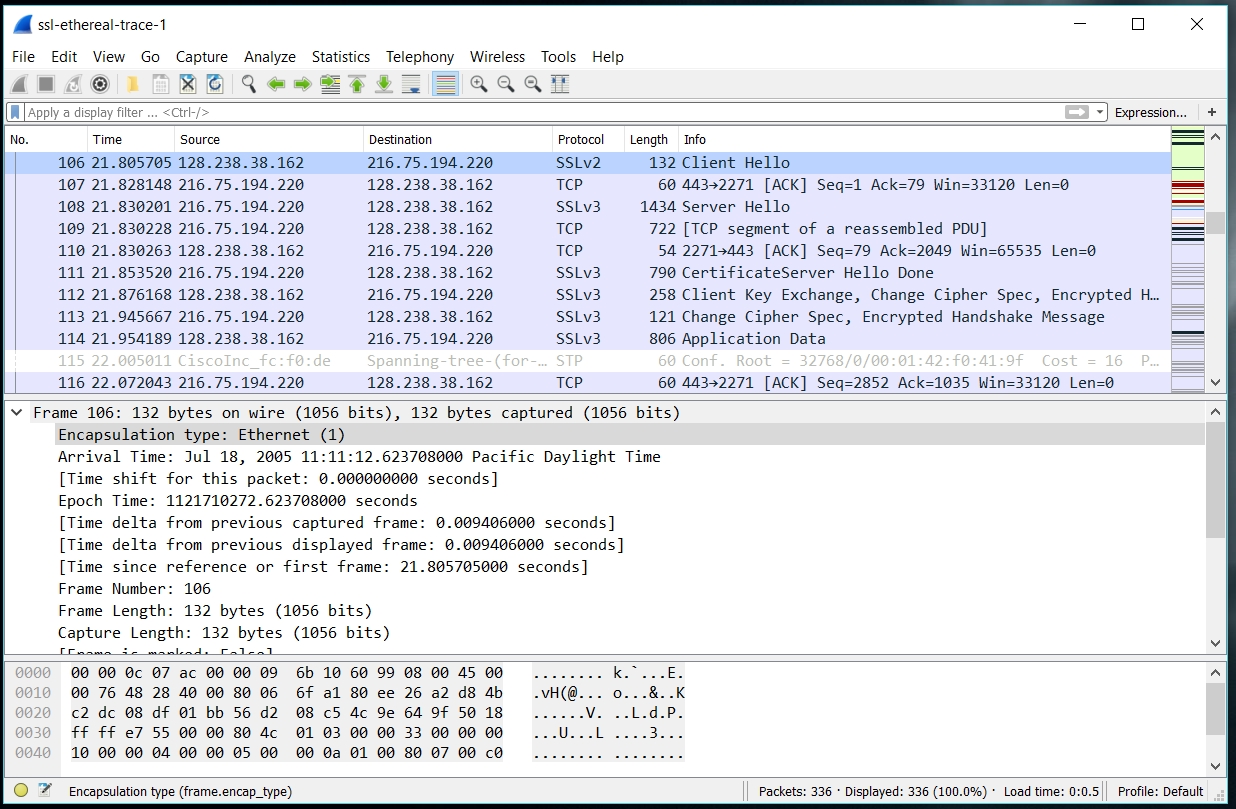
Broc Nickodemus

Lab 8

1. For each of the first 8 Ethernet frames, specify the source of the frame (client or server), determine the number of SSL records that are included in the frame, and list the SSL record types that are included in the frame. Draw a timing diagram between client and server, with one arrow for each SSL record.



|  |  |  |  |
| --- | --- | --- | --- |
| Frame | Source | Destination | Type |
| 106 | 128.238.38.162 | 216.75.194.220 | Client Hello |
| 108 | 216.75.194.220 | 128.238.38.162 | Server Hello |
| 111 | 216.75.194.220 | 128.238.38.162 | Hello Done |
| 112 | 128.238.38.162 | 216.75.194.220 | Client Key Exchange |
| 113 | 216.75.194.220 | 128.238.38.162 | Change Cipher |
| 114 | 128.238.38.162 | 216.75.194.220 | App Data |
| 122 | 216.75.194.220 | 128.238.38.162 | App Data |
| 127 | 216.75.194.220 | 128.238.38.162 | App Data |

