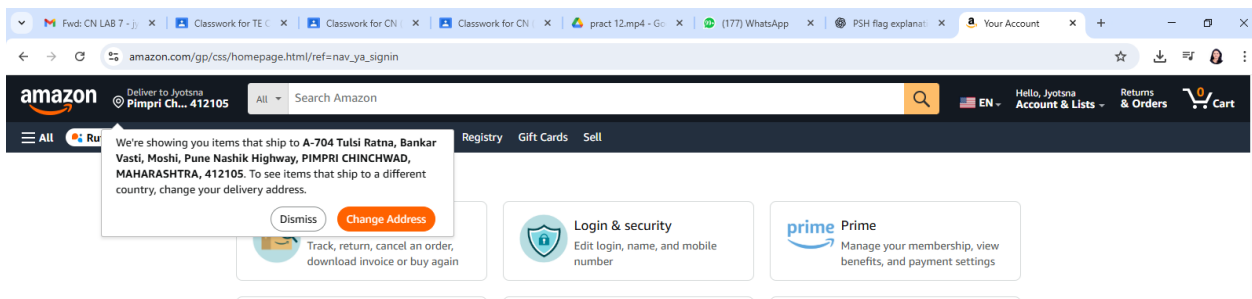


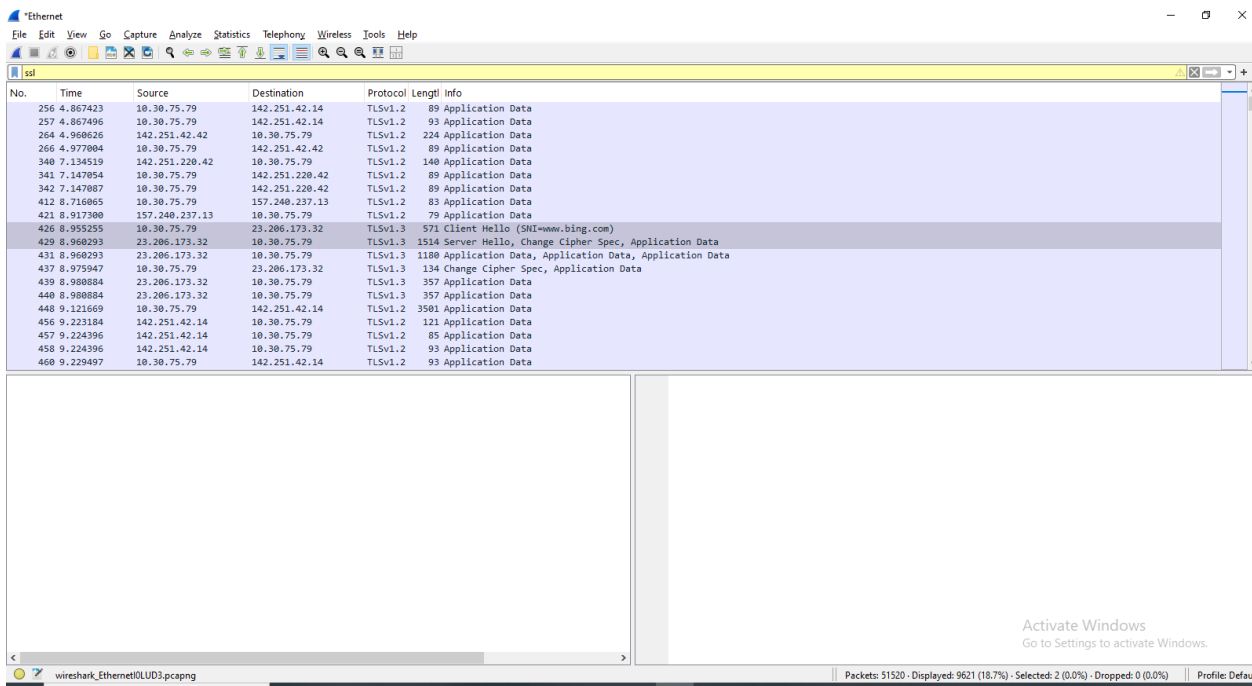
12. To study the SSL protocol by capturing the packets using Wireshark tool while visiting any SSL secured website (banking, e-commerce etc.).

1. Open Wireshark first

2. Open Amazon and login



3. Stop packet capturing on Wireshark



4. Right click on Client hello → follow → TLS Stream → you will get a popup close that by doing this you will get one command on Wireshark as follows

tcp.stream eq 20

Wireshark interface showing a packet capture on 'Ethernet'. The packet list on the left shows several TCP and TLSv1.3 packets. Packet 426 is selected, showing its details in the middle pane and the raw packet data in hexadecimal and ASCII in the bottom pane.

