

Cryptography and Network Security Lab

Assignment No 16

Batch – B4

Title:

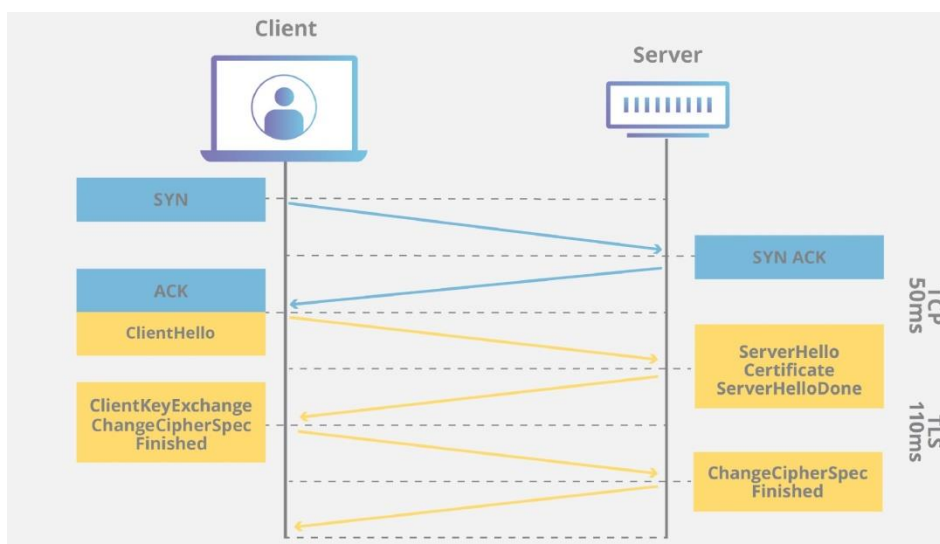
Implementation of SSL_TSL

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)

ssl						
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
9	0.088543	192.168.1.102	173.194.79.106	TLSv1	252	Client Key Exchange
10	0.105145	173.194.79.106	192.168.1.102	TLSv1	113	Change Cipher Spec
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
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps TCP Option - No-Operation (NOP) TCP Option - No-Operation (NOP) TCP Option - Timestamps: TSval 1222755773, TSecr 1520057963 [Timestamps] [Time since first frame in this TCP stream: 0.105436000 seconds] [Time since previous frame in this TCP stream: 0.000235000 seconds] [SEQ/ACK analysis] TCP payload (173 bytes) Transport Layer Security TLSv1 Record Layer: Application Data Protocol: http-over-tls Content Type: Application Data (23) Version: TLS 1.0 (0x0301) Length: 168 Encrypted Application Data: 52e78fc0f73eeca76cc499ad794fd69ee412be8ba893114f5d8906232bdd0 [Application Data Protocol: http-over-tls]						
0000	00 16 b6 e3 e9 8d 70 56	81 a2 05 1d 08 00 45 00pV.....E.			
0010	00 e1 60 fd 40 00 40 06	19 df c0 a8 01 66 ad c2	..`.@.f..			
0020	4f 6a eb 55 01 bb 4f 70	a8 1b 4c 74 61 13 80 18	Oj.U..Op..Lta...			
0030	ff ff 7c 62 00 00 01 01	08 0a 48 e1 c5 bd 5a 9a	.. b....H..Z.			
0040	3e 6b 17 03 01 00 a8 52	e7 8f c0 f7 3e ec 8a 76	>k....R....>..v			
0050	cc 49 9a d7 94 fd 69 ee	41 2b e8 ba 89 31 14 f5	..I....i..A+...1..			
0060	d8 90 62 32 bd d0 92 4f	0d c7 d9 9f d7 c2 77 75	..b2...0.....wu			
0070	5d 45 76 0f ff 2c 13 aa	41 95 86 9f a3 a6 0d 65]Ev...A.....e			
0080	c3 98 e7 08 e0 f0 36 5e	94 d8 b1 2d 41 c9 1c a96^....-A...			
0090	6d 29 4c 5e 6b 7e 50 12	81 30 6a 1b 82 77 a9 37	m)L^k-P...0j..w.7			
00a0	be 1a 61 93 19 85 77 ee	35 de 4a cb a9 58 29 cf	..a...w.5.J..X).			
00b0	6c 57 c2 22 d9 ba a9 61	09 bf 99 a8 25 98 ba 6b	lW."...a...%..k			
00c0	86 73 9a 2e 39 10 83 ff	e1 18 8e 79 d9 12 19 e3	..s..q@... ..v..RT.			

