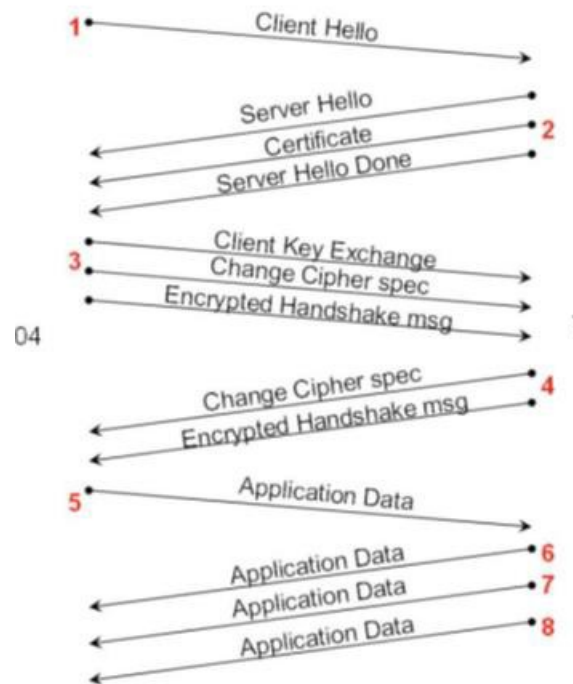


1. Visit your bank website or some of your favourite purchase website for capturing SSL. Be sure to exit without any 'dangerous' transaction.
2. Locate the below messages for your SSL transaction by filtering for SSL transactions and categorize them from 1-8 as per below figure.



a) Client Hello

Wireshark packet capture showing a TLSv1.2 Client Hello message. The packet list shows frame 8 as the Client Hello. The packet details pane shows the TLSv1.2 Record Layer: Handshake Protocol: Client Hello. The packet bytes pane shows the raw hex and ASCII data.

No.	Time	Source	Destination	Protocol	Length	Info
8	0.144748	192.168.0.105	52.163.89.138	TLSv...	250	Client Hello
13	0.199318	52.163.89.138	192.168.0.105	TLSv...	1293	Server Hello, Certificate, Certificate Status, Server Key Exchange,
15	0.201277	192.168.0.105	52.163.89.138	TLSv...	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
23	0.250414	52.163.89.138	192.168.0.105	TLSv...	105	Change Cipher Spec, Encrypted Handshake Message
25	0.271698	192.168.0.105	52.163.89.138	TLSv...	455	Application Data
26	0.271898	192.168.0.105	52.163.89.138	TLSv...	1389	Application Data
28	0.329508	52.163.89.138	192.168.0.105	TLSv...	653	Application Data

Frame 8: 250 bytes on wire (2000 bits), 250 bytes captured (2000 bits) on interface \Device\NPF_{8DD29CF6-2337-4B28-9F1E-596458C8B67C}, id 0

Ethernet II, Src: IntelCor_06:0b:53 (5c:87:9c:06:0b:53), Dst: Tp-LinkT_64:16:70 (98:da:c4:64:16:70)

Internet Protocol Version 4, Src: 192.168.0.105, Dst: 52.163.89.138

Transmission Control Protocol, Src Port: 1032, Dst Port: 443, Seq: 1, Ack: 1, Len: 196

Transport Layer Security

✓ TLSv1.2 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 191

Handshake Protocol: Client Hello

Client Hello

0000 98 da c4 64 16 70 5c 87 9c 06 0b 53 08 00 45 00 ...d.p\...S...E.

0010 00 ec 45 c3 40 00 80 06 65 0a c0 a8 00 69 34 a3 ..E.@...e...i4.

0020 59 8a 04 08 01 bb 2f d3 f9 2a c5 8b 51 bc 50 18 Y...../*.*.Q.P.

0030 02 05 db bb 00 00 16 03 03 00 bf 01 00 00 bb 03#.....

0040 03 5f cf 9f fe 5d 7e 40 c7 e5 e5 23 99 91 a5 20 ...~@...#...

b) Server Hello, Certificate, Server Hello Done

The screenshot shows a Wireshark capture of a TLS handshake. The packet list on the left shows several packets, with packet 13 (1293 bytes) selected. The packet details pane on the right shows the structure of the TLSv1.2 Record Layer, including the Handshake Protocol: Multiple Handshake Messages. The packet bytes pane at the bottom shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
8	0.144748	192.168.0.105	52.163.89.138	TLSv...	250	Client Hello
13	0.199318	52.163.89.138	192.168.0.105	TLSv...	1293	Server Hello, Certificate, Certificate Status, Server Key Exchange, ...
15	0.201277	192.168.0.105	52.163.89.138	TLSv...	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
23	0.250414	52.163.89.138	192.168.0.105	TLSv...	105	Change Cipher Spec, Encrypted Handshake Message
25	0.271698	192.168.0.105	52.163.89.138	TLSv...	455	Application Data
26	0.271898	192.168.0.105	52.163.89.138	TLSv...	1389	Application Data
28	0.329508	52.163.89.138	192.168.0.105	TLSv...	653	Application Data

