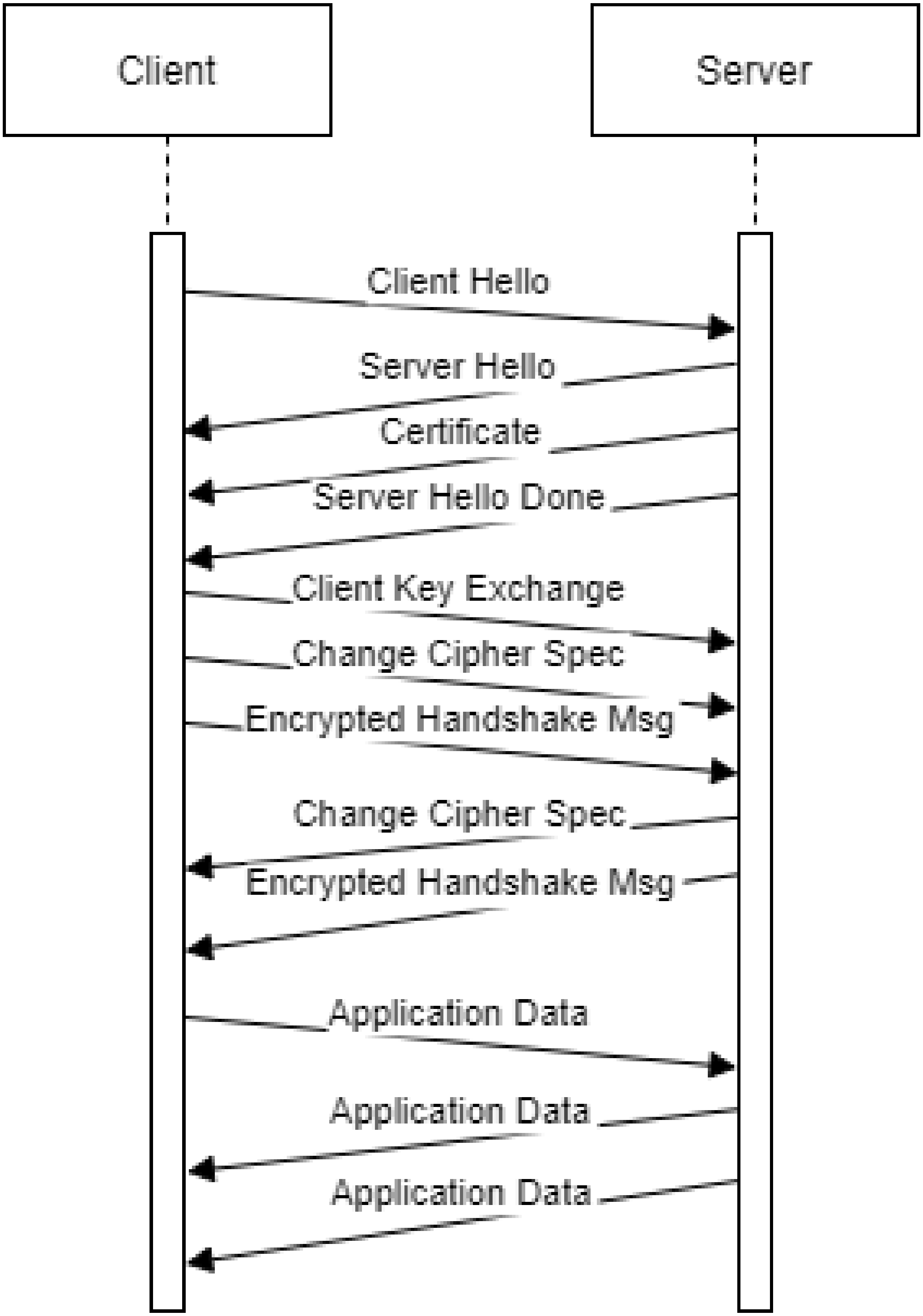
COMPUTER NETWORK
Lab 8

Student name: Nguyễn Minh Tâm
ID: 1952968

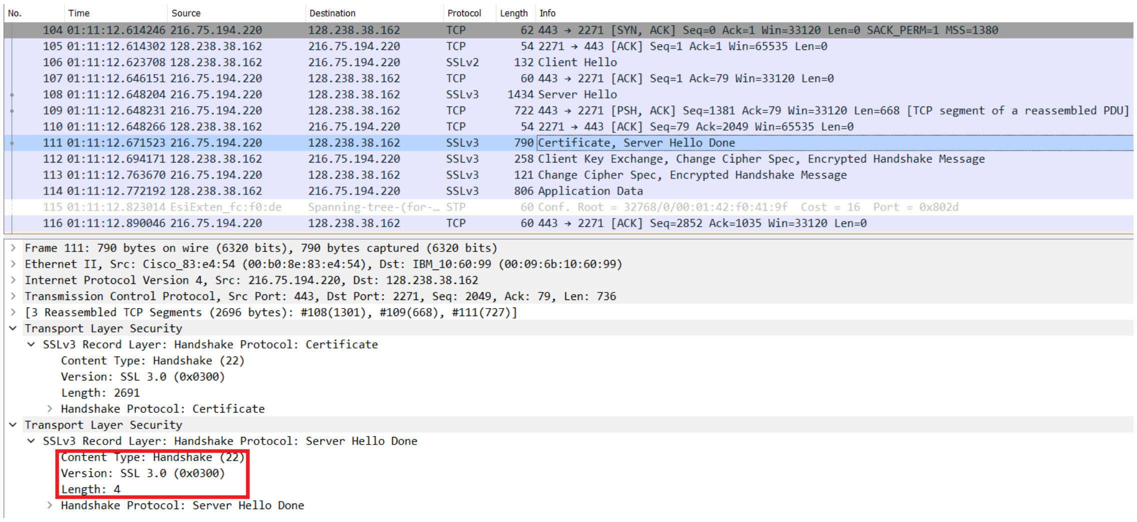
1. For each of the first 8 Ethernet frames, specify the source of the frame (client or server), determine the number of SSL records that are included in the frame, and list the SSL record types that are included in the frame. Draw a timing diagram between client and server, with one arrow for each SSL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

Frame	Source	SSL count	SSL Type
106	Client	1	Client Hello
