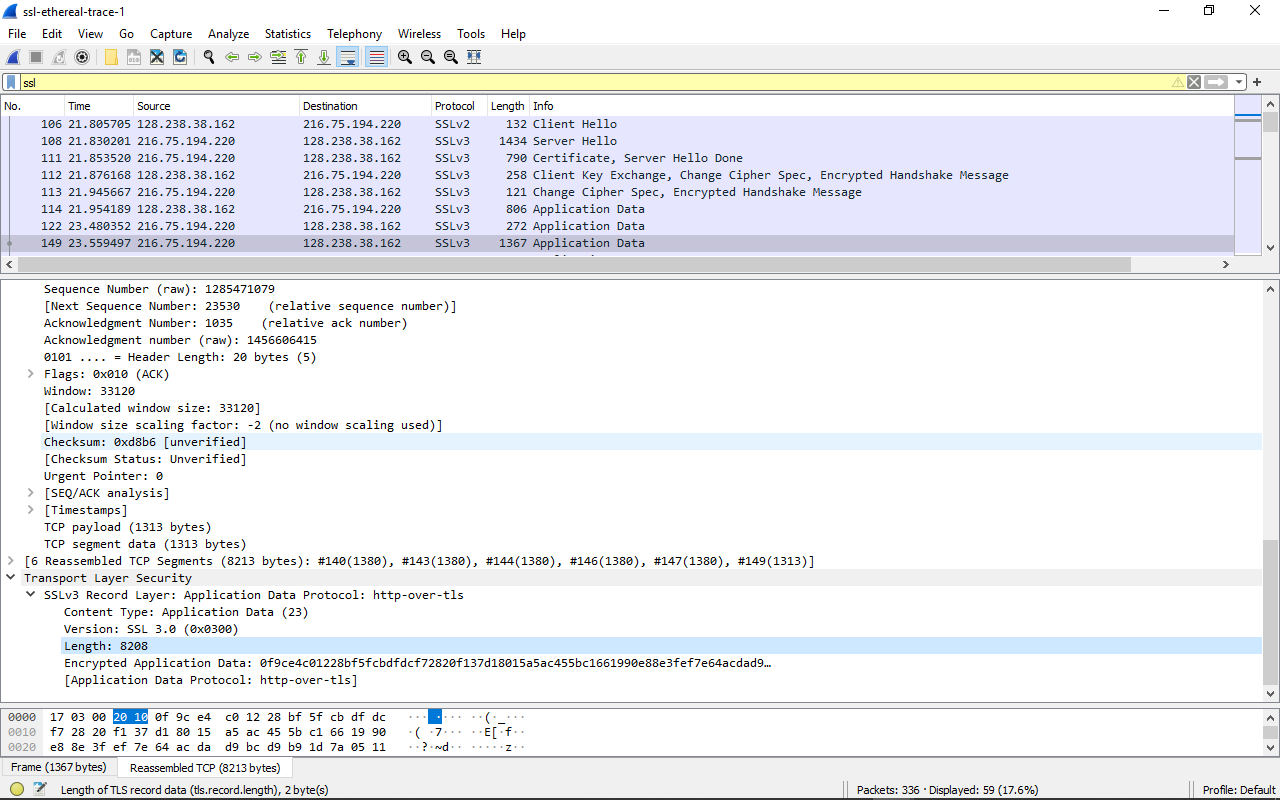
Họ và tên: Lê Trung Sơn

MSSV: 1810482

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 106:

128.238.38.162 - 216.75.194.220

Số SSL record layer - 1

SSL record type - Client Hello

- Frame 108:

216.75.194.220 - 128.238.38.162

Số SSL record layer - 1

SSL record type - Handshake Protocol: Server Hello

- Frame 111:

216.75.194.220 - 128.238.38.162

Số SSL record layer - 2

SSL record type - Handshake Protocol: Certificate, Handshake Protocol: Server Hello Done

- Frame 112:

128.238.38.162 - 216.75.194.220

Số SSL record layer - 3

SSL record type - Handshake Protocol: Client Key Exchange, Change Cipher Spec Protocol: Change Cipher Spec, Handshake Protocol: Encrypted Handshake Message

- Frame 113:

216.75.194.220 - 128.238.38.162

Số SSL record layer - 2

SSL record type - Change Cipher Spec Protocol: Change Cipher Spec, Handshake Protocol: Encrypted Handshake Message

- Frame 114:

