

Cryptography & Network Security Lab

SSL/TLS Lab

Name: Sakshi Sanjay Desai

PRN: 2019BTECS00021

Aim: To observe SSL/TLS (Secure Sockets Layer/ Transport Layer Security) in action. SSL/TLS is used to secure TCP connections, and it is widely used as part of the secure web: HTTPS is SSL over HTTP

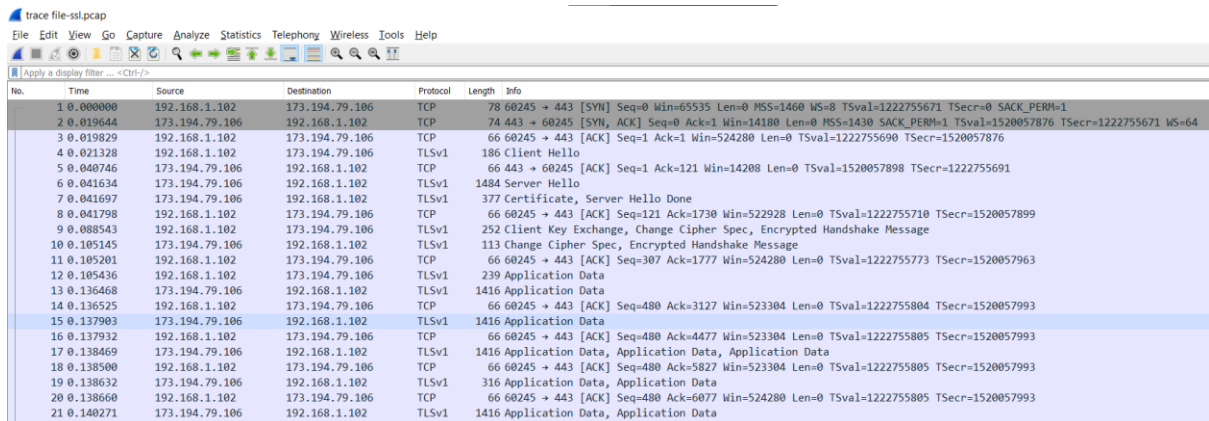
Theory: Secure Socket Layer (SSL) provides security to the data that is transferred between web browser and server. SSL encrypts the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.

Secure Socket Layer Protocols:

- SSL record protocol
- Handshake protocol
- Change-cipher spec protocol
- Alert protocol

Procedure:

STEP 1: Open a Trace you should use a supplied trace file trace-ssl.pcap.



