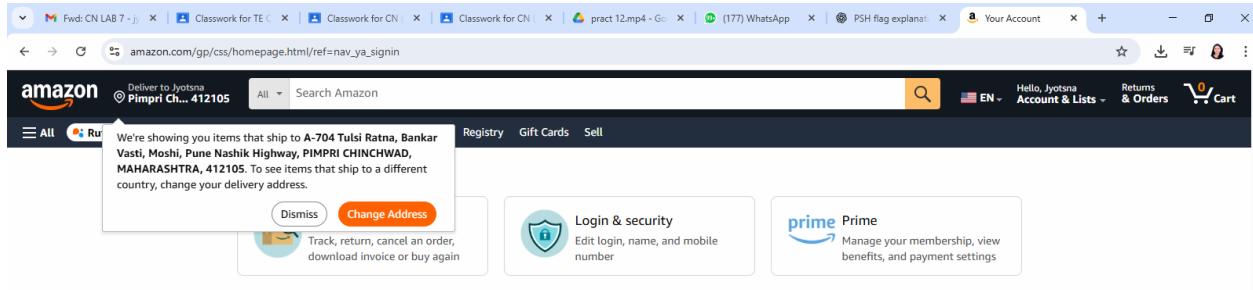


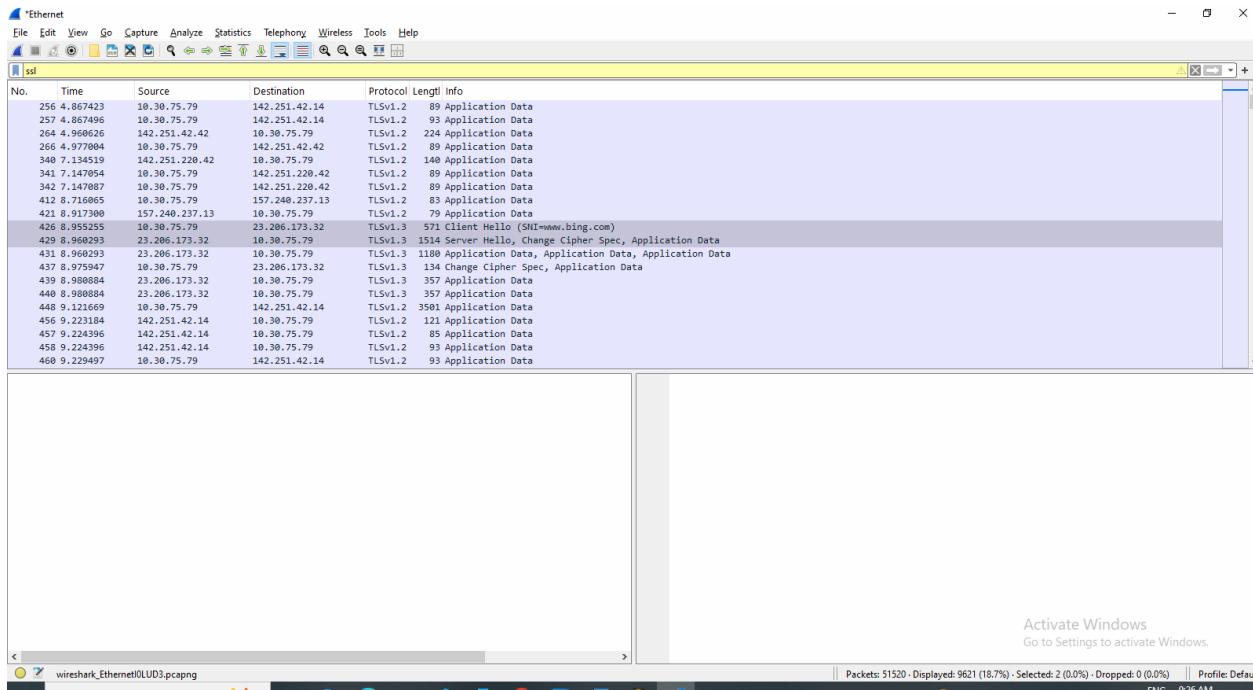
12. To study the SSL protocol by capturing the packets using Wireshark tool while visiting anySSL secured website (banking, e-commerce etc.).

