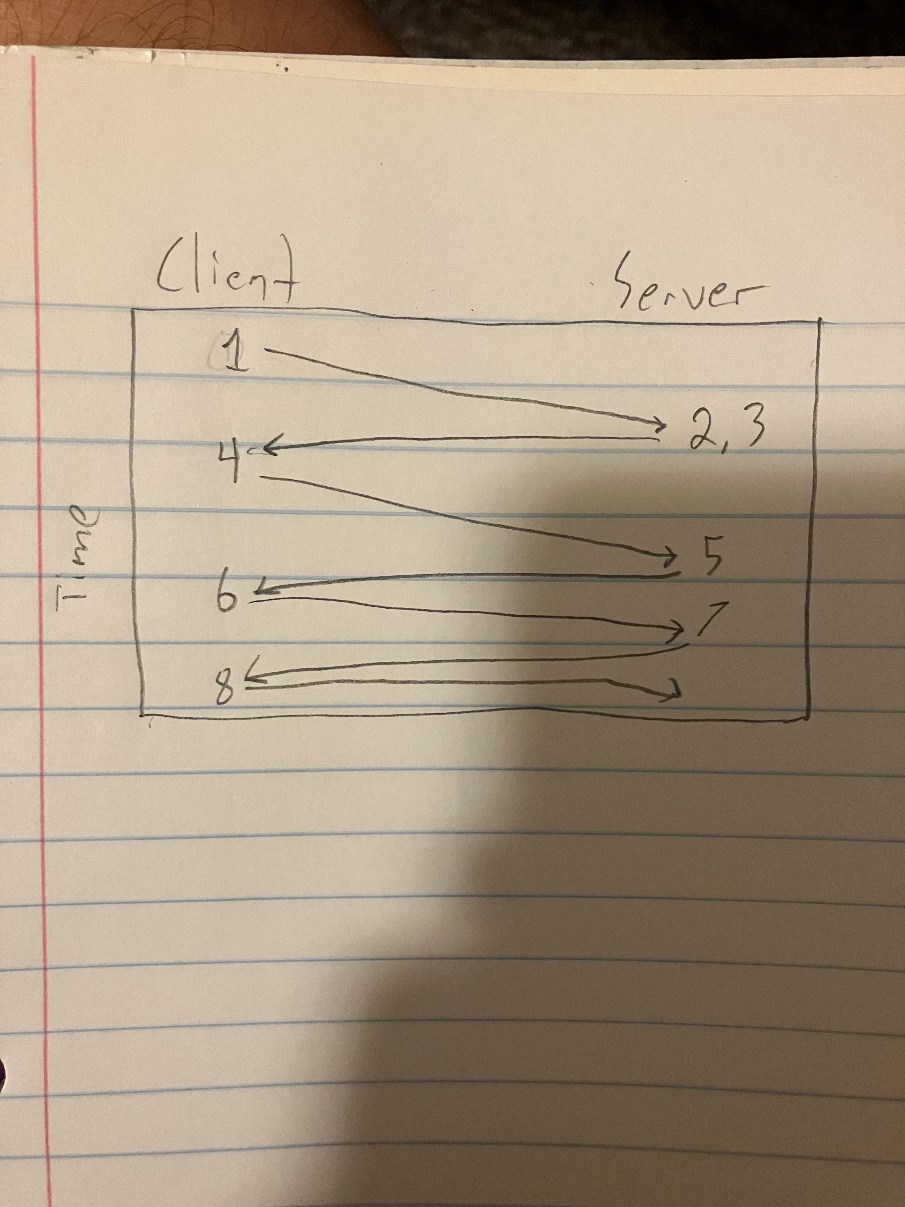
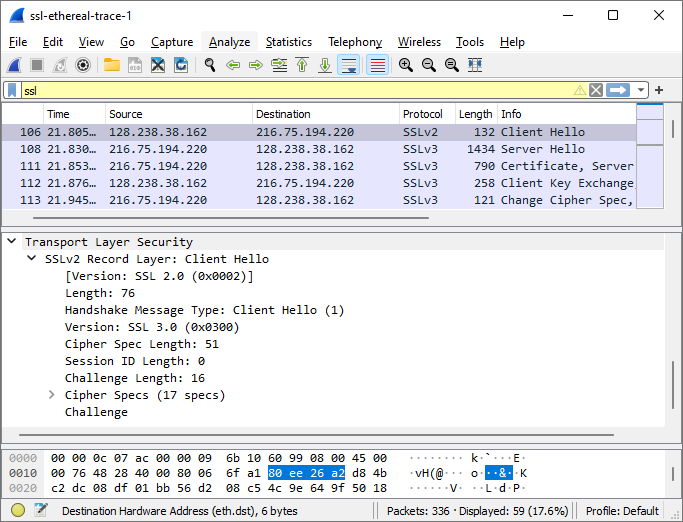
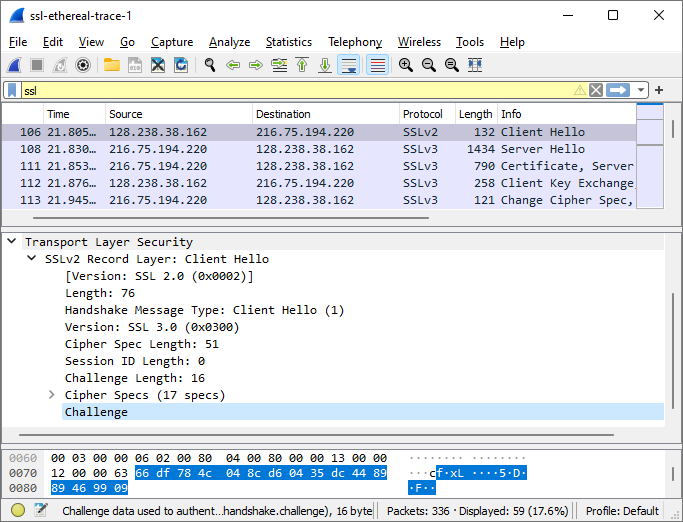
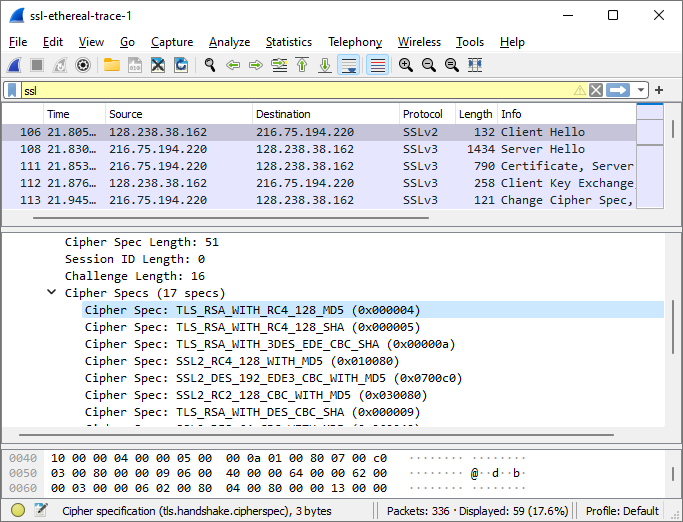
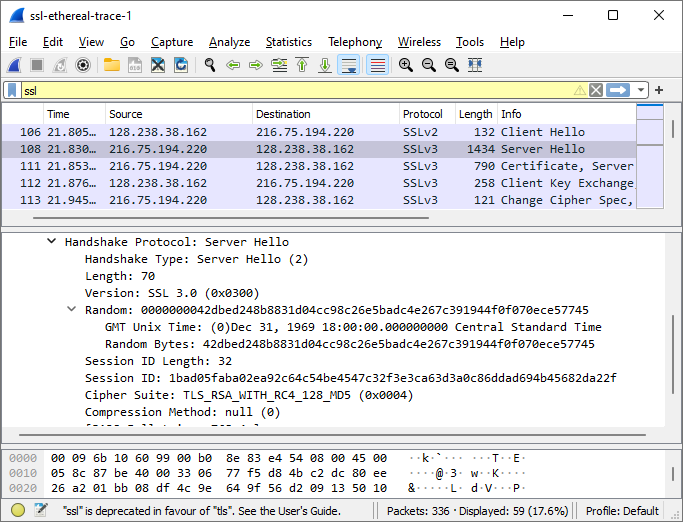
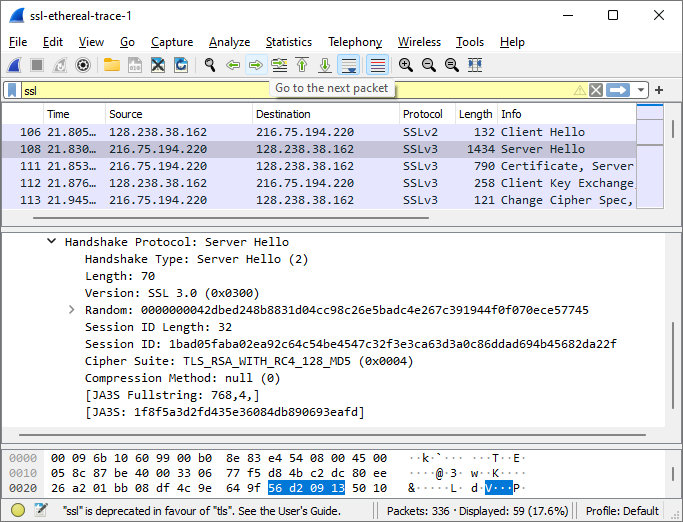