The image shows a Wireshark packet capture of an SSL/TLS session. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help), a toolbar, and a packet list pane. The packet list pane shows 21 packets. The first packet is a TCP SYN from 192.168.1.102 to 173.194.79.106. The second packet is a TCP ACK from 173.194.79.106 to 192.168.1.102. The third packet is a TCP ACK from 192.168.1.102 to 173.194.79.106. The fourth packet is a TLSv1 Client Hello from 192.168.1.102 to 173.194.79.106. The fifth packet is a TLSv1 Server Hello from 173.194.79.106 to 192.168.1.102. The sixth packet is a TLSv1 Certificate from 173.194.79.106 to 192.168.1.102. The seventh packet is a TLSv1 Server Hello Done from 173.194.79.106 to 192.168.1.102. The eighth packet is a TLSv1 Client Key Exchange from 192.168.1.102 to 173.194.79.106. The ninth packet is a TLSv1 Change Cipher Spec from 192.168.1.102 to 173.194.79.106. The tenth packet is a TLSv1 Change Cipher Spec from 173.194.79.106 to 192.168.1.102. The eleventh packet is a TLSv1 Application Data from 192.168.1.102 to 173.194.79.106. The twelfth packet is a TLSv1 Application Data from 173.194.79.106 to 192.168.1.102. The thirteenth packet is a TLSv1 Application Data from 192.168.1.102 to 173.194.79.106. The fourteenth packet is a TLSv1 Application Data from 173.194.79.106 to 192.168.1.102. The fifteenth packet is a TLSv1 Application Data from 192.168.1.102 to 173.194.79.106. The sixteenth packet is a TLSv1 Application Data from 173.194.79.106 to 192.168.1.102. The seventeenth packet is a TLSv1 Application Data from 192.168.1.102 to 173.194.79.106. The eighteenth packet is a TLSv1 Application Data from 173.194.79.106 to 192.168.1.102. The nineteenth packet is a TLSv1 Application Data from 192.168.1.102 to 173.194.79.106. The twentieth packet is a TLSv1 Application Data from 173.194.79.106 to 192.168.1.102. The twenty-first packet is a TLSv1 Application Data from 192.168.1.102 to 173.194.79.106.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	173.194.79.106	TCP	78	60245 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=1222755671 TSecr=0 SACK_PERM=1
2	0.019644	173.194.79.106	192.168.1.102	TCP	74	443 → 60245 [SYN, ACK] Seq=0 Ack=1 Win=14180 Len=0 MSS=1430 SACK_PERM=1 TSval=1520057876 TSecr=1222755671 WS=64
3	0.019829	192.168.1.102	173.194.79.106	TCP	66	60245 → 443 [ACK] Seq=1 Ack=1 Win=524280 Len=0 TSval=1222755690 TSecr=1520057876
4	0.021328	192.168.1.102	173.194.79.106	TLSv1	186	Client Hello
5	0.040746	173.194.79.106	192.168.1.102	TCP	66	443 → 60245 [ACK] Seq=1 Ack=121 Win=14208 Len=0 TSval=1520057898 TSecr=1222755691
6	0.041634	173.194.79.106	192.168.1.102	TLSv1	1484	Server Hello
7	0.041697	173.194.79.106	192.168.1.102	TLSv1	377	Certificate, Server Hello Done
8	0.041798	192.168.1.102	173.194.79.106	TCP	66	60245 → 443 [ACK] Seq=121 Ack=1730 Win=522928 Len=0 TSval=1222755710 TSecr=1520057899
9	0.088543	192.168.1.102	173.194.79.106	TLSv1	252	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10	0.105145	173.194.79.106	192.168.1.102	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
11	0.105201	192.168.1.102	173.194.79.106	TCP	66	60245 → 443 [ACK] Seq=307 Ack=1777 Win=524280 Len=0 TSval=1222755773 TSecr=1520057963
12	0.105436	192.168.1.102	173.194.79.106	TLSv1	239	Application Data
13	0.136468	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data
14	0.136525	192.168.1.102	173.194.79.106	TCP	66	60245 → 443 [ACK] Seq=480 Ack=3127 Win=523304 Len=0 TSval=1222755804 TSecr=1520057993
15	0.137903	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data
16	0.137932	192.168.1.102	173.194.79.106	TCP	66	60245 → 443 [ACK] Seq=480 Ack=4477 Win=523304 Len=0 TSval=1222755805 TSecr=1520057993
17	0.138469	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data, Application Data, Application Data
18	0.138500	192.168.1.102	173.194.79.106	TCP	66	60245 → 443 [ACK] Seq=480 Ack=5827 Win=523304 Len=0 TSval=1222755805 TSecr=1520057993
19	0.138632	173.194.79.106	192.168.1.102	TLSv1	316	Application Data, Application Data
20	0.138660	192.168.1.102	173.194.79.106	TCP	66	60245 → 443 [ACK] Seq=480 Ack=6077 Win=524280 Len=0 TSval=1222755805 TSecr=1520057993
21	0.140271	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data, Application Data

