##### GROUP 31

##### Department of Computer Science

##### NETWORK LAB 2

##### Assignment Title: Network Traffic Analysis with Wireshark

##### Hemant yadav

##### Mohit Kumar

##### Avinav Yadav

##### 210101049 210101068 210101025

##### 11 Oct 2023

### 1. Introduction

The objective of this assignment is to perform a comprehensive network traffic analysis using Wireshark, a powerful network packet capturing and analysis tool. The chosen application for this analysis is "Jio Cinema," a popular online streaming platform. The assignment aims to gain insights into how Jio Cinema functions at the network level, understand the protocols and methods it uses, and evaluate its performance under different network conditions.

Chosen Application: Jio Cinema

Jio Cinema is a digital platform that offers a wide range of movies, TV shows, and exclusive content to its subscribers. As an online streaming service, it relies heavily on efficient network protocols and mechanisms to deliver high-quality content to users.

### Methodology

###### Step 1: Download Wireshark

Open a web browser and navigate to the official Wireshark website: www.wireshark.org.

On the Wireshark website's homepage, you will typically find a prominent download link. Click on it to access the download page.

Choose the appropriate version of Wireshark for your operating system (Windows, macOS, or Linux). Ensure you select the correct version (32-bit or 64-bit) that matches your system.

Click on the download link to start downloading the Wireshark installer. The download may take a few minutes to complete.

###### Step 2: Install Wireshark

Locate the downloaded installer file (e.g., "Wireshark-X.Y.Z.exe" for Windows, or a similar file for your OS) in your Downloads folder or the designated download location.

Double-click the installer file to begin the installation process.

Follow the on-screen instructions provided by the installer. This typically involves accepting the license agreement, choosing installation options (such as whether to install WinPcap or Npcap, which are packet capture libraries), and selecting additional components you want to install along with Wireshark.

During the installation, you may be prompted to install WinPcap or Npcap (packet capture libraries) if they are not already installed on your system. These libraries are essential for Wireshark to capture packets.

Once the installation is complete, you will have the option to launch Wireshark immediately. You can choose to do so or manually launch Wireshark later from your computer's applications menu.

###### Step 3: Set Up Packet Capture

Launch Wireshark by clicking on its icon in the Start Menu (Windows) or Applications (macOS/Linux).

Upon opening Wireshark, you will be presented with a list of available network interfaces. Select the network interface through which you want to capture packets (e.g., Wi-Fi or Ethernet). Click on the interface to highlight it.

After selecting the desired interface, click the "Start" or "Capture" button to initiate packet capture. Wireshark will start capturing packets on the chosen interface.

To stop packet capture, simply click the "Stop" or "Capture" button again.

You can apply display filters to focus on specific types of packets or protocols during packet analysis. Use the filter bar at the top of the Wireshark window to enter filter expressions.

To save captured packets for further analysis or reporting, go to "File" > "Save" and choose a file format (e.g., pcap) and a location to save the capture file.

Wireshark is now installed and configured for packet capture on your system. You can proceed with your network traffic analysis by performing the tasks outlined in your assignment.

### Task 1: List of Protocols and Packet Formats and

### Task 2 : Value of different fields

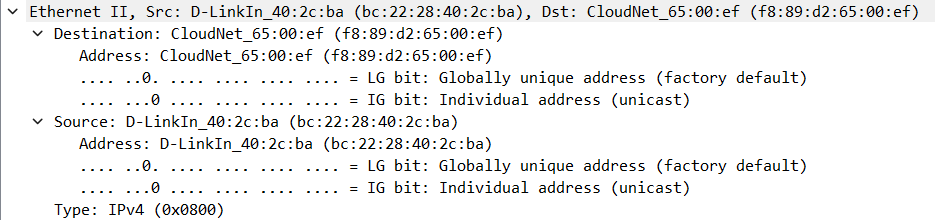
### Data Link Layer

Ethernet II :

Ethernet is a widely used LAN technology. Ethernet packet starts with a preamble which enables the receiver to synchronise and know that a data frame is about to be sent.

