Week 4

MICT 1

Groep: Disco Ninja’s

Robin Chel 1241141

Jeroen van den Hurk 1071149

Luc Janssens 1070649

Kevin de Waal 1072153

Met een snelle scan door de data file hebben wij geconstateerd dat er een foto file in stond.

Deze hebben we proberen te recoveren met Remo recover. Helaas moest je de software kopen om hem er uit te krijgen maar de asoftware vertelde ons dat het een jfif file was.   
Hierna hebben we de specs van jfif opgezocht en zelf het plaatje uit de data gehaald.

Deze data begint op 00002000 met de hex waarde FF D8 en eindigt op 0009FF10 met FF D9



Zoals je ziet is er zowel het origineel en de thumbnail aanwezig in de data.

Verder hebben we met Bulk Extractor (http://www.forensicswiki.org/wiki/Bulk\_extractor) wat url’s gevonden in de data.

# BANNER FILE NOT PROVIDED (-b option)

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

# Feature-Recorder: domain

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

# Feature-File-Version: 1.1

20513 www.iec.ch \x00\x00\x00\x00\x16IEC http://www.iec.ch\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x16IEC

20546 www.iec.ch \x00\x00\x00\x00\x16IEC http://www.iec.ch\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00

23049 ns.adobe.com \xDC\xFFm\xFF\xFF\xFF\xE1\x126http://ns.adobe.com/xap/1.0/\x00<?xpac

23262 www.w3.org lns:rdf="http://www.w3.org/1999/02/22-rdf-

23349 ns.adobe.com lns:xmp="http://ns.adobe.com/xap/1.0/" xmlns

23389 purl.org mlns:dc="http://purl.org/dc/elements/1.1

23440 ns.adobe.com otoshop="http://ns.adobe.com/photoshop/1.0/"

23489 ns.adobe.com s:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xm

23535 ns.adobe.com s:stEvt="http://ns.adobe.com/xap/1.0/sType/R

23598 ns.adobe.com s:stRef="http://ns.adobe.com/xap/1.0/sType/R

# BANNER FILE NOT PROVIDED (-b option)

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

# Feature-Recorder: domain

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

# Histogram-File-Version: 1.1

n=6 ns.adobe.com

n=2 www.iec.ch

n=1 purl.org

n=1 www.w3.org

# 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>

# BANNER FILE NOT PROVIDED (-b option)

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

# Feature-Recorder: url

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

# Feature-File-Version: 1.1

20506 http://www.iec.ch desc\x00\x00\x00\x00\x00\x00\x00\x16IEC http://www.iec.ch\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x16IEC

20539 http://www.iec.ch \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x16IEC http://www.iec.ch\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00

23042 http://ns.adobe.com/xap/1.0/ \xFD)\xFD\xBA\xFEK\xFE\xDC\xFFm\xFF\xFF\xFF\xE1\x126http://ns.adobe.com/xap/1.0/\x00<?xpacket begin

23255 http://www.w3.org/1999/02/22-rdf-syntax-ns# :RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Descript

23342 http://ns.adobe.com/xap/1.0/ t="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:dc="http

23382 http://purl.org/dc/elements/1.1/ 1.0/" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:photosho

23433 http://ns.adobe.com/photoshop/1.0/ mlns:photoshop="http://ns.adobe.com/photoshop/1.0/" xmlns:xmpMM="h

23482 http://ns.adobe.com/xap/1.0/mm/ /" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stEvt="h

23528 http://ns.adobe.com/xap/1.0/sType/ResourceEvent# /" xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#" xmlns:stRef="h

23591 http://ns.adobe.com/xap/1.0/sType/ResourceRef# #" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorToo

# BANNER FILE NOT PROVIDED (-b option)

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

# Feature-Recorder: url

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

# Histogram-File-Version: 1.1

n=2 http://ns.adobe.com/xap/1.0/

n=2 http://www.iec.ch

n=1 http://ns.adobe.com/photoshop/1.0/

n=1 http://ns.adobe.com/xap/1.0/mm/

n=1 http://ns.adobe.com/xap/1.0/sType/ResourceEvent#

n=1 http://ns.adobe.com/xap/1.0/sType/ResourceRef#

n=1 http://purl.org/dc/elements/1.1/

n=1 http://www.w3.org/1999/02/22-rdf-syntax-ns#

# BANNER FILE NOT PROVIDED (-b option)

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

# Feature-Recorder: url

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

# Histogram-File-Version: 1.1

n=6 ns.adobe.com

n=2 www.iec.ch

n=1 purl.org

n=1 www.w3.org