ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA KHOA HỌC & KỸ THUẬT MÁY TÍNH

MẠNG MÁY TÍNH (CO3094)

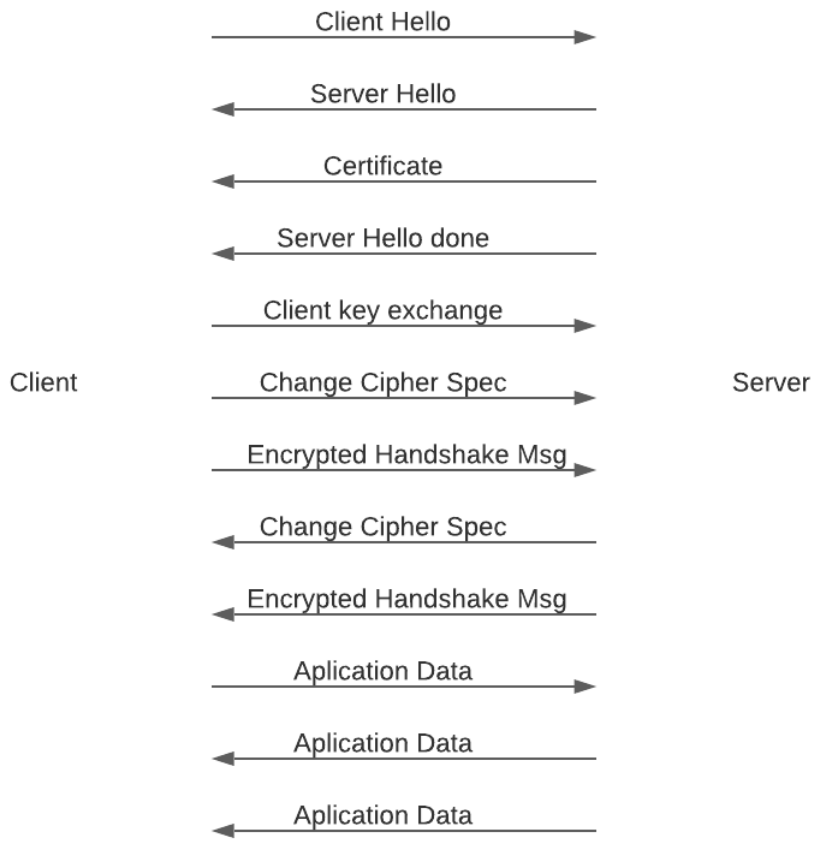
Báo cáo Lab 8: Wireshark Lab – SSL

Giảng viên: Nguyễn Tấn Đạt
SV thực hiện: Đinh Như Tân – 1915040

Tp. Hồ Chí Minh, Tháng 10/2021

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	Frame Source of the frame	Number of SSL record	SSL record 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

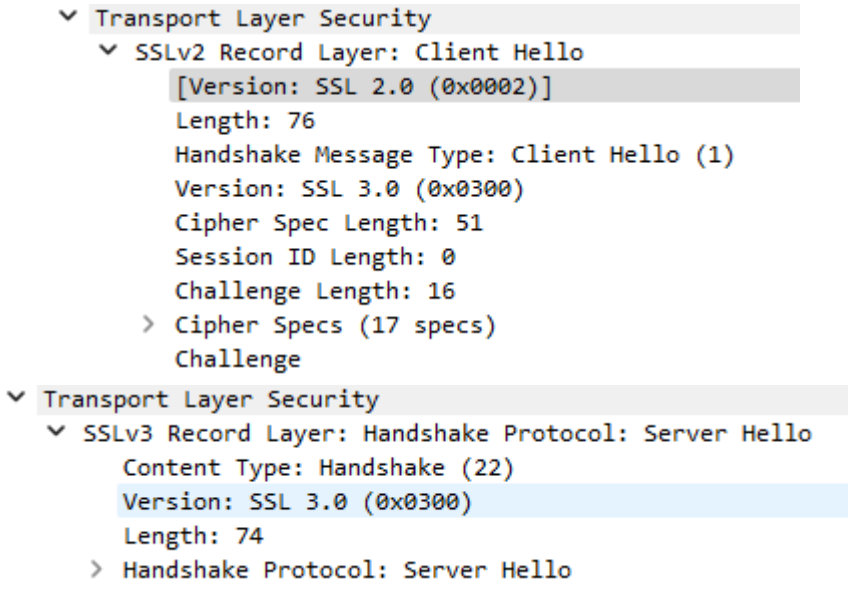


2. Each of the SSL records begins with the same three fields (with possibly different values). One of these fields is "content type" and has length of one byte. List all three fields and their lengths

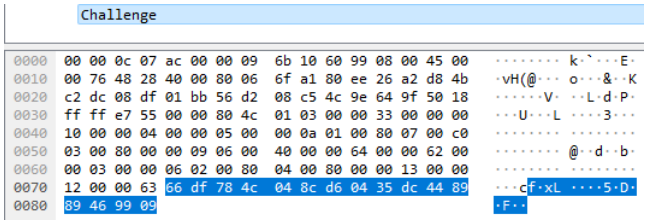
   - *Content type: 1 byte*

- *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?
   The content type is 22, for Handshake Message, with a handshake type of 01, Client Hello



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?
   Value of the challenge: 66df784c048cd60435dc448989469909



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?
   The first suite uses RSA for public-key algorithm, RC4 for symmetric-key algorithm and MD5 for hash algorithm.

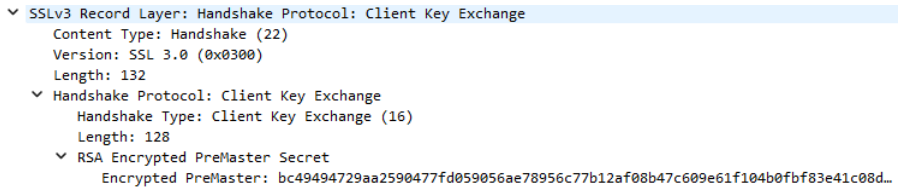
6. Locate the ServerHello SSL record. Does this record specify a chosen cipher suite? What are the algorithms in the chosen cipher suite?
   The cipher suite uses RSA for public-key algorithm, RC4 for symmetric-key algorithm and MD5 for hash algorithm

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?
Yes, the nonce is 32 bytes long (4 bytes time + 28 bytes data). The purpose is to prevent a replay attack.

8. Does this record include a session ID? What is the purpose of the session ID?
Yes. It provides a unique persistent identifier for the SSL session which is sent in the clear. The client may resume the same session later by using the server provided session ID when it sends the Client Hello.

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?
There is no certificate, it is in another record. It does fit into a 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?
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.



11. What is the purpose of the Change Cipher Spec record? How many bytes is the record in your trace?
The purpose of the Change Cipher Spec record is to indicate that the content of the following SSL records sent by the client (data, not header) will be encrypted. This record is 6 bytes long (5 bytes header+1 byte message segment).

12. In the encrypted handshake record, what is being encrypted? How?
In the encrypted handshake record, a MAC of the concatenation of all the previous handshake messages sent from this client is generated and sent to the server.

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, the server will also send a Change Cipher Spec record and encypted handshake to the client. The server's encypted handshake record is different from that sent by 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 encypted 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

15. Comment on and explain anything else that you found interesting in the trace.
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 client. After a response from the client then application data can be sent.