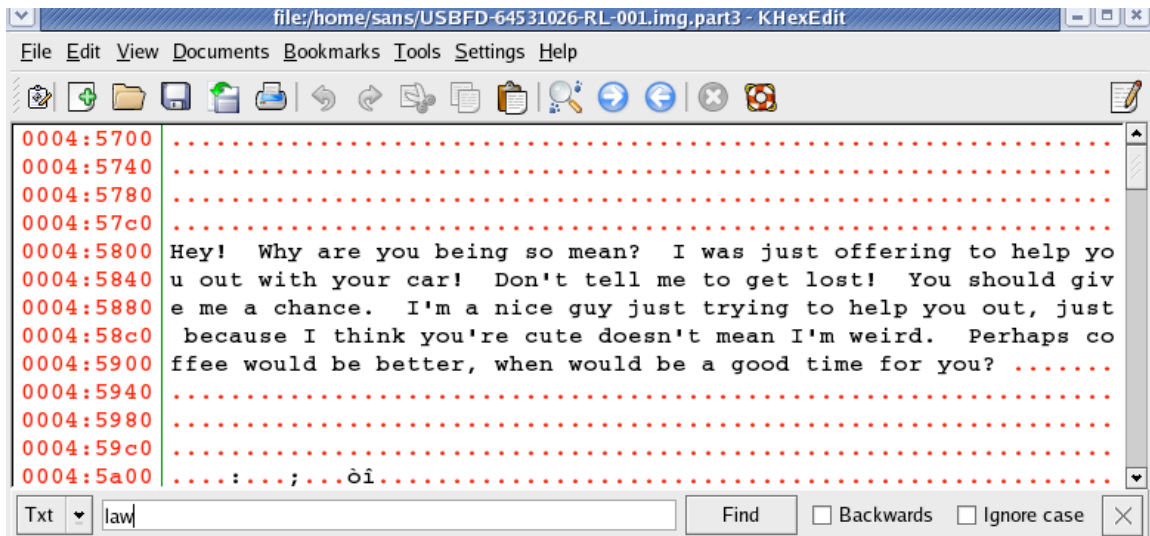


Figure 8 Partition 3 in Hex-editor view

As we find that third part of the image contains interesting files, we should try to mount it and get the files. There are several parameters that have to be specified while trying to mount an image, read-only to maintain integrity, no execution allowed to safeguard forensic workstation from potential malicious code, and no time modification. Only with these parameters, image integrity and the data obtained from therein will be forensically-sound.

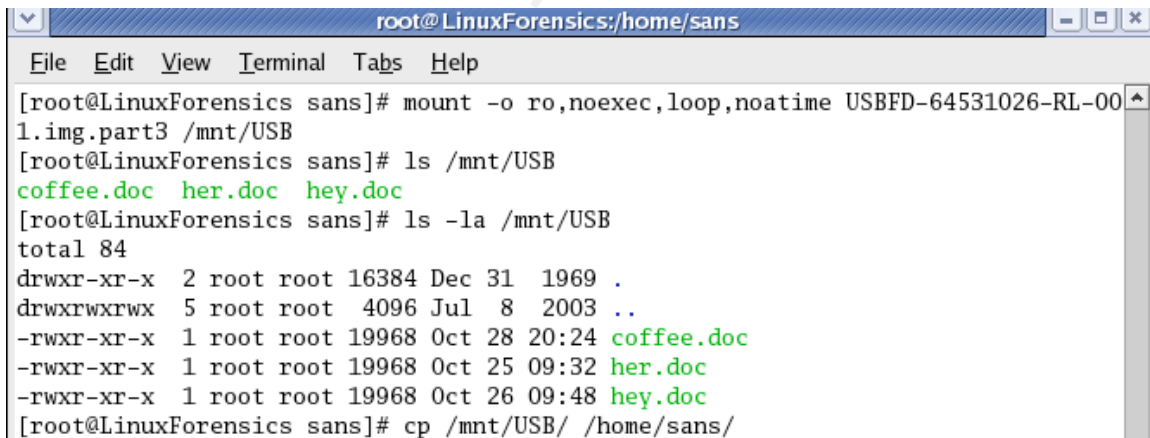


Figure 9 Files on file system

As we have established a read-only access, we should copy the files into a working folder and further analyze the files from there. The word document is opened one by one using OpenOffice Writer, and document contents with author name could be seen as follows:

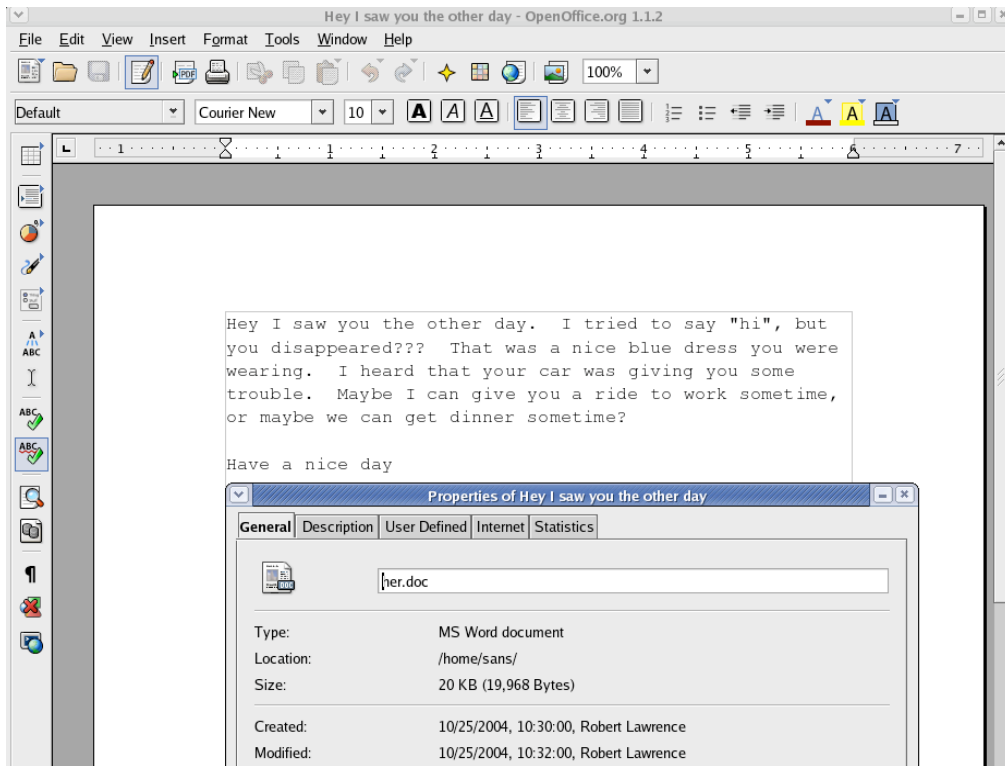


Figure 10 Robert's first email on Oct, 25 2004

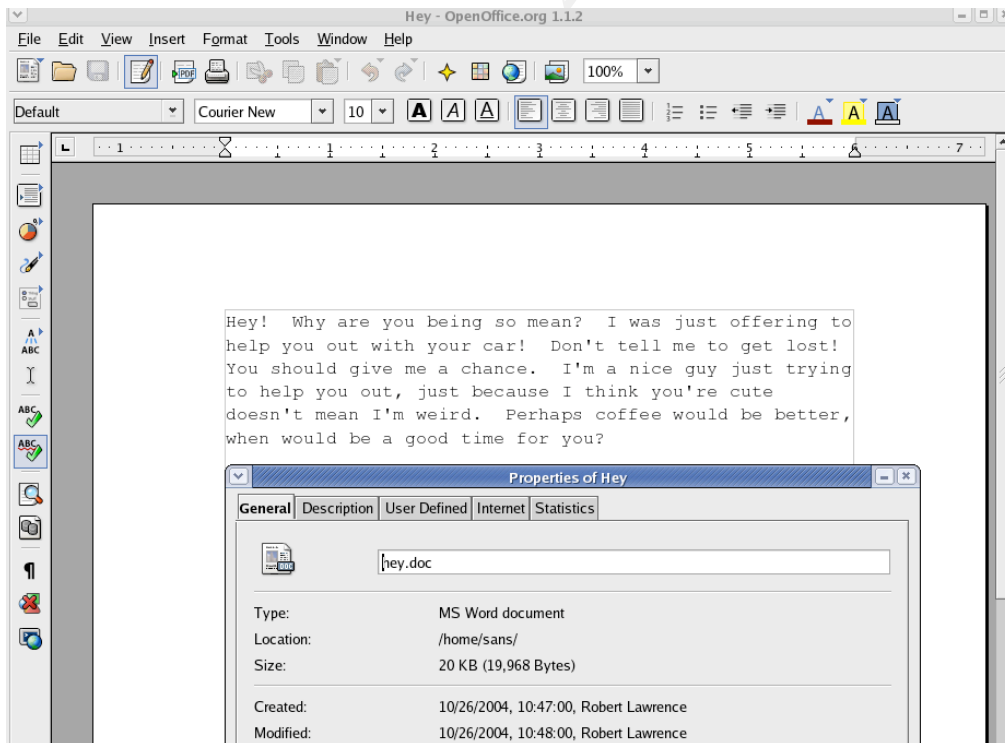


Figure 11 Robert's second email dated Oct 26 2004

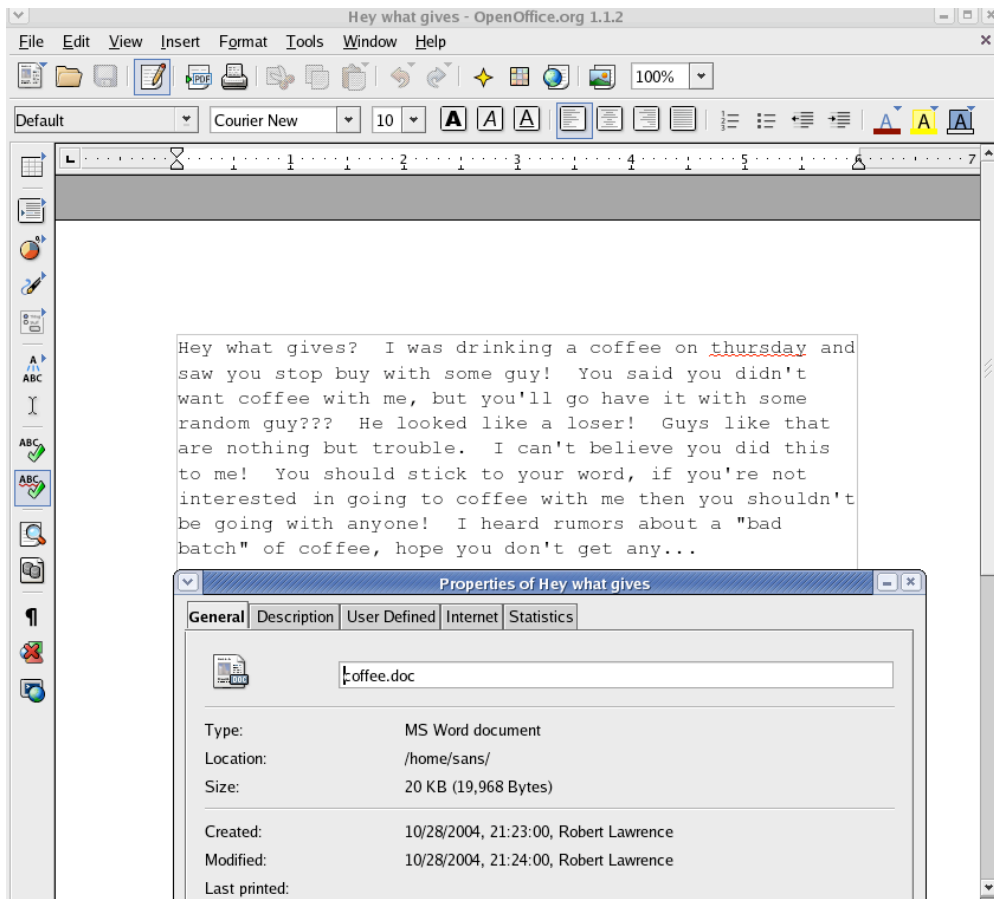
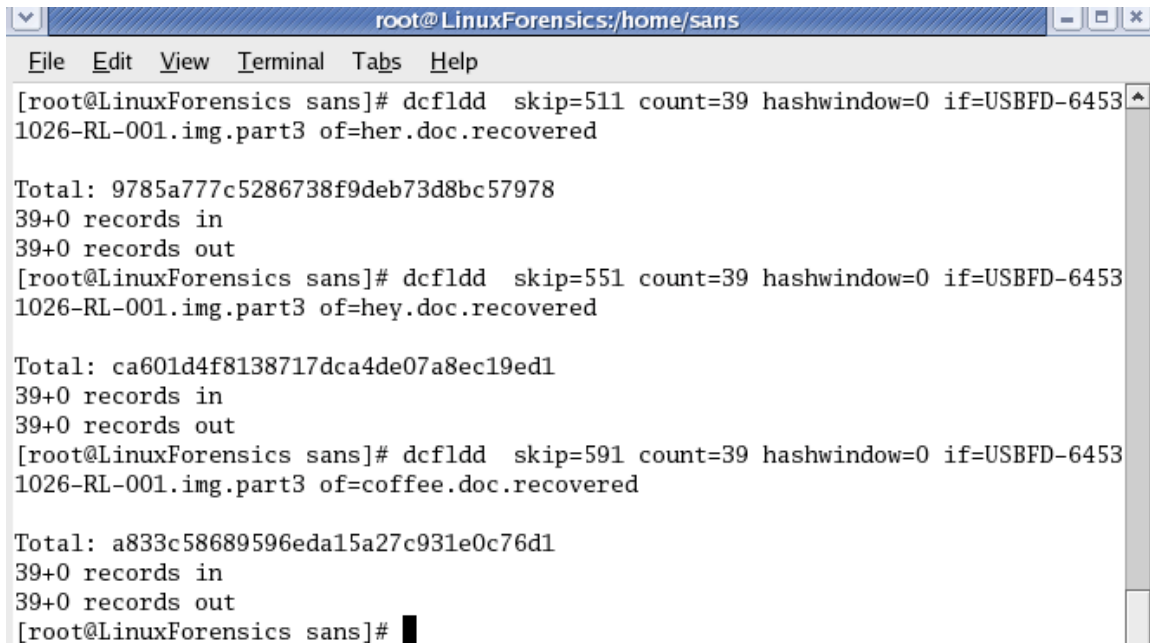


Figure 12 Robert's third email dated Oct 28

At this point, we have obtained some significant evidence that Mr. Lawrence has written emails consistent with Ms. Conlay's report. He tried to write her email with aggressive contents and did mention about Ms. Conlay's meeting with her friend. Despite the facts, we have to gather more information to further verify if Mr. Lawrence sent the email to her, and how he did it.

Let's approach the case further using command-line utilities provided by The Sleuth Kit tools version 1.72.

The first tool we will use is 'fls' to see the file system layer of the partition, and followed by 'istat' to find more information on the starting inode of the file. From the information gathered we can then carve out the files manually. A few examples is shown here, the complete steps can be read at appendix 3.



```

root@LinuxForensics:/home/sans
File Edit View Terminal Tabs Help
[root@LinuxForensics sans]# dcfldd skip=511 count=39 hashwindow=0 if=USBFD-6453
1026-RL-001.img.part3 of=her.doc.recovered

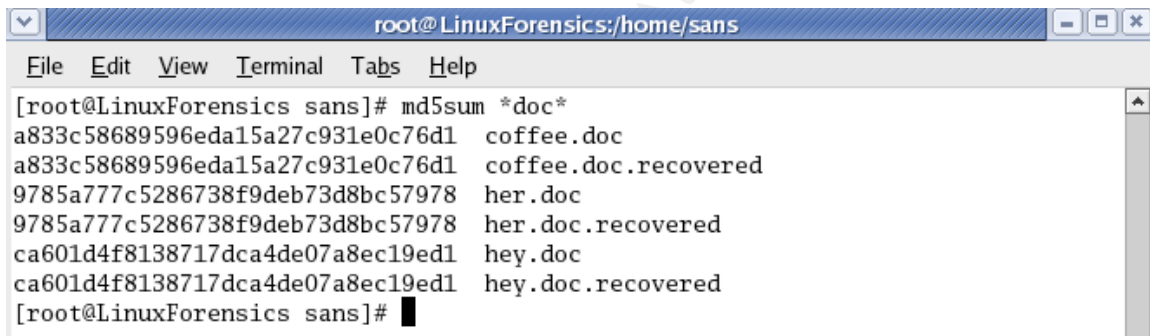
Total: 9785a777c5286738f9deb73d8bc57978
39+0 records in
39+0 records out
[root@LinuxForensics sans]# dcfldd skip=551 count=39 hashwindow=0 if=USBFD-6453
1026-RL-001.img.part3 of=hey.doc.recovered

Total: ca601d4f8138717dca4de07a8ec19ed1
39+0 records in
39+0 records out
[root@LinuxForensics sans]# dcfldd skip=591 count=39 hashwindow=0 if=USBFD-6453
1026-RL-001.img.part3 of=coffee.doc.recovered

Total: a833c58689596eda15a27c931e0c76d1
39+0 records in
39+0 records out
[root@LinuxForensics sans]#

```

Figure 13 Retrieving Files from disk image



```

root@LinuxForensics:/home/sans
File Edit View Terminal Tabs Help
[root@LinuxForensics sans]# md5sum *doc*
a833c58689596eda15a27c931e0c76d1 coffee.doc
a833c58689596eda15a27c931e0c76d1 coffee.doc.recovered
9785a777c5286738f9deb73d8bc57978 her.doc
9785a777c5286738f9deb73d8bc57978 her.doc.recovered
ca601d4f8138717dca4de07a8ec19ed1 hey.doc
ca601d4f8138717dca4de07a8ec19ed1 hey.doc.recovered
[root@LinuxForensics sans]#

```

Figure 14 Comparing Retrieve files from file system and disk image

We have seen that by carving out the files, we have identical files compared to the files copied by mounting the partition. This would confirm that the files are not modified with certain manipulation on file system level. One note to take is although the length shown as 40 sectors, the real data is stored in 39 sectors. The reason for rounding to additional sector is that cluster in this file system is 2, so each file should have sectors allocated by multiple of two. 'fls' is smart enough to provide us with the real file size of 19968 bytes or 39 sectors.

File Recovery

'fls' result provided an important clue that there are deleted files. File recovery using the same method is needed to recover the file. Flowchart for file recovery using freely available tool is described in appendix 2. Readers are recommended to go through appendix 3 for command used and information obtained. Summary of these findings will be presented in main section of this paper.

_ap.gif

From 'fls' output, it is clear that the file most probably is a GIF picture file. After retrieving the file using dcfldd, on inode entry 17 sectors 2525 to 2541, the file is viewed using Eye of Gnome 2.8.0 from Fedora Core 3.0. It has 300x200 pixel resolution, and was made by Microsoft MapPoint. The highlighted place is an intersection that may be useful in our next section.

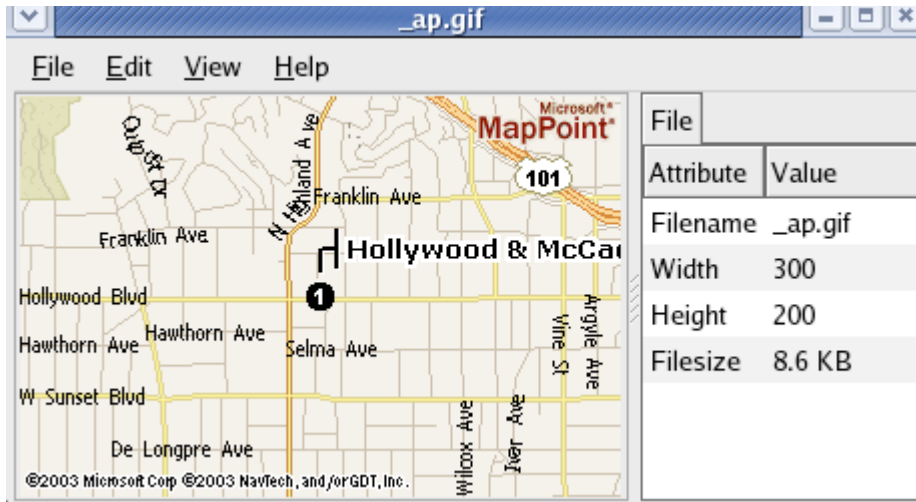


Figure 15 Recovered Image File

```
[root@LinuxForensics recovered]# file _ap.gif
_ap.gif: GIF image data, version 89a, 300x200
```

_apture

'fls' indicated that this deleted files has inode entry of 15, with size of 53,056 bytes and occupying sector 2421-2524. The file type is tcpdump capture format made with version 2.4. Further analysis will be conducted to see the traffic information at next section.

```
[root@LinuxForensics recovered]# file _apture
_apture: tcpdump capture file (little-endian) - version 2.4
Ethernet, capture length 4096)
```

Windump.exe

Discussed in Program Identification section.

WinPcap_3_1_beta_3.exe

Discussed in Program Identification section.

