TRƯỜNG ĐẠI HỌC BÁCH KHOA

ĐẠI HỌC QUỐC GIA TP HỒ CHÍ MINH

HOMEWORK

MẠNG MÁY TÍNH (THỰC HÀNH) – LAB 8

Giảng viên hướng dẫn: Ths. Bùi Xuân Giang

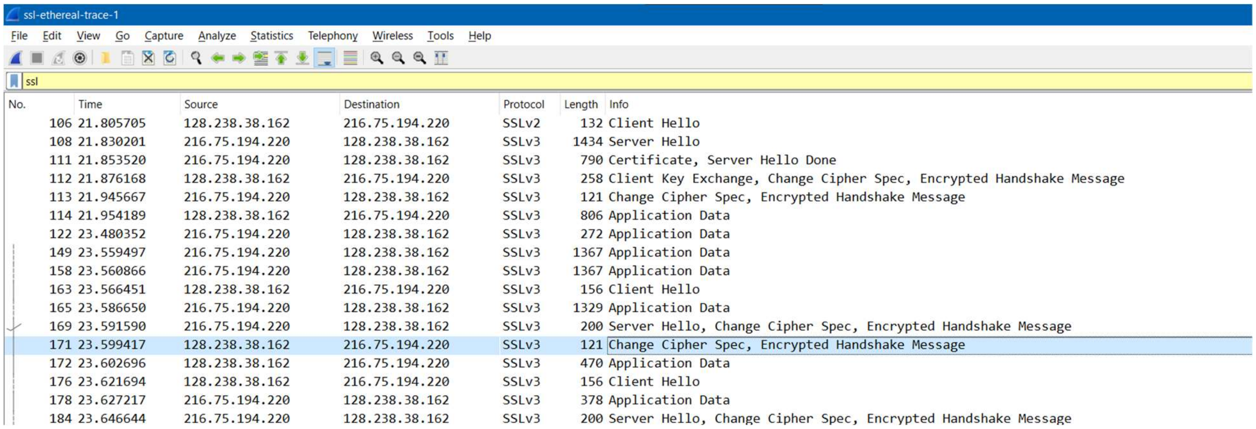
Sinh viên thực hiện: Trần Minh Tân

Mã số sinh viên: 2012018

Lớp: L10.

Thành phố Hồ Chí Minh – 2022

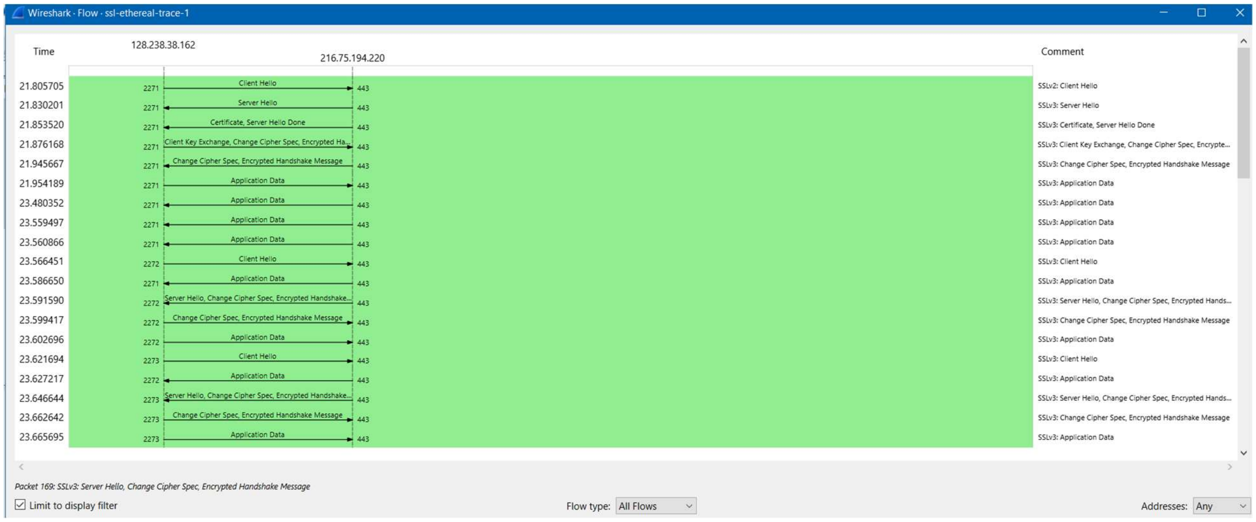
1. For each of the first 8 Ethernet frames, specify the source of the frame (client or server), determine the number of SSL records that are included in the frame, and list the SSL record types that are included in the frame. Draw a timing diagram between client and server, with one arrow for each SSL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



