

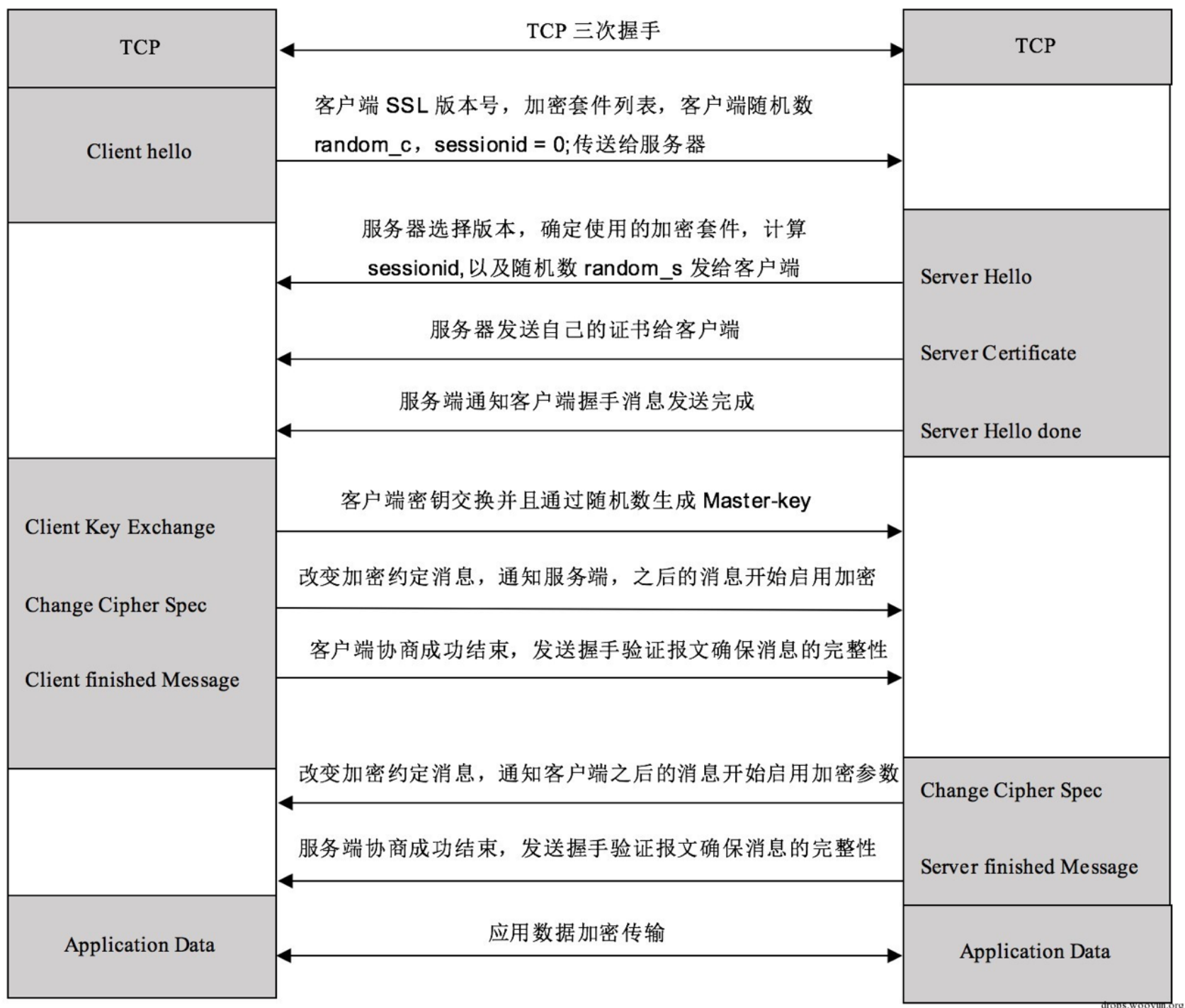
# 谈HTTPS中间人攻击与证书校验 (一)

## 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。

Realtek Ethernet Controller - Wireshark

文件(F) 编辑(E) 视图(V) 定位(G) 抓包(C) 分析(A) 统计(S) 电信(V) 工具(T) 帮助(H)

