

# Assignment-02

## 805 - Digital Forensic

Abu Syeed Sajid Ahmed

1. What manufacturer does the camera belong to? (if any found)
2. What is the camera model?
3. For questions 1 and 2, when was the photo taken?

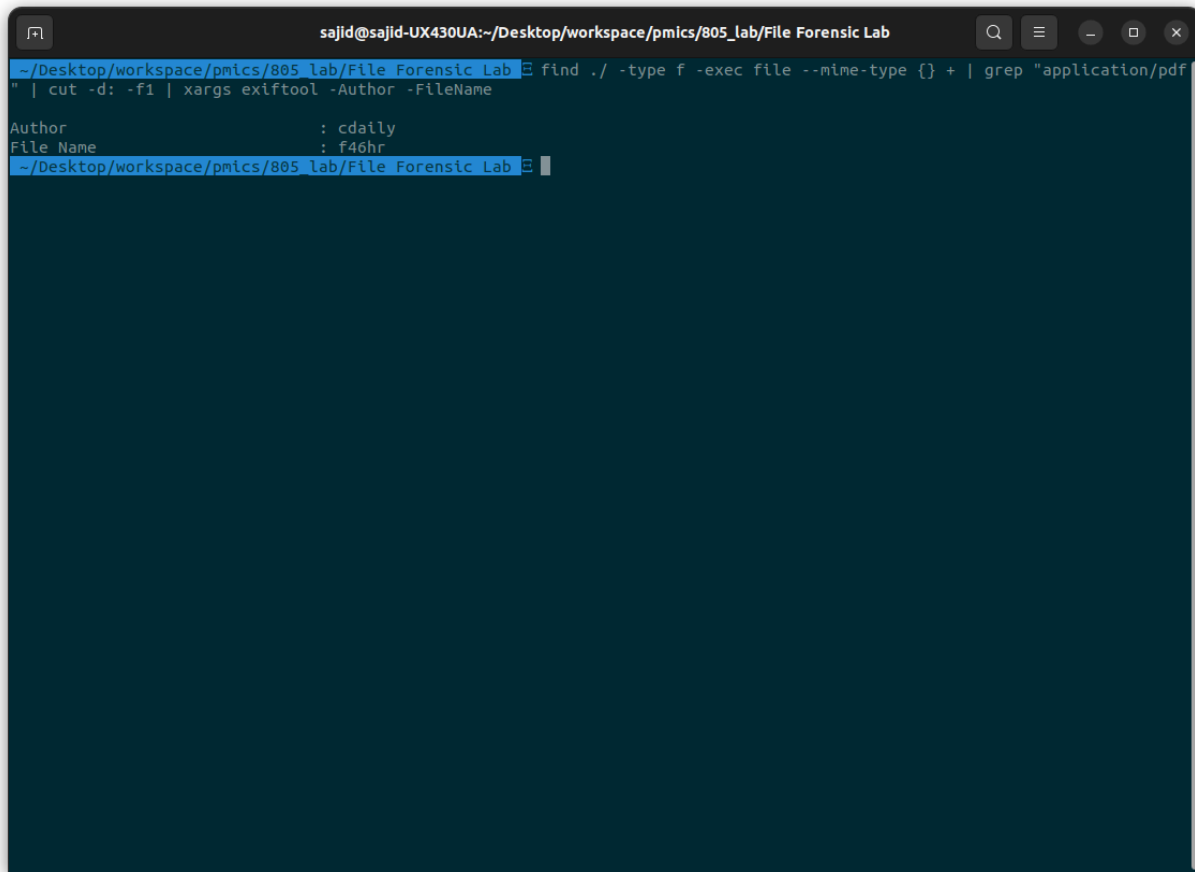
Answer:

```
sajid@sajid-UX430UA:~/Desktop/workspace/pmics/805_lab/File Forensic Lab
~/Desktop/workspace/pmics/805_lab/File Forensic Lab find ./ -type f -exec file --mime-type {} + | grep "image/" | cut -d: -f1 | xargs exiftool -Make -Model -CreateDate

===== ./IMG.jpg
Make                : realme
Camera Model Name   : realme 8 Pro
Create Date         : 2024:01:20 23:58:13
===== ./smartlocker.png
===== ./reot3
===== ./xeqha
===== ./SRMZ9HQM.JPG
Make                : Canon
Camera Model Name   : Canon EOS 20D
Create Date         : 2004:12:20 20:39:39
===== ./e26g8
===== ./locker.png
Create Date         : 2019:09:22 19:51:19-06:00
===== ./$RAQK1ET.JPG
Make                : EASTMAN KODAK COMPANY
Camera Model Name   : KODAK CX4310 DIGITAL CAMERA
Create Date         : 2002:01:01 12:02:26
===== ./ensho
===== ./heide
Make                : Google
Camera Model Name   : Pixel 2
Create Date         : 2018:08:29 19:31:19
===== ./SR7ZL4WH.JPG
Make                : Canon
Camera Model Name   : Canon EOS 20D
Create Date         : 2011:08:08 17:27:12
===== ./SR5SBPBH.JPG
Make                : OLYMPUS IMAGING CORP.
Camera Model Name   : FE280,X820,C520
Create Date         : 2009:07:20 13:35:15
===== ./mezi1
===== ./SRWVTDAT.JPG
Make                : Canon
Camera Model Name   : Canon EOS 20D
Create Date         : 2006:06:08 17:03:56
14 image files read
~/Desktop/workspace/pmics/805_lab/File Forensic Lab
```

