

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

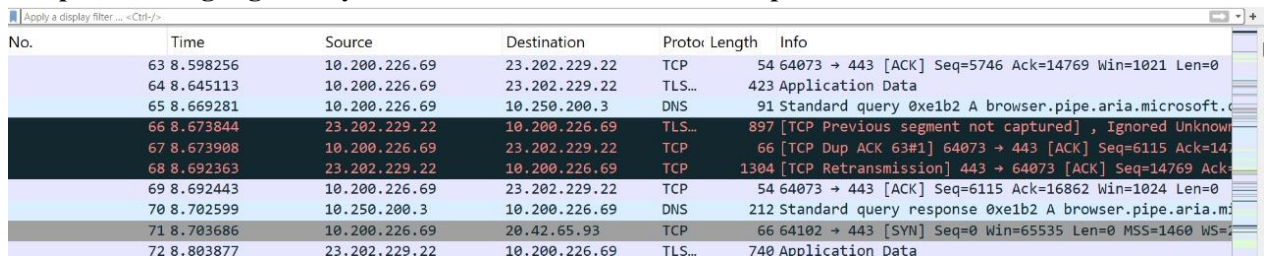
**Wireshark**

**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?



No.	Time	Source	Destination	Protocol	Length	Info
63	8.598256	10.200.226.69	23.202.229.22	TCP	54	64073 → 443 [ACK] Seq=5746 Ack=14769 Win=1021 Len=0
64	8.645113	10.200.226.69	23.202.229.22	TLS...	423	Application Data
65	8.669281	10.200.226.69	10.250.200.3	DNS	91	Standard query 0xe1b2 A browser.pipe.aria.microsoft.c
66	8.673844	23.202.229.22	10.200.226.69	TLS...	897	[TCP Previous segment not captured] , Ignored Unknown
67	8.673908	10.200.226.69	23.202.229.22	TCP	66	[TCP Dup ACK 63#1] 64073 → 443 [ACK] Seq=6115 Ack=147
68	8.692363	23.202.229.22	10.200.226.69	TCP	1304	[TCP Retransmission] 443 → 64073 [ACK] Seq=14769 Ack=
69	8.692443	10.200.226.69	23.202.229.22	TCP	54	64073 → 443 [ACK] Seq=6115 Ack=16862 Win=1024 Len=0
70	8.702599	10.250.200.3	10.200.226.69	DNS	212	Standard query response 0xe1b2 A browser.pipe.aria.m
71	8.703686	10.200.226.69	20.42.65.93	TCP	66	64102 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=
72	8.803877	23.202.229.22	10.200.226.69	TLS...	740	Application Data

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 display filter field of Wireshark and answer with the count of the total number of displayed packets for each of the filters.

### a. frame contains “iitdh”

The screenshot shows the Wireshark interface with the filter 'frame contains iitdh' applied. The packet list displays 23 packets, all of which are DNS queries or responses to www.iitdh.ac.in. The packet details pane shows the structure of a DNS query packet.

No.	Time	Source	Destination	Protocol	Length	Info
1274	50.663803	10.200.226.69	10.250.200.3	DNS	75	Standard query 0x69ac HTTPS www.iitdh.ac.in
1276	50.664533	10.200.226.69	10.250.200.3	DNS	75	Standard query 0x6d82 AAAA www.iitdh.ac.in
1277	50.665447	10.250.200.3	10.200.226.69	DNS	75	Standard query response 0x69ac HTTPS www.iitdh.ac.in
1282	50.666291	10.250.200.3	10.200.226.69	DNS	75	Standard query response 0x6d82 AAAA www.iitdh.ac.in
1287	50.666931	10.200.226.69	10.195.250.62	TLS...	1950	Client Hello (SNI=www.iitdh.ac.in)
1577	51.165576	10.200.226.69	10.195.250.62	TLS...	2585	Client Hello (SNI=www.iitdh.ac.in)
1578	51.166843	10.200.226.69	10.195.250.62	TLS...	2585	Client Hello (SNI=www.iitdh.ac.in)
1601	51.174408	10.200.226.69	10.195.250.62	TLS...	1950	Client Hello (SNI=www.iitdh.ac.in)
1602	51.174877	10.200.226.69	10.195.250.62	TLS...	1950	Client Hello (SNI=www.iitdh.ac.in)
1610	51.175435	10.200.226.69	10.195.250.62	TLS...	1950	Client Hello (SNI=www.iitdh.ac.in)
4876	53.369477	10.200.226.69	10.195.250.62	TLS...	1950	Client Hello (SNI=www.iitdh.ac.in)
7819	59.551154	10.200.226.69	10.250.200.3	DNS	75	Standard query 0x167f HTTPS www.iitdh.ac.in

Frame 1274: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 0  
Ethernet II, Src: Intel\_08:44:45 (c8:cb:9e:08:44:45), Dst: Cisco\_f3:aa:00:00:00:00  
Internet Protocol Version 4, Src: 10.200.226.69, Dst: 10.250.200.3  
User Datagram Protocol, Src Port: 51419, Dst Port: 53  
Domain Name System (query)

0000 8c 94 61 f3 aa c3 c8 cb 9e 08 44 45 00 00 45 00 ..a.....DE..  
0010 00 3d 91 d7 00 00 00 11 00 00 0a c8 e2 45 0a fa ..=.....E..  
0020 c8 03 c8 db 00 35 00 29 c0 45 69 ac 01 00 00 01 .....5.)Ei...  
0030 00 00 00 00 00 03 77 77 77 05 69 69 74 64 68 .....w ww iit  
0040 02 61 63 02 69 6e 00 00 41 00 01 ..ac.in.. A..

