Computer Networks Lab, Assignment 2

Suyash Gaurav

210010054

1 Part - 1

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

Packets highlighted in black indicate the packets is having some problems, such as delivered out-of-order and other TCP-related problems.

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

Command: **http.request.method == "GET" or http.request.method == "POST"**

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

DNS communicates via UDP, a connectionless and lightweight protocol designed for small queries and responses in a single packet. HTTP is based on TCP, a connection-oriented protocol that ensures reliable, bidirectional communication. Because of the potential size of HTTP messages, TCP is ideal for handling web pages or large files that may span multiple packets.

2 Part - 2

1. List the different protocols that appear in the protocol column in the unfiltered packet-listing window in wireshark GUI?

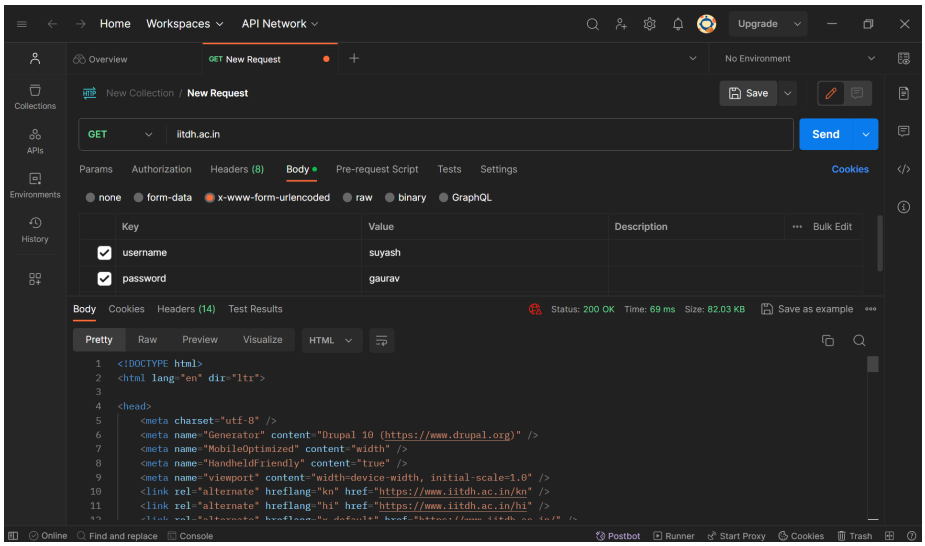
HTTP: Hypertext Transfer Protocol (Secure) for web browsing.
DHCP: Dynamic Host Configuration Protocol for IP address allocation.
TCP: Transmission Control Protocol for reliable communication.
UDP: User Datagram Protocol for connectionless communication.
ARP: Address Resolution Protocol for mapping IP addresses to MAC addresses.

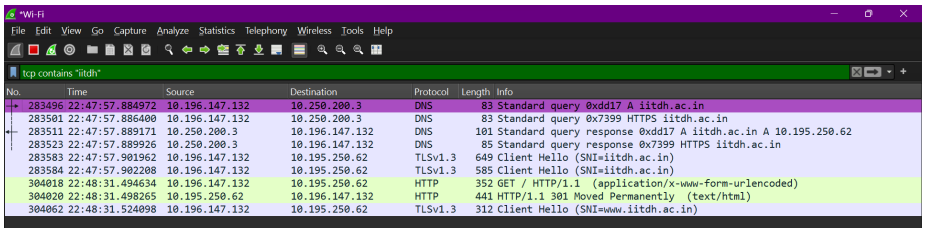
2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received for the web page you visited in your web browser? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)

I have sent a **GET** request to **iitdh.ac.in** using **Postman** service as shown in 1st picture below and server responded with status OK. 2nd picture depicts the pack-

ets corresponding to each trip (client to server and vice-versa).

Time Taken will be the difference of the timestamp of the HTTP GET message and the timestamp of the HTTP OK as shown in **time column (time-of-day)** in Wireshark.



