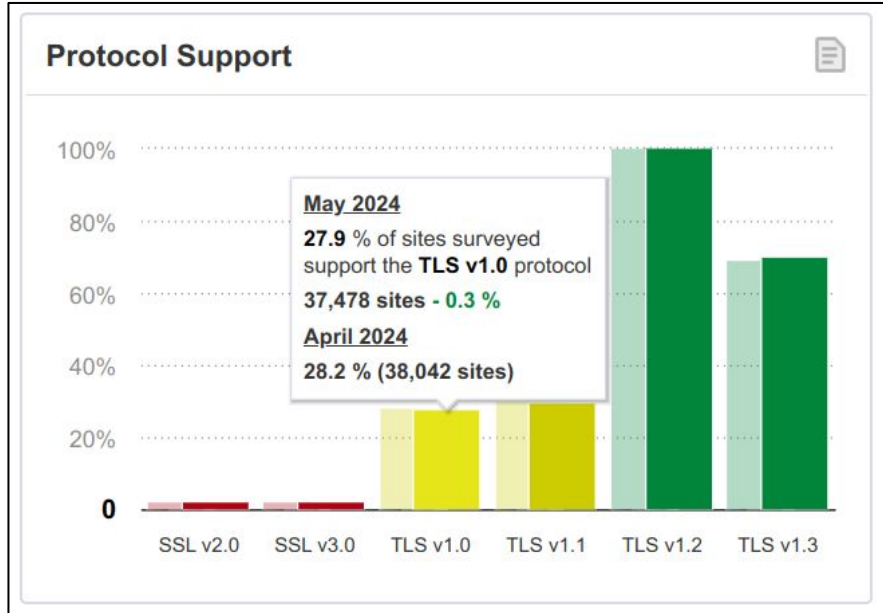


LAB 06 Presentation Layer

Jennessa Sierra & Andres Hung
CMPS1192 Networking Fundamentals
November 7, 2024

Lab Adjustments



Most websites using TLS 1.2 or 1.3

Category: Best Current Practice
Published: March 2021
ISSN: 2070-1721
Authors: K. Moriarty S. Farrell
CIS Trinity College Dublin

RFC 8996 Deprecating TLS 1.0 and TLS 1.1

TLS 1.0 and TLS 1.1 not recommended since 2021

We use TLS 1.2 as it is the most similar to previous versions.

Step 1: Capture Trace

```
^ andreshung ~ curl --tlsv1 --insecure https://news.ycombinator.com > out
```

% Total	% Received	% Xferd	Average Speed	Time	Time	Time	Current
			Dload	Upload	Total	Spent	Speed
100	36505	0	36505	0	0	75613	0
						--:--:--	--:--:--
						--:--:--	--:--:--
						--:--:--	75736



Connection - secure connection settings

The connection to this site is encrypted and authenticated using TLS

1.2, ECDHE_ECDSA with X25519, and AES_256_GCM.

Step 2: Trace Inspection

Wireshark Inspection

tls && ((dns.qry.name contains "api.waketime.com" ip.host contains "api.waketime.com"))					
No.	Source	Destination	Protocol	Length	Info
14	85.41.117.34.bc.googl...	192.168.18.35	TLSv1.2	106	Application Data
15	192.168.18.35	85.41.117.34.bc.google	TLSv1.2	109	Application Data
36	192.168.18.35	news.ycombinator.com	TLSv1.2	583	Client Hello (SNI=news.ycombinator.com)
42	news.ycombinator.com	192.168.18.35	TLSv1.2	1466	Server Hello
44	news.ycombinator.com	192.168.18.35	TLSv1.2	947	Certificate, Server Key Exchange, Server Hello Done
46	192.168.18.35	news.ycombinator.com	TLSv1.2	159	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
48	news.ycombinator.com	192.168.18.35	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
49	192.168.18.35	news.ycombinator.com	TLSv1.2	159	Application Data
50	news.ycombinator.com	192.168.18.35	TLSv1.2	135	Application Data
51	192.168.18.35	news.ycombinator.com	TLSv1.2	138	Application Data
53	192.168.18.35	news.ycombinator.com	TLSv1.2	104	Application Data
62	news.ycombinator.com	192.168.18.35	TLSv1.2	570	Application Data
63	192.168.18.35	news.ycombinator.com	TLSv1.2	108	Application Data
101	news.ycombinator.com	192.168.18.35	TLSv1.2	1466	Application Data
124	news.ycombinator.com	192.168.18.35	TLSv1.2	1466	Application Data, Application Data
126	news.ycombinator.com	192.168.18.35	TLSv1.2	1235	Application Data
129	192.168.18.35	news.ycombinator.com	TLSv1.2	121	Application Data
130	192.168.18.35	news.ycombinator.com	TLSv1.2	97	Encrypted Alert
174	85.41.117.34.bc.googl...	192.168.18.35	TLSv1.2	100	Application Data

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

> Frame 49: 159 bytes on wire (1272 bits), 159 bytes captured (1272 bits) on interface	0000	94 b2 71 b2
> Ethernet II, Src: CloudNetwork_4e:98:15 (4c:82:a9:4e:98:15), Dst: HuaweiTechno_b2:b	0010	00 91 af d8
> Internet Protocol Version 4, Src: 192.168.18.35 (192.168.18.35), Dst: news.ycombina	0020	e6 cf 82 ae
> Transmission Control Protocol, Src Port: 33454 (33454), Dst Port: https (443), Seq:	0030	02 22 5c cc
> Transport Layer Security	0040	d9 84 17 03
> TLSv1.2 Record Layer: Application Data Protocol: HyperText Transfer Protocol 2	0050	18 97 47 33
Content Type: Application Data (23)	0060	dc 2e 3b 34
Version: TLS 1.2 (0x0303)	0070	d3 e1 a6 67
Length: 88	0080	34 e6 a4 bc
Encrypted Application Data: 4468e82a6456d04e7b18974733d52fd046a5e5bc8d18a9d00c	0090	a3 c4 2c 83
[Application Data Protocol: HyperText Transfer Protocol 2]		

