

Step2:

No.	Time	Source	Destination	Protocol	Length	Info
870...	3140.0668...	13.107.18.11	10.15.70.220	TLSv1.2	173	Application Data
870...	3143.8535...	104.248.182.131	10.15.70.220	TLSv1.2	93	Application Data
870...	3143.8560...	10.15.70.220	104.248.182.131	TLSv1.2	97	Application Data
870...	3143.9460...	10.15.70.220	203.205.254.91	SSL	364	Continuation Data
871...	3144.3660...	203.205.254.91	10.15.70.220	SSL	202	Continuation Data
871...	3145.7724...	10.15.70.220	52.45.119.166	TLSv1.2	583	Client Hello
871...	3145.8538...	52.45.119.166	10.15.70.220	TLSv1.2	211	Server Hello, Change Cipher Spec, Encrypted Handshake Message
871...	3145.8557...	10.15.70.220	52.45.119.166	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
871...	3145.8572...	10.15.70.220	52.45.119.166	TLSv1.2	1405	Application Data
871...	3145.8572...	10.15.70.220	52.45.119.166	TLSv1.2	189	Application Data
871...	3145.9399...	52.45.119.166	10.15.70.220	TLSv1.2	1413	Application Data
871...	3157.1684...	10.15.70.220	104.248.182.131	TLSv1.2	109	Application Data
871...	3157.9838...	13.107.18.11	10.15.70.220	TLSv1.2	173	Application Data

[Window size scaling factor: 64]
[Checksum: 0x0660 (unverified)]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[SEQ/ACK analysis]
[Timestamps]
TCP payload (31 bytes)
Transport Layer Security
TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
Content Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 26
Encrypted Application Data: ac3650a2092ff1c9597258e612261954904c76a9fc3b9f1a...

0000 00 86 9c 04 b7 10 f4 5c 89 9a 80 a3 08 00 45 02E.
0010 00 53 00 00 40 00 00 06 ca 3c 0a 0f 46 dc 68 f8 .S..@. <..F.h.
0020 b6 83 e1 47 01 bb 56 10 9d 04 88 8c 83 66 80 18 ...G..V.f..
0030 08 00 06 60 00 00 01 01 08 0a 0c e2 cb b2 27 85
0040 e5 7b 17 03 03 00 1a ac 36 50 a2 09 2f f1 c9 59 .{.....6P../..Y
0050 72 58 e6 12 26 19 54 90 4c 76 a9 fc 3b 9f 1a b4 rX...&.T. LV...;
0060 0a

What is the Content-Type for a record containing “Application Data”?
Application Data (23)

What version constant is used in your trace, and which version of TLS does it represent?
TLS 1.2 (0x0303)
TLSv1.2

Does the Length cover the Record Layer header as well as payload, or only the payload?
Only the payload

Step3:

ssl

No.	Time	Source	Destination	Protocol	Length	Info
4	0.036328	10.15.70.220	172.217.164.100	TLSv1	299	Client Hello
6	0.080175	172.217.164.100	10.15.70.220	TLSv1.2	1440	Server Hello
7	0.080519	172.217.164.100	10.15.70.220	TLSv1.2	1261	Certificate, Server Key Exchange, Server Hello Done
9	0.087721	10.15.70.220	172.217.164.100	TLSv1.2	151	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10	0.113664	172.217.164.100	10.15.70.220	TLSv1.2	109	Change Cipher Spec, Encrypted Handshake Message
12	0.114052	10.15.70.220	172.217.164.100	TLSv1.2	111	Application Data
13	0.114120	10.15.70.220	172.217.164.100	TLSv1.2	114	Application Data
14	0.114145	10.15.70.220	172.217.164.100	TLSv1.2	100	Application Data
15	0.114193	10.15.70.220	172.217.164.100	TLSv1.2	127	Application Data
16	0.138929	172.217.164.100	10.15.70.220	TLSv1.2	127	Application Data
17	0.138935	172.217.164.100	10.15.70.220	TLSv1.2	96	Application Data
20	0.139197	10.15.70.220	172.217.164.100	TLSv1.2	96	Application Data
23	0.207438	172.217.164.100	10.15.70.220	TLSv1.2	722	Application Data

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

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 228

▼ Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 224

Version: TLS 1.2 (0x0303)

▼ Random: a07e182535a6259c8d62ac57ba6bcd8b4b9c078fa2aeaf4c...

