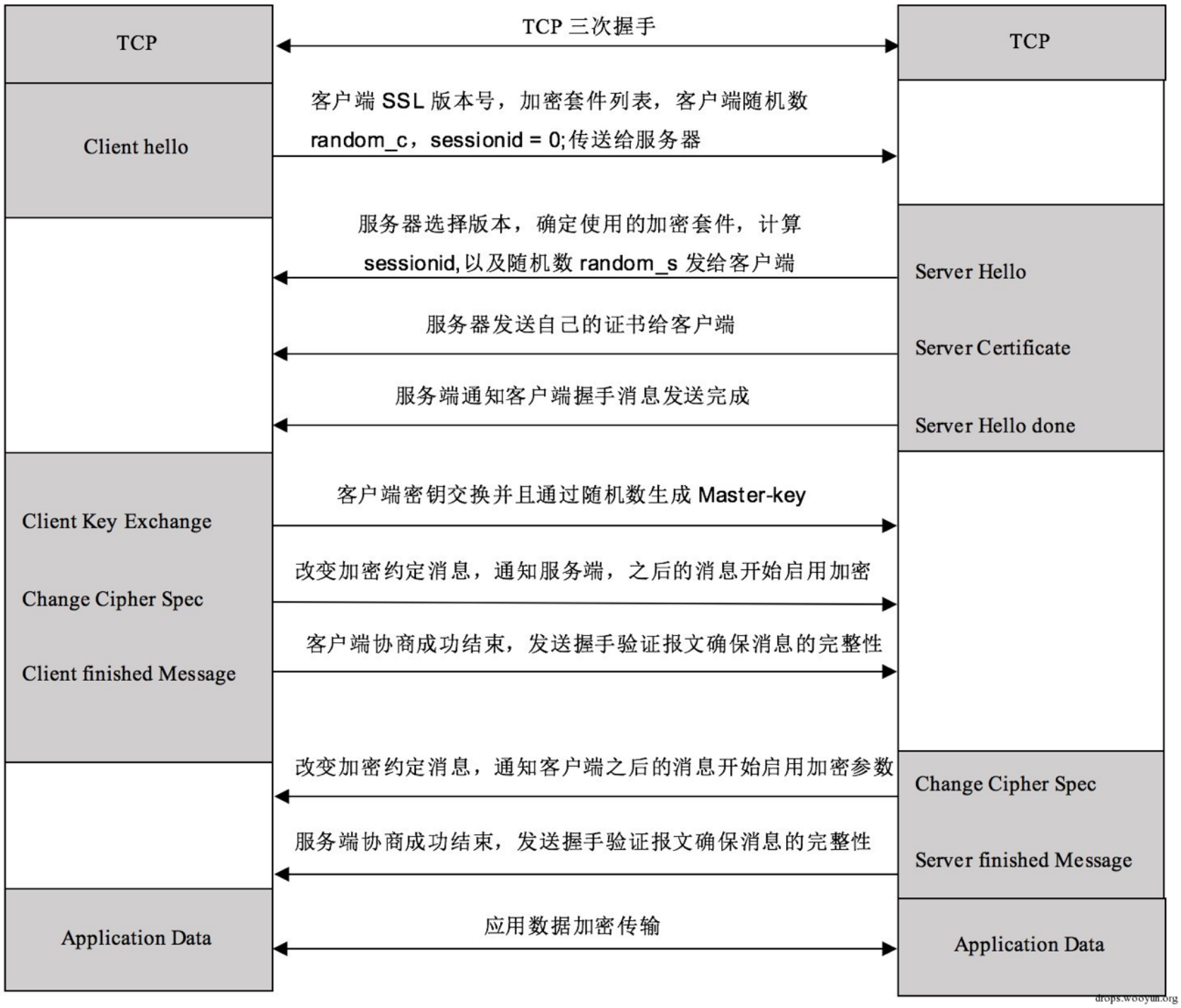
谈HTTPS中间人攻击与证书校验（一）

一、前言

随着安全的普及，https通信应用越发广泛，但是由于对https不熟悉导致开发人员频繁错误的使用https，例如最常见的是未校验https证书从而导致“中间人攻击”，并且由于修复方案也一直是个坑，导致修复这个问题时踩各种坑，故谨以此文简单的介绍相关问题。

