

### 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（客户端和服务端），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。绘制客户端和服务端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

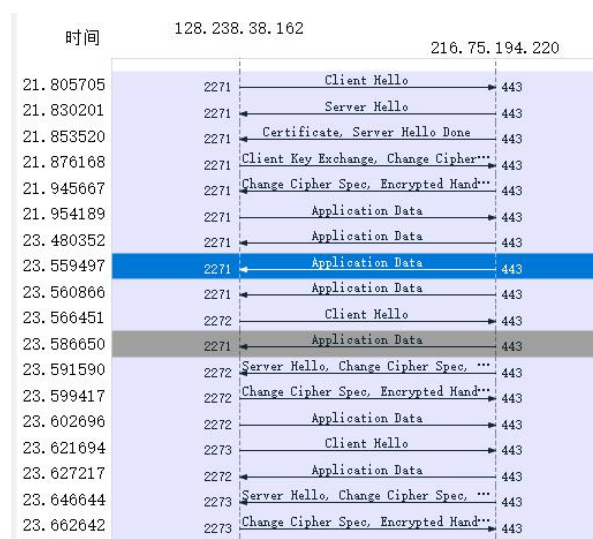
第四个帧：来源：128.238.38.162，数量：3，记录类型：SSL 3.0

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。

|     |           |                |                |
|-----|-----------|----------------|----------------|
| 106 | 21.805705 | 128.238.38.162 | 216.75.194.220 |
| 108 | 21.830201 | 216.75.194.220 | 128.238.38.162 |
| 111 | 21.853520 | 216.75.194.220 | 128.238.38.162 |
| 112 | 21.876168 | 128.238.38.162 | 216.75.194.220 |
| 113 | 21.945667 | 216.75.194.220 | 128.238.38.162 |
| 114 | 21.954189 | 128.238.38.162 | 216.75.194.220 |
| 122 | 23.480352 | 216.75.194.220 | 128.238.38.162 |

|  |  |
|--|--|
| <ul style="list-style-type: none"> <li>&gt; Frame 108: 1434 bytes on wire (11472 bits), 1434 byte</li> <li>&gt; Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54),</li> <li>&gt; Internet Protocol Version 4, Src: 216.75.194.220, Dst</li> <li>&gt; Transmission Control Protocol, Src Port: 443, Dst Por</li> <li>▼ Transport Layer Security <ul style="list-style-type: none"> <li>▼ SSLv3 Record Layer: Handshake Protocol: Server Hell <ul style="list-style-type: none"> <li>Content Type: Handshake (22)</li> <li>Version: SSL 3.0 (0x0300)</li> <li>Length: 74</li> </ul> </li> </ul> </li> </ul> | 0030 81 60 cc 13 00 00 16<br>0040 00 00 00 00 00 42 db<br>0050 26 e5 ba dc 4e 26 7c<br>0060 45 20 1b ad 05 fa ba<br>0070 c3 2f 3e 3c a6 3d 3a<br>0080 a2 2f 00 04 00 16 03<br>0090 7c 00 05 48 30 82 05<br>00a0 02 02 10 66 a5 0f 16<br>00b0 64 f4 a1 30 0d 06 09<br>00c0 05 00 30 81 dc 31 0b |
|--|--|

|  |   |
|--|---|
| <ul style="list-style-type: none"> <li>&gt; Frame 108: 1434 bytes on wire (11472 bits), 1434 byte</li> <li>&gt; Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54),</li> <li>&gt; Internet Protocol Version 4, Src: 216.75.194.220, Dst</li> <li>&gt; Transmission Control Protocol, Src Port: 443, Dst Por</li> <li>▼ Transport Layer Security <ul style="list-style-type: none"> <li>▼ SSLv3 Record Layer: Handshake Protocol: Server Hell <ul style="list-style-type: none"> <li>Content Type: Handshake (22)</li> <li>Version: SSL 3.0 (0x0300)</li> <li>Length: 74</li> </ul> </li> </ul> </li> </ul> | 0030 81 60 cc 13 00 00 16<br>0040 00 00 00 00 00 42 db ed<br>0050 26 e5 ba dc 4e 26 7c 39<br>0060 45 20 1b ad 05 fa ba 02<br>0070 c3 2f 3e 3c a6 3d 3a 0c<br>0080 a2 2f 00 04 00 16 03 00<br>0090 7c 00 05 48 30 82 05 44<br>00a0 02 02 10 66 a5 0f 16 30<br>00b0 64 f4 a1 30 0d 06 09 2a<br>00c0 05 00 30 81 dc 31 0b 30 |
|--|---|

