LAB-1

ZOOM:

1.The protocols used by zoom are TCP,TLS,DNS,SSDP,QUIC,UDP.

Here's a brief explanation of each:

TCP (Transmission Control Protocol)

- A transport-layer protocol that provides reliable, connection-oriented communication over IP networks.
- Ensures data is delivered in the correct order and retransmits lost or corrupted packets.

TLS (Transport Layer Security)

- A cryptographic protocol that provides end-to-end encryption and authentication over a network.
- Typically used to secure web traffic (HTTPS) and ensure the integrity of data in transit.

DNS (Domain Name System)

- A protocol that translates human-readable domain names into IP addresses.
- Acts as a phonebook for the internet, allowing devices to communicate with each other using easy-to-remember domain names.

SSDP (Simple Service Discovery Protocol)

- A protocol used for discovering and advertising services on a network.
- Allows devices to announce their presence and capabilities, making it easier for other devices to find and use them.

QUIC (Quick UDP Internet Connections)

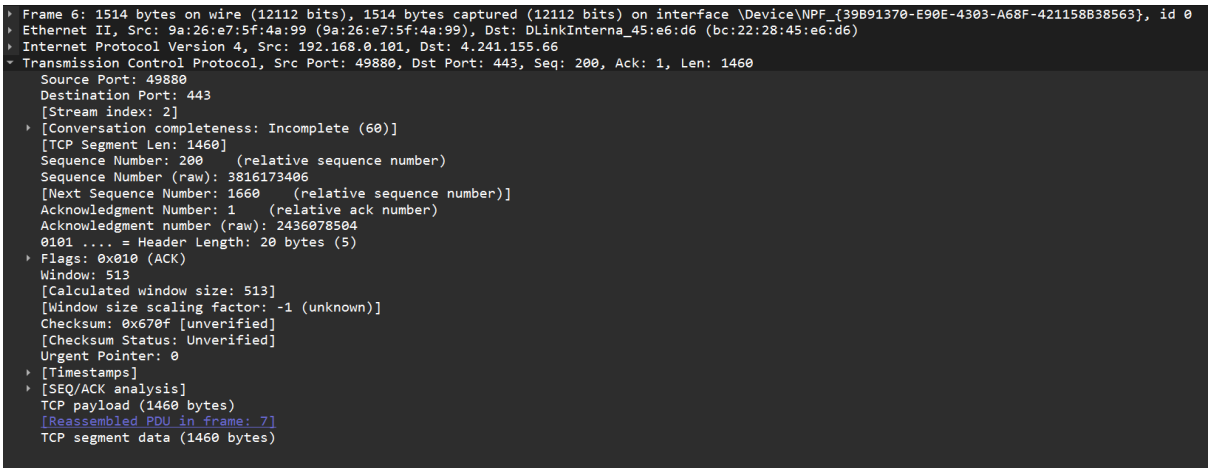
- A transport-layer protocol designed by Google to improve the performance and security of web traffic.
- Aims to reduce latency and improve multiplexing, making it a potential replacement for TCP and TLS.

UDP (User Datagram Protocol)

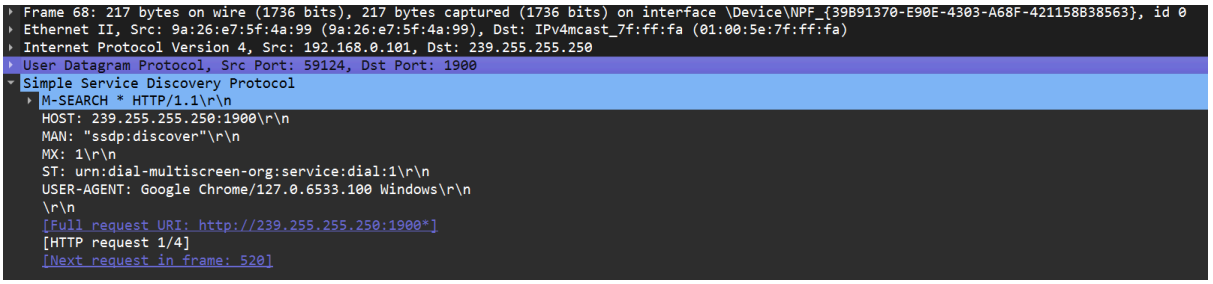
- A transport-layer protocol that provides best-effort, connectionless communication over IP networks.
- Does not guarantee delivery or order of packets, but is often used for applications that require fast transmission and can tolerate some packet loss (e.g., online gaming, video streaming).

2.

