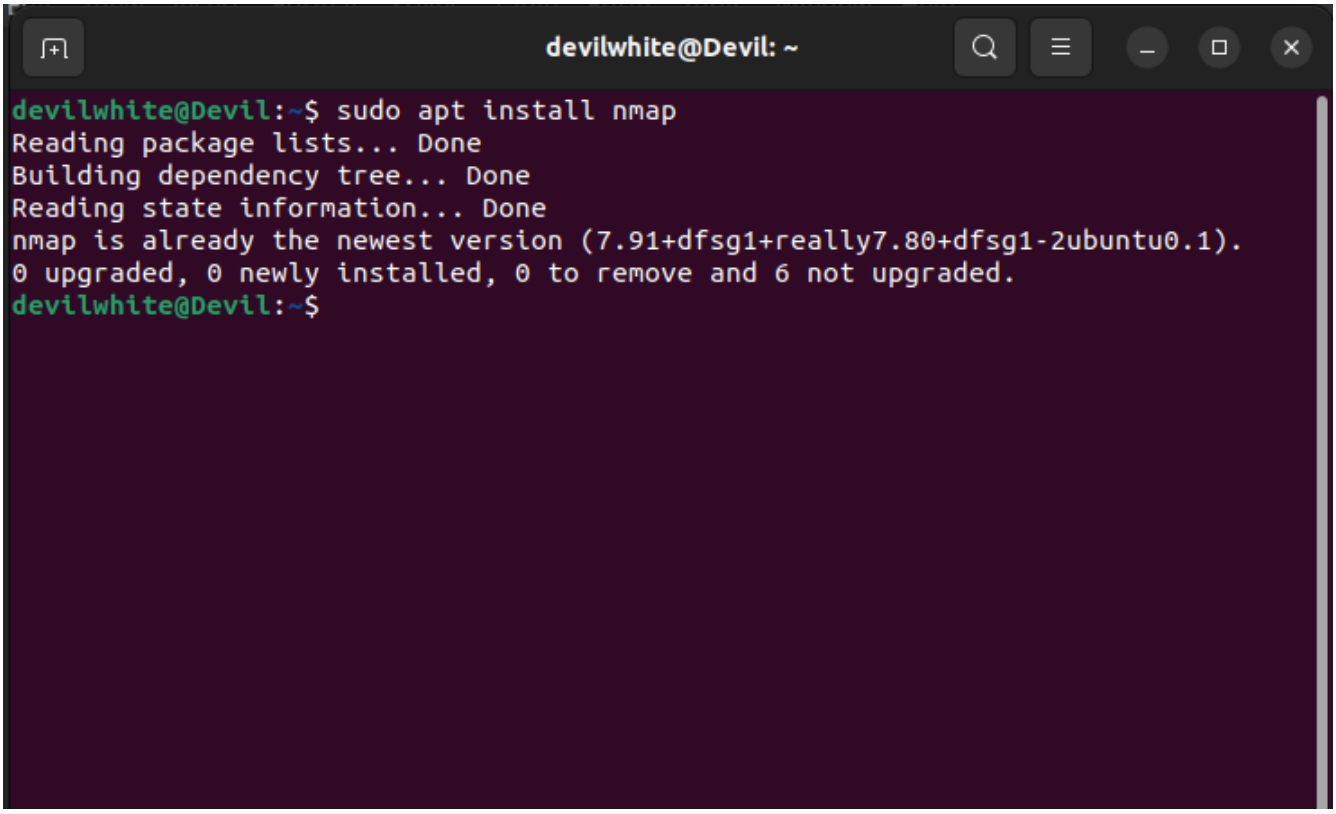
Cyber Security Intermediate Tasks

Task 1: Perform a Basic Vulnerability Scan

- **Install Nmap: use the following command to install Nmap**

  sudo apt install nmap



- **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
```

devilwhite@Devil: ~

```
Nmap done: 1 IP address (1 host up) scanned in 4.52 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.

Debuging 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).

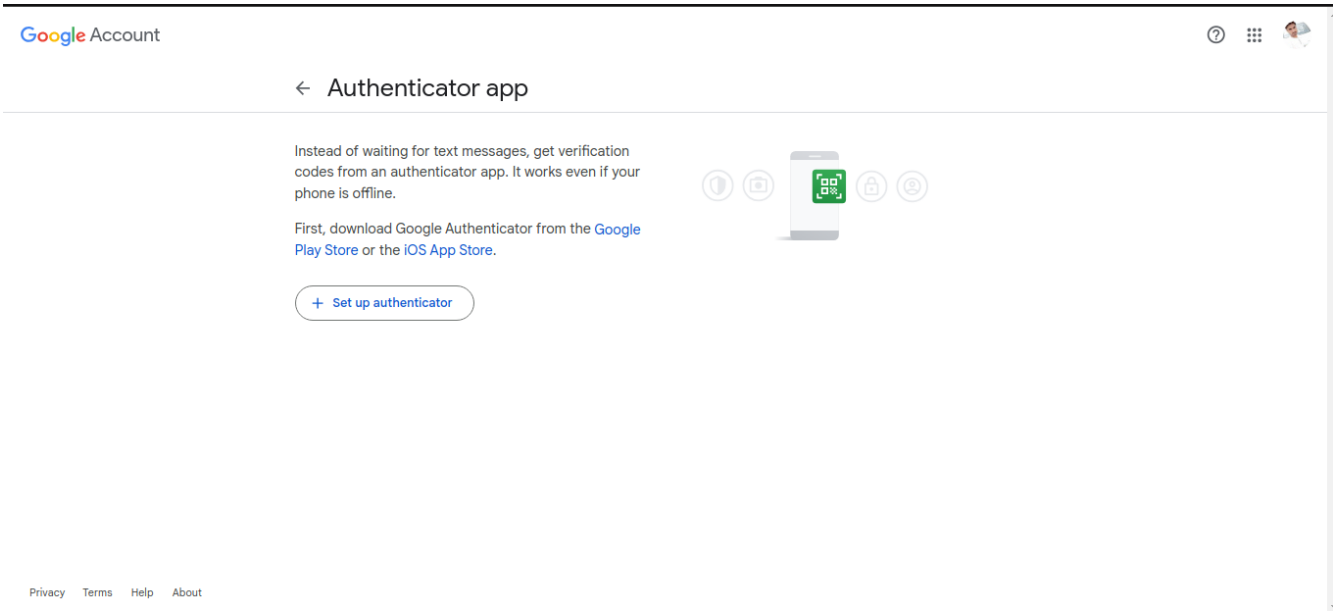
4. **Errors**:
    - There are some errors related to the `clamav-exec` and `firewall-bypass` scripts indicating incorrect port specifications or issues connecting to helper ports.
5. **HTTP Responses**:
    - Responses from the server for various checks suggest that certain methods (like `DEBUG` for ASP.NET) are not supported, and some paths return a 404 status, indicating they do not exist.