|  |   |
|--|---|
| <ul style="list-style-type: none"> <li>&gt; Frame 108: 1434 bytes on wire (11472 bits), 1434 byte</li> <li>&gt; Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54),</li> <li>&gt; Internet Protocol Version 4, Src: 216.75.194.220, Dst</li> <li>&gt; Transmission Control Protocol, Src Port: 443, Dst Por</li> <li>▼ Transport Layer Security <ul style="list-style-type: none"> <li>▼ SSLv3 Record Layer: Handshake Protocol: Server Hell <ul style="list-style-type: none"> <li>Content Type: Handshake (22)</li> <li>Version: SSL 3.0 (0x0300)</li> <li>Length: 74</li> </ul> </li> </ul> </li> </ul> | 0030 81 60 cc 13 00 00 16 03<br>0040 00 00 00 00 00 42 db ed 24<br>0050 26 e5 ba dc 4e 26 7c 39 19<br>0060 45 20 1b ad 05 fa ba 02 ea<br>0070 c3 2f 3e 3c a6 3d 3a 0c 86<br>0080 a2 2f 00 04 00 16 03 00 0a<br>0090 7c 00 05 48 30 82 05 44 30<br>00a0 02 02 10 66 a5 0f 16 30 de<br>00b0 64 f4 a1 30 0d 06 09 2a 86<br>00c0 05 00 30 81 dc 31 0b 30 09 |
|--|---|

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）

|     |           |                |                |       |                       |
|-----|-----------|----------------|----------------|-------|-----------------------|
| 163 | 23.566451 | 128.238.38.162 | 216.75.194.220 | SSLv3 | 156 Client Hello      |
| 165 | 23.566559 | 216.75.194.220 | 128.238.38.162 | SSLv2 | 1320 Application Data |

|   |  |
|---|--|
| <ul style="list-style-type: none"> <li>Transmission Control Protocol, Src Port: 2272, Dst Port: 443, Seq: 1, Ack: 1, Len: 102</li> <li>Transport Layer Security <ul style="list-style-type: none"> <li>▼ SSLv3 Record Layer: Handshake Protocol: Client Hello <ul style="list-style-type: none"> <li>Content Type: Handshake (22)</li> <li>Version: SSL 3.0 (0x0300)</li> <li>Length: 97</li> </ul> </li> <li>Handshake Protocol: Client Hello</li> </ul> </li> </ul> | 0000 00 00 0c 07<br>0010 00 8e 48 45<br>0020 c2 dc 08 e0<br>0030 ff ff a3 b1<br>0040 00 42 db fd<br>0050 e6 ef 21 ef<br>0060 1c 20 1b ad<br>0070 c3 2f 3e 3c |
|---|--|

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？

|     |           |                |                |       |
|-----|-----------|----------------|----------------|-------|
| 158 | 23.560866 | 216.75.194.220 | 128.238.38.162 | SSLv3 |
| 163 | 23.566451 | 128.238.38.162 | 216.75.194.220 | SSLv3 |
| 165 | 23.566550 | 216.75.194.220 | 128.238.38.162 | SSLv3 |

> Transmission Control Protocol, Src Port: 2272, Dst Port: 443, Seq: 1, Ack: 1, Len: 102

✓ Transport Layer Security

- SSLv3 Record Layer: Handshake Protocol: Client Hello
  - Content Type: Handshake (22)
  - Version: SSL 3.0 (0x0300)
  - Length: 97
  - Handshake Protocol: Client Hello
    - Handshake Type: Client Hello (1)
    - Length: 93
    - Version: SSL 3.0 (0x0300)
    - Random: 42dbf0c21b781c6c644b84fe4efa7be6ef21efc98e350355e90695001e79031c
    - Session ID Length: 32
    - Session ID: 1bad05faba02ea92c64c54be4547c32f3e3ca63d3a0c86ddad694b45682da22f

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?

