

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

10	0.052174	171.159.65.173	192.168.0.113	TLSv1	660	Server Hello, Certificate, Server Hello Done
----	----------	----------------	---------------	-------	-----	--

Handshake Type: Server Hello (2)
Length: 70
Version: TLS 1.0 (0x0301)
Random: 00001d36bcc58f019a75e6766774414b90c3d943a04e80485a07fc029007942e
Session ID Length: 32
Session ID: 42693258f3db7792f0405aed029deac9a08b9fd63475378ee20ec0052f5bbe30
Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
Compression Method: null (0)
[JA3S Fullstring: 769,4,]

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

4896 bytes

10	0.052174	171.159.65.173	192.168.0.113
11	0.052310	192.168.0.113	171.159.65.173

[JA3S: 53611273a714cb4789c8222932efd5a7]

Handshake Protocol: Certificate
Handshake Type: Certificate (11)
Length: 4899
Certificates Length: 4896
Certificates (4896 bytes)

Handshake Protocol: Server Hello Done
Handshake Type: Server Hello Done (14)

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

34 Suites

4	0.014683	192.168.0.113	171.159.65.173	TLSv1	224 Client H
5	0.033187	171.159.65.173	192.168.0.113	TCP	64 443 → 86
6	0.035888	171.159.65.173	192.168.0.113	TCP	1514 443 → 86

Version: TLS 1.0 (0x0301)

- > Random: 4adfac91abf242ac0a9a31cb9f34a11a7b3f0b364551d51c5551ebe845aca79d
- Session ID Length: 0
- Cipher Suites Length: 68
- ✓ Cipher Suites (34 suites)
 - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
 - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
 - Cipher Suite: TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0xc008)

9d 00 00 44 c0 0a c0 14 00 88 00 87 00 39 00 38 ...D... ..9·8

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

TLS_RSA_WITH_RC4_128_MD5 (0x0004)

10	0.052174	171.159.65.173	192.168.0.113	TLSv1	660 Server Hello, Ce
----	----------	----------------	---------------	-------	----------------------

Handshake Type: Server Hello (2)

Length: 70

Version: TLS 1.0 (0x0301)

- > Random: 00001d36bcc58f019a75e6766774414b90c3d943a04e80485a07fc029007942e
- Session ID Length: 32
- Session ID: 42693258f3db7792f0405aed029deac9a08b9fd63475378ee20ec0052f5bbe30
- Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
- Compression Method: null (0)
- [JA3S Fullstring: 769,4,]

34 75 37 8e e2 0e c0 05 2f 5b be 30 00 04 00 0b 4u7..... /Γ.0....

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

12	0.217465	192.168.0.113	171.159.65.173	TLSv1	236 Client Key Exchange,
13	0.231765	171.159.65.173	192.168.0.113	TCP	64 443 → 8044 [ACK] Seq:
14	0.251517	171.159.65.173	192.168.0.113	TLSv1	97 Change Cipher Spec

Handshake Type: Client Key Exchange (16)

Length: 130

✓ RSA Encrypted PreMaster Secret

Encrypted PreMaster length: 128

Encrypted PreMaster: 6b0343e5cbb68c01eb43ba2af299f91ccbe5bfd1ef7592489d7504be1055ac9c:

TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec

Content Type: Change Cipher Spec (20)

Version: TLS 1.0 (0x0301)

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

Bank of America

10	0.052174	171.159.65.173	192.168.0.113	TLSv1	660 Server Hello, Certificate, Server Hello Done
11	0.052310	192.168.0.113	171.159.65.173	TCP	54 8044 → 443 [ACK] Seq=008087501 Ack=3610744875 Win

Handshake Type: Certificate (11)

Length: 4899

Certificates Length: 4896

Certificates (4896 bytes)

Certificate Length: 1493

✓ Certificate: 308205d1308204b9a003020102021039b99ab4618d2f94dcf1451f42b90bfb300d06092a... (id-at-commonName=www.bankofamerica.com, signedCertificate)