计算机网络实验十一

安全套接层（SSL）

信息学部 朱婉婷

主要内容

一、实验原理

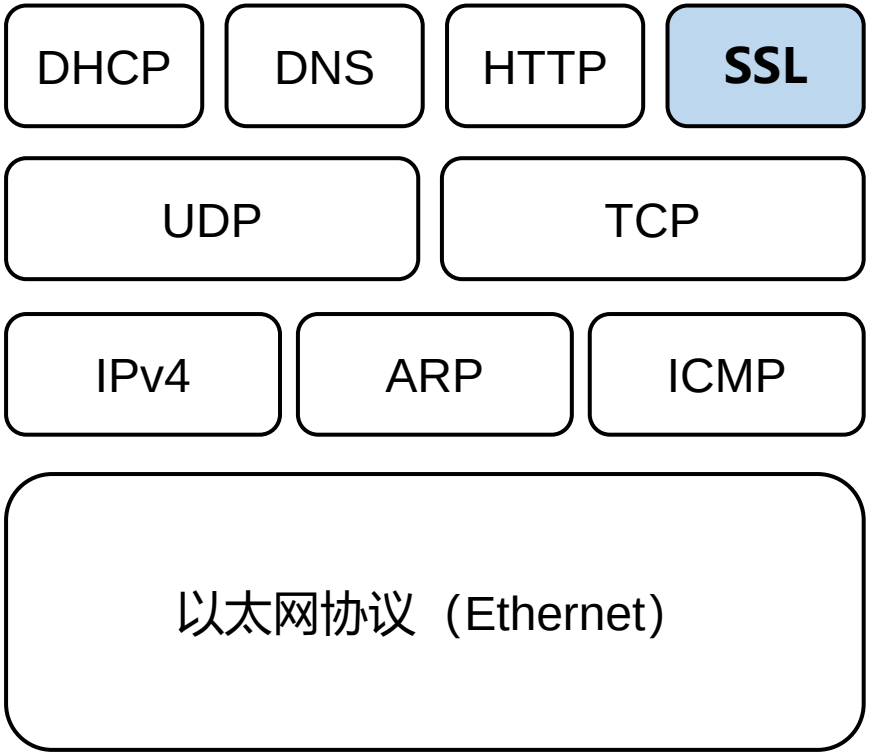
二、实验步骤

三、实验结果及分析

SSL简介

◆安全套接层 (Secure Socket Layer，SSL)

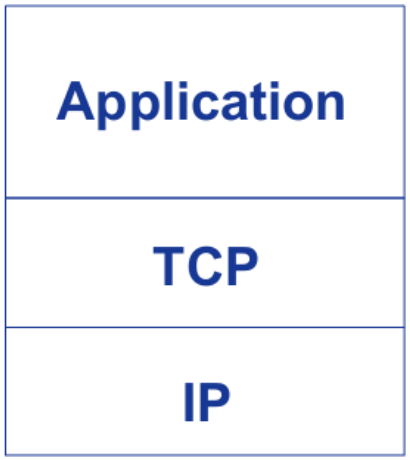
- 广泛部署的安全协议，可对互联网客户与服务器之间传送的数据进行加密和鉴别。
- 为网景（Netscape）所研发，自身发展到3.0，后来IETF进行了标准化，改名为传输层安全协议（Transport Layer Security，TLS）。可以说，TLS 1.0就是SSL 3.1版本。
- TLS/SSL在传输层与应用层之间对网络连接进行加密。



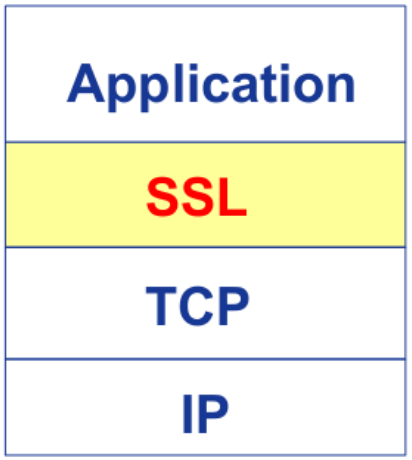
SSL简介

◆SSL的位置

- 在发送方，SSL 接收应用层的数据，对数据进行加密，然后把加了密的数据送往 TCP 套接字。
- 在接收方，SSL 从 TCP 套接字读取数据，解密后把数据交给应用层。



正常应用



采用SSL的应用

SSL简介

◆SSL协议栈，SSL不是一个单独的协议，而是两层协议。

- 底层是SSL记录协议层（SSL Record Protocol Layer）；
- 高层是SSL握手协议层（SSL HandShake Protocol Layer）。
  - SSL握手协议（SSL HandShake Protocol）
  - SSL更改密码规格协议（SSL Change Cipher Spec Protocol）
  - SSL警告协议（SSL Alert Protocol）
  - 应用数据协议（Application Data Protocol）

SSL简介

◆SSL 提供的三个主要功能

- SSL 服务器鉴别：允许用户证实服务器的身份。具有 SSL 功能的浏览器维持一个表，上面有一些可信赖的认证中心 CA (Certificate Authority)和它们的公钥。
- 加密的 SSL 会话：客户和服务器交互的所有数据都在发送方加密，在接收方解密。
- SSL 客户鉴别：允许服务器证实客户的身份。

◆SSL提供的三个特性

- 机密性：SSL协议使用密钥加密通信数据。
- 可靠性：服务器和客户都会被认证，客户的认证是可选的。
- 完整性：SSL协议会对传送的数据进行完整性检查。

SSL握手协议

- 本实验重点介绍SSL中的握手协议，握手协议是客户端和服务器用SSL连接通信时使用的第一个子协议。
- 该协议允许服务器和客户端相互验证，协商加密算法以及建立密钥，用来保护在SSL记录中发送的数据。协商结果是SSL记录协议的基础。
- 握手协议是在应用程序的数据传输之前使用的。

