SSL/TLS Assignment

- This is an individual lab assignment.
- The due date is Wednesday, November 17.
- 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?

```
> Random: 00001d36bcc58f019a75e6766774414b90c3d943a04e80485a07fc029007942e
  Session ID Length: 32
  Session ID: 42693258f3db7792f0405aed029deac9a08b9fd63475378ee20ec0052f5bbe30
  Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
  Compression Method: null (0)
```

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

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

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

```
  Session ID Length: 0
  Cipher Suites Length: 68
> Cipher Suites (34 suites)
```

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

```
  Session ID Length: 32
  Session ID: 42693258f3db7792f0405aed029deac9a08b9fd63475378ee20ec0052f5bbe30
  Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
  Compression Method: null (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?

```
v RSA Encrypted PreMaster Secret
    Encrypted PreMaster length: 128
    Encrypted PreMaster: 6b0343e5cbb68c01eb43ba2af299f91ccbe5bfd1ef7592489d7504be1055ac9c1698d313…
```

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

```
  v Server Name Indication extension
      Server Name list length: 24
      Server Name Type: host_name (0)
      Server Name length: 21
      Server Name: www.bankofamerica.com
```