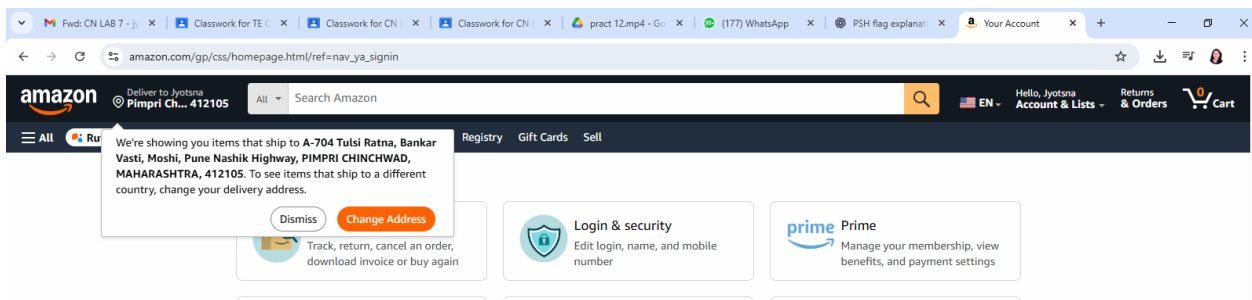


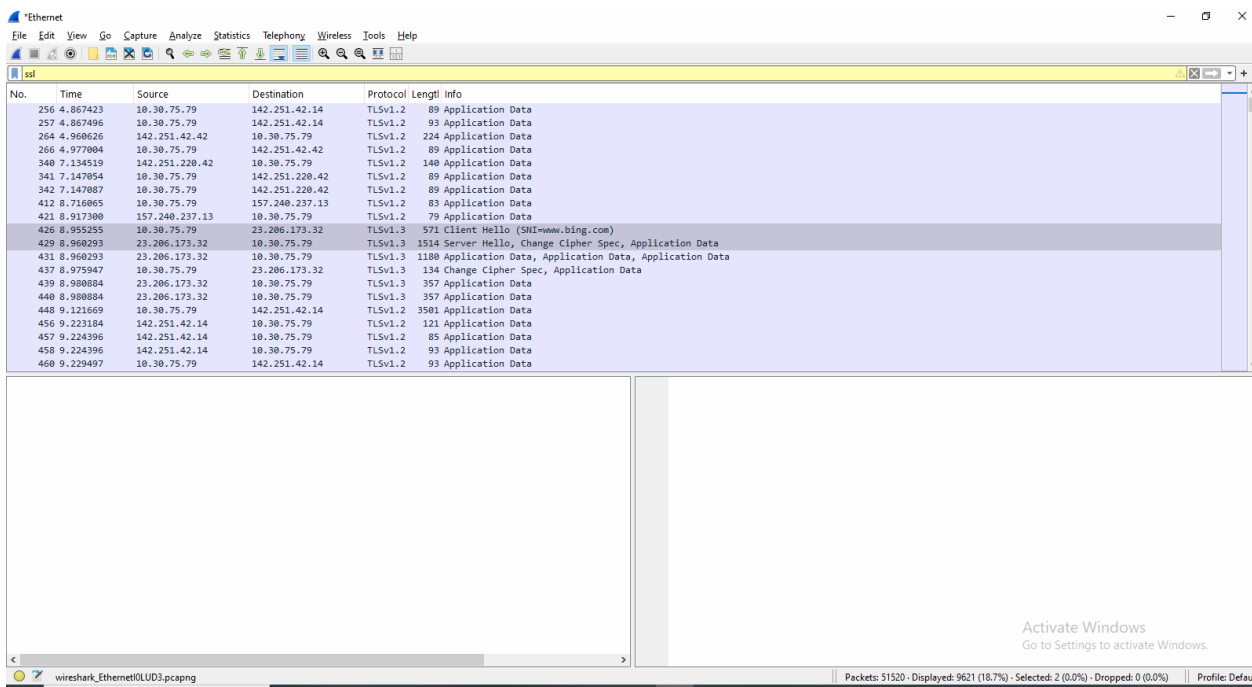
12. To study the SSL protocol by capturing the packets using Wireshark tool while visiting any SSL secured website (banking, e-commerce etc.).

