

Step 1. Capture a trace

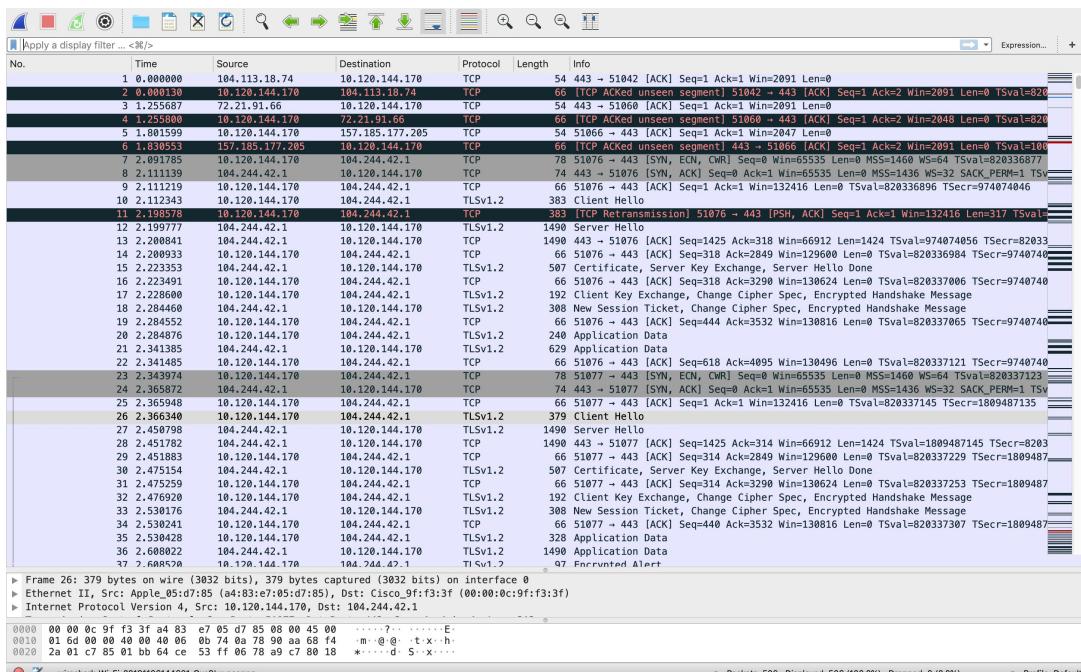
- 1) Find a URL, I am using this one, <http://www.twitter.com>.
- 2) Fetch the URL with wget command.

```
→ ~ wget --secure-protocol=TLSv1 --no-check-certificate https://www.twitter.com
--2019-11-06 14:46:17-- https://www.twitter.com/
Resolving www.twitter.com (www.twitter.com)... 104.244.42.1, 104.244.42.65
Connecting to www.twitter.com (www.twitter.com)|104.244.42.1|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://twitter.com/ [following]
--2019-11-06 14:46:17-- https://twitter.com/
Resolving twitter.com (twitter.com)... 104.244.42.1, 104.244.42.65
Connecting to twitter.com (twitter.com)|104.244.42.1|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 311425 (304K) [text/html]
Saving to: 'index.html.4'

index.html.4      100%[=====] 304.13K   685KB/s    in 0.4s

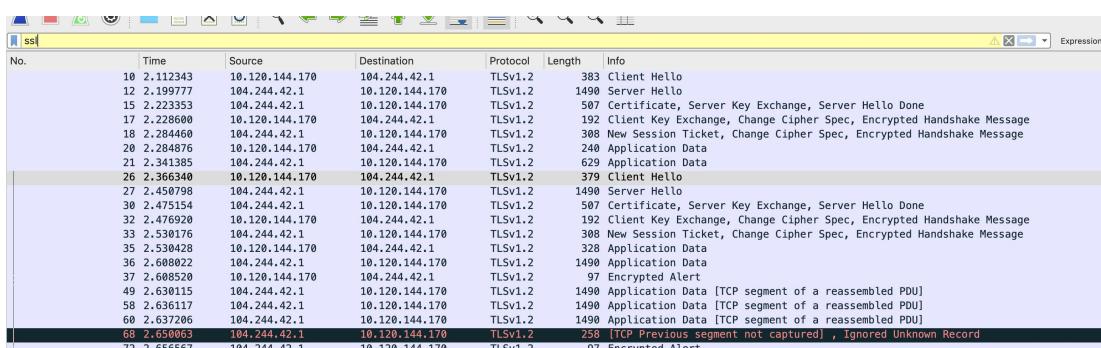
2019-11-06 14:46:18 (685 KB/s) - 'index.html.4' saved [311425/311425]
```

- 3) Set up the filter to be ‘tcp port 443’, then repeat the wget command in 2) step.