23 or 0x17

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

> Frame 49: 159 bytes on wire (1272 bits), 159 bytes captured (1272 bits) on interface	0000	94 b2 71 b2 bc
> Ethernet II, Src: CloudNetwork_4e:98:15 (4c:82:a9:4e:98:15), Dst: HuaweiTechno_b2:b	0010	00 91 af d8 40
> Internet Protocol Version 4, Src: 192.168.18.35 (192.168.18.35), Dst: news.ycombina	0020	e6 cf 82 ae 01
> Transmission Control Protocol, Src Port: 33454 (33454), Dst Port: https (443), Seq:	0030	02 22 5c cc 00
> Transport Layer Security	0040	d9 84 17 03 03
✓ TLSv1.2 Record Layer: Application Data Protocol: HyperText Transfer Protocol 2	0050	18 97 47 33 d5
Content Type: Application Data (23)	0060	dc 2e 3b 34 bd
Version: TLS 1.2 (0x0303)	0070	d3 e1 a6 67 22
Length: 88	0080	34 e6 a4 bc 43
Encrypted Application Data: 4468e82a6456d04e7b18974733d52fd046a5e5bc8d18a9d00c	0090	a3 c4 2c 83 1b
[Application Data Protocol: HyperText Transfer Protocol 2]		

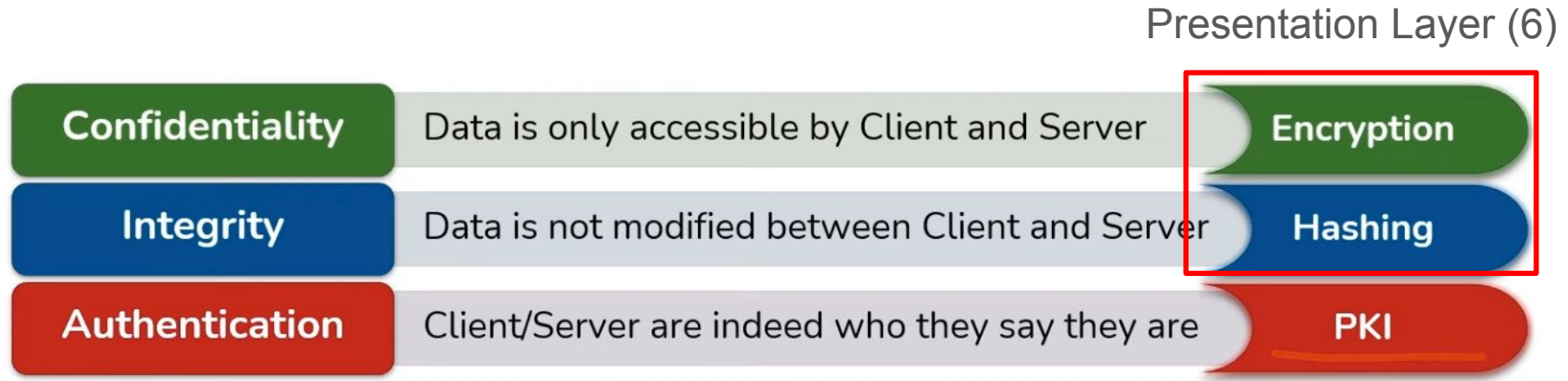
Version constant 0x0303, which represents TLS v1.2

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

> Frame 49: 159 bytes on wire (1272 bits), 159 bytes captured (1272 bits) on interface	0000	94 b2 71 b2 bc d1 4c 82 a9 4e 98 15 08 00 45 00
> Ethernet II, Src: CloudNetwork_4e:98:15 (4c:82:a9:4e:98:15), Dst: HuaweiTechno_b2:b	0010	00 91 af d8 40 00 40 06 ff 1a c0 a8 12 23 d1 d8
> Internet Protocol Version 4, Src: 192.168.18.35 (192.168.18.35), Dst: news.ycombina	0020	e6 cf 82 ae 01 bb 2c d1 12 82 50 3c eb e8 80 18
> Transmission Control Protocol, Src Port: 33454 (33454), Dst Port: https (443), Seq:	0030	02 22 5c cc 00 00 01 01 08 0a 2a 54 e3 d3 79 28
> Transport Layer Security	0040	d9 84 17 03 03 00 58 14 68 e8 2a 64 56 d0 4e 7b
✓ TLSv1.2 Record Layer: Application Data Protocol: HyperText Transfer Protocol 2	0050	18 97 47 33 35 2f 30 16 a5 e5 bc 8d 18 a9 d0 0d
Content Type: Application Data (23)	0060	dc 2e 3b 34 bd 71 ca 1f 77 ba 59 86 da f6 6e 99
Version: TLS 1.2 (0x0303)	0070	d3 e1 a6 67 22 4a b8 5e 5b 71 2d b4 76 f5 b7 ca
Length: 88	0080	34 e6 a4 bc 43 a1 9c 9a e5 c2 32 6d bb f6 f5 fc
Encrypted Application Data: 4468e82a6456d04e7b18974733d52fd046a5e5bc8d18a9d00c	0090	a3 c4 2c 83 1b d5 ec 99 c3 a8 ee 43 98 af c2
[Application Data Protocol: HyperText Transfer Protocol 2]		

