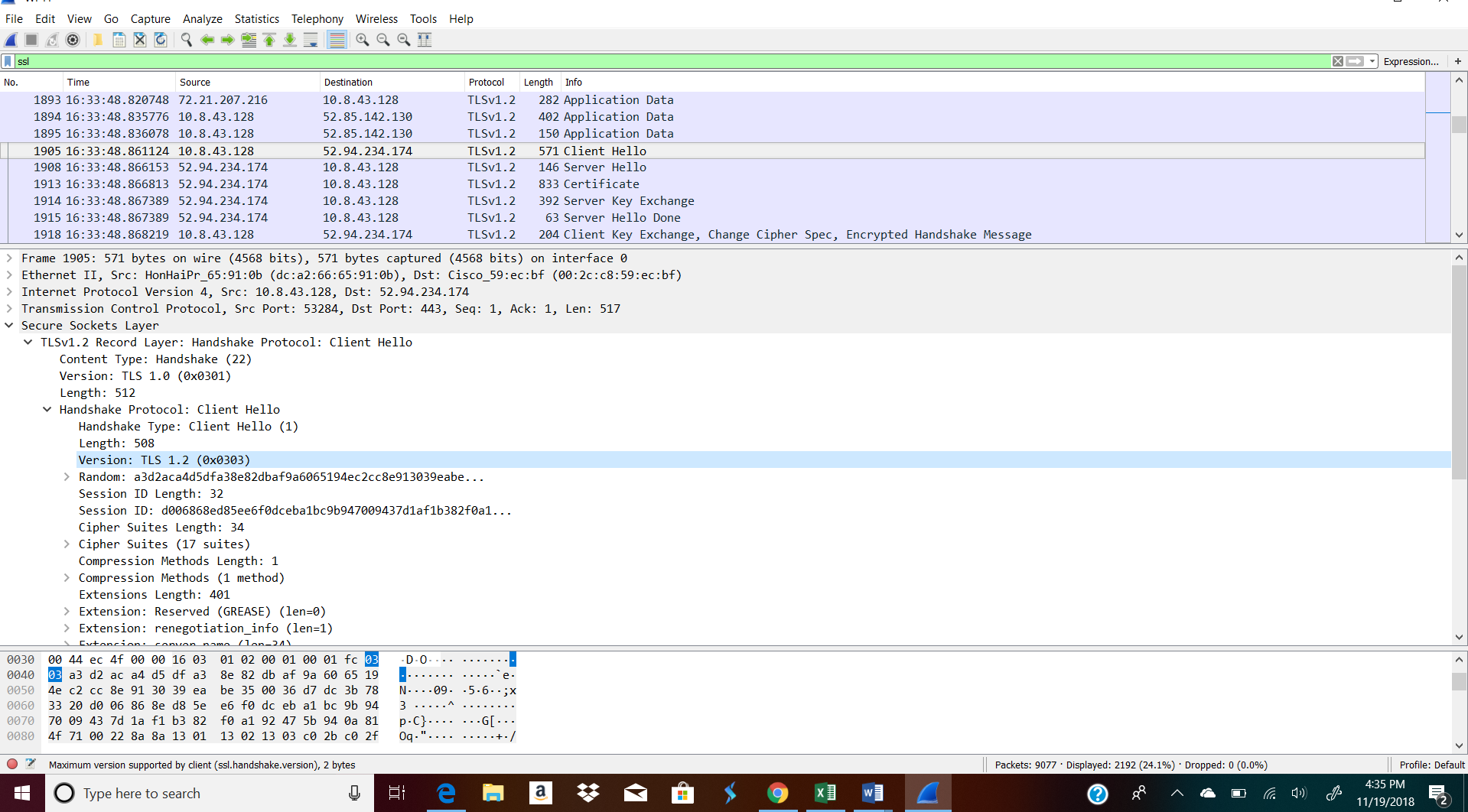
Rishi Sharma

Lab 8

11/19/18