Image Details

Listing of all the files in the image

Based on the previous section, the files on the image are as follows:

```
[root@LinuxForensics recovered]# ls -l
total 3296
-rw-r--r--  1 root root   8814 Mar 20 01:04 _ap.gif
-rw-r--r--  1 root root  53056 Mar 20 01:02 _apture
-rwxr-xr-x  1 root root  19968 Mar 19 14:06 coffee.doc
-rwxr-xr-x  1 root root  19968 Mar 19 14:06 her.doc
-rwxr-xr-x  1 root root  19968 Mar 19 14:06 hey.doc
-rw-r--r--  1 root root 450560 Mar 20 01:08 windump.exe
-rw-r--r--  1 root root 486400 Mar 20 01:16 WinPcap_3_1_beta_3.exe
```

True name of programs/files used by Mr. Lawrence

Previous section has discussed files recovered one by one and their details. Let's summarize the result on the following table:

No.	Recovered File Name	Real File Name	Program Name	Description
1.	_ap.gif	map.gif	Microsoft MapPoint	Location Map
2.	_apture	capture	Windump/tcpdump	Traffic capture
3.	coffee.doc	coffee.doc	Microsoft Office 10	Document
4.	her.doc	her.doc	Microsoft Office 10	Document
5.	hey.doc	hey.doc	Microsoft Office 10	Document
6.	windump.exe	windump.exe	Windump v.3.8.3	Sniffer windows-based
7.	WinPcap_3_1_beta_3.exe	WinPcap_3_1_beta_3.exe	WinPcap Library v3.1.Beta3	Packet capture library for windump/tcpdump

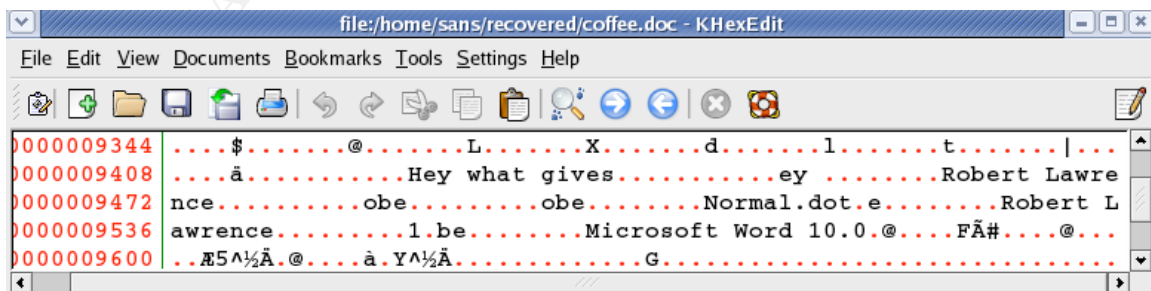
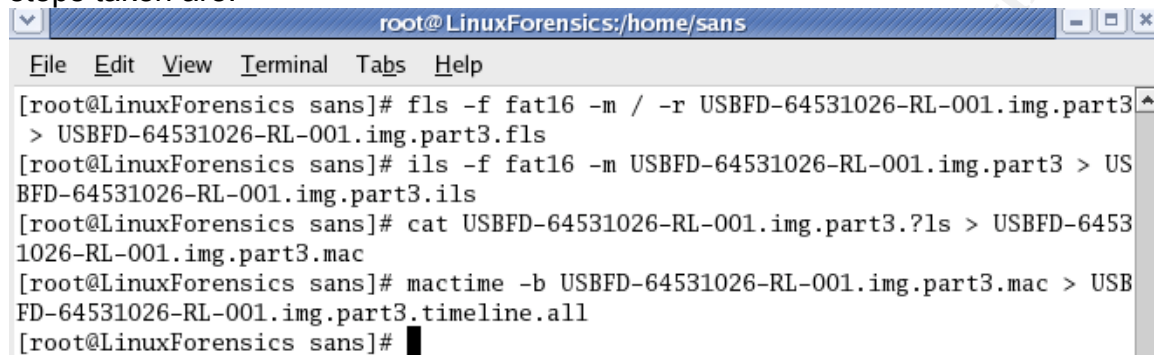


Figure 16 Metadata Information for Word Documents

MAC Time for files in the image

MAC timeline can be derived from the following tools: fls, ils and mactime. The steps taken are:



```

root@LinuxForensics:/home/sans
File Edit View Terminal Tabs Help
[root@LinuxForensics sans]# fls -f fat16 -m / -r USBFD-64531026-RL-001.img.part3
> USBFD-64531026-RL-001.img.part3.fl
[root@LinuxForensics sans]# ils -f fat16 -m USBFD-64531026-RL-001.img.part3 > US
BFD-64531026-RL-001.img.part3.ils
[root@LinuxForensics sans]# cat USBFD-64531026-RL-001.img.part3.?ls > USBFD-6453
1026-RL-001.img.part3.mac
[root@LinuxForensics sans]# mactime -b USBFD-64531026-RL-001.img.part3.mac > USB
FD-64531026-RL-001.img.part3.timeline.all
[root@LinuxForensics sans]#

```

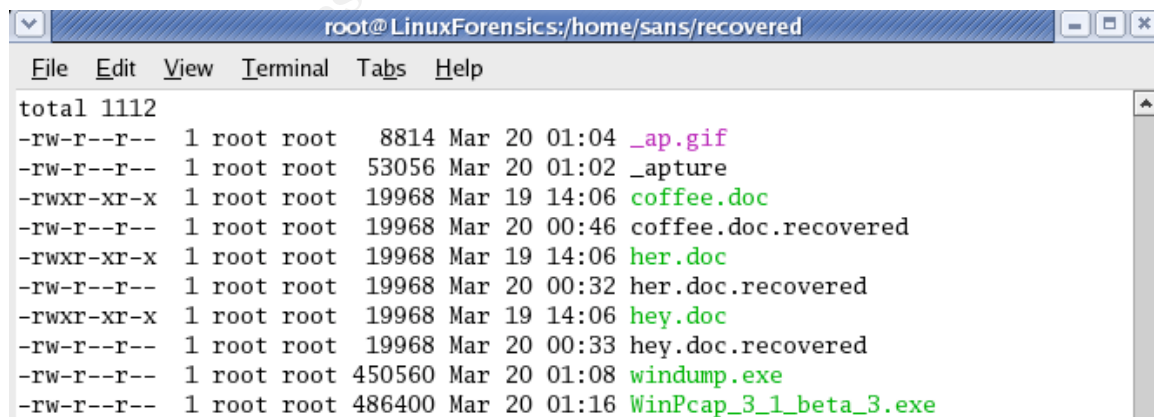
Figure 17 Creating MAC time line

The output of these commands is available at appendix 4. Descriptions of these tools are available at Examination Details section.

File Owners

FAT file systems do not have a concept of ownership and groups. Therefore, it can't be determined from file system metadata alone who owns the files. The image was derived from USB flash drive belonging to Mr. Lawrence located at his cubicle, and word files contain his name as the author. The facts presented themselves that Mr. Lawrence owns the files.

File Sizes



```

root@LinuxForensics:/home/sans/recovered
File Edit View Terminal Tabs Help
total 1112
-rw-r--r-- 1 root root 8814 Mar 20 01:04 _ap.gif
-rw-r--r-- 1 root root 53056 Mar 20 01:02 _apture
-rwxr-xr-x 1 root root 19968 Mar 19 14:06 coffee.doc
-rw-r--r-- 1 root root 19968 Mar 20 00:46 coffee.doc.recovered
-rwxr-xr-x 1 root root 19968 Mar 19 14:06 her.doc
-rw-r--r-- 1 root root 19968 Mar 20 00:32 her.doc.recovered
-rwxr-xr-x 1 root root 19968 Mar 19 14:06 hey.doc
-rw-r--r-- 1 root root 19968 Mar 20 00:33 hey.doc.recovered
-rw-r--r-- 1 root root 450560 Mar 20 01:08 windump.exe
-rw-r--r-- 1 root root 486400 Mar 20 01:16 WinPcap_3_1_beta_3.exe

```

Figure 18 Recovered files size in bytes

MD5 Hash of Recovered Files

```
[root@LinuxForensics recovered]# md5sum *
9bc3923cf8e72fd405d7cea8c8781011 _ap.gif
2097b7b0a9fedb4238b67e976c4ae1cb _apture
a833c58689596eda15a27c931e0c76d1 coffee.doc
a833c58689596eda15a27c931e0c76d1 coffee.doc.recovered
9785a777c5286738f9deb73d8bc57978 her.doc
9785a777c5286738f9deb73d8bc57978 her.doc.recovered
ca601d4f8138717dca4de07a8ec19ed1 hey.doc
ca601d4f8138717dca4de07a8ec19ed1 hey.doc.recovered
79375b77975aa53a1b0507496107bff7 windump.exe
3c6144401664d5c8567b36c0c7f01731 WinPcap_3_1_beta_3.exe
[root@LinuxForensics recovered]#
```

Figure 19 MD5 hash of Recovered Files

Keywords

To generate keywords from the image, 'strings' command will be used. The tool with `--radix=d` parameter will present any human-readable word of four characters or more. For a quick and dirty search on a media image, strings normally coupled with pre-defined interesting keywords to search. On a very large image, it will help to pin-point certain important information.

```
[root@LinuxForensics recovered]# strings -radix=d ../USBFD-64531026-RL-001.img.part3 > USBFD-64531026-RL-001.img.str
```

Forensic Details

Based on information previously gathered in our first two sections, we have leads that Mr. Lawrence used Windump, WinPcap library, Microsoft MapPoint. We will discuss in more details how Mr. Lawrence used the programs.

Windump.exe

Windump is a win32 port of well-known sniffer tcpdump. A sniffer is a program that listens to all network traffic. It will need WinPcap library to get access to raw network data. WinPcap will be discussed in the next sub-section. Although there are many sniffers for windows platform, windump is free open-source that does not cost anything and the syntax almost the same as tcpdump. Users of tcpdump will find windump very familiar. Windump homepage is at <http://windump.polito.it/> (unreachable on March 20, 2005), and mirrored at <http://windump.mirror.ethereal.com/>. Windump.exe that was recovered is version 3.8.3 (May 03, 2004), and is the current version. MD5 hash proved that recovered windump.exe exactly the same as the one available at official websites.

Mr. Lawrence copied/downloaded windump.exe on Oct 27th, 2004 16:24:04 and the last time windump used was on Oct 28th, 2004. This information is derived from MAC timeline on appendix 4.

WinPcap_3_1_beta_3.exe

WinPcap is an architecture for packet capture and network analysis for win32 platform. It includes a kernel-level packet filter, a low-level dynamic link library (packet.dll), and a high-level and independent library (wpcap.dll)². The official page for the program is <http://winpcap.polito.it> (unreachable on March 20, 2005), and mirrored at <http://winpcap.mirror.ethereal.com>. Ethereal will need the libraries to function.

