

# Lab 8 – SSL/TLS

IT 520-A – Enterprise Infrastructure & Networks



Capture your packets in an SSL session. To do this, you should go to your favorite e-commerce site and begin the process of purchasing an item (but terminating before making the actual purpose!). After capturing the packets with Wireshark, you should set the filter so that it displays only the Ethernet frames that contain SSL records sent from and received by your host. (An SSL record is the same thing as an SSL message.)

Your Wireshark GUI should be displaying only the Ethernet frames that have SSL records. It is important to keep in mind that an Ethernet frame may contain one or more SSL records. (This is very different from HTTP, for which each frame contains either one complete HTTP message or a portion of a HTTP message.) Also, an SSL record may not completely fit into an Ethernet frame, in which case multiple frames will be needed to carry the record. Locate the “Client Hello” and “Server Hello” frame and use the frames to answer the questions.

- *(For each of these questions, take a screenshot of Wireshark, and attach it to your answer) - Questions without Full Screenshot will not be graded. A lab submission template is available on canvas. Your screenshot should indicate the time and date on your computer.*
- *Include a terminal screenshot showing computer IP address on the front page before Question 1, and a full PRINT of the HTTP OK message as the last page.*

*Lab will NOT be graded if either of these two is missing.*

*Questions:*

*Client Hello Record:*



1. What is the SSL/TLS version of the of the Client Hello frame?

Wireshark packet capture interface showing a TLS handshake. The packet list displays several packets, with packet 5665 (Client Hello) selected. The packet details pane shows the TLSv1.2 Record Layer: Handshake Protocol: Client Hello structure. The packet bytes pane displays the raw hex and ASCII data.

No.	Time	Source	Destination	Protocol	Length	Info
5643	5.858613	10.0.0.106	23.160.0.254	TLSv1..	605	Application Data
5644	5.877690	52.46.157.171	10.0.0.106	TLSv1..	328	Application Data
5653	6.074807	23.160.0.254	10.0.0.106	TLSv1..	964	Application Data
5665	6.129608	10.0.0.106	52.223.241.5	TLSv1..	583	Client Hello
5666	6.148890	52.223.241.5	10.0.0.106	TLSv1..	1514	Server Hello
5667	6.151417	52.223.241.5	10.0.0.106	TLSv1..	1514	Certificate [TCP segment of a reassembled PDU]
5668	6.151419	52.223.241.5	10.0.0.106	TLSv1..	164	Server Key Exchange, Server Hello Done
5671	6.154650	10.0.0.106	52.223.241.5	TLSv1..	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
5672	6.173333	52.223.241.5	10.0.0.106	TLSv1..	117	Change Cipher Spec, Encrypted Handshake Message
5674	6.174005	10.0.0.106	52.223.241.5	TLSv1..	1436	Application Data
5680	6.191256	52.223.241.5	10.0.0.106	TLSv1..	95	Application Data
5694	6.208338	52.223.241.5	10.0.0.106	TLSv1..	832	Application Data
5698	6.218931	10.0.0.106	99.84.218.130	TLSv1..	201	Application Data

Frame 5665: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface 0  
Ethernet II, Src: Apple77:70:03 (38:f9:d3:77:70:03), Dst: ArrisGro\_8a:ad:ef (10:56:11:8a:ad:ef)  
Internet Protocol Version 4, Src: 10.0.0.106, Dst: 52.223.241.5  
Transmission Control Protocol, Src Port: 49437, Dst Port: 443, Seq: 1, Ack: 1, Len: 517  
Transport Layer Security  
▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello  
Content Type: Handshake (22)  
Version: TLS 1.0 (0x0301)  
Length: 512  
Handshake Protocol: Client Hello

