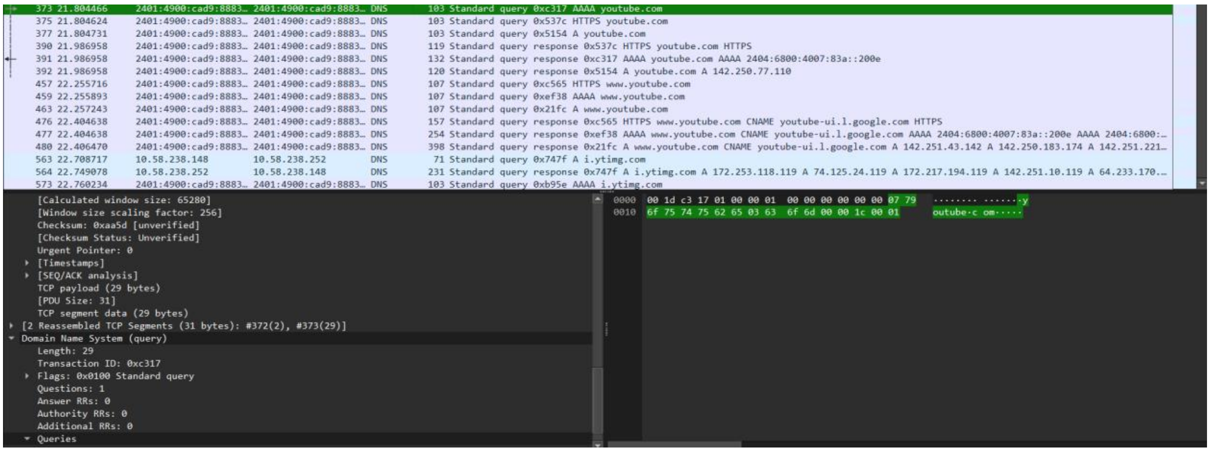
TASK 3

1.DNS



```
373 21.804466   2401:4900:cad9:8883… 2401:4900:cad9:8883… DNS   103 Standard query 0xc317 AAAA youtube.com
375 21.804624   2401:4900:cad9:8883… 2401:4900:cad9:8883… DNS   103 Standard query 0x537c HTTPS youtube.com
377 21.804731   2401:4900:cad9:8883… 2401:4900:cad9:8883… DNS   103 Standard query 0x5154 A youtube.com
390 21.986958   2401:4900:cad9:8883… 2401:4900:cad9:8883… DNS   119 Standard query response 0x537c HTTPS youtube.com HTTPS
391 21.986958   2401:4900:cad9:8883… 2401:4900:cad9:8883… DNS   132 Standard query response 0xc317 AAAA youtube.com AAAA 2404:6800:4007:83a::200e
392 21.986958   2401:4900:cad9:8883… 2401:4900:cad9:8883… DNS   120 Standard query response 0x5154 A youtube.com A 142.250.77.110
457 22.255716   2401:4900:cad9:8883… 2401:4900:cad9:8883… DNS   107 Standard query 0xc565 HTTPS www.youtube.com
459 22.255893   2401:4900:cad9:8883… 2401:4900:cad9:8883… DNS   107 Standard query 0xef38 AAAA www.youtube.com
463 22.257243   2401:4900:cad9:8883… 2401:4900:cad9:8883… DNS   107 Standard query 0x21fc A www.youtube.com
476 22.404638   2401:4900:cad9:8883… 2401:4900:cad9:8883… DNS   157 Standard query response 0xc565 HTTPS www.youtube.com CNAME youtube-ui.l.google.com HTTPS
477 22.404638   2401:4900:cad9:8883… 2401:4900:cad9:8883… DNS   254 Standard query response 0xef38 AAAA www.youtube.com CNAME youtube-ui.l.google.com AAAA 2404:6800:4007:83a::200e AAAA 2404:6800:…
480 22.406470   2401:4900:cad9:8883… 2401:4900:cad9:8883… DNS   398 Standard query response 0x21fc A www.youtube.com CNAME youtube-ui.l.google.com A 142.251.43.142 A 142.250.183.174 A 142.251.221…
563 22.708717   10.58.238.148        10.58.238.252        DNS    71 Standard query 0x747f A i.ytimg.com
564 22.749078   10.58.238.252        10.58.238.148        DNS   231 Standard query response 0x747f A i.ytimg.com A 172.253.118.119 A 74.125.24.119 A 172.217.194.119 A 142.251.10.119 A 64.233.170.…
573 22.760234   2401:4900:cad9:8883… 2401:4900:cad9:8883… DNS   103 Standard query 0xb95e AAAA i.ytimg.com
```

```
    [Calculated window size: 65280]
    [Window size scaling factor: 256]
    Checksum: 0xaa5d [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ [Timestamps]
  ▸ [SEQ/ACK analysis]
    TCP payload (29 bytes)
    [PDU Size: 31]
    TCP segment data (29 bytes)
▸ [2 Reassembled TCP Segments (31 bytes): #372(2), #373(29)]
▾ Domain Name System (query)
    Length: 29
    Transaction ID: 0xc317
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
```

```
0000  00 1d c3 17 01 00 00 01  00 00 00 00 00 00 07 79   ········ ·······y
0010  6f 75 74 75 62 65 03 63  6f 6d 00 00 1c 00 01      outube·c om·····
```