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, Server Hello Done
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	23.559497	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

Line	Source	Destination	SSL type	SSL records
106	128.238.38.162	216.75.194.220	Client Hello	1
108	216.75.194.220	128.238.38.162	Server Hello	1
111	128.238.38.162	216.75.194.220	Certificate, Server Hello Done	2
112	128.238.38.162	216.75.194.220	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	3
113	216.75.194.220	128.238.38.162	Change Cipher Spec, Encrypted Handshake Message	1
114	128.238.38.162	216.75.194.220	Application Data	1
122	216.75.194.220	128.238.38.162	Application Data	1
149	216.75.194.220	128.238.38.162	Application Data	1

Timing diagram:



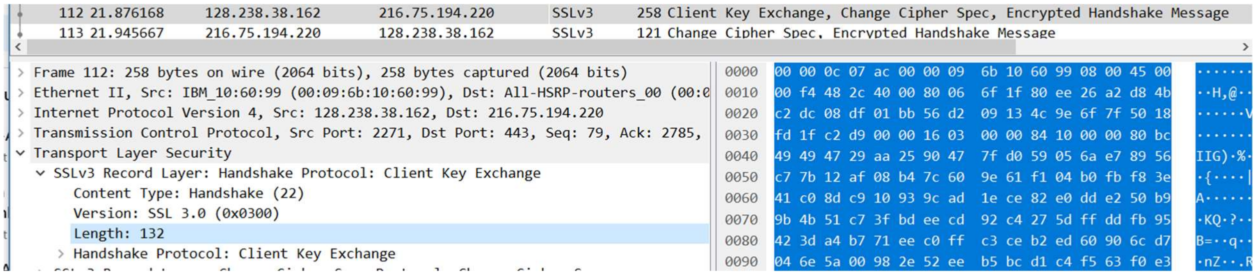
```
Time        128.238.38.162                                              Comment
                        216.75.194.220
21.805705   2271 Client Hello                                     443   SSLv2: Client Hello
21.830201   2271 Server Hello                                     443   SSLv3: Server Hello
21.853520   2271 Certificate, Server Hello Done                   443   SSLv3: Certificate, Server Hello Done
21.876168   2271 Client Key Exchange, Change Cipher Spec, Encrypted Ha... 443   SSLv3: Client Key Exchange, Change Cipher Spec, Encrypte...
21.945667   2271 Change Cipher Spec, Encrypted Handshake Message  443   SSLv3: Change Cipher Spec, Encrypted Handshake Message
21.954189   2271 Application Data                                 443   SSLv3: Application Data
23.480352   2271 Application Data                                 443   SSLv3: Application Data
23.559497   2271 Application Data                                 443   SSLv3: Application Data
23.560866   2271 Application Data                                 443   SSLv3: Application Data
23.566451   2272 Client Hello                                     443   SSLv3: Client Hello
23.586650   2271 Application Data                                 443   SSLv3: Application Data
23.591590   2272 Server Hello, Change Cipher Spec, Encrypted Handshake... 443   SSLv3: Server Hello, Change Cipher Spec, Encrypted Hands...
23.599417   2272 Change Cipher Spec, Encrypted Handshake Message  443   SSLv3: Change Cipher Spec, Encrypted Handshake Message
23.602696   2272 Application Data                                 443   SSLv3: Application Data
23.621694   2273 Client Hello                                     443   SSLv3: Client Hello
23.627217   2272 Application Data                                 443   SSLv3: Application Data
23.646644   2273 Server Hello, Change Cipher Spec, Encrypted Handshake... 443   SSLv3: Server Hello, Change Cipher Spec, Encrypted Hands...
23.662642   2273 Change Cipher Spec, Encrypted Handshake Message  443   SSLv3: Change Cipher Spec, Encrypted Handshake Message
23.665695   2273 Application Data                                 443   SSLv3: Application Data

Packet 169: SSLv3: Server Hello, Change Cipher Spec, Encrypted Handshake Message
```

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.

- Content type: 1 byte.