Wireshark: Wi-Fi-MMMPL02.pcapng | Packets: 13231 - Displayed: 23 (0.2%) - Dropped: 0 (0.0%) | Profile: Default

Total number of displayed packets = 23

## b. http.request.method==GET

No.	Time	Source	Destination	Protocol	Length	Info
768	50.209803	10.200.226.69	34.107.221.82	HTTP	357	GET /canonical.html HTTP/1.1
804	50.318833	10.200.226.69	34.107.221.82	HTTP	374	GET /success.txt?ipv4 HTTP/1.1
1459	51.018914	10.200.226.69	34.107.221.82	HTTP	374	GET /success.txt?ipv4 HTTP/1.1
1462	51.027261	10.200.226.69	34.107.243.93	HTTP	686	GET / HTTP/1.1
1497	51.075167	10.200.226.69	10.195.250.62	HTTP	562	GET / HTTP/1.1
1554	51.154937	10.200.226.69	10.195.250.62	HTTP	560	GET /libraries/superfish/css/superfish.css?spjpm HTTP/1.1
1570	51.160999	10.200.226.69	10.195.250.62	HTTP	571	GET /core/modules/views/css/views-responsive-grid.css HTTP/1.1
1579	51.167856	10.200.226.69	10.195.250.62	HTTP	577	GET /core/modules/system/css/components/clearfix.module.css HTTP/1.1
1588	51.170552	10.200.226.69	10.195.250.62	HTTP	574	GET /core/modules/system/css/components/align.module.css HTTP/1.1
1592	51.171921	10.200.226.69	10.195.250.62	HTTP	579	GET /core/modules/system/css/components/fieldgroup.module.css HTTP/1.1
1593	51.172143	10.200.226.69	10.195.250.62	HTTP	585	GET /core/modules/system/css/components/container-inline.module.css HTTP/1.1
1623	51.178483	10.200.226.69	10.195.250.62	HTTP	571	GET /core/modules/system/css/components/is.module.css HTTP/1.1

> Frame 804: 374 bytes on wire (2992 bits), 374 bytes captured (2992 bits) on interface 0  
> Ethernet II, Src: Intel\_08:44:45 (c8:cb:9e:08:44:45), Dst: Cisco\_f3:aa:00:00:00:00  
> Internet Protocol Version 4, Src: 10.200.226.69, Dst: 34.107.221.82  
> Transmission Control Protocol, Src Port: 64700, Dst Port: 80, Seq: 1, A  
> Hypertext Transfer Protocol

0000 8c 94 61 f3 aa c3 c8 cb 9e 08 44 45 08 00 45 00 ..a.....DE-  
0010 01 68 ad 21 40 00 80 06 00 00 0a c8 e2 45 22 6b ..h!@.....  
0020 dd 52 fc bc 00 50 5d 61 65 6f 78 39 39 04 50 18 ..R..Pjaeox95  
0030 02 00 ee 25 00 00 47 45 54 20 2f 73 75 63 63 65 ..%..GE T /su  
0040 73 73 2e 74 78 74 3f 69 70 76 34 20 48 54 50 ss.txt?i pv4 t  
0050 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 64 65 74 65 /1.1..Ho st: c  
0060 63 74 70 6f 72 74 61 6c 2e 66 69 72 65 66 6f 78 ctportal .fire  
0070 2e 63 6f 6d 0d 0a 55 73 65 72 2d 41 67 65 6e 74 .com..Us er-Ag  
0080 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 : Mozill a/5.0  
0090 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 indows N T 10.  
00a0 57 69 6e 36 34 3b 20 78 36 34 3b 20 72 76 3a 31 Win64; x 64; r  
00b0 33 34 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 30 34.0) Ge cko/2  
00c0 30 31 30 31 20 46 69 72 65 66 6f 78 2f 31 33 34 0101 Fir efox/  
00d0 2e 30 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d .0..Acce pt: \*  
00e0 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 -Accept- Langu

wireshark\_Wi-FiMMPL02.pcapng Packets: 13231 - Displayed: 127 (1.0%) - Dropped: 0 (0.0%) Profile: Default

Total number of displayed packets = 127

## c. http.request.method==POST

No.	Time	Source	Destination	Protocol	Length	Info
856	50.402940	10.200.226.69	202.144.79.8	OCSP	495	Request
862	50.404504	10.200.226.69	202.144.79.8	OCSP	495	Request
1073	50.457595	10.200.226.69	202.144.79.8	OCSP	495	Request
1088	50.464460	10.200.226.69	202.144.79.8	OCSP	495	Request
1104	50.471759	10.200.226.69	202.144.79.6	OCSP	495	Request
1116	50.480988	10.200.226.69	202.144.79.8	OCSP	495	Request
1181	50.527443	10.200.226.69	202.144.79.8	OCSP	495	Request
1197	50.555401	10.200.226.69	202.144.79.8	OCSP	495	Request
1212	50.566811	10.200.226.69	202.144.79.8	OCSP	495	Request
1232	50.600534	10.200.226.69	142.250.195.131	OCSP	498	Request
1249	50.627562	10.200.226.69	202.144.79.6	OCSP	495	Request
1270	50.653672	10.200.226.69	142.250.195.131	OCSP	498	Request

> Frame 856: 495 bytes on wire (3960 bits), 495 bytes captured (3960 bits) on interface 0  
> Ethernet II, Src: Intel\_08:44:45 (c8:cb:9e:08:44:45), Dst: Cisco\_f3:aa:00:00:00:00  
> Internet Protocol Version 4, Src: 10.200.226.69, Dst: 202.144.79.8  
> Transmission Control Protocol, Src Port: 64704, Dst Port: 80, Seq: 1, A  
> Hypertext Transfer Protocol  
> Online Certificate Status Protocol

