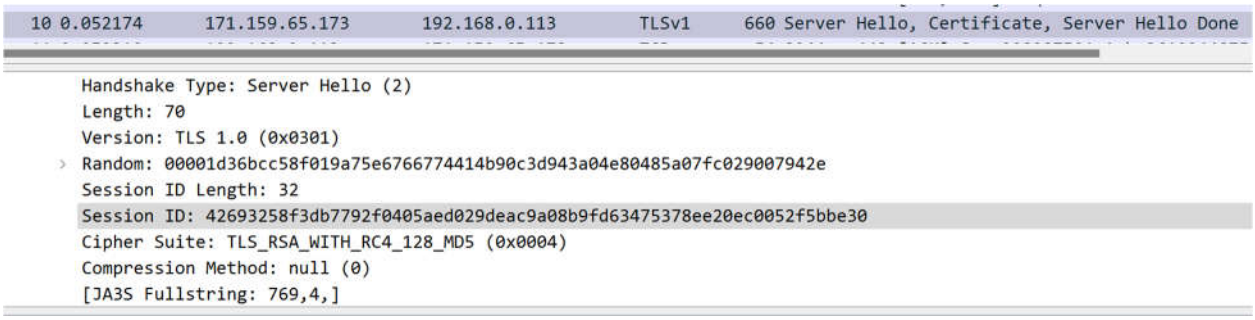
SSL/TLS Assignment

- This is an individual lab assignment.
- The due date is Tonight.
- For this assignment, you will need to use Wireshark and the attached "**https-justlaunchpage**".
- Please make the solutions readable and highlight the answers.
- Follow the usual naming convention.

Note: Provide screenshots for each answer.

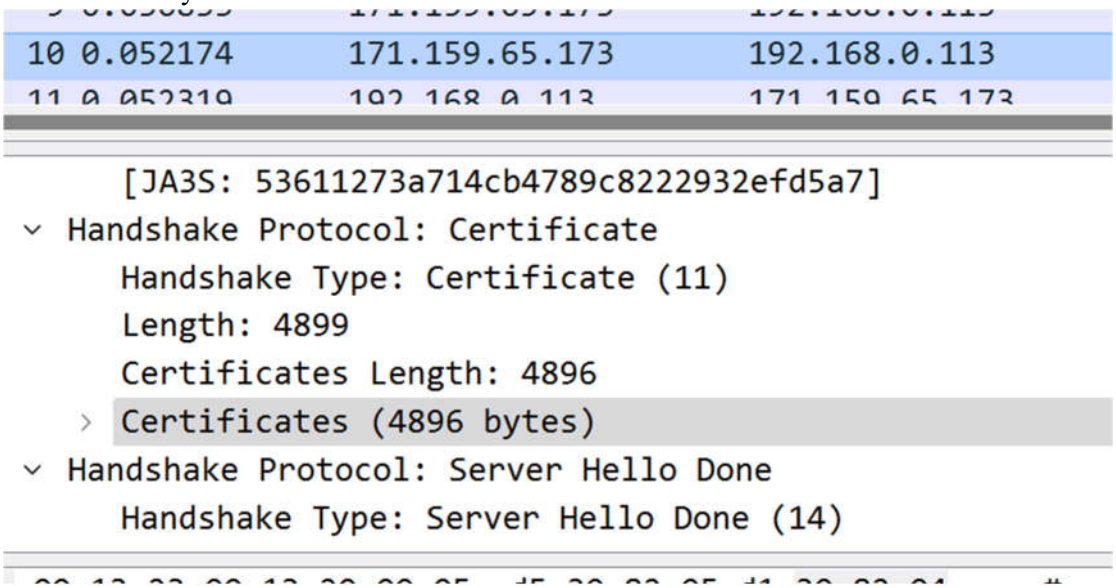
1. What is the session ID of the SSL/TLS handshaking?

Session ID: 42693258f3db7792f0405aed029deac9a08b9fd63475378ee20ec0052f5bbe30



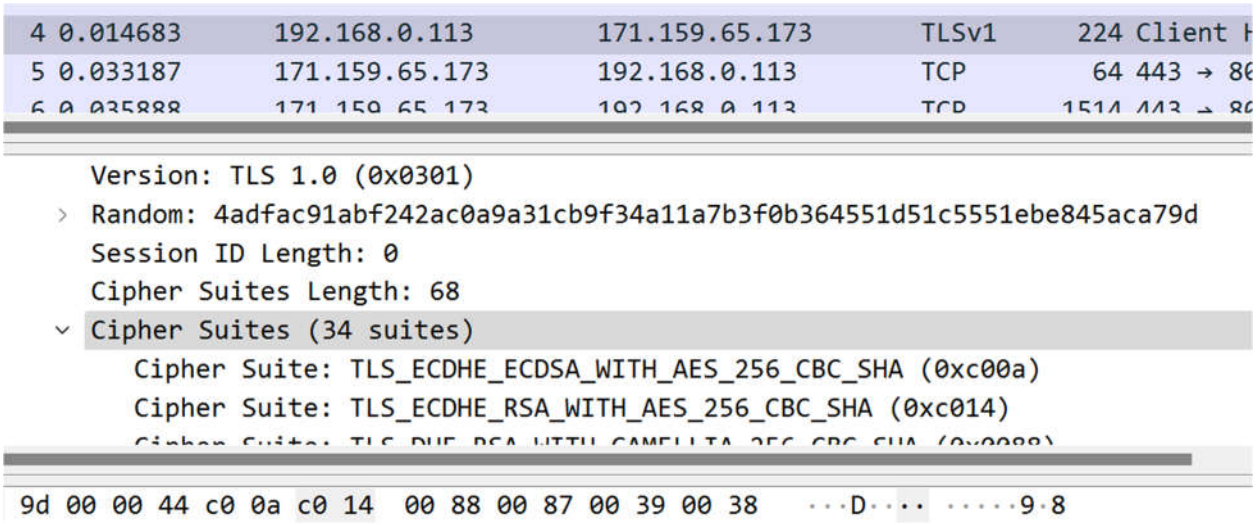
2. What is the length (bytes) of the certificate that the server shared with the client?

