

**Name: Mayesha Sadia**

**EDGE ID: 2111269**

**Date: 05 October,2024**

**CASE 1:**

1<sup>st</sup> Image:

- 1) 2024:09:25 22:18:34
- 2) Unknown(OPPO)
- 3) Baseline DCT, Huffman Coding
- 4) 4000
- 5) 2024:09:25 21:16:00.871+06:00

```
root@kali: /media/sf_JU_mayesha/Img/ExTracted File
File Actions Edit View Help

(kali㉿kali)-[~]
$ sudo -i
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
(root㉿kali)-[~]
# cd /media/sf_JU_mayesha/Img

(root㉿kali)-[/media/sf_JU_mayesha/Img]
# ls
'ExTracted File'  drive-download-20241005T064826Z-001.zip

(root㉿kali)-[/media/sf_JU_mayesha/Img]
# cd /media/sf_JU_mayesha/Img/ExTracted File
cd: string not in pwd: /media/sf_JU_mayesha/Img/ExTracted

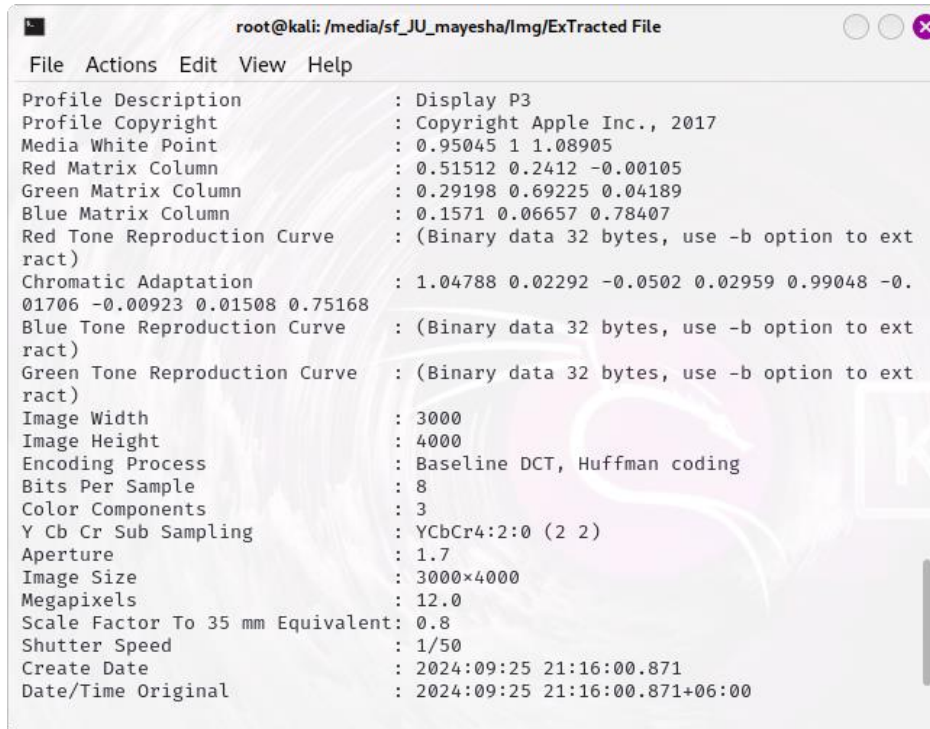
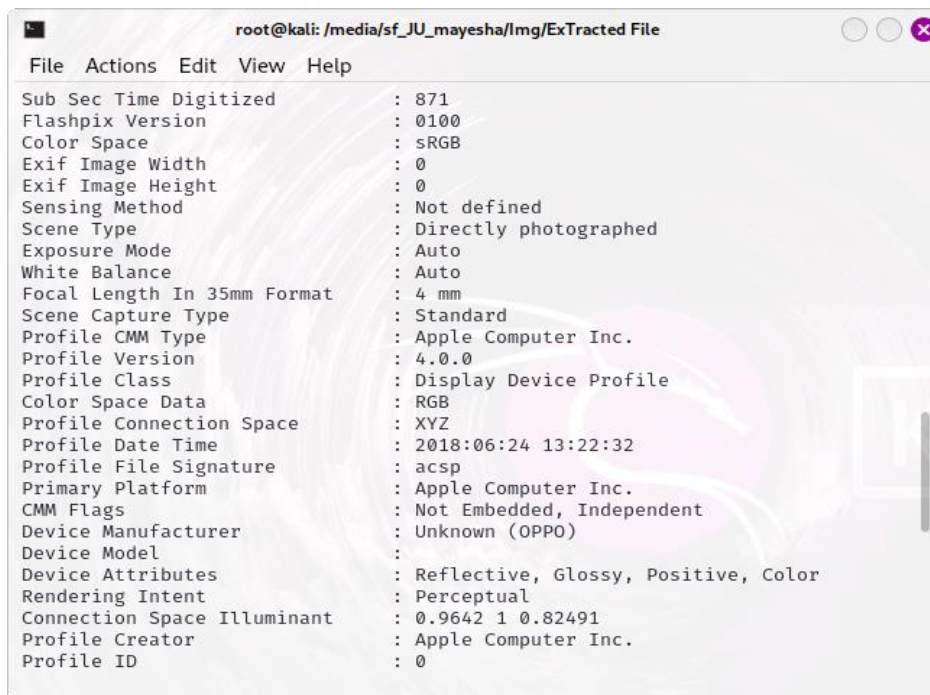
(root㉿kali)-[/media/sf_JU_mayesha/Img]
# cd /media/sf_JU_mayesha/Img/ExTracted\ File

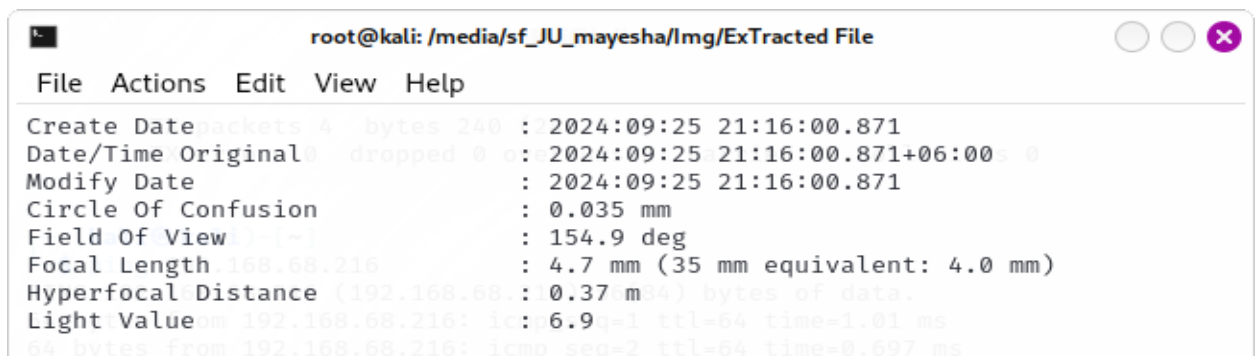
(root㉿kali)-[/media/sf_JU_mayesha/Img/ExTracted File]
# ls
IMG20240925211600.jpg  IMG20240925221834.jpg

(root㉿kali)-[/media/sf_JU_mayesha/Img/ExTracted File]
# exiftool IMG20240925211600.jpg
ExifTool Version Number      : 12.76
```

```
root@kali: /media/sf_JU_mayesha/Img/ExTracted File
File Actions Edit View Help
(root@kali)-[/media/sf_JU_mayesha/Img/ExTracted File]
# exiftool IMG20240925211600.jpg
ExifTool Version Number      : 12.76
File Name                    : IMG20240925211600.jpg
Directory                   : .
File Size                    : 4.3 MB
File Modification Date/Time  : 2024:10:05 02:49:12-04:00
File Access Date/Time       : 2024:10:05 03:04:56-04:00
File Inode Change Date/Time  : 2024:10:05 02:49:12-04:00
File Permissions             : -rwxrwx---
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
JFIF Version                 : 1.01