SFD (start frame delimiter): indicates the start of the frame(1 byte). Destination Address gives the station MAC address where the packet is to intended to be sent. The first bit indicates whether it is an individual address or a group address. The source address consists of six bytes, and it is used to identify the sending station. Type : field is the one which differentiates between 802.3 and Ethernet II (Type of Ethernet).

User Data block : contains the payload data to be sent and it may be up to 1500 bytes long. FCS contains Cyclic Redundancy Check (CRC) for error detection and analysis.



### Network Layer

##### IPV4 :

IP is responsible to deliver data packets from the source host to the destination host. The packet header contains various fields.

Version indicates the version of IP used in this case, 4. Header length specifies the length of IP header.

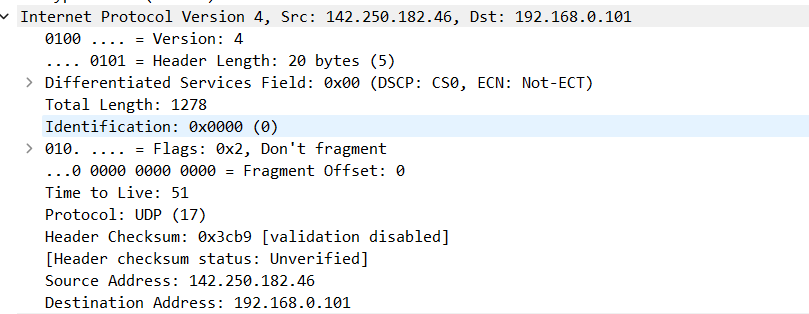
Total length specifies the total length of the datagram (in bytes).

DF bit stands for Do Not Fragment and MF stands for More Fragment bits.

Time to live indicates the maximum number of hops a datagram can take to reach the destination.

Protocol field tells the next level protocol to the network layer at the destination side.

Source/Destination Address contains the logical address of sender and receiver datagram. Options are used for Record route, Source routing, Padding etc.

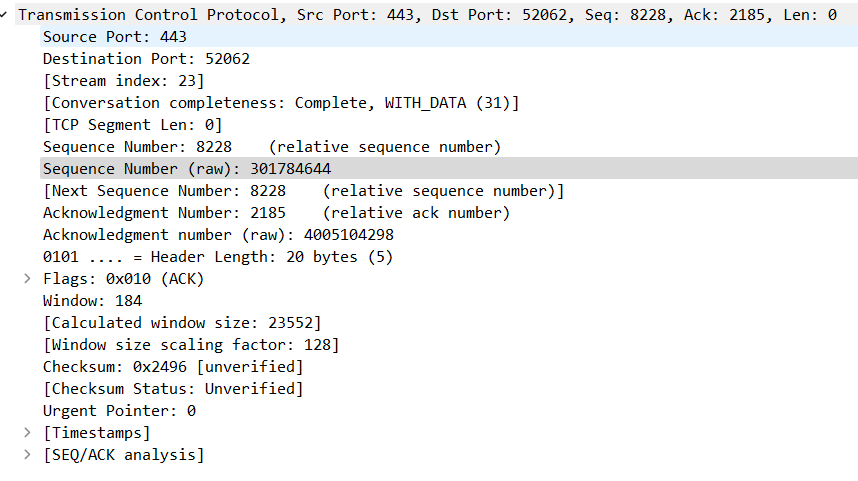


### Transport Layer :

##### 1. TCP (Transmission Control Protocol):

Packet Format: TCP packets have a structured format consisting of a header and a data payload.TCP is used for organizing data in a way that ensures the secure transmission between the server and client.

