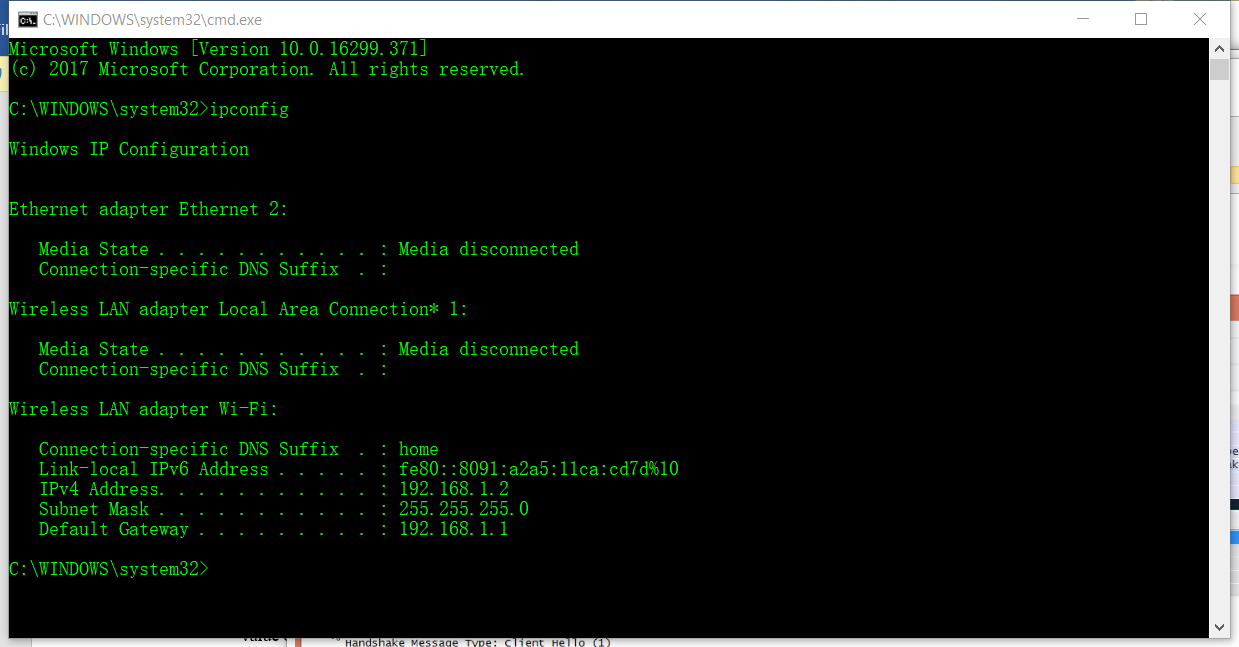
Wenjie Xu Lab 8

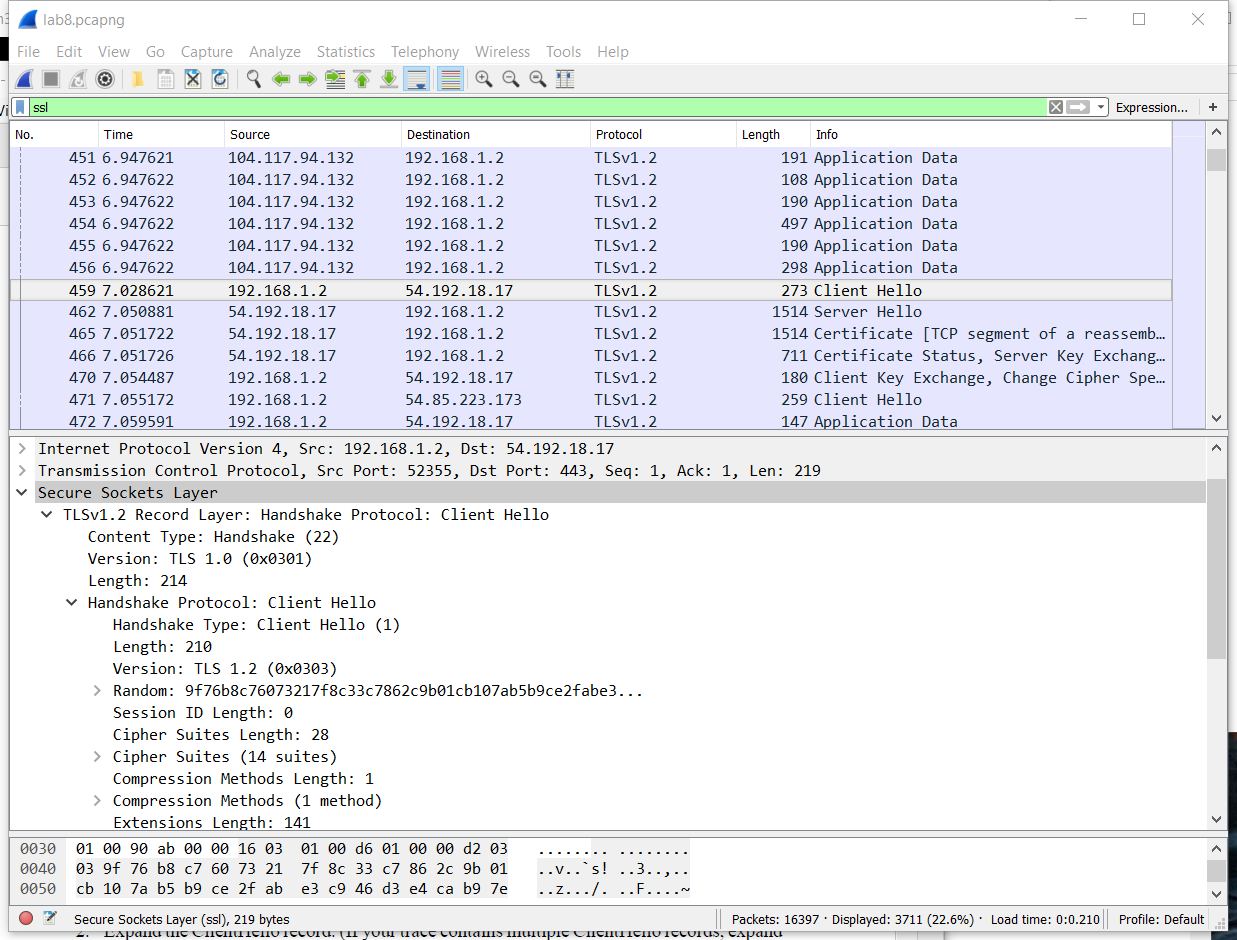
• My computer’s IP address is 192.168.1.2



Client Hello Record:

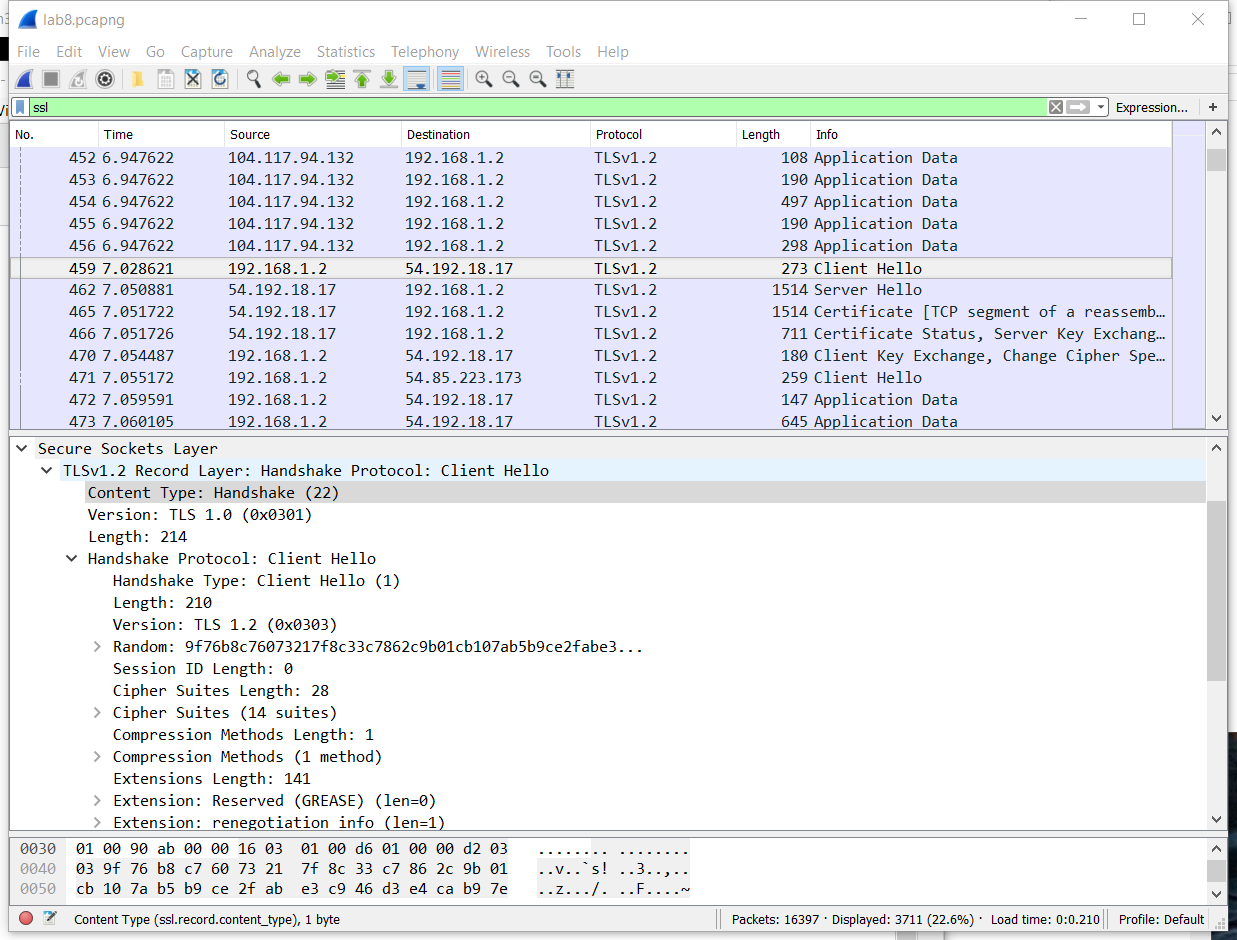
1. What is the SSL/TLS version of the of the Client Hello frame?