Step 2. Inspect the Trace and TCP Segment Structure

To begin with, type in ‘ssl’ in the filter.



Answer the following questions to show your understanding of SSL records:

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

Application Data (23)

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

TLS 1.2 (0x0303)

3. Does the Length cover the Record Layer header as well as payload, or only the payload?

Only the payload.

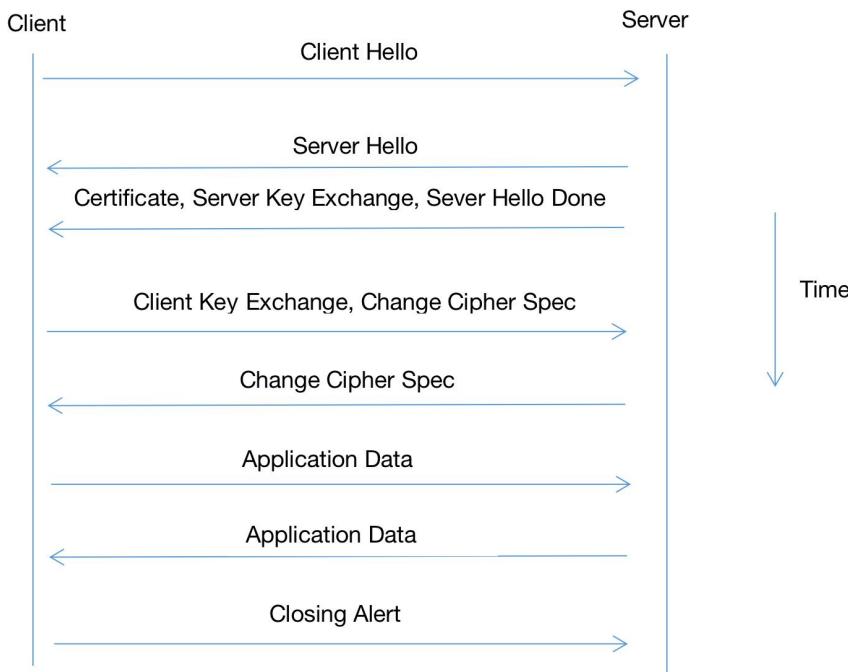
No.	Time	Source	Destination	Protocol	Length	Info
18	2.284460	104.244.42.1	10.120.144.170	TLSv1.2	308	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
20	2.284876	10.120.144.170	104.244.42.1	TLSv1.2	240	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
21	2.341385	104.244.42.1	10.120.144.170	TLSv1.2	629	Application Data
26	2.366240	10.120.144.170	104.244.42.1	TLSv1.2	370	Client Hello

Frame 20: 240 bytes on wire (1920 bits), 240 bytes captured (1920 bits) on interface 0
 ▷ Ethernet II, Src: Apple_05:d7:85 (a4:83:e7:05:d7:85), Dst: Cisco_9f:f3:3f (00:00:0c:9f:f3:3f)
 ▷ Internet Protocol Version 4, Src: 10.120.144.170, Dst: 104.244.42.1
 ▷ Transmission Control Protocol, Src Port: 51076, Dst Port: 443, Seq: 444, Ack: 3532, Len: 174
 ▷ Transport Layer Security
 ▷ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
 Content Type: Application Data (23)
 Version: TLS 1.2 (0x0303)
 Length: 169
 Encrypted Application Data: 2a7c06bf7dc86fc432a2ddc9e73b6127acefa47a3f65075c...

