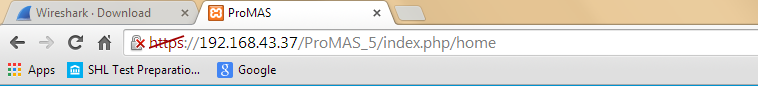
On data request such as web page made on a server during internet communication runs through multiple program layers on a server.

Demonstration of the working of SSL following below used Wireshark network analysis tool to capture and analyze communication packets between server (web-server: 192.168.43.37) and the client (Web-browser: 192.168.46.228). The snippets below show some of the packet information relevant to a particular step in the SSL working process.

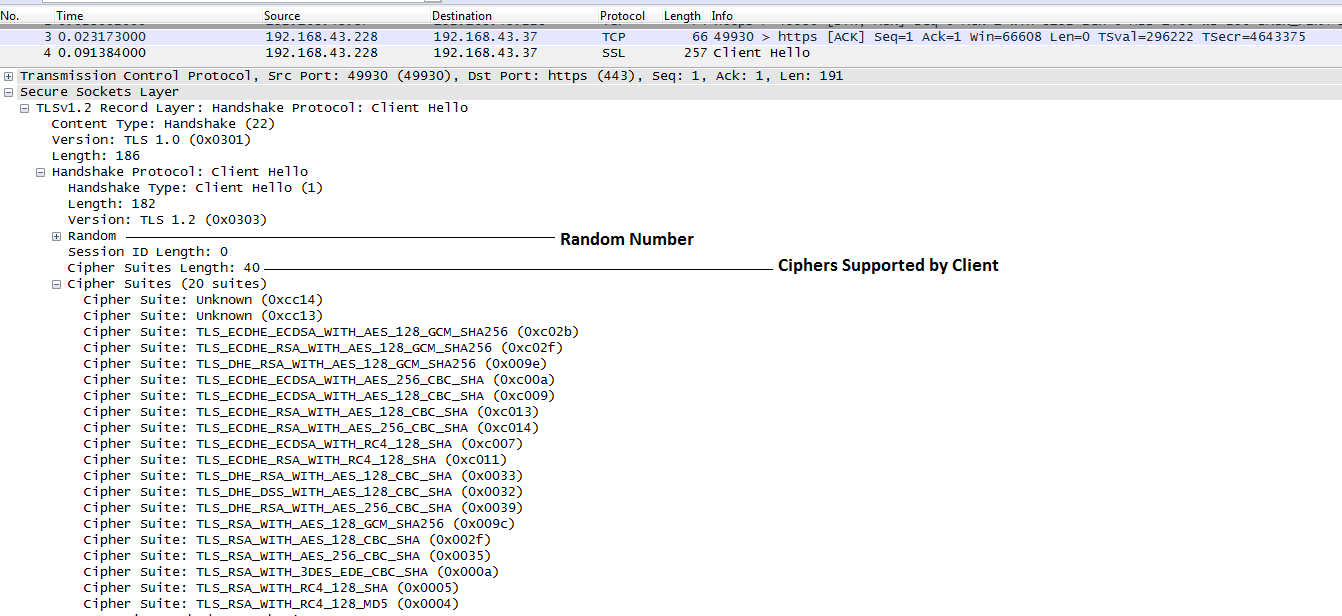
On using secure communication between server and client, a client (web browser) sends a request on high level protocol such as HTTP, IMAP and FTP then these protocol process the request through the secure connection that is SSL if the request is meant for a secure connection. A secure connection on HTTP protocol is demonstrated below.



Once the request is submitted hand shake mechanism is initiated this involves several steps as follows.

