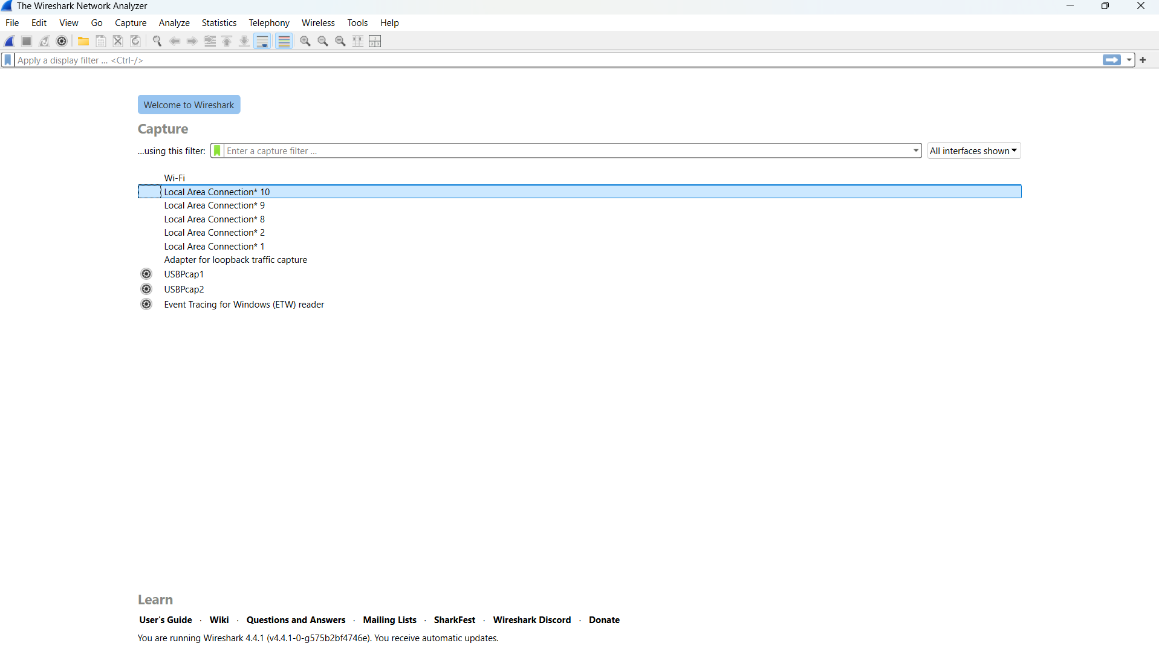
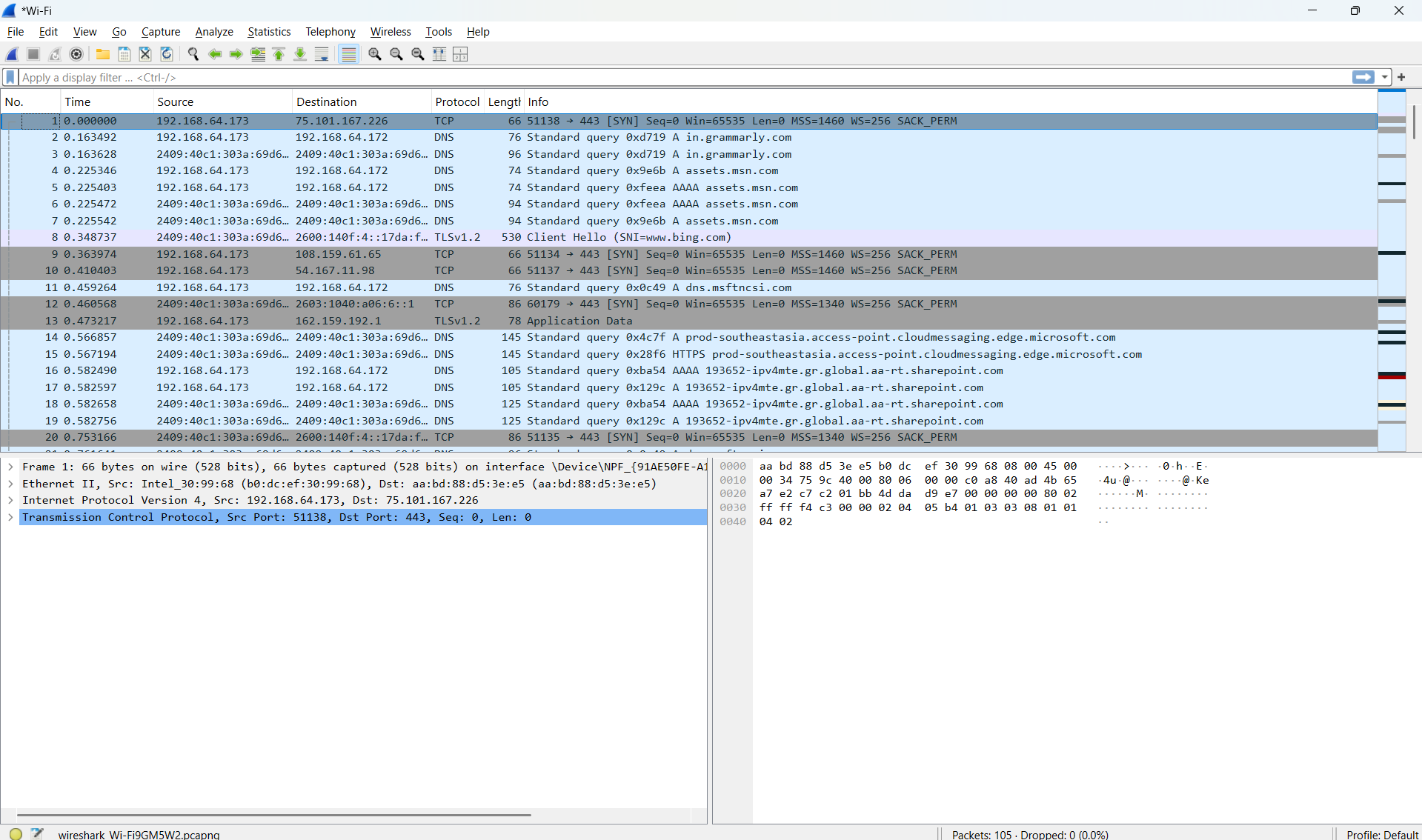
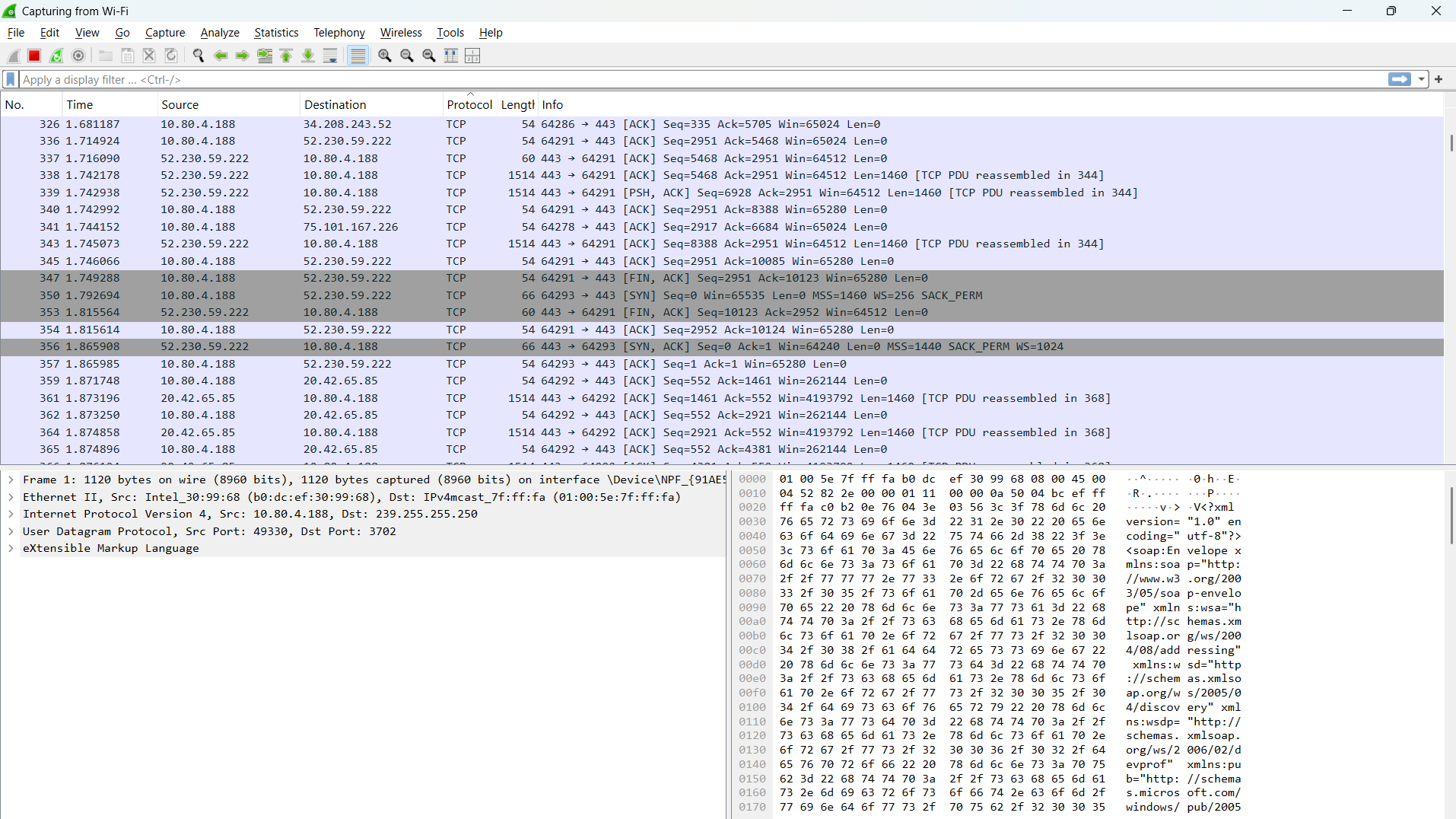
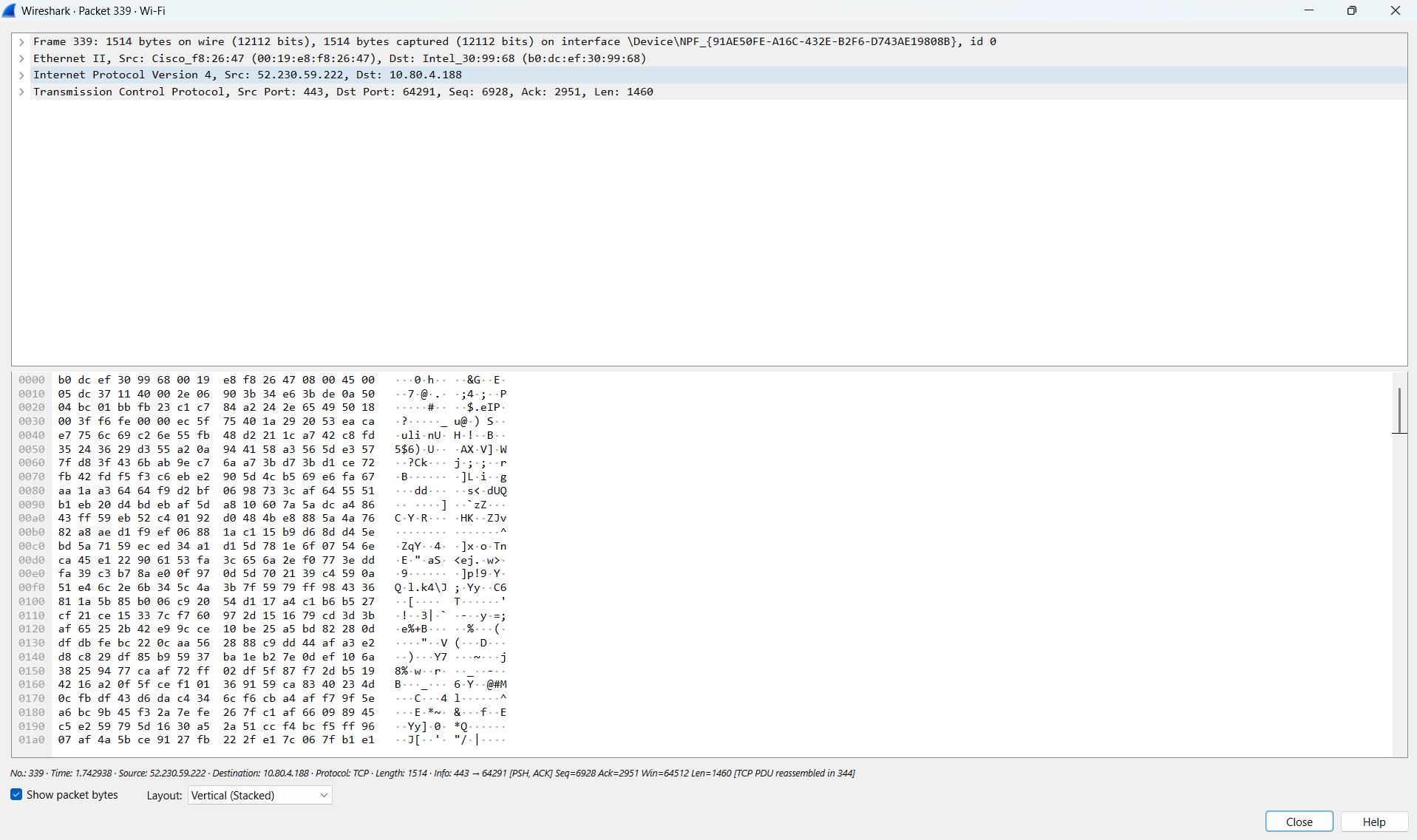
**Aim**: Monitor the live/real time network and analyze the concepts of various networking protocols like IP, TCP, UDP, etc.

