Mohan Kumar

Wireshark Filters

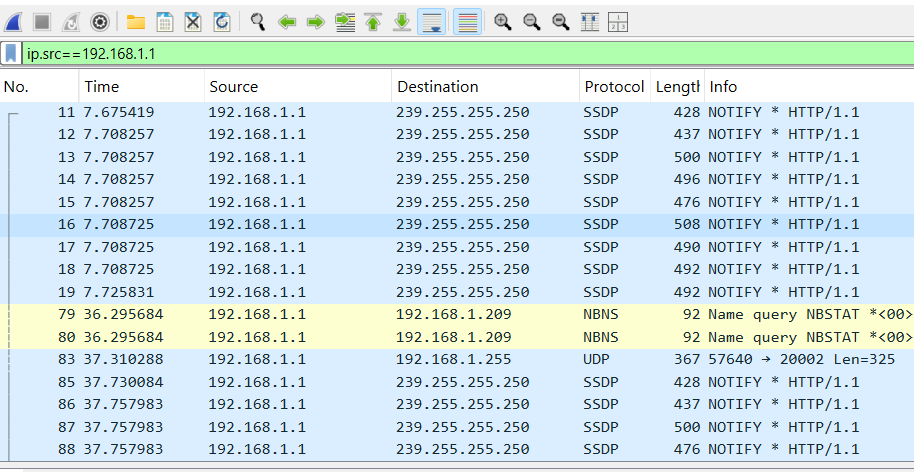
Top 10



1. **Source IP:**

Filter the traffic by the Source IP and shows the traffic from the source IP that we have

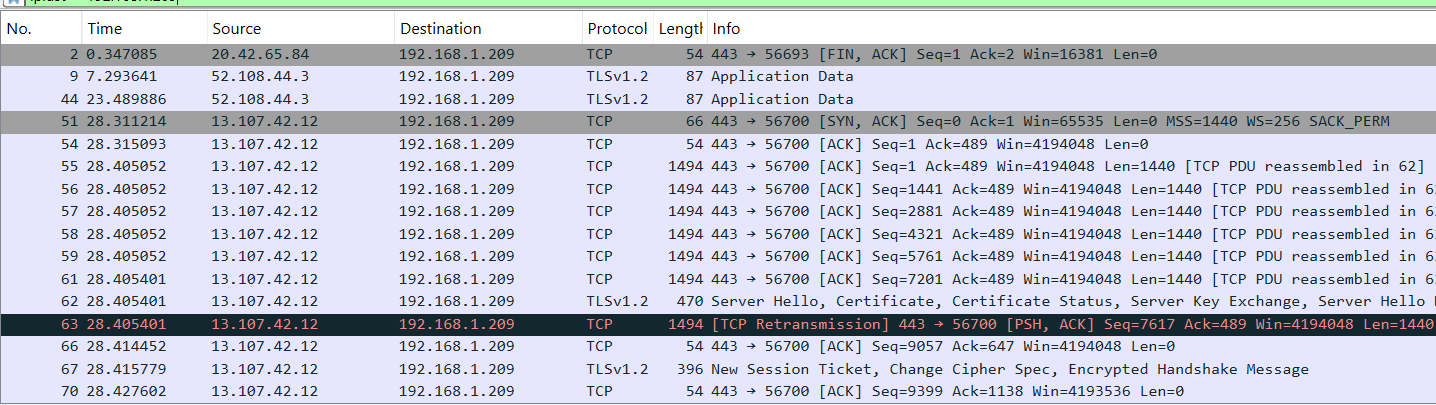
**Ip.src==192.168.1.1**



1. **Destination IP:**

Filter the traffic by destination IP only. It will display the traffic reached to the destination IP