Client 🡺 Client Hello 🡺 Server

Server 🡺 Server Hello 🡺 Client

Server 🡺 Hello Done 🡺 Client

Client 🡺 Client Key Exchange 🡺 Server

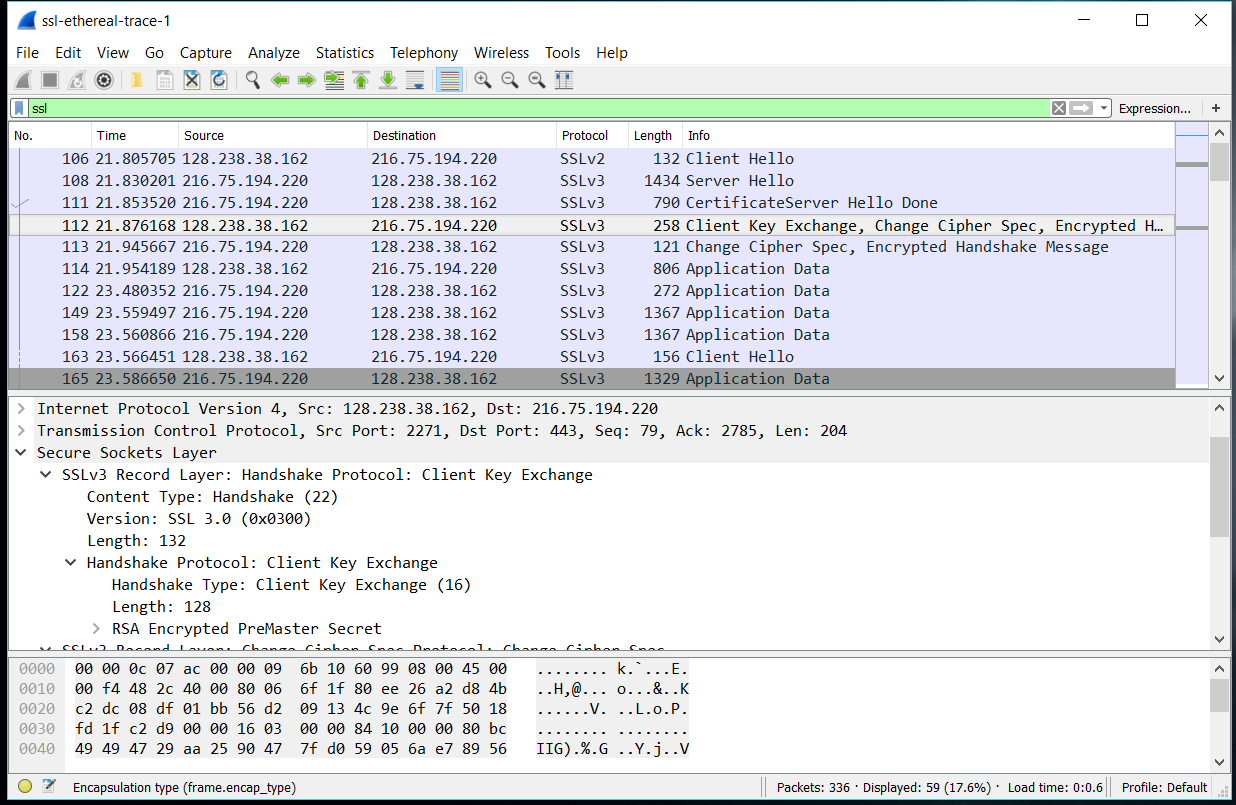
Server 🡺 Change Cipher 🡺 Client

Client 🡺 App Data 🡺 Server

Server 🡺 App Data 🡺 Client

Server 🡺 App Data 🡺 Client

2. Each of the SSL records begins with the same three fields (with possibly different values). One of these fields is “content type” and has length of one byte. List all three fields and their lengths.



