Final Year B. Tech, Sem VII 2022-23 PRN – 2020BTECS00211

Name – Aashita Narendra Gupta Cryptography And Network Security Lab Batch: B4

Practical No – 16

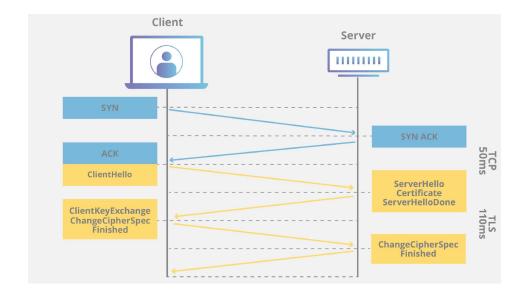
Title: To observe SSL/TLS (Secure Sockets Layer/ Transport Layer Security)in action.

Theory:

SSL

SSL (Secure Sockets Layer) and its successor, TLS (Transport Layer Security), are protocols for establishing authenticated and encrypted links between networked computers. Although the SSL protocol was deprecated with the release of TLS 1.0 in 1999, it is still common to refer to these related technologies as "SSL" or "SSL/TLS." The most current version is TLS 1.3, defined in RFC 8446

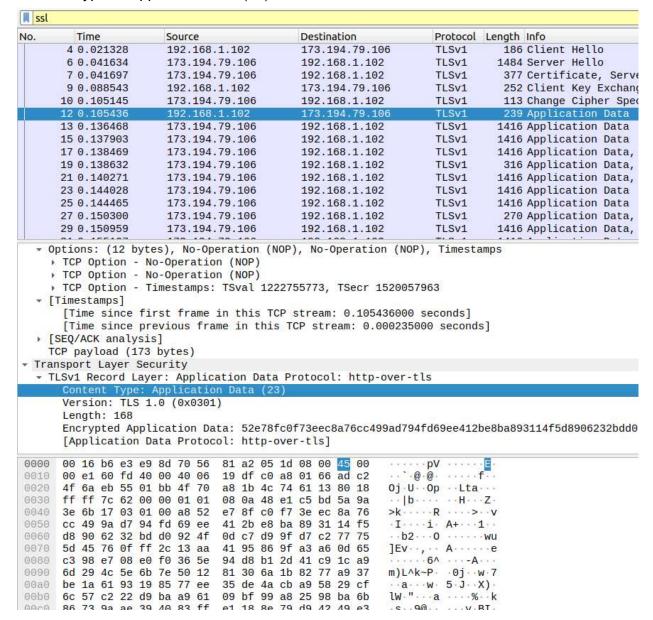
TLS (Transport Layer Security), released in 1999, is the successor to the SSL (Secure Sockets Layer) protocol for authentication and encryption. TLS 1.3 is defined in in RFC 8446 (August 2018).



Questions:

1. What is the Content-Type for a record containing Application Data?

Content-Type is: Application Data (23)

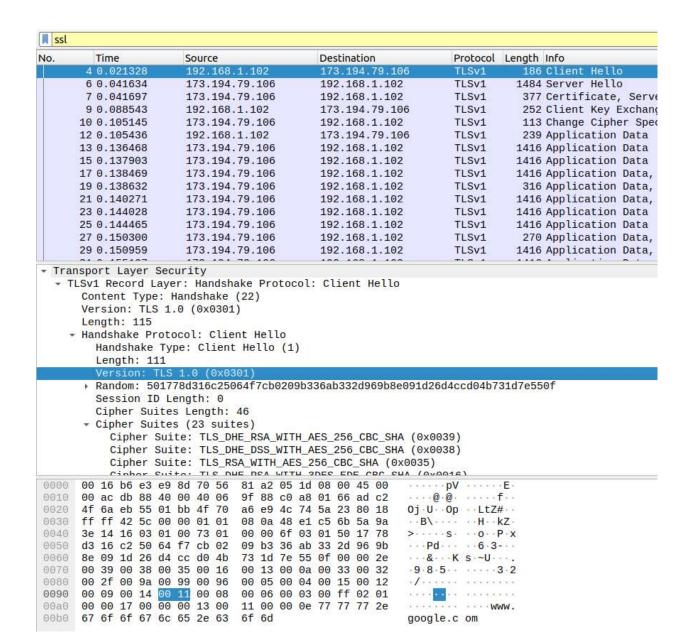


2. What version constant is used in your trace, and which version of TLS does it represent?

Ans:

TLS version: 1.0

TLS version constant: 0x0301



4.1 Hello Message

1. How long in bytes is the random data in the Hellos? Both the Client and Server include this random data (a nonce) to allow the establishment of session keys.

Ans:

