

# GROUP NUMBER - 29

## Team Members -

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

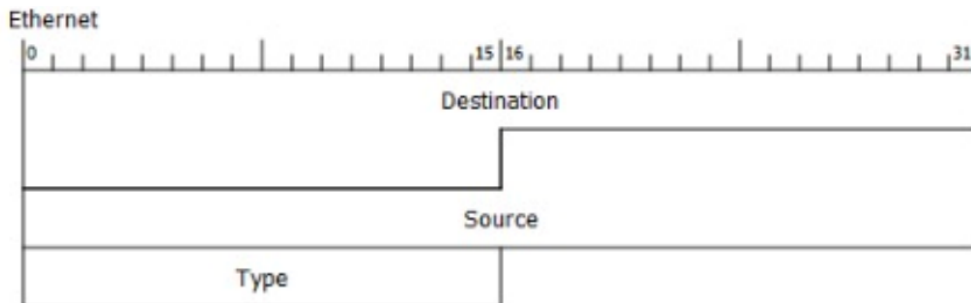


## Wireshark Analysis of Network traffic for *Flipkart*

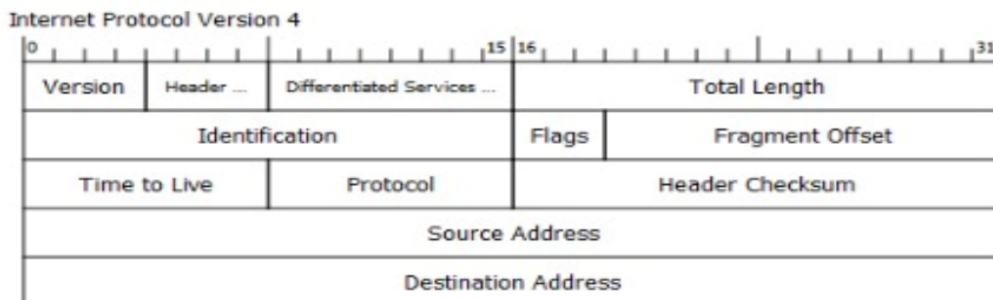
### Task 1 : Protocols Used

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