0000 8c 94 61 f3 aa c3 c8 cb 9e 08 44 45 08 00 45 00 ..a.....DE-  
0010 01 e1 21 ff 40 00 80 06 00 00 0a c8 e2 45 ca 90 ..!.@.....  
0020 4f 08 fc c0 00 50 e3 99 08 98 37 5a 1f 27 50 18 O...P...7Z  
0030 02 00 08 7a 00 00 50 4f 53 54 20 2f 20 48 54 54 ...z..PO ST /  
0040 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 72 31 31 P/1.1..H ost:  
0050 2e 6f 2e 6c 65 6e 63 72 2e 6f 72 67 0d 0a 55 73 .o.lencr .org  
0060 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c er-Agent : Moz  
0070 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e a/5.0 (W indow  
0080 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 T 10.0; Win64  
0090 36 34 3b 20 72 76 3a 31 33 34 2e 30 29 20 47 65 64; rv:1 34.0)  
00a0 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 69 72 cko/2010 0101  
00b0 65 66 6f 78 2f 31 33 34 2e 30 0d 0a 41 63 63 65 efox/134 .0..A  
00c0 70 74 3a 20 2a 2f 2a 0d 0a 41 63 63 65 70 74 2d pt: \*/\* .Acce  
00d0 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 55 53 2c Language : en-  
00e0 65 6e 3b 71 3d 30 2e 35 0d 0a 41 63 63 65 70 74 en;q=0.5 .Acc

wireshark\_Wi-FiMMPL02.pcapng Packets: 13231 - Displayed: 83 (0.6%) - Dropped: 0 (0.0%) Profile: Default

Total number of displayed packets = 83



#### d. tcp

No.	Time	Source	Destination	Protocol	Length	Info
850	50.399787	10.200.226.69	34.107.221.82	TCP	54	64700 → 80 [ACK] Seq=321 Ack=217 Win=130816 Len=0
851	50.399819	34.149.100.209	10.200.226.69	TLS...	349	New Session Ticket, Change Cipher Spec, Finished
852	50.399819	34.149.100.209	10.200.226.69	HTT...	123	SETTINGS[0], WINDOW_UPDATE[0]
853	50.399898	10.200.226.69	34.149.100.209	TCP	54	64701 → 443 [ACK] Seq=312 Ack=3442 Win=130816 Len=0
854	50.402471	202.144.79.8	10.200.226.69	TCP	66	80 → 64704 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=
855	50.402685	10.200.226.69	202.144.79.8	TCP	54	64704 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
856	50.402940	10.200.226.69	202.144.79.8	OCSP	495	Request
857	50.403981	202.144.79.8	10.200.226.69	TCP	66	80 → 64703 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=
858	50.404080	10.200.226.69	202.144.79.8	TCP	54	64703 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
859	50.404144	34.160.144.191	10.200.226.69	TLS...	349	New Session Ticket, Change Cipher Spec, Finished
860	50.404198	34.160.144.191	10.200.226.69	HTT...	123	SETTINGS[0], WINDOW_UPDATE[0]
861	50.404233	10.200.226.69	34.160.144.191	TCP	54	64702 → 443 [ACK] Seq=310 Ack=3369 Win=130816 Len=0

> Frame 856: 495 bytes on wire (3960 bits), 495 bytes captured (3960 bits) on interface 0  
 > Ethernet II, Src: Intel\_08:44:45 (c8:cb:9e:08:44:45), Dst: Cisco\_f3:aa:00:00:00:00  
 > Internet Protocol Version 4, Src: 10.200.226.69, Dst: 202.144.79.8  
 > Transmission Control Protocol, Src Port: 64704, Dst Port: 80, Seq: 1, A  
 > Hypertext Transfer Protocol  
 > Online Certificate Status Protocol

0000 8c 94 61 f3 aa c3 c8 cb 9e 08 44 45 08 00 45 00 ...a...DE...  
 0010 01 e1 21 ff 40 00 80 06 00 00 0a c8 e2 45 ca 90 ...!:@...  
 0020 4f 08 fc c0 00 50 e3 99 08 98 37 5a 1f 27 50 18 O...P...7Z...  
 0030 02 00 08 7a 00 00 50 4f 53 54 20 2f 20 48 54 54 ...z...PO ST /  
 0040 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 72 31 31 P/1.1...H ost:  
 0050 2e 6f 2e 6c 65 6e 63 72 2e 6f 72 67 0d 0a 55 73 .o.lencr...org:  
 0060 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c er-Agent : Moz  
 0070 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e a/5.0 (W indow  
 0080 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 T 10.0; Win64  
 0090 36 34 3b 20 72 76 3a 31 33 34 2e 30 29 20 47 65 64; rv:1 34.0)  
 00a0 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 69 72 cko/2010 0101  
 00b0 65 66 6f 78 2f 31 33 34 2e 30 0d 0a 41 63 63 65 efox/134 .0...A  
 00c0 70 74 3a 20 2a 2f 2a 0d 0a 41 63 63 65 70 74 2d pt: \*/\*...Acce  
 00d0 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 55 53 2c Language : en-  
 00e0 65 6e 3b 71 3d 30 2e 35 0d 0a 41 63 63 65 70 74 en;q=0.5 ...Acc

Transmission Control Protocol: Protocol      Packets: 13231 - Displayed: 9154 (69.2%) - Dropped: 0 (0.0%)      Profile: Default

Total number of displayed packets = 9154

#### e. tls

No.	Time	Source	Destination	Protocol	Length	Info
831	50.375249	34.149.100.209	10.200.226.69	TLS...	631	Certificate, Server Key Exchange, Server Hello Done
835	50.376390	10.200.226.69	34.149.100.209	TLS...	147	Client Key Exchange, Change Cipher Spec, Finished
839	50.383210	34.160.144.191	10.200.226.69	TLS...	2554	Server Hello
840	50.383210	34.160.144.191	10.200.226.69	TLS...	558	Certificate, Server Key Exchange, Server Hello Done
843	50.384834	10.200.226.69	34.160.144.191	TLS...	147	Client Key Exchange, Change Cipher Spec, Finished
851	50.399819	34.149.100.209	10.200.226.69	TLS...	349	New Session Ticket, Change Cipher Spec, Finished
852	50.399819	34.149.100.209	10.200.226.69	HTT...	123	SETTINGS[0], WINDOW_UPDATE[0]
859	50.404144	34.160.144.191	10.200.226.69	TLS...	349	New Session Ticket, Change Cipher Spec, Finished
860	50.404198	34.160.144.191	10.200.226.69	HTT...	123	SETTINGS[0], WINDOW_UPDATE[0]
911	50.416805	10.200.226.69	34.120.237.76	TLS...	1964	Client Hello (SNI=img-getpocket.cdn.mozilla.net)
917	50.417543	10.200.226.69	34.120.237.76	TLS...	1964	Client Hello (SNI=img-getpocket.cdn.mozilla.net)
920	50.418166	10.200.226.69	34.120.237.76	TLS...	1964	Client Hello (SNI=img-getpocket.cdn.mozilla.net)