128.238.38.162 - 216.75.194.220

Số SSL record layer - 1

SSL record type - Application Data Protocol: http-over-tls

- Frame 122:

216.75.194.220 - 128.238.38.162

Số SSL record layer - 1

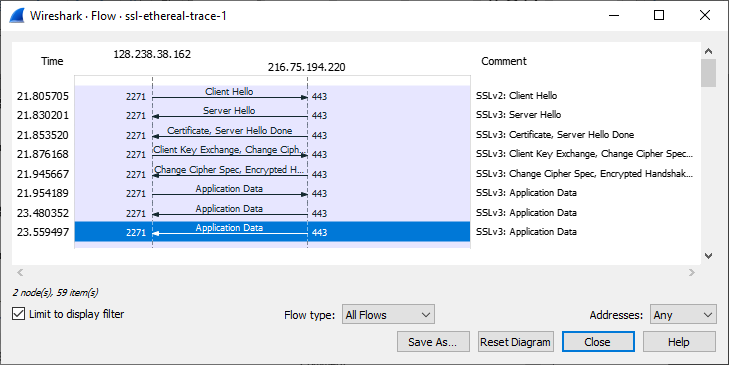
SSL record type - Application Data Protocol: http-over-tls

- Frame 149:

216.75.194.220 - 128.238.38.162

number of SSL record type - 1

SSL record type - Application Data Protocol: http-over-tls



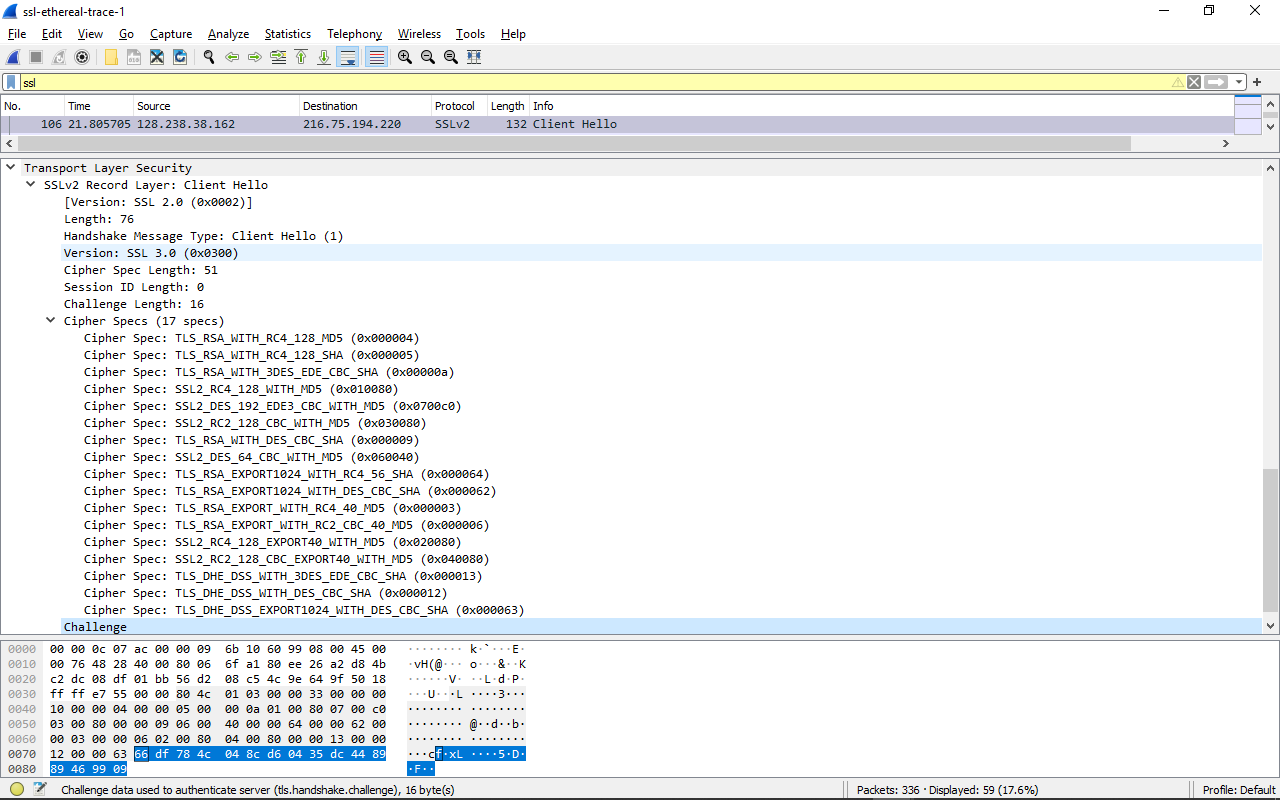
2. Each of the SSL records begins with the same three fields (with possibly different values). One of these fields is “content type” and has length of one byte. List all three fields and their lengths.