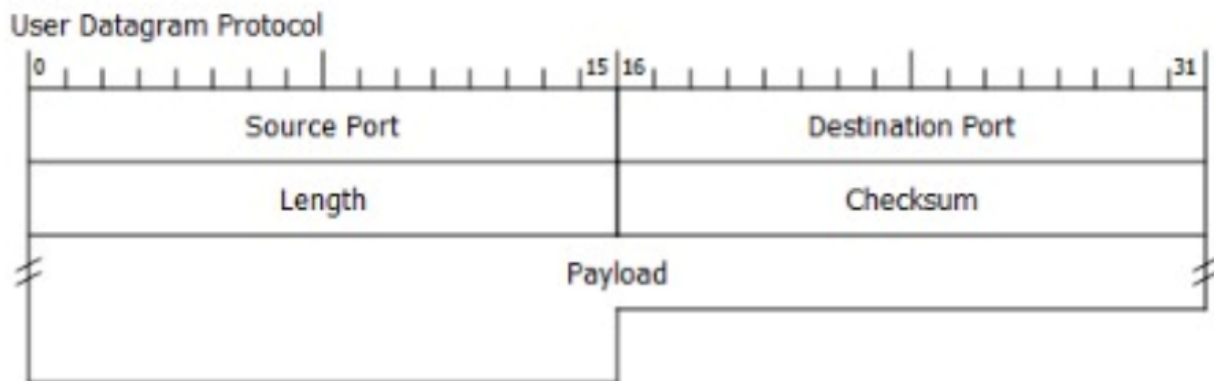
#### a) Link Layer: Ethernet II



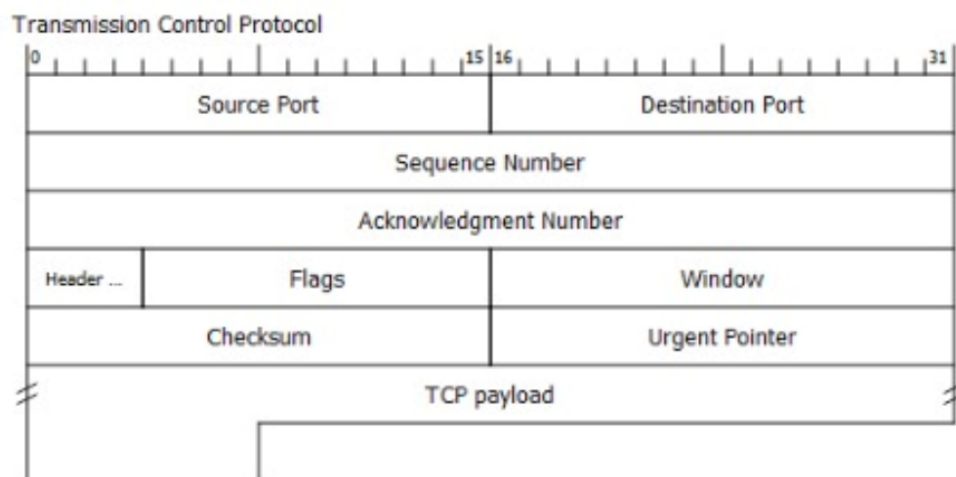
#### b) Transport Layer : IPv4



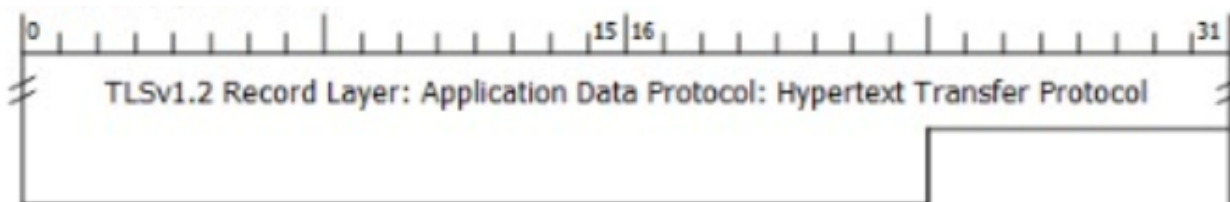
c) **Network Layer** : UDP(User Datagram Protocol)



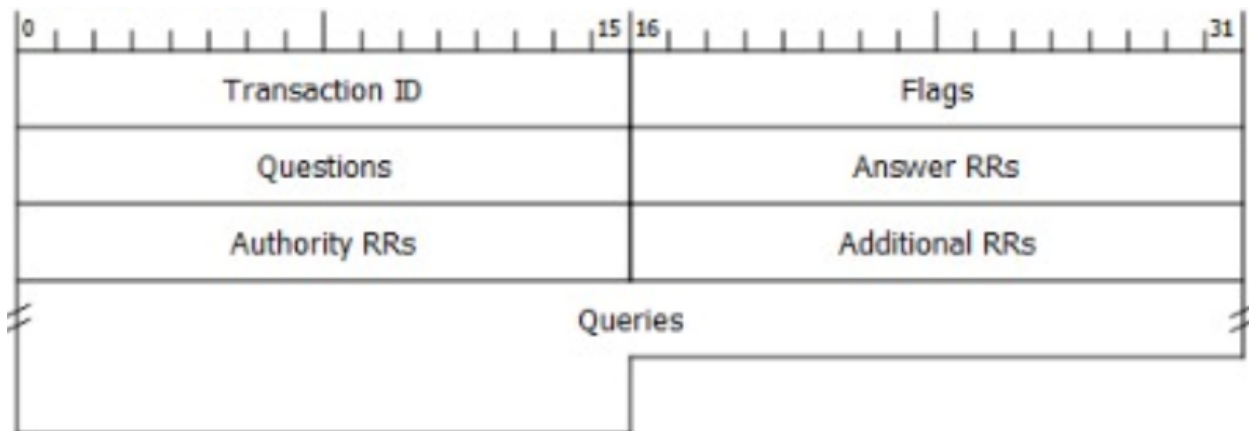
d) **Network Layer**: TCP(Transmission Control Protocol).



