GIAC Certified Forensic Analyst
GCFA

Practical Assignment
Version 2.0

Option 1:

Analyze a 64MB
Lexar Media
USB JumpDrive
Image

Submitted by:
Joseph Chen
January 12, 2005

Table of Content

Abstract

This report is prepared for GIAC Certified Forensic Analyst practical assignment version 2.0, Option #1; Analyze a 64MB Lexar Media USB JumpDrive Image.

It is a USB drive (image) collected from a company's internal incident related to a sexual harassment case. The USB drive is the only evidence collected that may have been related to this incident.

In the "Executive Summary" section of this report, all the findings are summarized according to the sequence of events. It provides an overview of the evidences found in normal English for readers to easily understand what has happened and what law was potentially violated.

In "Examination Detail" section of this report, all examination steps are listed in detail which include what tools were used during the investigation and explain step by step why the tools were used. It also discloses all the contents in the USB drive image, which includes the deleted and none-deleted files.

In the "Image Detail" section, all files' information are listed, which include the MD5 signature, the file size, the file owner for each file, as well as when the last access time was, when it was created and when it was written to the USB drive. The keywords found during the investigation are also listed.

The "Forensic Detail" section addresses what programs were used by the suspect, how he used those programs, when the suspect ran the programs and what program parameters were used during the incident.

In the "Program Identification" section of this report, the how-to has been demonstrated in order to prove the true identity of the recovered programs in this incident and the details about the program.

The "Legal Implications" section lists the potentially violated law, briefs the penalty and several exceptions for that law.

The "Recommendations" section lists several suggestions to the security administrator which include the security policy suggestions and potential follow-up actions.

The "Additional Information" section includes all resources available on the Internet for readers who are interested in learning more in depth related to this incident.

The last two sections, "List of references", lists all materials which were consulted when writing this report. And the "Appendix" section includes the timeline generated by Autopsy Forensics Browser for this incident.

1. Executive Summary

(Note: For privacy protection, all names have been replaced with “xxxx”, and I use name initials to represent the persons involved.)

The xxxx company’s security administrator Mr. M.M. has asked me to analyze a USB drive image he’s gotten from an internal security incident. He briefed me that on the afternoon of Friday Oct. 29, Ms. L.C. contacted corporate security, stating she was being harassed by Mr. R.L.. She stated that R.L. has made numerous attempts to meet her, both during and outside of work. She also stated that he has contacted her at her personal email address, and that his emails have become increasingly aggressive. On the evening of Thursday Oct. 28, Ms. L.C. was at a coffee shop with a friend when Mr. R.L. appeared. The next day she contacted corporate security. In the search of Mr. R.L.’s cubicle, it turned up this USB flash drive.

After my investigation, I found that Mr. R.L. used “Microsoft Word[1] 10.0 (MS Word 2002)” software to write a Word document named “`her.doc`” at 08:32, Oct. 25. It contains:

```
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
```

Then at 08:48, Oct. 26, Mr. R.L. used same program to write another Word document named “`hey.doc`”. It contains:

```
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?
```

At 16:23, Oct. 27, he downloaded[2] “`WinPcap_3_1_beta_3.exe`” file (from Internet[3]). It is a computer software “driver” used by the next file he downloaded at 16:24, Oct. 27 named “`WinDump.exe`”.

WinDump[4] is computer software which can do real-time eavesdropping (wiretapping) on the content of network communication. WinPcap[5] is the required windows-base Pcap (packet capture) “driver” for WinDump.

The “driver”[6] is “a piece of software that enables a computer to communicate

[1] Microsoft Word, A computer word processing software published by Microsoft. http://office.microsoft.com/en-us/FX010857991033.aspx

[2] Download, To transfer a file or files from one computer to another. http://www.netlingo.com/lookup.cfm?term=download

[3] Internet, http://www.netlingo.com/lookup.cfm?term=Internet

[4] WinDump, http://windump.polito.it/

[5] WinPcap, http://winpcap.polito.it/docs/docs31beta4/html/index.html

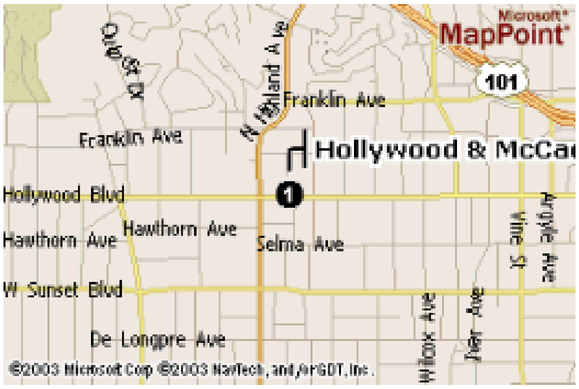
with a peripheral device".

At 11:08, Oct. 28, he captured an email sent by xxxx (Hotmail login name: xxxx) to xxxx@hotmail.com in a file call "`capture`". This email contains:

```
Subject: RE: coffee,
Sure, coffee sounds great.  Let's meet at the coffee shop on the corner Hollywood and
McCadden.  It's a nice out of the way spot.


See you at 7pm!


-xxxx.
```

(This wiretapping activity may violate the "Wiretap Act"[7], 18 U.S.C. §§ 2510-2522 if he is not qualified for the list of exceptions.)

After he got that email message, he went to Internet "MSN Maps and Directions" website, downloaded a map at 11:17, Oct. 28 and saved it as "`map.gif`" on the USB flash drive. It contains the following graphic:



It is a map that shows the area of Hollywood & McCadden, which was indicated in the email he captured.

At 19:24, Oct. 28, Mr. R.L. wrote another Word document named "`coffee.doc`". It contains:

```
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...
```

[6] Driver, http://dictionary.reference.com/search?q=driver

[7] Wiretap Act, SANS Institute, Track 8 – System Forensics, Investigation & Response, Volume 8.5 page 29~30, SANS Press, Nov-17~23, 2004. 18 U.S.C. §§ 2510-2522, UNITED STATES CODE ANNOTATED TITLE 18. CRIMES AND CRIMINAL PROCEDURE PART I--CRIMES CHAPTER 119--WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS. http://www.cybercrime.gov/wiretap2510_2522.htm

Base on all the findings and the statement Ms. L.C reported to Mr. M.M., it supported that the `her.doc, hey.doc,` and `coffee.doc` were sent to Ms. L.C. but I cannot prove it. However, I can prove these three files are created with Mr. R.L.'s identification within the hidden portion of document.

Microsoft Office (Word) 2000 and above has tracking mechanism to automatically keep tracking of who used it to save the document. This user information is the registered person that Microsoft Word was licensed to[8]. Base on this hidden information, at least we can say these three documents were saved by MS Word registered to Mr. R.L.

Also, another thing I can prove is he did eavesdrop Ms. L.C.'s email communication which may violate the "Wiretap Act", 18 U.S.C. §§ 2511[9] if he is not qualified for the exceptions.

2. Examination Details

Mr. M.M. is the security administrator at xxxx. He asked me to analyze a USB drive image and provide him with a report for my findings. He gave me an image with a chain of custody form with following information:

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

A disk "image"[10] is a copy of original evidence generally collected by a tool that performs bit-level copying from one location to another.

After I got this image, I brought up my forensics workstation. It is a fresh installed Fedora Core 2, loaded with static-built forensics response-kit I got from SANS Golden Gate 2004 Track 8 System Forensics, Investigation & Response Class[11] . Inside the Track 8 CD, it contains several static-built open source Linux/Win2K_XP tools and Sleuth Kit forensics tools in response kit. For more detail of these tools, please refer to the last paragraph "Additional Information".

After I got the USB image file `USBFD-64531026-RL-001.img`, I ran a MD5 checksum against that image to make sure it was not altered. The tool used

[8] SANS Institute, Track 8 – System Forensics, Investigation & Response, Volume 8.4 page 109~112, SANS Press, 17~23 Nov. 2004.

[9] 18 U.S.C. 2511. Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited. 5 Jan. 2005 <http://www.cybercrime.gov/usc2511.htm>

[10] Image, SANS Institute, Track 8 – System Forensics, Investigation & Response, Volume 8.1 page 17, SANS Press. 17~23 Nov. 2004

[11] Response-kit, SANS Institute, Track 8 – System Forensics, Investigation & Response, CD, SANS Press. 17~23 Nov. 2004.

was md5sum[12] from my response toolkit.

