**Task 5: Capture and Analyze Network Traffic Using Wireshark**

Objective: **Capture live network packets and identify basic protocols and traffic types**

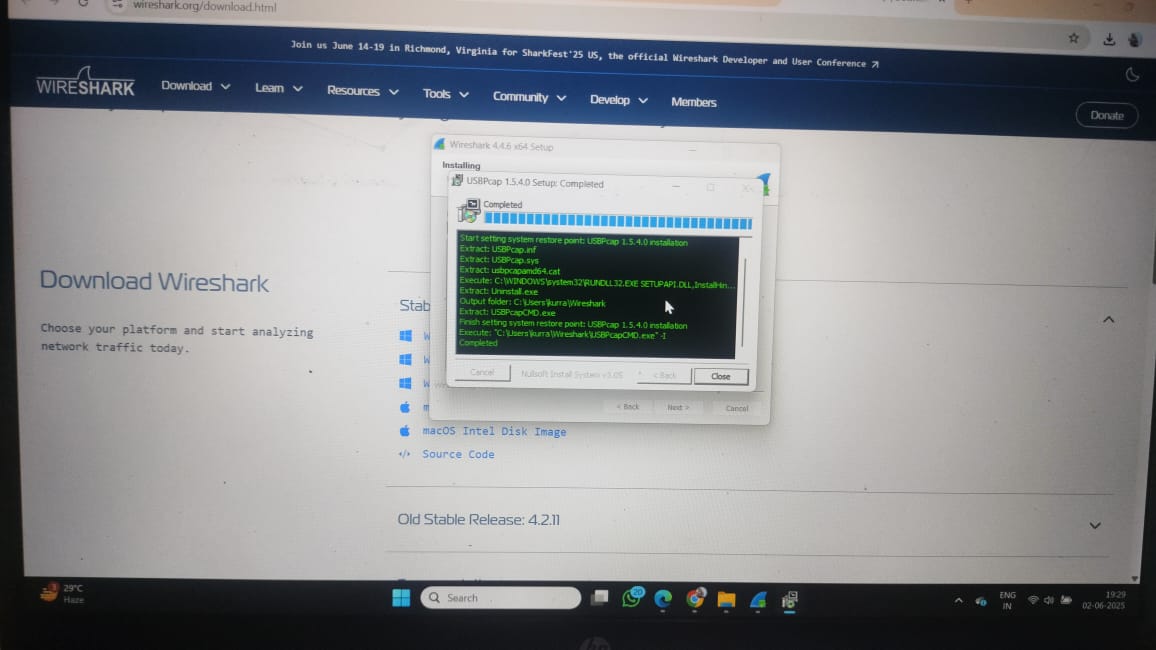
Tools: **Wireshark (free).**

Deliverables: **A packet capture (.pcap) file and a short report of protocols identified.**