0000	00 00 0c 9f f3 3f a4 83 e7 05 d7 85 08 00 45 00?.....E
0010	00 e2 00 00 40 00 40 00 00 ff 08 78 90 aa 68 f4	...@...x-h...
0020	2a 01 c7 84 01 bb 78 7e 00 91 a7 97 e1 0e 80 18	*.....~.....
0030	00 00 2a 6f 00 00 01 01 00 30 e5 59 a9 3a 0f	:o.....0 Y :..
0040	30 d1 17 03 03 00 a9 2a 7e 06 bf 7d c8 6f c4 32	0.....* ...o-2
0050	a2 00 c7 e7 3b 61 27 ac e7 a4 7a 0d 62 07 5c 4ba'....z?e`V
0060	d5 f2 7c d9 2b f1 e7 84 0e a9 1d 0d 27 0d 27*....L.....
0070	ad a2 7f 2a 83 f3 1c a4 14 c5 ab 77 d3 8d 5	B-I-Hv-6-4...
0080	42 d8 49 05 48 76 ef db 36 da fd 34 02 00 e6	M-a533 xh-P...
0090	4d e4 bc a9 65 e9 33 ff 78 68 9b 0f c7 50 18 0bP...m-P...
00a0	05 ec a9 de 8a e9 96 ae 50 f5 c3 6d ee 93 29 0bP...m-P...
00b0	d0 ed 7a 44 b4 a0 35 fd 14 92 2f 09 eb 15 0d d5	..D@5.....
00c0	07 06 a6 06 a7 f5 14 11 98 22 1f 7a 7d 2e a6 40	..".z)...@
00d0	38 21 a0 e7 74 d3 e4 2e 5f 86 72 df 37 b4 29	8!..t...r-7-)
00e0	ac a9 0d 60 e2 de 8a 4a 55 25 50 2f 9e 2e c2 0a	U%P/...

Step 3. The SSL Handshake

Overall Handshake



Hello Messages

Answer the following questions:

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.

32 bytes.

No.	Time	Source	Destination	Protocol	Length	Info
10	2.112343	10.120.144.170	104.244.42.1	TLSv1.2	383	Client Hello
12	2.199777	104.244.42.1	10.120.144.170	TLSv1.2	1490	Server Hello
15	2.223353	104.244.42.1	10.120.144.170	TLSv1.2	507	Certificate, Server Key Exchange, Server Hello Done
17	2.228600	10.120.144.170	104.244.42.1	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message

▼ Transport Layer Security

▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello

- Content Type: Handshake (22)
- Version: TLS 1.0 (0x0301)
- Length: 312

▼ Handshake Protocol: Client Hello

- Handshake Type: Client Hello (1)
- Length: 308
- Version: TLS 1.2 (0x0303)

► Random: b83ae6745d8c79f85c0b7ab5109867aabbe8d3c9d7d5638f4...

Session ID Length: 32

Session ID: 334761ea3df2165670481946706bc6ef8c05856caa9a33e7...

Cipher Suites Length: 62

0000	00 00 0c 9f f3 3f a4 83	c7 05 d7 85 08 00 45 00?.....E
0010	01 71 00 00 40 00 06 0b	70 00 70 90 aa 68 f4	*q @: p x-h
0020	2a 01 c7 84 01 bb f8 7e	0b d6 a7 97 d3 43 80 18	*.....~.....C
0030	08 15 9e c2 00 00 01 01	08 0a 30 e5 59 01 3a 0f0 Y:..
0040	30 be 16 03 01 01 38 01	00 01 34 03 03 b8 3a e6	0.....8.....4.....
0050	74 5d 8c 79 f8 5c 0b 7a	b5 10 98 67 aa be 8d 3c	t]y-\z ..g...<
0060	9d 7d 56 38 f4 07 ac 04	95 2d 64 ed 5c 20 33 47	.jV8....-d\ 3G
0070	61 ea 3d f2 16 56 70 48	19 46 70 6b c6 ef 8c 05	a=...vpH -Fpk...
0080	85 6c aa 9a 33 e7 ed 92	8c b2 52 89 d7 e8 00 3e	.l-3...R...>
0090	13 02 13 03 13 01 ca 2c	c0 30 00 9f cc a0 cc a8@.....

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.

32 bytes.

No.	Time	Source	Destination	Protocol	Length	Info
10	2.112343	10.120.144.170	104.244.42.1	TLSv1.2	383	Client Hello
12	2.199777	104.244.42.1	10.120.144.170	TLSv1.2	1490	Server Hello
15	2.223353	104.244.42.1	10.120.144.170	TLSv1.2	507	Certificate, Server Key Exchange, Server Hello Done
17	2.228600	10.120.144.170	104.244.42.1	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message

▼ Transport Layer Security

▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello

- Content Type: Handshake (22)
- Version: TLS 1.0 (0x0301)
- Length: 312

▼ Handshake Protocol: Client Hello

- Handshake Type: Client Hello (1)
- Length: 308
- Version: TLS 1.2 (0x0303)

► Random: b83ae6745d8c79f85c0b7ab5109867aabbe8d3c9d7d5638f4...