Recommendations:

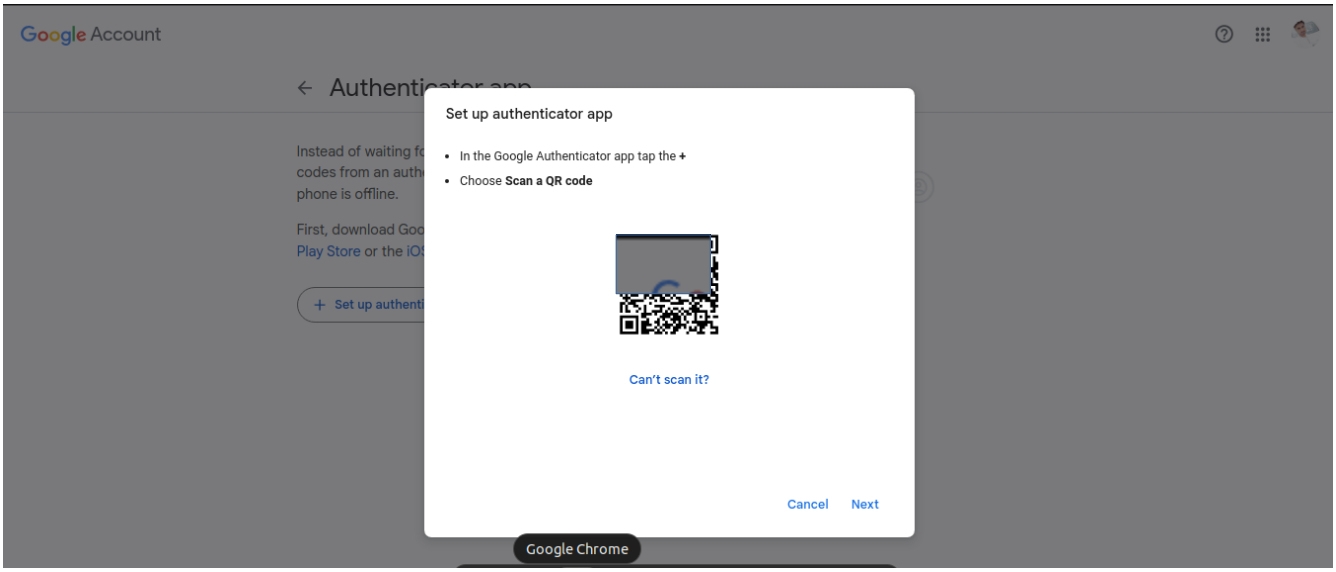
- **Further Testing**: Depending on the context, you may want to try more specific scripts related to the services running on the open ports, especially on port 80.
- **Review Configuration**: If this is your server, review its security configurations to ensure it's hardened against attacks.
- **Monitoring**: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

