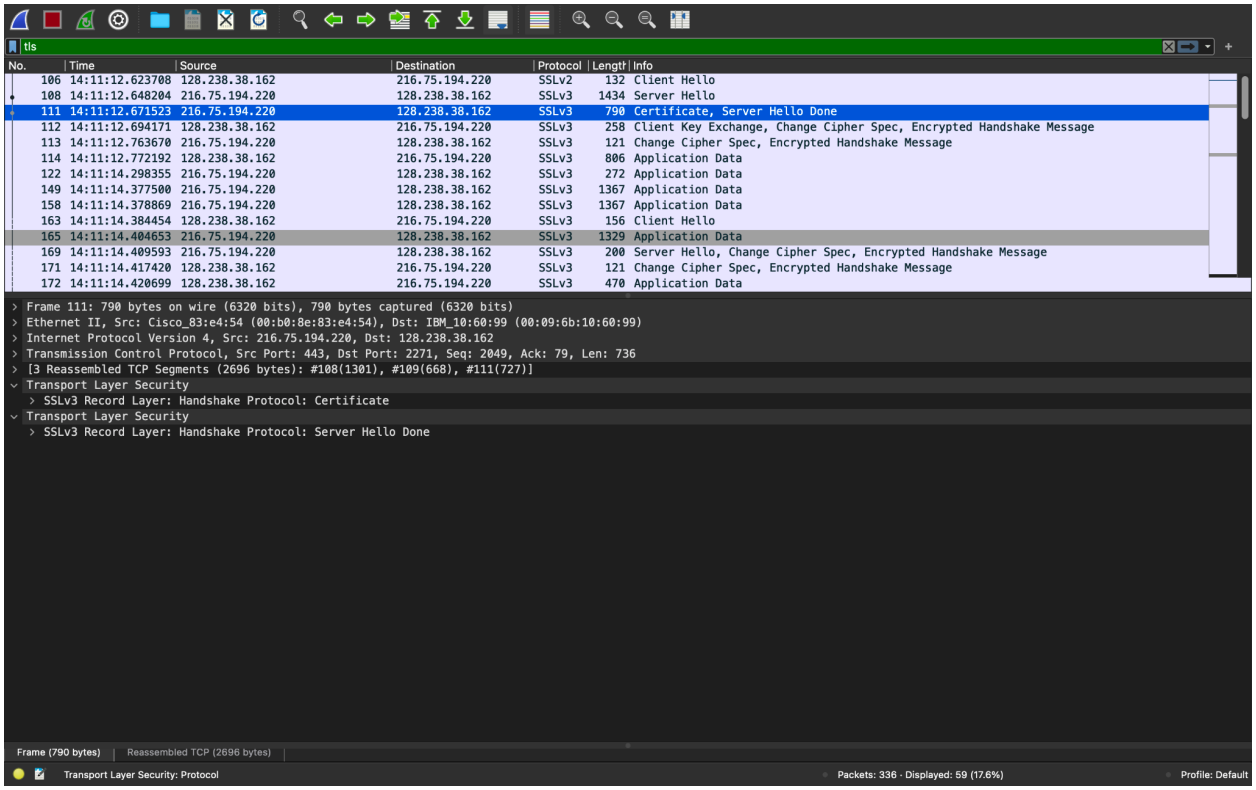
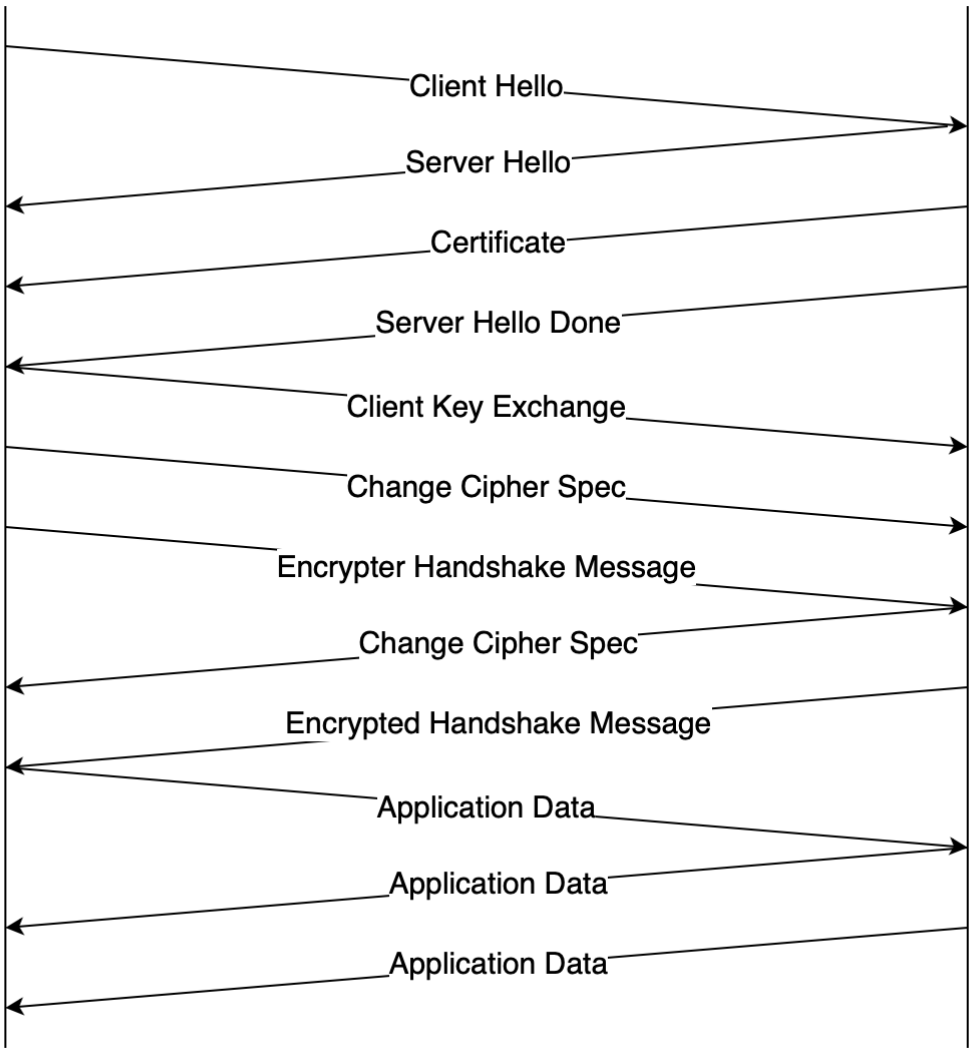
Foundation of Computer Networks - Wireshark Project
Bhavin Oza (bo2115)