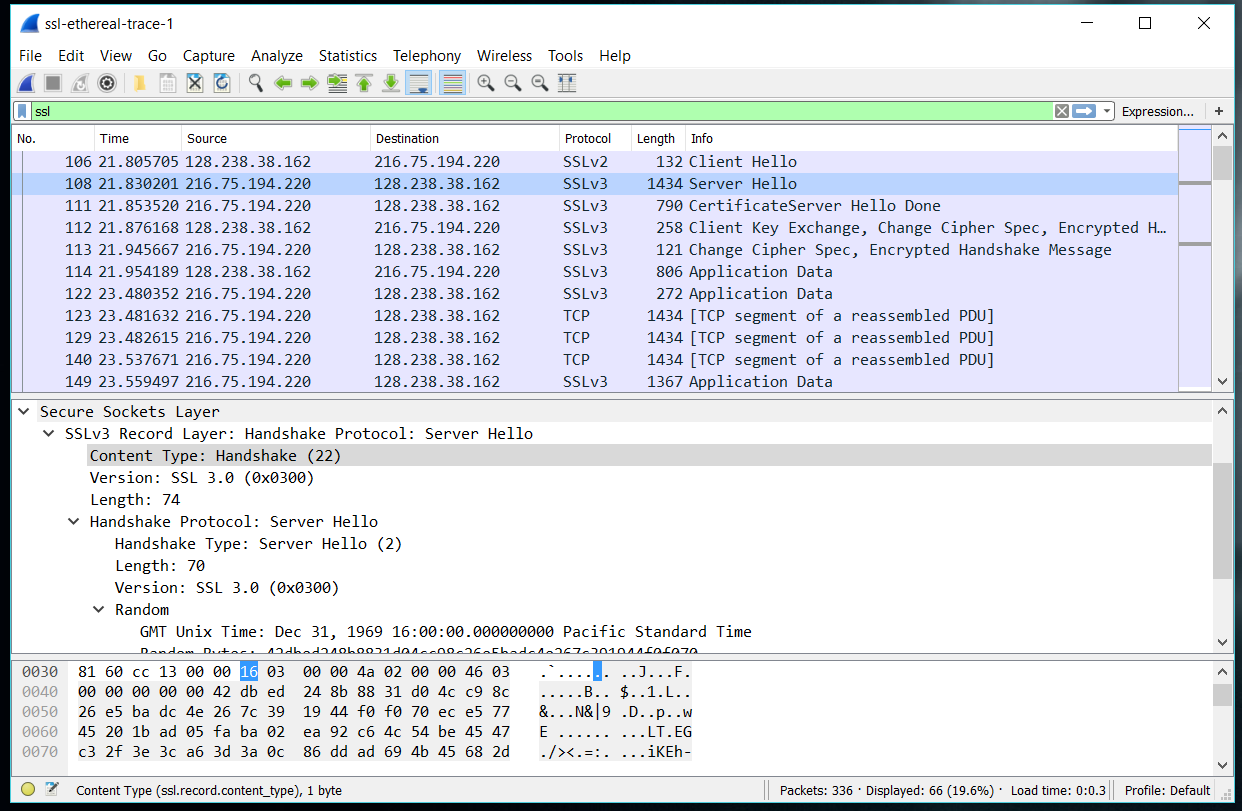
Content Type = 1 byte

Version = 2 bytes

Length = 2 bytes

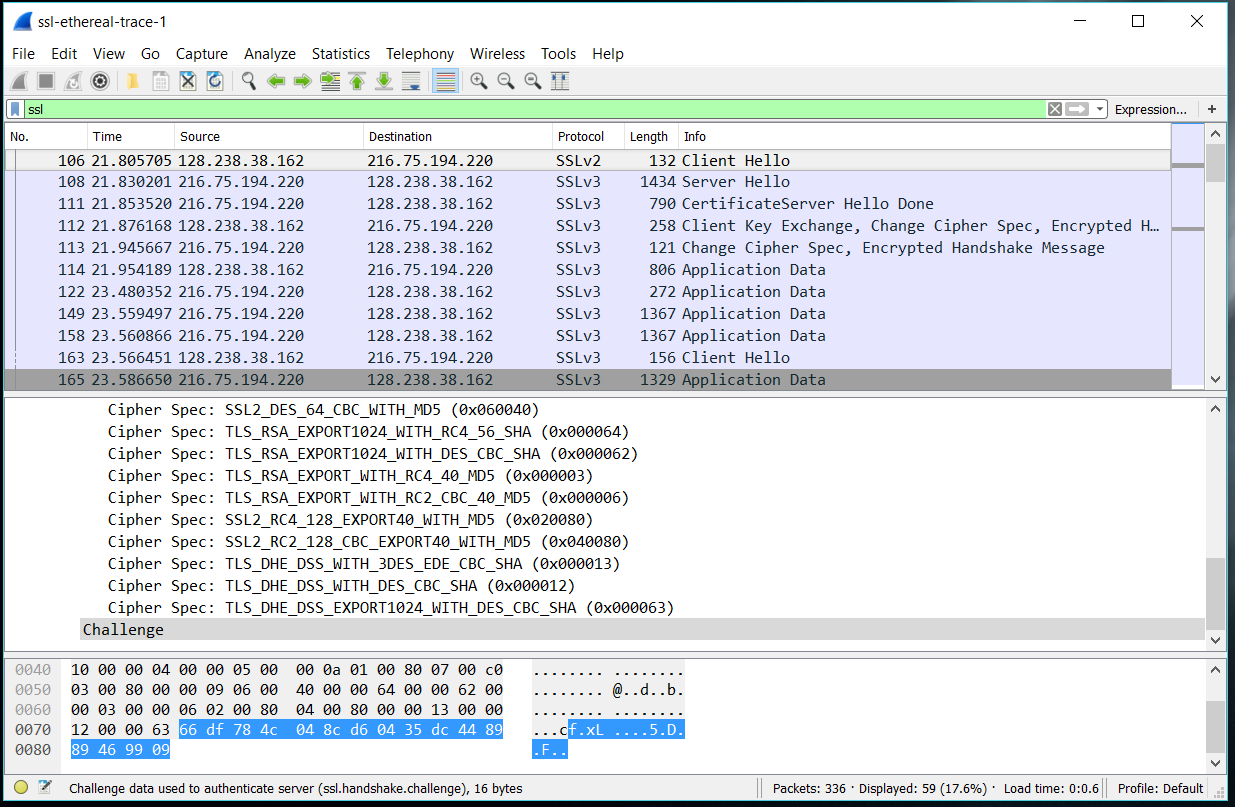
ClientHello Record:

3. Expand the ClientHello record. (If your trace contains multiple ClientHello records, expand the frame that contains the first one.) What is the value of the content type?



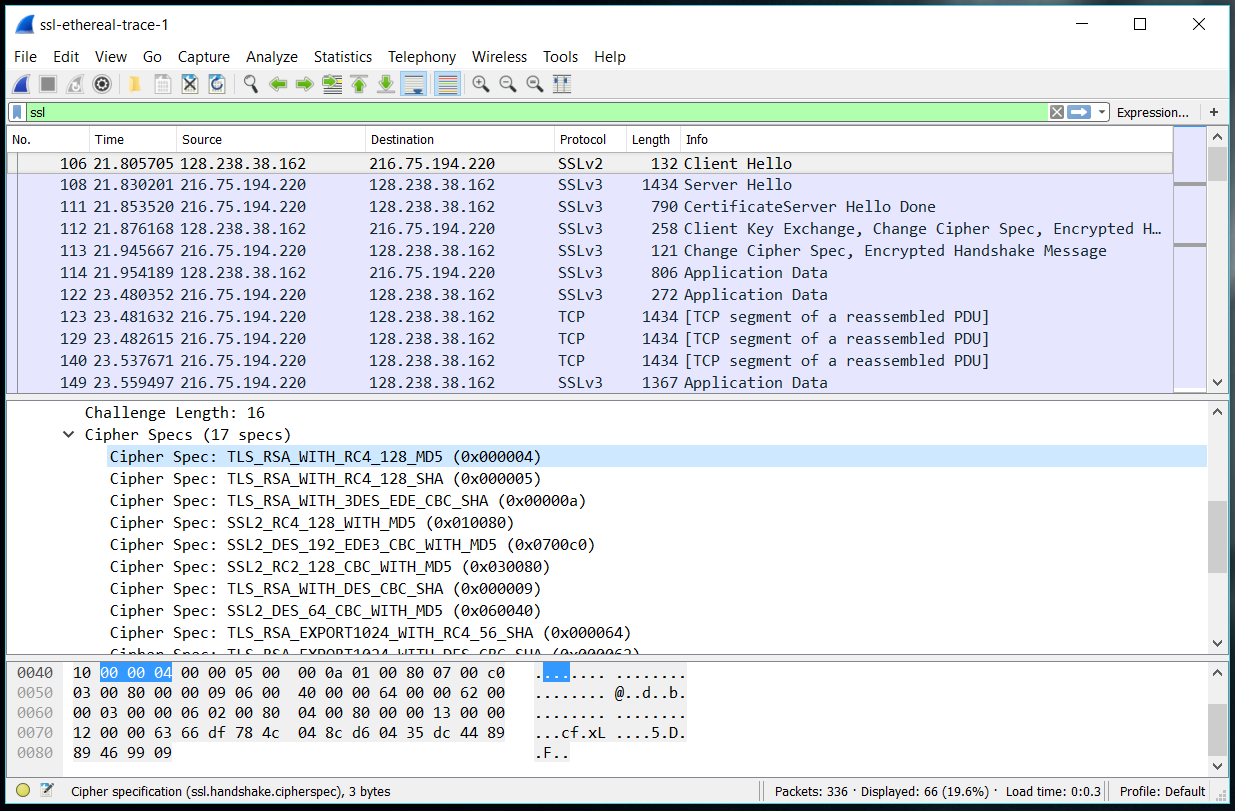
The content type is 22

4. Does the ClientHello record contain a nonce (also known as a “challenge”)? If so, what is the value of the challenge in hexadecimal notation?



Yes, it contains 66 df 78 4c 04 8c d6 04 35 dc 44 89 89 46 99 09

5. Does the ClientHello record advertise the cyber suites it supports? If so, in the first listed suite, what are the public-key algorithm, the symmetric-key algorithm, and the hash algorithm?

