COMPUTER NETWORK LAB

LAB 8

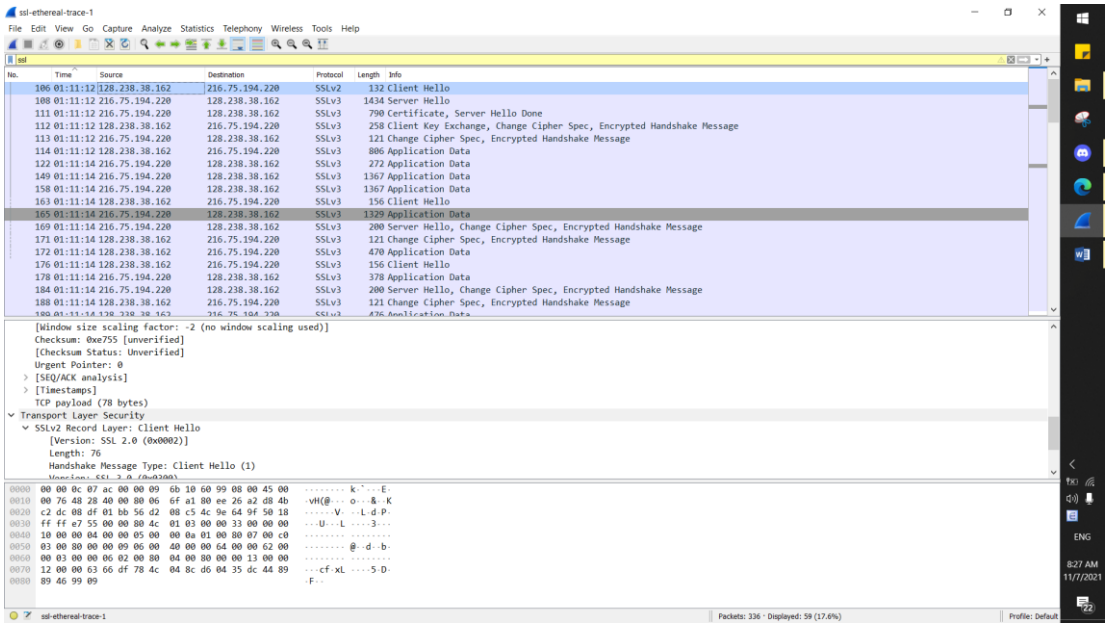
Name: Đinh Hoàng Anh

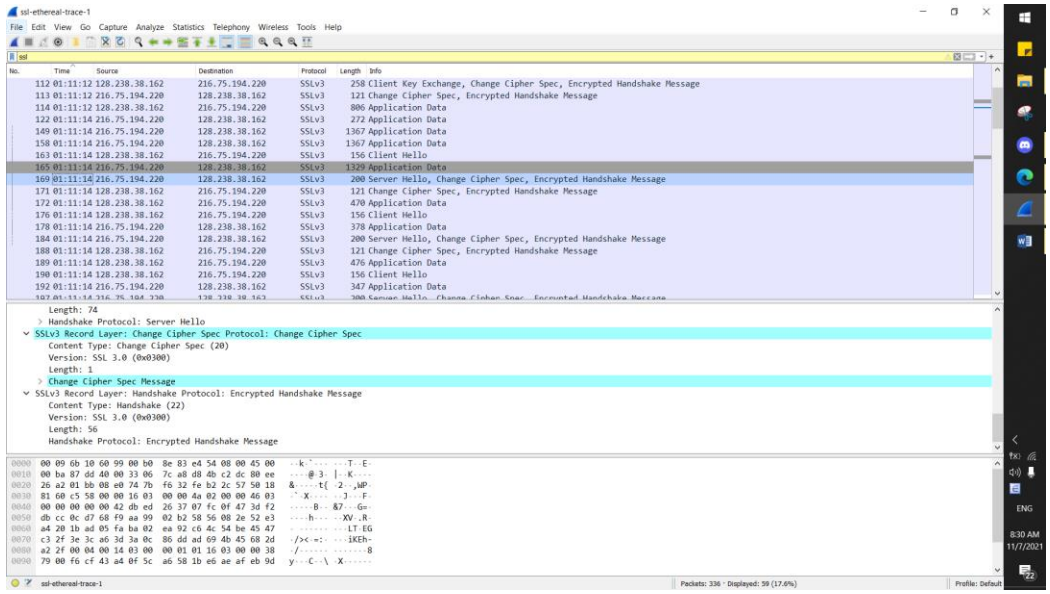
Student ID: 1952553

LAB 8

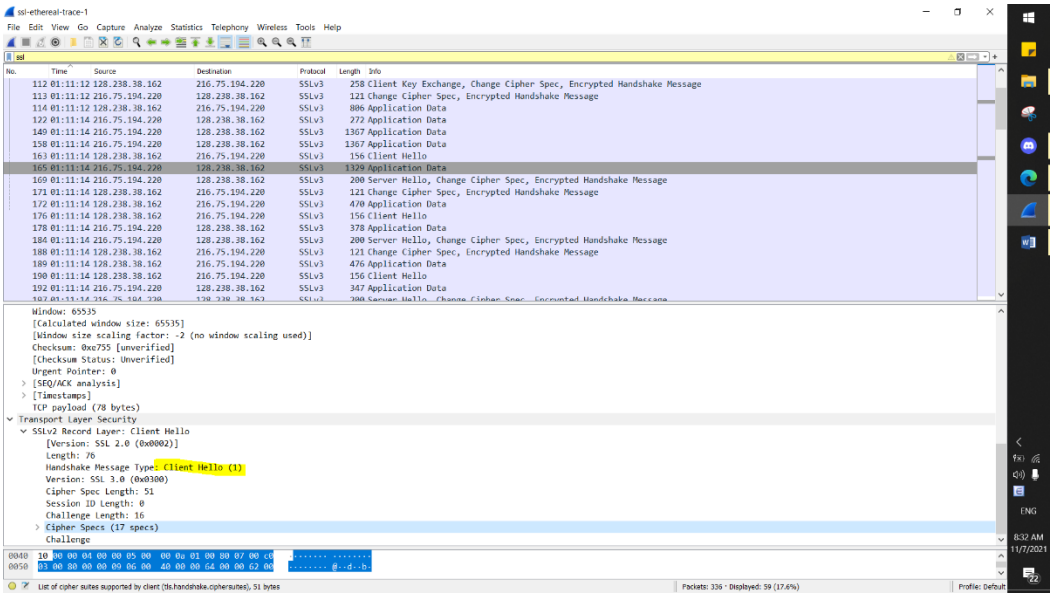
1.

Frame	Source	Destination	SSL Count	SSL Type
106	128.238.38.162	216.75.194.220	1	Client Hello
108	216.75.194.220	128.238.38.162	1	Server Hello
111	216.75.194.220	128.238.38.162	2	Server Hello Done
112	128.238.38.162	216.75.194.220	3	Client Key Exchange
113	216.75.194.220	128.238.38.162	2	Change Cipher Spec
114	128.238.38.162	216.75.194.220	1	Application Data
122	216.75.194.220	128.238.38.162	1	Application Data
149	216.75.194.220	128.238.38.162	1	Application Data





