ENTERPRISE INFRASTRUCTURE AND NETWORKS

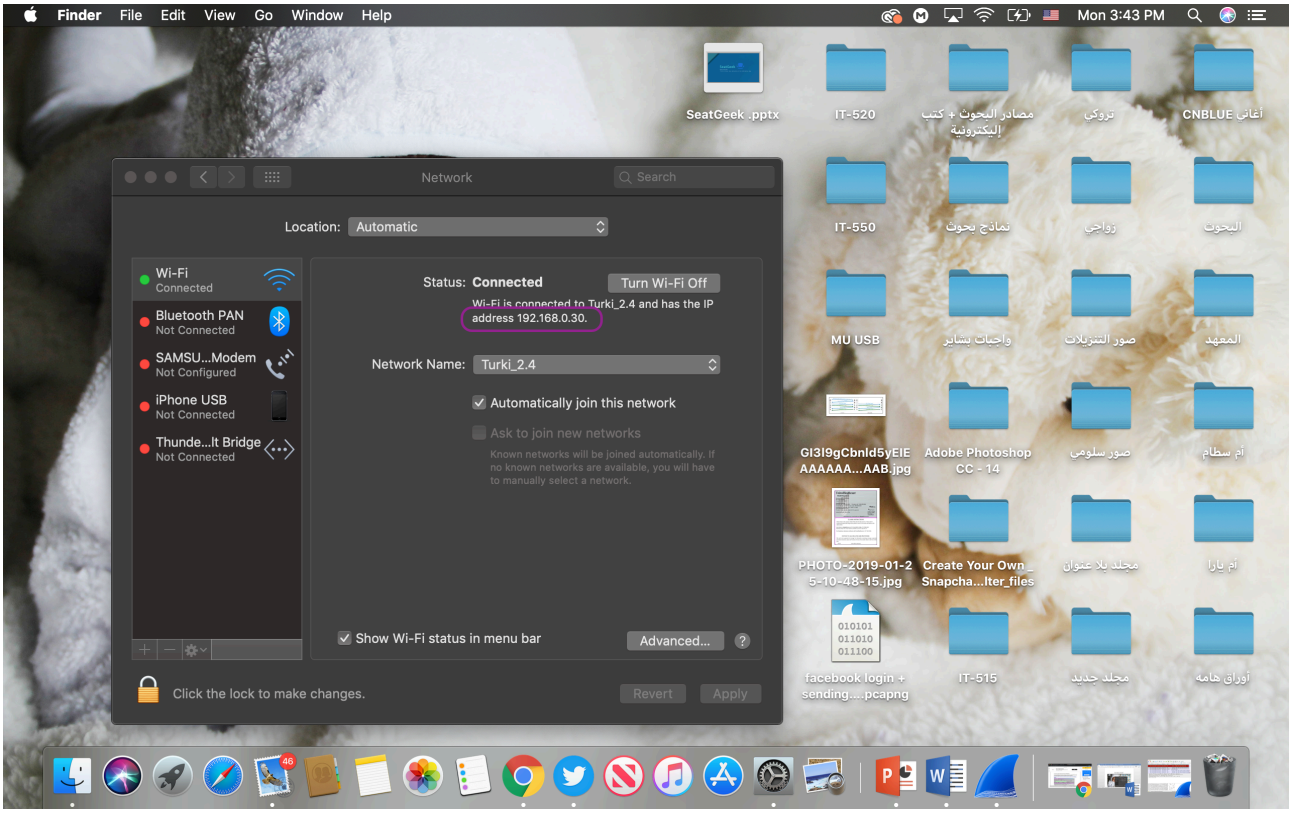
IT 520

Lab #8

Dalal Alshahil

Due to: 04/023/2019

My IP Address is : 192.168.0.30.