1).

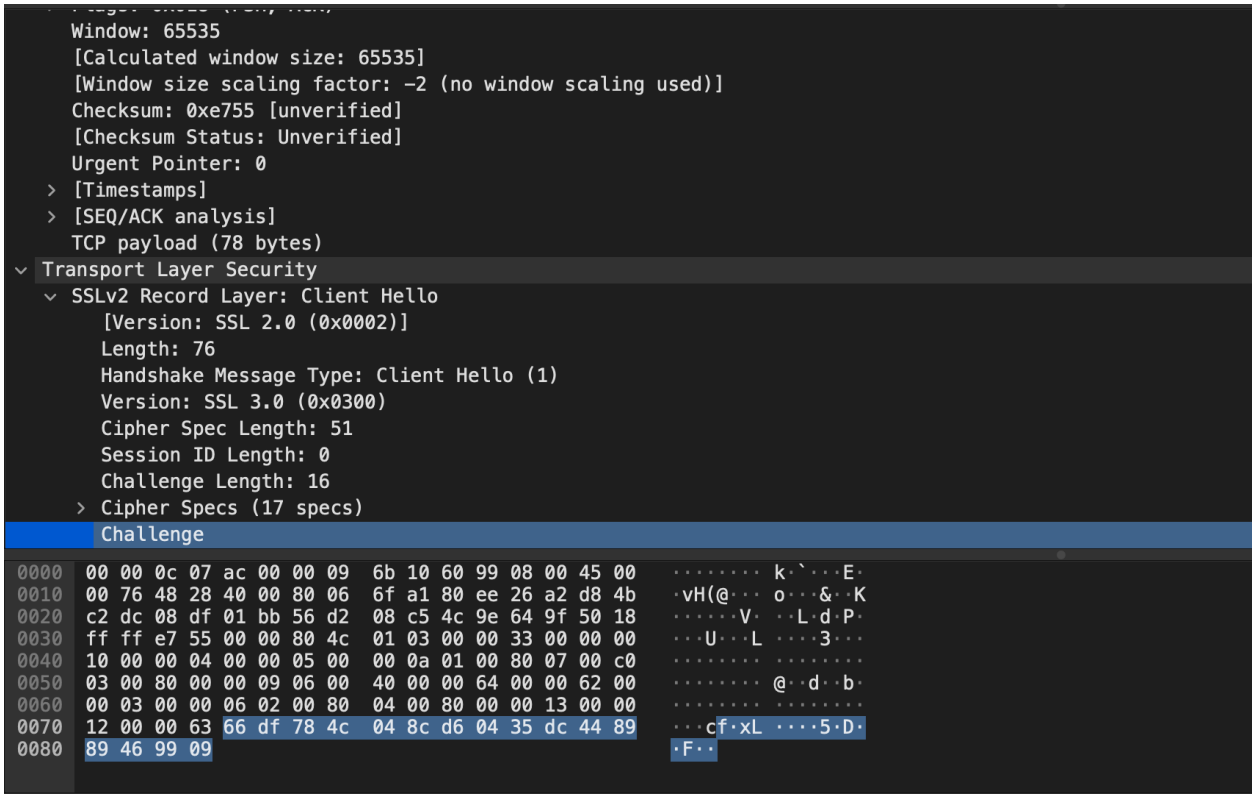
Frame	Source	SSL Count	SSL Type
106	128.238.38.162	1	Client Hello
108	216.75.194.220	1	Server Hello
111	216.75.194.220	2	Certificate, Server Hello Done
112	128.238.38.162	3	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
113	216.75.194.220	2	Change Cipher Spec, Encrypted Handshake Message
114	128.238.38.162	1	Application Data
122	216.75.194.220	1	Application Data
149	216.75.194.220	1	Application Data

Foundation of Computer Networks - Wireshark Project
Bhavin Oza (bo2115)



