



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

## Interested in learning more?

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

**GCFA PRACTICAL ASSIGNMENT V 2.0**  
**OPTION 1 – ANALYSIS OF AN IMAGE PROVIDED FROM THE GIAC**  
**WEBSITE**

**PRESENTED BY: JUAN CARLOS REYES MUÑOZ**

**DATE OF SUBMISSION: 28/02/2005**

# TABLE OF CONTENTS

<a href="#"><u>Abstract</u></a>	3
<a href="#"><u>Executive Summary</u></a>	3
<a href="#"><u>Examination details</u></a>	4
<a href="#"><u>Image details</u></a>	24
<a href="#"><u>Forensic details</u></a>	27
<a href="#"><u>Program Identification</u></a>	29
<a href="#"><u>Legal Implications</u></a>	31
<a href="#"><u>Recommendations</u></a>	32
<a href="#"><u>Additional Information</u></a>	33
<a href="#"><u>References</u></a>	33

## **Abstract**

---

This paper is intended to investigate, using forensic procedures, the case stated in the GIAC Website in which an employee of a company named CC Terminals has contacted corporate security stating a potentially harassment behavior from other employee.

The document contains an executive summary of the findings as well as technical examination of one piece of evidence collected, using forensic procedures in order to demonstrate the way the evidence must be handles, preserved, analyzed and presented in a courtroom, as well as how that evidence collected and analyzed can support a trial and/or a corporate disciplinary process.

It includes also a legal section, based on the local laws and then correlates the evidence found with the statement made by the employee; and how that evidence can support or dismiss that statement as well as the local laws that could be broken.

## **Executive Summary**

---

The investigation centered on one copy of a storage media found on the desk of Mr. Robert Lawrence; provided by Mr. Mark Mawer, security administrator at CC Terminals, based on the statement made by Ms. Leila Conlay who was concerned about the attitude to her from Mr. Lawrence.

Using fully documented procedures, to keep the integrity of the media and preserve the evidence admissibility, was possible to determine that Mr. Lawrence attempted to meet her sometimes and the evidence found is completely consistent with Ms Conlay statement.

At first, in October 25 and 26 – 2004, two documents that appear to be the first emails stated by Ms. Conlay were found. In those documents, Mr. Lawrence was offering help and he invited her to go for a coffee. It seems that Ms. Conlay rejected those invitations.

Evidence was also found supporting the fact that Mr. Lawrence decided on October 27 and 28 – 2004 to start monitoring the internet activity and specifically the personal email address of Ms. Conlay. Because of this, he was able to read one specific email in which Ms. Conlay, from her own personal email address, accepts one invitation for coffee from other person, and give some directions about the place in which the encounter will be done. This is a violation of the Colombian Politics Constitution, as in Article # 15 establishes the Fundamental right to personal privacy, and furthermore, states the inviolability of every way of correspondence and/or any way of private communications, which must not be intercepted unless a legal warrant is issued for that specific purpose.

After that, Mr. Lawrence searched in the Internet for a map showing the place in which

Ms. Conlay will stop for a coffee that night, and according to Ms. Conlay statement, it seems Mr. Lawrence decided to appear in that place.

There is evidence that Mr. Lawrence then sent another email to Ms. Conlay, this time a little more aggressive, but not threatening.

This behavior can be considered as an attempted violation of the Colombian Politics Constitution, Art. 38, which states the freedom of association and relation to other persons. Additionally, the Law No. 248<sup>th</sup> of December of 1995 states the Sexual Harassment in workplace as a way of female violence (art. 2) and also states the freedom of association (art. 4)

In the Examination Details Section below, it is possible to find all of the evidence referenced in this executive summary.

## Examination details

---

The image was provided by CC Terminals' Security Administrator, Mark Mawer thru the GIAC website, with the accompanying Chain of Custody form:

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

Then, the file was downloaded from the following URL:

<<https://www.giac.org/GCFAPractical2.0-USBImageAndInfo.zip.gz>>

An Image is an expected bit-by-bit copy of the original media, in this case, we are talking about the Lexar 64MB USB Flashdrive, and as stated in the Chain of Custody, a file named USBFD-64531026-RL-001.img was found in the compressed file.

The image was downloaded in a Windows workstation connected to the internet, which is not the forensic station.

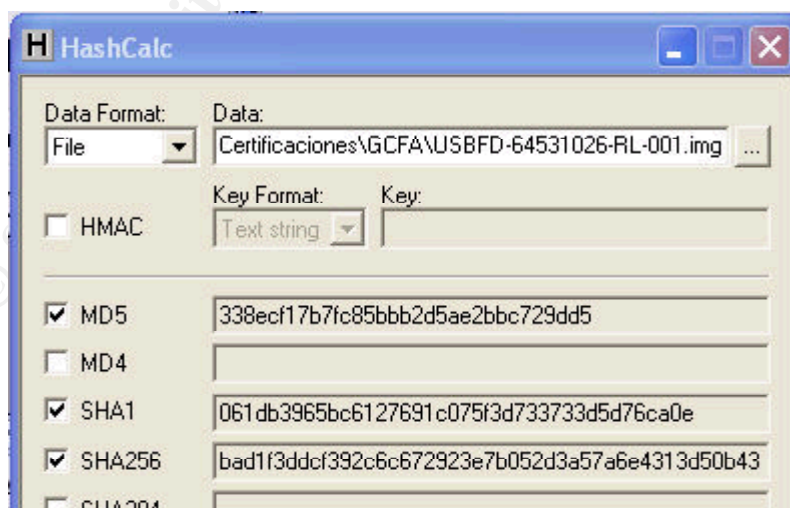
The forensic station uses Linux Fedora Core 3 as its operating system, with special forensic utilities and is isolated from internet but connected to the windows workstation via Secure Shell.

In order to ensure the integrity of the image and/or media analyzed, there are some cautions taken in the forensic station:

- When the forensic station is networked with the Windows workstation, the internet connection in the Windows workstation is closed. Once the forensic station has finished transactions with the Windows workstation, they are disconnected each other (and if needed, the Windows workstation can connect to the Internet again).
- There is configured in the forensic station one special drive acting only as an evidence locker. This drive is used for storing images from seized media, as an independent hard disk to prevent any damages on the forensic station operating system. The drive was sterilized (completely wiped with zeroes in all of the unused disk space) to ensure the evidence will not be affected by other data previously existing on that disk.
- As a way to keep the integrity of the evidence locker, an MD5 hash of the entire disk is taken after any case creation or modification, to ensure that the media is not being altered by any other means.
- There are rough procedures to keep the integrity on the file system itself, including the periodically MD5 hash (or after major updates) of the most relevant binaries, mainly the forensic tools, the contents of the /etc directory and some relevant operating system binaries and daemons, selected accordingly to the internal policy.
- The time of the forensic station is checked and if needed adjusted periodically and specifically before starting any investigation.

Now that the cautions and policies taken for the liturgical forensic analysis in order to minimize the data loss and evidence corruption have been stated, is possible to proceed onto the image examination.

The downloaded zip file is extracted, which results in an image file that is checked for integrity in the Windows workstation, using MD5 hash. The MD5 check ensures that the image downloaded is exactly the same (bit-by-bit) than the one provided by Mr. Mawer:



The MD5 hash calculated using a tool named HashCalc, matches the one provided in the Chain of Custody, which means that it is exactly the same file. Any digit changed in the

MD5 sum could mean that the evidence was altered, which is not the case now. HashCalc is a utility from Slavasoft <<http://www.slavasoft.com/hashcalc/>> that “allows to compute message digests, checksums and HMACs for files, as well as for text and hex strings.”

For the records, here is the catalogue of the image file (obtained just looking at the file properties in the Windows workstation):

**File Name:** USBFD-64531026-RL-001.img  
**File Size:** 62.439.424 bytes  
**MD5:** 338ecf17b7fc85bbb2d5ae2bbc729dd5  
**Creation Date:** 26/10/2004 03:58:36  
**Modification Date:** 26/10/2004 03:58:36

Knowing that the image file is an exact copy of the one provided by Mr. Mawer thru the GIAC website, is possible to proceed with the image analysis in the forensic station. However, at first sight, it can be noticed that there are one inconsistency, regarding the dates of the events vs. the date of the image. In the case description, all the events occur until October 28, but the image creation date as well as the modification date appears to be in October 26. A full analysis of the image will be done in order to try to clear this fact.

At first step, the MD5 sum is calculated for the Evidence Locker in the forensic station, taking the hash for the entire disk located in /dev/hdb. This MD5 is compared with the one previous taken in the last modification of the Evidence locker, and matches. An additional comparison of the MD5 hashes of the files controlled by the internal policy is made in order to ensure everything is fine for proceeding with the investigation.

Now that the integrity check has been done and it is ok to continue, the image is transferred from the Windows workstation to the forensic station using SSH to prevent any eavesdropping in the network, and of course, disconnecting the Windows workstation from the Internet.

For evidence handling purposes, the original copy of the image file remains in the Windows workstation untouched, and is transferred to a sterile media (Sanitized and double checked CDROM). Again, one MD5 hash is taken from that CD, which matches the original one (in the Windows station as well as in the Chain of custody provided) and all of the further analysis, will be made on the copy that has been transferred to a forensic station. Doing that way ensures the analysis will not broke the chain of custody, which is a “Prosecutor’s primary tool in authenticating electronic evidence” (Vacca, p. 155), showing that a reliable copying process were used.

For most of the analysis, the tool used will be Brian Carrier’s “The SleuthKit” with the help of the “Autopsy Forensic Browser”. Those two sets of open-source tools are very helpful in the media analysis improving evidence collection, preservation and presentation. For detailed information, please visit <[www.sleuthkit.org](http://www.sleuthkit.org)>.

