GROUP NUMBER - 29

Team Members -

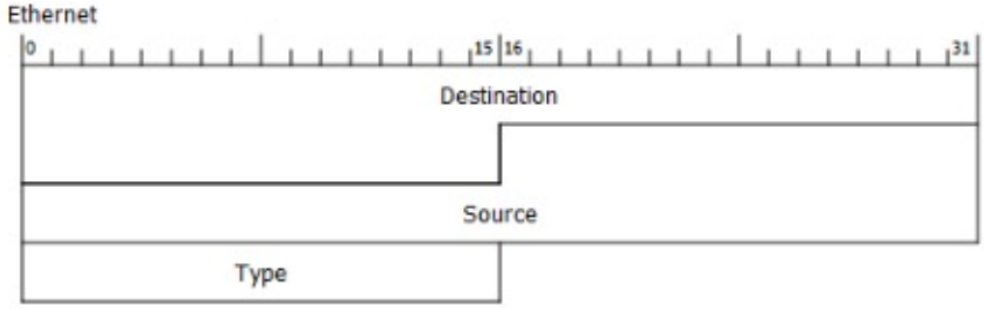
1) Mayank Choudhary
2) Prince Kumar
3) Tarun Kumar

*Wireshark Analysis of Network traffic for **Flipkart***

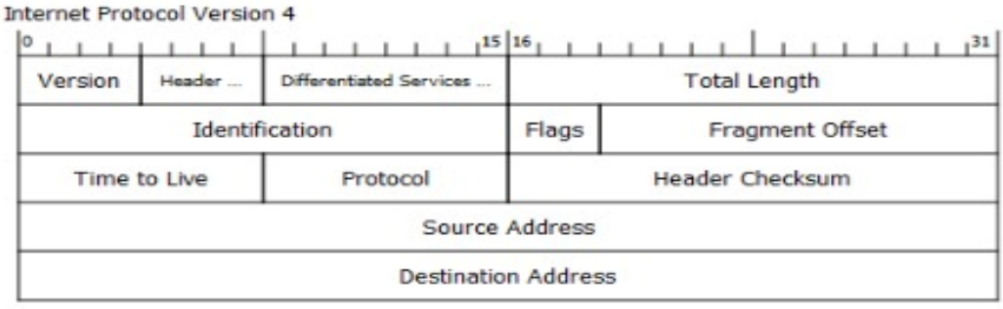
Task 1 : Protocols Used

The various protocols used by the application at different layers along with their packet diagram are :

