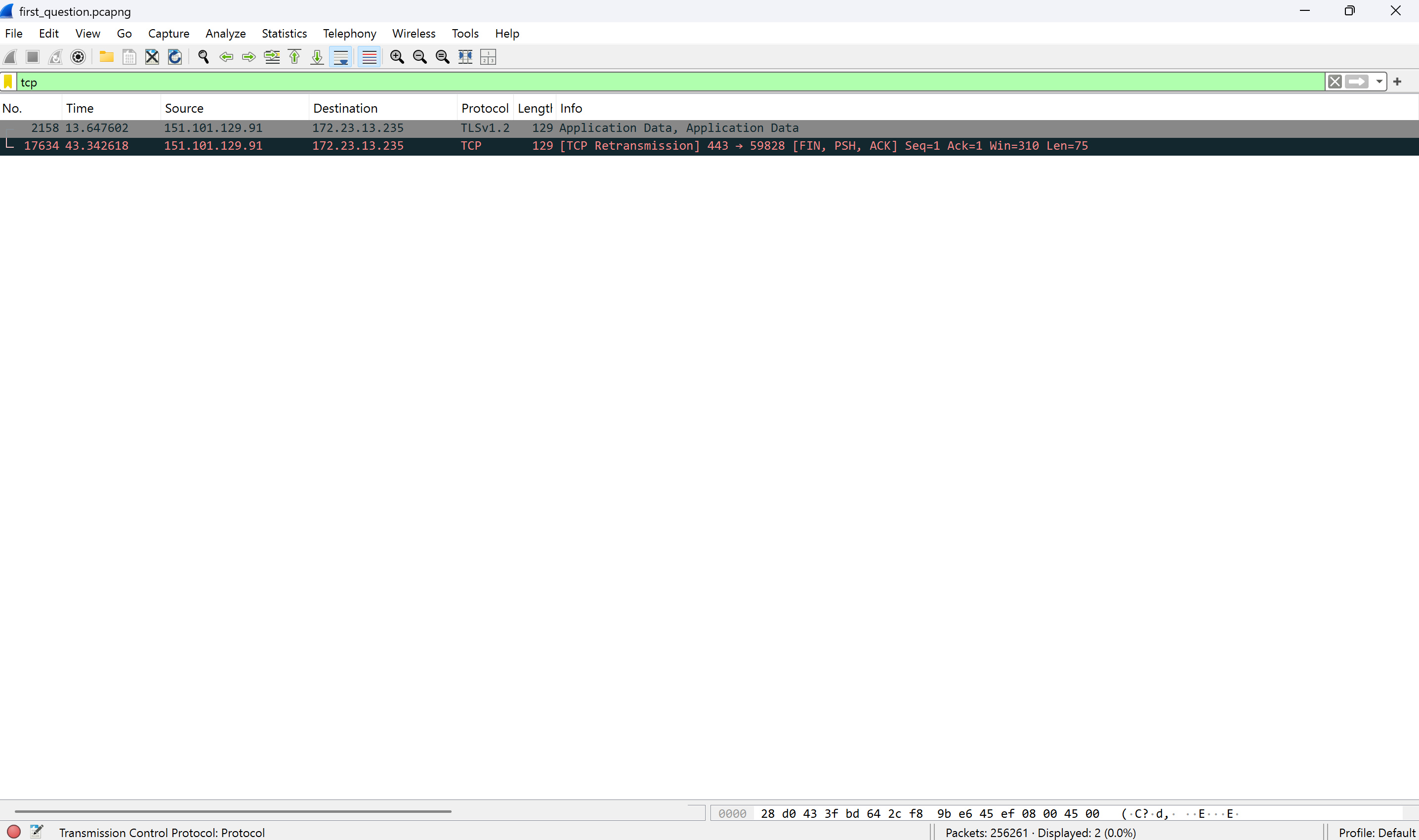
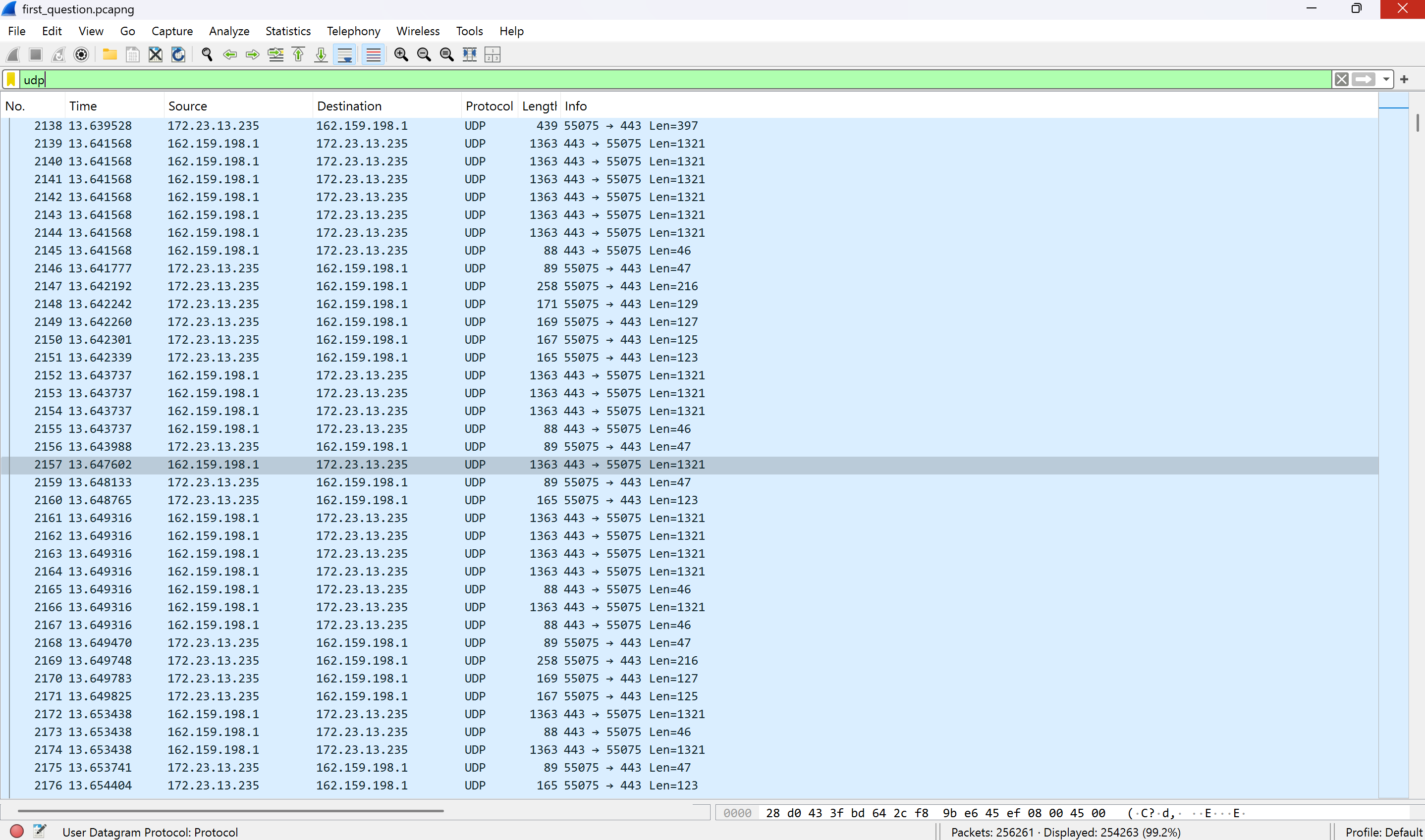
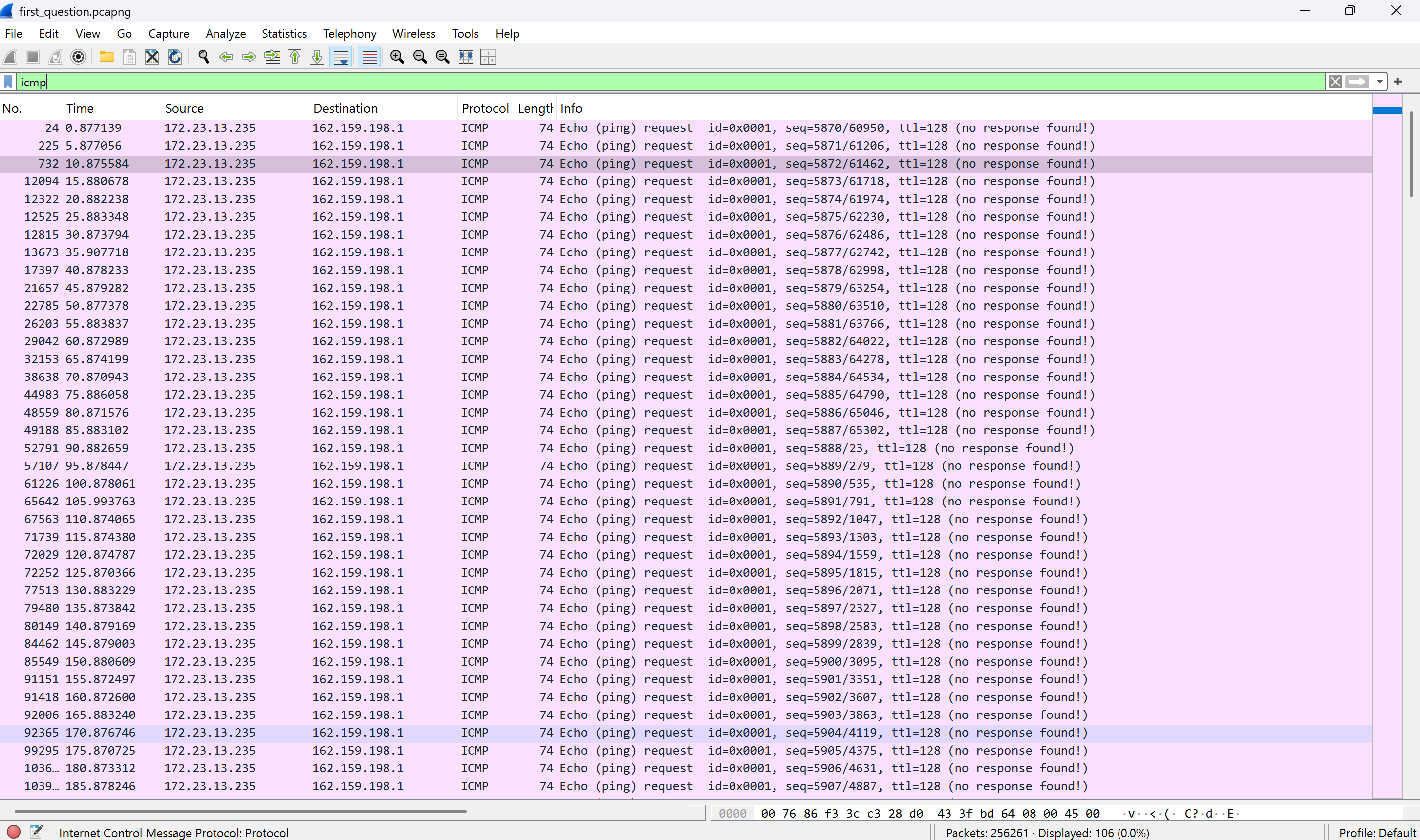
Wireshark Lab Assignment ( 2022csb1102 Prakhar Maurya)  
Question 1:

Tcp protocol: 

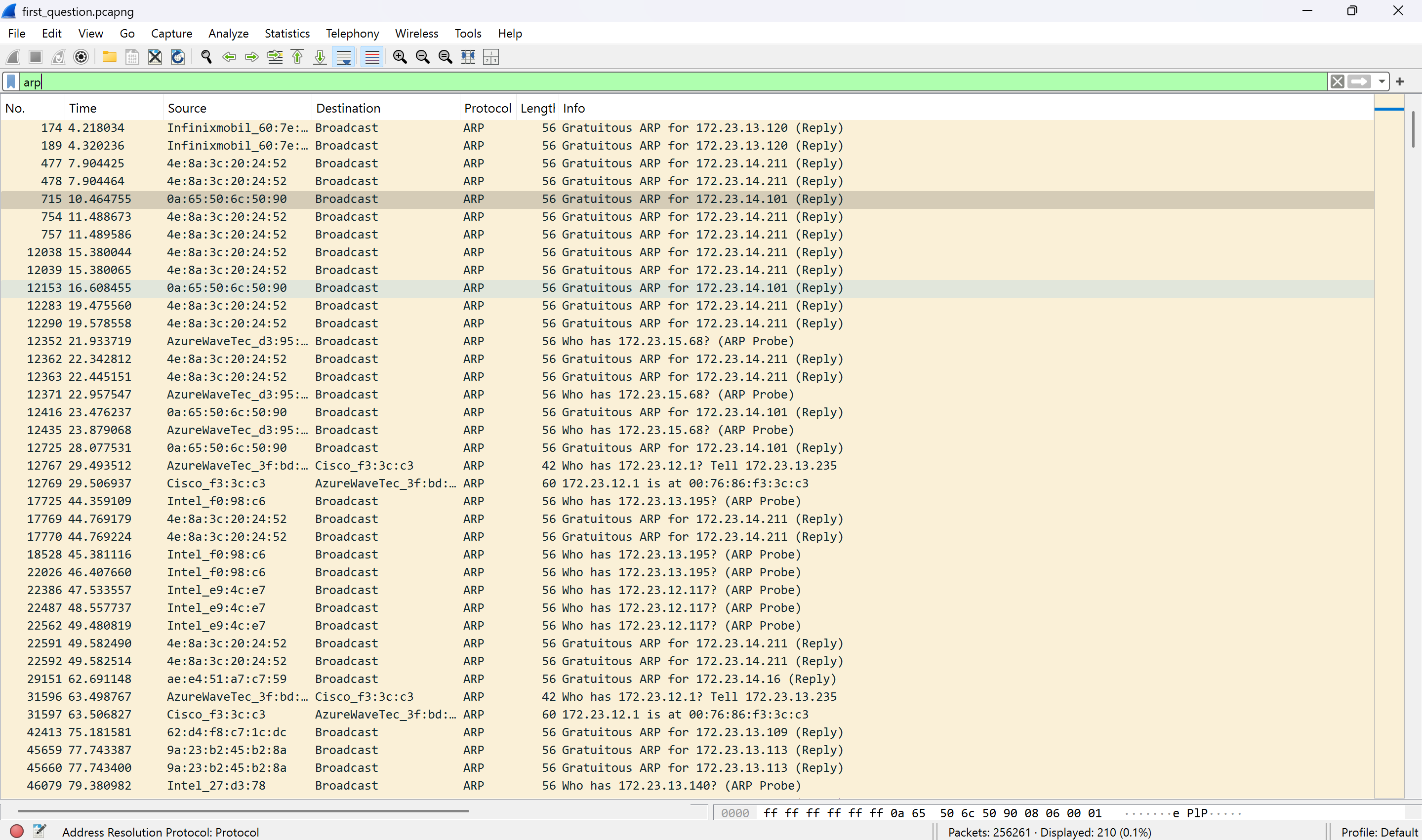
UDP protocol:



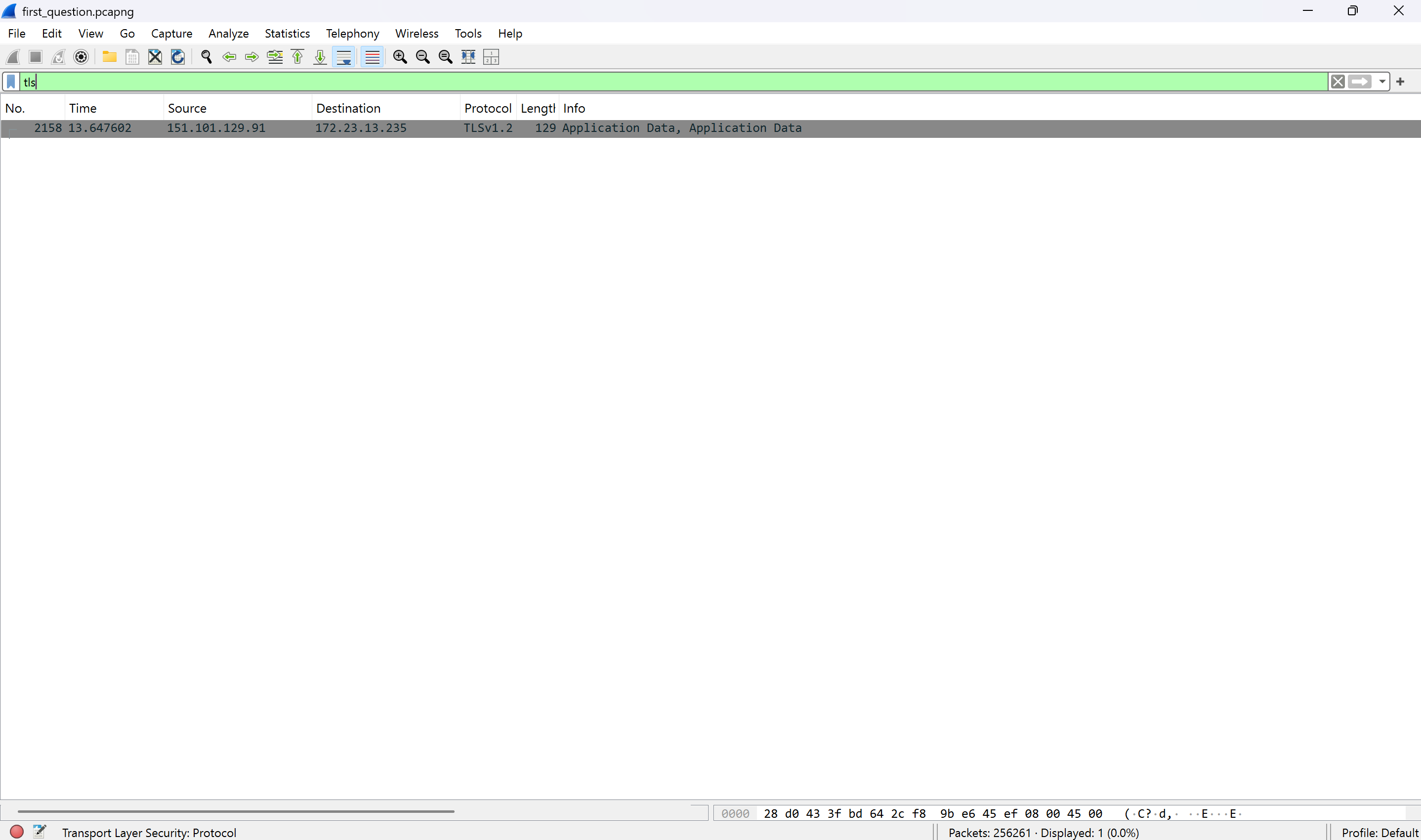
ICMP protocol:



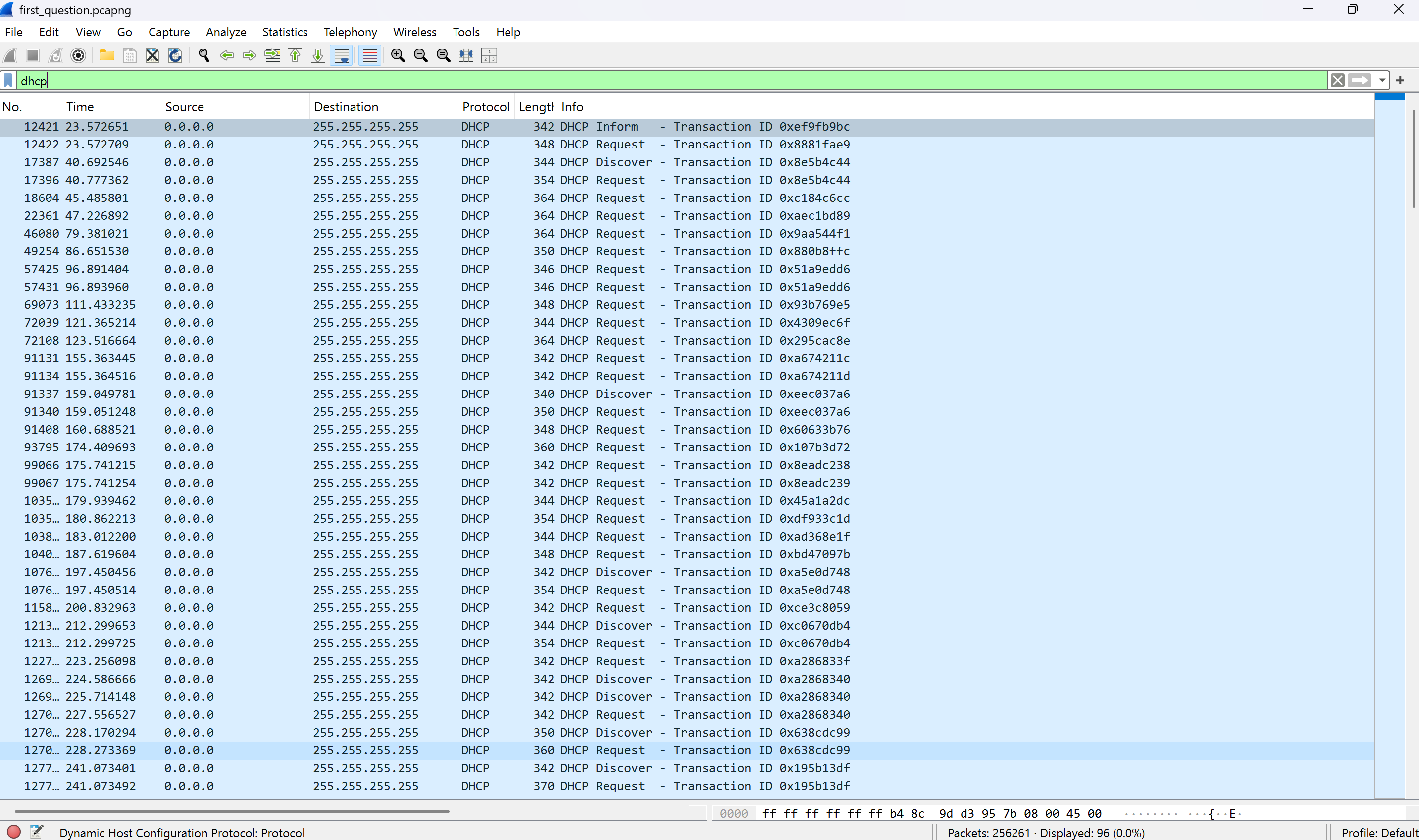
ARP protocol:



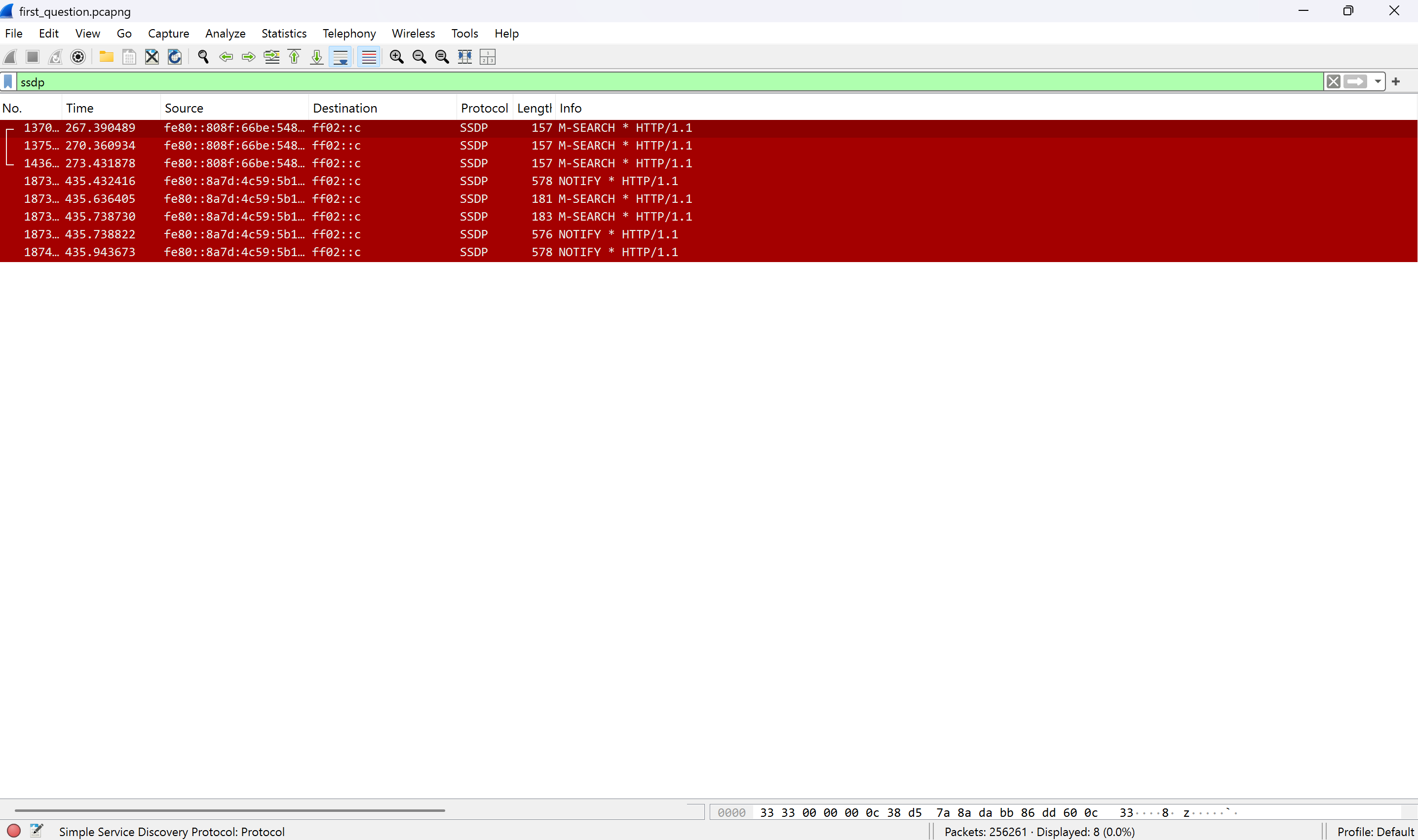
TLS protocol:



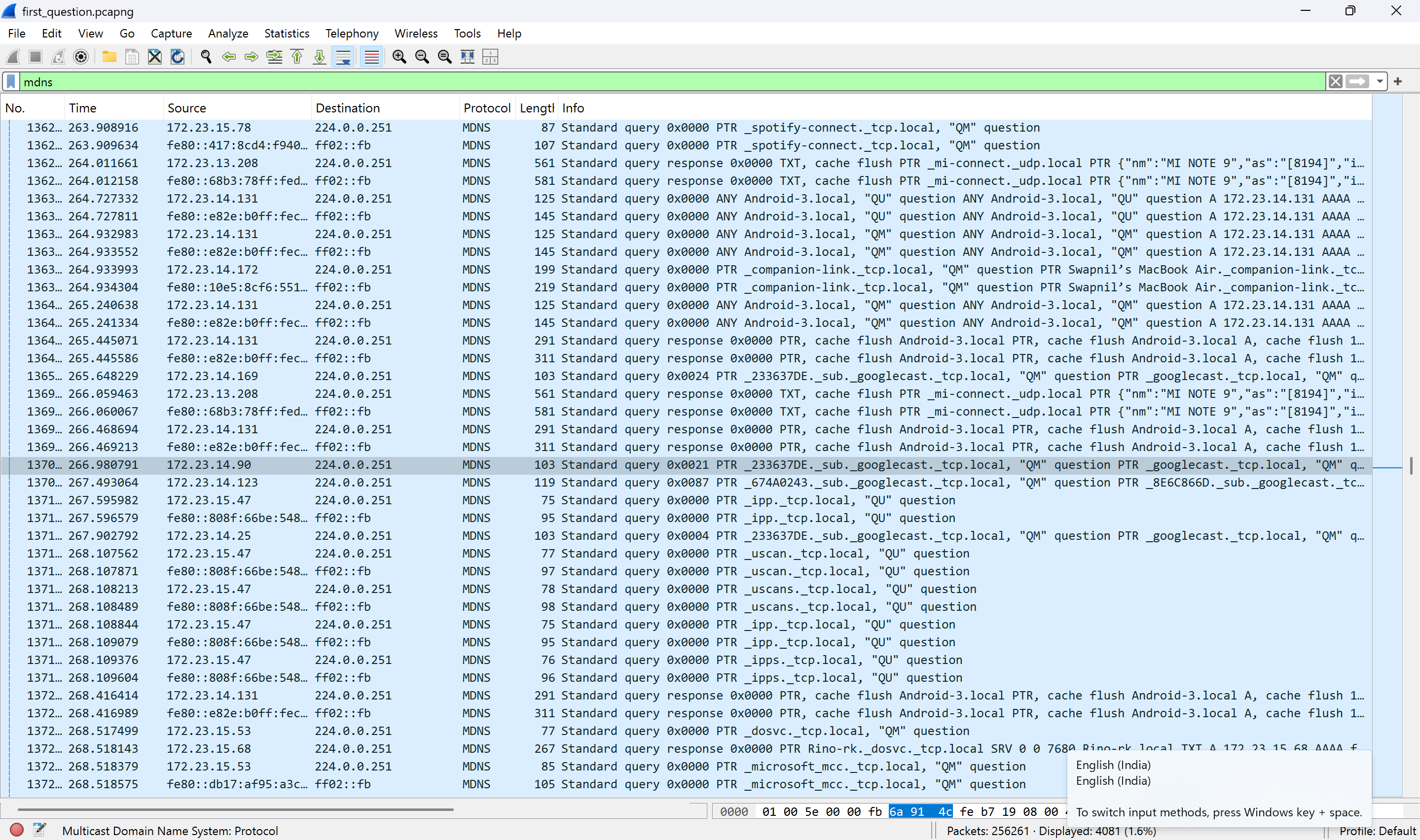
DHCP protocol:



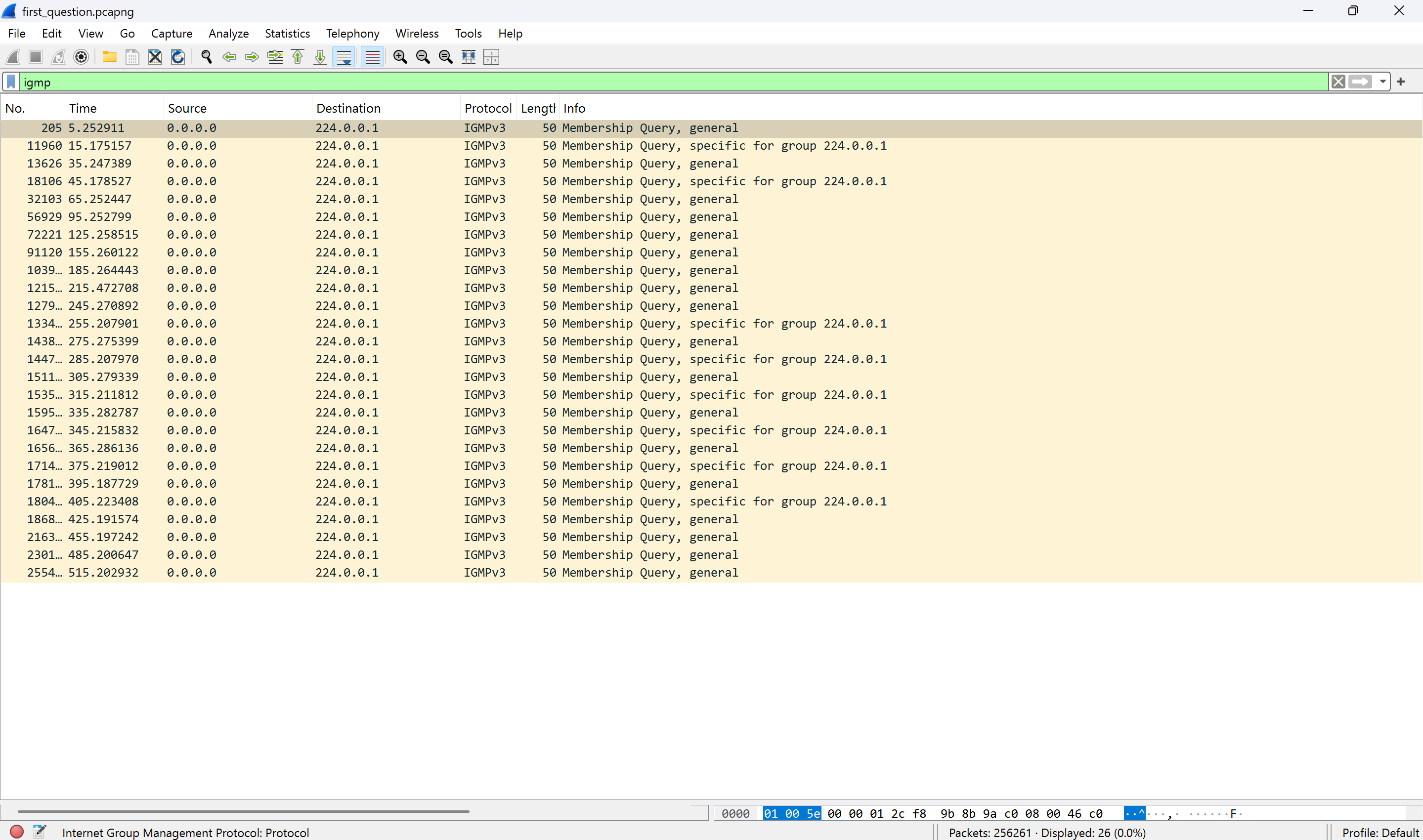
SSDP protocol:



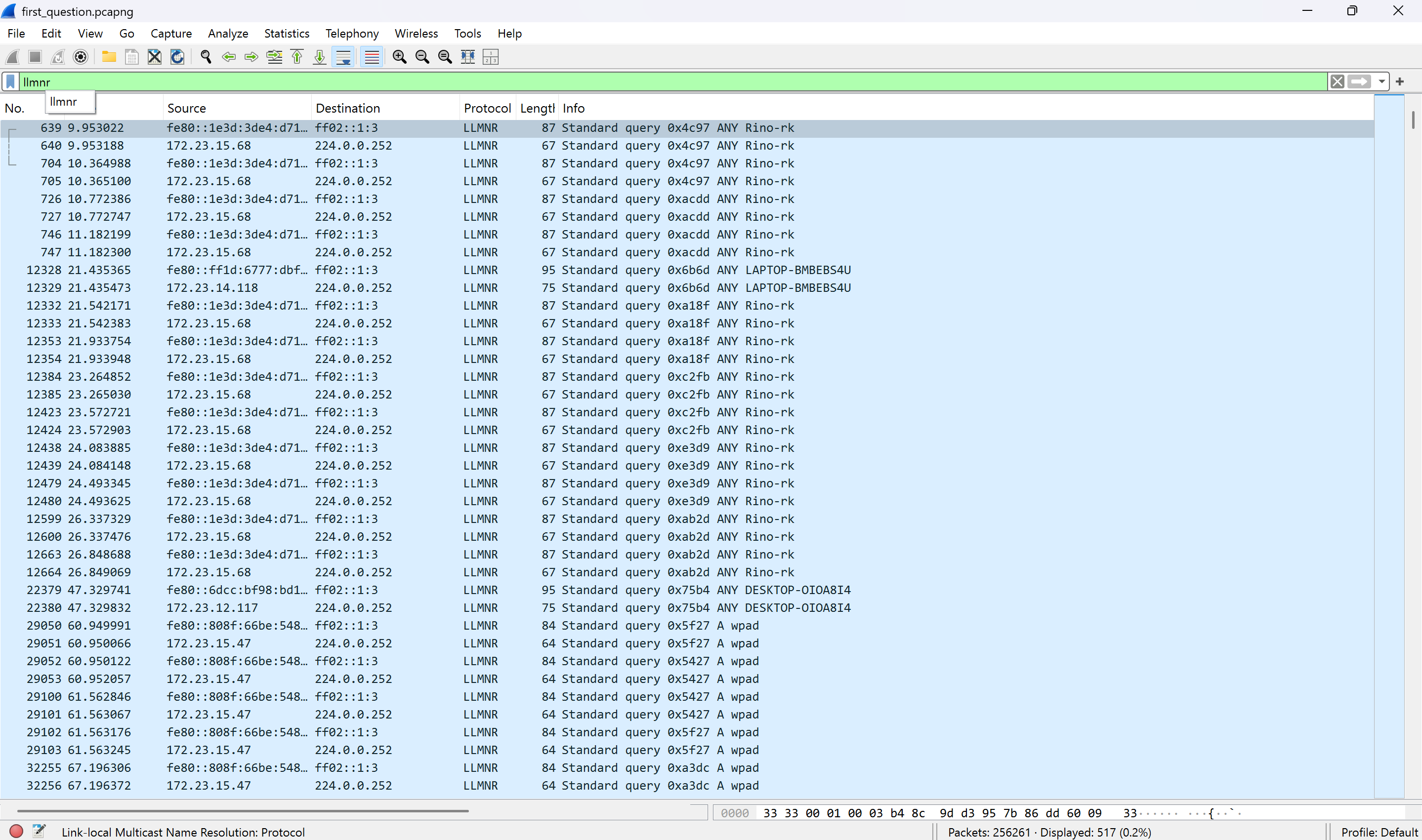
MDNS protocol:



IGMP protocol:



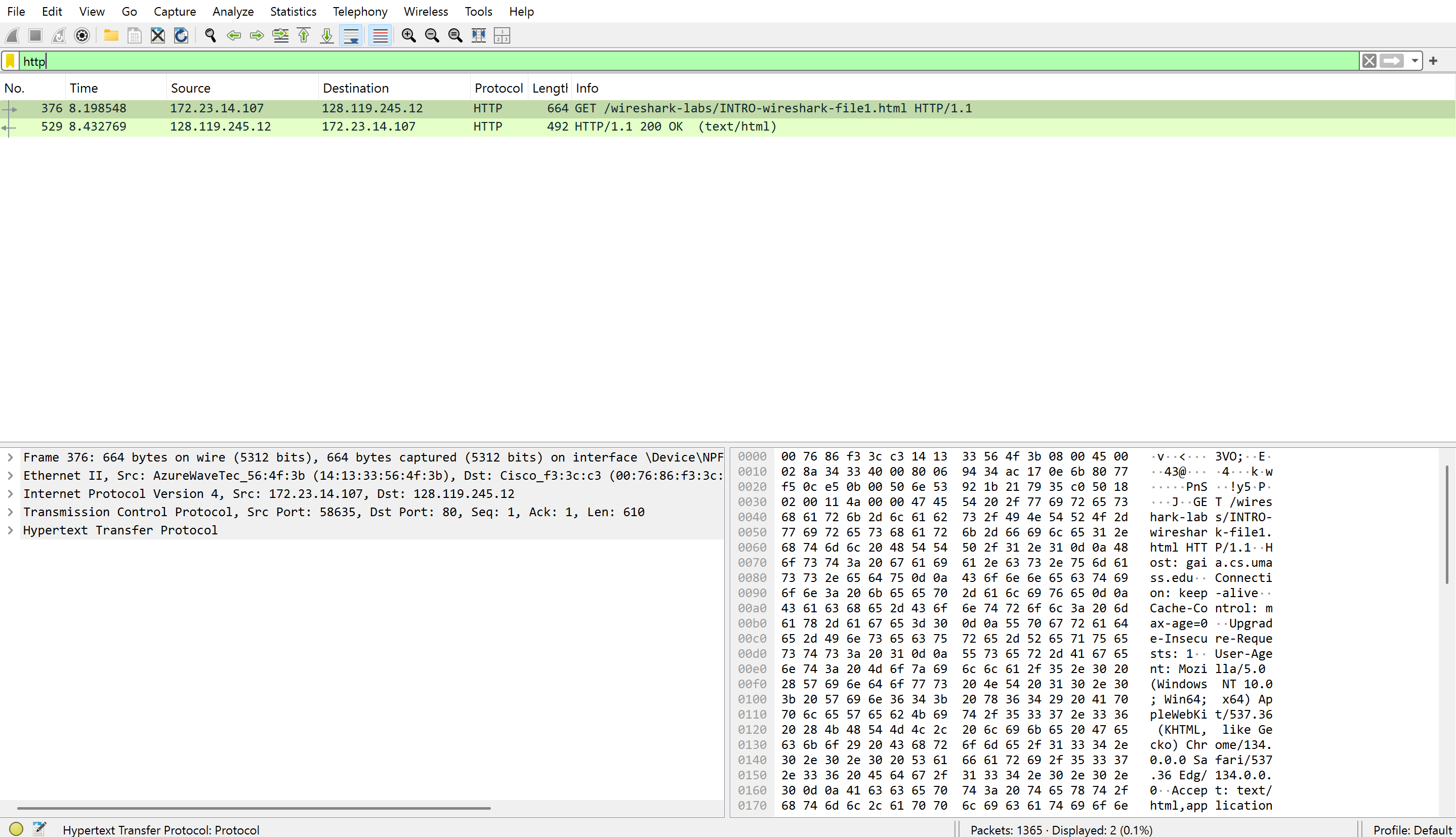
LLMNR protocol:



So the 10 protocols were:

1. TCP
2. UDP
3. ARP
4. TLS
5. MDNS
6. IGMP
7. ICMP
8. DHCP
9. SSDP
10. LLMNR

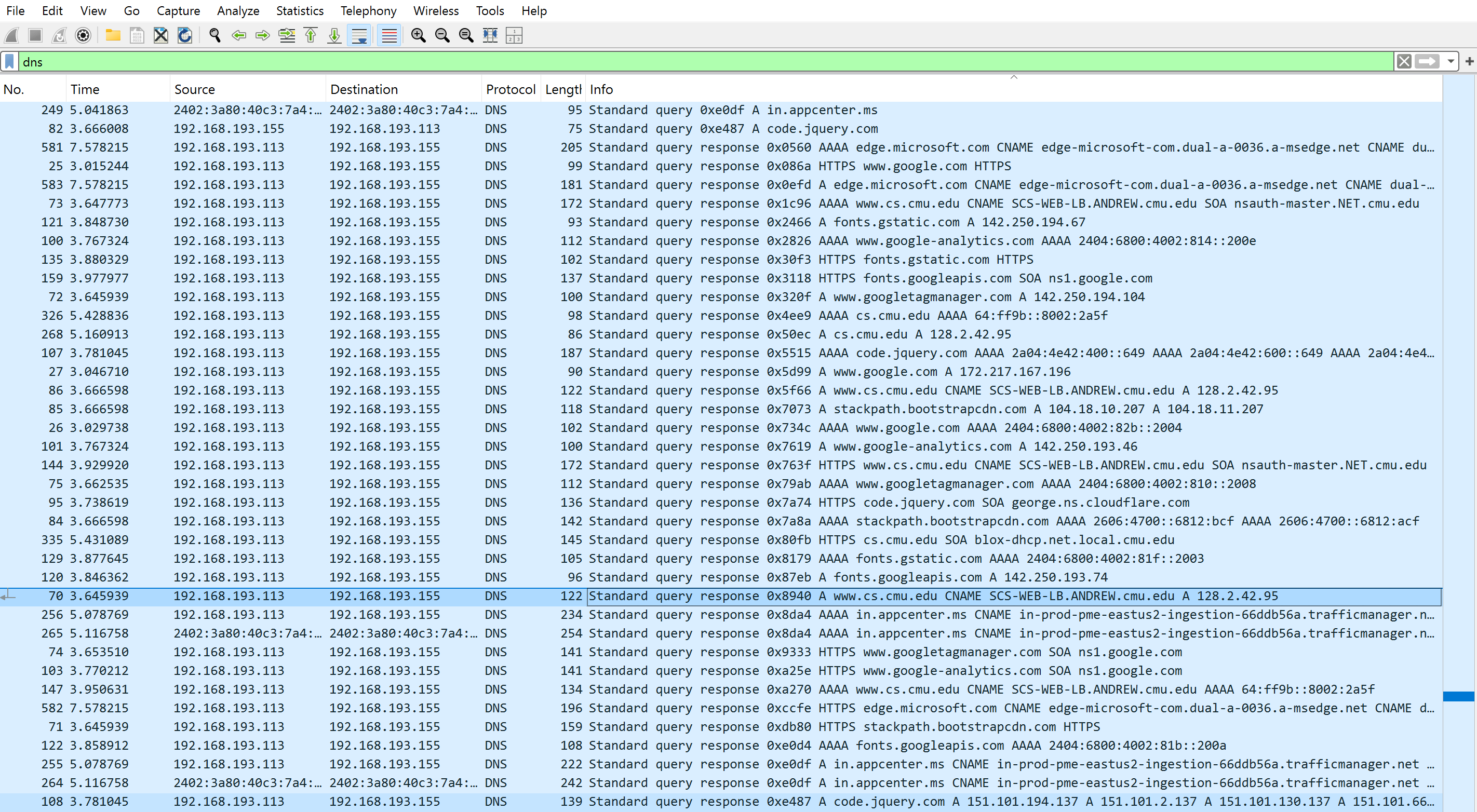
Question 2:

  
  
Packet #376 at time 8.198548 seconds: I sent an HTTP GET request to "/wireshark-labs/INTRO-wireshark-file1.html."  
Packet #529 at time 8.432769 seconds: I received the HTTP 200 OK response from the server.

The time difference between these packets is:  
8.432769 - 8.198548 = 0.234221 seconds (or about 234 milliseconds).

This means it took approximately 234 milliseconds for my computer to receive the server's response after sending the request.