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

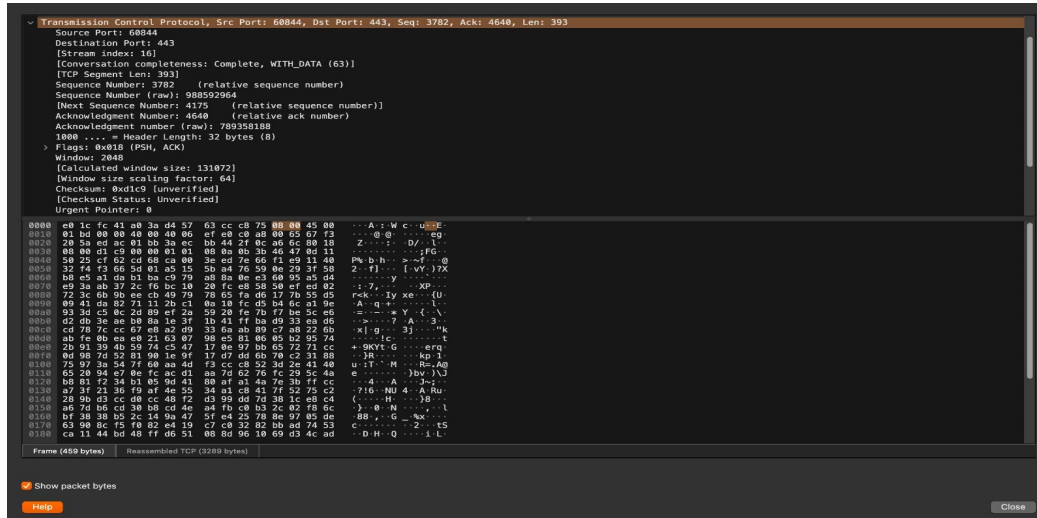
Source Port: 53

Destination Port: 18275

```
[Header checksum status: Good]
[Calculated Checksum: 80d4c]
Source Address: 172.17.1.1
Destination Address: 192.168.0.101
User Datagram Protocol: Src Port: 53, Dst Port: 18275
Source Port: 53
Destination Port: 18275
Length: 245
Checksum: 0x0814 (unverified)
[Checksum Status: Unverified]
[Stream index: 6]
[Timestamps]
  [Time since first frame: 0.005147000 seconds]
  [Time since previous frame: 0.005147000 seconds]
UDP payload (227 bytes)
Domain Name System (response)
Transaction ID: 0x9185
Flags: 0x0180 Standard query response, No error
Questions: 1
0000 d4 57 63 cc c8 75 e0 1c fc 41 a0 3a 08 00 45 00 Wc.u...A...E
0010 91 00 00 78 00 00 11 20 4c ac 11 01 01 c8 00 ...>...L...
0020 00 65 00 35 47 03 00 75 69 14 01 05 01 00 00 01 eSGC...
0030 00 02 00 04 00 02 03 77 77 00 05 0c 69 78 00 ...w...flap
0040 01 72 74 03 03 0f 6d 00 00 01 00 01 c8 0c 00 02 art.com...
0050 00 01 00 00 05 00 02 c8 10 c8 10 00 01 00 01 ...ig...Z...
0060 00 00 01 5f 00 04 07 73 28 5a c8 10 00 02 00 01 tradns...
0070 00 00 04 00 00 35 00 73 64 06 73 31 34 00 75 6c ...s dns14 ul
0080 74 72 01 04 0e 73 03 0f 72 67 00 c8 10 00 02 00 tradns...
0090 61 78 01 04 0e 73 08 19 c8 10 00 02 00 01 00 ltradns...
00a0 00 04 00 00 73 08 06 73 31 34 00 75 6c 74 ...sdns14 u
00b0 02 01 00 00 03 00 65 74 00 c8 10 00 02 00 01 radns ne...
00c0 00 00 04 00 00 35 00 73 64 06 73 31 34 00 75 6c ...s dns14 ul
00d0 74 72 01 04 0e 73 03 0f 69 7a 00 c8 0d 00 01 00 tradns b...
00e0 01 00 00 04 00 00 0c 0a 0c 0c c8 0d 00 01 00 ...m...
00f0 01 00 00 04 00 00 10 00 01 10 01 00 00 00 ...s...
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0110 00 00 00 00 00 00 00 00 00 00 00 00 00 00
No. 280, Time: 10.789125, Source: 172.17.1.1, Destination: 192.168.0.101, Protocol: DNS, Length: 278, Info: Standard query response...3.32 B0 NS sdns14.ultradns.org NS sdns14.ultradns.com NS sdns14.ultradns.net NS sdns14.ultradns.biz A 100.104.140.14 AAAA 2610:a1:1001::e
Show packet bytes
Help Close
```