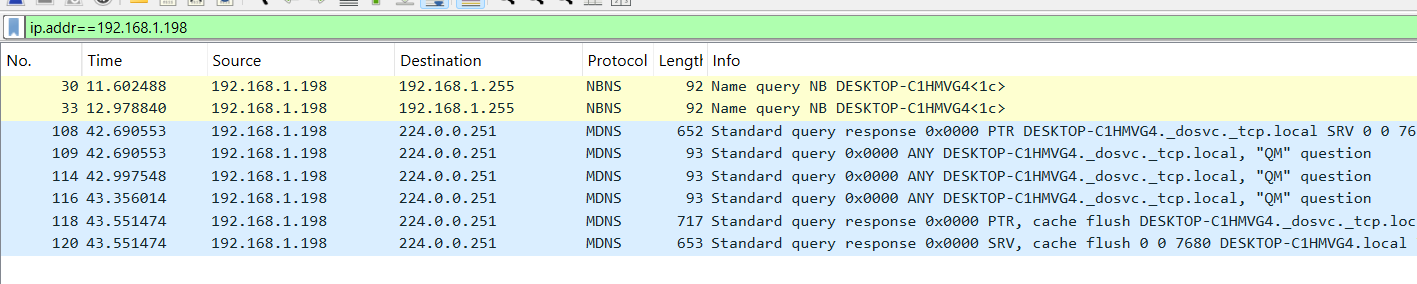
**Ip.dst==192.168.1.209**



1. **IP address:**

Filter the traffic by specific IP address. It will display the whole communication of the specific IP

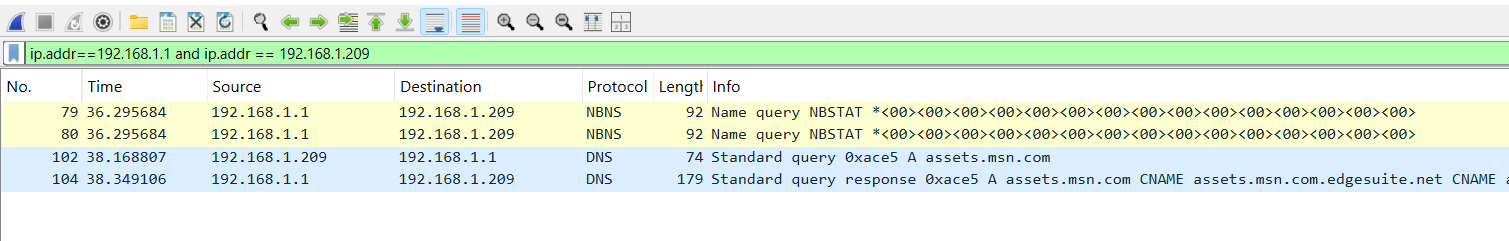
**Ip.addr==192.168.1.198**

****

1. **Between two hosts:**

Filter the traffic generated as a conversation between two hosts

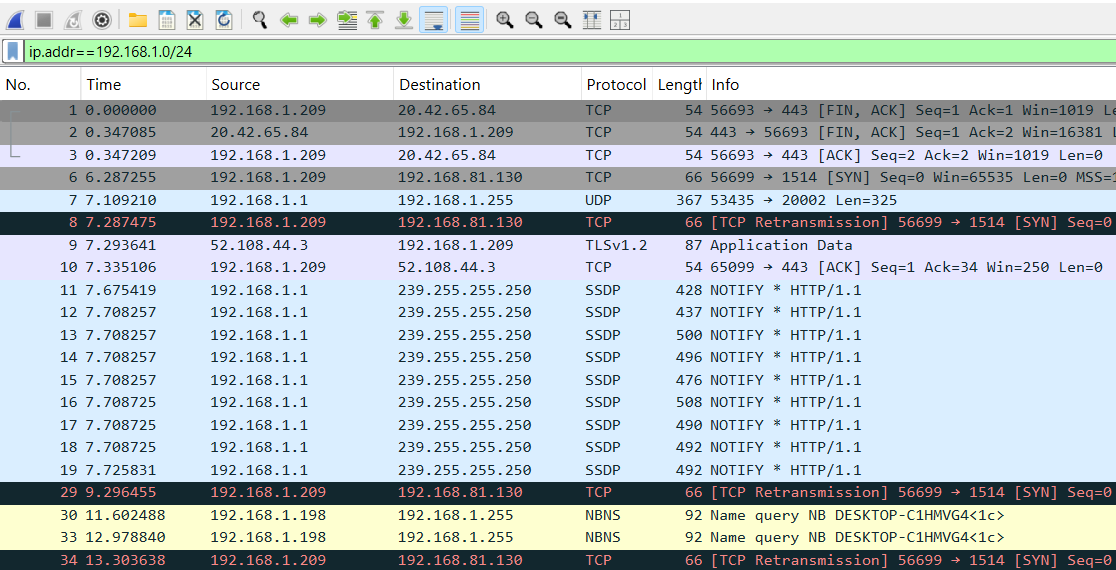
**ip.addr==192.168.1.1 and ip.addr == 192.168.1.209**