过滤: `ip.dst == 110.75.231.156 or ip.src == 110.75.231.156` 表达式... 清除 应用

No.	Time	Source	Destination	Protocol	Info
209	2.698470	192.168.2.141	110.75.231.156	TCP	51821 > https [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2 SACK_PERM=1
210	2.707880	110.75.231.156	192.168.2.141	TCP	https > 51821 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1440 SACK_PERM=1
211	2.707978	192.168.2.141	110.75.231.156	TCP	51821 > https [ACK] Seq=1 Ack=1 Win=64800 Len=0
212	2.708584	192.168.2.141	110.75.231.156	TLSv1.2	Client Hello
217	2.720169	110.75.231.156	192.168.2.141	TCP	https > 51821 [ACK] Seq=1 Ack=215 Win=15544 Len=0
218	2.721057	110.75.231.156	192.168.2.141	TLSv1.2	Server Hello
219	2.721058	110.75.231.156	192.168.2.141	TCP	[TCP segment of a reassembled PDU] 三次握手
220	2.721137	192.168.2.141	110.75.231.156	TCP	51821 > https [ACK] Seq=215 Ack=2881 Win=64800 Len=0
221	2.722633	110.75.231.156	192.168.2.141	TLSv1.2	Certificate, Server Hello Done
222	2.723675	192.168.2.141	110.75.231.156	TLSv1.2	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
254	2.738971	110.75.231.156	192.168.2.141	TLSv1.2	Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message
300	2.836096	192.168.2.141	110.75.231.156	TLSv1.2	Application Data
301	2.855623	110.75.231.156	192.168.2.141	TCP	[TCP segment of a reassembled PDU]
302	2.858832	110.75.231.156	192.168.2.141	TCP	[TCP segment of a reassembled PDU]
303	2.858883	192.168.2.141	110.75.231.156	TCP	51821 > https [ACK] Seq=1314 Ack=7389 Win=64800 Len=0
304	2.862979	110.75.231.156	192.168.2.141	TCP	[TCP segment of a reassembled PDU]
305	2.863754	110.75.231.156	192.168.2.141	TCP	[TCP segment of a reassembled PDU]
306	2.863816	192.168.2.141	110.75.231.156	TCP	51821 > https [ACK] Seq=1314 Ack=10269 Win=64800 Len=0

## 2.Client Hello

No.	Time	Source	Destination	Protocol	Info
1456	5.064443	110.75.231.156	192.168.2.141	TCP	https > 64018 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=14
1459	5.064613	192.168.2.141	110.75.231.156	TCP	64018 > https [ACK] Seq=1 Ack=1 Win=64800 Len=0
1464	5.070706	192.168.2.141	110.75.231.156	TLSv1.2	Client Hello
1468	5.078594	110.75.231.156	192.168.2.141	TCP	https > 64018 [ACK] Seq=1 Ack=518 Win=15544 Len=0

Frame 1464: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits)

Ethernet II, Src: f8:a9:63:ba:a5:62 (f8:a9:63:ba:a5:62), Dst: 88:25:93:07:88:f4 (88:25:93:07:88:f4)

Internet Protocol, Src: 192.168.2.141 (192.168.2.141), Dst: 110.75.231.156 (110.75.231.156)

Transmission Control Protocol, Src Port: 64018 (64018), Dst Port: https (443), Seq: 1, Ack: 1, Len: 517

Secure Socket Layer

- TLSv1.2 Record Layer: Handshake Protocol: Client Hello
  - Content Type: Handshake (22)
  - Version: TLS 1.0 (0x0301)
  - Length: 512
  - Handshake Protocol: Client Hello
    - Handshake Type: Client Hello (1)
    - Length: 508
    - Version: TLS 1.2 (0x0303)
    - Random
      - gmt\_unix\_time: Sep 10, 2024 21:19:00.000000000 中国标准时间
      - random\_bytes: 71fe4815d243411eeeca9a1b29f5615353287f1860668111b...
    - Session ID Length: 32
    - Session ID: 3a89b58b119aeef793eb9638b8fa9cce56d5044c739b65b...
    - Cipher Suites Length: 32
    - Cipher Suites (16 suites)
      - Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02b)
      - Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02f)
      - Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0x009e)
      - Cipher Suite: Unknown (0xcc14)
      - Cipher Suite: Unknown (0xcc13)
      - Cipher Suite: Unknown (0xcc15)
      - Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA (0xc00a)
      - Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0xc014)
      - Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0039)
      - Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA (0xc009)
      - Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0xc013)
      - Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x0033)
      - Cipher Suite: TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0x009c)

