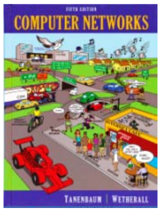
Solutions – SSL/TLS



The solutions below are based on our capture and use of tools. Your answers will differ in the details if they are based on your own capture and use of tools in a different network setting. Nonetheless, we expect our solutions to help you understand whether your answers are correct.

Step 2: Inspect the Trace

Answers to the questions:

1. A Content-Type value of 23 indicates “Application Data”.
2. For our trace, the version constant 0x0301 represents TLS 1.0
3. The Length covers only the payload of the Record Layer.

Step 3: The SSL Handshake

Overall Handshake

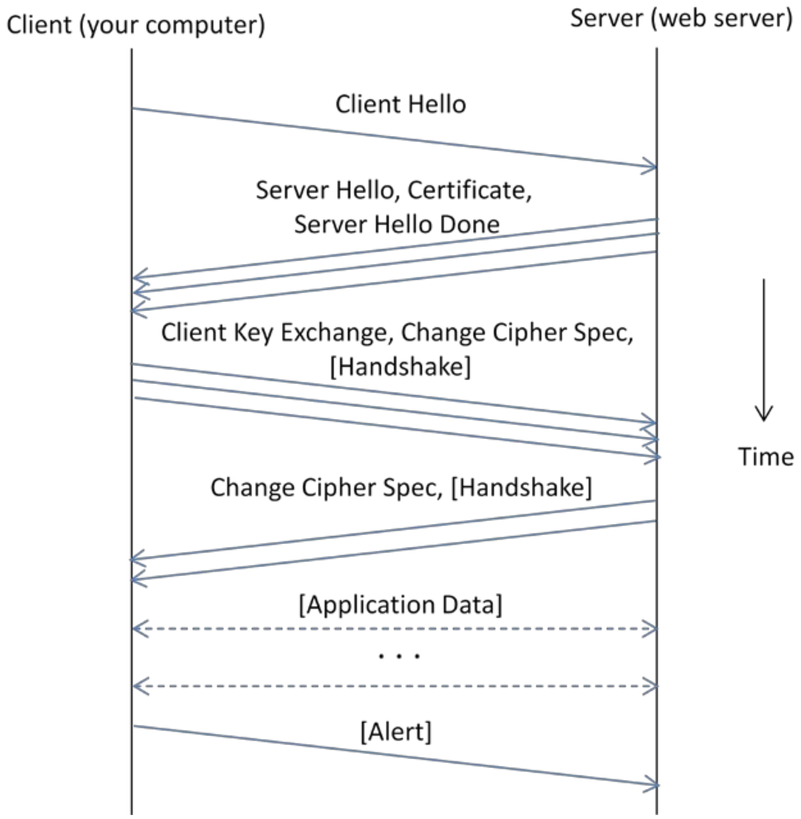


Figure 1: Timeline of the SSL messages in the connection

Notes:

- Your figure may vary due to slight differences in SSL/TLS versions, as well as differences in server behavior, but the overall construction should be similar.
- Messages in parenthesis "[]" are encrypted so we cannot see their contents. Thus we cannot observe the kind of the last Handshake message or the kind of Alert message.
- See how this figure corresponds to Fig. 8-50 of your text. In that figure, we are able to look within encrypted messages, plus different names are used for some of the messages.

Answers to the questions:

Hello Message

1. The random data is 28 bytes long for both client and server. (It does not include the timestamp, which is not random.)
2. The session ID sent by the server is 32 bytes long.
3. For our trace, the cipher method is TLS_RSA_WITH_RC4_128_SHA (0x0005). Your answer will depend on the server and your installation and use of `curl` / `wget`. For example, on our Client Hello we can see 32 cipher suites that are supported. Any one might be chosen by the server.

Certificate Message

4. The server sends a certificate to the client, since it is the browser that wants to verify the identity of the server. It is also possible for the server to request certificates from the client, but this behavior is not normally used by web applications.

Client Key Exchange and Change Cipher Messages

5. The Client Key Exchange has a Content-Type of 22, indicating the Handshake protocol. This is the same as for the Hello and Certificate messages, as they are part of the Handshake protocol. The Change Cipher Spec message has a Content-Type of 20, indicating the Change Cipher Spec protocol. That is, this message is part of its own protocol and not the Handshake protocol.
6. Both sides send the Change Cipher Spec message immediately before they switch to sending encrypted contents. The message is an indication to the other side.
7. The contents of the Change Cipher Spec message are simply the value 1 as a single byte. Actually, it is the value "1" encrypted under the current scheme, which uses no encryption for the handshake so that we can see it.

Alert Message

8. The Content-Type value is 21 for Alert. This is a new protocol, different from the Handshake, Change Cipher Spec and Application Data values that we have already seen.
9. The alert is encrypted; we cannot see its contents. Wireshark also describes the message as an "Encrypted Alert". Presumably is it a "close_notify" alert to signal that the connection is ending, but we cannot be certain.

[END]