Computer Networks 1

Lab 8

Wireshark Lab: SSL v8.0

Student Name: **Nguyễn Quý Hải**

Student No.: **2052974**

I. Objectives

In this lab, we'll explore several aspects of the HTTP protocol:

- Investigate the IP protocol
- Focusing on the IP datagram
- Investigate the various fields in the IP datagram
- Study IP fragmentation in detail

II. Content

1. Capturing packets from an execution of traceroute

- Following the lab's guide.

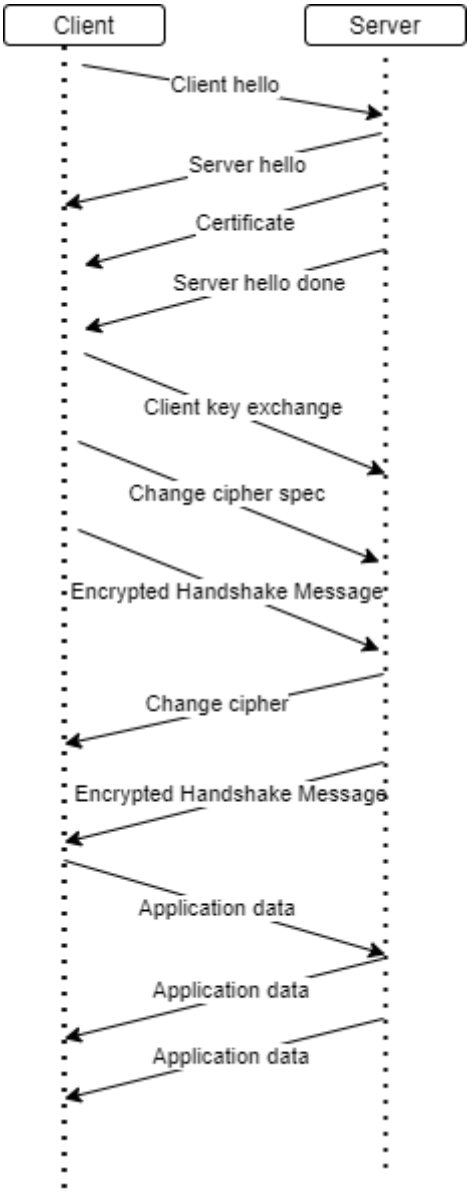
2. A look at the captured trace

- Q1: 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	SSL records	SSL type
106	Client	1	Client hello
108	Server	1	Server hello
111	Server	2	Certificate Server hello done
112	Client	3	Client Key Exchange Change Cipher Spec Encrypted Handshake Message
113	Server	2	Change Cipher Spec Encrypted Handshake Message
114	Client	1	Application data

122	Server	1	Application data
149	Server	1	Application data



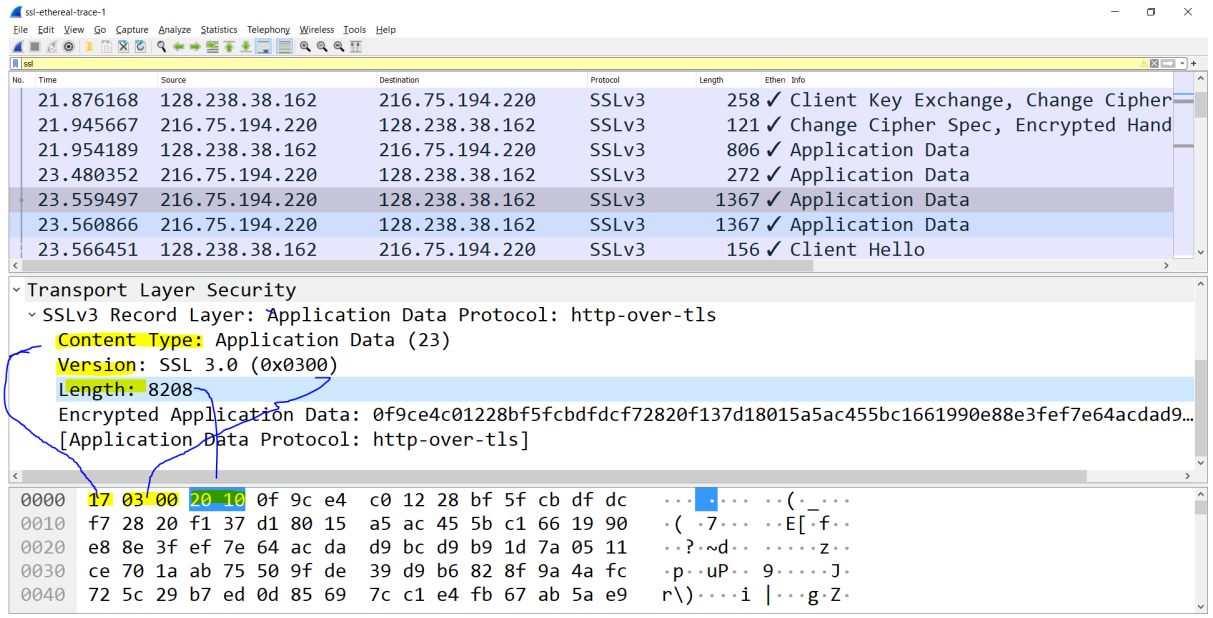
[Timing diagram between client and server]

