5th Task SUBMISSION REPORT OF ELEVATE LABS CYBERSECURITY INTERNSHIP

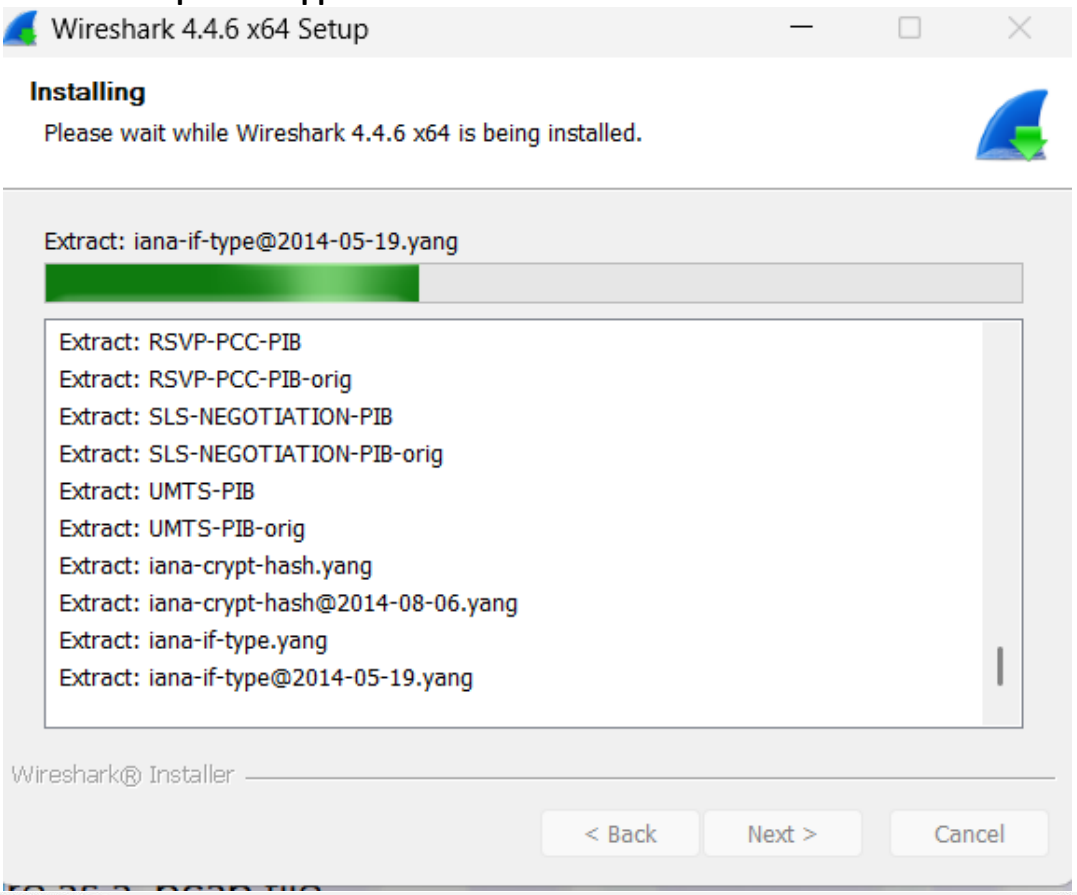
NAME	**ADARSH SHARMA**
Submitted to:	**Elevate Labs**
Name of the Academic Institute	**Ganpat University**

