



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 VERSION 1.5

PRESENTED BY: Manuel Humberto Santander Peláez

Date of submission: 12/22/2004

Table of contents

<u>1</u>	<u>abstract</u>	<u>4</u>
<u>2</u>	<u>Part one</u>	<u>4</u>
<u>2.1</u>	<u>Examination details</u>	<u>4</u>
<u>2.2</u>	<u>Image Details</u>	<u>10</u>
<u>2.2.1</u>	<u>Listing of all the files in the image</u>	<u>10</u>
<u>2.2.2</u>	<u>File/MACtime information for image</u>	<u>11</u>
<u>2.2.3</u>	<u>True name of the program/file used by Mr. Leszczynski.</u>	<u>11</u>
<u>2.2.4</u>	<u>File owner(s)</u>	<u>11</u>
<u>2.2.5</u>	<u>File size</u>	<u>12</u>
<u>2.2.6</u>	<u>MD5 hash of the file</u>	<u>12</u>
<u>2.2.7</u>	<u>Key words found that are associated with the program/file.</u>	<u>12</u>
<u>2.3</u>	<u>Forensic Details</u>	<u>13</u>
<u>2.4</u>	<u>Program Identification</u>	<u>31</u>
<u>2.5</u>	<u>Legal implication</u>	<u>35</u>
<u>2.6</u>	<u>Additional Information</u>	<u>40</u>
<u>3</u>	<u>Part 2</u>	<u>40</u>
<u>3.1</u>	<u>Synopsis of Case Facts</u>	<u>40</u>
<u>3.2</u>	<u>Describe the system(s) you'll be analyzing</u>	<u>42</u>
<u>3.3</u>	<u>Hardware</u>	<u>43</u>
<u>3.4</u>	<u>Image Media</u>	<u>44</u>
<u>3.5</u>	<u>Media Analysis of the system</u>	<u>44</u>
<u>3.5.1</u>	<u>Internet explorer history analysis</u>	<u>46</u>
<u>3.5.2</u>	<u>System Registry</u>	<u>55</u>

<u>3.5.3 Signs of sniffers</u>	59
<u>3.6 Timeline Analysis</u>	60
<u>3.7 Recover deleted files</u>	62
<u>3.8 String search</u>	63
<u>3.9 Conclusions</u>	64
<u>4 References</u>	<u>68</u>

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

1 abstract

Internet has evolved to be a network where electronic mail were the main way of communicating to a network which deals with great amount of activities of the daily life of the people, such as to order food, to pay invoices, to buy objects, between many other uses, This made possible that the crimes that before were made in the real world have been transferred to the electronic world, becoming computer crime.

This document details the probatory process of two facts in which the forensic investigation methodology was applied: Information robbery of a company with technical destiny to the industrial espionage using of steganografía and robbery of money by means of the clonación of cards debit in a bank.

It was possible to prove on first case the information robbery while in second wasn't possible, because there was a leak on the banking application design.

2 Part one

2.1 Examination details

As a premise, the Forensics Station used to perform the analysis is not networked to prevent any possible external intrusion coming from the network. The image was obtained from the SANS Web site using the following URL: http://www.giac.org/gcfa/v1_5.gz using Microsoft Internet Explorer within a networked station with Internet access. After downloading and using cygwin and the response toolkit for windows, the image was decompressed and md5 hashed, as seen in figure 2.

Then, using a USB Flash drive, the image was uploaded to the Forensics Station. The md5 hash was verified again, as seen in figure 3.

The md5 hashes in both cases are the same as the hash wroted on the Chain of Custody form. The image integrity is ok and it's safe to continue.

Figure 1: Image Filesystem Information

```
[root@poseidon imagenes]# fsstat -f fat12 v1_5
```

```
FILE SYSTEM INFORMATION
```

```
-----
```

```
File System Type: FAT
```

```
OEM Name: mkdosfs
```

```
Volume ID: 0x408bed14
```

```
Volume Label (Boot Sector): RJL
```

```
Volume Label (Root Directory): RJL
```

```
File System Type Label: FAT12
```

```
Sectors before file system: 0
```

```
File System Layout (in sectors)
```

```
Total Range: 0 - 2871
```

```
* Reserved: 0 - 0
```

```
** Boot Sector: 0
```

```
* FAT 0: 1 - 9
```

```
* FAT 1: 10 - 18
```

```
* Data Area: 19 - 2871
```

```
** Root Directory: 19 - 32
```

```
** Cluster Area: 33 - 2871
```

```
METADATA INFORMATION
```

```
-----
```

```
Range: 2 - 45426
```

```
Root Directory: 2
```

```
CONTENT INFORMATION
```

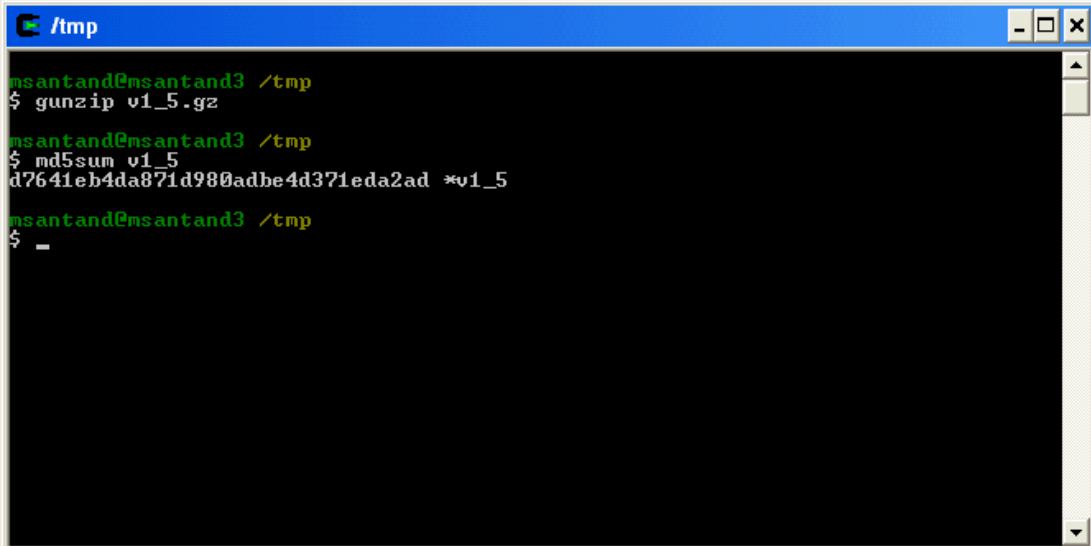
```
-----
```

Sector Size: 512
Cluster Size: 512
Total Cluster Range: 2 - 2840

FAT CONTENTS (in sectors)

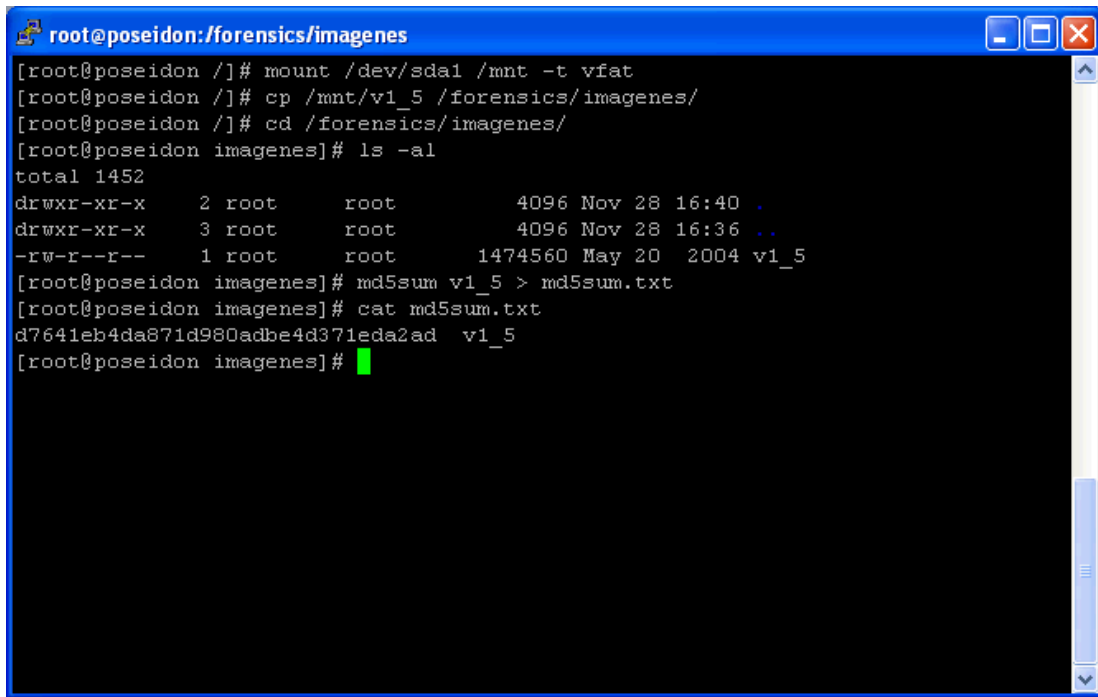
105-187 (83) -> EOF
188-250 (63) -> EOF
251-316 (66) -> EOF
317-918 (602) -> EOF
919-1340 (422) -> EOF
1341-1384 (44) -> EOF

Figure 2: First hash of the image when it was downloaded



```
msantand@msantand3 /tmp
$ gunzip v1_5.gz
msantand@msantand3 /tmp
$ md5sum v1_5
d7641eb4da871d980adbe4d371eda2ad *v1_5
msantand@msantand3 /tmp
$ -
```

Figure 3: Integrity verification after uploading the image to the forensic station



```
root@poseidon:/forensics/imagenes
[root@poseidon ~]# mount /dev/sda1 /mnt -t vfat
[root@poseidon ~]# cp /mnt/v1_5 /forensics/imagenes/
[root@poseidon ~]# cd /forensics/imagenes/
[root@poseidon imagenes]# ls -al
total 1452
drwxr-xr-x  2 root    root      4096 Nov 28 16:40 .
drwxr-xr-x  3 root    root      4096 Nov 28 16:36 ..
-rw-r--r--  1 root    root     1474560 May 20  2004 v1_5
[root@poseidon imagenes]# md5sum v1_5 > md5sum.txt
[root@poseidon imagenes]# cat md5sum.txt
d7641eb4da871d980adbe4d371eda2ad  v1_5
[root@poseidon imagenes]#
```

Figure 4: Mounting the image read-only

© SANS Institute 2000 - 2005, Author


```
-rw-r--r-- 1 root root 39 Nov 28 16:41 md5sum.txt
-rw-r--r-- 1 root root 1474560 May 20 2004 v1_5
-rw-r--r-- 1 root root 144162 Dec 2 17:07 v1_5.str
```

```
[root@poseidon imagenes]#
```

It's important now to create the timeline of the floppy to check all the files created, modified or deleted. This will provide information on how facts happened:

Figure 6: Floppy TimeLine

Day of the Week	Month	Day	Year	Time	Size	Type of access	Permissions	UID	GID	Sector	Name
Sat	Feb	3	2001	19:44:16	36864	n...	-/rwxrwxrwx	0	0	5	/CamShell.dll (AMSHELL_DLL) (deleted)
					36864	n...	-/rwxrwxrwx	0	0	5	<v1 5- AMSHELL_DLL-dead-5>
Thu	Apr	22	2004	16:31:06	33423	n...	-/rwxrwxrwx	0	0	17	/Internal Lab Security Policy.doc (INTERN~2.DOC)
					32256	n...	-/rwxrwxrwx	0	0	13	/Internal Lab Security Policy1.doc (INTERN~1.DOC)
Fri	Apr	23	2004	10:53:56	727	n...	-/rwxrwxrwx	0	0	28	/ ndex.htm (deleted)
					727	n...	-/rwxrwxrwx	0	0	28	<v1 5- ndex.htm-dead-28>
Fri	Apr	23	2004	11:54:32	215895	n...	-/rwxrwxrwx	0	0	23	/Remote Access Policy.doc (REMOTE~1.DOC)
Fri	Apr	23	2004	11:55:26	307935	n...	-/rwxrwxrwx	0	0	20	/Password Policy.doc (PASSWO~1.DOC)
Fri	Apr	23	2004	14:10:50	22528	n...	-/rwxrwxrwx	0	0	27	/Acceptable Encryption Policy.doc (ACCEPT~1.DOC)
Fri	Apr	23	2004	14:11:10	42496	n...	-/rwxrwxrwx	0	0	9	/Information Sensitivity Policy.doc (INFORM~1.DOC)
Sun	Apr	25	2004	00:00:00	0	a...	-/rwxrwxrwx	0	0	3	/RJL (Volume Label Entry)
Sun	Apr	25	2004	10:53:40	0	m.c	-/rwxrwxrwx	0	0	3	/RJL (Volume Label Entry)
Mon	Apr	26	2004	00:00:00	727	a...	-/rwxrwxrwx	0	0	28	/ ndex.htm (deleted)
					36864	a...	-/rwxrwxrwx	0	0	5	/CamShell.dll (AMSHELL_DLL) (deleted)
					32256	a...	-/rwxrwxrwx	0	0	13	/Internal Lab Security Policy1.doc (INTERN~1.DOC)
					215895	a...	-/rwxrwxrwx	0	0	23	/Remote Access Policy.doc (REMOTE~1.DOC)
					22528	a...	-/rwxrwxrwx	0	0	27	/Acceptable Encryption Policy.doc (ACCEPT~1.DOC)
					33423	a...	-/rwxrwxrwx	0	0	17	/Internal Lab Security Policy.doc (INTERN~2.DOC)
					307935	a...	-/rwxrwxrwx	0	0	20	/Password Policy.doc (PASSWO~1.DOC)
					727	a...	-/rwxrwxrwx	0	0	28	<v1 5- ndex.htm-dead-28>
					36864	a...	-/rwxrwxrwx	0	0	5	<v1 5- AMSHELL_DLL-dead-5>
					42496	a...	-/rwxrwxrwx	0	0	9	/Information Sensitivity Policy.doc (INFORM~1.DOC)
Mon	Apr	26	2004	09:46:18	36864	c	-/rwxrwxrwx	0	0	5	/CamShell.dll (AMSHELL_DLL) (deleted)
					36864	c	-/rwxrwxrwx	0	0	5	<v1 5- AMSHELL_DLL-dead-5>
Mon	Apr	26	2004	09:46:20	42496	c	-/rwxrwxrwx	0	0	9	/Information Sensitivity Policy.doc (INFORM~1.DOC)
Mon	Apr	26	2004	09:46:22	32256	c	-/rwxrwxrwx	0	0	13	/Internal Lab Security Policy1.doc (INTERN~1.DOC)
Mon	Apr	26	2004	09:46:24	33423	c	-/rwxrwxrwx	0	0	17	/Internal Lab Security Policy.doc (INTERN~2.DOC)
Mon	Apr	26	2004	09:46:26	307935	c	-/rwxrwxrwx	0	0	20	/Password Policy.doc (PASSWO~1.DOC)
Mon	Apr	26	2004	09:46:36	215895	c	-/rwxrwxrwx	0	0	23	/Remote Access Policy.doc (REMOTE~1.DOC)
Mon	Apr	26	2004	09:46:44	22528	c	-/rwxrwxrwx	0	0	27	/Acceptable Encryption Policy.doc (ACCEPT~1.DOC)
Mon	Apr	26	2004	09:47:36	727	c	-/rwxrwxrwx	0	0	28	/ ndex.htm (deleted)
					727	c	-/rwxrwxrwx	0	0	28	<v1 5- ndex.htm-dead-28>

The unallocated sectors file also will be generated to look for data inside them. This file will be used to recover information of the company or used programs if it's deleted:

Figure 7: Generating the unallocated sectors file from the image

```
[root@poseidon imagenes]# dls -f fat12 v1_5 > v1_5.dls
```

```
[root@poseidon imagenes]# ls -al
total 2388
drwxr-xr-x  2 root  root   4096 Dec  8 22:41 .
drwxr-xr-x  3 root  root   4096 Nov 28 16:36 ..
-rw-r--r--  1 root  root    39 Nov 28 16:41 md5sum.txt
-rw-r--r--  1 root  root 1474560 May 20  2004 v1_5
-rw-r--r--  1 root  root  798208 Dec  8 22:41 v1_5.dls
-rw-r--r--  1 root  root  144162 Dec  2 17:07 v1_5.str
[root@poseidon imagenes]#
```

The timeline shows a DLL program. Because we want to know what that program is., we'll perform a search using a dirty word list to search. These words will be, initially, DLL, dll, EXE, exe.

All the remaining steps performed on the image are detailed at 1.3 and they are:

- Interesting keyword search into the strings file
- Recovering the CamShell.dll deleted file
- Hex edit the recovered file.
- Internet search for program related to the Interesting keyword search.
- Program test with the files inside the image
- Recover of the files stolen from the company information systems

After all the examination performed to the image, we can conclude the following:

- Mr. Leszczynski modified the files:
 - Information_Sensitivity_Policy.doc
 - Internal_Lab_Security_Policy1.doc
 - Internal_Lab_Security_Policy.doc
 - Password_Policy.doc
 - Remote_Access_Policy.doc
 - Acceptable_Encryption_Policy.doc

- After that, he formatted the floppy, read all the doc files and camouflaged the client database, the unpublished schematics and the opportunity.txt file where Robert specifies all the information he's going to pass to Rift.

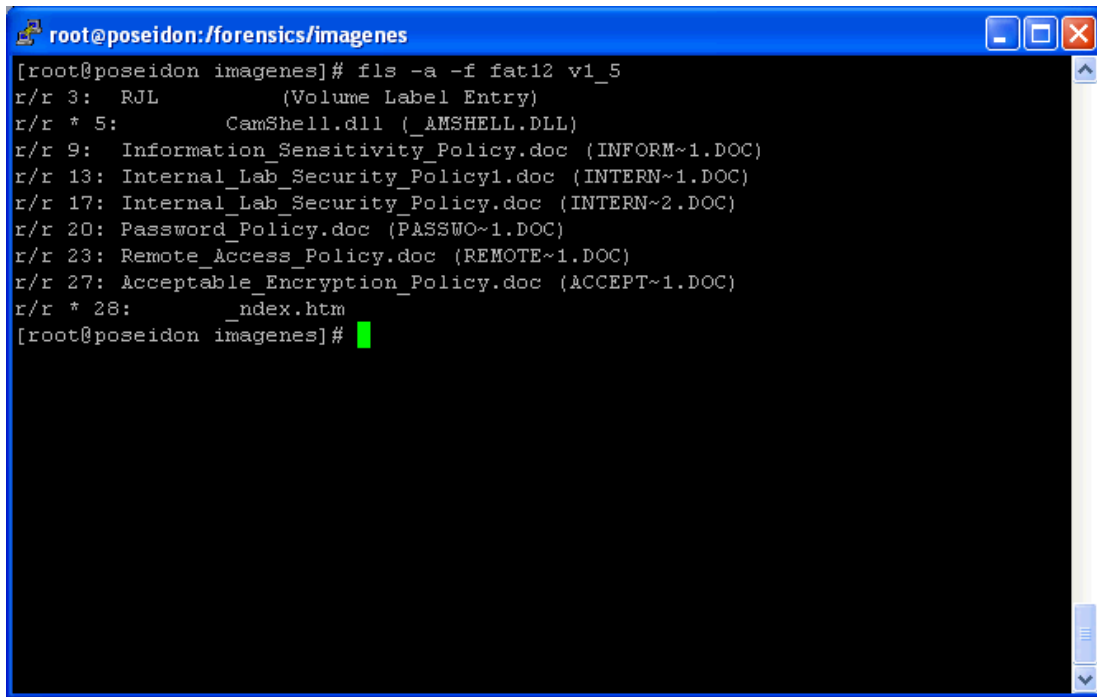
In some point, Robert had to find the secret information from a server, information system or any other computer resource. Robert was successful, because the files were camouflaged and ready to leave the company building inside the floppy. This seems to prove that he's the one that has been leaking information to Rift, but should be confirmed by investigating inside all the tampered systems and resources.

The Security Administrator should revoke all the permissions under Internet acces and all the information systems where Robert has access granted and then begin to seek inside the application log to detect when he grabbed all the last information about the schematics and the clients and make the correspondence with timelines of the e-mails that he sent from the company or his pc hard drive. He also has to verify the log of proxy and e-mail transactions, because this could be a way of sending out the company strategic information to Rift.

2.2 Image Details

2.2.1 Listing of all the files in the image

Figure 8: File List from the Image



```
root@poseidon:/forensics/imagenes
[root@poseidon imagenes]# ls -a -f fat12 v1_5
r/r 3:  RJL          (Volume Label Entry)
r/r * 5:  CamShell.dll  (_AMSHHELL.DLL)
r/r 9:  Information_Sensitivity_Policy.doc (INFORM~1.DOC)
r/r 13: Internal_Lab_Security_Policy1.doc (INTERN~1.DOC)
r/r 17: Internal_Lab_Security_Policy.doc (INTERN~2.DOC)
r/r 20: Password_Policy.doc (PASSWO~1.DOC)
r/r 23: Remote_Access_Policy.doc (REMOTE~1.DOC)
r/r 27: Acceptable_Encryption_Policy.doc (ACCEPT~1.DOC)
r/r * 28: _ndex.htm
[root@poseidon imagenes]#
```

The files tagged with a star are deleted. Those files will be recovered in the next chapters of this document.

2.2.2 File/MACtime information for image

Figure 9: Timestamp from Image

© SANS Institute 2000 - 2005, Author

```
msantand@msantand3 /cygdrive/d/GCFA
$ mac -d .
MAC.pl
Collect MAC times and owner from files in a directory.
Usage: [perl] mac.pl [-d dir] [-s] [-h/?] [> myfile.csv]
-d Directory to search. May be a mapped dir, or UNC path
  (default: current working directory)
-s Check subdirectories
By default, search starts at current dir, looking at all files.
NOTE: Beginning and end of search are timestamped. Output is in CSV format
for easy opening in Excel.
Copyright 2000/2001 H. Carvey keydet89@yahoo.com.
Start search,1102543006,Wed Dec 8 16:56:46 2004
File,Size,Last Access,Last Modification,Creation
.\v1_5.1474560,EPM\msantand,Thu May 20 12:34:16 2004,Thu May 20 12:34:16 2004,Tu
e Dec 7 22:19:14 2004
Search complete,1102543006,Wed Dec 8 16:56:46 2004
msantand@msantand3 /cygdrive/d/GCFA
$
```

Access time: May 20 2004 12:34:16

Modification time: May 20 2004 12:34:16

Creation time: Dec 7 2004 22:19:14

2.2.3 True name of the program/file used by Mr. Leszczynski.

Reading locations 0xB676 to 0xB6A2 from the image, the program name used by Mr. Leszczynski is camouflage, as seen on figure 9.

2.2.4 File owner(s)

FAT12 doesn't have inside the structure the concept of owner and group, so the file owner that will be provided is the one of the image inside the ext3 filesystem of the Linux Computer Forensic Station. From figure 3, File owner is root. File group is root.

