Họ tên : Lê Bảo Khánh
MSSV : 1911363
Lớp : L01

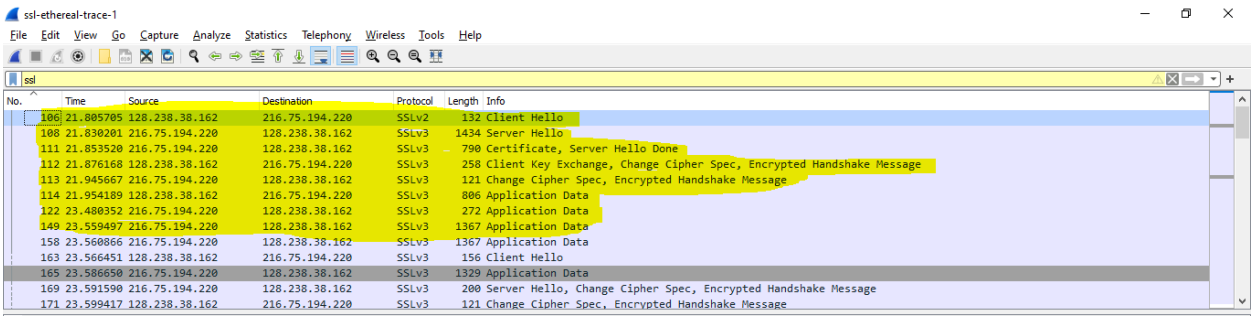
LAB 8

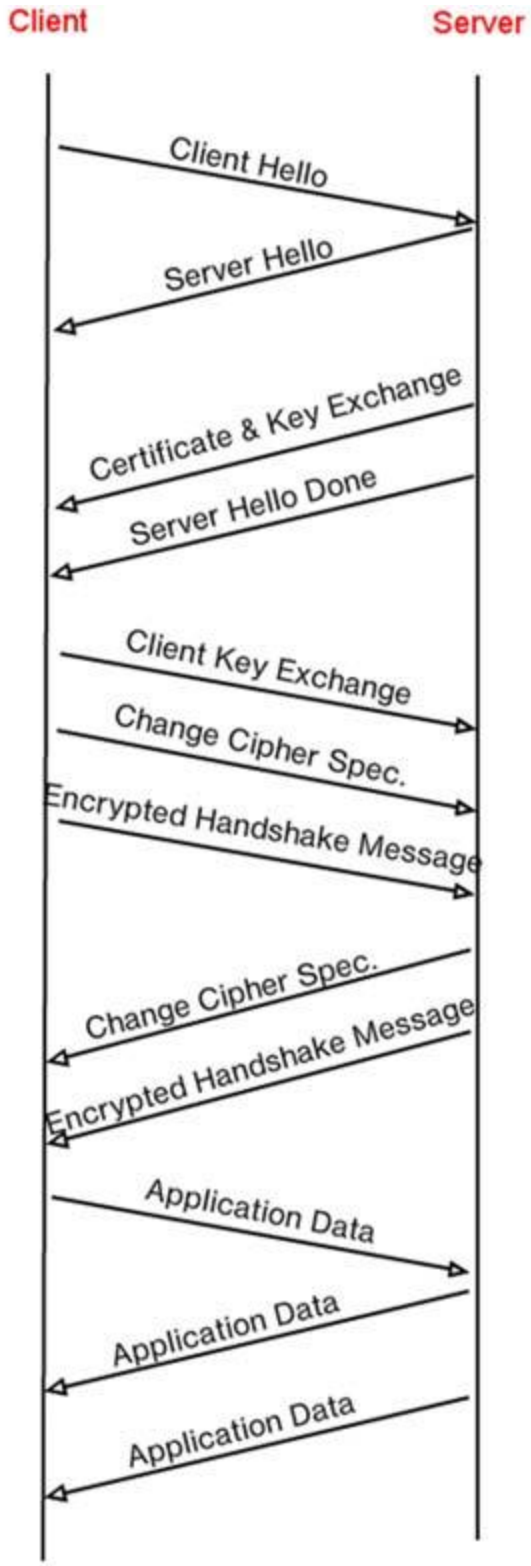
(using the file ssl-etherealtrace-1 packet trace)

Question 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.

