Forensic Examination of USB Data storage artifact

Client: CC Terminals

Author: Ben Reardon BE, CISSP
Date: 31 March 2005

As part of requirements for
GIAC Certified Forensic Analyst (GCFA)

Practical Assignment
Version 2.0
Option 1

Table of Contents

1. **Abstract** 1

2. **Document Conventions** 2

3. **Definitions** 2

4. **Executive Summary** 3

5. **Background** 4

6. **Examination Details** 5

6.1 Preservation of Image 6
6.2 Documentation of Image Integrity 6
6.3 File typing of image 7
6.4 Examination of Partition Table using “mmls” 7
6.5 Extraction of partitions using “dd” 8
6.6 Extracting human readable strings 9
6.7 Introducing the “Dirty Words” list 10
6.8 Extracting “Dirty words” from the data structure 11
6.9 Autopsy Forensic Browser 11

7. **Image Details** 12

7.1 File analysis using the mount utility 12
7.2 File analysis using Autopsy 13
7.3 Impact of File system type on MAC Times 14
7.4 Examination of undeleted file space 14
7.4.1 Undeleted File `her.doc` 15
7.4.2 Undeleted File `hey.doc` 15
7.4.3 Undeleted File `coffee.doc` 16
7.5 Examination of deleted file space 16
7.5.1 Deleted File `_apture` 17
7.5.2 Deleted file `_ap.gif` 19
7.5.3 Deleted File `WinDump.exe` 19
7.5.4 Deleted File `WinPcap_3_1_beta_3.exe` 22

8. **Forensic examination of WinDump and WinPcap** 24

8.1 Relationship between WinDump and WinPcap 24
8.2 Description 24
8.3 Potential Uses 24
8.4 Installation of WinPcap 25

8.5 Installation of WinDump 25
8.6 Usage 25
8.7 Extracting information from the data capture 26
8.8 Time of use 27

9. Timeline Summary 29

10. Legal and Policy Implications 30

10.1 Organisational Policies 30
10.1.1 Acceptable Use Policy 30
10.1.2 Code of conduct 30
10.1.3 Privacy Policy 31
10.2 Legal Considerations 31
10.2.1 Sexual harassment Legislation 31
10.2.2 Workplace bullying Taskforce 31
10.2.3 Telecommunication (Interception) Act 1979 32

11. Recommendations 32

12. Additional Information 34

12.1 Technical Matters 34
12.2 Legal Matters 35

13. References 35

List of Figures

Figure 1: Autopsy “File Analysis Screenshot” 13
Figure 2: Ethereal “Find Packet” String Search. 17
Figure 3: Street map by MapPoint. 19
Figure 4: File WinDump.exe viewed in Hex editor. 20
Figure 5: MD5 comparisons of WinDump.exe (retrieved and source file). 21
Figure 6: Autopsy details - WinPcap 3 1 beta 3.exe 23
Figure 7: Notepad view of binary file apture 27

1. Abstract

This assignment constitutes one of the admission requirements to the GIAC Certified Forensic Analyst (GCFA) certification program.

The purpose of the assignment is for the writer to demonstrate the following

- A mastery and deep understanding of technical forensic analysis tools and methods.
- General investigative skills.
- Quality report writing skills.

This report has been prepared to answer the questions posed by the assignment requirements, as well as attempting to provide a useful reference to any individual interested in the area of Forensic methodology. The report is written in the form of a professional report that is to be provided to the Client (CC Terminals) by the company that has been commissioned to conduct the investigation and author the report (BJR Forensics).
All companies, individuals and circumstances mentioned in this report are fictional. Any resemblance to any company, individual or set of circumstances (past, present or future) are entirely co-incidental and unintended.

This report is necessarily highly technical in many areas.
It has been prepared following an intensive 6-day training course in Forensic methodology and the usage of a wide range of Forensic tools.
The intended audience for the majority of this document possesses a substantial IT background in the Windows and UNIX environment, preferably with a broad understanding of Forensic methods, file systems and investigative methods.

2. Document Conventions

The following table illustrates the conventions used to denote the various contexts of text.

`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
http://nnnnn.com.au	Web URL's are shown in this style.
Quotation	A citation or quotation from a book or web site is in this style.

3. Definitions

The following table defines abbreviations used in this document

USB	Universal Serial Bus
MAC	Modified, Accessed, Created times
MSB	Minimum Security Baseline
SOE	Standard Operating Environment
TIA	Telecommunications (Interception) Act
SANS	SysAdmin, Audit, Network, Security
GIAC	Global Information Assurance Certification

4. Executive Summary

BJR Forensics have been commissioned by CC Terminals to conduct a forensic investigation following a complaint made by a female staff member (Ms Conlay) against a male staff member (Mr. Lawrence).

Ms Conlay claims that fellow staff member, Mr. Lawrence, was harassing her. The harassment allegedly took place both inside and outside of work hours. According to Ms Conlay's statement, a series of incidents culminated in an after-hours encounter while Ms Conlay was dining with a third party. Actions by Mr. Lawrence during the following day led finally to Ms Conlay making a formal complaint to her employer.

A statement by Mr. Lawrence on this matter is not available at the time this report was compiled.

The purpose of the commission is to attempt to establish the validity of Ms Conlay's claims of harassment. Further to forensic analysis, recommendations for ongoing actions, policy compliance and legal comment are also made within this report.

The findings of this commission strongly support Ms Conlay's claim of harassment by Mr. Lawrence.

The evidence supporting this outcome was retrieved from a data storage device found in Mr. Lawrence's work area. Most likely through the use of electronic interception software found on the device, parts of Ms Conlay's private email conversations appear to have been intercepted by Mr. Lawrence.
This information included the location of Ms Conlay's after hours rendezvous with a third party. The form of this information includes an email conversation, and a street directory map showing the location of the rendezvous. The files that contained this information were deleted from the storage device, however were retrieved using forensically sound methodology.

In addition to the deleted files, several data files were retrieved that appear to be authored by Mr. Lawrence. These files indicate a series of communication from Mr. Lawrence to Ms Conlay. At no stage was any reciprocal communication observed. The nature of these communications grew steadily more aggressive and ultimately became hostile enough for Ms Conlay to raise the complaint against Mr. Lawrence.

The forensic analysis supports the concept that Mr. Lawrence is in clear breach of the internal policies of CC Terminals. These breaches are explored in detail and should be considered during any course of action that CC Terminals may consider appropriate against Mr. Lawrence.

5. Background

The following background information describes the circumstances of this case.

> -------------------------~~---------------------------
>
> *Robert Lawrence is employed at CC Terminals, a credit card processing firm. Robert works as a sales representative, selling credit card processing terminals. Leila Conlay is also a sales representative at CC Terminals.*
>
> *On the afternoon of Friday October 29th, Leila contacted corporate security, stating she was being harassed by Robert Lawrence. Leila stated that Robert has made numerous attempts to meet her, both during and outside of work. Leila also stated that Robert has contacted her at her personal email address, and that his emails have become increasingly aggressive. On the evening of Thursday October 28th, Leila was at a coffee shop with a friend when Robert appeared. The next day she contacted corporate security.*
>
> *An after hours search of Robert's cubicle turned up a USB Flashdrive. The security administrator Mark Mawer has asked you to analyze the USB drive and provide a report of your findings prior to returning it to Robert. He provides you with a chain of custody form with the following information:*
>
> -------------------------~~---------------------------

6. Examination Details

The key piece of evidence in this case is a USB Flashdrive found in the work area of Mr. Lawrence in an after-hours search. The artifact was released to BJR Forensics by the security Administrator for CC Terminals, Mr. Mark Mawer. Identification attributes are attached to the artifact in a non-destructive manner. This identification allows for positive identification of the evidence at any time, and supports the requirements of a verifiable chain of custody.
The evidence handover process is recorded in the evidence custody journal, which is held in a secure safe.
The following table shows the attributes documented in the journal.

Case ID	1064
Case name	CC Terminals
Evidence ID	1064-1
Owner of evidence	CC Terminals / Mr. Robert Lawrence
Evidence obtained date	29 October 2004
Evidence obtained location	CC Terminals – Robert Lawrence work area
Form of identification	Tag
Identification Information	Tag #: USBFD-64531026-RL-001 Description: 64M Lexar Media JumpDrive Serial #: JDSP064-04-5000C Image: USBFD-64531026-RL-001.img MD5: 338ecf17b7fc85bbb2d5ae2bbc729dd5
Evidence Released by (name+sign)	Mark Mawer (signed......)
Released date/time	29 October 2004 17:30
Evidence Accepted by (name+sign)	Ben Reardon (signed......)
Accepted date/time	29 October 2004 17:30
Special Instructions	None given

Due to the potential nature of subsequent proceedings and likelihood of law enforcement involvement, fingerprinting analysis of the USB Flashdrive was considered. In this case, fingerprinting was not considered necessary, however care was taken to handle the specimen with minimal disturbance.

All tools that are used in the forensic analysis of this image are open source and freely available on the internet. These tools are forensically sound in that they conform to the key requirements of verification and repeatability, such that the results may be verified against any other forensically sound tools.
In order to support third party verification efforts, the methods used are recorded in this document to the extent that precise commands are available so that an independent competent forensic professional may validate the results.

6.1 Preservation of Image

Immediately upon receipt of the USB image, preservation of its pristine state was achieved.
The purpose of the discipline of preservation is to ensure that the evidence has not been tampered with, or altered in any unknown and/or unrepeatable way as a result of any subsequent forensic analysis.
Once the integrity of the image was assured, analysis was performed on copies, allowing for a comparison of the copy and original at any stage. This guarantees the copies have not been changed and are still relevant and dependable.

The platform on which the forensic analysis was carried out was Linux Fedora Core 2 (kernel 2.6.5-1.358)
Immediately the image was loaded onto the system, appropriate file permissions were applied to give the following attributes.

	Read file	Write to file	Execute
Owner (root)	**Yes**	No	**Yes**
Group	No	No	No
Other	No	No	No

This corresponds to the standard UNIX file permission triplet of “500”.

