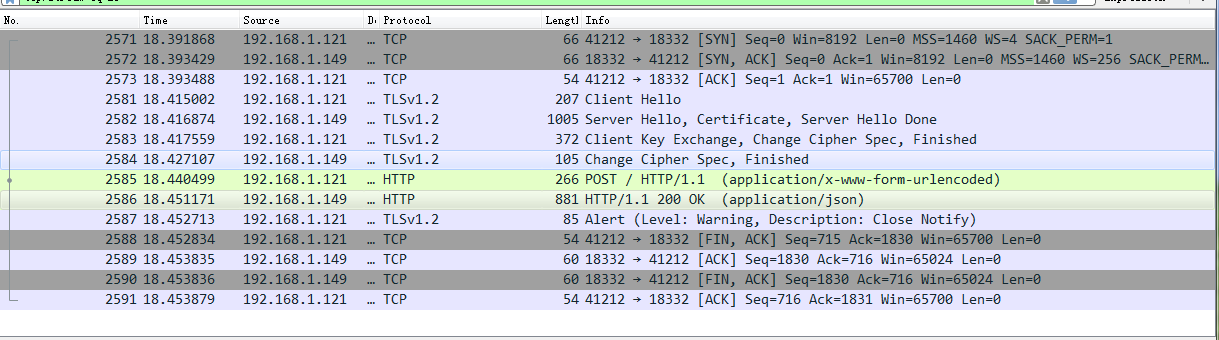
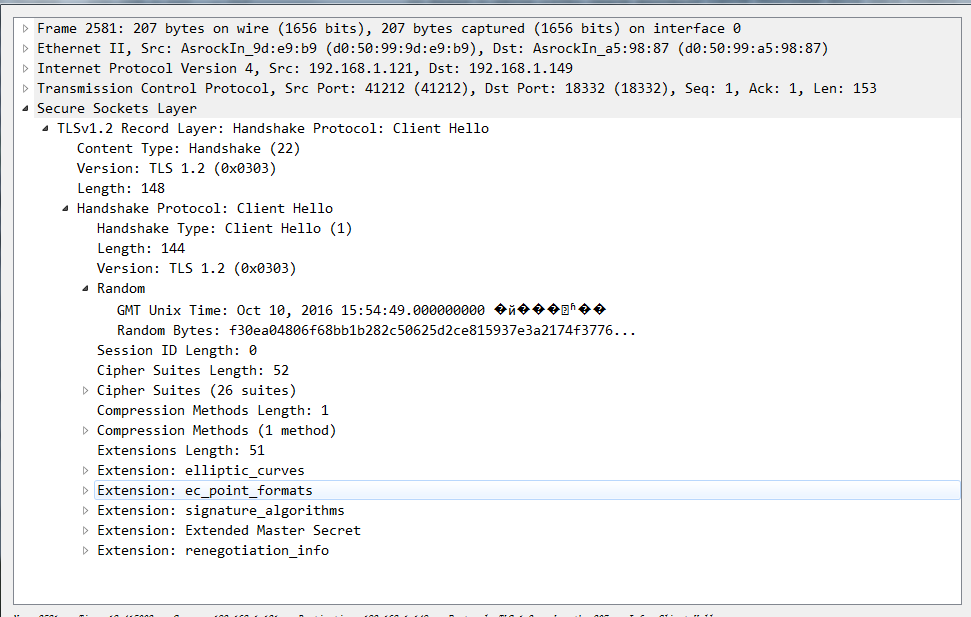
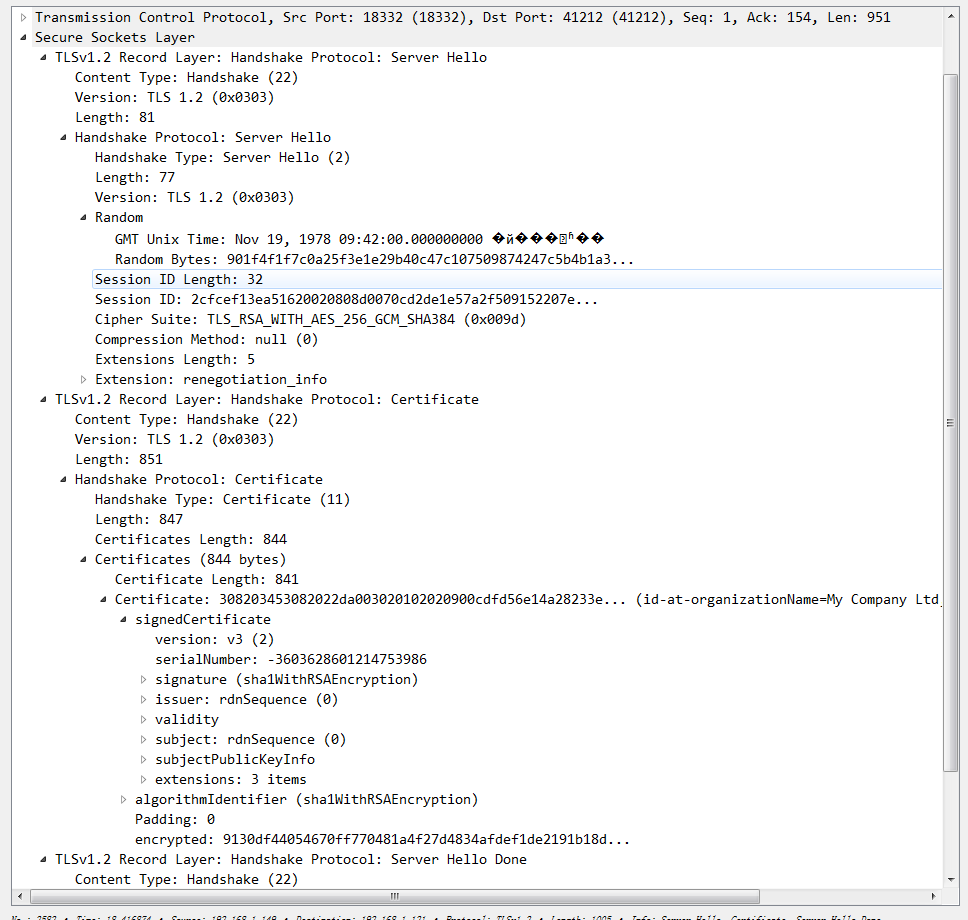
客户端向服务端发送RPC命令，经过证书加密后，抓包工具抓到的数据如下：



