**SSL/TLS Lab Exercise**

|  |
| --- |
| * This is an individual assignment. * The due date is Tuesday, November 21, 2017 4:00 (sec01) /7:00 (sec76). * For this assignment, you will need to use Wireshark. * Follow the usual naming convention. |

1. What is the session ID of the SSL/TLS handshaking? List the first four hex-digits only.

2. What is the length (bytes) of the certificate that the server shared with the client?

3A. How many cipher suites are supported by the client’s browser?

3B. What is the cipher suite that the server selected?

4. What is the length of the RSA Encrypted PreMaster Secret that is used to generate the Master Secret and session keys by the server and client?

5. What is the name of the company that the client is talking with?