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

After I have made sure that the image file I got is exactly the same as the image shown on the chain of custody form. I used the file[13] tool to exam the content type.

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

The image is a x86 boot sector, which means it is a physical drive image, In order to find out the file system partition on that physical drive image, I used mmls[14] with -t dos option (All x86 base system use the DOS type) to find the partition tables:

```
[root@LinuxForensics]# 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)
```

From the DOS partition table, I found that it is a DOS FAT16[15] file system partition starting from the sector #32 with length of 121,919 sectors and each sector contains 512 bytes. I used the tool dd[16] to extract out the DOS FAT16 logical partition and ran md5sum to get the MD5 checksum for that FAT16 partition image:

```
[root@LinuxForensics]# dd if=USBFD-64531026-RL-001.img bs=512 skip=32 count=121919
of=usbfat16.img
121919+0 records in
121919+0 records out
[root@LinuxForensics]# md5sum usbfat16.img
5f830a763e2144483f78113a8844ad52  usbfat16.img
```

After I got the FAT16 partition image, I used the file tool again to exam the content and verify the extraction.

```
[root@LinuxForensics]# file usbfat16.img
usbfat16.img: x86 boot sector, code offset 0x3c, OEM-ID "MSWIN4.1", sectors/cluster 2,
root entries 512, Media descriptor 0xf8, sectors/FAT 239, heads 17, hidden sectors 32,
sectors 121919 (volumes > 32 MB) , serial number 0x0, unlabeled, FAT (16 bit)
```

After I verified the FAT16 partition image, I used another tool fsstat[17] to find the

[12] md5sum manual, http://www.gnu.org/software/coreutils/manual/html_chapter/coreutils_6.html#SEC26

[13] file, SANS Institute, Track 8 – System Forensics, Investigation & Response, Volume 8.2/8.3 page 114, SANS Press, 17~23 Nov. 2004.

[14] mmls, http://www.sleuthkit.org/sleuthkit/man/mmls.html

[15] FAT16, http://www.pcwebopedia.com/TERM/F/file_allocation_table_FAT.html, http://www.microsoft.com/resources/documentation/windows/98/all/reskit/en-us/part2/wrkc10.mspx

[16] dd, http://www.gnu.org/software/coreutils/manual/html_chapter/coreutils_11.html#IDX793

file system information:

```
[root@LinuxForensics]# fsstat -f fat16 usbfat16.img
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: FAT

OEM Name: MSWIN4.1
Volume ID: 0x0
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory):
File System Type Label: FAT16

Sectors before file system: 32

File System Layout (in sectors)
Total Range: 0 - 121918
* Reserved: 0 - 0
** Boot Sector: 0
* FAT 0: 1 - 239
* FAT 1: 240 - 478
* Data Area: 479 - 121918
** Root Directory: 479 - 510
** Cluster Area: 511 - 121918

METADATA INFORMATION
--------------------------------------------
Range: 2 - 1942530
Root Directory: 2

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 1024
Total Cluster Range: 2 - 60705

FAT CONTENTS (in sectors)
--------------------------------------------
511-550 (40) -> EOF
551-590 (40) -> EOF
591-630 (40) -> EOF
```

From the `fsstat` output, I found the FAT cluster[18] size is 1024-byte with 512-byte in the sector size, which means the minimum storage size is 1024-byte even when file is less than 512-bytes[19]. The storage block incremental is 1024-byte. The Root directory is at cluster #2.

I used `fls`[20] to find out what file names were stored in the root directory (cluster # 2). This `fls` tool can display the filename stored under root directory. If the file was deleted, it indicated with a * mark.

```
[root@LinuxForensics]# fls -f fat16 usbfat16.img 2
r/r 3:  her.doc
r/r 4:  hey.doc
r/r * 7:        WinPcap_3_1_beta_3.exe (_INPCA~1.EXE)
```

[17] fsstat, http://www.sleuthkit.org/sleuthkit/man/fsstat.html
[18] cluster, http://www.pcwebopedia.com/TERM/c/cluster.html
[19] http://www.pcwebopedia.com/TERM/S/slack_space.html The unused space between the end-of-file to end-of-cluster call "slack space". Only Windows file system has slack space, Linux/Unix file system will pad to end of fragment (Linux fragment call inode, Windows fragment call cluster)
[20] fls, http://www.sleuthkit.org/sleuthkit/man/fls.html

```
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
```

From the `fls` output, I found four files were deleted: `WinPcap_3_1_beta_3.exe`, `WinDump.exe`, `_apture`, `_ap.gif`.

After I got this basic information, I used Autopsy Forensics Browser[21] from SleuthKit.org to generate the timeline[22] and for file recovery.

From Autopsy, I generated a report for `WinDump.exe` and recovered back the deleted file "`WinDump.exe`".

```
                 Autopsy Dir Entry Report

--------------------------------------------------------------
                    GENERAL INFORMATION

Dir Entry: 14
Pointed to by file(s):
  E:\WinDump.exe (_INDUMP.EXE) (deleted)
MD5 of istat output: 2b89bf93a2d3f549602f3b4478ecba76
SHA-1 of istat output: 53f91755e82b3c39e4f84e38fb85fb143700e9b5

Image: /forensics/CC-Terminals/USB/images/usbfat16.img
Image Type: fat16

Date Generated: Wed Dec 29 02:10:42 2004
Investigator: JosephChen

--------------------------------------------------------------
                   META DATA INFORMATION

Directory Entry: 14
Not Allocated
File Attributes: File, Archive
Size: 450560
Num of links: 0
Name: _INDUMP.EXE

Directory Entry Times:
Written:       Wed Oct 27 16:24:02 2004
Accessed:      Thu Oct 28 00:00:00 2004
Created:       Wed Oct 27 16:24:04 2004

Sectors:
1541 1542

Recovery:
1541 1542 1543 1544 1545 1546 1547 1548
1549 1550 1551 1552 1553 1554 1555 1556
1557 1558 1559 1560 1561 1562 1563 1564
1565 1566 1567 1568 1569 1570 1571 1572
1573 1574 1575 1576 1577 1578 1579 1580
…………
…………
```

[21] Autopsy Forensics Browser, http://www.sleuthkit.org/autopsy/index.php
[22] Timeline, you can find the timeline at appendix.

```
2397 2398 2399 2400 2401 2402 2403 2404
2405 2406 2407 2408 2409 2410 2411 2412
2413 2414 2415 2416 2417 2418 2419 2420

File Type: MS-DOS executable (EXE), OS/2 or MS Windows

--------------------------------------------------------------
                   VERSION INFORMATION

Autopsy Version: 2.03
The Sleuth Kit Version: 1.72
```

Then, I ran `md5sum` for its MD5 signature.

```
[root@LinuxForensics]# md5sum WinDump.exe
79375b77975aa53a1b0507496107bff7  WinDump.exe
```

After I recovered the `WinDump.exe` successfully, I try to use the Autopsy again to recover the `WinPcap_3_1_beta_3.exe` file; I found it reported using the sector number 591 to 630 with file size 485,810 bytes. But it did not make sense to store 485,810 bytes of data in a total of (512 x 40=) 20,480 bytes storage area. I also found the sectors #591 to 630 are occupied by `coffee.doc` file and the file size is 19,968 bytes.

```
                 Autopsy Dir Entry Report

--------------------------------------------------------------
                    GENERAL INFORMATION

Dir Entry: 10
Pointed to by file(s):
  E:\WinPcap_3_1_beta_3.exe (_INPCA~1.EXE) (deleted)
MD5 of istat output: 653868dca52612e564b7b4d720330cf3
SHA-1 of istat output: 7e851b1d34db7bcf71c7078420fcff44f382cb08

Image: /forensics/CC-Terminals/USB/images/usbfat16.img
Image Type: fat16

Date Generated: Wed Dec 29 21:27:43 2004
Investigator: JosephChen

--------------------------------------------------------------
                   META DATA INFORMATION

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

File Type: empty

--------------------------------------------------------------
                   VERSION INFORMATION

Autopsy Version: 2.03
The Sleuth Kit Version: 1.72


                 Autopsy Dir Entry Report

--------------------------------------------------------------
                    GENERAL INFORMATION

Dir Entry: 18
Pointed to by file(s):
  E:\coffee.doc
MD5 of istat output: caa90dbb46b2e831e66b0ce434b2fe4c
SHA-1 of istat output: 0123fc5d7f4059f9dc9c2b3815b342043cfb1d2e

Image: /forensics/CC-Terminals/USB/images/usbfat16.img
Image Type: fat16

Date Generated: Wed Dec 29 21:29:56 2004
Investigator: JosephChen

--------------------------------------------------------------
                   META DATA INFORMATION

Directory Entry: 18
Allocated
File Attributes: File, Archive
Size: 19968
Num of links: 1
Name: coffee.doc

Directory Entry Times:
Written:       Thu Oct 28 19:24:48 2004
Accessed:      Thu Oct 28 00:00:00 2004
Created:       Thu Oct 28 19:24:46 2004

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

File Type: Microsoft Office Document

--------------------------------------------------------------
                   VERSION INFORMATION

Autopsy Version: 2.03
The Sleuth Kit Version: 1.72
```

