CS 342: Computer Networks Laboratory
Assignment 1

Group 84
Shubham Kumar Jha 220123081
Vineet Ansal 220123069

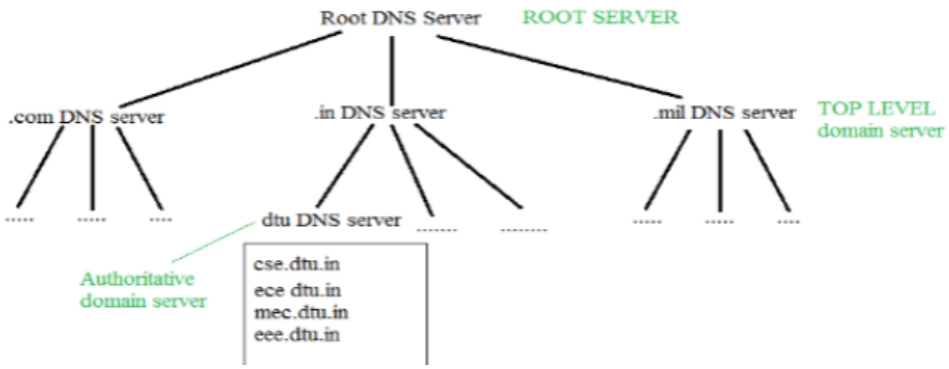
Drive link to all the traces: [Google Drive]

Question 1.

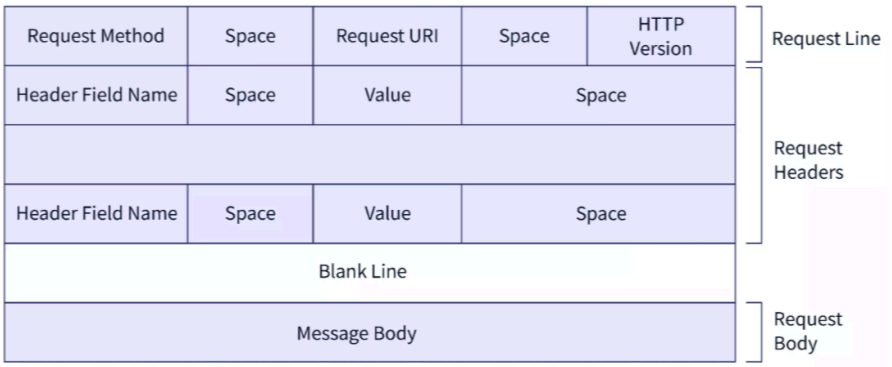
Application Layer:

Protocols:

1. DNS -Domain Name System is also an application layer protocol which converts domain names into IP addresses.



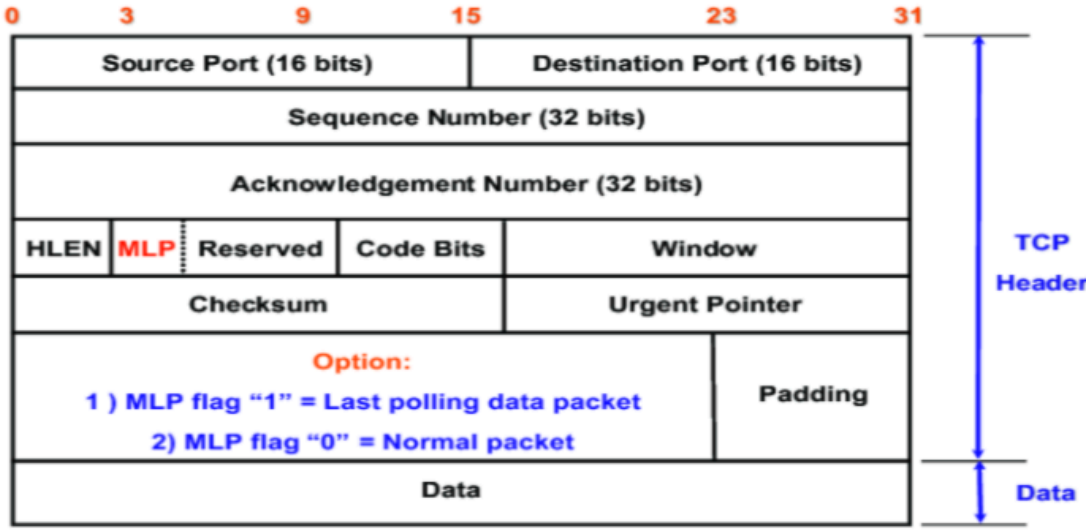
2.HTTP - HTTP is an application layer protocol designed to transfer information between networked devices and runs on top of other layers of the network protocol stack.



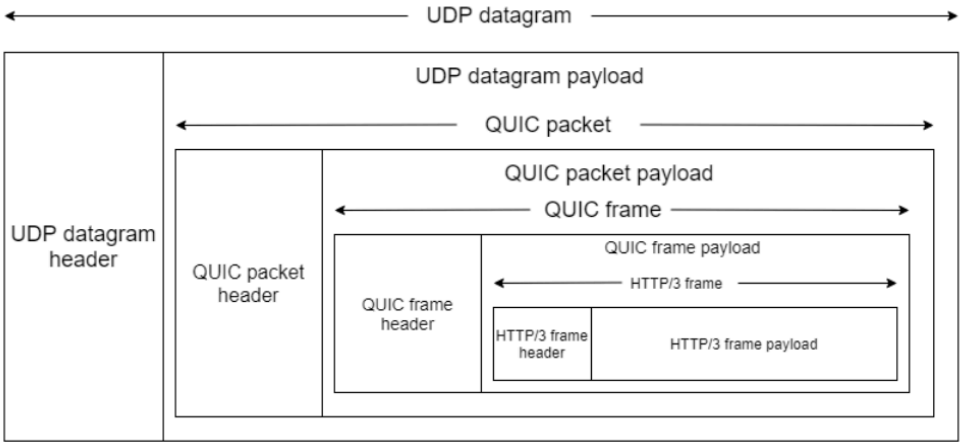
Transport Layer Protocol:

Protocols:

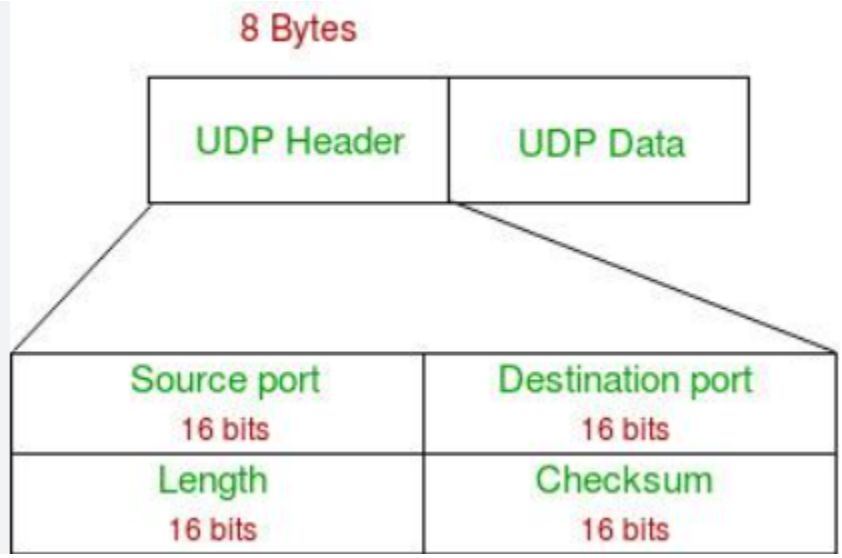
1. Transmission Control Protocol (TCP) is a communications standard that enables application programs and computing devices to exchange messages over a network. It is designed to send packets across the internet and ensure the successful delivery of data and messages over networks.



2. QUIC is a general-purpose transport layer network protocol.QUIC (Quick UDP Internet Connections, is an experimental transport layer network protocol designed by Google. The overall goal is to reduce latency compared to that of TCP. QUIC is similar to TCP+TLS+HTTP/2 implemented on UDP.



3. User Datagram Protocol (UDP) is a Transport Layer protocol. UDP is a part of the Internet Protocol suite, referred to as UDP/IP suite. Unlike TCP, it is an unreliable and connectionless protocol. So, there is no need to establish a connection before data transfer.



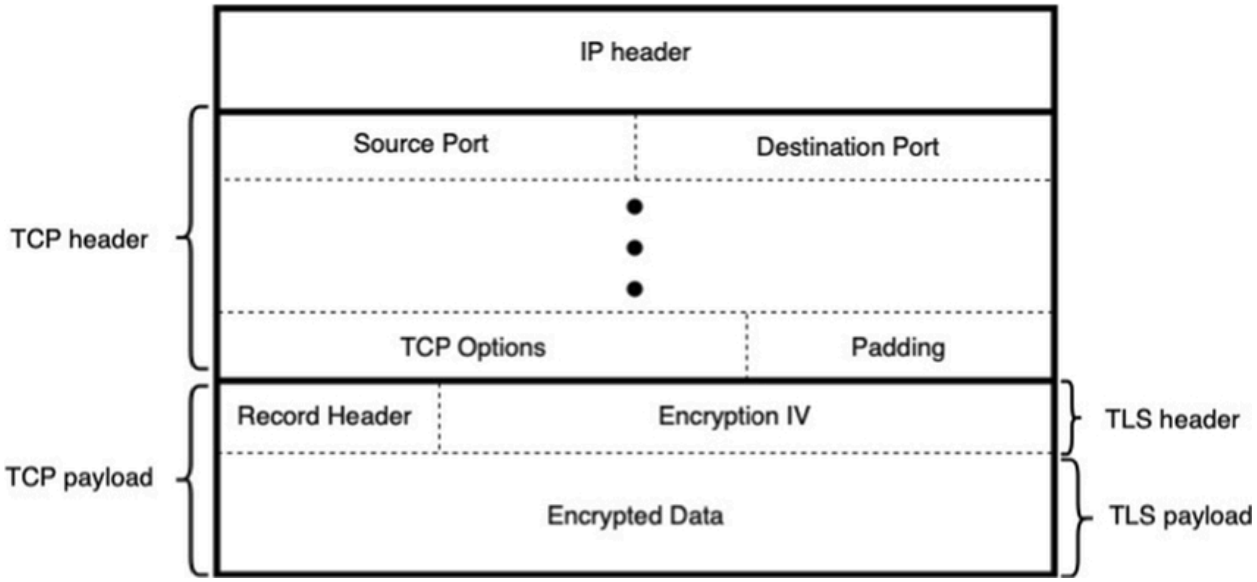
Securtiy Layer Protocols:

Protocols:

1. SSL: Secure Socket Layer (SSL) provides security to the data that is transferred between web browser and server. SSL encrypts the link between a web server and

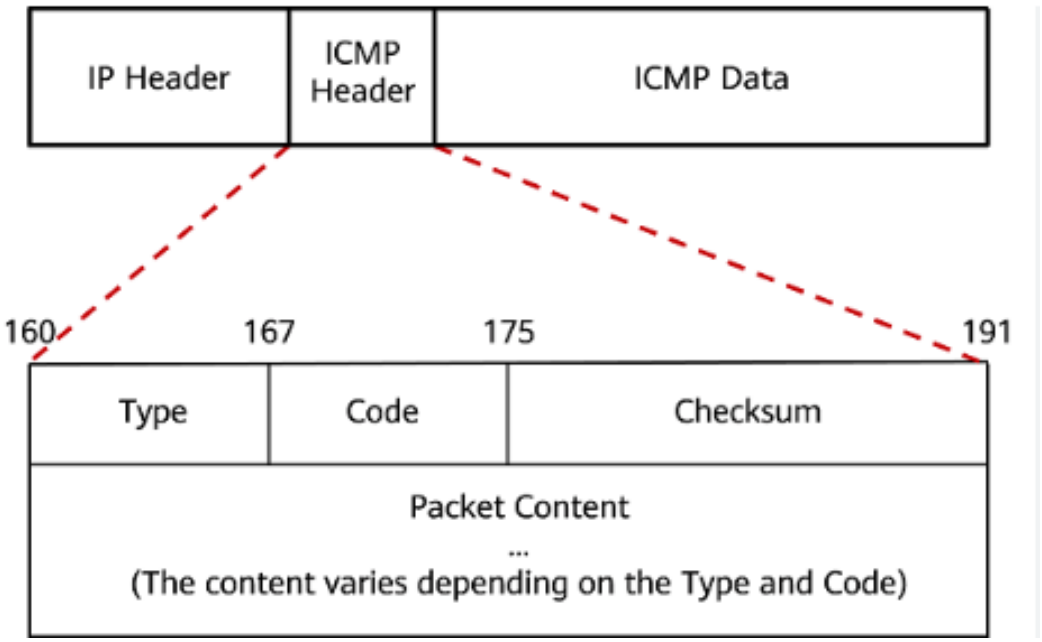
a browser, ensuring that all data passed between them remains private and free from attack.

