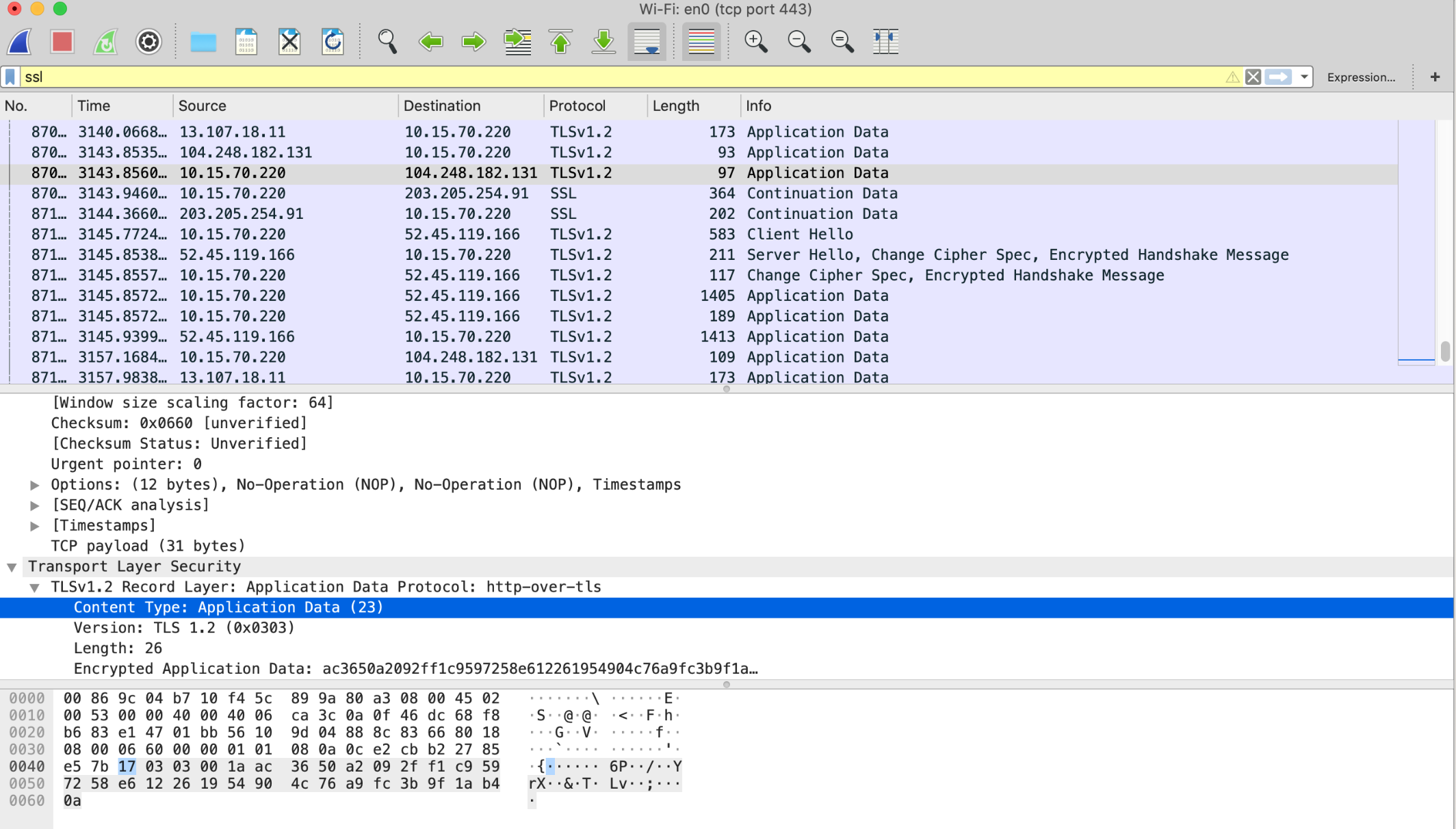
Step2:



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?