Length only covers the payload (highlighted in blue)

Purpose of SSL/TLS



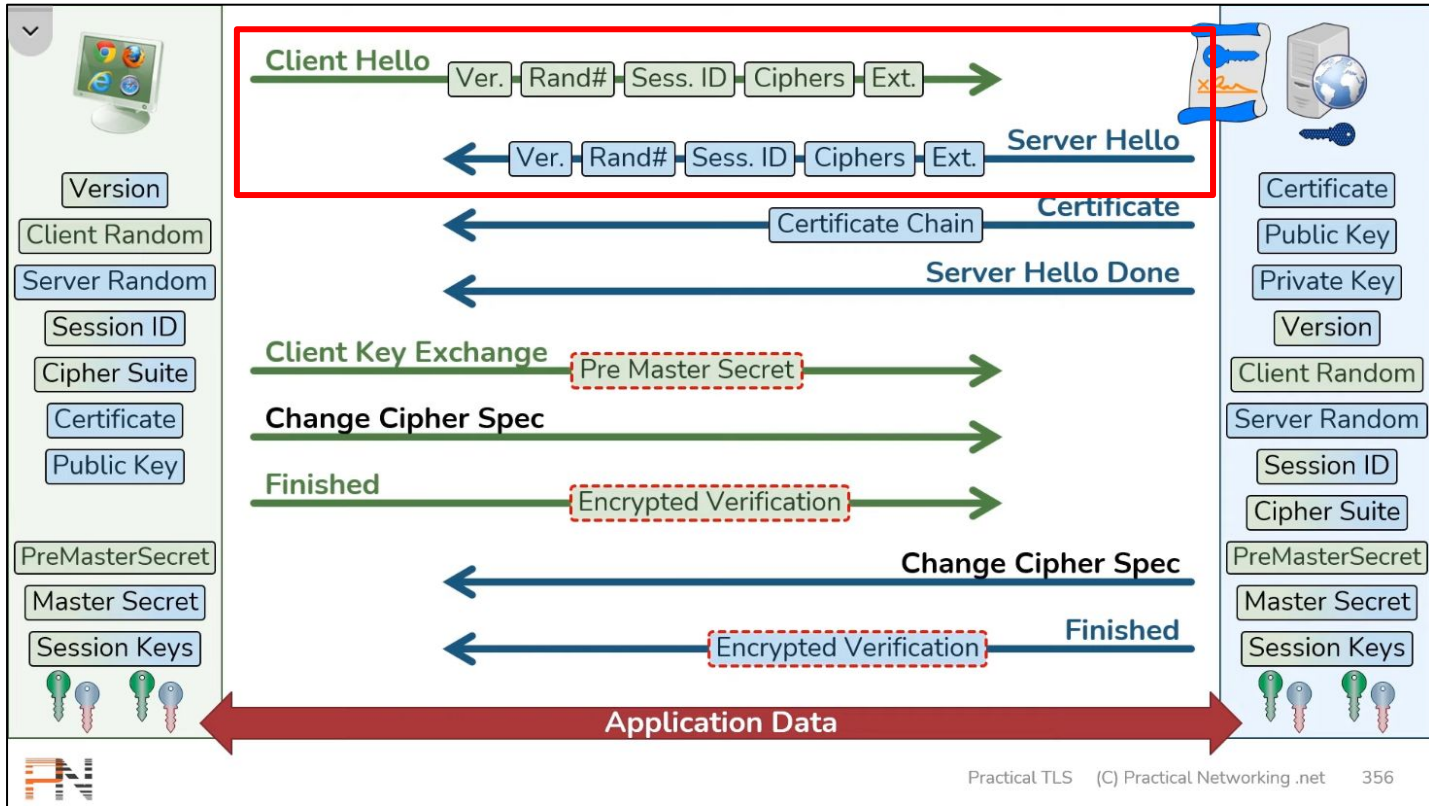
Secure Sockets Layer/ Transport Layer Security

Used in HTTPS, prevent man-in-the-middle attacks.

SSL/TLS exists above Transport Layer (4) but below Application Layer (7)

Step 3: The SSL Handshake

TLS Handshake Overview



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.

The image shows a Wireshark packet capture of a TLSv1.2 Client Hello. The packet structure is as follows:

- Frame 36: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface
- Ethernet II, Src: CloudNetwork_4e:98:15 (4c:82:a9:4e:98:15), Dst: HuaweiTechno_b
- Internet Protocol Version 4, Src: 192.168.18.35 (192.168.18.35), Dst: news.ycomb
- Transmission Control Protocol, Src Port: 33454 (33454), Dst Port: https (443), S
- 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
 - Handshake Type: Client Hello (1)
 - Length: 508
 - Version: TLS 1.2 (0x0303)
 - Random: b9f184dd69e4cc12bc172646581f31d926f372dc176b1193dd9d378437728464
 - GMT Unix Time: Nov 8, 2068 09:12:29.000000000 CST
 - Random Bytes: 69e4cc12bc172646581f31d926f372dc176b1193dd9d378437728464
 - Session ID Length: 32

The random data is 28 bytes long, as indicated by the 'Random Bytes' field in the Client Hello message.

The random data is 28 bytes long for Hellos

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.