2. TLS: Transport Layer Security, or TLS, is a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet. A primary use case of TLS is encrypting the communication between web applications and servers, such as web browsers loading a website.I captured TLSv1.2 and TLSv1.3 that is Transfer Layer Security which is the successor to Secure Socket Layer (SSL).



Network Layer Protocol:

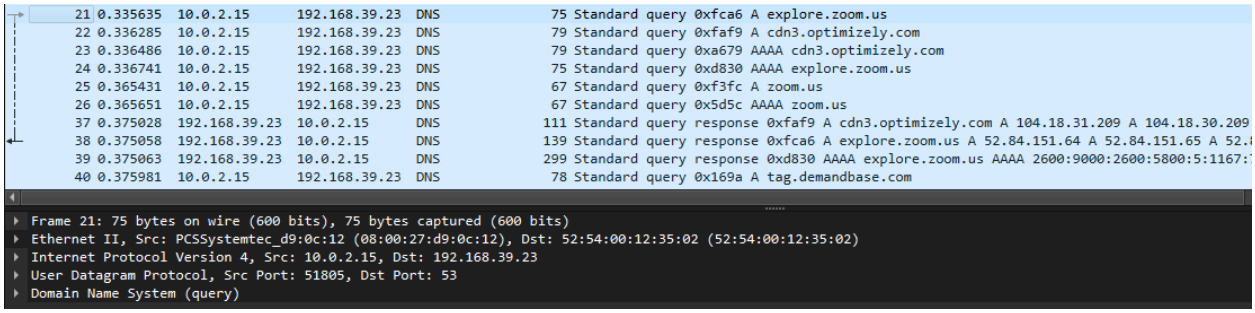
1. The Internet Control Message Protocol (ICMP) is a network layer protocol used by network devices to diagnose network communication issues. ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner. Commonly, the ICMP protocolis used on network devices, such as routers.



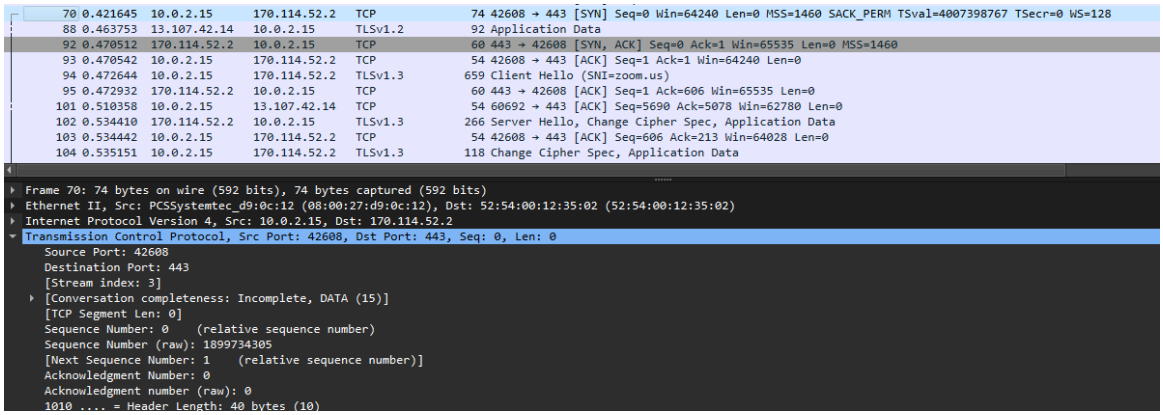
Question 2.

1. Zoom:

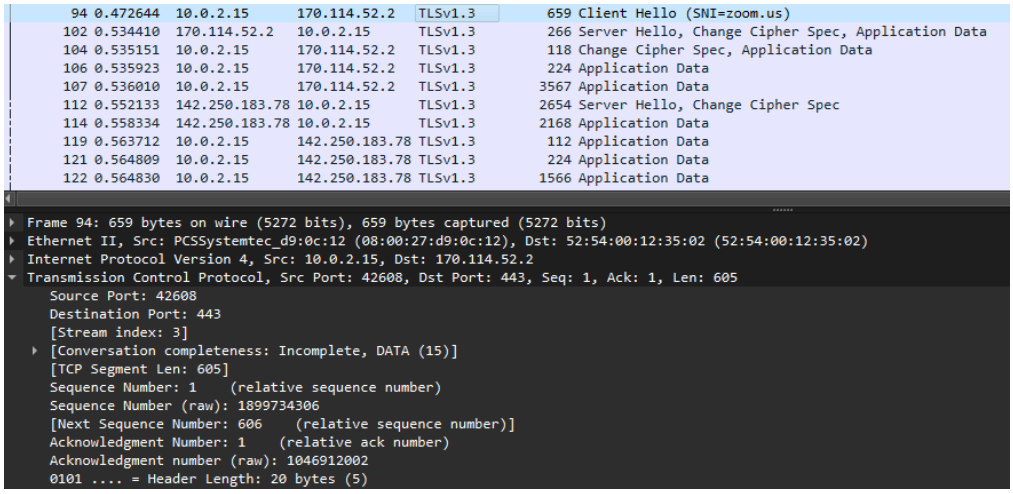
DNS: Src IP and Dst IP can be seen in lines 21 to 38



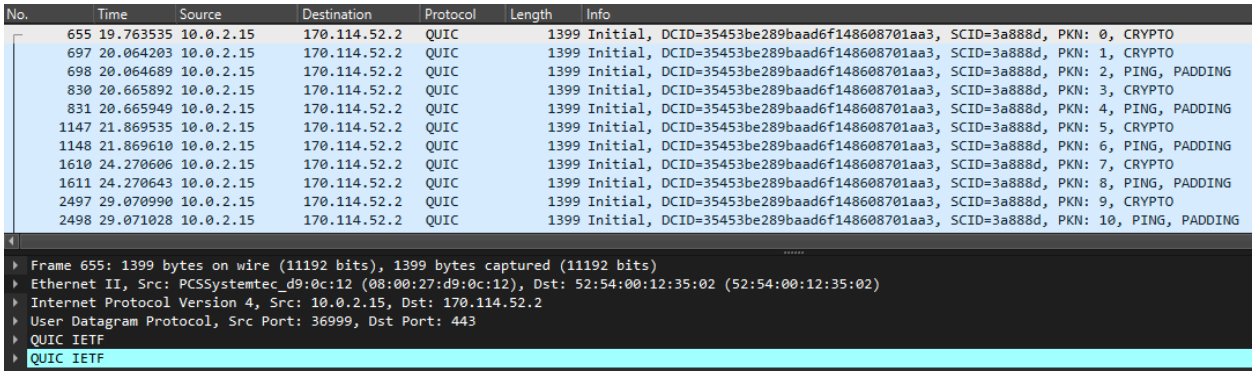
TCP: Src IP and Dst IP can be seen in lines 70 and 92