Session ID Length: 32

Session ID: 334761ea3df2165670481946706bc6ef8c05856caa9a33e7...

Cipher Suites Length: 62

0000	00 00 0c 9f f3 3f a4 83	c7 05 d7 85 08 00 45 00?.....E
0010	01 71 00 00 40 00 06 0b	70 00 70 90 aa 68 f4	*q @: p x-h
0020	2a 01 c7 84 01 bb f8 7e	0b d6 a7 97 d3 43 80 18	*.....~.....C
0030	08 15 9e c2 00 00 01 01	08 0a 30 e5 59 01 3a 0f0 Y:..
0040	30 be 16 03 01 01 38 01	00 01 34 03 03 b8 3a e6	0.....8.....4.....
0050	74 5d 8c 79 f8 5c 0b 7a	b5 10 98 67 aa be 8d 3c	t]y-\z ..g...<
0060	9d 7d 56 38 f4 07 ac 04	95 2d 64 ed 5c 20 33 47	.jV8....-d\ 3G
0070	61 ea 3d f2 16 56 70 48	19 46 70 6b c6 ef 8c 05	a=...vpH -Fpk...
0080	85 6c aa 9a 33 e7 ed 92	8c b2 52 89 d7 e8 00 3e	.l-3...R...>
0090	13 02 13 03 13 01 ca 2c	c0 30 00 9f cc a0 cc a8@.....

3. What Cipher method 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.

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f).

No.	Time	Source	Destination	Protocol	Length	Info
10	2.112343	10.120.144.170	104.244.42.1	TLSv1.2	383	Client Hello
12	2.199777	104.244.42.1	10.120.144.170	TLSv1.2	1490	Server Hello
15	2.223353	104.244.42.1	10.120.144.170	TLSv1.2	507	Certificate, Server Key Exchange, Server Hello Done
17	2.228600	10.120.144.170	104.244.42.1	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message

▼ Transport Layer Security

▼ TLSv1.2 Record Layer: Handshake Protocol: Server Hello

- Content Type: Handshake (22)
- Version: TLS 1.2 (0x0303)
- Length: 61

▼ Handshake Protocol: Server Hello

- Handshake Type: Server Hello (2)
- Length: 57
- Version: TLS 1.2 (0x0303)

► Random: 39a7c47e70a23db411011011b20db023005d32bd9ea11f7...

Session ID Length: 0

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

Compression Method: null (0)

0060	2b d9 ea 11 f7 12 9f 60	47 84 08 a8 d6 00 c0 2f	+.....` G...../
------	-------------------------	-------------------------	-----------------

Certificate Messages

4. 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.

The server.

No.	Time	Source	Destination	Protocol	Length	Info
10	2.112343	10.120.144.170	104.244.42.1	TLSv1.2	383	Client Hello
12	2.199777	104.244.42.1	10.120.144.170	TLSv1.2	1490	Server Hello
15	2.223353	104.244.42.1	10.120.144.170	TLSv1.2	507	Certificate, Server Key Exchange, Server Hello Done
17	2.228600	10.120.144.170	104.244.42.1	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message

► [3 Reassembled TCP Segments (2876 bytes): #12(1358), #13(1424), #15(94)]

▼ Transport Layer Security

- ▼ TLSv1.2 Record Layer: Handshake Protocol: Certificate
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 2873
- ▼ Handshake Protocol: Certificate
 - Handshake Type: Certificate (11)
 - Length: 2867
 - Certificates Length: 2864

► Certificates (2864 bytes)

▼ Transport Layer Security

- ▼ TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange

No.	Time	Source	Destination	Protocol	Length	Info
0000	16.03.03.00.37.00.00.0b..	33.00.00.00.00.06.75.30	...-7... 3...0..u0			
0010	82.06.71.30.05.59.a0	03.02.01.02.02.10.07.a2	:q@-Y.....			
0020	71.40.cf.d9.fc.94.27	51.4f.85.55.42.6f.30.0d	@-0...Y 00-UB00-			
0030	06.09.2a.86.48.86.f7.0d	01.01.0b.05.00.30.70.31	*-H... 0p1			
0040	b6.39.09.06.03.55.04.06	13.02.55.53.31.15.30.13	.0...U...-US1-0.			

