

# SSL Session

---

## 1. Difference between HTTP and HTTPS

HTTP	HTTPS
HTTP stands for HyperText Transfer Protocol.	HTTPS stands for HyperText Transfer Protocol Secure
Uses port number 80 for communication	Uses port number 443 for communication
It works at application layer	It works at transport layer
In HTTP, encryption is absent	In HTTPS, encryption is present
HTTP is faster than HTTPS	HTTPS is slower than HTTP

## 2. A SSL session is consists of the following steps.

- 2.1. **Connect:** When a client sends connection request to the application server. If the application server is on a secure port, the TCP/IP server sends this request to the SSL server labeling things which identify the certificate to ensure a secure connection. Once verified the SSL server sends the request to the application server. Hence, in total 2 connections are formed, client to SSL server and SSL server to application server. The intervention of SSL server is transparent to the application server and the client. To them it looks like they are communicating directly.
- 2.2. **Handshake:** After successful connection the client initiates handshake protocol to produce the cryptographic parameters for the session. In respond to his the SSL server sends the application server's certificate to the client, asking for clients certificate in return to authenticate it.
- 2.3. **Data transmission:** Once the handshake is complete, the client sends encrypted data over the network. The SSL server receives it, decrypts it and sends unencrypted data to the application server. The application server responds by sending unencrypted data to the SSL server then encrypts it and sends it to the client.
- 2.4. **Close:** When a close request is initiated from either side, the SSL certificate sends a close request to the other party and cleans up the connection.

## 3. Where are SSL certificates stored?

- 3.1. **Windows:** The certificate store is located in the registry under the HKEY\_LOCAL\_MACHINE root. This type of certificate store is local to a user account on the computer. This certificate store is located in the registry under the HKEY\_CURRENT\_USER root.

3.2. **Linux:** The default location to store certificates is /etc/ssl/certs.

**4.** Private keys and personal certificates are stored in keystores. Public keys and CA certificates are stored in truststores. A truststore is a keystore that by convention contains only trusted keys and certificates.

**5.** SSL one way and two way handshakes

**5.1. SSL one way handshake**

- 5.1.1. In this process the client posts a request to the server to connect.
- 5.1.2. Server in return shares their public certificate to client for authentication.
- 5.1.3. Client on receiving shares the certificate to the respected CA's for authentication.
- 5.1.4. Once the certificate is authenticated by the CA's, the SSL/TLS client shares a random byte string to client and server which will be used for secure connection. The random byte is itself encrypted.
- 5.1.5. After successful authentication the client and server starts communicating.

**5.2. SSL two way handshake**

- 5.2.1. In this process, the client posts a request to the server to connect.
- 5.2.2. Server shares their public certificate to client for authentication.
- 5.2.3. Client on receiving shares the certificate to the respected CA's for authentication.
- 5.2.4. Once the certificate is authenticated by the CA's, the SSL/TLS client shares their public certificate to the server and the server authenticates it by sharing it to the respective CA's.
- 5.2.5. On successful authentication of both the parties, they connect with each other and data sharing takes place.

**6.** SSL/TLS versions and ciphers:

**6.1. TLS 1.3 Supported Ciphers**

- 6.1.1. AEAD-AES128-GCM-SHA256
- 6.1.2. AEAD-AES256-GCM-SHA384
- 6.1.3. AEAD-CHACHA20-POLY1305-SHA256

**6.2. TLS 1.2 supported ciphers**

- 6.2.1. CDHE-ECDSA-AES128-GCM-SHA256
- 6.2.2. ECDHE-ECDSA-CHACHA20-POLY1305
- 6.2.3. ECDHE-RSA-AES128-GCM-SHA256
- 6.2.4. ECDHE-RSA-CHACHA20-POLY1305
- 6.2.5. ECDHE-ECDSA-AES128-SHA256
- 6.2.6. ECDHE-ECDSA-AES128-SHA
- 6.2.7. ECDHE-RSA-AES128-SHA256

