Fight crime.
Unravel incidents... one byte at a time.

Interested in learning more?
Check out the list of upcoming events offering "Advanced Incident Response, Threat Hunting, and Digital Forensics (FOR508)" at http://digital-forensics.sans.org/events/
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
    capture ............................................................................................................................... 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
    capture (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 separate 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:

- **command**: Operating system commands are represented in this font style. This style indicates a command that is entered at a command prompt or shell.
- **filename**: Filenames, paths, and directory names are represented in this style.
- **computer output**: The results of a command and other computer output are in this style.
- **URL**: Web URL's are shown in this style.
- **Quotation**: 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.
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 3.0.

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:
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.

![Figure 1 Verifying image integrity](image)

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:

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

(* 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.

![Figure 2 mmls output from image file](image)

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.

![Figure 3 Using dcfldd to separate each segment](image)
Leonard Ong

Examination Details

Figure 4 Segments of image file

The 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
```

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

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.
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.

**Figure 5** ‘file’ command applied to image parts

**Figure 6** Partition 1 in Hex Editor view

**Figure 7** Partition 2 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.

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:
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?

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.
Leonard Ong

Examination Details

Figure 13 Retrieving Files from disk image

```
[root@LinuxForensics sans]# dcfldd skip=511 count=39 hashwindow=0 if=USBFD-6453 1028-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 1028-RL-001.img.part3 of=hey.doc.recovered
Total: ca601d4f8138f170ca4de07a8ec19ed1
39-0 records in
39-0 records out
[root@LinuxForensics sans]# dcfldd skip=591 count=39 hashwindow=0 if=USBFD-6453 1028-RL-001.img.part3 of=coffee.doc.recovered
Total: a833c5889596eda15a27c931e0c76d1
39-0 records in
39-0 records out

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.

![Recovered Image File](image.png)

**Figure 15 Recovered Image File**

```bash
[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.

```bash
[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:

```bash
[root@LinuxForensics recovered]# ls -l
```

<table>
<thead>
<tr>
<th>File Name</th>
<th>Program Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>_ap.gif</td>
<td>Microsoft MapPoint</td>
<td>Location Map</td>
</tr>
<tr>
<td>capture</td>
<td>Windump/tcpdump</td>
<td>Traffic capture</td>
</tr>
<tr>
<td>coffee.doc</td>
<td>Microsoft Office 10</td>
<td>Document</td>
</tr>
<tr>
<td>her.doc</td>
<td>Microsoft Office 10</td>
<td>Document</td>
</tr>
<tr>
<td>hey.doc</td>
<td>Microsoft Office 10</td>
<td>Document</td>
</tr>
<tr>
<td>windump.exe</td>
<td>Windump v.3.8.3</td>
<td>Sniffer windows-based</td>
</tr>
<tr>
<td>WinPcap_3_1_beta_3.exe</td>
<td>WinPcap Library v3.1.Beta3</td>
<td>Packet capture library for windump/tcpdump</td>
</tr>
</tbody>
</table>

## 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:

<table>
<thead>
<tr>
<th>No.</th>
<th>Recovered File Name</th>
<th>Real File Name</th>
<th>Program Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>_ap.gif</td>
<td>map.gif</td>
<td>Microsoft MapPoint</td>
<td>Location Map</td>
</tr>
<tr>
<td>2.</td>
<td>capture</td>
<td>capture</td>
<td>Windump/tcpdump</td>
<td>Traffic capture</td>
</tr>
<tr>
<td>3.</td>
<td>coffee.doc</td>
<td>coffee.doc</td>
<td>Microsoft Office 10</td>
<td>Document</td>
</tr>
<tr>
<td>4.</td>
<td>her.doc</td>
<td>her.doc</td>
<td>Microsoft Office 10</td>
<td>Document</td>
</tr>
<tr>
<td>5.</td>
<td>hey.doc</td>
<td>hey.doc</td>
<td>Microsoft Office 10</td>
<td>Document</td>
</tr>
<tr>
<td>6.</td>
<td>windump.exe</td>
<td>windump.exe</td>
<td>Windump v.3.8.3</td>
<td>Sniffer windows-based</td>
</tr>
</tbody>
</table>

