[redacted]

实验目的：

了解 SSL 的工作原理。

实验结果：

1. 对于前 8 个以太网帧，请分别指出每一个帧的来源（客户端和服务器），确定每个帧包含的 SSL 记录的数量，并且列出包含 SSL 记录的类型。绘制客户端和服务器含有箭头指向的时序图。

106	21.805705	128.238.38.162	216.75.194.220	SSLv2	132 Client Hello
108	21.830201	216.75.194.220	128.238.38.162	SSLv3	1434 Server Hello
111	21.853520	216.75.194.220	128.238.38.162	SSLv3	790 Certificate, Server Hello Done
112	21.876168	128.238.38.162	216.75.194.220	SSLv3	258 Client Key Exchange, Change Cipher
113	21.945667	216.75.194.220	128.238.38.162	SSLv3	121 Change Cipher Spec, Encrypted Hand
114	21.954189	128.238.38.162	216.75.194.220	SSLv3	806 Application Data
122	23.480352	216.75.194.220	128.238.38.162	SSLv3	272 Application Data
149	23.559497	216.75.194.220	128.238.38.162	SSLv3	1367 Application Data

第一个帧：来源：128.238.38.162，数量：1，记录类型：SSL 2.0

第二个帧：来源：216.75.194.220，数量：1，记录类型：SSL 3.0

第三个帧：来源：216.75.194.220，数量：2，记录类型：SSL 3.0

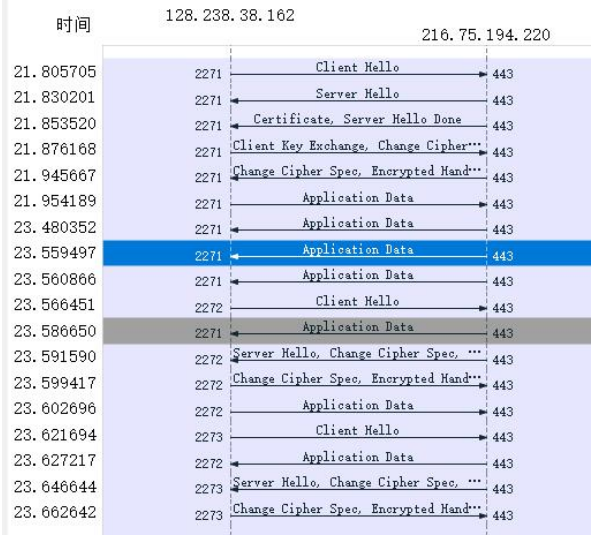
第四个帧：来源：128.238.38.162，数量：3，记录类型：SSL 3.0