TLS: Src IP and Dst IP can be seen in lines 94,104 and 106

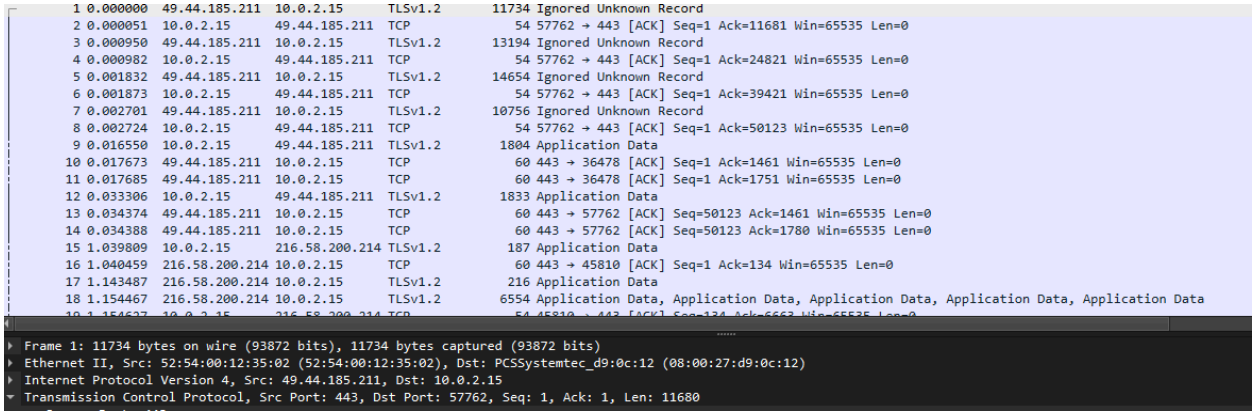


QUIC: Src IP and Dst IP can be observed

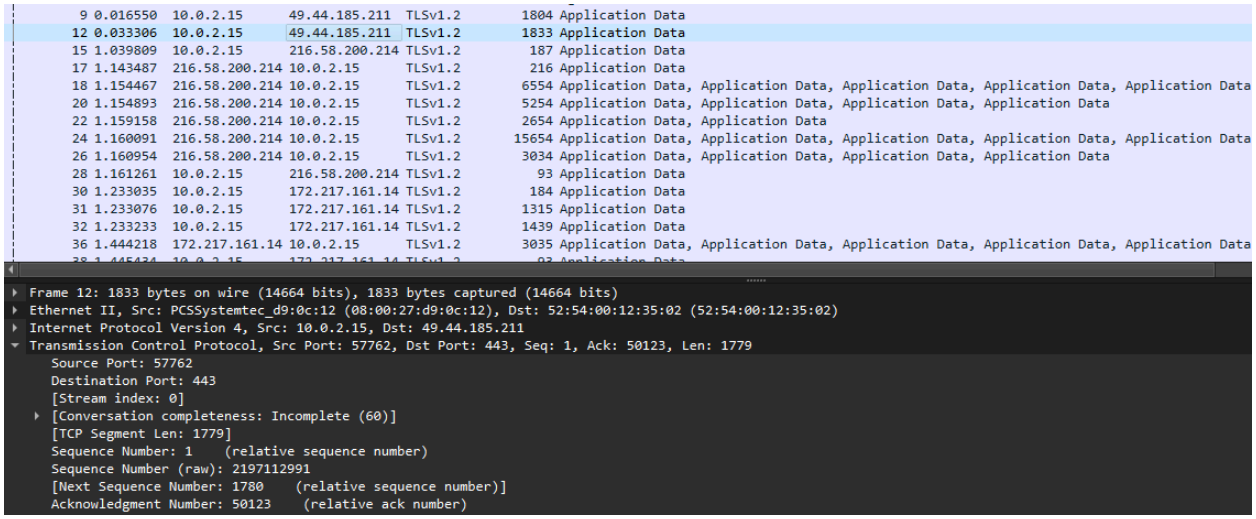


2. Live Sports

TCP: Src IP and Dest IP can be observed

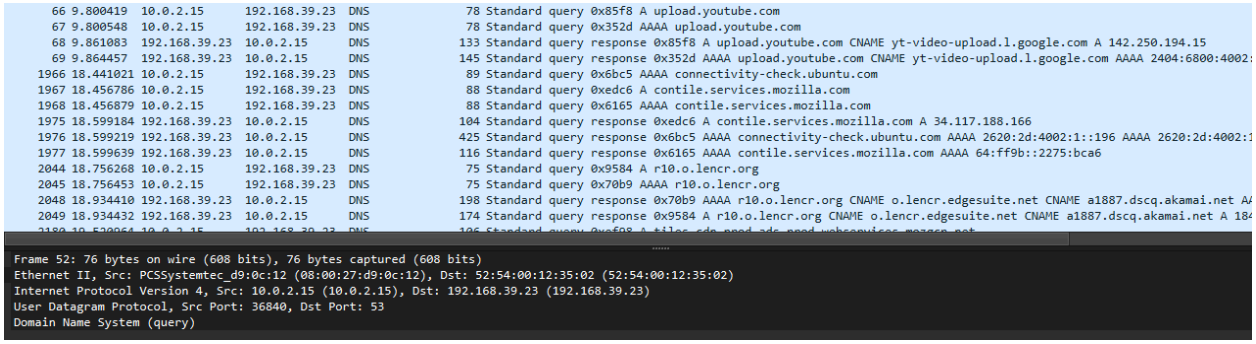


TLS: Src IP and Dest IP can be observed

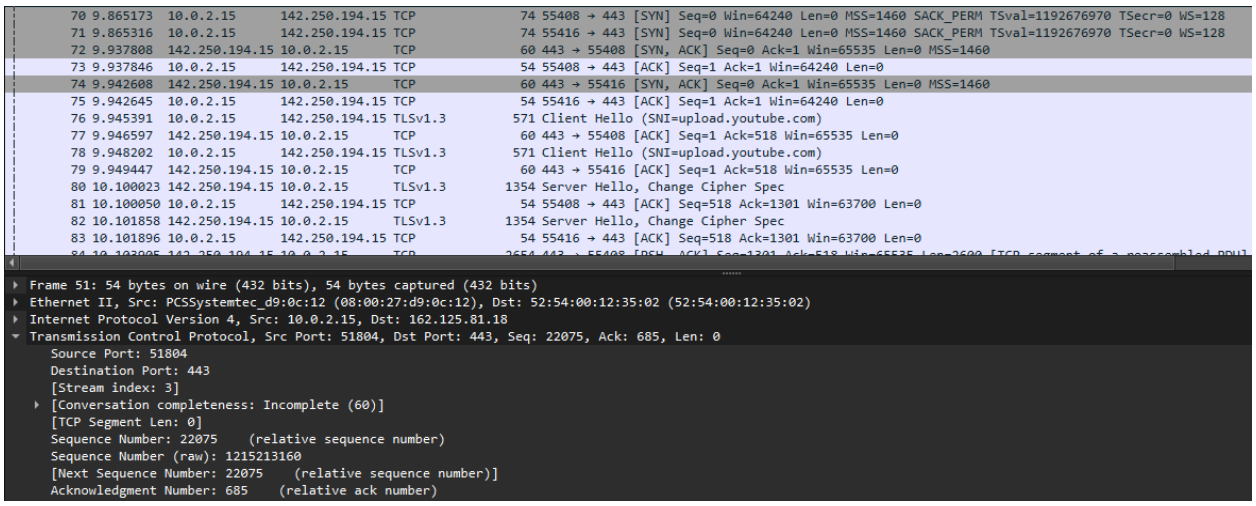


3. YouTube Upload

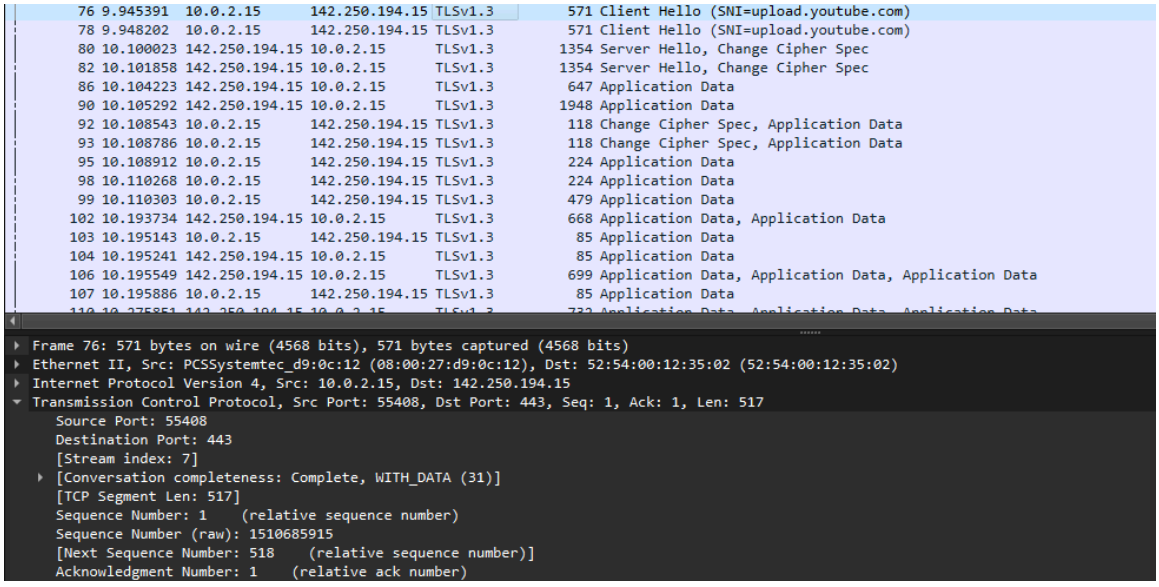
DNS: Src IP and Dest IP can be seen in lines 66 to 69



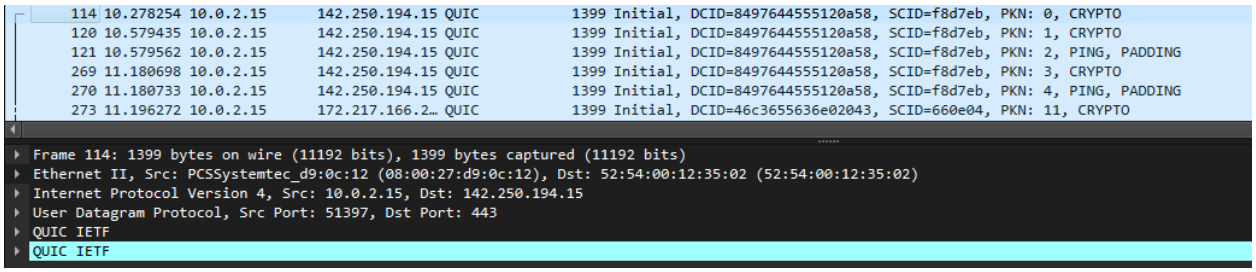
TCP: Src IP and Dest IP can be seen in lines 70 to 74



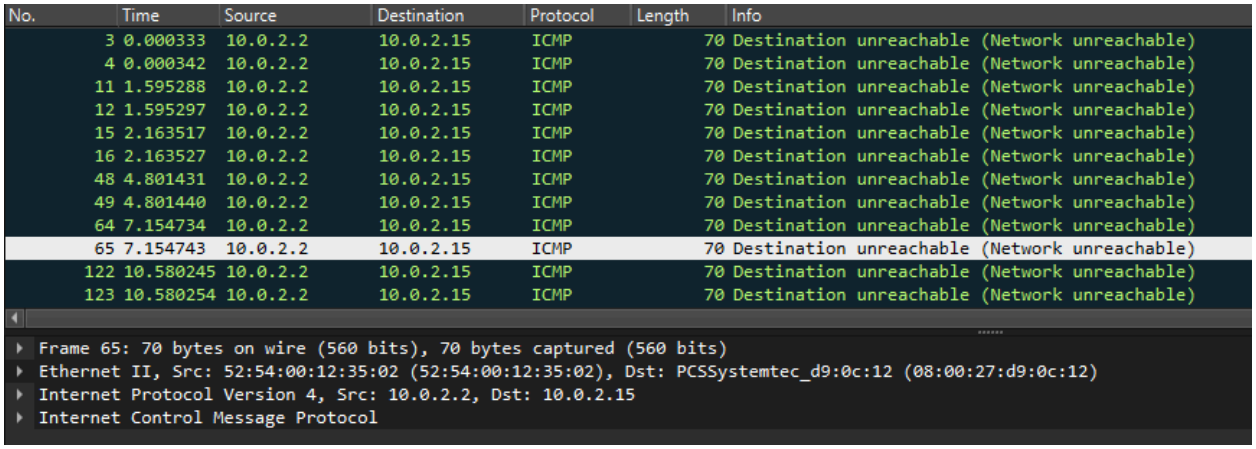
TLS: Src IP and Dest IP can be seen in lines 76 onwards



QUIC: Src IP and Dest IP can be seen in lines 114, 120 and 121

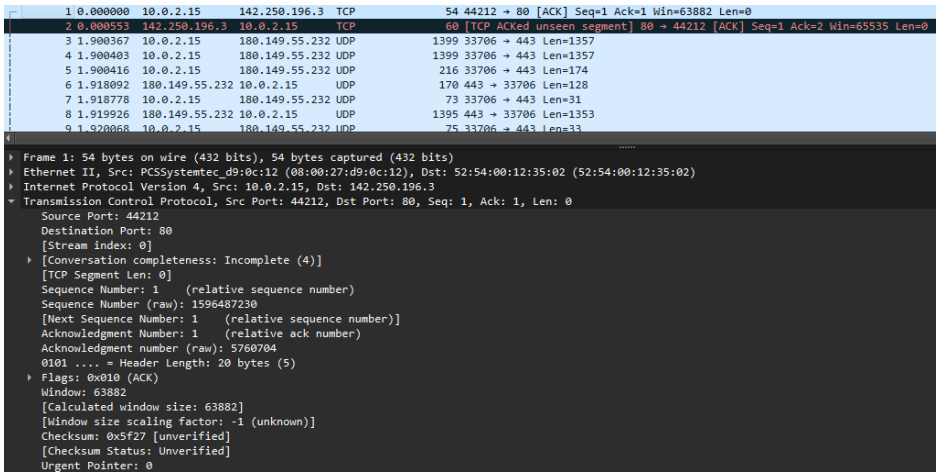


ICMP:

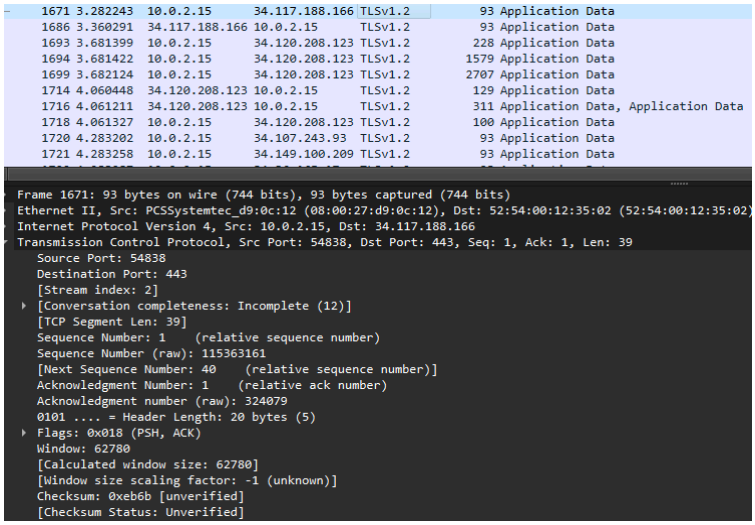


4. YouTube Downloading and Buffering:

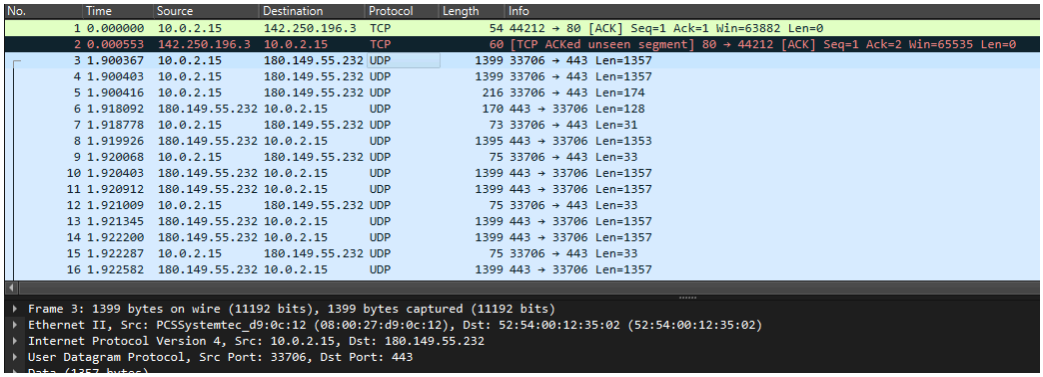
TCP: Src IP and Dst IP can be seen in lines 1 and 2