GMT Unix Time: Apr 29, 2055 06:31:17.000000000 PDT

Random Bytes: 35a6259c8d62ac57ba6bcd8b4b9c078fa2aeaf4cd7fab5de...

Session ID Length: 0

Cipher Suites Length: 92

► Cipher Suites (46 suites)

```

0040 52 9a 16 03 01 00 e4 01 00 00 e0 03 03 a0 7e 18 R.....~
0050 25 35 a6 25 9c 8d 62 ac 57 ba 6b cd 8b 4b 9c 07 %5%..b.W.k.K.
0060 8f a2 ae af 4c d7 fa b5 de cd 3a 88 ea 00 00 5c ...L...:...\
0070 c0 30 c0 2c c0 28 c0 24 c0 14 c0 0a 00 9f 00 6b .0.,(. $ .....k
0080 00 39 cc a9 cc a8 cc aa ff 85 00 c4 00 88 00 81 .9.....
0090 00 9d 00 3d 00 35 00 c0 00 84 c0 2f c0 2b c0 27 ...=5.../+.
00a0 c0 23 c0 13 c0 09 00 9e 00 67 00 33 00 be 00 45 .#.....g.3...E
00b0 00 9c 00 3c 00 2f 00 ba 00 41 c0 11 c0 07 00 05 ...</...A.....
00c0 00 04 c0 12 c0 08 00 16 00 0a 00 ff 01 00 00 5b .....

```

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

Packets: 60 - Displayed: 29 (48.3%)

Profile: Default

ssl

No.	Time	Source	Destination	Protocol	Length	Info
4	0.036328	10.15.70.220	172.217.164.100	TLSv1	299	Client Hello
6	0.080175	172.217.164.100	10.15.70.220	TLSv1.2	1440	Server Hello
7	0.080519	172.217.164.100	10.15.70.220	TLSv1.2	1261	Certificate, Server Key Exchange, Server Hello Done
9	0.087721	10.15.70.220	172.217.164.100	TLSv1.2	151	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10	0.113664	172.217.164.100	10.15.70.220	TLSv1.2	109	Change Cipher Spec, Encrypted Handshake Message
12	0.114052	10.15.70.220	172.217.164.100	TLSv1.2	111	Application Data
13	0.114120	10.15.70.220	172.217.164.100	TLSv1.2	114	Application Data
14	0.114145	10.15.70.220	172.217.164.100	TLSv1.2	100	Application Data
15	0.114193	10.15.70.220	172.217.164.100	TLSv1.2	127	Application Data
16	0.138929	172.217.164.100	10.15.70.220	TLSv1.2	127	Application Data
17	0.138935	172.217.164.100	10.15.70.220	TLSv1.2	96	Application Data
20	0.139197	10.15.70.220	172.217.164.100	TLSv1.2	96	Application Data
23	0.207438	172.217.164.100	10.15.70.220	TLSv1.2	722	Application Data

▼ Transport Layer Security

▼ TLSv1.2 Record Layer: Handshake Protocol: Server Hello

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 96

▼ Handshake Protocol: Server Hello

Handshake Type: Server Hello (2)

Length: 92

Version: TLS 1.2 (0x0303)

▼ Random: 5dc3716bf7fee9bc88e49cf68f976a40d73933843bab73c9...

GMT Unix Time: Nov 6, 2019 17:20:43.000000000 PST

Random Bytes: f7fee9bc88e49cf68f976a40d73933843bab73c9444f574e...

