Enhancing Digital Government and Economy
Mid Term Exam

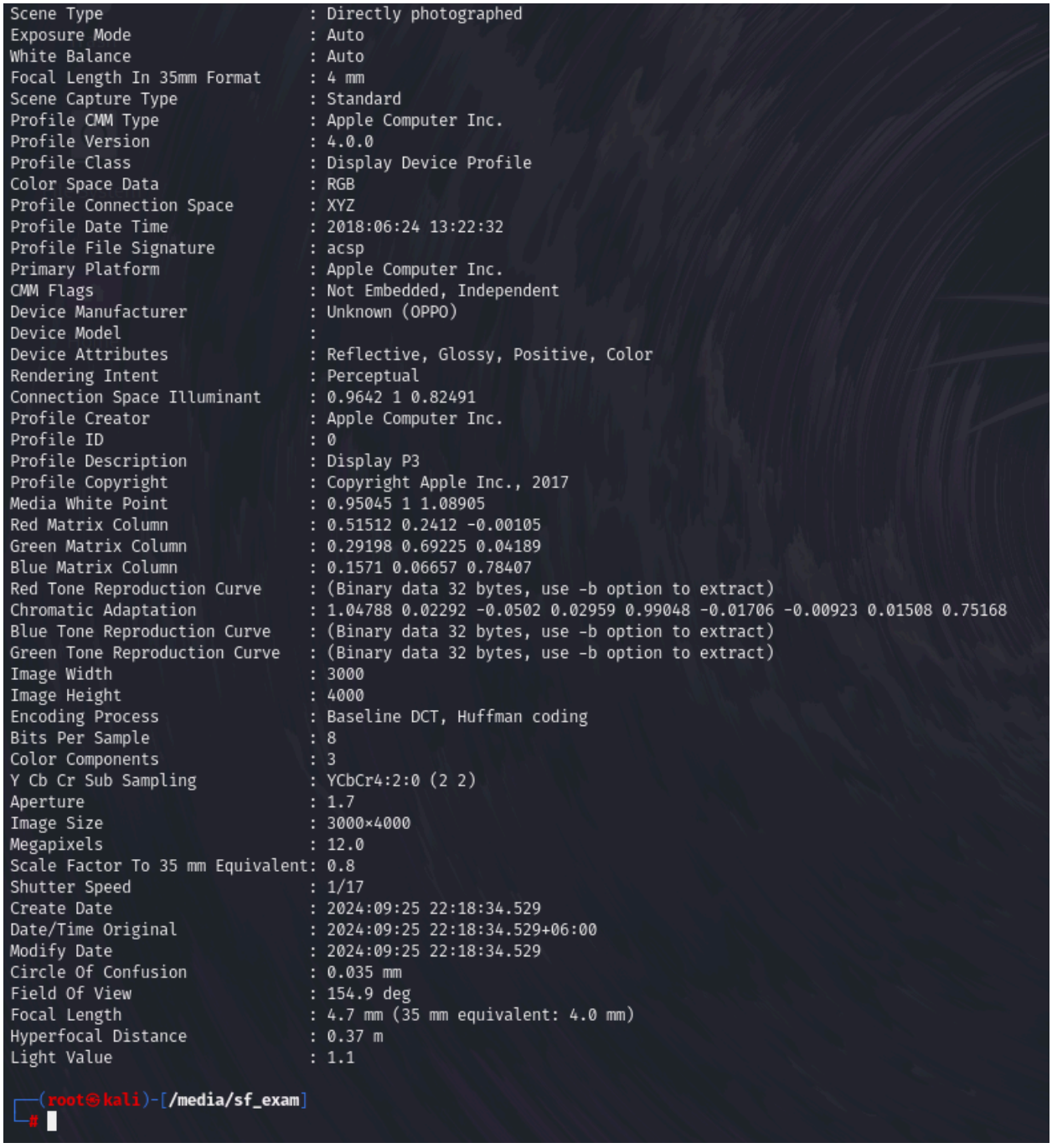
Submitted by,
Name: Koushiki Devi Agarwalla
Batch: JUR2B11
ID: 2111271

Institute Of Information Technology
Jahangirnagar University

Case-01

image 01

Information of this image:



```
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)
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
Image Size                      : 3000×4000
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

┌──(root㉿kali)-[/media/sf_exam]
└─#
```