第五个帧：来源：216.75.194.220，数量：2，记录类型：SSL 3.0

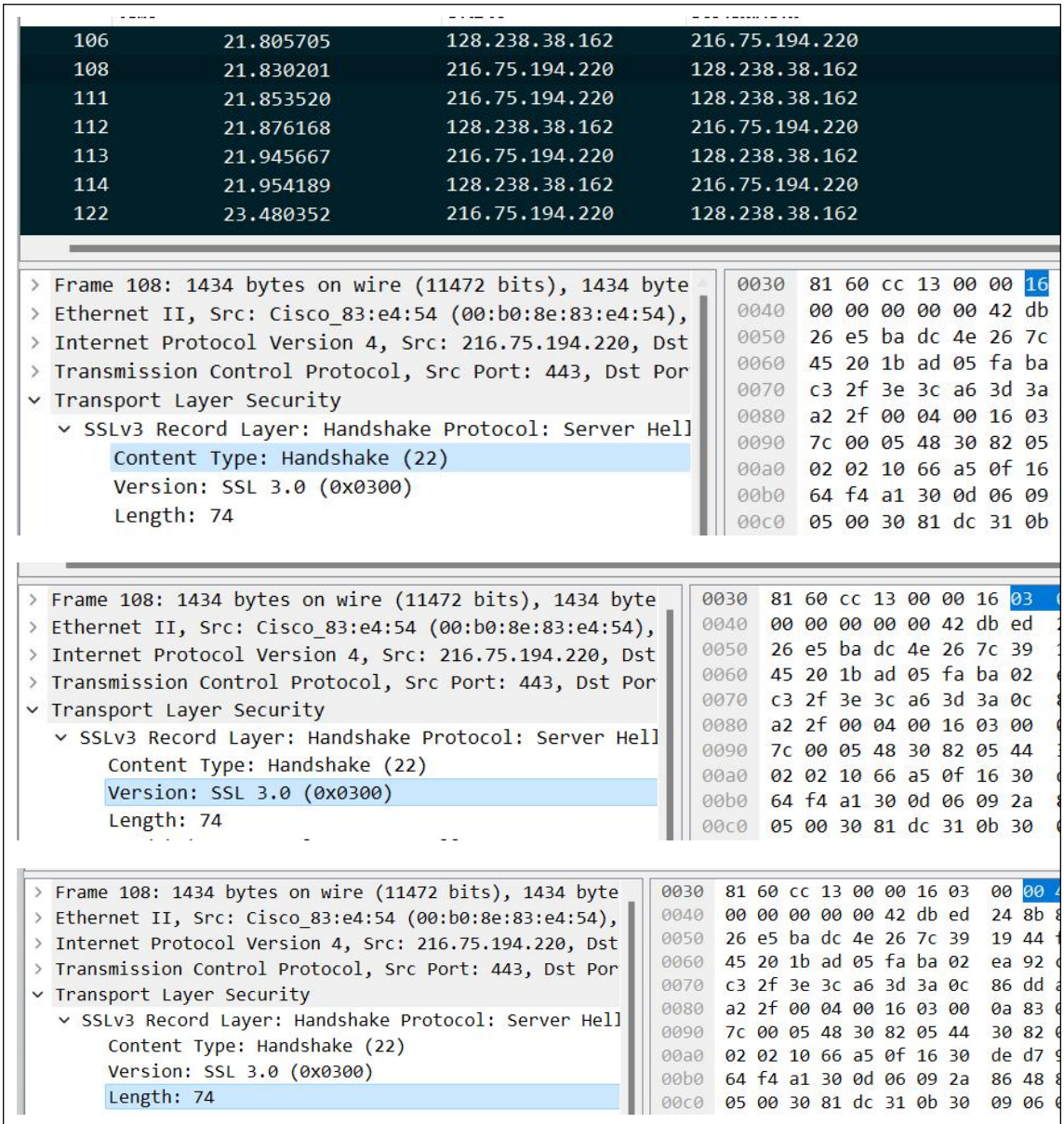
第六个帧：来源：128.238.38.162，数量：1，记录类型：SSL 3.0