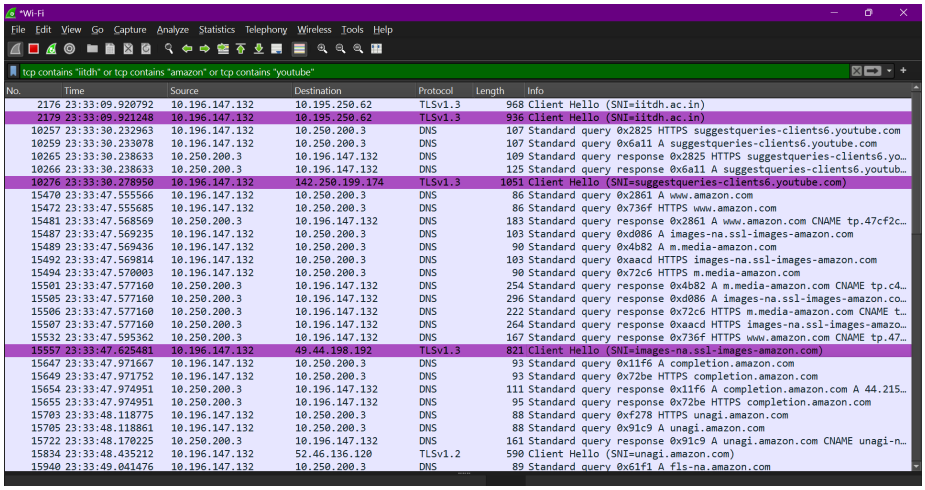


3. What is the Internet (IP) address of the URL you visited and what is the Internet address of your computer?

I have opened following websites: **iitdh.ac.in, www.amazon.in, www.youtube.com** in my browser.

Screenshots of Wireshark with filter command:
tcp contains "iitdh" or tcp contains "amazon" or tcp contains "youtube" is shown below. Clearly,

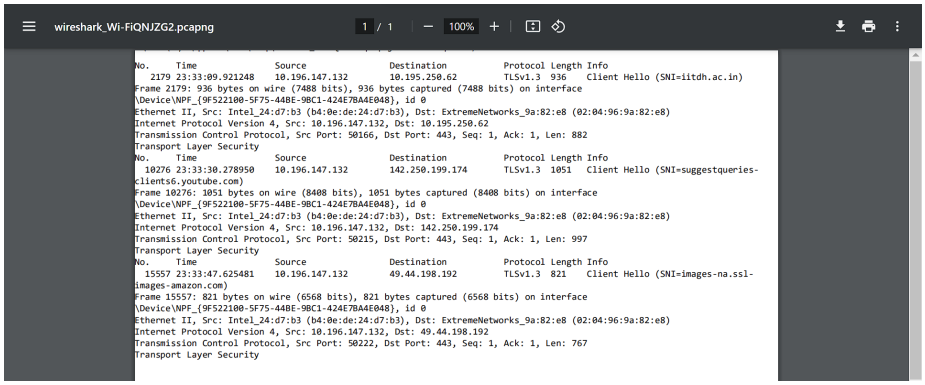
My computer IP address: 10.196.147.132 (in Source Column)
Amazon IP Address: 49.44.198.192 (in Destination Column)
IIT Dh IP Address: 10.195.250.62 (in Destination Column)
Youtube IP Address: 142.250.199.174 (in Destination Column)



4. Print the two HTTP messages displayed in wireshark GUI after you had visited the above URL through your web browser. To do so, select Print from the Wireshark File command menu, and select "Selected Packet Only" and then click Print.

Attached the pdf screenshot of HTTP messages for each

URL **iitdh.ac.in, www.amazon.in, www.youtube.com**:



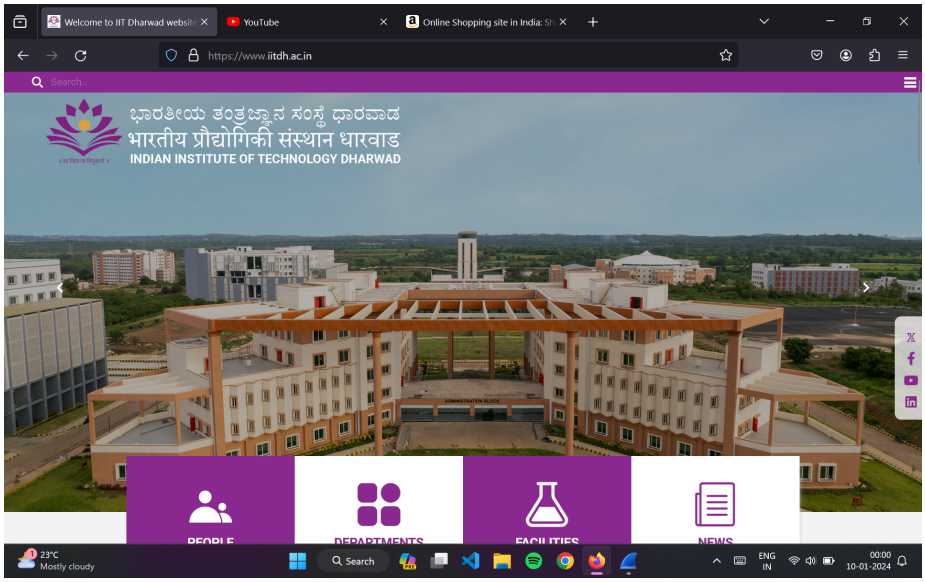
5. Execute the above steps on Google Chrome, Safari, or any other browsers also, check whether you will be able to see http protocol. Write down your analysis with screenshots.