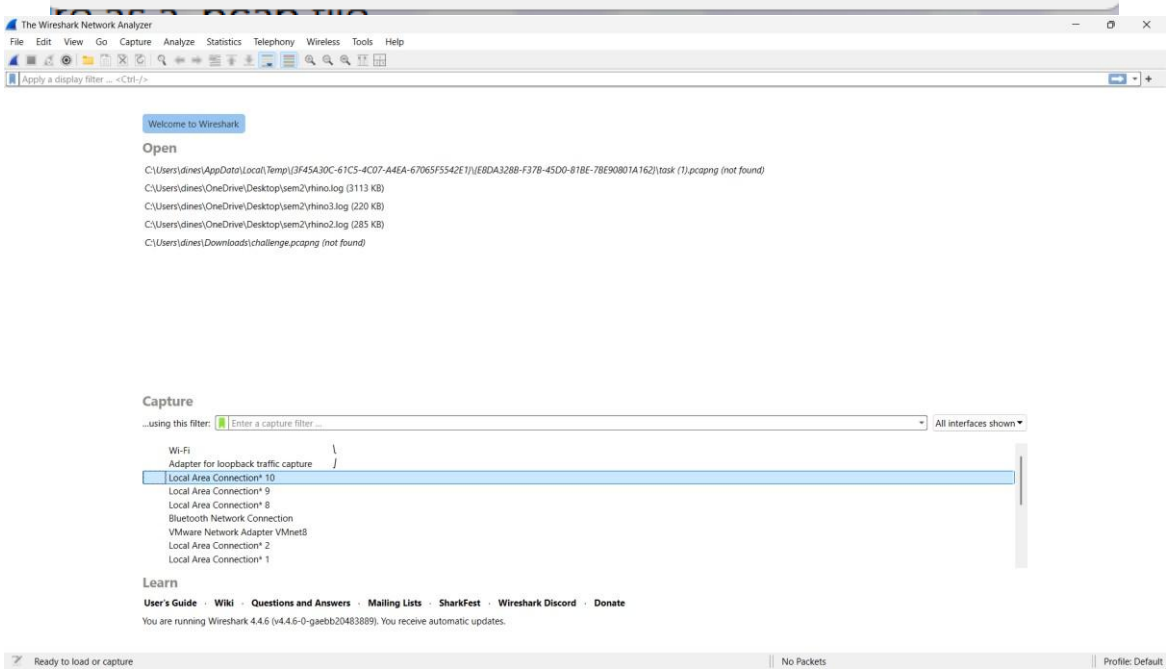
REPORT SUBMITTED TO

As part of the Cyber Security Internship, I have completed "Task 5th: Capture and Analyze Network Traffic Using Wireshark." by following all steps as instructed. Below is a detailed summary of each step followed during the task:

Task 5th: Capture and Analyze Network Traffic Using Wireshark

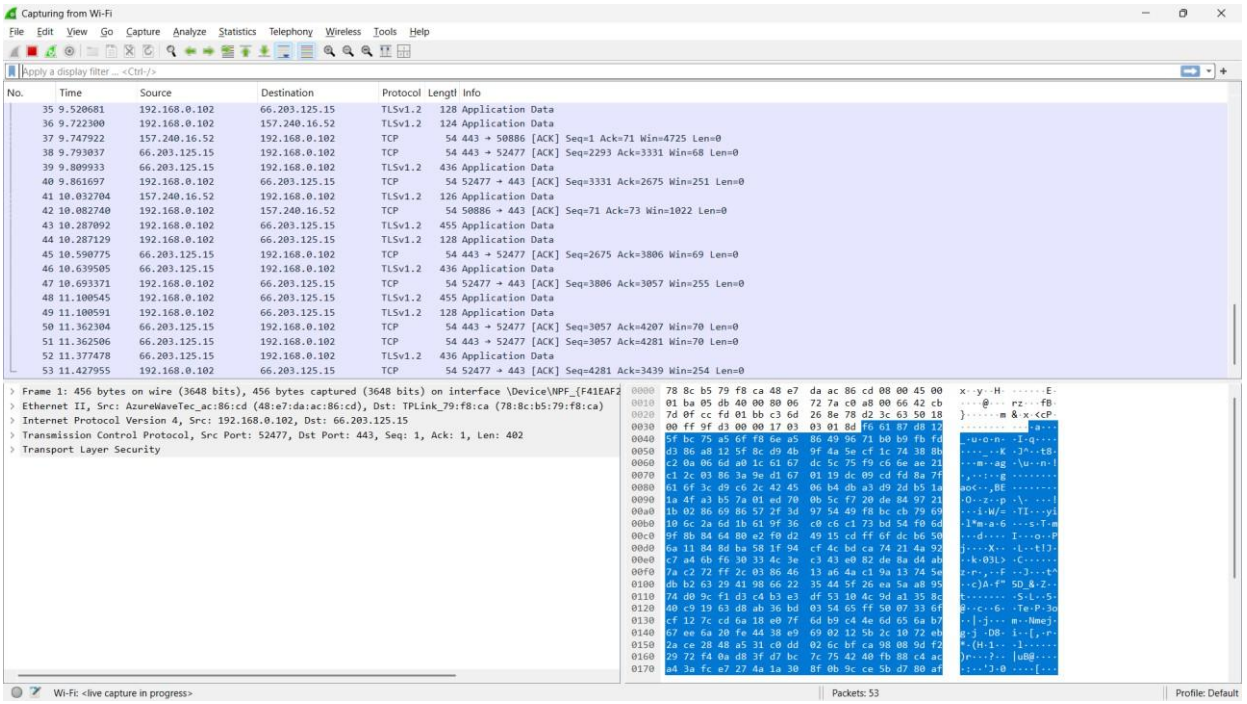
1. **Install Wireshark.**
   - **Download from: https://www.wireshark.org/download.html**
   - **Install and open the application.**

