

FINAL REPORT OF HOFFMANN FORENSIC CHALLENGE

Case Number: 001
Case Description: Hoffmann forensic challenge for Linux magazine
Tools Used: Libewf, Revit, Afflib, Testdisk, Sleuthkit, Autopsy, Steghide, Foremost, Dev-C++
Operating System: Linux bt 2.6.21.5 on Intel® Core™2 CPU T7200 @ 2.00 GHz
Microsoft Windows XP SP 2 on Intel® Core™2 2.00 GHz

Image Details

Date/Time Image Acquired: 09/10/2007 11:23:45
Image Name: mmc_challenge.E01
Description: Hoffmann forensic challenge for Linux magazine
Hash: ff810a83895039486e813c675ada6b39
Notes: MMC San disk found in digital camera
Drive Used to Store Image: /root/
/root/backup/

Activity logs:

```
bt ~ # curl -o mmc_challenge.E01 http://www.linuxmag.nl/download/application/octet-stream/472af4e029380mmc_challenge.E01
```

% Total	% Received	% Xferd	Average Speed	Time	Time	Time	Current
			Dload	Upload	Total	Spent	Left
100	792k	100	792k	0	0	203k	0
						0:00:03	0:00:03
						--:--:--	408k

```
bt ~ # dd if=/root/mmc_challenge.E01 of=/root/backup/mmc_challenge1.E01
1585+1 records in
1585+1 records out
811769 bytes (812 kB) copied, 0.0242805 s, 33.4 MB/s
```

```
bt ~ # md5 mmc_challenge.E01
8ee46a834e1a5c4f2279cbcd63a10621    mmc_challenge.E01
```

```
bt ~ # img_stat mmc_challenge.E01
IMAGE FILE INFORMATION
```

Image Type: ewf

Size of data in bytes: 6799360
MD5 hash of data: ff810a83895039486e813c675ada6b39

```
bt ~ # img_stat /root/backup/mmc_challenge1.E01
IMAGE FILE INFORMATION
```

Image Type: ewf

Size of data in bytes: 6799360
MD5 hash of data: ff810a83895039486e813c675ada6b39

```
bt ~ # ewfinfo -d dm mmc_challenge.E01
```

ewfinfo 20070512 (libewf 20070512, zlib 1.2.3, libcrypto 0.9.8, libuuid)

Acquiry information

Case number: 1
Description: <http://www.linuxmag.nl/nl/4137085f61440#> Hoffmann forensic challenge for Linux magazine
Examiner name: TGP
Evidence number: 1
Notes: MMC San disk found in digital camera
Acquiry date: 09/10/2007 11:23:45
System date: 09/10/2007 11:23:45
Operating system used: Linux
Software version used: 20070512
Password: N/A

Media information

Media type: fixed disk
Media is physical: yes
Amount of sectors: 13280
Bytes per sector: 512
Media size: 6799360
Error granularity: 64
Compression type: best compression
GUID: 00000000-0000-0000-0000-000000000000
MD5 hash in file: ff810a83895039486e813c675ada6b39

bt ~ # ewfverify mmc_challenge.E01
ewfverify 20070512 (libewf 20070512, zlib 1.2.3, libcrypto 0.9.8, libuuid)

Verify started at: Tue Dec 25 20:04:55 2007

This could take a while.

Verify completed at: Tue Dec 25 20:04:55 2007

Read: 6.4 MB (6799360 bytes) in 0 second(s).

MD5 hash stored in file: ff810a83895039486e813c675ada6b39
MD5 hash calculated over data: ff810a83895039486e813c675ada6b39

ewfverify: SUCCESS

Result Analysis Summary

Based on the image files and document found by our forensic tools, we conclude that:

1. The list of the other terrorists is presented in the following 'secret.txt' file along with a suspected picture in 00502400.jpg image file.
2. Based on the aforementioned text file, the attack was planned on January 2nd 2008.
3. They planned to attack several places in Keukenhof, Lisse, Netherlands, which is presented in 00523c00.jpg image file.
4. They concealed the information concerning the dates of the attack inside an image file with a picture of a microprocessor. This information was concealed using steghide tool and encrypted it with an unknown password utilizing rijndael-128

encryption technique. Thus, to craft the password and reveal the secret file, we have to reassemble an odt file in order to be in a correct Open Office Document format.

