网络协议笔记5-应用层3（HTTPS）

- https译为超文本传输安全协议，即HTTP协议增加了SSL协议或一个TLS协议（SSL协议的升级版本）来加密报文的
- https的默认端口号是443
- TLS协议可以用于其他协议，比如FTP->FTPS,SMTP->SMTPS

TLS

- 译为传输层安全性协议，前身为SSL（安全套接层）
- TLS工作在应用层和传输层之间，作为桥梁
- 使用TLS：
    - 需要支付证书的费用
    - 需要加解密的消耗
    - 会降低访问速度

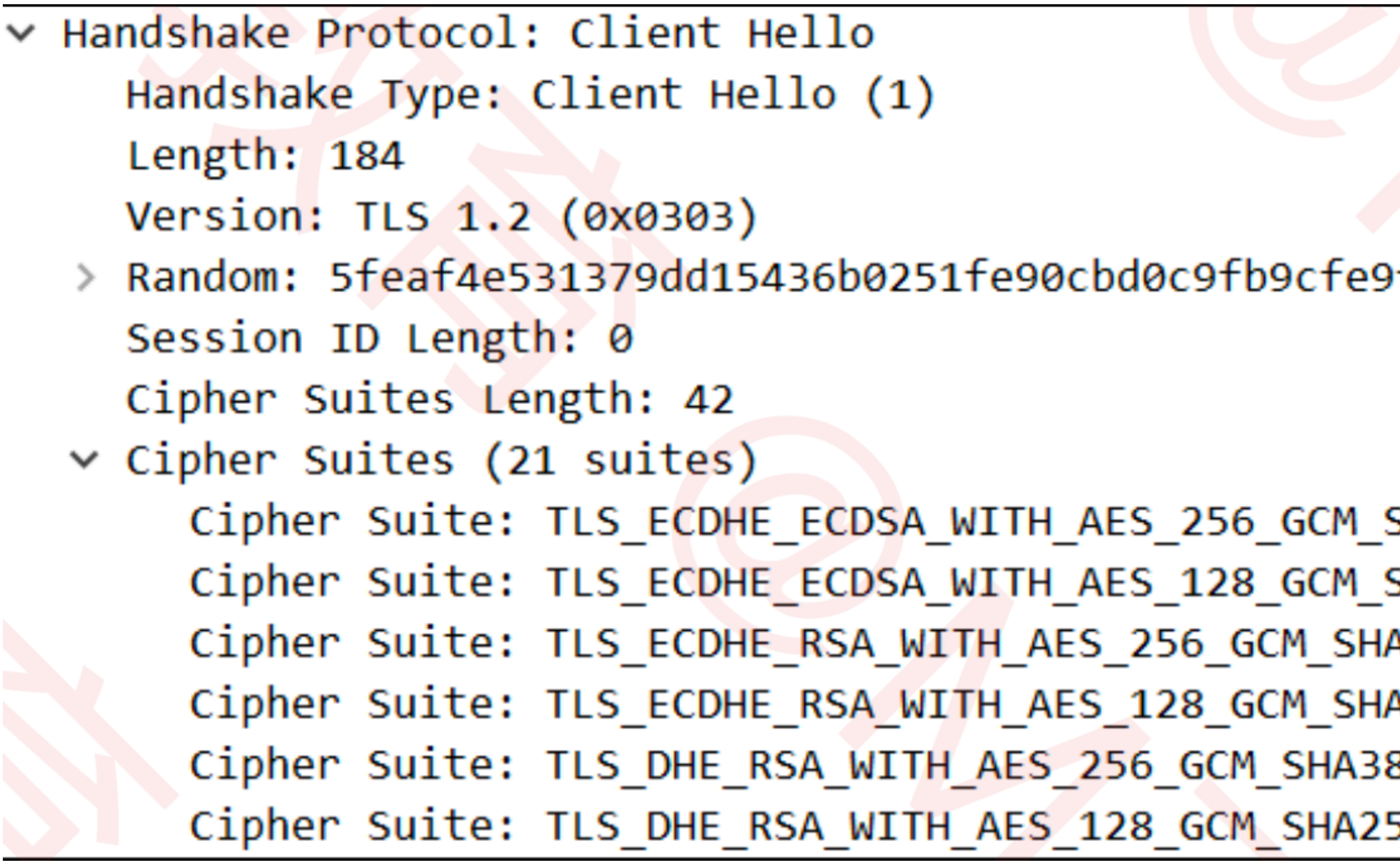
HTTPS的通讯过程

- 分为3阶段

1. TCP的3次握手
2. TLS的连接
3. HTTP的请求和响应

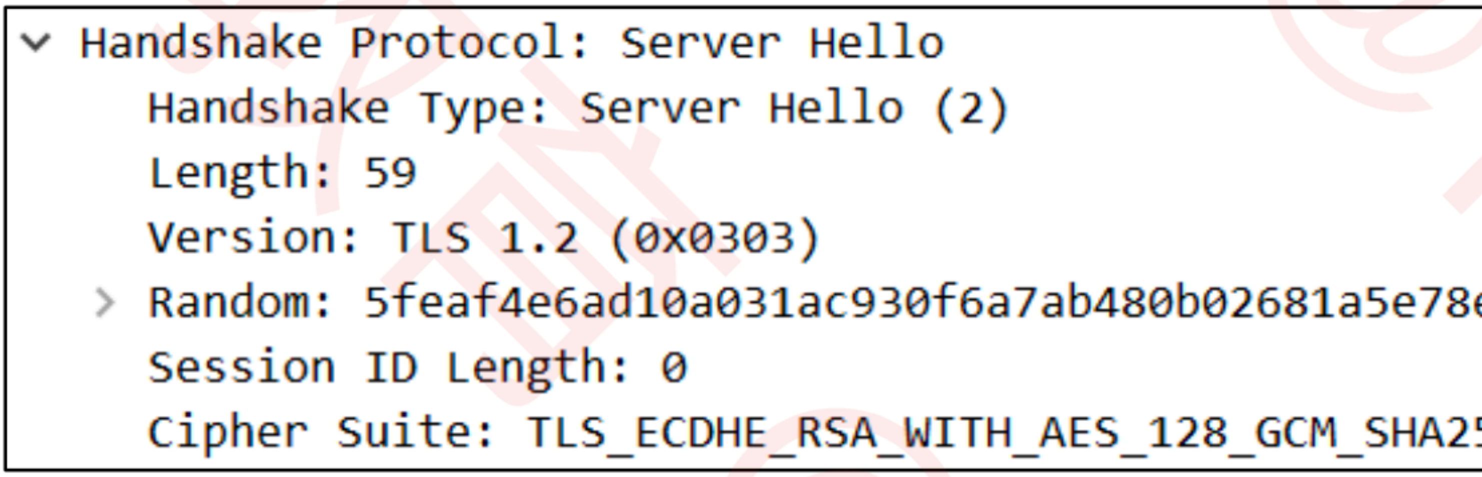
TLS1.2的连接过程（每次交互会有ACK确认响应回复）

1. 客户端发送给服务器： Client Hello
    - 包含TLS版本号
    - 支持的加密组件：指所使用的加密算法和密钥长度
    - 一个随机数