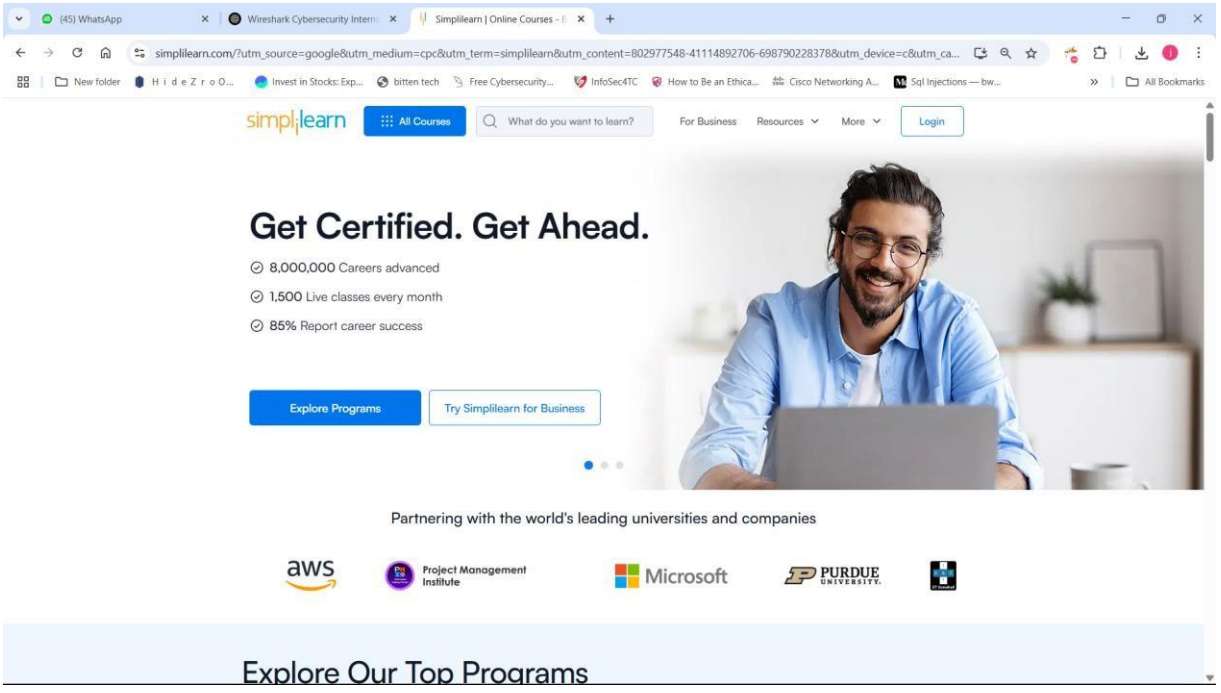




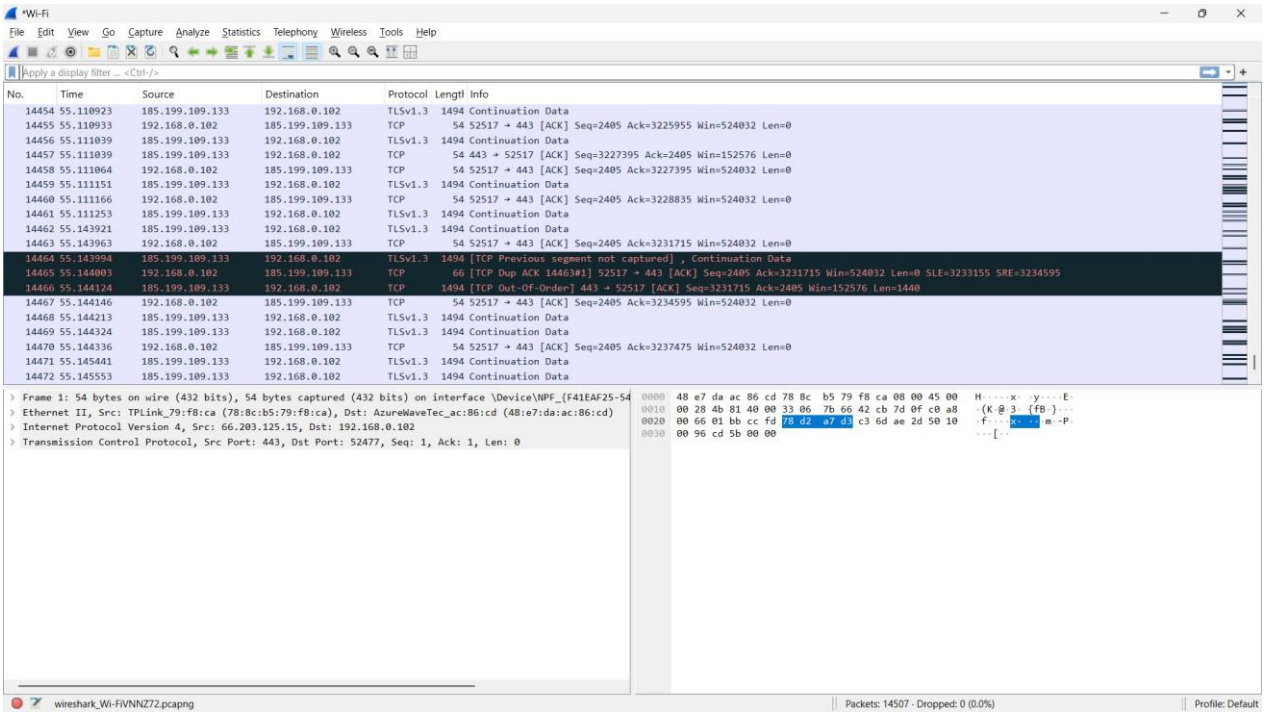
Task 5th: Capture and Analyze Network Traffic Using Wireshark

