**Lab Practical #09:**

Study Packet capture and header analysis by Wireshark (HTTP, TCP, UDP, IP, etc.)

**Practical Assignment #09:**

1. **Explain usage of Wireshark tool.**

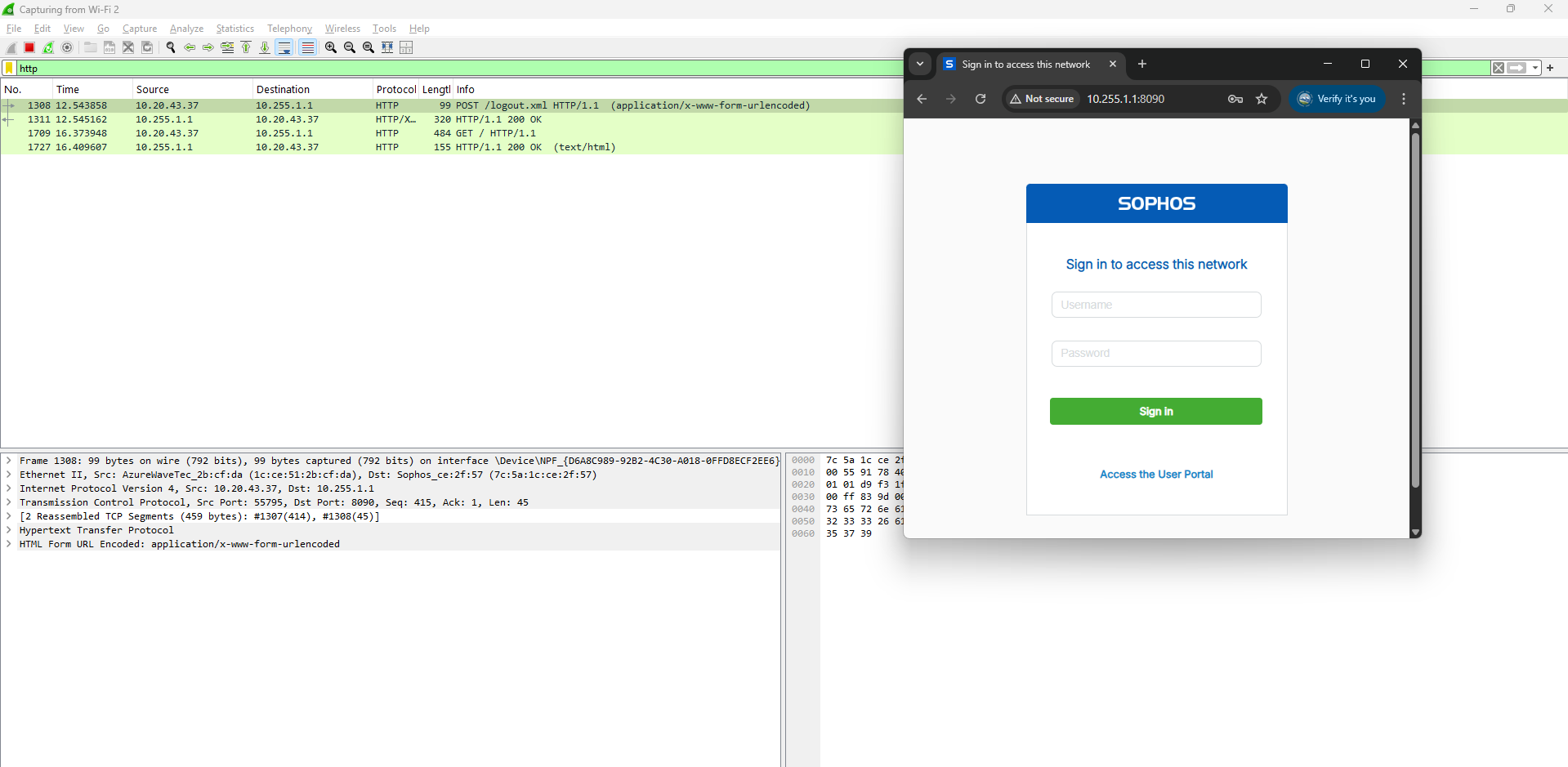
Wireshark is one of the most widely used network protocol analyzers (also called a packet sniffer). It helps network administrators, cybersecurity professionals, and students analyze the traffic moving across a network in real time.