本文第一节主要讲述https的握手过程，第二节主要讲述常见的“https中间人攻击”场景，第三节主要介绍证书校验修复方案，各位看官可根据自己口味浏览。

二、HTTPS握手过程

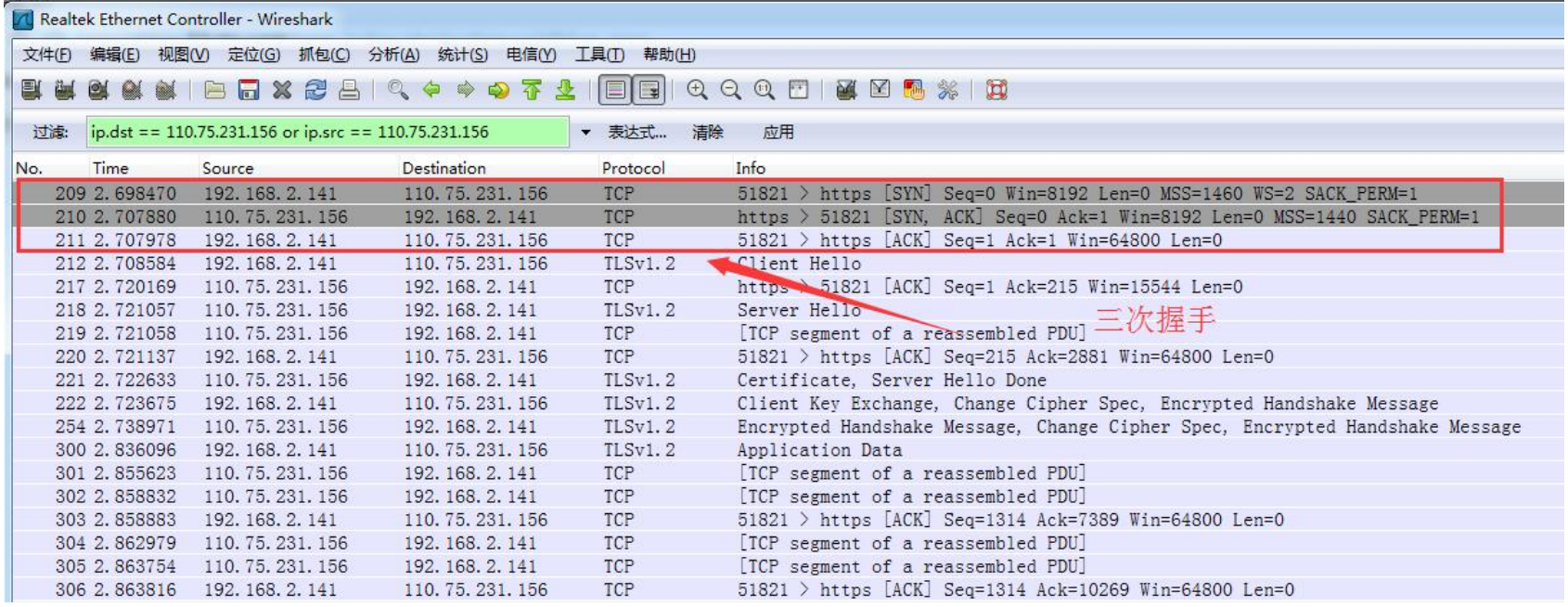


首先来看下https的工作原理，上图大致介绍了https的握手流程，后续我们通过抓包看下每个握手包到底干了些什么神奇的事。

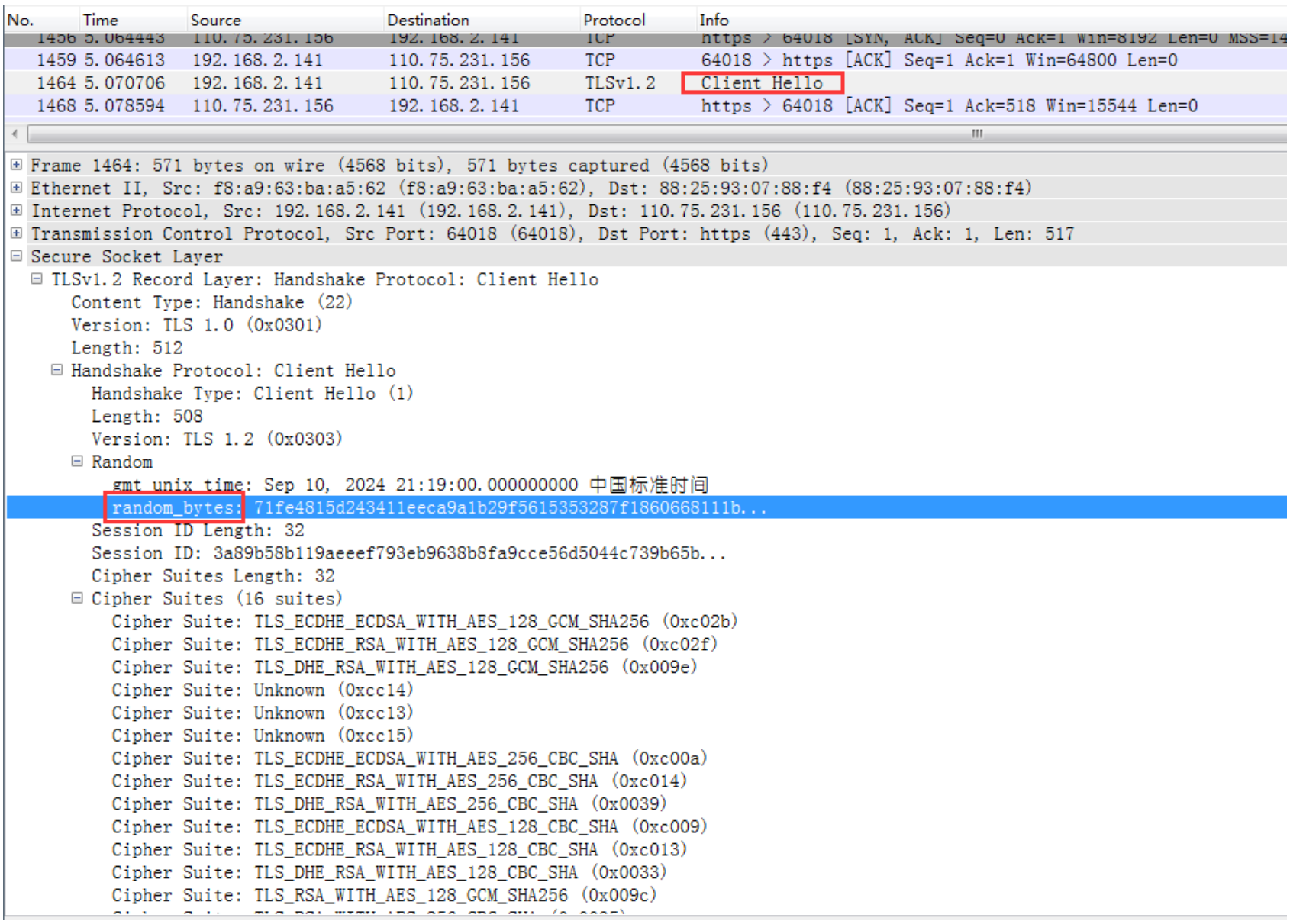
注：本文所有内容以TLS_RSA_WITH_AES_128_CBC_SHA加密组件作为基础进行说明，其他加密组件以及TLS版本会存在一定差异，例如TLS1.3针对移动客户端有了很大的改动，现在的ECDHE等密钥交换算法与RSA作为密钥交换算法也完全不一样，所以有些地方和大家实际操作会存在一定出入。