2. Start capturing on your active network interface.

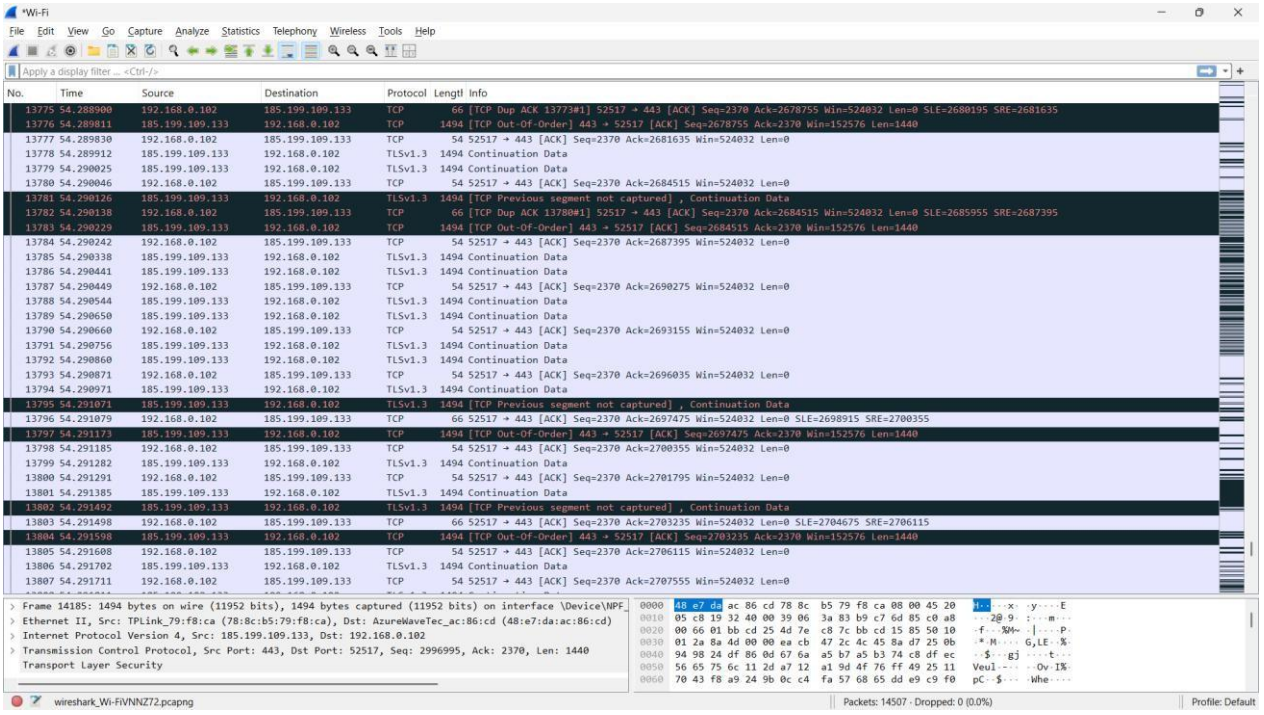




Task 5th: Capture and Analyze