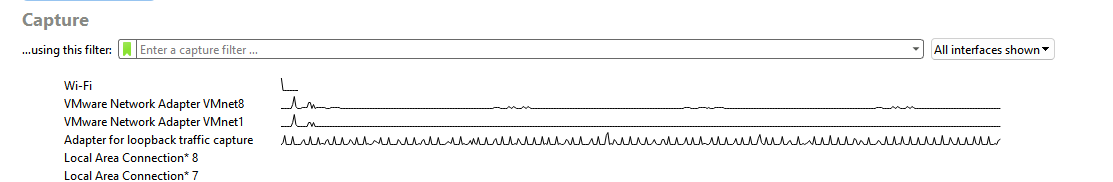
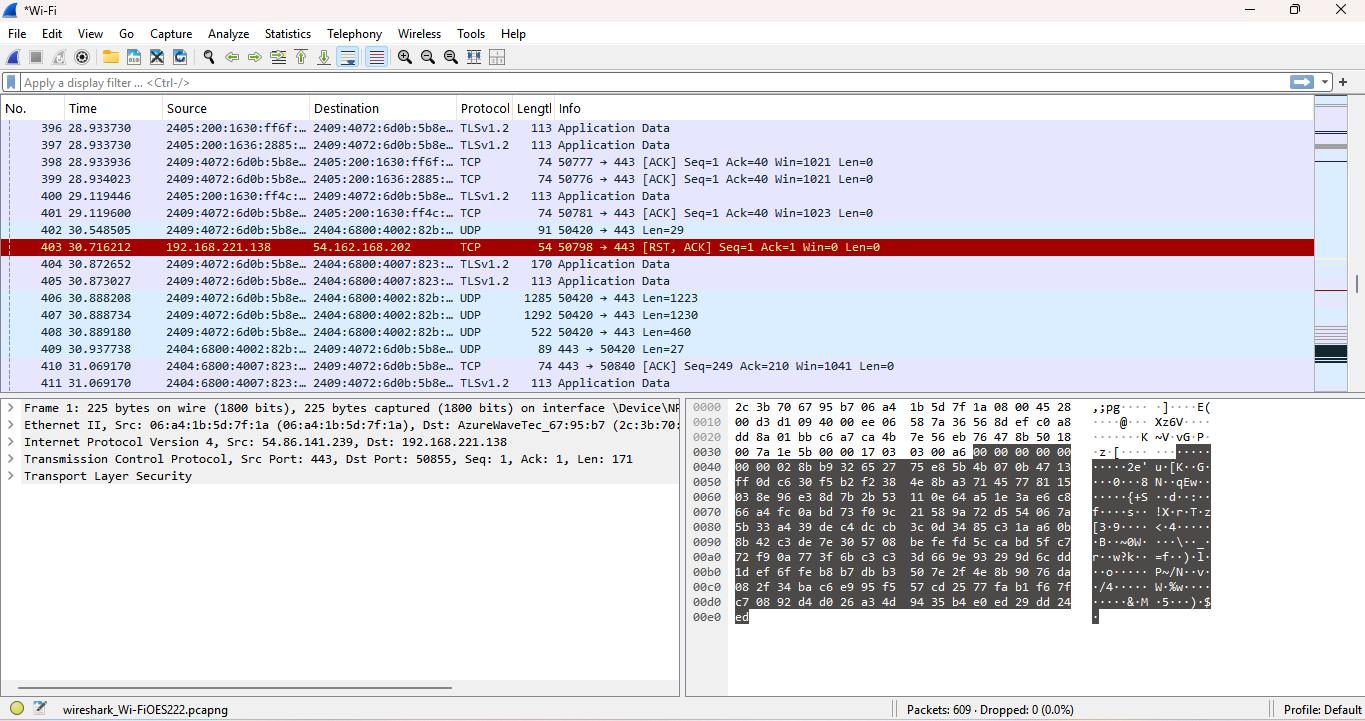
WIRESHARK Tutorials Hands On!



This indicates which Network Interface Cards (NICs) are picking traffic.

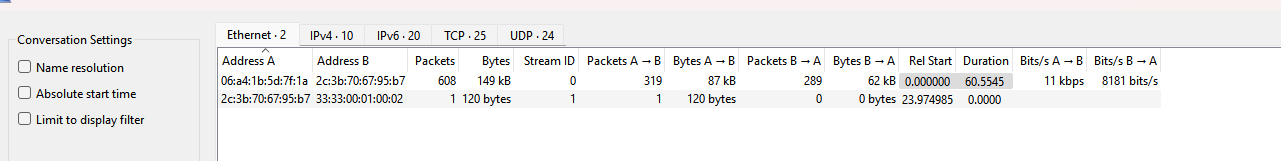
While double clicking the Wi Fi it automatically captures packets:



At bottom you will get to know that “609” (No of packets) are captured.

