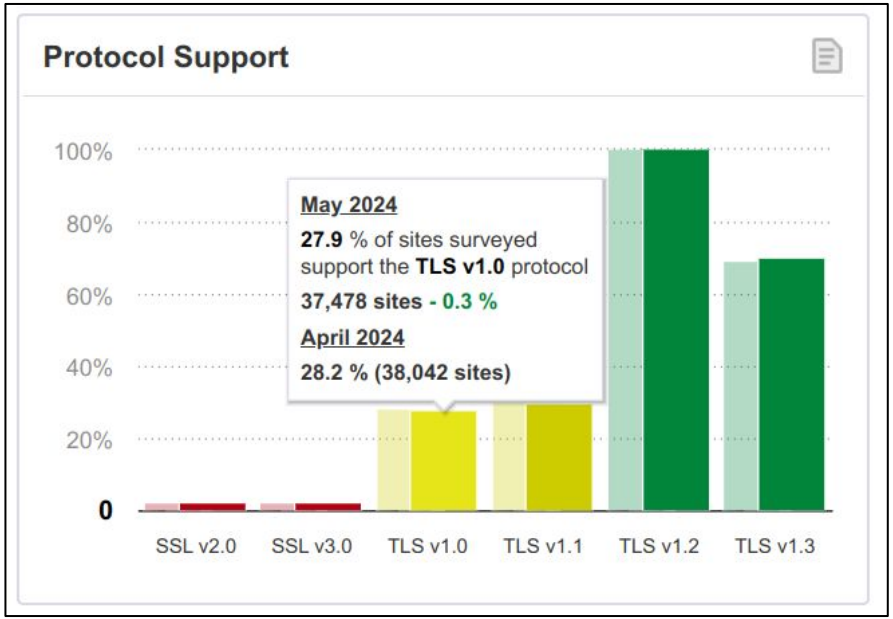
LAB 06 Presentation Layer

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

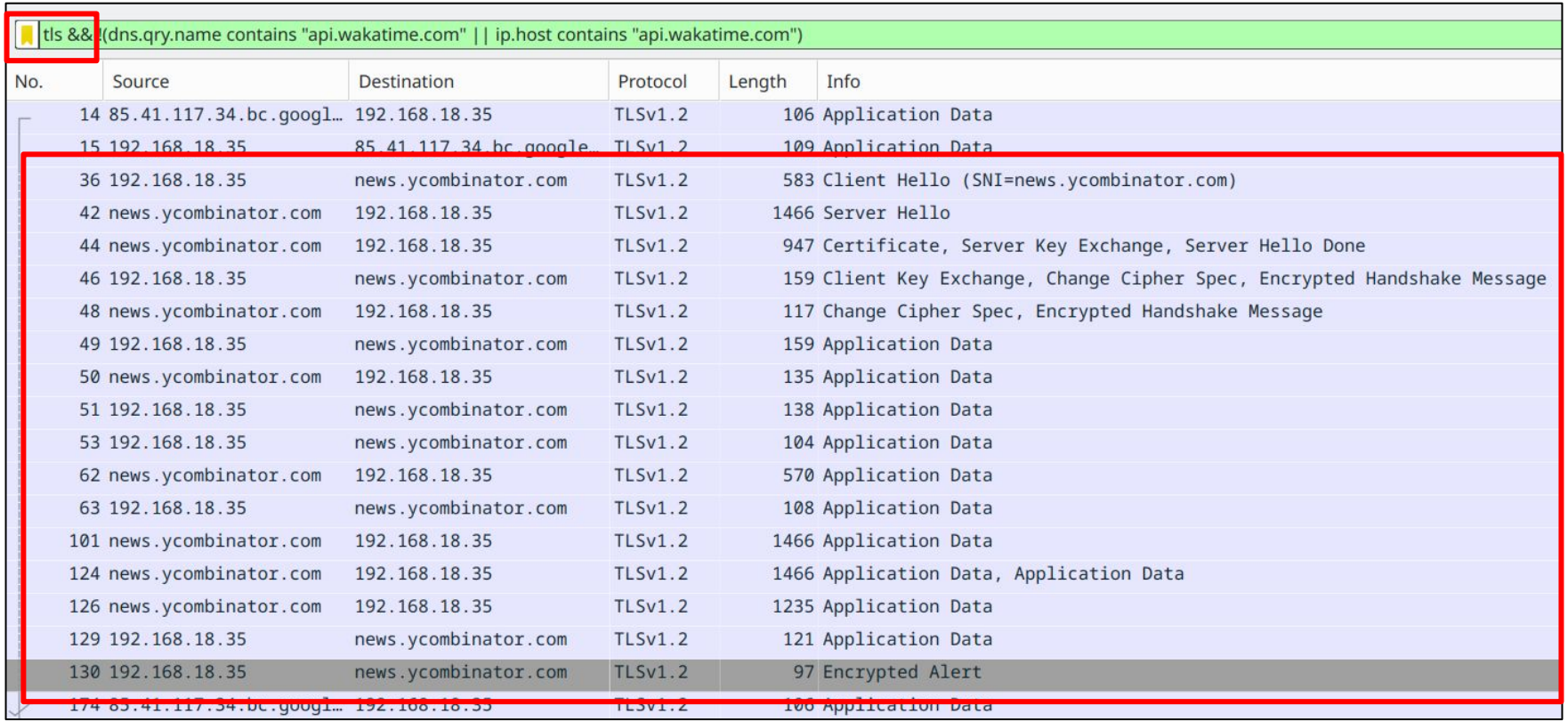
We use TLS 1.2 as it is the most similar to previous versions.

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    Left  Speed
100 36505    0 36505    0     0  75613      0 --:--:-- --:--:-- --:--:-- 75736
```

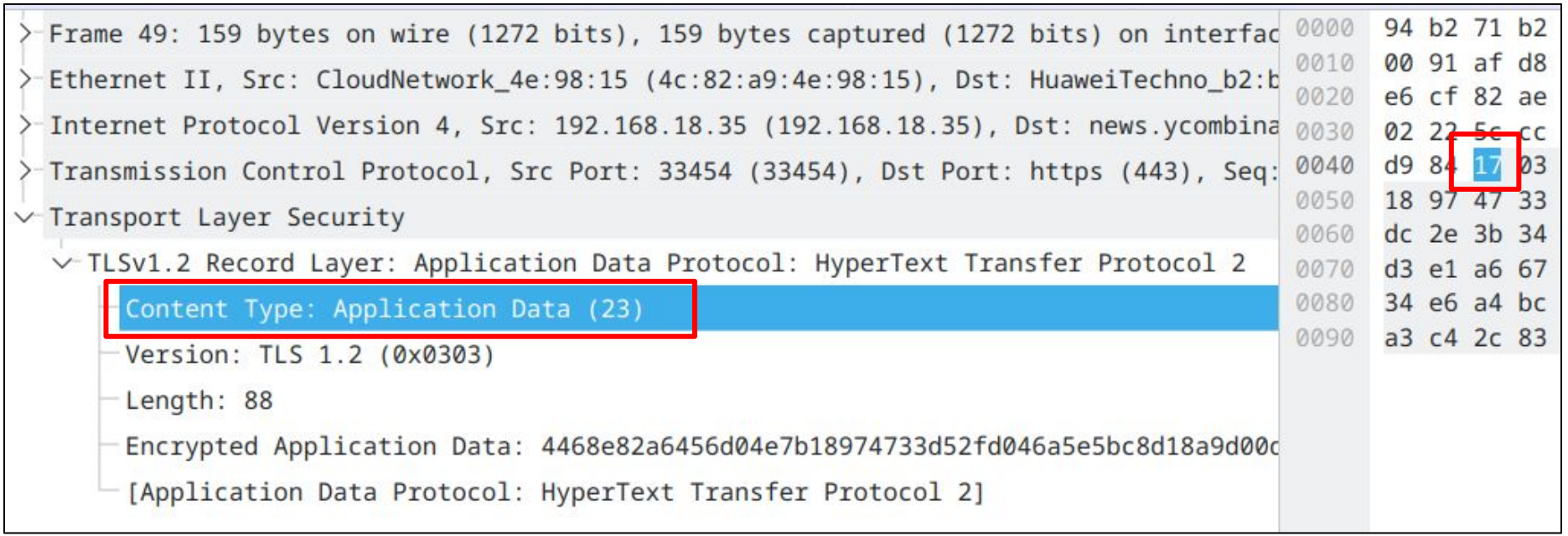
Step 2: Trace Inspection

Wireshark Inspection



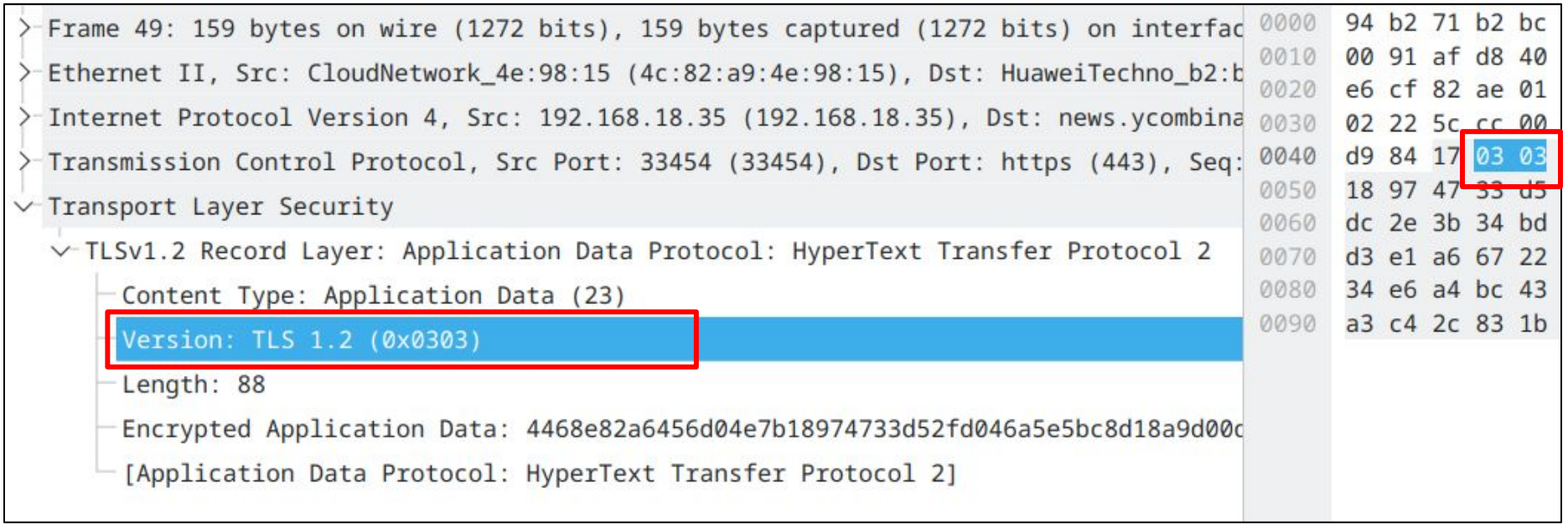
No.	Source	Destination	Protocol	Length	Info
