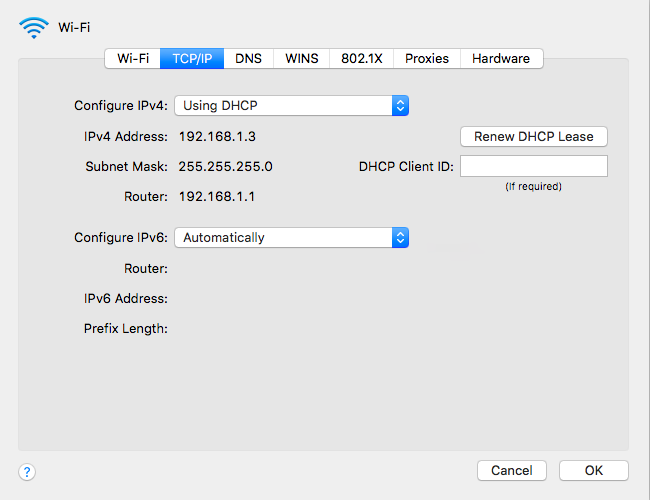
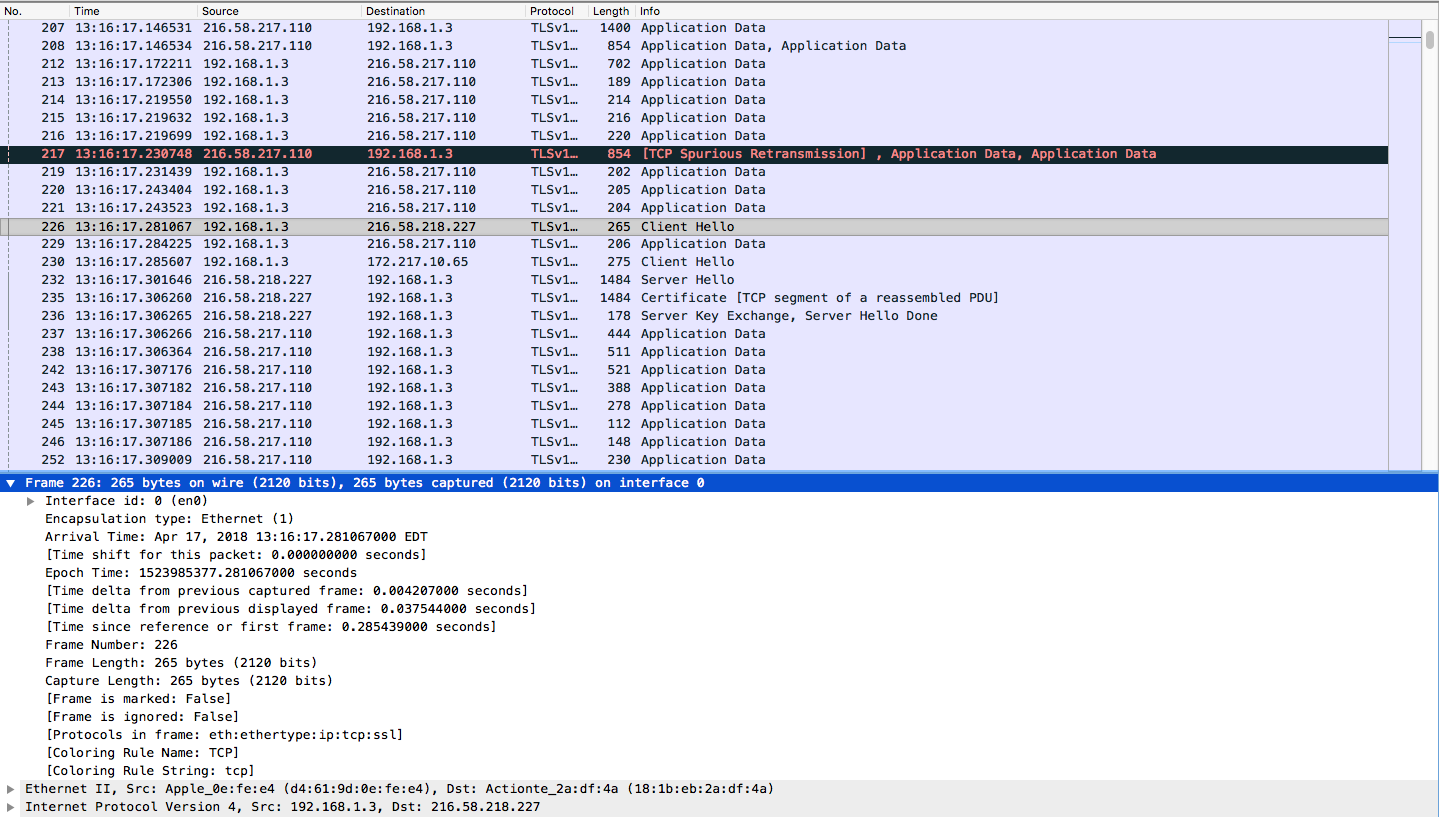
Name: Yohannes Woldegerima

