Computer Network (Lab session -11)

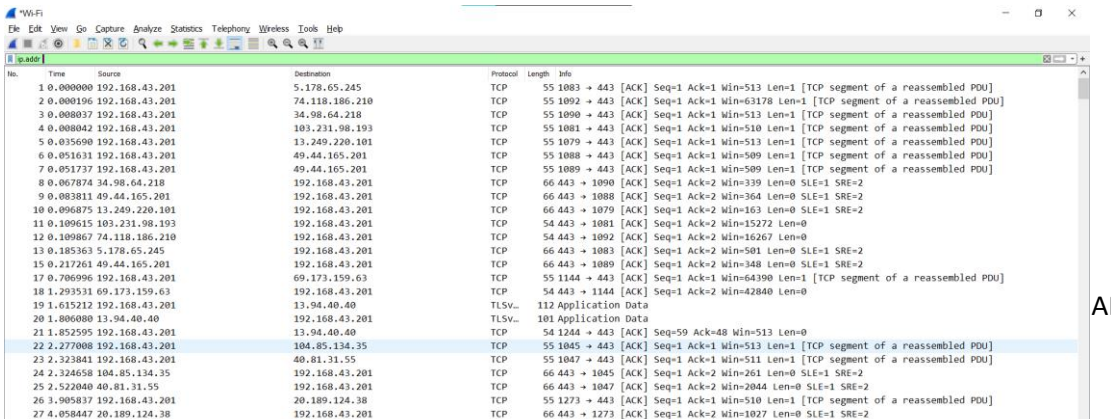
Wireshark with IP & ICMP protocol

Q-1) Wireshark Software

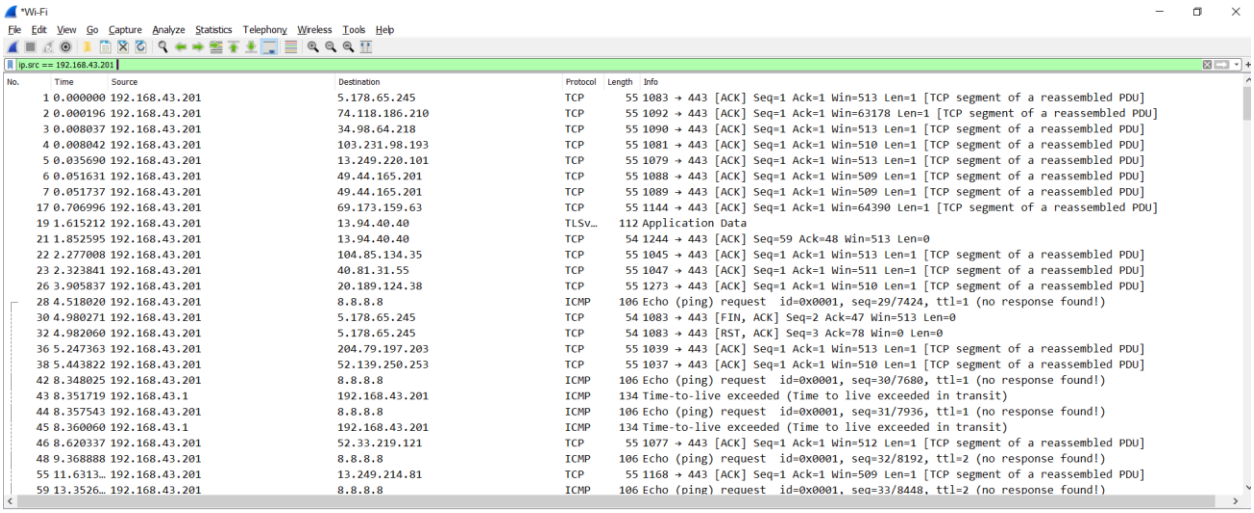
A -> Capture analyze IP protocol message being exchanged.

B -> Capture analyze ICMP message being exchanged.