1. Open Wireshark first

2. Open Amazon and login



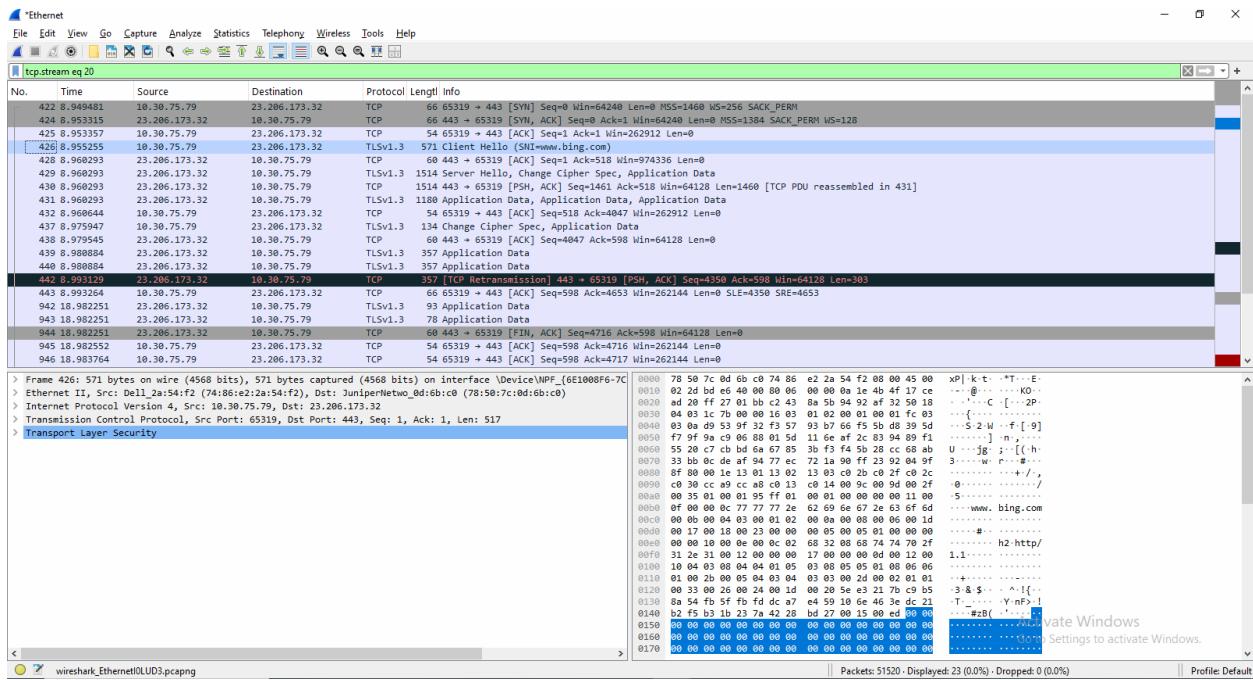
3. Stop packet capturing on wire shark



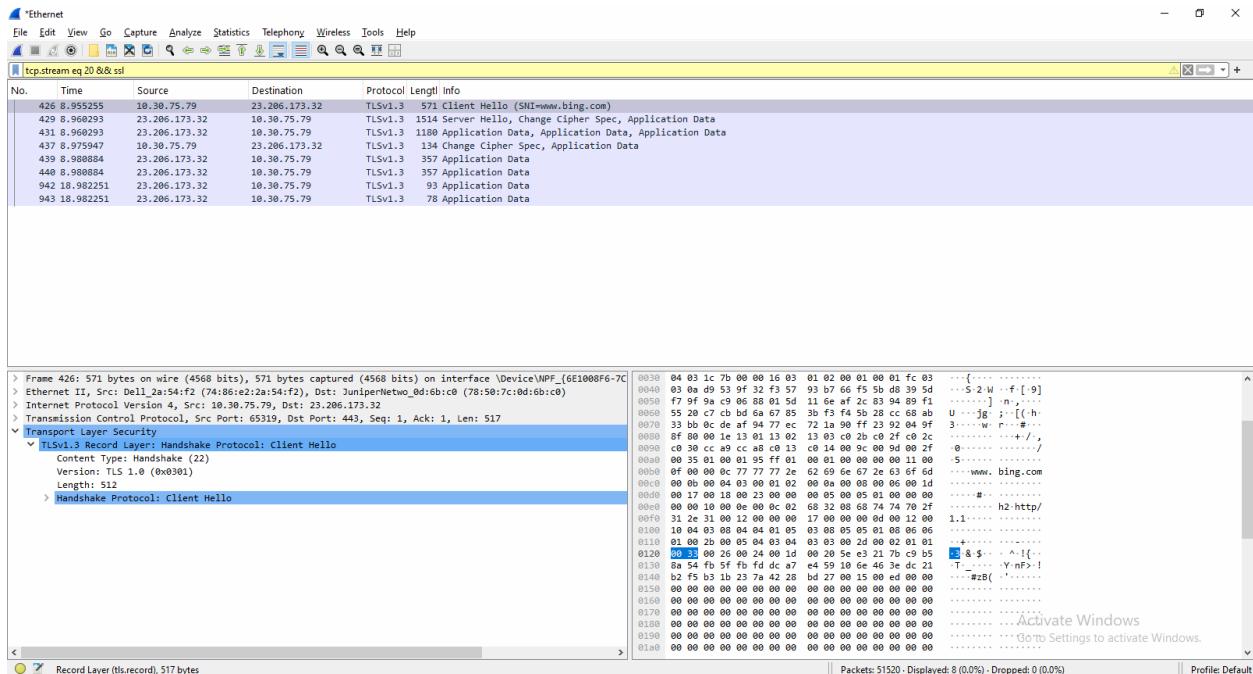
4. Right click Click on →> Client hello → follow → TLS Stream → you will get popup close that

by doing this you will get one command on Wireshark as follow

## tcp.stream eq 20



## 5. tcp.stream eq 20 && ssl



Ethernet

tcp.stream eq 20 && ssl

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
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

Version: TLS 1.2 (0x0301)  
Length: 512  
↳ Handshake Protocol: Client Hello  
Handshake Type: Client Hello (1)  
Length: 508  
> Version: TLS 1.2 (0x0301)  
Random: 0ad9539f32f35793b766f55bd8395df79f9ac90688015d116eaf2c839489f155  
Session ID Length: 32  
Session ID: c7cbdd6a7853bf3f45b28cc68ab33bb0cdeaf9477ec721a90ff2392049f8f80  
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=6)  
> Extension: status\_request (len=5)  
> Extension: application\_layer\_protocol\_negotiation (len=14)

Activate Windows  
Settings to activate Windows.

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

Packets: 51520 - Displayed: 8 (0.0%) - Dropped: 0 (0.0%)

Profile: Default

Ethernet

tcp.stream eq 20 && ssl

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
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

Random: 0ad9539f32f35793b766f55bd8395df79f9ac90688015d116eaf2c839489f155  
