Trần Tinh Chí – 1351063
Lê Lưu Quỳnh Giao – 1351012
Nguyễn Đắc Phúc – 1351060

Wireshark SSL

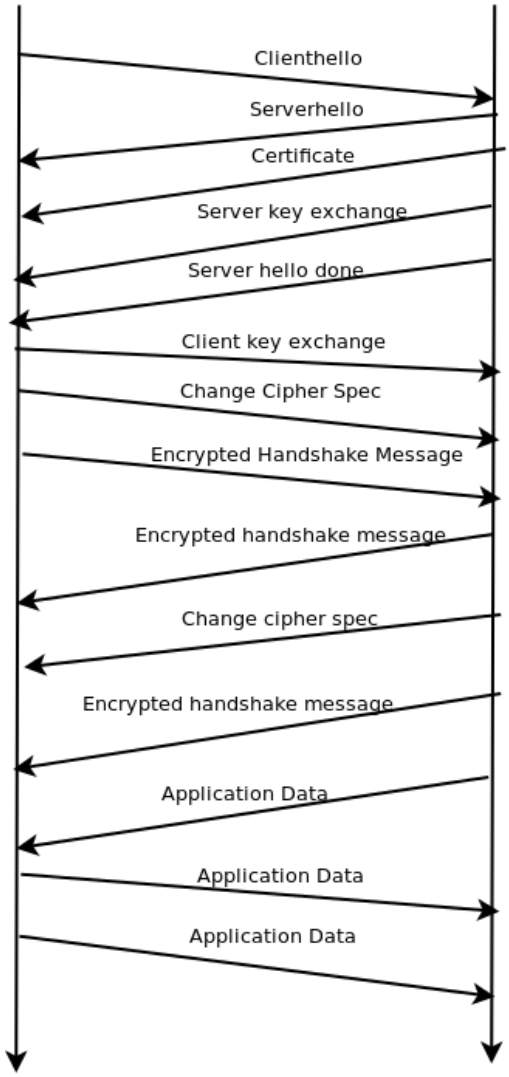
[1] For each of the first 8 Ethernet frames, specify the source of the frame (client or server), determine the number of SSL records that are included in the frame, and list the SSL record types that are included in the frame. Draw a timing diagram between client and server, with one arrow for each SSL record.

Frame	Source	Number of SSLs	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
127	Server	1	Application Data

The following diagram is generated by Wireshark Flow Graph, and it is not full graph.

The following diagram is drawn manually.
The left side is client, and the right side is server.

Trần Tinh Chí – 1351063
Lê Lưu Quỳnh Giao – 1351012
Nguyễn Đắc Phúc – 1351060



[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.

```
Secure Sockets Layer
▼ SSLv3 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: SSL 3.0 (0x0300)
      Length: 74
```

Content Type : 1 byte
Version : 2 bytes
Length : 2 bytes

(Note that I only get all of those 3 fields in SSLv3, not SSLv2)

Trần Tinh Chí – 1351063
Lê Lưu Quỳnh Giao – 1351012
Nguyễn Đắc Phúc – 1351060

[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?

```
  163 23.566451  128.238.38.162  216.75.194.220  SSLv3   156 Client Hello
  165 23.586650  216.75.194.220  128.238.38.162  SSLv3  1329 Application Da
  169 23.591590  216.75.194.220  128.238.38.162  SSLv3   200 Server Hello,
    Checksum: 0xa3b1 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▶ [SEQ/ACK analysis]
Secure Sockets Layer
  ▼ SSLv3 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: SSL 3.0 (0x0300)
      Length: 97
    ▶ Handshake Protocol: Client Hello
```

Because frame 106 is SSLv2, thus I did not find any "Content type" field. Therefore, I choose frame 163, which is the 2nd Client Hello frame.

- The value is Handshake (is 22).

[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?