14	85.41.117.34.bc.googl…	192.168.18.35	TLSv1.2	106	Application Data
15	192.168.18.35	85.41.117.34.bc.google…	TLSv1.2	109	Application Data
36	192.168.18.35	news.ycombinator.com	TLSv1.2	583	Client Hello (SNI=news.ycombinator.com)
42	news.ycombinator.com	192.168.18.35	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	106	Application Data

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



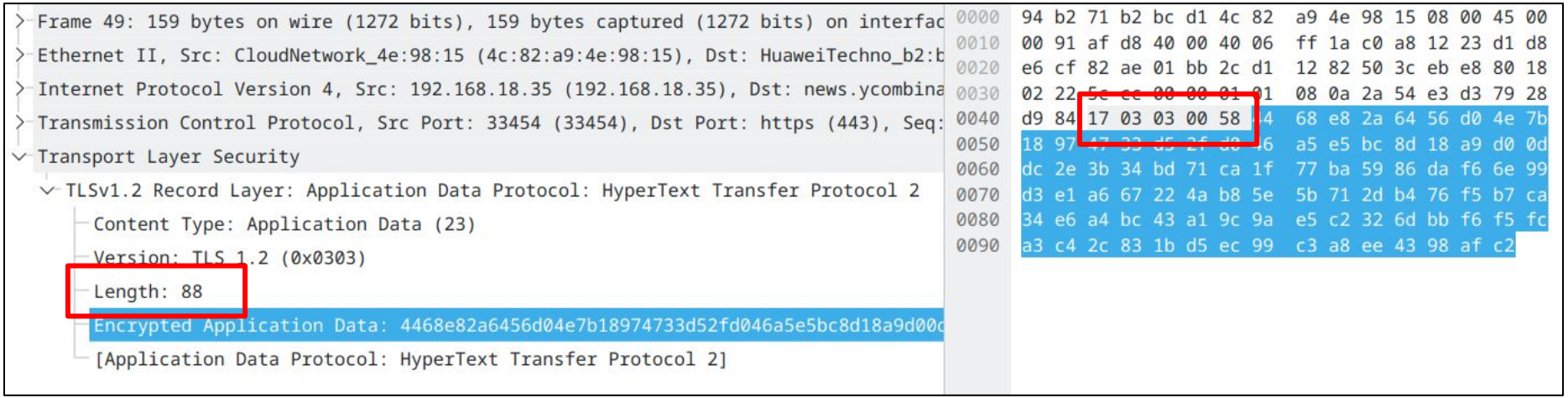
23 or 0x17

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



Version constant 0x0303, which represents TLS v1.2

