

Week #5

Week 5 - Understanding Transport layer and Network Layer

SRN : PES2UG20CS237

Name : P K Navin Shrinivas

Section : D

Task 1 : UDP and DNS

- Opening wireshark and filtering for DNS and UDP signals specific to my ip address.
- Pinging www.pluralsight.com to generate DNS packets.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------------------------------|--------|---|----------|--------|------|
| 6 | 1.060... 10.1.10... 192.168... DNS | 1... | Standard query 0x2ffe A www.pluralsight.com OPT | | | UE2 |
| 7 | 1.060... 192.168... 10.1.10... DNS | 1... | Standard query response 0x2ffe Format error A www.pluralsight.com OPT | | | UE |

Filtered packets

```
navin@usermachine:~ » dig www.pluralsight.com

; <>> DiG 9.18.1 <>> www.pluralsight.com
;; global options: +cmd
;; Got answer:
;; →HEADER← opcode: QUERY, status: FORMERR, id: 12286
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: ba9a2fe3b83195f2 (echoed)
;; QUESTION SECTION:
;www.pluralsight.com.           IN      A

;; Query time: 0 msec
;; SERVER: 192.168.3.2#53(192.168.3.2) (UDP)
;; WHEN: Thu Mar 31 05:46:32 UTC 2022
;; MSG SIZE  rcvd: 60
```

dig command to generate UDP packets

- (Q) My predictions for UDP structure :

| | |
|-------------------------|--------------------------|
| 2 bytes for source port | 2 bytes for dest port |
| 2 bytes for length | 2 bytes for UDP checksum |
| X bytes for payload | X bytes of payload |

- (Q) And in wireshark : Hence concluding predictions were right!

```

    ↳ Internet Protocol Version 4, Src: 10.1.10.41, Dst: 192.168.3.2
    ↳ User Datagram Protocol, Src Port: 58300, Dst Port: 53
      Source Port: 58300
      Destination Port: 53
      Length: 68
      Checksum: 0xd829 [unverified]
        [Checksum Status: Unverified]
        [Stream index: 0]
    ↳ [Timestamps]
      UDP payload (60 bytes)
    ↳ Domain Name System (query)
  
```

UDP in Wireshark

- Why is the checksum “unverified” in wireshark UDP packets? It is because these UDP packets were generated by dig, iptrace or tcpdump will calculate these checksums and lead to “verified” status.

```

    ↳ User Datagram Protocol, Src Port: 58300, Dst Port: 53
      Source Port: 58300
      Destination Port: 53
      Length: 68
      Checksum: 0xd829 [unverified] [unverified]
        [Checksum Status: Unverified]
        [Stream index: 0]
    ↳ [Timestamps] Unverified Checksum in UDP
      UDP payload (60 bytes)
    ↳ Domain Name System (query)
  
```

Task 2 :TCP

- Download the file from
<http://www.gutenberg.org/ebooks/2383.txt.utf-8>
 - Open up wireshark and keep it prime to filter TCP packets from and to
<http://www.ini740.com/Lab2/lab2a.html>
 - Upload the files and stop wireshark, wireshark output :

| No. | Time | Source | Destination | Protocol | Length | Info |
|--------|------------|--------------|--------------|----------|--------|--------------------------------|
| → 2... | 101.299... | 10.1.10.41 | 128.2.131.88 | HTTP | 473 | POST /Lab2/lab2b.html HTTP/1.1 |
| ← 2... | 103.281... | 128.2.131.88 | 10.1.10.41 | HTTP | 991 | HTTP/1.1 200 OK (text/html) |

- (Q) What is the source/dest ip address and source port? IP :

```
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0xdd5e [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.1.10.41
Destination Address: 128.2.131.88
Transmission Control Protocol, Src Port: 36102, Dst Port: 80, Seq: 0, Len: 0
Source Port: 36102
Destination Port: 80
[Stream index: 8]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 0]
Sequence Number: 0      (relative sequence number)
Sequence Number (raw): 2906858569
```

- Point of this task is to observe TCP packets, hence filter for them :

Task 2b : TCP Basics

- (Q14) Sequence number of SYN packets are 0, SYN segments can be identified using the TCP flag segments. Yes wireshark can display absolute seq numbers by :

edit->preference->protocols->tcp->untick
relative
numbering.

```
1010 .... = Header Length: 40 bytes (10)
Flags: 0x002 (SYN)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.... = ECN-Echo: Not set
    .... ..0.... = Urgent: Not set
    .... .0.... = Acknowledgment: Not set
    .... 0... = Push: Not set
    .... .0... = Reset: Not set
    .... .... .1. = Syn: Set
    .... .... .0 = Fin: Not set
[TCP Flags: .....S..]
Window: 64240
[Calculated window size: 642401
```

