

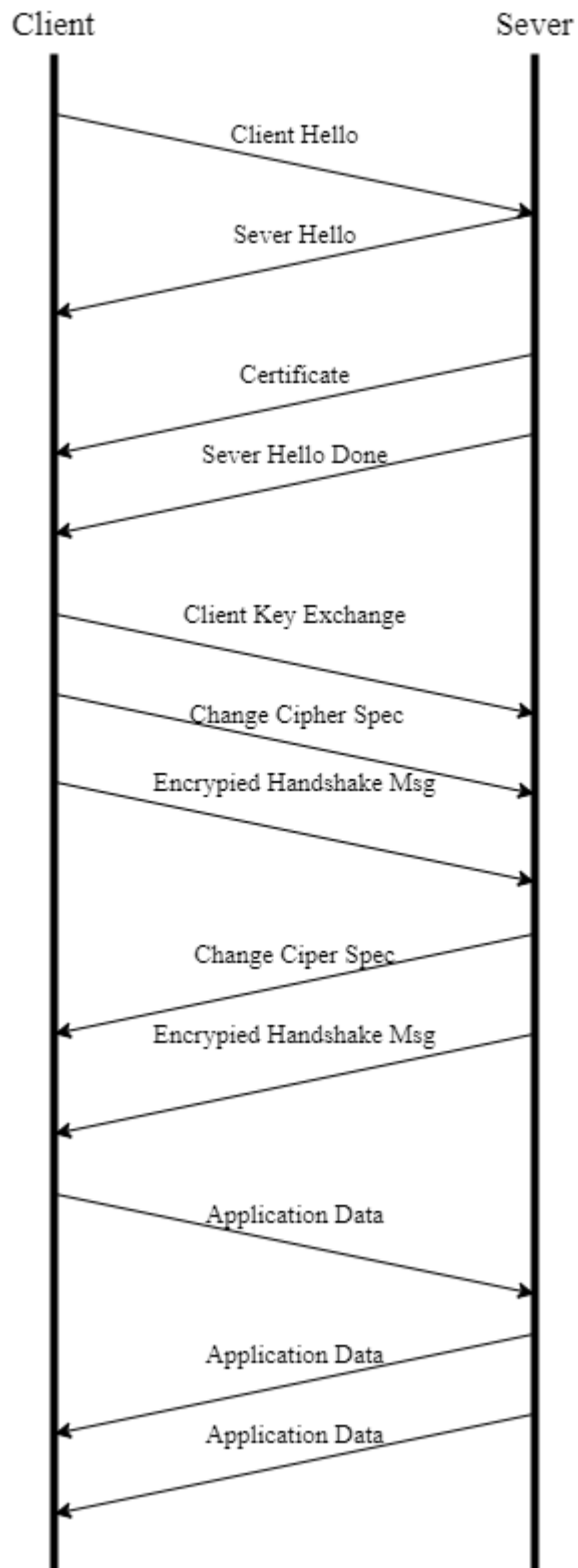
Lab_8a_Wireshark_SSL_v8.0

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.	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

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

Answer:

- Content Type: 1 byte

- Version: 2 bytes
- Length: 2 bytes

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 03	..J..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	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	./.....
0090	7c 00 05 48 30 82 05 44 30 82 04 2c a0 03 02 01	..H0.D0.,...
00a0	02 02 10 66 a5 0f 16 30 de d7 94 9e 62 be 44 31	...f..0...b.D1
00b0	64 f4 a1 30 0d 06 09 2a 86 48 86 f7 0d 01 01 05	d..0...*..H.....
00c0	05 00 30 81 dc 31 0b 30 09 06 03 55 04 06 13 02	..0..1.0...U....
00d0	47 42 31 17 30 15 06 03 55 04 0a 13 0e 43 6f 6d	GB1.0...U....Com
00e0	6f 64 6f 20 4c 69 6d 69 74 65 64 31 1d 30 1b 06	odo Limi ted1.0..