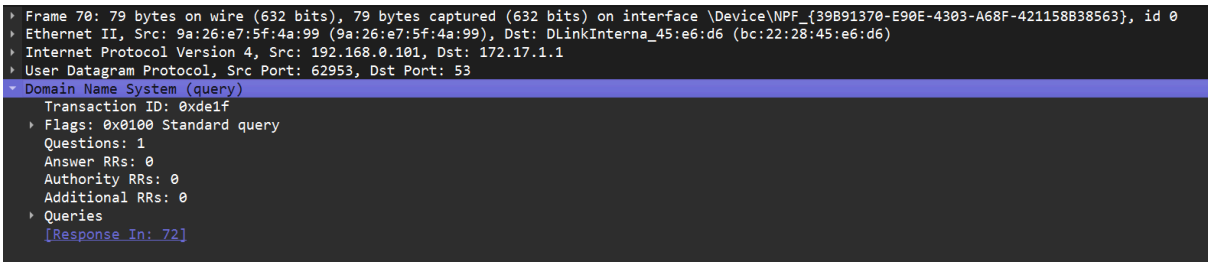
TCP



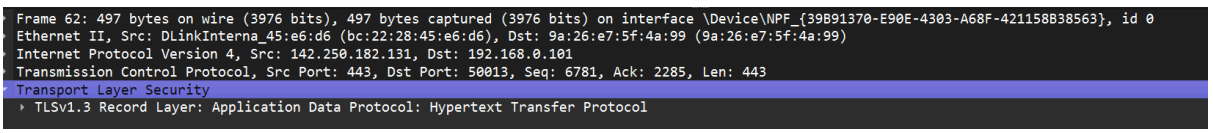
SSDP



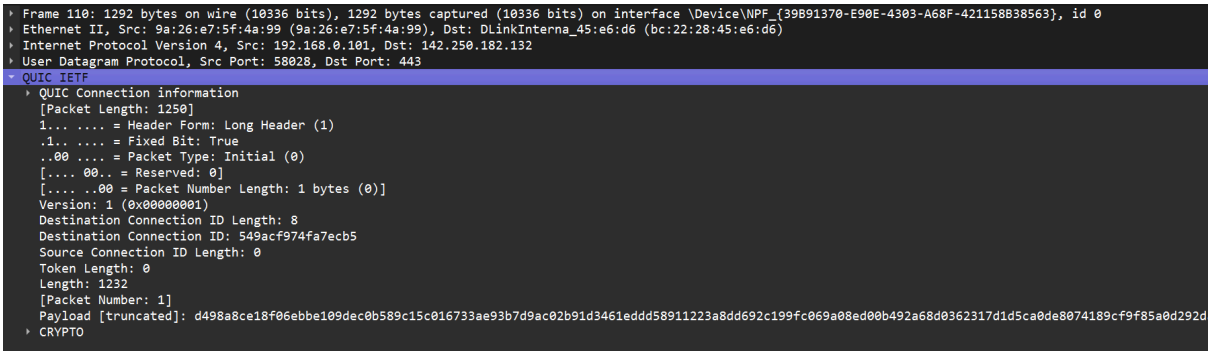
DNS



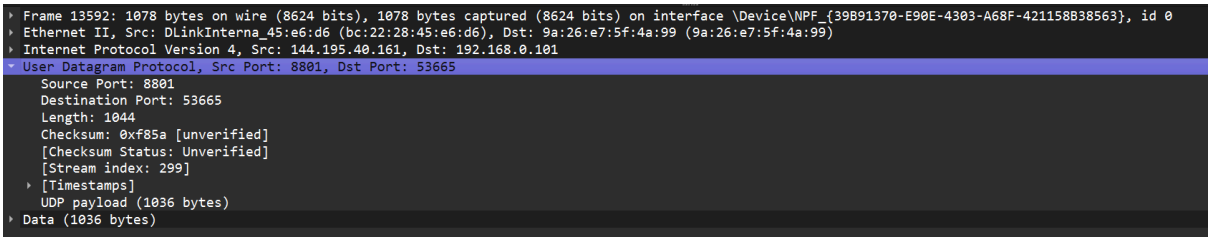
TLS



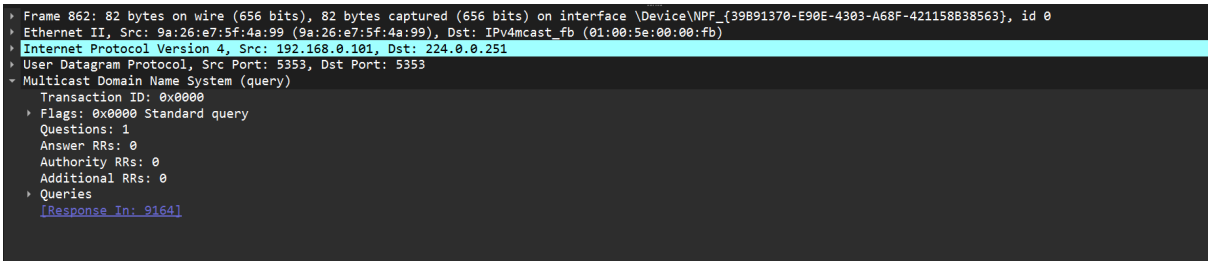
QUIC



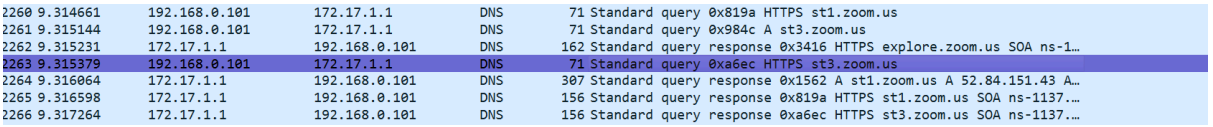
UDP



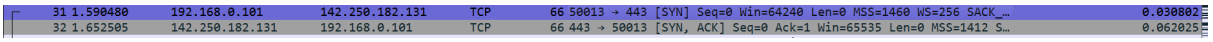
mDNS



3.



There is a DNS query and response (handshaking happens.)



A TCP SYN request is followed up by a TCP SYN,ACK response leading to establishment of a connection with the zoom server.

4. **DNS (Domain Name System):**DNS helps resolve the Zoom domain name to an IP address, allowing your device to connect to Zoom's servers.

TCP (Transmission Control Protocol):TCP helps establish and maintain a reliable connection between your device and Zoom's servers, allowing data to be transmitted back and forth.

TLSv1.3 (Transport Layer Security):TLSv1.3 helps establish a secure communication channel over TCP, allowing sensitive data (such as login credentials) to be transmitted securely.

UDP (User Datagram Protocol):UDP helps transmit real-time data (such as video and audio) during the call, allowing for low-latency communication.

SSDP (Simple Service Discovery Protocol):SSDP is not directly used in Zoom, but it is a protocol used for discovering and advertising services on a network. In the context of Zoom, it could be used to discover and connect to peripherals such as cameras and microphones.

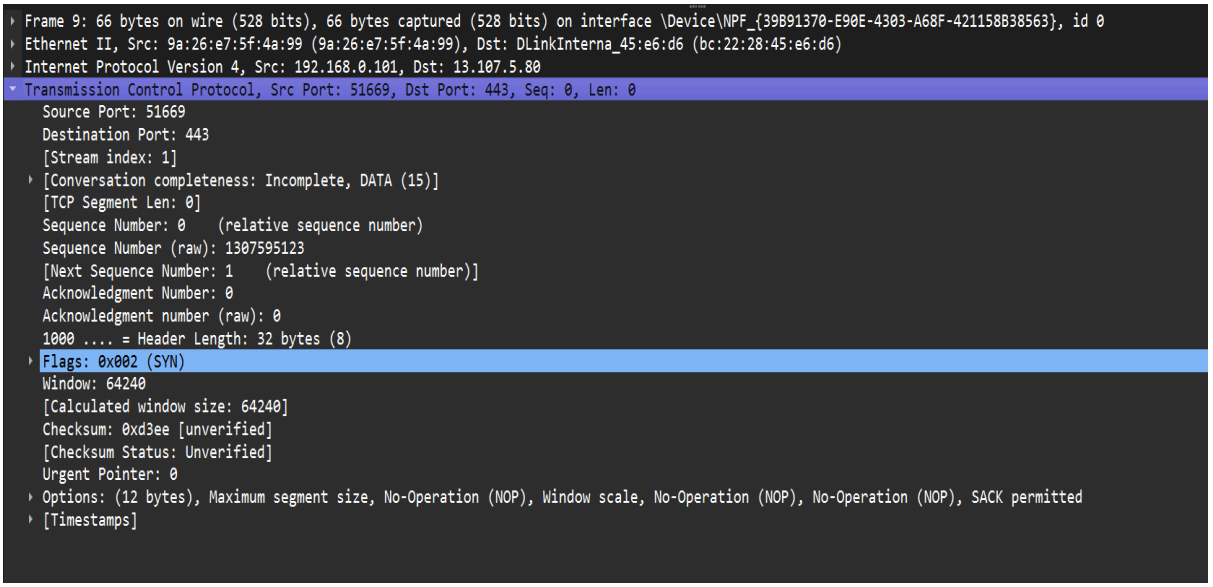
5.

Statistic	Value
Throughput	5.09b/sec
Round-Trip Time (RTT)	124.05ms
Average Packet Size	860.03Bytes
Min Packet Size	42 Bytes
Max Packet Size	1514 Bytes
Number of Packets Lost	5348.2
Number of UDP Packets	41741
Number of TCP Packets	11727

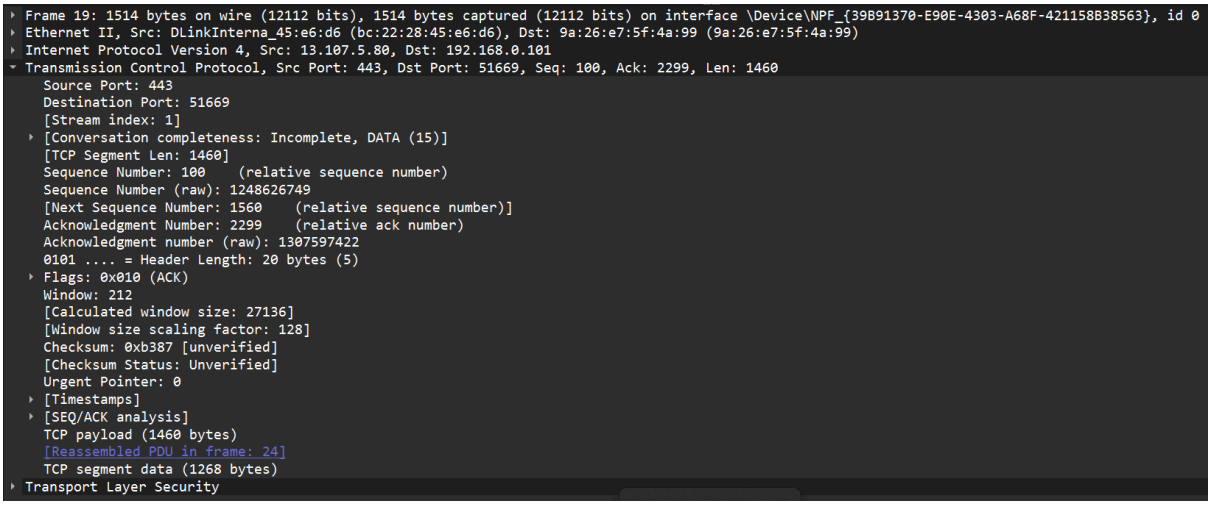
6.Zoom uses multiple ip addresses so that by distributing traffic across multiple IP addresses, Zoom can load balance their infrastructure more efficiently, ensuring that no single server or cluster becomes overwhelmed.

YOUTUBE DOWNLOAD:

1.Protocols used are TCP,DNS and TSLv1.3
TCP:



TSL:



3,4.To download a video from YouTube, the client (browser or software) establishes a connection with the server using:

1. TCP 3-way handshake: SYN, SYN-ACK, and ACK packets.
2. TLS handshake: Client Hello, Server Hello, Certificate, Client Key Exchange, and Change Cipher Spec.
3. Encrypted data transfer: Client sends HTTP requests, server responds with encrypted video data.
4. TCP segmentation and reassembly: Client receives and reassembles video data.
5. Decryption and video playback: Client decrypts data, passes to video player.

5.the observed values in your answer, preferably using tables.