The image shows a Wireshark packet capture of a TLSv1.2 Server Hello message. The packet is Frame 42, 1466 bytes on wire. The protocol stack is Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Transport Layer Security. The TLSv1.2 Record Layer is expanded to show the Handshake Protocol: Server Hello. The Handshake Protocol: Server Hello is further expanded to show the following fields:

- Content Type: Handshake (22)
- Version: TLS 1.2 (0x0303)
- Length: 106
- Handshake Protocol: Server Hello
 - Handshake Type: Server Hello (2)
 - Length: 102
 - Version: TLS 1.2 (0x0303)
 - Random: 8b75b7fd2c7896f111d77d5bfbac220f700dba5f52166cddda8db10a361a23a
 - Session ID Length: 32**
 - Session ID: 9743124111ae629f108e20e6e37874af904e36a4348d697d1c75f1024147
 - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)

The Session ID Length field is highlighted in blue and has a red box around it. The Session ID field is also highlighted in blue. The packet bytes are displayed in hexadecimal and ASCII on the right side of the packet list.

The session identifier sent by the server is 32 bytes long

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.

Frame 42: 1466 bytes on wire (11728 bits), 1466 bytes captured (11728 bits) on interface
> Ethernet II, Src: HuaweiTechno_b2:bc:d1 (94:b2:71:b2:bc:d1), Dst: CloudNetwork_4
> Internet Protocol Version 4, Src: news.ycombinator.com (209.216.230.207), Dst: 1
> Transmission Control Protocol, Src Port: https (443), Dst Port: 33454 (33454), S
✓ Transport Layer Security
 ✓ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
 Content Type: Handshake (22)
 Version: TLS 1.2 (0x0303)
 Length: 106
 ✓ Handshake Protocol: Server Hello
 Handshake Type: Server Hello (2)
 Length: 102
 Version: TLS 1.2 (0x0303)
 Random: 8b75b7fd3cc7896f111d77d5bfbae220f700dba5f52166cddda8db10a361a23a
 Session ID Length: 32
 Session ID: 9743124111ae629f108e20e6e37874af904e36a4348d697d1c75f1024147;
 Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
 Compression Method: null (0)

0080 36 a4 34 8d 69 7d 1c 75 f1 02 41 47 27 e8 c0 2c
0090 00 00 1e ff 01 00 01 00 00 00 00 00 0b 00 04
00a0 03 00 01 02 00 10 00 05 00 03 02 68 32 00 17 00
00b0 00 16 03 03 07 f3 0b 00 07 ef 00 07 ec 00 03 8b
00c0 30 82 03 87 30 82 03 0e a0 03 02 01 02 02 12 04
00d0 95 ff 10 bf 5d 1d 52 42 5c 95 5b 4b 85 bc e7 4a
00e0 a4 30 0a 06 08 2a 86 48 ce 3d 04 03 03 30 32 31
00f0 0b 30 09 06 03 55 04 06 13 02 55 53 31 16 30 14
0100 06 03 55 04 0a 13 0d 4c 65 74 27 73 20 45 6e 63
0110 72 79 70 74 31 0b 30 09 06 03 55 04 03 13 02 45
0120 35 30 1e 17 0d 32 34 31 30 32 37 30 38 30 32 31
0130 34 5a 17 0d 32 35 30 31 32 35 30 38 30 32 31 33
0140 5a 30 1f 31 1d 30 1b 06 03 55 04 03 13 14 6e 65
0150 77 73 2e 79 63 6f 6d 62 69 6e 61 74 6f 72 2e 63
0160 6f 6d 30 59 30 13 06 07 2a 86 48 ce 3d 02 01 06
0170 08 2a 86 48 ce 3d 03 01 07 03 42 00 04 cf 81 73
0180 cf a7 6d ad d7 d4 42 b3 39 4b 88 50 f0 30 b2 b2
0190 08 73 0e a6 ab 90 13 dd df f2 bf ff 15 e6 cb 45
01a0 6a 52 83 e2 c5 c0 bb ad 35 a0 0b b7 e5 6f 19 ac
01b0 4f 38 4d f4 4a 73 e9 33 54 69 25 0e f0 a3 82 02
01c0 15 30 82 02 11 30 0e 06 03 55 1d 0f 01 01 ff 04
01d0 04 03 02 07 80 30 1d 06 03 55 1d 25 04 16 30 14
01e0 06 08 2b 06 01 05 05 07 03 01 06 08 2b 06 01 05
01f0 05 07 03 02 30 0c 06 03 55 1d 13 01 01 ff 04 02

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)

