Interested in learning more?

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

Forensic Investigation of
USB Flashdrive Image
for CC Terminals

GIAC Certified Forensic
Analyst (GCFA)

Practical Assignment

Version 2.0

Assignment Option 1

Submitted
March 10, 2005

Rhonda Diggs, CISSP
Las Vegas, NV
Sept 28 – Oct 4, 2004

Table of Contents

Abstract

This report details the examination of a USB Flashdrive image for evidence of harassment. It will explain the forensic methodology used, the results of the investigation, the legal implications and recommendations to help avoid similar situations in the future.

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.

1.0 Executive Summary

This report details the forensic Investigation of the image of a USB Flashdrive received from Mark Mawer, security administrator for CC Terminals. Mr. Mawer requested that this image be examined for evidence relating to an employee's complaint of harassment. Leila Conlay, a sales representative for CC Terminals, reported to corporate security on October 29, 2004 that she was being harassed by Robert Lawrence who is also a sales representative for CC Terminals. Ms. Conlay stated that Mr. Lawrence has attempted to meet her both at work and outside of work including an appearance at a coffee shop where she was meeting a friend on October 28, 2004, in addition, he has her private email address and has been sending progressively more aggressive emails.

After validating the integrity of the image and processing the image with several well known and respected forensics tools, the examination of the image file found evidence of seven files, four of which had been deleted. Fortunately, three of the deleted files were able to be recovered intact and the one that could not be recovered intact was able to be positively identified. Three of the files were Microsoft Word documents which contained text consistent with the aggressive emails reported by Ms. Conlay. One of the files was a graphical image containing a map of the location of the coffee shop where Ms. Conlay met her friend. Two of the remaining files were programs which, when installed and run on a Windows computer, allow network traffic to be observed and recorded. Use of these programs on a corporate network by an individual who is not responsible for network security may be a violation of The Wiretap Act which can be punishable by up to five years in prison [1]. The final file found on the USB Flashdrive image contained recorded network traffic which included an email message sent by Ms. Conlay to her friend with the address of the coffee shop and the time of their meeting. The dates that all of these files were created, accessed, and deleted are consistent with the time frame of the harassment reported by Ms. Conlay occurring from October 25, 2004 to October 28, 2004.

Based on this evidence, it is possible to conclude that a person using this USB Flashdrive was harassing Ms. Conlay. There is forensic evidence that this person was Mr. Lawrence. Based on information embedded in the documents, the Microsoft Word program used to write the documents on the image was registered to Robert Lawrence. Finally, the person using this USB Flashdrive knew when and where Ms. Conlay was meeting her friend and looked up the address of the coffee shop in a mapping program. Based on Ms. Conlay's statement, it was Robert Lawrence who appeared at the coffee shop and subsequently sent her a threatening email.

2.0 Examination Details

This section of the report will provide detailed information about the forensic methodology and tools which were used and provide a step by step walk through of the examination.

2.1 The Forensic Computer and Tools

The forensic computer used for this examination was a Dell Latitude D600 laptop with 512 MB of RAM and a 30 GB hard drive. The laptop's operating system is Fedora Core 2 and the kernel version is 2.6.5-1.358. Forensic tools and programs used during this investigation include:

Autopsy Forensic Browser version 2.03
Ethereal Network Protocol Analyzer version 0.10.3
VMware Workstation version 4.5
OpenOffice.org 1.1.1
```
md5sum
fdisk
mmls
file
dd
strings
```

2.1.1 Autopsy Forensic Browser - http://www.sleuthkit.org/autopsy/

Autopsy Forensic Browser is a well known open source forensic tool. Here is a description of the tool and it's features from the web site [2] http://www.sleuthkit.org/autopsy/desc.php :

> The Autopsy Forensic Browser is a graphical
> interface to the command line digital forensic analysis
> tools in The Sleuth Kit. Together, The Sleuth Kit and
> Autopsy provide many of the same features as
> commercial digital forensics tools for the analysis of
> Windows and UNIX file systems (NTFS, FAT, FFS,
> EXT2FS, and EXT3FS).
>
> Evidence Search Techniques
>   * File Listing: Analyze the files and directories,
> including the names of deleted files. (screenshot)
>   * File Content: The contents of files can be viewed
> in raw, hex, or the ASCII strings can be extracted.
> When data is interpretted, Autopsy sanitizes it to
> prevent damage to the local analysis system.

3

Autopsy does not use any client-side scripting languages. (screenshot) (Sleuth Kit Informer #1)

    * Hash Databases: Lookup unknown files in a hash database to quickly identify it as good or bad. Autopsy uses the NIST National Software Reference Library (NSRL) and user created databases of known good and known bad files. (screenshot)

    * File Type Sorting: Sort the files based on their internal signatures to identify files of a known type. Autopsy can also extract only graphic images (including thumbnails). The extension of the file will also be compared to the file type to identify files that may have had their extension changed to hide them. (screenshot)

    * Timeline of File Activity: In some cases, having a timeline of file activity can help identify areas of a file system that may contain evidence. Autopsy can create timelines that contain entries for the Modified, Access, and Change (MAC) times of both allocated and unallocated files. (screenshot)

    * Keyword Search: Keyword searches of the file system image can be performed using ASCII strings and grep regular expressions. Searches can be performed on either the full file system image or just the unallocated space. An index file can be created for faster searches. Strings that are frequently searched for can be easily configured into Autopsy for automated searching. (screenshot)

    * Meta Data Analysis: Meta Data structures contain the details about files and directories. Autopsy allows you to view the details of any meta data structure in the file system. This is useful for recovering deleted content. Autopsy will search the directories to identify the full path of the file that has allocated the structure. (screenshot)

    * Data Unit Analysis: Data Units are where the file content is stored. Autopsy allows you to view the contents of any data unit in a variety of formats including ASCII, hexdump, and strings. The file type is also given and Autopsy will search the meta data

4

structures to identify which has allocated the data
unit. (screenshot)
    * Image Details: File system details can be viewed,
including on-disk layout and times of activity. This
mode provides information that is useful during data
recovery. (screenshot)

2.1.2 Ethereal Network Protocol Analyzer - http://www.ethereal.com/

In this case, the Ethereal Network Protocol Analyzer was used to evaluate the
network traffic capture file recorded with WinDump. Here is the description of the
tool and it's features from the web site [3] – http://www.ethereal.com/docs/user-
guide-sp/#ChIntroWhatIs

Ethereal is a network packet analyzer. A network
packet analyzer will try to capture network packets
and tries to display that packet data as detailed as
possible.
The following are some of the many features Ethereal
provides:

   *Available for UNIX and Windows.
   *Capture live packet data from a network interface.
   *Display packets with very detailed protocol
information.
   *Open and Save packet data captured.
   *Import and Export packet data from and to a lot of
other capture programs.
   *Filter packets on many criteria.
   *Search for packets on many criteria.
   *Colorize packet display based on filters.
   *Create various statistics.

2.1.3 VMware Workstation - http://www.vmware.com/

VMware Workstation allows multiple operating systems to be run virtually on the
same computer. This is very useful for installing and analyzing software that is
discovered in a forensic investigation. Here is a description of the tool and it's
features from the web site [4]
http://www.vmware.com/products/desktop/ws_features.html:
"Powerful Virtual Machine Software for the Technical Professional
Essential features such as virtual networking, live snapshots, drag and drop and
shared folders, and PXE support make VMware Workstation the most powerful
and indispensable tool for enterprise IT developers and system administrators."

5

2.1.4 OpenOffice.org - http://www.openoffice.org/

According to their web site [5], "OpenOffice.org is a free productivity suite compatible with all major office suites". In this case, OpenOffice.org was used on my Linux forensic computer to examine the three Microsoft Word documents found on partition 2 of the USB Flashdrive image. It was also used to create this report.

2.1.5 md5sum

The Linux command md5sum is used to verify the integrity of a file. As stated on the web site [6] http://www.linux-mag.com/2000-10/security_04.html :
"md5sum can be used to create a "fingerprint" of a file. The fingerprint is strongly dependent upon the contents of the file to which md5sum is applied. Any changes to the file will result in a completely different fingerprint" (Wreski 4).The md5sum command is used often in forensic investigation to validate the integrity of the original image and to document each file created or recovered by the investigation so the findings can be validated by another investigator at a later date.

2.1.6 fdisk

The Linux command fdisk is used to examine or change the partition table [7]. In this case, it was used to examine the original USB Flashdrive image for partition information.

2.1.7 mmls

The command mmls is a SleuthKit command used to display the layout of the media management systems, which include partition tables and disk labels as stated on the web site [8] http://www.sleuthkit.org/sleuthkit/man/mmls.html. In this case, it was used to examine the original USB Flashdrive image for partition information.

2.1.8 file

As stated on the web site [9] http://unixhelp.ed.ac.uk/CGI/man-cgi?file , the file command attempts to determine file type. "File tests each argument in an attempt to classify it. There are three sets of tests, performed in this order: filesystem tests, magic number tests, and language tests. The first test that succeeds causes the file type to be printed." In this case, the file command was used to gather information about the files that were generated and recovered during the investigation.

6

2.1.9 dd

As stated on the web site [10] http://wiki.linuxquestions.org/wiki/Dd , "The dd command copies data from one place to another. Dd can copy a CD to an ISO file, copy one partition to another, or restore an image file to a disk. Using the seek and count options, an individual sector of a disk can be extracted without having to wait for the entire rest of the disk to be read." In this case, the dd command was used to create the partition image files and to create specific sector image files for further investigation. As stated by Kevin Mandia, Chris Prosise and Matt Pepe in their book Incident Response & Computer Forensics [11], " The dd utility is the most reliable tool for creating a true forensic duplicate image. As long as the operating system kernel (Linux, Solaris, Osx or FreeBSD) recognizes the storage medium, dd will perform a complete, bit-for-bit copy of the original" (157).

2.1.10 strings

As stated on the web site [12] http://docsrv.sco.com:8457/en/AdvBashHowto/external.html , "Use the strings command to find printable strings in a binary or data file. It will list sequences of printable characters found in the target file" (Cooper). In this case, the strings command was used to evaluate partition image files for strings of text relevant to this case.

2.2 The Forensic Investigation Methodology

The forensic investigation methodology used for this examination was developed by the SANS Institute and taught by Rob Lee in the Systems Forensics, Investigation & Response class. It consists of the eight steps shown below [13]:

1. Verification
2. System Description
3. Evidence Collection
4. Timeline Creation and Analysis
5. OS-Specific Media Analysis
6. Data Recovery
7. String Search
8. Reporting (5)

In this case, the first three steps of the methodology were performed by corporate security at CC Terminals. Based on the complaint by Ms. Conlay, they had verification of a possible security incident. The USB Flashdrive was found in Robert Lawrence's work area during an after hours search by corporate security in response to Ms. Conlay's complaint. Corporate security then created a digital

7

image of the USB Flashdrive in a forensically sound manner. One possible
process for creating a forensically sound digital image might be as shown below:

1. Take a md5 hash of the USB Flashdrive [11] (201)
2. Create a digital image of the USB Flashdrive using dd
3. Take another md5 hash of the USB Flashdrive
4. Compare md5 hashes to insure that no changes were made to the original
   USB Flashdrive in the process of creating the digital image
5. Take a md5 hash of the digital image
6. Compare md5 hashes of the USB Flashdrive and the digital image

The remaining five steps comprise the methodology I used in my examination of
the digital image and are detailed below starting with Subsection 2.3.3.
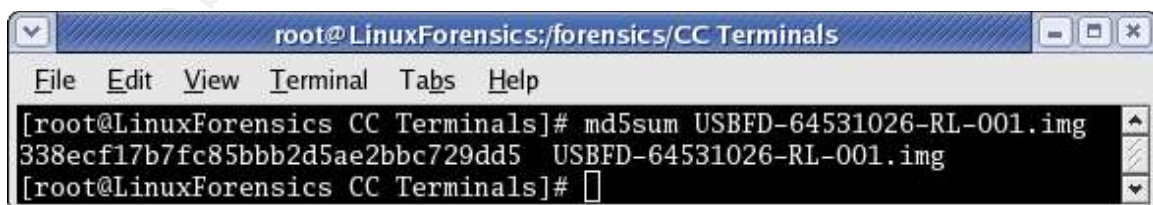
2.3 The Investigation

This section details the step by step process I used to examine the digital image
of the USB Flashdrive.