---

**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:

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

Figure 18 Recovered files size in bytes
**MD5 Hash of Recovered Files**

```
[root@LinuxForensics recovered]# md5sum *
9bc3923cf8a72fd405d7cea8c8781011  _ap.gif
2097b7b0a9fedb4238b67e970c4ae1cb  _apture
a833c58e89596eda15a27c933e0c76d1  coffee.doc
a833c58e89596eda15a27c933e0c76d1  coffee.doc.recovered
9785a777c5286738f9de73d8bc57978  her.doc
9785a777c5286738f9de73d8bc57978  her.doc.recovered
c6c601d4f8138717dca4de07a8ec19ed1  hey.doc
ca601d4f8138717dca4de07a8ec19ed1  hey.doc.recovered
7937b77975aa53a1b0507496107b7f7  windump.exe
3c614441664d5c8567b36c0c7f01731  WinPcap_3_1_beta_3.exe
```

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).

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.

<table>
<thead>
<tr>
<th>No.</th>
<th>IP address</th>
<th>Mac Addr.</th>
<th>FQDN</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.2.1</td>
<td>00:0c:41:50:29:2c</td>
<td>N/A</td>
<td>Default Gateway. LinksysG</td>
</tr>
<tr>
<td>2</td>
<td>192.168.2.104</td>
<td>00:90:4b:5e:e3:cf</td>
<td>N/A</td>
<td>Ms. Conlay's</td>
</tr>
<tr>
<td>3</td>
<td>192.168.2.255</td>
<td>ff:ff:ff:ff:ff:ff</td>
<td>N/A</td>
<td>Broadcast address</td>
</tr>
<tr>
<td>4</td>
<td>64.4.34.250</td>
<td>N/A (Default GW)</td>
<td><a href="http://www.bay12.hotmail.com">www.bay12.hotmail.com</a></td>
<td>Hotmail server</td>
</tr>
<tr>
<td>5</td>
<td>207.68.178.16</td>
<td>N/A (Default GW)</td>
<td>rad.msn.com</td>
<td>MSN Ad server</td>
</tr>
<tr>
<td>6</td>
<td>207.68.177.124</td>
<td>N/A (Default GW)</td>
<td>h.msn.com</td>
<td>MSN Ad server</td>
</tr>
<tr>
<td>7</td>
<td>63.209.188.62</td>
<td>N/A (Default GW)</td>
<td>Unknown.level3.net</td>
<td>Banner server</td>
</tr>
<tr>
<td>8</td>
<td>216.73.86.40</td>
<td>N/A (Default GW)</td>
<td>annyadvip2.doubleclick.net</td>
<td>DoubleClick Ad server</td>
</tr>
<tr>
<td>9</td>
<td>64.166.13.75</td>
<td>N/A (Default GW)</td>
<td>N/A</td>
<td>Unknown</td>
</tr>
</tbody>
</table>
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&Direcions (online). It is also offered online at [http://mappoint.msn.com](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.

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/(fs2ptp55gebxk255f3g5s245)/map.aspx?L=USA&C=34.10157%2c-118.33695&A=7.16667&P=|34.10157%2c-118.33695|)
Leonard Ong

Forensic Details

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:

<table>
<thead>
<tr>
<th>No</th>
<th>Date</th>
<th>Time</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Oct 25</td>
<td>08:32:08</td>
<td>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.</td>
</tr>
<tr>
<td>2</td>
<td>Oct 26</td>
<td>08:48:10</td>
<td>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.</td>
</tr>
<tr>
<td>3</td>
<td>Oct 27</td>
<td>16:23:54</td>
<td>WinPcap_3_1_Beta_3.exe download/copy to USB flash drive started</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>16:23:56</td>
<td>WinPcap_3_1_Beta_3.exe download/copy was completed</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>16:24:04</td>
<td>Windump.exe download/copy to USB flash drive started</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>16:24:06</td>
<td>Windump.exe download/copy to USB flash drive completed</td>
</tr>
<tr>
<td>7</td>
<td>Oct 28</td>
<td>Before 11:08:24</td>
<td>WinPcap_3_1_Beta_3.exe was accessed for installation.</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td>Windump.exe was started</td>
</tr>
<tr>
<td>9</td>
<td></td>
<td>11:08:24</td>
<td>_apture file created</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>11:11:00</td>
<td>_apture file written (ongoing network traffic)</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td>11:17:44</td>
<td>_ap.gif was created.</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td>11:17:46</td>
<td>_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.</td>
</tr>
<tr>
<td>13</td>
<td></td>
<td>19:24:46</td>
<td>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</td>
</tr>
<tr>
<td>Time</td>
<td>Event Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>--------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14:24:48</td>
<td>Coffee.doc saved to USB flash drive</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oct 29 AM</td>
<td>Ms. Conlay reported the harassment to Corp. Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16 PM</td>
<td>Mr. Lawrence’s cubicle was searched and USB drive was confiscated.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.

