Global Information Assurance Certification Paper

GIAC Certified Forensic Analyst (GCFA)
Practical Assignment Version 2.0
Option (a)
First Attempt

Yijia Zhou, Craig
Network Security Engineer
March 29th, 2005.

Abstract

This document is prepared to obtain the GCFA certification. Option-1 (practical assignment) is selected. The content outlines the procedures used in this media analysis project from technical and legal perspective. Areas being covered are: technical forensic tools and steps, result analysis, legal implication findings, and recommendations to the affected parties.

Index

Executive Summary

On October 30th, 2004, Mark Mawer, a security officer from CC Terminals Corporation, requested forensic analysis on a seized USB drive. Mark provided the following background information:

Leila Conlay, a sales representative from CC Terminals, reported on the afternoon of October 29th that she has being harassed by her colleague Robert Lawrence. According to Leila, Robert had made numerous attempts to meet her, both during and outside of work, he had also send emails to her personal email address, the content of the emails was provocative and aggressive, especially the most recent ones. To Leila's surprise, Robert managed to find her while she was at a coffee shop with a friend on the evening of Thursday October 28th.

A USB Flash drive was seized during afterhours search of Robert's cubicle, the drive has the following characteristics:

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

Custody chain and integrity of this article is recorded for evidence admissibility preservation.

The image was downloaded from the pointed URL (*https://www.giac.org/GCFAPractical2.0-USBImageAndInfo.zip.gz*) on January 20th 2005. Following is a brief summary after a thoroughly analysis of the drive:

We conclude that Ms. Conlay's accusation is legitimate. Mr. Lawrence had, conceivably, violated both the "Sexual Harassment" and "Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited" law. The breaching of either one is considered a criminal activity, which may lead to law suit and imprisonment.

Three recovered word documents indicated that Mr. Lawrence had sent emails to Ms. Conlay. The content of the emails is full of harassments and unsolicited propositions. Most of the emails were dated from 25th to 28th of October, 2004. Please refer to 'Image Details' section for complete email content.

We have also identified that Mr. Lawrence had used a software tool to intercept communication between Ms. Conlay's computer and an internet mail server at

11:08 am October 28th. In this email communication, Ms. Conlay had used her personal address (flowergirl96@hotmail.com) and made an appointment with her friend at a coffee shop. A picture file was identified on the same drive that pointed the exact location of the appointment. We are confident that Mr. Lawrence used the intercepted information to find Ms. Conlay in the coffee shop.

Based on the evidence, I suggest soliciting help and advisory from the company attorney and legal counsel immediately. Reporting to local law enforcement is highly recommended.

Examination Detail

In this section, media analysis steps are outlined in a chronological order. Tools, commands, and screen shots are included for reference. To keep the chain of custody, a MD5 hash is performed on every result file and the hash value is listed in Appendix-B. The tools and commands used are from a credible source and are kept identical during examination as shown by MD5 hash values in Appendix-C.

Before jumping into technical details, a quick summary of the forensic workstation is as below:

Dell Laptop, P-III CPU with 512 MB Ram,
Complete installed Redhat Linux-9 with kernel 2.40.20-6
Sleuth Kit 1.72 and Autopsy 2.0.3,
Ethereal 0.9.8,
KHexEdit 0.8.5,
VMWARE 4.0 with Standard Windows 2000 server, MS Office 2000.

Step-1 Download Image

The image was downloaded from the pointed URL *(https://www.giac.org/GCFAPractical2.0-USBImageAndInfo.zip.gz)*. '***File***[1]' command found that the image was in Gzip compress format, thus '***Gunzip***' command was used to decompress the image. The result file has MD5 value of '338ecf17b7fc85bbb2d5ae2bbc729dd5'. This proved the result image was the exact copy of the image seized by Mark Mawer.

```
[root@LinuxForensics GCFA]# ls -l
total 748
-rw-r--r--    1 root     root       760459 Mar 18 11:56 GCFAPractical2.0-USBImageAndInfo.zip.gz
[root@LinuxForensics GCFA]# file GCFAPractical2.0-USBImageAndInfo.zip.gz
GCFAPractical2.0-USBImageAndInfo.zip.gz: gzip compressed data, was "USBFD-64531026-RL-001.img", from Unix, max
compression
[root@LinuxForensics GCFA]# gunzip -N GCFAPractical2.0-USBImageAndInfo.zip.gz
[root@LinuxForensics GCFA]# ls -l
total 61040
-rw-r--r--    1 root     root     62439424 Oct 26 01:58 USBFD-64531026-RL-001.img
```

[1] File - classify object file type based on file system test, magic number test and language test. Reference site: http://www.ctssn.com/man/index.cgi?section=all&topic=file

```
[root@LinuxForensics GCFA]# md5sum USBFD-64531026-RL-001.img
338ecf17b7fc85bbb2d5ae2bbc729dd5  USBFD-64531026-RL-001.img
```

Screenshot-1, Gunzip the downloaded media.

Step-2 Splitting the image with "mmls[2]" and "dd[3]"

Before data analysis, the raw image must be split into logical partitions. '***mmls***' command was used to display the layout of media partition table. Result is showed in Screenshot-2.

A quick summary of 'mmls' result:

The smallest data block (sector) on this image is 512 bytes,
partition '00' takes only 1 sector that consists of Master Boot Record,
partition '01' is 'unallocated', and it contains no user data,
partition '02' is in FAT16 format, this appears to be the only partition that hosts user data. (For disk partition information, please refer to 'Additional Information' section).

```
[root@LinuxForensics GIAC]# 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 GIAC]#
```

Screenshot-2, mmls command output

'***dd***' was used to extract partition '02'. The result file was named 'USBFD-Partition-02.img' and it has MD5 hash value of '5f830a763e2144483f78113a8844ad52'.

```
[root@LinuxForensics GIAC]# dd if=USBFD-64531026-RL-001.img bs=512 skip=32 count=121919 of=USBFD-Partition-
02.img
121919+0 records in
121919+0 records out
[root@LinuxForensics GIAC]# md5sum USBFD-Partition-02.img
5f830a763e2144483f78113a8844ad52  USBFD-Partition-02.img
[root@LinuxForensics GIAC]#
```

Screenshot-3, extract partition '02' using 'dd'

Step-3 Creating a case in Autopsy [4]

To further the analysis, I created a case in 'Autopsy', a browser interface to using the Sleuth Kit[5] and the Coroner's Toolkit[6]. Please see reference section for more detail of the tools.