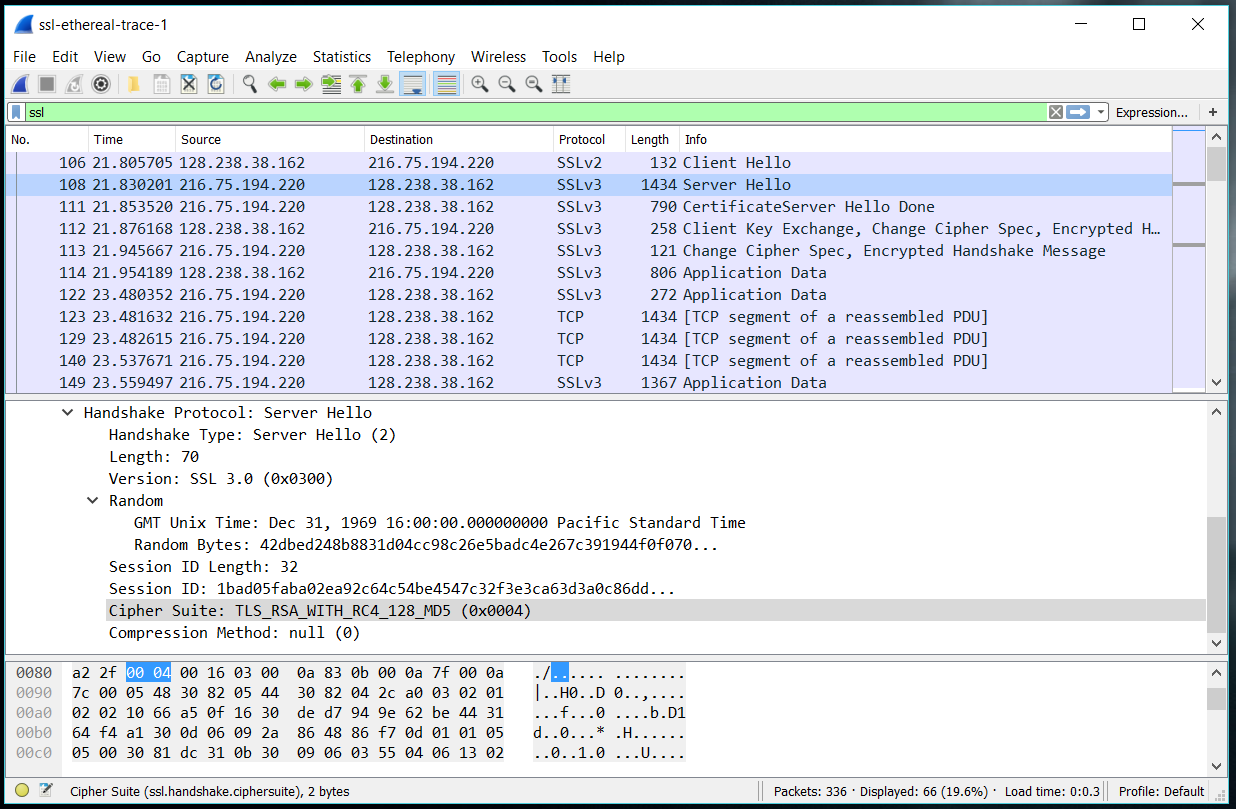


Yes, the first suite uses RSA for its public key, RC4 for its symmetric key, and MD5 for its hash

ServerHello Record:

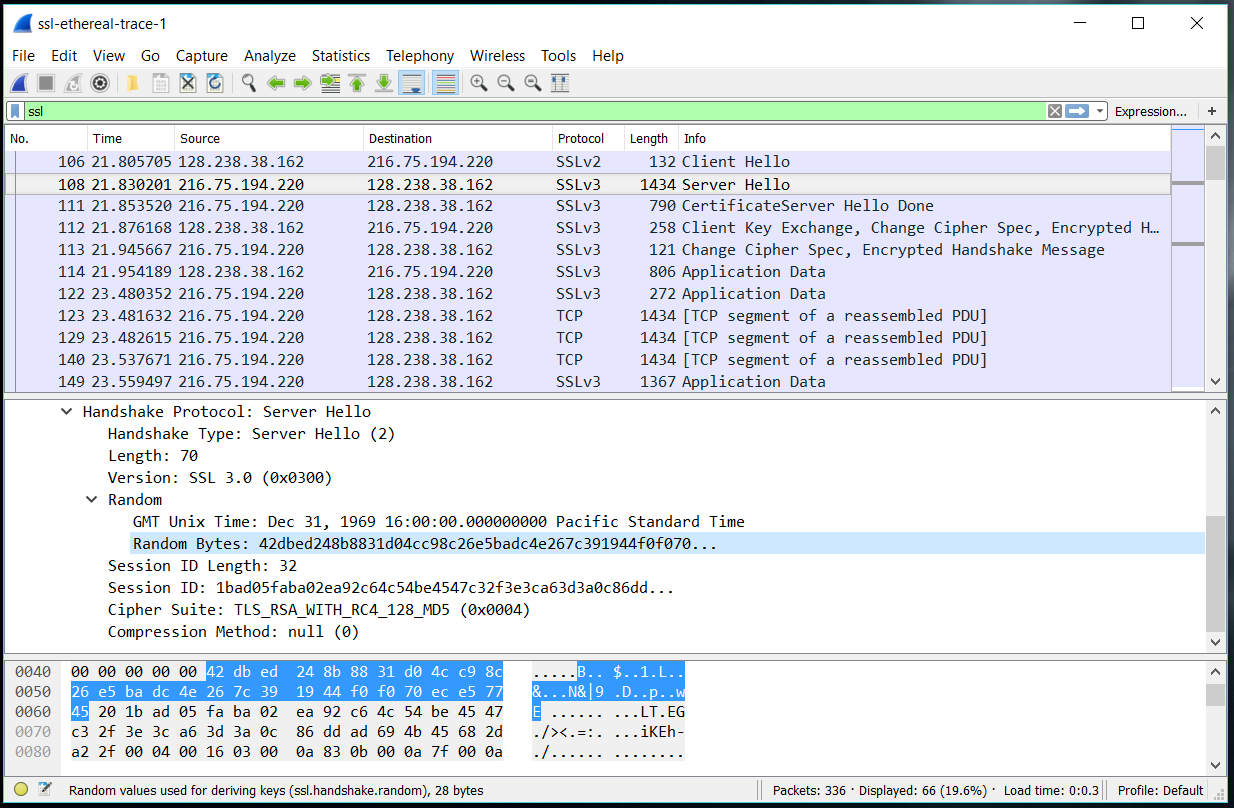
6. Locate the ServerHello SSL record. Does this record specify a chosen cipher suite? What are

the algorithms in the chosen cipher suite?



It is the same as the Client Hello and uses RSA for its public key, RC4 for its symmetric key, and MD5 for its hash.

7. Does this record include a nonce? If so, how long is it? What is the purpose of the client and server nonces in SSL?



Yes, it generated random bytes.

8. Does this record include a session ID? What is the purpose of the session ID?

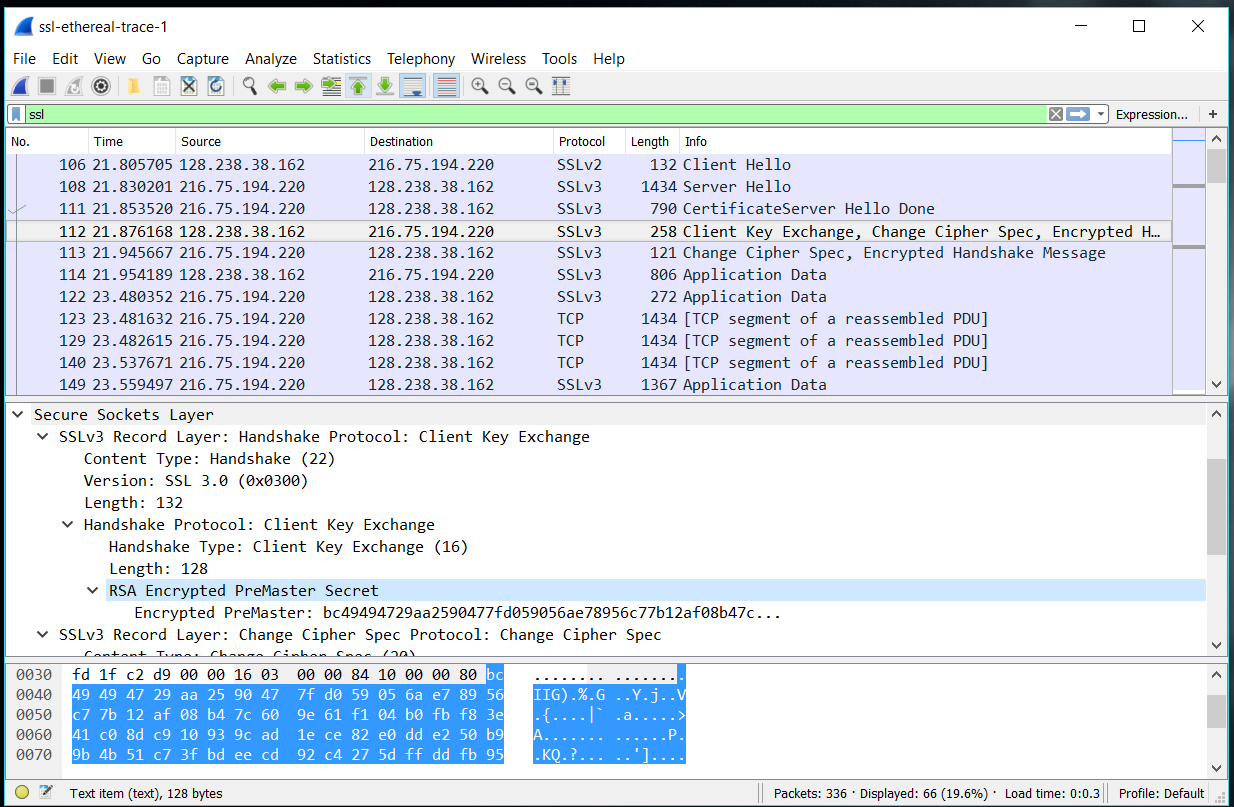
Yes, the client may come back to the session at a later point in time.

