CS 315: Computer Networks Lab
Spring 2024-25, IIT Dharwad
Assignment-2
Getting started with Wireshark
Jan 19, 2025

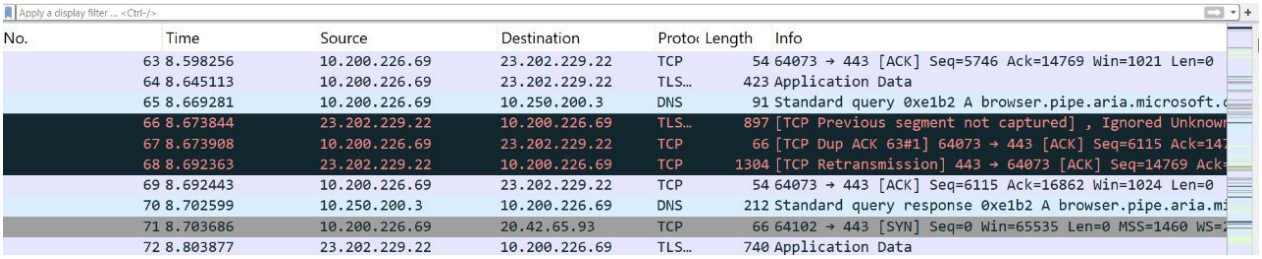
Wireshark

Objective: The objective of this assignment is to familiarize oneself with the Wireshark interface.

Part-1

Answer the following

1. **If a packet is highlighted by black, what does it mean for the packet?**



Black-highlighted packets in Wireshark indicate TCP issues like **"TCP ACKed unseen segment"** (acknowledging data not captured) or **"TCP Previous segment not captured"** (missing preceding segment). These often result from packet loss during capture or high network traffic.

2. **What is the filter command for listing all outgoing http traffic?**

   For listing all outgoing HTTP traffic consists of HTTP requests, that maybe done through GET (or) POST. We would like to view all of them,

   so the filter command would be:

   - http.request
   - http.request.method==”GET”
   - http.request.method==”POST”

3. **Why does DNS use Follow UDP Stream while http use Follow TCP Stream?**

   DNS uses **Follow UDP Stream** because it operates on the connectionless **UDP protocol**, which is faster and ideal for small, lightweight requests like domain name resolution. Since DNS queries are small and time-sensitive, using UDP ensures quick performance.

   HTTP uses **Follow TCP Stream** because it relies on the connection-oriented **TCP protocol**, which provides reliable data delivery. This is essential for transferring larger files, web pages, images, and other critical data where packet loss must be avoided. TCP ensures all data is delivered correctly and in order, avoiding the complexity of retransmissions at the application layer. Thus, DNS prioritizes **performance**, while HTTP prioritizes **reliability**.

Part-2

Answer the following questions

1. **List any 5 protocols you observe inside the entire trace file.**

   In the unfiltered packet-listing window of Wireshark, the **Protocol** column displays the types of protocols detected in the captured traffic. Common protocols include:

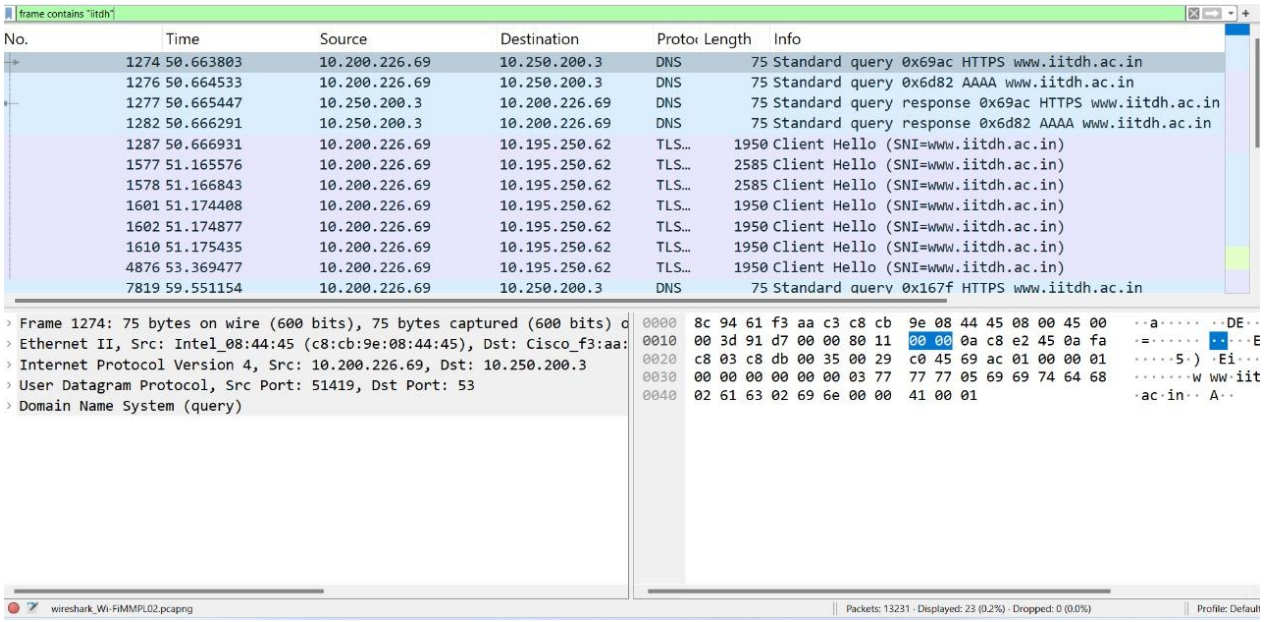
   Commonly Observed Protocols in a Wireshark Trace File:

   1. **TCP (Transmission Control Protocol)**: Ensures reliable data transfer between devices over the network.
   2. **HTTP (HyperText Transfer Protocol)**: Facilitates communication for web requests and responses.
   3. **TLS (Transport Layer Security)**: Secures encrypted connections, commonly used for HTTPS.
   4. **DNS (Domain Name System)**: Resolves human-readable domain names into IP addresses.
   5. **ICMP (Internet Control Message Protocol)**: Used for error reporting and network diagnostics (e.g., ping).

