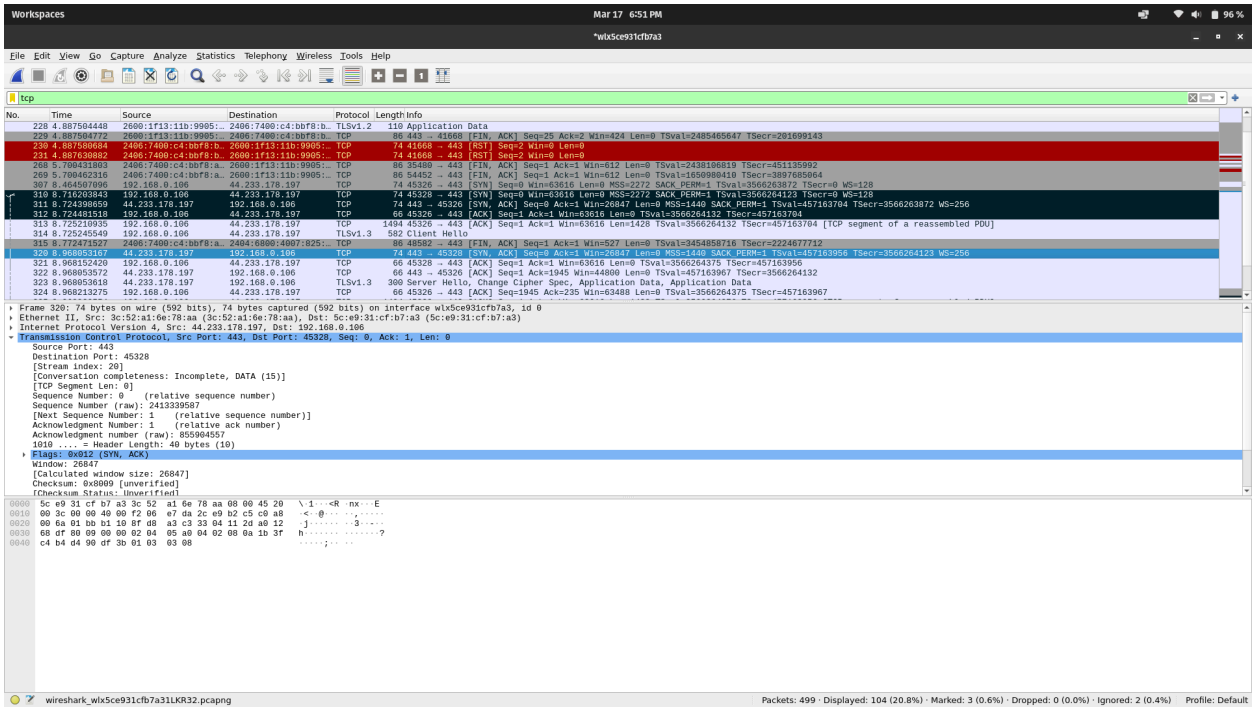
Name: J Kevin Immanuel
College: VIT Chennai

Q2)

