

CNS LAB

Batch: B1

Assignment: 10

PRN No: 2020BTECS00006

Name: Samrat Vishwas Jadhav

Aim: To observe SSL/TLS (Secure Sockets Layer/ Transport Layer Security) in action. SSL/TLS is used to secure TCP connections, and it is widely used as part of the secure web: HTTPS is SSL over HTTP.

2 STEP 1: Open a Trace you should use a supplied trace file trace-ssl.pcap.

File → Open → open from folder containing file.

3 STEP 2: Inspect the Trace

Now we are ready to look at the details of some SSL messages. To begin, enter and apply a display filter of ssl. This filter will help to simplify the display by showing only SSL and TLS messages. It will exclude other TCP segments that are part of the trace, such as Acks and connection open/close. Select a TLS message somewhere in the middle of your trace for the Info field reads Application Data, and expand its Secure Sockets Layer block (by using triangular icon on left side). Application Data is a generic TLS message carrying contents for the application, such as the web page. It is a good place for us to start looking at TLS messages. Look for the following protocol blocks and fields in the message

- The lower layer protocol blocks are TCP and IP because SSL runs on top of TCP/IP.
- The SSL layer contains a TLS Record Layer. This is the foundational sublayer

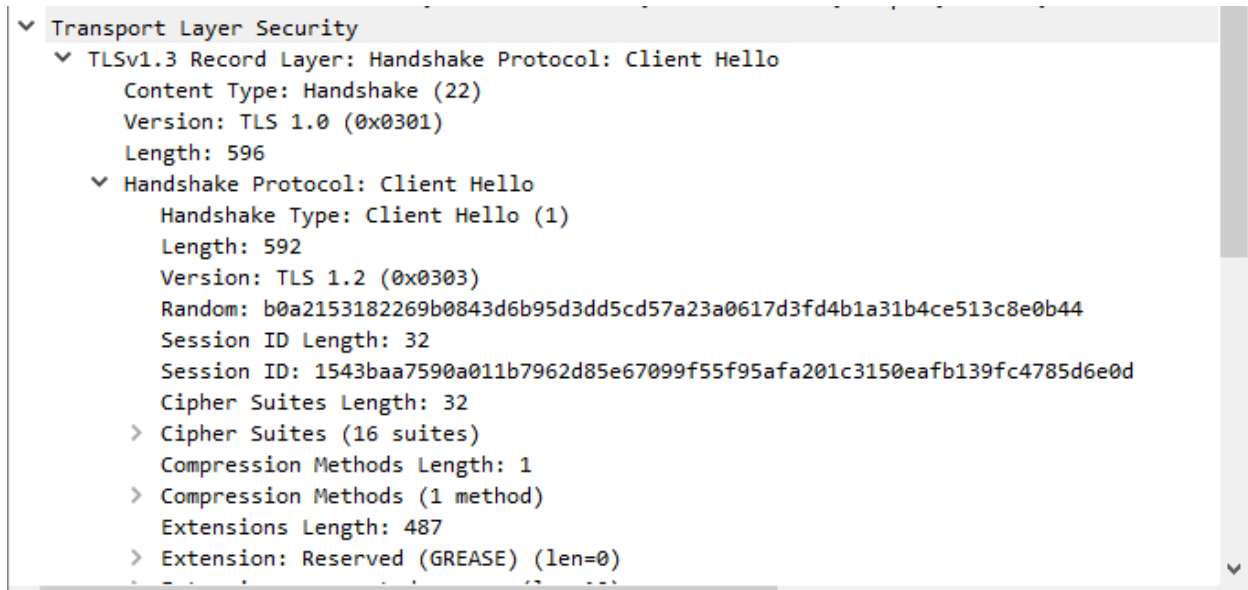
- Each record starts with a Content Type field. This tells us what is in the contents of the record. Then comes a Version identifier. It will be a constant value for the SSL connection.

- It is followed by a Length field giving the length of the record.
- Last comes the contents of the record. Application Data records are sent after SSL has secured the connection, so the contents will show up as encrypted data.

Note that, unlike other protocols we will see such as DNS, there may be multiple records in a single message. Each record will show up as its own block. Look at the Info column, and you will see messages with more than one block.

Answer the following questions to show your understanding of SSL records:

[illegible]



1. What is the Content Type for a record containing Application Data?:

Content Type: Handshake(22)

2. What version constant is used in your trace, and which version of TLS does it represent?

Version : 1.0 (0x0301)

4 Step 3: The SSL Handshake

An important part of SSL is the initial handshake that establishes a secure connection.