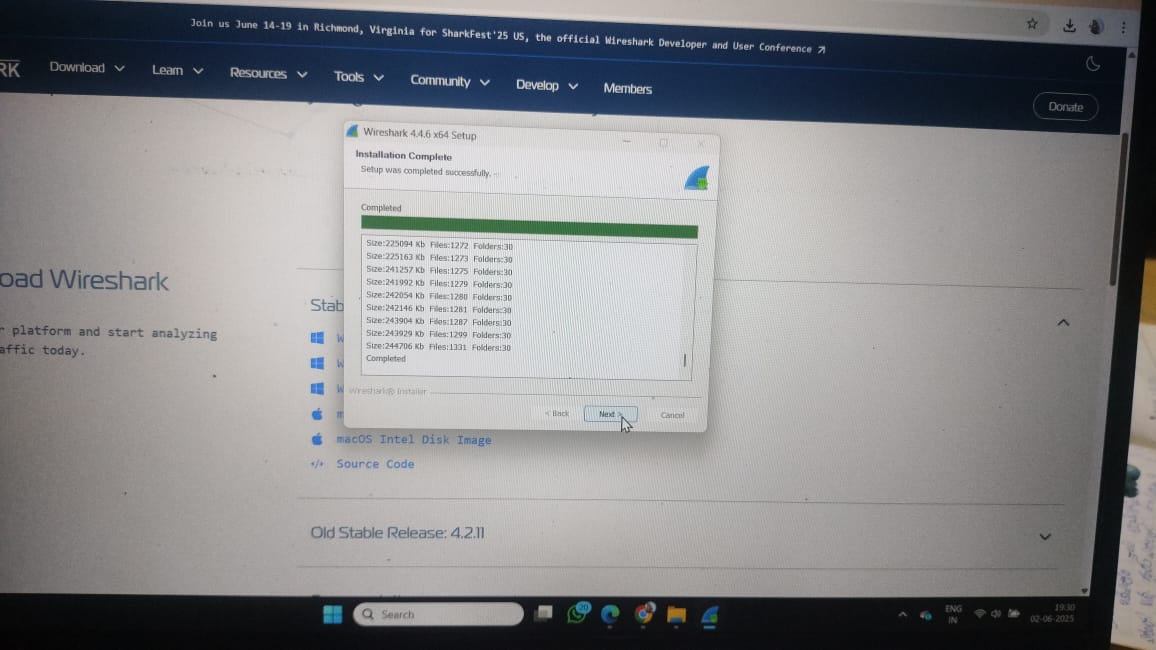
**🔧 Step 1: Install Wireshark**

**What to do:**

1. Go to https://www.wireshark.org/download.html.
2. Download the installer based on your operating system (Windows/macOS/Linux).



1. Run the installer and follow the on-screen instructions.
2. On Windows, during installation, allow **WinPcap** or **Npcap** to be installed — this is required to capture packets.

