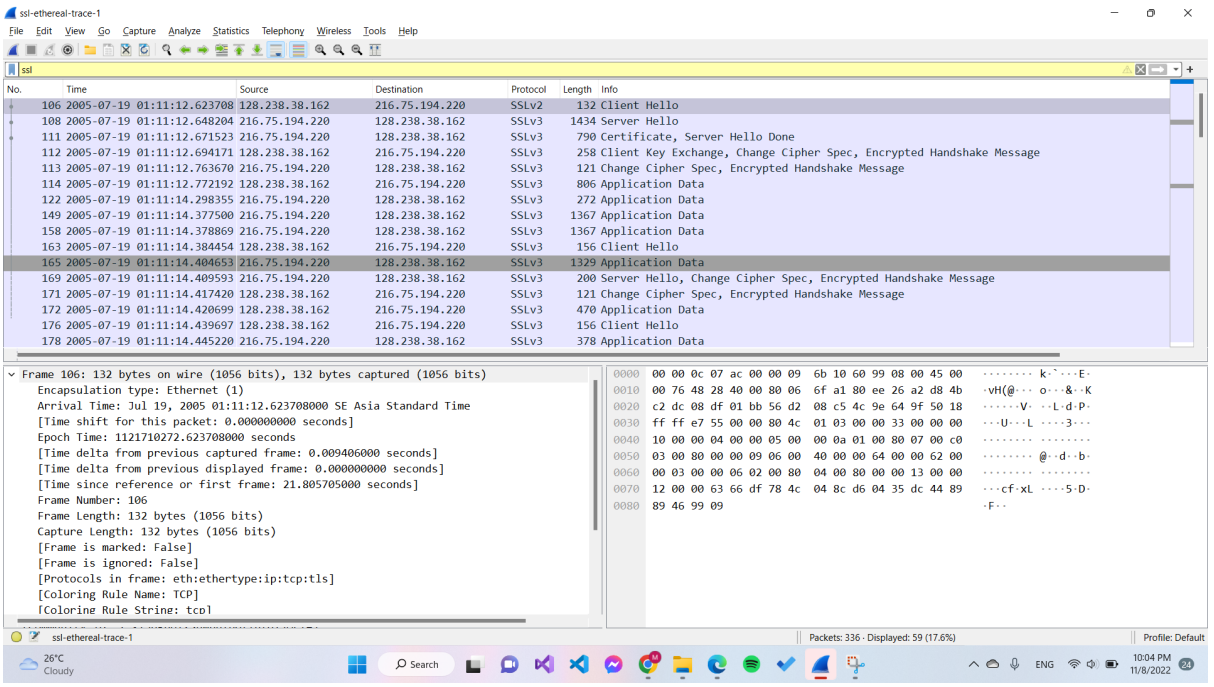
Wireshark Lab: SSL v8.0

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.

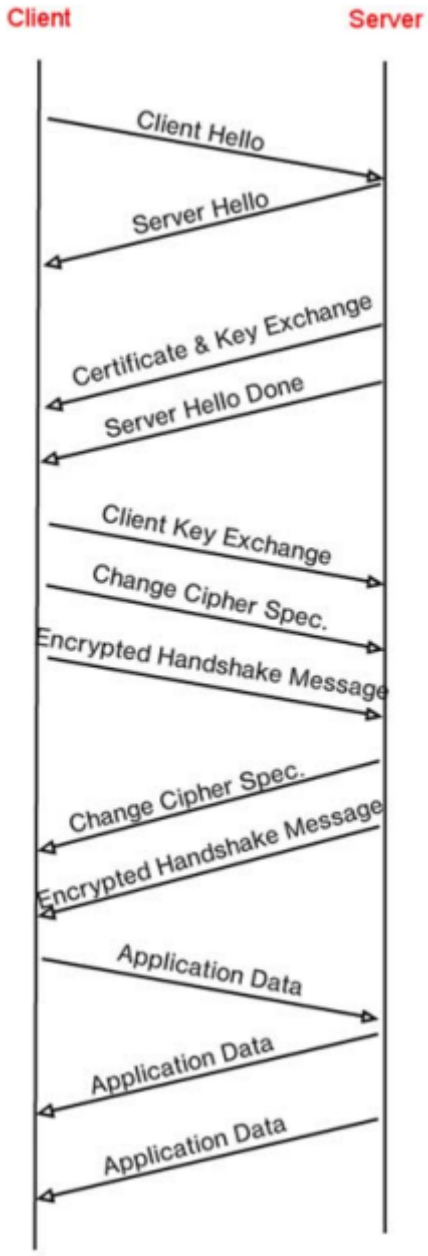
   Answer:



Frame	Source	Destination	SSL Count	SSL Type
106	128.238.38.162	216.75.194.220	1	Client Hello
108	216.75.194.220	128.238.38.162	1	Server Hello
111	216.75.194.220	128.238.38.162	2	Server Hello Done
112	128.238.38.162	216.75.194.220	3	Client Key

