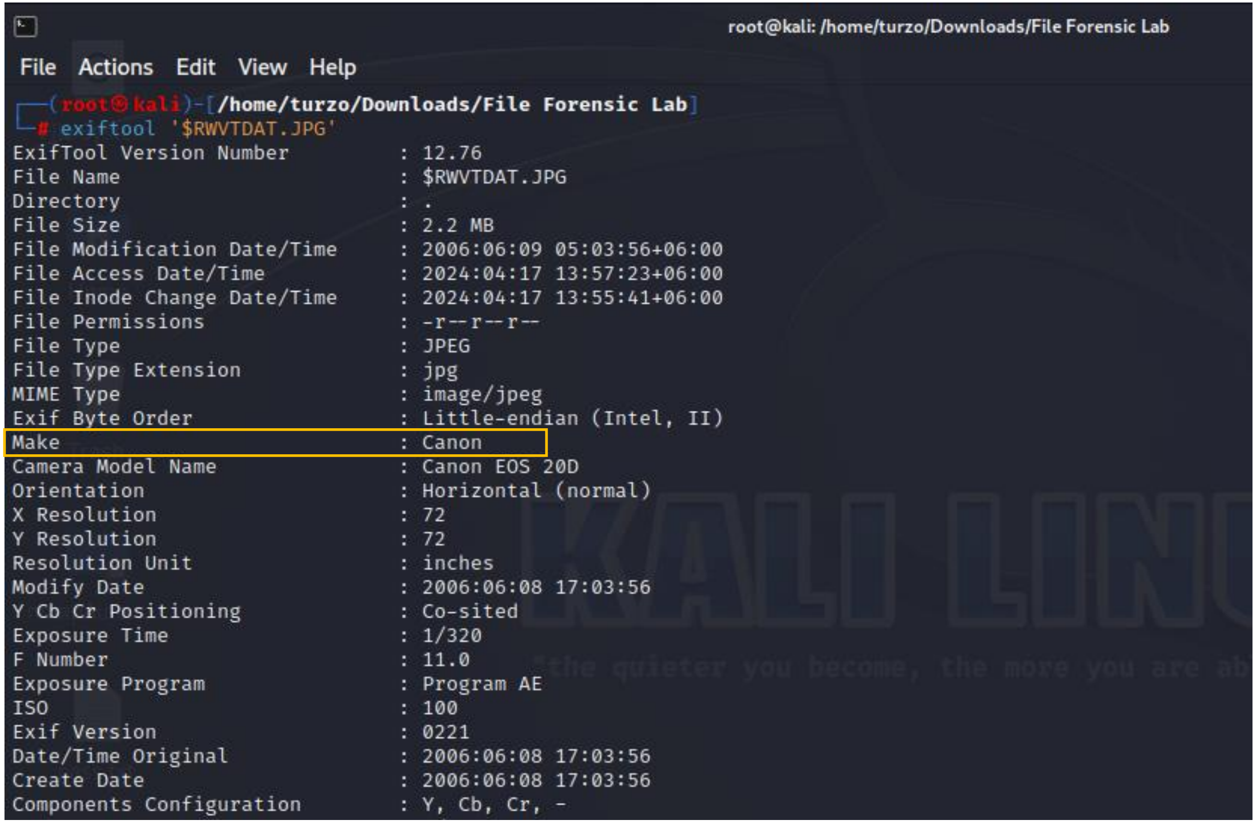
Assignment 02

805 - Digital Forensics

Turzo Roy – 30015

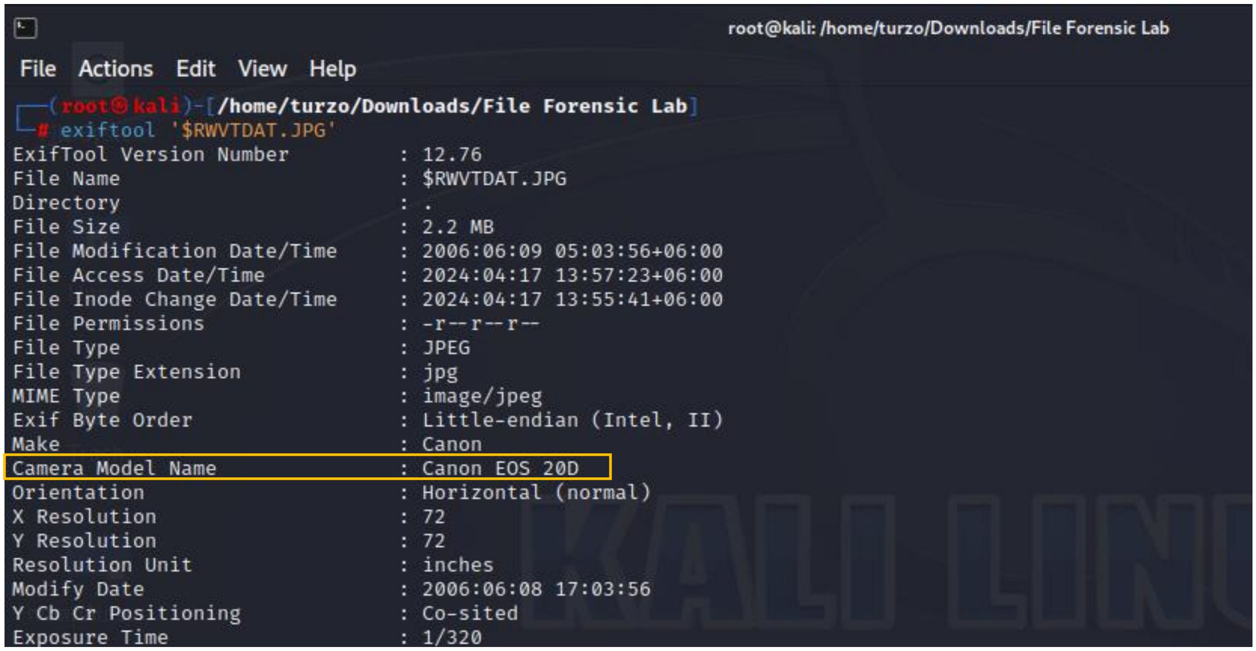
1. What manufacturer does the camera belong to? (if any found)



root@kali: /home/turzo/Downloads/File Forensic Lab
File Actions Edit View Help

```
┌──(root㉿kali)-[/home/turzo/Downloads/File Forensic Lab]
└─# exiftool '$RWVTDAT.JPG'
ExifTool Version Number         : 12.76
File Name                       : $RWVTDAT.JPG
Directory                       : .
File Size                       : 2.2 MB
File Modification Date/Time     : 2006:06:09 05:03:56+06:00
File Access Date/Time           : 2024:04:17 13:57:23+06:00
File Inode Change Date/Time     : 2024:04:17 13:55:41+06:00
File Permissions                : -r--r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Little-endian (Intel, II)
Make                            : Canon
Camera Model Name               : Canon EOS 20D
Orientation                     : Horizontal (normal)
X Resolution                    : 72
Y Resolution                    : 72
Resolution Unit                 : inches
Modify Date                     : 2006:06:08 17:03:56
Y Cb Cr Positioning             : Co-sited
Exposure Time                   : 1/320
F Number                        : 11.0
Exposure Program                : Program AE
ISO                             : 100
Exif Version                    : 0221
Date/Time Original              : 2006:06:08 17:03:56
Create Date                     : 2006:06:08 17:03:56
Components Configuration        : Y, Cb, Cr, -
```

