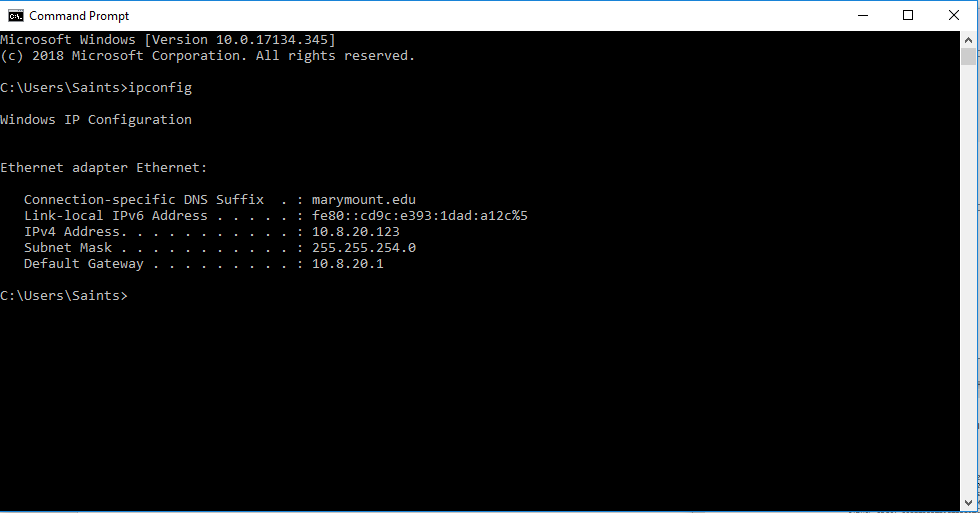
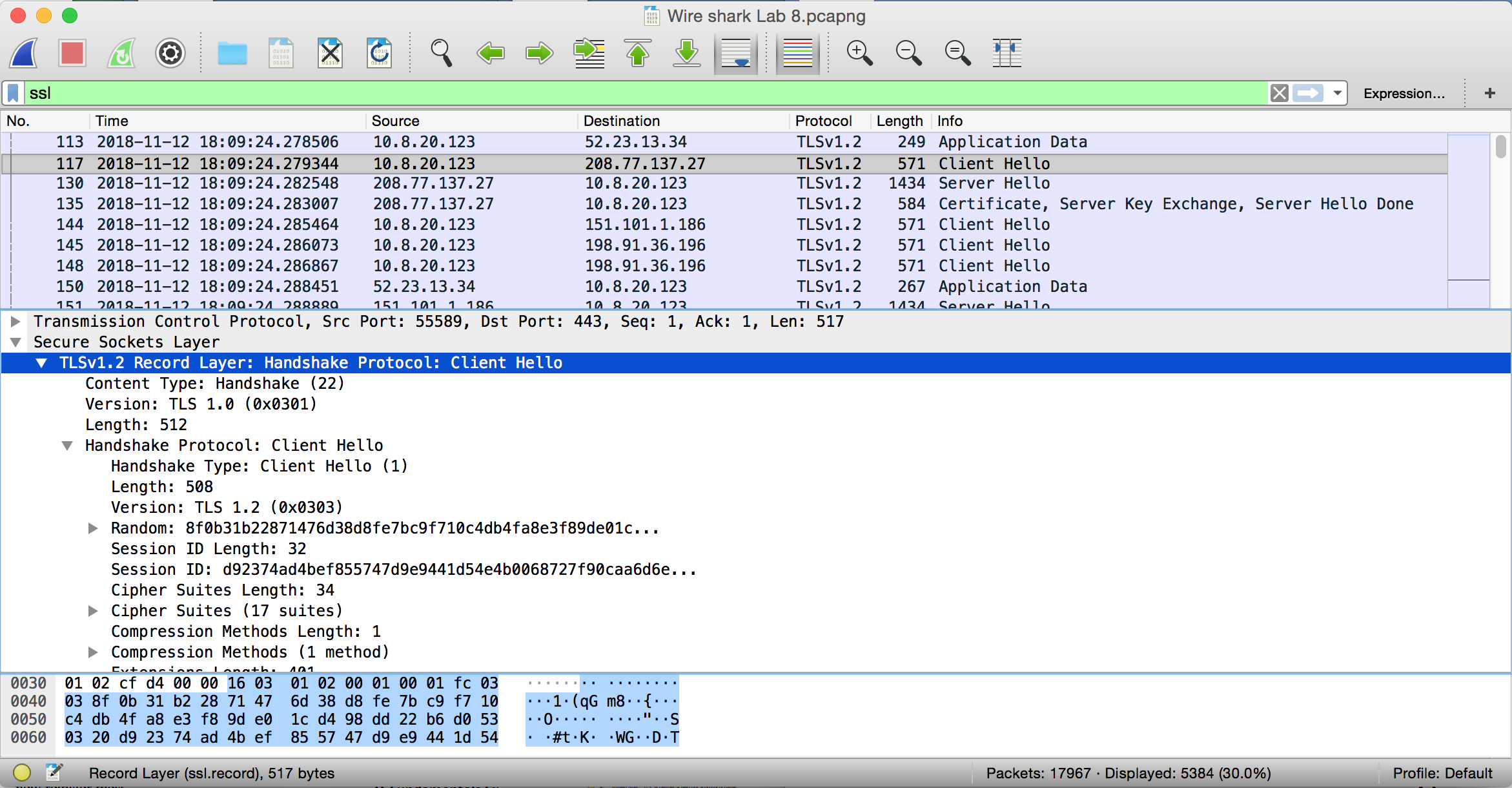
Lab 8-SSL/TLS



