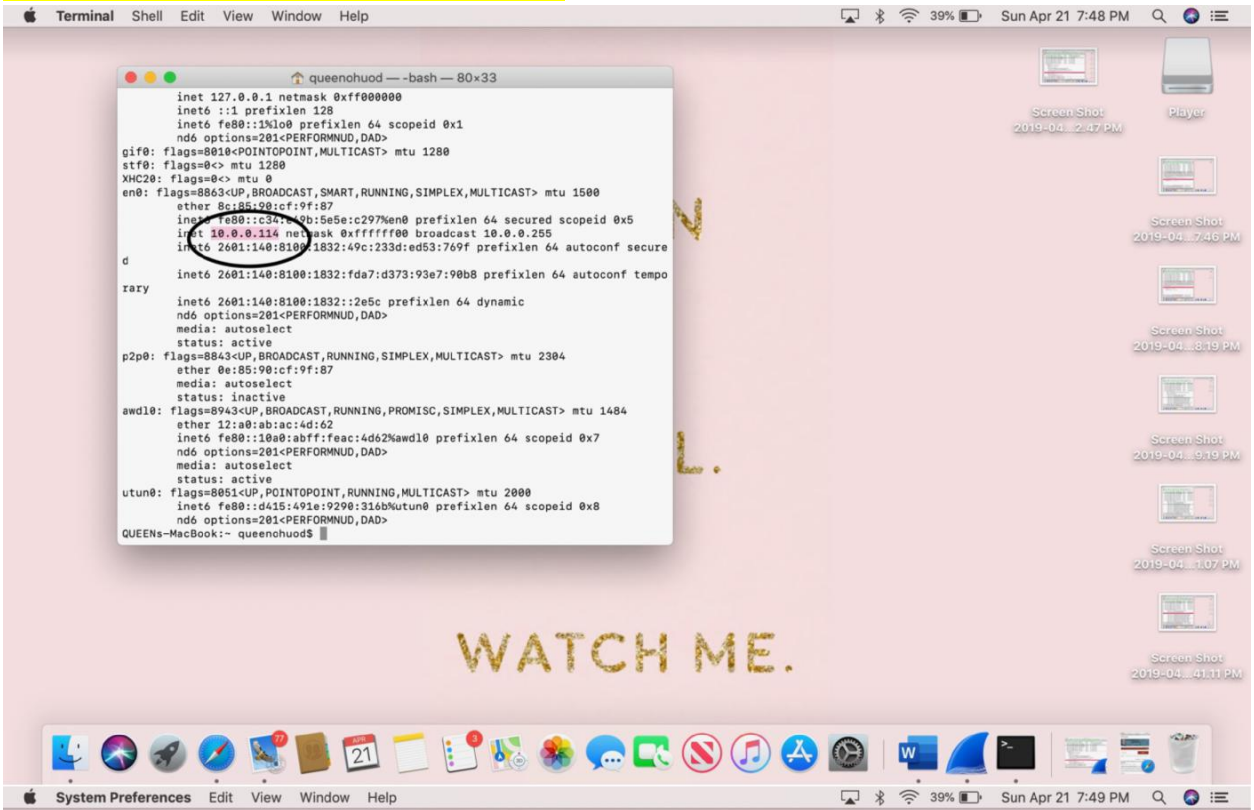
Enterprise Infrastructure & Networks

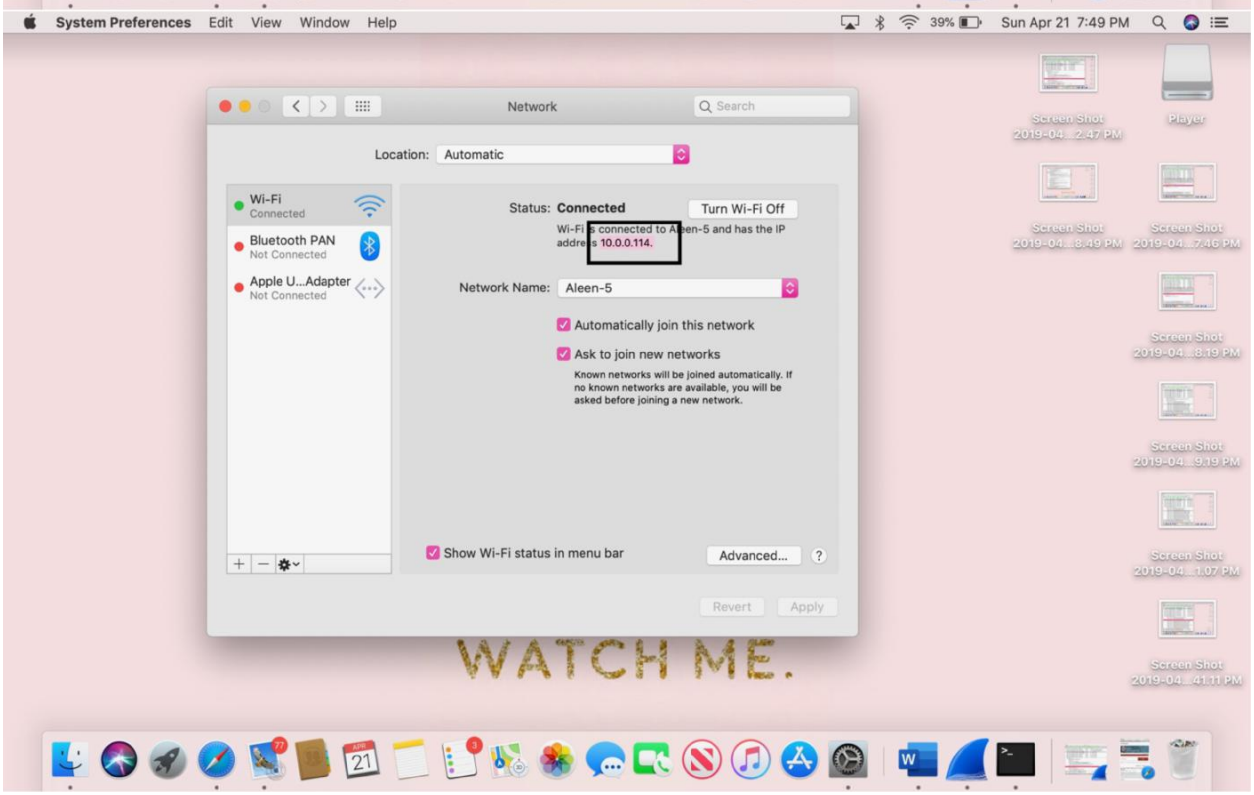
IT -520