The handshake proceeds in several phases. There are slight differences for different versions of TLS and depending on the encryption scheme that is in use. The usual outline for a brand new connection is:

- Client (the browser) and Server(the web server) both send their Hellos
- Server sends its certificate to Client to authenticate (and optionally asks for Client Certificate)

- Client sends keying information and signals a switch to encrypted data.
- Server signals a switch to encrypted data.
- Both Client and Server send encrypted data.
- An Alert is used to tell the other party that the connection is closing. Note that there is also a mechanism to resume sessions for repeat connections between the same client and server to skip most of steps b and c.

4.1 Hello Message

Find and inspect the details of the Client Hello and Server Hello messages, including expanding the Handshake protocol block within the TLS Record. For these initial messages, an encryption scheme is not yet established so the contents of the record are visible to us. They contain details of the secure connection setup in a Handshake protocol format.

Answer the following questions.

1. How long in bytes is the random data in the Hellos? Both the Client and Server include this random data (a nonce) to allow the establishment of session keys.

→ Length of random Bytes: 28

No.	Time	Source	Destination	Protocol	Length	Info
2546	10.567688	164.100.192.102	10.4.2.215	TLSv1.2	1514	Application Data
2553	10.568540	164.100.192.102	10.4.2.215	TLSv1.2	1514	Application Data
2624	10.583564	164.100.192.102	10.4.2.215	TLSv1.2	1514	Application Data
2641	10.584776	10.4.2.215	142.250.192.99	TLSv1.3	655	Client Hello
2645	10.585333	10.4.2.215	142.250.192.99	TLSv1.3	591	Client Hello
2650	10.585561	164.100.192.102	10.4.2.215	TLSv1.2	1514	Application Data
2659	10.587165	164.100.192.102	10.4.2.215	TLSv1.2	1514	Application Data
2672	10.588733	164.100.192.102	10.4.2.215	TLSv1.2	1514	Application Data
2679	10.589107	164.100.192.102	10.4.2.215	TLSv1.2	1514	Application Data
2686	10.591370	164.100.192.102	10.4.2.215	TLSv1.2	1514	Application Data
2693	10.597694	164.100.192.102	10.4.2.215	TLSv1.2	1514	Application Data