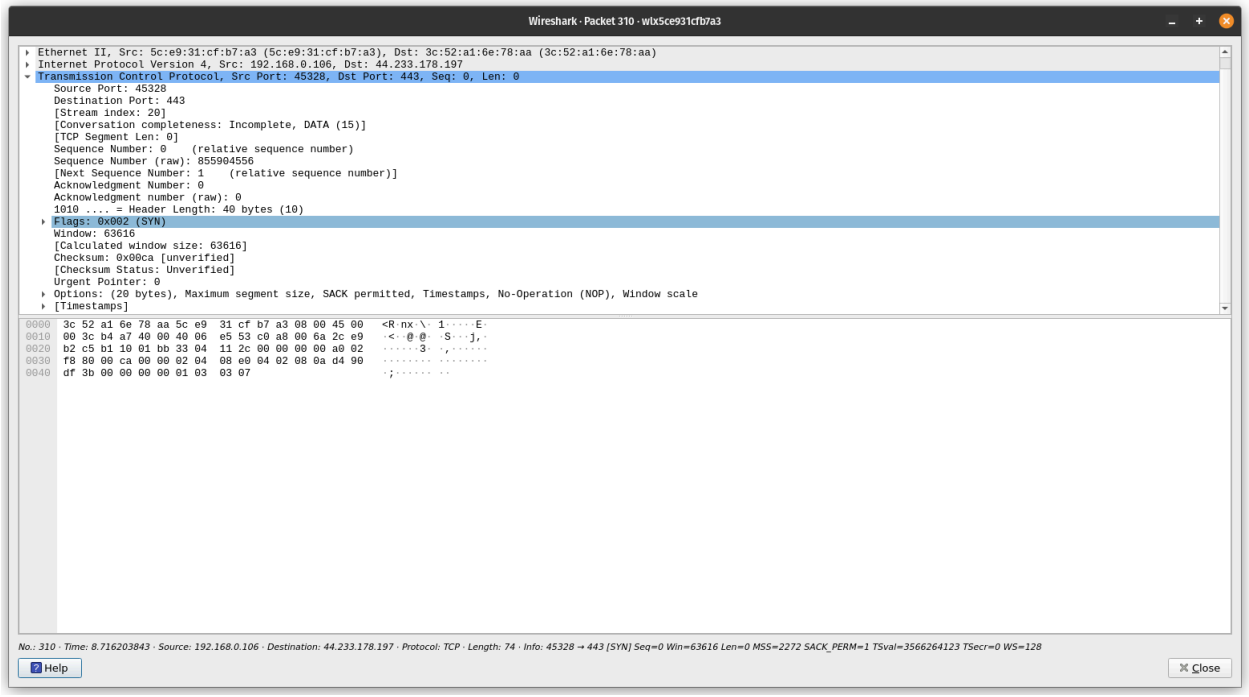
TCP;



The three Dark-blue color highlighted packets are TCP packets. Each one contains a specific meaning.

There are two IP mentioned: Source and Header. Each denote the client and server.

Frame1: SYN:

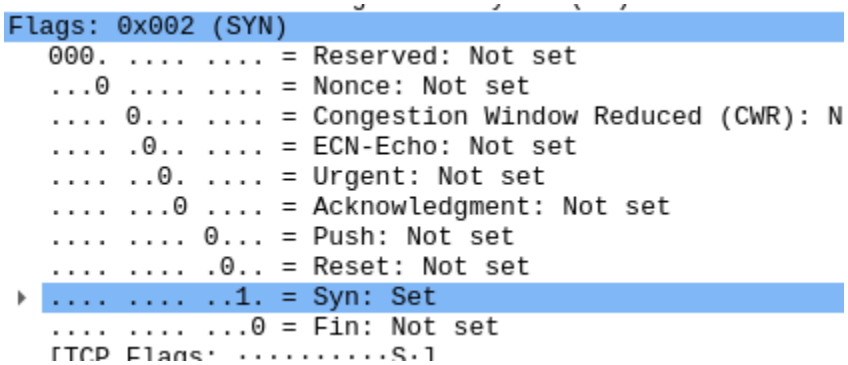


Source is 192.168.0.106 (System) and Destination is 44.233.178.197 (Server).