Answer: The SSL/TLS version of the ClientHello frame is TLS 1.2



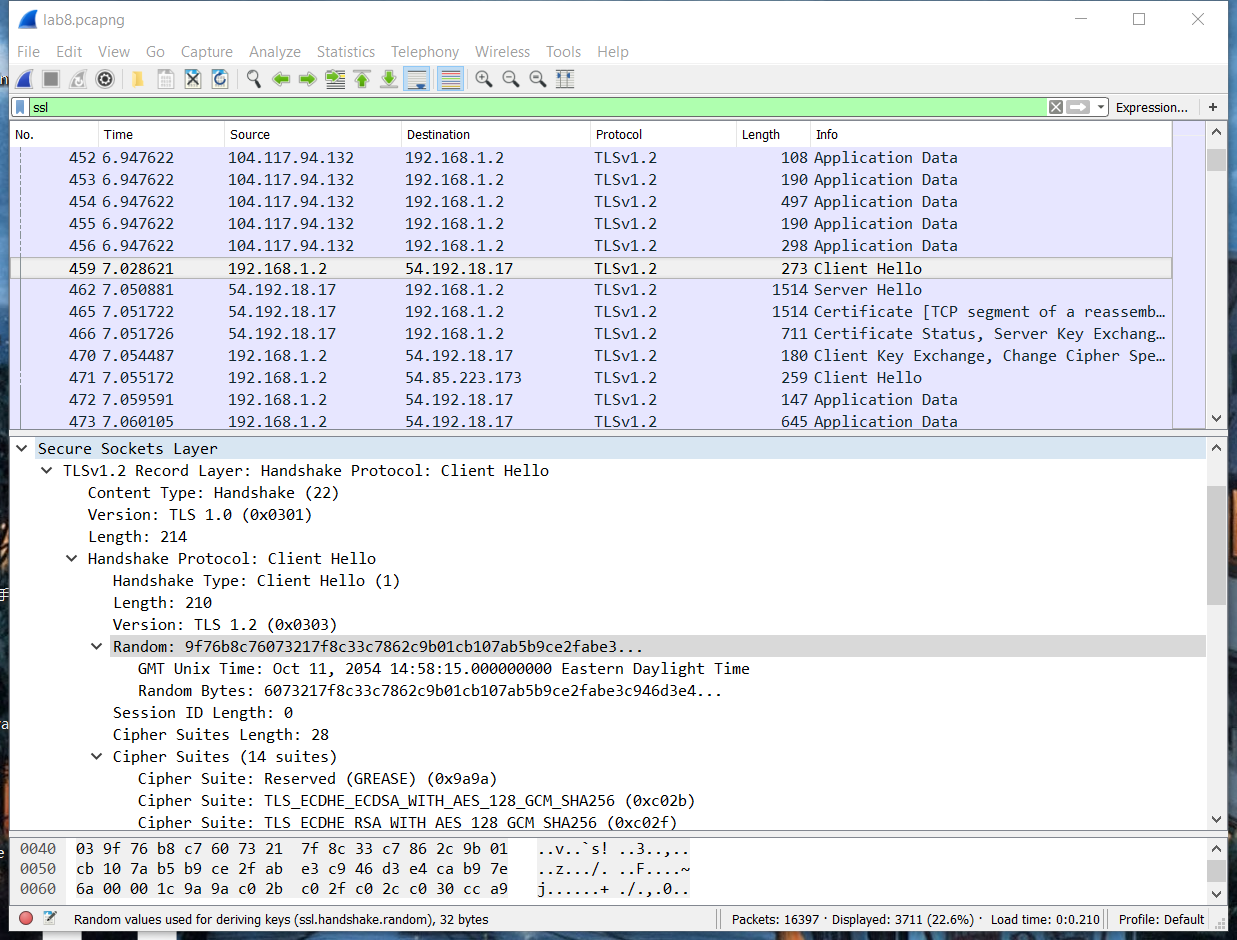
2. Expand the ClientHello record. (If your trace contains multiple ClientHello records, expand the frame that contains the first one.) What is the value of the content type?

Answer: The value of the content type is Handshake (22).



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

Answer: Yes, the record contains a nonce. The value of the challenge is 9f:76:b8:c7:60:73:21:7f:8c:33:c7:86:2c:9b:01:cb:10:7a:b5:b9:ce:2f:ab:e3:c9:46:d3:e4:ca:b9:7e:6a