0040 28 05 16 03 01 02 00 01 00 01 fc 03 03 9d a9 66 (.....f  
0050 41 3c 08 0d c7 a2 1a 3f 5e 00 e8 9a 21 6c 47 57 Ac.....? A...lGw  
0060 6a f8 9e 71 8f 25 07 70 0a d3 e4 97 25 20 0f 70 j-q% x...% p  
0070 af 35 6f 1e b1 af 55 e0 a6 3b 5c b4 1d fe f5 12 5o...U...; \.....  
0080 1b f9 34 25 02 98 8b 48 34 1a 53 d4 0d 2d 00 34 4%...H 4:S...4  
0090 13 03 13 01 13 02 c0 2c c0 2b c0 24 c0 23 c0 0a .....+ \$-#-  
00a0 c0 09 cc a9 c0 30 c0 2f c0 28 c0 27 c0 14 c0 13 .....0 / : ( '.....  
00b0 cc a8 00 9d 00 9c 00 3d 00 3c 00 35 00 2f c0 08 .....= < \$ /...  
00c0 c0 12 00 0a 01 00 01 7f ff 01 00 01 00 00 00 00 .....  
00d0 25 00 23 00 00 20 76 69 64 65 6f 2d 77 65 61 76 %-#- vi deo-weav  
00e0 65 72 2e 69 61 64 30 33 2e 68 6c 73 2e 74 74 76 er.iad03 .hls.ttv  
00f0 6e 77 2e 6e 65 74 00 17 00 00 00 0d 00 18 00 16 nw.net... ..  
0100 04 03 00 04 04 01 05 03 02 03 00 05 00 05 01 .....  
0110 08 06 06 01 02 01 00 05 00 05 01 00 00 00 00 33 .....3  
0120 74 00 00 00 12 00 00 00 10 00 30 00 2e 02 68 32 t.....-0...h2  
0130 05 68 32 2d 31 36 05 68 32 2d 31 35 05 68 32 2d h2-16-h 2-15-h2-  
0140 31 34 08 73 70 64 79 2f 33 2e 31 06 73 70 64 79 14-spdy/ 3.1-spdy

Record Layer (tls.record), 517 bytes  
Packets: 19215 - Displayed: 4915 (25.6%) - Dropped: 0 (0.0%)  
Profile: Default

- Expand the ClientHello record. (If your trace contains multiple ClientHello records, expand

The image shows a Wireshark packet capture of a TLS handshake. The packet list on the left shows a ClientHello record at frame 5665. The packet details pane on the right shows the expanded ClientHello record, including the Version (TLS 1.0), Length (512), and the Handshake Protocol (Client Hello). The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
5643	5.858613	10.0.0.106	23.160.0.254	TLSv1..	605	Application Data
5644	5.877690	52.46.157.171	10.0.0.106	TLSv1..	328	Application Data
5653	6.074807	23.160.0.254	10.0.0.106	TLSv1..	964	Application Data
5665	6.129608	10.0.0.106	52.223.241.5	TLSv1..	583	Client Hello
5666	6.148890	52.223.241.5	10.0.0.106	TLSv1..	1514	Server Hello
5667	6.151417	52.223.241.5	10.0.0.106	TLSv1..	1514	Certificate [TCP segment of a reassembled PDU]
5668	6.151419	52.223.241.5	10.0.0.106	TLSv1..	164	Server Key Exchange, Server Hello Done
5671	6.154650	10.0.0.106	52.223.241.5	TLSv1..	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
5672	6.173333	52.223.241.5	10.0.0.106	TLSv1..	117	Change Cipher Spec, Encrypted Handshake Message
5674	6.174005	10.0.0.106	52.223.241.5	TLSv1..	1436	Application Data
5680	6.191256	52.223.241.5	10.0.0.106	TLSv1..	95	Application Data
5694	6.208338	52.223.241.5	10.0.0.106	TLSv1..	832	Application Data
5698	6.218931	10.0.0.106	99.84.218.130	TLSv1..	201	Application Data