Exif Byte Order              : Little-endian (Intel, II)
Make                        : OPPO
Camera Model Name           : OPPO A95
Orientation                  : Horizontal (normal)
X Resolution                 : 72
Y Resolution                 : 72
Resolution Unit              : inches
Modify Date                  : 2024:09:25 21:16:00
Y Cb Cr Positioning         : Centered
Interoperability Index      : R98 - DCF basic file (sRGB)
Interoperability Version    : 1.0
Exposure Time                : 1/50
F Number                     : 1.7
```

```
root@kali: /media/sf_JU_mayesha/Img/ExTracted File
File Actions Edit View Help
Interoperability Version      : 1.0
Exposure Time                 : 1/50
F Number                      : 1.7
Exposure Program              : Program AE
ISO                           : 122
Exif Version                  : 0220
Date/Time Original            : 2024:09:25 21:16:00
Create Date                   : 2024:09:25 21:16:00
Offset Time Original          : +06:00
Components Configuration     : Y, Cb, Cr, -
Shutter Speed Value           : 1/50
Aperture Value                : 1.7
Brightness Value              : 1.43
Exposure Compensation         : 0
Max Aperture Value            : 1.7
Metering Mode                 : Center-weighted average
Flash                         : Off, Did not fire
Focal Length                  : 4.7 mm
Maker Note Unknown Text      : (Binary data 146 bytes, use -b option to extract)
Warning                       : Invalid EXIF text encoding for UserComment
User Comment                  : oplus_34
Sub Sec Time                  : 871
Sub Sec Time Original         : 871
Sub Sec Time Digitized        : 871
Flashpix Version              : 0100
Color Space                   : sRGB
```