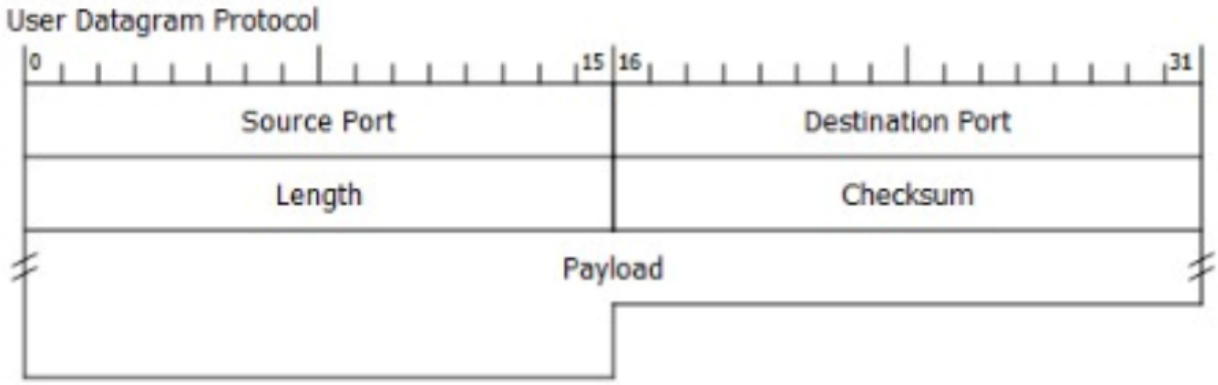
a) **Link Layer**: Ethernet II



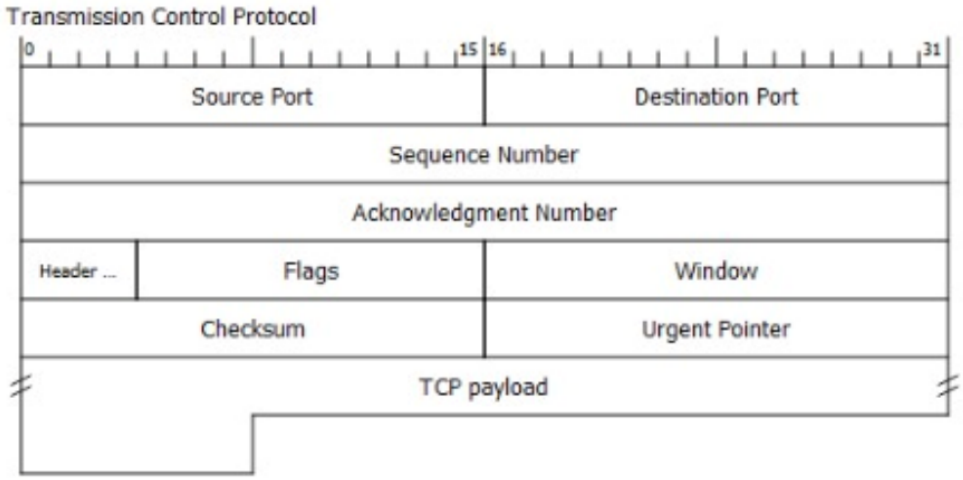
b) **Transport Layer :** IPv4



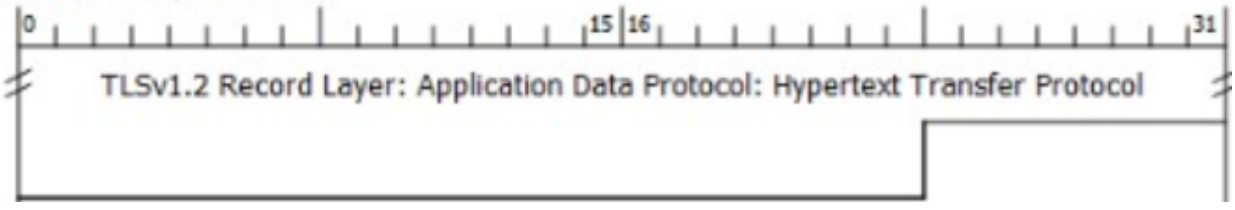
c) **Network Layer :** UDP(User Datagram Protocol)



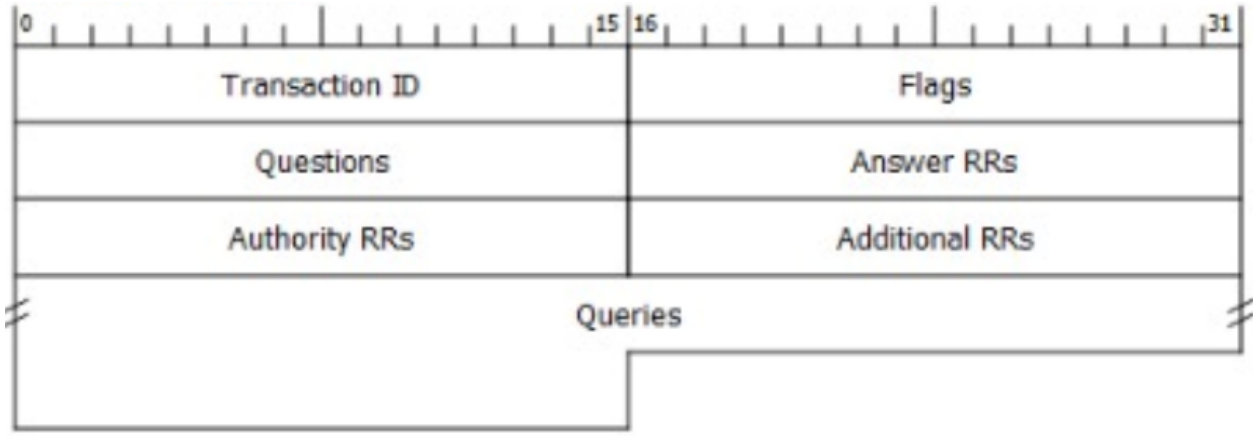
d) **Network Layer:** TCP(Transmission Control Protocol).



e) **Application Layer:** TLSv1.2(Transport Layer Security version 1.2) for security and HTTP