- Content type = 1 byte

- Version = 2 bytes

- Length = 2 bytes

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?



- Không thấy content type

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?

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

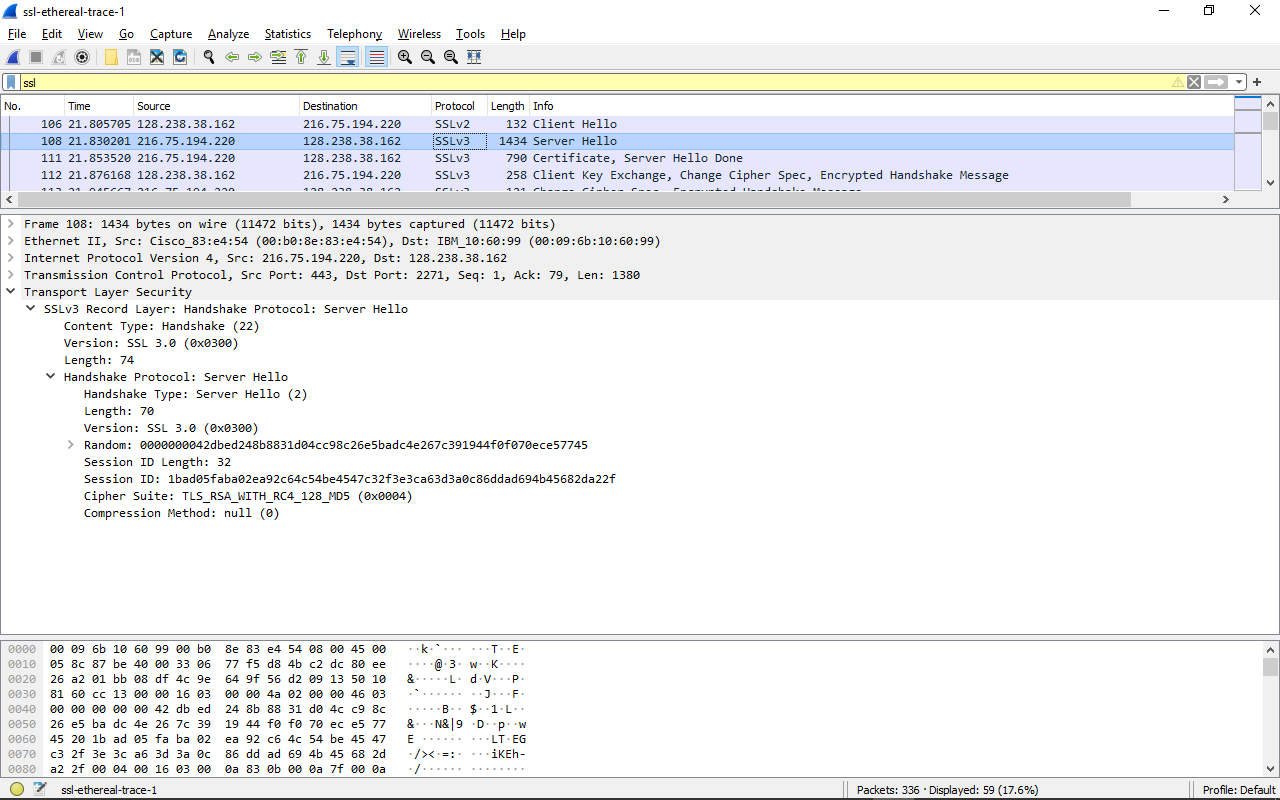
5. Does the ClientHello record advertise the cyber suites it supports? If so, in the first listed suite, what are the public-key algorithm, the symmetric-key algorithm, and the hash algorithm?

- Public key algorithm: RSA

- Symmetric‐key algorithm: RC4

- Hash algorithm: MD5

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



- Public key algorithm: RSA

- Symmetric‐key algorithm: RC4

- Hash algorithm: 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?

- Record có một nonce kiểu Random. Nonce có kích thước 32 bit, trong đó 28 cho data và 4 cho time. Mục đích là để ngăn chặn một cuộc tấn công.