5. The following result summary describes our approaches and techniques to reveal the sensitive information on an acquired image.

Attached Files Highlight

Odt file

wachtwoord=slechtetijden
steghide gebruiken om te extracten

secret.txt

Contact codenaam e-mail gsm
piet de spier despier@mail.com 06-11111111
karel de gok degok@mail.com 06-22222222
henk de arm dearm@email.com 06-33333333
johan de teen deteen@postvak.nl 06-44444444
sondra de oorbel deoorbel@postbak.nl 06-55555555
jimmy oerwoud oerwoude@jungle.nl 06-66666666
bertus de melker demelker@mail.com 06-77777777

2 januari worden de bloemetjes buiten gezet

Result Summary

Case 001 for Hoffmann Forensic Challenge

Case Summary: Locating and recovering files on an acquired image file.

Tester Name: XXX

Test Date: 26/12/2007

Operating System: Linux bt 2.6.21.5

Tools used: Sleuthkit 2.09
Revit 07-alpha-20070804
Testdisk 6.8
Foremost 1.5.3
Autopsy 2.08
Stegdetect 0.5

Output files locations: /root/revived/
/root/revived1/
/root/revived2/
/root/testdisk-6.8/linux/recup_dir
/root/recovery/

Hash recovered files: 00502400.jpg - 270a0a913fa9603db8121fdf78d63ac
00509c00.jpg - 589032f2ec313816ef36772a08808db0
00509c1e.tif - 5f5782bf373988bf9effc935ce930d70

00523c00.jpg - 59bcfa18339749f1d25a6d30a2668a64
005ac000.jpg - e92a8f1202253443274122572bbb00d3
vol2-1.file5.odt - 5547959106670e5c989585c4720b7526

Log file highlights:

revit 20070804

Target directory: revived
Configuration file: file_types.conf
Block size: 512

Started: Tue Dec 25 21:45:45 2007

Revived file

Definition: jpeg
Filename: /complete/00502400.jpg
Start offset: 05252096 (0x00502400)
End offset: 05282069 (0x00509915)
Offset range(s): 05252096 (0x00502400) - 05264384 (0x00505400)
05265408 (0x00505800) - 05282304 (0x00509a00)
File size: 28 kB (28949 bytes)
Calculated MD5: 270a0a913fa9603db8121fdf78d63aca

Revived file

Definition: jpeg
Filename: /complete/00509c00.jpg
Start offset: 05282816 (0x00509c00)
End offset: 05388827 (0x00523a1b)
Offset range(s): 05282816 (0x00509c00) - 05295104 (0x0050cc00)
05296128 (0x0050d000) - 05389312 (0x00523c00)
File size: 102 kB (104987 bytes)
Calculated MD5: 589032f2ec313816ef36772a08808db0

Revived file

Definition: tiff_big_endian
Filename: /embedded/00509c00.jpg/complete/00509c1e.tif
Start offset: 05282846 (0x00509c1e)
End offset: 05282860 (0x00509c2c)
Offset range(s): 05282816 (0x00509c00) - 05283328 (0x00509e00)
File size: 14 bytes
Calculated MD5: 5f5782bf373988bf9effc935ce930d70

Revived file

Definition: jpeg
Filename: /complete/00523c00.jpg
Start offset: 05389312 (0x00523c00)
End offset: 05502428 (0x0053f5dc)
Offset range(s): 05389312 (0x00523c00) - 05401600 (0x00526c00)
05402624 (0x00527000) - 05502464 (0x0053f600)
File size: 109 kB (112092 bytes)
Calculated MD5: 59bcfa18339749f1d25a6d30a2668a64