1.TCP三次握手

我访问的支付宝的官网www.alipay.com抓取的数据。

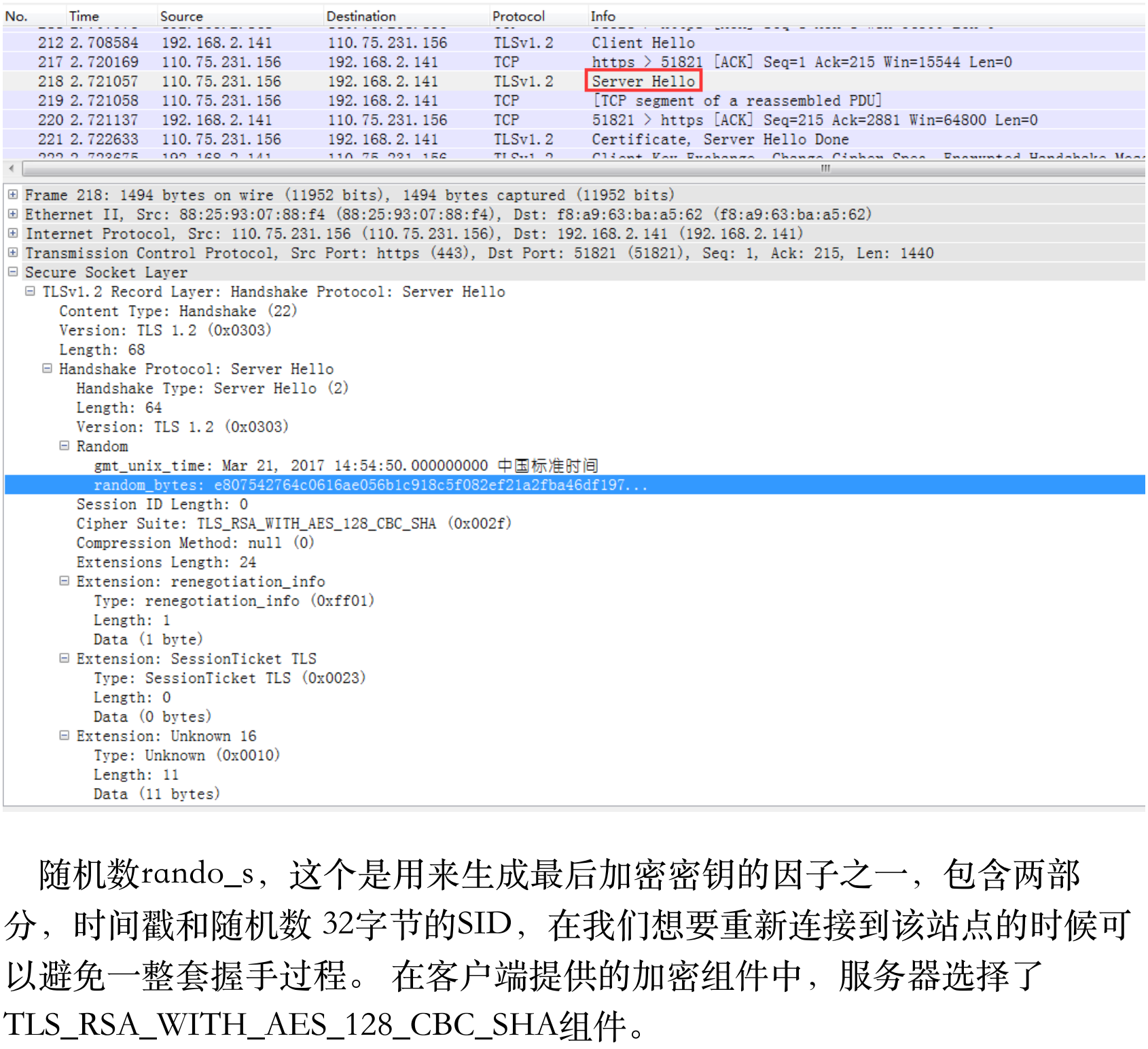


2.Client Hello



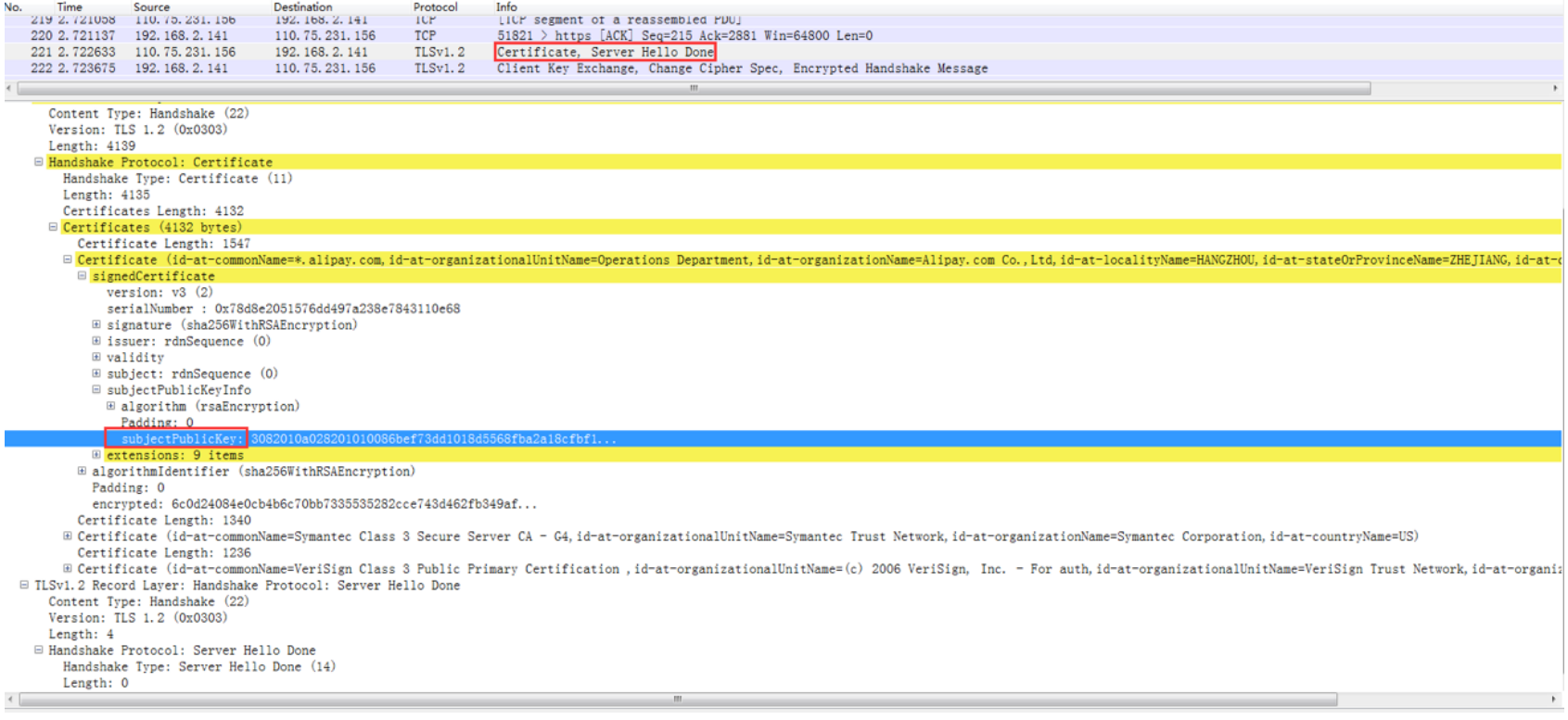
TLS的版本号和随机数random_c：这个是用来生成最后加密密钥的因子之一，它包含两部分，时间戳和随机数 session-id：用来标识会话，第一次握手时为空，如果以前建立过，可以直接带过去从而避免完全握手 Cipher Suites加密组件列表：浏览器所支持的加密算法的清单客户端支持的加密签名算法的列表，让服务器进行选择 扩展字段：比如密码交换算法的参数、请求主机的名字，用于单ip多域名的情况指定域名。

