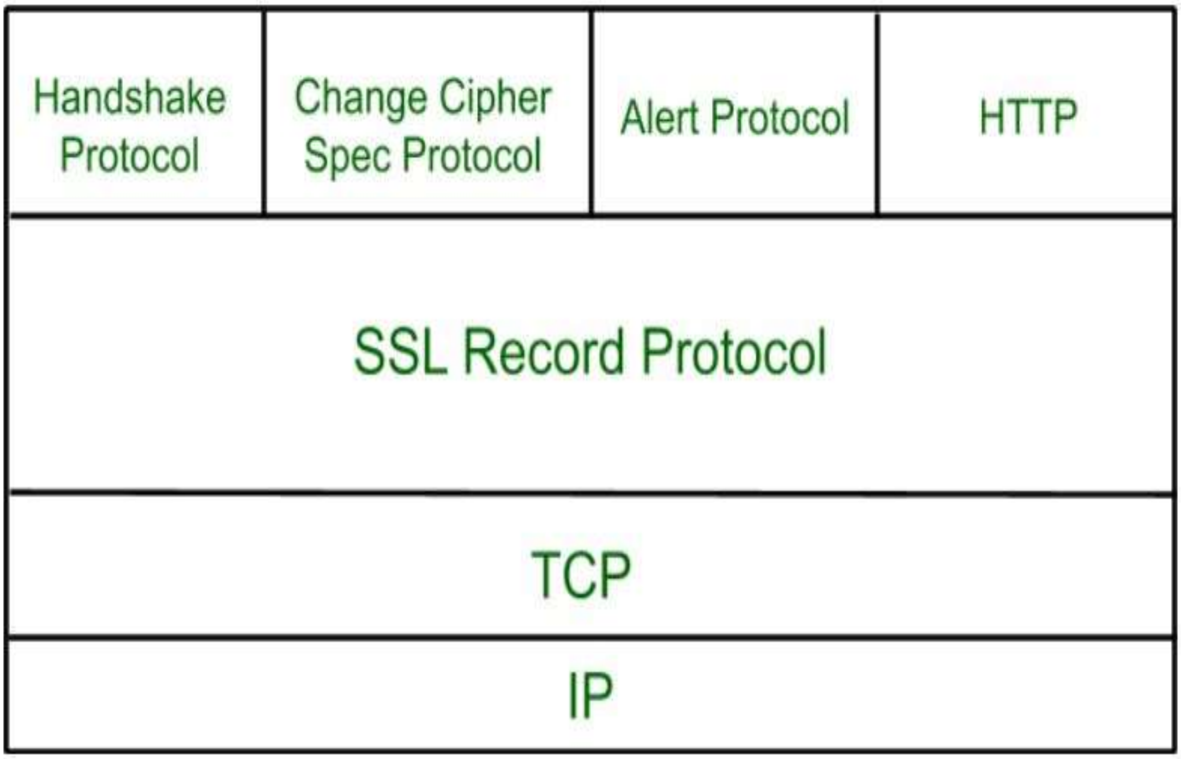
Secure Socket Layer (SSL)

Secure Socket Layer (SSL) provides security to the data that is transferred between web browser and server. SSL encrypt 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

SSL Protocol Stack:

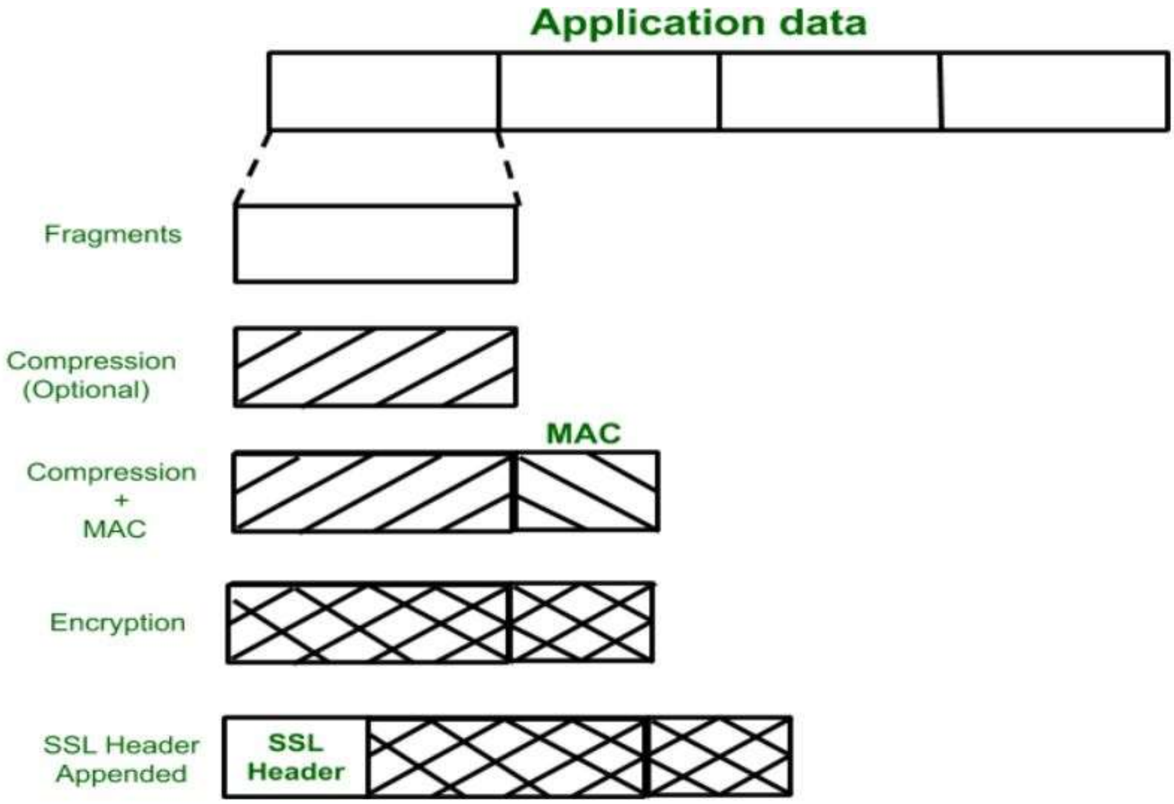


SSL Record Protocol:

SSL Record provide two services to SSL connection.

- Confidentiality
- Message Integrity

In SSL Record Protocol application data is divided into fragments. The fragment is compressed and then encrypted MAC (Message Authentication Code) generated by algorithms like SHA (Secure Hash Protocol) and MD5 (Message Digest) is appended. After that encryption of the data is done and in last SSL header is appended to the data.

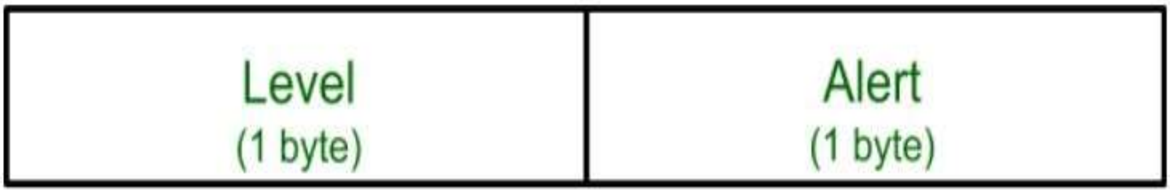


Handshake Protocol:
Handshake Protocol is used to establish sessions. This protocol allow client and server to authenticate each other by sending a series of messages to each other. Handshake protocol uses four phases to complete its cycle.

- **Phase-1:** In Phase-1 both Client and Server send hello-packets to each other. In this IP session, cipher suite and protocol version are exchanged for security purpose.
- **Phase-2:** Server send his certificate and Server-key-exchange. Server end the phase-2 by sending Server-hello-end packet.
- **Phase-3:** In this phase Client reply to the server by sending his certificate and Client-exchange-key.
- **Phase-4:** In Phase-4 Change-cipher suite occurred and after this Handshake Protocol ends.

Change-cipher Protocol:
This protocol uses SSL record protocol. Unless Handshake Protocol is completed, the SSL record Output will be in pending state. After handshake protocol the Pending state is converted into Current state.
Change-cipher protocol consists of single message which is 1 byte in length and can have only one value. This protocol purpose is to cause the pending state to be copied into current state.

Alert Protocol:
This protocol is used to convey SSL-related alerts to the peer entity. Each message in this protocol contain 2 bytes.



Level (1 byte)	Alert (1 byte)

Level is further classified into two parts:

- **Warning:**
  This Alert have no impact on the connection between sender and receiver.
- **Fatal Error:**
  This Alert breaks the connection between sender and receiver.

Silent Features of Secure Socket Layer:

- Advantage of this approach is that the service can be tailored to the specific needs of the given application.
- Secure Socket Layer was originated by Netscape.
- SSL is designed to make use of TCP to provide reliable end-to-end secure service.
- This is two-layered protocol.

Difference between Secure Socket Layer (SSL) and Transport Layer Security (TLS)

SSL stands for Secure Socket Layer while TLS stands for Transport Layer Security. Both Secure Socket Layer and Transport Layer Security are the protocols used to provide the security between web browser and web server.
The main difference between Secure Socket Layer and Transport Layer Security is that. In SSL (Secure Socket Layer), Message digest is used to create master secret and It provides the basic security services which are **Authentication** and **confidentiality**. while In TLS (Transport Layer Security), Pseudo-random function is used to create master secret.
There are some differences between SSL and TLS which are given below:

S.NO	SSL	TLS
1.	SSL stands for Secure Socket Layer.	TLS stands for Transport Layer Security.

2.	SSL (Secure Socket Layer) supports **Fortezza** algorithm.	TLS (Transport Layer Security) does not supports **Fortezza** algorithm.
3.	SSL (Secure Socket Layer) is the 3.0 version.	TLS (Transport Layer Security) is the 1.0 version.
4.	In SSL(Secure Socket Layer), Message digest is used to create master secret.	In TLS(Transport Layer Security), Pseudo-random function is used to create master secret.
5.	In SSL(Secure Socket Layer), Message Authentication Code protocol is used.	In TLS(Transport Layer Security), Hashed Message Authentication Code protocol is used.
6.	SSL (Secure Socket Layer) is complex than TLS(Transport Layer Security).	TLS (Transport Layer Security) is simple.