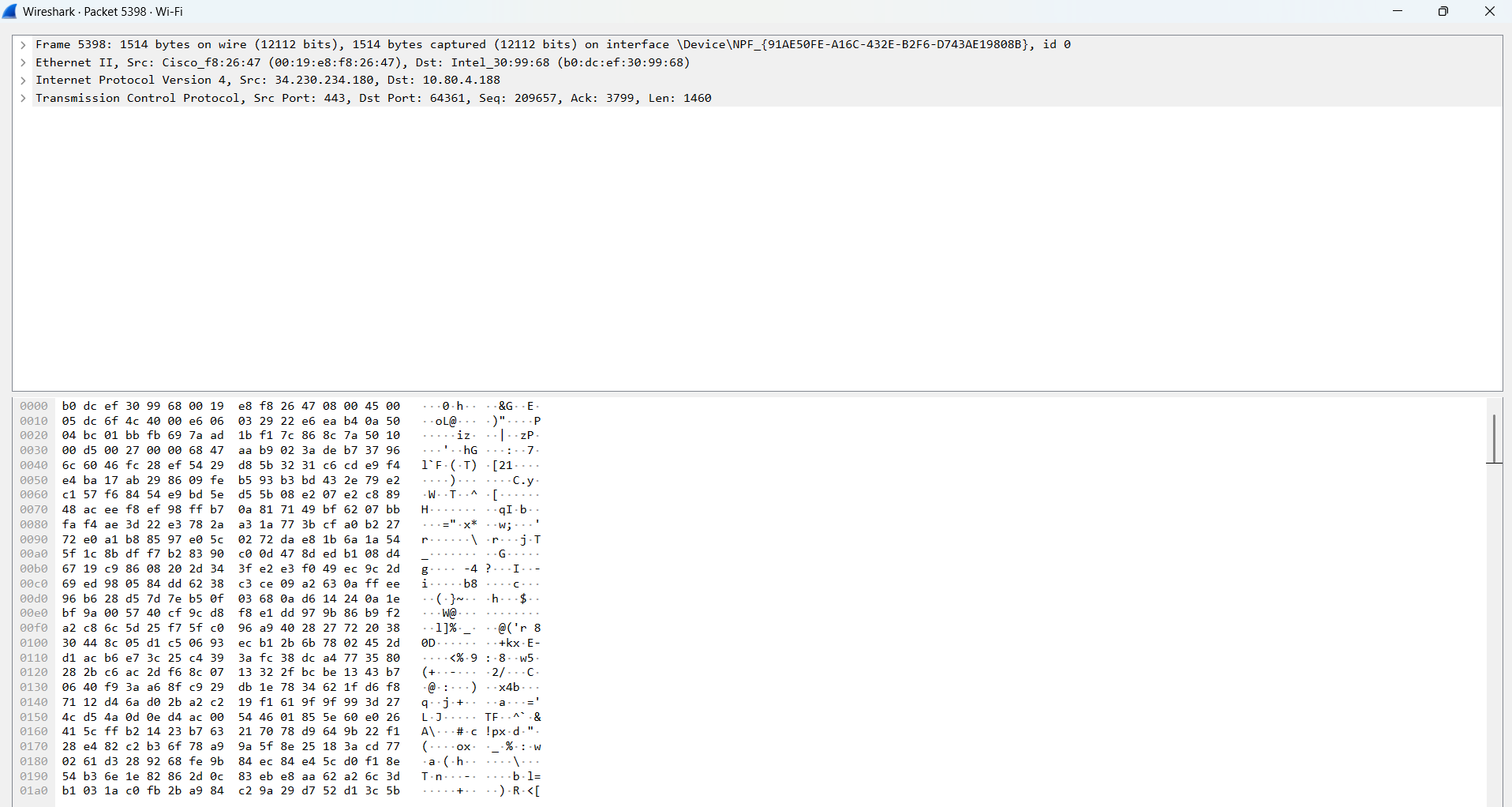
**Step – 1:-** Open Wireshark

**Step – 2 :-**  Select the Network from which you want to communicate

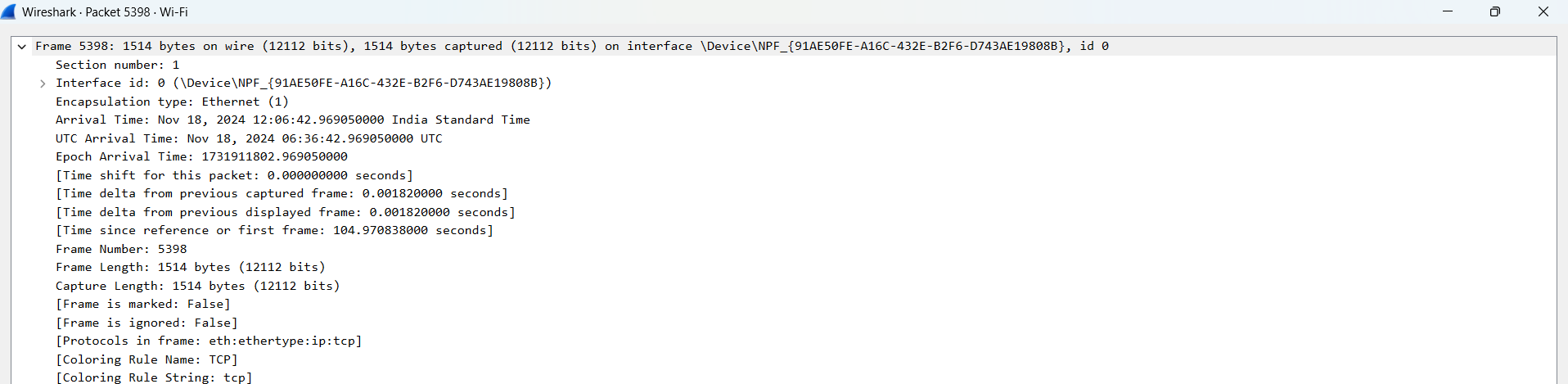


**Step – 3 :-**  Now when we press Protocol button it will sort the packet based on protocol used.

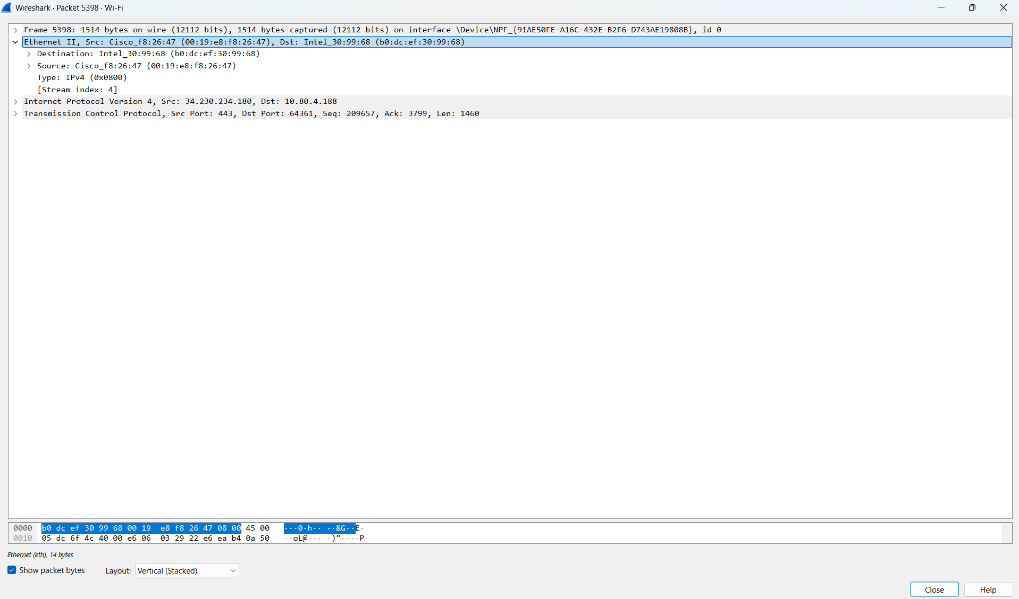