> Frame 2641: 655 bytes on wire (5240 bits), 655 bytes captured (5240 bits) on interface \Dev	0040	03 b0 a2 15 31 82 26 9b 08 43 d6 b9 5d 3d d5 cd1.....C.....
> Ethernet II, Src: IntelCor_2c:89:c2 (ac:7b:a1:2c:89:c2), Dst: ExtremeN_1:fb:b0 (00:04:96:a	0050	57 a2 3a 06 17 d3 fd 4b 1a 31 b4 ce 51 3c 8e 0b	W:.....K 1.....Q<...
> Internet Protocol Version 4, Src: 10.4.2.215, Dst: 142.250.192.99	0060	44 20 15 43 ba a7 59 0a 01 1b 79 62 d8 5e 67 09	D: C.....Y.....yb..g.
> Transmission Control Protocol, Src Port: 52389, Dst Port: 443, Seq: 1, Ack: 1, Len: 601	0070	9f 55 f9 5a fa 20 1c 31 50 ea fb 13 9f c4 78 5d	U:Z.....1 P.....x]
> Transport Layer Security	0080	6e 0d 00 20 0a 0a 13 01 13 02 13 03 c0 2b c0 2f	n.....+...../
> TLSv1.3 Record Layer: Handshake Protocol: Client Hello	0090	c0 2c c0 30 cc a9 cc a8 c0 13 c0 14 00 9c 00 9d0.....
Content Type: Handshake (22)	00a0	00 2f 00 35 01 00 01 e7 1a 1a 00 00 0a 00 0a	/:5.....
Version: TLS 1.0 (0x0301)	00b0	00 08 aa a0 0d 10 01 00 18 00 12 00 00 44 69h2.....D1
Length: 596	00c0	00 05 00 03 02 68 32 00 00 00 16 00 14 00 00 11h2.....D1
> Handshake Protocol: Client Hello	00d0	66 6f 6e 74 73 2e 67 73 74 61 74 69 63 2e 63 6f	fontsgs.tatic.co
Handshake Type: Client Hello (1)	00e0	6d fe 0d 01 1a 00 00 01 00 01 6f 00 20 9d 51 af	m.....Q:
Length: 592	00f0	f6 e3 b7 dc 4f 91 8f d8 e4 a1 7e e9 36 24 12 ff0.....65\$
Version: TLS 1.2 (0x0303)	0100	1b 89 a1 af 37 76 4a 2a 49 b3 3a 54 06 00 f0 36203*.....AT...
Random: b0a2153182269b0843d6b95d3dd5cd57a23a0617d3fd4b1a31b4ce513c8e0b44	0110	a0 2c 9c b7 37 78 fa 7b 27 6a db da ba 70 1c 017x{.....j.....p
Session ID Length: 32	0120	8a 2a d4 35 c8 1c fb 6c 28 1b 56 8b 2e 1b 1d 7c5.....1 (V.....v
Session ID: 1543baa7590a011b7962d85e67099f55f95afa201c3150eafb139fc4785d6e0d	0130	b0 63 10 d4 0d 61 c9 80 91 e3 4a cc 01 ba de 125.....1 (V.....v
Cipher Suites Length: 32	0140	89 a3 81 1c 7f 65 99 1d d6 f2 6e 34 2d d2 33 30e.....n4.....30
Cipher Suites (16 suites)	0150	e4 c1 42 0f cb a9 80 7c b8 b2 77 03 84 14 07 86B.....j.....w.....
Compression Methods Length: 1	0160	6c d0 af d2 62 bf 22 bc 4c af 93 92 4f d5 3c 00b.....L.....0<...
Compression Methods (1 method)	0170	91 99 a0 2e e5 8f ea ab 5f da ab 60 a2 8e 2c 96K.....
Extensions Length: 487	0180	ec 9b ec ce a4 70 fa 04 e1 60 4f 3f 27 59 70 d9x.....03Yw
Extension: Reserved (GREASE) (len=0)	0190	07 ec 8f 4c bb 14 06 5f 6a bd 50 45 bb 3d f1 f6L.....j.....PE...
	01a0	54 9f ea 19 6f 7e 00 e1 6f 5a b6 2a 4c 88 63 f6ow.....o2*L.....c
	01b0	9b 10 cb 14 78 6f 70 67 af 1d a1 af 8e 3c 3b 26x.....x.....p.....WS
	01c0	f0 d7 49 c7 d3 39 25 78 05 32 1f 2c cd 1f 4c 02I.....9X.....2.....L
	01d0	6e ce c2 e6 1a 4d a5 f6 1a c6 d7 8a 02 52 a6 3dG.....n.....h.....2.....R

2. How long in bytes is the session identifier sent by the server? This identifier allows later resumption of the session with an abbreviated handshake when both the client and server indicate the same value. In our case, the client likely sent no session ID as there was nothing to resume.

→ Session Identifier Length: 32 (Bytes 110 - 141)

No.	Time	Source	Destination	Protocol	Length	Info
3349	10.775788	164.100.192.102	10.4.2.215	TLSv1.2	1514	Application Data, Application Data
3355	10.783410	164.100.192.102	10.4.2.215	TLSv1.2	1514	Application Data
3369	10.792209	142.250.192.99	10.4.2.215	TLSv1.3	1466	Server Hello, Change Cipher Spec
3372	10.792209	142.250.192.99	10.4.2.215	TLSv1.3	304	Application Data
3381	10.792968	142.250.192.99	10.4.2.215	TLSv1.3	1466	Server Hello, Change Cipher Spec
3385	10.793213	142.250.192.99	10.4.2.215	TLSv1.3	305	Application Data
3396	10.796128	10.4.2.215	142.250.192.99	TLSv1.3	128	Change Cipher Spec, Application Data
3397	10.796671	10.4.2.215	142.250.192.99	TLSv1.3	128	Change Cipher Spec, Application Data
3408	10.797602	10.4.2.215	142.250.192.99	TLSv1.3	146	Application Data
3422	10.798891	10.4.2.215	142.250.192.99	TLSv1.3	533	Application Data
3423	10.799012	10.4.2.215	142.250.192.99	TLSv1.3	139	Application Data