4896 bytes



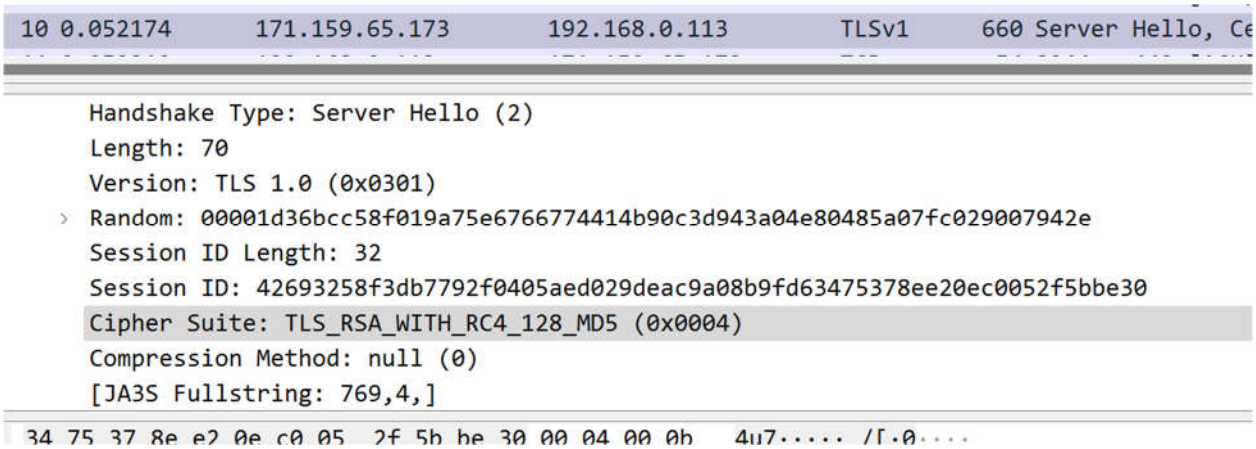
3A. How many cipher suites are supported by the client's browser?

34 Suites



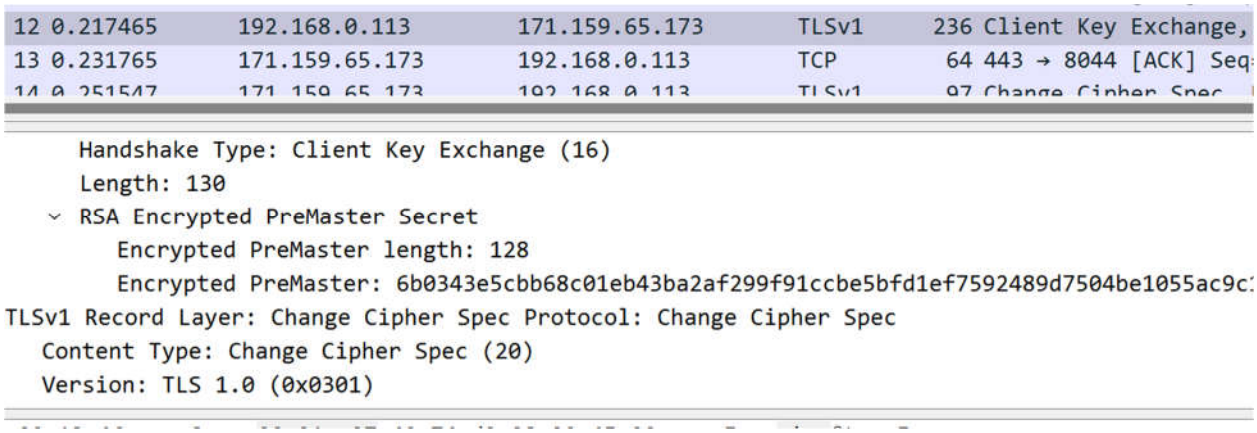
3B. What is the cipher suite that the server selected?

TLS_RSA_WITH_RC4_128_MD5 (0x0004)



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?

128 bytes



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

Bank of America