2). Content Type is 1 byte
Version is 2 bytes
Length is 2 bytes

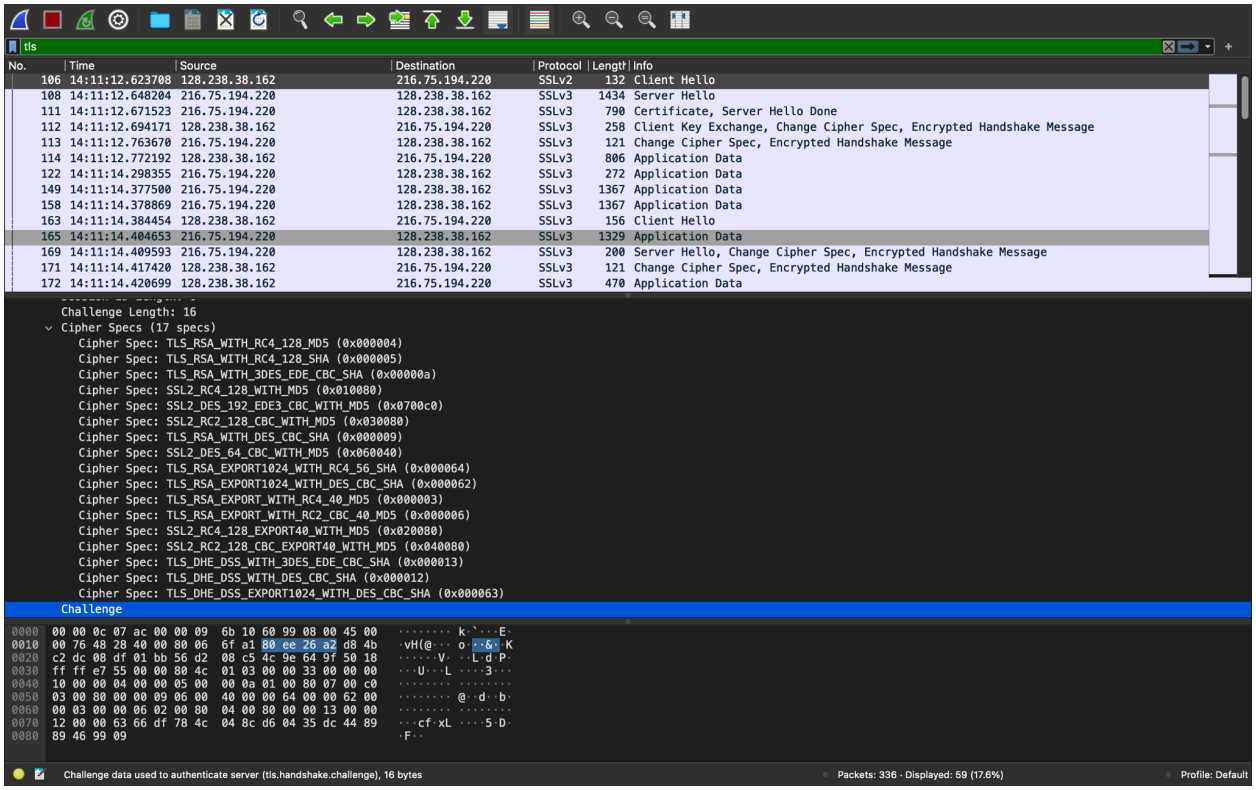
3). The value of Content Type is 22



