



Digital Forensics Report

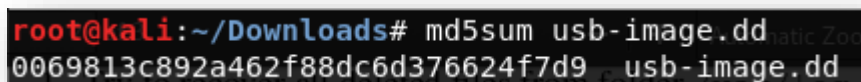
Luís Aguiar 80950 & Jorge Pereira 81428 & Filipe Azevedo 82468

1 Objectives of the investigation

In this case we were given an image of a pen drive. All we knew about this image is that it had a FAT32 file system. The goal was to find 15 hidden files in this image and check if there is any relationship between them.

2 Artifacts for analysis

As previously stated the only file that was delivered to us was an image of a pen. So, we checked the md5 fingerprint to be sure that the image that was delivered to us was not adulterated.



```
root@kali:~/Downloads# md5sum usb-image.dd
0069813c892a462f88dc6d376624f7d9  usb-image.dd
```

Figure 1 - MD5 fingerprint of the pen drive image

3 Evidence to look for

After verifying the integrity of the image, we proceeded with the investigation. We tried to look for some metadata of the file system, but as soon as we tried to do it, we were only faced with a message saying: "No metadata for you". We also verified that the owner of this pen drive had zeroed the location of the metadata, leaving only the previously mentioned message. This indicated that the person who did this had some knowledge about the operation of file systems, namely FAT, and that they were possibly trying to hide some interesting content in this pen drive.

4 Examination details

Since all of the file system metadata had been deleted, we concluded that we would need to perform manual search, to possibly find some interesting files on the pen drive.

Fortunately, we were able to find some directory entries (structure that stores some metadata of the files), and from there we were able to identify that there were 15 files in that pen drive, some of which had already been erased. With some relatively simple calculations, we were able to get the location of the beginning of each file. We also knew the size of each file, since this information is in the directory entries found previously, and if they were stored sequentially on memory, we had all the information to try to recover all 15 files. And so, we got the evidences below.

Name	Id	Timestamp	Size (bytes)	MD5	Description
2003_document.doc	01	2005-03-09 13:25:50	19968	80bb460201eb3475 6ea199ca8513d430	A Microsoft Word document that we were not able to open. However we did extract it and it contain a text file inside containing a description of the Microsoft Word 6.0 Binary File Format.
domopers.wmv	02	2005-03-09 13:25:50	8037267	63c0c6986cf0a446cb 54b0ac65a921a5	A WMV file containing a video of some sort of doll dancing.
enterprise.wav	03	2005-03-09 13:25:50	318895	7629b89adade055f6 783dc1773274215	A WAV file containing lines from a star trek episode.
haxor2.jpg	04	2005-03-09 13:25:50	24367	84e1dceac2eb127fef 5bfdcb0eae324b	We were not able to open this file despite the file signature being that of a JPG file. We then assume that the file is not sequential in memory (1).
holly.xls	05	2005-03-09 13:25:50	23040	7917baf0219645afef 8b381570c41211	A XLS file containing some statistics.
lin_12.pdf	06	2005-03-09 13:25:50	1399508	e026ec863410725ba 1f5765a1874800d	A PDF file containing a paper about "Prudent Engineering Practice for Cryptographic Protocols".
nlin_14.pdf	07	2005-03-09 13:25:50	122434	5b3e806e8c9c06a47 5cd45bf821af709	A PDF file containing some slides about "Cryptographic Protocol Analysis Via Strand Spaces".
paul.jpg	08	2005-03-09 13:25:50	29885	37a49f97ed279832c d4f7bd002c826a2	A JPG file containing an image of a man with a guitar.
pumpkin.jpg	09	2005-03-09 13:25:50	444314	6c9859e5121ff54d5 d6298f65f0bf3b3	A JPG image containing two cats and a pumpkin.
shark.jpg	10	2005-03-09 13:25:50	99298	d83428b8742a075b 57b0dc424cd297c4	A JPG, containing an image of a shark.
sm1.gif	11	2005-03-09 13:25:50	5498	d25fb845e6a41395a daed8bd14db7bf2	A GIF file containing the words "Graphics" and "Graphics.com".
surf.mov	12	2005-03-09 13:25:50	550653	5328d2b066f428ea9 5b2793849ab97fa	A MOV file containing a video of a man surfing.
surf.wmv	13	2005-03-09 13:25:50	1032914	dad9cb3981cb9880a 8bcc72e42c30f9f	A WMV file containing another video of a man surfing, this time with some background music.
test.ppt	14	2005-03-09 13:25:50	11264	7b74c2c608d92f4bb 76c1d3b6bd1decc	A Microsoft PowerPoint document file containing one slide saying "Test I am a pretty girl".
wword60t.zip	15	2005-03-09 13:25:50	78899	c0be59d49b7ee0fdc 492d2df32f2c6c6	A ZIP file containing the exact same text file we found when we extracted the evidence 02

(1) Despite our efforts (we even tried to use some tools) we were unable to identify the content (nor know the information that was in the middle of the file) regarding the evidence 04. So, we declared it as irrecoverable.

5 Analysis results

The recovered files have no apparent relationship, nor do they seem to be compromising files. As previously stated, it was not possible to recover the contents of evidence 04, which may be a starting point for future investigations. But as the entire file system metadata was destroyed leaving a message to indicate this, we can conclude that someone with some knowledge of the file systems had access to the pen. This can be corroborated by the evidence 01 (a Microsoft Word document), since it was used to hide a text file inside. Although it has a seemingly innocent content.

6 Conclusions

With this investigation it was not possible to conclude anything about the files found in the pen drive. That is, they all appear to be innocent files.

10th November 2017, Instituto Superior Técnico

Luís Aguiar - 80950

Jorge Pereira - 81428

Filipe Azevedo - 82468