---

[2] mmls - part of Sleuth Kit, display image partition information: http://www.Sleuthkit.org/Sleuthkit/man/mmls.html
[3] dd - a tool that reads a block of data from an input file and writes it to an output file. http://www.ctssn.com/man/index.cgi?section=all&topic=dd
[4] Autopsy – is a graphical interface to The Sleuth Kit and it can automate the process of creating and viewing a time line. Ref site: http://www.sleuthkit.org/autopsy/
[5] The Sleuth Kit - is a collection of UNIX-based command line tools that allow you to investigate a computer: http://www.sleuthkit.org/sleuthkit/
[6] The Coroner's Toolkit (TCT) is a collection of programs by Dan Farmer and Wietse Venema for a post-mortem analysis of a UNIX system after break-in. http://www.porcupine.org/forensics/tct.html

1. A case was created with the following information:
   Case Name: CC Terminals
   Description: req. by Mark Mawer
   Investigator: Null (* since I am the only investigator)
2. A new host was added with the following information:
   Hostname: host1
   Description: One USB Flash Drive only
   Time zone: PDT *(I used PDT since I am in the same TZ as CC Terminals people)*
   Timeskew Adjustment: 0
3. The image was added with the following information:
   Location: /images/windowsforensics/GIAC/USBFD-Partition-02.img
   Copy: selected
   File system: FAT16
   Mount Point: /
   Data Integrity: Calculate the hash value for this image.

4. 'BODY' and timeline file were created in 'Autopsy'.

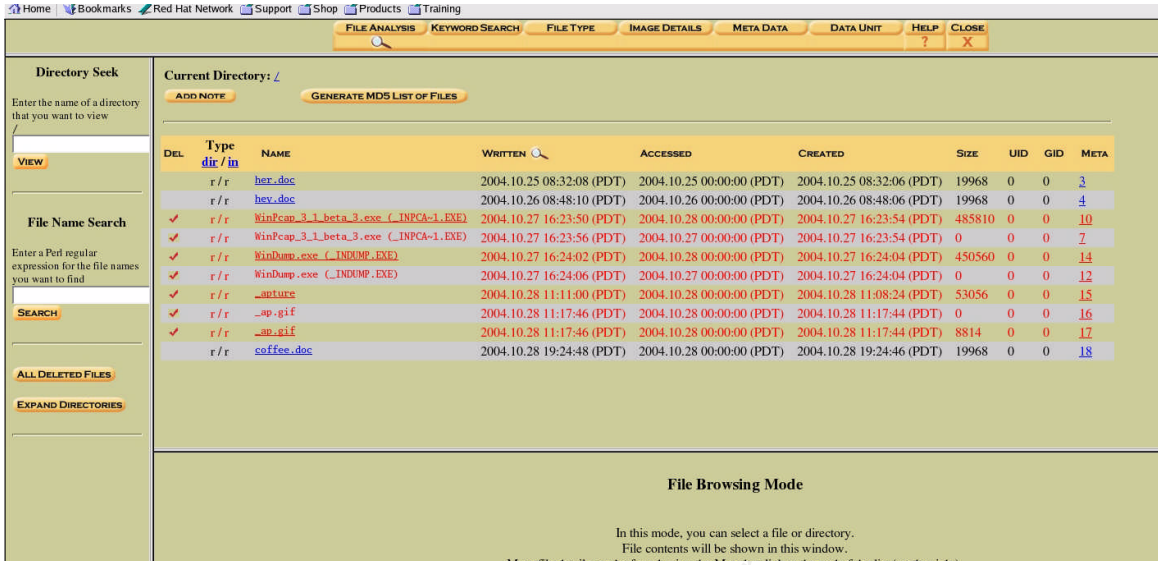
'BODY' file creation was the first step. Autopsy automatically run two commands, '***fls***' and '***ils***', on image file 'USBFD-Partition-02.img -- *'fls*[7] *–r –m'* and *'ils*[8] *–m'.* The two commands are used to list all the file system layer and meta data layer information. The 'BODY' file was saved as '/forensics/CCTerminals/host1/output/body' with MD5 value of '2850C0E1CF826D2311E40D360570F4F4'.

In the second step, the '***mactime***[9]' tool was fed the output from the two commands to generate an actual timeline file. The timeline file was saved as '/forensics/CCTerminals/host1/output/timeline.txt' with MD5 value of'1F85DE244A800763EF3A82FBEC5C89B9', (Attached in Appendix-A).

Step-4 File recovery

Before actual file recovery happened, the following information was collected from Autopsy 'File Analysis' window:

[7] fls - Lists allocated and deleted file names in a directory, http://www.sleuthkit.org/sleuthkit/man/fls.html
[8] ils - Lists the meta data structures and their contents in a pipe delimited format, http://www.sleuthkit.org/sleuthkit/man/ils.html
[9] Mactime –part of sleuth Kit, it takes input from the fls and ils tools to create a timeline of file activity, http://www.sleuthkit.org/sleuthkit/man/mactime.html



Screenshot-4, Autopsy 'File Analysis' view.

Despite three duplicated file names pointed to by different 'inode' numbers as showed in the last column, there are seven files on this image. File names in blue showed existing files, file names in red showed deleted files.