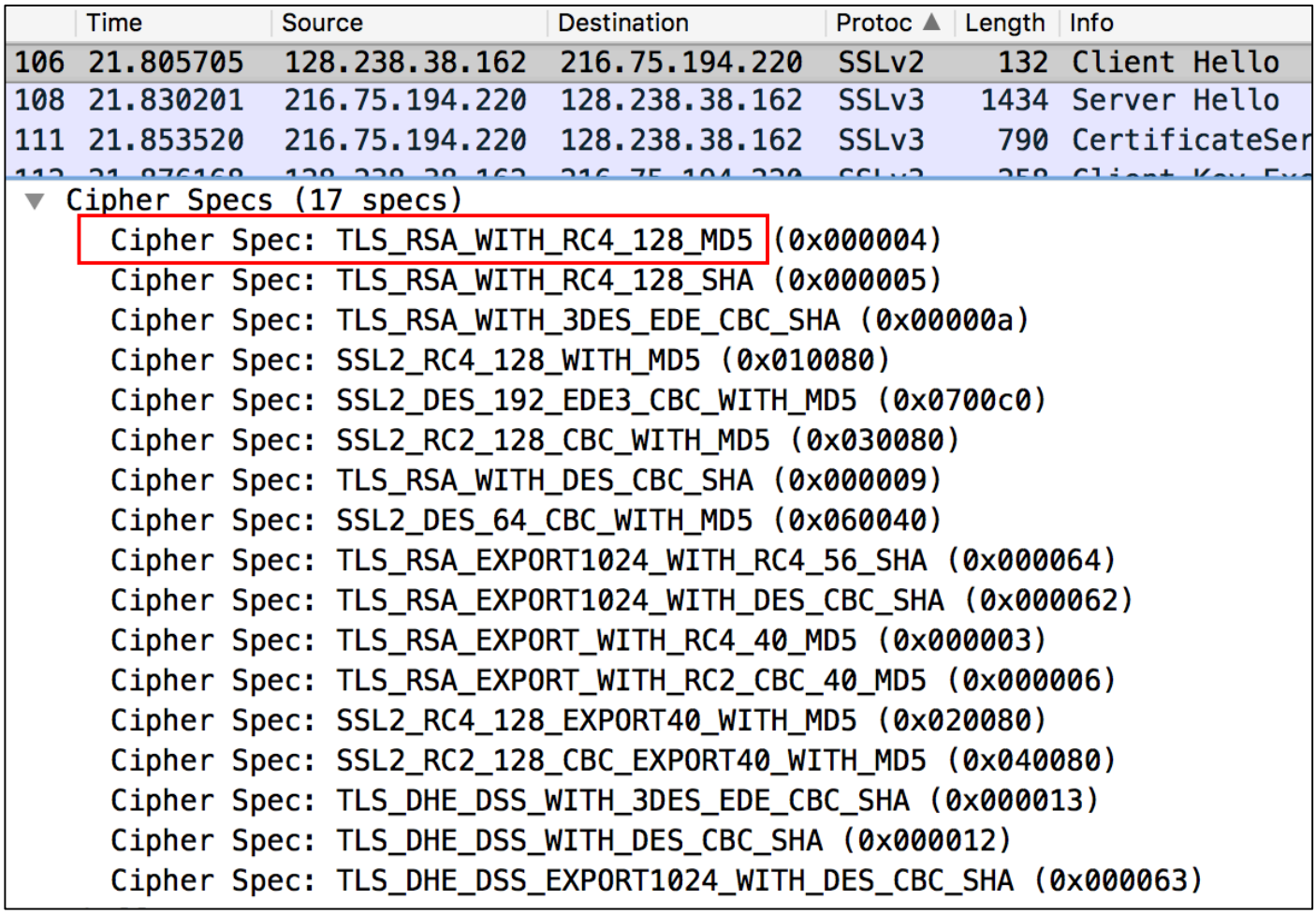
```
  ▼ SSLv2 Record Layer: Client Hello
      [Version: SSL 2.0 (0x0002)]
      Length: 76
      Handshake Message Type: Client Hello (1)
      Version: SSL 3.0 (0x0300)
      Cipher Spec Length: 51
      Session ID Length: 0
      Challenge Length: 16
    ▶ Cipher Specs (17 specs)
      Challenge

0020  c2 dc 08 df 01 bb 56 d2  08 c5 4c 9e 64 9f 50 18   ......V. ..L.d.P.
0030  ff ff e7 55 00 00 80 4c  01 03 00 00 33 00 00 00   ...U...L ....3...
0040  10 00 00 04 00 00 05 00  00 0a 01 00 80 07 00 c0   ........ ........
0050  03 00 80 00 00 09 06 00  40 00 00 64 00 00 62 00   ........ @..d..b.
0060  00 03 00 00 06 02 00 80  04 00 80 00 00 13 00 00   ........ ........
0070  12 00 00 63 66 df 78 4c  04 8c d6 04 35 dc 44 89   ...cf.xL ....5.D.
0080  89 46 99 09                                       .F..
```