Client Hello Record:

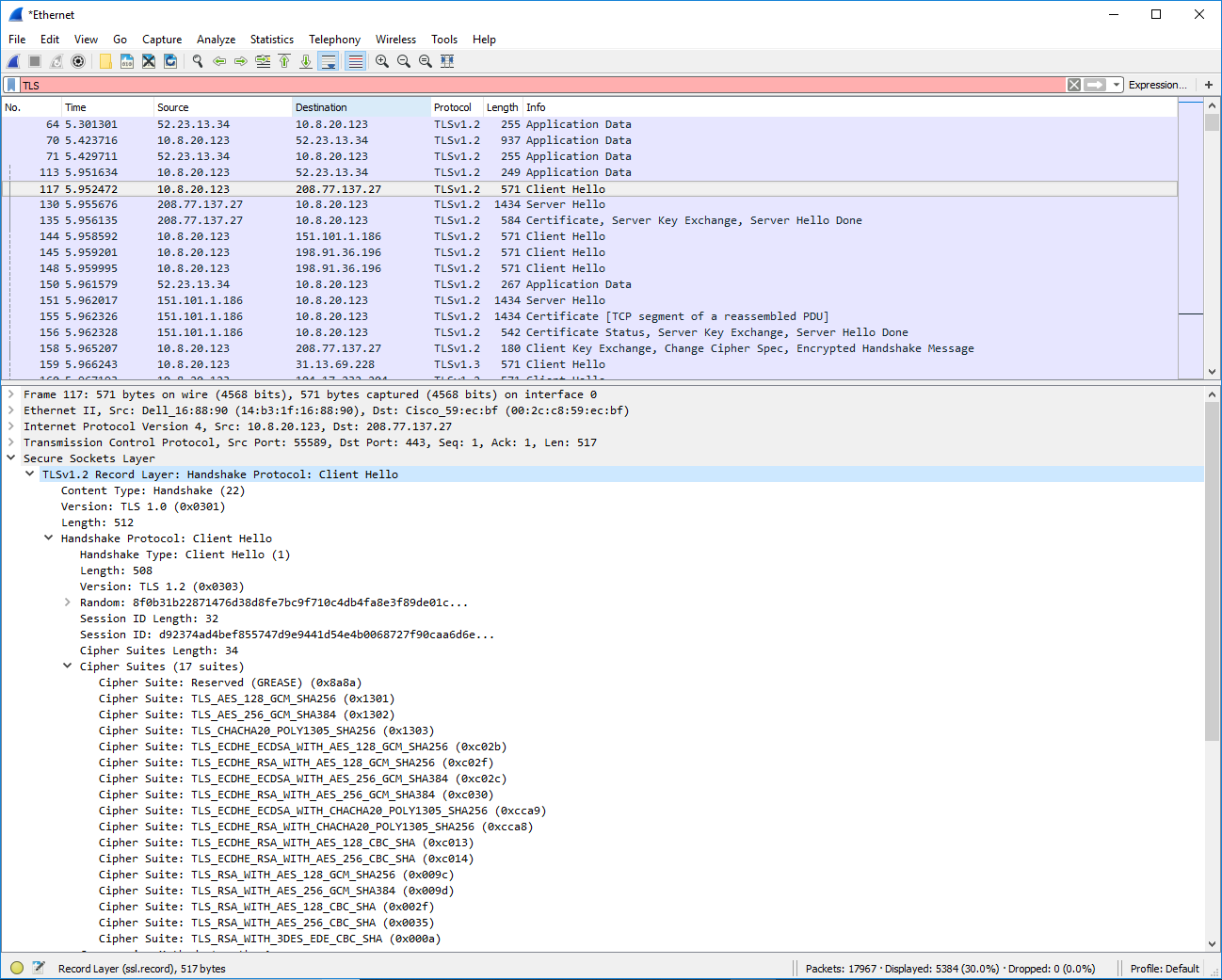
1. What is the SSL/TLS version of the of the Client Hello frame?



