CNS LAB ESE

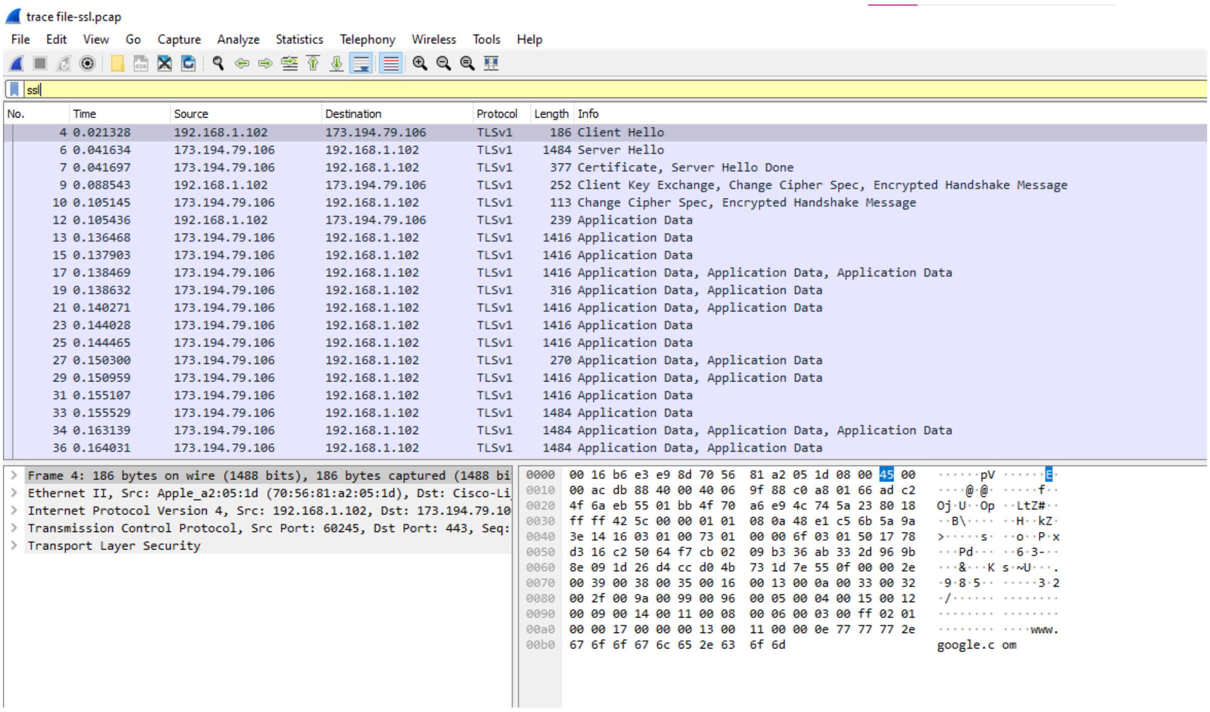
Name: Pratik Mukharu Raut

PRN: 2019BTECS00050

Title: Analyze SSL using Wireshark and answer the following

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.

-


trace file-ssl.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssl

```
No.  Time      Source          Destination     Protocol Length Info
   4 0.021328  192.168.1.102   173.194.79.106  TLSv1     186 Client Hello
   6 0.041634  173.194.79.106  192.168.1.102   TLSv1    1484 Server Hello
   7 0.041697  173.194.79.106  192.168.1.102   TLSv1     377 Certificate, Server Hello Done
   9 0.088543  192.168.1.102   173.194.79.106  TLSv1     252 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  10 0.105145  173.194.79.106  192.168.1.102   TLSv1     113 Change Cipher Spec, Encrypted Handshake Message
  12 0.105436  192.168.1.102   173.194.79.106  TLSv1     239 Application Data
  13 0.136468  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data
  15 0.137903  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data
  17 0.138469  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data, Application Data, Application Data
  19 0.138632  173.194.79.106  192.168.1.102   TLSv1     316 Application Data, Application Data
  21 0.140271  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data, Application Data
  23 0.144028  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data
  25 0.144465  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data
  27 0.150300  173.194.79.106  192.168.1.102   TLSv1     270 Application Data, Application Data
  29 0.150959  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data, Application Data
  31 0.155107  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data
  33 0.155529  173.194.79.106  192.168.1.102   TLSv1    1484 Application Data
  34 0.163139  173.194.79.106  192.168.1.102   TLSv1    1484 Application Data, Application Data, Application Data
  36 0.164031  173.194.79.106  192.168.1.102   TLSv1    1484 Application Data, Application Data
```

```
> Frame 4: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bi
> Ethernet II, Src: Apple_a2:05:1d (70:56:81:a2:05:1d), Dst: Cisco-Li
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 173.194.79.10
> Transmission Control Protocol, Src Port: 60245, Dst Port: 443, Seq:
> Transport Layer Security
```

```
0000  00 16 b6 e3 e9 8d 70 56  81 a2 05 1d 08 00 45 00   ······pV ······E·
0010  00 ac db 88 40 00 40 06  9f 88 c0 a8 01 66 ad c2   ····@·@· ·····f··
0020  4f 6a eb 55 01 bb 4f 70  a6 e9 4c 74 5a 23 80 18   Oj·U··Op ··LtZ#··
0030  ff ff 42 5c 00 00 01 01  08 0a 48 e1 c5 6b 5a 9a   ··B\···· ··H··kZ·
0040  3e 14 16 03 01 00 73 01  00 00 6f 03 01 50 17 78   >·····s· ··o··P·x
0050  d3 16 c2 50 64 f7 cb 02  09 b3 36 ab 33 2d 96 9b   ···Pd··· ··6·3-··
0060  8e 09 1d 26 d4 cc d0 4b  73 1d 7e 55 0f 00 00 2e   ···&···K s·~U···.
0070  00 39 00 38 00 35 00 16  00 13 00 0a 00 33 00 32   ·9·8·5·· ·····3·2
0080  00 2f 00 9a 00 99 00 96  00 05 00 04 00 15 00 12   ·/······ ········
0090  00 09 00 14 00 11 00 08  00 06 00 03 00 ff 02 01   ········ ········
00a0  00 00 17 00 00 00 13 00  11 00 00 0e 77 77 77 2e   ········ ····www.
00b0  67 6f 6f 67 6c 65 2e 63  6f 6d                     google.c om
```