3.Sever Hello



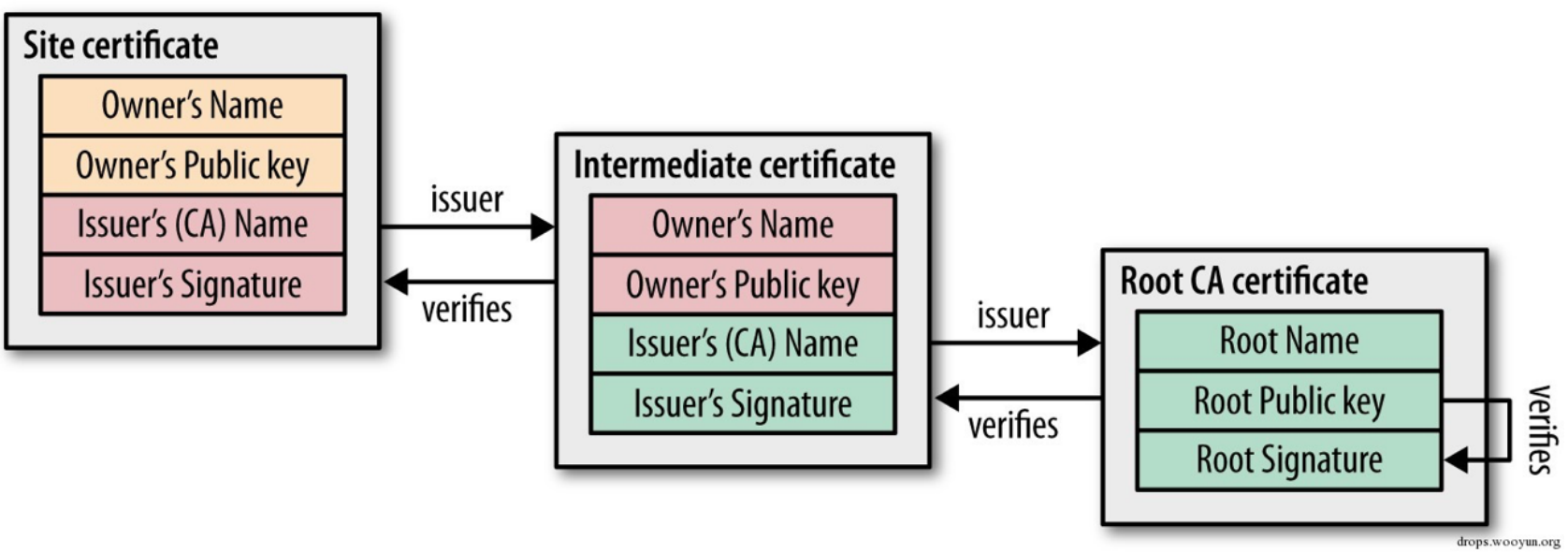
随机数rando_s，这个是用来生成最后加密密钥的因子之一，包含两部分，时间戳和随机数 32字节的SID，在我们想要重新连接到该站点的时候可以避免一整套握手过程。 在客户端提供的加密组件中，服务器选择了TLS_RSA_WITH_AES_128_CBC_SHA组件。

4.Certificate

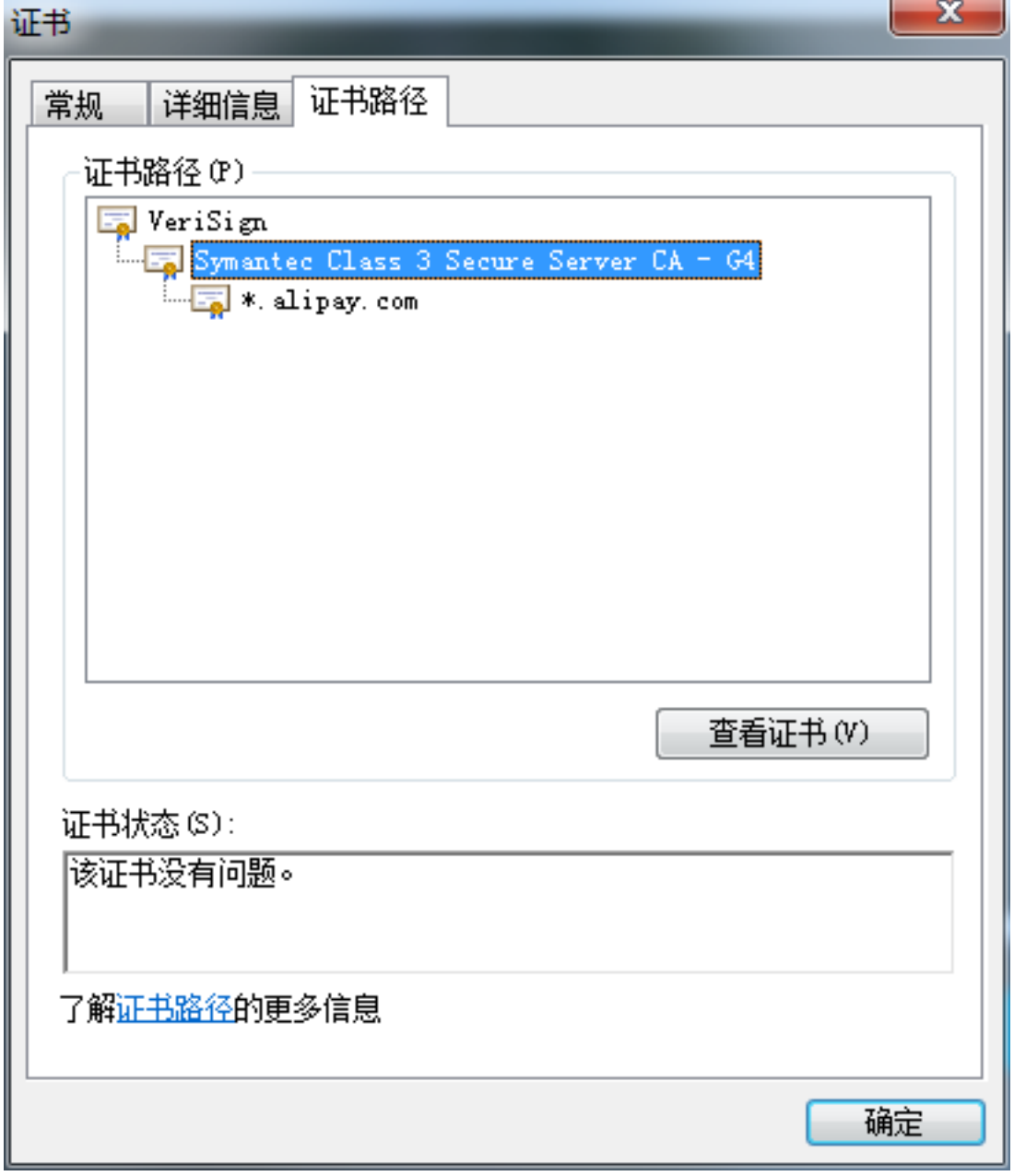


证书是https里非常重要的主体，可用来识别对方是否可信，以及用其公钥做密钥交换。可以看见证书里面包含证书的颁发者，证书的使用者，证书的公钥，颁发者的签名等信息。其中Issuer Name是签发此证书的CA名称,用来指定签发证书的CA的可识别的唯一名称(DN, Distinguished Name)，用于证书链的认证，这样通过各级实体证书的验证，逐渐上溯到链的终止点，即可信任的根CA，如果到达终点在自己的信任列表内未发现可信任的CA则认为此证书不可信。