Network Traffic Using Wireshark

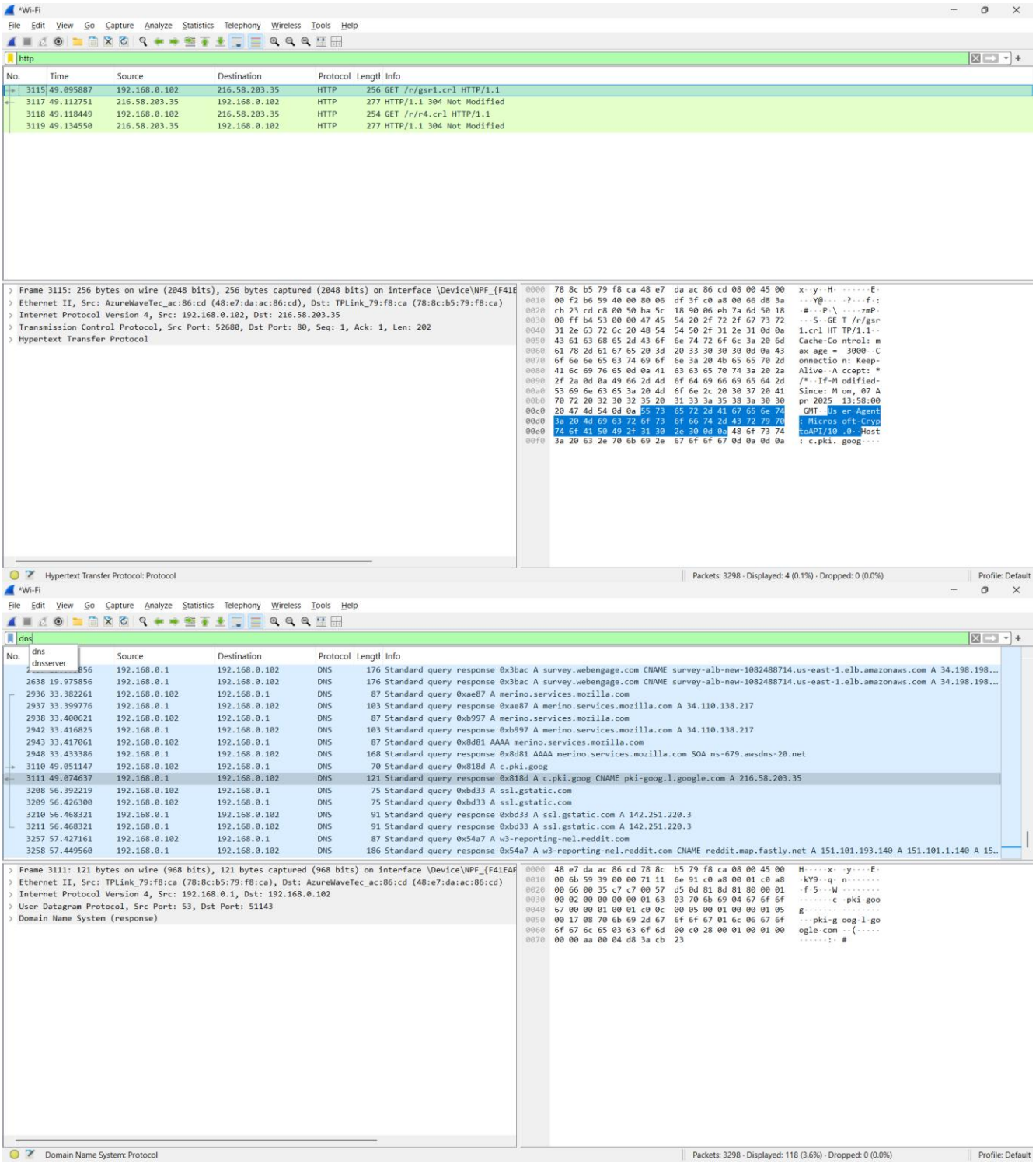


4. Stop capture after a minute.