SYN Identification

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------|--------------|---------------|----------|--------|---|
| 224 | 94.7031... | 10.1.10.41 | 54.68.82.156 | TCP | 56 | 39644 - 443 [ACK] Seq=2854338923 Ack=3373276650 Win=501 Len=0 |
| 229 | 94.7031... | 10.1.10.41 | 108.159.15... | TCP | 56 | 39644 - 443 [ACK] Seq=2931889710 Ack=2650907141 Win=501 Len=0 |
| 230 | 94.7031... | 10.1.10.41 | 108.159.15... | TCP | 56 | 39644 - 443 [TCP Dup ACK 2049] [TCP ACKed unseen segment] 443 [ACK] Seq=2650907141 Ack=2531889711 Win=245 Len=0 |
| 231 | 97.7036... | 54.68.82.156 | 10.1.10.41 | TLS | 123 | Application Data |
| 232 | 97.7037... | 10.1.10.41 | 54.68.82.156 | TCP | 56 | 39644 - 443 [ACK] Seq=2854338923 Ack=3373276717 Win=501 Len=0 |
| 235 | 100.732... | 54.68.82.156 | 10.1.10.41 | TLS | 123 | Application Data |
| 236 | 100.732... | 10.1.10.41 | 54.68.82.156 | TCP | 56 | 39644 - 443 [ACK] Seq=29068687330 Ack=3791606914 TSecr=0 TSval=3791606914 TSerr=0 WS=128 |
| 241 | 101.116... | 10.1.10.41 | 128.2.131.88 | TCP | 76 | 36102 - 80 [SYN] Seq=44689999 Win=64256 Len=0 |
| 242 | 101.117... | 128.2.131.88 | 10.1.10.41 | TCP | 15 | 36102 - 80 [ACK] Seq=44689999 Win=64256 Len=0 MSS=1460 SACK_PERM=1 WS=128 |
| 243 | 101.117... | 10.1.10.41 | 128.2.131.88 | TCP | 56 | 36102 - 80 [ACK] Seq=2906858570 Win=92256 Len=0 |
| 245 | 101.117... | 10.1.10.41 | 128.2.131.88 | TCP | 15 | 36102 - 80 [ACK] Seq=2906858570 Ack=43468894 Win=64256 Len=1460 [TCP segment of a reassembled PDU] |
| 246 | 101.117... | 10.1.10.41 | 128.2.131.88 | TCP | 15 | 36102 - 80 [ACK] Seq=2906860030 Ack=43468894 Win=64256 Len=1460 [TCP segment of a reassembled PDU] |
| 247 | 101.117... | 10.1.10.41 | 128.2.131.88 | TCP | 15 | 36102 - 80 [ACK] Seq=2906861490 Ack=43468894 Win=64256 Len=1460 [TCP segment of a reassembled PDU] |
| 248 | 101.117... | 10.1.10.41 | 128.2.131.88 | TCP | 15 | 36102 - 80 [ACK] Seq=2906862490 Ack=43468894 Win=64256 Len=1460 [TCP segment of a reassembled PDU] |
| 249 | 101.117... | 10.1.10.41 | 128.2.131.88 | TCP | 15 | 36102 - 80 [ACK] Seq=2906863414 Ack=43468894 Win=64256 Len=1460 [TCP segment of a reassembled PDU] |
| 250 | 101.117... | 10.1.10.41 | 128.2.131.88 | TCP | 15 | 36102 - 80 [ACK] Seq=2906867330 Ack=43468894 Win=64256 Len=1460 [TCP segment of a reassembled PDU] |
| 251 | 101.117... | 10.1.10.41 | 128.2.131.88 | TCP | 15 | 36102 - 80 [ACK] Seq=2906868790 Ack=43468894 Win=64256 Len=1460 [TCP segment of a reassembled PDU] |
| 252 | 101.117... | 10.1.10.41 | 128.2.131.88 | TCP | 15 | 36102 - 80 [ACK] Seq=2906868790 Ack=43468894 Win=64256 Len=1460 [TCP segment of a reassembled PDU] |

Relative TCP seq numbering

- (Q15) SYNACK has a relative sequence number of 1, ACK number of SYNACK packets is 1, this is because the server is asking for the best bit waiting for the three way handshake. The Flag field in TCP packets shows it is a SYNACK packet:

```
1000.... = Header Length: 32 bytes (8)
Flags: 0x012 (SYN, ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.... = ECN-Echo: Not set
    .... ..0.... = Urgent: Not set
    .... .1.... = Acknowledgment: Set
    .... 0... = Push: Not set
    .... .0... = Reset: Not set
    .... .... .1. = Syn: Set
    .... .... .0 = Fin: Not set
```

- (Q16) TCP SEQ number (relative) of HTTP post is : 1702361, this I feel is the entirty of uploaded content and remaining payload (1702278) are for headers.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------|----------|--------------|--------------|--------|------------------------------------|
| | | 101.2... | 10.1.10.41 | 128.2.131... | HTTP | 473 POST /Lab2/lab2b.html HTTP/1.1 |
| | | 103.2... | 128.2.131... | 10.1.10.41 | HTTP | 991 HTTP/1.1 200 OK (text/html) |

```

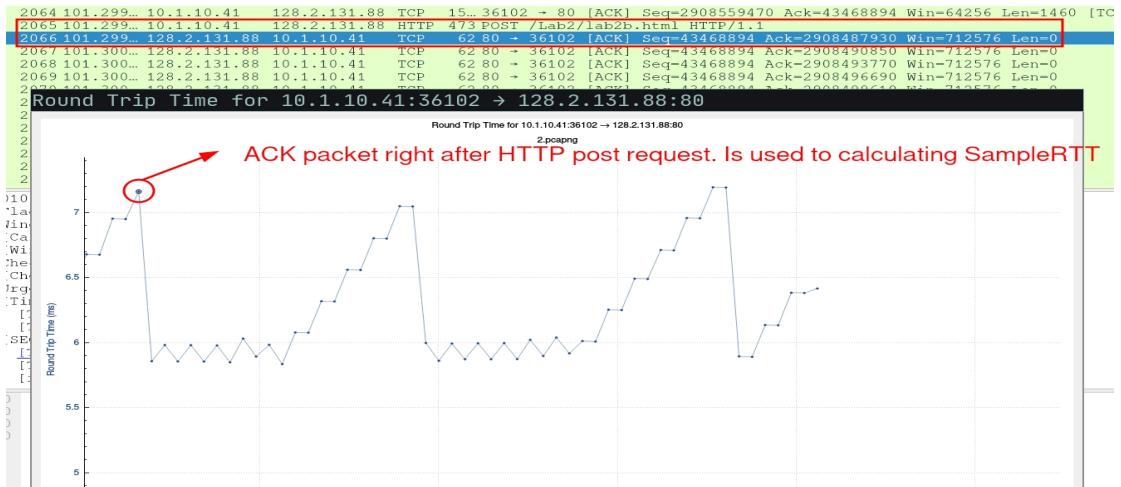
> Frame 2065: 473 bytes on wire (3784 bits), 473 bytes captured (3784 bits) on interface any, i
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 10.1.10.41, Dst: 128.2.131.88
- Transmission Control Protocol, Src Port: 36102, Dst Port: 80, Seq: 1702361, Ack: 1, Len: 417
  Source Port: 36102
  Destination Port: 80
  [Stream index: 8]
  [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 417]
  Sequence Number: 1702361 (relative sequence number)
  Sequence Number (raw): 2908560930
  [Next Sequence Number: 1702778 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 43468894
  0101 .... = Header Length: 20 bytes (5)
  - Flags: 0x018 (PSH, ACK)
    000. .... = Reserved: Not set
      0 = None... = Not set