The SYN packet is SYNCHRONIZATION, where the client sends a request to the server establishing connection

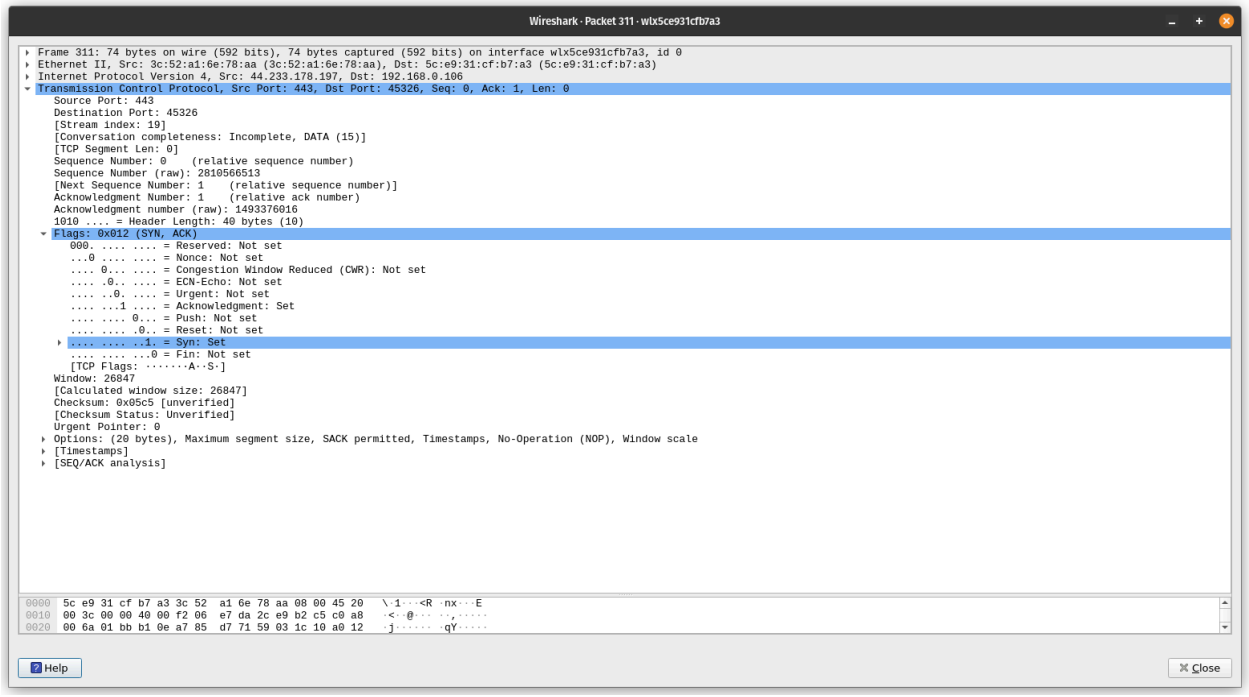
The sequence number is 0 (Although it is relative, the actual sequence number will be high). This means that this is the first request packet.

The window size is 63616



The flags show that only SYN is set, confirming that this is a SYNCHRONIZE packet.

FRAME 2: SYN+ACK:



Source is 44.233.178.197 (Server) and destination is 192.168.0.106 (System).