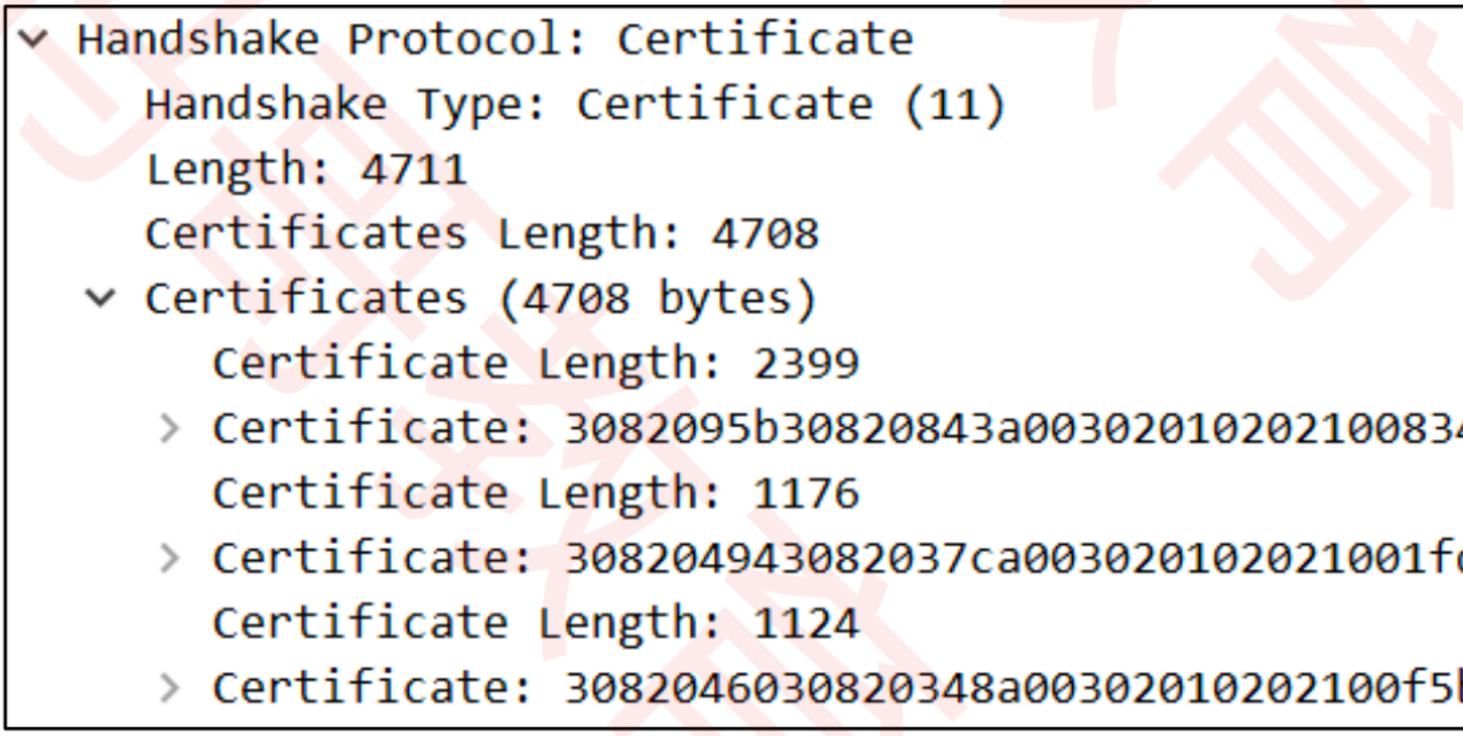
```
v Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 184
    Version: TLS 1.2 (0x0303)
  > Random: 5feaf4e531379dd15436b0251fe90cbd0c9fb9cfe9
    Session ID Length: 0
    Cipher Suites Length: 42
  v Cipher Suites (21 suites)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_S
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_S
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA
      Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA38
      Cipher Suite: TLS_DHE_RSA_WITH_AES_128_GCM_SHA25
```