Frame 5665: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface 0  
 Ethernet II, Src: Apple\_77:70:03 (38:f9:d3:77:70:03), Dst: ArrisGro\_Ba:ad:ef (10:56:11:8a:ad:ef)  
 Internet Protocol Version 4, Src: 10.0.0.106, Dst: 52.223.241.5  
 Transmission Control Protocol, Src Port: 49437, Dst Port: 443, Seq: 1, Ack: 1, Len: 517  
 Transport Layer Security  
 TLSv1.2 Record Layer: Handshake Protocol: Client Hello  
 Content Type: Handshake (22)  
 Version: TLS 1.0 (0x0301)  
 Length: 512  
 Handshake Protocol: Client Hello

0040 20 05 16 03 01 02 00 01 00 01 fc 03 03 9d a9 66 (- .....f  
 0050 41 3c 08 0d c7 a2 1a 3f 5e 00 e8 9a 21 6c 47 57 A.....? ^...!LGW  
 0060 6a f8 9e 71 8f 25 07 78 0a d3 e4 97 25 20 0f 70 j..q..x ....% .p  
 0070 af 35 6f 1e b1 af 55 e0 a6 3b 5c b4 1d fe f5 12 .5o...U. .;\.....  
 0080 1b f9 34 25 02 98 8b 48 34 1a 53 d4 0d 2d 00 34 ..4...H 4:S...4  
 0090 13 03 13 01 13 02 c0 2c c0 2b c0 24 c0 23 c0 0a .....+.\$#..  
 00a0 c0 09 cc a9 c0 30 c0 2f c0 28 c0 27 c0 14 c0 13 .....0/.{.'.....  
 00b0 cc a8 00 9d 00 9c 00 3d 00 3c 00 35 00 2f c0 08 .....=<.5./...  
 00c0 c0 12 00 0a 01 00 01 7f ff 01 00 01 00 00 00 00 .....  
 00d0 25 00 23 00 00 20 76 69 64 65 6f 2d 77 65 61 76 %-#.. vi deo-weav  
 00e0 65 72 2e 69 61 64 30 33 2e 68 6c 73 2e 74 74 76 er.iad03 .hls.ttv  
 00f0 6e 77 2e 6e 65 74 00 17 00 00 00 00 18 00 16 mw.net.....  
 0100 04 03 08 04 04 01 05 03 02 03 08 05 08 05 01 .....  
 0110 08 06 06 01 02 01 00 05 00 05 01 00 00 00 33 .....3  
 0120 74 00 00 00 12 00 00 00 10 00 30 00 2e 02 68 32 t.....-0...h2  
 0130 05 68 32 2d 31 36 05 68 32 2d 31 35 05 68 32 2d -h2-16-h 2-15-h2-  
 0140 31 34 08 73 70 64 79 2f 33 2e 31 06 73 70 64 79 14-spdy/ 3.1-spdy

the frame that contains the first one.) What is the value of the content type?

- Does the Client Hello record contain a nonce (also known as a “challenge”)? If so, what is

the value of the challenge in hexadecimal notation?