Revived file

Definition: jpeg

Filename: /complete/005ac000.jpg
Start offset: 05947392 (0x005ac000)
End offset: 06055796 (0x005c6774)
Offset range(s): 05947392 (0x005ac000) - 06055936 (0x005c6800)
File size: 105 kB (108404 bytes)
Calculated MD5: e92a8f1202253443274122572bbb00d3

Finished: Tue Dec 25 21:45:46 2007

Input data: mmc_challenge.E01
Input data size: 6.4 MB (6799360 bytes)
Input MD5: ff810a83895039486e813c675ada6b39

Autopsy Hex Report

----- GENERAL INFORMATION

File: /1//file5.odt
MD5 of file: 5547959106670e5c989585c4720b7526
SHA-1 of file: 4c4cf02b7e4031a59b88fd3705c6007e1d4c8629

Image: /root/.autopsy_cases/Hoffman01/localhost/images/mmc_challenge.E01'
Offset: 16 to 13247
File System Type: ext

Date Generated: Wed Dec 26 17:16:03 2007
Investigator: unknown

VERSION INFORMATION

Autopsy Version: 2.08
The Sleuth Kit Version: 2.09

Activity Logs:

bt ~ # mmls mmc_challenge.E01
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

	Slot	Start	End	Length	Description
00:	----	0000000000	0000000000	0000000001	Primary Table (#0)
01:	----	0000000001	0000000015	0000000015	Unallocated
02:	00:00	0000000016	0000013247	0000013232	Linux (0x83)
03:	----	0000013248	0000013279	0000000032	Unallocated

bt ~ # revit -Ae mmc_challenge.E01
Status: at 100%.
analyzed 6.4 MB (6799360 bytes) of total 6.4 MB (6799360 bytes).
completion in 0 second(s) with 6.4 MB/s (6799360 bytes/second).

Analysis of input successful at: Tue Dec 25 21:45:46 2007

Analyzed: 6.4 MB (6799360 bytes) in 1 second(s) with 6.4 MB/s (6799360 bytes/second).

Calculated MD5: ff810a83895039486e813c675ada6b39
bt ~ # revit -Ae -c mpeg.conf -t revived1 mmc_challenge.E01
Status: at 100%.
analyzed 6.4 MB (6799360 bytes) of total 6.4 MB (6799360 bytes).
completion in 0 second(s) with 3.2 MB/s (3399680 bytes/second).

Analysis of input successful at: Tue Dec 25 21:51:32 2007

Analyzed: 6.4 MB (6799360 bytes) in 2 second(s) with 3.2 MB/s (3399680 bytes/second).
Calculated MD5: ff810a83895039486e813c675ada6b39
bt ~ # revit -Ae -c elf32.conf -t revived2 mmc_challenge.E01
Status: at 100%.
analyzed 6.4 MB (6799360 bytes) of total 6.4 MB (6799360 bytes).
completion in 0 second(s) with 3.2 MB/s (3399680 bytes/second).

Analysis of input successful at: Tue Dec 25 21:54:01 2007

Analyzed: 6.4 MB (6799360 bytes) in 2 second(s) with 3.2 MB/s (3399680 bytes/second).
Calculated MD5: ff810a83895039486e813c675ada6b39

bt linux # testdisk_static /root/mmc_challenge.E01

Tue Dec 25 22:53:43 2007
Command line: TestDisk

TestDisk 6.8, Data Recovery Utility, August 2007
Christophe GRENIER <grenier@cgsecurity.org>
<http://www.cgsecurity.org>
Linux version (ext2fs lib: 1.39, ntfs lib: 9:0:0, reiserfs lib: 0.3.1-rc8, ewf lib: 20070512)
Using locale 'C'.
Hard disk list
Disk /dev/sda - 100 GB / 93 GiB - CHS 12161 255 63, sector size=512