Now the Autopsy forensic browser is started with a set of common options:

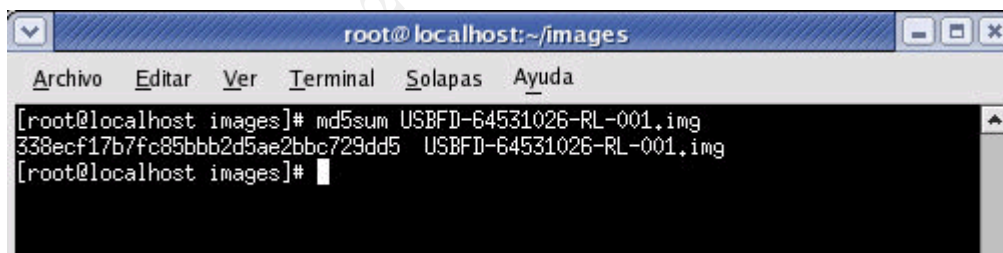
- c:** This option mounts a web server in a given port, it is safe to generate a cookie value for security reasons (we don't want everybody to connect to the server)
- d /root/evlocker:** The path to the evidence locker (In this case, the partition /dev/hdb1 mounted on that mount point and sanitized as described above)
- p 31685:** Again, for security reasons, it is better to have the control of the port that is opened by the server.

Now, the Forensic browser is started and the new case is created. Below, the case catalog as created in the Forensic Browser:

**Case Name:** 64531026  
**Description:** GCFA Certification  
**Created:** Fri Feb 11 16:23:49 2005  
**Investigators:** jcreyes

Unfortunately, the Autopsy Forensic Browser lacks of auto-interpretation of images, and when a hard disk, or a USB Flash (in this case) doesn't have its FAT entry at the very first sector, that image cannot be treated directly, so before adding a new image to the case recently created, there are some previous steps to take.

At first, again it is better to ensure the integrity of the image in the forensic station:



```
root@localhost:~/images
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[root@localhost images]# md5sum USBFD-64531026-RL-001.img
338ecf17b7fc85bbb2d5ae2bbc729dd5  USBFD-64531026-RL-001.img
[root@localhost images]#
```

Well, the MD5 remains the same as the one calculated for the Windows Workstation and most important, it is the same provided in the Chain of Custody.

Now, it is a good idea to see what the command "file" gives when ran against the image file:

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

The file command attempts to give information regarding the file type of the file that is passed as an argument. In this case, the command returned "x86 boot sector". That



means the image file is a complete drive dump, probably with partition table, partition definitions and inter-partition spaces. In order to check if that is correct, it is better to look with a Hex editor at the very first sectors of the image. The editor chosen is KHexEdit, a graphical Hex editor for Linux with too much capabilities and built-in tools.

Now it is a careful review. The editor can be run in read-only mode, but the integrity of the image must be preserved. Therefore, the plan right now is to look at the first sectors, try to find the offset for a FAT/Superblock entry (or magic number) and then close the editor and check the MD5 again to ensure nothing has been altered.

Looking the first block, it seems to be a normal Partition Table block, matching the exact 512 bytes (see figure1). The Partition Table stores information about the logical drives existing in the media analyzed (called partitions). Now, there must be a FAT block, probably 15 or 31 bytes ahead of the first block (depending of the FAT type). It is better to run a search on the image for the MAGIC number (55 AA). The magic number is a standard signature that defines the ending of most of the FAT entries. In a 512 bytes-per-sector disk, is possible to find the starting FAT entry just locating the 55 AA Magic and counting back the 510 remaining bytes. When an "EB 3C" chain is found exactly at 510 bytes, it is probably one FAT entry (one of the partitions listed in the partition table). The "EB 3C" instruction is commonly know as the Jump Instruction (or Jump Code) and is one of the mandatory items inside a FAT block, delimiting its starting offset.

© SANS Institute 2000 - 2005

0000:0000	33 c0 8e d0 bc 00 7c fb 50 07 50 1f fc be 1b 7c	3 . .   P.P. .
0000:0010	bf 1b 06 50 57 b9 e5 01 f3 a4 cb bd be 07 b1 04	..PW . . . .
0000:0020	38 6e 00 7c 09 75 13 83 c5 10 e2 f4 cd 18 8b f5	8n.  .u. . . .
0000:0030	83 c6 10 49 74 19 38 2c 74 f6 a0 b5 07 b4 07 8b	. . It.8,t . . . .
0000:0040	f0 ac 3c 00 74 fc bb 07 00 b4 0e cd 10 eb f2 88	<.t . . . . .
0000:0050	4e 10 e8 46 00 73 2a fe 46 10 80 7e 04 0b 74 0b	N. F.s* F..~.t.
0000:0060	80 7e 04 0c 74 05 a0 b6 07 75 d2 80 46 02 06 83	.~.t. .u .F...
0000:0070	46 08 06 83 56 0a 00 e8 21 00 73 05 a0 b6 07 eb	F...V.. !.s. .
0000:0080	bc 81 3e fe 7d 55 aa 74 0b 80 7e 10 00 74 c8 a0	.> }U t..~.t
0000:0090	b7 07 eb a9 8b fc 1e 57 8b f5 cb bf 05 00 8a 56	. . . .W. . . .V
0000:00a0	00 b4 08 cd 13 72 23 8a c1 24 3f 98 8a de 8a fc	. . .r# \$?. . .
0000:00b0	43 f7 e3 8b d1 86 d6 b1 06 d2 ee 42 f7 e2 39 56	C . . . . B 9V
0000:00c0	0a 77 23 72 05 39 46 08 73 1c b8 01 02 bb 00 7c	.w#r.9F.s. . .
0000:00d0	8b 4e 02 8b 56 00 cd 13 73 51 4f 74 4e 32 e4 8a	.N..V. .sQOtN2 .
0000:00e0	56 00 cd 13 eb e4 8a 56 00 60 bb aa 55 b4 41 cd	V. .V. ` U A
0000:00f0	13 72 36 81 fb 55 aa 75 30 f6 c1 01 74 2b 61 60	.r6. U u0 .t+a`
0000:0100	6a 00 6a 00 ff 76 0a ff 76 08 6a 00 68 00 7c 6a	j.j. v. v.j.h. j
0000:0110	01 6a 10 b4 42 8b f4 cd 13 61 61 73 0e 4f 74 0b	.j. B. .aas.Ot.
0000:0120	32 e4 8a 56 00 cd 13 eb d6 61 f9 c3 49 6e 76 61	2 .V. . a Inva
0000:0130	6c 69 64 20 70 61 72 74 69 74 69 6f 6e 20 74 61	lid partition ta
0000:0140	62 6c 65 00 45 72 72 6f 72 20 6c 6f 61 64 69 6e	ble.Error loadin
0000:0150	67 20 6f 70 65 72 61 74 69 6e 67 20 73 79 73 74	g operating syst
0000:0160	65 6d 00 4d 69 73 73 69 6e 67 20 6f 70 65 72 61	em.Missing opera
0000:0170	74 69 6e 67 20 73 79 73 74 65 6d 00 00 00 00 00	ting system.....
0000:0180	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:0190	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:01a0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:01b0	00 00 00 00 00 2c 44 63 18 2e 07 c3 00 00 80 01	.....,Dc.. . . .
0000:01c0	01 00 04 10 20 f9 20 00 00 00 3f dc 01 00 00 00	.....? . . . .
0000:01d0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:01e0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:01f0	00 00 00 00 00 00 00 00 00 00 00 00 00 55 aa	.....U

Figure 1. First Sector (0x0000 to 0x01f0, showing the Boot Sector)

