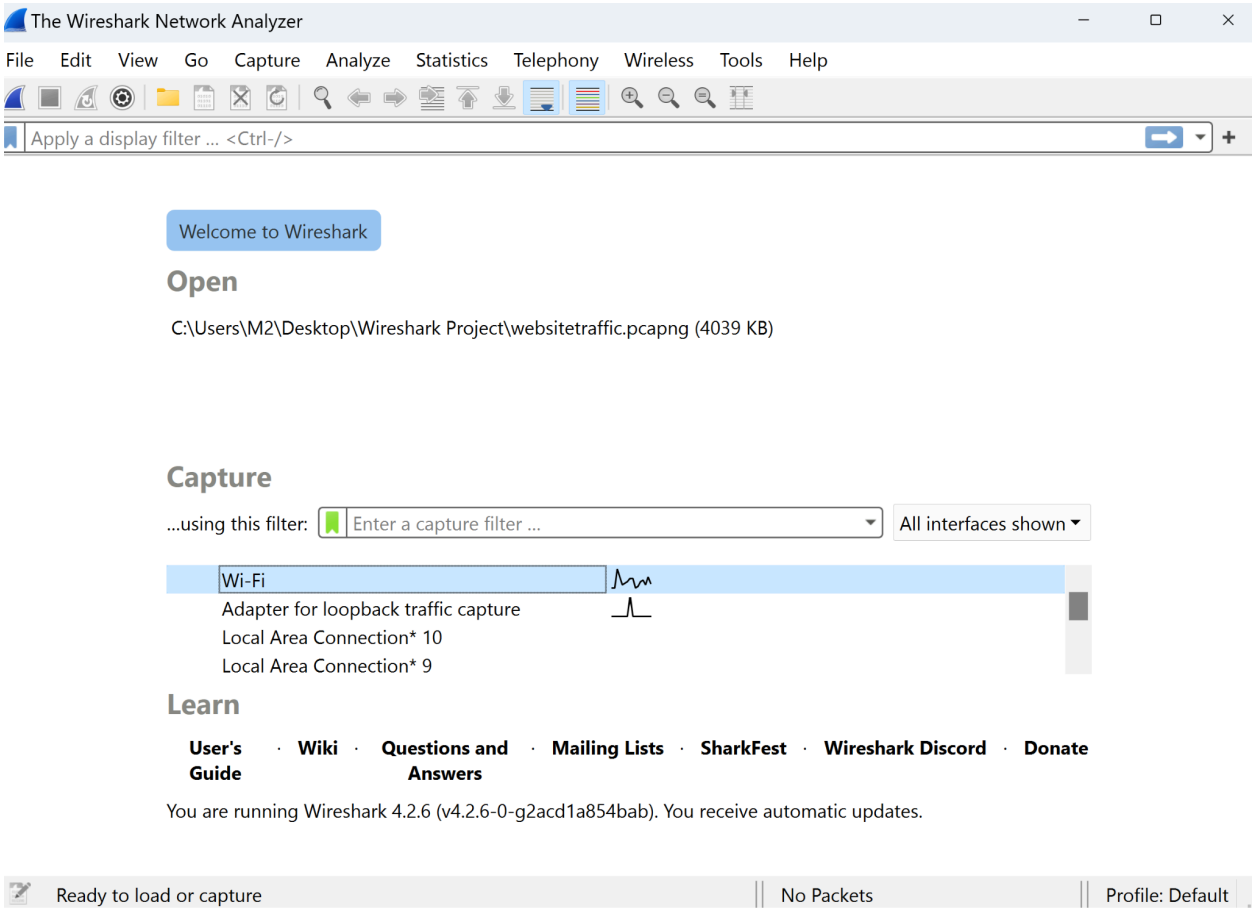
Using Nmap to Generate ARP Requests and Capturing Them with Wireshark