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

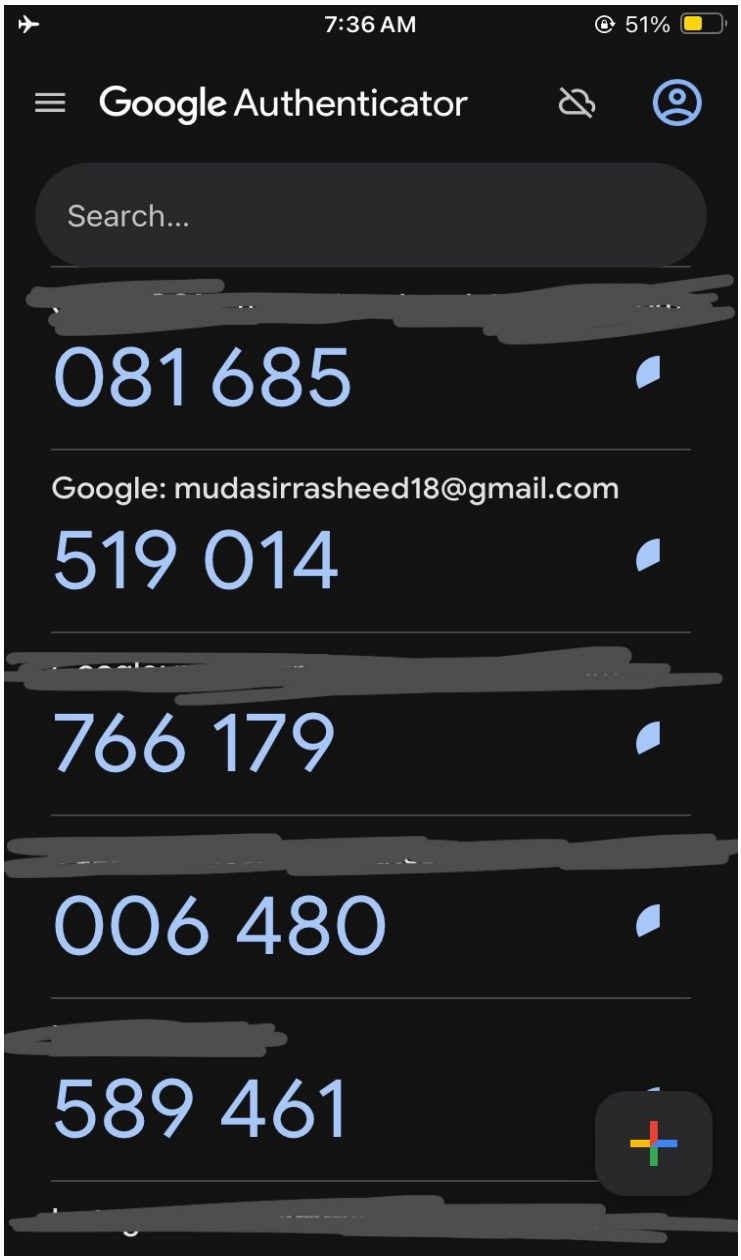
- **Email/Gmail:**



- **Scan QR code:-**

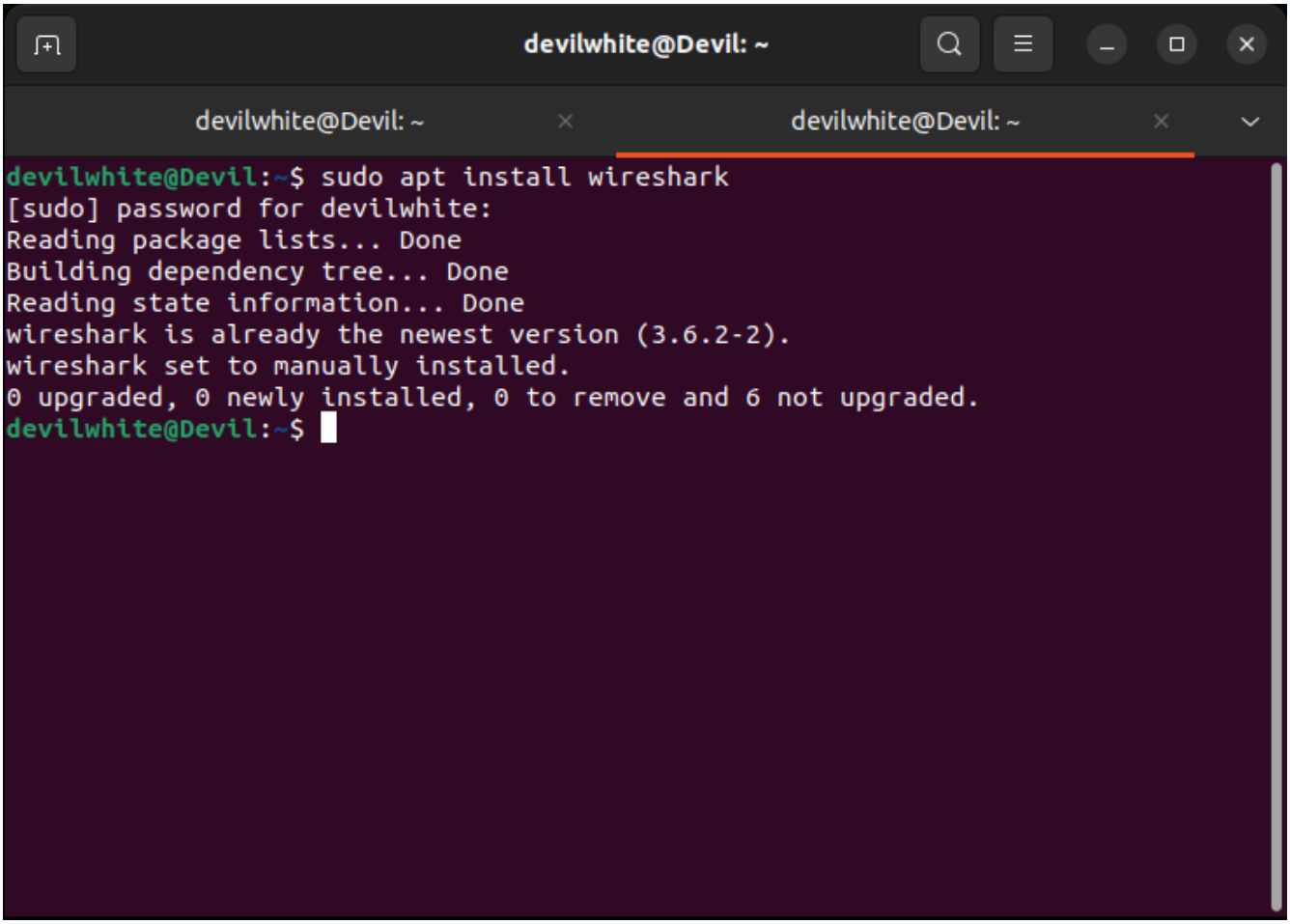


Scan QR and press next to enter code generated by Authentication app we will see the screen like below:-