- ✓ Cipher Specs (17 specs)
  - Cipher Spec: TLS\_RSA\_WITH\_RC4\_128\_MD5 (0x000004)
  - Cipher Spec: TLS\_RSA\_WITH\_RC4\_128\_SHA (0x000005)
  - Cipher Spec: TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (0x00000a)
  - Cipher Spec: SSL2\_RC4\_128\_WITH\_MD5 (0x010080)
  - Cipher Spec: SSL2\_DES\_192\_EDE3\_CBC\_WITH\_MD5 (0x0700c0)
  - Cipher Spec: SSL2\_RC2\_128\_CBC\_WITH\_MD5 (0x030080)
  - Cipher Spec: TLS\_RSA\_WITH\_DES\_CBC\_SHA (0x000009)
  - Cipher Spec: SSL2\_DES\_64\_CBC\_WITH\_MD5 (0x060040)
  - Cipher Spec: TLS\_RSA\_EXPORT1024\_WITH\_RC4\_56\_SHA (0x000064)
  - Cipher Spec: TLS\_RSA\_EXPORT1024\_WITH\_DES\_CBC\_SHA (0x000062)
  - Cipher Spec: TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 (0x000003)
  - Cipher Spec: TLS\_RSA\_EXPORT\_WITH\_RC2\_CBC\_40\_MD5 (0x000006)
  - Cipher Spec: SSL2\_RC4\_128\_EXPORT40\_WITH\_MD5 (0x020080)
  - Cipher Spec: SSL2\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5 (0x040080)
  - Cipher Spec: TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA (0x000013)
  - Cipher Spec: TLS\_DHE\_DSS\_WITH\_DES\_CBC\_SHA (0x000012)
  - Cipher Spec: TLS\_DHE\_DSS\_EXPORT1024\_WITH\_DES\_CBC\_SHA (0x000063)
- Challenge

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?



|     |           |                |                |
|-----|-----------|----------------|----------------|
| 106 | 21.805705 | 128.238.38.162 | 216.75.194.220 |
| 108 | 21.830201 | 216.75.194.220 | 128.238.38.162 |
| 111 | 21.853520 | 216.75.194.220 | 128.238.38.162 |
| 112 | 21.876168 | 128.238.38.162 | 216.75.194.220 |
| 113 | 21.945667 | 216.75.194.220 | 128.238.38.162 |
| 114 | 21.954189 | 128.238.38.162 | 216.75.194.220 |
| 122 | 23.480352 | 216.75.194.220 | 128.238.38.162 |
| 149 | 23.559497 | 216.75.194.220 | 128.238.38.162 |
| 158 | 23.560866 | 216.75.194.220 | 128.238.38.162 |
| 163 | 23.566451 | 128.238.38.162 | 216.75.194.220 |
| 165 | 23.586650 | 216.75.194.220 | 128.238.38.162 |
| 169 | 23.591500 | 216.75.194.220 | 128.238.38.162 |

- SSLv3 Record Layer: Handshake Protocol: Server Hello
  - Content Type: Handshake (22)
  - Version: SSL 3.0 (0x0300)
  - Length: 74
  - Handshake Protocol: Server Hello
    - Handshake Type: Server Hello (2)
    - Length: 70
    - Version: SSL 3.0 (0x0300)
    - Random: 0000000042dbed248b8831d04cc98c26e5badc4e267c391944f0f070ece57745
    - Session ID Length: 32
    - Session ID: 1bad05faba02ea92c64c54be4547c32f3e3ca63d3a0c86ddad694b45682da22f
    - Cipher Suite: TLS\_RSA\_WITH\_RC4\_128\_MD5 (0x0004)
    - Compression Method: null (0)

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 中客户端和服务端随机数用来干什么？

|     |           |                |                |       |   |
|-----|-----------|----------------|----------------|-------|---|
| 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 Spec, Encrypted Handshake  |
| 113 | 21.945667 | 216.75.194.220 | 128.238.38.162 | SSLV3 | 121 Change Cipher Spec, Encrypted Handshake Message               |
| 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 | 222 Application Data  |
| 149 | 23.559497 | 216.75.194.220 | 128.238.38.162 | SSLV3 | 1367 Application Data   |
| 158 | 23.560866 | 216.75.194.220 | 128.238.38.162 | SSLV3 | 1367 Application Data   |
| 163 | 23.566451 | 128.238.38.162 | 216.75.194.220 | SSLV3 | 156 Client Hello  |
| 165 | 23.586650 | 216.75.194.220 | 128.238.38.162 | SSLV3 | 1329 Application Data   |
| 169 | 23.591500 | 216.75.194.220 | 128.238.38.162 | SSLV3 | 200 Server Hello, Change Cipher Spec, Encrypted Handshake Message |
| 171 | 23.599417 | 128.238.38.162 | 216.75.194.220 | SSLV3 | 121 Change Cipher Spec, Encrypted Handshake Message               |
| 172 | 23.602696 | 128.238.38.162 | 216.75.194.220 | SSLV3 | 470 Application Data  |
| 176 | 23.621694 | 128.238.38.162 | 216.75.194.220 | SSLV3 | 156 Client Hello  |