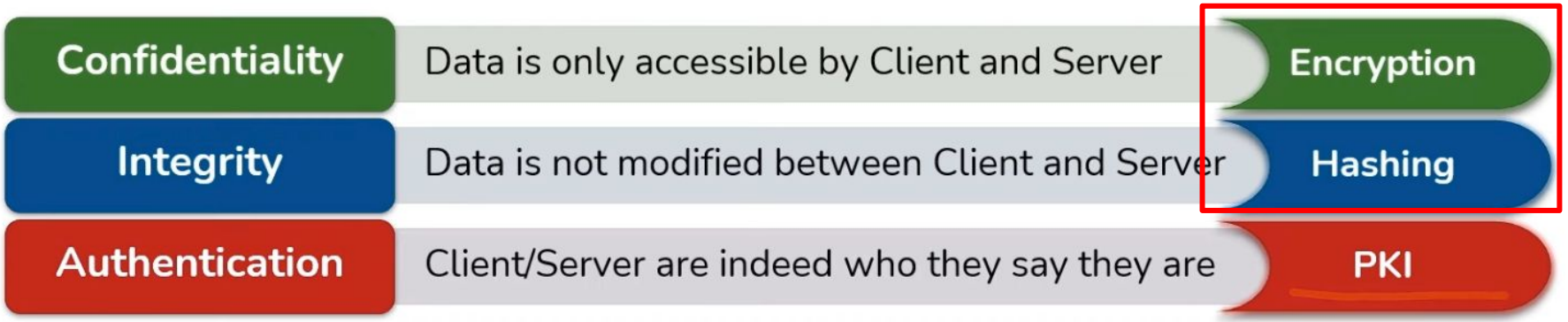
3. Does the Length cover the Record Layer header as well as payload, or only the payload?



Length only covers the payload (highlighted in blue)

Purpose of SSL/TLS

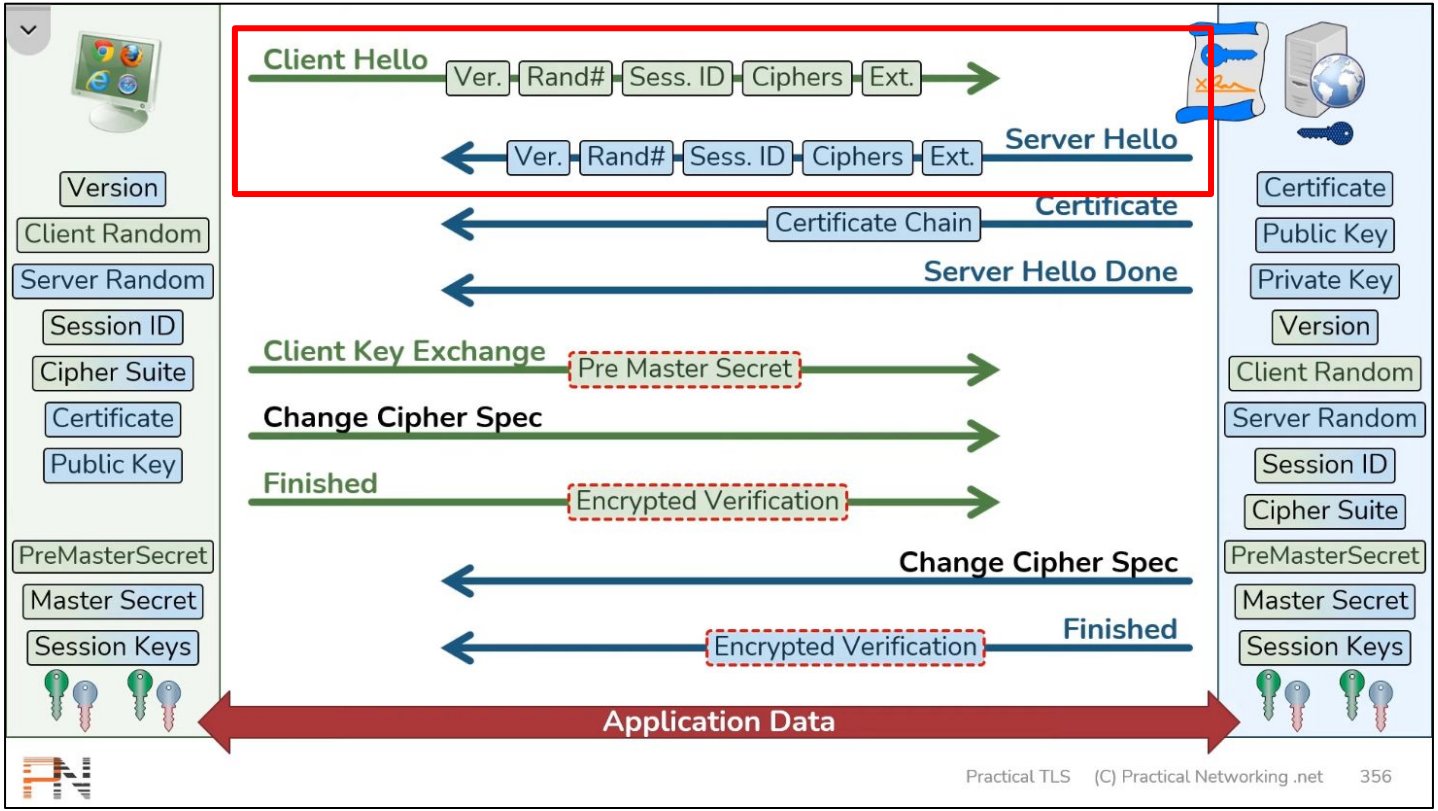
Presentation Layer (6)



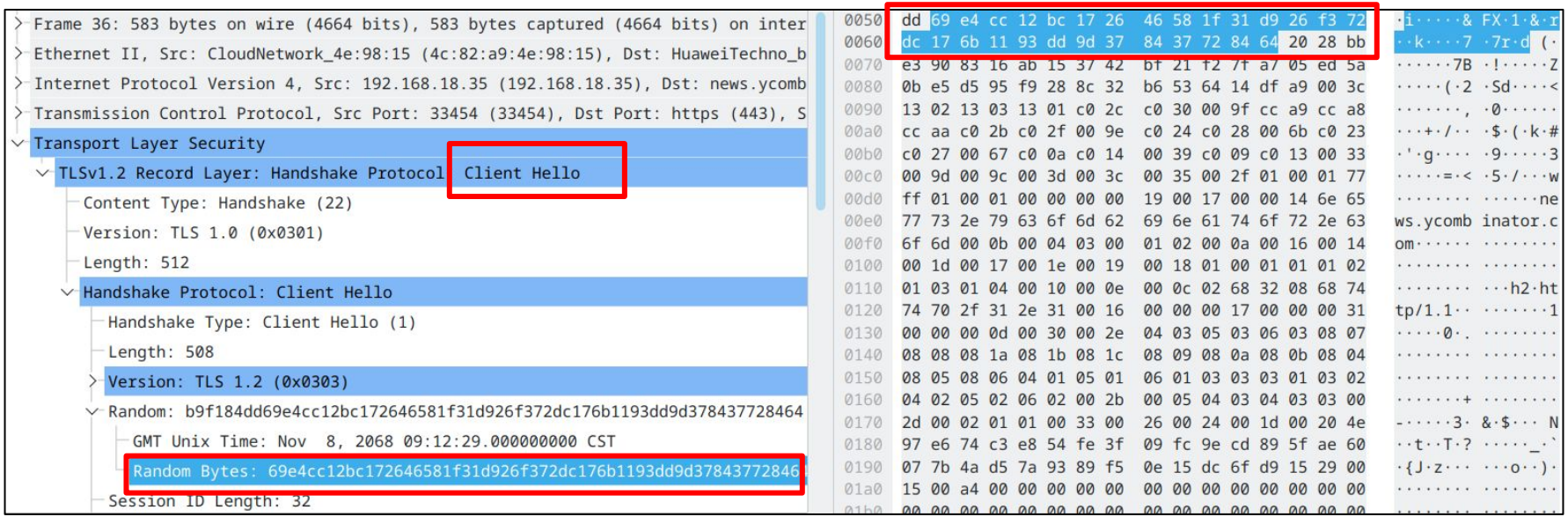
Secure Sockets Layer/ Transport Layer Security
Used in HTTPS, prevent man-in-the-middle attacks.
SSL/TLS exists above Transport Layer (4) but below Application Layer (7)

Step 3: The SSL Handshake

TLS Handshake Overview

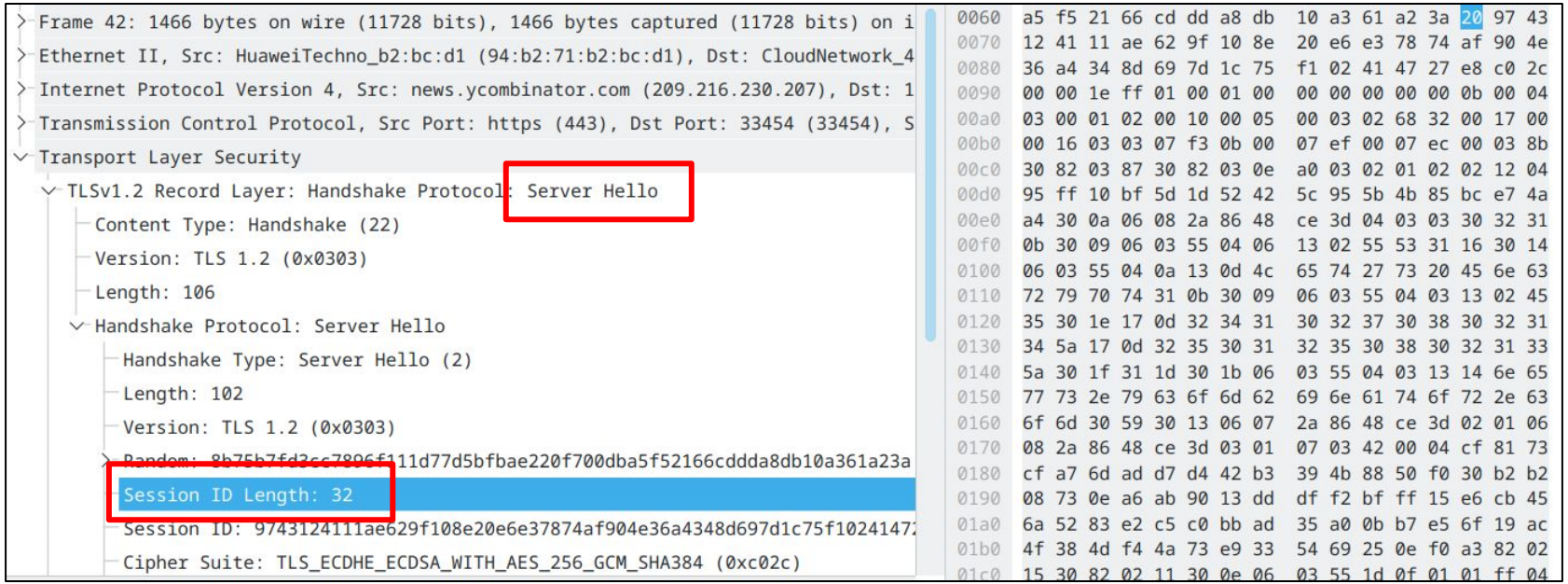


1. How long in bytes is the random data in the Hellos? Both the Client and Server include this random data (a nonce) to allow the establishment of session keys.



