

Lab 5 – Understanding Transport and Network Layer using Wireshark

NAME: VISHWAS M

SRN: PES2UG20CS390

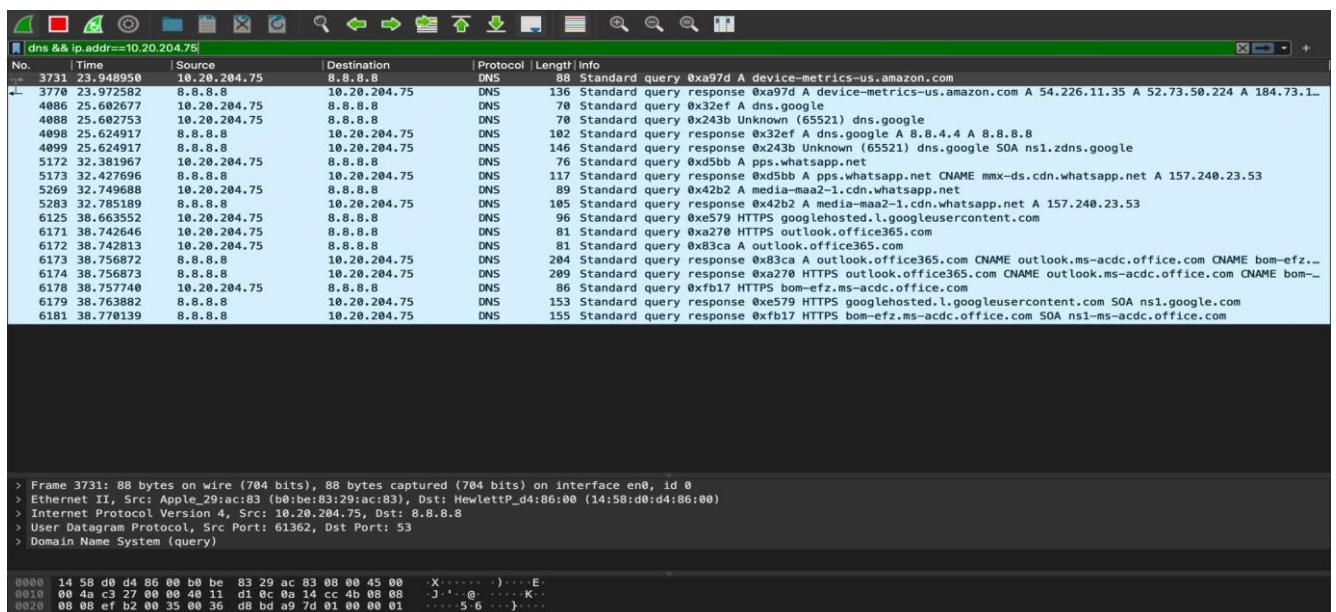
DATE:6/04/22

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.