ANSWER:

No.	Frame	Source	Destination	SSL Count	SSL Type
1	106	128.238.38.162	216.75.194.220	1	Client Hello
2	108	216.75.194.220	128.238.38.162	1	Server Hello
3	111	216.75.194.220	128.238.38.162	2	Server Hello Done
4	112	128.238.38.162	216.75.194.220	3	Client Key Exchange
5	113	216.75.194.220	128.238.38.162	2	Change Cipher Spec
6	114	128.238.38.162	216.75.194.220	1	Application Data
7	122	216.75.194.220	128.238.38.162	1	Application Data
8	149	216.75.194.220	128.238.38.162	1	Application Data



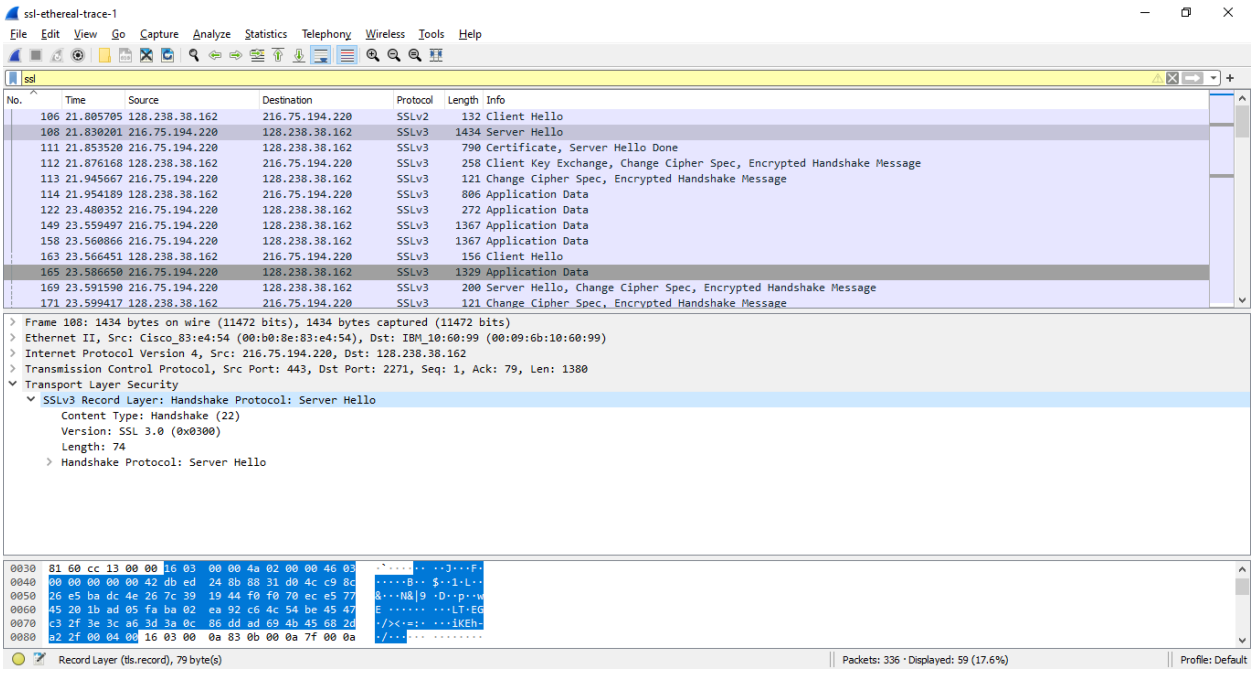


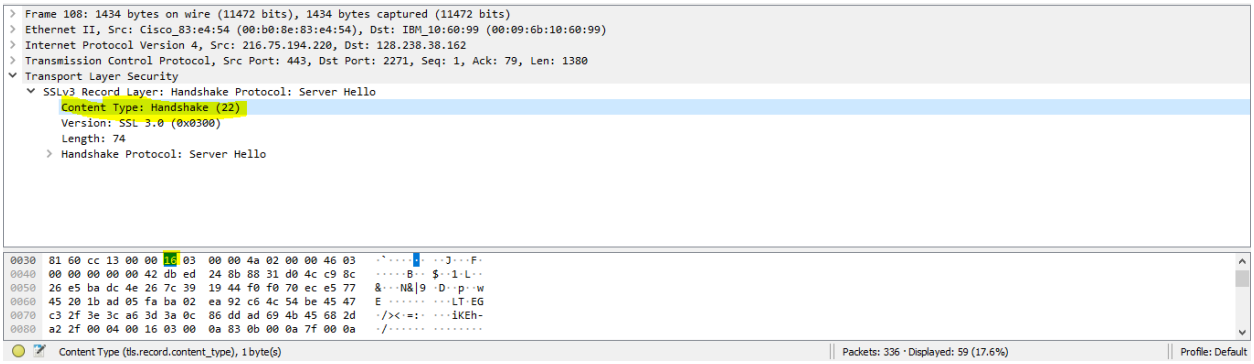
Question 2 Each of the SSL records begins with the same three fields (with possibly different

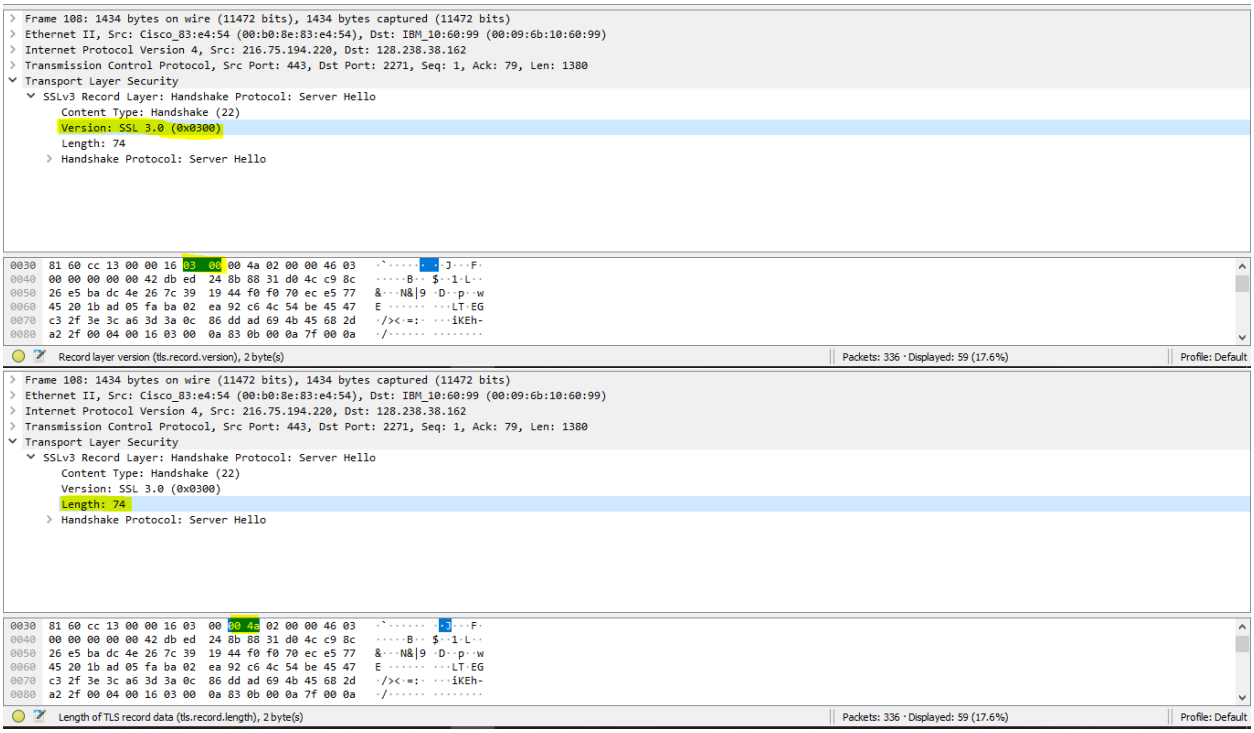
values). One of these fields is “content type” and has length of one byte. List all three fields and their lengths.

ANSWER:

Content Type = 1 byte
Version = 2 bytes
Length = 2 bytes







ClientHello Record:

Question 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?