|   |  |      |   |                   |
|---|--|------|---|-------------------|
| > Ethernet II, Src: Cisco 83:e4:54 (00:b0:b0:83:e4:54), Dst: IBM 10:60:99 (00:09:6b:10:60:99) |  | 0040 | 00 00 00 00 00 42 db ed 24 0b 80 31 d0 4c c0 8c | .....->..         |
| > Internet Protocol Version 4, Src: 216.75.194.220, Dst: 128.238.38.162                       |  | 0050 | 20 05 ba dc 4e 26 7c 39 19 44 f0 f0 70 ec e5 77 | ...b&19 .0:~p..   |
| > Transmission Control Protocol, Src Port: 443, Dst Port: 2271, Seq: 1, Ack: 79, Len: 1380    |  | 0060 | 45 20 1b ad 05 fa ba 02 ea 92 c6 4c 54 be 45 47 | .....-LT.E        |
| > Transport Layer Security  |  | 0070 | c3 2f 3e 3c a6 3d 3a 0c 86 dd ad 69 4b 45 68 2d | .....iKEh         |
| SSLv3 Record Layer: Handshake Protocol: Server Hello  |  | 0080 | a2 2f 00 04 00 16 03 00 0a 83 0b 00 0a 7f 00 0a | .....             |
| Content Type: Handshake (22)  |  | 0090 | 7c 00 05 48 30 82 05 44 30 82 04 2c a0 03 02 01 | ..H0-D 0:~...     |
| Version: SSL 3.0 (0x0300)   |  | 00a0 | 02 02 10 66 a5 0f 16 30 de 47 94 9e 62 be 44 31 | ...f...0 ....b-D  |
| Length: 74  |  | 00b0 | 64 f4 a1 30 0d 06 09 2a 86 48 86 f7 0d 01 01 05 | d-0-...* ..H-U... |
| Handshake Protocol: Server Hello  |  | 00c0 | 05 00 30 81 dc 31 0b 30 09 06 03 55 04 06 13 02 | -0-0-1-0 ...U-... |
| Handshake Type: Server Hello (2)  |  | 00d0 | 47 42 31 17 30 15 06 03 55 04 0a 13 0e 43 6f 6d | GB1-0-...U-...Co  |
| Version: SSL 3.0 (0x0300)   |  | 00e0 | 6f 64 6f 20 4c 69 6d 69 74 65 64 31 1d 30 1b 06 | odo Limi ted1-0-  |
| Length: 70  |  | 00f0 | 03 55 04 0b 13 14 43 6f 6d 6f 64 6f 20 54 72 75 | -U-...Co modo Tr  |
| Random: 0000000042dbed248b8831d04cc98c26e5badc4e267c391944f0f070ece57745                      |  | 0100 | 73 74 20 4e 65 74 77 6f 72 db 31 46 30 44 06 03 | st Netwo rkiF00-  |
| Session ID Length: 32   |  | 0110 | 55 04 0b 13 3d 54 65 72 6d 73 20 61 6e 64 20 43 | U-...Ter ms and   |
| Session ID: 1bad05faba02ea92c64c54be4547c32f3e3ca63d3a0c86ddad694b45682da22f                  |  | 0120 | 6f 6e 64 69 74 69 6f 6e 73 20 6f 66 20 75 73 65 | ondition s of us  |
| Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)   |  | 0130 | 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 63 6f 6d | : http://www.co   |
| Compression Method: null (0)  |  | 0140 | 6f 64 6f 2e 6e 65 74 2f 72 65 70 6f 73 69 74 6f | odo.net/ reposi   |
| [JA3S Fullstring: 768,4]  |  | 0150 | 72 79 31 1f 30 1d 06 03 55 64 0b 13 16 28 63 29 | ry1-0-...U-...[c  |
| [JA3C: 1f8f5a3d3fd43ca36a8a4d8a0a0c3a3fd1]  |  | 0160 | 32 30 30 32 20 43 6f 6d 6f 64 6f 20 4c 69 6d 69 | 2002 Com odo Lim  |
|   |  | 0170 | 74 65 64 31 2c 30 2a 06 03 55 04 03 13 23 43 6f | ted1,0*-...U-...c |

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

能够多次随机数生成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？

|     |           |                |                |       |  |
|-----|-----------|----------------|----------------|-------|--|
| 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                  |
| 158 | 23.560866 | 216.75.194.220 | 128.238.38.162 | SSLV3 | 1367 Application Data                  |