The recovered file was WinPcap version 3.1.Beta3, and the latest version is Beta4. Mr. Lawrence copied/downloaded the file on Oct 27th 2004 16:23:54 and used it last on Oct 28th 2004.

Microsoft Word 10

Mr. Lawrence typed three word documents with content relevant to Ms. Conlay's report. The last time the program was used is to create coffee.doc file on Oct 28th, 2004 19:24:48. Microsoft word is a word processor and part of Microsoft Office suite. Within the word documents' metadata, Mr. Lawrence name was found.

² <http://winpcap.mirror.ethereal.com/default.htm>

apture (Network capture) analysis

We have analyzed most part of the file system, except the network capture file. Logically the filename may be 'capture'. FAT file system removes first character of a file name when it is deleted. To analyze the file, ethereal 0.10.6 is used to load up the file.

As we are concerned about MAC time line in this forensic effort, the time column needs to be changed to absolute time rather than relative. To do this, in Ethereal, View -> Time Display Format -> Date and Time of the Day. Ethereal is now ready for us to do analysis.

The first packet seems to be a common connection between a local host to a public web server in the Internet. Following TCP Stream feature in Ethereal can be used to compile the information in this connection into a human readable format. Filter: (ip.addr eq 192.168.2.104 and ip.addr eq 64.4.34.250) and (tcp.port eq 2038 and tcp.port eq 80).

```
POST /cgi-bin/premail/2452 HTTP/1.1
(post – sending information to webserver)
Referer: http://by12fd.bay12.hotmail.msn.com/cgi-bin/compose?&curmbox=F000000001&a=27d6f510deac1bac5415e72029263cd9
(previous page was 'compose' page, where Ms. Conlay write her email)
<snip>
curmbox=F000000001&HrsTest=&_HMaction=Send&FinalDest=&subaction=&plaintext=&login=flowergirl96&msg=&start=&len=&attfile=&attlistfile=&eurl=&type=&src=&ref=&ru=&msgid=b16479b18beec291196189c78555223c_1098692452&RTEbgcolor=&encodedto=SamGuarillo@hotmail.com&encodedcc=&encodedbcc=&deleteUponSend=0&importance=&sigflag=&newmail=new&to=SamGuarillo@hotmail.com&cc=&bcc=&subject=RE%3Acoffee&body=Sure%2C+coffee+sound+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-LeilaHTTP/1.1 100 Continue
(Email from 'flowergirl96', recipient is 'SamGuarillo@hotmail.com', Subject 'RE: coffee', and email body)
<Snip>
<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/hotmail_____
(Confirming message has been sent)
<Snip>
```

Let's look again at the information contain in the TCP stream above. The activity shows that Ms. Conlay (flowergirl96@hotmail.com) was sending an email, through her hotmail mailbox, to Sam Guarillo (SamGuarillo@hotmail.com) with subject 'RE: Coffee'. The subject would indicate that Ms. Conlay was replying to

Mr. Guarillo invitation to have a coffee. The content of the email tells us that Ms. Conlay agreed to the invitation and will be meeting Mr. Guarillo at a coffee shop on corner of Hollywood and McCadden at 7 PM.

From: flowergirl96@hotmail.com
 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

A reconstruction of email sent. To facilitate the reconstruction, the email format in HTML format decoded manually. A few useful and commonly used codes are + for space, %0A and %0D for new line. All other ASCII table can be found at <http://www.lookuptables.com/>

The rest of the traffic can be filtered using negation of above filter:

```
!( (ip.addr eq 192.168.2.104 and ip.addr eq 64.4.34.250) and
(tcp.port eq 2038 and tcp.port eq 80))
```

There are SNMP traps that are unusual as they broadcast the log to local segment rather than to a specific host. This can indicate either a misconfiguration on web-interface that logging host is set to broadcast address or unauthorized modification. There is no sufficient information to prove/disprove the cause.

MAC addresses view in Ethereal provided another valuable information that the gateway is a LinksysG, which most likely a wireless router 802.11g. Client on the network uses MAC from GemTek (<http://www.gemtek.com.tw>). The company does not offer any wired NIC adapter, but total wireless solution offering. Therefore, it can be concluded that the capture was done for over-the-air traffic.

No.	IP address	Mac Addr.	FQDN	Note
1	192.168.2.1	00:0c:41:50:29:2c	N/A	Default Gateway. LinksysG
2	192.168.2.104	00:90:4b:5e:e3:cf	N/A	Ms. Conlay's
3	192.168.2.255	ff:ff:ff:ff:ff:ff	N/A	Broadcast address
4	64.4.34.250	N/A (Default GW)	www.bay12.hotmail.com	Hotmail server
5	207.68.178.16	N/A (Default GW)	rad.msn.com	MSN Ad server
6	207.68.177.124	N/A (Default GW)	h.msn.com	MSN Ad server
7	63.209.188.62	N/A (Default GW)	Unknown.level3.net	Banner server
8	216.73.86.40	N/A (Default GW)	annyadvip2.doubleclick.net	DoubleClick Ad server
9	64.166.13.75	N/A (Default	N/A	Unknown

		GW)		
--	--	-----	--	--

Most the other network packets and the servers listed on the table are insignificant, as they indicate extra connections from Ms. Conlay's activity on hotmail. Web-based email normally came with advertising banners and this was what exactly happened.

The fact that Mr. Lawrence has obtained information on Ms. Conlay's appointments, personal email addresses confirmed that Mr. Lawrence has prior knowledge and grounds for showing up on the coffee shop. He later sent coffee.doc document describing his observation on the coffee shop. Although from available information, we can't see that Mr. Lawrence did sent Ms. Conlay the emails, this can easily reproduced upon request to Ms. Conlay.

Microsoft MapPoint

MapPoint is a technology from Microsoft that provides business mapping, navigation and integration with Microsoft office for business intelligence. One product for end-users market is Microsoft Streets&Trips 2005, Pocket Streets 2005 and MSN Maps&Directions (online). It is also offered online at <http://mappoint.msn.com>. Mr. Lawrence was known to use Microsoft MapPoint from the upper-right mark 'Microsoft MapPoint' on _ap.gif. Mr. Lawrence could have use the service to get a map of meeting location and save the map into USB flash drive.

A quick check on Google for 'McCadden Hollywood', provided information that the place is in CA state. Using the available information, we can reproduce how Mr. Lawrence got his map.

1. Browse to <http://mappoint.msn.com>
2. Enter 'Hollywood & McCadden' on Street Address
3. Enter state 'CA' (Either Zip Code, City, or State is needed)
4. Mappoint will suggest a short listed location, in this case one option
5. Voila ! the exact location with recovered Map with correct magnification.

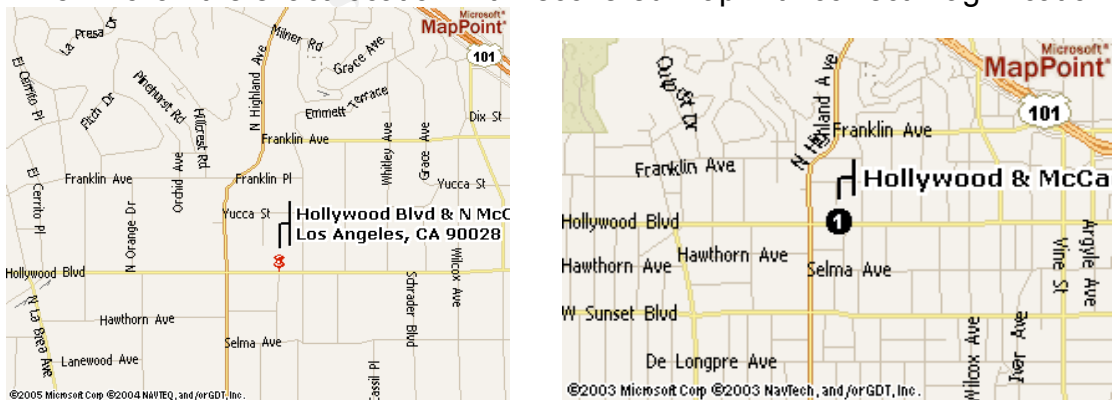


Figure 20 Map generated from Microsoft MapPoint (left) and recovered Map (right)

[http://mappoint.msn.com/\(fs2ptp55gebxxk255f3g5s245\)/map.aspx?L=USA&C=34.10157%2c-118.33695&A=7.16667&P=|34.10157%2c-](http://mappoint.msn.com/(fs2ptp55gebxxk255f3g5s245)/map.aspx?L=USA&C=34.10157%2c-118.33695&A=7.16667&P=|34.10157%2c-)

118.33695|1|Hollywood+Blvd+%26+N+McCadden+Pl%2c+Los+Angeles%2c+CA+90028|L1|

Timeline

MAC timeline has been generated and can be found at Appendix 4. The timeline on this section is to reconstruct what may have happened as follows:

No	Date	Time	Events
1	Oct 25	08:32:08	Mr. Lawrence accessed her.doc for the last time. It may be so that the letter was sent to Ms. Conlay. The email contains a greeting and some personal observation to Ms. Conlay. He also offered a ride and a dinner to her.
2	Oct 26	08:48:10	Mr. Lawrence accessed hey.doc for the last time. It is also presume that the letter may be sent to Ms. Conlay. He expressed his disappointment to her rejection (on his first offer). He tried to defend himself and invite her for a coffee.
3	Oct 27	16:23:54	WinPcap_3_1_Beta_3.exe download/copy to USB flash drive started
4		16:23:56	WinPcap_3_1_Beta_3.exe download/copy was completed
5		16:24:04	Windump.exe download/copy to USB flash drive started
6		16:24:06	Windump.exe download/copy to USB flash drive completed
7	Oct 28	Before 11:08:24	WinPcap_3_1_Beta_3.exe was accessed for installation.
8			Windump.exe was started
9		11:08:24	_apture file created
10		11:11:00	_apture file written (ongoing network traffic)
11		11:17:44	_ap.gif was created.
12		11:17:46	_ap.gif written completely. For Mr. Lawrence to download a map containing the real location of meeting appointment, He needs to have a complete access to the information. It is concluded that between 11:11:00 to 11:17:44, he has analyzed the network traffic and completed MapPoint query.
13		19:24:46	Coffee.doc created on file system. The document contains a statement that he was on the same place as meeting point and saw Ms. Conlay with her friend. He was terrible upset and forcing her not to socialize as she has rejected his offer. The last part was a cynical statement. This would also mean that Mr. Lawrence had gone to the meeting point and saw for

			himself the meeting between Ms. Conlay and Mr. Guarillo.
14		19:24:48	Coffee.doc saved to USB flash drive
15	Oct 29	AM	Ms. Conlay reported the harassment to Corp. Security
16		PM	Mr. Lawrence's cubicle was searched and USB drive was confiscated.