To ensure that the file is owned by the root account, the chown command must be issued as shown.

```
root@LinuxForensics image# chown root USBFD-64531026-RL-001.img
root@LinuxForensics image# chmod 500 USBFD-64531026-RL-001.img
root@LinuxForensics image# ls -al USBFD-64531026-RL-001.img
-r-x------  1 root root 62439424 Mar  9 22:53 USBFD-64531026-RL-001.img
root@LinuxForensics image#
```

Further in the analysis, we will see another technique of “mounting the image as a file system” in read only mode. This has a similar result, in that it maintains integrity of the system by ensuring files cannot be changed, however is a fundamentally different method.

6.2 Documentation of Image Integrity

Documentation of the image integrity is performed by the use of the MD5 hashing algorithm. This tool provides a one-way fingerprinting functionality. This tool takes the entire image file as an input, and outputs a 32 byte unique “fingerprint” called an “MD5 checksum”. Since it is virtually mathematically impossible (see ref [a]) that two different files will never share the same MD5 checksum, this implies that any two files that have the same MD5 hash are identical down to the byte.

```
root@LinuxForensics image# md5sum USBFD-64531026-RL-001.img
338ecf17b7fc85bbb2d5ae2bbc729dd5  USBFD-64531026-RL-001.img
root@LinuxForensics image#
```

The unique MD5 hash of the image is “338ecf17b7fc85bbb2d5ae2bbc729dd5”, which is unique to this image file. Any file with a different MD5 hash must be a fundamentally different file, and any file with the same MD5 sum will be the same file.
At various stages of the investigation, this property of the MD5 hashing algorithm is used to carry out checks on integrity of the files by comparing checksums with those determined and protected at the early stages of investigation.

At this stage, the evidence was considered protected in terms of its ongoing integrity and could therefore be confidently used as a benchmark throughout the investigation.

6.3 File typing of image

The file utility runs a series of tests against an input file in an effort to provide classification information as follows.

```
root@LinuxForensics image# file USBFD-64531026-RL-001.img
USBFD-64531026-RL-001.img: x86 boot sector
root@LinuxForensics image#
```

6.4 Examination of Partition Table using “mmls”

It is possible to run rudimentary analysis of the raw image file by simply extracting any human readable strings from it (this is covered later) . However, it is more helpful to extract and examine the partitions that comprise the raw image. This way, access to deleted file locations, and MAC times may be recovered.
Extracting the partition table from the image was carried out using the sleuthkit tool mmls. The mmls tool requires as input an image file and the media type.

It is most common for USB Flashdrives to be DOS formatted. Due to the wide support of the DOS format on the vast majority of platforms, this is the most useful format for flash drive manufacturers to use for these highly portable USB storage devices. Because of this, the –t option following mmls command specifies DOS as the type of file system.

```
root@LinuxForensics image# mmls -t dos USBFD-64531026-RL-001.img
DOS Partition Table
Units are in 512-byte sectors

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

A summary of these partitions follows
00: The primary partition table always takes up exactly the first sector of the disk.
01: Unallocated space. This is space left over from the primary partition sector, so will probably not have any data in it (only 31 sectors in size). It is however possible that this very small area of the image can still contain information left over from previous installs of the media.
02: This partition contains the data. The FAT16 format of the partition is important to note, the manner in which it stores the time that a file was accessed is explored later.
It is also a useful exercise to calculate the size of this partition in well-known terms.

121919 sectors * 512 bytes/sector * 1/(1024*1024) MByte/Byte = 59.53 MB

6.5 Extraction of partitions using "dd"

With the partition structures understood, the interesting partitions were extracted from the raw base image using the tool dd.
While there are many uses for the dd tool, it was used to segment the raw image into the original partitions. The segments that dd extracted were simply the partition boundaries reported by the mmls tool, used in the previous section.

A brief summary of the fields used with the dd tool follows.
if= input file, in this case, the raw USB image.
of= tells dd what file to store the resultant extracted partition as.
skip= tells dd where to skip to before starting the extraction, dd will start extracting from this point onwards. In the case of partition 02, the partition begins at block 32, which means dd must use a skip value of 32.
count= option tells dd how many blocks to extract. In the case of partition 2, mmls reported that the partition is 121919 blocks in size.

To check that the tool pulls the right amount of data from the raw image, a simple size calculation was performed as follows

121919 Blocks * 512KB/Block= 62422528 KB

The following command shows the extraction of partition 02: using dd with the options described above. As shown by the ls command, the size of the resultant file matches the expected value precisely.

```
root@LinuxForensics image# dd if=USBFD-64531026-RL-001.img of=USBFD-64531026-RL-001.partition2.dd skip=32 count=121919
121919+0 records in
121919+0 records out
root@LinuxForensics image# ls -al USBFD-64531026-RL-001.partition2.dd
-r-x------  1 root root 62422528 Mar 10 19:03 USBFD-64531026-RL-001.partition2.dd
```

Throughout the investigation, integrity of the various images and files was an imperative, so the file permission triplet of 500 was always assigned after creation of these files. MD5 checksums were also calculated for these extracted partitions in order to check the integrity throughout the investigation.

```
root@LinuxForensics image# chmod 500 USBFD-64531026-RL-001.partition*
root@LinuxForensics image# md5 USBFD-64531026-RL-001.partition*
51596dda30fc38f0df3556d6f115256d   USBFD-64531026-RL-001.partition1.dd
5f830a763e2144483f78113a8844ad52   USBFD-64531026-RL-001.partition2.dd
```

These md5 checksums were now saved to a text file and even this was protected using the triplet 500, so that it could be relied upon for future reference.

```
root@LinuxForensics image# md5 USBFD-64531026-RL-001.partition* > md5.sums
root@LinuxForensics image# chmod 500 md5.sums
root@LinuxForensics image# cat md5.sums
51596dda30fc38f0df3556d6f115256d   USBFD-64531026-RL-001.partition1.dd
5f830a763e2144483f78113a8844ad52   USBFD-64531026-RL-001.partition2.dd
root@LinuxForensics image#
```

6.6 Extracting human readable strings

The partitions extracted using the dd tool are in binary form. It is useful to extract any human readable strings that appear within the image. These strings may belong to deleted files, even those not referenced by inode structures.

The UNIX strings tool is used to extract text strings into a file for analysis at a

later stage.
It may also be useful to determine the exact byte a particular string occurs within the partition, so that the surrounding data structures may be viewed. To achieve this, the radix option is used to give the offset in bytes to the location of the string. In this way, the data structure can be accurately located and the vicinity searched for interesting data.

Using the strings tool to examine the small 31 block Partition 01: shown on the mmls output reveals no strings. Indeed opening this partition file with a hex editor shows nothing but zero's which means there is no data in this part of the image.

The following output shows the commands to extract the strings on the data partition (which was extracted earlier using the dd tool).
After the file is protected, the third command shows the first 10 entries, as an example of the strings attained.

```
root@LinuxForensics gcfa# strings --radix=d ./image/USBFD-64531026-RL-001.partition2.dd > ./image/USBFD-64531026-RL-001.partition2.dd.strings

root@LinuxForensics gcfa# chmod 500 ./image/USBFD-64531026-RL-001.partition2.dd.strings

root@LinuxForensics gcfa# head ./image/USBFD-64531026-RL-001.partition2.dd.strings
      3 MSWIN4.1
     43 NO NAME    FAT16   3
    104 8N$}
    201 r>8-t
    215 at=Nt
    389 Invalid system disk
    411 Disk I/O error
    428 Replace the disk, and then press any key
    472 IO      SYSMSDOS   SYS
 245248 HER     DOC
root@LinuxForensics gcfa#
```

6.7 Introducing the "Dirty Words" list

In any investigation, there exist certain words that would be of interest if they found as data. This list of interesting words is often called a "dirty words list". The appearance of these words could provide a lead into another aspect by analyzing the adjacent words and data structures.
An initial dirty words is prepared in the beginning of an investigation and words are added to it as information emerges.
In this case, the following words were considered interesting from the outset.

These words were based purely on the 3 paragraph case brief given in the Background briefing

Leila
Conlay
Robert
Lawrence
CC Terminals
coffee
Thursday
email

These words are saved in a file called dirtywords.txt.

6.8 Extracting "Dirty words" from the data structure

The strings extracted earlier were now examined for occurrences of any of the "dirty words".

The grep tool was used to find occurrences of the dirty words within the extracted strings.
An example of the grep command follows, showing the first 10 lines of output from this command. Note the byte offset given at the start of each string group, which was enabled by using the radix option described earlier.

```
root@LinuxForensics gcfa# grep -f dirtywords.txt ./image/USBFD-64531026-RL-
001.partition2.dd.strings | head
 271104 Robert Lawrence
 271172 Robert Lawrence
 284672 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?
 291560 Robert Lawrence
 291628 Robert Lawrence
 305152 Hey what gives?  I was drinking a coffee on thursday and saw you stop buy with
some guy!  You said you didn't want coffee with me, but you'll go have it with some random
guy???  He looked like a loser!  Guys like that are nothing but trouble.  I can't believe you did
this to me!  You should stick to your word, if you're not interested in going to coffee with me
then you shouldn't be going with anyone!  I heard rumors about a "bad batch" of coffee, hope
you don't get any...
 312052 Robert Lawrence
 312120 Robert Lawrence
1099198 GetTimeZoneInformation
1099412 GetFileInformationByHandle
root@LinuxForensics gcfa#
```

Clearly, there is interesting data that relates to this case at byte offset 284672 and 305152.
The files that represent these strings will be examined later using different

methods. The point of highlighting this method here is to support the validity of the forensic tools by producing the same results with more than one tool.

6.9 Autopsy Forensic Browser

Once the partitions are extracted, documented and protected, it is useful at this stage to introduce the “Autopsy Forensic Browser v2.03” [ref 2]. This package carries out many of the tasks performed by the tools in the Sleuthkit toolset. Autopsy is written by Brian Carrier as open source software.
It supplies a usable web based interface to the Sleuthkit toolset, in addition to substantial reporting and event sequencing tools.

7. Image Details

This section provides an analysis of the various files found on the USB device and describes how these may support Ms Conlay's complaint.

7.1 File analysis using the mount utility

To view the undeleted files on the image, the UNIX mount command was used. This method does not show deleted files, rather it replicates the file system as it would be seen on a normal computer as a drive letter.

Options for the mount command are briefly explained as follows.

ro – mount as read only, this means it is impossible for the files to be written to, even with root access. The fact that the file system is mounted in read only mode overrides any file permissions that may be associated within the file system.
loop – mount as loop device.
noatime – this option preserves the "Accessed" time of files when a file is read, or in any other way accessed. Note that mounting as read only also ensures no changes are made any MAC times, however the noatime is use here for completeness.
noexec - do not execute files. This is a safety precaution in case there is malicious code on the file system.
auto – This option automatically detects the type of file system being mounted. In this case, it was known partition was formatted as FAT16. The auto option is on by default, however the command is described for completeness.

The following output shows the dd command being used.