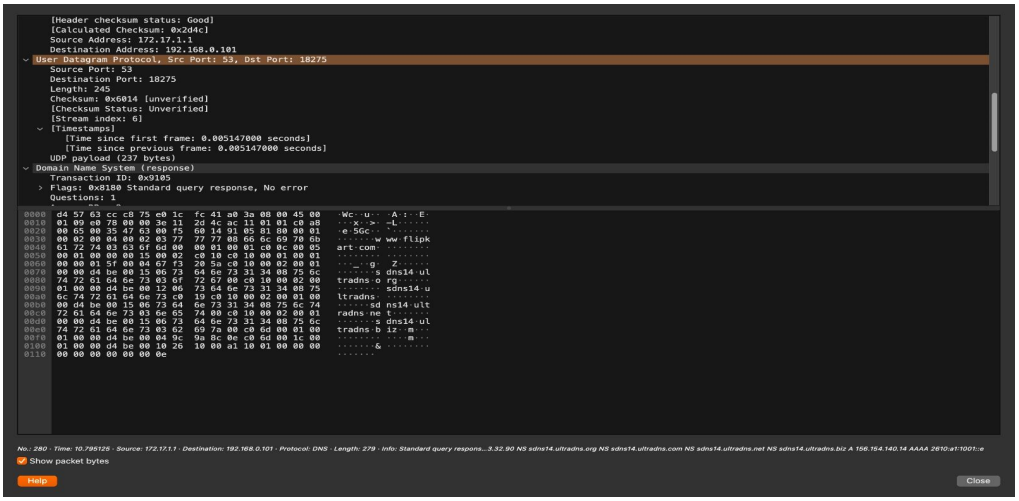
f) **Application Layer:** DNS(Domain Name System)



Task 2 : Values Observed.

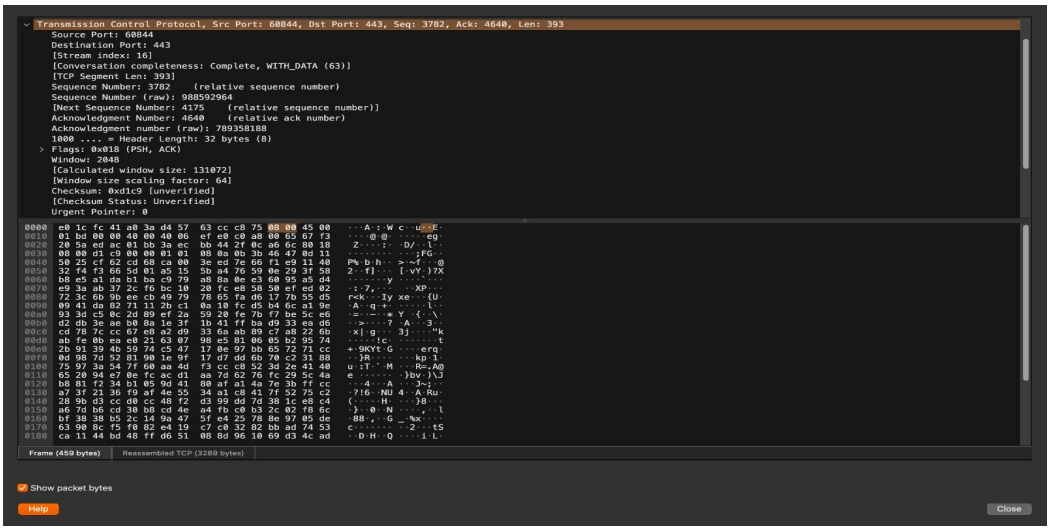
1) UDP

The following is an example of a UDP packet in a DNS request here
Source Port: 53
Destination Port: 18275