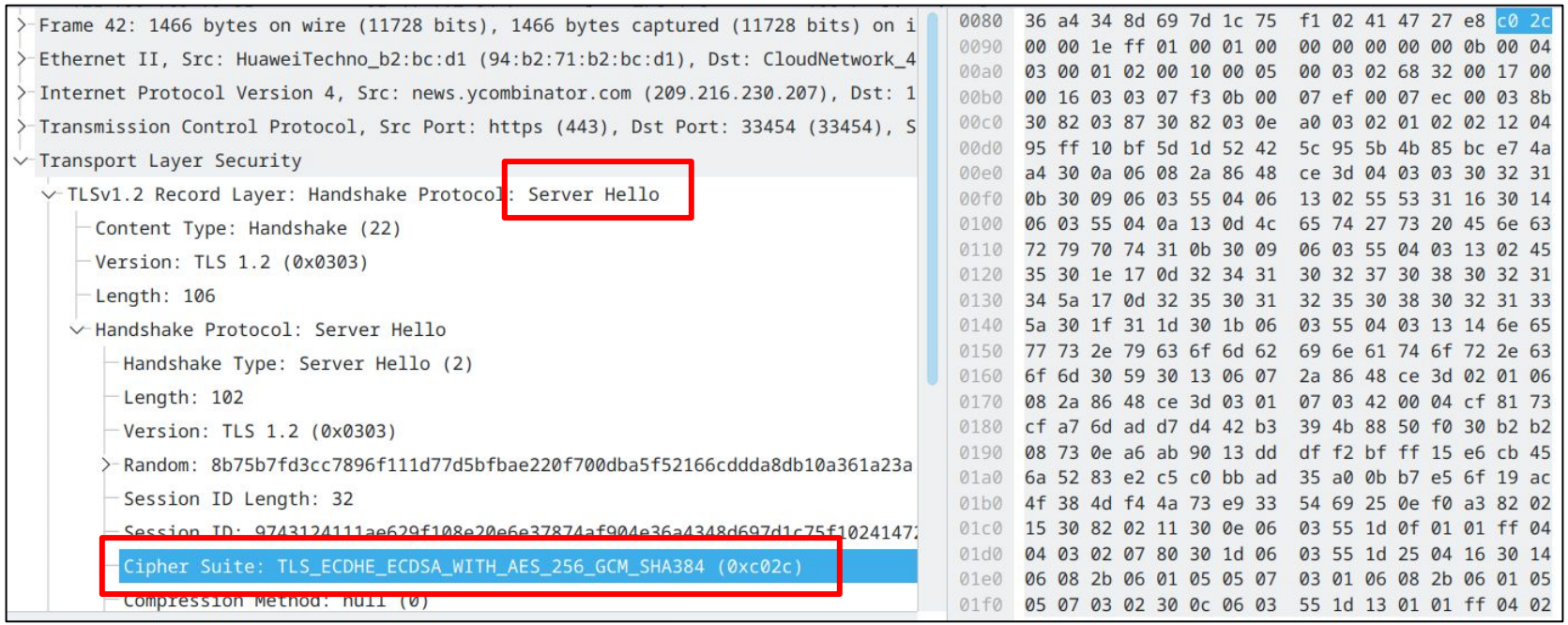
The random data is 28 bytes long for Hellos

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.



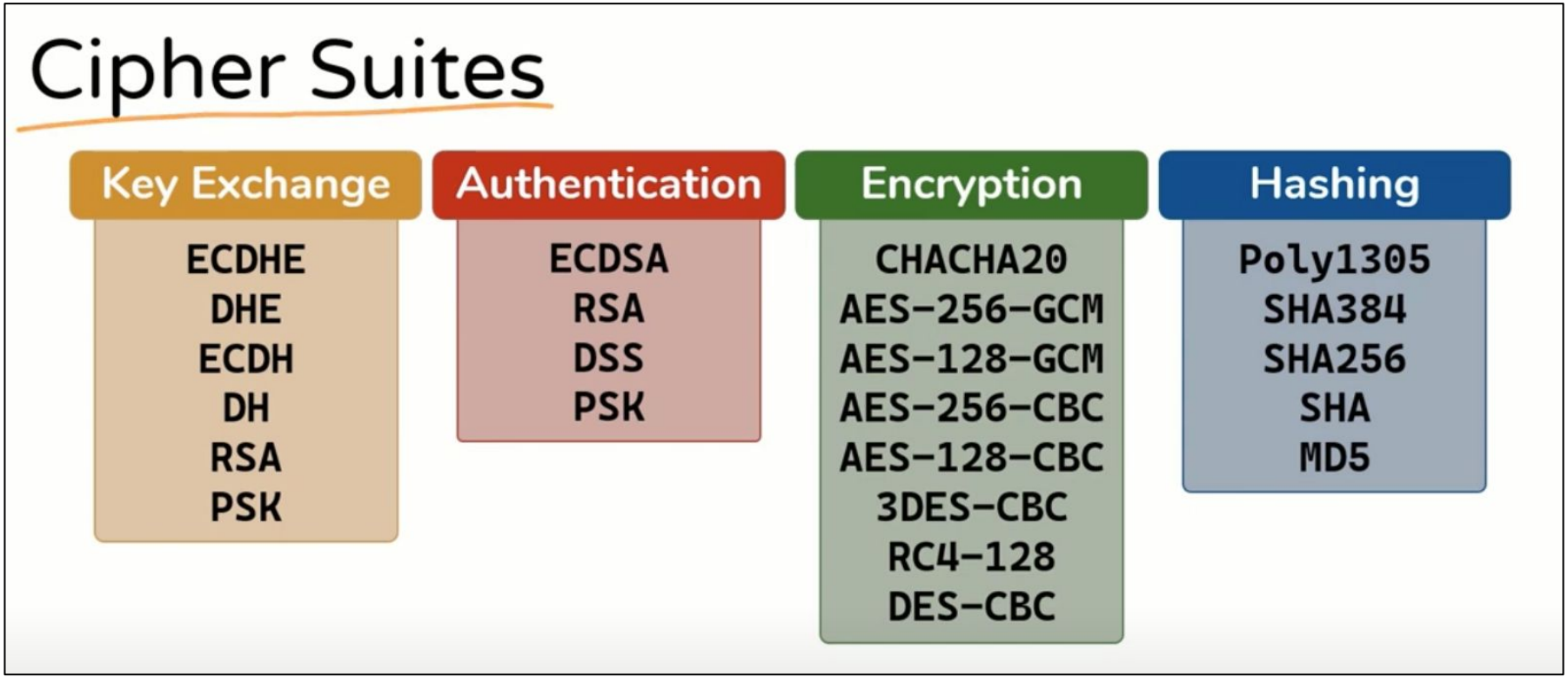
The session identifier sent by the server is 32 bytes long

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.

