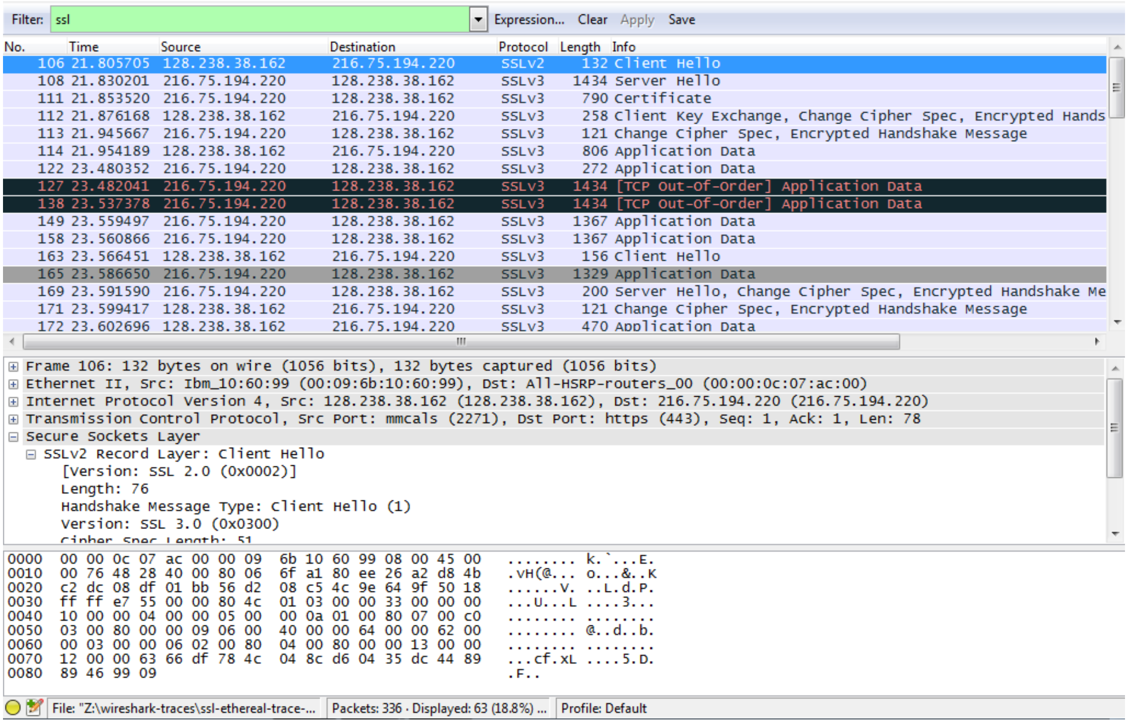
Lab 7

1. For each of the first 8 Ethernet frames, specify the source of the frame (client or server), determine the number of SSL records that are included in the frame, and list the SSL record types that are included in the frame. Draw a timing diagram between client and server, with one arrow for each SSL record.

Answer



```
No.   Time       Source          Destination     Protocol Length Info
  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
  112 21.876168  128.238.38.162  216.75.194.220  SSLv3     258 Client Key Exchange, Change Cipher Spec, Encrypted Hands
  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
  127 23.482041  216.75.194.220  128.238.38.162  SSLv3    1434 [TCP Out-Of-Order] Application Data
  138 23.537378  216.75.194.220  128.238.38.162  SSLv3    1434 [TCP Out-Of-Order] 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 Me
  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
```

