

# Computer Networks 1

## Lab 8

### Wireshark Lab: SSL v8.0

Student Name: Nguyễn Quý Hải

Student No.: 2052974

#### I. Objectives

In this lab, we'll explore several aspects of the HTTP protocol:

- Investigate the IP protocol
- Focusing on the IP datagram
- Investigate the various fields in the IP datagram
- Study IP fragmentation in detail

#### II. Content

##### 1. Capturing packets from an execution of traceroute

- Following the lab's guide.

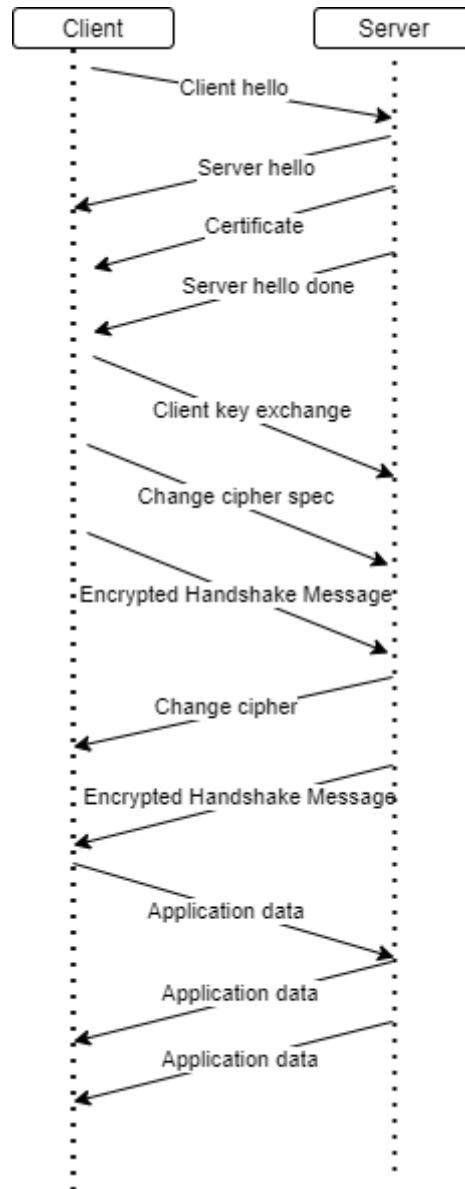
##### 2. A look at the captured trace

- Q1: 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:

Frame	Source	SSL records	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
149	Server	1	Application data



[ Timing diagram between client and server]

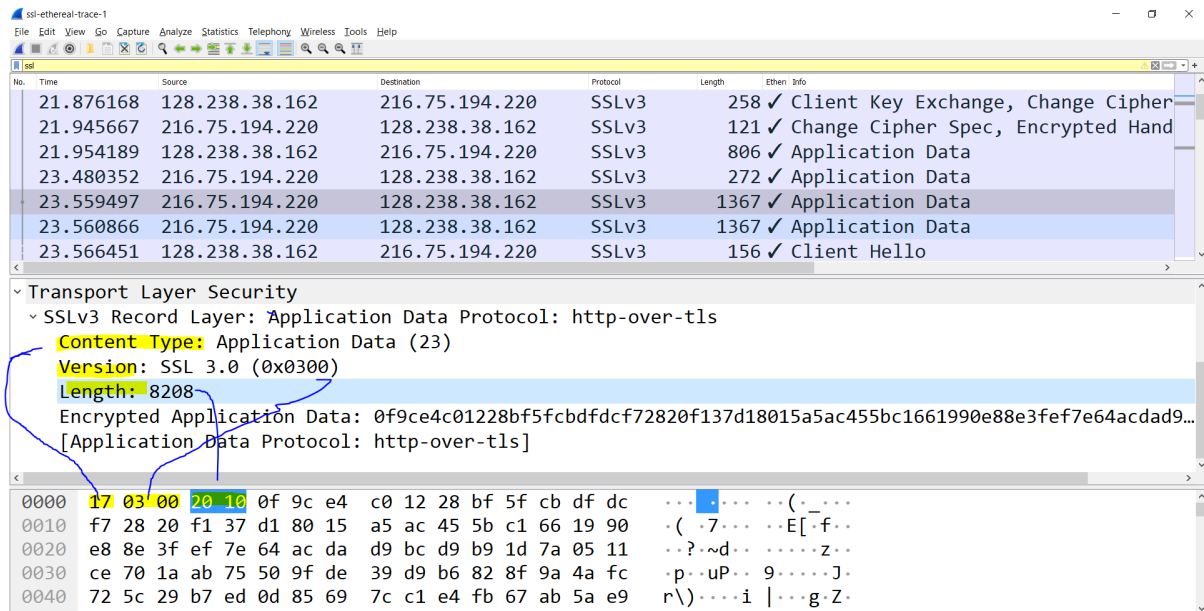
My source link:

<https://drive.google.com/file/d/1LGOCFhLzkXm01LXgA9WboECE7dF5fORW/view?usp=sharing>

- Q2. 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



Wireshark capture of an SSLv3 record. The record is expanded to show the Content Type (Application Data), Version (SSL 3.0), and Length (8208). The encrypted application data is shown in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Ethernet Info
21.876168		128.238.38.162	216.75.194.220	SSLv3	258	✓ Client Key Exchange, Change Cipher
21.945667		216.75.194.220	128.238.38.162	SSLv3	121	✓ Change Cipher Spec, Encrypted Hand
21.954189		128.238.38.162	216.75.194.220	SSLv3	806	✓ Application Data
23.480352		216.75.194.220	128.238.38.162	SSLv3	272	✓ Application Data
23.559497		216.75.194.220	128.238.38.162	SSLv3	1367	✓ Application Data
23.560866		216.75.194.220	128.238.38.162	SSLv3	1367	✓ Application Data
23.566451		128.238.38.162	216.75.194.220	SSLv3	156	✓ Client Hello

Transport Layer Security

SSLv3 Record Layer: Application Data Protocol: http-over-tls

Content Type: Application Data (23)

Version: SSL 3.0 (0x0300)

Length: 8208

Encrypted Application Data: 0f9ce4c01228bf5fcbdfdcf72820f137d18015a5ac455bc1661990e88e3fef7e64acdad9...

[Application Data Protocol: http-over-tls]

0000 17 03 00 20 10 0f 9c e4 c0 12 28 bf 5f cb df dc ... .. ( \_ ...

0010 f7 28 20 f1 37 d1 80 15 a5 ac 45 5b c1 66 19 90 ... ( .7... ..E[.f...

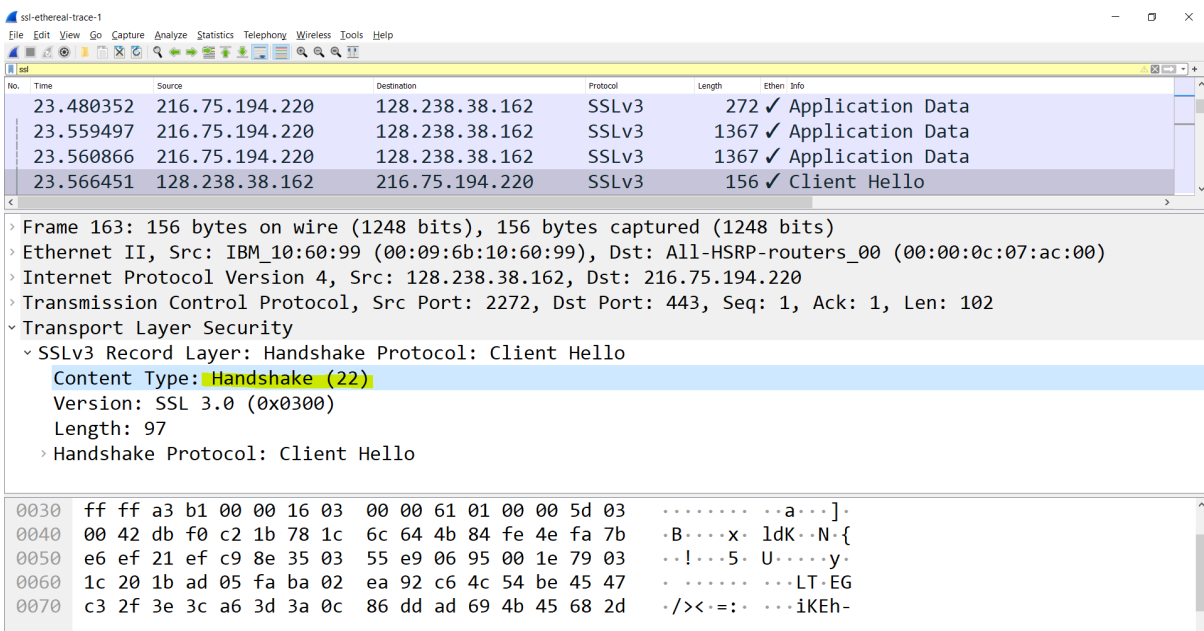
0020 e8 8e 3f ef 7e 64 ac da d9 bc d9 b9 1d 7a 05 11 ... ? ~ d ... ..z...