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

No.	Time	Source	Destination	Protocol	Info
212	2.708584	192.168.2.141	110.75.231.156	TLSv1.2	Client Hello
217	2.720169	110.75.231.156	192.168.2.141	TCP	https > 51821 [ACK] Seq=1 Ack=215 Win=15544 Len=0
218	2.721057	110.75.231.156	192.168.2.141	TLSv1.2	Server Hello
219	2.721058	110.75.231.156	192.168.2.141	TCP	[TCP segment of a reassembled PDU]
220	2.721137	192.168.2.141	110.75.231.156	TCP	51821 > https [ACK] Seq=215 Ack=2881 Win=64800 Len=0
221	2.722633	110.75.231.156	192.168.2.141	TLSv1.2	Certificate, Server Hello Done
222	2.722675	192.168.2.141	110.75.231.156	TLSv1.2	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
Frame 218: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits)					
Ethernet II, Src: 88:25:93:07:88:f4 (88:25:93:07:88:f4), Dst: f8:a9:63:ba:a5:62 (f8:a9:63:ba:a5:62)					
Internet Protocol, Src: 110.75.231.156 (110.75.231.156), Dst: 192.168.2.141 (192.168.2.141)					
Transmission Control Protocol, Src Port: https (443), Dst Port: 51821 (51821), Seq: 1, Ack: 215, Len: 1440					
Secure Socket Layer					
TLSv1.2 Record Layer: Handshake Protocol: Server Hello					
Content Type: Handshake (22)					
Version: TLS 1.2 (0x0303)					
Length: 68					
Handshake Protocol: Server Hello					
Handshake Type: Server Hello (2)					
Length: 64					
Version: TLS 1.2 (0x0303)					
Random					
gmt_unix_time: Mar 21, 2017 14:54:50.000000000 中国标准时间					
random_bytes: e807542764c0616ae056b1c918c5f082ef21a2fba46df197...					
Session ID Length: 0					
Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)					
Compression Method: null (0)					
Extensions Length: 24					
Extension: renegotiation_info					
Type: renegotiation_info (0xff01)					
Length: 1					
Data (1 byte)					
Extension: SessionTicket TLS					
Type: SessionTicket TLS (0x0023)					
Length: 0					
Data (0 bytes)					
Extension: Unknown 16					
Type: Unknown (0x0010)					
Length: 11					
Data (11 bytes)					

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



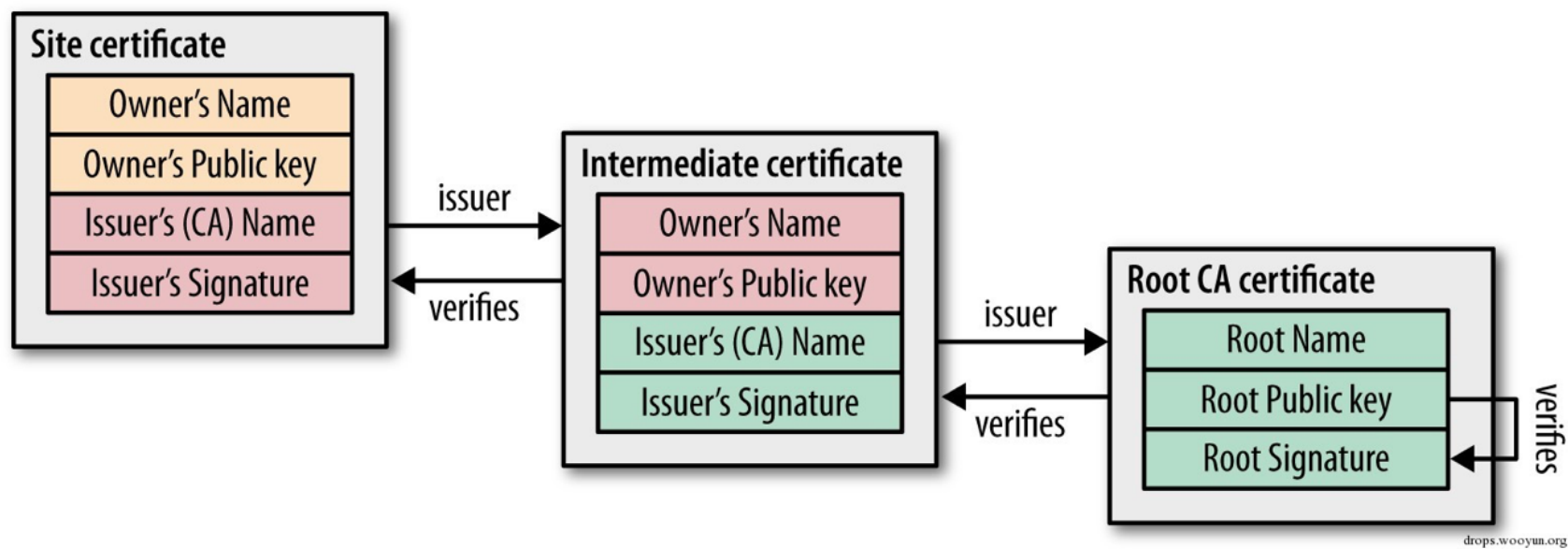
No.	Time	Source	Destination	Protocol	Info
219	2.721058	110.75.231.156	192.168.2.141	ICP	ICP segment or a reassembled PDU
220	2.721137	192.168.2.141	110.75.231.156	TCP	51821 > https [ACK] Seq=215 Ack=2881 Win=64800 Len=0
221	2.722633	110.75.231.156	192.168.2.141	TLSv1.2	Certificate, Server Hello Done
222	2.723675	192.168.2.141	110.75.231.156	TLSv1.2	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message