My source link:
https://drive.google.com/file/d/1LGOCFhLzkXm01LXgA9WboECE7dF5fORW/view?usp=sharing

- Q2. 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.

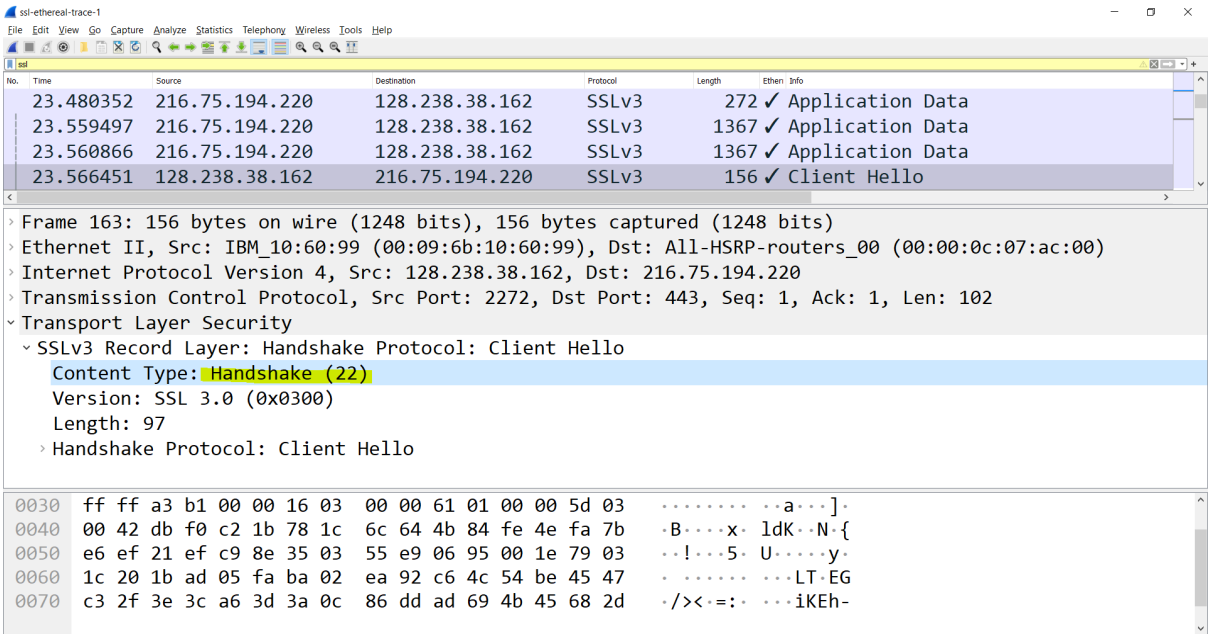
Answer:

- Content type: 1 byte
- Version: 2 bytes
- Length: 2 bytes



- Q3: 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?

