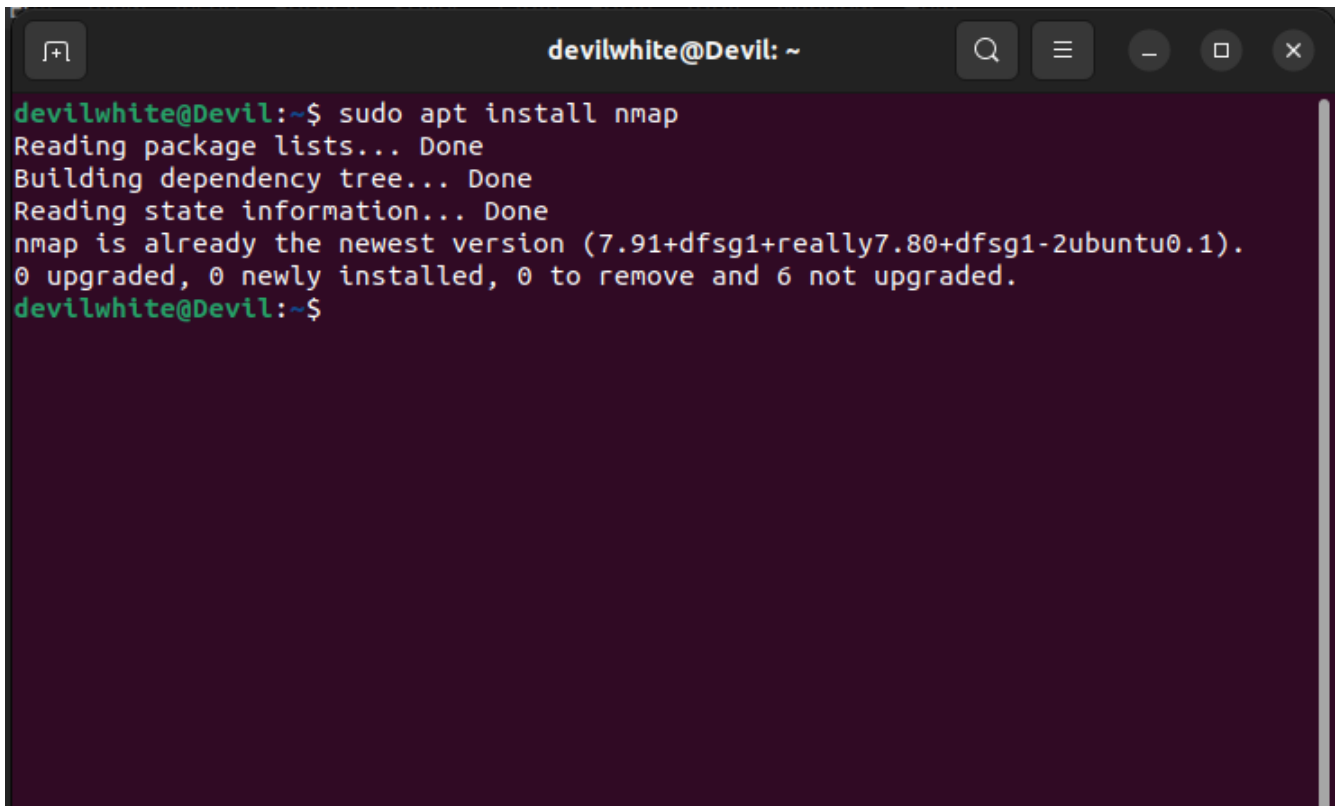


# Cyber Security Intermediate Tasks

## Task 1: Perform a Basic Vulnerability Scan

- Install Nmap: use the following command to install Nmap

`sudo apt install nmap`

A terminal window with a dark purple background. The title bar at the top reads "devilwhite@Devil: ~" and includes standard window controls (minimize, maximize, close) on the right. The terminal text shows the command "sudo apt install nmap" being executed. The output indicates that nmap is already the newest version (7.91) and that 0 packages were upgraded, 0 newly installed, 0 to be removed, and 6 not upgraded. The prompt returns to "devilwhite@Devil:~\$".

```
devilwhite@Devil:~$ sudo apt install nmap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nmap is already the newest version (7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1).
0 upgraded, 0 newly installed, 0 to remove and 6 not upgraded.
devilwhite@Devil:~$
```

- Perform a Scan with Nmap

Ping scan: use the following command to detect the live hosts on the network

`nmap -sn <network_ip_range>`

```
devilwhite@Devil: ~  
devilwhite@Devil:~$ sudo apt install nmap  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
nmap is already the newest version (7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1).  
0 upgraded, 0 newly installed, 0 to remove and 6 not upgraded.  
devilwhite@Devil:~$ nmap -sn 192.168.0.121/24  
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-06 05:47 PKT  
Nmap scan report for 192.168.0.1 (192.168.0.1)  
Host is up (0.033s latency).  
Nmap scan report for 192.168.0.102 (192.168.0.102)  
Host is up (0.22s latency).  
Nmap scan report for 192.168.0.105 (192.168.0.105)  
Host is up (1.2s latency).  
Nmap scan report for 192.168.0.107 (192.168.0.107)  
Host is up (0.019s latency).  
Nmap scan report for 192.168.0.121 (192.168.0.121)  
Host is up (0.00064s latency).  
Nmap done: 256 IP addresses (5 hosts up) scanned in 16.65 seconds  
devilwhite@Devil:~$
```

- Service Version Detection and OS Scan:

`sudo nmap -sS -sV -O <target_ip>`

```
devilwhite@Devil: ~  
devilwhite@Devil:~$ sudo nmap -sS -sV -O -Pn 192.168.0.102  
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-06 06:06 PKT  
Nmap scan report for 192.168.0.102 (192.168.0.102)  
Host is up (0.019s latency).  
All 1000 scanned ports on 192.168.0.102 (192.168.0.102) are closed  
MAC Address: D6:73:60:3C:CF:90 (Unknown)  
Too many fingerprints match this host to give specific OS details  
Network Distance: 1 hop  
  
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 4.92 seconds  
devilwhite@Devil:~$ sudo nmap -sS -sV -O -Pn 192.168.0.104  
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-06 06:07 PKT  
Nmap scan report for 192.168.0.104 (192.168.0.104)  
Host is up (0.028s latency).  
All 1000 scanned ports on 192.168.0.104 (192.168.0.104) are closed  
MAC Address: 74:C1:7D:BC:B6:77 (Infinix mobility limited)  
Too many fingerprints match this host to give specific OS details  
Network Distance: 1 hop  
  
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 24.23 seconds
```

Nmap done: 1 IP address (1 host up) scanned in 4.32 seconds

devilwhite@Devil:~\$ sudo nmap -sS -sV -O 192.168.0.121

Starting Nmap 7.80 ( <https://nmap.org> ) at 2024-10-06 06:05 PKT

Nmap scan report for 192.168.0.121 (192.168.0.121)

Host is up (0.00030s latency).