No.	Time	Source	Destination	Protocol	Length	Info
422	8.949481	10.30.75.79	23.206.173.32	TCP	66	65519 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
424	8.953315	23.206.173.32	10.30.75.79	TCP	66	443 → 65519 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1384 SACK_PERM WS=128
425	8.953357	10.30.75.79	23.206.173.32	TCP	54	65519 → 443 [ACK] Seq=1 Ack=1 Win=262912 Len=0
426	8.955255	10.30.75.79	23.206.173.32	TLSv1.3	571	Client Hello (SN=www.bing.com)

Details of Packet 426 (TLSv1.3):

- Frame 426: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface \Device\NPF_{6E1008F6-7C}
- Ethernet II, Src: Dell_2a:54:f2 (74:8b:e2:2a:54:f2), Dst: JuniperNetwo_0d:6b:c0 (78:50:7c:0d:6b:c0)
- Internet Protocol Version 4, Src: 10.30.75.79, Dst: 23.206.173.32
- Transmission Control Protocol, Src Port: 65519, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
- Transport Layer Security
 - TLSv1.3 Record Layer: Handshake Protocol: Client Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 512
 - Handshake Protocol: Client Hello

Raw packet data (hex and ASCII) is displayed in the bottom pane.

5. tcp.stream eq 20 && ssl

Wireshark interface showing a packet capture on 'Ethernet'. The packet list on the left shows several TLSv1.3 packets. Packet 426 is selected, showing its details in the middle pane and the raw packet data in hexadecimal and ASCII in the bottom pane.

No.	Time	Source	Destination	Protocol	Length	Info
426	8.955255	10.30.75.79	23.206.173.32	TLSv1.3	571	Client Hello (SN=www.bing.com)
429	8.960293	23.206.173.32	10.30.75.79	TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
431	8.960293	23.206.173.32	10.30.75.79	TLSv1.3	1180	Application Data, Application Data, Application Data
437	8.975947	23.206.173.32	10.30.75.79	TLSv1.3	134	Change Cipher Spec, Application Data
439	8.980884	23.206.173.32	10.30.75.79	TLSv1.3	357	Application Data
440	8.980884	23.206.173.32	10.30.75.79	TLSv1.3	357	Application Data
942	18.982251	23.206.173.32	10.30.75.79	TLSv1.3	93	Application Data
943	18.982251	23.206.173.32	10.30.75.79	TLSv1.3	78	Application Data

Details of Packet 426 (TLSv1.3):

- Frame 426: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface \Device\NPF_{6E1008F6-7C}
- Ethernet II, Src: Dell_2a:54:f2 (74:8b:e2:2a:54:f2), Dst: JuniperNetwo_0d:6b:c0 (78:50:7c:0d:6b:c0)
- Internet Protocol Version 4, Src: 10.30.75.79, Dst: 23.206.173.32
- Transmission Control Protocol, Src Port: 65519, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
- Transport Layer Security
 - TLSv1.3 Record Layer: Handshake Protocol: Client Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 512
 - Handshake Protocol: Client Hello

Raw packet data (hex and ASCII) is displayed in the bottom pane.

Wireshark interface showing a packet capture on the 'Ethernet' interface. The packet list shows a TLSv1.3 Client Hello (No. 426) and subsequent Application Data packets. The packet details pane is expanded for the Client Hello, showing fields like Version, Session ID, Cipher Suites, and Extensions. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Version: TLS 1.0 (0x0301)
Length: 512
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 508
> Version: TLS 1.2 (0x0303)
Random: 0ad9539f32f35793b766f55bd8395df79f9ac90688015d116eaf2c839489f155
Session ID Length: 32
Session ID: c7cbbd6a67853bf3f45b28c68ab33b0cdeaf9477ec721a90ff2392049f8f80
Cipher Suites Length: 30
> Cipher Suites (15 suites)
Compression Methods Length: 1
> Compression Methods (1 method)
> Extensions Length: 405
> Extension: renegotiation_info (len=1)
> Extension: server_name (len=17) name=www.bing.com
> Extension: ec_point_formats (len=4)
> Extension: supported_groups (len=8)
> Extension: session_ticket (len=0)
> Extension: status_request (len=5)
> Extension: application_layer_protocol_negotiation (len=14)

Wireshark interface showing the same packet capture. The packet details pane is expanded for the TLSv1.3 Client Hello, showing the list of cipher suites. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Random: 0ad9539f32f35793b766f55bd8395df79f9ac90688015d116eaf2c839489f155
Session ID Length: 32
Session ID: c7cbbd6a67853bf3f45b28c68ab33b0cdeaf9477ec721a90ff2392049f8f80
Cipher Suites Length: 30
> Cipher Suites (15 suites)
Cipher Suite: TLS_AES_128_GCM_SHA256 (0xc1301)
Cipher Suite: TLS_AES_256_GCM_SHA384 (0xc1302)
Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0xc1303)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xc03a)
Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc03b)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
Compression Methods Length: 1