验证证书链的时候，用上一级的公钥对证书里的签名进行解密，还原对应的摘要值，再使用证书信息计算证书的摘要值，最后通过对比两个摘要值是否相等，如果不相等则认为该证书不可信，如果相等则认为该级证书链正确，以此类推对整个证书链进行校验。



二级机构的证书。


证书
常规
详细信息
证书路径
证书路径(P)
VeriSign
Symantec Class 3 Secure Server CA - G4
*.alipay.com
查看证书(V)
证书状态(S):
该证书没有问题。
了解证书路径的更多信息
确定

支付宝官网签名证书。

证书

常规 | 详细信息 | 证书路径

证书信息

这个证书的目的如下:

- 保证远程计算机的身份
- 向远程计算机证明您的身份

颁发给: *.alipay.com

颁发者: Symantec Class 3 Secure Server CA - G4

有效期从 2016/ 3/ 2 **到** 2017/ 4/ 2

颁发者说明(S)

了解证书的详细信息

确定

证书

常规 | 详细信息 | 证书路径

显示(S): <所有>

字段	值
版本	V3
序列号	78 d8 e2 05 15 76 dd 49...
签名算法	sha256RSA
签名哈希算法	sha256
颁发者	Symantec Class 3 Secure...
有效期从	2016年3月2日 8:00:00
到	2017年4月2日 7:59:59

```
CN = *.alipay.com
OU = Operations Department
O = Alipay.com Co.,Ltd
L = HANGZHOU
S = ZHEJIANG
C = CN
```

编辑属性(E)... 复制到文件(C)...

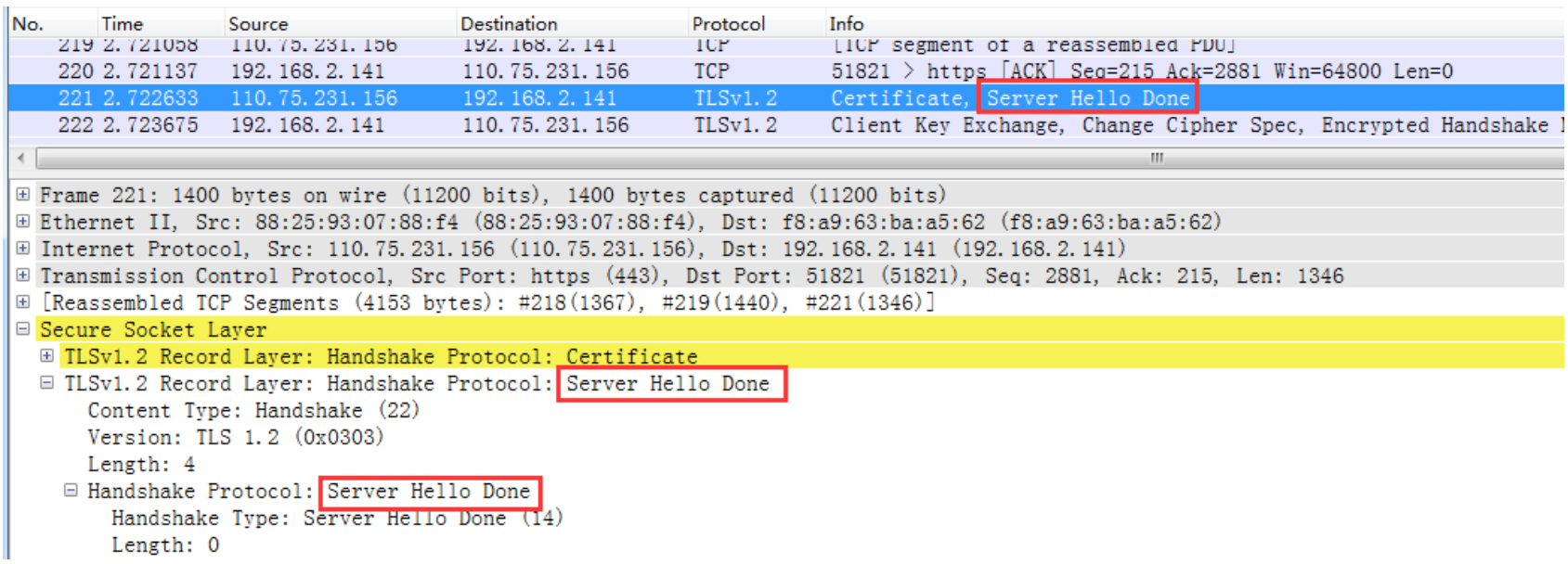
了解证书详细信息的更多信息

确定

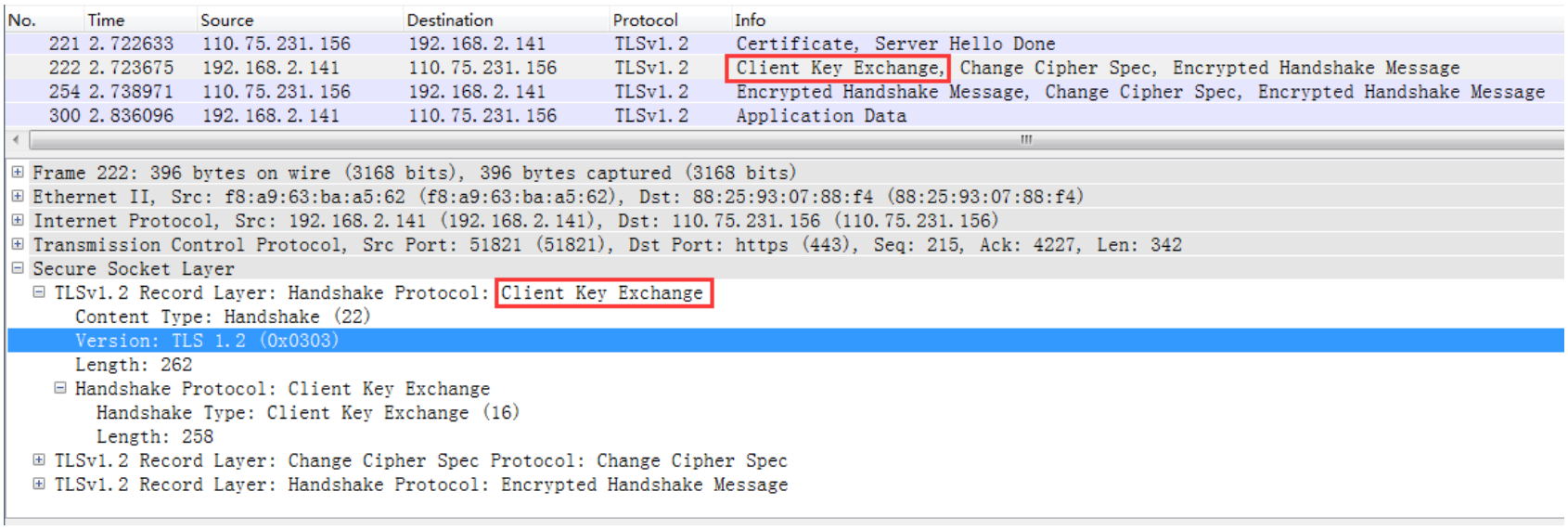
不仅仅进行证书链的校验，此时还会进行另一个协议即Online Certificate Status Protocol, 该协议为证书状态在线查询协议，一个实时查询证书是否吊销的方式，客户端发送证书的信息并请求查询，服务器返回正常、吊销或未知中的任何一个状态，这个查询地址会附在证书中供客户端使用。