Not shown: 998 closed ports

| PORT | STATE | SERVICE | VERSION |
|------|-------|---------|---------|
|------|-------|---------|---------|

|        |      |      |                                |
|--------|------|------|--------------------------------|
| 80/tcp | open | http | Apache httpd 2.4.52 ((Ubuntu)) |
|--------|------|------|--------------------------------|

|         |      |                 |  |
|---------|------|-----------------|--|
| 902/tcp | open | ssl/vmware-auth | VMware Authentication Daemon 1.10 (Uses VNC, SOAP) |
|---------|------|-----------------|--|

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux\_kernel:2.6.32

OS details: Linux 2.6.32

Network Distance: 0 hops

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 9.56 seconds

devilwhite@Devil:~\$ sudo nmap -sS -sV -O 192.168.0.1

Starting Nmap 7.80 ( <https://nmap.org> ) at 2024-10-06 06:05 PKT

Nmap scan report for 192.168.0.1 (192.168.0.1)

Host is up (0.013s latency).

Not shown: 997 closed ports

| PORT | STATE | SERVICE | VERSION |
|------|-------|---------|---------|
|------|-------|---------|---------|

|        |      |     |                                      |
|--------|------|-----|--------------------------------------|
| 22/tcp | open | ssh | Dropbear sshd 2012.55 (protocol 2.0) |
|--------|------|-----|--------------------------------------|

|        |      |      |                             |
|--------|------|------|-----------------------------|
| 80/tcp | open | http | TP-LINK TD-W8968 http admin |
|--------|------|------|-----------------------------|

|          |      |      |   |
|----------|------|------|---|
| 1900/tcp | open | upnp | Portable SDK for UPnP devices 1.6.19 (Linux 2.6.36; UPnP 1.0) |
|----------|------|------|---|

MAC Address: B0:4E:26:7F:D8:F2 (Tp-link Technologies)

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux\_kernel:2.6

OS details: Linux 2.6.23 - 2.6.38

Network Distance: 1 hop

Service Info: OS: Linux; Device: WAP; CPE: cpe:/o:linux:linux\_kernel, cpe:/h:tp-link:td-w8968, cpe:/o:linux:linux\_kernel:2.6.36

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 12.58 seconds

- **Vulnerability Scan:** Use Nmap scripts (NSE scripts) for more in-depth analysis:

**Sudo nmap --script vuln <target\_ip>**

```
devilwhite@Devil: ~  
Host is up (0.052s latency).  
Nmap scan report for 192.168.0.121 (192.168.0.121)  
Host is up (0.0014s latency).  
Nmap done: 256 IP addresses (5 hosts up) scanned in 4.55 seconds  
devilwhite@Devil:~$ sudo nmap --script vuln 192.168.0.102  
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-06 06:15 PKT  
Nmap scan report for 192.168.0.102 (192.168.0.102)  
Host is up (0.011s latency).  
All 1000 scanned ports on 192.168.0.102 (192.168.0.102) are closed  
MAC Address: D6:73:60:3C:CF:90 (Unknown)  
  
Nmap done: 1 IP address (1 host up) scanned in 12.87 seconds  
devilwhite@Devil:~$ sudo nmap --script vuln 192.168.0.121  
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-06 06:15 PKT  
Nmap scan report for 192.168.0.121 (192.168.0.121)  
Host is up (0.000036s latency).  
Not shown: 998 closed ports  
PORT      STATE SERVICE  
80/tcp    open  http  
|_clamav-exec: ERROR: Script execution failed (use -d to debug)  
|_http-csrf: Couldn't find any CSRF vulnerabilities.  
|_http-dombased-xss: Couldn't find any DOM based XSS.  
|_http-enum:  
|_ /server-status/: Potentially interesting folder  
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.  
902/tcp   open  iss-realsecure  
|_clamav-exec: ERROR: Script execution failed (use -d to debug)  
  
Nmap done: 1 IP address (1 host up) scanned in 32.21 seconds
```

## Scan Summary

- **Host Status:** The host is up, with a very low latency.
- **Open Ports:**
  - **80/tcp:** Running HTTP
  - **902/tcp:** Running ISS RealSecure

## Script Execution Errors

- **clamav-exec:** This script failed during execution, which might indicate an issue with the script or the service configuration.
- **http-csrf:** No CSRF vulnerabilities were found.
- **http-dombased-xss:** No DOM-based XSS vulnerabilities were found.
- **http-stored-xss:** No stored XSS vulnerabilities were found.

- **http-enum:** The /server-status/ endpoint was flagged as a potentially interesting folder, which could be worth investigating further.