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

Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 20

No.	Time	Source	Destination	Protocol	Length	Info
422	8.949481	18.30.75.79	23.206.173.32	TCP	66	65319 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
424	8.953315	23.206.173.32	18.30.75.79	TCP	66	443 → 65319 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1384 SACK_PERM=128
425	8.953357	18.30.75.79	23.206.173.32	TCP	54	65319 → 443 [ACK] Seq=1 Ack=1 Win=262912 Len=0
426	8.955255	18.30.75.79	23.206.173.32	TLSv1.3	571	Client Hello (SNI=www.bing.com)
428	8.960293	23.206.173.32	18.30.75.79	TCP	60	443 → 65319 [ACK] Seq=1 Ack=518 Win=974336 Len=0
429	8.960293	23.206.173.32	18.30.75.79	TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
430	8.960293	23.206.173.32	18.30.75.79	TCP	1514	443 → 65319 [PSH, ACK] Seq=1461 Ack=518 Win=64128 Len=1460 [TCP PDU reassembled in 431]
431	8.960293	23.206.173.32	18.30.75.79	TLSv1.3	1180	Application Data, Application Data, Application Data
432	8.960644	18.30.75.79	23.206.173.32	TCP	54	65319 → 443 [ACK] Seq=518 Ack=4847 Win=262912 Len=0
437	8.975947	18.30.75.79	23.206.173.32	TLSv1.3	134	Change Cipher Spec, Application Data
438	8.979545	23.206.173.32	18.30.75.79	TCP	60	443 → 65319 [ACK] Seq=4847 Ack=598 Win=64128 Len=0
439	8.980884	23.206.173.32	18.30.75.79	TLSv1.3	357	Application Data
440	8.980884	23.206.173.32	18.30.75.79	TLSv1.3	357	Application Data
442	8.993120	23.206.173.32	18.30.75.79	TCP	357	[RST] Retransmission 443 → 65319 [PSH, ACK] Seq=4358 Ack=598 Win=64128 Len=303
443	8.993264	18.30.75.79	23.206.173.32	TCP	60	65319 → 443 [ACK] Seq=598 Ack=4653 Win=262144 Len=0 SLE=459 SR=4653
942	18.982251	23.206.173.32	18.30.75.79	TLSv1.3	93	Application Data
943	18.982251	23.206.173.32	18.30.75.79	TLSv1.3	78	Application Data
944	18.982251	23.206.173.32	18.30.75.79	TCP	60	443 → 65319 [FIN, ACK] Seq=4716 Ack=598 Win=64128 Len=0
945	18.982552	18.30.75.79	23.206.173.32	TCP	54	65319 → 443 [ACK] Seq=598 Ack=4716 Win=262144 Len=0
946	18.983764	18.30.75.79	23.206.173.32	TCP	54	65319 → 443 [ACK] Seq=598 Ack=4717 Win=262144 Len=0

```
> Frame 426: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface Device\VMFP_{6E1008F6-7C}
> Ethernet II, Src: Dell_2a:54:54:f2 (74:b6:e2:2a:54:f2), Dst: JuniperNetw_08:d0:b0c (78:50:7c:d0:b0c)
> Internet Protocol Version 4, Src: 18.30.75.79, Dst: 23.206.173.32
> Transmission Control Protocol, Src Port: 65319, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
> Transport Layer Security
    0000 78 50 7c d0 b0 c2 a 54 f2 08 00 45 00 xp|k:t:"T":E:
    0010 02 2d bd e6 a8 00 00 06 00 0a 1e 4b 47 17 ce |@.....K0...
    0020 ad 28 ff 27 01 b0 c2 43 8a 54 92 af 32 58 18 |.....C[ :ZP
    0030 04 03 1c 7b 00 00 16 83 01 02 00 01 fc 03 00 |.....
    0040 05 2a 09 53 9f 32 f3 53 97 b7 66 55 3b 08 39 5d |...S~W+:[.]
    0050 ff 9f 9a c9 06 08 01 54 11 6e af 2c 83 94 09 f1 |.....#B|..
    0060 55 0a 07 cb bd ea 67 85 3b f3 54 5b 28 cc 68 40 |U---jg-[]{h-
    0070 33 bb 0c de a4 77 ee c7 1a 90 ff 23 92 04 9f 0c |3:.....:
    0080 8f 00 00 1e 13 81 13 02 13 03 c0 2b c0 2f c0 2c |.....
    0090 c0 30 c0 c0 cc a0 c0 13 c0 14 00 00 9d 00 2f |.....
    00a0 00 35 01 00 01 95 ff 01 00 01 00 00 00 00 00 |.....5
    00b0 0f 00 00 c0 77 77 77 2e 62 69 6e 67 2e 63 6f 6d |.....www.bing.com
    00c0 00 00 00 04 03 00 01 02 00 0a 08 00 06 00 1d |.....
    00d0 00 17 00 18 00 23 00 00 00 05 05 01 00 00 00 |.....
    00e0 00 00 10 00 0e 00 c0 62 68 32 68 74 7a 70 2f |.....h2/http/
    00f0 31 2e 31 00 12 00 00 17 00 00 00 0d 00 12 00 |.....1.1
    0100 10 04 03 00 04 04 01 05 03 00 05 05 01 08 06 0e |.....
    0110 01 00 2b 00 05 04 03 04 03 00 2d 00 02 01 01 01 |.....
    0120 00 33 00 26 00 24 00 1d 00 20 5e 03 21 7b c9 05 |.....&-&-Y
    0130 8a 54 fb 5f bf fd cd 47 e4 59 10 6e 46 3e cd 21 |T.....YnF:
    0140 b2 f5 13 13 2a 42 00 00 00 00 00 15 00 ed 00 00 |.....
    0150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....
    0160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....
    0170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....
```