ANSWER:

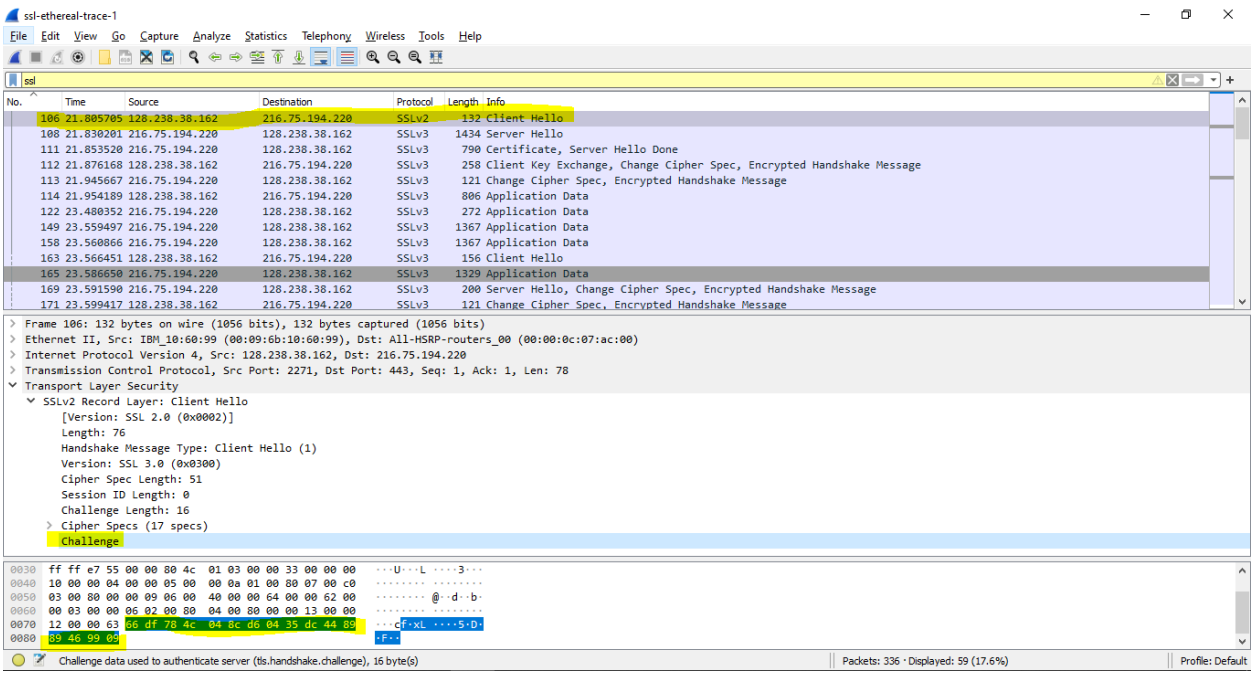
Content type: 22

Question 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?

ANSWER:

Yes

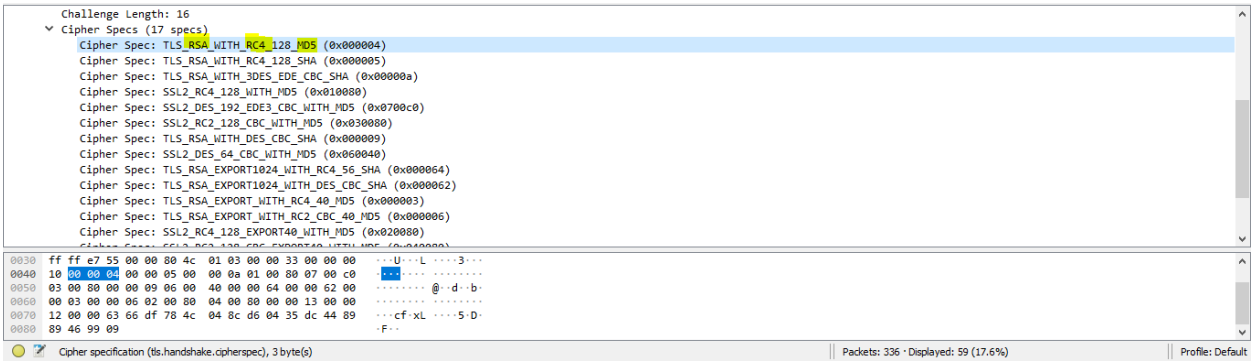
66 df 78 4c 04 8c d6 04 35 dc 44 89 89 46 99 09



Question 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?

