FORENSIC ANALYSIS OF USB MEDIA EVIDENCE

Jesús Alexander García
Luis Alejandro Franco
Juan David Urrea
Carlos Alfonso Torres
Manuel Fernando Gutiérrez

UPB
2012
Content

INTRODUCTION .......................................................................................................................... 3
OBJECTIVE ................................................................................................................................. 4
EVIDENCE ACQUISITION ........................................................................................................... 4
EVIDENCE EXAMINATION ......................................................................................................... 8
  Preparation........................................................................................................................................ 8
  Host system information: .............................................................................................................. 8
  Guest virtualized Forensic Workstation: ......................................................................................... 8
Examination...................................................................................................................................... 9
  File System Analysis Results ....................................................................................................... 9
  Extraction Analysis Results ........................................................................................................... 11
  Forensic Analysis Results ............................................................................................................. 13
  Forensic Carving Results ............................................................................................................. 15
CONCLUSIONS ............................................................................................................................ 24
INTRODUCTION

Information is an important asset in any company, but sometimes can’t be seen its real value unless it is not available of this, in the case of forensic analysis is necessary to find information that may have been deleted by experts in order to complicate the process of obtaining this. Is here where the importance of both basic and advanced knowledge in information management, as this is stored on devices, metadata, differences between different storage media and tools are available for this process. Below is set forth in detail the forensic analysis to a USB storage device for information which may or may not be stored on this device.
OBJECTIVE

Obtain the major amount of information related to crimes of human and drug trafficking that is contained in the digital storage media that were delivered to forensic analysis group.

EVIDENCE ACQUISITION

Before performing forensic analysis on the USB storage device, we must ensure that this will not be modified, to hide, to change or add information that may alter the process of collecting evidence.

The first person to have contact with the USB storage device was the researcher Juan Urrea, who received first-hand the USB storage device from Mr. Reinaldo Mayol. However, for the analysis of the USB storage device and to avoid altering of the evidence, we take a snapshot of the device’s file system. The following is the procedure for obtaining the image.

The researcher Juan Urrea received the USB storage device with serial00187D0F5675EBA1, model DT108, 4GB capacity, manufactured in China, size 4x2 cm, blue and black, in Room 211 of Block 11 in Universidad Pontificia Bolivariana, on 17 March 2012 and he take it under his custody for two days, then proceeded to give it to Jesus Garcia researcher who take custodian until the time of the snapshot of the device on which would be carried out forensic analysis. The following explains in detail the procedure to take the snapshot the USB storage device.

On Tuesday 20 March, the researchers Manuel Gutierrez and Jesus Garcia around 8:50 AM (-5 GMT) reached room 211 of Block 11 of the Universidad Pontificia Bolivariana, to perform the procedure for generating an image (snapshot) processing of the evidence. There were several drawbacks to start this procedure; due to lack of tools in the computer equipment chosen for this, so the researchers decided to take another PC.

To ensure the integrity of the data that were in the USB storage device was used an external tool (blocker) that can connect the device, and allow the copy or creation of information without altering its content.

Image 1
Initial State of Digital Media Evidence
Image 2
Sector Count of Blocker Information

Image 3
Serial Media of Blocker Information
Around 10 am, begins the process of making the image of the USB device. To take a snapshot of the device was used a tool that is the operating system Backtrack r1, dc3dd which allows exact images of a storage device.

The process lasted about 1 hour.
Once finished making the image (snapshot) on which will be performed the forensic analysis is necessary to sign it (with SHA) to ensure the integrity of the proceedings and rule manipulations that compromise the process.

For this was used the gpg tool, which was signed with the image. There is not image of the signature process only gpg
EVIDENCE EXAMINATION

The evidence analysis refers to the interpretation of the recovered data and his location in a logical format. The purpose of this phase is turning the acquired data in to evidence. The analysis is often executed in three steps: Preparation - Extraction – Interpretation

Preparation

Is the process of prepare the resources for the evidence examination; it includes hardware components, software tools and storage capacity. The investigation process was followed through virtualized environment with VMware Player.

