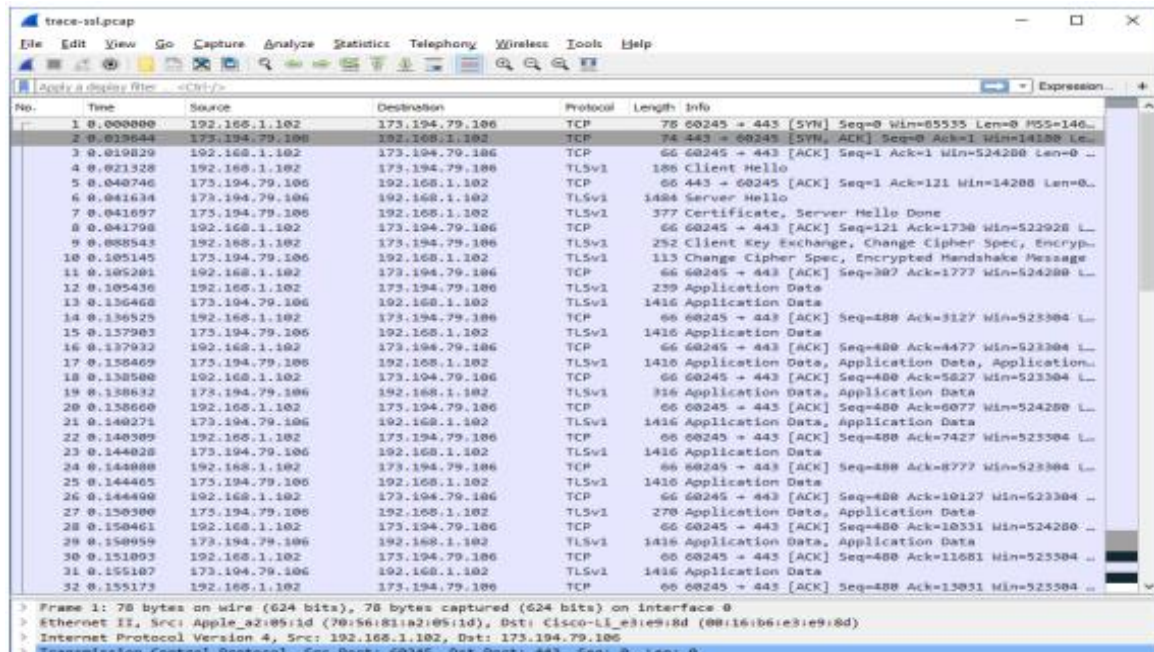


Experiment No. 13

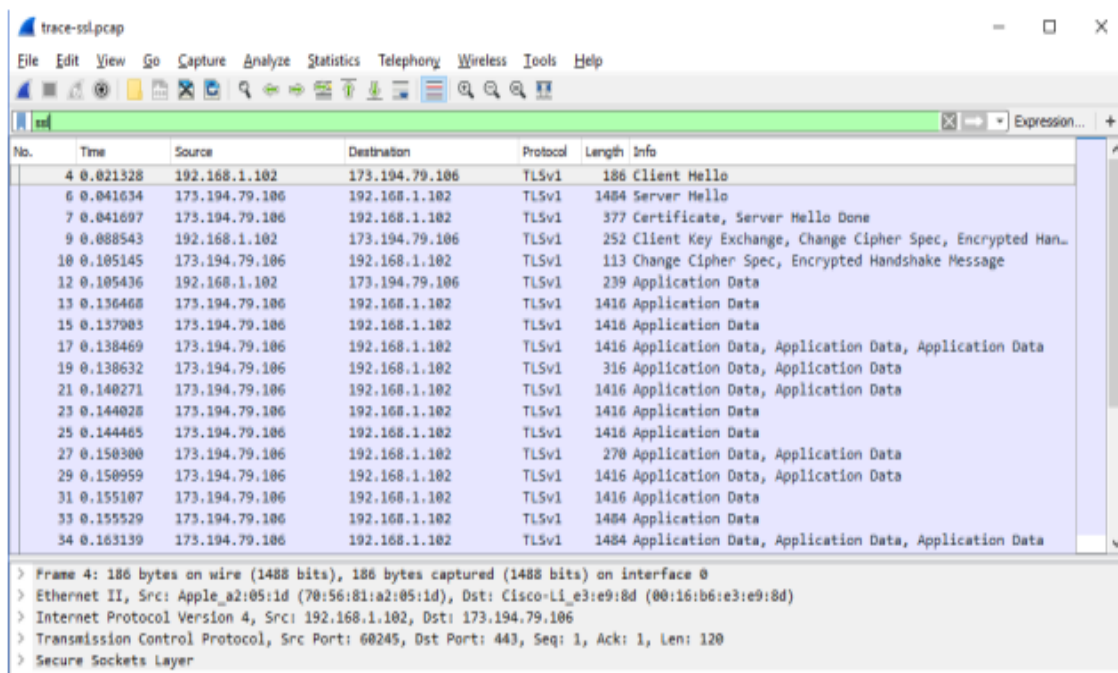
To study the SSL protocol by capturing the packets using Wireshark tool while visiting any SSL secured website (banking, e-commerce etc.).