This tells me I lost the data stored in sector 591 to 630, which had been overwritten by the new `coffee.doc` file. I calculated 485,810 bytes should use 475 clusters (which equals 950 sectors). It should start from sector #591 to 1540. The sectors #591 to 630 have been overwritten. However, the sectors

#631 to 1540 are still unallocated which indicates that the rest of the file is still recoverable from those unallocated sectors. I used `dd` to extract sectors #591 to 1540 (total 950 sectors, 475 clusters, 486,400 bytes) from `usbfat16.img` to a file named `recover_WinPcap_3_1_beta_3.exe.raw`. After I extracted this file, I used Hex Editor `khexedit` [23] to strip out the 485,811-byte to 486,400-byte (which are extra bytes, slack space) and first 20,480 bytes (those 40 sectors are used by the `coffee.doc` file.) out of `recover_WinPcap_3_1_beta_3.exe.raw` file and saved as `last_910_of_recover_WinPcap_3_1_beta_3.exe.raw` and ran `md5sum` against it for MD5 signature.

```
[root@LinuxForensics]# dd if=usbfat16.img of=recover_WinPcap_3_1_beta_3.exe.raw bs=512
skip=591 count=950
950+0 records in
950+0 records out

[root@LinuxForensics]# md5sum last_910_of_recover-WinPcap_3_1_beta_3.exe.raw
70553e1c186284f46b46c9521bba629b  last_910_of_recover-WinPcap_3_1_beta_3.exe.raw
```

After that, I used the Autopsy to recover rest of `_apture` and `_ap.gif` file. On the `Autopsy Dir Entry Report` for `_apture`, it shows `File Type: tcpdump capture file (little-endian) - version 2.4 (Ethernet, capture length 4096)` which indicated it is some network traffic captured by the WinDump, so I recovered it and saved as “`capture`”.

```
                 Autopsy Dir Entry Report

--------------------------------------------------------------
                    GENERAL INFORMATION

Dir Entry: 15
Pointed to by file(s):
  E:\_apture (deleted)
MD5 of istat output: e30f70844d3a47cef1de85553fa31654
SHA-1 of istat output: a46bbb1364712cc4a8364ab8d9447caa08cfbd80

Image: /forensics/CC-Terminals/USB/images/usbfat16.img
Image Type: fat16

Date Generated: Wed Dec 29 02:11:30 2004
Investigator: JosephChen

--------------------------------------------------------------
                   META DATA INFORMATION

Directory Entry: 15
Not Allocated
File Attributes: File, Archive
Size: 53056
Num of links: 0
Name: _apture

Directory Entry Times:
Written:       Thu Oct 28 11:11:00 2004
Accessed:      Thu Oct 28 00:00:00 2004
Created:       Thu Oct 28 11:08:24 2004

Sectors:
```

[23] Hex Editor, khexedit, http://home.online.no/~espensa/khexedit/

```
2421 2422

Recovery:
2421 2422 2423 2424 2425 2426 2427 2428
2429 2430 2431 2432 2433 2434 2435 2436
2437 2438 2439 2440 2441 2442 2443 2444
2445 2446 2447 2448 2449 2450 2451 2452
2453 2454 2455 2456 2457 2458 2459 2460
2461 2462 2463 2464 2465 2466 2467 2468
2469 2470 2471 2472 2473 2474 2475 2476
2477 2478 2479 2480 2481 2482 2483 2484
2485 2486 2487 2488 2489 2490 2491 2492
2493 2494 2495 2496 2497 2498 2499 2500
2501 2502 2503 2504 2505 2506 2507 2508
2509 2510 2511 2512 2513 2514 2515 2516
2517 2518 2519 2520 2521 2522 2523 2524

File Type: tcpdump capture file (little-endian) - version 2.4 (Ethernet, capture length
4096)

--------------------------------------------------------------
                   VERSION INFORMATION

Autopsy Version: 2.03
The Sleuth Kit Version: 1.72
```

I used `Ethereal`[24] to read the content of `capture` file. In the `capture` file, I found Mr. R.L. captured one email Ms. L.C. (Hotmail login ID: xxxxx) sent to xxxxx@hotmail.com .

```
Subject: RE: coffee,
Sure, coffee sounds great.  Let’s meet at the coffee shop on the corner Hollywood and
McCadden.  It’s a nice out of the way spot.


See you at 7pm!


-xxxx.
```

I used the `strings`[25] tool against the `capture` file and `grep`[26] for `coffee` to get this string.

```
[root@LinuxForensics]# strings capture | grep -i coffee
curmbox=F000000001&HrsTest=&_HMaction=Send&FinalDest=&subaction=&plaintext=&login=xxxx&msg
=&start=&len=&attfile=&attlistfile=&eurl=&type=&src=&ref=&ru=&msghdrid=b16479b18beec291196
189c78555223c_1098692452&RTEbgcolor=&encodedto=xxxx@hotmail.com&encodedcc=&encodedbcc=&del
eteUponSend=0&importance=&sigflag=&newmail=new&to=xxxx@hotmail.com&cc=&bcc=&subject=RE%3A+
coffee&body=Sure%2C+coffee+sounds+great.++Let%27s+meet+at+the+coffee+shop+on+the+corner+Ho
llywood+and+McCadden.++It%27s+a+nice+out+of+the+way+spot.%0D%0A%0D%0ASee+you+at+7pm%21%0D%
0A%0D%0A-xxxx.6
[root@LinuxForensics]#
```

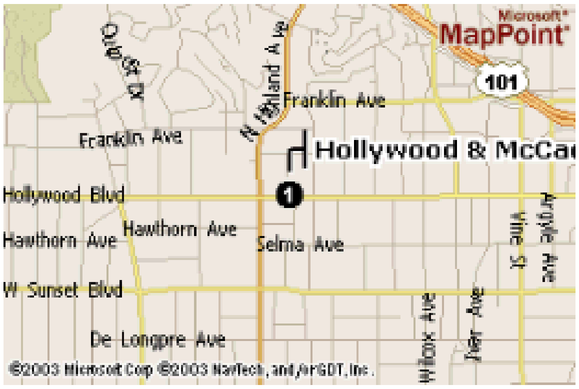
On the Autopsy report for `_ap.gif`, it is indicated as a GIF image data. So I recovered it and saved it as “`_ap.gif`”. Then use the Mozilla[27] web browser to

[24] Ethereal, an open source network protocol analyzer, http://www.ethereal.com/
[25] strings, SANS Institute, Track 8 – System Forensics, Investigation & Response, Volume 8.1. page 10. SANS Press, 17~23 Nov. 2004.
[26] grep, http://www.gnu.org/software/grep/doc/
[27] Mozilla web browser, the new version has been renamed to Firefox 1.0 http://www.mozilla.org/

view the GIF image.

```
                 Autopsy Dir Entry Report

--------------------------------------------------------------
                    GENERAL INFORMATION

Dir Entry: 17
Pointed to by file(s):
  E:\_ap.gif (deleted)
MD5 of istat output: feda4575d94bda7327908bae4d53fbe2
SHA-1 of istat output: 731c559f6d97c1d63d7bcb9a6e6b4bd6b4fba121

Image: /forensics/CC-Terminals/USB/images/usbfat16.img
Image Type: fat16

Date Generated: Wed Dec 29 02:12:34 2004
Investigator: JosephChen

--------------------------------------------------------------
                   META DATA INFORMATION

Directory Entry: 17
Not Allocated
File Attributes: File, Archive
Size: 8814
Num of links: 0
Name: _ap.gif

Directory Entry Times:
Written:       Thu Oct 28 11:17:46 2004
Accessed:      Thu Oct 28 00:00:00 2004
Created:       Thu Oct 28 11:17:44 2004

Sectors:
2525 2526

Recovery:
2525 2526 2527 2528 2529 2530 2531 2532
2533 2534 2535 2536 2537 2538 2539 2540
2541 2542

File Type: GIF image data, version 89a, 300 x 200

--------------------------------------------------------------
                   VERSION INFORMATION

Autopsy Version: 2.03
The Sleuth Kit Version: 1.72
```

The recovered `_ap.gif` show as below, so I believed the original file name should be “`map.gif`”.