Client Key Exchange and Change Cipher Messages

5. At the Record Layer, what Content-Type values are used to indicate each of these messages? Say whether the values are the same or different than that used for the Hello and Certificate messages. Note that this question is asking you to look at the Record Layer and not an inner Handshake Protocol.

The values are represented as integers, and they are different.

Application data type has a value of 23, while hello message is of Handshake data type, its value is 22.

No.	Time	Source	Destination	Protocol	Length	Info
18	2.284460	104.244.42.1	10.120.144.170	TLSv1.2	308	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
20	2.284876	10.120.144.170	104.244.42.1	TLSv1.2	240	Application Data
21	2.341385	104.244.42.1	10.120.144.170	TLSv1.2	629	Application Data
26	2.366340	10.120.144.170	104.244.42.1	TLSv1.2	379	Client Hello

► Frame 20: 240 bytes on wire (1920 bits), 240 bytes captured (1920 bits) on interface 0

► Ethernet II, Src: Apple_05:d7:85 (a4:83:e7:05:d7:85), Dst: Cisco_9f:f3:3f (00:00:0c:9f:f3:3f)

► Internet Protocol Version 4, Src: 10.120.144.170, Dst: 104.244.42.1

► Transmission Control Protocol, Src Port: 51076, Dst Port: 443, Seq: 444, Ack: 3532, Len: 174

▼ Transport Layer Security

- ▼ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
 - Content Type: Application Data (23)
 - Version: TLS 1.2 (0x0303)
 - Length: 169
 - Encrypted Application Data: 2a7c06bf7dc86fc432a2ddc9e73b6127acefa47a3f65075...

No.	Time	Source	Destination	Protocol	Length	Info
0000	00.00.0c.9f.f3.3f.a4.83	e7.05.d7.85.08.00.45.00?.....E			
0010	00.e2.00.40.00.00.0b	ff.0a.78.90.aa.68.f4	:@-x-h:			
0020	2a.c1.7c.84.01.bb.18.7e	0d.91.a7.97.e1.0e.08.18	*-~...			
0030	08.2a.6t.00.00.01.01	08.0a.30.e5.59.a9.3a.0f	*o-0 Y:			
0040	30.d1.17.03.03.09.2a	7c.06.bf.7d.c8.6f.c4.32	0*-* -}-o-2			
0040	a9.44.r-q.a7.4h.k1.77.sr	af.7a.2f.45.a7.kr.4h	...-a-.-s--.k-			

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

Both the server and the client.

No.	Time	Source	Destination	Protocol	Length	Info
15	2.223353	104.244.42.1	10.120.144.170	TLSv1.2	507	Certificate, Server Key Exchange, Server Hello Done
17	2.228600	10.120.144.170	104.244.42.1	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
18	2.284460	104.244.42.1	10.120.144.170	TLSv1.2	308	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
20	2.284876	10.120.144.170	104.244.42.1	TLSv1.2	240	Application Data

► Frame 18: 308 bytes on wire (2464 bits), 308 bytes captured (2464 bits) on interface 0

► Ethernet II, Src: Cisco_05:22:c0 (40:55:39:05:22:c0), Dst: Apple_05:d7:85 (a4:83:e7:05:d7:85)

► Internet Protocol Version 4, Src: 104.244.42.1, Dst: 10.120.144.170

► Transmission Control Protocol, Src Port: 51076, Dst Port: 443, Seq: 3290, Ack: 444, Len: 242

▼ Transport Layer Security

- TLSv1.2 Record Layer: Handshake Protocol: New Session Ticket
- TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
- TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message

No.	Time	Source	Destination	Protocol	Length	Info
15	2.223353	104.244.42.1	10.120.144.170	TLSv1.2	507	Certificate, Server Key Exchange, Server Hello Done
17	2.228600	10.120.144.170	104.244.42.1	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
18	2.284460	104.244.42.1	10.120.144.170	TLSv1.2	308	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
20	2.284876	10.120.144.170	104.244.42.1	TLSv1.2	240	Application Data