```
root@LinuxForensics mnt# mount -o ro,loop,noatime,noexec,auto /gcfa/image/USBFD-
64531026-RL-001.partition2.dd /mnt/USB_partition2/
root@LinuxForensics mnt# ls -al /mnt/USB_partition2/
total 80
drwxr-xr-x  2 root root 16384 Jan  1  1970 .
drwxr-xr-x  8 root root  4096 Mar 11 13:33 ..
-rwxr-xr-x  1 root root 19968 Oct 28 19:24 coffee.doc
-rwxr-xr-x  1 root root 19968 Oct 25 08:32 her.doc
-rwxr-xr-x  1 root root 19968 Oct 26 08:48 hey.doc
```

The `file` utility was run against these files, to determine the type of these files.

```
root@LinuxForensics mnt# file /mnt/USB_partition2/*
/mnt/USB_partition2/coffee.doc: Microsoft Office Document
/mnt/USB_partition2/her.doc:    Microsoft Office Document
/mnt/USB_partition2/hey.doc:    Microsoft Office Document
root@LinuxForensics mnt#
```

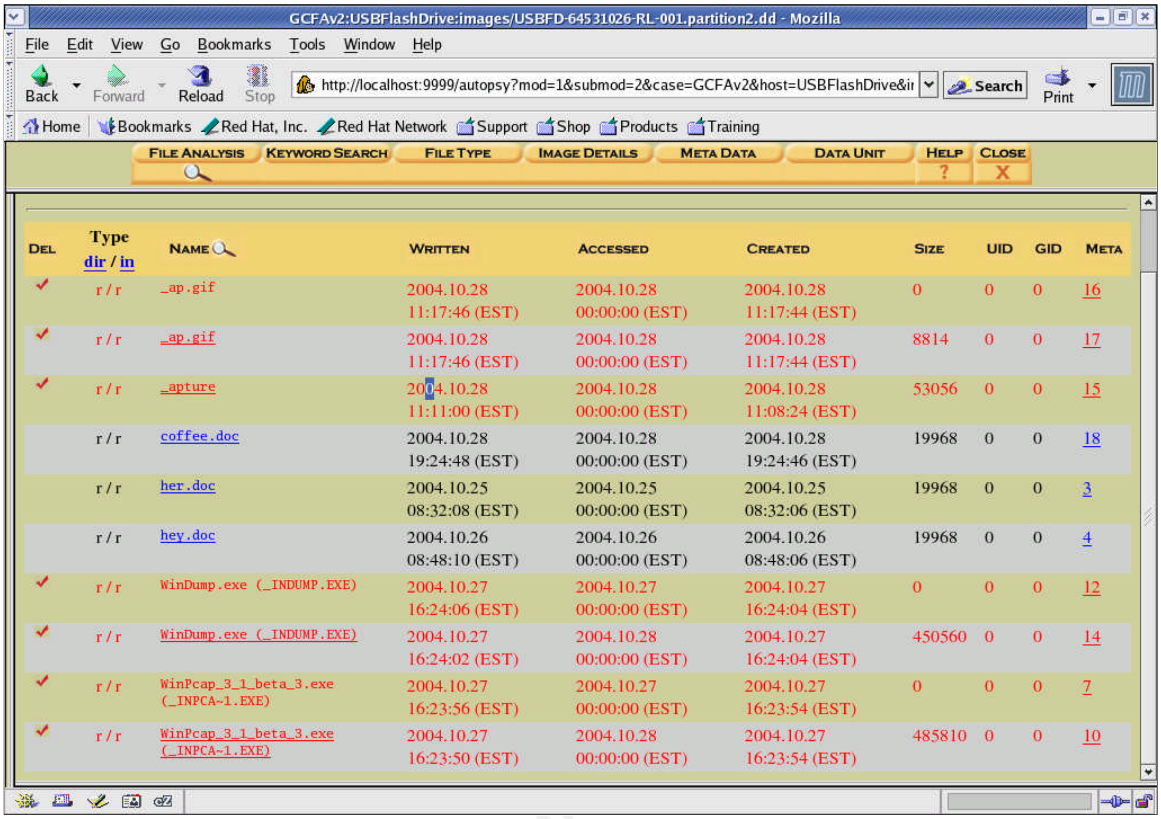
In order to compare these files with those recovered by alternative methods, MD5 checksums are required. Write access must first be re-granted to the previously created checksum file. The file triplet 700 allows full access to root for the addition of the MD5's of the word documents. After the completion of these a
additions, the file is locked down once more to read only (triplet 500)

```
root@LinuxForensics image# chmod 700 md5.sums
root@LinuxForensics image# md5 /mnt/USB_partition2/*.doc >> md5.sums
root@LinuxForensics image# chmod 500 md5.sums
root@LinuxForensics image# cat md5.sums
51596dda30fc38f0df3556d6f115256d     USBFD-64531026-RL-001.partition1.dd
5f830a763e2144483f78113a8844ad52     USBFD-64531026-RL-001.partition2.dd
a833c58689596eda15a27c931e0c76d1     /mnt/USB_partition2/coffee.doc
9785a777c5286738f9deb73d8bc57978     /mnt/USB_partition2/her.doc
ca601d4f8138717dca4de07a8ec19ed1     /mnt/USB_partition2/hey.doc
root@LinuxForensics image#
```

We will see later that these MD5 checksums are identical to the sums produced by other forensically sound methods.

7.2 File analysis using Autopsy

The screenshot shown below shows the allocated and unallocated (deleted) files that exist on the data partition as reported by the “file analysis” function of the Autopsy tool. The MAC times, size, ownership and Metadata information for the file structure is also shown.


GCFAv2:USBFlashDrive:images/USBFD-64531026-RL-001.partition2.dd - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
http://localhost:9999/autopsy?mod=1&submod=2&case=GCFAv2&host=USBFlashDrive&i
Search Print
Home Bookmarks Red Hat, Inc. Red Hat Network Support Shop Products Training
FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META
✓	r / r	_ap.gif	2004.10.28 11:17:46 (EST)	2004.10.28 00:00:00 (EST)	2004.10.28 11:17:44 (EST)	0	0	0	16
✓	r / r	_ap.gif	2004.10.28 11:17:46 (EST)	2004.10.28 00:00:00 (EST)	2004.10.28 11:17:44 (EST)	8814	0	0	17
✓	r / r	_apture	2004.10.28 11:11:00 (EST)	2004.10.28 00:00:00 (EST)	2004.10.28 11:08:24 (EST)	53056	0	0	15
	r / r	coffee.doc	2004.10.28 19:24:48 (EST)	2004.10.28 00:00:00 (EST)	2004.10.28 19:24:46 (EST)	19968	0	0	18
	r / r	her.doc	2004.10.25 08:32:08 (EST)	2004.10.25 00:00:00 (EST)	2004.10.25 08:32:06 (EST)	19968	0	0	3
	r / r	hey.doc	2004.10.26 08:48:10 (EST)	2004.10.26 00:00:00 (EST)	2004.10.26 08:48:06 (EST)	19968	0	0	4
✓	r / r	WinDump.exe (_INDUMP.EXE)	2004.10.27 16:24:06 (EST)	2004.10.27 00:00:00 (EST)	2004.10.27 16:24:04 (EST)	0	0	0	12
✓	r / r	WinDump.exe (_INDUMP.EXE)	2004.10.27 16:24:02 (EST)	2004.10.28 00:00:00 (EST)	2004.10.27 16:24:04 (EST)	450560	0	0	14
✓	r / r	WinPcap_3_1_beta_3.exe (_INPCA~1.EXE)	2004.10.27 16:23:56 (EST)	2004.10.27 00:00:00 (EST)	2004.10.27 16:23:54 (EST)	0	0	0	7
✓	r / r	WinPcap_3_1_beta_3.exe (_INPCA~1.EXE)	2004.10.27 16:23:50 (EST)	2004.10.28 00:00:00 (EST)	2004.10.27 16:23:54 (EST)	485810	0	0	10

Figure 1: Autopsy "File Analysis Screenshot"

7.3 Impact of File system type on MAC Times

The FAT16 file system displays the "Accessed Time" of a file to the nearest *date* only [ref 6]. The Accessed time shown by the MAC times of a FAT file structure will show the date that the file was accessed, not the time. The remaining fields Modified (Written), and Created show the time accurate to the second.
This is important for this investigation as it means we cannot determine the exact time a file was last accessed, rather we know the *day* it was accessed.

Because of this behavior, the fields under the Accessed column on the Autopsy output show 00:00:00 as the accessed time.

Another facet of the FAT file system is that the times stored are not time zone aware and are stored as raw offsets from GMT.

7.4 Examination of undeleted file space

As seen earlier with the mounted image, there exist three undeleted files. Autopsy shows these as blue on the screenshot shown in Figure 1. These files can be retrieved by using the export option that Autopsy provides.

The file extensions suggest these files may be word processor files. However, file extensions can easily be changed, so the ".doc" file extension by no means confirms that the files are word processor files.

To confirm the nature of these files, the file command was used and this confirmed they are of the type "Microsoft Office Document".