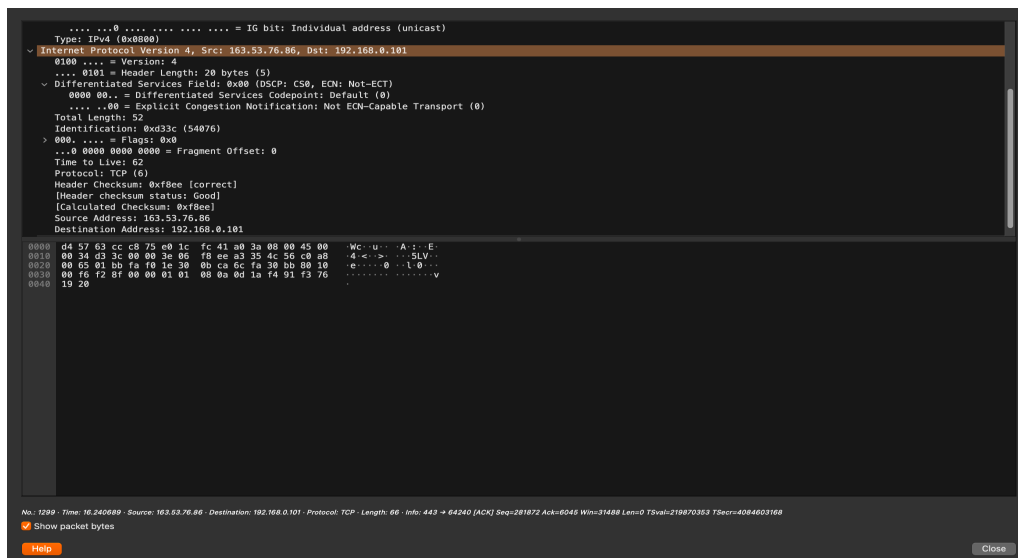
## 2) TCP

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



## 3) IPv4

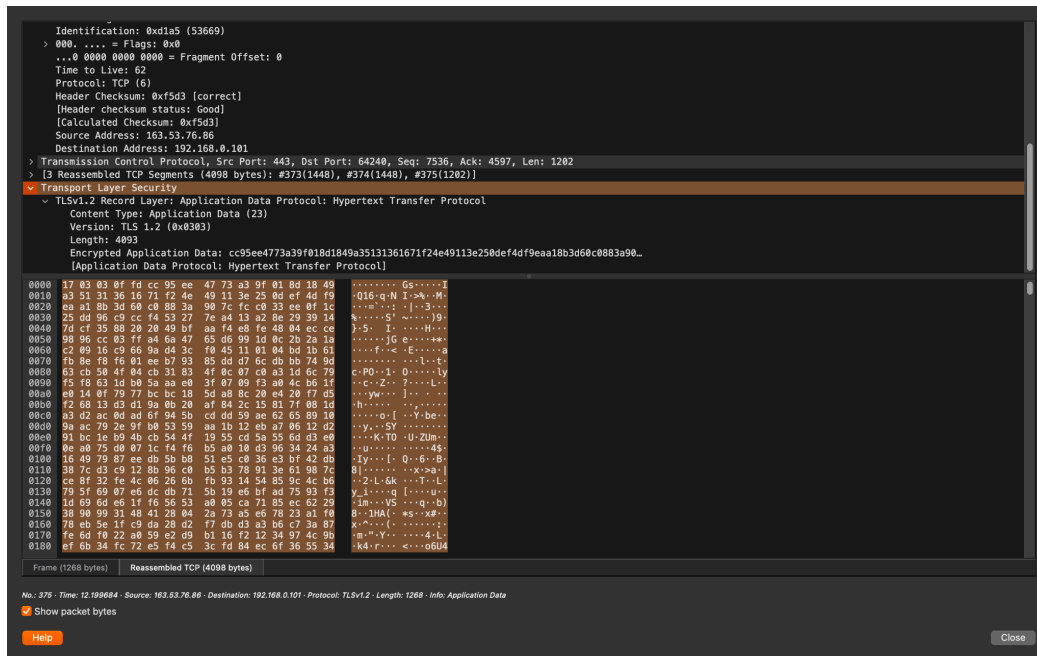
For HTTP requests the IPv4 packets have  
Source IP : 163.53.76.86  
Dst IP : 192.168.0.101



## 4) Tlsv1.2

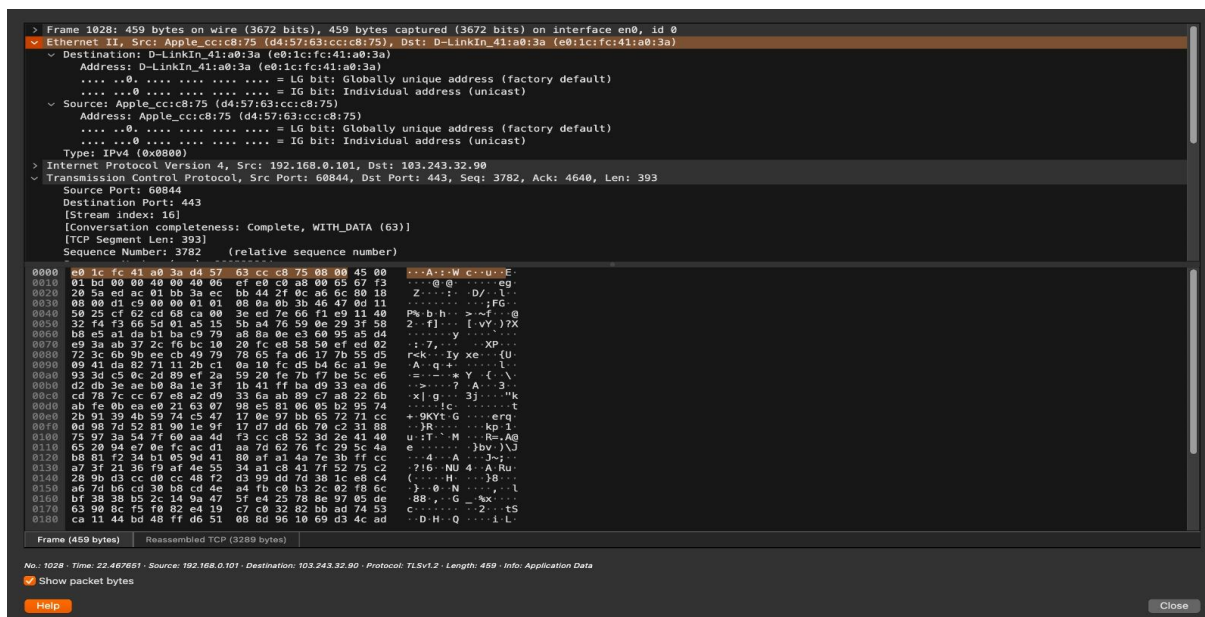
HTTP Protocol sent by flipkart server to user

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	49.301460	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	49.304600	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	49.305000	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	49.308830	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.