Frame 13: 1293 bytes on wire (10344 bits), 1293 bytes captured (10344 bits) on interface \Device\NPF_{8DD29CF6-2337-4B28-9F1E-596458C8B67C}, id 0
Ethernet II, Src: Tp-LinkT_64:16:70 (98:da:c4:64:16:70), Dst: IntelCor_06:0b:53 (5c:87:9c:06:0b:53)
Internet Protocol Version 4, Src: 52.163.89.138, Dst: 192.168.0.105
Transmission Control Protocol, Src Port: 443, Dst Port: 1032, Seq: 5761, Ack: 197, Len: 1239
[5 Reassembled TCP Segments (6999 bytes): #9(1440), #10(1440), #11(1440), #12(1440), #13(1239)]
Transport Layer Security
 TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages
 Content Type: Handshake (22)
 Version: TLS 1.2 (0x0303)
 Length: 6994
 Handshake Protocol: Server Hello
 Handshake Protocol: Certificate
 Handshake Protocol: Certificate Status
 Handshake Protocol: Server Key Exchange
 Handshake Protocol: Server Hello Done

Server Hello, Certificate and Server Hello Done

0000 5c 87 9c 06 0b 53 98 da c4 64 16 70 08 00 45 00 \...S...d.p..E.
0010 04 ff 31 98 40 00 74 06 81 22 34 a3 59 8a c0 a8 ..1.@.t..4.Y..
0020 00 69 01 bb 04 08 c5 8b 68 3c 2f d3 f9 ee 50 18 .i.....h</...P.
0030 04 05 49 63 00 00 b7 94 ea 31 31 02 91 6a 1b d6 ..Ic....11..j..

c) Client key exchange, Change Cipher Spec, Encrypted Handshake Msg

The screenshot shows a Wireshark capture of a TLS handshake. The packet list on the left shows several packets, with packet 15 (147 bytes) selected. The packet details pane on the right shows the structure of the TLSv1.2 Record Layer, including the Handshake Protocol: Client Key Exchange, Change Cipher Spec, and Encrypted Handshake Message. The packet bytes pane at the bottom shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
8	0.144748	192.168.0.105	52.163.89.138	TLSv...	250	Client Hello
13	0.199318	52.163.89.138	192.168.0.105	TLSv...	1293	Server Hello, Certificate, Certificate Status, Server Key Exchange, ...
15	0.201277	192.168.0.105	52.163.89.138	TLSv...	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
23	0.250414	52.163.89.138	192.168.0.105	TLSv...	105	Change Cipher Spec, Encrypted Handshake Message
25	0.271698	192.168.0.105	52.163.89.138	TLSv...	455	Application Data
26	0.271898	192.168.0.105	52.163.89.138	TLSv...	1389	Application Data
28	0.329508	52.163.89.138	192.168.0.105	TLSv...	653	Application Data

Frame 15: 147 bytes on wire (1176 bits), 147 bytes captured (1176 bits) on interface \Device\NPF_{8DD29CF6-2337-4B28-9F1E-596458C8B67C}, id 0
Ethernet II, Src: IntelCor_06:0b:53 (5c:87:9c:06:0b:53), Dst: Tp-LinkT_64:16:70 (98:da:c4:64:16:70)
Internet Protocol Version 4, Src: 192.168.0.105, Dst: 52.163.89.138
Transmission Control Protocol, Src Port: 1032, Dst Port: 443, Seq: 197, Ack: 7000, Len: 93
Transport Layer Security
 TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
 TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
 TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message

Client Key Exchange, Change Cipher Spec and Encrypted Handshake Message

0000 98 da c4 64 16 70 5c 87 9c 06 0b 53 08 00 45 00 ...d.p\...S..E.
0010 00 85 45 c5 40 00 80 06 65 6f c0 a8 00 69 34 a3 ..E.@...eo...i4.
0020 59 8a 04 08 01 b6 2f d3 f9 ee c5 8b 6d 13 50 18 Y...../.....m.P.
0030 02 05 f7 1e 00 00 16 03 03 00 25 10 00 00 21 20%...!
0040 4b 46 e7 4e d1 9e bf fb 75 95 a2 b2 0b e2 ae c3 KF.N....u.....

d) Change cipher spec and encrypted handshake messages

The screenshot shows a Wireshark capture of a TLS handshake. The packet list on the left shows several packets, with packet 23 (105 bytes) selected. The packet details pane on the right shows the following structure:

- Frame 23: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface \Device\NPF_{8DD29CF6-2337-4B28-9F1E-596458C8B67C}, id 0
- Ethernet II, Src: Tp-LinkT_64:16:70 (98:da:c4:64:16:70), Dst: IntelCor_06:0b:53 (5c:87:9c:06:0b:53)
- Internet Protocol Version 4, Src: 52.163.89.138, Dst: 192.168.0.105
- Transmission Control Protocol, Src Port: 443, Dst Port: 1032, Seq: 7000, Ack: 290, Len: 51
- Transport Layer Security
 - TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
 - TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message

The packet bytes pane at the bottom shows the raw data of the selected packet, which is a Change Cipher Spec message followed by an Encrypted Handshake Message.

e) Application Data(from source 192.168.0.105)

The screenshot shows a Wireshark capture of a TLS application data packet. The packet list on the left shows several packets, with packet 25 (455 bytes) selected. The packet details pane on the right shows the following structure:

- Frame 25: 455 bytes on wire (3640 bits), 455 bytes captured (3640 bits) on interface \Device\NPF_{8DD29CF6-2337-4B28-9F1E-596458C8B67C}, id 0
- Ethernet II, Src: IntelCor_06:0b:53 (5c:87:9c:06:0b:53), Dst: Tp-LinkT_64:16:70 (98:da:c4:64:16:70)
- Internet Protocol Version 4, Src: 192.168.0.105, Dst: 52.163.89.138
- Transmission Control Protocol, Src Port: 1032, Dst Port: 443, Seq: 290, Ack: 7051, Len: 401
- Transport Layer Security
 - TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
 - Content Type: Application Data (23)
 - Version: TLS 1.2 (0x0303)
 - Length: 396
 - Encrypted Application Data: 0000000000000001c4787ca266dcc464052ac756ff48a51df5fe3b596d2155febb97c316...
 - [Application Data Protocol: http-over-tls]

The packet bytes pane at the bottom shows the raw data of the selected packet, which is an Application Data packet (http-over-tls).

Application Data from server to my computer

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No.	Time	Source	Destination	Protocol	Length	Info
8	0.144748	192.168.0.105	52.163.89.138	TLSv...	250	Client Hello
13	0.199318	52.163.89.138	192.168.0.105	TLSv...	1293	Server Hello, Certificate, Certificate Status, Server Key Exchange,
15	0.201277	192.168.0.105	52.163.89.138	TLSv...	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
23	0.250414	52.163.89.138	192.168.0.105	TLSv...	105	Change Cipher Spec, Encrypted Handshake Message
25	0.271698	192.168.0.105	52.163.89.138	TLSv...	455	Application Data
26	0.271898	192.168.0.105	52.163.89.138	TLSv...	1389	Application Data
28	0.329508	52.163.89.138	192.168.0.105	TLSv...	653	Application Data

> Frame 28: 653 bytes on wire (5224 bits), 653 bytes captured (5224 bits) on interface \Device\NPF_{8DD29CF6-2337-4B28-9F1E-596458C8B67C}, id 0

> Ethernet II, Src: Tp-LinkT_64:16:70 (98:da:c4:64:16:70), Dst: IntelCor_06:0b:53 (5c:87:9c:06:0b:53)

> Internet Protocol Version 4, Src: 52.163.89.138, Dst: 192.168.0.105

> Transmission Control Protocol, Src Port: 443, Dst Port: 1032, Seq: 7051, Ack: 2026, Len: 599

> Transport Layer Security

> TLSv1.2 Record Layer: Application Data Protocol: http-over-tls

Content Type: Application Data (23)

Version: TLS 1.2 (0x0303)

Length: 594

Encrypted Application Data: 000000000000001411ea8c004ed2bb3dcc17e32d5f8baef7b58a256150a46bb02eff2ce...

[Application Data Protocol: http-over-tls]

Application Data from server to my computer

0030 04 05 5c 56 00 00 17 03 03 02 52 00 00 00 00 00 ..\V....R....

0040 00 00 01 41 1e a8 c0 04 ed 2b b3 dc c1 7e 32 d5 ...A....+...~2.

0050 f8 ba ef 7b 58 a2 56 15 0a 46 bb 02 ef f2 ce d5 ...{X.V.F.....

0060 70 be 07 f5 26 bf 6b 65 74 59 39 52 ee 7e 4e 01 p...&•ke tY9R~N.

0070 b9 59 76 97 65 eb 97 4e f7 92 45 b1 05 b0 b0 05 •YV•e•N•E.....

Record Layer (tls.record), 599 bytes

Packets: 2302 · Displayed: 523 (22.7%) · Dropped: 0 (0.0%)

Profile: Default

21:37 08-12-2020