2. 服务器发送给客户端：Server Hello - 包含TLS版本号 - 选择的加密组件：在第一步中客户端支持加密组件列表中选择的 - 一个随机数



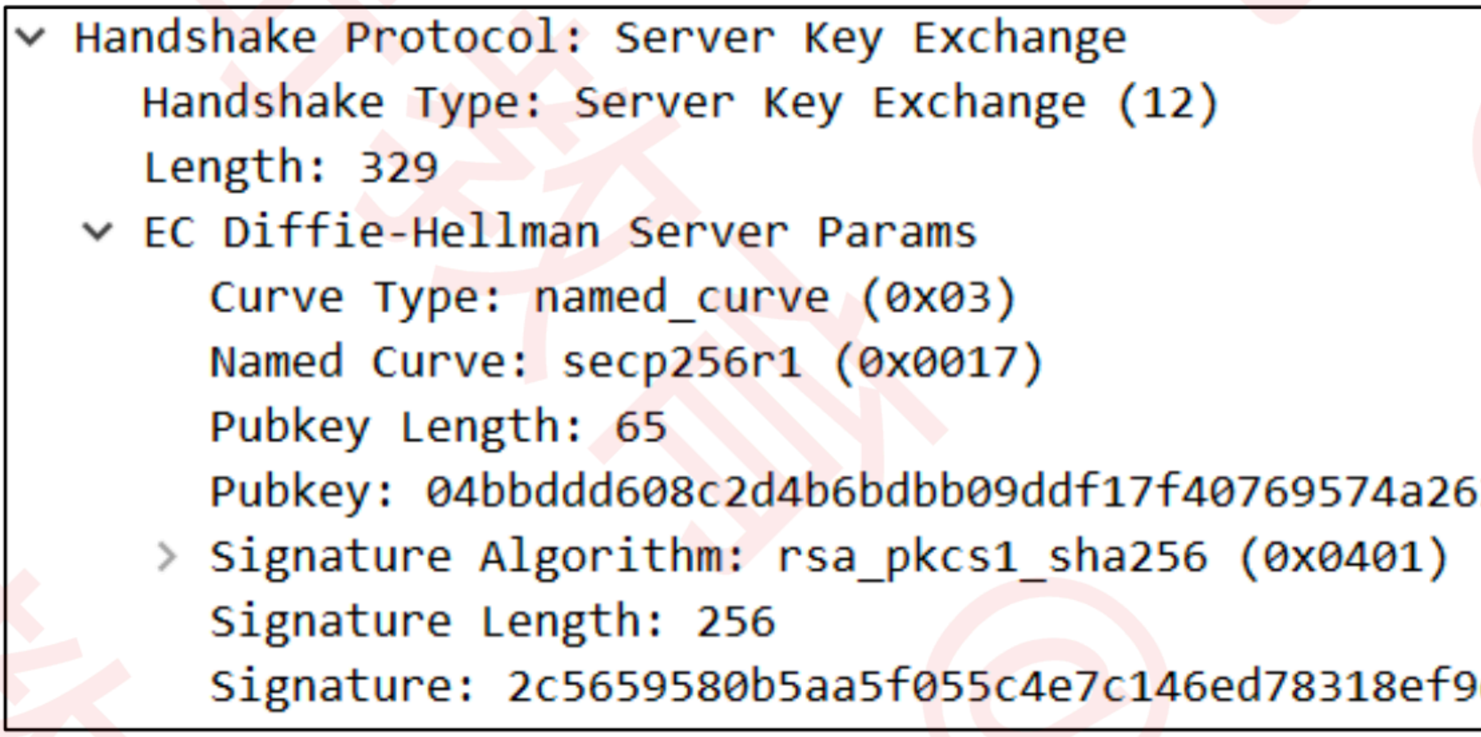
```
v Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 59
    Version: TLS 1.2 (0x0303)
  > Random: 5feaf4e6ad10a031ac930f6a7ab480b02681a5e78e
    Session ID Length: 0
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA25
```

3. 服务器发送给客户端：Certificate - 包含服务器的被CA签名过的公钥证书



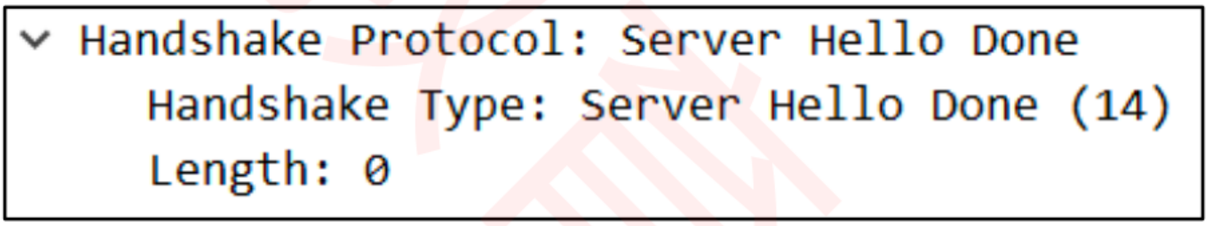
```
v Handshake Protocol: Certificate
    Handshake Type: Certificate (11)
    Length: 4711
    Certificates Length: 4708
  v Certificates (4708 bytes)
      Certificate Length: 2399
    > Certificate: 3082095b30820843a00302010202100834
      Certificate Length: 1176
    > Certificate: 30820494308203 7ca003020102021001fc
      Certificate Length: 1124
    > Certificate: 308204603082 0348a003020102021 00f5b
```