**Step – 4 :-**  Now when we press one of the packet it will open the packet and show every detsils.

**Step – 5 :-**  Now we will analyze one TCP Packet

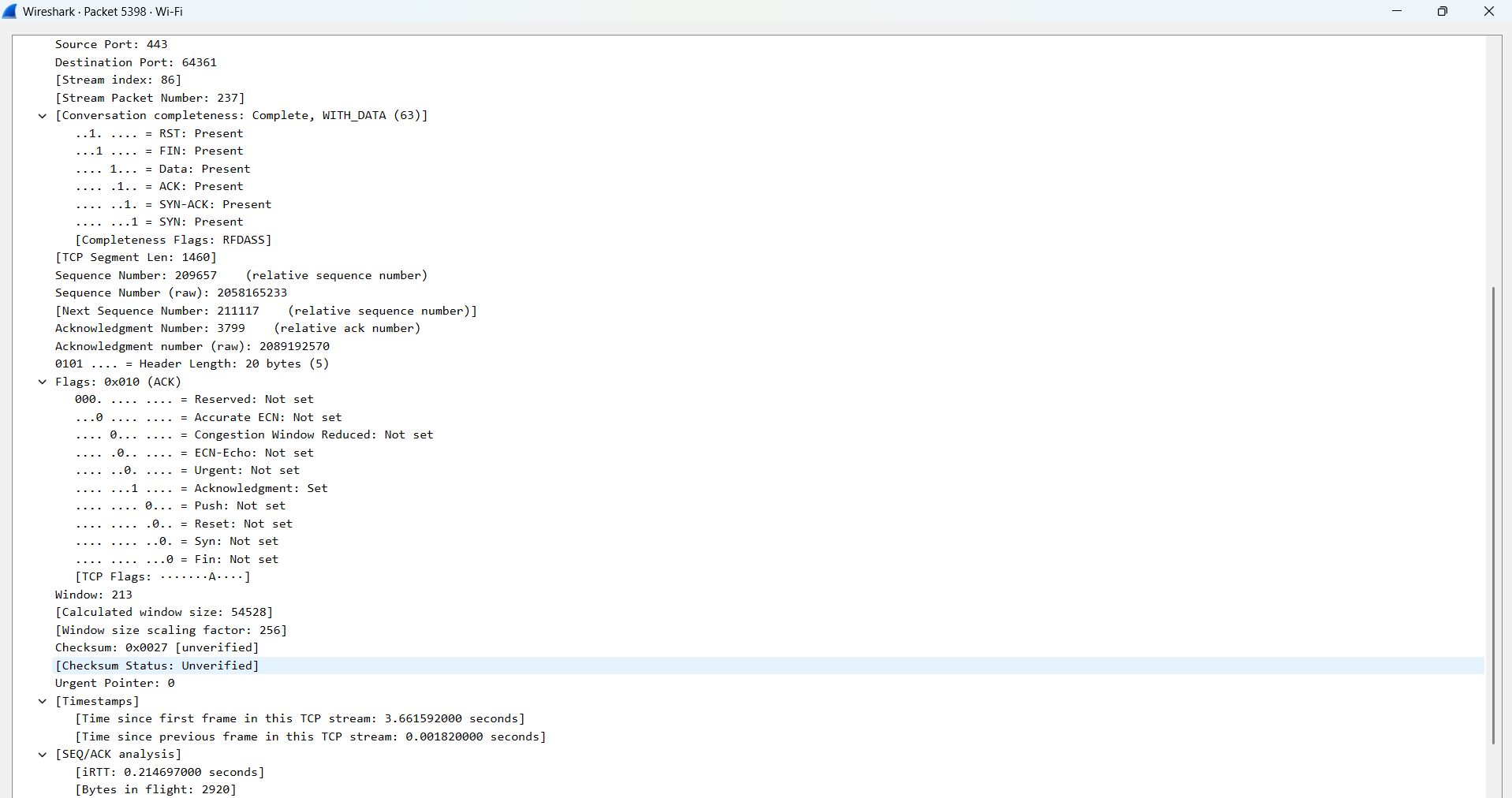
**Step – 7 :-**  Analysis of TCP Packet



* It is the timing details and frame length and frame no.