第七个帧：来源：216.75.194.220，数量：1，记录类型：SSL 3.0

第八个帧：来源：216.75.194.220，数量：1，记录类型：SSL 3.0

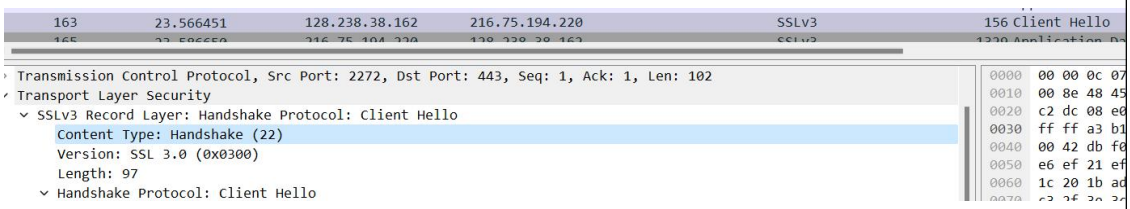


2. 每个 SSL 记录都以相同的三个字段开头（可能具有不同的值）。其中一个字段是“内容类型”，长度为一个字节。列出所有三个字段及其长度。



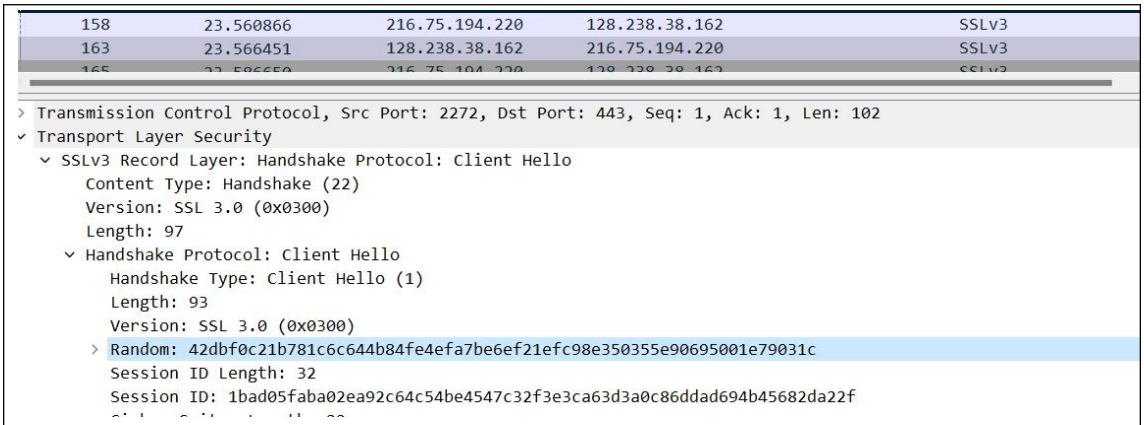
如图，Content Type 为 1 字节，Version 字段为 2 字节，Length 字段为 2 字节。

3.展开 ClientHello 记录。（如果跟踪包含多个 ClientHello 记录，请展开包含第一个记录的帧。）内容类型的值是多少？
（第一个 ClientHello 记录是 SSL2 类型，无 Content Type 字段）