9. Does this record contain a certificate, or is the certificate included in a separate record. Does the certificate fit into a single Ethernet frame?

I could not find a certificate so it must be included in a separate record. Yes, it fits onto a single Ethernet frame.

Client Key Exchange Record:

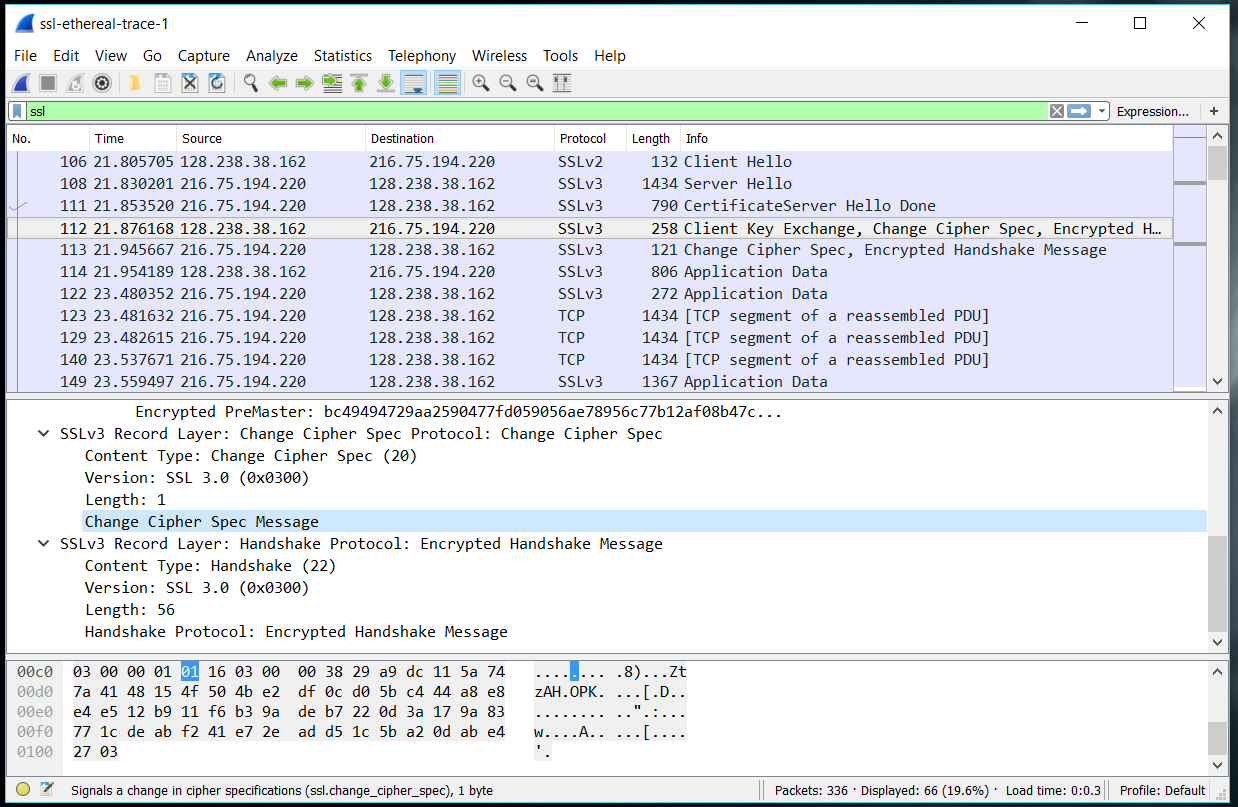
10. Locate the client key exchange record. Does this record contain a pre-master secret? What is this secret used for? Is the secret encrypted? If so, how? How long is the encrypted secret?