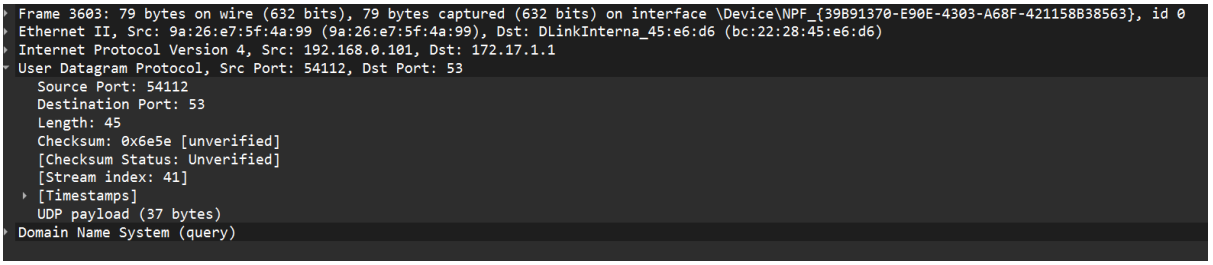
Statistic	Value
Throughput	22.25bps
Round-Trip Time (RTT)	509.677ms
Average Packet Size	1135.13 Bytes
Min Packet Size	42 Bytes
Max Packet Size	1514 Bytes
Number of Packets Lost	------
Number of UDP Packets	41349
Number of TCP Packets	643
Number of Responses per Request	-------

6. Data is transferred from a single location.

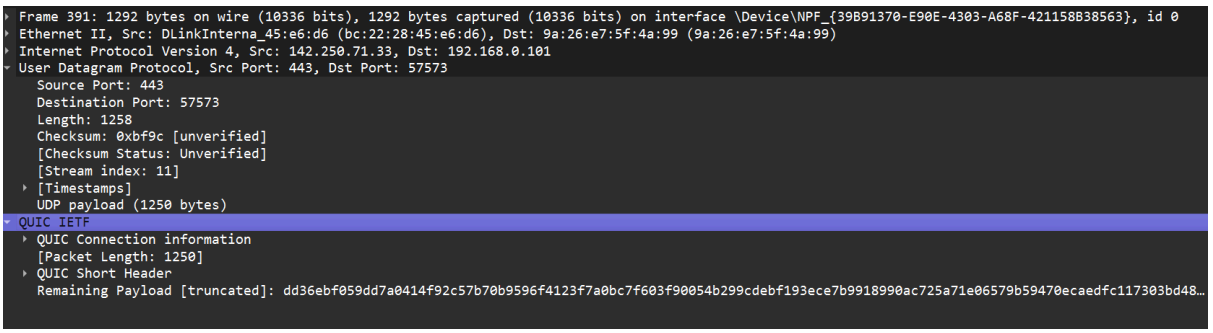
NPTEL:

Protocols used are SSDP,TCP, TLS, UDP,QUIC

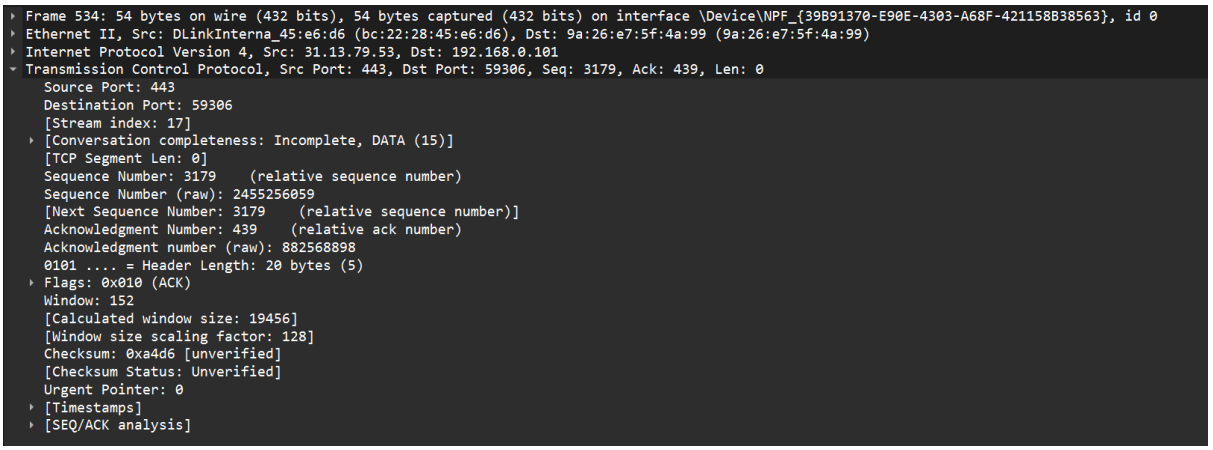
DNS



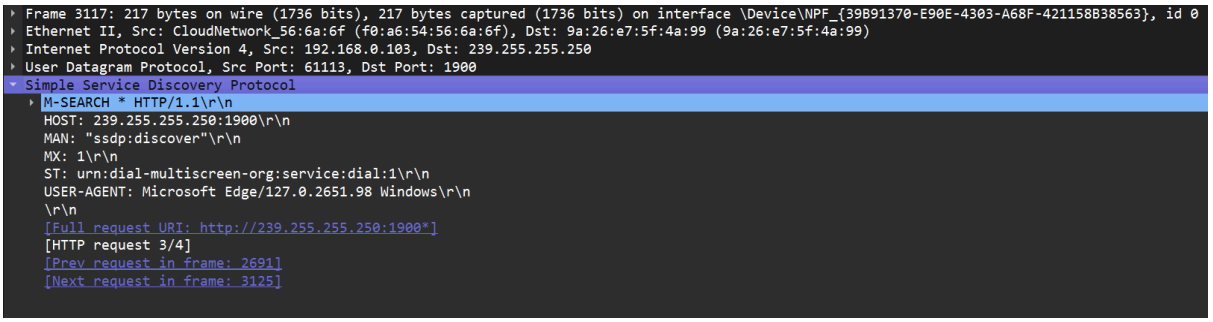
QUIC



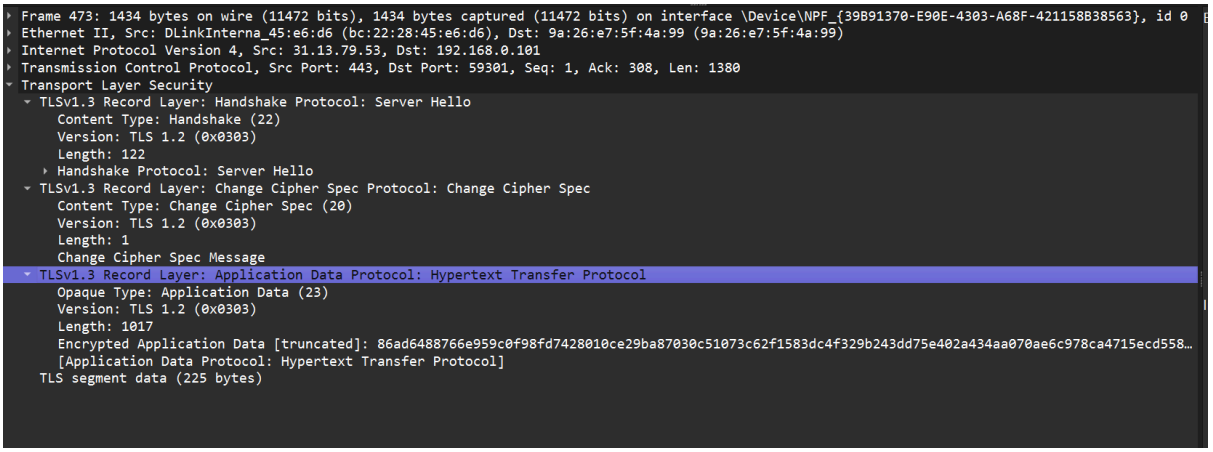
TCP



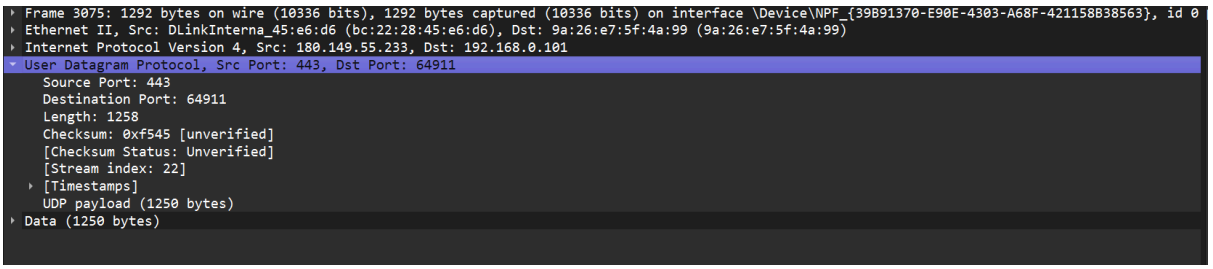
SSDP



TLS:



UDP:



3,4.

- **SSDP**: Enables devices and services to discover each other on a network, facilitating automatic service discovery and integration.
- **DNS**: Translates human-readable domain names into IP addresses, allowing applications to locate and connect to servers using easy-to-remember names.
- **TCP**: Provides reliable, ordered, and error-checked delivery of data, ensuring that application data is transmitted accurately and in the correct sequence.
- **UDP**: Supports fast, low-overhead data transmission suitable for real-time applications where speed is crucial and occasional data loss is acceptable.
- **TLSv1.3**: Ensures secure data transmission by encrypting communication between clients and servers, protecting sensitive information from eavesdropping and tampering.
- **QUIC**: Improves web performance by reducing latency and optimising data transfer over UDP, enhancing the speed and reliability of application interactions.