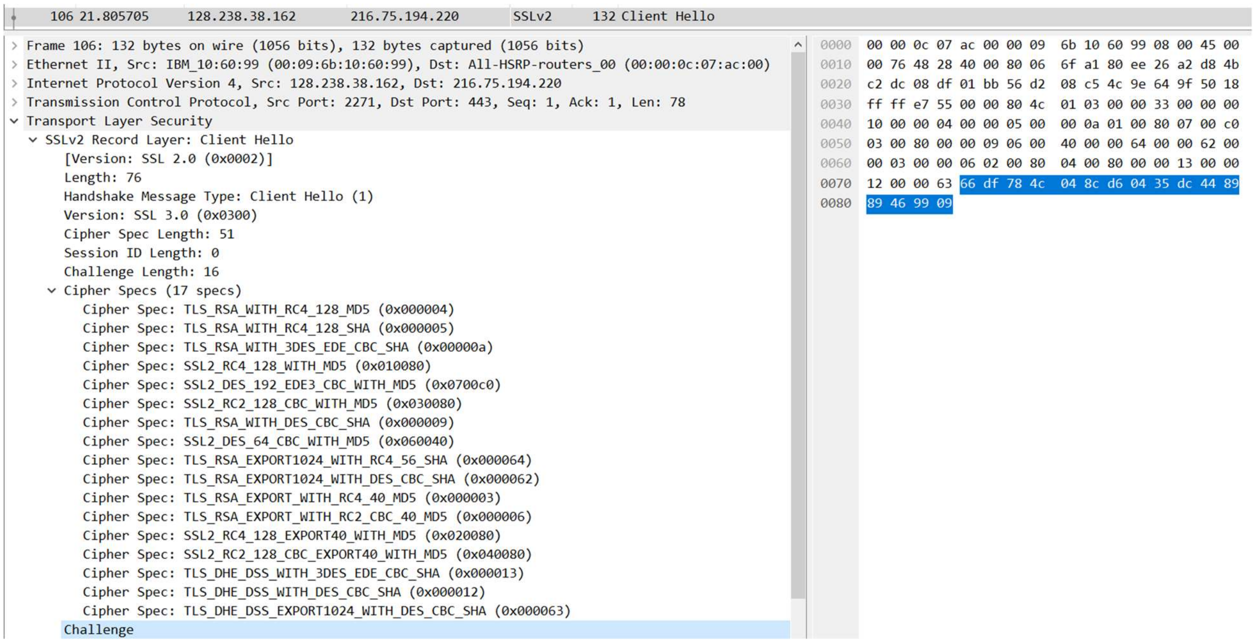
- Version: 2 bytes.

- Length: 2 bytes.



```
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

> 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 (00:0
> 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,
v Transport Layer Security
  v SSLv3 Record Layer: Handshake Protocol: Client Key Exchange
      Content Type: Handshake (22)
      Version: SSL 3.0 (0x0300)
      Length: 132
    > Handshake Protocol: Client Key Exchange

0000  00 00 0c 07 ac 00 00 09  6b 10 60 99 08 00 45 00   ·······
0010  00 f4 48 2c 40 00 80 06  6f 1f 80 ee 26 a2 d8 4b   ··H,@··
0020  c2 dc 08 df 01 bb 56 d2  09 13 4c 9e 6f 7f 50 18   ······V
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)·%·
0050  c7 7b 12 af 08 b4 7c 60  9e 61 f1 04 b0 fb f8 3e   ·{····|
0060  41 c0 8d c9 10 93 9c ad  1e ce 82 e0 dd e2 50 b9   A······
0070  9b 4b 51 c7 3f bd ee cd  92 c4 27 5d ff dd fb 95   ·KQ·?··
0080  42 3d a4 b7 71 ee c0 ff  c3 ce b2 ed 60 90 6c d7   B=··q··
0090  04 6e 5a 00 98 2e 52 ee  b5 bc d1 c4 f5 63 f0 e3   ·nZ···.R
```

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?



```
    106 21.805705    128.238.38.162    216.75.194.220    SSLv2    132 Client Hello
```

```
> 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
    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
```

```
0000  00 00 0c 07 ac 00 00 09  6b 10 60 99 08 00 45 00
0010  00 76 48 28 40 00 80 06  6f a1 80 ee 26 a2 d8 4b
0020  c2 dc 08 df 01 bb 56 d2  08 c5 4c 9e 64 9f 50 18
0030  ff ff e7 55 00 00 80 4c  01 03 00 00 33 00 00 00
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
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
0080  89 46 99 09
```

Content type value 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?

Yes it is. The value of the challenge in hexadecimal notation is 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?