![Figure 21 Removing slack space](http://www.sans.org/images/2005-02-15-13-31-43-5149.png)

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

**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.

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

```

```
[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

```

```
00000485632 | .IÊ±í.i.uí∑š́ ŀ.A, .J.°...9X.9j%Oo..UbI?AV.%iÇý...$/Isnecai...''Ya
00000485696 | .S*U*y ,u...89Ed. 'HlO .°.Ai.cç,mgá..%° .à{mù.ý8*5.hAb..b58.Cç
00000495760 | .°.P6,09Q. &é...ë.ë...1...1...1...1...1...1...1...1...1...1...1...1...1...1...1...1...1...1...1...1...1...1...1...1...1...1...1...1...1...1...1...1...1...1...1...1...1
```

Figure 21 Removing slack space

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

Program Identification

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
4511ee3b4e5d8150c3551406f7a27c0  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](image)

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](image)

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. The bill could be viewed on [http://statutes.agc.gov.sg/](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

---

(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 uses 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

   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 Statuses Online

   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

   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

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

5. Farmer, Venema. Addison-Wesley. Forensic Discovery. 2005
## Appendix 1 – Investigation Time Line

Time is in GMT (UTC +0)

<table>
<thead>
<tr>
<th>No.</th>
<th>Date</th>
<th>Time</th>
<th>Activity</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>19/03/05</td>
<td>09.00-09.45</td>
<td>Preparation</td>
<td>Acquiring a laptop with clean hard drive to do forensic</td>
</tr>
<tr>
<td>2</td>
<td>09.45-09.50</td>
<td>Media Boot</td>
<td>Start Fedora Core 3 install</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>09.50-10.05</td>
<td>Media Check</td>
<td>Test media for errors – PASS</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>10.05-11.40</td>
<td>Install</td>
<td>Ref. Forensics Installation Guide for Track 8 Student v3.0</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>11.40-11.50</td>
<td>Image Hash</td>
<td>Verified Image MD5 checksum</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>11.50-12.10</td>
<td>Install Tools</td>
<td>Using Track 8 Unix CD-rom</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>12.10-13.00</td>
<td>Image</td>
<td>Acquire Image and verify MD5</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>Paused</td>
<td>Dinner, Call it a day.</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>20/03/05</td>
<td>01.00-02.00</td>
<td>Image (Cont)</td>
<td>Breaking Image file into partition image files</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td>Analyze each image files for interesting content</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td>Retrieving files on file system</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td>02.00-04.00</td>
<td>Recovery</td>
<td>Recovery of deleted files</td>
</tr>
<tr>
<td>13</td>
<td></td>
<td>Paused</td>
<td>Lunch</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td>05.00-08.00</td>
<td>Analysis</td>
<td>Analyze recovered files in relation to the case.</td>
</tr>
<tr>
<td>15</td>
<td></td>
<td>08.00-10.00</td>
<td>Network Capture</td>
<td>Analyze network capture using Ethereal</td>
</tr>
<tr>
<td>16</td>
<td></td>
<td>10.00-12.00</td>
<td>MAC Time</td>
<td>Generate MAC timeline</td>
</tr>
<tr>
<td>17</td>
<td></td>
<td></td>
<td>Program Identification</td>
<td>Analyze program used and verify the program to releases from official websites.</td>
</tr>
<tr>
<td>18</td>
<td></td>
<td></td>