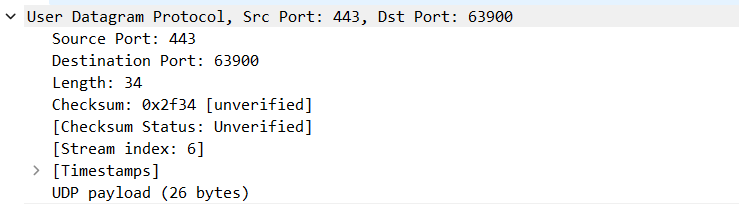
Header: The TCP header includes fields such as Source Port, Destination Port, Sequence Number, Acknowledgment Number, Flags (e.g., SYN, ACK, FIN), Window Size, Checksum, and Urgent Pointer.



##### 2.User Datagram Protocol :

UDP (User Datagram Protocol) is a communications protocol that is primarily used for establishing low-latency and loss-tolerating connections between applications on the internet.

**Source Port** :is a 16-bit field that identifies the port of the sending application. **Destination Port :**is a 16-bit field which identifies the port of the sending application. **Length :**specifies the combined length of UDP Header and Encapsulated data. Checksum is used for error control and calculated on UDP Header, encapsulated data and IP pseudo-header.



### Application Layer:

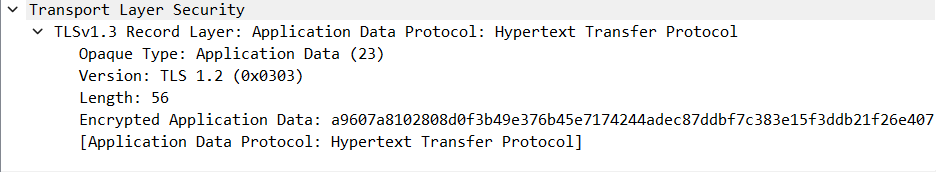
##### 1. HTTPS (Hypertext Transfer Protocol):

Packet Format: HTTP packets are typically text-based and follow a request-response structure. Each packet consists of two main parts: the header and the body.

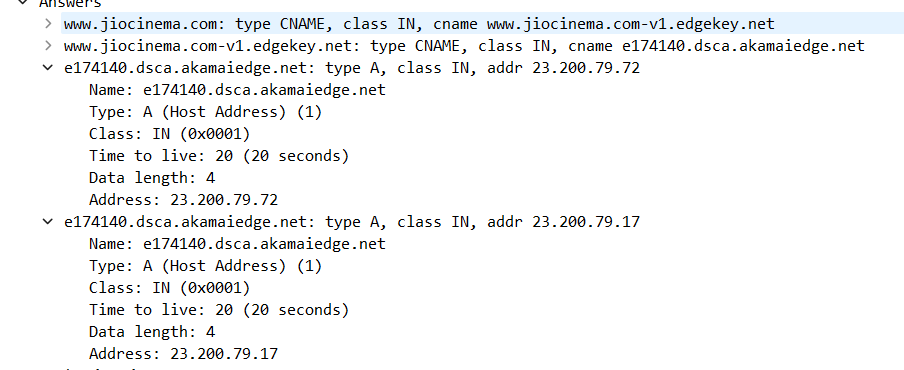
Header: The header contains metadata and information about the HTTP request or response, including fields like "Request Line" (for requests) or "Status Line" (for responses), "Headers" (such as "Host," "User-Agent," and "Content-Type"), and a blank line indicating the end of the header.

Body: The body contains the actual data being transmitted, such as web page content or multimedia content (e.g., video streams).

2.TLSv1.3 (SSL) : TLSv1.3 provides security in communication by encrypting the application data.The basic unit of data in SSL(Secure Socket Layer) is a record. Each record consists of a five-byte record header, followed by data. The record format is Type ( Handshake, Application Data, Alert and Change Cipher Spec), Version and Length. MAC is the message authentication code.



##### 3.DNS (Domain Name System):



Packet Format: DNS packets follow a structured format with a header and sections.

Header: The DNS header contains fields like Transaction ID, Flags, Question Count, Answer Count, Authority Count, and Additional Count.

Question Section: Contains the domain name being queried and the query type (e.g., A for IPv4 address, AAAA for IPv6 address).

Answer Section: Contains the resolved IP address or other DNS records in response to the query.

