



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Computer Forensics (ACCD5000)

Warmup Activity

Task 1: Individual Activity – Analysis of Data from the acquired Image

When opening the link, we are redirected on a one drive with few documents such as:

- ransom-letter.docx a word document
- ransom-letter.pdf a pdf document
- the tutorial document
- letter-image.jpg an image

This is all about a ransom demand for Gato a cute little cat.

1) Analyse of the documents:

When analysing a ransom demand in a pdf we need first to analyse the content and ask what the threats and the demand are; in this case we need to give a certain amount. They are asking for XMR 3.14159 in Monero in cryptocurrency, it is a mix between XMR, the symbol for Monero, a privacy-focused cryptocurrency and the first few digits of the mathematical constant pi. It is either that or Bitcoins, BTC 0.0165, as of today, here are a possibility of conversation: 0.0165 BTC is approximately £560.04.

Another important thing to do is get the metadata of the picture below. I did download Exiftool for that. When downloading it you must extract to unzip the file. Then you download the picture in the file called letter-image.jpg and put it in Exiftool. Then a console opens with all the information, the metadata of the image. We obtain this:

```
C:\Users\Administrateur\Downloads\exiftool-12.76 (1)\exiftool(-k).exe
Exiftool Version Number : 12.76
File Name : letter-image.jpg
Directory : C:\Users\Administrateur\Downloads\exiftool-12.76 (1)
File Size : 127 kB
Zone Identifier : Exif
File Modification Date/Time : 2024:02:04 21:37:39+00:00
File Access Date/Time : 2024:02:04 21:38:36+00:00
File Creation Date/Time : 2024:02:04 21:37:37+00:00
File Permissions : -rw-rw-rw-
File Type : JPEG
File Type Extension : jpg
MIME Type : image/jpeg
JFIF Version : 1.01
Exif Byte Order : little-endian (Intel, II)
Compression : JPEG (old-style)
Make : Canon
Camera Model Name : Canon EOS R6
Orientation : Horizontal (normal)
X Resolution : 300
Y Resolution : 300
Resolution Unit : inches
Software : GIMP 2.10.28
Modify Date : 2022:02:15 17:23:40
Exposure Time : 1/200
F Number : 2.8
Exposure Program : Manual
ISO : 640
Sensitivity Type : Recommended Exposure Index
Recommended Exposure Index : 640
Exif Version : 0231
Date/Time Original : 2022:02:25 13:37:33
Create Date : 2022:02:25 13:37:33
Offset Time : +01:00
Offset Time Original : +03:00
Offset Time Digitized : +03:00
Shutter Speed Value : 1/200
Aperture Value : 2.8
Exposure Compensation : 0
Max Aperture Value : 1.8
Metering Mode : Multi-segment
Flash : No Flash
Focal Length : 50.0 mm
User Comment : THM{238956}
Sub Sec Time Original : 42
```

```
C:\Users\Administrateur\Downloads\exiftool-12.76 (1)\exiftool(-k).exe
Chromaticity Colorant : Unknown
Chromaticity Channel 1 : 0.64 0.33002
Chromaticity Channel 2 : 0.3 0.60001
Chromaticity Channel 3 : 0.15001 0.06
Device Mfg Desc : GIMP
Device Model Desc : sRGB
Current IPIC Digest : b417d6571f8aba97a1e64afbdedafbdb
Coded Character Set : UTF8
Envelope Record Version : 4
Date Created : 2022:02:15
Digital Creation Date : 2021:11:05
Digital Creation Time : 14:06:13+03:00
Application Record Version : 4
Time Created : 17:23:40-17:23
Image Width : 1200
Image Height : 800
Encoding Process : Progressive DCT, Huffman coding
Bits Per Sample : 8
Color Components : 3
Y Cb Cr Sub Sampling : YCbCr4:4:4 (1 1)
Aperture : 2.8
Image Size : 1200x800
Megapixels : 0.960
Scale Factor To 35 mm Equivalent : 0.7
Shutter Speed : 1/200
Create Date : 2022:02:25 13:37:33.42+03:00
Date/Time Original : 2022:02:25 13:37:33.42+03:00
Modify Date : 2022:02:15 17:23:40+01:00
Thumbnail Image : (Binary data 4941 bytes, use -b option to extract)
GPS Latitude : 51 deg 30' 51.90" N
GPS Longitude : 0 deg 5' 38.73" W
Date/Time Created : 2022:02:15 17:23:40-17:23
Digital Creation Date/Time : 2021:11:05 14:06:13+03:00
Circle Of Confusion : 0.043 mm
Depth Of Field : 0.06 m (0.76 - 0.82 m)
Field Of View : 54.9 deg
Focal Length : 50.0 mm (35 mm equivalent: 34.6 mm)
GPS Position : 51 deg 30' 51.90" N, 0 deg 5' 38.73" W
Hyperfocal Distance : 20.58 m
Light Value : 7.9
Lens ID : Canon EF 50mm f/1.8 STM
-- press ENTER --
```

Relevant information of the metadata of the letter-image.jpg for this case:

1. Camera Settings:

Model used: Canon EOS R6

2. Date and Time:

2022:02:25 13:37:33

3. Geolocation:

GPS Latitude: 51 deg 30' 51.90" N

GPS Longitude : 0 deg 5' 38.73" W

GPS position : 51 deg 30' 51.90" N, 0 deg 5' 38.73" W

The coordinates lead to this place in London:

