

Họ tên : Lê Bảo Khánh
MSSV : 1911363
Lớp : L01

LAB 8

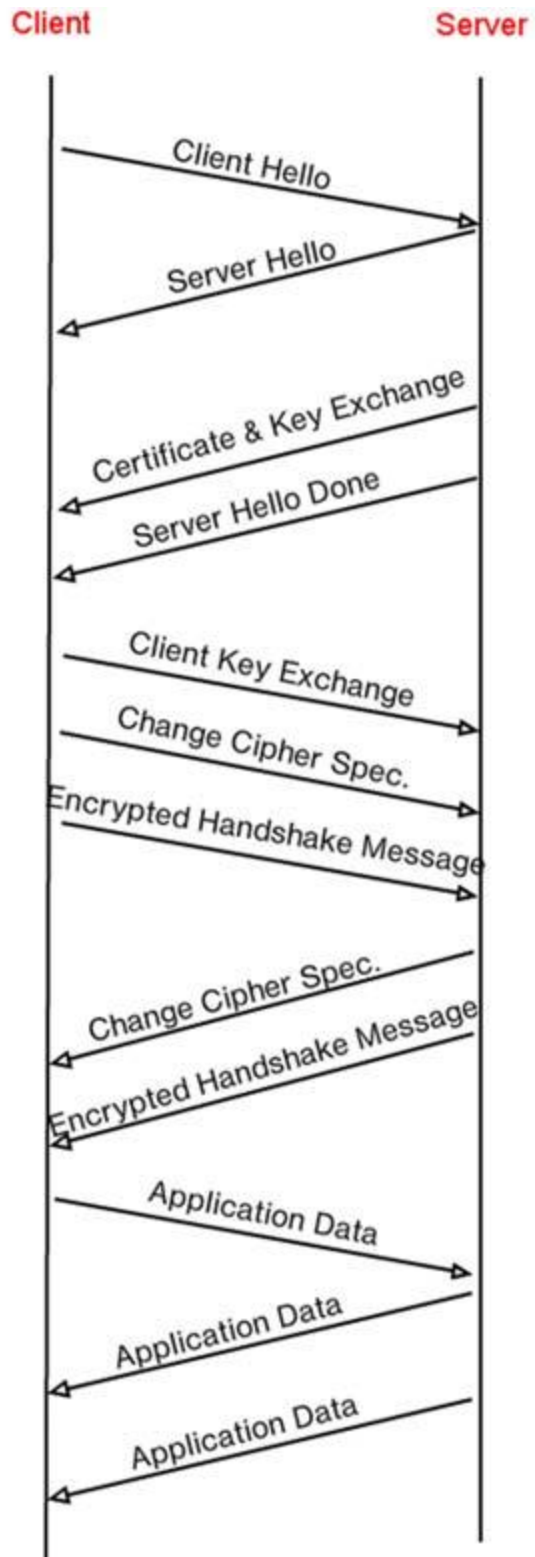
(using the file ssl-etherealtrace-1 packet trace)

Question 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.

ANSWER:

No.	Frame	Source	Destination	SSL Count	SSL Type
1	106	128.238.38.162	216.75.194.220	1	Client Hello
2	108	216.75.194.220	128.238.38.162	1	Server Hello
3	111	216.75.194.220	128.238.38.162	2	Server Hello Done
4	112	128.238.38.162	216.75.194.220	3	Client Key Exchange
5	113	216.75.194.220	128.238.38.162	2	Change Cipher Spec
6	114	128.238.38.162	216.75.194.220	1	Application Data
7	122	216.75.194.220	128.238.38.162	1	Application Data
8	149	216.75.194.220	128.238.38.162	1	Application Data

No.	Time	Source	Destination	Protocol	Length	Info
106	21.885705	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	23.568066	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



Question 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.