   These protocols represent different layers of the OSI model and showcase the diversity of network traffic captured.

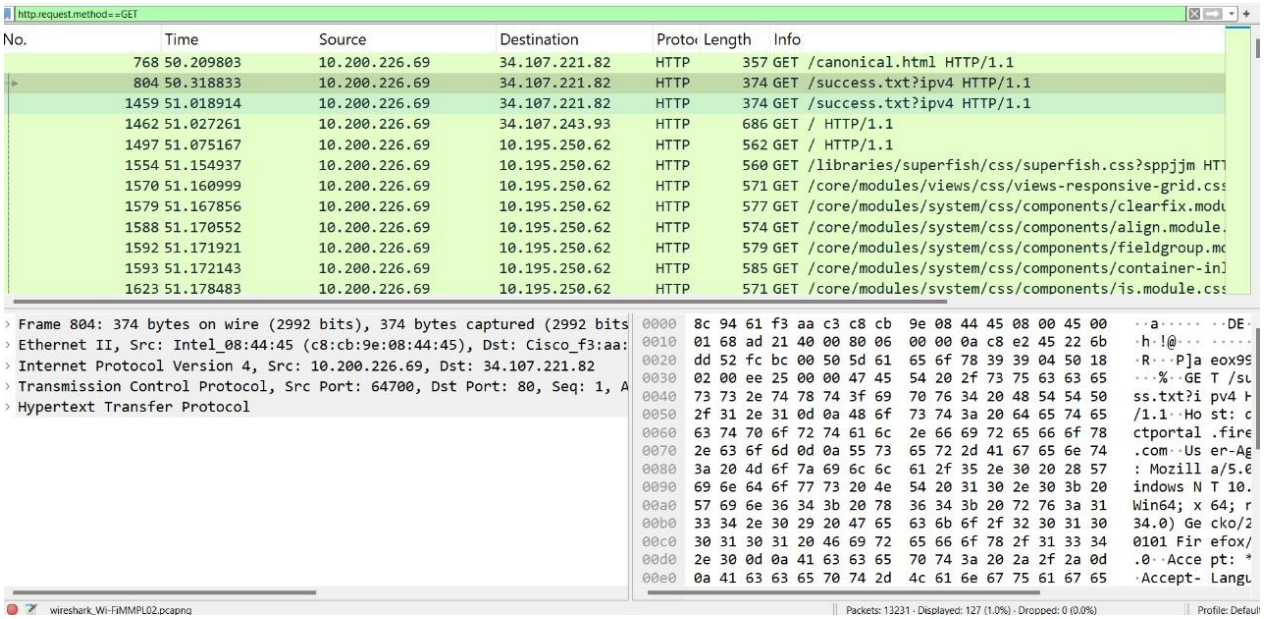
2. **Use the following filters in the <u>display filter field</u> of Wireshark and answer with the count of the total number of displayed packets for each of the filters.**

   a. **frame contains "iitdh"**



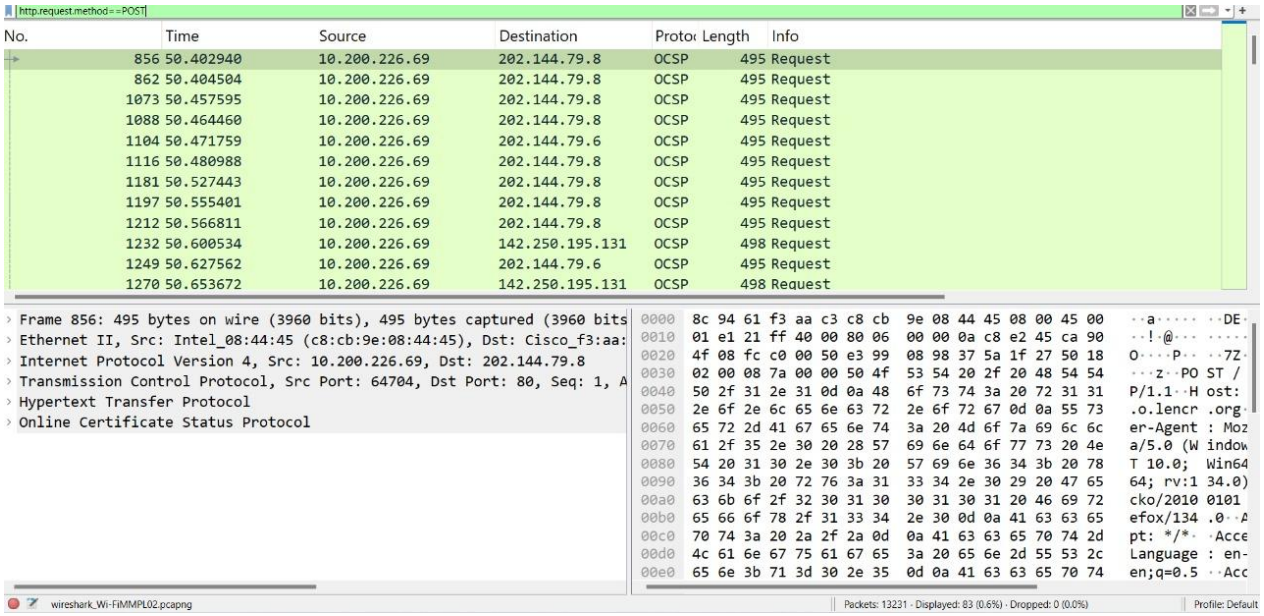
Total number of displayed packets = **23**