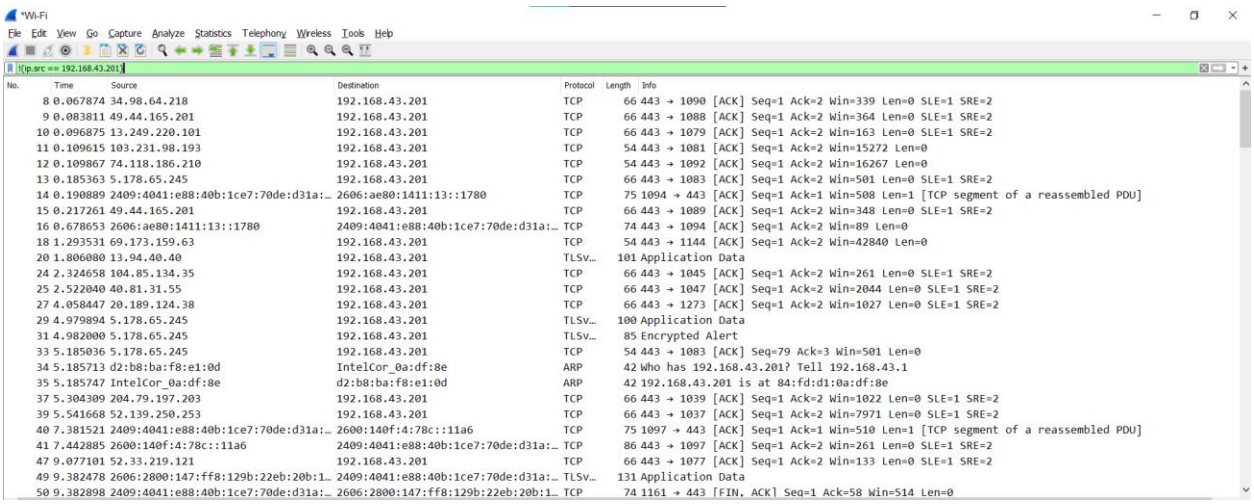
- Wireshark is the world's foremost and widely-used network protocol analyzer. We also perform practical on TCP, UDP protocol, DNS services and HTTP response.
- Now working with IP protocol, that give us the full information about IP address. Like Source address, destination address and IPV6 address.
- IPv4 is a **32-bit address** in which each group represents 8 bits ranging from 0 to 255.
- IPv6 is a 128-bit address. Ip.addr gives the all the address where no condition.



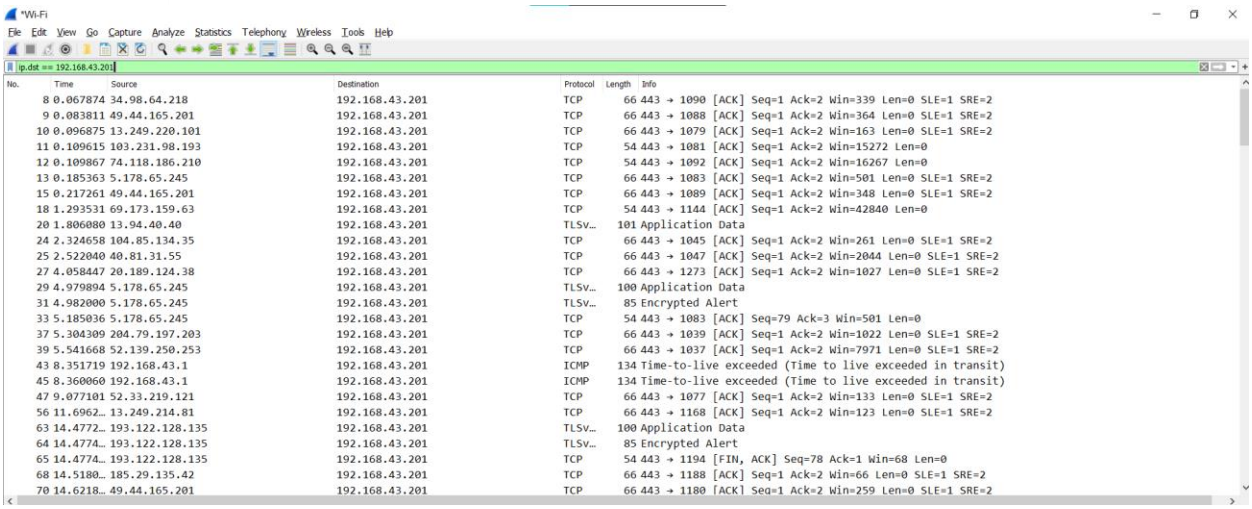
- Ip.src == 192.168.43.201 gives the source IP address where source is only on 192.168.43.201