(Click on bottom Transport layer security thrn again click on arrow you will get all details)

7.If you do right click on server hello →follow → TLS Stream → you will get popup close that by doing this you will get one command on Wireshark as follow

Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcpstream eq 20

No.	Time	Source	Destination	Protocol	Length	Info
422	8.949481	10.30.75.79	23.206.173.32	TCP	66	65519 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
424	8.953315	23.206.173.32	10.30.75.79	TCP	66	443 → 65519 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1384 SACK_PERM WS=128
425	8.953357	10.30.75.79	23.206.173.32	TCP	54	65519 → 443 [ACK] Seq=1 Ack=1 Win=262912 Len=0
426	8.955255	10.30.75.79	23.206.173.32	TLSv1.3	571	Client Hello (SNL=mmr.bing.com)
428	8.960293	23.206.173.32	10.30.75.79	TCP	60	443 → 65519 [ACK] Seq=1 Ack=518 Win=974336 Len=0
429	8.960293	23.206.173.32	10.30.75.79	TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
430	8.960293	23.206.173.32	10.30.75.79	TCP	1514	443 → 65519 [PSH, ACK] Seq=1461 Ack=518 Win=64128 Len=1460 [TCP PDU reassembled in 431]
431	8.960293	23.206.173.32	10.30.75.79	TLSv1.3	1180	Application Data, Application Data, Application Data
432	8.960644	10.30.75.79	23.206.173.32	TCP	54	65519 → 443 [ACK] Seq=518 Ack=4047 Win=262912 Len=0
437	8.975947	10.30.75.79	23.206.173.32	TLSv1.3	134	Change Cipher Spec, Application Data
438	8.979545	23.206.173.32	10.30.75.79	TCP	60	443 → 65519 [ACK] Seq=4047 Ack=598 Win=64128 Len=0
439	8.980884	23.206.173.32	10.30.75.79	TLSv1.3	357	Application Data
440	8.980884	23.206.173.32	10.30.75.79	TLSv1.3	357	Application Data
442	8.991892	23.206.173.32	10.30.75.79	TCP	574	[TCP Reset=1310] 443 → 65519 [PSH, ACK] Seq=4350 Ack=598 Win=64128 Len=303
443	8.993264	10.30.75.79	23.206.173.32	TCP	66	65519 → 443 [ACK] Seq=598 Ack=4653 Win=262144 Len=0 SLE=4350 SRE=4653
942	18.982251	23.206.173.32	10.30.75.79	TLSv1.3	93	Application Data
943	18.982251	23.206.173.32	10.30.75.79	TLSv1.3	78	Application Data
944	18.982251	23.206.173.32	10.30.75.79	TCP	60	443 → 65519 [FIN, ACK] Seq=4716 Ack=598 Win=64128 Len=0
945	18.982552	10.30.75.79	23.206.173.32	TCP	54	65519 → 443 [ACK] Seq=598 Ack=4716 Win=262144 Len=0
946	18.983764	10.30.75.79	23.206.173.32	TCP	54	65519 → 443 [ACK] Seq=598 Ack=4717 Win=262144 Len=0

> Frame 429: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{6E10E...}

> Ethernet II, Src: JuniperNetwo_8d:6b:c0 (78:50:7c:8d:6b:c0), Dst: Dell_2a:54:f2 (74:86:e2:2a:54:f2)

> Internet Protocol Version 4, Src: 23.206.173.32, Dst: 10.30.75.79

> Transmission Control Protocol, Src Port: 443, Dst Port: 65519, Seq: 1, Ack: 518, Len: 1460

Transport Layer Security

TLsv1.3 Record Layer: Handshake Protocol: Server Hello

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 122

Handshake Protocol: Server Hello

Handshake Type: Server Hello (2)

Length: 118

Version: TLS 1.2 (0x0303)

Random: a8e951447fac815a46af424f7b2592b6833cdce8d36dc7234fa892f4aff674

Session ID Length: 32

Session ID: c7cbbd6a67853bf3f45b28cc68ab33b0cdeaf9477ec721a90ff2392049f8f80

Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)

Compression Method: null (0)

Extensions Length: 46

Extension: supported_versions (len=2) TLS 1.3

Extension: key_share (len=36) v25610

Random values used for deriving keys (tls.handshake.random): 32 bytes

Packets: 51520 - Displayed: 23 (0.0%) - Dropped: 0 (0.0%)

Profile: Default

ENG 9:41 AM