Host system information:
Intel® Core ™ i7 CPU 860 @ 2.80GHz
10 GB of RAM
1TB HDD
Operating System: Dual partition with Windows XP Service Pack 3 CentOS 6

Guest virtualized Forensic Workstation:
Backtrack 5 R1 Virtual Appliance

Tools:

<table>
<thead>
<tr>
<th>Forensic Analysis Tools</th>
<th>bulk_extractor</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>evtparse</td>
</tr>
<tr>
<td></td>
<td>Exiftool</td>
</tr>
<tr>
<td></td>
<td>missidentify</td>
</tr>
<tr>
<td></td>
<td>Mork</td>
</tr>
<tr>
<td></td>
<td>Pref</td>
</tr>
<tr>
<td></td>
<td>PTK</td>
</tr>
<tr>
<td></td>
<td>Readpst</td>
</tr>
<tr>
<td></td>
<td>Reglookup</td>
</tr>
<tr>
<td></td>
<td>Stegdetect</td>
</tr>
<tr>
<td></td>
<td>Vinetto</td>
</tr>
<tr>
<td></td>
<td>Encase</td>
</tr>
<tr>
<td></td>
<td>Pci Recovery</td>
</tr>
<tr>
<td></td>
<td>Linux Recovery</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Forensic Carving Tools</th>
<th>Fatback</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Foremost</td>
</tr>
<tr>
<td></td>
<td>Magic rescue</td>
</tr>
<tr>
<td></td>
<td>Recoverjpeg</td>
</tr>
<tr>
<td></td>
<td>Safecopy</td>
</tr>
<tr>
<td></td>
<td>Scalpel</td>
</tr>
<tr>
<td></td>
<td>scrounge-ntfs</td>
</tr>
<tr>
<td></td>
<td>Testdisk</td>
</tr>
</tbody>
</table>
Examination

In this stage, the extraction of the data from the drive is based on the file system present on the drive and may include data from such areas as active files, deleted files, slack space and unallocated space. The following steps show us how we got the results, everything doing since the image file

1. Extract the image from zip file

2. The file was renamed to FinalForense.dat and moved to the investigation folder:
3. Verify the SHA-256 sum of the image file, in order to establish that the file not have been altered:

```
3.
  Verify
  the
  SHA
  256
  sum
  of
  the
  image
  file,
  in
  order
  to
  establish
  that
  the
  file
  not
  have
  been
  altered:
```

```
root@bt:~/ForensicUPB

root@bt:~/.ForensicUPB# ls 
FinalForensce.dat FinalForensce.dat.gpg FinalUPT.zip.001
root@bt:~/.ForensicUPB#
```

4. The image file was mounted in the file system and the content is listed

```
root@bt:~/.ForensicUPB# shasum -a 256 FinalForensce.dat
13e75f9e2b1fe3a802b55e05e701f310167d77e6c2a779999e5c2657e9a9142b FinalForensce.dat
root@bt:~/.ForensicUPB#
```

```
root@bt:~/.ForensicUPB# mount -o loop FinalForensce.dat /mnt/diskUPB/
root@bt:~/.ForensicUPB# cd /mnt/diskUPB/
root@bt:~/.ForensicUPB# ls 
lost+found
```

```
Finding 1:
As result of the command, we did not find any relevant file in the folder structure.
```

Once the forensic image is obtained, is possible to get the USB information with a fully examination of first data block Encase Forensics on the disk view and the sleuth kit tools as show below

File System: Ext3
Total Inodes: 240000
Total Blocks: 958727
Reserved Blocks: 47936
Free Blocks: 925372
Free Inodes 239989
First data block: 0
Block Size: 2 -> 4096
Fragment Size: 2 -> 4096
Number of blocks per group: 32768
Number of inodes per group: 8000
Last Mounted: 16 mar 2012 - 5 39 18 pm
Last Written: 16 mar 2012 – 5: 40 :14 pm
Mount count: 01
Signature: 53ef
File system state: 01
First non-reserved inode: 11
Size of inode structure: 256

It’s remarkable that the total number of inodes is 11 more than free inodes which means there are just 11 used inodes and it’s known these are reserved inodes. So the first thing we can conclude is that there are not used inodes with metadata files. To make this conclusion more reliable we examined the total information of 30 groups of blocks (See fstab appended). Group 0 have used the first directory entry for parents of directories and every inodes from the others groups are unused.

**Extraction Analysis Results**

With free inodes we can conclude that the inodes bitmap of inodes are empty of ones on each entry unless the reserved inodes Hence like this partition was an ext3 file system is so possible that there will be no results for direct blocks on the inode tables which is verified by going into the disk view of Encase. This is done by checking the group descriptor for the file system is examined in block 2.
By this we know that the inode table for the first group begins at block 238. When examining the group 238 and the information observed in the first table of the size of the inode structure is 256 bytes we can view information of each of the 11 reserved inodes and data. We review the direct blocks they point to each of the inode and if there is any other information in its structure and is not common programs reviewed data recovery that may be relevant to the investigation found no positive results for this analysis. On the other hand emphasizes the inode 8 having blocks housing the journal for later review logs blocks of transactions on the file system. For this and we know that the inode structure is 256 and we started in block 238 we see this block more 256 * (8-1) = 1792 and direct blocks are offset 40 to 99 and found the block 426486 the following blocks.