### Debugging the Script Execution:

```
devilwhite@Devil: ~  
devilwhite@Devil:~$ sudo nmap --script vuln -d 192.168.0.121  
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-06 06:17 PKT  
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)  
----- Timing report -----  
  hostgroups: min 1, max 100000  
  rtt-timeouts: init 1000, min 100, max 10000  
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000  
  parallelism: min 0, max 0  
  max-retries: 10, host-timeout: 0  
  min-rate: 0, max-rate: 0  
-----  
NSE: Using Lua 5.3.  
NSE: Arguments from CLI:  
NSE: Loaded 105 scripts for scanning.  
NSE: Script Pre-scanning.  
NSE: Starting runlevel 1 (of 2) scan.  
Initiating NSE at 06:17  
NSE: Starting broadcast-avahi-dos.  
NSE: [broadcast-avahi-dos] dns.query() got zero responses attempting to resolve  
query: _services._dns-sd._udp.local  
NSE: Finished broadcast-avahi-dos.  
Completed NSE at 06:18, 10.00s elapsed  
NSE: Starting runlevel 2 (of 2) scan.  
Initiating NSE at 06:18  
Completed NSE at 06:18, 0.00s elapsed  
mass_rdns: Using DNS server 127.0.0.53  
Initiating Parallel DNS resolution of 1 host. at 06:18  
mass_rdns: 0.01s 0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]  
Completed Parallel DNS resolution of 1 host. at 06:18, 0.00s elapsed  
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF:
```

```
devilwhite@Devil: ~  
NSE: Finished http-cookie-flags against 192.168.0.121:80.  
Completed NSE at 06:18, 0.01s elapsed  
Nmap scan report for 192.168.0.121 (192.168.0.121)  
Host is up, received localhost-response (0.000036s latency).  
Scanned at 2024-10-06 06:18:08 PKT for 21s  
Not shown: 998 closed ports  
Reason: 998 resets  
PORT      STATE SERVICE      REASON  
80/tcp    open  http         syn-ack ttl 64  
|_ http-csrf: Couldn't find any CSRF vulnerabilities.  
|_ http-dombased-xss: Couldn't find any DOM based XSS.  
|_ http-enum:  
|_ /server-status/: Potentially interesting folder  
|_ http-iis-webdav-vuln:  
|_ ERROR: This web server is not supported.  
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.  
902/tcp   open  iss-realsecure syn-ack ttl 64  
Final times for host: srtt: 36 rttvar: 7  to: 100000  
  
NSE: Script Post-scanning.  
NSE: Starting runlevel 1 (of 2) scan.  
Initiating NSE at 06:18  
Completed NSE at 06:18, 0.00s elapsed  
NSE: Starting runlevel 2 (of 2) scan.  
Initiating NSE at 06:18  
Completed NSE at 06:18, 0.00s elapsed  
Read from /usr/bin/./share/nmap: nmap-payloads nmap-services.  
Nmap done: 1 IP address (1 host up) scanned in 32.94 seconds  
Raw packets sent: 1000 (44.000KB) | Rcvd: 2002 (84.088KB)  
devilwhite@Devil:~$
```

The scan output indicates several points of interest:

### 1. Open Ports Discovered:

- **Port 80 (HTTP):** The most common port for web services.
- **Port 902:** Typically associated with VMware services.

### 2. Scripts Executed:

- Various scripts targeting known vulnerabilities in web applications, including checks for specific CVEs (Common Vulnerabilities and Exposures).

### 3. Key Findings:

- The Nmap output mentions that the site might not be vulnerable to certain attacks, like the `http-vuln-cve2013-7091`.
- Several checks, such as `http-vuln-cve2015-1427` and others, indicated that either the service is not running or the server is configured to prevent such attacks (e.g., returning a 404 Not Found).

#### 4. Errors:

- There are some errors related to the `clamav-exec` and `firewall-bypass` scripts indicating incorrect port specifications or issues connecting to helper ports.

#### 5. HTTP Responses:

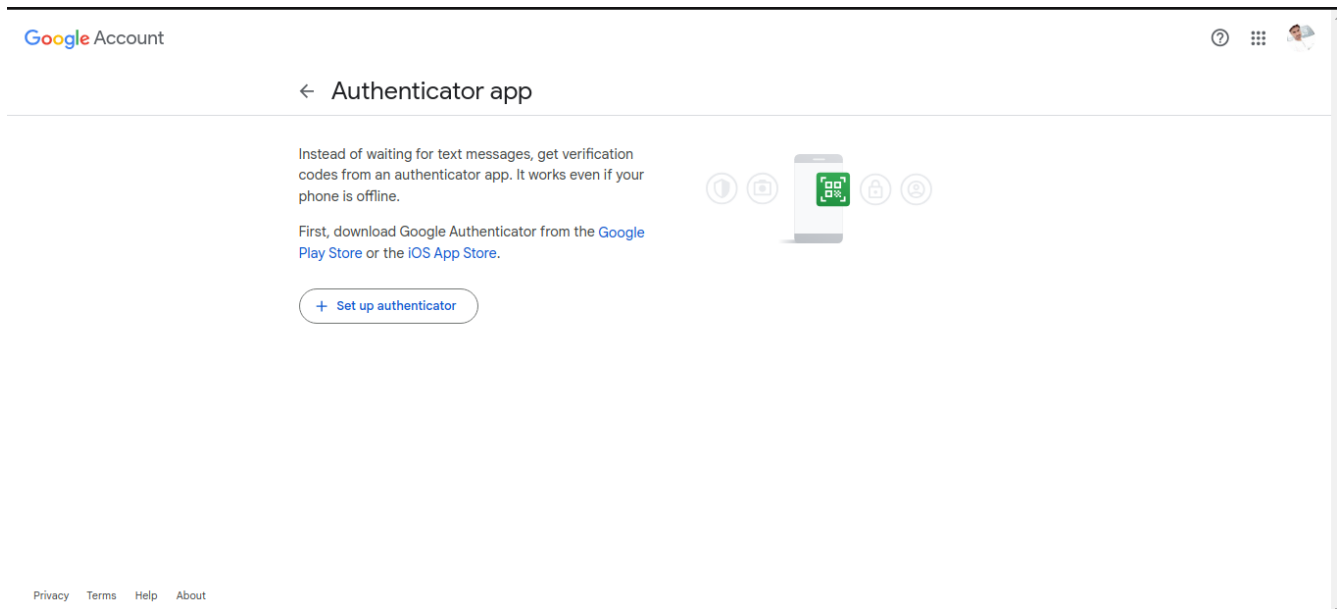
- Responses from the server for various checks suggest that certain methods (like `DEBUG` for ASP.NET) are not supported, and some paths return a 404 status, indicating they do not exist.