108	Server	1	Server Hello
111	Server	2	Certificate Server Hello Done
112	Client	3	Client Key Exchange Change Cipher Spec Encrypted Handshake Message
113	Server	2	Change Cipher Spec Encrypted Handshake Message
114	Client	1	Application Data
122	Server	1	Application Data
127	Server	1	Application Data



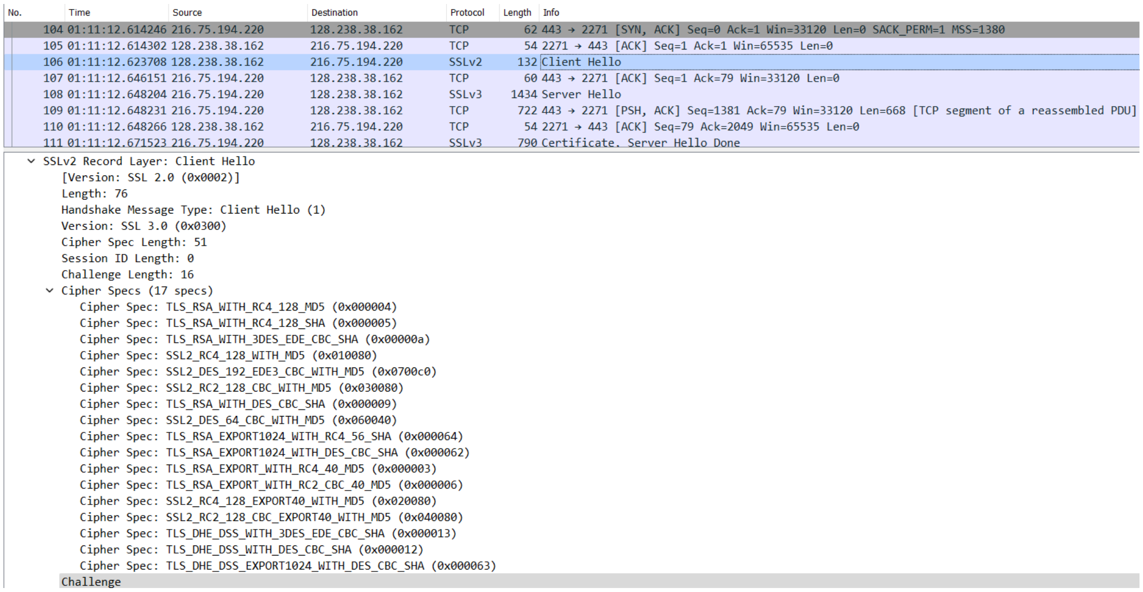
2. Each of the SSL records begins with the same three fields (with possibly different values). One of these fields is “content type” and has length of one byte. List all three fields and their lengths.