> Frame 108: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits)  
> Ethernet II, Src: Cisco\_83:e4:54 (00:b0:8e:83:e4:54), Dst: IBM\_10:60:99 (00:09:6b:10:60:99)  
> Internet Protocol Version 4, Src: 216.75.194.220, Dst: 128.238.38.162  
> Transmission Control Protocol, Src Port: 443, Dst Port: 2271, Seq: 1, Ack: 79, Len: 1380  
▼ Transport Layer Security  
    ▼ SSLV3 Record Layer: Handshake Protocol: Server Hello  
        Content Type: Handshake (22)  
        Version: SSL 3.0 (0x0300)  
        Length: 74  
        ▼ Handshake Protocol: Server Hello  
            Handshake Type: Server Hello (2)  
            Length: 70  
            Version: SSL 3.0 (0x0300)  
            > Random: 000000042dbed248b8831d04cc98c26e5badc4e267c391944f0f70ece57745  
                Session ID Length: 32  
                Session ID: 1bad05fab02ea92c64c54be4547c32f3e3ca63d3a0c86ddad694b45682da22f  
                Cipher Suite: TLS\_RSA\_WITH\_RC4\_128\_MD5 (0x0004)  
                Compression Method: null (0)

0060 45 26 1b ad 05 fa ba 02 ea 92 c6 4c 54  
0070 c3 2f 3e 3c a6 3d 3a 0c 86 dd ad 69 4b  
0080 a2 2f 00 04 00 16 03 00 0a 83 0b 00 0a  
0090 7c 00 05 48 30 82 05 44 30 82 04 2c a0  
00a0 02 02 10 66 a5 0f 16 30 de d7 94 9e 62  
00b0 64 f4 a1 30 0d 06 09 2a 86 48 86 f7 0d  
00c0 05 00 30 81 dc 31 0b 30 09 06 03 55 04  
00d0 47 42 31 17 30 15 06 03 55 04 0a 13 0e  
00e0 6f 64 6f 20 4c 69 6d 69 74 65 64 31 1d  
00f0 03 55 04 0b 13 14 43 6f 6d 6f 64 6f 20  
0100 73 74 20 4e 65 74 77 6f 72 6b 31 46 30  
0110 55 04 0b 13 3d 54 65 72 6d 73 20 61 6e  
0120 6f 6e 64 69 74 69 6f 6e 73 20 6f 66 20  
0130 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e  
0140 6f 64 6f 2e 6e 65 74 2f 72 65 70 6f 73  
0150 72 79 31 1f 30 1d 06 03 55 04 0b 13 16  
0160 32 30 30 32 20 43 6f 6d 6f 64 6f 20 4c  
0170 74 65 64 31 2c 30 2a 06 03 55 04 03 13  
0180 6d 6f 64 6f 20 43 6c 61 73 73 20 33 20  
0190 75 72 69 74 70 20 53 65 72 76 69 63 65

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？

|     |           |                |                |       |  |
|-----|-----------|----------------|----------------|-------|--|
| 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                  |
| 158 | 23.560866 | 216.75.194.220 | 128.238.38.162 | SSLV3 | 1367 Application Data                  |

> Frame 111: 790 bytes on wire (6320 bits), 790 bytes captured (6320 bits)  
> Ethernet II, Src: Cisco\_83:e4:54 (00:b0:8e:83:e4:54), Dst: IBM\_10:60:99 (00:09:6b:10:60:99)  
> Internet Protocol Version 4, Src: 216.75.194.220, Dst: 128.238.38.162  
> Transmission Control Protocol, Src Port: 443, Dst Port: 2271, Seq: 2049, Ack: 79, Len: 736  
> [3 Reassembled TCP Segments (2696 bytes): #108(1301), #109(668), #111(727)]  
▼ Transport Layer Security  
    ▼ SSLV3 Record Layer: Handshake Protocol: Certificate  
        Content Type: Handshake (22)  
        Version: SSL 3.0 (0x0300)  
        Length: 2691  
        ▼ Handshake Protocol: Certificate  
            Handshake Type: Certificate (11)  
            Length: 2687  
            Certificates Length: 2684  
            Certificates (2684 bytes)

0000 00 09 6b 10 60 99 00 b0 8e 83 e4 54 08  
0010 03 08 87 c0 40 00 33 06 7a 77 d8 4b c2  
0020 26 a2 01 bb 08 df 4c 9e 6c 9f 56 d2 09  
0030 81 60 a6 5e 00 00 90 4c 4d 4c ec f5 88  
0040 d0 2f ff 79 90 01 d8 51 64 e7 2f b1 08  
0050 ad fa b2 80 96 ab ac 8b b5 4c b4 74 c2  
0060 e8 23 31 f4 2a b9 61 1b bd ce a4 5b 31  
0070 9c 9c fb b2 0f d7 c5 3b bf cc 5a ab 0f  
0080 89 22 a6 90 20 d3 b3 6c be 12 f3 e3 24  
0090 ae 43 5a da 16 76 e8 1f 02 03 01 00 0f  
00a0 d9 30 82 01 d5 30 45 06 03 55 1d 1f 04  
00b0 30 3a a0 38 a0 36 86 34 68 74 74 70 34  
00c0 77 77 2e 70 75 62 6c 69 63 2d 74 72 75  
00d0 63 6f 6d 2f 63 67 69 2d 62 69 6e 2f 43  
00e0 32 30 31 38 2f 63 64 70 2e 63 72 6c 34  
00f0 55 1d 0e 04 16 04 14 36 e0 e8 7c 6d 94  
0100 99 e5 42 76 4d 70 b3 50 30 ac 5e 30 83