#### Recommendations:

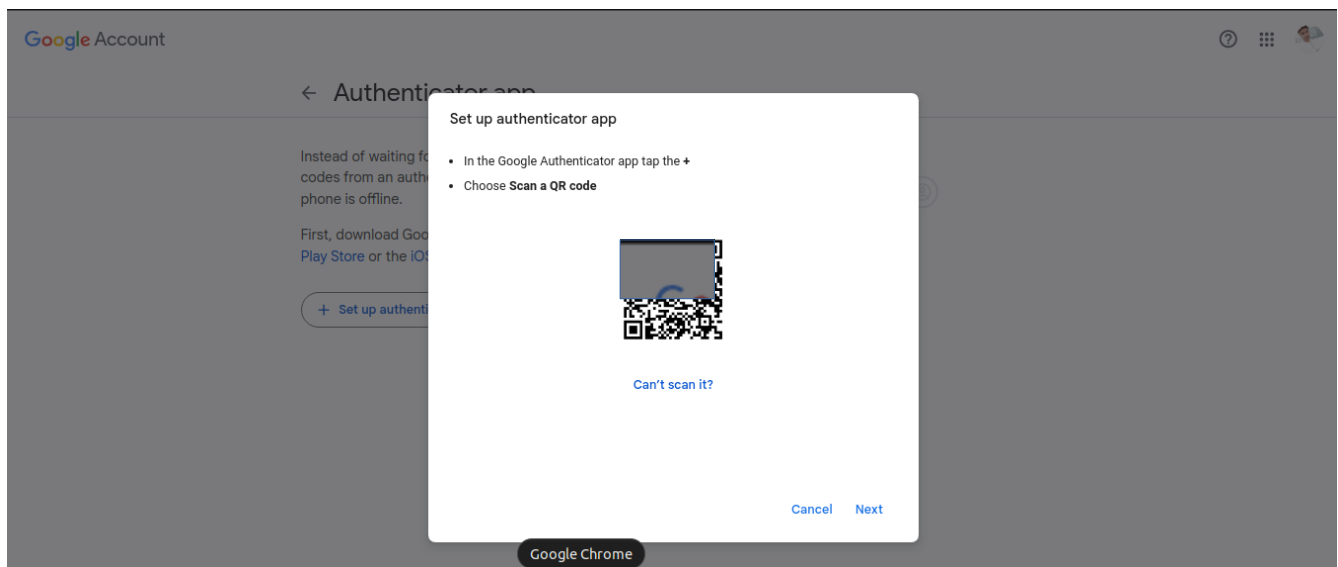
- **Further Testing:** Depending on the context, you may want to try more specific scripts related to the services running on the open ports, especially on port 80.
- **Review Configuration:** If this is your server, review its security configurations to ensure it's hardened against attacks.
- **Monitoring:** Implement monitoring to detect any suspicious activities or potential breaches in real time.