5.

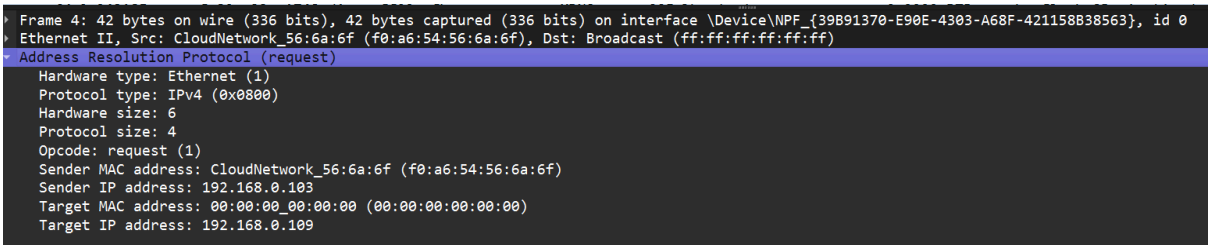
Statistic	Value
Throughput	21.25B/sec
Round-Trip Time (RTT)	297.6ms
Average Packet Size	91295Bytes
Min Packet Size	1142 Bytes
Max Packet Size	91514 Bytes
Number of Packets Lost	------
Number of UDP Packets	3841
Number of TCP Packets	796
Number of Responses per Request	-------

6. As we can see this uses multiple ip addresses for load balancing and redundancy.

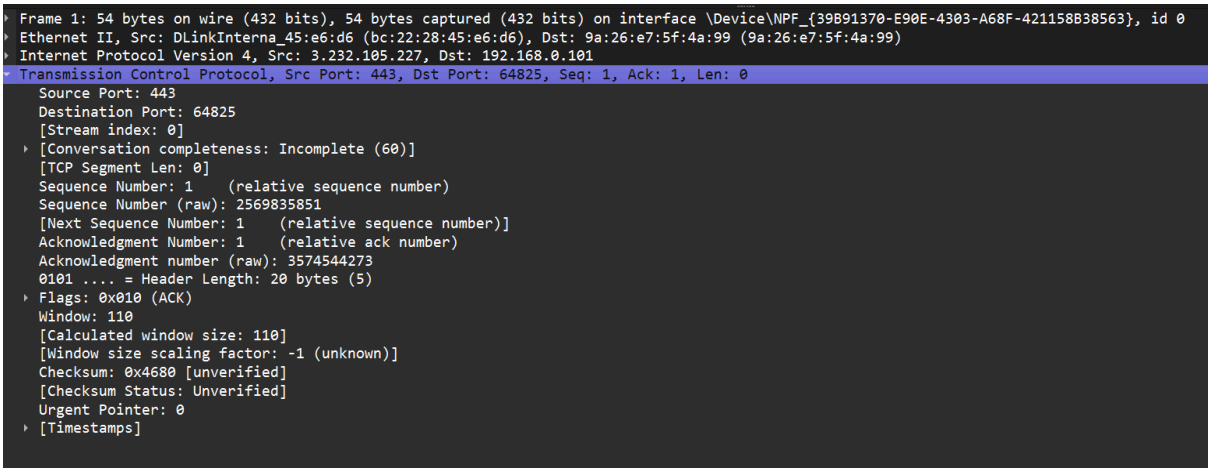
MS TEAMS:

Protocols used are TCP,ARP,TLS,DNS,UDP,STUN,SSDP

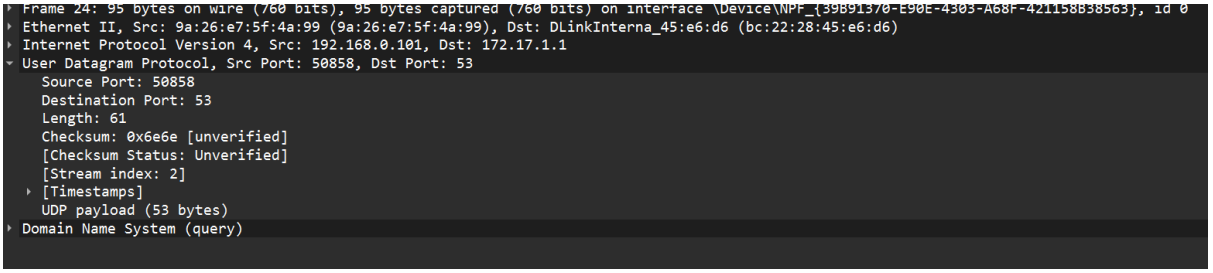
ARP:



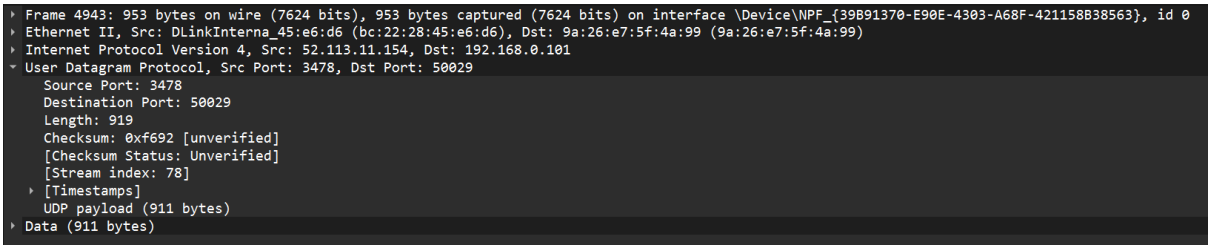
TCP:



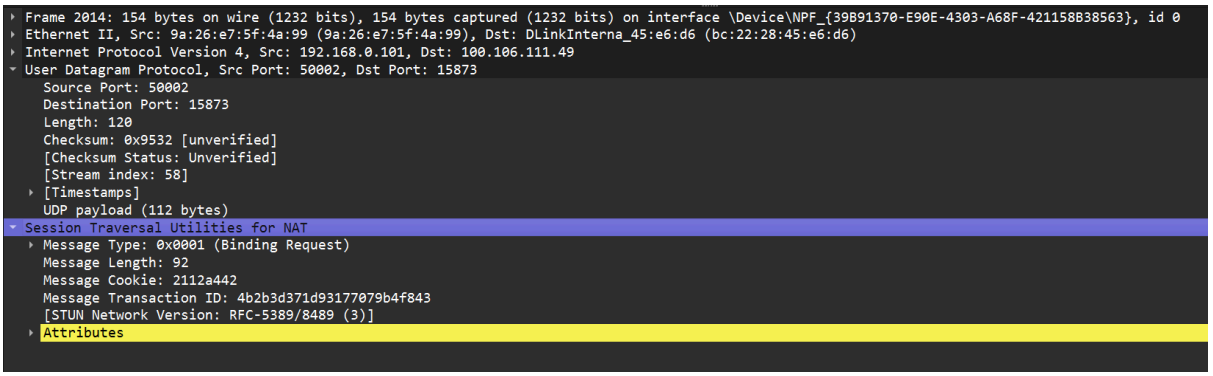
DNS



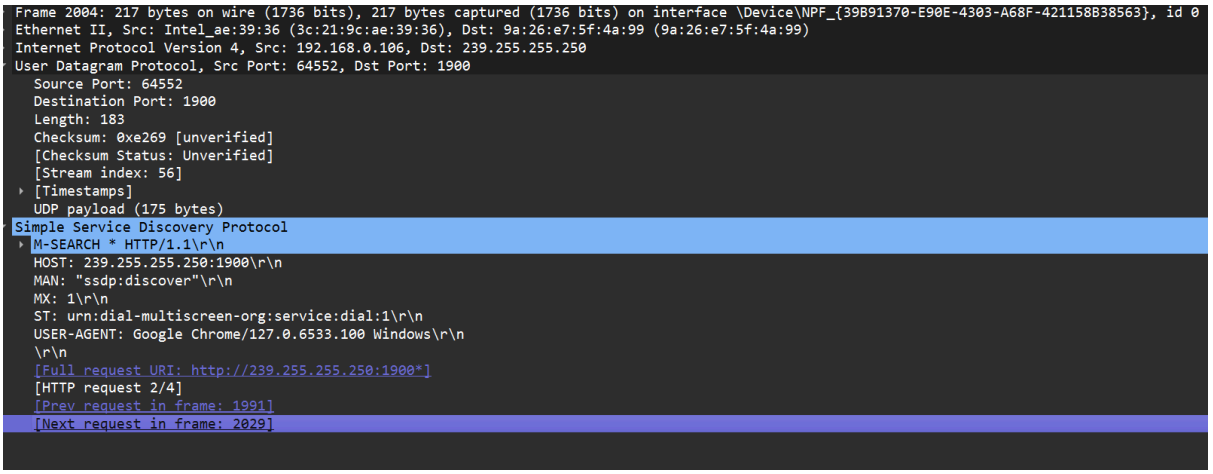
UDP:



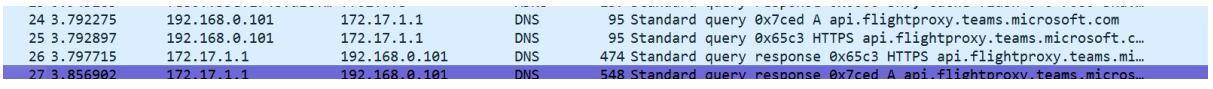
STUN:



SSDP:



3,4.The following are the DNS and TLS queries and responses.



```
40 4.300824     192.168.0.101      20.190.145.143     TLSv1.3   357 Client Hello (SNI=login.microsoftonline.com)
41 4.378541     20.190.145.143     192.168.0.101      TLSv1.3   153 Hello Retry Request, Change Cipher Spec
```

```
2000 21.977656     192.168.0.101      14.139.82.6        STUN      154 Binding Request user: LTwe:chVv
2001 21.977952     192.168.0.101      14.139.82.6        STUN      154 Binding Request user: MCXc:OloF
2002 22.290346     192.168.0.101      14.139.82.6        STUN      154 Binding Request user: LTwe:chVv
2003 22.290593     192.168.0.101      14.139.82.6        STUN      154 Binding Request user: MCXc:OloF
```

STUN protocols play a crucial role in Microsoft Teams calls, particularly in establishing and maintaining audio and video connections. In MS Teams, STUN is used to traverse Network Address Translation (NAT) and firewalls, allowing devices behind a NAT to communicate with each other.

Here's a high-level overview of how STUN is used in MS Teams calls:

1. Initial Connection Establishment: When a user initiates a Teams call, the client sends a SIP (Session Initiation Protocol) request to the Teams server. The server responds with a SIP response containing the IP address and port of the A/V Edge Server.
2. STUN Binding Request: The Teams client sends a STUN binding request to the A/V Edge Server to establish a binding between the client's internal IP address and a public IP address. This binding is necessary for NAT traversal.
3. STUN Binding Response: The A/V Edge Server responds with a STUN binding response, which includes the public IP address and port that the client can use to communicate with the server.
4. Media Session Establishment: The Teams client and A/V Edge Server establish a media session using the public IP address and port obtained through STUN. This media session is used for audio and video communication.
5. TURN (Traversal Using Relays around NAT) Server: If the client is behind a symmetric NAT or a firewall that blocks incoming traffic, the Teams client may need to use a TURN server to relay audio and video traffic. The TURN server acts as a relay between the client and the A/V Edge Server.

5.

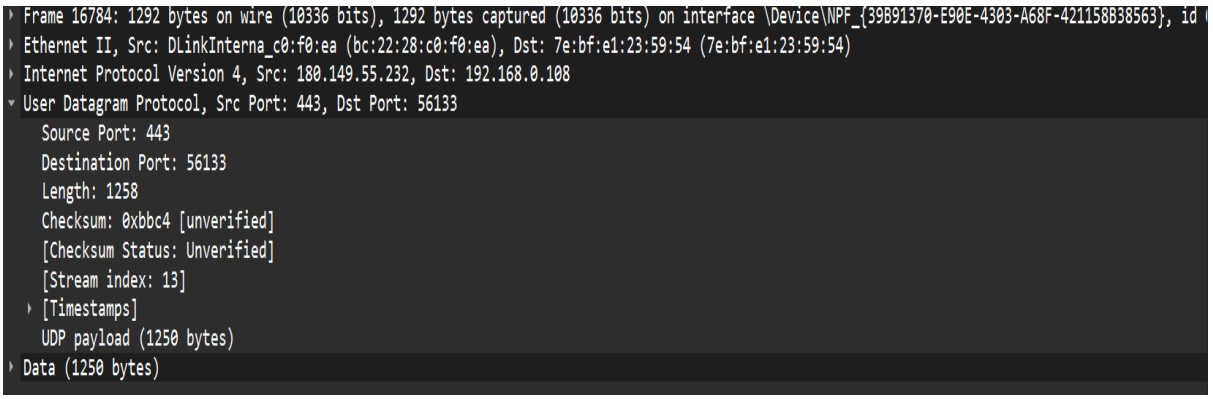
Statistic	Value
Throughput	6.754/sec
Round-Trip Time (RTT)	7.7ms
Average Packet Size	817.05 Bytes
Min Packet Size	42 Bytes
Max Packet Size	1454 Bytes

Number of Packets Lost	------
Number of UDP Packets	3891
Number of TCP Packets	4504
Number of Responses per Request	-------

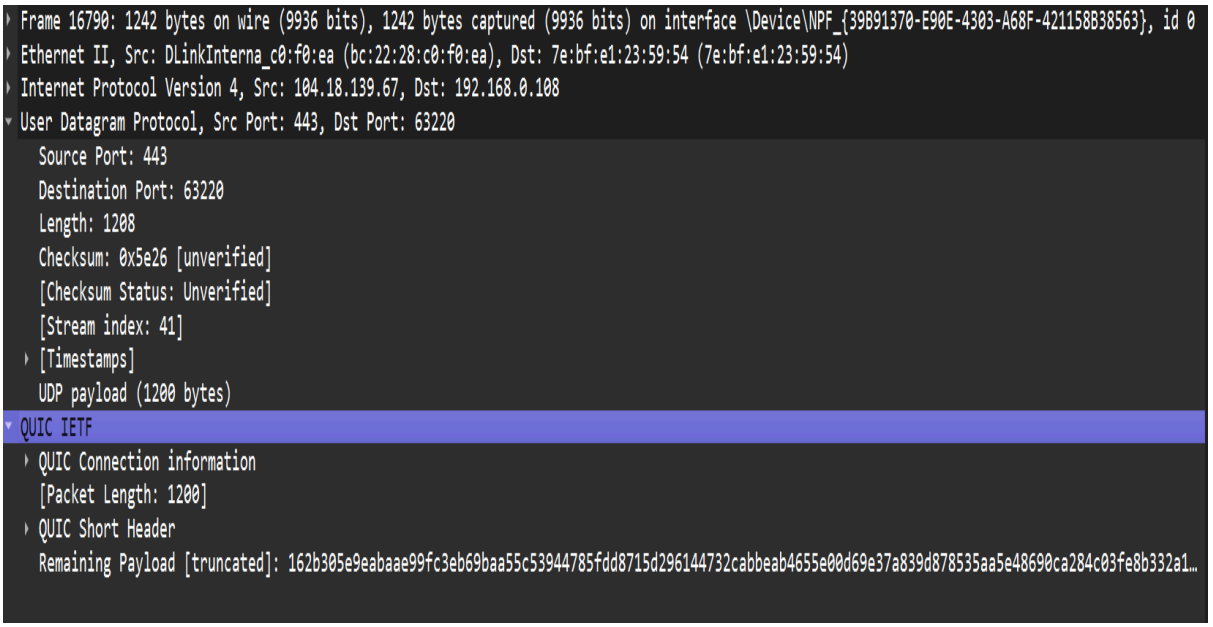
6. It uses different ip addresses for the same reasons stated above.

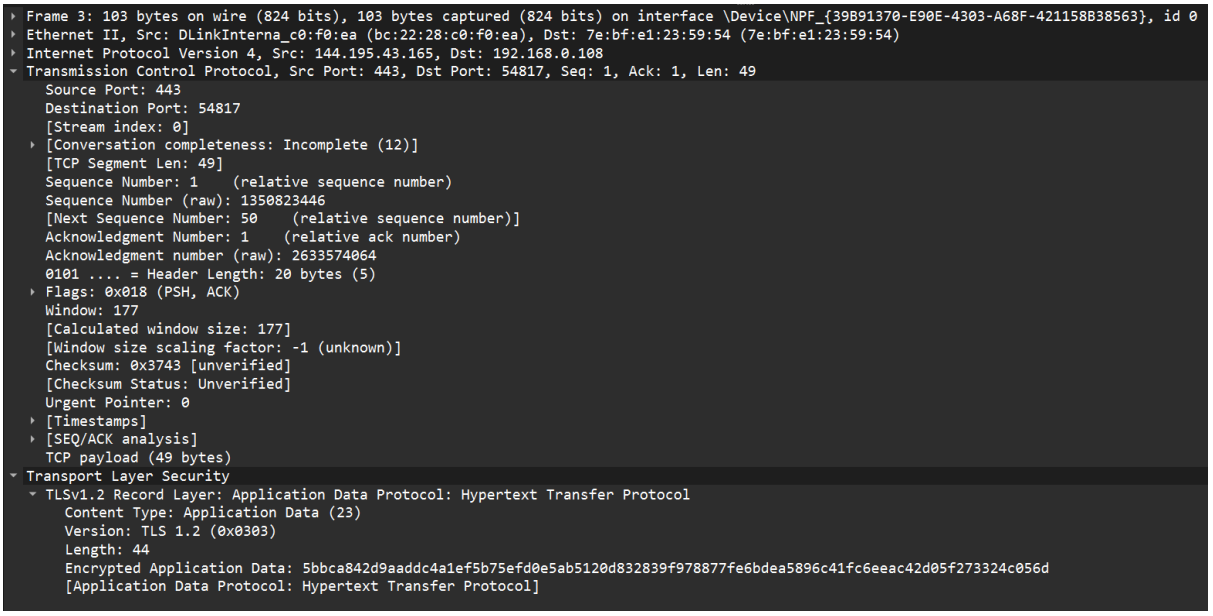
ONLINE GAMES:

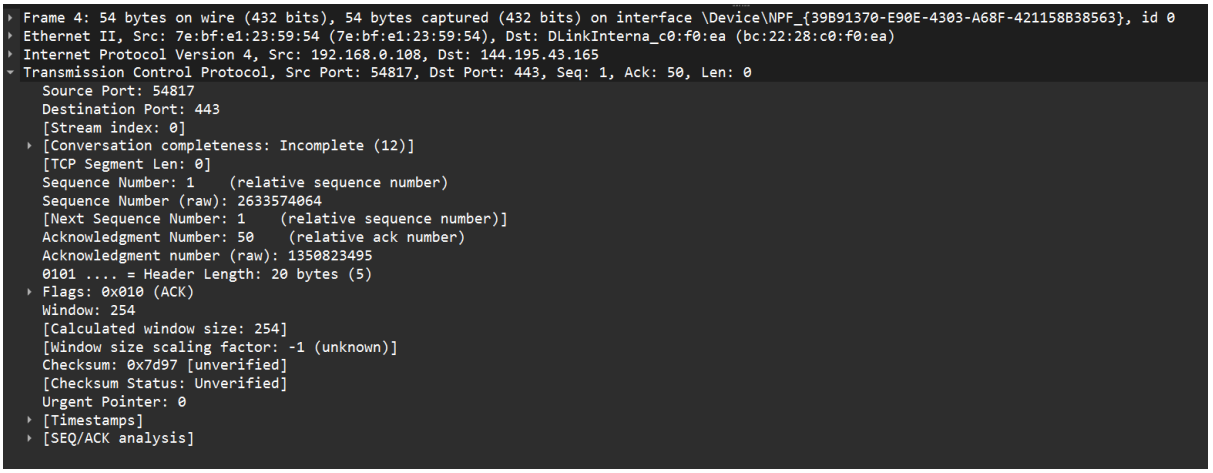
1.Protocols used are TCP,TLS,UDP,QUIC.
2.
UDP:



QUIC:


Frame 16790: 1242 bytes on wire (9936 bits), 1242 bytes captured (9936 bits) on interface \Device\NPF_{39B91370-E90E-4303-A68F-421158B38563}, id 0
Ethernet II, Src: DLinkInterna_c0:f0:ea (bc:22:28:c0:f0:ea), Dst: 7e:bf:e1:23:59:54 (7e:bf:e1:23:59:54)
Internet Protocol Version 4, Src: 104.18.139.67, Dst: 192.168.0.108
User Datagram Protocol, Src Port: 443, Dst Port: 63220
Source Port: 443
Destination Port: 63220
Length: 1208
Checksum: 0x5e26 [unverified]
[Checksum Status: Unverified]
[Stream index: 41]
[Timestamps]
UDP payload (1200 bytes)
QUIC IETF
QUIC Connection information
[Packet Length: 1200]
QUIC Short Header
Remaining Payload [truncated]: 162b305e9eabaae99fc3eb69baa55c53944785fdd8715d296144732cabbeab4655e00d69e37a839d878535aa5e48690ca284c03fe8b332a1…


Frame 3: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface \Device\NPF_{39B91370-E90E-4303-A68F-421158B38563}, id 0
Ethernet II, Src: DLinkInterna_c0:f0:ea (bc:22:28:c0:f0:ea), Dst: 7e:bf:e1:23:59:54 (7e:bf:e1:23:59:54)
Internet Protocol Version 4, Src: 144.195.43.165, Dst: 192.168.0.108
Transmission Control Protocol, Src Port: 443, Dst Port: 54817, Seq: 1, Ack: 1, Len: 49
Source Port: 443
Destination Port: 54817
[Stream index: 0]
[Conversation completeness: Incomplete (12)]
[TCP Segment Len: 49]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 1350823446
[Next Sequence Number: 50 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 2633574064
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 177
[Calculated window size: 177]
[Window size scaling factor: -1 (unknown)]
Checksum: 0x3743 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
TCP payload (49 bytes)
Transport Layer Security
TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
Content Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 44
Encrypted Application Data: 5bbca842d9aaddc4a1ef5b75efd0e5ab5120d832839f978877fe6bdea5896c41fc6eeac42d05f273324c056d
[Application Data Protocol: Hypertext Transfer Protocol]


Frame 4: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{39B91370-E90E-4303-A68F-421158B38563}, id 0
Ethernet II, Src: 7e:bf:e1:23:59:54 (7e:bf:e1:23:59:54), Dst: DLinkInterna_c0:f0:ea (bc:22:28:c0:f0:ea)
Internet Protocol Version 4, Src: 192.168.0.108, Dst: 144.195.43.165
Transmission Control Protocol, Src Port: 54817, Dst Port: 443, Seq: 1, Ack: 50, Len: 0
Source Port: 54817
Destination Port: 443
[Stream index: 0]
[Conversation completeness: Incomplete (12)]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 2633574064
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 50 (relative ack number)
Acknowledgment number (raw): 1350823495
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window: 254
[Calculated window size: 254]
[Window size scaling factor: -1 (unknown)]
Checksum: 0x7d97 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]

The above are TLS and TCP.

3,4:TCP (Transmission Control Protocol): TCPis used for reliable, ordered communication between clients and servers. In chess.com, TCP might be used for:

- Initial connection establishment: When a user logs in, TCP is used to establish a connection between the client and the server.
- Game state updates: TCP is used to send game state updates, such as moves, to the server and other connected clients.
- Chat and messaging: TCP is used for chat and messaging between players.

TLS (Transport Layer Security): TLS is used to encrypt and secure communication between clients and servers. In chess.com, TLS might be used for:

- Secure authentication: TLS is used to encrypt authentication credentials, such as usernames and passwords, when users log in.
- Secure game data: TLS is used to encrypt game data, such as moves and game state, to prevent eavesdropping and tampering.

UDP (User Datagram Protocol): UDP is used for fast, unreliable communication between clients and servers. In chess.com, UDP might be used for:

- Real-time game updates: UDP is used to send real-time game updates, such as piece movements, to connected clients.
- Voice chat: UDP is used for voice chat between players.

QUIC (Quick UDP Internet Connections): QUIC is a modern transport protocol that provides a balance between reliability and performance. In chess.com, QUIC might be used for:

- Low-latency game updates: QUIC is used to send low-latency game updates, such as piece movements, to connected clients.
- Real-time analytics: QUIC is used to send real-time analytics data, such as player behaviour and game metrics, to the server.

5.

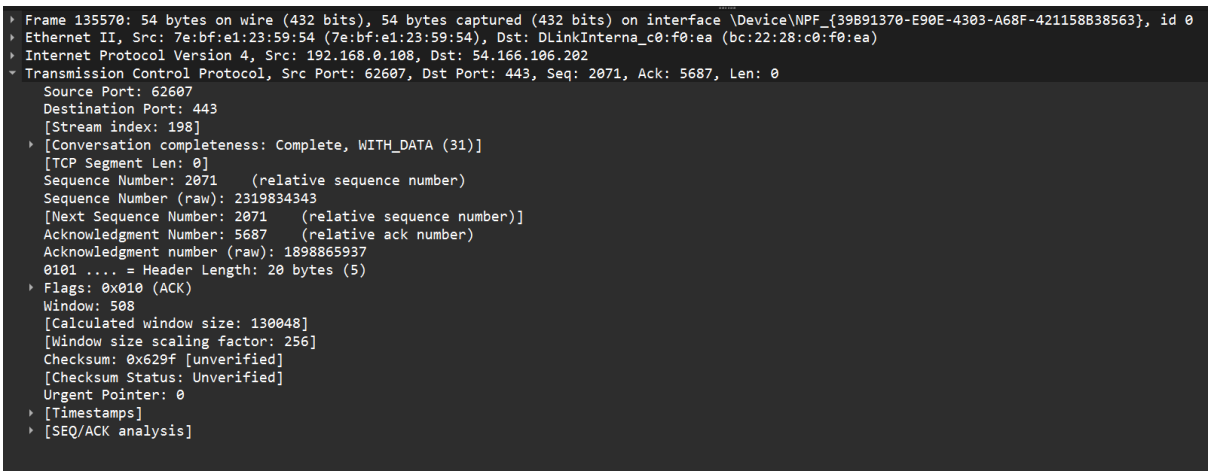
Statistic	Value
Throughput	1.437b/sec
Round-Trip Time (RTT)	14.9ms
Average Packet Size	736.89Bytes
Min Packet Size	—--
Max Packet Size	—---
Number of Packets Lost	------
Number of UDP Packets	13737
Number of TCP Packets	5648
Number of Responses per Request	-------

6.same ip address is used.