SSL握手协议

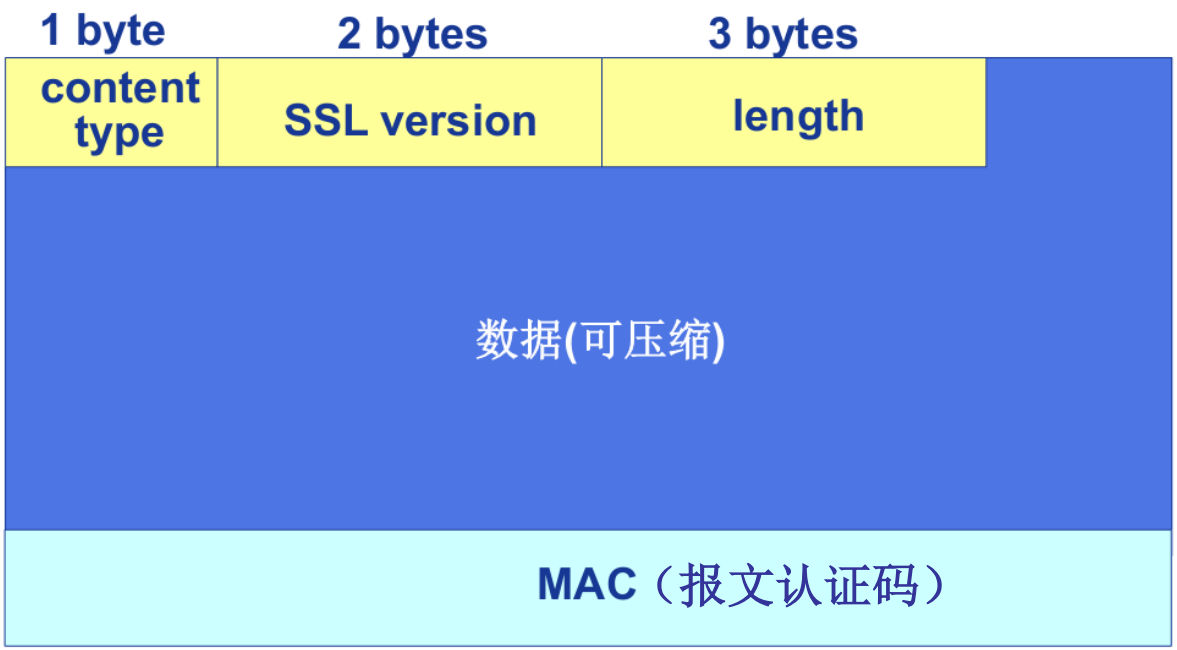
◆握手协议包含以下3个字段：

- Type：表示消息类型；
- Length：表示消息长度，字节数；
- Content：与消息相关的参数。

1 byte	3 bytes	
Type	Length	Content

SSL记录协议

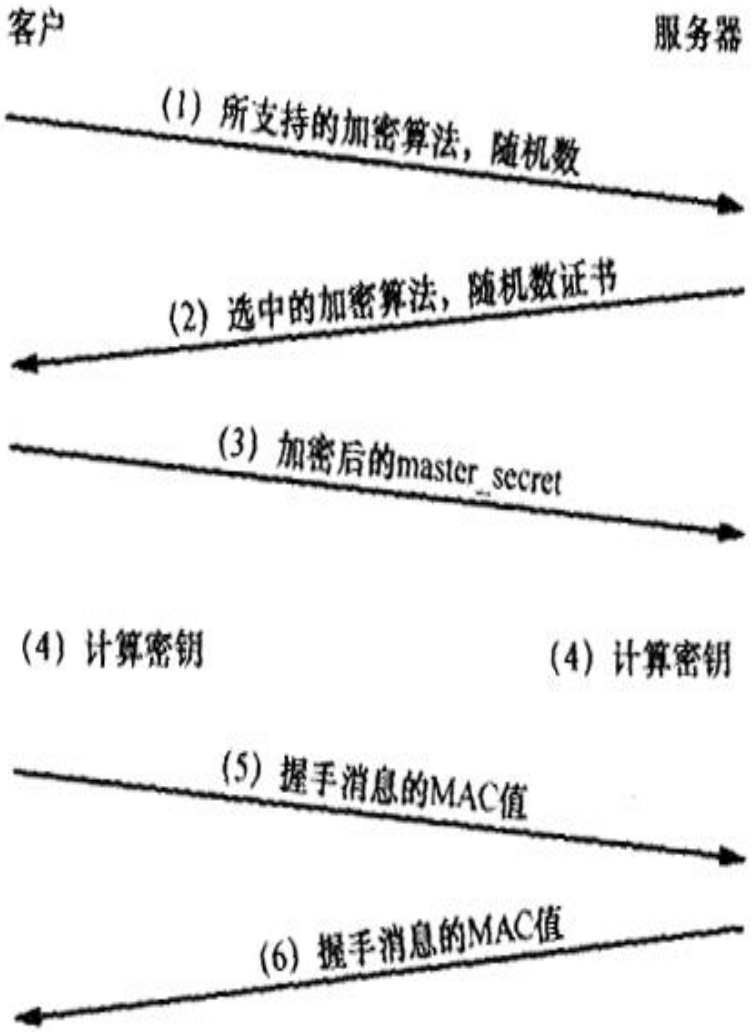
- 一个记录由两部分组成：记录头和数据。
- 所有数据（含SSL握手信息）都被封装在记录中。
- 数据和MAC（报文认证码）是加密的。



SSL握手过程

◆基本握手过程

- 1. 客户端将它所支持的算法列表和一个用作产生密钥的随机数发送给服务器；
- 2. 服务器从算法列表中选择一种加密算法，并将它和一份包含服务器公用密钥的证书发送给客户端；该证书还包含了用于认证目的的服务器标识，服务器同时还提供了一个用作产生密钥的随机数；
- 3. 客户端对服务器的证书进行验证，并抽取服务器的公用密钥；然后，再产生一个称作预主密钥（pre_master_secret）的随机密码串，并使用服务器的公用密钥对其进行加密，并将加密后的信息发送给服务器；

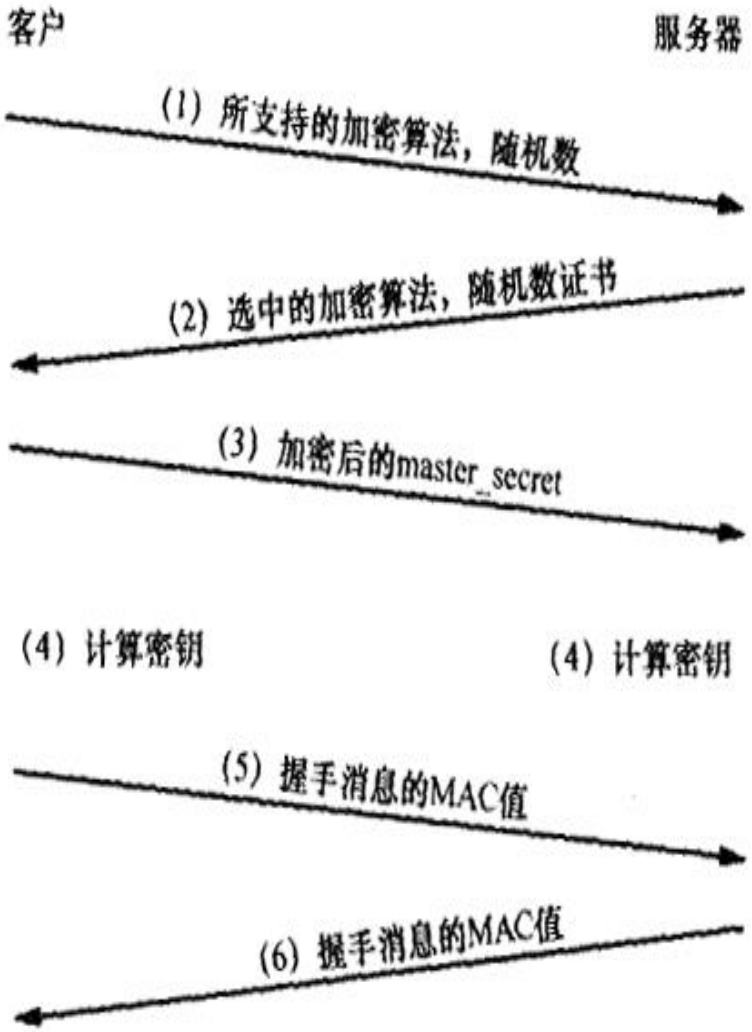


SSL握手过程

◆基本握手过程

- 4.客户端与服务器端根据pre_master_secret以及客户端与服务器的随机数值独立计算出加密和MAC密钥。
- 5.客户端将所有握手消息的报文认证码（MAC）值发送给服务器；
- 6.服务器将所有握手消息的报文认证码（MAC）值发送给客户端。