Length of Random data filed: 32 bytes

_	Time	Source	Destination	Protocol	Length Info
	4 0.021328	192.168.1.102	173.194.79.106	TLSv1	186 Client Hello
	6 0.041634	173.194.79.106	192.168.1.102	TLSv1	1484 Server Hello
	7 0.041697	173.194.79.106	192.168.1.102	TLSv1	377 Certificate, Ser
	9 0.088543	192.168.1.102	173.194.79.106	TLSv1	252 Client Key Excha
	10 0.105145	173.194.79.106	192.168.1.102	TLSv1	113 Change Cipher Sp
	12 0.105436	192.168.1.102	173.194.79.106	TLSv1	239 Application Data
	13 0.136468	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data
	15 0.137903	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data
	17 0.138469	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data
	19 0.138632	173.194.79.106	192.168.1.102	TLSv1	316 Application Data
	21 0.140271	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data
	23 0.144028	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data
	25 0.144465	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data
	27 0.150300	173.194.79.106	192.168.1.102	TLSv1	270 Application Data
	29 0.150959	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data
	GMT Unix	Time: Jul 31, 2012 1	9b336ab332d969b8e091d2 1:48:59.000000000 IST		
	GMT Unix Random By Session ID Cipher Suit Cipher Suit Compression Compression Extensions	Time: Jul 31, 2012 1 /tes: 16c25064f7cb020 Length: 0 les Length: 46 les (23 suites) Methods Length: 2 Methods (2 methods) Length: 23	1:48:59.000000000 IST 9b336ab332d969b8e091d2		
	GMT Unix Random By Session ID Cipher Suit Cipher Suit Compression Compression Extensions	Time: Jul 31, 2012 1 /tes: 16c25064f7cb020 Length: 0 les Length: 46 les (23 suites) Methods Length: 2 Methods (2 methods) Length: 23	1:48:59.000000000 IST 9b336ab332d969b8e091d2	26d4ccd04b7	31d7e550f
	GMT Unix Random By Session ID Cipher Suit Cipher Suit Compression Compression Extensions	Time: Jul 31, 2012 1 /tes: 16c25064f7cb020 Length: 0 les Length: 46 les (23 suites) Methods Length: 2 Methods (2 methods) Length: 23 Server pame (len=10) 9 8d 70 56 81 a2 05	1:48:59.000000000 IST 9b336ab332d969b8e091d2 1d 08 00 45 00	26d4ccd04b7	31d7e550f
0010	GMT Unix Random By Session ID Cipher Suit Cipher Suit Compression Compression Extensions Extensions 00 16 b6 e3 e 00 ac db 88 4	Time: Jul 31, 2012 1 /tes: 16c25064f7cb020 Length: 0 res Length: 46 res (23 suites) Methods Length: 2 Methods (2 methods) Length: 23 Length: 23 Server pame (len=10) 9 8d 70 56 81 a2 05 0 00 40 06 9f 88 c0	1:48:59.000000000 IST 9b336ab332d969b8e091d2 1d 08 00 45 00 a8 01 66 ad c2	26d4ccd04b7	31d7e550f
9010 9020	GMT Unix Random By Session ID Cipher Suit Cipher Suit Compression Compression Extensions Fatonsion 00 16 b6 e3 e 00 ac db 88 4 4f 6a eb 55 0	Time: Jul 31, 2012 1 /tes: 16c25064f7cb020 Length: 0 les Length: 46 les (23 suites) Methods Length: 2 Methods (2 methods) Length: 23 Length: 23 9 8d 70 56 81 a2 05 0 00 40 06 9f 88 c0 1 bb 4f 70 a6 e9 4c	1:48:59.000000000 IST 9b336ab332d969b8e091d2 1d 08 00 45 00 a8 01 66 ad c2 74 5a 23 80 18 0j U	pV	31d7e550f
0010 0020 0030	GMT Unix Random By Session ID Cipher Suit Cipher Suit Compression Compression Extensions 00 16 b6 e3 e 00 ac db 88 4 4f 6a eb 55 0 ff ff 42 5c 0	Time: Jul 31, 2012 1 /tes: 16c25064f7cb020 Length: 0 les Length: 46 les (23 suites) Methods Length: 2 Methods (2 methods) Length: 23 Length: 23 Length: 23 Length: 23 Length: 24 Length: 25 Length: 26 Length: 26 Length: 27 Length: 28	1:48:59.000000000 IST 9b336ab332d969b8e091d2 1d 08 00 45 00 a8 01 66 ad c2 74 5a 23 80 18 Oj U e1 c5 6b 5a 9a B\	PO	31d7e550f E. ¢ ⟨Z.
0010 0020 0030 0040	GMT Unix Random By Session ID Cipher Suit Cipher Suit Compression Compression Extensions 5xtonsion 00 16 b6 e3 e 00 ac db 88 4 4f 6a eb 55 0 ff ff 42 5c 0 3e 14 16 03 0	Time: Jul 31, 2012 1 /tes: 16c25064f7cb020 Length: 0 les Length: 46 les (23 suites) Methods Length: 2 Methods (2 methods) Length: 23 Server pame (lon=10) 9 8d 70 56 81 a2 05 0 00 40 06 9f 88 c0 1 bb 4f 70 a6 e9 4c 0 00 01 01 08 0a 48 1 00 73 01 00 00 6f	1:48:59.000000000 IST 9b336ab332d969b8e091d2 1d 08 00 45 00 a8 01 66 ad c2 74 5a 23 80 18 0j U e1 c5 6b 5a 9a B\ 03 01 50 17 78	pV	31d7e550f E-
0010 0020 0030 0040	GMT Unix Random By Session ID Cipher Suit Cipher Suit Compression Compression Extensions Extensions On 16 b6 e3 e 00 ac db 88 4 4f 6a eb 55 0 ff ff 42 5c 0 3e 14 16 03 0	Time: Jul 31, 2012 1 /tes: 16c25064f7cb020 Length: 0 les Length: 46 les (23 suites) Methods Length: 2 Methods (2 methods) Length: 23 Server pame (length: 2) 9 8d 70 56 81 a2 05 0 00 40 06 9f 88 c0 1 bb 4f 70 a6 e9 4c 0 00 01 01 08 0a 48 1 00 73 01 00 00 6f 4 f7 cb 02 09 b3 36	1:48:59.000000000 IST 9b336ab332d969b8e091d2 1d 08 00 45 00 a8 01 66 ad c2 r4 5a 23 80 18 0j U e1 c5 6b 5a 9a B\ 03 01 50 17 78 ab 33 2d 96 9b		31d7e550f
0010 0020 0030 0040 0050	GMT Unix Random By Session ID Cipher Suit Cipher Suit Compression Compression Extensions 00 16 b6 e3 e 00 ac db 88 4 4f 6a eb 55 0 ff ff 42 5c 0 3e 14 16 03 0 d3 16 c2 50 6 8e 09 1d 26 d	Time: Jul 31, 2012 1 /tes: 16c25064f7cb020 Length: 0 les Length: 46 les (23 suites) Methods Length: 2 Methods (2 methods) Length: 23 Length: 23 Server pame /len=10) 9 8d 70 56 81 a2 05 0 00 40 06 9f 88 c0 1 bb 4f 70 a6 e9 4c 0 00 01 01 08 0a 48 1 00 73 01 00 00 6f 4 f7 cb 02 09 b3 36 4 cc d0 4b 73 1d 7e	1:48:59.000000000 IST 9b336ab332d969b8e091d2 1d 08 00 45 00 a8 01 66 ad c2 74 5a 23 80 18 0j U e1 c5 6b 5a 9a B\ 03 01 50 17 78 ab 33 2d 96 9b 55 0f 00 00 2e&	pV	31d7e550f
0010 0020 0030 0040 0050 0060	GMT Unix Random By Session ID Cipher Suit Cipher Suit Compression Compression Extensions Extensions 00 16 b6 e3 e 00 ac db 88 4 4f 6a eb 55 0 ff ff 42 5c 0 3e 14 16 03 0 d3 16 c2 50 6 8e 09 1d 26 d 00 39 00 38 0 00 2f 00 9a 0	Time: Jul 31, 2012 1 /tes: 16c25064f7cb020 Length: 0 res Length: 46 res (23 suites) Methods Length: 2 Methods (2 methods) Length: 23 Length: 23 Server pame (len=10) 9 8d 70 56 81 a2 05 0 00 40 06 9f 88 c0 1 bb 4f 70 a6 e9 4c 0 00 01 01 08 0a 48 1 00 73 01 00 00 6f 4 f7 cb 02 09 b3 36 4 cc d0 4b 73 1d 7e 0 35 00 16 00 13 00 0 99 00 96 00 05 00	1:48:59.000000000 IST 9b336ab332d969b8e091d2 1d 08 00 45 00 a8 01 66 ad c2 74 5a 23 80 18 0j U e1 c5 6b 5a 9a B\ 03 01 50 17 78 ab 33 2d 96 9b 55 0f 00 00 2e 0a 00 33 00 32 9 8	pV	31d7e550f
0010 0020 0030 0040 0050 0060 0070	GMT Unix Random By Session ID Cipher Suit Cipher Suit Compression Compression Extensions 00 16 b6 e3 e 00 ac db 88 4 4f 6a eb 55 0 ff ff 42 5c 0 3e 14 16 03 0 d3 16 c2 50 6 8e 09 14 26 d 00 39 00 38 0 00 2f 00 9a 0 00 09 00 14 0	Time: Jul 31, 2012 1 /tes: 16c25064f7cb020 Length: 0 res Length: 46 res (23 suites) Methods Length: 2 Methods (2 methods) Length: 23 Length: 23 9 8d 70 56 81 a2 05 0 00 40 06 9f 88 c0 1 bb 4f 70 a6 e9 4c 0 00 01 01 08 0a 48 1 00 73 01 00 00 6f 4 f7 cb 02 09 b3 36 4 cc d0 4b 73 1d 7e 0 35 00 16 00 13 00 0 99 00 96 00 05 00 0 11 00 08 00 06 00	1:48:59.000000000 IST 9b336ab332d969b8e091d2 1d 08 00 45 00 a8 01 66 ad c2 74 5a 23 80 18 0j U e1 c5 6b 5a 9a B\ 03 01 50 17 78 ab 33 2d 96 9b 55 0f 00 00 2e 0a 00 33 00 32 9 8 04 00 15 00 12 / · · 0 03 00 ff 02 01 · · · ·	pV	31d7e550f E
0010 0020 0030 0040 0050 0060 0070 0080 0090	GMT Unix Random By Session ID Cipher Suit Cipher Suit Compression Extensions Fitansions 00 16 b6 e3 e 00 ac db 88 4 4f 6a eb 55 0 ff ff 42 5c 0 3e 14 16 03 0 d3 16 c2 50 6 8e 09 14 26 d 00 39 00 38 0 00 2f 00 9a 0 00 09 00 14 0 00 00 17 00 0	Time: Jul 31, 2012 1 /tes: 16c25064f7cb020 Length: 0 les Length: 46 les (23 suites) Methods Length: 2 Methods (2 methods) Length: 23 Length: 23 Length: 23 Length: 23 Length: 24 Length: 25 Length: 26 Length: 27 Length: 27 Length: 27 Length: 28 Length: 28 Length: 29 Length: 20 Length: 20 Length: 20 Length: 21 Length: 23 Length: 24 Length: 26	1:48:59.000000000 IST 9b336ab332d969b8e091d2 1d 08 00 45 00 a8 01 66 ad c2 74 5a 23 80 18 0j U e1 c5 6b 5a 9a	pV	31d7e550f E
90000 9010 9020 9030 9040 9050 9060 9080 9090 9090	GMT Unix Random By Session ID Cipher Suit Cipher Suit Compression Compression Extensions 00 16 b6 e3 e 00 ac db 88 4 4f 6a eb 55 0 ff ff 42 5c 0 3e 14 16 03 0 d3 16 c2 50 6 8e 09 14 26 d 00 39 00 38 0 00 2f 00 9a 0 00 09 00 14 0 00 00 17 00 0	Time: Jul 31, 2012 1 /tes: 16c25064f7cb020 Length: 0 les Length: 46 les (23 suites) Methods Length: 2 Methods (2 methods) Length: 23 Length: 23 Length: 23 Length: 23 Length: 24 Length: 25 Length: 26 Length: 27 Length: 27 Length: 27 Length: 28 Length: 28 Length: 29 Length: 20 Length: 20 Length: 20 Length: 21 Length: 23 Length: 24 Length: 26	1:48:59.000000000 IST 9b336ab332d969b8e091d2 1d 08 00 45 00 a8 01 66 ad c2 74 5a 23 80 18 0j U e1 c5 6b 5a 9a	pV	31d7e550f E