After capturing the packets, I filtered the packets at search bar by typing DNS, these are all the DNS packets.

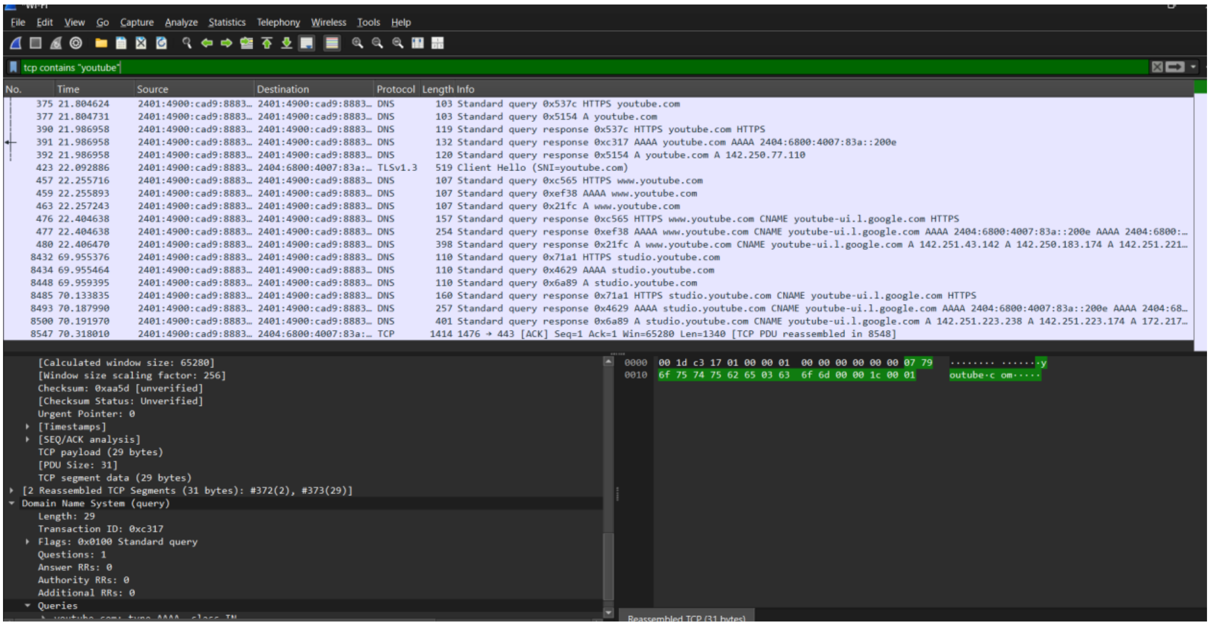
The capture shows both A (IPv4) and AAAA (IPv6) DNS queries for youtube.com. DNS responses returned multiple IP addresses, indicating CDN-based load balancing. The domain www.youtube.com was resolved using a CNAME record pointing to youtube-ui.l.google.com.

When I search youtube url, the browser breaks down the url into different parts and dns will kick off first find the server ip for the request. And send the response in multiple DNS, because the server picks up the fastest and reliable one. This will leads to loadbalancing.

- **A** **-** ip v4 address
- **AAA** **-** ip v6 address

We can se the responses are in AAA which shows that the response in ipv6 address. Because ipv6 have lot of address due to growth of digital gadgets usage we are moving towards ipv6 address.