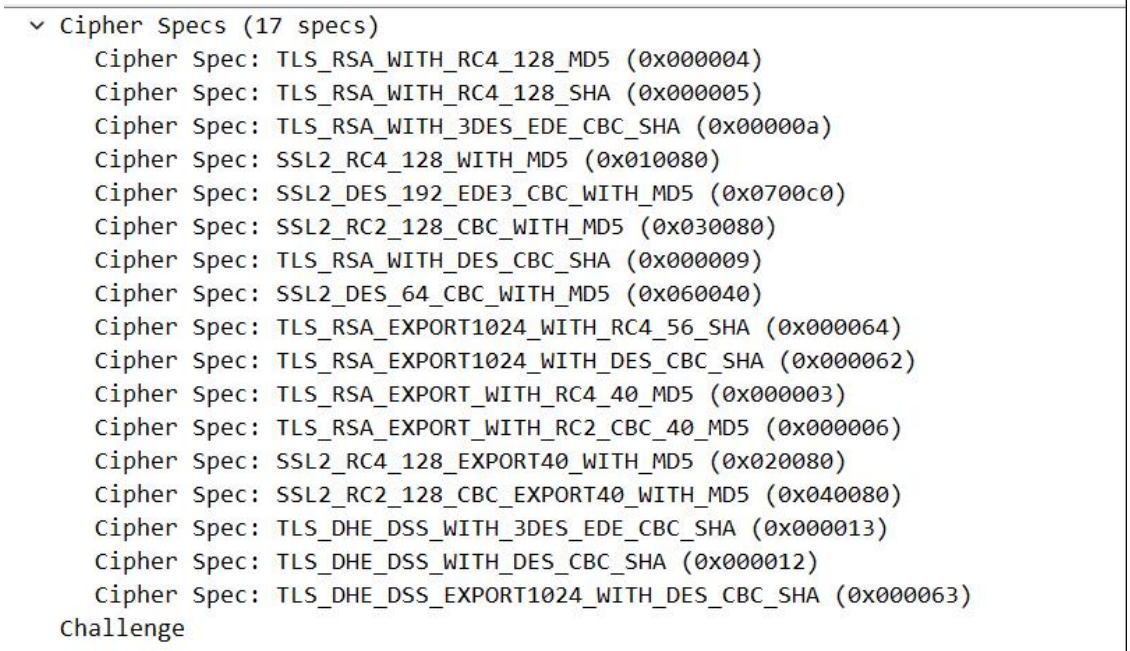
如图，是 Handshake(22)，握手协议

4.ClientHello 记录是否包含随机数（也称为“挑战码”（ challenge））？ 如果是 这样，十六进制的挑战码值是多少？



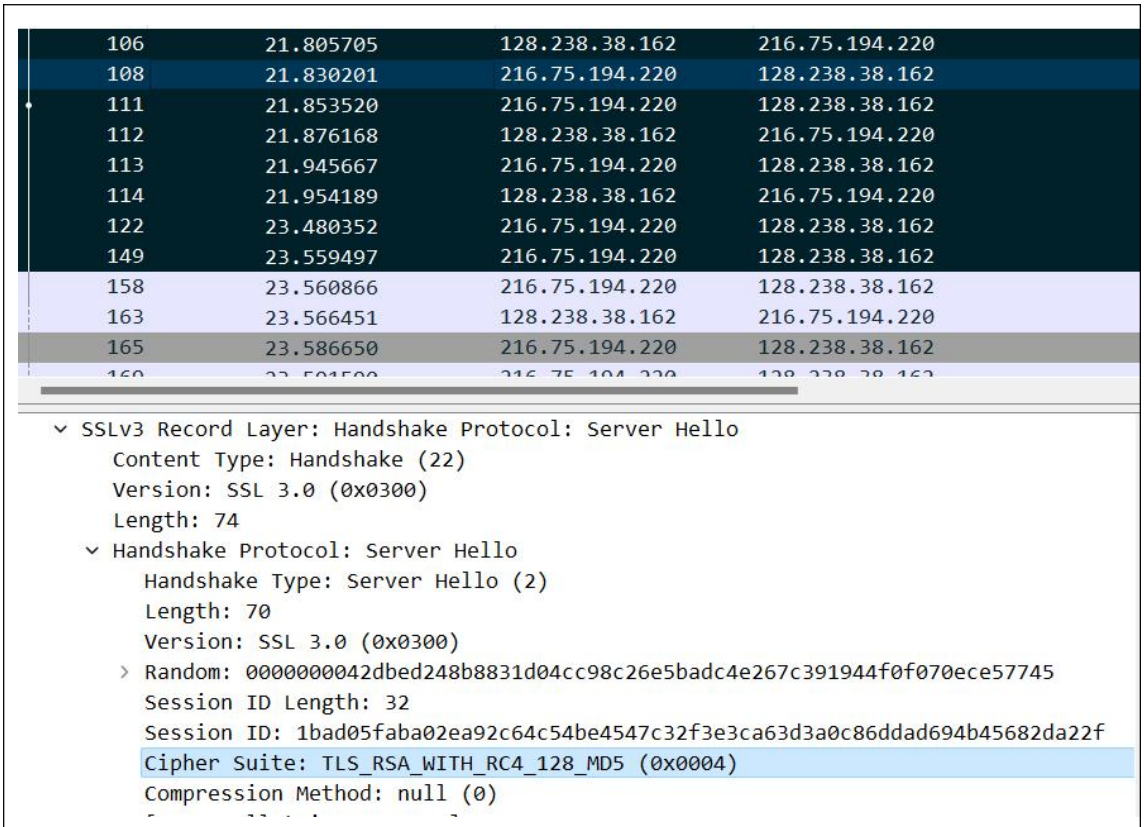
Random:
42dbf0c21b781c6c644b84fe4efa7be6ef21efc98e350355e90695001e79031c