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



3. The content type is 22, for Handshake Message, with a handshake type of 01, Client Hello

4. 66 df 78 4c 04 8c d6 04 35 dc 44 89 89 46 99 09

5. Public key algorithm: RSA

Symmetric-key algorithm: RC4

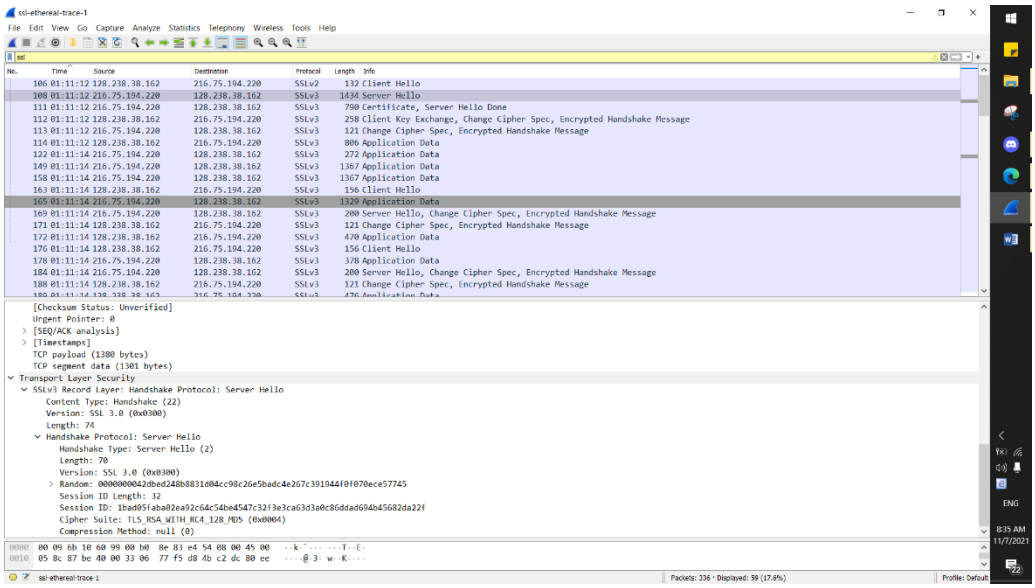
Hash algorithm: MD5

6. Public key algorithm: RSA

Symmetric-key algorithm: RC4

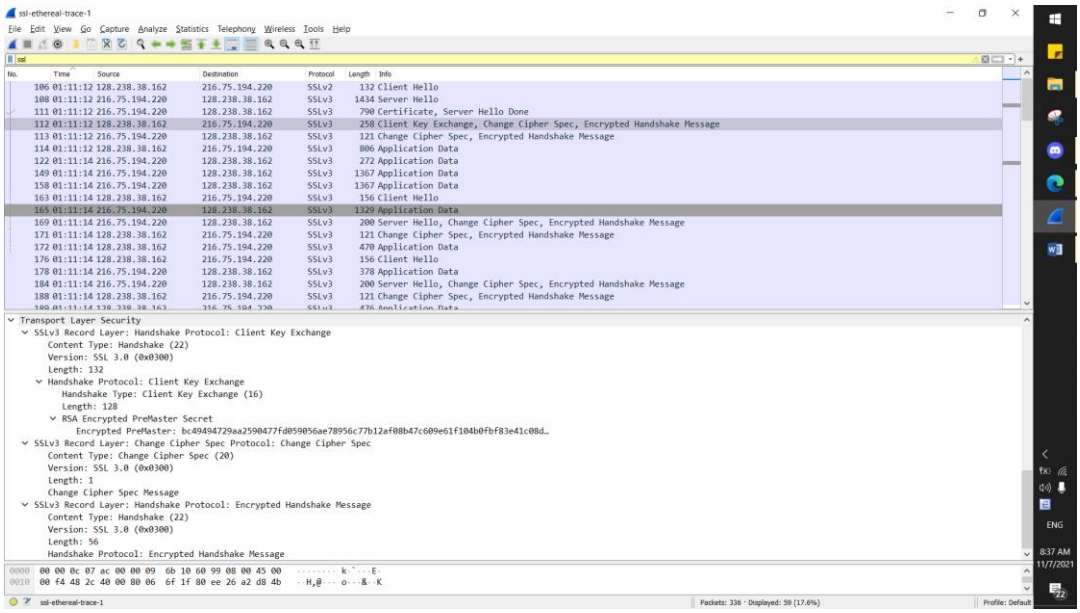
Hash algorithm: MD5

7. Yes, it is 32 bits long (28bits data + 4 bits time), it is used for attack preventing



8. Yes, the session ID in the record is an identifier for SSL session. This ID could let the client to resume the session later by using the session ID.

