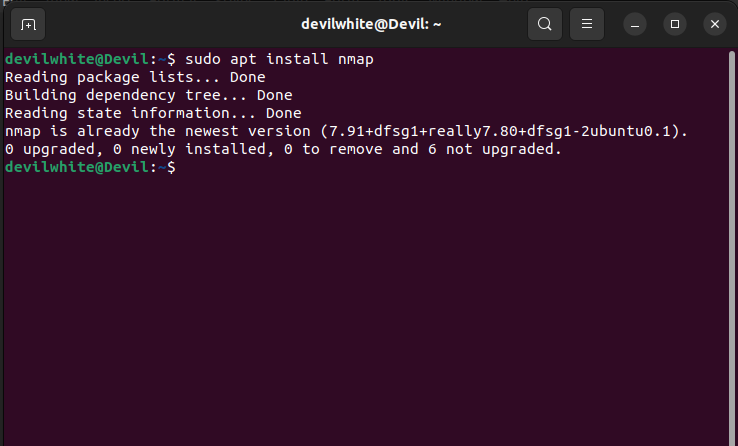
**Cyber Security Intermediate Tasks**

**Task 1: Perform a Basic Vulnerability Scan**

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

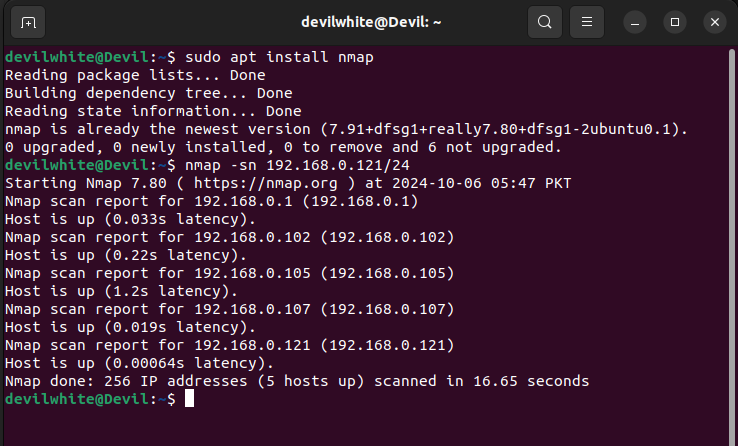
**sudo apt install nmap**

****

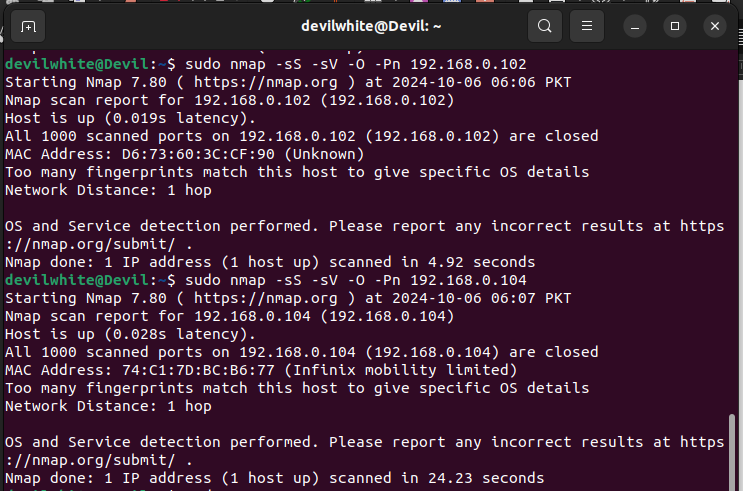
* **Perform a Scan with Nmap**

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

**nmap -sn <network\_ip\_range>**

* Service Version Detection and OS Scan:

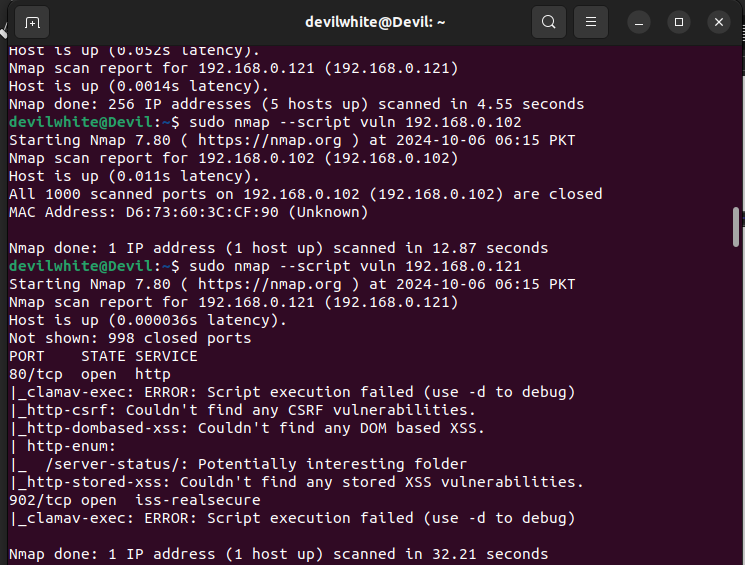
**sudo nmap -sS -sV -O <target\_ip>**





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

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

****

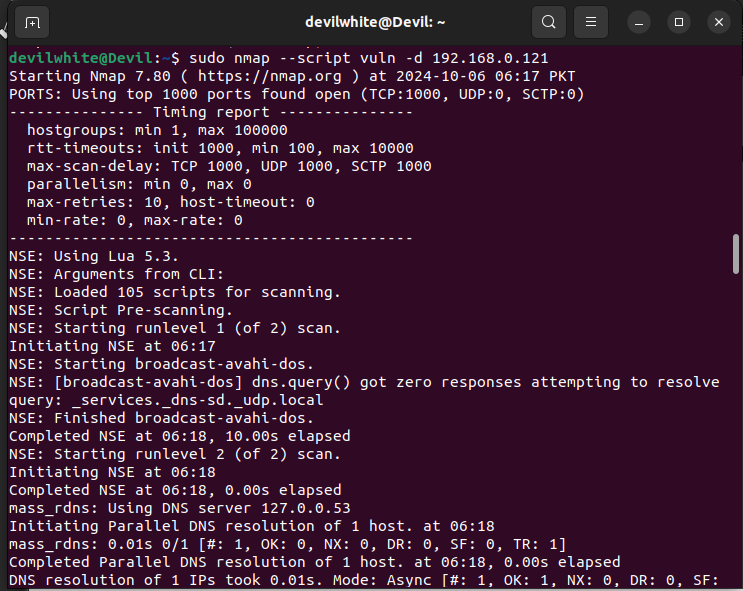
### **Scan Summary**

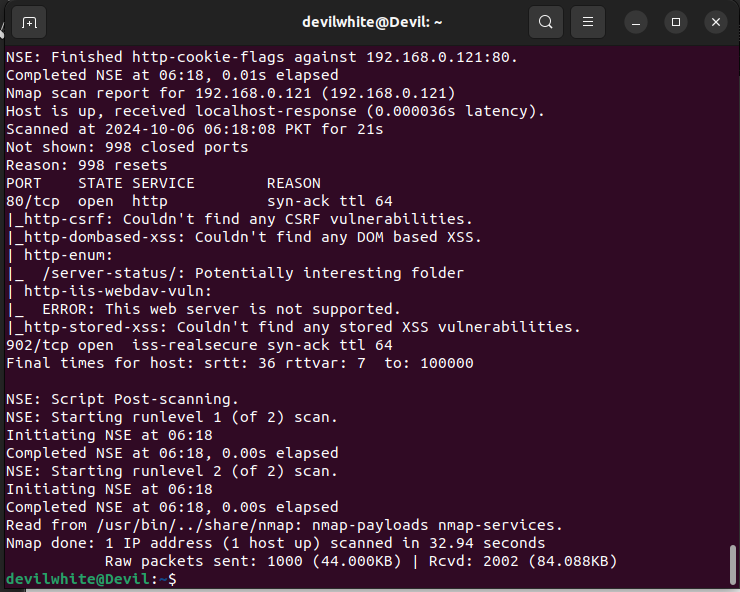
* Host Status: The host is up, with a very low latency.
* Open Ports:
  + 80/tcp: Running HTTP
  + 902/tcp: Running ISS RealSecure