Computer IP address screenshot

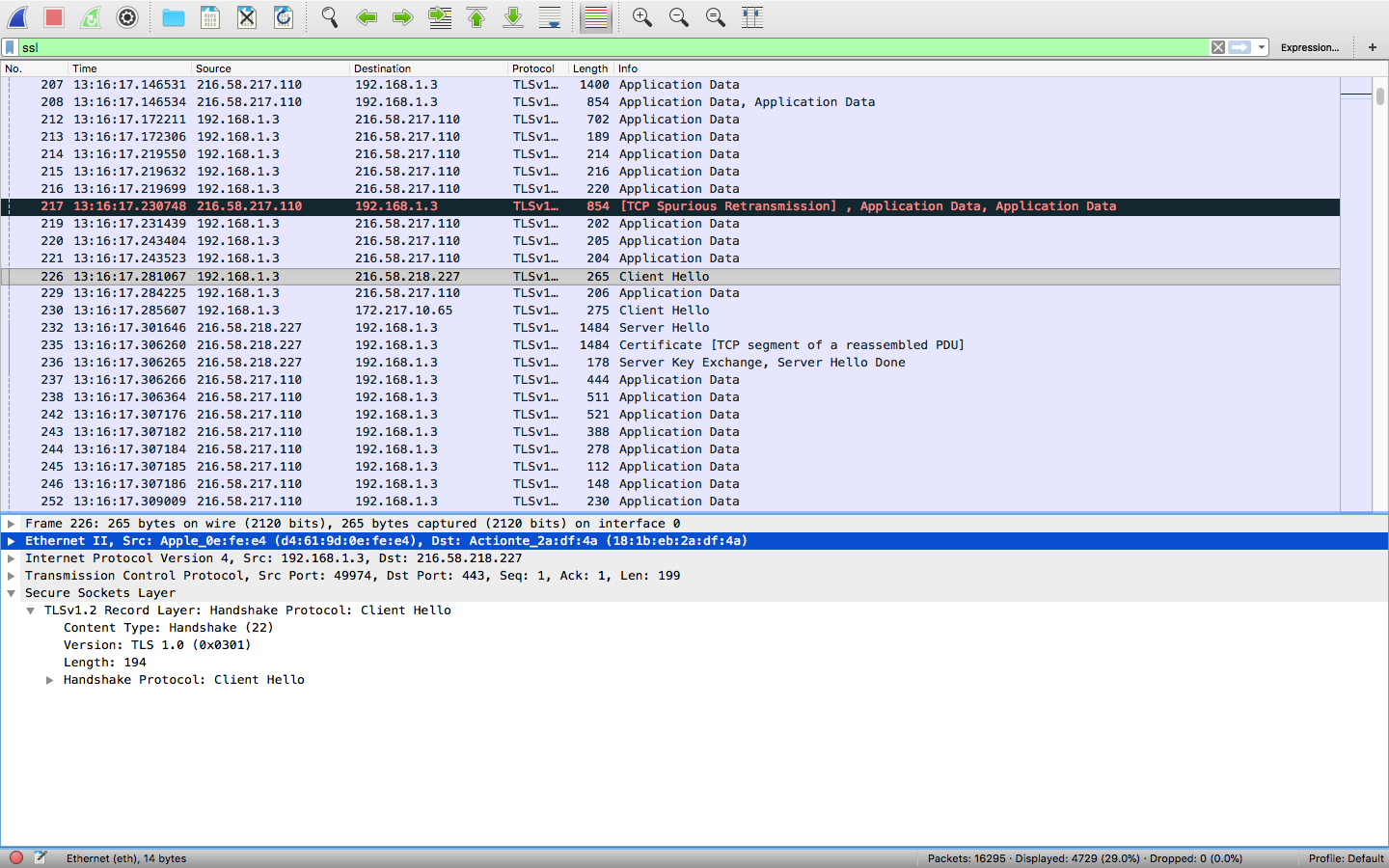


1. Client Hello Record: 1. What is the SSL/TLS