2. How long in bytes is the session identifier sent by the server? This identifier allows later resumption of the session with an abbreviated handshake when both the client and server indicate the same value. In our case, the client likely sent no session ID as there was nothing to resume.

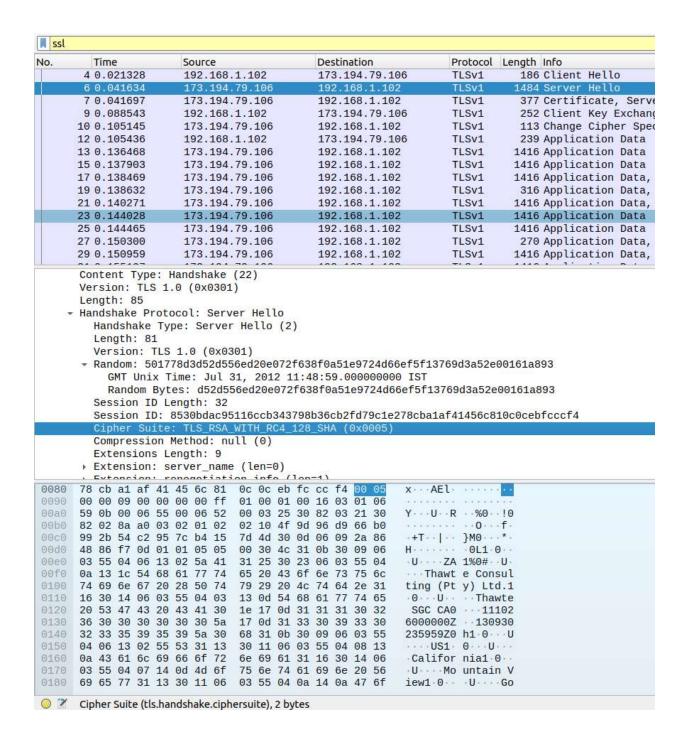
Ans: Session ID length: 32

0.	Time	Source	Destination	Protocol	Length Info
	4 0.021328	192.168.1.102	173.194.79.106	TLSv1	186 Client Hello
	6 0.041634	173,194.79.106	192.168.1.102	TLSv1	1484 Server Hello
	7 0.041697	173.194.79.106	192.168.1.102	TLSv1	377 Certificate, Se
	9 0.088543	192.168.1.102	173.194.79.106	TLSv1	252 Client Key Exch
	10 0.105145	173.194.79.106	192.168.1.102	TLSv1	113 Change Cipher S
	12 0.105436	192.168.1.102	173.194.79.106	TLSv1	239 Application Dat
	13 0.136468	173.194.79.106	192.168.1.102	TLSv1	1416 Application Dat
	15 0.137903	173.194.79.106	192.168.1.102	TLSv1	1416 Application Dat
	17 0.138469	173.194.79.106	192.168.1.102	TLSv1	1416 Application Dat
	19 0.138632	173.194.79.106	192.168.1.102	TLSv1	316 Application Dat
	21 0.140271	173.194.79.106	192.168.1.102	TLSv1	1416 Application Dat
	23 0.144028	173.194.79.106	192.168.1.102	TLSv1	1416 Application Dat
	25 0.144465	173.194.79.106	192.168.1.102	TLSv1	1416 Application Dat
	27 0.150300	173.194.79.106	192.168.1.102	TLSv1	270 Application Dat
	29 0.150959	173.194.79.106	192.168.1.102	TLSv1	1416 Application Dat
	Handshake T Length: 81	ype: Server Hello (2)		
	Version: TL Random: 501 GMT Unix Random By Session ID	The state of the s	11:48:59.0000000000 2f638f0a51e9724d66e	IST f5f13769d3a52e	e00161a893
	Version: TL Random: 501 GMT Unix Random By Session ID Session ID: Cipher Suit	778d3d52d556ed20e07 Time: Jul 31, 2012 tes: d52d556ed20e07 Length: 32 8530bdac95116ccb34 e: TLS_RSA_WITH_RC4	11:48:59.0000000000 2f638f0a51e9724d66e 3798b36cb2fd79c1e27	IST f5f13769d3a52e	e00161a893
	Version: TL Random: 501 GMT Unix Random By Session ID Session ID: Cipher Suit Compression	778d3d52d556ed20e07 Time: Jul 31, 2012 tes: d52d556ed20e07 Length: 32 8530bdac95116ccb34 e: TLS_RSA_WITH_RC4 Method: null (0)	11:48:59.0000000000 2f638f0a51e9724d66e 3798b36cb2fd79c1e27	IST f5f13769d3a52e	e00161a893
	Version: TL Random: 501 GMT Unix Random By Session ID Session ID: Cipher Suit Compression Extensions	778d3d52d556ed20e07 Time: Jul 31, 2012 tes: d52d556ed20e07 Length: 32 8530bdac95116ccb34 e: TLS_RSA_WITH_RC4 Method: null (0) Length: 9	11:48:59.0000000000 2f638f0a51e9724d66e 3798b36cb2fd79c1e27	IST f5f13769d3a52e	e00161a893
	Version: TL Random: 501 GMT Unix Random By Session ID Session ID: Cipher Suit Compression Extensions Extension:	778d3d52d556ed20e07 Time: Jul 31, 2012 tes: d52d556ed20e07 Length: 32 8530bdac95116ccb34 e: TLS_RSA_WITH_RC4 Method: null (0) Length: 9 server_name (len=0)	11:48:59.0000000000000002f638f0a51e9724d66e 3798b36cb2fd79c1e27 _128_SHA (0x0005)	IST f5f13769d3a52e	e00161a893
1966	Version: TL Random: 501 GMT Unix Random By Session ID Session ID: Cipher Suit Compression Extension:	778d3d52d556ed20e07 Time: Jul 31, 2012 tes: d52d556ed20e07 Length: 32 8530bdac95116ccb34 e: TLS_RSA_WITH_RC4 Method: null (0) Length: 9 server_name (len=0)	11:48:59.0000000000000002f638f0a51e9724d66e 3798b36cb2fd79c1e27 _128_SHA (0x0005)	IST f5f13769d3a52e 8cba1af41456c8	e00161a893 810c0cebfcccf4
	Version: TL Random: 501 GMT Unix Random By Session ID Session ID: Cipher Suit Compression Extensions Extension: Session: 10	778d3d52d556ed20e07 Time: Jul 31, 2012 tes: d52d556ed20e07 Length: 32 8530bdac95116ccb34 e: TLS_RSA_WITH_RC4 Method: null (0) Length: 9 server_name (len=0)	11:48:59.000000000 2f638f0a51e9724d66e 3798b36cb2fd79c1e27 _128_SHA (0x0005)	IST f5f13769d3a52e 8cba1af41456c8	e00161a893 810c0cebfcccf4
070	Version: TL Random: 501 GMT Unix Random By Session ID Session ID: Cipher Suit Compression Extensions Extension: Session: 66 ef 5f 13 76 bd ac 95 11 66	778d3d52d556ed20e07 Time: Jul 31, 2012 rtes: d52d556ed20e07 Length: 32 8530bdac95116ccb34 e: TLS_RSA_WITH_RC4 Method: null (0) Length: 9 server_name (len=0) renegatiation info 6 9d 3a 52 e0 01 63 c cb 34 37 98 b3 66	11:48:59.000000000000000000000000000000000000	IST f5f13769d3a52e 8cba1af41456c8 fv:Ra_	e00161a893 810c0cebfcccf4