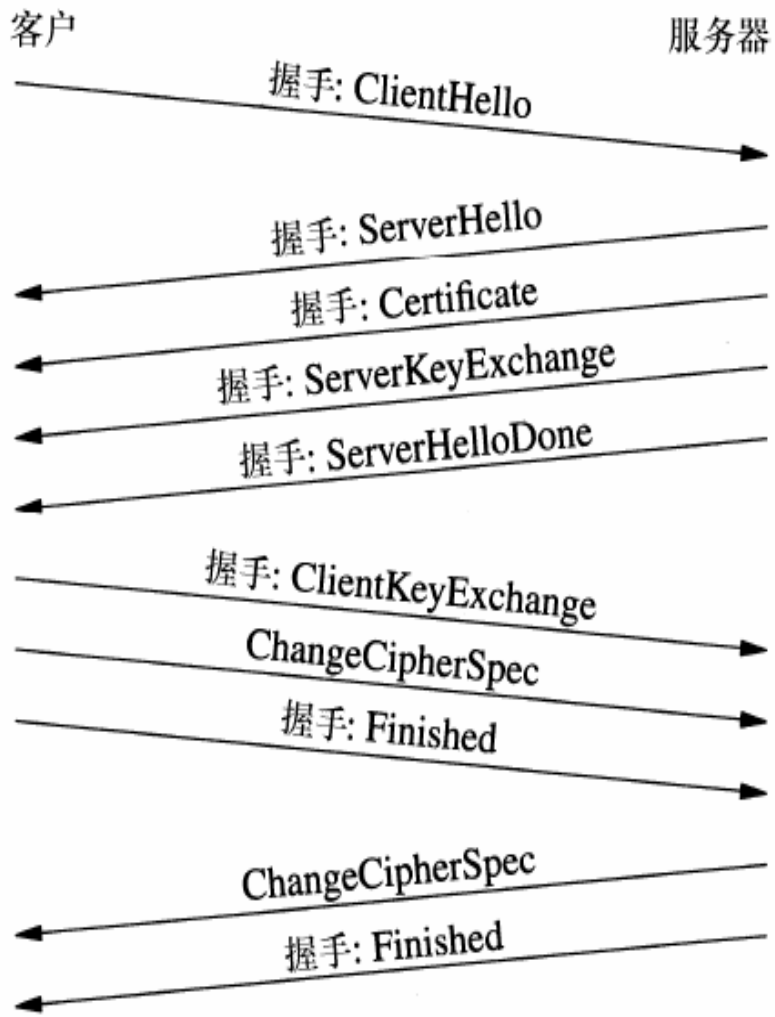
- 最后2步的意义：保护握手过程免遭篡改。最后2步传输的消息是加密的。



SSL握手过程

◆实际的SSL连接

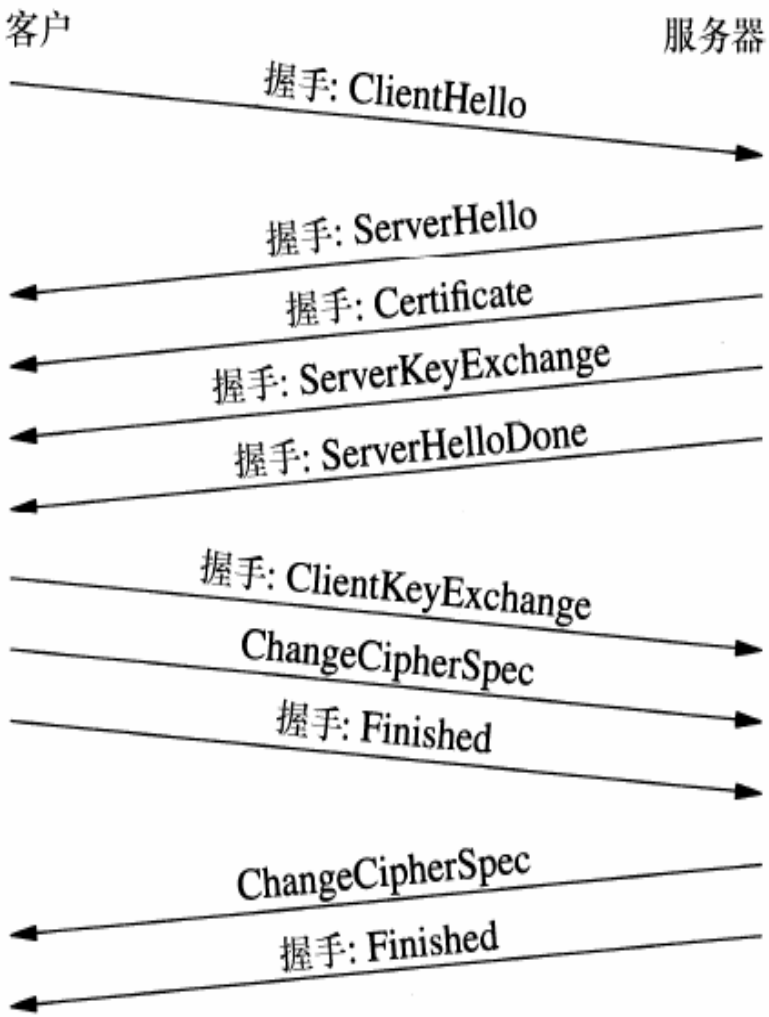
- SSL握手协议的握手过程由于版本、认证方式、加密算法以及密钥交换算法等选择的不同会有相应的步骤省略。
- 本实验主要介绍基于椭圆曲线（ECDHE）算法作为密钥交换算法的握手过程。



SSL握手过程

◆实际的SSL连接（Hello阶段）

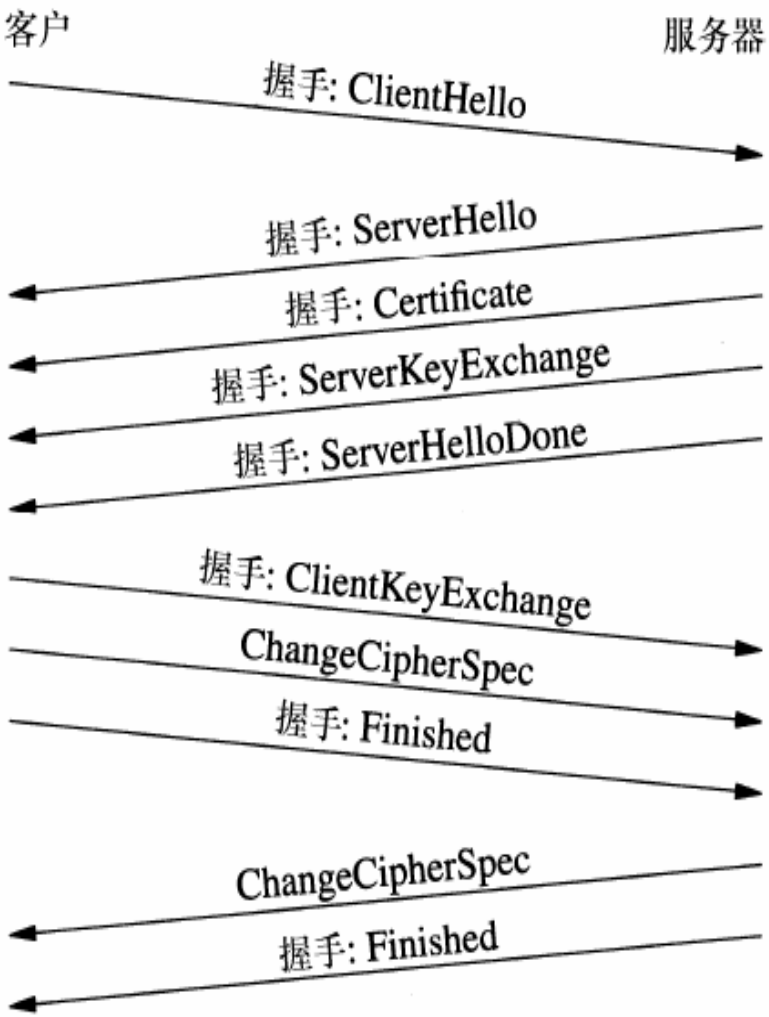
- **Client Hello**:客户端发起握手协商操作，它将发送一个ClientHello消息给服务器，消息中明确了其所支持的SSL/TLS版本、Cipher suite加密算法组合等，可以让服务器选择，并提供了一个客户端随机数，用于以后生成会话密钥使用。
- **Sever Hello**: 服务器将返回一个ServerHello消息，该消息包含了服务器选择的协议版本、加密算法，以及服务器随机数、会话ID等内容。其中，服务器选择的协议版本应小于等于客户端ClientHello中的协议版本。