5.ClientHello 记录是否通知了它所支持密码加密套件（suite）？如果是这样，请在第一个密码套件， 分别指出非对称密钥加密算法，对称密钥加密算法，哈希算法分别都是什么？



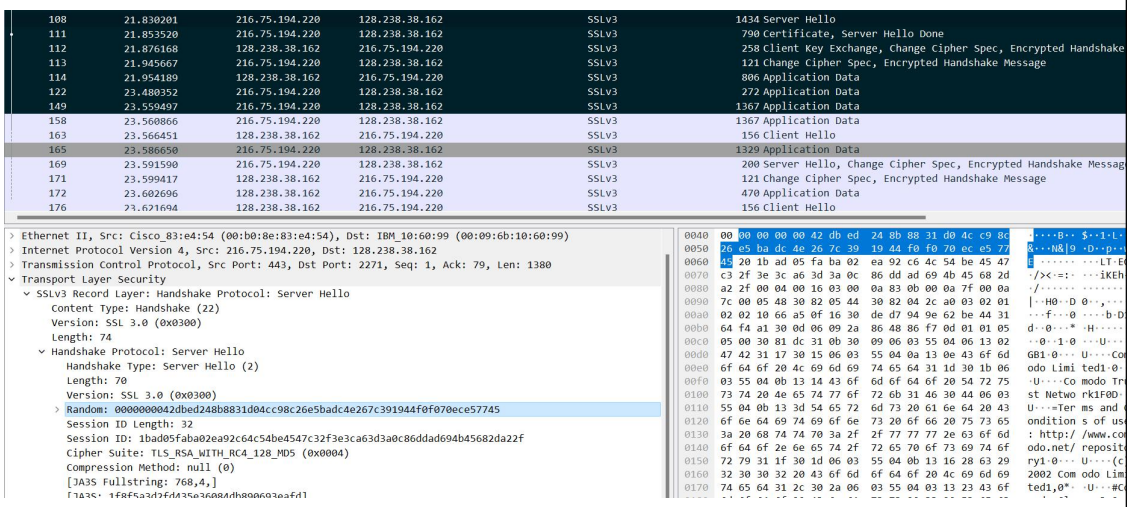
如图，密码套件为 Cipher Spec: TLS_RSA_WITH_3DES_EDE_CBC_SHA
非对称密钥加密算法：RSA
对称密钥加密算法：3DES
哈希算法：SHA

6. 找到 ServerHello SSL 记录。 此记录是否指定了之前的密码套件之一？ 选择的密码套件中有哪些算法？



指定了之前的一个密码套件
其中含有算法：
非对称密钥加密算法：RSA；
对称密钥加密算法：RC4_128；
哈希算法：MD5

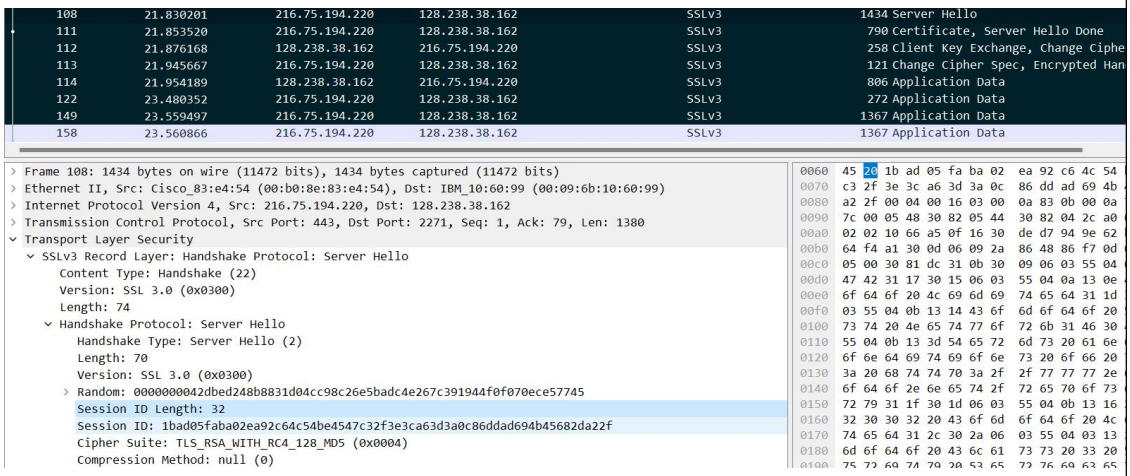
7.此记录是否包含随机数？如果有，它有多长？SSL 中客户端和服务器段随机数用来干什么？