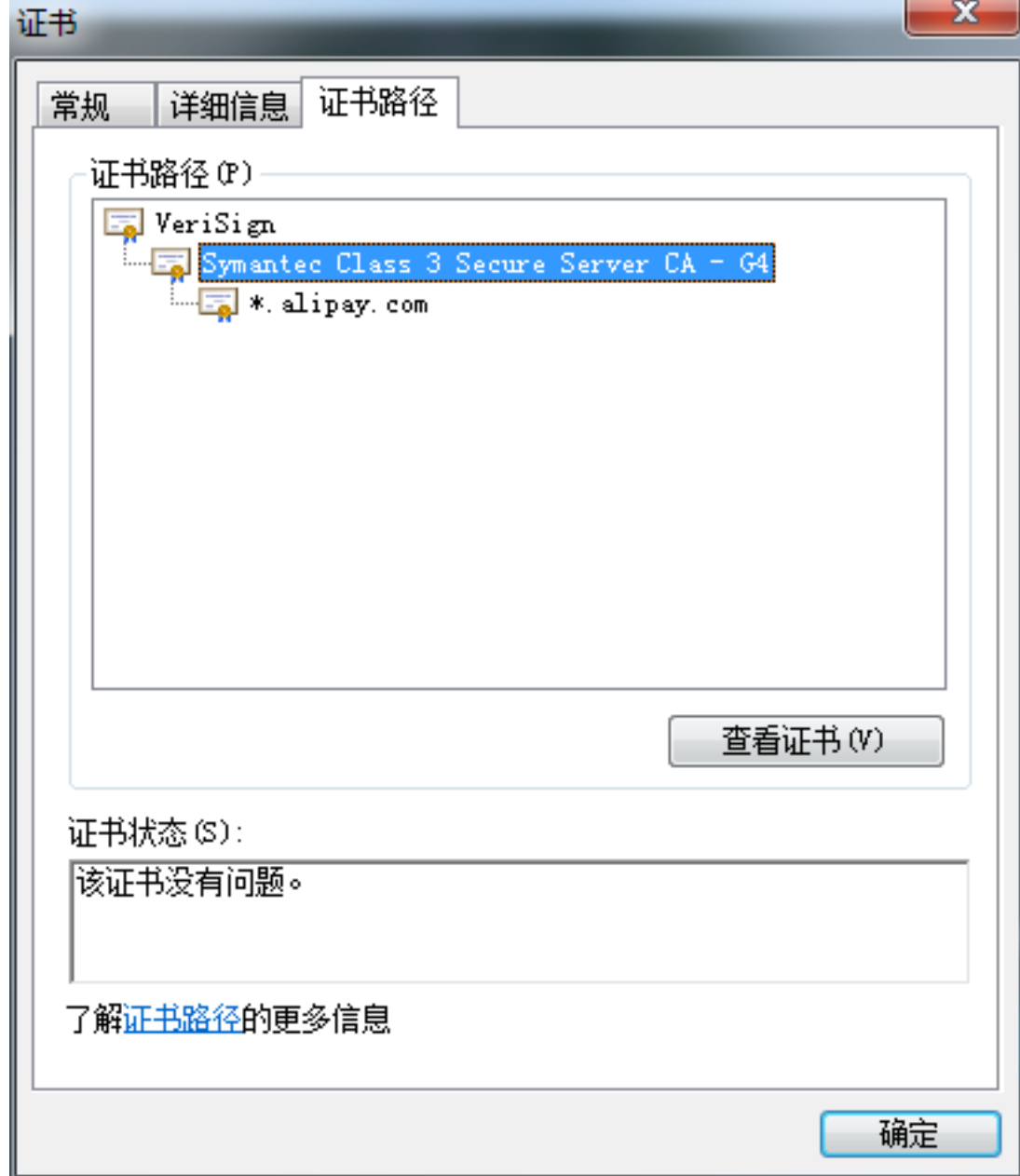
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 4139
Handshake Protocol: Certificate
Handshake Type: Certificate (11)
Length: 4135
Certificates Length: 4132
Certificates (4132 bytes)
Certificate Length: 1547
Certificate (id-at-commonName=*.alipay.com, id-at-organizationalUnitName=Operations Department, id-at-organizationName=Alipay.com Co., Ltd, id-at-localityName=HANGZHOU, id-at-stateOrProvinceName=ZHEJIANG, id-at-countryName=CN)
signedCertificate
version: v3 (2)
serialNumber: 0x78d8e2051576dd497a238e7843110e68
signature (sha256WithRSAEncryption)
issuer: rdnSequence (0)
validity
subject: rdnSequence (0)
subjectPublicKeyInfo
algorithm (rsaEncryption)
padding: 0
subjectPublicKey: 3082010a028201010086bef73dd1018d5568fba2a18cfbf1...
extensions: 9 items
algorithmIdentifier (sha256WithRSAEncryption)
padding: 0
encrypted: 6c0d24084e0cb4b6c70bb7335535282cce743d462fb349af...
Certificate Length: 1340
Certificate (id-at-commonName=Symantec Class 3 Secure Server CA - G4, id-at-organizationalUnitName=Symantec Trust Network, id-at-organizationName=Symantec Corporation, id-at-countryName=US)
Certificate Length: 1236
Certificate (id-at-commonName=VeriSign Class 3 Public Primary Certification, id-at-organizationalUnitName=(c) 2006 VeriSign, Inc. - For auth, id-at-organizationalUnitName=VeriSign Trust Network, id-at-organizationName=VeriSign, Inc.)
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 4
Handshake Protocol: Server Hello Done
Handshake Type: Server Hello Done (14)
Length: 0