SSL握手过程

◆实际的SSL连接（Key Agreement）

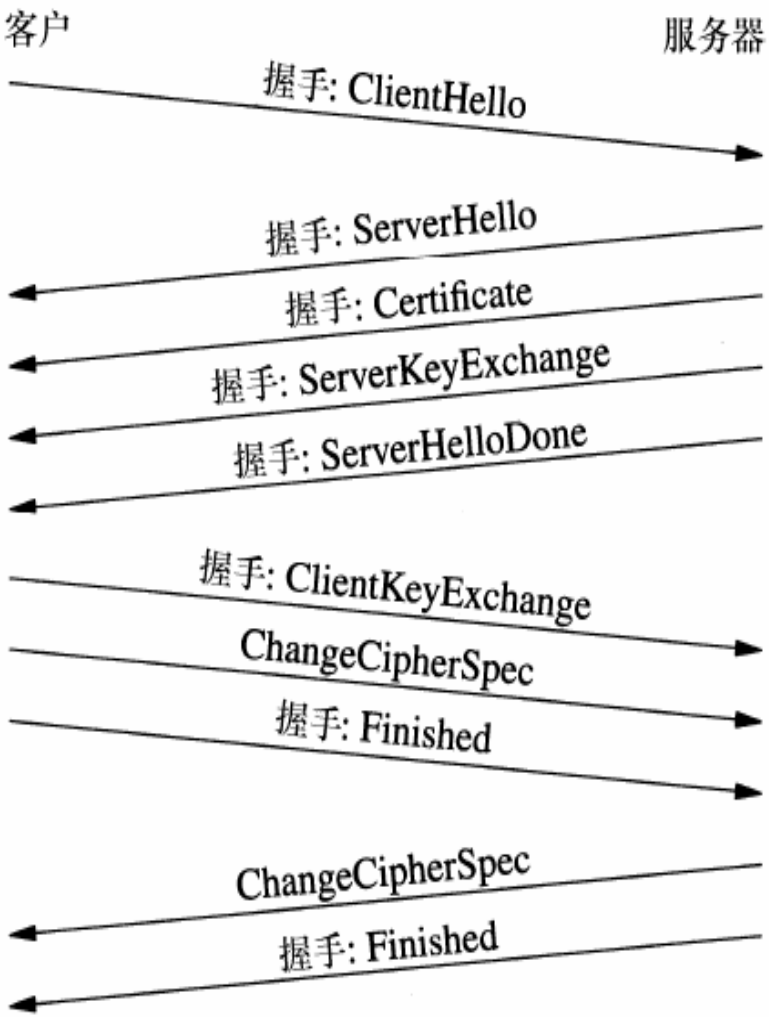
- **Certificate**:服务器发送，该消息包含了服务器的证书等信息，可通过证书链认证该证书的真实性。根据选择的加密算法组合的不同，服务器证书中的公钥也可被用于加密后面握手过程中生成的Premaster secret。
- **Server Key Exchange**:服务器发送，消息中包含了服务器这边的EC Diffie-Hellman算法相关参数。此消息一般只在选择使用相应加密算法组合时才会由服务器发出。
- **Server Hello Done**:服务器发送，告知客户端服务器这边握手相关的消息发送完毕。
- **Client Key Exchange**:客户端发送，消息中包含客户端这边的EC Diffie-Hellman算法相关参数，然后服务器和客户端都可根据接收到的对方参数和自身参数运算出Premaster secret，为生成会话密钥做准备。



SSL握手过程

◆实际的SSL连接（Finished）

- **Change Cipher Spec**:客户端发送，通知服务器以后客户端会以加密方式发送数据。
- **Finished**:客户端使用之前握手过程中获得的服务器随机数、客户端随机数、Premaster secret计算生成会话密钥，然后使用该会话密钥加密之前所有收发握手消息的Hash和MAC值，发送给服务器，服务器将相同的会话密钥（使用相同方法生成）解密此消息，校验其中的Hash和MAC值。
- **Change Cipher Spec**:服务器发送，通知客户端以后服务器会以加密方式发送数据。
- **Finished**:服务器使用会话密钥加密（生成方式与客户端相同，使用握手过程中获得的服务器随机数、客户端随机数、Premaster secret计算生成）之前所有收发握手消息的Hash和MAC值，发送给客户端去校验。



SSL握手过程

◆SSL握手消息类型及参数

消息类型	参数
hello_request	Null
client_hello	版本，随机数，会话ID，密码参数，压缩方法
server_hello	
certificate	X.509v3证书
server_key_exchange	参数，签名
certificate_request	类型，CA
server_done	Null
certificate_verify	签名
client_key_exchange	参数，签名
Finished	Hash值

思考题

思考题：同学们有兴趣可以网上搜索基于其他算法的SSL握手过程，阐述其基本原理，分析异同之处。

主要内容

一、实验原理

二、实验步骤

三、实验结果及分析

实验环境搭建

列出本次实验所使用的平台和相关软件，以下为例：

（打开cmd指令窗口，输入指令“ipconfig /all”查看）

1、主机：联想笔记本（Win10系统）；主机IP地址：192.168.1.106；子网掩码：255.255.255.0；主机网卡MAC地址：34-F6-4B-C0-90-40。

2、网络连接方式：无线连接；默认网关地址：192.168.1.1。

3、抓包工具：Wireshark （v3.6.2）。

实验具体步骤

- 由于HTTPS实际上应用了安全套接层（即SSL）作为HTTP应用层的子层，所以本次实验利用访问具有https://URL形式的网址来抓取SSL初次握手报文。
  - 例如：北工大官网“https://www.bjut.edu.cn”；
  - 或，在校园内进行校园网络连接时，进入的网关入口界面“https://lgn.bjut.edu.cn”。

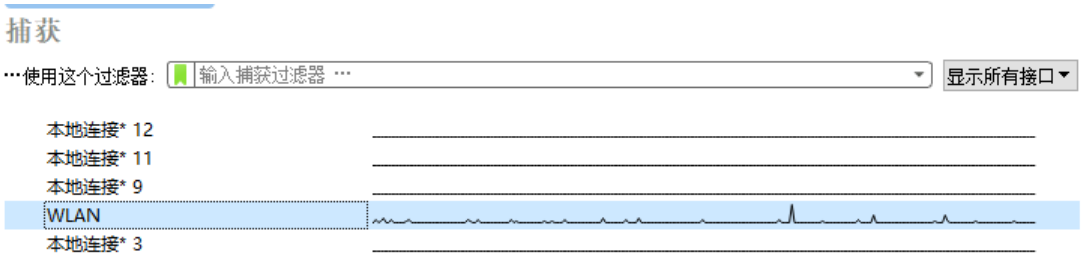
- TLS是SSL的标准化产物。SSL 3.0和TLS 1.0有轻微差别，但两种规范其实大致相同。所以本次实验通过追踪TLS流来观察SSL握手过程。

实验具体步骤

1、通过ping命令获取网站IP地址，例：北工大官网IP122.9.167.87。

```
正在 Ping bjut-edu-cn.cname.saaswaf.com [122.9.167.87] 具有 32 字节的数据:
来自 122.9.167.87 的回复: 字节=32 时间=42ms TTL=39
来自 122.9.167.87 的回复: 字节=32 时间=43ms TTL=39
```

