GCFA assignment version 2.0 (November 18, 2004) Option 1

Name of Student : YUEN, Cheuk Wai (SD759427)
Date Submitted : April 16 10:53AM (Hong Kong Time GMT+8)
Descriptive title : CISSP

Attempted Examination:	GCFA Challenge
Trainings Received:	Local Classes.
Native Language:	Cantonese (Dialect of Chinese)

This is the first submission of the current paper.

Table of Contents

I. Executive Summary

A suspected harassment case has been reported to corporate security on October 29, 2004: sales representative Mr. Robert Lawrence was reported to harass sales representative Ms. Leila Conlay through emails and in person both during and outside of work. Security administrator has authorized the initiation of a computer forensic investigation upon finding a USB drive in Mr. Lawrence's cubicle.

The following evidences were found in the USB drive and suggest Mr. Lawrence had spied upon the privacy of Ms. Conlay, complied harassing emails and installed unauthorized software in his workstation(s):

a. Mail bodies of harassing emails;
b. An electronic copy of a private email by Ms. Conlay obtained through unauthorized and unethical means;
c. Programs used to spy on Ms. Conlay's privacy.

In addition, usages of a "network sniffer" – capable of stealing corporate sales and other sensitive information from the network, and is not required by Mr. Lawrence's job function – had been detected in the scene. The evidence suggests Mr. Lawrence had violated corporate security policy and gained unauthorized access to electronic information not in his custody; investigations on whether Mr. Lawrence had used a network sniffer to perform other unethical acts are recommended.

Nevertheless, the investigator has also identified a number of concerns during the investigation; and suggests the following in depth investigations be performed before concluding:

a. A forensic analysis on Mr. Lawrence's workstation(s);
b. Review attendance records or departmental user sign-on logs of Mr. Lawrence and Ms. Leila on Oct 2004, days 27 to 28;
c. Review Internet access records on proxy servers for the period Oct 27 2004 16:00 to 16:30 and Oct 28 2004 11:00 – 11:30.

II. Objectives of the Investigation

The objectives of the current investigation include:

1. Investigate the following in a forensic copy of evidence received:

    a. List all files in the forensic copy of evidence
    b. Identify the MAC time information of the files in (a)
    c. Identify the owner of the files in (a)
    d. Identify the file size of the files in (a)
    e. Maintain accurate MD5 hash of the files in (a)

2. Analyze the data in (1) to:

    a. Identify any programs used by Mr. Lawrence
    b. Identify how was a program in (a) used
    c. Identify when was a program in (a) used

III. Computer Evidence Analyzed

A forensic copy of the USB Drive obtained in Mr. Lawrence's cubicle has been created by Security Administrator (Mark Mawer), the name of this forensic copy is USBFD-64531026-RL-001.img (thereafter refer as IMAGE) and has been compressed to ease handling.

Evidence#	1
Tag #:	USBFD-64531026-RL-001
Description:	64M Lexar Media JumpDrive
Serial #:	JDSP064-04-5000C
Image:	USBFD-64531026-RL-001.img
MD5:	338ecf17b7fc85bbb2d5ae2bbc729dd5
Obtained by:	Mark Mawer (Security Administrator)

IV. Relevant Findings

The findings in the current investigation are as follow:

1. Evidence suggests offensive messages were complied by Mr. Lawrence was found in the IMAGE (evidence #2, #3 and #4).
2. Evidence suggests Mr. Lawrence had spied on Ms. Conlay's privacy was found in the IMAGE:
   a. Private email messages of Ms. Conlay was found in the IMAGE (evidence #5 and subordinates);
   b. A map referring to the contents in Ms. Conlay's private email was found in the IMAGE. Suggests Mr. Lawrence had read the private message of Ms. Conlay (evidence #6);
   c. Programs used to spy on Ms. Conlay's privacy were found in the IMAGE. Suggests Mr. Lawrence had spied on Ms. Conlay's privacy on purpose (evidence #7 and #8). In addition, use of these programs is also a violation of corporate security policy.

Useful information to comprehend this paper has been included in Appendix I. Details of the evidences identified have been attached in Appendix II:

V. Investigative Details and Supporting Details

A. Methodology Applied

The general accepted practices of computer forensics will be followed to identify, acquire, analyze, and present the evidences.

In the identification phase, the type of investigation to be performed will be accessed and a preliminary plan to list the tasks to be performed based on the data to collect will be established; other factors including forensic equipment requirements, social profile (if needed) will be accessed as well.

In the acquisition phase, sufficient data will be collected for analysis in a later phase for evidences. Maintaining accuracy and integrity of the data are crucial to a successful prosecution if the evidences are presented in a court later. Thus, techniques used to collect the data must not change the data themselves.

In the analysis phase, the data are analyzed by various techniques such as correlations, aggregations, transformations … etc, to prove or disprove hypotheses made. In practice, there are multiple rounds of acquisition and analysis, until sufficient evidences are collected.

Lastly, in the presentation phase, evidences identified will be grouped and presented. They will be further verified for validity.

B. Examination Environment

To investigate the content of the IMAGE, all investigation was done on equipment emulated by Microsoft Virtual PC 2004. The forensic workstation on the emulated platform has no network connection to the host equipment and allow using an “undo disk” to prevent persistent information to be stored.

Information of the host equipment:

- Intel PentiumM 1.6GHz processor
- Windows XP Traditional Chinese and Service Pack 2 and latest patches
- Microsoft Virtual PC 2004
- Norton AntiVirus
- Timezone GMT+8 (Hong Kong)

Information of the forensic workstation on the emulated PC guest:

- Windows 2000 Professional English
- Hex Workshop
- NWDIFF
- VDK
- MD5SUM
- Default TimeZone (GMT-8) (Pacific Time with Daylight Saving Time)

A brief description of some of the programs used has been attached in Appendix III.

C. Examinations Performed and Findings

1. **A working copy of the IMAGE (contents of evidence #1) has been extracted from the zip file.**

2. **The image is renamed to case0604.img and is marked as read only.**

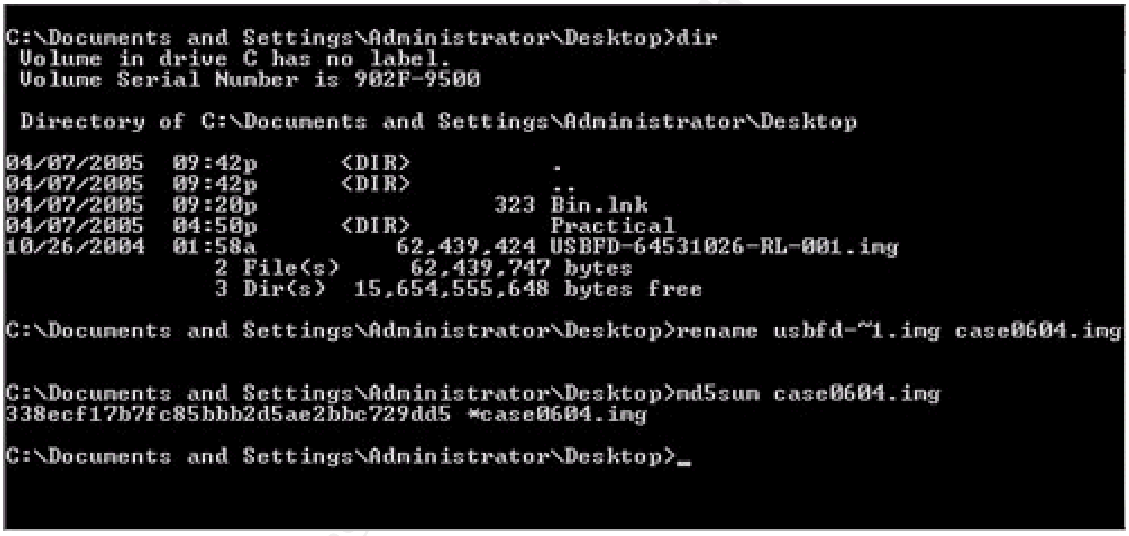
Making the image read only is a good practice; the results of the investigation will not be changed as long as disk content is not overwritten accidentally. The renaming is to reduce typing later.

3. **The MD5 sum of the IMAGE has been verified against the chain of custody.**

The following was executed on a command window (cmd.exe):

```
md5sum case0604.img
```

The result was “338ecf17b7fc85bbb2d5ae2bbc729dd5” and matched the information in the chain of custody received from the security administrator.



```
C:\Documents and Settings\Administrator\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 902F-9500

 Directory of C:\Documents and Settings\Administrator\Desktop

04/07/2005  09:42p      <DIR>          .
04/07/2005  09:42p      <DIR>          ..
04/07/2005  09:20p                 323 Bin.lnk
04/07/2005  04:50p      <DIR>          Practical
10/26/2004  01:58a          62,439,424 USBFD-64531026-RL-001.img
               2 File(s)     62,439,747 bytes
               3 Dir(s)  15,654,555,648 bytes free

C:\Documents and Settings\Administrator\Desktop>rename usbfd-~1.img case0604.img


C:\Documents and Settings\Administrator\Desktop>md5sum case0604.img
338ecf17b7fc85bbb2d5ae2bbc729dd5 *case0604.img

C:\Documents and Settings\Administrator\Desktop>_
```

To support investigations to the contents in the USB drive, the security administration has created a disk image (IMAGE). The IMAGE is an exact copy of the USB drive in terms of contents created by bit-stream data copy. A hard disk holds data in streams of 0s and 1s; a bit-stream copy is a lossless duplication of a storage medium. On a formatted hard disk, a file system is created to organize the data into files; in addition, a master boot record is created in the first sector of a storage medium to describe the layout of a disk. These structures may provide information to the investigation and will be included in the bit-stream image.

A MD5 sum is then generated on the IMAGE; the MD5 sum serves as a signature and ensure integrity of a file, any changes in contents of the IMAGE or the USB drive will cause a different MD5 sum be generated.

MD5 itself is a hash algorithm to generate a 16-byte digest (representing 2^128 possible values) based on the content of the IMAGE. While a pair of different files could share the same digest theoretically (called birthday pair), there is no known method to construct a sibling to match both the hash and to carry meaningful contents. Therefore, verifying the MD5 sum to be identical assures the content being investigated has not been tampered (from the time of receiving it from the security administrator)

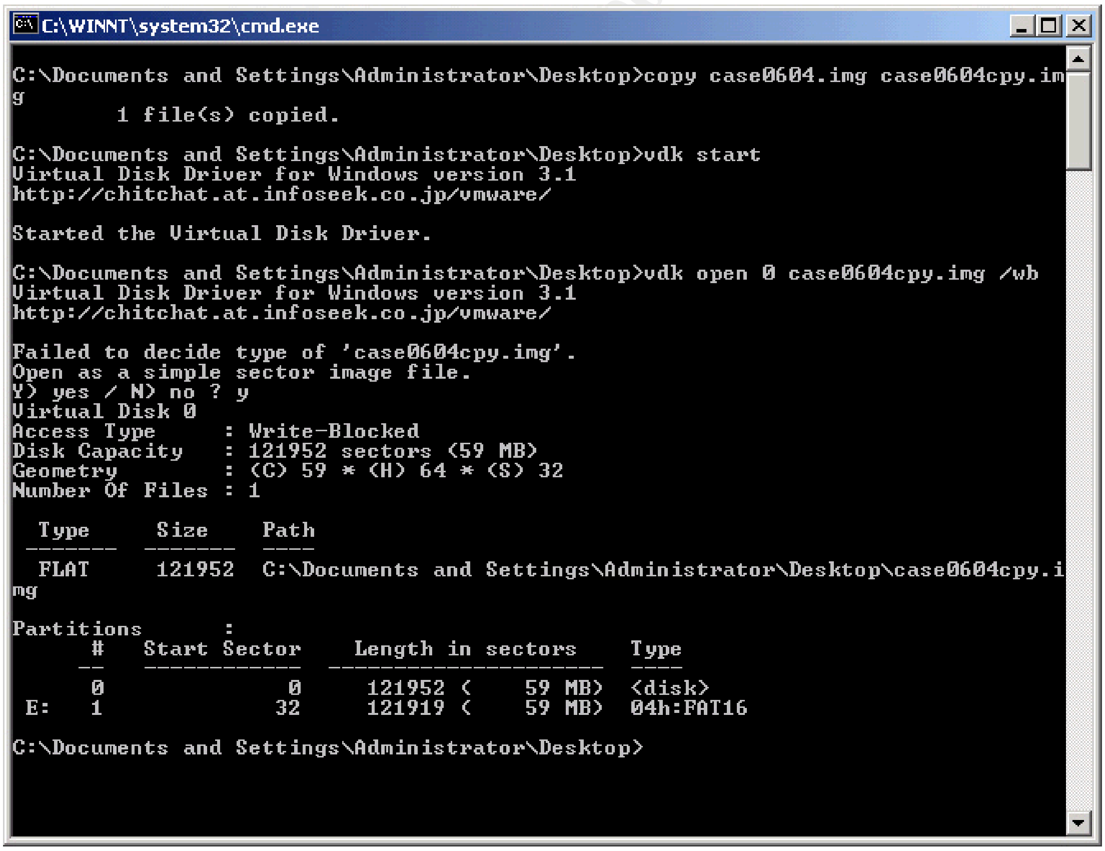
4. A copy of the IMAGE was mounted in write blocker mode with VDK, and the disk content is scanned through.

The following was executed on a command window (cmd.exe):

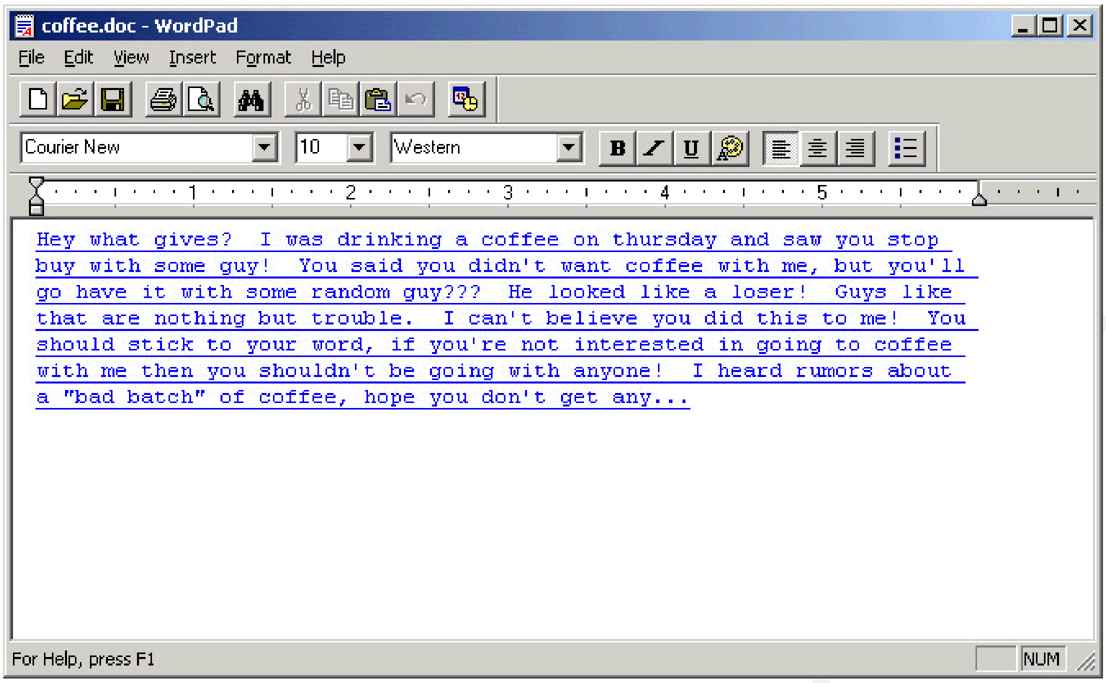
```
vdk start
vdk open 0 case0604cpy.img /wb
```

The VDK mounted drive was opened in a Windows Explorer, 3 Microsoft Word documents (coffee.doc, hey.doc and her.doc) were found, they were scanned with WordPad and offensive messages were found, in "coffee.doc" written on 28 October 2004 7:24PM in particular. The following was executed to close the mounted drive:

```
vdk close 0
vdk stop
```



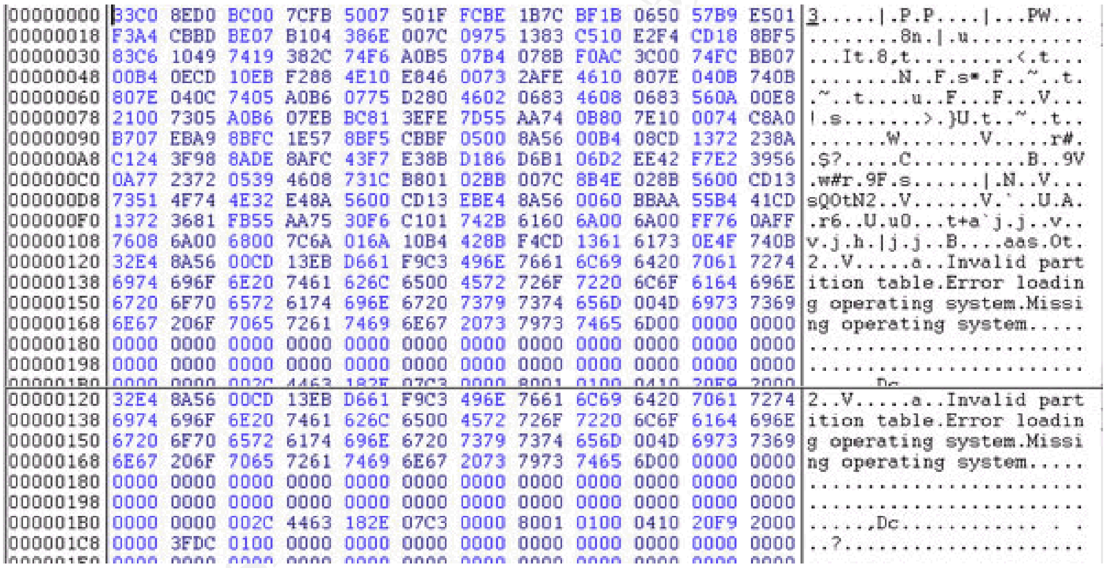
```
C:\Documents and Settings\Administrator\Desktop>copy case0604.img case0604cpy.im
g
        1 file(s) copied.

C:\Documents and Settings\Administrator\Desktop>vdk start
Virtual Disk Driver for Windows version 3.1
http://chitchat.at.infoseek.co.jp/vmware/

Started the Virtual Disk Driver.

C:\Documents and Settings\Administrator\Desktop>vdk open 0 case0604cpy.img /wb
Virtual Disk Driver for Windows version 3.1
http://chitchat.at.infoseek.co.jp/vmware/

Failed to decide type of 'case0604cpy.img'.
Open as a simple sector image file.
Y) yes / N) no ? y
Virtual Disk 0
Access Type     : Write-Blocked
Disk Capacity   : 121952 sectors (59 MB)
Geometry        : (C) 59 * (H) 64 * (S) 32
Number Of Files : 1

  Type      Size     Path
  -------   -------  ----
  FLAT      121952   C:\Documents and Settings\Administrator\Desktop\case0604cpy.i
mg

Partitions       :
      #   Start Sector    Length in sectors     Type
      --  ------------  ---------------------   ----
      0              0     121952 (     59 MB)  <disk>
 E:   1             32     121919 (     59 MB)  04h:FAT16

C:\Documents and Settings\Administrator\Desktop>
```



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...

The documents do indicate possibility of harassment, later investigations must identify if they were indeed written by Mr. Lawrence.