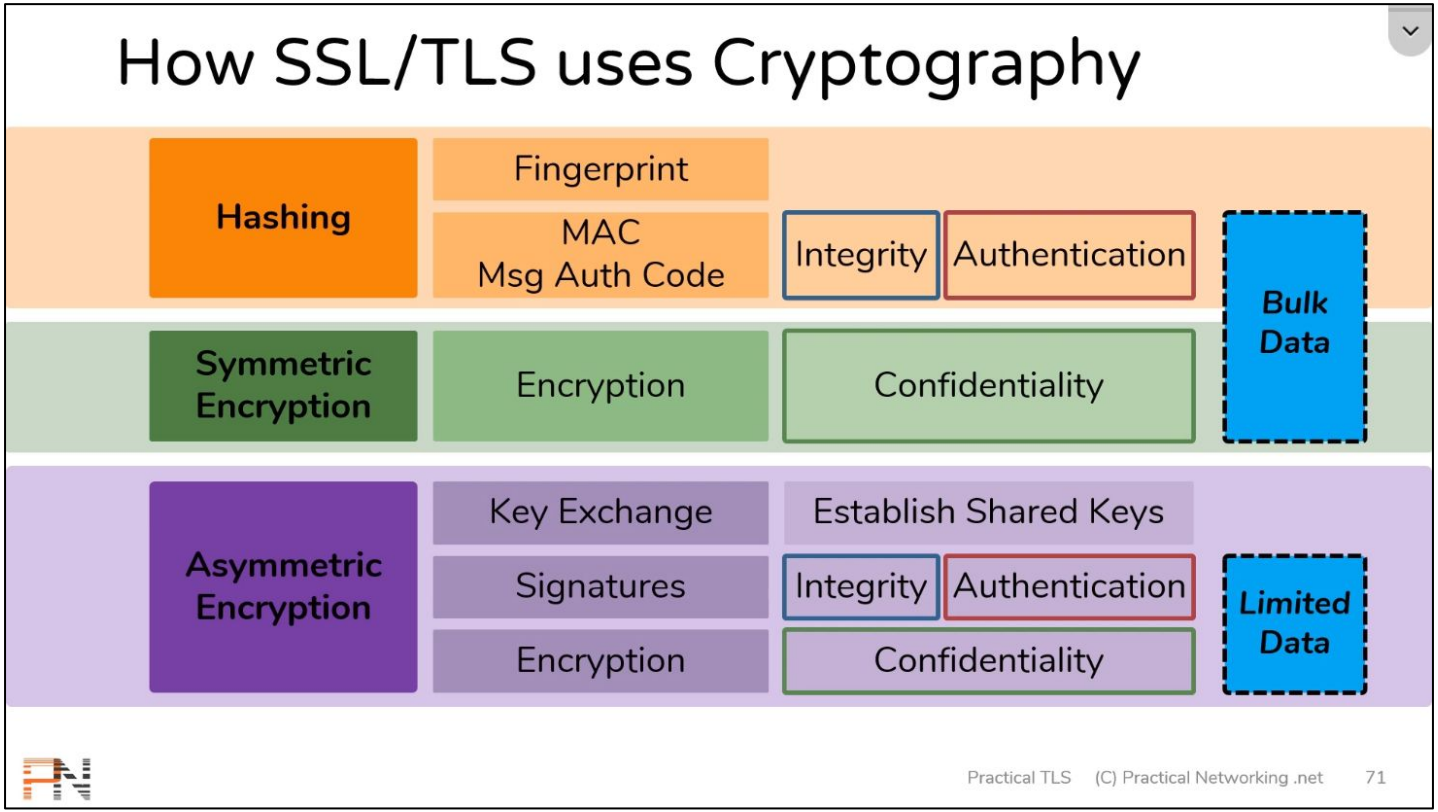


TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)

Presentation Layer (Layer 6) in Action

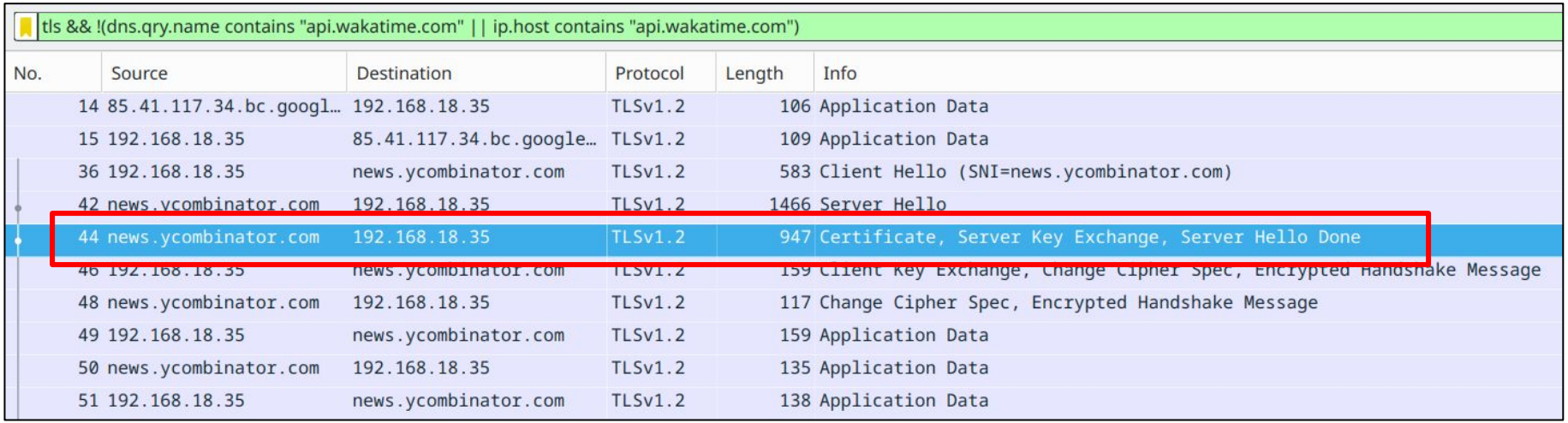


Presentation Layer (Layer 6) in Action



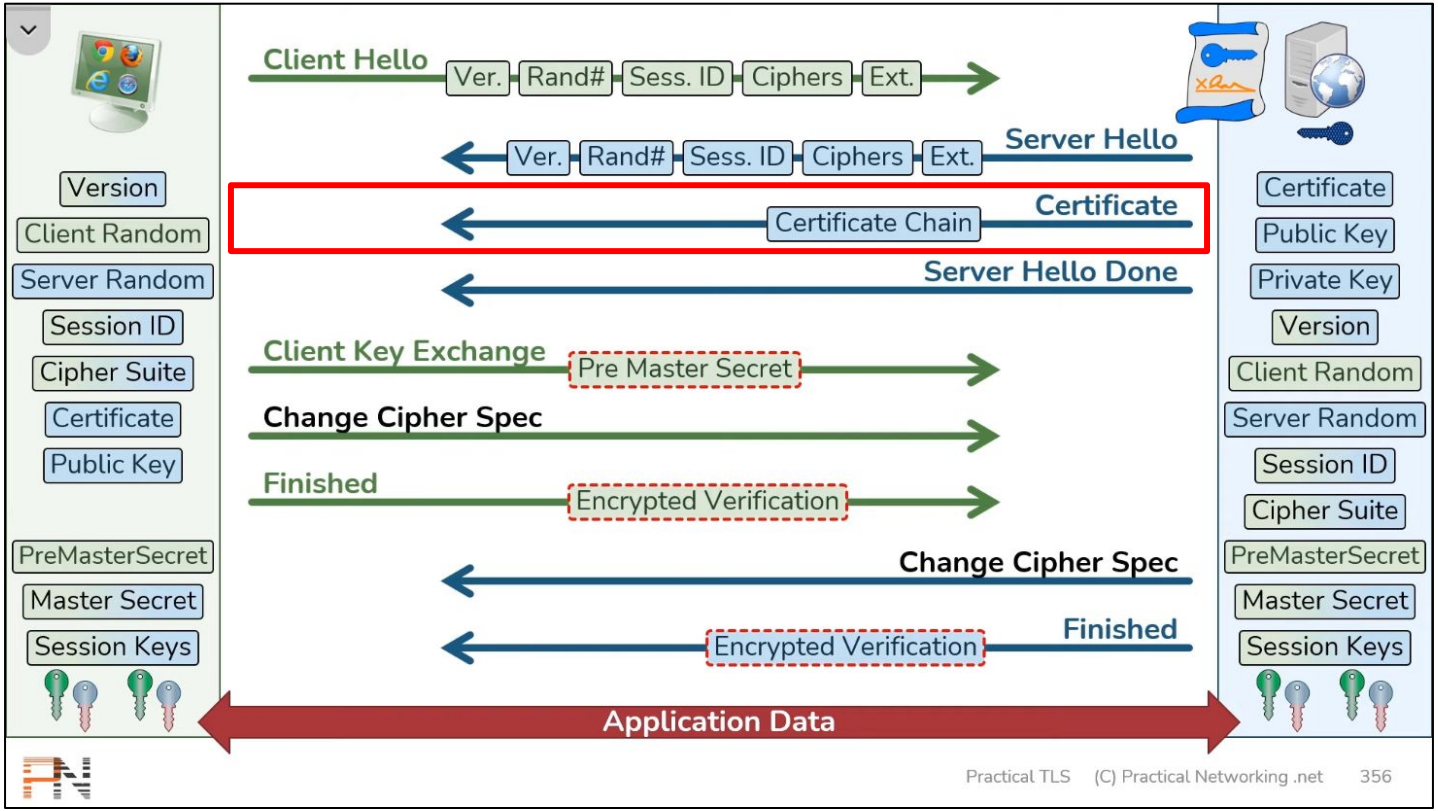
Certificate Messages

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.