4). Yes.

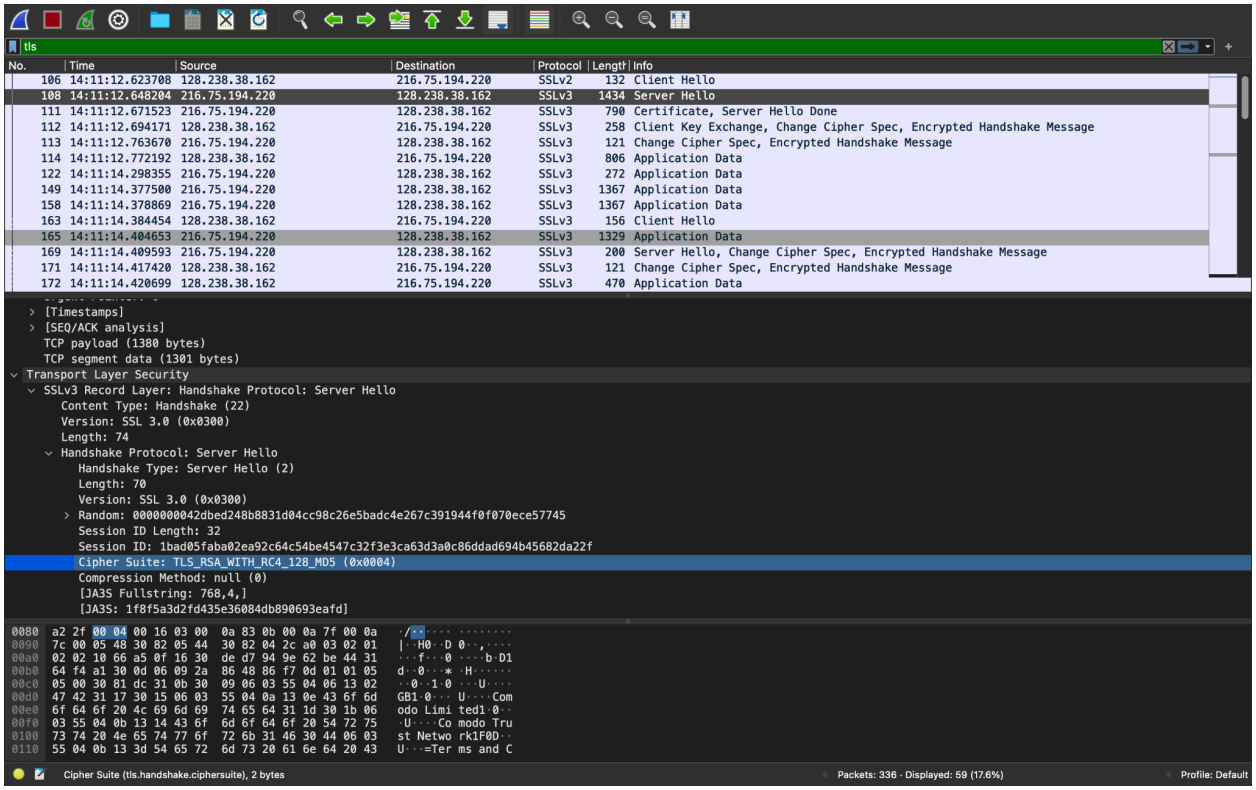
The value of Challenge is 66 df 78 4c 04 8c d6 04 35 dc 44 89 89 46 99 09