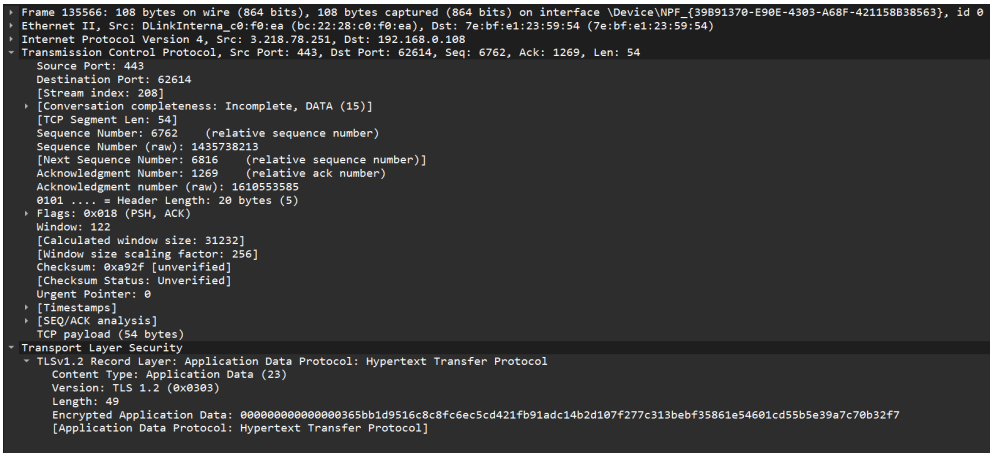
DROPBOX:

1.Protocols used are TCP,TLS.

TCP:



TLS:



Dropbox uses TCP and TLS to establish secure and reliable connections between clients and servers. Here's an overview of how TCP and TLS are used in Dropbox:

TCP (Transmission Control Protocol):

- File uploads and downloads: TCP is used to establish a connection between the client (Dropbox desktop or mobile app) and the server for file uploads and downloads. TCP ensures that files are transferred reliably and in the correct order.
- Syncing: TCP is used to synchronise files and folders between the client and server. When a user makes changes to a file or folder, TCP is used to send the updates to the server and other connected clients.
- API calls: TCP is used to make API calls to the Dropbox server for various operations, such as creating folders, deleting files, and retrieving file metadata.

TLS (Transport Layer Security):

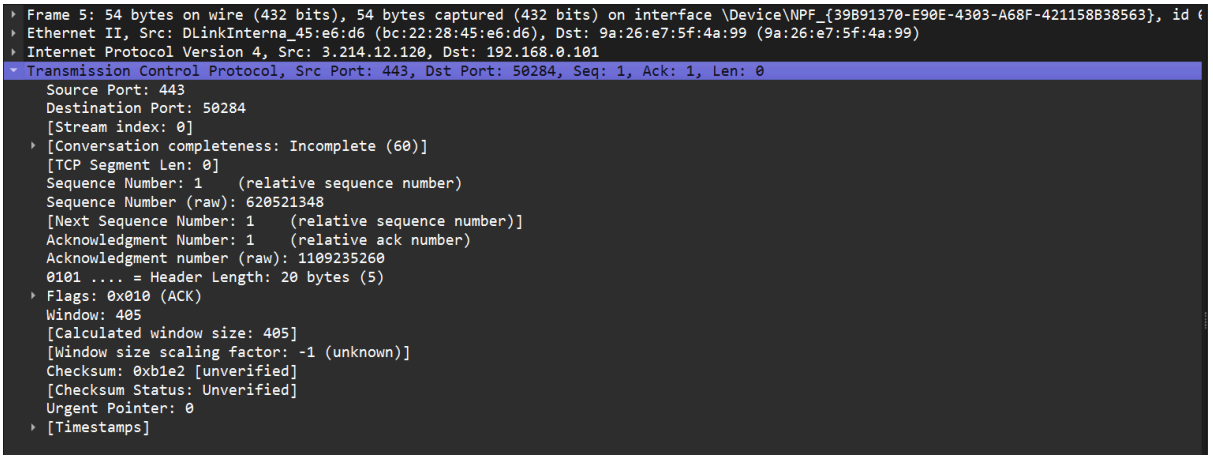
- Encryption: TLS is used to encrypt all data transmitted between the client and server, ensuring that files and metadata are protected from eavesdropping and tampering.
- Authentication: TLS is used to authenticate the client and server, ensuring that the client is communicating with the genuine Dropbox server and not an impersonator.
- Secure key exchange: TLS is used to establish a secure key exchange between the client and server, allowing them to negotiate a shared secret key for encrypting and decrypting data.

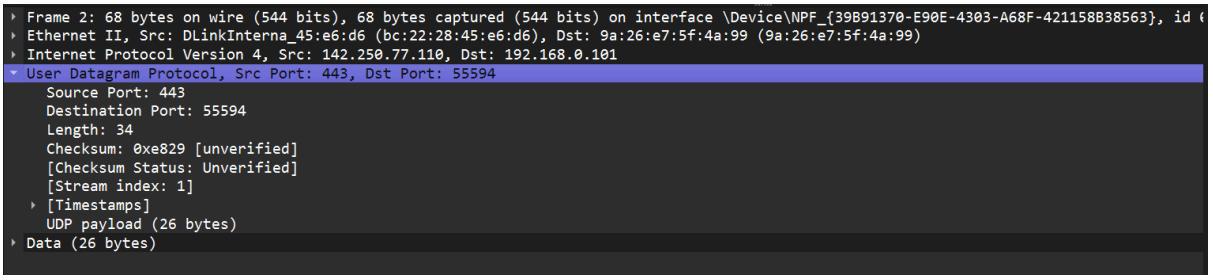
5.

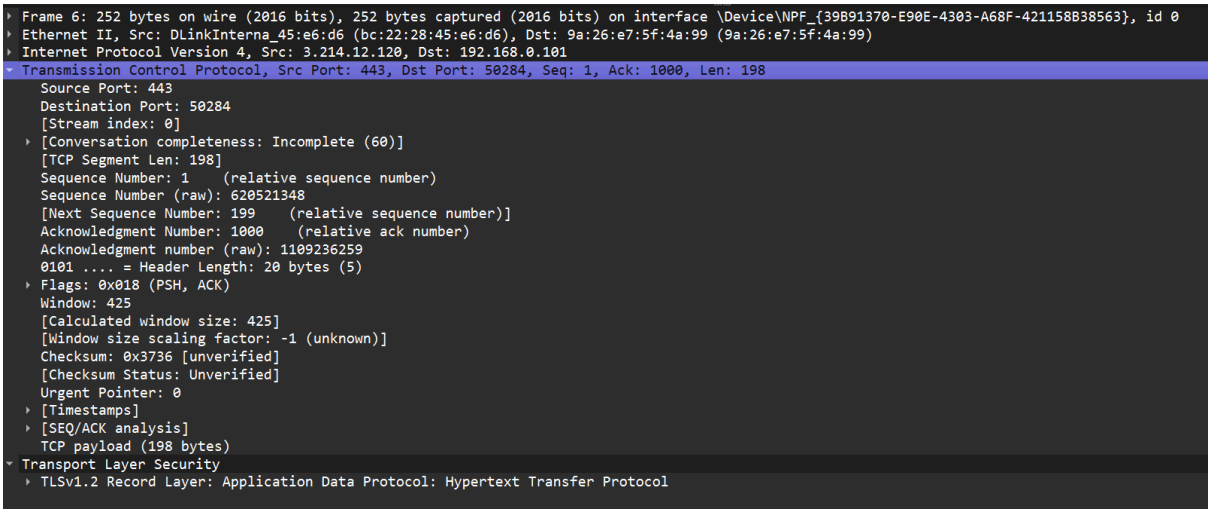
Statistic	Value
Throughput	1.7036b/sec
Round-Trip Time (RTT)	394.772ms
Average Packet Size	1060.89 Bytes
Min Packet Size	—---
Max Packet Size	—---
Number of Packets Lost	------
Number of UDP Packets	1986
Number of TCP Packets	13348
Number of Responses per Request	-------

LIVESTREAM:

1.Protocols used are TCP,TLS,UDP.