No.	Frame	Source	Destination	SSL Count	SSL Type
1	4	192.168.1.102	173.194.79.106	1	Client Hello
2	6	173.194.73.106	192.168.1.102	1	Server Hello
3	7	173.194.79.106	192.168.1.102	2	Server Hello Done
4	9	192.168.1.102	173.194.79.106	3	Client Key Exchange
5	10	173.194.79.106	192.168.1.102	2	Change Cipher
6	12	192.168.1.102	173.194.79.106	1	App Data
7	13	173.194.79.106	192.168.1.102	1	App Data
8	15	173.194.79.106	192.168.1.102	1	App data

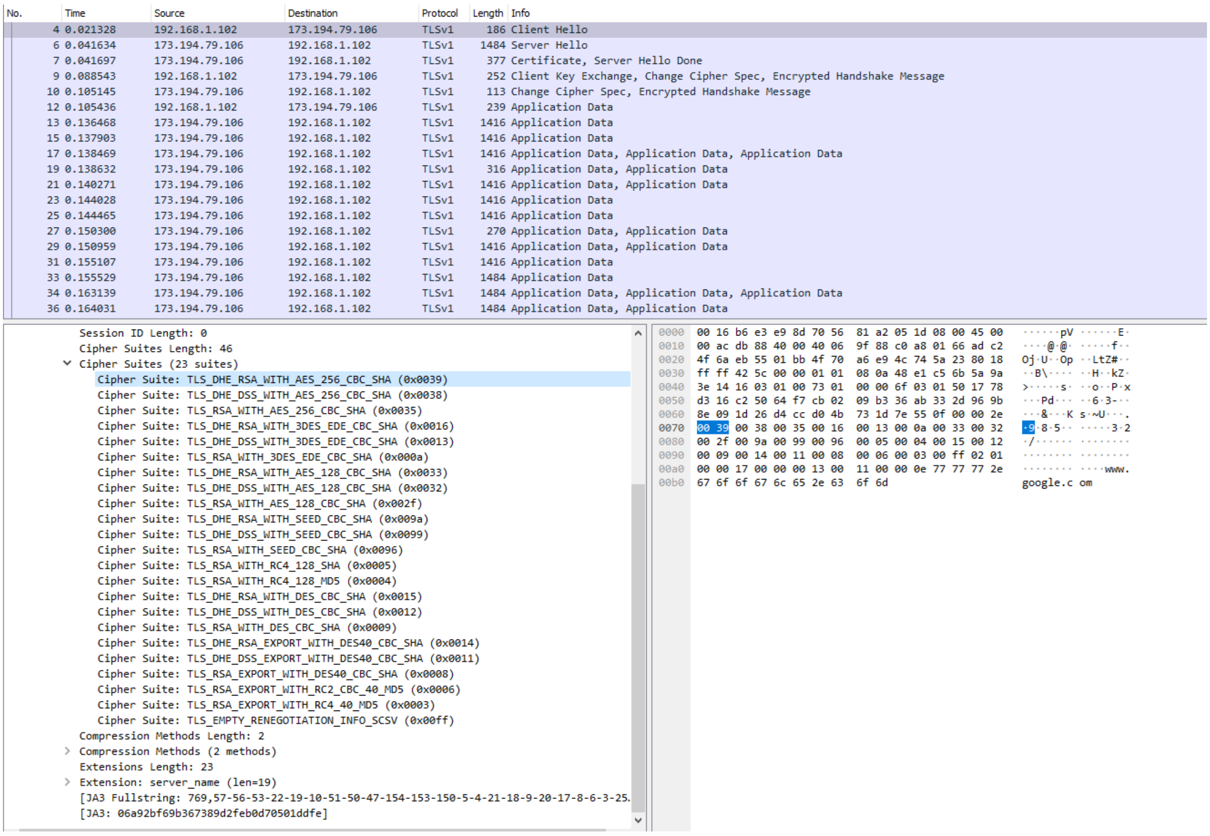
2. Each of the SSL records begins with the same three fields (with possibly different values). One of these fields is “content type” and has length of one byte. List all three fields and their lengths.