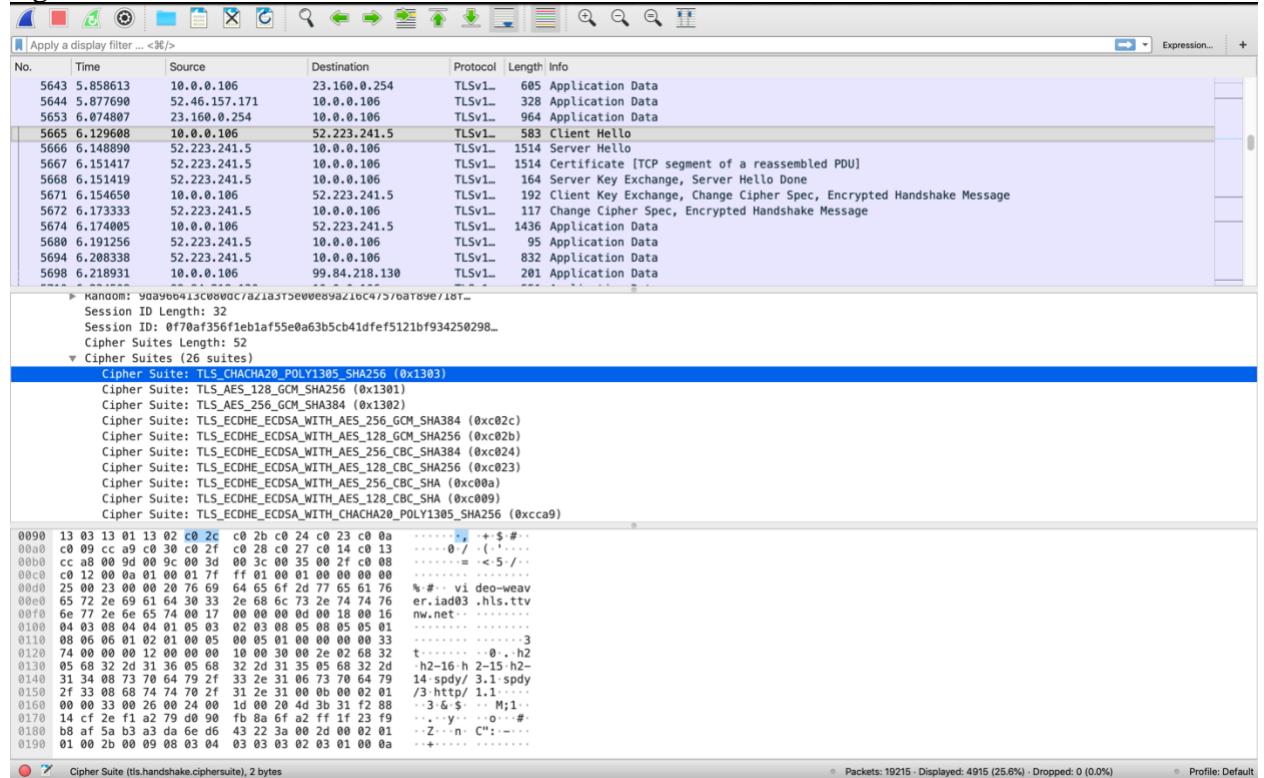
When I checked Wireshark it is not showing nonce or challenge at all at the Clint hello record