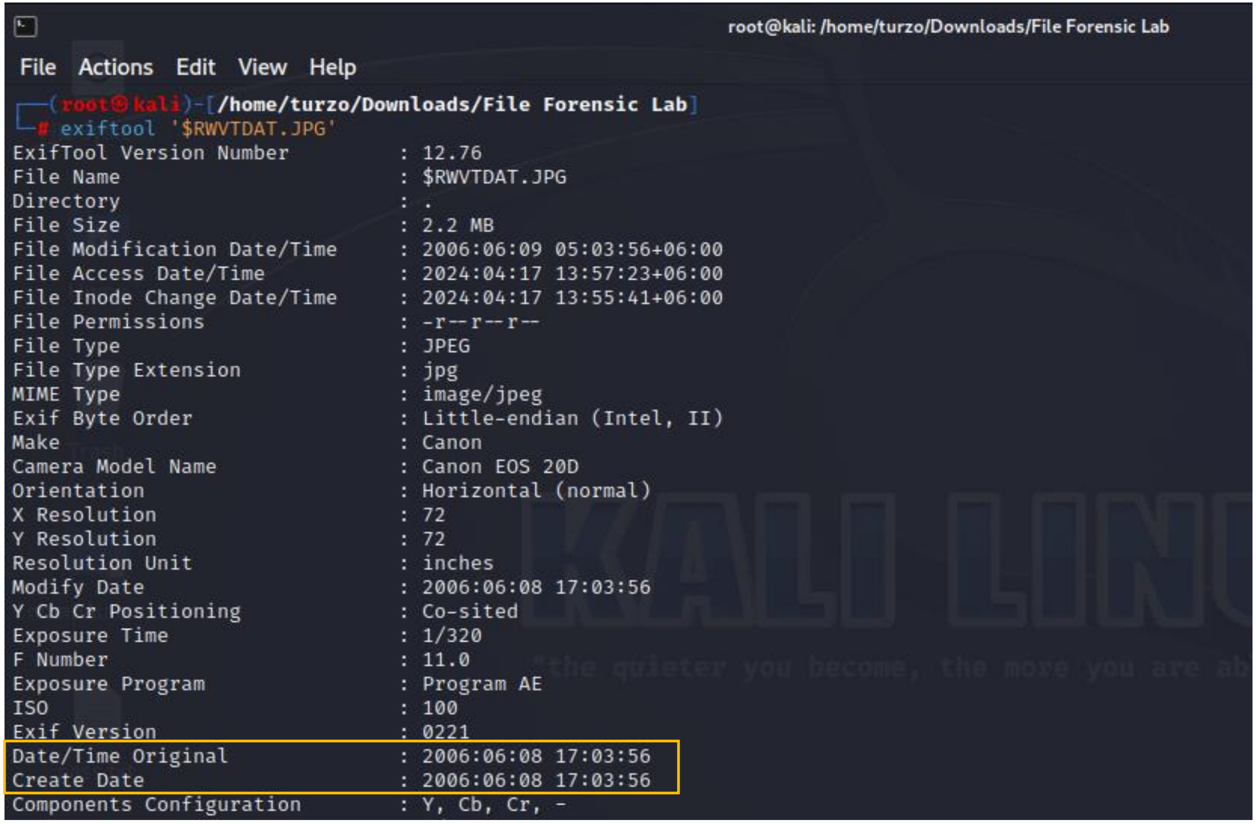
2. What is the camera model?



root@kali: /home/turzo/Downloads/File Forensic Lab
File Actions Edit View Help

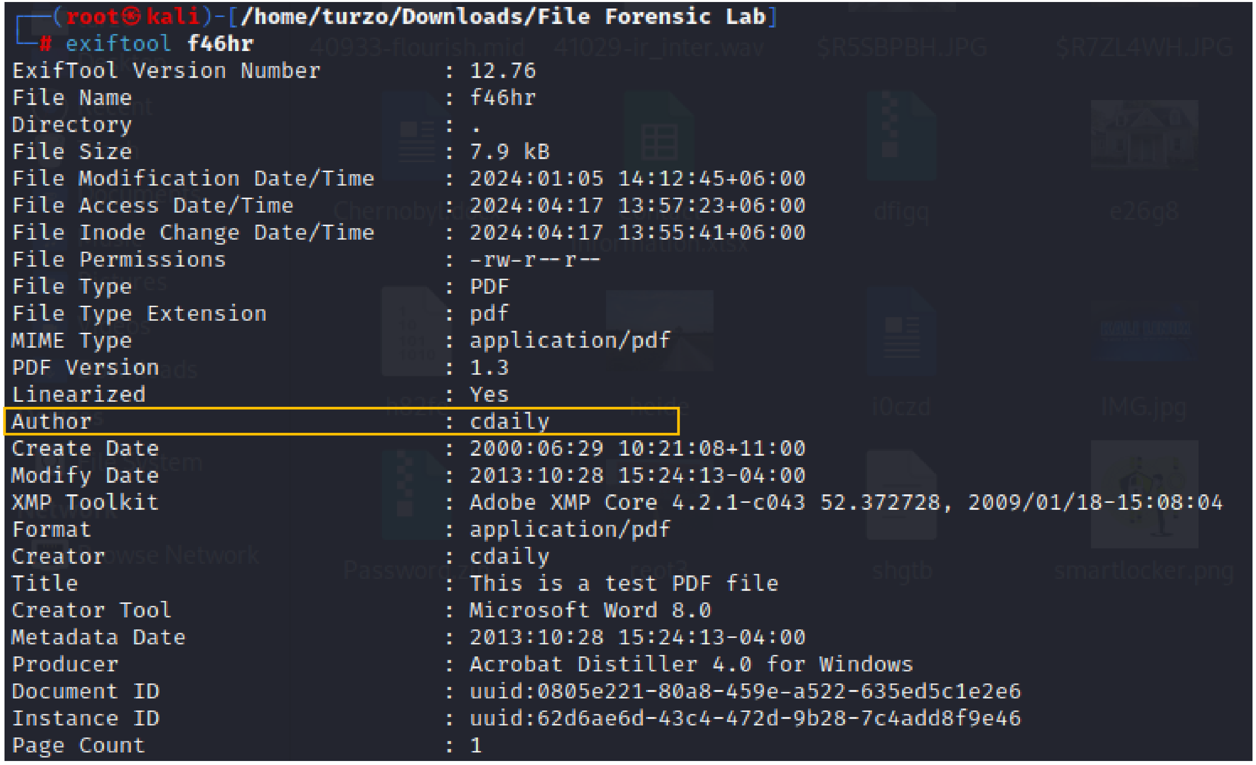
```
┌──(root㉿kali)-[/home/turzo/Downloads/File Forensic Lab]
└─# exiftool '$RWVTDAT.JPG'
ExifTool Version Number         : 12.76
File Name                       : $RWVTDAT.JPG
Directory                       : .
File Size                       : 2.2 MB
File Modification Date/Time     : 2006:06:09 05:03:56+06:00
File Access Date/Time           : 2024:04:17 13:57:23+06:00
File Inode Change Date/Time     : 2024:04:17 13:55:41+06:00
File Permissions                : -r--r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Little-endian (Intel, II)
Make                            : Canon
Camera Model Name               : Canon EOS 20D
Orientation                     : Horizontal (normal)
X Resolution                    : 72
Y Resolution                    : 72
Resolution Unit                 : inches
Modify Date                     : 2006:06:08 17:03:56
Y Cb Cr Positioning             : Co-sited
Exposure Time                   : 1/320
```