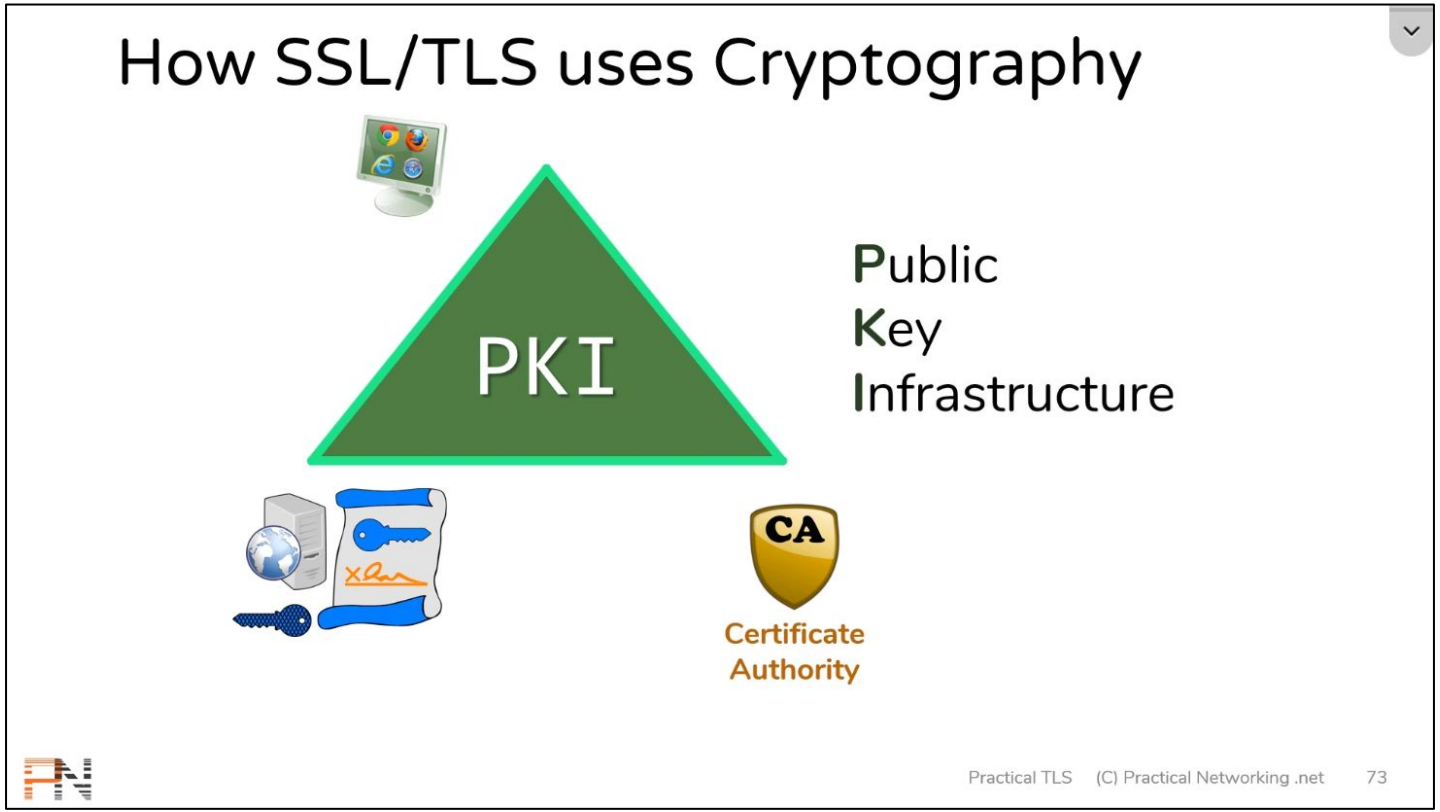


Only the server (client optional)

TLS Handshake Overview

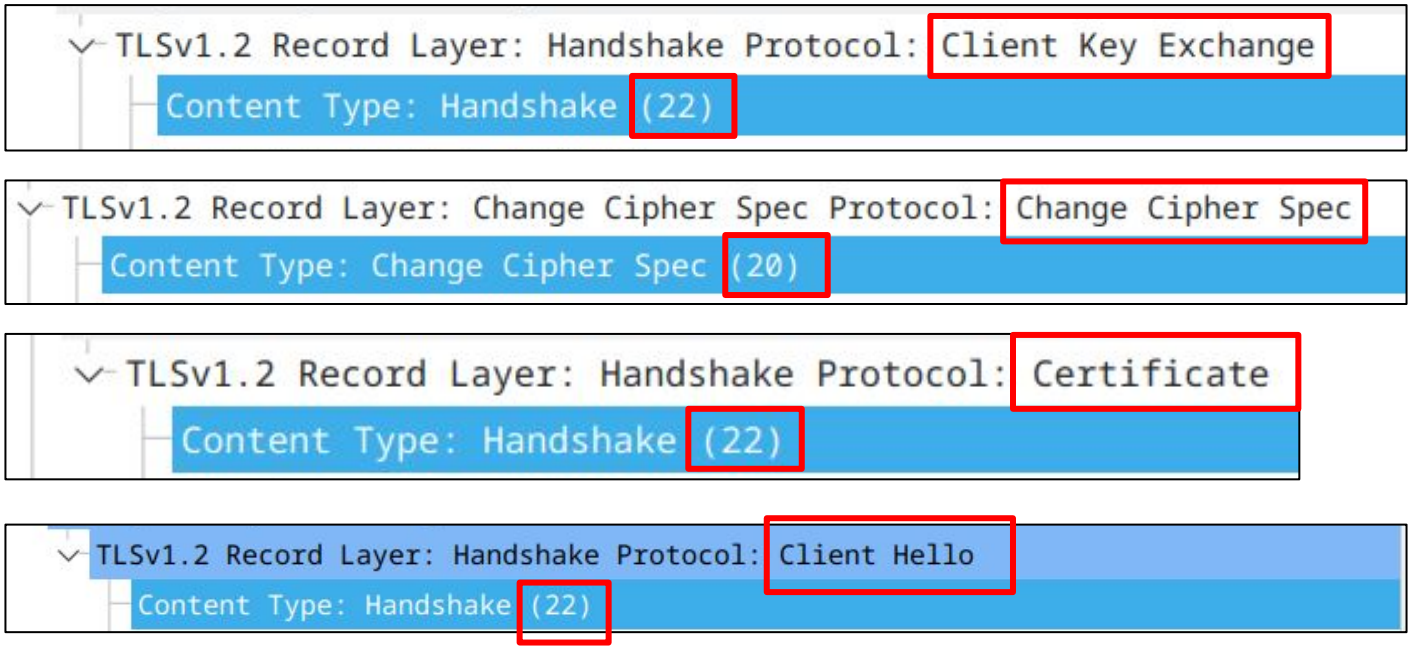


How Certificates are Used



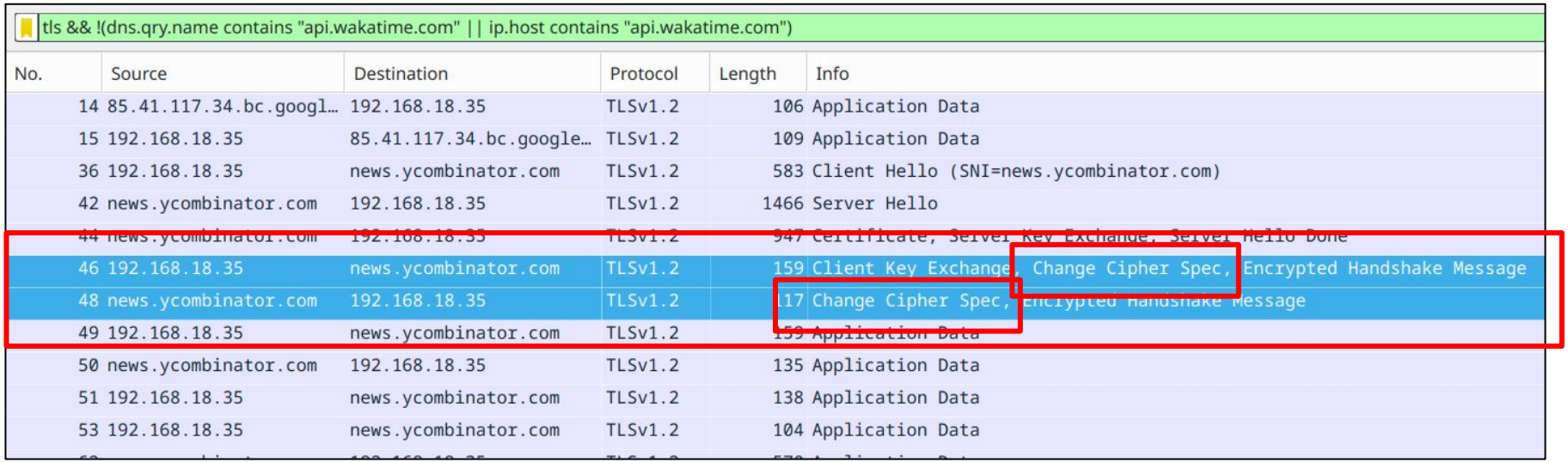
Client Key Exchange and Change Cipher Messages

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.



