

ZU  
YD

# MICT1 Groep 3

---

## WEEKOPDRACHTEN WEEK 6

### AUTEURS

**Tristan Janssen**

**Chris Kuipers**

**Juul Steins**

**Mick Ubags**

### Zuyd Hogeschool

Faculteit ICT

### OPLEIDING

HBO-ICT

### MODULE

MICT1

## Opdracht

Onderzoek het bestand “file6” en vind het verborgen bericht. Probeer daarnaast bestanden uit de RAM- en/of Disk-slack te vinden.

## Resultaat

De herstelde PNG:



## Methode

Het bestand is onderzocht aan de hand van de online Hex Editor HexEd.it. Het voordeel van deze Hex Editor is dat deze volledig is gebaseerd op HTML5 en JavaScript, en dus platform onafhankelijk werkt.

## Bevindingen

Aan de hand van de beschreven methode zijn onderstaande resultaten gevonden.

### End of Central Directory

Door gebruik te maken van een snelle, handmatige analyse met behulp van een Hex Editor werd er aan het einde van het bestand een PK signature gevonden. Deze trailer duidt mogelijk op een ZIP-bestand.

Gevonden signature: 0x504B0506

Op basis van de ZIP file format specification lijkt dit op de signature van een End of Central Directory record (EOCD). Als er wordt gekeken naar de lengte van de EOCD lijkt dit te kloppen. Op basis hiervan kunnen de volgende veronderstellingen worden gemaakt:

(Offset n=0x000DBF48)

Off-set	Bytes	Beschrijving	Bevinding
n+0	4	End of central directory	
n+4	2	Number of this disk	Disk 0
n+6	2	Disk where central directory starts	Disk 0
n+8	2	Number of central directory records on this disk	1 Central Directory record
n+10	2	Total number of central directory records	1 Central Directory Record
n+12	4	Size of central directory (bytes)	48 bytes groot
n+16	4	Offset of start of central directory, relative to start of archive	Central Directory start op offset 0x000DBF18
n+20	2	Comment length (n)	Geen comment

## Central Directory

Op basis van deze bevindingen kan de Central directory worden geanalyseerd. Deze start op offset 0x000DBF18.

Offset	Bytes	Beschrijving	Bevindingen
0	4	Central directory file header signature = 0x02014b50	
4	2	Version made by	0x033F
6	2	Version needed to extract (minimum)	0x030A
8	2	General purpose bit flag	Null
10	2	Compression method	Geen compressie
12	2	File last modification time	23:30:56 Local
14	2	File last modification date	2016-03-20
16	4	CRC-32	0xE2E04522
20	4	Compressed size	900856 bytes
24	4	Uncompressed size	900856 bytes
28	2	File name length (n)	2 tekens
30	2	Extra field length (m)	Null
32	2	File comment length (k)	Null
34	2	Disk number where file starts	Disk 0
36	2	Internal file attributes	Null
38	4	External file attributes	0x81B48020

Offset	Bytes	Beschrijving	Bevindingen
42	4	Relative offset of local file header. This is the number of bytes between the start of the first disk on which the file occurs, and the start of the local file header. This allows software reading the central directory to locate the position of the file inside the .ZIP file.	Null (Dus aan het begin)
46	n	File name	Bestandsnaam: x2

Hieruit valt o.a. te concluderen dat dhr. Van den Bos een late werker is, het bestand is op 20 maart om half 12 's avonds voor het laatst aangepast.

000DBF00	5C 7E 62 A8 A5 9F C4 CB	D7 64 6A 62 AC 91 76 FF	\~bzÑf_Tdjbæv
000DBF10	C4 C4 3D 7B 00 40 07 00	50 4B 01 02 3F 03 0A 03	—={.@..PK..?...
000DBF20	00 00 00 00 DC BB 74 48	22 45 E0 E2 F8 BE 0D 00	...tH"EæT°J...
000DBF30	F8 BE 0D 00 02 00 00 00	00 00 00 00 00 00 20 80	°J.....C
000DBF40	B4 81 00 00 00 00 78 32	50 4B 05 06 00 00 00 00	ü....x2PK....
000DBF50	01 00 01 00 30 00 00 00	18 BF 0D 00 00 00 +	....0.....