0030 ce 70 1a ab 75 50 9f de 39 d9 b6 82 8f 9a 4a fc ... p ..uP... 9... ..J...

0040 72 5c 29 b7 ed 0d 85 69 7c c1 e4 fb 67 ab 5a e9 ... r\)... ..i |...g.Z...

- Q3: 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: It is 22 (Handshake)



Wireshark capture of an SSLv3 record. The record is expanded to show the Content Type (Handshake), Version (SSL 3.0), and Length (97). The handshake protocol is shown in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Ethernet Info
23.480352		216.75.194.220	128.238.38.162	SSLv3	272	✓ Application Data
23.559497		216.75.194.220	128.238.38.162	SSLv3	1367	✓ Application Data
23.560866		216.75.194.220	128.238.38.162	SSLv3	1367	✓ Application Data
23.566451		128.238.38.162	216.75.194.220	SSLv3	156	✓ Client Hello

Frame 163: 156 bytes on wire (1248 bits), 156 bytes captured (1248 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: 2272, Dst Port: 443, Seq: 1, Ack: 1, Len: 102

Transport Layer Security

SSLv3 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: SSL 3.0 (0x0300)

Length: 97

Handshake Protocol: Client Hello

0030 ff ff a3 b1 00 00 16 03 00 00 61 01 00 00 5d 03 ... ..a...]

0040 00 42 db f0 c2 1b 78 1c 6c 64 4b 84 fe 4e fa 7b ... B...x..ldK..N{

0050 e6 ef 21 ef c9 8e 35 03 55 e9 06 95 00 1e 79 03 ... !...5..U...y.