3. For question 1 and 2, when was the photo taken?



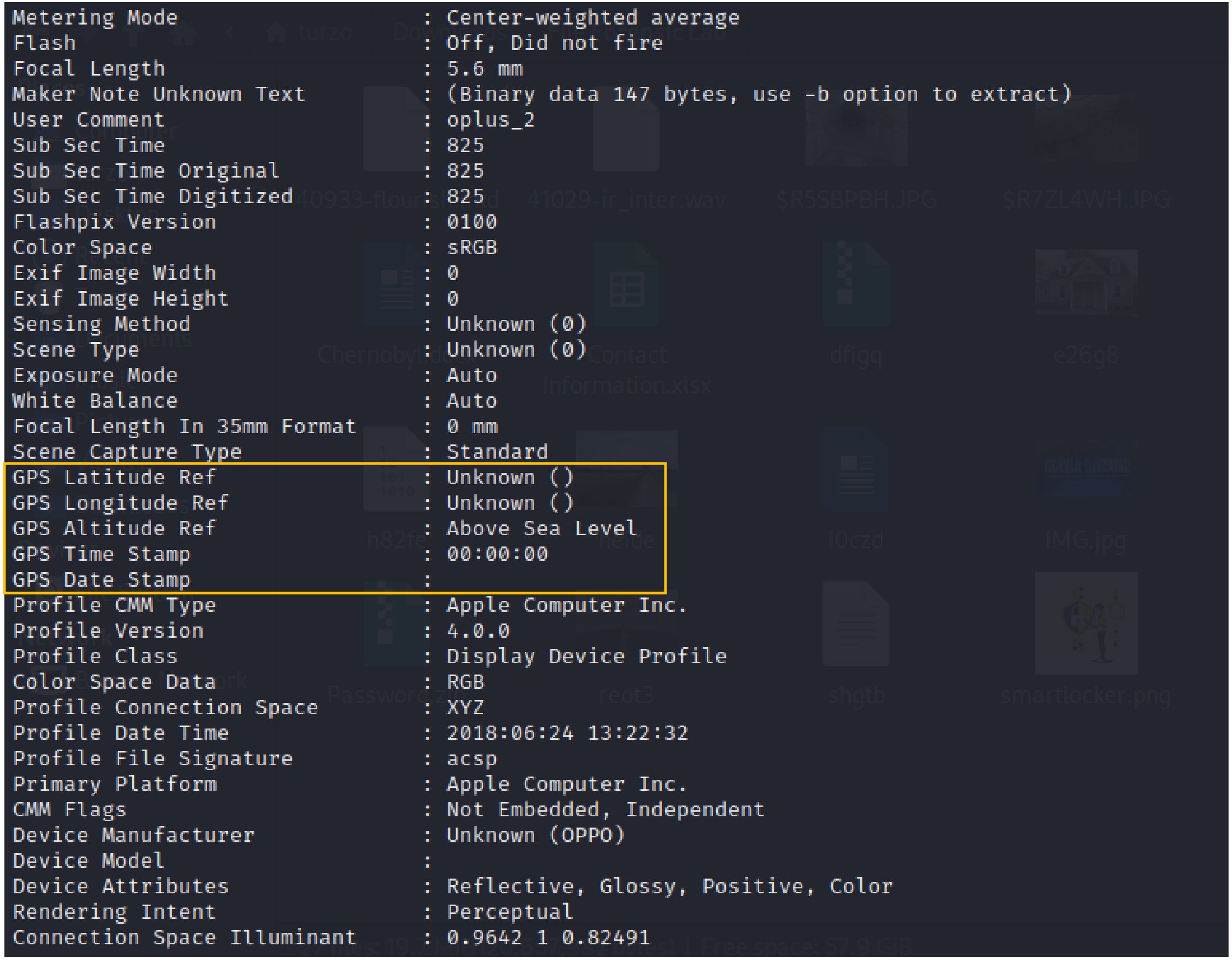
```
┌──(root㉿kali)-[/home/turzo/Downloads/File Forensic Lab]
└─# exiftool '$RWVTDAT.JPG'
ExifTool Version Number         : 12.76
File Name                       : $RWVTDAT.JPG
Directory                       : .
File Size                       : 2.2 MB
File Modification Date/Time     : 2006:06:09 05:03:56+06:00
File Access Date/Time           : 2024:04:17 13:57:23+06:00
File Inode Change Date/Time     : 2024:04:17 13:55:41+06:00
File Permissions                : -r--r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Little-endian (Intel, II)
Make                            : Canon
Camera Model Name               : Canon EOS 20D
Orientation                     : Horizontal (normal)
X Resolution                    : 72
Y Resolution                    : 72
Resolution Unit                 : inches
Modify Date                     : 2006:06:08 17:03:56
Y Cb Cr Positioning             : Co-sited
Exposure Time                   : 1/320
F Number                        : 11.0
Exposure Program                : Program AE
ISO                             : 100
Exif Version                    : 0221
Date/Time Original              : 2006:06:08 17:03:56
Create Date                     : 2006:06:08 17:03:56
Components Configuration        : Y, Cb, Cr, -
```