Frame 3369: 1466 bytes on wire (11728 bits), 1466 bytes captured (11728 bits) on interface	
Ethernet II, Src: ExtremeN_01:fb:0b (00:04:96:a1:fb:0b), Dst: IntelCor_2c:89:c2 (ac:7b:a1:2	
Internet Protocol Version 4, Src: 142.250.192.99, Dst: 10.4.2.215	
Transmission Control Protocol, Src Port: 443, Dst Port: 52389, Seq: 1, Ack: 602, Len: 1412	
Transport Layer Security	
<ul style="list-style-type: none"> TLSv1.3 Record Layer: Handshake Protocol: Server Hello <ul style="list-style-type: none"> Content Type: Handshake (22) Version: TLS 1.2 (0x0303) Length: 122 Handshake Protocol: Server Hello <ul style="list-style-type: none"> Handshake Type: Server Hello (2) Length: 118 Version: TLS 1.2 (0x0303) Random: e3d30df550c037a087b63c263541fc9546aea3fa9ae82653e9318120b7fa3f31 Session ID Length: 32 Session ID: 1543baa7590a011b7962d85e67099f55f95afa201c3150eafb139fc4785d6e0d Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301) Compression Method: null (0) Extensions Length: 46 Extension: key_share (len=36) Extension: supported_versions (len=2) [JA3S Fullstring: 771,4865,51-43] 	

Offset	Hex	ASCII
0060	31 2e 15 43 ba a7 59 0a 01 1b 79 62 d8 5e 67 09	1.C.Y. .yb.g.
0070	9f 55 f9 5a fa 20 1c 31 50 ea fb 13 9f c4 78 5d	.U.Z. .1 P....x]
0080	6e 0d 13 01 00 00 2e 00 33 00 24 00 1d 00 20 cb	n..... 3.\$....
0090	d0 5a d0 d6 4f a4 9a 1e a3 dd 29 3f f6 d7 cc 29	.Z.O....?)?....
00a0	be 37 30 93 80 94 82 54 4d fb 46 e2 90 a0 48 00	.70....T M-F...H
00b0	2b 00 02 05 04 14 03 03 00 01 01 17 03 03 10 fc	4.....
00c0	95 4b fa 1e 77 9a 3f 80 5b b1 67 e3 b8 d4 d4 c7	.K.w.?. [g....
00d0	16 bd 8e 5f 7d 96 47 f8 89 4c 04 cc 78 ac 44 6aG. L.x.xDj
00e0	ad 1c 68 78 71 44 ac 27 16 65 59 32 28 61 7a 99	..hxqDL' .eY2(az
00f0	57 e6 ed b2 85 8b a5 04 d2 d2 bb 73 4f ae f0 7e	W.....s0..w
0100	eb 1c bb da db d8 de 9e d0 9b 40 38 65 a4 8b 5688e..V
0110	51 5a 3a 59 51 7c 73 df 1c c0 4b 7c b4 18 74 aa	QZ[YQ[s. .k .t.
0120	67 9a 39 5b 7e 1f 4a 08 0e 94 8a 17 69 7e 3c fe	8:9[-J. ...l.w.
0130	df fb 79 a6 9b 3f c5 6e 26 52 cb 53 42 d4 6f ea	.y.?.n &R.SB.o
0140	69 d1 1f 72 f8 e2 13 ab cf 32 77 8c 0d 46 1b 86	l.....2w..F..
0150	6d 52 10 cd 91 95 e3 58 a2 38 60 11 83 85 e5 f0	mR.....X..8'....
0160	e8 7c 89 bd 4d 24 d1 a9 b2 b8 82 da ea c2 fd 28	...MS... ..(
0170	e6 b4 6c a9 aa 32 b1 a3 97 59 a6 ea 2e 12 73 0b	.1..2...Y....s
0180	7b fd f1 22 1f 09 ad 2d 24 80 b9 c8 e7 0e a0 10	}. ".... \$.
0190	b5 78 77 e2 87 83 12 d8 bb 36 99 4a 4b a0 8d 64	xw.....6-JK..d
01a0	db 83 4d 2a 2b b0 a2 16 d0 8a 68 0f 63 ac 52 27	..M*+....h.c.R
01b0	70 a9 a1 dd 5a 36 c5 e3 76 cf 67 f5 36 ea 80 28	p...Z6...v.g.6.(
01c0	8b 1f 6e 67 1f cc 0b ac da a3 e1 1e 88 b9 21 97	..ng..... ..l
01d0	d6 b4 24 e4 6b 60 64 b2 41 e7 15 1f 83 19 62 e0	Act..kld..Amdbws
01e0	2d 04 17 c4 3e e2 9a 35 30 71 cc 3c 43 7e 59 77	...>...5 0q.cC.vw
01f0	6b 24 0e 32 57 6e 0e 5a 80 18 69 c1 27 3f d9 68	00g..2m..2..1..7..h

3. What Cipher suite is chosen by the Server? Give its name and value. The Client will list the different cipher methods it supports, and the Server will pick one of these methods to use.