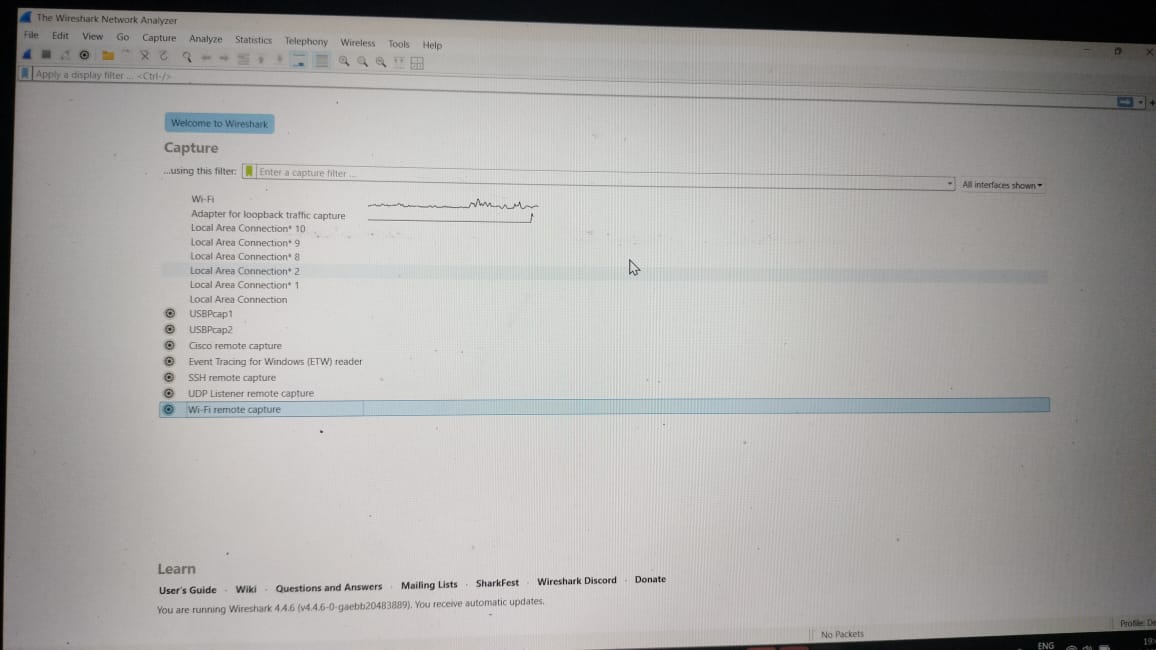


**Purpose:**  
Wireshark is a network protocol analyzer. Installing it lets you capture and view real-time network data.

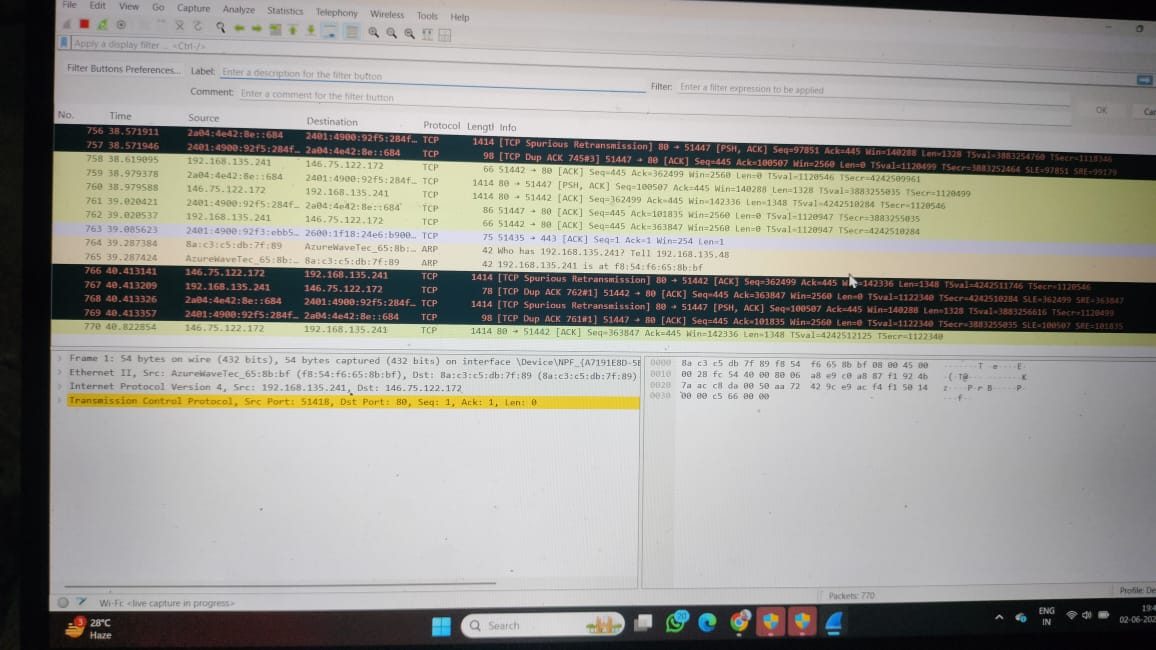
**🌐 Step 2: Start Capturing on Active Network Interface**

**What to do:**

1. Open Wireshark.
2. On the main screen, you’ll see a list of available network interfaces.



1. Identify the active interface (e.g., Wi-Fi if you're on wireless, or Ethernet if wired).
2. Double-click the active interface to start capturing packets.