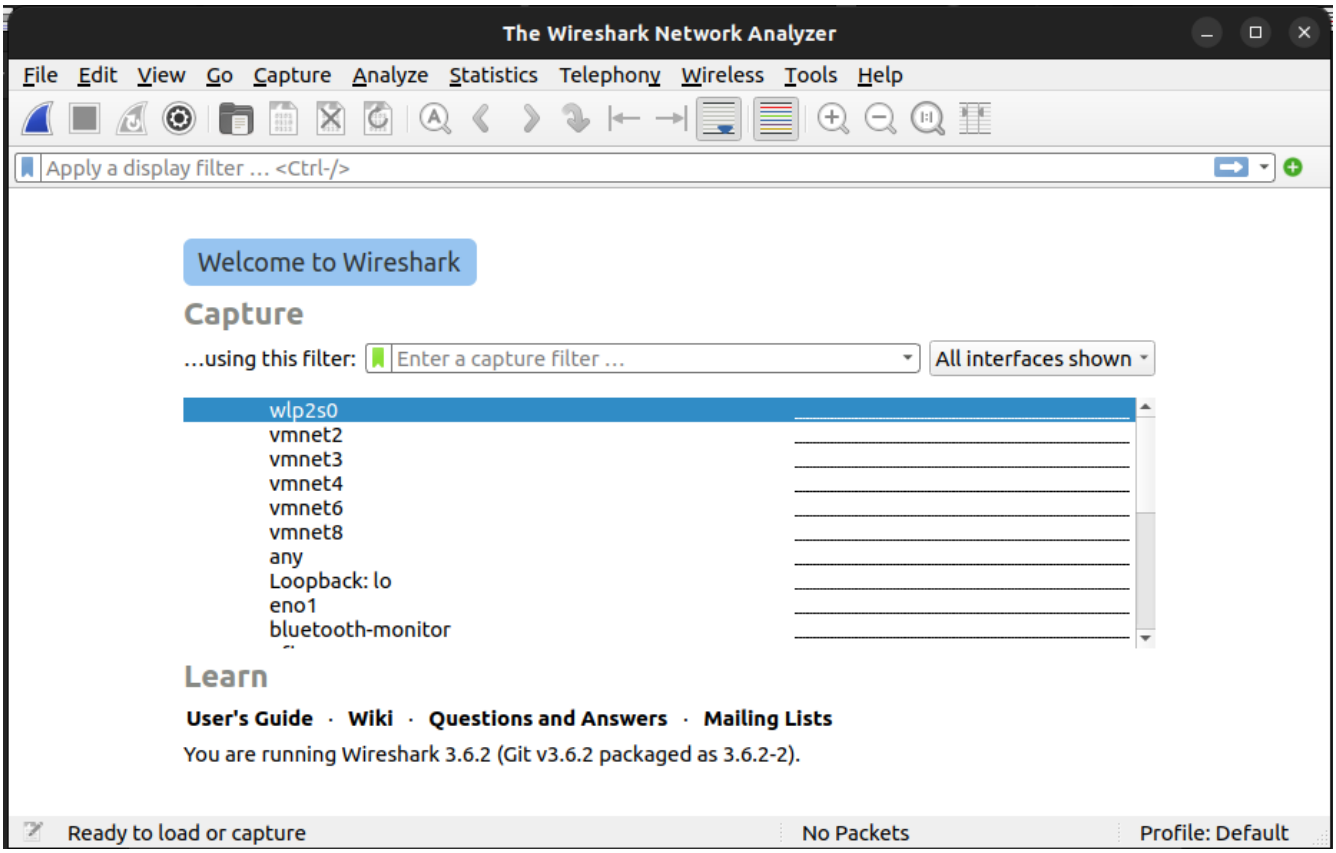
Task 3: Analyze Network Traffic

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

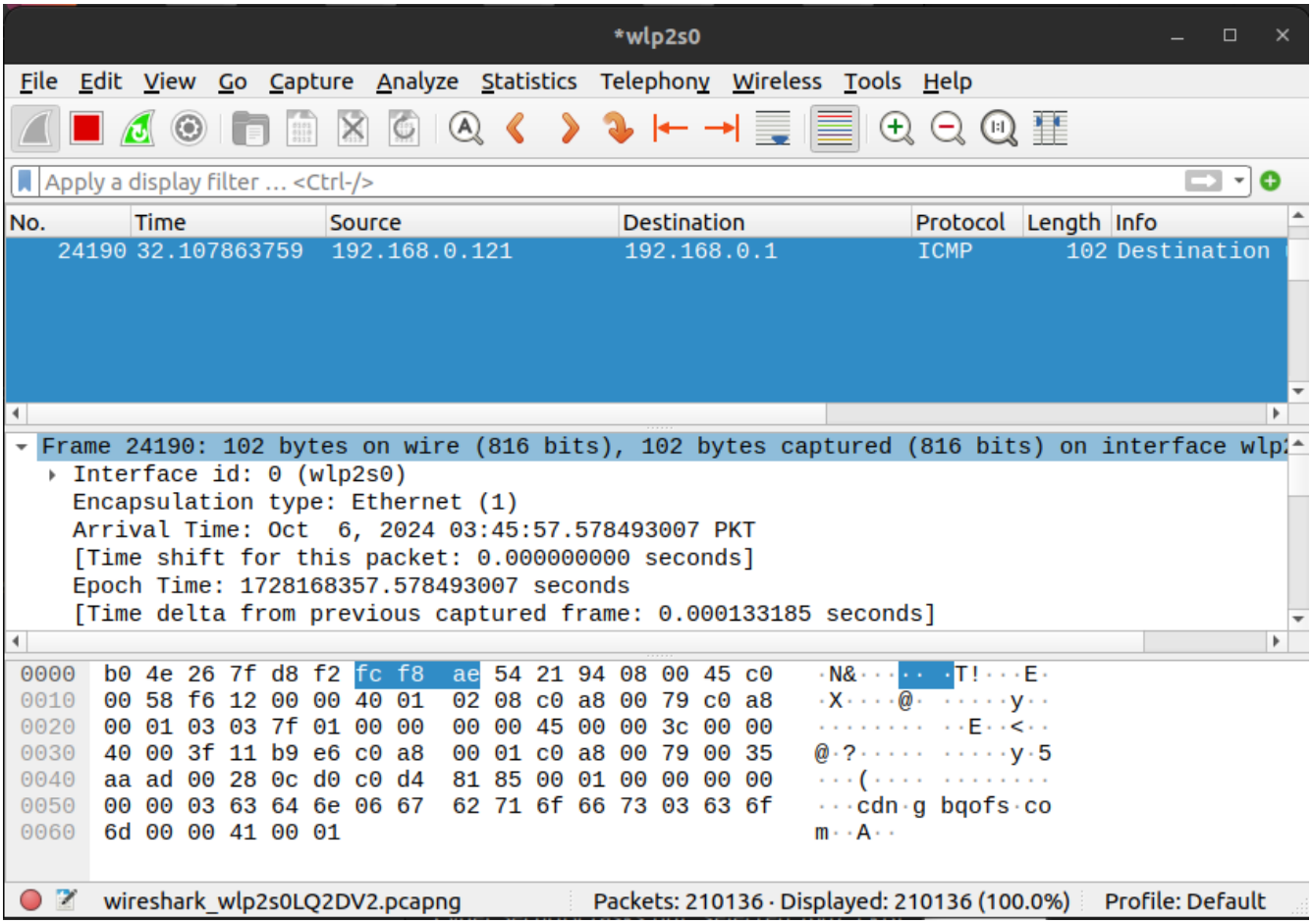


- **Step 2: Capture Network Traffic**

To capture packets, open Wireshark: Start Wireshark and select the network interface you want to capture (e.g., `eth0`, `wlan0`, `wlps0`).