- 6.2.8. ECDHE-RSA-AES128-SHA
- 6.2.9. AES128-GCM-SHA256
- 6.2.10. AES128-SHA256
- 6.2.11. ES128-SHA
- 6.2.12. ECDHE-ECDSA-AES256-GCM-SHA384
- 6.2.13. ECDHE-ECDSA-AES256-SHA384
- 6.2.14. ECDHE-RSA-AES256-GCM-SHA384
- 6.2.15. ECDHE-RSA-AES256-SHA384
- 6.2.16. ECDHE-RSA-AES256-SHA
- 6.2.17. AES256-GCM-SHA384
- 6.2.18. AES256-SHA256
- 6.2.19. AES256-SHA

## 7. Use SSL to sniff SSL handshake

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 39 && ssl

No.	Time	Source	Destination	Protocol	Length	Info
4551	28.454036	192.168.1.131	23.106.127.53	TLSv1.3	682	Client Hello
4552	28.516090	23.106.127.53	192.168.1.131	TLSv1.3	299	Server Hello, Change Cipher Spec, Application Data, Application Data
4553	28.517203	192.168.1.131	23.106.127.53	TLSv1.3	134	Change Cipher Spec, Application Data
4555	28.517929	192.168.1.131	23.106.127.53	TLSv1.3	644	Application Data
4561	28.580250	23.106.127.53	192.168.1.131	TLSv1.3	341	Application Data
4564	28.581973	23.106.127.53	192.168.1.131	TLSv1.3	68	Application Data

> Frame 4555: 644 bytes on wire (5152 bits), 644 bytes captured (5152 bits) on interface \Device\NPF\_{2A2...}

> Ethernet II, Src: LiteonTe\_de:4c:29 (00:f4:8d:de:4c:29), Dst: Netgear\_ff:2d:f4 (cc:40:d0:ff:2d:f4)

> Internet Protocol Version 4, Src: 192.168.1.131, Dst: 23.106.127.53

> Transmission Control Protocol, Src Port: 52016, Dst Port: 443, Seq: 2169, Ack: 246, Len: 590

> [2 Reassembled TCP Segments (2050 bytes): #4554(1460), #4555(590)]

Transport Layer Security

▼ TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol

Opaque Type: Application Data (23)

Version: TLS 1.2 (0x0303)

Length: 2045

Encrypted Application Data: 64cdc7eee6d0cba4d722291800c62236e7795b73ee8427e652f63932ca11496e86050

[Application Data Protocol: Hypertext Transfer Protocol]

```

0000 cc 40 d0 ff 2d f4 00 f4 8d de 4c 29 08 00 45 00 @...
0010 02 76 4f e8 40 00 06 4f cf c0 a8 01 83 17 6a v0@
0020 7f 35 cb 30 01 bb de 51 1d 2e 49 76 d6 3e 50 18 50
0030 02 00 b4 5d 00 00 62 0c da 84 8b da 44 63 91 fc ]
0040 2e 5e d6 27 84 26 75 3d 3d 5e 99 d5 61 be 8e a0 ^'x
0050 a4 2f ac 02 32 5c 79 ca 9e d6 5e 2c 1e e6 1e b0 /2
0060 8d aa dc 38 9d b6 7c 08 1c f1 bb a3 0a d6 fe 53 8
0070 a8 9f a0 83 a3 60 5a de 1c 24 46 5d 25 03 bd 70 ^
0080 be a4 95 38 6a 42 09 1d 47 c9 6c 96 75 2f b0 c1 8jE
0090 c6 0c 2d 4b 8e d7 f4 e4 7f 8a 71 fd 7d 83 37 e4 K
00a0 8b 51 72 53 c2 aa 3f 24 85 48 94 37 f1 e5 64 e4 QrS
00b0 a3 b5 e4 6a 58 90 f3 fc 0b 23 ea 09 a7 fb c0 06 jX
00c0 d3 d8 09 e8 23 85 b0 c0 6c ac f0 9f 5f 86 99 3b #
00d0 00 31 5a f6 12 84 3d 7d bf 74 e4 35 5d fb ab b4 12
00e0 39 05 a9 71 c8 ee 46 1c 19 bc 98 8c 0a 7f e4 97 9-q
00f0 bb 55 c0 97 19 02 0d b4 35 77 93 69 dd 8e 09 09 U
0100 ce fd c6 6e 6a d5 0a fa 49 8c 00 d1 15 10 88 3a nj

```