► Frame 17: 192 bytes on wire (1536 bits), 192 bytes captured (1536 bits) on interface 0

► Ethernet II, Src: Apple_05:d7:85 (a4:83:e7:05:d7:85), Dst: Cisco_9f:f3:3f (00:00:0c:9f:f3:3f)

► Internet Protocol Version 4, Src: 10.120.144.170, Dst: 104.244.42.1

► Transmission Control Protocol, Src Port: 51076, Dst Port: 443, Seq: 318, Ack: 3290, Len: 126

▼ Transport Layer Security

- TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
- TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
- TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message

7. What are the contents carried inside the Change Cipher Spec message? Look past the ContentType and other headers to see the message itself.

Change Cipher Spec Message: 01

No.	Time	Source	Destination	Protocol	Length	Info
15	2.228603	104.244.42.1	10.120.144.170	TLSv1.2	50	Certificate, Server Key Exchange, Server Hello Done
17	2.228600	10.120.144.170	104.244.42.1	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
18	2.284460	104.244.42.1	10.120.144.170	TLSv1.2	308	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
20	2.284876	10.120.144.170	104.244.42.1	TLSv1.2	240	Application Data

► Frame 18: 308 bytes on wire (2464 bits), 308 bytes captured (2464 bits) on interface 0
 ► Ethernet II, Src: Cisco_05:22:c2 (40:55:39:05:22:c2), Dst: Apple_05:d7:85 (a4:83:e7:05:d7:85)
 ► Internet Protocol Version 4, Src: 104.244.42.1, Dst: 10.120.144.170
 ► Transmission Control Protocol, Src Port: 443, Dst Port: 51076, Seq: 3290, Ack: 444, Len: 242
 ▼ Transport Layer Security
 ▶ TLSv1.2 Record Layer: Handshake Protocol: New Session Ticket
 ▶ TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
 Content Type: Change Cipher Spec (20)
 Version: TLS 1.2 (0x0303)
 Length: 1
Change Cipher Spec Message
 ▶ TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message

0000	a4 83 e7 05 d7 85 40 55 39 05 22 c2 08 00 45 00@U 9 "- E-
0010	01 26 4d 46 40 00 3e 06 c2 e4 68 f4 2a 01 0a 78	.6J @> ~Fh *~ x
0020	90 aa 01 bb c7 84 97 e0 1c f8 7e 0d 91 80 18~
0030	08 2b cf ae 00 01 01 08 0a 3a 0f 3d 1c 30 e5	+.....: 0 0
0040	59 72 16 03 03 00 ba 00 0b 00 01 fa 40 00	Yr.....@~
0050	b6 61 92 60 0d 5d 3e 59 74 60 a7 07 67 70 07 9a	.a~]>Y t~gp..
0060	b6 b8 22 65 bd a3 28 a5 0b bf 07 02 86 0d	..e...-+.....=+
0070	8d 12 e0 3b 86 a8 1f 26 20 9f fc 8a ad 3d 2b 7c;...-+.....=+
0080	15 2a 7c 75 0b 40 66 bb 5d c5 37 42 1a cc 2d 4d	*[u:@f.]7B ..M
0090	e1 6c 45 a0 9a 31 a6 04 3f f6 89 9a 1a 45 ad f8	..E~1- 7- ..F
00a0	02 f8 80 80 49 50 2d a7 88 c6 14 80 52 44 68	..I P- .Rb
00b0	77 23 5c 29 fd 03 00 3c 73 88 c6 14 80 52 44 68	wZJM -s su!^5e-
00c0	72 ac 9e 0a 53 94 f0 82 b4 c9 16 cd 8f bc	r...S- ..
00d0	b5 b7 4d 8c 20 dc 52 0f fe 5b 41 3c 2b 96 4f 65R- [A~+0e
00e0	23 7e 96 69 dd c6 39 12 e4 fc 5b 2d f2 85 95 73	#~i-:9- ..[...s
00f0	c1 0a 8d b1 e9 4d 5d c4 89 d1 90 e4 68 9e 16 18MV- ..h...
0100	bf 14 03 03 00 01 01 16 03 03 00 28 9e a6 12 28(....(
0110	da 4f 07 3d 57 a9 67 f2 af af 05 3b ch ca 3a 0cW...-.