2.3.1 Chain of Custody and Validation of the USB Flashdrive image

I received the digital image from Mark Mawer with the following chain of custody
information:

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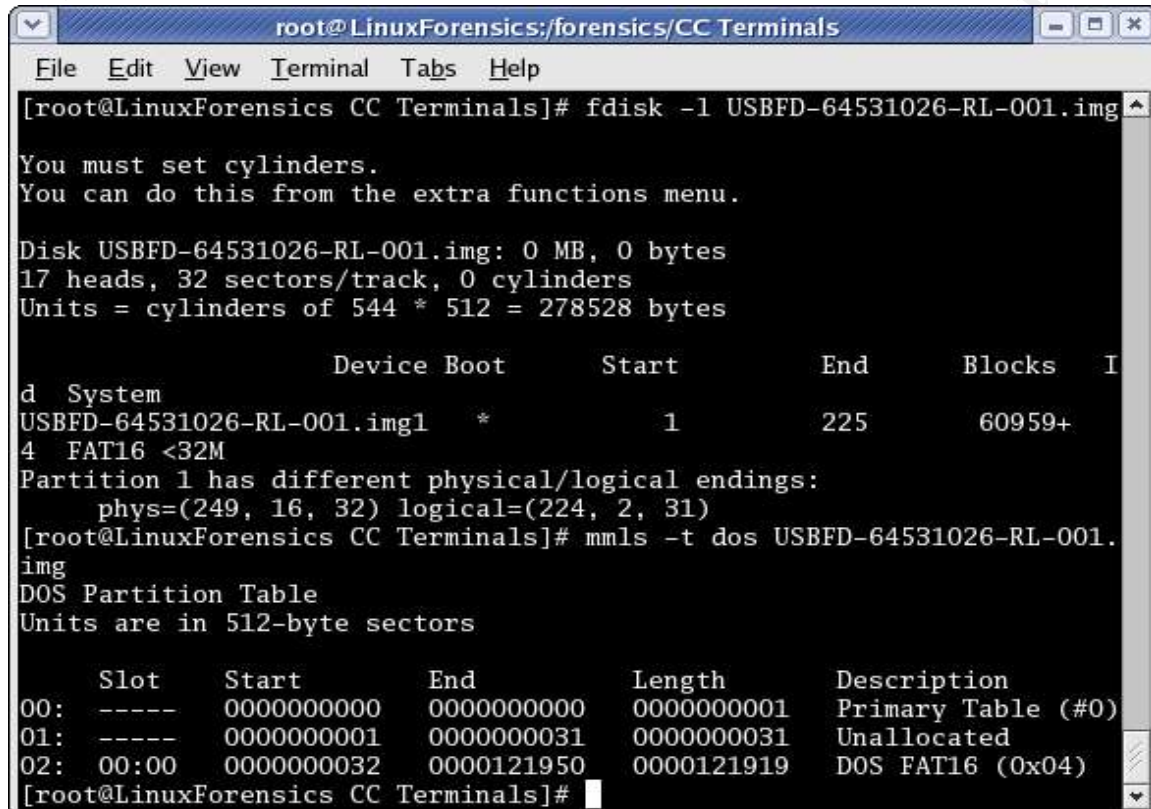MD5: 338ecf17b7fc85bbb2d5ae2bbc729dd5

After copying the digital image to my forensic computer, I ran md5sum to verify
the integrity of the image. The md5 hashes match as shown below:


```
root@LinuxForensics:/forensics/CC Terminals
File   Edit   View   Terminal   Tabs   Help
[root@LinuxForensics CC Terminals]# md5sum USBFD-64531026-RL-001.img
338ecf17b7fc85bbb2d5ae2bbc729dd5  USBFD-64531026-RL-001.img
[root@LinuxForensics CC Terminals]# []
```

8

2.3.2 Separation of the USB Flashdrive image into partition images

The first step in evaluating the image is to determine the number and type of partitions the image contains by running the `fdisk` and `mmls` commands on the image.

```
root@LinuxForensics:/forensics/CC Terminals

File  Edit  View  Terminal  Tabs  Help

[root@LinuxForensics CC Terminals]# fdisk -l USBFD-64531026-RL-001.img

You must set cylinders.
You can do this from the extra functions menu.

Disk USBFD-64531026-RL-001.img: 0 MB, 0 bytes
17 heads, 32 sectors/track, 0 cylinders
Units = cylinders of 544 * 512 = 278528 bytes

                     Device Boot      Start          End      Blocks    I
d  System
USBFD-64531026-RL-001.img1    *           1          225       60959+
4   FAT16 <32M
Partition 1 has different physical/logical endings:
     phys=(249, 16, 32) logical=(224, 2, 31)
[root@LinuxForensics CC Terminals]# 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 CC Terminals]#
```
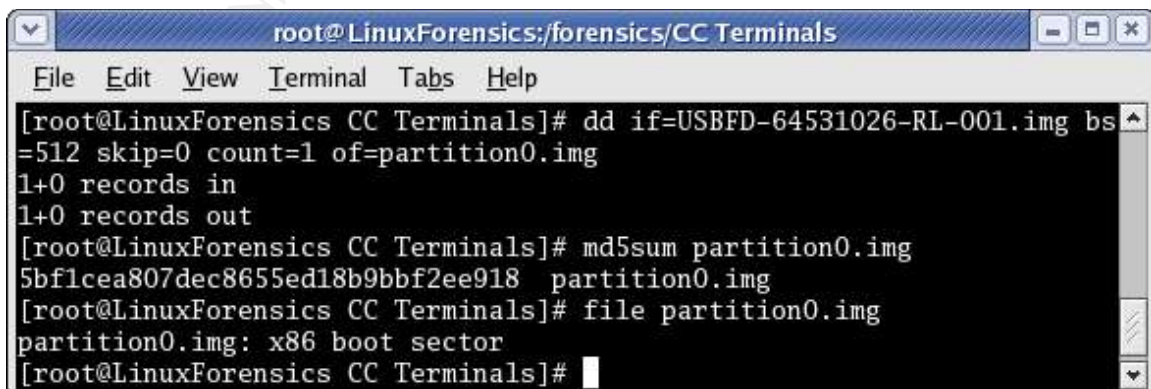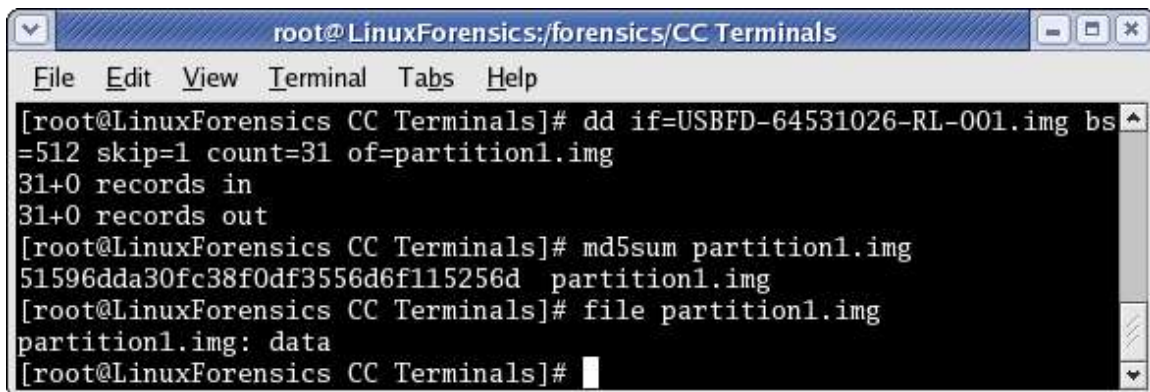
Each of the partitions must be separated out for analysis – this is accomplished using the `dd` command as shown below. Then the `md5sum` and `file` commands are run on the newly created partition image files.

```
root@LinuxForensics:/forensics/CC Terminals

File  Edit  View  Terminal  Tabs  Help

[root@LinuxForensics CC Terminals]# dd if=USBFD-64531026-RL-001.img bs
=512 skip=0 count=1 of=partition0.img
1+0 records in
1+0 records out
[root@LinuxForensics CC Terminals]# md5sum partition0.img
5bf1cea807dec8655ed18b9bbf2ee918  partition0.img
[root@LinuxForensics CC Terminals]# file partition0.img
partition0.img: x86 boot sector
[root@LinuxForensics CC Terminals]#
```
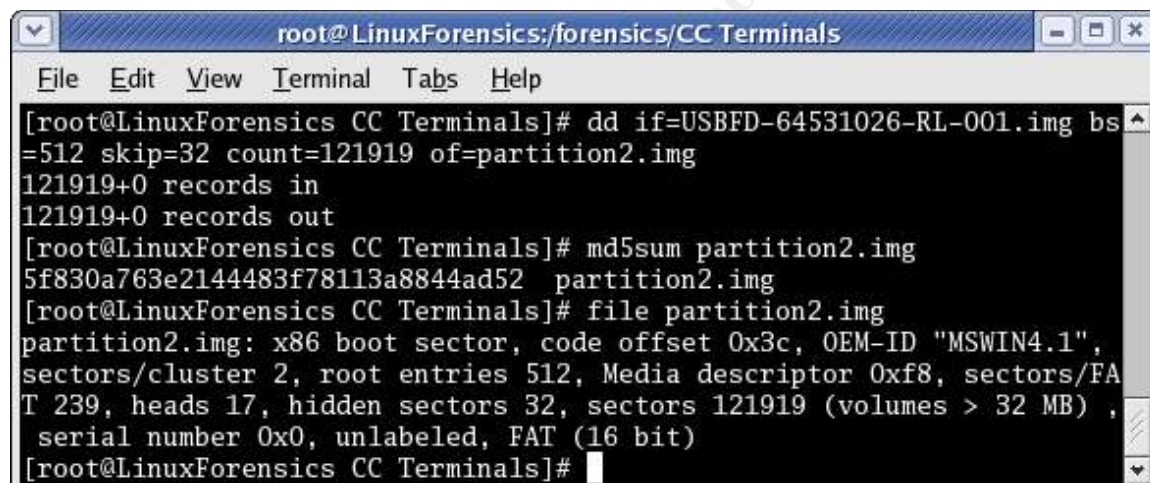
9

```
root@LinuxForensics:/forensics/CC Terminals
File  Edit  View  Terminal  Tabs  Help
[root@LinuxForensics CC Terminals]# dd if=USBFD-64531026-RL-001.img bs
=512 skip=1 count=31 of=partition1.img
31+0 records in
31+0 records out
[root@LinuxForensics CC Terminals]# md5sum partition1.img
51596dda30fc38f0df3556d6f115256d  partition1.img
[root@LinuxForensics CC Terminals]# file partition1.img
partition1.img: data
[root@LinuxForensics CC Terminals]#
```



```
root@LinuxForensics:/forensics/CC Terminals
File  Edit  View  Terminal  Tabs  Help
[root@LinuxForensics CC Terminals]# dd if=USBFD-64531026-RL-001.img bs
=512 skip=32 count=121919 of=partition2.img
121919+0 records in
121919+0 records out
[root@LinuxForensics CC Terminals]# md5sum partition2.img
5f830a763e2144483f78113a8844ad52  partition2.img
[root@LinuxForensics CC Terminals]# file partition2.img
partition2.img: x86 boot sector, code offset 0x3c, OEM-ID "MSWIN4.1",
sectors/cluster 2, root entries 512, Media descriptor 0xf8, sectors/FA
T 239, heads 17, hidden sectors 32, sectors 121919 (volumes > 32 MB) ,
 serial number 0x0, unlabeled, FAT (16 bit)
[root@LinuxForensics CC Terminals]#
```

Next the partition image files are loaded into the Autopsy Forensic Browser for analysis. After opening a new case called CCTerminals, I used the Add Host button to add a host named USBFD-64531026-RL-001. Next, I used the Add Image button to add each partition image file into the case. The partition 0 and 1 image files were entered with a File System Type of raw. The partition 2 image file was entered with a File System Type of FAT16, which was determined by the mmls command the was run on the original USB Flashdrive image and the file command which was run on the partition 2 image file. The Mount Point selected for the partition 2 image file was E:\. Since FAT16 is a Windows File System Type, all subsequent investigation will be evaluated from that perspective.