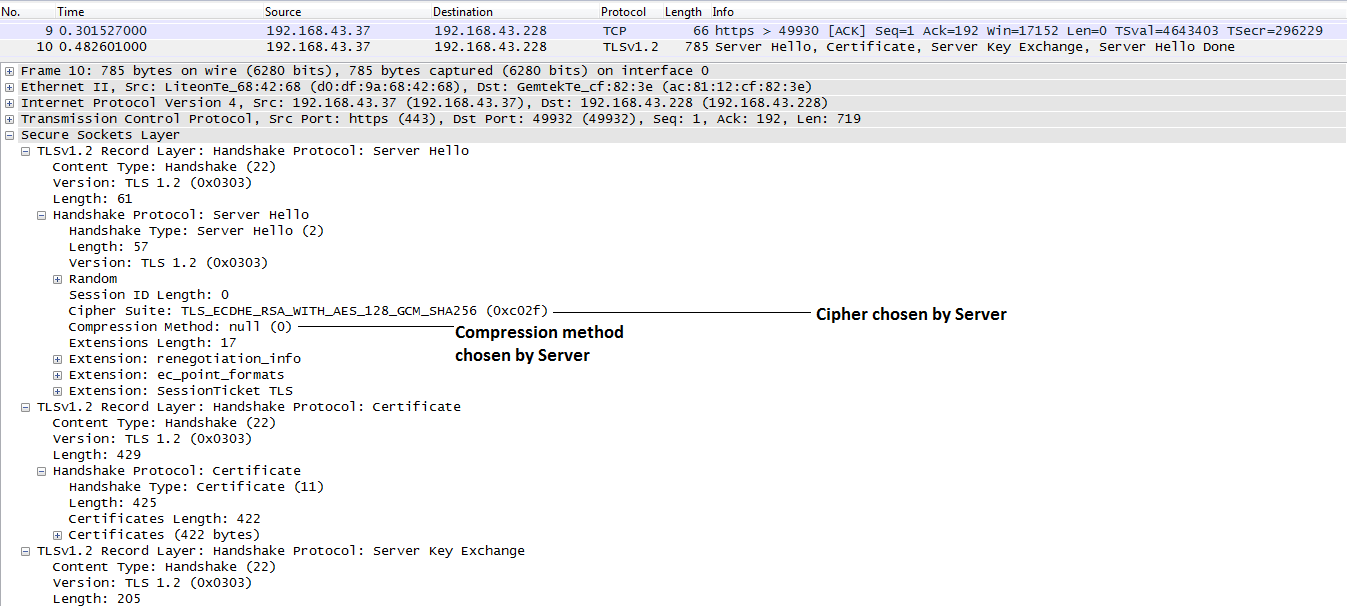
1. Client hello

First the client computer (web browser) sends hello message to the server, the hello message contains key exchange methods, cipher as the way to encrypt data between server and client, hash methods for data integrity and authentication of data, SSL version used on the client computer and random number used for computing master secrete that used to calculate encryption keys.



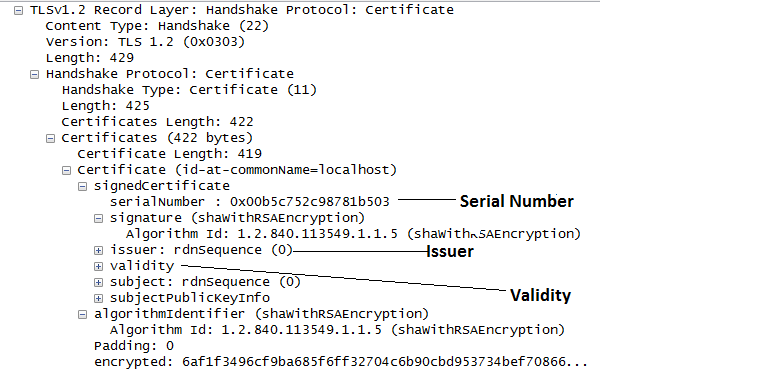
1. Server hello

Then server sends hello message back to the client with the list of chosen key exchange methods, cipher as the way to encrypt data between server and client, hash methods from the one suggested by the client hello message

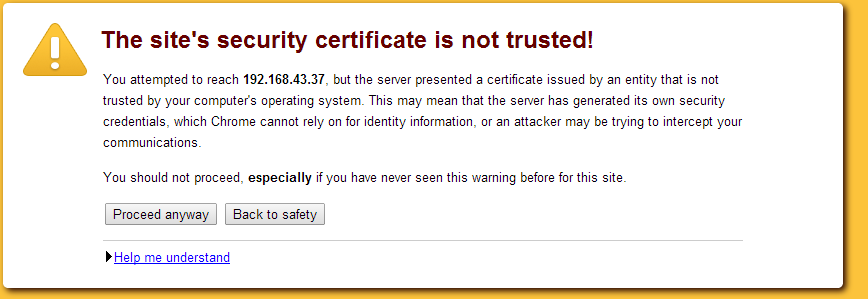


1. Server sends certificate

The next step is server send certificate to the client that contains serial number, public key, certificate issuer, validity period of the certificate and other relevant information.