The image shows a Wireshark packet capture window titled 'trace-sslpcap'. The packet list on the left shows 32 packets. The selected packet is packet 1, which is a TCP SYN packet from 192.168.1.102 to 173.194.79.106 on port 443. The packet details pane on the right shows the TCP header and the application data. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

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
2	0.013644	173.194.79.106	192.168.1.102	TCP	74	443 → 60245 [SYN, ACK] Seq=0 Ack=1 Win=14180 Len=0
3	0.019629	192.168.1.102	173.194.79.106	TCP	66	60245 → 443 [ACK] Seq=1 Ack=1 Win=524288 Len=0
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=14288 Len=0
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
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=524288 Len=0
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
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
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
19	0.138632	173.194.79.106	192.168.1.102	TLSv1	316	Application Data, Application Data
20	0.138669	192.168.1.102	173.194.79.106	TCP	66	60245 → 443 [ACK] Seq=480 Ack=6077 Win=524288 Len=0
21	0.140271	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data, Application Data
22	0.140309	192.168.1.102	173.194.79.106	TCP	66	60245 → 443 [ACK] Seq=480 Ack=7427 Win=523304 Len=0
23	0.144028	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data
24	0.144080	192.168.1.102	173.194.79.106	TCP	66	60245 → 443 [ACK] Seq=480 Ack=8777 Win=523304 Len=0
25	0.144465	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data
26	0.144490	192.168.1.102	173.194.79.106	TCP	66	60245 → 443 [ACK] Seq=480 Ack=10127 Win=523304 Len=0
27	0.150300	173.194.79.106	192.168.1.102	TLSv1	270	Application Data, Application Data
28	0.150461	192.168.1.102	173.194.79.106	TCP	66	60245 → 443 [ACK] Seq=480 Ack=10331 Win=524288 Len=0
29	0.150959	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data, Application Data
30	0.151093	192.168.1.102	173.194.79.106	TCP	66	60245 → 443 [ACK] Seq=480 Ack=11681 Win=523304 Len=0
31	0.155107	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data
32	0.155173	192.168.1.102	173.194.79.106	TCP	66	60245 → 443 [ACK] Seq=480 Ack=13031 Win=523304 Len=0

Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 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: 0, Len: 0



The image shows a Wireshark packet capture window titled 'trace-sslpcap'. The packet list on the left shows 34 packets. The selected packet is packet 4, which is a TLSv1 Client Hello packet from 192.168.1.102 to 173.194.79.106. The packet details pane on the right shows the TLSv1 header and the application data. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

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

Frame 4: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits) on interface 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
Secure Sockets Layer

trace-ssl.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssl

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	143	Change Cipher Spec, Encrypted Handshake Message
12	0.105436	192.168.1.102	173.194.79.106	TLSv1	239	Application Data
13	0.135468	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

Expand this packet

Frame 12: 239 bytes on wire (1912 bits), 239 bytes captured (1912 bits) on interface 0

Ethernet II, Src: Apple_a2:05:1d (70:50:01:a2:05:1d), Dst: Cisco-Li_e3:e9:8d (00:16:b0: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: 387, Ack: 1777, Len: 173

Secure Sockets Layer

- TLSv1 Record Layer: Application Data Protocol: http-over-tls
 - Content Type: Application Data (23)
 - Version: TLS 1.0 (0x0301)
 - Length: 168
 - Encrypted Application Data: 52e78fc0f73eec8a76cc409ad794fd69ee412be0ba03114...

SSL block expanded

trace-ssl.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssl

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

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

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: 501778d3d52d556ed20e072f638f0a51e9724d66ef5f1376...

GMT Unix Time: Jul 31, 2012 07:18:59.000000000 GMT Daylight Time

Random Bytes: d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e0...

Session ID Length: 32

Session ID: 8530bdac95116ccb343798b36cb2fd79c1e278cba1af4145...

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

Secure Sockets Layer

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: 308203213082028aa00302010202104f9d96d966b0992b54... (id-at-commonName=www.google.com,id-at-organizationName=Goo

Certificate Length: 807

> Certificate: 308203233082028ca003020102020430000002300d06092a... (id-at-commonName=Thawte SGC CA,id-at-organizationName=Thaw