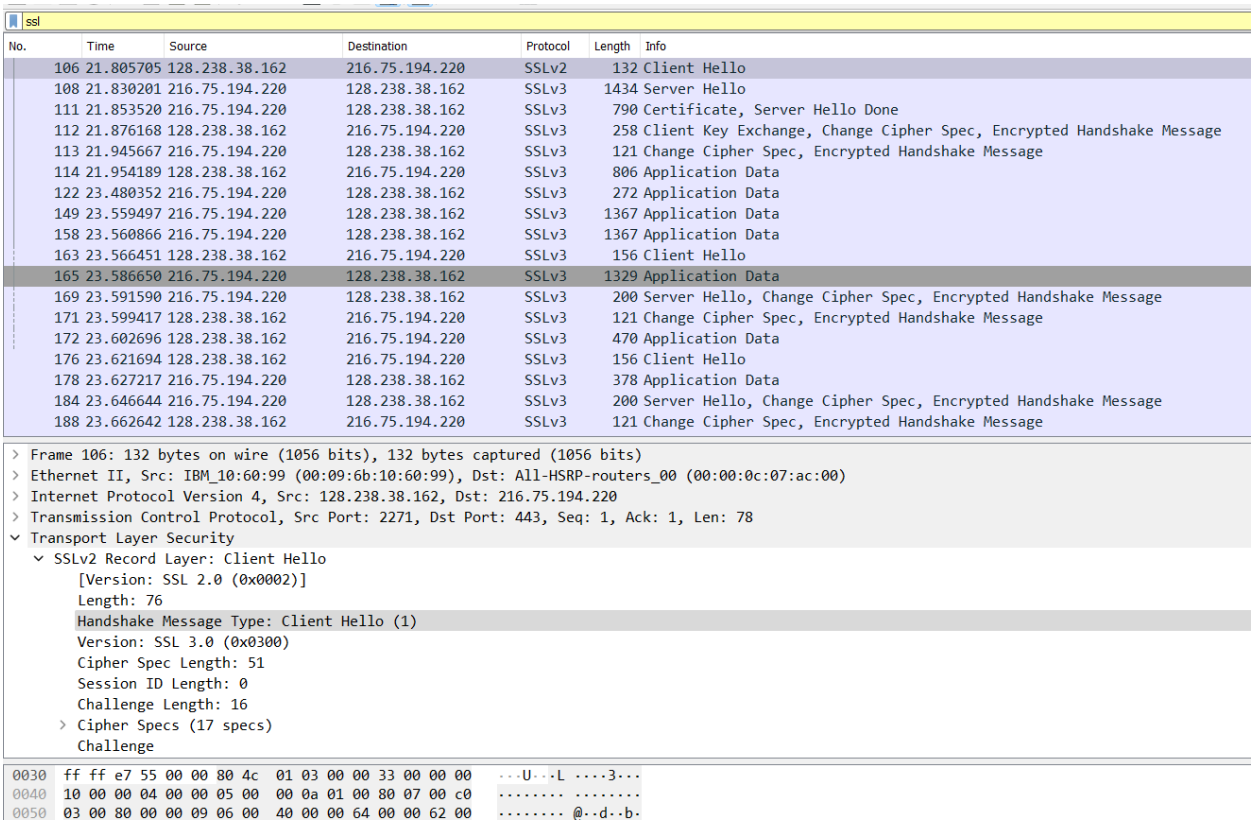
1/

Frame	Source	Destination	SSL Count	SSL Type
106	128.238.38.162	216.75.194.220	1	Client Hello
108	216.75.194.220	128.238.38.162	1	Server Hello
111	216.75.194.220	128.238.38.162	2	Server Hello Done
112	128.238.38.162	216.75.194.220	3	Client Key Exchange
113	216.75.194.220	128.238.38.162	2	Change Cipher Spec
114	128.238.38.162	216.75.194.220	1	Application Data
122	216.75.194.220	128.238.38.162	1	Application Data
149	216.75.194.220	128.238.38.162	1	Application Data