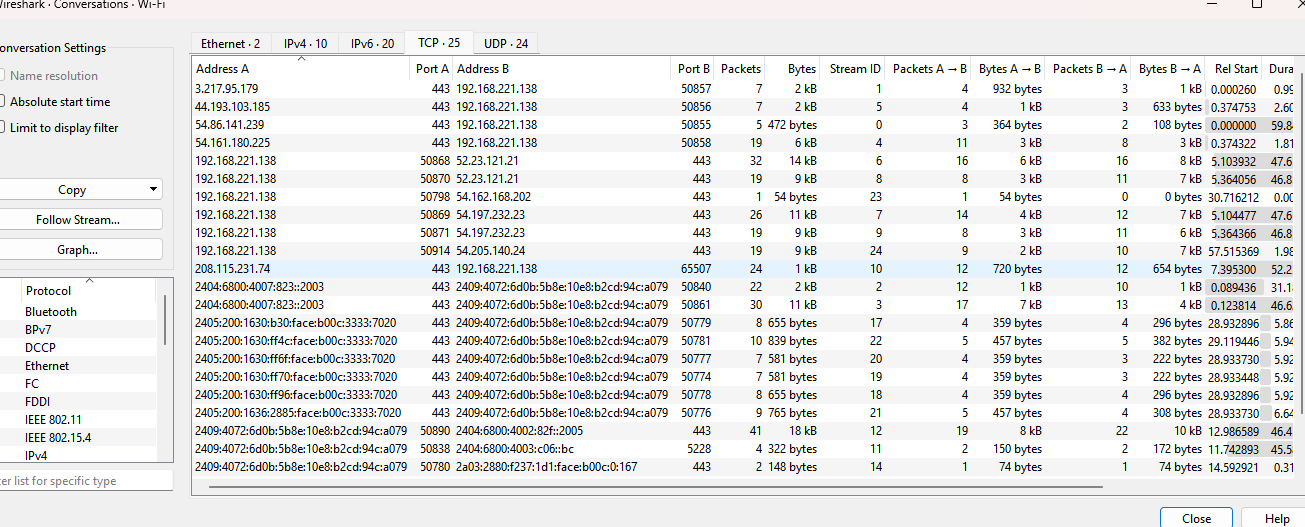
PACKET CAPTURE (PCAP):

Click STATISTICS on top and click conversation,



You can see all of the Conversation that part of PCAP that are captured.

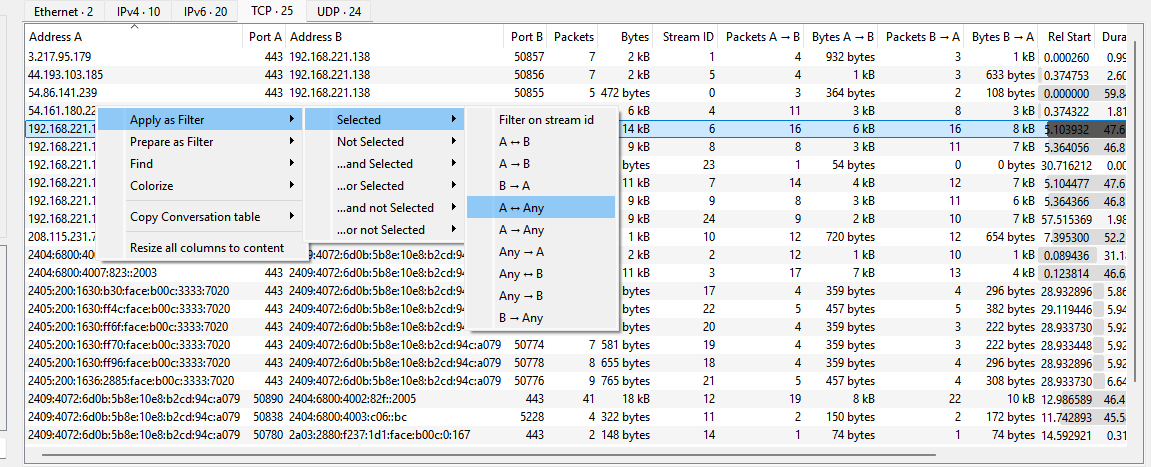
Click TCP on top to capture specific TCP packets:

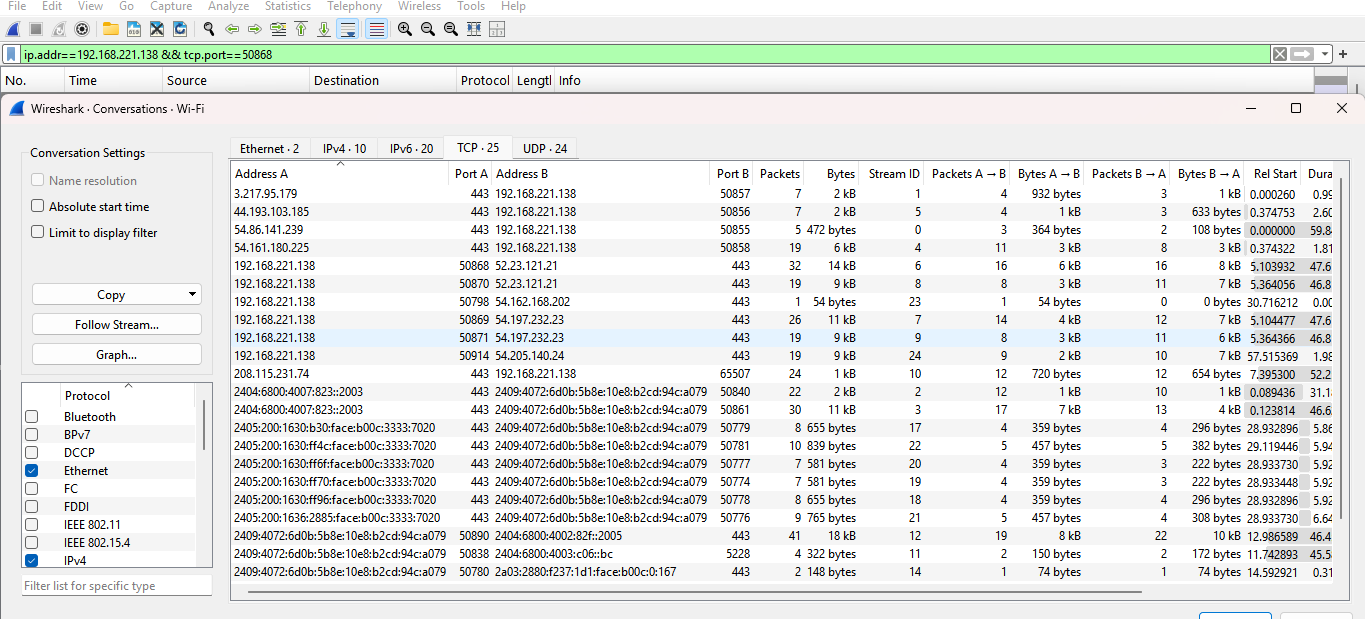


Can observe how many packets were sent and how many bits, duration of conversation and more information.

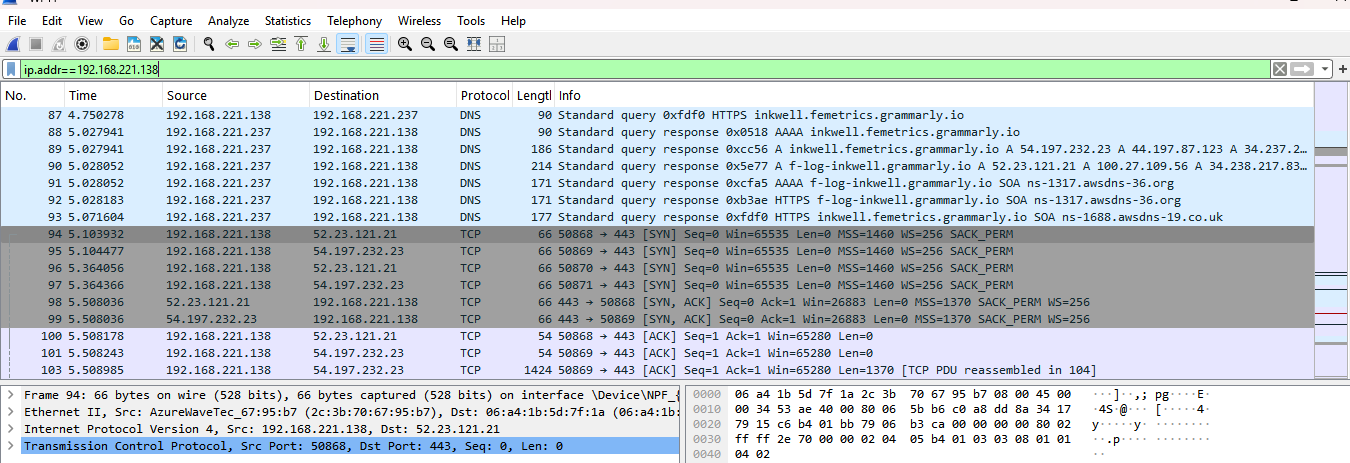
PACKETS FILTERING:

Right click your own IP 🡪 apply as filter 🡪 selected 🡪 select any as per your requirements





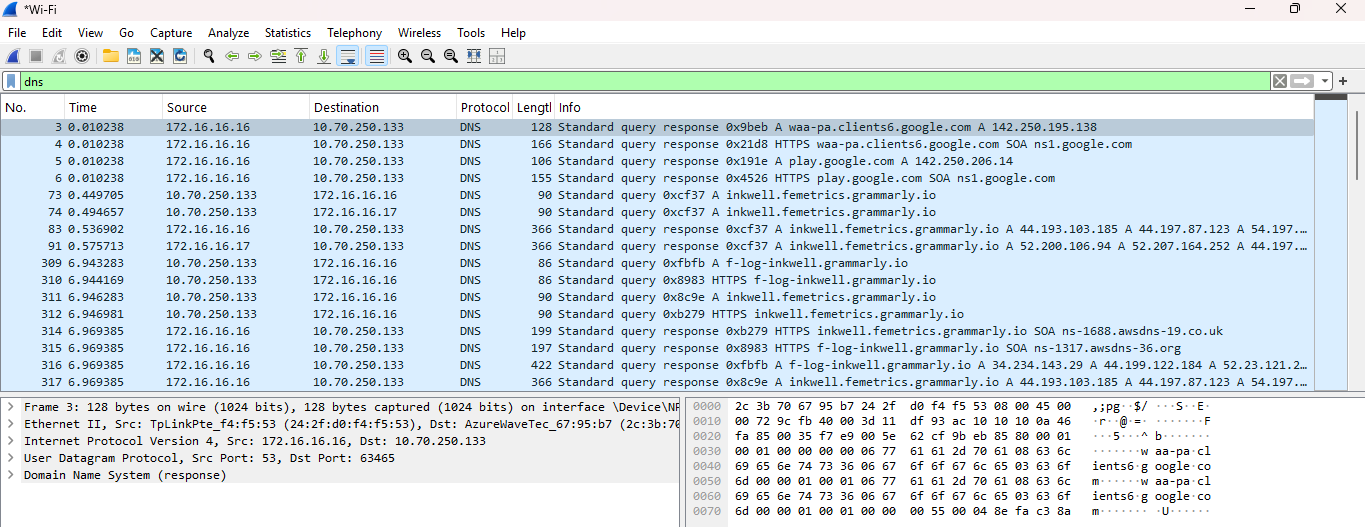
You will notice that a filter is automatically put up on “top bar” because we have the ports in here, the filter included the port. If you don’t want port , you can remove that particular part