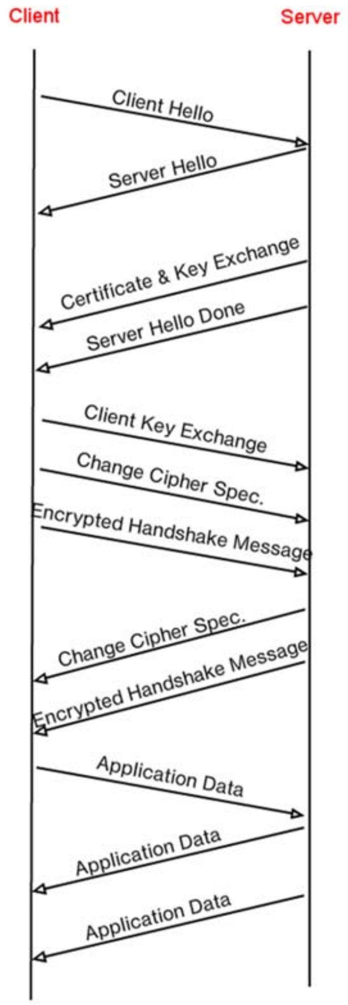
```
⊞ Frame 106: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits)
⊞ Ethernet II, Src: Ibm_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
⊞ Internet Protocol Version 4, Src: 128.238.38.162 (128.238.38.162), Dst: 216.75.194.220 (216.75.194.220)
⊞ Transmission Control Protocol, Src Port: mmcals (2271), Dst Port: https (443), Seq: 1, Ack: 1, Len: 78
⊟ Secure Sockets Layer
  ⊟ SSLv2 Record Layer: Client Hello
      [Version: SSL 2.0 (0x0002)]
      Length: 76
      Handshake Message Type: Client Hello (1)
      Version: SSL 3.0 (0x0300)
      Cipher Spec Length: 51
```

```
0000  00 00 0c 07 ac 00 00 09  6b 10 60 99 08 00 45 00   ........ k.`...E.
0010  00 76 48 28 40 00 80 06  6f a1 80 ee 26 a2 d8 4b   .vH(@... o...&..K
0020  c2 dc 08 df 01 bb 56 d2  08 c5 4c 9e 64 9f 50 18   ......V. ..L.d.P.
0030  ff ff e7 55 00 00 80 4c  01 03 00 00 33 00 00 00   ...U...L ....3...
0040  10 00 00 04 00 00 05 00  00 0a 01 00 80 07 00 c0   ........ ........
0050  03 00 80 00 00 09 06 00  40 00 00 64 00 00 62 00   ........ @..d..b.
0060  00 03 00 00 06 02 00 80  04 00 80 00 00 13 00 00   ........ ........
0070  12 00 00 63 66 df 78 4c  04 8c d6 04 35 dc 44 89   ...cf.xL ....5.D.
0080  89 46 99 09                                        .F..
```

File: "Z:\wireshark-traces\ssl-ethereal-trace-... Packets: 336 · Displayed: 63 (18.8%) ... Profile: Default

Figure 1

No.	Frame	Source	Destination	SSL Count	SSL Type
1	106	128.238.38.162	216.75.194.220	1	Client Hello
2	108	216.75.194.220	128.238.38.162	1	Server Hello
3	111	216.75.194.220	128.238.38.162	2	Server Hello Done
4	112	128.238.38.162	216.75.194.220	3	Client Key Exchange
5	113	216.75.194.220	128.238.38.162	2	Change Cipher Spec
6	114	128.238.38.162	216.75.194.220	1	Application Data
7	122	216.75.194.220	128.238.38.162	1	Application Data
8	127	216.75.194.220	128.238.38.162	1	Application Data



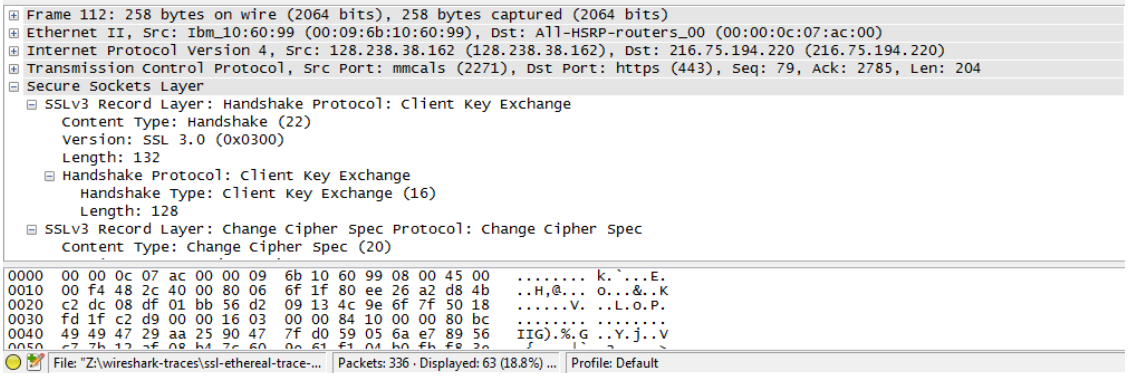
2. Each of the SSL records begins with the same three fields (with possibly different values). One of these fields is "content type" and has length of one byte. List all three fields and their lengths.