'her.doc' pointed to inode-3 with size of 19968 bytes.
'hey.doc' pointed to inode-4 with size of 19968 bytes.
'coffee.doc' pointed to inode-18 with size of 19968 bytes.
'WinPcap_3_1_beta_3.exe' pointed to inode-10 with size of 485810 bytes
'WinDump.exe' pointed to inode-14 with size of 450560 bytes
'_apture' pointed to inode-15 with size of 53056 bytes
'_ap.gif' pointed to inode-17 with size of 8814 bytes
** Noticed that Inode 7, 12, 16 did not point to any sector and thus the file size was '0'.

Similar information was verified via '***fls***' tool as displayed in screenshot-5.

```
[root@LinuxForensics GIAC]# fls -f fat16 USBFD-Partition-02.img
r/r 3:  her.doc
r/r 4:  hey.doc
r/r * 7:        WinPcap_3_1_beta_3.exe (_INPCA~1.EXE)
r/r * 10:       WinPcap_3_1_beta_3.exe (_INPCA~1.EXE)
r/r * 12:       WinDump.exe (_INDUMP.EXE)
r/r * 14:       WinDump.exe (_INDUMP.EXE)
r/r * 15:       _apture
r/r * 16:       _ap.gif
r/r * 17:       _ap.gif
r/r 18: coffee.doc
[root@LinuxForensics GIAC]#
```
Screenshot-5, 'fls' output.

With 'inode' number information, '***istat***[10]' tool was used to display the meta layer statistics, then 'icat[11]' tool was used to capture that inode associated data

[10] Istat – part of Sleuth Kit that can display meta layer information for a given inode.
[11] icat – part of Sleuth Kit that can capture raw data from all associated sectors from a given inode.

sectors, thus recover the file.

```
[root@LinuxForensics GIAC]# istat -f fat16 USBFD-Partition-02.img 3
Directory Entry: 3
Allocated
File Attributes: File, Archive
Size: 19968
Num of links: 1
Name: her.doc

Directory Entry Times:
Written:        Mon Oct 25 08:32:08 2004
Accessed:       Mon Oct 25 00:00:00 2004
Created:        Mon Oct 25 08:32:06 2004

Sectors:
511 512 513 514 515 516 517 518
......
[root@LinuxForensics GIAC]# icat -f fat16 USBFD-Partition-02.img 3 > her.doc
[root@LinuxForensics GIAC]# ls -l her.doc
-rw-r--r--    1 root     root        19968 Mar 16 13:23 her.doc
[root@LinuxForensics GIAC]# md5sum her.doc
9785a777c5286738f9deb73d8bc57978  her.doc
[root@LinuxForensics GIAC]#
```

Screenshot-6, 'her.doc' was recovered from inode 3.

As seen in Screenshot-6, 'her.doc' was recovered with MD5 value of '9785a777c5286738f9deb73d8bc57978'.

Following similar steps, 'hey.doc' was recovered as seen in Screenshot-8 with MD5 value of 'ca601d4f8138717dca4de07a8ec19ed1'.

```
 [root@LinuxForensics GIAC]# icat -f fat16 USBFD-Partition-02.img 4 > hey.doc
[root@LinuxForensics GIAC]# ls -l hey.doc
-rw-r--r--    1 root     root        19968 Mar 16 13:31 hey.doc
[root@LinuxForensics GIAC]# md5sum hey.doc
ca601d4f8138717dca4de07a8ec19ed1  hey.doc
[root@LinuxForensics GIAC]#
```

Screenshot-8, recover 'hey.doc' from inode 4.

'coffee.doc' was also recovered from inode 18 with MD5 value of 'a833c58689596eda15a27c931e0c76d1', as seen in Screenshot-9.

```
 [root@LinuxForensics GIAC]# icat -f fat16 USBFD-Partition-02.img 18 > coffee.doc
[root@LinuxForensics GIAC]# ls -l coffee.doc
-rw-r--r--    1 root     root        19968 Mar 16 13:35 coffee.doc
[root@LinuxForensics GIAC]# md5sum coffee.doc
a833c58689596eda15a27c931e0c76d1  coffee.doc
[root@LinuxForensics GIAC]#
```

Screenshot-9, 'coffee.doc' was recovered from inode 18.

Output from 'istat' command indicated that inode 14 was a deleted file. However, the file can still be retrieved from its recovery sectors.

```
[root@LinuxForensics GIAC]# istat -f fat16 USBFD-Partition-02.img 14 | more
Directory Entry: 14
Not Allocated
File Attributes: File, Archive
Size: 450560
Num of links: 0
Name: _INDUMP.EXE

Directory Entry Times:
```

```
Written:        Wed Oct 27 16:24:02 2004
Accessed:       Thu Oct 28 00:00:00 2004
Created:        Wed Oct 27 16:24:04 2004

Sectors:
1541 1542

Recovery:
1541 1542 1543 1544 1545 1546 1547 1548
.................
```

Screenshot-10, inode 14 information

Using ***'icat-r'***, 'WinDump.exe' was successfully recovered and it has MD5 hash value of '79375b77975aa53a1b0507496107bff7', as seen in Screenshot-11.

```
[root@LinuxForensics GIAC]# icat -f fat16 USBFD-Partition-02.img -r 14  > WinDump.exe
[root@LinuxForensics GIAC]# ls -l WinDump.exe
-rw-r--r--    1 root     root       450560 Mar 16 14:21 WinDump.exe
[root@LinuxForensics GIAC]# md5sum WinDump.exe
79375b77975aa53a1b0507496107bff7  WinDump.exe
```

Screenshot-11. 'WinDump.exe' was recovered from inode 14.

