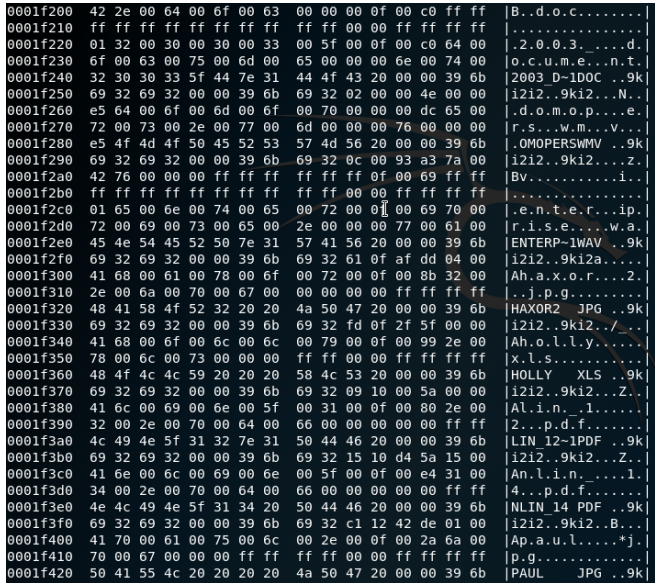


# The Case of the Pen Drive

## Examination Log

Examiners: Luís Aguiar 80950, Jorge Pereira 81428, Filipe Azevedo 82468

Date / Time	Description
06-11-2017, 17h00	Luis, Filipe and Jorge calculated the md5 of the image of the pen, and verified that the file was not changed before it was delivered to them.
17h10	They used a hexadecimal editor to see the content of the pen, in an attempt to find some metadata. But unfortunately, they came across the message: "NO META DATA FOR YOU!!!".
17h15	From there, since the file system of the pen was FAT32, they tried to find the FAT or the root directory or even some others directory entries.
17h20	<p>Using again a hexadecimal editor, they did a manual search. Since what they were looking for would have to be at the beginning of the pen, they searched there first.</p> <p>They managed to find something that looks like some directory entries.</p>  <p>Figure 1 - Interesting things founded</p>
18h00	To find out if these were in fact directory entries, they looked for a file whose extension only appears once – a WAV file – and then they consulted a list of signatures of files online ( <a href="https://goo.gl/Vcg9FT">https://goo.gl/Vcg9FT</a> ). They looked for its signature in the rest of the image of the pen to find where that file actually started. And the signature was found in the position 007D2A00h which meant that this was the beginning of the first cluster of the file. They did the same thing for a GIF file (since it only appears once too) and found that it started at position 00A2D200h and the first cluster of this file was the cluster number 1416h. With this information they were able to find the size of one cluster by doing: $(00A2D200h - 007D2A00h) / (1416h - 0F61h) = 800h = 2048d$ .

