Question 2

Use Wireshark to capture and analyze DNS, TCP, UDP traffic and packet header, packet flow, options and flags

DNS (Domain name system)

It contains all ip address of the domain name (Ex:google.com). The ip address is then used to send packet to the destination.

Types:

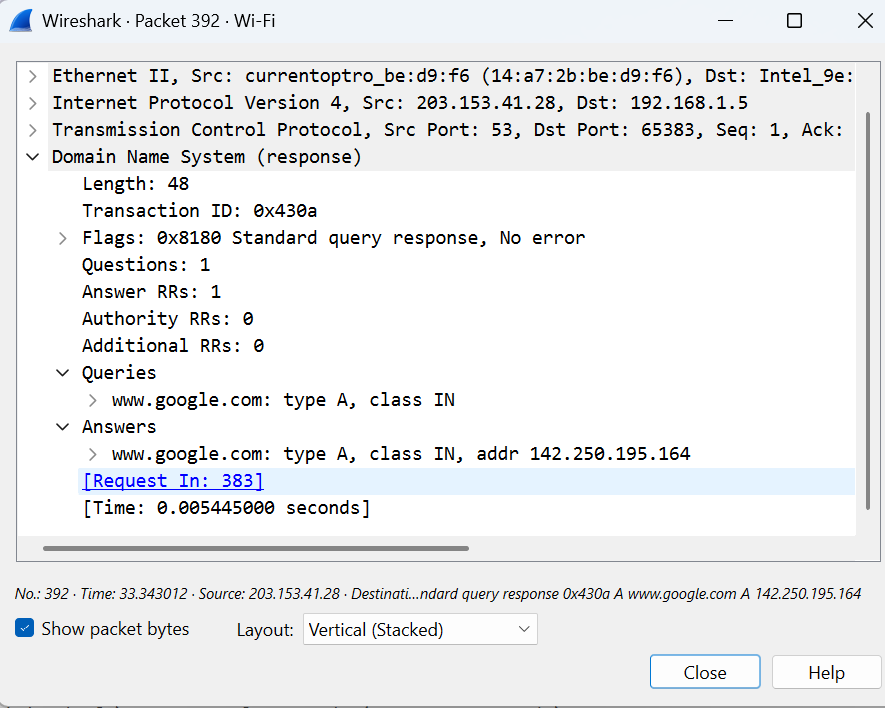
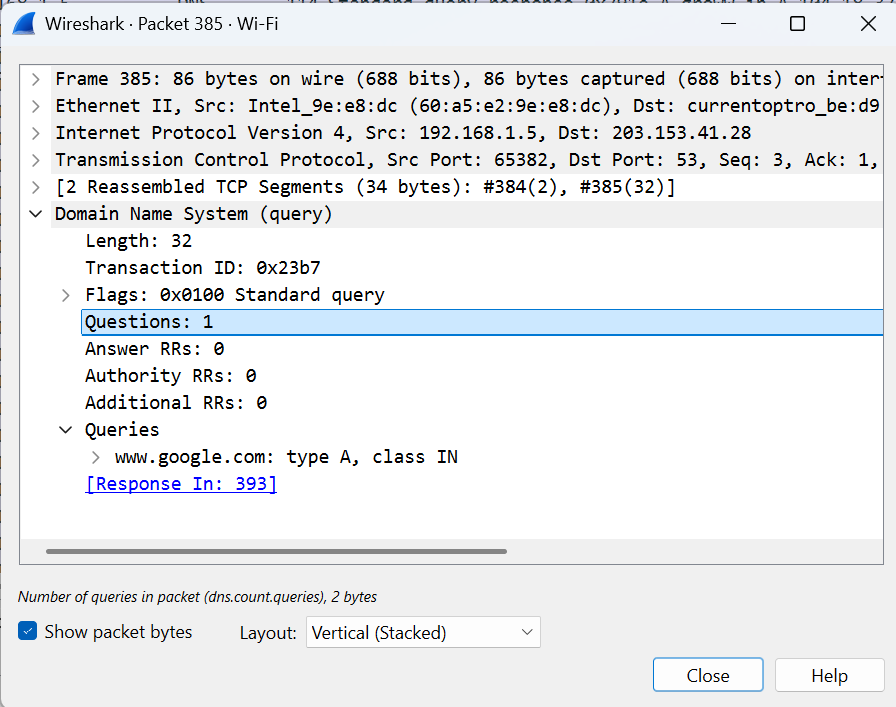
Recursive Resolver: Found in ISP or google public DNS (8.8.8.8)

Root DNS Servers: Top Level server (eg: “.”)