Content Type (tls.record.content_type) 1 byte

Transport Layer Security

SSLv3 Record Layer: Handshake Protocol: Server Hello

Content Type: Handshake (22)

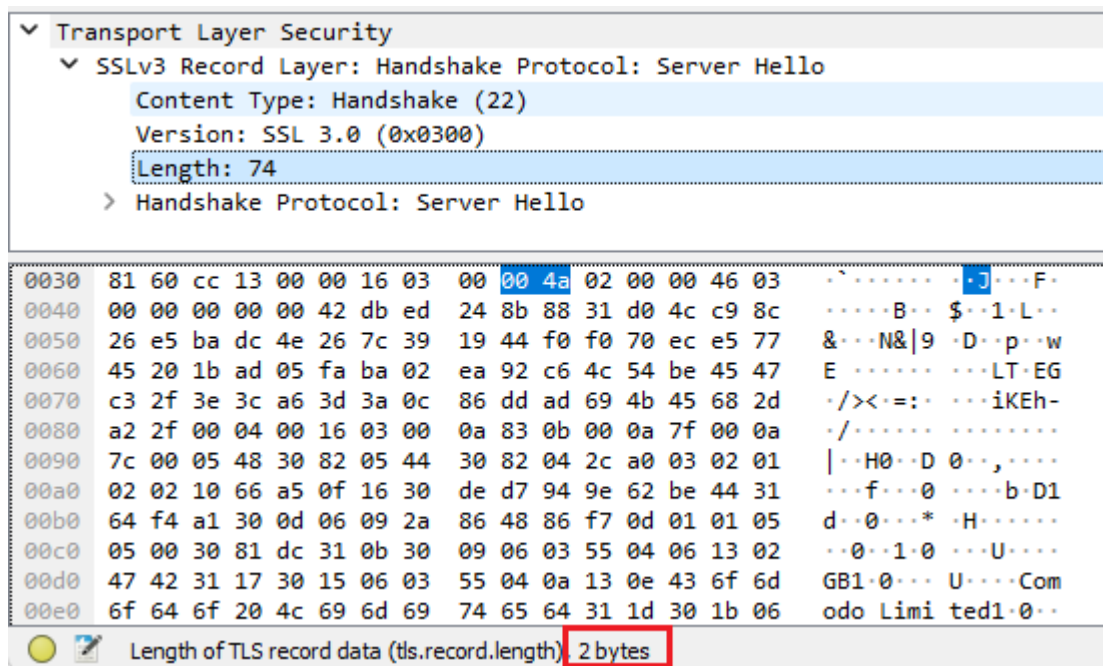
Version: SSL 3.0 (0x0300)

Length: 74

> Handshake Protocol: Server Hello

0030	81 60 cc 13 00 00 16 03 00 00 4a 02 00 00 46 03	..J..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	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	./.....
0090	7c 00 05 48 30 82 05 44 30 82 04 2c a0 03 02 01	..H0.D0.,...
00a0	02 02 10 66 a5 0f 16 30 de d7 94 9e 62 be 44 31	...f..0...b.D1
00b0	64 f4 a1 30 0d 06 09 2a 86 48 86 f7 0d 01 01 05	d..0...*..H.....
00c0	05 00 30 81 dc 31 0b 30 09 06 03 55 04 06 13 02	..0..1.0...U....
00d0	47 42 31 17 30 15 06 03 55 04 0a 13 0e 43 6f 6d	GB1.0...U....Com
00e0	6f 64 6f 20 4c 69 6d 69 74 65 64 31 1d 30 1b 06	odo Limi ted1.0..

Record layer version (tls.record.version) 2 bytes



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

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, Cha
188	23.662642	128.238.38.162	216.75.194.220	SSLv3	121 Change Cipher Spec
189	23.665695	128.238.38.162	216.75.194.220	SSLv3	476 Application Data
190	23.666238	128.238.38.162	216.75.194.220	SSLv3	156 Client Hello
192	23.666377	216.75.194.220	128.238.38.162	SSLv3	378 Application Data

```
> Frame 176: 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:0
> Internet Protocol Version 4, Src: 128.238.38.162, Dst: 216.75.194.220
> Transmission Control Protocol, Src Port: 2273, 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
      Handshake Type: Client Hello (1)
      Length: 93
      Version: SSL 3.0 (0x0300)
      > Random: 42dbf0c2033de6c8af29184c919a336821965ccec631bf56181b19381cdc3049
      Session ID Length: 32
      Session ID: 1bad05faba02ea92c64c54be4547c32f3e3ca63d3a0c86ddad694b45682da22f
      Cipher Suites Length: 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?

Answer: The ClientHello Record contains a Challenge and it is: 66 df 78 4c 04 8c d6 04 35 dc 44 89 89 46 99 09.

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, S
112	21.876168	128.238.38.162	216.75.194.220	SSLv3	258 Client Key Excl
113	21.945667	216.75.194.220	128.238.38.162	SSLv3	121 Change Cipher :
114	21.954189	128.238.38.162	216.75.194.220	SSLv3	806 Application Da
122	23.480352	216.75.194.220	128.238.38.162	SSLv3	272 Application Da
149	23.559497	216.75.194.220	128.238.38.162	SSLv3	1367 Application Da
150	23.560355	216.75.194.220	128.238.38.162	SSLv3	1367 Application Da

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 00k.`...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 18V...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 cipher 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

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, S
112	21.876168	128.238.38.162	216.75.194.220	SSLv3	258 Client Key Exc
113	21.945667	216.75.194.220	128.238.38.162	SSLv3	121 Change Cipher
114	21.954189	128.238.38.162	216.75.194.220	SSLv3	806 Application Da
122	23.480352	216.75.194.220	128.238.38.162	SSLv3	272 Application Da


