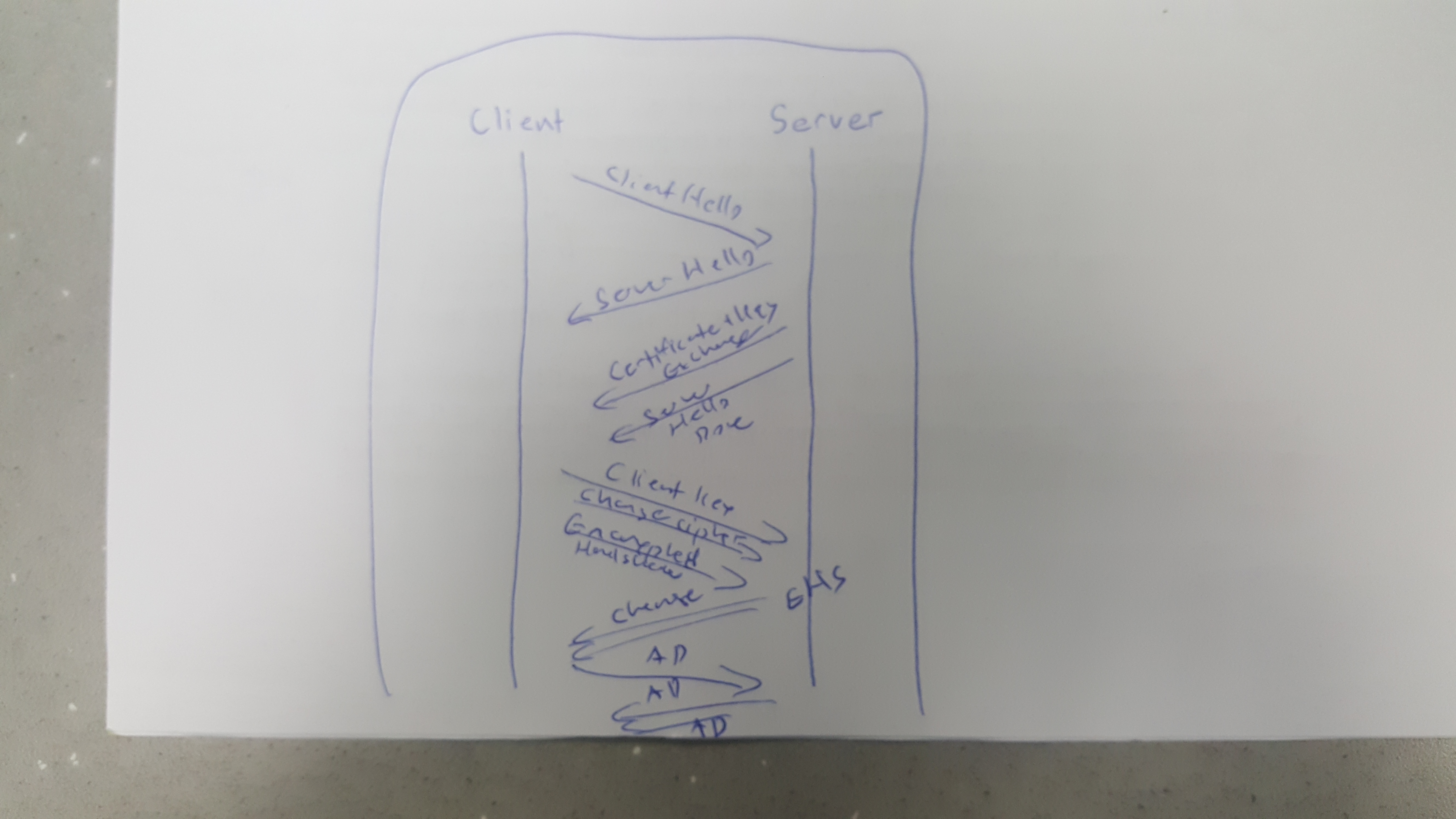
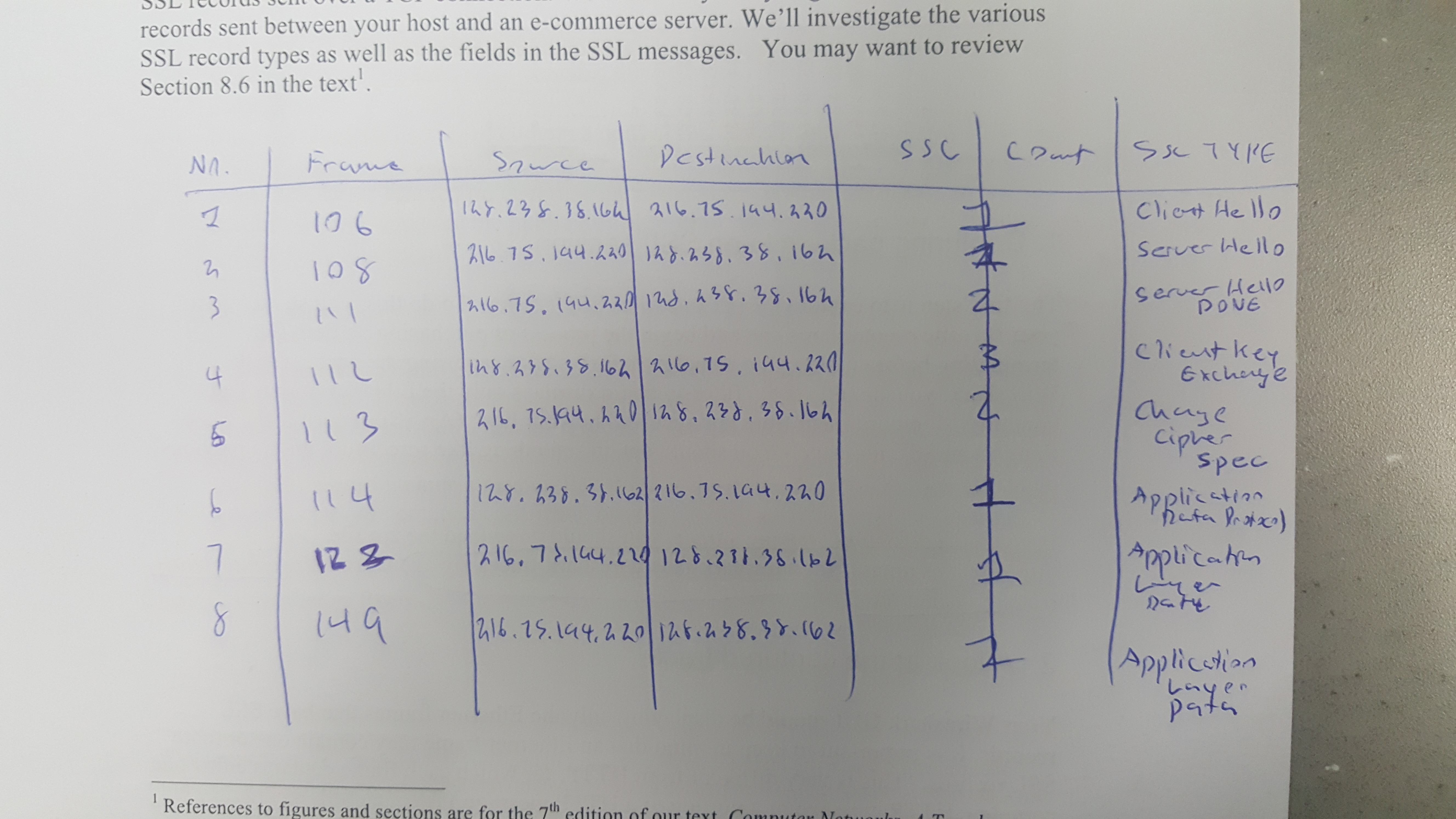
Franklin Nuth