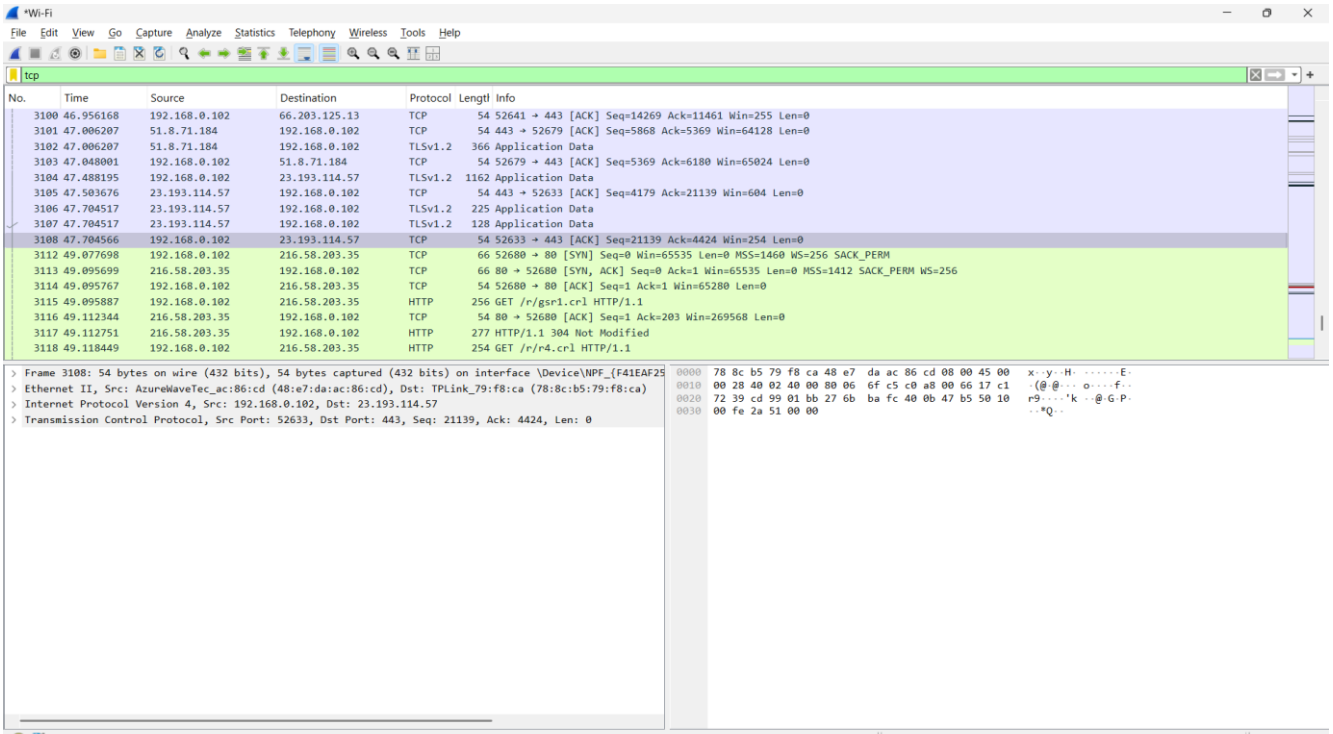


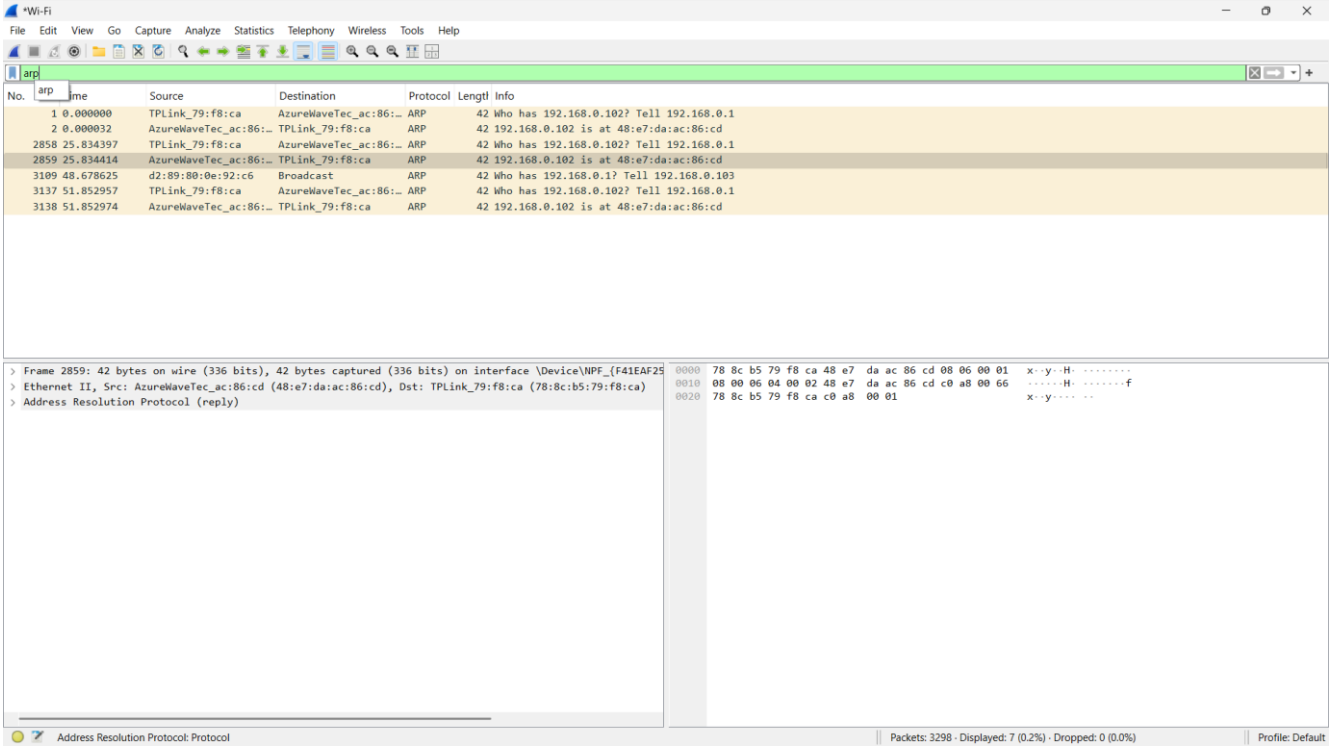
Task 5th: Capture and Analyze Network Traffic Using Wireshark

