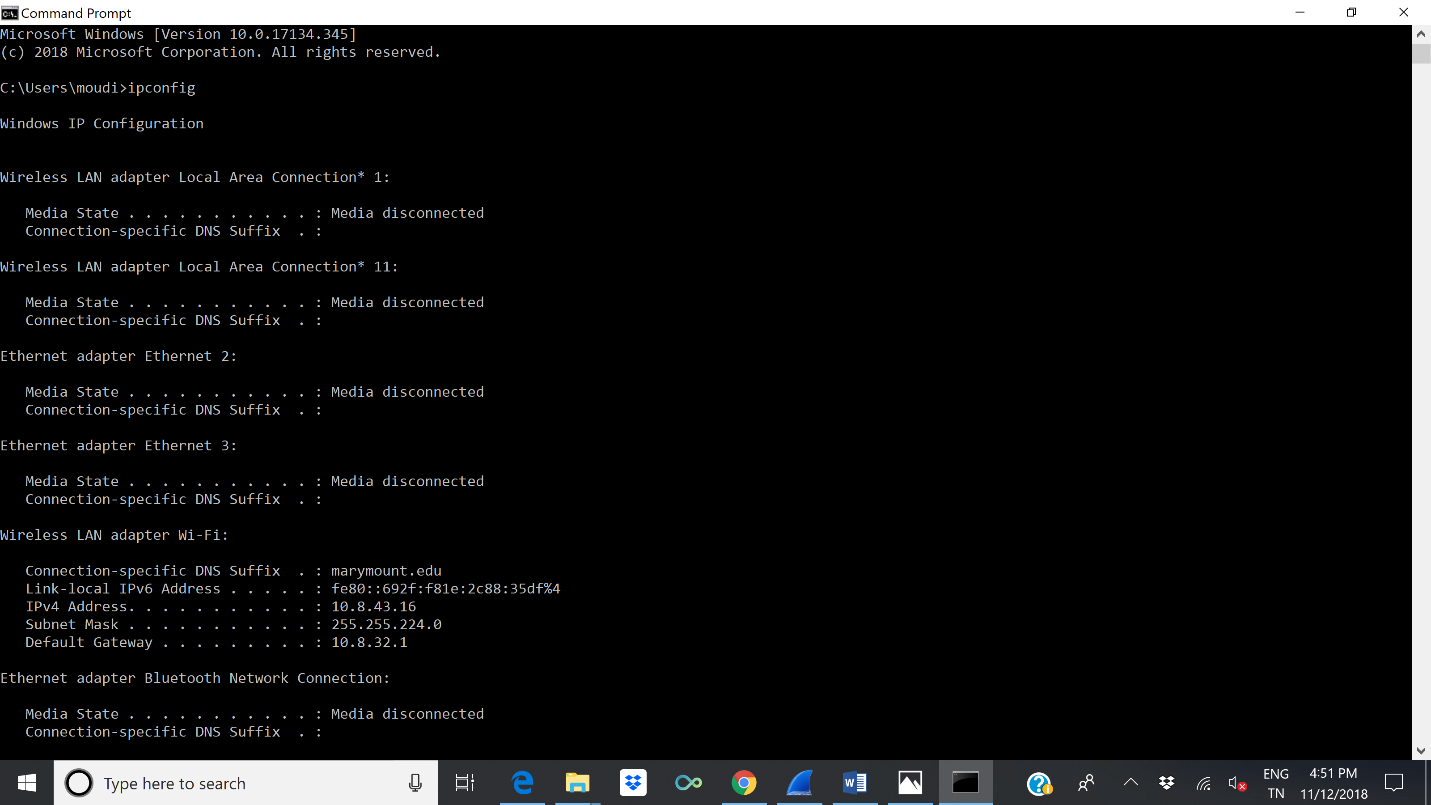
Moudie Alhousainan

Lab 8 – SSL/TLS IT 520-A – Enterprise Infrastructure & Networks Due Date: 11/12/18 (Handed in at the beginning of class)