## Task 2: Implement Two-Factor Authentication (2FA)

- **Email/Gmail:**

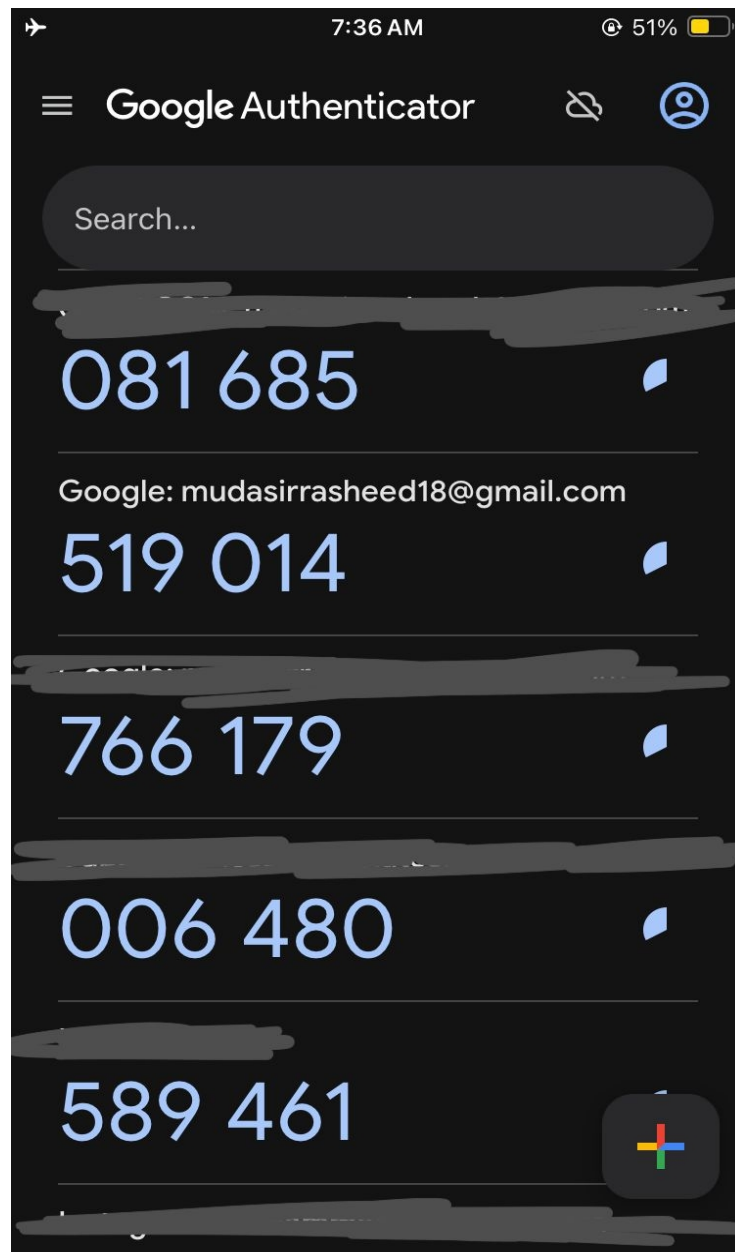


- **Scan QR code:-**



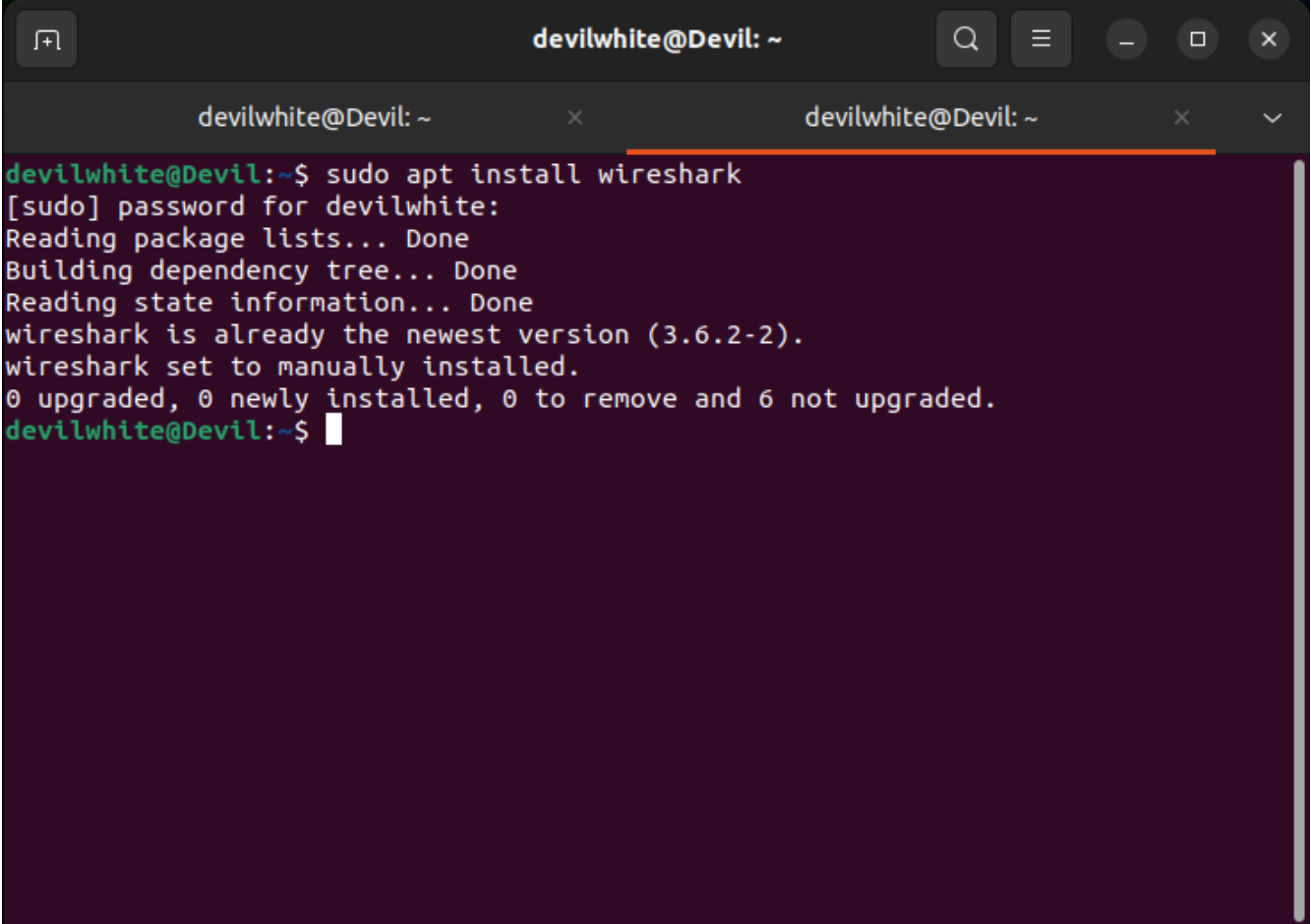


Scan QR and press next to enter code generated by Authentication app we will see the screen like below:-



### Task 3: Analyze Network Traffic

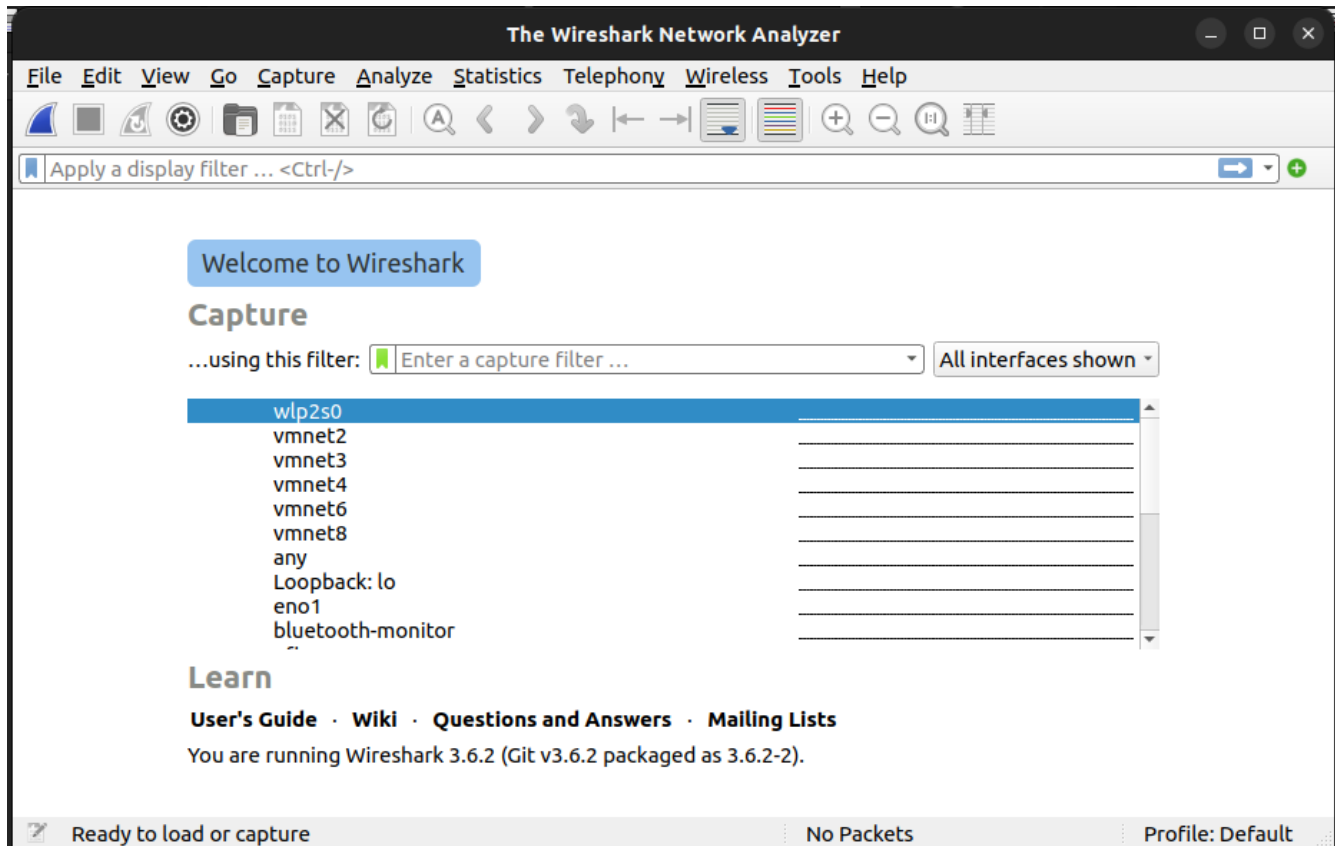
- **Step 1: Install Wireshark:** use the following command to install WireShark  
`sudo apt install wireshark`

A terminal window titled 'devilwhite@Devil: ~' with standard window controls. The terminal shows the execution of 'sudo apt install wireshark'. It prompts for a password, then displays the progress of package list reading, dependency tree building, and state information reading, all marked as 'Done'. It then reports that 'wireshark is already the newest version (3.6.2-2)' and 'wireshark set to manually installed.' Finally, it shows the summary: '0 upgraded, 0 newly installed, 0 to remove and 6 not upgraded.' The prompt returns to 'devilwhite@Devil:~\$' with a cursor.

```
devilwhite@Devil:~$ sudo apt install wireshark
[sudo] password for devilwhite:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
wireshark is already the newest version (3.6.2-2).
wireshark set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 6 not upgraded.
devilwhite@Devil:~$
```

- **Step 2: Capture Network Traffic**

To capture packets, open Wireshark: Start Wireshark and select the network interface you want to capture (e.g., eth0, wlan0, wlp2s0).