→ Cipher Suite used by the Server is:

Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)

> Frame 3369: 1466 bytes on wire (11728 bits), 1466 bytes captured (11728 bits) on interface	0000 6e 0d 13 01 00 00 2e 00 33 00 24 00 1d 00 20 cb n.....3\$...
> Ethernet II, Src: ExtremeN_al:fb:0b (00:04:96:a1:fb:0b), Dst: IntelCor_2c:89:c2 (ac:7b:a1:2	0000 d0 5a d0 d6 4f a4 9a 1e a3 dd 29 3f f6 d7 cc 29 .Z..O...?)?..)
> Internet Protocol Version 4, Src: 142.250.192.99, Dst: 10.4.2.215	0000 be 37 30 93 80 94 82 54 4d fb 46 e2 90 a0 48 00 .70...T M.F...H
> Transmission Control Protocol, Src Port: 443, Dst Port: 52389, Seq: 1, Ack: 602, Len: 1412	0000 2b 00 02 03 04 14 03 03 00 01 01 17 03 03 10 fc +.....
> Transport Layer Security	0000 95 4b fa 1e 77 9a 3f 80 5b b1 67 e3 b8 d4 d4 c7 .K.w.? [.g...x
▼ TLSv1.3 Record Layer: Handshake Protocol: Server Hello	0000 16 bd 8e 5f 7d 96 47 f8 89 4c 04 cc 78 ac 44 6a ...).G. .L.x.Dj
Content Type: Handshake (22)	0000 ad 1c 68 78 71 44 4c 27 16 65 59 32 28 61 7a 99 ..hxqDL. eY2(az
Version: TLS 1.2 (0x0303)	0000 57 e6 ed b2 85 0b a5 04 d2 2d bb 73 4f ae f9 7e W.....-s0..w
Length: 122	0100 e6 1c bb da db d8 de 9e d9 9b 40 38 65 a4 8b 56@B...V
▼ Handshake Protocol: Server Hello	0110 51 5a 3a 59 51 7c 73 df 1c c0 4b 7c b4 18 74 aa QZ:VQ s. ...X .t
Handshake Type: Server Hello (2)	0120 67 9a 39 5b 7e 1f 4a 88 8e 94 8a 17 69 7e 3c fe g.9[~.J. ...i.<c
Length: 118	0130 df fb 79 a6 9b 3f c5 6e 26 52 cb 53 42 d4 6f ea .y.?.n &R.SB.o
Version: TLS 1.2 (0x0303)	0140 69 d1 1f 72 f8 e2 13 ab cf 32 77 8c 0d 46 1b 8e i...r....2w..F
Random: e3d30df55c0c37a087b63c263541fc9546aea3fa9ae82653e9318120b7fa3f31	0150 6d 52 10 cd 91 95 e3 58 a2 38 60 11 83 85 e5 f0 mR.....X.8'.....
Session ID Length: 32	0160 e8 7c 89 bd 4d 24 d1 a9 b2 b8 82 da ea c2 f2 28 . .N\$.(
Session ID: 1543baa7590a011b7962d85e67099f55f95afa201c3150eafb139fc4785d6e0d	0170 e6 b4 6c a9 aa 32 b1 a3 97 59 ae a6 2e 12 73 0b .1..2...Y...s
Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)	0180 fb 7d f1 22 1f 09 ad 2d 24 80 b9 c8 e7 0e a0 10 .).".\$.
Compression Method: null (0)	0190 b8 78 77 e2 87 83 12 d8 bb 36 99 4a 4b a8 8d 64 .xw.....6.JK..d
Extensions Length: 46	01a0 db 83 4d 2a 2b b0 a2 16 d0 8a 68 0f 63 ac 52 27 ..H*....h.c.R'
> Extension: key_share (len=36)	01b0 70 a9 a1 dd 5a 36 c5 e3 76 cf 67 f5 36 ea 80 28 p...26...v.g.B..(
> Extension: supported_versions (len=2)	01c0 8b 1f 6e 67 1f cc 0b ac da a3 e1 1e 88 b9 21 97 .ng.....!..
[JA3S Fullstring: 771,4865,51-43]	01d0 d6 b4 24 e4 6b 60 64 b2 41 e7 15 1f 83 19 62 e0 ..\$.k'd. A...<b
	01e0 2d 04 17 c4 3e e2 9a 35 30 71 cc 3c 43 7e 59 77 ..>...5 Oq.<C.Ww
	01f0 6b 24 0e 32 57 6e 0e 5a 80 18 69 c1 27 3f d9 68 \$\$.2Mn.Z...W...b
	0200 17 15 ab 31 9b 8a e9 92 80 02 2e 9a 1d fe 5b d5 ...1.....[
	0210 c9 8b 19 a6 31 08 71 06 7c dh 0b 8b ea 12 9a f6 7c dh 0b 8b ea 12 9a f6

