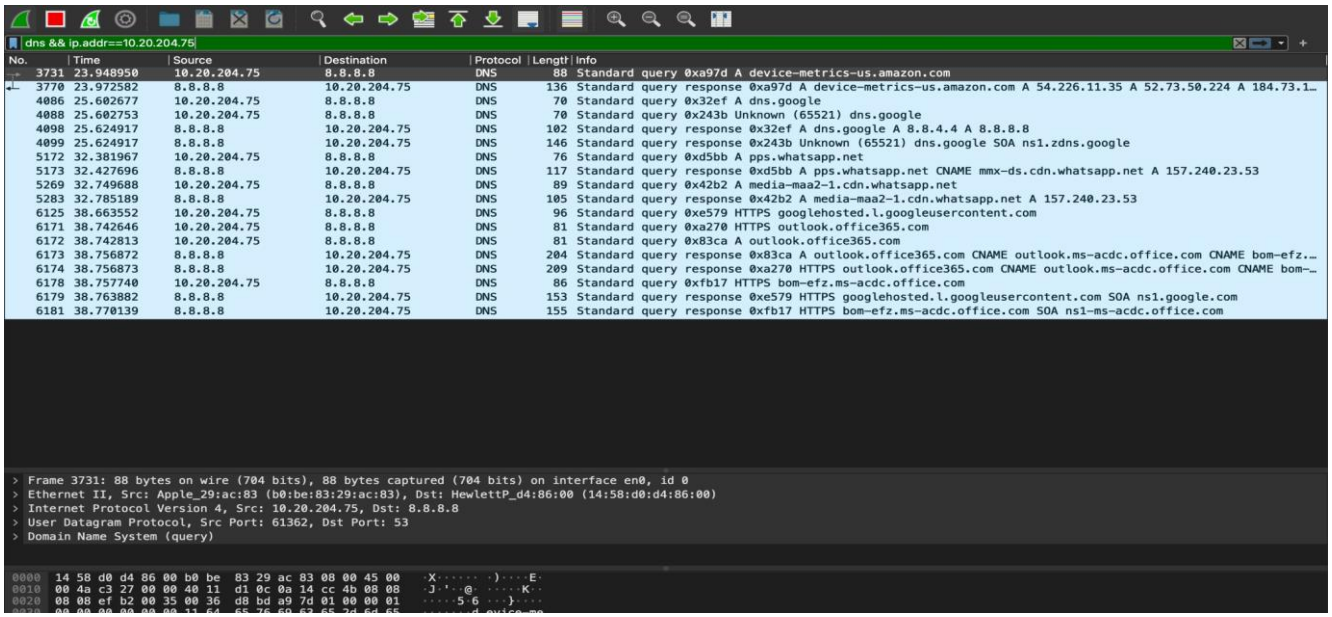
Lab 5 – Understanding Transport and Network Layer using Wireshark

NAME: VISHWAS M
SRN: PES2UG20CS390
DATE:6/04/22
SEC: F

Step 1: UDP and DNS

Procedures

1) Answer: So basically UDP headers contain source port, destination port, header length where all of these are of 2 bytes each. When there is a calculator with us we can calculate checksum.