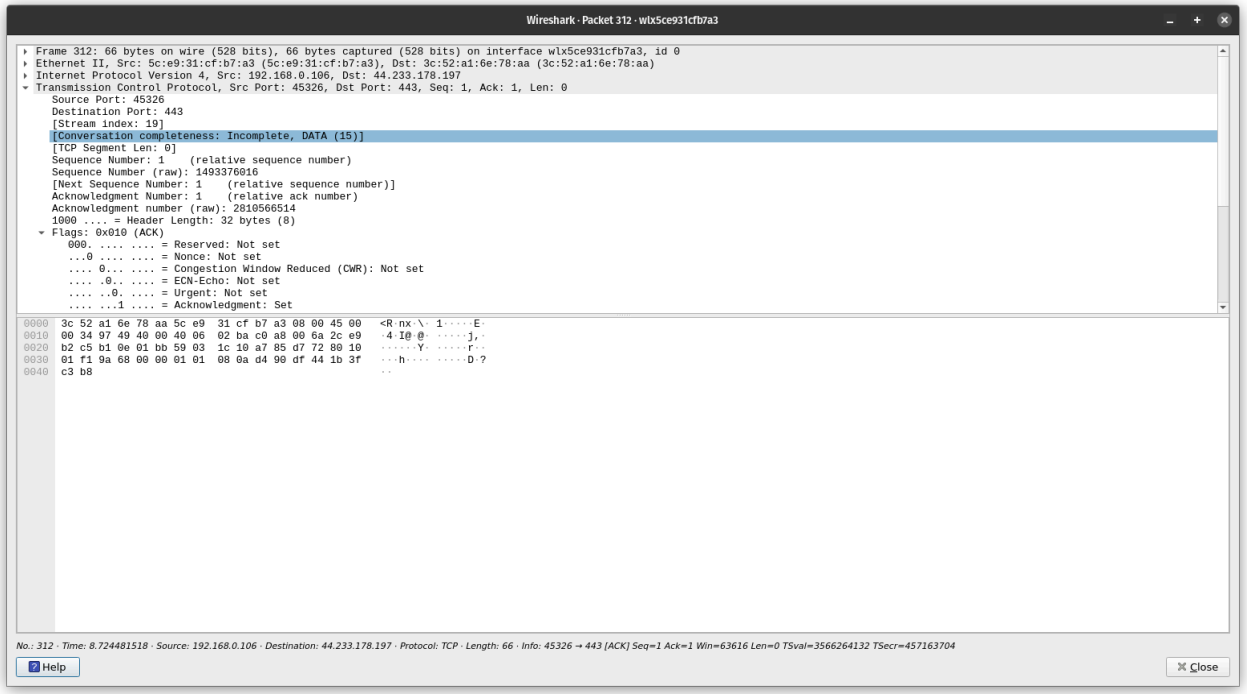
This is the second packet: SYN+ACK. This packet is a reply from server to client, acknowledging the client's request and the server is ready to establish a connection.

The window size mentioned is 26847.

According to the flags, the SYN and ACK bits are set.

Sequence number is 0 and ACK number is 1

FRAME 3: ACK:



Source is 192.168.0.106 (System) and Destination is 44.233.178.197 (Server).

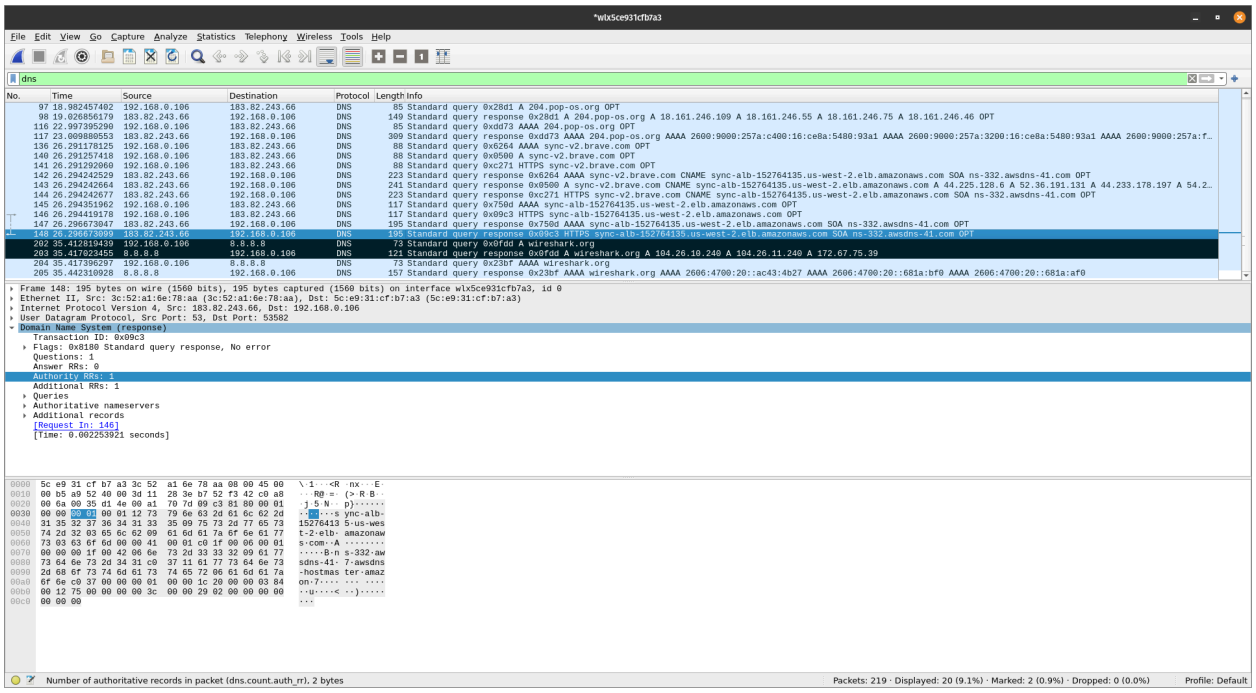
This is from client to server, acknowledging the server's response and is ready to start establishing connection.