Ans:

Content Type = 1 byte

Version = 2 bytes

Length = 4 bytes



```
No.   Time      Source          Destination     Protocol Length Info
    4 0.021328  192.168.1.102   173.194.79.106  TLSv1     186 Client Hello
    6 0.041634  173.194.79.106  192.168.1.102   TLSv1    1484 Server Hello
    7 0.041697  173.194.79.106  192.168.1.102   TLSv1     377 Certificate, Server Hello Done
    9 0.088543  192.168.1.102   173.194.79.106  TLSv1     252 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
   10 0.105145  173.194.79.106  192.168.1.102   TLSv1     113 Change Cipher Spec, Encrypted Handshake Message
   12 0.105436  192.168.1.102   173.194.79.106  TLSv1     239 Application Data
   13 0.136468  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data
   15 0.137903  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data
   17 0.138469  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data, Application Data, Application Data
   19 0.138632  173.194.79.106  192.168.1.102   TLSv1     316 Application Data, Application Data
   21 0.140271  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data, Application Data
   23 0.144028  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data
   25 0.144465  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data
   27 0.150300  173.194.79.106  192.168.1.102   TLSv1     270 Application Data, Application Data
   29 0.150959  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data, Application Data
   31 0.155107  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data
   33 0.155529  173.194.79.106  192.168.1.102   TLSv1    1484 Application Data
   34 0.163139  173.194.79.106  192.168.1.102   TLSv1    1484 Application Data, Application Data, Application Data
   36 0.164031  173.194.79.106  192.168.1.102   TLSv1    1484 Application Data, Application Data
```

```
        Session ID Length: 0
        Cipher Suites Length: 46
      ⌄ Cipher Suites (23 suites)
           Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
           Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
           Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
           Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)
           Cipher Suite: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)
           Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
           Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
           Cipher Suite: TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)
           Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
           Cipher Suite: TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x009a)
           Cipher Suite: TLS_DHE_DSS_WITH_SEED_CBC_SHA (0x0099)
           Cipher Suite: TLS_RSA_WITH_SEED_CBC_SHA (0x0096)
           Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
           Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
           Cipher Suite: TLS_DHE_RSA_WITH_DES_CBC_SHA (0x0015)
           Cipher Suite: TLS_DHE_DSS_WITH_DES_CBC_SHA (0x0012)
           Cipher Suite: TLS_RSA_WITH_DES_CBC_SHA (0x0009)
           Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0x0014)
           Cipher Suite: TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA (0x0011)
           Cipher Suite: TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (0x0008)
           Cipher Suite: TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x0006)
           Cipher Suite: TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x0003)
           Cipher Suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
        Compression Methods Length: 2
      > Compression Methods (2 methods)
        Extensions Length: 23
      > Extension: server_name (len=19)
        [JA3 Fullstring: 769,57-56-53-22-19-10-51-50-47-154-153-150-5-4-21-18-9-20-17-8-6-3-25.
        [JA3: 06a92bf69b367389d2feb0d70501ddfe]
```

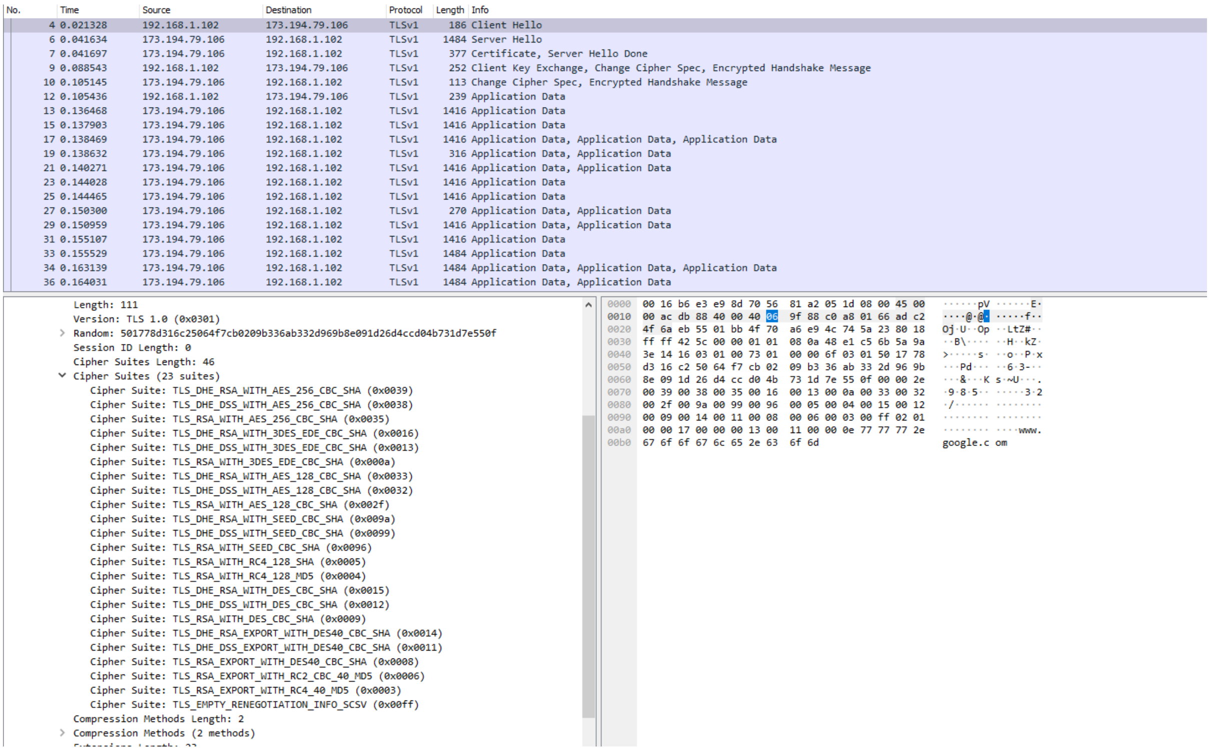
```
0000  00 16 b6 e3 e9 8d 70 56  81 a2 05 1d 08 00 45 00   ······pV ······E·
0010  00 ac db 88 40 00 40 06  9f 88 c0 a8 01 66 ad c2   ····@·@· ·····f··
0020  4f 6a eb 55 01 bb 4f 70  a6 e9 4c 74 5a 23 80 18   Oj·U··Op ··LtZ#··
0030  ff ff 42 5c 00 00 01 01  08 0a 48 e1 c5 6b 5a 9a   ··B\···· ··H··kZ·
0040  3e 14 16 03 01 00 73 01  00 00 6f 03 01 50 17 78   >·····s· ··o··P·x
0050  d3 16 c2 50 64 f7 cb 02  09 b3 36 ab 33 2d 96 9b   ···Pd··· ··6·3-··
0060  8e 09 1d 26 d4 cc d0 4b  73 1d 7e 55 0f 00 00 2e   ···&···K s·~U···.
0070  00 39 00 38 00 35 00 16  00 13 00 0a 00 33 00 32   ·9·8·5·· ·····3·2
0080  00 2f 00 9a 00 99 00 96  00 05 00 04 00 15 00 12   ·/······ ········
0090  00 09 00 14 00 11 00 08  00 06 00 03 00 ff 02 01   ········ ········
00a0  00 00 17 00 00 00 13 00  11 00 00 0e 77 77 77 2e   ········ ····www.
00b0  67 6f 6f 67 6c 65 2e 63  6f 6d                     google.c om
```