Foundation of Computer Networks - Wireshark Project
Bhavin Oza (bo2115)

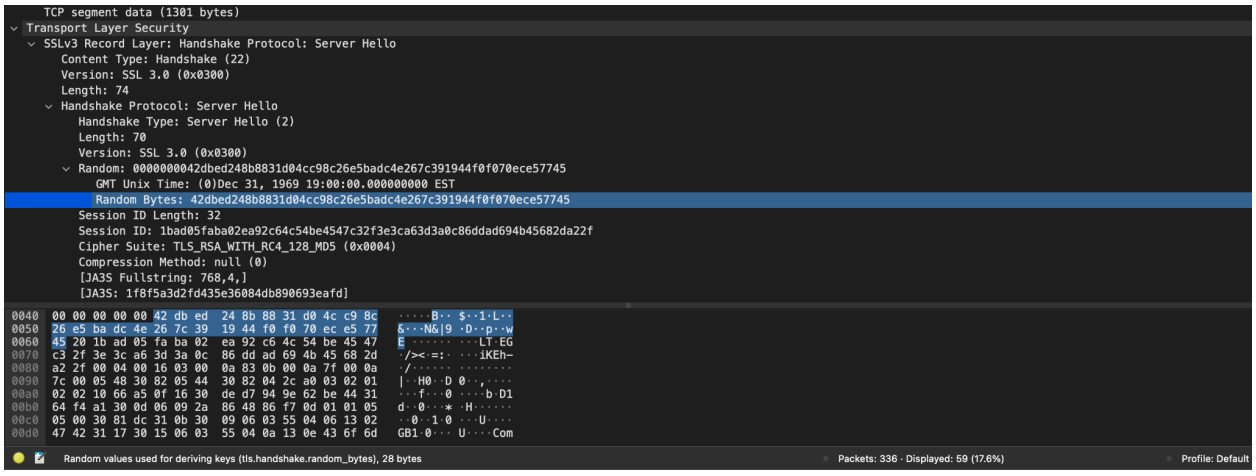


5). Yes.
RSA for public cryptography algorithm.
RC4 for symmetric key cipher
MD5 hash algorithm

Foundation of Computer Networks - Wireshark Project
Bhavin Oza (bo2115)