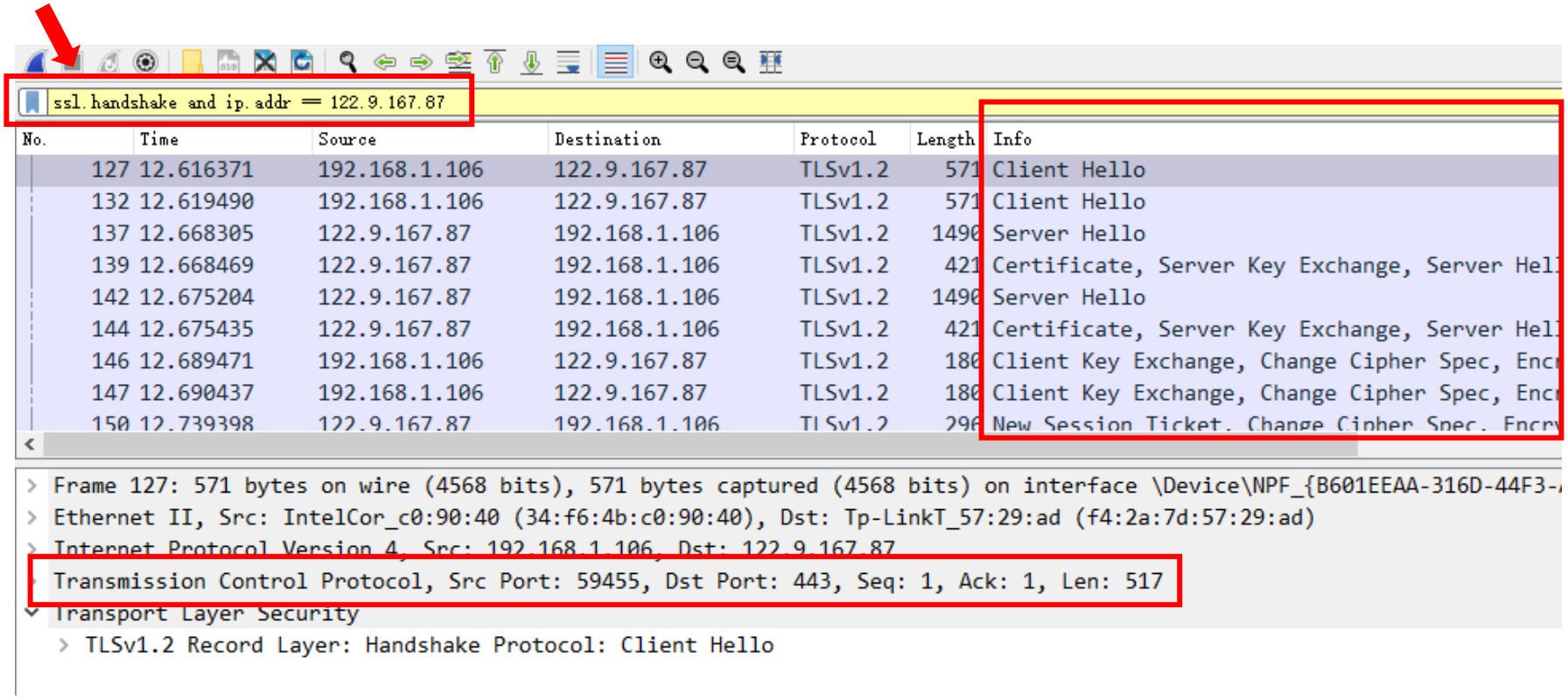
2、打开Wireshark软件，双击本次实验正在使用的网络接口，开始进行抓包。



3、然后打开浏览器，在网页地址栏中输入网址，例：对北京工业大学官网进行访问。注意网址形式“https://www.bjut.edu.cn”。

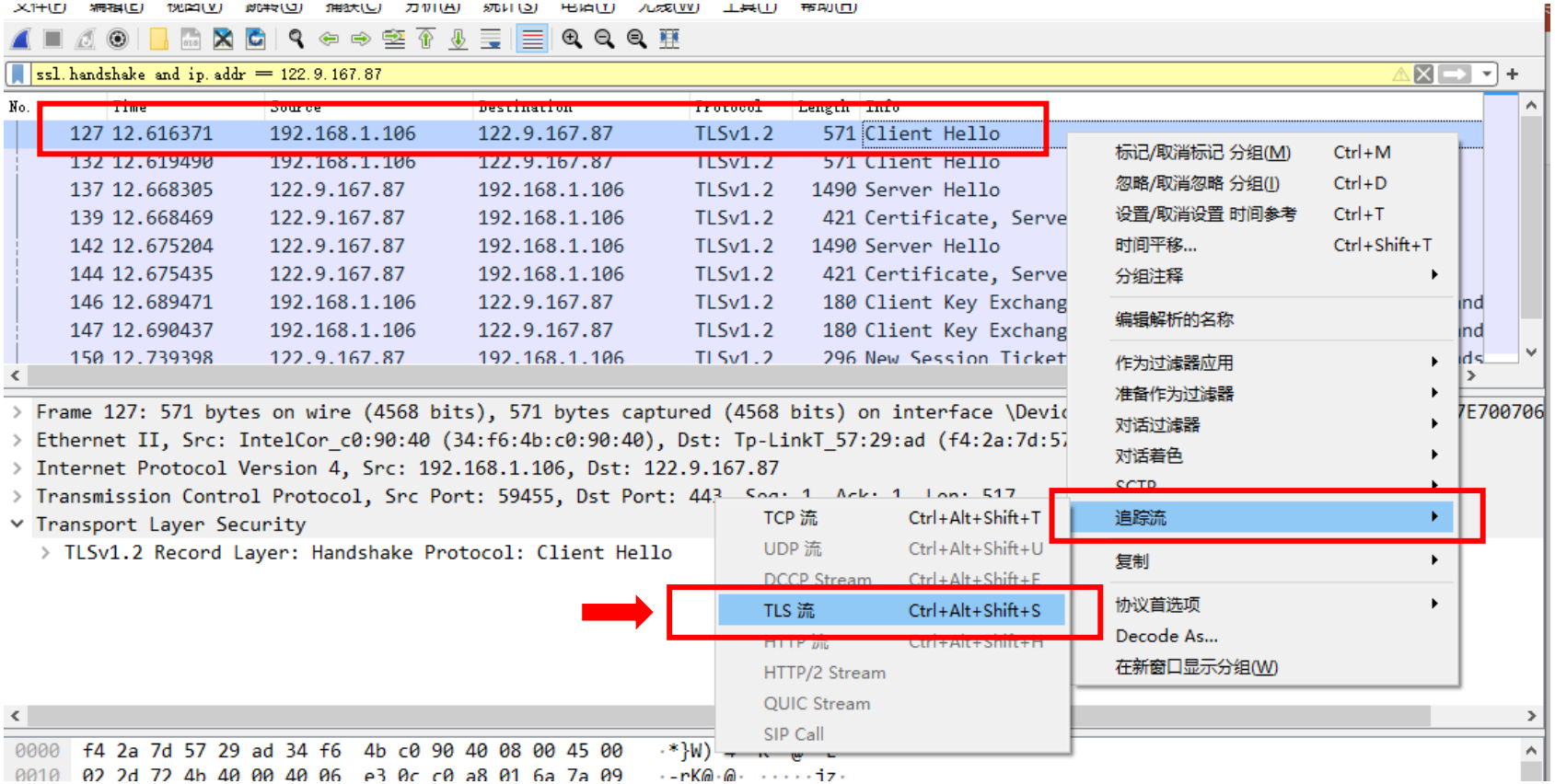
实验具体步骤

4、停止抓包，在过滤器里输入“ssl.handshake and ip.addr == 122.9.167.87”过滤条件。



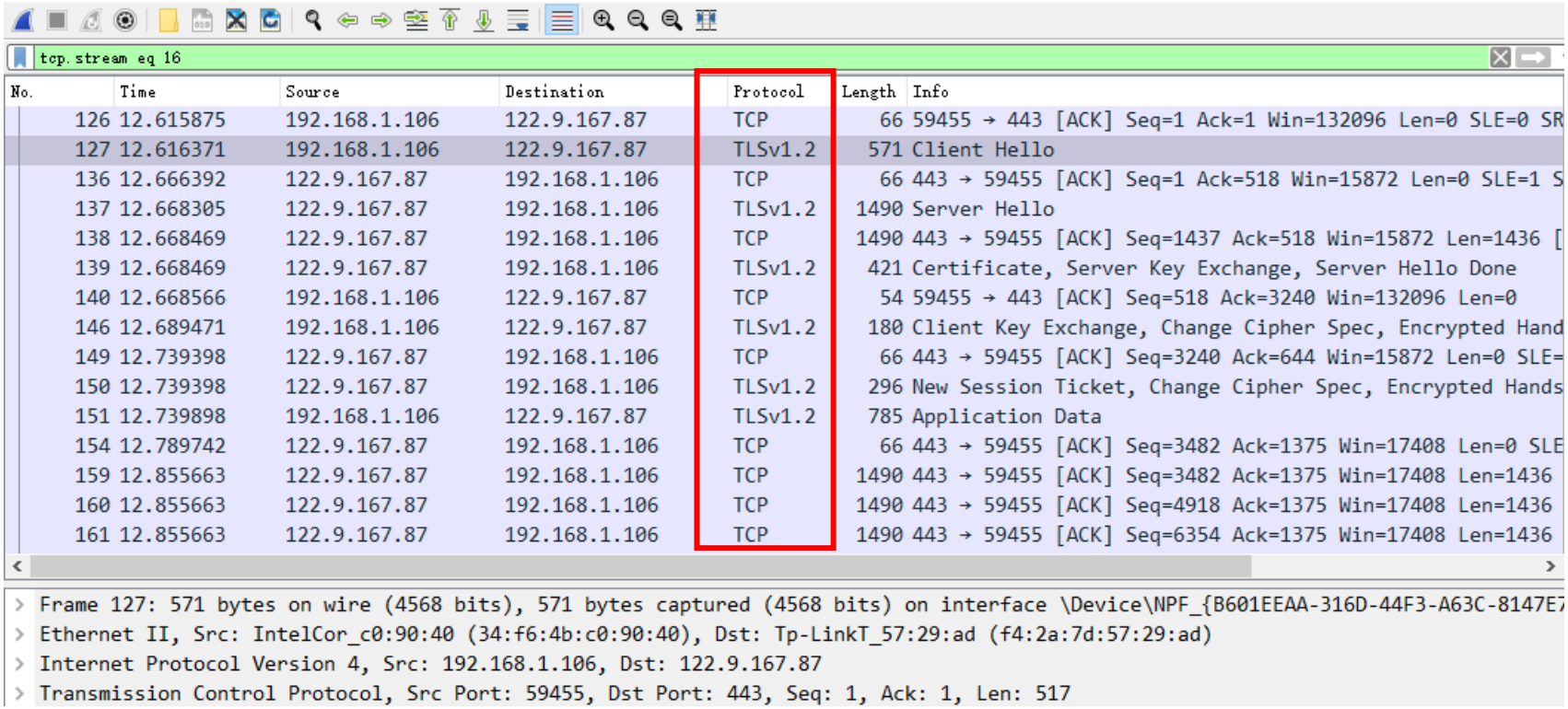
实验具体步骤

5、选中Info项为Client Hello的报文，右键点击，随后选取“追踪流->TLS流”进行TLS流跟踪，随后进行报文分析。



实验具体步骤

5、选中Info项为Client Hello的数据报，右键点击，随后选取“追踪流->TLS流”进行TLS流跟踪，随后进行报文分析。



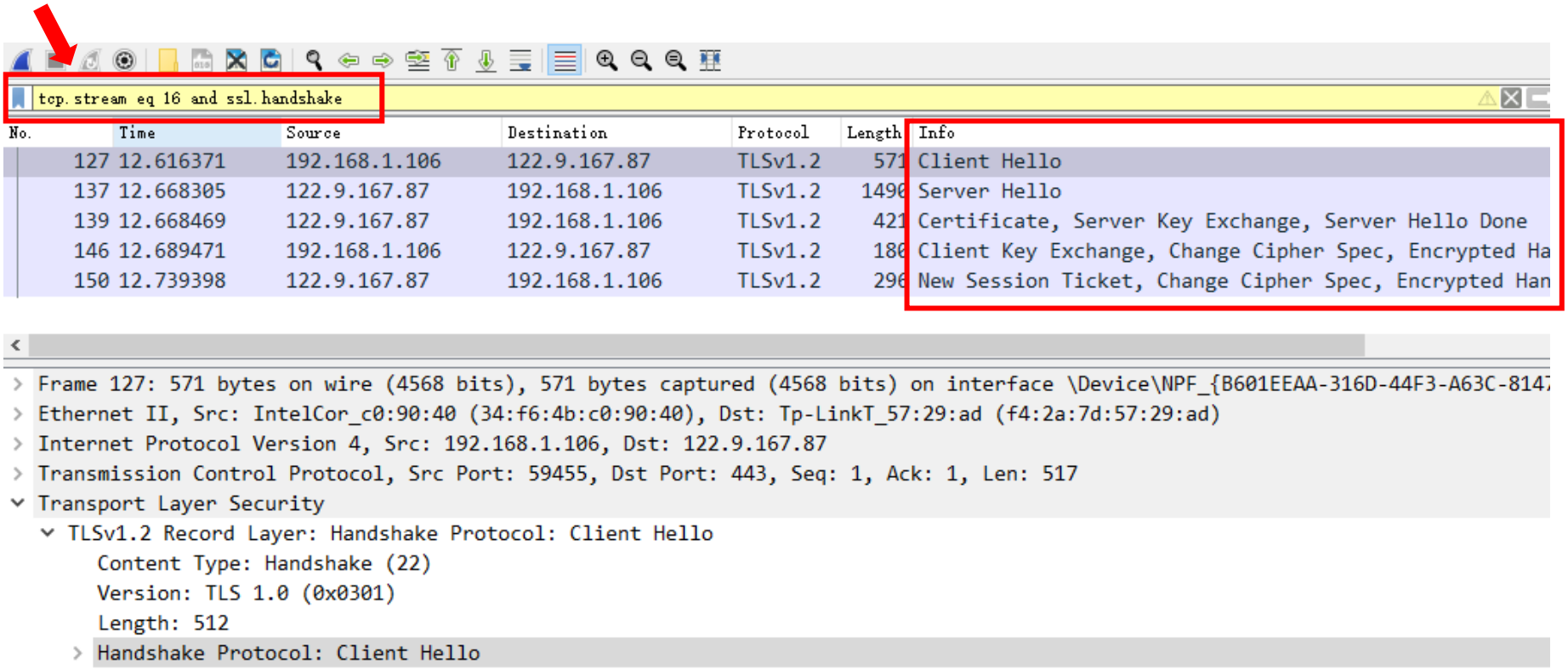
tcp.stream eq 16

No.	Time	Source	Destination	Protocol	Length	Info
126	12.615875	192.168.1.106	122.9.167.87	TCP	66	59455 → 443 [ACK] Seq=1 Ack=1 Win=132096 Len=0 SLE=0 SR
127	12.616371	192.168.1.106	122.9.167.87	TLSv1.2	571	Client Hello
136	12.666392	122.9.167.87	192.168.1.106	TCP	66	443 → 59455 [ACK] Seq=1 Ack=518 Win=15872 Len=0 SLE=1 S
137	12.668305	122.9.167.87	192.168.1.106	TLSv1.2	1490	Server Hello
138	12.668469	122.9.167.87	192.168.1.106	TCP	1490	443 → 59455 [ACK] Seq=1437 Ack=518 Win=15872 Len=1436 [
139	12.668469	122.9.167.87	192.168.1.106	TLSv1.2	421	Certificate, Server Key Exchange, Server Hello Done
140	12.668566	192.168.1.106	122.9.167.87	TCP	54	59455 → 443 [ACK] Seq=518 Ack=3240 Win=132096 Len=0