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？



|     |           |                |                |       |  |
|-----|-----------|----------------|----------------|-------|--|
| 112 | 21.876168 | 128.238.38.162 | 216.75.194.220 | SSLV3 | 258 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message |
| 113 | 21.945667 | 216.75.194.220 | 128.238.38.162 | SSLV3 | 121 Change Cipher Spec, Encrypted Handshake Message                      |
| 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 | 23.559407 | 216.75.194.220 | 128.238.38.162 | SSLV3 | 1367 Application Data  |
| 158 | 23.560866 | 216.75.194.220 | 128.238.38.162 | SSLV3 | 1367 Application Data  |

|  |  |  |  |  |   |
|--|--|--|--|--|---|
| > Frame 112: 258 bytes on wire (2064 bits), 258 bytes captured (2064 bits) on interface 0<br>> Ethernet II, Src: IDN 10:60:99 (00:09:6b:10:60:99), Dst: All-MSRP-routers_00 (00:00:0c:07:ac:00)<br>> Internet Protocol Version 4, Src: 128.238.38.162, Dst: 216.75.194.220<br>> Transmission Control Protocol, Src Port: 2271, Dst Port: 443, Seq: 79, Ack: 2785, Len: 204<br>> Transport Layer Security<br>> SSLv3 Record Layer: Handshake Protocol: Client Key Exchange<br>Content Type: Handshake (22)<br>Version: SSL 3.0 (0x0300)<br>Length: 132<br>> Handshake Protocol: Client Key Exchange<br>Handshake Type: Client Key Exchange (16)<br>Length: 128<br>> RSA Encrypted PreMaster Secret<br>Encrypted PreMaster: bc49494729aa2590477fd059056ae78956c77b12af08b47c609e61f104b0fbf83e41c08d...<br>> SSLv3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec<br>Content Type: Change Cipher Spec (20)<br>Version: SSL 3.0 (0x0300)<br>Length: 1<br>Change Cipher Spec Message<br>> SSLv3 Record Layer: Handshake Protocol: Encrypted Handshake Message<br>Content Type: Handshake (22)<br>Version: SSL 3.0 (0x0300)<br>Length: 56<br>Handshake Protocol: Encrypted Handshake Message |  |  |  |  | 0000 00 00 0c 07 ac 00 00 00 6b 10 60 99 08 00 45 00 .....k...<br>0010 00 f4 48 2c 40 00 80 06 6f 1f 80 ee 26 a2 d8 4b ...H...<br>0020 c2 dc 08 df 01 bb 56 d2 09 13 4c 9e 6f 7f 50 18 .....V...<br>0030 fd 1f c2 d9 00 00 16 03 00 00 84 10 00 00 80 bc .....<br>0040 49 49 47 29 aa 25 90 47 7f d0 59 05 6a e7 89 56 IIG)%-G...<br>0050 c7 7b 12 af 08 b4 7c 60 9e 61 f1 04 b0 fb f8 3e {...}...<br>0060 41 c0 8d c9 10 93 9c ad 1e ce 82 e0 dd e2 50 b9 A...<br>0070 9b 4b 51 c7 3f bd ee cd 92 c4 27 5d ff dd fb 95 ...KQ?...<br>0080 42 3d a4 b7 71 ee c0 ff c3 ce b2 ed 60 90 6c d7 B...q...<br>0090 04 6e 5a 00 98 2e 52 ee b5 bc d1 c4 f5 63 f0 e3 -nZ...R...<br>00a0 44 29 f1 c6 ba 64 58 79 46 9e 3e c4 fd d7 9b 7a D)...dx F-><br>00b0 02 04 00 32 f6 1d 7a a1 2d cf d2 1a 18 64 29 14 ...2...Z...<br>00c0 03 00 00 01 01 16 03 00 00 38 29 a9 dc 11 5a 74 .....8)<br>00d0 7a 41 48 15 4f 50 4b e2 df 0c d0 5b c4 44 a8 e8 ZAH-OPK...<br>00e0 e4 e5 12 b9 11 f6 b3 9a de b7 22 0d 3a 17 9a 83 ...KQ?...<br>00f0 77 1c de ab f2 a1 e7 2e ad d5 1c 5b a2 0d ab e4 W...A...<br>0100 27 03 ..... |
|--|--|--|--|--|---|