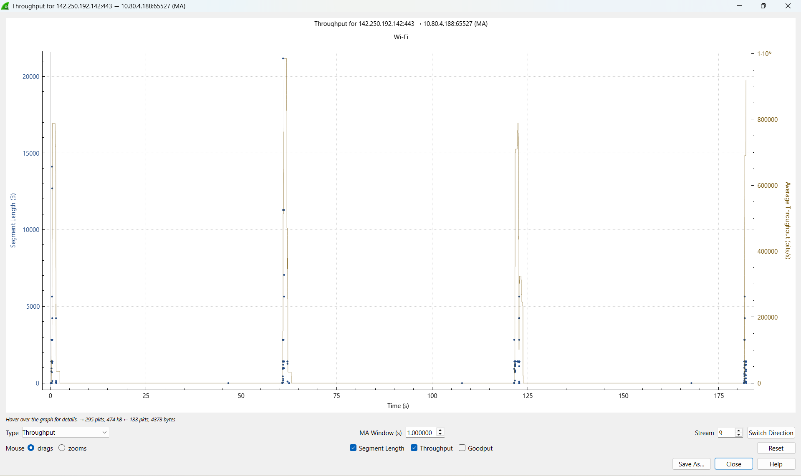
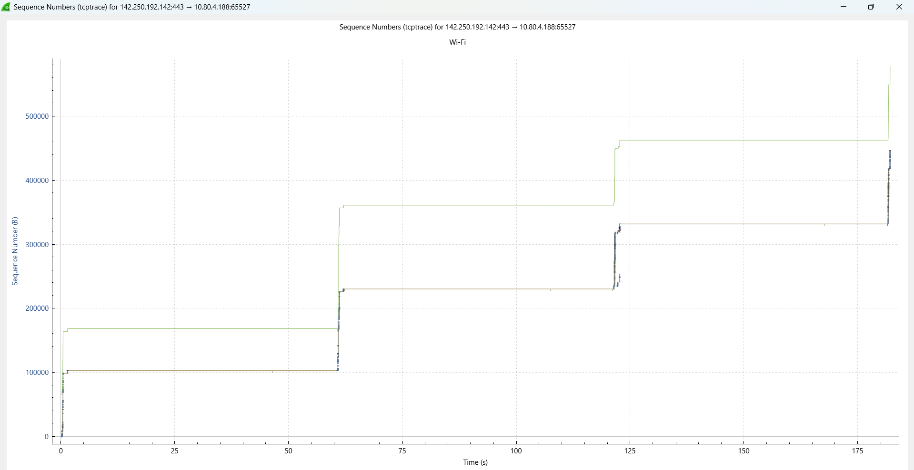
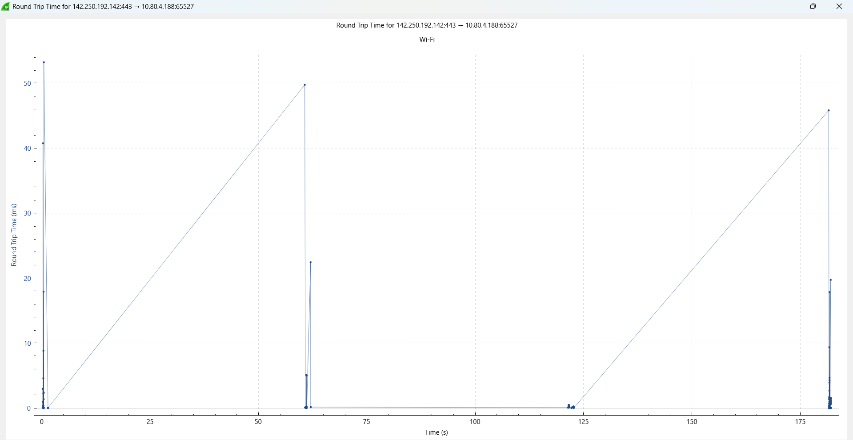
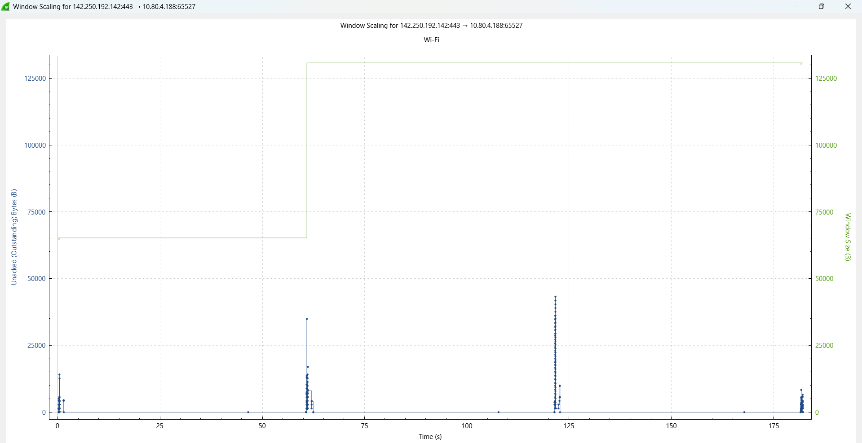
**Step – 8:-**  It is showing the source and destination IP Address:-

**Step – 9:-**  It is showing the TCP related details stored in the packets: like header section src and destination port no flags , checksum , length , timestamps.