5. The first sector of the IMAGE was opened in HexWorkshop.



```
00000000 33C0 8ED0 BC00 7CFB 5007 501F FCBE 1B7C BF1B 0650 57B9 E501 3.....|.P.P....|...PW...
00000018 F3A4 CBBD BE07 B104 386E 007C 0975 1383 C510 E2F4 CD18 8BF5 ........8n.|.u..........
00000030 83C6 1049 7419 382C 74F6 A0B5 07B4 078B F0AC 3C00 74FC BB07 ...It.8,t.........<.t...
00000048 00B4 0ECD 10EB F288 4E10 E846 0073 2AFE 4610 807E 040B 740B ........N..F.s*.F..~..t.
00000060 807E 040C 7405 A0B6 0775 D280 4602 0683 4608 0683 560A 00E8 .~..t....u..F...F...V...
00000078 2100 7305 A0B6 07EB BC81 3EFE 7D55 AA74 0B80 7E10 0074 C8A0 !.s.......>.}U.t..~..t..
00000090 B707 EBA9 8BFC 1E57 8BF5 CBBF 0500 8A56 00B4 08CD 1372 238A .......W.......V.....r#.
000000A8 C124 3F98 8ADE 8AFC 43F7 E38B D186 D6B1 06D2 EE42 F7E2 3956 .$?.....C..........B..9V
000000C0 0A77 2372 0539 4608 731C B801 02BB 007C 8B4E 028B 5600 CD13 .w#r.9F.s......|.N..V...
000000D8 7351 4F74 4E32 E48A 5600 CD13 EBE4 8A56 0060 BBAA 55B4 41CD sQOtN2..V......V.`..U.A.
000000F0 1372 3681 FB55 AA75 30F6 C101 742B 6160 6A00 6A00 FF76 0AFF .r6..U.u0...t+a`j.j..v..
00000108 7608 6A00 6800 7C6A 016A 10B4 428B F4CD 1361 6173 0E4F 740B v.j.h.|j.j..B....aas.Ot.
00000120 32E4 8A56 00CD 13EB D661 F9C3 496E 7661 6C69 6420 7061 7274 2..V.....a..Invalid part
00000138 6974 696F 6E20 7461 626C 6500 4572 726F 7220 6C6F 6164 696E ition table.Error loadin
00000150 6720 6F70 6572 6174 696E 6720 7379 7374 656D 004D 6973 7369 g operating system.Missi
00000168 6E67 206F 7065 7261 7469 6E67 2073 7973 7465 6D00 0000 0000 ng operating system.....
00000180 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ........................
00000198 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ........................
000001B0 0000 0000 002C 4463 182E 07C3 0000 8001 0100 0410 20F9 2000 ......Dc................
```

```
00000120 32E4 8A56 00CD 13EB D661 F9C3 496E 7661 6C69 6420 7061 7274 2..V.....a..Invalid part
00000138 6974 696F 6E20 7461 626C 6500 4572 726F 7220 6C6F 6164 696E ition table.Error loadin
00000150 6720 6F70 6572 6174 696E 6720 7379 7374 656D 004D 6973 7369 g operating system.Missi
00000168 6E67 206F 7065 7261 7469 6E67 2073 7973 7465 6D00 0000 0000 ng operating system.....
00000180 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ........................
00000198 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ........................
```

```
000001B0 0000 0000 002C 4463 182E 07C3 0000 8001 0100 0410 20F9 2000 ......,Dc...............
000001C8 0000 3FDC 0100 0000 0000 0000 0000 0000 0000 0000 0000 0000 ..?.....................
```

It was identified the disk to contain a Master Boot Record (MBR) and a single partition of information, the information of the first partition has been extracted as follow:

	Information identified	Byte Offset from 0x1BE	Value
a.	Value of 0x80 indicates the partition is active.	0	0x80
b.	Value of 4 indicates the partition is FAT16 formatted.	4	0x04
c.	The first partition starts at LBA address of 0x20; therefore it starts at 16,384 bytes (32 * 512) or 0x4000 from the beginning of the disk.	8-11	0x20 (32)
d.	The size of the partition is 121,919 sectors (0x01dc3f). Thus, the size of disk is roughly 59.5MB.	12-15	0x1DC3F (121,919)

It was identified the total size of disk to be 121,952 sectors or 62,439,424 bytes.

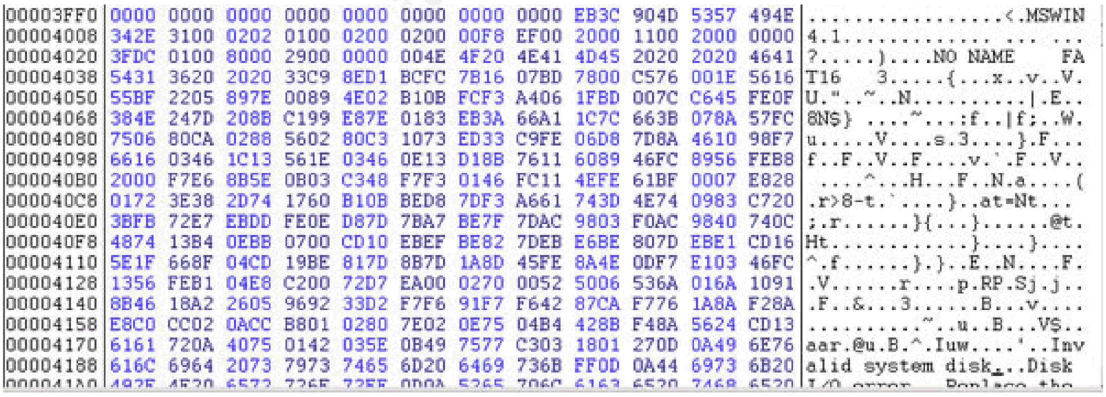
The disk geometry was reviewed to gain an idea of what is on the disk to support planning for further analysis.

The disk we are analyzing has a Master Boot Record (MBR). MBR has a size of 512 bytes; it includes a program to boot the computer from the active partition and a partition table to define the layout of storage areas (partitions). The partition table includes four entries of 8 bytes each and defines the layout of the disk.

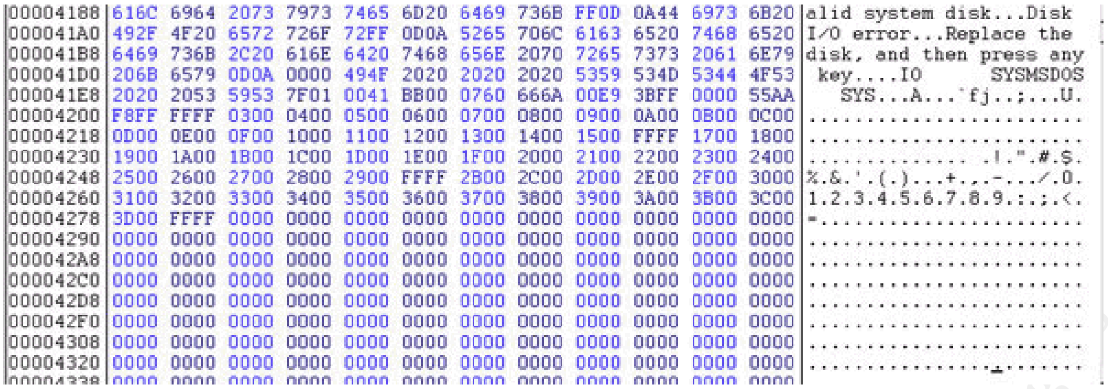
In our case, the partition table has only 1 entry (marked in physical address 0x1BE – 0x1CD inclusive), indicating the disk to contain only 1 partition. This partition is formatted by DOS (point b. above) and occupies the remaining of the disk. A brief review on the partition table and the file system contents will be the next step to assess what to collect for subsequent investigations.

One question is that it is not a common practice to place an MBR in a USB drive without making the first partition bootable (msdos.sys and io.sys were not found, as described in later investigations). In addition, the partition type indicator (value 0x04) suggested the volume to be <= 32MB, yet the actual disk size is 59.2MB. In addition, the disk is very clean, that most of its data area are filled by 0s.

6. The first partition (at 0x4000) of the IMAGE was reviewed using a hex editor.



```
00003FF0 0000 0000 0000 0000 0000 0000 0000 0000 EB3C 904D 5357 494E ...............<.MSWIN
00004008 342E 3100 0202 0100 0200 0200 00F8 EF00 2000 1100 2000 0000 4.1............ ... ...
00004020 3FDC 0100 8000 2900 0000 004E 4F20 4E41 4D45 2020 2020 4641 ?.....)....NO NAME    FA
00004038 5431 3620 2020 33C9 8ED1 BCFC 7B16 07BD 7800 C576 001E 5616 T16   3.....{...x..v..V.
00004050 55BF 2205 897E 0089 4E02 B10B FCF3 A406 1FBD 007C C645 FE0F U."..~..N..........|.E..
00004068 384E 247D 208B C199 E87E 0183 EB3A 66A1 1C7C 663B 078A 57FC 8N$} ....~...:f..|f;..W.
00004080 7506 80CA 0288 5602 80C3 1073 ED33 C9FE 06D8 7D8A 4610 98F7 u.....V....s.3....}.F...
00004098 6616 0346 1C13 561E 0346 0E13 D18B 7611 6089 46FC 8956 FEB8 f..F..V..F....v.`.F..V..
000040B0 2000 F7E6 8B5E 0B03 C348 F7F3 0146 FC11 4EFE 61BF 0007 E828  ....^...H...F..N.a....(
000040C8 0172 3E38 2D74 1760 B10B BED8 7DF3 A661 743D 4E74 0983 C720 .r>8-t.`....}..at=Nt...
000040E0 3BFB 72E7 EBDD FE0E D87D 7BA7 BE7F 7DAC 9803 F0AC 9840 740C ;.r......}{...}......@t.
000040F8 4874 13B4 0EBB 0700 CD10 EBEF BE82 7DEB E6BE 807D EBE1 CD16 Ht.............}....}....
00004110 5E1F 668F 04CD 19BE 817D 8B7D 1A8D 45FE 8A4E 0DF7 E103 46FC ^.f......}.}..E..N....F.
00004128 1356 FEB1 04E8 C200 72D7 EA00 0270 0052 5006 536A 016A 1091 .V......r....p.RP.Sj.j..
00004140 8B46 18A2 2605 9692 33D2 F7F6 91F7 F642 87CA F776 1A8A F28A .F..&...3......B...v....
00004158 E8C0 CC02 0ACC B801 0280 7E02 0E75 04B4 428B F48A 5624 CD13 ..........~..u..B...V$..
00004170 6161 720A 4075 0142 035E 0B49 7577 C303 1801 270D 0A49 6E76 aar.@u.B.^.Iuw....'..Inv
00004188 616C 6964 2073 7973 7465 6D20 6469 736B FF0D 0A44 6973 6B20 alid system disk...Disk
000041A0 492F 4F20 6572 726F 72FF 0D0A 5265 706C 6163 6520 7468 6520 I/O error...Replace the
```



```
00004188 616C 6964 2073 7973 7465 6D20 6469 736B FF0D 0A44 6973 6B20 alid system disk...Disk
000041A0 492F 4F20 6572 726F 72FF 0D0A 5265 706C 6163 6520 7468 6520 I/O error...Replace the
000041B8 6469 736B 2C20 616E 6420 7468 656E 2070 7265 7373 2061 6E79 disk, and then press any
000041D0 206B 6579 0D0A 0000 494F 2020 2020 2020 5359 534D 5344 4F53  key....IO      SYSMSDOS
000041E8 2020 2053 5953 7F01 0041 BB00 0760 666A 00E9 3BFF 0000 55AA    SYS...A...`fj..;...U.
00004200 F8FF FFFF 0300 0400 0500 0600 0700 0800 0900 0A00 0B00 0C00 ........................
00004218 0D00 0E00 0F00 1000 1100 1200 1300 1400 1500 FFFF 1700 1800 ........................
00004230 1900 1A00 1B00 1C00 1D00 1E00 1F00 2000 2100 2200 2300 2400 .............. .!.".#.$.
00004248 2500 2600 2700 2800 2900 FFFF 2B00 2C00 2D00 2E00 2F00 3000 %.&.'.(.)...+.,.-.../.0.
00004260 3100 3200 3300 3400 3500 3600 3700 3800 3900 3A00 3B00 3C00 1.2.3.4.5.6.7.8.9.:.;.<.
00004278 3D00 FFFF 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 =.......................
00004290 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ........................
000042A8 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ........................
000042C0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ........................
000042D8 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ........................
000042F0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ........................
00004308 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ........................
00004320 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ........................
00004338 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
```

The boot sector in the first partition was reviewed, the following information has been identified:

	Information identified	Byte Offset from 0x4000	Value
a.	The OEM name indicates the file system is created in a Windows 95 OSR2 or Windows 98 system.	3-10	"MSWIN4.1"
b.	Each cluster contains 2 sectors, or 1,024 bytes.	13	0x02 (2)
c.	There is 1 reserved sector.	14 – 15	0x01 (1)
d.	The file system has 2 file allocation tables.	16	0x02 (2)
e.	The file system can contain 512 entries in the root directory.	17-18	0x200 (512)
f.	Number of sectors per file allocation table is 239.	22-23	0xEF (239)
g.	The volume is formatted in FAT16	43-53	"FAT16 "

For a file system formatted with FAT, the first sector is always the boot sector. It contains an OEM ID, the bootstrap program (a linkage to the "kernel loader" to start the operating system), the BIOS Parameter Block (BPB) and the extend BPB (bytes 12 to 62 in FAT16). Valuable information about the file system can be read in the BPB and the extended BPB.

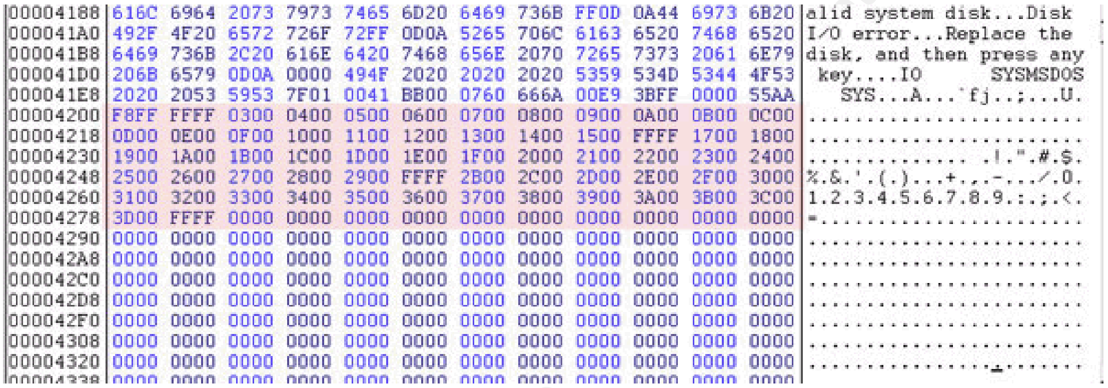
In this case, firstly, the OEM ID ("MSWIN4.1") (point a. above) indicates the file system was formatted by a Windows 95 OSR2 or a Windows 98 system; and installation of driver software is necessary to support proper functioning of USB devices in these operating systems. Therefore, the device driver for the USB drive is likely to exist in Lawrence's workstation if it is running Windows 98 or Windows 95 OSR2, if he is using Windows 2000 or XP, traces of USB device installations can be identified in the local machine registry hive under \System\CurrentControlSet\Enum\* and possibly in the event log as well. In addition, it has been identified the cluster size to be 2 sectors (point b. above). Depending on the file size, up to 1023 bytes of spaces in the last cluster allocated to a file could be left unused. These spaces are called slack spaces and may store information of a previously deleted file or other contents.

After the boot sector, there are 2 file allocation tables (FAT): the first is the original and the second a backup copy for contingency. The root directory and data area come after the 2 file allocation tables.

As the file system being analyzed holds 512 entries in its root directory (point e. above), and each entry in FAT16 is 32 bytes, we can calculated the root directory to occupy 32 sectors on the disk. The information up till this point allows us to identify the disk layout.

Region Descriptions	Starting Sector	Ending Sector	Region Size in Sectors	Region Size in Bytes
Master Boot Record	0x000000	0x000000	1	512
Unused	0x000001	0x00001F	31	15,872
First Partition Boot Sector	0x000020	0x000020	1	512
First Partition File Allocation Table	0x000021	0x00010F	239	122,368
First Partition File Allocation Table Backup	0x000110	0x0001FE	239	122,368
First Partition Root Directory	0x0001FF	0x00021E	32	16,384
First Partition Data Region	0x00021F	0x01DC5E	121,408	62,160,896
First Partition Data Region that cannot be used	0x01DC5F	0x01DC5F	1	512

7. **The file allocation table (in 0x4200) in the first partition was reviewed using a hex editor.**



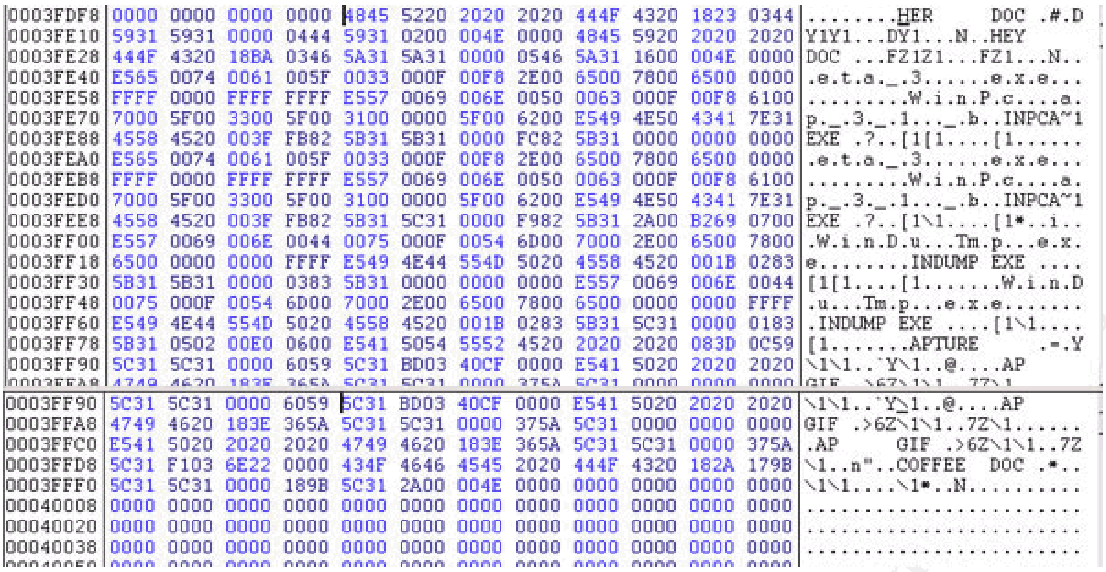
```
00004188 616C 6964 2073 7973 7465 6D20 6469 736B FF0D 0A44 6973 6B20 alid system disk...Disk
000041A0 492F 4F20 6572 726F 72FF 0D0A 5265 706C 6163 6520 7468 6520 I/O error...Replace the
000041B8 6469 736B 2C20 616E 6420 7468 656E 2070 7265 7373 2061 6E79 disk, and then press any
000041D0 206B 6579 0D0A 0000 494F 2020 2020 2020 5359 534D 5344 4F53  key....IO      SYSMSDOS
000041E8 2020 2053 5953 7F01 0041 BB00 0760 666A 00E9 3BFF 0000 55AA    SYS...A...`fj..;...U.
00004200 F8FF FFFF 0300 0400 0500 0600 0700 0800 0900 0A00 0B00 0C00 ........................
00004218 0D00 0E00 0F00 1000 1100 1200 1300 1400 1500 FFFF 1700 1800 ........................
00004230 1900 1A00 1B00 1C00 1D00 1E00 1F00 2000 2100 2200 2300 2400 .............. .!.".#.$.
00004248 2500 2600 2700 2800 2900 FFFF 2B00 2C00 2D00 2E00 2F00 3000 %.&.'.(.)...+.,.-.../.0.
00004260 3100 3200 3300 3400 3500 3600 3700 3800 3900 3A00 3B00 3C00 1.2.3.4.5.6.7.8.9.:.;.<.
00004278 3D00 FFFF 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 =.......................
00004290 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ........................
000042A8 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ........................
000042C0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ........................
000042D8 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ........................
000042F0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ........................
00004308 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ........................
00004320 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................_.......
00004338 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
```

The File Allocation Table (FAT) was reviewed, it is identified that only the initial portion of the data region is currently being used.