1. **By subnet:**

Filter the traffic by whole traffic in a specific subnet. We can divide traffic by specific subnet

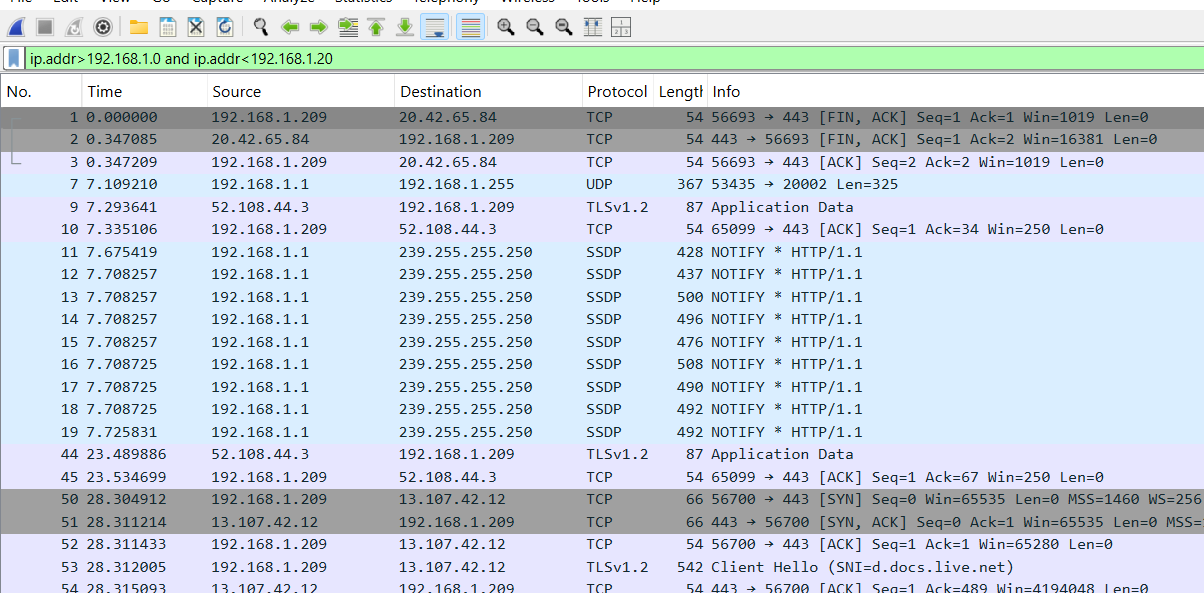
**Ip.addr==192.168.1.0/24**

****

1. **Filter by range of IP**

Filter the traffic by range of IPs by maximum and minimum IPs.