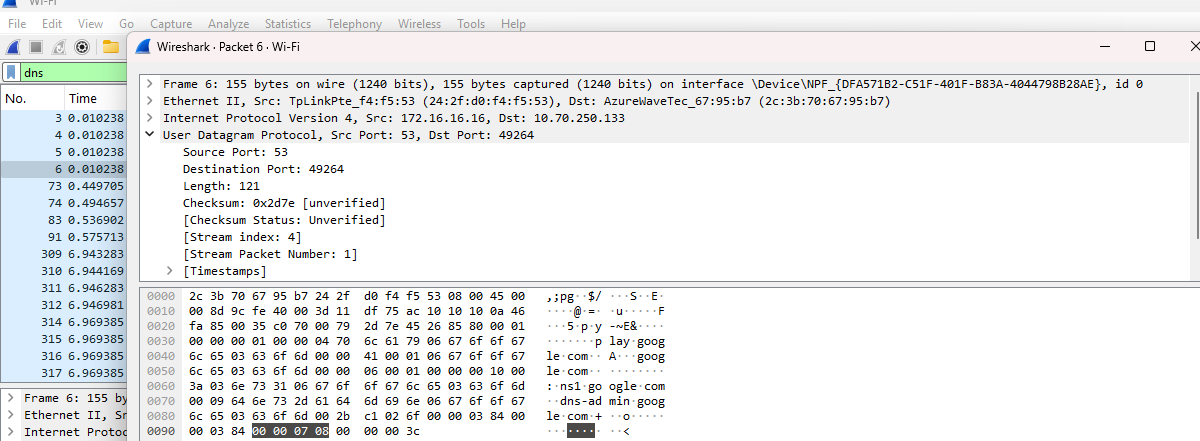
Can analyze any packets were sent from this IP.

**DAY 2:**

DNS Packet filtering:



DNS checking:

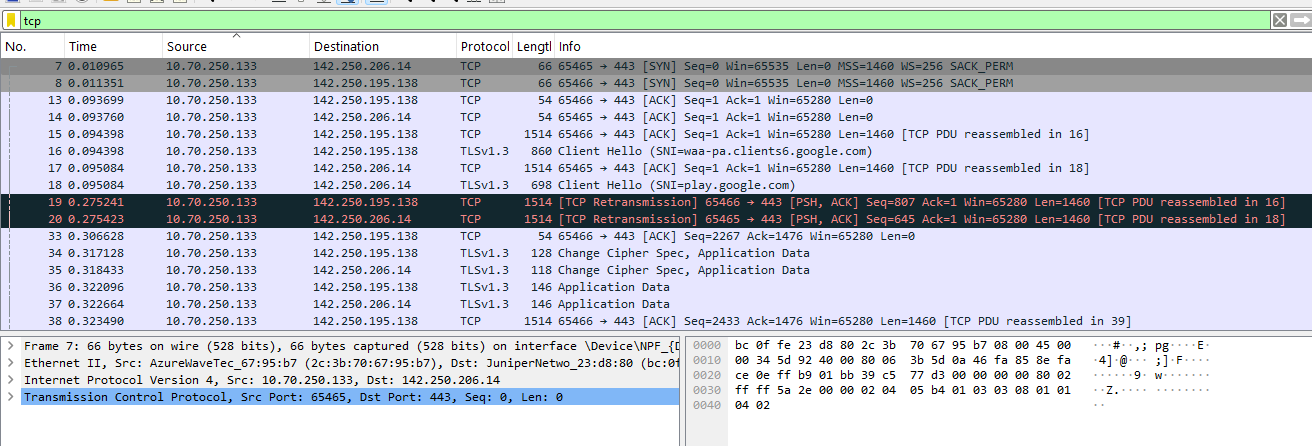


How many DNS quries has been sent from my PC? (apply dns.count.queries filter)