### 4..Task 3: Sequence of Messages Exchanged:

##### 1. Browsing Content Library:

Sequence of Messages:

The user's device sends an HTTP GET request to the Jio Cinema server, specifying the content library URI.

The Jio Cinema server responds with an HTTP 200 OK status, providing the list of available content.

The user's device may send subsequent HTTP requests to retrieve additional details about specific content items, such as video titles, descriptions, and thumbnails.

The server responds with the requested content details.

##### 2. Initiating Video Playback:

Sequence of Messages:

The user selects a video for playback within the Jio Cinema application.

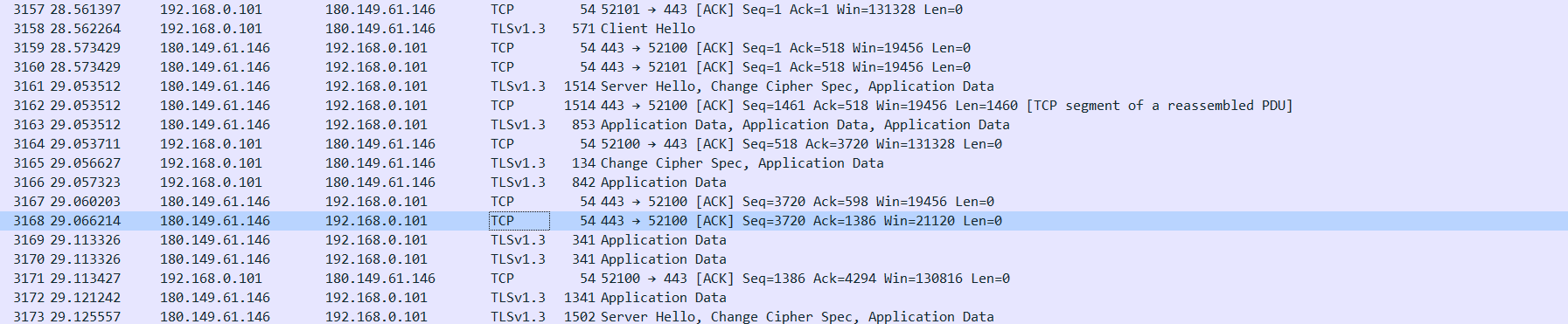
The user's device sends an HTTP request to the Jio Cinema server, requesting the video stream. This request may include information about the selected video.

The server responds with an HTTP 200 OK status and begins streaming the video content in chunks.

The user's device receives video chunks and may send periodic acknowledgments to the server to confirm successful receipt.

The user can pause, seek, or stop playback, resulting in corresponding HTTP requests to the server.

Handshaking Sequence: Video playback typically involves a handshake during the initial request and response, where the server acknowledges the request and starts delivering video content. Subsequent interactions for playback control (pause, seek, stop) may also include simple handshakes.



##### 3. User Authentication and Account Management:

##### Sequence of Messages:

The user logs into their Jio Cinema account by providing credentials.

The user's device sends an HTTP POST request with the login information to the server.

The server validates the credentials and responds with an appropriate status (e.g., 200 OK for successful login).

The user may access account management features, such as updating their profile, changing preferences, or viewing subscription information.

These actions involve various HTTP requests and responses for account-related functionalities.

Handshaking Sequence: The login process typically involves an initial handshake to validate the user's credentials. Subsequent account management actions follow standard request-response patterns.

##### 4. Adaptive Bitrate Streaming:

Sequence of Messages:

During video playback, the Jio Cinema application monitors the user's network conditions.

If the network conditions deteriorate (e.g., increased latency or reduced bandwidth), the application may send a request to the server to switch to a lower bitrate version of the video.

The server acknowledges the request and begins delivering the video in the requested bitrate.

### 5..Task 4:Reason for using perticular protocol:

##### 1. HTTPS (Hypertext Transfer Protocol):

Use in Jio Cinema: HTTP is used for requesting and delivering web pages and multimedia content. In Jio Cinema, HTTP is likely used for various tasks, including fetching video metadata, loading web pages, and initiating video streaming sessions. It is essential for content retrieval and communication with Jio Cinema's servers.