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

Figure 9: Hex edit from Image showing locations B550 to B770

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
0000B550	73	00	69	00	74	00	69	00	76	00	65	00	20	00	69	00	s.i.t.i.v.e..i.
0000B560	6E	00	66	00	6F	00	72	00	6D	00	61	00	74	00	69	00	n.f.o.r.m.a.t.i.
0000B570	6F	00	6E	00	20	00	73	00	61	00	66	00	65	00	20	00	o.n..s.a.f.e..
0000B580	66	00	72	00	6F	00	6D	00	20	00	70	00	72	00	79	00	f.r.o.m..p.r.y.
0000B590	69	00	6E	00	67	00	20	00	65	00	79	00	65	00	73	00	i.n.g..e.y.e.s.
0000B5A0	2E	00	00	00	CC	00	A8	00	01	00	4C	00	65	00	67	00	...I...Leg.
0000B5B0	61	00	6C	00	43	00	6F	00	70	00	79	00	72	00	69	00	a.l.C.o.p.y.r.i.
0000B5C0	67	00	68	00	74	00	00	00	43	00	6F	00	70	00	79	00	g.h.t...C.o.p.y.
0000B5D0	72	00	69	00	67	00	68	00	74	00	20	00	28	00	63	00	r.i.g.h.t... (c.
0000B5E0	29	00	20	00	32	00	30	00	30	00	30	00	2D	00	32	00)...2.0.0.0.-2.
0000B5F0	30	00	30	00	31	00	20	00	62	00	79	00	20	00	54	00	0.0.1...b.y..T.
0000B600	77	00	69	00	73	00	74	00	65	00	64	00	20	00	50	00	w.i.s.t.e.d...P.
0000B610	65	00	61	00	72	00	20	00	50	00	72	00	6F	00	64	00	e.a.r...P.r.o.d.
0000B620	75	00	63	00	74	00	69	00	6F	00	6E	00	73	00	2C	00	u.c.t.i.o.n.s...
0000B630	20	00	41	00	6C	00	6C	00	20	00	72	00	69	00	67	00	...A.l.l...r.i.g.
0000B640	68	00	74	00	73	00	20	00	72	00	65	00	73	00	65	00	h.t.s...r.e.s.e.
0000B650	72	00	76	00	65	00	64	00	20	00	77	00	6F	00	72	00	r.v.e.d...w.o.r.
0000B660	6C	00	64	00	77	00	69	00	64	00	65	00	2E	00	00	00	l.d.w.i.d.e....
0000B670	38	00	16	00	01	00	50	00	72	00	6F	00	64	00	75	00	8....P.r.o.d.u.
0000B680	63	00	74	00	4E	00	61	00	6D	00	65	00	00	00	00	00	c.t.N.a.m.e....
0000B690	43	00	61	00	6D	00	6F	00	75	00	66	00	6C	00	61	00	C.a.m.o.u.f.l.a.
0000B6A0	67	00	65	00	00	00	00	00	34	00	14	00	01	00	46	00	g...4...F.
0000B6B0	69	00	6C	00	65	00	56	00	65	00	72	00	73	00	69	00	i.l.e.V.e.r.s.i.
0000B6C0	6F	00	6E	00	00	00	00	00	31	00	2E	00	30	00	31	00	o.n...1...0.1.
0000B6D0	2E	00	30	00	30	00	30	00	31	00	00	00	38	00	14	00	...0.0.0.1...8...
0000B6E0	01	00	50	00	72	00	6F	00	64	00	75	00	63	00	74	00	...P.r.o.d.u.c.t.
0000B6F0	56	00	65	00	72	00	73	00	69	00	6F	00	6E	00	00	00	V.e.r.s.i.o.n...
0000B700	31	00	2E	00	30	00	31	00	2E	00	30	00	30	00	30	00	1...0.1...0.0.0.
0000B710	31	00	00	00	34	00	12	00	01	00	49	00	6E	00	74	00	1...4...I.n.t.
0000B720	65	00	72	00	6E	00	61	00	6C	00	4E	00	61	00	6D	00	e.r.n.a.l.N.a.m.
0000B730	65	00	00	00	43	00	61	00	6D	00	53	00	68	00	65	00	e...C.a.m.S.h.e.
0000B740	6C	00	6C	00	00	00	00	00	44	00	1A	00	01	00	4F	00	l.l...D...O.
0000B750	72	00	69	00	67	00	69	00	6E	00	61	00	6C	00	46	00	r.i.g.i.n.a.l.F.
0000B760	69	00	6C	00	65	00	6E	00	61	00	6D	00	65	00	00	00	i.l.e.n.a.m.e...
0000B770	43	00	61	00	6D	00	53	00	68	00	65	00	6C	00	6C	00	C.a.m.S.h.e.l.l.

2.2.5 File size

From Figure 3, File size is 1474760 bytes.

2.2.6 MD5 hash of the file

As seen on figure 2, the md5 hash value of the image is d7641eb4da871d980adbe4d371eda2ad.

2.2.7 Key words found that are associated with the program/file.

DLL, dll, EXE, exe, CamShell.dll, Twisted Pear Productions, camouflage

2.3 Forensic Details

Using the strings file, it's time to look for any sign of programs. The dll's will be searched first, because there's a track from one of them that was modified and deleted (CamShell.dll), according to the FAT data and the timeline of the floppy:

As seen on figure 10, there are two interesting locations: 9793 and 40016. Using dcat to location 9793, the sector number has to be determined using the following formula:

$$Sector = \frac{decimallocation}{sectorsize} = \frac{9793}{512} = 19.126953125$$

Figure 10: Locations on the image of "dll" keyword

```
root@poseidon:/forensics/imagenes
[root@poseidon imagenes]# grep [Dd][Ll][Ll] v1_5.str
 9793 AMSHELLDLL
24944 ole32.dll
25180 shell32.dll
26104 advapi32.dll
27576 VBA6.DLL
28360 C:\WINDOWS\SYSTEM\MSVBVM60.DLL\3
38644 MSVBVM60.DLL
39208 DllFunctionCall
40016 CamShell.dll
40029 DllCanUnloadNow
40045 DllGetClassObject
40063 DllRegisterServer
40081 DllUnregisterServer
[root@poseidon imagenes]#
```

Figure 11 information look like the fat contents. Because we already have printed the fat contents, this information is useless, so we pick the other location:

$$Sector = \frac{decimallocation}{sectorsize} = \frac{40016}{512} = 78.15625$$

Figure 11: Contents of sector 19 and 20

```

root@poseidon:/forensics/imagenes
[root@poseidon imagenes]# dcat -a -f fat12 -u 512 v1_5 19 2
RJL      ....V.O.O...V.O.....C.a.m.S.h...9e.l.l...d.l...l...AMSHELLDLL . .M
.O.O....C*....C.l.i.c.y....d.o.c.....e.n.s.i.t...i.v.i.t.y_...P.o
.I.n.f.o.r...m.a.t.i.o.n...S.INFORM~1DOC ...M.O.O..eq.OJ....C.c.y.1...d...o
c.....S.e.c.u.r...i.t.y_...P.o...l.i..I.n.t.e.r...n.a.l...L.a...b...
INTERN~1DOC .D.M.O.O....O...~.C.c.y...d.o...#c.....S.e.c.u.r...#i
t.y_...P.o...l.i..I.n.t.e.r...#n.a.l...L.a...b...INTERN~2DOC .[.M.O.O....O....
B.c.y...d.o...c.....P.a.s.s.w...o.r.d...P.o...l.i.PASSWO~1DOC .l.M
.O.O...^..O.....B_P.o.l.i...c.y...d.o.c.....R.e.m.o.t...e...A.c.c.e...s.s
REMOTE~1DOC ...M.O.O...^..Ox.WK..C.c.y...d.o...c.....c.r.y.p.t...i
o.n...P.o...l.i..A.c.c.e.p...t.a.b.l.e...E.n.ACCEPT~1DOC .Z.M.O.O..Yq.O...X..
.NDEX   HTM .B.M.O.O...V.O.....
.....
.....
[root@poseidon imagenes]# █

```

Figure 12: Information for file using sector 78

```

[root@poseidon imagenes]# dstat -f fat12 v1_5 78
Sector: 78
Not Allocated
Cluster: 47
[root@poseidon imagenes]# ifind -a -f fat12 -d 78 v1_5
5
[root@poseidon imagenes]# ffind -a -f fat12 v1_5 5
* /CamShell.dll (_AMSHHELL.DLL)

```

The i-node 5 represents a deleted file with interesting content. It's time to recover the file to look for any keyword from the dirty word list or any other information that could be useful:

Figure 13: Recovery procedure for i-node 5

```
[root@poseidon imagenes]# icat -rf fat12 v1_5 5 > /forensics/imagenes/CamShell.dll
```

```
[root@poseidon imagenes]# file /forensics/imagenes/CamShell.dll
```

```
/forensics/imagenes/CamShell.dll: HTML document text
```

```
[root@poseidon imagenes]# ls -al CamShell.dll
```

```
-rw-r--r-- 1 root root 36864 Dec 6 22:24 CamShell.dll
```

This doesn't look like a DLL, because the File Type is HTML. We'll use a Hex Editor to clarify the contents of the file.

The HTML file located at the beginning of the recovered file has a size of 726 bytes, as seen on figure 7. The following bytes are zero until location 4096, which seems to be the start of a new file. Advancing in the file, it appears many keywords with the same name as Windows operating system calls, which suggest that this file could be a DLL, as seen on figure 15.

Going forward to location 29268 as seen on figure 16, there's the URL of the application, including the company name that created it.

Now the dirty word list is: DLL, dll, EXE, exe, CamShell.dll, Twisted Pear Productions, camouflage. The next action is to load <http://camouflage.freemove.co.uk> to try to find the application that we're looking for.

The browser returns an "unknown host" error. That means the web site doesn't exist. Using nslookup and querying the Domain Name Server for freemove.co.uk appears that the domain exist and the DNS for the domain are pointed to pridns1.svr.pol.co.uk (195.92.193.4), pridns4.svr.pol.co.uk (195.92.168.157), pridns3.svr.pol.co.uk (195.92.67.18) and pridns2.svr.pol.co.uk (195.92.195.161). However, when the site <http://www.freemove.co.uk> is opened, a welcome page from Wanadoo at United Kingdom appears (no freemove reference). Using a "ANY" query type for camouflage.freemove.co.uk appears a "HINFO" information: "1047865802". There's no ip address resolving to a machine or a recursive DNS directive "IN NS".

Asking directly to pridns1.svr.pol.co.uk (195.92.193.4), which is authoritative for the domain, using a “ANY” query type, the answer is the same. This means that the page is no longer resident under the freeserve domain.

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

Figure 14: Hex content of CamShell.dll

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000272	5B	77	61	76	65	2F	63	61	62	73	2F	66	6C	61	73	68	kwave/cabs/flash
00000288	2F	73	77	66	6C	61	73	68	2E	63	61	62	23	76	65	72	/swflash.cab#ver
00000304	73	69	6F	6E	3D	36	2C	30	2C	30	2C	30	22	0D	0A	20	sion=6,0,0,0"...
00000320	57	49	44	54	48	3D	22	38	30	30	22	20	48	45	49	47	WIDTH="800" HEIG
00000336	48	54	3D	22	36	30	30	22	20	69	64	3D	22	62	61	6C	HT="600" id="bal
00000352	6C	61	72	64	22	20	41	4C	49	47	4E	3D	22	22	3E	0D	lard" ALIGN="">.
00000368	0A	20	3C	50	41	52	41	4D	20	4E	41	4D	45	3D	6D	6F	. <PARAM NAME=mo
00000384	76	69	65	20	56	41	4C	55	45	3D	22	62	61	6C	6C	61	vie VALUE="balla
00000400	72	64	2E	73	77	66	22	3E	20	3C	50	41	52	41	4D	20	rd.swf"> <PARAM
00000416	4E	41	4D	45	3D	71	75	61	6C	69	74	79	20	56	41	4C	NAME=quality VAL
00000432	55	45	3D	68	69	67	68	3E	20	3C	50	41	52	41	4D	20	UE=high> <PARAM
00000448	4E	41	4D	45	3D	62	67	63	6F	6C	6F	72	20	56	41	4C	NAME=bgcolor VAL
00000464	55	45	3D	23	43	43	43	43	43	43	3E	20	3C	45	4D	42	UE=#CCCCCC> <EMB
00000480	45	44	20	73	72	63	3D	22	62	61	6C	6C	61	72	64	2E	ED src="ballard.
00000496	73	77	66	22	20	71	75	61	6C	69	74	79	3D	68	69	67	swf" quality=hig
00000512	68	20	62	67	63	6F	6C	6F	72	3D	23	43	43	43	43	43	h bgcolor=#CCCC
00000528	43	20	20	57	49	44	54	48	3D	22	38	30	30	22	20	48	C WIDTH="800" H
00000544	45	49	47	48	54	3D	22	36	30	30	22	20	4E	41	4D	45	EIGHT="600" NAME
00000560	3D	22	62	61	6C	6C	61	72	64	22	20	41	4C	49	47	4E	="ballard" ALIGN
00000576	3D	22	22	0D	0A	20	54	59	50	45	3D	22	61	70	70	6C	="... TYPE="appl
00000592	69	63	61	74	69	6F	6E	2F	78	2D	73	68	6F	63	6B	77	ication/x-shockw
00000608	61	76	65	2D	66	6C	61	73	68	22	20	50	4C	55	47	49	ave-flash" PLUGI
00000624	4E	53	50	41	47	45	3D	22	68	74	74	70	3A	2F	2F	77	NSPAGE="http://w
00000640	77	77	2E	6D	61	63	72	6F	6D	65	64	69	61	2E	63	6F	ww.macromedia.co
00000656	6D	2F	67	6F	2F	67	65	74	66	6C	61	73	68	70	6C	61	m/go/getflashpla
00000672	79	65	72	22	3E	3C	2F	45	4D	42	45	44	3E	0D	0A	3C	yer"></EMBED>.<<
00000688	2F	4F	42	4A	45	43	54	3E	0D	0A	3C	2F	63	65	6E	74	/OBJECT>.<</cent
00000704	65	72	3E	0D	0A	3C	2F	42	4F	44	59	3E	0D	0A	3C	2F	er>.<</BODY>.<</
00000720	48	54	4D	4C	3E	0D	0A	00	00	00	00	00	00	00	00	00	HTML>.....
00000736	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000752	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000768	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000784	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000800	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

Figure 15: Windows Operating System Calls

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00010880	74	65	78	74	4D	65	6E	75	5F	51	75	65	72	79	43	6F	textMenu_QueryCo
00010896	6E	74	65	78	74	4D	65	6E	75	00	00	00	5F	5F	76	62	ntextMenu...__vb
00010912	61	42	6F	6F	6C	56	61	72	00	00	00	00	5F	5F	76	62	aBoolVar...__vb
00010928	61	4F	62	6A	53	65	74	41	64	64	72	65	66	00	00	00	aObjSetAddrRef...
00010944	5F	5F	76	62	61	41	70	74	4F	66	66	73	65	74	00	00	__vbaAptOffset...
00010960	5F	5F	76	62	61	41	72	79	44	65	73	74	72	75	63	74	__vbaAryDestruct
00010976	00	00	00	00	49	53	68	65	6C	6C	45	78	74	49	6E	69	...IShellExtIni
00010992	74	5F	49	6E	69	74	69	61	6C	69	7A	65	00	00	00	00	t_initialize....
00011008	5F	5F	76	62	61	53	74	72	56	61	72	43	6F	70	79	00	__vbaStrVarCopy.
00011024	5F	5F	76	62	61	41	72	79	55	6E	6C	6F	63	6B	00	00	__vbaAryUnlock...
00011040	5F	5F	76	62	61	47	65	6E	65	72	61	74	65	42	6F	75	__vbaGenerateBou
00011056	6E	64	73	45	72	72	6F	72	00	00	00	00	5F	5F	76	62	ndsError...__vb
00011072	61	41	72	79	4C	6F	63	6B	00	00	00	00	49	43	6F	6E	aAryLock...ICon
00011088	74	65	78	74	4D	65	6E	75	00	00	00	00	5F	5F	76	62	textMenu...__vb
00011104	61	53	74	72	32	56	65	63	00	00	00	00	5F	5F	76	62	aStr2Vec...__vb
00011120	61	41	72	79	4D	6F	76	65	00	00	00	00	5F	5F	76	62	aAryMove...__vb
00011136	61	53	74	72	43	61	74	00	5F	5F	76	62	61	53	74	72	aStrCat...vbaStr
00011152	54	6F	55	6E	69	63	6F	64	65	00	00	00	5F	5F	76	62	ToUnicode...__vb
00011168	61	46	72	65	65	56	61	72	00	00	00	00	E4	14	02	00	aFreeVar...ä...
00011184	00	00	00	00	C0	00	00	00	00	00	00	46	5F	5F	76	62	...Ä...F__vb
00011200	61	53	74	72	56	61	72	4D	6F	76	65	00	5F	5F	76	62	aStrVarMove...__vb
00011216	61	53	74	72	4D	6F	76	65	00	00	00	00	5F	5F	76	62	aStrMove...__vb
00011232	61	53	74	72	43	6F	70	79	00	00	00	00	5F	5F	76	62	aStrCopy...__vb
00011248	61	45	72	72	6F	72	4F	76	65	72	66	6C	6F	77	00	00	aErrorOverflow...
00011264	5F	5F	76	62	61	46	72	65	65	53	74	72	00	00	00	00	__vbaFreeStr...
00011280	5F	5F	76	62	61	53	65	74	53	79	73	74	65	6D	45	72	__vbaSetSystemEr
00011296	72	6F	72	00	3C	2D	00	37	00	00	00	00	01	00	00	00	ror.<-.?.....
00011312	00	00	00	00	4C	2D	00	37	88	2D	00	37	8C	65	00	37	...L-.? =-.7 e.7
00011328	00	00	00	00	00	00	00	00	70	C8	60	00	00	00	00	00	...pE'.....
00011344	5F	5F	76	62	61	53	74	72	54	6F	41	6E	73	69	00	00	__vbaStrToAnsi...
00011360	2B	3D	FB	FC	FA	A0	68	10	A7	38	08	00	2B	33	71	B5	+="üüü h.\$8...+3qp
00011376	89	74	55	29	0B	99	D4	11	94	13	00	40	95	49	0A	D4	!tU).!Ö.!!@!I.Ö
00011392	2A	3D	FB	FC	FA	A0	68	10	A7	38	08	00	2B	33	71	B5	*="üüü h.\$8...+3qp
00011408	88	74	55	29	0B	99	D4	11	94	13	00	40	95	49	0A	D4	!tU).!Ö.!!@!I.Ö

© SANS Institute 2000 - 2005, Author retains full

Figure 16: Application URL

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00029104	00	00	00	00	00	00	00	00	00	00	00	00	44	00	00	00D...
00029120	00	00	56	00	61	00	72	00	46	00	69	00	6C	00	65	00	..Var.File.
00029136	49	00	6E	00	66	00	6F	00	00	00	00	00	24	00	04	00	Info...\$...
00029152	00	00	54	00	72	00	61	00	6E	00	73	00	6C	00	61	00	..Trans.la.
00029168	74	00	69	00	6F	00	6E	00	00	00	00	00	09	04	B0	04	tion.....*
00029184	B8	03	00	00	01	00	53	00	74	00	72	00	69	00	6E	00Str.in.
00029200	67	00	46	00	69	00	6C	00	65	00	49	00	6E	00	66	00	g.File.Inf.
00029216	6F	00	00	00	94	03	00	00	01	00	30	00	34	00	30	00	o...0.4.0.
00029232	39	00	30	00	34	00	42	00	30	00	00	00	64	00	4C	00	9.0.4.B.0...d.L.
00029248	01	00	43	00	6F	00	6D	00	6D	00	65	00	6E	00	74	00	..Com.men.t.
00029264	73	00	00	00	68	00	74	00	74	00	70	00	3A	00	2F	00	s...http://
00029280	2F	00	77	00	77	00	77	00	2E	00	63	00	61	00	6D	00	/www...cam.
00029296	6F	00	75	00	66	00	6C	00	61	00	67	00	65	00	2E	00	ou.flage...
00029312	66	00	72	00	65	00	65	00	73	00	65	00	72	00	76	00	fre.es.serv.
00029328	65	00	2E	00	63	00	6F	00	2E	00	75	00	6B	00	00	00	e...co.uk...
00029344	54	00	32	00	01	00	43	00	6F	00	6D	00	70	00	61	00	T.2...Com.pa.
00029360	6E	00	79	00	4E	00	61	00	6D	00	65	00	00	00	00	00	ny.Name....
00029376	54	00	77	00	69	00	73	00	74	00	65	00	64	00	20	00	Twisted...
00029392	50	00	65	00	61	00	72	00	20	00	50	00	72	00	6F	00	Pea.r...Pro.
00029408	64	00	75	00	63	00	74	00	69	00	6F	00	6E	00	73	00	du.cti.on.s.
00029424	00	00	00	00	B0	00	88	00	01	00	46	00	69	00	6C	00	...*.I...Fil.
00029440	65	00	44	00	65	00	73	00	63	00	72	00	69	00	70	00	e.Descrip.
00029456	74	00	69	00	6F	00	6E	00	00	00	00	00	4B	00	65	00	tion...Ke.
00029472	65	00	70	00	73	00	20	00	66	00	69	00	6C	00	65	00	eps...file.
00029488	73	00	20	00	63	00	6F	00	6E	00	74	00	61	00	69	00	s...cont.ai.
00029504	6E	00	69	00	6E	00	67	00	20	00	73	00	65	00	6E	00	ning...sen.
00029520	73	00	69	00	74	00	69	00	76	00	65	00	20	00	69	00	s.i.t.i.v.e...i.
00029536	6E	00	66	00	6F	00	72	00	6D	00	61	00	74	00	69	00	n.f.o.r.m.a.t.i.
00029552	6F	00	6E	00	20	00	73	00	61	00	66	00	65	00	20	00	o.n...safe...
00029568	66	00	72	00	6F	00	6D	00	20	00	70	00	72	00	79	00	f.r.o.m...pr.y.
00029584	69	00	6E	00	67	00	20	00	65	00	79	00	65	00	73	00	ing...eye.s.
00029600	2E	00	00	00	CC	00	A8	00	01	00	4C	00	65	00	67	00	...I...Leg.
00029616	61	00	6C	00	43	00	6F	00	70	00	79	00	72	00	69	00	a.l.Cop.y.r.i.
00029632	67	00	68	00	74	00	00	00	43	00	6F	00	70	00	79	00	g.h.t...C.op.y.

Using an alternate way, we'll use google to look for the dirty word list. First we try with the following string: camouflage CamShell.dll download.

Nothing interesting comes up at figure 17, so we try: "Twisted pear productions" camouflage download, at figure 18.

The first link of figure 18 is shown at figure 19. There's an association of the keyword "Twisted Pear Productions" with "camouflage" and the URL at figure 14. From this page we can conclude that the application name is Camouflage. There's a URL providing the camouflage software version 1.1.1 but there's no proof of this version being the latest one. We'll check other URLs for the latest version.

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

Figure 17: Google search for “camouflage CamShell.dll download”

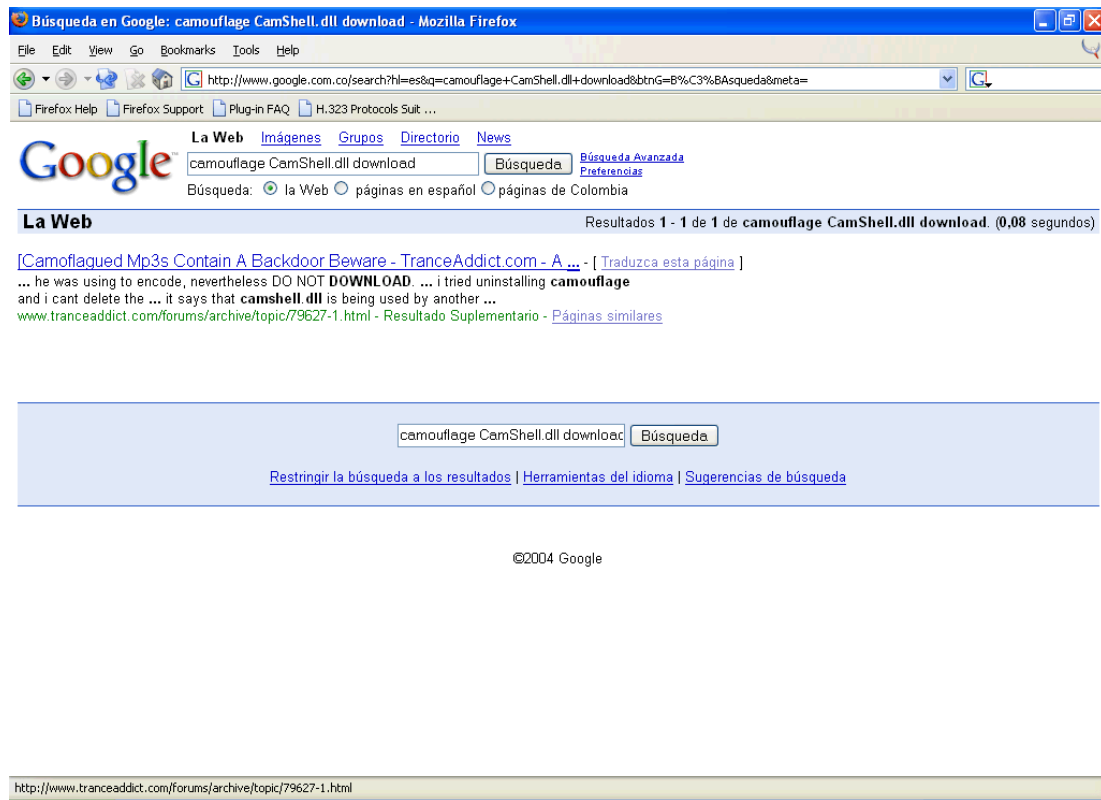


Figure 18: Google search for: "Twisted pear productions" camouflage download

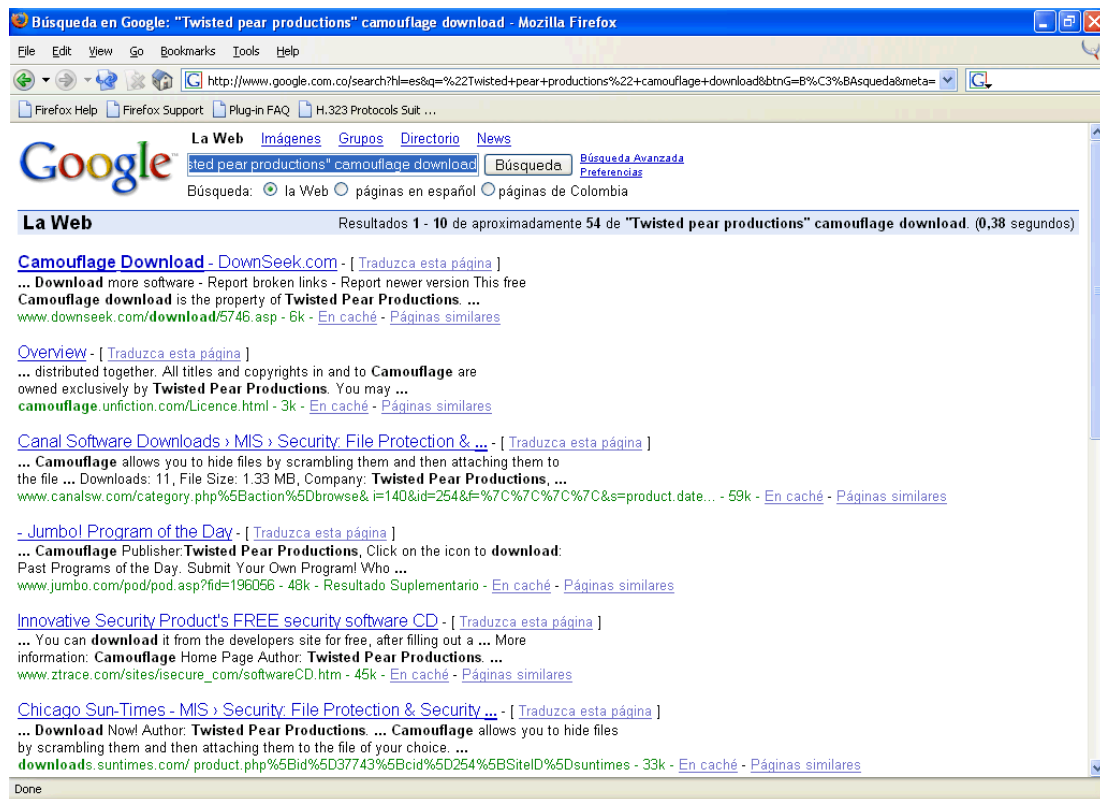


Figure 19: First link from figure 11
(http://www.downseek.com/download/5746.asp)



Following the second link at figure 18, a mirror page for Camouflage Home Page appears (Figure 20). The download link from this page allows downloading version 1.2.1, which is the latest one. The software was downloaded and installed on a Windows machine. The figure 21 provides information about the created directory and all the contents inside it.