Ans:
Content type: 1 byte
Version: 2 bytes
Length: 2 bytes



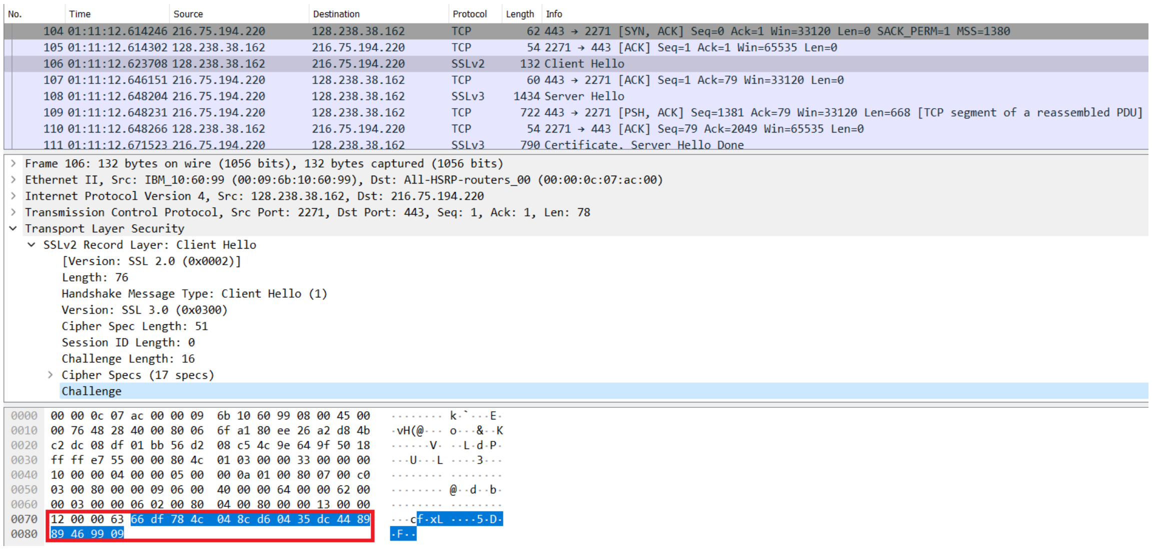
```
No.    Time               Source            Destination            Protocol  Length Info
   104 01:11:12.614246 216.75.194.220    128.238.38.162         TCP         62 443 → 2271 [SYN, ACK] Seq=0 Ack=1 Win=33120 Len=0 SACK_PERM=1 MSS=1380
   105 01:11:12.614302 128.238.38.162    216.75.194.220         TCP         54 2271 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
   106 01:11:12.623708 128.238.38.162    216.75.194.220         SSLv2      132 Client Hello
   107 01:11:12.646151 216.75.194.220    128.238.38.162         TCP         60 443 → 2271 [ACK] Seq=1 Ack=79 Win=33120 Len=0
   108 01:11:12.648204 216.75.194.220    128.238.38.162         SSLv3     1434 Server Hello
   109 01:11:12.648231 216.75.194.220    128.238.38.162         TCP        722 443 → 2271 [PSH, ACK] Seq=1381 Ack=79 Win=33120 Len=668 [TCP segment of a reassembled PDU]
   110 01:11:12.648266 128.238.38.162    216.75.194.220         TCP         54 2271 → 443 [ACK] Seq=79 Ack=2049 Win=65535 Len=0
   111 01:11:12.671523 216.75.194.220    128.238.38.162         SSLv3      790 Certificate, Server Hello Done
   112 01:11:12.694171 128.238.38.162    216.75.194.220         SSLv3      258 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
   113 01:11:12.763670 216.75.194.220    128.238.38.162         SSLv3      121 Change Cipher Spec, Encrypted Handshake Message
   114 01:11:12.772192 128.238.38.162    216.75.194.220         SSLv3      806 Application Data
   115 01:11:12.823014 EsiExten_fc:f0:de Spanning-tree-(for-… STP         60 Conf. Root = 32768/0/00:01:42:f0:41:9f  Cost = 16  Port = 0x802d
   116 01:11:12.890046 216.75.194.220    128.238.38.162         TCP         60 443 → 2271 [ACK] Seq=2852 Ack=1035 Win=33120 Len=0

> 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)]
v Transport Layer Security
  v SSLv3 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: SSL 3.0 (0x0300)
      Length: 2691
    > Handshake Protocol: Certificate
v Transport Layer Security
  v SSLv3 Record Layer: Handshake Protocol: Server Hello Done
      Content Type: Handshake (22)
      Version: SSL 3.0 (0x0300)
      Length: 4
    > Handshake Protocol: Server Hello Done
```