1. **The photo was taken** - 2024-9-25
2. **Device Manufacture-** Unknown (OPPO)
3. **Encoding process**-Baseline DCT, Huffman coding
4. **Image height:** 4000
5. **Image taken** : 2024:09:25 22:18:34

Case 1

Image02

Image Information

6. **The photo was taken** - 2024-9-25
7. **Device Manufacture-** Unknown (OPPO)
8. **Encoding process**-Baseline DCT, Huffman coding
9. **Image height:** 4000

10. **Image taken** : 2024:09:25 21:16:00

Case 02

Target IP : 192.168.68.216

Ans. to the question no.1

Network Mapper(nmap) is an open-source instrument utilized for security auditing and network exploration. Users can use it to scan networks for devices that are in use, open ports, and services that are operating on those devices.

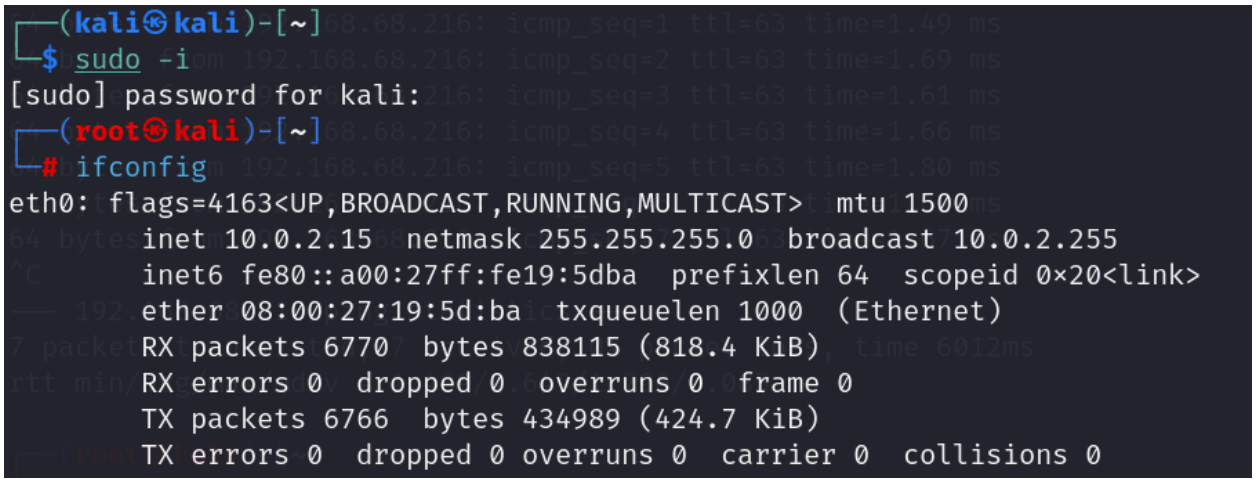
Nmap is an effective tool for network managers and security experts since it supports a variety of scanning methods, such as TCP, UDP, and stealth scans. Additionally, it contains a scripting engine (NSE) that enables users to create unique scripts for more sophisticated exploitation and scanning.

Nmap is useful for a number of things, such as:

- Device mapping on a network is known as network inventory.
- Finding vulnerabilities and misconfigurations through security auditing.
- Finding out which services and versions are operating on open ports is known as "service detection."

Ans. to the question no.2

To find machines own IP address ,the command used is : ifconfig



Ans. to the question no.3

Commands to find open ports on a target IP:
nmap <target ip>

```
┌──(root㉿kali)-[~]
└─# nmap 192.168.68.216
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-05 03:36 EDT
Nmap scan report for 192.168.68.216
Host is up (0.0044s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
143/tcp  open  imap
443/tcp  open  https
445/tcp  open  microsoft-ds
5001/tcp open  commplex-link
8080/tcp open  http-proxy
8081/tcp open  blackice-icecap

Nmap done: 1 IP address (1 host up) scanned in 4.82 seconds
```

Ans. to the question no.4

To find service version, command used: nmap -sV <target ip> -p 80

Service Version : STATE SERVICE VERSION

```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.68.216 -p 80
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-05 03:37 EDT
Nmap scan report for 192.168.68.216
Host is up (0.00050s latency).

PORT   STATE SERVICE VERSION
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 ... )

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.31 seconds
```

Ans. to the question no.5

To find operating system running on the machine, command used: nmap -sV <target ip> -O
Operating System : Linux