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



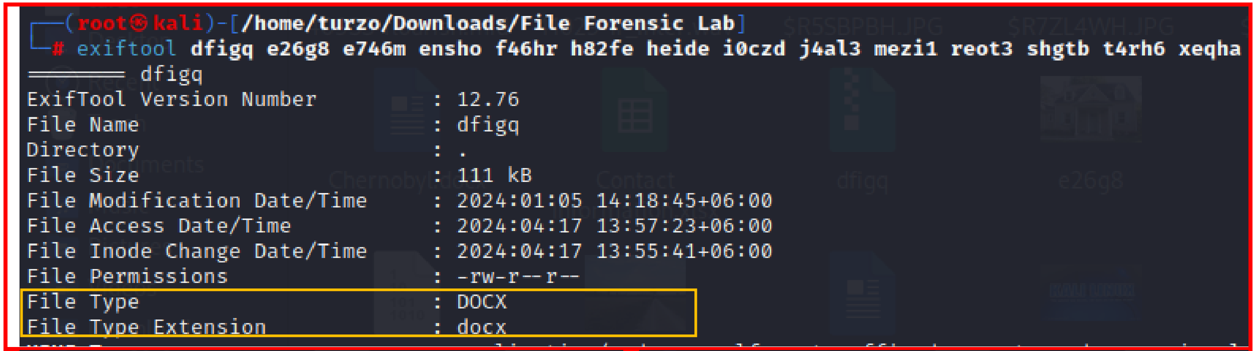
```
┌──(root㉿kali)-[/home/turzo/Downloads/File Forensic Lab]
└─# exiftool f46hr
ExifTool Version Number         : 12.76
File Name                       : f46hr
Directory                       : .
File Size                       : 7.9 kB
File Modification Date/Time     : 2024:01:05 14:12:45+06:00
File Access Date/Time           : 2024:04:17 13:57:23+06:00
File Inode Change Date/Time     : 2024:04:17 13:55:41+06:00
File Permissions                : -rw-r--r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.3
Linearized                      : Yes
Author                          : cdaily
Create Date                     : 2000:06:29 10:21:08+11:00
Modify Date                     : 2013:10:28 15:24:13-04:00
XMP Toolkit                     : Adobe XMP Core 4.2.1-c043 52.372728, 2009/01/18-15:08:04
Format                          : application/pdf
Creator                         : cdaily
Title                           : This is a test PDF file
Creator Tool                    : Microsoft Word 8.0
Metadata Date                   : 2013:10:28 15:24:13-04:00
Producer                        : Acrobat Distiller 4.0 for Windows
Document ID                     : uuid:0805e221-80a8-459e-a522-635ed5c1e2e6
Instance ID                     : uuid:62d6ae6d-43c4-472d-9b28-7c4add8f9e46
Page Count                      : 1
```

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

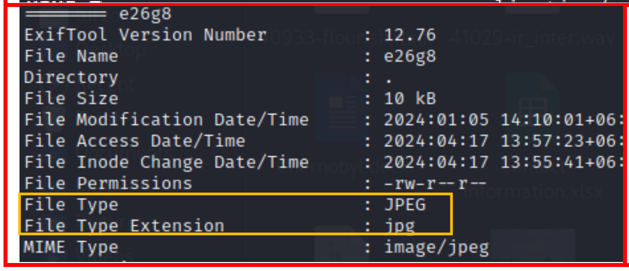


```
Metering Mode                   : Center-weighted average
Flash                           : Off, Did not fire
Focal Length                    : 5.6 mm
Maker Note Unknown Text         : (Binary data 147 bytes, use -b option to extract)
User Comment                    : oplus_2
Sub Sec Time                    : 825
Sub Sec Time Original           : 825
Sub Sec Time Digitized          : 825
Flashpix Version                : 0100
Color Space                     : sRGB
Exif Image Width                : 0
Exif Image Height               : 0
Sensing Method                  : Unknown (0)
Scene Type                      : Unknown (0)
Exposure Mode                   : Auto
White Balance                   : Auto
Focal Length In 35mm Format     : 0 mm
Scene Capture Type              : Standard
GPS Latitude Ref                : Unknown ()
GPS Longitude Ref               : Unknown ()
GPS Altitude Ref                : Above Sea Level
GPS Time Stamp                  : 00:00:00
GPS Date Stamp                  :
Profile CMM Type                : Apple Computer Inc.
Profile Version                 : 4.0.0
Profile Class                   : Display Device Profile
Color Space Data                : RGB
Profile Connection Space        : XYZ
Profile Date Time               : 2018:06:24 13:22:32
Profile File Signature          : acsp
Primary Platform                : Apple Computer Inc.
CMM Flags                       : Not Embedded, Independent
Device Manufacturer             : Unknown (OPPO)
Device Model                    :
Device Attributes               : Reflective, Glossy, Positive, Color
Rendering Intent                : Perceptual
Connection Space Illuminant     : 0.9642 1 0.82491
```

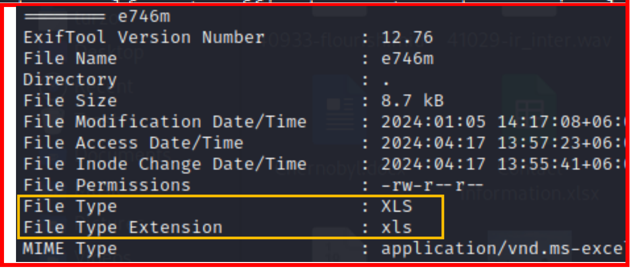
6. Find the extensions of all the files? (Only files without extension)