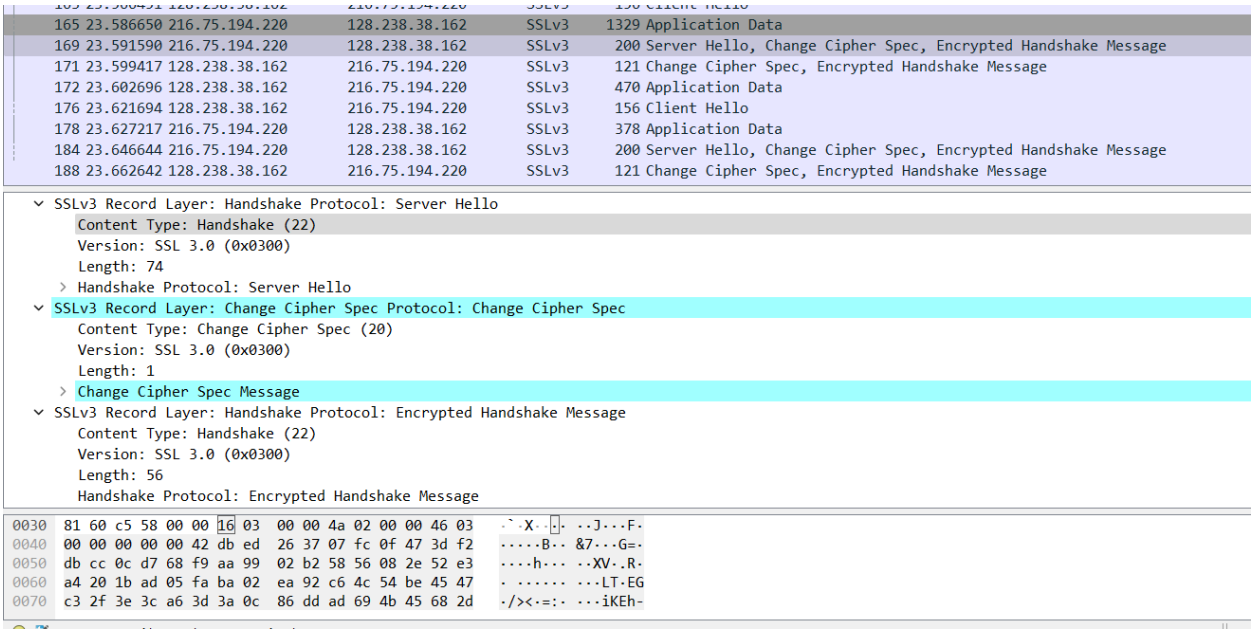


2/

Content type : 1 byte

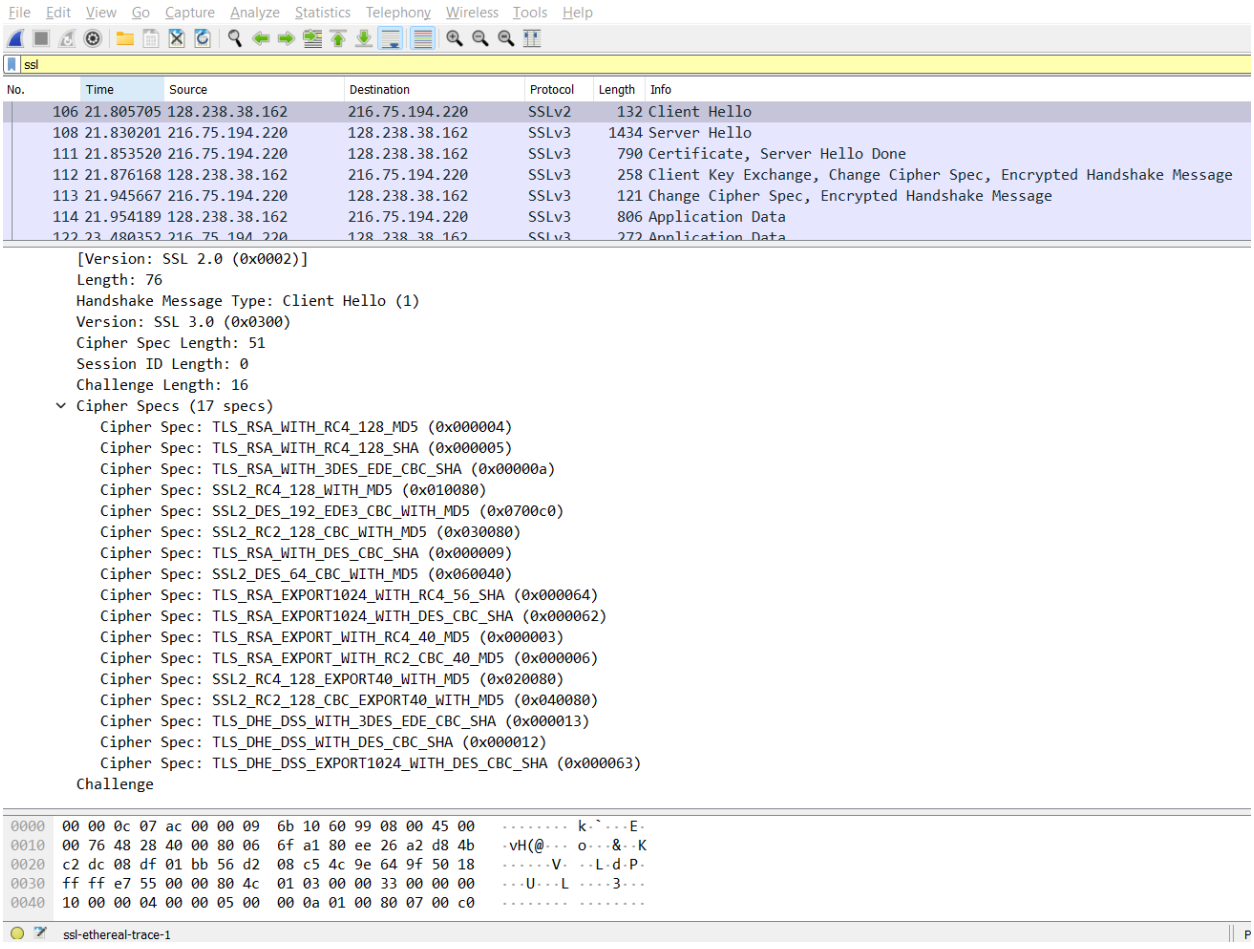
Version: 2 bytes

Length: 2 bytes

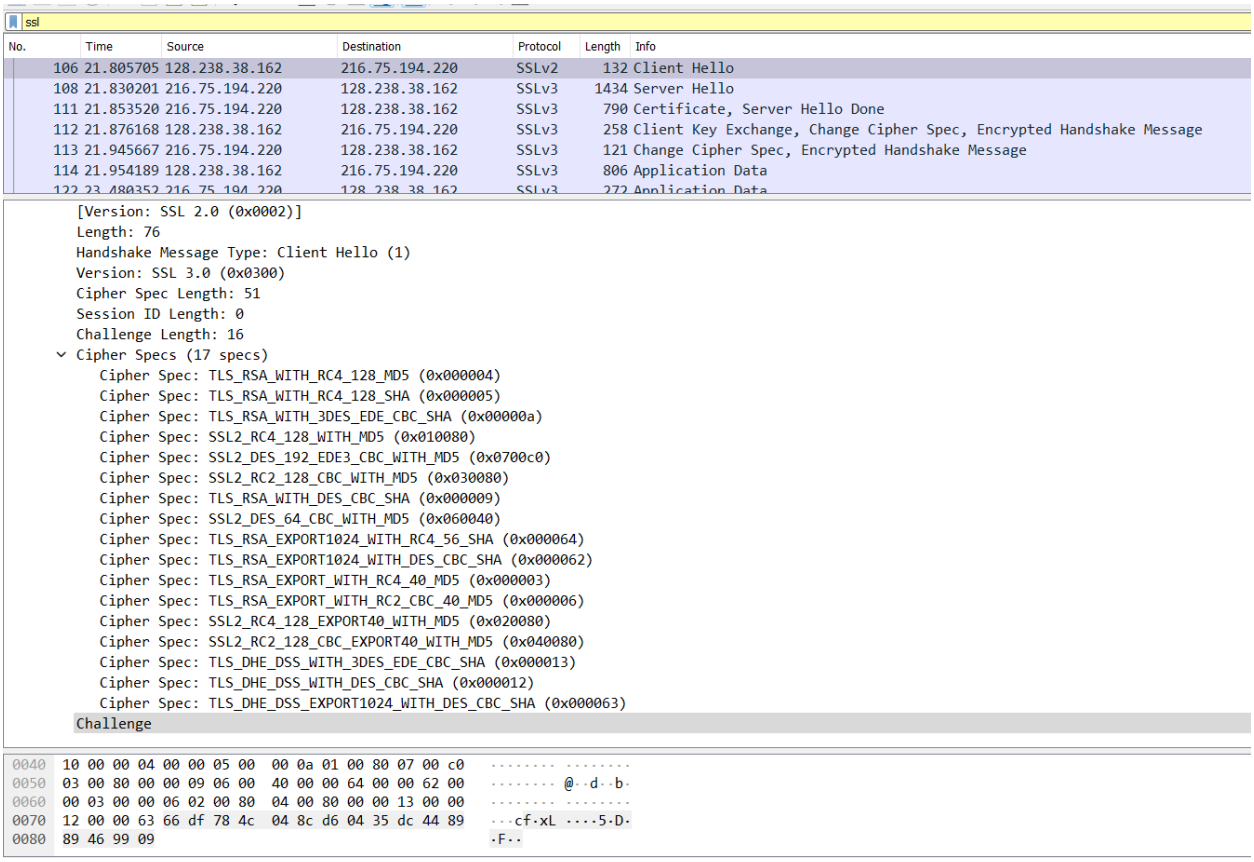


3/

The content type is 22, for Handshake Message, with a handshake type of 01, Client Hello.



4/



ssl

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

```
[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_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
```

```
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..
```