076 086	Version: TL Random: 501 GMT Unix Random By Session ID Session ID: Cipher Suit Compression Extension: Extension: Extension: 66 ef 5f 13 76 bd ac 95 11 66 78 cb a1 af 45	778d3d52d556ed20e07 Time: Jul 31, 2012 rtes: d52d556ed20e07 Length: 32 8530bdac95116ccb34 e: TLS_RSA_WITH_RC4 Method: null (0) Length: 9 server_name (len=0) rongestiation info 6 9d 3a 52 e0 01 63 c cb 34 37 98 b3 66 1 45 6c 81 0c 0c el	11:48:59.000000000000000000000000000000000000	IST f5f13769d3a52e 8cba1af41456c8 fv:Ra- l:47l xAEL	e00161a893 810c0cebfcccf4
076 086 096	Version: TL Random: 501 GMT Unix Random By Session ID Session ID: Cipher Suit Compression Extensions Extension: 66 ef 5f 13 70 bd ac 95 11 60 78 cb a1 af 40	778d3d52d556ed20e07 Time: Jul 31, 2012 rtes: d52d556ed20e07 Length: 32 8530bdac95116ccb34 e: TLS_RSA_WITH_RC4 Method: null (0) Length: 9 server_name (len=0) reposetiation info 6 9d 3a 52 e0 01 63 c cb 34 37 98 b3 60 1 45 6c 81 0c 0c el 0 00 00 ff 01 00 03	11:48:59.000000000000000000000000000000000000	IST f5f13769d3a52e 8cba1af41456c8 fv:Ra- l-47 - l xAEl	e00161a893 810c0cebfcccf4
076 086 096 0a6	Version: TL Random: 501 GMT Unix Random By Session ID Session ID: Cipher Suit Compression Extension: Extension: 66 ef 5f 13 76 bd ac 95 11 66 78 cb a1 af 4 00 00 09 00 06 59 0b 00 06 55	778d3d52d556ed20e07 Time: Jul 31, 2012 Tes: d52d556ed20e07 Length: 32 8530bdac95116ccb34 e: TLS_RSA_WITH_RC4 Method: null (0) Length: 9 server_name (len=0) renegation info 6 9d 3a 52 e0 01 60 c cb 34 37 98 b3 66 c cb 34 37 98 b3 66 c cb 34 37 98 b3 66 c d5 34 37 98 b3 66 d1 45 6c 81 0c 0c el 0 00 00 ff 01 00 00 5 00 06 52 00 03 20	11:48:59.000000000000000000000000000000000000	IST f5f13769d3a52e 8cba1af41456c8 fv:R - a - - l 47 - l - v x - AEl	e00161a893 810c0cebfcccf4
076 086 096 0a6 0b6	Version: TL Random: 501 GMT Unix Random By Session ID Session ID: Cipher Suit Compression Extension: Extension: Cipher Suit Compression Extension: Extension: Compression Extension: Extension: Compression Extension Ex	778d3d52d556ed20e07 Time: Jul 31, 2012 Tes: d52d556ed20e07 Length: 32 8530bdac95116ccb34 e: TLS_RSA_WITH_RC4 Method: null (0) Length: 9 server_name (len=0) renegatiation info 6 9d 3a 52 e0 01 63 c cb 34 37 98 b3 60 1 45 6c 81 0c 0c e1 0 00 00 ff 01 00 03 5 00 06 52 00 03 23 3 02 01 02 02 10 41	11:48:59.000000000000000000000000000000000000	IST f5f13769d3a52e 8cba1af41456c8 f v : R - a - -	e00161a893 210c0cebfcccf4 2 0 3 0 4 0 5 0 9 0 9 0
076 086 096 0a6 0b6	Version: TL Random: 501 GMT Unix Random By Session ID Session ID: Cipher Suit Compression Extension: Extension: Factorial 66 ef 5f 13 76 bd ac 95 11 66 78 cb a1 af 4: 00 00 99 00 00 59 0b 00 06 5: 82 02 8a a0 03 99 2b 54 c2 9:	778d3d52d556ed20e07 Time: Jul 31, 2012 Tes: d52d556ed20e07 Length: 32 8530bdac95116ccb34 e: TLS_RSA_WITH_RC4 Method: null (0) Length: 9 server_name (len=0) renegation info 6 9d 3a 52 e0 01 60 c cb 34 37 98 b3 66 c cb 34 37 98 b3 66 c cb 34 37 98 b3 66 c d5 34 37 98 b3 66 d1 45 6c 81 0c 0c el 0 00 00 ff 01 00 00 5 00 06 52 00 03 20	11:48:59.000000000000000000000000000000000000	IST f5f13769d3a52e 8cba1af41456c8 fv:R - a - - l 47 - l - v x - AEl	e00161a893 210c0cebfcccf4 2 0 3 0 4 0 5 0 5 0 7 0 7 0 8 10 8 10 8 10 8 10 8 10 8 10 8 10 8
076 086 096 0a6 0b6 0c6	Version: TL Random: 501 GMT Unix Random By Session ID Session ID: Cipher Suit Compression Extension: Extension: 66 ef 5f 13 76 bd ac 95 11 66 78 cb a1 af 4: 00 00 09 00 00 59 0b 00 06 5: 82 02 8a a0 0: 99 2b 54 c2 9: 48 86 f7 0d 0:	778d3d52d556ed20e07 Time: Jul 31, 2012 rtes: d52d556ed20e07 Length: 32 8530bdac95116ccb34 e: TLS_RSA_WITH_RC4 Method: null (0) Length: 9 server_name (len=0) renegatiation_info_6 6 9d 3a 52 e0 01 63 c cb 34 37 98 b3 60 1 45 6c 81 0c 0c el 0 00 00 ff 01 00 03 5 00 06 52 00 03 23 3 02 01 02 02 10 41 5 7c b4 15 7d 4d 30 1 01 05 05 00 30 40	11:48:59.000000000000000000000000000000000000	IST f5f13769d3a52e 8cba1af41456c8 f v : R · a · · · · l · 47 · l · · x · · AEl · · · · · · · · · Y · U · R · %0 · · · · · · · · · · · · +T · · }M0	e00161a893 210c0cebfcccf4 2 - 0 2 - 0 3 - 0 4 - 0 5 - 0 5 - 0 6 - 0 7 - 0 8 - 0 9 -
076 086 096 0a6 0b6 0c6 0d6	Version: TL Random: 501 GMT Unix Random By Session ID Session ID: Cipher Suit Compression Extensions Extension: Extension	778d3d52d556ed20e07 Time: Jul 31, 2012 rtes: d52d556ed20e07 Length: 32 8530bdac95116ccb34 e: TLS_RSA_WITH_RC4 Method: null (0) Length: 9 server_name (len=0) reneartiation info 6 9d 3a 52 e0 01 6: c cb 34 37 98 b3 60 1 45 6c 81 0c 0c el 0 00 00 ff 01 00 0: 5 00 06 52 00 03 25 3 02 01 02 02 10 41 5 7c b4 15 7d 4d 33 1 01 05 05 00 30 40 3 02 5a 41 31 25 30	11:48:59.000000000000000000000000000000000000	IST f5f13769d3a52e 8cba1af41456c8 fv:R - a	00161a893 210c0cebfcccf4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
