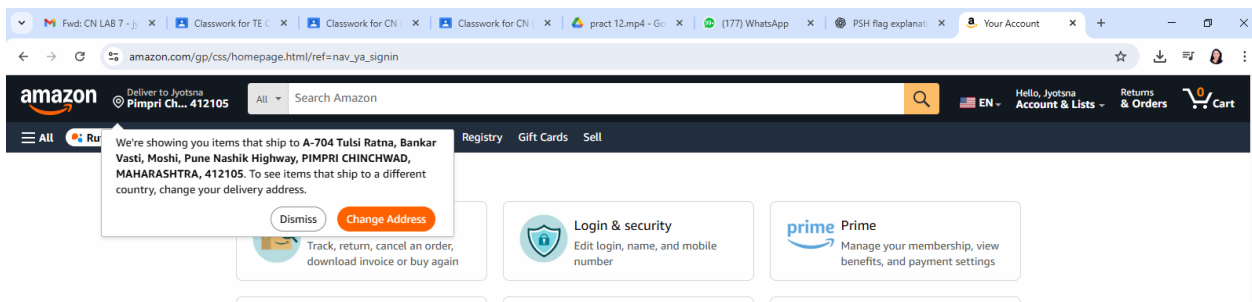


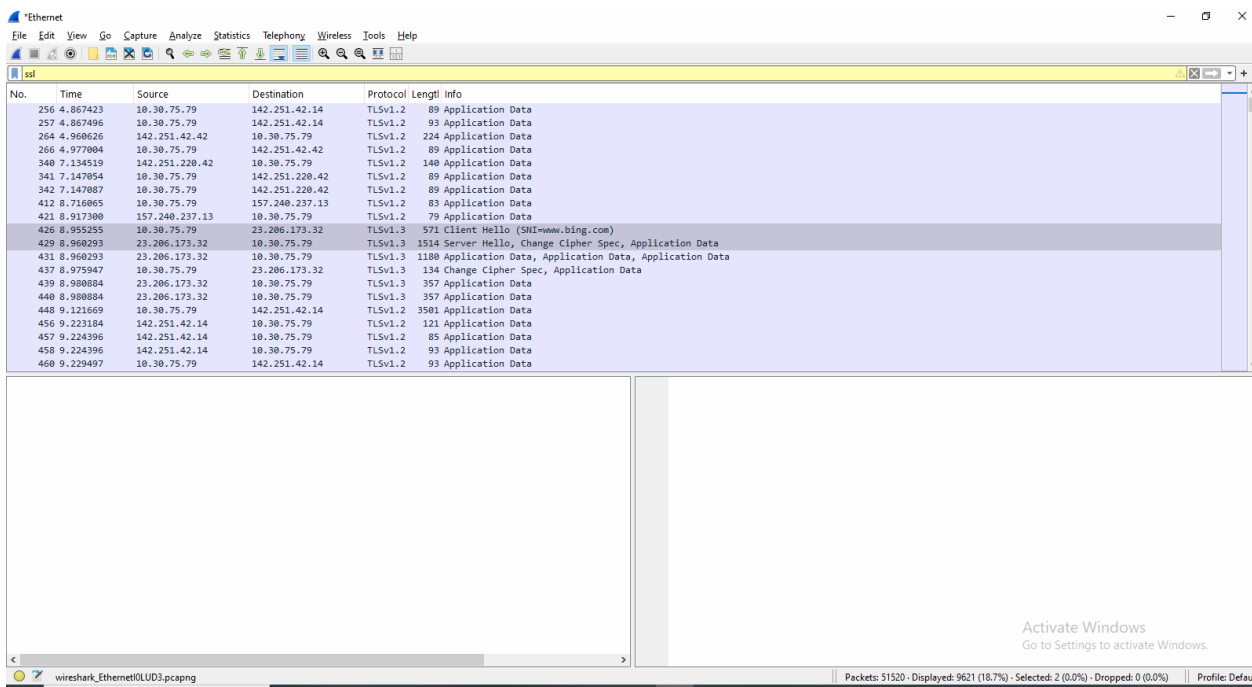
12. To study the SSL protocol by capturing the packets using Wireshark tool while visiting any SSL secured website (banking, e-commerce etc.).