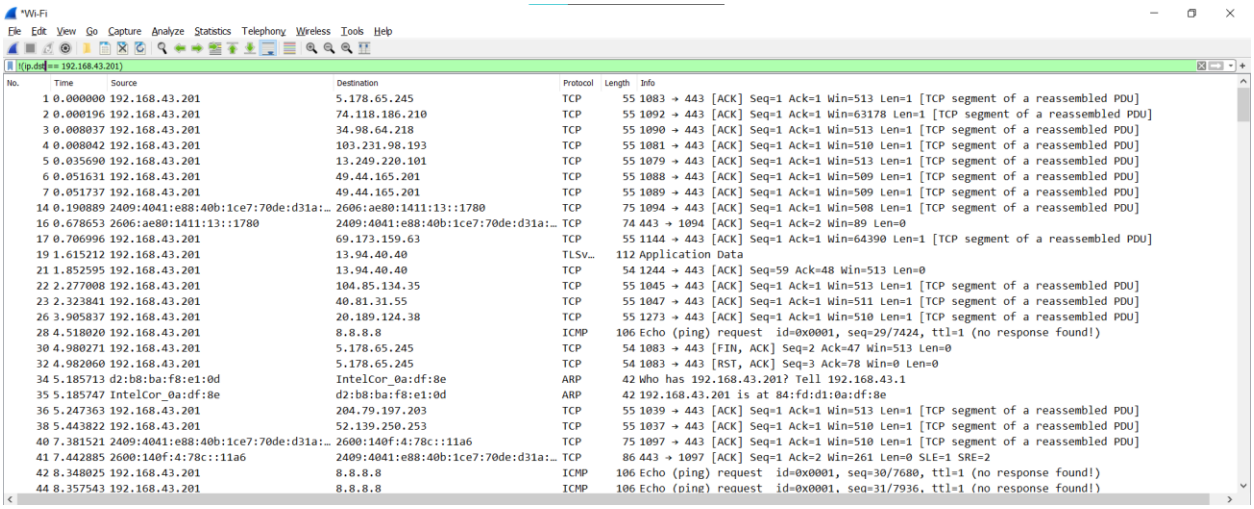
- ! (Ip.src == 192.168.43.201) gives the source IP address where source is not 192.168.43.201



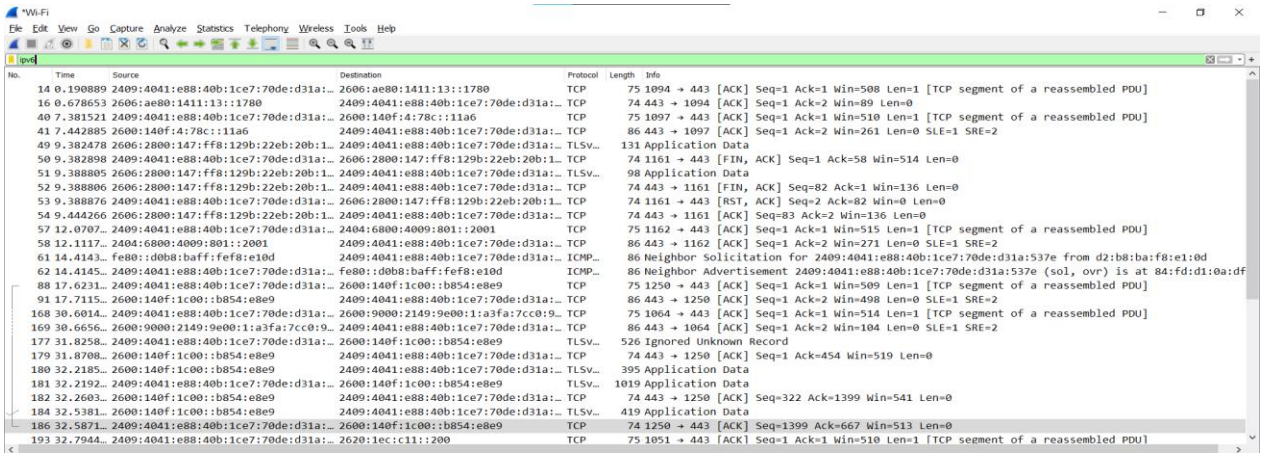
- Ip.dst == 192.168.43.201 gives the destination IP address where destination is only on 192.168.43.201