For a FAT16 formatted media, storages are allocated in clusters. The clusters allocated are marked in the file allocation table as a link list with nodes of 2 bytes. The first node start from the 5th byte in the file allocation table (the first 2 nodes = first 4 bytes are not used), the content value could be a number from (0x0003 to 0xFFEF) to indicate the next cluster of data, 0xFFF7 to indicate bad sector, or 0xFFF8 to 0xFFFF to indicate end of file.

Thus, we can see 3 contiguous files in our case, and all the spaces used by these files are allocated from the beginning of the partition. There is a good chance for us to chain up non-overwritten clusters to recover part or whole of deleted files in the disk in this case, since most clusters are not overwritten by another file.

8. **The root directory (in 0x3FE00) in the first partition was reviewed using a hex editor.**



```
0003FDF8 0000 0000 0000 0000 4845 5220 2020 2020 444F 4320 1823 0344 ........HER     DOC .#.D
0003FE10 5931 5931 0000 0444 5931 0200 004E 0000 4845 5920 2020 2020 Y1Y1...DY1...N..HEY
0003FE28 444F 4320 18BA 0346 5A31 5A31 0000 0546 5A31 1600 004E 0000 DOC ...FZ1Z1...FZ1...N..
0003FE40 E565 0074 0061 005F 0033 000F 00F8 2E00 6500 7800 6500 0000 .e.t.a._.3......e.x.e...
0003FE58 FFFF 0000 FFFF FFFF E557 0069 006E 0050 0063 000F 00F8 6100 .........W.i.n.P.c....a.
0003FE70 7000 5F00 3300 5F00 3100 0000 5F00 6200 E549 4E50 4341 7E31 p._.3._.1..._.b..INPCA~1
0003FE88 4558 4520 003F FB82 5B31 5B31 0000 FC82 5B31 0000 0000 0000 EXE .?..[1[1....[1......
0003FEA0 E565 0074 0061 005F 0033 000F 00F8 2E00 6500 7800 6500 0000 .e.t.a._.3......e.x.e...
0003FEB8 FFFF 0000 FFFF FFFF E557 0069 006E 0050 0063 000F 00F8 6100 .........W.i.n.P.c....a.
0003FED0 7000 5F00 3300 5F00 3100 0000 5F00 6200 E549 4E50 4341 7E31 p._.3._.1..._.b..INPCA~1
0003FEE8 4558 4520 003F FB82 5B31 5C31 0000 F982 5B31 2A00 B269 0700 EXE .?..[1\1....[1*..i..
0003FF00 E557 0069 006E 0044 0075 000F 0054 6D00 7000 2E00 6500 7800 .W.i.n.D.u...Tm.p...e.x.
0003FF18 6500 0000 0000 FFFF E549 4E44 554D 5020 4558 4520 001B 0283 e........INDUMP EXE ....
0003FF30 5B31 5B31 0000 0383 5B31 0000 0000 0000 E557 0069 006E 0044 [1[1....[1.......W.i.n.D
0003FF48 0075 000F 0054 6D00 7000 2E00 6500 7800 6500 0000 0000 FFFF .u...Tm.p...e.x.e.......
0003FF60 E549 4E44 554D 5020 4558 4520 001B 0283 5B31 5C31 0000 0183 .INDUMP EXE ....[1\1....
0003FF78 5B31 0502 00E0 0600 E541 5054 5552 4520 2020 2020 083D 0C59 [1.......APTURE     .=.Y
0003FF90 5C31 5C31 0000 6059 5C31 BD03 40CF 0000 E541 5020 2020 2020 \1\1..`Y\1..@....AP

0003FF90 5C31 5C31 0000 6059 5C31 BD03 40CF 0000 E541 5020 2020 2020 \1\1..`Y\1..@....AP
0003FFA8 4749 4620 183E 365A 5C31 5C31 0000 375A 5C31 0000 0000 0000 GIF .>6Z\1\1..7Z\1......
0003FFC0 E541 5020 2020 2020 4749 4620 183E 365A 5C31 5C31 0000 375A .AP     GIF .>6Z\1\1..7Z
0003FFD8 5C31 F103 6E22 0000 434F 4646 4545 2020 444F 4320 182A 179B \1..n"..COFFEE  DOC .*..
0003FFF0 5C31 5C31 0000 189B 5C31 2A00 004E 0000 0000 0000 0000 0000 \1\1....\1*..N..........
00040008 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ........................
00040020 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ........................
00040038 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ........................
```

The root directory was reviewed, it was identified that some files have been created but are now deleted from the USB drive; 16 file entries including 13 deleted entries and 0 directory entries were found. Some of the files used long file names and span over multiple entries.

Each directory entry in FAT16 (FAT12/32 as well) is 32 bytes and could refer to a directory or a file with 8.3 naming convention to hold information such as time of last modified, accessed and creation, file size … etc. Nevertheless, FAT16 do not store ownership information and the resolution of time in FAT16 is 2 seconds for the last modified and the created timestamps; also, only date information is recorded for last accessed timestamp.

In our case, a few points have been identified. One, there are deleted files, as the first byte of some FAT entries has value of 0xE5 indicating that they are free for reuse. Second, instances of "Windump.exe" and "WinPcap_3_1_beta_3.exe" had a long file name and span over several entries. Lastly, only a small number of root directory entries are in use.

Point to puzzle is some file entries repeated themselves; from the investigator's own experiences, this might happen when a file is saved through Microsoft Internet Explorer, copied over the network, … etc. Yet it is unsure at this point if they did actually happened, however. In addition, "Windump.exe" can be represented by a single directory entry but is now spanning over several entries.

9. **AccessData FTK evaluation was installed to the forensic workstation for further investigations.**

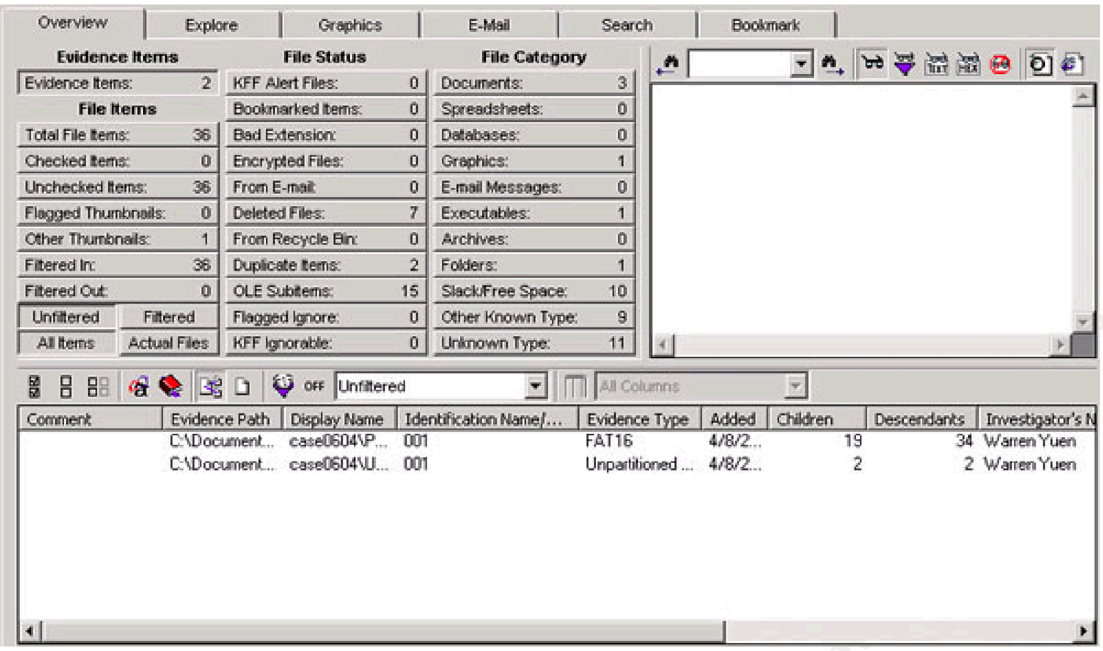
Since only a few files (including deleted files) have been identified on the IMAGE, evaluation version of AccessData FTK software, capable of processing 5,000 files have been chosen to support further investigation. The advantages of choosing FTK is that the image we are processing has only a few entries and used only very limited spaces. Also, FTK is easy to install and requires minimal configuration, thus is ideal to complete the investigation before the assigned deadline.

10. Information in the IMAGE was analyzed with FTK

FTK found 36 items from the IMAGE, to summarize the information found:

- 3 Microsoft Word documents (as identified earlier);
- 7 deleted files including duplicates of:
  - Map ("!ap.gif") of a part in Hollywood, Los Angeles created/downloaded using Microsoft MapPoint.
  - Executable "Windump.exe"
  - An unknown file with the name "WinPcap_3_1_beta_3.exe"
  - An unknown file with the name "!apture"
- The executables were created and accessed on 27 October, while the map "!ap.gif" and the unknown "!apture" file were created on 28 October. The offensive text "Coffee.doc" was written on late 28 October.
- One instance of "WinPcap_3_1_beta_3.exe", "WinDump.exe" and "!ap.gif" has a logical size of 0 bytes.
- Other items included slack spaces, master boot record, empty spaces … etc.

File in root directory (* indicates deleted file)	Identified File Type	Created Time (Sorted)	Modified Time	Logical Size
her.doc	Microsoft Word XP Document	25/10/2004 8:32:06	25/10/2004 8:32:08	19968
hey.doc	Microsoft Word XP Document	26/10/2004 8:48:06	26/10/2004 8:48:10	19968
WinPcap_3_1_beta_3.exe*	Unknown File Type	27/10/2004 16:23:54	27/10/2004 16:23:56	0
WinPcap_3_1_beta_3.exe*	Unknown File Type	27/10/2004 16:23:54	27/10/2004 16:23:50	485810
WinDump.exe*	Unknown File Type	27/10/2004 16:24:04	27/10/2004 16:24:06	0
WinDump.exe*	Executable File	27/10/2004 16:24:04	27/10/2004 16:24:02	450560
!apture*	Unknown File Type	28/10/2004 11:08:24	28/10/2004 11:11:00	53056
!ap.gif*	Unknown File Type	28/10/2004 11:17:44	28/10/2004 11:17:46	0
!ap.gif*	GIF File	28/10/2004 11:17:44	28/10/2004 11:17:46	8814
coffee.doc	Microsoft Word XP Document	28/10/2004 19:24:46	28/10/2004 19:24:48	19968

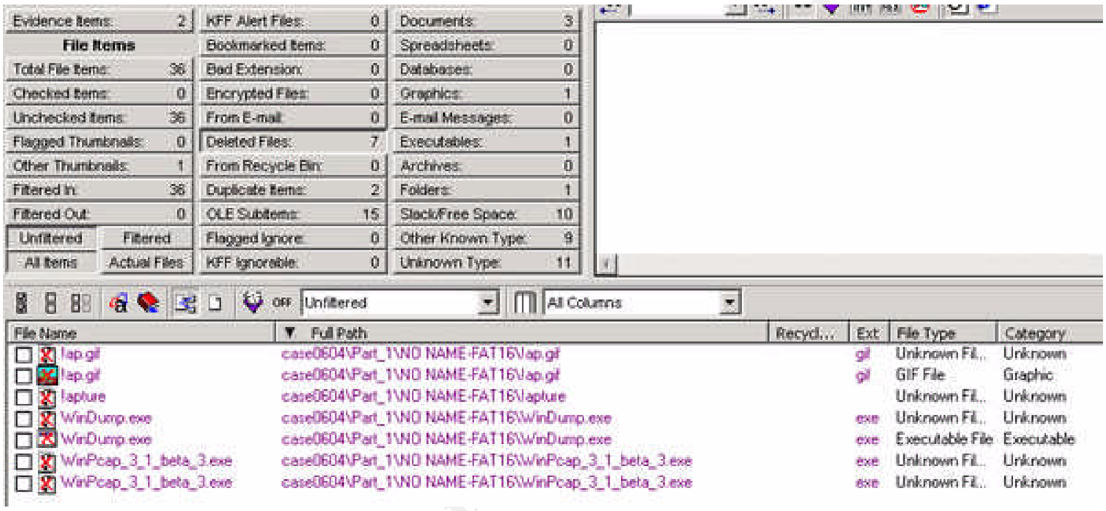


Evidence Items		File Status		File Category	
Evidence Items:	2	KFF Alert Files:	0	Documents:	3
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	36	Bad Extension:	0	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	1
Unchecked Items:	36	From E-mail:	0	E-mail Messages:	0
Flagged Thumbnails:	0	Deleted Files:	7	Executables:	1
Other Thumbnails:	1	From Recycle Bin:	0	Archives:	0
Filtered In:	36	Duplicate Items:	2	Folders:	1
Filtered Out:	0	OLE Subitems:	15	Slack/Free Space:	10
Unfiltered	Filtered	Flagged Ignore:	0	Other Known Type:	9
All Items	Actual Files	KFF Ignorable:	0	Unknown Type:	11

Unfiltered

All Columns

Comment	Evidence Path	Display Name	Identification Name/...	Evidence Type	Added	Children	Descendants	Investigator's N
	C:\Document...	case0604\P...	001	FAT16	4/8/2...	19	34	Warren Yuen
	C:\Document...	case0604\U...	001	Unpartitioned ...	4/8/2...	2	2	Warren Yuen

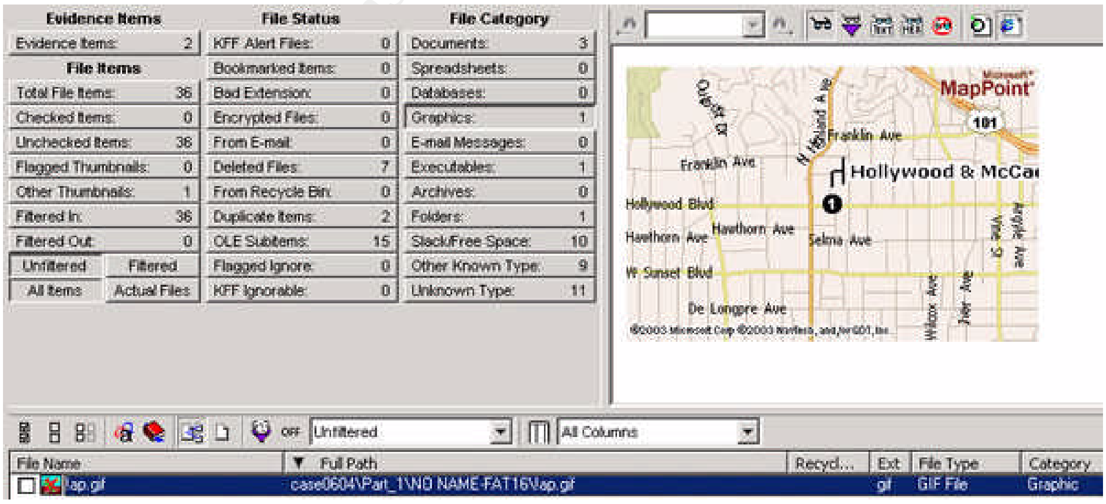


Evidence Items:	2	KFF Alert Files:	0	Documents:	3
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	36	Bad Extension:	0	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	1
Unchecked Items:	36	From E-mail:	0	E-mail Messages:	0
Flagged Thumbnails:	0	Deleted Files:	7	Executables:	1
Other Thumbnails:	1	From Recycle Bin:	0	Archives:	0
Filtered In:	36	Duplicate Items:	2	Folders:	1
Filtered Out:	0	OLE Subitems:	15	Slack/Free Space:	10
Unfiltered	Filtered	Flagged Ignore:	0	Other Known Type:	9
All Items	Actual Files	KFF Ignorable:	0	Unknown Type:	11

Unfiltered

All Columns

File Name	▼ Full Path	Recycl...	Ext	File Type	Category
□ !ap.gif	case0604\Part_1\NO NAME-FAT16\!ap.gif		gif	Unknown Fil...	Unknown
□ !ap.gif	case0604\Part_1\NO NAME-FAT16\!ap.gif		gif	GIF File	Graphic
□ !apture	case0604\Part_1\NO NAME-FAT16\!apture			Unknown Fil...	Unknown
□ WinDump.exe	case0604\Part_1\NO NAME-FAT16\WinDump.exe		exe	Unknown Fil...	Unknown
□ WinDump.exe	case0604\Part_1\NO NAME-FAT16\WinDump.exe		exe	Executable File	Executable
□ WinPcap_3_1_beta_3.exe	case0604\Part_1\NO NAME-FAT16\WinPcap_3_1_beta_3.exe		exe	Unknown Fil...	Unknown
□ WinPcap_3_1_beta_3.exe	case0604\Part_1\NO NAME-FAT16\WinPcap_3_1_beta_3.exe		exe	Unknown Fil...	Unknown



Evidence Items		File Status		File Category	
Evidence Items:	2	KFF Alert Files:	0	Documents:	3
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	36	Bad Extension:	0	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	1
Unchecked Items:	36	From E-mail:	0	E-mail Messages:	0
Flagged Thumbnails:	0	Deleted Files:	7	Executables:	1
Other Thumbnails:	1	From Recycle Bin:	0	Archives:	0
Filtered In:	36	Duplicate Items:	2	Folders:	1
Filtered Out:	0	OLE Subitems:	15	Slack/Free Space:	10
Unfiltered	Filtered	Flagged Ignore:	0	Other Known Type:	9
All Items	Actual Files	KFF Ignorable:	0	Unknown Type:	11

Unfiltered

All Columns

File Name	▼ Full Path	Recycl...	Ext	File Type	Category
□ !ap.gif	case0604\Part_1\NO NAME-FAT16\!ap.gif		gif	GIF File	Graphic

A number of items are of particular interest. One, the programs "WinDump" and "WinPcap" are well-known freeware network sniffer to steal packets off a network; "WinPcap" enables a network card to operate in promiscuous mode and capture packets intended for other nodes on a network, and WinDump is capable of saving the captured packets for further analysis. In addition, considering the file creation time, the file "!apture" is likely to be a network packet dump and information in "!ap.gif" is probably generated with reference to information in "!apture". Also, for one of the "Windump.exe", the last modified time (Oct 27 16:24:02) is 2 seconds earlier than its creation time (Oct 27 16:24:04), suggesting the file has been copied from another source or location.

In addition, FTK has confirmed the "*.doc" files to be Microsoft Word documents; therefore, we may attempt to recover the file owner information from the Microsoft Word document files.

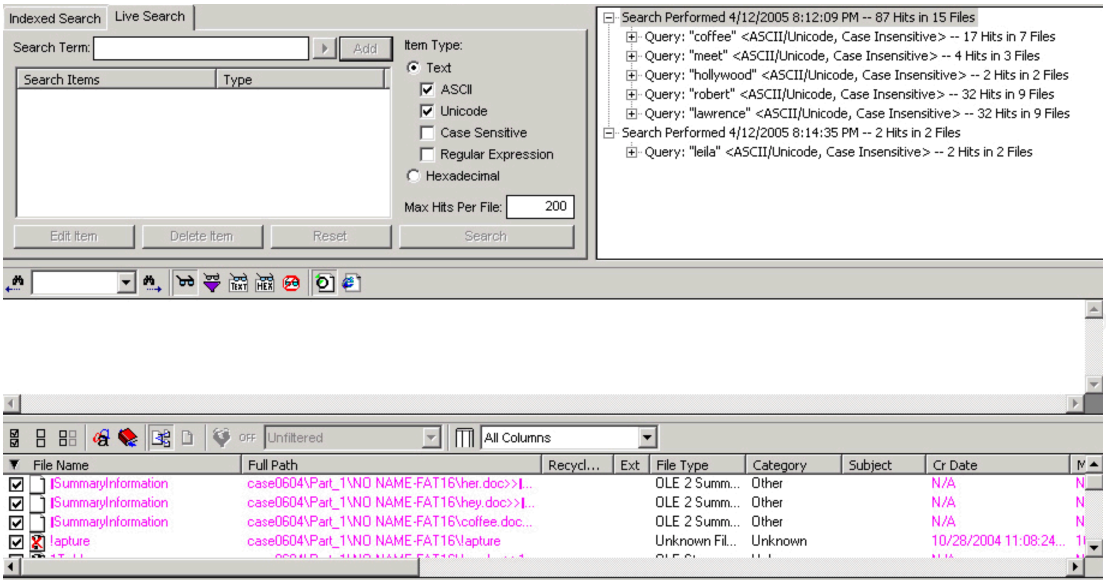
Therefore, the following will be the subject of further analysis: i) to test if the files "WinPcap_3_1_beta3.exe" and "WinDump.exe" are the network sniffer programs with the same name; ii) to confirm if the file "!apture" is a packet capture file; iii) to confirm if the information in the GIF file "!ap" is contained in "!apture"; and iv) to retrieve additional information form Microsoft Word documents.