In this case, the MAGIC number was found at 0x01FE and counting back the 512 bytes gives an offset of 0x4000 as the starting of the FAT block. FAT means File Allocation Table, and contains information about the data structure on the logical drive, and there are some other very helpful data, including the OEM name, the type of FAT, the Volume name (see figure 2). Additionally, to prove this first set of technical conclusions, the command mmls is issued to the image file, now trying the option “-t dos” (it appears to be a FAT16 entry). Mmls is a tool that helps find the offset for different partitions into the drive.

```
[root@forensics images]# /root/sleuthkit/bin/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)

The results of mmls appear to confirm the findings made with the Hex Editor: One primary Table (1 block-sized), 31 Sectors unallocated (15872 Bytes Zero-Padded, which along

with the Primary Table is the common structure for FAT 16) and starting at sector 32 (0x4000) the FAT 16 block and then, the data area.

0000:4000	eb 3c 90 4d 53 57 49 4e 34 2e 31 00 02 02 01 00	<.MSWIN4.1.....
0000:4010	02 00 02 00 00 f8 ef 00 20 00 11 00 20 00 00 00	.....
0000:4020	3f dc 01 00 80 00 29 00 00 00 00 4e 4f 20 4e 41	? ....)....NO NA
0000:4030	4d 45 20 20 20 20 46 41 54 31 36 20 20 20 33 c9	ME FAT16 3
0000:4040	8e d1 bc fc 7b 16 07 bd 78 00 c5 76 00 1e 56 16	. {.. x. v..V.
0000:4050	55 bf 22 05 89 7e 00 89 4e 02 b1 0b fc f3 a4 06	U ".~...N. .
0000:4060	1f bd 00 7c c6 45 fe 0f 38 4e 24 7d 20 8b c1 99	. .  E .8N\$} .
0000:4070	e8 7e 01 83 eb 3a 66 a1 1c 7c 66 3b 07 8a 57 fc	~.. :f . f;..W
0000:4080	75 06 80 ca 02 88 56 02 80 c3 10 73 ed 33 c9 fe	u...V...s 3
0000:4090	06 d8 7d 8a 46 10 98 f7 66 16 03 46 1c 13 56 1e	. }.F.. f..F..V.
0000:40a0	03 46 0e 13 d1 8b 76 11 60 89 46 fc 89 56 fe b8	.F...v..`F .V
0000:40b0	20 00 f7 e6 8b 5e 0b 03 c3 48 f7 f3 01 46 fc 11	. .^.. H .F .
0000:40c0	4e fe 61 bf 00 07 e8 28 01 72 3e 38 2d 74 17 60	N a .. (.r>8-t..`
0000:40d0	b1 0b be d8 7d f3 a6 61 74 3d 4e 74 09 83 c7 20	. } at=Nt..
0000:40e0	3b fb 72 e7 eb dd fe 0e d8 7d 7b a7 be 7f 7d ac	; r . .}{ .}
0000:40f0	98 03 f0 ac 98 40 74 0c 48 74 13 b4 0e bb 07 00	.. .@t.Ht. . .
0000:4100	cd 10 eb ef be 82 7d eb e6 be 80 7d eb e1 cd 16	. .} .} .
0000:4110	5e 1f 66 8f 04 cd 19 be 81 7d 8b 7d 1a 8d 45 fe	^f... .}.}..E
0000:4120	8a 4e 0d f7 e1 03 46 fc 13 56 fe b1 04 e8 c2 00	.N. .F .V .
0000:4130	72 d7 ea 00 02 70 00 52 50 06 53 6a 01 6a 10 91	r ...p.RP.Sj.j..
0000:4140	8b 46 18 a2 26 05 96 92 33 d2 f7 f6 91 f7 f6 42	.F. &...3 . B
0000:4150	87 ca f7 76 1a 8a f2 8a e8 c0 cc 02 0a cc b8 01	. v... . .
0000:4160	02 80 7e 02 0e 75 04 b4 42 8b f4 8a 56 24 cd 13	...~..u. B. .V\$ .
0000:4170	61 61 72 0a 40 75 01 42 03 5e 0b 49 75 77 c3 03	aar.@u.B.^Iuw .
0000:4180	18 01 27 0d 0a 49 6e 76 61 6c 69 64 20 73 79 73	...'Invalid sys
0000:4190	74 65 6d 20 64 69 73 6b ff 0d 0a 44 69 73 6b 20	tem disk ..Disk
0000:41a0	49 2f 4f 20 65 72 72 6f 72 ff 0d 0a 52 65 70 6c	I/O error ..Repl
0000:41b0	61 63 65 20 74 68 65 20 64 69 73 6b 2c 20 61 6e	ace the disk, an
0000:41c0	64 20 74 68 65 6e 20 70 72 65 73 73 20 61 6e 79	d then press any
0000:41d0	20 6b 65 79 0d 0a 00 00 49 4f 20 20 20 20 20 20	key....IO
0000:41e0	53 59 53 4d 53 44 4f 53 20 20 20 53 59 53 7f 01	SYSMSDOS SYS..
0000:41f0	00 41 bb 00 07 60 66 6a 00 e9 3b ff 00 00 55 aa	.A ...`fj. ; ..U

Figure 2. FAT Block Contents

Now it is possible to proceed with the analysis. First, the MD5 has to be checked to ensure integrity:

```

root@localhost:~/images
Archivo  Editor  Ver  Terminal  Solapas  Ayuda
[root@localhost images]# md5sum USBFD-64531026-RL-001.img
338ecf17b7fc85bbb2d5ae2bbc729dd5  USBFD-64531026-RL-001.img
[root@localhost images]# md5sum USBFD-64531026-RL-001.img
338ecf17b7fc85bbb2d5ae2bbc729dd5  USBFD-64531026-RL-001.img
[root@localhost images]#

```

Again, the hashes match exactly. Now, it is time to proceed to chop the image file, using the offset found above (0x4000, 32 Sectors) and generate a new image only of the unique partition found, using dd.

Dd is a tool that helps in the creation of bit-by-bit images, with some particularities, including the use of parameters to define block sizes; and the capability of seek or skip a

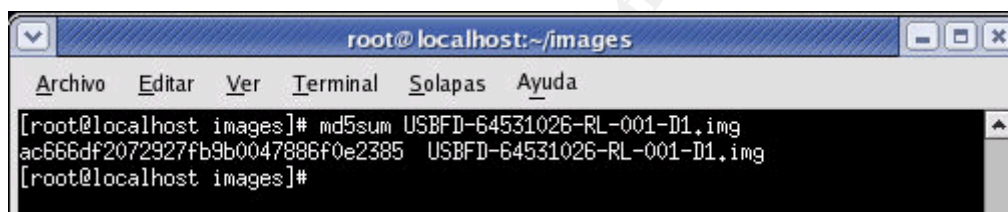


given number of blocks inside an image.

```
[root@forensics images]# dd if=USBFD-64531026-RL-001.img of=USBFD-64531026-RL-001-D1.img bs=512 skip=32
121920+0 registros leidos
121920+0 registros escritos
[root@forensics images]#
```

At this point, it is important to issue a new label for the piece of evidence in the Chain of Custody:

**Tag #:** USBFD-64531026-RL-001-D1  
**Description:** 64M Lexar Media JumpDrive Unique Partition  
**Serial #:** JDSP064-04-5000C  
**Image:** USBFD-64531026-RL-001-D1.img  
**MD5:** ac666df2072927fb9b0047886f0e2385  
**Creation Date:** Feb 11, 18:03



Now, the first shot will be trying to mount the new image file as a block device (simulating the image file as if it were a real disk) and take a look inside, in order to watch for some still visible files contained in that disk. That could be done using the mount command and taking advantage of the loopback device present on Linux machines.

The loopback device will do the trick of mounting the file as a block device (in Linux, Block devices are all of the devices that use block storage, such as hard drives, floppy drives, usb flash drives).

```
[root@forensics images]# mount -t vfat -o ro,loop USBFD-64531026-RL-001-D1.img /mnt/usbflash/
```

```
[root@forensics images]# mount
/dev/hda1 on / type ext3 (rw)
none on /proc type proc (rw)
none on /sys type sysfs (rw)
none on /dev/pts type devpts (rw,gid=5,mode=620)
usbfs on /proc/bus/usb type usbfs (rw)
none on /dev/shm type tmpfs (rw)
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw)
/root/images/USBFD-64531026-RL-001-D1.img on /mnt/usbflash type vfat
(ro,loop=/dev/loop0)
```

The command mount is used with the “ro” and “loop” options, to ensure two things: “loop”

is for the utilization of the loopback device and “ro” is for be aware and mount the image file as read-only,. That will help us to protect the integrity of the image file.

Now it is possible to browse the image as a common storage device:

```
[root@forensics images]# cd /mnt/usbflash/  
[root@forensics usbflash]# ls  
coffee.doc  her.doc  hey.doc  
[root@forensics usbflash]# ls -la  
total 84  
drwxr-xr-x  2 root root 16384 dic 31  1969 .  
drwxr-xr-x  3 root root  4096 feb  7 20:27 ..  
-rwxr-xr-x  1 root root 19968 oct 28 19:24 coffee.doc  
-rwxr-xr-x  1 root root 19968 oct 25 08:32 her.doc  
-rwxr-xr-x  1 root root 19968 oct 26 08:48 hey.doc  
[root@forensics usbflash]#
```

That is a first attempt, and showed some results: three files, apparently MS word files in three different dates. The simplest action that could be taken here is to copy the files to another location, but that will not help too much. It is preferable to mount the image on the evidence locker and inspect the raw contents of the blocks being used by those files in order to search for slack space or something hidden.

Well, the curiosity is fed up for now, and it is better to proceed into the image analysis directly on the Autopsy Forensic Browser. During the process, the Browser was instructed to calculate and compare the MD5 hash of the new image.

