Intro to Digital Forensics

Learn about digital forensics and related processes and experiment with a practical example

Task 1 Introduction To Digital Forensics

Question	Answer
Consider the desk in the photo above. In addition to the smartphone, camera, and SD cards, what would be interesting for digital forensics?	laptop

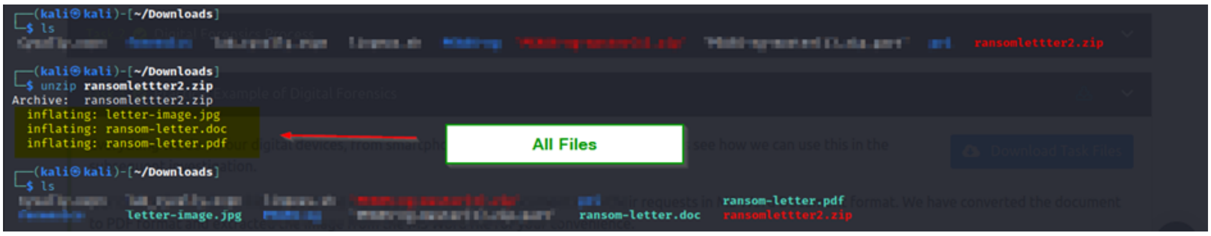
Task 2 Digital Forensics Process

Question	Answer
It is essential to keep track of who is handling it at any point in time to ensure that evidence is admissible in the court of law. What is the name of the documentation that would help establish that?	Chain of Custody

Task 3 Practical Example of Digital Forensics

- ➔ I downloaded the task file to my local machine by clicking the "Download Task File" button.
- ➔ After downloading the task file, I proceeded to unzip it.

Command: unzip ransomlettter2.zip

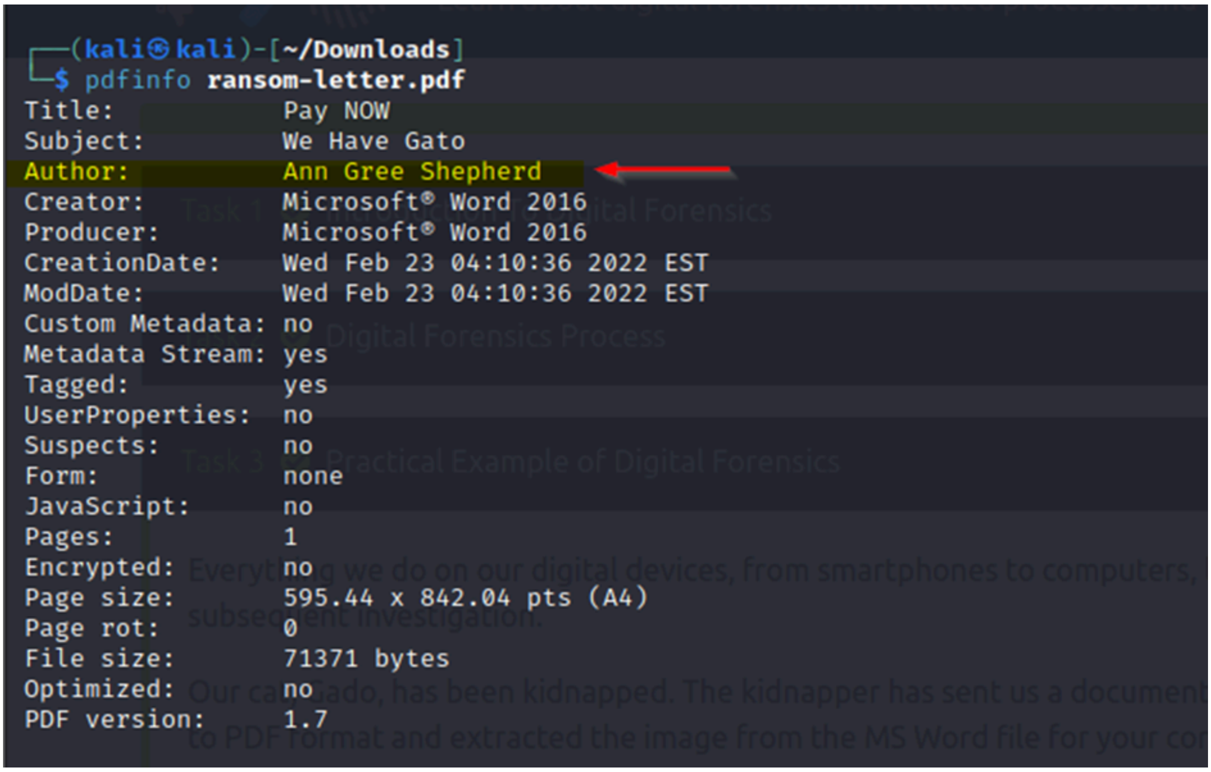


```
┌──(kali㉿kali)-[~/Downloads]
└─$ ls
[redacted]  ransomlettter2.zip

┌──(kali㉿kali)-[~/Downloads]
└─$ unzip ransomlettter2.zip
Archive:  ransomlettter2.zip
  inflating: letter-image.jpg
  inflating: ransom-letter.doc
  inflating: ransom-letter.pdf

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
[redacted]  ransom-letter.pdf
[redacted]  letter-image.jpg  [redacted]  ransom-letter.doc  ransomlettter2.zip
```