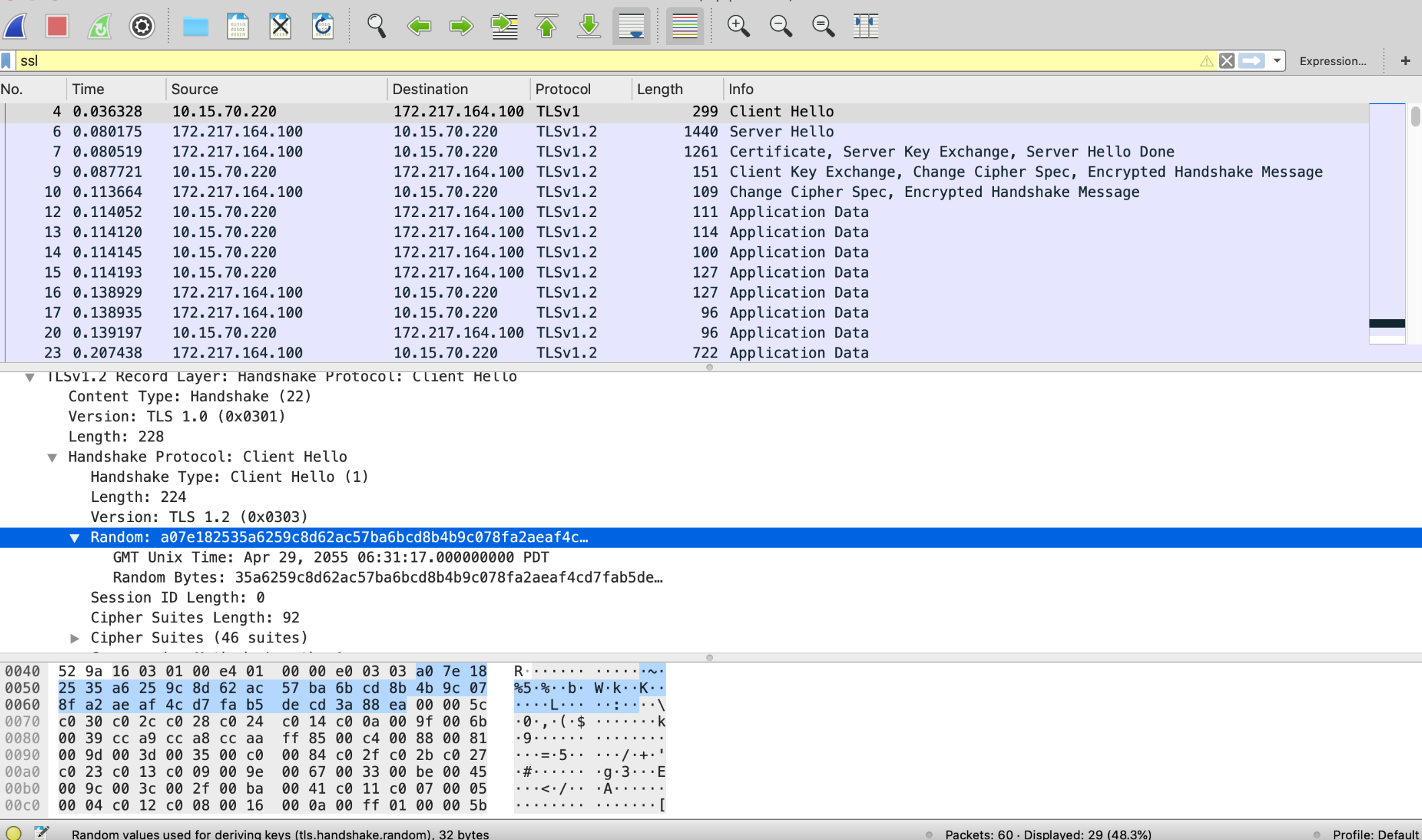
TLS 1.2 (0x0303)