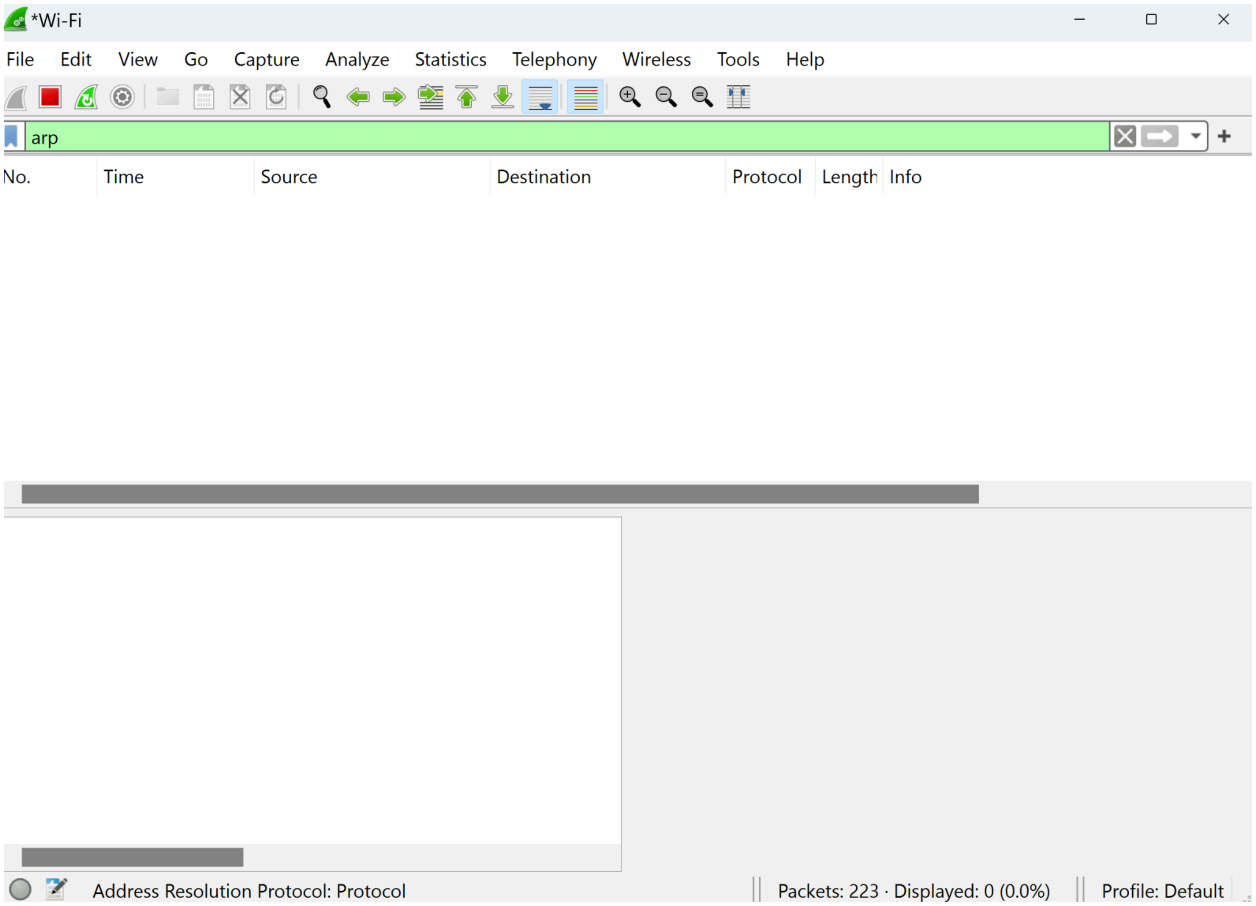
---

Step 1: Open Wireshark and Set Up for Capturing

1. **Launching Wireshark**: I opened Wireshark from my Start menu or desktop.
2. **Selecting a Network Interface**: Wireshark showed me a list of network interfaces, and I chose Wifi.



3. **Starting Capture**: I clicked the blue shark fin button to start capturing traffic on the selected interface.
4. **Filtering for ARP Traffic**: In the display filter bar at the top of Wireshark, I typed `arp` to filter only ARP traffic. This way, I could focus on ARP packets as they appeared.