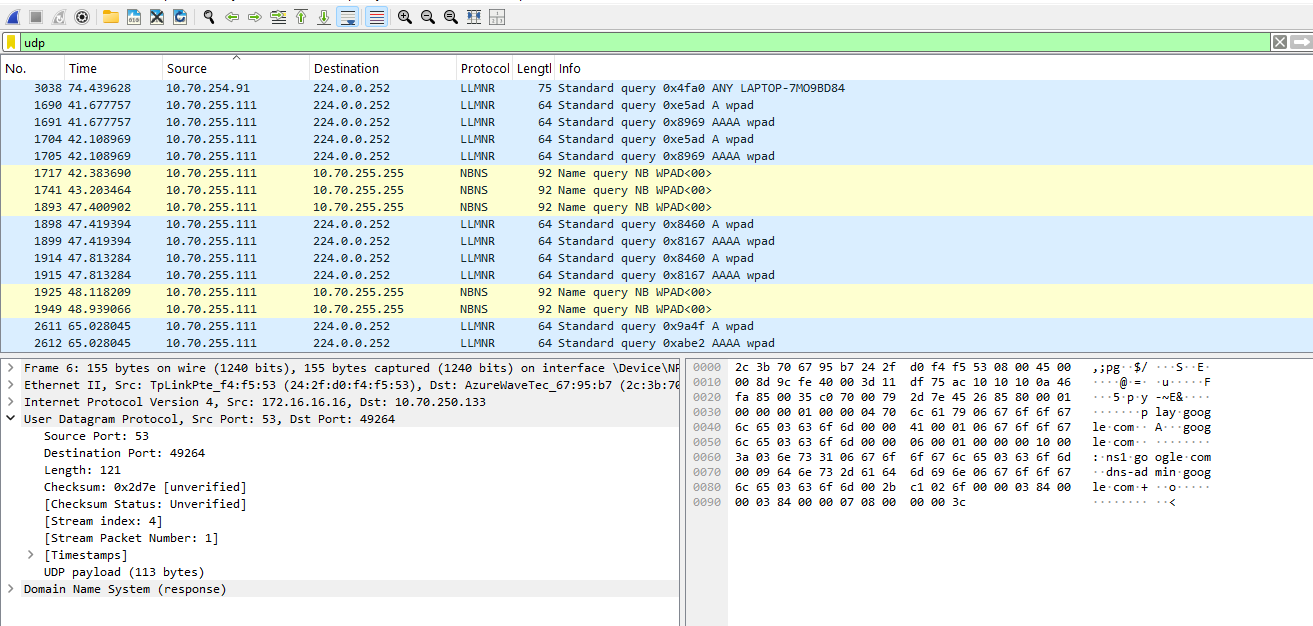


If I want to filter the query which has been sent to google.com ? (dns.qry.name == “google.com” ) use this filter.

If u want to analyse TCP traffic then use TCP filter:

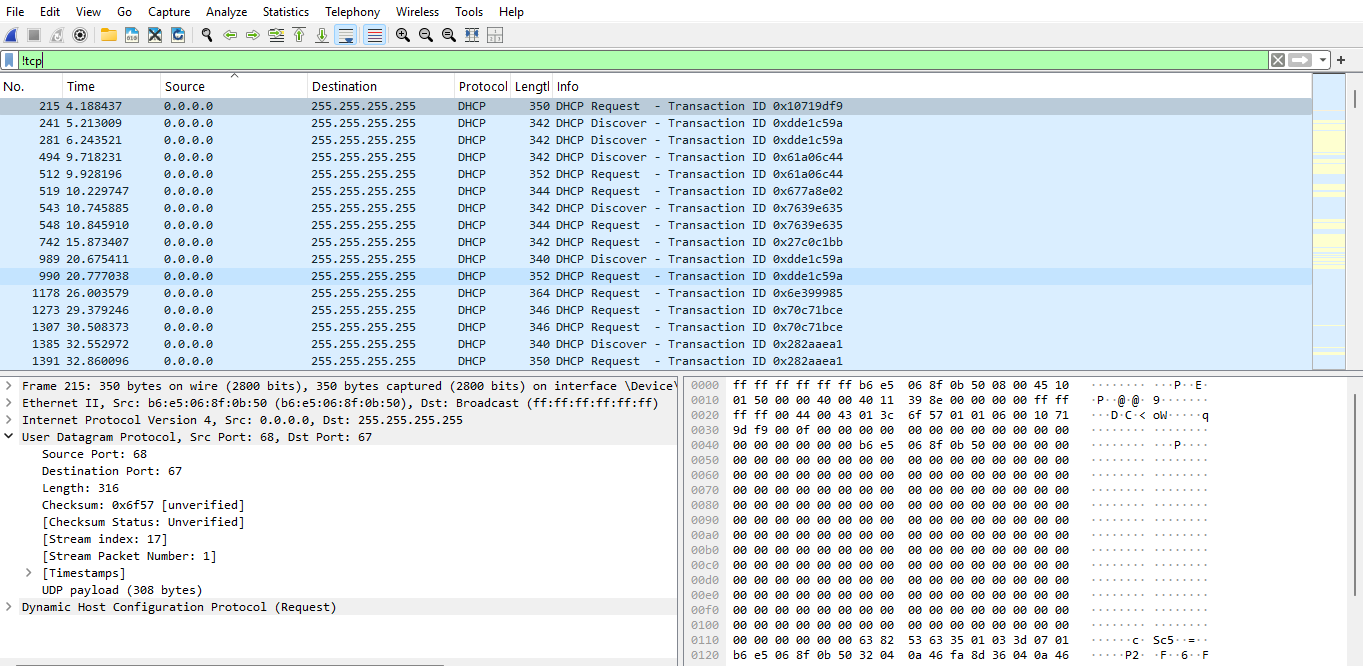


To filter UDP packets:

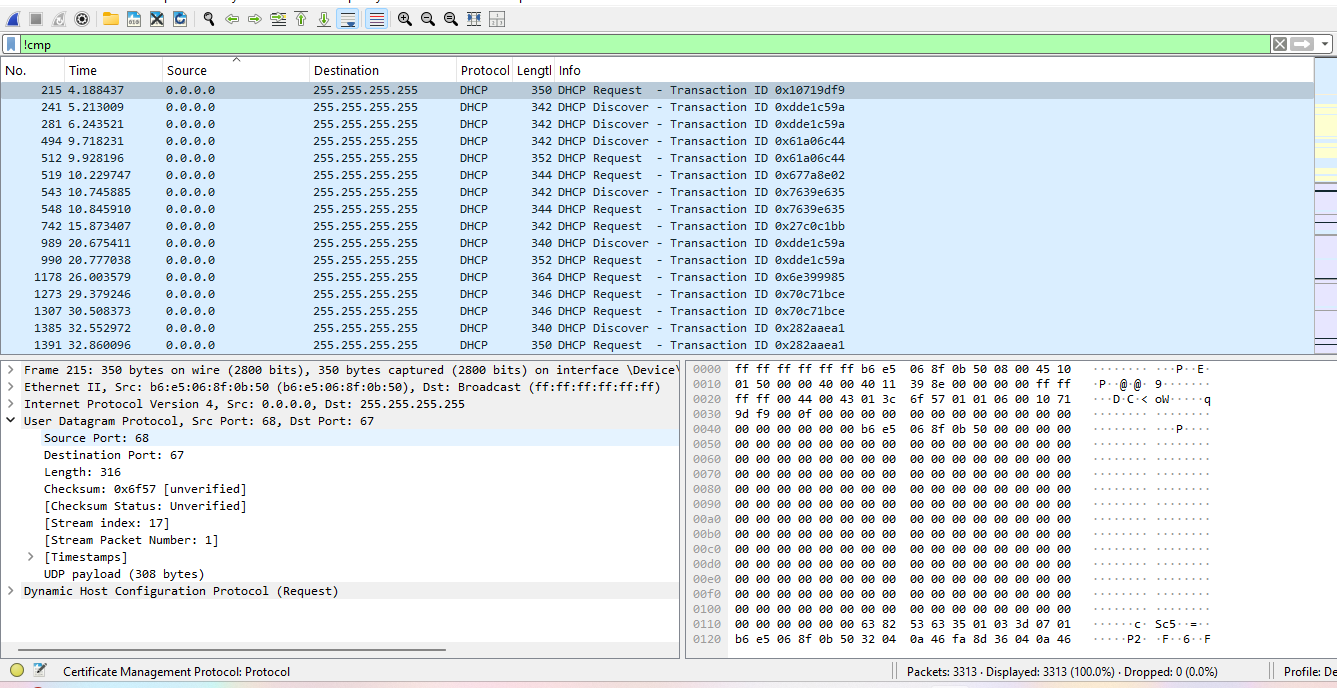


🡪To filer ICMP use filter icmp.

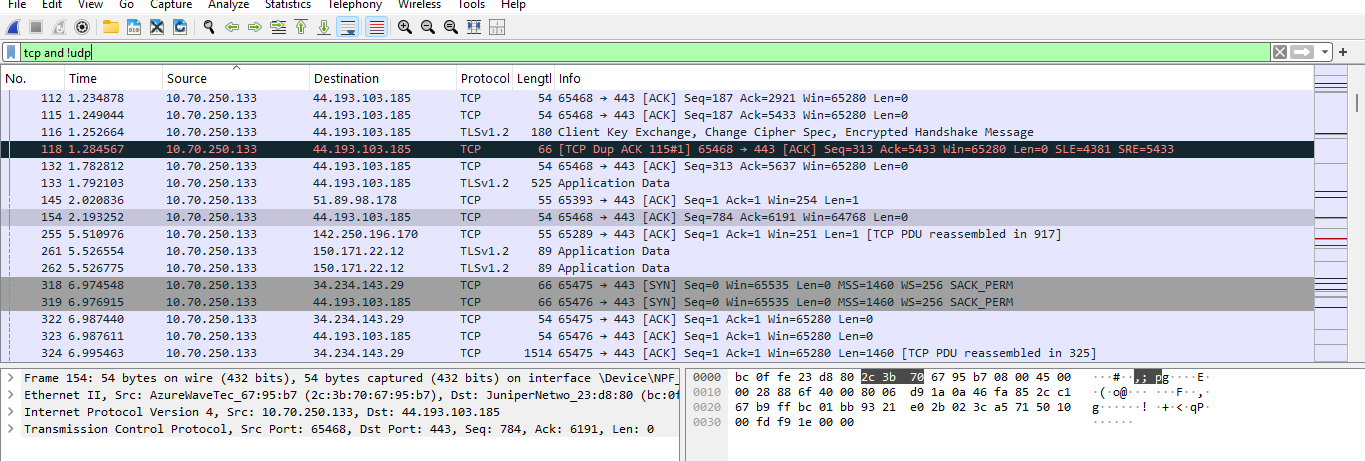
🡪 filtering all the packets except TCP: use !tcp filter.



* Filters all the packets except ICMP use filter !icmp.