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

5/

Public key algorithm: RSA

Symmetric-key algorithm: RC4

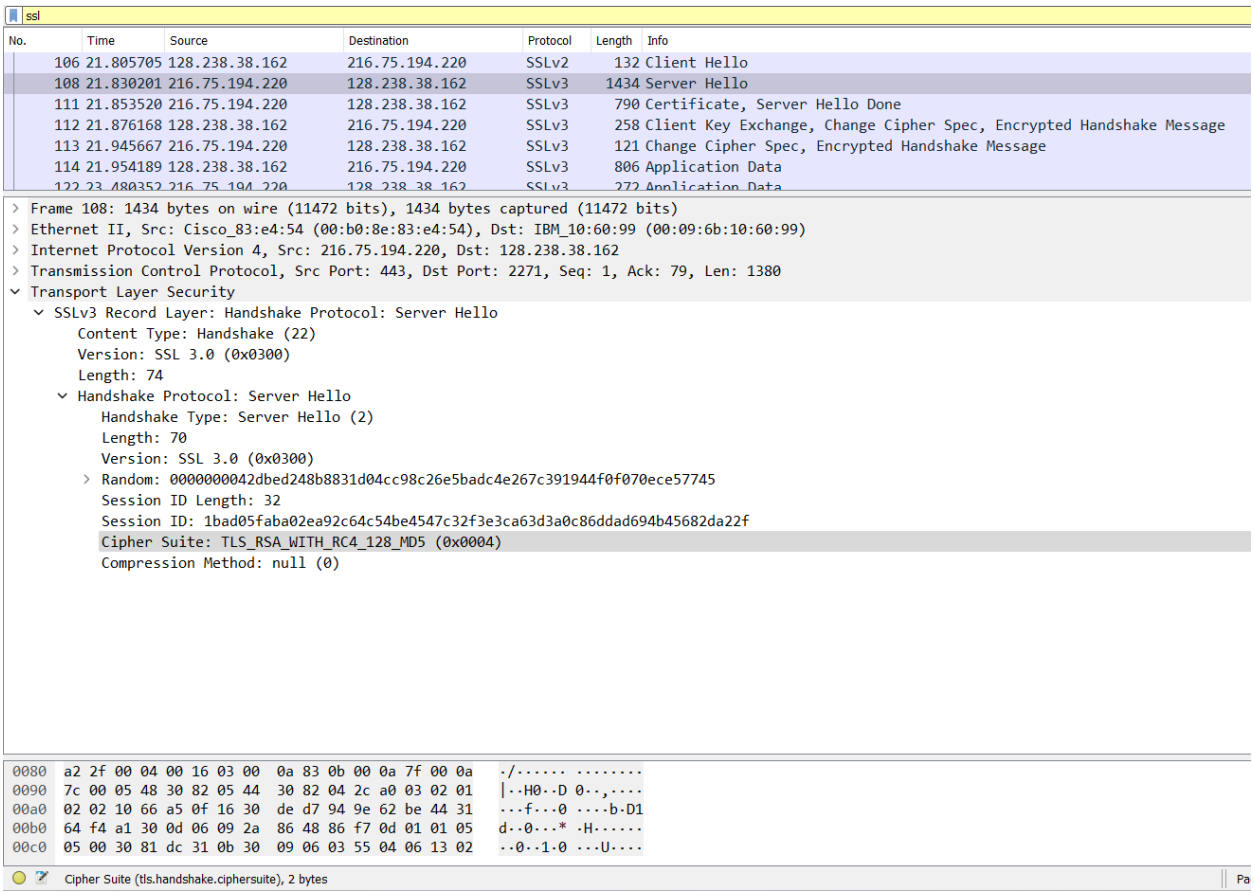
Hash algorithm: MD5

6/

Public key algorithm: RSA

Symmetric-key algorithm: RC4

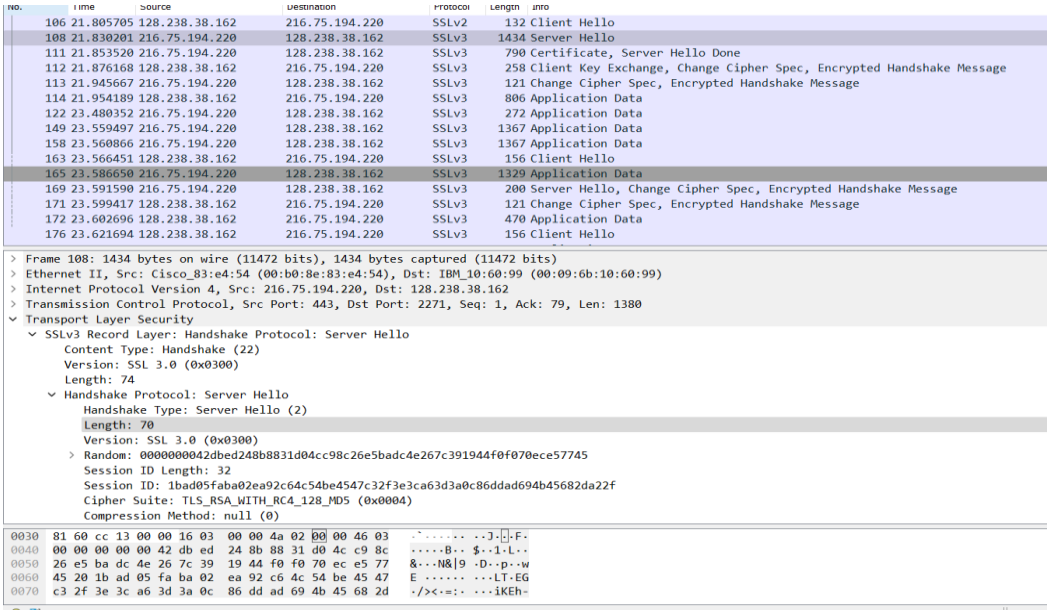
Hash algorithm: MD5