```
root@LinuxForensics exported from Autopsy# file *.doc
coffee.doc: Microsoft Office Document
her.doc:    Microsoft Office Document
hey.doc:    Microsoft Office Document
```

To ensure that the tools being used are forensically sound, these files should be identical to those retrieved earlier using the mounted file system. This check was done by comparing the MD5 sums of the two sets of files.

```
root@LinuxForensics gcfa# md5 /mnt/USB_partition2/*
a833c58689596eda15a27c931e0c76d1 /mnt/USB_partition2/coffee.doc
9785a777c5286738f9deb73d8bc57978 /mnt/USB_partition2/her.doc
ca601d4f8138717dca4de07a8ec19ed1 /mnt/USB_partition2/hey.doc

root@LinuxForensics gcfa# md5 /gcfa/exported\ from\ Autopsy/*.doc
a833c58689596eda15a27c931e0c76d1 /gcfa/exported from Autopsy/coffee.doc
9785a777c5286738f9deb73d8bc57978 /gcfa/exported from Autopsy/her.doc
ca601d4f8138717dca4de07a8ec19ed1 /gcfa/exported from Autopsy/hey.doc
root@LinuxForensics gcfa#
```

Since these two sets of MD5 checksums are identical, this confirms the two methods produced precisely identical files, so supports the forensic soundness of the tools being used. This match is expected of any forensically sound tool.

The retrieved documents were now examined in order to provide additional information relevant to the case.

7.4.1 Undeleted File `her.doc`

her.doc	
Type	Microsoft Office Document
Size	19968 bytes
user/group	nobody/nobody

Last Modified	Monday 25 October 2004 08:32:08
Last Accessed	Monday 25 October 2004 00:00:00
Created	Monday 25 October 2004 08:32:06
Word data - Author	Robert Lawrence
Content	Hey I saw you the other day. I tried to say "hi", but you disappeared??? That was a nice blue dress you were wearing. I heard that your car was giving you some trouble. Maybe I can give you a ride to work sometime, or maybe we can get dinner sometime? Have a nice day

7.4.2 Undeleted File `hey.doc`

`hey.doc`	
Type	Microsoft Office Document
Size	19968 bytes
user/group	nobody/nobody
Last Modified	Tuesday 26 October 2004 08:48:10
Last Accessed	Tuesday 26 October 2004 00:00:00
Created	Tuesday 26 October 2004 08:48:06
Word data - Author	Robert Lawrence
Content	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?

7.4.3 Undeleted File `coffee.doc`

`coffee.doc`	
Type	Microsoft Office Document
Size	19968 bytes
user/group	nobody/nobody
Last Modified	Thursday 28 October 2004 19:24:48
Last Accessed	Thursday 28 October 2004 00:00:00
Created	Thursday 28 October 2004 19:24:46
Word data - Author	Robert Lawrence

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

7.5 Examination of deleted file space

Although some files had been deleted from the media, the data structure is intact. Therefore it was possible to extract 4 interesting deleted files from the unallocated portions of the image.

These 4 files are shown as red on the Autopsy screen capture on Figure 1. Details of these file are analyzed in this section.

7.5.1 Deleted File `_apture`

`_apture`	
Type	tcpdump capture file (little-endian) - version 2.4 (Ethernet, capture length 4096)
Size	53056 bytes
user/group	nobody/nobody
Last Modified	Thursday 28 October 2004 11:11:00
Last Accessed	Thursday 28 October 2004 00:00:00
Created	Thursday 28 October 2004 11:08:24

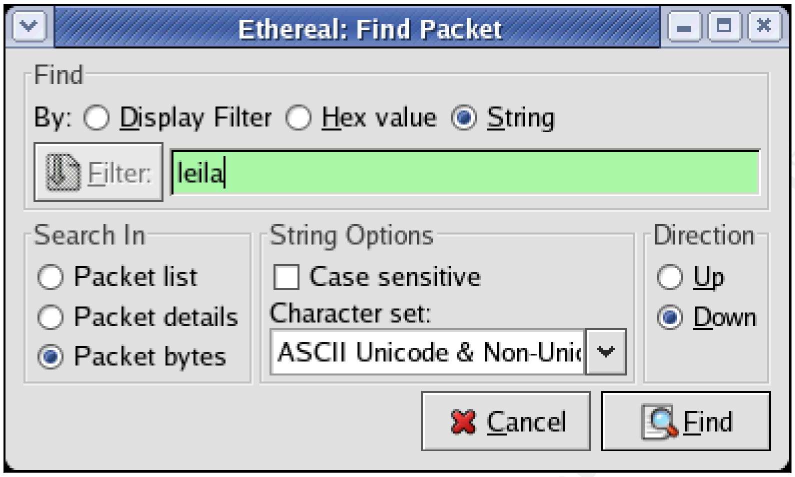
Being a tcpdump file, the file can be opened in tcdump or a similar network monitoring tool such as “Ethereal” [ref 1]. When opened, the contents of this file reveal numerous network connections occurring over an Ethernet TCP/IP network.

Analysis of the data streams using Ethereal reveals the following points of interest

The Network traffic was dominated by a TCP conversation between an internal network 192.168.2.104 and an external group of web servers.

The nature and content of the traffic suggests this is a standard http conversation to the Microsoft hotmail email service. There are numerous references to hotmail and associated services in the network traffic flows.

A simple text search was carried out within Ethereal to identify any occurrences of the words in the dirty words list. For example, any occurrence of the word “Leila” within the data streams was considered interesting. The following screenshot shows functionality of searching for Hex or plain string occurrences from within the data streams.



Find

By: ○ Display Filter ○ Hex value ● String

Filter: leila

Search In

○ Packet list
○ Packet details
● Packet bytes

String Options

□ Case sensitive

Character set: ASCII Unicode & Non-Unic

Direction

○ Up
● Down

Figure 2: Ethereal “Find Packet” String Search.

An occurrence of this string exists in the following POST command.

```
POST /cgi-bin/premail/2452 HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/vnd.ms-
powerpoint, application/msword, */*
Referer: http://by12fd.bay12.hotmail.msn.com/cgi-
bin/compose?&curmbox=F000000001&a=27d6f510deac1bac5415e72029263cd9
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)
Host: by12fd.bay12.hotmail.msn.com
Content-Length: 576
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: MC1=V=3&GUID=49A9B22A05294A1A81F11881BF3C264B; y=1;
MSPAuth=5Qr3f0LU3B54zQBmCG3iUtdaiAo608EFiBYmrtzv6oAL1cQ1ayApRce4N7XCEkk%2aa5e9H9c
W
S5x%21xBTivKy%2aSEwg%24%24;
MSPProf=5e1XcTCShGOf1gQhcClTXJM67JMAbywIG67BmEwf%2aNbKWq2vOyMjJTO2P1%2aaU%2av
iM
Tcr8nestOX6uJi5QYv9nb%21V3ReGZPm3yhrewvAYzs3vjyK4rdsGyuC2UGGRIga01ksxgsOTye%2aN6x
6R
SiEoVSY1B7nwcTwqlcErZoYBZYceDYvmlHy2W1RBkki3tMoJtq2IN4ZFwblNM%24;
PIM=1%2clang%2cEN%2ctabstyle%2c4%2ccluster%2cby12fd%252ebay12%252ehotmail%252emsn%2
52
ecom%2ctimestamp%2c1098692237%2csection%2cpersonal%2csubsection%2cInvalidSubSection;
mid=29ede1b79f320aa332327a4460; HMSatchmo=0; HMP1=1;
HMSC0899=224flowergirl96%40hotmail%2ecomrEM%2a5jEHcXVGV4%2aAWzQ6w%2a0KAj39KgAbJw
M3
dx89O12eFCP8QpvDRxtOmG0LfDW%2azTT3QAp7%2aslY6H2QtQ5HQXNkLZglQmXIy9iEXRtDjJoz9O
Yjo
xLF3Ma%2axDVQGszV4go%2au43pw8jYIglxM0UW%21z0ldqqhUN1TQ4ctSsc5TvwyIbDyDgcRpTSWI4
a5
eks5ccQVXfG4uV1JekTVpqRyBUcsm9mPtf5j55s7ZhD82ttArNKHEJD92eufZJ8AVnTljxVkdfoHs%2aAyv
%2
a4HRUpaX5MT3RkmxfvaHdNIXwLGY3eGw2iYFxTBWHxOhAZMfocojMk6YQHaSLzEp4ueB3Cq0fUl29nd
Ie
9jfW71zZRlTOxLaRk0LgudQuu%2aGGwyJX%21WH%2aUfLO%2aeKlnyxDTIY35xVxy0LwJQ7wGI7fxd%
2a
TBu%2apX7tNZYmw6n4bzSUMtIXi6f