Answer

Content Type = 1 byte

Version = 2 bytes

Length = 2 bytes



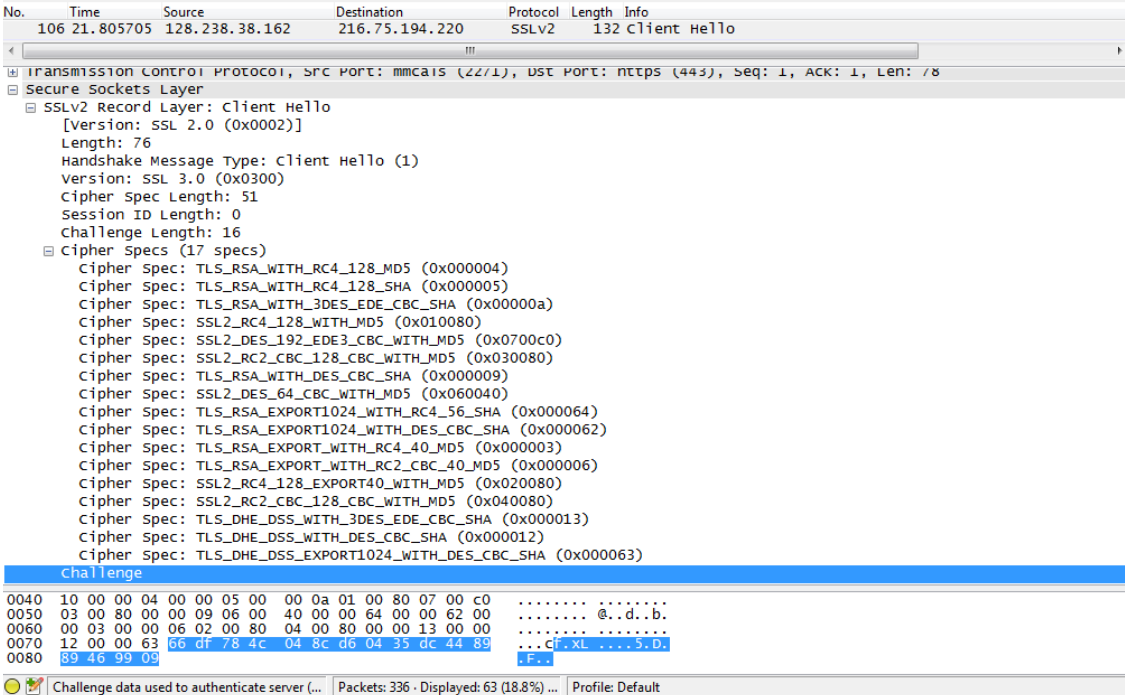
```
⊞ Frame 112: 258 bytes on wire (2064 bits), 258 bytes captured (2064 bits)
⊞ Ethernet II, Src: Ibm_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
⊞ Internet Protocol Version 4, Src: 128.238.38.162 (128.238.38.162), Dst: 216.75.194.220 (216.75.194.220)
⊞ Transmission Control Protocol, Src Port: mmcals (2271), Dst Port: https (443), Seq: 79, Ack: 2785, Len: 204
⊟ Secure Sockets Layer
  ⊟ SSLv3 Record Layer: Handshake Protocol: Client Key Exchange
      Content Type: Handshake (22)
      Version: SSL 3.0 (0x0300)
      Length: 132
    ⊟ Handshake Protocol: Client Key Exchange
        Handshake Type: Client Key Exchange (16)
        Length: 128
  ⊟ SSLv3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)

0000  00 00 0c 07 ac 00 00 09  6b 10 60 99 08 00 45 00   ........ k.`...E.
0010  00 f4 48 2c 40 00 80 06  6f 1f 80 ee 26 a2 d8 4b   ..H,@... o...&..K
0020  c2 dc 08 df 01 bb 56 d2  09 13 4c 9e 6f 7f 50 18   ......V. ..L.o.P.
0030  fd 1f c2 d9 00 00 16 03  00 00 84 10 00 00 80 bc   ........ ........
0040  49 49 47 29 aa 25 90 47  7f d0 59 05 6a e7 89 56   IIG).%.G ..Y.j..V
```

File: "Z:\wireshark-traces\ssl-ethereal-trace-... | Packets: 336 · Displayed: 63 (18.8%) ... | Profile: Default

3. Expand the ClientHello record. (If your trace contains multiple ClientHello records, expand the frame that contains the first one.) What is the value of the content type?