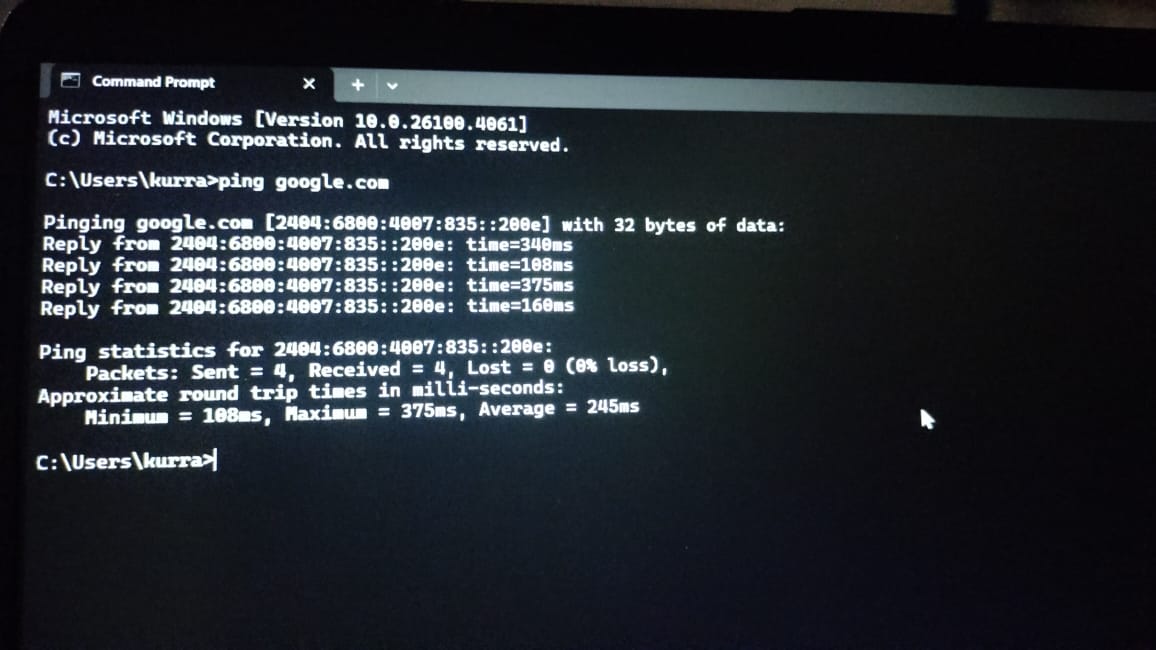


**Purpose:**  
Wireshark must listen to the correct interface to capture your actual internet traffic.

**🌍 Step 3: Generate Traffic (Simulate Network Activity)**

**What to do:**

1. While Wireshark is capturing:
   * Open a browser and visit a few websites (e.g., http://example.com, https://google.com)
   * Open Command Prompt or Terminal and type: ping google.com



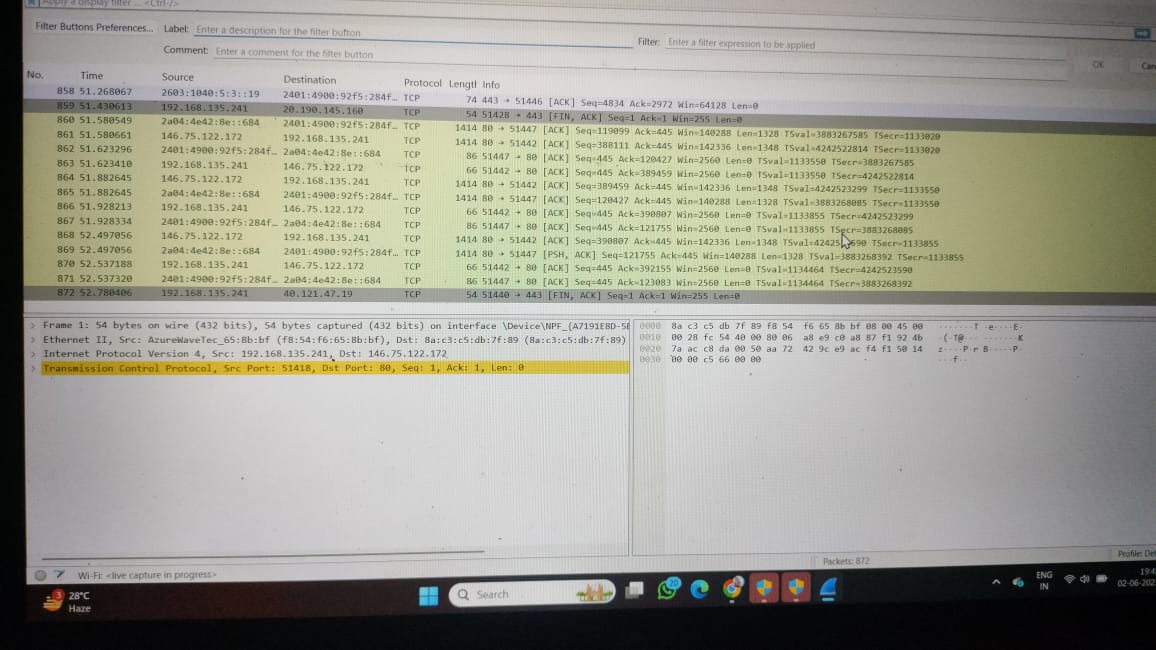
1. You can also open apps like email clients or YouTube for more diverse traffic.