Top Level Domain Server : Manage .com, .org, .net etc

Authoritative DNS server : Holds actual ip address of the domain

Here we have DNS Query askng for ip address of google.com and we also have a DNS response from the router stating the reply with ip address of google.com



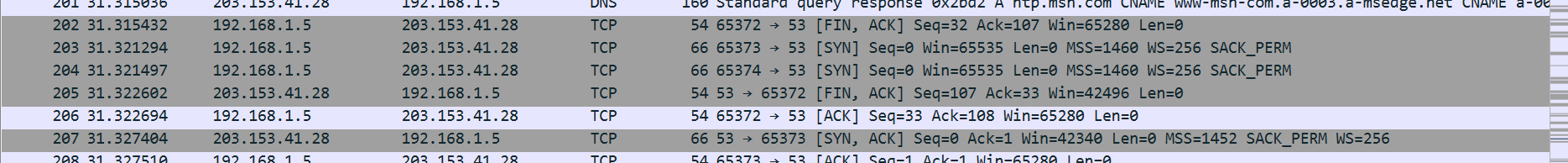
TCP (Transmission control protocol)

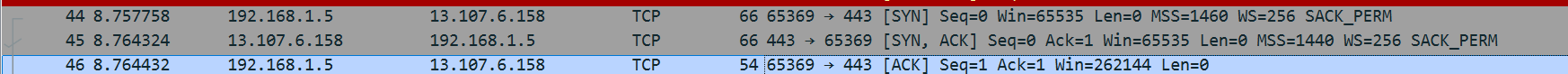
It is used for reliable communication. The protocol Ensure data delivered is accurate and in order. The transmission follow like

Connection Establishment (3 way handshake [SYN, SYN-ACK, ACK])

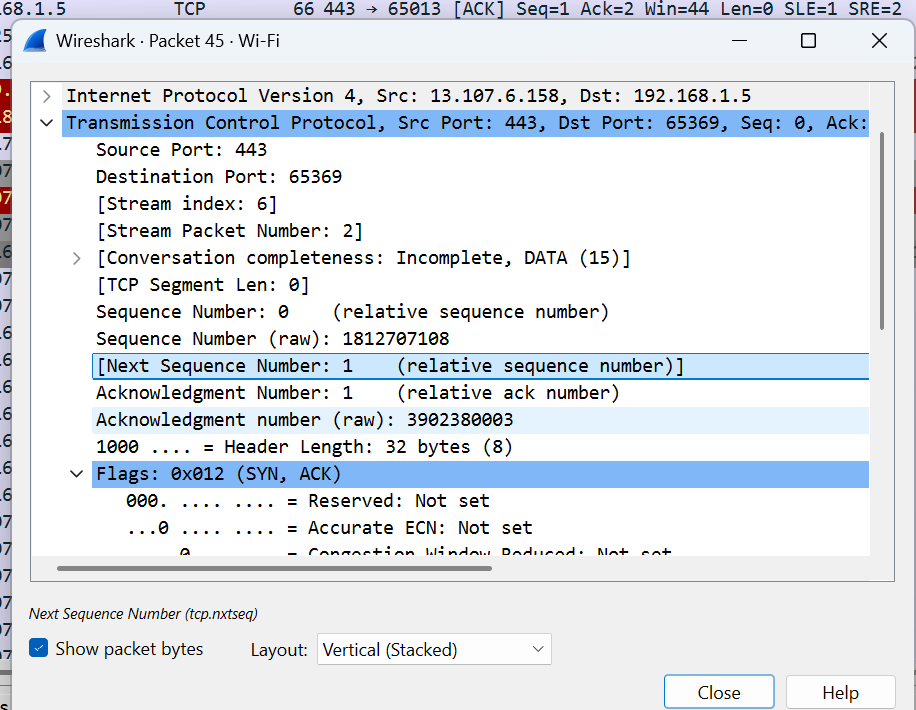
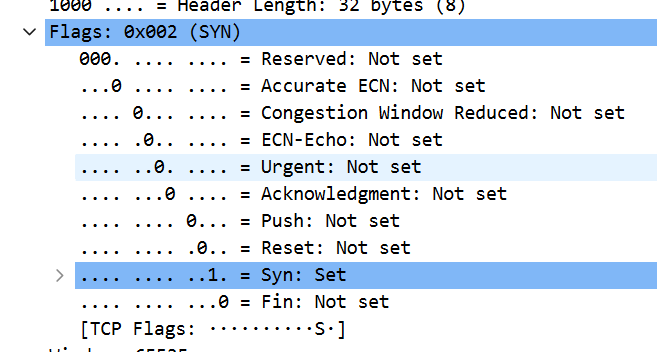
Data Transfer

Connection Termination (4 way Handshake [FIN, FIN-ACK, FIN,ACK])