```

- (Q17) Sample RTT is simply the time taken to ACK a given segment, but to get smoother EstimatedRTT we take many samples from recent packets :

| | A | B | C | D |
|---|--------------------|-------------------|----------------------|----------------|
| 1 RTT From 11 packets after HTTP POST request | | | | |
| 2 | Relative SEQ # | Response to SEQ # | RTT as per Wireshark | EstimatedRTT |
| 3 | 2066 | 1992 | 0.005857519 | 0.005857519 |
| 4 | 2067 | 1995 | 0.005854865 | 0.00585718725 |
| 5 | 2068 | 1998 | 0.005853887 | 0.005856774719 |
| 6 | 2069 | 2001 | 0.005848369 | 0.005855724004 |
| 7 | 2070 | 2004 | 0.005892719 | 0.005860348378 |
| 8 | 2071 | 2007 | 0.005834262 | 0.005857087581 |
| 9 | 2072 | 2009 | 0.006075354 | 0.005884370883 |
| 10 | 2073 | 2011 | 0.006315608 | 0.005938275523 |
| 11 | 2074 | 2013 | 0.006557328 | 0.006015657083 |
| 12 | 2075 | 2015 | 0.006799189 | 0.006113598572 |
| 13 | 2076 | 2017 | 0.007047824 | 0.006230376751 |
| 14 | SUM of 11 RTT's: | | 0.067936924 | 0.06532691974 |
| 15 | Average/SampleRTT: | | 0.005643582273 | 0.005938810886 |

[Source](#)



Now calculating the EstimatedRTT (In Table):

$$\text{EstimatedRTT} = (1 - \alpha) * \text{EstimatedRTT} + \alpha * \text{SampleRTT}$$

- Exponential weighted moving average
- influence of past sample decreases exponentially fast
- typical value: $\alpha = 0.125$

- (Q18) The window size on packets from A to B indicate how much buffer space is available on A for receiving packets. So when B receives a packet with window size 1, it would tell B how many bytes it is allowed to send to A. Hence looking at the window sizes here on responses (ACK). We also see the windows are scaled with a factor of 128. Lowest observed window size : 32128

| | | | | |
|-----------------------------|--------------|--------|-----------------------------|-----------------------------|
| 232 97.7037... 10.1.10.41 | 54.68.82.156 | TCP | 56 39644 → 443 [ACK] | Seq=2854338923 Ack=3373; |
| 235 100.732... 54.68.82.156 | 10.1.10.41 | TLS... | 123 Application Data | |
| 236 100.732... 10.1.10.41 | 54.68.82.156 | TCP | 15... 36102 → 80 [ACK] | Seq=2854338923 Ack=3373; |
| 241 101.117... 10.1.10.41 | 128.2.131.88 | TCP | 76 36102 → 80 [SYN] | Seq=2906858569 Win=64240 |
| 242 101.117... 128.2.131.88 | 10.1.10.41 | TCP | 68 80 → 36102 [SYN, ACK] | Seq=43468893 Ack=2906858570 |
| 243 101.117... 10.1.10.41 | 128.2.131.88 | TCP | 56 36102 → 80 [ACK] | Ack=43468893 |
| 245 101.117... 10.1.10.41 | 128.2.131.88 | TCP | 15... 36102 → 80 [ACK] | Seq=2906858570 Ack=43468893 |
| 246 101.117... 10.1.10.41 | 128.2.131.88 | TCP | 15... 36102 → 80 [ACK] | Seq=2906860030 Ack=43468893 |
| 247 101.117... 10.1.10.41 | 128.2.131.88 | TCP | 15... 36102 → 80 [ACK] | Seq=2906861490 Ack=43468893 |
| 248 101.117... 10.1.10.41 | 128.2.131.88 | TCP | 15... 36102 → 80 [ACK] | Seq=2906862950 Ack=43468893 |
| 249 101.117... 10.1.10.41 | 128.2.131.88 | TCP | 15... 36102 → 80 [PSH, ACK] | Seq=2906864410 Ack=43468893 |
| 250 101.117... 10.1.10.41 | 128.2.131.88 | TCP | 15... 36102 → 80 [ACK] | Seq=2906865870 Ack=43468893 |
| 251 101.117... 10.1.10.41 | 128.2.131.88 | TCP | 15... 36102 → 80 [ACK] | Seq=2906867330 Ack=43468893 |
| 252 101.117... 10.1.10.41 | 128.2.131.88 | TCP | 15... 36102 → 80 [ACK] | Seq=2906868790 Ack=43468893 |
| 253 101.117... 10.1.10.41 | 128.2.131.88 | TCP | 15... 36102 → 80 [ACK] | Seq=2906870250 Ack=43468893 |
| 254 101.117... 10.1.10.41 | 128.2.131.88 | TCP | 15... 36102 → 80 [PSH, ACK] | Seq=2906871710 Ack=43468893 |
| 255 101.118... 128.2.131.88 | 10.1.10.41 | TCP | 62 80 → 36102 [ACK] | Seq=43468894 Ack=2906860 |
| 256 101.118... 10.1.10.41 | 128.2.131.88 | TCP | 15... 36102 → 80 [ACK] | Seq=2906873170 Ack=43468894 |