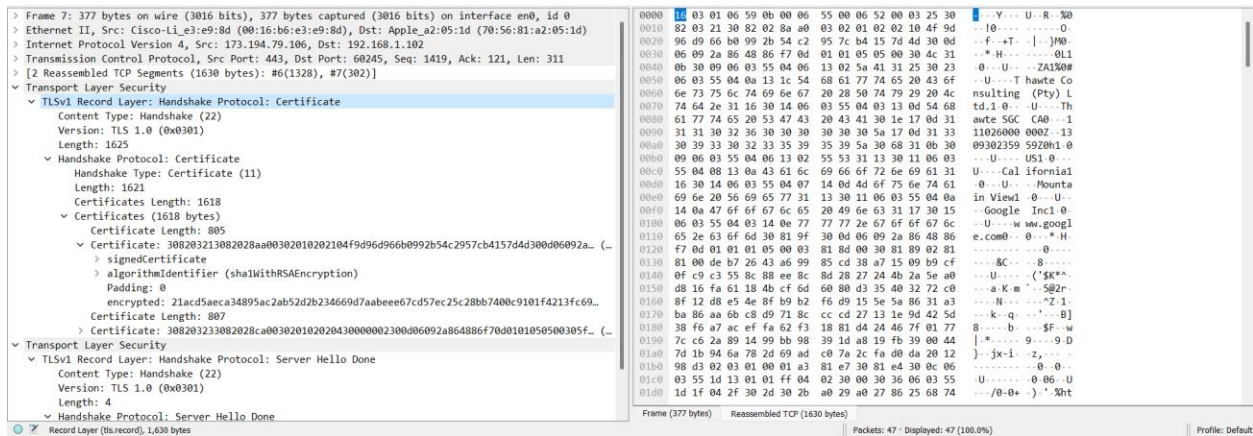
4.2 Certificate Messages

Next, find and inspect the details of the Certificate message, including expanding the Handshake proto-col block within the TLS Record. As with the Hellos, the contents of the Certificate message are visible because an encryption scheme is not yet established. It should come after the Hello messages.

Answer the following questions:

1. Who sends the Certificate, the client, the server, or both? A certificate is sent by one party to let the other party authenticate that it is who it claims to be. Based on this usage, you should be able to guess who sends the certificate and check the messages in your trace.

→ In this packet tract only server is sending its certificate. But there might be the case that the server could ask the client to provide its own certificate for the identity of the client.



A Certificate message will contain one or more certificates, as needed for one party to verify the identity of the other party from its roots of trust certificates. You can inspect those certificates in your browser.

4.3 Client Key Exchange and Change Cipher Messages

Find and inspect the details of the Client Key Exchange and Change Cipher messages, expanding their various details. The key exchange message is sent to pass keying information so that both sides will have the same secret session key. The change cipher message signal a switch to a new encryption scheme to the other party. This means that it is the last unencrypted message sent by the party.