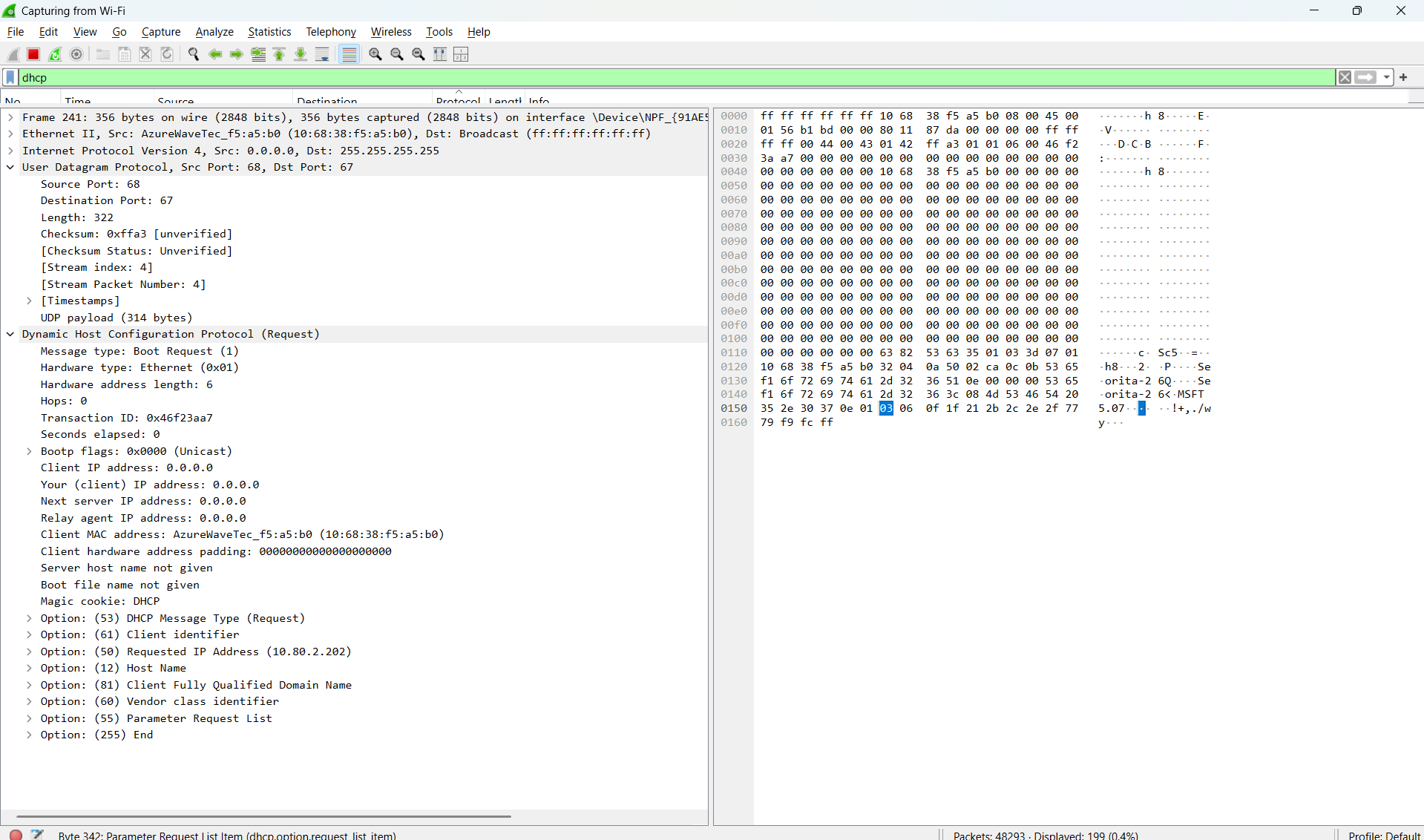
****

* Source Port (65527):
* It is the port number the client (source) uses to send the packet.
* Destination Port (443):
* This is the port number used by the server (destination), which is associated with HTTPS most of the time.
* Sequence Number (2299):
* This is the relative sequence number of the first byte in the data of the segment. It's used for keeping track of the order in which bytes were sent.
* Acknowledgment Number (98531):
* Indicates the next byte of data the sender of this segment expects to receive. It's an acknowledgment of the previous packet.
* TCP Segment Length (0):
* Length of data payload in this TCP segment. In this case, it is 0 which means no data is carried in this packet. It most probably is an acknowledgment.
* Flags (0x010 - ACK):
* Indicates what kind of control information in the packet is. In this case, ACK means it is an acknowledgment.
* Header Length (20 bytes):
* The size of the TCP header. The average minimum size is 20 bytes.
* Ethernet II and IP Information:
* Source MAC Address Intel\_30:99:68: The source MAC address of the device which transmitted the packet.
* Destination MAC Address Cisco\_f8:26:47: The destination MAC address of the device which will receive the packet.
* Source IP 10.80.4.192: The source IP address of the client.
* Destination IP 142.250.192.142: The destination IP address of the server.

**Step – 10:-**  It is showing the TCP related details stored in the packets: like header section src and destination port no flags , checksum , length , timestamps

****

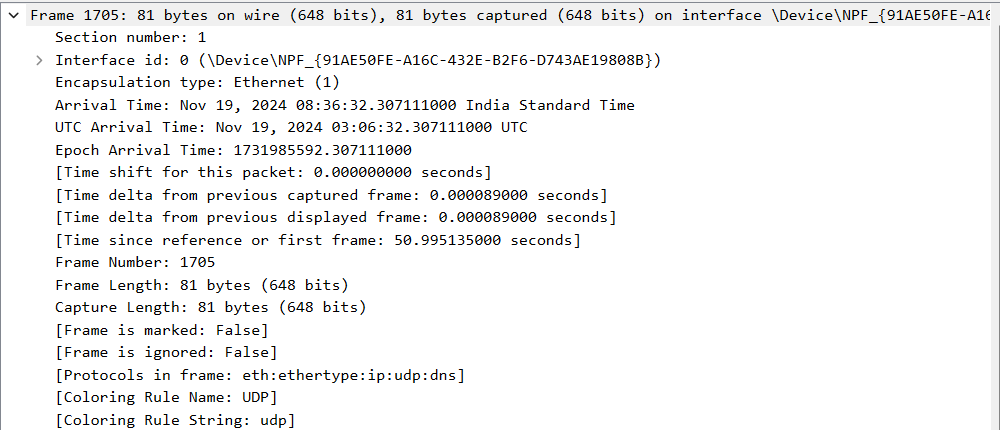
**Step - 11:-**  now we will analyze the UDP Packet.

****

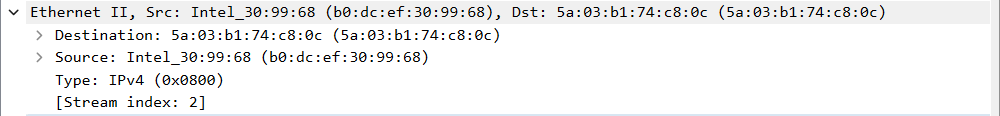
**UDP Packet Details**

1. **Source Port (68):**  
   The port used by the client to send the packet. This is the standard DHCP Client port.
2. **Destination Port (67):**  
   The port used by the server to receive the packet. This is the standard DHCP Server port.
3. **Length (322):**  
   Represents the total size of the UDP packet, including both the header and the payload.
4. **Checksum:**  
   Used to verify the integrity of the UDP packet. In this capture, it is marked as "unverified."
5. **UDP Payload (314 bytes):**  
   The actual data being transported in the UDP segment.

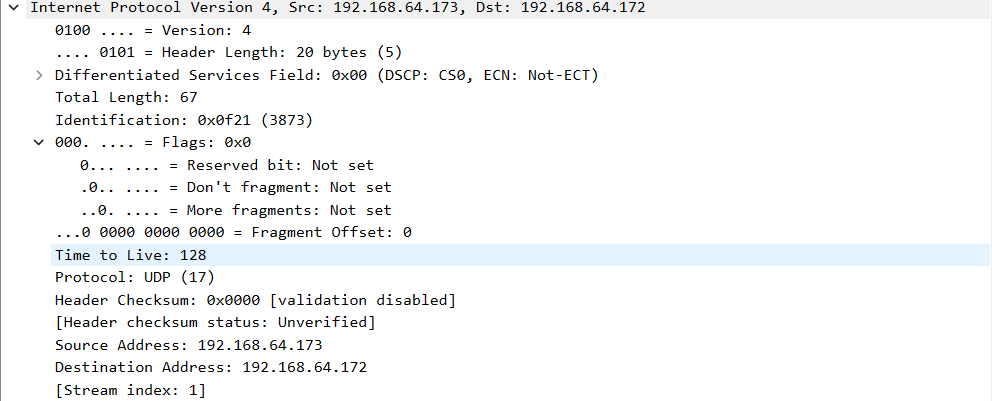
**Step - 12:-**  It us showing the timing related details of UDP Packet.

****

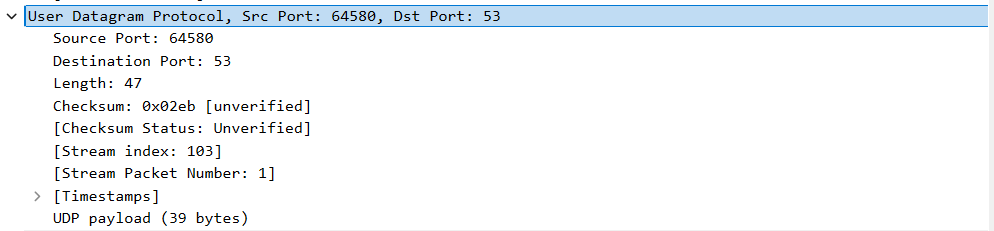
**Step - 13:-**  It is showing the ip related details of UDP Packet.