Yes, it does. It is in frame 106 (the SSLv2 one).
The client hello challenge value is 66 df 78 4c 04 8c d6 04 35 dc 44 89 89 46 99 09

Trần Tinh Chí – 1351063
Lê Lưu Quỳnh Giao – 1351012
Nguyễn Đắc Phúc – 1351060

[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?

Yes, it does.



The first listed suite:

- 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?

The cipher suite uses

- RSA for public key crypto
- RC4 for the symmetric-key cipher

Trần Tinh Chí – 1351063
Lê Lưu Quỳnh Giao – 1351012
Nguyễn Đắc Phúc – 1351060

- MD5 hash algorithm.

```
Handshake Protocol: Server Hello
   Handshake Type: Server Hello (2)
   Length: 70
   Version: SSL 3.0 (0x0300)
▶  Random
   Session ID Length: 32
   Session ID: 1bad05faba02ea92c64c54be4547c32f3e3c
   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
      GMT Unix Time: Jan  1, 1970 08:00:00.000000000 IDT
      Random Bytes: 42dbed248b8831d04cc98c26e5badc4e267c391944f0f070...
```

Yes, it includes a nonce in the Random field.
The nonce has length of 32 bits long:

- 28 bits for random data
- 4 bits for the time.

It is used to prevent a replay attack.

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

```
Handshake Protocol: Server Hello
   Handshake Type: Server Hello (2)
   Length: 70
   Version: SSL 3.0 (0x0300)
▶  Random
   Session ID Length: 32
   Session ID: 1bad05faba02ea92c64c54be4547c32f3e3c
   Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
```

It is a unique identifier for the SSL session.
The client may go back to the same session later by using the server provided session ID when it sends the ClientHello.

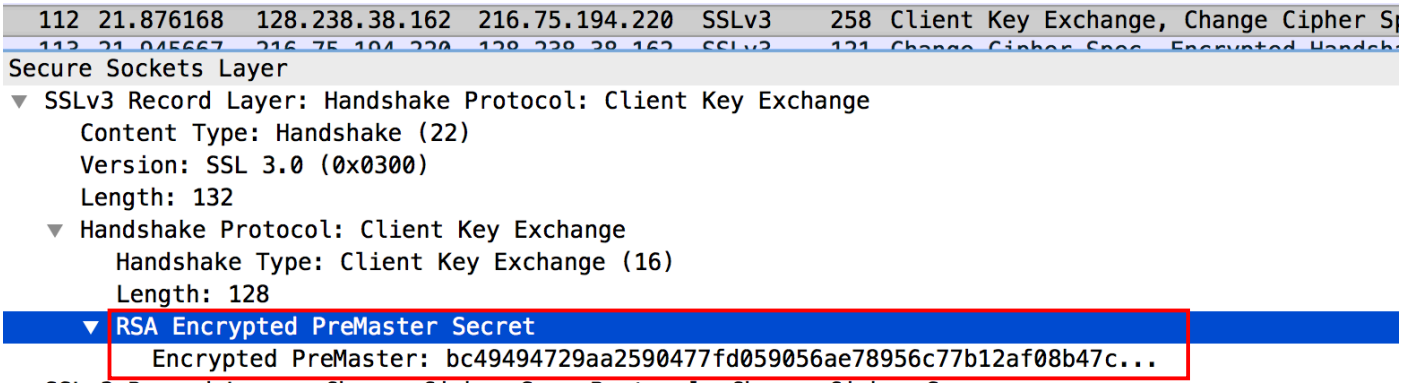
[9] Does this record contain a certificate, or is the certificate included in a separated record. Does the certificate fit into a single Ethernet frame?