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 Help

tcp.stream eq 20

Time

Source

Destination

Protocol

Length

Info

422

8.949481

10.30.75.79

23.206.173.32

TCP

66

65319 → 443 [SYN]

Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

423

8.953315

23.206.173.32

10.30.75.79

TCP

66

443 → 65319 [SYN]

Seq=0 Ack=1 Win=64240 Len=0 MSS=1384 SACK_PERM WS=128

424

8.955255

10.30.75.79

23.206.173.32

TLSv1.3

571

Client Hello (SNI=www.bing.com)

428

8.960293

23.206.173.32

10.30.75.79

TCP

60

443 → 65319 [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 → 65319 [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

8.960664

10.30.75.79

23.206.173.32

TCP

54

65319 → 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 → 65319 [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

443

8.993149

23.206.173.32

10.30.75.79

TCP

357

[RST Retransmission] 443 → 65319 [PSH, ACK]

Seq=4358 Ack=598 Win=64128 Len=303

443

8.993264

23.206.173.32

10.30.75.79

TCP

66

65319 → 443 [ACK]

Seq=598 Ack=4653 Win=262144 Len=0 SLEN=358 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 → 65319 [FIN, ACK]

Seq=4716 Ack=598 Win=64128 Len=0

945

18.982552

10.30.75.79

23.206.173.32

TCP

54

65319 → 443 [ACK]

Seq=598 Ack=4716 Win=262144 Len=0

946

18.983764

10.30.75.79

23.206.173.32

TCP

54

65319 → 443 [ACK]

Seq=598 Ack=4716 Win=262144 Len=0

Frame 426: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface vDevice\NPF_{6E1008F6-7C}

Ethernet II, Src: Dell2a:54:f2 (74:8e:e2:2a:54:f2), Dst: JuniperNetwo_bd: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: 65319, Dst Port: 443, Seq: 1, Ack: 1, Len: 517

Transport Layer Security

0000

78 50 7c 0d 6b c0 74 86 e2 2a 54 f2 08 00 45 00

xP|k:t:~T:~E

0010

02 2d bd ee 40 08 80 06 00 00 00 00 00 00 00 00

.....@.....K0.....

0020

ad 20 ff 27 01 b0 c2 43 8a 50 94 92 af 32 50 18

.....@.....C|.....P.....

0030

04 03 1c 70 86 16 03 01 02 00 00 00 01 fc 03

.....@.....@.....f.....c.....

0040

03 0a 0d 53 9f 32 f3 57 83 b7 65 5b 28 39 5d

.....@.....@.....5-2W:f:[9]

0050

ff 9f 0a c0 06 08 01 5d 11 6e af 2c 83 94 91 4f

.....@.....@.....U.....@.....f.....

0060

57 50 c7 cb 6a 67 85 b0 f3 f4 5b 28 c8 6a ab

.....@.....@.....U.....@.....f.....

0070

33 bd 06 de af 94 77 ce 72 1a 00 ff 23 92 04 9f

.....@.....@.....U.....@.....f.....

0080

8f 00 0e 1e 13 01 13 02 13 03 0b 20 2f c0 2c

.....@.....@.....U.....@.....f.....

0090

c0 30 cc a0 cc a0 c0 0c 14 04 0c 00 00 2f

.....@.....@.....U.....@.....f.....

00a0

00 35 01 00 01 95 ff 01 00 01 00 00 00 11 00

.....@.....@.....U.....@.....f.....

00b0

0f 00 00 0c 77 77 77 2e 62 69 6e 67 2e 63 6f 6d

.....@.....@.....U.....@.....f.....

00c0

00 00 00 84 03 00 01 02 00 00 88 80 86 06 1d

.....@.....@.....U.....@.....f.....

00d0

00 17 00 10 00 23 00 00 00 05 00 05 01 00 00

.....@.....@.....U.....@.....f.....

00e0

00 00 10 00 00 00 0c 02 68 32 08 68 70 70 2f

.....@.....@.....U.....@.....f.....

00f0

31 2e 31 00 12 00 00 00 17 00 00 00 0d 00 12 00

.....@.....@.....U.....@.....f.....

0100

10 04 03 08 04 04 01 05 03 00 05 05 01 08 06 06

.....@.....@.....U.....@.....f.....

0110

01 00 23 00 05 04 01 04 03 03 00 2d 00

5. tcp.stream eq 20 && ssl

The image displays a Wireshark packet capture analysis of a TLS handshake. The top pane shows a list of packets, with packet 426 selected. The middle pane shows the packet details for the TLSv1.3 Client Hello, including the frame structure and the handshake protocol. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
426	8.955255	10.30.75.79	23.206.173.32	TLSv1.3	571	Client Hello (SHA=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	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	10.902251	23.206.173.32	10.30.75.79	TLSv1.3	93	Application Data
943	10.902251	23.206.173.32	10.30.75.79	TLSv1.3	78	Application Data

Packet Details:

- Frame 426: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface \Device\NPF_{6E1000F6-7C}
 - Ethernet II, Src: Dell_2a:54:f2 (74:8e:e2:2a:54:f2), Dst: JuniperNetwo_Bd: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: 65319, 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 Data:

```

0030 04 03 1c 7b 00 00 16 03 01 02 00 01 00 01 fc 03 ...{...f.[.h]
0040 03 0a d9 53 9f 32 73 57 93 b7 66 f5 5b d8 39 5d ...S.2M...f.[.h]
0050 07 ff 9f 9a c9 06 88 01 5d 11 6e af c2 83 04 89 f1 ...w...
0060 55 20 c7 cb bd fa 67 85 3b f3 f4 5b 28 cc 68 ab U...jg...{[.h]
0070 33 b0 0c de af 94 77 ec 72 1a 00 ff 23 92 04 9f ...e...+f...
0080 0f 00 0e 1e 13 01 13 02 13 03 c0 2b c0 2f c0 2c ...e...+f...
0090 c0 30 cc a9 cc a8 c0 13 c0 14 00 3c 0d 60 2f ...-S...
00a0 00 35 01 00 01 95 ff 01 00 01 00 00 00 00 11 00 ...www.bing.com
00b0 0f 00 00 0c 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 00 00 00 05 01 0d ...
00d0 00 17 00 18 00 23 00 00 05 00 05 01 00 00 00 ...h2 http/
00e0 00 00 10 00 0e 00 0c 02 68 32 08 68 74 70 2f ...1.1...
00f0 31 2e 31 00 12 00 00 00 17 00 00 00 0d 00 12 00 ...h2 http/
0100 10 04 03 00 04 04 01 05 03 00 05 01 00 00 06 06 ...+...
0110 01 00 2b 05 04 03 04 03 03 00 2d 00 02 01 01 ...+...
0120 00 26 00 24 0d 1d 00 20 5e e3 21 70 c9 05 ...8.S...YnF...
0130 8a 54 fb 5f fb fd dc a7 e4 59 10 6e 46 2e dc 21 ...h2 http/
0140 b2 f5 b3 1b 23 7a 42 29 bd 27 00 15 00 ed 00 00 ...+...
0150 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 ...
0170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
0180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
0190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
01a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...

```

Summary:

- Record Layer (16 records), 517 bytes
- Packets: 51520 - Displayed: 8 (0.0%) - Dropped: 0 (0.0%)
- Profile: Default

Wireshark interface showing a TLS handshake capture. The packet list on the left shows packets 426 through 943. Packet 426 is selected, showing details for the TLSv1.3 Client Hello. The details pane on the right shows the structure of the Client Hello, including the random value, session ID, cipher suites, and extensions. The packet bytes pane on the right shows the raw data of the Client Hello.

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

Version: TLS 1.0 (0x0301)
Length: 512
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 508
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)

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

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

Wireshark interface showing the same TLS handshake capture. The packet list on the left shows packets 426 through 943. Packet 426 is selected, showing details for the TLSv1.3 Client Hello. The details pane on the right shows the structure of the Client Hello, including the random value, session ID, cipher suites, and extensions. The packet bytes pane on the right shows the raw data of the Client Hello.

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

Random: 0ad9539f32f35793b766f55bd8395df79f9ac90688015d116eaf2c839489f155
Session ID Length: 32
Session ID: c7cbbd6a67853bf3f45b28cc68ab33b0cdeaf9477ec721a90ff2392049f8f80
Cipher Suites Length: 30
Cipher Suites (15 suites)
Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc030)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xccab)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc013)
Cipher Suite: TLS_ECDHE_ECDSA_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