b. http.request.method==GET



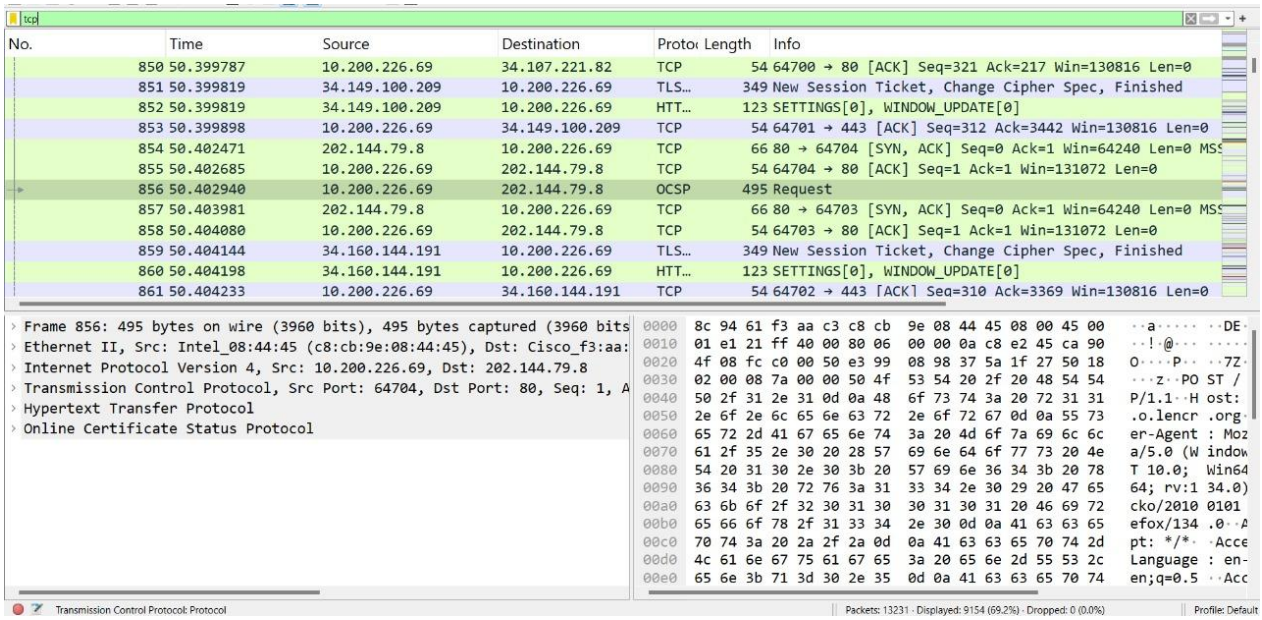
Total number of displayed packets = **127**

c. http.request.method==POST



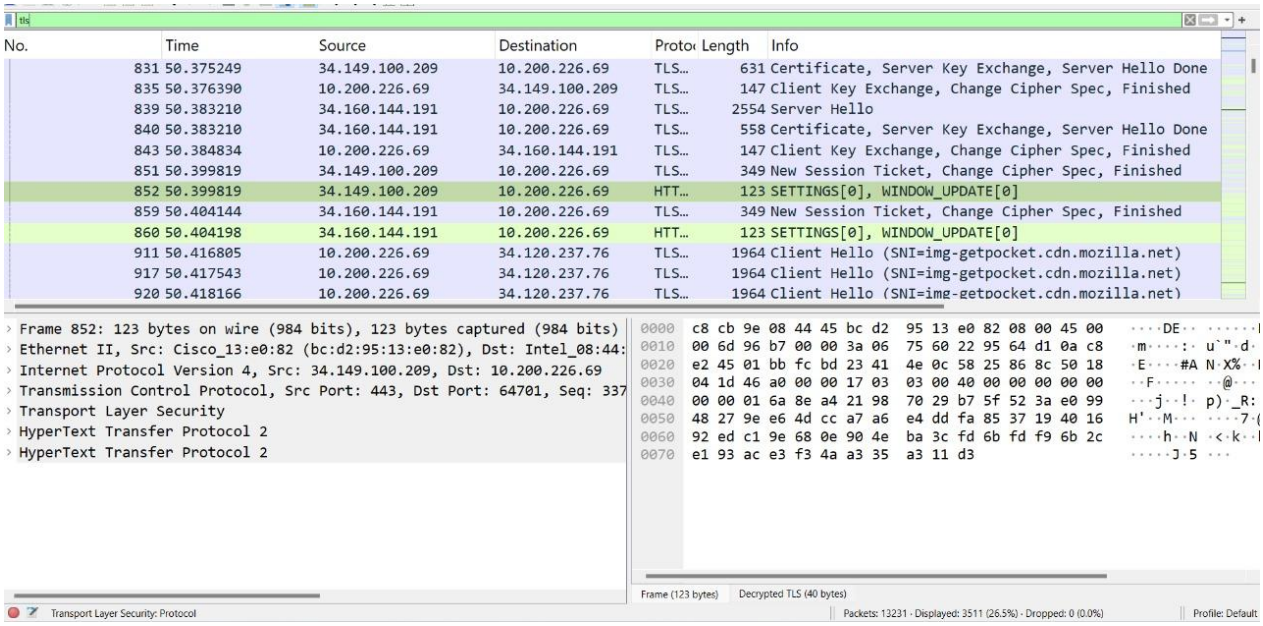
Total number of displayed packets = **83**