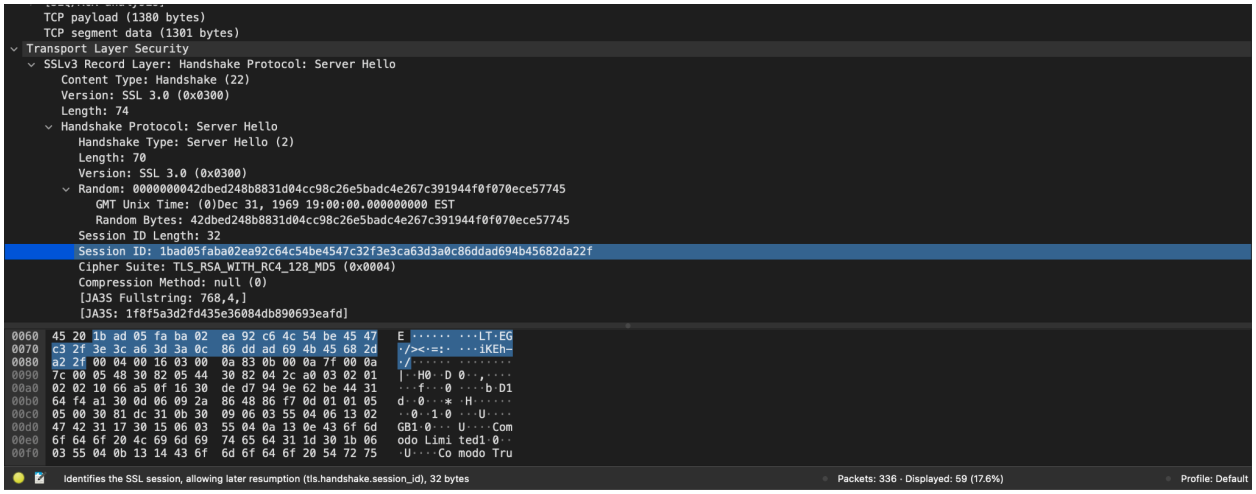


6). Yes.
RSA for public cryptography algorithm
RC4 for symmetric key cipher
MD5 hash algorithm



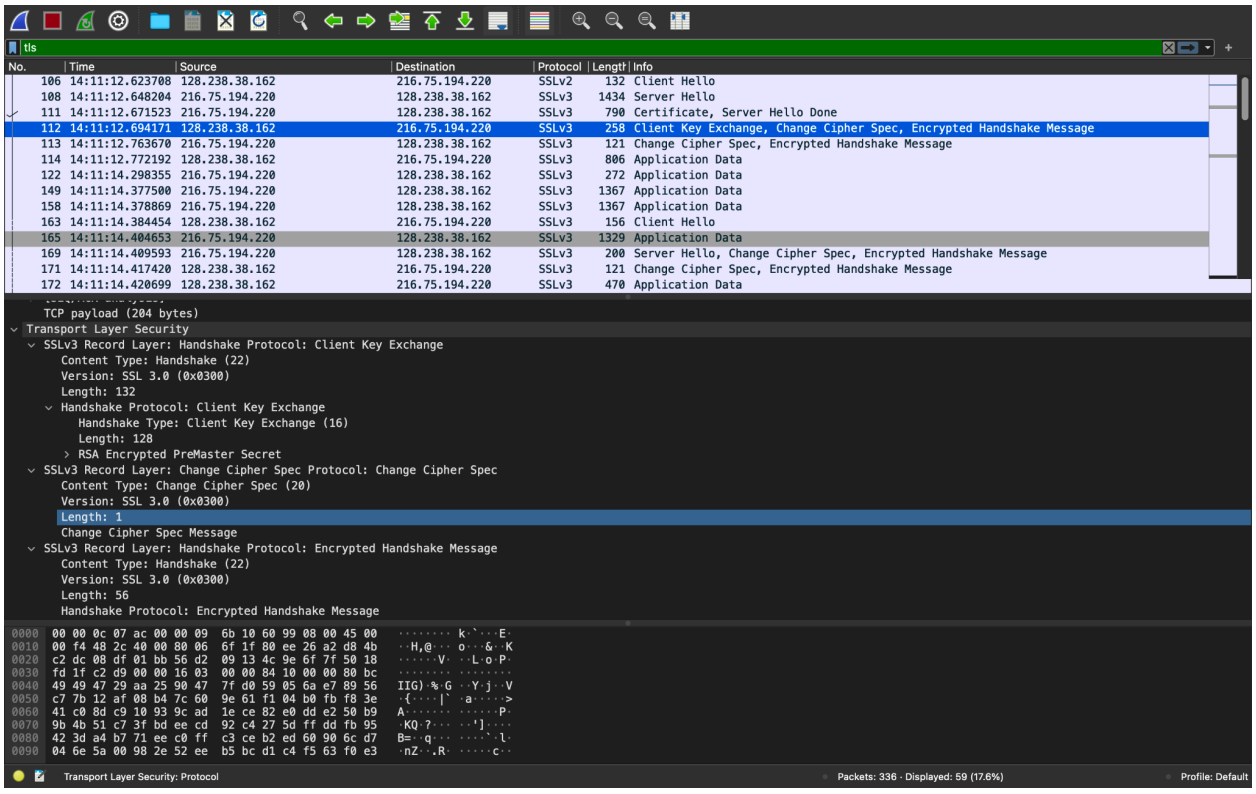
7). Yes.
The nonce is known as random bytes as shown above, which is 28 bytes long
The purpose of the nonce is to avoid replay attacks.