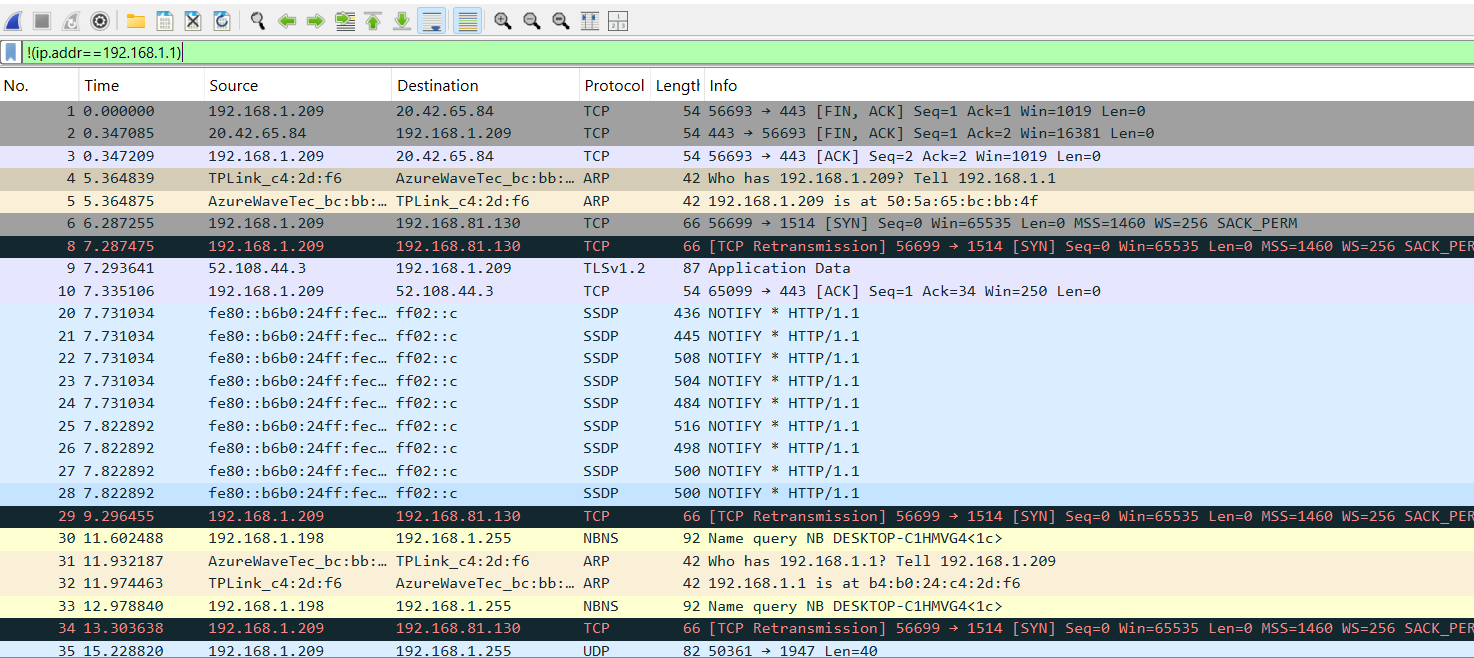
**Ip.addr>192.168.1.0 and ip.addr<192.168.1.20**



1. **Filtering out a Host or a subnet:**

We can filter the traffic with entering “**!**” Symbol it indicates **Boolean not** sign