如图，包含，
Random:
0000000042dbed248b8831d04cc98c26e5badc4e267c391944f0f070ece57745
长度为 32bytes，

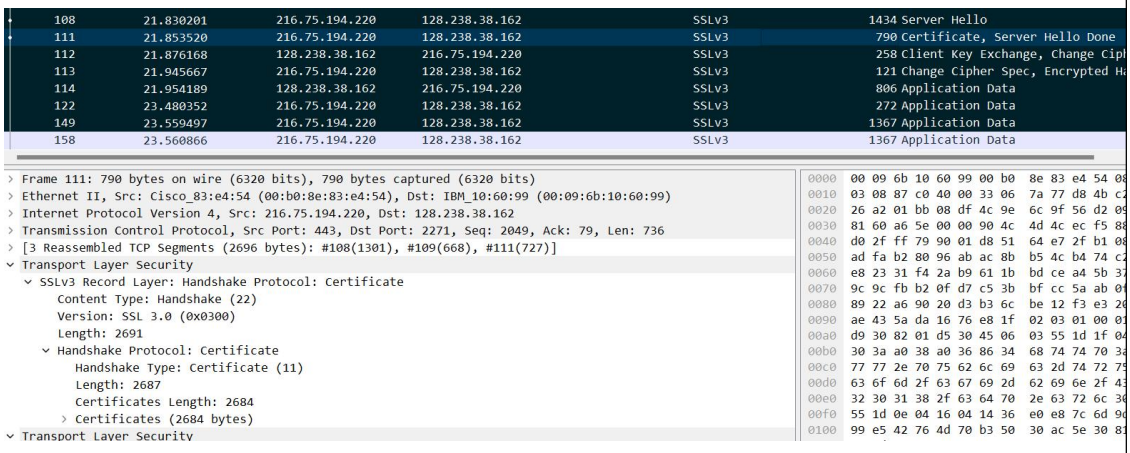
能够多次随机数生成为未来生成对称密钥提高安全性能。

8. 此记录是否包含会话 ID？ 会话 ID 的目的是什么？



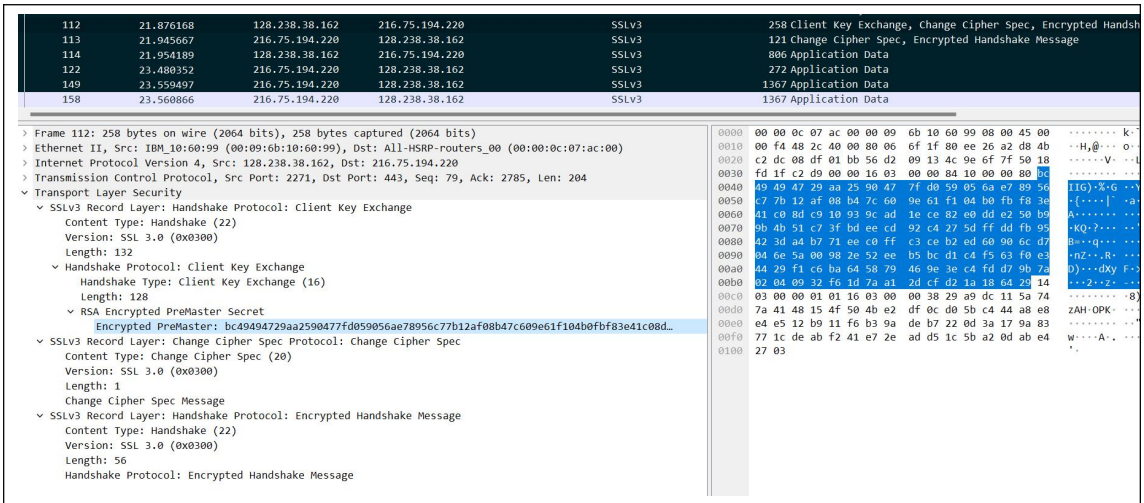
包含，目的是用一定时间内端口连接快速恢复连接过程。
服务器将约定的 Session 参数存储在 TLS 缓存中，并生成与其对应的 Session id。它与 Server Hello 一起发送到客户端。客户端可以写入约定的参数到此 Session id，并给定到期时间。客户端在 Client Hello 中将包含此 id。如果客户端在此到期时间之前再次连接到服务器，则服务器可以检查与 Session id 对应的缓存参数，并重用它们而无需完全握手。这样服务器和客户端都可以节省大量的计算成本。