0060 1c 20 1b ad 05 fa ba 02 ea 92 c6 4c 54 be 45 47 ... ..LT.EG

0070 c3 2f 3e 3c a6 3d 3a 0c 86 dd ad 69 4b 45 68 2d ... /><.=:..iKEh-

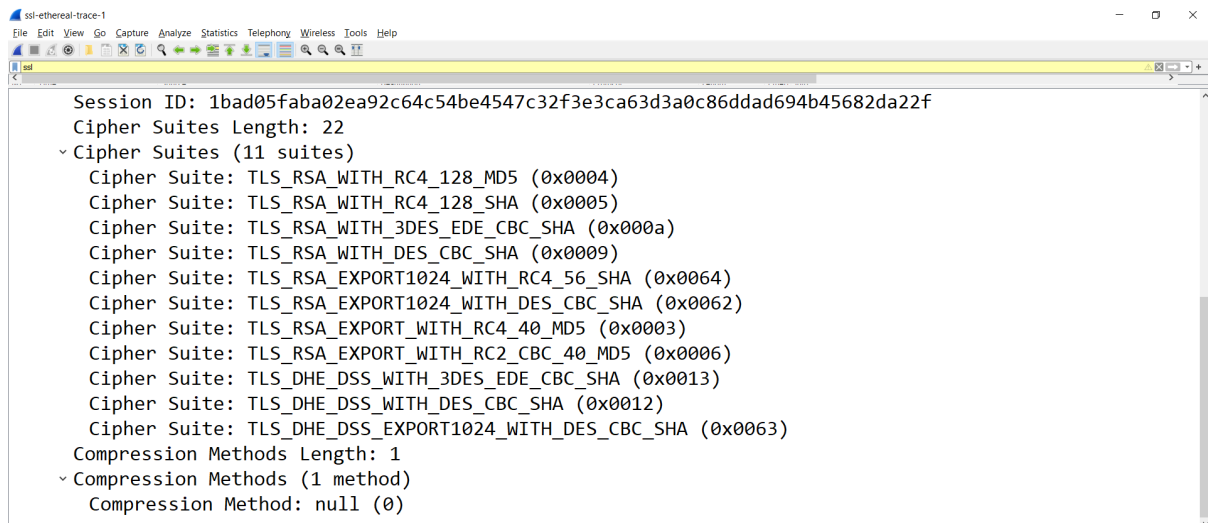
- Q4. Does the ClientHello record contain a nonce (also known as a “challenge”)? If so, what is the value of the challenge in hexadecimal notation?

**Answer:**

- Q5. 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:** Yes

- Public-key algorithm: RSA
- Symmetric-key algorithm: RC4, DES, 3DES,
- Hash algorithm: MD5, SHA

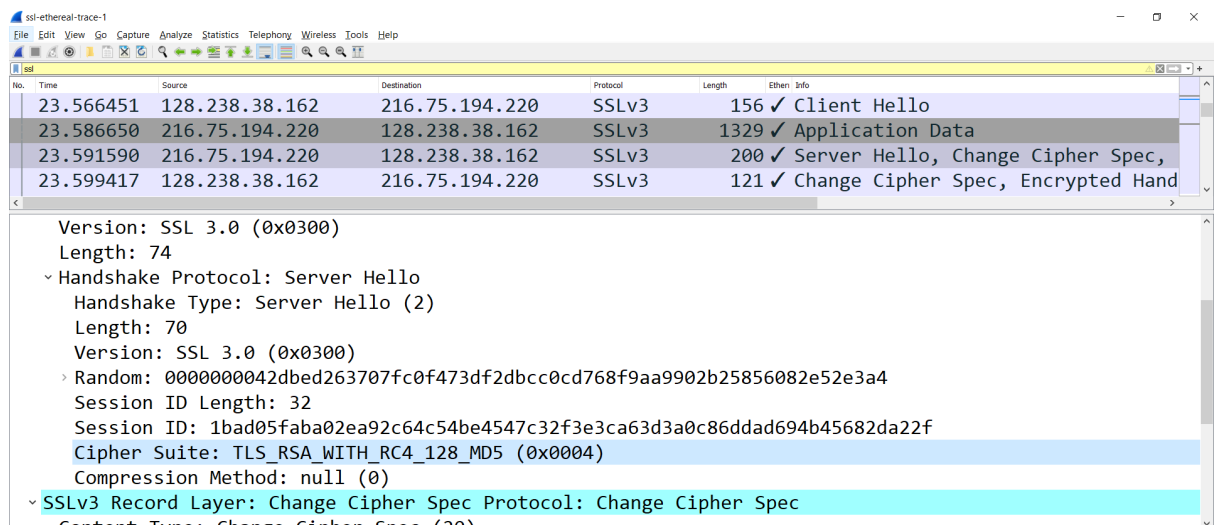


```

Session ID: 1bad05faba02ea92c64c54be4547c32f3e3ca63d3a0c86ddad694b45682da22f
Cipher Suites Length: 22
✓ Cipher Suites (11 suites)
  Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
  Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
  Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
  Cipher Suite: TLS_RSA_WITH_DES_CBC_SHA (0x0009)
  Cipher Suite: TLS_RSA_EXPORT1024_WITH_RC4_56_SHA (0x0064)
  Cipher Suite: TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA (0x0062)
  Cipher Suite: TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x0003)
  Cipher Suite: TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x0006)
  Cipher Suite: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)
  Cipher Suite: TLS_DHE_DSS_WITH_DES_CBC_SHA (0x0012)
  Cipher Suite: TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA (0x0063)
Compression Methods Length: 1
✓ Compression Methods (1 method)
  Compression Method: null (0)
  
```

- Q6: Locate the ServerHello SSL record. Does this record specify a chosen cipher suite? What are the algorithms in the chosen cipher suite?