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

ssl						
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, Serve
9	0.088543	192.168.1.102	173.194.79.106	TLSv1	252	Client Key Exchang
10	0.105145	173.194.79.106	192.168.1.102	TLSv1	113	Change Cipher Spec
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,
Transport Layer Security						
TLSv1 Record Layer: Handshake Protocol: Client Hello						
Content Type: Handshake (22)						
Version: TLS 1.0 (0x0301)						
Length: 115						
Handshake Protocol: Client Hello						
Handshake Type: Client Hello (1)						
Length: 111						
Version: TLS 1.0 (0x0301)						
Random: 501778d316c25064f7cb0209b336ab332d969b8e091d26d4ccd04b731d7e550f						
Session ID Length: 0						
Cipher Suites Length: 46						
Cipher Suites (23 suites)						
Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)						
Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)						
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)						
Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)						
0000	00 16 b6 e3 e9 8d 70 56	81 a2 05 1d 08 00 45 00pV.....E.			
0010	00 ac db 88 40 00 40 06	9f 88 c0 a8 01 66 ad c2@.f..			
0020	4f 6a eb 55 01 bb 4f 70	a6 e9 4c 74 5a 23 80 18	Oj.U..Op..LtZ#..			
0030	ff ff 42 5c 00 00 01 01	08 0a 48 e1 c5 6b 5a 9a	..B\....H..kZ.			
0040	3e 14 16 03 01 00 73 01	00 00 6f 03 01 50 17 78	>.....s...o..P.x			
0050	d3 16 c2 50 64 f7 cb 02	09 b3 36 ab 33 2d 96 9b	...Pd....6.3...			
0060	8e 09 1d 26 d4 cc d0 4b	73 1d 7e 55 0f 00 00 2e	...&...K s~U...			
0070	00 39 00 38 00 35 00 16	00 13 00 0a 00 33 00 32	.9.8.5...3.2			
0080	00 2f 00 9a 00 99 00 96	00 05 00 04 00 15 00 12	./.....			
0090	00 09 00 14 00 11 00 08	00 06 00 03 00 ff 02 01			
00a0	00 00 17 00 00 00 13 00	11 00 00 0e 77 77 77 2ewww.			
00b0	67 6f 6f 67 6c 65 2e 63	6f 6d	google.c om			

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

ssl							
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, Serve	
	9 0.088543	192.168.1.102	173.194.79.106	TLSv1	252	Client Key Exchang	
	10 0.105145	173.194.79.106	192.168.1.102	TLSv1	113	Change Cipher Spec	
	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,	
Content Type: Handshake (22)							
Version: TLS 1.0 (0x0301)							
Length: 115							
Handshake Protocol: Client Hello							
Handshake Type: Client Hello (1)							
Length: 111							
Version: TLS 1.0 (0x0301)							
Random: 501778d316c25064f7cb0209b336ab332d969b8e091d26d4ccd04b731d7e550f							
GMT Unix Time: Jul 31, 2012 11:48:59.000000000 IST							
Random Bytes: 16c25064f7cb0209b336ab332d969b8e091d26d4ccd04b731d7e550f							
Session ID Length: 0							
Cipher Suites Length: 46							
Cipher Suites (23 suites)							
Compression Methods Length: 2							
Compression Methods (2 methods)							
Extensions Length: 23							
Extensions: server_name (len=10)							
0000	00 16 b6 e3 e9 8d 70 56	81 a2 05 1d 08 00 45 00pV.....E.				
0010	00 ac db 88 40 00 40 06	9f 88 c0 a8 01 66 ad c2@.f..				
0020	4f 6a eb 55 01 bb 4f 70	a6 e9 4c 74 5a 23 80 18	Oj.U..Op..LtZ#.				
0030	ff ff 42 5c 00 00 01 01	08 0a 48 e1 c5 6b 5a 9a	..B\....H..kZ.				
0040	3e 14 16 03 01 00 73 01	00 00 6f 03 01 50 17 78	>.....s..o..P.x				
0050	d3 16 c2 50 64 f7 cb 02	09 b3 36 ab 33 2d 96 9b	...Pd....6.3...				
0060	8e 09 1d 26 d4 cc d0 4b	73 1d 7e 55 0f 00 00 2e	...&...K s~U...				
0070	00 39 00 38 00 35 00 16	00 13 00 0a 00 33 00 32	.9.8.5...3.2				
0080	00 2f 00 9a 00 99 00 96	00 05 00 04 00 15 00 12	./.....				
0090	00 09 00 14 00 11 00 08	00 06 00 03 00 ff 02 01				
00a0	00 00 17 00 00 00 13 00	11 00 00 0e 77 77 77 2ewww.				
00b0	67 6f 6f 67 6c 65 2e 63	6f 6d	google.c om				
Random values used for deriving keys (tls.handshake.random), 32 bytes							