7/

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

8/



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/

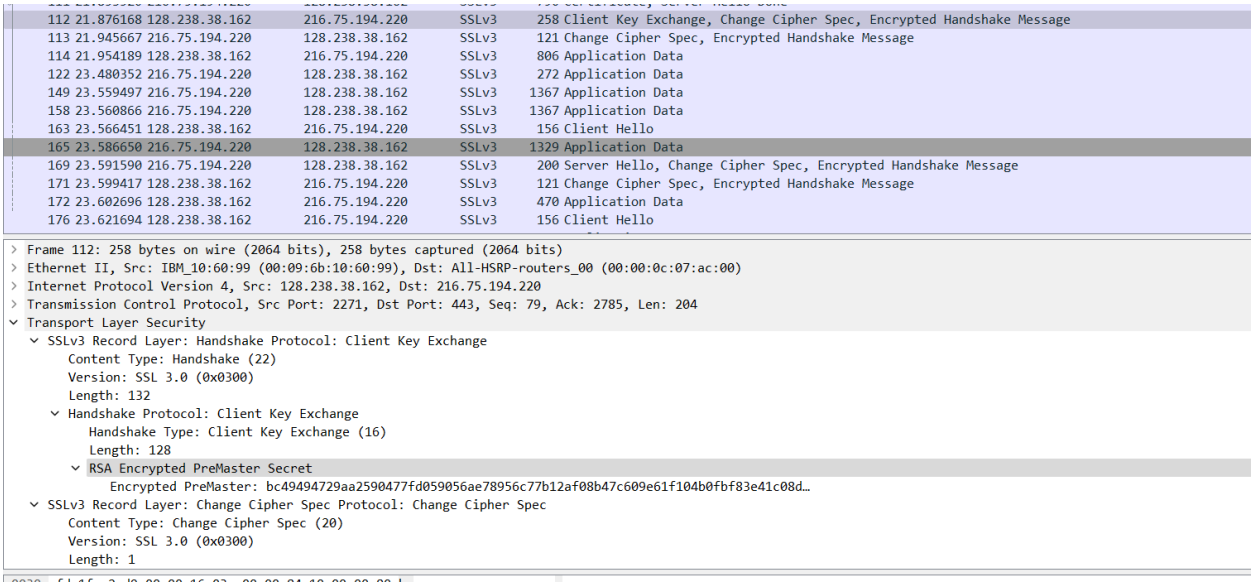
No, there is no certificate in this record. The certificate is in the separate record. Yes, the certificate fit into a single Ethernet frame.