**Purpose:**  
This creates visible, analyzable traffic in the capture (like HTTP, HTTPS, DNS, ICMP).

**⏹ Step 4: Stop Capture After a Minute**

**What to do:**

1. Let the capture run for about **1 minute**.
2. Click the red square “Stop” button at the top toolbar in Wireshark.



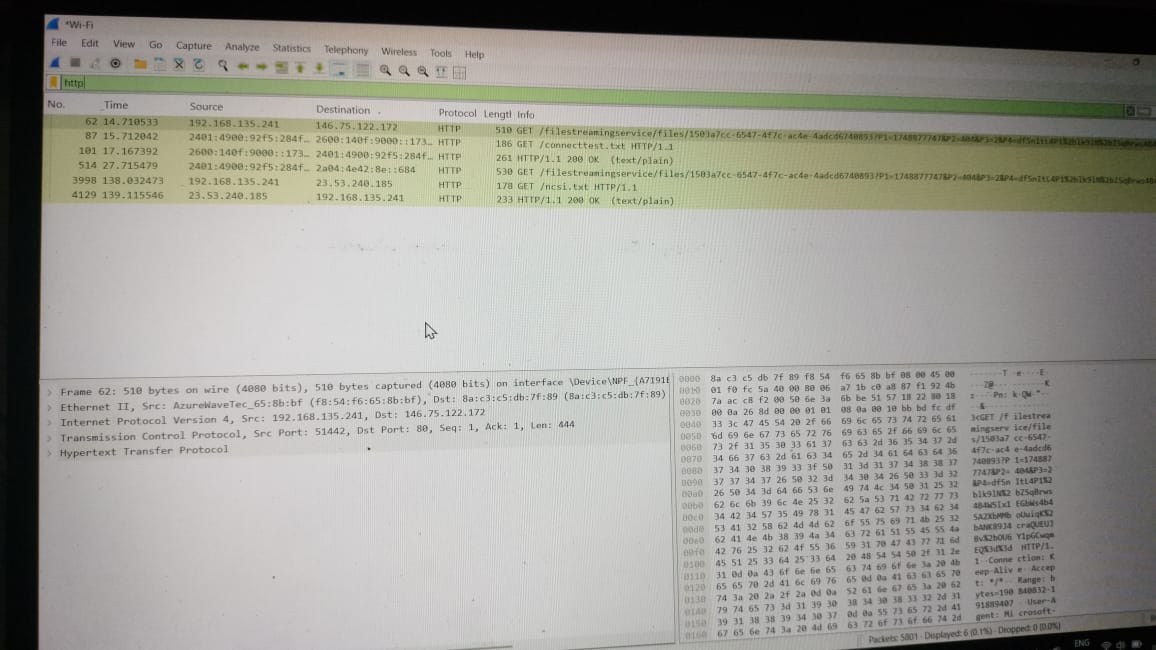
**Purpose:**  
You only need a small sample to analyze multiple protocols. A minute of traffic is plenty.