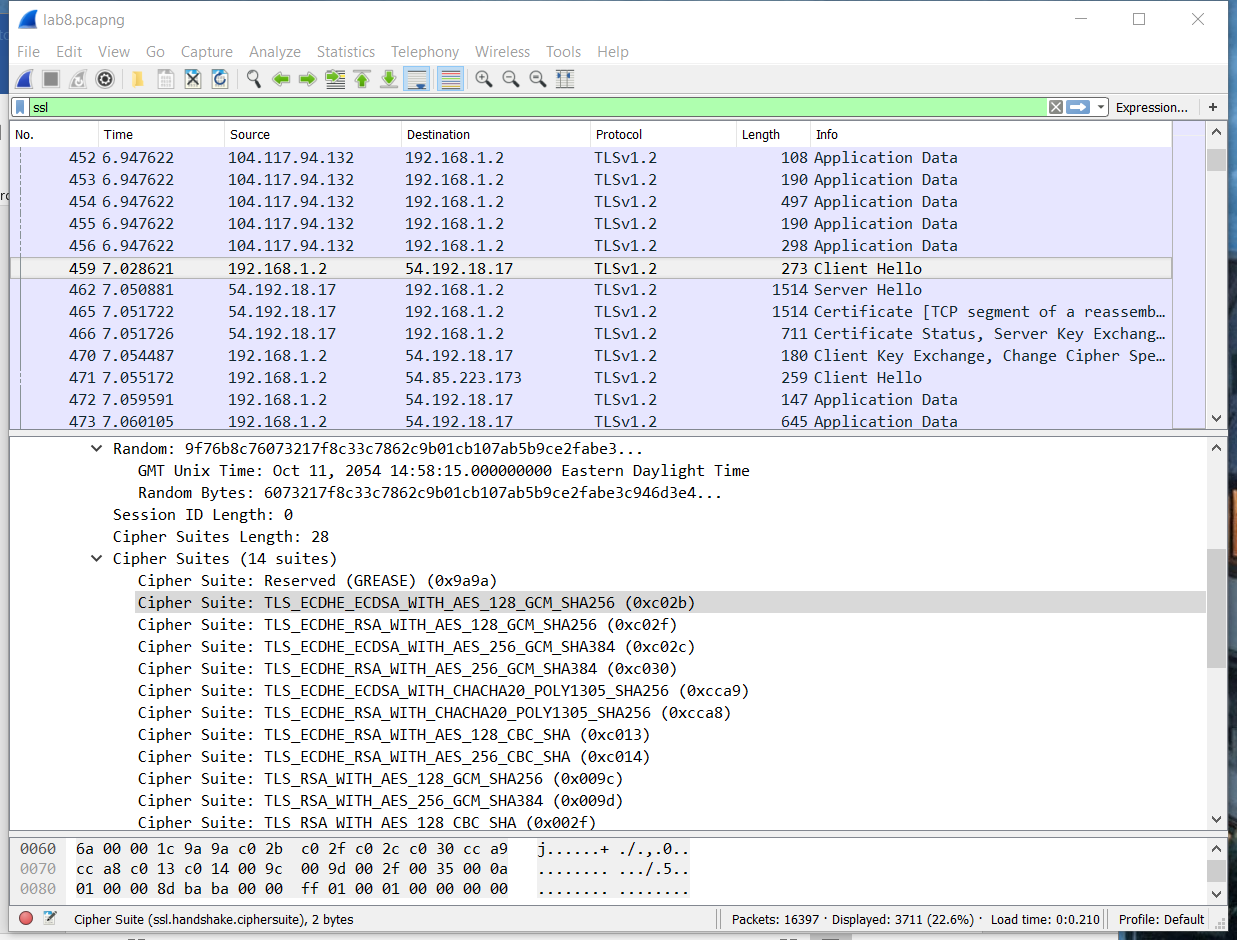
4. Does the ClientHello record advertise the cyber suites it supports? If so, in the first listed suite, what are the public-key algorithm, the symmetric-key algorithm, and the hash algorithm?

Answer: Yes, the ClientHello record advertises that the cipher suites it supports.

The public-key algorithm is ECDHE (Elliptic Curve Diffie-Hellman)

The symmetric-key algorithm is AES

The hash algorithm is 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?

Answer: Yes, the record specifies a chosen cipher suite.

The public-key algorithm is ECDHE (Elliptic Curve Diffie-Hellman)

The symmetric-key algorithm is AES

The hash algorithm is SHA