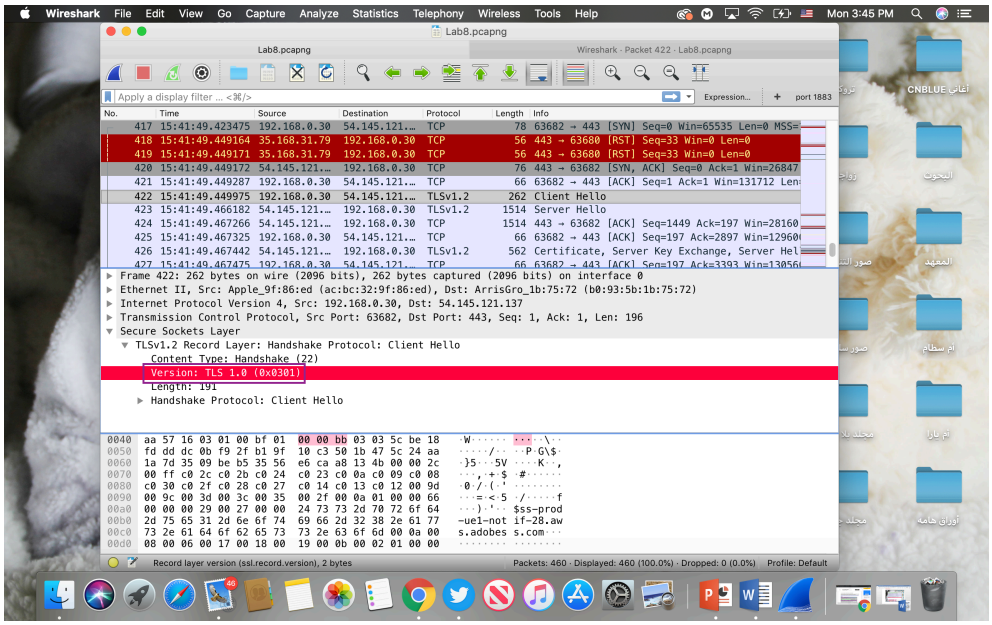


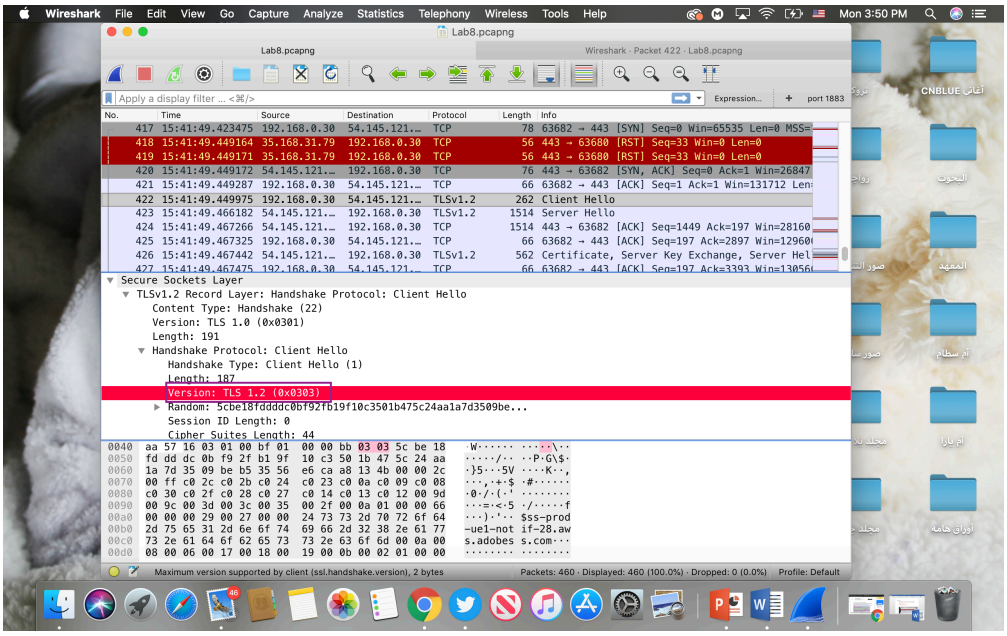
Question #1:

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

TLS version: 1.0

TLS version: 1.2

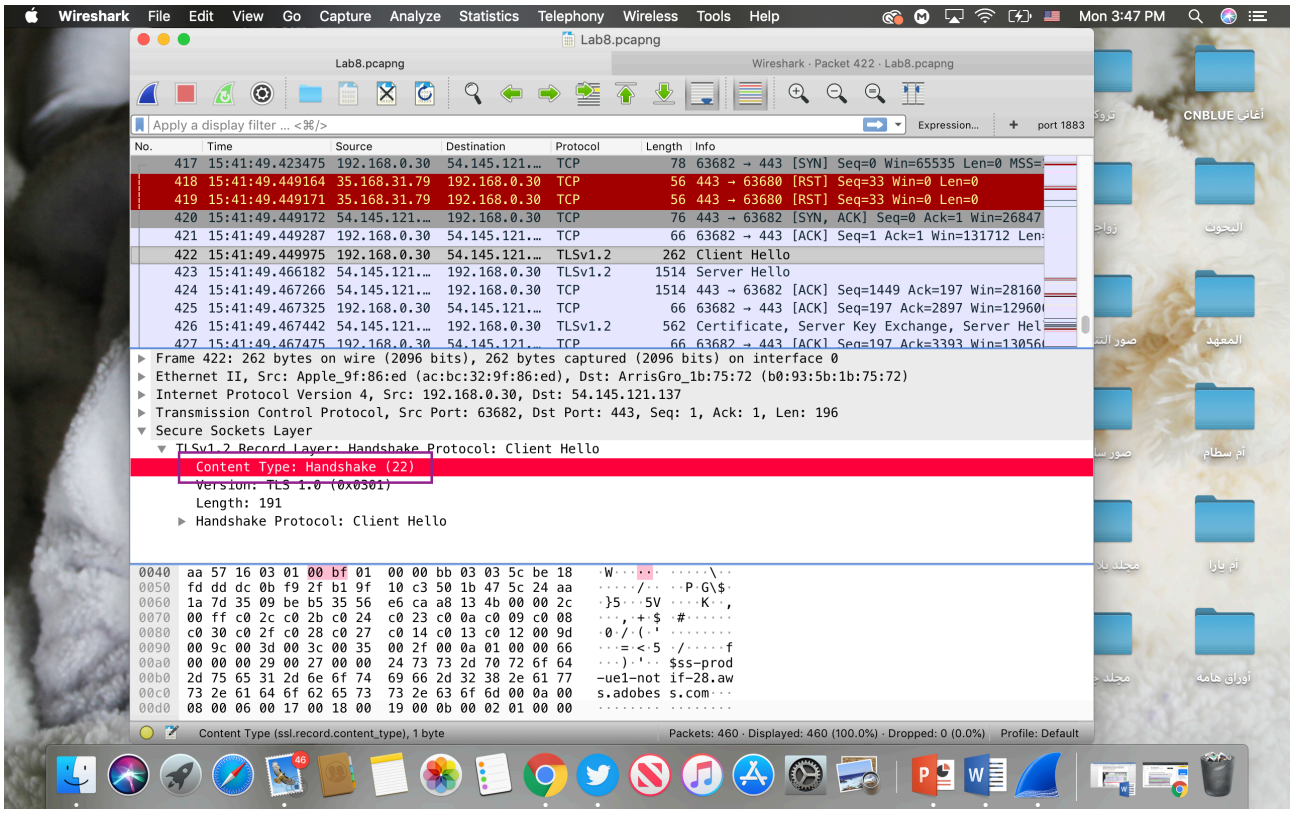




Question #2:

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?

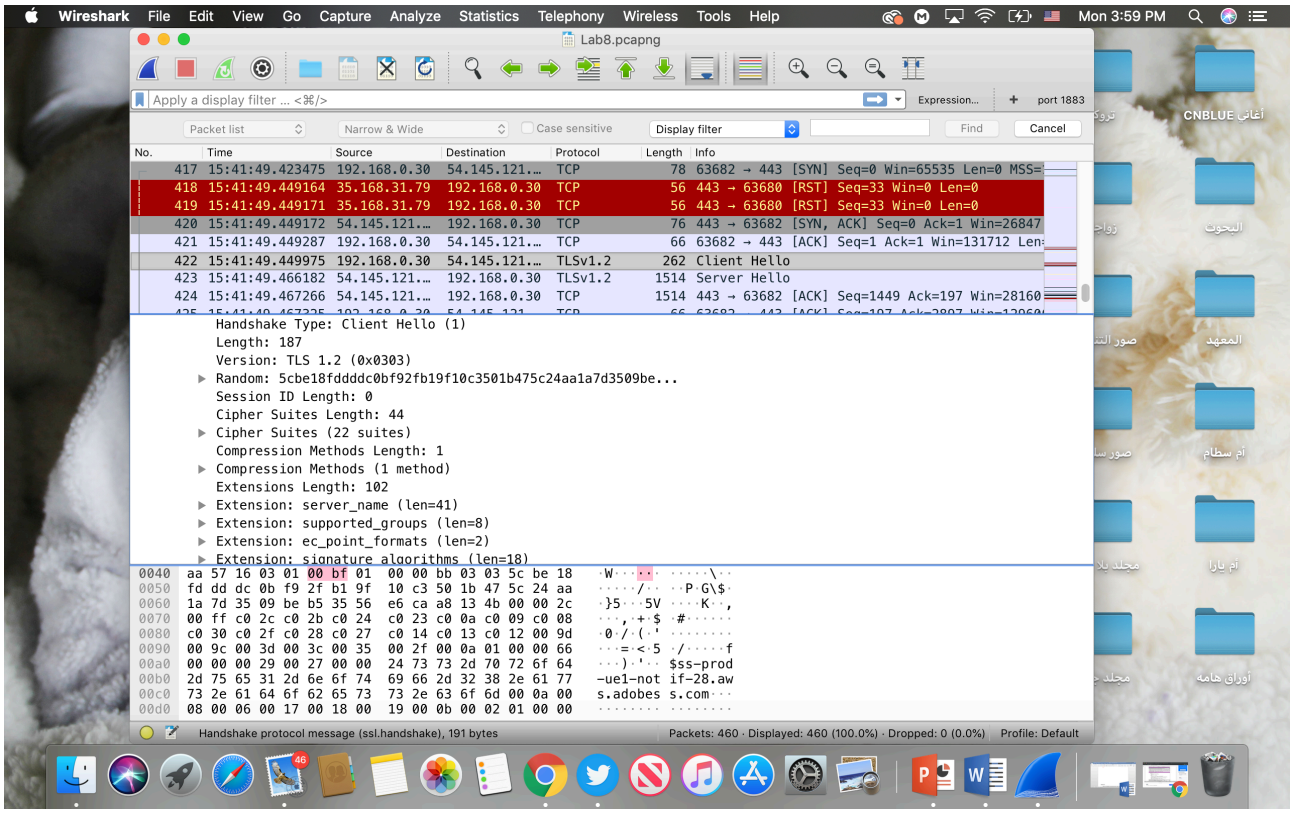
Content Type: Handshake (22)