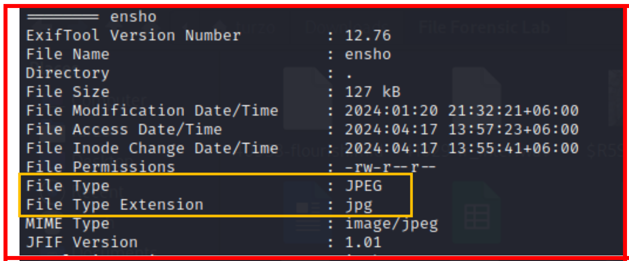
```
┌──(root㉿kali)-[/home/turzo/Downloads/File Forensic Lab]
└─# exiftool dfigq e26g8 e746m ensho f46hr h82fe heide i0czd j4al3 mezi1 reot3 shgtb t4rh6 xeqha
======== dfigq
ExifTool Version Number         : 12.76
File Name                       : dfigq
Directory                       : .
File Size                       : 111 kB
File Modification Date/Time     : 2024:01:05 14:18:45+06:00
File Access Date/Time           : 2024:04:17 13:57:23+06:00
File Inode Change Date/Time     : 2024:04:17 13:55:41+06:00
File Permissions                : -rw-r--r--
File Type                       : DOCX
File Type Extension             : docx
```



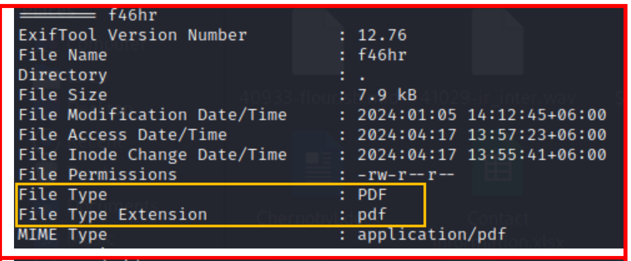
```
======== e26g8
ExifTool Version Number         : 12.76
File Name                       : e26g8
Directory                       : .
File Size                       : 10 kB
File Modification Date/Time     : 2024:01:05 14:10:01+06:
File Access Date/Time           : 2024:04:17 13:57:23+06:
File Inode Change Date/Time     : 2024:04:17 13:55:41+06:
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
```



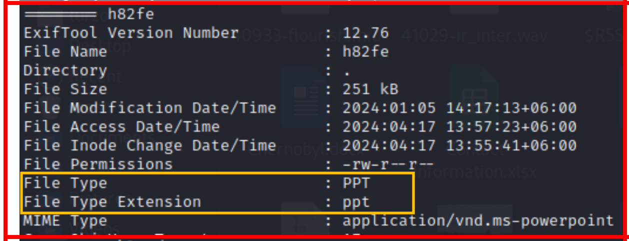
```
======== e746m
ExifTool Version Number         : 12.76
File Name                       : e746m
Directory                       : .
File Size                       : 8.7 kB
File Modification Date/Time     : 2024:01:05 14:17:08+06:
File Access Date/Time           : 2024:04:17 13:57:23+06:
File Inode Change Date/Time     : 2024:04:17 13:55:41+06:
File Permissions                : -rw-r--r--
File Type                       : XLS
File Type Extension             : xls
MIME Type                       : application/vnd.ms-exce
```



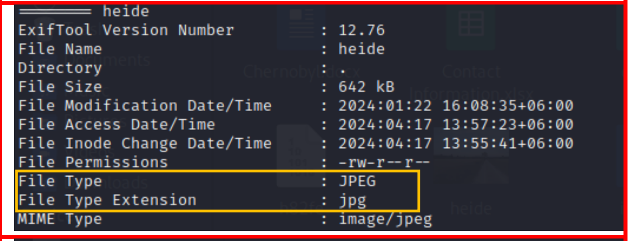
```
======== ensho
ExifTool Version Number         : 12.76
File Name                       : ensho
Directory                       : .
File Size                       : 127 kB
File Modification Date/Time     : 2024:01:20 21:32:21+06:00
File Access Date/Time           : 2024:04:17 13:57:23+06:00
File Inode Change Date/Time     : 2024:04:17 13:55:41+06:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
```



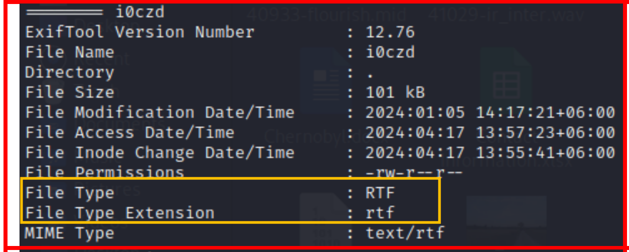
```
======== f46hr
ExifTool Version Number         : 12.76
File Name                       : f46hr
Directory                       : .
File Size                       : 7.9 kB
File Modification Date/Time     : 2024:01:05 14:12:45+06:00
File Access Date/Time           : 2024:04:17 13:57:23+06:00
File Inode Change Date/Time     : 2024:04:17 13:55:41+06:00
File Permissions                : -rw-r--r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
```



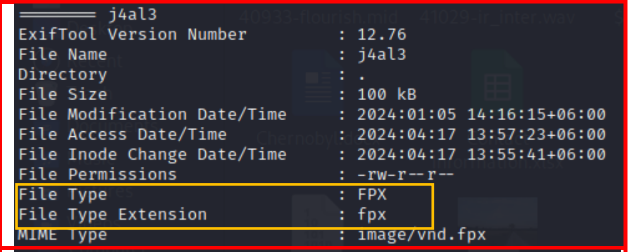
```
======== h82fe
ExifTool Version Number         : 12.76
File Name                       : h82fe
Directory                       : .
File Size                       : 251 kB
File Modification Date/Time     : 2024:01:05 14:17:13+06:00
File Access Date/Time           : 2024:04:17 13:57:23+06:00
File Inode Change Date/Time     : 2024:04:17 13:55:41+06:00
File Permissions                : -rw-r--r--
File Type                       : PPT
File Type Extension             : ppt
MIME Type                       : application/vnd.ms-powerpoint
```



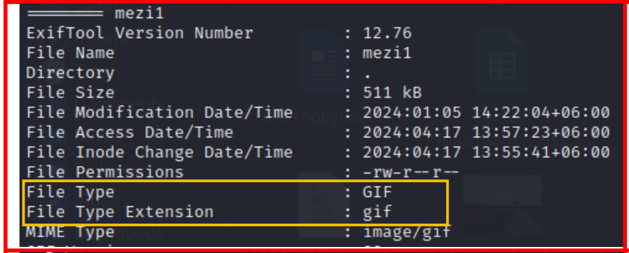
```
======== heide
ExifTool Version Number         : 12.76
File Name                       : heide
Directory                       : .
File Size                       : 642 kB
File Modification Date/Time     : 2024:01:22 16:08:35+06:00
File Access Date/Time           : 2024:04:17 13:57:23+06:00
File Inode Change Date/Time     : 2024:04:17 13:55:41+06:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
```