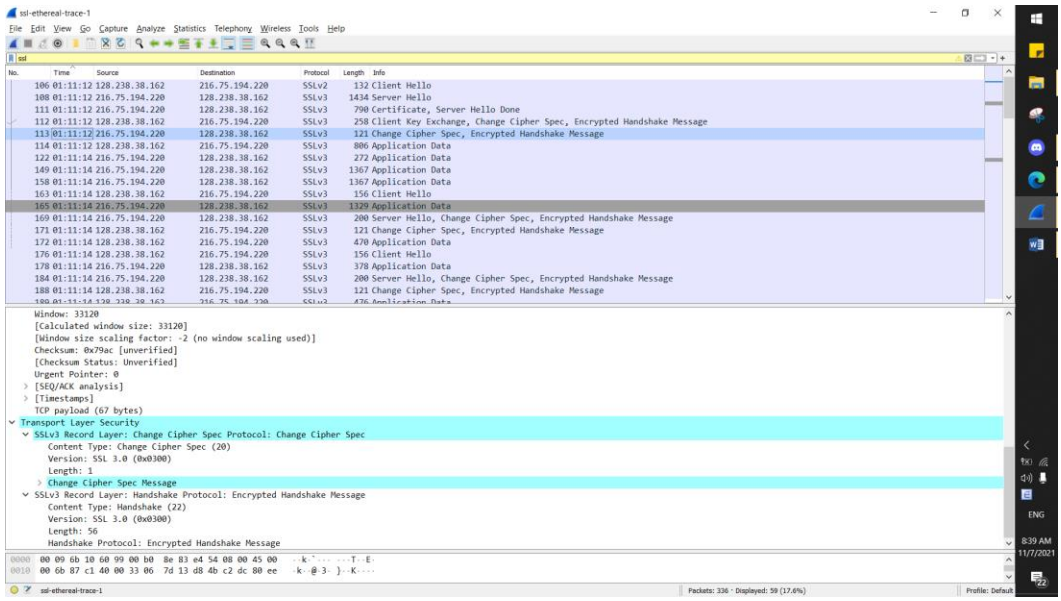
9. No, there is no certificate in this record. The certificate is in the separate record. Yes, the certificate fit into a single Ethernet frame.



10. Yes, this record contain a pre-master secret.

This secret is used for creating master secret

The secret is encrypted by public key, the encrypted secret is 120 bytes



11. Purpose of the Change Cipher Spec record is: used to indicate the content of the next SSL records will be encrypted. It is 6 bytes.

12. All handshake messages and MAC addresses are concatenated and encrypted. They are sent to the server

13. Yes, the server also send a change cipher record and an encrypted handshake

15. No comment