[Stream index: 8]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 0]
Sequence Number: 43468894
[Next Sequence Number: 43468894]
Acknowledgment Number: 2906860030
0101 ... Header Length: 20 bytes (5)
Flags: 0x0100 (ACK)
Window: 251
[Calculated window size: 32128]
[Window size scaling factor: 128]
Checksum: 0xe7c7 [unverified]

- (Q19) No, there are no retransmitted packets, I checked for these by filtering them using : `tcp.analysis.retransmission` :

| tcp.analysis.retransmission | | | | | | |
|-----------------------------|------|--------|-------------|----------|--------|------|
| No. | Time | Source | Destination | Protocol | Length | Info |
| | | | | | | |

- (Q20) Comparing Sequence number of 2 consecutive ACK's will give us the answer we need, I am comparing these two :

| | |
|---|---|
| 423 101.171... 128.2.131.88 10.1.10.41 TCP 62 80 → 36102 [ACK] | 423 101.171... 128.2.131.88 10.1.10.41 TCP 62 80 → 36102 [ACK] |
| 424 101.172... 128.2.131.88 10.1.10.41 TCP 62 80 → 36102 [ACK] | 424 101.172... 128.2.131.88 10.1.10.41 TCP 62 80 → 36102 [ACK] |
| 425 101.172... 128.2.131.88 10.1.10.41 TCP 62 80 → 36102 [ACK] | 425 101.172... 128.2.131.88 10.1.10.41 TCP 62 80 → 36102 [ACK] |
| 426 101.172... 128.2.131.88 10.1.10.41 TCP 62 80 → 36102 [ACK] | 426 101.172... 128.2.131.88 10.1.10.41 TCP 62 80 → 36102 [ACK] |
| 427 101.172... 10.1.10.41 128.2.131.88 TCP 15... 36102 → 80 [ACK] | 427 101.172... 10.1.10.41 128.2.131.88 TCP 15... 36102 → 80 [ACK] |
| 428 101.172... 10.1.10.41 128.2.131.88 TCP 15... 36102 → 80 [ACK] | 428 101.172... 10.1.10.41 128.2.131.88 TCP 15... 36102 → 80 [ACK] |

| | |
|--|--|
| [Conversation completeness: Incomplete, DATA (15)] | [Conversation completeness: Incomplete, DATA (15)] |
| [TCP Segment Len: 0] | [TCP Segment Len: 0] |
| Sequence Number: 43468894 | Sequence Number: 43468894 |
| [Next Sequence Number: 43468894] | [Next Sequence Number: 43468894] |
| Acknowledgment Number: 2907016250 | Acknowledgment Number: 2907017710 |
| 0101 = Header Length: 20 bytes (5) | 0101 = Header Length: 20 bytes (5) |
| Flags: 0x010 (ACK) | Flags: 0x010 (ACK) |
| Window: 1232 | Window: 1255 |
| [Calculated window size: 157696] | [Calculated window size: 160640] |
| [Window size scaling factor: 128] | [Window size scaling factor: 128] |
| Checksum: 0x81b4 [unverified] | Checksum: 0x7be9 [unverified] |
| [Checksum Status: Unverified] | [Checksum Status: Unverified] |
| Urgent Pointer: 0 | Urgent Pointer: 0 |
| ‣ [Timestamps] | ‣ [Timestamps] |
| ‣ [SEQ/ACK analysis] | ‣ [SEQ/ACK analysis] |

Subtracting the two sequence number gives us : 1460, this the amount of bytes ACK'ed in each ACK response. Also, here we can see where the server is ACK'ing every other packet :

| | | |
|---------------------------------------|-----|------------------------|
| 358 101.124.. 128.2.131.88 10.1.10.41 | TCP | 62 80 → 36102 [ACK] |
| 359 101.124.. 128.2.131.88 10.1.10.41 | TCP | 62 80 → 36102 [ACK] |
| 360 101.124.. 10.1.10.41 128.2.131.88 | TCP | 15... 36102 → 80 [ACK] |
| 361 101.124.. 128.2.131.88 10.1.10.41 | TCP | 62 80 → 36102 [ACK] |
| 362 101.124.. 10.1.10.41 128.2.131.88 | TCP | 15... 36102 → 80 [ACK] |
| 363 101.124.. 128.2.131.88 10.1.10.41 | TCP | 62 80 → 36102 [ACK] |
| 364 101.124.. 10.1.10.41 128.2.131.88 | TCP | 15... 36102 → 80 [ACK] |
| 365 101.124.. 10.1.10.41 128.2.131.88 | TCP | 15... 36102 → 80 [ACK] |
| 366 101.124.. 128.2.131.88 10.1.10.41 | TCP | 62 80 → 36102 [ACK] |
| 367 101.125.. 10.1.10.41 128.2.131.88 | TCP | 15... 36102 → 80 [ACK] |
| 368 101.125.. 10.1.10.41 128.2.131.88 | TCP | 15... 36102 → 80 [ACK] |
| 369 101.125.. 10.1.10.41 128.2.131.88 | TCP | 15... 36102 → 80 [ACK] |
| 370 101.125.. 10.1.10.41 128.2.131.88 | TCP | 15... 36102 → 80 [ACK] |
| 371 101.125.. 10.1.10.41 128.2.131.88 | TCP | 15... 36102 → 80 [PSH, |

[Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 0]

Sequence Number: 43468894

[Next Sequence Number: 43468894]

Acknowledgment Number: 2906930110

0101 = Header Length: 20 bytes (5)