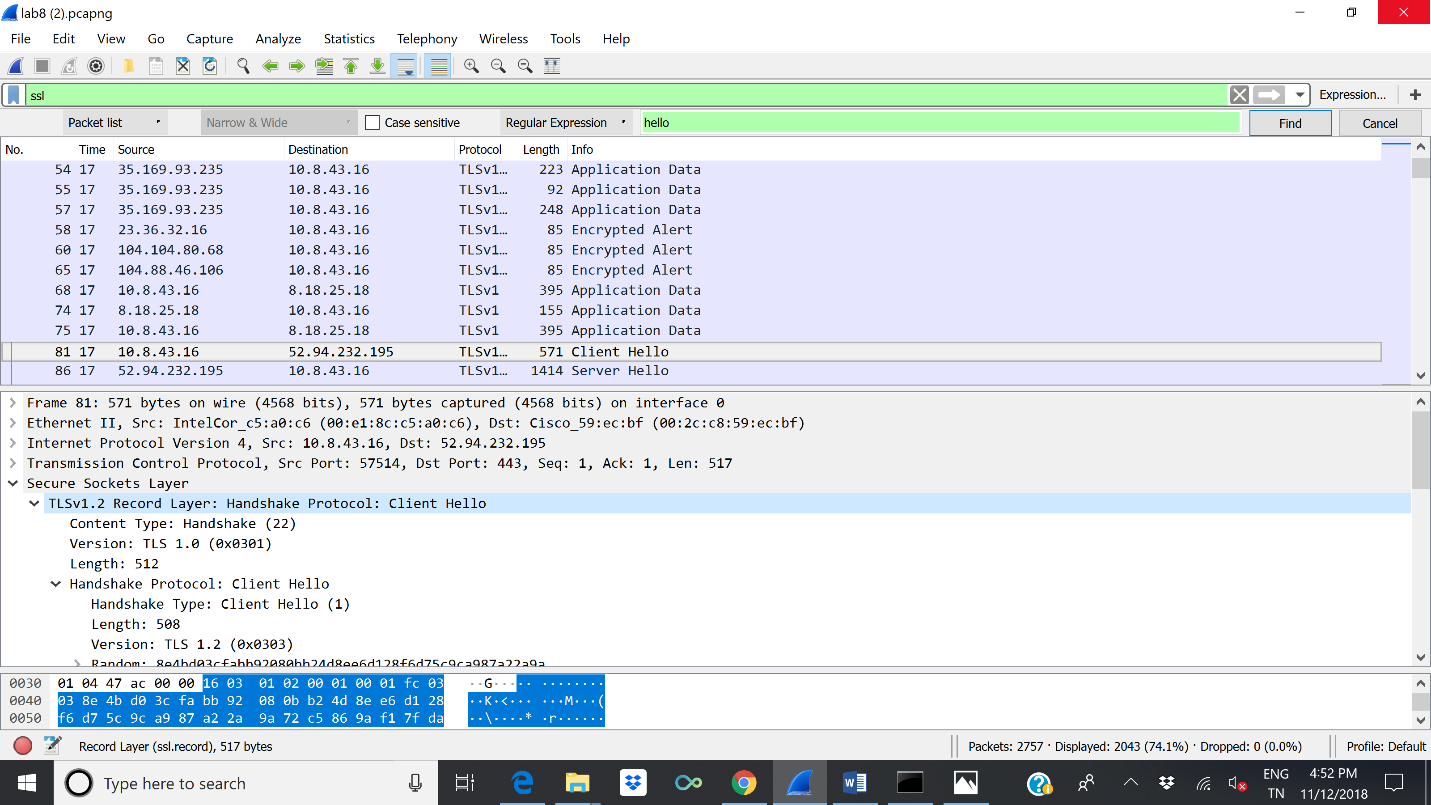
Questions:



Client Hello Record:

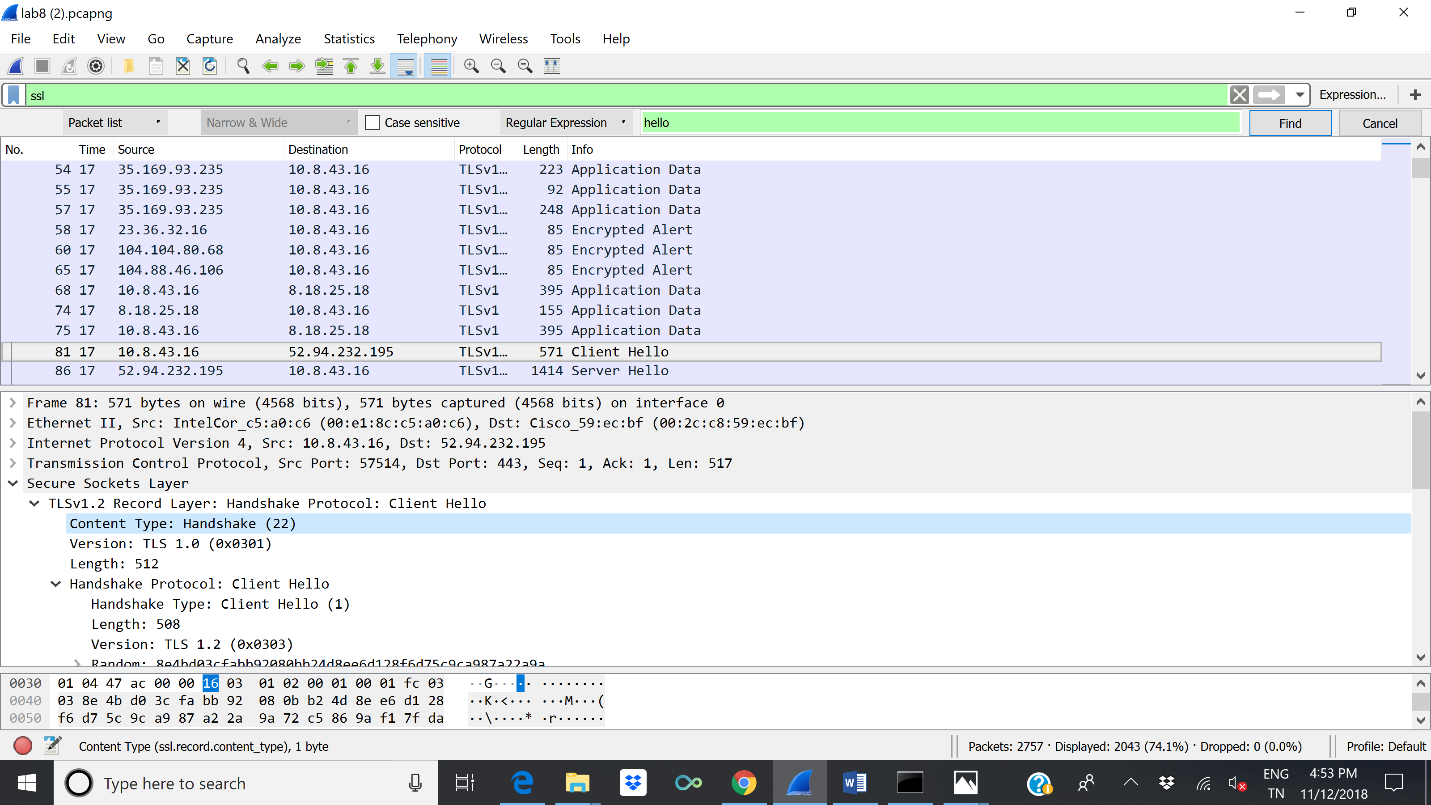
1. What is the SSL/TLS version of the of the Client Hello frame?