## ZIP-file Header

Vervolgens is de header van de ZIP-file onder de loep genomen. Hier zou de Header signature 0x04034B50 verwacht worden. Echter ziet de signature van file6 ziet er anders uit:

0x0403B4AF

De aanname wordt gemaakt dat de Header van file6 mogelijk corrupt is. Hierbij wordt de signature aangepast naar de signature van een ZIP-file: 0x04034B50.

Vervolgens blijkt de CRC-32 checksum in de header af te wijken van de checksum in de footer.

Header	Footer
0x1D1FBADD	0xE2E04522

De checksum op offset 0xE is vervangen door 0xE2E04522 waarna de ZIP-file kon worden uitgepakt.

## Bestand x2

Het eerste dat opvalt bij de analyse van het bestand x2 is dat de header doet vermoeden dat het een corrupt rar bestand betreft, de header start met 0xAD617221 in Ascii: .ar! (lijkt op Rar!)

Als het magic number van x2 wordt vergeleken met het magic number uit de RAR File Format Specification dan verschilt alleen de eerste byte:

x2 bestand	File Format
0xAD6172211A0700	0x526172211A0700

Ook hier wordt de header van het RAR bestand geanalyseerd, zoals weergegeven in onderstaande tabellen.

### Archive Header

Veldnaam	Bytes	Beschrijving	Bevindingen
<b>HEAD_CRC</b>	2	CRC of fields HEAD_TYPE to RESER-VED2	0xCF90
<b>HEAD_TYPE</b>	1	Header Type: 0x73	0x73
<b>HEAD_FLAGS</b>	2	Bit Flags (Please see 'Bit Flags for MAIN_HEAD' table for all possibilities).	Null
<b>HEAD_SIZE</b>	2	Archive header total size including archive comments	13 bytes
<b>Reserved 1+2</b>	6	Onbekend	Null

### File Header

Veldnaam	Bytes	Beschrijving	Bevindingen
<b>HEAD_CRC</b>	2	CRC of fields from HEAD_TYPE to FILEATTR and file name	0xF580
<b>HEAD_TYPE</b>	1	Header Type: 0x74	0x74
<b>HEAD_FLAGS</b>	2	Bit Flags (Please see 'Bit Flags for File in Archive' table for all possibilities)	0x8090
<b>HEAD_SIZE</b>	2	File header full size including file name and comments	35 bytes
<b>PACK_SIZE</b>	4	Compressed file size	900794 bytes
<b>UNP_SIZE</b>	4	Uncompressed file size	898232 bytes
<b>HOST_OS</b>	1	Operating system used for archiving (See the 'Operating System Indicators' table for the flags used)	UNIX
<b>FILE_CRC</b>	4	File CRC	0x5D11CD92
<b>FTIME</b>	4	Date and time in standard MS DOS format	2016-03-20 23:21:40 Local
<b>UNP_VER</b>	1	RAR version needed to extract file (Version number is	Version 2.9

		encoded as 10 * Major version + minor version.)	
<b>METHOD</b>	1	Packing method (Please see 'Packing Method' table for all possibilities)	Normale compressie
<b>NAME_SIZE</b>	2	File name size	1 byte
<b>ATTR</b>	4	File attributes	0xB4810000
<b>HIGH_PACK_SIZE</b>	4	High 4 bytes of 64-bit value of compressed file size. Optional value, presents only if bit 0x100 in HEAD_FLAGS is set.	N.v.t.
<b>HIGH_UNP_SIZE</b>	4	High 4 bytes of 64-bit value of uncompressed file size. Optional value, presents only if bit 0x100 in HEAD_FLAGS is set.	N.v.t.
<b>FILE_NAME</b>	NAME_SIZE bytes	File name - string of NAME_SIZE bytes size	1 byte: x
<b>SALT</b>	8	present if (HEAD_FLAGS & 0x400) != 0	N.v.t.
<b>EXT_TIME</b>	variable size	present if (HEAD_FLAGS & 0x1000) != 0	N.v.t.