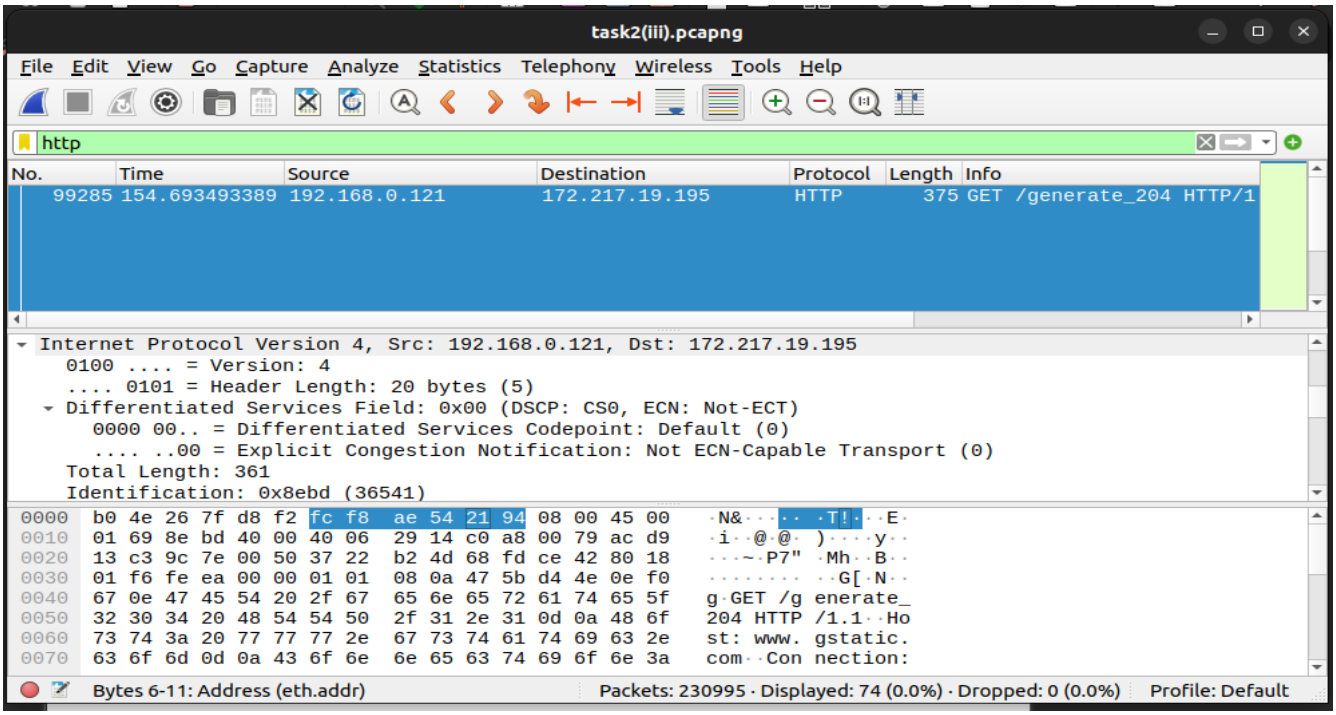


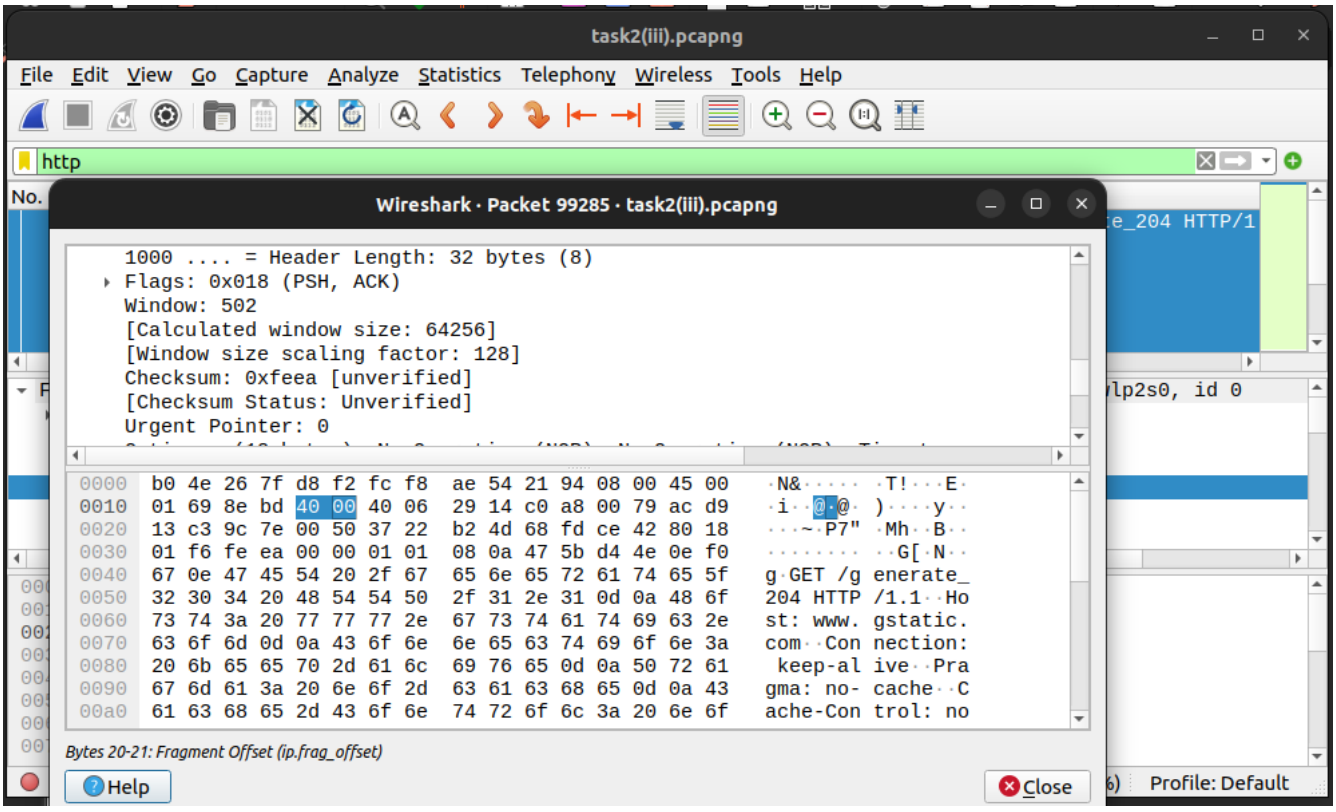
Double click on the interface and capturing will starts and looks like the following:-