				Exchange
113	216.75.194.220	128.238.38.162	2	Change Cipher Spec
114	128.238.38.162	216.75.194.220	1	Application Data
122	216.75.194.220	128.238.38.162	1	Application Data
127	216.75.194.220	128.238.38.162	1	Application Data

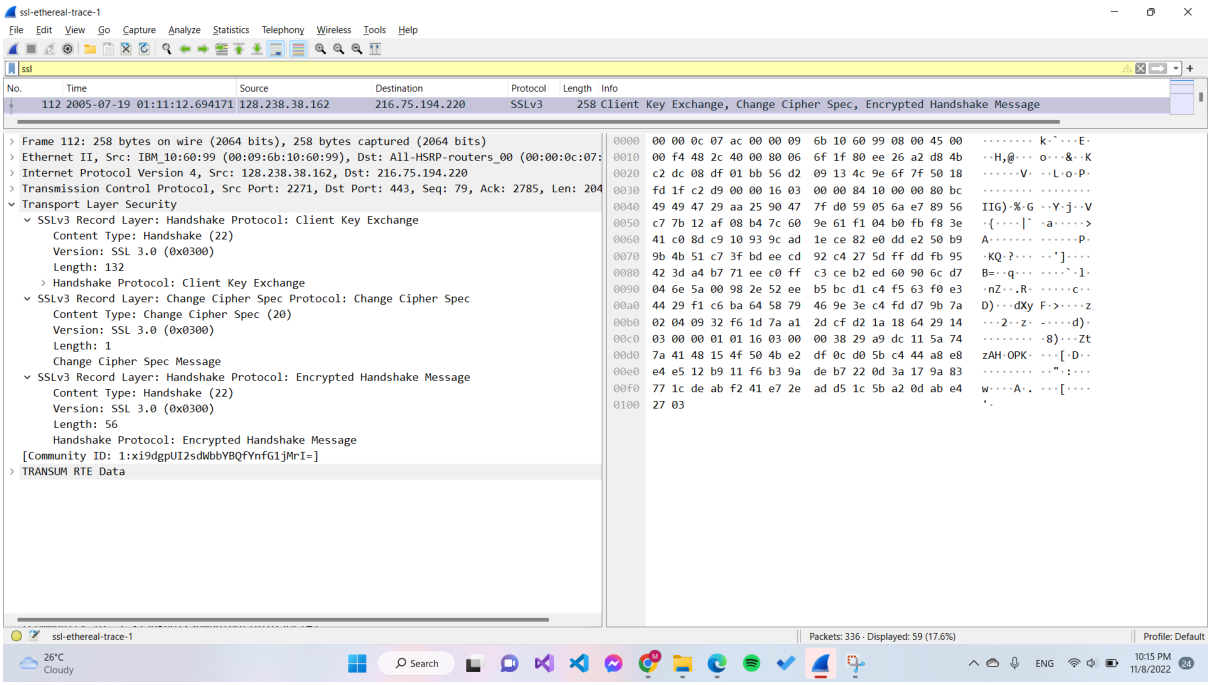
Wireshark Lab: SSL v8.0



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:

Wireshark Lab: SSL v8.0



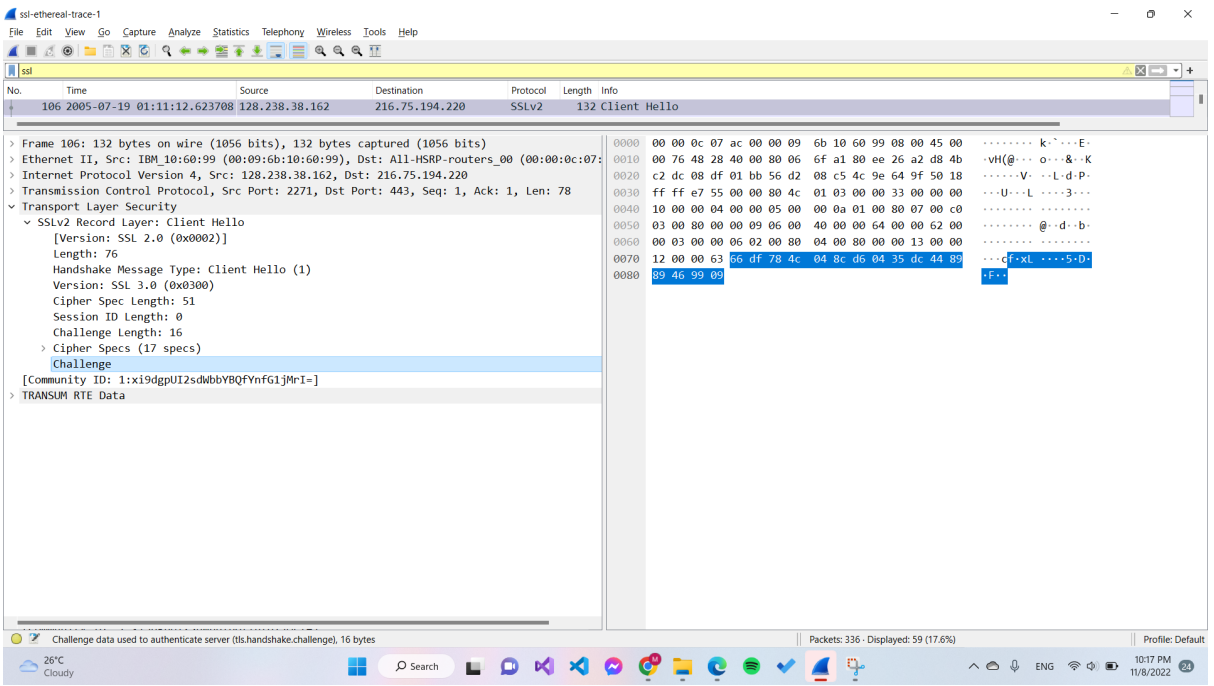
Content Type = 1 byte

Version = 2 bytes

Length = 2 bytes

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:



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?

   Answer:

   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?

   Answer:

   Public key algorithm is RSA

   Symmetric-key algorithm is RC4

   Hash algorithm is MD5

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 is RSA

   Symmetric-key algorithm is RC4

   Hash algorithm is MD5

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?

   Answer:

   Yes, it is 32 bits long (28bits data + 4 bits time), it is used for attack preventing.

8. 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. This ID could let the client to resume the session later by using the session ID.

Wireshark Lab: SSL v8.0

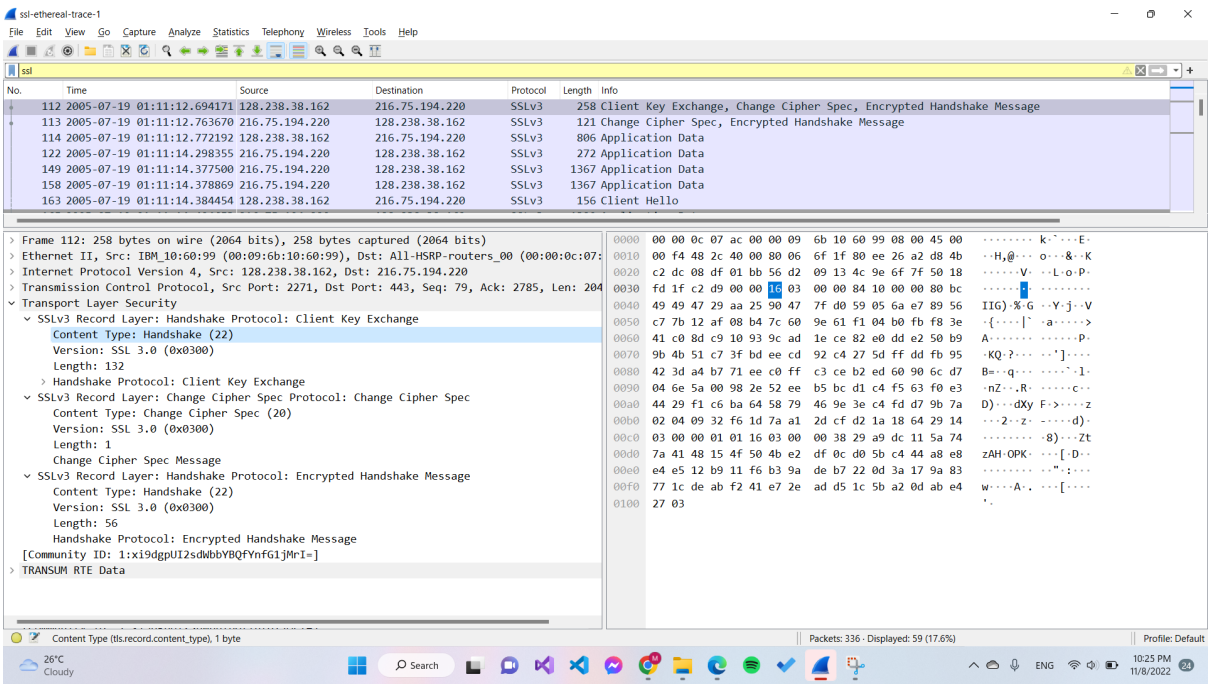
9. Does this record contain a certificate, or is the certificate included in a separate record. Does the certificate fit into a single Ethernet frame?

   Answer:

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

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, this record contains 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 120 bytes.

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.

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

    Answer:

    All handshake messages and MAC addresses are concatenated and encrypted. They are sent to the server.

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.

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.

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

    Answer:

    No more comment, everything as expected.