Week 4

MICT 1

Groep: Disco Ninja’s

Robin Chel 1241141

Jeroen van den Hurk 1071149

Luc Janssens 1070649

Kevin de Waal 1072153

## What we found

In het bestand van week 4 hebben wij 2 afbeeldingen gevonden. Een grote afbeelding en een thumbnail daarvan.



Figuur 1 - Afbeelding

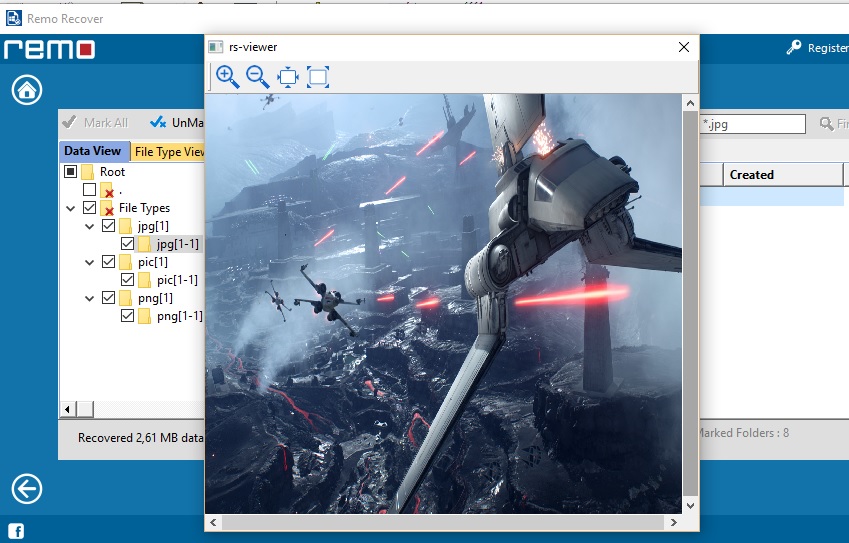


Figuur 2 - Thumbnail afbeelding

## Where we found it & How we found it

Met een programma genaamd Bulk Extractor : <http://www.forensicswiki.org/wiki/Bulk_extractor> zijn wij erachter gekomen dat er een afbeelding .

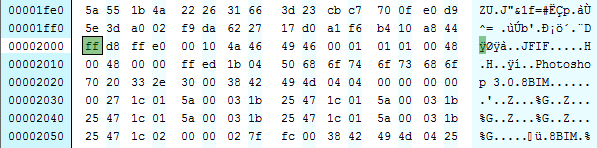
Met behulp van Remo Recover konden wij zien welke afbeelding er aanwezig was in het bestand. Echter moesten we betalen voor de volledige versie om deze te herstellen.



Figuur 3 - Remo Recover

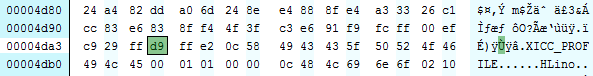
In Remo konden wij zien dat het een JPG betreft. Voordat wij verder zijn gegaan hebben wij ons eerst verdiept in het JPG bestandformaat, met bijbehorende specs. Wij hebben de volgende website daar voor gebruikt <https://en.wikipedia.org/wiki/JPEG>. Hieruit blijkt dat een JPG start met de hex waarde “FF D8”. Deze waarde hebben wij gezocht en gevonden in het bestand. Zie onderstaande afbeelding.

De offset is 00002000. Echter blijkt dat een een JFIF is en geen JPG. Na ons verdiept te hebben in het JFIF formaat komen we tot de conclusie dat dit nagenoeg het zelfde is als een JPG, alleen meer compressie. <https://en.wikipedia.org/wiki/JPEG_File_Interchange_Format>



Figuur 4 - JFIF

De JFIF moet eindigen met de hex waarde: “FF D9”, deze hebben wij ook gevonden zoals te zien is in Figuur 5 - JFIF einde.



Figuur - JFIF einde

De code die hiertussen staat hebben wij eruit gehaald en opgeslagen als een .JFIF bestand. Hier kwam een thumbnail uit. Niet de grote afbeelding zoals wij die eerder hadden gezien bij Remo. Hierop zijn we verder gaan zoeken en hebben nog een afsluiter gevonden op offset 0009FF10.

De code van offset 00002000 tot offset 0009FF10 heeft het grote JFIF bestand opgeleverd. De thumbnail zat in dit bestand.

Bij de bovengenoemde offset stond ook een header van een GIF file, deze was echter corrupt omdat er geen einde stond.

Verder hebben wij nog een PNG header gevonden op offset 000A0000 maar deze was leeg.

# BANNER FILE NOT PROVIDED (-b option)

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

# Feature-Recorder: exif

# Filename: C:\Users\robin\Dropbox\MICT 1\exercises\week4\data - kopie.img

# Feature-File-Version: 1.1

8192 bfc999bf38cd391c77e432ac6f31acf6 <exif><ifd0.tiff.Orientation>1</ifd0.tiff.Orientation><ifd0.tiff.XResolution>72/1</ifd0.tiff.XResolution><ifd0.tiff.YResolution>72/1</ifd0.tiff.YResolution><ifd0.tiff.ResolutionUnit>2</ifd0.tiff.ResolutionUnit><ifd0.tiff.Software>Adobe Photoshop CC 2014 (Macintosh)</ifd0.tiff.Software><ifd0.tiff.DateTime>2016:01:13 12:07:13</ifd0.tiff.DateTime><ifd0.exif.ColorSpace>1</ifd0.exif.ColorSpace><ifd0.exif.PixelXDimension>1920</ifd0.exif.PixelXDimension><ifd0.exif.PixelYDimension>1080</ifd0.exif.PixelYDimension><ifd1.tiff.Compression>6</ifd1.tiff.Compression><ifd1.tiff.XResolution>72/1</ifd1.tiff.XResolution><ifd1.tiff.YResolution>72/1</ifd1.tiff.YResolution><ifd1.tiff.ResolutionUnit>2</ifd1.tiff.ResolutionUnit><ifd1.tiff.JPEGInterchangeFormat>310</ifd1.tiff.JPEGInterchangeFormat><ifd1.tiff.JPEGInterchangeFormatLength>4426</ifd1.tiff.JPEGInterchangeFormatLength></exif>