2<sup>nd</sup> Image:

- 1) 2024:09:25 21:16:00
- 2) Unknown(OPPO)
- 3) Baseline DCT, Huffman Coding
- 4) 4000
- 5) 2024:09:25 22:18:34.529+06:00

```

(root@kali)-[/media/sf_JU_mayesha/Img/ExTracted File]
# exiftool IMG20240925221834.jpg
ExifTool Version Number      : 12.76
File Name                    : IMG20240925221834.jpg
Directory                    : .
File Size                    : 4.4 MB
File Modification Date/Time  : 2024:10:05 02:49:12-04:00
File Access Date/Time       : 2024:10:05 03:22:27-04:00
File Inode Change Date/Time  : 2024:10:05 02:49:12-04:00
File Permissions             : -rwxrwx---
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
Exif Byte Order              : Little-endian (Intel, II)
Make                        : OPPO
Camera Model Name            : OPPO A95
Orientation                  : Horizontal (normal)

```

```

root@kali: /media/sf_JU_mayesha/Img/ExTracted File
File Actions Edit View Help
Make : OPPO
Camera Model Name : OPPO A95
Orientation : Horizontal (normal)
X Resolution : 72
Y Resolution : 72
Resolution Unit : inches
Modify Date : 2024:09:25 22:18:34
Y Cb Cr Positioning : Centered
Interoperability Index : R98 - DCF basic file (sRGB)
Interoperability Version : 1.0
Exposure Time : 1/17
F Number : 1.7
Exposure Program : Program AE
ISO : 2288
Exif Version : 0220
Date/Time Original : 2024:09:25 22:18:34
Create Date : 2024:09:25 22:18:34
Offset Time Original : +06:00
Components Configuration : Y, Cb, Cr, -
Shutter Speed Value : 1/17
Aperture Value : 1.7
Brightness Value : 42949668.68
Exposure Compensation : 0
Max Aperture Value : 1.7
Metering Mode : Center-weighted average
Flash : Off, Did not fire
Focal Length : 4.7 mm