333	4.233416	192.168.0.9	104.104.60.244	TCP	66 5597 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
334	4.233508	192.168.0.9	104.104.60.244	TCP	66 5598 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
335	4.233581	192.168.0.9	104.104.60.244	TCP	66 5599 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
336	4.233650	192.168.0.9	104.104.60.244	TCP	66 5600 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
380	4.251089	104.104.60.244	192.168.0.9	TCP	66 443 → 5597 [SYN, ACK] Seq=0 Ack=1 Win=18352 Len=0 MSS=1360 SACK_PERM WS=128
381	4.251089	104.104.60.244	192.168.0.9	TCP	66 443 → 5598 [SYN, ACK] Seq=0 Ack=1 Win=18352 Len=0 MSS=1360 SACK_PERM WS=128
383	4.251187	192.168.0.9	104.104.60.244	TCP	54 5597 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0
384	4.251224	192.168.0.9	104.104.60.244	TCP	54 5598 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0
388	4.251397	192.168.0.9	104.104.60.244	TLSv1.2	571 Client Hello
390	4.251530	192.168.0.9	104.104.60.244	TLSv1.2	571 Client Hello
417	4.257490	104.104.60.244	192.168.0.9	TCP	66 443 → 5599 [SYN, ACK] Seq=0 Ack=1 Win=18352 Len=0 MSS=1360 SACK_PERM WS=128
419	4.257536	192.168.0.9	104.104.60.244	TCP	54 5599 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0
420	4.257643	192.168.0.9	104.104.60.244	TLSv1.2	571 Client Hello
421	4.265905	104.104.60.244	192.168.0.9	TCP	66 443 → 5600 [SYN, ACK] Seq=0 Ack=1 Win=18352 Len=0 MSS=1360 SACK_PERM WS=128
422	4.265987	192.168.0.9	104.104.60.244	TCP	54 5600 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0
423	4.266340	104.104.60.244	192.168.0.9	TCP	54 443 → 5598 [ACK] Seq=1 Ack=518 Win=19456 Len=0
424	4.266369	192.168.0.9	104.104.60.244	TLSv1	571 Client Hello
425	4.267134	104.104.60.244	192.168.0.9	TCP	54 443 → 5597 [ACK] Seq=1 Ack=518 Win=19456 Len=0
442	4.272363	104.104.60.244	192.168.0.9	TCP	54 443 → 5599 [ACK] Seq=1 Ack=518 Win=19456 Len=0
444	4.272773	104.104.60.244	192.168.0.9	TCP	54 443 → 5600 [ACK] Seq=1 Ack=518 Win=19456 Len=0
500	4.675991	104.104.60.244	192.168.0.9	TLSv1.2	200 Server Hello, Change Cipher Spec, Encrypted Handshake Message
501	4.676150	192.168.0.9	104.104.60.244	TLSv1.2	105 Change Cipher Spec, Encrypted Handshake Message

#### 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

3861	30.783245	192.168.0.9	104.104.60.244	TLSv1.2	149 Application Data
3865	30.822075	104.104.60.244	192.168.0.9	TCP	60 443 → 5597 [ACK] Seq=257875 Ack=8841 Win=20832 Len=0
3873	30.869646	104.104.60.244	192.168.0.9	TLSv1.2	208 Application Data
3875	30.869777	104.104.60.244	192.168.0.9	TLSv1.2	263 Application Data
3876	30.869789	192.168.0.9	104.104.60.244	TCP	54 5597 → 443 [ACK] Seq=8841 Ack=258238 Win=131328 Len=0
3877	30.870174	192.168.0.9	104.104.60.244	TLSv1.2	96 Application Data
3878	30.871585	104.104.60.244	192.168.0.9	TCP	60 443 → 5597 [ACK] Seq=258238 Ack=8883 Win=20832 Len=0
4156	54.342540	192.168.0.9	104.104.60.244	TLSv1.2	151 Application Data
4157	54.342574	192.168.0.9	104.104.60.244	TLSv1.2	100 Application Data
4158	54.346730	104.104.60.244	192.168.0.9	TCP	60 443 → 5597 [ACK] Seq=258238 Ack=8900 Win=20832 Len=0
4159	54.346730	104.104.60.244	192.168.0.9	TCP	60 443 → 5597 [ACK] Seq=258238 Ack=9026 Win=20832 Len=0
4160	54.499434	104.104.60.244	192.168.0.9	TLSv1.2	100 Application Data
4161	54.499434	104.104.60.244	192.168.0.9	TLSv1.2	210 Application Data