* Filter all TCP and other packets and not UDP: use tcp and !udp filter

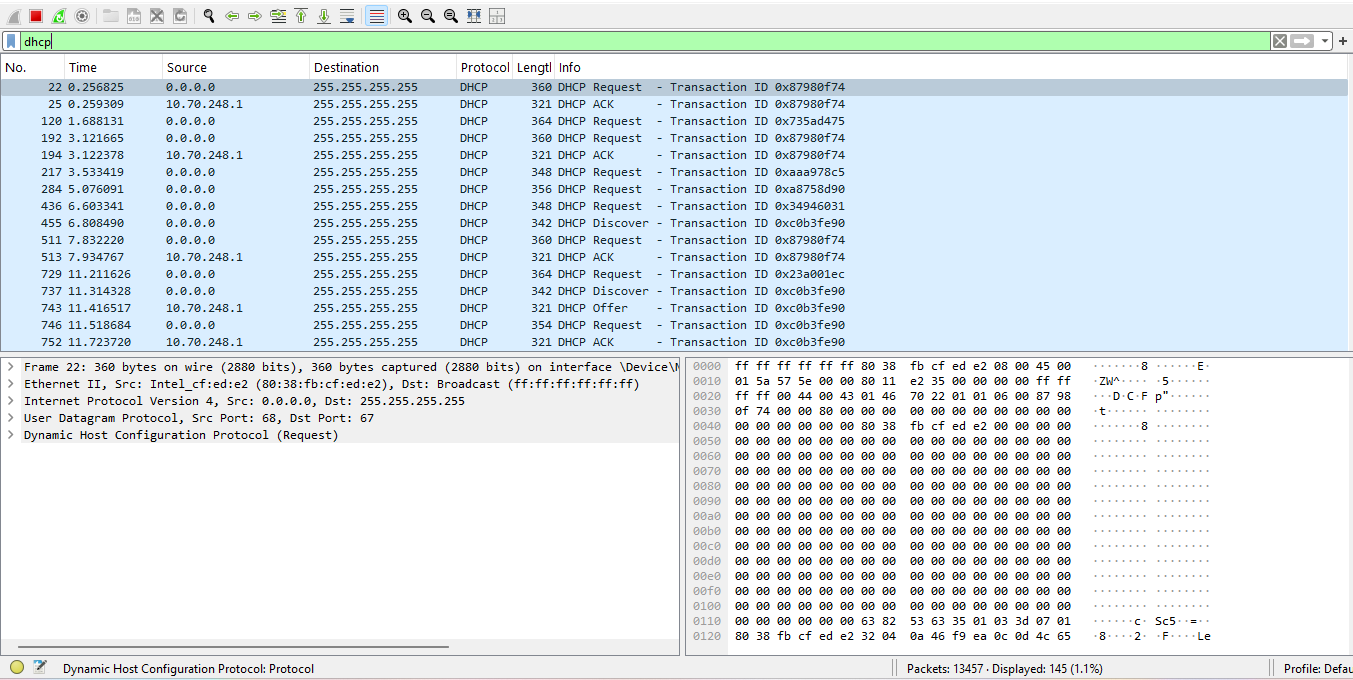


DHCP PACKET ANALYSING:

Working of DHCP is;

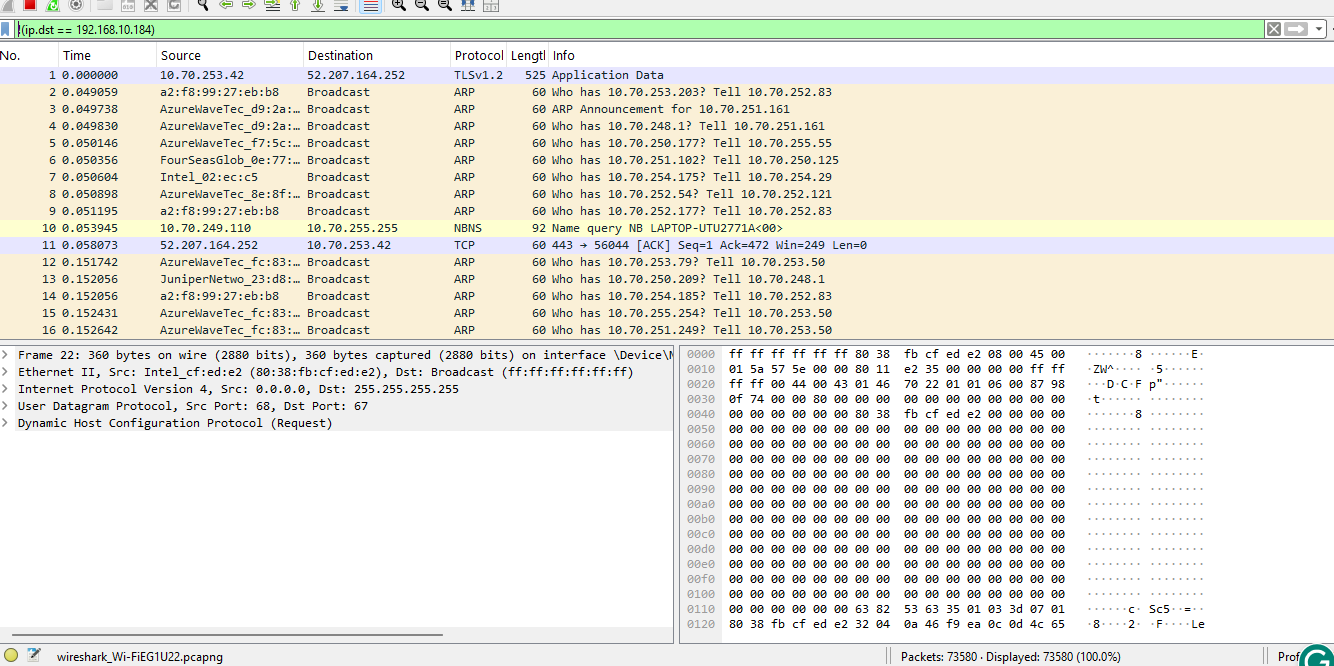
**DHCP Process in OSI Model:**

1. **DHCP Discover** (Layer 2 & 3) → Client broadcasts to find a DHCP server.
2. **DHCP Offer** (Layer 2 & 3) → Server responds with an available IP.
3. **DHCP Request** (Layer 2 & 3) → Client requests the offered IP.
4. **DHCP Acknowledgment (ACK)** (Layer 2 & 3) → Server confirms and assigns theIP