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

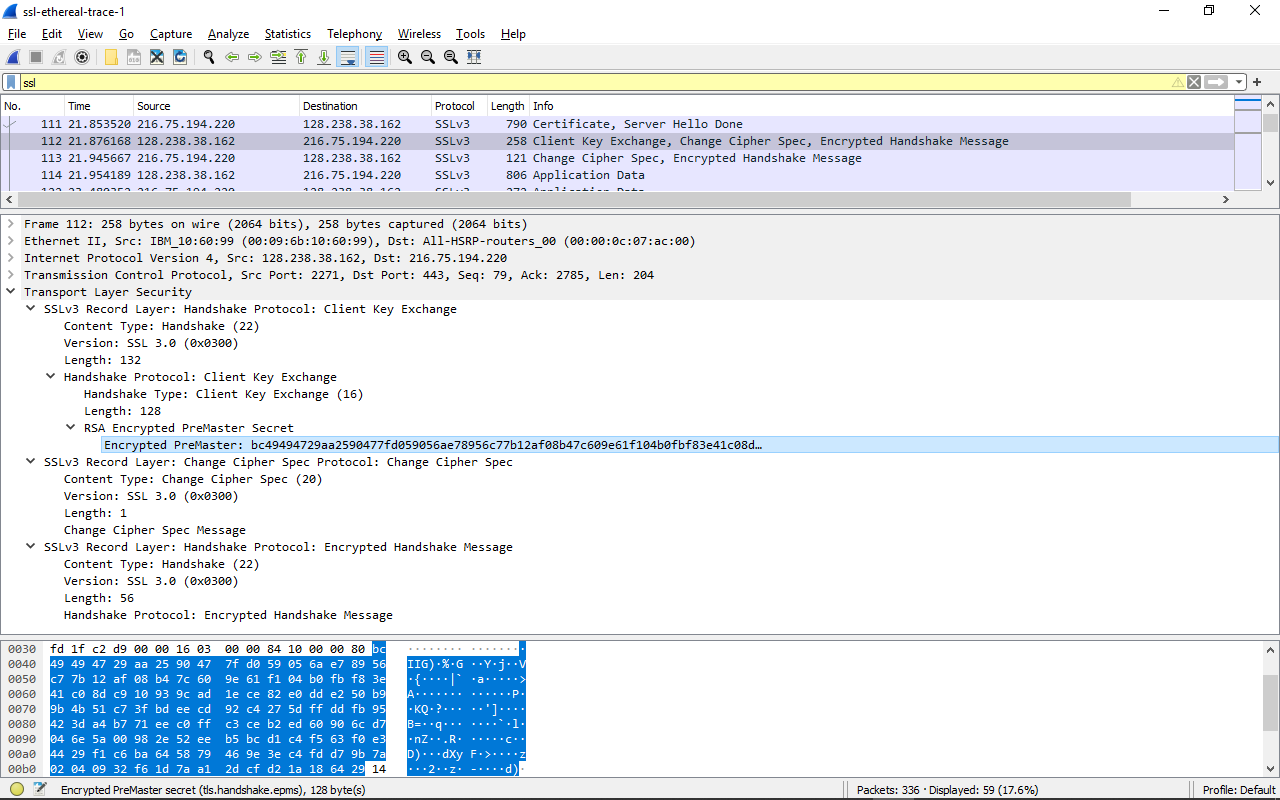
- Nó có 1 session ID. Được dùng để cung cấp cho người dùng quyền truy cập duy nhất vào kết nối 1 cách an toàn trong lần truy cập đó.

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?

- Không có certificate

- Certificate phù hợp với 1 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?



- Record có bao gồm pre-master secret.

- Secret này được dùng để xác thực key.

- Secret này được mã hóa.

- Nó có kích thước là 128 bytes

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

- Change Cipher Spec được sử dụng để cho biết nội dung của các bản ghi SSL tiếp theo sẽ được mã hóa. Nó có kích thước là 6 bytes.

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

- Tất cả các handshake messages và địa chỉ MAC đều được nối tiếp và mã hóa. Chúng được gửi đến máy chủ.

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?

- Máy chủ có gửi change cipher record và encrypted handshake record đến client.

- Sự khác nhau là nó bao gồm tất cả các message được gửi từ 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?

- Thuật toán mã hóa đối xứng được sử dụng để mã hóa application data.

- Các bản ghi chứa application data bao gồm MAC.

- Wireshark không phân biệt giữa application data được mã hóa và MAC.

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