5.Server Hello Done

这是一个零字节信息，用于告诉客户端整个server hello过程已经结束。



6.ClientKeyExchange



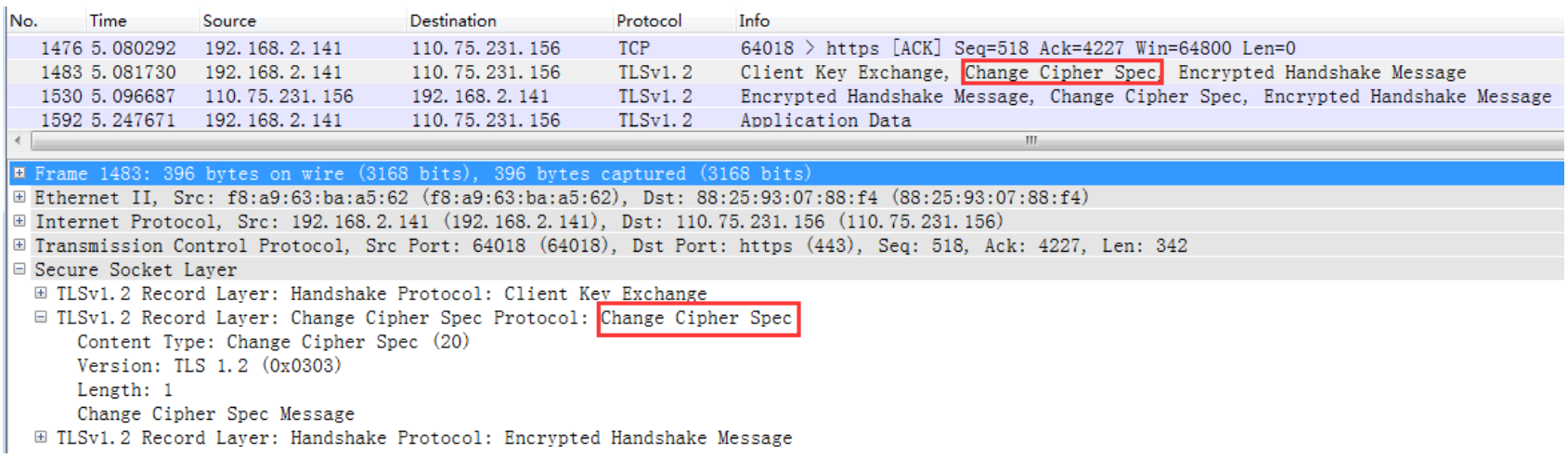
客户端在验证证书有效之后发送ClientKeyExchange消息，ClientKeyExchange消息中，会设置48字节的premaster secret（因为的TLS版本的原因，这里没有显示premaster），通过密钥交换算法加密发送premaster secret的值，例如通过 RSA公钥加密premaster secret的得到Encrypted PreMaster传给服务端。PreMaster前两个字节是TLS的版本号，该版本号字段是用来防止版本回退攻击的。

从握手包到目前为止，已经出现了三个随机数(客户端的random_c，服务

端的random_s，premaster secret)，使用这三个随机数以及一定的算法即可获得对称加密AES的加密主密钥Master-key，主密钥的生成非常的精妙。