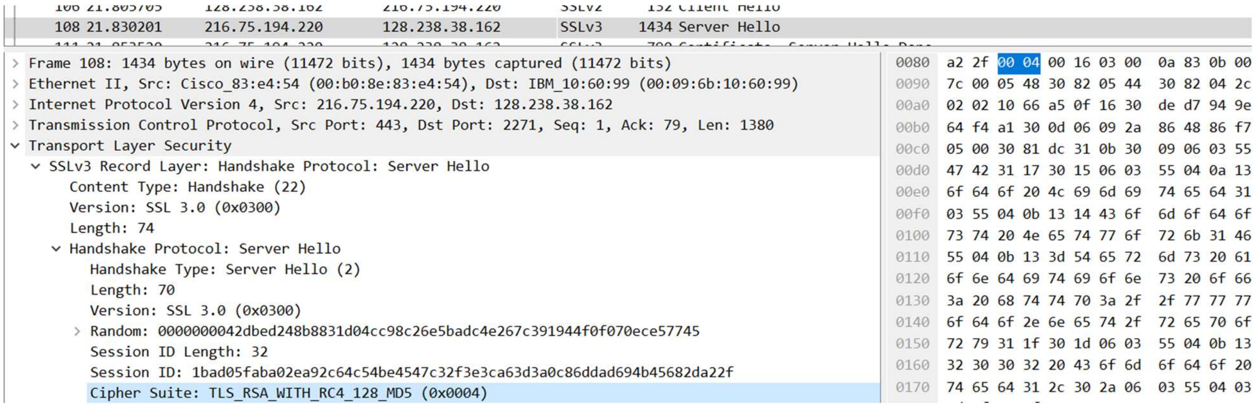
- Public key algorithm: RSA

- 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?

Yes, they are RSA, RC4 and MD5.



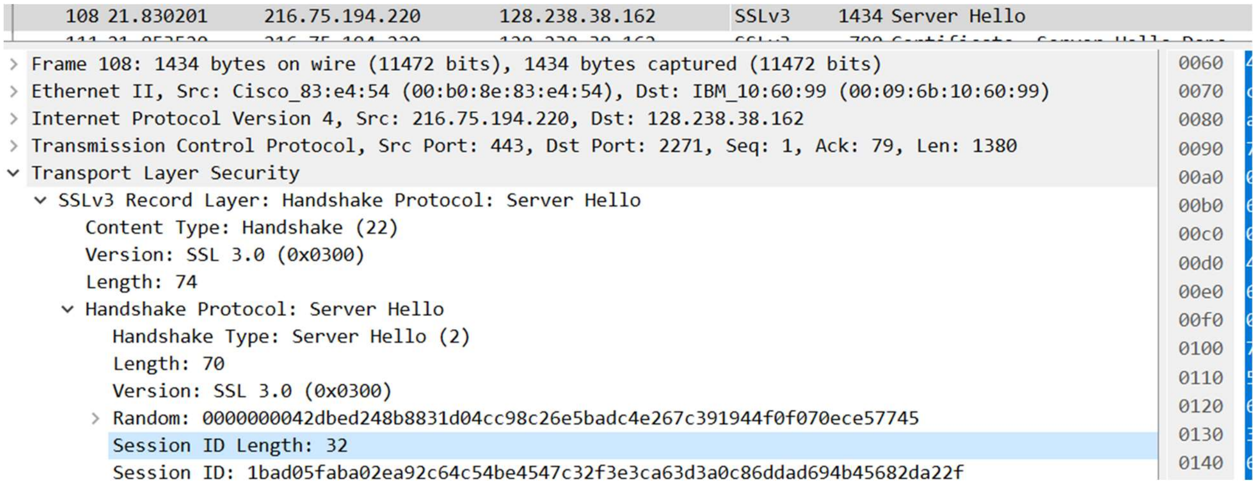
```
    108 21.830201    216.75.194.220    128.238.38.162    SSLv3    1434 Server Hello

> 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
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)
```

```
0080  a2 2f 00 04 00 16 03 00  0a 83 0b 00
0090  7c 00 05 48 30 82 05 44  30 82 04 2c
00a0  02 02 10 66 a5 0f 16 30  de d7 94 9e
00b0  64 f4 a1 30 0d 06 09 2a  86 48 86 f7
00c0  05 00 30 81 dc 31 0b 30  09 06 03 55
00d0  47 42 31 17 30 15 06 03  55 04 0a 13
00e0  6f 64 6f 20 4c 69 6d 69  74 65 64 31
00f0  03 55 04 0b 13 14 43 6f  6d 6f 64 6f
0100  73 74 20 4e 65 74 77 6f  72 6b 31 46
0110  55 04 0b 13 3d 54 65 72  6d 73 20 61
0120  6f 6e 64 69 74 69 6f 6e  73 20 6f 66
0130  3a 20 68 74 74 70 3a 2f  2f 77 77 77
0140  6f 64 6f 2e 6e 65 74 2f  72 65 70 6f
0150  72 79 31 1f 30 1d 06 03  55 04 0b 13
0160  32 30 30 32 20 43 6f 6d  6f 64 6f 20
0170  74 65 64 31 2c 30 2a 06  03 55 04 03
```

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?