An item to puzzle is the file "!apture" was created on Oct 28 11:08 and modified on 11:11; if it is indeed a packet capture, it is unlikely for the capture to be done on random, given the short duration of the file. Reviewing the contents of "!apture" may provide some clues on the matter.

A point to note is the information in the map supported our initial setting of the time zone to GMT-8, since Hollywood, LA is on the Pacific timezone.

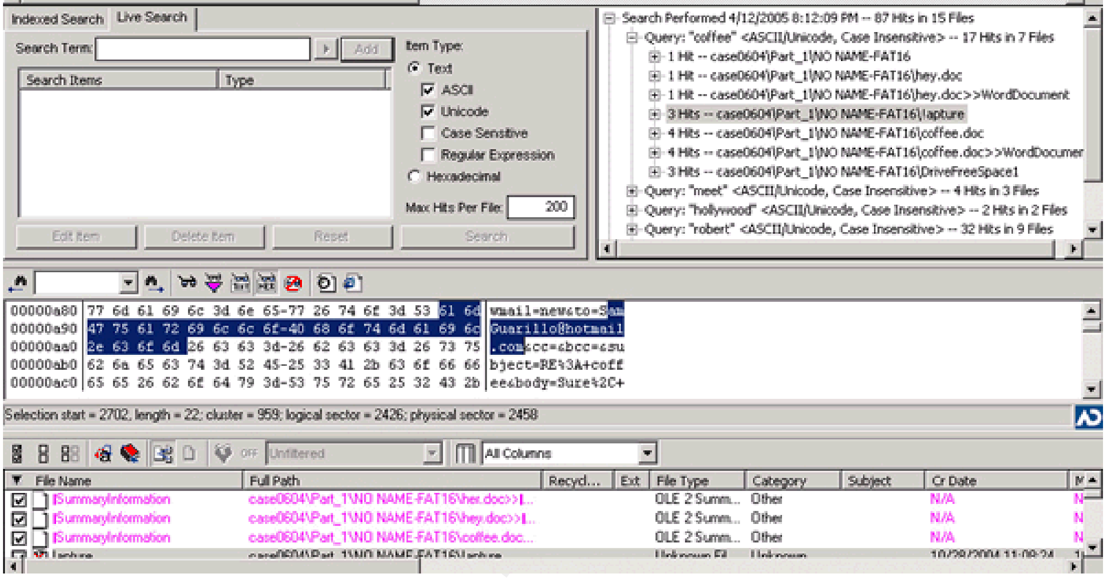
11. String searches were performed on the IMAGE with FTK

The following words (ignoring letter cases) were searched in the IMAGE: "Robert", "Lawrence", "Leila", "Conlay", "Coffee", "meet", "Hollywood", "Blvd", "Sam", "flowergirl" and "hotmail". The results: "Coffee" – 17 hits; "Meet" – 4 hits; "Hollywood" – 2 hits; "Robert Lawrence" – 32 hits; "Leila" – 2 hits; "Hotmail" – 68 hits; "Sam" – 34 hits and "Flowergirl" – 6 hits. The words "Hollywood", "Leila", "Hotmail", "Sam" and "Flowergirl" were all found in the deleted file "!apture".



```
⊟ Search Performed 4/12/2005 8:12:09 PM -- 87 Hits in 15 Files
   ⊞ Query: "coffee" <ASCII/Unicode, Case Insensitive> -- 17 Hits in 7 Files
   ⊞ Query: "meet" <ASCII/Unicode, Case Insensitive> -- 4 Hits in 3 Files
   ⊞ Query: "hollywood" <ASCII/Unicode, Case Insensitive> -- 2 Hits in 2 Files
   ⊞ Query: "robert" <ASCII/Unicode, Case Insensitive> -- 32 Hits in 9 Files
   ⊞ Query: "lawrence" <ASCII/Unicode, Case Insensitive> -- 32 Hits in 9 Files
⊟ Search Performed 4/12/2005 8:14:35 PM -- 2 Hits in 2 Files
   ⊞ Query: "leila" <ASCII/Unicode, Case Insensitive> -- 2 Hits in 2 Files
```

	File Name	Full Path	Recycl...	Ext	File Type	Category	Subject	Cr Date	M
☑	♦SummaryInformation	case0604\Part_1\NO NAME-FAT16\her.doc>>♦...			OLE 2 Summ...	Other		N/A	N
☑	♦SummaryInformation	case0604\Part_1\NO NAME-FAT16\hey.doc>>♦...			OLE 2 Summ...	Other		N/A	N
☑	♦SummaryInformation	case0604\Part_1\NO NAME-FAT16\coffee.doc...			OLE 2 Summ...	Other		N/A	N
☑	!apture	case0604\Part_1\NO NAME-FAT16\!apture			Unknown Fil...	Unknown		10/28/2004 11:08:24...	1(

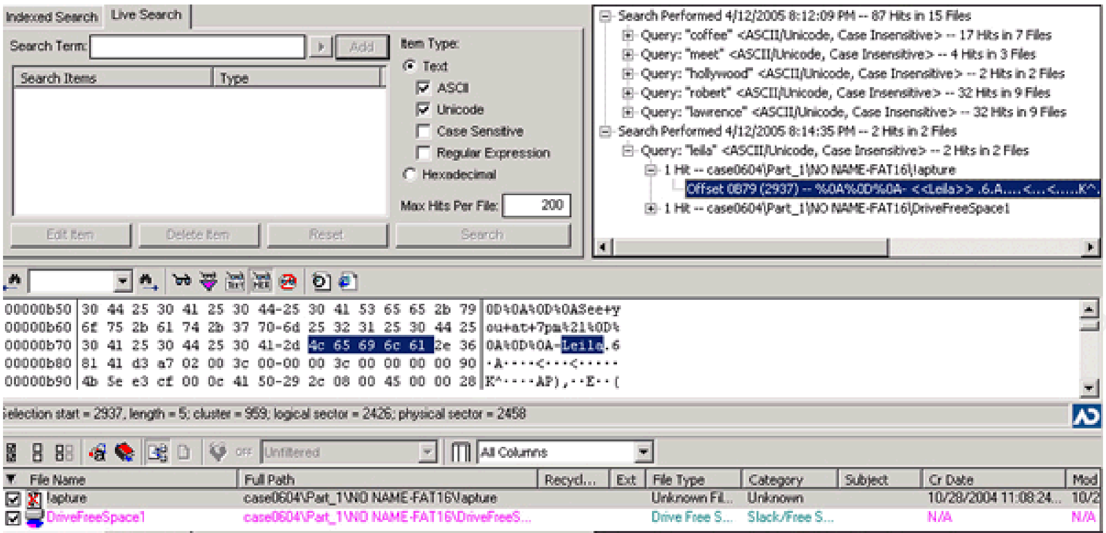


```
⊟ Search Performed 4/12/2005 8:12:09 PM -- 87 Hits in 15 Files
   ⊟ Query: "coffee" <ASCII/Unicode, Case Insensitive> -- 17 Hits in 7 Files
      ⊞ 1 Hit -- case0604\Part_1\NO NAME-FAT16
      ⊞ 1 Hit -- case0604\Part_1\NO NAME-FAT16\hey.doc
      ⊞ 1 Hit -- case0604\Part_1\NO NAME-FAT16\hey.doc>>WordDocument
      ⊞ 3 Hits -- case0604\Part_1\NO NAME-FAT16\!apture
      ⊞ 4 Hits -- case0604\Part_1\NO NAME-FAT16\coffee.doc
      ⊞ 4 Hits -- case0604\Part_1\NO NAME-FAT16\coffee.doc>>WordDocumer
      ⊞ 3 Hits -- case0604\Part_1\NO NAME-FAT16\DriveFreeSpace1
   ⊞ Query: "meet" <ASCII/Unicode, Case Insensitive> -- 4 Hits in 3 Files
   ⊞ Query: "hollywood" <ASCII/Unicode, Case Insensitive> -- 2 Hits in 2 Files
   ⊞ Query: "robert" <ASCII/Unicode, Case Insensitive> -- 32 Hits in 9 Files
```

```
00000a80 77 6d 61 69 6c 3d 6e 65-77 26 74 6f 3d 53 61 6d wmail=new&to=Sam
00000a90 47 75 61 72 69 6c 6c 6f-40 68 6f 74 6d 61 69 6c Guarillo@hotmail
00000aa0 2e 63 6f 6d 26 63 63 3d-26 62 63 63 3d 26 73 75 .com&cc=&bcc=&su
00000ab0 62 6a 65 63 74 3d 52 45-25 33 41 2b 63 6f 66 66 bject=RE%3A+coff
00000ac0 65 65 26 62 6f 64 79 3d-53 75 72 65 25 32 43 2b ee&body=Sure%2C+
```

Selection start = 2702, length = 22; cluster = 959; logical sector = 2426; physical sector = 2458

	File Name	Full Path	Recycl...	Ext	File Type	Category	Subject	Cr Date	M
☑	♦SummaryInformation	case0604\Part_1\NO NAME-FAT16\her.doc>>♦...			OLE 2 Summ...	Other		N/A	N
☑	♦SummaryInformation	case0604\Part_1\NO NAME-FAT16\hey.doc>>♦...			OLE 2 Summ...	Other		N/A	N
☑	♦SummaryInformation	case0604\Part_1\NO NAME-FAT16\coffee.doc...			OLE 2 Summ...	Other		N/A	N
☑	!apture	case0604\Part_1\NO NAME-FAT16\!apture			Unknown Fil...	Unknown		10/28/2004 11:08:24...	1



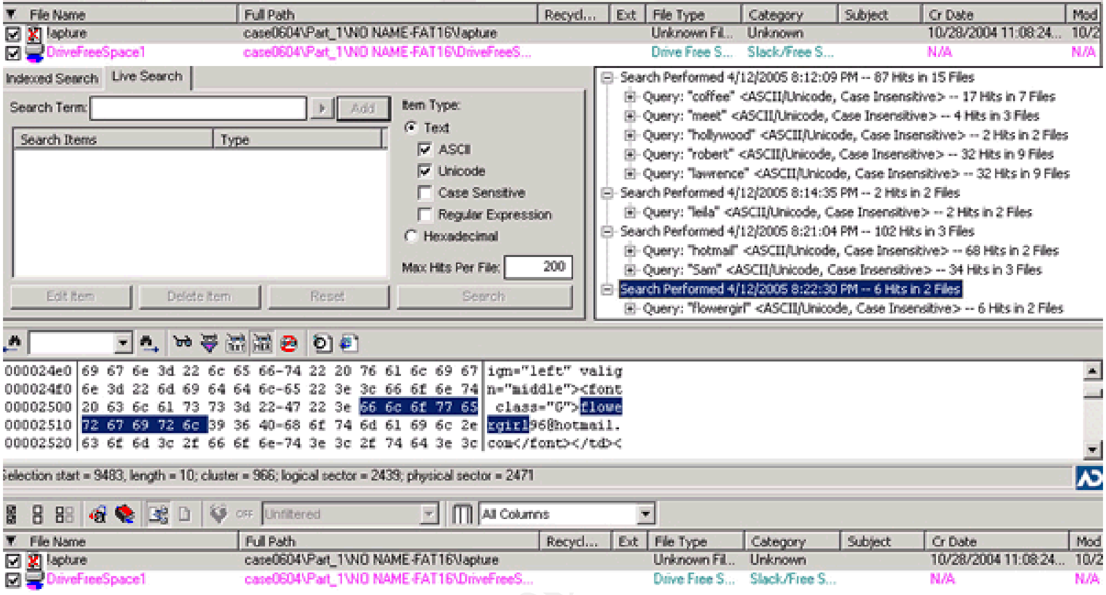
Item Type:
● Text
☑ ASCII
☑ Unicode
☐ Case Sensitive
☐ Regular Expression
○ Hexadecimal
Max Hits Per File: 200

```
⊟ Search Performed 4/12/2005 8:12:09 PM -- 87 Hits in 15 Files
   ⊞ Query: "coffee" <ASCII/Unicode, Case Insensitive> -- 17 Hits in 7 Files
   ⊞ Query: "meet" <ASCII/Unicode, Case Insensitive> -- 4 Hits in 3 Files
   ⊞ Query: "hollywood" <ASCII/Unicode, Case Insensitive> -- 2 Hits in 2 Files
   ⊞ Query: "robert" <ASCII/Unicode, Case Insensitive> -- 32 Hits in 9 Files
   ⊞ Query: "lawrence" <ASCII/Unicode, Case Insensitive> -- 32 Hits in 9 Files
⊟ Search Performed 4/12/2005 8:14:35 PM -- 2 Hits in 2 Files
   ⊟ Query: "leila" <ASCII/Unicode, Case Insensitive> -- 2 Hits in 2 Files
      ⊟ 1 Hit -- case0604\Part_1\NO NAME-FAT16\!apture
         Offset 0B79 (2937) -- %0A%0D%0A- <<Leila>> .6.A....<...<.....K^.
      ⊞ 1 Hit -- case0604\Part_1\NO NAME-FAT16\DriveFreeSpace1
```

```
00000b50 30 44 25 30 41 25 30 44-25 30 41 53 65 65 2b 79 0D%0A%0D%0ASee+y
00000b60 6f 75 2b 61 74 2b 37 70-6d 25 32 31 25 30 44 25 ou+at+7pm%21%0D%
00000b70 30 41 25 30 44 25 30 41-2d 4c 65 69 6c 61 2e 36 0A%0D%0A-Leila.6
00000b80 81 41 d3 a7 02 00 3c 00-00 00 3c 00 00 00 00 90 ·A····<···<·····
00000b90 4b 5e e3 cf 00 0c 41 50-29 2c 08 00 45 00 00 28 K^····AP),··E··(
```

Selection start = 2937, length = 5; cluster = 959; logical sector = 2426; physical sector = 2458

	File Name	Full Path	Recycl...	Ext	File Type	Category	Subject	Cr Date	Mod
☑	!apture	case0604\Part_1\NO NAME-FAT16\!apture			Unknown Fil...	Unknown		10/28/2004 11:08:24...	10/2
☑	DriveFreeSpace1	case0604\Part_1\NO NAME-FAT16\DriveFreeS...			Drive Free S...	Slack/Free S...		N/A	N/A



Item Type:
● Text
☑ ASCII
☑ Unicode
☐ Case Sensitive
☐ Regular Expression
○ Hexadecimal
Max Hits Per File: 200

```
⊟ Search Performed 4/12/2005 8:12:09 PM -- 87 Hits in 15 Files
   ⊞ Query: "coffee" <ASCII/Unicode, Case Insensitive> -- 17 Hits in 7 Files
   ⊞ Query: "meet" <ASCII/Unicode, Case Insensitive> -- 4 Hits in 3 Files
   ⊞ Query: "hollywood" <ASCII/Unicode, Case Insensitive> -- 2 Hits in 2 Files
   ⊞ Query: "robert" <ASCII/Unicode, Case Insensitive> -- 32 Hits in 9 Files
   ⊞ Query: "lawrence" <ASCII/Unicode, Case Insensitive> -- 32 Hits in 9 Files
⊟ Search Performed 4/12/2005 8:14:35 PM -- 2 Hits in 2 Files
   ⊞ Query: "leila" <ASCII/Unicode, Case Insensitive> -- 2 Hits in 2 Files
⊟ Search Performed 4/12/2005 8:21:04 PM -- 102 Hits in 3 Files
   ⊞ Query: "hotmail" <ASCII/Unicode, Case Insensitive> -- 68 Hits in 2 Files
   ⊞ Query: "Sam" <ASCII/Unicode, Case Insensitive> -- 34 Hits in 3 Files
⊟ Search Performed 4/12/2005 8:22:30 PM -- 6 Hits in 2 Files
   ⊞ Query: "flowergirl" <ASCII/Unicode, Case Insensitive> -- 6 Hits in 2 Files
```

```
000024e0 69 67 6e 3d 22 6c 65 66-74 22 20 76 61 6c 69 67 ign="left" valig
000024f0 6e 3d 22 6d 69 64 64 6c-65 22 3e 3c 66 6f 6e 74 n="middle"><font
00002500 20 63 6c 61 73 73 3d 22-47 22 3e 66 6c 6f 77 65  class="G">flowe
00002510 72 67 69 72 6c 39 36 40-68 6f 74 6d 61 69 6c 2e rgirl96@hotmail.
00002520 63 6f 6d 3c 2f 66 6f 6e-74 3e 3c 2f 74 64 3e 3c com</font></td><
```

Selection start = 9483, length = 10; cluster = 966; logical sector = 2439; physical sector = 2471

	File Name	Full Path	Recycl...	Ext	File Type	Category	Subject	Cr Date	Mod
☑	!apture	case0604\Part_1\NO NAME-FAT16\!apture			Unknown Fil...	Unknown		10/28/2004 11:08:24...	10/2
☑	DriveFreeSpace1	case0604\Part_1\NO NAME-FAT16\DriveFreeS...			Drive Free S...	Slack/Free S...		N/A	N/A

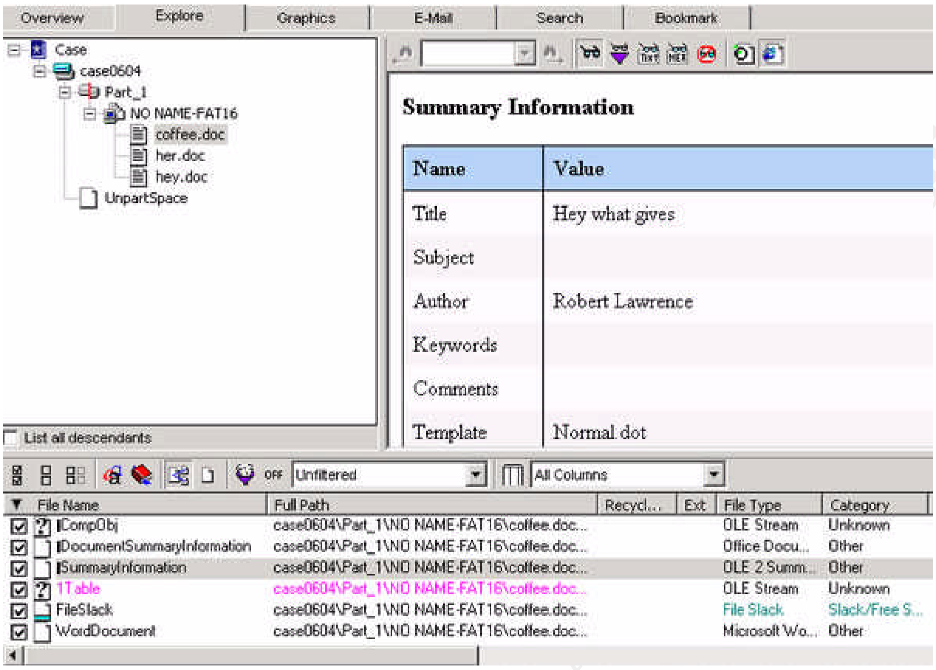
Before recovering the deleted files and performing further analysis, an exhaustive string search was performed on the IMAGE as a whole. The information collected may prevent errors if it reveals conflicting elements, and may ease subsequent investigations.