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

|     |           |                |                |       |  |
|-----|-----------|----------------|----------------|-------|--|
| 111 | 21.876168 | 128.238.38.162 | 216.75.194.220 | SSLV3 | 258 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message |
| 112 | 21.876168 | 128.238.38.162 | 216.75.194.220 | SSLV3 | 121 Change Cipher Spec, Encrypted Handshake Message                      |
| 113 | 21.945667 | 216.75.194.220 | 128.238.38.162 | SSLV3 | 806 Application Data   |
| 114 | 21.954189 | 128.238.38.162 | 216.75.194.220 | SSLV3 | 272 Application Data   |
| 122 | 23.480352 | 216.75.194.220 | 128.238.38.162 | SSLV3 | 1367 Application Data  |
| 149 | 23.559407 | 216.75.194.220 | 128.238.38.162 | SSLV3 | 1367 Application Data  |
| 158 | 23.560866 | 216.75.194.220 | 128.238.38.162 | SSLV3 | 156 Client Hello   |
| 163 | 23.566451 | 128.238.38.162 | 216.75.194.220 | SSLV3 | 1329 Application Data  |
| 165 | 23.586650 | 216.75.194.220 | 128.238.38.162 | SSLV3 | 200 Server Hello, Change Cipher Spec, Encrypted Handshake Message        |
| 169 | 23.591590 | 216.75.194.220 | 128.238.38.162 | SSLV3 | 121 Change Cipher Spec, Encrypted Handshake Message                      |
| 171 | 23.599417 | 128.238.38.162 | 216.75.194.220 | SSLV3 | 470 Application Data   |
| 172 | 23.602696 | 128.238.38.162 | 216.75.194.220 | SSLV3 | 156 Client Hello   |
| 176 | 23.621694 | 128.238.38.162 | 216.75.194.220 | SSLV3 | 378 Application Data   |
| 178 | 23.627217 | 216.75.194.220 | 128.238.38.162 | SSLV3 | 200 Server Hello, Change Cipher Spec, Encrypted Handshake Message        |
| 184 | 23.646644 | 216.75.194.220 | 128.238.38.162 | SSLV3 | 121 Change Cipher Spec, Encrypted Handshake Message                      |
| 188 | 23.662642 | 128.238.38.162 | 216.75.194.220 | SSLV3 |  |

|  |  |  |  |  |   |
|--|--|--|--|--|---|
| Length: 132<br>> Handshake Protocol: Client Key Exchange<br>Handshake Type: Client Key Exchange (16)<br>Length: 128<br>> RSA Encrypted PreMaster Secret<br>Encrypted PreMaster: bc49494729aa2590477fd059056ae78956c77b12af08b47c609e61f104b0fbf83e41c08d...<br>> SSLv3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec<br>Content Type: Change Cipher Spec (20)<br>Version: SSL 3.0 (0x0300)<br>Length: 1<br>Change Cipher Spec Message<br>> SSLv3 Record Layer: Handshake Protocol: Encrypted Handshake Message<br>Content Type: Handshake (22)<br>Version: SSL 3.0 (0x0300)<br>Length: 56<br>Handshake Protocol: Encrypted Handshake Message |  |  |  |  | 0000 00 00 0c 07 ac 00 00 00 6b 10 60 99 08 00 45 00 .....k...<br>0010 00 f4 48 2c 40 00 80 06 6f 1f 80 ee 26 a2 d8 4b ...H...<br>0020 c2 dc 08 df 01 bb 56 d2 09 13 4c 9e 6f 7f 50 18 .....V...<br>0030 fd 1f c2 d9 00 00 16 03 00 00 84 10 00 00 80 bc .....<br>0040 49 49 47 29 aa 25 90 47 7f d0 59 05 6a e7 89 56 IIG)%-G...<br>0050 c7 7b 12 af 08 b4 7c 60 9e 61 f1 04 b0 fb f8 3e {...}...<br>0060 41 c0 8d c9 10 93 9c ad 1e ce 82 e0 dd e2 50 b9 A...<br>0070 9b 4b 51 c7 3f bd ee cd 92 c4 27 5d ff dd fb 95 ...KQ?...<br>0080 42 3d a4 b7 71 ee c0 ff c3 ce b2 ed 60 90 6c d7 B...q...<br>0090 04 6e 5a 00 98 2e 52 ee b5 bc d1 c4 f5 63 f0 e3 -nZ...R...<br>00a0 44 29 f1 c6 ba 64 58 79 46 9e 3e c4 fd d7 9b 7a D)...dx F-><br>00b0 02 04 00 32 f6 1d 7a a1 2d cf d2 1a 18 64 29 14 ...2...Z...<br>00c0 03 00 00 01 01 16 03 00 00 38 29 a9 dc 11 5a 74 .....8)<br>00d0 7a 41 48 15 4f 50 4b e2 df 0c d0 5b c4 44 a8 e8 ZAH-OPK...<br>00e0 e4 e5 12 b9 11 f6 b3 9a de b7 22 0d 3a 17 9a 83 ...KQ?...<br>00f0 77 1c de ab f2 a1 e7 2e ad d5 1c 5b a2 0d ab e4 W...A...<br>0100 27 03 ..... |
|--|--|--|--|--|---|