Session ID Length: 32

Session ID: 96513583e1a25e1b50bc0499fb52de15e96af3f9e7a38e7d...

```

0040 79 69 16 03 03 00 60 02 00 00 5c 03 03 5d c3 71 y1.....\..].q
0050 6b f7 fe e9 bc 88 e4 9c f6 8f 97 6a 40 d7 39 33 k.....j@.93
0060 84 3b ab 73 c9 44 4f 57 4e 47 52 44 01 20 96 51 .;s.DOW NGRD. .Q
0070 35 83 e1 a2 5e 1b 50 bc 04 99 fb 52 de 15 e9 6a 5.....^P.....R...j
0080 f3 f9 e7 a3 8e 7d 1c 70 39 9f 04 93 80 99 cc a9 .....}p 9.....
0090 00 00 14 ff 01 00 01 00 00 0b 00 02 01 00 00 10 .....
00a0 00 05 00 03 02 68 32 16 03 03 09 1e 0b 00 09 1a .....h2.....
00b0 00 09 17 00 04 c3 30 82 04 bf 30 82 03 a7 a0 03 .....0.....
00c0 02 01 02 02 11 00 ed 7f 80 a1 37 93 02 56 08 00 .....7...V...

```

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.

Client: 32 bytes.

Server: 32 bytes.

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 ID: 32 bytes.

3. What Cipher method 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: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)

4. 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.

Server

5. At the Record Layer, what Content-Type values are used to indicate each of these messages? Say whether the values are the same or different than that used for the Hello and Certificate messages. Note that this question is asking you to look at the Record Layer and not an inner Handshake Protocol.

Content Type: Handshake (22)

22

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

Both

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

▼ Transport Layer Security

▼ TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
Content Type: Change Cipher Spec (20)
Version: TLS 1.2 (0x0303)
Length: 1

Change Cipher Spec Message

▼ TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 32
Handshake Protocol: Encrypted Handshake Message

0000	f4 5c 89 9a 80 a3 00 86 9c 04 b7 10 08 00 45 00	·\····· ·····E·
0010	00 5f 49 4e 00 00 7b 06 54 22 ac d9 a4 64 0a 0f	·_IN··{· T"···d··
0020	46 dc 01 bb e3 63 c9 d2 b1 39 f7 20 4f 81 80 18	F····c·· ·9· 0··
0030	00 f0 47 10 00 00 01 01 08 0a a4 f1 52 f1 0c eb	··G····· ····R··
0040	79 9a 14 03 03 00 01 01 16 03 03 00 20 25 81 7a	y····· ····%·z
0050	45 0a 7b 1b 8f b9 65 fe c2 83 25 6c fd 52 a7 0c	E·{···e· ··%l·R··
0060	10 8f fe 97 13 d2 d1 ec e7 c8 14 a8 61	······ ····a

Change Cipher Spec Message 01

8. At the Record Layer, what Content-Type value is used to signal an alert?

▼ Transport Layer Security		
▼ TLSv1.2 Record Layer: Encrypted Alert		
Content Type: Alert (21)		
Version: TLS 1.2 (0x0303)		
Length: 18		
Alert Message: Encrypted Alert		
0000	00 86 9c 04 b7 10 f4 5c 89 9a 80 a3 08 00 45 00\E.
0010	00 4b 00 00 40 00 40 06 98 84 0a 0f 46 dc ac d9	·K··@·@·F·
0020	a4 64 e3 63 01 bb f7 20 50 5b c9 d2 e3 31 80 18	·d·c· · · P[· · ·1·
0030	07 ff c5 c9 00 00 01 01 08 0a 0c eb 7a 14 a4 f1z·
0040	53 52 15 03 03 00 12 7d 6e 3d 3e 51 e2 76 be ca	SR· · · · } n=>Q·v·
0050	33 25 e2 21 fd a4 93 8c 8f	3%·!· · · ·

Alert (21)

9. Tell us whether the contents of the alert are encrypted or sent in the clear? To check this, see whether you can read the contents of the alert to see what kind of alert has been sent.

Encrypted

=====

Grades:

95/100

Comments:

Step3 Overall Handshake(-5): missing drawing of handshake timeline