可以使用wireshark抓包工具

安全传输层协议

肯定实现TCP3次握手，不然怎么传输证书什么的呢！！！

首先协商用什么样的协议连接。  
1.客户端发送一个类型为Client Hello的TLS握手包，携带客户端支持的TLS协议版本， 支持的密钥交换算法的集合。Content-Type：Handshake，以及随机数Random1。

2.Server Hello的TLS握手包中携带服务器选取的特定的密钥交换算法，以及随机数Random2，这两个随机数会在后续生成对称密钥的时候用到。

3.Certificate的TLS握手包携带自己的数字证书。

4.Server Hello Done的TLS握手包发送给客户端。客户端随后验证证书可靠性，如不可靠，则发出预警，并询问是否手动设置信任关系。

5.客户端生成密钥，使用Random1和Random2生成Random3，用服务器公钥加密，生成PreMater Key，在Client Key Exchange的TLS握手包携带

6.客户端发送Change Cipher Spec（Client），和服务器端说明，此后的通信都是用密钥了，这是一条消息信息。

7.Encrypted Handshake Message（Client），是Client Finished 包，且这是第一个密钥加密的包，服务端接收到之后，如果能解密，则说明一切正常。

8. Change Cipher Spec（Server），和客户端说明，服务器此后的通信都是密钥加密了，这也是一个消息信息。

9. Encrypted Handshake Message（Server），是Server Finished包。