curmbox=F000000001&HrsTest=&_HMaction=Send&FinalDest=&subaction=&plaintext=&login=flowergirl9
6
&msg=&start=&len=&attfile=&attlistfile=&eurl=&type=&src=&ref=&ru=&msghdrid=b16479b18beec291196
18
9c78555223c_1098692452&RTEbgcolor=&encodedto=SamGuarillo@hotmail.com&encodedcc=&encod
edb
cc=&deleteUponSend=0&importance=&sigflag=&newmail=new&to=SamGuarillo@hotmail.com&cc=&bcc=
&
subject=RE%3A+coffee&body=Sure%2C+coffee+sounds+great.++Let%27s+meet+at+the+coffee+shop+
on
+the+corner+Hollywood+and+McCadden.++It%27s+a+nice+out+of+the+way+spot.%0D%0A%0D%0ASee
+
you+at+7pm%21%0D%0A%0D%0A-LeilaHTTP/1.1 100 Continue
```

The interesting parts of the POST command are highlighted in yellow in the sample above. A summary of the interesting parts of the email follows. Note that since certain special characters cannot be represented properly within an http POST command, special characters are encoded in Unicode format [ref 3].

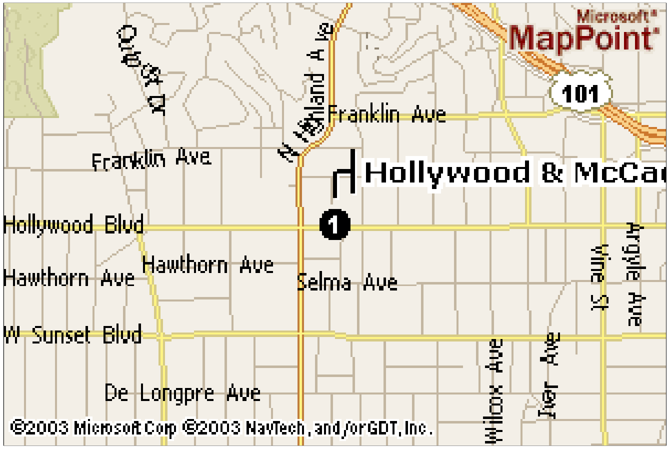
From: flowergirl96@hotmail.com
To: SamGuarillo@hotmail.com
Subject: Coffee
Body: Sure, coffee sounds great. Let's meet at the coffee shop on the corner Hollywood and McCadden. It's a nice out of the Way spot.

See you at 7pm!

-Leila

The email appears to be a invitation from Leila to a third party by the name Sam Guarillo. The invitation details meeting time, and a specific location.
Note also that this output contains Ms Conlay's personal email address. Mr. Lawrence may have contacted Ms Conlay at this address, as her initial statement describes.

7.5.2 Deleted file `_ap.gif`

`_ap.gif`	
Type	GIF image data, version 89a, 300 x 200
Size	8814 bytes
user/group	nobody/nobody
Last Modified	Thursday 28 October 2004 11:17:46
Last Accessed	Thursday 28 October 2004 00:00:00
Created	Thursday 28 October 2004 11:17:44
Content	 **Figure 3: Street map by MapPoint.**

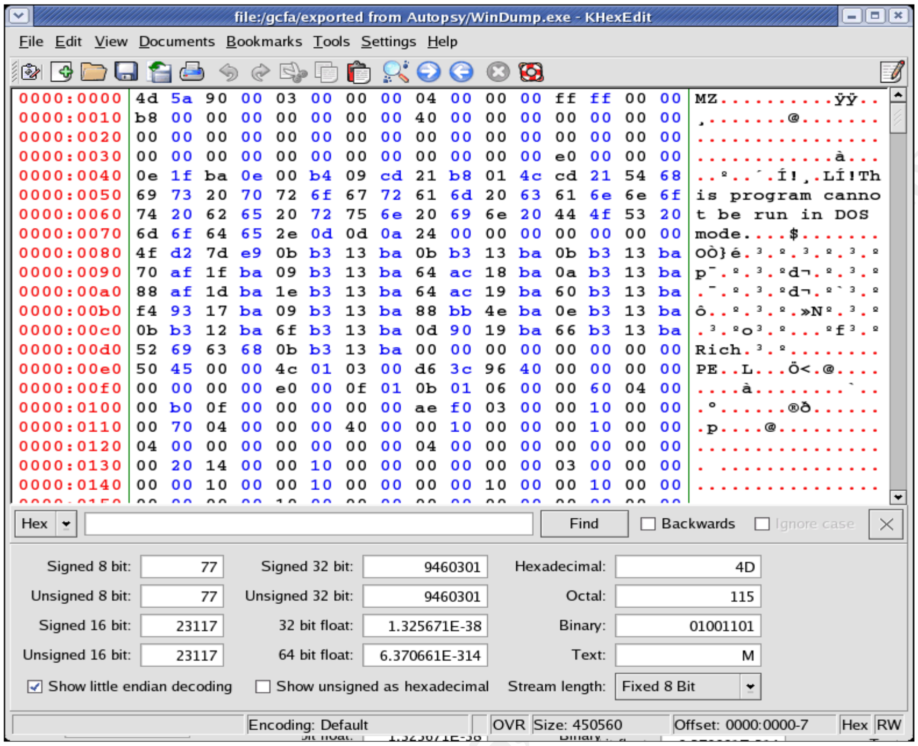
Notes	This file appears to be a street reference map showing the location “Corner of Hollywood and McCadden” This is the same location that Leila Conlay planned to meet Sam Guarillo at 7:00pm Thursday 28th October.

7.5.3 Deleted File `WinDump.exe`

`WinDump.exe`	
Type	MS-DOS executable (EXE), OS/2 or MS Windows
Size	450560 bytes
MD5 checksum	79375b77975aa53a1b0507496107bff7
user/group	nobody/nobody
Last Modified	Wednesday 27 October 2004 16:24:02
Last Accessed	Thursday 28 October 2004 00:00:00
Created	Wednesday 27 October 2004 16:24:04

From the MAC times, note that the file was created on the file system in the afternoon of Wednesday 27 October. It was last accessed sometime during the day of Thursday 28 October. For an executable file, this access is normally in the form of program execution. The timings relating to the running of this file is examined in more detail later.

This file was retrieved from its unallocated location using the Autopsy export function. Figure 4 shows the file opened up in a hex editor. Note the file header begins with “4d 5a” in Hexadecimal (MZ in ASCII), which is the standard Portable Executable File header.



file:/gcfa/exported from Autopsy/WinDump.exe - KHexEdit
File Edit View Documents Bookmarks Tools Settings Help

```
0000:0000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ..........ÿÿ..
0000:0010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ¸.......@.......
0000:0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0000:0030 00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00 ............à...
0000:0040 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 ..º..´.Í!¸.LÍ!Th
0000:0050 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f is program canno
0000:0060 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 t be run in DOS 
0000:0070 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 mode....$.......
0000:0080 4f d2 7d e9 0b b3 13 ba 0b b3 13 ba 0b b3 13 ba OÒ}é.³.º.³.º.³.º
0000:0090 70 af 1f ba 09 b3 13 ba 64 ac 18 ba 0a b3 13 ba p¯.º.³.ºd¬.º.³.º
0000:00a0 88 af 1d ba 1e b3 13 ba 64 ac 19 ba 60 b3 13 ba .¯.º.³.ºd¬.º`³.º
0000:00b0 f4 93 17 ba 09 b3 13 ba 88 bb 4e ba 0e b3 13 ba ô..º.³.º.»Nº.³.º
0000:00c0 0b b3 12 ba 6f b3 13 ba 0d 90 19 ba 66 b3 13 ba .³.ºo³.º...ºf³.º
0000:00d0 52 69 63 68 0b b3 13 ba 00 00 00 00 00 00 00 00 Rich.³.º........
0000:00e0 50 45 00 00 4c 01 03 00 d6 3c 96 40 00 00 00 00 PE..L...Ö<.@....
0000:00f0 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 60 04 00 ....à........`..
0000:0100 00 b0 0f 00 00 00 00 00 ae f0 03 00 00 10 00 00 .°......®ð......
0000:0110 00 70 04 00 00 00 40 00 00 10 00 00 00 10 00 00 .p....@.........
0000:0120 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 ................
0000:0130 00 20 14 00 00 10 00 00 00 00 00 00 03 00 00 00 . ..............
0000:0140 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 ................
```

Hex | | Find | □ Backwards | □ Ignore case

Signed 8 bit:	77	Signed 32 bit:	9460301	Hexadecimal:	4D
Unsigned 8 bit:	77	Unsigned 32 bit:	9460301	Octal:	115
Signed 16 bit:	23117	32 bit float:	1.325671E-38	Binary:	01001101
Unsigned 16 bit:	23117	64 bit float:	6.370661E-314	Text:	M

☑ Show little endian decoding □ Show unsigned as hexadecimal Stream length: Fixed 8 Bit

Encoding: Default | OVR | Size: 450560 | Offset: 0000:0000-7 | Hex | RW

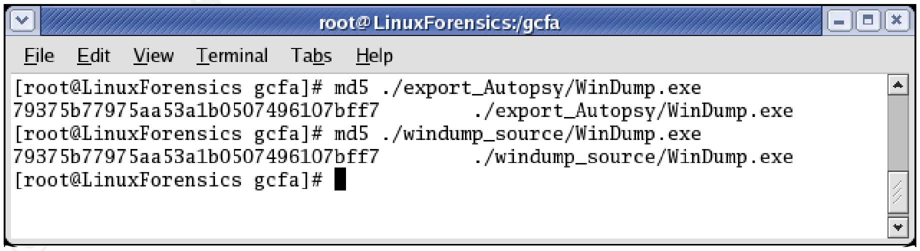
Figure 4: File WinDump.exe viewed in Hex editor.

The strings tool was then used to extract humanly readable strings of characters as before.
Within the resultant strings output, there appeared to be numerous references to various to the well-known “tcpdump” utility. This is used within a UNIX environment to carry out network traffic analysis. Since these files are referenced from within the WinDump.exe file, it is likely that the WinDump.exe file has some form of network monitoring ability.
The following output shows a sample of 10 occurrences of the word tcpdump occurring within the file windump.exe.

```
root@LinuxForensics export_Autopsy# cat WinDump.exe.strings | grep tcpdump | head
@(#) $Header: /tcpdump/master/tcpdump/addrtoname.c,v 1.96.2.6 2004/03/24 04:14:31 guy
Exp $ (LBL)
@(#) $Header: /tcpdump/master/tcpdump/bpf_dump.c,v 1.14.2.2 2003/11/16 08:51:04 guy Exp
$ (LBL)
@(#) $Header: /tcpdump/master/tcpdump/missing/datalinks.c,v 1.1.2.3 2003/11/16 09:29:48
guy Exp $ (LBL)
@(#) $Header: /tcpdump/master/tcpdump/missing/dlnames.c,v 1.2.2.3 2003/11/18 23:12:12
guy Exp $ (LBL)
@(#) $Header: /tcpdump/master/tcpdump/gmpls.c,v 1.2.2.2 2003/11/16 08:51:05 guy Exp $
(LBL)
@(#) $Header: /tcpdump/master/tcpdump/gmt2local.c,v 1.7.2.2 2003/11/16 08:51:06 guy Exp
$ (LBL)
@(#) $Header: /tcpdump/master/tcpdump/missing/inet_aton.c,v 1.4.2.2 2003/11/16 08:52:01
guy Exp $
@(#) $Header: /tcpdump/master/tcpdump/missing/inet_ntop.c,v 1.5.2.2 2003/11/16 08:52:01
guy Exp $
@(#) $Header: /tcpdump/master/tcpdump/missing/inet_pton.c,v 1.4.2.2 2003/11/16 08:52:01
guy Exp $
@(#) $Header: /tcpdump/master/tcpdump/machdep.c,v 1.10.2.3 2003/12/15 03:53:42 guy Exp
$ (LBL)
root@LinuxForensics export_Autopsy#
```

A simple Google search was carried out for the term “WinDump”. The results were dominated by links to the website http://windump.polito.it/. By examining this site [ref 4] , it is clear that the package is indeed the windows port of the UNIX tcpdump facility.

To confirm that the file was in fact the same package as the one described on the site, the source of the windump.exe was downloaded from the site in order for comparison.