076 086 096 0a6 0b6 0c6 0d6	Version: TL Random: 501 GMT Unix Random By Session ID Session ID: Cipher Suit Compression Extensions Extensions: Extension: 66 ef 5f 13 70 bd ac 95 11 60 78 cb a1 af 4: 00 00 09 00 00 59 0b 00 06 59 82 02 8a a0 00 99 2b 54 c2 99 48 86 f7 0d 00 03 55 04 06 1: 0a 13 1c 54 66	778d3d52d556ed20e07 Time: Jul 31, 2012 rtes: d52d556ed20e07 Length: 32 8530bdac95116ccb34 e: TLS_RSA_WITH_RC4 Method: null (0) Length: 9 server_name (len=0) reneartiation info 6 9d 3a 52 e0 01 63 c cb 34 37 98 b3 60 1 45 6c 81 0c 0c el 0 00 00 ff 01 00 03 5 00 06 52 00 03 25 3 02 01 02 02 10 41 5 7c b4 15 7d 4d 33 1 01 05 05 00 30 46 3 02 5a 41 31 25 30 8 61 77 74 65 20 43	11:48:59.000000000000000000000000000000000000	IST f5f13769d3a52e 8cba1af41456c8 fv:R - a 	00161a893 810c0cebfcccf4 9.0 y
076 086 096 006 006 006 006 006	Version: TL Random: 501 GMT Unix Random By Session ID Session ID: Cipher Suit Compression Extension: Extension	778d3d52d556ed20e07 Time: Jul 31, 2012 rtes: d52d556ed20e07 Length: 32 8530bdac95116ccb34: e: TLS_RSA_WITH_RC4 Method: null (0) Length: 9 server_name (len=0) renegatiation info 6 9d 3a 52 e0 01 6: c cb 34 37 98 b3 60 1 45 6c 81 0c 0c el 0 00 00 ff 01 00 0: 5 00 06 52 00 03 25 3 02 01 02 02 10 41 5 7c b4 15 7d 4d 30 1 01 05 05 00 30 46 3 02 5a 41 31 25 30 8 61 77 74 65 20 43 0 28 50 74 79 29 20	11:48:59.000000000000000000000000000000000000	IST f5f13769d3a52e 8cba1af41456c8 fv:R a - 	00161a893 010c0cebfcccf4 0 0 y · · · · · · · · · · · · · · · · · · ·
076 086 096 0a6 0c6 0d6 0d6 106	Version: TL Random: 501 GMT Unix Random By Session ID Session ID: Cipher Suit Compression Extension: Extension	778d3d52d556ed20e07 Time: Jul 31, 2012 rtes: d52d556ed20e07 Length: 32 8530bdac95116ccb34 e: TLS_RSA_WITH_RC4 Method: null (0) Length: 9 server_name (len=0) reneartiation info 6 9d 3a 52 e0 01 60 c cb 34 37 98 b3 60 1 45 6c 81 0c 0c el 0 00 00 ff 01 00 00 5 00 06 52 00 03 25 3 02 01 02 02 10 41 5 7c b4 15 7d 4d 30 1 01 05 05 00 30 40 3 02 5a 41 31 25 30 8 61 77 74 65 20 43 0 28 50 74 79 29 20 3 55 04 03 13 0d 54	11:48:59.000000000000000000000000000000000000	IST f5f13769d3a52e 8cba1af41456c8 f _ v : R	00161a893 10c0cebfcccf4 10c0cebfcccf4 y
076 086 096 066 066 066 076 116	Version: TL Random: 501 GMT Unix Random By Session ID Session ID: Cipher Suit Compression Extensions Extension: 66 ef 5f 13 76 bd ac 95 11 66 78 cb a1 af 43 00 00 09 00 06 59 0b 00 06 56 82 02 8a a0 03 99 2b 54 c2 93 48 86 f7 0d 03 55 04 06 13 08 13 1c 54 66 74 69 6e 67 26 16 30 14 06 03 20 53 47 43 26	778d3d52d556ed20e07 Time: Jul 31, 2012 rtes: d52d556ed20e07 Length: 32 8530bdac95116ccb34 e: TLS_RSA_WITH_RC4 Method: null (0) Length: 9 server_name (len=0) reneartiation info 6 9d 3a 52 e0 01 6: c cb 34 37 98 b3 60 1 45 6c 81 0c 0c el 0 00 00 ff 01 00 0: 5 00 06 52 00 03 25 3 02 01 02 02 10 41 5 7c b4 15 7d 4d 30 1 01 05 05 00 30 40 3 02 5a 41 31 25 30 8 61 77 74 65 20 43 0 28 50 74 79 29 20 3 55 04 03 13 0d 54 0 43 41 30 1e 17 00	11:48:59.000000000000000000000000000000000000	IST f5f13769d3a52e 8cba1af41456c8 f _ v :R	00161a893 010c0cebfcccf4 00 y · · · · · · · · · · · · · · · · · · ·
0076 0086 0096 0066 0066 0066 0076 0116 0126	Version: TL Random: 501 GMT Unix Random By Session ID Session ID: Cipher Suit Compression Extensions Extension: 66 ef 5f 13 76 bd ac 95 11 66 78 cb a1 af 43 00 00 09 00 06 59 0b 00 06 53 82 02 8a a0 03 99 2b 54 c2 93 48 86 f7 0d 03 03 55 04 06 13 04 13 1c 54 63 74 69 6e 67 22 16 30 14 06 03 20 53 47 43 20 36 30 30 30 30	778d3d52d556ed20e07 Time: Jul 31, 2012 (tes: d52d556ed20e07 Length: 32 8530bdac95116ccb34 e: TLS_RSA_WITH_RC4 Method: null (0) Length: 9 server_name (len=0) reneartiation info 6 9d 3a 52 e0 01 63 c cb 34 37 98 b3 66 c b 34 37 98 b3 66 c c b 34 37 98 b3 67 d 50 00 00 00 00 00 d 60 00 00 00 00 00 d 70 00 00	11:48:59.000000000000000000000000000000000000	IST f5f13769d3a52e 8cba1af41456c8 f _ v : R	#10c0cebfcccf4
9066 9076 9086 9096 9006 9006 9016 91126 91126 91136	Version: TL Random: 501 GMT Unix Random By Session ID Session ID: Cipher Suit Compression Extension: Extension	778d3d52d556ed20e07 Time: Jul 31, 2012 (tes: d52d556ed20e07 Length: 32 8530bdac95116ccb34 e: TLS_RSA_WITH_RC4 Method: null (0) Length: 9 server_name (len=0) 1000 30 35 2 e0 01 65 1000 65 2 e0 01 65 1000 65 2 e0 03 25 1000 65 2 e0 05 1000 65 2 e0	11:48:59.000000000000000000000000000000000000	F - V : R - a - A - A - A - A - A - A - A - A - A	00161a893 210c0cebfcccf4 00 y 00 y 00