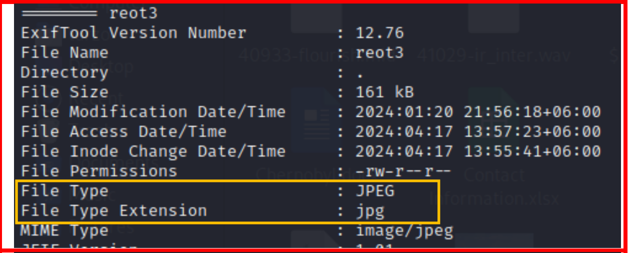
```
======== i0czd
ExifTool Version Number         : 12.76
File Name                       : i0czd
Directory                       : .
File Size                       : 101 kB
File Modification Date/Time     : 2024:01:05 14:17:21+06:00
File Access Date/Time           : 2024:04:17 13:57:23+06:00
File Inode Change Date/Time     : 2024:04:17 13:55:41+06:00
File Permissions                : -rw-r--r--
File Type                       : RTF
File Type Extension             : rtf
MIME Type                       : text/rtf
```



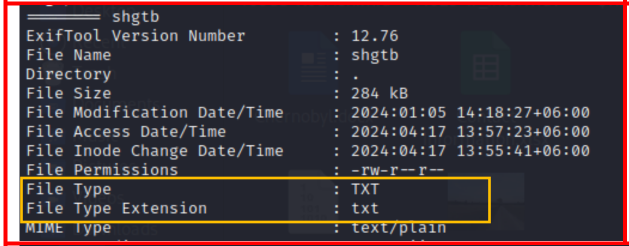
```
======== j4al3
ExifTool Version Number         : 12.76
File Name                       : j4al3
Directory                       : .
File Size                       : 100 kB
File Modification Date/Time     : 2024:01:05 14:16:15+06:00
File Access Date/Time           : 2024:04:17 13:57:23+06:00
File Inode Change Date/Time     : 2024:04:17 13:55:41+06:00
File Permissions                : -rw-r--r--
File Type                       : FPX
File Type Extension             : fpx
MIME Type                       : image/vnd.fpx
```



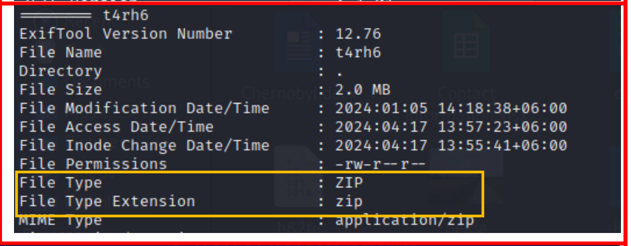
```
======== mezi1
ExifTool Version Number         : 12.76
File Name                       : mezi1
Directory                       : .
File Size                       : 511 kB
File Modification Date/Time     : 2024:01:05 14:22:04+06:00
File Access Date/Time           : 2024:04:17 13:57:23+06:00
File Inode Change Date/Time     : 2024:04:17 13:55:41+06:00
File Permissions                : -rw-r--r--
File Type                       : GIF
File Type Extension             : gif
MIME Type                       : image/gif
```



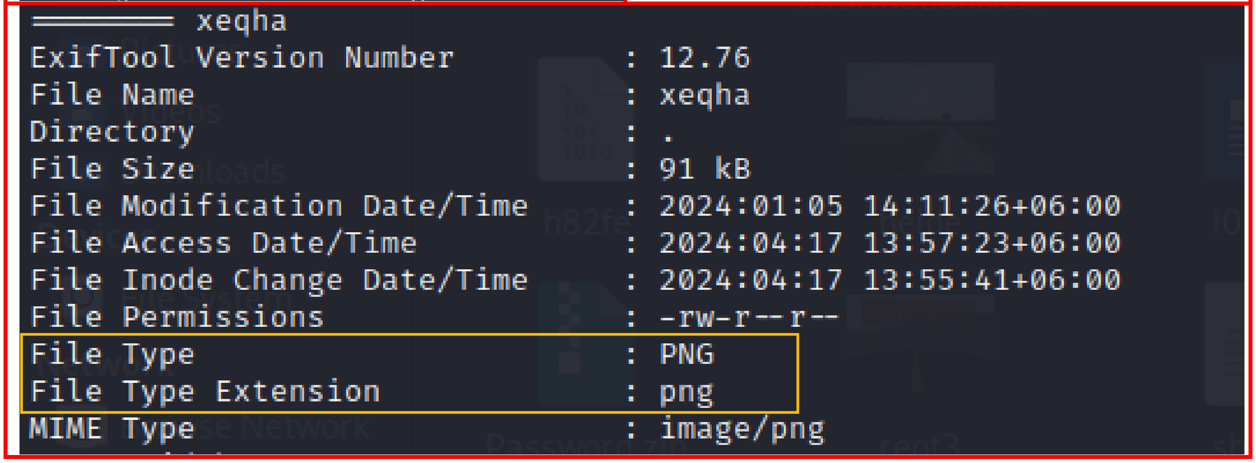
```
======== reot3
ExifTool Version Number         : 12.76
File Name                       : reot3
Directory                       : .
File Size                       : 161 kB
File Modification Date/Time     : 2024:01:20 21:56:18+06:00
File Access Date/Time           : 2024:04:17 13:57:23+06:00
File Inode Change Date/Time     : 2024:04:17 13:55:41+06:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
```



```
======== shgtb
ExifTool Version Number         : 12.76
File Name                       : shgtb
Directory                       : .
File Size                       : 284 kB
File Modification Date/Time     : 2024:01:05 14:18:27+06:00
File Access Date/Time           : 2024:04:17 13:57:23+06:00
File Inode Change Date/Time     : 2024:04:17 13:55:41+06:00
File Permissions                : -rw-r--r--
File Type                       : TXT
File Type Extension             : txt
MIME Type                       : text/plain
```