In this case we have three possibilities for recovering data without having any metadata of files that maybe were in the allocated space of disk before file system was deleted. These are: looking for journals descriptors, file carving and see block to block for relevant data.

In order take as little time as possible we started with journal examination with ext3grep tool. This tool performance an examination of journals blocks which are pointed on inode 8 how is showed before, in this case looking for specified inodes or blocks on transactions done. This doesn’t have any results.

The second possibility was data carving which look for file signatures on the whole disk. For making this search several utilities like encase, linuxrecovery, pcrecovery, bulk_extractor etc which are described later and that were used in order to find any kind of signature file that make sense with the goal investigation.

The last option available to obtain data relevant to the investigation was to look block by block in hexadecimal and aschis. Initially a division is performed on each of the blocks 958,727 and is checked one by one. The information found in each block is also examined in WinHex without getting any relation to the objective of the investigation, however it was very easy for any of the data passed unnoticed by manual analysis as more than 900,000 blocks so the last review covered generating a report in ENCASE for all consecutive blocks that did not have any information which was subsequently used to carry out a script that would reduce the number of blocks and blocks indicate only that had information. Once done, we review again having fewer blocks again finding all signatures of the files found in file carving process but without substantial data were related to the investigation.

So then and once they are made all the options approach to this type of digital evidence can be concluded that there is no storage in this medium any information that directly relates to the type of research that is taking in this case.
Forensic Analysis Results

1. **Bulk_extractor**: Is an utility that scans many types of information and outputs information that it finds in them. This tool does not look at file system structures on the input, this search common strings and each found item is put as a file in the specified output folder.

Once the process is finished, we check the output folder to view the results files:
In the file where the email information is collected, the content of the file reveals some email accounts:

Finding 2:
There is not sufficient data to establish a criminal behavior, with the tracking of suspicious accounts.
Forensic Carving Results

1. **Foremost**: is a tool specialized in file carving. It takes image files and search for file headers, in order to recover files. It returns information to the user by putting the files found to a predetermined directory set by the user.

   ```
   root@wolverine:~/.forensicUIB# foremost -v -o foremost_result/ -i finalforensic.dat
   Foremost Version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
   Audit File
   Foremost started at Fri Apr 20 20:57:06 2012
   Invocation: foremost -v -o foremost_result/ -i finalforensic.dat
   Output directory: /home/user/UIB/foremost_result
   Configuration file: /usr/local/etc/foremost.conf
   Processing: finalforensic.dat
   -------------------------------------------
   File: finalforensic.dat
   Start: Fri Apr 20 20:57:06 2012
   Length: 3 GB (3926948464 bytes)
   Num  Name (bs=512)  Size  File Offset  Comment
   0     No Files
   ---------------------------------------------
   Foremost results:
   0 FILES EXTRACTED
   Foremost finished at Fri Apr 20 20:57:56 2012
   ```

   As result of the use of the utility, no files were found in the disk image.

2. **Scalpel**: is a well known file carving utility that searches a database of known file header and footer signatures, and attempts to carve files from a disk image file.

   The command used is:
This tool identifies the following types of files:

<table>
<thead>
<tr>
<th>File type</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pgp</td>
<td>\x99\x00 \x95\x01 \x95\x00 \xa6\x00</td>
</tr>
</tbody>
</table>
| mpg       | Header: \x00\x00\x01\xba  
|           | Footer: \x00\x00\x01\xbb |
| Rpm       | \xed\xab               |

The found files are corrupt, because they can not be read by any known program. In the attachment you can see a detail of the previous result. (See scalpel.docx)

3. Sleuth kit (fls): This tool Generate a log of deleted files.

The command used is:

```
# fls -f ext3 -d -r -v -p /root/Desktop/final.dat
```

The options used are:

- find deleted files (-d),
- recursively display directories (-r),
- show the full path of the files (-p),
- verbose mode (-v), see what's happening.