'_apture' was successfully recovered from inode 15. It has a MD5 value of '2097b7b0a9fedb4238b67e976c4ae1cb', as seen in screenshot-12. I suspected that the original file name should be 'capture' instead of '_apture', so the result was renamed to 'capture'.

```
[root@LinuxForensics GIAC]# icat -f fat16 USBFD-Partition-02.img -r 15 > _apture
[root@LinuxForensics GIAC]# ls -l _apture
-rw-r--r--    1 root     root        53056 Mar 16 14:35 _apture
[root@LinuxForensics GIAC]# md5sum _apture
2097b7b0a9fedb4238b67e976c4ae1cb  _apture
[root@LinuxForensics GIAC]# mv _apture capture
```

Screenshot-12, '_apture' was recovered from inode 15.

'_ap.gif' file was recovered from inode 17 with MD5 value of '9bc3923cf8e72fd405d7cea8c8781011'. Logically, the file name should be map.gif instead of '_ap.gif', so it was renamed to 'map.gif'.

```
[root@LinuxForensics GIAC]# icat -f fat16 USBFD-Partition-02.img -r 17 > _ap.gif
[root@LinuxForensics GIAC]# ls -l _ap.gif
-rw-r--r--    1 root     root         8814 Mar 16 14:54 _ap.gif
[root@LinuxForensics GIAC]# md5sum _ap.gif
9bc3923cf8e72fd405d7cea8c8781011  _ap.gif
[root@LinuxForensics GIAC]# mv _ap.gif map.gif
```

Screenshot-13, 'map.gif' was recovered from inode 17.

It was a bit tricky to recover 'WinPcap_3_1_beta_3.exe' from inode 10. '***istat***' command produced the following information, as seen in Screenshot-14.

```
[root@LinuxForensics GIAC]# istat -f fat16 USBFD-Partition-02.img 10
Directory Entry: 10
Not Allocated
File Attributes: File, Archive
Size: 485810
Num of links: 0
Name: _INPCA~1.EXE

Directory Entry Times:
Written:        Wed Oct 27 16:23:50 2004
Accessed:       Thu Oct 28 00:00:00 2004
Created:        Wed Oct 27 16:23:54 2004
```

```
Sectors:
591 592 593 594 595 596 597 598
599 600 601 602 603 604 605 606
607 608 609 610 611 612 613 614
615 616 617 618 619 620 621 622
623 624 625 626 627 628 629 630

Recovery:
File recovery not possible
[root@LinuxForensics GIAC]#
```

Screenshot-14, inode 10 meta information showed from 'istat; tool.

Inode 10 pointed to 'WinPcap_3_1_beta_3.exe' with size of 485810 bytes. Theoretically, it should occupy 949 sectors ((485810 + 511) / 512 = 949), but '***istat***' only displayed 40 sectors (from 591 to 630). The 'istat' result also indicated that file recovery was not possible.

'***ifind***'[12] tool was used to examine the inode number of sectors 591, 592, and 630. The result indicated that all sectors belonged to inode 18. Recalled from previous file recovery, inode 18 was used by 'coffee.doc'. Obviously, this was contributed by disk fragmentation, the first 40 sectors were occupied by the new file - 'coffee.doc'.

```
[root@LinuxForensics GIAC]# ifind -f fat16 USBFD-Partition-02.img -d 591
18
[root@LinuxForensics GIAC]# ifind -f fat16 USBFD-Partition-02.img -d 592
18
[root@LinuxForensics GIAC]# ifind -f fat16 USBFD-Partition-02.img -d 630
18
```

Screenshot-15, 'ifind' on sector 591, 592, and 630

Assuming data was continuously allocated on the image, 'WinPcap' should be stored from sector 591 to 1540, (591+949 =1540). Although the first 40 sectors (591-630) were occupied by 'coffee.doc', the remaining 909 sectors should still contain data. Base on this assumption, 'dd' command was used to cut out the remaining part. The result was saved to 'part-inode-10.raw' with size of 465408 bytes and MD5 value of 'cdfcf8565e622daf838b8f5c692eb11b'.

```
[root@LinuxForensics GIAC]# dd if=USBFD-Partition-02.img bs=512 skip=631 count=909 of=part-inode-10.raw
909+0 records in
909+0 records out
[root@LinuxForensics GIAC]# ls -l part-inode-10.raw
-rw-r--r--    1 root     root       465408 Mar 16 15:38 part-inode-10.raw
[root@LinuxForensics GIAC]# md5sum part-inode-10.raw
cdfcf8565e622daf838b8f5c692eb11b  part-inode-10.raw
[root@LinuxForensics GIAC]#
```

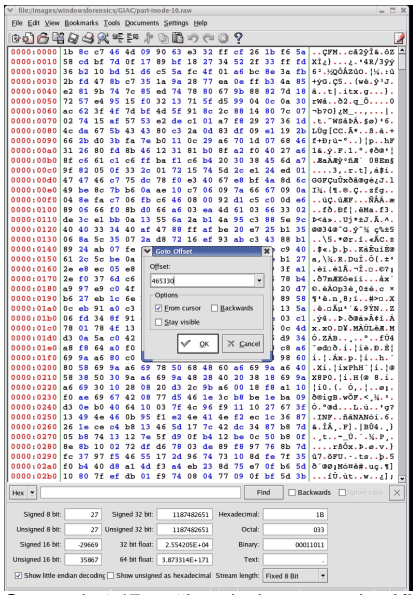
Screenshot-16, 'part-inode-10.raw' was cut out by 'dd' command.

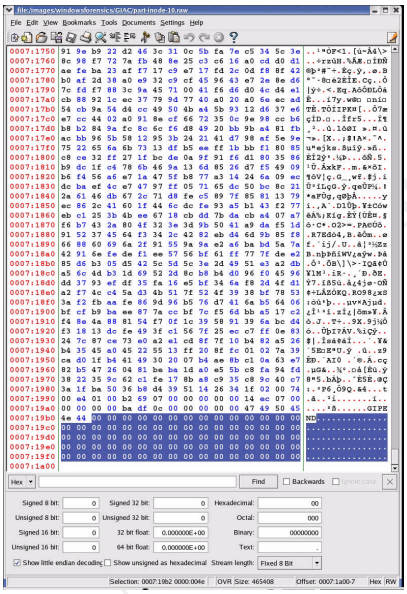
Knowing from 'istat' result, file 'WinPcap_3_1_beta_3.exe' has size of 485810 bytes, minus the first 20480 bytes (512 x 40 = 20480), the remaining part should be 465330 bytes (485810 – 20480 = 465330). Since 'part-inode-10.raw' had a size of 465408 bytes, it is certain that there is slack space [13]at the end of the recovered file. The slack space needs to be eliminated.