Foundation of Computer Networks - Wireshark Project
Bhavin Oza (bo2115)



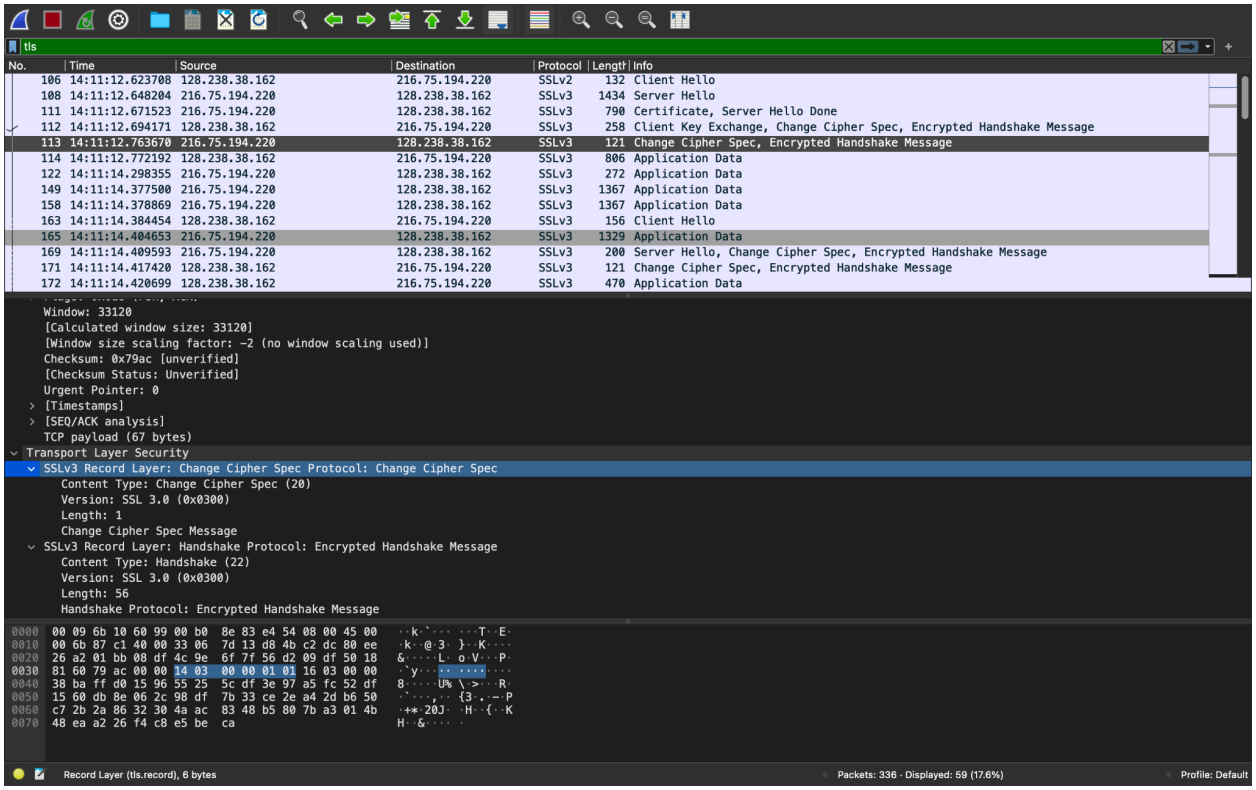
8). Yes, and the session ID is 32 bytes long
The purpose of the Session ID is it provides a persistent identifier for the SSL session. The client may resume the same session later by using server provided session ID

9). No.
The certificate is in another record



10). Yes. The client and server share the same master key and it is 128 bytes long