© SANS Institute 2000 - 2005, Author retains full rights.

Program Identification

Windump.exe

_indump.exe (Windump.exe) is a deleted file with size of 450, 560 bytes, inode entry of 14 and sector 1541-2420. The same procedure is taken by using dcfldd to carve the file from partition image. Readers are pointed to appendix 3 for file comprehensive recovery techniques used.

Windump is a well-known windows port of 'tcpdump' tool. VMware environment was setup on forensic workstation with Windows XP Professional SP2. It is also possible to use another forensics workstation with Windows Operating system in lieu of vmware. The file run successfully just like original windump executable file. Further checking the file's hash is exactly the same as original release from http://windump.mirror.ethereal.com/install/bin/windump_3_8_3_beta/WinDump.exe. Windump file found on the drive is version 3.8.3 beta.

```
[root@LinuxForensics recovered]# file windump.exe
windump.exe: MS-DOS executable (EXE), OS/2 or MS Windows
[root@LinuxForensics recovered]# md5sum windump.exe*
79375b77975aa53a1b0507496107bff7  windump.exe
79375b77975aa53a1b0507496107bff7  windump.exe.orig
```

```
F:\>windump -help
windump version 3.8.3 beta, based on tcpdump version 3.8.3
```

WinPcap_3_1_beta_3.exe

_inPcap_3_1_beta_3.exe (WinPcap_3_1_beta_3.exe) is the largest undeleted file and the most difficult to recover. Command 'istat' warned that the file recovery is not possible. It has inode entry of 7, starting sector 591 and file size of 485810 bytes. As the starting sector and file size is known, we can then compute the ending sector by dividing total file size to sector unit size and add it to starting sector. In this case, to fit a file of that size 950 sectors are needed (round up to nearest cluster). 'dcfldd' is then used to carve out the file for 950 sectors from sector 591. The file is not the final result yet, as we have to clean-up slack space from sector rounding-up. KHexEdit is used to remove remaining data from offset 485810. Offset count starts from 0, so offset 485810 is referring to the first redundant extra byte of the file (485811th byte). The file saved as WinPcap_3_1_beta_3.exe.Carved.

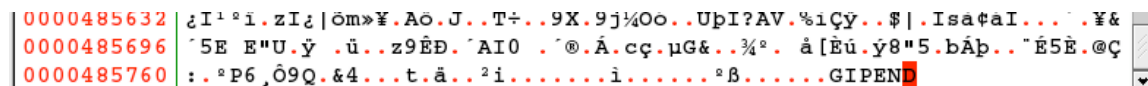


Figure 21 Removing slack space

Original file was downloaded from official mirror site at http://winpcap.mirror.ethereal.com/install/bin/WinPcap_3_1_beta_3.exe.

The original site was unreachable when this paper is written. At this point the recovered file and the original file have the same size but different MD5 hash. Looking carefully, the file has been overwritten from sector 591 to 630 by coffee.doc file. The timeline confirms that coffee.doc is created Oct 28th, while WinPcap_3_1_beta_3.exe was last written on Oct 27th. In summary, the file is no longer intact and has coffee.doc file on beginning part of the file.

```
[root@LinuxForensics recovered]# file WinPcap_3_1_beta_3.exe
WinPcap_3_1_beta_3.exe: Microsoft Office Document

[root@LinuxForensics recovered]# ls -l WinPcap_3_1_beta_3.exe*
-rw-r--r--  1 root root 486400 Mar 20 01:16 WinPcap_3_1_beta_3.exe
-rw-r--r--  1 root root 485810 Mar 20 01:59
WinPcap_3_1_beta_3.exe.Carved
-rwxr-xr-x  1 root root 485810 Mar 20 01:41
WinPcap_3_1_beta_3.exe.Orig

[root@LinuxForensics recovered]# md5sum WinPcap_3_1_beta_3.exe*
3c6144401664d5c8567b36c0c7f01731  WinPcap_3_1_beta_3.exe
4511ee3b4e5d8150c035a140dfba72c0  WinPcap_3_1_beta_3.exe.Orig
```

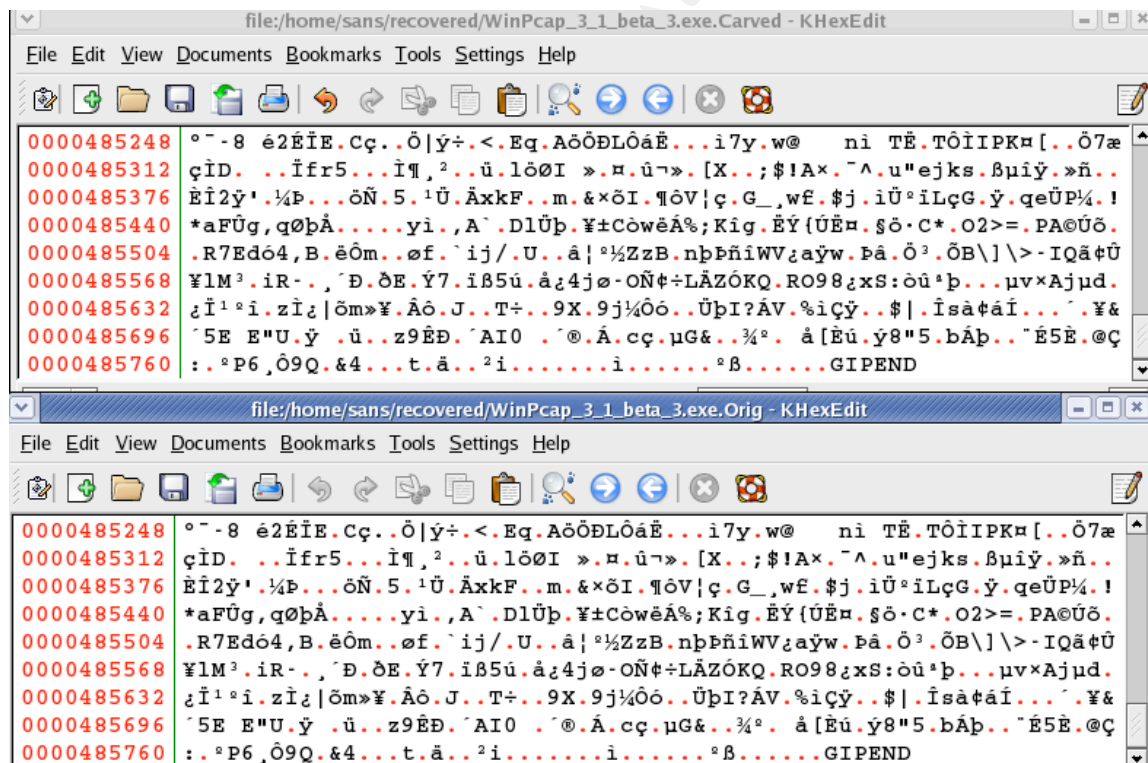


Figure 22 Both files have same data at end after recovered file removing slack.

In order to verify that recovered file is indeed a real file, we need to find the degree of file integrity. To achieve this, overlapping portion has to be removed.

A freeware tool 'cmp' is used to find the differences between original and recovered file as follows:

```
[root@LinuxForensics recovered]# cmp -l WinPcap_3_1_beta_3.exe.Carved
WinPcap_3_1_beta_3.exe.Orig > WinPcap_3_1_beta_3.exe.cmp
(snip)
19966 0 10
19967 0 162
19968 0 10
```

The file has differences up to byte 19968, and the rest was an exact match. The number is consistent with file size of coffee.doc that overwrites the file. To obtain a high-confidence level that the file has large degree of common pattern, a MD5 has will be needed. First, both files have to be carved to remove the first 19968 byte by using KHexEdit.

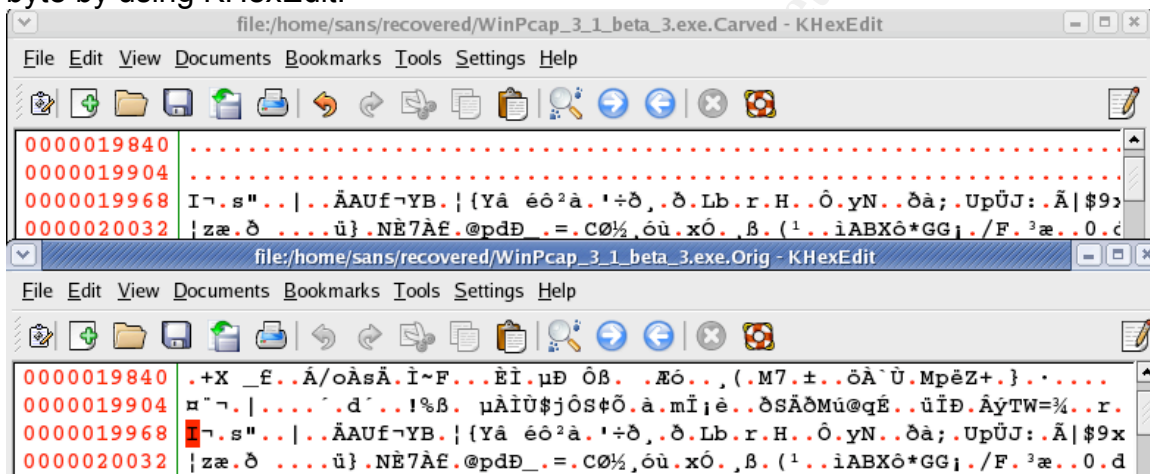


Figure 23 Differences before offset 19968

Once we have both files removed of their first 19968 bytes, we have two new files and they have exact MD5 hash.

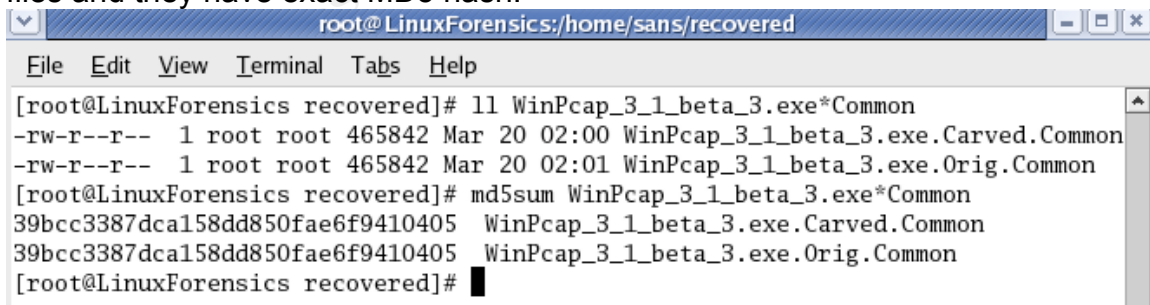


Figure 24 Common pattern

Based on this information, there is 95.89% (465842 out of 485810 bytes) match between the two files on hash-level. Therefore, we can confidently take the recovered file content is indeed the same file as the filename suggest in official site and its mirrors.