**Answer:** Yes, it is Cipher Suite: TLS\_RSA\_WITH\_RC4\_128\_MD5 (0x0004)



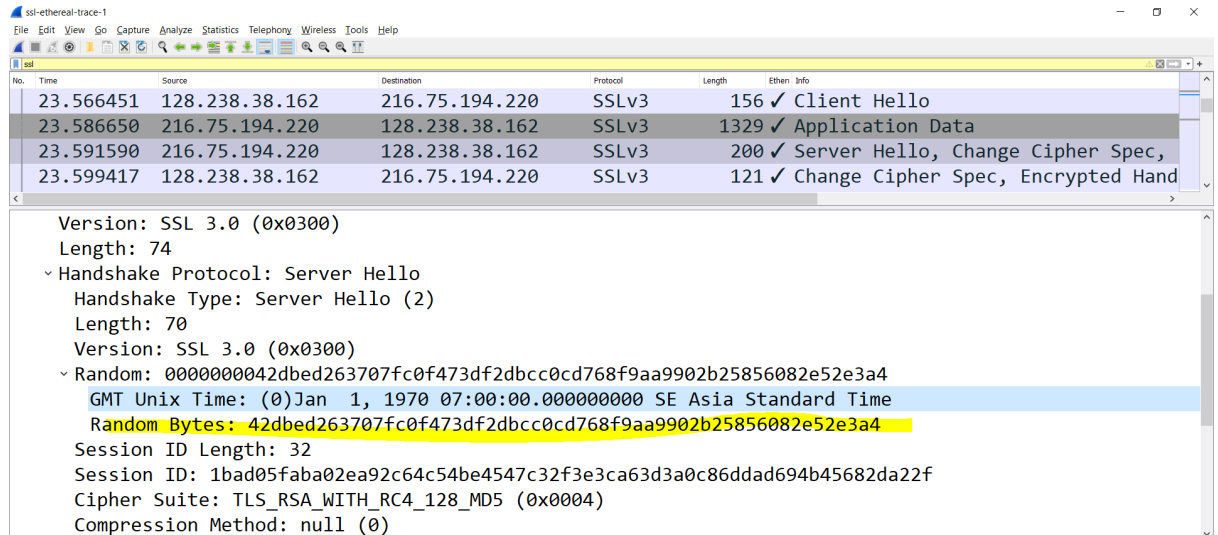
No.	Time	Source	Destination	Protocol	Length	Ether. Info
23.566451	128.238.38.162	216.75.194.220	SSLv3	156	✓ Client Hello	
23.586650	216.75.194.220	128.238.38.162	SSLv3	1329	✓ Application Data	
23.591590	216.75.194.220	128.238.38.162	SSLv3	200	✓ Server Hello, Change Cipher Spec,	
23.599417	128.238.38.162	216.75.194.220	SSLv3	121	✓ Change Cipher Spec, Encrypted Handshake	

```

Version: SSL 3.0 (0x0300)
Length: 74
✓ Handshake Protocol: Server Hello
  Handshake Type: Server Hello (2)
  Length: 70
  Version: SSL 3.0 (0x0300)
  Random: 0000000042dbed263707fc0f473df2dbcc0cd768f9aa9902b25856082e52e3a4
  Session ID Length: 32
  Session ID: 1bad05faba02ea92c64c54be4547c32f3e3ca63d3a0c86ddad694b45682da22f
  Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
  Compression Method: null (0)
✓ SSLv3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
  Content Type: Change Cipher Spec (20)
  
```

- Q7. 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. Altogether, it is 32 bytes. 4 bytes for GMT Unix time and 28 bytes for data. The purpose of this is to prevent a replay attack.