10/

Yes, this record contain a pre-master secret.

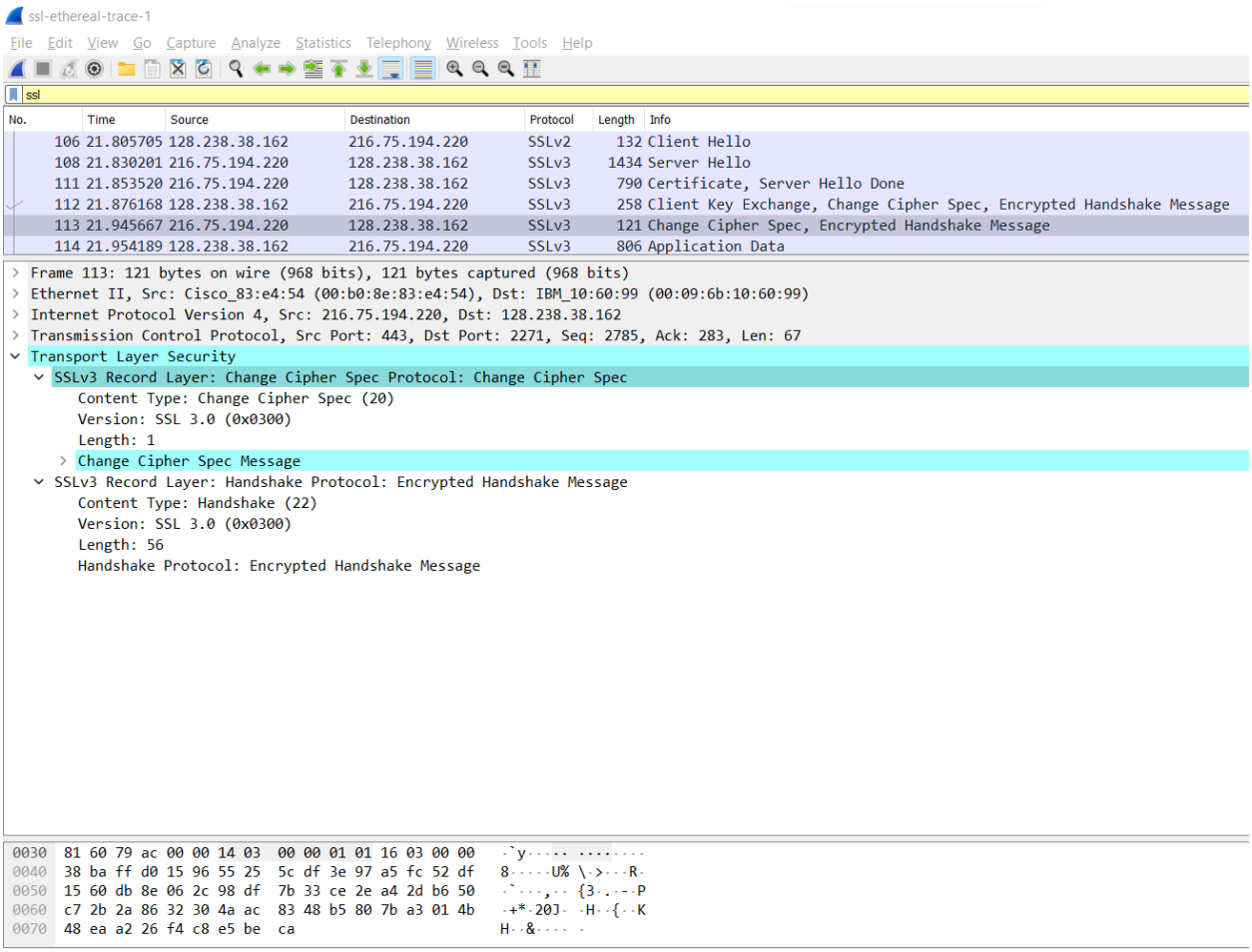
This secret is used for creating master secrect.

The secret is encrypted by public key, the encrypted secret is 120 bytes.



11/

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



12/

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

13/

Yes, the server also send a change cipher record and an encrypted handshake record to the client.

14/

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/ No comment.