Computer Networks

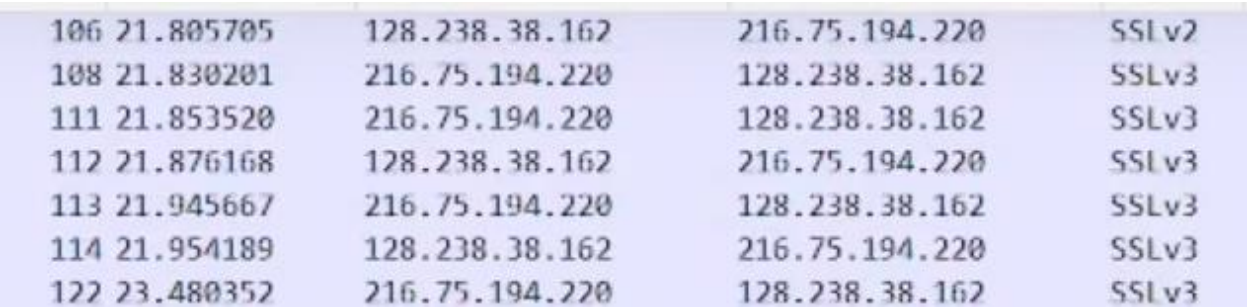
Lab 8

SSL v8.0

Student Name: Dương Gia Lâm

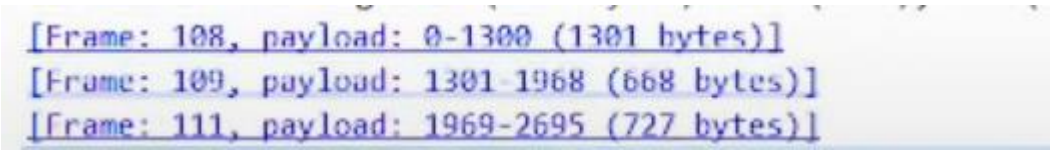
Student No:2211806

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.



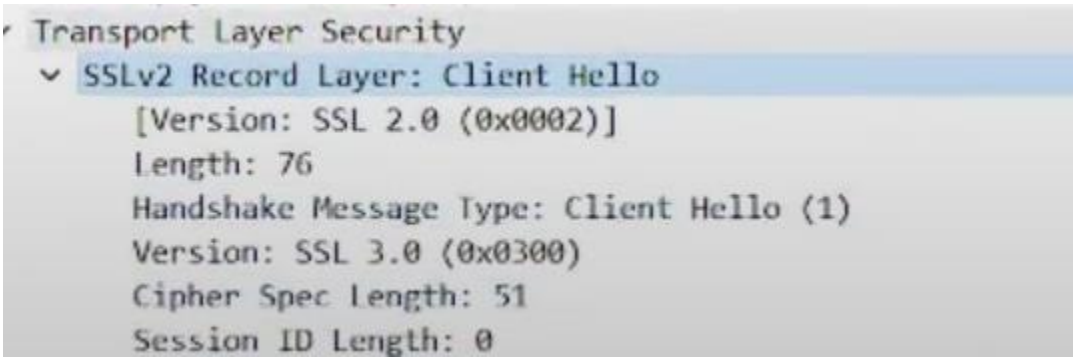
106	21.805705	128.238.38.162	216.75.194.220	SSLv2
108	21.830201	216.75.194.220	128.238.38.162	SSLv3
111	21.853520	216.75.194.220	128.238.38.162	SSLv3
112	21.876168	128.238.38.162	216.75.194.220	SSLv3
113	21.945667	216.75.194.220	128.238.38.162	SSLv3
114	21.954189	128.238.38.162	216.75.194.220	SSLv3
122	23.480352	216.75.194.220	128.238.38.162	SSLv3

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.



```
[Frame: 108, payload: 0-1300 (1301 bytes)]
[Frame: 109, payload: 1301-1968 (668 bytes)]
[Frame: 111, payload: 1969-2695 (727 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?