No, it does not contain the Certificate.
The certificate is in frame 111.
Furthermore, I see that the Certificate is in frame 111 only, thus it fits into a single Ethernet frame.

Trần Tinh Chí – 1351063
Lê Lưu Quỳnh Giao – 1351012
Nguyễn Đắc Phúc – 1351060

[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?

Yes, it contains a Pre-Master secret.



The server and client use Pre-master secret to make a master secret

- It is used to generate session keys for MAC and encryption.

The secret is encrypted using the public key of the server, which was extracted by the client from the certificate sent by the server.
The secret has the length of 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 record is used to indicate that the SSL records' contents which is sent by the client (only data, not header) will be encrypted.
This record has the length of 6 bytes:

- 5 for the header
- 1 for the message segment.

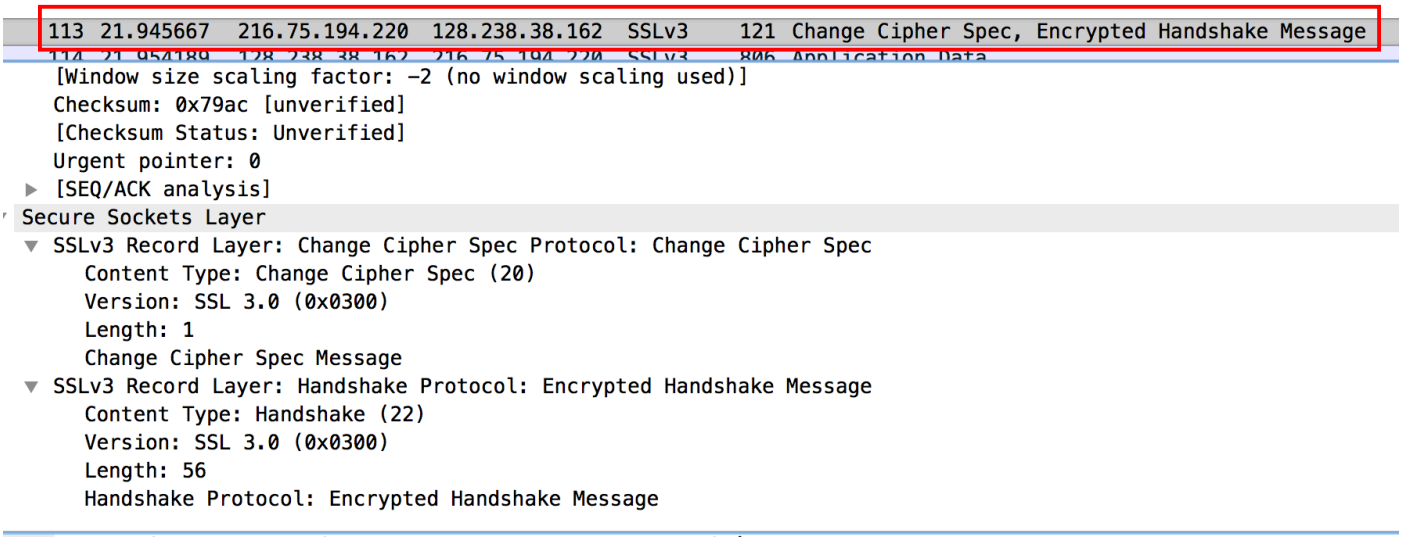
[12] In the encrypted handshake record, what is being encrypted? How?

The data type contains a *fragment* of the application data stream, followed by a MAC on the fragment, then padding and padding length, are all encrypted.

[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?

Yes, it does.

Trần Tinh Chí – 1351063
Lê Lưu Quỳnh Giao – 1351012
Nguyễn Đắc Phúc – 1351060



The Change Cipher records are the same for server and client.

The server's Encrypted Handshake record is different from the one 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.

[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?

Application data is encrypted using Symmetric Key encryption algorithm chosen in the handshake phase (in this case is 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.

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

I see that the frame 106 uses SSLv2 protocol, and the later frames use SSLv3.