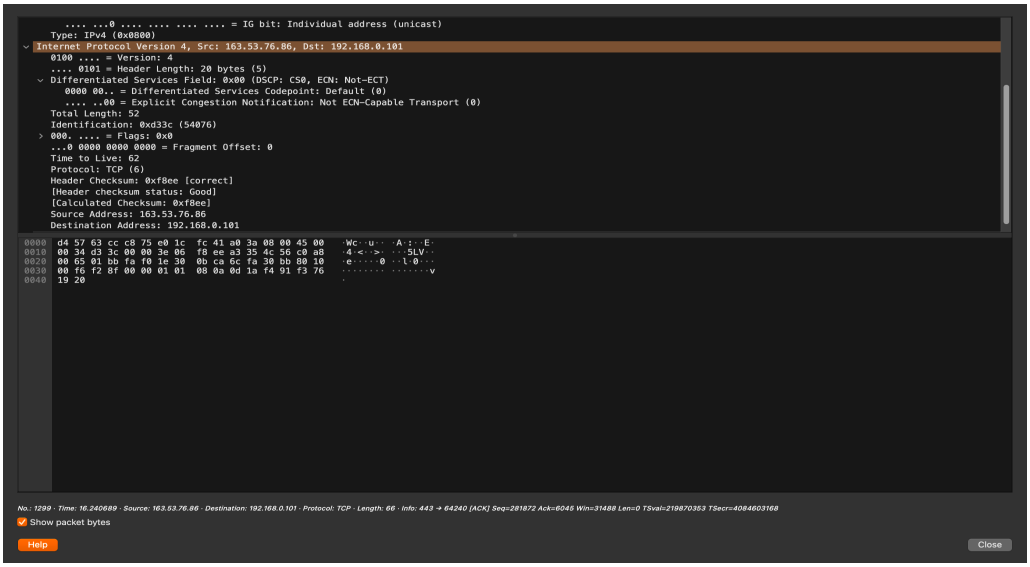
2) TCP

The following is an example of a TCP packet, here
Source Port : 60844
Destination Port : 443



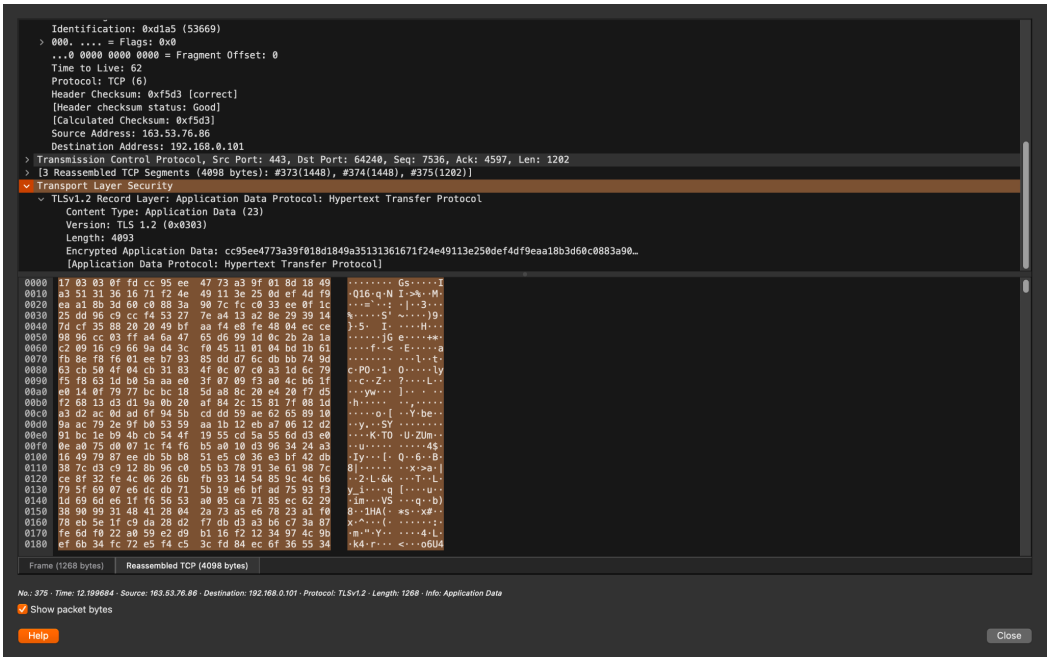
3) IPv4

For HTTP requests the IPv4 packets have
Source IP : 163.53.76.86
Dst IP : 192.168.0.101