> Frame 852: 123 bytes on wire (984 bits), 123 bytes captured (984 bits) on interface 0  
 > Ethernet II, Src: Cisco\_13:e0:82 (bc:d2:95:13:e0:82), Dst: Intel\_08:44:45:00:00:00  
 > Internet Protocol Version 4, Src: 34.149.100.209, Dst: 10.200.226.69  
 > Transmission Control Protocol, Src Port: 443, Dst Port: 64701, Seq: 337  
 > Transport Layer Security  
 > HyperText Transfer Protocol 2  
 > HyperText Transfer Protocol 2

0000 c8 cb 9e 08 44 45 bc d2 95 13 e0 82 08 00 45 00 ...DE...  
 0010 00 6d 96 b7 00 00 3a 06 75 60 22 95 64 d1 0a c8 .m...: u" d  
 0020 e2 45 01 bb fc bd 23 41 4e 0c 58 25 86 8c 50 18 -E...#A N:X%...  
 0030 04 1d 46 a0 00 00 17 03 03 00 40 00 00 00 00 00 ...F...@...  
 0040 00 00 01 6a 8e a4 21 98 70 29 b7 5f 52 3a e0 99 ...j...! p)\_R:  
 0050 48 27 9e e6 4d cc a7 a6 e4 dd fa 85 37 19 40 16 H'.M...7...  
 0060 92 ed c1 9e 68 0e 90 4e ba 3c fd 6b fd f9 6b 2c ...h.N <k...  
 0070 e1 93 ac e3 f3 4a a3 35 a3 11 d3 ...J.5 ...

Transport Layer Security: Protocol      Frame (123 bytes)    Decrypted TLS (40 bytes)      Packets: 13231 - Displayed: 3511 (26.5%) - Dropped: 0 (0.0%)      Profile: Default

Total number of displayed packets = 3511

## f. tcp and tls

No.	Time	Source	Destination	Protocol	Length	Info
831	50.375249	34.149.100.209	10.200.226.69	TLS...	631	Certificate, Server Key Exchange, Server Hello Done
835	50.376390	10.200.226.69	34.149.100.209	TLS...	147	Client Key Exchange, Change Cipher Spec, Finished
839	50.383210	34.160.144.191	10.200.226.69	TLS...	2554	Server Hello
840	50.383210	34.160.144.191	10.200.226.69	TLS...	558	Certificate, Server Key Exchange, Server Hello Done
843	50.384834	10.200.226.69	34.160.144.191	TLS...	147	Client Key Exchange, Change Cipher Spec, Finished
851	50.399819	34.149.100.209	10.200.226.69	TLS...	349	New Session Ticket, Change Cipher Spec, Finished
852	50.399819	34.149.100.209	10.200.226.69	HTT...	123	SETTINGS[0], WINDOW_UPDATE[0]
859	50.404144	34.160.144.191	10.200.226.69	TLS...	349	New Session Ticket, Change Cipher Spec, Finished
860	50.404198	34.160.144.191	10.200.226.69	HTT...	123	SETTINGS[0], WINDOW_UPDATE[0]
911	50.416805	10.200.226.69	34.120.237.76	TLS...	1964	Client Hello (SNI=img-getpocket.cdn.mozilla.net)
917	50.417543	10.200.226.69	34.120.237.76	TLS...	1964	Client Hello (SNI=img-getpocket.cdn.mozilla.net)
920	50.418166	10.200.226.69	34.120.237.76	TLS...	1964	Client Hello (SNI=img-getpocket.cdn.mozilla.net)

> Frame 852: 123 bytes on wire (984 bits), 123 bytes captured (984 bits) > Ethernet II, Src: Cisco_13:e0:82 (bc:d2:95:13:e0:82), Dst: Intel_08:44: > Internet Protocol Version 4, Src: 34.149.100.209, Dst: 10.200.226.69 > Transmission Control Protocol, Src Port: 443, Dst Port: 64701, Seq: 337 > Transport Layer Security > HyperText Transfer Protocol 2 > HyperText Transfer Protocol 2	<pre> 0000 c8 cb 9e 08 44 45 bc d2 95 13 e0 82 08 00 45 00 ...DE... 0010 00 6d 96 b7 00 00 3a 06 75 60 22 95 64 d1 0a c8 ...m...: u" d 0020 e2 45 01 bb fc bd 23 41 4e 0c 58 25 86 8c 50 18 ...E...#A N:X%..l 0030 04 1d 46 a0 00 00 17 03 03 00 40 00 00 00 00 00 ...F.....@... 0040 00 00 01 6a 8e a4 21 98 70 29 b7 5f 52 3a e0 99 ...j...! p) _R: 0050 48 27 9e e6 4d cc a7 a6 e4 dd fa 85 37 19 40 16 H'.M...7( 0060 92 ed c1 9e 68 0e 90 4e ba 3c fd 6b fd f9 6b 2c ...h.N &lt;k..l 0070 e1 93 ac e3 f3 4a a3 35 a3 11 d3 .....J.5 ... </pre>
--	---

Transport Layer Security: Protocol

Frame (123 bytes) | Decrypted TLS (40 bytes)

Packets: 13231 - Displayed: 3151 (23.8%) - Dropped: 0 (0.0%)

Profile: Default

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.