```



```
root@kali: /media/sf_JU_mayesha/Img/ExTracted File
File Actions Edit View Help
Maker Note Unknown Text (Binary data 147 bytes, use -b option to extract)
Warning : Invalid EXIF text encoding for UserComment
User Comment : oplus_34
Sub Sec Time : 529
Sub Sec Time Original : 529
Sub Sec Time Digitized : 529
Flashpix Version : 0100
Color Space : sRGB
Exif Image Width : 0
Exif Image Height : 0
Sensing Method : Not defined
Scene Type : Directly photographed
Exposure Mode : Auto
White Balance : Auto
Focal Length In 35mm Format : 4 mm
Scene Capture Type : Standard
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)
```

```
root@kali: /media/sf_JU_mayesha/Img/ExTracted File
File Actions Edit View Help
Device Model :
Device Attributes : Reflective, Glossy, Positive, Color
Rendering Intent : Perceptual
Connection Space Illuminant : 0.9642 1 0.82491
Profile Creator : Apple Computer Inc.
Profile ID : 0
Profile Description : Display P3
Profile Copyright : Copyright Apple Inc., 2017
Media White Point : 0.95045 1 1.08905
Red Matrix Column : 0.51512 0.2412 -0.00105
Green Matrix Column : 0.29198 0.69225 0.04189
Blue Matrix Column : 0.1571 0.06657 0.78407
Red Tone Reproduction Curve : (Binary data 32 bytes, use -b option to extract)
Chromatic Adaptation : 1.04788 0.02292 -0.0502 0.02959 0.99048 -0.01706 -0.00923 0.01508 0.75168
Blue Tone Reproduction Curve : (Binary data 32 bytes, use -b option to extract)
Green Tone Reproduction Curve : (Binary data 32 bytes, use -b option to extract)
Image Width : 3000
Image Height : 4000
Encoding Process : Baseline DCT, Huffman coding
Bits Per Sample : 8
Color Components : 3
Y Cb Cr Sub Sampling : YCbCr4:2:0 (2 2)
Aperture : 1.7
```

```
root@kali: /media/sf_JU_mayesha/Img/ExTracted File
File Actions Edit View Help
01706 -0.00923 0.01508 0.75168 (3200 0 0)
Blue Tone Reproduction Curve : (Binary data 32 bytes, use -b option to extract)
Green Tone Reproduction Curve : (Binary data 32 bytes, use -b option to extract)
Image Width : 3000
Image Height : 4000
Encoding Process : Baseline DCT, Huffman coding
Bits Per Sample : 8
Color Components : 3
Y Cb Cr Sub Sampling : YCbCr4:2:0 (2 2)
Aperture : 1.7
Image Size : 3000x4000
Megapixels : 12.0
Scale Factor To 35 mm Equivalent: 0.8
Shutter Speed : 1/17
Create Date : 2024:09:25 22:18:34.529
Date/Time Original : 2024:09:25 22:18:34.529+06:00
Modify Date : 2024:09:25 22:18:34.529
Circle Of Confusion : 0.035 mm
Field Of View : 154.9 deg
Focal Length : 4.7 mm (35 mm equivalent: 4.0 mm)
Hyperfocal Distance : 0.37 m
Light Value : 1.1
```

## CASE 2:

1)Nmap: Network Mapper is an open source linux command that used to scan IP address and ports in a network.