Presentation Layer (Layer 6) in Action

Cipher Suites

Key Exchange

ECDHE
DHE
ECDH
DH
RSA
PSK

Authentication

ECDSA
RSA
DSS
PSK

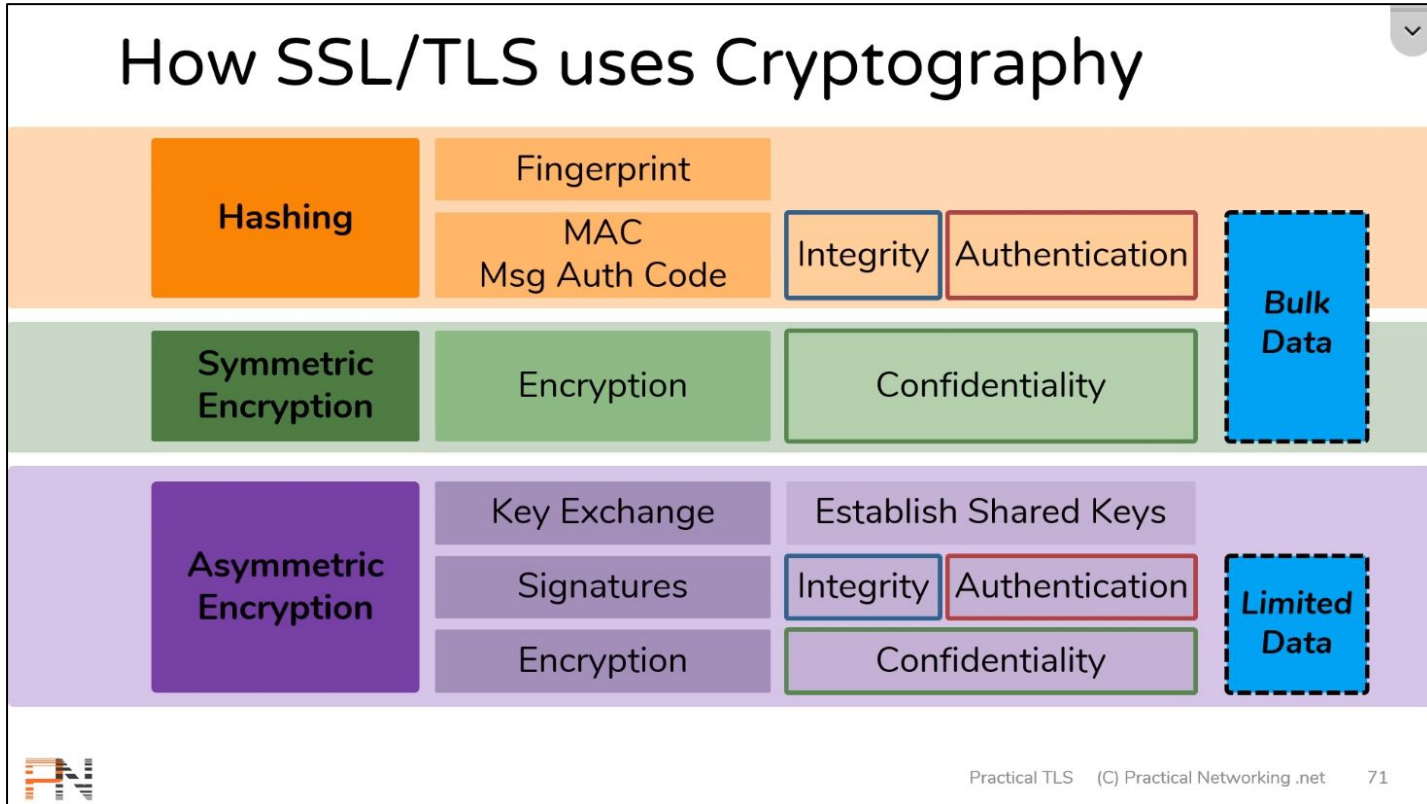
Encryption

CHACHA20
AES-256-GCM
AES-128-GCM
AES-256-CBC
AES-128-CBC
3DES-CBC
RC4-128
DES-CBC

Hashing

Poly1305
SHA384
SHA256
SHA
MD5

Presentation Layer (Layer 6) in Action



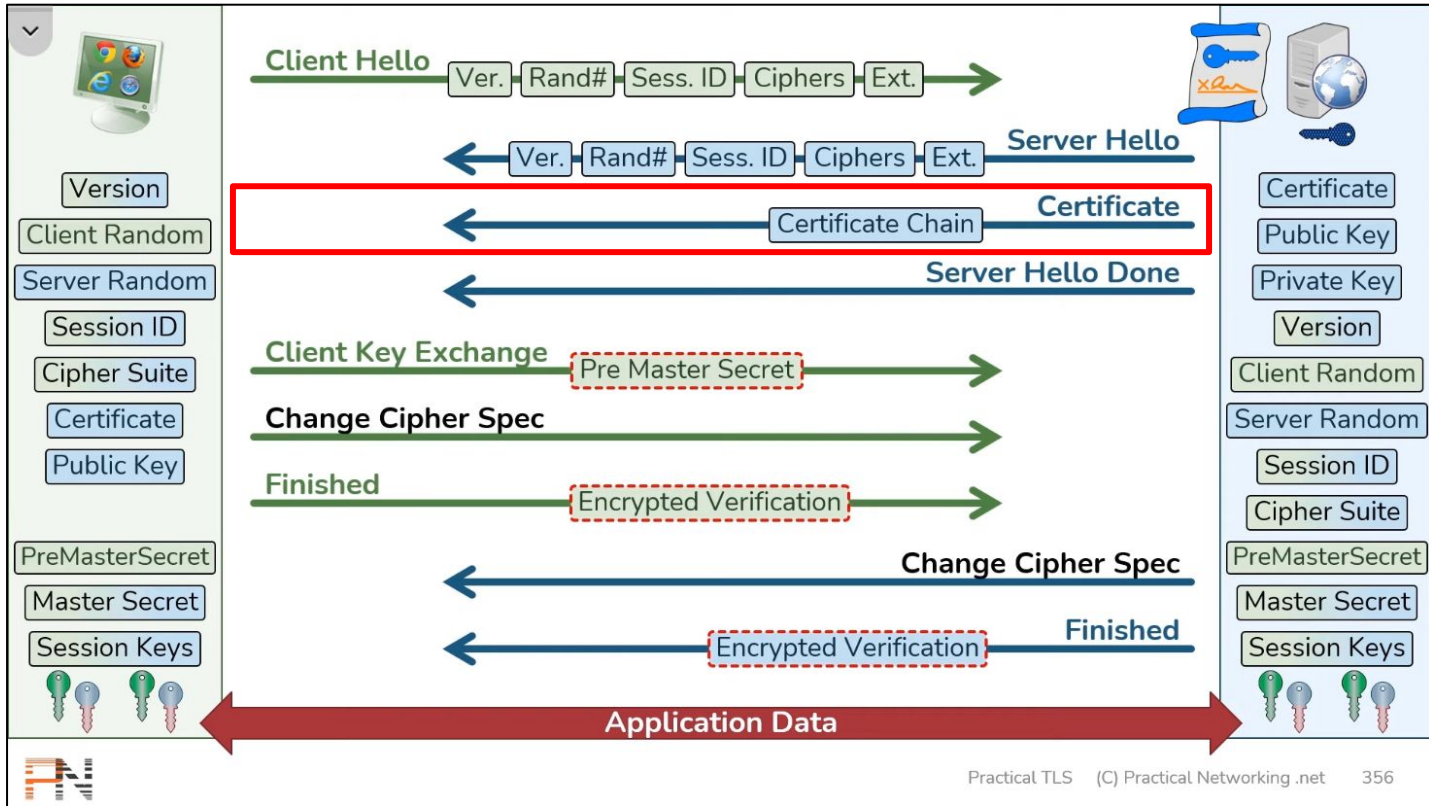
Certificate Messages

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.