De RAR file kon succesvol worden uitgepakt, dit uitgepakte bestand is vervolgens weer in de Hex Editor geopend.

### Bestand x

Tijdens de initiële analyse van het bestand x heeft de structuur veel weg van een PNG afbeelding. Echter zijn een aantal “sleutelwoorden” niet in de juiste samenstelling:

<b>PNG Standaard</b>	<b>Bestand x</b>
IHRD	HIRD
tIME	ItEM
pHYs	p YH s
bKGD	b GK D

Het lijkt erop alsof het PNG bestand Middle Endian geencodeerd is. Om het bestand van Middle Endian om te schrijven naar Big Endian wordt er gebruik gemaakt van Unix dd:

```
dd conv=swab if=mict1/x of=mict1/x_swapped
```

```
christian@doritos: ~
x
christian@doritos:~$ mkdir mict1
christian@doritos:~$ mv x mict1/
'x' -> 'mict1/x'
christian@doritos:~$ dd conv=swab if=mict1/x of=mict1/x_swapped
1754+1 records in
1754+1 records out
898232 bytes (898 kB) copied, 0.00864827 s, 104 MB/s
christian@doritos:~$
```

Dit levert het volgende resultaat.

Voor:

00000000	AF 76 B8 B1 0A 0D 0A 1A   00 00 00 0D 00	48 49 52 44	>>v...HIRD
00000010	00 00 0F 04 00 00 73 02   06 08 00 00 60 00 3A 70		....s....`p
00000020	00 5B 00 00 62 06 47 4B   00 44 00 FF 00 FF A0 FF		[..b.GK.D. . á
00000030	A7 BD 00 93 00 00 70 09   59 48 00 73 0B 00 00 13		„.ô..p.YH.s....
00000040	0B 00 01 13 9A 00 18 9C   00 00 07 00 49 74 45 4D		....Ü...£....ItEM

Na:

00000000	76 AF B1 B8 0D 0A 1A 0A   00 00 00 0D 49 48 44 52	v...IHDR
00000010	00 00 04 0F 00 00 02 73   08 06 00 00 60 70 3A	....s....`p:
00000020	5B 00 00 00 06 62 4B 47   44 00 FF 00 FF 00 FF A0	[...bKGD. . á
00000030	BD A7 93 00 00 00 09 70   48 59 73 00 00 0B 13 00	„.ô...pHYs....
00000040	00 0B 13 01 00 9A 9C 18   00 00 00 07 74 49 4D 45	....Ü£....tIME

Het enige dat nu nog rest is de PNG header herstellen: de eerste vier bytes moeten worden geflipped:

Voor	Na
0x76 AF B1 B8	0x89 50 4E 47 0D

Nu is de PNG met een normale Image Viewer te openen. In de afbeelding staat ook het verborgen bericht: "It's true. All of it."

## Bronnen

Bron	URL
Zuyd Repository op GitHub	<a href="https://github.com/ZuydUniversity/MICT1">https://github.com/ZuydUniversity/MICT1</a>
Online Hex Editor	<a href="https://hexed.it">https://hexed.it</a>
Wikipedia ZIP File Format Specification	<a href="https://en.wikipedia.org/wiki/Zip_%28file_format%29">https://en.wikipedia.org/wiki/Zip_%28file_format%29</a>
ForensicWiki RAR File Format Specification	<a href="http://www.forensicswiki.org/wiki/RAR">http://www.forensicswiki.org/wiki/RAR</a>
World Wide Web Consortium PNG File Format Specification	<a href="https://www.w3.org/TR/PNG/">https://www.w3.org/TR/PNG/</a>