9. 此记录是否包含证书，或者证书是否包含在单独的记录中。 证书是否适合一个单独的以太网帧传输？



不包含证书，证书包含在一个单独的记录里

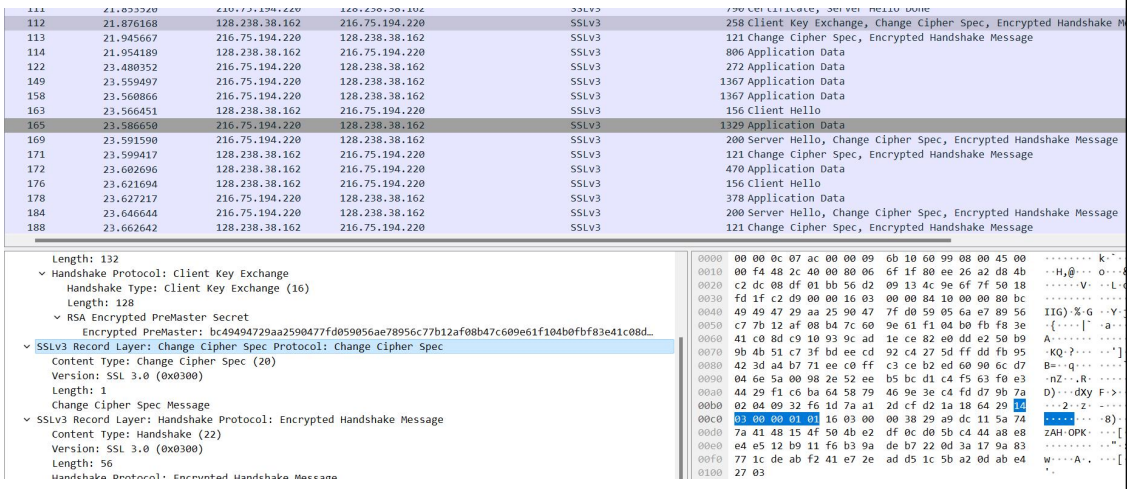
10. 找到客户端密钥交换记录。 此记录是否包含前主密钥(pre-master secret)？ 这个前主密钥用于什么？ 前主密钥加密了吗？ 如果是这样，为什么？ 加密的前主密钥有多长？



如图，此记录包含前主密钥，长 128bytes

已经有 RSA 方法进行加密，客户端根据之前从服务器端收到的随机数，按照不同的密钥交换算法，算出一个 pre-master，发送给服务器，服务器端收到 pre-master 算出 main master。而客户端自己通过 pre-master 算出 main master。这样双方就算出了对称密钥。