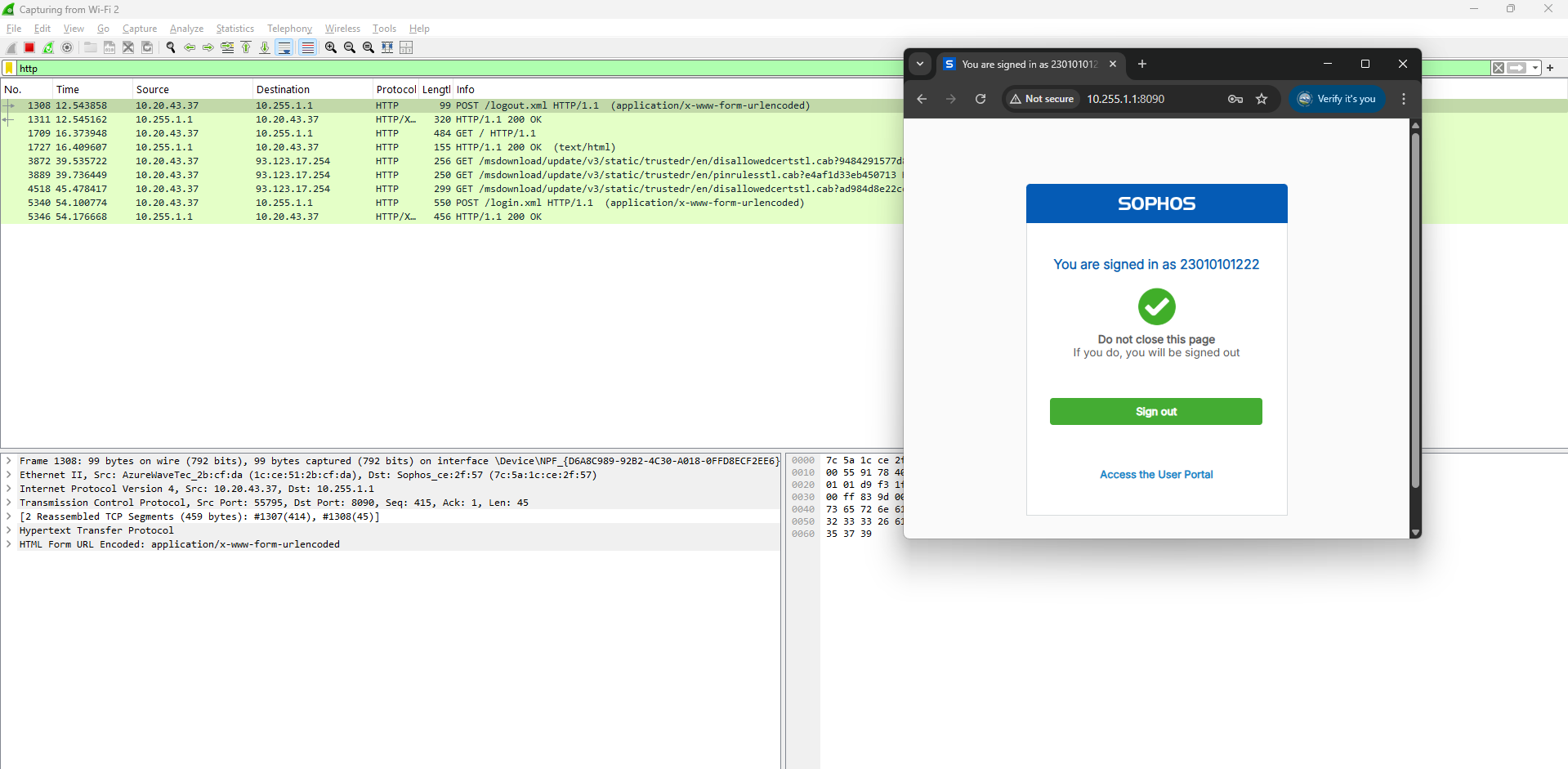
Uses Of WireShark:

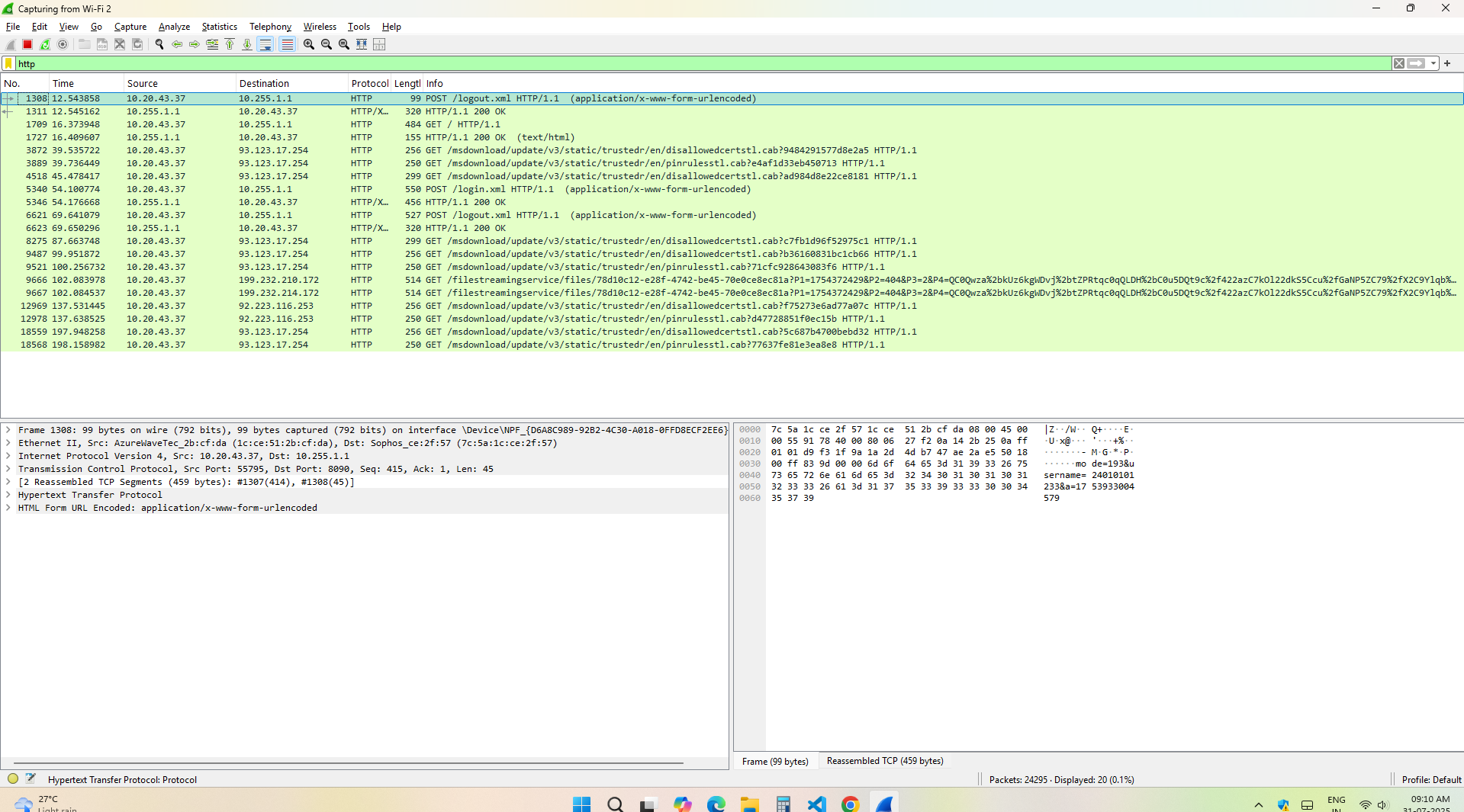
* Wireshark captures live network traffic and logs every packet.
* It analyses and decodes hundreds of protocols in detail.
* It helps troubleshoot issues like latency, packet loss, and misconfigurations.
* It is used for security analysis to detect suspicious or malicious traffic.
* It is useful for learning and researching how networks and protocols work.
* It provides powerful features like filters, statistics, and graphs for better analysis.