Yes, the length of this nonce is 32 bits long (28bits data + 4 bits time). The purpose of the client and server nonces in SSL is used for attack preventing.

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



```
    108 21.830201    216.75.194.220    128.238.38.162    SSLv3    1434 Server Hello

> 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
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
```

```
0060
0070
0080
0090
00a0
00b0
00c0
00d0
00e0
00f0
0100
0110
0120
0130
0140
```

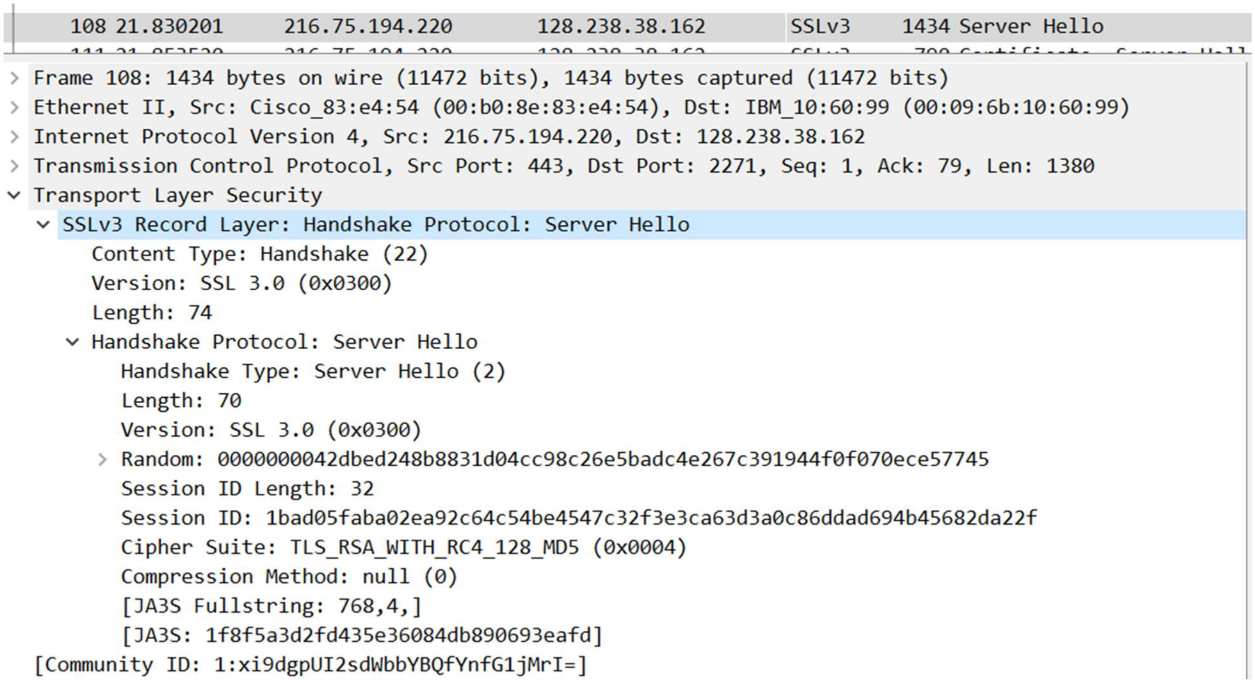
Yes, the purpose of the session ID is help the client to resume the session later by using this session ID.

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?

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?

Yes, it contains a pre-master secret. This secret is used for creating the master secret. The secret is encrypted by public key, whose length is 120 bytes.



```
   108 21.830201      216.75.194.220       128.238.38.162       SSLv3     1434 Server Hello
> 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
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)
        [JA3S Fullstring: 768,4,]
        [JA3S: 1f8f5a3d2fd435e36084db890693eafd]
  [Community ID: 1:xi9dgpUI2sdWbbYBQfYnfG1jMrI=]
```

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

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

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

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?

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?

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.

I don’t have any comments here.