2.3.3 Timeline Creation and Analysis

In a forensic investigation, it is vital to know when files were created, accessed and deleted. That information is called a timeline or MACtimes. As discussed by Dan Farmer and Wietse Venema in their book, Forensic Discovery [14], MACtimes refers to three time attributes associated with any file or directory in commonly used file systems. The three attributes are shown below:

> atime – last time file was accessed
> mtime – last time file contents were modified
> ctime – last time file contents or meta data were modified (18)

Since there is no file structure to capture timeline information on partitions 0 and 1 (file system type is raw), only partition 2 is used for this step in the forensic investigation methodology. I created the timeline in the Autopsy Forensic Browser by clicking on the File Activity Time Lines button and then on the Create Data File button. I selected the partition 2 image file and clicked OK to create the data file. Then I clicked on the Create Timeline button and clicked OK accepting the default starting and ending dates of None so that all of the timeline data in partition 2 would be included in the output. The timeline can then be viewed by clicking on the View Timeline button, selecting the correct timeline file and then clicking OK. The complete timeline of file activity on partition 2 is shown below:

Mon Oct 25 2004 00:00:00	19968 .a. -/-rwxrwxrwx 0	0	3	E:\/her.doc
Mon Oct 25 2004 08:32:06	19968 ..c -/-rwxrwxrwx 0	0	3	E:\/her.doc
Mon Oct 25 2004 08:32:08	19968 m.. -/-rwxrwxrwx 0	0	3	E:\/her.doc
Tue Oct 26 2004 00:00:00	19968 .a. -/-rwxrwxrwx 0	0	4	E:\/hey.doc
Tue Oct 26 2004 08:48:06	19968 ..c -/-rwxrwxrwx 0	0	4	E:\/hey.doc
Tue Oct 26 2004 08:48:10	19968 m.. -/-rwxrwxrwx 0	0	4	E:\/hey.doc
Wed Oct 27 2004 00:00:00	450560 .a. -/-rwxrwxrwx 0	0	12	E:\/WinDump.exe (_INDUMP.EXE) (deleted)
	0 .a. -rwxrwxrwx 0	0	12	<partition2.img-_INDUMP.EXE-dead-12>
	485810 .a. -/-rwxrwxrwx 0	0	7	E:\/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE)(deleted)
	0 .a. -rwxrwxrwx 0	0	7	<partition2.img-_INPCA~1.EXE-dead-7>
Wed Oct 27 2004 16:23:50	485810 m.. -rwxrwxrwx 0	0	10	<partition2.img-_INPCA~1.EXE-dead-10>
	485810 m.. -/-rwxrwxrwx 0	0	10	E:\/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE)(deleted)
Wed Oct 27 2004 16:23:54	0 ..c -rwxrwxrwx 0	0	7	<partition2.img-_INPCA~1.EXE-dead-7>
	485810 ..c -/-rwxrwxrwx 0	0	7	E:\/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE)(deleted)
	485810 ..c -/-rwxrwxrwx 0	0	10	E:\/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE)(deleted)
	485810 ..c -rwxrwxrwx 0	0	10	<partition2.img-_INPCA~1.EXE-dead-10>
Wed Oct 27 2004 16:23:56	485810 m.. -/-rwxrwxrwx 0	0	7	E:\/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE)(deleted)
	0 m.. -rwxrwxrwx 0	0	7	<partition2.img-_INPCA~1.EXE-dead-7>
Wed Oct 27 2004 16:24:02	450560 m.. -rwxrwxrwx 0	0	14	<partition2.img-_INDUMP.EXE-dead-14>
	450560 m.. -/-rwxrwxrwx 0	0	14	E:\/WinDump.exe (_INDUMP.EXE) (deleted)
Wed Oct 27 2004 16:24:04	450560 ..c -/-rwxrwxrwx 0	0	14	E:\/WinDump.exe (_INDUMP.EXE) (deleted)
	0 ..c -rwxrwxrwx 0	0	12	<partition2.img-_INDUMP.EXE-dead-12>
	450560 ..c -rwxrwxrwx 0	0	14	<partition2.img-_INDUMP.EXE-dead-14>
	450560 ..c -/-rwxrwxrwx 0	0	12	E:\/WinDump.exe (_INDUMP.EXE) (deleted)
Wed Oct 27 2004 16:24:06	0 m.. -rwxrwxrwx 0	0	12	<partition2.img-_INDUMP.EXE-dead-12>
	450560 m.. -/-rwxrwxrwx 0	0	12	E:\/WinDump.exe (_INDUMP.EXE) (deleted)
Thu Oct 28 2004 00:00:00	8814 .a. -rwxrwxrwx 0	0	17	<partition2.img-_ap.gif-dead-17>
	450560 .a. -rwxrwxrwx 0	0	14	<partition2.img-_INDUMP.EXE-dead-14>
	8814 .a. -/-rwxrwxrwx 0	0	17	E:\/_ap.gif (deleted)
	0 .a. -rwxrwxrwx 0	0	16	<partition2.img-_ap.gif-dead-16>
	485810 .a. -rwxrwxrwx 0	0	10	<partition2.img-_INPCA~1.EXE-dead-10>
	8814 .a. -/-rwxrwxrwx 0	0	16	E:\/_ap.gif (deleted)
	485810 .a. -/-rwxrwxrwx 0	0	10	E:\/WinPcap_3_1_beta_3.exe (_INPCA~1.EXE)(deleted)
	53056 .a. -rwxrwxrwx 0	0	15	<partition2.img-_apture-dead-15>
	450560 .a. -/-rwxrwxrwx 0	0	14	E:\/WinDump.exe (_INDUMP.EXE) (deleted)
	53056 .a. -/-rwxrwxrwx 0	0	15	E:\/_apture (deleted)
	19968 .a. -/-rwxrwxrwx 0	0	18	E:\/coffee.doc
Thu Oct 28 2004 11:08:24	53056 ..c -rwxrwxrwx 0	0	15	<partition2.img-_apture-dead-15>
	53056 ..c -/-rwxrwxrwx 0	0	15	E:\/_apture (deleted)
Thu Oct 28 2004 11:11:00	53056 m.. -/-rwxrwxrwx 0	0	15	E:\/_apture (deleted)
	53056 m.. -rwxrwxrwx 0	0	15	<partition2.img-_apture-dead-15>
Thu Oct 28 2004 11:17:44	8814 ..c -/-rwxrwxrwx 0	0	17	E:\/_ap.gif (deleted)
	8814 ..c -/-rwxrwxrwx 0	0	16	E:\/_ap.gif (deleted)
	8814 ..c -rwxrwxrwx 0	0	17	<partition2.img-_ap.gif-dead-17>
	0 ..c -rwxrwxrwx 0	0	16	<partition2.img-_ap.gif-dead-16>
Thu Oct 28 2004 11:17:46	8814 m.. -/-rwxrwxrwx 0	0	16	E:\/_ap.gif (deleted)
	0 m.. -rwxrwxrwx 0	0	16	<partition2.img-_ap.gif-dead-16>
	8814 m.. -rwxrwxrwx 0	0	17	<partition2.img-_ap.gif-dead-17>
	8814 m.. -/-rwxrwxrwx 0	0	17	E:\/_ap.gif (deleted)
Thu Oct 28 2004 19:24:46	19968 ..c -/-rwxrwxrwx 0	0	18	E:\/coffee.doc
Thu Oct 28 2004 19:24:48	19968 m.. -/-rwxrwxrwx 0	0	18	E:\/coffee.doc

While it is possible for MACtime information to be modified by a person wishing
to cover their tracks [14] (21), that does not appear to be the case here since the
dates of activity in the timeline match the dates of activity reported by Ms.
Conlay. The first date for which we see file activity is October 25, 2004 and the
last date is October 28, 2004. This timeline is consistent with time frame Ms.
Conlay reported she was harassed. Analysis of the timeline shows activity on

seven files, four of which were deleted. The first two entries in the timeline are very straightforward. The file, her.doc, was created at 08:32:06 on October 25, 2004. The file contents were last modified at 08:32:08 on October 25, 2004 and the file has not been deleted. The file, hey.doc, was created at 08:48:06 on October 26, 2004. The file contents were last modified at 08:48:10 on October 26, 2004 and the file has not been deleted. The programs WinPcap_3_1_beta_3.exe and WinDump.exe were created and deleted on October 27, 2004 and the files capture and map.gif were created and deleted on October 28, 2004. The final entry, for the file coffee.doc, was created at 19:24:46 on October 28, 2004. The file contents were last modified at 19:24:48 on October 28, 2004 and the file has not been deleted.

2.3.4 OS-Specific Media Analysis

This step would normally involve the examination of operating system specific files and processes [15] (33). However, while the `mmls` and `file` commands show that partitions 0 and 2 are x86 boot sectors and partition 2 contains operating system files, this investigation is focused on finding evidence of harassment not hacking so no further action was taken on this step.

2.3.5 Data Recovery

When a file is deleted in the FAT file system, the data is not actually removed but the sectors where the data is stored are marked unallocated so that they can be reused as needed by the operating system [16] (118). As long as the sectors have not been reused, it is possible to recover a file which has been deleted intact. Data recovery is very straightforward using the Autopsy Forensic Browser. Of the seven files identified on the partition 2 image, four of them have been deleted. Three of them - _ap.gif (map.gif), _apture (capture), and _INDUMP.EXE (WinDump.exe) - are intact and easily recovered using the File Analysis button, then selecting the file which you would like to recover. It is important to select a file that is not 0 bytes in size. The file will then appear in the File Browsing Mode window in the lower part of the screen. Near the top of the File Browsing Mode window there is a link named Export. Clicking on the Export link will give you the option to save the file in a specific directory. I saved all three recovered files to the /forensics/CCTerminals1 directory on my forensic computer for further analysis. The md5 hashes of all of the recovered files are contained in the Image Details Section starting with Subsection 3.3.2. While it is not possible to recover the file _INPCA~1.EXE (WinPcap_3_1_beta_3.exe) intact, it is possible to positively identify it. Complete details on the identification of this file are contained in Subsection 5.1.

2.3.6 String Search

A string search or keyword search is a quick way to identify the location of evidence relating to an investigation. In this case, the following keyword searches were run on the partition 2 image:

	# of Results	Usefulness
Leila	1 ASCII	Very useful – located email Ms Conlay sent to Sam Guarillo with time and location of meeting at coffee shop in the capture file, also added hotmail as keyword
Conlay	0	
Robert	6 ASCII 7 Unicode	Very useful – located Robert Lawrence's name multiple times in three Microsoft Word documents – her.doc, hey.doc, and coffee.doc
Lawrence	Same results as for Robert	
coffee	9 ASCII	Useful – located the word coffee in two Microsoft Word documents, hey.doc and coffee.doc, and in the email in the capture file
hotmail	34 ASCII	Very useful – located Ms. Conlay's personal email address, flowergirl96@hotmail.com in the capture file
GUID	8 ASCII	None – no instances of GUID in the Microsoft Word documents

All searches were run in the Autopsy Forensic Browser using the Keyword Search button and selecting the ACSII, Unicode, and Case Insensitive check boxes.

2.3.7 Reporting
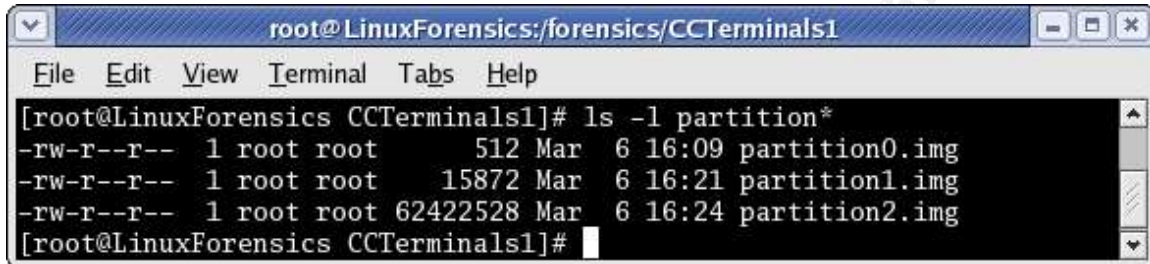
This report constitutes the completion of the final step in the forensic investigation methodology. The results of this investigation support Ms. Conlay's report of harassment by Robert Lawrence. Based on forensic evidence in the documents found on the partition 2 image, the copy of Microsoft Word used to create the documents was licensed to Robert Lawrence. The text of these documents is consistent with the tone and content of the emails Ms. Conlay reported receiving. No PID_GUID information was found in these documents so they cannot be tied to a specific MAC (Media Access Control) address on a specific computer. Based on the evidence of the capture file, a sniffer was set up to record network traffic and the email Ms. Conlay sent to Sam Guardillo

14

arranging the time and location of their meeting at the coffee shop was recorded. Based on the evidence in the _ap.gif (map.gif) file, the person using the USB Flashdrive looked up the location of the coffee shop using the program MapPoint and saved the resulting image. Based on Ms. Conlay's complaint, Robert Lawrence appeared at the coffee shop at the time she was meeting with Sam Guardillo and she subsequently received a email she felt was threatening from him.

