**COMPUTER NETWORKS**

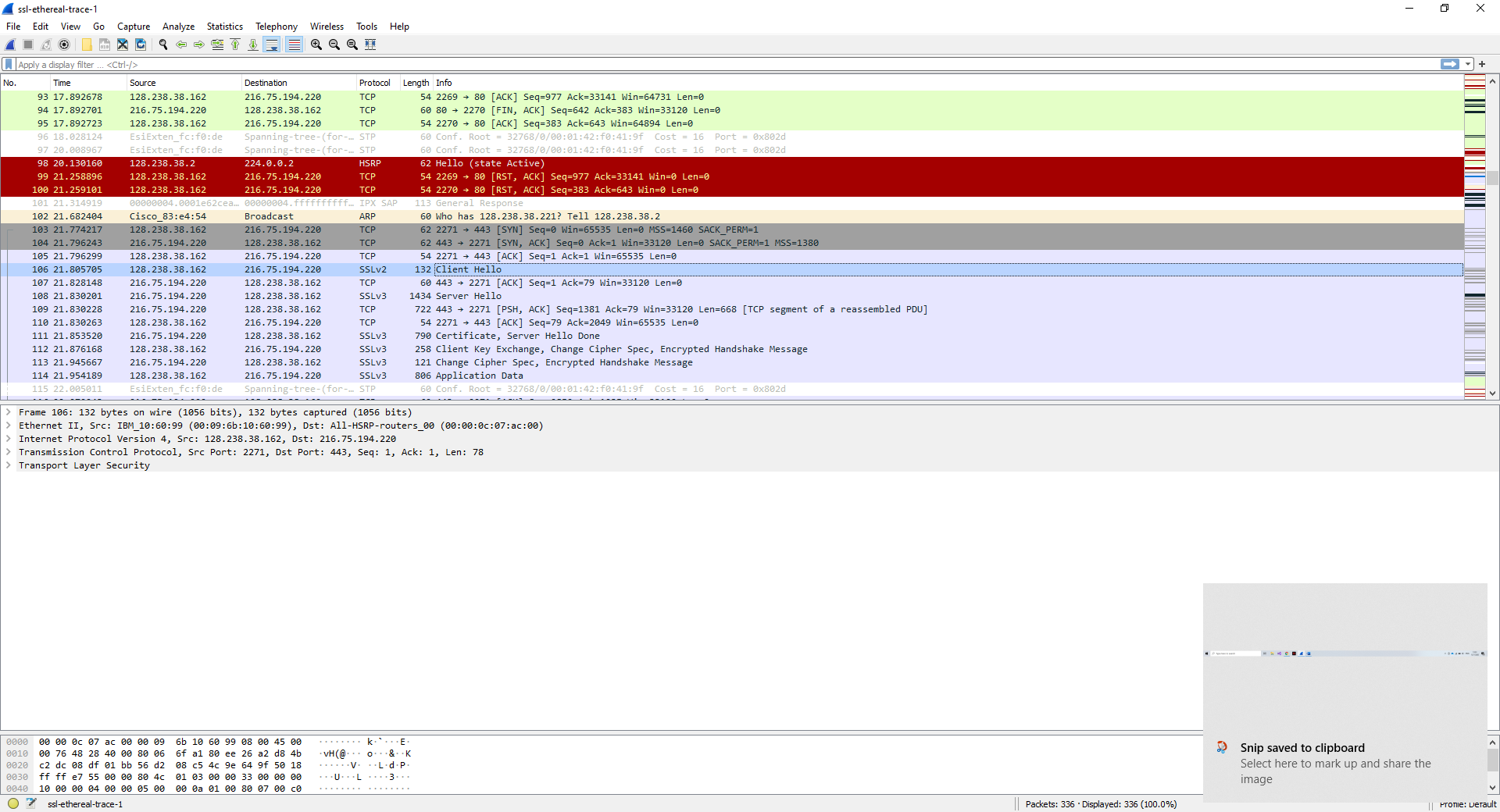
**Lab 8**

**Name: Nguyễn Đặng Anh Phương**

**Student ID: 1813621**

**Answer the questions:**

Screenshot for SSL Sessions (from packet trace the lab provided):



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 1:

Source: Client

Record : 1

- Type 1: Client Hello

Frame 2:

Source: Server

Records: 1

- Type 22: Handshake

Farme 3:

Source: Server

Records: 2

- Type 11: Certificate

- Type 14: Server Hello Done

Frame 4:

Source: Client

Records: 3

- Type 22: Handshake

- Type 20: Change Cipher Spec

- Type 22: Handshake

Frame 5:

Source: Server

Records: 2

- Type 20: Change Cipher Spec

- Type 22: Handshake

Frame 6:

Source: Client

Records: 1

- Type 23: Application Data

Frame 7:

Source: Server

Records: 1

- Type 23: Application Data

Frame 8:

Source: Client

Records: 1

- Type 23: Application

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

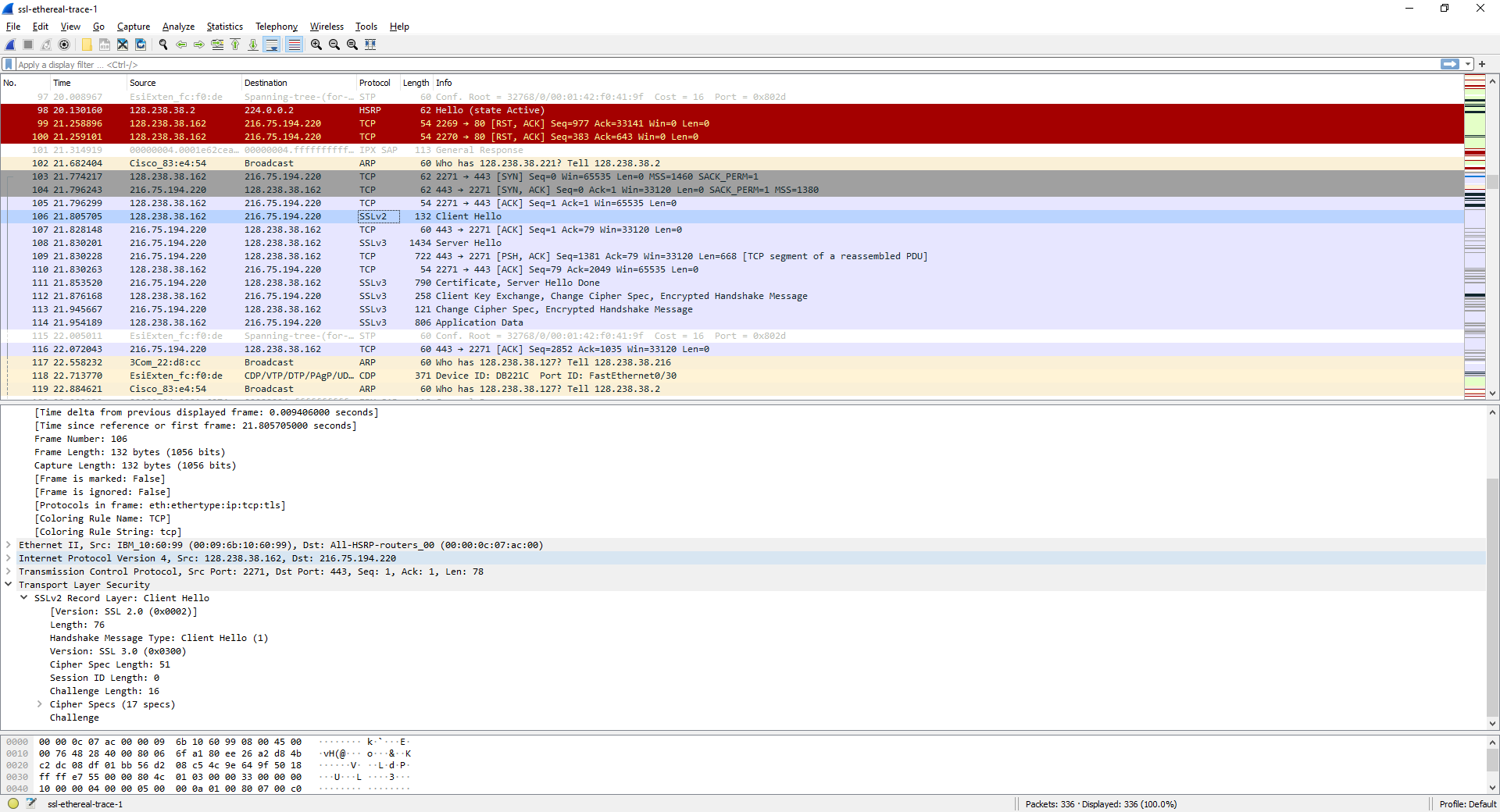
three fields and their lengths.

**Answer:**

- Content Type: 1 byte.

- Version: 2 bytes.

- Length: 2 bytes.

****

*Client Hello record screenshot*

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 value of content type: Client Hello (1)

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?