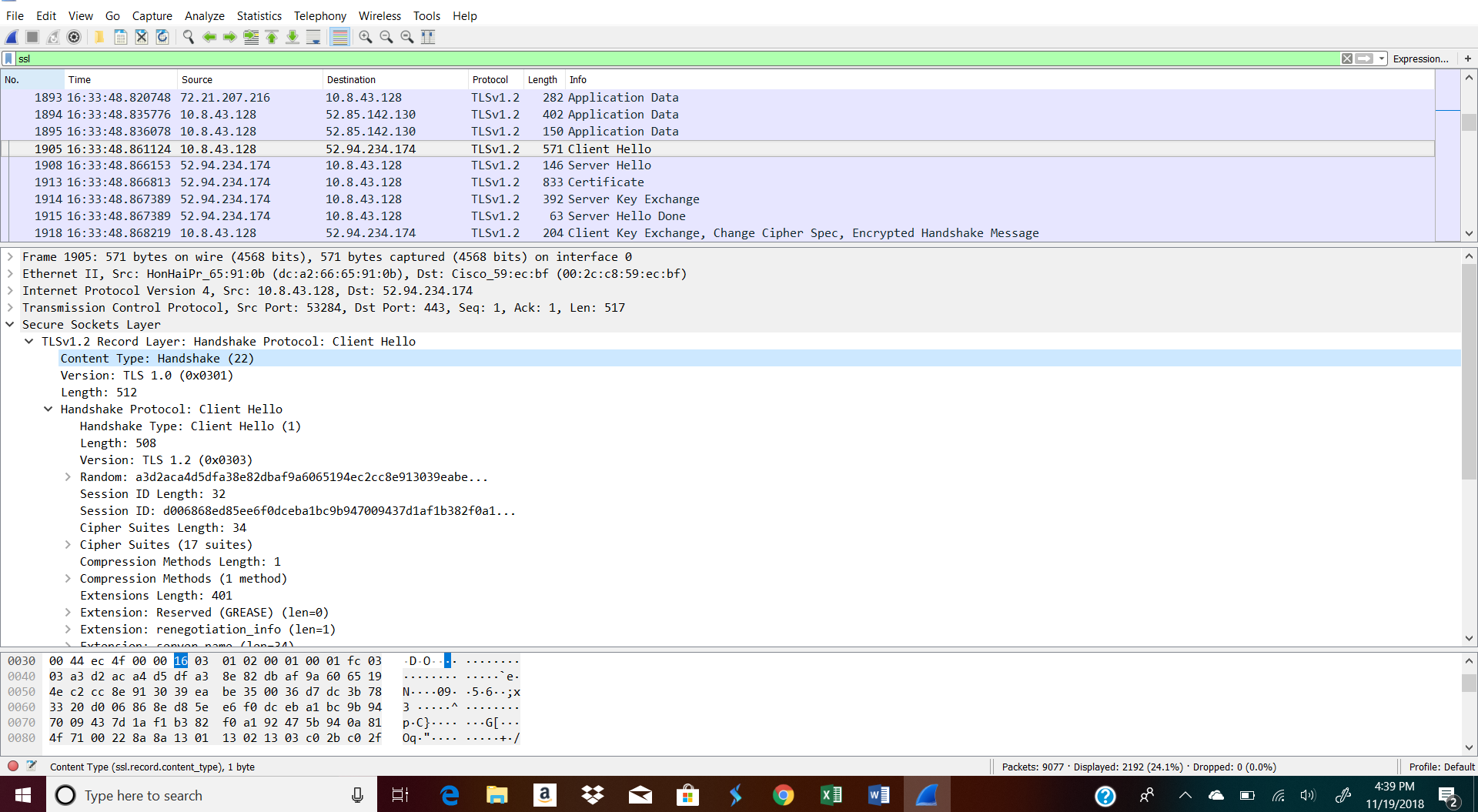
1. What is the SSL/TLS version of the of the Client Hello frame?