ClientHello Record

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?

Ans:

Content Type is 22



```
No.   Time      Source          Destination     Protocol Length Info
    4 0.021328  192.168.1.102   173.194.79.106  TLSv1     186 Client Hello
    6 0.041634  173.194.79.106  192.168.1.102   TLSv1    1484 Server Hello
    7 0.041697  173.194.79.106  192.168.1.102   TLSv1     377 Certificate, Server Hello Done
    9 0.088543  192.168.1.102   173.194.79.106  TLSv1     252 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
   10 0.105145  173.194.79.106  192.168.1.102   TLSv1     113 Change Cipher Spec, Encrypted Handshake Message
   12 0.105436  192.168.1.102   173.194.79.106  TLSv1     239 Application Data
   13 0.136468  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data
   15 0.137903  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data
   17 0.138469  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data, Application Data, Application Data
   19 0.138632  173.194.79.106  192.168.1.102   TLSv1     316 Application Data, Application Data
   21 0.140271  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data, Application Data
   23 0.144028  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data
   25 0.144465  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data
   27 0.150300  173.194.79.106  192.168.1.102   TLSv1     270 Application Data, Application Data
   29 0.150959  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data, Application Data
   31 0.155107  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data
   33 0.155529  173.194.79.106  192.168.1.102   TLSv1    1484 Application Data
   34 0.163139  173.194.79.106  192.168.1.102   TLSv1    1484 Application Data, Application Data, Application Data
   36 0.164031  173.194.79.106  192.168.1.102   TLSv1    1484 Application Data, Application Data
```

```
        Length: 111
        Version: TLS 1.0 (0x0301)
      > Random: 501778d316c25064f7cb0209b336ab332d969b8e091d26d4ccd04b731d7e550f
        Session ID Length: 0
        Cipher Suites Length: 46
      v Cipher Suites (23 suites)
          Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
          Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
          Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
          Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)
          Cipher Suite: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)
          Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
          Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
          Cipher Suite: TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)
          Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
          Cipher Suite: TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x009a)
          Cipher Suite: TLS_DHE_DSS_WITH_SEED_CBC_SHA (0x0099)
          Cipher Suite: TLS_RSA_WITH_SEED_CBC_SHA (0x0096)
          Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
          Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
          Cipher Suite: TLS_DHE_RSA_WITH_DES_CBC_SHA (0x0015)
          Cipher Suite: TLS_DHE_DSS_WITH_DES_CBC_SHA (0x0012)
          Cipher Suite: TLS_RSA_WITH_DES_CBC_SHA (0x0009)
          Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0x0014)
          Cipher Suite: TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA (0x0011)
          Cipher Suite: TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (0x0008)
          Cipher Suite: TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x0006)
          Cipher Suite: TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x0003)
          Cipher Suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
        Compression Methods Length: 2
      > Compression Methods (2 methods)
```

```
0000  00 16 b6 e3 e9 8d 70 56  81 a2 05 1d 08 00 45 00   ······pV ······E·
0010  00 ac db 88 40 00 40 06  9f 88 c0 a8 01 66 ad c2   ····@·@· ·····f··
0020  4f 6a eb 55 01 bb 4f 70  a6 e9 4c 74 5a 23 80 18   Oj·U··Op ··LtZ#··
0030  ff ff 42 5c 00 00 01 01  08 0a 48 e1 c5 6b 5a 9a   ··B\···· ··H··kZ·
0040  3e 14 16 03 01 00 73 01  00 00 6f 03 01 50 17 78   >·····s· ··o··P·x
0050  d3 16 c2 50 64 f7 cb 02  09 b3 36 ab 33 2d 96 9b   ···Pd··· ··6·3-··
0060  8e 09 1d 26 d4 cc d0 4b  73 1d 7e 55 0f 00 00 2e   ···&···K s·~U···.
0070  00 39 00 38 00 35 00 16  00 13 00 0a 00 33 00 32   ·9·8·5·· ·····3·2
0080  00 2f 00 9a 00 99 00 96  00 05 00 04 00 15 00 12   ·/······ ········
0090  00 09 00 14 00 11 00 08  00 06 00 03 00 ff 02 01   ········ ········
00a0  00 00 17 00 00 00 13 00  11 00 00 0e 77 77 77 2e   ········ ····www.
00b0  67 6f 6f 67 6c 65 2e 63  6f 6d                     google.c om
```