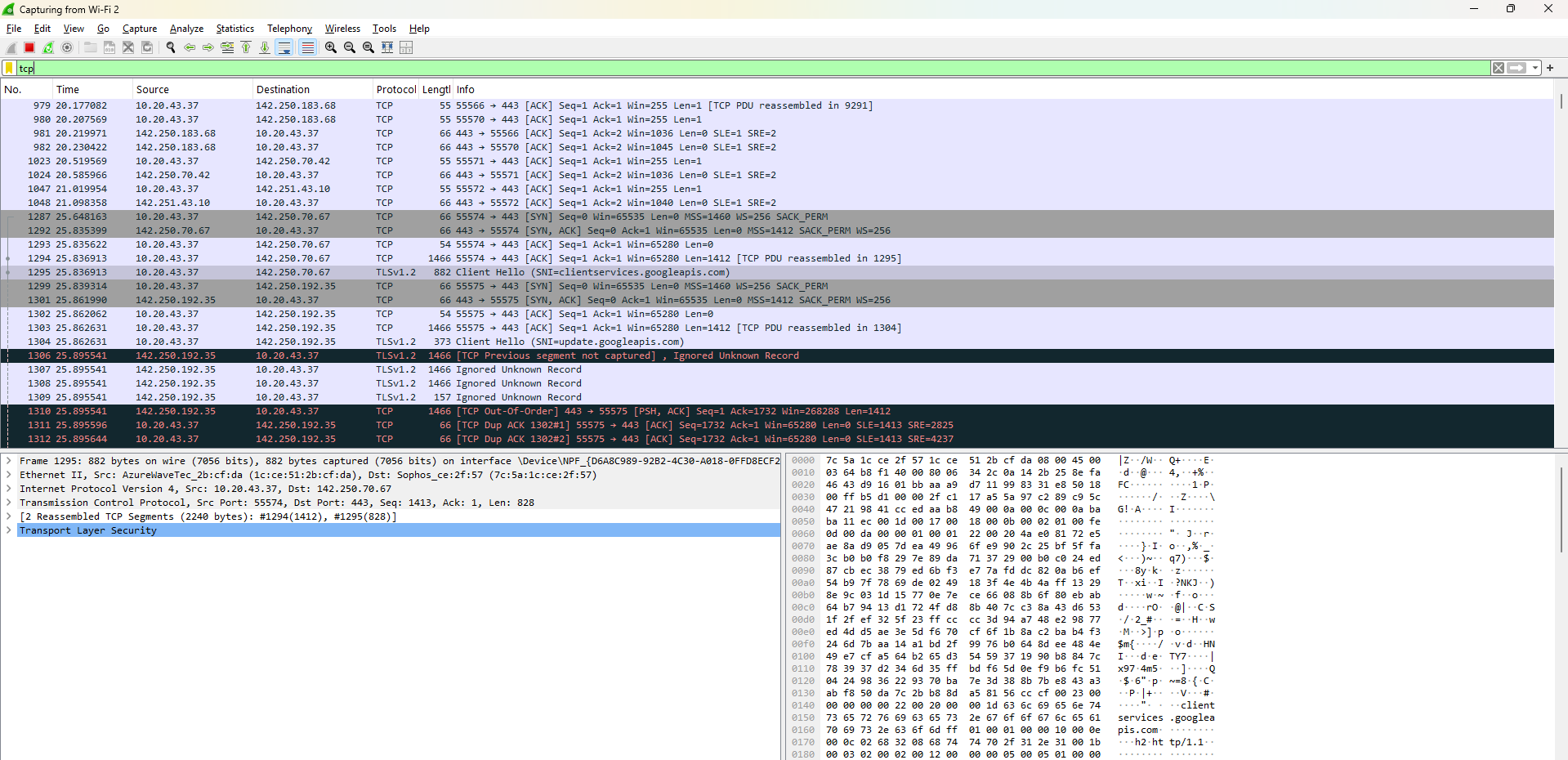
1. **Packet capture and header analysis by Wireshark (HTTP, TCP, UDP, IP, etc.)**