Professor Ronny Bull

CSC323-A

November 21, 2017

**SSL**

1. 
2. The three content fields and their lengths are Content Type (1), Version (2), and Length (2).
3. The value of the Content Type in ClientHello is 22.
4. Yes, the ClientHello record does contain a nonce. The value of the challenge in hexadecimal notation is 04 8c d6 04 35 dc 44 89 84 49 99 09.
5. No, it does not advertise the cyber suites it supports.
6. Yes, the record specified a chosen cipher suite. The algorithms in the cyber suite are RSA, RCH, and MD5.
7. No, the record does not contain a nonce. The purpose of nonces in SSL is used to prevent attacks.
8. Yes, it does include a session ID. The purpose of the session ID is to keep SSL sessions.
9. No, this record does not contain a certificate. The certificate is included in a different record. Yes, it can fit into a single Ethernet frame.
10. Yes, client key exchange record contains a pre-master secret. This secret is used for session key. It is encrypted, and it is 128 bits long.
11. The purpose of the Change Cipher Record is to indicate the next SSL record encryption. The record in the trace is 5 bits long.
12. In the encrypted handshake record, the handshakes messages and MACs are being encrypted by being sent to the server.
13. Yes, the server’s encrypted handshake contains all messages. The records are different in that the client received the rest of the messages.
14. The application data is being encrypted through an algorithm. Yes, it included a MAC. No, Wireshark does not distinguish between the encrypted data and the MAC.
15. I find nothing strange about this trace.