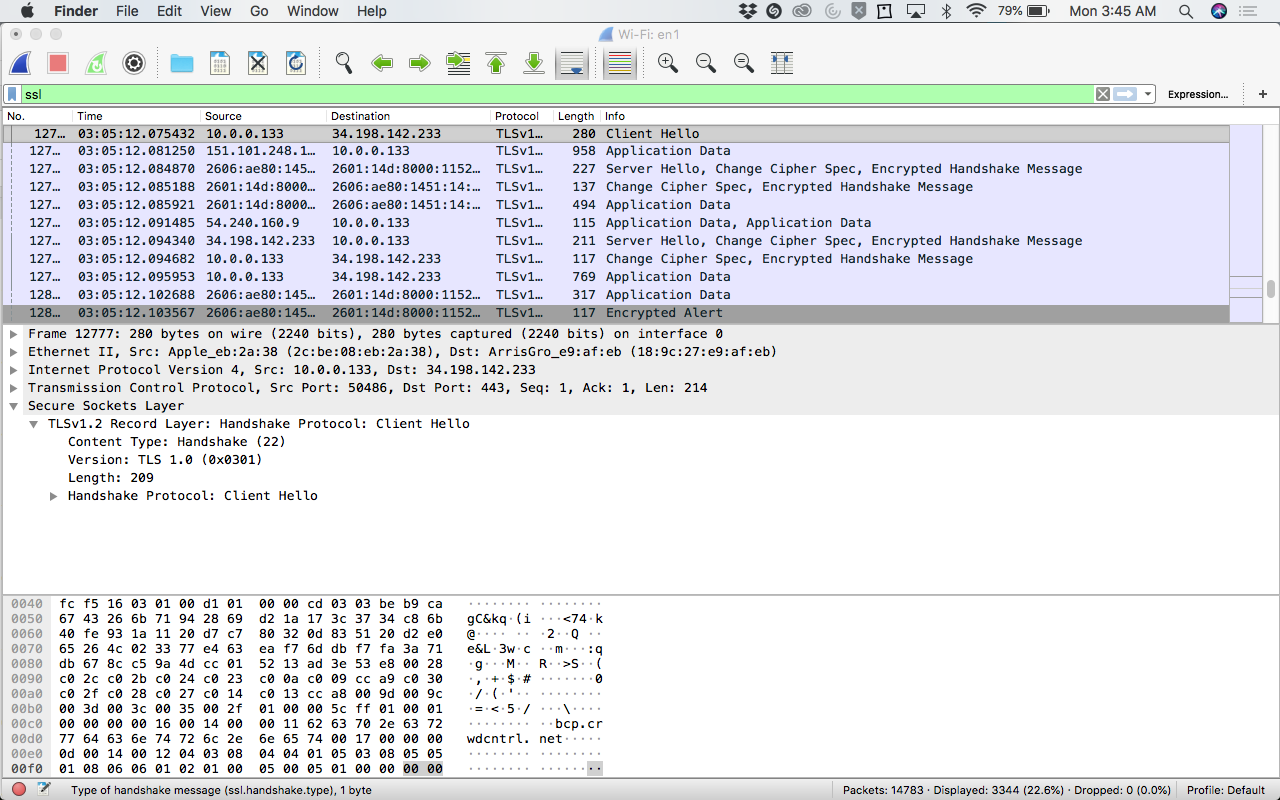
Kadijatu Bah

11/19/2018

Lab 8

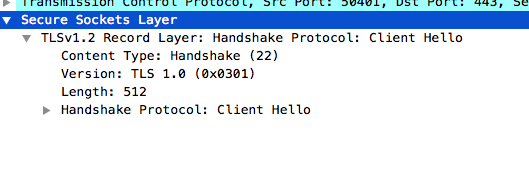


Questions:

Client Hello Record:

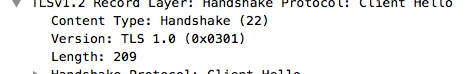
1. What is the SSL/TLS version of the of the Client Hello frame?

* ***TLS 1.0 (0x0301)***



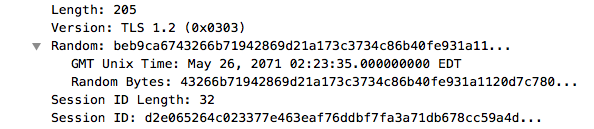
1. Expand the ClientHello record. (If your trace contains multiple ClientHello records, expand the frame that contains the first one.) What is the value of the content type?

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

******

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?

* ***Yes it does, it is be:b9:ca:67:43:26.***

******

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?

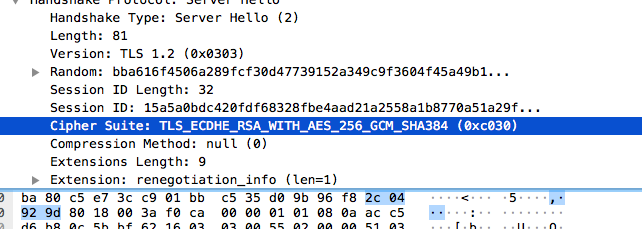
* ***Yes it does.***
* ***Public-key: ECDHE, ECDSAuki***
* ***Symmetric-key: AES(256), GCM, TLS***
* ***Hash: SHA-384***

******

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, the record specifies a chosen cipher suite.***
* ***The algorithms chosen are TLS, ECDHE, RSA, with AES 256, GCM, SHA384 (0x030).***

******