4. 服务器发送给客户端：Server Key Exchange - 包含实现ECDHE算法的其中一个参数（Server Params） - ECDHE是密钥交换算法，为了防止伪造，Server Params经过了服务器私钥签名



```
v Handshake Protocol: Server Key Exchange
    Handshake Type: Server Key Exchange (12)
    Length: 329
  v EC Diffie-Hellman Server Params
      Curve Type: named_curve (0x03)
      Named Curve: secp256r1 (0x0017)
      Pubkey Length: 65
      Pubkey: 04bbddd608c2d4b6bdbb09ddf17f40769574a26
    > Signature Algorithm: rsa_pkcs1_sha256 (0x0401)
      Signature Length: 256
      Signature: 2c5659580b5aa5f055c4e7c146ed78318ef9
```

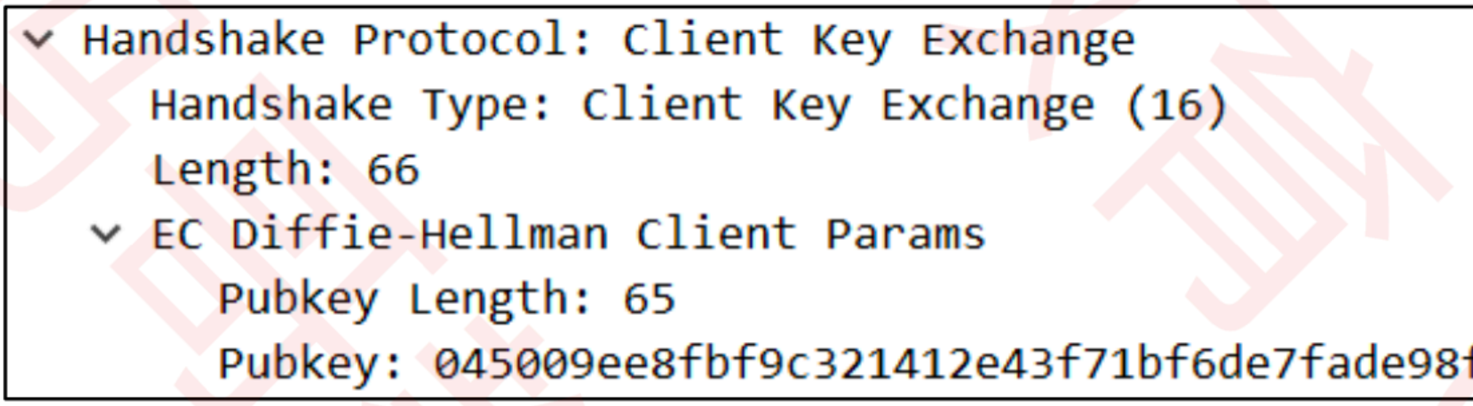
5. 服务器发送给客户端：Server Hello Done - 告诉客户端协商部分已经结束 - 此时，客户端与服务器通过明文共享了Client Random、Server Random、 Server params - 客户端拿到了服务器的公钥证书，接下来会验证公钥的真实性



```
v Handshake Protocol: Server Hello Done
    Handshake Type: Server Hello Done (14)
    Length: 0
```