No.	Time	Source	Destination	Protocol	Length	Ethernet Info
23.566451		128.238.38.162	216.75.194.220	SSLv3	156	✓ Client Hello
23.586650		216.75.194.220	128.238.38.162	SSLv3	1329	✓ Application Data
23.591590		216.75.194.220	128.238.38.162	SSLv3	200	✓ Server Hello, Change Cipher Spec,
23.599417		128.238.38.162	216.75.194.220	SSLv3	121	✓ Change Cipher Spec, Encrypted Hand

Version: SSL 3.0 (0x0300)  
Length: 74  
Handshake Protocol: Server Hello  
Handshake Type: Server Hello (2)  
Length: 70  
Version: SSL 3.0 (0x0300)  
Random: 0000000042dbed263707fc0f473df2dbcc0cd768f9aa9902b25856082e52e3a4  
GMT Unix Time: (0)Jan 1, 1970 07:00:00.00000000 SE Asia Standard Time  
Random Bytes: 42dbed263707fc0f473df2dbcc0cd768f9aa9902b25856082e52e3a4  
Session ID Length: 32  
Session ID: 1bad05faba02ea92c64c54be4547c32f3e3ca63d3a0c86ddad694b45682da22f  
Cipher Suite: TLS\_RSA\_WITH\_RC4\_128\_MD5 (0x0004)  
Compression Method: null (0)

- Q8. Does this record include a session ID? What is the purpose of the session ID?

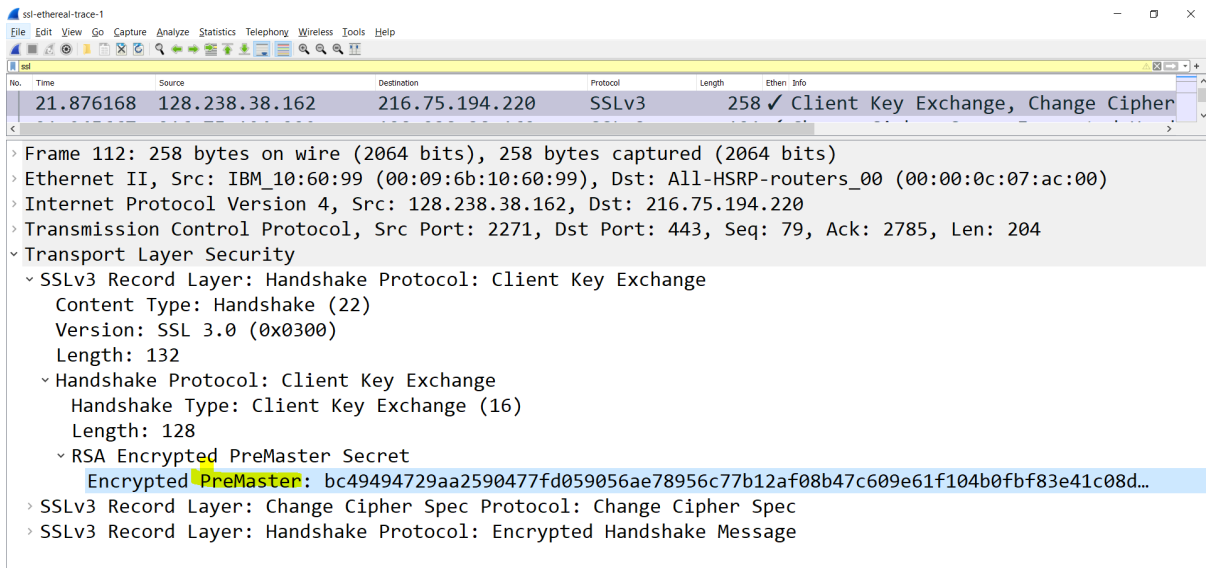
**Answer:** Yes, as you can see in the screenshot above. The main purpose of the session ID is to identify a session, a series of related message exchanges. In E-commerce, it is often used to identify a user that has logged into a website.

- Q9. 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:** There is no certificate in this record, it is in another record. It does fit into a single Ethernet frame.

