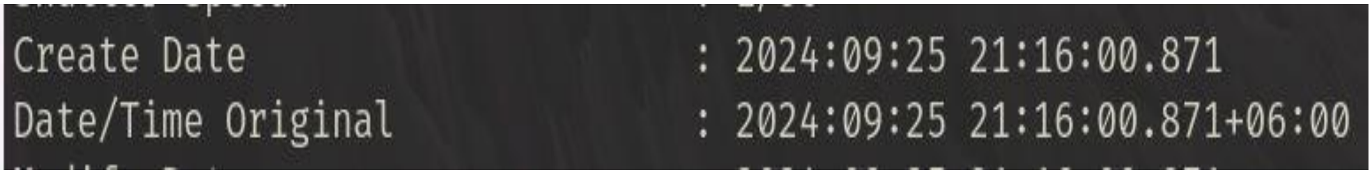
Mst. Sumiya Siddika

Id: 2111262

Case 1:

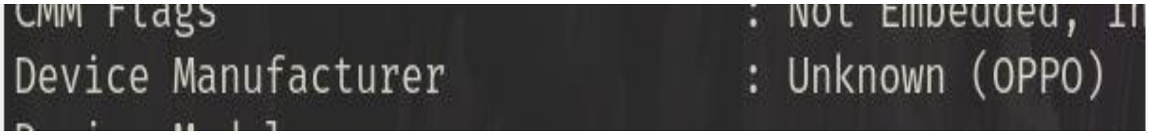
For image 1

Answer 01:



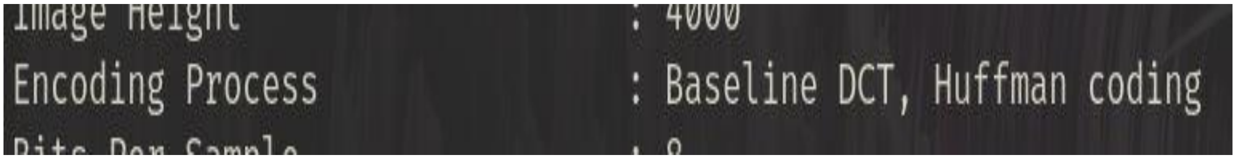
```
Create Date                     : 2024:09:25 21:16:00.871
Date/Time Original              : 2024:09:25 21:16:00.871+06:00
```

Answer 02:



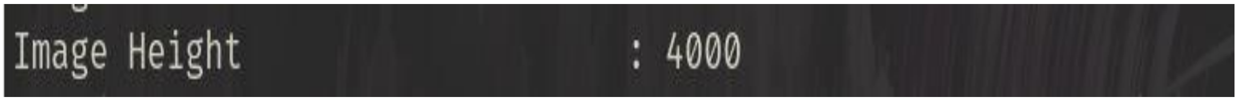
```
CMM Flags                       : Not Embedded, In
Device Manufacturer             : Unknown (OPPO)
```

Answer 03:



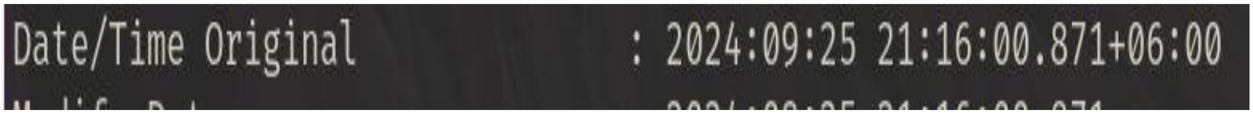
```
Image Height                    : 4000
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
```

Answer 04:



```
Image Height                    : 4000
```

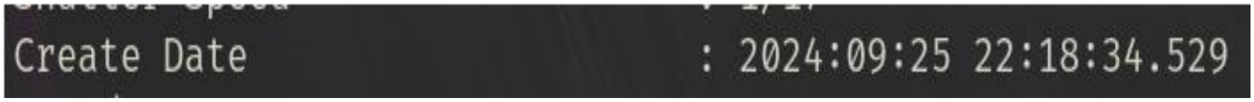
Answer 05:



```
Date/Time Original              : 2024:09:25 21:16:00.871+06:00
```