```
[root@LinuxForensics gcfa]# md5 ./export_Autopsy/WinDump.exe
79375b77975aa53a1b0507496107bff7        ./export_Autopsy/WinDump.exe
[root@LinuxForensics gcfa]# md5 ./windump_source/WinDump.exe
79375b77975aa53a1b0507496107bff7        ./windump_source/WinDump.exe
[root@LinuxForensics gcfa]#
```

Figure 5: MD5 comparisons of WinDump.exe (retrieved and source file).

Since the file retrieved from the USB specimen produces an identical MD5 checksum to that downloaded from the Internet site, the files are identical. According to the documentation for the WinDump package, the network packet capture drivers within the WinPcap package need to installed in order for the WinDump package to function.

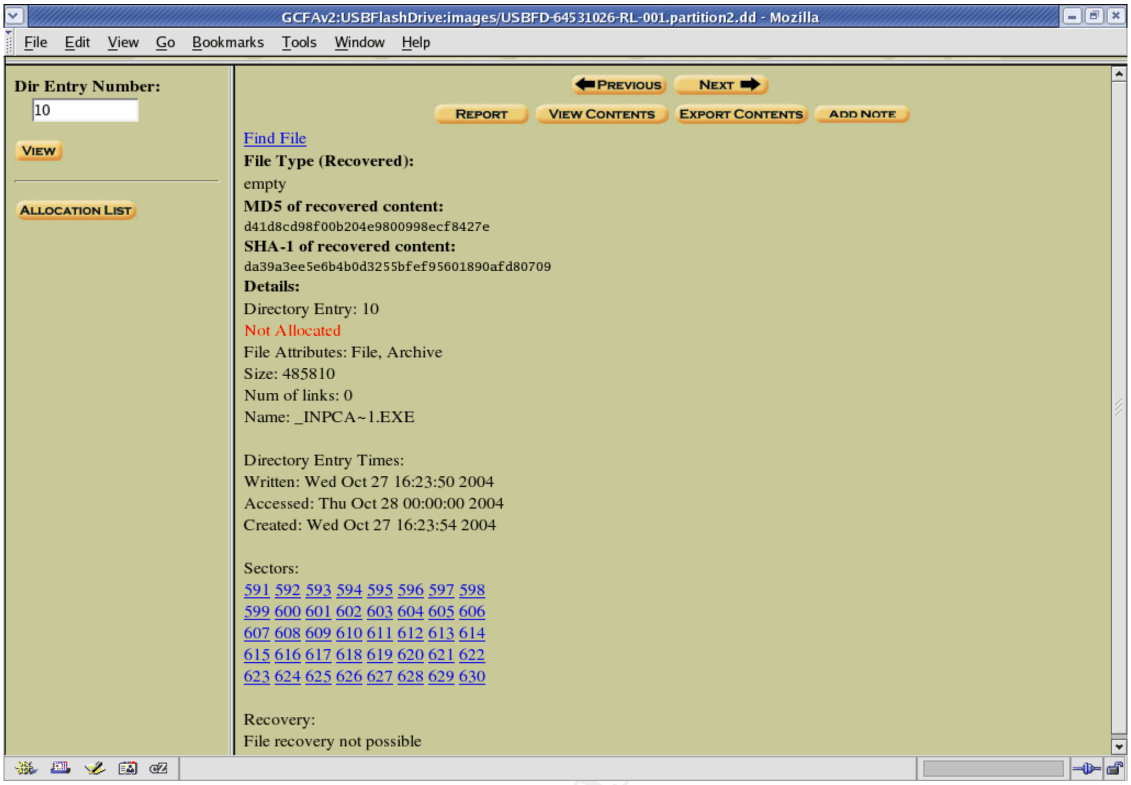
7.5.4 Deleted File `WinPcap_3_1_beta_3.exe`

WinPcap_3_1_beta_3.exe	
Type	MS-DOS executable (EXE), OS/2 or MS Windows
Size	485810 bytes
MD5 checksum	d41d8cd98f00b204e9800998ecf8427e
user/group	nobody/nobody
Last Modified	Wednesday 27 October 2004 16:23:50
Last Accessed	Thursday 28 October 2004 00:00:00
Created	Wednesday 27 October 2004 16:23:54

WinPcap [ref 5]is a library of software required by WinDump. The WinPcap software is a separate download, the current version is WinPcap_3_1_beta_4.exe.
It appears that the file extracted from the specimen is a previous version - beta 3. The maintainers of the software make these older versions available at http://windump.polito.it/misc/bin/WinPcap_3_1_beta_3.exe

To confirm that the file on the specimen is the same as the one available from the internet, the source of the file was downloaded from the site, for comparison.

Since the data structure for the file still exists, Autopsy is able to report on the file size, and MAC times described above. However, parts of the file must have been overwritten by subsequent disk writes, so the file cannot be recovered in entirety.
The following screenshot shows the Autopsy's output of file's details. Note the partial list of sectors it refers to, and the "File recovery not possible".


GCFAv2:USBFlashDrive:images/USBFD-64531026-RL-001.partition2.dd - Mozilla
File Edit View Go Bookmarks Tools Window Help
Previous
Next
Report
View Contents
Export Contents
Add Note
View
Allocation List

Dir Entry Number:
10

Find File
File Type (Recovered):
empty
MD5 of recovered content:
d41d8cd98f00b204e9800998ecf8427e
SHA-1 of recovered content:
da39a3ee5e6b4b0d3255bfef95601890afd80709
Details:
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

Figure 6: Autopsy details - WinPcap_3_1_beta_3.exe

Since the file is not recoverable, comparisons using MD5 checksums are not possible. Instead, the size of the file reported by Autopsy can be compared to that downloaded from http://windump.polito.it/misc/bin/WinPcap_3_1_beta_3.exe

Autopsy reports a size of 485810 (see screenshot above). The following confirms that the size of the file downloaded from the original source is identical. Considering the fact that this file is required by the WinDump package, and the file size is identical to the one available at the source site, it is extremely likely that this is the same file as downloaded from the source site.
The following output shows the size of the file that has been downloaded from the source site (highlighted as yellow).

```
root@LinuxForensics winpcap_source# ls -al
total 488
drwxr-xr-x   2 root root   4096 Mar 26 06:52 .
drwxr-xr-x   8 root root   4096 Mar 26 06:51 ..
-r-x------   1 root root 485810 Mar 26 06:52 WinPcap_3_1_beta_3.exe
root@LinuxForensics winpcap_source#
```

8. Forensic examination of WinDump and WinPcap

This section examines the main programs that would have allowed Mr. Lawrence to covertly monitor and intercept traffic originating from Ms Conlay's PC.

8.1 Relationship between WinDump and WinPcap

As described in the previous section, WinPcap is used by WinDump and must be installed on the system in order for WinDump to capture network packets. In this case, the primary package we examine is WinDump, since it is the tool that has allowed the network traffic to be collected.

8.2 Description

The WinDump package provides passive network monitoring functionality. Under normal circumstances, the host PC would simply disregard any traffic not specifically destined to it.
The WinDump package allows the host PC to read and process data streams that belong to neighboring hosts.
In human terms, the actions of this package would be analogous to eavesdropping on a conversation that you were not intended to hear.

The following description of WinDump is available at http://windump.polito.it/

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

8.3 Potential Uses

A typical uses of the WinDump software is for the analysis of network traffic, this can be useful while developing or debugging systems. Since the tool allows network traffic to be observed, captured and analyzed, it provides the developer a deeper understanding of how various software components interact at a very fine level of granularity.

Another use of the software is for nefarious purposes. Since the software allows for any network traffic to be inspected, this would allow a malicious individual to use the software to gain information to which he/she is not authorized.

The WinDump software would be of no value to an individual in the Credit Card

Terminal Sales Industry. Furthermore, such technology is not required for a Salesperson to carry out their job function.

8.4 Installation of WinPcap

The WinPcap package is available from
http://winpcap.polito.it/install/default.htm, currently at version 3.1 (beta 4).
It is installed most simply by the auto-installer executable, and following the instructions during the installation process.
A reboot is required after installation.

In order to install the package, the user must have administrator privileges to do so. In a corporate environment, these access rights are not generally available to normal users.

WinPcap also requires the user to be an administrator during the first execution of the program. This allows the driver to be dynamically installed on the system using the administrator's access rights. Any subsequent usage of the tool can then be a normal user (non-administrator).
This is explained in detail in the Winpcap FAQ's
http://winpcap.polito.it/misc/faq.htm#Q-7

8.5 Installation of WinDump

The WinDump package is a sole executable file called windump.exe. This file is downloaded from the source site and simply run in a command prompt. The file can exist anywhere on a system (e.g. in the local windows directory, or alternatively located on a removable device).

8.6 Usage

The windump.exe file is run at the command line with some simple options. The various options are described below and are available in full detail at http://windump.polito.it/docs/manual.htm.

The following **–D** option shows the network adapters installed.

```
C:\>winDump -D
1.\Device\NPF_GenericNdisWanAdapter (Generic NdisWan adapter)
2.\Device\NPF_{4BE66757-AD36-4C9D-98CA-41C804990310} (ADM8511 USB
To Fast Ethernet Adapter NDIS 5.0 Miniport Driver (Microsoft's
Packet Scheduler) )
3.\Device\NPF_{9E5F0689-882F-46F7-A693-BB8F8C403BB7} (Intel 8255x-
based Integrated Fast Ethernet (Microsoft's Packet Scheduler) )
C:\>
```

The **–i** option allows the selection of the network adapter

The following output shows WinDump listening on a local network adapter, and reporting on some subsequent ssh traffic on TCP port 22 on this adapter.