d. tcp



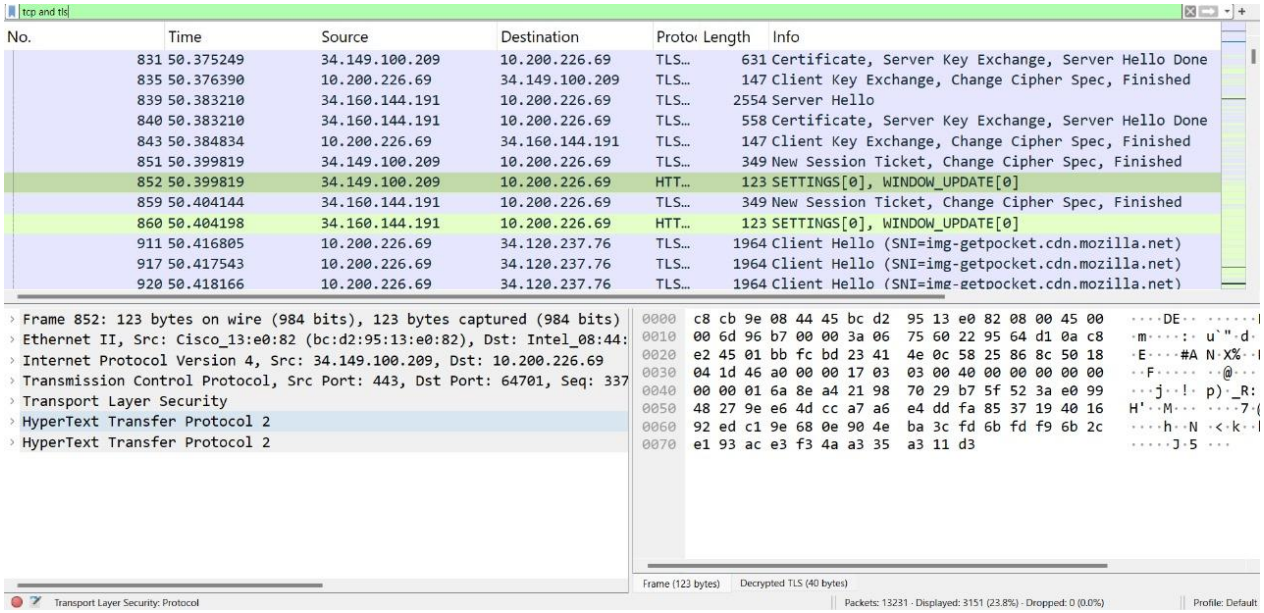
Total number of displayed packets = **9154**

e. tls



Total number of displayed packets = **3511**

f. tcp and tls

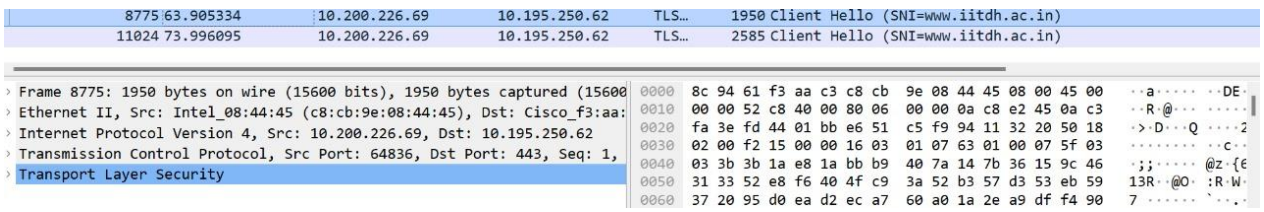


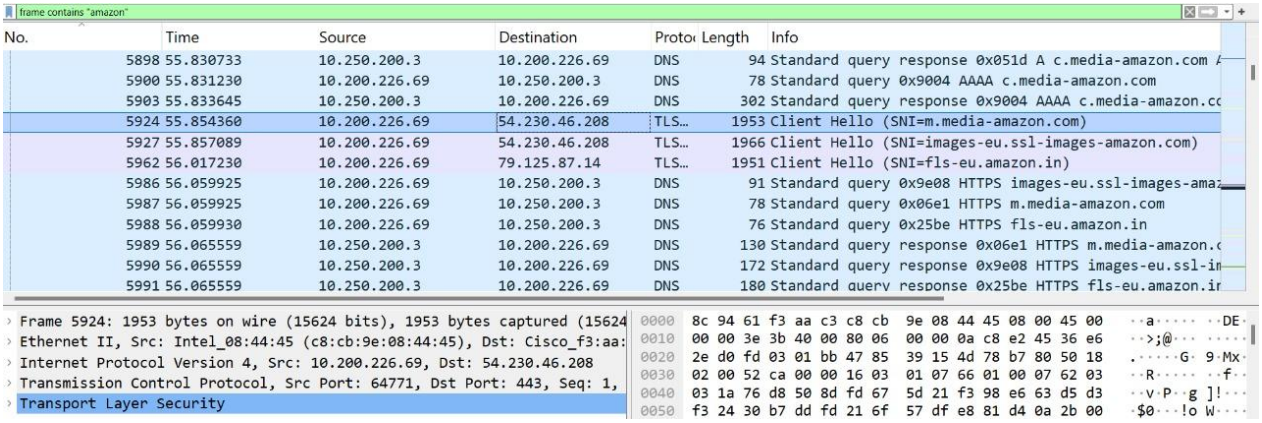
Total number of displayed packets = **3151**