18h20	With the information obtained previously, it was then possible to calculate the location of the first cluster, by doing: 00A2D200h – 1416h * 800h or even 007D2A00h - 0F61h * 800h. Since the result was the same, they found it safe to say that the first cluster is in the position 22200h.																											
18h25	<div>With the previously calculated location of the first cluster, the size of each cluster, and the following information about the directory entries:</div> <table><tr><th>Offset</th><th>Length</th><th>Description</th></tr><tr><td>0x00</td><td>8 bytes</td><td>Filename</td></tr><tr><td>0x08</td><td>3 bytes</td><td>Filename extension</td></tr><tr><td>0x0b</td><td>1 byte</td><td>File attributes</td></tr><tr><td>0x0c</td><td>10 bytes</td><td>Reserved</td></tr><tr><td>0x16</td><td>2 bytes</td><td>Time created or last updated</td></tr><tr><td>0x18</td><td>2 bytes</td><td>Date created or last updated</td></tr><tr><td>0x1a</td><td>2 bytes</td><td>Starting cluster number for file</td></tr><tr><td>0x1c</td><td>4 bytes</td><td>File size in bytes</td></tr></table> <div>Figure 2 - Information about the directory entries</div> <div>And assuming the files were written to consecutive clusters, they attempted to extract the files as follows using the <b>dd</b> tool (for example, for the first one in that appears in the figure 1 – a Microsoft Word Document):</div> <div>dd skip=12278272 count=19968 if=usb-image.dd bs=1 &gt; 2003document.doc</div> <div>Where:</div> <div>skip = size of a single cluster * number of the first cluster of the file + position of the first cluster;</div> <div>count = size of the file (obtain from the directory entry).</div>	Offset	Length	Description	0x00	8 bytes	Filename	0x08	3 bytes	Filename extension	0x0b	1 byte	File attributes	0x0c	10 bytes	Reserved	0x16	2 bytes	Time created or last updated	0x18	2 bytes	Date created or last updated	0x1a	2 bytes	Starting cluster number for file	0x1c	4 bytes	File size in bytes
Offset	Length	Description																										
0x00	8 bytes	Filename																										
0x08	3 bytes	Filename extension																										
0x0b	1 byte	File attributes																										
0x0c	10 bytes	Reserved																										
0x16	2 bytes	Time created or last updated																										
0x18	2 bytes	Date created or last updated																										
0x1a	2 bytes	Starting cluster number for file																										
0x1c	4 bytes	File size in bytes																										
18h30	They succeeded and were able to extract the Microsoft Word document. However, they were not able to open it. So, knowing that a Microsoft Word document is just a zip file, they extracted it and managed to find a <i>TXT</i> file that contained a binary format description of Microsoft Word 6.																											
18h40	By performing the calculations explained previously for all the files with directory entries, they were able to retrieve the 15 files (all ids, names, and some description can be founded on the <i>table 1</i> at the end of this file). However, the evidence 04, could not be fully recovered, but its magic number at the beginning and at the end matched the expected. They assumed there was a cluster in the middle that had been rewritten.																											
18h45	They made a bash script, with all the commands (and all calculations already done) needed to collect the 15 files obtained from the pen drive image. The script is in the attached files with a md5 fingerprint of 43e58c735edb4a4ccfd1b8c74e2df9f2.																											
07-11-2017, 16h00	They tried to use the <b>foremost</b> tool and the <b>scalpel</b> tool to try to get full evidence 04, but they were not successful. Although one of the tools revealed more than the 15 alleged files, they were all corrupted and therefore were not considered relevant since they were not found in the directory entries mentioned in Figure 1.																											

-- Table 1 --

Name	Id	Timestamp	Size (bytes)	MD5	Description
<b>2003_document.doc</b>	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.
<b>domopers.wmv</b>	02	2005-03-09 13:25:50	8037267	63c0c6986cf0a446cb 54b0ac65a921a5	A WMV file containing a video of some sort of doll dancing.
<b>enterprise.wav</b>	03	2005-03-09 13:25:50	318895	7629b89adade055f6 783dc1773274215	A WAV file containg lines from a star trek episode.
<b>haxor2.jpg</b>	04	2005-03-09 13:25:50	24367	84e1dceac2eb127fef 5bfdbc0eae324b	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).
<b>holly.xls</b>	05	2005-03-09 13:25:50	23040	7917baf0219645afef 8b381570c41211	A XLS file containing some statistics.
<b>lin_12.pdf</b>	06	2005-03-09 13:25:50	1399508	e026ec863410725ba 1f5765a1874800d	A PDF file containing a paper about "Prudent Engineering Practice for Cryptographic Protocols".
<b>nlin_14.pdf</b>	07	2005-03-09 13:25:50	122434	5b3e806e8c9c06a47 5cd45bf821af709	A PDF file containing some slides about "Cryptographic Protocol Analysis Via Strand Spaces".
<b>paul.jpg</b>	08	2005-03-09 13:25:50	29885	37a49f97ed279832c d4f7bd002c826a2	A JPG file containing an image of a man with a guitar.
<b>pumpkin.jpg</b>	09	2005-03-09 13:25:50	444314	6c9859e5121ff54d5 d6298f65f0bf3b3	A JPG image containing two cats and a pumpkin.
<b>shark.jpg</b>	10	2005-03-09 13:25:50	99298	d83428b8742a075b 57b0dc424cd297c4	A JPG, containing an image of a shark.
<b>sm1.gif</b>	11	2005-03-09 13:25:50	5498	d25fb845e6a41395a daed8bd14db7bf2	A GIF file containing the words "Graphics" and "Graphics.com".
<b>surf.mov</b>	12	2005-03-09 13:25:50	550653	5328d2b066f428ea9 5b2793849ab97fa	A MOV file containing a video of a man surfing.
<b>surf.wmv</b>	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.
<b>test.ppt</b>	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".
<b>wword60t.zip</b>	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