Yes, it is used to create the master secret that makes the session key. The secret is encrypted and its length is 128 bytes.

Change Cipher Spec Record (sent by client) and Encrypted Handshake Record:

11. What is the purpose of the Change Cipher Spec record? How many bytes is the record in your trace?

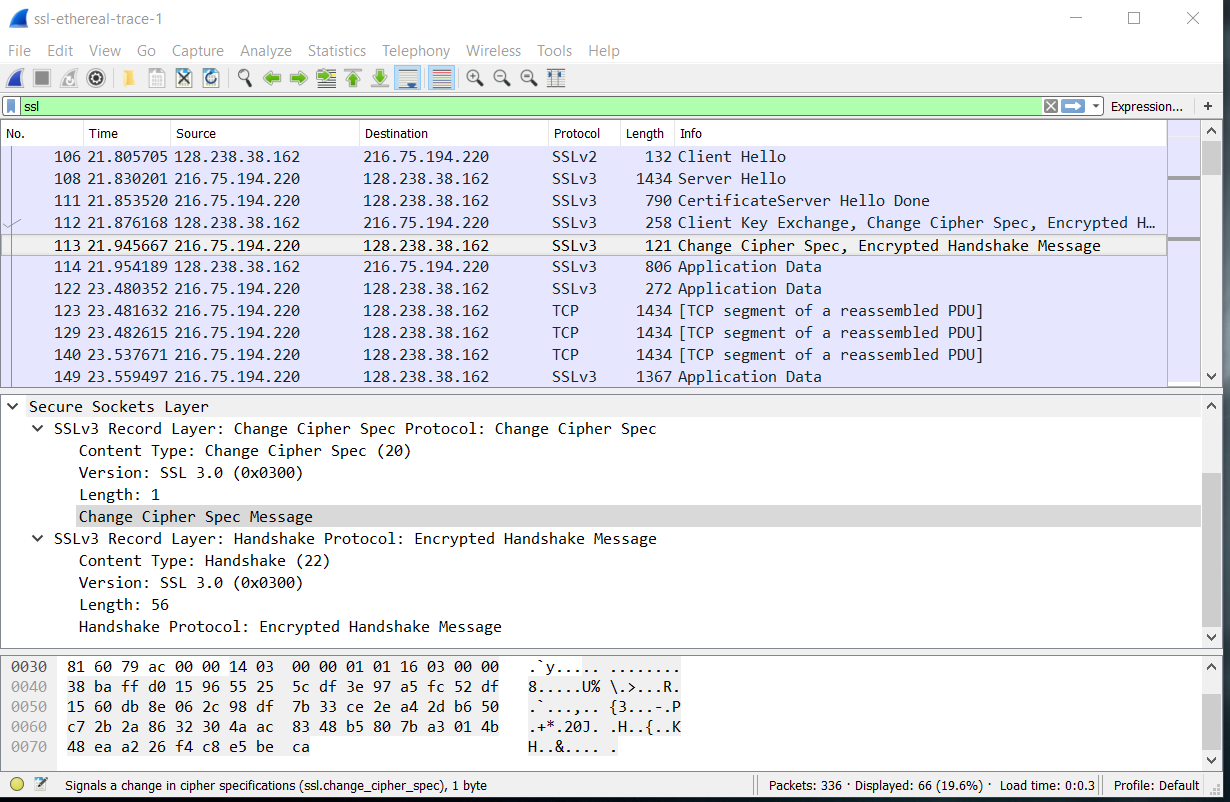


It is used to indicate that the next message is encrypted. It is 1 byte.

12. In the encrypted handshake record, what is being encrypted? How?

All handshake messages are encrypted and the mac addresses of the computers are also encrypted. Wireshark does this by looking for the ssl records and those handshakes. The encryption then occurs after the change cipher spec message.

13. Does the server also send a change cipher record and an encrypted handshake record to the client? How are those records different from those sent by the client?



Yes, the server handshake did contain all the messages sent from the server. Those records are different because they were not sent from the client.

Application Data:

14. How is the application data being encrypted? Do the records containing application data include a MAC? Does Wireshark distinguish between the encrypted application data and the MAC?

The symmetric encryption algorithm (RC4) encrypts the application data. Yes, they contain a mac but Wireshark did not distinguish between the encrypted data and the mac.

15. Comment on and explain anything else that you found interesting in the trace.

I thought this was a boring trace.