**Solution:**

TLSv1.2

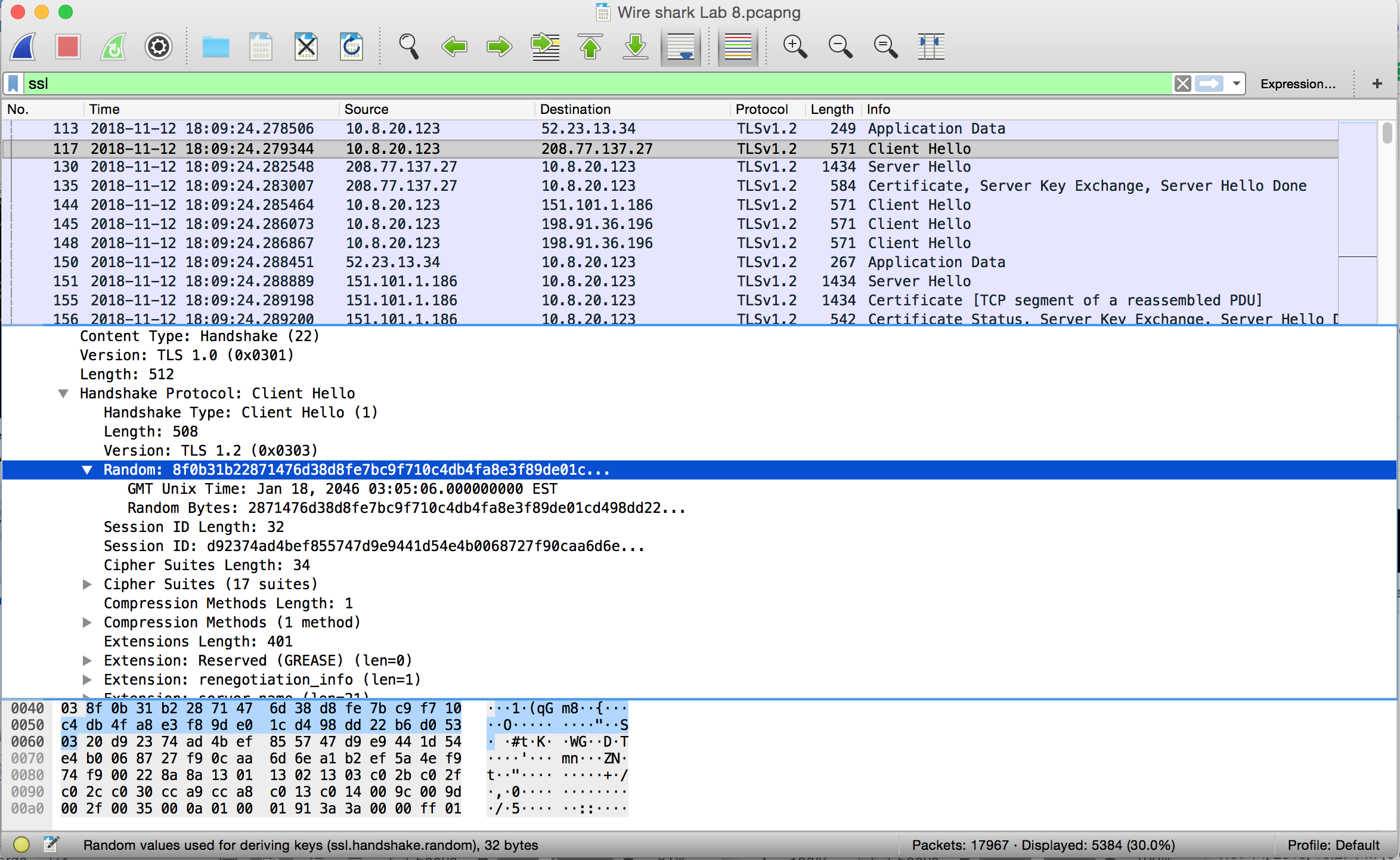
1. Expand the ClientHello record. (If your trace contains multiple ClientHello records, expand the frame that contains the first one.) What is the value of the content type?