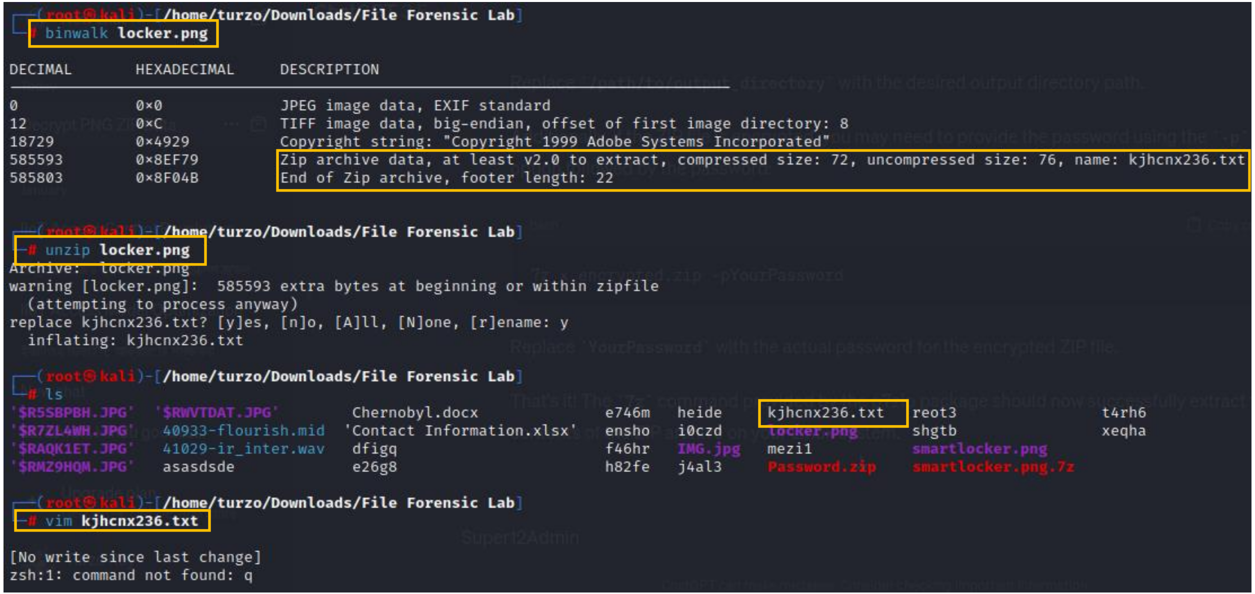


```
======== t4rh6
ExifTool Version Number         : 12.76
File Name                       : t4rh6
Directory                       : .
File Size                       : 2.0 MB
File Modification Date/Time     : 2024:01:05 14:18:38+06:00
File Access Date/Time           : 2024:04:17 13:57:23+06:00
File Inode Change Date/Time     : 2024:04:17 13:55:41+06:00
File Permissions                : -rw-r--r--
File Type                       : ZIP
File Type Extension             : zip
MIME Type                       : application/zip
```

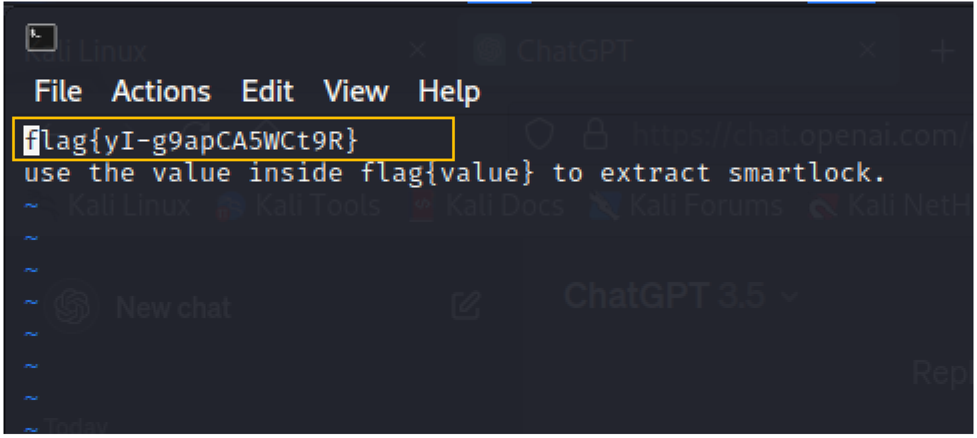


```
======== xeqha
ExifTool Version Number         : 12.76
File Name                       : xeqha
Directory                       : .
File Size                       : 91 kB
File Modification Date/Time     : 2024:01:05 14:11:26+06:00
File Access Date/Time           : 2024:04:17 13:57:23+06:00
File Inode Change Date/Time     : 2024:04:17 13:55:41+06:00
File Permissions                : -rw-r--r--
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
```

7. Find the flag from locker.png?

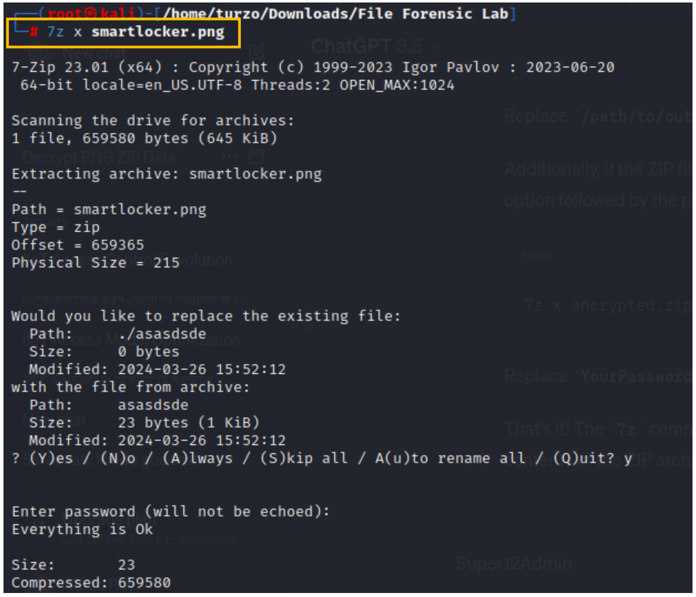


```
┌──(root㉿kali)-[/home/turzo/Downloads/File Forensic Lab]
└─# binwalk locker.png

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
585803        0x8F04B         End of Zip archive, footer length: 22


┌──(root㉿kali)-[/home/turzo/Downloads/File Forensic Lab]
└─# unzip locker.png
Archive:  locker.png
warning [locker.png]:  585593 extra bytes at beginning or within zipfile
  (attempting to process anyway)
replace kjhcnx236.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
  inflating: kjhcnx236.txt

┌──(root㉿kali)-[/home/turzo/Downloads/File Forensic Lab]
└─# ls
'$R5SBPBH.JPG'  '$RWVTDAT.JPG'        Chernobyl.docx              e746m  heide   kjhcnx236.txt  reot3               t4rh6
'$R7ZL4WH.JPG'   40933-flourish.mid  'Contact Information.xlsx'  ensho  i0czd   locker.png     shgtb               xeqha
'$RAQK1ET.JPG'   41029-ir_inter.wav   dfigq                       f46hr  IMG.jpg  mezi1          smartlocker.png
'$RMZ9HQM.JPG'   asasdsde             e26g8                       h82fe  j4al3   Password.zip   smartlocker.png.7z

┌──(root㉿kali)-[/home/turzo/Downloads/File Forensic Lab]
└─# vim kjhcnx236.txt

[No write since last change]
zsh:1: command not found: q
```