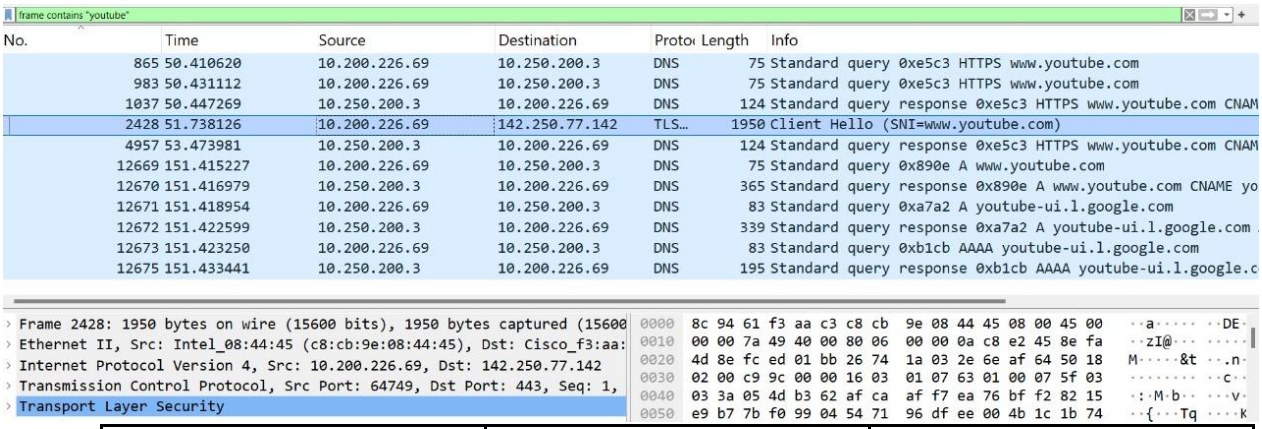
3. a) Analyze the network traffic for requests to the following domains: iitdh, Amazon, and YouTube. For iitdh and Amazon, identify the ClientHello packet, and for YouTube, identify the first standard HTTPS packet. Fill in the table below with the Domain, Source IP, and Destination IP for each case:

For iitdh and Amazon, to identify the ClientHello packet-
To isolate the **TLS ClientHello** packets,
Apply the filter:
frame contains == "iitdh.ac.in"
frame contains == "amazon.in"
frame contains == "youtube.com"

- This will show all ClientHello packets sent to servers for iitdh.ac.in, amazon.in and youtube.com.
- Choose the **first ClientHello packet** with the relevant Destination IP.







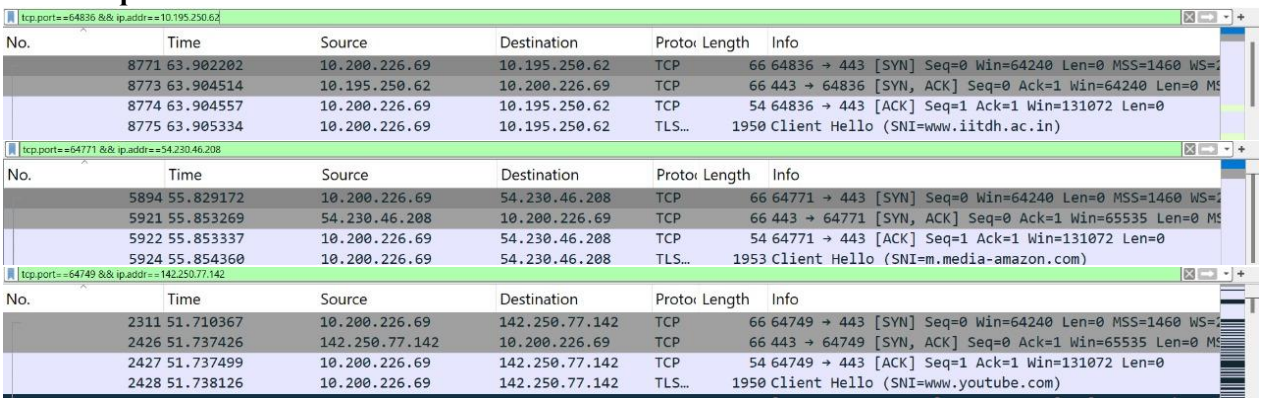
Domain	Source IP	Destination IP
iitdh.ac.in	**10.200.226.69**	**10.195.250.62**
amazon.in	**10.200.226.69**	**54.230.46.208**
youtube.com	**10.200.226.69**	**142.250.77.142**

b) For the observed packets in Q3.a), find the source and destination port numbers and fill the following table

Domain	Source Port	Destination Port
iitdh.ac.in	**64836**	**443**
amazon.in	**64771**	**443**
youtube.com	**64749**	**443**

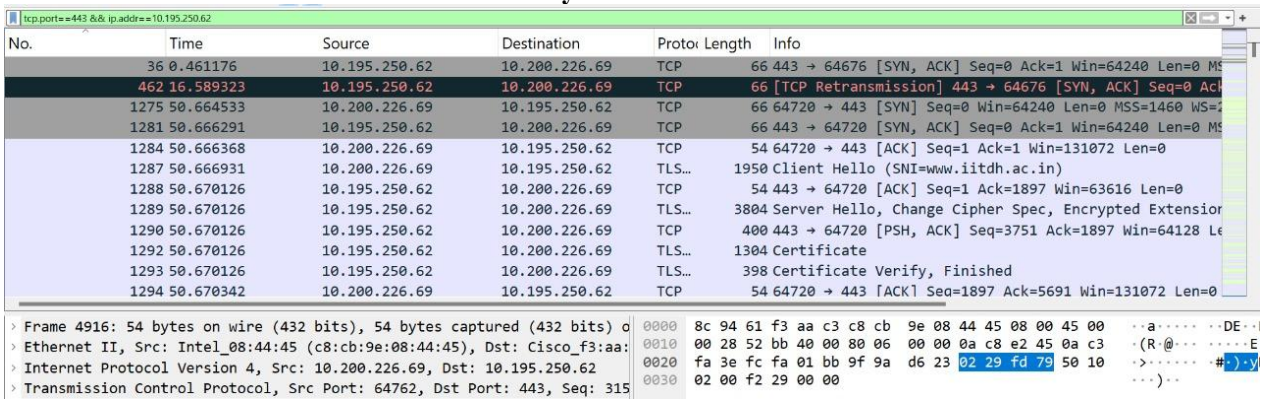
Hint: In the filter field, type tcp.port==sourceport and press enter to observe all the traces, such as handshakes or replies between your system and the requested domain names.