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

ssl						
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
9	0.088543	192.168.1.102	173.194.79.106	TLSv1	252	Client Key Exchange
10	0.105145	173.194.79.106	192.168.1.102	TLSv1	113	Change Cipher Spec
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
Content Type: Handshake (22)						
Version: TLS 1.0 (0x0301)						
Length: 85						
Handshake Protocol: Server Hello						
Handshake Type: Server Hello (2)						
Length: 81						
Version: TLS 1.0 (0x0301)						
Random: 501778d3d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e00161a893						
GMT Unix Time: Jul 31, 2012 11:48:59.000000000 IST						
Random Bytes: d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e00161a893						
Session ID Length: 32						
Session ID: 8530bdac95116ccb343798b36cb2fd79c1e278cba1af41456c810c0cebfc4						
Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)						
Compression Method: null (0)						
Extensions Length: 9						
Extension: server_name (len=0)						
Extension: renegotiation_info (len=1)						
0060	66 ef 5f 13 76 9d 3a 52	e0 01 61 a8 93 20 85 30	f _ v : R _ a _			
0070	bd ac 95 11 6c cb 34 37	98 b3 6c b2 fd 79 c1 e2	... l 47 ... l y ..			
0080	78 cb a1 af 41 45 6c 81	0c 0c eb fc cc f4 00 05	x ... AEI ...			
0090	00 00 09 00 00 00 00 ff	01 00 01 00 16 03 01 06	...			
00a0	59 0b 00 06 55 00 06 52	00 03 25 30 82 03 21 30	Y ... U ... R ... %0 ... !0			
00b0	82 02 8a a0 03 02 01 02	02 10 4f 9d 96 d9 66 b0 0 ... f			
00c0	99 2b 54 c2 95 7c b4 15	7d 4d 30 0d 06 09 2a 86	+ T } M0 ... *			
00d0	48 86 f7 0d 01 01 05 05	00 30 4c 31 0b 30 09 06	H 0 L 1 0 ...			
00e0	03 55 04 06 13 02 5a 41	31 25 30 23 06 03 55 04	U Z A 1 % 0 # ... U			
00f0	0a 13 1c 54 68 61 77 74	65 20 43 6f 6e 73 75 6c	... Thawt e Consul			
0100	74 69 6e 67 20 28 50 74	79 29 20 4c 74 64 2e 31	ting (Pt y) Ltd.1			
0110	16 30 14 06 03 55 04 03	13 0d 54 68 61 77 74 65	0 ... U ... Thawt			
0120	20 53 47 43 20 43 41 30	1e 17 0d 31 31 31 30 32	SGC CA0 ... 11102			
0130	36 30 30 30 30 30 5a 17	0d 31 33 30 39 33 30	6000000Z ... 130930			
0140	32 33 35 39 35 39 5a 30	68 31 0b 30 09 06 03 55	235959Z0 h1 0 ... U			
0150	04 06 13 02 55 53 31 13	30 11 06 03 55 04 08 13	... US1 0 ... U ...			
0160	0a 43 61 6c 69 66 6f 72	6e 69 61 31 16 30 14 06	Califor nia1 0 ...			