**Solution:**

The content Type is Handshake (22)

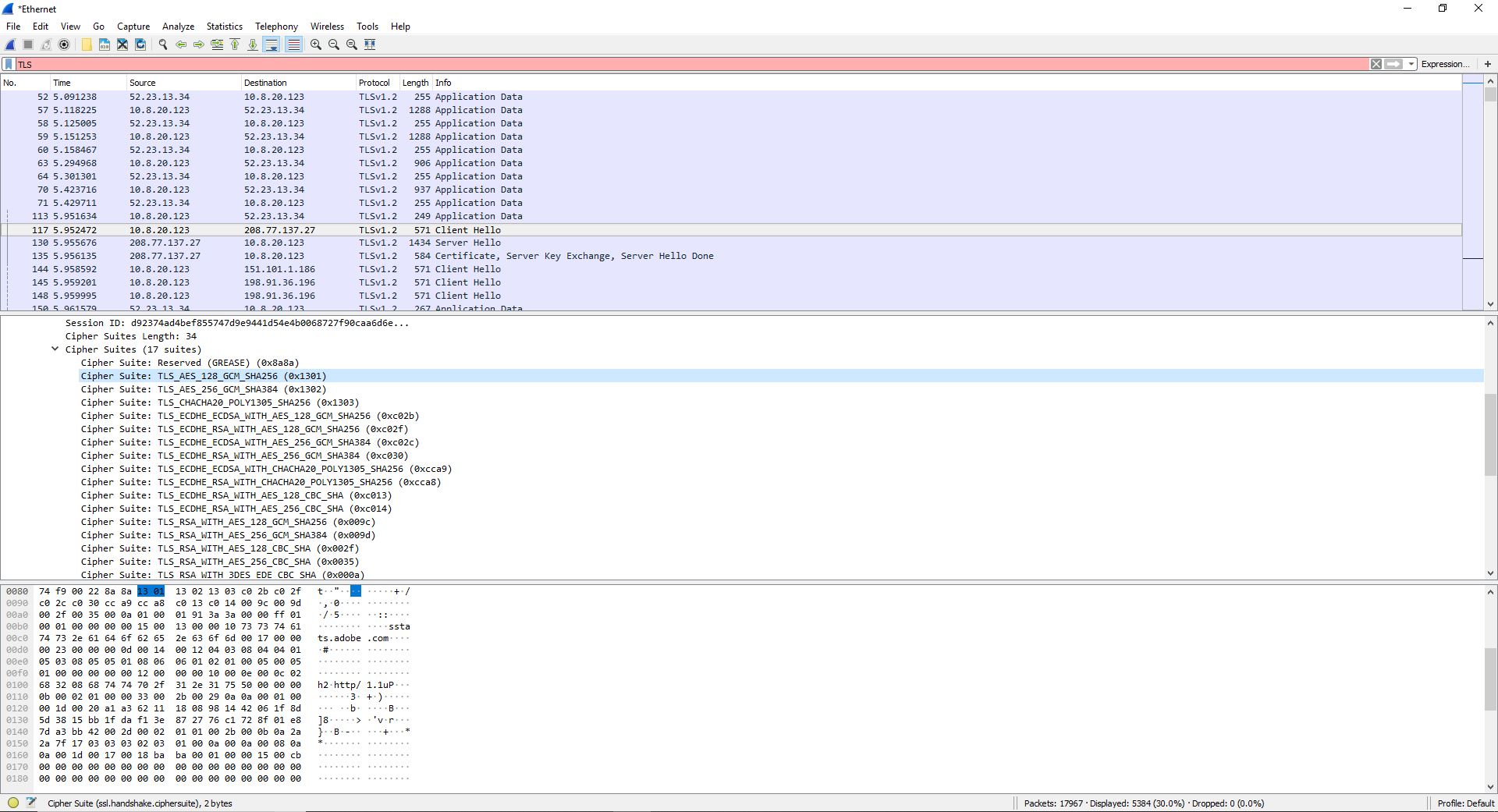
1. Does the ClientHello record contain a nonce (also known as a “challenge”)? If so, what is the value of the challenge in hexadecimal notation?

****

**Solution:**

Random: 8f:0b:31:b2:28:71:47:6d:38:d8:fe:7b:c9:f7:10:c4:db:4f:a8:e3:f8:9d:e0:1c:d4:98:dd:22:b6:d0:53

4.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 hash algorithm?