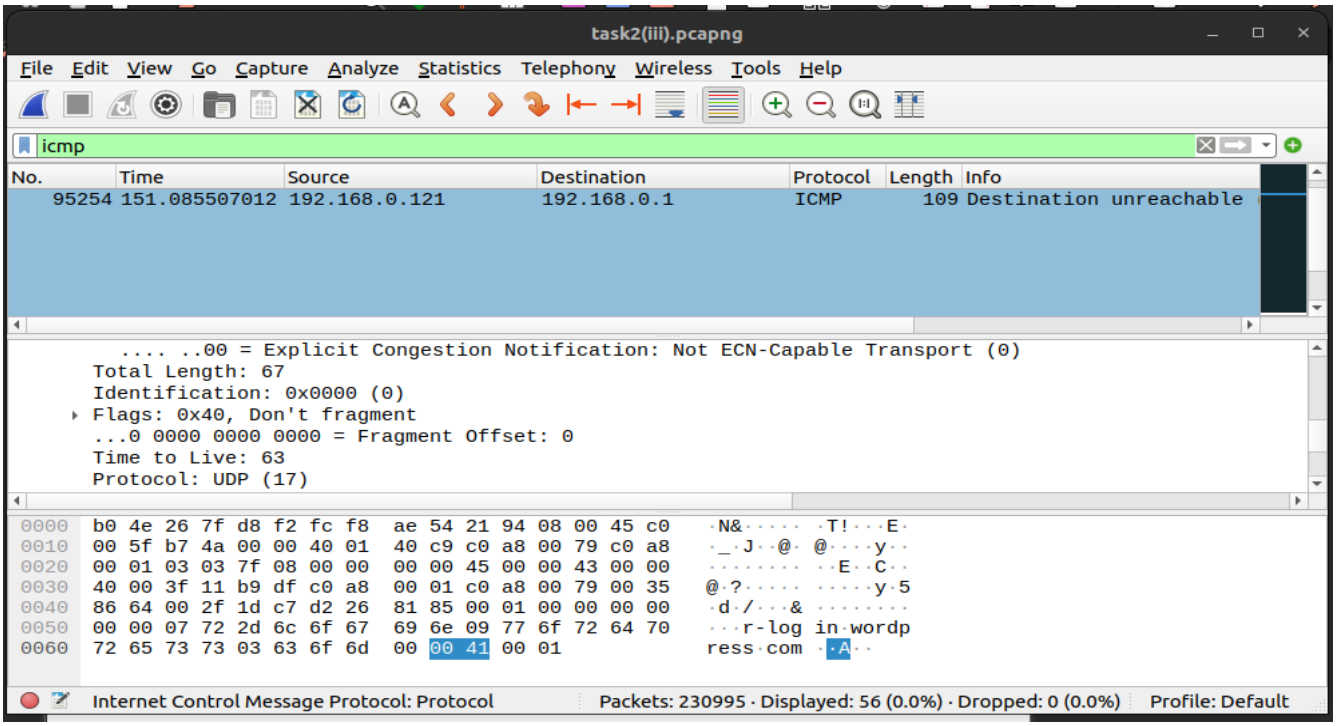
- **Step 3: Analyze Captured Packets**
- **Filter Packets:** To narrow down analysis, we can filter by protocol.