- Q10: 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?

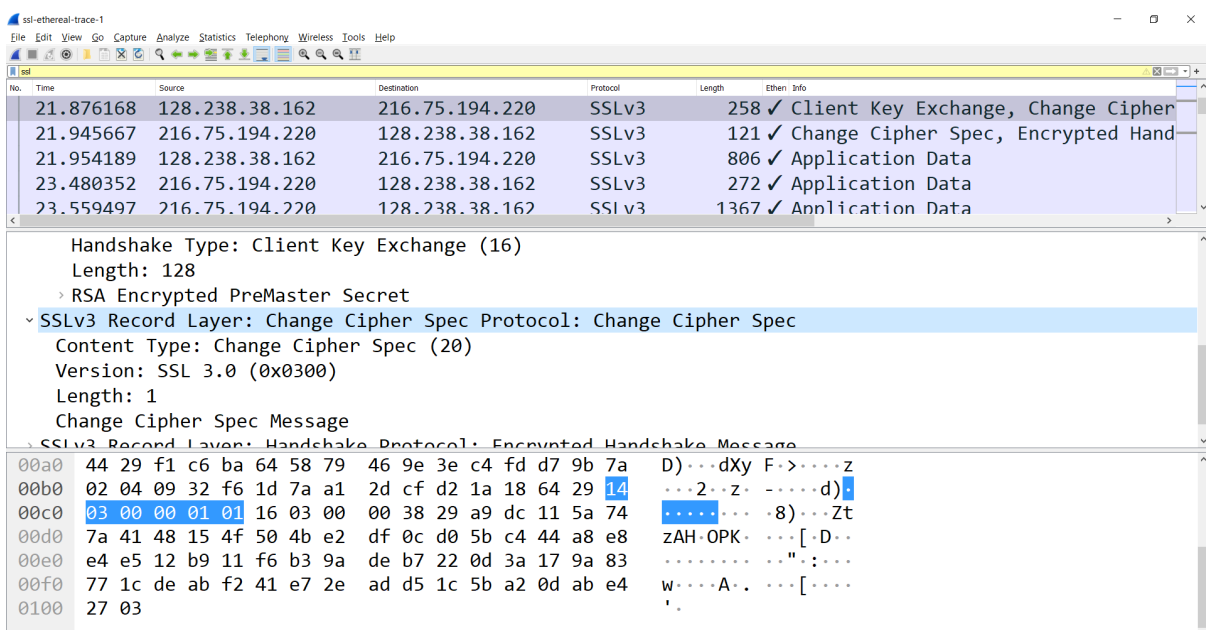
**Answer:** Yes, it does contain a premaster secret. It is used by both the server and client to make a master secret, which is used to generate session keys for MAC and encryption. The secret gets encrypted using the server's public key, which the client extracted from the certificate sent by the server. The secret is 128 bytes long



- Q11: What is the purpose of the Change Cipher Spec record? How many bytes is the record in your trace?

**Answer:** The purpose of the Change Cipher Spec record is to indicate that the contents of the following SSL records sent by the client (data, not header) will be encrypted. The record in my trace is 6 bytes:

- 1 byte for Content type,
- 2 bytes for version,
- 2 bytes for length
- And the last for Change Cipher Spec Message



- Q12. In the encrypted handshake record, what is being encrypted? How?

**Answer:** In the encrypted handshake record, a MAC of the concatenation of all the previous handshake messages sent from this client is generated, encrypted and sent to the server.

- Q13. 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 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.

- Q14: 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:** Application data is encrypted using symmetric key encryption algorithm chosen in the handshake phase (RC4) using the keys generated using the pre-master key and nonces from both client and server. The client encryption key is used to encrypt the data being sent from client to server and the server encryption key is used to encrypt the data being sent from the server to the client.

- Q15. Comment on and explain anything else that you found interesting in the trace.

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

Also, during resumes the handshake process is slightly different from the initial one. The client does not need another cert so the server never sends it. It just has to send a new nonce followed by Change Cipher Spec and Encrypted Handshake records from the server to the client. After a response from the client then application data can be sent.