Answer



```
No.     Time        Source           Destination      Protocol Length Info
    106 21.805705   128.238.38.162   216.75.194.220   SSLv2       132 Client Hello

⊞ Transmission Control Protocol, Src Port: mmcals (2271), Dst Port: https (443), Seq: 1, Ack: 1, Len: 78
⊟ Secure Sockets Layer
  ⊟ SSLv2 Record Layer: Client Hello
      [Version: SSL 2.0 (0x0002)]
      Length: 76
      Handshake Message Type: Client Hello (1)
      Version: SSL 3.0 (0x0300)
      Cipher Spec Length: 51
      Session ID Length: 0
      Challenge Length: 16
    ⊟ 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_CBC_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_CBC_128_CBC_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

0040  10 00 00 04 00 00 05 00  00 0a 01 00 80 07 00 c0   ........ ........
0050  03 00 80 00 00 09 06 00  40 00 00 64 00 00 62 00   ........ @..d..b.
0060  00 03 00 00 06 02 00 80  04 00 80 00 00 13 00 00   ........ ........
0070  12 00 00 63 66 df 78 4c  04 8c d6 04 35 dc 44 89   ...cf.xL ....5.D.
0080  89 46 99 09                                        .F..
```

Challenge data used to authenticate server (... | Packets: 336 · Displayed: 63 (18.8%) ... | Profile: Default

The content type is 22

4. Does the ClientHello record contain a nonce (also known as a “challenge”)? If so, what is the value of the challenge in hexadecimal notation?

Answer

66 df 78 4c 04 8c d6 04 35 dc 44 89 89 46 99 09

5. Does the ClientHello record advertise the cyber suites it supports? If so, in the first listed suite, what are the public-key algorithm, the symmetric-key algorithm, and the hash algorithm?

Answer

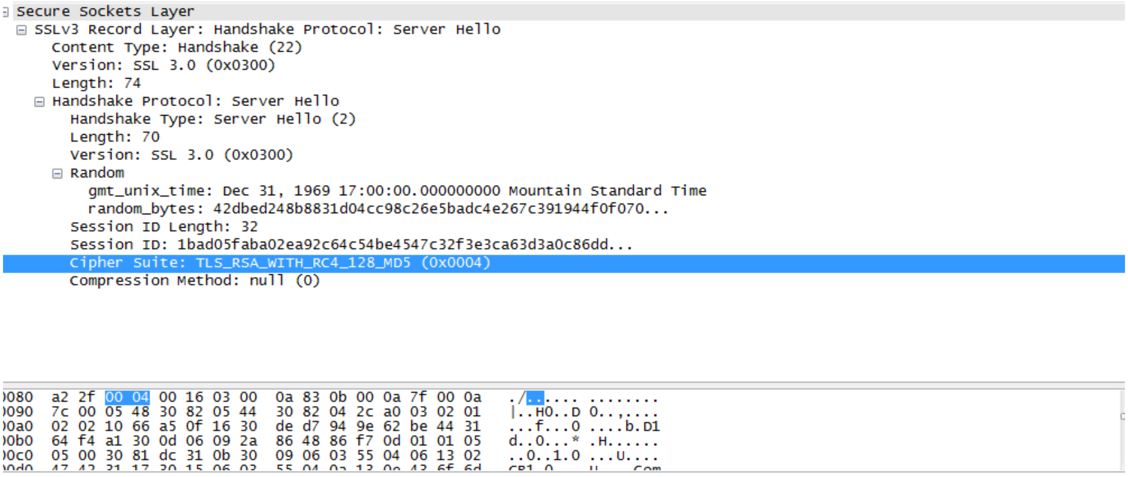
Public key algorithm: RSA

Symmetric-key algorithm: RC4

Hash algorithm: MD5

6. Locate the ServerHello SSL record. Does this record specify a chosen cipher suite? What are the algorithms in the chosen cipher suite?

Answer



```
⊟ Secure Sockets Layer
  ⊟ 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
          gmt_unix_time: Dec 31, 1969 17:00:00.000000000 Mountain Standard Time
          random_bytes: 42dbed248b8831d04cc98c26e5badc4e267c391944f0f070...
        Session ID Length: 32
        Session ID: 1bad05faba02ea92c64c54be4547c32f3e3ca63d3a0c86dd...
        Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
        Compression Method: null (0)
```

```
0080  a2 2f 00 04 00 16 03 00  0a 83 0b 00 0a 7f 00 0a   ./...... ........
0090  7c 00 05 48 30 82 05 44  30 82 04 2c a0 03 02 01   |..H0..D 0..,....
00a0  02 02 10 66 a5 0f 16 30  de d7 94 9e 62 be 44 31   ...f...0 ....b.D1
00b0  64 f4 a1 30 0d 06 09 2a  86 48 86 f7 0d 01 01 05   d..0...* .H......
00c0  05 00 30 81 dc 31 0b 30  09 06 03 55 04 06 13 02   ..0..1.0 ...U....
```

Same as above question,

Public key algorithm: RSA

Symmetric-key algorithm: RC4

Hash algorithm: MD5

7. Does this record include a nonce? If so, how long is it? What is the purpose of the client and server nonces in SSL?

Answer

Yes, it is 32 bits long (28bits data + 4 bits time), it is used for attack preventing.

