

SSL/TLS Assignment

- This is an individual lab assignment.
- The due date is Wednesday, November 18.
- 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?

8	0.036437	192.168.0.113	171.159.65.173	TCP	54	8044 → 443 [ACK] Seq=908987501 Ack=3610242809 Win=6
9	0.036833	171.159.65.173	192.168.0.113	TCP	1514	443 → 8044 [PSH, ACK] Seq=3610242809 Ack=908987501
10	0.052174	171.159.65.173	192.168.0.113	TLSv1	660	Server Hello, Certificate, Server Hello Done
11	0.052319	192.168.0.113	171.159.65.173	TCP	54	8044 → 443 [ACK] Seq=908987501 Ack=3610244875 Win=6
12	0.217465	192.168.0.113	171.159.65.173	TLSv1	236	Client Key Exchange, Change Cipher Spec, Encrypted
13	0.231765	171.159.65.173	192.168.0.113	TCP	64	443 → 8044 [ACK] Seq=3610244875 Ack=908987683 Win=4
14	0.251547	171.159.65.173	192.168.0.113	TLSv1	97	Change Cipher Spec, Encrypted Handshake Message

Length:	70
Version:	TLS 1.0 (0x0301)
Random:	00001d36bcc58f019a75e6766774414b90c3d943a04e8048...
Session ID Length:	32
Session ID:	42693258f3db7792f0405aed029deac9a08b9fd63475378e...
Cipher Suite:	TLS_RSA_WITH_RC4_128_MD5 (0x0004)
Compression Method:	null (0)
Handshake Protocol:	Certificate

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

10	0.052174	171.159.65.173	192.168.0.113	TLSv1	660	Server Hello, Certificate, Server Hello Done
11	0.052319	192.168.0.113	171.159.65.173	TCP	54	8044 → 443 [ACK] Seq=908987501 Ack=3610244875 Wi
12	0.217465	192.168.0.113	171.159.65.173	TLSv1	236	Client Key Exchange, Change Cipher Spec, Encrypt
13	0.231765	171.159.65.173	192.168.0.113	TCP	64	443 → 8044 [ACK] Seq=3610244875 Ack=908987683 Wi
14	0.251547	171.159.65.173	192.168.0.113	TLSv1	97	Change Cipher Spec, Encrypted Handshake Message
15	0.252454	192.168.0.113	171.159.65.173	TLSv1	767	Application Data

Length:	4981
Handshake Protocol:	Server Hello
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?

1	0.000000	192.168.0.113	171.159.65.173	TCP	66	8044 → 443 [SYN]	Seq=908987330 Win=8192 Len=0 MS...
2	0.014028	171.159.65.173	192.168.0.113	TCP	66	443 → 8044 [SYN, ACK]	Seq=3610239888 Ack=9089873...
3	0.014206	192.168.0.113	171.159.65.173	TCP	54	8044 → 443 [ACK]	Seq=908987331 Ack=3610239889 Win...
4	0.014683	192.168.0.113	171.159.65.173	TLSv1	224	Client Hello	
5	0.033187	171.159.65.173	192.168.0.113	TCP	64	443 → 8044 [ACK]	Seq=3610239889 Ack=908987501 Win...
6	0.035888	171.159.65.173	192.168.0.113	TCP	1514	443 → 8044 [ACK]	Seq=3610239889 Ack=908987501 Win...
7	0.036346	171.159.65.173	192.168.0.113	TCP	1514	443 → 8044 [ACK]	Seq=3610241349 Ack=908987501 Win...

Random: 4adf91abf242ac0a9a31cb9f34a11a7b3f0b364551d51c...