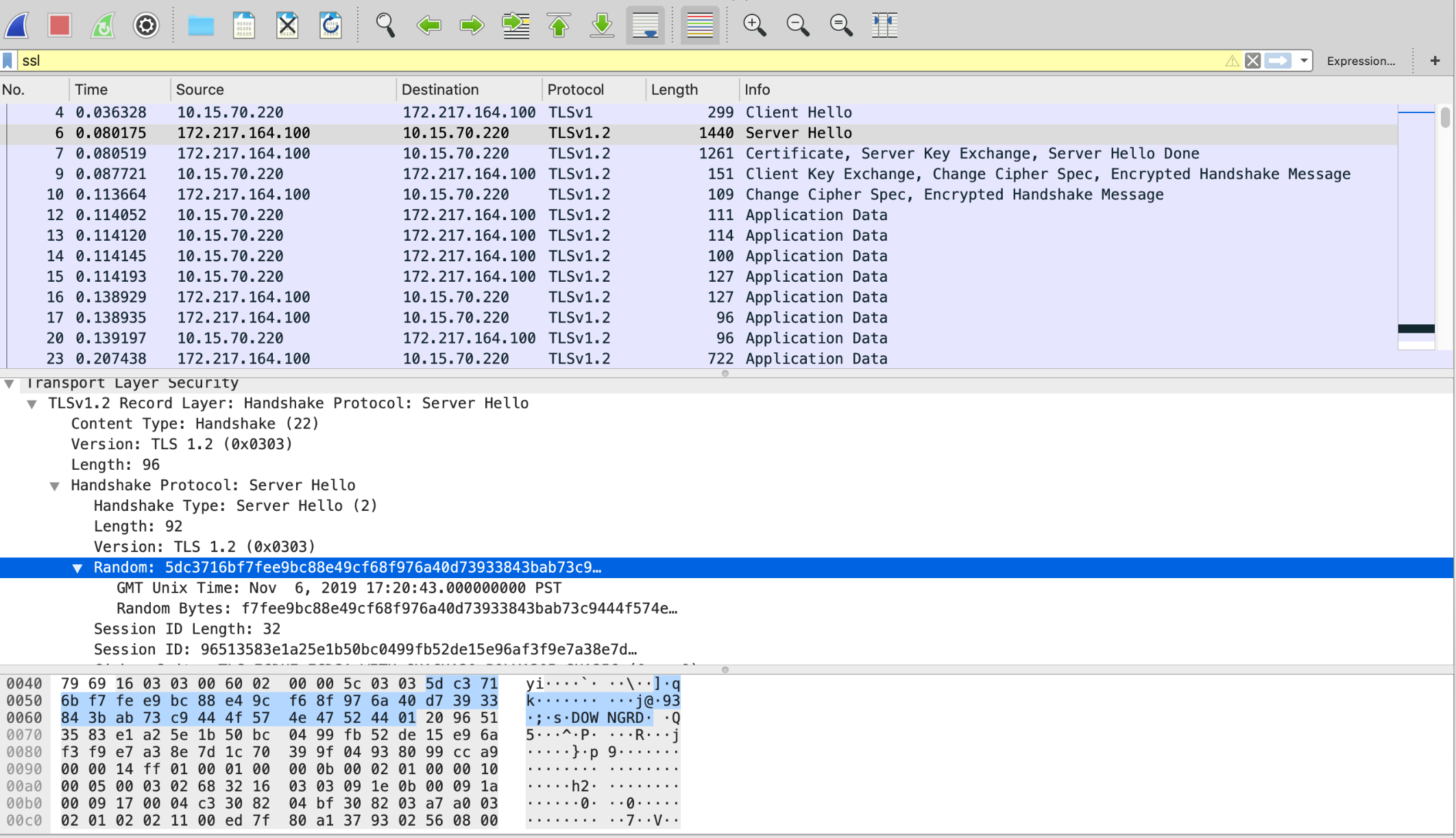
TLSv1.2

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.

﻿﻿

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.