Window size is 497

Under flags section, only ACK is set

Sequence number is 1 and Ack number is 1

DNS:

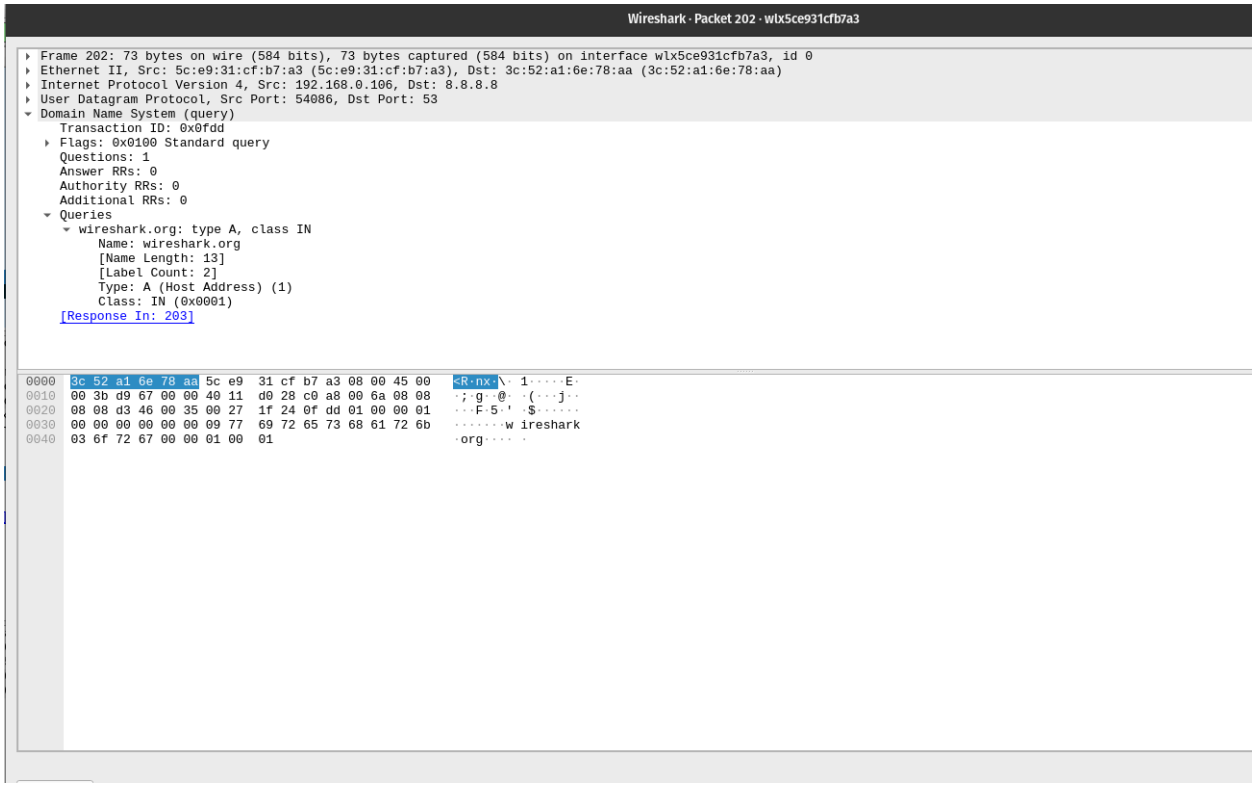


The two packets marked in black are the DNS query and response packets.