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。

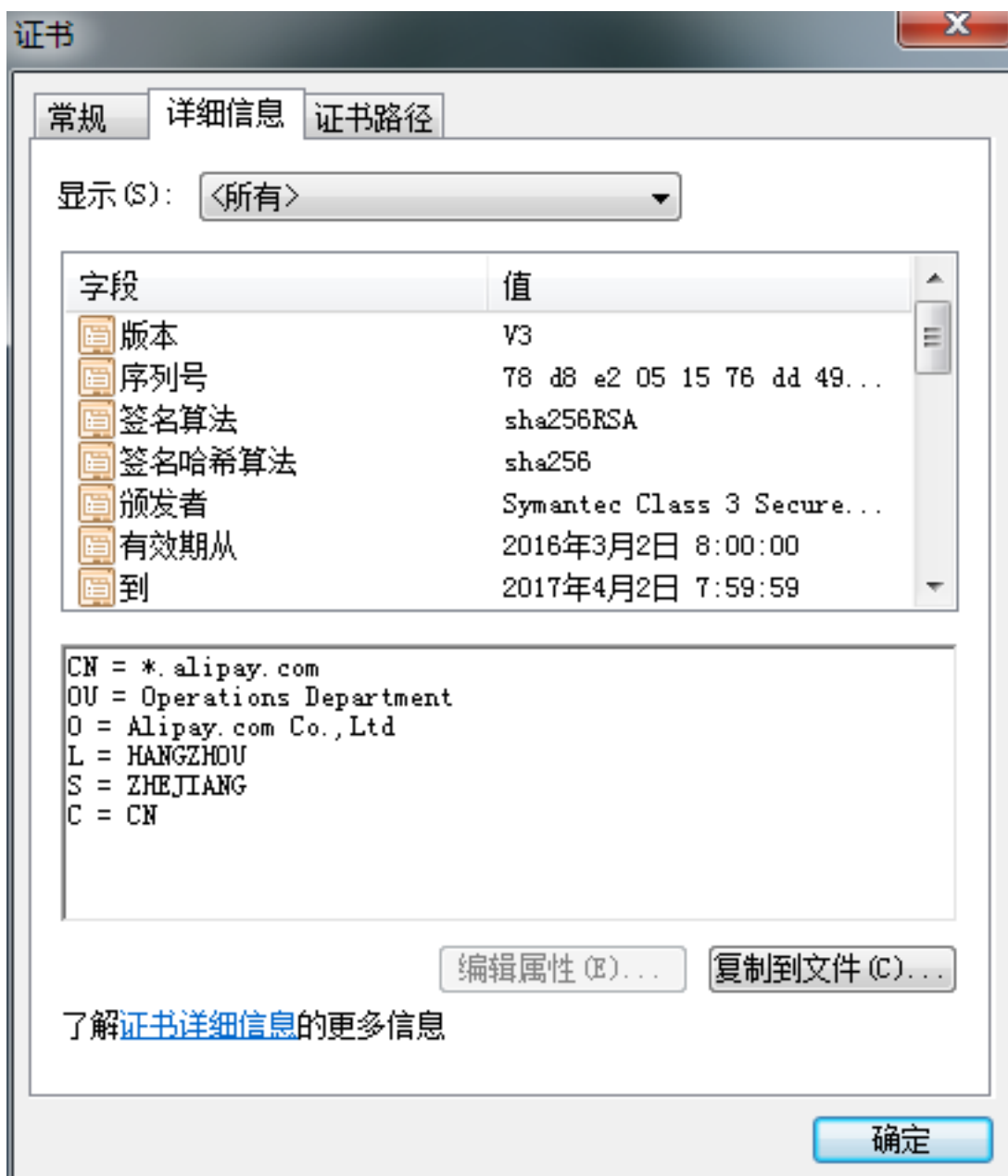
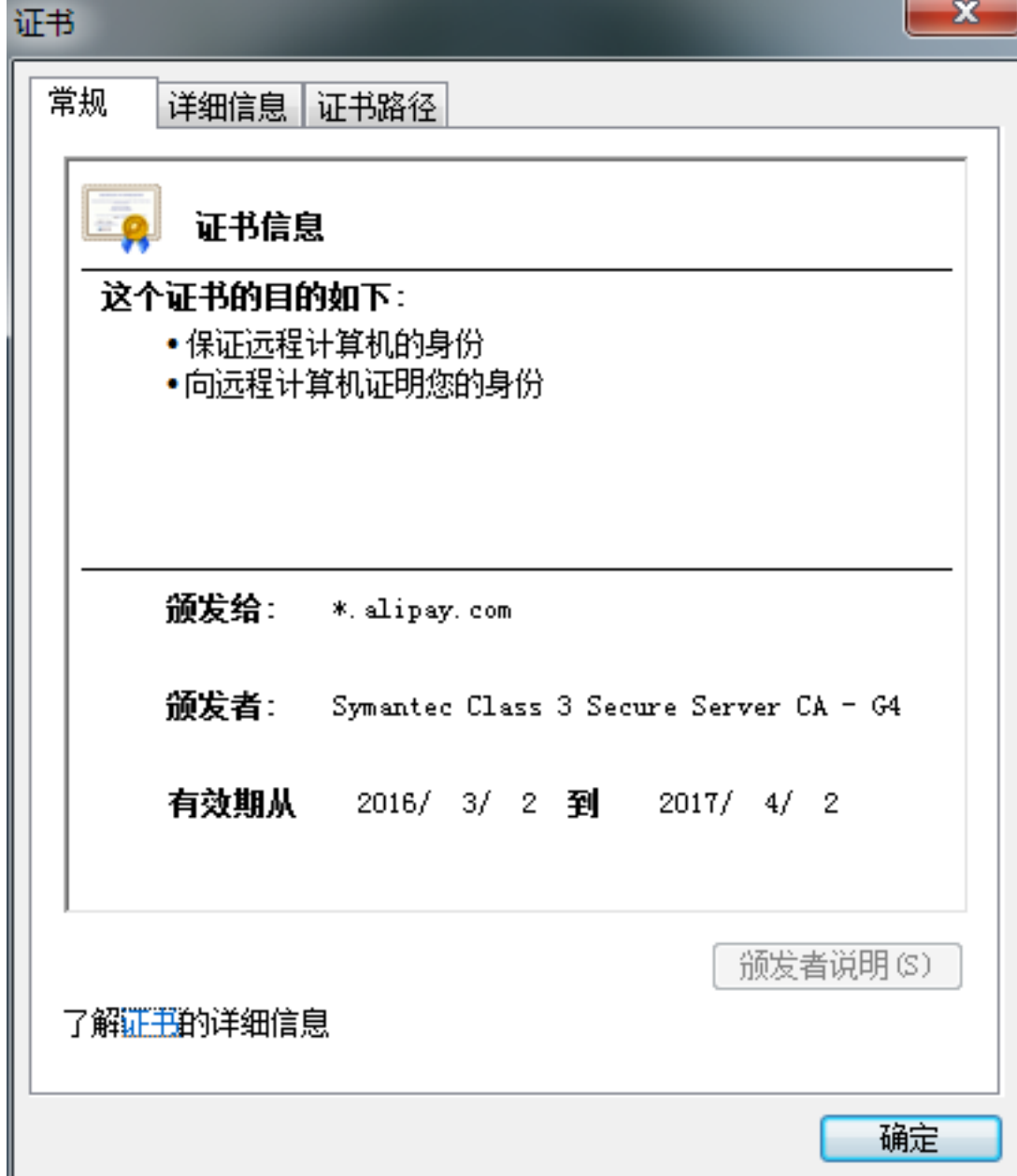
验证证书链的时候，用上一级的公钥对证书里的签名进行解密，还原对应的摘要值，再使用证书信息计算证书的摘要值，最后通过对比两个摘要值是否相等，如果不相等则认为该证书不可信，如果相等则认为该级证书链正确，以此类推对整个证书链进行校验。