If you don’t want a particular IP use, [!(ip.dst == 192.168.10.184)] filter

You will not see any Info about this IP

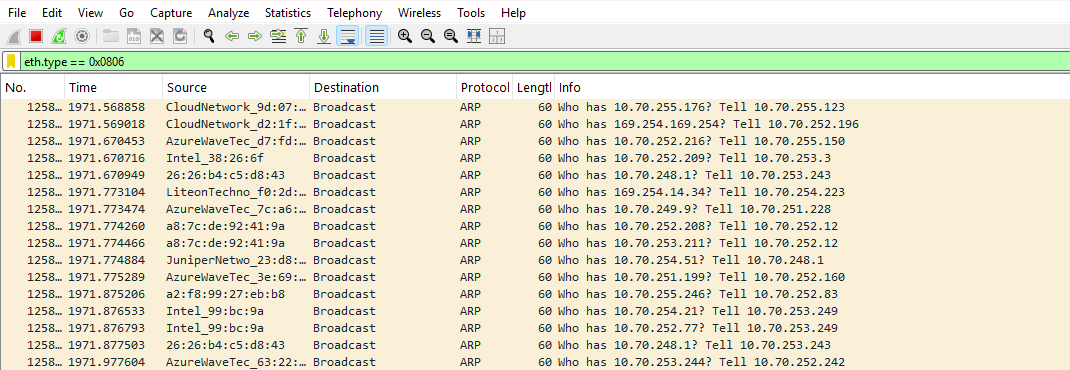


What is Ether type? What is the use of Ether type? (interview question)

* Ether type will define what is the next packet, whether it is an IP packet / ARP packet or it is an DNS packet.

Filter to find **Ethertype** is [!(eth.type == 0\*0800)]

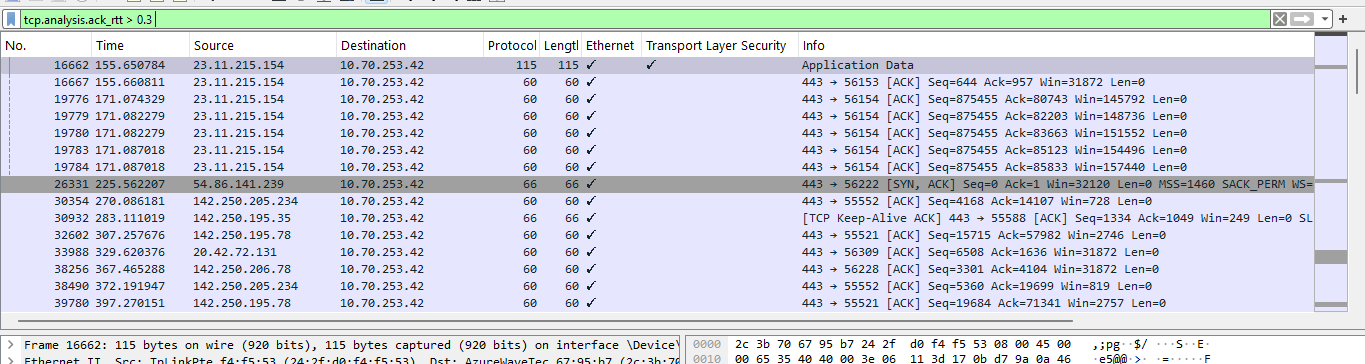
If you want to find only the IP packet ether type, use [ eth.type == 0\*0800 ]



TROUBLESHOOTING: (NETWORK SLOWNESS)

Check High Latency (Slow Response Times)

Use [tcp.analysis.ack\_rtt > 0.3] filter



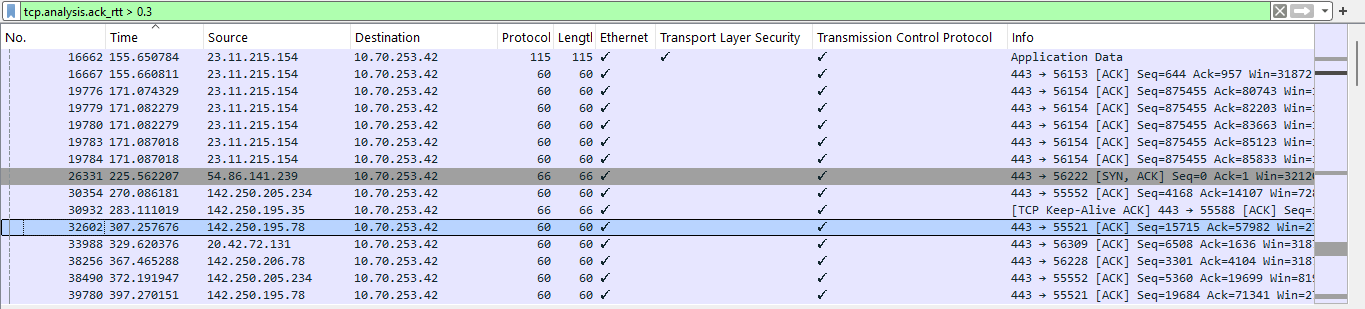
This filter is used to **identify packets with high Round-Trip Time (RTT)**, which can indicate **network slowness issues**.

**High RTT Packets (Potential Delay)**

* **What it means**: These packets took longer than **300ms** to receive an acknowledgment (ACK).
* **Impact**: High RTT means **slow responses**, possibly due to **network congestion, packet loss, or a slow server**.

**Example from your capture:**

* **Packet No. 16662** has an RTT issue, suggesting possible network latency.
* If most packets have **RTT > 300ms**, the network is experiencing **latency issues**.



2. Check Packet Loss (Retransmissions & Duplicates)

Use [tcp.analysis.retransmission] filter