3. Expand the ClientHello record. What is the value of the content type?
   Ans: The content type is 22, for Handshake Message, with a handshake type of 01, Client Hello.



```
No.    Time               Source            Destination            Protocol  Length Info
   104 01:11:12.614246 216.75.194.220    128.238.38.162         TCP         62 443 → 2271 [SYN, ACK] Seq=0 Ack=1 Win=33120 Len=0 SACK_PERM=1 MSS=1380
   105 01:11:12.614302 128.238.38.162    216.75.194.220         TCP         54 2271 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
   106 01:11:12.623708 128.238.38.162    216.75.194.220         SSLv2      132 Client Hello
   107 01:11:12.646151 216.75.194.220    128.238.38.162         TCP         60 443 → 2271 [ACK] Seq=1 Ack=79 Win=33120 Len=0
   108 01:11:12.648204 216.75.194.220    128.238.38.162         SSLv3     1434 Server Hello
   109 01:11:12.648231 216.75.194.220    128.238.38.162         TCP        722 443 → 2271 [PSH, ACK] Seq=1381 Ack=79 Win=33120 Len=668 [TCP segment of a reassembled PDU]
   110 01:11:12.648266 128.238.38.162    216.75.194.220         TCP         54 2271 → 443 [ACK] Seq=79 Ack=2049 Win=65535 Len=0
   111 01:11:12.671523 216.75.194.220    128.238.38.162         SSLv3      790 Certificate, Server Hello Done

  v 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
    v 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
```

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: The value of the challenge in hexadecimal notation: 66 df 78 4c 04 8c d6 04 35 dc 44 89 89 46 99 09.