TLS: Src IP and Dst IP

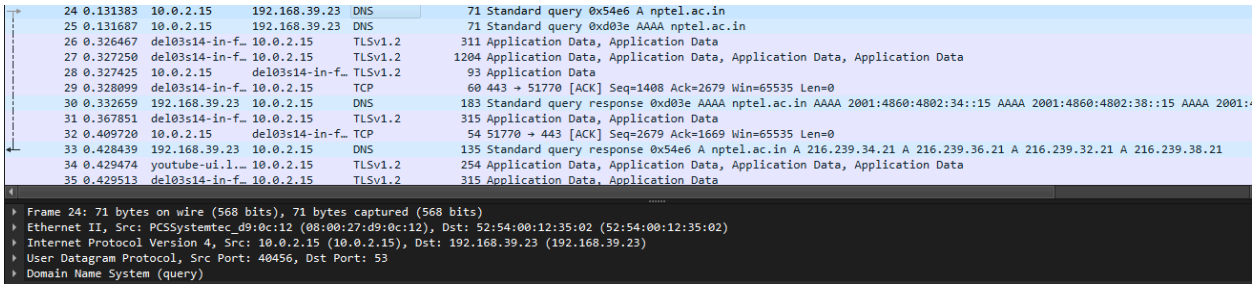


UDP: Src IP and Dst IP

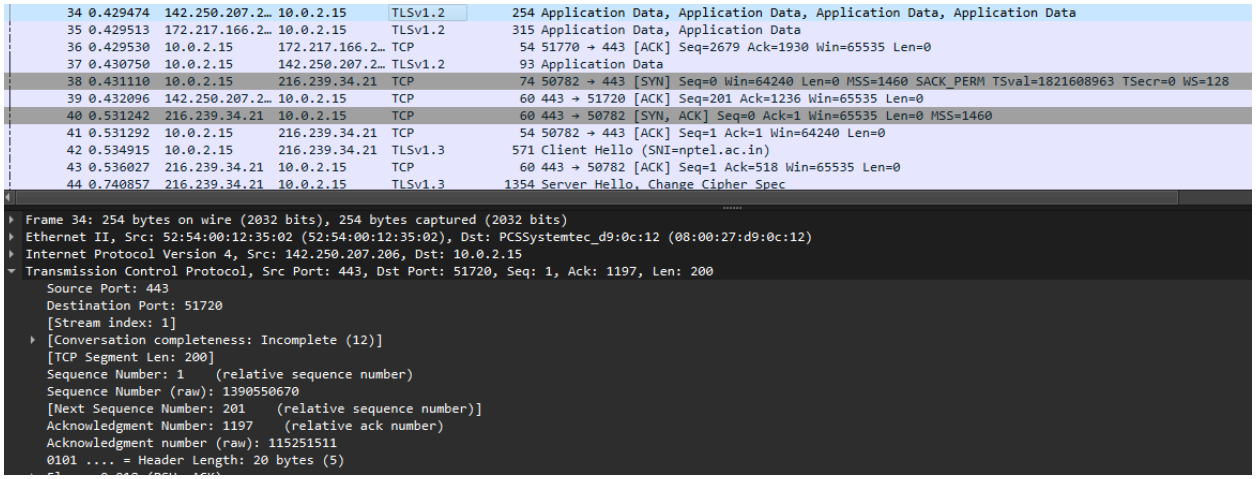


5. NPTEL

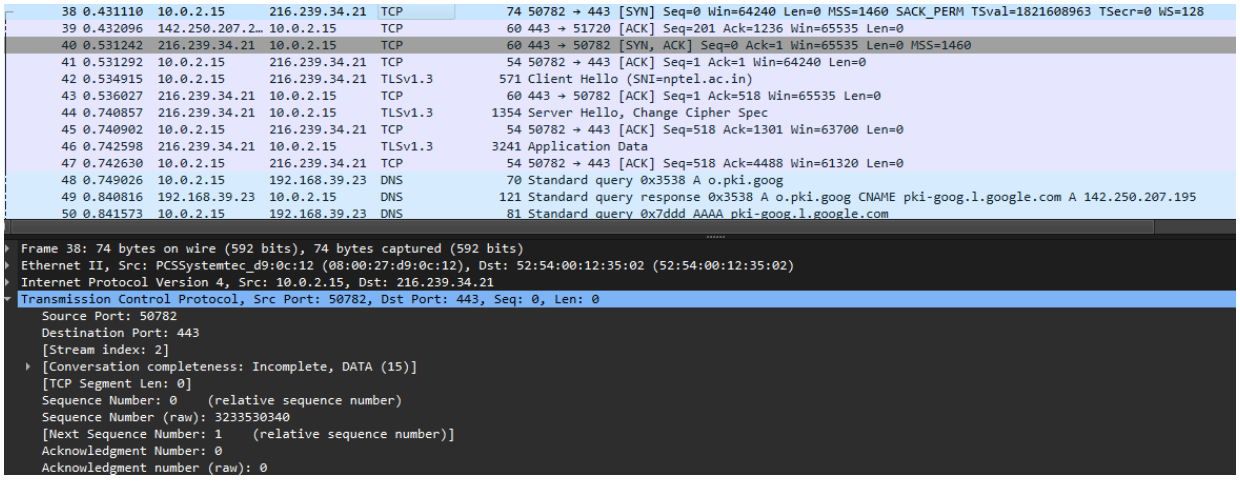
DNS: DNS lookup can be seen in lines 24 and 25, and response in lines 30 and 33



TLS: Src IP and Dst IP can be seen in lines 35 and 36



TCP: Src IP and Dst IP can be seen in lines 38 and 40

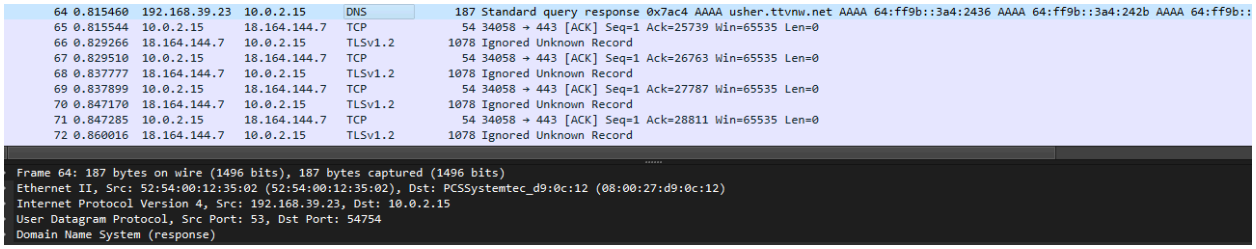


QUIC: Src IP and Dst IP can be observed

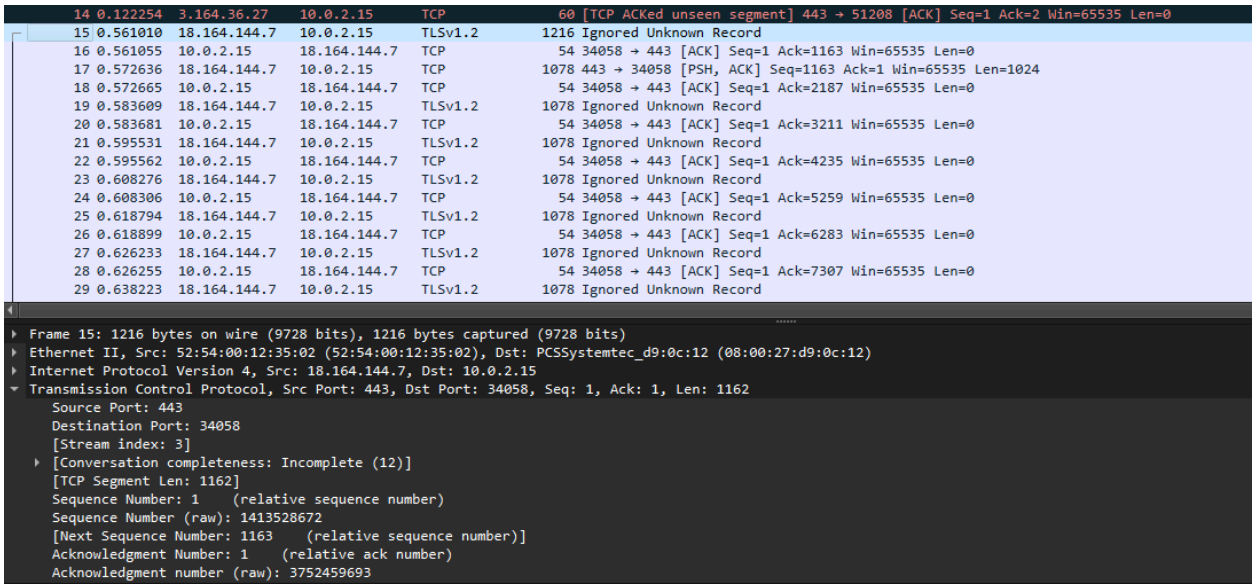
–	255	4.978239	10.0.2.15	104.17.25.14	QUIC	1399 Initial, DCID=6acd186299398ecea395693cea, SCID=ddb6a9, PKN: 0, CRYPTO
	319	5.281024	10.0.2.15	104.17.25.14	QUIC	1399 Initial, DCID=6acd186299398ecea395693cea, SCID=ddb6a9, PKN: 1, CRYPTO
	320	5.281116	10.0.2.15	104.17.25.14	QUIC	1399 Initial, DCID=6acd186299398ecea395693cea, SCID=ddb6a9, PKN: 2, PING, PADDING
	587	5.883975	10.0.2.15	104.17.25.14	QUIC	1399 Initial, DCID=6acd186299398ecea395693cea, SCID=ddb6a9, PKN: 3, CRYPTO
	588	5.884055	10.0.2.15	104.17.25.14	QUIC	1399 Initial, DCID=6acd186299398ecea395693cea, SCID=ddb6a9, PKN: 4, PING, PADDING
	1116	7.085000	10.0.2.15	104.17.25.14	QUIC	1399 Initial, DCID=6acd186299398ecea395693cea, SCID=ddb6a9, PKN: 5, CRYPTO
	1117	7.085051	10.0.2.15	104.17.25.14	QUIC	1399 Initial, DCID=6acd186299398ecea395693cea, SCID=ddb6a9, PKN: 6, PING, PADDING
	2021	9.486131	10.0.2.15	104.17.25.14	QUIC	1399 Initial, DCID=6acd186299398ecea395693cea, SCID=ddb6a9, PKN: 7, CRYPTO
	2022	9.486189	10.0.2.15	104.17.25.14	QUIC	1399 Initial, DCID=6acd186299398ecea395693cea, SCID=ddb6a9, PKN: 8, PING, PADDING
	3944	14.286875	10.0.2.15	104.17.25.14	QUIC	1399 Initial, DCID=6acd186299398ecea395693cea, SCID=ddb6a9, PKN: 9, CRYPTO
	3945	14.286977	10.0.2.15	104.17.25.14	QUIC	1399 Initial, DCID=6acd186299398ecea395693cea, SCID=ddb6a9, PKN: 10, PING, PADDING
	5535	23.888524	10.0.2.15	104.17.25.14	QUIC	1399 Initial, DCID=6acd186299398ecea395693cea, SCID=ddb6a9, PKN: 11, CRYPTO
–	5536	23.888580	10.0.2.15	104.17.25.14	QUIC	1399 Initial, DCID=6acd186299398ecea395693cea, SCID=ddb6a9, PKN: 12, PING, PADDING
	6527	31.767811	10.0.2.15	49.44.76.47	QUIC	1399 Initial, DCID=8f81284a062fbb2eef98347969, SCID=1654bc, PKN: 0, CRYPTO
	6629	32.067544	10.0.2.15	49.44.76.47	QUIC	1399 Initial, DCID=8f81284a062fbb2eef98347969, SCID=1654bc, PKN: 1, CRYPTO
	6630	32.067584	10.0.2.15	49.44.76.47	QUIC	1399 Initial, DCID=8f81284a062fbb2eef98347969, SCID=1654bc, PKN: 2, PING, PADDING