- ➔ To determine the author of the attached PDF file "ransom-letter.pdf," I used the pdfinfo tool..

- ➔ The pdfinfo tool helps us to read the metadata of a pdf file

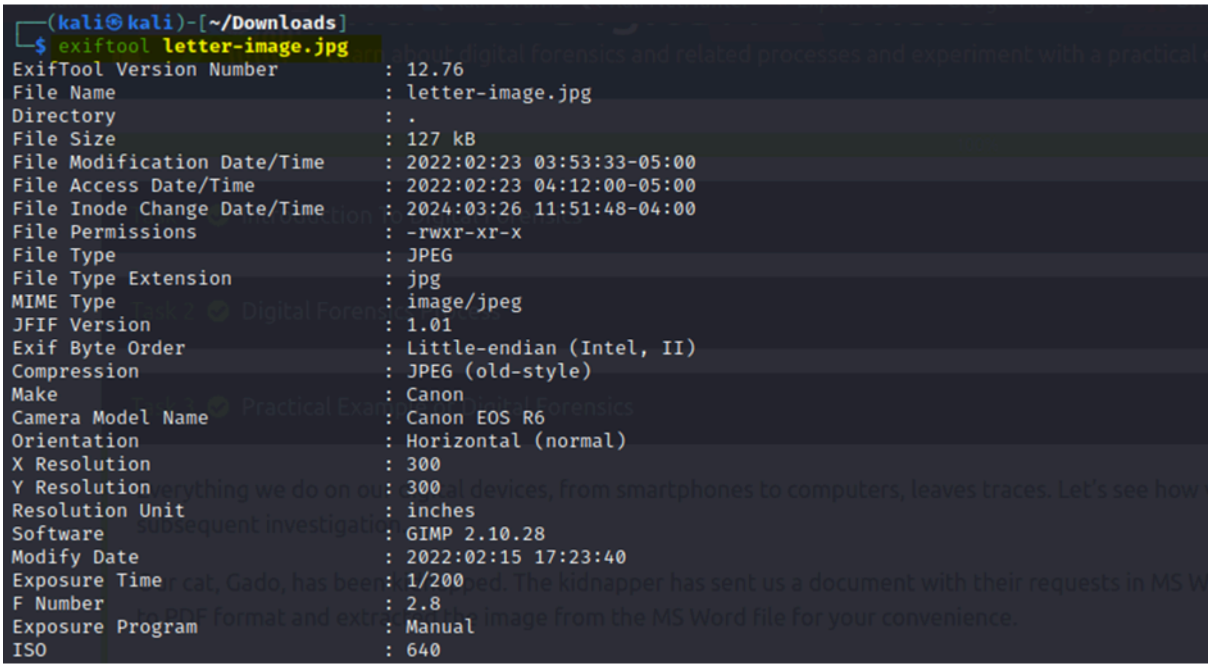
Command: **pdfinfo ransom-letter.pdf**
Answer: **Ann Gree Shepherd**