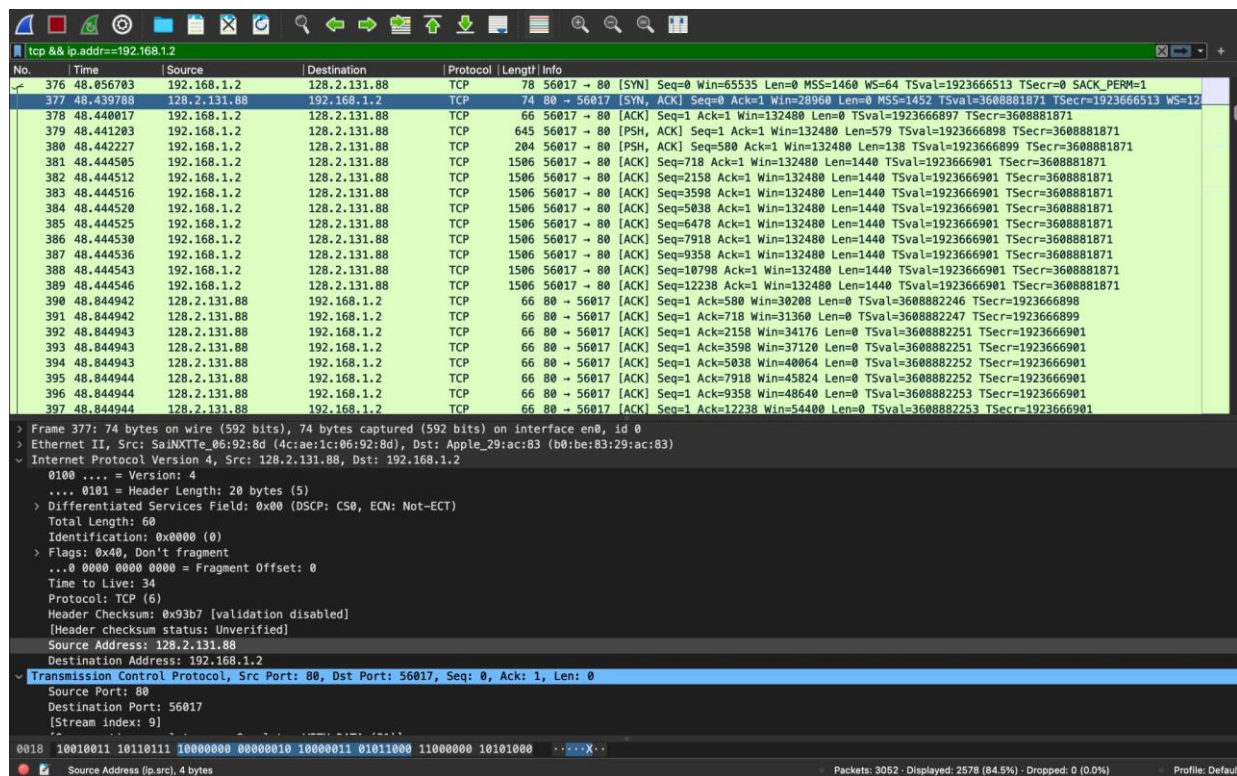
Step 2: TCP

1) IP Address of the client: 192.168.1.2

Destination Port: :56017

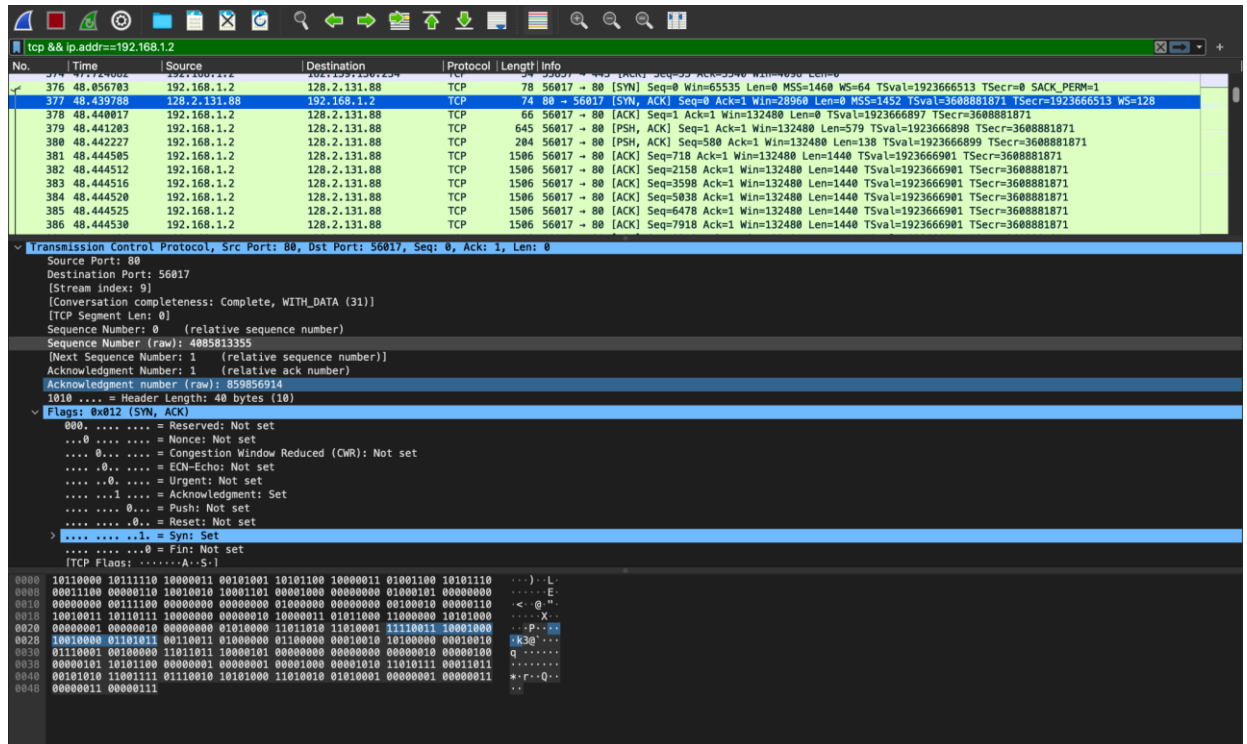
IP Address of the server : 128.2.131.88