Due to: April/23/2019

Ohuod Althiyabi

MY IP address is: 10.0.0.114



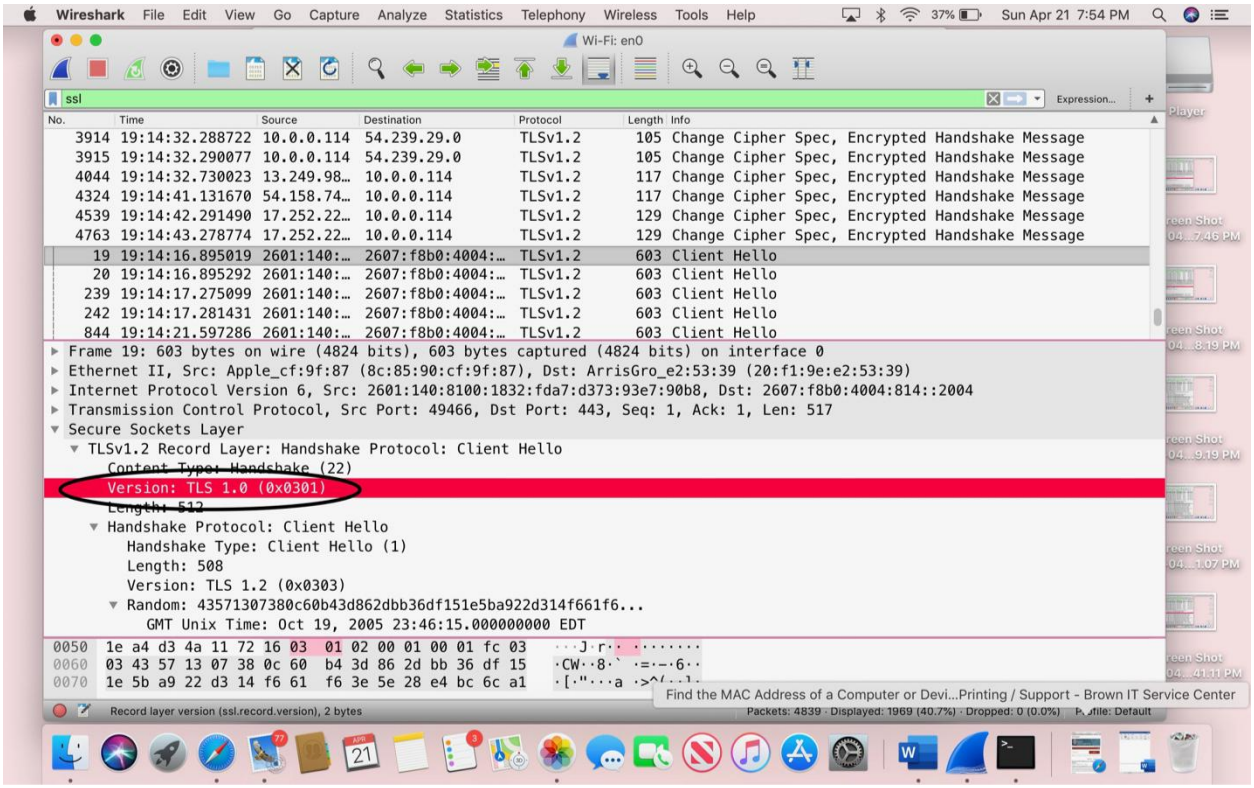


Questions:

1. Client Hello Record:

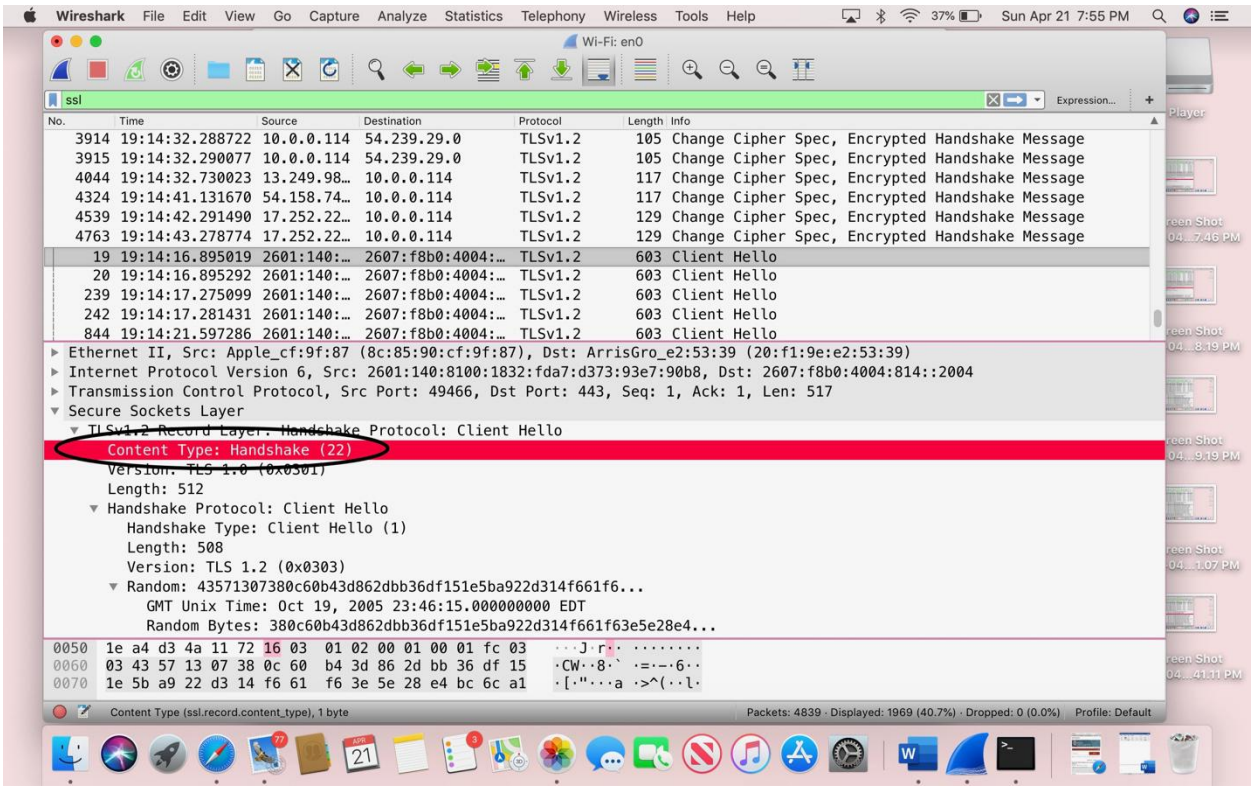
- What is the SSL/TLS version of the of the Client Hello frame?