Step 2: Use Nmap to Generate ARP Requests

1. **Opening Command Prompt**: I opened the Command Prompt on my Windows machine by pressing `Win + R`, typing `cmd`, and pressing `Enter`.

2. **Using Nmap for Scanning**: To generate ARP requests, I used Nmap to scan my local network. This scan sent ARP requests to identify live hosts on the network.

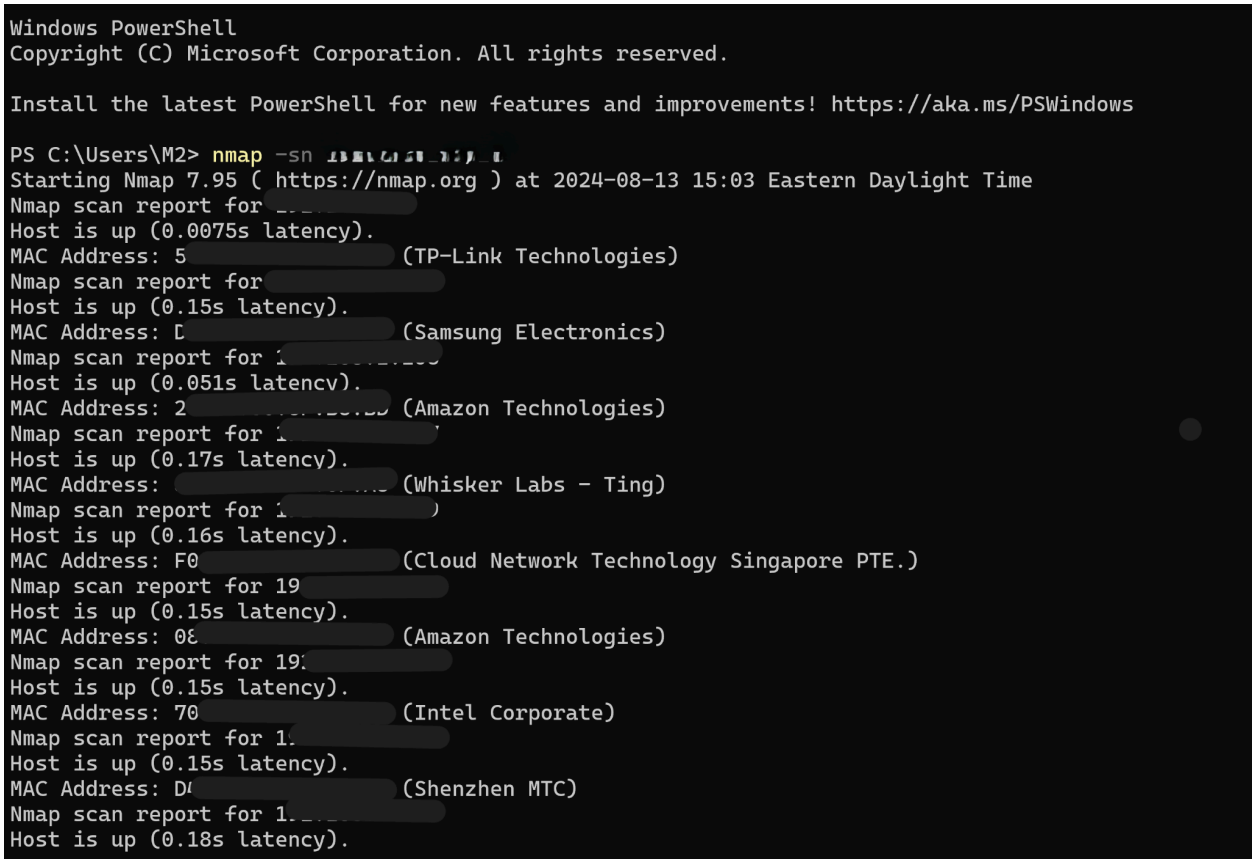
Basic ARP Scan: I ran the following command:
`nmap -sn [my_network]/24`

- I replaced `[my_network]` with my local network range.