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 throttle 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

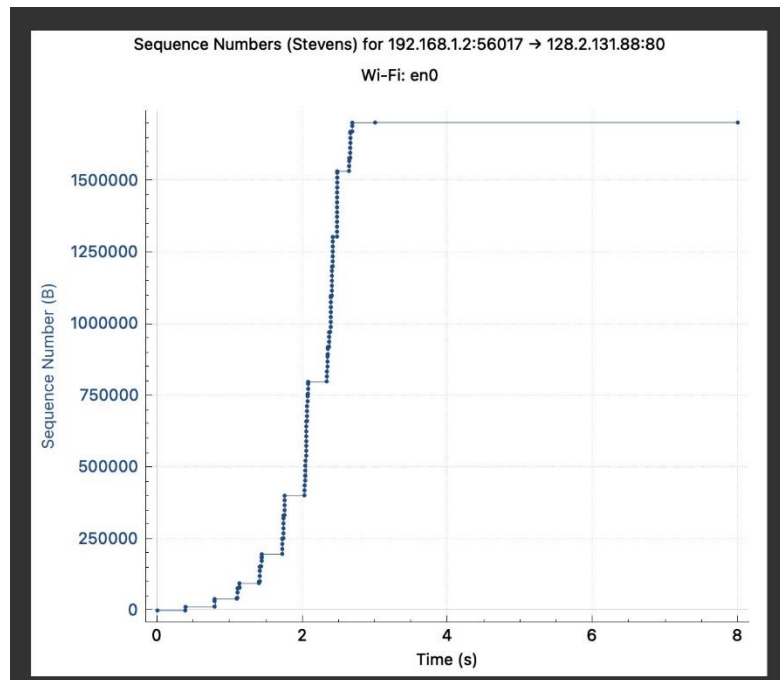
I calculated this in statistics ->Packet length