15

3.0 Image Details
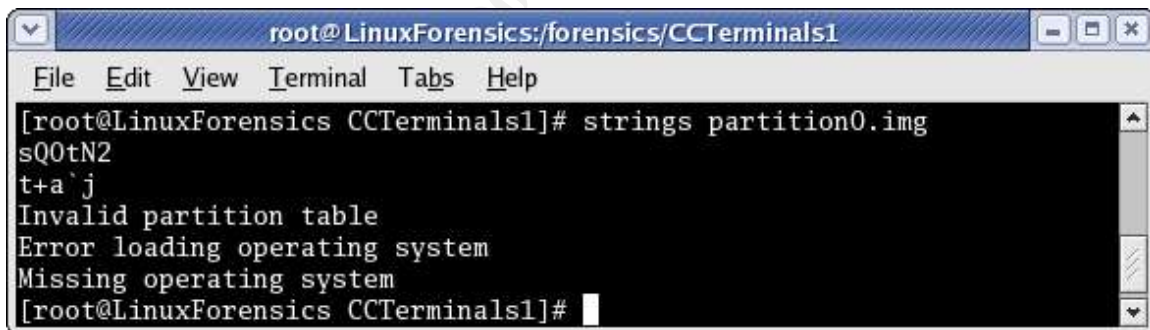
This section of the report will contain more detailed information about each of the three partition image files. The Subsection 3.3 will also contain detailed information about each of the files that were identified on the partition 2 image file.

```
root@LinuxForensics:/forensics/CCTerminals1
File  Edit  View  Terminal  Tabs  Help
[root@LinuxForensics CCTerminals1]# ls -l partition*
-rw-r--r--  1 root root      512 Mar  6 16:09 partition0.img
-rw-r--r--  1 root root    15872 Mar  6 16:21 partition1.img
-rw-r--r--  1 root root 62422528 Mar  6 16:24 partition2.img
[root@LinuxForensics CCTerminals1]#
```

3.1 Partition 0
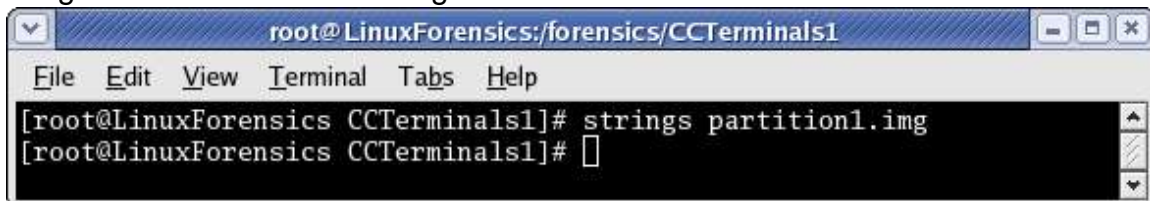
Based on the results of the strings command shown below, the partition 0 image file contains data consistent with its function as a x86 boot sector but it contains no evidence of harassment by Mr. Lawrence.

```
root@LinuxForensics:/forensics/CCTerminals1
File  Edit  View  Terminal  Tabs  Help
[root@LinuxForensics CCTerminals1]# strings partition0.img
sQ0tN2
t+a`j
Invalid partition table
Error loading operating system
Missing operating system
[root@LinuxForensics CCTerminals1]#
```

3.2 Partition 1

Based on the results of the strings command shown below, the partition 1 image file contains no meaningful data.
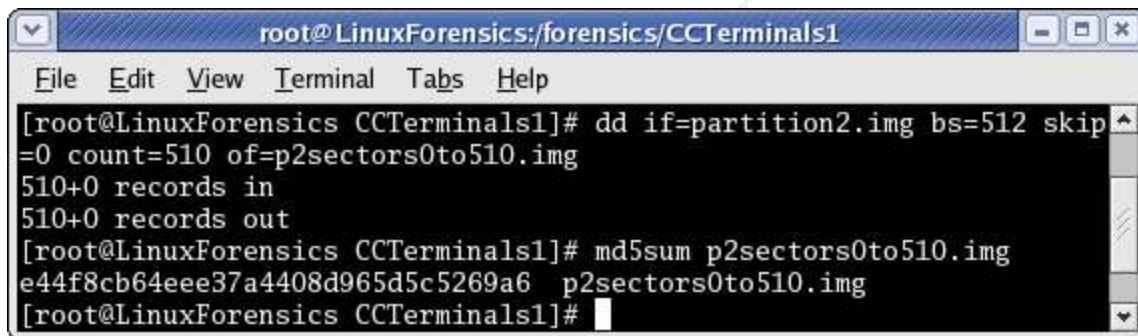
```
root@LinuxForensics:/forensics/CCTerminals1
File  Edit  View  Terminal  Tabs  Help
[root@LinuxForensics CCTerminals1]# strings partition1.img
[root@LinuxForensics CCTerminals1]#
```

16

3.3 Partition 2

The partition 2 image file contains the bulk of the original USB Flashdrive image and as such is the primary focus of this investigation. Sectors are typically the smallest addressable data unit in a FAT file system [17] (406). Within the partition 2 image file, sectors 0 through 630 are allocated (in use) and sectors 631 through 121918 are unallocated (available to be used or reused). Information on all sectors (0 – 121918) in the partition 2 image is shown below.
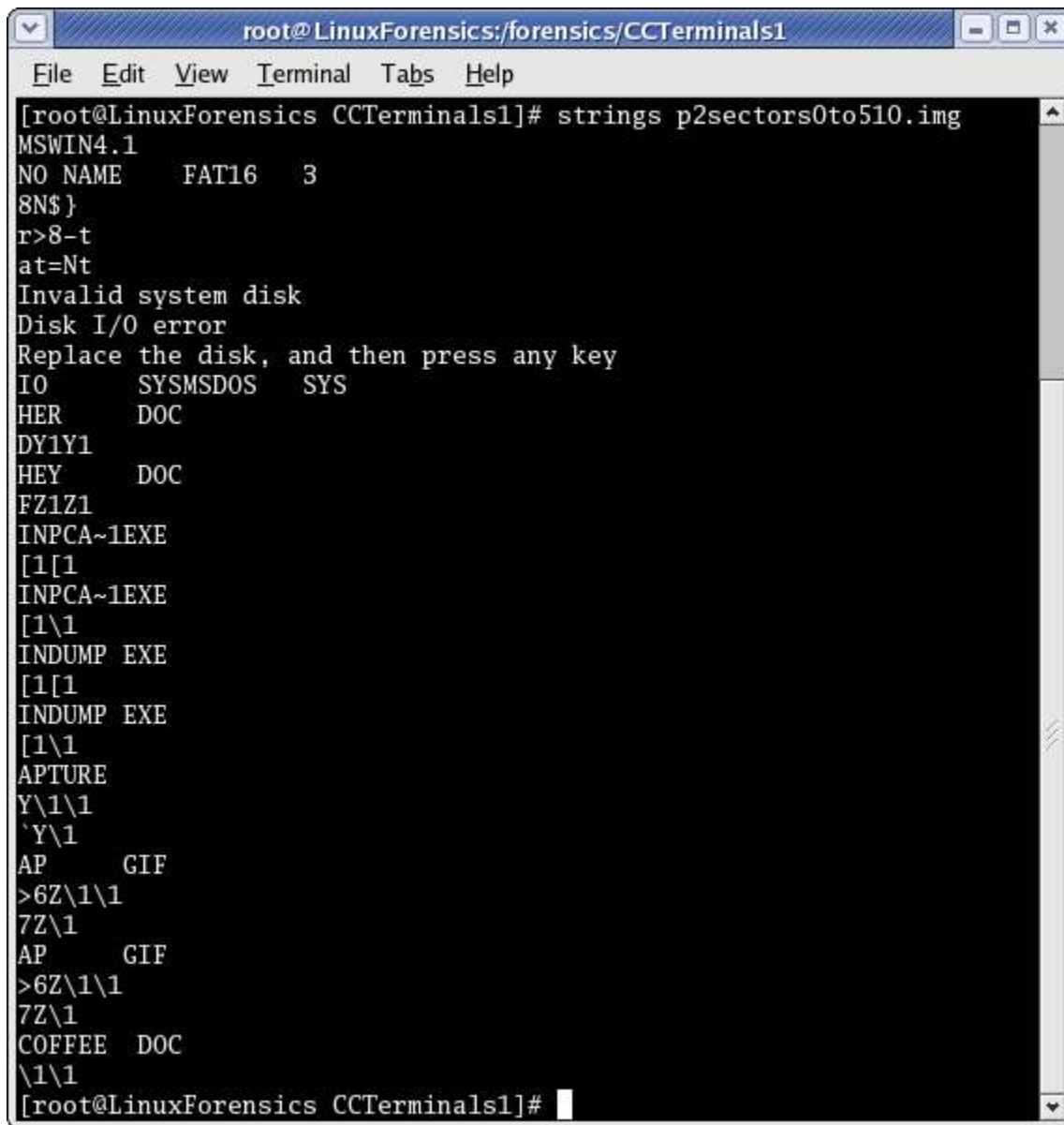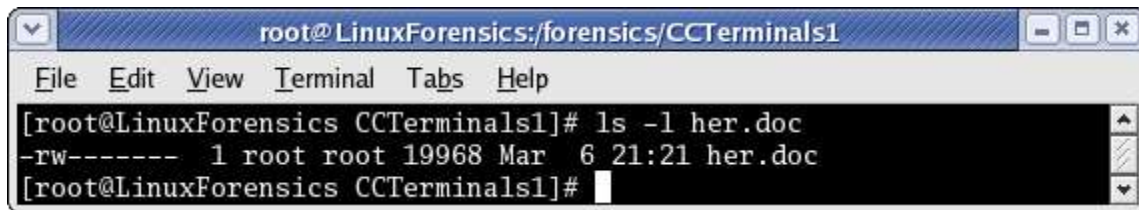
3.3.1 Sectors 0 - 510

I determined that sectors 0 – 510 of the partition 2 image file contained no evidence relating to the reported harassment by using the dd command to create an separate image file containing sectors 0 - 510 from the partition 2 image.

Then I ran the strings command to identify any text in the newly created image file. As shown below, sectors 0 – 510 on the partition 2 image contain operating system files and meta data, but do not contain evidence of harassment by Mr. Lawrence.

17

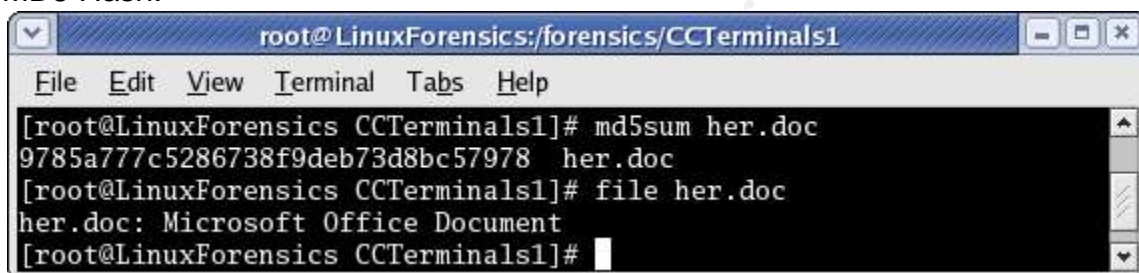```
root@LinuxForensics:/forensics/CCTerminals1

File   Edit   View   Terminal   Tabs   Help

[root@LinuxForensics CCTerminals1]# strings p2sectors0to510.img
MSWIN4.1
NO NAME   FAT16   3
8N$}
r>8-t
at=Nt
Invalid system disk
Disk I/O error
Replace the disk, and then press any key
IO   SYSMSDOS   SYS
HER   DOC
DY1Y1
HEY   DOC
FZ1Z1
INPCA~1EXE
[1[1
INPCA~1EXE
[1\1
INDUMP EXE
[1[1
INDUMP EXE
[1\1
APTURE
Y\1\1
`Y\1
AP   GIF
>6Z\1\1
7Z\1
AP   GIF
>6Z\1\1
7Z\1
COFFEE DOC
\1\1
[root@LinuxForensics CCTerminals1]#
```

### 3.3.2 Sectors 511 - 550 File 1 – her.doc

File Name on Image:      her.doc
Deleted:                 No
MACtime Information:     October 25, 2004 c 08:48:06 m 08:48:10
The above information was determined using Autopsy Forensic Browser
File Owner:              FAT16 does not provide file owner information
File Size (bytes):       19968

18