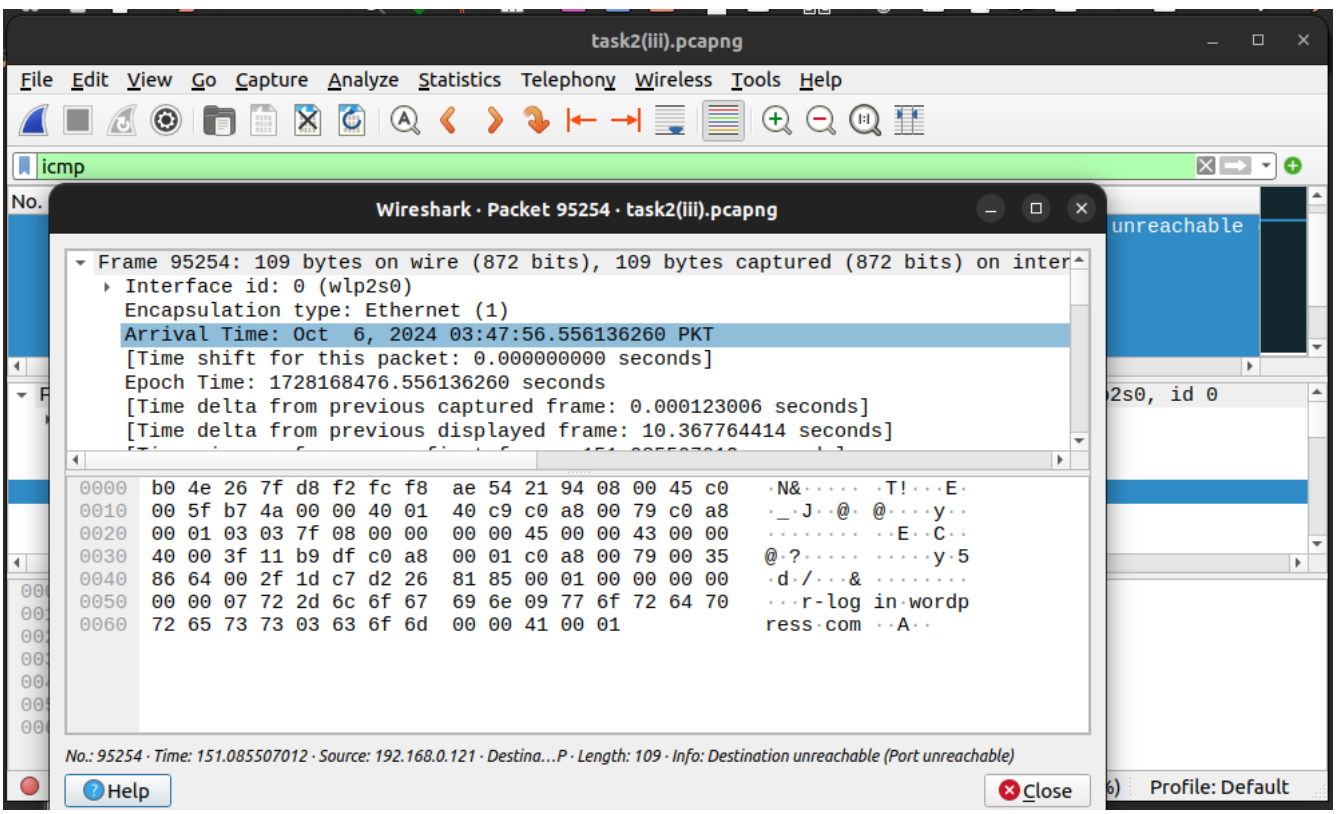
  To capture HTTP traffic: write http in the search box