```
Transport Layer Security
  SSLv2 Record Layer: Client Hello
      [Version: SSL 2.0 (0x0002)]
      Length: 76
      Handshake Message Type: Client Hello (1)
      Version: SSL 3.0 (0x0300)
      Cipher Spec Length: 51
      Session ID Length: 0
```

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?

this is challenge in heximal

```
12 00 00 63 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?

ở dòng đầu tiên dùng thuật toán RSA cho chữ ký và RC4 cho mã hóa dữ liệu với độ dài 128-bit, và MD5 cho hàm băm.

```
Cipher Specs (17 specs)
   Cipher Spec: TLS_RSA_WITH_RC4_128_MD5 (0x000004)
```

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

```
Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
```

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?

```
Random: 0000000042dbed248b8831d04cc98c26e5badc4e267c391944f0f070ece57745
```

nonce để ngăn chặn các cuộc tấn công replay

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

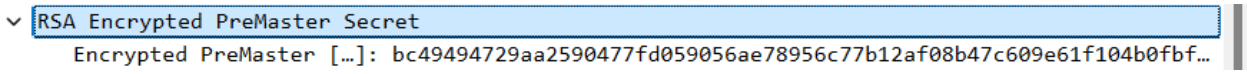
```
Session ID: 1bad05faba02ea92c64c54be4547c32f3e3ca63d3a0c86ddad694b45682da22f
```

quản lý phiên làm việc và **tối ưu hóa hiệu suất** bằng cách cho phép **tiếp tục phiên làm việc** mà không phải bắt tay lại từ đầu

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?

don’t have a certificate

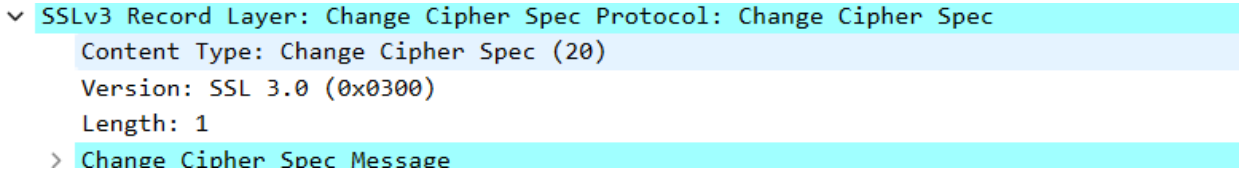
10. Locate the client key exchange record. Does this record contain a pre-master secret? What is this secret used for? Is the secret encrypted? If so, how? How long is the encrypted secret?



- **Pre-master secret** được sử dụng để tạo ra các **session keys**. Các **session keys** này sẽ được sử dụng trong giai đoạn mã hóa và giải mã dữ liệu trong phiên làm việc giữa client và server.
- Mỗi phiên làm việc sẽ có một **session key** riêng biệt, giúp bảo vệ dữ liệu trong suốt phiên làm việc đó.

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

TLS/SSL giúp thông báo cho cả **client** và **server** rằng họ sẽ bắt đầu sử dụng các **session keys** mới.



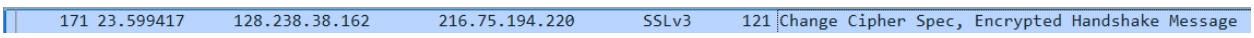
12. In the encrypted handshake record, what is being encrypted? How?

Các dữ liệu được mã hóa trong **Encrypted Handshake** thường là:

- **Server Hello** và **Client Hello**: Thông tin bắt tay được bảo vệ bằng cách sử dụng các **session keys**.

Mã hóa thường được thực hiện với các thuật toán như **AES**, **RC4**, hoặc **ChaCha20**

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?



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?

dữ liệu ứng dụng được mã hóa bằng **mã hóa đối xứng** (symmetric encryption) sau khi thiết lập một kênh mã hóa an toàn giữa client và server

Wireshark có khả năng phân biệt giữa **dữ liệu ứng dụng đã mã hóa** và **MAC** trong bản ghi TLS.