### 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**:**

****

****

**The scan output indicates several points of interest:**

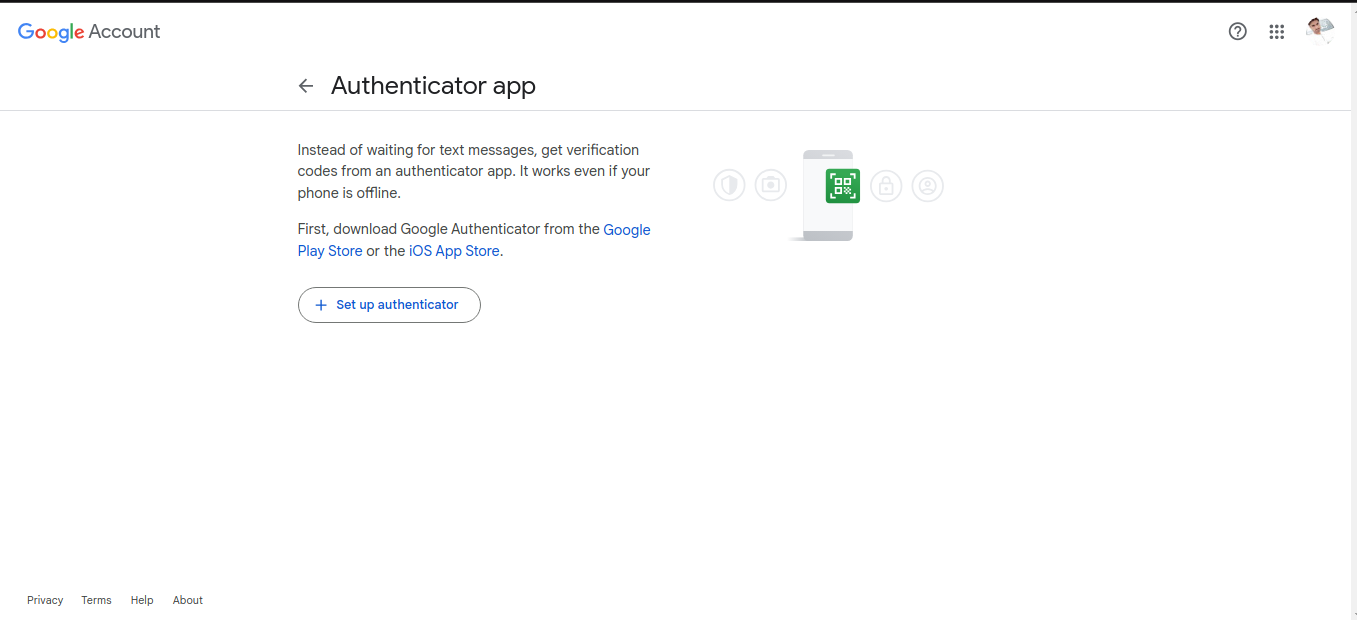
1. Open Ports Discovered:
   * Port 80 (HTTP): The most common port for web services.
   * Port 902: Typically associated with VMware services.
2. Scripts Executed:
   * Various scripts targeting known vulnerabilities in web applications, including checks for specific CVEs (Common Vulnerabilities and 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:**

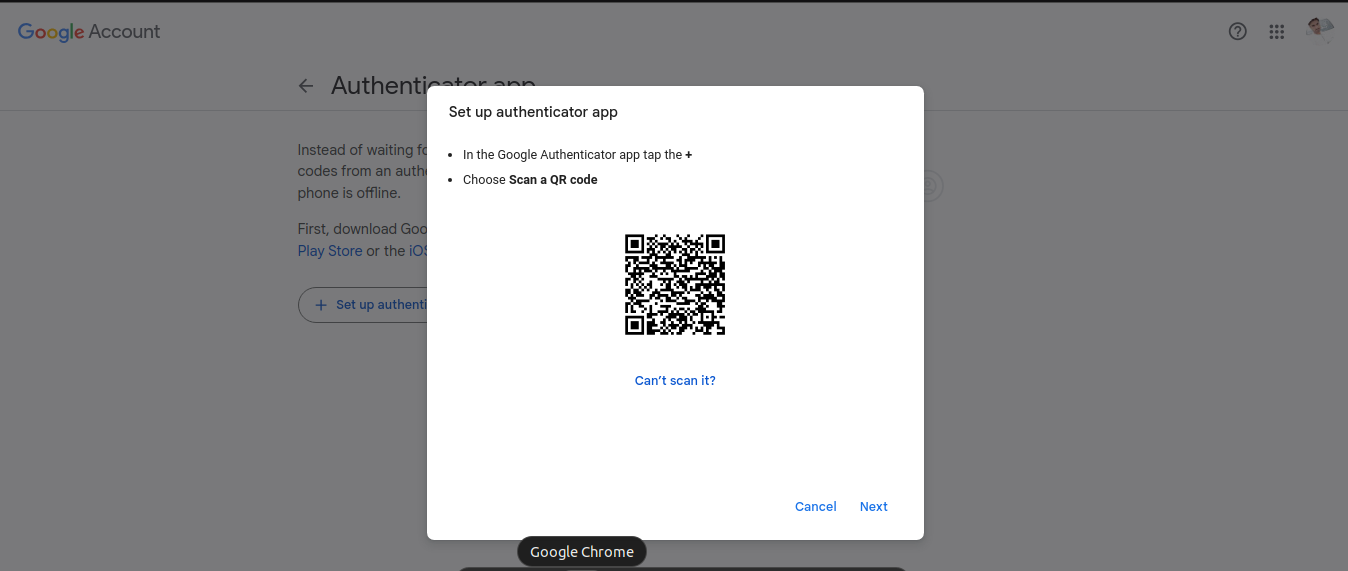
* Further Testing: Depending on the context, you may want to try more specific scripts related to the services running on the open ports, especially on port 80.
* Review Configuration: If this is your server, review its security configurations to ensure it's hardened against attacks.
* Monitoring: Implement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

