Week 6

MICT 1

Groep: Disco Ninja’s

Robin Chel 1241141

Jeroen van den Hurk 1071149

Luc Janssens 1070649

Kevin de Waal 1072153

## What we found

Onderstaande afbeelding hebben wij gevonden uit het bestand x.



“It’s true. All of it”

## Where we found it

De PNG was verstopt een file structuur. Het eerste bestand was een zip file met een kapotte header. Toen kwam het volgende bestand eruit wat een rar bestand was. Hierna kwam een bestand eruit wat een PNG was ( met wat aanpassingen welke besproken worden in “How we found it”).

File6 -> x2 -> x -> PNG

## How we found it

### File6

Dit is het originele bestand. Wij hebben het bekeken en getest op verschillende bekende bestandsformaten. Bulk extractor heeft een rar bestand gevonden in het bestand. Bestand nogmaals bekeken en toen op known compressie bestanden gekeken op ZIP en RAR bestanden.

Via de volgende website: <http://www.fileformat.info/format/zip/corion.htm>

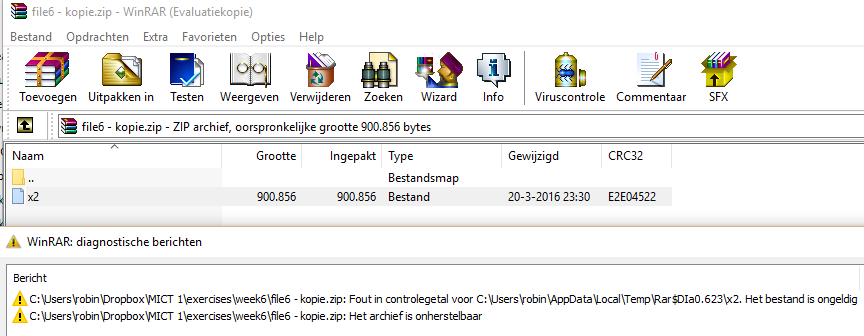
Een Zip bestand moet eindeigen met PK 05 06 in BIN waarde = 50 4b 05 06.

Op het einde van het bestand staat op locatie (regel) 000DBF48 de bovengenoemde bin waarde.

Op deze manier zijn we er achtergekomen dat het om een zip bestand gaat. Alleen de header ( het begin ) komt niet overeen.

Volgens de website: <http://www.fileformat.info/format/zip/corion.htm> moet een Zip bestand beginnen met PK 03 04. Als gekeken wordt naar het begin van het bestand staat echter AF B4 03 04.

Dit hebben we veranderd in 50 4b. File6 opgeslagen als zip bestand en proberen te openen.



We kunnen zien dat er een bestand inzit wat x2 heet alleen we kunnen het bestand nog niet uitpakken. Hier hebben behoorlijk om lopen vloeken want we konden het probleem niet vinden. Op het eind van de zip file staat ook wat informatie over het bestand. Toen zijn we tot de conclusie gekomen dat de CRC Header niet overeenkomt. Onderaan het bestand file6 staat op locatie 000DBF28 -> 22 45 E0 E2. Boven in het bestand staat DD BA 1F 1D. Toen we deze waarde aangepast hadden naar 22 45 E0 E2 konden we het bestand x2 uit de zip halen.

### X2

Het bestand x2 hebben we vernoemnd naar x2.img en toen Bulkextractor laten lopen. Hier is uitgekomen dat het een rar bestand moet zijn.

*# BANNER FILE NOT PROVIDED (-b option)*

*# BULK\_EXTRACTOR-Version: 1.5.1 ($Rev: 10844 $)*

*# Feature-Recorder: rar*

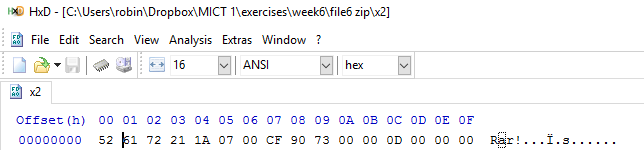
*# Filename: C:\Users\robin\Dropbox\MICT 1\exercises\week6\file6 zip\x2.img*

*# Feature-File-Version: 1.1*

*20 x <rar\_component><name>x</name><flags>0x0000</flags><version>29</version><compression\_method>normal</compression\_method><uncompr\_size>898232</uncompr\_size><compr\_size>900794</compr\_size><file\_attr>0x81B4</file\_attr><lastmoddate>2016-03-20T23:21:40Z</lastmoddate><host\_os>Unix</host\_os><crc32>0x92CD115D</crc32></rar\_component>*

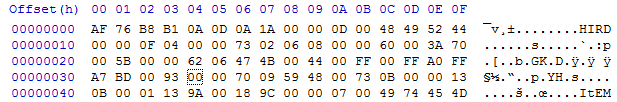
We hebben gekeken naar de Header van een rar formaat op deze website : <http://www.forensicswiki.org/wiki/RAR>

Dan komen we tot de conclusie dat de header(AD 61 72 21 1A 07 00 ) niet overeenkomt de header van een rar formaat. Dit moet 0x 52 61 72 21 1A 07 00 zijn.

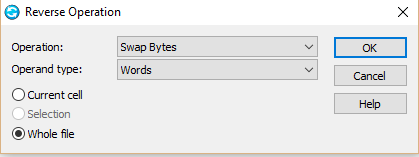


Het bestand kan worden uitgepakt. Hier uit komt het bestand x.

### X

Wanneer bestand x bekeken wordt in de hex editor komen we tot de conclusie dat het bestand waarschijnlijk een PNG bestand is. Dit baseren wij op de headers die in het bestand staan. Echter zijn de bits verwisseld. 

HIRD moet zijn IHDR, p YH s moet zijn pHYs en ItEM moet zijn tIME. De bits lijken verwisseld te zijn. Op deze manier kan het bestand echter niet geopened worden. Gelukkig heeft NEO hex editor de mogelijk om de bytes te swappen.



Nu de bytes weer op de goede volgorde staan, moet alleen de header van de PNG nog aangepast worden. De waarde wordt 89 50 4E 47 0D volgens <https://en.wikipedia.org/wiki/Portable_Network_Graphics>

Wanneer het bestand is opgeslagen als PNG kunnen we deze openen.