****

**Step - 14:-**  It is showing the details about the flags of UDP Packet.

****

**Step - 15:-**  It is showing the details about the header of UDP Packet.

****

**Step - 16:-**  Now we will analyze the IP Protocol.

**Definition:-**

* Internet Protocol (IP) is a set of rules that defines the format of data carried over the internet or a local network. It is the primary communication protocol for forwarding packets across network boundaries, which permits internetworking.

**Types of IP:-**

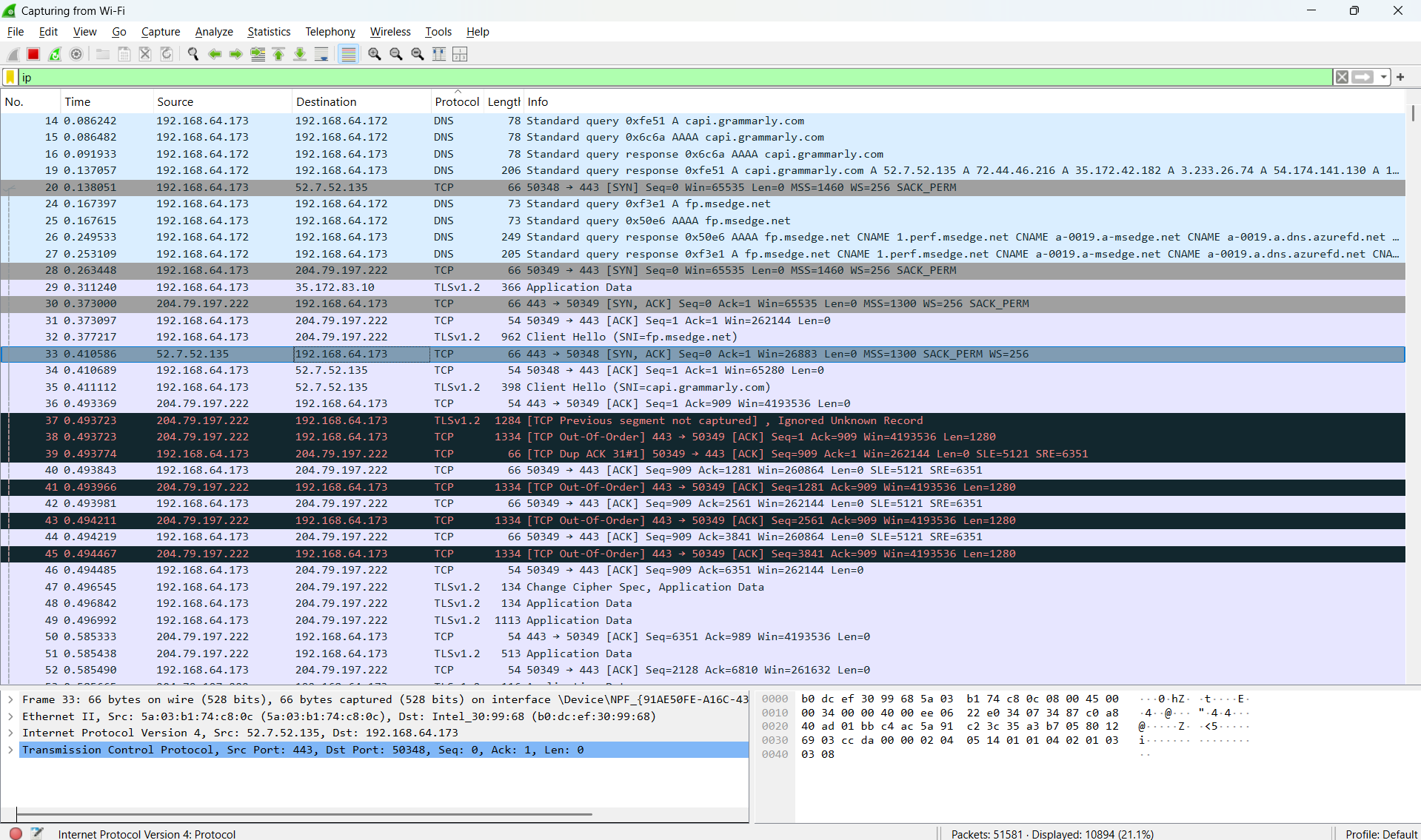
* + IPv4: Uses a 32-bit address format (for example 192.168.1.1). It supports around 4.3 billion unique addresses.
  + IPv6: Uses a 128-bit address format (for example 2001:0db8:85a3::8a2e:0370:7334). It supports a vastly larger address space.