ANSWER:

Public key algorithm: RSA
Symmetric-key algorithm: RC4
Hash algorithm: MD5

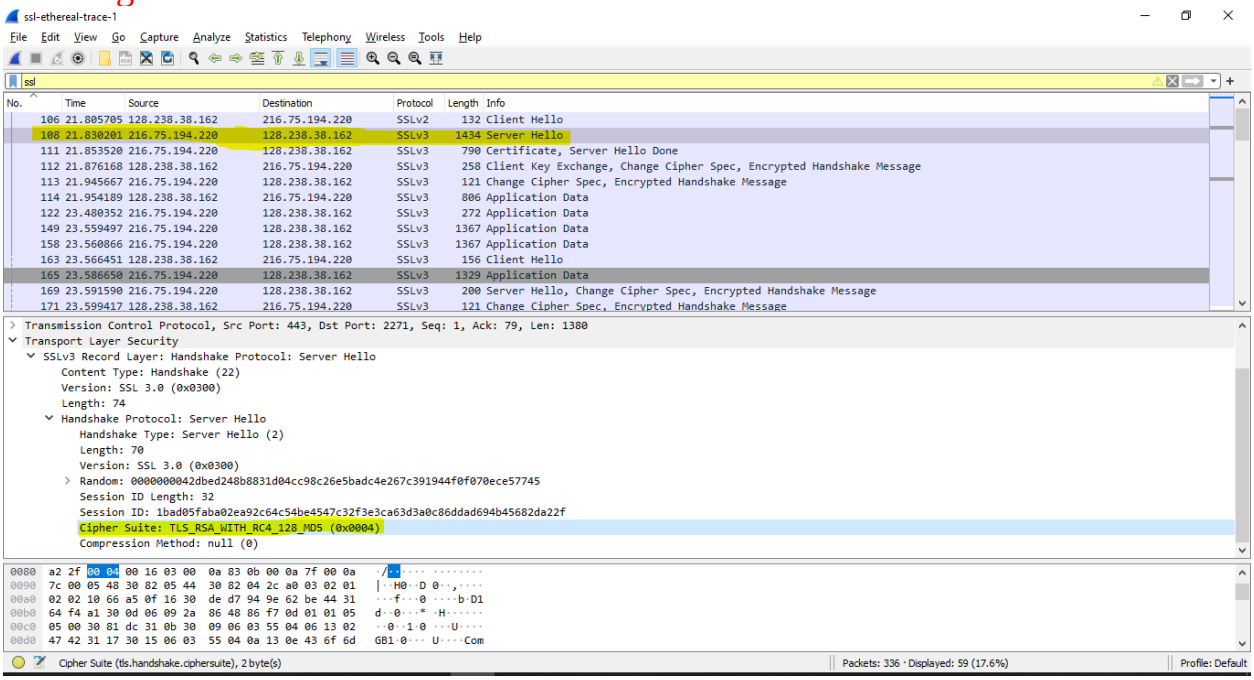


ServerHello Record:

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

ANSWER:

Public key algorithm: RSA
Symmetric-key algorithm: RC4
Hash algorithm: MD5



<u>Question 7:</u> Does this record include a nonce? If so, how long is it? What is the purpose of the client and server nonces in SSL?