6. TWITCH

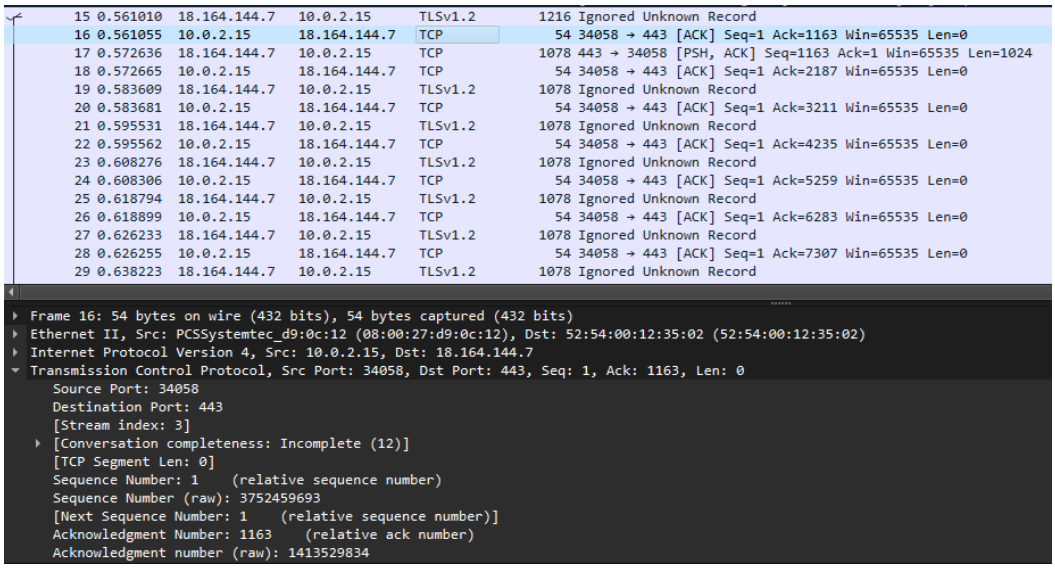
DNS : Src IP and Dst IP can be seen on line 64



TLS: Src IP and Dst IP can be seen in lines 15, 19 and 21

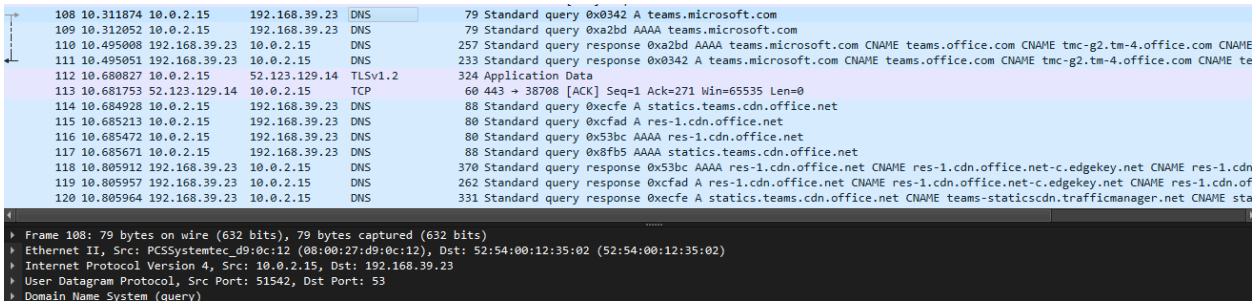


TCP: src IP and dest IP can be seen in lines 16, 17 and 18

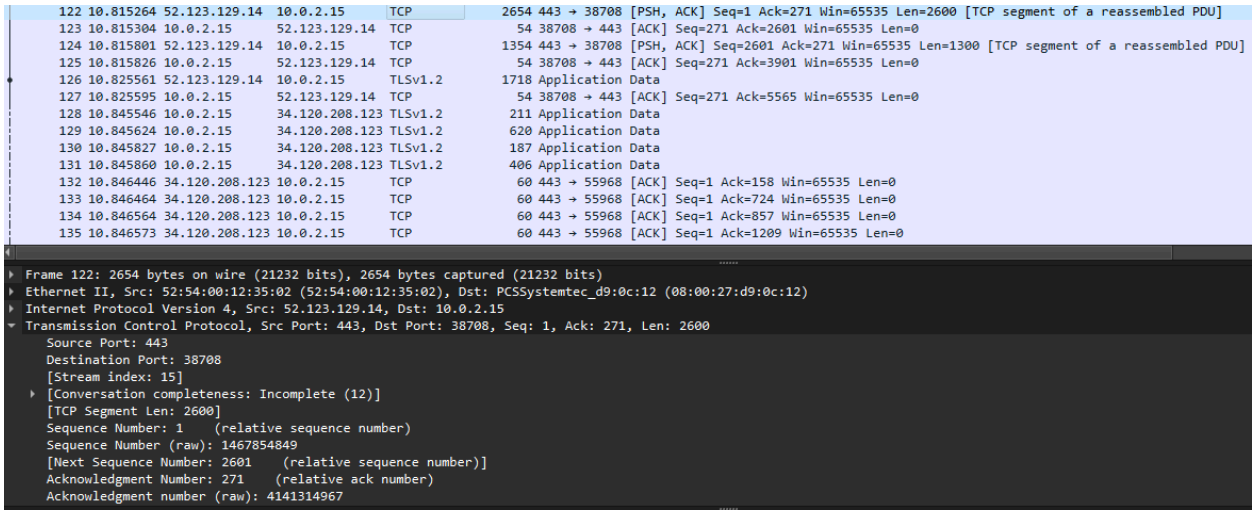


7. MS TEAMS

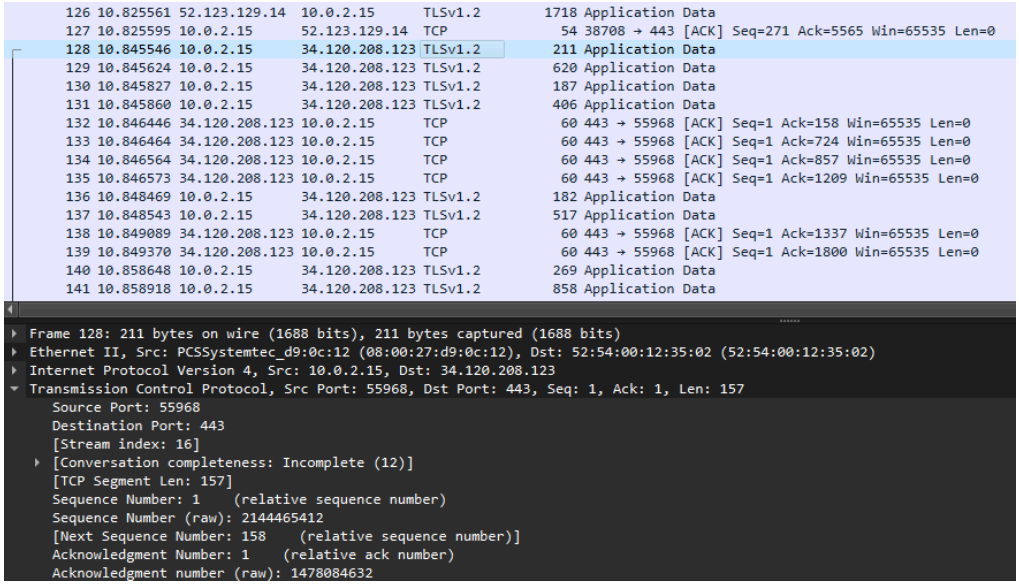
DNS: Src IP and Dest IP can be seen in light blue



TCP: Src IP and Dest IP can be seen in line 122 to125

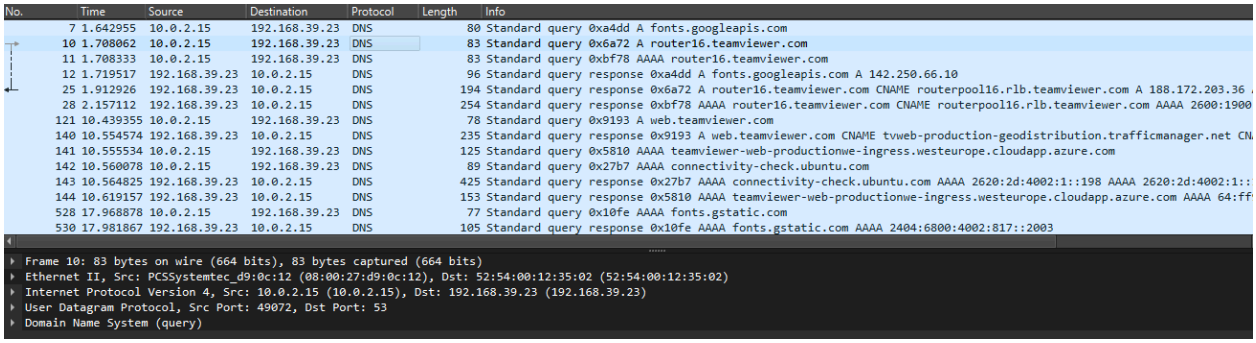


TLS: Src IP and Dest IP can be seen in line 128 to 131



8. P2P Connectivity(Team Viewer)

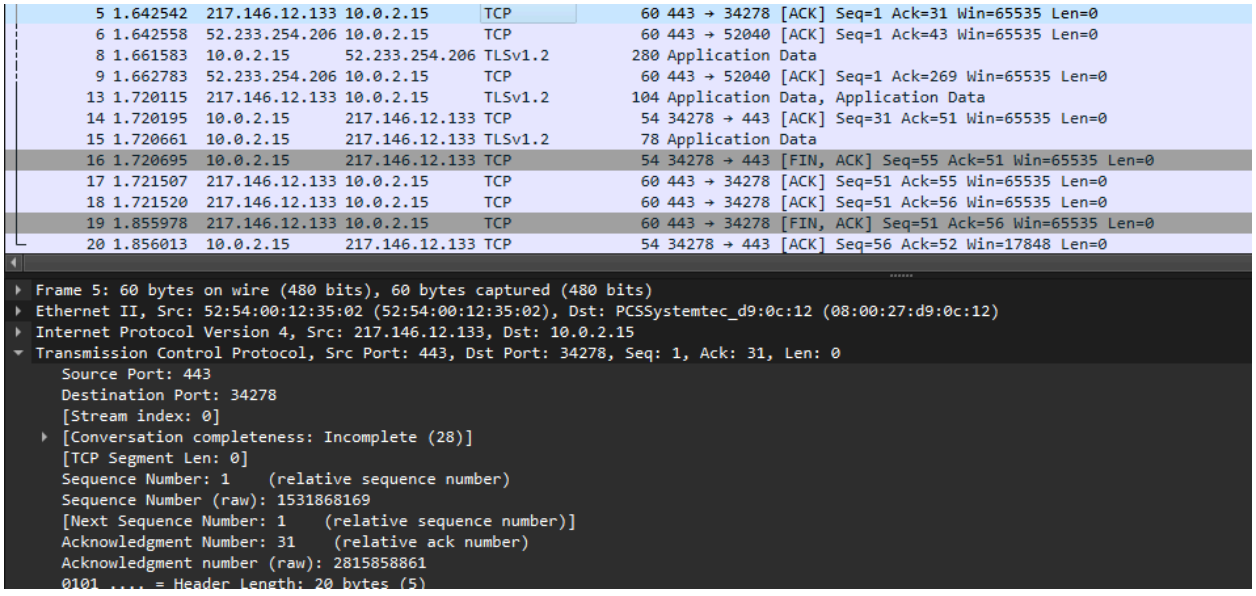
DNS: Src IP and Dest IP can be seen in lines 10, 11, and 25