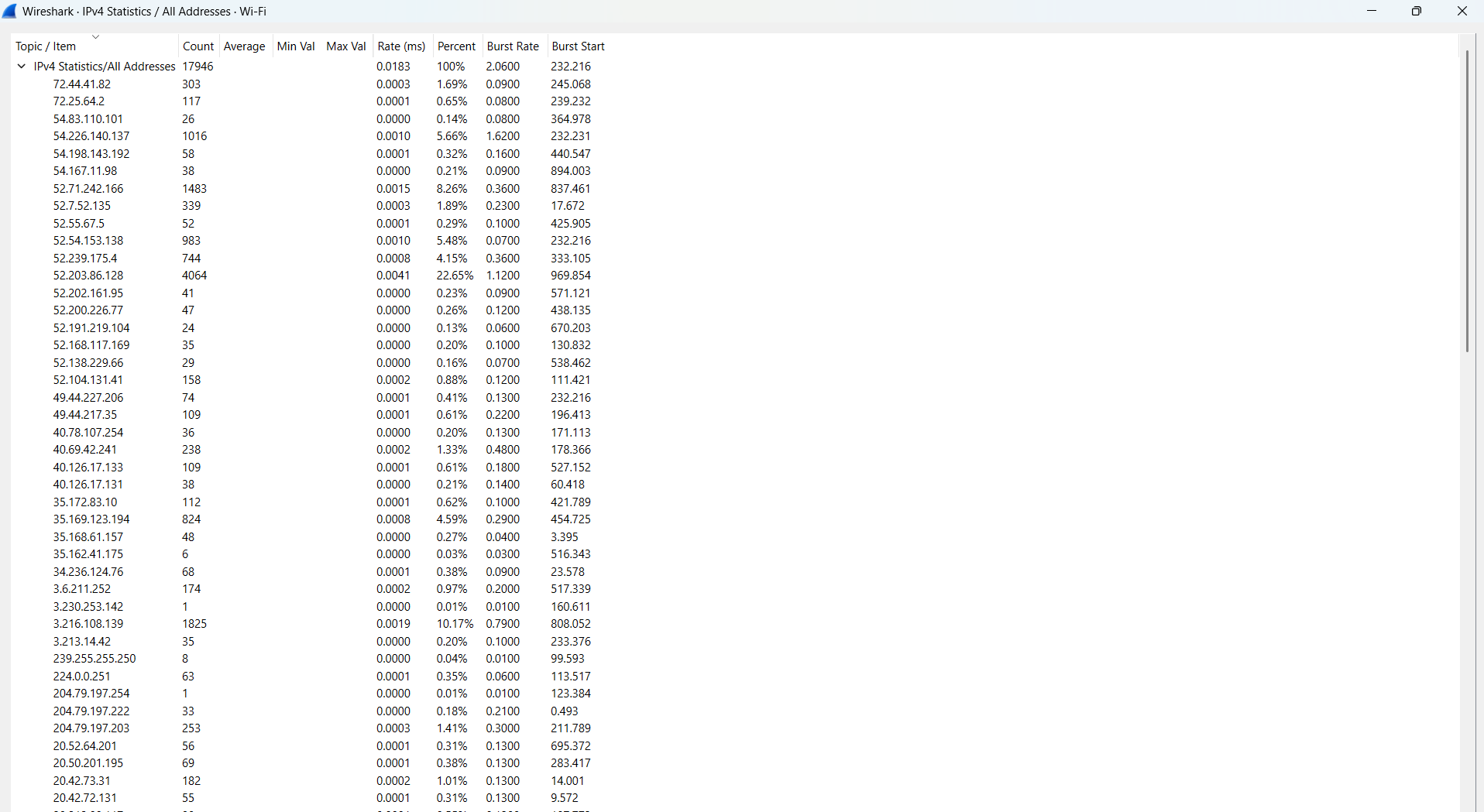
**Applications :-**

* Identifying: Scans a network for its devices.
* Routing: Transfers the data packets between one device and another, but on different networks.

**Protocols Built on IP:-**

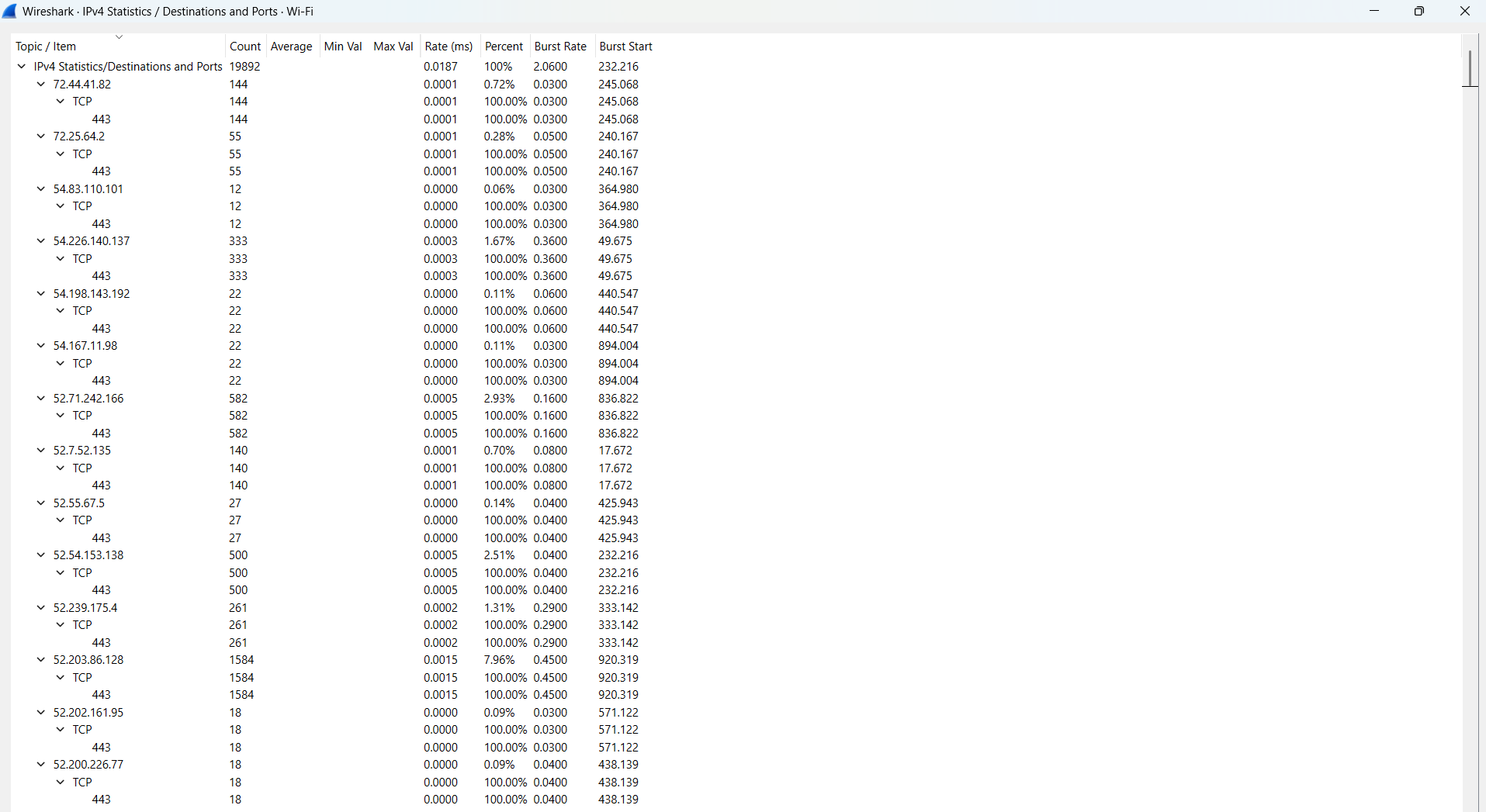
* + **TCP (Transmission Control Protocol):** Reliable, connection-oriented protocol.
  + **UDP (User Datagram Protocol):** Faster, connectionless protocol.

****To analyze the IP search ip in search bar

**Step - 17:-**  Now we go to the Statistics > IPv4 Statistics > all address

It is Showing all IP Address to which my laptop is communication

**Step - 18:-**  Now we go to the Statistics > IPv4 Statistics > Destination and Ports

****

It shows the Destination Adress Protocol and Port No Used for Communication.

**Conclusion:-**

Through this experiment, I learned to analyze TCP packets and what types of details with the data is sent. And the importance of all flags. How ACK is important. and show the actual packet what is sent and what is received. I learned to analyze the UDP packets ,its hearder and flags we learned the theory about the protocol by performing this experiment I learned to live monitor the packets and learned how

IP address is used in various Protocol like TCP and UDP.