2. TCP


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp contains "youtube"

```
No.   Time       Source                Destination           Protocol Length Info
  375 21.804624  2401:4900:cad9:8883… 2401:4900:cad9:8883… DNS       103 Standard query 0x537c HTTPS youtube.com
  377 21.804731  2401:4900:cad9:8883… 2401:4900:cad9:8883… DNS       103 Standard query 0x5154 A youtube.com
  390 21.986958  2401:4900:cad9:8883… 2401:4900:cad9:8883… DNS       119 Standard query response 0x537c HTTPS youtube.com HTTPS
  391 21.986958  2401:4900:cad9:8883… 2401:4900:cad9:8883… DNS       132 Standard query response 0xc317 AAAA youtube.com AAAA 2404:6800:4007:83a::200e
  392 21.986958  2401:4900:cad9:8883… 2401:4900:cad9:8883… DNS       120 Standard query response 0x5154 A youtube.com A 142.250.77.110
  423 22.092886  2401:4900:cad9:8883… 2404:6800:4007:83a:… TLSv1.3   519 Client Hello (SNI=youtube.com)
  457 22.255716  2401:4900:cad9:8883… 2401:4900:cad9:8883… DNS       107 Standard query 0xc565 HTTPS www.youtube.com
  459 22.255893  2401:4900:cad9:8883… 2401:4900:cad9:8883… DNS       107 Standard query 0xef38 AAAA www.youtube.com
  463 22.257243  2401:4900:cad9:8883… 2401:4900:cad9:8883… DNS       107 Standard query 0x21fc A www.youtube.com
  476 22.404638  2401:4900:cad9:8883… 2401:4900:cad9:8883… DNS       157 Standard query response 0xc565 HTTPS www.youtube.com CNAME youtube-ui.l.google.com HTTPS
  477 22.404638  2401:4900:cad9:8883… 2401:4900:cad9:8883… DNS       254 Standard query response 0xef38 AAAA www.youtube.com CNAME youtube-ui.l.google.com AAAA 2404:6800:4007:83a::200e AAAA 2404:6800:…
  480 22.406470  2401:4900:cad9:8883… 2401:4900:cad9:8883… DNS       398 Standard query response 0x21fc A www.youtube.com CNAME youtube-ui.l.google.com A 142.251.43.142 A 142.250.183.174 A 142.251.221…
 8432 69.955376  2401:4900:cad9:8883… 2401:4900:cad9:8883… DNS       110 Standard query 0x71a1 HTTPS studio.youtube.com
 8434 69.955464  2401:4900:cad9:8883… 2401:4900:cad9:8883… DNS       110 Standard query 0x4629 AAAA studio.youtube.com
 8448 69.959395  2401:4900:cad9:8883… 2401:4900:cad9:8883… DNS       110 Standard query 0x6a89 A studio.youtube.com
 8485 70.133835  2401:4900:cad9:8883… 2401:4900:cad9:8883… DNS       160 Standard query response 0x71a1 HTTPS studio.youtube.com CNAME youtube-ui.l.google.com HTTPS
 8493 70.187990  2401:4900:cad9:8883… 2401:4900:cad9:8883… DNS       257 Standard query response 0x4629 AAAA studio.youtube.com CNAME youtube-ui.l.google.com AAAA 2404:6800:4007:83a::200e AAAA 2404:68…
 8500 70.191970  2401:4900:cad9:8883… 2401:4900:cad9:8883… DNS       401 Standard query response 0x6a89 A studio.youtube.com CNAME youtube-ui.l.google.com A 142.251.223.238 A 142.251.223.174 A 172.217…
 8547 70.318010  2401:4900:cad9:8883… 2404:6800:4007:83a:… TCP      1414 1476 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=1340 [TCP PDU reassembled in 8548]
```

```
    [Calculated window size: 65280]
    [Window size scaling factor: 256]
    Checksum: 0xaa5d [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ [Timestamps]
  ▸ [SEQ/ACK analysis]
    TCP payload (29 bytes)
    [PDU Size: 31]
    TCP segment data (29 bytes)
▸ [2 Reassembled TCP Segments (31 bytes): #372(2), #373(29)]
▾ Domain Name System (query)
    Length: 29
    Transaction ID: 0xc317
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
```

```
0000  00 1d c3 17 01 00 00 01  00 00 00 00 00 00 07 79   ········ ·······y
0010  6f 75 74 75 62 65 03 63  6f 6d 00 00 1c 00 01      outube·c om·····
```

TCP- Transmission Control Protocol, is more secure and reliable connection, it follows 3 way handshake like data, acknowledgement, data. It sends the data after the acknowledgement of previous frame.

Here the server has an established connection earlier, packet 1447-143. Client has established the connection through text called SNI, visible because TLS is not full established.

Here tcp takes place instead of udp because pf the reliability and no place buffering while streaming a video.

- TLS data is split across multiple TCP packets
- Wireshark reassembles them
- This packet alone does NOT contain full TLS message

TLS Is an abbreviation of Transmission Layer Securiy, it is used to secure the application that works on public networks, without security Anyone can see our data. HTTP is an insecure protocol any one can access the plain text, to resolve this HTTPS came in existence. TLS make wrap with HTTP to create the HTTPS.