Foundation of Computer Networks - Wireshark Project
Bhavin Oza (bo2115)

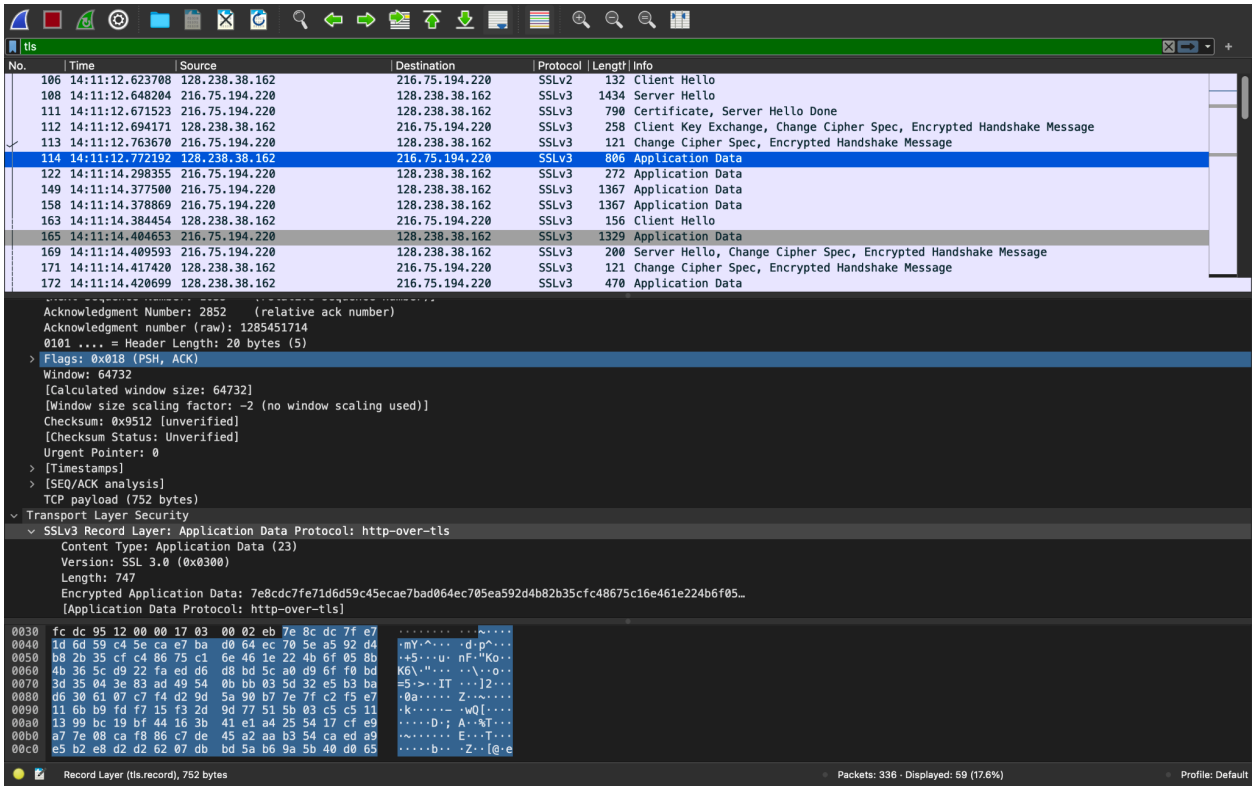


11). The purpose of the Change Cipher Spec is to indicate that the content will be encrypted by the client and sent.
The length is 1 byte long.

12). MAC address of all the previous handshake are encrypted, and sent from client to server

13). Yes
The difference is that the sender is server and previous the client was sender

Foundation of Computer Networks - Wireshark Project
Bhavin Oza (bo2115)



14).
Application data is being encrypted using one of the cipher suite algorithms chosen in the handshake phase.
Yes it includes MAC.
Yes, the wireshark distinguishes between encrypted application data and the MAC

15). The first client hello message is sent by SSLv2 and the others are sent by SSLv3.
The certificate is sent only in the first handshake process, after the first handshake client sends only a nonce.
The server sends the encrypted handshake and change cipher spec record to the client.