[12] ifind – to find out the inode number associated with the given sector number. Ref site: http://www.Sleuthkit.org/Sleuthkit/man/ifind.html

[13] Slack Space - unused space in a disk cluster. Reference site, http://www.webopedia.com/TERM/S/slack_space.html

A Linux version of Hex Editor - KHexEdit was used to cut the slack space. KHexEdit, which comes with Redhat 9 KDE package, is an editor for the raw data of binary files. Reference URL: http://home.online.no/~espensa/khexedit/





Screenshot-17, cutting slack space using KHexEdit.

The result file was saved to 'part-WinPcap_3_1_beta_3.exe' with MD5 value of '70553e1c186284f46b46c9521bba629b'.

```
[root@LinuxForensics GIAC]# ls -l part-WinPcap_3_1_beta_3.exe
-rw-r--r--    1 root     root       465330 Mar 16 15:59 part-WinPcap_3_1_beta_3.exe
[root@LinuxForensics GIAC]# md5sum part-WinPcap_3_1_beta_3.exe
70553e1c186284f46b46c9521bba629b  part-WinPcap_3_1_beta_3.exe
[root@LinuxForensics GIAC]#
```

Screenshot-18, 'part-WinPcap_3_1_beta_3.exe was recovered

Step-5 Timeline Analysis

Timeline analysis is always crucial in forensic analysis. This kind of analysis can help to find out file activities. In particular, a FAT File system has the following time stamps:

- ***Written**: When the file was last written to. It is the ONLY required time in the FAT file system.*
- ***Accessed**: When the file was last accessed. In FAT, it is only accurate to the day (not minute). It is an optional value, so some Operating Systems may not update it.*
- ***Created**: When the file was created. It is also optional.*

Above information was referenced from "Timelines" section in Autopsy "Help" page. For more information regarding FAT16 file system specification and timeline, please refer to Reference section.

Examination of the timeline file (see in Appendix-A) produced the following results:

- "her.doc" was created on Mon Oct 25 2004 08:32:06, and last written on Mon Oct 25 2004 08:32:08, last access time was on the same day.

- "hey.doc" was created on Tue Oct 26 2004 08:48:06, and last written on Tue Oct 26 2004 08:48:10, last access time was on the same day.

- On Wed Oct 27 2004 16:23:54, 'WinPcap_3_1_beta_3.exe' was created on this image, last written time was Wed Oct 27 2004 16:23:56. It was last accessed (run) on Thu Oct 28 2004.

- 'WinPcap_3_1_beta_3.exe' and 'WinDump' was created at the same time It was last written on Wed Oct 27 2004 16:24:06. It was last accessed on Thu Oct 28 2004.

- '_apture' was created on Thu Oct 28 2004 11:08:24, last written on Thu Oct 28 2004 11:11:00, and last accessed on the same day.

- '_ap.gif' was created on Thu Oct 28 2004 11:17:44, last written on Thu Oct 28 2004 11:17:46, and last accessed on the same day..

- On Thu Oct 28 2004 19:24:46, 'coffee.doc' was created, last written time on Thu Oct 28 2004 19:24:48, and last accessed on the same day.

Step-6 File Examination

In this step, '***file***' command was used to classify file type. The result showed that 'her.doc', 'hey.doc' and 'coffee.doc' are Microsoft Office Documents, 'map.gif' is a GIF image file, 'WinDump.exe' is MS-DOC executable program, and 'part-WinPcap_3_1_beta_3.exe' is a data file because this file was only partially recovered and could not be correctly recognized by 'file' command.

```
[root@LinuxForensics GIAC]# file *
capture:                    tcpdump capture file (little-endian) - version 2.4 (Ethernet,
capture length 4096)
coffee.doc:                 Microsoft Office Document
her.doc:                    Microsoft Office Document
hey.doc:                    Microsoft Office Document
map.gif:                    GIF image data, version 89a, 300 x 200
part-WinPcap_3_1_beta_3.exe: data
WinDump.exe:                MS-DOS executable (EXE), OS/2 or MS Windows
[root@LinuxForensics GIAC]#
```

Screenshot-19, 'file' command result showed file types.

Word Document Examination

The first Word document – 'her.doc' was opened in MS Word, the contents was displayed as below:

> *"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"*

This looked like a draft email that Mr. Lawrence prepared before sent to Ms. Conlay. From the timeline analysis, this file was created on Mon Oct 25 2004 08:32, last modified a few seconds later, and last accessed on the same day. Therefore, it was reasonable to assume that Mr. Lawrence sent out the first harassment email on Mon Oct 25 2004.

The second Word document 'hey.doc' was opened in MS Word, the content was displayed as below:

> *"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? "*

This appeared to be the second email Mr. Lawrence sent to Ms. Conlay. From timeline analysis, it was it was sent out on October 26th.

The last Word document 'coffee.doc' was opened in MS Word and the following message appeared:

> *"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..."*

Obviously, this was the last email that Mr. Lawrence sent to Ms. Conlay. According to timeline record, it was sent out on 2004 Oct 28th at 19:24:46. It was noted that Mr. Lawrence did mention the fact that he went to the coffee shop and saw Ms. Conlay and her friend.