2)

```
kali@kali: ~  
File Actions Edit View Help  
Primary Platform : Apple Computer Inc.  
(kali@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
Device inet 192.168.68.243 netmask 255.255.255.0 broadcast 192.168.68.255  
ether 08:00:27:c6:84:ab txqueuelen 1000 (Ethernet)  
Profile RX packets 22213 bytes 1876875 (1.7 MiB)  
Profile RX errors 0 dropped 91 overruns 0 frame 0  
Profile TX packets 121815 bytes 7371388 (7.0 MiB)  
Profile TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
Media White Point : 0.93845 1 1.06985  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
Device inet 127.0.0.1 netmask 255.0.0.0  
ether ::1 prefixlen 128 scopeid 0x10<host>  
loop txqueuelen 1000 (Local Loopback)  
Profile RX packets 4 bytes 240 (240.0 B)  
Profile RX errors 0 dropped 0 overruns 0 frame 0  
Profile TX packets 4 bytes 240 (240.0 B)  
Profile TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

3)

```
DEVICE MODEL :  
(kali@kali)-[~]  
$ nmap 192.168.68.216 : Reflective, Glossy, Positive, Color : Perceptual  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-05 03:29 EDT  
Nmap scan report for 192.168.68.216 Apple Computer Inc.  
Host is up (0.00090s latency). : 0  
Not shown: 991 closed tcp ports (conn-refused)  
PORT STATE SERVICE : Copyright Apple Inc., 2017  
22/tcp open ssh : 0.95045 1 1.08905  
80/tcp open http : 0.51512 0.2412 -0.00105  
139/tcp open netbios-ssn : 0.29198 0.69225 0.04189  
143/tcp open imap : 0.1571 0.06657 0.78407  
443/tcp open https : Curve : (Binary data 32 bytes, use -b option to ext  
445/tcp open microsoft-ds :  
5001/tcp open complex-link : 1.04788 0.02292 -0.0502 0.02959 0.99048 -0.  
8080/tcp open http-proxy : 75168  
8081/tcp open blackice-icecap : (Binary data 32 bytes, use -b option to ext  
ract)  
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds -b option to ext
```



4)

```
Device Model :  
(kali@kali)-[~]  
$ nmap -sV 192.168.68.216 -p 80 Perceptual  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-05 03:31 EDT  
Nmap scan report for 192.168.68.216 Apple Computer Inc.  
Host is up (0.00052s latency). : 0  
Profile Description : Display P3  
PORT STATE SERVICE VERSION : Copyright Apple Inc., 2017  
80/tcp open http Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1  
ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5  
mod_ssl/2.2.14 OpenSSL ... ) : 0.29198 0.69225 0.04189  
Blue Matrix Column : 0.1571 0.06657 0.78407  
Service detection performed. Please report any incorrect results at https://n  
map.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 6.21 seconds.02959 0.99048 -0.  
01706 -0.00923 0.01508 0.75168
```

5)

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nmap -A 192.168.68.216  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-05 03:32 EDT  
Nmap scan report for 192.168.68.216  
Host is up (0.0025s latency). : Reflective, Glossy, Positive, Color  
Not shown: 991 closed tcp ports (conn-refused)  
PORT STATE SERVICE VERSION : 0.9643 1 0.52491  
22/tcp open ssh OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; proto  
col 2.0) : 0  
| ssh-hostkey: : Display P3  
| 1024 ea:83:1e:45:5a:a6:8c:43:1c:3c:e3:18:dd:fc:88:a5 (DSA)  
| 2048 3a:94:d8:3f:e0:a2:7a:b8:c3:94:d7:5e:00:55:0c:a7 (RSA)  
80/tcp open http Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5  
.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/  
2.6.5 mod_ssl/2.2.14 OpenSSL ... ) : 0.1571 0.06657 0.78407  
| http-methods: : Binary data 32 bytes, use --b option to ext  
| Potentially risky methods: TRACE  
|_ http-server-header: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu  
4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ss  
l/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1  
|_ http-title: owaspbwa OWASP Broken Web Applications  
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) : 0  
143/tcp open imap Courier Imapd (released 2008)  
|_ imap-capabilities: IMAP4rev1 THREAD=REFERENCES IDLE ACL2=UNIONA0001 THREAD=  
ORDEREDSUBJECT completed CAPABILITY OK ACL UIDPLUS NAMESPACE CHILDREN SORT QU  
OTA : Baseline DCT, Huffman coding  
443/tcp open ssl/http Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5
```