```
root@LinuxForensics:/forensics/CCTerminals1
File  Edit  View  Terminal  Tabs  Help
[root@LinuxForensics CCTerminals1]# ls -l her.doc
-rw-------   1 root root 19968 Mar  6 21:21 her.doc
[root@LinuxForensics CCTerminals1]#
```

Complete Text: 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
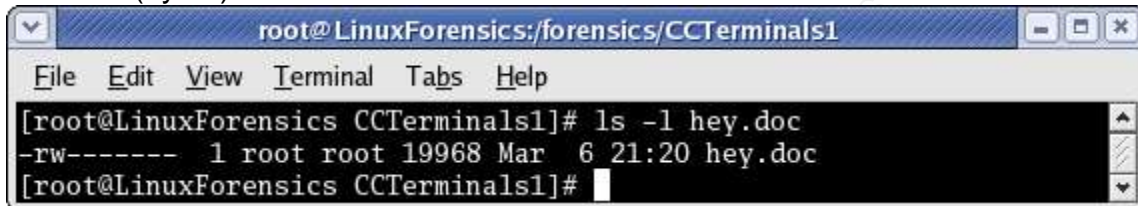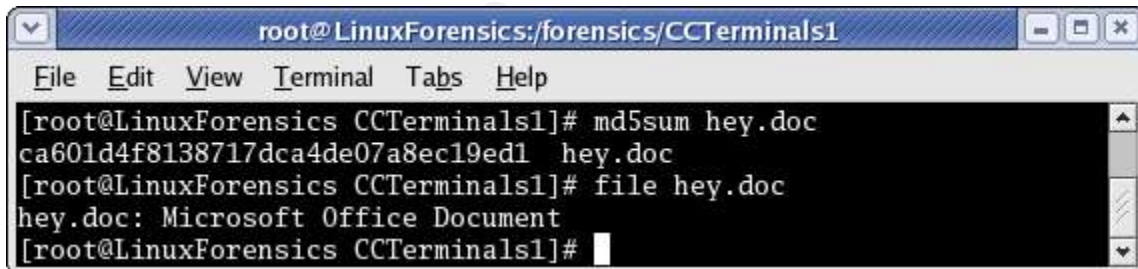can give you a ride to work sometime, or maybe we can get dinner
sometime?

Have a nice day

Keywords: Leila Conlay Robert Lawrence hotmail coffee GUID

MD5 Hash:

```
root@LinuxForensics:/forensics/CCTerminals1
File  Edit  View  Terminal  Tabs  Help
[root@LinuxForensics CCTerminals1]# md5sum her.doc
9785a777c5286738f9deb73d8bc57978  her.doc
[root@LinuxForensics CCTerminals1]# file her.doc
her.doc: Microsoft Office Document
[root@LinuxForensics CCTerminals1]#
```

Comments: The copy of Microsoft Word used to create this
                          document was licensed to Robert Lawrence

```
Properties of Hey I saw you the other day

General | Description | User Defined | Internet | Statistics

                    her.doc

Type:            MS Word document
Location:        /forensics/CCTerminals1/
Size:            20 KB (19,968 Bytes)

Created:         10/25/2004, 09:30:00, Robert Lawrence
Modified:        10/25/2004, 09:32:00, Robert Lawrence
Last printed:
Editing time:    00:02:00
Document number: 1

☑ Apply user data                               Delete

Template:        Normal.dot

                          OK    Cancel    Help    Reset
```

19
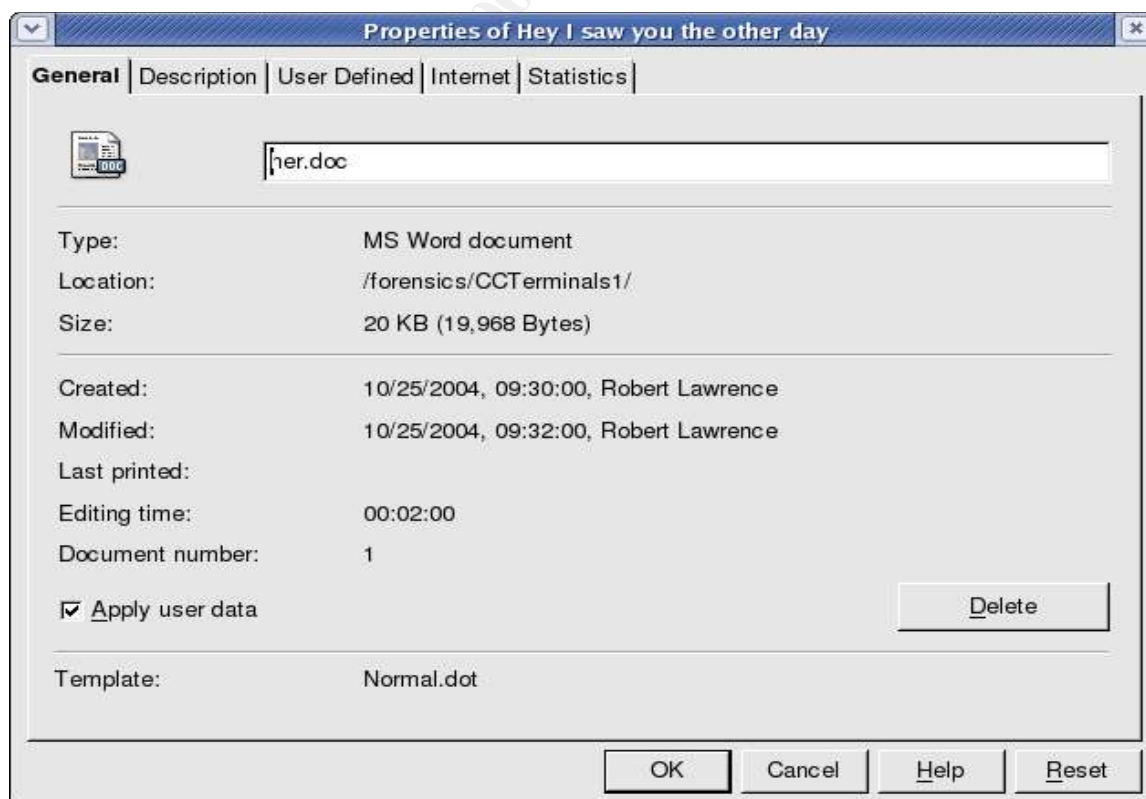
3.3.3 Sectors 551 - 590 File 2 – hey.doc

File Name on Image: hey.doc
Deleted: No
MACtime Information: October 26, 2004 c 08:32:06 m 08:32:08
The above information was determined using Autopsy Forensic Browser
File Owner: FAT16 does not provide file owner information
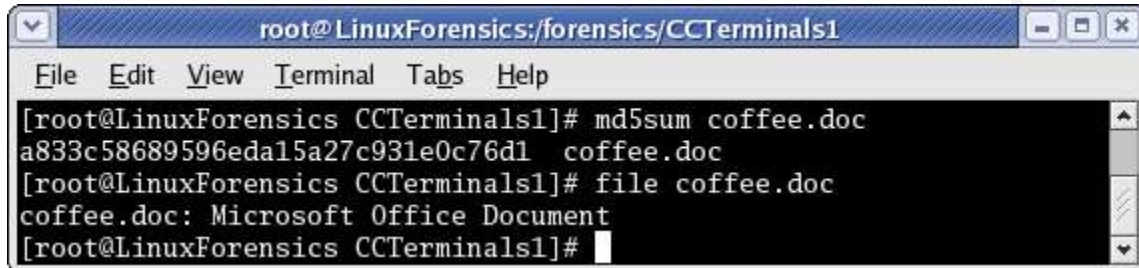File Size (bytes):   19968

Complete Text: 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?
Keywords: Leila Conlay Robert Lawrence hotmail coffee GUID
MD5 Hash:

Comments: The copy of Microsoft Word used to create this
                           document was licensed to Robert Lawrence
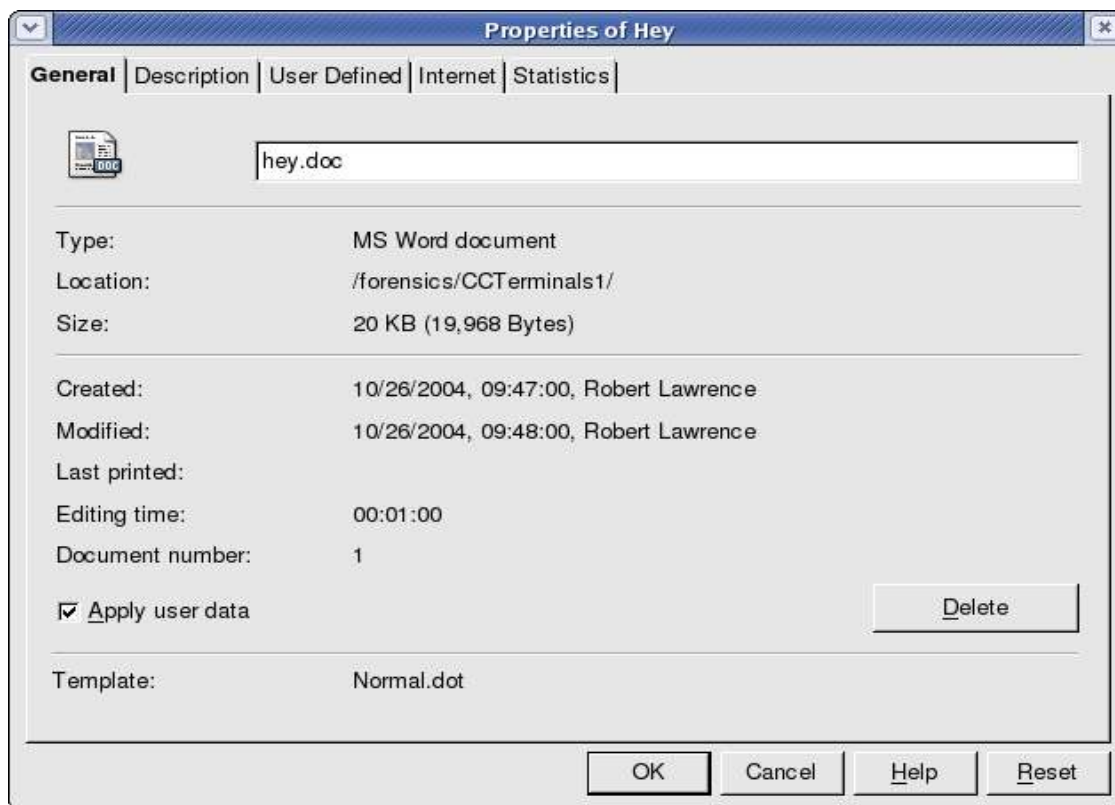
3.3.4 Sectors 591 - 630 File 3 – coffee.doc
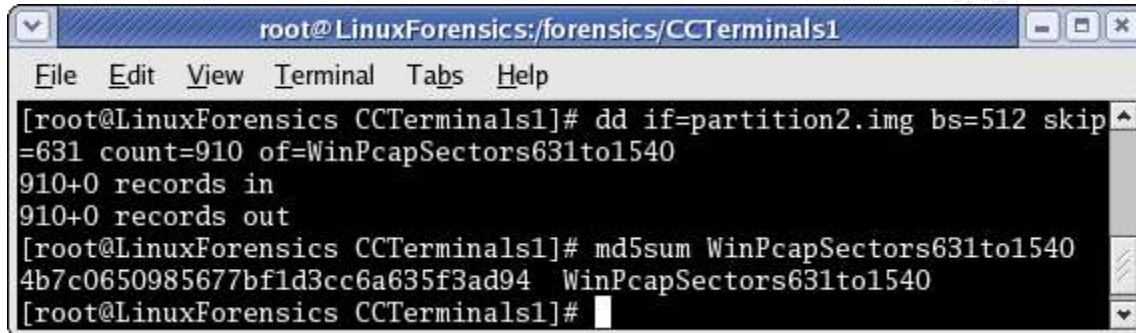
File Name on Image: coffee.doc
Deleted: No
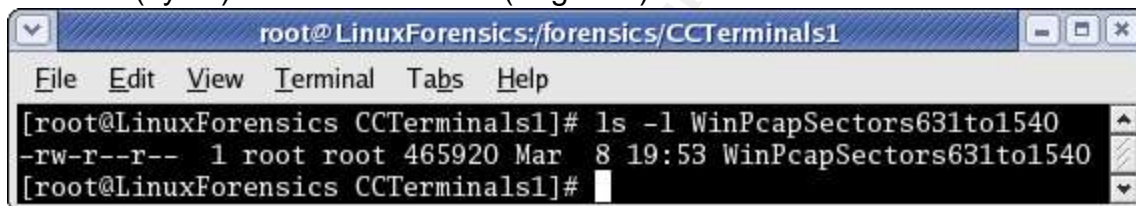MACtime Information: October 28, 2004 c 19:24:46 m 19:24:48
The above information was determined using Autopsy Forensic Browser
File Owner: FAT16 does not provide file owner information
File Size (bytes):   19968
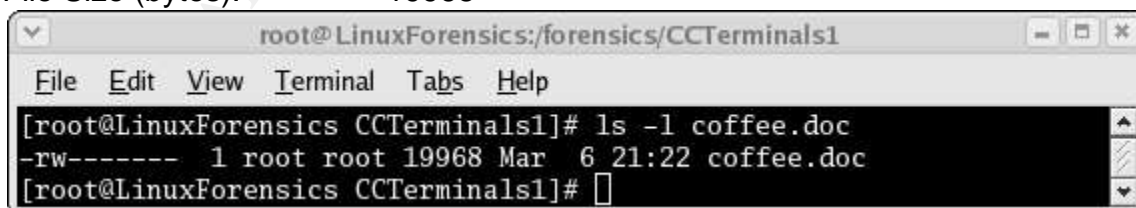
Complete Text: Hey what gives?   I was drinking a coffee on
thursday and saw you stop buy with some guy!   You said you didn't want
coffee with me, but you'll go have it with some random guy???   He
looked like a loser!   Guys like that are nothing but trouble.   I can't
believe you did this to me!   You should stick to your word, if you're

21

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...

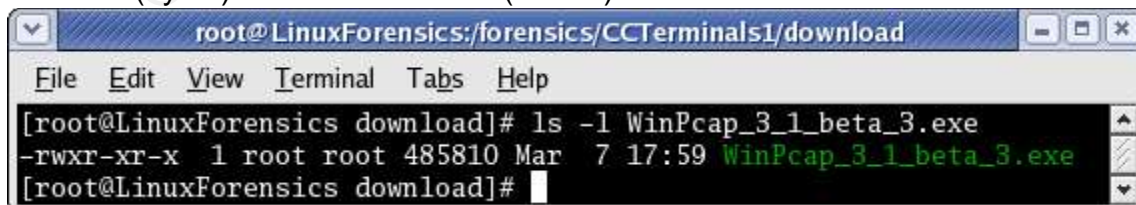Keywords: Leila Conlay Robert Lawrence hotmail coffee GUID

MD5 Hash:

```
root@LinuxForensics:/forensics/CCTerminals1

File  Edit  View  Terminal  Tabs  Help

[root@LinuxForensics CCTerminals1]# md5sum coffee.doc
a833c58689596eda15a27c931e0c76d1  coffee.doc
[root@LinuxForensics CCTerminals1]# file coffee.doc
coffee.doc: Microsoft Office Document
[root@LinuxForensics CCTerminals1]#
```

Comments: The copy of Microsoft Word used to create this
                             document was licensed to Robert Lawrence

```
Properties of Hey what gives

General | Description | User Defined | Internet | Statistics |

         coffee.doc

Type:              MS Word document
Location:          /forensics/CCTerminals1/
Size:              20 KB (19,968 Bytes)

Created:           10/28/2004, 20:23:00, Robert Lawrence
Modified:          10/28/2004, 20:24:00, Robert Lawrence
Last printed:
Editing time:      00:01:00
Document number:   1

☑ Apply user data                              Delete

Template:          Normal.dot

                          OK    Cancel    Help    Reset
```
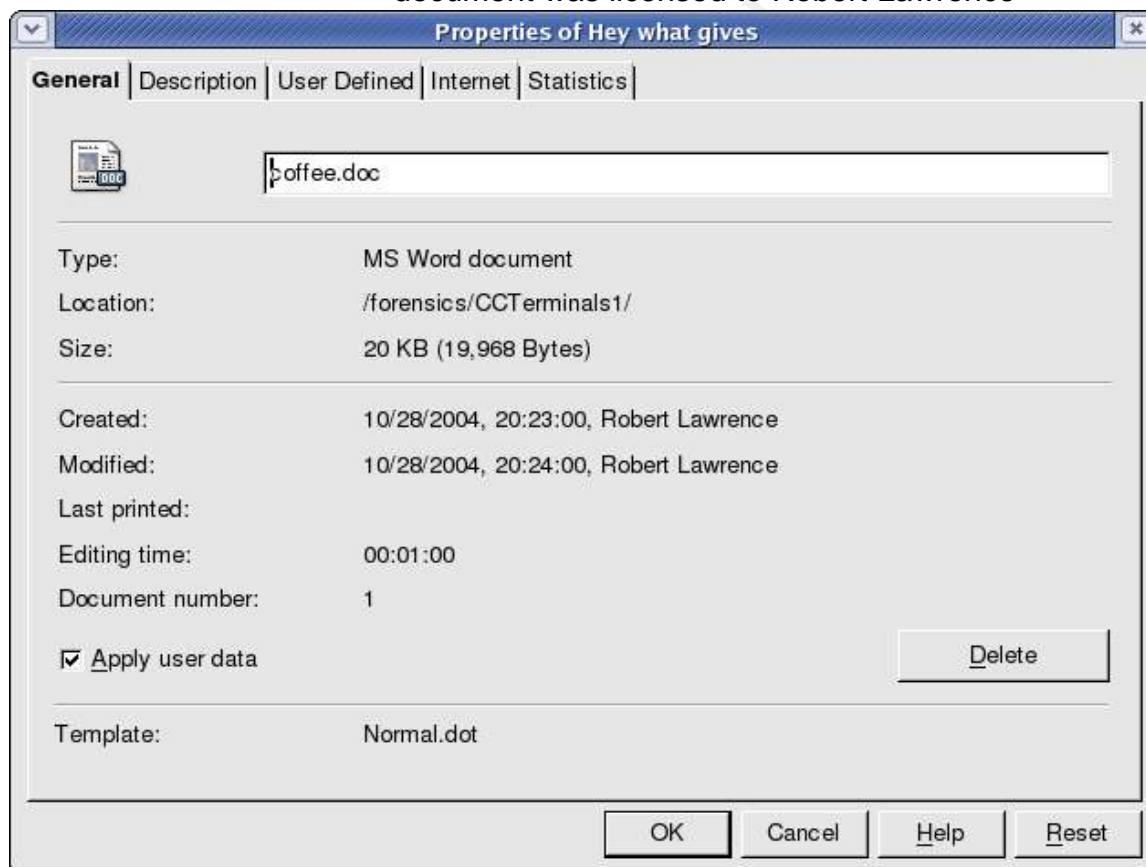
3.3.5 Sectors 631 - 1540 File 4 – WinPcap_3_1_beta_3.exe (fragment)

File Name on Image: _INPCA~1.EXE
Deleted: Yes
MACtime Information: October 27, 2004 c 16:23:54 m 16:23:50

22

The above information was determined using Autopsy Forensic Browser

File Owner: FAT16 does not provide file owner information

Since only part of this file still exists, I used the `dd` command to create an separate image file containing sectors 631 – 1540 from the partition 2 image for further analysis as shown below:.

MD5 Hash:

File Size (bytes):   465920 (fragment)

True File Name: WinPcap_3_1_beta_3.exe

Comments: It is not possible to recover _INPCA~1.EXE since some of the sectors have been reused for the file coffee.doc. The md5 hash above is for the portion of _INPCA~1.EXE that still exists in sectors 631 through 1540. This does not correlate to the md5 hash of the complete WinPcap_3_1_beta_3.exe program downloaded from the Internet and shown below. A complete discussion of the identification of this program can be found in Subsection 5.1.
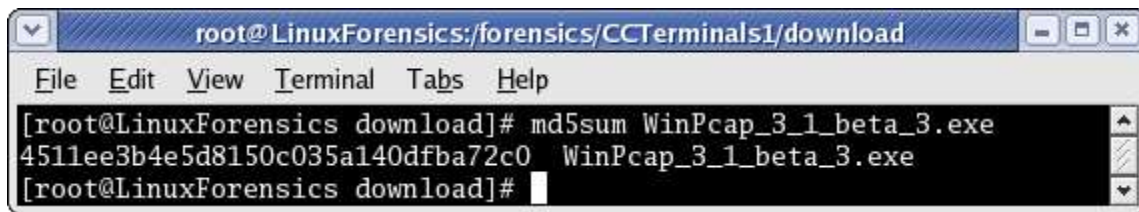
File Size (bytes):   485810 (full file)
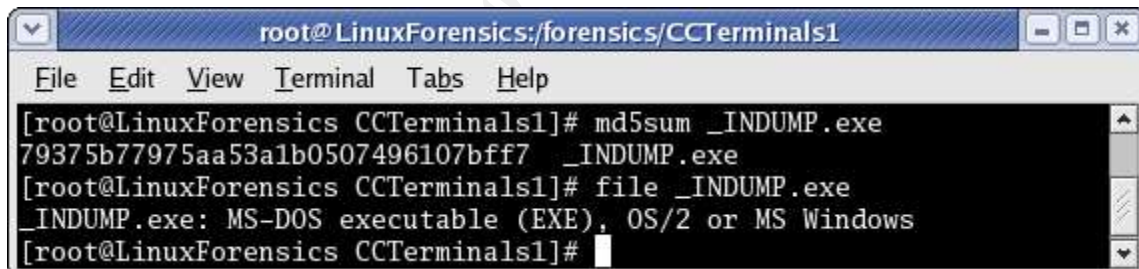

MD5 Hash:
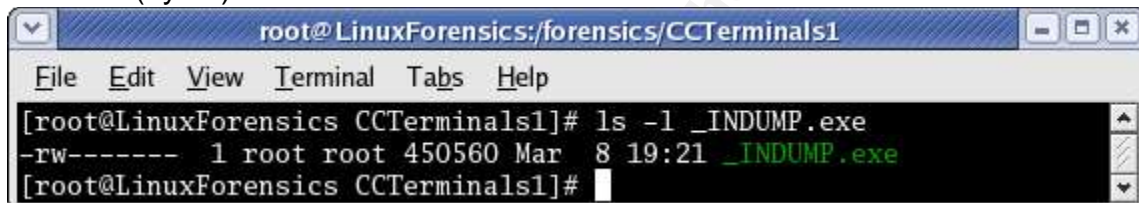
3.3.6 Sectors 1541 - 2420 File 5 – WinDump.exe

File Name on Image: _INDUMP.EXE
Deleted: Yes
MACtime Information: October 27, 2004 c 16:24:04 m 16:24:02
The above information was determined using Autopsy Forensic Browser
File Owner: FAT16 does not provide file owner information
File Size (bytes):   450560

MD5 Hash:
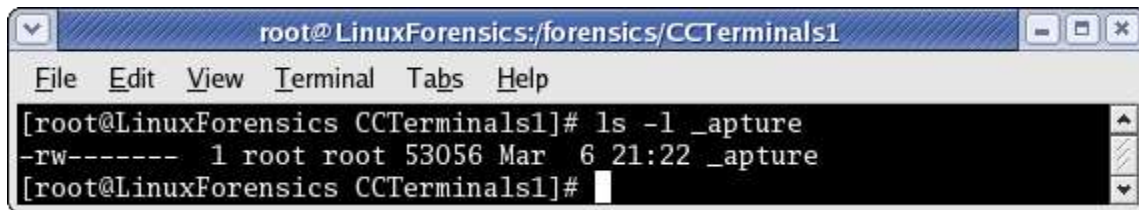
True File Name: WinDump.exe
Comments: A complete discussion of the identification of this
                        program's true name can be found in Subsection
                        5.2.

3.3.7 Sectors 2421 - 2524 File 6 - capture

File Name on Image: _apture
Deleted: Yes
MACtime Information: October 28, 2004 c 11:08:24 m 11:11:00
The above information was determined using Autopsy Forensic Browser
File Owner: FAT16 does not provide file owner information
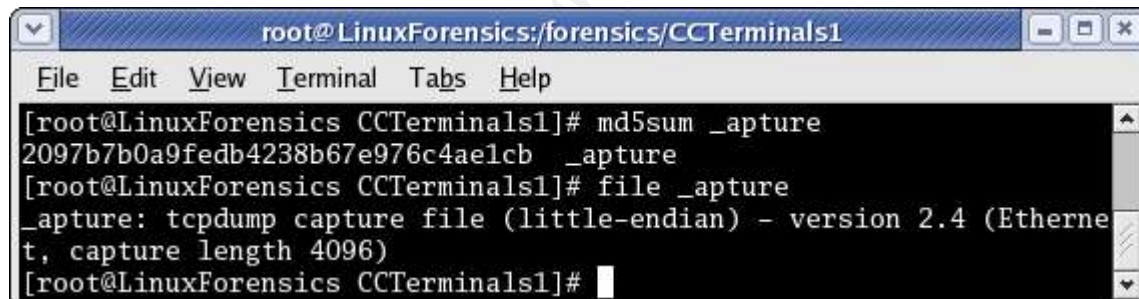File Size (bytes):   53056

24

Partial Text:
curmbox=F000000001&HrsTest=&_HMaction=Send&FinalDest=&subaction=&pl
aintext=&login=flowergirl96&msg=&start=&len=&attfile=&attlistfile=&eurl=&type=
&src=&ref=&ru=&msghdrid=b16479b18beec291196189c78555223c_109869245
2&RTEbgcolor=&encodedto=SamGuarillo@hotmail.com&encodedcc=&encoded
bcc=&deleteUponSend=0&importance=&sigflag=&newmail=new&to=SamGuarill
o@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

MD5 Hash:

True File Name: capture
Comments: True name was determined by the file type

3.3.8 Sectors 2525 - 2542 File 7 – map.gif

File Name on Image: _ap.gif
Deleted: Yes
MACtime Information: October 28, 2004 c 11:17:44 m 11:17:46
The above information was determined using Autopsy Forensic Browser
File Owner: FAT16 does not provide file owner information
File Size (bytes):   8814

MD5 Hash:
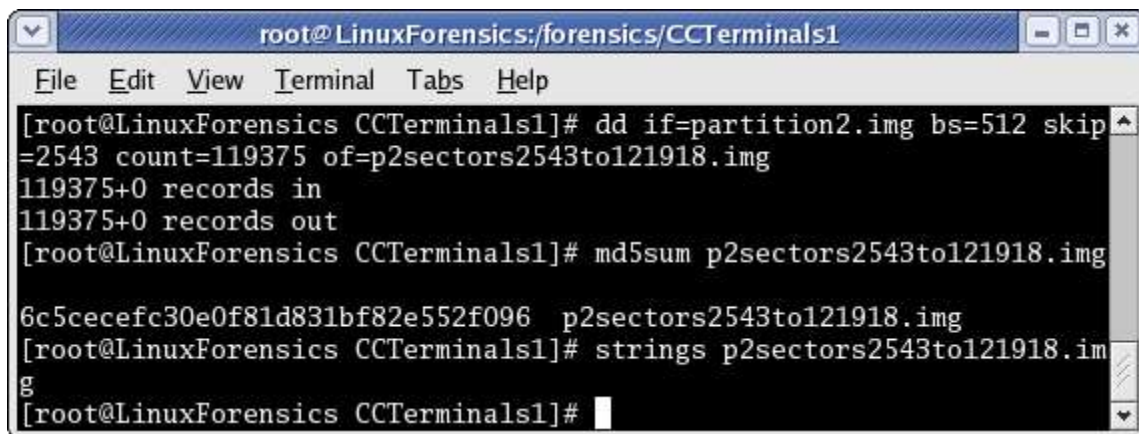
True File Name: map.gif
Comments: True file name was determined by contents of file as
                          shown below

3.3.9 Sectors 2543 - 121918

I determined that remaining sectors of the partition 2 image file contained no
data useful to this investigation by using the dd command to create an separate
image file containing sectors 2543 – 121918 from the partition 2 image file. Then
I ran the strings command to identify any text in the newly created image file.
No data was returned by the strings command as shown below:

26

4.0 Forensics Details

This section will discuss the use of the two programs found on the partition 2 image. A complete discussion of the process used to identify these programs is contained in Section 5.0. There is a connection between these two programs, a version of WinPcap must be installed before WinDump.exe can be used.

4.1 Description of WinPcap_3_1_beta_3.exe

The web site [18] http://winpcap.polito.it/, which distributes the WinPcap program has the following description of it's function and components:

> WinPcap is an open source library for packet capture
> and network analysis for the Win32 platforms. It
> includes a kernel-level packet filter, a low-level
> dynamic link library (packet.dll), and a high-level and
> system-independent library (wpcap.dll, based on
> libpcap version 0.6.2).
> The packet filter is a device driver that adds to
> Windows 95, 98, ME, NT, 2000, XP and 2003 the
> ability to capture and send raw data from a network
> card, with the possibility to filter and store in a buffer
> the captured packets.
> Packet.dll is an API that can be used to directly
> access the functions of the packet driver, offering a
> programming interface independent from the
> Microsoft OS.
> Wpcap.dll exports a set of high level capture
> primitives that are compatible with libpcap, the well
> known Unix capture library. These functions allow to
> capture packets in a way independent from the
> underlying network hardware and operating system.

The person using WinPcap must have Administrator privileges on a Windows NT/2000/XP computer to run the program for the first time as documented in the FAQ section of the web site [18] at http://winpcap.polito.it/misc/faq.htm#Q-7.

> Q-7: Do I need to be Administrator in order to execute
> programs based on WinPcap on Windows
> NT/2000/XP?
> A: Yes/no. The security model of WinPcap is quite
> poor, and we plan to work on it in the future. At the
> moment, if you execute a WinPcap-based application
> for the first time since the last reboot, you must be
> administrator. At the first execution, the driver will be

> dynamically installed in the system, and from that
> moment every user will be able to use WinPcap to
> sniff the packets.

4.2 Description of WinDump.exe

The web site [19] http://windump.polito.it/, which distributes the WinDump
program has the following description of it's function:
"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."

4.3 Installation and Use of Programs

A Windows 2000 Professional VMware session was used to test the installation
and validate the functioning of the two programs. Since the
WinPcap_3_1_beta_3.exe program could not be recovered from the partition 2
image file, I am using the copy of the program that I downloaded from [20]
ftp://gd.tuwien.ac.at/infosys/security/polito.it/winpcap/ for this installation.