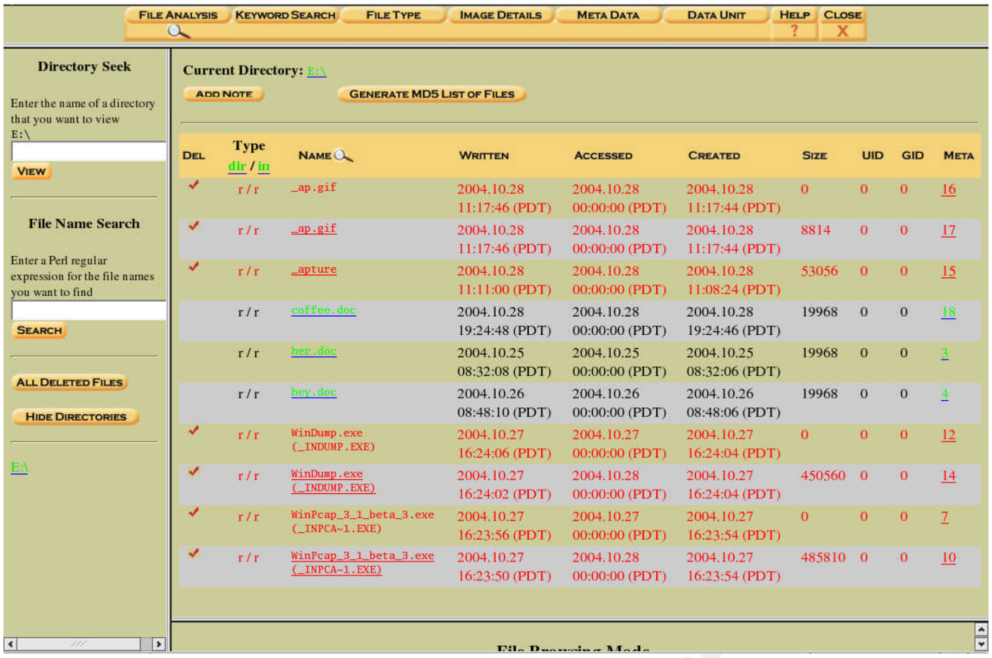
The last file on the USB image is "`coffee.doc`". Here is the content:

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

After all these investigations and according to what Ms. L.C. reported to Mr. M.M., one thing we can confirm is that Mr. R.L. did wiretap Ms. L.C.'s email communication and found out the 7:00pm appointment at the coffee shop. He then searched the MSN map to get the location of that coffee shop, and went there before 7:00pm on Oct. 28. After he saw Ms. L.C at coffee shop, he wrote her an email which is the "`coffee.doc`" after 19:24, Oct. 28 to Ms. L.C.

3. Image Details

By using `fls` tool with `-l` switch, we can get a list of files in the image `usbfat16.img` or from Autopsy's `FILE ANALYSIS` tab.



Current Directory: E:\

Del	Type dir / in	Name	Written	Accessed	Created	Size	UID	GID	Meta
✓	r / r	_ap.gif	2004.10.28 11:17:46 (PDT)	2004.10.28 00:00:00 (PDT)	2004.10.28 11:17:44 (PDT)	0	0	0	16
✓	r / r	_ap.gif	2004.10.28 11:17:46 (PDT)	2004.10.28 00:00:00 (PDT)	2004.10.28 11:17:44 (PDT)	8814	0	0	17
✓	r / r	_apture	2004.10.28 11:11:00 (PDT)	2004.10.28 00:00:00 (PDT)	2004.10.28 11:08:24 (PDT)	53056	0	0	15
	r / r	coffee.doc	2004.10.28 19:24:48 (PDT)	2004.10.28 00:00:00 (PDT)	2004.10.28 19:24:46 (PDT)	19968	0	0	18
	r / r	her.doc	2004.10.25 08:32:08 (PDT)	2004.10.25 00:00:00 (PDT)	2004.10.25 08:32:06 (PDT)	19968	0	0	3
	r / r	hey.doc	2004.10.26 08:48:10 (PDT)	2004.10.26 00:00:00 (PDT)	2004.10.26 08:48:06 (PDT)	19968	0	0	4
✓	r / r	WinDump.exe (_INDUMP.EXE)	2004.10.27 16:24:06 (PDT)	2004.10.27 00:00:00 (PDT)	2004.10.27 16:24:04 (PDT)	0	0	0	12
✓	r / r	WinDump.exe (_INDUMP.EXE)	2004.10.27 16:24:02 (PDT)	2004.10.28 00:00:00 (PDT)	2004.10.27 16:24:04 (PDT)	450560	0	0	14
✓	r / r	WinPcap_3_1_beta_3.exe (_INPCA~1.EXE)	2004.10.27 16:23:56 (PDT)	2004.10.27 00:00:00 (PDT)	2004.10.27 16:23:54 (PDT)	0	0	0	7
✓	r / r	WinPcap_3_1_beta_3.exe (_INPCA~1.EXE)	2004.10.27 16:23:50 (PDT)	2004.10.28 00:00:00 (PDT)	2004.10.27 16:23:54 (PDT)	485810	0	0	10

```
[root@LinuxForensics]# fls -f fat -l usbfat16.img
r/r 3:  her.doc 2004.10.25 08:32:08 (PDT)       2004.10.25 00:00:00 (PDT)       2004.10.25
08:32:06 (PDT)       19968    0       0
r/r 4:  hey.doc 2004.10.26 08:48:10 (PDT)       2004.10.26 00:00:00 (PDT)       2004.10.26
08:48:06 (PDT)       19968    0       0
r/r * 7:        WinPcap_3_1_beta_3.exe (_INPCA~1.EXE)    2004.10.27 16:23:56 (PDT)
2004.10.27 00:00:00 (PDT)       2004.10.27 16:23:54 (PDT)       0       0       0
r/r * 10:       WinPcap_3_1_beta_3.exe (_INPCA~1.EXE)    2004.10.27 16:23:50 (PDT)
2004.10.28 00:00:00 (PDT)       2004.10.27 16:23:54 (PDT)       485810  0       0
r/r * 12:       WinDump.exe (_INDUMP.EXE)       2004.10.27 16:24:06 (PDT)       2004.10.27
00:00:00 (PDT)       2004.10.27 16:24:04 (PDT)       0       0       0
r/r * 14:       WinDump.exe (_INDUMP.EXE)       2004.10.27 16:24:02 (PDT)       2004.10.28
00:00:00 (PDT)       2004.10.27 16:24:04 (PDT)       450560  0       0
r/r * 15:       _apture 2004.10.28 11:11:00 (PDT)       2004.10.28 00:00:00 (PDT)
2004.10.28 11:08:24 (PDT)       53056   0       0
r/r * 16:       _ap.gif 2004.10.28 11:17:46 (PDT)       2004.10.28 00:00:00 (PDT)
2004.10.28 11:17:44 (PDT)       0       0       0
r/r * 17:       _ap.gif 2004.10.28 11:17:46 (PDT)       2004.10.28 00:00:00 (PDT)
2004.10.28 11:17:44 (PDT)       8814    0       0
r/r 18: coffee.doc      2004.10.28 19:24:48 (PDT)       2004.10.28 00:00:00 (PDT)
2004.10.28 19:24:46 (PDT)       19968   0       0
```