Tcpdump capture file examination

Since 'capture' was a tcpdump capture file, '***ethereal***[14]' could be a perfect tool for examination. 'Ethereal' is a open source network packet analyzer

After opening 'capture' file in 'ethereal' application, it was observed that all packets captured were between 2004-10-18 11:10:54 to 2004-10-28 11:10:55. Except SNMP broadcasting traffic, the rest of all packets were HTTP/TCP transactions between an internal private IP address (192.168.2.104) and a few external IP addresses. DNS lookup results for those external IP are as below:

64.4.34.250 -	www.bay12.hotmail.com
207.68.178.16	rad.msn.com
207.68.177.124	h.msn.com

After highlighting the first TCP packet, and using 'Follow TCP Stream' Option lead to the following screen:

Screenshot-20, Examine the first HTTP package

Obviously, this transaction recorded someone who accessing his/her hotmail account. The brown color text on top contained a message posted by the client, the blue color text was the html page sent back from the hotmail server. Inside the brown text, the following lines was captured, as seen highlighted in Screenshot-24.

"curmbox=F000000001&HrsTest=&_HMaction=Send&FinalDest=&subaction=&plaintext=&login=flowergirl96&msg=&start=&len=&attfile=&attlistfile=&url=&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%0

[14] ethereal – open source tool for network package analyzer, reference site: http://www.ethereal.com

D%0ASee+you+at+7pm%21%0D%0A%0D%0A-Leila"

This appeared to be a private email sent from the hotmail account 'flowergirl96@hotmail.com' to another account 'SamGuarillo@hotmail.com'. Most likely, 'Flowergirl96@hotmail.com' was Ms. Conlay's personal email account, and 'SamGuarillo@hotmail.com' was her friend's personal account.

After consulting the ASCII table in http://www.lookuptables.com/, the actual email was tranlated as below:

> *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*

From timeline analysis, we know that this file was last written on Thu Oct 28 2004 11:11:00. The packages were captured on Oct 28th 2004 around 11:10am according to the 'Time' column.

Graphic file - 'map.gif' examination

This is how the 'map.gif' file looks like in a Mozilla browser::

Screenshot-21, map.gif

This must be the map near the vicinity of the coffee shop where Leila had an appointment with her friend. The "map.gif" was last written on Thu Oct 28 2004 11:17:46, a few minutes after the 'capture' file was last written. Therefore, It is reasonable to believe that Mr. Lawrence captured the network traffic, revealed the appointment email, and find out the appointment location from the map

The "Microsoft MapPoint" logo one the top of this file could be the application Mr. Lawrence used to generate this graphic file. This could be something worth further investigation on Mr. Lawrence's computer.

The question which remained was: What program did Mr. Lawrence use to

capture network traffic? The question can be answered in 'Forensic Details' section.

Image Details

Based on examination results and output from the Autopsy tool, following is the quick summary of the entire image:

1:	Name:	her.doc
	TrueName:	her.doc
	Last written time:	2004.10.25 08:32:08 (PDT)
	Last accessed time:	2004.10.25 (PDT)
	Last created time:	2004.10.25 08:32:06 (PDT)
	File owner:	UID: 0, GID: 0
	File size:	19968
	MD5:	9785a777c5286738f9deb73d8bc57978
2:	Name:	hey.doc
	TrueName:	hey.doc
	Last written time:	2004.10.26 08:48:10 (PDT)
	Last accessed time:	2004.10.26 (PDT))
	Last created time:	2004.10.26 08:48:06
	File owner:	UID: 0, GID: 0
	File size:	19968
	MD5:	ca601d4f8138717dca4de07a8ec19ed1
3.	Name:	_INPCA~1.EXE
	TrueName:	WinPcap_3_1_beta_3.exe
	Recovered file name:	part-WinPcap_3-1_beta_3.exe
	Last written time:	2004.10.27 16:23:56 (PDT)
	Last accessed time:	2004.10.28 (PDT)
	Last created time:	2004.10.27 16:23:54 (PDT)
	File owner:	UID: 0, GID: 0
	File size:	485810 (only 465330 recovered)
	MD5:	70553e1c186284f46b46c9521bba629b
4.	Name:	_INDUMP.EXE
	TrueName:	WinDump.exe
	Last written time	2004.10.27 16:24:06 (PDT)
	Last accessed time:	2004.10.28 (PDT)
	Last created time:	2004.10.27 16:24:04 (PDT)
	File owner:	UID: 0, GID: 0
	File size:	450560
	MD5:	79375b77975aa53a1b0507496107bff7
5.	Name:	_apture
	TrueName:	capture

	Last written time:	2004.10.28 11:11:00 (PDT)
	Last accessed time:	2004.10.28 (PDT)
	Last created time:	2004.10.28 11:08:24 (PDT)
	File owner:	UID: 0, GID: 0
	File size:	53056
	MD5:	2097b7b0a9fedb4238b67e976c4ae1cb
6.	Name:	_ap.gif
	TrueName:	map.gif
	Last written time:	2004.10.28 11:17:46 (PDT)
	Last accessed time:	2004.10.28 (PDT)
	Last created time:	2004.10.28 11:17:44 (PDT)
	File owner:	UID: 0, GID: 0
	File size:	8814
	MD5:	9bc3923cf8e72fd405d7cea8c8781011
7.	Name:	coffee.doc
	TrueName:	coffee.doc
	Last written time:	2004.10.28 19:24:48 (PDT)
	Last accessed time:	2004.10.28 (PDT)
	Last created time:	2004.10.28 19:24:46 (PDT)
	File owner:	UID: 0, GID: 0
	File size:	19968
	MD5:	a833c58689596eda15a27c931e0c76d1

Forensic Details

Based on the examination detailed in 'Program identification' section, it can be certain that two recovered windows executables are the exact copy of the well-known sniff programs - "**WinDump**[15]" and "**WinPcap**[16]". Referenced from their respective official web site, **WinDump** is a Windows version of tcpdump, which can be used to watch and diagnose network traffic. **WinPcap** is an open source library used for packet capturing and network analysis on 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).