4. Name of the author if any PDF file found?

Ans:



```
sajid@sajid-UX430UA:~/Desktop/workspace/pmics/805_lab/File Forensic Lab
~/Desktop/workspace/pmics/805_lab/File Forensic Lab find ./ -type f -exec file --mime-type {} + | grep "application/pdf"
" | cut -d: -f1 | xargs exiftool -Author -FileName
Author          : cdaily
File Name       : f46hr
~/Desktop/workspace/pmics/805_lab/File Forensic Lab
```

5. What are the GPS coordinates of the camera? (if any found)

Ans:

```
sajid@sajid-UX430UA:~/Desktop/workspace/pmics/805_lab/File Forensic Lab
~/Desktop/workspace/pmics/805_lab/File Forensic Lab exiftool -gps:all .
===== ./IMG.jpg
GPS Latitude Ref      : Unknown ()
GPS Longitude Ref     : Unknown ()
GPS Altitude Ref      : Above Sea Level
GPS Time Stamp        : 00:00:00
GPS Date Stamp        :
===== ./smartlocker.png
===== ./SRMZ9HQM.JPG
Warning: [minor] Possibly incorrect maker notes offsets (fix by -30?) - ./SRMZ9HQM.JPG
===== ./41029-ir_inter.wav
Error: File is empty - ./41029-ir_inter.wav
===== ./Password.zip
===== ./locker.png
===== ./Chernobyl.docx
===== ./SRAQK1ET.JPG
===== ./Contact Information.xlsx
===== ./SR7ZL4WH.JPG
===== ./SR5SBPBH.JPG
===== ./SRWVTDAT.JPG
    1 directories scanned
    12 image files read
X E ~/Desktop/workspace/pmics/805_lab/File Forensic Lab
```

6. Find the extensions of all the files? (Only files without extension)

Ans:

```
sajid@sajid-UX430UA:~/Desktop/workspace/pmics/805_lab/File Forensic Lab
~/Desktop/workspace/pmics/805_lab/File Forensic Lab exiftool -mimeType -ext '' -f ./
===== ./reot3
MIME Type : image/jpeg
===== ./f46hr
MIME Type : application/pdf
===== ./xeqha
MIME Type : image/png
===== ./j4al3
MIME Type : image/vnd.fpx
===== ./e26g8
MIME Type : image/jpeg
===== ./t4rh6
MIME Type : application/zip
===== ./ensho
MIME Type : image/jpeg
===== ./i0czd
MIME Type : text/rtf
===== ./e746m
MIME Type : application/vnd.ms-excel
===== ./heide
MIME Type : image/jpeg
===== ./mez11
MIME Type : image/gif
===== ./shgtb
MIME Type : text/plain
===== ./dfiqq
MIME Type : application/vnd.openxmlformats-officedocument.wordprocessingml.document
===== ./h82fe
MIME Type : application/vnd.ms-powerpoint
=====
1 directories scanned
14 image files read
~/Desktop/workspace/pmics/805_lab/File Forensic Lab
```

7. Find the flag from locker.png?

Ans:

```
sajid@sajid-UX430UA:~/Desktop/workspace/pmics/805_lab/File Forensic Lab
~/Desktop/workspace/pmics/805_lab/File Forensic Lab binwalk locker.png

DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0          JPEG image data, EXIF standard
12           0xC          TIFF image data, big-endian, offset of first image directory: 8
18729        0x4929       Copyright string: "Copyright 1999 Adobe Systems Incorporated"
585593       0x8EF79      Zip archive data, at least v2.0 to extract, compressed size: 72, uncompressed size: 76, name: kjhcnx236.txt
585903       0x8F04B      End of Zip archive, footer length: 22

~/Desktop/workspace/pmics/805_lab/File Forensic Lab unzip locker.png
Archive:  locker.png
warning [locker.png]:  585593 extra bytes at beginning or within zipfile
(attempting to process anyway)
  inflating: kjhcnx236.txt

* ~/Desktop/workspace/pmics/805_lab/File Forensic Lab ls
'$R5SBPBH.JPG'  40933-flourish.mid      e26g8  heide      locker.png      smartlocker.png
'$R7ZL4WH.JPG'  41029-ir_inter.wav      e746m  i0czd      mezi1          t4rh6
'$RAQK1ET.JPG'  Chernobyl.docx          enshe  IMG.jpg    Password.zip    xeqha
'$RMZ9HQM.JPG'  'Contact Information.xlsx' f46hr  j4al3      reot3
'$RWVTDAT.JPG'  dfiqg                  h82fe  kjhcnx236.txt shgtb

~/Desktop/workspace/pmics/805_lab/File Forensic Lab cat kjhcnx236.txt
flag{yI-g9apCA5Wct9R}
use the value inside flag{value} to extract smartlock.
~/Desktop/workspace/pmics/805_lab/File Forensic Lab
```