client发送ClientHello，指定版本，随机数(RN)，所有支持的密码套件(CipherSuites)：



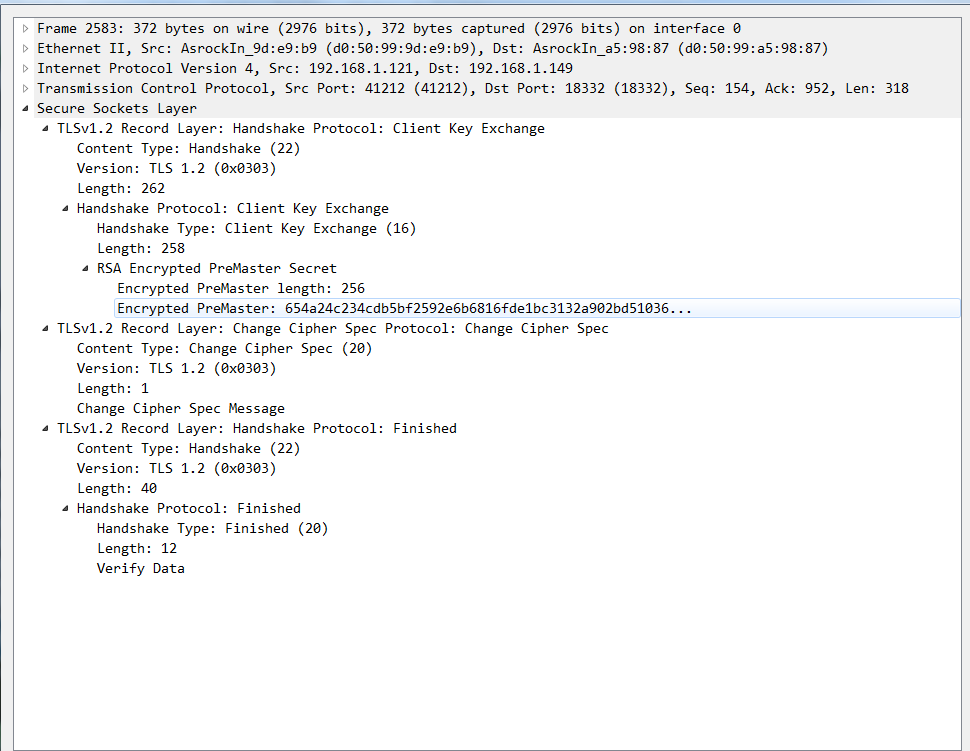
server回应ServerHello，指定版本，RN，选择CipherSuites，会话ID(Session ID)：