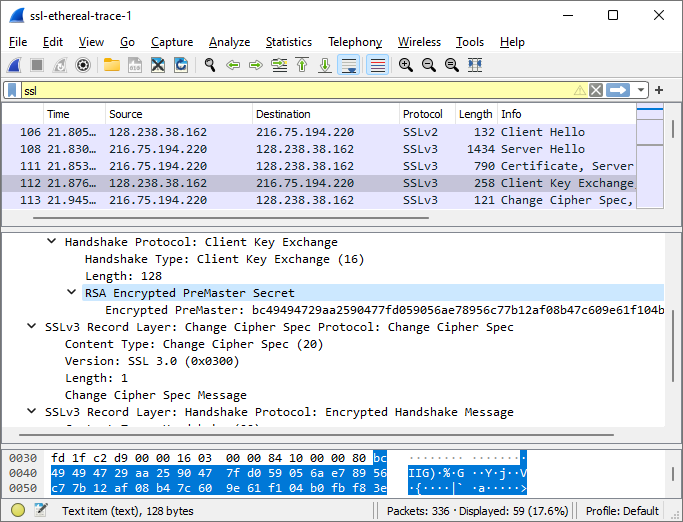
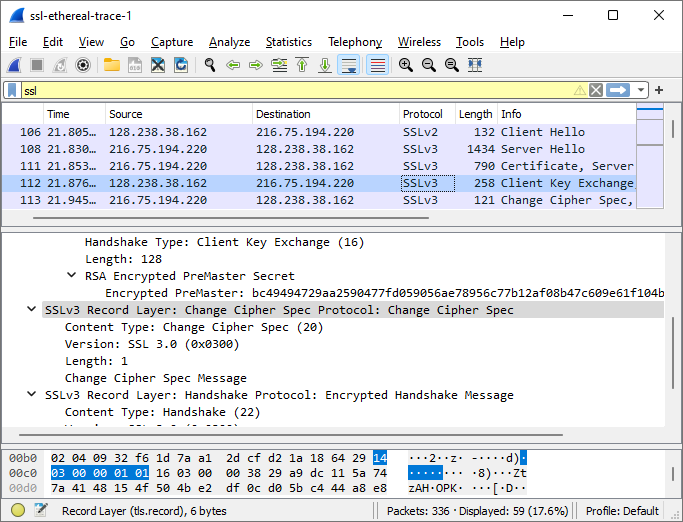
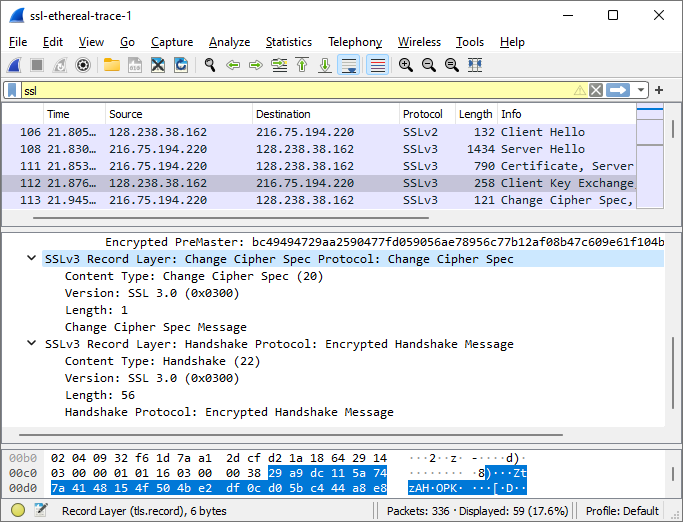
1. For each of the first 8 Ethernet frames, specify the source of the frame (client or server), determine the number of SSL records that are included in the frame, and list the SSL record types that are included in the frame. Draw a timing diagram between client and server, with one arrow for each SSL record.