Legal Implications

Based from evidence gathered, Mr. Lawrence is known to have breach both company's Acceptable Use Policy and laws. He has sniffed network traffic and start violating Ms. Conlay's privacy. For the benefits of reader and variety to other papers, Singapore Laws will be used as reference in this section.

Law

Relevant offences that Mr. Lawrence committed according to legal statuses are:

Computer Misuse Act

A common law statute used for computer-related crime is "Computer Misuse Act (Of Singapore)". The bill was introduced to parliament on June 1st 1998, passed on June 29th 1998, and come into force on August 1st 1998.³ The bill could be viewed on <http://statutes.agc.gov.sg/> in chapter 50A.

1. Unauthorised access to computer material

3. —(1) *Subject to subsection (2), any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$5,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding \$10,000 or to imprisonment for a term not exceeding 3 years or to both.*

(Mr. Lawrence has run sniffer to listen to Ms. Conlay private communication)

2. Access with intent to commit or facilitate commission of offence

4. —(1) *Any person who causes a computer to perform any function for the purpose of securing access to any program or data held in any computer with intent to commit an offence to which this section applies shall be guilty of an offence.*

(Mr. Lawrence used the information from Ms. Conlay's email to further his harassment)

3. Unauthorised use or interception of computer service

6. —(1) Subject to subsection (2), any person who knowingly —
(a) *secures access without authority to any computer for the purpose of obtaining, directly or indirectly, any computer service;*
(b) *intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of an electro-magnetic, acoustic, mechanical or other device; or*

3

<http://www.ida.gov.sg/idaweb/pnr/infopage.jsp?infopagecategory=infoecon:pnr&versionid=1&info pageid=1234>

(c) uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence under paragraph (a) or (b),

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding \$20,000 or to imprisonment for a term not exceeding 5 years or to both.

(Mr. Lawrence intercepts company's network traffic and use the information for his own personal purposes)

Miscellaneous Offences (Public Order and Nuisance) Act

Intentional harassment, alarm or distress

13A. —(1) *Any person who in a public place or in a private place, with intent to cause harassment, alarm or distress to another person —*

(a) uses threatening, abusive or insulting words or behaviour; or

(b) displays any writing, sign or other visible representation which is threatening, abusive or insulting,

thereby causing that person or any other person harassment, alarm or distress, shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$5,000.

(Potential offences if Mr. Lawrence furthers his harassment to the next level)

Penal code (Chapter 224)

Word or gesture intended to insult the modesty of a woman.

509. *Whoever, intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen by such woman, or intrudes upon the privacy of such woman, shall be punished with imprisonment for a term which may extend to one year, or with fine, or with both.*

(Mr. Lawrence intruded Ms. Conlay's privacy and modesty by sending aggressive email to her personal email address and stalking her to her personal appointment)

The potential punishment for the conduct would sufficiently put Mr. Lawrence behind the bar or given fine or both. For enforcement agencies to act on these offences, a police report has to be filed either by Ms. Conlay or the company. The agencies will follow-up with prosecution at their discretion.

Company Policies

Companies normally would have a set of policies that governs acceptable use of their network. For a good reference, we shall use policy templates provided by SANS at <http://www.sans.org/resources/policies/>.

Acceptable Use Policy

An employee is allowed to use the network for personal use within reasonable limits (4.1.2). The policy also specifies that the following are unacceptable:

- computing assets to be used to engage in sexual harassment
- Conducting security breaches (inclusive of accessing data which the employee is not intended recipient).
- Executing any form of network monitoring which will intercept data not intended for employee's host.
- Sending any form of harassment via email, telephone or paging.

Further more the policy states that violation of AUP will result in disciplinary action to the employee up to and including termination of employment.

Ethics Policy

Section 4.2.1 describes employees will treat everyone fairly, have mutual respect, promote a team environment and avoid the intent and appearance of unethical or compromising practices. Section 4.5 describes unethical behaviors that include harassment, using corporate assets for personal use. The enforcement will follow the AUP above.

Email Policy

Section 3.1 states prohibited use of email that includes creation or distribution of offensive messages. Enforcement will follow AUP.

Based on the policies above, it is clear that Mr. Lawrence has violated many policies for his actions. As described in the policies, he could have his employment terminated for violations.

Recommendations

The recommended course of action is to pass the investigation report to human resources. Human resources will work with corporate security and line manager of Mr. Lawrence to decide the disciplinary actions. Ms. Conlay's report has to be taken seriously, now that we have evidence against Mr. Lawrence, or otherwise she could sue the company for not protecting her rights.

Likewise, Mr. Lawrence should be getting disciplinary actions for what he did, and depending on company policies and his contribution to the company, he may be severely warned or has his employment terminated. The case should be an example for all other employees for violating company policies. In a scenario, where Mr. Lawrence furthers his advances to intolerable level, a police report may have to be filed immediately and the enforcement agency will take the case from there.

The case also shows that the company does not have sufficient level of control over its network resources. Control is defined as safeguard or measure to reduce or eliminate the impact of a threat (ISACA). For example, wireless network was provided without any encryption, this will enable anyone from accessing company's intranet and gain access to confidential information. There also no control over software that an employee can install. In large enterprises, local admin right normally is not granted or there is a strict group policy (GPO) that disallow additional hardware (USB Flash drive for example) to be connected and installation of additional software. It is also known that access to the internet does not go through a web proxy, but rather a direct connection via gateway. A web proxy is highly recommended so that additional layer of filtering can be put in place. Wireless network should not be used at all unless with secure WPA.

Internal audit followed by external audit would be needed to ensure that the right controls are put into place. Due to the company's nature in financial industry, it should have a strong control over information security. The leak of information could mean non-compliance to regulatory requirement on sufficient protection for information. We have seen many financial institutions lost thousands of its customers' details and credit card numbers. The recent bill introduced in California requires organizations to inform every individual that have their data leaked or compromised. This requirement would also mean company will lose its credibility due to public announcement of the compromise and lost of opportunity of sales.

The case will also test on company's policies. Good policies should govern the acceptable use policy, define unacceptable practices and its consequences. Even if the company has a set of good policies, it has to be socialized to current and future employees. One way to do it is to have a short session on a policy on each strategy sharing session and induction for new employees.

Additional Information

1. National University of Singapore's Index to law in Singapore
(<http://www.lib.nus.edu.sg/lb/internet/spore.html>)

The website lists many legislations and law-related sites. This website would be very useful to research applicable laws in Singapore used to work on a case. As a forensic investigator/analyst, we may be asked to be expert witness in courts. By understanding applicable laws and its correct interpretations, we can use it to align our investigation with required laws. It will also provide the knowledge of actions that are covered in law and hence as basis for a case.

2. Singapore Statutes Online
(<http://statutes.agc.gov.sg/>)

Online Singapore legislations. Mostly used by attorneys, lawyers and law students, the website provides easy and convenient access to Singapore legislations. The legal implication section of this paper uses the website significantly to find relevant Acts.

3. Dan Farmer's Website
(<http://www.fish.com/security/forensics.html>)

The class handouts and whitepapers on tools and methodology aid the courseware and helped in conducting forensic investigation.

4. The Sleuth Kit's official website
(<http://www.sleuthkit.org/sleuthkit/index.php>)

This paper uses TSK for most of its investigation efforts, and through TSK the analysis can be done.

References

1. SANS Institute. Courseware. Security 508: System Forensics, Investigation & Response. 2004
2. SANS Institute. Online. Forensic Installation Guide for Track 8 Students, Version 3.0.
3. Calishain, Dornfest. Oreilly. Google Hacks. 2003
4. Carvey. Addison-Wesley. Windows Forensics and Incident Recovery. 2005
5. Farmer, Venema. Addison-Wesley. Forensic Discovery. 2005
6. SANS Institute. Online. Security Policy Templates. Available at: <http://www.sans.org/resources/policies/>. Accessed at March 20, 2005
7. Singapore Statutes OnLine. Online. Computer Misuse Act. Available at: <http://statutes.agc.gov.sg/> (Chapter 50A). Accessed at March 20, 2005
8. Singapore Statutes OnLine. Online. Miscellaneous Offenses (Public order and nuisance). Available at: <http://statutes.agc.gov.sg/> Accessed at March 20, 2005
9. Singapore Statutes OnLine. Online. Penal Code. Available at: <http://statutes.agc.gov.sg/> (Chapter 224) Accessed at March 20, 2005.
10. WinPcap. Online. The WinPcap manual and tutorial. Available at: <http://winpcap.mirror.ethereal.com/docs/default.htm> Accessed at March 20, 2005.
11. WinDump. Online. WinDump FAQ. Available at: <http://winpcap.mirror.ethereal.com/misc/faq.htm>. Accessed at March 20, 2005.
12. WinDump. Online. WinDump Documentatation. Available at: <http://windump.mirror.ethereal.com/docs/manual.htm>. Accessed at March 20, 2005
13. MSN MapPoint. Online. MSN MapPoint. Available at: <http://mappoint.msn.com>. Accessed at March 20, 2005.
14. LookupTable.com. Online. ASCII table. Available at: <http://www.lookuptables.com/>. Accessed at March 20, 2005.