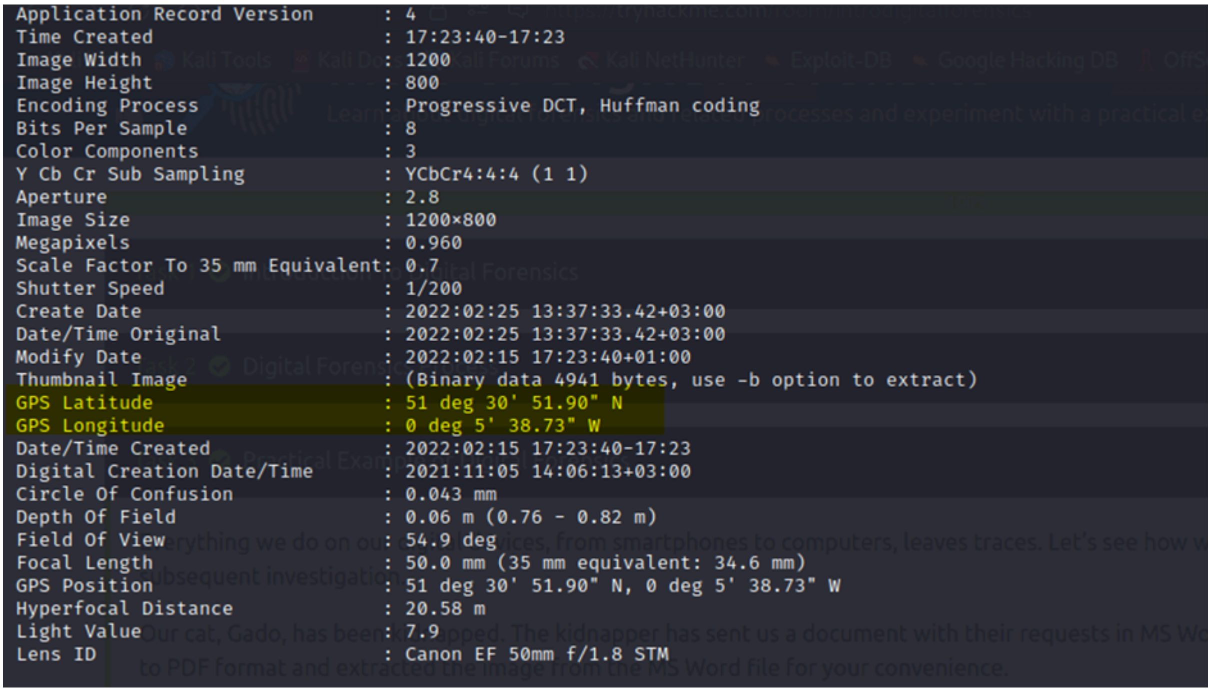
```
┌──(kali㉿kali)-[~/Downloads]
└─$ pdfinfo ransom-letter.pdf
Title:          Pay NOW
Subject:        We Have Gato
Author:         Ann Gree Shepherd
Creator:        Microsoft® Word 2016
Producer:       Microsoft® Word 2016
CreationDate:   Wed Feb 23 04:10:36 2022 EST
ModDate:        Wed Feb 23 04:10:36 2022 EST
Custom Metadata: no
Metadata Stream: yes
Tagged:         yes
UserProperties: no
Suspects:       no
Form:           none
JavaScript:     no
Pages:          1
Encrypted:      no
Page size:      595.44 x 842.04 pts (A4)
Page rot:       0
File size:      71371 bytes
Optimized:      no
PDF version:    1.7
```

- ➔ To identify the location where the kidnappers captured the image attached to their document, I used exiftool to extract the GPS coordinates and google map to reveal the location by street name.
- ➔ The exiftool reads the EXIF data from images
- ➔ EXIF means Exchangeable Image File Format

Command: **exiftool letter-image.jpg**



```
┌──(kali㉿kali)-[~/Downloads]
└─$ exiftool letter-image.jpg
ExifTool Version Number         : 12.76
File Name                       : letter-image.jpg
Directory                       : .
File Size                       : 127 kB
File Modification Date/Time     : 2022:02:23 03:53:33-05:00
File Access Date/Time           : 2022:02:23 04:12:00-05:00
File Inode Change Date/Time     : 2024:03:26 11:51:48-04:00
File Permissions                : -rwxr-xr-x
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
```