```
Calculating MD5 of images/USBFD-64531026-RL-001-D1.img (this could take a while)  
+ Current MD5: AC666DF2072927FB9B0047886F0E2385
```

The MD5 matches again, and is ok to proceed.

Now it is possible to look into the image of the Flash Disk and watch the files found when the image was mounted using the loopback device (the three probably MS Office files, as well as other files that have been deleted:

DEL	dir / in	NAME	WRITTEN	ACCESSED	CREATED	Size	UID	GID
✓	r / r	<u>_ap.gif</u>	2004.10.28 11:17:46 (COT)	2004.10.28 00:00:00 (COT)	2004.10.28 11:17:44 (COT)	0	0	0
✓	r / r	<u>_ap.gif</u>	2004.10.28 11:17:46 (COT)	2004.10.28 00:00:00 (COT)	2004.10.28 11:17:44 (COT)	8814	0	0
✓	r / r	<u>_apture</u>	2004.10.28 11:11:00 (COT)	2004.10.28 00:00:00 (COT)	2004.10.28 11:08:24 (COT)	53056	0	0
	r / r	<u>coffee.doc</u>	2004.10.28 19:24:48 (COT)	2004.10.28 00:00:00 (COT)	2004.10.28 19:24:46 (COT)	19968	0	0
	r / r	<u>her.doc</u>	2004.10.25 08:32:08 (COT)	2004.10.25 00:00:00 (COT)	2004.10.25 08:32:06 (COT)	19968	0	0
	r / r	<u>hey.doc</u>	2004.10.26 08:48:10 (COT)	2004.10.26 00:00:00 (COT)	2004.10.26 08:48:06 (COT)	19968	0	0
✓	r / r	<u>WinDump.exe</u> ( <u>_INDUMP.EXE</u> )	2004.10.27 16:24:06 (COT)	2004.10.27 00:00:00 (COT)	2004.10.27 16:24:04 (COT)	0	0	0
✓	r / r	<u>WinDump.exe</u> ( <u>_INDUMP.EXE</u> )	2004.10.27 16:24:02 (COT)	2004.10.28 00:00:00 (COT)	2004.10.27 16:24:04 (COT)	450560	0	0
✓	r / r	<u>WinPcap_3_1_beta_3.exe</u> ( <u>_INPCA~1.EXE</u> )	2004.10.27 16:23:56 (COT)	2004.10.27 00:00:00 (COT)	2004.10.27 16:23:54 (COT)	0	0	0
✓	r / r	<u>WinPcap_3_1_beta_3.exe</u> ( <u>_INPCA~1.EXE</u> )	2004.10.27 16:23:50 (COT)	2004.10.28 00:00:00 (COT)	2004.10.27 16:23:54 (COT)	485810	0	0

Now, there is a nice list of files stored in the Flash drive in which the following files:

- Coffee.doc
- Her.doc
- Hey.doc

Still exists in the drive and those others:

- \_ap.gif
- \_apture
- WinDump.exe
- WinPcap\_3\_1\_beta\_3.exe

Are deleted files.

At first sight, the DOC files may be the text of the emails that Ms. Conlay stated Mr. Lawrence sent to her; the EXE files may be programs.

The finding of those files / programs could be the evidence needed in order to support or discard Ms. Conlay Concerns, so the next step will be to recover all of the files, label them as potential evidence (exhibits) and start analyzing the files each, chronologically.

In the last screenshot, there are three (3) files:

- \_ap.gif
- WinDump.exe
- WinPcap\_3\_1\_beta\_3.exe

Those are 0 bytes length. After a further check of the blocks containing that files, it was noticed that there were just pointer entries of the original files, before deleted.

In order to analyze the files chronologically, it is needed to know the timeline of the contents of the image, which is as follows:

#### **Exhibit A:**

**Tag #:** USBFD-64531026-RL-001-D1-XA

**Description:** Timeline

**Size:** 5841 bytes

**Image:** USBFD-64531026-RL-001-D1.img

**MD5:** 0b799cc18c7c1577cb1dc6536f7228b4

**Exhibit Creation Date:** Feb 11, 17:36

The Complete timeline could be seen in the next page. For interpretation purposes, is important to keep in mind that the FAT 16 file system does not store the accessed time, but only the accessed date, so all of the accessed entries are automatically set to 00:00:00, and that only means the file was accessed in any time on the referred date. Additionally, as the image was taken from an USB Drive (a mountable storage device), the drive letter E will be shown in the timeline, but is safe to consider that the drive letter was used only for examination process.

## EXHIBIT A (Continuation) – FILE ACTIVITY TIMELINE OF THE IMAGE PROVIDED

Mon Oct 25 2004 00:00:00	19968	.a.	E:\her.doc
Mon Oct 25 2004 08:32:06	19968	..c	E:\her.doc
Mon Oct 25 2004 08:32:08	19968	m..	E:\her.doc
Tue Oct 26 2004 00:00:00	19968	.a.	E:\hey.doc
Tue Oct 26 2004 08:48:06	19968	..c	E:\hey.doc
Tue Oct 26 2004 08:48:10	19968	m..	E:\hey.doc
Wed Oct 27 2004 00:00:00	0	.a.	<USBFD-64531026-RL-001-D1.img-_INPCA~1.EXE-dead-7>
	450560	.a.	E:\WinDump.exe (_INDUMP.EXE) (deleted)
	0	.a.	<USBFD-64531026-RL-001-D1.img-_INDUMP.EXE-dead-12>
	485810	.a.	E:\WinPcap 3 1 beta 3.exe (_INPCA~1.EXE) (deleted)
Wed Oct 27 2004 16:23:50	485810	m..	<USBFD-64531026-RL-001-D1.img-_INPCA~1.EXE-dead-10>
	485810	m..	E:\WinPcap 3 1 beta 3.exe (_INPCA~1.EXE) (deleted)
Wed Oct 27 2004 16:23:54	0	..c	<USBFD-64531026-RL-001-D1.img-_INPCA~1.EXE-dead-7>
	485810	..c	E:\WinPcap 3 1 beta 3.exe (_INPCA~1.EXE) (deleted)
	485810	..c	<USBFD-64531026-RL-001-D1.img-_INPCA~1.EXE-dead-10>
	485810	..c	E:\WinPcap 3 1 beta 3.exe (_INPCA~1.EXE) (deleted)
Wed Oct 27 2004 16:23:56	485810	m..	E:\WinPcap 3 1 beta 3.exe (_INPCA~1.EXE) (deleted)
	0	m..	<USBFD-64531026-RL-001-D1.img-_INPCA~1.EXE-dead-7>
Wed Oct 27 2004 16:24:02	450560	m..	<USBFD-64531026-RL-001-D1.img-_INDUMP.EXE-dead-14>
	450560	m..	E:\WinDump.exe (_INDUMP.EXE) (deleted)
Wed Oct 27 2004 16:24:04	450560	..c	E:\WinDump.exe (_INDUMP.EXE) (deleted)
	450560	..c	E:\WinDump.exe (_INDUMP.EXE) (deleted)
	450560	..c	<USBFD-64531026-RL-001-D1.img-_INDUMP.EXE-dead-14>
	0	..c	<USBFD-64531026-RL-001-D1.img-_INDUMP.EXE-dead-12>
Wed Oct 27 2004 16:24:06	0	m..	<USBFD-64531026-RL-001-D1.img-_INDUMP.EXE-dead-12>
	450560	m..	E:\WinDump.exe (_INDUMP.EXE) (deleted)
Thu Oct 28 2004 00:00:00	8814	.a.	E:\_ap.gif (deleted)
	485810	.a.	<USBFD-64531026-RL-001-D1.img-_INPCA~1.EXE-dead-10>
	8814	.a.	<USBFD-64531026-RL-001-D1.img-_ap.gif-dead-17>
	8814	.a.	E:\_ap.gif (deleted)
	485810	.a.	E:\WinPcap 3 1 beta 3.exe (_INPCA~1.EXE) (deleted)
	450560	.a.	<USBFD-64531026-RL-001-D1.img-_INDUMP.EXE-dead-14>
	450560	.a.	E:\WinDump.exe (_INDUMP.EXE) (deleted)
	53056	.a.	E:\_apture (deleted)
	19968	.a.	E:\coffee.doc
	0	.a.	<USBFD-64531026-RL-001-D1.img-_ap.gif-dead-16>
	53056	.a.	<USBFD-64531026-RL-001-D1.img-_apture-dead-15>
Thu Oct 28 2004 11:08:24	53056	..c	<USBFD-64531026-RL-001-D1.img-_apture-dead-15>
	53056	..c	E:\_apture (deleted)
Thu Oct 28 2004 11:11:00	53056	m..	<USBFD-64531026-RL-001-D1.img-_apture-dead-15>



		53056	m..	E:\/_apture (deleted)
Thu Oct 28 2004 11:17:44	8814	..c		E:\/_ap.gif (deleted)
	0	..c		<USBFD-64531026-RL-001-D1.img-_ap.gif-dead-16>
	8814	..c		<USBFD-64531026-RL-001-D1.img-_ap.gif-dead-17>
	8814	..c		E:\/_ap.gif (deleted)
Thu Oct 28 2004 11:17:46	8814	m..		<USBFD-64531026-RL-001-D1.img-_ap.gif-dead-17>
	8814	m..		E:\/_ap.gif (deleted)
	8814	m..		E:\/_ap.gif (deleted)
	0	m..		<USBFD-64531026-RL-001-D1.img-_ap.gif-dead-16>
Thu Oct 28 2004 19:24:46	19968	..c		E:\/_coffee.doc
Thu Oct 28 2004 19:24:48	19968	m..		E:\/_coffee.doc

### Color Convention:

<b>Created</b>
<b>Modified</b>
<b>Accessed</b>

According to the timeline, in October 25 at 08:32:06 the first word document was created, and immediately modified (2 seconds after creation timestamp). An in-depth analysis of the file shows that this is a MS Word Version 10.0 file, and there are no other content hidden in that file, as well as there are no evidence that the document was emailed other than the testimony of Ms. Conlay. Here the details:

#### Exhibit B:

**Tag #:** USBFD-64531026-RL-001-D1-XB  
**Description:** Recovered file - HER.DOC  
**Position:** 0X3FE00 - 0x44A5D  
**Size:** 19968 bytes  
**Image:** USBFD-64531026-RL-001-D1.img  
**MD5:** 9785a777c5286738f9deb73d8bc57978  
**Exhibit Creation Date:** Feb 11<sup>th</sup>, 18:03  
**MAC Time:** Created: 2004/10/25 08:32:06  
Modified: 2004/10/25 08:32:08  
Accessed: 2004/10/25

The text of this document has the following content:

Hey I saw you the other day. I tried to say "hi", but you disappeared??? That was a nice blue dress you were wearing. I heard that your car was giving you some trouble. Maybe I can give you a ride to work sometime, or maybe we can get dinner sometime?

Have a nice day

The text of the file seems to be a simple communication offering help, but it is consistent with Ms. Conlay statement.

On October 26 at 08:48:06, a second word document is created, and now four seconds after creation timestamp it is modified. Again, in-depth analysis of the file shows that this is a MS Word Version 10.0 file, and there are no other content hidden in that file, as well as there are no evidence that the document was emailed other than the testimony of Ms. Conlay. Now the details:

#### Exhibit C:

**Tag #:** USBFD-64531026-RL-001-D1-XC  
**Description:** Recovered file - HEY.DOC  
**Position:** 0X44E00 - 0x49BF0  
**Size:** 19968 bytes  
**Image:** USBFD-64531026-RL-001-D1.img

**MD5:** ca601d4f8138717dca4de07a8ec19ed1  
**Exhibit Creation Date:** Feb 11<sup>th</sup>, 19:36  
**MAC Time:** Created: 2004/10/26 08:48:06  
Modified: 2004/10/26 08:48:10  
Accessed: 2004/10/26

The text of this document has the following content:

Hey! Why are you being so mean? I was just offering to help you out with your car! Don't tell me to get lost! You should give me a chance. I'm a nice guy just trying to help you out, just because I think you're cute doesn't mean I'm weird. Perhaps coffee would be better, when would be a good time for you?

Again, the text of the file seems to be a simple communication now performing an invitation (apparently the help offered before was rejected, which could indicate the previous message was delivered to Ms. Conlay), and again it is consistent with Ms. Conlay statement.

Now, following the chronological order provided by the timeline, in October 27 at 16:23:54 and at 16:24:04 two executable files (windump.exe and winpcap\_3\_1\_beta\_3.exe, respectively) were created. Those programs are known “sniffing” programs, or in other words, programs that are used to eavesdrop packages (or portions of data) that travel unencrypted over a local area network. Those programs may be used for spying other users’ activities in the network.

#### Exhibit D:

**Tag #:** USBFD-64531026-RL-001-D1-XD  
**Description:** Deleted file - WINPCAP\_3\_1\_BETA\_3.EXE  
**Position:** 0X49E00 - 0x13DC6D  
**Size:** 485810 bytes  
**Image:** USBFD-64531026-RL-001-D1.img  
**MD5:** b794de4b88068ae80de523c3b35eeaab  
**Exhibit Creation Date:** Feb 11<sup>th</sup>, 20:03  
**MAC Time:** Created: 2004/10/27 16:23:54  
Modified: 2004/10/27 16:23:56  
Accessed: 2004/10/28

#### Exhibit E:

**Tag #:** USBFD-64531026-RL-001-D1-XE  
**Description:** Deleted file - WINDUMP.EXE

**Position:** 0XC0A00 - 0x107514  
**Size:** 450560 bytes  
**Image:** USBFD-64531026-RL-001-D1.img  
**MD5:** 79375b77975aa53a1b0507496107bff7  
**Exhibit Creation Date:** Feb 11<sup>th</sup>, 20:17  
**MAC Time:** Created: 2004/10/27 16:24:04  
Modified: 2004/10/27 16:24:06  
Accessed: 2004/10/28

For the complete details regarding the functions, possible use (in the case), and verification of this programs, please refer to the “Program identification Section” and “Forensic Details” below, in this report.

To continue the investigation, at this point will be assumed that the programs found have not been altered or that they do not have any hidden code. All the support regarding this supposition will be analyzed in the sections mentioned earlier.

At October 28, 11:08:24, another file appears in the investigation, now some file named “\_apture”. An in-depth analysis of the file shows that it appears to be a TCPDUMP format file. TCPDUMP is another program originally created for UNIX that collects the network traffic data, and ported to Windows as Windump. This fact will support the theory that the programs found earlier (windump and winpcap) were used and maybe this file could be the result of the execution of those programs, which are needed each other. For details about the architecture and form of execution of those programs, please refer to the “Program identification Section” and “Forensic Details” below, in this report).

#### Exhibit F:

**Tag #:** USBFD-64531026-RL-001-D1-XF  
**Description:** Deleted file - \_APTURE (Maybe “Capture”?)  
**Position:** 0X12EAA00 - 0x13B93F  
**Size:** 53056 bytes  
**Image:** USBFD-64531026-RL-001-D1.img  
**MD5:** 2097b7b0a9fedb4238b67e976c4ae1cb  
**Exhibit Creation Date:** Feb 11<sup>th</sup>, 20:42  
**MAC Time:** Created: 2004/10/28 11:08:24  
Modified: 2004/10/28 11:11:00  
Accessed: 2004/10/28

In order to prove if this is a TCPDUMP-formatted file, it will be loaded into a program named “Ethereal”, which is able to read and show in a very friendly user interface the data collected from TCPDUMP. Ethereal ([www.ethereal.com](http://www.ethereal.com)) is another program that sniffs the network and records all the packets that it can see.

As expected, Ethereal is able to read and show the file recovered:

No.	Time	Source	Destination	Protocol	Info
1	0.00000	192.168.2.104	64.4.34.250	TCP	2038 > http [SYN] Seq=0 Ack=0 Win=
2	0.00215	192.168.2.1	192.168.2.255	SNMP	TRAP-V1 1.3.6.1.4.1.3955.1.1.0
3	0.02425	64.4.34.250	192.168.2.104	TCP	http > 2038 [SYN, ACK] Seq=0 Ack=
4	0.02427	192.168.2.104	64.4.34.250	TCP	2038 > http [ACK] Seq=1 Ack=1 Win=
5	0.02445	192.168.2.104	64.4.34.250	HTTP	POST /cgi-bin/premail/2452 HTTP/1
6	0.02447	192.168.2.104	64.4.34.250	HTTP	Continuation
7	0.02449	192.168.2.104	64.4.34.250	HTTP	Continuation
8	0.08547	64.4.34.250	192.168.2.104	TCP	http > 2038 [ACK] Seq=1 Ack=1737
9	0.08628	64.4.34.250	192.168.2.104	HTTP	HTTP/1.1 100 Continue
10	0.13581	64.4.34.250	192.168.2.104	HTTP	HTTP/1.1 200 OK
11	0.13587	192.168.2.104	64.4.34.250	TCP	2038 > http [ACK] Seq=2313 Ack=36
12	0.14460	64.4.34.250	192.168.2.104	HTTP	Continuation
13	0.16837	64.4.34.250	192.168.2.104	HTTP	Continuation
14	0.16846	192.168.2.104	64.4.34.250	TCP	2038 > http [ACK] Seq=2313 Ack=32
15	0.17724	64.4.34.250	192.168.2.104	HTTP	Continuation

Frame 1 (62 bytes on wire (62 bytes captured))

This file usually contains too many data, so it is better to continue extracting and analyzing the files in order to obtain a few keywords for this case for using them in a keyword search.

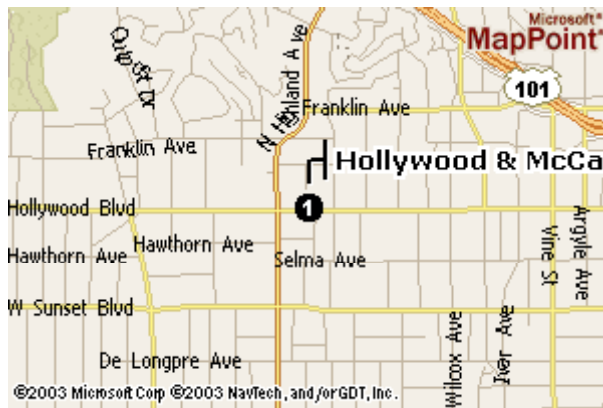
For now, at this point it is possible to prove that Mr. Lawrence at least has been using software to monitor the network traffic, which may be prohibited in CC Terminal's organizational information security policies, and may have some sensitive information about the organization or other employees. Additionally, this fact shows that Mr. Lawrence has enough skills to use this kind of programs and that he knows how to use them (or has been assisted to).

The same day (October 28, but at 11:17:44) another file is created, now it appears to be a GIF file (a picture or drawing), named "\_ap.gif".

#### Exhibit G:

**Tag #:** USBFD-64531026-RL-001-D1-XG  
**Description:** Deleted file - \_AP.GIF (Maybe "map.gif"?)  
**Position:** 0X13BA00 - 0x13DC6D  
**Size:** 8814 bytes  
**Image:** USBFD-64531026-RL-001-D1.img  
**MD5:** 9bc3923cf8e72fd405d7cea8c8781011  
**Exhibit Creation Date:** Feb 11<sup>th</sup>, 20:42  
**MAC Time:** Created: 2004/10/28 11:17:44  
Modified: 2004/10/28 11:17:46  
Accessed: 2004/10/28

Now the contents of the file:



This is interesting. Ms Conlay stated that Mr. Lawrence appeared in a coffee shop, and the finding of this map could indicate that Mr. Lawrence did not just “stop by”. However, still there is no evidence for such conclusion.

At last, another Word Document created at October 28, 19:24:46. Again, in-depth analysis of the file shows that this is a MS Word Version 10.0 file, and there are no other content hidden in that file, as well as there are no evidence that the document was emailed other than the testimony of Ms. Conlay.

#### Exhibit H:

**Tag #:** USBFD-64531026-RL-001-D1-XH  
**Description:** Recovered file - COFEE.DOC  
**Position:** 0X49E00 - 0x4EBFF  
**Size:** 19968 bytes  
**Image:** USBFD-64531026-RL-001-D1.img  
**MD5:** a833c58689596eda15a27c931e0c76d1  
**Exhibit Creation Date:** Feb 11<sup>th</sup>, 20:58  
**MAC Time:** Created: 2004/10/28 19:24:46  
Modified: 2004/10/28 19:24:48  
Accessed: 2004/10/28

The content of the file:

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...

As stated by Ms. Conlay, this last text appears to be more aggressive, but no threat or improper language was found that might indicate danger. The fact is that this last text implies some event happened before, and is consistent with ms. Conlay statement about the coffee shop.

It seems the key is located in the capture file and the map file, so now it is a good idea to keyword search the entire image looking initially for five specific words:

- Leila
- Conlay
- Robert
- Lawrence
- Hollywood

Hollywood is included because the map appears to be very specific about a location, maybe the location of the coffee shop stated by Ms. Conlay.

That first attempt did the following results:

```
[root@forensics images]# strings USBFD-64531026-RL-001.img | grep -i conlay
[root@forensics images]# strings USBFD-64531026-RL-001.img | grep -i leila
curmbox=F000000001&HrsTest=&_HMaction=Send&FinalDest=&subaction=&plaintext=&l
ogin=flowergirl96&msg=&start=&len=&attfile=&attlistfile=&url=&type=&src=&ref
=&ru=&msghdrid=b16479b18beec291196189c78555223c_1098692452&RTEbgcolor=&encode
dto=SamGuarillo@hotmail.com&encodedcc=&encodedbcc=&deleteUponSend=0&importanc
e=&sigflag=&newmail=new&to=SamGuarillo@hotmail.com&cc=&bcc=&subject=RE%3A+cof
fee&body=Sure%2C+coffee+sounds+great.++Let%27s+meet+at+the+coffee+shop+on+the
+corner+Hollywood+and+McCadden.++It%27s+a+nice+out+of+the+way+spot.%0D%0A%0D%
0ASee+you+at+7pm%21%0D%0A%0D%0A-Leila.6
[root@forensics images]# strings USBFD-64531026-RL-001.img | grep -i robert
Robert Lawrence
Robert Lawrence
Robert Lawrence
Robert Lawrence
Robert Lawrence
Robert Lawrence
[root@forensics images]# strings USBFD-64531026-RL-001.img | grep -i lawrence
Robert Lawrence
Robert Lawrence
Robert Lawrence
Robert Lawrence
Robert Lawrence
Robert Lawrence
[root@forensics images]# strings USBFD-64531026-RL-001.img | grep -i
hollywood
curmbox=F000000001&HrsTest=&_HMaction=Send&FinalDest=&subaction=&plaintext=&l
ogin=flowergirl96&msg=&start=&len=&attfile=&attlistfile=&url=&type=&src=&ref
=&ru=&msghdrid=b16479b18beec291196189c78555223c_1098692452&RTEbgcolor=&encode
dto=SamGuarillo@hotmail.com&encodedcc=&encodedbcc=&deleteUponSend=0&importanc
e=&sigflag=&newmail=new&to=SamGuarillo@hotmail.com&cc=&bcc=&subject=RE%3A+cof
```