Client发送ClientKeyExchange，用于与server交换session key，

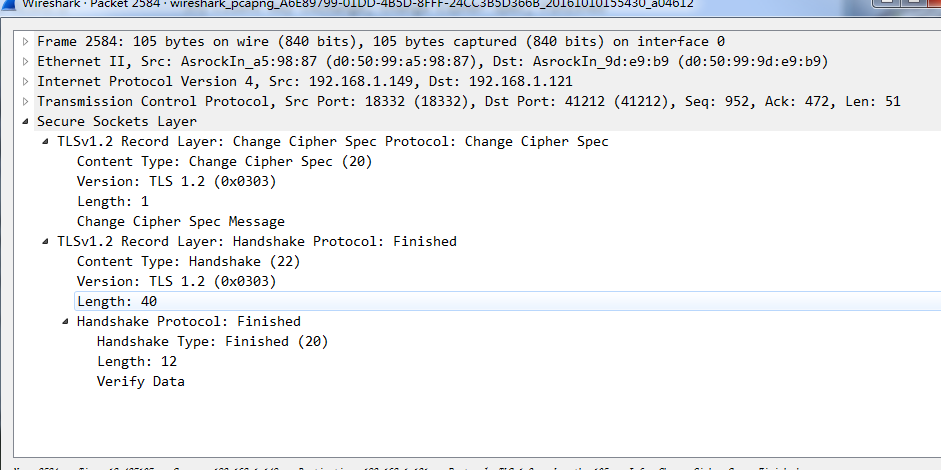
Client发送ChangeCipherSpec，指示Server从现在开始发送的消息都是加密过的，

Client发送Finishd，包含了前面所有握手消息的hash，可以让server验证握手过程是否被第三方篡改

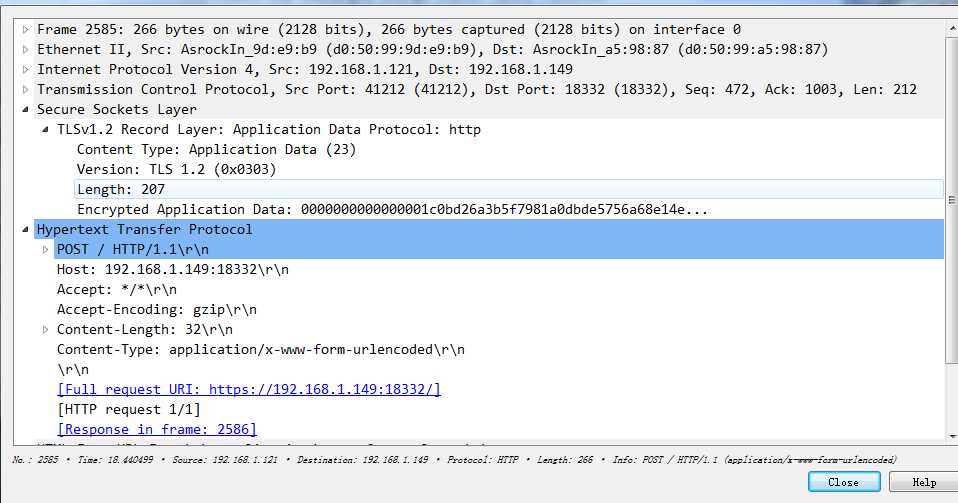


Server发送ChangeCipherSpec，指示Client从现在开始发送的消息都是加密过的

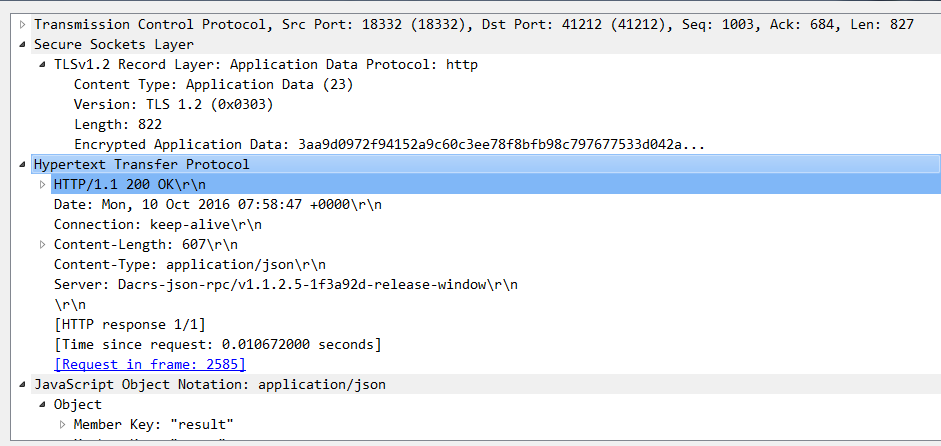
Server发送Finishd，包含了前面所有握手消息的hash，可以让client验证握手过程是否被第三方篡改，并且证明自己是Certificate密钥的拥有者，即证明自己的身份



客户端通过http发送RPC数据请求：



服务端返回给客户端的数据：application/json是明文数据



https通过抓包工具，加密无效，证书没有起作用；

比特币版本0.12.0提示SSL加密模式不在支持：