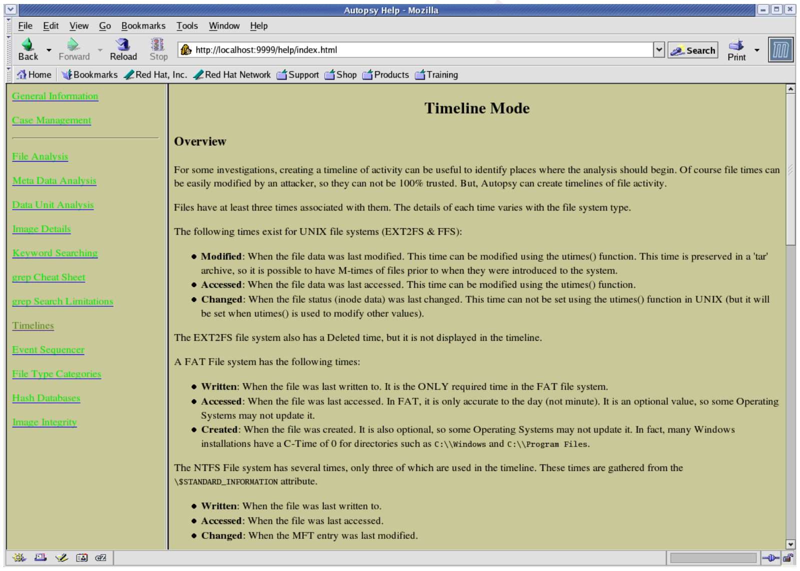
On the `fls -l` output, the meaning for the format of output data "`r/r * 10: WinPcap_3_1_beta_3.exe (_INPCA~1.EXE)   2004.10.27 16:23:50 (PDT) 2004.10.28 00:00:00 (PDT)      2004.10.27 16:23:54 (PDT) 485810  0       0`" as following:

1. r/r: first "r" is the type according to the directory entry and the second "r" is the type according to metadata structure. Normally these two should be the same.
2. *: indicates it is a deleted file (entry).
3. 10: indicates it is stored in "metadata entry[28]" #10.

[28] The Metadata structure in FAT file system call "Directory Entry". Every single file store in FAT file system has one entry in the "Root Directory".

4. WinPcap_3_1_beta_3.exe: the associated “File Name”.
5. 2004.12.27 16:23:50 (PDT): indicates the last “Written Time” (M-time). This column is the only required value by the FAT file system’s specification. It shows the last time when the file was written to system.
6. 2004.10.28 00:00:00 (PDT): indicates the last “Access Time” (A-time). This time is optional and is only accurate to the day, not to the hours or seconds on the FAT file system.
7. 2004.10.27 16:23:54 (PDT): indicates the “Created Time” (C-time) in FAT file system. It is the time when the file was created. It is an optional value according to the FAT file system’s specification.
8. 485810: indicates the “File Size”. If it is “0” no link will be shown with the name.
9. 0: indicates the “UID”, User ID of the file owner. “0” normally means the user “root” in Unix system.
10. 0: indicates the “GID”, Group ID for the file owner. “0” normally means the group “root” in Unix system.

As we can see, all the “Access Time” entries above show the date with 00:00:00 timestamp. This is due to the FAT file system’s limitation. The Autopsy Online Help Timeline page and the File Analysis page explain how the FAT file system handles the time stamp and how the Autopsy Forensic Browser displays the output.[29]



Timeline Mode

Overview

For some investigations, creating a timeline of activity can be useful to identify places where the analysis should begin. Of course file times can be easily modified by an attacker, so they can not be 100% trusted. But, Autopsy can create timelines of file activity.

Files have at least three times associated with them. The details of each time varies with the file system type.

The following times exist for UNIX file systems (EXT2FS & FFS):

- **Modified**: When the file data was last modified. This time can be modified using the utimes() function. This time is preserved in a 'tar' archive, so it is possible to have M-times of files prior to when they were introduced to the system.
- **Accessed**: When the file data was last accessed. This time can be modified using the utimes() function.
- **Changed**: When the file status (inode data) was last changed. This time can not be set using the utimes() function in UNIX (but it will be set when utimes() is used to modify other values).

The EXT2FS file system also has a Deleted time, but it is not displayed in the timeline.

A FAT File system has the following times:

- **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, so some Operating Systems may not update it. In fact, many Windows installations have a C-Time of 0 for directories such as `C:\\Windows` and `C:\\Program Files`.

The NTFS File system has several times, only three of which are used in the timeline. These times are gathered from the `\$STANDARD_INFORMATION` attribute.

- **Written**: When the file was last written to.
- **Accessed**: When the file was last accessed.
- **Changed**: When the MFT entry was last modified.

Also, on the Autopsy `FILE ANALYSIS` screenshot or `fls -l` output, we can see all files’ UID and GID are “0”. The UID=0 and GID=0 is due to the missing security (permission) information on FAT file system.

Below is the list of MD5 signature for each file:

[29] Autopsy Forensic Browser 2.03 Online help manual

her.doc:	9785a777c5286738f9deb73d8bc57978
hey.doc:	ca601d4f8138717dca4de07a8ec19ed1
coffee.doc:	a833c58689596eda15a27c931e0c76d1
capture:	2097b7b0a9fedb4238b67e976c4ae1cb
map:	9bc3923cf8e72fd405d7cea8c8781011
WinDump.exe:	79375b77975aa53a1b0507496107bff7
Original WinPcap_3_1_beta_3.exe:	4511ee3b4e5d8150c035a140dfba72c0
Recovered part of WinPcap_3_1_beta_3.exe:	70553e1c186284f46b46c9521bba629b

```
[root@LinuxForensics]# md5sum her.doc
9785a777c5286738f9deb73d8bc57978  her.doc
[root@LinuxForensics]# md5sum hey.doc
ca601d4f8138717dca4de07a8ec19ed1  hey.doc
[root@LinuxForensics]# md5sum coffee.doc
a833c58689596eda15a27c931e0c76d1  coffee.doc
[root@LinuxForensics]# md5sum capture
2097b7b0a9fedb4238b67e976c4ae1cb  capture
[root@LinuxForensics]# md5sum map.gif
9bc3923cf8e72fd405d7cea8c8781011  map.gif
[root@LinuxForensics]# md5sum WinDump.exe
79375b77975aa53a1b0507496107bff7  WinDump.exe
[root@LinuxForensics]# md5sum DL-WinPcap_3_1_beta_3.exe
4511ee3b4e5d8150c035a140dfba72c0  DL-WinPcap_3_1_beta_3.exe
[root@LinuxForensics]# md5sum last_910_of_recover-WinPcap_3_1_beta_3.exe.raw
70553e1c186284f46b46c9521bba629b  last_910_of_recover-WinPcap_3_1_beta_3.exe.raw
```

Below is the key words found in the files:

```
[root@LinuxForensics]# strings her.doc
bjbj
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
Hey I saw you the other day
Xxxxxxxx (Mr. R.L.'s name)
Normal.dot
Xxxxxxxx (Mr. R.L.'s name)
Microsoft Word 10.0
Hey I saw you the other day
Title
Microsoft Word Document
MSWordDoc
Word.Document.8
```

```
[root@LinuxForensics]# strings hey.doc
bjbj
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?
Xxxxxxxx (Mr. R.L.'s name)
Normal.dot
Xxxxxxxx (Mr. R.L.'s name)
Microsoft Word 10.0
Title
Microsoft Word Document
```

```
MSWordDoc
Word.Document.8


[root@LinuxForensics]# strings coffee.doc
bjbj
E_u^
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...
Hey what gives
Xxxxxxxx (Mr. R.L.'s name)
Normal.dot
Xxxxxxxx (Mr. R.L.'s name)
Microsoft Word 10.0
Hey what gives
Title
`eu^
Microsoft Word Document
MSWordDoc
Word.Document.8


[root@LinuxForensics]# strings capture |grep coffee
curmbox=F000000001&HrsTest=&_HMaction=Send&FinalDest=&subaction=&plaintext=&login=xxx&msg=
&start=&len=&attfile=&attlistfile=&eurl=&type=&src=&ref=&ru=&msghdrid=b16479b18beec2911961
89c78555223c_1098692452&RTEbgcolor=&encodedto=xxxx@hotmail.com&encodedcc=&encodedbcc=&dele
teUponSend=0&importance=&sigflag=&newmail=new&to=xxxx@hotmail.com&cc=&bcc=&subject=RE%3A+c
offee&body=Sure%2C+coffee+sounds+great.++Let%27s+meet+at+the+coffee+shop+on+the+corner+Hol
lywood+and+McCadden.++It%27s+a+nice+out+of+the+way+spot.%0D%0A%0D%0ASee+you+at+7pm%21%0D%0
A%0D%0A-xxxx.6
[root@LinuxForensics]#

[root@LinuxForensics]# strings usbfat16.img | grep coffee
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?
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...
curmbox=F000000001&HrsTest=&_HMaction=Send&FinalDest=&subaction=&plaintext=&login=xxxx&msg
=&start=&len=&attfile=&attlistfile=&eurl=&type=&src=&ref=&ru=&msghdrid=b16479b18beec291196
189c78555223c_1098692452&RTEbgcolor=&encodedto=xxxx@hotmail.com&encodedcc=&encodedbcc=&del
eteUponSend=0&importance=&sigflag=&newmail=new&to=xxxx@hotmail.com&cc=&bcc=&subject=RE%3A+
coffee&body=Sure%2C+coffee+sounds+great.++Let%27s+meet+at+the+coffee+shop+on+the+corner+Ho
llywood+and+McCadden.++It%27s+a+nice+out+of+the+way+spot.%0D%0A%0D%0ASee+you+at+7pm%21%0D%
0A%0D%0A-xxxx.6
[root@LinuxForensics]#
```