Double click on the interface and capturing will start and looks like the following:-

The image shows the Wireshark network protocol analyzer interface. The title bar indicates the capture interface is \*wlp2s0. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains icons for various functions like packet capture, zoom, and packet list management. Below the toolbar is a filter bar with the text 'Apply a display filter ... <Ctrl-/>'. The main packet list pane shows a single entry for packet 24190, which is an ICMP packet from source 192.168.0.121 to destination 192.168.0.1. The packet details pane shows the frame structure: Frame 24190: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface wlp2s0. The packet structure includes Interface id: 0 (wlp2s0), Encapsulation type: Ethernet (1), Arrival Time: Oct 6, 2024 03:45:57.578493007 PKT, [Time shift for this packet: 0.000000000 seconds], Epoch Time: 1728168357.578493007 seconds, and [Time delta from previous captured frame: 0.000133185 seconds]. The packet bytes pane shows the raw data in hexadecimal and ASCII. The status bar at the bottom indicates the file is wireshark\_wlp2s0LQ2DV2.pcapng, with 210136 packets displayed (100.0%) using the Default profile.

| No.   | Time         | Source        | Destination | Protocol | Length | Info        |
|-------|--------------|---------------|-------------|----------|--------|-------------|
| 24190 | 32.107863759 | 192.168.0.121 | 192.168.0.1 | ICMP     | 102    | Destination |

Frame 24190: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface wlp2s0

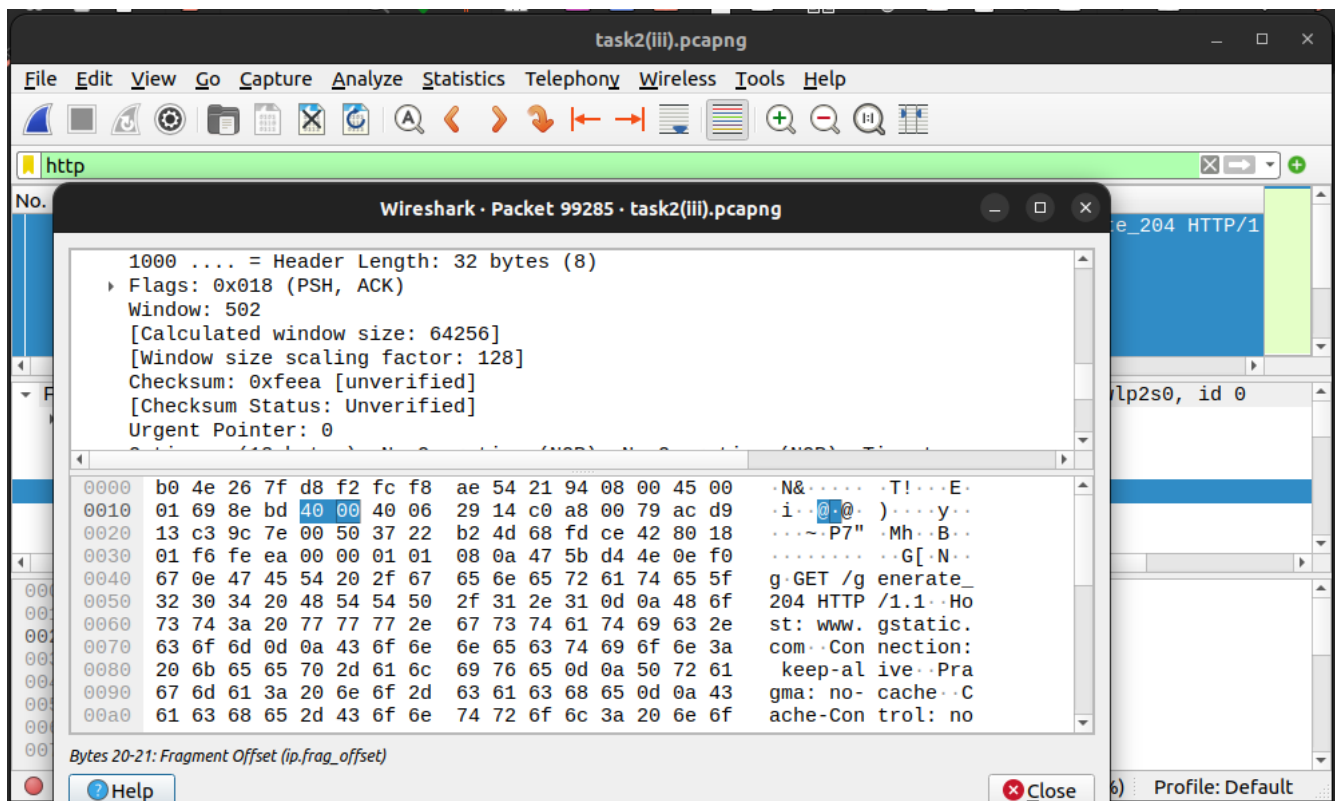
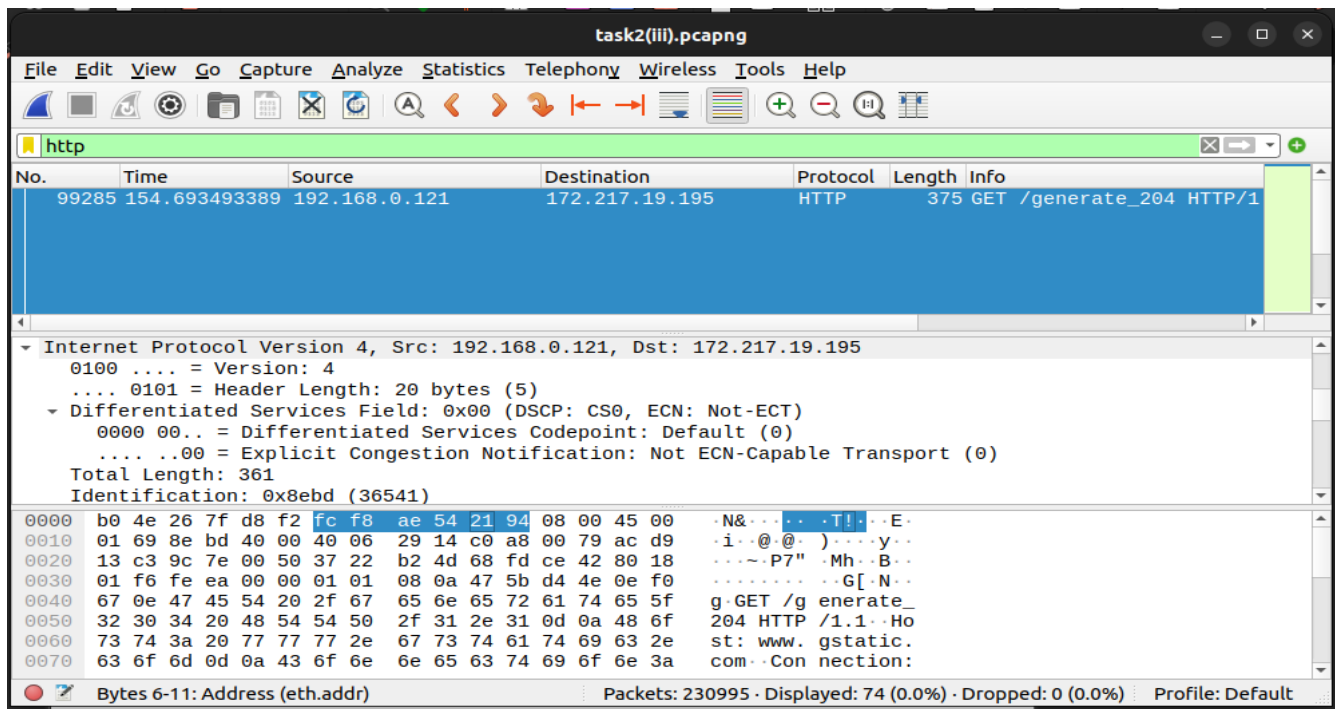
- Interface id: 0 (wlp2s0)
- Encapsulation type: Ethernet (1)
- Arrival Time: Oct 6, 2024 03:45:57.578493007 PKT
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1728168357.578493007 seconds
- [Time delta from previous captured frame: 0.000133185 seconds]