The MD5 hash of the CamShell.dll file is shown at figure 22:

Using the read-only mounted image, we'll copy all the DOC files from the root directory of the image to analyze them with camouflage. This is shown in figure 23.

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

**Figure 20: Mirror from Camouflage Home Page
(<http://camouflage.unfiction.com>)**

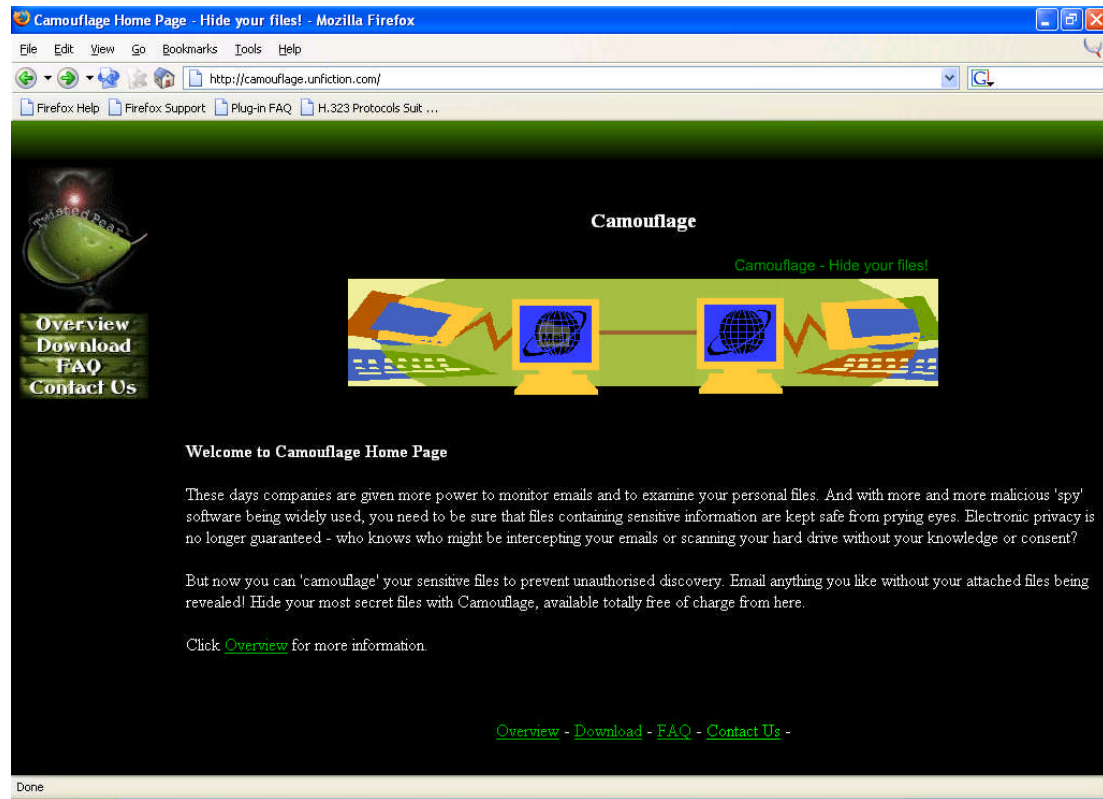


Figure 21: Camouflage executable directory

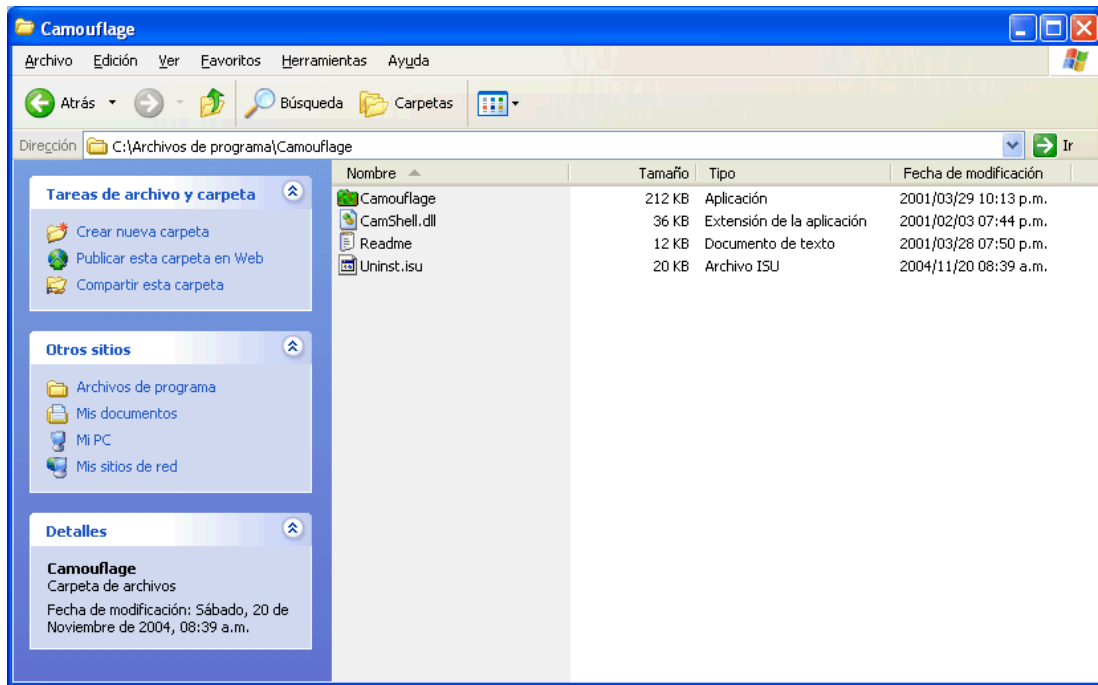
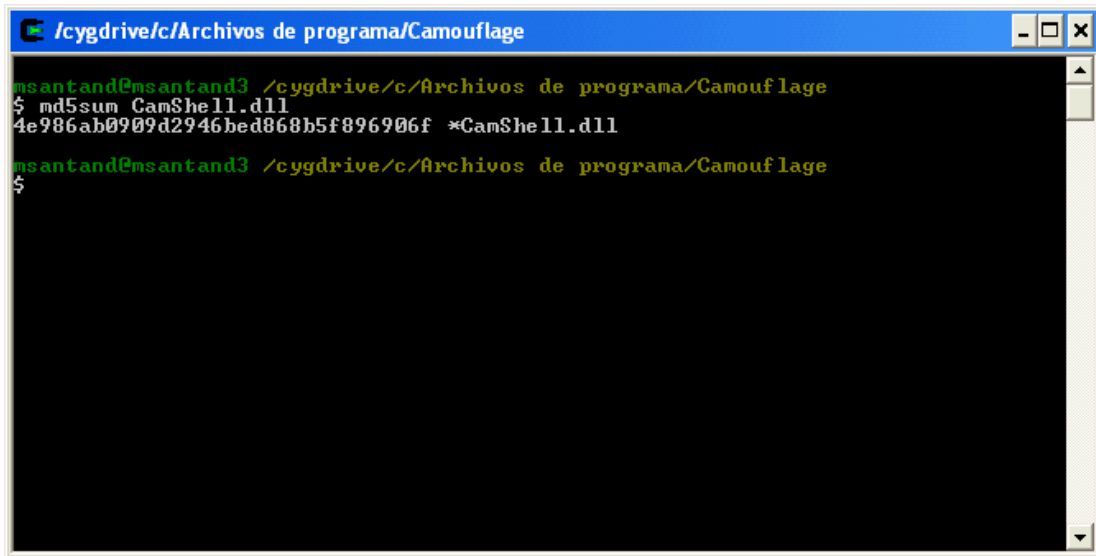


Figure 22: MD5 hash of CamShell.dll

© SANS Institute 2000 - 2005, Author



```
msantand@msantand3 /cygdrive/c/Archivos de programa/Camouflage
$ md5sum CamShell.dll
4e986ab0909d2946bed868b5f896906f *CamShell.dll
msantand@msantand3 /cygdrive/c/Archivos de programa/Camouflage
$
```

Figure 23: Copying files from the read-only mounted image

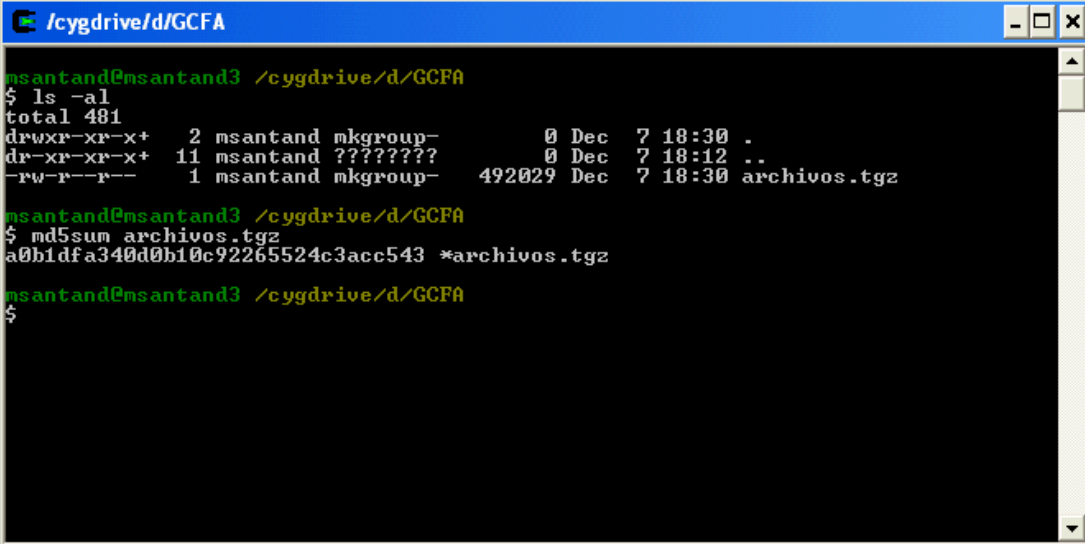
© SANS Institute 2000 - 2005, Author retains full rights.

```
root@poseidon:/mnt
[root@poseidon imagenes]# mount
/dev/cciss/c0d0p1 on / type ext3 (rw)
none on /proc type proc (rw)
usbdevfs on /proc/bus/usb type usbdevfs (rw)
/dev/cciss/c0d0p2 on /archivos type ext3 (rw)
none on /dev/pts type devpts (rw,gid=5,mode=620)
none on /dev/shm type tmpfs (rw)
/dev/cciss/c0d0p3 on /usr type ext3 (rw)
/forensics/imagenes/v1_5 on /mnt type vfat (ro,loop=/dev/loop0)
[root@poseidon imagenes]# cd /mnt
[root@poseidon mnt]# tar czvf /forensics/imagenes/archivos.tgz .
./
./Information_Sensitivity_Policy.doc
./Internal_Lab_Security_Policy1.doc
./Internal_Lab_Security_Policy.doc
./Password_Policy.doc
./Remote_Access_Policy.doc
./Acceptable_Encryption_Policy.doc
[root@poseidon mnt]# md5sum /forensics/imagenes/archivos.tgz
a0bidfa340d0b10c92265524c3acc543  /forensics/imagenes/archivos.tgz
[root@poseidon mnt]#
```

From figures 23 and 24 we can conclude that checksums are ok and it's safe to continue.

© SANS Institute 2000 - 2005, Author

Figure 24: MD5 Hash verification



```
msantand@msantand3 /cygdrive/d/GCFA
$ ls -al
total 481
drwxr-xr-x+  2 msantand mkgroup-    0 Dec  7 18:30 .
dr-xr-xr-x+ 11 msantand ?????????  0 Dec  7 18:12 ..
-rw-r--r--   1 msantand mkgroup- 492029 Dec  7 18:30 archivos.tgz

msantand@msantand3 /cygdrive/d/GCFA
$ md5sum archivos.tgz
a0b1dfa340d0b10c92265524c3acc543 *archivos.tgz

msantand@msantand3 /cygdrive/d/GCFA
$
```

The camouflage software is a steganography tool. That means that it's able to scramble information of a file inside another without making the host file to lose any of its properties. That's why a photo can be seen as it is, a Word document can be edited, modified, same as any other document.

The files are unpacked and in each of them the uncamouflage operation is performed with right click. All the files except Internal_Lab_Security_Policy.doc showed the message seen at figure 25.

The uncamouflage operation for Internal_Lab_Security_Policy.doc showed the following message seen at figure 26.

The Opportunity.txt file is shown at figure 27 by double clicking the file.

This is the first proof of Robert stealing information for Rift. Now we have to look for the Client Authorized table database and the Schematics. We

previously tried to uncamouflage the other files with no success. There's an interesting keyword on figure 27 called "*First Name*". Let's try to uncamouflage the files using their first part of the name (first name keyword delimited by "_") as their password.

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

Figure 25: Uncamouflage operation for all files except Internal_Lab_Security_Policy.doc

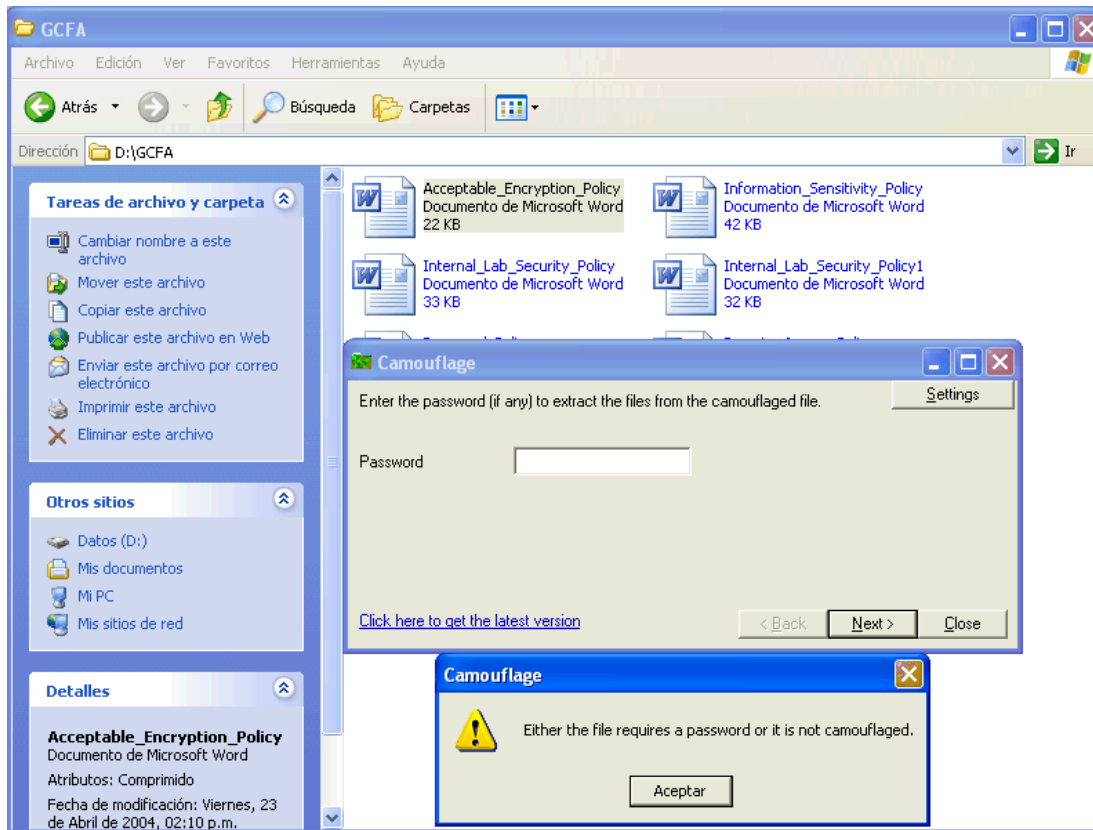
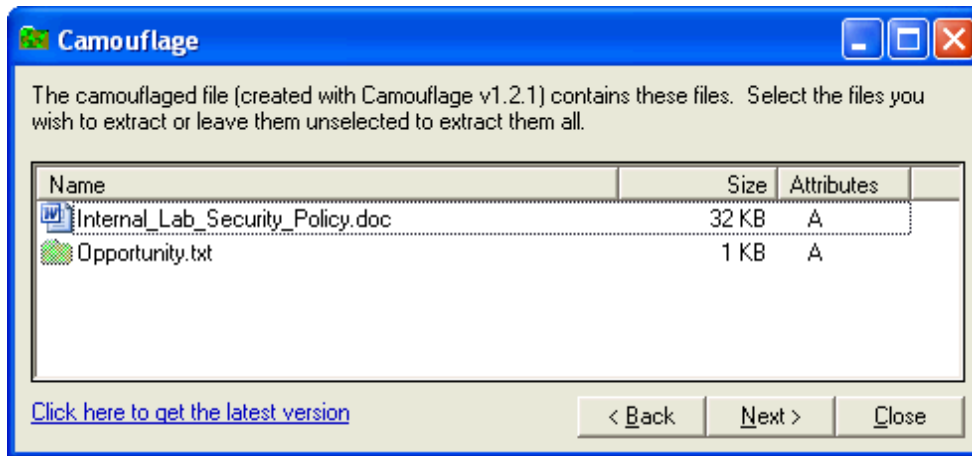
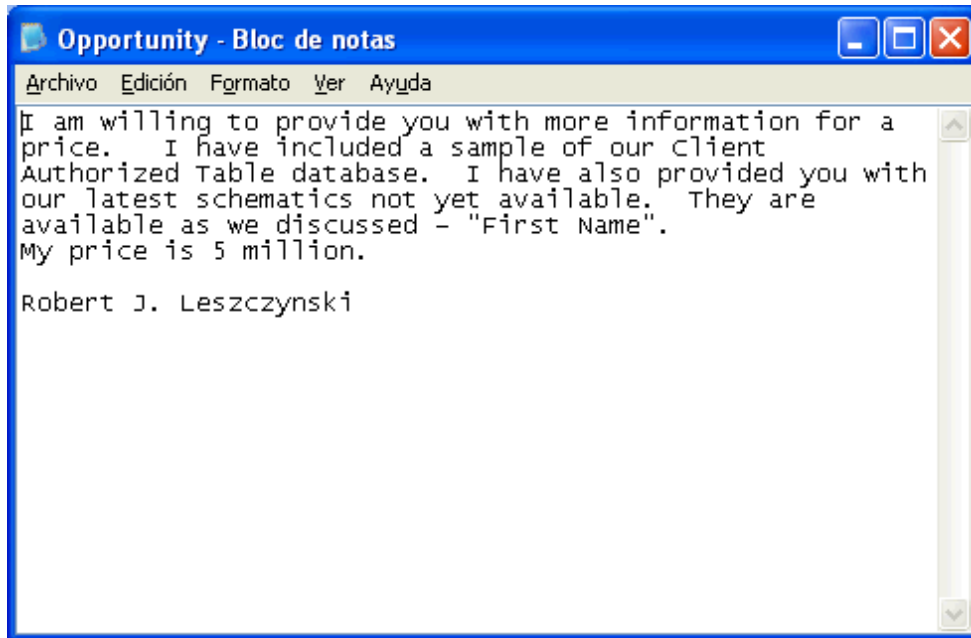


Figure 26: Uncamouflage operation for file Internal_Lab_Security_Policy.doc



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

Figure 27: Camouflaged file “Opportunity.txt” inside the file Internal_Lab_Security_Policy.doc



The files Acceptable_Encryption_Policy.doc and Information_Sensitivity_Policy.doc showed the message at figure 28.

The message showed by Password_Policy.doc is displayed at figure 29.

The message showed by Remote_Access_Policy.doc is displayed at figure 30.

Figure 29 files looks like the schematics we're looking for. We can look at this jpeg files at figure 32.

File at figure 30 looks like the client database we're looking for. We can look at this database at figure 31.

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

Figure 28: Message provided by files Acceptable_Encryption_Policy.doc and Information_Sensitivity_Policy.doc

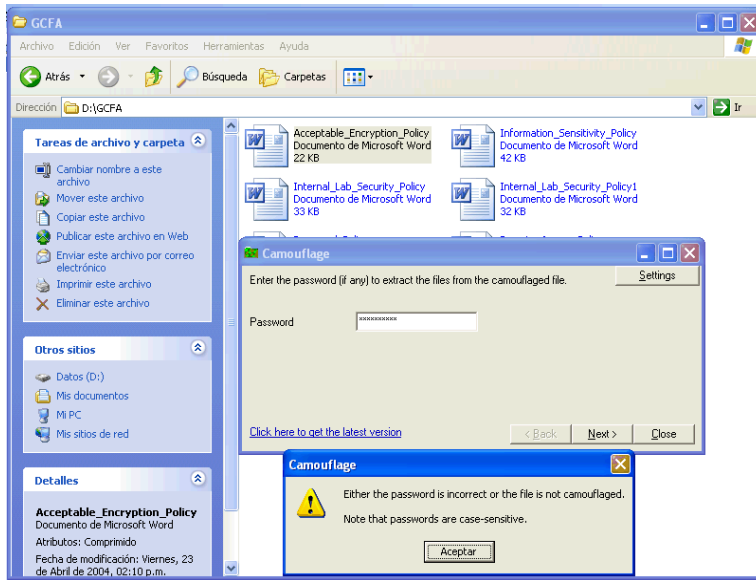


Figure 29: Message shown by uncamouflage operation for file Password_Policy.doc

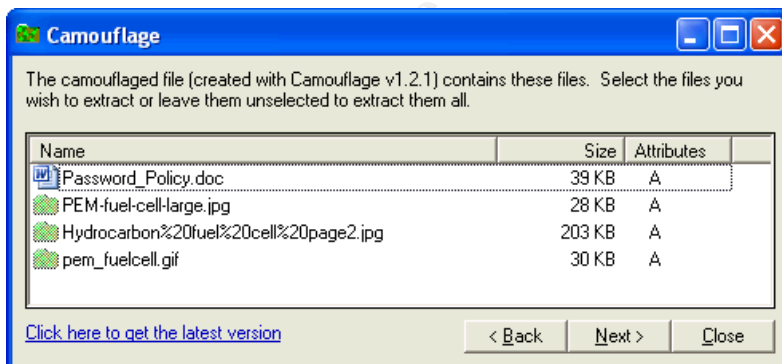


Figure 30: Message shown by uncamouflage operation for file

Remote_Access_Policy.doc

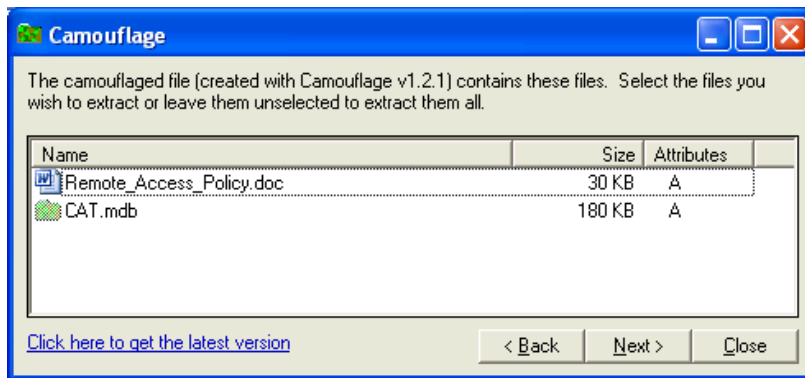


Figure 31: Client database camouflaged at file Password_Policy.doc

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

Microsoft Excel - Libro2

Archivo Edición Ver Insertar Formato Herramientas Datos Quicksheet Ventana ?