The output of last command is:

```
1044 m/l/s=0/0/0 u/g=0/0 macd=0/0/0/0
1045 m/l/s=0/0/0 u/g=0/0 macd=0/0/0/0
1046 m/l/s=0/0/0 u/g=0/0 macd=0/0/0/0 ...
239992 m/l/s=0/0/0 u/g=0/0 macd=0/0/0/0
239993 m/l/s=0/0/0 u/g=0/0 macd=0/0/0/0
239994 m/l/s=0/0/0 u/g=0/0 macd=0/0/0/0
239995 m/l/s=0/0/0 u/g=0/0 macd=0/0/0/0
```
The tool does not detect deleted files, because the image used does not contain metadata information, and most of the data blocks are empty. (See Section Fsstat)

4. Sleuth kit (fsstat): This tool displays the details associated with a file system.

The command used is:

```
# fsstat -f ext3 /root/Desktop/final.dat
```

The output is:

```
Total Inodes: 240000
Total Blocks: 958727
Reserved Blocks: 47936
Free Blocks: 925372
Free Inodes 239989
First data Block: 0
Block Size: 2 -> 4096
Fragment Size: 2 -> 4096
Number of blocks per group: 32768
Number of inodes per group: 8000
Last Mounted: 16 mar 2012 - 5:39:18 pm
Last Written: 16 mar 2012 - 5:40:14 pm
Mount count: 01
Signature: 53ef
File system state: 01
First non-reserved inode: 11
Size of inode structure: 256
```

The Output the last command is:
5. **Linux recovery**: This tool is designed to recover the erased or damaged information that is kept on Ext2/Ext3 partitions. Can recover files accidentally deleted and which has been erased long time ago. It is also capable of restoring corrupted files and can read and recover the information located on an inaccessible drive.

Below it can see the use of the tool:

---

**Step 1: Mount Image**

---
Step 2: Choose the evidence

Step 3: Scan the image
Step 4: Explore files recovered

The results are:

- A text file which contains an email with academic discussion between some teachers. *(See linuxRecovery.docx)*

- An XML file which contains a particular configuration of a device from Apple (Mac, iPhone, etc). *(See linuxRecovery.docx)*

The found files are not substantial evidence in the investigation.

PCI Recovery

First, we try to get back the file system with the tool PCI File Recovery, to do so, we take the image, and mount it with FTK Imager as a file system from the pc:

File > Image Mounting
Now, in the PCI File Recovery, we chose Open Unit.

In the Tab Physical Unit, we looked for the disk that FTK Imager has Created and selected it, then chose Find Logical Units.
Then, And chose between the latest options

As a result we obtain a representation of the files that can be recovered with this tool.
With this tool, we find out some text files that could be configurations files from some Mac OS X programs like itunes.

Nothing relevant could be find out with this tool, because most of the found files, were incomplete and was no possible its visualization.

There are three kinds of data that was found with these technique, mail, video in mpeg format and jpg image. Email was totally recovered although its content was not relevant for the investigation. Video was found on block 47860 with this signature `x00\x00\x01xBA` and jpg image was found in block 54446 with signature `xFFxD8xFF`. What is not good for the last files was that no one of these belongs to any real image or video but a sequence of data.
CONCLUSIONS

1. Ext3 is a fully challenge environment in forensics tasks because it actually of zeros every pointer of inodes when a file is deleted.

2. It is impossible to know and use all tools available for data recovery, but knowing how they conduct their procedures, can give you the knowledge so that you can generate search options and be able to achieve results that may be particular an investigation.

3. Sector by Sector analysis of disks is not a good first option especially if you have very large disks, so you should always look the way for any information, report or searched hits which give you a relationship with blocks that can be finally examined even if you don’t have metadata files.

4. Knowing the structure of a file system not only provides the ability to get the most out of data that still exist in this but the possibility of discarding values that should not be immersed in the structure and can be very important in research.

5. To ensure the integrity of the information it is necessary that the investigator use all the tools that the researcher has at hand, as well as create a digital signature for image.

6. The conservation of the chain of custody can be the determining factor in an investigation.

7. It is necessary to make a proper process of documentation, not only because is the procedure required by the forensic analysis, but because it helps the researcher in the process of the analysis of the evidence and diminishes the impact of the human error.

8. Ensuring the integrity of the copies made of the evidence is just as important as the original.

9. There is no storage in this medium any information that directly relates to the type of research that is taking in this case.

10. Is important to do the forensic investigation on a copy of the device to be analyzed to avoid modification, alteration and rewrite of the information because there is the possibility that this may help a third one.