On **Firefox**, I am able to see the HTTP protocols packets:

On **Chrome**, I am not able to see the HTTP protocol packets:

On **Microsoft Edge**, I am only able to see the HTTP protocol for **YouTube**, for others it is not showing:

Explanations: Chrome may have strict policies that limit the visibility of HTTP packets. The ability to capture packets in different browsers depends on developer tools and network monitoring capabilities. Firefox's broad developer tools allow for the viewing of all URLs, Edge may have limitations, and Chrome's stricter security measures might restrict packet visibility.



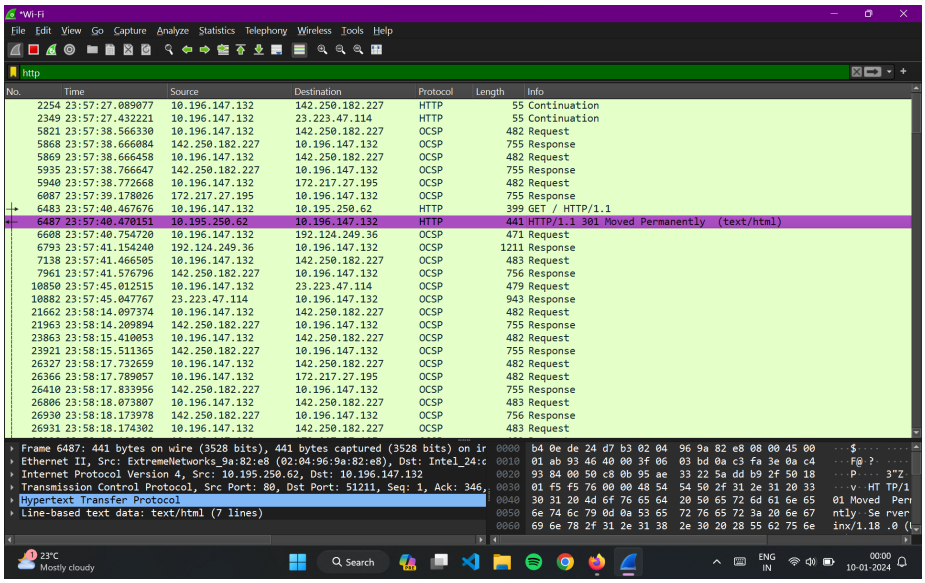
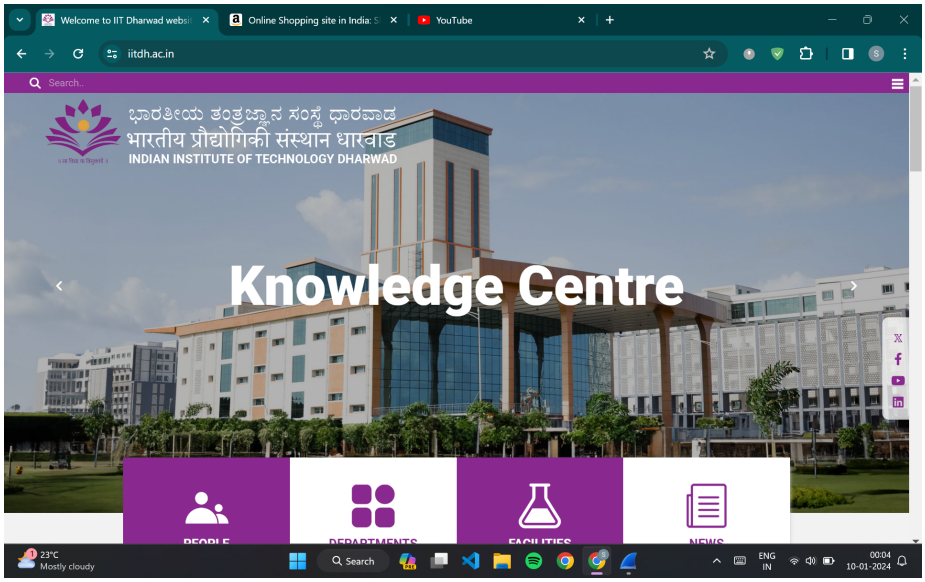