<td>Paused</td>
<td>Lunch</td>
</tr>
<tr>
<td>19</td>
<td>21/03/05</td>
<td>01.00-04.00</td>
<td>Time line</td>
<td>Reconstructing events from available information.</td>
</tr>
<tr>
<td>20</td>
<td></td>
<td></td>
<td>Legal implication</td>
<td>Study relevant legal statuses and organization policy</td>
</tr>
<tr>
<td>21</td>
<td></td>
<td>04.00-05.00</td>
<td>Paused</td>
<td>Lunch</td>
</tr>
<tr>
<td>22</td>
<td></td>
<td>05.00-12.00</td>
<td>Writing Report</td>
<td>Writing official reports, transferring notes to report.</td>
</tr>
<tr>
<td>23</td>
<td></td>
<td>12.00-13.00</td>
<td>Proof reading</td>
<td>Proof-read reports for mistakes</td>
</tr>
<tr>
<td>24</td>
<td></td>
<td>13.00</td>
<td>Submission</td>
<td>Report submitted to Corporate security.</td>
</tr>
<tr>
<td>25</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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:
Accessed:Wed Oct 27 00:00:00 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:
Accessed:Thu Oct 28 00:00:00 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:
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:
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
Leonard Ong

Appendix 3

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]# dcf1dd 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]# dcf1dd 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]# dcf1dd 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]# md5sum *doc*
a833c58689596eda15a27c931e0c76d1  coffee.doc
a833c58689596eda15a27c931e0c76d1  coffee.doc.recovered
9785a777c5286738f9deb73d8bc57978  her.doc
9785a777c5286738f9deb73d8bc57978  her.doc.recovered
c601d4f8138717dca4de07a8ec19ed1  hey.doc
c601d4f8138717dca4de07a8ec19ed1  hey.doc.recovered
[root@LinuxForensics sans]# md5sum *doc*
a833c58689596eda15a27c931e0c76d1  coffee.doc
a833c58689596eda15a27c931e0c76d1  coffee.doc.recovered
9785a777c5286738f9deb73d8bc57978  her.doc
9785a777c5286738f9deb73d8bc57978  her.doc.recovered
c601d4f8138717dca4de07a8ec19ed1  hey.doc
c601d4f8138717dca4de07a8ec19ed1  hey.doc.recovered
[root@LinuxForensics sans]# md5sum *doc*
a833c58689596eda15a27c931e0c76d1  coffee.doc
a833c58689596eda15a27c931e0c76d1  coffee.doc.recovered
9785a777c5286738f9deb73d8bc57978  her.doc
9785a777c5286738f9deb73d8bc57978  her.doc.recovered
c601d4f8138717dca4de07a8ec19ed1  hey.doc
c601d4f8138717dca4de07a8ec19ed1  hey.doc.recovered
[root@LinuxForensics sans]#

[root@LinuxForensics sans]# dcf1dd 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
2097b7b0a9fededb4238b67e976c4ae1cb  _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]# dcfldd skip=1541 count=880 hashwindow=0 if=USBFD-64531026-RL-001.img.part3 of=windump.exe
768 blocks (0Mb) written.
Total: 79375b77975a53a1b0507496107bff7
880+0 records in
880+0 records out

[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
-rw-r--r-- 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
-rwxr-xr-x 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*
79375b77975a53a1b0507496107bff7 windump.exe
79375b77975a53a1b0507496107bff7 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*
b794de4b88068ae80de523c3b35eeab 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

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mon Oct 25 2004 00:00</td>
<td>19:68</td>
<td>a. –/-.</td>
</tr>
<tr>
<td>Mon Oct 25 2004 00:00</td>
<td>19:68</td>
<td>c. –/-.</td>
</tr>
<tr>
<td>Mon Oct 25 2004 00:00</td>
<td>19:68</td>
<td>m. –/-.</td>
</tr>
<tr>
<td>Mon Oct 25 2004 00:00</td>
<td>19:68</td>
<td>c. –/-.</td>
</tr>
<tr>
<td>Mon Oct 25 2004 00:00</td>
<td>19:68</td>
<td>m. –/-.</td>
</tr>
<tr>
<td>Tue Oct 26 2004 00:00</td>
<td>19:68</td>
<td>a. –/-.</td>
</tr>
<tr>
<td>Tue Oct 26 2004 00:00</td>
<td>19:68</td>
<td>c. –/-.</td>
</tr>
<tr>
<td>Tue Oct 26 2004 00:00</td>
<td>19:68</td>
<td>m. –/-.</td>
</tr>
<tr>
<td>Tue Oct 26 2004 00:00</td>
<td>19:68</td>