146	12.689471	192.168.1.106	122.9.167.87	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Hand
149	12.739398	122.9.167.87	192.168.1.106	TCP	66	443 → 59455 [ACK] Seq=3240 Ack=644 Win=15872 Len=0 SLE=
150	12.739398	122.9.167.87	192.168.1.106	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypted Hands
151	12.739898	192.168.1.106	122.9.167.87	TLSv1.2	785	Application Data
154	12.789742	122.9.167.87	192.168.1.106	TCP	66	443 → 59455 [ACK] Seq=3482 Ack=1375 Win=17408 Len=0 SLE
159	12.855663	122.9.167.87	192.168.1.106	TCP	1490	443 → 59455 [ACK] Seq=3482 Ack=1375 Win=17408 Len=1436
160	12.855663	122.9.167.87	192.168.1.106	TCP	1490	443 → 59455 [ACK] Seq=4918 Ack=1375 Win=17408 Len=1436
161	12.855663	122.9.167.87	192.168.1.106	TCP	1490	443 → 59455 [ACK] Seq=6354 Ack=1375 Win=17408 Len=1436

```
> Frame 127: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface \Device\NPF_{B601EEAA-316D-44F3-A63C-8147E7
> Ethernet II, Src: IntelCor_c0:90:40 (34:f6:4b:c0:90:40), Dst: Tp-LinkT_57:29:ad (f4:2a:7d:57:29:ad)
> Internet Protocol Version 4, Src: 192.168.1.106, Dst: 122.9.167.87
> Transmission Control Protocol, Src Port: 59455, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
```