8775	63.905334	10.200.226.69	10.195.250.62	TLS...	1950	Client Hello (SNI=www.iitdh.ac.in)
11024	73.996095	10.200.226.69	10.195.250.62	TLS...	2585	Client Hello (SNI=www.iitdh.ac.in)

> Frame 8775: 1950 bytes on wire (15600 bits), 1950 bytes captured (15600) > Ethernet II, Src: Intel_08:44:45 (c8:cb:9e:08:44:45), Dst: Cisco_f3:aa: > Internet Protocol Version 4, Src: 10.200.226.69, Dst: 10.195.250.62 > Transmission Control Protocol, Src Port: 64836, Dst Port: 443, Seq: 1, > Transport Layer Security	<pre> 0000 8c 94 61 f3 aa c3 c8 cb 9e 08 44 45 08 00 45 00 ...a...DE... 0010 00 00 52 c8 40 00 80 06 00 00 0a c8 e2 45 0a c3 ...R:@... 0020 fa 3e fd 44 01 bb e6 51 c5 f9 94 11 32 20 50 18 ...&gt;D...Q...2 0030 02 00 f2 15 00 00 16 03 01 07 63 01 00 07 5f 03 ...c... 0040 03 3b 3b 1a e8 1a bb b9 40 7a 14 7b 36 15 9c 46 ...;...@z...{ 0050 31 33 52 e8 f6 40 4f c9 3a 52 b3 57 d3 53 eb 59 13R...@...:R.W 0060 37 20 95 d0 ea d2 ec a7 60 a0 1a 2e a9 df f4 90 7 ... ..'. </pre>
--	---



frame contains "amazon"						
No.	Time	Source	Destination	Protocol	Length	Info
5898	55.830733	10.250.200.3	10.200.226.69	DNS	94	Standard query response 0x051d A c.media-amazon.com
5900	55.831230	10.200.226.69	10.250.200.3	DNS	78	Standard query 0x9004 AAAA c.media-amazon.com
5903	55.833645	10.250.200.3	10.200.226.69	DNS	302	Standard query response 0x9004 AAAA c.media-amazon.com
5924	55.854360	10.200.226.69	54.230.46.208	TLS...	1953	Client Hello (SNI=m.media-amazon.com)
5927	55.857089	10.200.226.69	54.230.46.208	TLS...	1966	Client Hello (SNI=images-eu.ssl-images-amazon.com)
5962	56.017230	10.200.226.69	79.125.87.14	TLS...	1951	Client Hello (SNI=f1s-eu.amazon.in)
5986	56.059925	10.200.226.69	10.250.200.3	DNS	91	Standard query 0x9e08 HTTPS images-eu.ssl-images-amazon.com
5987	56.059925	10.200.226.69	10.250.200.3	DNS	78	Standard query 0x06e1 HTTPS m.media-amazon.com
5988	56.059930	10.200.226.69	10.250.200.3	DNS	76	Standard query 0x25be HTTPS f1s-eu.amazon.in
5989	56.065559	10.250.200.3	10.200.226.69	DNS	130	Standard query response 0x06e1 HTTPS m.media-amazon.com
5990	56.065559	10.250.200.3	10.200.226.69	DNS	172	Standard query response 0x9e08 HTTPS images-eu.ssl-images-amazon.com
5991	56.065559	10.250.200.3	10.200.226.69	DNS	180	Standard query response 0x25be HTTPS f1s-eu.amazon.in
> Frame 5924: 1953 bytes on wire (15624 bits), 1953 bytes captured (15624 bits) on interface 0 > Ethernet II, Src: Intel_08:44:45 (c8:cb:9e:08:44:45), Dst: Cisco_f3:aa:00:00:00:00 > Internet Protocol Version 4, Src: 10.200.226.69, Dst: 54.230.46.208 > Transmission Control Protocol, Src Port: 64771, Dst Port: 443, Seq: 1, Len: 1953 > Transport Layer Security						

frame contains "youtube"						
No.	Time	Source	Destination	Protocol	Length	Info
865	50.410620	10.200.226.69	10.250.200.3	DNS	75	Standard query 0xe5c3 HTTPS www.youtube.com
983	50.431112	10.200.226.69	10.250.200.3	DNS	75	Standard query 0xe5c3 HTTPS www.youtube.com
1037	50.447269	10.250.200.3	10.200.226.69	DNS	124	Standard query response 0xe5c3 HTTPS www.youtube.com CNAM
2428	51.738126	10.200.226.69	142.250.77.142	TLS...	1950	Client Hello (SNI=www.youtube.com)
4957	53.473981	10.250.200.3	10.200.226.69	DNS	124	Standard query response 0xe5c3 HTTPS www.youtube.com CNAM
12669	151.415227	10.200.226.69	10.250.200.3	DNS	75	Standard query 0x890e A www.youtube.com
12670	151.416979	10.250.200.3	10.200.226.69	DNS	365	Standard query response 0x890e A www.youtube.com CNAME yo
12671	151.418954	10.200.226.69	10.250.200.3	DNS	83	Standard query 0xa7a2 A youtube-ui.l.google.com
12672	151.422599	10.250.200.3	10.200.226.69	DNS	339	Standard query response 0xa7a2 A youtube-ui.l.google.com
12673	151.423250	10.200.226.69	10.250.200.3	DNS	83	Standard query 0xb1cb AAAA youtube-ui.l.google.com
12675	151.433441	10.250.200.3	10.200.226.69	DNS	195	Standard query response 0xb1cb AAAA youtube-ui.l.google.com
> Frame 2428: 1950 bytes on wire (15600 bits), 1950 bytes captured (15600 bits) on interface 0 > Ethernet II, Src: Intel_08:44:45 (c8:cb:9e:08:44:45), Dst: Cisco_f3:aa:00:00:00:00 > Internet Protocol Version 4, Src: 10.200.226.69, Dst: 142.250.77.142 > Transmission Control Protocol, Src Port: 64749, Dst Port: 443, Seq: 1, Len: 1950 > Transport Layer Security						