Session ID Length: 32  
Session ID: c7cbdd6a7853bf3f45b28cc68ab33bb0cdeaf9477ec721a90ff2392049f8f80  
Cipher Suites Length: 30  
↳ Cipher Suites (15 suites)  
Cipher Suite: TLS\_AES\_128\_GCM\_SHA256 (0x1301)  
Cipher Suite: TLS\_AES\_256\_GCM\_SHA384 (0x1303)  
Cipher Suite: TLS\_ChaCha20\_Poly1305\_SHA256 (0x1302)  
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 (0xc032)  
Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc030)  
Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_CHACHA20\_POLY1305\_SHA256 (0xccaa)  
Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256 (0xccab)  
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)

Activate Windows  
Settings to activate Windows.

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

Packets: 51520 - Displayed: 8 (0.0%) - Dropped: 0 (0.0%)

Profile: Default

(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

The screenshot shows a Wireshark capture of a TLS handshake. The timeline pane displays a sequence of TCP segments between two hosts. The last segment, which contains the Server Hello message, is highlighted in blue. The details pane shows the structure of the TLS record, specifically the Handshake Protocol: Server Hello message. The bytes pane shows the raw hex and ASCII representation of the message. The status bar at the bottom indicates that 5150 packets were captured, 23 were displayed, and 0 were dropped.