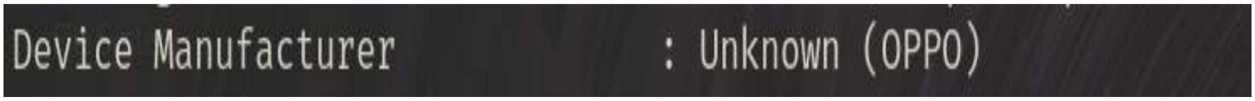
For image 2:

Answer 01:



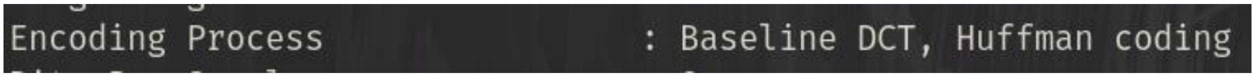
```
Create Date                     : 2024:09:25 22:18:34.529
```

Answer 02:



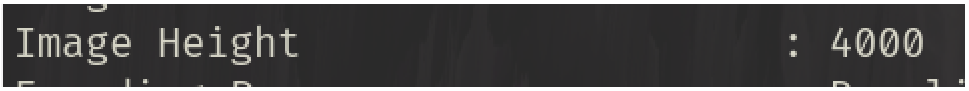
```
Device Manufacturer             : Unknown (OPPO)
```

Answer 03:



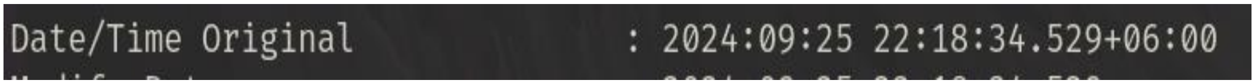
```
Encoding Process                : Baseline DCT, Huffman coding
```

Answer 04:



```
Image Height                    : 4000
```

Answer 05:



```
Date/Time Original              : 2024:09:25 22:18:34.529+06:00
```

Case 02:

Answer 01:

Nmap: Nmap (Network Mapper) is an open-source tool used for network exploration, security auditing, and vulnerability scanning. It is widely used by system administrators and security professionals to discover devices on a network, identify open ports, and determine the services and operating systems running on those devices.

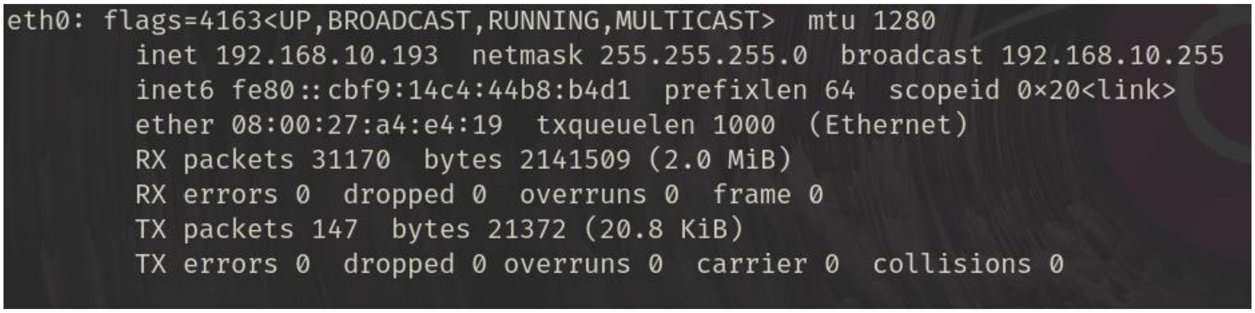
Key Features of Nmap:

1. **Host Discovery**: Identifies devices on a network by sending different types of probes to determine whether they are active.
2. **Port Scanning**: Determines which ports are open on a device, revealing available services.
3. **Service and Version Detection**: Identifies what services (and their versions) are running on open ports.
4. **OS Detection**: Uses a series of techniques to determine the operating system of the target device.
5. **Scriptable Interaction**: Nmap's scripting engine (NSE) allows for more advanced detection and vulnerability analysis by using Lua scripts.

6. **Network Inventory**: Can be used to create a detailed inventory of devices and services on a network.