Latest services use https which is safe and secure and hard to capture.

##### 2. TCP (Transmission Control Protocol):

Use in Jio Cinema: TCP ensures reliable and ordered delivery of data between the client (viewer) and Jio Cinema's servers. It is crucial for streaming high-quality videos without data loss or out-of-order delivery. TCP establishes and maintains a connection for video streaming, ensuring smooth playback and minimizing buffering.

Most of streaming used TCP with TLSv1.3 protocol as provided in screenshot.

##### 3.DNS (Domain Name System):

Use in Jio Cinema: DNS plays a critical role in Jio Cinema by resolving domain names (e.g., jiocinema.com) to their corresponding IP addresses. This is essential for users to access Jio Cinema's servers and content. When a user requests to watch a video or browse the platform, DNS ensures that their request reaches the correct server by resolving domain names into IP addresses.

#### **4.Ethernet II:**

Ethernet is the most widely used data link layer protocol. It is preferred over other protocols because of its reliable data transfer, high speed and security. It involves proper error handling and flow control mechanisms for error handling along with CRC for error detection and preamble for synchronization.

1. IPv4:

Internet Protocol version 4 is a connection less protocol which enables data communication over packet switched networks like the internet. It is generally used with the TCP protocol as TCP is only compatible with IP at network Layer. IP is neither reliable nor guarantees ordered data transfer therefore TCP is needed to supplement these shortcomings of IP protocol.

1. TLS:

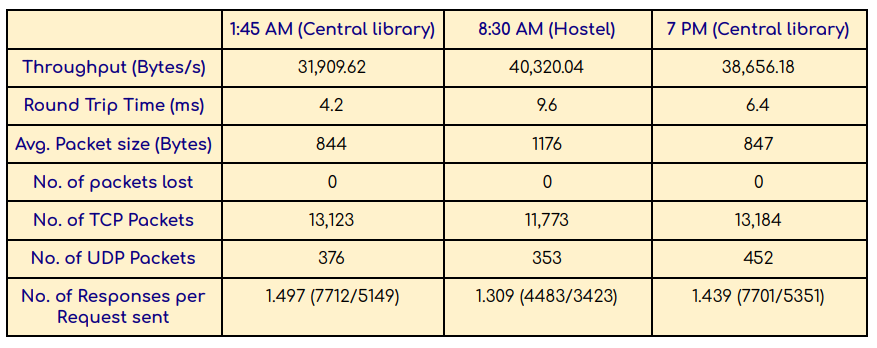
TLSv1.3 is a Secure Sockets Layer (SSL) protocol which encrypts the application data and prevents hackers who snoop packets to get any important information and prevent unwanted eavesdropping. So, all the login credentials (e.g. your email and password) are safely transmitted from client to server in encrypted format so that no hacker can get access of user data.

### .Task:5 Caching:

Jio Cinema use caching to in hence user experience and decrease packet latency. It mainly uses these type of caching technologies at different levels .

1. Content Delivery Network (CDN) Caching: Streaming services utilize CDNs to distribute content globally. CDNs cache content on servers located closer to end-users. This reduces the distance data needs to travel, improving streaming quality and reducing latency.
2. Browser and Application Caching: Web browsers and mobile applications frequently cache certain elements, such as images, CSS files, and JavaScript scripts. Caching at the client-side helps in faster page loading and smoother user experiences.
3. Server-Side Caching: Jio Cinema's servers implement caching for frequently requested content, such as popular movies or TV shows. When a user requests content, the server can check if it already has a cached copy and serve that instead of fetching it again from the source.

### Task6 :Statistics:



Network was stable all the time but change in latency and throughput was noticed.

Because of less web traffic Morning throughput was more than Evening and Noon.

No lost packet was recorded.TCP/UDP ratio was stable mostly.

### END OF REPORT