Partition	Start	End	Size in sectors
Linux	0 0 17	0 210 18	13232

superblock 0, blocksize=1024

Image /root/mmc_challenge.E01 - 6799 KB / 6640 KiB - CHS 0 255 63

Partition	Start	End	Size in sectors
P Linux	0 0 17	0 254 63	16049

Structure: Ok. Use Up/Down Arrow keys to select partition.
Use Left/Right Arrow keys to CHANGE partition characteristics:
*=Primary bootable P=Primary L=Logical E=Extended D=Deleted
Keys A: add partition, L: load backup, T: change type, P: list files,
Enter: to continue
EXT3 Sparse superblock, 8217 KB / 8024 KiB

P Linux	0 0 17	0 254 63	16049
---------	--------	----------	-------

Use Right arrow to change directory, q to quit
Directory /

drwxr-xr-x 0 0 1024 9-Oct-2007 12:58 .

```
drwxr-xr-x  0  0   1024 9-Oct-2007 12:58 ..
drwx----- 0  0  12288 9-Oct-2007 12:56 lost+found
-rw-----  0  0  28949 9-Oct-2007 12:58 file1.jpg
-rw-----  0  0 104987 9-Oct-2007 12:58 file2.jpg
-rw-----  0  0  37000 9-Oct-2007 12:58 file4.jpg
-rw-----  0  0 439911 9-Oct-2007 12:58 file5.odt
```

Directory /lost+found

```
drwx----- 0  0  12288 9-Oct-2007 12:56 .
drwxr-xr-x  0  0   1024 9-Oct-2007 12:58 ..
```

Partition	Start	End	Size in sectors
1 P Linux	0 0 17	0 254 63	16049

[Quit] [Write]
Return to main menu

TestDisk exited normally

bt linux # photorec_static /root/mmc_challenge.E01

PhotoRec 6.8, Data Recovery Utility, August 2007
Christophe GRENIER <grenier@cgsecurity.org>
<http://www.cgsecurity.org>

Image /root/mmc_challenge.E01 - 6799 KB / 6640 KiB (RO)

Partition	Start	End	Size in sectors
D empty	0 0 1	0 210 50	13280 [Whole disk]
1 P Linux	0 0 17	0 210 18	13232

[Search] [Options] [File Opt] [Quit]
Start file recovery

Do you want to save recovered files in /root/testdisk-6.8/linux ? [Y/N]
Do not choose to write the files to the same partition they were stored on.

To select another directory, use the arrow keys.

```
drwxrwxr-x 500 500 4096 13-Aug-2007 17:18 1
drwxrwxr-x 500 500 4096 25-Dec-2007 23:09 .
drwxrwxr-x 500 500 4096 13-Aug-2007 17:18 ..
```

Image /root/mmc_challenge.E01 - 6799 KB / 6640 KiB (RO)

Partition	Start	End	Size in sectors
D empty	0 0 1	0 210 50	13280 [Whole disk]

1 files saved in /root/testdisk-6.8/linux/recup_dir directory.
Recovery completed.
jpg: 1 recovered

1 P Linux	0 0 17	0 210 18	13232
-----------	--------	----------	-------

To recover lost files, PhotoRec need to know the filesystem type where the file were stored:

[EXT2/EXT3] EXT2/EXT3 filesystem
[Other] FAT/NTFS/HFS+/ReiserFS/...

Image /root/mmc_challenge.E01 - 6799 KB / 6640 KiB (RO)

Partition	Start	End	Size in sectors
1 P Linux	0 0 17	0 210 18	13232

4 files saved in /root/testdisk-6.8/linux/recup_dir directory.