实验具体步骤

6、在过滤器里现有过滤条件的基础上增加“…… and ssl.handshake”过滤条件，随后进行报文分析。



主要内容

一、实验原理

二、实验步骤

三、实验结果及分析

Client Hello报文

实验结果：

No.	Time	Source	Destination	Protocol	Length	Info
127	12.616371	192.168.1.106	122.9.167.87	TLSv1.2	571	Client Hello
137	12.668305	122.9.167.87	192.168.1.106	TLSv1.2	1490	Server Hello
139	12.668469	122.9.167.87	192.168.1.106	TLSv1.2	421	Certificate, Server Key Exchange, Server Hello Done
146	12.689471	192.168.1.106	122.9.167.87	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Hand
150	12.739398	122.9.167.87	192.168.1.106	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypted Hands

```
Transport Layer Security
  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: abc8ca84d29a33c58642d12dbb1bbb2345e3e0dad6f98d14f338877d83[redacted]
      Session ID Length: 32
      Session ID: 84f55b9a6807cb0320a0aed500ab3d0b5944a56080f15fca797887d7e97106f4
      Cipher Suites Length: 32
      Cipher Suites (16 suites)
      Compression Methods Length: 1
      Compression Methods (1 method)
      Extensions Length: 403
      Extension: Reserved (GREASE) (len=0)
      Extension: server_name (len=20)
      Extension: extended master secret (len=0)
```

记录头：内容类型、版本、长度

握手类型、长度、版本

随机数，用于生成会话密钥

会话ID

密码套件，支持的加密算法

支持的压缩方法

扩展

Server Hello报文

实验结果：

No.	Time	Source	Destination	Protocol	Length	Info
127	12.616371	192.168.1.106	122.9.167.87	TLSv1.2	571	Client Hello
137	12.668305	122.9.167.87	192.168.1.106	TLSv1.2	1490	Server Hello
139	12.668469	122.9.167.87	192.168.1.106	TLSv1.2	421	Certificate, Server Key Exchange, Server Hello Done
146	12.689471	192.168.1.106	122.9.167.87	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Hand
150	12.739398	122.9.167.87	192.168.1.106	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypted Hands

```
> Transmission Control Protocol, Src Port: 443, Dst Port: 59455, Seq: 1, Ack: 518, Len: 1436
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 65
    v Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 61
        Version: TLS 1.2 (0x0303)
      > Random: ba48b3b3d06bdc94e3dcfd6e0b0dc1fa381584670e39d16dd96f058b5ac1
        Session ID Length: 0
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
        Compression Method: null (0)
        Extensions Length: 21
      > Extension: server_name (len=0)
      > Extension: renegotiation_info (len=1)
      > Extension: ec_point_formats (len=4)
      > Extension: session_ticket (len=0)
```

记录头：内容类型、版本、长度

握手类型、长度、版本

随机数，用于生成会话密钥

会话ID长度

服务器选择的加密算法组合

服务器选择的压缩方法

扩展

密钥交换算法：ECDHE_RSA

加密算法：AES_256_GCM

散列算法：SHA384

Certificate报文

实验结果：

No.	Time	Source	Destination	Protocol	Length	Info
127	12.616371	192.168.1.106	122.9.167.87	TLSv1.2	571	Client Hello
137	12.668305	122.9.167.87	192.168.1.106	TLSv1.2	1490	Server Hello
139	12.668469	122.9.167.87	192.168.1.106	TLSv1.2	421	Certificate, Server Key Exchange, Server Hello Done
146	12.689471	192.168.1.106	122.9.167.87	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Hand
150	12.739398	122.9.167.87	192.168.1.106	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypted Hands

```
> Transmission Control Protocol, Src Port: 443, Dst Port: 59455, Seq: 2873, Ack: 518, Len: 367
> [3 Reassembled TCP Segments (2822 bytes): #137(1366), #138(1436), #139(20)]
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 2817
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 2813
        Certificates Length: 2810
      v Certificates (2810 bytes)
          Certificate Length: 1637
        > Certificate: 308206613082054 9a00302010202100aba3a957fc4675e3ee35239074f4a0d300d06092a… (id-at-commonName=*.bjut.edu.cn,
          Certificate Length: 1167
        > Certificate: 3082048b30820373a00302010202100546fe1823f7e1941da39fce14c46173300d06092a… (id-at-commonName=GeoTrust RSA C
```

证书，携带服务器的公钥信息和到根CA的整个证书链信息，可用于客户端验证服务器端的身份，和对预主密钥（premaster secret）进行加密。

Server Key Exchange报文

实验结果：

No.	Time	Source	Destination	Protocol	Length	Info
127	12.616371	192.168.1.106	122.9.167.87	TLSv1.2	571	Client Hello
137	12.668305	122.9.167.87	192.168.1.106	TLSv1.2	1490	Server Hello
139	12.668469	122.9.167.87	192.168.1.106	TLSv1.2	421	Certificate, Server Key Exchange, Server Hello Done
146	12.689471	192.168.1.106	122.9.167.87	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Hand
150	12.739398	122.9.167.87	192.168.1.106	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypted Hands

```
        Certificate Length: 1167
      > Certificate: 3082048b30820373a0030201020210054 6fe1823f7e1941da39fce14c46173300d06092a… (id-at-commonName=GeoTrust RSA (
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 333
    Handshake Protocol: Server Key Exchange
      Handshake Type: Server Key Exchange (12)
      Length: 329
      EC Diffie-Hellman Server Params
        Curve Type: named_curve (0x03)
        Named Curve: secp256r1 (0x0017)
        Pubkey Length: 65
        Pubkey: 0433c7219aa65cc935683ac248860b3728217c08f3dd0f15354a2ac6951e57114ce0cf77…
      > Signature Algorithm: rsa_pkcs1_sha512 (0x0601)
        Signature Length: 256
        Signature: 430e0d64ca40e5678d0d0b31bd4bc76f97769acfea423d345108ab0c2044d38cafb27537…
  > TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
```

服务器这边ECDHE算法的相关参数。

Server Hello Done报文

实验结果：

No.	Time	Source	Destination	Protocol	Length	Info
127	12.616371	192.168.1.106	122.9.167.87	TLSv1.2	571	Client Hello
137	12.668305	122.9.167.87	192.168.1.106	TLSv1.2	1490	Server Hello
139	12.668469	122.9.167.87	192.168.1.106	TLSv1.2	421	Certificate, Server Key Exchange, Server Hello Done
146	12.689471	192.168.1.106	122.9.167.87	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Ha
150	12.739398	122.9.167.87	192.168.1.106	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypted Han

```
> Transmission Control Protocol, Src Port: 443, Dst Port: 59455, Seq: 2873, Ack: 518, Len: 367
> [3 Reassembled TCP Segments (2822 bytes): #137(1366), #138(1436), #139(20)]
v Transport Layer Security
  > TLSv1.2 Record Layer: Handshake Protocol: Certificate
v Transport Layer Security
  > TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
  v TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 4
    v Handshake Protocol: Server Hello Done
        Handshake Type: Server Hello Done (14)
        Length: 0
```

服务器通知客户端握手相关的消息发送完毕。

Client Key Exchange报文

实验结果：

No.	Time	Source	Destination	Protocol	Length	Info
127	12.616371	192.168.1.106	122.9.167.87	TLSv1.2	571	Client Hello
137	12.668305	122.9.167.87	192.168.1.106	TLSv1.2	1490	Server Hello
139	12.668469	122.9.167.87	192.168.1.106	TLSv1.2	421	Certificate, Server Key Exchange, Server Hello Done
146	12.689471	192.168.1.106	122.9.167.87	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handsha
150	12.739398	122.9.167.87	192.168.1.106	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypted Handshak

```
> Internet Protocol Version 4, Src: 192.168.1.106, Dst: 122.9.167.87
> Transmission Control Protocol, Src Port: 59455, Dst Port: 443, Seq: 518, Ack: 3240, Len: 126
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 70
    v Handshake Protocol: Client Key Exchange
        Handshake Type: Client Key Exchange (16)
        Length: 66
      v EC Diffie-Hellman Client Params
          Pubkey Length: 65
          Pubkey: 04a45768ed85f7c2c7554ab5aa8e0553b91d5280f75227cd83d33c622fe5fc3e470243eb…
  > TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
  > TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
```