the SSL/TLS version :1.2



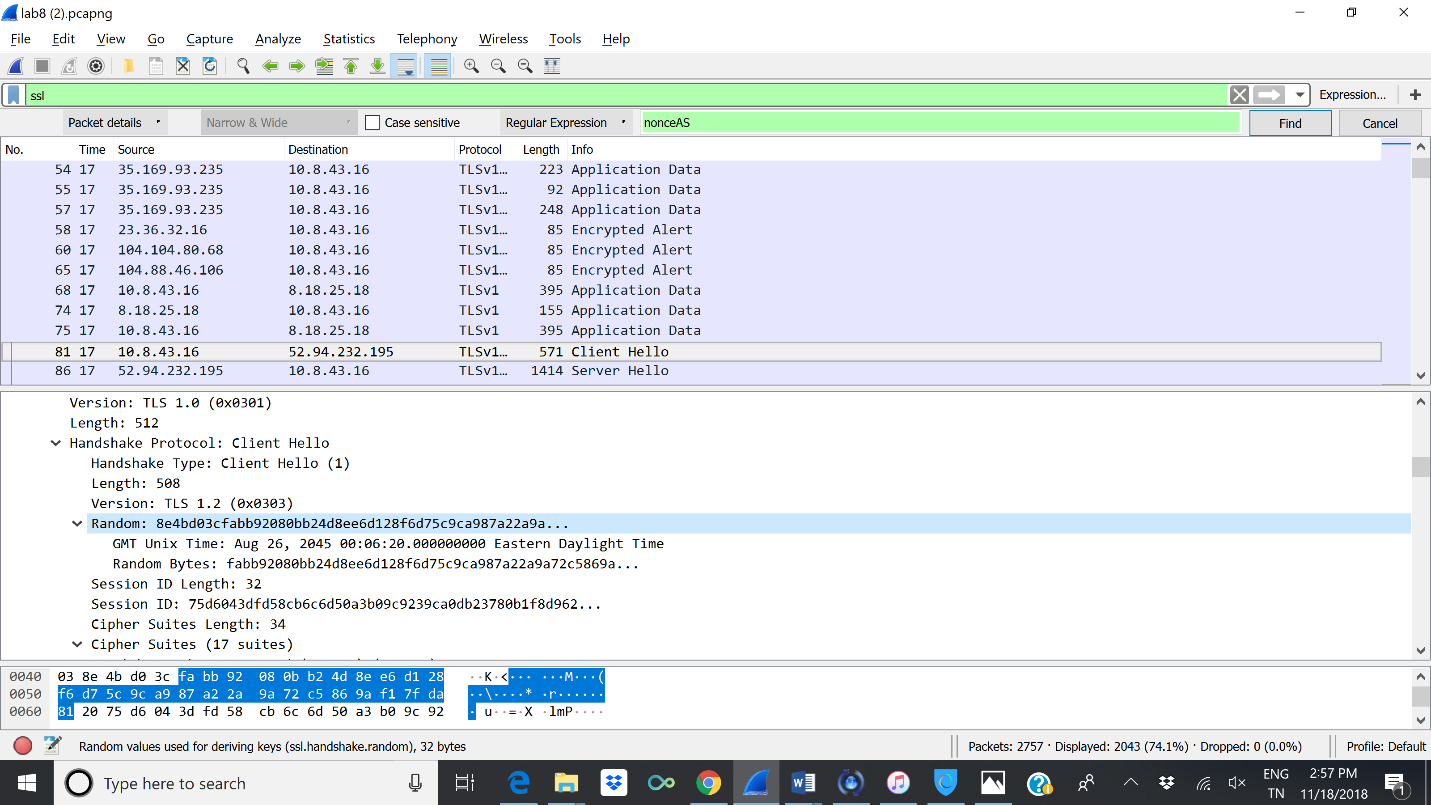
1. Expand the ClientHello record. (If your trace contains multiple ClientHello records, expand the frame that contains the first one.) What is the value of the content type?