‣ Flags: 0x010 (ACK)

Window: 1119

[Calculated window size: 143232]

[Window size scaling factor: 128]

Checksum: 0xd2a2 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

‣ [Timestamps]

‣ [SEQ/ACK analysis]

- (Q21) The HTTP response has a “time since request” value of 1.98 seconds, the HTTP POST has a content size of 1702219 bytes. This gives us a throughput of : ~840KB/second

Task 2c : Statistics

- (Q22) The most common packet length is 1280-2559 :

| Topic / Item | Count | Average | Min Val | Max Val | Rate (ms) | Percent | Burst Rate | Burst Start |
|------------------|-------------|----------------|-------------|-------------|---------------|---------------|---------------|----------------|
| Packet Lengths | 2111 | 867.26 | 44 | 1516 | 0.0202 | 100% | 12.9800 | 101.171 |
| 0-19 | 0 | - | - | - | 0.0000 | 0.00% | - | - |
| 20-39 | 0 | - | - | - | 0.0000 | 0.00% | - | - |
| 40-79 | 880 | 61.68 | 44 | 78 | 0.0084 | 41.69% | 4.8300 | 101.171 |
| 80-159 | 60 | 111.75 | 80 | 159 | 0.0006 | 2.84% | 0.0400 | 46.801 |
| 160-319 | 3 | 224.33 | 183 | 245 | 0.0000 | 0.14% | 0.0100 | 89.279 |
| 320-639 | 1 | 473.00 | 473 | 473 | 0.0000 | 0.05% | 0.0100 | 101.300 |
| 640-1279 | 1 | 991.00 | 991 | 991 | 0.0000 | 0.05% | 0.0100 | 103.282 |
| 1280-2559 | 1166 | 1516.00 | 1516 | 1516 | 0.0112 | 55.23% | 8.1700 | 101.186 |
| 2560-5119 | 0 | - | - | - | 0.0000 | 0.00% | - | - |
| 5120 and greater | 0 | - | - | - | 0.0000 | 0.00% | - | - |

- (Q23) Throughput and other statistics :

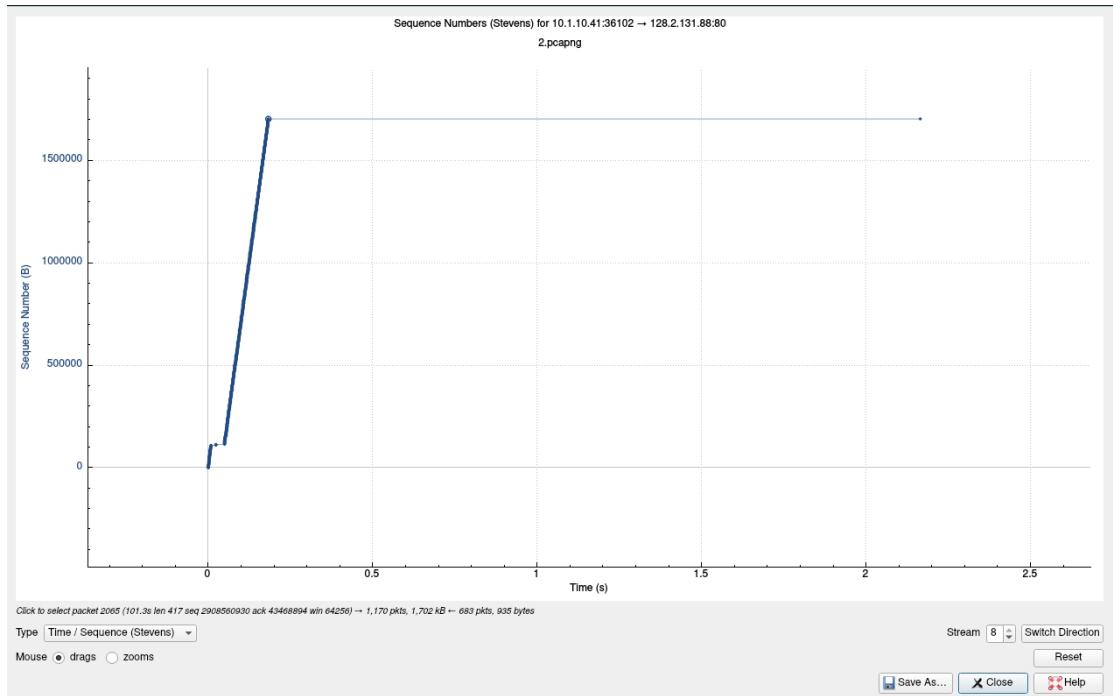
| Measurement | Captured | Displayed | Marked |
|------------------------|----------|------------------|--------|
| Packets | 2111 | 2111 (100.0%) | - |
| Time span, s | 104.257 | 104.257 | - |
| Average pps | 20.2 | 20.2 | - |
| Average packet size, B | 867 | 867 | - |
| Bytes | 1830780 | 1830780 (100.0%) | 0 |
| Average bytes/s | 17 k | 17 k | - |
| Average bits/s | 140 k | 140 k | - |