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.**

tcp.port==64836 && ip.addr==10.195.250.62						
No.	Time	Source	Destination	Protocol	Length	Info
8771	63.902202	10.200.226.69	10.195.250.62	TCP	66	64836 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=2
8773	63.904514	10.195.250.62	10.200.226.69	TCP	66	443 → 64836 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MS
8774	63.904557	10.200.226.69	10.195.250.62	TCP	54	64836 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
8775	63.905334	10.200.226.69	10.195.250.62	TLS...	1950	Client Hello (SNI=www.iitdh.ac.in)
tcp.port==64771 && ip.addr==54.230.46.208						
No.	Time	Source	Destination	Protocol	Length	Info
5894	55.829172	10.200.226.69	54.230.46.208	TCP	66	64771 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=2
5921	55.853269	54.230.46.208	10.200.226.69	TCP	66	443 → 64771 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MS
5922	55.853337	10.200.226.69	54.230.46.208	TCP	54	64771 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
5924	55.854360	10.200.226.69	54.230.46.208	TLS...	1953	Client Hello (SNI=m.media-amazon.com)
tcp.port==64749 && ip.addr==142.250.77.142						
No.	Time	Source	Destination	Protocol	Length	Info
2311	51.710367	10.200.226.69	142.250.77.142	TCP	66	64749 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=2
2426	51.737426	142.250.77.142	10.200.226.69	TCP	66	443 → 64749 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MS
2427	51.737499	10.200.226.69	142.250.77.142	TCP	54	64749 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
2428	51.738126	10.200.226.69	142.250.77.142	TLS...	1950	Client Hello (SNI=www.youtube.com)

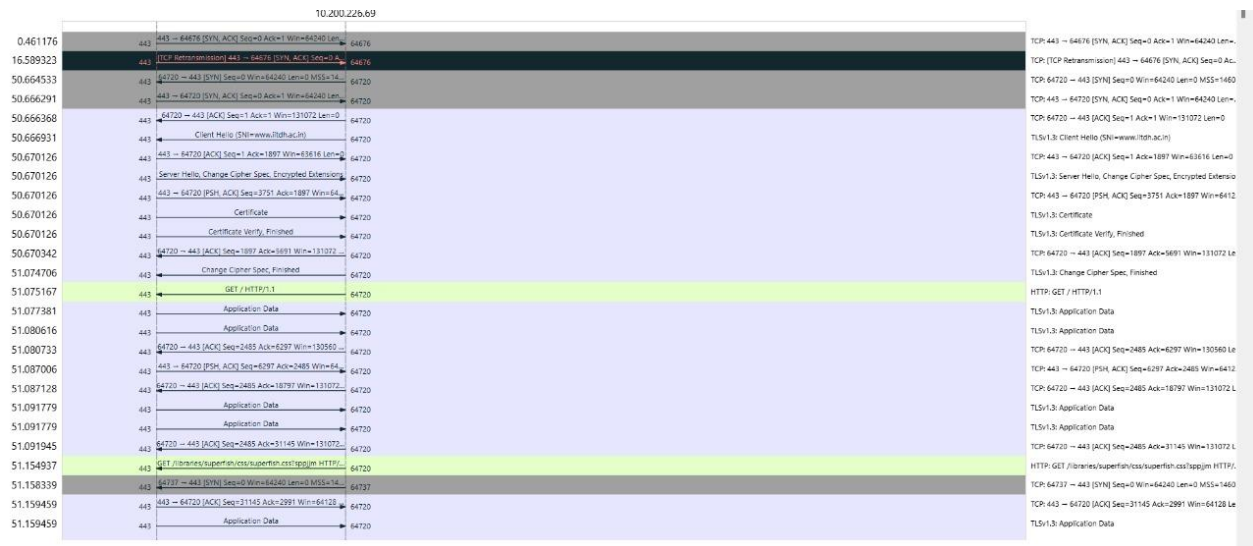
Domain	First SYN Timestamp (T <sub>syn</sub> )	Final ACK Timestamp (T <sub>ack</sub> )	TCP Handshake Time=T <sub>ack</sub> -T <sub>syn</sub>
iitdh.ac.in	63.902202	63.904557	0.002355
amazon.in	55.829172	55.853337	0.024165
youtube.com	51.710367	51.737499	0.027132

**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.**

tcp.port==443 && ip.addr==10.195.250.62						
No.	Time	Source	Destination	Protocol	Length	Info
36	0.461176	10.195.250.62	10.200.226.69	TCP	66	443 → 64676 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MS
462	16.589323	10.195.250.62	10.200.226.69	TCP	66	[TCP Retransmission] 443 → 64676 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MS
1275	50.664533	10.200.226.69	10.195.250.62	TCP	66	64720 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=2
1281	50.666291	10.195.250.62	10.200.226.69	TCP	66	443 → 64720 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MS
1284	50.666368	10.200.226.69	10.195.250.62	TCP	54	64720 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
1287	50.666931	10.200.226.69	10.195.250.62	TLS...	1950	Client Hello (SNI=www.iitdh.ac.in)
1288	50.670126	10.195.250.62	10.200.226.69	TCP	54	443 → 64720 [ACK] Seq=1 Ack=1897 Win=63616 Len=0
1289	50.670126	10.195.250.62	10.200.226.69	TLS...	3804	Server Hello, Change Cipher Spec, Encrypted Extension
1290	50.670126	10.195.250.62	10.200.226.69	TCP	400	443 → 64720 [PSH, ACK] Seq=3751 Ack=1897 Win=64128 Le
1292	50.670126	10.195.250.62	10.200.226.69	TLS...	1304	Certificate
1293	50.670126	10.195.250.62	10.200.226.69	TLS...	398	Certificate Verify, Finished
1294	50.670342	10.200.226.69	10.195.250.62	TCP	54	64720 → 443 [ACK] Seq=1897 Ack=5691 Win=131072 Len=0

> Frame 4916: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on 0	0000	8c 94 61 f3 aa c3 c8 cb 9e 08 44 45 08 00 45 00	..a.....DE..
> Ethernet II, Src: Intel_08:44:45 (c8:cb:9e:08:44:45), Dst: Cisco_f3:aa:00:00:28:52	0010	00 28 52 bb 40 00 80 06 00 00 0a c8 e2 45 0a c3	..(R_@.....E
> Internet Protocol Version 4, Src: 10.200.226.69, Dst: 10.195.250.62	0020	fa 3e fc fa 01 bb 9f 9a d6 23 02 29 fd 79 50 10	..>.....+..-v
> Transmission Control Protocol, Src Port: 64762, Dst Port: 443, Seq: 315	0030	02 00 f2 29 00 00	....)