Explanation:

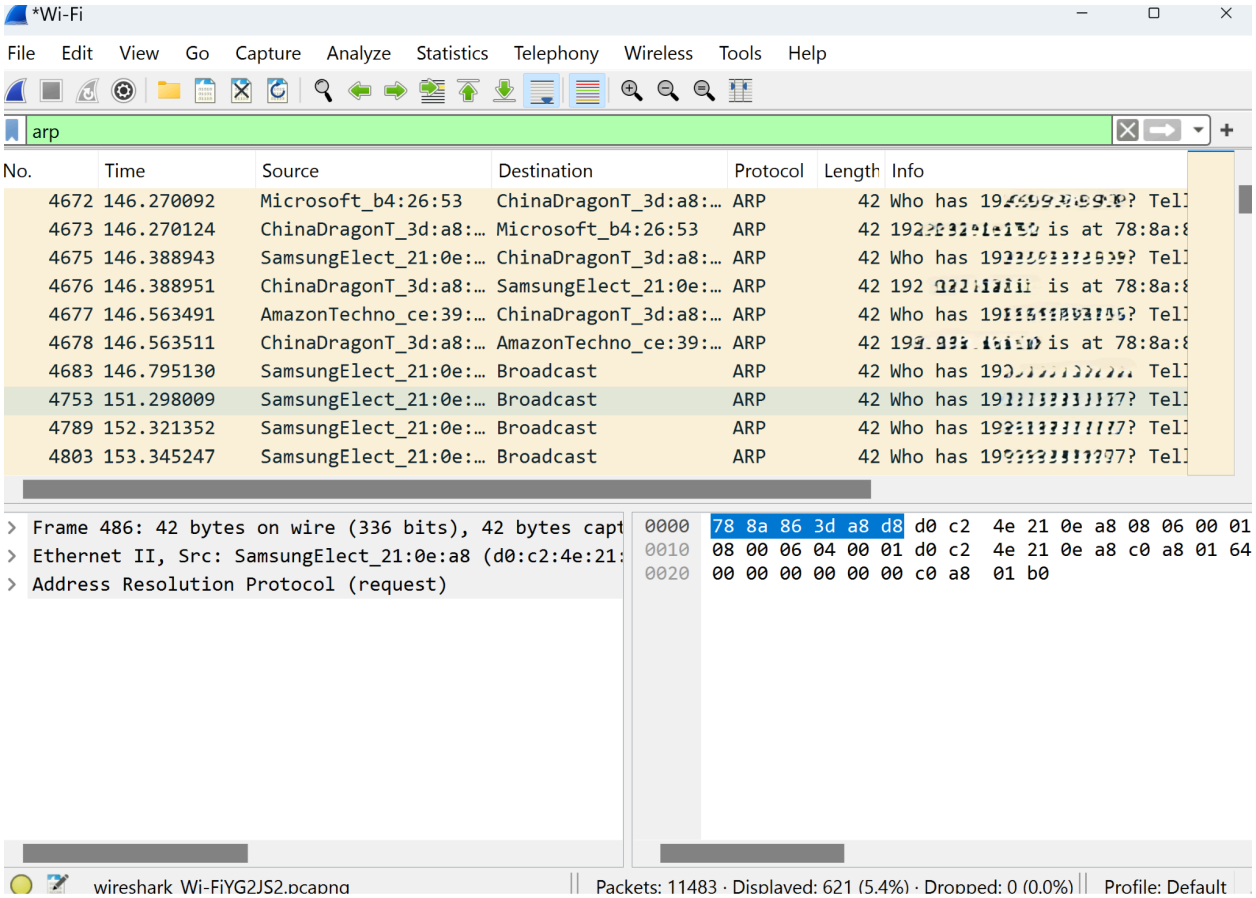
- `nmap`: This is the command to invoke Nmap.
- `-sn`: This option tells Nmap to perform a "ping scan," which sends ARP requests without conducting a full port scan.
- `[my_network]/24`: This specifies the range of IP addresses on my local network. The `/24` subnet mask means I'm scanning all 256 addresses in a typical home network range.

3. **Running the Scan**: After typing the command, I pressed `Enter`, and Nmap started scanning the network, generating ARP requests in the process.