```
C:\>winDump -i \Device\NPF_{9E5F0689-882F-46F7-A693-BB8F8C403BB7}
winDump: listening on \Device\NPF_{9E5F0689-882F-46F7-A693-
BB8F8C403BB7}
23:20:37.982211 arp who-has LINUXFORENSICS tell STONKER
23:20:37.982404 arp reply LINUXFORENSICS is-at 00:d0:59:4a:6b:7a
23:20:37.982412 IP STONKER.1057 > LINUXFORENSICS.22: P
3298065723:3298065743(20)
 ack 1917741173 win 63945
23:20:37.992378 IP LINUXFORENSICS.22 > STONKER.1057: P 1:21(20) ack
20 win 7504
23:20:38.100758 IP STONKER.1057 > LINUXFORENSICS.22: . ack 21 win
63940
23:20:38.185560 IP STONKER.1057 > LINUXFORENSICS.22: P 20:40(20)
ack 21 win 6394
0
23:20:38.195355 IP LINUXFORENSICS.22 > STONKER.1057: P 21:41(20)
ack 40 win 7504
```

The **-w** option writes the output to a file in binary format so that it can be read later

The **-s** option is the "snaplength" that indicates how deep inside the data packet WinDump should process. Data in the packet that occurs after the snaplength variable is disregarded by WinDump. The default snaplength is 68 bytes, normally this is enough to debug network problems, and allows for optimal performance.
Setting the snaplength to zero forces WinDump to capture the entire packet (including headers and full data).
Inspecting the entire packet structure can require significant processing under heavily loaded network, however the network at CC Terminals appears to be relatively lightly loaded.

Using these command line options, it is probable that the following command has been used to produce the data file "_apture".

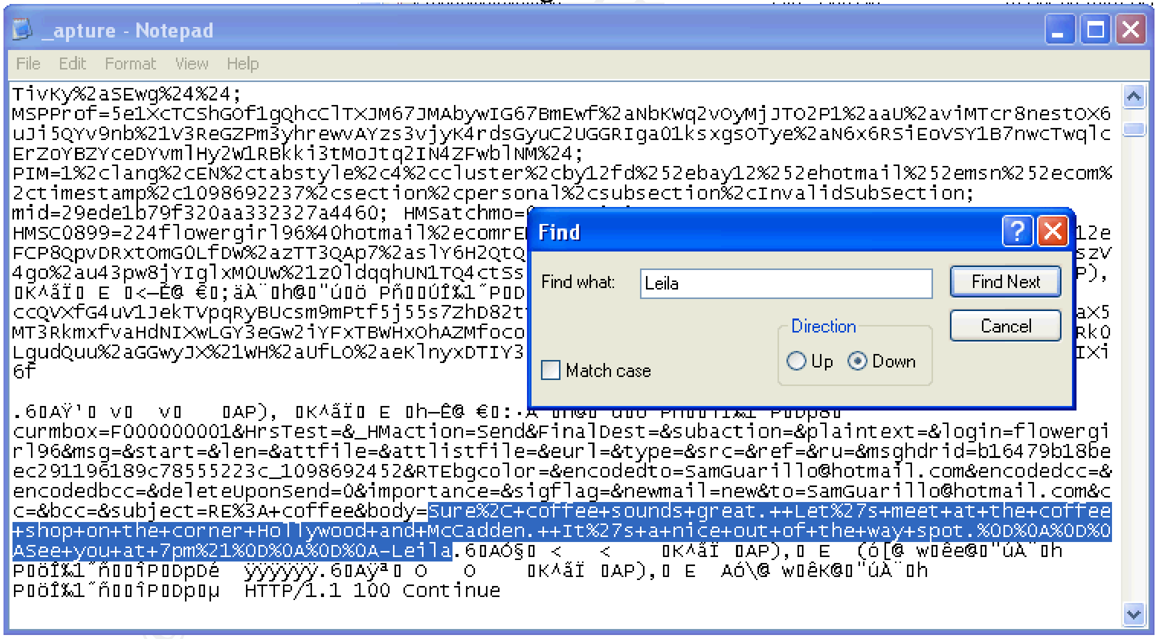
```
C:\>windump -i \Device\NPF_{4BE66757-AD36-4C9D-98CA-41C804990310} -
w capture -s 0
```

8.7 Extracting information from the data capture

Once the binary file is created by capturing the network traffic, the data file must

be examined by the malicious party.
This can be done in the following ways, listed in increasing level of likelihood and ease of execution.

- Use WinDump to re-query the binary file. As well as writing binary files, WinDump can be used to query these files in a command line environment.
- Graphical implementations of network monitoring tools such as Ethereal can be used to read these binary files, search for strings and filter out a specific conversation from the mass of data.
- For relatively small network traces such as this, it is a simple task to extract humanly readable strings from the binary file and examine these separately.
- It is most likely that Mr. Lawrence simply opened the file _apture with a text file editor and carried out a search for the word “Leila”. Even though the file contains binary data, the information pertaining to Ms Conlay’s plans for coffee with Sam Guarillo appears as clear ASCII text.
  The following screenshot shows the binary file when opened by notepad.exe. A simple text search for the word “Leila” shows the location of the interesting email text.



```
TivKy%2aSEwg%24%24;
MSPProf=5e1XcTCShGOf1gQhcClTXJM67JMAbywIG67BmEwf%2aNbKwq2vOyMjJTO2P1%2aaU%2aviMTcr8nestOX6
uJi5QYv9nb%21V3ReGZPm3yhrewvAYzs3vjyK4rdsGyuC2UGGRIgaO1ksxgsOTye%2aN6x6RSiEoVSY1B7nwcTwqlc
ErZoYBZYceDYvmlHy2W1RBkki3tMoJtq2IN4ZFwblNM%24;
PIM=1%2clang%2cEN%2ctabstyle%2c4%2ccluster%2cby12fd%252ebay12%252ehotmail%252emsn%252ecom%
2ctimestamp%2c1098692237%2csection%2cpersonal%2csubsection%2cInvalidSubsection;
mid=29ede1b79f320aa332327a4460; HMSatchmo=
HMSC0899=224flowergirl96%40hotmail%2ecomrE                                         12e
FCP8QpvDRxtOmGOLfDW%2azTT3QAp7%2aslY6H2QtQ                                         szV
4go%2au43pw8jYIglxMOUW%21zOldqqhUN1TQ4ctSs                                         P),
□K^ãÏ□ E □<—Ê@ €□;äA¨□h@□"ú□ö Pñ□□ÚÎ%1˜P□D
ccQVxfG4uV1JekTVpqRyBUcsm9mPtf5j55s7ZhD82tt                                        aX5
MT3RkmxfvaHdNIXwLGY3eGw2iYFxTBWHxOhAZMfoco                                         RkO
LgudQuu%2aGGwyJX%21WH%2aUfLO%2aeKlnyxDTIY3                                         IXi
6f