It is TLS 1.0(0*0301)



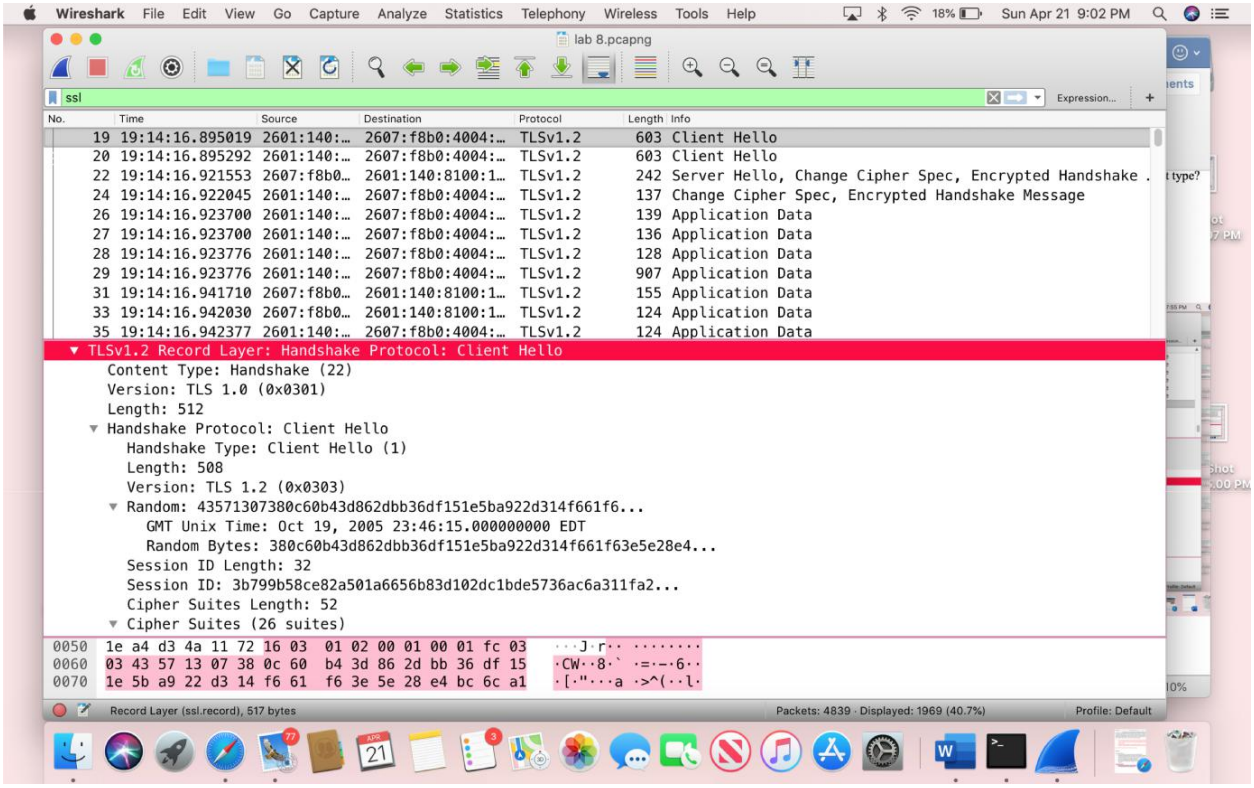
- Expand the ClientHello record. (If your trace contains multiple ClientHello records, expand the frame that contains the first one.) What is the value of the content type?