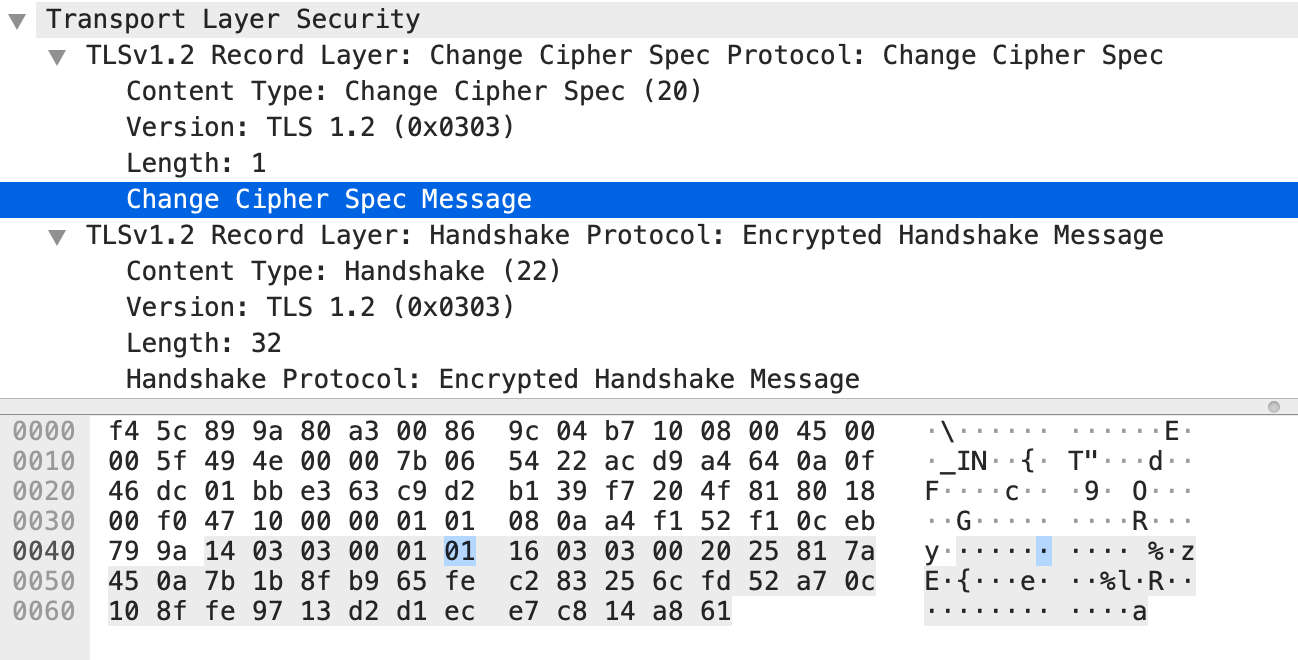


22

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

Both

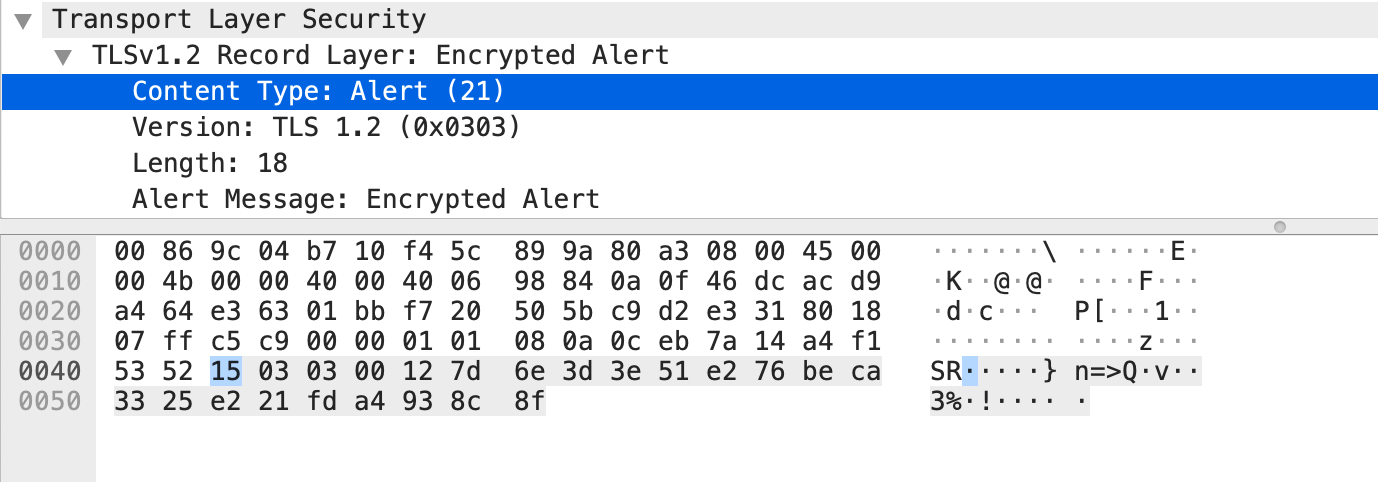
7. What are the contents carried inside the Change Cipher Spec message? Look past the Content-Type and other headers to see the message itself.



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