```
fee&body=Sure%2C+coffee+sounds+great.++Let%27s+meet+at+the+coffee+shop+on+the
+corner+Hollywood+and+McCadden.++It%27s+a+nice+out+of+the+way+spot.%0D%0A%0D%
0ASee+you+at+7pm%21%0D%0A%0D%0A-Leila.6
[root@forensics images]#
```

The results showed a special line (the one in bold font), that appears to be a hotmail transaction. The only way to get a hotmail transaction in the image is if it is part of the capture file of the sniffing programs, so it is time to inspect again that capture file.

After a very extensive analysis of the capture file, loaded with Ethereal, it is possible to conclude that the contents are a normal hotmail transaction, between the hotmail servers and a local network IP address 192.168.2.104.

The package No. 7 contains the most important and useful information:

#### Exhibit I:

**Tag #:** USBFD-64531026-RL-001-D1-XI

**Description:** Package Captured

**Image:** USBFD-64531026-RL-001-D1.img

**Exhibit Creation Date:** Feb 11<sup>th</sup>, 21:42

```
0000 00 0c 41 50 29 2c 00 90 4b 5e e3 cf 08 00 45 00 ..AP),... K^....E.
0010 02 68 97 ca 40 00 80 06 3a b7 c0 a8 02 68 40 04 .h...@... :....h@.
0020 22 fa 07 f6 00 50 f1 16 06 ee ce 89 31 98 50 18 "....P.. ....1.P.
0030 44 70 38 03 00 00 63 75 72 6d 62 6f 78 3d 46 30 Dp8...cu rmbox=F0
0040 30 30 30 30 30 30 30 31 26 48 72 73 54 65 73 74 00000001 &HrsTest
0050 3d 26 5f 48 4d 61 63 74 69 6f 6e 3d 53 65 6e 64 =&_HMact ion=Send
0060 26 46 69 6e 61 6c 44 65 73 74 3d 26 73 75 62 61 &FinalDe st=&suba
0070 63 74 69 6f 6e 3d 26 70 6c 61 69 6e 74 65 78 74 ction=&p laintext
0080 3d 26 6c 6f 67 69 6e 3d 66 6c 6f 77 65 72 67 69 =&login= flowergi
0090 72 6c 39 36 26 6d 73 67 3d 26 73 74 61 72 74 3d rl96&msg =&start=
00a0 26 6c 65 6e 3d 26 61 74 74 66 69 6c 65 3d 26 61 &len=&at tfile=&a
00b0 74 74 6c 69 73 74 66 69 6c 65 3d 26 65 75 72 6c ttlistfi le=&eurl
00c0 3d 26 74 79 70 65 3d 26 73 72 63 3d 26 72 65 66 =&type=& src=&ref
00d0 3d 26 72 75 3d 26 6d 73 67 68 64 72 69 64 3d 62 =&ru=&ms ghdrId=b
00e0 31 36 34 37 39 62 31 38 62 65 65 63 32 39 31 31 16479b18 beec2911
00f0 39 36 31 38 39 63 37 38 35 35 35 32 32 33 63 5f 96189c78 555223c_
0100 31 30 39 38 36 39 32 34 35 32 26 52 54 45 62 67 10986924 52&RTEbg
0110 63 6f 6c 6f 72 3d 26 65 6e 63 6f 64 65 64 74 6f color=&e ncodedto
0120 3d 53 61 6d 47 75 61 72 69 6c 6c 6f 40 68 6f 74 =SamGuar illo@hot
0130 6d 61 69 6c 2e 63 6f 6d 26 65 6e 63 6f 64 65 64 mail.com &encoded
0140 63 63 3d 26 65 6e 63 6f 64 65 64 62 63 63 3d 26 cc=&enco dedbcc=&
0150 64 65 6c 65 74 65 55 70 6f 6e 53 65 6e 64 3d 30 deleteUp onSend=0
0160 26 69 6d 70 6f 72 74 61 6e 63 65 3d 26 73 69 67 &importa nce=&sig
0170 66 6c 61 67 3d 26 6e 65 77 6d 61 69 6c 3d 6e 65 flag=&ne wmail=ne
0180 77 26 74 6f 3d 53 61 6d 47 75 61 72 69 6c 6c 6f w&to=Sam Guarillo
0190 40 68 6f 74 6d 61 69 6c 2e 63 6f 6d 26 63 63 3d @hotmail .com&cc=
01a0 26 62 63 63 3d 26 73 75 62 6a 65 63 74 3d 52 45 &bcc=&su bject=RE
01b0 25 33 41 2b 63 6f 66 66 65 65 26 62 6f 64 79 3d %3A+coff ee&body=
01c0 53 75 72 65 25 32 43 2b 63 6f 66 66 65 65 2b 73 Sure%2C+ coffee+s
01d0 6f 75 6e 64 73 2b 67 72 65 61 74 2e 2b 2b 4c 65 ounds+gr eat.++Le
01e0 74 25 32 37 73 2b 6d 65 65 74 2b 61 74 2b 74 68 t%27s+me et+at+th
01f0 65 2b 63 6f 66 66 65 65 2b 73 68 6f 70 2b 6f 6e e+coffee +shop+on
0200 2b 74 68 65 2b 63 6f 72 6e 65 72 2b 48 6f 6c 6c +the+cor ner+Holl
```



0210	79 77 6f 6f 64 2b 61 6e	64 2b 4d 63 43 61 64 64	ywood+an d+McCadd
0220	65 6e 2e 2b 2b 49 74 25	32 37 73 2b 61 2b 6e 69	en.++It% 27s+a+ni
0230	63 65 2b 6f 75 74 2b 6f	66 2b 74 68 65 2b 77 61	ce+out+o f+the+wa
0240	79 2b 73 70 6f 74 2e 25	30 44 25 30 41 25 30 44	y+spot.% 0D%0A%0D
0250	25 30 41 53 65 65 2b 79	6f 75 2b 61 74 2b 37 70	%0ASee+y ou+at+7p
0260	6d 25 32 31 25 30 44 25	30 41 25 30 44 25 30 41	m%21%0D% 0A%0D%0A
0270	2d 4c 65 69 6c 61		-Leila

From this packet, it is possible to conclude that Ms. Conlay sent an email message to the email address of <[SamGuarillo@hotmail.com](mailto:SamGuarillo@hotmail.com)> from which appears to be her own email address (flowergirl96), and the body of the message was:

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

See you at 7pm

-Leila.

With this piece of the puzzle, now it is possible to rebuild the events.

Additionally to the analysis of the files found, the whole image was checked for other hidden instructions, files, documents, and nothing more was found.

The package showed has a timestamp of Oct. 28 13:10:54. The first package logged was at that time, and the last one was at Oct. 28 13:10:55. There is one inconsistency in the modification time of the capture file (Oct. 28 11:11:00), regarding an exactly two hours of difference between the arrival time of the packages as windump logged them and the MAC times of the capture file. This difference may occur for bad time synchronization, keeping in mind that there is an USB Flash drive and the files contained may be opened in more than one computer.

## Conclusions

Mr. Lawrence has attempted to contact Ms. Conlay, in October 25 and 26, as showed in Exhibits B and C. Apparently, Ms Conlay has rejected him, and Mr. Lawrence has used two programs, which will help him to monitor some of the network activities of Ms. Conlay (exhibits D and E). As a result of that monitoring he got access to an email sent from ms. Conlay in October 28 in which she accepted an invitation for a coffee and give her party a place where they can meet (Exhibit I). With this information, Mr. Lawrence searched the internet for a map of that location (Hollywood and McCadden) as exhibit G demonstrates; and went to that place (according to Ms Conlay statement).

After that, Mr. Lawrence sent Ms. Conlay a new email showed in Exhibit H.

This behavior is completely consistent with the statement of Ms. Conlay, and the evidence

supports it. However, there is a detail that must be solved in order to maintain the admissibility of the evidence, regarding the inconsistency expressed in the begging of the analysis about the image creation timestamp as well as the time inconsistency found between the modification time of the capture file and the timestamps of the packages found in the Windump log. It is recommended to ask Mr. Mawer details about the procedures he took to get the image.

## Image details

---

All of the details regarding the image are extensively discussed in the section "Examination details", including the chronological analysis, the tools used and any other information to support the when and the how the following details were found.

### Details of the Image File:

**Tag #:** USBFD-64531026-RL-001  
**Description:** 64M Lexar Media JumpDrive  
**Serial #:** JDSP064-04-5000C  
**Image:** USBFD-64531026-RL-001.img  
**MD5:** 338ecf17b7fc85bbb2d5ae2bbc729dd5  
**Creation Date:** 26/10/2004 03:58:36  
**Modification Date:** 26/10/2004 03:58:36

### Information about the Image:

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)

### Information about the Contents of the Image:

(Please see the next page)

## File Details:

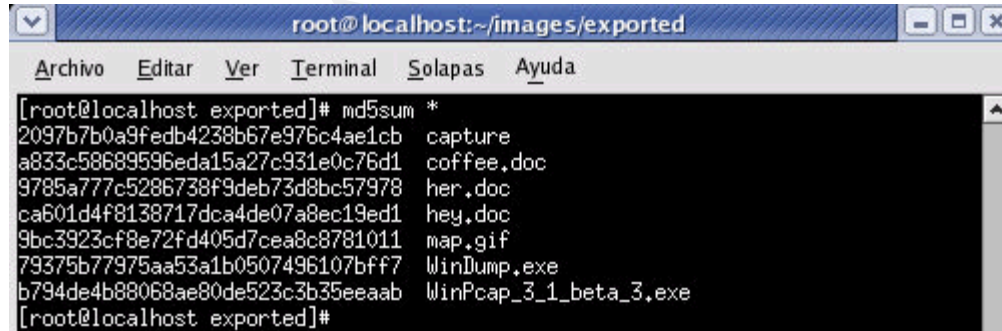
File name found	True File name	MAC Time	Owner		Size (bytes)
			User	Group	
Her.doc	Her.doc	C: Oct 25 2004 08:32:06 M: Oct 25 2004 08:32:08 A: Oct 25 2004 No Time (FAT16)	N/A (not supported by FAT)	N/A (not supported by FAT)	19968
Hey.doc	Hey.doc	C: Oct 26 2004 08:48:06 M: Oct 26 2004 08:48:10 A: Oct 26 2004 No Time (FAT16)	N/A (not supported by FAT)	N/A (not supported by FAT)	19968
WinPcap_3_1_beta_3.exe	WinPcap_3_1_beta_3.exe	C: Oct 27 2004 16:23:54 M: Oct 27 2004 16:23:56 A: Oct 28 2004 No Time (FAT16)	N/A (not supported by FAT)	N/A (not supported by FAT)	485810
WinDump.exe	WinDump.exe	C: Oct 27 2004 16:24:04 M: Oct 27 2004 16:24:06 A: Oct 28 2004 No Time (FAT16)	N/A (not supported by FAT)	N/A (not supported by FAT)	450560
?apture	capture	C: Oct 28 2004 11:08:24 M: Oct 28 2004 11:11:00 A: Oct 28 2004 No Time (FAT16)	N/A (not supported by FAT)	N/A (not supported by FAT)	53056
?ap	map	C: Oct 28 2004 11:17:44 M: Oct 28 2004 11:17:46 A: Oct 28 2004 No Time (FAT16)	N/A (not supported by FAT)	N/A (not supported by FAT)	8814
Cofee.doc	Cofee.doc	C: Oct 28 2004 19:24:46 M: Oct 28 2004 19:24:48 A: Oct 28 2004 No Time (FAT16)	N/A (not supported by FAT)	N/A (not supported by FAT)	19968

## MD5 hashes and keywords:

File name found	True File name	MD5	Keywords
Her.doc	Her.doc	9785A777C5286738F9DEB73D8BC57978	Microsoft Office Word
Hey.doc	Hey.doc	CA601D4F8138717DCA4DE07A8EC19ED1	Microsoft Office Word
WinPcap_3_1_beta_3.exe	WinPcap_3_1_beta_3.exe	B794DE4B88068AE80DE523C3B35EEAAB	
WinDump.exe	WinDump.exe	79375B77975AA53A1B0507496107BFF7	Windump
?apture	capture	2097B7B0A9FEDB4238B67E976C4AE1CB	TCPDUMP
?ap	map	9BC3923CF8E72FD405D7CEA8C8781011	GIF89

Cofee.doc  
Cofee.doc  
A833C58689596EDA15A27C931E0C76D1  
Microsoft Office Word

## Screenshots:



A screenshot of a terminal window titled "root@localhost:~/images/exported". The window has a menu bar with "Archivo", "Editar", "Ver", "Terminal", "Solapas", and "Ayuda". The terminal content shows the command "[root@localhost exported]# md5sum \*" and its output, which lists seven files with their corresponding MD5 hashes. The files are: capture, coffee.doc, her.doc, hey.doc, map.gif, WinDump.exe, and WinPcap\_3.1\_beta\_3.exe.