4. Forensic Details

As addressed in the “Examination Details” section, I recovered the program used by Mr. R.L. “`WinDump.exe`“. I used the Google Internet search engine to find more information about WinDump and I found the WinPcap is a required component to run the WinDump. Because I did not fully recover the

"`WinPcap_3_1_beta_3.exe`", so I try to get the same WinPcap version as shown on the file name "version 3.1 beta 3" from the Internet. I was able to download the "`WinPcap_3_1_beta_3.exe`" from following URL[30]: ftp://gd.tuwien.ac.at/infosys/security/polito.it/winpcap/WinPcap_3_1_beta_3.exe. It is one of the mirrors sites for WinPcap project.

WinDump is an open source network sniffer[31] program used to capture data packet over the network wire. WinPcap is a packet capturing driver which is required by running WinDump.

From the timeline, we can see that at 16:23, Oct. 27, Mr. R.L. downloaded the `WinPcap_3_1_beta_3.exe`, and then he downloaded the `WinDump.exe` at 16:24, Oct. 27. After he downloaded these two files, he installed the WinPcap and ran the WinDump without –w switch sometime during Oct 27. (He might ran `WinDump -D` to get a list of interface name on his system. And/or captured the packets and output to screen to make sure that the program ran as expected.) The exact access time is not available; this is due to the fact that the FAT file system timestamp is only required when the file is written (M-time) to the system. The last accessed time (A-time) is optional and is only accurate to the day (not to the minute). The file deleted time is not available in FAT file system timestamp.

At 11:08, Oct. 28, Mr. R.L. started the `WinDump` with `-w capture host 192.168.2.104` to sniff traffic associated with 192.168.2.104 and save the captured packets to file name "`capture`".

The WinDump program syntax with switches[32]:

```
windump [ -aBdDeflnNOpqRStvxX ] [ -c count ] [ -F file ]

         [ -i interface ] [ -m module ] [ -r file ]

         [ -s snaplen ] [ -T type ] [ -w file ]

         [ -E algo:secret ] [ expression ]
```

```
Win32 specific extensions
-B Set driver's buffer size to size in KiloBytes. The default buffer size is 1 megabyte
    (i.e. 1000). If there is any loss of packets during the capture, the suggestion is to
    increase the kernel buffer size by means of this switch, since the dimension of the
    driver's buffer influences heavily the capture performance.
-D Print the list of the interface cards available on the system. For every network
adapter, this switch returns the number, the name and the description. The user can start
the capture on a specific adapter typing  'WinDump -i name' or 'WinDump -i number'. If the
machine has more than one network adapter, WinDump without parameters starts on the first
network interface available on the system.

-w  Write the raw packets to file rather than parsing and printing them out. They can
    later be printed with the -r option. Standard output is used if file is ``-''.
```

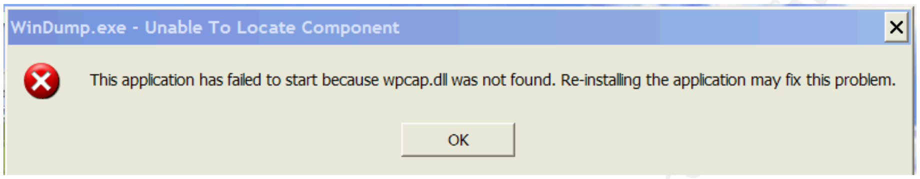
[30] URL. Uniform Resource Locator, http://www.pcwebopedia.com/TERM/U/URL.html

[31] Sniffer, a computer software program use to intercept the network communication.

[32] WinDump manual, http://windump.polito.it/docs/manual.htm

```
Example:
C:\>windump -D
1.\Device\NPF_GenericNdisWanAdapter (Generic NdisWan adapter)
2.\Device\NPF_{F0A27EB6-4FB2-4DF8-A18D-80BD0D749249} (b57w2k1 Broadcom NetXtreme Gigabit
Ethernet Driver)
3.\Device\NPF_{32C0344A-A27D-404E-84BB-934B16F1ECFD} (VMware Virtual Ethernet Adapter)
4.\Device\NPF_{A815FFD0-C77E-43F4-A154-E2EA78ED55DC} (w22n5110 Intel(R) PRO/Wireless
2200BG Network Connection)
5.\Device\NPF_{21399FEA-790D-4F55-9404-5BB0C4A9B177} (VMware Virtual Ethernet Adapter)
6.\Device\NPF_{E3627245-D752-4A12-AD26-96B77E811233} (cp_vna Check Point Virtual Network
Adapter (Microsoft's Packet Scheduler) )

C:\>
```

In order to run the WinDump, the WinPcap driver (wpcap.dll) has to be installed. If not installed, it would pop-up an error message:


WinDump.exe - Unable To Locate Component

This application has failed to start because wpcap.dll was not found. Re-installing the application may fix this problem.

5. Program Identification

The program `WinDump.exe` is the WinDump (version 3.8.3 beta). It can be downloaded from following URLs for source code and pre-compile binary executable:

http://windump.polito.it/install/bin/windump_3_8_3_beta/WinDump.exe
http://windump.polito.it/install/bin/windump_3_8_3_beta/WDumpSrc.zip

The program `WinPcap_3_1_beta_3.exe` is WinPcap (version 3.1 beta 3). The current available downloadable version on official WinPcap web site http://winpcap.polito.it/install/default.htm is WinPcap 3.1 beta 4 which is not the suspected software version. I searched the mirror site at Goodie Domain Service (Vienna University of Technology) for `WinPcap_3_1_beta_3.exe`. I found it is available at following URL for source code and pre-compile binary executable:

ftp://gd.tuwien.ac.at/infosys/security/polito.it/winpcap/WinPcap_3_1_beta_3.exe
ftp://gd.tuwien.ac.at/infosys/security/polito.it/winpcap/wpcapsrc_3_1_beta_3.zip

After I downloaded the `WinDump.exe` executable, I saved it as “DL-WinDump.exe” and ran `md5sum` against it. (Due to the lack of Microsoft Visual C++ 6.0, I cannot compile the WinDump from the source code I downloaded; however, I downloaded this executable from the WinDump’s official web site, which could be the same source from where Mr. R.L. got the file.)

```
[root@LinuxForensics]# md5sum DL-WinDump.exe
```

```
79375b77975aa53a1b0507496107bff7  DL-WinDump.exe
```

I compared the MD5 signature with the one from recovered `WinDump.exe` file.

```
[root@LinuxForensics]# md5sum WinDump.exe
79375b77975aa53a1b0507496107bff7  WinDump.exe
```

It appears identical which means it is exactly the same program binary.

For the `WinPcap_3_1_beta_3.exe`, I downloaded the executable from above URL and saved as “`DL-WinPcap_3_1_beta_3.exe`”. However, for the deleted “`WinPcap_3_1_beta_3.exe`” file, I can only recover the last 910 sectors out of 950 sectors. In order for me to compare these two file, I used Hex Editor `khexedit` to strip off the first 20,480 bytes (40 sectors) out of `DL-WinPcap_3_1_beta_3.exe` file then saved as `last_910_of_DL-WinPcap_3_1_beta_3.exe.raw` file, then I ran `md5sum` against it for MD5 signature and compared it with the recovered `last_910_of_recover-WinPcap_3_1_beta_3.exe.raw` file.

```
[root@LinuxForensics]# md5sum last_910_of_DL-WinPcap_3_1_beta_3.exe.raw
70553e1c186284f46b46c9521bba629b  last_910_of_DL-WinPcap_3_1_beta_3.exe.raw

[root@LinuxForensics]# md5sum last_910_of_recover-WinPcap_3_1_beta_3.exe.raw
70553e1c186284f46b46c9521bba629b  last_910_of_recover-WinPcap_3_1_beta_3.exe.raw
```

The two files’ MD5 signatures show identical. This strongly indicates that the deleted `WinPcap_3_1_beta_3.exe` file is same as the one I got from ftp://gd.tuwien.ac.at/infosys/security/polito.it/winpcap/WinPcap_3_1_beta_3.exe.