11. 编码改变记录目的是什么？在您的跟踪中本记录有多少字节



告诉服务器已经计算好加密密钥，以后将会用商定的加密方式和密钥加密传输了，在我的跟踪中该记录有 6 个字节。

12. 在加密的握手记录中，什么是加密的？ 为什么？
消息校验码是加密的，这个校验码是包含之前所有连接消息的摘要加密格式，只有服务器可以解开，因为在建立连接中，存在可能连接消息被侦听和更改的情况，因此还需要进行信息摘要计算和加密传输，判断是否存在异常，如果异常，将会直接关闭连接。

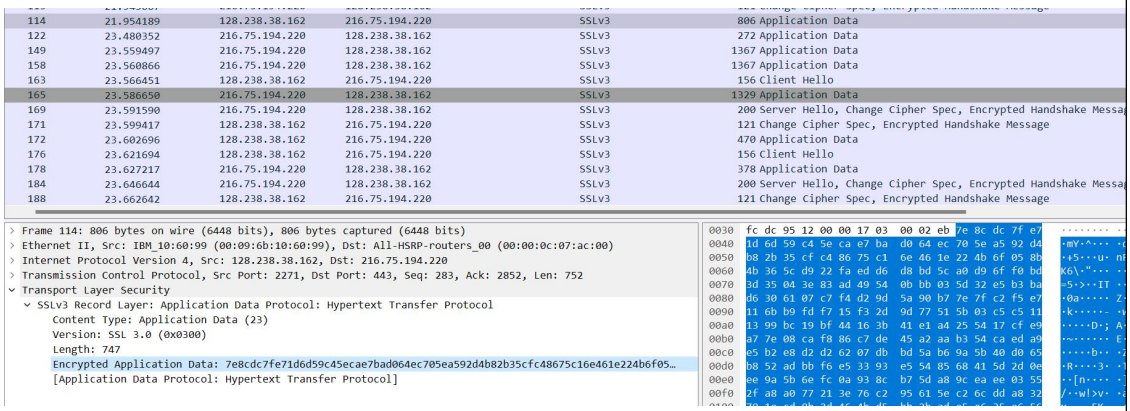
13. 服务器是否还向客户端发送更改编码记录和加密的握手记录？ 这些记录与客户发送的记录有何不同？

```
            Encrypted PreMaster: bc49494729aa2590477fd059056ae78956c77b12af08b47c609e61f104b0fbf83e41c08d…
  ⌄ SSLv3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
        Content Type: Change Cipher Spec (20)
        Version: SSL 3.0 (0x0300)
        Length: 1
        Change Cipher Spec Message
  ⌄ SSLv3 Record Layer: Handshake Protocol: Encrypted Handshake Message
        Content Type: Handshake (22)
        Version: SSL 3.0 (0x0300)
        Length: 56
        Handshake Protocol: Encrypted Handshake Message
```

```
  ⌄ SSLv3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
        Content Type: Change Cipher Spec (20)
        Version: SSL 3.0 (0x0300)
        Length: 1
        Change Cipher Spec Message
  ⌄ SSLv3 Record Layer: Handshake Protocol: Encrypted Handshake Message
        Content Type: Handshake (22)
        Version: SSL 3.0 (0x0300)
        Length: 56
        Handshake Protocol: Encrypted Handshake Message
```

如图，可以看出，服务器向客户发了。没有不同，加密握手记录中同样是包含之前所有连接消息摘要的加密形式，用以供客户端解密，判断是否存在异常选择处理。

14. 如何加密应用程序数据？ 包含应用程序数据的记录是否包含消息认证码 MAC？ Wireshark 是否区分加密的应用程序数据和消息认证码 MAC？



消息首先将会被分段，然后压缩，再计算其消息验证码，然后使用对称密码进行加密，在服务端收到密文之后，进行解密，客户端收到服务端的数据之后进行解密，然后双方使用各自的 MAC 对数据的完整性是否被串改进行验证。这个数据里同时包括消息本身和消息认证码，所以比消息本身要长，但是加密过，所以无法区分。

15. 请您指出和解释您在跟踪中发现的任何其他内容。
跟踪中，没有发现其他内容。