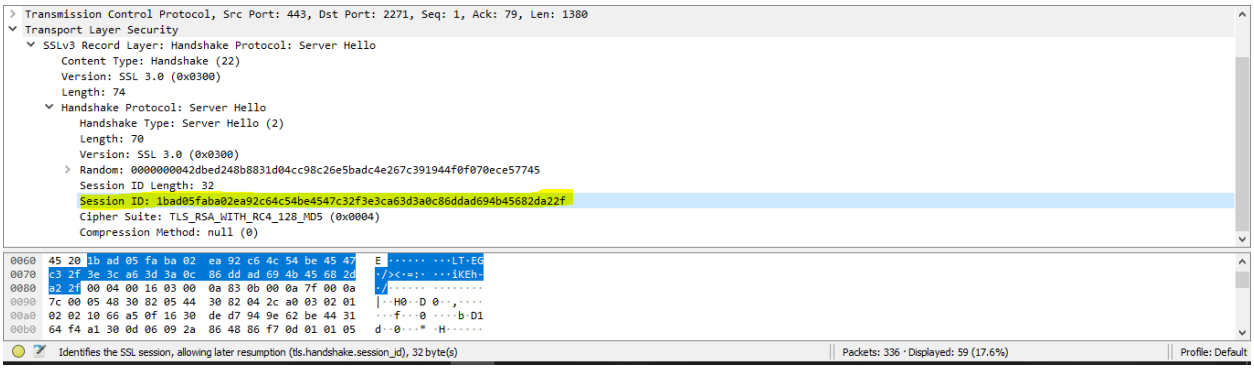
ANSWER:

Yes
32 bits long = 28bits data + 4 bits time
It is used for attack preventing.

<u>Question 8:</u> Does this record include a session ID? What is the purpose of the session ID?

ANSWER:

Yes
The session ID in the record is an identifier for SSL session.
=> Let the client to resume the session later by using the session ID.



Question 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?

ANSWER:

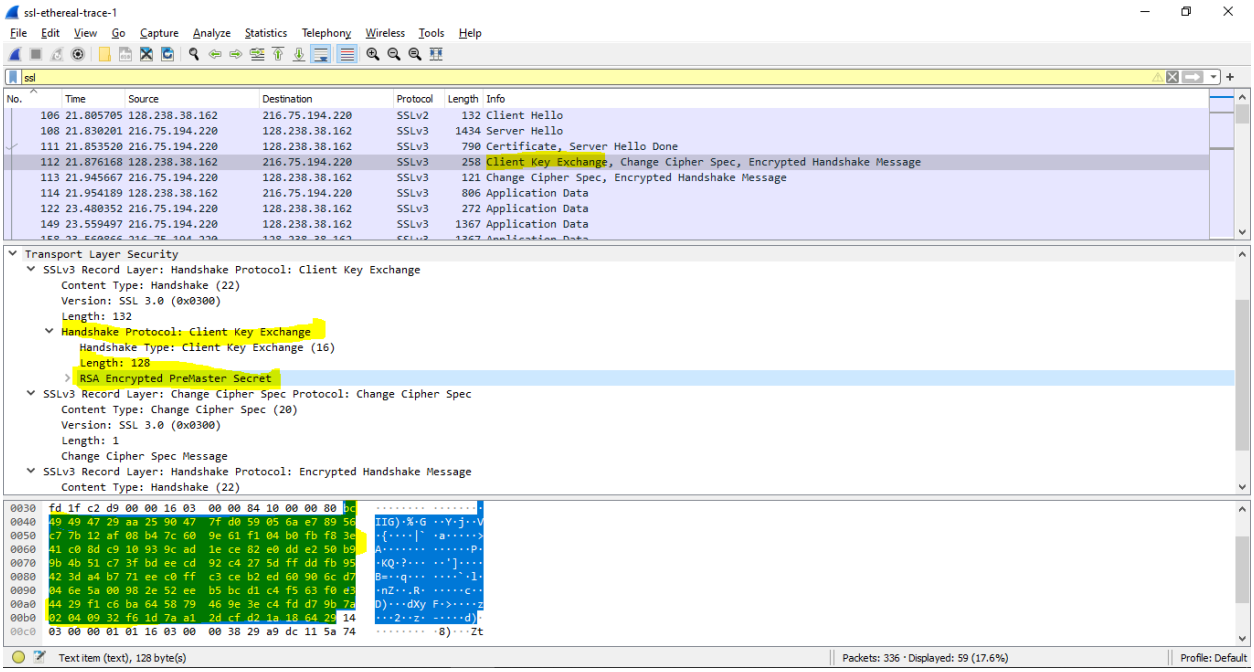
No, there is no certificate in this record. The certificate is in the separate record.
Yes, the certificate fit into a 1 Ethernet frame.