No.	Time	Source	Destination	Protocol	Length	Info
7	1.642955	10.0.2.15	192.168.39.23	DNS	80	Standard query 0xa4dd A fonts.googleapis.com
10	1.708062	10.0.2.15	192.168.39.23	DNS	83	Standard query 0x6a72 A router16.teamviewer.com
11	1.708333	10.0.2.15	192.168.39.23	DNS	83	Standard query 0xbf78 AAAA router16.teamviewer.com
12	1.719517	192.168.39.23	10.0.2.15	DNS	96	Standard query response 0xa4dd A fonts.googleapis.com A 142.250.66.10
25	1.912926	192.168.39.23	10.0.2.15	DNS	194	Standard query response 0x6a72 A router16.teamviewer.com CNAME routerpool16.rlb.teamviewer.com A 188.172.203.36
28	2.157112	192.168.39.23	10.0.2.15	DNS	254	Standard query response 0xbf78 AAAA router16.teamviewer.com CNAME routerpool16.rlb.teamviewer.com AAAA 2600:1900
121	10.439355	10.0.2.15	192.168.39.23	DNS	78	Standard query 0x9193 A web.teamviewer.com
140	10.554574	192.168.39.23	10.0.2.15	DNS	235	Standard query response 0x9193 A web.teamviewer.com CNAME tvweb-production-geodistribution.trafficmanager.net CN
141	10.555534	10.0.2.15	192.168.39.23	DNS	125	Standard query 0x5810 AAAA teamviewer-web-productionwe-ingress.westeurope.cloudapp.azure.com
142	10.560078	10.0.2.15	192.168.39.23	DNS	89	Standard query 0x27b7 AAAA connectivity-check.ubuntu.com
143	10.564825	192.168.39.23	10.0.2.15	DNS	425	Standard query response 0x27b7 AAAA connectivity-check.ubuntu.com AAAA 2620:2d:4002:1::198 AAAA 2620:2d:4002:1::
144	10.619157	192.168.39.23	10.0.2.15	DNS	153	Standard query response 0x5810 AAAA teamviewer-web-productionwe-ingress.westeurope.cloudapp.azure.com AAAA 64:ff
528	17.968878	10.0.2.15	192.168.39.23	DNS	77	Standard query 0x10fe AAAA fonts.gstatic.com
530	17.981867	192.168.39.23	10.0.2.15	DNS	105	Standard query response 0x10fe AAAA fonts.gstatic.com AAAA 2404:6800:4002:817::2003

```
▸ Frame 10: 83 bytes on wire (664 bits), 83 bytes captured (664 bits)
▸ Ethernet II, Src: PCSSystemtec_d9:0c:12 (08:00:27:d9:0c:12), Dst: 52:54:00:12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 192.168.39.23 (192.168.39.23)
▸ User Datagram Protocol, Src Port: 49072, Dst Port: 53
▸ Domain Name System (query)
```

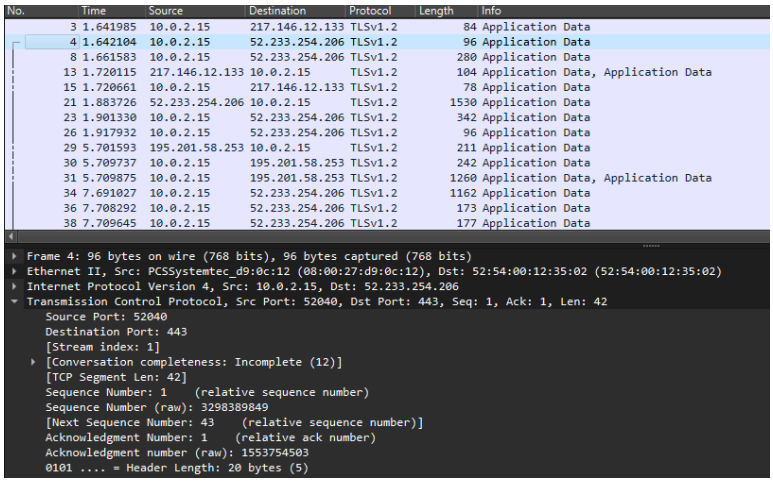
TCP: Src IP and Dest IP can be seen in lines 5 and 6



5	1.642542	217.146.12.133	10.0.2.15	TCP	60	443 → 34278 [ACK] Seq=1 Ack=31 Win=65535 Len=0
6	1.642558	52.233.254.206	10.0.2.15	TCP	60	443 → 52040 [ACK] Seq=1 Ack=43 Win=65535 Len=0
8	1.661583	10.0.2.15	52.233.254.206	TLSv1.2	280	Application Data
9	1.662783	52.233.254.206	10.0.2.15	TCP	60	443 → 52040 [ACK] Seq=1 Ack=269 Win=65535 Len=0
13	1.720115	217.146.12.133	10.0.2.15	TLSv1.2	104	Application Data, Application Data
14	1.720195	10.0.2.15	217.146.12.133	TCP	54	34278 → 443 [ACK] Seq=31 Ack=51 Win=65535 Len=0
15	1.720661	10.0.2.15	217.146.12.133	TLSv1.2	78	Application Data
16	1.720695	10.0.2.15	217.146.12.133	TCP	54	34278 → 443 [FIN, ACK] Seq=55 Ack=51 Win=65535 Len=0
17	1.721507	217.146.12.133	10.0.2.15	TCP	60	443 → 34278 [ACK] Seq=51 Ack=55 Win=65535 Len=0
18	1.721520	217.146.12.133	10.0.2.15	TCP	60	443 → 34278 [ACK] Seq=51 Ack=56 Win=65535 Len=0
19	1.855978	217.146.12.133	10.0.2.15	TCP	60	443 → 34278 [FIN, ACK] Seq=51 Ack=56 Win=65535 Len=0
20	1.856013	10.0.2.15	217.146.12.133	TCP	54	34278 → 443 [ACK] Seq=56 Ack=52 Win=17848 Len=0

```
▸ Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
▸ Ethernet II, Src: 52:54:00:12:35:02 (52:54:00:12:35:02), Dst: PCSSystemtec_d9:0c:12 (08:00:27:d9:0c:12)
▸ Internet Protocol Version 4, Src: 217.146.12.133, Dst: 10.0.2.15
▾ Transmission Control Protocol, Src Port: 443, Dst Port: 34278, Seq: 1, Ack: 31, Len: 0
    Source Port: 443
    Destination Port: 34278
    [Stream index: 0]
  ▸ [Conversation completeness: Incomplete (28)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1531868169
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 31    (relative ack number)
    Acknowledgment number (raw): 2815858861
    0101 .... = Header Length: 20 bytes (5)
```

TLS: Src IP and Dest IP can be seen in lines 4, 8, 23 and 26

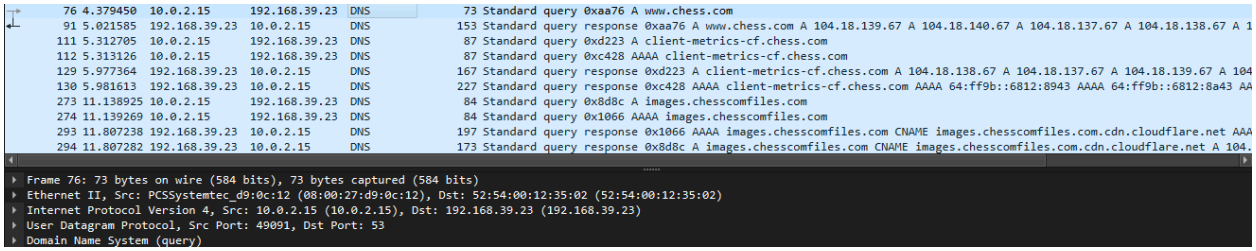


No.	Time	Source	Destination	Protocol	Length	Info
3	1.641985	10.0.2.15	217.146.12.133	TLSv1.2	84	Application Data
4	1.642104	10.0.2.15	52.233.254.206	TLSv1.2	96	Application Data
8	1.661583	10.0.2.15	52.233.254.206	TLSv1.2	280	Application Data
13	1.720115	217.146.12.133	10.0.2.15	TLSv1.2	104	Application Data, Application Data
15	1.720661	10.0.2.15	217.146.12.133	TLSv1.2	78	Application Data
21	1.883726	52.233.254.206	10.0.2.15	TLSv1.2	1530	Application Data
23	1.901330	10.0.2.15	52.233.254.206	TLSv1.2	342	Application Data
26	1.917932	10.0.2.15	52.233.254.206	TLSv1.2	96	Application Data
29	5.701593	195.201.58.253	10.0.2.15	TLSv1.2	211	Application Data
30	5.709737	10.0.2.15	195.201.58.253	TLSv1.2	242	Application Data
31	5.709875	10.0.2.15	195.201.58.253	TLSv1.2	1260	Application Data, Application Data
34	7.691027	10.0.2.15	52.233.254.206	TLSv1.2	1162	Application Data
36	7.708292	10.0.2.15	52.233.254.206	TLSv1.2	173	Application Data
38	7.709645	10.0.2.15	52.233.254.206	TLSv1.2	177	Application Data

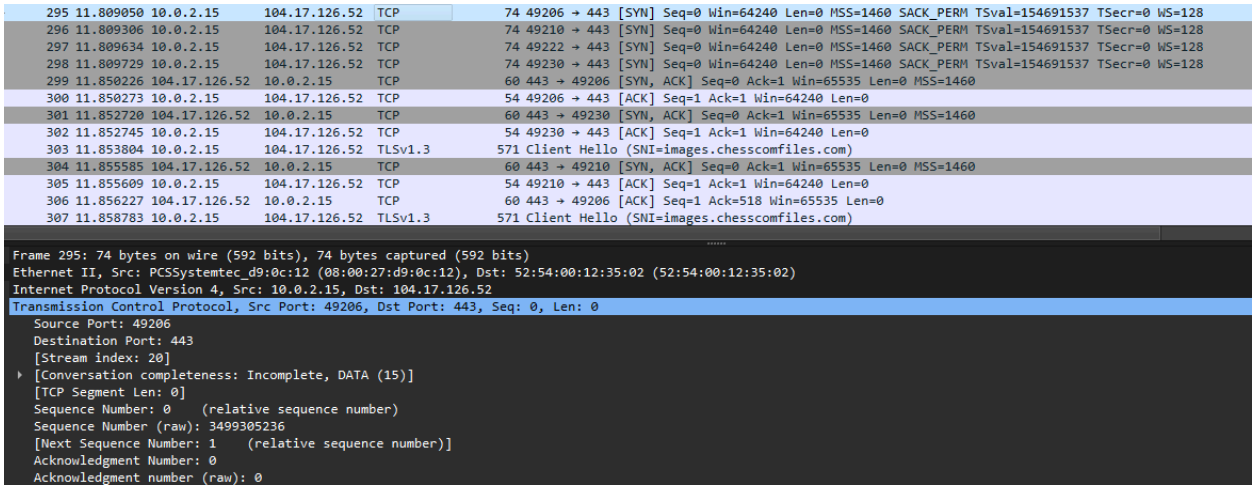
```
▸ Frame 4: 96 bytes on wire (768 bits), 96 bytes captured (768 bits)
▸ Ethernet II, Src: PCSSystemtec_d9:0c:12 (08:00:27:d9:0c:12), Dst: 52:54:00:12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 52.233.254.206
▾ Transmission Control Protocol, Src Port: 52040, Dst Port: 443, Seq: 1, Ack: 1, Len: 42
    Source Port: 52040
    Destination Port: 443
    [Stream index: 1]
  ▸ [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 42]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3298389849
    [Next Sequence Number: 43    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1553754503
    0101 .... = Header Length: 20 bytes (5)
```