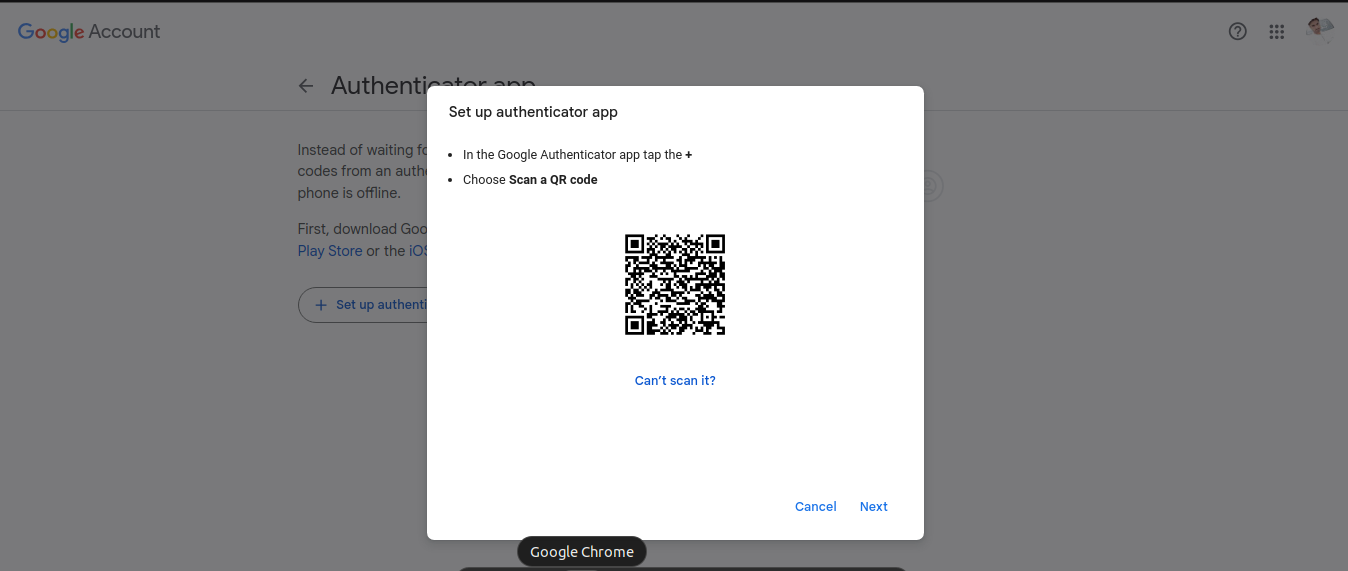
**Task 2: Implement Two-Factor Authentication (2FA)**