8. Does this record include a session ID? What is the purpose of the session ID?

Answer

Yes, the session ID in the record is an identifier for SSL session. This ID could let the client to resume the session later by using the session ID.

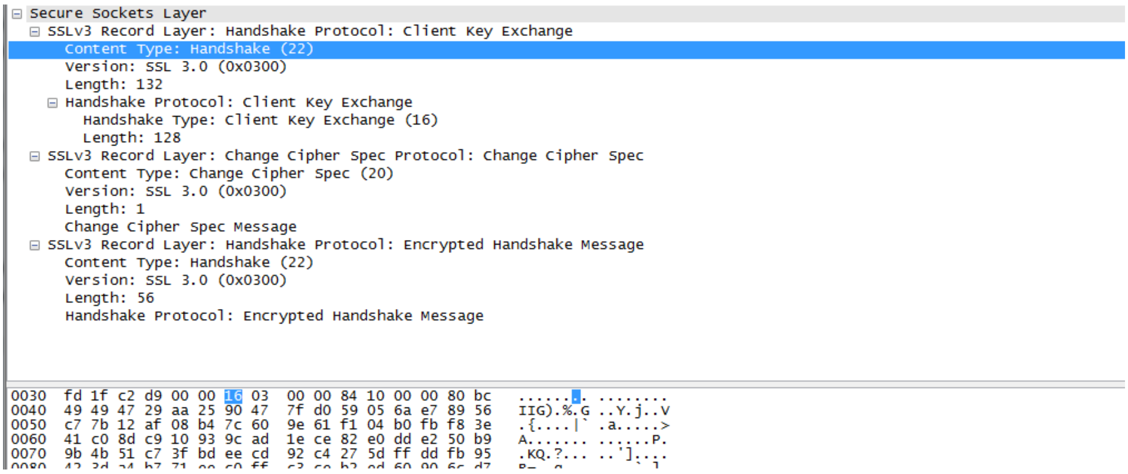
9. Does this record contain a certificate, or is the certificate included in a separate record. Does the certificate fit into a single Ethernet frame?

Answer

No, there is no certificate in this record. The certificate is in the separate record. Yes, the certificate fit into a single Ethernet frame.

10. Locate the client key exchange record. Does this record contain a pre-master secret? What is this secret used for? Is the secret encrypted? If so, how? How long is the encrypted secret?

Answer



```
⊟ Secure Sockets Layer
  ⊟ SSLv3 Record Layer: Handshake Protocol: Client Key Exchange
      Content Type: Handshake (22)
      Version: SSL 3.0 (0x0300)
      Length: 132
    ⊟ Handshake Protocol: Client Key Exchange
        Handshake Type: Client Key Exchange (16)
        Length: 128
  ⊟ 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

0030  fd 1f c2 d9 00 00 16 03  00 00 84 10 00 00 80 bc   ........ ........
0040  49 49 47 29 aa 25 90 47  7f d0 59 05 6a e7 89 56   IIG).%.G ..Y.j..V
0050  c7 7b 12 af 08 b4 7c 60  9e 61 f1 04 b0 fb f8 3e   .{....|` .a.....>
0060  41 c0 8d c9 10 93 9c ad  1e ce 82 e0 dd e2 50 b9   A....... ......P.
0070  9b 4b 51 c7 3f bd ee cd  92 c4 27 5d ff dd fb 95   .KQ.?... ..']....
```

Yes, this record contains a pre-master secret. The master secret is created using this pre-master secret. The master key is used to create session key. The secret is encrypted by public key, the encrypted secret is 120 bytes.

11. What is the purpose of the Change Cipher Spec record? How many bytes is the record in your trace?

Answer

The Change Cipher Spec record is used to indicate the content of the next SSL records will be encrypted. It is 6 bytes.

12. In the encrypted handshake record, what is being encrypted? How?

Answer

All handshake messages and MAC addresses are concatenated and encrypted. They are sent to the server.

13. Does the server also send a change cipher record and an encrypted handshake record to the client? How are those records different from those sent by the client?

Answer

Yes, the server's encrypted handshake contains all the handshake messages sent from the server. Other contains messages sent from client.

14. How is the application data being encrypted? Do the records containing application data include a MAC? Does Wireshark distinguish between the encrypted application data and the MAC?

Answer

The symmetric encryption algorithm is used to encrypt the application data. Yes, the records containing application data include a MAC. No, Wireshark did not distinguish between the encrypted application data and the MAC.

15. Comment on and explain anything else that you found interesting in the trace.

Answer

No more comment, everything as expected.