5. Filter captured packets by protocol (e.g., HTTP, DNS, TCP).



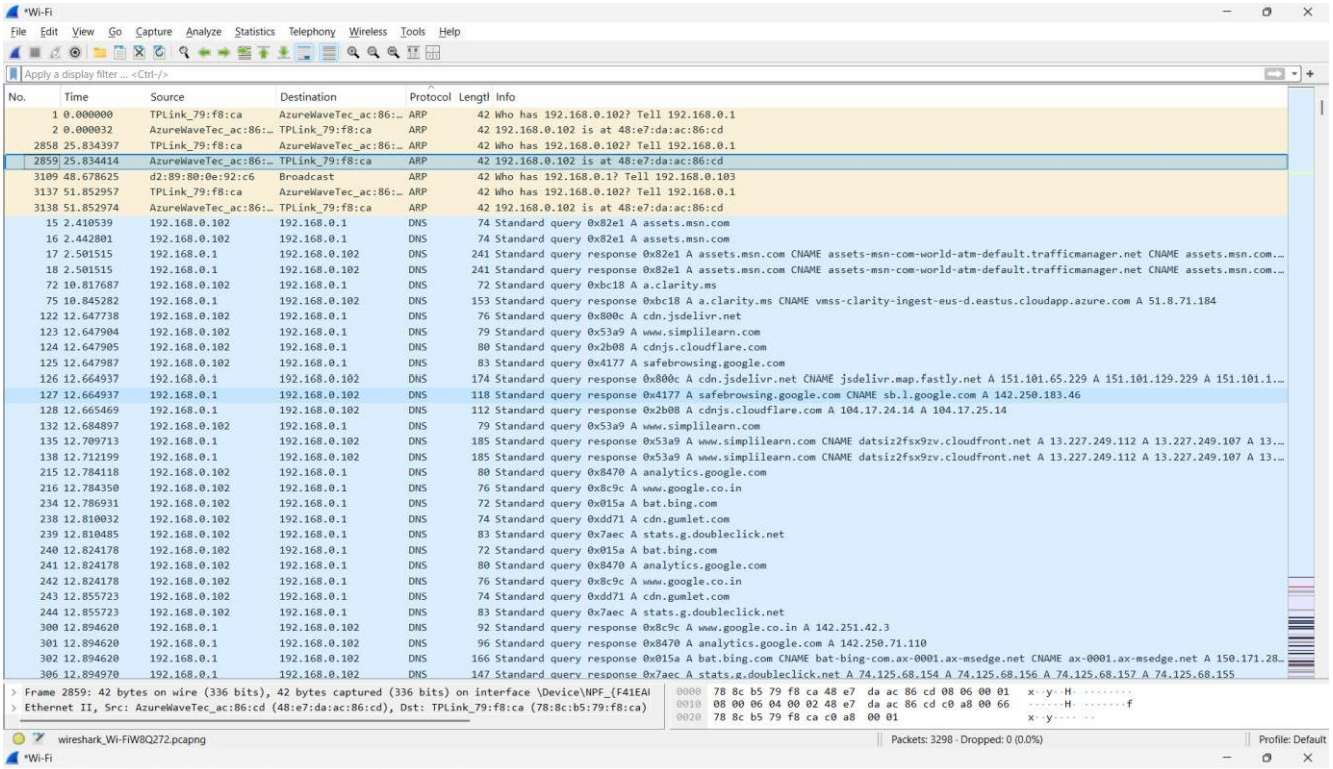
Task 5th: Capture and Analyze Network Traffic Using Wireshark