No.	Time	Source	Destination	Protocol	Length	Info
67	3.609421	2607:f8b0:4004:805...	2601:151:c000:5b20...	TLSv1..	540	Application Data
70	3.618868	2607:f8b0:4004:805...	2601:151:c000:5b20...	TLSv1..	241	Application Data
71	3.618875	2607:f8b0:4004:805...	2601:151:c000:5b20...	TLSv1..	162	Application Data
72	3.618877	2607:f8b0:4004:805...	2601:151:c000:5b20...	TLSv1..	132	Application Data
77	3.611987	2601:151:c000:5b20...	2607:f8b0:4004:805...	TLSv1..	132	Application Data
79	3.612751	10.0.0.106	99.84.220.24	TLSv1..	583	Client Hello
81	3.632849	99.84.220.24	10.0.0.106	TLSv1..	1514	Server Hello
84	3.632855	99.84.220.24	10.0.0.106	TLSv1..	997	Certificate, Certificate Status, Server Key Exchange, Server Hello Done
88	3.641313	2601:151:c000:5b20...	2607:f8b0:4004:805...	TLSv1..	159	Application Data
89	3.643747	10.0.0.106	17.249.105.246	TLSv1..	789	Application Data
91	3.664056	10.0.0.106	99.84.220.24	TLSv1..	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
93	3.682060	99.84.220.24	10.0.0.106	TLSv1..	117	Change Cipher Spec, Encrypted Handshake Message
94	3.682061	99.84.220.24	10.0.0.106	TLSv1..	135	Application Data
Session ID Length: 34						
Session ID: 6b2a0e7ae144f9c08fe22cedb874055d308d99d9779da2ce..						
Cipher Suites Length: 52						
► Cipher Suites (26 suites)						
Compression Methods Length: 1						
► Compression Methods (1 method)						
Extensions Length: 383						
► Extension: renegotiation_info (len=1)						
► Extension: server_name (len=19)						
► Extension: extended_master_secret (len=0)						
► Extension: signature_algorithms (len=24)						
► Extension: status_request (len=5)						
► Extension: next_protocol_negotiation (len=0)						
► Extension: signed_certificate_timestamp (len=0)						
► Extension: application_layer_protocol_negotiation (len=48)						
0090	13 03 13 01 13 02 c0 2c	c0 2b c0 24 c0 23 c0 0a	....., +-\$.#..			
00a0	c0 09 cc a9 c0 30 c0 2f	c0 28 c0 27 c0 14 c0 13	.....0 / .{.'....			
00b0	cc a8 00 9d 00 9c 00 3d	00 3c 00 35 00 2f c0 08	.....~<5 / ..			
00c0	c0 12 00 0a 01 00 01 7f	ff 01 00 01 00 00 00 00	.....			
00d0	13 00 11 00 00 0e 77 77	77 2e 61 6d 61 7a 6f 6e	.....ww w.amazon			
00e0	2e 63 6f 6d 00 17 00 00	00 0d 00 18 00 16 04 03	.....com.....			
00f0	08 04 04 01 05 03 02 03	08 05 08 05 05 01 08 06	.....			
0100	06 01 02 01 00 05 00 05	01 00 00 00 00 33 74 00	.....3T.....			
0110	00 00 12 00 00 00 10 00	30 00 2e 02 68 32 05 68	.....0..h2-h			
0120	32 2d 31 36 05 68 32 2d	31 35 05 68 32 2d 31 34	2-16-h2- 15-h2-14			
0130	08 73 70 64 79 2f 33 2e	31 06 73 70 64 79 2f 33	-spdy/3. 1-spdy/3			
0140	08 68 74 74 70 2f 31 2e	31 00 0b 00 02 01 00 00	http/1. 1.....			
0150	33 00 26 00 24 00 1d 00	20 7d d5 c5 6c b2 e9 aa	3-G-\$-... }..1...			
0160	2f 9c 65 69 72 de 35 97	03 f2 9c dc 47 da fa 32	/-eir-5- ....G..2			
0170	68 09 b5 4d f5 79 e2 a5	14 00 2d 00 02 01 01 00	h..M.y.....			
0180	2b 00 09 08 03 04 03 03	03 02 03 01 00 0a 00 0a	.....			
0190	00 08 00 1d 00 17 00 18	00 19 00 15 00 a9 00 00	.....			

This is a screen shot of the Client hello record and it is not showing nonce or challenge

- Does the ClientHello record advertise the cyber suites it supports? If so, in the first listed

Suite, what are the public-key algorithm, the symmetric-key algorithm, and the mdash algorithm?