* **Email/Gmail:**

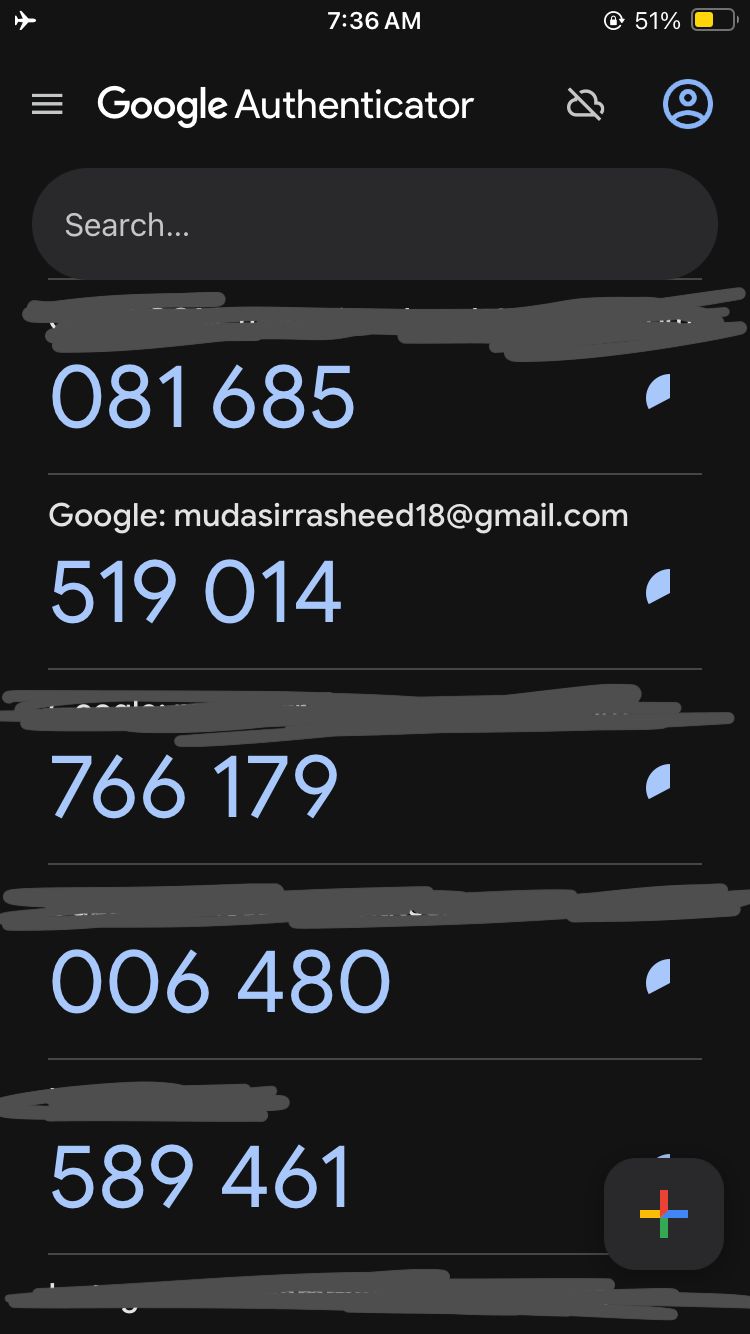


* **Scan QR code:-**



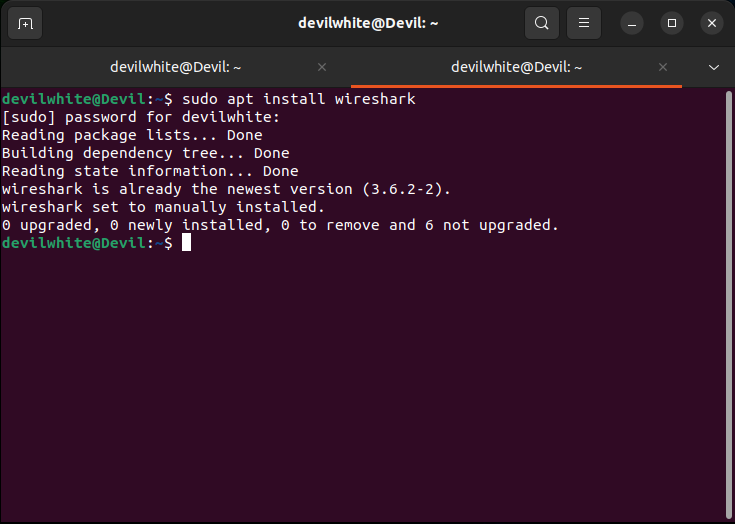


Scan QR and press next to enter code generated by Authentication app we will see the screen like below:-