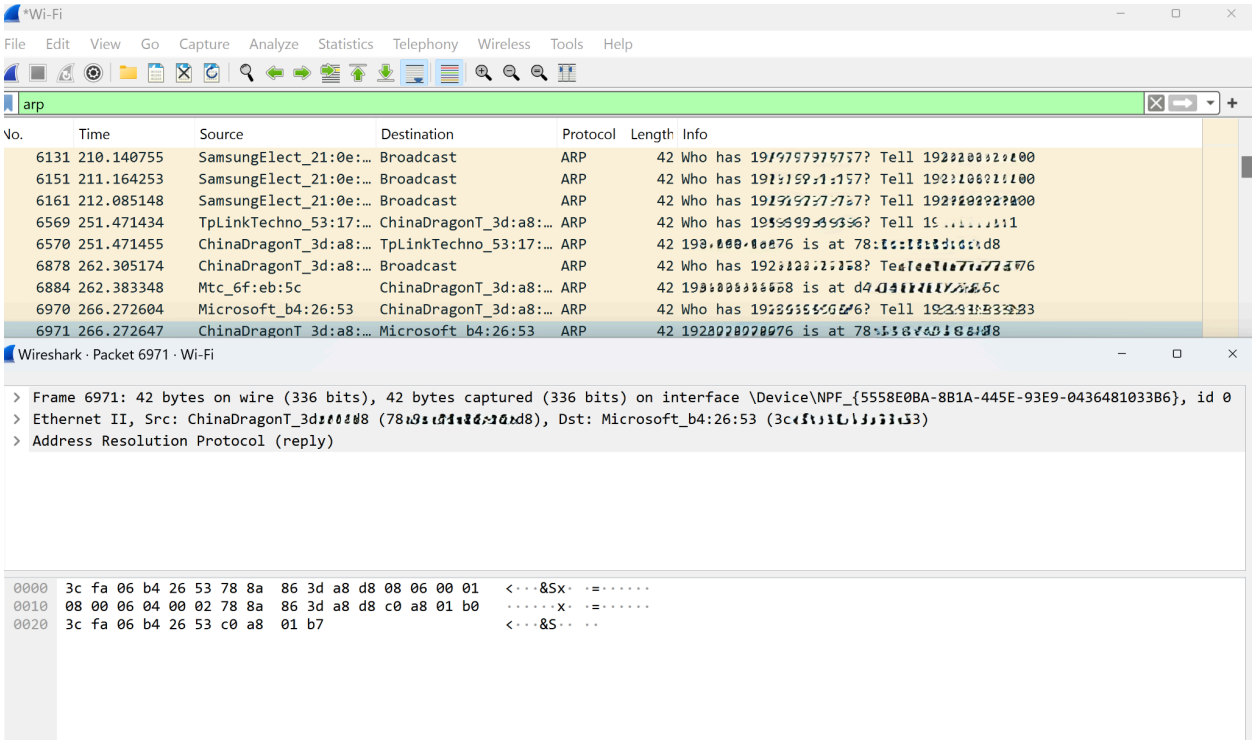


Step 3: Capture ARP Requests in Wireshark

1. **Checking Wireshark for ARP Traffic**: I switched back to Wireshark and saw ARP requests appearing in real-time as a result of the Nmap scan.



2. **Inspecting the ARP Packets**:
    - I clicked on an ARP packet in the list to highlight it.
    - The packet details pane showed me the ARP request and reply information.
    - I could see who was asking for which IP address and the MAC address involved.



Step 4: Stop the Capture and Save the Data

1. **Stopping Capture**: Once I had captured enough ARP requests, I clicked the red square button to stop the capture.
2. **Saving the Capture**:
    - I went to `File` > `Save As` and chose a location and filename to save my capture file.
    - I saved the file with a `.pcapng` extension.

Step 5: Analyzing the Capture

Conclusion

By following these steps, I successfully used Nmap to generate ARP requests and captured them using Wireshark. This exercise demonstrates my understanding of basic network scanning and packet analysis techniques.