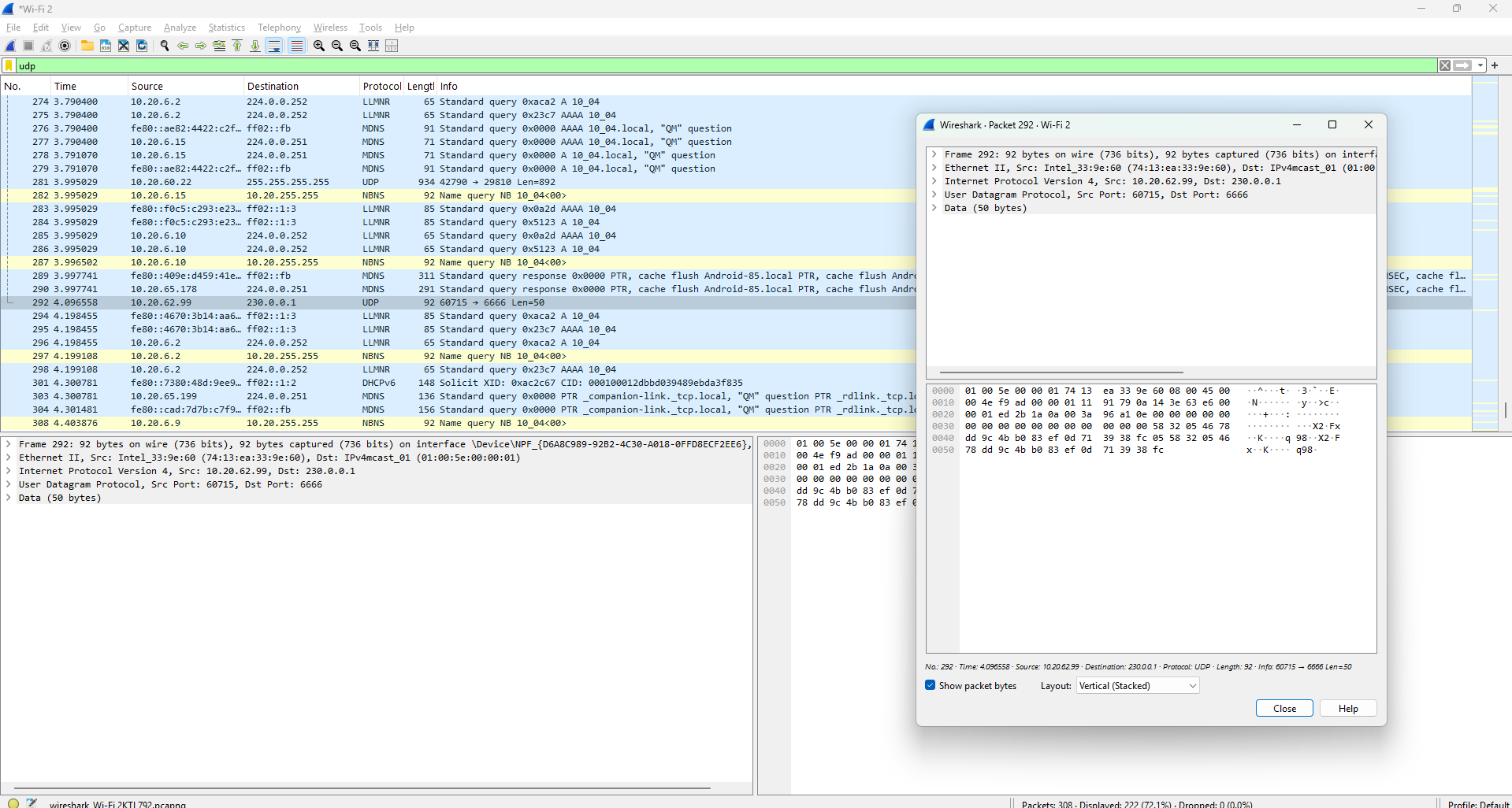
**1)HTTP:**