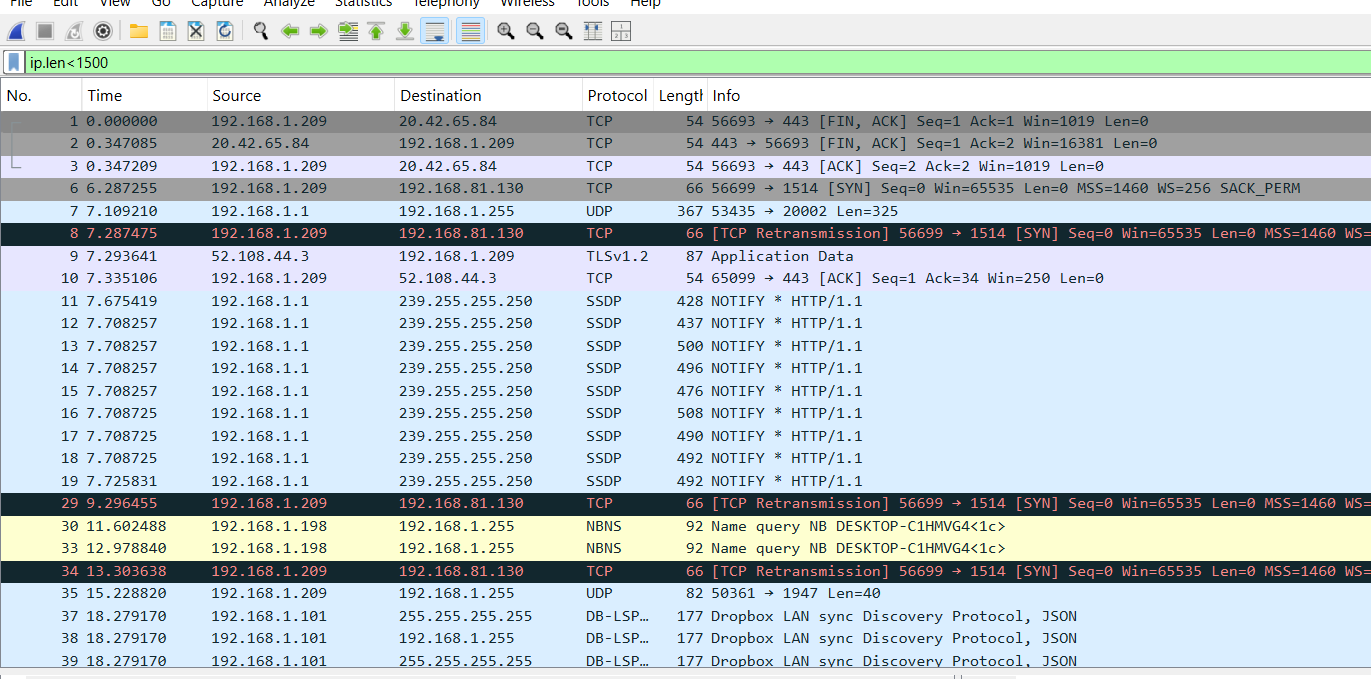
**!(Ip.addr==192.168.1.1)**

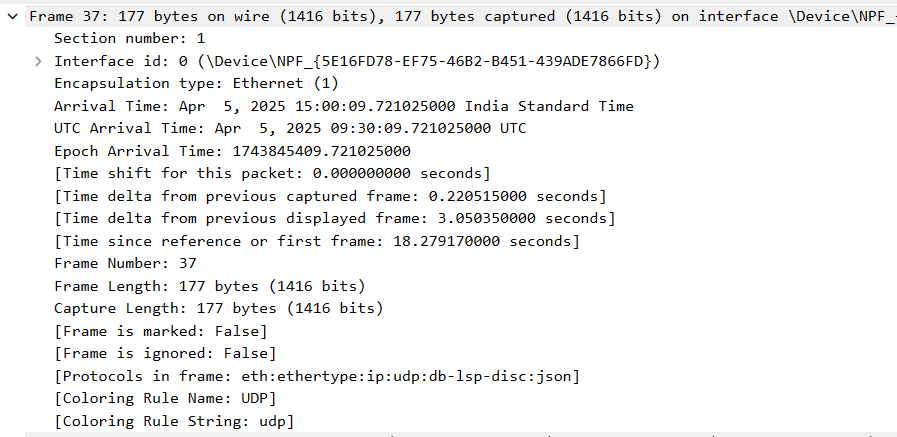


1. **Filter packets less than or greater than a specific size**

It will filter the packets by the length By default the packet length is 1500

**Ip.len<1500**

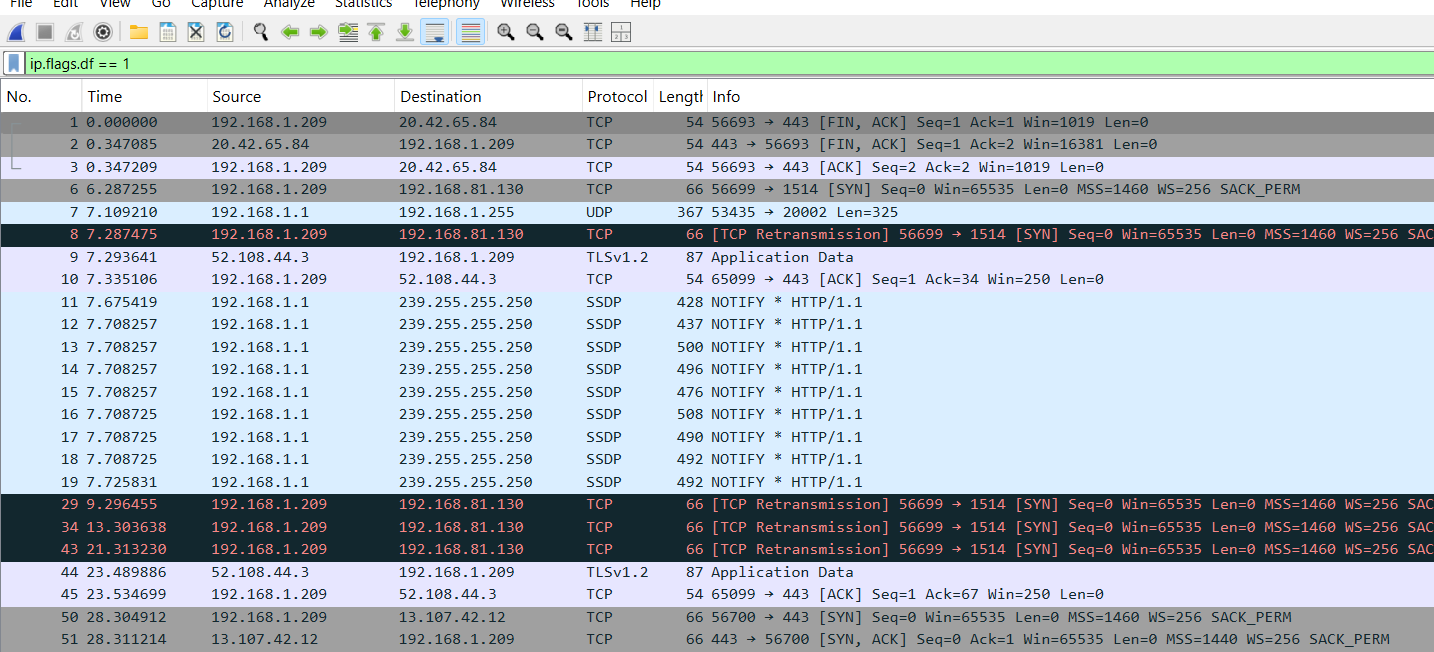


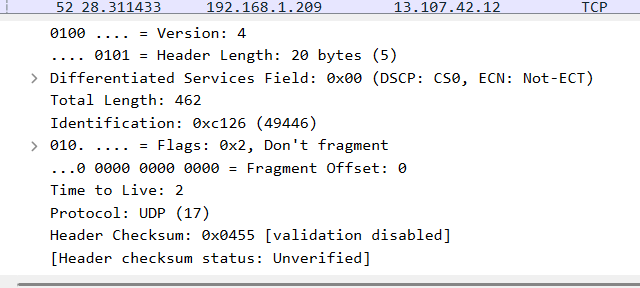


1. **Packets should not be fragmented**