The words for initial search were chosen with respective to the information identified until this point. “Robert”, “Lawrence”, “Leila” , “Conlay” were the name of the suspect and the victim in our case; “Coffee”, “meet” has been the subject in “Hey.doc” and “Coffee.doc”; “Hollywood” and “Blvd” are information revealed in the map “!ap.gif”. The words “Sam”, “flowergirl” and “hotmail” were included upon completing our initial search, as email address have been seen in our search of “Hollywood”, in the file “!apture”. In short, it appears that “!apture” included email communications between flowergirl96@hotmail.com and SamGuarillo@hotmail.com.

12. The document information in the Microsoft Word files were reviewed with FTK.

Information acquired in the document summary section of the Microsoft Word document files were listed below:

File name	Title	Created	Last Saved
Coffee.doc	Hey what gives	10/28/2004 7:23:00 PM	10/28/2004 7:24:00 PM
Her.doc	Hey I saw you the other day	10/25/2004 8:30:00 AM	10/25/2004 8:32:00 AM
Hey.doc	Hey	10/26/2004 8:47:00 AM	10/26/2004 8:48:00 AM



Summary Information

Name	Value
Title	Hey what gives
Subject	
Author	Robert Lawrence
Keywords	
Comments	
Template	Normal.dot

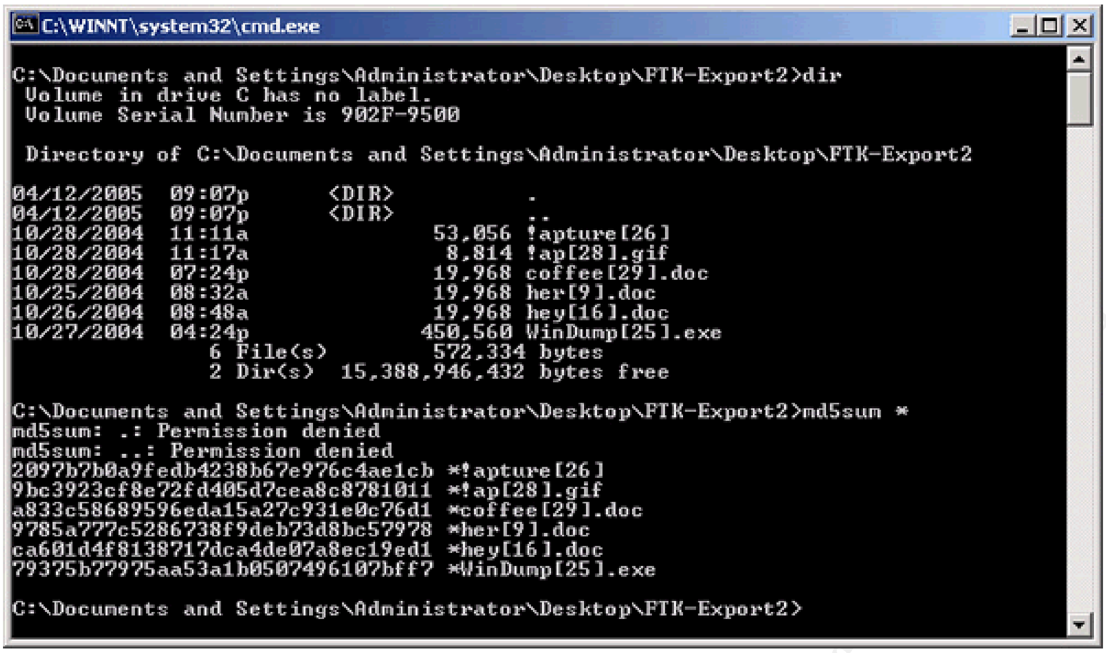
	File Name	Full Path	Recycl...	Ext	File Type	Category
☑	▮CompObj	case0604\Part_1\NO NAME-FAT16\coffee.doc...			OLE Stream	Unknown
☑	▮DocumentSummaryInformation	case0604\Part_1\NO NAME-FAT16\coffee.doc...			Office Docu...	Other
☑	▮SummaryInformation	case0604\Part_1\NO NAME-FAT16\coffee.doc...			OLE 2 Summ...	Other
☑	1Table	case0604\Part_1\NO NAME-FAT16\coffee.doc...			OLE Stream	Unknown
☑	FileSlack	case0604\Part_1\NO NAME-FAT16\coffee.doc...			File Slack	Slack/Free S...
☑	WordDocument	case0604\Part_1\NO NAME-FAT16\coffee.doc...			Microsoft Wo...	Other

In addition, it was identified that all files were created with “Microsoft Word 10.0” (Microsoft Office XP) and is of component object class “Word.Document.8” (version 8). “Robert Lawrence” was identified as the “Last Author” in all three documents.

There was a difference in timestamps between those carried in Microsoft Word and those in the file system collected earlier. It can be accounted by the fact that creation timestamp in the file system records when the document is first saved to the disk, while creation timestamp in Microsoft Word records when a file is first edited before it is saved to disk. In addition, Microsoft Office does not store the timestamp down to number of seconds.

13. Information in FTK was exported for further analysis.

Files (including actual and delete files) were exported through FTK. All instances of “WinPcap_3_1_beta_3.exe”, and the 3 files with logical size of 0 bytes were not recovered. MD5 sums were generated on the recovered files.

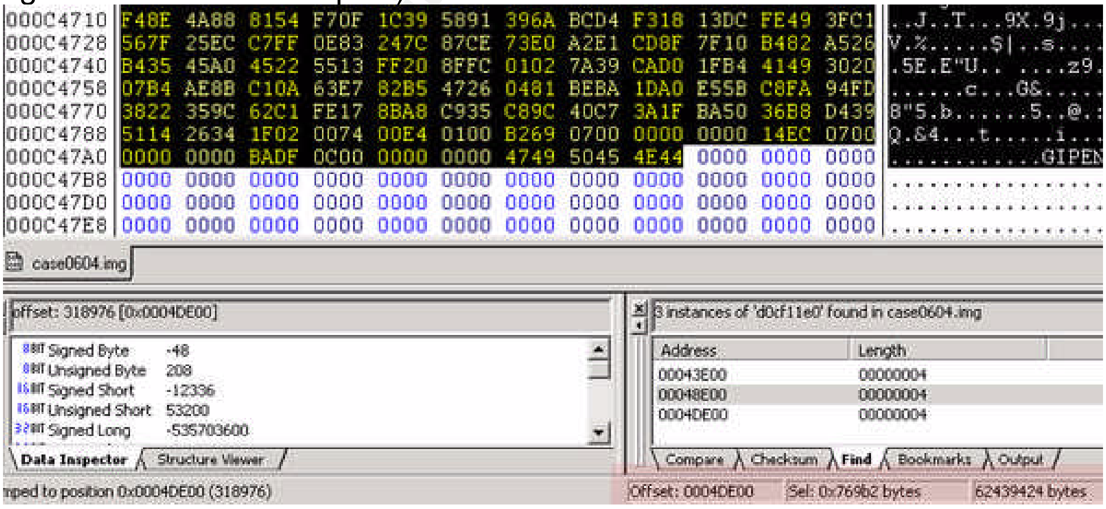


```
C:\Documents and Settings\Administrator\Desktop\FTK-Export2>dir
 Volume in drive C has no label.
 Volume Serial Number is 902F-9500

 Directory of C:\Documents and Settings\Administrator\Desktop\FTK-Export2

04/12/2005  09:07p      <DIR>          .
04/12/2005  09:07p      <DIR>          ..
10/28/2004  11:11a              53,056 !apture[26]
10/28/2004  11:17a               8,814 !ap[28].gif
10/28/2004  07:24p              19,968 coffee[29].doc
10/25/2004  08:32a              19,968 her[9].doc
10/26/2004  08:48a              19,968 hey[16].doc
10/27/2004  04:24p             450,560 WinDump[25].exe
               6 File(s)        572,334 bytes
               2 Dir(s)  15,388,946,432 bytes free

C:\Documents and Settings\Administrator\Desktop\FTK-Export2>md5sum *
md5sum: .: Permission denied
md5sum: ..: Permission denied
2097b7b0a9fedb4238b67e976c4ae1cb *!apture[26]
9bc3923cf8e72fd405d7cea8c8781011 *!ap[28].gif
a833c58689596eda15a27c931e0c76d1 *coffee[29].doc
9785a777c5286738f9deb73d8bc57978 *her[9].doc
ca601d4f8138717dca4de07a8ec19ed1 *hey[16].doc
79375b77975aa53a1b0507496107bff7 *WinDump[25].exe

C:\Documents and Settings\Administrator\Desktop\FTK-Export2>
```

For each 32 bytes directory entry in FAT, the last 6 bytes contain the starting cluster and the file size information; if the information were lost, chance of automatic recovery of data is slim. In our case, FTK was not able to recover the 3 files with zero-ed starting cluster and logical file size. However, since all these entries were duplicated (in file name at least), the content had been recovered through their alternate entries. In addition, manual recovery (or through other tools) of "WinPcap_3_1_beta_3.exe" may be possible, since one of its two entries has a valid starting cluster and logical file size.

14. WinPcap_3_1_beta_3.exe was recovered manually from the IMAGE.

Using HexWorkshop, 485,810 bytes (0x769b2) of data from physical address 0x4DE00 was extracted and saved to "WinPcap". the MD5 sum of the recovered data was "b794de4b88068ae80de523c3b35eeaab" (See lower right hand corner in figure below shaded in pink).



```
000C4710 F48E 4A88 8154 F70F 1C39 5891 396A BCD4 F318 13DC FE49 3FC1 ..J..T...9X.9j...
000C4728 567F 25EC C7FF 0E83 247C 87CE 73E0 A2E1 CD8F 7F10 B482 A526 V.%.....$|..s....
000C4740 B435 45A0 4522 5513 FF20 8FFC 0102 7A39 CAD0 1FB4 4149 3020 .5E.E"U.. ....z9.
000C4758 07B4 AE8B C10A 63E7 82B5 4726 0481 BEBA 1DA0 E55B C8FA 94FD ......c...G&.....
000C4770 3822 359C 62C1 FE17 8BA8 C935 C89C 40C7 3A1F BA50 36B8 D439 8"5.b......5..@.:
000C4788 5114 2634 1F02 0074 00E4 0100 B269 0700 0000 0000 14EC 0700 Q.&4...t.....i...
000C47A0 0000 0000 BADF 0C00 0000 0000 4749 5045 4E44 0000 0000 0000 ............GIPEN
000C47B8 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 .................
000C47D0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 .................
000C47E8 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 .................
```

offset: 318976 [0x0004DE00]

8BIT Signed Byte	-48
8BIT Unsigned Byte	208
16BIT Signed Short	-12336
16BIT Unsigned Short	53200
32BIT Signed Long	-535703600

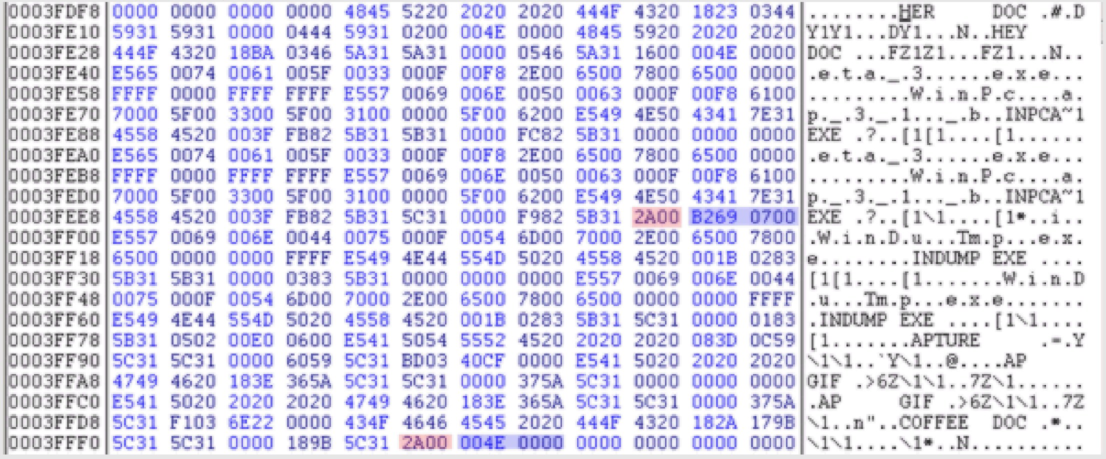
3 instances of 'd0cf11e0' found in case0604.img

Address	Length
00043E00	00000004
00048E00	00000004
0004DE00	00000004

mped to position 0x0004DE00 (318976)

Offset: 0004DE00 Sel: 0x769b2 bytes 62439424 bytes

Reviewing the root directory content, it can be confirmed that both “Coffee.doc” and “WinPcap_3_1_beta_3.exe” start at cluster 42 (0x2a) or physical address 0x4DE00. In addition, the size and starting cluster information of the deleted files reveals that deleted file were allocated on the disk in a consecutive order and did not overwrite each other; making manual recovery of deleted files much simpler.



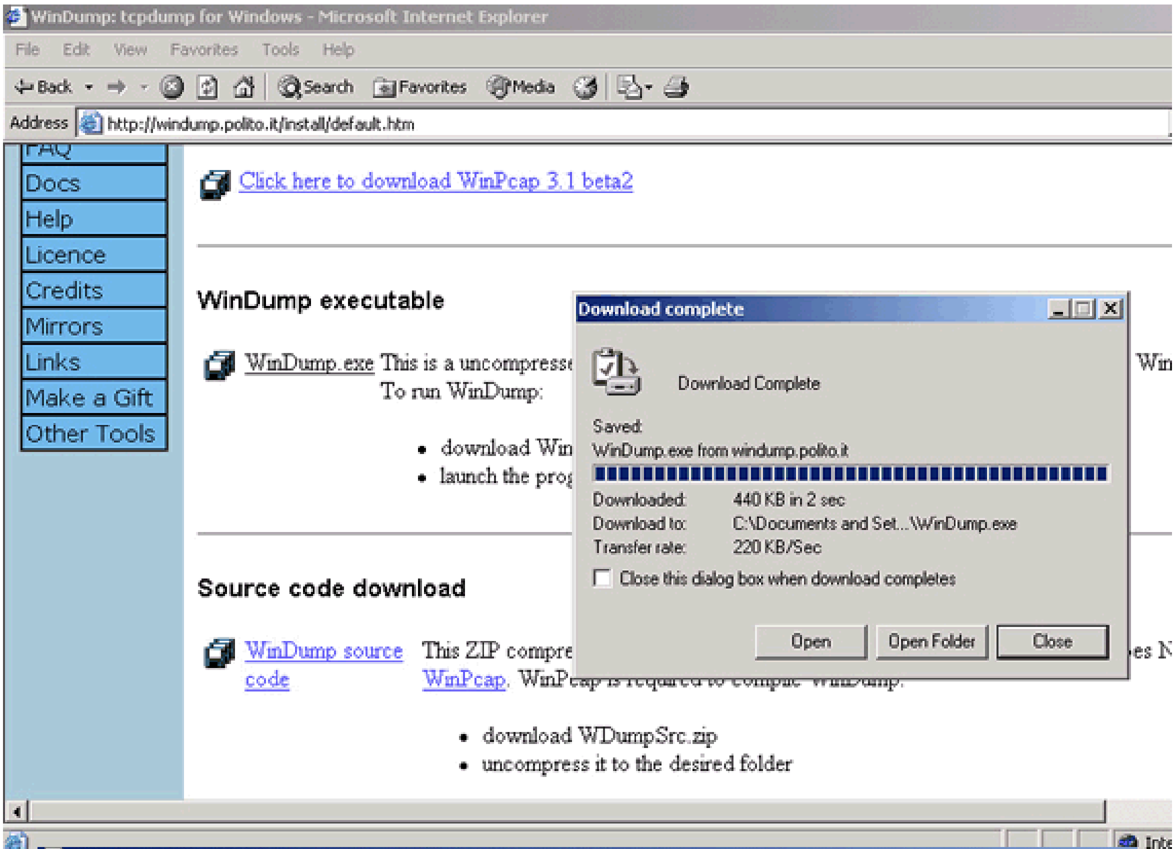
```
0003FDF8 0000 0000 0000 0000 4845 5220 2020 2020 444F 4320 1823 0344 ........HER     DOC .#.D
0003FE10 5931 5931 0000 0444 5931 0200 004E 0000 4845 5920 2020 2020 Y1Y1...DY1...N..HEY
0003FE28 444F 4320 18BA 0346 5A31 5A31 0000 0546 5A31 1600 004E 0000 DOC ...FZ1Z1...FZ1...N..
0003FE40 E565 0074 0061 005F 0033 000F 00F8 2E00 6500 7800 6500 0000 .e.t.a._.3......e.x.e...
0003FE58 FFFF 0000 FFFF FFFF E557 0069 006E 0050 0063 000F 00F8 6100 .........W.i.n.P.c....a.
0003FE70 7000 5F00 3300 5F00 3100 0000 5F00 6200 E549 4E50 4341 7E31 p._.3._.1..._.b..INPCA~1
0003FE88 4558 4520 003F FB82 5B31 5B31 0000 FC82 5B31 0000 0000 0000 EXE .?..[1[1....[1......
0003FEA0 E565 0074 0061 005F 0033 000F 00F8 2E00 6500 7800 6500 0000 .e.t.a._.3......e.x.e...
0003FEB8 FFFF 0000 FFFF FFFF E557 0069 006E 0050 0063 000F 00F8 6100 .........W.i.n.P.c....a.
0003FED0 7000 5F00 3300 5F00 3100 0000 5F00 6200 E549 4E50 4341 7E31 p._.3._.1..._.b..INPCA~1
0003FEE8 4558 4520 003F FB82 5B31 5C31 0000 F982 5B31 2A00 B269 0700 EXE .?..[1\1....[1*..i..
0003FF00 E557 0069 006E 0044 0075 000F 0054 6D00 7000 2E00 6500 7800 .W.i.n.D.u...Tm.p...e.x.
0003FF18 6500 0000 0000 FFFF E549 4E44 554D 5020 4558 4520 001B 0283 e........INDUMP EXE ....
0003FF30 5B31 5B31 0000 0383 5B31 0000 0000 0000 E557 0069 006E 0044 [1[1....[1.......W.i.n.D
0003FF48 0075 000F 0054 6D00 7000 2E00 6500 7800 6500 0000 0000 FFFF .u...Tm.p...e.x.e.......
0003FF60 E549 4E44 554D 5020 4558 4520 001B 0283 5B31 5C31 0000 0183 .INDUMP EXE ....[1\1....
0003FF78 5B31 0502 00E0 0600 E541 5054 5552 4520 2020 2020 083D 0C59 [1.......APTURE      .=.Y
0003FF90 5C31 5C31 0000 6059 5C31 BD03 40CF 0000 E541 5020 2020 2020 \1\1..`Y\1..@....AP
0003FFA8 4749 4620 183E 365A 5C31 5C31 0000 375A 5C31 0000 0000 0000 GIF .>6Z\1\1..7Z\1......
0003FFC0 E541 5020 2020 2020 4749 4620 183E 365A 5C31 5C31 0000 375A .AP      GIF .>6Z\1\1..7Z
0003FFD8 5C31 F103 6E22 0000 434F 4646 4545 2020 444F 4320 182A 179B \1..n"..COFFEE  DOC .*..
0003FFF0 5C31 5C31 0000 189B 5C31 2A00 004E 0000 0000 0000 0000 0000 \1\1....\1*..N..........
```

Also, since “Coffee.doc” is 19,968 (0x4e00) bytes and “WinPcap_3_1_beta_3.exe” is 485,810 bytes (0x769b2) in logical size, the first 39 sectors (approximately 4.1%) of “WinPcap_3_1_beta_3.exe” was overwritten by “Coffee.doc”. the slack spaces of “Coffee.doc” at the 40th sector is thus part of the deleted “WinPcap_3_1_beta_3.exe”.