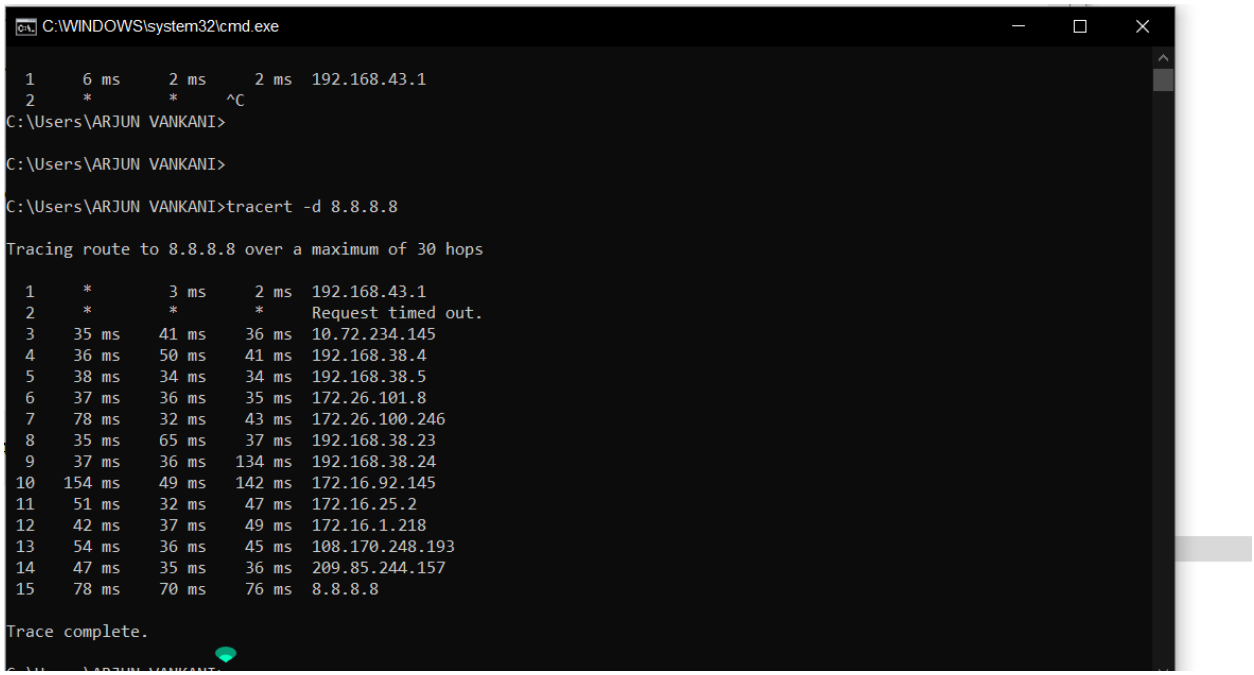
- !(Ip.dst == 192.168.43.201) gives the destination IP address where destination is not 192.168.43.201