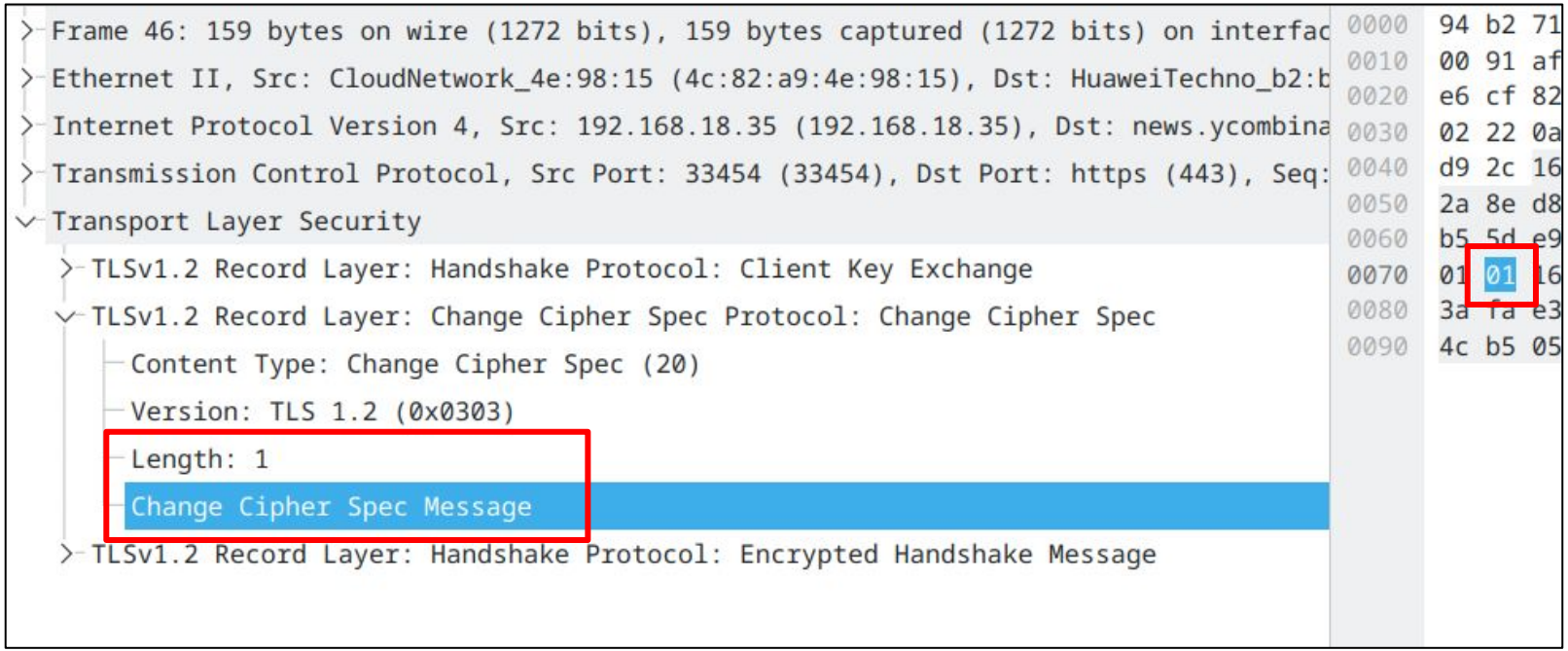
The only different one is Change Cipher Spec. The rest are the same.

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



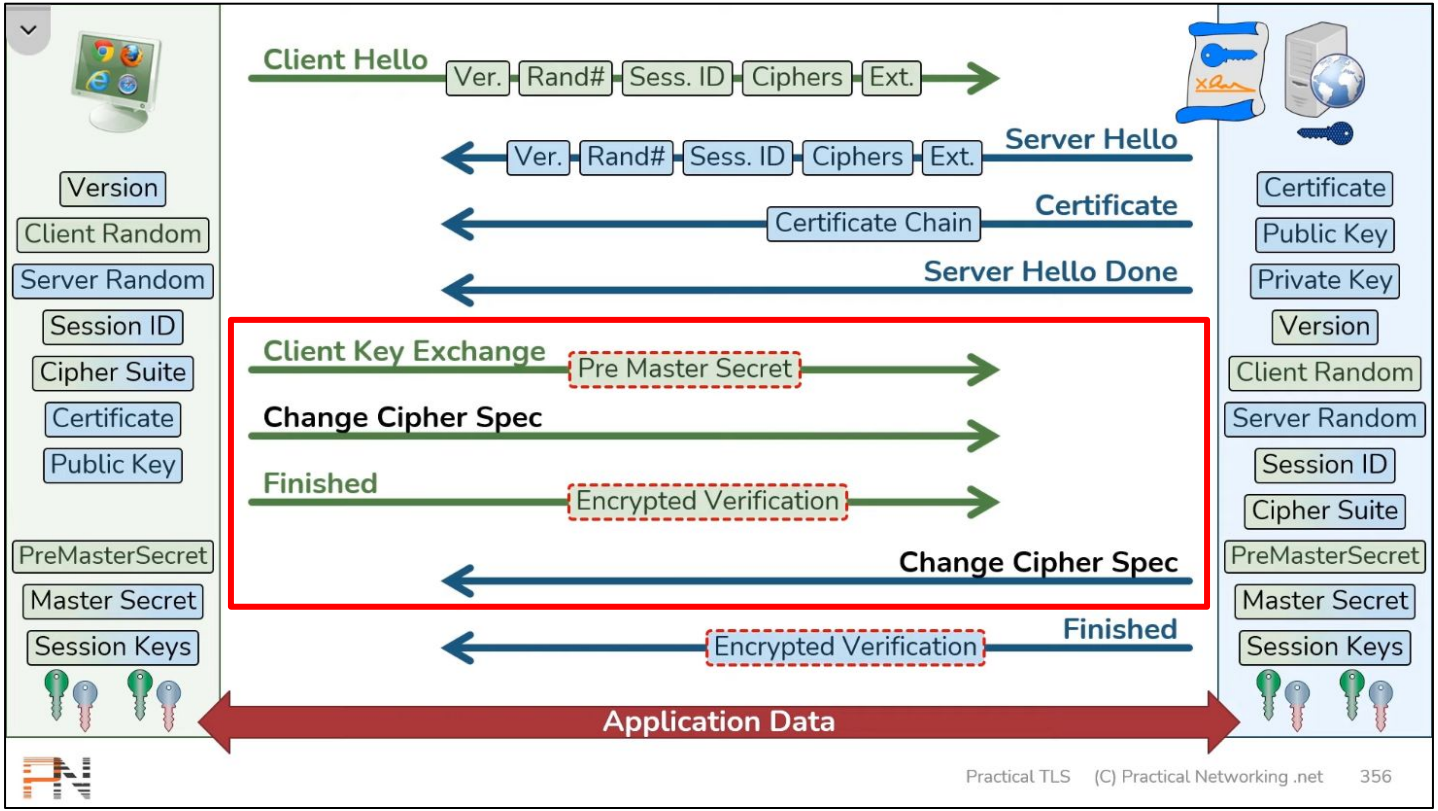
Both client and server

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.



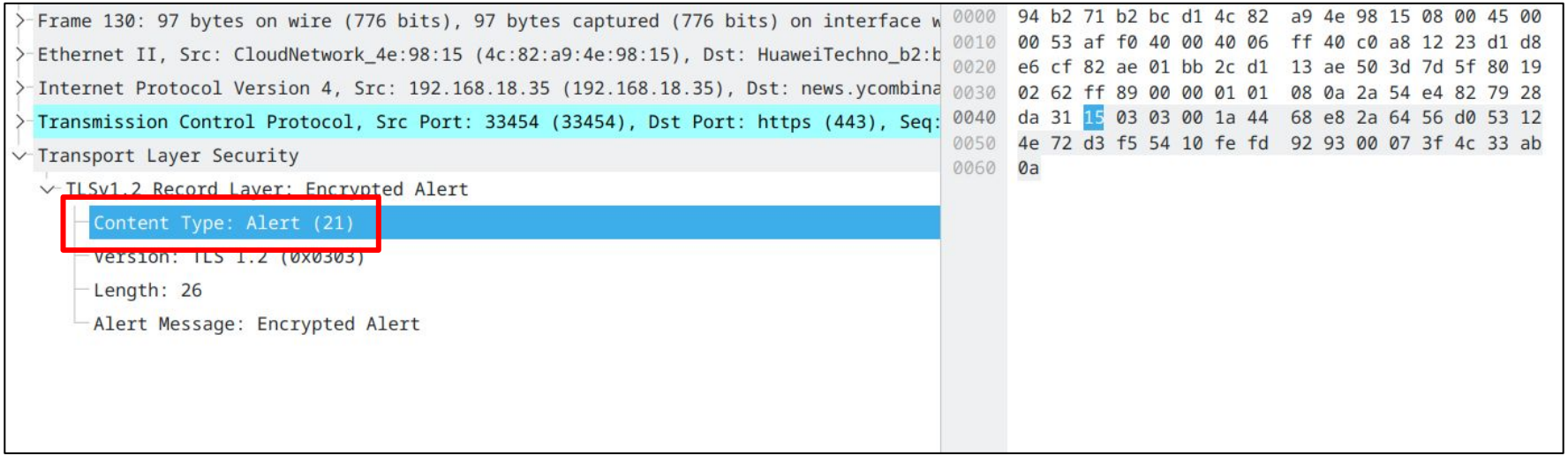
The content is just a single byte that contains the value 1