Escribe una pregunta

Arial 10

Responder con cambios... Terminar revisión...

	A	B	C	D	E	F	G	H	I	J	K	L	M
	First	Last	Phone	Company	Address	Address1	City	State	Zipcode	Account	Password		
1	Patrick	Roy		The Magic Lamp	4150 Regents Park	Row #170	Calgary	CAN	R4316DF	roythema	rJag6Q00		
2	Edward	Cash	212-562-0997	E & C Inc.	76 S. King St	Suite 300	Santa Barbara	CA	80124	cashking	Of8uQ1fC		
3	Jerry	Jackson	410-677-7223	Double J's	11561 W. 27 St.		Baltimore	MD	20278	jack27st	JLbW3Pq5		
4	Jodie	Kelly		Data Movers	7256 Beerwah Ave.	Suite 110	Wetherby	U.K.	LS22 6RG	kellbeer	tmu0ENOK		
5	Bob	Esposito	703-233-2048	Cook Labs	245 Main St		Alexandria	VA	20231	espomain	y4NSHMNF		
6	Jeff	Hayes	404-893-5521	Big Sky First	90 Old Saw Mill Rd		Billings	MT	59332	hayeolds	3R30bb7i		
7	Marie	Horton	800-234-king	King Labs, Inc.	700 King Labs Ave	Suite 900	Biloxi	MS	39533	hortking	Yk7Sr4pA		
8	Lenny	Jones	877-Get-done	Quick Printing	99 E. Grand View Dr		Omaha	NE	56098	joneeast	B68y48RH		
9	Steve	Bei	616-833-0129	Island Labs	65 Kiwi Way		Honolulu	HA	93991	beikiwiw	JDH20u26		
10	Roger	Forrester	210-586-2312	TCFL	188 Greenville Rd		Austin	TX	77239	forrgree	si4OW6UV		
11	David	Lee	866-554-0922	Tech Vision	300 Lone Grove Lane		Wichita	KS	30189	leetechw	O1A26a3k		
12													
13													
14													
15													
16													
17													
18													
19													
20													
21													
22													
23													
24													
25													
26													
27													
28													
29													
30													
31													
32													
33													

Datos externos

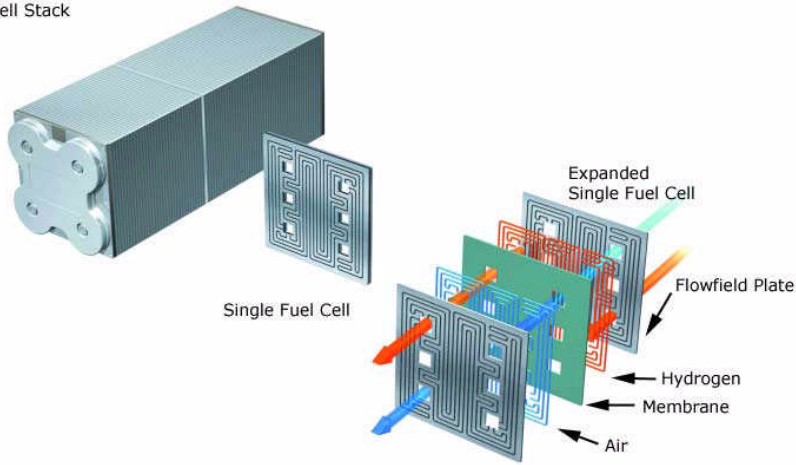
CAT

Listo

Figure 32: Schematics camouflaged at file Password_Policy.doc

Design of a PEM Fuel Cell

Fuel Cell Stack



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

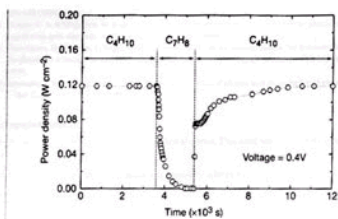


Figure 3 Effect of switching fuel type on the cell with the Cu-ceria composite anode at 973 K. The power density of the cell is shown as a function of time. The fuel was switched from *n*-butane (C₄H₁₀) to toluene (C₇H₈) and back to *n*-butane.

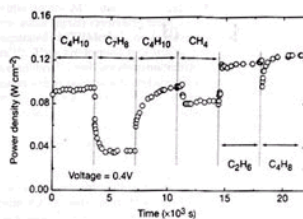
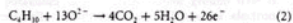
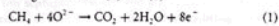


Figure 4 Effect of switching fuel type on the cell with the Cu-doped ceria composite anode at 973 K. The power density is shown as a function of time. The fuels were: *n*-butane (C₄H₁₀), toluene (C₇H₈), *n*-butane, methane (CH₄), ethane (C₂H₆), and 1-butene (C₄H₈).

Single crystals
amorphous
ionic antiferroelectrics
ground state

higher temperature. Visual inspection of a cell after two days in *n*-butane at 1,073 K showed that the anode itself remained free of the tar deposits that covered the alumina walls.

Although it is possible that the power generated from *n*-butane fuels resulted from oxidation of H₂—formed by gas-phase reactions of *n*-butane that produce hydrocarbons with a lower C:H ratio—other evidence shows that this is not the case. First, experiments were conducted in which the cell was charged with *n*-butane and then operated in a batch mode without flow. After 30 minutes of batch operation with the cell short-circuited, GC analysis showed that all of the *n*-butane in the cell had been converted completely to CO₂ and water. (Negligible amounts of CO₂ were formed in a similar experiment with an open circuit.) Second, analysis of the CO₂ formed under steady-state flow conditions, shown in Fig. 2, demonstrates that the rate of CO₂ formation increased linearly with the current density. (It was not possible for us to quantify the amount of water formed in our system.) Figure 2 includes data for both *n*-butane at 973 K, and methane at 973 K and 1,073 K. The lines in the figure were calculated assuming complete oxidation of methane (the dashed line) and *n*-butane (the solid line) to CO₂ and water according to reactions (1) and (2):



With methane, only trace levels of CO were observed along with CO₂, so that the agreement between the data points and the calculation demonstrates consistency in the measurements and no leaks in the cell. With *n*-butane, simultaneous, gas-phase, free-radical reactions to give hydrocarbons with various C:H ratios make quantification more difficult; however, the data still suggest that complete oxidation is the primary reaction. Furthermore, the batch experiments show that the secondary products formed by gas-phase reactions are ultimately oxidized as well. Taken together, these results demonstrate the direct, electrocatalytic oxidation of a higher hydrocarbon in a SOFC.

Along with our observation of stable power generation with *n*-butane for 48 hours, Fig. 3 further demonstrates the stability of the composite anodes against coke formation. Aromatic molecules, such as toluene, are expected to be precursors to the formation of graphitic coke deposits. In Fig. 3, the power density was measured at 973 K and 0.4 V while the fuel was switched from dry *n*-butane, to 0.033 bar of toluene in He for 30 minutes, and back to dry *n*-butane. The data show that the performance decreased rapidly in the presence of toluene. Upon switching back to dry *n*-butane, however,

the current density returned to 0.12 W cm⁻² after one hour. Because the return was not instantaneous, it appears that carbon formation occurred during exposure to toluene, but that the anode is self-cleaning. We note that the electrochemical oxidation of soot has been reported by others¹¹.

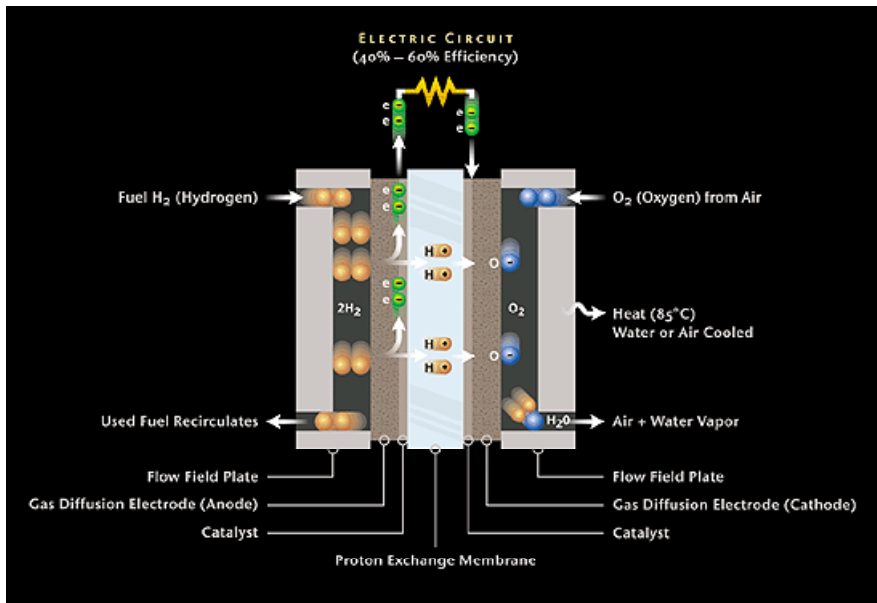
The data in Fig. 4 show that further improvements in cell performance can be achieved. For these experiments, samaria-doped ceria was substituted for ceria in the anode, and the current densities were measured at a potential of 0.4 V at 973 K. The power densities for H₂ and *n*-butane in this particular cell were approximately 20% lower than for the first cell, which is within the range of our ability to reproduce cells. However, the power densities achieved for some other fuels were significantly higher. In particular, stable power generation was now observed for toluene. Similarly, Fig. 4 shows that methane, ethane and 1-butene could be used as fuels to produce electrical energy. The data show transients for some of the fuels, which are at least partially due to switching.

The role of samaria in enhancing the results for toluene and some of the other hydrocarbons is uncertain. While samaria is used to enhance mixed (ionic and electronic) conductivity in ceria and could increase the active, three-phase boundary in the anode, samaria is also an active catalyst¹². Other improvements in the performance of SOFCs are possible. For example, the composite anodes could be easily attached to the cathode-supported, thin-film electrolytes that have been used by others to achieve very high power densities⁹. In addition to raising the power density, thinner electrolytes may also allow lower operating temperatures.

Additional research is clearly necessary for commercial development of fuel cells which generate electrical power directly from hydrocarbons; however, the work described here suggests that SOFCs have an intriguing future as portable, electric generators and possibly even as energy sources for transportation. The simplicity afforded by not having to reform the hydrocarbon fuels is a significant advantage of these cells. □

Received 13 September 1999; accepted 26 January 2000.

1. Steele, B. C. H. Running on natural gas. *Nature* **406**, 620–621 (1999).
2. Service, R. F. Bringing fuel cells down to earth. *Science* **285**, 482–485 (1999).
3. Perry Murray, E., Tsai, T. & Barnett, S. A. A direct-methane fuel cell with a ceria-based anode. *Nature* **406**, 649–651 (1999).
4. Palma, E. S., Zolotarev, J., Vohs, J. M. & Gorte, R. J. Ceria-based anodes for the direct oxidation of methane in solid oxide fuel cells. *Langmuir* **11**, 4832–4837 (1995).
5. Park, S., Craciun, R., Vohs, J. M. & Gorte, R. J. Direct oxidation of hydrocarbons in a solid oxide fuel cell: I. methane oxidation. *J. Electrochem. Soc.* **146**, 3603–3605 (1999).
6. Steele, B. C. H., Kelly, J., Middleton, P. H. & Rudkin, R. Oxidation of methane in solid-state electrochemical reactors. *Solid State Ionics* **28**, 1547–1552 (1988).
7. Lloyd, A. C. The power plant in your basement. *Sci. Am.* **281**(1), 80–86 (1999).

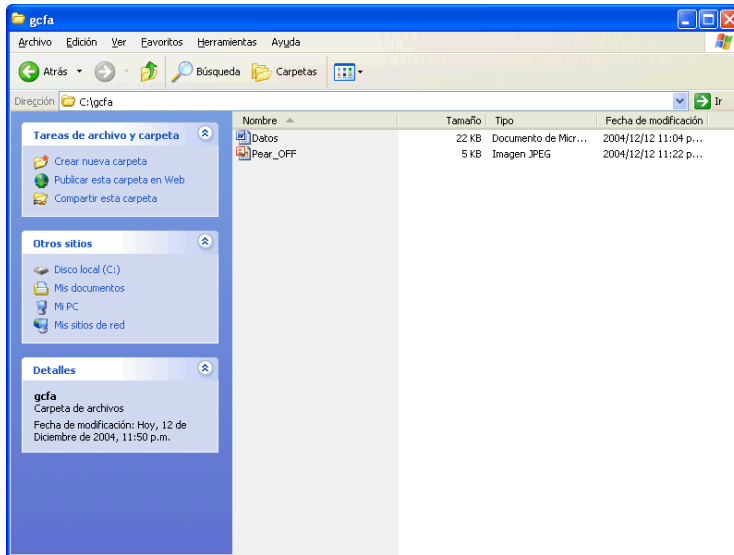


The program used is steganography software to scramble information from a file inside another. It was used to camouflage the schematics of the fuel cells and the client database of Ballard Industries.

The uncamouflage operation of the Camouflage software locates the scrambled file inside the "normal" one. It was shown in figures 26, 29 and 30.

Now we'll show the camouflage operation. Consider the following two files:

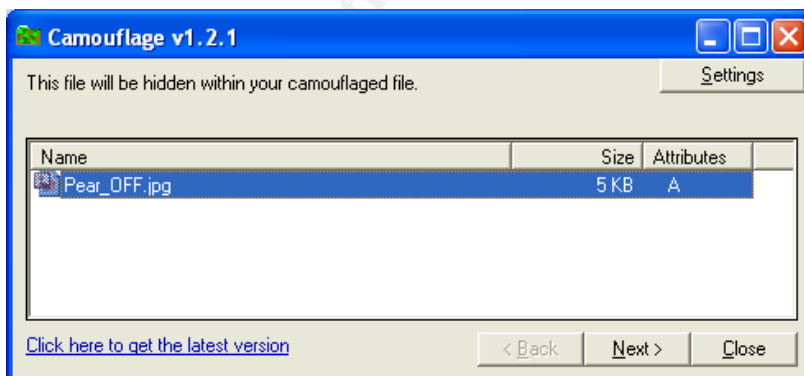
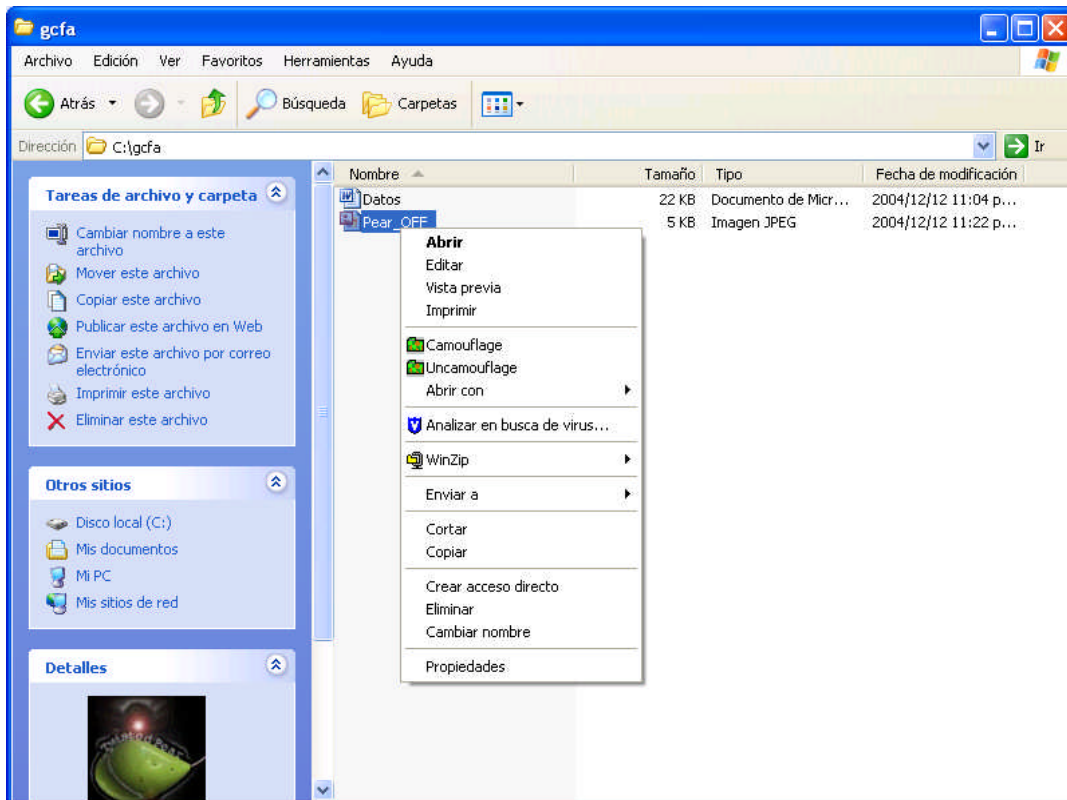
Figure 33: Camouflage example using two files

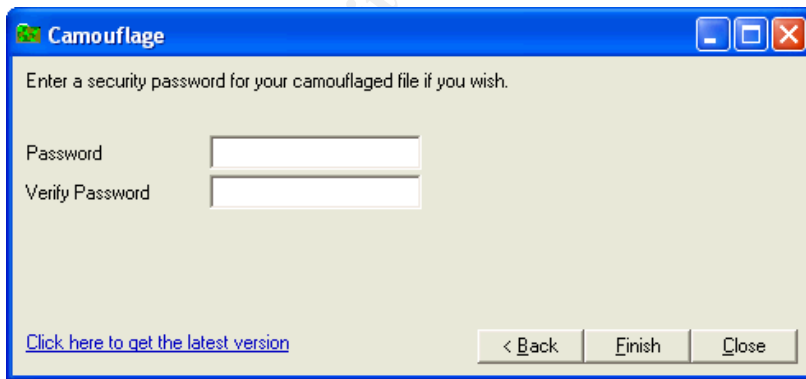
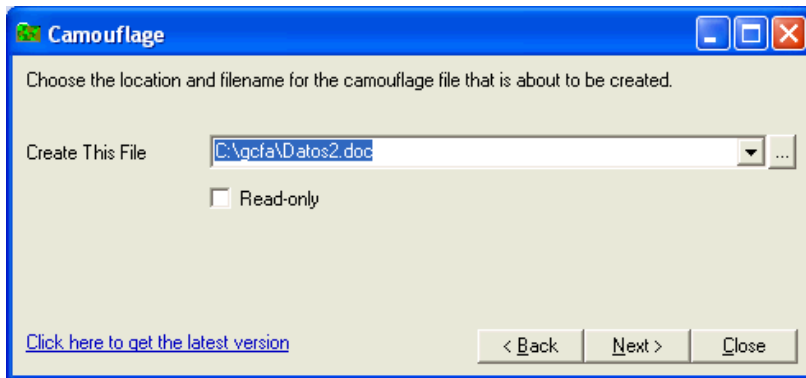
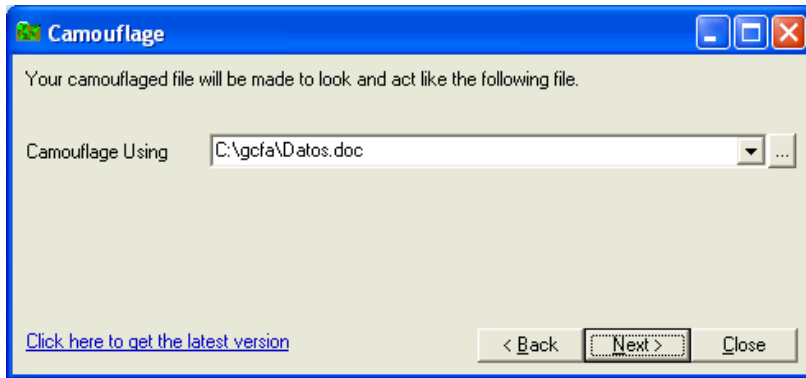


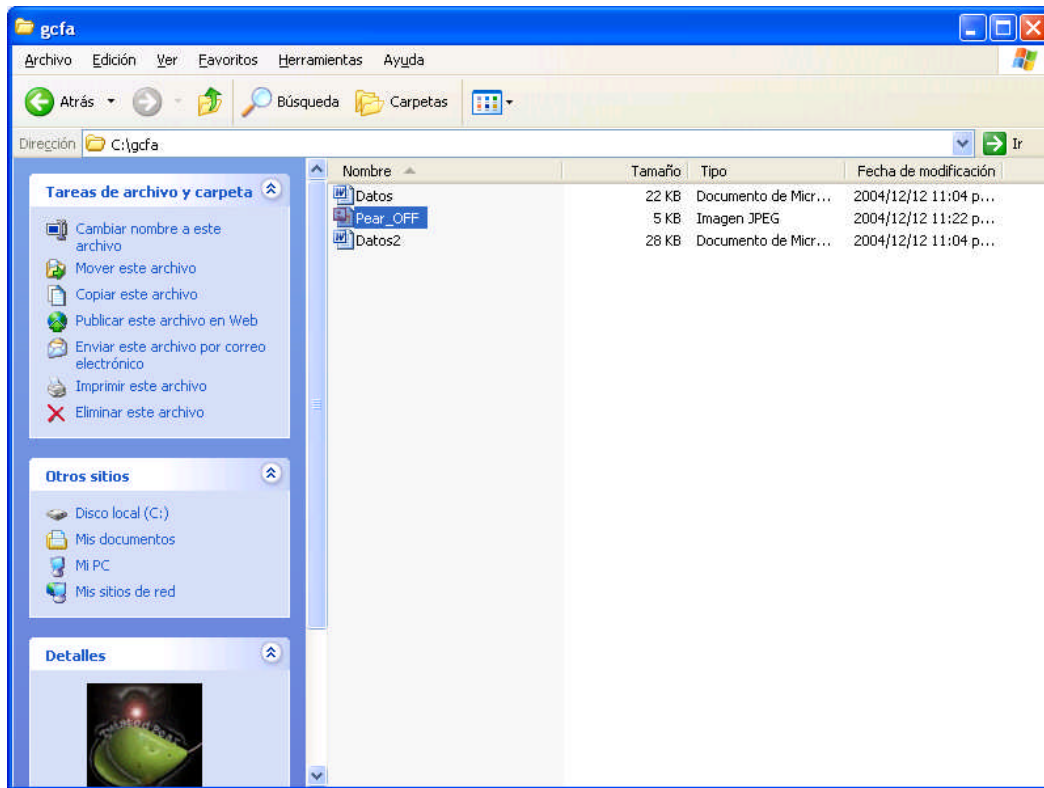
We'll camouflage Pear_OFF.jpg inside Datos.doc file. The procedure is shown on figure 34. The output file will be Datos2.doc. If we perform the uncamouflage operation on Datos2.doc, we'll see the message displayed at figure 35.

From the timeline displayed at figure 6 and knowing that the files that got camouflaged files are Remote_Access_Policy.doc, Password_Policy.doc and Internal_Lab_Security_Policy.doc, we conclude that the last time that the camouflage software was used was in April 26 2004 – 9:46:36 A.M, corresponding to the time where Remote_Access_Policy.doc was created again in the floppy.

Figure 34: Camouflage procedure on two files

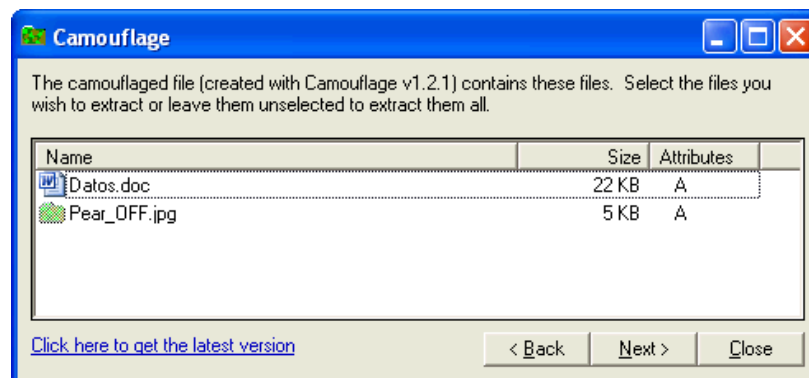






© SANS Institute 2000 - 2005, Author retains full rights.

Figure 35: Uncamouflage operation for Datos2.doc



2.4 Program Identification

We tried to locate the software previously and using google it was possible to locate the mirror <http://camouflage.unfiction.com> (figure 20) for the original site <http://www.camouflage.freemove.co.uk>, which no longer exist

Since there's no possibility of downloading sources for camouflage from <http://camouflage.unfiction.com> because there's no link for that, we'll try to locate them using google and the string: "Twisted pear productions" camouflage source download, on figure 36.

Nothing comes up, so we try with a tool called copernic, which uses the following search engines: Altavista, AOL Search, Compuserve, Copernic, Espotting, FAST Search, FindWhat, HotBot, LookSmart, Lycos, Mamma.com, MSN Web Search, Netscape Netcenter, Open Directory Project, Teoma, WiseNut, Yahoo! on figure 37.