version of the of the Client Hello frame?



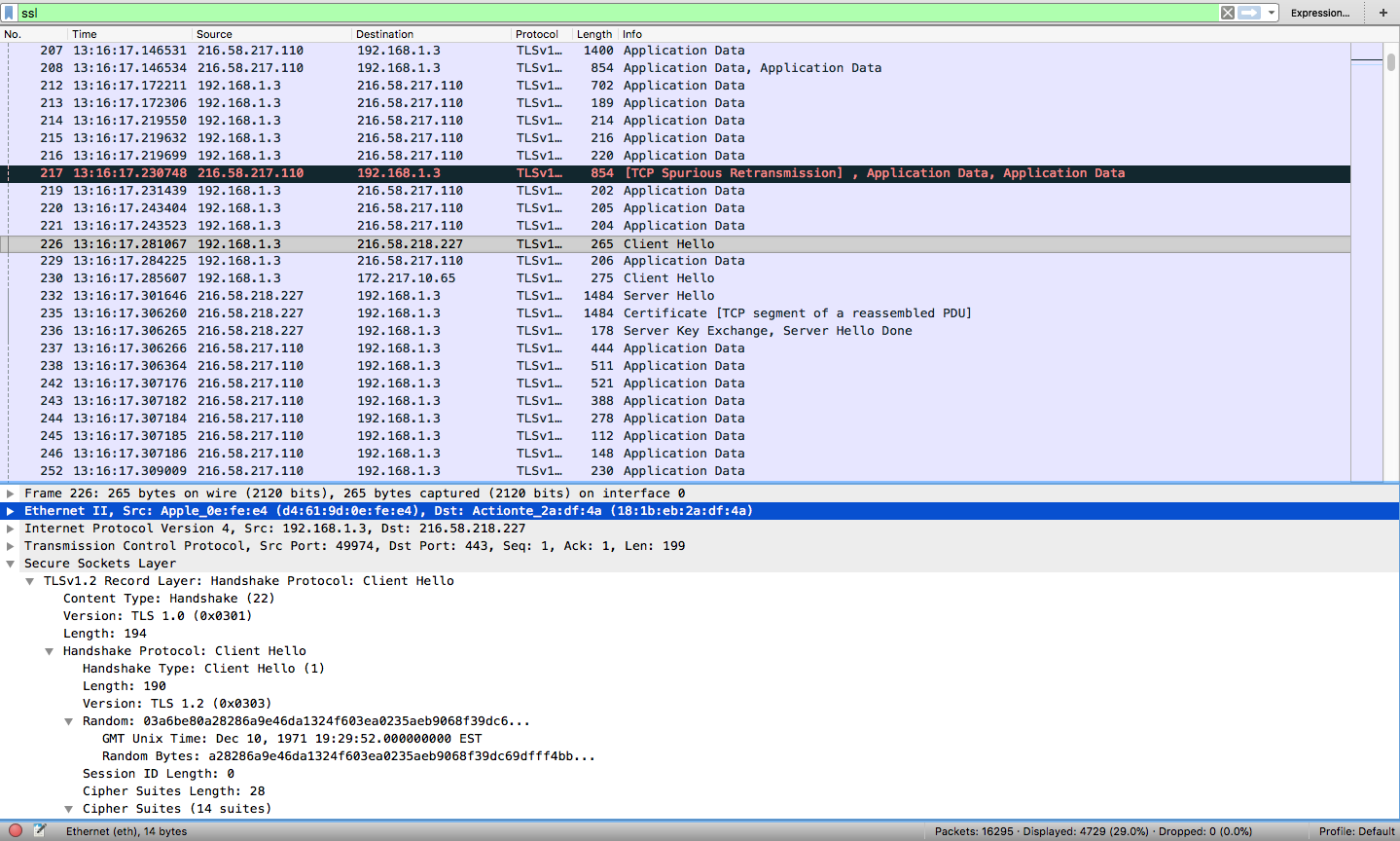
The frame is 226 and has a protocol of TCP