**🔍 Step 5: Filter Captured Packets by Protocol**

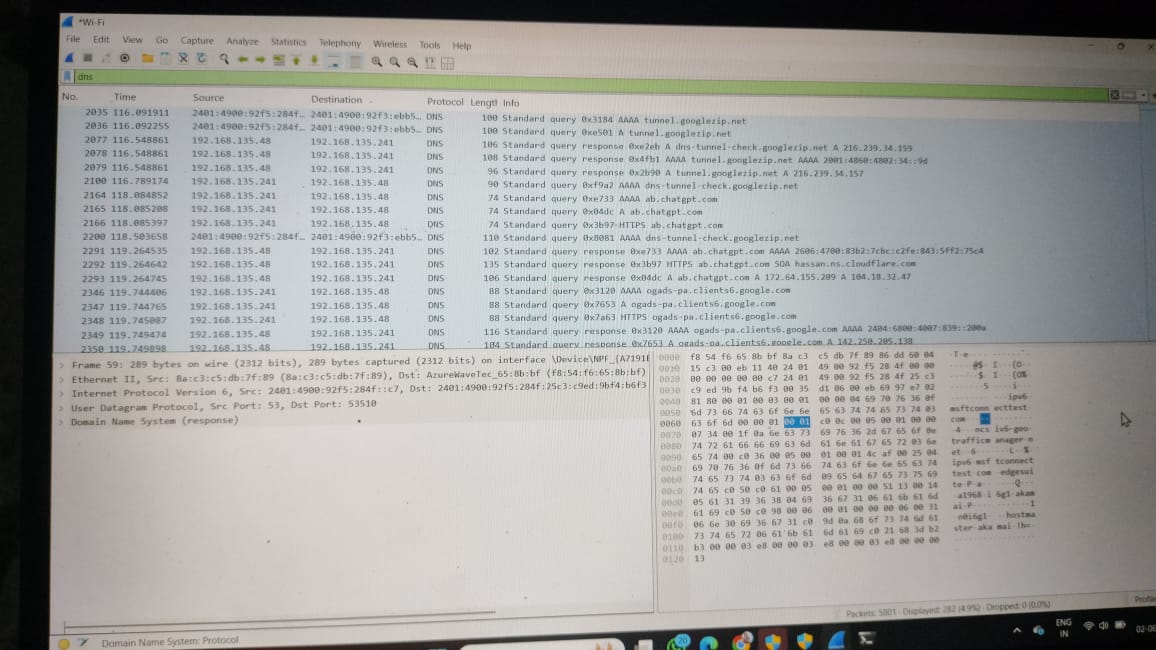
**What to do:**  
Use the **filter bar** (just below the toolbar) to view specific protocol packets.

**Try filtering with:**

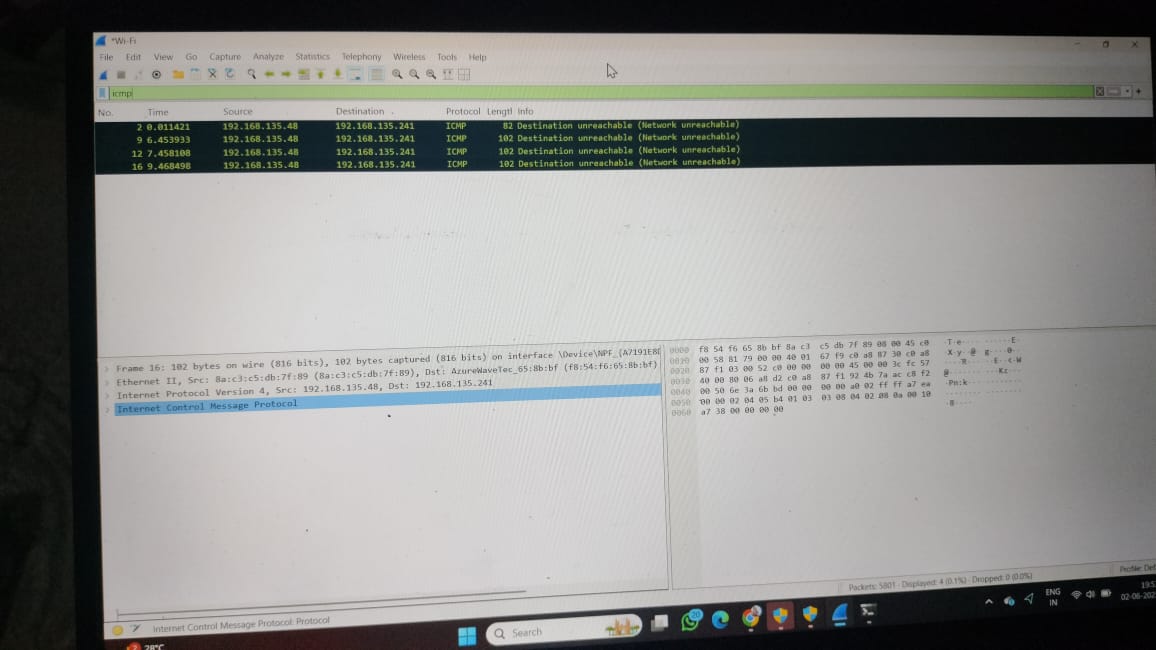
* http – Shows HTTP requests/responses.