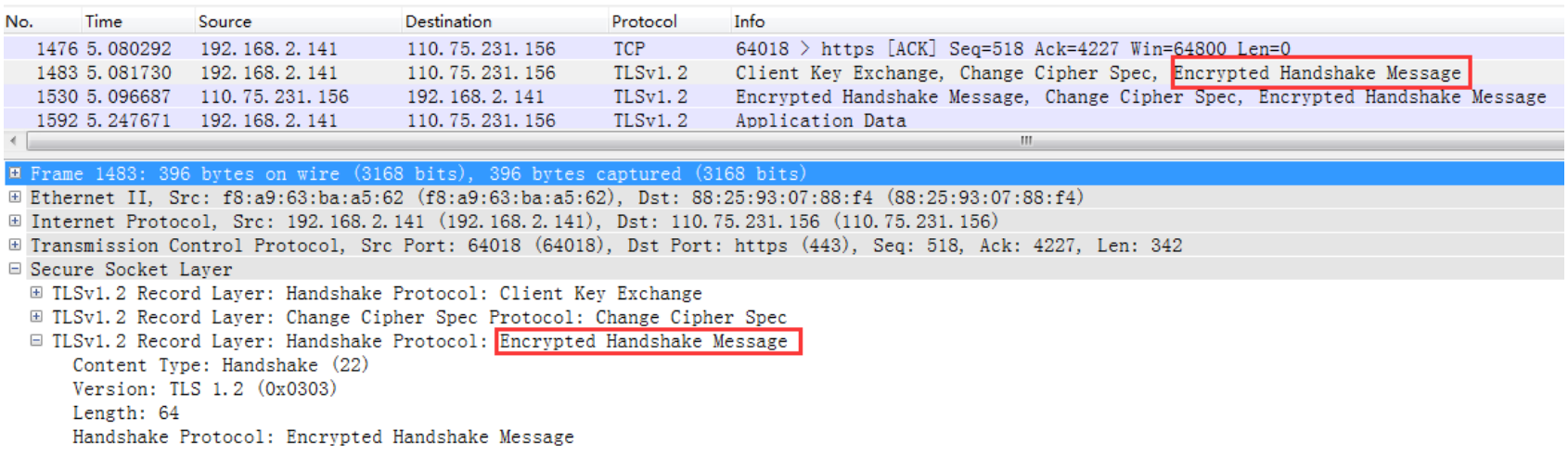
7.Change Cipher Spec

发送一个不加密的信息，浏览器使用该信息通知服务器后续的通信都采用协商的通信密钥和加密算法进行加密通信。



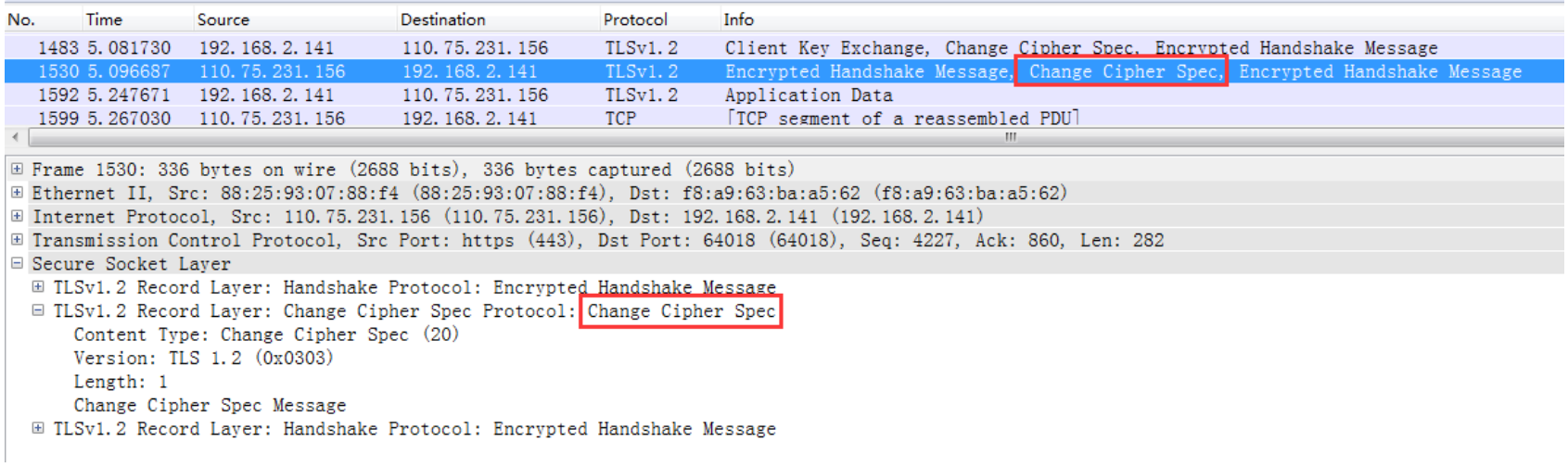
8.Encrypted Handshake Message

验证加密算法的有效性，结合之前所有通信参数的 hash 值与其它相关信息生成一段数据，采用协商密钥 session secret 与算法进行加密，然后发送给服务器用于数据与握手验证，通过验证说明加密算法有效。



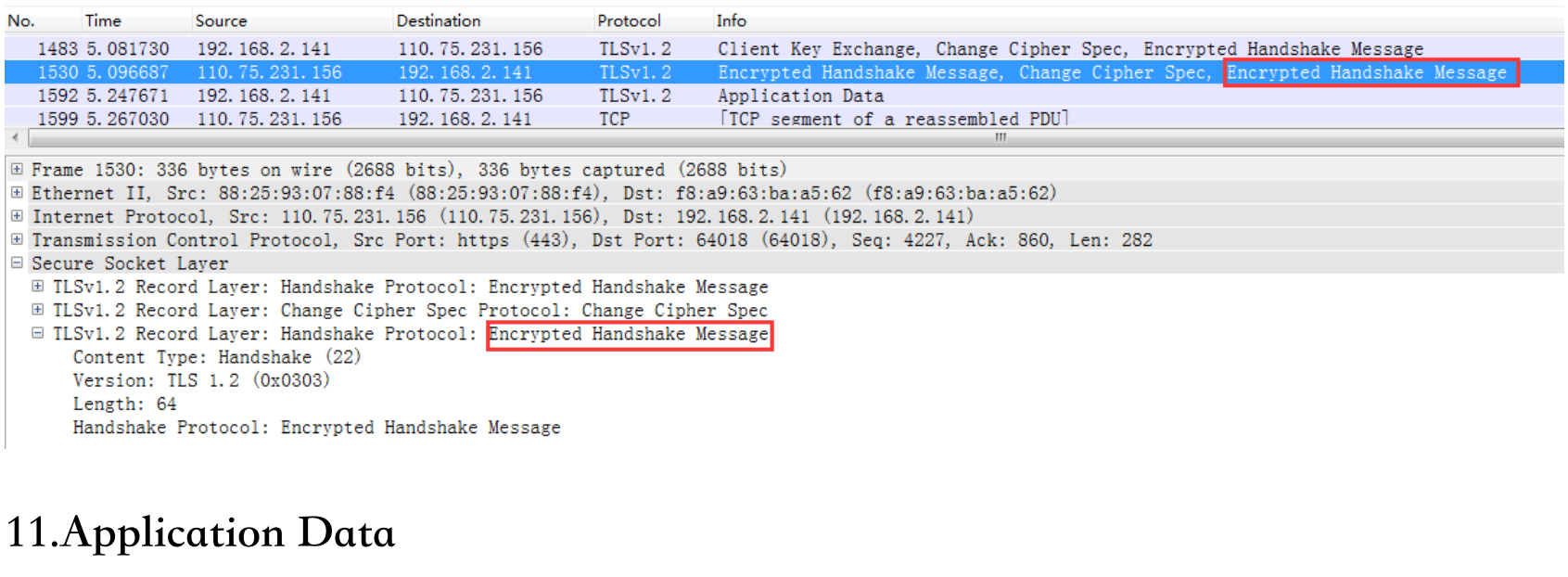
9.Change_cipher_spec

Encrypted Handshake Message通过验证之后，服务器同样发送 change_cipher_spec 以通知客户端后续的通信都采用协商的密钥与算法进行加密通信。