The value is 22 handshake



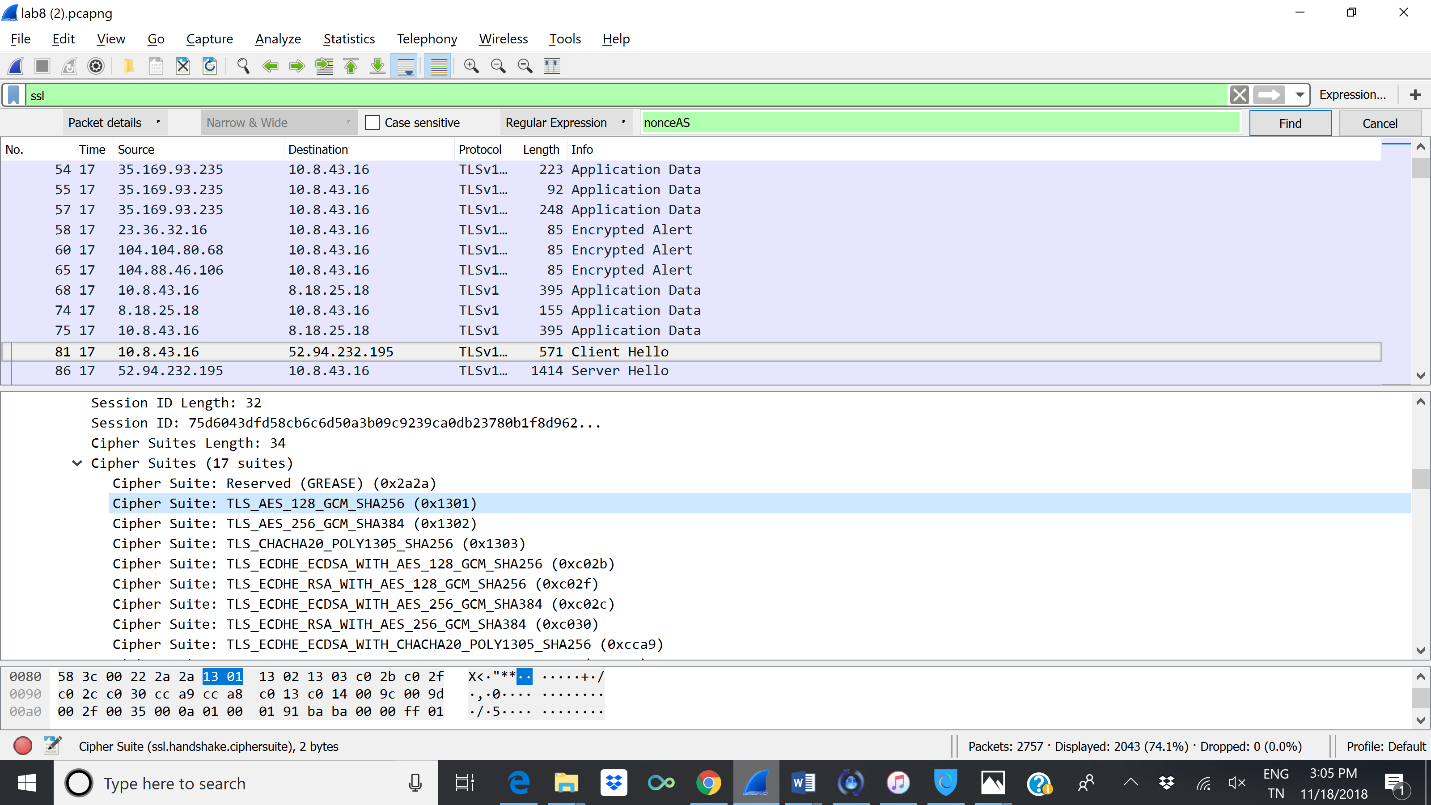
1. Does the ClientHello record contain a nonce (also known as a “challenge”)? If so, what is the value of the challenge in hexadecimal notation?

Random 8e4bd03cfabb92080bb24d8ee6d128f6d75c9ca987a22a9a72c5869af17fda81



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 AES , the symmetric-key algorithm GCM, and the hash algorithm SHA



Server Hello Record:

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

the public-key algorithm ECDHE-RSA , the symmetric-key algorithm AES, and the hash algorithm GCM-SHA