```

> 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:
> 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
▼ Transport Layer Security
  ▼ 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)
    Cipher Spec: TLS_RSA_WITH_RC4_128_MD5 (0x000004)

```

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

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, S
112	21.876168	128.238.38.162	216.75.194.220	SSLv3	258 Client Key Exc
113	21.945667	216.75.194.220	128.238.38.162	SSLv3	121 Change Cipher
114	21.954189	128.238.38.162	216.75.194.220	SSLv3	806 Application Da
122	23.480352	216.75.194.220	128.238.38.162	SSLv3	272 Application Da


```

> 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
    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?

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

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. This ID could let the client to resume the session later by using the 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?

Answer: 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?

Answer: Yes, it does contain a pre-master secret. It is used by both the server and client to make a master secret, which used to generate session keys for MAC and encryption. The secret gets encrypted using the server's public key, which the client extracted from their certificate sent by the sever. The encrypted secret is 56 bytes.

No.	Time	Source	Destination	Protocol	Length	Info
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

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

Offset	Hex	ASCII
0060	41 c0 8d c9 10 93 9c ad 1e ce 82 e0 dd e2 50 b9	A.....P
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·...·...·1·
0090	04 6e 5a 00 98 2e 52 ee b5 bc d1 c4 f5 63 f0 e3	·nZ·...R·...·c·
00a0	44 29 f1 c6 ba 64 58 79 46 9e 3e c4 fd d7 9b 7a	D)·...dXy F·>·...z
00b0	02 04 09 32 f6 1d 7a a1 2d cf d2 1a 18 64 29 14	·...2·...z·...·d)·
00c0	03 00 00 01 01 16 03 00 00 38 29 a9 dc 11 5a 74	·...·...·8)·...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 83	·...·...·...·...·...
00f0	77 1c de ab f2 41 e7 2e ad d5 1c 5b a2 0d ab e4	·w·...A·...·[·...·...
0100	27 03	·...

Handshake protocol message (tls.handshake), 56 bytes

Packets: 336 · Displayed: 1

11.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. This record is 6 bytes long: 5 for header and 1 for message segment

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

> 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

▼ Transport Layer Security

 ▼ 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

0000	00 09 6b 10 60 99 00 b0 8e 83 e4 54 08 00 45 00	..k.....T..E..
0010	00 6b 87 c1 40 00 33 06 7d 13 d8 4b c2 dc 80 ee	.k..@.3.}.K....
0020	26 a2 01 bb 08 df 4c 9e 6f 7f 56 d2 09 df 50 18	&.....L. o.V...P..
0030	81 60 79 ac 00 00 14 03 00 00 01 01 16 03 00 00	..y.....
0040	38 ba ff d0 15 96 55 25 5c df 3e 97 a5 fc 52 df	8.....U% \>...R..
0050	15 60 db 8e 06 2c 98 df 7b 33 ce 2e a4 2d b6 50	..{3...-P..
0060	c7 2b 2a 86 32 30 4a ac 83 48 b5 80 7b a3 01 4b	..+*.20J..H...{..K..
0070	48 ea a2 26 f4 c8 e5 be ca	H..&.....

Record Layer (tls.record), 6 bytes

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

Answer: 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?

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.

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.

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.
- Also, during resumes the handshake process is slightly different from the initial one. The client does not need another cert to 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. After a response from the client then application data can be sent