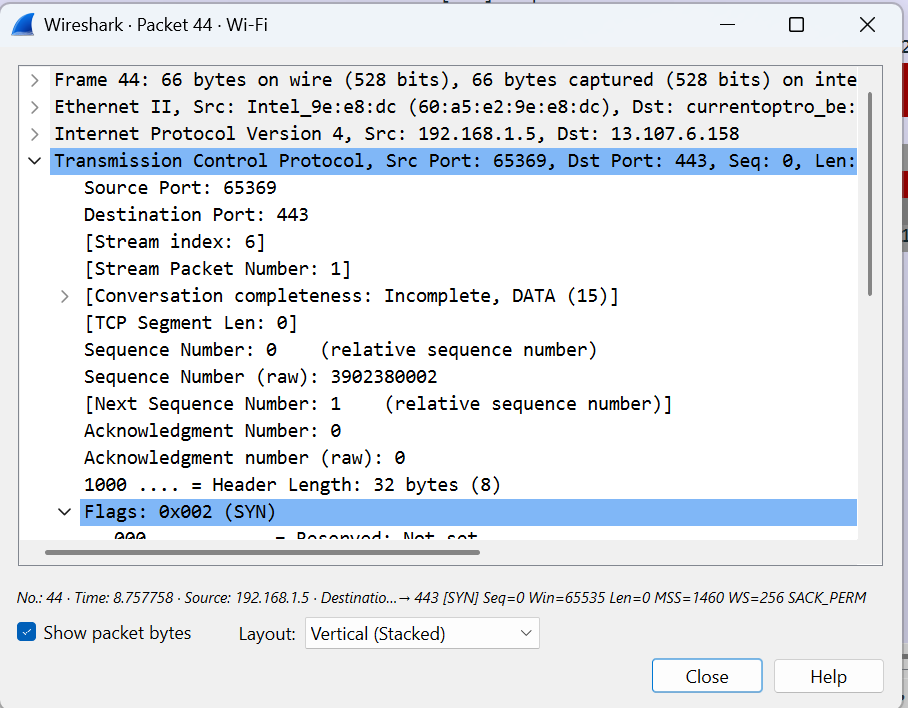




Each packet header contains Stream Index which helps to group the conversation. Stream Index tell whether the packet belongs to same conversation or not. Each packet contains a flag section telling which packet is transmitted whether ack, syn or fin etc

In the SYN packet given below we have Seq Number, Seq Number raw, Ack Number, Next Seq Number, Ack Number raw.



Sequence number is used to find the data transmission order. Let’s say a packet is send to router with seq number as 1000 with 10 byte of data. The router will ack with ack number as 1010 which could be your next seq numbers. The next seq number in the packet refere to the expected seq number which will come next. The seq number raw is nothing but the actual seq number going on. This is same for ack number

PORTS:

80 : HTTP

443 : HTTPS

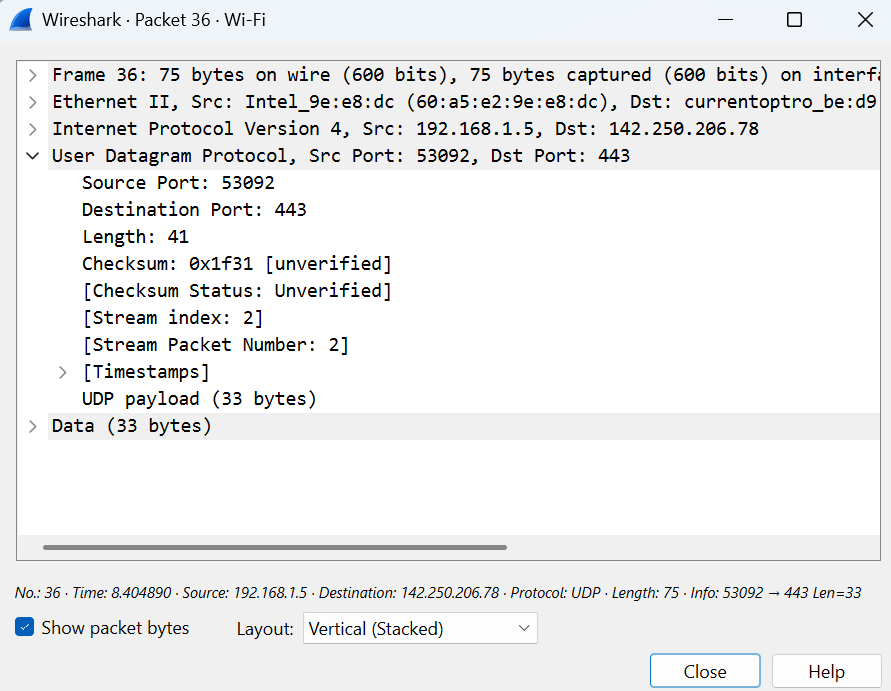
25 : SMTP

21 : FTP

22 : SSH

UDP (User Datagram packet)

This protocol is not a reliable one. This does not guarantee the packet delivery. It just Unicast the packets to the network. It will not have concern about the delivery. But compare to TCP is light and fast. It has small header then TCP, here we don’t have seq and raw numbers. It only has 8 bytes in header.



PORTS:

53 : DNS

67/68 DHCP

161 : SNMP

123 : NTP

500 : VPN