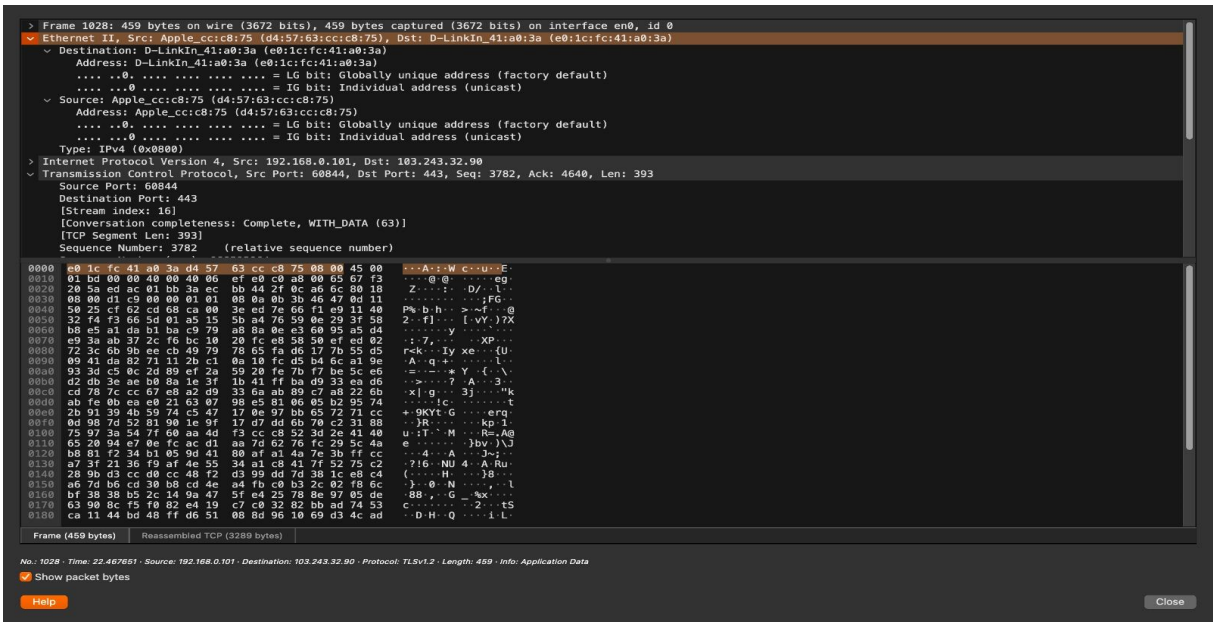
4) Tlsv1.2

HTTP Protocol sent by flipkart server to user
Length: 4093



5) Ethernet

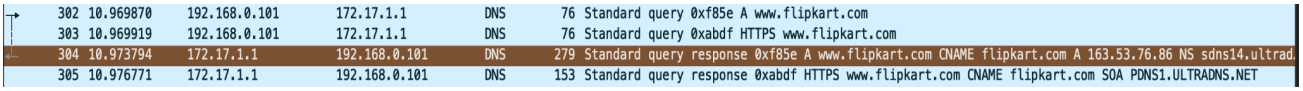
Depending upon the direction of requests/data flow, the source and destination address for the link layer can be as follows:



Task 3: Message Sequences for the functionalities

1)DNS:

Dns query sent by the server and query response sent by the server.



302	10.969870	192.168.0.101	172.17.1.1	DNS	76	Standard query 0xf85e A www.flipkart.com
303	10.969919	192.168.0.101	172.17.1.1	DNS	76	Standard query 0xabdf HTTPS www.flipkart.com
304	10.973794	172.17.1.1	192.168.0.101	DNS	279	Standard query response 0xf85e A www.flipkart.com CNAME flipkart.com A 163.53.76.86 NS sdns14.ultrad
305	10.976771	172.17.1.1	192.168.0.101	DNS	153	Standard query response 0xabdf HTTPS www.flipkart.com CNAME flipkart.com SOA PDNS1.ULTRADNS.NET

2)Video Play:

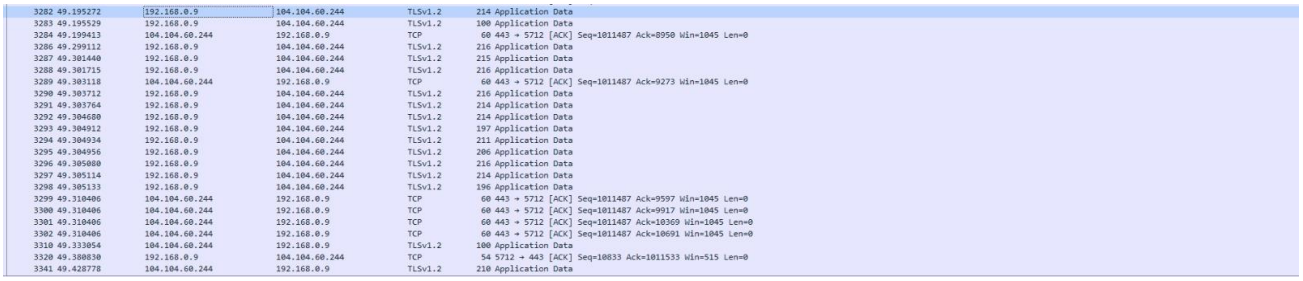
i)Ethernet II: This protocol enables the collision-free interconnection of multiple devices via a common bus. It also gives error free transmission of packets.