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？

|     |           |                |                |       |   |
|-----|-----------|----------------|----------------|-------|---|
| 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   |
| 158 | 23.560866 | 216.75.194.220 | 128.238.38.162 | SSLv3 | 1367 Application Data   |
| 163 | 23.566451 | 128.238.38.162 | 216.75.194.220 | SSLv3 | 156 Client Hello  |
| 165 | 23.586650 | 216.75.194.220 | 128.238.38.162 | SSLv3 | 1329 Application Data   |
| 169 | 23.591590 | 216.75.194.220 | 128.238.38.162 | SSLv3 | 200 Server Hello, Change Cipher Spec, Encrypted Handshake Message |
| 171 | 23.599417 | 128.238.38.162 | 216.75.194.220 | SSLv3 | 121 Change Cipher Spec, Encrypted Handshake Message               |
| 172 | 23.602696 | 128.238.38.162 | 216.75.194.220 | SSLv3 | 470 Application Data  |
| 176 | 23.621694 | 128.238.38.162 | 216.75.194.220 | SSLv3 | 156 Client Hello  |
| 178 | 23.627217 | 216.75.194.220 | 128.238.38.162 | SSLv3 | 378 Application Data  |
| 184 | 23.646644 | 216.75.194.220 | 128.238.38.162 | SSLv3 | 200 Server Hello, Change Cipher Spec, Encrypted Handshake Message |
| 188 | 23.662642 | 128.238.38.162 | 216.75.194.220 | SSLv3 | 121 Change Cipher Spec, Encrypted Handshake Message               |

> Frame 114: 806 bytes on wire (6448 bits), 806 bytes captured (6448 bits) on interface 0

> Ethernet II, Src: Intel 82:55:08:00:00:00, Dst: All 01:00:00:00:00:00

> Internet Protocol Version 4, Src: 128.238.38.162, Dst: 216.75.194.220

> Transmission Control Protocol, Src Port: 2271, Dst Port: 443, Seq: 283, Ack: 2852, Len: 752

> Transport Layer Security

> SSLv3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol

> Content Type: Application Data (23)

> Version: SSL 3.0 (0x0300)

> Length: 747

> Encrypted Application Data: 7e8cdc7fe71d6d59c45ecae7bad064ec705ea592d4b2b35cfc48675c16e461e224b6f05...

[Application Data Protocol: Hypertext Transfer Protocol]

0030 f0 dc 95 12 00 00 17 03 00 02 eb 7e 8c de 7f e7

0040 1d 6d 59 c4 5a c4 67 ba d0 64 ec 70 5e a5 92 d0

0050 08 2b 35 cf c4 86 75 c1 6e 46 1c 22 4b 6f 95 8b

0060 4b 36 5c d9 22 fa ed d6 d8 bd 5c a0 d9 6f f0 bd

0070 3d 35 04 3e 83 ad 49 54 0b bb 03 5d 32 e5 b3 ba

0080 46 30 61 07 c7 f4 d2 9d 5a 90 b7 7e 7f c2 f5 e7

0090 11 60 b9 fd f7 15 f3 2d 9d 77 51 50 03 c5 c5 11

00a0 13 09 bc 19 bf 44 16 3b 41 e1 a4 25 54 17 c1 6e

00b0 a7 7e 08 ca f8 86 c7 de 45 a2 aa b3 5a ca ed a9

00c0 e5 b2 e8 d2 d2 62 07 db bd 5a b6 9a 5b 40 d0 e5

00d0 08 52 ad bb f6 e5 33 93 e5 54 85 68 41 5d 2d 0e

00e0 ee 9a 5b 6e fc 0a 93 8c b7 5d a8 9c ea ee 03 95

00f0 2f a8 a0 77 21 3e 76 c2 95 61 5e c2 6c dd a8 32

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。