The image shows a Wireshark packet capture of a TLS handshake. The top pane displays a list of packets, with packet 5665 (Client Hello) selected. The middle pane shows the details of the selected packet, including the Session ID, Cipher Suites, and the selected Cipher Suite (TLS\_CHACHA20\_POLY1305\_SHA256). The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
5643	5.858613	10.0.0.106	23.160.0.254	TLSv1_	605	Application Data
5644	5.877690	52.46.157.171	10.0.0.106	TLSv1_	328	Application Data
5653	6.074807	23.160.0.254	10.0.0.106	TLSv1_	964	Application Data
5665	6.129608	10.0.0.106	52.223.241.5	TLSv1_	583	Client Hello
5666	6.148890	52.223.241.5	10.0.0.106	TLSv1_	1514	Server Hello
5667	6.151417	52.223.241.5	10.0.0.106	TLSv1_	1514	Certificate [TCP segment of a reassembled PDU]
5668	6.151419	52.223.241.5	10.0.0.106	TLSv1_	164	Server Key Exchange, Server Hello Done
5671	6.154650	10.0.0.106	52.223.241.5	TLSv1_	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
5672	6.173333	52.223.241.5	10.0.0.106	TLSv1_	117	Change Cipher Spec, Encrypted Handshake Message
5674	6.174005	10.0.0.106	52.223.241.5	TLSv1_	1436	Application Data
5680	6.191256	52.223.241.5	10.0.0.106	TLSv1_	95	Application Data
5694	6.208338	52.223.241.5	10.0.0.106	TLSv1_	832	Application Data
5698	6.218931	10.0.0.106	99.84.218.130	TLSv1_	201	Application Data

Handshake details:

- Session ID Length: 32
- Session ID: 0f70af356f1eb1af55e0a63b5cb41dfe5121bf934250298...
- Cipher Suites Length: 52
- Cipher Suites (26 suites):
  - Cipher Suite: TLS\_CHACHA20\_POLY1305\_SHA256 (0xc1303)
  - Cipher Suite: TLS\_AES\_128\_GCM\_SHA256 (0xc1301)
  - Cipher Suite: TLS\_AES\_256\_GCM\_SHA384 (0xc1302)
  - Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc02c)
  - Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02b)
  - Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384 (0xc024)
  - Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 (0xc023)
  - Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA (0xc00a)
  - Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA (0xc009)
  - Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_CHACHA20\_POLY1305\_SHA256 (0xc0a9)

Raw packet data (hex):

```
0090 13 03 13 01 13 02 c0 2c c0 2b c0 24 c0 23 c0 0a .....+-$#...
00a0 c0 09 cc a9 c0 30 c0 2f c0 28 c0 27 c0 14 c0 13 .....0/({'...
00b0 cc a8 00 9d 00 9c 00 3d 00 3c 00 35 00 2f c0 08 .....=<5/...
00c0 c0 12 00 0a 01 00 01 7f ff 01 00 01 00 00 00 .....
00d0 25 00 23 00 00 20 76 69 64 65 6f 2d 77 65 61 76 %-#-v1 deo-weav
00e0 65 72 2e 69 61 64 30 33 2e 68 6c 73 2e 74 74 76 er.iad03 .hls.ttv
00f0 6e 77 2e 6e 65 74 00 17 00 00 00 0d 00 18 00 16 nw.net.....
0100 04 03 08 04 04 01 05 03 02 03 08 05 08 05 05 01 .....
0110 08 06 06 01 02 01 00 05 00 05 01 00 00 00 00 33 .....3
0120 74 00 00 00 12 00 00 00 10 00 30 00 2e 02 68 32 t-----0..h2
0130 05 68 32 2d 31 36 05 68 32 2d 31 35 05 68 32 2d -h2-16 h 2-15 h2-
0140 31 34 08 73 70 64 79 2f 33 2e 31 00 73 70 64 79 14-spdy/ 3.1-spdy
0150 2f 33 08 68 74 74 70 2f 31 2e 31 00 0b 00 02 01 /3-http/ 1.1....
0160 00 00 33 00 26 00 24 00 1d 00 20 4d 3b 31 f2 88 --3-&$- M;1..
0170 14 cf 2e f1 a2 79 d0 90 fb 8a 6f a2 ff 1f 23 f9 ...y- -o-#-
0180 b8 cf 5a b3 a3 da 6e d6 43 22 3a 00 2d 00 02 01 --Z-n- C!:-...
0190 01 00 2b 00 09 08 03 04 03 03 03 02 03 01 00 0a ...+-.....
```

Server Hello Record:

1. Locate the ServerHello SSL record. Does this record specify a chosen cipher suite? What

are the algorithms in the chosen cipher suite?