ANSWER:

Content Type = 1 byte

Version = 2 bytes

Length = 2 bytes

The image shows a Wireshark capture of an SSLv3 handshake. The top pane displays a list of packets, with packet 108 selected. The middle pane shows the details of packet 108, highlighting the 'Content Type: Handshake (22)' field. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Packet 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

Transport Layer Security

SSLv3 Record Layer: Handshake Protocol: Server Hello

Content Type: Handshake (22)

Version: SSL 3.0 (0x0300)

Length: 74

Handshake Protocol: Server Hello

Raw packet data (hex):

```
0030  01 60 cc 13 00 00 16 03 00 00 4a 02 00 00 46 03  ....B...$.J...F...
0040  00 00 00 00 00 42 db ed 24 8b 88 31 00 4c c9 8c  ....B...$.1.L...
0050  26 e5 ba dc 4e 26 7c 39 19 44 f0 f0 70 ec e5 77  &...N&[9 .D.p.w...
0060  45 20 1b ad 05 fa ba 02 ea 92 c6 4c 54 be 45 47  E.....LT.EG...
0070  c3 2f 3e 3c a6 3d 3a 0c 86 dd ad 69 4b 45 68 2d  /><=:...iKEh-...
0080  a2 2f 00 04 00 16 03 00 0a 83 0b 00 0a 7f 00 0a  /.....
```

Content Type (tls.record.content_type), 1 byte(s)

Packets: 336 · Displayed: 59 (17.6%)

Profile: Default

> 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

▼ Transport Layer Security

 ▼ SSLv3 Record Layer: Handshake Protocol: Server Hello

 Content Type: Handshake (22)

 Version: SSL 3.0 (0x0300)

 Length: 74

 > Handshake Protocol: Server Hello

0030 81 60 cc 13 00 00 16 05 00 00 4a 02 00 00 46 03J...F..

0040 00 00 00 00 00 42 db ed 24 8b 88 31 d0 4c c9 8cB...\$.1.L..

0050 26 e5 ba dc 4e 26 7c 39 19 44 f0 f0 70 ec e5 77 &...N&[9 .D: p:w

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

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

0080 a2 2f 00 04 00 16 03 00 0a 83 0b 00 0a 7f 00 0a -/.....

Record layer version (tls.record.version), 2 byte(s) Packets: 336 · Displayed: 59 (17.6%) Profile: Default

> 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

▼ Transport Layer Security

 ▼ SSLv3 Record Layer: Handshake Protocol: Server Hello

 Content Type: Handshake (22)

 Version: SSL 3.0 (0x0300)

 Length: 74

 > Handshake Protocol: Server Hello

0030 81 60 cc 13 00 00 16 03 00 00 4a 02 00 00 46 03J...F..

0040 00 00 00 00 00 42 db ed 24 8b 88 31 d0 4c c9 8cB...\$.1.L..

0050 26 e5 ba dc 4e 26 7c 39 19 44 f0 f0 70 ec e5 77 &...N&[9 .D: p:w

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

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

0080 a2 2f 00 04 00 16 03 00 0a 83 0b 00 0a 7f 00 0a -/.....

Length of TLS record data (tls.record.length), 2 byte(s) Packets: 336 · Displayed: 59 (17.6%) Profile: Default

ClientHello Record:

Question 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?

ANSWER:

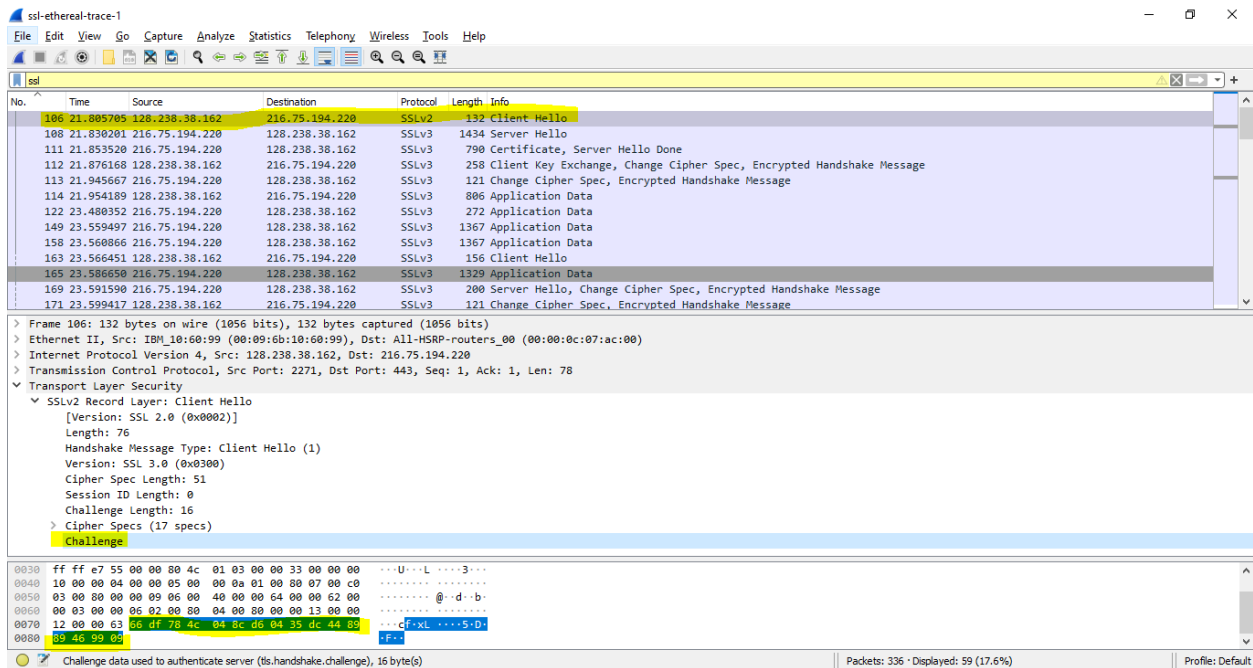
Content type: 22

Question 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?

ANSWER:

Yes

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



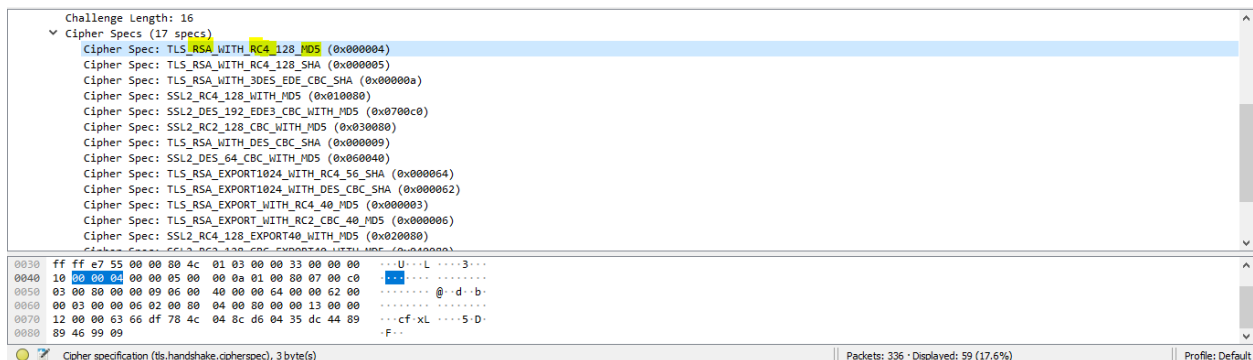
Question 5: Does the ClientHello record advertise the cyber suites it supports? If so, in the first listed suite, what are the public-key algorithm, the symmetric-key algorithm, and the hash algorithm?

ANSWER:

Public key algorithm: RSA

Symmetric-key algorithm: RC4

Hash algorithm: MD5

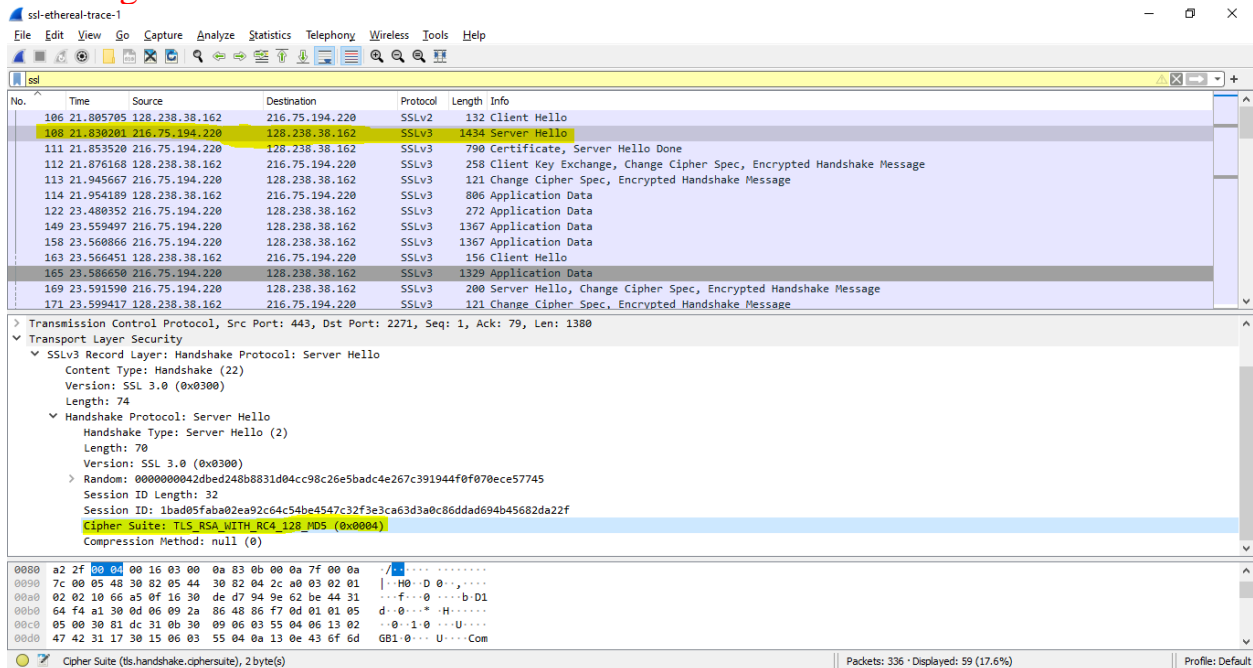


ServerHello Record:

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

ANSWER:

Public key algorithm: RSA
Symmetric-key algorithm: RC4
Hash algorithm: MD5



Question 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?

ANSWER:

Yes

32 bits long = 28bits data + 4 bits time

It is used for attack preventing.

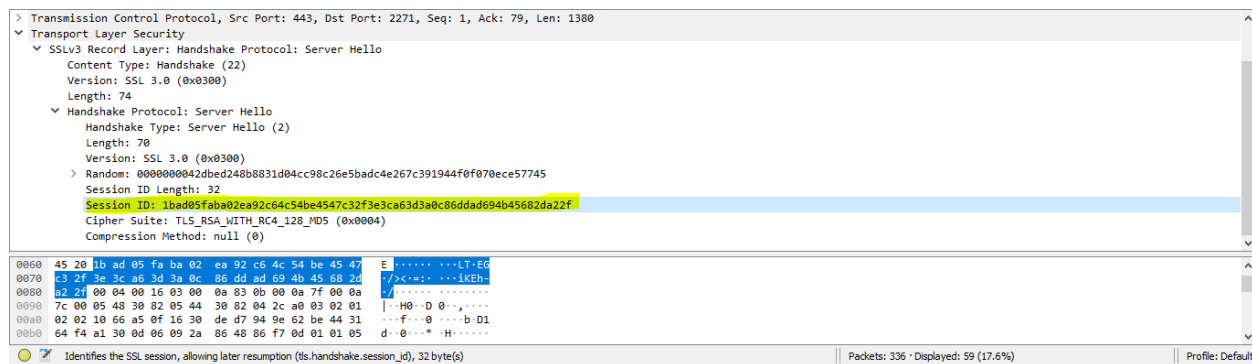
Question 8: Does this record include a session ID? What is the purpose of the session ID?

ANSWER:

Yes

The session ID in the record is an identifier for SSL session.