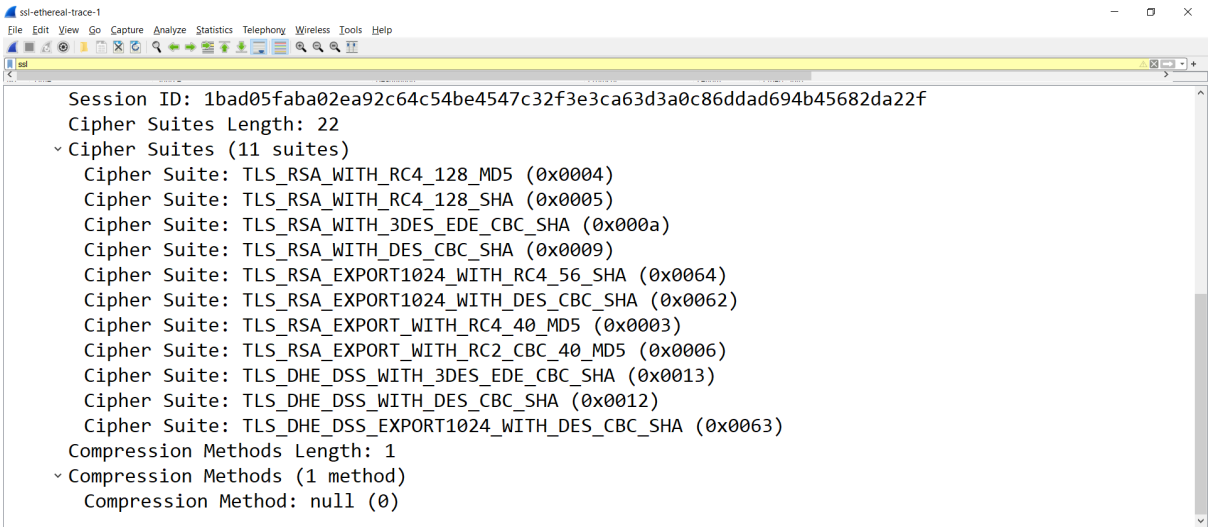
  Answer: It is 22 (Handshake)



- Q4. Does the ClientHello record contain a nonce (also known as a “challenge”)? If so, what is the value of the challenge in hexadecimal notation?

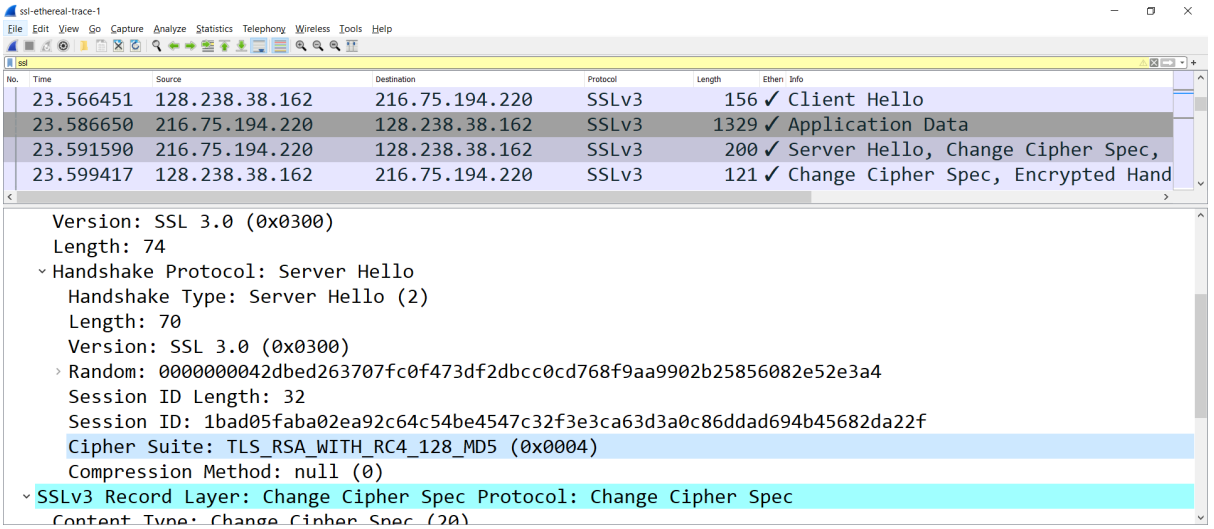
  Answer:
- Q5. Does the ClientHello record advertise the cyber suites it supports? If so, in the first listed suite, what are the public-key algorithm, the symmetric-key algorithm, and the hash algorithm?