ii) IPv4: It is required for the clients to get connected to the internet to the application server.

iii) TCP: It is required to establish a reliable connection to play the media fluently.

iv)TLSv1.2: This is used to encrypt the data before transferring it.

v)DNS: Used in the beginning to extract the video from youtube server

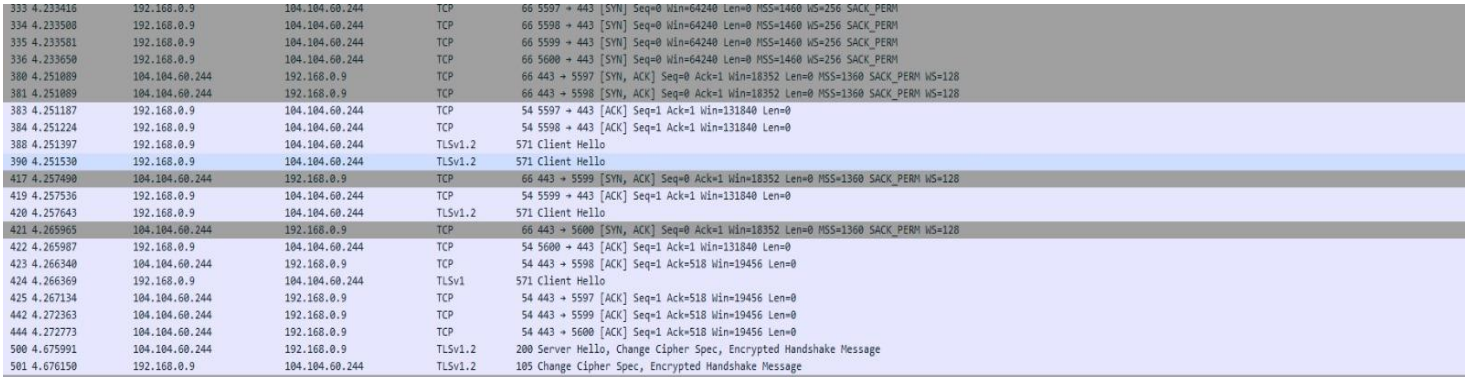


3282	49.195272	192.168.0.9	104.104.60.244	TLSv1.2	214	Application Data
3283	49.195529	192.168.0.9	104.104.60.244	TLSv1.2	100	Application Data
3284	49.199413	104.104.60.244	192.168.0.9	TCP	60	443 → 5712 [ACK] Seq=1011487 Ack=8950 Win=1045 Len=0
3286	49.299112	192.168.0.9	104.104.60.244	TLSv1.2	216	Application Data
3287	49.301440	192.168.0.9	104.104.60.244	TLSv1.2	215	Application Data
3288	49.301715	192.168.0.9	104.104.60.244	TLSv1.2	216	Application Data
3289	49.303118	104.104.60.244	192.168.0.9	TCP	60	443 → 5712 [ACK] Seq=1011487 Ack=9273 Win=1045 Len=0
3290	49.303712	192.168.0.9	104.104.60.244	TLSv1.2	216	Application Data
3291	49.303764	192.168.0.9	104.104.60.244	TLSv1.2	214	Application Data
3292	49.304680	192.168.0.9	104.104.60.244	TLSv1.2	214	Application Data
3293	49.304912	192.168.0.9	104.104.60.244	TLSv1.2	197	Application Data
3294	49.304934	192.168.0.9	104.104.60.244	TLSv1.2	211	Application Data
3295	49.304956	192.168.0.9	104.104.60.244	TLSv1.2	206	Application Data
3296	49.305080	192.168.0.9	104.104.60.244	TLSv1.2	216	Application Data
3297	49.305114	192.168.0.9	104.104.60.244	TLSv1.2	214	Application Data
3298	49.305133	192.168.0.9	104.104.60.244	TLSv1.2	196	Application Data
3299	49.310406	104.104.60.244	192.168.0.9	TCP	60	443 → 5712 [ACK] Seq=1011487 Ack=9597 Win=1045 Len=0
3300	49.310406	104.104.60.244	192.168.0.9	TCP	60	443 → 5712 [ACK] Seq=1011487 Ack=9917 Win=1045 Len=0
3301	49.310406	104.104.60.244	192.168.0.9	TCP	60	443 → 5712 [ACK] Seq=1011487 Ack=10369 Win=1045 Len=0
3302	49.310406	104.104.60.244	192.168.0.9	TCP	60	443 → 5712 [ACK] Seq=1011487 Ack=10691 Win=1045 Len=0
3310	49.333054	104.104.60.244	192.168.0.9	TLSv1.2	100	Application Data
3320	49.380830	192.168.0.9	104.104.60.244	TCP	54	5712 → 443 [ACK] Seq=10833 Ack=1011533 Win=515 Len=0
3341	49.428778	104.104.60.244	192.168.0.9	TLSv1.2	210	Application Data