- (Q24) Details about conversation between hosts is as follows :

| Ethernet | IPv4 · 12 | IPv6 · 1 | TCP · 9 | UDP · 6 | Address A | Address B | Packets | Bytes | Packets A → B | Bytes A → B | Packets B → A | Bytes B → A | Rel Start | Duration | Bits/s A → B | Bits/s B → A |
|--------------|-----------------|----------|---------|---------|-----------|-----------|---------|-------|---------------|-------------|---------------|-------------|-----------|----------|--------------|--------------|
| 10.1.10.21 | 10.1.10.255 | | 4 | 527 | 4 | 527 | 0 | 0 | 73.851272 | 29.8901 | | | 0 | 141 | | |
| 10.1.10.29 | 10.1.10.255 | | 1 | 245 | 1 | 245 | 0 | 0 | 89.279014 | 0.0000 | | | 0 | 1 | | |
| 10.1.10.41 | 192.168.254.1 | | 5 | 298 | 2 | 112 | 3 | 186 | 0.000000 | 0.5316 | | | 186 | 1,685 | | |
| 10.1.10.41 | 108.159.15.119 | | 24 | 1,434 | 13 | 752 | 11 | 682 | 6.613564 | 95.1916 | | | 682 | 63 | | |
| 10.1.10.41 | 142.250.195.65 | | 4 | 308 | 2 | 151 | 2 | 157 | 46.801058 | 0.0365 | | | 157 | 33 k | | |
| 10.1.10.41 | 142.250.196.34 | | 4 | 308 | 2 | 151 | 2 | 157 | 46.801304 | 0.0309 | | | 157 | 39 k | | |
| 10.1.10.41 | 142.250.193.164 | | 4 | 308 | 2 | 151 | 2 | 157 | 47.801961 | 0.0981 | | | 157 | 12 k | | |
| 10.1.10.41 | 34.120.115.102 | | 4 | 308 | 2 | 151 | 2 | 157 | 49.803385 | 0.1036 | | | 157 | 11 k | | |
| 10.1.10.41 | 34.120.208.123 | | 4 | 322 | 2 | 158 | 2 | 164 | 50.803972 | 0.0561 | | | 164 | 22 k | | |
| 10.1.10.41 | 192.168.3.2 | | 10 | 997 | 5 | 384 | 5 | 613 | 101.116150 | 2.2203 | | | 613 | 1,383 | | |
| 10.1.10.41 | 128.2.131.88 | | 1,853 | 1,811 k | 1,170 | 1,768 k | 683 | 43 k | 101.116860 | 2.1651 | | | 43 k | 6,533 k | | |
| 54.68.82.156 | 10.1.10.41 | | 70 | 6,265 | 35 | 4,305 | 35 | 1,960 | 1.701126 | 101.9966 | | | 1,960 | 337 | | |

Task 3 : Congestion Control

- (Q25 and Q26) The observed graph using wiresharks TCP graphs is :



Task 4 : Network layer

- The DNS query was made with www.pluralsight.com as the Domain name. These were the observed query packets in wireshark

| | | | | |
|---------------|----------------|----------------|--------|---|
| 6 1.06045... | 10.1.10.41 | 192.168.3.2 | DNS | 104 Standard query 0x2ffe A www.pluralsight.com OPT |
| 7 1.06095... | 192.168.3.2 | 10.1.10.41 | DNS | 104 Standard query response 0x2ffe Format error A www.pluralsight.com OPT |
| 8 2.04525... | 10.1.10.41 | 142.250.196... | TLS... | 95 Application Data |
| 9 2.04575... | 142.250.196... | 10.1.10.41 | TCP | 62 443 + 46670 [ACK] Seq=2344398112 Ack=530350761 Win=254 Len=0 |
| 10 2.08803... | 142.250.196... | 10.1.10.41 | TLS... | 95 Application Data |
| 11 2.13140... | 10.1.10.41 | 142.250.196... | TCP | 56 46670 + 443 [ACK] Seq=530350761 Ack=2344398151 Win=501 Len=0 |
| 12 3.00605... | 10.1.10.29 | 10.1.10.255 | NBNS | 94 Name query NB LAPTOP-0EJNE4JS<1c> |
| 13 3.04600... | 10.1.10.41 | 142.250.193... | TLS... | 95 Application Data |
| 14 3.04629... | 142.250.193... | 10.1.10.41 | TCP | 62 443 + 44352 [ACK] Seq=1530572871 Ack=879007816 Win=352 Len=0 |

| |
|---|
| > Frame 6: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface any, id 0 |
| > Linux cooked capture v1 |
| > Internet Protocol Version 4, Src: 10.1.10.41, Dst: 192.168.3.2 |
| > User Datagram Protocol, Src Port: 58300, Dst Port: 53 |
| > Domain Name System (query) |
| > Transaction ID: 0x2ffe |
| > Flags: 0x0120 Standard query |
| > Questions: 1 |
| > Answer RRs: 0 |
| > Authority RRs: 0 |
| > Additional RRs: 1 |
| > Queries |
| > Additional records |
| [Response In: ?] |
| 0000 00 04 00 01 00 06 bc e9 2f 8c 1c 4e 00 00 08 00 / . N . . . |
| 0010 45 00 00 58 d5 01 00 00 40 11 cd bf 0a 01 0a 29 E . X . . . @ . D . . . |
| 0020 c0 a8 03 02 e3 bc 00 35 00 44 d8 29 2f fe 01 20 5 . D . / . . |
| 0030 00 01 00 00 00 00 00 01 03 77 77 77 0b 70 6c 75 www.piu |
| 0040 72 61 6c 73 69 67 68 74 03 63 6f 6d 00 00 01 00 ralsight .com . . . |
| 0050 01 00 00 29 d4 00 00 00 00 00 00 0c 00 0a 00 08 |
| 0060 ba 9a 2f e3 b8 31 95 f2 |

- (Q28 and Q29) All the needed fields do match up
- (Q31) TTL is set as 64, my OS being arch derivative of linux running on linux 5.16.