8. Find the flag from smartlocker.png?

```
sajid@sajid-UX430UA:~/Desktop/workspace/pmics/805_lab/Fil...
~/Desktop/workspace/pmics/805_lab/File Forensic Lab binwalk smartlocker.png

DECIMAL      HEXADECIMAL    DESCRIPTION
-----
0            0x0            JPEG image data, JFIF standard 1.01
659365      0xA0FA5        Zip archive data, encrypted compressed size: 43, uncompressed size: 23, name: asasdsde
659558      0xA1066        End of Zip archive, footer length: 22

~/Desktop/workspace/pmics/805_lab/File Forensic Lab 7z x smartlocker.png

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,4 CPUs Intel(R) Core(TM) i7-7500U
CPU @ 2.70GHz (806E9),ASM,AES-NI)

Scanning the drive for archives:
1 file, 659580 bytes (645 KiB)

Extracting archive: smartlocker.png
--
Path = smartlocker.png
Type = zip
Offset = 659365
Physical Size = 215

Would you like to replace the existing file:
  Path:      ./asasdsde
  Size:      23 bytes (1 KiB)
  Modified:  2024-03-26 15:52:12
with the file from archive:
  Path:      asasdsde
  Size:      23 bytes (1 KiB)
  Modified:  2024-03-26 15:52:12
? (Y)es / (N)o / (A)lways / (S)kip all / A(u)to rename all / (Q)uit? y

Enter password (will not be echoed):
Everything is Ok

Size:      23
Compressed: 659580
~/Desktop/workspace/pmics/805_lab/File Forensic Lab ls
'SR55BPBH.JPG'      41029-ir_inter.wav      e746m      i0czd      Password      xeqha
'SR7ZL4WH.JPG'      asasdsde                 enshe      IMG.jpg     Password.zip
'SRAQK1ET.JPG'      Chernobyl.docx           f46hr      j4al3      reot3
'SRMZ9HQM.JPG'      'Contact Information.xlsx' h82fe      kjhcnx236.txt shgtb
'SRMVTDAT.JPG'      dfigq                   hash.txt   locker.png  smartlocker.png
40933-flourish.mid  e26g8                   heide      mezi1      t4rh6
~/Desktop/workspace/pmics/805_lab/File Forensic Lab cat asasdsde
Password: Super12Admin
```

9. Find the password inside password.zip file?

Ans:

```
sajid@sajid-UX430UA:~/Desktop/workspace/pmics/805_lab/File Forensic Lab
~/Desktop/workspace/pmics/805_lab/File Forensic Lab john-the-ripper.zip2john Password.zip > hash.txt

~/Desktop/workspace/pmics/805_lab/File Forensic Lab ls
'$R5S8PBH.JPG' 40933-flourish.mid dfigq h82fe j4a13 reot3
'$R7ZL4WH.JPG' 41029-ir_inter.wav e26g8 hash.txt kjhcnx236.txt shgtb
'$RAQK1ET.JPG' asasdsde e746m heide locker.png smartlocker.png
'$RMZ9HQM.JPG' Chernobyl.docx ensho i0czd mezi1 t4rh6
'$RWVTDAT.JPG' 'Contact Information.xlsx' f46hr IMG.jpg Password.zip xeqha

~/Desktop/workspace/pmics/805_lab/File Forensic Lab john-the-ripper --format=zip hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Cracked 1 password hash (is in /home/sajid/snap/john-the-ripper/639/.john/john.pot), use "--show"
No password hashes left to crack (see FAQ)

~/Desktop/workspace/pmics/805_lab/File Forensic Lab john-the-ripper --format=zip hash.txt --show
Password.zip/Password:2020:Password:Password.zip:Password.zip

1 password hash cracked, 0 left

~/Desktop/workspace/pmics/805_lab/File Forensic Lab 7z x Password.zip -p2020

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,4 CPUs Intel(R) Core(TM) i7-7500U
CPU @ 2.70GHz (806E9),ASM,AES-NI)

Scanning the drive for archives:
1 file, 217 bytes (1 KiB)

Extracting archive: Password.zip
--
Path = Password.zip
Type = zip
Physical Size = 217

Everything is Ok

Size: 25
Compressed: 217

~/Desktop/workspace/pmics/805_lab/File Forensic Lab ls
'$R5S8PBH.JPG' 41029-ir_inter.wav e746m i0czd Password xeqha
'$R7ZL4WH.JPG' asasdsde ensho IMG.jpg Password.zip
'$RAQK1ET.JPG' Chernobyl.docx f46hr j4a13 reot3
'$RMZ9HQM.JPG' 'Contact Information.xlsx' h82fe kjhcnx236.txt shgtb
'$RWVTDAT.JPG' dfigq hash.txt locker.png smartlocker.png
40933-flourish.mid e26g8 heide mezi1 t4rh6

~/Desktop/workspace/pmics/805_lab/File Forensic Lab cat Password
Password: SuperAdminJohn

~/Desktop/workspace/pmics/805_lab/File Forensic Lab
```