Therefore, if the “WinPcap_3_1_beta_3.exe” we recovered from the IMAGE is indeed the WinPcap installer program, the recovered binaries will be identical to the genuine “WinPcap_3_1_beta_3.exe” starting from the 40th sector and on.

15. Genuine WinPcap and WinDump were downloaded and compared against files recovered from the IMAGE.

Genuine WinPcap 3.1 beta 3 and WinDump 3.8.3 beta were downloaded from the official download site. The md5 values were “4511ee3b4e5d8150c035a140dfba72c0” and “79375b77975aa53a1b0507496107bff7” respectively.


WinDump: tcpdump for Windows - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://windump.polito.it/install/default.htm
FAQ
Docs
Help
Licence
Credits
Mirrors
Links
Make a Gift
Other Tools

Click here to download WinPcap 3.1 beta2

WinDump executable

WinDump.exe This is a uncompresse… Win
To run WinDump:

- download Win…
- launch the prog…

Source code download

WinDump source code This ZIP compre… …es N…
WinPcap. WinPcap is required to compile WinDump.

- download WDumpSrc.zip
- uncompress it to the desired folder

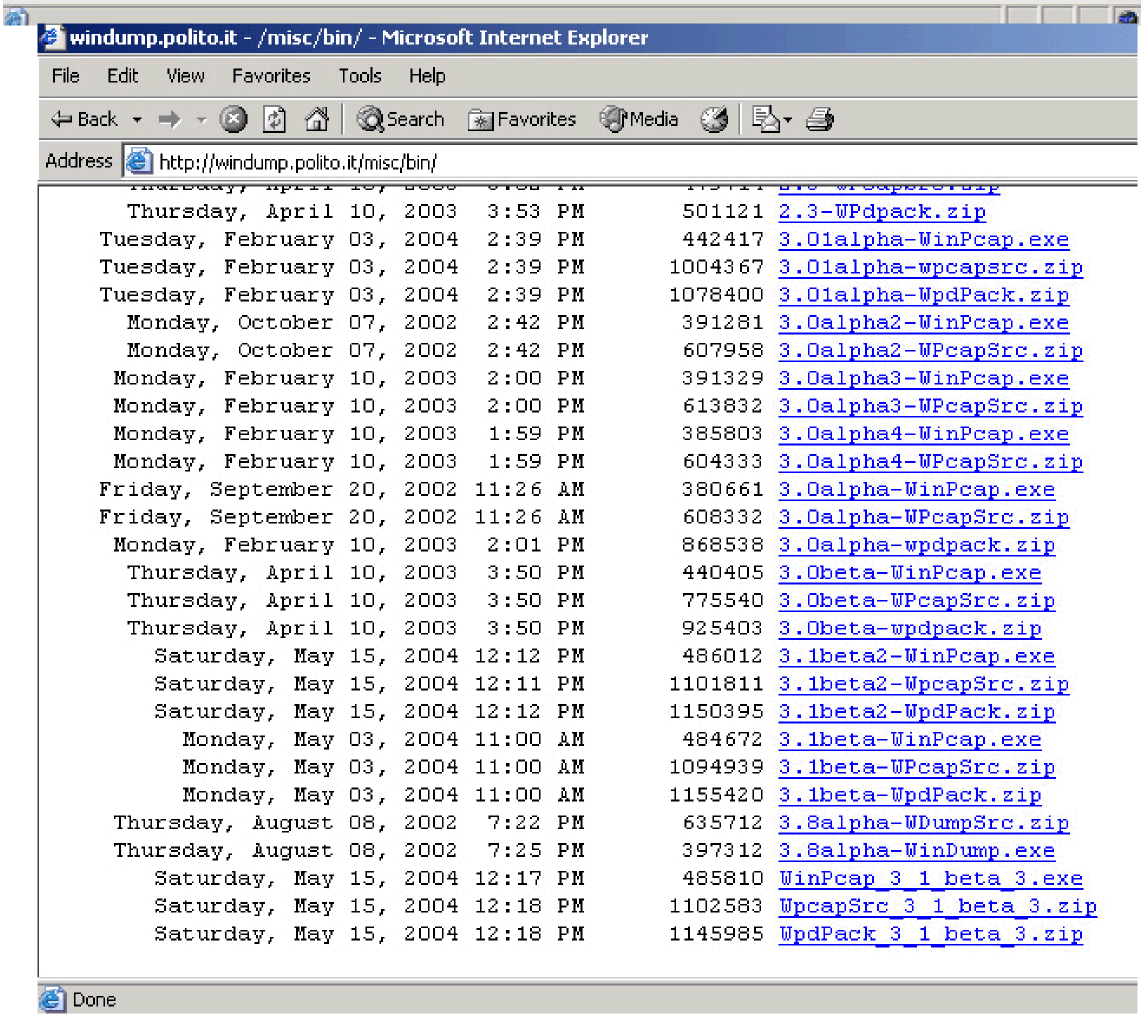
Download complete

Download Complete

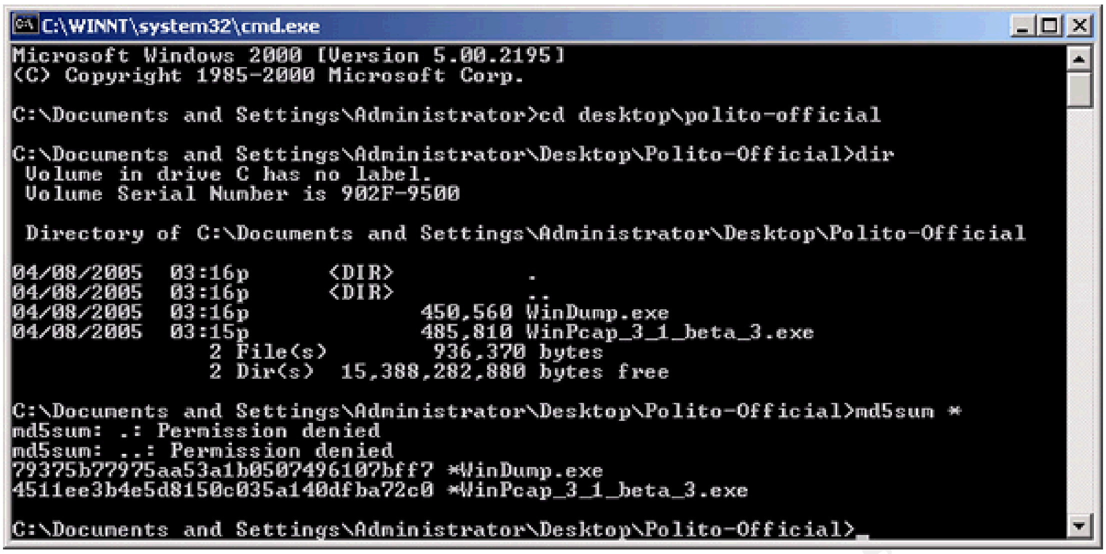
Saved:
WinDump.exe from windump.polito.it

Downloaded: 440 KB in 2 sec
Download to: C:\Documents and Set...\WinDump.exe
Transfer rate: 220 KB/Sec

□ Close this dialog box when download completes


windump.polito.it - /misc/bin/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://windump.polito.it/misc/bin/
Done

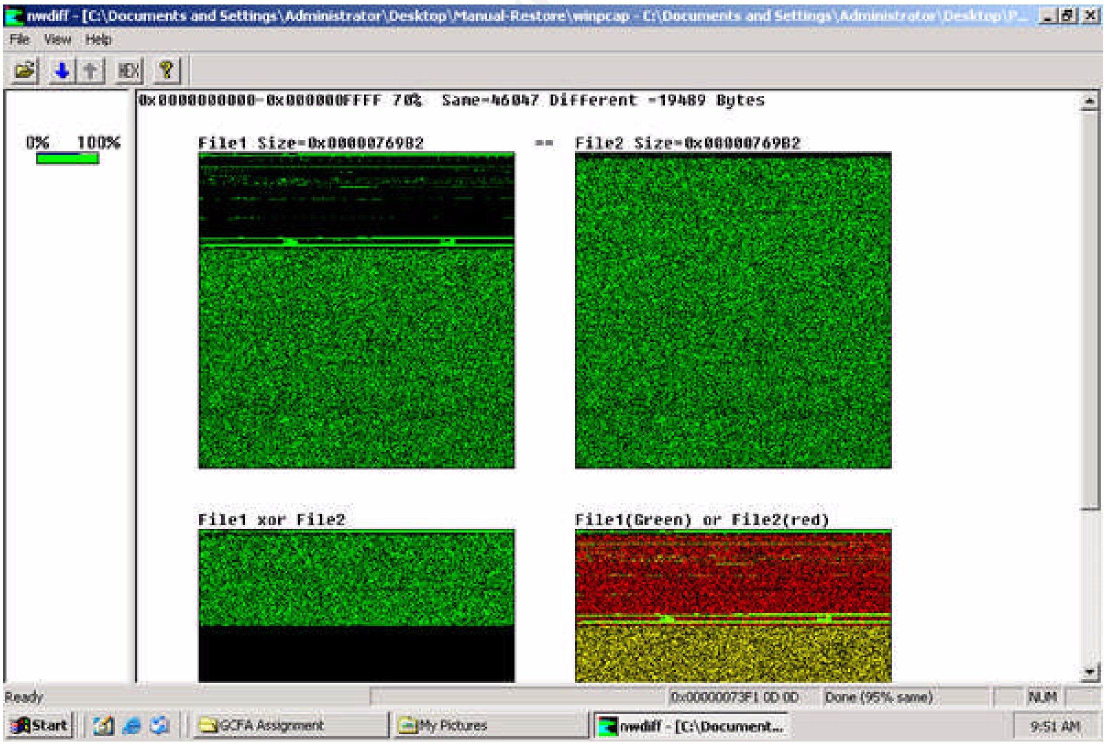
```
  Thursday, April 10, 2003  3:53 PM      501121 2.3-WPdpack.zip
 Tuesday, February 03, 2004  2:39 PM      442417 3.01alpha-WinPcap.exe
 Tuesday, February 03, 2004  2:39 PM     1004367 3.01alpha-wpcapsrc.zip
 Tuesday, February 03, 2004  2:39 PM     1078400 3.01alpha-WpdPack.zip
  Monday, October 07, 2002  2:42 PM      391281 3.0alpha2-WinPcap.exe
  Monday, October 07, 2002  2:42 PM      607958 3.0alpha2-WPcapSrc.zip
 Monday, February 10, 2003  2:00 PM      391329 3.0alpha3-WinPcap.exe
 Monday, February 10, 2003  2:00 PM      613832 3.0alpha3-WPcapSrc.zip
 Monday, February 10, 2003  1:59 PM      385803 3.0alpha4-WinPcap.exe
 Monday, February 10, 2003  1:59 PM      604333 3.0alpha4-WPcapSrc.zip
Friday, September 20, 2002 11:26 AM      380661 3.0alpha-WinPcap.exe
Friday, September 20, 2002 11:26 AM      608332 3.0alpha-WPcapSrc.zip
 Monday, February 10, 2003  2:01 PM      868538 3.0alpha-wpdpack.zip
  Thursday, April 10, 2003  3:50 PM      440405 3.0beta-WinPcap.exe
  Thursday, April 10, 2003  3:50 PM      775540 3.0beta-WPcapSrc.zip
  Thursday, April 10, 2003  3:50 PM      925403 3.0beta-wpdpack.zip
    Saturday, May 15, 2004 12:12 PM      486012 3.1beta2-WinPcap.exe
    Saturday, May 15, 2004 12:11 PM     1101811 3.1beta2-WpcapSrc.zip
    Saturday, May 15, 2004 12:12 PM     1150395 3.1beta2-WpdPack.zip
      Monday, May 03, 2004 11:00 AM      484672 3.1beta-WinPcap.exe
      Monday, May 03, 2004 11:00 AM     1094939 3.1beta-WPcapSrc.zip
      Monday, May 03, 2004 11:00 AM     1155420 3.1beta-WpdPack.zip
 Thursday, August 08, 2002  7:22 PM      635712 3.8alpha-WDumpSrc.zip
 Thursday, August 08, 2002  7:25 PM      397312 3.8alpha-WinDump.exe
    Saturday, May 15, 2004 12:17 PM      485810 WinPcap_3_1_beta_3.exe
    Saturday, May 15, 2004 12:18 PM     1102583 WpcapSrc_3_1_beta_3.zip
    Saturday, May 15, 2004 12:18 PM     1145985 WpdPack_3_1_beta_3.zip
```



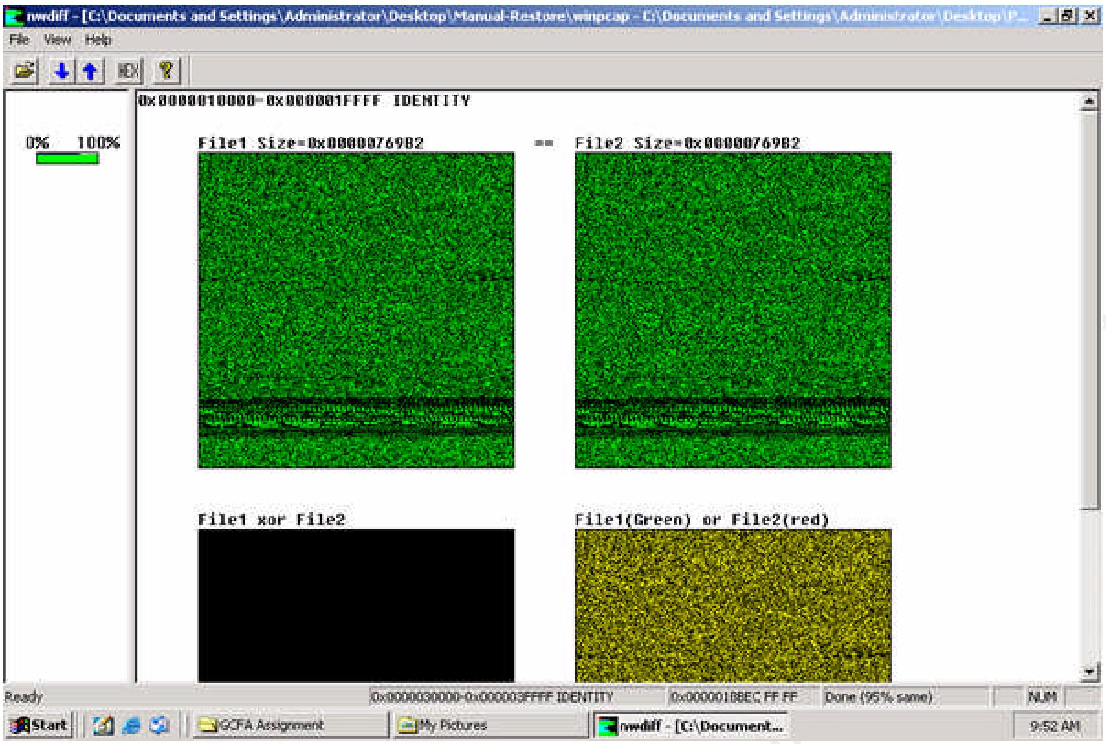
```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator>cd desktop\polito-official

C:\Documents and Settings\Administrator\Desktop\Polito-Official>dir
 Volume in drive C has no label.
 Volume Serial Number is 902F-9500

 Directory of C:\Documents and Settings\Administrator\Desktop\Polito-Official

04/08/2005  03:16p      <DIR>          .
04/08/2005  03:16p      <DIR>          ..
04/08/2005  03:16p             450,560 WinDump.exe
04/08/2005  03:15p             485,810 WinPcap_3_1_beta_3.exe
               2 File(s)        936,370 bytes
               2 Dir(s)  15,388,282,880 bytes free

C:\Documents and Settings\Administrator\Desktop\Polito-Official>md5sum *
md5sum: .: Permission denied
md5sum: ..: Permission denied
79375b77975aa53a1b0507496107bff7 *WinDump.exe
4511ee3b4e5d8150c035a140dfba72c0 *WinPcap_3_1_beta_3.exe

C:\Documents and Settings\Administrator\Desktop\Polito-Official>_
```

The MD5 values between the genuine and the recovered files were compared, it was identified that the “WinDump.exe” in the IMAGE is a genuine version of WinDump 3.8.3 beta.

A binary comparison between the genuine “WinPcap_3_1_beta_3.exe” and our recovered image was done using NWDiff. It was identified that the two files to be **95%** identical (shown in the status bar of NWDIFF); for the data between 0x0 – 0xFFFF alone, the two files are **70%** identical; the rest of the file from 0x10000 and afteward are identical to each other. A graphical representation of “File1 xor File2” (lower left) and “File1 or File2” (lower right) indicated that all differences are located at the beginning of the files. It is thus safe to conclude that the recovered “WinPcap_3_1_beta_3.exe” is a genuine version of WinPCap 3.1 Beta 3.



```
0x0000000000-0x000000FFFF 70%  Same=46047 Different =19489 Bytes
```



```
nwdiff - [C:\Documents and Settings\Administrator\Desktop\Manual-Restore\winpcap - C:\Documents and Settings\Administrator\Desktop\P...
0x0000010000-0x000001FFFF IDENTITY
File1 Size=0x00000769B2    ==    File2 Size=0x00000769B2
File1 xor File2                  File1(Green) or File2(red)
Ready    0x0000030000-0x000003FFFF IDENTITY    0x000001BBEC FF FF    Done (95% same)
```

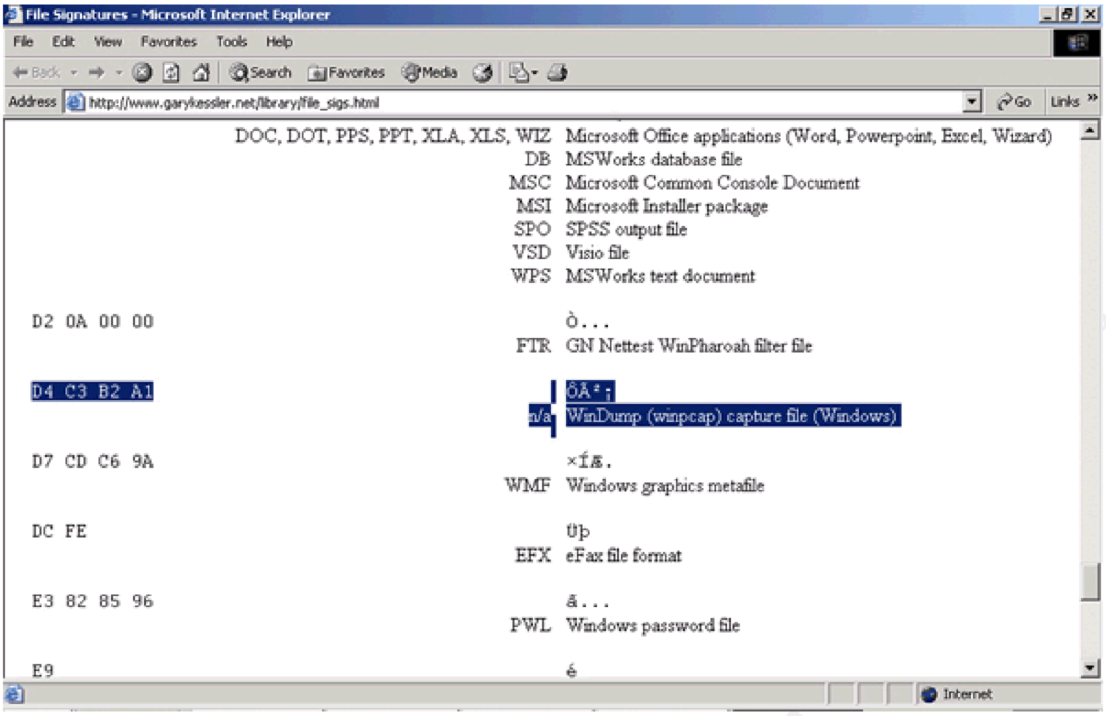
As part of the recovered file has been overwritten, and with the tools at hand, performing a binary comparison consume less time and provides a good enough confirmation on the identity of the unknown WinPcap recovered in the IMAGE.