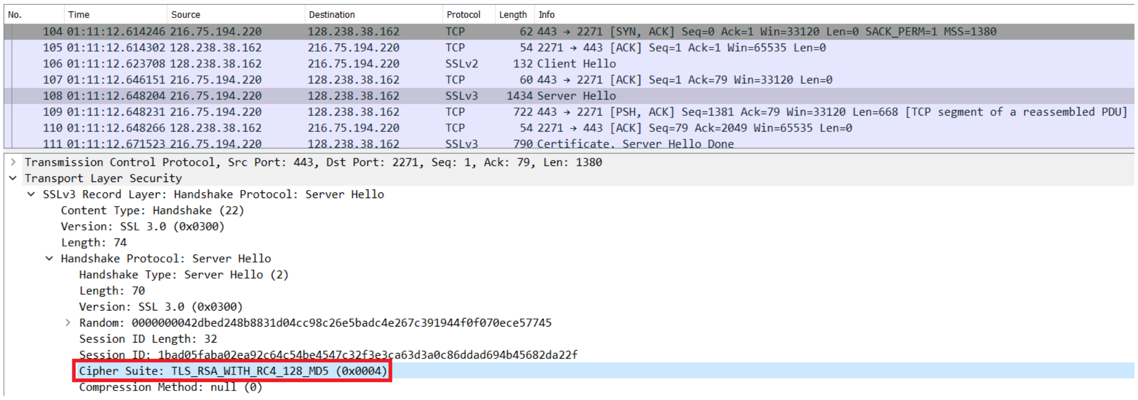
```
No.  Time            Source          Destination     Protocol Length Info
 104 01:11:12.614246 216.75.194.220  128.238.38.162  TCP        62 443 → 2271 [SYN, ACK] Seq=0 Ack=1 Win=33120 Len=0 SACK_PERM=1 MSS=1380
 105 01:11:12.614302 128.238.38.162  216.75.194.220  TCP        54 2271 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
 106 01:11:12.623708 128.238.38.162  216.75.194.220  SSLv2     132 Client Hello
 107 01:11:12.646151 216.75.194.220  128.238.38.162  TCP        60 443 → 2271 [ACK] Seq=1 Ack=79 Win=33120 Len=0
 108 01:11:12.648204 216.75.194.220  128.238.38.162  SSLv3    1434 Server Hello
 109 01:11:12.648231 216.75.194.220  128.238.38.162  TCP       722 443 → 2271 [PSH, ACK] Seq=1381 Ack=79 Win=33120 Len=668 [TCP segment of a reassembled PDU]
 110 01:11:12.648266 128.238.38.162  216.75.194.220  TCP        54 2271 → 443 [ACK] Seq=79 Ack=2049 Win=65535 Len=0
 111 01:11:12.671523 216.75.194.220  128.238.38.162  SSLv3     790 Certificate, Server Hello Done
```

```
> 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, Dst: 216.75.194.220
> Transmission Control Protocol, Src Port: 2271, Dst Port: 443, Seq: 1, Ack: 1, Len: 78
v Transport Layer Security
  v 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)
        Challenge
```

```
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··
```

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: The first suite uses RSA for public key crpto, RC4 for the symmetric-key cipher and uses the MD5 hash algorithm.