In order to better understand the two programs, both of them (downloaded version) were uploaded to VMWARE Windows 2000 system for examination. WinPcap_3_1_beta_3.exe was installed first; it is the compulsory dynamic link library (wpcap.dll) for WinDump. After WinPcap installation, WinDump can be launched in command line with vast amount of options, which makes almost any kinds of wiretap job possible.

[15] WinDump - A port of TcpDump to Windows. It is a command-line tool, Ref site: http://windump.polito.it

[16] WinPcap - WinPcap is an architecture for packet capture and network analysis for the Win32 platforms, Ref site: http://winpcap.polito.it

For example: 'windump -i INTERFACE-1 –host 192.168.2.104 –w capture' will listen on INTERFACE-1 and capture all network traffic for host 192.168.2.104 and output to 'capture'.

Recalled from timeline analysis, both programs were downloaded from Internet on October 27th, 2004 around 16:23. They were used on October 28th, 2004 around 11:10am to capture network traffic from Leila's computer (IP 192.168.2.104), the output was saved to a file called 'capture'.

Program Identification

With two programs' name and version number, a google search quickly leaded me to their respective official site:

WinDump: http://windump.polito.it/
WinPcap: http://winpcap.polito.it/

WinDump.exe was found and downloaded from its official download link: *http://windump.polito.it/install/bin/windump_3_8_3_beta/WinDump.exe*, and saved to a file named 'Download -WinDump.exe'. The downloaded WinDump.exe has a MD5 value of '79375b77975aa53a1b05074961076ff7'.

On WinPcap official site, *http://winpcap.polito.it/install/default.htm*, only version 3.1 beta 4 is available at the moment. However, one of its mirror site – 'ftp://gd.tuwien.ac.at/infosys/security/polito.it/winpcap/' does have version 3.1 beta 3 available. The program was then downloaded from that ftp link and saved to 'Download-WinPcap_3_1_beta_3.exe with MD5 value of '4511ee3b4e5d8150c035a140dfba72c0'.

```
[root@LinuxForensics GIAC]# md5sum Download*.exe
79375b77975aa53a1b0507496107bff7  Download-WinDump.exe
4511ee3b4e5d8150c035a140dfba72c0  Download-WinPcap_3_1_beta_3.exe
[root@LinuxForensics GIAC]#
```

Screenshot-22, MD5 after cutting the downloaded image.

It is certain that the recovered WinDump.exe and downloaded WinDump.exe are the same copy, because they have the exact MD5 hash of – '79375b77975aa53a1b05074961076ff7'.

However, the downloaded WinPcap has different MD5 hash from recovered WinPcap. This is because the recovered WinPcap only contains the last 465330 bytes of data. Due to disk defragmentation, the first 20480 bytes of disk space were used by 'coffee.doc'.

To have an apple to apple comparison, we cut the first 20480 bytes of 'Download-WinPcap_3_1_beta_3.exe' using KHexEdit. The MD5 hash of the resulted file 'part-Download-WinPcap_3_1_beta_3.exe' is '70553e1c186284f46b46c9521bba629b', which is the same as that of the recovered 'part-WinPcap_3_1_beta_3.exe'. So to a certain degree, it can be stated that the original file that existed on this image was a copy of the original

WinPcap_3_1_beta_3.exe.

Legal implication

Based on collected evidence and current California statute, there are two violations in this incident; “Sexual Harassment’ and “Wiretap Act”.

Reference from: *California Law: Stalking, Harass Defined* http://lalabor.com/main/id/286.html#h
For the purposes of this section, "harasses" means engages in a knowing and willful course of conduct directed at a specific person that seriously alarms, annoys, torments, or terrorizes the person, and that serves no legitimate purpose.

Some particular example from *Sexual Harassment Definition (3): Verbal,* http://lalabor.com/main/id/122.html demonstrates the possible verbal & physical violation activities. From the spirit of the above definition, both aggressive email and capturing network traffic of Ms. Conlay are solid evidences of violation. The penalties that could be levied against the subject if he/she were convicted in court could be imprisonment in county jail for not more than one year, or by a fine of not more than one thousand dollars ($1,000), or by both that fine and imprisonment, or by imprisonment in the state prison.

Please note that application of this law requires willful intent on the part of the subject, which would need to be legally established alongside the course of conduct made plain from this analysis.

From the spirit of ‘18 U.S.C. §2511’, it is illegal to install any type of network sniffing program and use to capture private electric communication. Though there are three main exceptions: provider exception, consent of a party, and computer trespasser. However, Mr. Lawrence does not fall into any of them.

Summarized from 18 U.S.C. §2511 Wire and Electronic Communications Interception and Interception of Oral Communications. http://www.usdoj.gov/criminal/cybercrime/18usc2511.htm
Intentionally intercept, or endeavors to intercept any electric communication is considered violation, thus should be punished or should be subject to suit. The consequence for the convicted subject is fine or imprisoned not more than five years, or both.

Recommendations

Based on the media analysis results, I suggest the following actions:

- Follow the corporate Incident Response Policy, report the incident to HR

department, senior management, and company's attorney and legal counsel immediately.

- Carefully review employee handbook, make sure the policy regarding sexual harassment has been clearly stated and enough education has been given to employees. This may be evidence on the court to protect CC Terminals.

- Because of the criminal nature of this incident, need to consider reporting to local law enforcement. Involvement of local law enforcement will speed up the response time and better protect the company as well as Ms. Conlay.

- Perform a thorough investigation of Mr. Lawrence's computer. This could be the system where Mr. Lawrence launched the network sniffing program. The same system may have WinPcap_3_1_beta_3.exe library and Microsoft MapPoint application.

- Implement a tool to scan the network for NICs running in promiscuous mode to quickly identify sniffers and packet capture applications

- Implement a proxy sever to restrict and log internet access by internal computers or something to that affect.