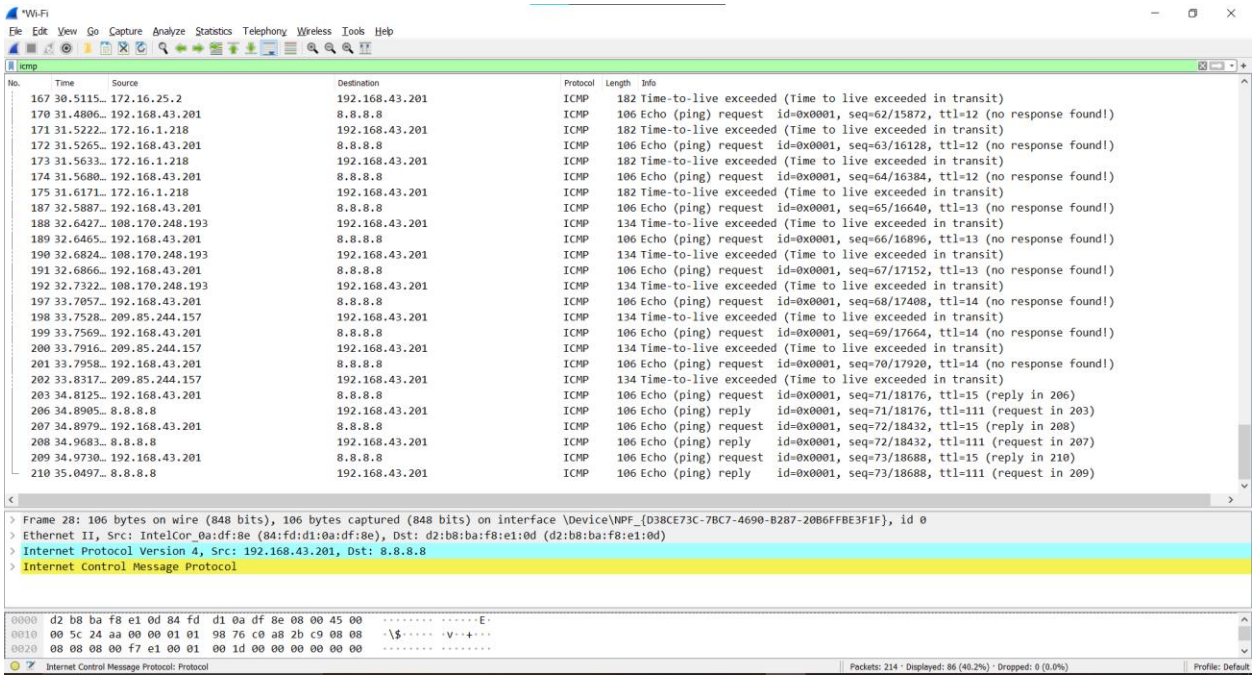
- Ipv6 gives all IP address



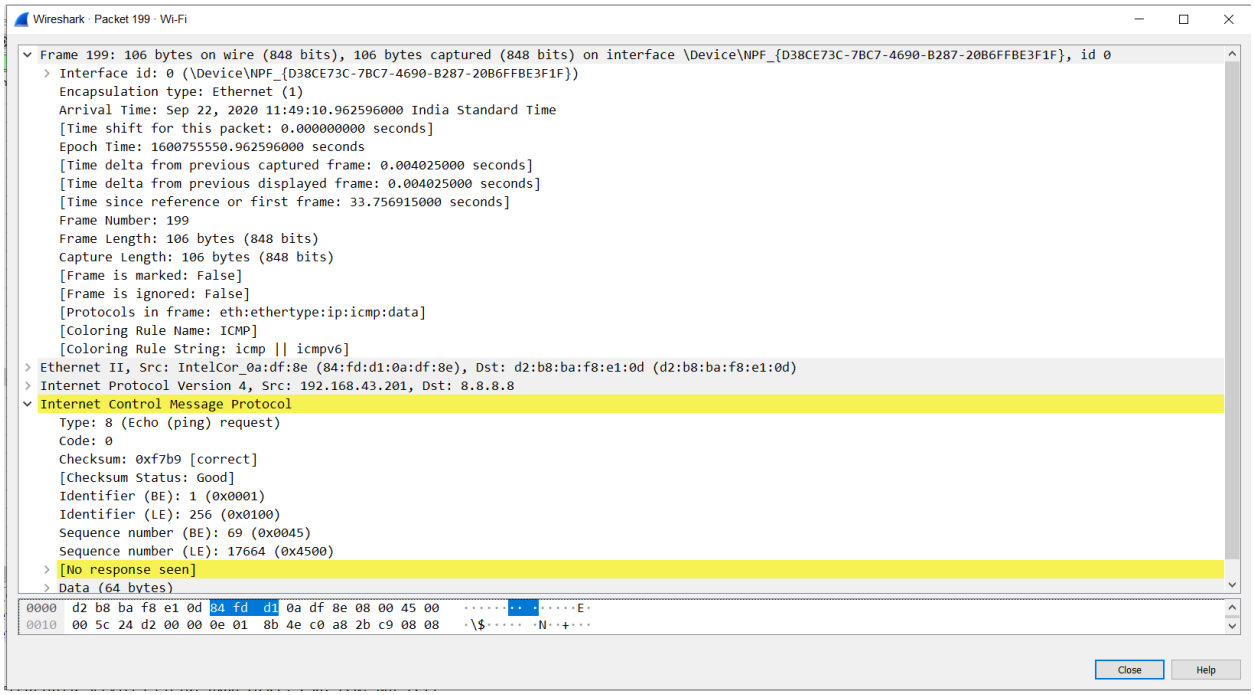
- ICMP protocol is Internet Control Message Protocol.
- Where we first run the command tracert-d 8.8.8.8 for google DNS public services.



- At the time we analysis the Wireshark software ICMP protocol.



This is for message request to DNS



This is for message reply to DNS