Subsection 5.1 contains a complete description of the process used to positively
identify this program. The WinDump.exe program used here is a copy of the
program _INDUNP.EXE that was recovered from the partition 2 image file,
renamed to WinDump.exe for clarity during this process. Subsection 5.2
contains a complete description of the process used to positively identify this
program.
Since WinPcap must be installed before WinDump can be used, I double clicked
on the WinPcap_3_1_beta_3.exe file to start the installation. A graphical
installation program started and I clicked the Next button on two screens to start
the installation. After the files were finished copying, a readme file appeared and
then a final screen stating that the installation was complete. WinDump.exe is
self-contained executable and does not need to be installed. WinDump.exe can
be run by double clicking on the file name but many more options can be used if
it is run from the command line. At this point I have successfully installed
WinPcap and successfully executed WinDump, verifying that the use of these
two programs allows network traffic to be sniffed from the computer these
programs are used on.

4.4 Analysis of Capture File

The capture file recovered from the partition 2 image file contains network traffic
from multiple IP addresses, indicating that the network card of the computer
using WinDump was in promiscuous mode. This means that all network traffic on

29

that subnet was being recorded not just traffic to and from the computer running WinDump and other computers on the network. While there might be reason for an end user to observe network traffic to and from their computer for troubleshooting purposes, there is no valid reason for an end user to be observing and recording all network traffic on their subnet. There are also serious legal implications of this behavior which are discussed more fully in Section 6.0.

The network traffic that was recorded in the capture file contains evidence relating to Ms. Conlay's assertion that Robert Lawrence appeared at the coffee shop where she was meeting a friend on October 28, 2004. Starting with the fourth entry in the file and using the Follow TCP Stream option in Ethereal, it is possible to view the traffic between the computer Ms. Conlay was using (192.168.2.104) and the Hotmail server (64.4.34.250) she was using to send an email to her friend with the time and location of their meeting at the coffee shop. The details of that email are shown below:

curmbox=F000000001&HrsTest=&_HMaction=Send&FinalDest=&subaction=&plaintext=&login=flowergirl96&msg=&start=&len=&attfile=&attlistfile=&eurl=&type=&src=&ref=&ru=&msghdrid=b16479b18beec291196189c78555223c_1098692452&RTEbgcolor=&encodedto=SamGuarillo@hotmail.com&encodedcc=&encodedbcc=&deleteUponSend=0&importance=&sigflag=&newmail=new&to=SamGuarillo@hotmail.com&cc=&bcc=&subject=RE%3A+coffee&body=Sure%2C+coffee+sounds+great.++Let%27s+meet+at+the+coffee+shop+on+the+corner+Hollywood+and+McCadden.++It%27s+a+nice+out+of+the+way+spot.%0D%0A%0D%0ASee+you+at+7pm%21%0D%0A%0D%0A-LeilaHTTP/1.1 100 Continue

Based on evidence in the files recovered from the partition 2 image file including the email with the time and location of Ms. Conlay's meeting at the coffee shop in the capture file, and the the map.gif file containing a map that appears to be that of the coffee shop at Hollywood and McCadden it is apparent that tracking Ms. Conlay's whereabouts and companions were the focus of these activities. This evidence is consistent with Ms. Conlay's complaint of harassment by Robert Lawrence.

5.0 Program Identification

This section will detail the process followed to positively identify the two programs recovered from the partition 2 image file.

5.1 WinPcap_3_1_beta_3.exe

Identifying the deleted program - _INPCA~1.EXE (WinPcap_3_1_beta_3.exe) – presents a challenge since the file coffee.doc was created after _INPCA~1.EXE (WinPcap_3_1_beta_3.exe) was deleted and some of the sectors were reused for coffee.doc when it was saved. While it is not possible to recover _INPCA~1.EXE (WinPcap_3_1_beta_3.exe) intact, it is possible to positively identify it. First I downloaded WinPcap_3_1_beta_3.exe from the Internet - since beta 4 has been released, it is a little difficult to find beta 3 but I located it at [20] ftp://gd.tuwien.ac.at/infosys/security/polito.it/winpcap/. Then I checked the size of the downloaded program and compared that to the size information for _INPCA~1.EXE (WinPcap_3_1_beta_3.exe) in the Autopsy Forensic Browser. The size for both is 485810 as shown below:

31

Next I opened the downloaded program in a hex editor. Since coffee.doc is located in sectors 591-630, I began looking for _INPCA~1.EXE (WinPcap_3_1_beta_3.exe) in sector 631. In Autopsy Forensic Browser, I clicked on the data unit button then enter 631 in the Sector Number box and then clicked the View button. Next I clicked on the link for hex display and copied the first piece of data in line 0 – 1b8cc746. In the hex editor, I searched the downloaded copy of WinPcap_3_1_beta_3.exe for 1b8cc746. I arranged the windows so that both are visible on the screen at the same time and scrolled through both programs, visually matching the data in both windows to positively identify WinPcap_3_1_beta_3.exe.
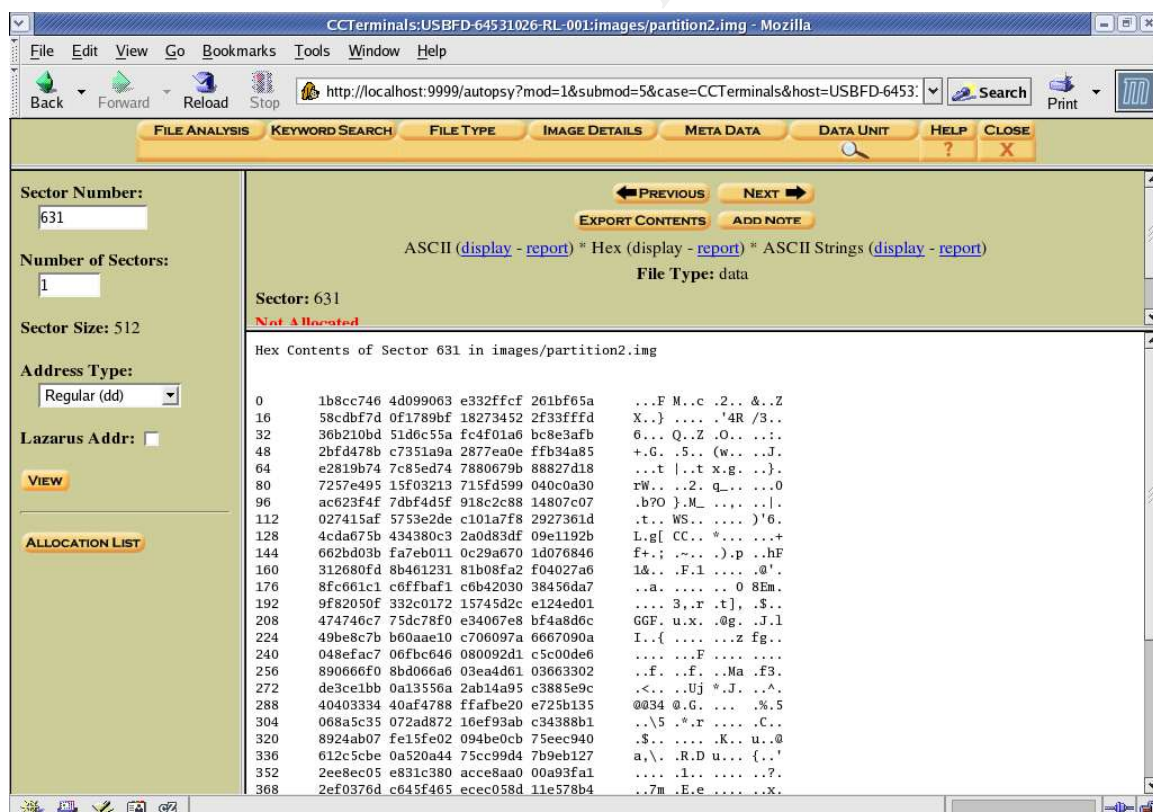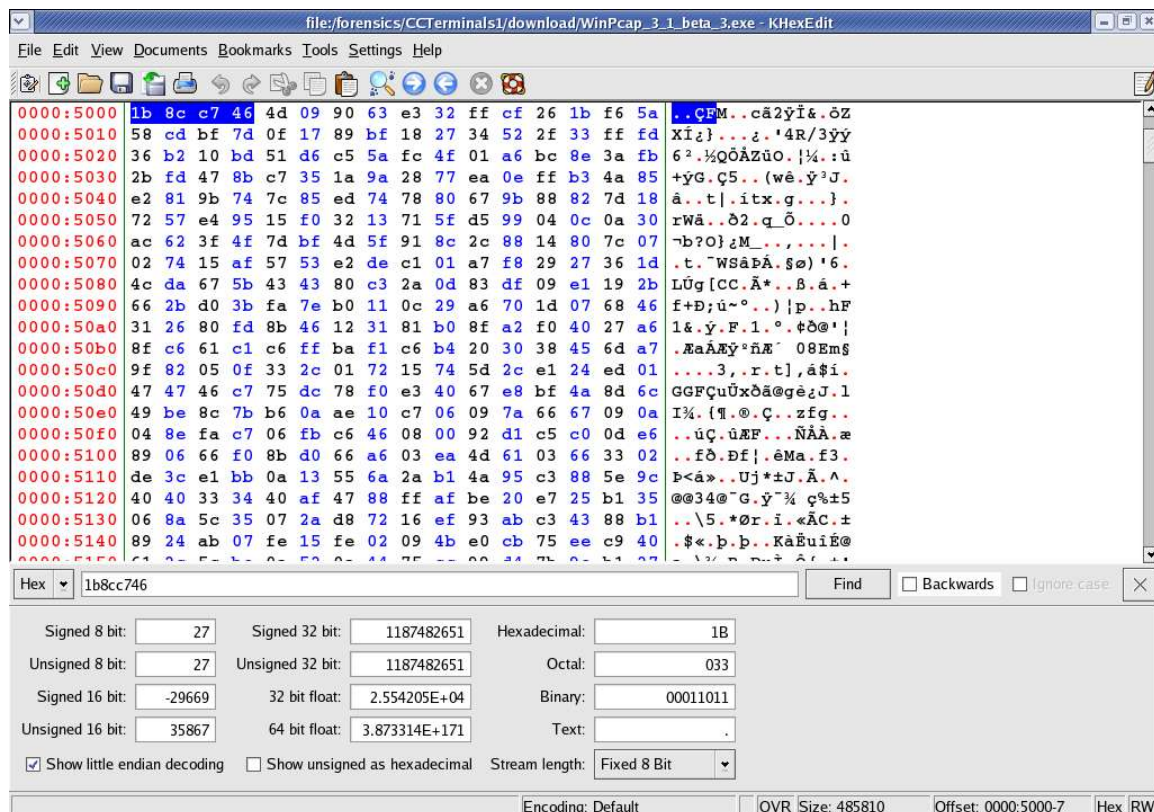
5.2 WinDump.exe

The most straightforward process for positively identifying the recovered program _INDUMP.EXE is to download a copy of the most logical match for the program (in this case, WinDump.exe) from a known site on the Internet and then run `md5sum` on both the downloaded program and the recovered program. If the md5 hashes match, the recovered program can be positively identified. In this case, I downloaded WinDump.exe from the web site where it distributed [19] – http://windump.polito.it/install/default.htm. I then ran `md5sum` on both the downloaded program and the recovered program. The md5 hashes match as shown below:

33
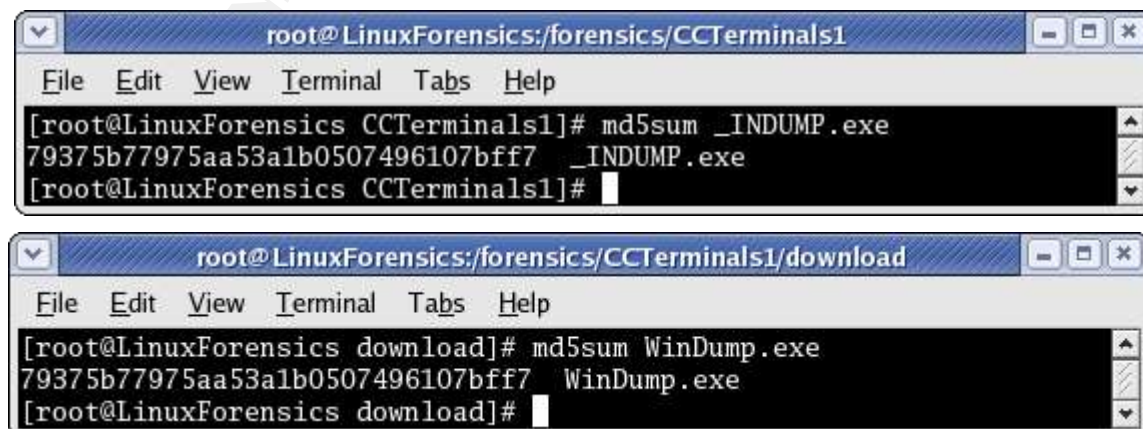
6.0 Legal Implications

This section will discuss the legal implications of the actions taken by Mr. Lawrence. It will also review potential company policy violations.

6.1 Federal Law

There are several federal laws which might apply to network packet sniffing but since the content of the network traffic was recorded in this case, that is a violation of the Wiretap Act. As stated by Ricard Salgado in the book Know Your Enemy, "Sniffing traffic on a network may be considered an interception of electronic communications and would fall within the scope of the WireTap Act. A violation of the Wiretap Act is no small matter. It can lead to a civil suit and may constitute a federal felony punishable by a fine and up to five years in prison" [1] (228). There are several exceptions to the Wiretap Act, such as the Provider Protection Exception, and the Consent of a Party Exception, however they do not appear to apply in this case. For the Provider Protection Exception to apply, Mr. Lawrence's job function would have to include responsibility for providing and securing network services at CC Terminals which is not consistent with his job title of sales representative. For the Consent of Party Exception to apply, Ms. Conlay (and the other users on the network at the time the network traffic was recorded) would have needed to consent to having their network traffic observed and recorded. There is no documentation indicating that Ms. Conlay or any of the other users on the network consented to the observation and recording of their network traffic by Mr. Lawrence. Based on the evidence contained in the recovered capture file on the partition 2 image file it appears that Mr. Lawrence is in violation of the Wiretap Act, however, it should be noted that some companies choose not to involve law enforcement in internal cases due to concerns about negative publicity.