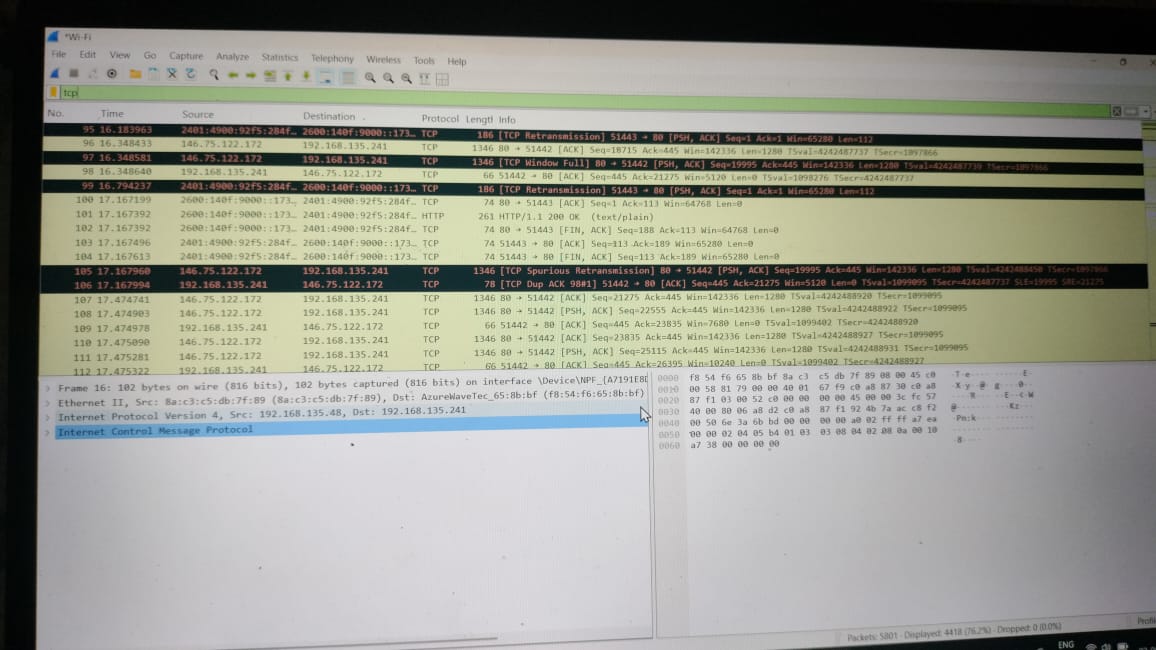
* dns – Shows domain name queries and replies.