Figure 1: HTTP protocols on Firefox



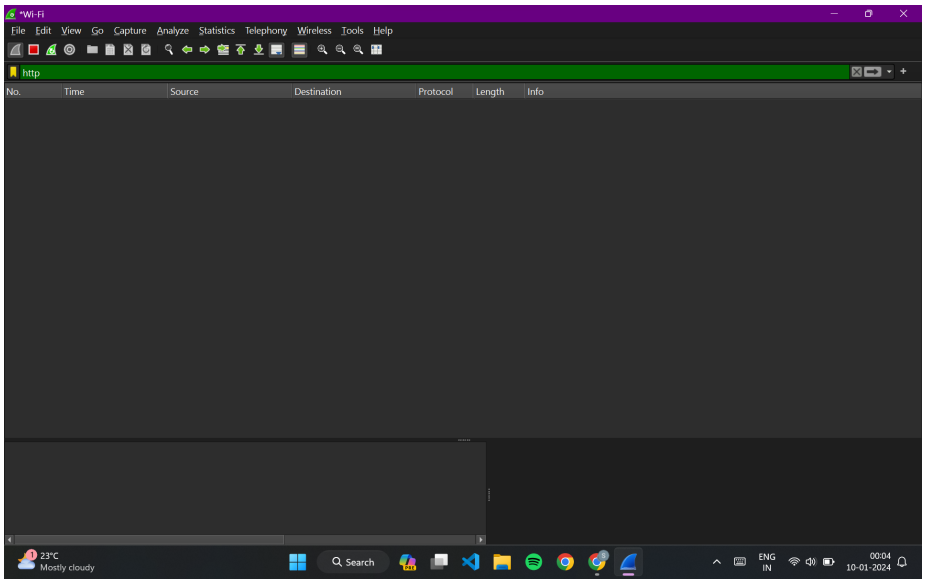
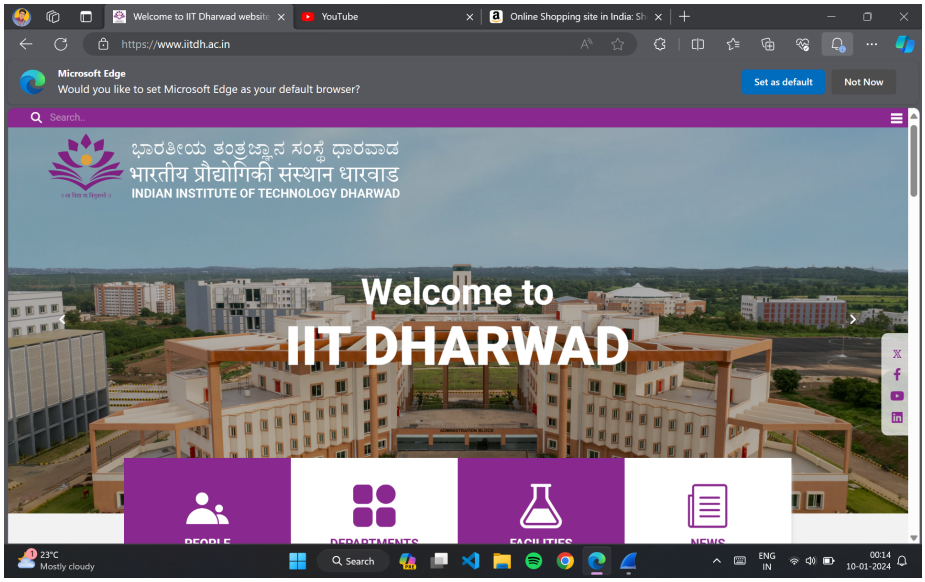


Figure 2: HTTP protocols on Chrome



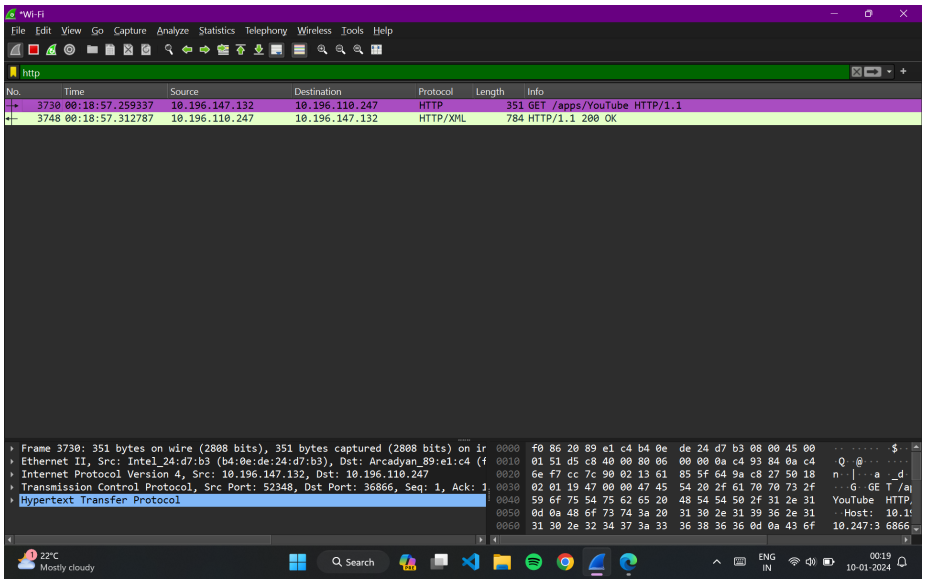


Figure 3: HTTP protocols on Microsoft Edge