3. What Cipher suite is chosen by the Server? Give its name and value. The Client will list the different cipher methods it supports, and the Server will pick one of these methods to use.

Ans:

Cipher Suit name: TLS_RSA_WITH_RC4_128_SHA (0x0005)



4.2 Certificate Messages

1. Who sends the Certificate, the client, the server, or both? A certificate is sent by one party to let the other party authenticate that it is who it claims to be. Based on this usage, you should be able to guess who sends the certificate and check the messages in your trace.

Ans: Server sends the certificate

	Time	Source	Destination	Protocol	Length Info
	4 0.021328	192.168.1.102	173.194.79.106	5 TLSv1	186 Client Hello
+	6 0.041634	173.194.79.106	192.168.1.102	TLSv1	1484 Server Hello
	7 0.041697	173.194.79.106	192.168.1.102	TLSv1	377 Certificate, Server Hello D
	9 0.088543	192.168.1.102	173.194.79.106		252 Client Key Exchange, Change
	10 0.105145	173.194.79.106	192.168.1.102	TLSv1	113 Change Cipher Spec, Encrypt
	12 0.105436	192.168.1.102	173.194.79.106		239 Application Data
	13 0.136468	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data
	15 0.137903	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data
	17 0.138469	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data, Applicati
	19 0.138632	173.194.79.106	192.168.1.102	TLSv1	316 Application Data, Applicati
	21 0.140271	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data, Applicati
	23 0.144028	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data
	25 0.144465	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data
	27 0.150300	173.194.79.106	192.168.1.102	TLSv1	270 Application Data, Applicati
	29 0.150959	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data, Applicati
· [2	Reassembled TCP	Segments (1630 bytes			11121 1: 0: 0
	ansport Layer Se		,	/1	
		er: Handshake Protoc	ol: Certificate		
		Handshake (22)	Selection - British Habita Marchaelettani		
	Version: TLS				
	Length: 1625				
10		tocol: Certificate			
		ype: Certificate (11)			
	Length: 162				
		s Length: 1618			
		s (1618 bytes)			
- Tra	ansport Layer Se				
			ol: Server Hello	Dono	
			001 001 110 110 110	Done	
	Content Type:	Handshake (22)		Done	
	Content Type: Version: TLS	Handshake (22)		Done	
	Content Type: Version: TLS 1 Length: 4	Handshake (22)		Done	
0000	Content Type: Version: TLS 1 Length: 4	Handshake (22) 1.0 (0x0301) 0 0b 00 06 55 00 06	52 00 03 25 30	····Y··· U··R·	
	Content Type: Version: TLS: Length: 4 16 03 01 06 55 82 03 21 30 82	Handshake (22) 1.0 (0x0301) 3 0b 00 06 55 00 06 2 02 8a a0 03 02 01	52 00 03 25 30 02 02 10 4f 9d	· · · · Y · · · · U · · R · · · · ! 0 · · · · · · ·	0.
9999	Content Type: Version: TLS 1 Length: 4 Hondobaka Drod 16 03 01 06 56 82 03 21 30 82 96 d9 66 b0 98	Handshake (22) 1.0 (0x0301) 0 0b 00 06 55 00 06 2 02 8a a0 03 02 01 0 2b 54 c2 95 7c b4	52 00 03 25 30 02 02 10 4f 9d 15 7d 4d 30 0d	Y UR- !0 f+T }	· O · 10 ·
0000 0010	Content Type: Version: TLS 1 Length: 4 Handshake Brod 16 03 01 05 5 82 03 21 30 83 96 d9 66 b0 99 06 09 2a 86 48	Handshake (22) 1.0 (0x0301) 2001 0 00 5 5 00 06 2 02 8a a0 03 02 01 9 2b 54 c2 95 7c b4 3 86 f7 0d 01 01 05	52 00 03 25 30 02 02 10 4f 9d 15 7d 4d 30 0d 05 00 30 4c 31	····Y··· U··R· ··!0··· ··f··+T· ··}!	0. M0. DL1
0000 0010 0020 0030 0040	Content Type: Version: TLS 1 Length: 4 Handshake Bree 16 03 01 06 58 82 03 21 30 88 96 09 66 b0 99 06 09 2a 86 48 0b 30 09 06 03	Handshake (22) 1.0 (0x0301) 2021: Sarvor Halla D 2 02 8a a0 03 02 01 2 2b 54 c2 95 7c b4 3 86 f7 0d 01 01 05 3 55 04 06 13 02 5a	52 00 03 25 30 02 02 10 4f 9d 15 7d 4d 30 0d 05 00 30 4c 31 41 31 25 30 23	Y UR. !0 f+T }! *.H	0. 40. 0.1.1 60#
0000 0010 0020 0030 0040 0050	Content Type: Version: TLS 1 Length: 4 Handblake Bred 16 03 01 06 55 82 03 21 30 82 96 d9 66 b0 99 06 09 28 86 48 0b 30 09 06 03 06 03 55 04 08	Handshake (22) 1.0 (0x0301) 2 0b 00 06 55 00 06 2 02 8a a0 03 02 01 9 2b 54 c2 95 7c b4 3 86 f7 0d 01 01 05 3 55 04 06 13 02 5a a 13 1c 54 68 61 77	52 00 03 25 30 02 02 10 4f 9d 15 7d 4d 30 0d 05 00 30 4c 31 41 31 25 30 23 74 65 20 43 6f	Y UR. !0 f+T }! *.H(.0UZAI! UT hawte	0. 40. 0.1 0.0 0.0 0.0 0.0
0000 0010 0020 0030 0040 0050 0060	Content Type: Version: TLS 1 Length: 4 Handshake Bred 16 03 01 06 53 82 03 21 30 82 96 d9 66 b0 93 06 09 2a 86 48 0b 30 09 06 03 06 03 55 04 06 6e 73 75 6c 74	Handshake (22) 1.0 (0x0301) 0 0b 00 06 55 00 06 2 02 8a a0 03 02 01 0 2b 54 c2 95 7c b4 3 86 f7 0d 01 01 05 3 55 04 06 13 02 5a 1 13 1c 54 68 61 77 1 69 6e 67 20 28 50	52 00 03 25 30 02 02 10 4f 9d 15 7d 4d 30 0d 05 00 30 4c 31 41 31 25 30 23 74 65 20 43 6f 74 79 29 20 4c	Y UR!0f+T. }!*.H0UZA19UT hawte nsulting (Pty	- O - 10 - 0L1 60# CO
0000 0010 0020 0030 0040 0050 0060 0070	Content Type: Version: TLS 1 Length: 4 Handshake Brod 16 03 01 06 55 82 03 21 30 82 96 d9 66 b0 93 06 09 2a 86 48 0b 30 09 06 03 06 03 55 04 06 6e 73 75 6c 74 74 64 2e 31 16	Handshake (22) 1.0 (0x0301) 0 0b 00 06 55 00 06 2 02 8a a0 03 02 01 0 2b 54 c2 95 7c b4 8 86 f7 0d 01 01 05 8 55 04 06 13 02 5a 1 3 1c 54 68 61 77 4 69 6e 67 20 28 50 6 30 14 06 03 55 04	52 00 03 25 30 02 02 10 4f 9d 15 7d 4d 30 0d 05 00 30 4c 31 41 31 25 30 23 74 65 20 43 6f 74 79 29 20 4c 03 13 0d 54 68	Y UR!0	- 0 · - 10 · - 11 1 - 12 60# - Co - Co - Co - Th
0000 0010 0020 0030 0040 0050 0060 0070 0080	Content Type: Version: TLS 1 Length: 4 Hondebake Dred 16 03 01 06 58 82 03 21 30 82 96 d9 66 b0 98 06 09 2a 86 48 0b 30 09 06 03 06 03 55 04 08 6e 73 75 6c 74 74 64 2e 31 16	Handshake (22) 1.0 (0x0301) 2001	52 00 03 25 30 02 02 10 4f 9d 15 7d 4d 30 0d 05 00 30 4c 31 41 31 25 30 23 74 65 20 43 6f 74 79 29 20 4c 03 13 0d 54 68 30 1e 17 0d 31	Y UR !0	00 · 10 ·
0000 0010 0020 0030 0040 0050 0060 0070 0080 0090	Content Type: Version: TLS 2 Length: 4 Handbake Breat 16 03 01 06 55 82 03 21 30 83 96 d9 66 b0 99 06 09 2a 86 48 0b 30 09 06 03 06 03 55 04 03 6e 73 75 6c 74 74 64 2e 31 16 61 77 74 65 20 31 31 30 32 36	Handshake (22) 1.0 (0x0301) 20 0b 00 06 55 00 06 2 02 8a a0 03 02 01 9 2b 54 c2 95 7c b4 8 86 f7 0d 01 01 05 8 55 04 06 13 02 5a a 13 1c 54 68 61 77 4 69 6e 67 20 28 50 6 30 14 06 03 55 04 6 53 47 43 20 43 41 6 30 30 30 30 30 30	52 00 03 25 30 02 02 10 4f 9d 15 7d 4d 30 0d 05 00 30 4c 31 41 31 25 30 23 74 65 20 43 6f 74 79 29 20 4c 03 13 0d 54 68 30 1e 17 0d 31 5a 17 0d 31 33	Y U.R!0	00. MO. DL1 60# CO L Th ·1