二级机构的证书。



支付宝官网签名证书。



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。

No.	Time	Source	Destination	Protocol	Info
219	2.721058	110.75.231.156	192.168.2.141	ICP	[ICP segment of a reassembled PDU]
220	2.721137	192.168.2.141	110.75.231.156	TCP	51821 > https [ACK] Seq=215 Ack=2881 Win=64800 Len=0
221	2.722633	110.75.231.156	192.168.2.141	TLSv1.2	Certificate, <b>Server Hello Done</b>
222	2.723675	192.168.2.141	110.75.231.156	TLSv1.2	Client Key Exchange, Change Cipher Spec, Encrypted Handshake

Frame 221: 1400 bytes on wire (11200 bits), 1400 bytes captured (11200 bits)

Ethernet II, Src: 88:25:93:07:88:f4 (88:25:93:07:88:f4), Dst: f8:a9:63:ba:a5:62 (f8:a9:63:ba:a5:62)

Internet Protocol, Src: 110.75.231.156 (110.75.231.156), Dst: 192.168.2.141 (192.168.2.141)

Transmission Control Protocol, Src Port: https (443), Dst Port: 51821 (51821), Seq: 2881, Ack: 215, Len: 1346

[Reassembled TCP Segments (4153 bytes): #218(1367), #219(1440), #221(1346)]

Secure Socket Layer

TLSv1.2 Record Layer: Handshake Protocol: Certificate

TLSv1.2 Record Layer: Handshake Protocol: **Server Hello Done**

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 4

Handshake Protocol: **Server Hello Done**

Handshake Type: Server Hello Done (14)

Length: 0

## 6.ClientKeyExchange

No.	Time	Source	Destination	Protocol	Info
221	2.722633	110.75.231.156	192.168.2.141	TLSv1.2	Certificate, Server Hello Done
222	2.723675	192.168.2.141	110.75.231.156	TLSv1.2	<b>Client Key Exchange</b> , Change Cipher Spec, Encrypted Handshake Message
254	2.738971	110.75.231.156	192.168.2.141	TLSv1.2	Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message
300	2.836096	192.168.2.141	110.75.231.156	TLSv1.2	Application Data

Frame 222: 396 bytes on wire (3168 bits), 396 bytes captured (3168 bits)

Ethernet II, Src: f8:a9:63:ba:a5:62 (f8:a9:63:ba:a5:62), Dst: 88:25:93:07:88:f4 (88:25:93:07:88:f4)

Internet Protocol, Src: 192.168.2.141 (192.168.2.141), Dst: 110.75.231.156 (110.75.231.156)

Transmission Control Protocol, Src Port: 51821 (51821), Dst Port: https (443), Seq: 215, Ack: 4227, Len: 342

Secure Socket Layer

TLSv1.2 Record Layer: Handshake Protocol: **Client Key Exchange**

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 262

Handshake Protocol: Client Key Exchange

Handshake Type: Client Key Exchange (16)

Length: 258

TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec

TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message

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。

No.	Time	Source	Destination	Protocol	Info
1476	5.080292	192.168.2.141	110.75.231.156	TCP	64018 > https [ACK] Seq=518 Ack=4227 Win=64800 Len=0
1483	5.081730	192.168.2.141	110.75.231.156	TLSv1.2	Client Key Exchange, <b>Change Cipher Spec</b> , Encrypted Handshake Message
1530	5.096687	110.75.231.156	192.168.2.141	TLSv1.2	Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message
1592	5.247671	192.168.2.141	110.75.231.156	TLSv1.2	Application Data

Frame 1483: 396 bytes on wire (3168 bits), 396 bytes captured (3168 bits)

Ethernet II, Src: f8:a9:63:ba:a5:62 (f8:a9:63:ba:a5:62), Dst: 88:25:93:07:88:f4 (88:25:93:07:88:f4)

Internet Protocol, Src: 192.168.2.141 (192.168.2.141), Dst: 110.75.231.156 (110.75.231.156)

Transmission Control Protocol, Src Port: 64018 (64018), Dst Port: https (443), Seq: 518, Ack: 4227, Len: 342

Secure Socket Layer

- TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
- TLSv1.2 Record Layer: Change Cipher Spec Protocol: **Change Cipher Spec**
  - Content Type: Change Cipher Spec (20)
  - Version: TLS 1.2 (0x0303)
  - Length: 1
  - Change Cipher Spec Message
- TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message

## 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。

No.	Time	Source	Destination	Protocol	Info
1476	5.080292	192.168.2.141	110.75.231.156	TCP	64018 > https [ACK] Seq=518 Ack=4227 Win=64800 Len=0
1483	5.081730	192.168.2.141	110.75.231.156	TLSv1.2	Client Key Exchange, Change Cipher Spec, <b>Encrypted Handshake Message</b>
1530	5.096687	110.75.231.156	192.168.2.141	TLSv1.2	Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message
1592	5.247671	192.168.2.141	110.75.231.156	TLSv1.2	Application Data