Still nothing comes up. Since there's no possible download for the sources, we'll try comparing the CamShell.dll located on the image and the one located at the installed program.

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

Figure 36: Google search for "Twisted pear productions" camouflage source download

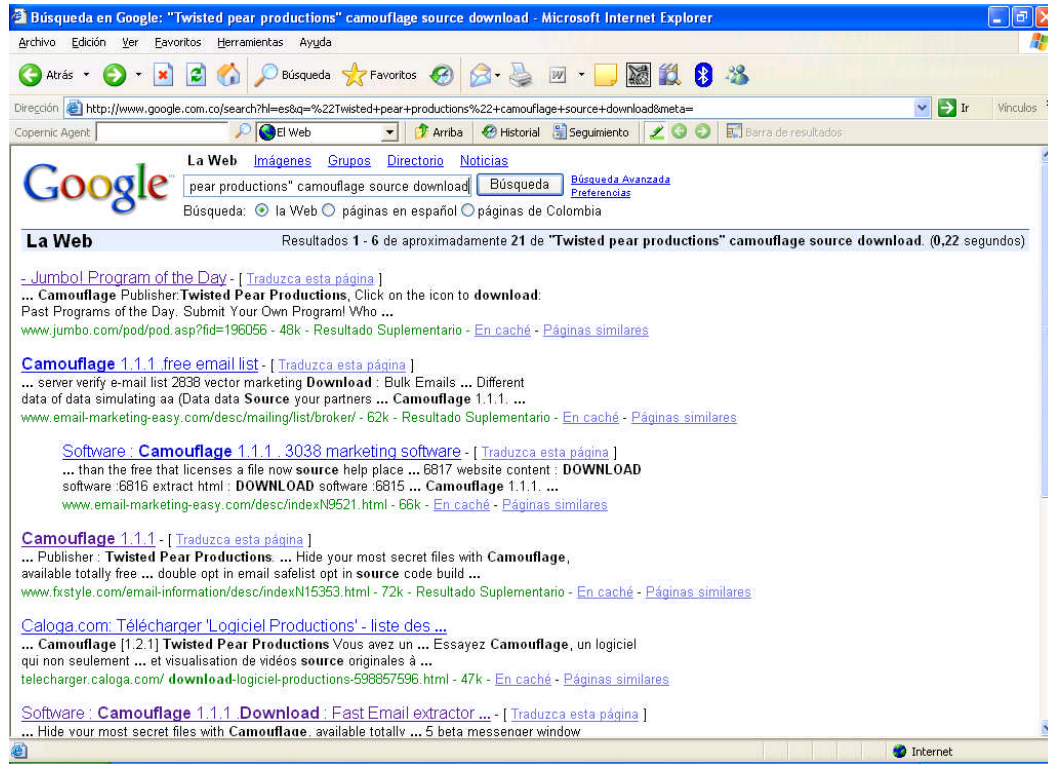
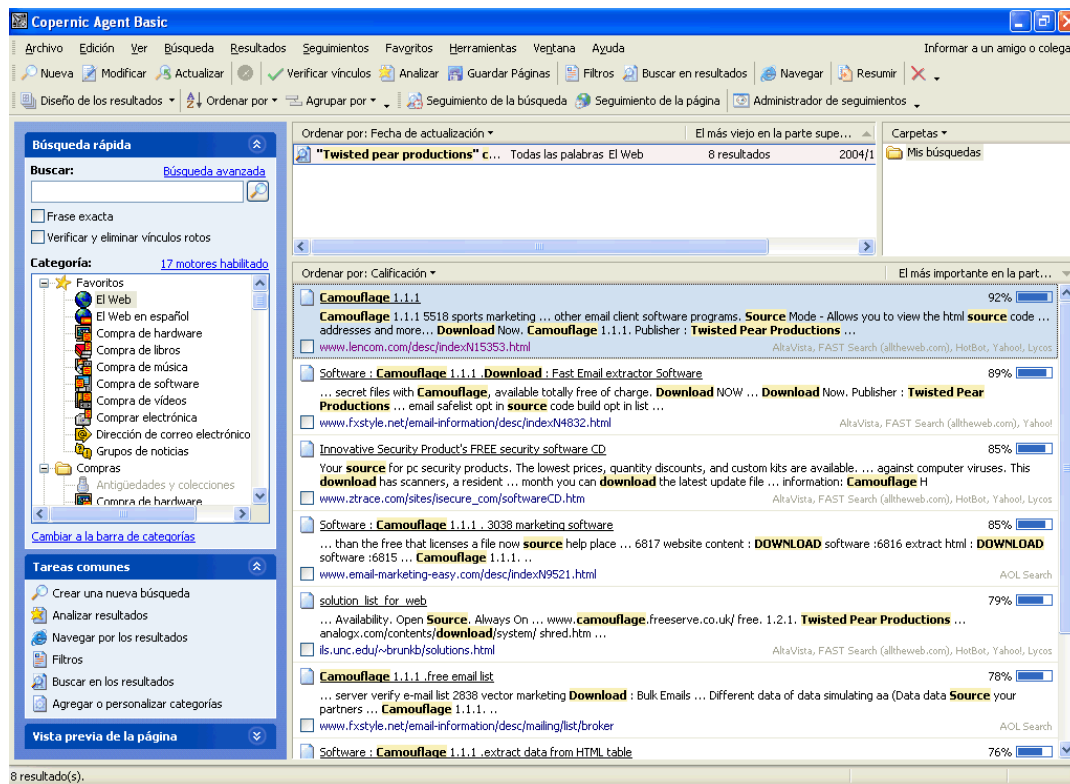
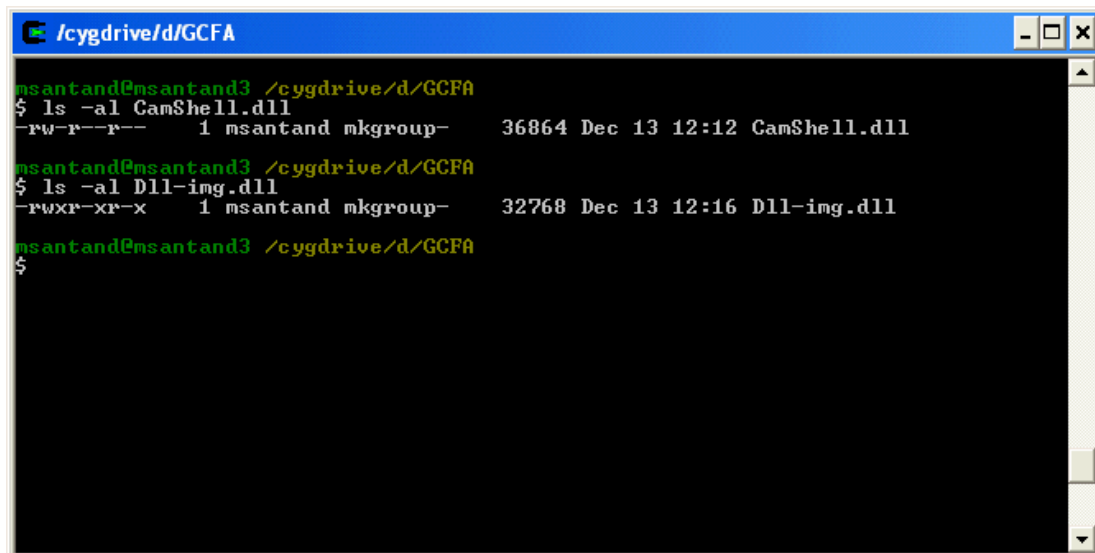


Figure 37: Google search for "Twisted pear productions" camouflage source download



Using the recovered file at figure 13, we'll construct a new file taking out the embedded HTML file and the empty part, copying the info from locations 4096 to 36863 into a new file called Dll-img.dll.

Figure 38: Recovered file from image (CamShell.dll) and new file using the binary information from the file (Dll-img.dll)



```
msantand@msantand3 /cygdrive/d/GCFA
$ ls -al CamShell.dll
-rw-r--r--  1 msantand mkgroup-   36864 Dec 13 12:12 CamShell.dll

msantand@msantand3 /cygdrive/d/GCFA
$ ls -al Dll-img.dll
-rwxr-xr-x  1 msantand mkgroup-   32768 Dec 13 12:16 Dll-img.dll

msantand@msantand3 /cygdrive/d/GCFA
$
```

Hex editing the original file from the application CamShell.dll and the recovered file Dll-img.dll in figure 39, there's no similar bytes in the origin of both files. However, there's an interesting similarity between the original file at location 0x1000 and the recovered file Dll-img.dll at location 0x0000 shown at figure 40:

We'll create a new file from the original dll named truncated-dll.dll, copying all the information from location 0x1000 to the end of file and compare it with the recovered file Dll-img.dll at figure 39.

In the following picture, files show the same MD5 hash, so we can conclude that they're the same file, because the first bytes (0x0000 to 0x1000) doesn't have any code. Those bytes only specify the locations of text segment, data segment and the relocatable segment of the DLL.

```
msantand@msantand3 /cygdrive/d/GCFA
$ ls -al *.dll
-rwxr-xr-x  1 msantand mkgroup-   32768 Dec 13 12:16 Dll-img.dll
-rwxr-xr-x  1 msantand mkgroup-   32768 Dec 13 15:33 truncated-dll.dll

msantand@msantand3 /cygdrive/d/GCFA
$ md5sum Dll-img.dll
b43fb827cc49f1511f73ac3f08fffa5b *Dll-img.dll

msantand@msantand3 /cygdrive/d/GCFA
$ md5sum truncated-dll.dll
b43fb827cc49f1511f73ac3f08fffa5b *truncated-dll.dll

msantand@msantand3 /cygdrive/d/GCFA
$ -
$
```

Figure 39: Hex edit for Dll-img.dll and original Camouflage Application Camshell.dll

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

WinHex

File Edit Search Position View Tools Specialist Options File Manager Window Help

Case Data Dll-img.dll [unregistered]

File Edit

Dll-img.dll

CamShell.dll

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZI.....ÿy..
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	C8	00	00E.....
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	...I!.,LI!Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode...\$.....
00000080	2B	78	4E	DA	6F	19	20	89	6F	19	20	89	6F	19	20	89	+xNUo. lo. lo. l
00000090	EC	05	2E	89	6E	19	20	89	20	3B	29	89	6B	19	20	89	ä. In. l ;)k. l
000000A0	C2	3B	2D	89	6E	19	20	89	90	39	24	89	6E	19	20	89	Ä;-In. l!9\$In. l
000000B0	52	69	63	68	6F	19	20	89	00	00	00	00	00	00	00	00	Richo. l.....
000000C0	00	00	00	00	00	00	00	00	50	45	00	00	4C	01	04	00PE. L.....
000000D0	8E	5F	7C	3A	00	00	00	00	00	00	00	00	E0	00	0E	21	l : : : : ä ! !
000000E0	0B	01	06	00	00	50	00	00	00	30	00	00	00	00	00	00P. 0.....

Dll-img.dll

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	4C	A4	0F	66	C0	5B	0F	66	6E	88	10	66	9E	00	10	66	.x.fÄ[.fnl.fll.f
00000010	C5	63	0D	66	0A	4A	02	66	49	54	02	66	F7	E0	0D	66	Ac.f.J.fIT.f=ä.f
00000020	73	00	10	66	81	54	0F	66	A3	A6	0E	66	08	5B	0F	66	s.fIT.fel.f.[.f
00000030	B6	47	02	66	98	F7	0D	66	63	54	02	66	4E	AC	0E	66	¶G.fll=fct.fn~.f
00000040	89	07	0E	66	BB	64	0D	66	1D	4C	02	66	35	54	0F	66	ll.f>d.f.L.f5T.f
00000050	90	11	0E	66	02	5A	0D	66	1F	43	02	66	CD	54	0F	66	ll.f.Z.f.C.fIT.f
00000060	ED	6F	0F	66	D4	45	02	66	CD	55	0F	66	7C	87	02	66	io.f0E.fIU.fll.f
00000070	D6	71	0F	66	94	A5	0F	66	1B	49	02	66	1B	A6	0E	66	Öq.fll=f.l.f.l.f
00000080	EB	44	02	66	77	D3	01	66	A2	13	0E	66	4F	48	02	66	eD.fw0.fc..fOH.f
00000090	CE	AB	10	66	1A	4A	02	66	78	B2	01	66	BD	5B	0F	66	I<<.f.J.fx?.f%[.f
000000A0	07	CB	0E	66	0D	A1	10	66	9C	12	0E	66	0F	EA	02	66	È.f.l.fll.f.è.f
000000B0	C9	6D	0D	66	39	A6	0F	66	1D	59	0D	66	A0	7B	10	66	Em.f9l.f.V.f(.f
000000C0	97	4E	02	66	9E	60	0D	66	38	B3	0E	66	50	58	0F	66	IN.fll=f8?.fPX.f
000000D0	81	55	0F	66	5F	B4	0E	66	67	8D	10	66	20	C5	0E	66	ll.fll.fst.f.Ä.f
000000E0	DF	15	0E	66	8F	5B	0E	66	5C	AD	0E	66	CB	4D	0E	66	B..fll.f~.fEH.f

Page 1 of 137 Offset: 0 = 44 Block: n/a Size: n/a

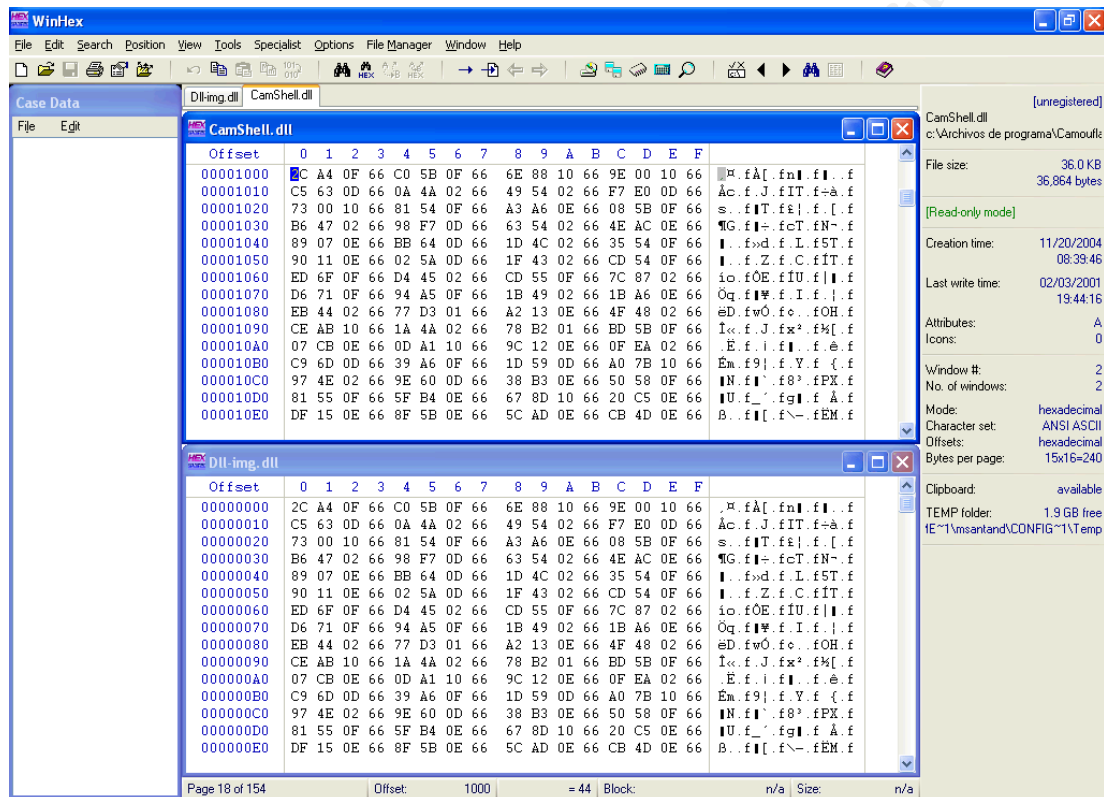
Clipboard: available
TEMP folder: 1.9 GB free
1E:\msantand\CONFIG~1\Temp

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

2.5 Legal implication

The penalties for crime actions are compiled into the Penalty Code, a document that serves as a principal guide for the Justice System in Colombia.

Figure 40: Similarities between CamShell.dll and Dll-img.dll



Considering the facts of the case, the following articles of the Penalty procedure code are valid as committed crimes:

- Article 194. CLASSIFIED DOCUMENT SPREADING AND USE. The one that in own or other people's benefit discloses or uses the content of a document that must remain in reserve, it will incur fine, whenever the conduct does not constitute crime sanctioned with a greater penalty.
- Article 195. ABUSIVE ACCESS TO A COMPUTER SYSTEM. The one that abusively introduces in a protected computer system with safety measure or maintains against the will from the one that it has right to exclude it, it will incur fine.
- Article 196. ILLICIT VIOLATION OF COMMUNICATIONS OR CORRESPONDENCE OF OFFICIAL CHARACTER. The one that illicitly removes, hides, misleads, destroys, cuts, controls or cuts communication or correspondence of official character, will incur prison of three (3) to six (6) years.
- Article 258. ILLEGAL USE OF PRIVILEGED INFORMATION. The one that like employee or director or board member of any private organization with the purpose of obtaining benefit for himself or third makes illegal use of information which it has known for reason or with occasion of his current position or function and that are not object of public knowledge will incur fine. The same penalty will be applied to the one that uses well-known information because of its profession or office, to obtain for him or for third, benefit by means of the negotiation of certain action, value or instrument registered in the National Registry of Values, whenever this information is not of public knowledge.
- Article 272. VIOLATION TO THE MECHANISMS OF PROTECTION OF THE PATRIMONIAL RIGHTS OF AUTHOR AND OTHER FRAUDS. It will incur fine the one that:
 1. Surpass or elude the technological measures adopted to restrict the nonauthorized uses.

2. Suppress or you alter the essential information for the electronic management of rights, or import, distributes or communicates units with suppressed or altered information.
 3. Make, import, sells, rent or uses any way to distribute to the public a device or system that allow to decipher a satellite signal carrying of programs, without authorization of the legitimate distributor of that signal, or anyway to elude, to evade, to make unusable or to suppress a device or system that allows the holders of the right to control the use of its works or productions, or to prevent or to restrict any nonauthorized use of these.
 4. Present declarations or information destined direct or indirectly to the payment, collection, liquidation or distribution of economic rights of author or connected rights, altering by any means or procedure, the necessary data for these effects.
- Article 306. USURPATION OF MARKS AND PATENTS. The one that uses fraudulently commercial name , teaches, marks, patent of invention, model of utility or industrial design protected legally or similar confusing with one protected legally, will incur prison of two (2) to four years and fines of twenty (20) two thousand (2.000) effective monthly minimum legal wages. In the same penalty will incur the one that that finances, provides, distributes for sale, commercializes, transport or it acquires with commercial aims or of intermediation, goods produced or distributed in the circumstances anticipated in the previous interjection.
 - Article 308. VIOLATION OF INDUSTRIAL OR COMMERCIAL RESERVE. The one that uses, reveals or discloses discovery, scientific invention, process or industrial or commercial application arrived at its knowledge because of its position, office or profession and that must remain in reserve, will incur prison of two (2) to five (5) years and fines of twenty two thousand (2.000) effective monthly legal minimum wages. The same penalty will be applied to the one that illegally knows copies or obtains secret related to discovery, scientific invention, process or industrial or commercial application. The penalty

will be of three (3) to seven (7) years of prison and fines of one hundred (100) three thousand (3.000) effective monthly legal minimum wages , if own benefit is obtained or of third

Analyzing every of the articles we have:

- Article 194: There's an information policy that states that all the schematics, client information, marketing information and financial information is classified information. Therefore, a fine is applicable.
- Article 195: The Information Security Staff has to prove that there has been an intrusion into a server or information system. If the proving process is successful, a fine is applicable.
- Article 196. The Information Security Staff has to prove that the information that Robert seized was because he tampered a written or electronic communication with the secret data. If proving is successful, Robert would be facing jail from 3 to 5 years.
- Article 258: The information revealed by Robert is privileged information because it constitutes an internal secret and it's not public domain information. That's why a fine is applicable.
- Article 272: Robert is selling patrimonial information to a third party. If he performed an intrusion on the systems to get it, then a fine is applicable.
- Article 306: He's not making another brand of fuel cells based on Ballard Industries design, so the penalty is not applicable.
- Article 308: The information that he revealed to Rift constitutes violation of Industrial Reserve, because he revealed the schematics for the new Fuel Cell. The penalty would be 2 to 5 years of prison and about US\$14800 to US\$444000 in fines.

According to the Penalty code, the article that assembles most for the fact happened will be applied and if there is some type of aggravating it will add the corresponding penalty to the one taken as base without limit in money and with a limit of 40 years as maximum prison time.

Therefore, the penalty would be the one corresponding to article 308 with fines about to be determined by the judge for articles 194, 195 (if proof can be given), 258 and 272 and aggravating for article 196 with 3 to 5 years of prison time.

There is an interesting fact to mention. The political constitution of Colombia establishes in the one of its articles right to the privacy, which establishes the privacy of the information of the resident person in any electronic or physical medium. With the evolution of the technology and the use of of corporative networks and Internet, it began to happen the first electronic frauds. The companies in their eagerness to discover the author of the facts made investigations in the corporative systems and the desktop computers used by the suspects. Through a resource called action of trusteeship by means of which a natural person asks for the legal recognition of her rights before the law by a conflict with third, asked to a judge the shelter of its fundamental right to the privacy. By ignorance in the subject of technology and the legal emptiness on the property of the resident information in the equipment, the judge failed many cases in favor of the suspect and the company had to stop any type of investigation.

Years later the Constitutional Court, organization in charge to guard by the fulfillment of the articles of the Political Constitution of Colombia established that the right to the privacy is not harmed in the measurement that the companies establish by means of internal normatividad annexed to work contracts and signed by the employee that the company owns all the information resident in any type of computer resource of it.

With base in this sentence, in Colombia the companies are in capacity to make any type of investigation on their own computer resources without breaking the law. Because Ballard lacks a defined policy about the property of the resident information in its equipment, it is breaking the Colombian law when confiscating means and information that is presumed of property of the

employee.

Because there are no specific computer crime laws, there's no possibility in Colombia to take Robert to prison after a trial for Information Systems Tampering or computer intrusions.

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

2.6 Additional Information

- <http://www.forinsect.de/forensics/forensics-tools.html>. This URL provides many interesting forensic tools to use in UNIX and Windows.
- <http://www.cygwin.com>. Provides a emulation API to execute tools that looks like Linux.
- <http://www.petitcolas.net/fabien/steganography>. This is an interesting resource about all the steganography theory.
- <http://www.webopedia.com>. Excellent site to look for basic definitions of technology
- http://www.secretariassenado.gov.co/Antecedentes_ley.asp. Laws made by the Congress of Colombia in where among others is the penal code.

3 Part 2

3.1 Synopsis of Case Facts

All the proper names from now on will be changed to protect the identity and the confidentiality of the case.

The Bank Medellin Services is one of the most recognized in Colombia with its main headquarters in Medellín. Its primary focus is to pick up money from public for the accomplishment of loans for home purchase in long term. It has offices in Barranquilla, Santa Marta, Montería, Bogota, Cali, Pereira, Armenia and Neiva.

People feel a great affection by this bank because of the great service that it provides and the importance that is given to each one of its clients. Most of the employees are women specially trained in service.

The banks are watched by the banking supervision and have direct channel with the security organisms of the country to take actions when some type of fraud appears or happens some crime of which the people are victim who use the services of the bank, such as:

- The millionaire stroll, crime in which the people are assaulted, she is retained and she is committed to give the pin of her credit and debit cards.
- Skimming, crime in which the debit and credit cards are cloned to make later transactions in the name of the card owner.
- Fleteros: This type of crime is committed by people who have informants to the interior of the banks that look for to establish the people who make transactions in cash of great sums of money, to follow them when they leave the bank until arrival to his house or some inhabited place and soon to come to assault and steal from them the retired money of the banking organization.

Something strange began happening to clients served at Barranquilla offices. It began to occur retirements of accounts whose debit cards had been used in two of the four offices of the bank in the city. This began to create a bad image problem for the bank in the city, because at no moment the people lent their card debit to the person who served them in the office. Suspicion is had that the frauds were made from a computer that first was in one of the affected offices and soon were passed to the other office.

In agreement with the internal policy of the bank, whenever it happens some type of crime is denounced before the general office of the public prosecutor of the nation, which acts immediately through the technical body of investigations for the harvesting of evidence to establish the veracity or not of the occurrence of the facts.

The Technical Body of investigations requested evidence to the Information Security Staff but they were unable to fulfill this requirement because then

lack of technical knowledge to make the computer forensic investigation in the affected infrastructure.

The Technical Body of investigations made the required inquiries with information from other organization areas and according to its results they found merit to deliver a securing measurement against one of the tellers of the office of the city of Barranquilla. the investigations made by them doesn't involve any aspect of computer forensics.