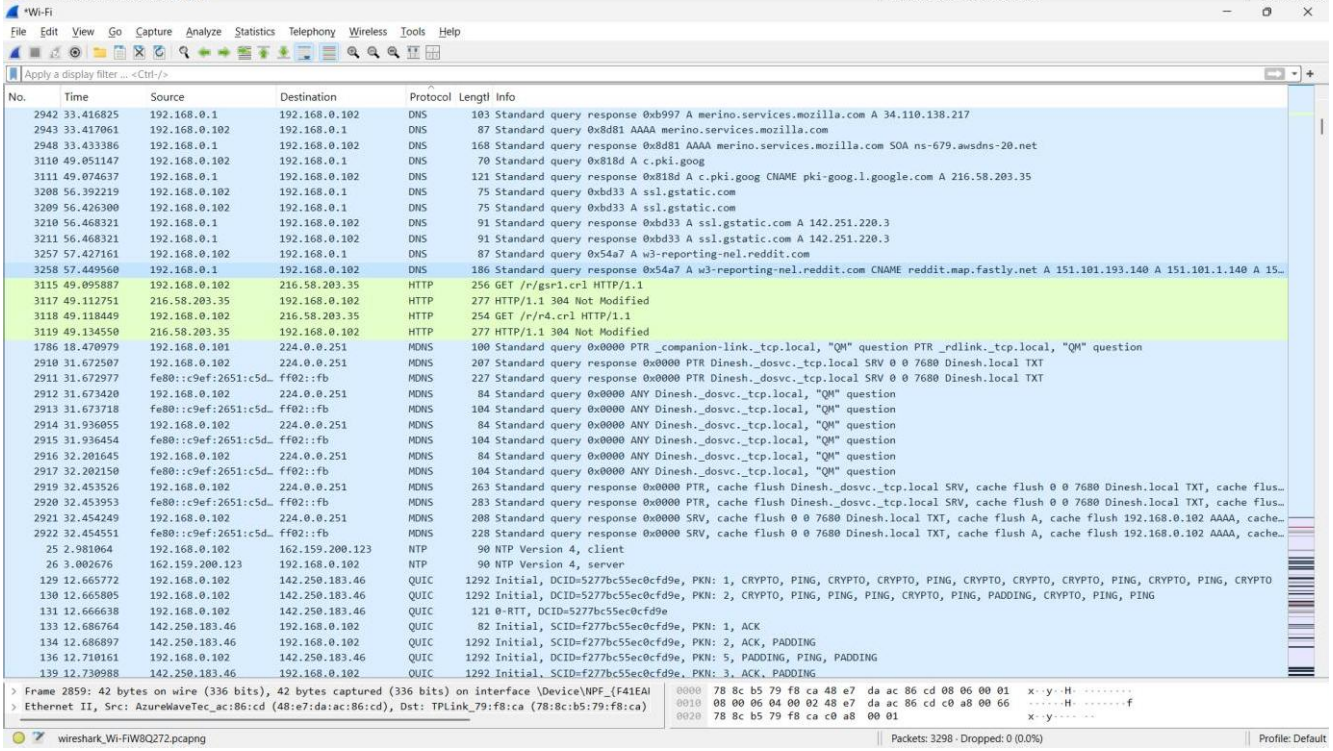




Task 5th: Capture and Analyze Network Traffic Using Wireshark

6. Identify at least 3 different protocols in the capture.



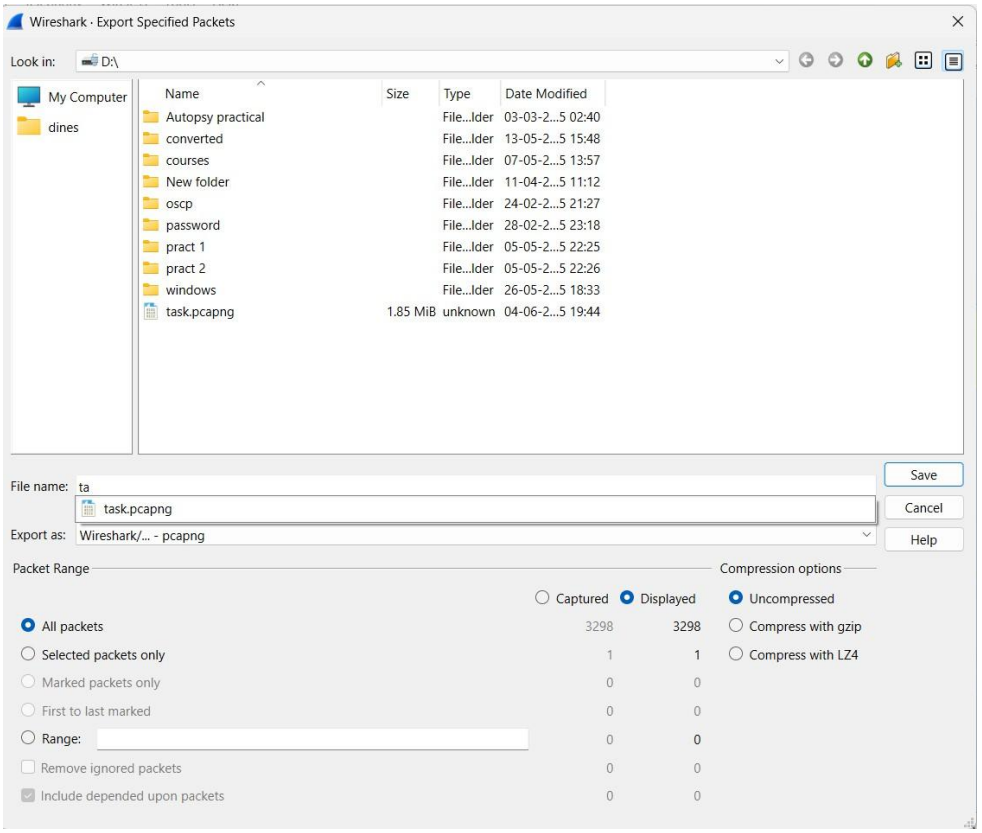


Task 5th: Capture and Analyze Network Traffic Using Wireshark

7. Export the capture as a .pcap file.

- **Go to File > Export Specified Packets or File > Save As.**
- **Save the file as .pcap**

  (e.g.,internship_capture.pcap).



8. Summarize your findings and packet details.

Cyber Security Wireshark Capture Summary

Date/Time of Capture: June 4, 2025

Duration: 1 minute

Interface: Wi-Fi (wlan0)

Protocols Observed:

1. **TCP – Core protocol used for reliable transport between devices.**
   - **Example: Connection established to 142.250.190.78 (Google IP).**

2. **DNS – Resolved domain names to IP addresses.**
    - **Example: www.google.com resolved to 142.250.190.78.**
3. **HTTP – Unencrypted web traffic.**
    - **Example: GET request to http://example.com/index.html.**

Interesting Observations:

- **Several TCP handshakes (SYN, SYN-ACK, ACK) visible.**
- **Multiple DNS queries and responses, showing hostname resolution.**
- **HTTP GET requests and responses with headers and HTML data.**
- **Minimal ICMP traffic from ping tests.**