Alert Messages

8. At the Record Layer, what Content-Type value is used to signal an alert?

Alert (21)

No.	Time	Source	Destination	Protocol	Length	Info
58	2.636117	104.244.42.1	10.120.144.170	TLSv1.2	1490	Application Data [TCP segment of a reassembled PDU]
60	2.637206	104.244.42.1	10.120.144.170	TLSv1.2	1490	Application Data [TCP segment of a reassembled PDU]
68	2.650063	104.244.42.1	10.120.144.170	TLSv1.2	258	[TCP Previous segment not captured] , Ignored Unknown Record
72	2.656567	104.244.42.1	10.120.144.170	TLSv1.2	97	Encrypted Alert

► Frame 72: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface 0
 ► Ethernet II, Src: Cisco_05:22:c2 (40:55:39:05:22:c2), Dst: Apple_05:d7:85 (a4:83:e7:05:d7:85)
 ► Internet Protocol Version 4, Src: 104.244.42.1, Dst: 10.120.144.170
 ► Transmission Control Protocol, Src Port: 443, Dst Port: 51076, Seq: 4095, Ack: 650, Len: 31
 ▼ Transport Layer Security
 ▶ TLSv1.2 Record Layer: Encrypted Alert
 Content Type: Alert (21)
 Version: TLS 1.2 (0x0303)
 Length: 26
 Alert Message: Encrypted Alert

0000	a4 83 e7 05 d7 85 40 55 39 05 22 c2 08 00 45 00@U 9 "- E-
0010	00 53 90 47 40 00 3e 06 7e 46 68 f4 2a 01 0a 78	.5 G@ > ~Fh *~ x
0020	90 aa 01 bb c7 84 a7 97 e3 41 f8 7e 0e 5f 80 18~
0030	08 2b d9 23 00 00 01 01 08 0a 3a 0f 30 fc 30 e5	+#...: 0 0
0040	5a e8 15 03 03 00 1a 9e a6 12 28 de 4f 97 3f 1d	Z.....(.-0-?
0050	46 2b df 43 67 76 fb 9e bc a0 e2 34 fd e2 84 db	F+Cgv...-4-?
0060	db	.

9. Tell us whether the contents of the alert are encrypted or sent in the clear? To check this, see whether you can read the contents of the alert to see what kind of alert has been sent.

Encrypted.

No.	Time	Source	Destination	Protocol	Length	Info
58	2.636117	104.244.42.1	10.120.144.170	TLSv1.2	1490	Application Data [TCP segment of a reassembled PDU]
60	2.637206	104.244.42.1	10.120.144.170	TLSv1.2	1490	Application Data [TCP segment of a reassembled PDU]
68	2.650063	104.244.42.1	10.120.144.170	TLSv1.2	258	[TCP Previous segment not captured] , Ignored Unknown Record
72	2.656567	104.244.42.1	10.120.144.170	TLSv1.2	97	Encrypted Alert

► Frame 72: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface 0
 ► Ethernet II, Src: Cisco_05:22:c2 (40:55:39:05:22:c2), Dst: Apple_05:d7:85 (a4:83:e7:05:d7:85)
 ► Internet Protocol Version 4, Src: 104.244.42.1, Dst: 10.120.144.170
 ► Transmission Control Protocol, Src Port: 443, Dst Port: 51076, Seq: 4095, Ack: 650, Len: 31
 ▼ Transport Layer Security
 ▶ TLSv1.2 Record Layer: Encrypted Alert
 Content Type: Alert (21)
 Version: TLS 1.2 (0x0303)
 Length: 26
 Alert Message: Encrypted Alert

0000	a4 83 e7 05 d7 85 40 55 39 05 22 c2 08 00 45 00@U 9 "- E-
0010	00 53 90 47 40 00 3e 06 7e 46 68 f4 2a 01 0a 78	.5 G@ > ~Fh *~ x
0020	90 aa 01 bb c7 84 a7 97 e3 41 f8 7e 0e 5f 80 18~
0030	08 2b d9 23 00 00 01 01 08 0a 3a 0f 30 fc 30 e5	+#...: 0 0
0040	5a e8 15 03 03 00 1a 9e a6 12 28 de 4f 97 3f 1d	Z.....(.-0-?
0050	46 2b df 43 67 76 fb 9e bc a0 e2 34 fd e2 84 db	F+Cgv...-4-?
0060	db	.