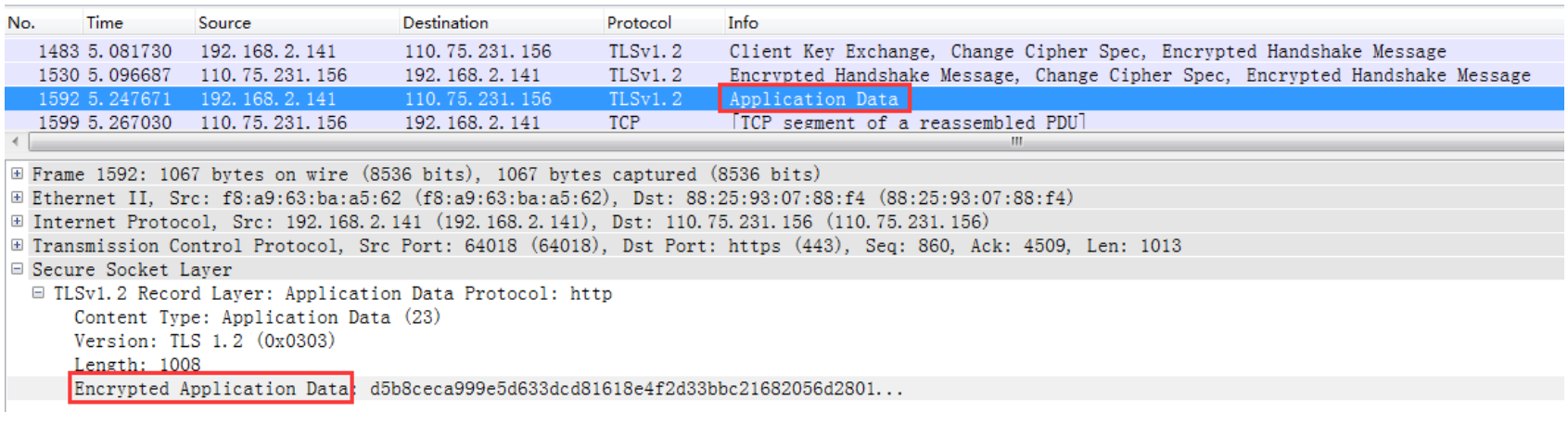
10.Encrypted Handshake Message

同样的，服务端也会发送一个Encrypted Handshake Message供客户端验证加密算法有效性。



11.Application Data

经过一大串的的计算之后，终于一切就绪，后续传输的数据可通过主密钥master key进行加密传输，加密数据查看图中的Encrypted Apploication Data字段数据，至此https的一次完整握手以及数据加密传输终于完成。



https里还有很多可优化并且很多精妙的设计，例如为了防止经常进行完整的https握手影响性能，于是通过sessionid来避免同一个客户端重复完成握手，但是又由于sessionid消耗的内存性能比较大，于是又出现了new session ticket，如果客户端表明它支持Session Ticket并且服务端也支持，那么在TLS

握手的最后一步服务器将包含一个“New Session Ticket”信息，其中包含了一个加密通信所需要的信息，这些数据采用一个只有服务器知道的密钥进行加密。这个Session Ticket由客户端进行存储，并可以在随后的一次会话中添加到 ClientHello消息的SessionTicket扩展中。虽然所有的会话信息都只存储在客户端上，但是由于密钥只有服务器知道，所以Session Ticket仍然是安全的，因此这不仅避免了性能消耗还保证了会话的安全性。

最后我们可以使用openssl命令来直观的看下https握手的流程：

```
[root@localhost ~]# openssl s_client -state -connect www.alipay.com:443
CONNECTED(00000003)
SSL_connect:before/connect initialization
SSL_connect:SSLv2/v3 write client hello A
SSL_connect:SSLv3 read server hello A
depth=3 C = US, O = "VeriSign, Inc.", OU = Class 3 Public Primary Certification Authority
verify return:1
depth=2 C = US, O = "VeriSign, Inc.", OU = VeriSign Trust Network, OU = "(c) 2006 VeriSign, Inc. - For authorized use only", CN = VeriSign Class 3 Public Primary Certifica
tion Authority - G5
verify return:1
depth=1 C = US, O = Symantec Corporation, OU = Symantec Trust Network, CN = Symantec Class 3 Secure Server CA - G4
verify return:1
depth=0 C = CN, ST = ZHEJIANG, L = HANGZHOU, O = "Alipay.com Co.,Ltd", OU = Operations Department, CN = *.alipay.com
verify return:1
SSL_connect:SSLv3 read server certificate A
SSL_connect:SSLv3 read server done A
SSL_connect:SSLv3 write client key exchange A
SSL_connect:SSLv3 write change cipher spec A
SSL_connect:SSLv3 write finished A
SSL_connect:SSLv3 flush data
SSL_connect:SSLv3 read server session ticket A
SSL_connect:SSLv3 read finished A
---
Certificate chain
 0 s:/C=CN/ST=ZHEJIANG/L=HANGZHOU/O=Alipay.com Co.,Ltd/OU=Operations Department/CN=*.alipay.com
   i:/C=US/O=Symantec Corporation/OU=Symantec Trust Network/CN=Symantec Class 3 Secure Server CA - G4
 1 s:/C=US/O=Symantec Corporation/OU=Symantec Trust Network/CN=Symantec Class 3 Secure Server CA - G4
   i:/C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c) 2006 VeriSign, Inc. - For authorized use only/CN=VeriSign Class 3 Public Primary Certification Authority - G5
 2 s:/C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c) 2006 VeriSign, Inc. - For authorized use only/CN=VeriSign Class 3 Public Primary Certification Authority - G5
   i:/C=US/O=VeriSign, Inc./OU=Class 3 Public Primary Certification Authority
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIGBzCCBO+gAwIBAgIQeNjiBRV23Ul6I454QxEOaDANBgkqhkiG9w0BAQsFADB+
MQswCQYDVQQGEwJVUzEdMBsGA1UEChMUU3lTYW50ZWMgQ29ycG9yYXRpb24xHzAd
BgNVBAsTFlN5bWFudGVjIFRydXN0IE5ldHdvcmsxLzAtBgNVBAMTJlN5bWFudGVj
IENsYXNzIDMgU2VjdXJlIFNlcnZlciBDQSAtIEc0MB4XDTE2MDMwMjAwMDAwMFoX
DTE3MDQwMTIzNTk1OVowgYcxCzAJBgNVBAYTAkNOMREwDwYDVQQIEwhaSEVKSUFO
RzERMA8GA1UEBxQISEFOR1pIT1UxGzAZBgNVBAoUEkFsaXBheS5jb20gQ28uLExO
ZDEeMBwGA1UECxQVT3BlcmF0aW9ucyBEZXBhcnRtZW50MRUwEwYDVQQDFAwqLmFs
aXBheS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCGvvc9OQGN
VWj7oqGM+/G8gQUrAZyIsPFCJimIOEhCfk/O/mXJNGamNRF+512fHDO7Ur8w1U+G
mtOaqyuvP8GnOlDy/7ll6f2xfCfrLnmifM82QuK8gKqTVPj15LltlVOAfJ7l4Qh2
1ALmIEJRGd/qJjySWxvzvOryi2sF5tHn7yOCArqANifV9vbFFUVYgwI88+8fQIre
MuUobmopu1kJQ1G+shdTGBQO29z2kL8RiBtCO2kn4AjqxpYn7KMb8c+Kxm3m19ln
fb/bjHhhXL8hKAjV6QjuzV+F/BeK1VDCKnnvTAcZD3MYDWmmOITcZ644EmUcCrNF
PdjtKuy8rO75AgMBAAGjggJ1MIICcTAjBgNVHREEHDAaggwqLmFsaXBheS5jb22C
```