STEP 2: Inspect the Trace

No.	Time	Source	Destination	Protocol	Length	Info
4	0.021328	192.168.1.102	173.194.79.106	TLSv1	186	Client Hello
6	0.041634	173.194.79.106	192.168.1.102	TLSv1	1484	Server Hello
7	0.041697	173.194.79.106	192.168.1.102	TLSv1	377	Certificate, Server Hello Done
9	0.088543	192.168.1.102	173.194.79.106	TLSv1	252	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10	0.105145	173.194.79.106	192.168.1.102	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
12	0.105436	192.168.1.102	173.194.79.106	TLSv1	239	Application Data
13	0.136468	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data
15	0.137903	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data
17	0.138469	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data, Application Data, Application Data
19	0.138632	173.194.79.106	192.168.1.102	TLSv1	316	Application Data, Application Data
21	0.140271	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data, Application Data
23	0.144028	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data
25	0.144465	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data
27	0.150300	173.194.79.106	192.168.1.102	TLSv1	270	Application Data, Application Data
29	0.150959	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data, Application Data
31	0.155107	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data
33	0.155529	173.194.79.106	192.168.1.102	TLSv1	1484	Application Data
34	0.163139	173.194.79.106	192.168.1.102	TLSv1	1484	Application Data, Application Data, Application Data
36	0.164031	173.194.79.106	192.168.1.102	TLSv1	1484	Application Data, Application Data
37	0.169767	173.194.79.106	192.168.1.102	TLSv1	1484	Application Data
39	0.170028	173.194.79.106	192.168.1.102	TLSv1	1484	Application Data, Application Data, Application Data
40	0.176414	173.194.79.106	192.168.1.102	TLSv1	130	Application Data, Application Data
42	0.177209	192.168.1.102	173.194.79.106	TLSv1	93	Encrypted Alert

> Frame 4: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits) on interface en0, id 0

> Ethernet II, Src: Apple_a2:05:1d (70:56:81:a2:05:1d), Dst: Cisco-Li_e3:e9:8d (00:16:b6:e3:e9:8d)

> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 173.194.79.106

> Transmission Control Protocol, Src Port: 60245, Dst Port: 443, Seq: 1, Ack: 1, Len: 120

Source Port: 60245

Destination Port: 443

[Stream index: 0]

70:56:81:a2:05:1d -> 00:16:b6:e3:e9:8d

trace file=ssl.pcapPackets: 47 · Dis

1. What is the Content Type for a record containing Application Data?

>> Content Type: Application Data (23)

```
> Frame 31: 1416 bytes on wire (11328 bits), 1416 bytes captured (11328
> Ethernet II, Src: Cisco-Li_e3:e9:8d (00:16:b6:e3:e9:8d), Dst: Apple_a
> Internet Protocol Version 4, Src: 173.194.79.106, Dst: 192.168.1.102
> Transmission Control Protocol, Src Port: 443, Dst Port: 60245, Seq: 1
> Transport Layer Security
  > TLSv1 Record Layer: Application Data Protocol: http-over-tls
    Content Type: Application Data (23)
    Version: TLS 1.0 (0x0301)
```

2. What version constant is used in your trace, and which version of TLS does it represent?

>> Version: TLS 1.0 (0x0301)

```
> Transmission Control Protocol, Src Port: 443, Dst Port: 60245, Seq
> Transport Layer Security
  > TLSv1 Record Layer: Application Data Protocol: http-over-tls
    Content Type: Application Data (23)
    Version: TLS 1.0 (0x0301)
    Length: 1345
    Encrypted Application Data: c8833a3a8a6faa82743be5cc8628be52
    [Application Data Protocol: http-over-tls]
```

Step 3: The SSL Handshake

Hello Message

1. How long in bytes is the random data in the Hellos? Both the Client and Server include this random data (a nonce) to allow the establishment of session keys.

```
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 115
  ▾ Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 111
    Version: TLS 1.0 (0x0301)
    > Random: 501778d316c25064f7cb0209b336ab332d969b8e091d26d4ccd04b731d7e550f
    Session ID Length: 0
    Cipher Suites Length: 46
  >> > Cipher Suites (23 suites)
```

Client Hello Random Data Length in bytes = **111**

```
  ▾ Transport Layer Security
    ▾ TLSv1 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 85
      ▾ Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 81
        Version: TLS 1.0 (0x0301)
        > Random: 501778d3d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e00161a893
        Session ID Length: 32
```

Server Hello Random Data Length in bytes = **81**

2. How long in bytes is the session identifier sent by the server? This identifier allows later resumption of the session with an abbreviated handshake when both the client and server indicate the same value. In our case, the client likely sent no session ID as there was nothing to resume.