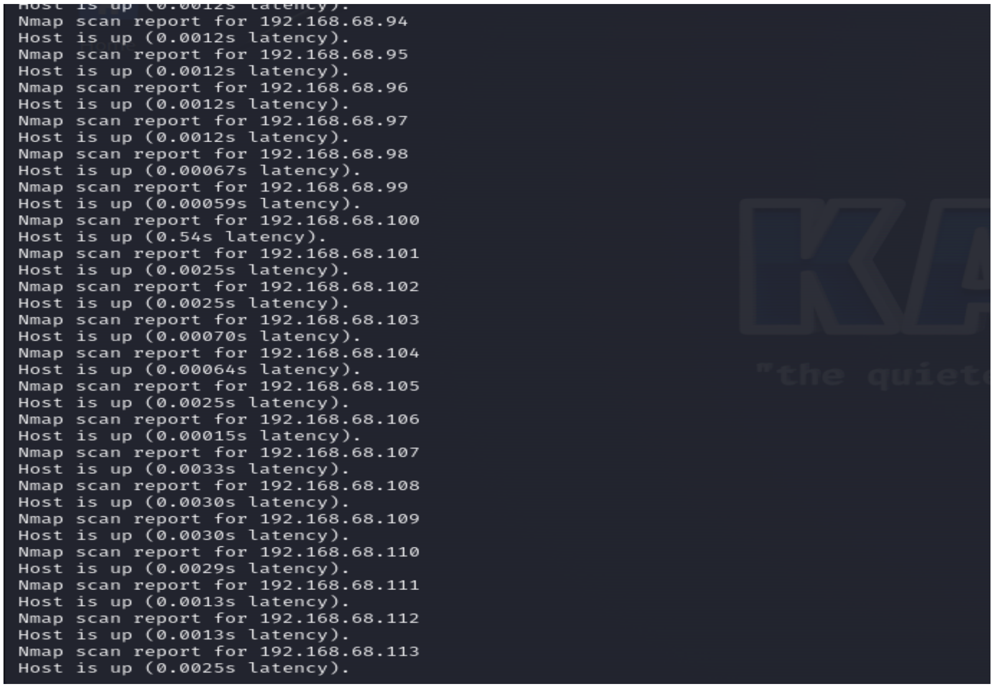
Nmap is a command-line tool, but it also has a graphical user interface called Zenmap. It is useful for network diagnostics, mapping out a network, and finding potential security vulnerabilities that can be exploited.

Answer 02:



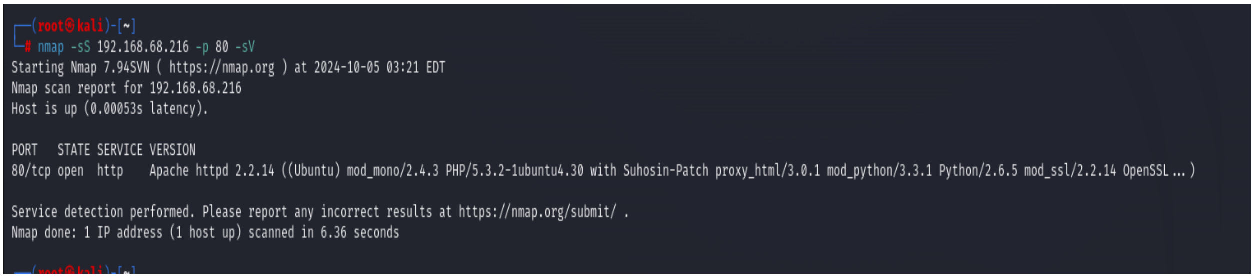
```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1280
        inet 192.168.10.193  netmask 255.255.255.0  broadcast 192.168.10.255
        inet6 fe80::cbf9:14c4:44b8:b4d1  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:a4:e4:19  txqueuelen 1000  (Ethernet)
        RX packets 31170  bytes 2141509 (2.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 147  bytes 21372 (20.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Answer 03:



```
Host is up (0.0012s latency).
Nmap scan report for 192.168.68.94
Host is up (0.0012s latency).
Nmap scan report for 192.168.68.95
Host is up (0.0012s latency).
Nmap scan report for 192.168.68.96
Host is up (0.0012s latency).
Nmap scan report for 192.168.68.97
Host is up (0.0012s latency).
Nmap scan report for 192.168.68.98
Host is up (0.00067s latency).
Nmap scan report for 192.168.68.99
Host is up (0.00059s latency).
Nmap scan report for 192.168.68.100
Host is up (0.54s latency).
Nmap scan report for 192.168.68.101
Host is up (0.0025s latency).
Nmap scan report for 192.168.68.102
Host is up (0.0025s latency).
Nmap scan report for 192.168.68.103
Host is up (0.00070s latency).
Nmap scan report for 192.168.68.104
Host is up (0.00064s latency).
Nmap scan report for 192.168.68.105
Host is up (0.0025s latency).
Nmap scan report for 192.168.68.106
Host is up (0.00015s latency).
Nmap scan report for 192.168.68.107
Host is up (0.0033s latency).
Nmap scan report for 192.168.68.108
Host is up (0.0030s latency).
Nmap scan report for 192.168.68.109
Host is up (0.0030s latency).
Nmap scan report for 192.168.68.110
Host is up (0.0029s latency).
Nmap scan report for 192.168.68.111
Host is up (0.0013s latency).
Nmap scan report for 192.168.68.112
Host is up (0.0013s latency).
Nmap scan report for 192.168.68.113
Host is up (0.0025s latency).
```

Answer 04:



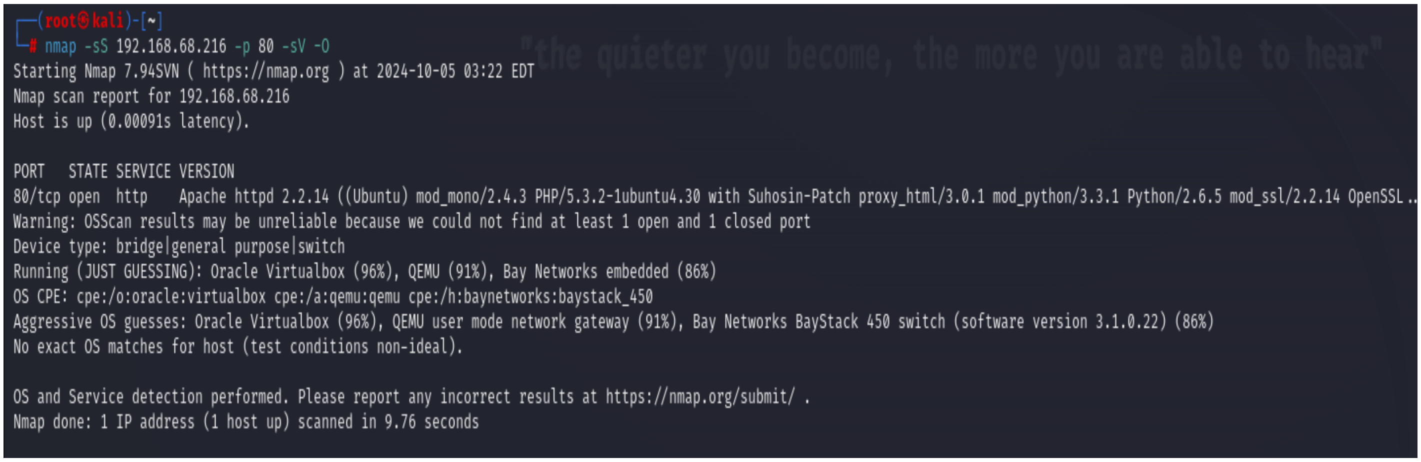
```
┌──(root㉿kali)-[~]
└─# nmap -sS 192.168.68.216 -p 80 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-05 03:21 EDT
Nmap scan report for 192.168.68.216
Host is up (0.00053s latency).

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 6.36 seconds

┌──(root㉿kali)-[~]
```

Answer 05:



```
┌──(root㉿kali)-[~]
└─# nmap -sS 192.168.68.216 -p 80 -sV -O
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-05 03:22 EDT
Nmap scan report for 192.168.68.216
Host is up (0.00091s 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 ..
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (91%), Bay Networks embedded (86%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (91%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (86%)
No exact OS matches for host (test conditions non-ideal).

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.76 seconds
```