<td>c. –/-.</td>
</tr>
<tr>
<td>Tue Oct 26 2004 00:00</td>
<td>19:68</td>
<td>m. –/-.</td>
</tr>
<tr>
<td>Wed Oct 27 2004 00:00</td>
<td>19:68</td>
<td>a. –/-.</td>
</tr>
<tr>
<td>Wed Oct 27 2004 00:00</td>
<td>19:68</td>
<td>c. –/-.</td>
</tr>
<tr>
<td>Wed Oct 27 2004 00:00</td>
<td>19:68</td>
<td>m. –/-.</td>
</tr>
<tr>
<td>Wed Oct 27 2004 00:00</td>
<td>19:68</td>
<td>c. –/-.</td>
</tr>
<tr>
<td>Wed Oct 27 2004 00:00</td>
<td>19:68</td>
<td>m. –/-.</td>
</tr>
<tr>
<td>Date/Time</td>
<td>Size</td>
<td>Mode</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------</td>
<td>--------</td>
</tr>
<tr>
<td>Wed Oct 27 2004</td>
<td>450560</td>
<td>rwxrwxrwx</td>
</tr>
</tbody>
</table>
# Upcoming SANS Forensics Training

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
<th>Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instructor-Led Training</td>
<td>Mid-May</td>
<td>Alexandria, VA</td>
<td>May 17, 2020 - May 22, 2020</td>
</tr>
<tr>
<td>Autumn Australia Live Online 2020</td>
<td>Australia</td>
<td>May 18, 2020 - May 29, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Live Online - FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics</td>
<td>United Arab Emirates</td>
<td>May 19, 2020 - Jun 06, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>Live Online - FOR498: Battlefield Forensics &amp; Data Acquisition</td>
<td></td>
<td>May 26, 2020 - Jun 05, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>Live Online - FOR578: Cyber Threat Intelligence</td>
<td>United Arab Emirates</td>
<td>May 27, 2020 - Jun 26, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>Instructor-Led Training</td>
<td>Jun 1</td>
<td>IL</td>
<td>Jun 01, 2020 - Jun 06, 2020</td>
</tr>
<tr>
<td>SANS Pacific Live Online 2020</td>
<td>Singapore</td>
<td>Jun 08, 2020 - Jun 19, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANSFIRE 2020</td>
<td>DC</td>
<td>Jun 13, 2020 - Jun 20, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Live Online - FOR585: Smartphone Forensic Analysis In-Depth</td>
<td>United Arab Emirates</td>
<td>Jun 15, 2020 - Jun 26, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>Live Online - FOR500: Windows Forensic Analysis</td>
<td></td>
<td>Jun 22, 2020 - Jul 03, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>SANS Asia Pacific Live Online 2020</td>
<td>Singapore</td>
<td>Jun 22, 2020 - Jun 27, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Cyber Defence Australia Online 2020</td>
<td>Australia</td>
<td>Jun 22, 2020 - Jul 04, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS DFIR: Summer Breach 2020</td>
<td>United Arab Emirates</td>
<td>Jul 06, 2020 - Jul 11, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>DFIR Summit &amp; Training 2020</td>
<td>Virtual - US Eastern</td>
<td>Jul 16, 2020 - Jul 25, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Summer Cases: SANS DFIR 2020</td>
<td>United Arab Emirates</td>
<td>Jul 20, 2020 - Jul 31, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Summer Surge</td>
<td>Wave 2</td>
<td>NC</td>
<td>Jul 27, 2020 - Aug 01, 2020</td>
</tr>
<tr>
<td>Live Online - FOR578: Cyber Threat Intelligence</td>
<td>United Arab Emirates</td>
<td>Jul 28, 2020 - Aug 27, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>South by Southeast Asia Online 2020</td>
<td>Singapore</td>
<td>Aug 03, 2020 - Aug 08, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Special Investigations Week - SANS DFIR 2020</td>
<td>United Arab Emirates</td>
<td>Aug 03, 2020 - Aug 08, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Instructor-Led Training</td>
<td>Aug 3 ET</td>
<td>MA</td>
<td>Aug 03, 2020 - Aug 08, 2020</td>
</tr>
<tr>
<td>Instructor-Led Training</td>
<td>Aug 3 MT</td>
<td>CA</td>
<td>Aug 03, 2020 - Aug 08, 2020</td>
</tr>
<tr>
<td>Instructor-Led Training</td>
<td>Aug 10 MT</td>
<td>WA</td>
<td>Aug 10, 2020 - Aug 15, 2020</td>
</tr>
</tbody>
</table>