.6□AŸ'□ v□  v□   □AP), □K^ãÏ□ E □h—Ê@ €□:·A
curmbox=F000000001&HrsTest=&_HMaction=Send&FinalDest=&subaction=&plaintext=&login=flowergi
rl96&msg=&start=&len=&attfile=&attlistfile=&eurl=&type=&src=&ref=&ru=&msghdrid=b16479b18be
ec29119618 9c78555223c_1098692452&RTEbgcolor=&encodedto=SamGuarillo@hotmail.com&encodedcc=&
encodedbcc=&deleteUponSend=0&importance=&sigflag=&newmail=new&to=SamGuarillo@hotmail.com&c
c=&bcc=&subject=RE%3A+coffee&body=Sure%2C+coffee+sounds+great.++Let%27s+meet+at+the+coffee
+shop+on+the+corner+Hollywood+and+McCadden.++It%27s+a+nice+out+of+the+way+spot.%0D%0A%0D%0
ASee+you+at+7pm%21%0D%0A%0D%0A-Leila.6□AÓ§□ <    <     □K^ãÏ □AP),□ E  (ó[@ w□êe@□"úA¨□h
P□öÎ%1˜ñ□□îP□DpDé  ÿÿÿÿÿÿ.6□Aÿª□ O    O     □K^ãÏ □AP),□ E  Aó\@ w□êK@□"úA¨□h
P□öÎ%1˜ñ□□îP□Dp□µ  HTTP/1.1 100 Continue
```

Find what: Leila

Direction: ○ Up ● Down

□ Match case

Figure 7: Notepad view of binary file _apture

8.8 Time of use

In order to determine the time the WinDump file was used, the MAC times were observed for both the WinDump tool and the resultant binary file “_apture”.

The key pieces of information are as follows.

- The WinDump file was accessed (i.e. executed) sometime during the day of Thursday 28 October. The limitations of the FAT file system do not allow for any more granularity in terms of the "Accessed time"
- The file _apture was created at 11:08:24. As described earlier, this file format is peculiar to network monitoring tools such as WinDump, so it is most likely that the WinDump tool was executed at the very same time on the Thursday and produced to file _apture.

This information further supports Ms Conlay's claims. The timing of access this information has enabled Mr. Lawrence to learn the place of meeting between Ms Conlay and Sam Guarillo and thus be present at this location as described in Ms Conlay's statement.

9. Timeline Summary

The following timeline summarizes the activities and events that have been determined both by forensic examination of the data, and the statement made by Ms Conlay. For details of the files mentioned, please refer to earlier analysis.

Monday 25 October 2004

08:32:06 Word document *her.doc* created by Mr. Lawrence.
This appears to be an initial approach to Mr. Conlay, the tone of the document is polite.

Tuesday 26 October 2004

08:48:06 Word document *hey.doc* created by Mr. Lawrence.
After apparently being told by Ms Conlay to "get lost", Mr. Lawrence created this more aggressive document in which he invites Ms Conlay for coffee.

Wednesday 27 October 2004

16:23:44 WinPcap program saved onto the USB device

16:24:04 WinDump program saved onto the USB device

Thursday 28 October 2004

11:08:24 Binary file _apture created as a result of executed network sniffer WinDump.
This file records the email from Ms Conlay and Sam Guarillo, including the address and time of planned rendezvous

11:17:44 Image _ap.gif created.
This shows the rendezvous location in the form of a street map.

~19:00:00 According to Ms Conlay's statement, Mr. Lawrence appeared at the location where she was to meet Sam Guarillo for coffee.

19:24:46 Word document *coffee.doc* created by Mr. Lawrence.
In this document, Mr. Lawrence admits to being at the rendezvous location and becomes very aggressive and threatening.

Friday 29 October 2004

n/a Ms Conlay contacts corporate security where complaint is made

10. Legal and Policy Implications

The legal, social and organizational implications of this case are explored in this section of the report.

The nature of this examination, in particular in relation the organizational polices of purely hypothetical. The existence and nature of any document mentioned is based upon common levels of policy maturity seen in many reputable organizations.

10.1 Organisational Policies

The various policies of CC Terminals were examined to determine where Mr. Lawrence or Ms Conlay might have been in breach. As a governance mechanism, all staff at CC Terminals must understand and accept these policies during the induction program. There is also a requirement for review and acceptance on a bi-annual basis, this ensures staff maintain a current awareness of the policies at CC Terminals.

10.1.1 Acceptable Use Policy

This policy has been written by the HR, IT and Legal departments of CC Terminals and is intended to describe the ways the computer environment at CC terminals may be used in an acceptable fashion. It also specifically describes examples of unacceptable use.

In this case, the following aspects of this policy have been breached

- Installation of unapproved software.
- Monitoring of communication not specifically intended for the consumption of the individual involved.
- Use of computer equipment for excessive, non work related activities.
- Use of computer equipment for non work related activities during work hours.

10.1.2 Code of conduct

This policy is written by the HR and legal departments. The policy is based on providing a work environment free from sexism, racism, and religious or any other form of persecution.

Mr. Lawrence did not uphold the ideals of the Code of conduct in that he has aggressively pursued, annoyed and made a fellow staff member feel unsafe. Although some contact may have occurred in an environment outside of the standard work hours, CC Terminals expects its staff members to abide by the ideals of its code of conduct in after hours affairs especially in relation to other staff members.

The fact that the computing environment at CC Terminals was used to a large extent by Mr. Lawrence to support his activities, CC Terminals are right to consider themselves key stakeholders in any after hour activities that directly pertain to this issue.

10.1.3 Privacy Policy

The forensic evidence does not support the notion that the Privacy Policy has been breached.
Due to the indiscriminate nature of the WinDump tool in terms of its ability to monitor traffic in an indiscriminate manner, it is fortunate that customer details did not appear to have been transmitted on the network at the time of monitoring. If this were the case, the Privacy Policy would possibly have been breached in that sensitive customer details would have been monitored and stored in an unapproved and insecure method.

10.2 Legal Considerations

As required by the assignment brief, the following comments are based on Australian Federal Law and the Laws of the State of Queensland at the time of writing.

10.2.1 Sexual harassment Legislation

Although not necessarily of a sexual nature, the behavior of Mr. Lawrence may be argued to be so (or soon become so). For this reason, the relevant sexual discrimination legislation is identified here.

Sexual harassment is prohibited under State and Federal legislation as follows

Australian Federal Legislation Sex Discrimination Act 1984
State of Queensland Legislation Anti-Discrimination Act 1991

In terms of the potential application of these laws to this case, the definition of harassment revolves around the concept of "reasonableness". It could be argued that Mr. Lawrence did not act in a reasonable manner in his covert means and aggressive communication toward Ms Conlay.

10.2.2 Workplace bullying Taskforce

Although not a specific act of Parliament, the Queensland Government maintains the "Workplace Bullying Taskforce". This organization would be interested in the behavior of Mr. Lawrence.
This taskforce has attempted to quantify fiscal losses that Industry bears in as a result of workplace bullying.
It attempts to provide an education and reporting framework for the following pieces of legislation.

Industrial Relations Act 1999
Workplace Relations Act 1996 (Commonwealth)
Workplace Health and Safety Act 1995
WorkCover Queensland Act 1996
Anti-Discrimination Act 1991
Training and Employment Act 2000
Public Service Act 1996
Public Sector Ethics Act 1994

10.1.3 Telecommunication (Interception) Act 1979

The covert methods used by Mr. Lawrence to obtain information not meant for him probably would not be in explicit contravention to the current laws.
Since the incident took place at a private company, by staff members and involved no other external parties, the matter would probably not be pursued by local Law enforcement on this basis alone.
The actions of Mr. Lawrence in respect to his means of intelligence gathering would be of very great interest to a legal investigation, but would not form the basis of any prosecution in and of itself.

To put this aspect of the case into perspective, apart from the tools used to intercept the communications, the information gathered by Mr. Lawrence could well have been gained simply from overhearing a verbal conversation not intended for his ears.

In terms of relevant legislation, the Australian Federal Legislation Telecommunication (Interception) Act 1979 is the most relevant in this area.
An important amendment to this Act has been sought on several occasions since 2002 and was eventually approved by the Senate in November 2004, and became Operative in Dec 15 2004. The amendments attempts to clarify the rights of law enforcement to monitor email and Voice traffic both in transit and in an intermediary storage system. During the passing of this amendment, there was much discussion from a good many Law enforcement Authorities, consumer groups, and Government bodies on the details of the amendment, it's real intent and it's likely ramifications once sunset clauses are enforced. Links to further information regarding this issue are available in the references section.

11. Recommendations

During the course of the investigation, activities were identified that could further support this investigation. Although the forensic analysis is highly supportive of Ms Conlay's claims, it is likely that the evidence could be argued to be "circumstantial" in a court of law. For this reason, it is recommended that the following additional investigative work be carried out, in an effort to further strengthen the case. Some of these recommendations may also help mitigate the risk of future incidents of this nature.

These recommendations are outlined as follows.

- Obtain a statement from Mr. Lawrence on his version of events. Depending on his position on the matter and his cooperation in the investigation, specific questions may then be crafted. For example, he could be queried about his knowledge of the WinDump tool, Word documents, or the deleted street map image showing the street location of Ms Conlay's whereabouts the night of Thursday 28 October 2004.

- Organize a password change for all CC Terminals staff. This is to lessen the risk of user/password combinations that may have been compromised.

- Inspect Mr. Lawrence's PC area for signs of modems, or wireless access points that might allow future access to his PC other than through the approved channels.

- Determine the level of access that Mr. Lawrence's user account has (and has had) on his PC. In order to install the WinPcap software, administrative privileges are required. If it can be confirmed that Mr. Lawrence's account had admin rights, the case against him would be strengthened.

- Review firewall and proxy logs from Mr. Lawrence's user account in an effort to determine if any software (including the WinDump tool) has been downloaded.

- Examine Mr. Lawrence's PC for additional information relating to the case. Of particular interest would be the existence of any additional network capture files produced by the WinDump tool.

- Rebuild Mr. Lawrence's PC to the SOE, since it can be considered compromised.

- Review Minimum Security Baseline for CC Terminal's user PC's.

- Consider a switched Ethernet environment, rather than a network supported by hubs, so that sniffing network traffic would not be a trivial matter. A network supported by hubs by definition broadcast traffic out on all data ports. This form of Infrastructure makes carrying out unauthorized sniffing of network traffic a trivial matter. Providing a switched environment will mitigate (but not entirely diminish) the risk of promiscuous network monitoring such as that carried out by Mr. Lawrence

- Review the Acceptable Usage Policy to determine if changes required following any issues arising from this case.

- Log files from Mr. Lawrence's PC (log on, log off, file access etc) should be examined. These may provide extra support that Mr. Lawrence was at his terminal at the times of interest.

- Building access records – these may also prove Mr. Lawrence was present at the times of interest.

- Seek witness accounts of Mr. Lawrence being at his desk at the times of interest.

- Fingerprinting of USB device should be considered if the potential of the situation calls for this level of forensic analysis.

12. Additional Information

While preparing this assignment, various useful links were discovered that (in addition to the SANS Track 8 course notes) assisted the author understand the topics within.
They are provided here to acknowledge such useful sites, as well as provide any reader of this document with additional information.

Due to the length constraints and the need to keep the within the assignment guidelines, some subjects could not be explained as rigorously as some would prefer. Another purpose of providing these links is to direct the reader to a detailed and exhaustive representation of such areas.

12.1 Technical Matters

[a] **MD5 hashing algorithm weaknesses**
http://www.schneier.com/blog/archives/2005/03/more_hash_funct.html
http://pintday.org/kjell/archive/2005/03/10/74

[b] **The FAT File system**
http://www.ntfs.com/fat-folder-structure.htm

[c] **Open Source UNIX forensic tools**
http://www.opensourceforensics.org/tools/unix.html

[d] **The Honeynet Project**
http://honeynet.org/

12.2 Legal Matters

[x] **Telecommunications (Interception) Act 1979**
http://www.efa.org.au/Issues/Privacy/tia-bill2004-sc.html

[y] **Queensland University of Technology - Faculty of Law**
Concepts of 'Reasonableness' in Sexual Harassment
Journal Vol 3 No 1 2003
http://www.law.qut.edu.au/about/ljj/editions/v3n1/pace.jsp

[z] **Queensland Government – Workplace Bullying**
http://www.whs.qld.gov.au/taskforces/bullying/

2. References

[1] **Ethereal – Network Protocol Analyzer**
http://www.ethereal.com/

[2] **Autopsy v2.03**
http://www.sleuthkit.org/autopsy/

[3] **URL Encoding/Decoding and Escaped code**
http://scriptasylum.com/tutorials/encdec/encode-decode.html

[4] **WinDump homepage**
http://windump.polito.it/

[5] **WinPcap homepage**
http://winpcap.polito.it/

[6] **FAT MAC times**
http://www.sleuthkit.org/sleuthkit/docs/skins_fat.html