3) Packets sent from local host:930

Remote host: 128.2.131.88

Packets sent from remote host:646

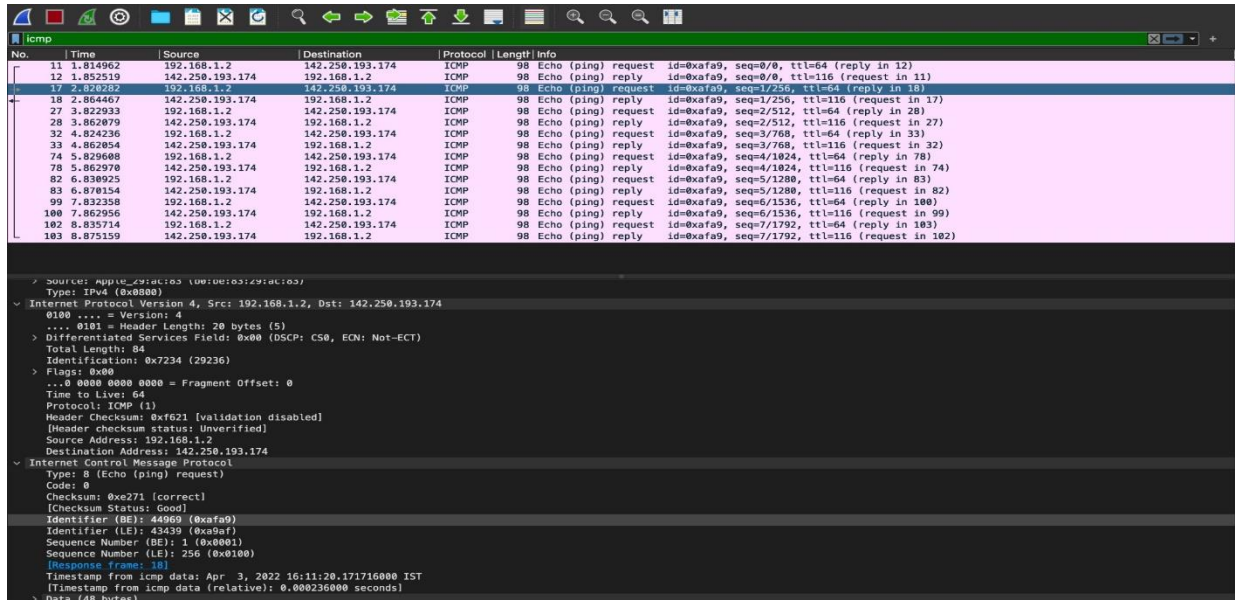
Step 3: Congestion Control



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



No.	Time	Source	Destination	Protocol	Length	Info
11	1.814962	192.168.1.2	142.250.193.174	ICMP	98	Echo (ping) request id=0xaf9, seq=0/0, ttl=64 (reply in 12)
12	1.852519	142.250.193.174	192.168.1.2	ICMP	98	Echo (ping) reply id=0xaf9, seq=0/0, ttl=116 (request in 11)
17	2.820282	192.168.1.2	142.250.193.174	ICMP	98	Echo (ping) request id=0xaf9, seq=1/256, ttl=64 (reply in 18)
18	2.864467	142.250.193.174	192.168.1.2	ICMP	98	Echo (ping) reply id=0xaf9, seq=1/256, ttl=116 (request in 17)
27	3.822933	192.168.1.2	142.250.193.174	ICMP	98	Echo (ping) request id=0xaf9, seq=2/512, ttl=64 (reply in 28)
28	3.862079	142.250.193.174	192.168.1.2	ICMP	98	Echo (ping) reply id=0xaf9, seq=2/512, ttl=116 (request in 27)
32	4.824236	192.168.1.2	142.250.193.174	ICMP	98	Echo (ping) request id=0xaf9, seq=3/768, ttl=64 (reply in 33)
33	4.862054	142.250.193.174	192.168.1.2	ICMP	98	Echo (ping) reply id=0xaf9, seq=3/768, ttl=116 (request in 32)
74	5.829608	192.168.1.2	142.250.193.174	ICMP	98	Echo (ping) request id=0xaf9, seq=4/1024, ttl=64 (reply in 78)
78	5.862970	142.250.193.174	192.168.1.2	ICMP	98	Echo (ping) reply id=0xaf9, seq=4/1024, ttl=116 (request in 74)
82	6.838925	192.168.1.2	142.250.193.174	ICMP	98	Echo (ping) request id=0xaf9, seq=5/1280, ttl=64 (reply in 83)
83	6.878154	142.250.193.174	192.168.1.2	ICMP	98	Echo (ping) reply id=0xaf9, seq=5/1280, ttl=116 (request in 82)
99	7.832358	192.168.1.2	142.250.193.174	ICMP	98	Echo (ping) request id=0xaf9, seq=6/1536, ttl=64 (reply in 100)
100	7.862956	142.250.193.174	192.168.1.2	ICMP	98	Echo (ping) reply id=0xaf9, seq=6/1536, ttl=116 (request in 99)
102	8.835714	192.168.1.2	142.250.193.174	ICMP	98	Echo (ping) request id=0xaf9, seq=7/1792, ttl=64 (reply in 103)
103	8.875159	142.250.193.174	192.168.1.2	ICMP	98	Echo (ping) reply id=0xaf9, seq=7/1792, ttl=116 (request in 102)

```
> Source: Apple_Library (00:0e:03:29:ac:03)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.2, Dst: 142.250.193.174
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x7234 (29236)
  > Flags: 0x00
    ... 0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0xf621 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.2
    Destination Address: 142.250.193.174
  > Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xe271 [correct]
    [Checksum Status: Good]
    Identifier (BE): 44969 (0xaf9)
    Identifier (LE): 43439 (0x9af)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Response frame: 10]
    Timestamp from icmp data: Apr  3, 2022 16:11:20.171716000 IST
    [Timestamp from icmp data (relative): 0.000236000 seconds]
  > Data (48 bytes)
```

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