Although we don’t have the fully recovered file, but with the same MD5 signature from same segment on two files, we can confidently say these two files are same file.

6. Legal Implications

Based on the information I gathered from the USB drive image, I found Mr. R.L. was doing real-time email communication interception which may violated the 18 U.S.C. §§ 2511[33] subsection (1)(a)

```
(1) Except as otherwise specifically provided in this chapter any person who-
    (a) intentionally intercepts, endeavors to intercept, or procures any other person to
        intercept or endeavor to intercept, any wire, oral, or electronic communication;
```

If he is convicted for this crime, the penalty is addressed on 18 U.S.C. §§ 2511 subsection (4) (a):

[33] 18 U.S.C. §§ 2511, Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited. http://www.cybercrime.gov/usc2511.htm

```
(4)
    (a) Except as provided in paragraph (b) of this subsection or in subsection (5),
        whoever violates subsection (1) of this section shall be fined under this title or
        imprisoned not more than five years, or both.
```

Within 18 U.S.C. §§ 2511 subsection (2), it addresses several exceptions for wiretapping[34]. Here are some of the exceptions:

1. Subsection (2)(a)(i), “Provider” exception: an authorized employee or agent of a service provider may intercept communication when it is for the self-defense purposes or when it’s necessary in order to render the service. However, it is not an unlimited monitoring. It should be tailored to generic monitoring for service quality control purposes, or only targets the unauthorized access incident in the service they provide, and minimizes the interception on unrelated communication to the incident.

2. Subsection (2)(c)-(d), “Consent” exception: when the person who is intercepting the communication is a party or one of the parties to the communication, and he or she has given prior consent to such interception. This consent can be delivered through the well drafted consent banner to notify the user about the interception before a user accesses the service, or obtain the written consent delivered through Acceptable Usage Policy signed by authorized users.

3. Subsection (2)(i), “Computer Trespasser” exception: sometimes it is not possible to consent or the party is not part of the communication. It is the trespasser who is using the system as pass-through to other downstream victims. This exception allows the law enforcement to intercept the communication to or from a hacker under certain restrictions. The trespasser should not be anyone known to the service provider to have an existing contractual relationship with service provider. 18 U.S.C. §§ 2510(21)(B). In order to apply for the computer trespass exception, it should meet several conditions list in §§ 2511(2)(i)(I~IV).

4. Subsection 2(g)(i), “Accessible to the public” exception: if the communication is configured so that the communication is readily accessible to the generic public.
5. Subsection (3)(b)(iv), “Inadvertently obtained criminal evidence” exception.
6. §§ 2510 subsection (5)(a), “Extension Telephone” exception.
7. Interception pursuant to court order under 18 U.S.C. §§ 2518 of the Wiretap Act.

7. Recommendations

[34] SANS Institute, Track 8 – System Forensics, Investigation & Response, Volume 8.5 page 29 ~ 37, SANS Press, 17~23 Nov. 2004.

Based on this investigation, several suggestions are made to the security administrator:

1. Work with Human Resource for this incident and take appropriate disciplinary actions, potentially contacting the law enforcement.
2. Create Corporate Acceptable Usage Policy (AUP), if not available. And some other applicable security policies. The AUP should state clearly that interception of communication is prohibited and subject to certain disciplinary and legal actions. These policies should be approved by Sr. management. A list of sample security policy templates can be found at http://www.sans.org/resources/policies/#template.
3. Work with Human Resource department, to make sure proper employee policies has been defined. The policy should address clearly that sexual harassment and stalking is prohibited and subject to certain disciplinary and/or legal actions. These policies should be approved by Sr. management.
4. Training for all security policies and employee policies to all employees. Maintain a document to prove that each employee was informed of their obligation to adhere to these policies.
5. Banner Warning, there should be pop-ups before accessing any company resources about following the AUP.
6. Create Incident Response Guide, if not available. Please refer to "FCC Computer Security Incident Guide." http://csrc.nist.gov/fasp/FASPDocs/incident-response/Incident-Response-Guide.pdf.

8. Additional Information

Tools used in this investigation, such as mmls, fsstat, fls, dls, and Autopsy forensic browser, you can find more in detail at URL: http://www.sleuthkit.org/sleuthkit/tools.php.

For the program WinPcap which was used by Mr. R.L. You can find how it works from the WinPcap online manual at http://winpcap.polito.it/docs/docs31beta4/html/index.html.

You also can find WinDump manual from http://windump.polito.it/docs/manual.htm to find how to use the WinDump.

To learn more about FAT file system. You can go to Microsoft online resource, Windows 98 resource kit to find it. http://www.microsoft.com/resources/documentation/windows/98/all/reskit/en-us/part2/wrkc10.mspx

To learn more information about "computer crime", and "intellectual property crime". You can go to http://www.cybercrime.gov/.

To learn more about Ethereal, the open source multi-platform protocol analyzer, you can go to http://www.ethereal.com/.

9. List of references

The following materials were consulted in the preparation of this report.

SANS Institute. GIAC Certification Program Sample Citation and Quotes Version 2.0. SANS/GIAC. 13 Nov. 2004. 8 Dec. 2004. <http://www.giac.org/GIACTC_citations.php>

Harnack, Andrew. Kleppinger, Eugene. Citation Styles. Bedford/St. Martin's. 2003. 4 Jan. 2005. <http://www.bedfordstmartins.com/online/cite5.html#1>

Microsoft Corporation, Microsoft Office (Word) Home Page. Microsoft Corporation. 5 Jan. 2005. <http://office.microsoft.com/en-us/FX010857991033.aspx>

Jansen, Eric. Netlingo Home Page search for "Internet". Netlingo.com. 10 Jan.2005. <http://www.netlingo.com/lookup.cfm?term=Internet>

Degioanni, Loris. Risso, Fulvio. Varenni, Gianluca. Viano Piero. NRG of ICSD at Lawrence Berkeley National Laboratory, University of California, Berkeley, CA. WinDump Home Page. WinDump Project. 5 Jan. 2005. <http://windump.polito.it/>

NetGroup at Politecnico di Torino. WinPcap Documentation. WinPcap Project Home Page. 5 Jan. 2005 <http://winpcap.polito.it/docs/docs31beta4/html/index.html>

Lexico Publishing Group, LLC. Home page search for driver. Dictionary.com. 5 Jan. 2005 <http://dictionary.reference.com/search?q=driver>

SANS Institute. Track 8 – System Forensics, Investigation & Response, Volume 8.5. SANS Press. 17~23 Nov. 2004

United States. Department of Justice. 18 U.S.C. 2510-2522. UNITED STATES CODE ANNOTATED TITLE 18. CRIMES AND CRIMINAL PROCEDURE PART I--CRIMES CHAPTER 119--WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS. 5 Jan. 2005 < http://www.cybercrime.gov/wiretap2510_2522.htm>

United States. Department of Justice. 18 U.S.C. 2511. Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited. 5 Jan. 2005 <http://www.cybercrime.gov/usc2511.htm>

SANS Institute, Track 8 – System Forensics, Investigation & Response, Volume 8.4. SANS Press, 17~23 Nov. 2004

SANS Institute, Track 8 – System Forensics, Investigation & Response, Volume 8.1. SANS Press, 17~23 Nov. 2004

SANS Institute, Track 8 – System Forensics, Investigation & Response, CD. SANS Press, 17~23 Nov. 2004

Free Software Foundation, Inc. Md5sum Manual. GNU Project Home Page. 5 Jan. 2005 <http://www.gnu.org/software/coreutils/manual/html_chapter/coreutils_6.html#SEC26>

Carrier, Brian. mmls manual. Sleuthkit.org. 5 Jan. 2005 <http://www.sleuthkit.org/sleuthkit/man/mmls.html>

Jupitermedia Corporation. Webopedia Home Page. JupiterWeb. 5 Jan. 2005 <http://www.pcwebopedia.com/TERM/F/file_allocation_table_FAT.html>

Microsoft Corporation. Windows 98 Resource Kit. Microsoft. 5 Jan. 2005 <http://www.microsoft.com/resources/documentation/windows/98/all/reskit/en-us/part2/wrkc10.mspx>