**Solution:**

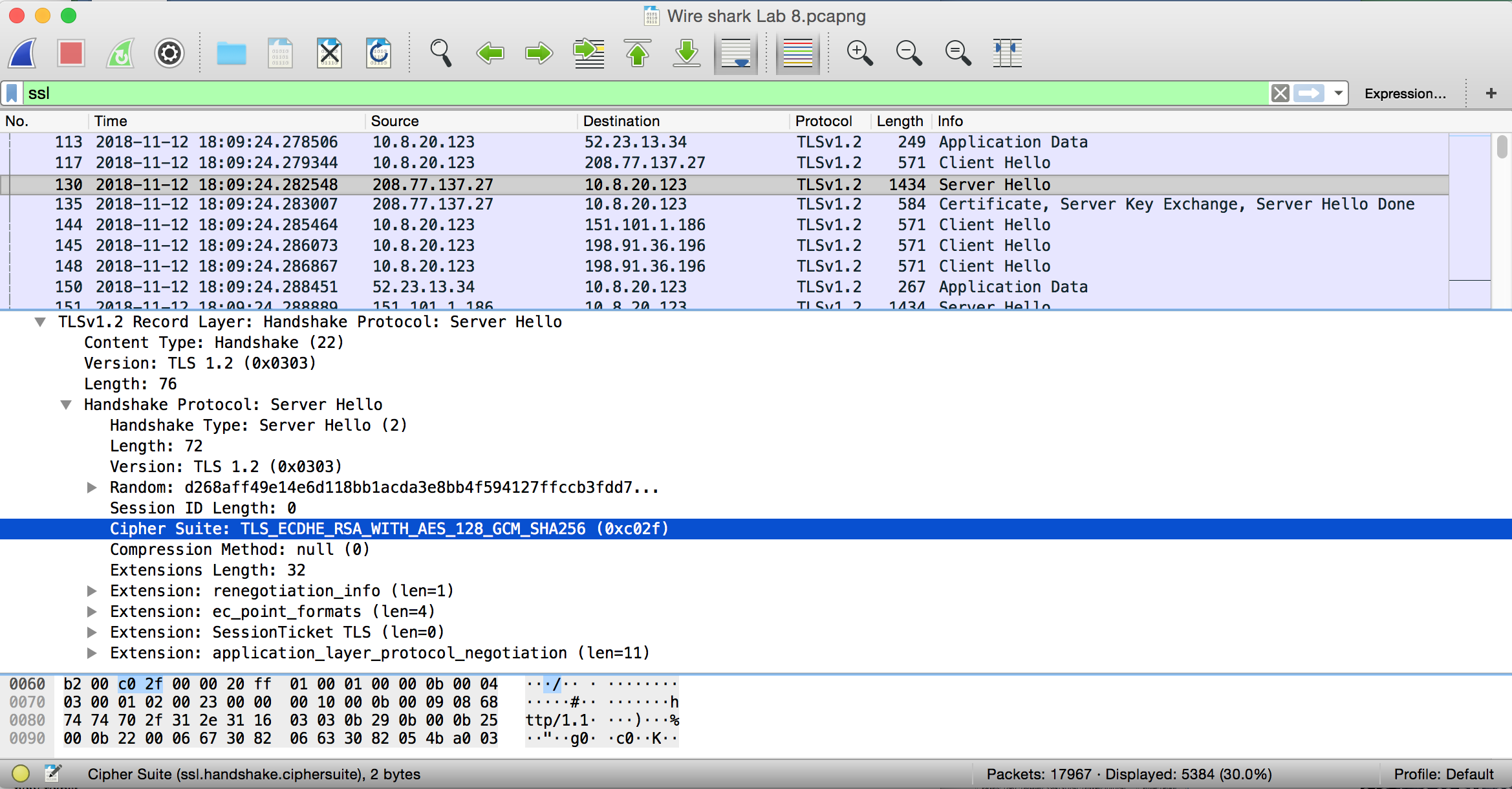
Public key algorithm: GCM

Symmetric‐key algorithm: AES

Hash algorithm: SHA256

**Server Hello Record:**

1. Locate the Server Hello SSL record. Does this record specify a chosen cipher suite? What are the algorithms in the chosen cipher suite?



**Solution:**

Yes, this record specifies a chosen cipher suite. TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02f).

Public key algorithm: GCM

Symmetric‐key algorithm: AES

Asymmetric‐key algorithm: RSA

Hash algorithm: SHA256