=> Let the client to resume the session later by using the session ID.



Question 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?

ANSWER:

No, there is no certificate in this record. The certificate is in the separate record.
Yes, the certificate fit into a 1 Ethernet frame.

Client Key Exchange Record:

Question 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?

ANSWER:

Yes, there is 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

ssl-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

Transport Layer Security

- SSLv3 Record Layer: Handshake Protocol: Client Key Exchange
 - Content Type: Handshake (22)
 - Version: SSL 3.0 (0x0300)
 - Length: 132
 - Handshake Protocol: Client Key Exchange
 - Handshake Type: Client Key Exchange (16)
 - Length: 128
 - RSA Encrypted PreMaster Secret
- 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
- SSLv3 Record Layer: Handshake Protocol: Encrypted Handshake Message
 - Content Type: Handshake (22)

0030 fd 1f c2 d9 00 00 16 03 00 00 84 10 00 00 80 3c
 0040 49 49 47 29 aa 25 90 47 7f d0 59 05 6a e7 89 56 IIG)X%G -Y-j-V
 0050 c7 b0 12 af 08 b4 7c 60 9e 61 f1 04 b0 fb f8 3e {...}~a+...+
 0060 41 c0 8d c9 10 93 9c ad 1e ce 02 e0 dd e2 50 b9 A+...+...P+
 0070 0b 4b 51 c7 2f ad ee cd 92 c4 27 5d ff d0 fb 95 KQ?...+...
 0080 42 3d a4 b7 71 ee c0 ff c3 ce b2 ed 60 90 6c d7 B+q+...+...l
 0090 04 6e 5a 00 98 2c 52 ee b5 bc d1 c4 f5 63 f0 a3 +NZ+.R+...+...
 00a0 44 29 f1 c6 ba 64 58 79 46 9e 3e c4 fd d7 9b 7a D)....dxy P>...+...
 00b0 02 04 09 32 f6 1d 7a a1 2d cf d2 1a 18 64 29 1c ...2...z...d...
 00c0 03 00 00 01 01 16 03 00 00 38 29 a9 dc 11 5a 748)....Zt

Text item (text), 128 byte(s) | Packets: 336 · Displayed: 59 (17.6%) | Profile: Default

Change Cipher Spec Record (sent by client) and Encrypted Handshake Record:

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

ANSWER:

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

ssl-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

Transport Layer Security

- SSLv3 Record Layer: Handshake Protocol: Client Key Exchange
 - Content Type: Handshake (22)
 - Version: SSL 3.0 (0x0300)
 - Length: 132
 - Handshake Protocol: Client Key Exchange
 - Handshake Type: Client Key Exchange (16)
 - Length: 128
 - RSA Encrypted PreMaster Secret
- 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
- SSLv3 Record Layer: Handshake Protocol: Encrypted Handshake Message
 - Content Type: Handshake (22)
 - Version: SSL 3.0 (0x0300)
 - Length: 56
 - Handshake Protocol: Encrypted Handshake Message

00b0 02 04 09 32 f6 1d 7a a1 2d cf d2 1a 18 64 29 1c ...2...z...d...
 00c0 03 00 00 01 01 16 03 00 00 38 29 a9 dc 11 5a 748)....Zt
 00d0 7a 41 48 15 4f 50 4b e2 df 0c d0 5b c4 44 a8 e8 zAH-OPK...[D...
 00e0 e4 e5 12 b9 11 f6 b3 9a de b7 22 0d 3a 17 9a 03+...+...
 00f0 77 1c de ab f2 41 e7 2e ad d5 1c 5b a2 0d ab e4 W+...A+...[...
 0100 27 03

Record Layer (tls.record), 6 byte(s) | Packets: 336 · Displayed: 59 (17.6%) | Profile: Default

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

ANSWER:

Handshake messages + MAC addresses are concatenated and encrypted, then they are sent to the server.

Question 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?

ANSWER:

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

Application Data:

Question 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?

ANSWER:

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.

Question 15: 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

Moreover, 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 client. The application data can be sent after a response from the client