Free Software Foundation, Inc. dd Manual. GNU Project Home Page. 5 Jan. 2005 <http://www.gnu.org/software/coreutils/manual/html_chapter/coreutils_11.html#IDX793>

Carrier, Brian. fsstat manual. Sleuthkit.org. 5 Jan. 2005 <http://www.sleuthkit.org/sleuthkit/man/fsstat.html>

Jupitermedia Corporation. Webopedia Home Page TERM cluster . JupiterWeb. 5 Jan. 2005 <http://www.pcwebopedia.com/TERM/c/cluster.html>

Jupitermedia Corporation. Webopedia Home Page TERM slack space. JupiterWeb. 5 Jan. 2005 <http://www.pcwebopedia.com/TERM/S/slack_space.html>

Carrier, Brian. fls manual. Sleuthkit.org. 5 Jan. 2005 <http://www.sleuthkit.org/sleuthkit/man/fls.html>

Carrier, Brian. Autopsy Forensic Browser. Sleuthkit.org. 5 Jan. 2005 <http://www.sleuthkit.org/autopsy/index.php>

Sand, Espen. The KHexEdit Handbook. Home Page. 5 Jan. 2005 <http://home.online.no/~espensa/khexedit/documentation/khexedit.html>

Combs, Gerald. Home Page. Ethereal Project. 5 Jan. 2005 <http://www.ethereal.com/>

SANS Institute, Track 8 – System Forensics, Investigation & Response, Volume 8.6. SANS Press, 17~23 Nov. 2004

Free Software Foundation, Inc. grep Manual. GNU Project Home Page. 5 Jan. 2005 <http://www.gnu.org/software/coreutils/manual/html_chapter/coreutils_11.html#IDX793>

Jupitermedia Corporation. Webopedia Home Page TERM URL. JupiterWeb. 5 Jan. 2005. <http://www.pcwebopedia.com/TERM/U/URL.html>

Jacobson, Van. Leres, Craig. and McCanne, Steven. all of the Lawrence Berkeley National Laboratory, University of California, Berkeley, CA. WinDump manual. Tcpdump.org. 5 Jan. 2005. <http://windump.polito.it/docs/manual.htm>

United States. Department of Justice. 18 U.S.C. 2511. Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited. 5 Jan. 2005 <http://www.cybercrime.gov/usc2511.htm>

SANS Institute, Track 8 – System Forensics, Investigation & Response, Volume 8.5. SANS Press, 17~23 Nov. 2004

United States. Department of Commerce. FCC Computer Security Incident Guide.”. National Institute of Standards and Technology Home Page. 5 Jan. 2005. <http://csrc.nist.gov/fasp/FASPDocs/incident-response/Incident-Response-Guide.pdf>

10. Apendix: Timeline

Here is the timeline I got from Autopsy:

```
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        7        <usbfat16.img-
                                                      _INPCA~1.EXE-dead-7>
                           485810 .a. -/-rwxrwxrwx 0       0        7
                                                      E:\/WinPcap_3_1_beta_3.exe
                                                      (_INPCA~1.EXE) (deleted)
                                0 .a. -rwxrwxrwx 0       0        12       <usbfat16.img-
                                                      _INDUMP.EXE-dead-12>
Wed Oct 27 2004 16:23:50   485810 m.. -/-rwxrwxrwx 0       0        10
                                                      E:\/WinPcap_3_1_beta_3.exe
                                                      (_INPCA~1.EXE) (deleted)
                           485810 m.. -rwxrwxrwx 0       0        10       <usbfat16.img-
                                                      _INPCA~1.EXE-dead-10>
Wed Oct 27 2004 16:23:54   485810 ..c -/-rwxrwxrwx 0       0        10
                                                      E:\/WinPcap_3_1_beta_3.exe
                                                      (_INPCA~1.EXE) (deleted)
                           485810 ..c -/-rwxrwxrwx 0       0        7
                                                      E:\/WinPcap_3_1_beta_3.exe
                                                      (_INPCA~1.EXE) (deleted)
                           485810 ..c -rwxrwxrwx 0       0        10       <usbfat16.img-
                                                      _INPCA~1.EXE-dead-10>
                                0 ..c -rwxrwxrwx 0       0        7        <usbfat16.img-
                                                      _INPCA~1.EXE-dead-7>
Wed Oct 27 2004 16:23:56        0 m.. -rwxrwxrwx 0       0        7        <usbfat16.img-
                                                      _INPCA~1.EXE-dead-7>
                           485810 m.. -/-rwxrwxrwx 0       0        7
                                                      E:\/WinPcap_3_1_beta_3.exe
                                                      (_INPCA~1.EXE) (deleted)
Wed Oct 27 2004 16:24:02   450560 m.. -rwxrwxrwx 0       0        14       <usbfat16.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        12
                                                      E:\/WinDump.exe (_INDUMP.EXE)
                                                      (deleted)
                           450560 ..c -/-rwxrwxrwx 0       0        14
                                                      E:\/WinDump.exe (_INDUMP.EXE)
                                                      (deleted)
                                0 ..c -rwxrwxrwx 0       0        12       <usbfat16.img-
                                                      _INDUMP.EXE-dead-12>
                           450560 ..c -rwxrwxrwx 0       0        14       <usbfat16.img-
                                                      _INDUMP.EXE-dead-14>
Wed Oct 27 2004 16:24:06        0 m.. -rwxrwxrwx 0       0        12       <usbfat16.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        16       E:\/_ap.gif
                                                      (deleted)
                             8814 .a. -rwxrwxrwx 0       0        17       <usbfat16.img-
                                                      _ap.gif-dead-17>
                             8814 .a. -/-rwxrwxrwx 0       0        17       E:\/_ap.gif
                                                      (deleted)
                           450560 .a. -/-rwxrwxrwx 0       0        14
                                                      E:\/WinDump.exe (_INDUMP.EXE)
                                                      (deleted)
                                0 .a. -rwxrwxrwx 0       0        16       <usbfat16.img-
                                                      _ap.gif-dead-16>
                           450560 .a. -rwxrwxrwx 0       0        14       <usbfat16.img-
                                                      _INDUMP.EXE-dead-14>
                            19968 .a. -/-rwxrwxrwx 0       0        18
                                                      E:\/coffee.doc
                           485810 .a. -rwxrwxrwx 0       0        10       <usbfat16.img-
                                                      _INPCA~1.EXE-dead-10>
                           485810 .a. -/-rwxrwxrwx 0       0        10
```

```
                                                       E:\/WinPcap_3_1_beta_3.exe
                                                       (_INPCA~1.EXE) (deleted)
                            53056 .a. -/-rwxrwxrwx 0        0        15       E:\/_apture
                                                       (deleted)
                            53056 .a. -rwxrwxrwx 0        0        15       <usbfat16.img-
                                                       _apture-dead-15>
Thu Oct 28 2004 11:08:24    53056 ..c -/-rwxrwxrwx 0        0        15       E:\/_apture
                                                       (deleted)
                            53056 ..c -rwxrwxrwx 0        0        15       <usbfat16.img-
                                                       _apture-dead-15>
Thu Oct 28 2004 11:11:00    53056 m.. -rwxrwxrwx 0        0        15       <usbfat16.img-
                                                       _apture-dead-15>
                            53056 m.. -/-rwxrwxrwx 0        0        15       E:\/_apture
                                                       (deleted)
Thu Oct 28 2004 11:17:44        0 ..c -rwxrwxrwx 0        0        16       <usbfat16.img-
                                                       _ap.gif-dead-16>
                             8814 ..c -/-rwxrwxrwx 0        0        16       E:\/_ap.gif
                                                       (deleted)
                             8814 ..c -/-rwxrwxrwx 0        0        17       E:\/_ap.gif
                                                       (deleted)
                             8814 ..c -rwxrwxrwx 0        0        17       <usbfat16.img-
                                                       _ap.gif-dead-17>
Thu Oct 28 2004 11:17:46     8814 m.. -rwxrwxrwx 0        0        17       <usbfat16.img-
                                                       _ap.gif-dead-17>
                             8814 m.. -/-rwxrwxrwx 0        0        17       E:\/_ap.gif
                                                       (deleted)
                             8814 m.. -/-rwxrwxrwx 0        0        16       E:\/_ap.gif
                                                       (deleted)
                                0 m.. -rwxrwxrwx 0        0        16       <usbfat16.img-
                                                       _ap.gif-dead-16>
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
```