客户端这边ECDHE算法的相关参数。

Change Cipher Spec报文

实验结果：

No.	Time	Source	Destination	Protocol	Length	Info
127	12.616371	192.168.1.106	122.9.167.87	TLSv1.2	571	Client Hello
137	12.668305	122.9.167.87	192.168.1.106	TLSv1.2	1490	Server Hello
139	12.668469	122.9.167.87	192.168.1.106	TLSv1.2	421	Certificate, Server Key Exchange, Server Hello Done
146	12.689471	192.168.1.106	122.9.167.87	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake
150	12.739398	122.9.167.87	192.168.1.106	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypted Handshake

```
> Frame 146: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface \Device\NPF_{B601EEAA-316D-44F3-A63C-8147E700706
> Ethernet II, Src: IntelCor_c0:90:40 (34:f6:4b:c0:90:40), Dst: Tp-LinkT_57:29:ad (f4:2a:7d:57:29:ad)
> Internet Protocol Version 4, Src: 192.168.1.106, Dst: 122.9.167.87
> Transmission Control Protocol, Src Port: 59455, Dst Port: 443, Seq: 518, Ack: 3240, Len: 126
v Transport Layer Security
  > TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
  v 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
```

更改密码规格协议报文，客户端通知服务器后续报文将采用加密方式发送数据，内容只有1个字节。

Finished报文（已被加密）

实验结果：

No.	Time	Source	Destination	Protocol	Length	Info
127	12.616371	192.168.1.106	122.9.167.87	TLSv1.2	571	Client Hello
137	12.668305	122.9.167.87	192.168.1.106	TLSv1.2	1490	Server Hello
139	12.668469	122.9.167.87	192.168.1.106	TLSv1.2	421	Certificate, Server Key Exchange, Server Hello Done
146	12.689471	192.168.1.106	122.9.167.87	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake
150	12.739398	122.9.167.87	192.168.1.106	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypted Handshake

```
> Frame 146: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface \Device\NPF_{B601EEAA-316D-44F3-A63C-8147E700706
> Ethernet II, Src: IntelCor_c0:90:40 (34:f6:4b:c0:90:40), Dst: Tp-LinkT_57:29:ad (f4:2a:7d:57:29:ad)
> Internet Protocol Version 4, Src: 192.168.1.106, Dst: 122.9.167.87
> Transmission Control Protocol, Src Port: 59455, Dst Port: 443, Seq: 518, Ack: 3240, Len: 126
v Transport Layer Security
  > TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
  > TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
  v TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 40
      Handshake Protocol: Encrypted Handshake Message
```

客户端计算并使用会话密钥，加密之前所有收发握手消息的Hash和MAC值，发送给服务器去校验。

Finished 消息是第一条用刚刚协商出来的算法加密保护的消息。接收方必须先确认Finished消息的内容是正确的，之后再开始在连接上发送和接收应用数据。

New Session Ticket 报文（选做）

客户端和服务器端建立了一次完整的握手过程后，服务器端将本次会话的参数进行加密后生成一个ticket票据，并将票据通过NewSessionTicket子消息发送给客户端，下一次连接时客户端如果希望恢复上一次会话而不是重新进行握手，就将“ticket票据”一起发送给服务器端，待服务器端解密校验无误后，进行一次简短的握手，恢复上一次会话。

No.	Time	Source	Destination	Protocol	Length	Info
127	12.616371	192.168.1.106	122.9.167.87	TLSv1.2	571	Client Hello
137	12.668305	122.9.167.87	192.168.1.106	TLSv1.2	1490	Server Hello
139	12.668469	122.9.167.87	192.168.1.106	TLSv1.2	421	Certificate, Server Key Exchange, Server Hello Done
146	12.689471	192.168.1.106	122.9.167.87	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake
150	12.739398	122.9.167.87	192.168.1.106	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypted Handshake

```
> Internet Protocol Version 4, Src: 122.9.167.87, Dst: 192.168.1.106
> Transmission Control Protocol, Src Port: 443, Dst Port: 59455, Seq: 3240, Ack: 644, Len: 242
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: New Session Ticket
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 186
    v Handshake Protocol: New Session Ticket
        Handshake Type: New Session Ticket (4)
        Length: 182
      v TLS Session Ticket
          Session Ticket Lifetime Hint: 300 seconds (5 minutes)
          Session Ticket Length: 176
          Session Ticket: 3a541bba4129e0f2a763350124f42406c7019367520086d009ee464402293aed704497f7…
  > TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
  > TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
```

Change Cipher Spec报文

实验结果：

No.	Time	Source	Destination	Protocol	Length	Info
127	12.616371	192.168.1.106	122.9.167.87	TLSv1.2	571	Client Hello
137	12.668305	122.9.167.87	192.168.1.106	TLSv1.2	1490	Server Hello
139	12.668469	122.9.167.87	192.168.1.106	TLSv1.2	421	Certificate, Server Key Exchange, Server Hello Done
146	12.689471	192.168.1.106	122.9.167.87	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake
150	12.739398	122.9.167.87	192.168.1.106	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypted Handshake

```
> Frame 150: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits) on interface \Device\NPF_{B601EEAA-316D-44F3-A63C-8147E700706
> Ethernet II, Src: Tp-LinkT_57:29:ad (f4:2a:7d:57:29:ad), Dst: IntelCor_c0:90:40 (34:f6:4b:c0:90:40)
> Internet Protocol Version 4, Src: 122.9.167.87, Dst: 192.168.1.106
> Transmission Control Protocol, Src Port: 443, Dst Port: 59455, Seq: 3240, Ack: 644, Len: 242
v Transport Layer Security
  > TLSv1.2 Record Layer: Handshake Protocol: New Session Ticket
  v 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
```

更改密码规格协议报文，服务器端通知客户端后续报文将采用加密方式发送数据。

Finished报文（已被加密）

实验结果：

No.	Time	Source	Destination	Protocol	Length	Info
127	12.616371	192.168.1.106	122.9.167.87	TLSv1.2	571	Client Hello
137	12.668305	122.9.167.87	192.168.1.106	TLSv1.2	1490	Server Hello
139	12.668469	122.9.167.87	192.168.1.106	TLSv1.2	421	Certificate, Server Key Exchange, Server Hello Done
146	12.689471	192.168.1.106	122.9.167.87	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake
150	12.739398	122.9.167.87	192.168.1.106	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypted Handshake

```
> Frame 150: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits) on interface \Device\NPF_{B601EEAA-316D-44F3-A63C-8147E700706
> Ethernet II, Src: Tp-LinkT_57:29:ad (f4:2a:7d:57:29:ad), Dst: IntelCor_c0:90:40 (34:f6:4b:c0:90:40)
> Internet Protocol Version 4, Src: 122.9.167.87, Dst: 192.168.1.106
> Transmission Control Protocol, Src Port: 443, Dst Port: 59455, Seq: 3240, Ack: 644, Len: 242
v Transport Layer Security
  > TLSv1.2 Record Layer: Handshake Protocol: New Session Ticket
  > TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
  v TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 40
      Handshake Protocol: Encrypted Handshake Message
```

服务器计算并使用会话密钥，加密之前所有收发握手消息的Hash和MAC值，发送给客户端去校验。

实验分析

请同学们根据个人实际的实验情况，进行实验结果截图，并撰写实验分析（不用绘制报文格式）：

- Client Hello报文实验分析：（略）
- Server Hello报文实验分析：（略）
- Certificate，Server Key Exchange，Server Hello Done报文实验分析：（略）
- Client Key Exchange，Change Cipher Spec，Finished报文实验分析：（略）
- Change Cipher Spec，Finished报文实验分析：（略）

谢谢