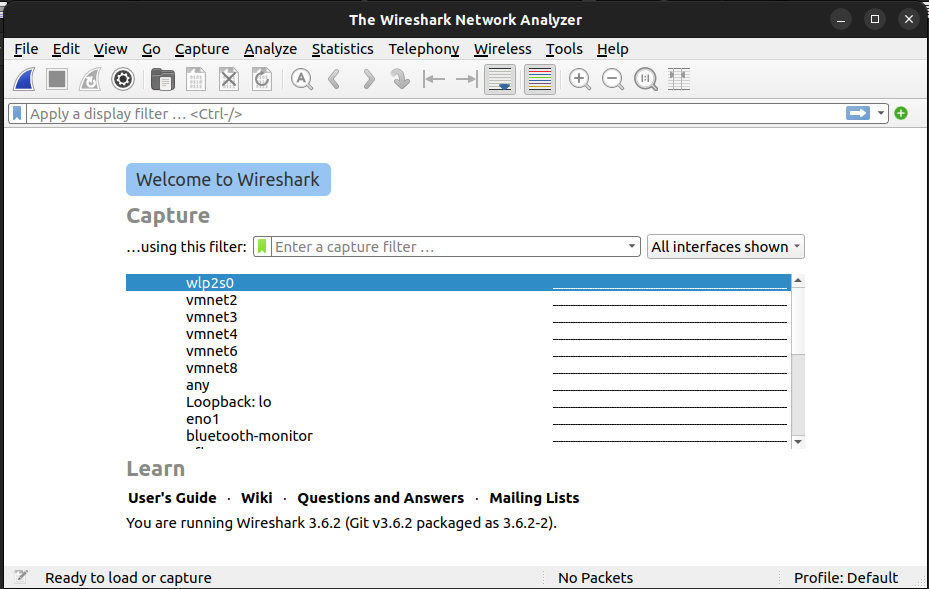
**Task 3: Analyze Network Traffic**

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

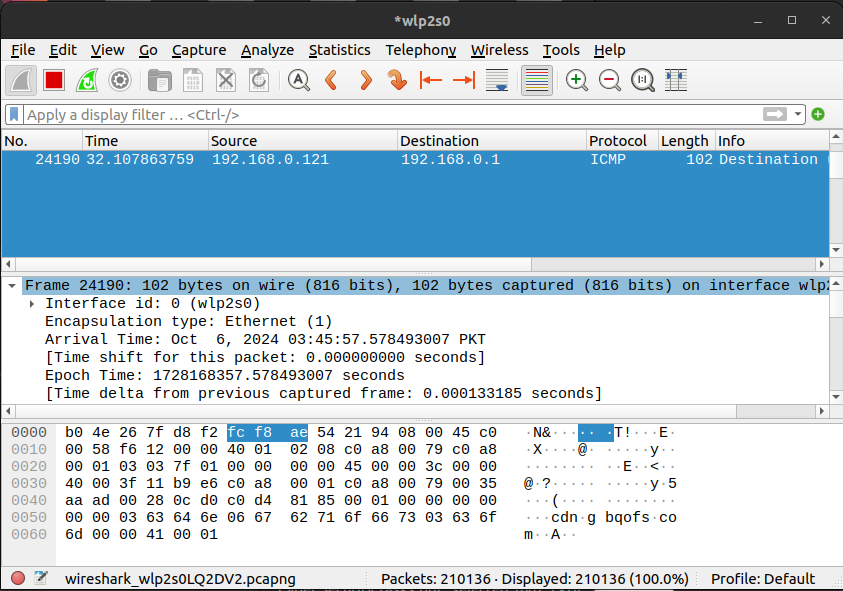
****

#### **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).

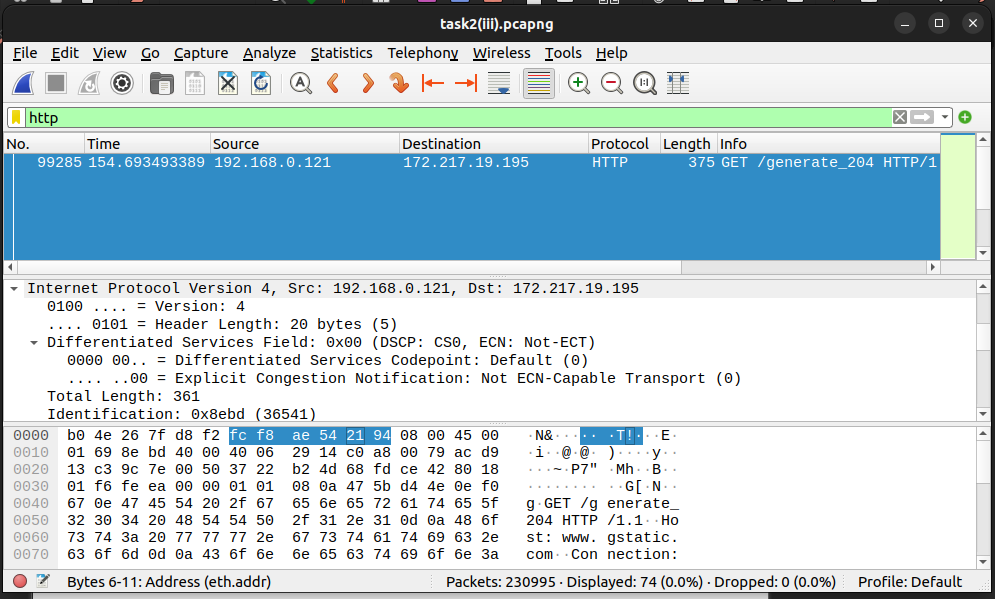


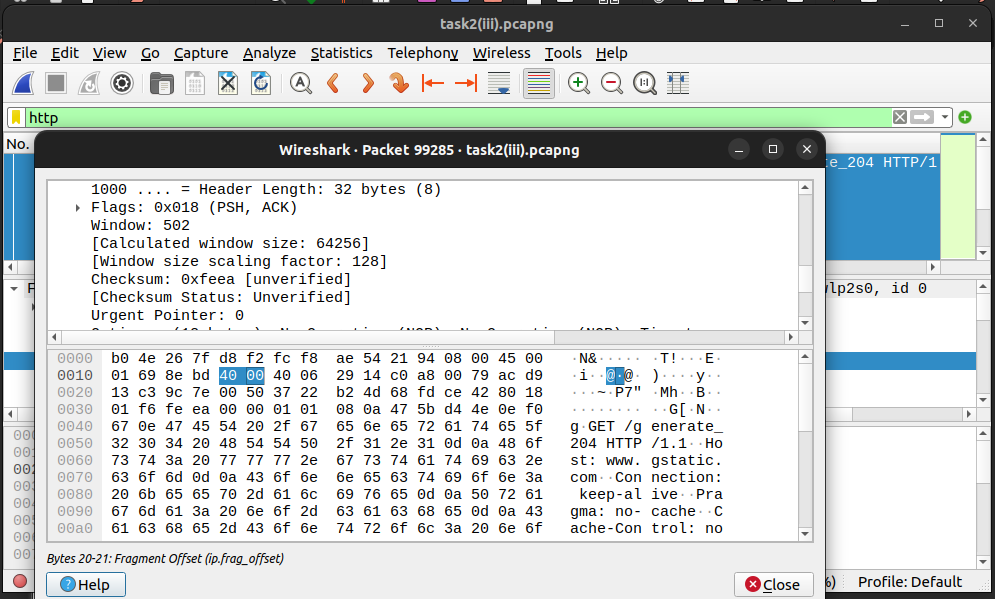
Double click on the interface and capturing will starts and looks like the following:-