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: MD5

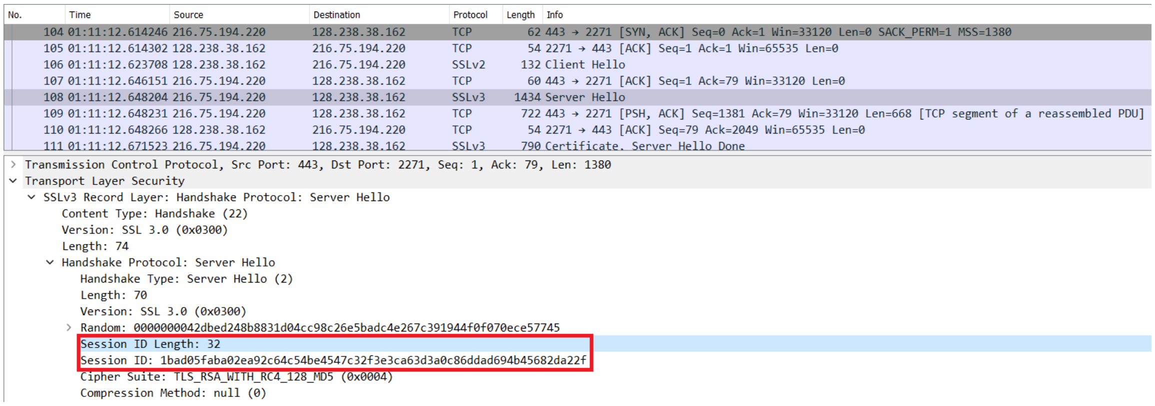


```
No.  Time            Source          Destination     Protocol Length Info
 104 01:11:12.614246 216.75.194.220  128.238.38.162  TCP        62 443 → 2271 [SYN, ACK] Seq=0 Ack=1 Win=33120 Len=0 SACK_PERM=1 MSS=1380
 105 01:11:12.614302 128.238.38.162  216.75.194.220  TCP        54 2271 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
 106 01:11:12.623708 128.238.38.162  216.75.194.220  SSLv2     132 Client Hello
 107 01:11:12.646151 216.75.194.220  128.238.38.162  TCP        60 443 → 2271 [ACK] Seq=1 Ack=79 Win=33120 Len=0
 108 01:11:12.648204 216.75.194.220  128.238.38.162  SSLv3    1434 Server Hello
 109 01:11:12.648231 216.75.194.220  128.238.38.162  TCP       722 443 → 2271 [PSH, ACK] Seq=1381 Ack=79 Win=33120 Len=668 [TCP segment of a reassembled PDU]
 110 01:11:12.648266 128.238.38.162  216.75.194.220  TCP        54 2271 → 443 [ACK] Seq=79 Ack=2049 Win=65535 Len=0
 111 01:11:12.671523 216.75.194.220  128.238.38.162  SSLv3     790 Certificate, Server Hello Done
```

```
> Transmission Control Protocol, Src Port: 443, Dst Port: 2271, Seq: 1, Ack: 79, Len: 1380
v Transport Layer Security
  v SSLv3 Record Layer: Handshake Protocol: Server Hello
        Content Type: Handshake (22)
        Version: SSL 3.0 (0x0300)
        Length: 74
      v 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)
```

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, this record includes a nonce listed uder Random.
   The nonce is 32 bits long, 28 for data and 4 for the time.
   The purpose is to prevent a replay attack.