Appendix 1 – Investigation Time Line

Time is in GMT (UTC +0)

No.	Date	Time	Activity	Information
1	19/03/05	09.00-09.45	Preparation	Acquiring a laptop with clean hard drive to do forensic
2		09.45-09.50	Media Boot	Start Fedora Core 3 install
3		09.50-10.05	Media Check	Test media for errors – PASS
4		10.05-11.40	Install	Ref. Forensics Installation Guide for Track 8 Student v3.0
5		11.40-11.50	Image Hash	Verified Image MD5 checksum
6		11.50-12.10	Install Tools	Using Track 8 Unix CD-rom
7		12.10-13.00	Image	Acquire Image and verify MD5
8			Paused	Dinner, Call it a day.
9	20/03/05	01.00-02.00	Image (Cont)	Breaking Image file into partition image files
10				Analyze each image files for interesting content
11				Retrieving files on file system
12		02.00-04.00	Recovery	Recovery of deleted files
13			Paused	Lunch
14		05.00-08.00	Analysis	Analyze recovered files in relation to the case.
15		08.00-10.00	Network Capture	Analyze network capture using Ethereal
16		10.00-12.00	MAC Time	Generate MAC timeline
17			Program Identification	Analyze program used and verify the program to releases from official websites.
18			Paused	Dinner, Call it a day.
19	21/03/05	01.00-04.00	Time line	Reconstructing events from available information.
20			Legal implication	Study relevant legal statuses and organization policy
21		04.00-05.00	Paused	Lunch
22		05.00-12.00	Writing Report	Writing official repots, transferring notes to report.
23		12.00-13.00	Proof reading	Proof-read reports for mistakes
24		13.00	Submission	Report submitted to Corporate security.
25				

Appendix 2 – File Recovery Flowchart

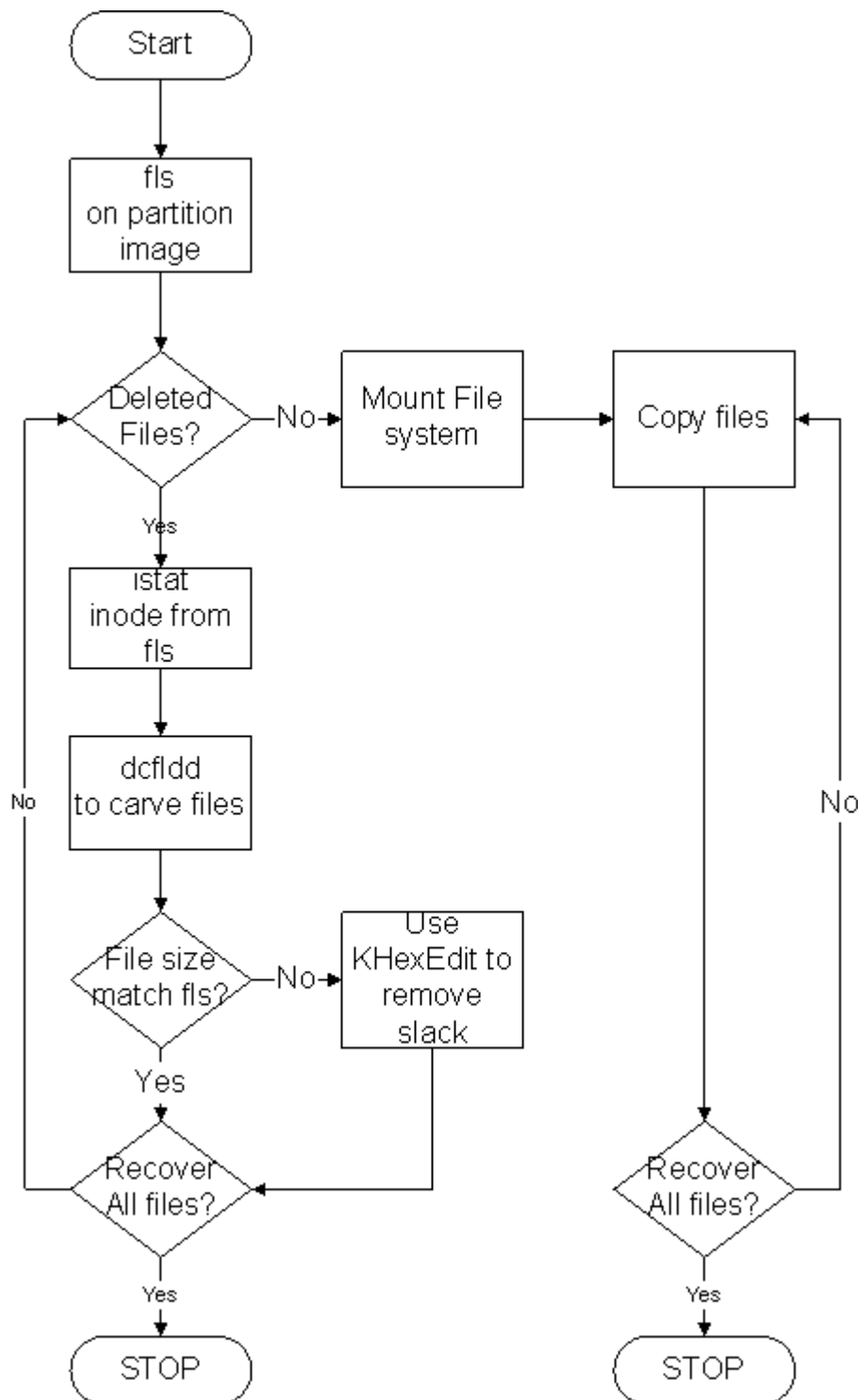


Figure 25 File Recovery Flowchart

Appendix 3 – Step by Step Activities

```
[root@LinuxForensics sans]# fls -f fat16 USBFD-64531026-RL-001.img.part3
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
```

```
[root@LinuxForensics sans]# istat -f fat16 USBFD-64531026-RL-001.img.part3 3
Directory Entry: 3
Allocated
File Attributes: File, Archive
Size: 19968
Num of links: 1
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
[root@LinuxForensics sans]#
```

```
[root@LinuxForensics sans]# istat -f fat16 USBFD-64531026-RL-001.img.part3 4
Directory Entry: 4
Allocated
File Attributes: File, Archive
Size: 19968
Num of links: 1
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
[root@LinuxForensics sans]#
```

```
[root@LinuxForensics sans]# istat -f fat16 USBFD-64531026-RL-
001.img.part3 7
Directory Entry: 7
Not Allocated
File Attributes: File, Archive
Size: 0
Num of links: 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
[root@LinuxForensics sans]#
```

```
[root@LinuxForensics sans]# istat -f fat16 USBFD-64531026-RL-
001.img.part3 10
Directory Entry: 10
Not Allocated
File Attributes: File, Archive
Size: 485810
Num of links: 0
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
[root@LinuxForensics sans]# istat -f fat16 USBFD-64531026-RL-
001.img.part3 12
Directory Entry: 12
Not Allocated
File Attributes: File, Archive
Size: 0
Num of links: 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

[root@LinuxForensics sans]# istat -f fat16 USBFD-64531026-RL-001.img.part3 14

Directory Entry: 14

Not Allocated

File Attributes: File, Archive

Size: 450560

Num of links: 0

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

1549 1550 1551 1552 1553 1554 1555 1556

(snip)

2405 2406 2407 2408 2409 2410 2411 2412

2413 2414 2415 2416 2417 2418 2419 2420

[root@LinuxForensics sans]#

[root@LinuxForensics sans]# istat -f fat16 USBFD-64531026-RL-001.img.part3 15

Directory Entry: 15

Not Allocated

File Attributes: File, Archive

Size: 53056

Num of links: 0

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

2429 2430 2431 2432 2433 2434 2435 2436

(snip)

2509 2510 2511 2512 2513 2514 2515 2516

2517 2518 2519 2520 2521 2522 2523 2524


```
[root@LinuxForensics sans]# istat -f fat16 USBFD-64531026-RL-001.img.part3 16
Directory Entry: 16
Not Allocated
File Attributes: File, Archive
Size: 0
Num of links: 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

```
[root@LinuxForensics sans]# istat -f fat16 USBFD-64531026-RL-001.img.part3 17
Directory Entry: 17
Not Allocated
File Attributes: File, Archive
Size: 8814
Num of links: 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:
2525 2526

```
Recovery:
2525 2526 2527 2528 2529 2530 2531 2532
2533 2534 2535 2536 2537 2538 2539 2540
2541 2542
[root@LinuxForensics sans]#
```

```
[root@LinuxForensics sans]# istat -f fat16 USBFD-64531026-RL-001.img.part3 18
Directory Entry: 18
Allocated
File Attributes: File, Archive
Size: 19968
Num of links: 1
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
[root@LinuxForensics sans]#

[root@LinuxForensics sans]# dcfldd skip=511 count=39 hashwindow=0
if=USBFD-64531026-RL-001.img.part3 of=her.doc.recovered

Total: 9785a777c5286738f9deb73d8bc57978
39+0 records in
39+0 records out
[root@LinuxForensics sans]# dcfldd skip=551 count=39 hashwindow=0
if=USBFD-64531026-RL-001.img.part3 of=hey.doc.recovered

Total: ca601d4f8138717dca4de07a8ec19ed1
39+0 records in
39+0 records out
[root@LinuxForensics sans]# dcfldd skip=591 count=39 hashwindow=0
if=USBFD-64531026-RL-001.img.part3 of=coffee.doc.recovered

Total: a833c58689596eda15a27c931e0c76d1
39+0 records in
39+0 records out
[root@LinuxForensics sans]#

[root@LinuxForensics sans]# md5sum *doc*
a833c58689596eda15a27c931e0c76d1 coffee.doc
a833c58689596eda15a27c931e0c76d1 coffee.doc.recovered
9785a777c5286738f9deb73d8bc57978 her.doc
9785a777c5286738f9deb73d8bc57978 her.doc.recovered
ca601d4f8138717dca4de07a8ec19ed1 hey.doc
ca601d4f8138717dca4de07a8ec19ed1 hey.doc.recovered
[root@LinuxForensics sans]#

[root@LinuxForensics sans]# dcfldd skip=2421 count=104 hashwindow=0
if=USBFD-64531026-RL-001.img.part3 of=_apture

Total: f7db6e0ecb4c3c51218d918c9c711cbd
104+0 records in
104+0 records out
[root@LinuxForensics sans]# md5sum _apture
2097b7b0a9fedb4238b67e976c4ae1cb _apture
[root@LinuxForensics sans]#

[root@LinuxForensics sans]# dcfldd skip=2525 count=18 hashwindow=0
if=USBFD-64531026-RL-001.img.part3 of=_ap.gif

Total: 40f95f34699273fd4d681bd68a7a3ab5
18+0 records in
18+0 records out
[root@LinuxForensics sans]# md5sum _ap.gif
9bc3923cf8e72fd405d7cea8c8781011 _ap.gif
[root@LinuxForensics sans]#
```

```
[root@LinuxForensics sans]# dcflddd skip=1541 count=880 hashwindow=0
if=USBFD-64531026-RL-001.img.part3 of=windump.exe
768 blocks (0Mb) written.
Total: 79375b77975aa53a1b0507496107bfff7
880+0 records in
880+0 records out
[root@LinuxForensics sans]#

[root@LinuxForensics sans]# dcflddd skip=591 count=950 hashwindow=0
if=USBFD-64531026-RL-001.img.part3 of=WinPcap_3_1_beta_3.exe
768 blocks (0Mb) written.
Total: 3c6144401664d5c8567b36c0c7f01731
950+0 records in
950+0 records out

[root@LinuxForensics sans]# mkdir recovered; cd recovered
[root@LinuxForensics recovered]# mv ../doc* .;mv ../*.exe .;mv ../_* .

