

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

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
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
188	23.662642	128.238.38.162	216.75.194.220	SSLv3	121 Change Cipher Spec, Encrypted Handshake Message

> 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
 > 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)
 Challenge

0030	ff ff e7 55 00 00 80 4c	01 03 00 00 33 00 00 00	...U...L3...
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..

2/

Content type : 1 byte

Version: 2 bytes

Length: 2 bytes

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
188	23.662642	128.238.38.162	216.75.194.220	SSLv3	121	Change Cipher Spec, Encrypted Handshake Message

SSLv3 Record Layer: Handshake Protocol: Server Hello

Content Type: Handshake (22)

Version: SSL 3.0 (0x0300)

Length: 74

Handshake Protocol: Server Hello

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

0030	81 60 c5 58 00 00 16 03	00 00 4a 02 00 00 46 03	...X... ..J...F..
0040	00 00 00 00 00 42 db ed	26 37 07 fc 0f 47 3d f2B... &7...G=.
0050	db cc 0c d7 68 f9 aa 99	02 b2 58 56 08 2e 52 e3	...h... ..XV..R..
0060	a4 20 1b ad 05 fa ba 02	ea 92 c6 4c 54 be 45 47LT.EG
0070	c3 2f 3e 3c a6 3d 3a 0c	86 dd ad 69 4b 45 68 2d	./><.=:.. ..iKEh-

3/

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

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
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

0000	00 00 0c 07 ac 00 00 09	6b 10 60 99 08 00 45 00 k.~...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...L3...
0040	10 00 00 04 00 00 05 00	00 0a 01 00 80 07 00 c0

4/

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..xL5.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

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

> 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)

0080a22f0004001603000a830b000a7f000a./.....

00907c000548308205443082042ca0030201|..H0..D0..,

00a002021066a50f1630ded7949e62be4431...f...0...b.D1

00b064f4a1300d06092a864886f70d010105d..0...*..H.....

00c005003081dc310b300906035504061302..0..1.0...U....

Cipher Suite (tls.handshake.ciphersuite), 2 bytes

7/

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

8/

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											
> 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)																	
0030	81	60	cc	13	00	00	16	03	00	00	4a	02	00	46	03J..F..	
0040	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	&...N8 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+

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 secret.

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

> 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 (00:00:0c: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: 79, Ack: 2785, Len: 204

> 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
 - Encrypted PreMaster: bc49494729aa2590477fd059056ae78956c77b12af08b47c609e61f104b0fbf83e41c08d...
 - SSLv3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
 - Content Type: Change Cipher Spec (20)
 - Version: SSL 3.0 (0x0300)
 - Length: 1

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.

ssl-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

> 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

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..&.....

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.