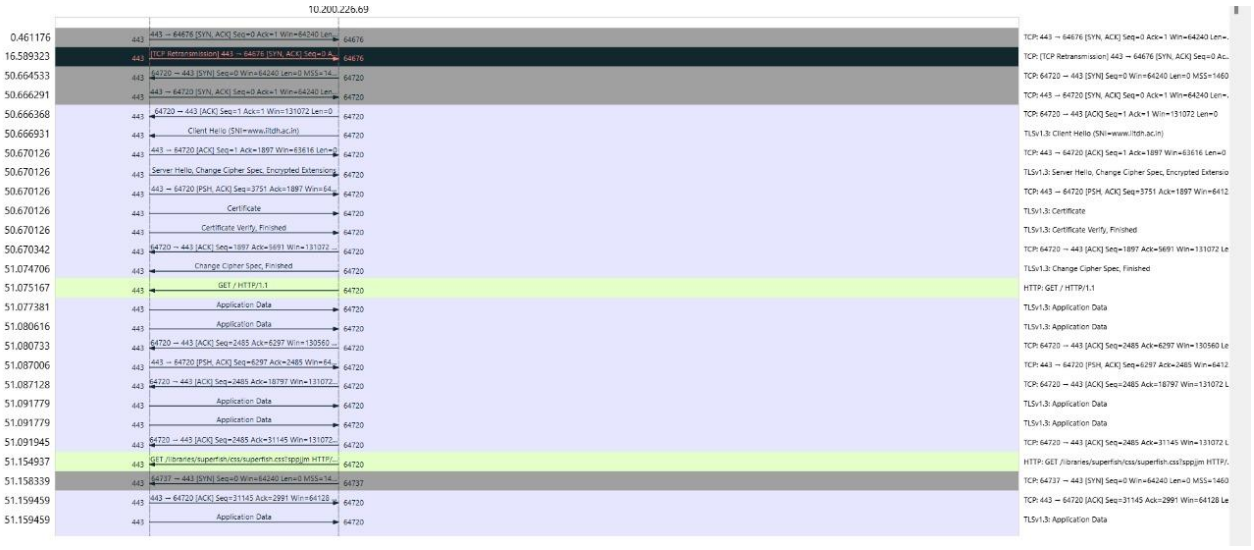
c) the time taken to complete the TCP handshake (SYN, SYNACK and ACK) for all the above-requested domain names.



Domain	**First SYN Timestamp** (T_syn)	**Final ACK Timestamp** (T_ack)	**TCP Handshake Time**=T_ack−Tsyn
iitdh.ac.in	63.902202	63.904557	0.002355
amazon.in	55.829172	55.853337	0.024165
youtube.com	51.710367	51.737499	0.027132

d) Use the filter: tcp.port==DEST_PORT inside the display filter of the Wireshark, where DEST_PORT is the port number for the iitdh.ac.in domain. Now goto Statistics->Flow Graph and observe the entire communication between your system and the iitdh.ac.in server. Take a screenshot and add it into your answer.





4. **In the request trace for the domain name "iitdh.ac.in", look for the first HTTP packet and answer the following questions:**

tcp.port==64836 && http.request.method==GET

No.	Time	Source	Destination	Protocol	Leng	Info
8784	63.912102	10.200.226.69	10.195.250.62	HTTP	1214	GET // HTTP/1.1
8790	63.932477	10.200.226.69	10.195.250.62	HTTP	1213	GET / HTTP/1.1

a) What is the HTTP request type

Look for the HTTP method in the packet details under Hypertext Transfer Protocol. Common request types are GET, POST, etc…

Here, the HTTP request type is **GET**

b) What is the version of the HTTP?

The HTTP version appears at the end of the request line, right after the method and the resource path.

GET/HTTP/1.1

In this, the HTTP version is HTTP/1.1. It could also be HTTP/2 in some cases, depending on the server.

c) What is the response status code for the above GET request packet?

Here, the response status code is 200, meaning the server successfully responded to the **GET** request.

http.response && ip.addr==10.195.250.62 && tcp.dstport==64836

No.	Time	Source	Destination	Protocol	Leng	Info
8789	63.923893	10.195.250.62	10.200.226.69	HTTP	853	HTTP/1.1 302 Found (text/html)
8800	63.942672	10.195.250.62	10.200.226.69	HTTP	996	HTTP/1.1 200 OK (text/html)

d) What is the time taken to receive the response (200 OK) for the above GET request packet? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display

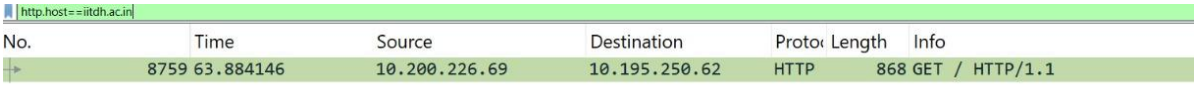
Format, then select Time-of-day.)