Version TLS 1.2



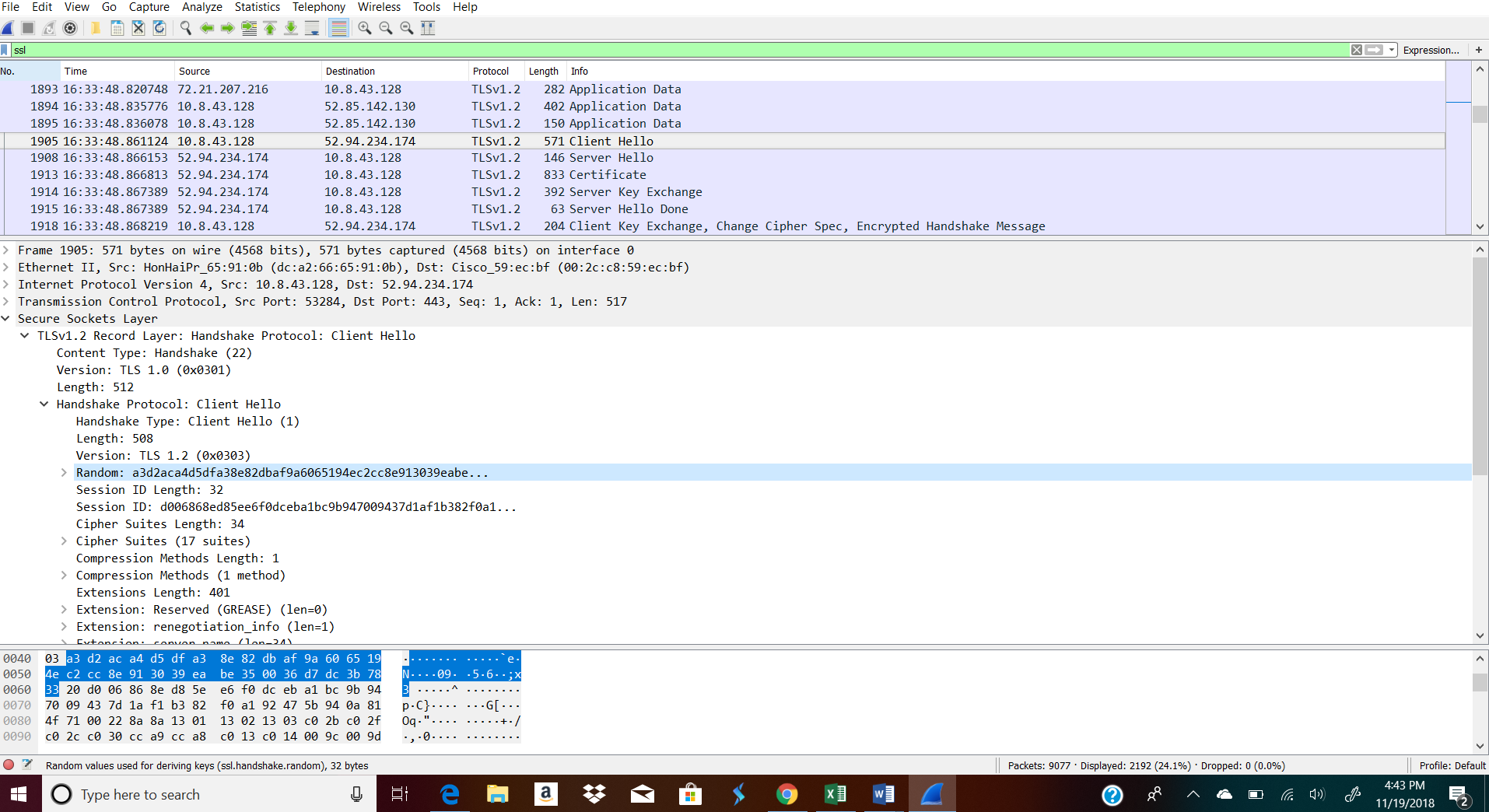
1. Expand the ClientHello record. (If your trace contains multiple ClientHello records, expand the frame that contains the first one.) What is the value of the content type?