  Answer: Yes
  - Public-key algorithm: RSA
  - Symmetric-key algorithm: RC4, DES, 3DES,
  - Hash algorithm: MD5, SHA



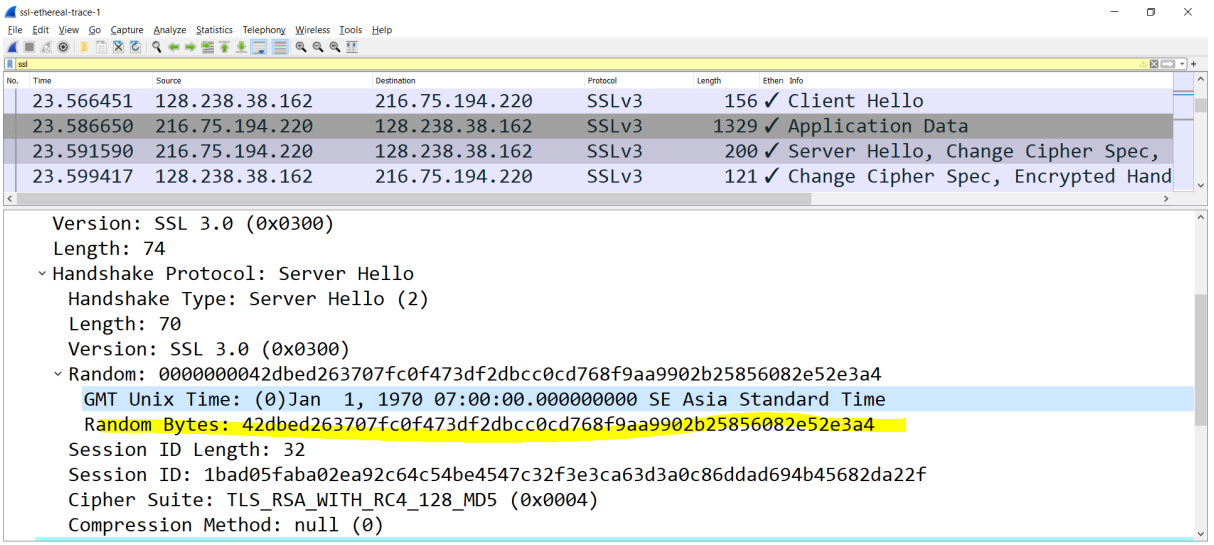
- Q6: Locate the ServerHello SSL record. Does this record specify a chosen cipher suite? What are the algorithms in the chosen cipher suite?

  Answer: Yes, it is Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)



- Q7. 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. Altogether, it is 32 bytes. 4 bytes for GMT Unix time and 28 bytes for data. The purpose of this is to prevent a replay attack.



- Q8. Does this record include a session ID? What is the purpose of the session ID?

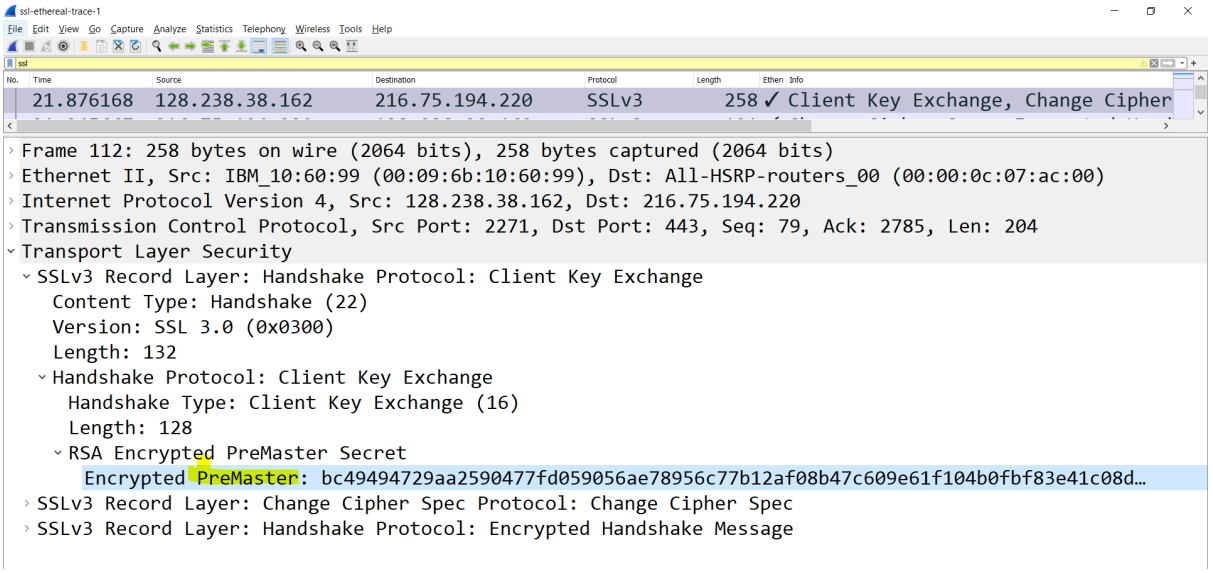
  Answer: Yes, as you can see in the screenshot above. The main purpose of the session ID is to identify a session, a series of related message exchanges. In E-commerce, it is often used to identify a user that has logged into a website.