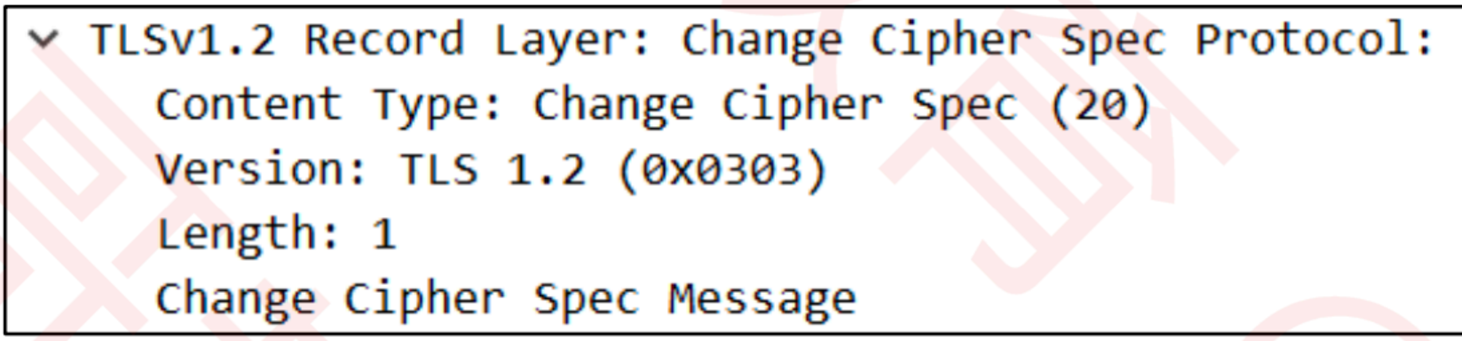
6. 客户端发送给服务器：Client Key Exchange - 实现ECDHE算法的另一个参数（Client Params） - 此时双方拥有了ECDHE算法的2个参数，可以通过该算法计算出一个新的密钥串：Pre-master secret - 然后用Client Random、Server Random、Pre-master secret生成一个主密钥 - 然后利用主密钥衍生出其他

密钥：双方发送用的会话密钥



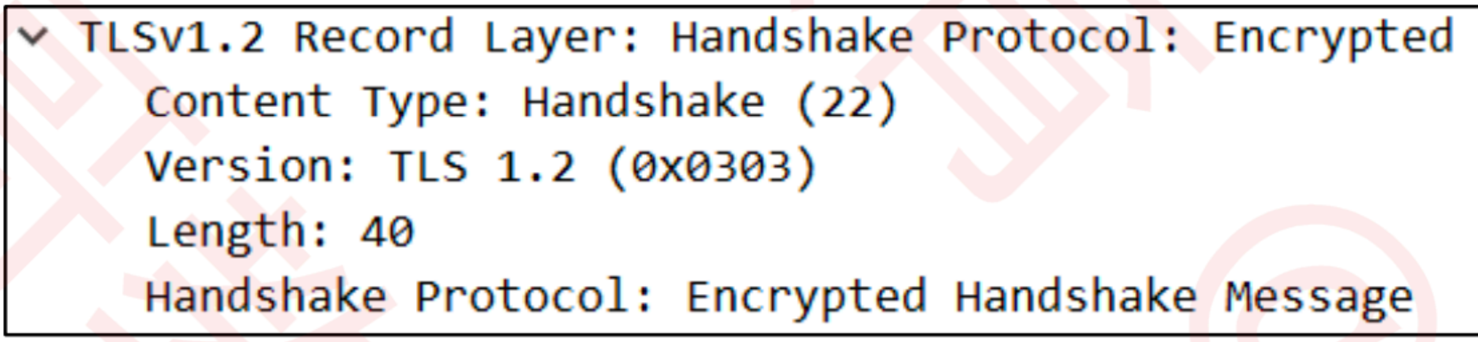
```
⌄ Handshake Protocol: Client Key Exchange
    Handshake Type: Client Key Exchange (16)
    Length: 66
  ⌄ EC Diffie-Hellman Client Params
      Pubkey Length: 65
      Pubkey: 045009ee8fbf9c321412e43f71bf6de7fade98
```