Content Type: Handshake



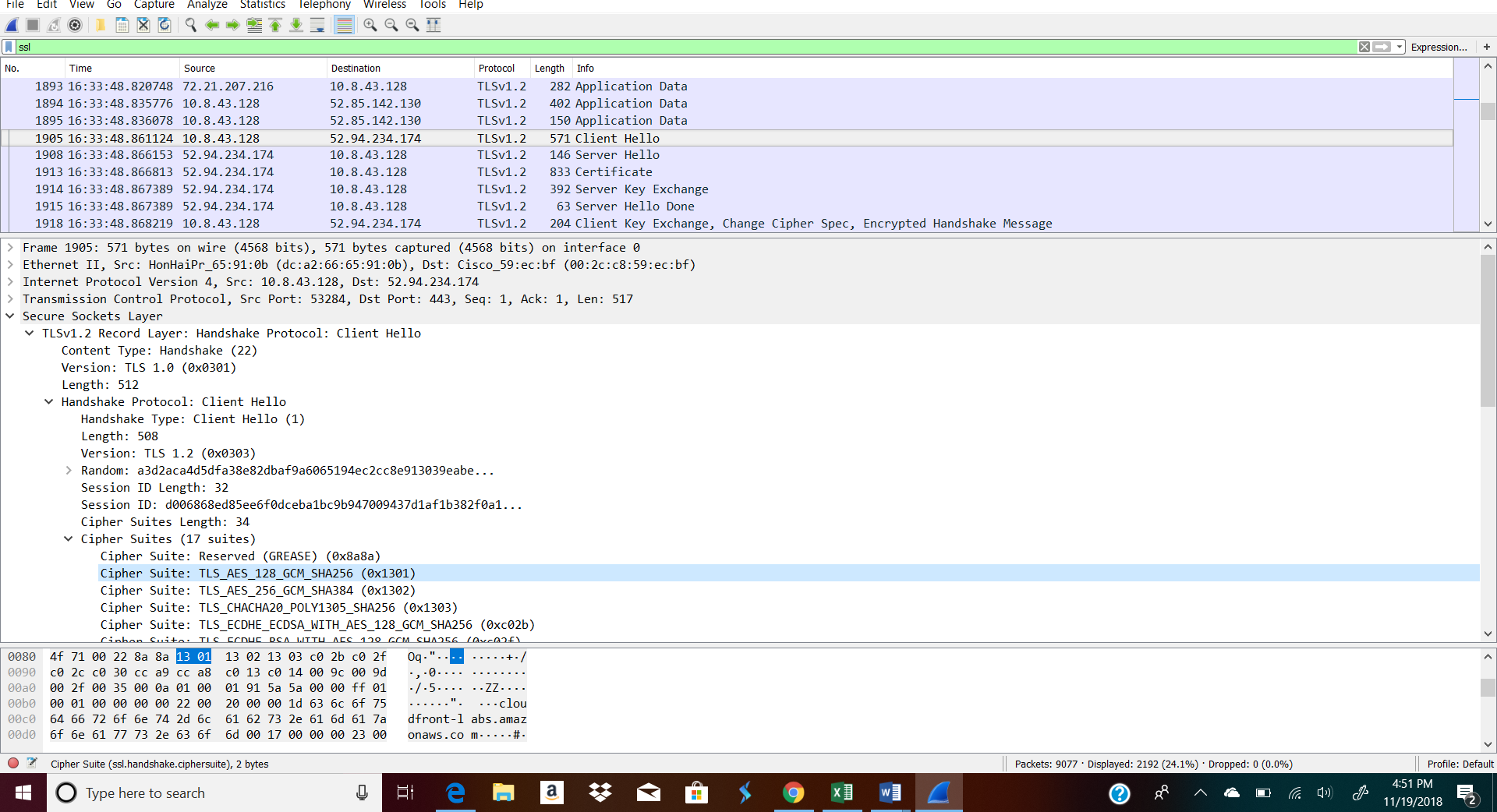
1. Does the ClientHello record contain a nonce (also known as a “challenge”)? If so, what is the value of the challenge in hexadecimal notation?

A3:d2:ac:a4:d5:df:a3:8e:82:db:af:9a:60:65:19:4e:c2:cc:8e:91:30:39:ea:be:35:00:36:d7:dc:3b:78:33



1. 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?

The public key algorithm is GCM. The symmetric key algorithm is AES. The hash algorithm is SHA256



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

Cipher Suite: TLS\_ECDHE\_RRSA\_WITH\_AES\_128\_CBC\_SHA