Packet 1: DNS Query:

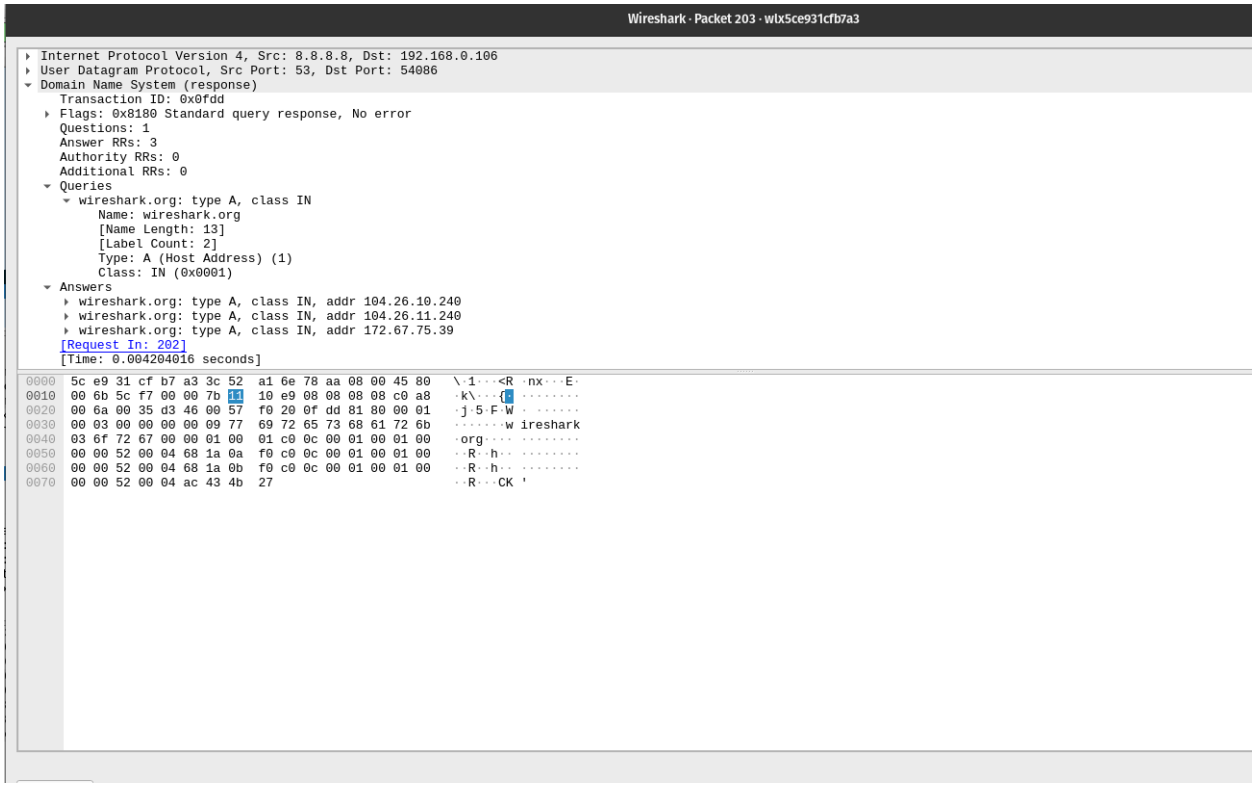
I use the command “nslookup wireshark.org 8.8.8.8” : ask 8.8.8.8 to resolve the domain name and give the IP addresses of wireshark.org

Query frame:



This is the query frame. This frame has a query to 8.8.8.8 to resolve wireshark.org into its ip addresses.