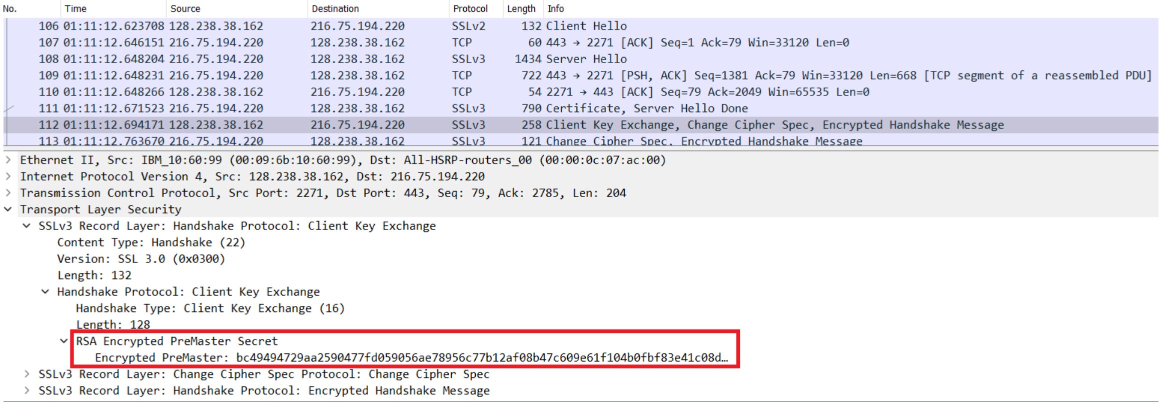
8. Does this record include a session ID? What is the purpose of the session ID?
   Ans:
   Yes, the session ID in the record is an identifier for SSL session. This ID could let the client to resume the session later by using the session ID.



```
No.     Time            Source          Destination     Protocol Length Info
    104 01:11:12.614246 216.75.194.220  128.238.38.162  TCP        62 443 → 2271 [SYN, ACK] Seq=0 Ack=1 Win=33120 Len=0 SACK_PERM=1 MSS=1380
    105 01:11:12.614302 128.238.38.162  216.75.194.220  TCP        54 2271 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
    106 01:11:12.623708 128.238.38.162  216.75.194.220  SSLv2     132 Client Hello
    107 01:11:12.646151 216.75.194.220  128.238.38.162  TCP        60 443 → 2271 [ACK] Seq=1 Ack=79 Win=33120 Len=0
    108 01:11:12.648204 216.75.194.220  128.238.38.162  SSLv3    1434 Server Hello
    109 01:11:12.648231 216.75.194.220  128.238.38.162  TCP       722 443 → 2271 [PSH, ACK] Seq=1381 Ack=79 Win=33120 Len=668 [TCP segment of a reassembled PDU]
    110 01:11:12.648266 128.238.38.162  216.75.194.220  TCP        54 2271 → 443 [ACK] Seq=79 Ack=2049 Win=65535 Len=0
    111 01:11:12.671523 216.75.194.220  128.238.38.162  SSLv3     790 Certificate, Server Hello Done

> Transmission Control Protocol, Src Port: 443, Dst Port: 2271, Seq: 1, Ack: 79, Len: 1380
v Transport Layer Security
  v SSLv3 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: SSL 3.0 (0x0300)
      Length: 74
    v 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)
```

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.

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 120 bytes.



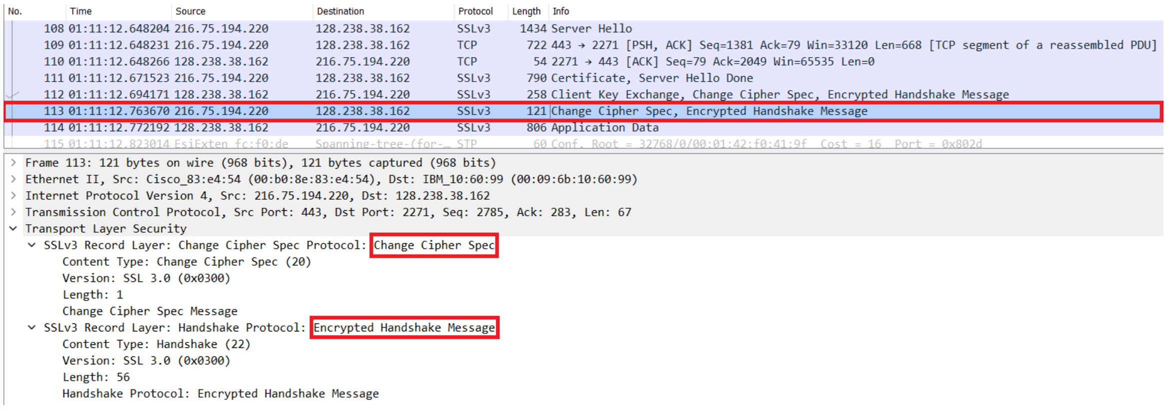
```
No.     Time            Source          Destination     Protocol Length Info
    106 01:11:12.623708 128.238.38.162  216.75.194.220  SSLv2     132 Client Hello
    107 01:11:12.646151 216.75.194.220  128.238.38.162  TCP        60 443 → 2271 [ACK] Seq=1 Ack=79 Win=33120 Len=0
    108 01:11:12.648204 216.75.194.220  128.238.38.162  SSLv3    1434 Server Hello
    109 01:11:12.648231 216.75.194.220  128.238.38.162  TCP       722 443 → 2271 [PSH, ACK] Seq=1381 Ack=79 Win=33120 Len=668 [TCP segment of a reassembled PDU]
    110 01:11:12.648266 128.238.38.162  216.75.194.220  TCP        54 2271 → 443 [ACK] Seq=79 Ack=2049 Win=65535 Len=0
    111 01:11:12.671523 216.75.194.220  128.238.38.162  SSLv3     790 Certificate, Server Hello Done
    112 01:11:12.694171 128.238.38.162  216.75.194.220  SSLv3     258 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
    113 01:11:12.763670 216.75.194.220  128.238.38.162  SSLv3     121 Change Cipher Spec, Encrypted Handshake Message

> 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, Dst: 216.75.194.220
> Transmission Control Protocol, Src Port: 2271, Dst Port: 443, Seq: 79, Ack: 2785, Len: 204
v Transport Layer Security
  v SSLv3 Record Layer: Handshake Protocol: Client Key Exchange
      Content Type: Handshake (22)
      Version: SSL 3.0 (0x0300)
      Length: 132
    v Handshake Protocol: Client Key Exchange
        Handshake Type: Client Key Exchange (16)
        Length: 128
      v RSA Encrypted PreMaster Secret
          Encrypted PreMaster: bc49494729aa2590477fd059056ae78956c77b12af08b47c609e61f104b0fbf83e41c08d…
  > SSLv3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
  > SSLv3 Record Layer: Handshake Protocol: Encrypted Handshake Message
```

