**Wireshark SSL/TLS Optional Assignment**

**Instructions:**

- This is an optional assignment and you don’t have to do it.

- Select your primary bank and log in.

1. Start the Wireshark Analyzer.

2. Long in to your bank.

3. Stop the analyzer.

- No late submission accepted. No excuse accepted. No electronic submission necessary or accepted.

- Bring a hard copy to the class on Oct 31.

- Total: 10 points (each 2 points).

You will find many SSL/TLS handshaking traffic. Pick the one that you think contains your bank’s info. Don’t ask me which one to pick. Use the display filter (ssl.handshake) to obtain only SSL/TLS handshaking traffic. For each question, describe where you found the info? Add the screen shots to support your answers.

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

Q2. What is the server's public key?

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

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

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

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