- Q9. 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: There is no certificate in this record, it is in another record. It does fit into a single Ethernet frame.

- Q10: 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?

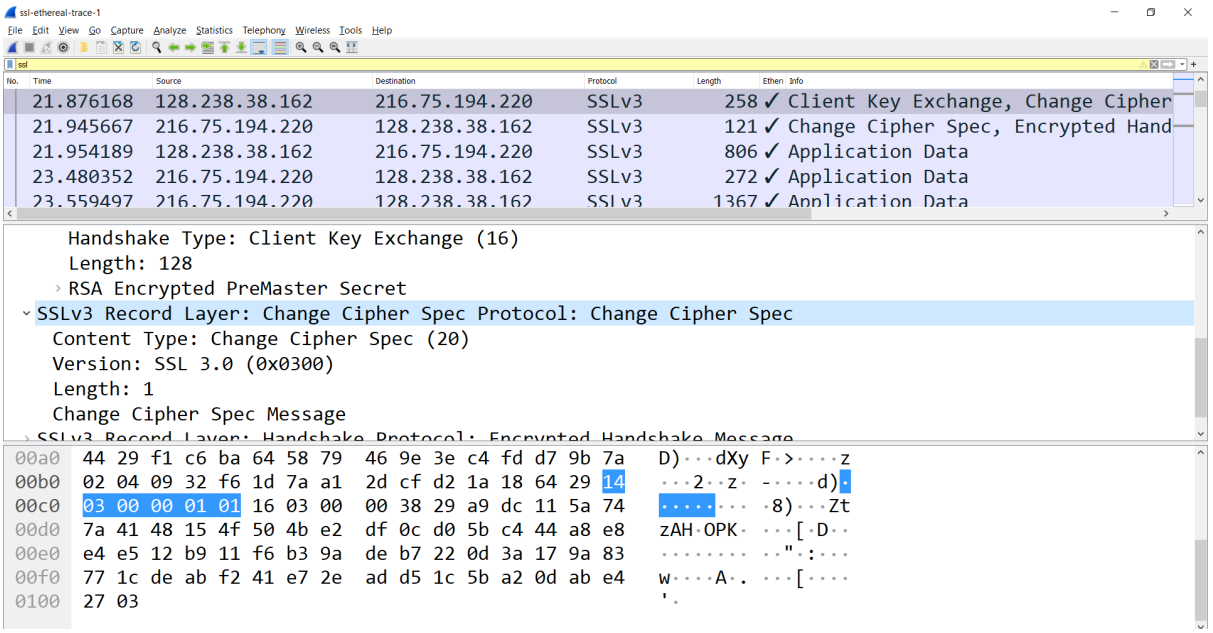
  Answer: Yes, it does contain a premaster secret. It is used by both the server and client to make a master secret, which is used to generate session keys for MAC and encryption. The secret gets encrypted using the server's public key, which the client extracted from the certificate sent by the server. The secret is 128 bytes long



- Q11: What is the purpose of the Change Cipher Spec record? How many bytes is the record in your trace?

  Answer: The purpose of the Change Cipher Spec record is to indicate that the contents of the following SSL records sent by the client (data, not header) will be encrypted. The record in my trace is 6 bytes:

  - 1 byte for Content type,
  - 2 bytes for version,
  - 2 bytes for length
  - And the last for Change Cipher Spec Message



- Q12. In the encrypted handshake record, what is being encrypted? How?

Answer: In the encrypted handshake record, a MAC of the concatenation of all the previous handshake messages sent from this client is generated, encrypted and sent to the server.

- Q13. 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 will also send a Change Cipher Spec record and encrypted handshake to the client.
  - The server's encrypted handshake record is different from that sent by the client because it contains the concatenation of all the handshake messages sent from the server rather than from the client. Otherwise the records would end up being the same.

- Q14: 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: Application data is encrypted using symmetric key encryption algorithm chosen in the handshake phase (RC4) using the keys generated using the pre-master key and nonces from both client and server. The client encryption key is used to encrypt the data being sent from client to server and the server encryption key is used to encrypt the data being sent from the server to the client.

- Q15. 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.
  Also, 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 the client. After a response from the client then application data can be sent.