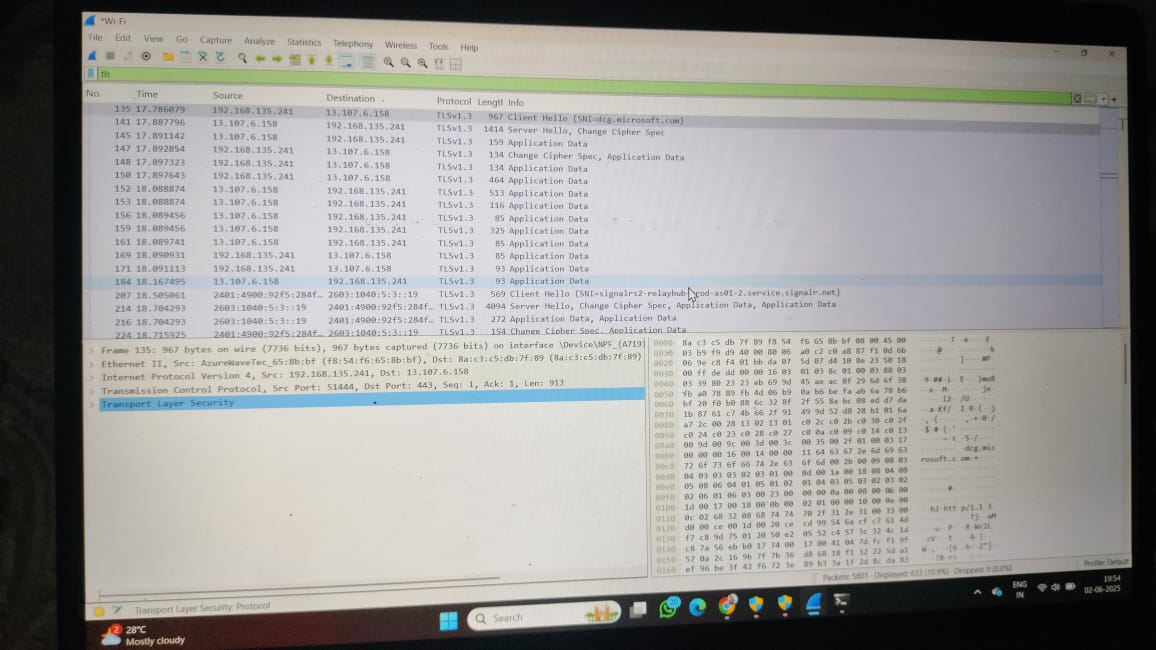
* icmp – Shows ping traffic.



* tcp – Shows all TCP traffic.



* tls – Shows encrypted HTTPS traffic.



**Why:**  
Filtering helps you isolate and study specific types of traffic without being overwhelmed by other data.

**🔎 Step 6: Identify At Least 3 Different Protocols**

**What to do:**  
Look at packet details and note:

* The **protocol name**
* What it's used for
* Example packet contents

**Example:**

1. **DNS** – Resolves domain names to IPs.
   * Filter: dns
   * Look for queries like A google.com
2. **HTTP** – Web browsing (unencrypted).
   * Filter: http
   * Look for GET/POST requests
3. **ICMP** – Used for ping.
   * Filter: icmp
   * Shows echo requests/replies

**Why:**  
Understanding common protocols is essential for network analysis.

**💾 Step 7: Export the Capture as a .pcap File**

**What to do:**

1. Go to **File > Save As**.
2. Choose a location and name, e.g., network\_traffic\_analysis.pcap.
3. Make sure the file format is set to **Wireshark/tcpdump/... - pcap**.
4. Click **Save**.



**Open file to capture and analyse network traffic using wireshark**

**Conclusion:**

**Capturing and analyzing network traffic with Wireshark provides valuable insight into how data moves across a network. Through this hands-on activity, we were able to observe real-time packet exchanges, identify multiple network protocols (such as DNS, HTTP, TCP, and ICMP), and understand how devices communicate over the internet.**

**This exercise enhanced our understanding of:**

* **Network layers and protocol functions**
* **How requests (like browsing a website or pinging a server) generate specific traffic**
* **The structure and content of packets in transit**

**By filtering and examining captured data, we developed fundamental skills in network troubleshooting, security monitoring, and protocol analysis — all of which are essential for anyone pursuing networking, cybersecurity, or IT.**

**Wireshark proves to be a powerful and accessible tool for visualizing network behavior and gaining a deeper awareness of how the internet works under the hood.**