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?

Ans:

ds 16 c2 50 64 f7 cb o2 o9 b3 36 ab 33 2d 96 9b

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?

Ans:

Public key algorithm: RSA

Symmetric-key algorithm: AES_256

Hash algorithm: SHA

ServerHello Record

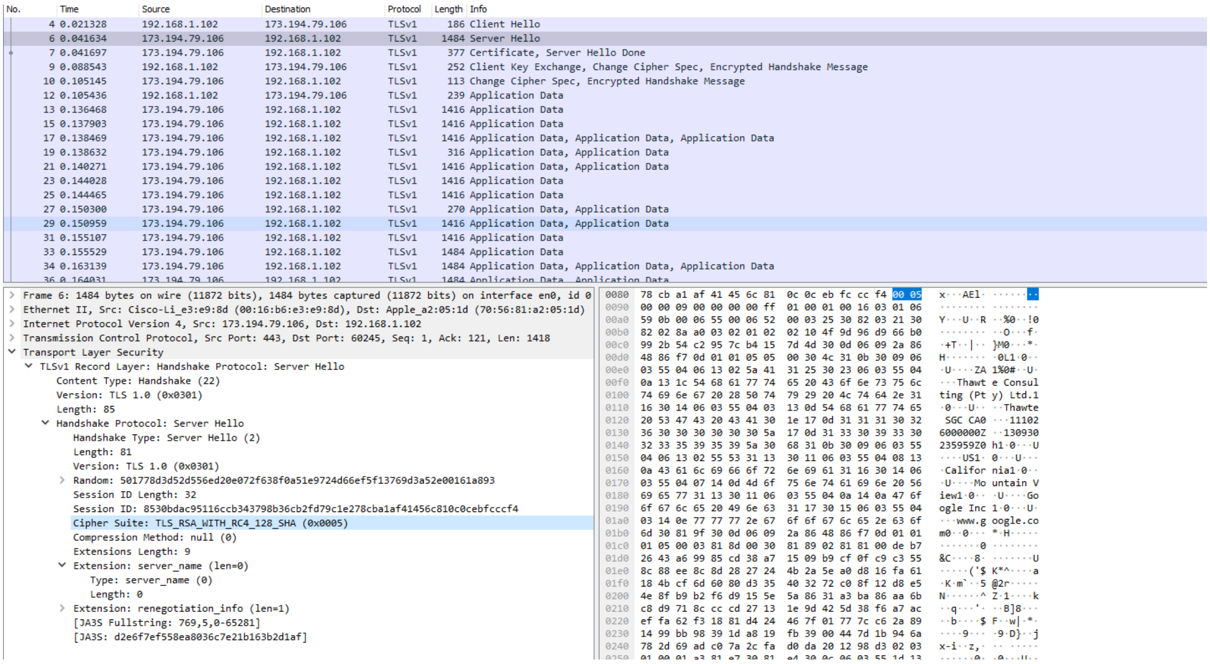
6. Locate the ServerHello SSL record. Does this record specify a chosen cipher suite? What are the algorithms in the chosen cipher suite?

Ans:

Public key algorithm: RSA

Symmetric-key algorithm: RC4

Hash algorithm: SHA



```
No.   Time      Source          Destination     Protocol Length Info
    4 0.021328  192.168.1.102   173.194.79.106  TLSv1     186 Client Hello
    6 0.041634  173.194.79.106  192.168.1.102   TLSv1    1484 Server Hello
    7 0.041697  173.194.79.106  192.168.1.102   TLSv1     377 Certificate, Server Hello Done
    9 0.088543  192.168.1.102   173.194.79.106  TLSv1     252 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
   10 0.105145  173.194.79.106  192.168.1.102   TLSv1     113 Change Cipher Spec, Encrypted Handshake Message
   12 0.105436  192.168.1.102   173.194.79.106  TLSv1     239 Application Data
   13 0.136468  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data
   15 0.137903  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data
   17 0.138469  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data, Application Data, Application Data
   19 0.138632  173.194.79.106  192.168.1.102   TLSv1     316 Application Data, Application Data
   21 0.140271  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data, Application Data
   23 0.144028  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data
   25 0.144465  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data
   27 0.150300  173.194.79.106  192.168.1.102   TLSv1     270 Application Data, Application Data
   29 0.150959  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data, Application Data
   31 0.155107  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data
   33 0.155529  173.194.79.106  192.168.1.102   TLSv1    1484 Application Data
   34 0.163139  173.194.79.106  192.168.1.102   TLSv1    1484 Application Data, Application Data, Application Data
   36 0.164031  173.194.79.106  192.168.1.102   TLSv1    1484 Application Data, Application Data
```

```
> Frame 6: 1484 bytes on wire (11872 bits), 1484 bytes captured (11872 bits) on interface en0, id 0
> Ethernet II, Src: Cisco-Li_e3:e9:8d (00:16:b6:e3:e9:8d), Dst: Apple_a2:05:1d (70:56:81:a2:05:1d)
> Internet Protocol Version 4, Src: 173.194.79.106, Dst: 192.168.1.102
> Transmission Control Protocol, Src Port: 443, Dst Port: 60245, Seq: 1, Ack: 121, Len: 1418
v Transport Layer Security
  v TLSv1 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 85
    v Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 81
        Version: TLS 1.0 (0x0301)
      > Random: 501778d3d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e00161a893
        Session ID Length: 32
        Session ID: 8530bdac95116ccb343798b36cb2fd79c1e278cba1af41456c810c0cebfcccf4
        Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
        Compression Method: null (0)
        Extensions Length: 9
      v Extension: server_name (len=0)
          Type: server_name (0)
          Length: 0
      > Extension: renegotiation_info (len=1)
        [JA3S Fullstring: 769,5,0-65281]
        [JA3S: d2e6f7ef558ea8036c7e21b163b2d1af]
```

```
0080  78 cb a1 af 41 45 6c 81  0c 0c eb fc cc f4 00 05   x···AEl· ········
0090  00 00 09 00 00 00 00 ff  01 00 01 00 16 03 01 06   ········ ········
00a0  59 0b 00 06 55 00 06 52  00 03 25 30 82 03 21 30   Y···U··R ··%0··!0
00b0  82 02 8a a0 03 02 01 02  02 10 4f 9d 96 d9 66 b0   ········ ··O···f·
00c0  99 2b 54 c2 95 7c b4 15  7d 4d 30 0d 06 09 2a 86   ·+T··|·· }M0···*·
00d0  48 86 f7 0d 01 01 05 05  00 30 4c 31 0b 30 09 06   H······· ·0L1·0··
00e0  03 55 04 06 13 02 5a 41  31 25 30 23 06 03 55 04   ·U····ZA 1%0#··U·
00f0  0a 13 1c 54 68 61 77 74  65 20 43 6f 6e 73 75 6c   ···Thawt e Consul
0100  74 69 6e 67 20 28 50 74  79 29 20 4c 74 64 2e 31   ting (Pt y) Ltd.1
0110  16 30 14 06 03 55 04 03  13 0d 54 68 61 77 74 65   ·0···U·· ··Thawte
0120  20 53 47 43 20 43 41 30  1e 17 0d 31 31 31 30 32    SGC CA0 ···11102
0130  36 30 30 30 30 30 30 5a  17 0d 31 33 30 39 33 30   6000000Z ··130930
0140  32 33 35 39 35 39 5a 30  68 31 0b 30 09 06 03 55   235959Z0 h1·0···U
0150  04 06 13 02 55 53 31 13  30 11 06 03 55 04 08 13   ····US1· 0···U···
0160  0a 43 61 6c 69 66 6f 72  6e 69 61 31 16 30 14 06   ·Califor nia1·0··
0170  03 55 04 07 14 0d 4d 6f  75 6e 74 61 69 6e 20 56   ·U····Mo untain V
0180  69 65 77 31 13 30 11 06  03 55 04 0a 14 0a 47 6f   iew1·0·· ·U····Go
0190  6f 67 6c 65 20 49 6e 63  31 17 30 15 06 03 55 04   ogle Inc 1·0···U·
01a0  03 14 0e 77 77 77 2e 67  6f 6f 67 6c 65 2e 63 6f   ···www.g oogle.co
01b0  6d 30 81 9f 30 0d 06 09  2a 86 48 86 f7 0d 01 01   m0··0··· *·H·····
01c0  01 05 00 03 81 8d 00 30  81 89 02 81 81 00 de b7   ·······0 ········
01d0  26 43 a6 99 85 cd 38 a7  15 09 b9 cf 0f c9 c3 55   &C····8· ·······U
01e0  8c 88 ee 8c 8d 28 27 24  4b 2a 5e a0 d8 16 fa 61   ·····('$ K*^····a
01f0  18 4b cf 6d 60 80 d3 35  40 32 72 c0 8f 12 d8 e5   ·K·m`··5 @2r·····
0200  4e 8f b9 b2 f6 d9 15 5e  5a 86 31 a3 ba 86 aa 6b   N······^ Z·1····k
0210  c8 d9 71 8c cc cd 27 13  1e 9d 42 5d 38 f6 a7 ac   ··q···'· ··B]8···
0220  ef fa 62 f3 18 81 d4 24  46 7f 01 77 7c c6 2a 89   ··b····$ F··w|·*·
0230  14 99 bb 98 39 1d a8 19  fb 39 00 44 7d 1b 94 6a   ····9··· ·9·D}··j
0240  78 2d 69 ad c0 7a 2c fa  d0 da 20 12 98 d3 02 03   x-i··z,· ·· ·····
0250  01 00 01 a3 81 e7 30 81  e4 30 0c 06 03 55 1d 13   ······0· ·0···U··
```

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?