Task 5 : ICMP

- Starting a new capture when simultaneously pinging : <http://www.cmuj.jp/> using the traceroute utility :

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|---------------|--------------|---------------|----------|--|------|
| 1 | 2.0.80266... | 192.168.1.11 | 192.168.1.10 | TCP | 76 55134 - 6443 [SYN] Seq=4032343836 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2797866597 | |
| 2 | 3.0.80272... | 192.168.1.10 | 192.168.1.11 | TCP | 56 6443 - 55134 [RST, ACK] Seq=0 Ack=4032343837 Win=0 Len=0 | |
| 3 | 4.0.86749... | 192.168.1.10 | 192.168.1.1 | DNS | 73 Standard query 0x9a09 A www.cmuj.jp | |
| 4 | 5.0.86752... | 192.168.1.10 | 192.168.1.1 | DNS | 73 Standard query 0x383e AAAA www.cmuj.jp | |
| 5 | 6.1.19670... | 192.168.1.1 | 192.168.1.10 | DNS | 103 Standard query response 0x9a09 A www.cmuj.jp CNAME cmuj.jp A 122.17.163.205 | |
| 6 | 7.1.19693... | 192.168.1.1 | 192.168.1.10 | DNS | 161 Standard query response 0x383e AAAA www.cmuj.jp CNAME cmuj.jp SOA mwns1.customer.ne.jp | |
| 7 | 8.1.19707... | 192.168.1.10 | 122.17.163... | UDP | 76 42279 - 33434 Len=32 | |
| 8 | 9.1.19711... | 192.168.1.10 | 122.17.163... | UDP | 76 40208 - 33435 Len=32 | |
| 9 | 10.1.19713... | 192.168.1.10 | 122.17.163... | UDP | 76 50608 - 33436 Len=32 | |
| 10 | 11.1.19715... | 192.168.1.10 | 122.17.163... | UDP | 76 45308 - 33437 Len=32 | |
| 11 | 12.1.19718... | 192.168.1.10 | 122.17.163... | UDP | 76 48426 - 33438 Len=32 | |
| 12 | 13.1.19720... | 192.168.1.10 | 122.17.163... | UDP | 76 40378 - 33439 Len=32 | |
| 13 | 14.1.19722... | 192.168.1.10 | 122.17.163... | UDP | 76 59242 - 33440 Len=32 | |
| 14 | 15.1.19725... | 192.168.1.10 | 122.17.163... | UDP | 76 33750 - 33441 Len=32 | |
| 15 | 16.1.19726... | 192.168.1.10 | 122.17.163... | UDP | 76 32888 - 33442 Len=32 | |
| 16 | 17.1.19728... | 192.168.1.10 | 122.17.163... | UDP | 76 40449 - 33443 Len=32 | |
| 17 | 18.1.19730... | 192.168.1.10 | 122.17.163... | UDP | 76 34649 - 33444 Len=32 | |
| 18 | 19.1.19733... | 192.168.1.10 | 122.17.163... | UDP | 76 59271 - 33445 Len=32 | |

DNS queries of traceroute

```
navin@usermachine:~ » traceroute www.cmuj.jp
traceroute to www.cmuj.jp (122.17.163.205), 30 hops max, 60 byte packets
  1 _gateway (192.168.1.1)  1.645 ms  1.871 ms  2.420 ms
  2 223.178.56.1 (223.178.56.1)  6.514 ms  6.484 ms  7.880 ms
  3 nsg-corporate-101.95.187.122.airtel.in (122.187.95.101)  8.944 ms nsg-corporate-97.95.187.122.airtel.in (122.187.95.97)  7.350 ms
    7.760 ms
  4 116.119.57.146 (116.119.57.146)  43.619 ms 182.79.137.2 (182.79.137.2)  46.414 ms 116.119.57.162 (116.119.57.162)  44.305 ms
  5 116.51.31.53 (116.51.31.53)  46.081 ms  46.061 ms  46.554 ms
  6 * *
  7 ae-4.r27.osakjp02.jp.bb.gin.ntt.net (129.250.2.67)  109.187 ms  107.904 ms ae-17.r31.tokyjp05.jp.bb.gin.ntt.net (129.250.2.243)
  109.019 ms
  8 ae-3.r03.tokyjp05.jp.bb.gin.ntt.net (129.250.3.56)  108.185 ms ae-2.r02.osakjp02.jp.bb.gin.ntt.net (129.250.2.128)  108.137 ms  1
  07.195 ms
  9 ae-0.r26.tkohk01.hk.bb.gin.ntt.net (129.250.5.28)  79.122 ms ae-1.ocn.osakjp02.jp.bb.gin.ntt.net (61.200.80.14)  108.354 ms ae-3
  .ocn.osakjp02.jp.bb.gin.ntt.net (61.200.80.78)  112.359 ms
  10 125.170.96.33 (125.170.96.33)  110.810 ms  109.014 ms ae-12.r30.tokyjp05.jp.bb.gin.ntt.net (129.250.2.50)  119.374 ms
  11 122.1.245.189 (122.1.245.189)  113.410 ms ae-0.r31.tokyjp05.jp.bb.gin.ntt.net (129.250.5.22)  122.375 ms 211.129.53.194 (211.129.
  53.194)  113.798 ms
  12 122.1.245.206 (122.1.245.206)  115.418 ms  114.542 ms 122.17.156.2 (122.17.156.2)  112.322 ms
  13 118.23.168.142 (118.23.168.142)  137.351 ms * *
  14 122.1.245.210 (122.1.245.210)  119.105 ms 211.129.53.194 (211.129.53.194)  114.364 ms 112.434 ms
  15 122.17.156.2 (122.17.156.2)  110.652 ms  112.248 ms 211.129.53.194 (211.129.53.194)  120.951 ms
  16 122.17.156.2 (122.17.156.2)  118.901 ms * *
  17 * *
  18 * *
```