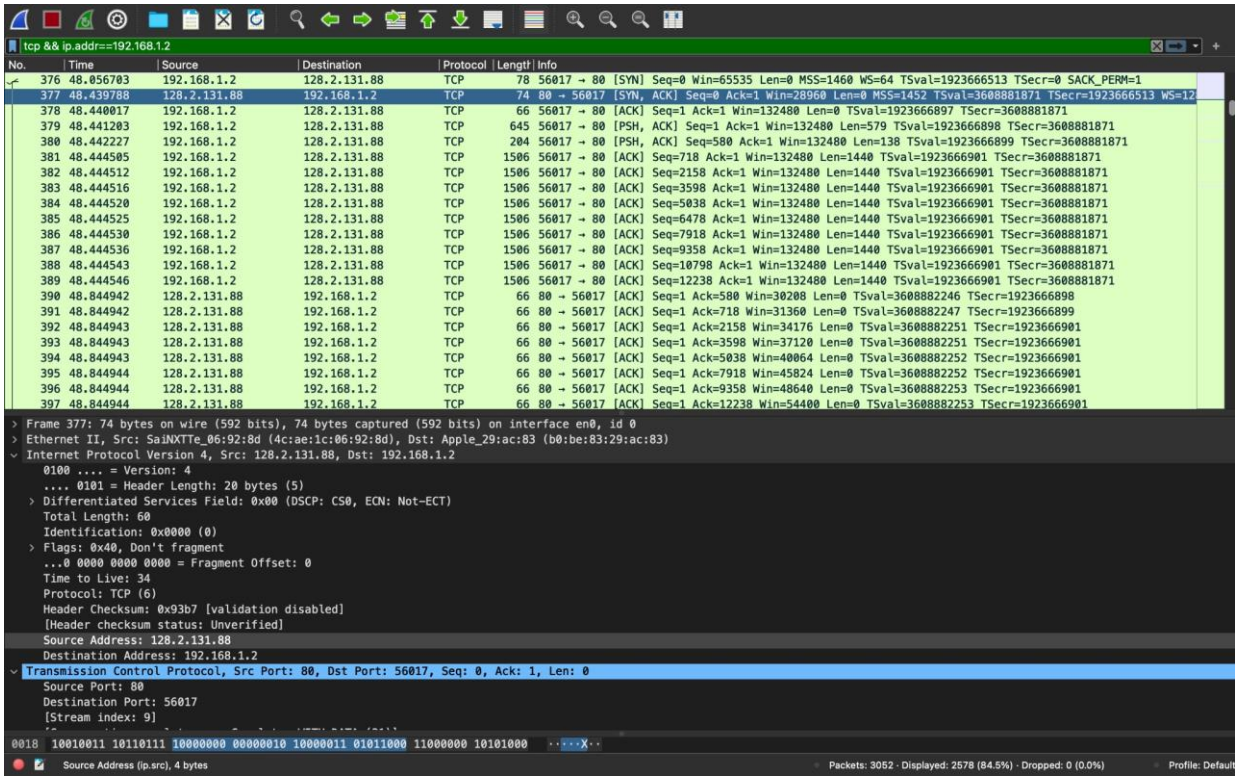
2)Answer: UDP checksum covers:

The reason is that Wireshark is very often used to capture the frames of the same pc that is running wireshark. This usually results in the checksums of the outgoing frames being incorrect since they are only calculated for transmission by the network card after they were already recorded by wireshark.TO avoid

constant “checksum error” messages it was decided to have the checksum disabled by default.