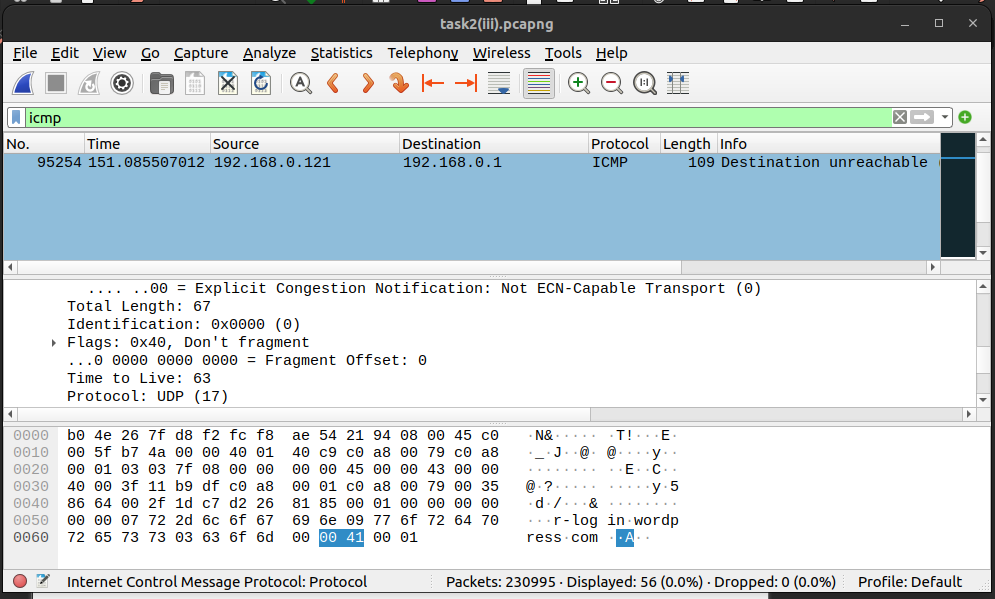
* Step 3: Analyze Captured Packets
* **Filter Packets:** To narrow down analysis, we can filter by protocol.

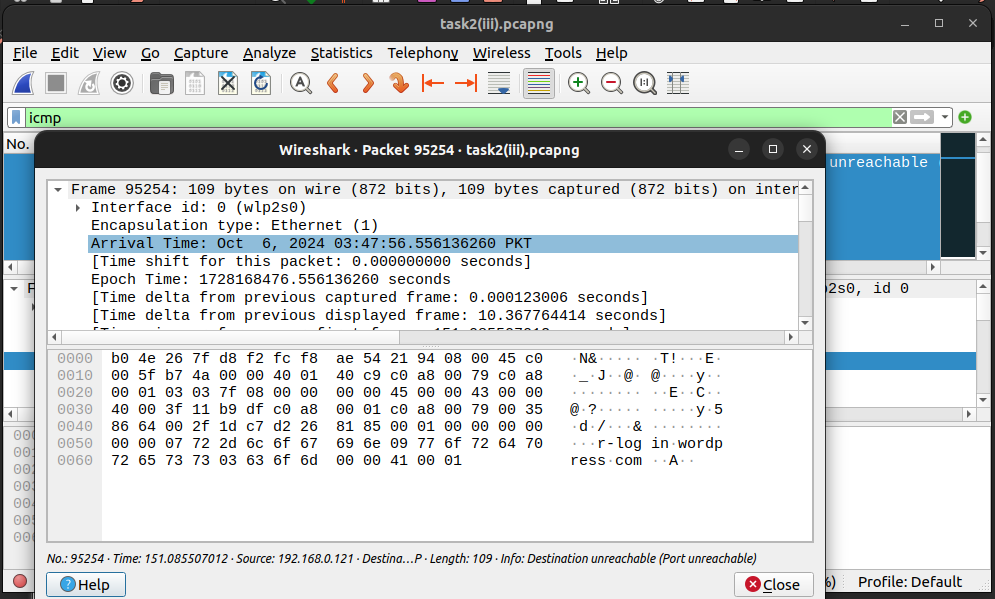
To capture HTTP traffic: write http in the search box