9. ONLINE GAME

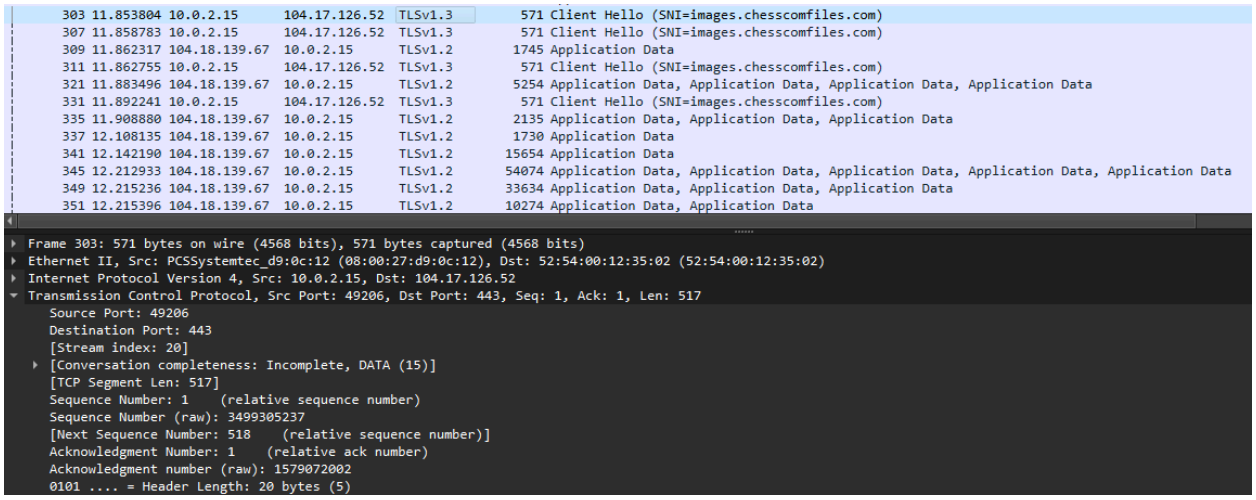
DNS: Src IP and Dest IP can be seen



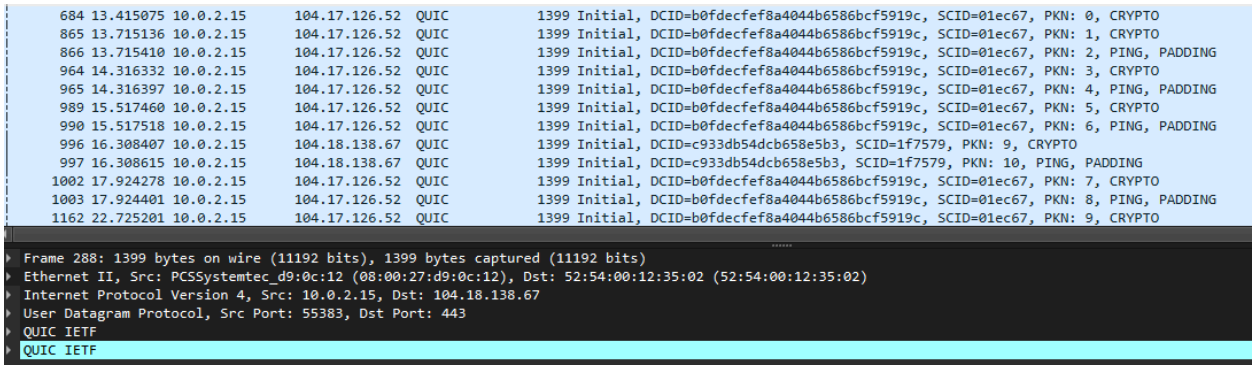
TCP: Src IP and Dest IP can be seen



TLS: Src IP and Dest IP can be seen in lines 303, 307 and 309

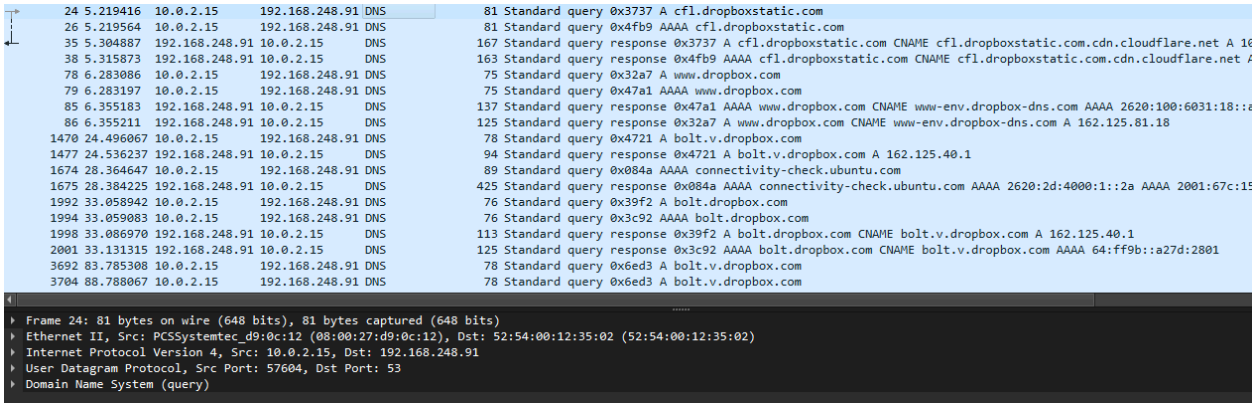


QUIC: Src IP and Dest IP can be seen in lines 684, 865 and 866



10. DROPBOX

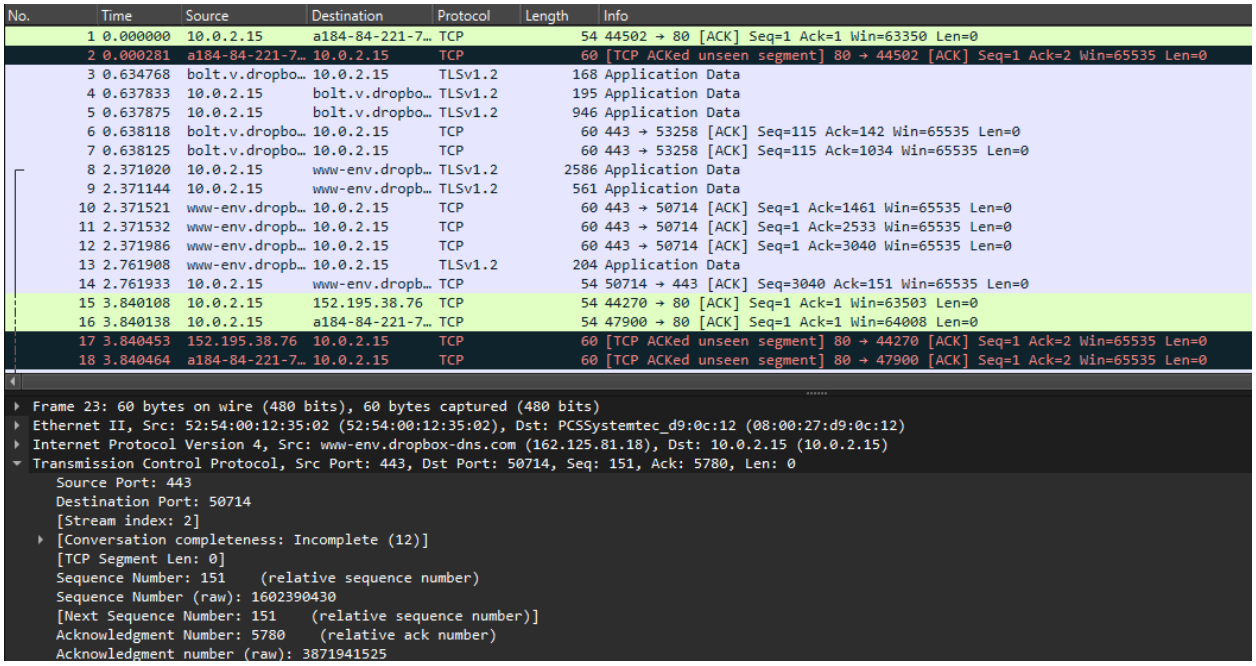
DNS : Src IP and Dst IP can be seen



```
    24 5.219416  10.0.2.15      192.168.248.91 DNS       81 Standard query 0x3737 A cfl.dropboxstatic.com
    26 5.219564  10.0.2.15      192.168.248.91 DNS       81 Standard query 0x4fb9 AAAA cfl.dropboxstatic.com
    35 5.304887  192.168.248.91 10.0.2.15      DNS      167 Standard query response 0x3737 A cfl.dropboxstatic.com CNAME cfl.dropboxstatic.com.cdn.cloudflare.net A 16
    38 5.315873  192.168.248.91 10.0.2.15      DNS      163 Standard query response 0x4fb9 AAAA cfl.dropboxstatic.com CNAME cfl.dropboxstatic.com.cdn.cloudflare.net A
    78 6.283086  10.0.2.15      192.168.248.91 DNS       75 Standard query 0x32a7 A www.dropbox.com
    79 6.283197  10.0.2.15      192.168.248.91 DNS       75 Standard query 0x47a1 AAAA www.dropbox.com
    85 6.355183  192.168.248.91 10.0.2.15      DNS      137 Standard query response 0x47a1 AAAA www.dropbox.com CNAME www-env.dropbox-dns.com AAAA 2620:100:6031:18::a
    86 6.355211  192.168.248.91 10.0.2.15      DNS      125 Standard query response 0x32a7 A www.dropbox.com CNAME www-env.dropbox-dns.com A 162.125.81.18
  1470 24.496067 10.0.2.15      192.168.248.91 DNS       78 Standard query 0x4721 A bolt.v.dropbox.com
  1477 24.536237 192.168.248.91 10.0.2.15      DNS       94 Standard query response 0x4721 A bolt.v.dropbox.com A 162.125.40.1
  1674 28.364647 10.0.2.15      192.168.248.91 DNS       89 Standard query 0x084a AAAA connectivity-check.ubuntu.com
  1675 28.384225 192.168.248.91 10.0.2.15      DNS      425 Standard query response 0x084a AAAA connectivity-check.ubuntu.com AAAA 2620:2d:4000:1::2a AAAA 2001:67c:15
  1992 33.058942 10.0.2.15      192.168.248.91 DNS       76 Standard query 0x39f2 A bolt.dropbox.com
  1994 33.059083 10.0.2.15      192.168.248.91 DNS       76 Standard query 0x3c92 AAAA bolt.dropbox.com
  1998 33.086970 192.168.248.91 10.0.2.15      DNS      113 Standard query response 0x39f2 A bolt.dropbox.com CNAME bolt.v.dropbox.com A 162.125.40.1
  2001 33.131315 192.168.248.91 10.0.2.15      DNS      125 Standard query response 0x3c92 AAAA bolt.dropbox.com CNAME bolt.v.dropbox.com AAAA 64:ff9b::a27d:2801
  3692 83.785308 10.0.2.15      192.168.248.91 DNS       78 Standard query 0x6ed3 A bolt.v.dropbox.com
  3704 88.788067 10.0.2.15      192.168.248.91 DNS       78 Standard query 0x6ed3 A bolt.v.dropbox.com

▸ Frame 24: 81 bytes on wire (648 bits), 81 bytes captured (648 bits)
▸ Ethernet II, Src: PCSSystemtec_d9:0c:12 (08:00:27:d9:0c:12), Dst: 52:54:00:12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.248.91
▸ User Datagram Protocol, Src Port: 57604, Dst Port: 53
▸ Domain Name System (query)
```