Answer the following questions:

1. Who sends the Change Cipher Spec message, the client, the server, or both?

→ The change cipher spec message is sent by both client and server. Client sent it first.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	173.194.79.106	TCP	78	60245 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=1222755671 TSecr=0 SACK_PERM
2	0.019644	173.194.79.106	192.168.1.102	TCP	74	443 → 60245 [SYN, ACK] Seq=0 Ack=1 Win=14180 Len=0 MSS=1430 SACK_PERM TSval=1520057876 TSecr=1222755671 WS=64
3	0.019829	192.168.1.102	173.194.79.106	TCP	66	60245 → 443 [ACK] Seq=1 Ack=1 Win=524280 Len=0 TSval=1222755690 TSecr=1520057876
4	0.021328	192.168.1.102	173.194.79.106	TLSv1	186	Client Hello
5	0.040766	173.194.79.106	192.168.1.102	TCP	66	443 → 60245 [ACK] Seq=1 Ack=121 Win=14208 Len=0 TSval=1520057898 TSecr=1222755691
6	0.041634	173.194.79.106	192.168.1.102	TLSv1	1484	Server Hello
7	0.041697	173.194.79.106	192.168.1.102	TLSv1	377	Certificate, Server Hello Done
8	0.041798	192.168.1.102	173.194.79.106	TCP	66	60245 → 443 [ACK] Seq=121 Ack=1730 Win=522928 Len=0 TSval=1222755710 TSecr=1520057899
9	0.088543	192.168.1.102	173.194.79.106	TLSv1	252	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10	0.105145	173.194.79.106	192.168.1.102	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
11	0.105201	192.168.1.102	173.194.79.106	TCP	66	60245 → 443 [ACK] Seq=307 Ack=1777 Win=524280 Len=0 TSval=1222755773 TSecr=1520057963
12	0.105436	192.168.1.102	173.194.79.106	TLSv1	239	Application Data
13	0.136468	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data
14	0.136525	192.168.1.102	173.194.79.106	TCP	66	60245 → 443 [ACK] Seq=480 Ack=3127 Win=523304 Len=0 TSval=1222755804 TSecr=1520057993
15	0.137903	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data
16	0.137932	192.168.1.102	173.194.79.106	TCP	66	60245 → 443 [ACK] Seq=480 Ack=4477 Win=523304 Len=0 TSval=1222755805 TSecr=1520057993
17	0.138469	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data, Application Data
18	0.138500	192.168.1.102	173.194.79.106	TCP	66	60245 → 443 [ACK] Seq=480 Ack=5827 Win=523304 Len=0 TSval=1222755805 TSecr=1520057993
19	0.138632	173.194.79.106	192.168.1.102	TLSv1	316	Application Data, Application Data
20	0.138660	192.168.1.102	173.194.79.106	TCP	66	60245 → 443 [ACK] Seq=480 Ack=6077 Win=524280 Len=0 TSval=1222755805 TSecr=1520057993
21	0.140271	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data, Application Data

2. What are the contents carried inside the Change Cipher Spec message? Look past the Content Type and other headers to see the message itself.

> Frame 10: 113 bytes on wire (904 bits), 113 bytes captured (904 bits) on interface en0, id 0

> Ethernet II, Src: Cisco-Li_e3:e9:8d (00:16:b6:e3:e9:8d), Dst: Apple_a2:05:1d (70:56:81:a2:05:1d)

> Internet Protocol Version 4, Src: 173.194.79.106, Dst: 192.168.1.102

> Transmission Control Protocol, Src Port: 60245, Seq: 1730, Ack: 307, Len: 47

▼ Transport Layer Security

 ▼ TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec

 Content Type: Change Cipher Spec (20)

 Version: TLS 1.0 (0x0301)

 Length: 1

 Change Cipher Spec Message

 ▼ TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message

 Content Type: Handshake (22)

 Version: TLS 1.0 (0x0301)

 Length: 36

 Handshake Protocol: Encrypted Handshake Message

```

0000  70 56 81 a2 05 1d 00 16  b6 e3 e9 8d 08 00 45 20  pV.....E
0010  00 63 64 8a 00 00 2f 06  67 b0 ad c2 4f 6a c0 a8  cd.../.g..0j..
0020  01 66 b1 bb e0 55 4c 7a  60 e4 4f 70 a8 1b 80 18  -f...Ult..Op...
0030  00 ef 2f ac 00 00 01 01  08 0a 5a 9a 3e 6b 48 e1  -//.....Z>kh...
0040  c5 ad 14 03 01 00 01 01  16 03 01 00 24 2d 92 e2  -.....$...
0050  26 2a f7 91 d1 a9 14 7c  d5 6e 05 70 87 69 be 20  &*.....n.p.i-
0060  a0 f1 62 f4 9a 36 24 1c  d0 11 bc 3c bb 92 2d aa  -b..6$...<...
0070  0d

```

→ The Change Cipher Spec Message contains following Fields:

- Content Type
- Version
- Length
- change cipher spec message