0000 0010 0020 0030 0040 0050 0060 0070 0080 0090 00a0	Content Type: Version: TLS 1 Length: 4 Handebake Bred 16 03 01 06 59 82 03 21 30 82 96 d9 66 b0 99 06 09 2a 86 48 0b 30 09 06 00 06 03 55 04 06 6e 73 75 6c 74 74 64 2e 31 16 61 77 74 65 20 31 31 30 32 36 30 39 33 30 32	Handshake (22) 1.0 (0x0301) 20 0b 00 06 55 00 06 2 02 8a a0 03 02 01 0 2b 54 c2 95 7c b4 3 86 f7 0d 01 01 05 3 55 04 06 13 02 5a 4 13 1c 54 68 61 77 4 69 6e 67 20 28 50 6 30 14 06 03 55 04 05 34 47 43 20 43 41 6 30 30 30 30 30 30 2 33 35 39 35 39 5a	52 00 03 25 30 02 02 10 4f 9d 15 7d 4d 30 0d 15 7d 2d 31 23 41 31 25 30 23 74 65 20 43 6f 74 79 29 20 4c 03 13 0d 54 68 31 30 54 68 31 70 31 33 30 68 31 0b 30	Y U.R!0	· 0 · · · · · · · · · · · · · · · · · ·
0000 0010 0020 0030 0040 0050 0060 0070 0080 0090 0080	Content Type: Version: TLS 1 Length: 4 Handshake Bred 16 03 01 06 55 82 03 21 30 82 96 d9 66 b0 95 06 09 2a 86 48 0b 30 09 06 03 06 03 55 04 06 6e 73 75 6c 74 74 64 2e 31 16 61 77 74 65 20 31 31 30 32 36 09 06 03 55 04	Handshake (22) 1.0 (0x0301) 20 0b 00 06 55 00 06 2 02 8a a0 03 02 01 2 2b 54 c2 95 7c b4 3 86 f7 0d 01 01 05 3 55 04 06 13 02 5a 3 13 1c 54 68 61 77 4 69 6e 67 20 28 50 6 30 14 06 03 55 04 0 53 47 43 20 43 41 0 53 30 30 30 30 30 30 2 33 35 39 35 39 58 4 06 13 02 55 53 31	52 00 03 25 30 02 02 10 4f 9d 15 7d 4d 30 0d 05 00 30 4c 31 44 31 25 30 23 74 65 20 43 6f 74 79 29 20 4c 03 13 0d 54 68 30 1e 17 0d 31 5a 17 0d 31 33 30 68 31 0b 30 13 30 11 06 03	Y U.R !0	00. 10. 10. 10. 10. 10. 10. 10. 10. 10.
0000 0010 0020 0030 0040 0050 0060 0070 0080 0090 0090 0000	Content Type: Version: TLS 1 Length: 4 Handshake Bred 16 03 01 06 55 82 03 21 30 82 96 d9 66 b0 95 06 09 2a 86 48 0b 30 09 06 03 06 03 55 04 06 6e 73 75 6c 74 74 64 2e 31 16 61 77 74 65 20 31 31 30 32 36 30 39 33 30 32 09 06 03 55 04 55 04 08 13 06	Handshake (22) 1.0 (0x0301) 20 0b 00 06 55 00 06 2 02 8a a0 03 02 01 2 2b 54 c2 95 7c b4 3 86 f7 0d 01 01 05 3 55 04 06 13 02 57 4 69 6e 67 20 28 50 3 01 4 06 03 55 04 0 53 47 43 20 43 41 0 53 30 30 30 30 30 30 14 06 13 02 55 53 31 14 43 61 6c 69 66 6f	52 00 03 25 30 02 02 10 4f 9d 15 7d 4d 30 0d 05 00 30 4c 31 41 31 25 30 23 74 65 20 43 6f 74 79 29 20 4c 03 13 0d 54 68 30 1e 17 0d 31 5a 17 0d 31 33 30 68 31 0b 30 13 30 11 06 03 72 6e 69 61 31	Y U.R !0	00. 10. 10. 10. 10. 10. 10. 10. 10. 10.
0000 0010 0020 0030 0040 0050 0060 0070 0080 0090 0080 0000 0000	Content Type: Version: TLS 1 Length: 4 Handchake Breat 16 03 01 06 56 82 03 21 30 83 96 09 66 b0 98 06 09 2a 86 48 0b 30 09 06 03 06 03 55 04 08 6e 73 75 6c 74 74 64 2e 31 16 61 77 74 65 20 31 31 30 32 36 30 39 33 30 33 09 06 03 55 04 16 30 14 06 03	Handshake (22) 1.0 (0x0301) 9 0b 00 06 55 00 06 2 02 8a a0 03 02 01 9 86 f7 0d 01 01 05 3 55 04 06 13 02 5a 1 13 1c 54 68 61 77 4 69 6e 67 20 28 50 6 30 14 06 03 55 04 9 53 47 43 20 43 41 6 30 30 30 30 30 30 2 33 35 39 35 39 5a 1 06 13 02 55 53 31 4 06 13 02 55 53 31 4 06 13 02 55 53 31 4 43 61 6c 69 66 6f 6 55 04 07 14 0d 4d	52 00 03 25 30 02 02 10 4f 9d 15 7d 4d 30 0d 05 00 30 4c 31 41 31 25 30 23 74 65 20 43 6f 74 79 29 20 4c 03 13 0d 54 68 30 1e 17 0d 31 5a 17 0d 31 33 30 68 31 0b 30 13 30 11 06 03 72 6e 69 61 31 6f 75 6e 74 61	Y U.R!0	00. 10. 10. 10. 10. 10. 10. 10. 10. 10.
0000 0010 0020 0030 0040 0050 0060 0070 0080 0090 0000	Content Type: Version: TLS 1 Length: 4 Handchake Breat 16 03 01 06 56 82 03 21 30 83 96 09 66 b0 98 06 09 2a 86 48 0b 30 09 06 03 06 03 55 04 08 6e 73 75 6c 74 74 64 2e 31 16 61 77 74 65 20 31 31 30 32 36 30 39 33 30 33 09 06 03 55 04 16 30 14 06 03	Handshake (22) 1.0 (0x0301) 20 0b 00 06 55 00 06 2 02 8a a0 03 02 01 2 2b 54 c2 95 7c b4 3 86 f7 0d 01 01 05 3 55 04 06 13 02 57 4 69 6e 67 20 28 50 3 01 4 06 03 55 04 0 53 47 43 20 43 41 0 53 30 30 30 30 30 30 14 06 13 02 55 53 31 14 43 61 6c 69 66 6f	52 00 03 25 30 02 02 10 4f 9d 15 7d 4d 30 0d 05 00 30 4c 31 41 31 25 30 23 74 65 20 43 6f 74 79 29 20 4c 03 13 0d 54 68 30 1e 17 0d 31 5a 17 0d 31 33 30 68 31 0b 30 13 30 11 06 03 72 6e 69 61 31 6f 75 6e 74 61	Y U.R !0	00. 10. 10. 10. 10. 10. 10. 10. 10. 10.
0000 0010 0020 0030 0040 0050 0060 0070 0080 0090 0000 0000 0000	Content Type: Version: TLS 1 Length: 4 Handbhake Breat 16 03 01 06 58 82 03 21 30 82 96 d9 66 b0 98 06 09 2a 86 48 0b 30 09 06 03 06 03 55 04 06 6e 73 75 6c 74 74 64 2e 31 10 61 77 74 65 23 31 31 30 32 36 30 39 33 30 32 09 06 03 55 04 55 04 08 13 06 69 6e 20 56 68	Handshake (22) 1.0 (0x0301) 2 0b 00 06 55 00 06 2 02 8a a0 03 02 01 9 2b 54 c2 95 7c b4 8 86 f7 0d 01 01 05 8 55 04 06 13 02 5a 13 1c 54 68 61 77 4 69 6e 67 20 28 50 53 14 06 03 55 04 55 30 14 06 03 55 04 53 35 39 35 39 5a 4 06 13 02 55 53 31 6 43 61 6c 69 66 64 6 55 77 31 13 30 11	52 00 03 25 30 02 02 10 4f 9d 15 7d 4d 30 0d 05 00 30 4c 31 41 31 25 30 23 74 65 20 43 6f 74 79 29 20 4c 03 13 0d 54 68 30 1e 17 0d 31 5a 17 0d 31 33 30 68 31 0b 30 13 30 11 06 03 72 6e 69 61 31 6f 75 6e 74 61	Y U.R!0	00. 10. 10. 10. 10. 10. 10. 10. 10. 10.
0000 0010 0020 0030 0040 0050 0060 0070 0080 0090 0000 0000 0000	Content Type: Version: TLS 1 Length: 4 Handbhake Breat 16 03 01 06 58 82 03 21 30 82 96 d9 66 b0 98 06 09 2a 86 48 0b 30 09 06 03 06 03 55 04 06 6e 73 75 6c 74 74 64 2e 31 10 61 77 74 65 23 31 31 30 32 36 30 39 33 30 32 09 06 03 55 04 55 04 08 13 06 69 6e 20 56 68	Handshake (22) 1.0 (0x0301) 9 0b 00 06 55 00 06 2 02 8a a0 03 02 01 9 86 f7 0d 01 01 05 3 55 04 06 13 02 5a 1 13 1c 54 68 61 77 4 69 6e 67 20 28 50 6 30 14 06 03 55 04 9 53 47 43 20 43 41 6 30 30 30 30 30 30 2 33 35 39 35 39 5a 1 06 13 02 55 53 31 4 06 13 02 55 53 31 4 06 13 02 55 53 31 4 43 61 6c 69 66 6f 6 55 04 07 14 0d 4d	52 00 03 25 30 02 02 10 4f 9d 15 7d 4d 30 0d 05 00 30 4c 31 41 31 25 30 23 74 65 20 43 6f 74 79 29 20 4c 03 13 0d 54 68 30 1e 17 0d 31 5a 17 0d 31 33 30 68 31 0b 30 13 30 11 06 03 72 6e 69 61 31 6f 75 6e 74 61	Y U.R!0	00. 10. 10. 10. 10. 10. 10. 10. 10. 10.