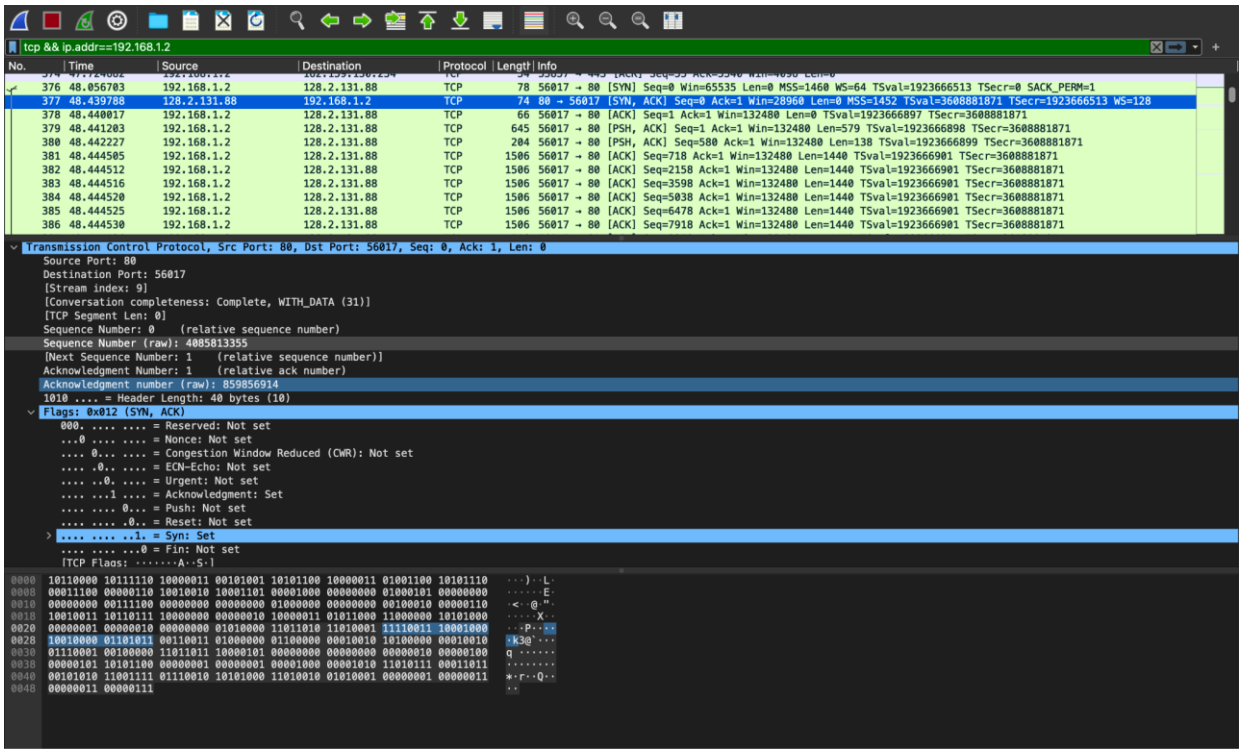
Step 2: TCP

1) IP Address of the client: 192.168.1.2
   Destination Port: :56017
   IP Address of the server : 128.2.131.88
   Source Port: 80



Step 2b: TCP Basics

1)



The sequence number of the SYN segment that is used to initiate the TCP connection is 0.
The SYN bit is set to 1 which indicates that it is a SYN segment.
Absolute sequence numbers can literally start from any random number. And it can continue to provide the successive sequence numbers in the upcoming segments.

2) Value of the sequence number sent by server : 0
Value of the Acknowledgement field in the server : 1
Server sends the next expecting sequence number as the acknowledgement number(here it is 1).And server determined the seq value as 0 because it should send the same sequence number that was sent by the client.
The SYN bit is set to 1 which indicates that it is a SYN segment.

3) Sequence number in HTTP POST : 1663589

4) TCP segment 1:0.24598567s
TCP segment 2:0.33768456s
TCP segment 3:0.25879578s
TCP segment 4:0.22564738s

5) minimum amount of buffer space is 1200 bytes
No lack of receiver buffer space ever throtle the server.

6) No retransmitted segments

7) 1460 bytes which is the MSS value.

8) throughput is 9.0675s.

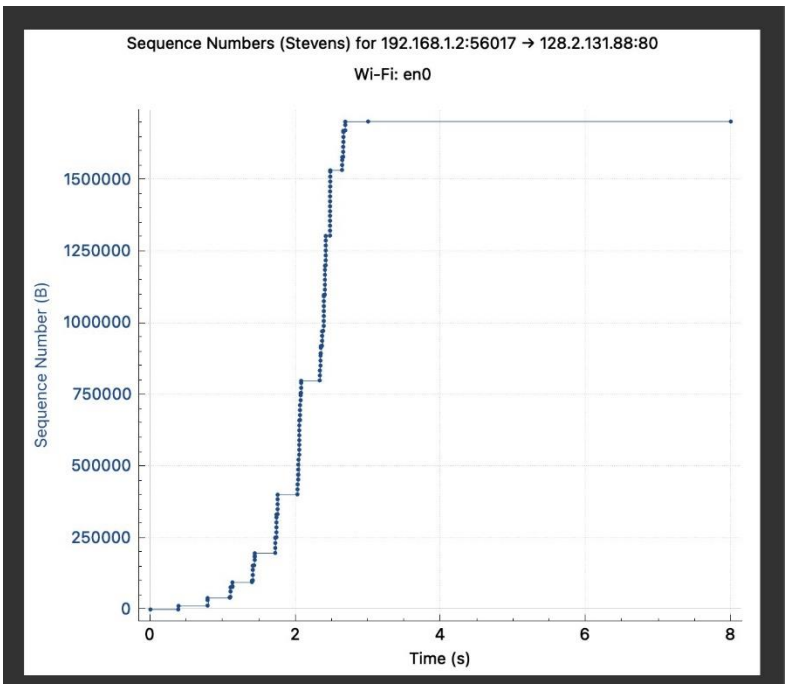
Step 2c: Statistics

1) Answer: second most common: 1280-2559
Second most common: 40-89
TCP packets less than 40 bytes are zero because rate(ms) is almost 0.
I got this answer in statistics->Packet Length.

2) Total packets:1747
Average throughput:1285.11bytes
I calculated this in statistics ->Packet length

3) Packets sent from local host:930
Remote host: 128.2.131.88
Packets sent from remote host:646

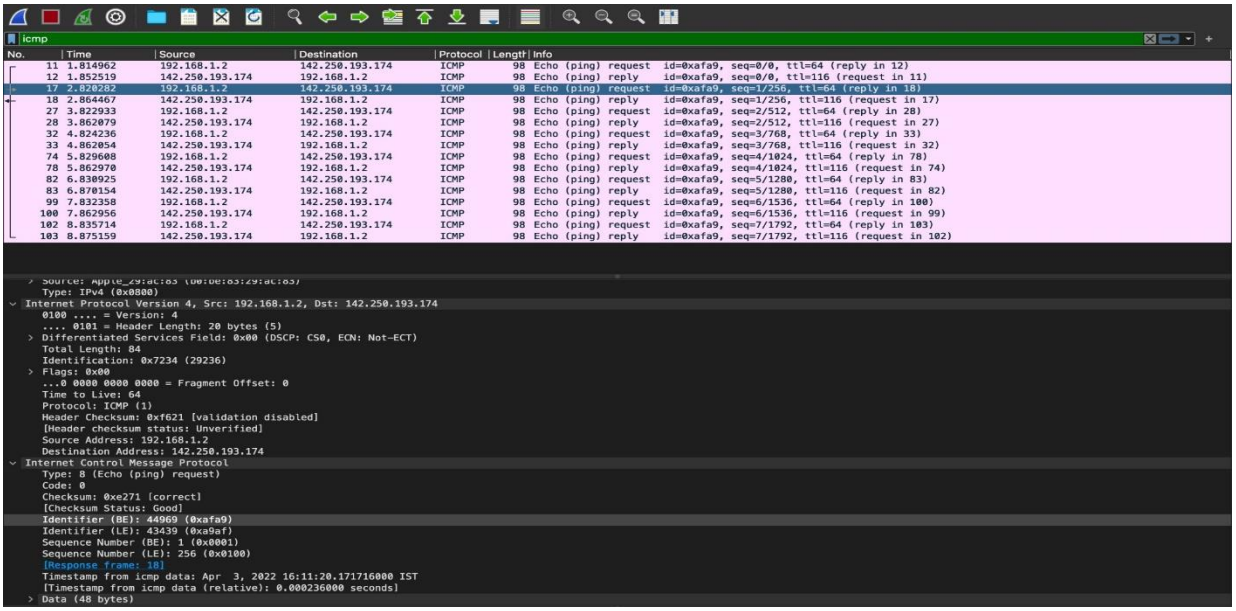
Step 3: Congestion Control



Step 4: The Network Layer

1) Yes, all the fields are matching and makes a perfect sense.
2) Fragment offset is 0.
3) TTL value will be 255 which is set by OS

Step 5: ICMP



1) Answers: Ping doesn't use a port number as traceroute uses port number 33434

For every hop port number increases by 1

2) Code:0

Type:0

Identifier:44969 (BE)

Identifier:43439 (LE)

Sequence number:1 (BE)

3) ICMP carry timestamps which actually makes it interesting.

4) We did it for ping