The image shows a Wireshark packet capture of a TLS handshake. The top pane displays a list of packets, with packet 5666 selected. The middle pane shows the details of the selected packet, and the bottom pane shows the raw packet data in hexadecimal and ASCII.

**Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
5643	5.858613	10.0.0.106	23.160.0.254	TLSv1..	605	Application Data
5644	5.877690	52.46.157.171	10.0.0.106	TLSv1..	328	Application Data
5653	6.074807	23.160.0.254	10.0.0.106	TLSv1..	964	Application Data
5665	6.129608	10.0.0.106	52.223.241.5	TLSv1..	583	Client Hello
5666	6.148890	52.223.241.5	10.0.0.106	TLSv1..	1514	Server Hello
5667	6.151417	52.223.241.5	10.0.0.106	TLSv1..	1514	Certificate [TCP segment of a reassembled PDU]
5668	6.151419	52.223.241.5	10.0.0.106	TLSv1..	164	Server Key Exchange, Server Hello Done
5671	6.154650	10.0.0.106	52.223.241.5	TLSv1..	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
5672	6.173333	52.223.241.5	10.0.0.106	TLSv1..	117	Change Cipher Spec, Encrypted Handshake Message
5674	6.174005	10.0.0.106	52.223.241.5	TLSv1..	1436	Application Data
5680	6.191256	52.223.241.5	10.0.0.106	TLSv1..	95	Application Data
5694	6.208338	52.223.241.5	10.0.0.106	TLSv1..	832	Application Data
5698	6.218931	10.0.0.106	99.84.218.130	TLSv1..	201	Application Data

**Packet 5666 Details:**

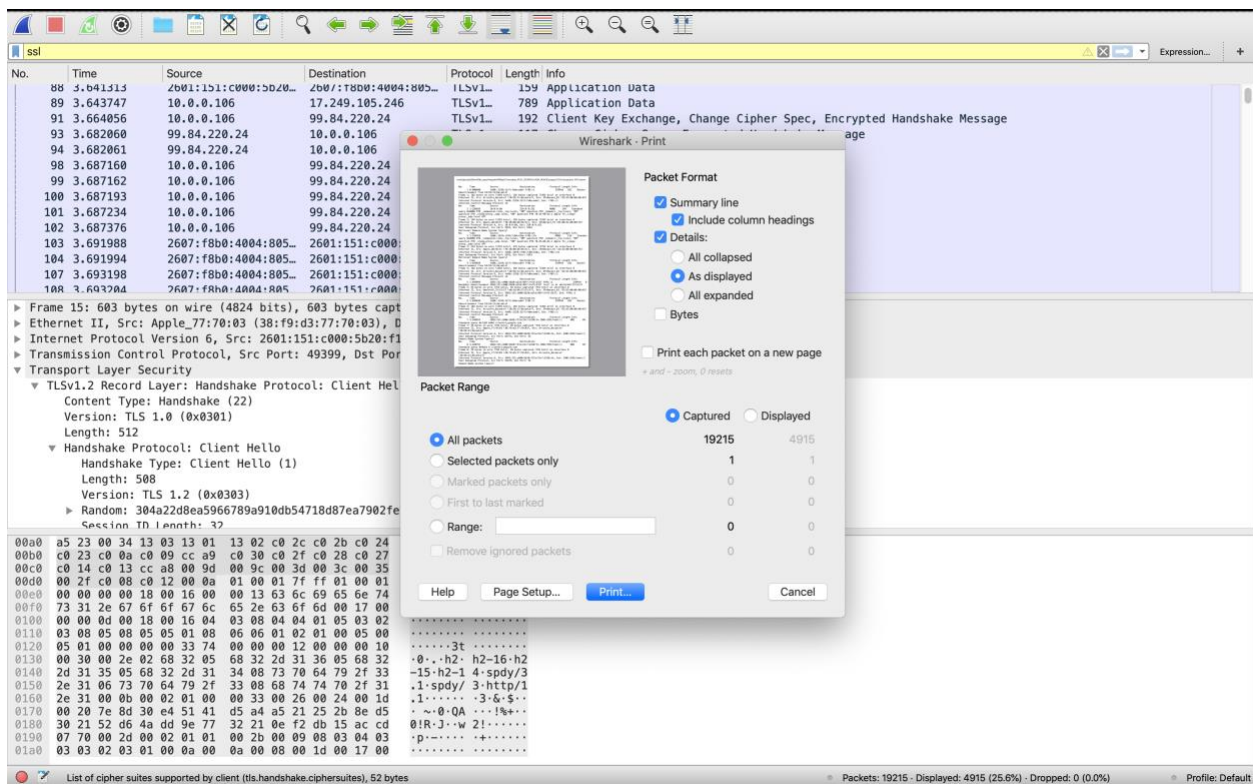
- Version: TLS 1.2 (0x0303)
- Length: 93
- Handshake Protocol: Server Hello
- Handshake Type: Server Hello (2)
- Length: 89
- Version: TLS 1.2 (0x0303)
- Random: 77e25fe7cf047239040f342fc8a409390ed59aaffcbce613..
- Session ID Length: 32
- Session ID: caf8701c7593a124c873f7eb706b5e7cc52ce0a88c5d5d53..
- Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02f)**
- Compression Method: null (0)
- Extensions Length: 17
- Extension: server\_name (len=0)
- Extension: renegotiation\_info (len=1)
- Extension: ec\_point\_formats (len=4)