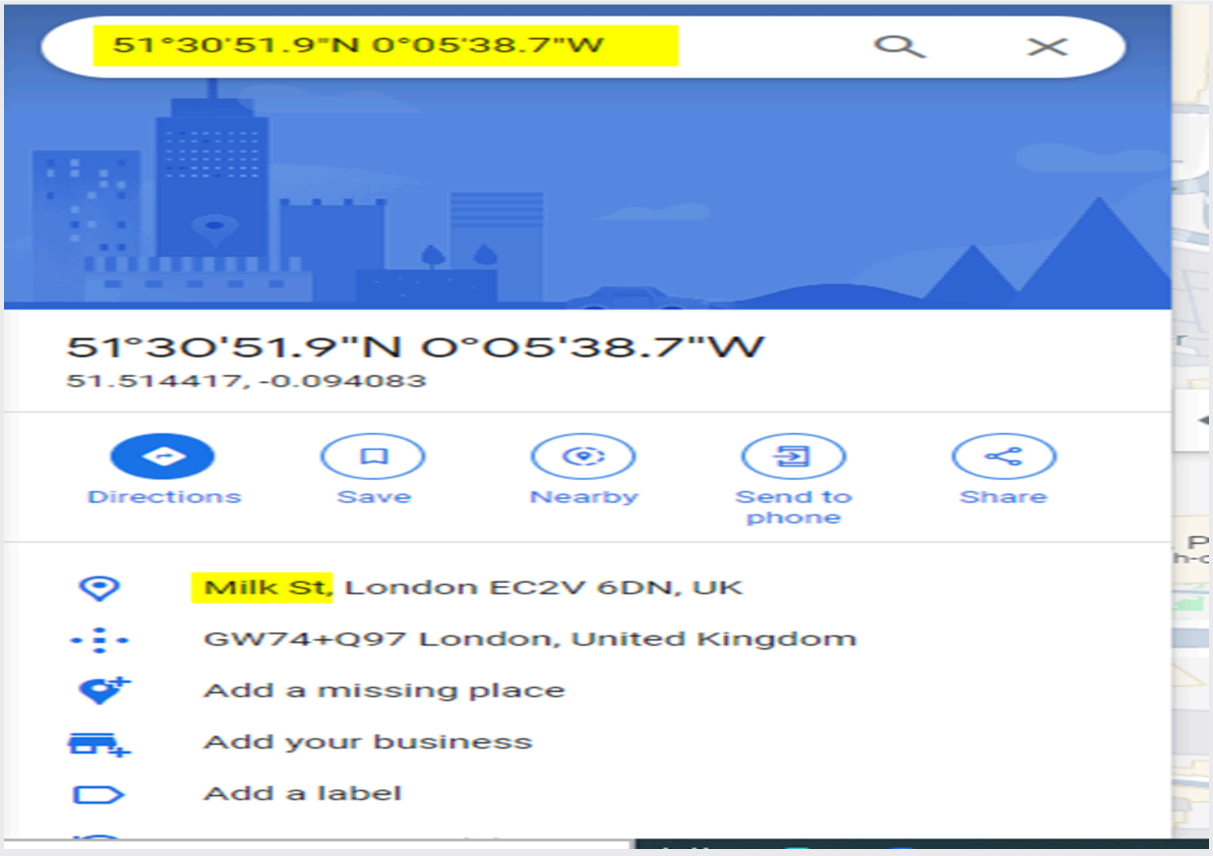
```
Application Record Version      : 4
Time Created                    : 17:23:40-17:23
Image Width                     : 1200
Image Height                    : 800
Encoding Process                : Progressive DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 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
```

Coordinates are:

GPS Latitude	: 51 deg 30' 51.90" N
GPS Longitude	: 0 deg 5' 38.73" W

➔ Using Google Maps and removing the extra zeros: **51°30'51.9"N 0°05'38.7"W**

Answer: Milk Street



51°30'51.9"N 0°05'38.7"W

51°30'51.9"N 0°05'38.7"W
51.514417, -0.094083

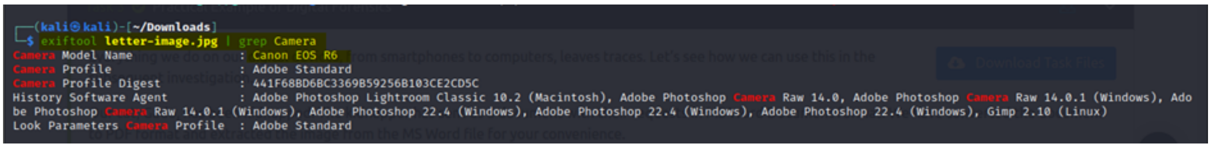
Milk St, London EC2V 6DN, UK

GW74+Q97 London, United Kingdom

➔ To know the model name of the camera used to take the photo

Command: **exiftool letter-image.jpg | grep Camera**

Answer: **Canon EOS R6**



```
┌──(kali㉿kali)-[~/Downloads]
└─$ exiftool letter-image.jpg | grep Camera
Camera Model Name               : Canon EOS R6
Camera Profile                  : Adobe Standard
Camera Profile Digest           : 441F68BD6BC3369B59256B103CE2CD5C
History Software Agent          : Adobe Photoshop Lightroom Classic 10.2 (Macintosh), Adobe Photoshop Camera Raw 14.0, Adobe Photoshop Camera Raw 14.0.1 (Windows), Ado
be Photoshop Camera Raw 14.0.1 (Windows), Adobe Photoshop 22.4 (Windows), Adobe Photoshop 22.4 (Windows), Adobe Photoshop 22.4 (Windows), Gimp 2.10 (Linux)
Look Parameters Camera Profile  : Adobe Standard
```

END!!!