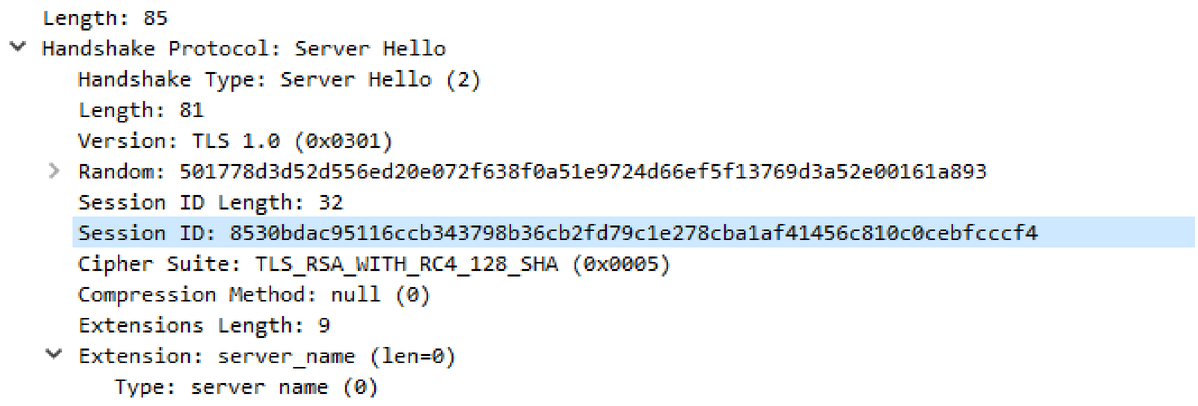
Ans:

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?

Ans:

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.



```
  Length: 85
Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 81
    Version: TLS 1.0 (0x0301)
    Random: 501778d3d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e00161a893
    Session ID Length: 32
    Session ID: 8530bdac95116ccb343798b36cb2fd79c1e278cba1af41456c810c0cebfcccf4
    Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
    Compression Method: null (0)
    Extensions Length: 9
    Extension: server_name (len=0)
        Type: server name (0)
```

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?

Ans:

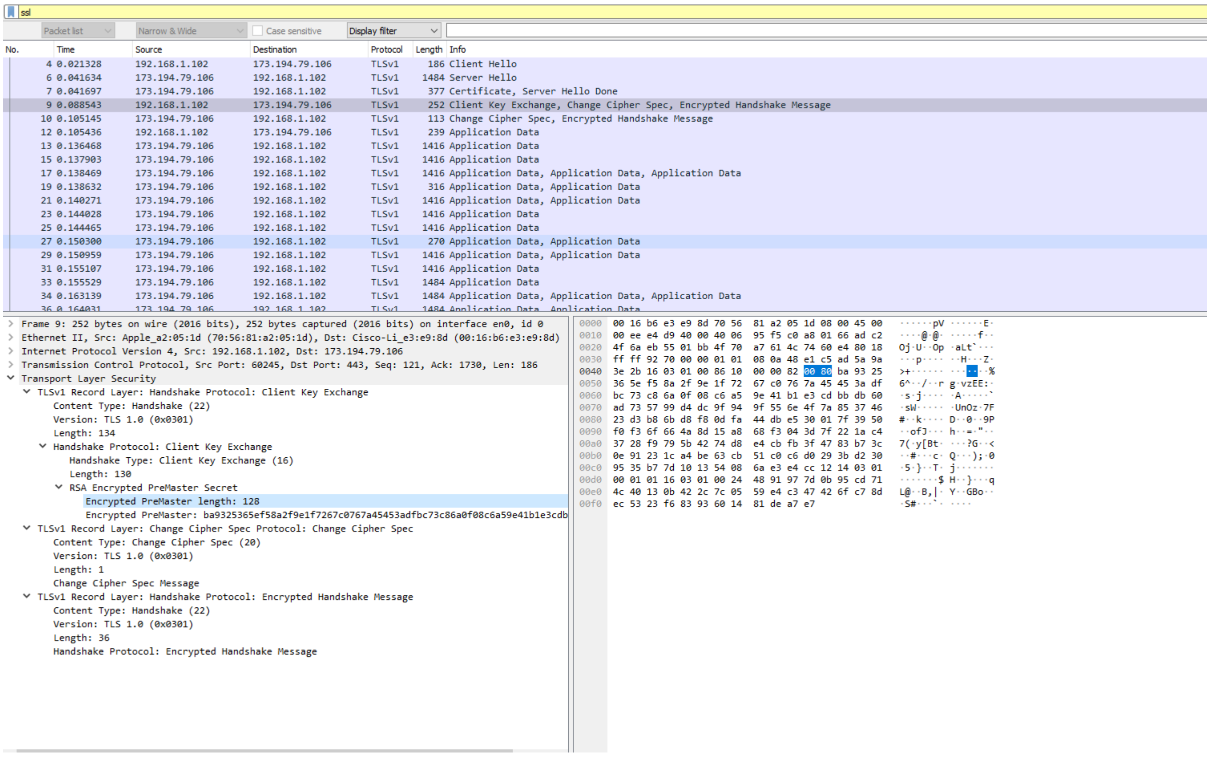
No, there is no certificate in this record. The certificate is in the separate record. Yes, the certificate fit into a single Ethernet frame.