In part, our comparison has been made easy as Microsoft Word documents carries empty spaces (allocated to the containers – a feature of "component document"), while the compressed installer programs are more packed and exhibits a different pattern.

A better approach could be extracting data in a genuine version of WinPcap from the 40th sector and on, and compare it against the portion of WinPcap not overwritten using MD5 comparison. Nevertheless, having read through and validated the output of NWDIFF, the investigator has sufficient confidence on the current interpretation.

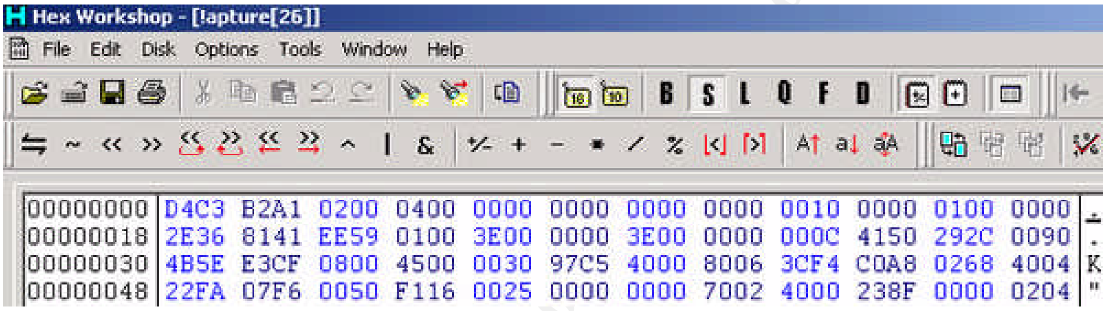
16. The file signature of "!apture" was reviewed and matched against information from the Internet

The file signature database (http://www.garykessler.net/library/file_sigs.html) was visited, and it was confirmed that a file beginning with "D4C3B2A1" to be a WinPcap capture file.
The first 4 bytes in "!apture" were then reviewed and confirmed the file to be a packet capture file.



File Signatures - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.garykessler.net/library/file_sigs.html
Go Links
Internet

```
                           DOC, DOT, PPS, PPT, XLA, XLS, WIZ  Microsoft Office applications (Word, Powerpoint, Excel, Wizard)
                                                         DB  MSWorks database file
                                                        MSC  Microsoft Common Console Document
                                                        MSI  Microsoft Installer package
                                                        SPO  SPSS output file
                                                        VSD  Visio file
                                                        WPS  MSWorks text document

D2 0A 00 00                                                  Ò...
                                                        FTR  GN Nettest WinPharoah filter file

D4 C3 B2 A1                                                  ÔÃ²¡
                                                        n/a  WinDump (winpcap) capture file (Windows)

D7 CD C6 9A                                                  ×ÍÆ.
                                                        WMF  Windows graphics metafile

DC FE                                                        Üþ
                                                        EFX  eFax file format

E3 82 85 96                                                  ã...
                                                        PWL  Windows password file

E9                                                           é
```



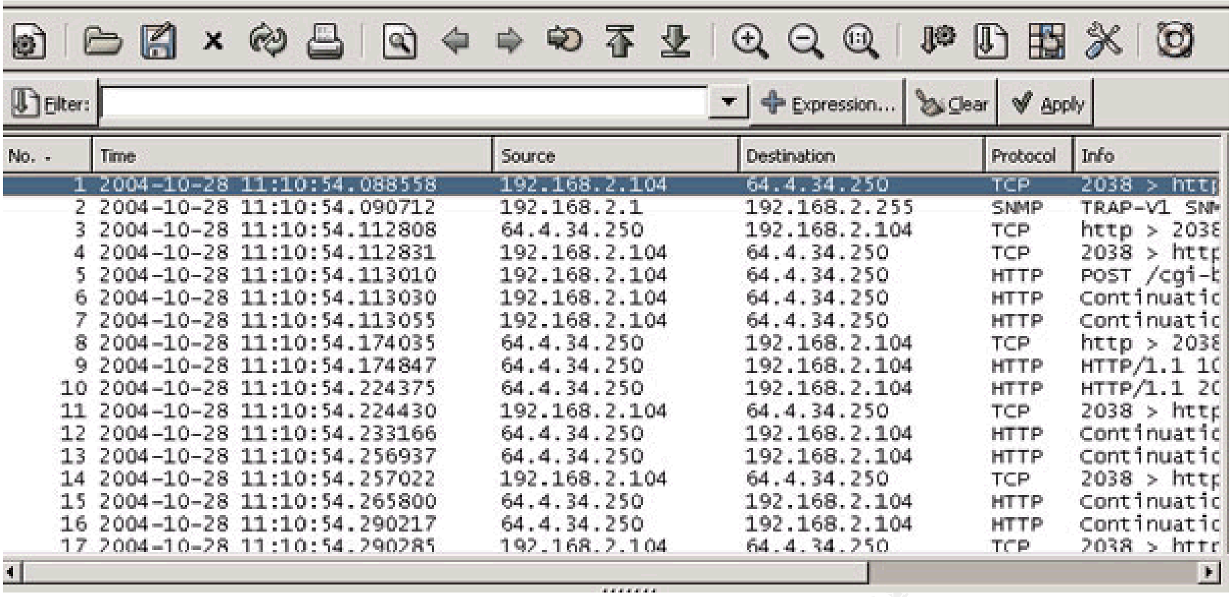
Hex Workshop - [!apture[26]]
File Edit Disk Options Tools Window Help

```
00000000 D4C3 B2A1 0200 0400 0000 0000 0000 0000 0010 0000 0100 0000
00000018 2E36 8141 EE59 0100 3E00 0000 3E00 0000 000C 4150 292C 0090
00000030 4B5E E3CF 0800 4500 0030 97C5 4000 8006 3CF4 C0A8 0268 4004
00000048 22FA 07F6 0050 F116 0025 0000 0000 7002 4000 238F 0000 0204
```

17. Network stream of information was extracted from "!apture"

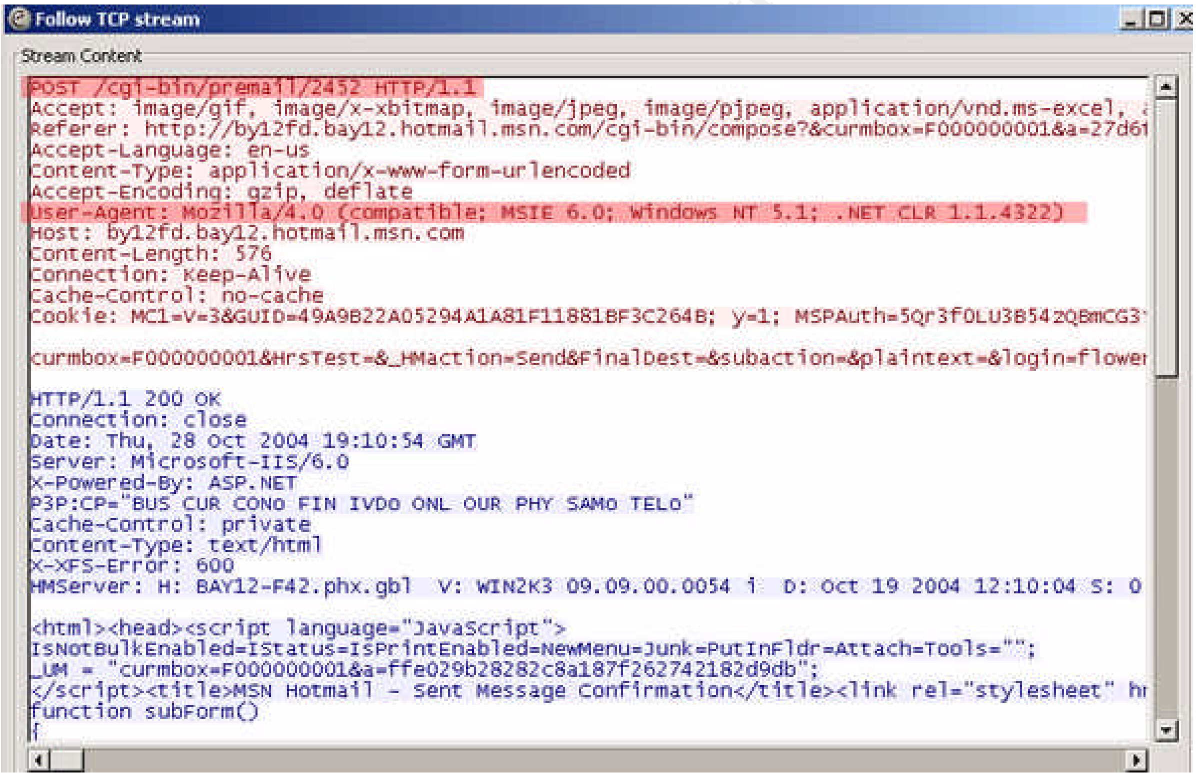
Ethereal version 0.10.8 was installed to the forensic workstation.

The file "!apture" was opened with Ethereal, it was identified that the capture is about 1 second long in time from Oct 28 2004 11:10:54 – 11:10:55.



No.	Time	Source	Destination	Protocol	Info
1	2004-10-28 11:10:54.088558	192.168.2.104	64.4.34.250	TCP	2038 > htt
2	2004-10-28 11:10:54.090712	192.168.2.1	192.168.2.255	SNMP	TRAP-V1 SN
3	2004-10-28 11:10:54.112808	64.4.34.250	192.168.2.104	TCP	http > 203
4	2004-10-28 11:10:54.112831	192.168.2.104	64.4.34.250	TCP	2038 > htt
5	2004-10-28 11:10:54.113010	192.168.2.104	64.4.34.250	HTTP	POST /cgi-b
6	2004-10-28 11:10:54.113030	192.168.2.104	64.4.34.250	HTTP	Continuati
7	2004-10-28 11:10:54.113055	192.168.2.104	64.4.34.250	HTTP	Continuati
8	2004-10-28 11:10:54.174035	64.4.34.250	192.168.2.104	TCP	http > 203
9	2004-10-28 11:10:54.174847	64.4.34.250	192.168.2.104	HTTP	HTTP/1.1 10
10	2004-10-28 11:10:54.224375	64.4.34.250	192.168.2.104	HTTP	HTTP/1.1 20
11	2004-10-28 11:10:54.224430	192.168.2.104	64.4.34.250	TCP	2038 > htt
12	2004-10-28 11:10:54.233166	64.4.34.250	192.168.2.104	HTTP	Continuati
13	2004-10-28 11:10:54.256937	64.4.34.250	192.168.2.104	HTTP	Continuati
14	2004-10-28 11:10:54.257022	192.168.2.104	64.4.34.250	TCP	2038 > htt
15	2004-10-28 11:10:54.265800	64.4.34.250	192.168.2.104	HTTP	Continuati
16	2004-10-28 11:10:54.290217	64.4.34.250	192.168.2.104	HTTP	Continuati
17	2004-10-28 11:10:54.290285	192.168.2.104	64.4.34.250	TCP	2038 > htt

A search for “flowergirl” was performed in the stream and one stream with HTTP data matching “flowergirl” was found. The stream of data was extracted to “capture1.txt” with md5 value of “1d9f54ecb95797bb5a31aae923c91b41”.

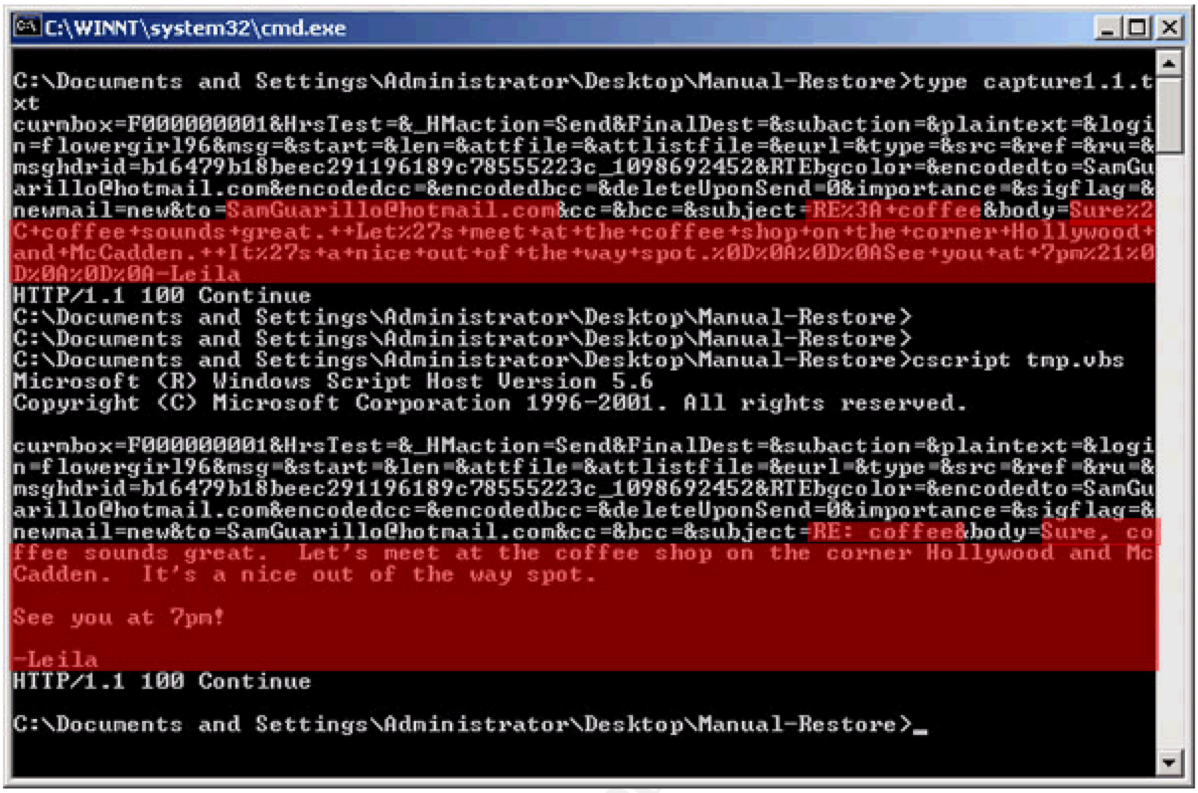


```
POST /cgi-bin/premail/2452 HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, a
Referer: http://by12fd.bay12.hotmail.msn.com/cgi-bin/compose?&curmbox=F000000001&a=27d61
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)
Host: by12fd.bay12.hotmail.msn.com
Content-Length: 576
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: MC1=V=3&GUID=49A9B22A05294A1A81F11881BF3C264B; y=1; MSPAuth=5Qr3f0LU3B542QBmCG3

curmbox=F000000001&HrsTest=&_HMaction=Send&FinalDest=&subaction=&plaintext=&login=flower

HTTP/1.1 200 OK
Connection: close
Date: Thu, 28 Oct 2004 19:10:54 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
P3P:CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo"
Cache-Control: private
Content-Type: text/html
X-XFS-Error: 600
HMServer: H: BAY12-F42.phx.gbl  V: WIN2K3 09.09.00.0054 i  D: Oct 19 2004 12:10:04 S: 0

<html><head><script language="JavaScript">
IsNotBulkEnabled=IStatus=IsPrintEnabled=NewMenu=Junk=PutInFldr=Attach=Tools="";
_UM = "curmbox=F000000001&a=ffe029b28282c8a187f262742182d9db";
</script><title>MSN Hotmail - Sent Message Confirmation</title><link rel="stylesheet" hr
function subForm()
{
```

The network stream in “capture1.txt” was reviewed and it was identified to include i) an email reply from flowergirl96@hotmail.com to SamGuarillo@hotmail.com using HTTP Post method to Hotmail (httpmail); and ii) a response HTML page from the Hotmail server.

The email reply being “posted” to the hotmail server was saved as “capture1.1.txt”, a message written by flowergirl96@hotmail.com on the topic of having coffee with

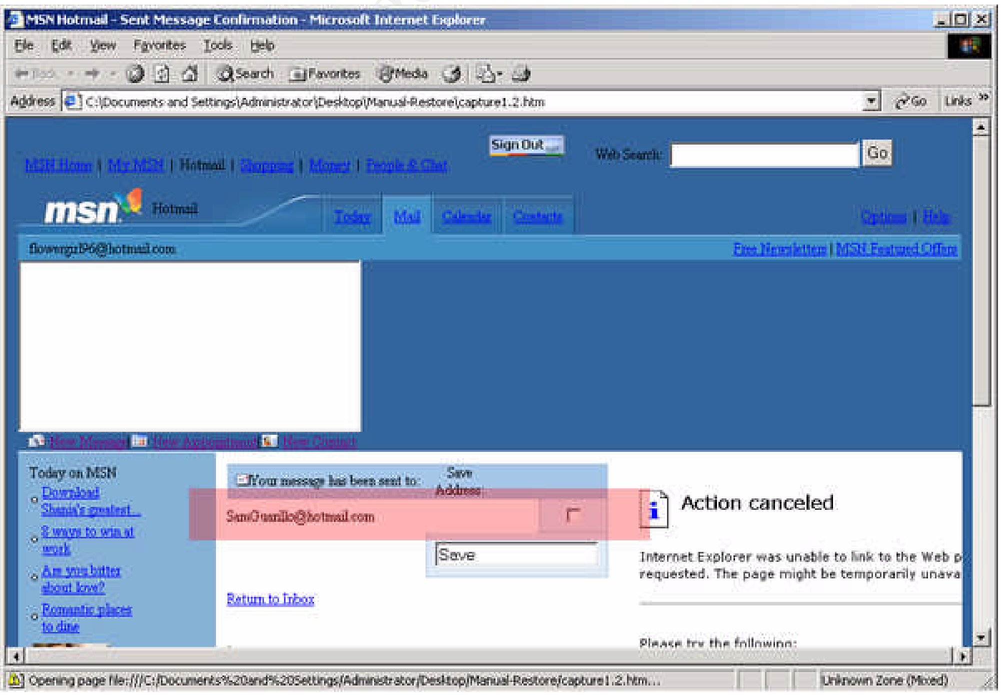
Sam at Hollywood & McCadden at 7:00PM of Oct 28 was identified when the stream was decoded. The location is Hollywood and McCadden where the recovered map "!ap.gif" referred.



C:\WINNT\system32\cmd.exe

```
C:\Documents and Settings\Administrator\Desktop\Manual-Restore>type capture1.1.t
xt
curmbox=F000000001&HrsTest=&_HMaction=Send&FinalDest=&subaction=&plaintext=&logi
n=flowergirl96&msg=&start=&len=&attfile=&attlistfile=&eurl=&type=&src=&ref=&ru=&
msghdrid=b16479b18beec291196189c78555223c_1098692452&RTEbgcolor=&encodedto=SamGu
arillo@hotmail.com&encodedcc=&encodedbcc=&deleteUponSend=0&importance=&sigflag=&
newmail=new&to=SamGuarillo@hotmail.com&cc=&bcc=&subject=RE%3A+coffee&body=Sure%2
C+coffee+sounds+great.++Let%27s+meet+at+the+coffee+shop+on+the+corner+Hollywood+
and+McCadden.++It%27s+a+nice+out+of+the+way+spot.%0D%0A%0D%0ASee+you+at+7pm%21%0
D%0A%0D%0A-Leila
HTTP/1.1 100 Continue
C:\Documents and Settings\Administrator\Desktop\Manual-Restore>
C:\Documents and Settings\Administrator\Desktop\Manual-Restore>
C:\Documents and Settings\Administrator\Desktop\Manual-Restore>cscript tmp.vbs
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

curmbox=F000000001&HrsTest=&_HMaction=Send&FinalDest=&subaction=&plaintext=&logi
n=flowergirl96&msg=&start=&len=&attfile=&attlistfile=&eurl=&type=&src=&ref=&ru=&
msghdrid=b16479b18beec291196189c78555223c_1098692452&RTEbgcolor=&encodedto=SamGu
arillo@hotmail.com&encodedcc=&encodedbcc=&deleteUponSend=0&importance=&sigflag=&
newmail=new&to=SamGuarillo@hotmail.com&cc=&bcc=&subject=RE: coffee&body=Sure, co
ffee sounds great.  Let's meet at the coffee shop on the corner Hollywood and Mc
Cadden.  It's a nice out of the way spot.

See you at 7pm!

-Leila
HTTP/1.1 100 Continue

C:\Documents and Settings\Administrator\Desktop\Manual-Restore>_
```

The HTML contents in the response stream was saved to "capture1.2.htm" and opened in an Internet Explorer; it showed a hotmail page requesting flowergirl96 to add SamGuarillo@hotmail.com into her address book.



MSN Hotmail - Sent Message Confirmation - Microsoft Internet Explorer

Address C:\Documents and Settings\Administrator\Desktop\Manual-Restore\capture1.2.htm

flowergirl96@hotmail.com

Your message has been sent to: SamGuarillo@hotmail.com

Save Address

Return to Inbox

Action canceled

Internet Explorer was unable to link to the Web p
requested. The page might be temporarily unava

Please try the following:

Opening page file:///C:/Documents%20and%20Settings/Administrator/Desktop/Manual-Restore/capture1.2.htm...

Unknown Zone (Mixed)

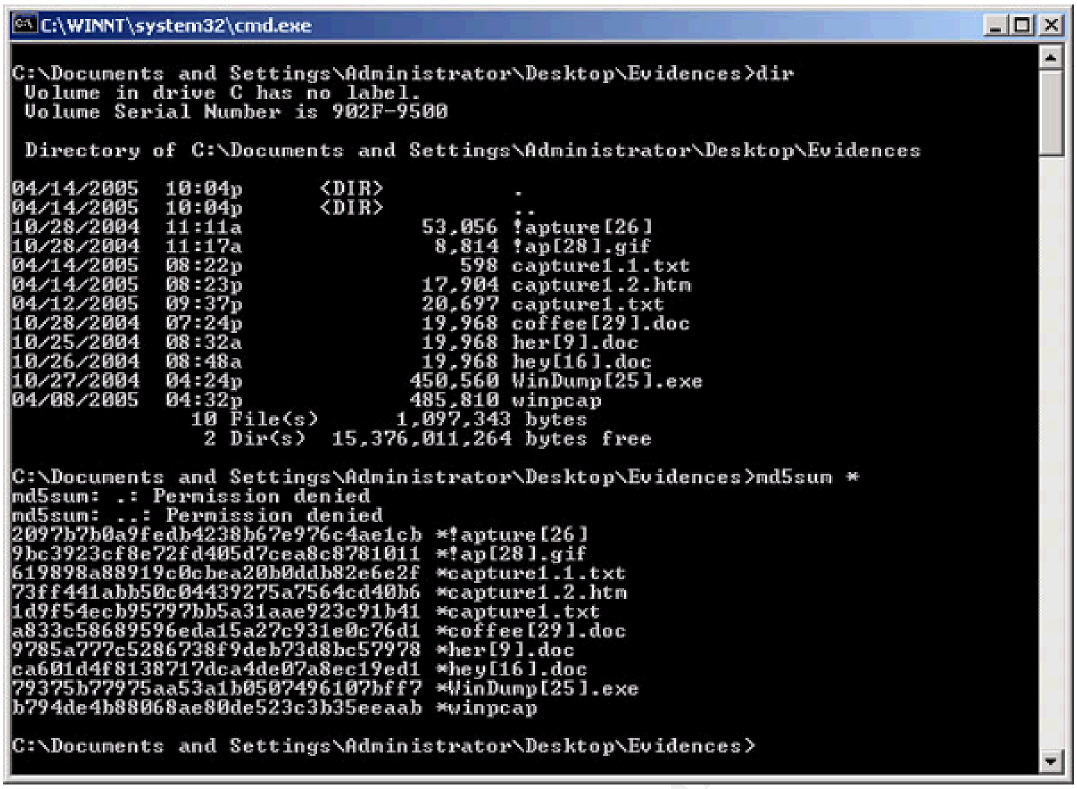
At this part of the investigation, Ethereal has been used to decode the content in the packet capture file. Since httpmail (and a number of other network protocols) do not encrypt mail contents, they can be spied by any workstations connected to the network. In this case, the email and html contents have been spied the use of Windump.

With reference to the content of the email from Ms. Conlay to “Sam”, one can believe the last message “Coffee.doc” found in the IMAGE was written by Mr. Lawrence at 7:24PM of Oct 28, 2004 after he had seen Ms. Conlay with “Sam” in the coffee shop at Hollywood & McCadden at 7:00PM of Oct 28, 2004. After Mr. Lawrence was rejected by Ms. Conlay on Oct 25 and Oct 26, he downloaded and installed a network sniffer “WinDump 3.8.3 Beta” on Oct 27 4pm and spied on network communications to and from Ms. Conlay’s workstation. On Oct 28 11:10, he captured a private email of Ms. Conlay to “Sam”, learning that Ms. Conlay will meet “Sam” at Hollywood area, he downloaded a map of the neighborhood at 11:17, and piggybacked Ms. Conlay at the same evening.

The following questions remained, nevertheless:

1. Is Leila’s workstation at work running WinXP (NT5.1) and MSIE6 as highlighted in the http header above? Is the IP address 192.168.2.104 (That is, is the workstation being “captured” correct)?
2. How did Mr. Lawrence learnt the very second when Leila is sending her email to Sam? How could Mr. Lawrence decode Ms. Leila’ private email from the capture only 8 minutes after its being recorded? Is there a more complete version of capture file located at another location?
3. Socially speaking, why is SamGuarillo not in Flowergirl96’s address book if they known each other well? Is this a coincidence?

18. Evidences collected were consolidated (by re-exporting from FTK and performing file system copies) to ease submission.



```
C:\Documents and Settings\Administrator\Desktop\Evidences>dir
 Volume in drive C has no label.
 Volume Serial Number is 902F-9500

 Directory of C:\Documents and Settings\Administrator\Desktop\Evidences

04/14/2005  10:04p      <DIR>          .
04/14/2005  10:04p      <DIR>          ..
10/28/2004  11:11a              53,056 !apture[26]
10/28/2004  11:17a               8,814 !ap[28].gif
04/14/2005  08:22p                 598 capture1.1.txt
04/14/2005  08:23p              17,904 capture1.2.htm
04/12/2005  09:37p              20,697 capture1.txt
10/28/2004  07:24p              19,968 coffee[29].doc
10/25/2004  08:32a              19,968 her[9].doc
10/26/2004  08:48a              19,968 hey[16].doc
10/27/2004  04:24p             450,560 WinDump[25].exe
04/08/2005  04:32p             485,810 winpcap
              10 File(s)      1,097,343 bytes
               2 Dir(s)  15,376,011,264 bytes free

C:\Documents and Settings\Administrator\Desktop\Evidences>md5sum *
md5sum: .: Permission denied
md5sum: ..: Permission denied
2097b7b0a9fedb4238b67e976c4ae1cb *!apture[26]
9bc3923cf8e72fd405d7cea8c8781011 *!ap[28].gif
619898a88919c0cbea20b0ddb82e6e2f *capture1.1.txt
73ff441abb50c04439275a7564cd40b6 *capture1.2.htm
1d9f54ecb95797bb5a31aae923c91b41 *capture1.txt
a833c58689596eda15a27c931e0c76d1 *coffee[29].doc
9785a777c5286738f9deb73d8bc57978 *her[9].doc
ca601d4f8138717dca4de07a8ec19ed1 *hey[16].doc
79375b77975aa53a1b0507496107bff7 *WinDump[25].exe
b794de4b88068ae80de523c3b35eeaab *winpcap

C:\Documents and Settings\Administrator\Desktop\Evidences>
```

VI. Investigative Leads and Other Recommendations

A number of evidences supported the claims by Ms. Conlay against Mr. Lawrence. Nevertheless, a number of concerns have been identified during the investigation. While each of them may not be significant, they suggest the current scenario be investigated further for a fair judgment on Mr. Lawrence.

A. Legally speaking, the investigator concern if the USB drive obtained could be used as approved evidence should this case is bring up to court. In part, the personal USB drive was neither obtained with Mr. Lawrence's consent, nor the corporate has been granted the authority required to seize private property during security investigation. Moreover, although our security administrator had found the USB Drive in Mr. Lawrence's cubicle, there is no evidence that Mr. Lawrence owns the USB Drive (other than his name appeared in the content of the drive). Lastly, even if Mr. Lawrence owns the USB Drive, he may not be the only user of the drive given the mobility of the USB Drive.

   Additional investigations, therefore, shall be carried out to confirm Mr. Lawrence's presence in the "crime scene" when the unethical acts (i.e. unauthorized sniffing of another staff's private email) were performed using company property (i.e. Mr. Lawrence's workstation at work). The following investigations are recommended to identify if Mr. Lawrence had downloaded, installed and used the network sniffer programs (Windump and WinPcap) and captured the private email of Ms. Conlay:

1. Review the attendance and corporate network sign-on record.

   To identify if Mr. Lawrence did use corporate workstation(s) including notebook computer to perform the packet capture, it is suggested to review Mr. Lawrence's attendance and domain sign on record for the period from Oct 27 16:00 – 16:30 and from Oct 28 11:00 – 11:30. The investigation shall reveal workstation(s) Mr. Lawrence logon to during the captioned period, such that comprehensive forensic analysis for traces of WinDump, WinPcap and Microsoft MapPoint can be launched on the logon-ed workstation(s). Note it is possible that Mr. Lawrence downloaded the WinPcap and WinDump program at home on Oct 27; but Mr. Lawrence had to install the programs and used at least one workstation connected to the corporate network to complete the packet capture on Oct 28.

2. Review the corporate proxy log and other necessary network logs.

   The logs shall be reviewed for three purposes: i) to identify if the WinDump and WinPcap were downloaded on Oct 27 through the corporate network; ii) to identify if Ms. Conlay's had connected to Hotmail on Oct 28; and iii) to identify if MapPoint server service has been accessed and queried on Oct 28.

3. Perform comprehensive forensic analysis on workstations used by Mr. Lawrence.

   The purpose of the analysis is to search for copies of evidences identified in the current forensic exercise. As described earlier, Mr. Lawrence requires at least one workstation connected to the corporate network to complete the packet capture. Thus, traces of installations of Windump and Winpcap will be the subject of investigation; in addition, traces of usage of the MapPoint server service and Windump shall exist on this workstation.

4. During the above investigations, it is recommended to refrain Mr. Lawrence from access to corporate resources according to the security guideline. This will prevent further damage and/or elimination of evidences should Mr. Lawrence did performed the unethical acts.

B. Technically speaking, the following points have been identified during the investigation, attempts to answer them shall be considered in the investigations recommended in (A) above:

1. There is an MBR in the USB drive, which is not a common practice; also the disk was so clean and appeared it may not have been used before (Section V (C), Step 5).
2. There are duplicate entries in the File Allocation Table (Section V (C), Step 8).
3. The packet capture file ("!apture") captured the exact second when Ms. Leila sent her private email to SamGuarillo (Section V (C), Step 10 & 17), this is unlikely to occur by chance.

C. For the corporate, a number of alerts have been identified in the investigation:

1. Staff may use unauthorized hardware/software within the corporate network.

   According to the corporate IT security policy, a staff is generally not allowed to use privately owned hardware/software at work. The reason is the IT security of personal hardware/software may not be up to par with the corporate standard, and cause additional risks to loss of or unauthorized access to corporate data.

   In this case, the USB Drive could have stored sensitive sales information (since Mr. Lawrence is of sales department). If it was passed to an outsider (including a competitor) either accidentally or intentionally, by Mr. Lawrence himself or by a third person, great damages could have been incurred to the corporate in tangible or intangible terms.

2. Staff may participate in unethical network sniffing.

   In accordance to corporate IT security policy, use of network sniffer is prohibited other than on authorized occasions. The policy must be enforced strictly.

   In one hand, network sniffing is a powerful tool to troubleshoot network problem; on the other hand, it could be an evil tool when used for an unethical purpose. In this case, use of a network sniffer has been detected to offend the personal privacy of Ms. Leila, which could mean another civil court case for the corporate if it is not handled correctly. In addition, a staff may be able to capture sensitive and unauthorized information from the network, and may cause additional damage to the corporate.

For this instance, the investigator would recommend investigations to whether Mr. Lawrence had used a network sniffer to capture restricted or confidential information be included in the investigations in (A) above.

VII. List of References

S.R.Haque. Microsoft Word 97 Binary File Format. 23 Jul. 2001 <http://www.aozw65.dsl.pipex.com/generator_wword8.htm>.

Recovery of Digital Evidence. 2004. Asian School of Cyber Laws. 8 Apr. 2005 <http://www.asianlaws.org/cyberlaw/library/cc/dig_evi.htm>.

Thomas Kjoernes. File Allocation Table - How It Seems To Work. 11 May 2000 <http://home.no.net/tkos/info/fat.html>.

Judd Robbins. An Explanation of Computer Forensics. 9 Sept. 2004 <http://www.computerforensics.net/forensics.htm>.

Andries Brouwer. The FAT filesystem. 20 Sept. 2002 <http://www.win.tue.nl/~aeb/linux/fs/fat/fat-1.html>

Gary C. Kessler. FILE SIGNATURES TABLE. 3 Apr. 2005 <http://www.garykessler.net/library/file_sigs.html>

Appendix I - Additional Information

Disk Concepts and Troubleshooting. 2005. Microsoft Corporation. <http://www.microsoft.com/resources/documentation/Windows/2000/server/reskit/en-us/prork/prcb_dis_zbxs.asp>

The chapter provides basic information to how a storage medium is layout to carry meaningful content. The subsections ("Master boot record" and "Boot Sector") are particular useful should a reader want to know why the investigator used a hex editor to review the disk, and the riches of information that the investigator attempted to identify.

WinDump: tcpdump for Windows. University of California, Lawrence Berkeley Laboratory. 3 May 2005. <http://windump.polito.it/>

WinPcap: the Free Packet Capture Library for Windows. University of California, Lawrence Berkeley Laboratory. 4 Nov. 2004. <http://winpcap.polito.it/>

The two web sites provide useful information on the capability of WinDump and WinPcap. In fact, the packet capture file analyzed in the assignment is simple, and cannot really demonstrate the full capability of Windump (or the damage it can do in a corporate environment), such as decoding packets in IPSec (a tunneling protocol). Interested readers may found pointers to the Sniffing FAQ by Robert Graham within WinDump "Docs" section to be useful as well.

UNERASER. File Recovery. Defining clusters chain for the deleted entry. Active@ Data Recovery Software. 5 Feb. 2005. <http://www.uneraser.com/assemble-clusters.htm>

The web site describes the general concepts and processes of recovering deleted files. The information on how to define a chain of clusters for recovery will be useful in understanding the technique used by the investigator to recover deleted files. It also provides a clue to why FTK cannot / do not automatically recover some of the binaries in the IMAGE.

Appendix II – List of Contents in the USB IMAGE

Evidence#	2
Full Path:	\her.doc
Exported to:	her[9].doc
File Type:	Microsoft Word XP Document
Created:	10/25/2004 8:32:06 AM
Accessed:	10/25/2004
Modified:	10/25/2004 8:32:08 AM
L-Size:	19968
Del:	No
Category:	Document
MD5:	9785A777C5286738F9DEB73D8BC57978

Evidence#	3
Full Path:	\hey.doc
Exported to:	hey[16].doc
File Type:	Microsoft Word XP Document
Created:	10/26/2004 8:48:06 AM
Accessed:	10/26/2004
Modified:	10/26/2004 8:48:10 AM
L-Size:	19968
Del:	No
Category:	Document
MD5:	CA601D4F8138717DCA4DE07A8EC19ED1

Evidence#	4
Full Path:	\coffee.doc
Exported to:	Coffee[29].doc
File Type:	Microsoft Word XP Document
Created:	10/28/2004 7:24:46 PM
Accessed:	10/28/2004
Modified:	10/28/2004 7:24:48 PM
L-Size:	19968
Del:	No
Category:	Document
MD5:	A833C58689596EDA15A27C931E0C76D1

Evidence#	5
Full Path:	\!apture
Exported to:	!apture[26]
File Type:	Windump Capture File
Created:	10/28/2004 11:08:24 AM
Accessed:	10/28/2004
Modified:	10/28/2004 11:11:00 AM
L-Size:	53056
Del:	Yes
Category:	Tcpdump capture variant
MD5:	2097B7B0A9FEDB4238B67E976C4AE1CB

Evidence#	5.1
Exported to:	Capture1.txt
File Type:	Extracted HTTP data stream
L-Size:	20697
MD5:	1d9f54ecb95797bb5a31aae923c91b41

Evidence#	5.1.1
Exported to:	Capture1.1.txt
File Type:	Extracted HTTP data stream
L-Size:	598
MD5:	619898a88919c0cbea20b0ddb82e6e2f

Evidence#	5.1.2
Exported to:	Capture1.2.htm
File Type:	Extracted HTTP data stream
L-Size:	17904
MD5:	73ff441abb50c04439275a7564cd40b6

Evidence#	6
Full Path:	\!ap.gif
Exported to:	!ap[28].gif
File Type:	GIF File
Created:	10/28/2004 11:17:44 AM
Accessed:	10/28/2004
Modified:	10/28/2004 11:17:46 AM
L-Size:	8814
Del:	Yes
Category:	Graphic
MD5:	9BC3923CF8E72FD405D7CEA8C8781011

Evidence#	7
Full Path:	\WinDump.exe
Exported to:	WinDump[25].exe
File Type:	WinDump 3.8.3 Beta Installer
Created:	10/27/2004 4:24:04 PM
Accessed:	10/28/2004
Modified:	10/27/2004 4:24:02 PM
L-Size:	450560
Del:	Yes
Category:	Executable
MD5:	79375B77975AA53A1B0507496107BFF7

Evidence#	8
Full Path:	\WinPcap_3_1_beta_3.exe
Exported to:	Winpcap
File Type:	Winpcap 3.1 beta 3 Installer
Created:	10/27/2004 4:23:54 PM
Accessed:	10/28/2004
Modified:	10/27/2004 4:23:50 PM
L-Size:	485810
Del:	Yes
Category:	Executable
MD5:	B794de4b88068ae80de523c3b35eeaab

Appendix III – Brief of Programs Used for Investigation

- *Microsoft Virtual PC 2004* (http://www.microsoft.com/windows/virtualpc/default.mspx)

Microsoft Virtual PC 2004 is a virtualization solution to allow a user to run multiple PC-based operating systems in a single workstation through emulation. Similar products include VMWare workstation.

- *Hex Workshop (http://www.bpsoft.com/)*

A powerful hex editor in the opinion of the investigator.

- *NWDIFF (http://www.geocities.co.jp/SiliconValley/1469/ToolNwdiff_Eng.html)*

Similar to the Microsoft WinDiff to compare two text files in GUI, NWDIFF perform comparison between two binary files in GUI.

- *VDK (http://chitchat.at.infoseek.co.jp/vmware/vdk.html)*

Virtual Disk Driver (VDK) is a driver to enable working with VMWare formatted virtual disks on a Windows host. While it has a number of limitations, it offers quick access to information in a disk image on Windows platform. The site contains a bunch of tools to work with VMWare disk images as well.

- *AccessData Forensic ToolKit (FTK) (http://www.accessdata.com/)*

AccessData FTK is actually a commercial software to perform thorough computer forensic examinations. Instead of using a wide variety of tools, FTK can be considered a "Swiss Army Knife" for an investigator. The downloadable trial version support forensic analysis on no more than 5,000 files.

- *Ethereal 0.10.8 (http://www.ethereal.com)*

Ethereal is a famous network protocol analyzer under GNU Public License (GPL), it understands a large number of protocols and includes powerful feature to simplify network flow analysis.