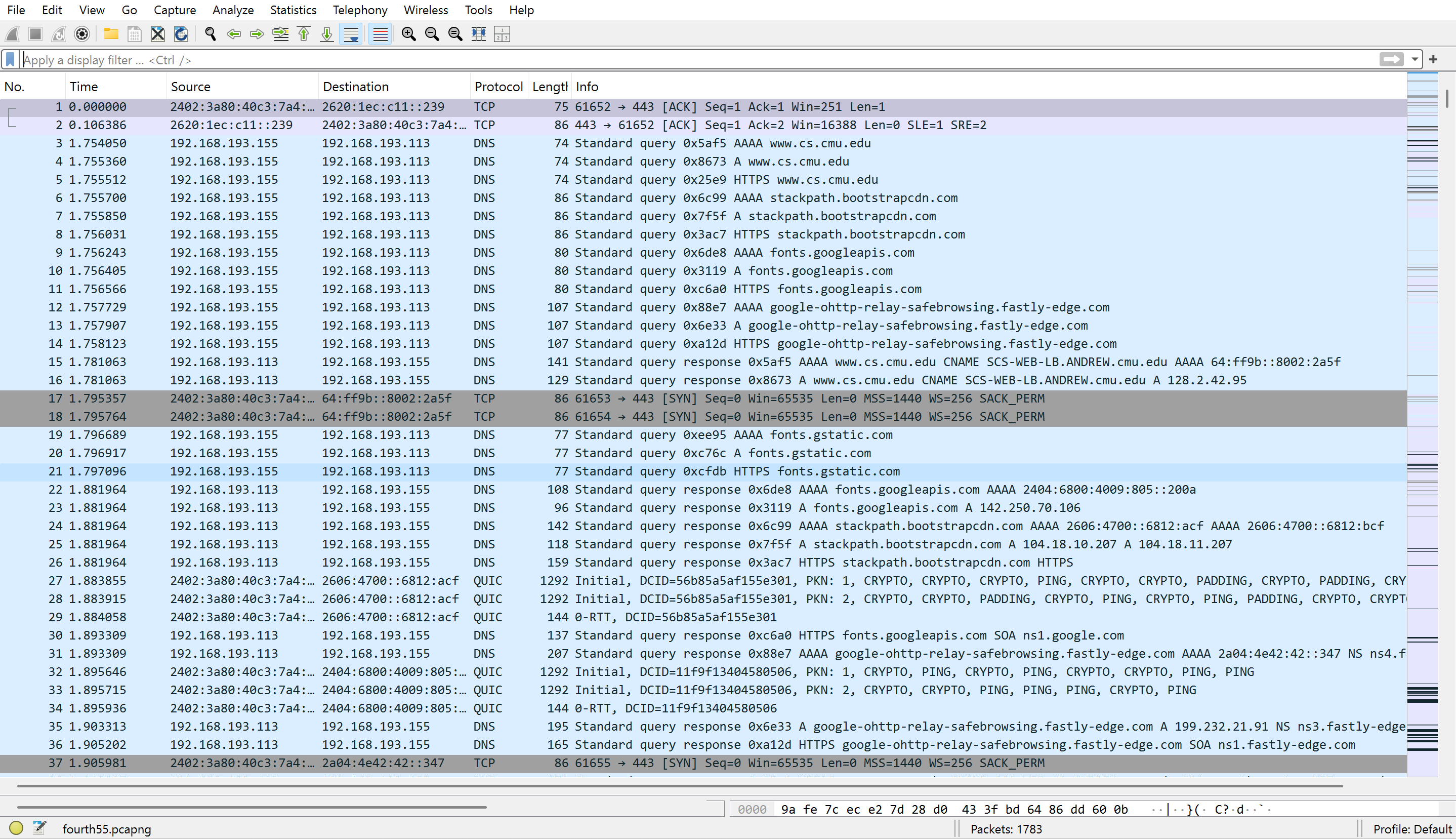
Question 3:



IP Addr of the web site is get from dns search response(selected row) = 128.2.42.95 My ip address is 192.168.193.155 (the destination column of the the selected row)

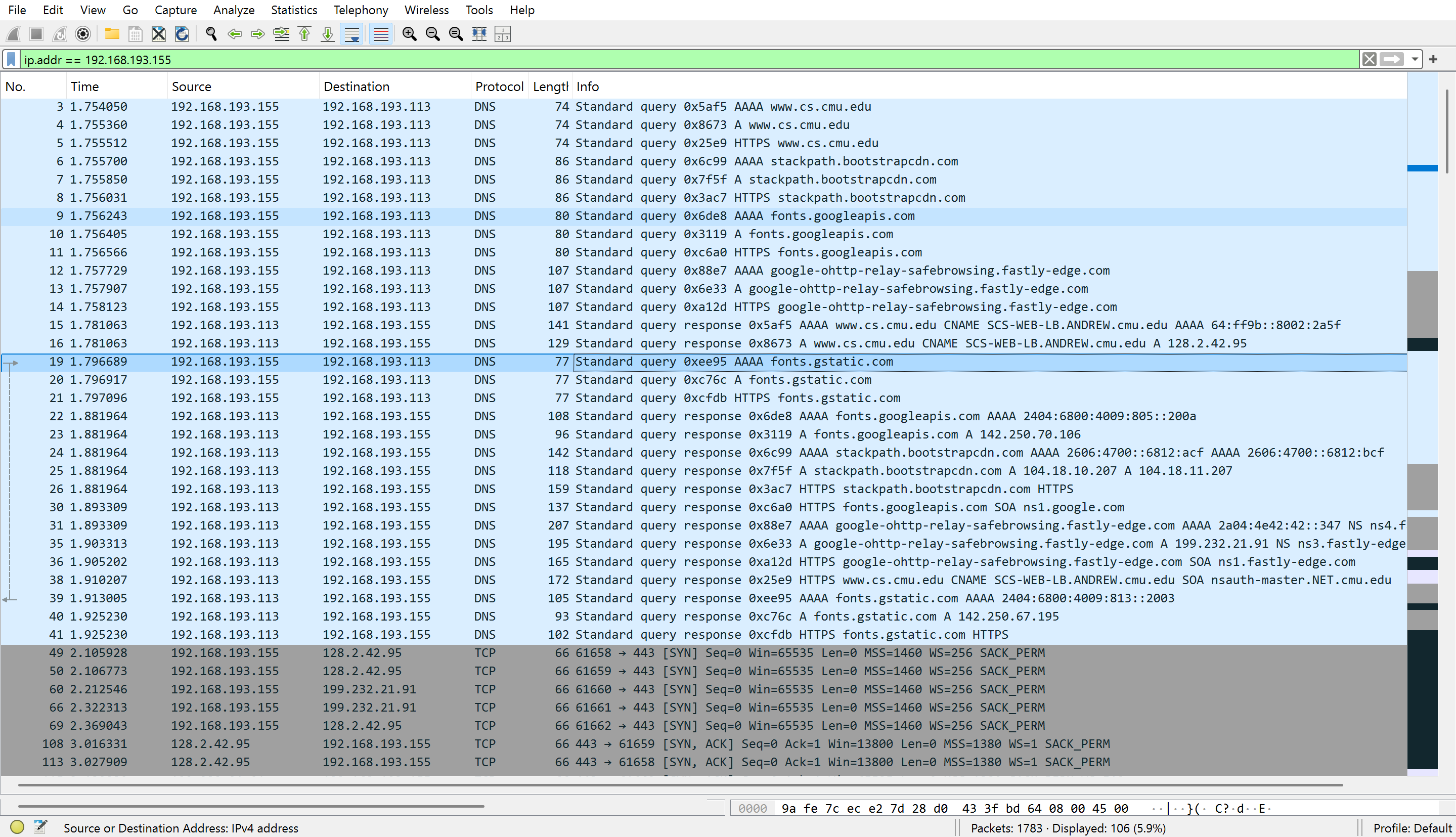
Question 4:

Total packets :1783



Packets containing my ip address = 1783(100%)

ip.addr == 193.168.193.155



Packets not containing my ip address = 0 (0%)

ip.addr != 193.168.193.155