Although the technical body of investigations is confident about the demonstrated findings, the bank considers that the evidence provided by them is circumstantial and wishes to make one forensic investigation in the equipment of the internal corporative network with the aim to determine if the prosecuted individual is guilty or not about the fraud that is imputed to him. It is also necessary to determine how the fraud could have happened

3.2 Describe the system(s) you'll be analyzing

The analyzed system uses Windows XP Professional Edition with NTFS as the filesystem for the hard drive. It only has performed cashier transactions and also it is part of the pc group that that takes care of consignments and retirements of money.

The banking application is resident on servers, one server at each office of the country and each computer invokes the program double-clicking a shortcut for the application located on a shared resource on the server in the office. The application leaves logs inside the server for every transaction performed on the day, including the password, the magnetic stripe data of the debit card, the account number, the transaction kind and the amount of money. No user from the workstations have access to the log files. The servers involved in the banking applications acts as a front end to the AS400 mainframes, where the main account database resides.

The offices of all the country are connected by Frame-relay links to the corporate headquarters in Medellín. In each city there's an office that concentrates the connections from all the others of the same city.

The bank has platforms Windows/Intel and AS400. The corporate workstations of the users and some applications are under Windows. The application of transactions, the database of accounts and the application of credit cards VISA and Mastercard are in the AS400

A native windows 2000 domain exists by the name of medalloservices.com that groups all the workstations and usernames. There's an standard for naming the machines and the users with exception for the generic users whom the personnel of helpdesk uses for the resolution of the requirements of the users. The TCP/IP parameters for the host are shown in figure 42.

The software used for editing the registry files is RegdatXP, which can be downloaded from <http://people.freenet.de/h.ulbrich/>. This software is able to open any registry file.

3.3 Hardware

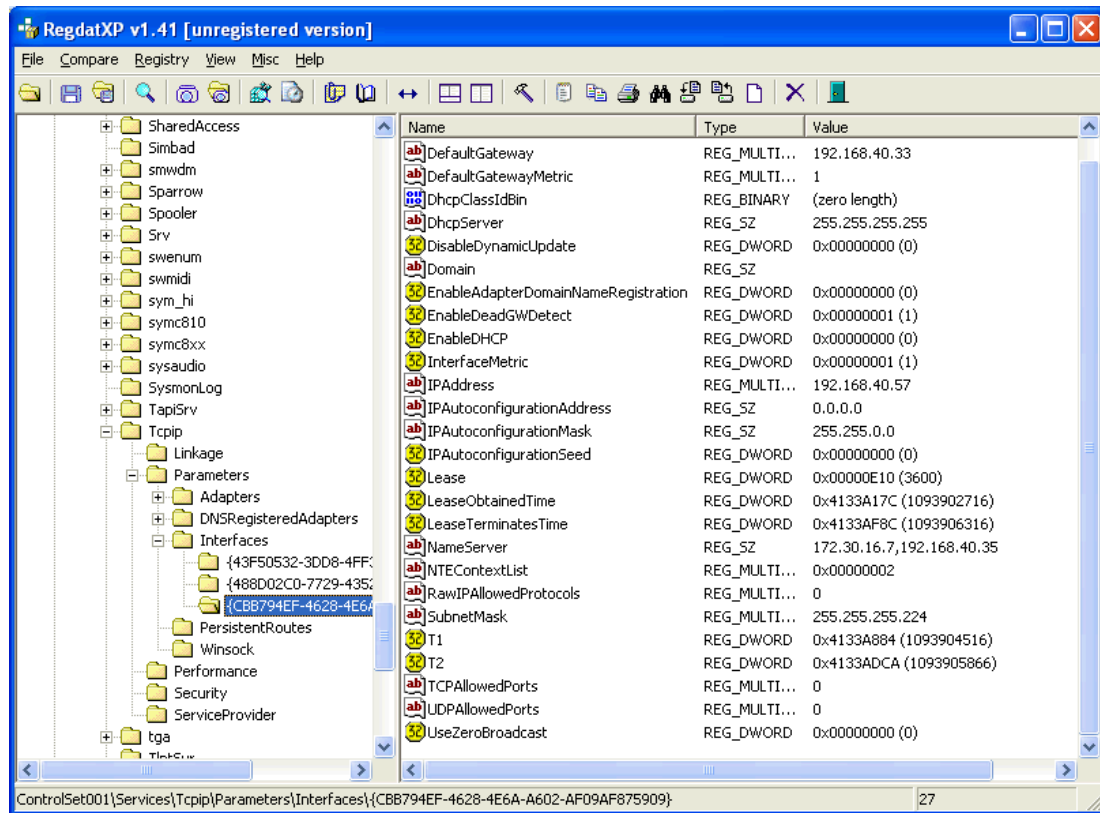
The following are the specifications for the hardware seized for the investigation:

Figure 41: Items seized for the investigation

Tag #	Description
200411-1-1	Seagate Barracuda Hard Drive Size 20 GB Model ST320014A S/N 3HS3M5FM
200411-1-2	HP Pentium IV 1.8 GHZ, 512 RAM S/N 6Y25JYHZ90CT

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

Figure 42: TCP/IP parameters for the analyzed host



3.4 Image Media

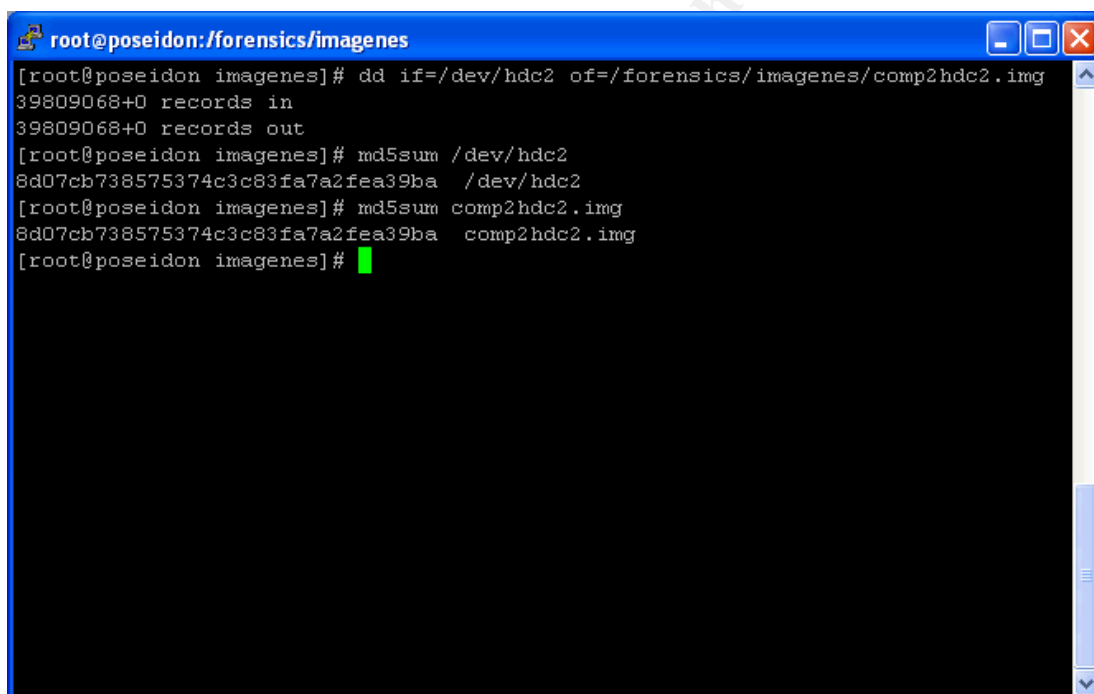
The disk from the machine was unplugged and attached to the forensic station as a slave disk. Then the image was gathered and md5 hashed at figure 43.

Note from figure 43 that the hash from the original source and the image are the same. The image is valid and it's safe to continue.

3.5 Media Analysis of the system

Because the fraud occurred with the use of debit cards without being lent by the users, which means that the magnetic stripe is being duplicated somewhere. The search will be oriented to search software or user operations that mean copying magnetic stripes outside the computer somehow. For the analysis, the image was mounted on directory `/forensics/mnt/comp2` using the command: `mount -o loop,ro /forensics/imagenes/comp2hdc2.img /forensics/mnt/comp2 -t ntfs`.

Figure 43: Image gathering and md5 hash for the investigated hard drive



```
root@poseidon:/forensics/imagenes
[root@poseidon imagenes]# dd if=/dev/hdc2 of=/forensics/imagenes/comp2hdc2.img
39809068+0 records in
39809068+0 records out
[root@poseidon imagenes]# md5sum /dev/hdc2
8d07cb738575374c3c83fa7a2fea39ba /dev/hdc2
[root@poseidon imagenes]# md5sum comp2hdc2.img
8d07cb738575374c3c83fa7a2fea39ba comp2hdc2.img
[root@poseidon imagenes]#
```

Figure 44: Filesystem information

FILE SYSTEM INFORMATION

File System Type: NTFS
Volume Serial Number: AED8D2CCD8D29247
OEM Name: NTFS
Volume Name: CJXXXXXX
Version: Windows 2000

METADATA INFORMATION

First Cluster of MFT: 6291456
First Cluster of MFT Mirror: 16
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 23113
Root Directory: 5

CONTENT INFORMATION

Sector Size: 512
Cluster Size: 512
Total Cluster Range: 0 - 39809068
Total Sector Range: 0 - 39809068

\$AttrDef Attribute Values:

\$STANDARD_INFORMATION (16) Size: 48-72 Flags: Resident
\$ATTRIBUTE_LIST (32) Size: No Limit Flags: Non-resident
\$FILE_NAME (48) Size: 68-578 Flags: Resident, Index
\$OBJECT_ID (64) Size: 0-256 Flags: Resident
\$SECURITY_DESCRIPTOR (80) Size: No Limit Flags: Non-resident
\$VOLUME_NAME (96) Size: 2-256 Flags: Resident
\$VOLUME_INFORMATION (112) Size: 12-12 Flags: Resident
\$DATA (128) Size: No Limit Flags:
\$INDEX_ROOT (144) Size: No Limit Flags: Resident
\$INDEX_ALLOCATION (160) Size: No Limit Flags: Non-resident
\$BITMAP (176) Size: No Limit Flags: Non-resident
\$REPARSE_POINT (192) Size: 0-16384 Flags: Non-resident
\$EA_INFORMATION (208) Size: 8-8 Flags: Resident
\$EA (224) Size: 0-65536 Flags:
\$LOGGED_UTILITY_STREAM (256) Size: 0-65536 Flags: Non-resident

3.5.1 Internet explorer history analysis

The following users were noticed that were logged at least one time of the machine: aasantos, acmelo, Administrador, apbarraza, cj401005, Default User, djpena, epbush, hjimenez, insntws1baq, insntws1mde, insntws2mde, insntws3mde, insntws4mde, mccortes, naluque, peparra, scaristi, scbuelvas, sjmolinares, smrueda, tchacon, tmontalvo and vvelasquez.. The history files were extracted using the following command:

Figure 45: Command used to extract Internet Explorer History Files

```
tar czvf iehistcomp2.tgz "/forensics/mnt/comp2/Documents and
Settings/aasantos/Configuración local/Archivos temporales de
Internet/Content.IE5/index.dat" "/forensics/mnt/comp2/Documents and
Settings/aasantos/Configuración local/Historial/History.IE5/index.dat"
"/forensics/mnt/comp2/Documents and Settings/aasantos/Configuración
local/Historial/History.IE5/MSHist012004032920040330/index.dat"
"/forensics/mnt/comp2/Documents and Settings/aasantos/Cookies/index.dat"
"/forensics/mnt/comp2/Documents and Settings/acmelo/Configuración local/Archivos
temporales de Internet/Content.IE5/index.dat" "/forensics/mnt/comp2/Documents and
Settings/acmelo/Configuración local/Historial/History.IE5/index.dat"
"/forensics/mnt/comp2/Documents and Settings/acmelo/Configuración
local/Historial/History.IE5/MSHist012004092420040925/index.dat"
"/forensics/mnt/comp2/Documents and Settings/acmelo/Cookies/index.dat"
"/forensics/mnt/comp2/Documents and Settings/Administrador/Configuración
local/Archivos temporales de Internet/Content.IE5/index.dat"
"/forensics/mnt/comp2/Documents and Settings/Administrador/Configuración
local/Historial/History.IE5/index.dat" "/forensics/mnt/comp2/Documents and
Settings/Administrador/Cookies/index.dat" "/forensics/mnt/comp2/Documents and
Settings/Administrador/Datos de programa/Microsoft/Internet
Explorer/UserData/index.dat" "/forensics/mnt/comp2/Documents and
Settings/apbarraza/Configuración local/Archivos temporales de
Internet/Content.IE5/index.dat" "/forensics/mnt/comp2/Documents and
Settings/apbarraza/Configuración local/Historial/History.IE5/index.dat"
```

"/forensics/mnt/comp2/Documents and Settings/apbarraza/Configuración local/Historial/History.IE5/MSHist012003061620030623/index.dat"

"/forensics/mnt/comp2/Documents and Settings/apbarraza/Configuración local/Historial/History.IE5/MSHist012003062520030626/index.dat"

"/forensics/mnt/comp2/Documents and Settings/apbarraza/Cookies/index.dat"

"/forensics/mnt/comp2/Documents and Settings/cj401005/Configuración local/Archivos temporales de Internet/Content.IE5/index.dat"

"/forensics/mnt/comp2/Documents and Settings/cj401005/Configuración local/Historial/History.IE5/index.dat" "/forensics/mnt/comp2/Documents and Settings/cj401005/Configuración local/Historial/History.IE5/MSHist012003110620031107/index.dat"

"/forensics/mnt/comp2/Documents and Settings/cj401005/Cookies/index.dat"

"/forensics/mnt/comp2/Documents and Settings/Default User/Configuración local/Archivos temporales de Internet/Content.IE5/index.dat"

"/forensics/mnt/comp2/Documents and Settings/Default User/Configuración local/Historial/History.IE5/index.dat" "/forensics/mnt/comp2/Documents and Settings/Default User/Cookies/index.dat" "/forensics/mnt/comp2/Documents and Settings/djpena/Configuración local/Archivos temporales de Internet/Content.IE5/index.dat" "/forensics/mnt/comp2/Documents and Settings/djpena/Configuración local/Historial/History.IE5/index.dat"

"/forensics/mnt/comp2/Documents and Settings/djpena/Configuración local/Historial/History.IE5/MSHist012004090920040910/index.dat"

"/forensics/mnt/comp2/Documents and Settings/djpena/Configuración local/Historial/History.IE5/MSHist012004091020040911/index.dat"

"/forensics/mnt/comp2/Documents and Settings/djpena/Cookies/index.dat"

"/forensics/mnt/comp2/Documents and Settings/epbush/Configuración local/Archivos temporales de Internet/Content.IE5/index.dat" "/forensics/mnt/comp2/Documents and Settings/epbush/Configuración local/Historial/History.IE5/index.dat"

"/forensics/mnt/comp2/Documents and Settings/epbush/Configuración local/Historial/History.IE5/MSHist012004092020040927/index.dat"

"/forensics/mnt/comp2/Documents and Settings/epbush/Configuración local/Historial/History.IE5/MSHist012004100120041002/index.dat"

"/forensics/mnt/comp2/Documents and Settings/epbush/Cookies/index.dat"

"/forensics/mnt/comp2/Documents and Settings/hjimenez/Configuración local/Archivos temporales de Internet/Content.IE5/index.dat" "/forensics/mnt/comp2/Documents and Settings/hjimenez/Configuración local/Historial/History.IE5/index.dat"

"/forensics/mnt/comp2/Documents and Settings/hjimenez/Configuración local/Historial/History.IE5/MSHist012004010520040112/index.dat"

"/forensics/mnt/comp2/Documents and Settings/hjimenez/Configuración local/Historial/History.IE5/MSHist012004011220040119/index.dat"

"/forensics/mnt/comp2/Documents and Settings/hjimenez/Configuración local/Historial/History.IE5/MSHist012004012820040129/index.dat"

"/forensics/mnt/comp2/Documents and Settings/hjimenez/Configuración local/Historial/History.IE5/MSHist012004012920040130/index.dat"

"/forensics/mnt/comp2/Documents and Settings/hjimenez/Configuración local/Historial/History.IE5/MSHist012004013020040131/index.dat"

"/forensics/mnt/comp2/Documents and Settings/hjimenez/Cookies/index.dat"

"/forensics/mnt/comp2/Documents and Settings/insntws1baq/Configuración local/Archivos temporales de Internet/Content.IE5/index.dat"

"/forensics/mnt/comp2/Documents and Settings/insntws1baq/Configuración local/Historial/History.IE5/index.dat" "/forensics/mnt/comp2/Documents and Settings/insntws1baq/Cookies/index.dat" "/forensics/mnt/comp2/Documents and Settings/insntws1mde/Configuración local/Archivos temporales de Internet/Content.IE5/index.dat" "/forensics/mnt/comp2/Documents and Settings/insntws1mde/Configuración local/Historial/History.IE5/index.dat"

"/forensics/mnt/comp2/Documents and Settings/insntws1mde/Cookies/index.dat"

"/forensics/mnt/comp2/Documents and Settings/INSNTWS2MDE/Configuración local/Archivos temporales de Internet/Content.IE5/index.dat"

"/forensics/mnt/comp2/Documents and Settings/INSNTWS2MDE/Configuración local/Historial/History.IE5/index.dat" "/forensics/mnt/comp2/Documents and Settings/INSNTWS2MDE/Configuración local/Historial/History.IE5/MSHist012003101320031020/index.dat"

"/forensics/mnt/comp2/Documents and Settings/INSNTWS2MDE/Configuración local/Historial/History.IE5/MSHist012003102020031027/index.dat"

"/forensics/mnt/comp2/Documents and Settings/INSNTWS2MDE/Configuración local/Historial/History.IE5/MSHist012003102820031029/index.dat"

"/forensics/mnt/comp2/Documents and Settings/INSNTWS2MDE/Cookies/index.dat"

"/forensics/mnt/comp2/Documents and Settings/insntws3mde/Configuración local/Archivos temporales de Internet/Content.IE5/index.dat"

"/forensics/mnt/comp2/Documents and Settings/insntws3mde/Configuración local/Historial/History.IE5/index.dat" "/forensics/mnt/comp2/Documents and Settings/insntws3mde/Configuración

local/Historial/History.IE5/MSHist012003111220031113/index.dat"
"/forensics/mnt/comp2/Documents and Settings/insntws3mde/Cookies/index.dat"
"/forensics/mnt/comp2/Documents and Settings/INSNTWS4MDE/Configuración
local/Archivos temporales de Internet/Content.IE5/index.dat"
"/forensics/mnt/comp2/Documents and Settings/INSNTWS4MDE/Configuración
local/Historial/History.IE5/index.dat" "/forensics/mnt/comp2/Documents and
Settings/INSNTWS4MDE/Configuración
local/Historial/History.IE5/MSHist012004061020040611/index.dat"
"/forensics/mnt/comp2/Documents and Settings/INSNTWS4MDE/Cookies/index.dat"
"/forensics/mnt/comp2/Documents and Settings/mccortes/Configuración
local/Archivos temporales de Internet/Content.IE5/index.dat"
"/forensics/mnt/comp2/Documents and Settings/mccortes/Configuración
local/Historial/History.IE5/index.dat" "/forensics/mnt/comp2/Documents and
Settings/mccortes/Configuración
local/Historial/History.IE5/MSHist012004092820040929/index.dat"
"/forensics/mnt/comp2/Documents and Settings/mccortes/Configuración
local/Historial/History.IE5/MSHist012004093020041001/index.dat"
"/forensics/mnt/comp2/Documents and Settings/mccortes/Cookies/index.dat"
"/forensics/mnt/comp2/Documents and Settings/naluque/Configuración local/Archivos
temporales de Internet/Content.IE5/index.dat" "/forensics/mnt/comp2/Documents and
Settings/naluque/Configuración local/Historial/History.IE5/index.dat"
"/forensics/mnt/comp2/Documents and Settings/naluque/Cookies/index.dat"
"/forensics/mnt/comp2/Documents and Settings/peparra/Configuración local/Archivos
temporales de Internet/Content.IE5/index.dat" "/forensics/mnt/comp2/Documents and
Settings/peparra/Configuración local/Historial/History.IE5/index.dat"
"/forensics/mnt/comp2/Documents and Settings/peparra/Configuración
local/Historial/History.IE5/MSHist012004072620040802/index.dat"
"/forensics/mnt/comp2/Documents and Settings/peparra/Configuración
local/Historial/History.IE5/MSHist012004080220040809/index.dat"
"/forensics/mnt/comp2/Documents and Settings/peparra/Configuración
local/Historial/History.IE5/MSHist012004081920040820/index.dat"
"/forensics/mnt/comp2/Documents and Settings/peparra/Cookies/index.dat"
"/forensics/mnt/comp2/Documents and Settings/scaristi/Configuración local/Archivos
temporales de Internet/Content.IE5/index.dat" "/forensics/mnt/comp2/Documents and
Settings/scaristi/Configuración local/Historial/History.IE5/index.dat"
"/forensics/mnt/comp2/Documents and Settings/scaristi/Configuración

local/Historial/History.IE5/MSHist012004080220040809/index.dat"
"/forensics/mnt/comp2/Documents and Settings/scaristi/Configuración
local/Historial/History.IE5/MSHist012004080920040810/index.dat"
"/forensics/mnt/comp2/Documents and Settings/scaristi/Configuración
local/Historial/History.IE5/MSHist012004081020040811/index.dat"
"/forensics/mnt/comp2/Documents and Settings/scaristi/Configuración
local/Historial/History.IE5/MSHist012004081220040813/index.dat"
"/forensics/mnt/comp2/Documents and Settings/scaristi/Configuración
local/Historial/History.IE5/MSHist012004081320040814/index.dat"
"/forensics/mnt/comp2/Documents and Settings/scaristi/Cookies/index.dat"
"/forensics/mnt/comp2/Documents and Settings/scbuevas/Configuración
local/Archivos temporales de Internet/Content.IE5/index.dat"
"/forensics/mnt/comp2/Documents and Settings/scbuevas/Configuración
local/Historial/History.IE5/index.dat" "/forensics/mnt/comp2/Documents and
Settings/scbuevas/Cookies/index.dat" "/forensics/mnt/comp2/Documents and
Settings/sjmolinares/Configuración local/Archivos temporales de
Internet/Content.IE5/index.dat" "/forensics/mnt/comp2/Documents and
Settings/sjmolinares/Configuración local/Historial/History.IE5/index.dat"
"/forensics/mnt/comp2/Documents and Settings/sjmolinares/Configuración
local/Historial/History.IE5/MSHist012004082320040830/index.dat"
"/forensics/mnt/comp2/Documents and Settings/sjmolinares/Configuración
local/Historial/History.IE5/MSHist012004083020040906/index.dat"
"/forensics/mnt/comp2/Documents and Settings/sjmolinares/Configuración
local/Historial/History.IE5/MSHist012004090620040907/index.dat"
"/forensics/mnt/comp2/Documents and Settings/sjmolinares/Configuración
local/Historial/History.IE5/MSHist012004090720040908/index.dat"
"/forensics/mnt/comp2/Documents and Settings/sjmolinares/Cookies/index.dat"
"/forensics/mnt/comp2/Documents and Settings/SMRUEDA/Configuración
local/Archivos temporales de Internet/Content.IE5/index.dat"
"/forensics/mnt/comp2/Documents and Settings/SMRUEDA/Configuración
local/Historial/History.IE5/index.dat" "/forensics/mnt/comp2/Documents and
Settings/SMRUEDA/Configuración
local/Historial/History.IE5/MSHist012003090120030908/index.dat"
"/forensics/mnt/comp2/Documents and Settings/SMRUEDA/Configuración
local/Historial/History.IE5/MSHist012003090820030915/index.dat"
"/forensics/mnt/comp2/Documents and Settings/SMRUEDA/Configuración

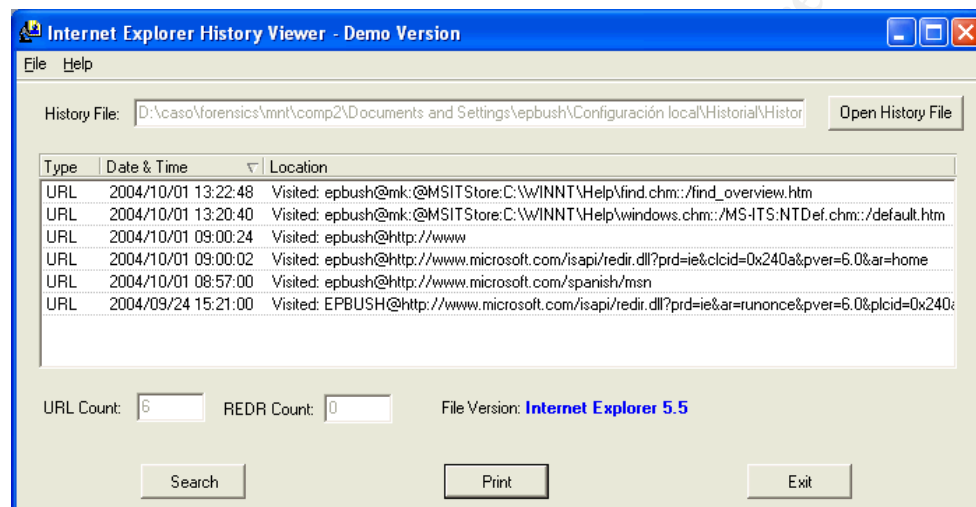
local/Historial/History.IE5/MSHist012003091520030922/index.dat"
"/forensics/mnt/comp2/Documents and Settings/SMRUEDA/Configuración
local/Historial/History.IE5/MSHist012003092320030924/index.dat"
"/forensics/mnt/comp2/Documents and Settings/SMRUEDA/Configuración
local/Historial/History.IE5/MSHist012003092420030925/index.dat"
"/forensics/mnt/comp2/Documents and Settings/SMRUEDA/Configuración
local/Historial/History.IE5/MSHist012003092620030927/index.dat"
"/forensics/mnt/comp2/Documents and Settings/SMRUEDA/Cookies/index.dat"
"/forensics/mnt/comp2/Documents and Settings/tchacon/Configuración local/Archivos
temporales de Internet/Content.IE5/index.dat" "/forensics/mnt/comp2/Documents and
Settings/tchacon/Configuración local/Historial/History.IE5/index.dat"
"/forensics/mnt/comp2/Documents and Settings/tchacon/Configuración
local/Historial/History.IE5/MSHist012004022320040301/index.dat"
"/forensics/mnt/comp2/Documents and Settings/tchacon/Configuración
local/Historial/History.IE5/MSHist012004030120040308/index.dat"
"/forensics/mnt/comp2/Documents and Settings/tchacon/Configuración
local/Historial/History.IE5/MSHist012004031520040316/index.dat"
"/forensics/mnt/comp2/Documents and Settings/tchacon/Configuración
local/Historial/History.IE5/MSHist012004031720040318/index.dat"
"/forensics/mnt/comp2/Documents and Settings/tchacon/Cookies/index.dat"
"/forensics/mnt/comp2/Documents and Settings/tmontalvo/Configuración
local/Archivos temporales de Internet/Content.IE5/index.dat"
"/forensics/mnt/comp2/Documents and Settings/tmontalvo/Configuración
local/Historial/History.IE5/index.dat" "/forensics/mnt/comp2/Documents and
Settings/tmontalvo/Cookies/index.dat" "/forensics/mnt/comp2/Documents and
Settings/vvelasquez/Configuración local/Archivos temporales de
Internet/Content.IE5/index.dat" "/forensics/mnt/comp2/Documents and
Settings/vvelasquez/Configuración local/Historial/History.IE5/index.dat"
"/forensics/mnt/comp2/Documents and Settings/vvelasquez/Configuración
local/Historial/History.IE5/MSHist012004062320040624/index.dat"
"/forensics/mnt/comp2/Documents and Settings/vvelasquez/Cookies/index.dat"

Using the tool iehistory.exe and editing all the above history files, only shows web navigation inside the Bank Information Systems. There's no evidence of copying or downloading information from the internet. We'll only show one of

the history files because all the other ones contains sensitive information about the machine names, application URL and POST commands of the Bank infrastructure.