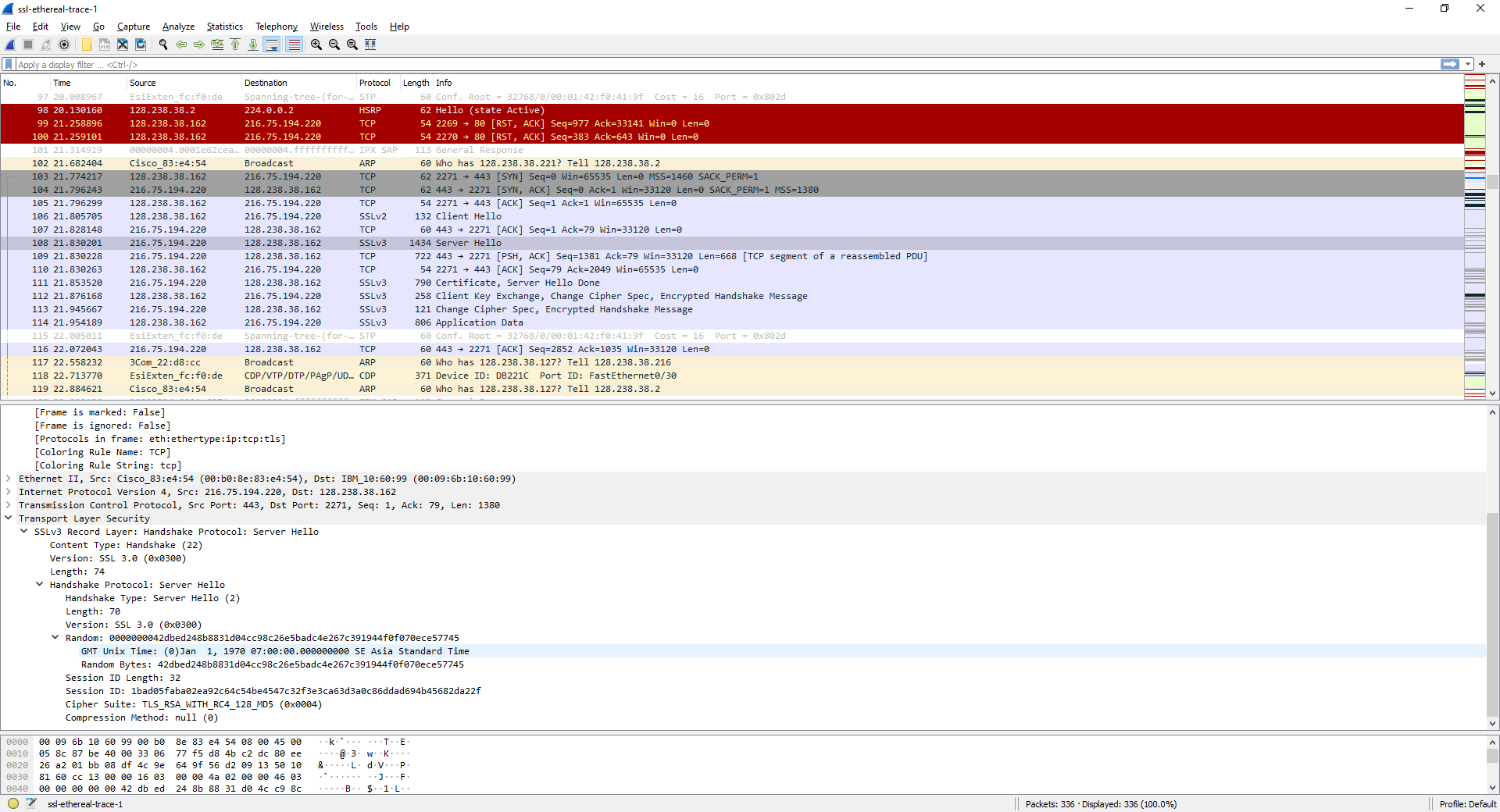
**Answer**: It does contain a challenge, the challenge’s value is [66 df 78 4c 04 8c d6 04 35 dc 44 89 89 46 99 09]

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:** Yes. The first listed suite is TLS\_RSA. The symmetric is RC4, the public-key is 128, the hash algorithm is MD5



*Server Hello record screenshot*

6. Locate the ServerHello SSL record. Does this record specify a chosen cipher

suite? What are the algorithms in the chosen cipher suite?

**Answer:** It has a cipher suite. The algoithm in the cipher suite 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:** The record doesn’t include any challenges. The nonce will show that they are duplicates and should be ignored.

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

**Answer:** Yes. To identify that a message is secure or not.

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:** The certificate must be contained in multiple frames because it’s too large (2684 bytes).

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. It’s used for verifying both parties completely understand the encryption method. The encryption also be encrypted (56 bytes).

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

record in your trace?

**Answer:** To tell the other party what Cipher version to use. The length is 1 byte.

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

**Answer:** PMS. By using the method in the previous message.

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. There is no difference.

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 application data is encrypted according to the server’s agreed on encryption method. Yes. No.

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

**Answer:** It’s so interesting to know how SSL works.