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

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.

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 (8784<sup>th</sup> packet)=63.912102

corresponding 200 OK response (8800<sup>th</sup> 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).

No.	Time	Source	Destination	Protocol	Length	Info
→	8759.63.884146	10.200.226.69	10.195.250.62	HTTP	868	GET / HTTP/1.1

No.	Time	Source	Destination	Protocol	Length	Info

No.	Time	Source	Destination	Protocol	Length	Info

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.

No.	Time	Source	Destination	Protocol	Length	Info
→	1730.36.379983	10.200.226.69	10.195.250.62	HTTP	1430	GET / HTTP/1.1
→	3016.60.790656	10.200.226.69	10.195.250.62	HTTP	2370	POST /visitors/_track?action_name=Indian%20Institute%20of

> Frame 1730: 1430 bytes on wire (11440 bits), 1430 bytes captured (11440) on interface 0 > Ethernet II, Src: Intel_08:44:45 (c8:cb:9e:08:44:45), Dst: Cisco_f3:aa:00:00:00:00 > Internet Protocol Version 4, Src: 10.200.226.69, Dst: 10.195.250.62 > Transmission Control Protocol, Src Port: 53016, Dst Port: 443, Seq: 189 > Transport Layer Security > Hypertext Transfer Protocol	0000 8c 94 61 f3 aa c3 c8 cb 9e 08 44 45 08 00 45 00 ...a... ..DE.. 0010 00 00 53 e1 40 00 80 06 00 00 0a c8 e2 45 0a c3 ...S...@... .. 0020 fa 3e cf 18 01 bb 2b ab e0 03 56 5d 33 54 50 18 ...>...+... ..V]3 0030 02 00 f2 15 00 00 17 03 03 05 5b 81 42 b3 e2 89 ... ..[...E.. 0040 9a d1 1f cc 4a 4d c6 6a 81 26 c3 e5 bc d7 23 1c ...JM...j...&... 0050 a7 67 f4 8c b9 cb e7 80 22 76 96 11 43 aa e5 43 ...g... .."v...C.. 0060 36 06 8d 5a 0a e9 c7 03 47 0b f1 31 07 03 f1 23 6...Z... ..G...1.. 0070 5b 07 fd 3f 89 b3 c2 6d 66 27 2c fa 65 82 75 2c [...?...m f',...e.. 0080 81 fb 1c 11 72 cc 3a f6 0c b1 9f 8f ab d5 00 09 ...r... ..E... 0090 77 a7 35 08 e9 b6 82 8b 45 ce 27 89 89 01 92 6b w...5... ..E... 00a0 a9 79 af 16 e7 a2 0a 14 23 44 cf 25 46 5e 89 b6 ...y... ..#D...F.. 00b0 e3 ea 0e b3 c9 68 f7 2d a5 c7 77 1a 78 72 69 ee ...h... ..w...x.. 00c0 7b b3 a7 79 d2 5a 54 b4 db f7 61 9b 02 52 44 ae {...y...ZT... ..a... 00d0 4e 07 d2 5d 37 eb df 83 96 3d fd 01 dd 46 97 47 N...7... ..=...
--	--

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"**.

http.host==iitdh.ac.in						
No.	Time	Source	Destination	Protocol	Length	Info
8759	63.884146	10.200.226.69	10.195.250.62	HTTP	868	GET / HTTP/1.1

frame contains "iitdh"						
No.	Time	Source	Destination	Protocol	Length	Info
1628	36.349521	10.200.226.69	10.250.200.3	DNS	83	Standard query 0xa73f A iitdh.ac.in
1632	36.349777	10.200.226.69	10.250.200.3	DNS	83	Standard query 0x7d03 HTTPS iitdh.ac.in
1637	36.352795	10.250.200.3	10.200.226.69	DNS	101	Standard query response 0xa73f A iitdh.ac.in A 10.195.250.62
1638	36.352795	10.250.200.3	10.200.226.69	DNS	85	Standard query response 0x7d03 HTTPS iitdh.ac.in
1653	36.357276	10.200.226.69	10.250.200.3	DNS	83	Standard query 0xa356 HTTPS iitdh.ac.in
1656	36.357437	10.200.226.69	10.250.200.3	DNS	83	Standard query 0xf9cc A iitdh.ac.in
1668	36.363262	10.200.226.69	10.250.200.3	DNS	83	Standard query 0x4546 HTTPS iitdh.ac.in
1670	36.363341	10.200.226.69	10.250.200.3	DNS	83	Standard query 0x93cd A iitdh.ac.in
1671	36.364383	10.250.200.3	10.200.226.69	DNS	85	Standard query response 0xa356 HTTPS iitdh.ac.in
1672	36.364383	10.250.200.3	10.200.226.69	DNS	101	Standard query response 0xf9cc A iitdh.ac.in A 10.195.250.62
1683	36.366588	10.250.200.3	10.200.226.69	DNS	101	Standard query response 0x93cd A iitdh.ac.in A 10.195.250.62
1684	36.366588	10.250.200.3	10.200.226.69	DNS	85	Standard query response 0x4546 HTTPS iitdh.ac.in