Question #3:

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

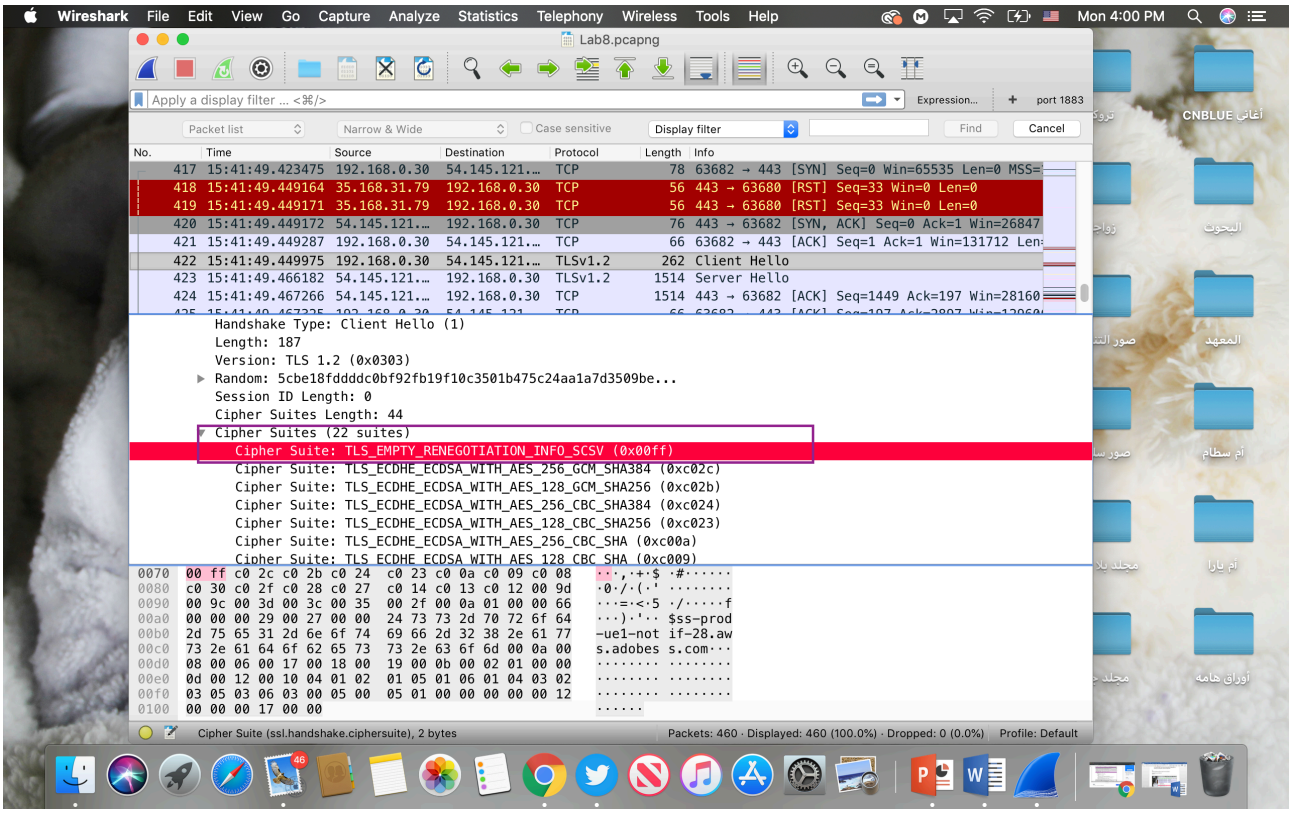
There is No Value of challenge.



Question #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?

Yes, The first suite uses EMPTY for public key crypto
RENEGOTIATION for the symmetric key cipher
and uses the SCSV hash algorithm.



Question #5:

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?

Yes, Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
The cipher suite uses RSA for public key crypto
AES for the symmetric key cipher
and uses the SHA256 hash algorithm.