[root@LinuxForensics recovered]# ls -l
total 3296
-rw-r--r-- 1 root root 8814 Mar 20 01:04 _ap.gif
-rw-r--r-- 1 root root 53056 Mar 20 01:02 _apture
-rwxr-xr-x 1 root root 19968 Mar 19 14:06 coffee.doc
-rw-r--r-- 1 root root 19968 Mar 20 00:46 coffee.doc.recovered
-rwxr-xr-x 1 root root 19968 Mar 19 14:06 her.doc
-rw-r--r-- 1 root root 19968 Mar 20 00:32 her.doc.recovered
-rwxr-xr-x 1 root root 19968 Mar 19 14:06 hey.doc
-rw-r--r-- 1 root root 19968 Mar 20 00:33 hey.doc.recovered
-rw-r--r-- 1 root root 450560 Mar 20 01:08 windump.exe
-rw-r--r-- 1 root root 486400 Mar 20 01:16 WinPcap_3_1_beta_3.exe
-rwxr-xr-x 1 root root 485810 Mar 20 01:41 WinPcap_3_1_beta_3.exe.Orig
-rw-r--r-- 1 root root 8704 Mar 20 00:53 xap.gif

[root@LinuxForensics recovered]# cp /media/Flash/windump.exe
windump.exe.orig

[root@LinuxForensics recovered]# md5sum windump.exe*
79375b77975aa53a1b0507496107bfff7 windump.exe
79375b77975aa53a1b0507496107bfff7 windump.exe.orig

[root@LinuxForensics recovered]# file windump.exe
windump.exe: MS-DOS executable (EXE), OS/2 or MS Windows

[root@LinuxForensics recovered]# ls -l WinPcap_3_1_beta_3.exe*
-rw-r--r-- 1 root root 486400 Mar 20 01:16 WinPcap_3_1_beta_3.exe
-rw-r--r-- 1 root root 485810 Mar 20 01:59
WinPcap_3_1_beta_3.exe.Carved
-rwxr-xr-x 1 root root 485810 Mar 20 01:41 WinPcap_3_1_beta_3.exe.Orig
[root@LinuxForensics recovered]#

[root@LinuxForensics recovered]# md5sum WinPcap_3_1_beta_3.exe*
3c6144401664d5c8567b36c0c7f01731 WinPcap_3_1_beta_3.exe
b794de4b88068ae80de523c3b35eeaab WinPcap_3_1_beta_3.exe.Carved
4511ee3b4e5d8150c035a140dfba72c0 WinPcap_3_1_beta_3.exe.Orig
```

```
[root@LinuxForensics recovered]# cmp -l WinPcap_3_1_beta_3.exe.Carved
WinPcap_3_1_beta_3.exe.Orig > WinPcap_3_1_beta_3.exe.cmp
```

```
....
```

```
19966  0 10
19967  0 162
19968  0 10
```

(Carve data out of overwritten part, resulting in *Common files)

```
[root@LinuxForensics recovered]# ll WinPcap_3_1_beta_3.exe*Common
-rw-r--r--  1 root root 465842 Mar 20 02:00
WinPcap_3_1_beta_3.exe.Carved.Common
-rw-r--r--  1 root root 465842 Mar 20 02:01
WinPcap_3_1_beta_3.exe.Orig.Common
```

```
[root@LinuxForensics recovered]# md5sum WinPcap_3_1_beta_3.exe*Common
39bcc3387dca158dd850fae6f9410405  WinPcap_3_1_beta_3.exe.Carved.Common
39bcc3387dca158dd850fae6f9410405  WinPcap_3_1_beta_3.exe.Orig.Common
[root@LinuxForensics recovered]# cd ..
```

Appendix 4 – MAC Timeline

Mon Oct 25 2004 00:00:00	19968 .a. -/-rwxxrwxrwx	0	0	3	/her.doc
Mon Oct 25 2004 08:32:06	19968 ..c -/-rwxxrwxrwx	0	0	3	/her.doc
Mon Oct 25 2004 08:32:08	19968 m.. -/-rwxxrwxrwx	0	0	3	/her.doc
Tue Oct 26 2004 00:00:00	19968 .a. -/-rwxxrwxrwx	0	0	4	/hey.doc
Tue Oct 26 2004 08:48:06	19968 ..c -/-rwxxrwxrwx	0	0	4	/hey.doc
Tue Oct 26 2004 08:48:10	19968 m.. -/-rwxxrwxrwx	0	0	4	/hey.doc
Wed Oct 27 2004 00:00:00	0 .a. -rwxxrwxrwx	0	0	7	<USBFD-64531026-RL-
001.img.part3-_INPCA~1.EXE-dead-7>	485810 .a. -/-rwxxrwxrwx	0	0	7	
/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)	450560 .a. -/-rwxxrwxrwx	0	0	12	/WinDump.exe
(_INDUMP.EXE) (deleted)					
001.img.part3-_INDUMP.EXE-dead-12>	0 .a. -rwxxrwxrwx	0	0	12	<USBFD-64531026-RL-
Wed Oct 27 2004 16:23:50	485810 m.. -rwxxrwxrwx	0	0	10	<USBFD-64531026-RL-
001.img.part3-_INPCA~1.EXE-dead-10>	485810 m.. -/-rwxxrwxrwx	0	0	10	
/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)	485810 ..c -rwxxrwxrwx	0	0	10	<USBFD-64531026-RL-
Wed Oct 27 2004 16:23:54	485810 ..c -rwxxrwxrwx	0	0	10	
001.img.part3-_INPCA~1.EXE-dead-10>	485810 ..c -/-rwxxrwxrwx	0	0	10	
/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)	0 ..c -rwxxrwxrwx	0	0	7	<USBFD-64531026-RL-
001.img.part3-_INPCA~1.EXE-dead-7>	485810 ..c -/-rwxxrwxrwx	0	0	7	
/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)	0 m.. -rwxxrwxrwx	0	0	7	<USBFD-64531026-RL-
Wed Oct 27 2004 16:23:56	0 m.. -rwxxrwxrwx	0	0	7	
001.img.part3-_INPCA~1.EXE-dead-7>	485810 m.. -/-rwxxrwxrwx	0	0	7	
/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)	450560 m.. -/-rwxxrwxrwx	0	0	14	/WinDump.exe
Wed Oct 27 2004 16:24:02	450560 m.. -/-rwxxrwxrwx	0	0	14	
(_INDUMP.EXE) (deleted)	450560 m.. -rwxxrwxrwx	0	0	14	<USBFD-64531026-RL-
001.img.part3-_INDUMP.EXE-dead-14>					

Wed Oct 27 2004 16:24:04	450560	..c	-rw-rw-rw-rw	0	0	14	<USBFD-64531026-RL-
001.img.part3-_INDUMP.EXE-dead-14>	450560	..c	-/-rw-rw-rw-rw	0	0	12	/WinDump.exe (_INDUMP.EXE)
(deleted)							
(deleted)	450560	..c	-/-rw-rw-rw-rw	0	0	14	/WinDump.exe (_INDUMP.EXE)
	0	..c	-rw-rw-rw-rw	0	0	12	<USBFD-64531026-RL-
001.img.part3-_INDUMP.EXE-dead-12>	450560	m..	-/-rw-rw-rw-rw	0	0	12	/WinDump.exe (_INDUMP.EXE)
Wed Oct 27 2004 16:24:06							
(deleted)	0	m..	-rw-rw-rw-rw	0	0	12	<USBFD-64531026-RL-
001.img.part3-_INDUMP.EXE-dead-12>	53056	.a.	-/-rw-rw-rw-rw	0	0	15	/_apture (deleted)
Thu Oct 28 2004 00:00:00	8814	.a.	-/-rw-rw-rw-rw	0	0	16	/_ap.gif (deleted)
	450560	.a.	-rw-rw-rw-rw	0	0	14	<USBFD-64531026-RL-
001.img.part3-_INDUMP.EXE-dead-14>	450560	.a.	-/-rw-rw-rw-rw	0	0	14	/WinDump.exe (_INDUMP.EXE)
(deleted)							
	19968	.a.	-/-rw-rw-rw-rw	0	0	18	/coffee.doc
	8814	.a.	-/-rw-rw-rw-rw	0	0	17	/_ap.gif (deleted)
	53056	.a.	-rw-rw-rw-rw	0	0	15	<USBFD-64531026-RL-
001.img.part3-_apture-dead-15>	485810	.a.	-rw-rw-rw-rw	0	0	10	<USBFD-64531026-RL-
001.img.part3-_INPCA~1.EXE-dead-10>	485810	.a.	-/-rw-rw-rw-rw	0	0	10	/WinPcap_3_1_beta_3.exe
(_INPCA~1.EXE) (deleted)	8814	.a.	-rw-rw-rw-rw	0	0	17	<USBFD-64531026-RL-
001.img.part3-_ap.gif-dead-17>	0	.a.	-rw-rw-rw-rw	0	0	16	<USBFD-64531026-RL-
001.img.part3-_ap.gif-dead-16>	53056	..c	-/-rw-rw-rw-rw	0	0	15	/_apture (deleted)
Thu Oct 28 2004 11:08:24	53056	..c	-rw-rw-rw-rw	0	0	15	<USBFD-64531026-RL-
001.img.part3-_apture-dead-15>	53056	m..	-/-rw-rw-rw-rw	0	0	15	/_apture (deleted)
Thu Oct 28 2004 11:11:00	53056	m..	-rw-rw-rw-rw	0	0	15	<USBFD-64531026-RL-
001.img.part3-_apture-dead-15>							

Thu Oct 28 2004 11:17:44	0	..c	-rwxrwxrwx	0	0	16	<USBFD-64531026-RL-
001.img.part3-_ap.gif-dead-16>	8814	..c	-rwxrwxrwx	0	0	17	<USBFD-64531026-RL-
001.img.part3-_ap.gif-dead-17>	8814	..c	-/-rwxrwxrwx	0	0	16	/_ap.gif (deleted)
	8814	..c	-/-rwxrwxrwx	0	0	17	/_ap.gif (deleted)
Thu Oct 28 2004 11:17:46	0	m..	-rwxrwxrwx	0	0	16	<USBFD-64531026-RL-
001.img.part3-_ap.gif-dead-16>	8814	m..	-rwxrwxrwx	0	0	17	<USBFD-64531026-RL-
001.img.part3-_ap.gif-dead-17>	8814	m..	-/-rwxrwxrwx	0	0	16	/_ap.gif (deleted)
	8814	m..	-/-rwxrwxrwx	0	0	17	/_ap.gif (deleted)
Thu Oct 28 2004 19:24:46	19968	..c	-/-rwxrwxrwx	0	0	18	/coffee.doc
Thu Oct 28 2004 19:24:48	19968	m..	-/-rwxrwxrwx	0	0	18	/coffee.doc