11. What is the purpose of the Change Cipher Spec record? How many bytes is the record in your trace?
    Ans: The purpose of the Change Cipher Spec record is to indicate that the

contents of the following SSL records sent by the client will be encrypted. The record is 6 bytes long: 5 for the header and 1 for the message segment.

12. In the encrypted handshake record, what is being encrypted? How?
    Ans: 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?
    Ans:
    Yes, the server will also send a Change Cipher Spec record and encrypted handshake to the client. The server's encrypted handshake record is different from that sent by the client because it contains the concatenation of all the handshake messages sent from the server rather than from the client. Otherwise the records would end up being the same.



```
No.  Time            Source           Destination      Protocol Length Info
 108 01:11:12.648204 216.75.194.220   128.238.38.162   SSLv3    1434 Server Hello
 109 01:11:12.648231 216.75.194.220   128.238.38.162   TCP       722 443 → 2271 [PSH, ACK] Seq=1381 Ack=79 Win=33120 Len=668 [TCP segment of a reassembled PDU]
 110 01:11:12.648266 128.238.38.162   216.75.194.220   TCP        54 2271 → 443 [ACK] Seq=79 Ack=2049 Win=65535 Len=0
 111 01:11:12.671523 216.75.194.220   128.238.38.162   SSLv3     790 Certificate, Server Hello Done
 112 01:11:12.694171 128.238.38.162   216.75.194.220   SSLv3     258 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
 113 01:11:12.763670 216.75.194.220   128.238.38.162   SSLv3     121 Change Cipher Spec, Encrypted Handshake Message
 114 01:11:12.772192 128.238.38.162   216.75.194.220   SSLv3     806 Application Data
 115 01:11:12.823014 EsiExten_fc:f0:de Spanning-tree-(for-… STP   60 Conf. Root = 32768/0/00:01:42:f0:41:9f  Cost = 16  Port = 0x802d

> Frame 113: 121 bytes on wire (968 bits), 121 bytes captured (968 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: 2785, Ack: 283, Len: 67
v Transport Layer Security
  v 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
  v SSLv3 Record Layer: Handshake Protocol: Encrypted Handshake Message
      Content Type: Handshake (22)
      Version: SSL 3.0 (0x0300)
      Length: 56
      Handshake Protocol: Encrypted Handshake Message
```

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?
    Ans:
    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.
    Ans:
    The version of SSL used changes from SSLv2 in the initial ClientHello message to SSLv3 in all following message exchanges.