- (Q35) The dest port increases by one in every sent packet, indicating that traceroute tries to reach the server in multiple ports, as seen here:

```

12 1.19718... 192.168.1.10 122.17.163... UDP 76 48426 → 33438 Len=32
13 1.19720... 192.168.1.10 122.17.163... UDP 76 40378 → 33439 Len=32
14 1.19723... 192.168.1.10 122.17.163... UDP 76 59242 → 33440 Len=32
15 1.19725... 192.168.1.10 122.17.163... UDP 76 33750 → 33441 Len=32
16 1.19726... 192.168.1.10 122.17.163... UDP 76 32888 → 33442 Len=32
17 1.19728... 192.168.1.10 122.17.163... UDP 76 40449 → 33443 Len=32
18 1.19730... 192.168.1.10 122.17.163... UDP 76 34649 → 33444 Len=32
19 1.19733... 192.168.1.10 122.17.163... UDP 76 59271 → 33445 Len=32
20 1.19736... 192.168.1.10 122.17.163... UDP 76 51505 → 33446 Len=32
21 1.19738... 192.168.1.10 122.17.163... UDP 76 56380 → 33447 Len=32
22 1.19740... 192.168.1.10 122.17.163... UDP 76 52533 → 33448 Len=32

▶ Frame 13: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface any, id 0
▶ Linux cooked capture v1
▶ Internet Protocol Version 4, Src: 192.168.1.10, Dst: 122.17.163.205
▶ User Datagram Protocol, Src Port: 40378, Dst Port: 33439
  ▶ Data (32 bytes)
    Data: 404142434445464748494a4b4c4d4e4f505152535455565758595a5b5c5d5e5f
      [Length: 32]

```

```

13 1.19720... 192.168.1.10 122.17.163... UDP 76 40378 → 33439 Len=32
14 1.19723... 192.168.1.10 122.17.163... UDP 76 59242 → 33440 Len=32
15 1.19725... 192.168.1.10 122.17.163... UDP 76 33750 → 33441 Len=32
16 1.19726... 192.168.1.10 122.17.163... UDP 76 32888 → 33442 Len=32
17 1.19728... 192.168.1.10 122.17.163... UDP 76 40449 → 33443 Len=32
18 1.19730... 192.168.1.10 122.17.163... UDP 76 34649 → 33444 Len=32
19 1.19733... 192.168.1.10 122.17.163... UDP 76 59271 → 33445 Len=32
20 1.19736... 192.168.1.10 122.17.163... UDP 76 51505 → 33446 Len=32
21 1.19738... 192.168.1.10 122.17.163... UDP 76 56380 → 33447 Len=32
22 1.19740... 192.168.1.10 122.17.163... UDP 76 52533 → 33448 Len=32

▶ Frame 14: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface any, id 0
▶ Linux cooked capture v1
▶ Internet Protocol Version 4, Src: 192.168.1.10, Dst: 122.17.163.205
▶ User Datagram Protocol, Src Port: 59242, Dst Port: 33440
  ▶ Data (32 bytes)
    Data: 404142434445464748494a4b4c4d4e4f505152535455565758595a5b5c5d5e5f
      [Length: 32]

```

- My chances at traceroute did not get a response back from the server, hence couldn't observe those packets.
- (Q37) ICMP packet do contain very interesting data values, The alphabets as seen here :

```

.... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 60
  Identification: 0xeffe (61438)
  ▶ Flags: 0x00
    ...0 0000 0000 = Fragment Offset: 0
  ▶ Time to Live: 2
  Protocol: UDP (17)
  Header Checksum: 0xe921 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.10
  Destination Address: 122.17.163.205
  ▶ User Datagram Protocol, Src Port: 45308, Dst Port: 33437
  ▶ Data (32 bytes)
    Data: 404142434445464748494a4b4c4d4e4f505152535455565758595a5b5c5d5e5f

0000 00 04 00 01 00 06 e0 d4 e8 32 73 8c 00 00 08 00 . . . . . . . .
0010 45 00 00 3c ef fe 00 00 02 11 e9 21 c0 a8 01 0a E . < . . . !
0020 7a 11 a3 cd b0 fc 82 9d 00 28 df ca 40 41 42 43 z . . . . . . @ABC
0030 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 DEFHIJK LMNOPQRS
0040 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f TUVWXYZ[ \ ]^_
```

- (Q38) We can observe the ping request and response followed by a bunch of UDP packets to a fixed port of 443 with random data.

```

5 0.00625... 192.168.1.10 122.17.163... ICMP 100 Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 6)
6 0.11892... 122.17.163... 192.168.1.10 ICMP 100 Echo (ping) reply id=0x0001, seq=1/256, ttl=52 (request in 5)
7 0.11951... 192.168.1.10 192.168.1.1 DNS 89 Standard query 0x26cf PTR 205.163.17.122.in-addr.arpa
8 0.12137... 192.168.1.1 192.168.1.10 DNS 114 Standard query response 0x26cf PTR 205.163.17.122.in-addr.arpa PTR
9 0.89454... 192.168.1.10 142.250.196... UDP 12... 37248 -> 443 Len=1246
10 0.89463... 192.168.1.10 142.250.196... UDP 12... 37248 -> 443 Len=1250
11 0.89465... 192.168.1.10 142.250.196... UDP 12... 37248 -> 443 Len=1250
12 0.89468... 192.168.1.10 142.250.196... UDP 12... 37248 -> 443 Len=1250
13 0.89470... 192.168.1.10 142.250.196... UDP 11... 37248 -> 443 Len=1142
14 0.89594... 192.168.1.10 172.217.163... UDP 12... 35668 -> 443 Len=1243
15 0.89601... 192.168.1.10 172.217.163... UDP 12... 35668 -> 443 Len=1250
16 0.89603... 192.168.1.10 172.217.163... UDP 12... 35668 -> 443 Len=1250
17 0.89606... 192.168.1.10 172.217.163... UDP 12... 35668 -> 443 Len=1250
18 0.89608... 192.168.1.10 172.217.163... UDP 12... 35668 -> 443 Len=1250

```

Frame 5: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0
 hex dump capture v1
 Internet Protocol Version 4, Src: 192.168.1.10, Dst: 122.17.163.205
 Internet Control Message Protocol