  The content type: Handshake (22)



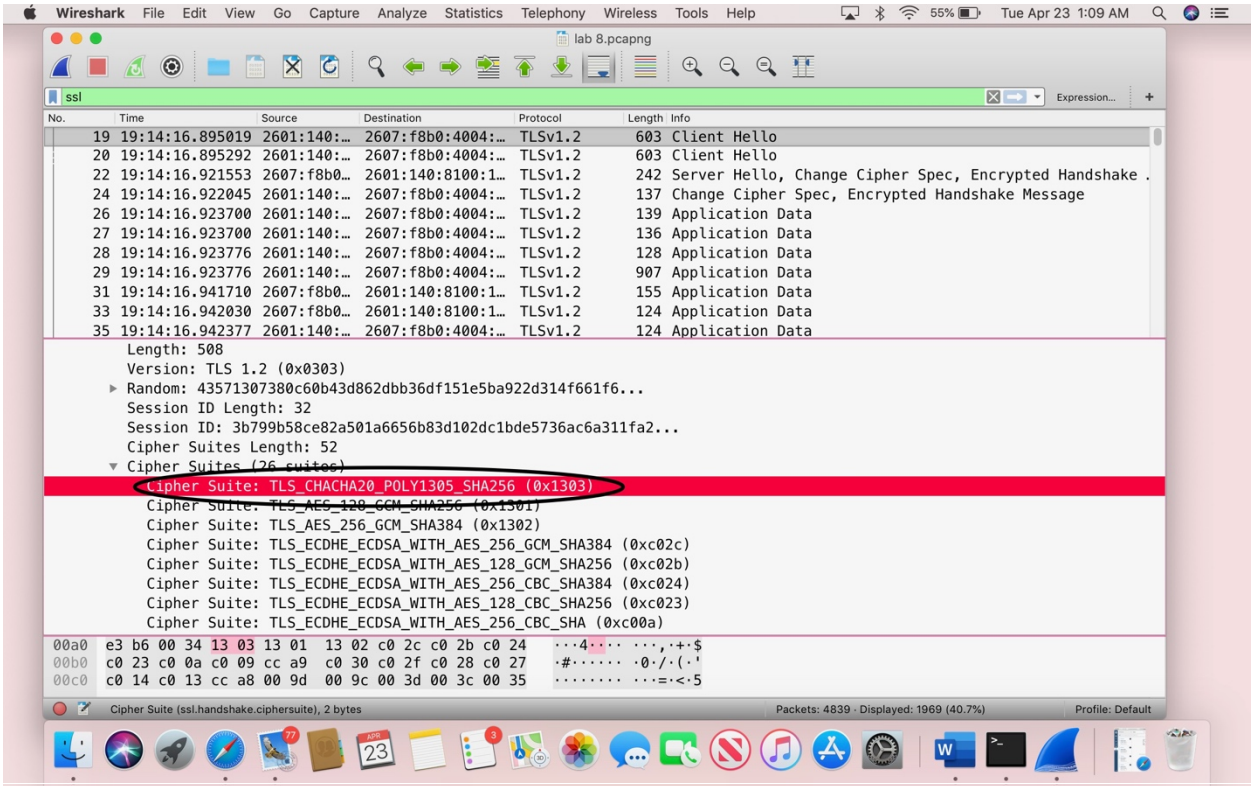
- Does the ClientHello record contain a nonce (also known as a "challenge")? If so, what is the value of the challenge in hexadecimal notation?