tls && !(dns.qry.name contains "api.wakatime.com" ip.host contains "api.wakatime.com")					
No.	Source	Destination	Protocol	Length	Info
14	85.41.117.34.bc.googl...	192.168.18.35	TLSv1.2	106	Application Data
15	192.168.18.35	85.41.117.34.bc.google...	TLSv1.2	109	Application Data
36	192.168.18.35	news.ycombinator.com	TLSv1.2	583	Client Hello (SNI=news.ycombinator.com)
42	news.ycombinator.com	192.168.18.35	TLSv1.2	1466	Server Hello
44	news.ycombinator.com	192.168.18.35	TLSv1.2	947	Certificate, Server Key Exchange, Server Hello Done
46	192.168.18.35	news.ycombinator.com	TLSv1.2	159	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
48	news.ycombinator.com	192.168.18.35	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
49	192.168.18.35	news.ycombinator.com	TLSv1.2	159	Application Data
50	news.ycombinator.com	192.168.18.35	TLSv1.2	135	Application Data
51	192.168.18.35	news.ycombinator.com	TLSv1.2	138	Application Data

Only the server (client optional)

TLS Handshake Overview



How Certificates are Used

How SSL/TLS uses Cryptography



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.

✓ TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
Content Type: Handshake (22)

✓ TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
Content Type: Change Cipher Spec (20)

✓ TLSv1.2 Record Layer: Handshake Protocol: Certificate
Content Type: Handshake (22)

✓ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22)

The only different one is Change Cipher Spec. The rest are the same.

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

tls && !(dns.qry.name contains "api.wakatime.com" ip.host contains "api.wakatime.com")					
No.	Source	Destination	Protocol	Length	Info
14	85.41.117.34.bc.googl...	192.168.18.35	TLSv1.2	106	Application Data
15	192.168.18.35	85.41.117.34.bc.google...	TLSv1.2	109	Application Data
36	192.168.18.35	news.ycombinator.com	TLSv1.2	583	Client Hello (SNI=news.ycombinator.com)
42	news.ycombinator.com	192.168.18.35	TLSv1.2	1466	Server Hello
44	news.ycombinator.com	192.168.18.35	TLSv1.2	947	Certificate, Server Key Exchange, Server Hello Done
46	192.168.18.35	news.ycombinator.com	TLSv1.2	159	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
48	news.ycombinator.com	192.168.18.35	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
49	192.168.18.35	news.ycombinator.com	TLSv1.2	159	Application Data
50	news.ycombinator.com	192.168.18.35	TLSv1.2	135	Application Data
51	192.168.18.35	news.ycombinator.com	TLSv1.2	138	Application Data
53	192.168.18.35	news.ycombinator.com	TLSv1.2	104	Application Data