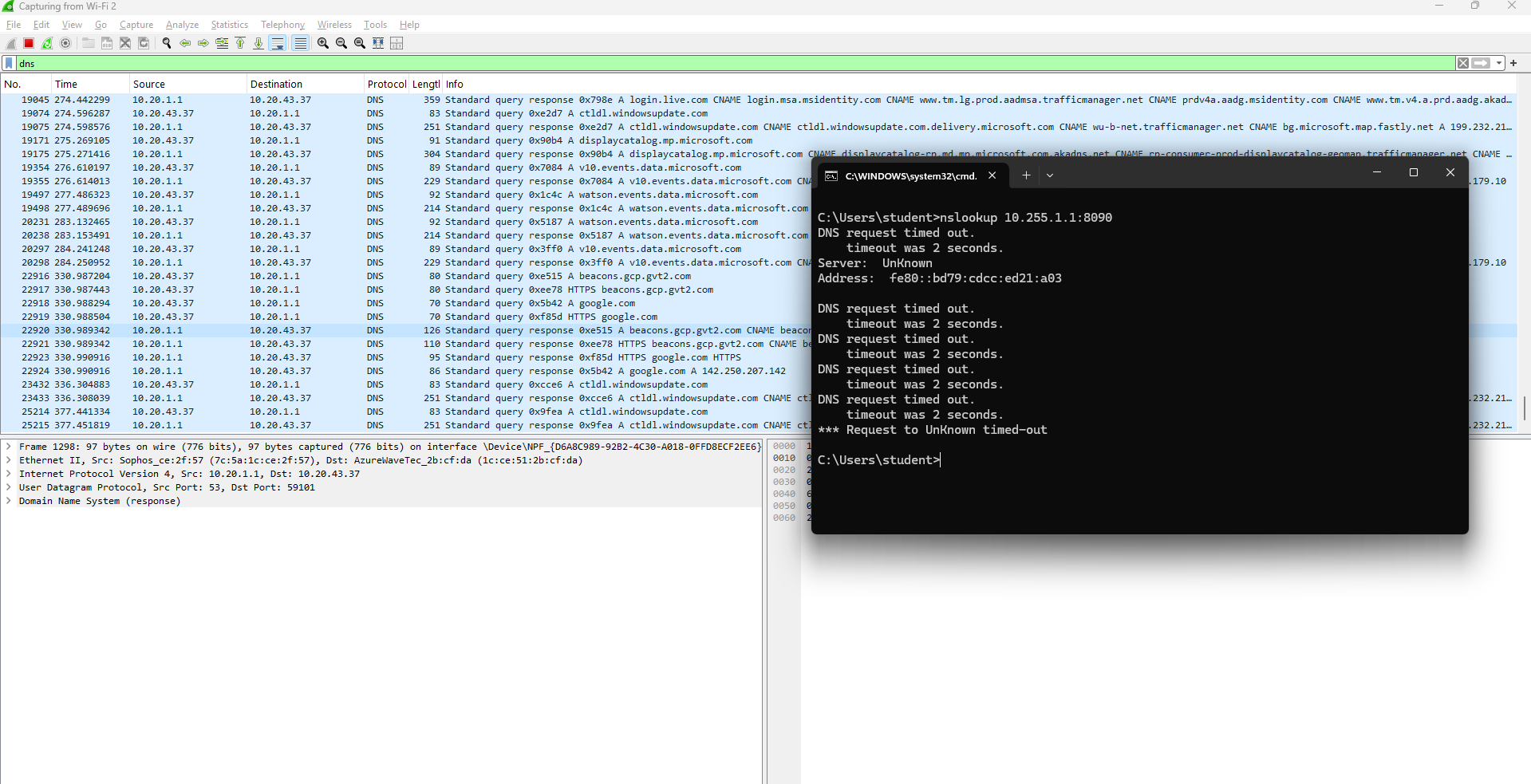
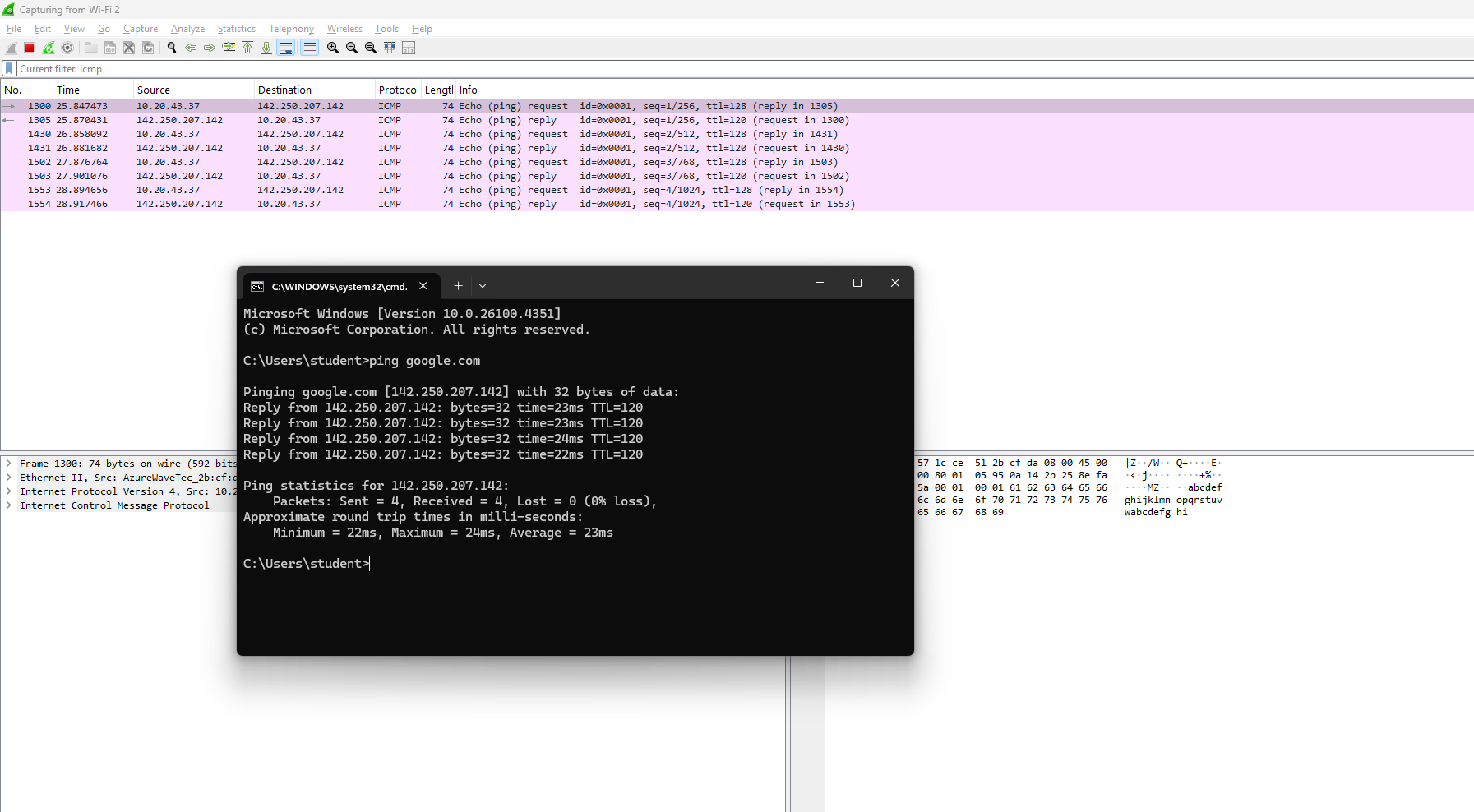




**2)TCP:  
**

**3)UDP:  
**

**4)DNS:**

**5)ICMP:  
**