Frame 1483: 396 bytes on wire (3168 bits), 396 bytes captured (3168 bits)

Ethernet II, Src: f8:a9:63:ba:a5:62 (f8:a9:63:ba:a5:62), Dst: 88:25:93:07:88:f4 (88:25:93:07:88:f4)

Internet Protocol, Src: 192.168.2.141 (192.168.2.141), Dst: 110.75.231.156 (110.75.231.156)

Transmission Control Protocol, Src Port: 64018 (64018), Dst Port: https (443), Seq: 518, Ack: 4227, Len: 342

Secure Socket Layer

- TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
- TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
- TLSv1.2 Record Layer: Handshake Protocol: **Encrypted Handshake Message**
  - Content Type: Handshake (22)
  - Version: TLS 1.2 (0x0303)
  - Length: 64
  - Handshake Protocol: Encrypted Handshake Message

## 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。

No.	Time	Source	Destination	Protocol	Info
1483	5.081730	192.168.2.141	110.75.231.156	TLSv1.2	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1530	5.096687	110.75.231.156	192.168.2.141	TLSv1.2	Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message
1592	5.247671	192.168.2.141	110.75.231.156	TLSv1.2	Application Data
1599	5.267030	110.75.231.156	192.168.2.141	TCP	[TCP segment of a reassembled PDU]

Frame 1530: 336 bytes on wire (2688 bits), 336 bytes captured (2688 bits)

Ethernet II, Src: 88:25:93:07:88:f4 (88:25:93:07:88:f4), Dst: f8:a9:63:ba:a5:62 (f8:a9:63:ba:a5:62)

Internet Protocol, Src: 110.75.231.156 (110.75.231.156), Dst: 192.168.2.141 (192.168.2.141)

Transmission Control Protocol, Src Port: https (443), Dst Port: 64018 (64018), Seq: 4227, Ack: 860, Len: 282

Secure Socket Layer

TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message

TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec

Content Type: Change Cipher Spec (20)

Version: TLS 1.2 (0x0303)

Length: 1

Change Cipher Spec Message

TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message

## 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。

No.	Time	Source	Destination	Protocol	Info
1483	5.081730	192.168.2.141	110.75.231.156	TLSv1.2	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1530	5.096687	110.75.231.156	192.168.2.141	TLSv1.2	Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message
1592	5.247671	192.168.2.141	110.75.231.156	TLSv1.2	Application Data
1599	5.267030	110.75.231.156	192.168.2.141	TCP	[TCP segment of a reassembled PDU]

Frame 1530: 336 bytes on wire (2688 bits), 336 bytes captured (2688 bits)

Ethernet II, Src: 88:25:93:07:88:f4 (88:25:93:07:88:f4), Dst: f8:a9:63:ba:a5:62 (f8:a9:63:ba:a5:62)

Internet Protocol, Src: 110.75.231.156 (110.75.231.156), Dst: 192.168.2.141 (192.168.2.141)

Transmission Control Protocol, Src Port: https (443), Dst Port: 64018 (64018), Seq: 4227, Ack: 860, Len: 282

Secure Socket Layer

TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message

TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec

TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 64

Handshake Protocol: Encrypted Handshake Message

## 11.Application Data

经过一大串的计算之后，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 Applocation 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。

No.	Time	Source	Destination	Protocol	Info
1483	5.081730	192.168.2.141	110.75.231.156	TLSv1.2	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1530	5.096687	110.75.231.156	192.168.2.141	TLSv1.2	Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message
1592	5.247671	192.168.2.141	110.75.231.156	TLSv1.2	Application Data
1599	5.267030	110.75.231.156	192.168.2.141	TCP	[TCP segment of a reassembled PDU]

Frame 1592: 1067 bytes on wire (8536 bits), 1067 bytes captured (8536 bits)

Ethernet II, Src: f8:a9:63:ba:a5:62 (f8:a9:63:ba:a5:62), Dst: 88:25:93:07:88:f4 (88:25:93:07:88:f4)

Internet Protocol, Src: 192.168.2.141 (192.168.2.141), Dst: 110.75.231.156 (110.75.231.156)

Transmission Control Protocol, Src Port: 64018 (64018), Dst Port: https (443), Seq: 860, Ack: 4509, Len: 1013

Secure Socket Layer

TLSv1.2 Record Layer: Application Data Protocol: http

Content Type: Application Data (23)

Version: TLS 1.2 (0x0303)

Length: 1008

Encrypted Application Data: d5b8ceca999e5d633dcd81618e4f2d33bbc21682056d2801...

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