No,



- Does the Client Hello 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 CHACHA20
- The symmetric-key algorithm is POLY1305
- The hash algorithm is SHA256



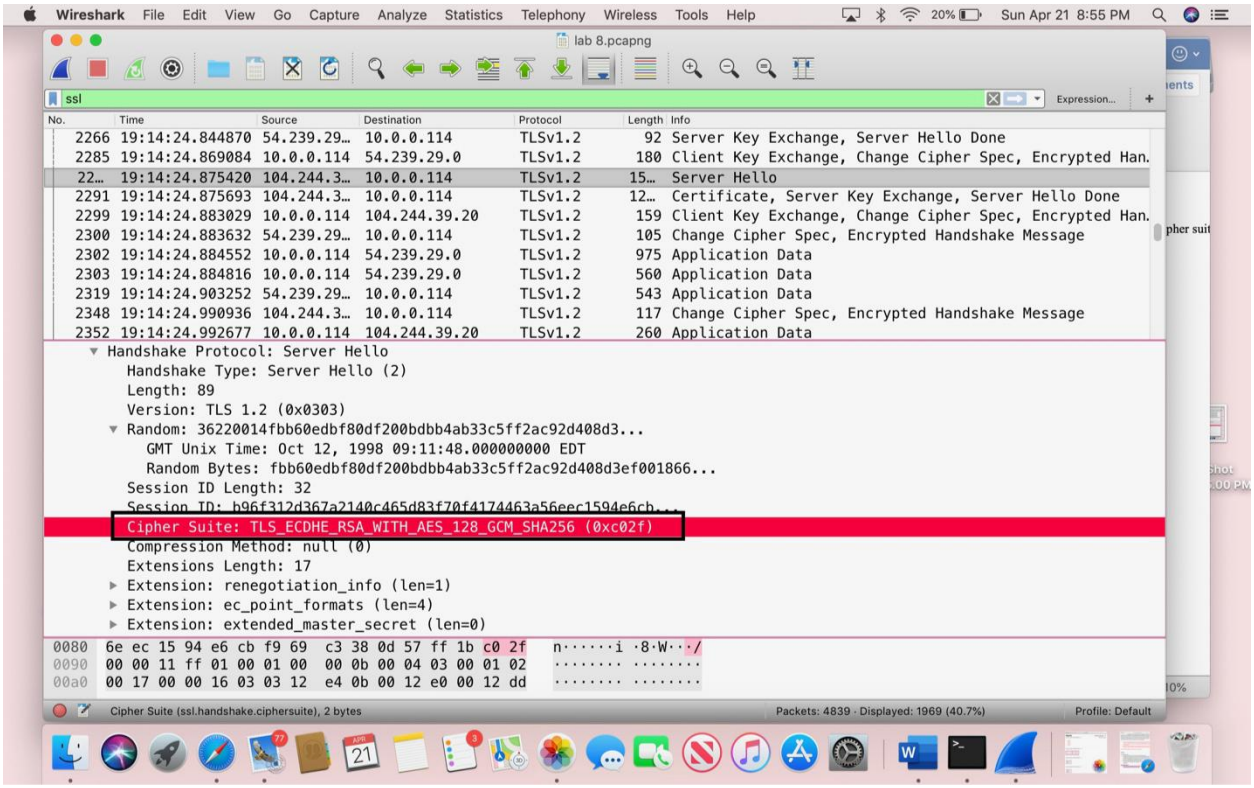
2. Server Hello Record:

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

YES

TLS_ECDHE_RSA

- The public-key algorithm is RSA
- The symmetric-key algorithm is GCM
- The hash algorithm is SHA256



I don’t find ok massage