Length of Session ID field (tls.handshake.session_id_length), 1 byte

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)

ssl						
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, Serve
	9 0.088543	192.168.1.102	173.194.79.106	TLSv1	252	Client Key Exchang
	10 0.105145	173.194.79.106	192.168.1.102	TLSv1	113	Change Cipher Spec
	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,
	31 0.155157	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data
Content Type: Handshake (22)						
Version: TLS 1.0 (0x0301)						
Length: 85						
Handshake Protocol: Server Hello						
Handshake Type: Server Hello (2)						
Length: 81						
Version: TLS 1.0 (0x0301)						
Random: 501778d3d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e00161a893						
GMT Unix Time: Jul 31, 2012 11:48:59.000000000 IST						
Random Bytes: d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e00161a893						
Session ID Length: 32						
Session ID: 8530bdac95116ccb343798b36cb2fd79c1e278cba1af41456c810c0cebfcccf4						
Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)						
Compression Method: null (0)						
Extensions Length: 9						
Extension: server_name (len=0)						
Extension: renegotiation_info (len=1)						
0080	78 cb a1 af 41 45 6c 81	0c 0c eb fc cc f4 00 05	x...AEI... ..			
0090	00 00 09 00 00 00 00 ff	01 00 01 00 16 03 01 06			
00a0	59 0b 00 06 55 00 06 52	00 03 25 30 82 03 21 30	Y...U..R ..%0..!0			
00b0	82 02 8a a0 03 02 01 02	02 10 4f 9d 96 d9 66 b00...f.			
00c0	99 2b 54 c2 95 7c b4 15	7d 4d 30 0d 06 09 2a 86	..+T... .}M0...*.			
00d0	48 86 f7 0d 01 01 05 05	00 30 4c 31 0b 30 09 06	H..... ..0L1.0..			
00e0	03 55 04 06 13 02 5a 41	31 25 30 23 06 03 55 04	..U...ZA 1%0#...U.			
00f0	0a 13 1c 54 68 61 77 74	65 20 43 6f 6e 73 75 6c	...Thawt e Consul			
0100	74 69 6e 67 20 28 50 74	79 29 20 4c 74 64 2e 31	ting (Pt y) Ltd.1			
0110	16 30 14 06 03 55 04 03	13 0d 54 68 61 77 74 65	..0...U... ..Thawte			
0120	20 53 47 43 20 43 41 30	1e 17 0d 31 31 31 30 32	SGC CA0 ...11102			
0130	36 30 30 30 30 30 30 5a	17 0d 31 33 30 39 33 30	6000000Z ...130930			
0140	32 33 35 39 35 39 5a 30	68 31 0b 30 09 06 03 55	235959Z0 h1.0...U			
0150	04 06 13 02 55 53 31 13	30 11 06 03 55 04 08 13	...US1. 0...U...			
0160	0a 43 61 6c 69 66 6f 72	6e 69 61 31 16 30 14 06	..Califor nia1.0..			
0170	03 55 04 07 14 0d 4d 6f	75 6e 74 61 69 6e 20 56	..U...Mo untain V			
0180	69 65 77 31 13 30 11 06	03 55 04 0a 14 0a 47 6f	iew1.0... ..U...Go			
Cipher Suite (tls.handshake.ciphersuite), 2 bytes						

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

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
10	0.105145	173.194.79.106	192.168.1.102	TLSv1	113	Change Cipher Spec, Encrypted
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
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

[2 Reassembled TCP Segments (1630 bytes): #6(1328), #7(302)]
 Transport Layer Security
 TLSv1 Record Layer: Handshake Protocol: Certificate
 Content Type: Handshake (22)
 Version: TLS 1.0 (0x0301)
 Length: 1625
 Handshake Protocol: Certificate
 Handshake Type: Certificate (11)
 Length: 1621
 Certificates Length: 1618
 Certificates (1618 bytes)
 Transport Layer Security
 TLSv1 Record Layer: Handshake Protocol: Server Hello Done
 Content Type: Handshake (22)
 Version: TLS 1.0 (0x0301)
 Length: 4
 Handshake Protocol: Server Hello Done