**Raw Packet Data:**

```
0080 e0 a8 8c 5d 5d 53 aa b8 07 fd d4 86 1c 00 c0 2f ...]]S...
0090 00 00 11 00 00 00 00 ff 01 00 01 00 00 0b 00 04 .....
00a0 03 00 01 02 16 03 03 09 f0 0b 00 09 ec 00 09 e9 .....
00b0 00 05 4b 30 82 05 47 30 62 04 2f a0 03 02 01 02 ..K0..G0..
00c0 02 10 02 8b a8 bb 46 ab 01 59 00 cf 2e 98 1e 68 .....F..Y...h
00d0 fb da 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0b 05 ..0...H.....
00e0 00 30 4d 31 0b 30 09 06 03 55 04 06 13 02 55 53 ..0M1.0...U...US
00f0 31 15 30 13 06 03 55 04 0a 13 0c 44 69 67 69 43 1-0...U...Digic
0100 65 72 74 20 49 6e 63 31 27 30 25 06 03 55 04 03 ert Incl '0%-U-
0110 13 1e 44 69 67 69 43 65 72 74 20 53 48 41 32 20 ..DigicE rt SHA2
0120 53 65 63 75 72 65 20 53 65 72 76 65 72 20 43 41 Secure S erver CA
0130 30 1e 17 0d 31 37 30 33 31 37 30 30 30 30 30 30 0...1703 17000000
0140 5a 17 0d 32 30 30 33 32 35 31 32 30 30 30 30 30 5a Z..20032 5120000Z
0150 30 7d 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 011-0...U...US1
0160 13 30 11 06 03 55 04 08 13 0a 43 61 6c 69 66 6f ..0...U...Califo
0170 72 6e 69 61 31 16 30 14 06 03 55 04 07 13 0d 53 rnial-0...U...S
0180 61 6e 20 46 72 61 6e 63 69 73 63 6f 31 21 30 1f an Franc isco1f0-
```

**Summary:** Cipher Suite (tls.handshake.ciphersuite), 2 bytes. Packets: 19215 - Displayed: 4915 (25.6%) - Dropped: 0 (0.0%) - Profile: Default





It is not allowing me to print so I screen shot the print page  
Also there is no ok message