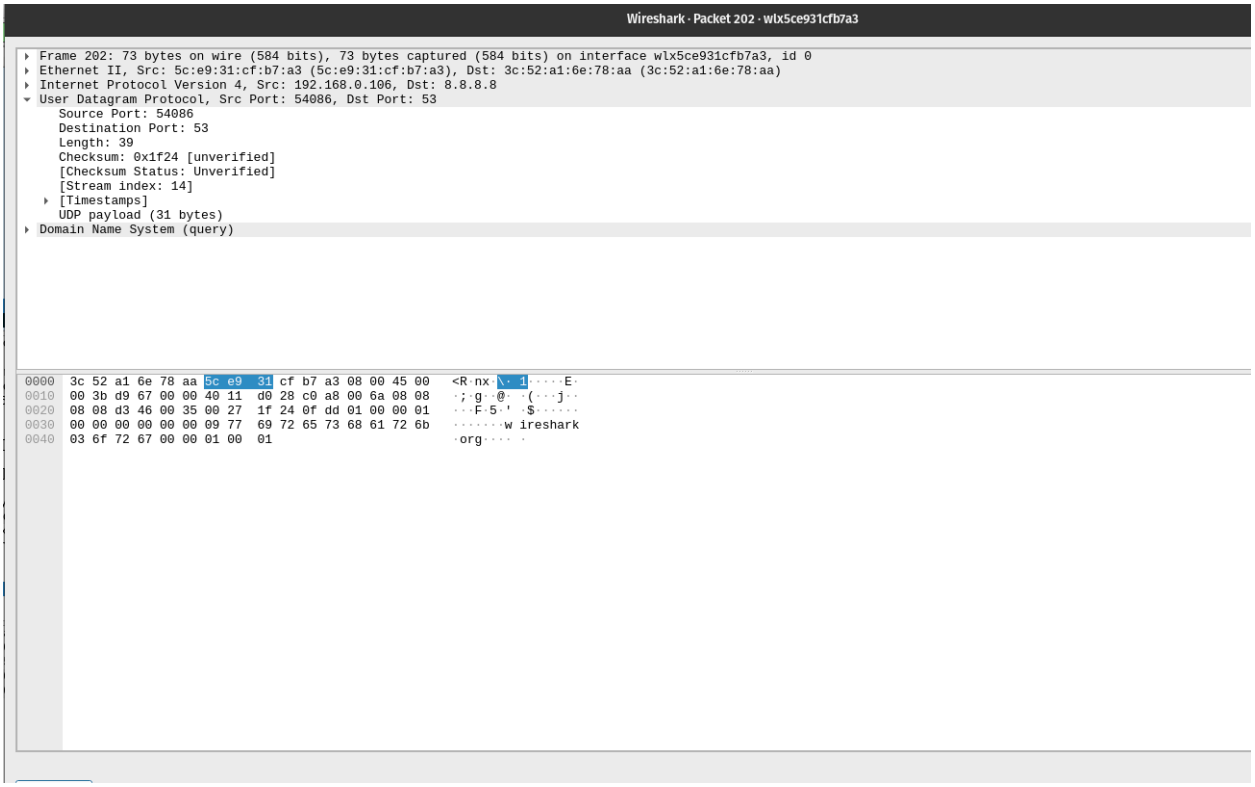
Response frame:



This is the response from 8.8.8.8, giving us the IP addresses of wireshark.org

UDP:

DNS protocol uses UDP, we will analyze the same frames:



Here we can see there is a section about User Datagram Protocol. It has a Source port 54086, Destination port 53, length of data (including headers) as 39. The data itself is the DNS query/response. There is a checksum to check if the packet received has no error/data loss.