0000	16 03 01 06 59 0b 00 06	55 00 06 52 00 03 25 30Y... U..R..%0
0010	82 03 21 30 82 02 8a a0	03 02 01 02 02 10 4f 9d	..!0.... ..0.
0020	96 d9 66 b0 99 2b 54 c2	95 7c b4 15 7d 4d 30 0d	..f..+T. . .}M0.
0030	06 09 2a 86 48 86 f7 0d	01 01 05 05 00 30 4c 31	..*.H... ..0L1
0040	0b 30 09 06 03 55 04 06	13 02 5a 41 31 25 30 23	.0...U... ..ZA1#0#
0050	06 03 55 04 0a 13 1c 54	68 61 77 74 65 20 43 6f	..U....T hawte Co
0060	6e 73 75 6c 74 69 6e 67	20 28 50 74 79 29 20 4c	nsulting (Pty) L
0070	74 64 2e 31 16 30 14 06	03 55 04 03 13 0d 54 68	td.1.0... .U....Th
0080	61 77 74 65 20 53 47 43	20 43 41 30 1e 17 0d 31	awte SGC CA0...1
0090	31 31 30 32 36 30 30 30	30 30 30 5a 17 0d 31 33	11026000 000Z..13
00a0	30 39 33 30 32 33 35 39	35 39 5a 30 68 31 0b 30	09302359 59Z0h1.0
00b0	09 06 03 55 04 06 13 02	55 53 31 13 30 11 06 03	...U.... US1.0...
00c0	55 04 08 13 0a 43 61 6c	69 66 6f 72 6e 69 61 31	U....Cal ifornia1
00d0	16 30 14 06 03 55 04 07	14 0d 4d 6f 75 6e 74 61	.0...U... ..Mounta
00e0	69 6e 20 56 69 65 77 31	13 30 11 06 03 55 04 0a	in View1 .0...U..

Frame (377 bytes) Reassembled TCP (1630 bytes)
 Record Layer (tls.record), 1,630 bytes

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
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

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

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
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

▶ Frame 9: 252 bytes on wire (2016 bits), 252 bytes captured (2016 bits) on interface en0, id 0
 ▶ Ethernet II, Src: Apple_a2:05:1d (78:56:81:a2:05:1d), Dst: Cisco-Li_e3:e9:8d (00:16:b6:e3:e9:8d)
 ▶ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 173.194.79.106
 ▶ Transmission Control Protocol, Src Port: 60245, Dst Port: 443, Seq: 121, Ack: 1730, Len: 186
 ▼ Transport Layer Security
 ▶ TLSv1 Record Layer: Handshake Protocol: Client Key Exchange
 Content Type: Handshake (22)
 Version: TLS 1.0 (0x0301)
 Length: 134
 ▶ Handshake Protocol: Client Key Exchange
 Handshake Type: Client Key Exchange (16)
 Length: 130
 ▶ RSA Encrypted PreMaster Secret
 ▶ TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
 Content Type: Change Cipher Spec (20)
 Version: TLS 1.0 (0x0301)
 Length: 1
 Change Cipher Spec Message
 ▶ TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
 Content Type: Handshake (22)
 Version: TLS 1.0 (0x0301)
 Length: 36
 Handshake Protocol: Encrypted Handshake Message

CODE:

```
#include<bits/stdc++.h>

using namespace std;

// returns x where (a * x) % b == 1
int mul_inv(int a, int b)
{
    int b0 = b, t, q;
    int x0 = 0, x1 = 1;
    if (b == 1) return 1;
    while (a > 1) {
        q = a / b;
```



```
        t = b, b = a % b, a = t;
        t = x0, x0 = x1 - q * x0, x1 = t;
    }
    if (x1 < 0) x1 += b0;
    return x1;
}

int chinese_remainder(int *n, int *a, int len)
{
    int p, i, prod = 1, sum = 0;

    for (i = 0; i < len; i++)
        prod *= n[i];

    cout<<"The Product of Divisors is: "<<prod<<endl;

    for (i = 0; i < len; i++) {
        p = prod / n[i];
        sum += a[i] * mul_inv(p, n[i]) * p;
    }

    return sum % prod;
}

int main(void)
{
    int n[] = { 5, 7, 9 };
    int r[] = { 2, 3, 2 };

    cout<<"The Divisors are: ";

    for(int i = 0;i < 3;i++)
        cout<<n[i]<<" ";

    cout<<"and their respective remainder are: ";

    for(int i = 0;i < 3;i++)
        cout<<r[i]<<" ";

    cout<<endl;

    int ans = chinese_remainder(n, r, sizeof(n)/sizeof(n[0]));

    cout<<"Output: "<<ans<<endl;
    return 0;
}
```

OUTPUT:

```
PS C:\Users\Admin\Desktop\WCE VII\CNS LAB\Assignment 14> cd "c:\Users\Admin\Desktop\WCE VII\CNS LAB\Assignment 14" ; if ($?) { g++ Chinese.cpp -o Chinese } ; if ($?) { .\Chinese }
The Divisors are: 5 7 9 and their respective remainder are: 2 3 2
The Product of Divisors is: 315
Output: 227
PS C:\Users\Admin\Desktop\WCE VII\CNS LAB\Assignment 14> █
```