Additional Information

[1] Brian Carrier, *TSK FAT File Recovery* http://www.sleuthkit.org/sleuthkit/docs/skins_fat.html

[2] Microsoft, *FAT32 File System Specification* http://www.microsoft.com/whdc/system/platform/firmware/fatgen.mspx

[3] *Sexual Harassment Definition (3): Verbal*, http://lalabor.com/main/id/122.html Examples of unacceptable verbal behaviors that may be in violation of the Organization's policy on sexual harassment

[4] *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, http://www.cybercrime.gov/s&smanual2002.htm * Guidelines for performing additional investigation on Mr. Lawrence's computer.

[5] Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited, <http://www.cybercrime.gov/usc2511.htm> US code concerning 'Wire, Oral, or Electronic Communication"

[6] Brian Carrier, *Splitting The Disk With mmls*, http://www.sleuthkit.org/informer/sleuthkit-informer-12.html, * Information regarding disk partition information and how to intercept mmls output.

Reference

[1] Brian Carrier , *Description of the FAT fsstat Output* http://www.Sleuthkit.org/informer/Sleuthkit-informer-18.html#fat

[2] Brian Carrier, *Autopsy description* http://www.Sleuthkit.org/autopsy/desc.php

[3] Brian Carrier, *File Activity Timelines*, http://www.sleuthkit.org/sleuthkit/docs/ref_timeline.html

[4] Brian Carrier, *Sleuth Kit,* http://www.sleuthkit.org/sleuthkit/desc.php

[5] *TCT tools*, http://www.fish.com/tct/, http://www.porcupine.org/forensics/tct.html

[6] Brian Carrier, *'dd' Acquisitions* http://www.Sleuthkit.org/informer/Sleuthkit-informer-11.html

[7] *What is Slack Space*, http://www.webopedia.com/TERM/S/slack_space.html

[8] *Ethereal User's Guide*, http://www.ethereal.com/docs/user-guide-sp/

[9] *ASCII code table*, http://www.lookuptables.com/

[10] ls – *standard Linux command to list directory contents.* http://www.ctssn.com/man/index.cgi?section=all&topic=ls

[11] md5sum - *compute and check MD5 message digest*. http://www.ctssn.com/man/index.cgi?section=all&topic=md5sum

[12] gunzip – *tool to decompress the gzip compressed file http://www.gzip.org/#intro*

[13] mmls – *part of Sleuth Kit, display image partition information*: http://www.Sleuthkit.org/Sleuthkit/man/mmls.html

[14] dd - *a tool that reads a block of data from an input file and writes it to an output file* http://www.ctssn.com/man/index.cgi?section=all&topic=dd

[15] fls - *Reference site for fls' detail:* http://www.Sleuthkit.org/Sleuthkit/man/fls.html

[16] lstat – *display meta layer info for a given inode:* http://www.Sleuthkit.org/Sleuthkit/man/istat.html

[17] icat - *capture content from all sectors that associated with the given inode*: http://www.Sleuthkit.org/Sleuthkit/man/icat.html

Appendix A Timeline.txt file

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

Appendix B MD5 value of all files.

File Name	MD5	Note
her.doc	9785a777c5286738f9deb73d8bc57978	
hey.doc	ca601d4f8138717dca4de07a8ec19ed1	
part-WinPcap_3_1_beta_3.exe	70553e1c186284f46b46c9521bba629b	
WinDump.exe	79375b77975aa53a1b0507496107bff7	
capture	2097b7b0a9fedb4238b67e976c4ae1cb	
map.gif	9bc3923cf8e72fd405d7cea8c8781011	
coffee.doc	a833c58689596eda15a27c931e0c76d1	
Download-WinPcap_3_1_beta_3.exe	4511ee3b4e5d8150c035a140dfba72c0	download from Internet
Part-Download-WinPcap_3_1_beta_3.exe	70553e1c186284f46b46c9521bba629b	download from Internet and cut the first 20480 bytes of data.
Download-WinDump.exe	79375b77975aa53a1b0507496107bff7	download from Internet

Appendix C Linux Commands & Tools MD5 value

```
# Standard Linux Commands & Tools      #
########################################
774cb14b70080573906bbd26df7a9c58  /bin/ls
1f3ebef14c6cddfb5558ceae5e07230c  /bin/mv
b9f61947f0d8c81439284cda8923e0cd  /usr/bin/md5sum
fd4da87b8e161766488bb906d336e050  /bin/cp
4ca39fa9c4c405ca0e31a9ec880b8f58  /bin/gunzip
fbb626479e56fd7d722eaa170717522a  /bin/dd
306c32091283c32426049d319cd06a16  /usr/bin/vmware
0a6cf17c411aa2e781bfcc6064490428  /usr/local/bin/autopsy
a0e8e279a22c75ffeacc1407ab4155c3  /bin/grep
6756949642336efe1fb32db1216932d0  /bin/cat
26d3d9daec310a7013afa9f86fba2a86  /usr/local/bin/strings

# Sleuth Kit Tools                     #
########################################
93f18736e2d24458833c017d12a62f5d  /usr/local/bin/ils
f623f3769c853397c5ac2dbfc3fb3446  /usr/local/bin/istat
4b9f0ac4f9b573c5cad87077b2d3fa88  /usr/local/bin/ifind
f321ce65d86c27e8e85e142f815f9fe5  /usr/local/bin/icat
881004cd5f9b7175e622b8207422c028  /usr/local/bin/dcat
74edd0489d645f22e3c1d85831cdd2f7  /usr/local/bin/dcalc
a516e76235f8e43dffe7f4a4357b5eba  /usr/local/bin/dls
32740f65e55f496595988e29987bca1d  /usr/local/bin/dstat
43f1f987603e7583d15317096a663d2a  /usr/local/bin/fsstat
4ba4977d6bd823ee2ac1f3ced954e5a4  /usr/local/bin/ffind
384c35beb41f9ae9715b4c136795f18a  /usr/local/bin/fls
e6b1cb8f2ea860e9c12694ae133a0e88  /usr/local/bin/mmls
```