4.3 Client Key Exchange and Change Cipher Messages

1. Who sends the Change Cipher Spec message, the client, the server, or both?

Ans: Both server and client sends the Change Cipher Spec message

No.	Time	Source	Destination	Protocol	Length Info
	4 0.021328	192.168.1.102	173.194.79.106	TLSv1	186 Client Hello
	6 0.041634	173.194.79.106	192.168.1.102	TLSv1	1484 Server Hello
	7 0.041697	173.194.79.106	192.168.1.102	TLSv1	377 Certificate, Server Hello Done
	9 0.088543	192.168.1.102	173.194.79.106	TLSv1	252 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
					113 Change Cipher Spec, Encrypted Handshake Message
	12 0.105436	192.168.1.102	173.194.79.106	TLSv1	239 Application Data
	13 0.136468	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data
	15 0.137903	173,194,79,106	192.168.1.102	TLSv1	1416 Application Data

2. What are the contents carried inside the Change Cipher Spec message? Lookpast the Content Type and other headers to see the message itself

Ans: Change Cipher Spec message contains:
Content Type, Version, Length and Change Cipher Spec Message

	Time	Source	Destination	Protocol	Length Info
	4 0.021328	192.168.1.102	173.194.79.106	TLSv1	186 Client Hello
	6 0.041634	173.194.79.106	192.168.1.102	TLSv1	1484 Server Hello
	7 0.041697	173.194.79.106	192.168.1.102	TLSv1	377 Certificate, Server Hello Done
	9 0.088543	192.168.1.102	173.194.79.106	TLSv1	252 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Messag
	10 0.105145	173.194.79.106	192.168.1.102	TLSv1	113 Change Cipher Spec, Encrypted Handshake Message
	12 0.105436	192.168.1.102	173.194.79.106	TLSv1	239 Application Data
	13 0.136468	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data
	15 0.137903	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data
	17 0.138469	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data, Application Data, Application Data
	19 0.138632	173.194.79.106	192.168.1.102	TLSv1	316 Application Data, Application Data
	21 0.140271	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data, Application Data
	23 0.144028	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data
	25 0.144465	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data
	27 0.150300	173.194.79.106	192.168.1.102	TLSv1	270 Application Data, Application Data
	29 0.150959	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data, Application Data
Tr Tr	ansmission Contr ansport Layer Se TLSv1 Record Lay	ol Protocol, Src Por curity er: Handshake Protoc	168.1.102, Dst: 173.1 t: 60245, Dst Port: 4 ol: Client Key Exchan	43, Seq: 12	1, Ack: 1730, Len: 186
Tr Tr	ansmission Contr ansport Layer Se TLSv1 Record Lay Content Type: Version: TLS 1 Length: 134 + Handshake Prot Handshake T	ol Protocol, Src Por curity ver: Handshake Protoc Handshake (22) 1.0 (0x0301) tocol: Client Key Excha ype: Client Key Excha	t: 60245, Dst Port: 4 ol: Client Key Exchan hange	43, Seq: 12	1, Ack: 1730, Len: 186
Tr Tr	ansmission Contr ansport Layer Se TLSv1 Record Lay Content Type: Version: TLS 1 Length: 134 + Handshake Prot Handshake T Length: 130	ol Protocol, Src Por- curity ver: Handshake Protoc Handshake (22) 1.0 (0x0301) cocol: Client Key Exc ype: Client Key Excha	t: 60245, Dst Port: 4 ol: Client Key Exchan hange	43, Seq: 12	1, Ack: 1730, Len: 186
Tr.	ansmission Contr ansport Layer Se TLSv1 Record Lay Content Type: Version: TLS 1 Length: 134 Handshake Prot Handshake T Length: 130 RSA Encrypt:	ol Protocol, Src Portourity ver: Handshake Protoc Handshake (22) 1.0 (0x0301) tocol: Client Key Exche ed PreMaster Secret	t: 60245, Dst Port: 4 ol: Client Key Exchan hange	43, Seq: 12	1, Ack: 1730, Len: 186

Conclusion:

1. SSL/TLS certificates are vital to any website, but especially important to the performance of online stores or eCommerce sites.