Client Key Exchange Record:

Question 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?

ANSWER:

Yes, there is a pre-master secret
The master secret is created using this pre-master secret. The master key is used to create session key.
The secret is encrypted by public key, the encrypted secret is 128 bytes

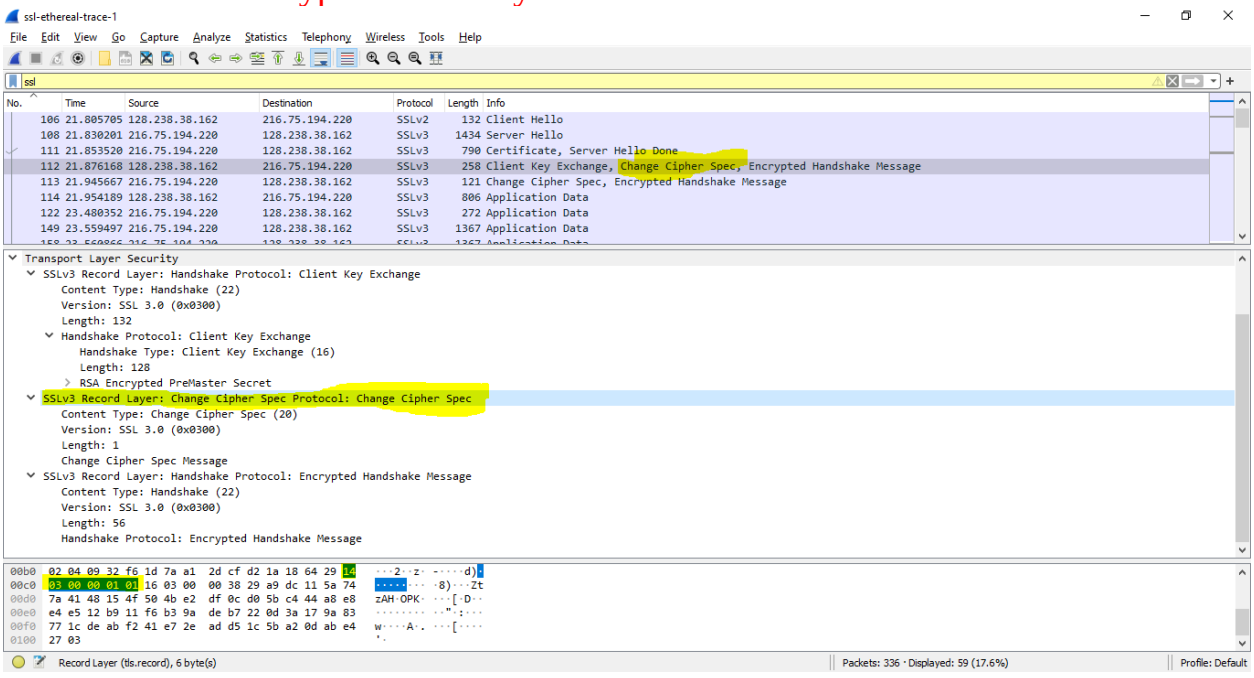


Change Cipher Spec Record (sent by client) and Encrypted Handshake Record:

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

ANSWER:

The Change Cipher Spec record is used to indicate the content of the next SSL records will be encrypted. It is 6 bytes.



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

ANSWER:

Handshake messages + MAC addresses are concatenated and encrypted, then they are sent to the server.

Question 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?

ANSWER:

Yes, the server's encrypted handshake contains all the handshake messages sent from the server. Other contains messages sent from client.

Application Data:

Question 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?

ANSWER:

The symmetric encryption algorithm is used to encrypt the application data.
Yes, the records containing application data include a MAC.
No, Wireshark did not distinguish between the encrypted application data and the MAC.

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

ANSWER:

The version of SSL used changes from SSLv2 in the initial ClientHello message to SSLv3 in all following message exchanges

Moreover, during resumes the handshake process is slightly different from the initial one. The client does not need another cert so the server never sends it. It just has to send a new nonce followed by Change Cipher Spec and Encrypted Handshake records from the server to client. The application data can be sent after a response from the client