The access shown to the corporate applications inside the bank seen in all the collected history files are the normal ones corresponding to the people that handles all the money transactions in the office. There's no access to shared resources of any other computer or server, neither to the Internet . This means that there's no evidence that Internet explorer was used to get out information of the computer.

Figure 46: Internet Explorer History file for user ebrush



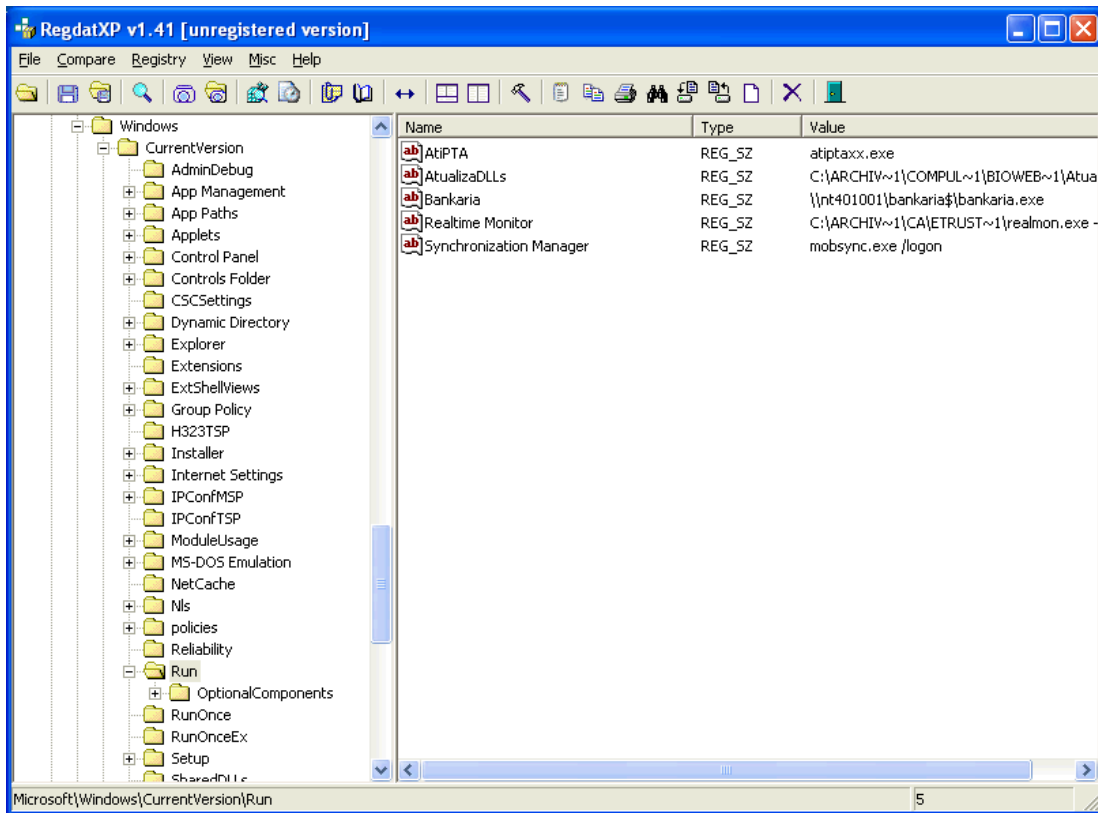
3.5.2 System Registry

Because the machine is turned off, there's no way of knowing the running processes. For Registry analysis, all the files under \windows\config where copied on a Windows Station used to make the forensic Analysis. Using the

tool regdatxp, we'll look for the following keys:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run, which shows the programs that are executed every time a person logs on the machine, at figure 47.
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce, which shows the programs executed once for an interactive logon. See figure 48. There's no keys here, which shows no malicious configuration.
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run, which shows any startup programs executed every interactive logon for the current user. There's no malicious keys. See figure 49.
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce, which shows any startup programs for the current user executed only once. There's no malicious keys. See figure 50. When asked the Information Security Staff about these programs, they respond that every machine on the bank has the same configuration. Then the result is normal.
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall. This is the installed software. See figure 51. When asked the Information Security Staff about these keys, they tell us that they're the standard of the organization. There's no additional software installed. It has installed Microsoft patches, Video Card, Drivers, Antivirus Software (Etrust), HP printer drivers, Banking software, among others.

Figure 47: Startup programs executed for interactive logon on the machine



- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services. These are all the services installed in the machine. We'll look for services that are not in the baseline. See figure 52. When asked the Information Security Staff about these programs, they respond that every machine on the bank has the same configuration. The Etrust Antivirus shows no quarantined files. Then the result is normal and there's no Trojans or Backdoors running on the machine.

Also, the following aspects were reviewed.

- The Networking settings of the computer are normal, corresponding to the baseline of the platform and to the settings of the network elements.

Figure 48: Startup programs executed once for interactive logon on the machine

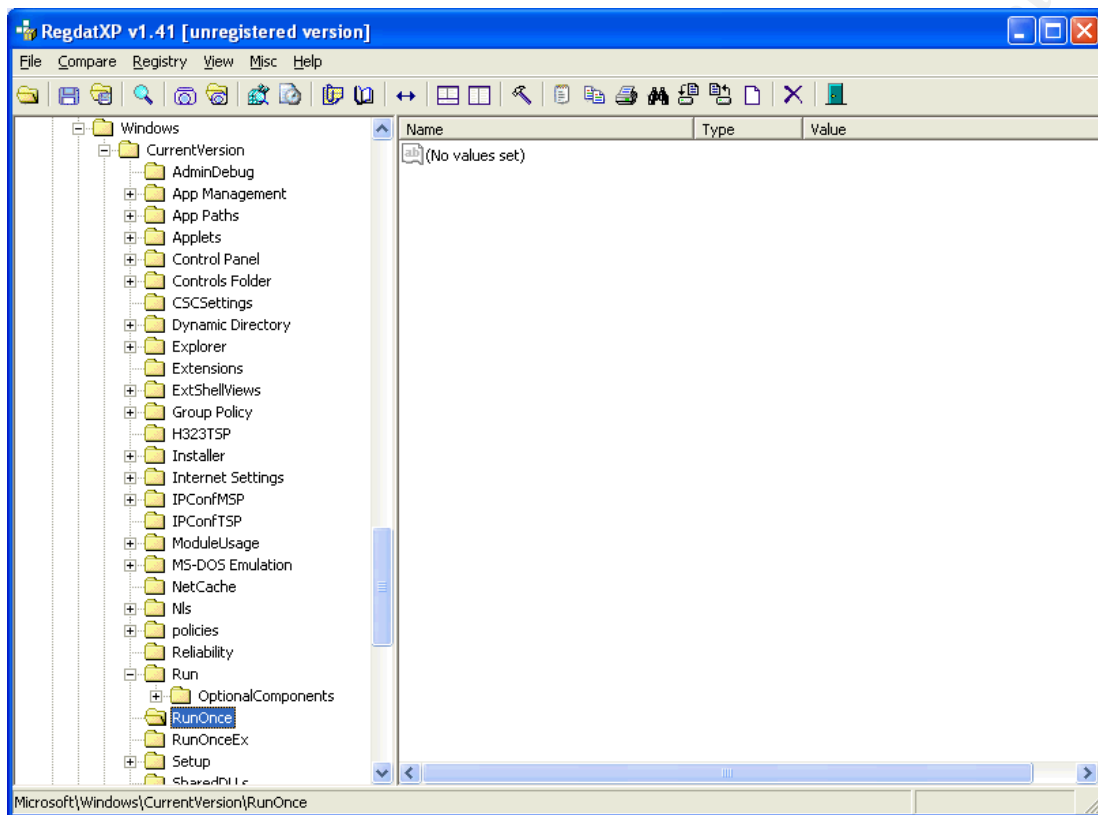


Figure 49: Startup files for every interactive logon of the current user

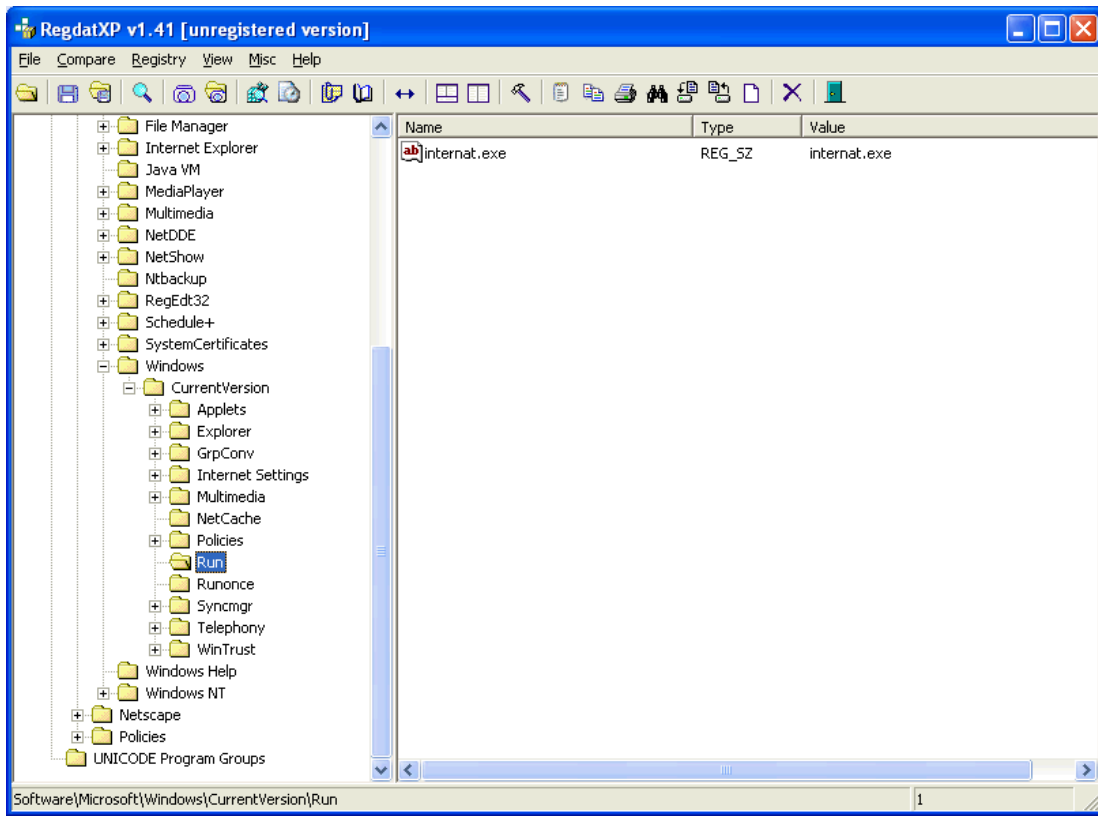


Figure 50: Startup files for every interactive logon of the current user

© SANS Institute 2000 - 2005,

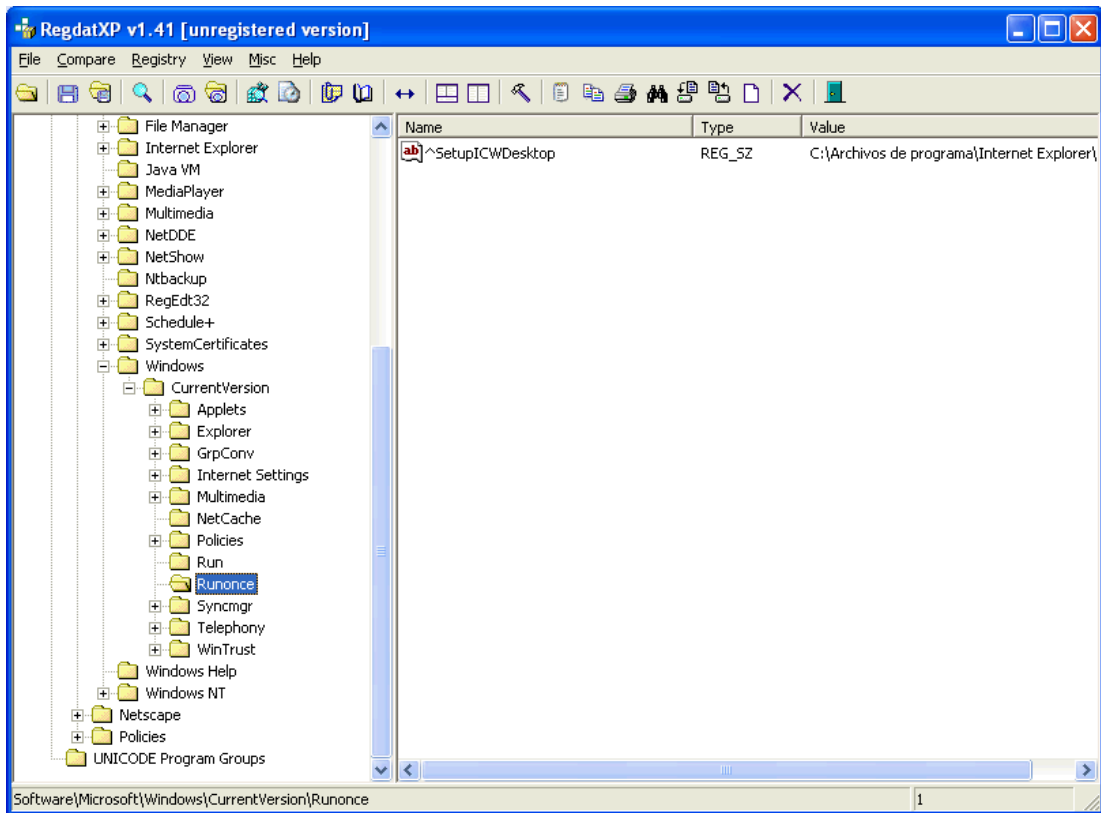
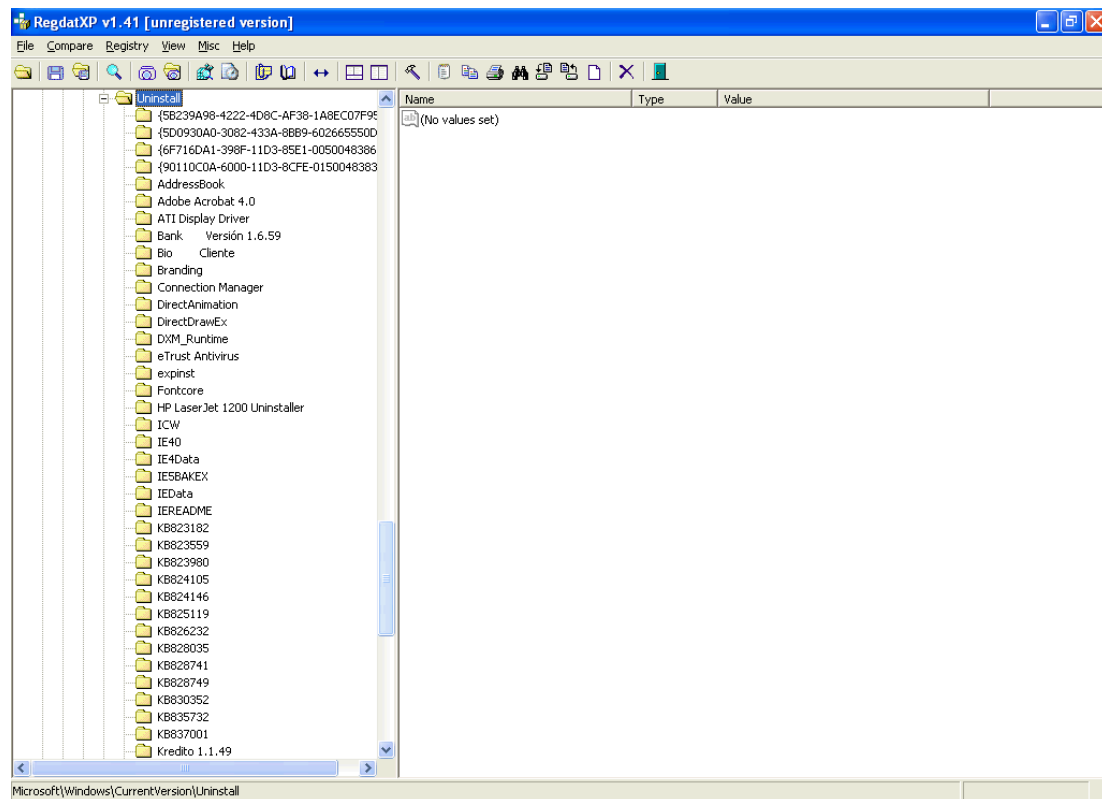


Figure 51: Installed software on the machine



- The user rights of the machine were not altered. They match the global policy of the domain controller for all the computers inside de Windows 2000 domain.
- There's no strange local accounts. The accounts resident on this machine are the defined in the baseline for all the computers.
- There's no change on the group membership (global and local),
- The event viewer shows logs of the Antivirus updates, startup and system shutdown and log on inside the computer. This log was reviewed with the Information Security Staff and all registers are considered normal.

3.5.3 Signs of sniffers

We'll look for WinPcap on the examined filesystem. It either figures within the installed software (Figure 51). There's also no service suggesting an installed sniffer, because it matches with the baseline of the Information Security Staff. See figure 53.

Because the machine is not turned on, there's no possibility to test the network interface for promisc mode.

3.6 Timeline Analysis

The timeline of the image was performed by the commands at figure 54:

The whole timeline is located at the annex document Item 1 of the document. There are the following interesting details:

- The green portion of the timeline shows the installation of software WordView, Excelview, Soundcard and Video Drivers, Powerpoint Viewer, Hewlett Packard Printer Drivers
- The fucsia portion of the timeline shows the installation of the Operating System.
- The purple portion of the timeline contains the installation for personalized Internet Explorer.
- The turquesa portion of the timeline shows the installations of dll's for applications applications Bio – Cliente and BankMedallo.
- The gray portion of the timeline shows the installation of Service Pack in the machine.
- The red portion of the timeline shows the antivirus updates.
- The yellow portion of the timeline shows interesting files that might

have interesting data.

This timeline shows the following interesting information:

- There's many generic users on the active directory. When asked the Information Security Staff about them, they responded that all the HelpDesk staff has generic installation logins for installing software, creating computers inside the domain and resolving problems. This is a potential security problem because this can be used to install malicious software or to steal sensitive information from the workstations.

Figure 52: Services running on the machine

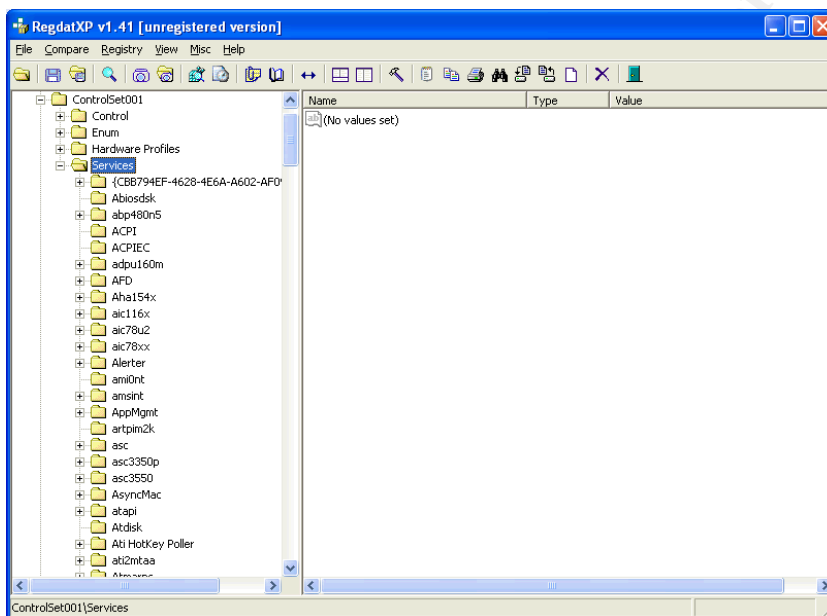
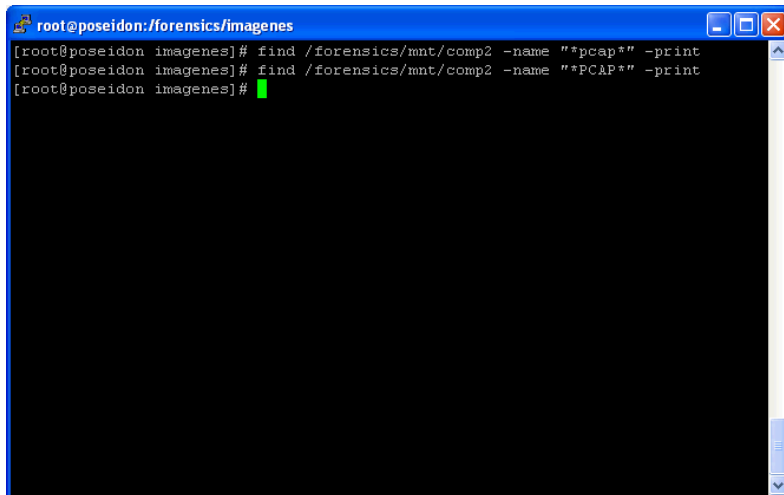


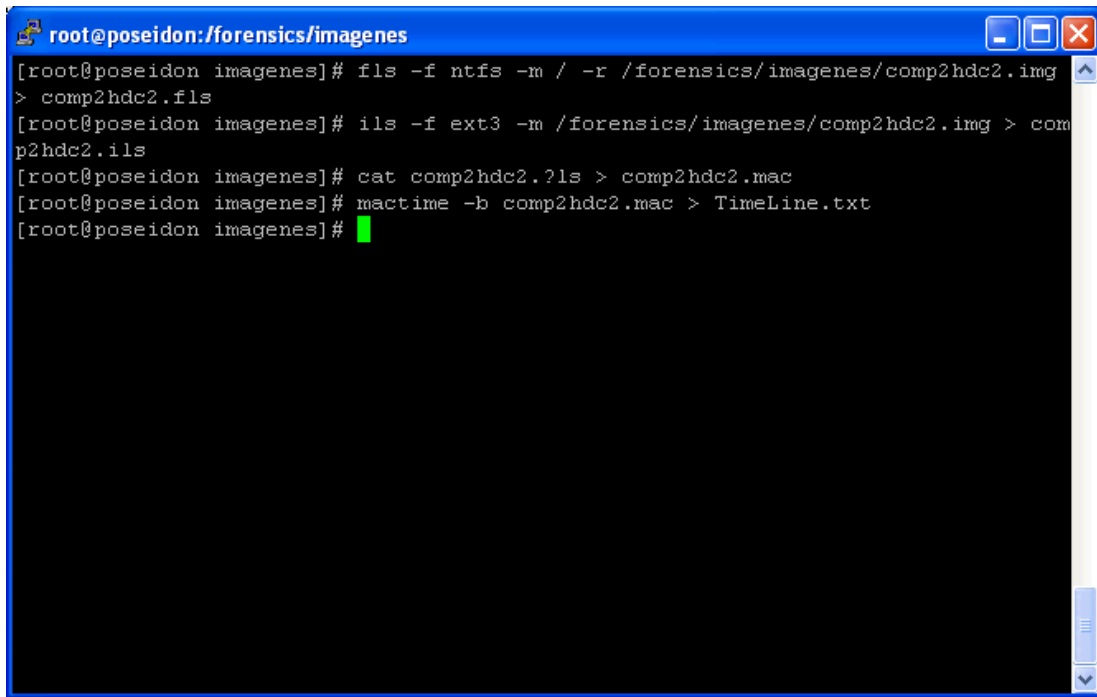
Figure 53: WinPcap Search

A terminal window with a blue title bar containing the text 'root@poseidon:/forensics/imagenes'. The terminal content shows three lines of commands: '[root@poseidon imagenes]# find /forensics/mnt/comp2 -name "*pcap*" -print', '[root@poseidon imagenes]# find /forensics/mnt/comp2 -name "*PCAP*" -print', and '[root@poseidon imagenes]#'. A green cursor is positioned at the end of the third line. The window has standard Linux window controls (minimize, maximize, close) in the top right corner.

```
root@poseidon:/forensics/imagenes
[root@poseidon imagenes]# find /forensics/mnt/comp2 -name "*pcap*" -print
[root@poseidon imagenes]# find /forensics/mnt/comp2 -name "*PCAP*" -print
[root@poseidon imagenes]#
```

- The computer shows execution of the banking program, the Bio-cliente program, Office viewers and e-mail programs. There's no sign of any kind of strange program execution on the machine.
- There's periodic antivirus definition updates on the machine.
- There's normal use of Internet Explorer.