Recovery completed.

jpg: 4 recovered

```
bt ~ # foremost -t all -o /root/recovery/ -i mmc_challenge.dd
```

```
Processing: mmc_challenge.dd
```

```
|*|
```

```
bt ~ # stegdetect 00502400.jpg
```

```
/root/00502400.jpg : negative
```

```
bt ~ # stegdetect 00523c00.jpg
```

```
/root//00523c00.jpg : negative
```

```
bt ~ #stegdetect 00509c00.jpg
```

```
/root/00509c00.jpg : negative
```

```
bt ~ # stegdetect 005ac000.jpg
```

```
/root//005ac000.jpg : negative
```

Expected Results: Document and image files are successfully carved from an image.

Actual Results: Different tools came up with different files.

Analysis: Using different file recovery tools, we were able to extract some images and documents which lead to a preliminary information concerning terrorist activities.

Case 001 for Hoffmann Forensic Challenge

Case Summary: Find a valuable information from a scrambled file which leads to a clue.

Tester Name: XXX

Test Date: 27/12/2007

Operating System: Microsoft Windows XP SP 2 on Intel Core2 Duo 2GHz

Tools used: Bloodshed Dev-C++ 4.9.9.2

Output files location: C:\

Log file highlights: -

Activity Logs:

```
C:\>random
```

```
Enter file name: vol2-1.file5.odt
```

```
There are 439912 characters in vol2-1.file5.odt
```

```
There are 756 lines
```

```
C:\>dir
```

```
Volume in drive C is Programs
```

```
Volume Serial Number is 0CE2-9F21
```

Directory of C:\

```
20-06-2007 14:10          0 AUTOEXEC.BAT
20-06-2007 14:10          0 CONFIG.SYS
26-12-2007 20:55 <DIR>      Dev-Cpp
27-12-2007 21:38 <DIR>      Documents and Setting
26-06-2007 08:19 <DIR>      I386
27-12-2007 22:35      439.912 out.odt
27-12-2007 11:26 <DIR>      Program Files
27-12-2007 11:50      17.224 random.exe
26-12-2007 18:17      439.911 vol2-1.file5.odt
26-12-2007 01:38 <DIR>      WINDOWS
          5 File(s)      897.047 bytes
          5 Dir(s)  7.111.213.056 bytes free
```

Expected Results: Recognize an accurate pattern of vol1-1.file5.odt file.
Actual Results: Random.c compiled binary was successfully reassembled the file into an Open Office Document format.
Analysis: Since we know that the extension of vol1-1.file5 is odt and scrambled version of this file contains KP, we figure out way to unscramble the file in order to become an accurate Open Office Document format. Inside this file, we found valuable information concerning password and tool which is used to encrypt a sensitive information.

Case 001 for Hoffmann Forensic Challenge

Case Summary: Extract sensitive information from a collection of suspected files.
Tester Name: XXX
Test Date: 28/12/2007
Operating System: Linux bt 2.6.21.5
Tools used: Steghide 0.5.1
Output files location: /root/
Log file highlights: -

Activity Logs:

```
bt ~ # steghide info 00509c00.jpg
"00509c00.jpg":
  format: jpeg
  capacity: 6.2 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
steghide: could not extract any data with that passphrase!
```

```
bt ~ # steghide info 005ac000.jpg
"005ac000.jpg":
  format: jpeg
  capacity: 6.2 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "secret.txt":
    size: 397.0 Byte
```

encrypted: rijndael-128, cbc
compressed: yes

```
bt ~ # steghide info 00523c00.jpg
"00523c00.jpg":
  format: jpeg
  capacity: 6.4 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
steghide: could not extract any data with that passphrase!
```

```
bt ~ # steghide info 00502400.jpg
"00502400.jpg":
  format: jpeg
  capacity: 1.5 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
steghide: could not extract any data with that passphrase!
```

```
bt ~ # steghide extract -sf 005ac000.jpg
Enter passphrase:
wrote extracted data to "secret.txt".
```

Expected Results:	Extract sensitive information.
Actual Results:	A text files successfully extracted from one jpeg file.
Analysis:	After careful tests on a collection of images found by different tools, we finally found one file that outputs a 'secret.txt' file which contains valuable information.