2016

MICT1 – Exercise Week 2

MICT1 – Group 1

Zuyd University

23-Feb-16

MICT1 – Exercise Week 2

Reverse Engineering Data – Exercise week 2

Group	Group 1	
Students	Delano Cörvers	(1306669)
	Davy Heutmekers	(1309730)
	Rik Kierkels	(1354442)
Module	MICT1 – Reverse Engineering Data	
Assignment	Exercise – Week 2	
School year	2015 – 2016	

Table of content

1 What we found

In the first file (PNG) we found the hint which we used to get the question from the second file.

The hint used the keyword 'MICT1Hint' with the content 'Het bericht in de andere file moet via ROT13 worden gedecodeerd. Succes!'. The keyword and content are separated by a one byte null character.

The question in the second file was encoded in ROT13. The keyword for the question is Zuyd and the converted string is 'Uit welk jaar is de film waarin de scene uit deze animatie voorkomt?'. The original ROT13 string is 'Hvg jryx wnne vf qr svyz jnneva qr fprar hvg qrmr navzngvr ibbexbzg?'.

2 Where we found it

First file: the hint

001c15f9 → 001c1640 using Hex Editor Neo

Second file

82840 → using Notepad++

3 How we found it

First file

In chapter 11.3.4.3 tEXt – Textual Data in the PNG Specification (https://www.w3.org/TR/PNG/) we found the information we needed for the text blocks.

The identifier of a text field is noted in decimals → 116 69 88 116. We converted these decimals to hexadecimals (74 45 58 74) and searched for them in the file using the Hex Editor Neo. The text field was found once in the file.

Second file

We installed the TextFX plugin for Notepad++, which has the functionality to convert text to ROT13 text and vice versa. We converted the entire file to ROT13, which would convert the actual ROT13 question to normal text. (ROT13 moves each alphabetical character up 13 places, which means that doing the conversion twice moves each character up 13 times resulting back into the normal alphabetical set).

We knew that there was a question in the file, so we searched for keywords that are commonly used in questions ('how', 'where', 'when', etc.). We found the question when we searched for the Dutch word 'waar'. The keyword (Zuyd) was normal text, the question ROT13.

We weren't sure our method for the second file was correct, as it was based on a lucky guess. We presumed there was an actual method to solve this problem. We asked T. Slot (22-Feb-16) to help us figure out the correct method. He confirmed that our method was valid, because we knew beforehand it was a question, so it makes sense to search for commonly used keywords in questions.

4 The answer to the question

Uit welk jaar is de film waarin de scene uit deze animatie voorkomt?

➔ 2015 (Star Wars: Episode VII - The Force Awakens)