Identify the Time column for the GET request (8784th packet)=63.912102

corresponding 200 OK response (8800th packet)=63.942672

Subtract the time of the request from the response =(63.942672-63.912102)= 0.030570

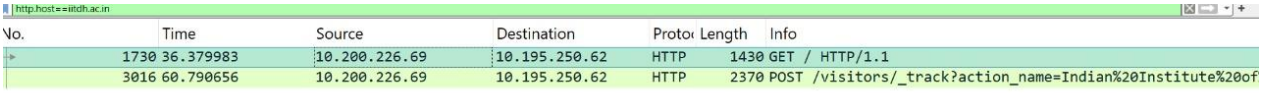
e) **Does the IP address of the domains you visited above same as you get their result using the command `host iitdh.ac.in` (change the domain in this command and check for other domains).**

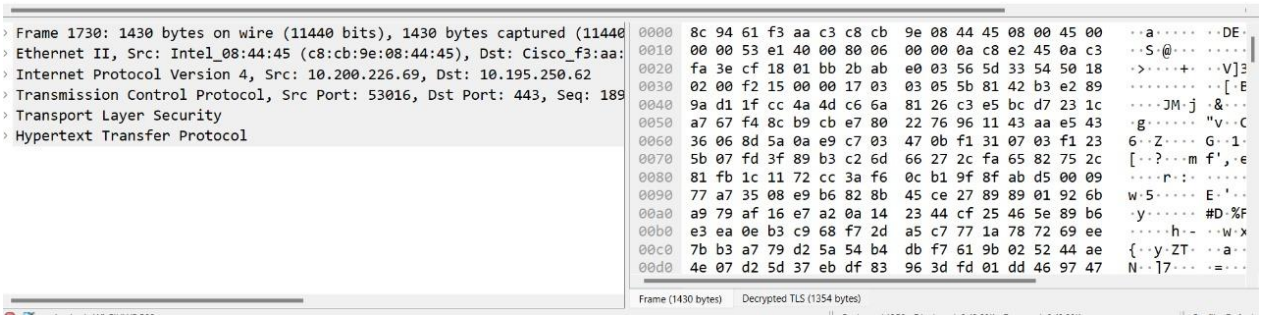


Yes, the IP address when **http.host==iitdh.ac.in** is the same as the IP address we got from the above commands which is 10.195.250.62 but for other domains.

We won't get any result with the filters **http.host==amazon.in** and **http.host==youtube.com** because both sites exclusively use HTTPS (HTTP over TLS) for secure communication. When HTTPS is used, the HTTP headers, including host, are encrypted and cannot be directly observed unless decrypted.

5. **Execute the above steps on Google Chrome, Safari or any other browsers also, check whether you will be able to see http protocol. Write down your analysis with screenshots.**