> Frame 1702: 1871 bytes on wire (14968 bits), 1871 bytes captured (14968 bits) on interface eth0		0000	8c 94 61 f3 aa c3 c8 cb	9e 08 44 45 08 00 45 00	..a.....DE..
> Ethernet II, Src: Intel_08:44:45 (c8:cb:9e:08:44:45), Dst: Cisco_f3:aa:00:00:00:00		0010	00 00 53 d8 40 00 80 06	00 00 0a c8 e2 45 0a c3	..S.@.....
> Internet Protocol Version 4, Src: 10.200.226.69, Dst: 10.195.250.62		0020	fa 3e cf 18 01 bb 2b ab	d8 9a 56 5d 1d 1a 50 18	..>.....+..V]
> Transmission Control Protocol, Src Port: 53016, Dst Port: 443, Seq: 1, Len: 868		0030	02 00 f2 15 00 00 16 03	01 07 14 01 00 07 10 03	.....2.....
> Transport Layer Security		0040	03 83 f7 13 c2 32 c4 99	8e 9f b3 0b a6 06 d7 47	.....2.....
		0050	ac 75 ad ad e1 be 0a b9	83 96 1b 9f b8 ac 02 ec	..u.....
		0060	f5 20 96 f4 37 3c ef 54	9a cc a6 33 ce a3 50 da	...7<T...3..
		0070	2d 38 08 6a 8a 3b 23 4d	1f 89 95 1a 1f 87 f2 5e	-8.j;#M.....
		0080	9a f7 00 20 ba ba 13 01	13 02 13 03 c0 2b c0 2f	...0.....
		0090	c0 2c c0 30 cc a9 cc a8	c0 13 c0 14 00 9c 00 9d	...0.....
		00a0	00 2f 00 35 01 00 06 a7	4a 4a 00 00 00 05 00 05	.../5...JJ...
		00b0	01 00 00 00 00 00 23 00	00 00 1b 00 03 02 00 02	.....#.....
		00c0	ff 01 00 01 00 00 0d 00	12 00 10 04 03 08 04 04	.....
		00d0	01 05 03 08 05 05 01 08	06 06 01 00 33 04 ef 04	.....3.....
		00e0	ed 3a 3a 00 01 00 11 ec	04 c0 66 e4 68 5d fa 85	...::.....f..h

No.	Time	Source	Destination	Protocol	Length	Info
4243	81.989506	10.250.200.3	10.200.226.69	DNS	160	Standard query response 0xe5ea A m.media-amazon.com C
4245	81.989922	10.250.200.3	10.200.226.69	DNS	166	Standard query response 0x807b HTTPS www.amazon.in Ch
4302	82.020790	10.250.200.3	10.200.226.69	TCP	166	[TCP Out-Of-Order] 53 → 53091 [PSH, ACK] Seq=1 Ack=35
4347	82.055687	10.200.226.69	18.161.215.8	TLS...	1873	Client Hello (SNI=www.amazon.in)
4348	82.056248	10.200.226.69	18.161.215.8	TLS...	1809	Client Hello (SNI=www.amazon.in)
4429	82.840876	10.200.226.69	10.250.200.3	DNS	93	Standard query 0xf4e3 HTTPS completion.amazon.com
4433	82.841764	10.200.226.69	10.250.200.3	DNS	93	Standard query 0xf1e5 A completion.amazon.com
4438	82.844672	10.250.200.3	10.200.226.69	DNS	95	Standard query response 0xf4e3 HTTPS completion.amazc
4480	82.874878	10.250.200.3	10.200.226.69	DNS	111	Standard query response 0xf1e5 A completion.amazon.cc
4492	82.915231	10.200.226.69	10.250.200.3	DNS	87	Standard query 0xbcb8 A unagi.amazon.in
4494	82.915312	10.200.226.69	10.250.200.3	DNS	87	Standard query 0x6eff HTTPS unagi.amazon.in
4499	82.919873	10.250.200.3	10.200.226.69	DNS	138	Standard query response 0xbcb8 A unagi.amazon.in CNAI

> Frame 4347: 1873 bytes on wire (14984 bits), 1873 bytes captured (14984 bits) on interface 0  
 > Ethernet II, Src: Intel\_08:44:45 (c8:cb:9e:08:44:45), Dst: Cisco\_f3:aa:00:00:00:00  
 > Internet Protocol Version 4, Src: 10.200.226.69, Dst: 18.161.215.8  
 > Transmission Control Protocol, Src Port: 53095, Dst Port: 443, Seq: 1, Len: 1873  
 > Transport Layer Security

No.	Time	Source	Destination	Protocol	Length	Info
9349	92.145677	10.250.200.3	10.200.226.69	DNS	138	Standard query response 0xb3cd HTTPS www.youtube.com
9387	92.201231	10.200.226.69	10.250.200.3	DNS	87	Standard query 0xf73 A www.youtube.com
9393	92.201482	10.200.226.69	10.250.200.3	DNS	87	Standard query 0x1af2 HTTPS www.youtube.com
9401	92.206012	10.250.200.3	10.200.226.69	DNS	379	Standard query response 0xf73 A www.youtube.com CNAI
9403	92.206012	10.250.200.3	10.200.226.69	DNS	138	Standard query response 0x1af2 HTTPS www.youtube.com
9435	92.279965	10.200.226.69	142.250.195.46	TLS...	1811	Client Hello (SNI=www.youtube.com)
11270	96.444727	10.200.226.69	10.250.200.3	DNS	92	Standard query 0x546b A accounts.youtube.com
11272	96.444846	10.200.226.69	10.250.200.3	DNS	92	Standard query 0xc800 HTTPS accounts.youtube.com
11278	96.447721	10.250.200.3	10.200.226.69	DNS	138	Standard query response 0x546b A accounts.youtube.com
11279	96.447721	10.250.200.3	10.200.226.69	DNS	122	Standard query response 0xc800 HTTPS accounts.youtube.com
11347	96.521770	10.200.226.69	142.250.195.78	TLS...	1880	Client Hello (SNI=accounts.youtube.com)

> Frame 11347: 1880 bytes on wire (15040 bits), 1880 bytes captured (15040 bits) on interface 0  
 > Ethernet II, Src: Intel\_08:44:45 (c8:cb:9e:08:44:45), Dst: Cisco\_f3:aa:00:00:00:00  
 > Internet Protocol Version 4, Src: 10.200.226.69, Dst: 142.250.195.78  
 > Transmission Control Protocol, Src Port: 53230, Dst Port: 443, Seq: 1, Len: 1880  
 > Transport Layer Security

## 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.