7. 客户端发送给服务器：Change Cipher Spec - 告诉服务器之后的通信会采用计算出来的会话密钥进行加密



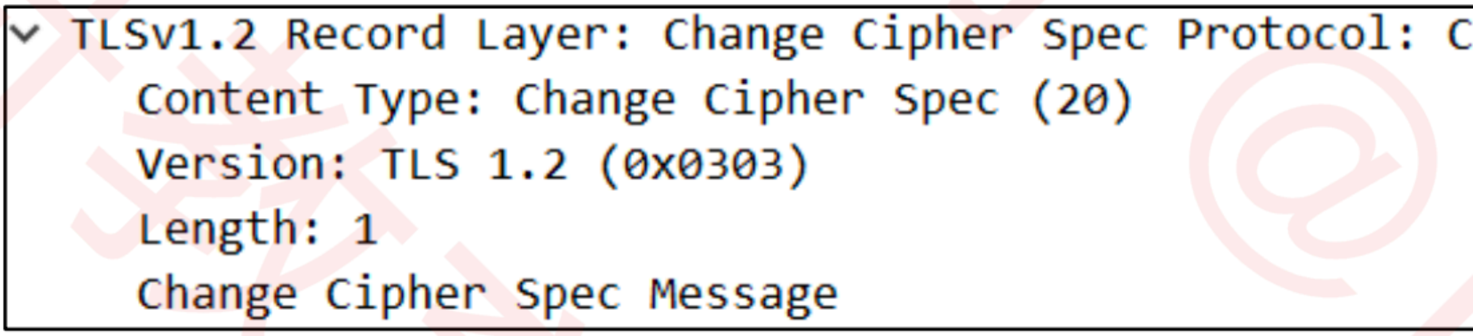
```
⌄ TLSv1.2 Record Layer: Change Cipher Spec Protocol:
    Content Type: Change Cipher Spec (20)
    Version: TLS 1.2 (0x0303)
    Length: 1
    Change Cipher Spec Message
```

8. 客户端发送给服务器：Finished - 包含此前全部报文整体校验值（摘要），加密后发送给服务器 - 此次握手是否成功，以服务器能否正确解密该报文为判定标准

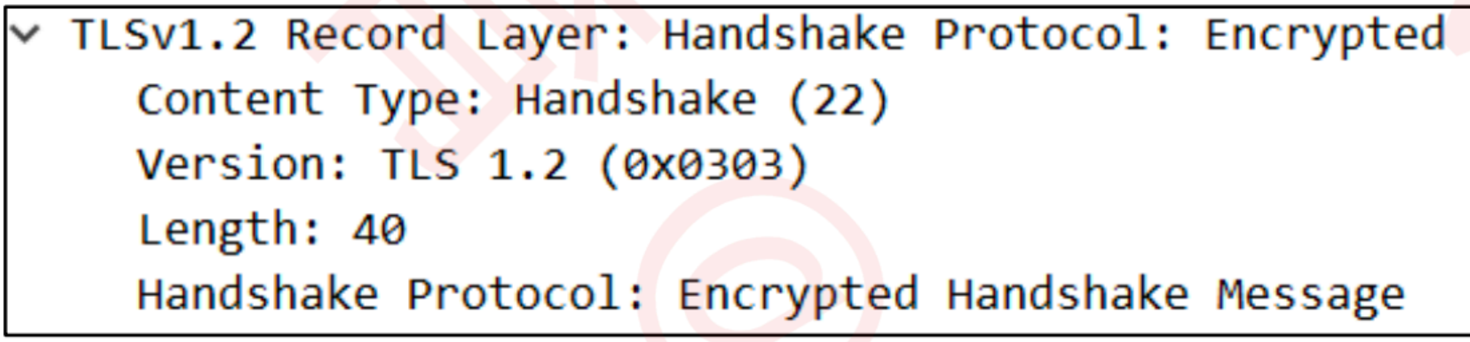


```
⌄ TLSv1.2 Record Layer: Handshake Protocol: Encrypted
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 40
    Handshake Protocol: Encrypted Handshake Message
```

9. 服务器发送给客户端：Change Cipher Spec 10. 服务器发送给客户端：Finished - 到此，双方验证加解密无误，握手结束，后面传递加密的HTTP请求和响应



```
⌄ TLSv1.2 Record Layer: Change Cipher Spec Protocol: C
    Content Type: Change Cipher Spec (20)
    Version: TLS 1.2 (0x0303)
    Length: 1
    Change Cipher Spec Message
```



```
⌄ TLSv1.2 Record Layer: Handshake Protocol: Encrypted
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 40
    Handshake Protocol: Encrypted Handshake Message
```