0000 b0 4e 26 7f d8 f2 fc f8 ae 54 21 94 08 00 45 c0 .N&... .T!...E.  
0010 00 58 f6 12 00 00 40 01 02 08 c0 a8 00 79 c0 a8 .X....@. ....y..  
0020 00 01 03 03 7f 01 00 00 00 00 45 00 00 3c 00 00 .....E.<..  
0030 40 00 3f 11 b9 e6 c0 a8 00 01 c0 a8 00 79 00 35 @.?. ....y.5  
0040 aa ad 00 28 0c d0 c0 d4 81 85 00 01 00 00 00 00 ...(. ....  
0050 00 00 03 63 64 6e 06 67 62 71 6f 66 73 03 63 6f ...cdn.g bqofs.co  
0060 6d 00 00 41 00 01 m..A..

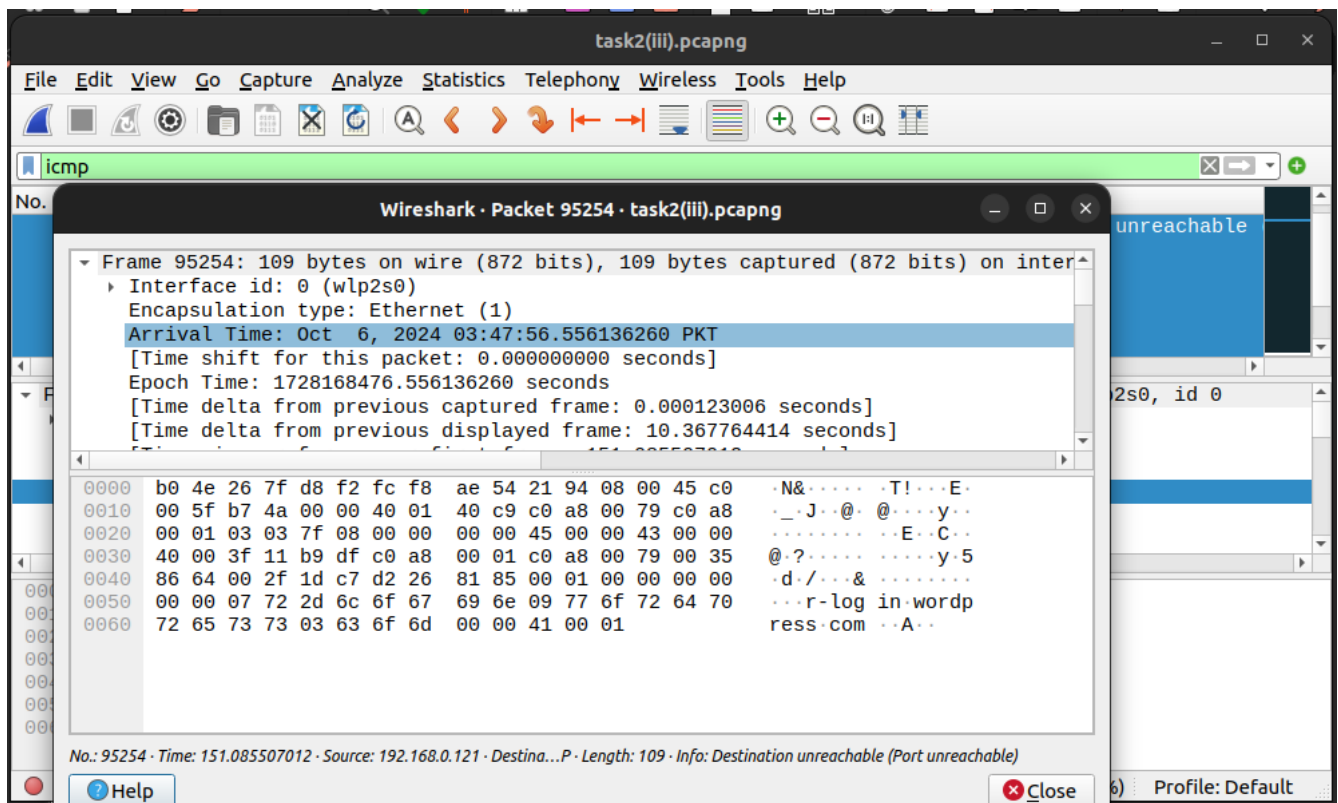
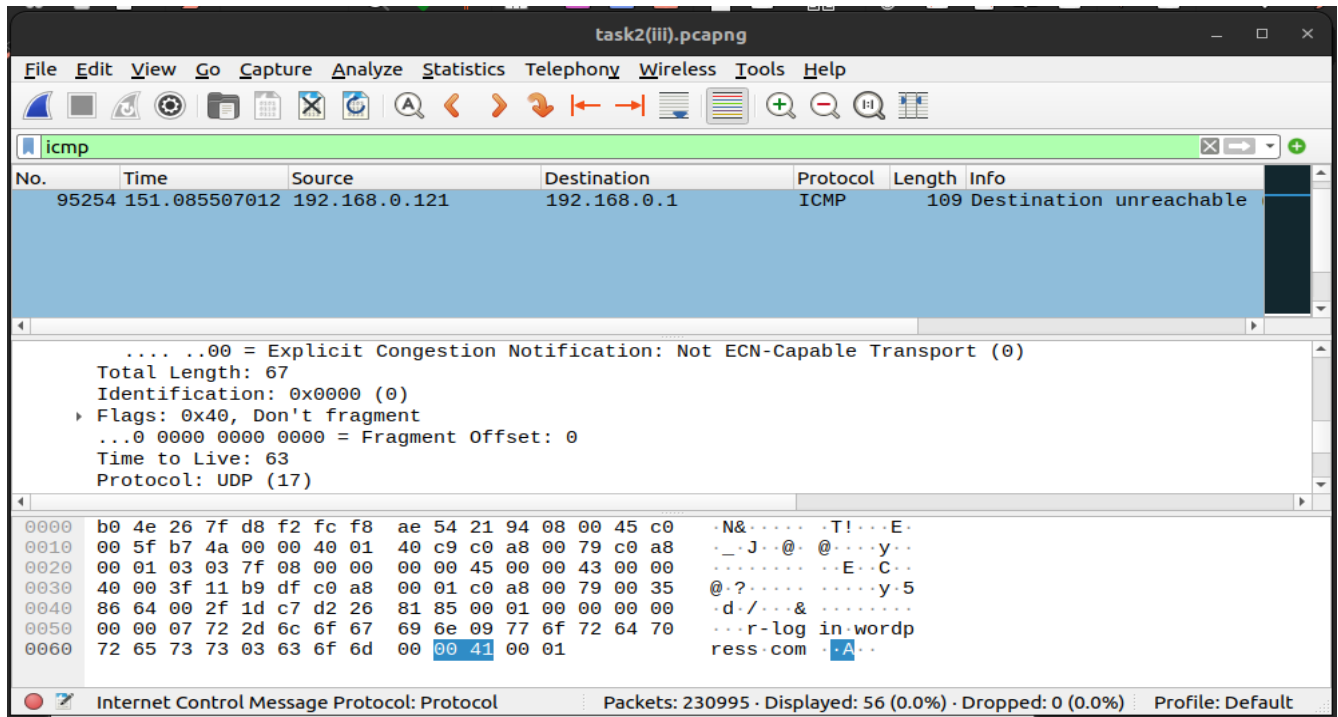
wireshark\_wlp2s0LQ2DV2.pcapng Packets: 210136 · Displayed: 210136 (100.0%) Profile: Default

- **Step 3: Analyze Captured Packets**
- **Filter Packets:** To narrow down analysis, we can filter by protocol.

To capture HTTP traffic: write http in the search box



To capture ICMP traffic (ping): write ICMP in the search box



For TCP & UDP traffic on port 80: write `tcp.port == 80 || udp.port == 80`

The image shows a Wireshark window titled "task2(iii).pcapng". The filter bar at the top contains the expression `tcp.port == 80 || udp.port == 80`. The packet list shows a single packet, No. 95252, at time 151.081925868, from source 192.168.0.121 to destination 45.135.106.143, protocol TCP, length 66. The packet details pane shows the following information:

- Destination Address: 45.135.106.143
- Transmission Control Protocol, Src Port: 45648, Dst Port: 873, Seq: 121, Ack: 140182809, Len: 0
- Source Port: 45648
- Destination Port: 873
- [Stream index: 0]
- [Conversation completeness: Incomplete (28)]
- [TCP Segment Len: 0]
- Sequence Number: 121 (relative sequence number)

The packet bytes pane shows the raw data of the TCP segment, starting with the sequence number 121 in hexadecimal (f8 f8 ae).

At the bottom, the status bar indicates: Transmission Control Protocol: Protocol, Packets: 230995, Displayed: 199504 (86.4%), Dropped: 0 (0.0%), Profile: Default.

The image shows the same Wireshark window, but with a packet details pane open for packet 99209. The filter bar still contains `tcp.port == 80 || udp.port == 80`. The packet list shows packet No. 99209 at time 154.6427342. The packet details pane shows the following information:

- Internet Protocol Version 4, Src: 192.168.0.121, Dst: 172.217.19.195
- 0100 .... = Version: 4
- .... 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- 0000 00.. = Differentiated Services Codepoint: Default (0)
- .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
- Total Length: 60
- Identification: 0x8ebb (36539)

The packet bytes pane shows the raw data of the IP packet, starting with the version 4 in hexadecimal (b0 4e 26 7f d8 f2 fc f8 ae).

At the bottom, the status bar indicates: Time shift applied, Packets: 230995, Displayed: 199504 (86.4%), Dropped: 0 (0.0%), Profile: Default.

- **Analyze Protocols:**
  - **TCP:** Ensure three-way handshakes and proper packet sequencing.
  - **HTTP/HTTPS:** Look at HTTP requests and responses. For HTTPS, the data will be encrypted.
  - **DNS:** You can observe DNS queries and responses.
  - **FTP, SSH:** Identify clear-text communication if applicable.