3)Handshaking

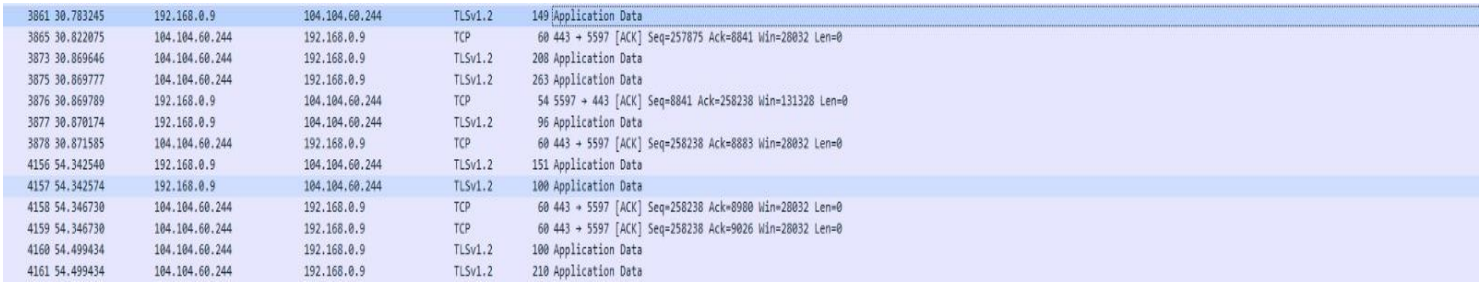
Multiple 3 way handshake has been made here. The client sends a message to initiate the connection by sending a SYN, the server accepts

it by sending an ACK and requests the client for connection by sending SYN along with the previous ACK.Finally the client sends back an ACK to the server to accept the connection. The specific connection starts by “Client Hello” which basically will include which TLS version the client supports and the cipher suites supported to which server replies with “Server Hello” which contains the SSL certificates and cipher suits it is going to use. Then the encryption keys are exchanged with the encrypted handshake messages and the messages are exchanged using TLSv1.2. Finally FIN is used by client to close the connection.



4)Link Click:

The user sends a package to the server to which the server responds with an ACK . Further the server then starts to send the requested packages



Task 4 : Relevance of the particular protocol used

The use of different protocols UDP,TCP,TLSV1.2 is a strategic choice that aligns with the specific requirements. Here's an explanation of how these protocols are relevant-

1) TCP (Transmission Control Protocol): Relevance for Flipkart: TCP is a connection-oriented protocol that provides reliable and ordered delivery of data packets between devices over a network. It ensures that data is transmitted accurately and in the correct order. This is crucial for e-commerce websites like Flipkart, where maintaining the integrity of data during transactions is paramount. For example, when you browse products, add items to your cart, and proceed to checkout, TCP ensures that all this information is transmitted reliably to the Flipkart servers.
2) TLS v1.2 (Transport Layer Security): Relevance for Flipkart: TLS is a cryptographic protocol that ensures secure communication over a network. It encrypts data during transmission, protecting it from eavesdroppers and ensuring the privacy and integrity of sensitive information like login credentials, personal details, and payment information. This is critical for an e-commerce platform like Flipkart, as it deals with a large volume of sensitive customer information during transactions.
3) UDP (User Datagram Protocol) for DNS: Relevance for Flipkart: DNS (Domain Name System) is used to translate human-readable domain names (like www.flipkart.com) into IP addresses that computers can use to locate the server. UDP is used for DNS queries because it is faster and more efficient for simple, one-time communications like DNS lookups. Flipkart relies on DNS to direct users to the correct servers hosting the website. This ensures that when you type "flipkart.com" in your browser, you're directed to the correct Flipkart server that hosts the website.