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_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0088)

Cipher Suite: TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0088)

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

8	0.036437	192.168.0.113	171.159.65.173	TCP	54	8044 → 443	[ACK] Seq=908987501 Ack=3610242809 Win=65535 Len=0
9	0.036833	171.159.65.173	192.168.0.113	TCP	1514	443 → 8044	[PSH, ACK] Seq=3610242809 Ack=908987501 Win=65535 Len=0
10	0.052174	171.159.65.173	192.168.0.113	TLSv1	660	Server Hello, Certificate, Server Hello Done	
11	0.052319	192.168.0.113	171.159.65.173	TCP	54	8044 → 443	[ACK] Seq=908987501 Ack=3610244875 Win=65535 Len=0
12	0.217465	192.168.0.113	171.159.65.173	TLSv1	236	Client Key Exchange, Change Cipher Spec, Encrypted	
13	0.231765	171.159.65.173	192.168.0.113	TCP	64	443 → 8044	[ACK] Seq=3610244875 Ack=908987683 Win=65535 Len=0

```

Version: TLS 1.0 (0x0301)
> Random: 00001d36bcc58f019a75e6766774414b90c3d943a04e8048...
Session ID Length: 32
Session ID: 42693258f3db7792f0405aed029deac9a08b9fd63475378e...
Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
Compression Method: null (0)
✖ Handshake Protocol: Certificate
Handshake Type: Certificate (11)

```

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?

9	0.036833	171.159.65.173	192.168.0.113	TCP	1514	443 → 8044 [PSH, ACK] Seq=3610242809 Ack=908987501
10	0.052174	171.159.65.173	192.168.0.113	TLSv1	660	Server Hello, Certificate, Server Hello Done
11	0.052319	192.168.0.113	171.159.65.173	TCP	54	8044 → 443 [ACK] Seq=908987501 Ack=3610244875 Win
12	0.217465	192.168.0.113	171.159.65.173	TLSv1	236	Client Key Exchange, Change Cipher Spec, Encrypt
13	0.231765	171.159.65.173	192.168.0.113	TCP	64	443 → 8044 [ACK] Seq=3610244875 Ack=908987683 Win
14	0.251547	171.159.65.173	192.168.0.113	TLSv1	97	Change Cipher Spec, Encrypted Handshake Message
15	0.252454	192.168.0.113	171.159.65.173	TLSv1	767	Application Data

Transmission Control Protocol, Src Port: 8044, Dst Port: 443, Seq: 908987501, Ack: 3610244875, Len: 182

Transport Layer Security

- ▼ TLSv1 Record Layer: Handshake Protocol: Client Key Exchange
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 134
 - ▼ Handshake Protocol: Client Key Exchange
 - Handshake Type: Client Key Exchange (16)
 - Length: 130
 - ▼ RSA Encrypted PreMaster Secret
 - Encrypted PreMaster length: 128
 - Encrypted PreMaster: 6b0343e5cbb68c01eb43ba2af299f91ccbe5bfd1ef759248...
- > TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
- > TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message

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

1	0.000000	192.168.0.113	171.159.65.173	TCP	66	8044 → 443	[SYN]	Seq=908987330	Win=8192	Len=0
2	0.014028	171.159.65.173	192.168.0.113	TCP	66	443 → 8044	[SYN, ACK]	Seq=3610239888	Ack=908987330	Len=0
3	0.014206	192.168.0.113	171.159.65.173	TCP	54	8044 → 443	[ACK]	Seq=908987331	Ack=3610239889	Len=0
4	0.014683	192.168.0.113	171.159.65.173	TLSv1	224	Client Hello				
5	0.033187	171.159.65.173	192.168.0.113	TCP	64	443 → 8044	[ACK]	Seq=3610239889	Ack=908987501	Len=0
6	0.035888	171.159.65.173	192.168.0.113	TCP	1514	443 → 8044	[ACK]	Seq=3610239889	Ack=908987501	Len=0
7	0.036346	171.159.65.173	192.168.0.113	TCP	1514	443 → 8044	[ACK]	Seq=3610241349	Ack=908987501	Len=0

```
Compression Methods Length: 1
> Compression Methods (1 method)
Extensions Length: 52
v Extension: server_name (len=26)
    Type: server_name (0)
    Length: 26
    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
> Extension: supported_groups (len=8)
> Extension: ec point formats (len=2)
```