## **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](http://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.

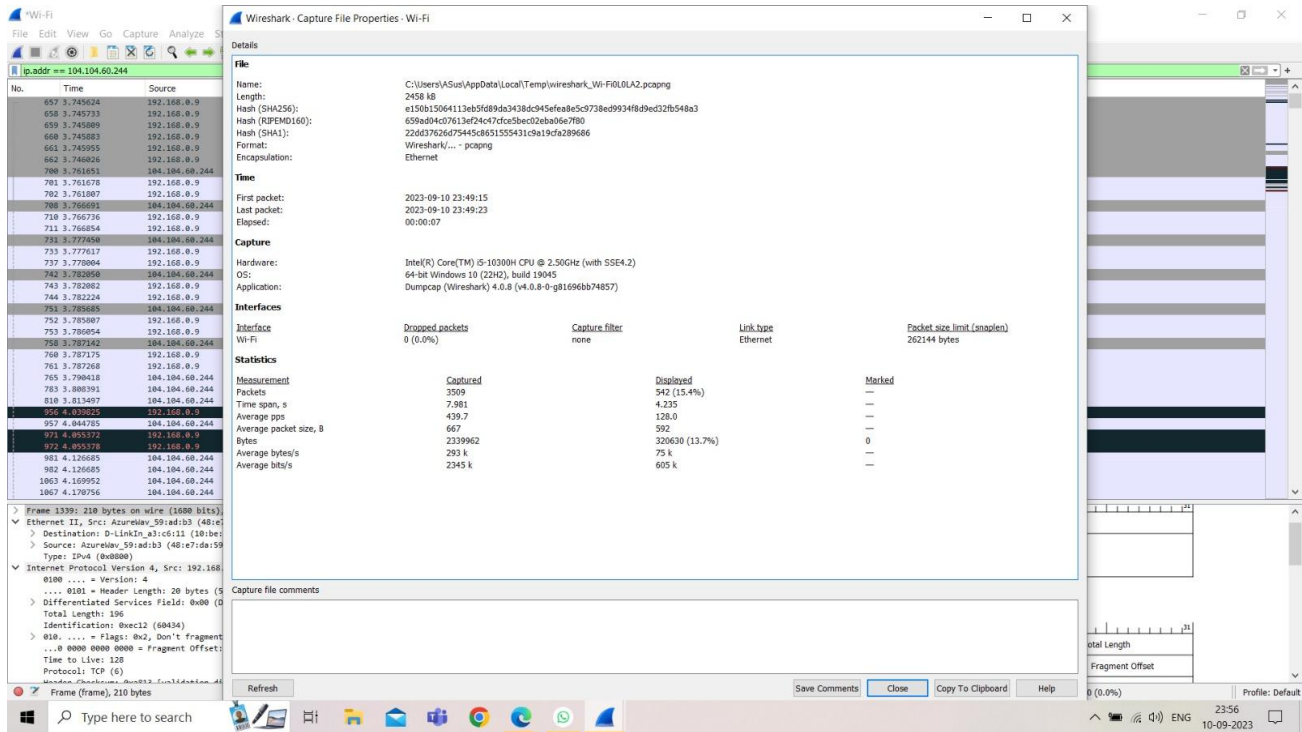
### **How Caching Mechanism is being observed?**

- 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 packets 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