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



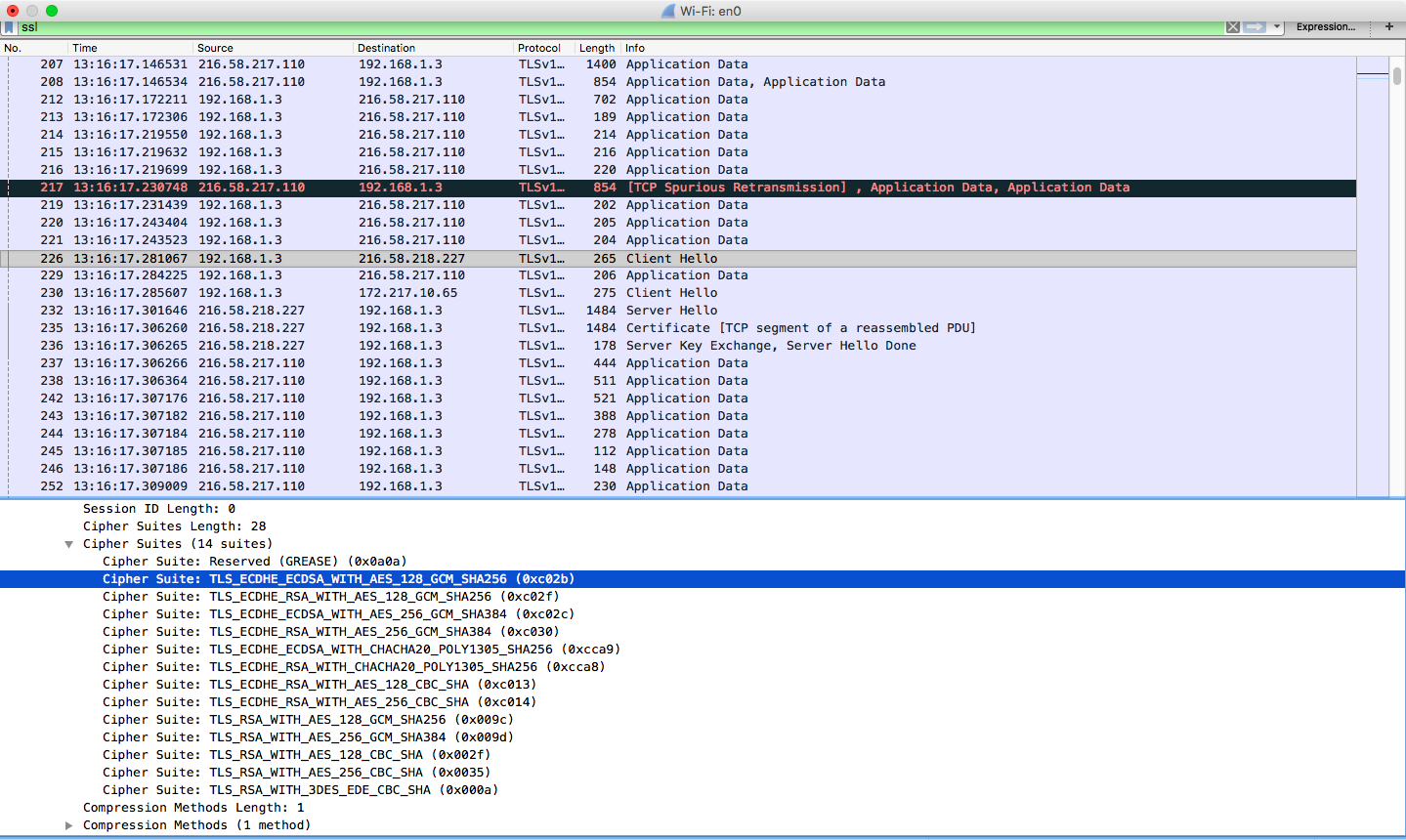
The Content Type is Handshake and value is 22

1. 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?