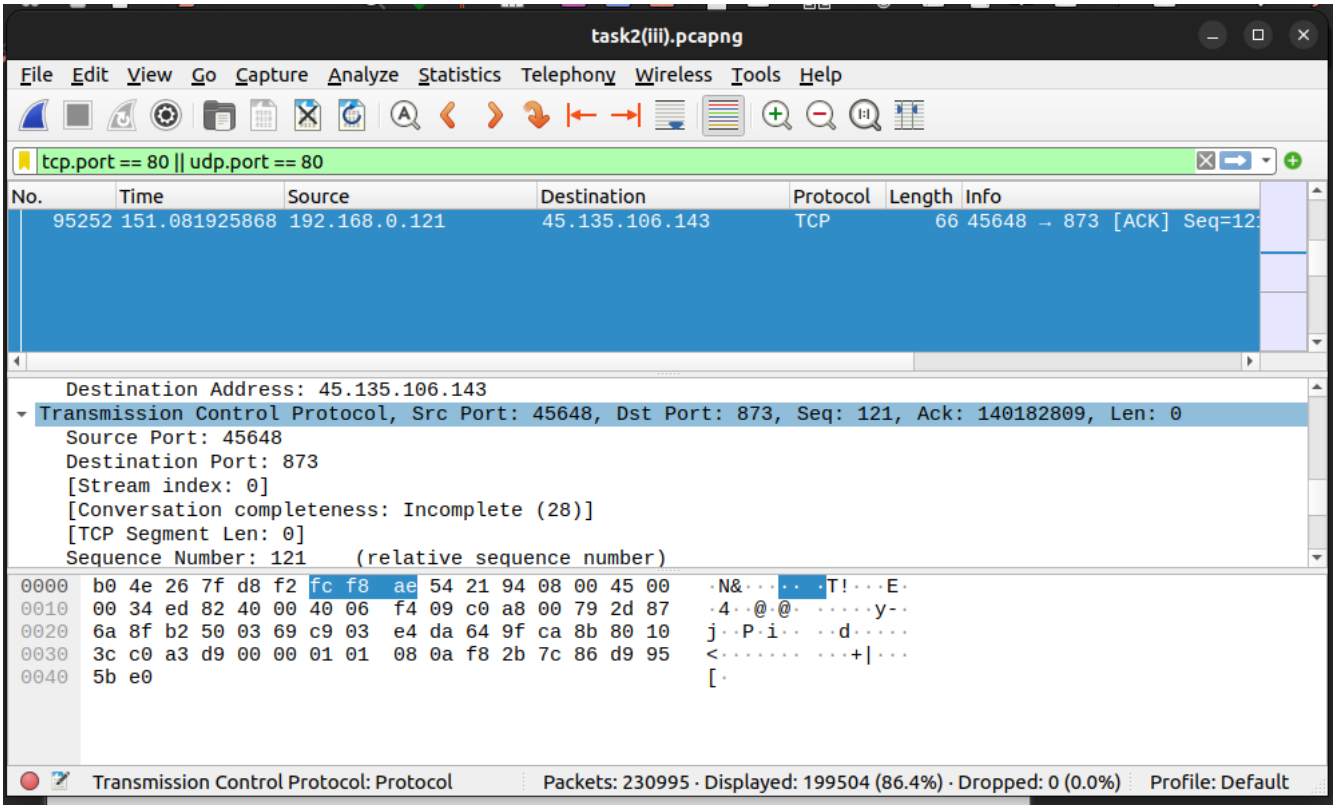


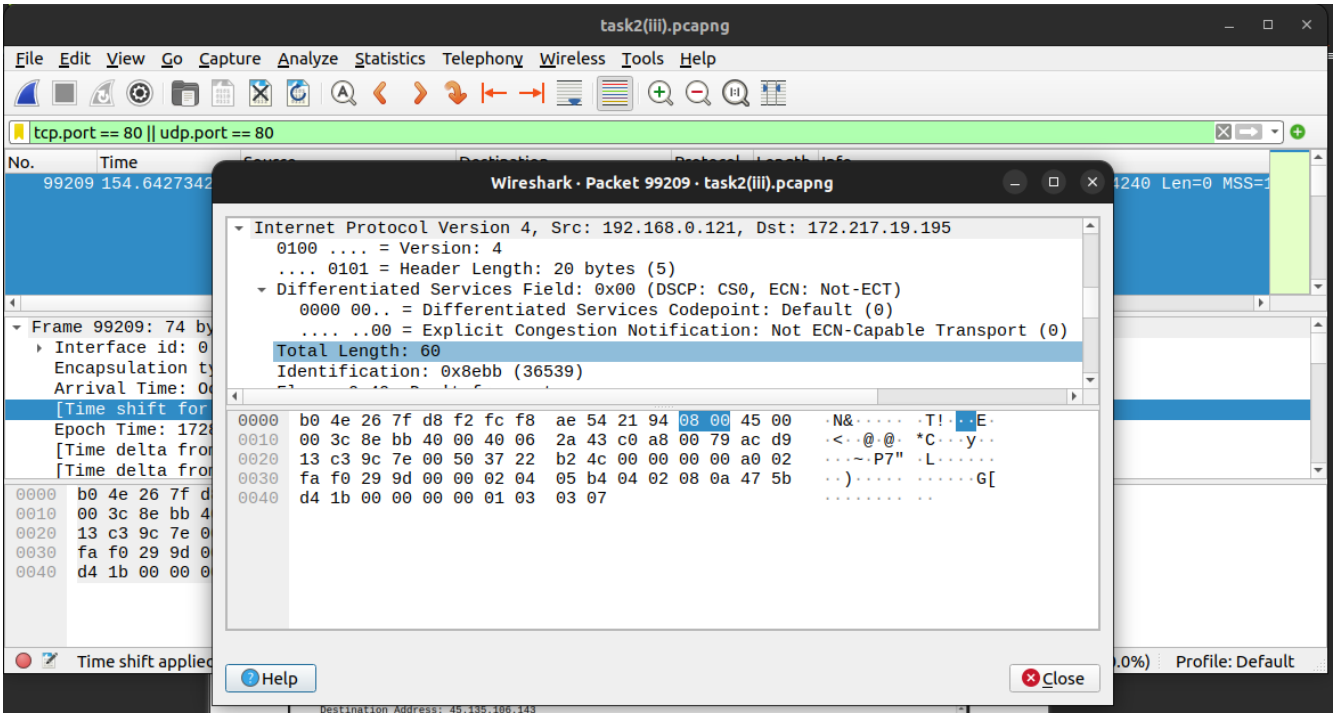
To capture ICMP traffic (ping): write ICMP in the search box





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





- **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.