TCP : Src IP and Dst IP can be seen



```
No.  Time      Source          Destination     Protocol Length Info
     1 0.000000  10.0.2.15       a184-84-221-7… TCP          54 44502 → 80 [ACK] Seq=1 Ack=1 Win=63350 Len=0
     2 0.000281  a184-84-221-7… 10.0.2.15       TCP          60 [TCP ACKed unseen segment] 80 → 44502 [ACK] Seq=1 Ack=2 Win=65535 Len=0
     3 0.634768  bolt.v.dropbo… 10.0.2.15       TLSv1.2     168 Application Data
     4 0.637833  10.0.2.15       bolt.v.dropbo… TLSv1.2     195 Application Data
     5 0.637875  10.0.2.15       bolt.v.dropbo… TLSv1.2     946 Application Data
     6 0.638118  bolt.v.dropbo… 10.0.2.15       TCP          60 443 → 53258 [ACK] Seq=115 Ack=142 Win=65535 Len=0
     7 0.638125  bolt.v.dropbo… 10.0.2.15       TCP          60 443 → 53258 [ACK] Seq=115 Ack=1034 Win=65535 Len=0
     8 2.371020  10.0.2.15       www-env.dropb… TLSv1.2    2586 Application Data
     9 2.371144  10.0.2.15       www-env.dropb… TLSv1.2     561 Application Data
    10 2.371521  www-env.dropb… 10.0.2.15       TCP          60 443 → 50714 [ACK] Seq=1 Ack=1461 Win=65535 Len=0
    11 2.371532  www-env.dropb… 10.0.2.15       TCP          60 443 → 50714 [ACK] Seq=1 Ack=2533 Win=65535 Len=0
    12 2.371986  www-env.dropb… 10.0.2.15       TCP          60 443 → 50714 [ACK] Seq=1 Ack=3040 Win=65535 Len=0
    13 2.761908  www-env.dropb… 10.0.2.15       TLSv1.2     204 Application Data
    14 2.761933  10.0.2.15       www-env.dropb… TCP          54 50714 → 443 [ACK] Seq=3040 Ack=151 Win=65535 Len=0
    15 3.840108  10.0.2.15       152.195.38.76  TCP          54 44270 → 80 [ACK] Seq=1 Ack=1 Win=63503 Len=0
    16 3.840138  10.0.2.15       a184-84-221-7… TCP          54 47900 → 80 [ACK] Seq=1 Ack=1 Win=64008 Len=0
    17 3.840453  152.195.38.76   10.0.2.15      TCP          60 [TCP ACKed unseen segment] 80 → 44270 [ACK] Seq=1 Ack=2 Win=65535 Len=0
    18 3.840464  a184-84-221-7… 10.0.2.15       TCP          60 [TCP ACKed unseen segment] 80 → 47900 [ACK] Seq=1 Ack=2 Win=65535 Len=0

▸ Frame 23: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
▸ Ethernet II, Src: 52:54:00:12:35:02 (52:54:00:12:35:02), Dst: PCSSystemtec_d9:0c:12 (08:00:27:d9:0c:12)
▸ Internet Protocol Version 4, Src: www-env.dropbox-dns.com (162.125.81.18), Dst: 10.0.2.15 (10.0.2.15)
▾ Transmission Control Protocol, Src Port: 443, Dst Port: 50714, Seq: 151, Ack: 5780, Len: 0
    Source Port: 443
    Destination Port: 50714
    [Stream index: 2]
  ▸ [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 0]
    Sequence Number: 151    (relative sequence number)
    Sequence Number (raw): 1602390430
    [Next Sequence Number: 151    (relative sequence number)]
    Acknowledgment Number: 5780    (relative ack number)
    Acknowledgment number (raw): 3871941525
```

TLS: Src IP and Dest IP can be seen

No.	Time	Source	Destination	Protocol	Length	Info
3	0.634768	162.125.40.1	10.0.2.15	TLSv1.2	168	Application Data
4	0.637833	10.0.2.15	162.125.40.1	TLSv1.2	195	Application Data
5	0.637875	10.0.2.15	162.125.40.1	TLSv1.2	946	Application Data
8	2.371020	10.0.2.15	162.125.81.18	TLSv1.2	2586	Application Data
9	2.371144	10.0.2.15	162.125.81.18	TLSv1.2	561	Application Data
13	2.761908	162.125.81.18	10.0.2.15	TLSv1.2	204	Application Data
19	5.200362	10.0.2.15	162.125.81.18	TLSv1.2	2581	Application Data
20	5.200474	10.0.2.15	162.125.81.18	TLSv1.2	267	Application Data
25	5.219497	10.0.2.15	104.16.100.29	TLSv1.2	181	Application Data
27	5.219669	10.0.2.15	104.16.100.29	TLSv1.2	193	Application Data
30	5.224476	10.0.2.15	162.125.81.18	TLSv1.2	2586	Application Data
31	5.224574	10.0.2.15	162.125.81.18	TLSv1.2	738	Application Data
36	5.315533	104.16.100.29	10.0.2.15	TLSv1.2	1500	Application Data
39	5.336238	104.16.100.29	10.0.2.15	TLSv1.2	595	Application Data
41	5.351229	104.16.100.29	10.0.2.15	TLSv1.2	1387	Application Data, Application Data
45	5.395792	104.16.100.29	10.0.2.15	TLSv1.2	1349	Application Data
47	5.420577	104.16.100.29	10.0.2.15	TLSv1.2	78	Application Data
49	5.451520	10.0.2.15	104.16.100.29	TLSv1.2	170	Application Data

```
▸ Frame 20: 267 bytes on wire (2136 bits), 267 bytes captured (2136 bits)
▸ Ethernet II, Src: PCSSystemtec_d9:0c:12 (08:00:27:d9:0c:12), Dst: 52:54:00:12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 162.125.81.18
▾ Transmission Control Protocol, Src Port: 50714, Dst Port: 443, Seq: 5567, Ack: 151, Len: 213
    Source Port: 50714
    Destination Port: 443
    [Stream index: 2]
  ▸ [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 213]
    Sequence Number: 5567    (relative sequence number)
    Sequence Number (raw): 3871941312
    [Next Sequence Number: 5780    (relative sequence number)]
    Acknowledgment Number: 151    (relative ack number)
    Acknowledgment number (raw): 1602390430
```

Question 3.

Handshaking: Every connection begins with a “client hello” where the client gives possible cypher suits from which the server selects one that is available to it and sends in a reply in “server hello”. After that, session keys are transferred, and data transfer starts.

Video Pause and Play:

During the play of the video, the application's data continues to flow, and handshaking packets keep coming.

Video Upload and Download:

For Upload and Download, packets per second increase as soon as video is set up for upload or download as there is a huge amount of data transfer.

Question 4.

1. DNS:

DNS (Domain Name System) is vital for almost all applications, especially in streaming services, as they need to lookup their servers to serve the content to the user:

1. Domain Resolution: Translates user-friendly domains (e.g., "zoom.us or youtube.com") to IP addresses, enabling server connections.
2. Content Delivery Optimization: Directs users to the nearest CDN nodes to reduce latency in video streaming.
3. Load Balancing: Distributes user requests across multiple servers for efficient traffic management, enhancing performance during high-load events.
4. Dynamic DNS: Facilitates connections for TeamViewer, allowing users to access devices with changing IP addresses seamlessly.

2. HTTP:

HTTP is essential for data delivery platforms like YouTube and Twitch, for video delivery and user interactions.

1. Video Streaming: Users send HTTP requests for videos, and servers respond with video data in smaller packets.
2. Metadata Transfer: HTTP transmits metadata to enhance user engagement.
3. Content Delivery: YouTube utilises a CDN, leveraging HTTP to route requests to the nearest server, reducing latency and optimising load times.
4. Real-time Interactions: User interactions during live streams are processed through HTTP requests, ensuring real-time engagement.
5. Twitch: Twitch uses HLS (HTTP Live Streaming), which segments live video into small chunks sent via HTTP, allowing adaptive streaming based on bandwidth.

3. TCP:

TCP is used in applications like Dropbox, NPTEL lectures, and YouTube for the following reasons:

1. Reliable Data Transfer: TCP ensures that all data packets are delivered accurately and in order. It is ideal for applications where data integrity is crucial, like file transfers and video streaming.

2. Error Correction: TCP provides error-checking mechanisms to detect and retransmit lost or corrupted packets, ensuring the content is delivered correctly.
3. Flow Control: TCP manages the flow of data to prevent overwhelming the network or the receiver, providing smooth and consistent data transfer rates.
4. Connection-Oriented Communication: TCP establishes a connection before data is sent, ensuring a stable and secure channel for communication, which is essential for continuous data streams like video lectures and online streaming.

4. UDP:

UDP is used in parts of YouTube downloading for the following reasons:

1. Lower Latency: UDP allows for faster data transmission by avoiding the overhead of connection setup and error correction, which is useful for streaming where real-time playback is prioritized over perfect data accuracy.
2. Efficient Bandwidth Usage: UDP is more efficient for broadcasting or multicasting, making it suitable for delivering video data to multiple users simultaneously without the need for separate connections.
3. Tolerance for Packet Loss: In streaming, occasional packet loss is acceptable as it doesn't significantly affect the user experience, making UDP a suitable choice where speed and efficiency are prioritized over perfect data delivery.
4. Adaptive Streaming: UDP can be combined with protocols like QUIC (which is built on UDP) to enable adaptive streaming, allowing YouTube to adjust video quality in real-time based on network conditions, improving the overall user experience.

5. TLS and SSL:

TLS and SSL are cryptographic protocols designed to provide secure communication over a computer network and are used by almost all applications that need to send cryptographic data rather than plain ASCII text. TLS is the successor to SSL, and they are used for the following purposes:

1. Data Encryption: TLS/SSL encrypts data to protect it from being intercepted by unauthorised parties.
2. Data Integrity: Ensures that data is not altered during transmission, safeguarding against tampering.
3. Authentication: Verifies the identity of the communicating parties using digital certificates.
4. Secure Browsing: Enables secure HTTPS connections for safe online transactions and browsing.

6. QUIC:

QUIC (Quick UDP Internet Connections) is used for:

1. Reduced Latency: Provides faster connection establishment than TCP through a zero-round-trip time (0-RTT) handshake.
2. Stream Multiplexing: Allows multiple data streams without head-of-line blocking, improving performance for applications like video streaming and gaming.
3. Built-in Encryption: Integrates TLS for secure connections, enhancing privacy and security.
4. Connection Resilience: Maintains connections even when the network changes, improving reliability in mobile environments.

7. ICMP:

ICMP (Internet Control Message Protocol) is primarily used for network diagnostics and error reporting during YouTube uploads.

1. Error Reporting: If there are network issues (e.g., a router on the path is down), ICMP can send error messages back to the user's device, allowing the system to respond appropriately, such as by retrying the upload.
2. Packet Handling: During the upload process, ICMP helps manage how data packets are handled by the network, ensuring that they reach the YouTube servers efficiently, even if there is network congestion or route changes.
3. Connectivity Verification: ICMP can be used to verify connectivity and determine the best routes to the YouTube servers, ensuring that the upload process is as fast and reliable as possible.

Question 5.

1. Zoom:

Measurement	Captured
Packets	10286
Time span, s	53.848
Average pps	191.0
Average packet size, B	2730
Bytes	28078472
Average bytes/s	521 k
Average bits/s	4171 k

2. Live Sports:

Measurement	Captured
Packets	554
Time span, s	16.925
Average pps	32.7
Average packet size, B	1813
Bytes	1004472
Average bytes/s	59 k
Average bits/s	474 k

3. YouTube Uploading:

Measurement	Captured
Packets	33146
Time span, s	213.912
Average pps	155.0
Average packet size, B	1230
Bytes	40757918
Average bytes/s	190 k
Average bits/s	1524 k

4. YouTube Downloading and Buffering:

Measurement	Captured
Packets	68446
Time span, s	43.247
Average pps	1582.7
Average packet size, B	948
Bytes	64889890
Average bytes/s	1500 k
Average bits/s	12 M

5. NPTEL Video Lectures:

Measurement	Captured
Packets	18357
Time span, s	76.556
Average pps	239.8
Average packet size, B	2618
Bytes	48057665
Average bytes/s	627 k
Average bits/s	5021 k

6. Twitch:

Measurement	Captured
Packets	9065
Time span, s	76.774
Average pps	118.1
Average packet size, B	997
Bytes	9035815
Average bytes/s	117 k
Average bits/s	941 k

7. MS Teams:

Measurement	Captured
Packets	3329
Time span, s	76.307
Average pps	43.6
Average packet size, B	1207
Bytes	4017753
Average bytes/s	52 k
Average bits/s	421 k

8. P2P Connectivity(Team Viewer):

Measurement	Captured
Packets	2446
Time span, s	71.678
Average pps	34.1
Average packet size, B	3377
Bytes	8260009
Average bytes/s	115 k
Average bits/s	921 k

9. Online Game:

Measurement	Captured
Packets	2469
Time span, s	71.100
Average pps	34.7
Average packet size, B	3933
Bytes	9710790
Average bytes/s	136 k
Average bits/s	1092 k

10. Dropbox:

Measurement	Captured
Packets	4300
Time span, s	114.239
Average pps	37.6
Average packet size, B	1021
Bytes	4392090
Average bytes/s	38 k
Average bits/s	307 k