Client Key Exchange Record

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?

Ans:

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 128 bytes



```
No.  Time      Source          Destination     Protocol Length Info
   4 0.021328  192.168.1.102   173.194.79.106  TLSv1     186 Client Hello
   6 0.041634  173.194.79.106  192.168.1.102   TLSv1    1484 Server Hello
   7 0.041697  173.194.79.106  192.168.1.102   TLSv1     377 Certificate, Server Hello Done
   9 0.088543  192.168.1.102   173.194.79.106  TLSv1     252 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  10 0.105145  173.194.79.106  192.168.1.102   TLSv1     113 Change Cipher Spec, Encrypted Handshake Message
  12 0.105436  192.168.1.102   173.194.79.106  TLSv1     239 Application Data
  13 0.136468  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data
  15 0.137903  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data
  17 0.138469  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data, Application Data, Application Data
  19 0.138632  173.194.79.106  192.168.1.102   TLSv1     316 Application Data, Application Data
  21 0.140271  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data, Application Data
  23 0.144028  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data
  25 0.144465  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data
  27 0.150300  173.194.79.106  192.168.1.102   TLSv1     270 Application Data, Application Data
  29 0.150959  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data, Application Data
  31 0.155107  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data
  33 0.155529  173.194.79.106  192.168.1.102   TLSv1    1484 Application Data
  34 0.163139  173.194.79.106  192.168.1.102   TLSv1    1484 Application Data, Application Data, Application Data
  36 0.164031  173.194.79.106  192.168.1.102   TLSv1    1484 Application Data, Application Data
```

```
> Frame 9: 252 bytes on wire (2016 bits), 252 bytes captured (2016 bits) on interface en0, id 0
> Ethernet II, Src: Apple_a2:05:1d (70:56:81:a2:05:1d), Dst: Cisco-Li_e3:e9:8d (00:16:b6:e3:e9:8d)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 173.194.79.106
> Transmission Control Protocol, Src Port: 60245, Dst Port: 443, Seq: 121, Ack: 1730, Len: 186
v Transport Layer Security
  v TLSv1 Record Layer: Handshake Protocol: Client Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 134
    v Handshake Protocol: Client Key Exchange
        Handshake Type: Client Key Exchange (16)
        Length: 130
      v RSA Encrypted PreMaster Secret
          Encrypted PreMaster length: 128
          Encrypted PreMaster: ba9325365ef58a2f9e1f7267c0767a45453adfbc73c86a0f08c6a59e41b1e3cdb
  v TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.0 (0x0301)
      Length: 1
      Change Cipher Spec Message
  v TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 36
      Handshake Protocol: Encrypted Handshake Message
```

```
0000  00 16 b6 e3 e9 8d 70 56  81 a2 05 1d 08 00 45 00   ······pV ······E·
0010  00 ee e4 d9 40 00 40 06  95 f5 c0 a8 01 66 ad c2   ····@·@· ·····f··
0020  4f 6a eb 55 01 bb 4f 70  a7 61 4c 74 60 e4 80 18   Oj·U··Op ·aLt`···
0030  ff ff 92 70 00 00 01 01  08 0a 48 e1 c5 ad 5a 9a   ···p···· ··H···Z·
0040  3e 2b 16 03 01 00 86 10  00 00 82 00 80 ba 93 25   >+······ ········%
0050  36 5e f5 8a 2f 9e 1f 72  67 c0 76 7a 45 45 3a df   6^··/··r g·vzEE:·
0060  bc 73 c8 6a 0f 08 c6 a5  9e 41 b1 e3 cd bb db 60   ·s·j···· ·A·····`
0070  ad 73 57 99 d4 dc 9f 94  9f 55 6e 4f 7a 85 37 46   ·sW····· ·UnOz·7F
0080  23 d3 b8 6b d8 f8 0d fa  44 db e5 30 01 7f 39 50   #··k···· D··0··9P
0090  f0 f3 6f 66 4a 8d 15 a8  68 f3 04 3d 7f 22 1a c4   ··ofJ··· h··="··
00a0  37 28 f9 79 5b 42 74 d8  e4 cb fb 3f 47 83 b7 3c   7(·y[Bt· ···?G··<
00b0  0e 91 23 1c a4 be 63 cb  51 c0 c6 d0 29 3b d2 30   ··#···c· Q···);·0
00c0  95 35 b7 7d 10 13 54 08  6a e3 e4 cc 12 14 03 01   ·5·}··T· j·······
00d0  00 01 01 16 03 01 00 24  48 91 97 7d 0b 95 cd 71   ·······$ H··}···q
00e0  4c 40 13 0b 42 2c 7c 05  59 e4 c3 47 42 6f c7 8d   L@··B,|· Y··GBo··
00f0  ec 53 23 f6 83 93 60 14  81 de a7 e7               ·S#···`· ····
```

11. Change Cipher Spec record? How many bytes is the record in your trace? In the encrypted handshake record, what is being encrypted? How?

Ans:

Content Type: change Cipher spec

Version: TLS (0x03)

Length: 1

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

Ans:

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

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

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?

Ans:

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

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