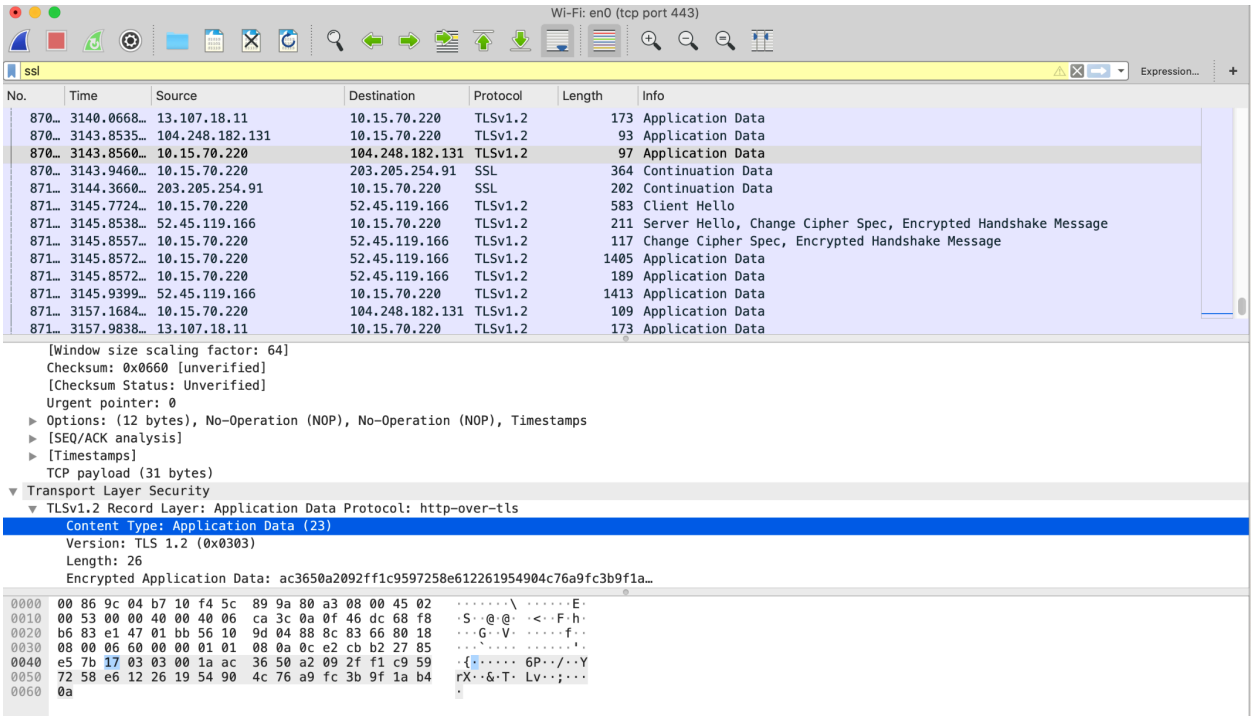
Step2:

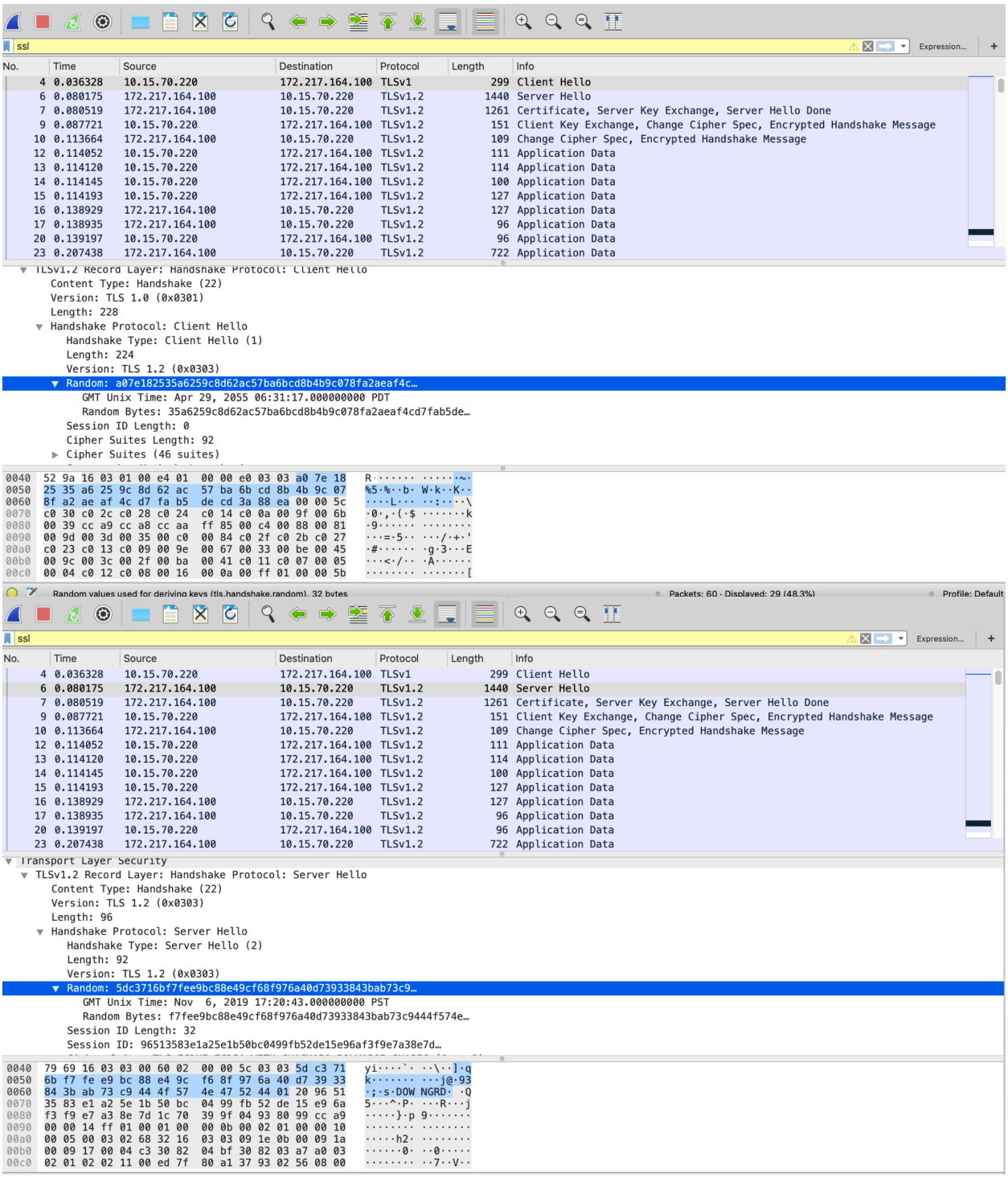


What is the Content-Type for a record containing “Application Data”?
Application Data (23)

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:



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 resump- tion 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.
Senssion ID: 32 bytes.

3. What Cipher method is chosen by the Server? Give its name and value. The Client will list the dif- ferent 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 mes- sages. Note that this question is asking you to look at the Record Layer and not an inner Hand- shake Protocol.

```
Content Type: Handshake (22)
```

22

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

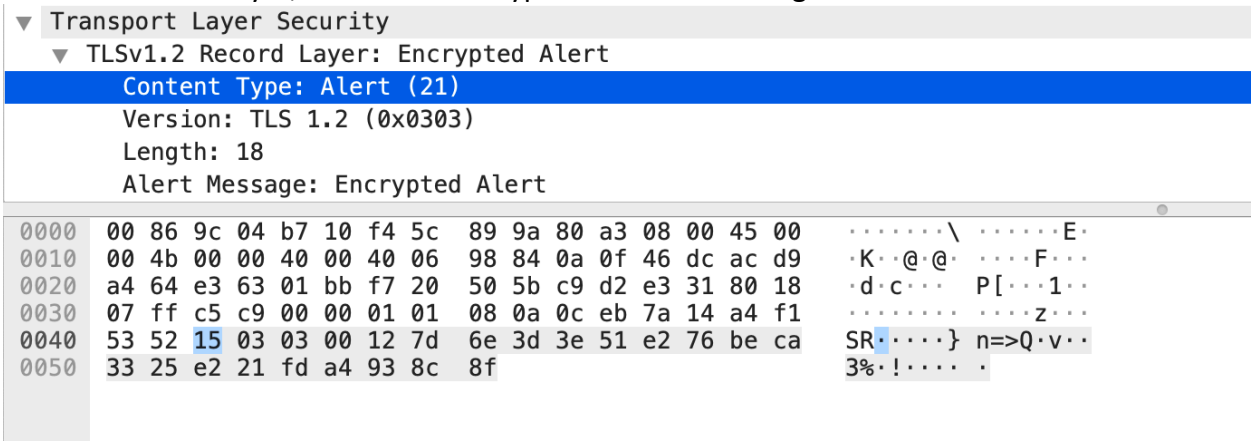
7. What are the contents carried inside the Change Cipher Spec message? Look past the Content-Type and other headers to see the message itself.

```
▼ 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· O···
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?



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