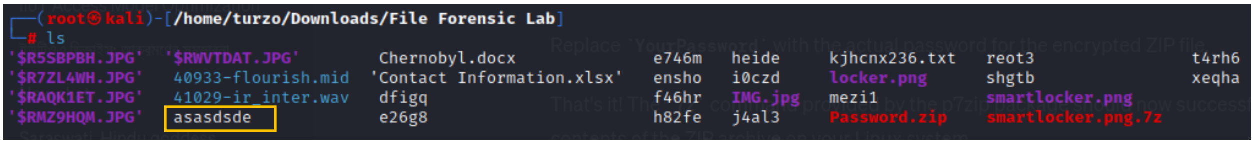


```
flag{yI-g9apCA5WCt9R}
use the value inside flag{value} to extract smartlock.
~
~
~
~
~
~
~
```

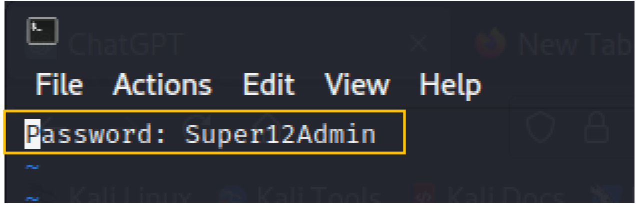
8. Find the flag from smartlocker.png?



```
┌──(root㉿kali)-[/home/turzo/Downloads/File Forensic Lab]
└─# 7z x smartlocker.png

7-Zip 23.01 (x64) : Copyright (c) 1999-2023 Igor Pavlov : 2023-06-20
 64-bit locale=en_US.UTF-8 Threads:2 OPEN_MAX:1024

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:     0 bytes
  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
```

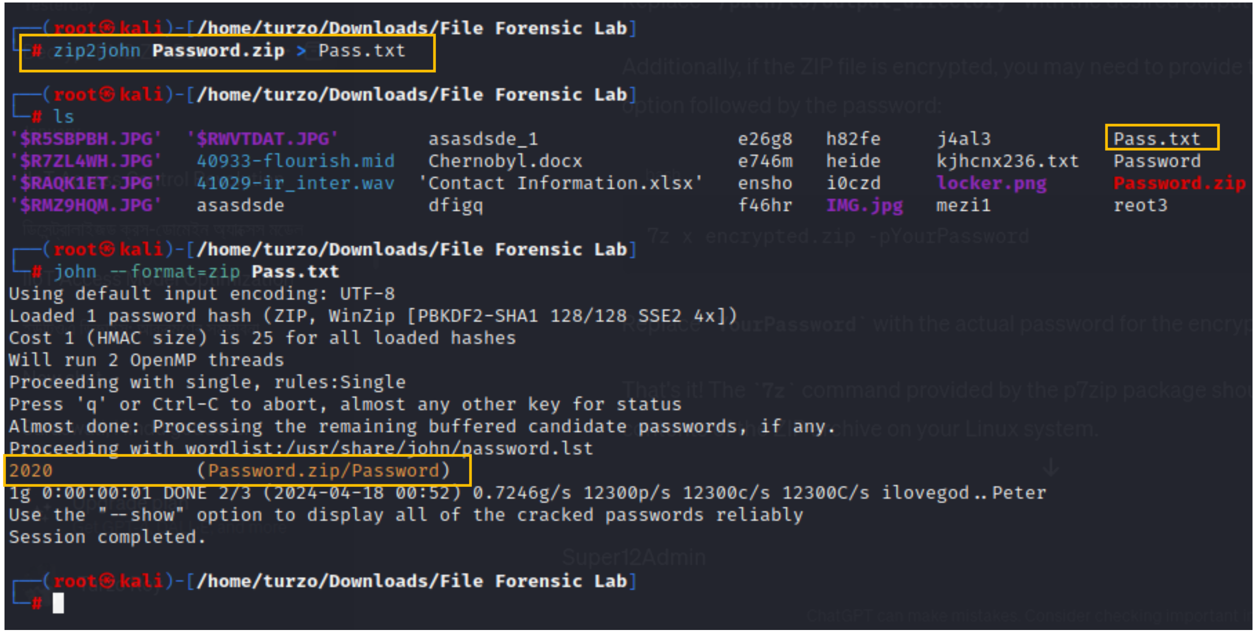


```
┌──(root㉿kali)-[/home/turzo/Downloads/File Forensic Lab]
└─# ls
'$R5SBPBH.JPG'  '$RWVTDAT.JPG'         Chernobyl.docx              e746m  heide    kjhcnx236.txt  reot3                 t4rh6
'$R7ZL4WH.JPG'   40933-flourish.mid  'Contact Information.xlsx'   ensho  i0czd    locker.png     shgtb                 xeqha
'$RAQK1ET.JPG'   41029-ir_inter.wav   dfigq                       f46hr  IMG.jpg  mezi1          smartlocker.png
'$RMZ9HQM.JPG'   asasdsde             e26g8                       h82fe  j4al3    Password.zip   smartlocker.png.7z
```



```
Password: Super12Admin
~
~
```

9. Find the password inside password.zip file?



```
┌──(root㉿kali)-[/home/turzo/Downloads/File Forensic Lab]
└─# zip2john Password.zip > Pass.txt

┌──(root㉿kali)-[/home/turzo/Downloads/File Forensic Lab]
└─# ls
'$R5SBPBH.JPG'  '$RWVTDAT.JPG'         asasdsde_1                   e26g8  h82fe    j4al3          Pass.txt
'$R7ZL4WH.JPG'   40933-flourish.mid   Chernobyl.docx               e746m  heide    kjhcnx236.txt  Password
'$RAQK1ET.JPG'   41029-ir_inter.wav  'Contact Information.xlsx'   ensho  i0czd    locker.png     Password.zip
'$RMZ9HQM.JPG'   asasdsde             dfigq                        f46hr  IMG.jpg  mezi1          reot3

┌──(root㉿kali)-[/home/turzo/Downloads/File Forensic Lab]
└─# john --format=zip Pass.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 SSE2 4x])
Cost 1 (HMAC size) is 25 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
2020             (Password.zip/Password)
1g 0:00:00:01 DONE 2/3 (2024-04-18 00:52) 0.7246g/s 12300p/s 12300c/s 12300C/s ilovegod..Peter
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(root㉿kali)-[/home/turzo/Downloads/File Forensic Lab]
└─# 
```