6.2 Company Policy

If CC Terminals has an Acceptable Use Policy which forbids the use of a network packet sniffer by unauthorized personal, then Mr. Lawrence may be found to be in violation of company policy. An Acceptable Use Policy is most enforceable when it has been communicated on a scheduled (usually yearly) basis and the employee must verify that they have received the communication in writing or by some other traceable means. The Acceptable Use Policy should contain clear consequences for prohibited behavior and the HR department should have documented processes for investigating and, if necessary, terminating employment for violations of the policy.

34

7.0 Recommendations

This section contains my recommendations for steps that could be implemented at CC Terminals to reduce the chance of a similar problem happening in the future.

7.1 Develop and Implement an Acceptable Use Policy

If not already in place, the development and implementation of an Acceptable Use Policy that includes network packet sniffing as a prohibited activity would be the first step in managing employee behavior. An Acceptable Use Policy should be reviewed and, if possible, signed by all employees on a yearly basis so that the consequences for unacceptable behavior are clearly communicated.

7.2 Review Hiring Practices

Review current hiring practices and, if needed, evaluate adding processes such as a background check to determine if an potential employee has had issues with harassment or violent behavior in the past.

7.3 Remove Administrator Privileges from End Users

Evaluate removing Administrator privileges from end users on Windows NT/2000/XP. One of the files in this case – WinPcap_3_1_beta_3.exe - required Administrator privileges to install on Windows NT/2000/XP. If none of the end users at CC Terminals had Administrator privileges on their computers running Windows NT/2000/XP then the network sniffing aspect of this case would have been more difficult for an end user to accomplish. There are potential consequences to removing Administrator privileges for end users so a complete cost / benefit analysis would need to be done before implementing this recommendation.

7.4 Implement a Network Intrusion Detection System

If not already in place, evaluate implementing a network intrusion detection / security scanning system. A properly configured and managed network intrusion detection / security scanning system can detect many types of potentially malicious behavior on the network This could include a computer with it's network card in promiscuous mode such as the one which was used by Mr. Lawrence to observe and record network traffic.

35

8.0 Additional Information

This section contains links to web sites with additional information on topics relevant to this investigation.

8.1 Acceptable Use Policy - Template

http://www.sans.org/resources/policies/Acceptable_Use_Policy.pdf
This web site provides a template for a Acceptable Use Policy that specifically defines network sniffing as a prohibited activity.

8.2 Workplace Management

http://www.workforce.com/
This web site containing a wealth of information regarding HR, legal, and staffing issues. It is a multifaceted site containing a Research Center with numerous articles relating to the workplace, a Community Center with forums on workplace issues, and a Commerce Center with vendors providing workplace related services. Free registration is required for some parts of the web site.

8.3 Legal Implications of Network Packet Sniffing

http://www.digitalchoke.com/daynotes/reports/Computer-Felony.pdf
This pdf file contains an in depth discussion of the various laws that apply to the use of network packet sniffers. It includes discussion of the provisions of the Wiretap Act, the Pen/Trap Act, and the Electronic Communications Privacy Act.

8.4 Overview of Network Packet Sniffing in the Workplace

http://computer.howstuffworks.com/workplace-surveillance2.htm
This web site provide a basic overview of how a network packet sniffer operates in the workplace however it focuses on employer monitoring employees, not employees monitoring company network traffic.

References

[1]   Salgado, Richard. "Legal Issues." <u>Know Your Enemy, Learning
         About Security Threats.</u> Ed. The Honeynet Project. Boston:Pearson
         Education, Inc., 2004. 225-252

[2]   Carrier, Brian. <u>Autopsy Forensic Browser</u>. March 8, 2005
         URL:http://www.sleuthkit.org/autopsy/

[3]   Author Unknown. <u>Ethereal: A Network Protocol Analyzer</u>.
         March 8, 2005 URL:http://www.ethereal.com/

[4]   Author Unknown. <u>Vmware – Virtual Infrastructure Software</u>.
         March 8, 2005 URL:http://www.vmware.com/

[5]   Author Unknown. <u>OpenOffice.org</u>. March 8, 2005
         URL:http://www.openoffice.org/

[6]   Wreski, David. "System Security." Linux Magazine. October 2000:4.
         March 8, 2005
         URL:http://www.linux-mag.com/2000-10/security_04.html

[7]   Author Unknown. <u>Unix man pages</u>. March 8, 2005
         URL:http://www.rt.com/man/fdisk.8.html

[8]   Carrier, Brian. <u>The Sleuth Kit</u>. March 8, 2005
         URL:http://www.sleuthkit.org/sleuthkit/man/mmls.html

[9]   Darwin, Ian. <u>UNIX man pages</u>. March 8, 2005
         URL:http://unixhelp.ed.ac.uk/CGI/man-cgi?file

[10]   Costyn. <u>LinuxQuestions.org</u>. March 8, 2005
         URL:http://wiki.linuxquestions.org/wiki/Dd

[11]   Mandia, Kevin, and Chris Prosise and Matt Pepe. <u>Incident
         Response & Computer Forensics Second Edition</u>. Emeryville, CA:
         McGraw-Hill / Osborne, 2003.

[12]   Cooper, Mendel. "Advanced Bash-Scripting HOWTO." <u>External Filters, Programs, and Commands</u>. March 8, 2005
        URL:http://docsrv.sco.com:8457/en/AdvBashHowto/external.html

[13]   SANS Institute. <u>Track 8 – Systems Forensics, Investigation & Response Windows 2000/XP & NTFS Filesystem Forensics</u>. 2004.

[14]   Farmer, Dan and Wietse Venema. <u>Forensic Discovery</u>. Upper Saddle River, NJ: Addison-Wesley, 2005.

[15]   SANS Institute. <u>Track 8 – Systems Forensics, Investigation & Response Forensic & Investigative Essentials</u>. 2004.

[16]   Davis, Chris and David Cowen and AaronPhilipp. Hacking Exposed Computer Forensics Secrets & Solutions. Emeryville, CA: McGraw-Hill / Osborne, 2005.

[17]   Lee, Rob. "Windows Computer Forensics." <u>Know Your Enemy, Learning About Security Threats.</u> Ed. The Honeynet Project. Boston:Pearson Education, Inc., 2004. 405-445

[18]   Author Unknown. <u>Windows Packet Capture Library</u>. March 9, 2005
        URL:http://winpcap.polito.it/

[19]   Author Unknown. <u>WinDump: tcpdump for Windows</u>. March 9, 2005
        URL:http://windump.polito.it/

[20]   Author Unknown. <u>Index</u>. March 8, 2005
        URL:ftp://gd.tuwien.ac.at/infosys/security/polito.it/winpcap/