3,4:In live streaming, TCP, TLS, and UDP are used in different ways to ensure reliable, secure, and efficient transmission of video and audio data. Here's a breakdown of how each protocol is used:

TCP (Transmission Control Protocol):

Used for metadata and control signals: TCP might be used for transmitting metadata, such as stream metadata, captions, or subtitles, as well as control signals, like pause, play, or seek commands.

TLS (Transport Layer Security):

- Used for encryption and authentication: TLS is used to encrypt and authenticate the live stream, ensuring that only authorized parties can access the content. This is particularly important for protecting sensitive or premium content.
- Used for secure key exchange: TLS is used to establish a secure key exchange between the streaming server and client, allowing them to negotiate a shared secret key for encrypting and decrypting the live stream.

UDP (User Datagram Protocol):

- Used for live video and audio transmission: UDP is commonly used for live streaming because it's a connectionless protocol that prioritises speed and efficiency over reliability. This allows for low-latency transmission of video and audio data.
- Used for Real-Time Protocol (RTP): UDP is used in conjunction with RTP, which provides a standardised way of transmitting real-time data, such as video and audio, over IP networks.
- Error correction and recovery: Since UDP doesn't guarantee delivery or order of packets, error correction and recovery mechanisms, such as Forward Error Correction (FEC) and retransmission, are used to ensure that the live stream is transmitted reliably.

5.

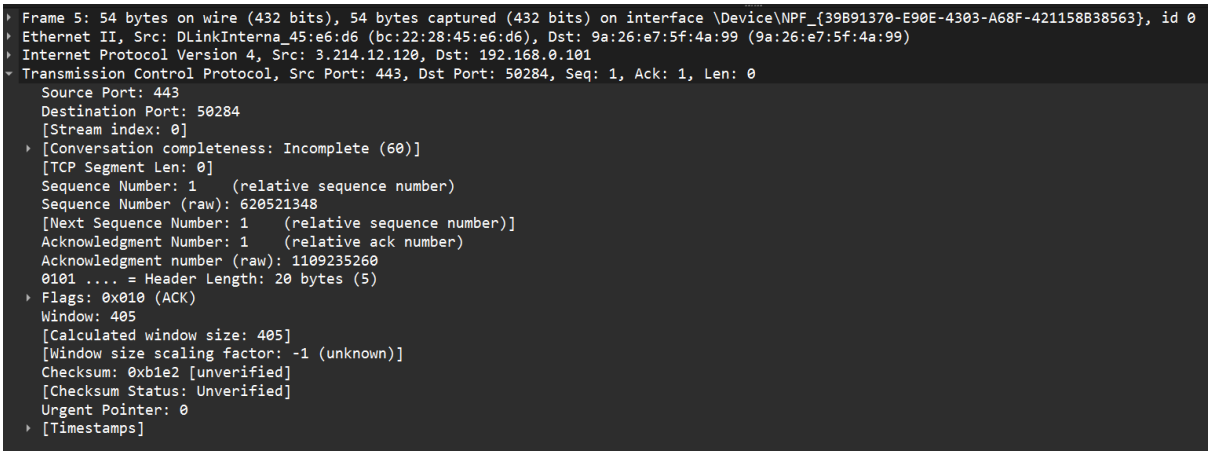
Statistic	Value
Throughput	2.233b/sec
Round-Trip Time (RTT)	566.252ms
Average Packet Size	910.02Bytes
Min Packet Size	—---
Max Packet Size	—-
Number of Packets Lost	------
Number of UDP Packets	14470
Number of TCP Packets	2678
Number of Responses per Request	-------

6. Uses the same ip address.

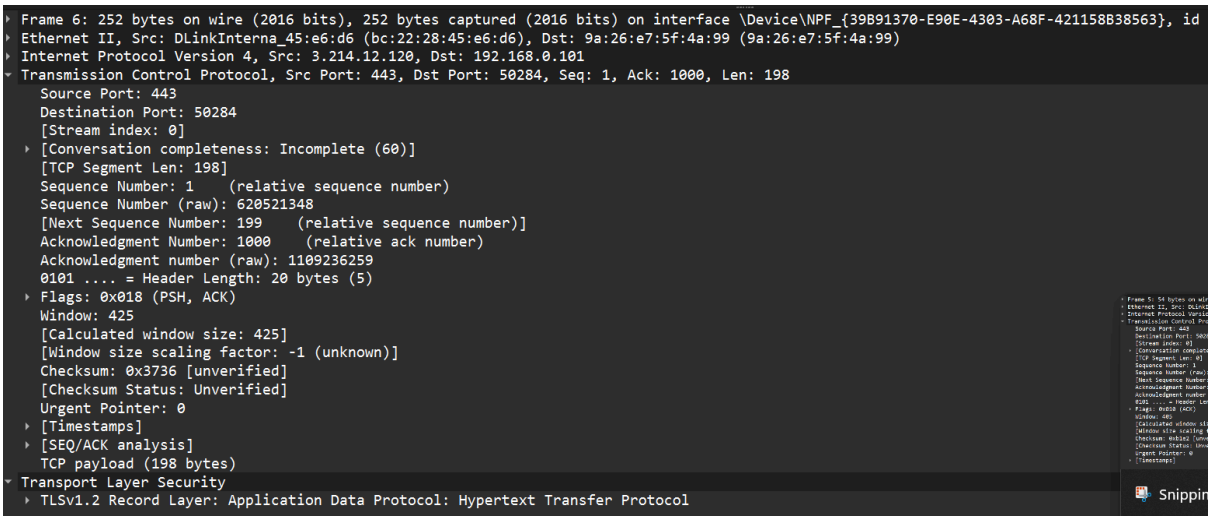
VIDEO UPLOAD:

Protocols used are TCP,TLS,UDP.

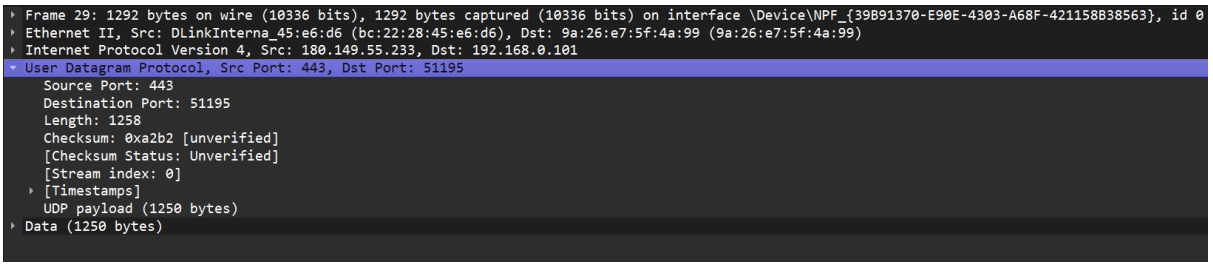
2.TCP:



TLS:



UDP:



YouTube uses a combination of TCP, TLS, UDP, and QUIC to upload videos. Here's a high-level overview of how each protocol is used:

TCP (Transmission Control Protocol):

- Initial connection establishment: TCP is used to establishan initial connection between the client (YouTube uploader) and the server. This connection is used to send metadata, such as video title, description, and tags.
- Chunked upload: TCP is used to upload video chunks, which are small segments of the video file. Each chunk is uploaded separately, and TCP ensures that the chunks are delivered reliably and in the correct order.

TLS (Transport Layer Security):

- Encryption and authentication: TLS is used to encrypt and authenticate the video upload, ensuring that only authorized parties can access the content. This is particularly important for protecting sensitive or premium content.
- Secure key exchange: TLS is used to establish a secure key exchange between the client and server, allowing them to negotiate a shared secret key for encrypting and decrypting the video data.

UDP (User Datagram Protocol):

- Real-time video upload: UDP is used for real-time video upload, where the video is uploaded in real-time, without waiting for the entire file to be uploaded. This allows for faster upload times and reduced latency.
- Error correction and recovery: Since UDP doesn't guarantee delivery or order of packets, error correction and recovery mechanisms, such as Forward Error Correction (FEC) and retransmission, are used to ensure that the video data is transmitted reliably.

QUIC (Quick UDP Internet Connections):

- Low-latency video upload: QUIC is used to upload video data with low latency, which is critical for real-time video upload. QUIC's 0-RTT connection establishment and multiplexing capabilities allow for faster and more efficient video upload.
- Improved error correction: QUIC's built-in error correction mechanisms, such as packet loss detection and retransmission, help to ensure that video data is transmitted reliably and efficiently.

5.

Statistic	Value
Throughput	7.168b/sec
Round-Trip Time (RTT)	499.742ms
Average Packet Size	1096.76Bytes
Min Packet Size	—----
Max Packet Size	—---
Number of Packets Lost	------
Number of UDP Packets	31699
Number of TCP Packets	996
Number of Responses per Request	-------

6.It has multiple addresses.