   1. 1)Client, 132, SSLv2, Client Hello
   2. 2)Server, 1434, SSLv3, Server Hello
   3. 3)Server, 790, SSLv3, Certificate Server Hello Done
   4. 4)Client, 258, SSLv3, Client Key Exchange Change Cipher Spec
   5. 5)Server, 121, SSLv3, Change Cipher Spec Encrypted Handshake Message
   6. 6)Client, 806, SSLv3, Application Data
   7. 7)Server, 272, SSLv3, Application Data
   8. 8)Server, 1367, SSLv3, Application Data
   9. Graphical user interface, text, application, email

      Description automatically generated
   10. 
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.
   1. Content Type, One Byte
   2. SSL Version, Two Bytes
   3. Length, Two Bytes­­
   4. 
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?
   1. As seen in the image above, the value of the content type is Client Hello1
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?
   1. Yes it Contains a challenge and the Hexadecimal value is 66 df 78 4c 04 35 dc 44 89 89 46 99 09.
   2. 
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?
   1. Yes, the client records the cyber suites it supports. For the first listed suite TLS, the public key algorithm is RSA, the symmetric key algorithm is RC4, and the hash algorithm is MD5
   2. 
6. Locate the ServerHello SSL record. Does this record specify a chosen cipher suite? What are the algorithms in the chosen cipher suite?
   1. Yes, the client records the cyber suites it supports. For the first listed suite TLS, the public key algorithm is RSA, the symmetric key algorithm is RC4, and the hash algorithm is MD5
   2. A picture containing graphical user interface

      Description automatically generated
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?
   1. Yes, there is a nonce, and it is listed under random. It is 32 bits long. The purpose is to prevent a replay attack
   2. 
8. Does this record include a session ID? What is the purpose of the session ID?
   1. Yes it does, and the purpose of it is to provide a unique identifier so that the client may resume the same session later by using the session ID.
   2. 
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?
   1. This record doesn’t contain a certificate, it is included in a separate record. Yes, the certificate fits 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?
    1. Yes, it contains a pre-master secret. It is used to make a master secret in order to generate session keys. Yes the secret is encrypted. It is encrypted by using the server’s public key. The secret is 128 bytes long.
    2. 
11. What is the purpose of the Change Cipher Spec record? How many bytes is the record in your trace?
    1. The purpose of the Change Cipher Spec record is to indicate that the following records will be encrypted. The record is 6 bytes long.
    2. 
12. In the encrypted handshake record, what is being encrypted? How?
    1. In the encrypted handshake record, the messages and MAC addresses are concatenated, encrypted, and then sent to the server.
    2. 
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?
    1. Yes, the server sends a change cipher record and an encrypted handshake record to the client. Those records are different from those sent by the client because it contains the concatenation of the handshake messages sent from the server as compared to being sent from the 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?
    1. The application data is being encrypted using the symmetric key encryption algorithm that is shown in an earlier question. Yes, the records containing application data include a MAC. No, Wireshark doesn’t distinguish between the encrypted application data and the MAC.
15. Comment on and explain anything else that you found interesting in the trace.
    1. I thought it was interesting that the Client Hello Protocol uses an SSLv2 protocol, while the rest of the SSL messages on the Wireshark trace use a SSLv3 protocol.