TLS Handshake Overview



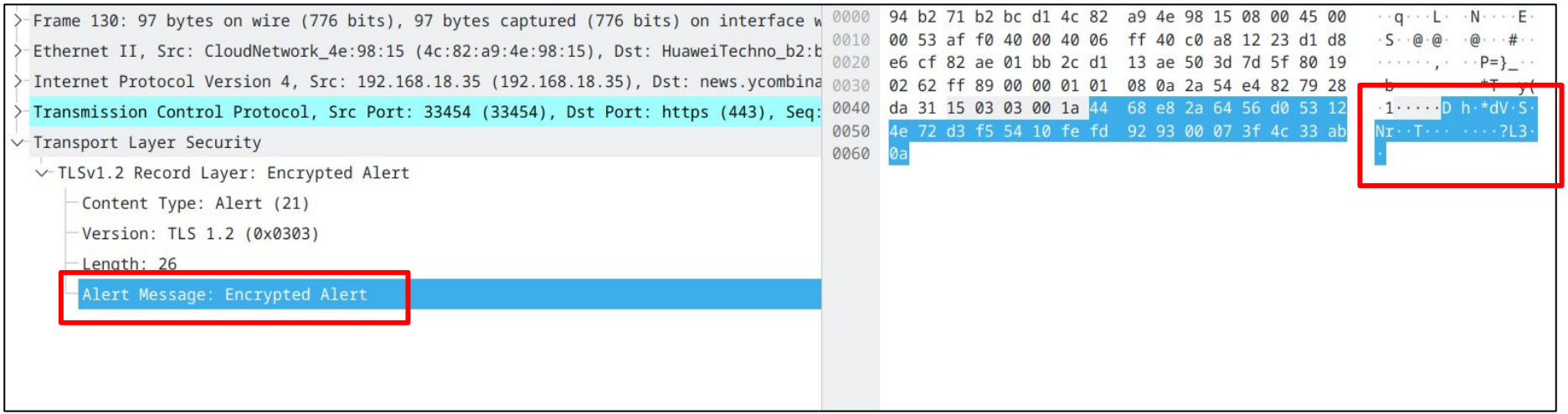
Alert Message

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



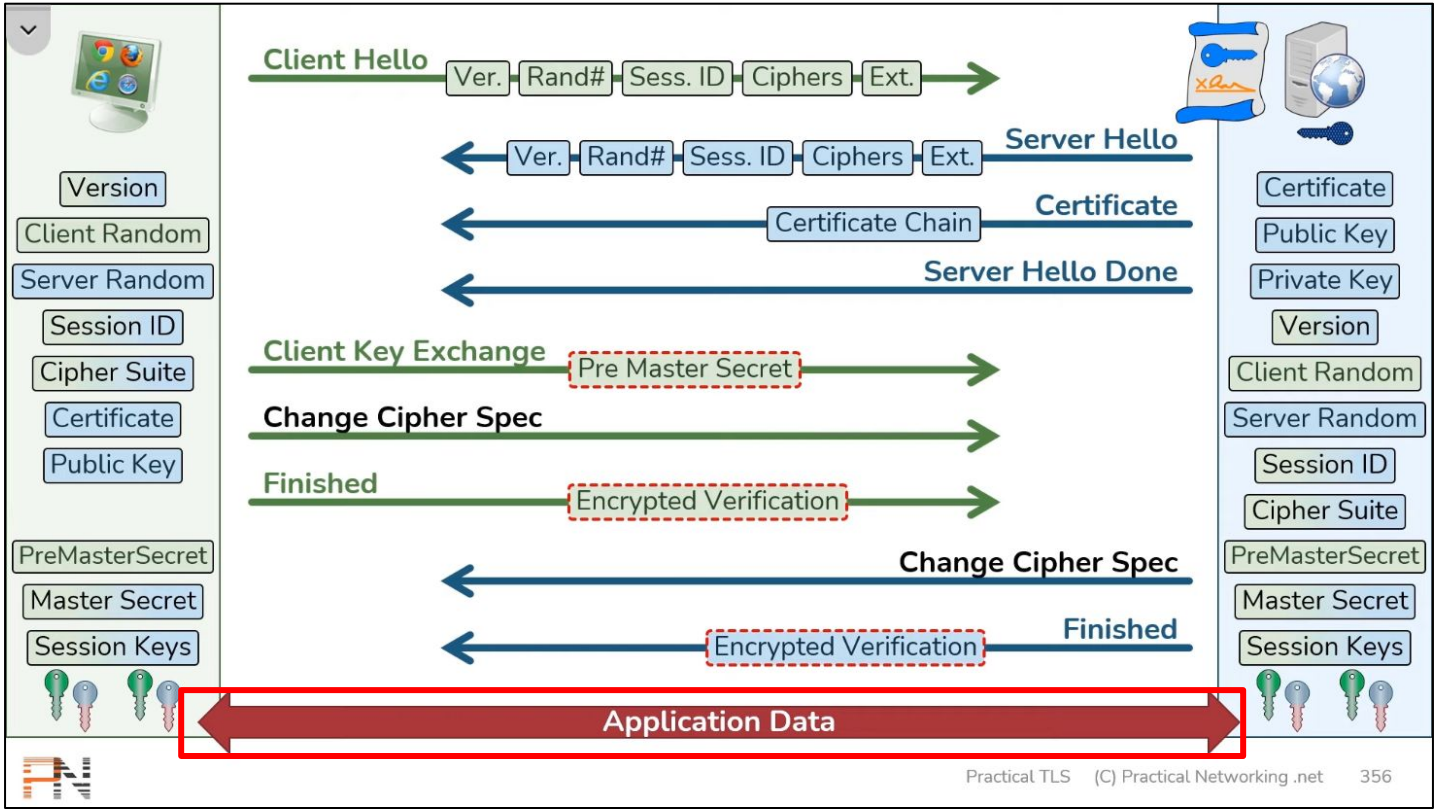
Content-Type 21 is used

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.

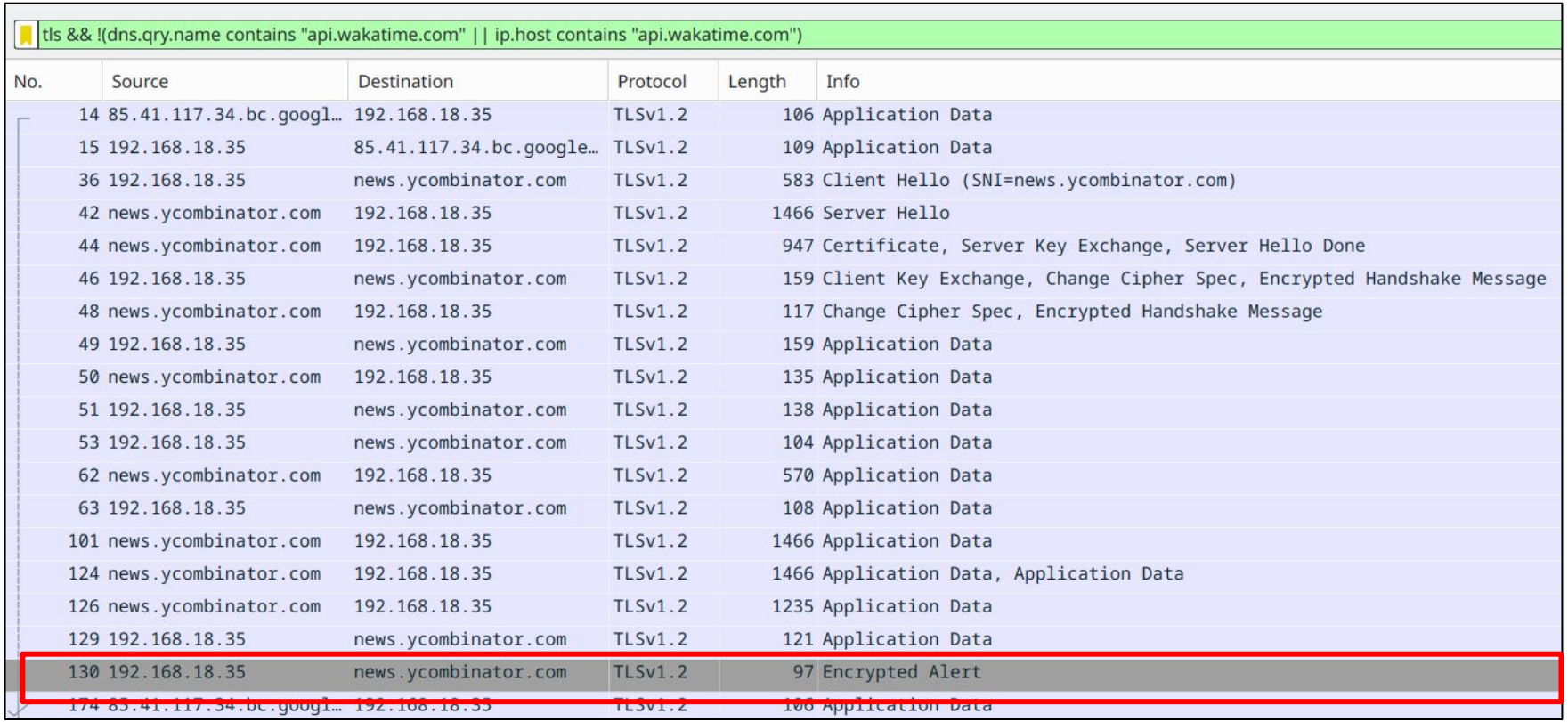


The contents are encrypted

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 TLSv1.2 106 Application Data