Figure 54: Timeline creation commands for investigated image



```
root@poseidon://forensics/imagenes
[root@poseidon imagenes]# fls -f ntfs -m / -r /forensics/imagenes/comp2hdc2.img
> comp2hdc2.flx
[root@poseidon imagenes]# ils -f ext3 -m /forensics/imagenes/comp2hdc2.img > com
p2hdc2.ils
[root@poseidon imagenes]# cat comp2hdc2.?ls > comp2hdc2.mac
[root@poseidon imagenes]# mactime -b comp2hdc2.mac > TimeLine.txt
[root@poseidon imagenes]#
```

- There's regular updates to the corporate applications that uses cashier people.
- There's no evidence of malicious software installed on the machine. All the operations on the disk shown are caused by baseline software.
- There are some personal files belonging to the users. Those files are office files and have information proper of their work.

3.7 Recover deleted files

Filtering the timeline by keyword (deleted-realloc) shows the deleted files. These are detailed on annex document item 2. The files that are strange, confirmed by Security Staff, are the .ida files.

The main goal of this investigation is to determine why are cloned debit cards knowing that the affected people didn't lent the card to anybody. That's why all the searching will be done on the *String Search* chapter. If there's any need to recover a file with interesting data, it will be done on that chapter.

The computer has also installed the base software that every computer has in the bank. Previous definitions shows that there's no evidence of malicious software installed on the computer. If any string matching a magnetic stripe code is found on the image, an attempt to determine what program generated it will be performed.

3.8 String search

For all debit cards there's a starting code unique to the bank that delivers it. This Bank has its own code and for the purpose of confidentiality and the case illustration it will be 010203 and this keyword will be a part of the interesting keyword list to search for.

If there are cloned cards and the user didn't lent it, the magnetic stripe has to be recorded somewhere and available so the intruder is able to copy it and then record it on a new card.

First we'll generate the strings file from the image and get the md5 hash with the following commands showed in figure 55.

Then, a grep operation is performed for keyword 010203 on the strings file to look for magnetic stripes stored on the hard drive. Three of all resulting locations are 2106024, 1692355 and 4184549. We'll perform a forensic analysis to know what file contains the keyword.

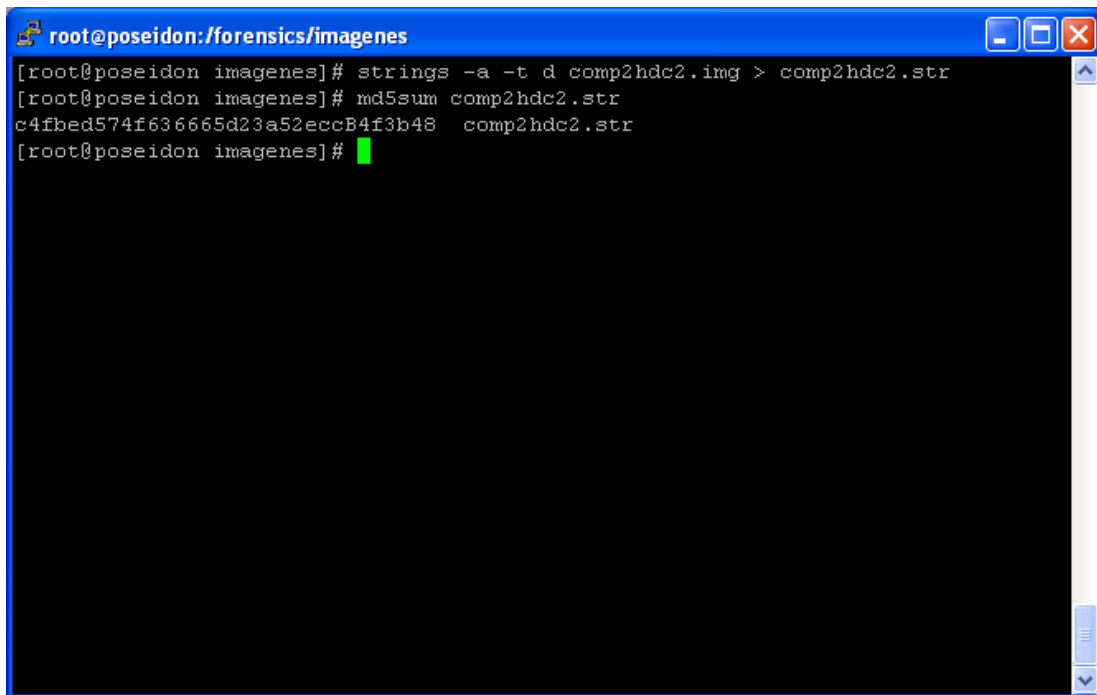
Let's test for status of all the clusters at figure 56. All of them are allocated.

Now we'll find all the i-nodes corresponding to the clusters. This can be seen on figure 57.

Now we'll find the file names corresponding to the i-nodes of figure 57. This can be seen on figure 58.

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

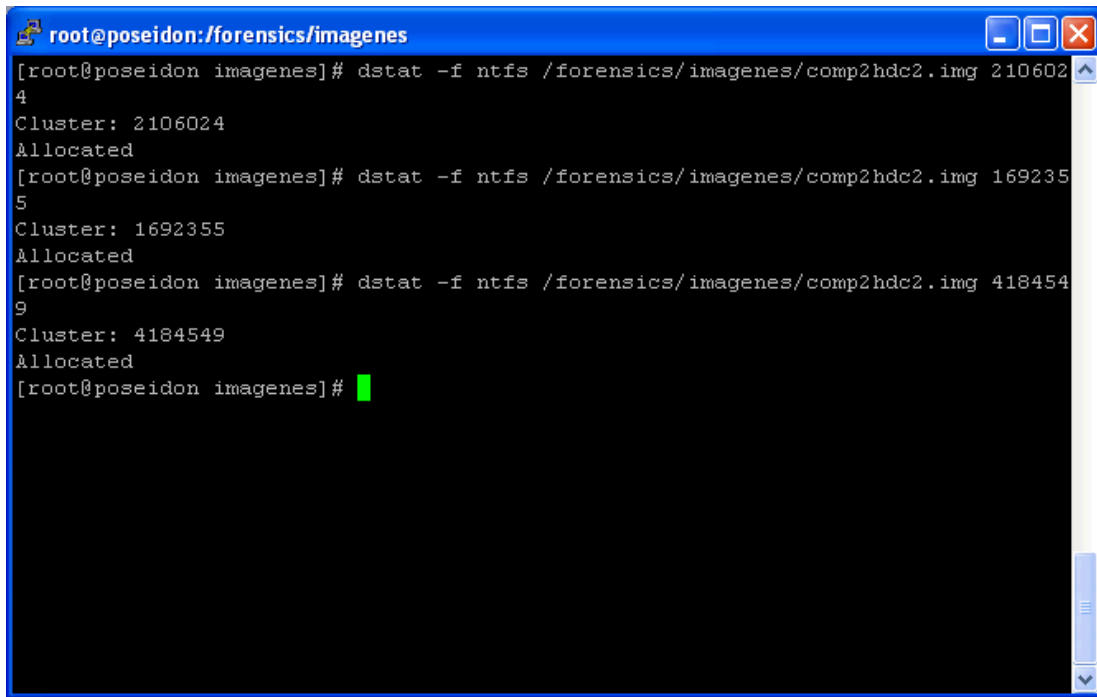
Figure 55: Strings file creation from analyzed image



```
root@poseidon:/forensics/imagenes
[root@poseidon imagenes]# strings -a -t d comp2hdc2.img > comp2hdc2.str
[root@poseidon imagenes]# md5sum comp2hdc2.str
c4fbcd574f636665d23a52eccB4f3b48 comp2hdc2.str
[root@poseidon imagenes]#
```

Figure 56: Status for clusters containing interesting information

© SANS Institute 2000 - 2005, Author

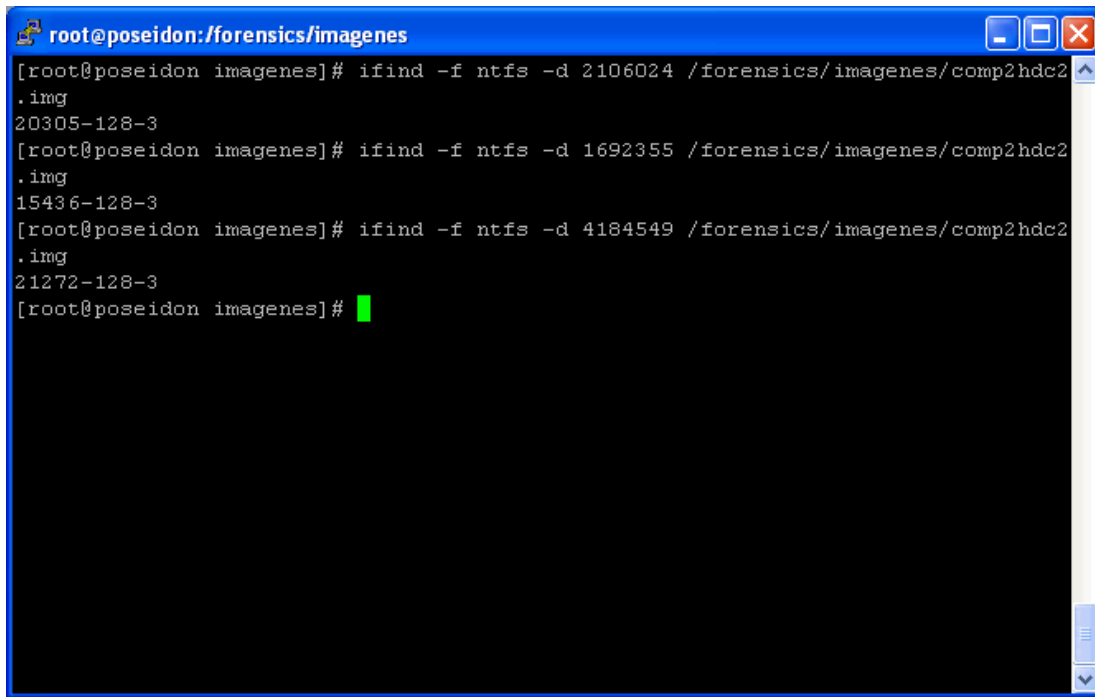
A terminal window titled 'root@poseidon://forensics/imagenes' with standard window controls. The terminal shows three sequential 'dstat' commands for the file '/forensics/imagenes/comp2hdc2.img'. Each command outputs the cluster number and the word 'Allocated'. The first command uses cluster 2106024, the second uses 1692355, and the third uses 4184549. The terminal ends with a green cursor on the prompt line.

```
root@poseidon://forensics/imagenes
[root@poseidon imagenes]# dstat -f ntfs /forensics/imagenes/comp2hdc2.img 2106024
4
Cluster: 2106024
Allocated
[root@poseidon imagenes]# dstat -f ntfs /forensics/imagenes/comp2hdc2.img 1692355
5
Cluster: 1692355
Allocated
[root@poseidon imagenes]# dstat -f ntfs /forensics/imagenes/comp2hdc2.img 4184549
9
Cluster: 4184549
Allocated
[root@poseidon imagenes]# █
```

When the files were edited, it was possible to find many magnetic stripes from valid debit cards. This verification was made with the Information Security Staff. Now we'll look for all ".adi" files on the image. The results are shown on figure 59.

All the files were edited and altogether were found 282 magnetic stripes. The bank staff verified all the magnetic stripes and they are all valid.

Figure 57: I-node corresponding to the allocated clusters of figure 56



```
root@poseidon:/forensics/imagenes
[root@poseidon imagenes]# ifind -f ntfs -d 2106024 /forensics/imagenes/comp2hdc2
.img
20305-128-3
[root@poseidon imagenes]# ifind -f ntfs -d 1692355 /forensics/imagenes/comp2hdc2
.img
15436-128-3
[root@poseidon imagenes]# ifind -f ntfs -d 4184549 /forensics/imagenes/comp2hdc2
.img
21272-128-3
[root@poseidon imagenes]#
```

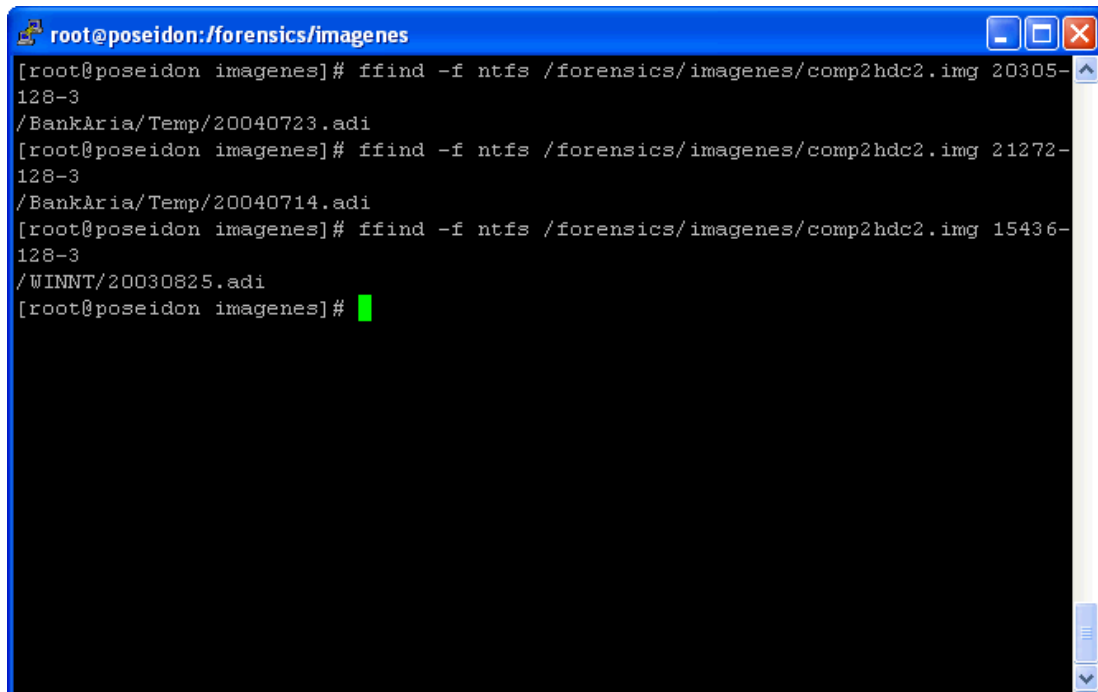
In order to confirm that this is a generalized problem in the bank, it was verified in other computers of one office of the city of Medellin, different from the one analyzed of the city of Barranquilla. The result was the same one, finding 35 .adi files with the magnetic stripes of debit cards used to perform transactions of the present month and the previous months.

3.9 Conclusions

The problem was originated because the Banking application generates logs with all the magnetic stripes of the office transactions transacted with card debit. This application has been running for over 4 years and nobody noticed this. All the computers with the banking software were verified for

.adi files and all of them had it with many magnetic stripes.

Figure 58: File names corresponding to i-nodes of figure 57



```
root@poseidon:/forensics/imagenes
[root@poseidon imagenes]# ffind -f ntfs /forensics/imagenes/comp2hdc2.img 20305-128-3
/BankAria/Temp/20040723.adi
[root@poseidon imagenes]# ffind -f ntfs /forensics/imagenes/comp2hdc2.img 21272-128-3
/BankAria/Temp/20040714.adi
[root@poseidon imagenes]# ffind -f ntfs /forensics/imagenes/comp2hdc2.img 15436-128-3
/WINNT/20030825.adi
[root@poseidon imagenes]#
```

The timeline contains information from access to the .adi files but the computer does not have information on the interactive logons made from it neither has synchronized the hour with all the computers of the bank, thus can be concluded that the information stealing could have been made by any person with account in the domain of the bank. The Bank will ask for the application supplier to fix the problem and deploy the installation to all the computers that uses it.

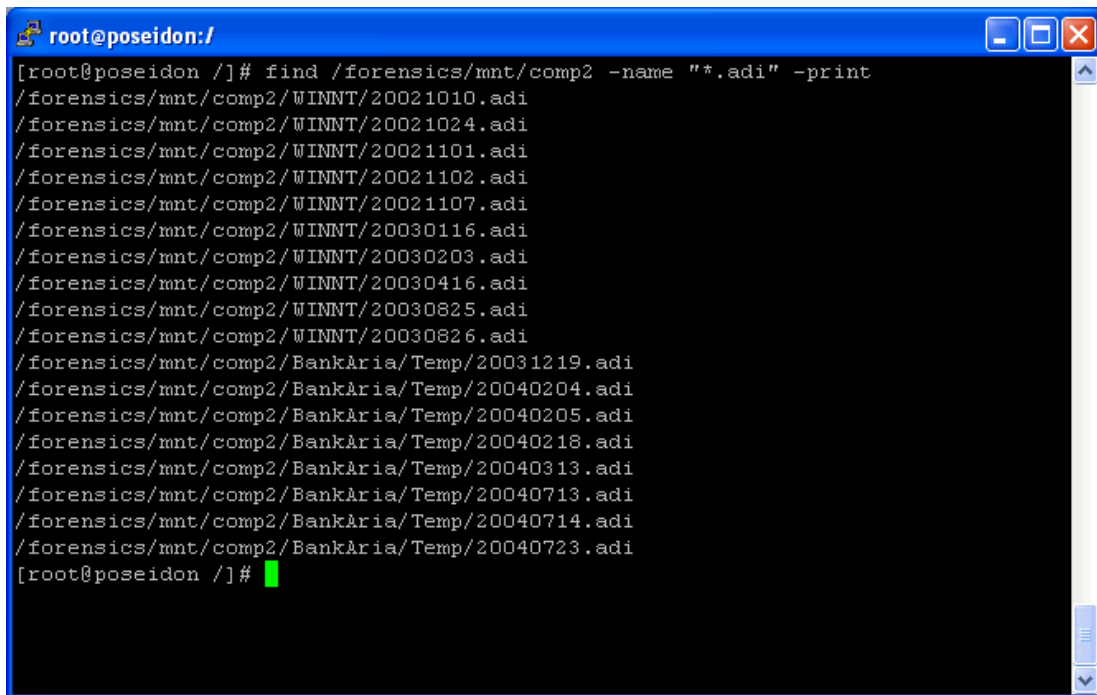
It is important to implement controls of perimetral security by means of intrusion detection systems and firewalls that allows to detect and prevent

nonauthorized access, provide evidence of all the intended operations and prevent that vulnerabilities of applications can be remotely exploited by just accessing a hard drive through the network.

The case opened before the competent authorities must follow its course with another type of registries and audits, because from the electronic point of view it is not possible to prove the culpability of the judged individual.

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

Figure 59:.adi files on image

A terminal window titled 'root@poseidon:/' with standard window controls (minimize, maximize, close) in the top right. The terminal displays the output of the command 'find /forensics/mnt/comp2 -name "*.adi" -print'. The output lists 24 .adi files, including those in the 'WINNT' and 'BankAria/Temp' subdirectories. The prompt '[root@poseidon /]# ' is visible at the end of the output.

```
[root@poseidon /]# find /forensics/mnt/comp2 -name "*.adi" -print
/forensics/mnt/comp2/WINNT/20021010.adi
/forensics/mnt/comp2/WINNT/20021024.adi
/forensics/mnt/comp2/WINNT/20021101.adi
/forensics/mnt/comp2/WINNT/20021102.adi
/forensics/mnt/comp2/WINNT/20021107.adi
/forensics/mnt/comp2/WINNT/20030116.adi
/forensics/mnt/comp2/WINNT/20030203.adi
/forensics/mnt/comp2/WINNT/20030416.adi
/forensics/mnt/comp2/WINNT/20030825.adi
/forensics/mnt/comp2/WINNT/20030826.adi
/forensics/mnt/comp2/BankAria/Temp/20031219.adi
/forensics/mnt/comp2/BankAria/Temp/20040204.adi
/forensics/mnt/comp2/BankAria/Temp/20040205.adi
/forensics/mnt/comp2/BankAria/Temp/20040218.adi
/forensics/mnt/comp2/BankAria/Temp/20040313.adi
/forensics/mnt/comp2/BankAria/Temp/20040713.adi
/forensics/mnt/comp2/BankAria/Temp/20040714.adi
/forensics/mnt/comp2/BankAria/Temp/20040723.adi
[root@poseidon /]#
```

Figure 60:Example of a .adi file

© SANS Institute 2000 - 2005, Author

```
root@poseidon:/forensics/mnt/comp2/WINNT
000022326771C
400252
CC00814140100000000001140100000140 00000037510000003810
CCCSC140100000140 00000037510000003810
CCCSC140100000140 00000037560000003810
000003834783CN
400297
000003834783CN
01218522001
1203014608
EFE=$265.22,LOC=$0.00,NAL=$0.00
000022326771C
EFE=$0.01,LOC=$0.00,NAL=$0.00
000022326771C
000022326771C
08600137985 0860013798
15601222
C000007481297
C000007481297 | 2003
EFE=$91.63,LOC=$0.00,NAL=$0.00
400566
ON00040100007763928
@
"20021024.adi" [readonly] [dos] 1031L, 58725C 48,1 2%
```

© SANS Institute 2000 - 2005, Author

4 References

- SANS Institute. Track 8 - System Forensics, Investigation and Response. Volume 8.2. SANS Press, Jan 28, 2004.
- "Windows TCP/IP Registry Entries". Microsoft Corporation. 16 Dec 2004. <<http://support.microsoft.com/default.aspx?scid=kb;en-us;158474>>
- The Sleuth Kit. Home Page. 16 Dec 2004. <<http://www.sleuthkit.org/sleuthkit/>>
- Cygwin Information and Installation. Home Page. 16 Dec 2004 <<http://www.cygwin.com>>
- Camouflage Home Page. Home Page. 22 Nov 2004 <<http://camouflage.unfiction.com>>
- Antecedentes de Ley desde la Ley 420 de 1998 y T́xtos de Ley desde La Ley 1 de 1992. Congreso de Colombia. 16 Dec 2004. <http://www.secretariasenado.gov.co/Antecedentes_ley1.asp>
- Seguis, Steve. "Querying Installed Software Remotely". Windows IT Pro. March 2004. December 16 2004. <<http://www.win2000mag.com/WindowsScripting/Article/ArticleID/41505/41505.html>>
- WinHex: Computer Forensics & Data Recovery Software, Hex Editor & Disk Editor. 2004. X-Ways Software Technology AG. 16 Dec 2004 <<http://www.sf-soft.de/winhex/index-m.html>>
- Windows Program Automatic Startup Locations. bleepingcomputer.com. 16 Dec 2004 <<http://www.bleepingcomputer.com/forums/index.php?showtutorial=44>>