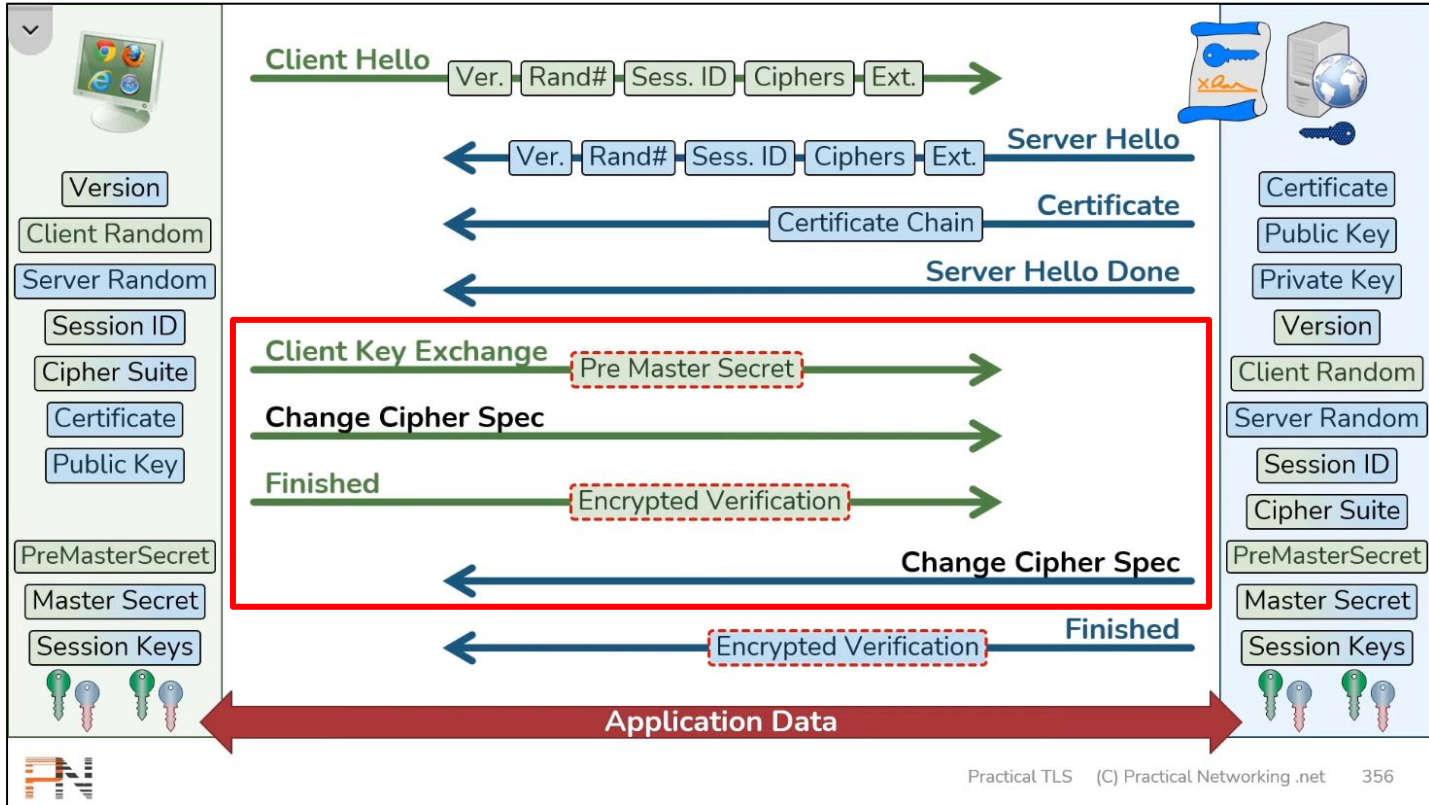
Both client and server

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

> Frame 46: 159 bytes on wire (1272 bits), 159 bytes captured (1272 bits) on interface	0000	94 b2 71
> Ethernet II, Src: CloudNetwork_4e:98:15 (4c:82:a9:4e:98:15), Dst: HuaweiTechno_b2:b	0010	00 91 af
> Internet Protocol Version 4, Src: 192.168.18.35 (192.168.18.35), Dst: news.ycombina	0020	e6 cf 82
> Transmission Control Protocol, Src Port: 33454 (33454), Dst Port: https (443), Seq:	0030	02 22 0a
> Transport Layer Security	0040	d9 2c 16
> TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange	0050	2a 8e d8
> TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec	0060	b5 5d e9
Content Type: Change Cipher Spec (20)	0070	01 01 16
Version: TLS 1.2 (0x0303)	0080	3a fa e3
Length: 1	0090	4c b5 05
Change Cipher Spec Message		
> TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message		

The content is just a single byte that contains the value 1

TLS Handshake Overview



Alert Message

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

The image shows a Wireshark packet capture of a TLSv1.2 Encrypted Alert. The packet list on the left shows the following layers:

- Frame 130: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface w
- Ethernet II, Src: CloudNetwork_4e:98:15 (4c:82:a9:4e:98:15), Dst: HuaweiTechno_b2:b
- Internet Protocol Version 4, Src: 192.168.18.35 (192.168.18.35), Dst: news.ycombina
- Transmission Control Protocol, Src Port: 33454 (33454), Dst Port: https (443), Seq:
- Transport Layer Security
 - TLSv1.2 Record Layer: Encrypted Alert
 - Content Type: Alert (21)**
 - Version: TLS 1.2 (0x0303)
 - Length: 26
 - Alert Message: Encrypted Alert

The packet details on the right show the raw data in hexadecimal and ASCII:

Offset	Hex	ASCII
0000	94 b2 71 b2 bc d1 4c 82	a9 4e 98 15 08 00 45 00
0010	00 53 af f0 40 00 40 06	ff 40 c0 a8 12 23 d1 d8
0020	e6 cf 82 ae 01 bb 2c d1	13 ae 50 3d 7d 5f 80 19
0030	02 62 ff 89 00 00 01 01	08 0a 2a 54 e4 82 79 28
0040	da 31 15 03 03 00 1a 44	68 e8 2a 64 56 d0 53 12
0050	4e 72 d3 f5 54 10 fe fd	92 93 00 07 3f 4c 33 ab
0060	0a	