ANS:

```
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 85
  ▾ Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 81
    Version: TLS 1.0 (0x0301)
    > Random: 501778d3d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e00161a893
    Session ID Length: 32
    Session ID: 8530bdac95116ccb343798b36cb2fd79c1e278cba1af41456c810c0cebfcccf4
    Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
    Compression Method: null (0)
    Extensions Length: 9
```

Server Session ID: 8530bdac95116ccb343798b36cb2fd79c1e278cba1af41456c810c0cebfcccf4

3. What Cipher suite is chosen by the Server? Give its name and value. The Client will list the different cipher methods it supports, and the Server will pick one of these methods to use.

```
> Random: 501778d3d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e00161a893
Session ID Length: 32
Session ID: 8530bdac95116ccb343798b36cb2fd79c1e278cba1af41456c810c0cebfcccf4
Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
Compression Method: null (0)
```

Cipher Suite: TLS_RSA_WITH_RCA_128_SHA

Certificate Messages

1. Who sends the Certificate, the client, the server, or both? A certificate is sent by one party to let the other party authenticate that it is who it claims to be. Based on this usage, you should be able to guess who sends the certificate and check the messages in your trace.

```
> Transmission Control Protocol, Src Port: 443, Dst Port: 60245, Seq
> [2 Reassembled TCP Segments (1630 bytes): #6(1328), #7(302)]
▼ Transport Layer Security
  ▼ TLSv1 Record Layer: Handshake Protocol: Certificate
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 1625
  ▼ Handshake Protocol: Certificate
    Handshake Type: Certificate (11)
    Length: 1621
    Certificates Length: 1618
  ▼ Certificates (1618 bytes)
    Certificate Length: 805
    > Certificate: 308203213082028aa00302010202104f9d96d966b1
    Certificate Length: 807
```

The Server sends the Certificate as the source port is 443, which is the server.

Client Key Exchange and Change Cipher Messages

1. Who sends the Change Cipher Spec message, the client, the server, or both?

<pre>> Ethernet II, Src: Apple_a2:05:1d (70:56:81:a2:05:1d), Dst: Cisco-Li_e3:e9:8d (00:16:b6:e3:e9:8d) > Internet Protocol Version 4, Src: 192.168.1.102, Dst: 173.194.79.106 > Transmission Control Protocol, Src Port: 60245, Dst Port: 443, Seq: 121, Ack: 1730, Len: 186 ▼ 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 ▼ TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec Content Type: Change Cipher Spec (20) Version: TLS 1.0 (0x0301) Length: 1 Change Cipher Spec Message ▼ TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message Content Type: Handshake (22)</pre>	<pre>> Ethernet II, Src: Cisco-Li_e3:e9:8d (00:16:b6:e3:e9:8d), Dst: Apple_a2:05:1d (70:56:81:a2:05:1d) > Internet Protocol Version 4, Src: 173.194.79.106, Dst: 192.168.1.102 > Transmission Control Protocol, Src Port: 443, Dst Port: 60245, Seq: 1730, Ack: 307, Len: 47 ▼ Transport Layer Security ▼ TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec Content Type: Change Cipher Spec (20) Version: TLS 1.0 (0x0301) Length: 1 Change Cipher Spec Message ▼ TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message Content Type: Handshake (22) Version: TLS 1.0 (0x0301) Length: 36 Handshake Protocol: Encrypted Handshake Message</pre>
---	---

Both server and client send the Change Cipher Spec message.

2. What are the contents carried inside the Change Cipher Spec message? Look past the Content Type and other headers to see the message itself.

- Transmission Control Protocol, Seq: 10000000, Len: 10000000, Seq: 10000000, Seq: 10000000
- Transport Layer Security
 - TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
 - Content Type: Change Cipher Spec (20)
 - Version: TLS 1.0 (0x0301)
 - Length: 1
 - Change Cipher Spec Message

Content Type: Change Cipher Spec (20)