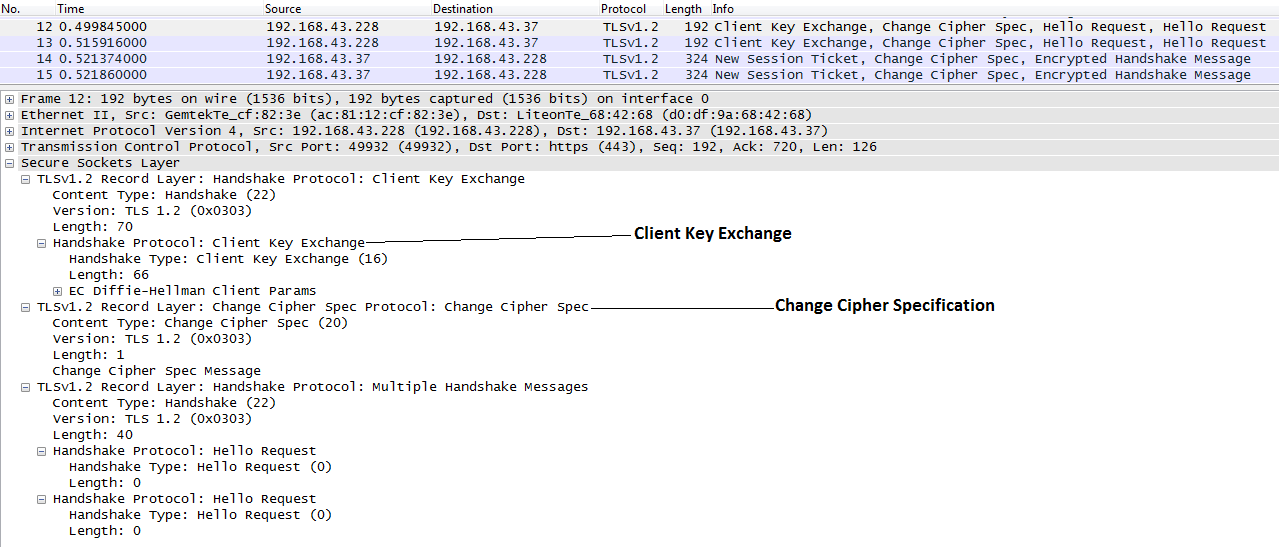


If the certificate is not signed by a verified issuer the client might prompt the user to proceed with an unsigned verification. In a Chrome browser the user would get a notification such as the one shown below.



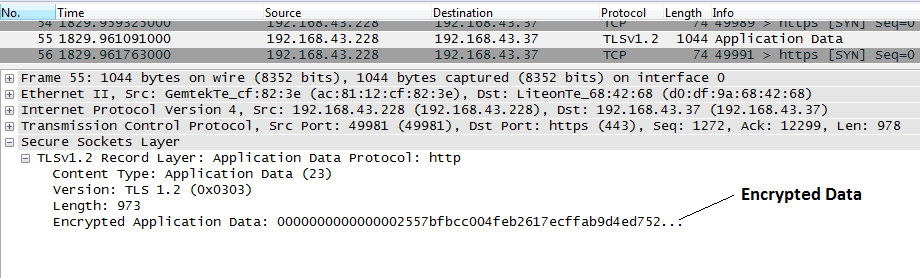
1. Client and server agree to start encryption

Both server and client sending hello packets. The packet contains the client key exchange information and the change cipher specification which was agreed on previously.



1. All communication between server and client is now encrypted

Because encrypting and decrypting with private and public key takes a lot of processing power, they are only used during the SSL Handshake to create a symmetric session key. After the secure connection is made, the session key is used to encrypt all transmitted data. Therefore server and client exchange data using the encryption specifications agreed until the SSL session expires after the validity period is reached.



As opposed to browser communication over SSL (https), http send unencrypted data. See example below where an attacker could intercept sensitive information.

