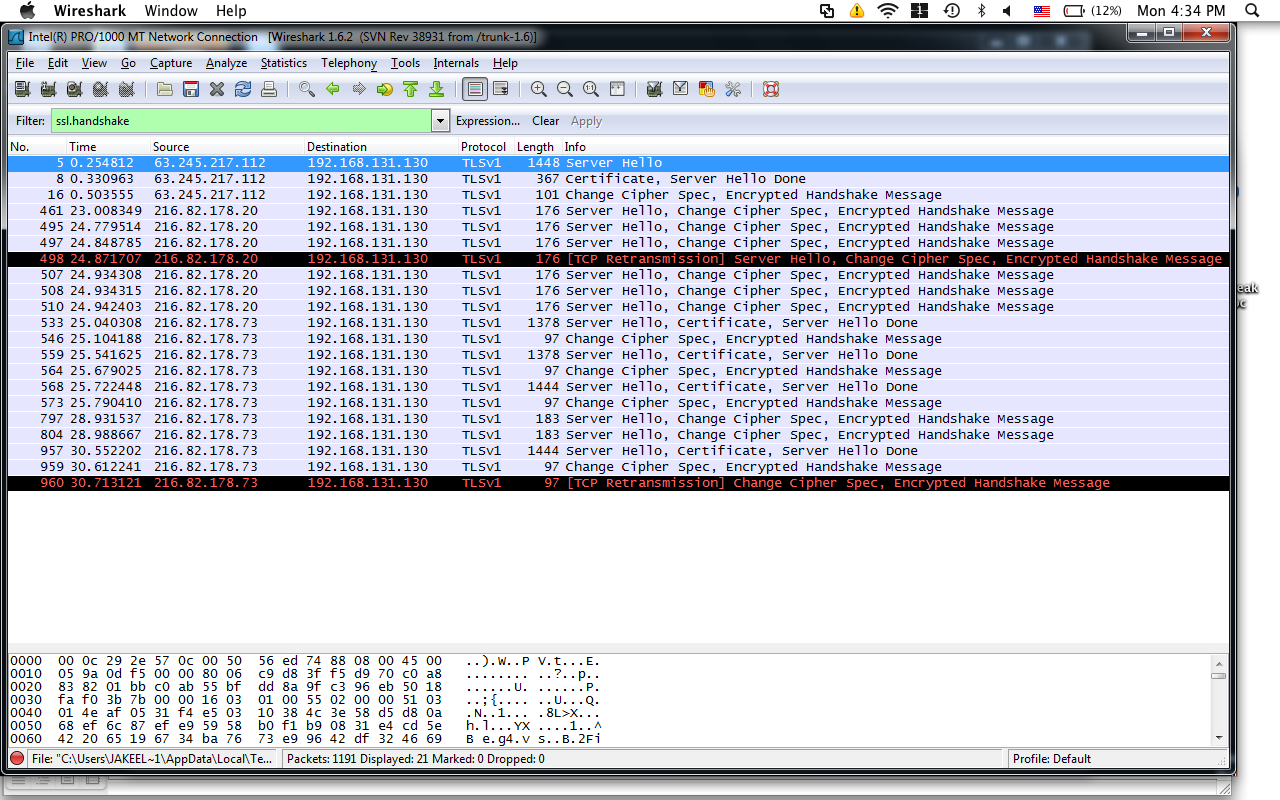
**Wireshark SSL/TLS Optional Assignment**



Q1. What is the session ID of the SSL/TLS handshaking?

Session ID: b8070000559f2873e27546a210a882f539af139ee653ed81...

----Was found in SSL under handshake protocol

Q2. What is the server's public key?

Cipher Suite: TLS\_RSA\_WITH\_RC4\_128\_MD5 (0x0004)

---was found in SSL under Handshake protocol

Q3A. What are the cipher suites that your browser supports?

Cipher Suite: TLS\_RSA\_WITH\_RC4\_128\_MD5 (0x0004)

---was found in SSL under Handshake protocol

Q3B. What is the cipher suite that the server selected? Explain what the selected cipher suite means (symmetric, asymmetric, and hashing)?

I believe it selected to use RSA which is an Asymmetric encryption

Q4. How do you know that your browser is talking with the company (your bank)?

The IP source and destination address changes and the handshake protocol has the Server Hello and responses

Q5. What is the symmetric session key that the client generated? How was it generated (the used algorithm, how encrypted)?

I could not find this