Task 5:Caching Mechanism

Caching is an essential technique used by e-commerce websites like Flipkart.com to improve the performance, speed, and responsiveness of their platform. It involves storing frequently accessed data or web page elements in a cache,which is a temporary and fast-access storage layer, to reduce the load on the web servers and minimize the time it takes to serve content to users.

How Caching Mechanism is being observed?

1) DNS responses include Time to Live(TTL) values which indicate caching. Cached DNS records can reduce the need for repeated DNS resolutions.

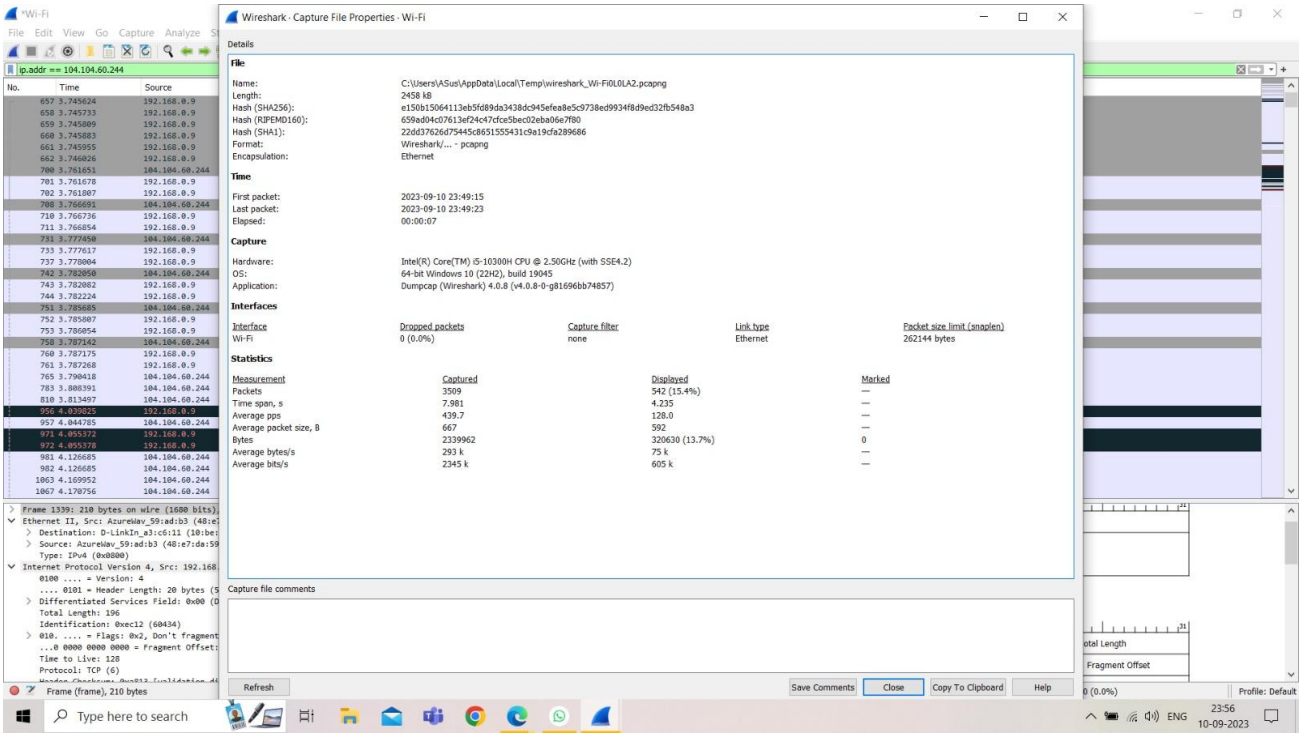
2) When visiting the same product again or playing the demo video again the number of packet exchanged is significantly less as the various resources such as images are cached locally.

3) Reduced response time for the same page which is being accessed again and again.

Conclusion

Caching is a complex and critical aspect of large-scale e-commerce websites like Flipkart.com, as it directly impacts the site's performance, user experience, and server load. The specific caching strategies and technologies employed may vary based on the evolving needs and technologies of the platform.

Task 6: Statistics



Statistics	Morning	Night
Throughput	605k bits/s	438k bits/s
RTT	0.08526	0.06458
Packet size	592	405
No. of Packets Lost	0	0
UDP Packets	0	0
TCP Packets	592	405
No. of responses/ request	1.3	2.4