Content-Type 21 is used

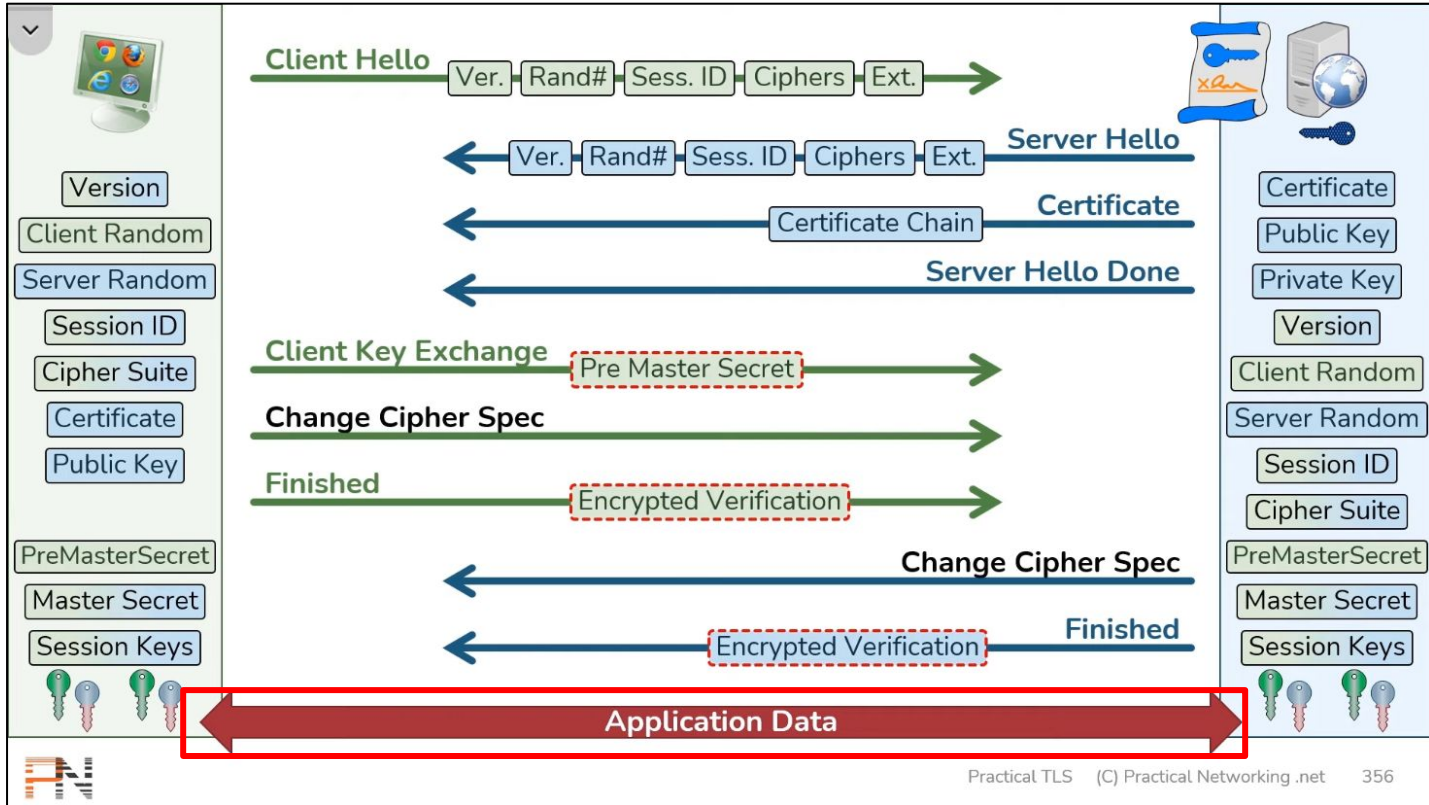
9. Tell us whether the contents of the alert are encrypted or sent in the clear? To check this, see whether you can read the contents of the alert to see what kind of alert has been sent.

Frame 130: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface w
> Ethernet II, Src: CloudNetwork_4e:98:15 (4c:82:a9:4e:98:15), Dst: HuaweiTechno_b2:b
> Internet Protocol Version 4, Src: 192.168.18.35 (192.168.18.35), Dst: news.ycombina
> Transmission Control Protocol, Src Port: 33454 (33454), Dst Port: https (443), Seq:
✓ 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 94 b2 71 b2 bc d1 4c 82 a9 4e 98 15 08 00 45 00 ..q...L..N...E
0010 00 53 af f0 40 00 40 06 ff 40 c0 a8 12 23 d1 d8 .S..@..@...#..
0020 e6 cf 82 ae 01 bb 2c d1 13 ae 50 3d 7d 5f 80 19P=}..
0030 02 62 ff 89 00 00 01 01 08 0a 2a 54 e4 82 79 28 ..b.....*T..y(
0040 da 31 15 03 03 00 1a 44 68 e8 2a 64 56 d0 53 12 ..1.....D h..*dV.S..
0050 4e 72 d3 f5 54 10 fe fd 92 93 00 07 3f 4c 33 ab Nr..T....?L3..
0060 0a

The contents are encrypted

TLS Handshake Overview



Alert

tls && !(dns.qry.name contains "api.wakatime.com" ip.host contains "api.wakatime.com")					
No.	Source	Destination	Protocol	Length	Info
14	85.41.117.34.bc.googl...	192.168.18.35	TLSv1.2	106	Application Data
15	192.168.18.35	85.41.117.34.bc.google...	TLSv1.2	109	Application Data
36	192.168.18.35	news.ycombinator.com	TLSv1.2	583	Client Hello (SNI=news.ycombinator.com)
42	news.ycombinator.com	192.168.18.35	TLSv1.2	1466	Server Hello
44	news.ycombinator.com	192.168.18.35	TLSv1.2	947	Certificate, Server Key Exchange, Server Hello Done
46	192.168.18.35	news.ycombinator.com	TLSv1.2	159	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
48	news.ycombinator.com	192.168.18.35	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
49	192.168.18.35	news.ycombinator.com	TLSv1.2	159	Application Data
50	news.ycombinator.com	192.168.18.35	TLSv1.2	135	Application Data
51	192.168.18.35	news.ycombinator.com	TLSv1.2	138	Application Data
53	192.168.18.35	news.ycombinator.com	TLSv1.2	104	Application Data
62	news.ycombinator.com	192.168.18.35	TLSv1.2	570	Application Data
63	192.168.18.35	news.ycombinator.com	TLSv1.2	108	Application Data
101	news.ycombinator.com	192.168.18.35	TLSv1.2	1466	Application Data
124	news.ycombinator.com	192.168.18.35	TLSv1.2	1466	Application Data, Application Data
126	news.ycombinator.com	192.168.18.35	TLSv1.2	1235	Application Data
129	192.168.18.35	news.ycombinator.com	TLSv1.2	121	Application Data
130	192.168.18.35	news.ycombinator.com	TLSv1.2	97	Encrypted Alert
174	85.41.117.34.bc.googl...	192.168.18.35	TLSv1.2	100	Application Data