```
[root@localhost exported]# md5sum *
2097b7b0a9fedb4238b67e976c4ae1cb  capture
a833c58689596eda15a27c931e0c76d1  coffee.doc
9785a777c5286738f9deb73d8bc57978  her.doc
ca601d4f8138717dca4de07a8ec19ed1  hey.doc
9bc3923cf8e72fd405d7cea8c8781011  map.gif
79375b77975aa53a1b0507496107bff7  WinDump.exe
b794de4b88068ae80de523c3b35eeaab  WinPcap_3.1_beta_3.exe
[root@localhost exported]#
```

## Forensic details

---

**Note:** All of the references to Exhibits in this section can be found in the Examination Details Section or in the Annex A, Catalogue of Evidence.

The findings made in the examination details section, showed two interesting programs used by Mr. Lawrence:

- Windump (Exhibit E)
- WinPcap\_3\_1\_Beta\_3.exe (Exhibit D)

Running a few searches on Google, the developer of both programs showed up, fully downloadable from [<http://windump.polito.it>](http://windump.polito.it) and [<http://winpcap.polito.it>](http://winpcap.polito.it)

According to the Windump website:

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

That means Windump is a packet sniffer, just like tcpdump. Packet sniffers “sniffs” all the data that travel over a network, in certain conditions and are very useful in network administration (when legally used) and to harvest sensitive data (such as passwords or some kind of other private information).

According to Exhibit E, the last time this program was accessed (executed, in this case) was at October 28<sup>th</sup>. Unfortunately FAT16 does not stores the last accessed time, only the date. However, this access date is consistent with the facts revealed by the evidence in the examination details section.

However, looking at the Windump requirements, it needs as a prerequisite the installation of WinPcap 3.1 beta 2 or higher. This relates to the other file found (WinPcap\_3\_1\_Beta\_3.exe, Exhibit D). This program is the packet capture library, needed by Windump to work.

According to the WinPcap website:

WinPcap is an open source library for packet capture and network analysis for the Win32 platforms. It includes a kernel-level packet filter, a low-level dynamic link library (packet.dll), and a high-level and system-independent library (wpcap.dll, based on libpcap version 0.6.2).

The packet filter is a device driver that adds to Windows 95, 98, ME, NT, 2000, XP and 2003 the ability to capture and send raw data from a network card, with the possibility to filter and store in a buffer the captured packets.

It seems that it is necessary to install the WinPcap library first, who creates a new server under the properties of the local area network device (in windows) and which apparently is the one who makes the real “sniffing”, sending the data to the other program named Windump.

Once Winpcap is installed, Windump uses that device acting as a User Interface to start the packet capturing.

All of the captured packages could be shown in the standard output, or can be sent to an external file. In this case, that external file appears to be the capture file (exhibit F) to log all of the activity in the format that later can be parsed with Windump itself or other program like Ethereal.

That means Windump cannot work without WinPcap (and specifically the version 3.1 beta 2 or superior) and all of the output is sent to a file, establishing the relationship between exhibits D, E and F.

Using the Windows station, a lab is performed in order to review the way of relationship of all of the three elements, confirming all of the statements made.

The options that Windump uses, are the same as tcpdump (Unix), after running the program start to capture live packets, and with the **-F** option the output can be redirected to a named file.

The use of this software is very simple, as it is just install and run.

All of these steps are clearly identified in the image, and according to the timeline, the WinPcap file creates and then the Windump file. Finally, the capture file is created:

```
Wed Oct 27 2004 16:23:54 485810 ..c E:\WinPcap_3_1_beta_3.exe (deleted)
Wed Oct 27 2004 16:24:04 450560 ..c E:\WinDump.exe (_INDUMP.EXE)
(deleted)
Thu Oct 28 2004 11:08:24 53056 ..c E:\_apture (deleted)
```

From those lines, it is possible to conclude that the WinPcap file was used first, then the Windump file. As those files were created at October 27, an installation can be assumed, and then, at October 28, when the Capture file is created, it is possible to assume that those programs were executed.

For confirmation, a look to the accessed dates of the programs and capture file can effectively show that those programs were used together:

```
Thu Oct 28 2004 00:00:00 485810 .a. E:\WinPcap_3_1_beta_3.exe (deleted)
450560 .a. E:\WinDump.exe (_INDUMP.EXE)
```

(deleted)

53056 .a. E:\/\_apture (deleted)

## Conclusion

From the analysis of the programs used by Mr. Lawrence, it was possible to establish a connection between the exhibits D, E and F, proving that the three files found are needed each other and supporting the evidence related to why that programs were found there.

## Program Identification

**Note:** All of the references to Exhibits in this section can be found in the Examination Details Section or in the Annex A, Catalogue of Evidence.

The sources for Windump 3.6.2 (versions used for Mr. Lawrence) were downloaded from the developer's web site, at <http://windump.polito.it/install/bin/WdumpSrc.zip>.

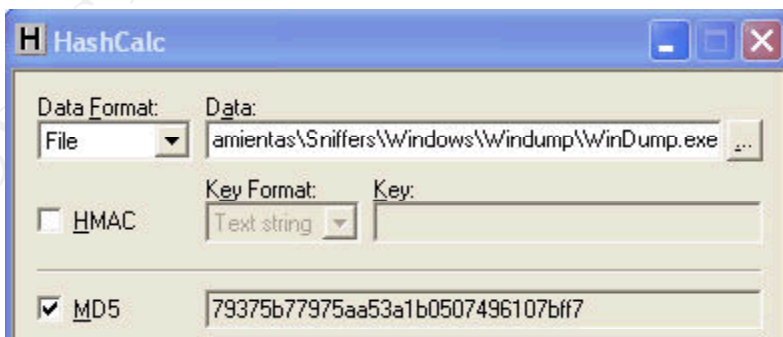
Those files were compiled under the Windows station, according to the instructions given using the Visual Studio 6 suite.

The building procedure, compiles the executable archives:

- WinDump.exe

There were no sources found for WinPcap 3.1 Beta 3, but the binary package was found and downloaded from [http://winpcap.polito.it/install/bin/WinPcap\\_3\\_1\\_beta3.exe](http://winpcap.polito.it/install/bin/WinPcap_3_1_beta3.exe)

Then, the MD5 hash was calculated for the executable Windump.exe, producing the following result:

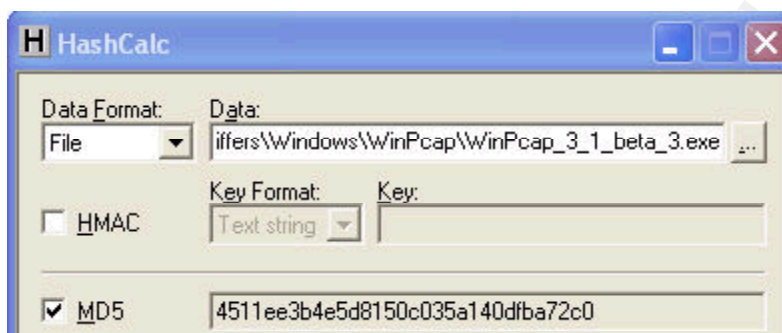


It matches with the MD5 calculated for the recovered file existing in the image and tagged in Exhibit E.

With this finding, it is possible to conclude that the Windump.exe sources downloaded from the developer's website (compiled locally) is exactly the same executable found in the image.

Now for the WinPcap\_3\_1\_Beta\_3.exe will follow the same procedure.

First proceeding with the MD5 calculation of the binary downloaded:



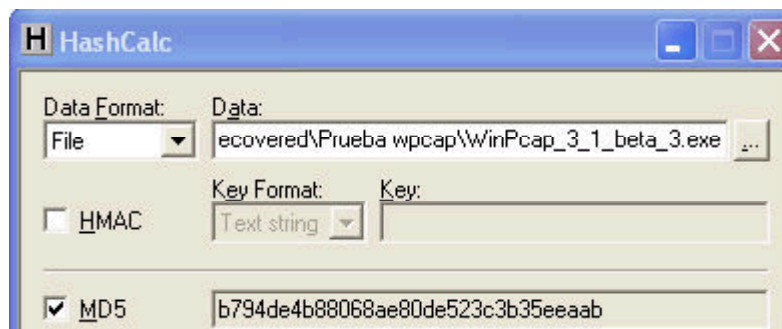
There is a mismatch in the MD5 calculation of the downloaded file and the one recovered and tagged in Exhibit D, which returned b794de4b88068ae80de523c3b35eeaab.

Looking closely at exhibit D, was possible to identify the recovered file as a Word Document, which contains the same text as the document recovered and tagged as Exhibit H (Cofee.doc). Additionally, it appears to be that the position of the document Coffe.doc (Exhibit H) and the Winpcap\_3\_1\_Beta\_3.exe starts at exactly the same offset in the image (0X49E00). That means the Winpcap\_3\_1\_Beta\_3.exe file was deleted and the file Coffee.doc was allocated at the same offset.

Now, it is time to do some tests in order to prove this hypothesis.

An exact copy (MD5 verified) of the two archives (Winpcap\_3\_1\_Beta\_3.exe, the one downloaded from the developer's website, and Coffee.doc recovered from the image) are taken to a separate folder, and with the Hex editor the first file (Winpcap\_3\_1\_Beta\_3.exe) is loaded. Now, with other instance of the Hex Editor, the file Coffee.doc is loaded, and completely copied. The write protection on the hex Editor is turned off, and the copied content from Coffee.doc is pasted to the Winpcap\_3\_1\_Beta\_3.exe file, overwriting the first sectors of the Winpcap\_3\_1\_Beta\_3.exe file, and thus creating a replica of the file obtained from the Image. If the MD5 Calculation resulting from this test matches the one obtained from the recovered file (exhibit D), it will be able to proof that the original file was exactly the same that was downloaded from the Winpcap developer's site.





As expected, the MD5 calculation of the new file matches the one obtained from the recovered file.

## Conclusions

The conclusions of this analysis supports the theory that the programs used by Mr. Lawrence were exactly the same as the ones obtained from the Windump / WinPcap developer's website, so it is expected that the functions are the same described in that website.

## Legal Implications

---

There are not too many legislation in Colombia for computer crimes (or computer related crimes). That is the reason for which some of the computer crimes are still treated as traditional crimes.

However, the Colombian Politics Constitution guarantees the privacy as a fundamental right that must be preserved. It particularly refers to the correspondence (mail or any other kind of personal correspondence) as well as other way of private communication, as elements that must not be intercepted unless a legal warrant is issued for that particular purpose, and only with the legalities that Colombian Laws establish (Art. 15).

In this case, Mr. Lawrence ran a program, which violated that fundamental right of Ms. Conlay, as that program eavesdropped some private information of her (her personal email contents, for example).

When Mr. Lawrence decided to use the information obtained with that program, then searching for specific details about a non working issues regarding Ms. Conlay; then going to some place in which he knows Ms. Conlay will be; and finally sending an email to her in a more aggressive way of speaking; he is potentially going against the Colombian Politics Constitution, which states that every person has other fundamental right of free association (relating with other persons as a democratic society, Art. 38). This right is stated also in the Law # 248 of December of 1995, defining additionally sexual harassment in the work place as a female violence (Art. 2)

It is safe to keep in mind that the only evidence found to support the case in court instances is related with the violation of the privacy of Ms. Conlay, by using the monitoring (sniffing) programs, for which the penalty is from six months to three years.

The collected evidence in this investigation does not support any other plea, regarding Sexual Harassment, Stalking or threatening, because no one of the documents found contained threats or improper language of any kind; and Mr. Lawrence's behavior has not been subject of investigation.

In the other hand, the use of programs that monitors network traffic can be a violation of internal information security procedures of the Company, an acceptable use of technological components, and this unauthorized use of programs could lead to a very sensitive information leakage.

## Recommendations

---

Based on the investigation findings, the following recommendations must be taken in order to follow-up:

- Mr. Mawer has to be asked about the details of the procedure he took to get the Image file from the USB Drive seized from Mr. Lawrence's desk, in order to clarify the inconsistency with the creation date of the image vs. the date of the files found inside, and regain admissibility of the whole evidence.
- Further investigation in Mr. Lawrence's PC is suggested, to search for other improper activities on the network. In this case, Mr. Lawrence perform an unauthorized monitoring on the network, and he got some private email information, and maybe this technique has been used to monitor other type of information inside CC Terminal, including sensitive data from the Company.
- Mr. Lawrence has to be confronted with the collected evidence, so he can make a statement about his actions.
- Internal information security and environmental policies have to be enforced, to prevent this type of situations in the future.
- If the company is legally empowered to, it is recommendable to investigate other activities and behaviors of Mr. Lawrence, in other scenarios like his social life, to establish a profile that could help to determine if the events related to Ms. Conlay can be a potential danger (can convert to a potentially destructive crime, getting physically).
- For further investigations, it is better to seize the data elements with presence of the

implicated subject, and try to avoid after-hours searching. This recommendation is oriented to avoid the risk in which the subject denies ownership of the data elements seized and/or the data itself.

## Additional Information

---

- **The Starman's Realm**

<[http://thestarman.pcministry.com/asm/mbr/MBR\\_in\\_detail.htm](http://thestarman.pcministry.com/asm/mbr/MBR_in_detail.htm)>. This page is very useful for the technical reader, because it is a very extensive and didactic resource for understanding Master Boot Records, Partition Tables and other details regarding media storage architectures.

- **Sniffing (network, wiretap, sniffer) FAQ**

<[http://www.secnf.net/misc/Sniffing\\_network\\_wiretap\\_sniffer\\_FAQ.html](http://www.secnf.net/misc/Sniffing_network_wiretap_sniffer_FAQ.html)>. This web page describes very accurately, what a sniffer is (network monitoring program used by Mr. Lawrence). It could be very helpful for understanding in a more detailed way the facts that are the key of this case.

- **Sniffer Dog threatens online privacy**

<[http://www.theregister.co.uk/2005/02/10/sniffer\\_dog\\_ruling/](http://www.theregister.co.uk/2005/02/10/sniffer_dog_ruling/)> Interesting article from The Register regarding the privacy associated with some kinds of “sniffing”. Helpful to understand some issues related to sniffers and warrants from an American legislation point of view.

## References

---

Vacca, John R. Computer Forensics: Crime Scene Investigation. Charles River Media, 2002.

Rude. Thomas. Next Generation data Forensics and Linux.

<[http://www.crazytrain.com/monkeyboy/Next\\_Generation\\_Forensics\\_Linux.pdf](http://www.crazytrain.com/monkeyboy/Next_Generation_Forensics_Linux.pdf)>. June 2002

Schweitzer, Douglas. Incident Response, Computer Forensic Toolkit. Wiley Publications, 2003

Littlejohn Shinder, Debra. Scene of the Cybercrime, Computer Forensics Handbook. Syngress, 2002

Marcella, Albert J; Greenfield Robert S. Cyber Forensics, A Field Manual for Collecting,

© SANS Institute 2000 - 2005, Author retains full rights.