Some applications do not want their packets to be fragmented in the network. When the devices on the path (routers, firewalls, switches, etc.) receive these packets, they check if they are larger than the MTU size, if so, the devices drop these packets, which causes failures. Following filter can be used.

**ip.flags.df == 1**

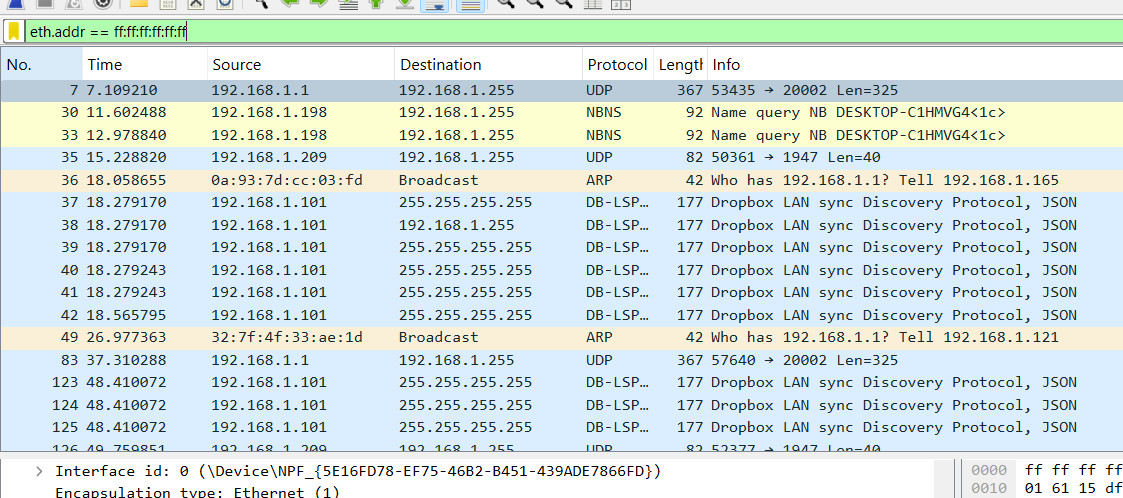
****

****

1. **Broadcast packets:**

Filter the packets which are broadcast in the network

**eth.addr == ff:ff:ff:ff:ff:ff**

****