Task 3: Analyze Network Traffic

* **OBJECTIVE**

Task: Monitor and analyze network traffic.

Details:

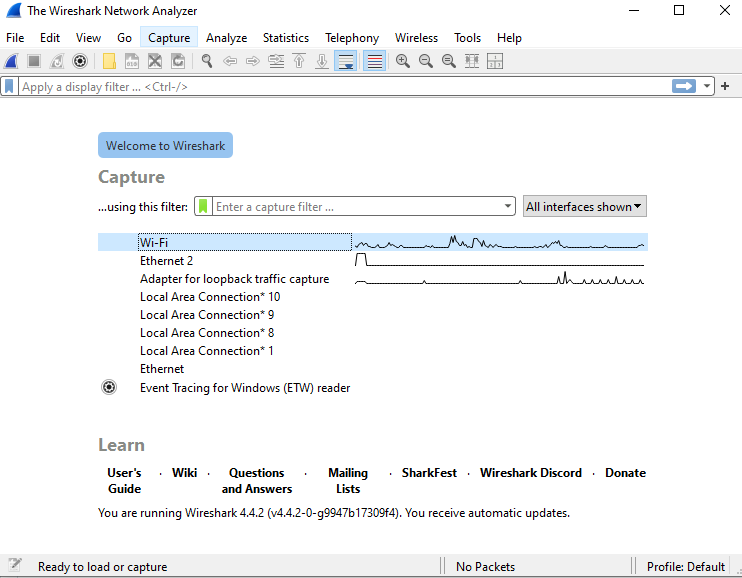
Use a tool like Wireshark to capture and analyze network packets.

Identify common network protocols and traffic patterns.

* **STEPS**

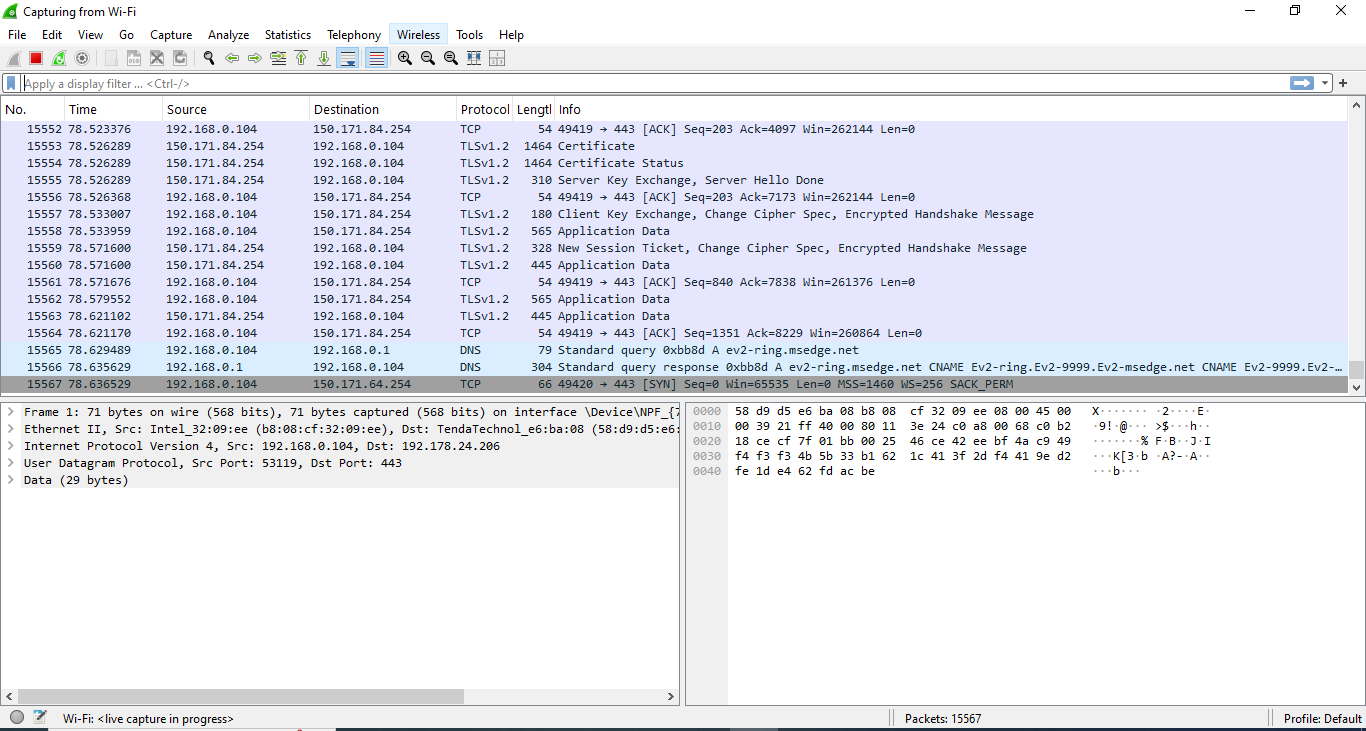
# 1: Launch Wireshark:

o Opened the Wireshark application, which displayed available network interfaces such as Wi-Fi and local area connections.



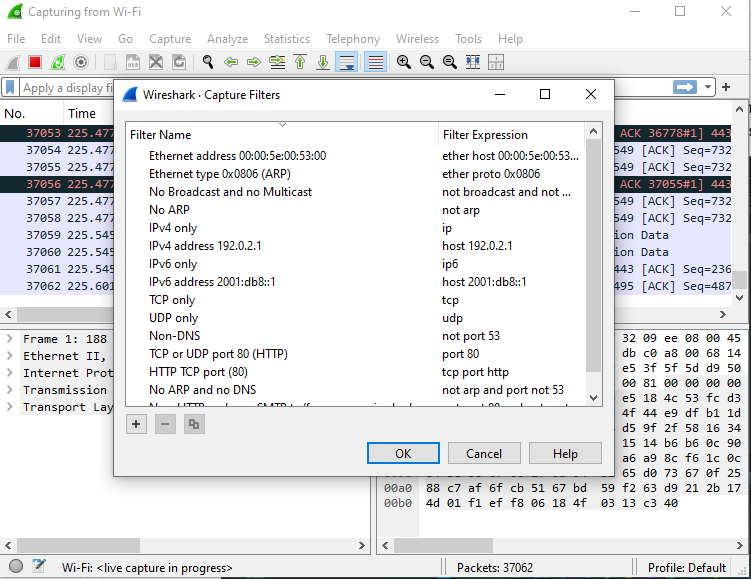
# 2: Select Network Interface:

* Choose the **Wi-Fi** interface to start monitoring the wireless network traffic.



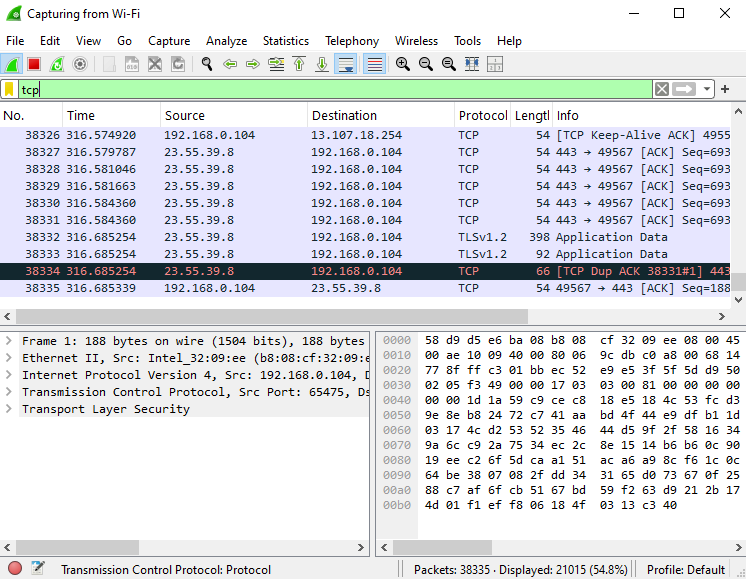
# 3: Capture Packets:

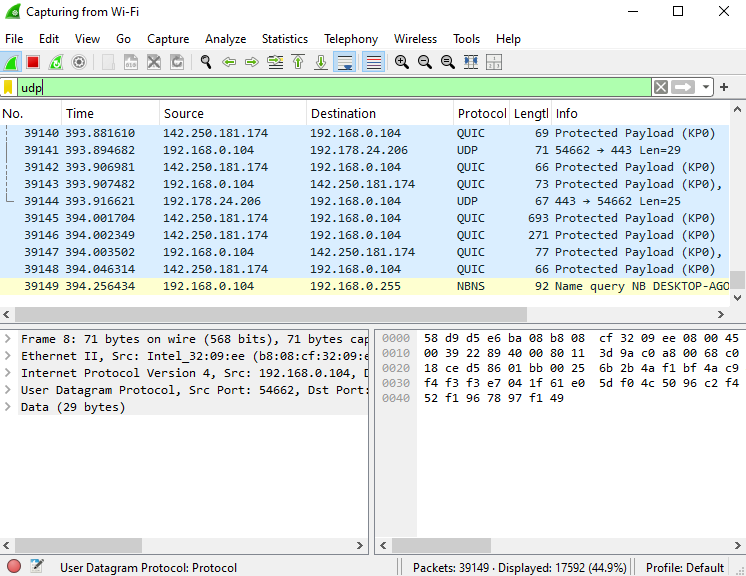
* Initiated the packet capture, allowing Wireshark to record all network traffic over the selected interface. I collected a total of **141 packets** for analysis.



# 4: Apply Display Filters:

* From the **Analyze** option in the top menu, I accessed the **Display Filter** section, which showed various predefined filters.
* In the top search bar labeled "Apply a display filter," I typed **tcp** to filter and display all TCP- related packets.
* Similarly, I applied the **udp** filter, which displayed only UDP packets.

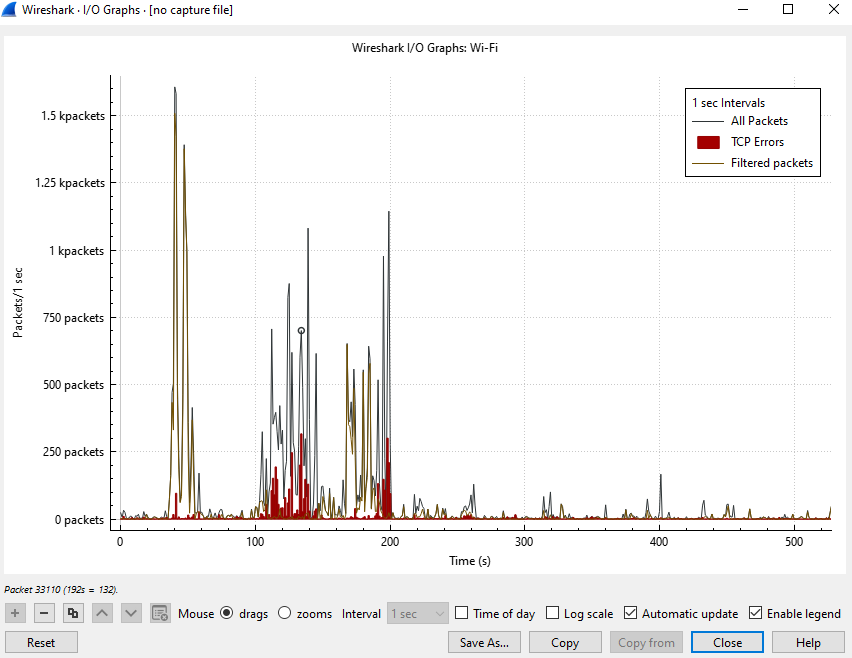




# 5: View I/O Graphs:

* Click on **Statistics** in the top menu and select **I/O Graphs** to view a graphical

representation of network traffic. The graph displayed TCP traffic errors, allowing for further analysis.



# 6: Analysis of Packets:

## Initial Handshake (TCP, TLS, ǪUIC):

* + - Packets 1-3 show the **TCP three-way handshake** between the local machine and an external server, indicating the start of a communication session.

## Encrypted Traffic:

* + - Many packets (such as 10, 12, 14) involve **encrypted TLS data**.

## ǪUIC Protocol:

* + - Packets like 50-90 involve ǪUIC, a relatively new protocol running over UDP for faster and more secure web communications (used by platforms like Google).

## Connection Resets and Alerts:

* + - Packets like 21 and 22 show **RST, and ACK flags**, indicating connection resets. Reset flags can suggest issues with connections or intentional termination.

## DNS Ǫueries:

* + - Packets 43 and 44 show **DNS queries** from your local machine to the router, specifically querying the domain google.com.