wreshark_EthernetIIOUD3.pcapng Packets: 51520 - Displayed: 23 (0.0%) - Dropped: 0 (0.0%) Profile: Default

5. tcp.stream eq 20 && ssl

The image displays a Wireshark packet capture of a TLSv1.3 handshake. The packet list on the left shows the following sequence:

- 426 8.955255 10.30.75.79 → 23.206.173.32 TLSv1.3 571 Client Hello (SHI=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 8.975907 10.30.75.79 → 23.206.173.32 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

The packet details pane on the right shows the structure of the Client Hello packet (Frame 426):

- 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 (74:86:e2:2a:54:f2), Dst: JuniperNetwo_0d:6b:c0 (78:5b:7c:0d:6b:c0)
- Internet Protocol Version 4, Src: 10.30.75.79, Dst: 23.206.173.32
- Transmission Control Protocol, Src Port: 65919, Dst Port: 443, Seq: 347, 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

The packet bytes pane at the bottom shows the raw hex and ASCII data for the Client Hello packet, including the TLSv1.3 Record Layer, Handshake Protocol, and Client Hello fields.

Wireshark interface showing a TLS handshake. The packet list on the left shows the following details:

No.	Time	Source	Destination	Protocol	Length	Info
426	8.955255	10.30.75.79	23.206.173.32	TLSv1.3	571	Client Hello (SNI=www.bing.com)
429	8.968293	23.206.173.32	10.30.75.79	TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
431	8.968293	23.206.173.32	10.30.75.79	TLSv1.3	1180	Application Data, Application Data, Application Data
437	8.975947	10.30.75.79	23.206.173.32	TLSv1.3	134	Change Cipher Spec, Application Data
439	8.980884	23.206.173.32	10.30.75.79	TLSv1.3	357	Application Data
448	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

The packet details pane for packet 426 (Client Hello) shows the following structure:

- 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: c7cbbd6a67853bf3f45b28cc68ab33b0cdeaf9477ec721a90ff2392049f8f80
- Cipher Suites Length: 30
- Cipher Suites (15 suites)
- Compression Methods Length: 1
- 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)

The packet bytes pane shows the raw data of the Client Hello message, including the random value and session ID.

Wireshark interface showing the same TLS handshake. The packet list on the left shows the following details:

No.	Time	Source	Destination	Protocol	Length	Info
426	8.955255	10.30.75.79	23.206.173.32	TLSv1.3	571	Client Hello (SNI=www.bing.com)
429	8.968293	23.206.173.32	10.30.75.79	TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
431	8.968293	23.206.173.32	10.30.75.79	TLSv1.3	1180	Application Data, Application Data, Application Data
437	8.975947	10.30.75.79	23.206.173.32	TLSv1.3	134	Change Cipher Spec, Application Data
439	8.980884	23.206.173.32	10.30.75.79	TLSv1.3	357	Application Data
448	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

The packet details pane for packet 429 (Server Hello) shows the following structure:

- Random: 0ad9539f32f35793b766f55bd8395df79f9ac90688015d116eaf2c839489f155
- Session ID Length: 32
- Session ID: c7cbbd6a67853bf3f45b28cc68ab33b0cdeaf9477ec721a90ff2392049f8f80
- Cipher Suites Length: 30
- Cipher Suites (15 suites)
- Compression Methods Length: 1
- 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)

The packet bytes pane shows the raw data of the Server Hello message, including the random value and session ID.

(Click on bottom Transport layer security then 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

The image shows a Wireshark packet capture of a network session. The packet list on the left shows a series of packets, with packet 429 selected. The packet details pane on the right shows the 'Transport Layer Security' section expanded, with 'Handshake Protocol: Server Hello' selected. The packet bytes pane on the right shows the raw hex and ASCII data of the selected packet.

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

Ethernet II, Src: JuniperNetwo_8d:8b:c0 (78:5b:7c:8d:8b: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: 65319, 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: a8e9c51447fac815a46af424f7b2582b6033cdce8d38dc7234fa892f4aff674
 - 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: raw_data (len=36) v25510

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