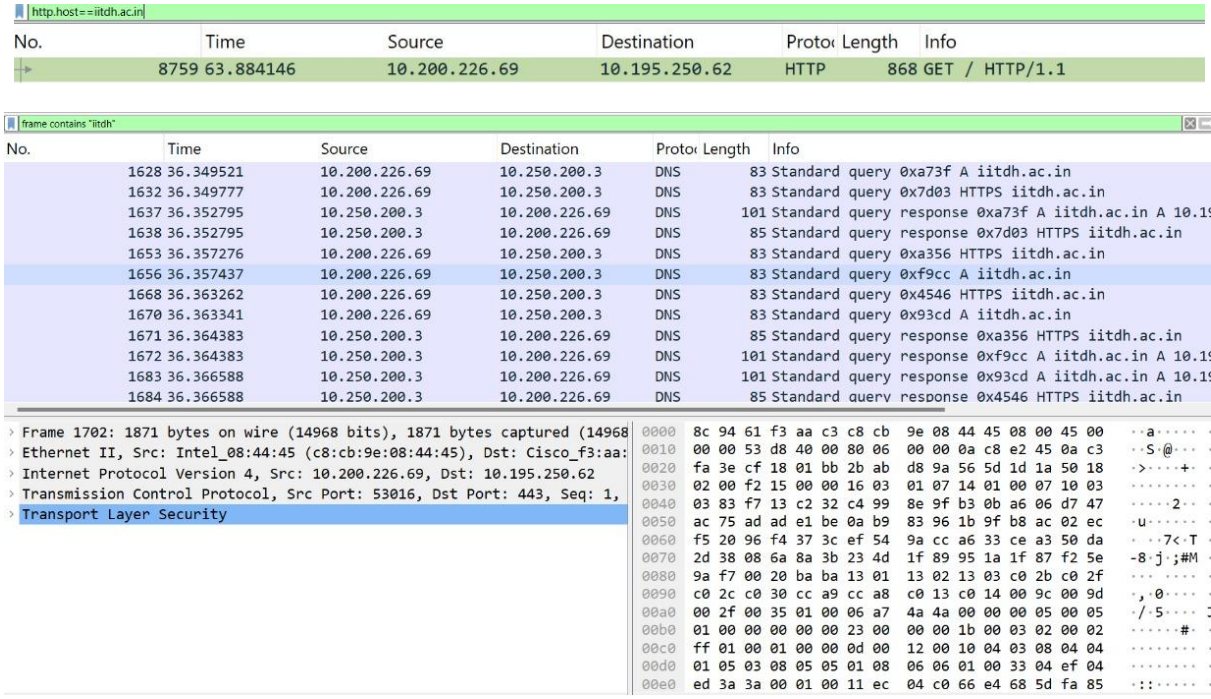


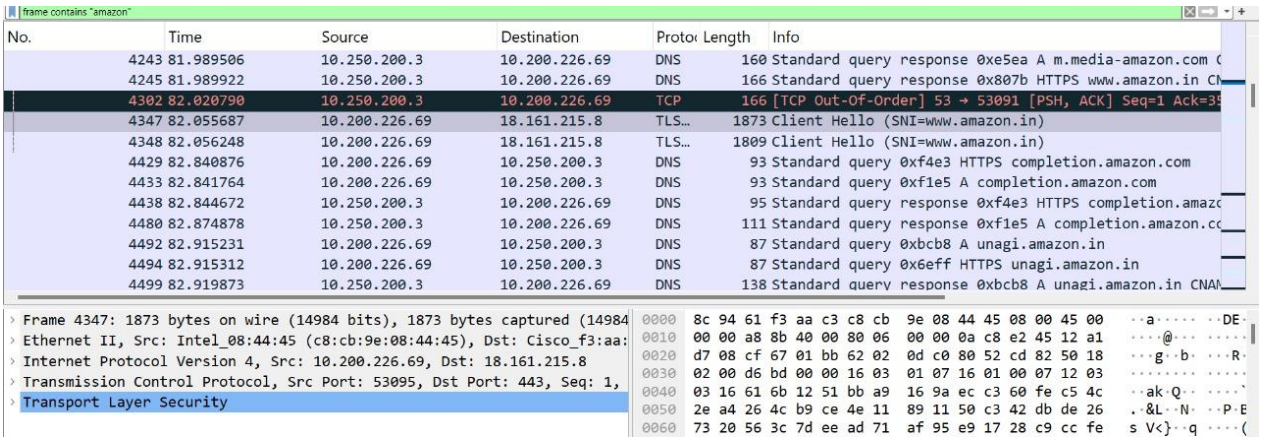


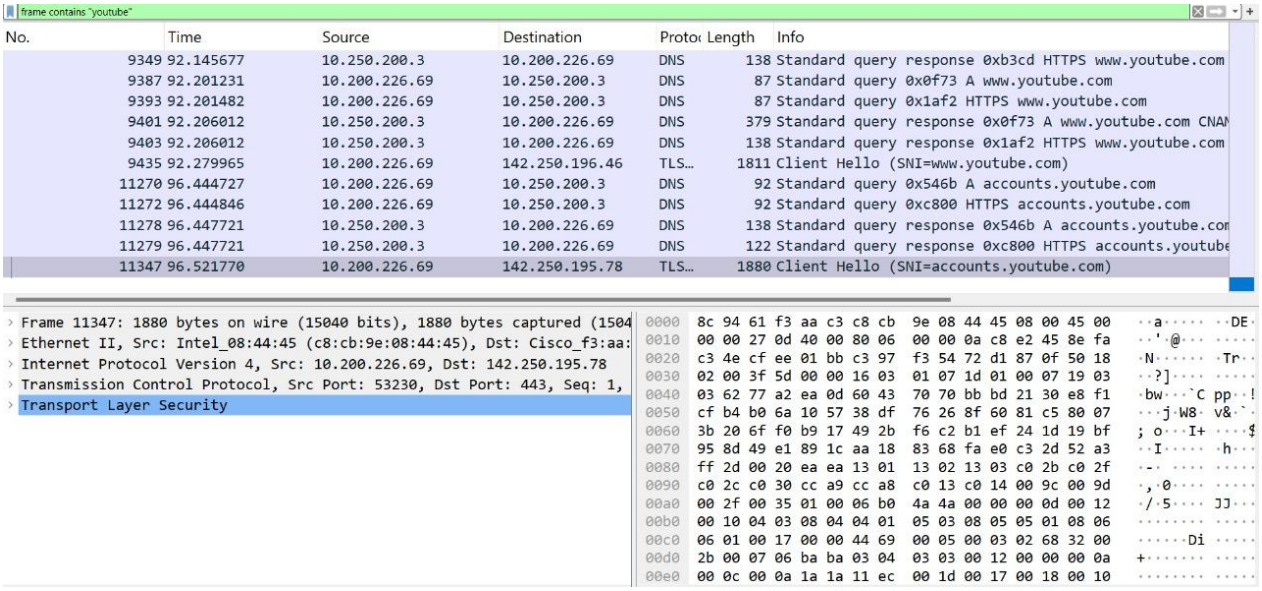
iitdh.ac.in:

- In **Google Chrome**:
  - No HTTP traffic visible due to HTTPS encryption.
  - After **TLS decryption** (using SSLKEYLOGFILE), HTTP traffic becomes visible when filtering with **http.host == "iitdh.ac.in".**

- In **Mozilla Firefox**:
  - Occasionally, plaintext HTTP (e.g., GET requests) is visible without decryption, likely due to how Firefox handles initial requests.
  - Without **TLS decryption** (using SSLKEYLOGFILE), HTTP traffic becomes visible when filtering with **http.host == "iitdh.ac.in".**







Summary from Screenshots-

Amazon and YouTube (amazon.in, youtube.com):

- Both exclusively use HTTP/2 or HTTP/3, where all traffic is encrypted.
- Even with decryption, HTTP traffic is not visible as these protocols do not expose plaintext HTTP headers.

Key Browser Comparison:

- Chrome requires decryption to reveal HTTP traffic for iitdh.ac.in.
- Firefox might show plaintext HTTP for some sites without decryption but behaves similarly to Chrome for Amazon and YouTube.

Conclusion:

- HTTPS or modern protocols like HTTP/2/3 prevent direct visibility of HTTP traffic, emphasizing improved security and performance.