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

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

(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 window titled '*Ethernet'. The packet list on the left shows a series of packets, with packet 429 selected. The packet details pane on the right shows the structure of the selected packet, which is a TLSv1.3 record. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
422	8.949481	10.30.175.79	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	10.30.175.79	TCP	66	443 → 65319 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1384 SACK_PERM WS=128
425	8.953357	10.30.175.79	23.206.173.32	TCP	54	65319 → 443 [ACK] Seq=1 Ack=1 Win=262912 Len=0
426	8.955255	10.30.175.79	23.206.173.32	TLSv1.3	571	Client Hello (SNL=www.bing.com)
428	8.960293	23.206.173.32	10.30.175.79	TCP	60	443 → 65319 [ACK] Seq=1 Ack=518 Win=974336 Len=0
429	8.960293	23.206.173.32	10.30.175.79	TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
430	8.960293	23.206.173.32	10.30.175.79	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	10.30.175.79	TLSv1.3	1180	Application Data, Application Data, Application Data
432	8.960644	10.30.175.79	23.206.173.32	TCP	54	65319 → 443 [ACK] Seq=518 Ack=4047 Win=262912 Len=0
437	8.975947	10.30.175.79	23.206.173.32	TLSv1.3	134	Change Cipher Spec, Application Data
438	8.979545	23.206.173.32	10.30.175.79	TCP	60	443 → 65319 [ACK] Seq=4047 Ack=598 Win=64128 Len=0
439	8.980884	23.206.173.32	10.30.175.79	TLSv1.3	357	Application Data
440	8.980884	23.206.173.32	10.30.175.79	TLSv1.3	357	Application Data
442	8.993324	23.206.173.32	10.30.175.79	TCP	66	65319 → 443 [ACK] Seq=598 Ack=4653 Win=262144 Len=0 SLE=4358 SRE=4653
942	18.982251	23.206.173.32	10.30.175.79	TLSv1.3	93	Application Data
943	18.982251	23.206.173.32	10.30.175.79	TLSv1.3	78	Application Data
944	18.982251	23.206.173.32	10.30.175.79	TCP	60	443 → 65319 [FIN, ACK] Seq=4716 Ack=598 Win=64128 Len=0
945	18.982552	10.30.175.79	23.206.173.32	TCP	54	65319 → 443 [ACK] Seq=598 Ack=4716 Win=262144 Len=0
946	18.983764	10.30.175.79	23.206.173.32	TCP	54	65319 → 443 [ACK] Seq=598 Ack=4717 Win=262144 Len=0

Packet Details:

- 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 (78:5b: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: 10.30.175.79
- 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

Packet Bytes:

0000 03 00 e9 c5 1d 47 fa c8 15 a4 6a f4 24 f7 b2 58G...j\$X
0001 2b 68 33 cd ce 8d d3 8d c7 23 4f a8 92 f4 af f6 ...h3.....00....
0002 74 20 c7 cb bd 6a 67 85 3b f3 f4 5b 28 cc 68 ab t...jg...:[(h
0003 33 bb 0c de af 94 77 ec 72 1a 90 ff 23 92 04 9f 3...w...r...#...
0004 8f 80 13 02 00 00 2e 00 20 00 02 03 04 00 33 003.....
0005 24 00 1d 00 20 06 13 eb 61 30 53 17 d0 09 e8 0d \$...-a05.....
0006 8b 71 2f cd 22 d4 12 5b f8 06 a3 b0 38 c8 53 e5 q/...[...8'S
0007 b8 e8 31 65 67 14 03 03 00 01 17 03 03 00 2e ...leg.....
0008 b3 a5 df 13 ef 91 bd e5 35 bf 85 16 03 d7 b6 93S.....
0009 7f 04 b7 d5 90 99 23 55 29 99 3e da 73 a4 c7U Z)>...
0010 eb 99 6a d9 ca 18 18 33 38 ae a2 44 51 ee 17 033 8'DQ...
0011 03 0e 63 a7 4c 85 30 8b 78 c9 2f 05 3b 01 cb 8e ...C'L0: x/r/j...
0012 07 e5 22 33 c3 5a f2 29 f3 96 0a b4 de 71 10 d3 ...72).....
0013 50 a5 33 2e 15 7e ea 32 39 7d 00 c9 17 01 1e 76 P-3...2 9)...1...
0014 f3 7a 88 3d c2 f5 36 77 6c c2 ee 88 21 ca 7a d5 2:m...dw 1...1...
0015 02 e2 a5 85 f2 5d 2d 73 1f bb e8 6a e5 cc 01 bc]-s
0016 4c e5 db d0 fc 95 bf c0 54 98 07 dc 26 1f ce 91T...1k...
0017 7a 68 1a b3 05 5c 64 81 ce a9 d1 d8 78 62 a7 88 zh...Vd...x...
0018 f0 02 f9 54 d8 97 1e 44 88 d8 1f 38 03 38 75 6b ...T...D...S-Buk
0019 ef b3 5c d7 34 3f b2 6d 15 21 22 8b a4 8a 35 0e ...49m...5...
0020 f0 a5 20 70 9f b0 30 a5 42 c7 e1 01 14 40 f0 d0 ...j(-B...B...
0021 f9 6c c7 ab 4f 99 5c d1 a0 8e 18 54 d9 ef cc c7 1-O\...v...
0022 f1 d2 50 73 02 64 d6 1b 0c e4 4a 1c 23 c7 0e 2f ...Ps:d...3...
0023 6d ad cd 4c fc 64 f7 2f b5 ba 66 09 07 bc 01 5a ...L.../...f...2