****

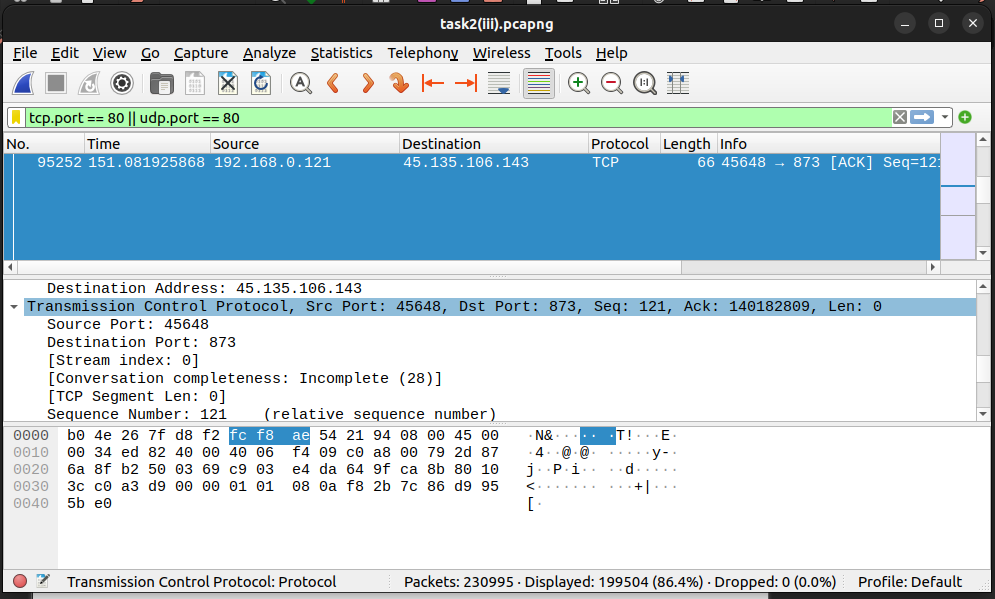


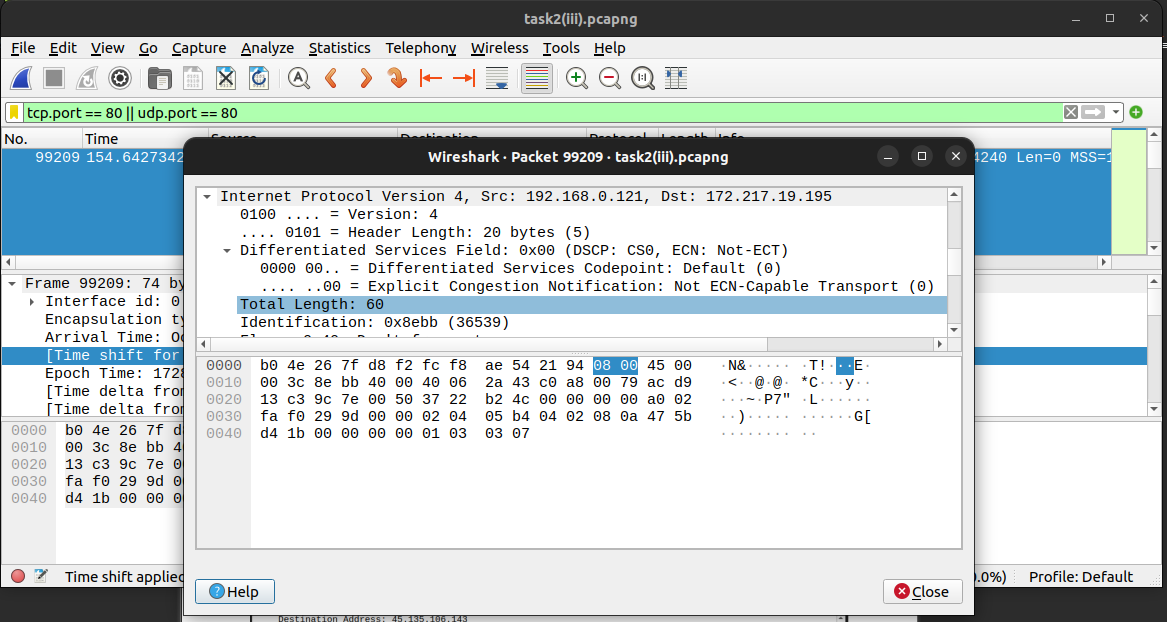
To capture ICMP traffic (ping): write ICMP in the search box

****

****

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.