It Doesn’t contain a nonce

1. 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 first cipher suit listed is Reserved (Grease) but

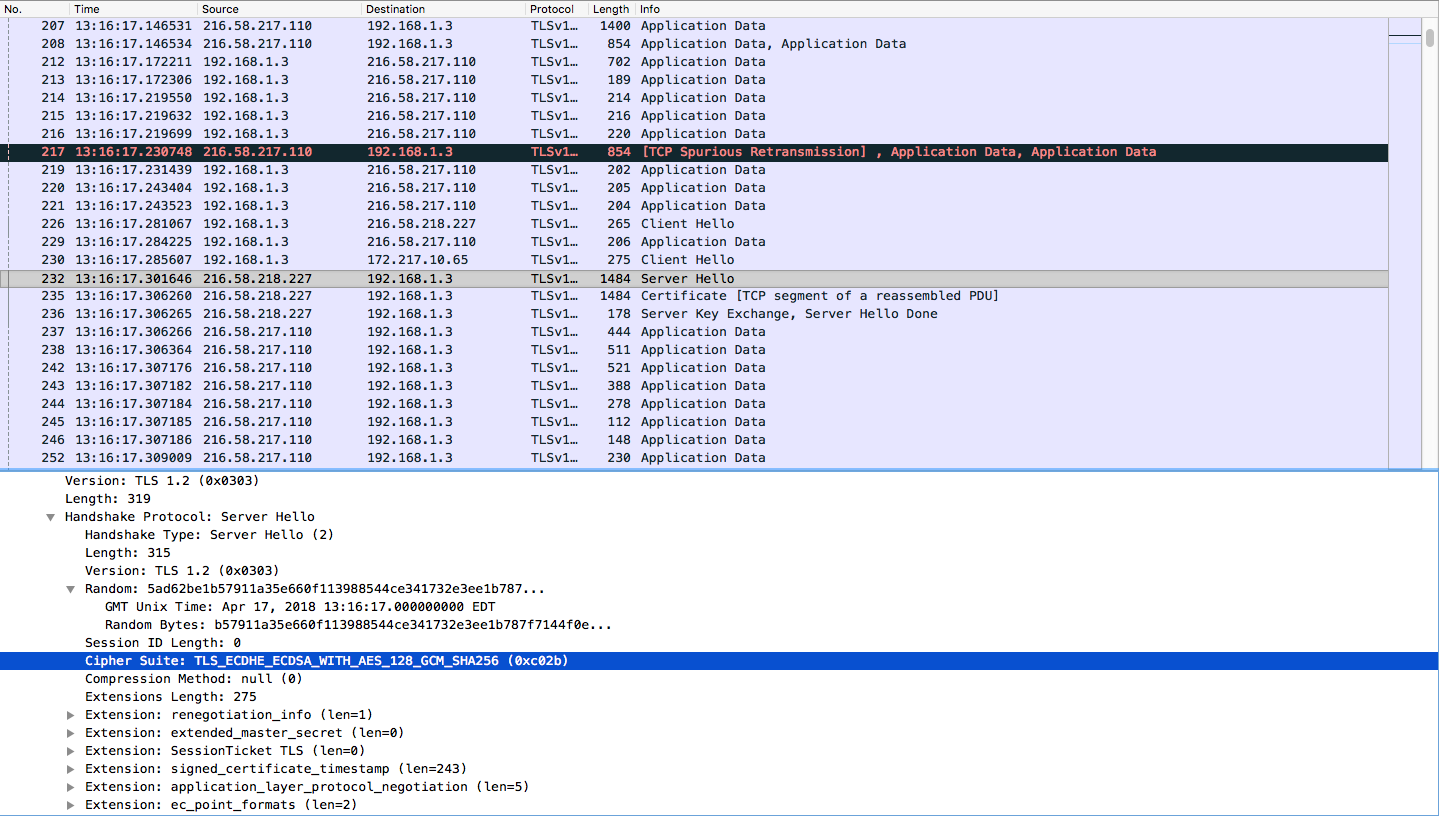
The Second listed suit ;

Public key algorithm: ECDHE\_ECDSA

Symmetric‐key algorithm: AES\_128\_GCM

Hash algorithm: SHA256

1. Server Hello Record: 1. Locate the Server Hello SSL record. Does this record specify a chosen cipher suite? What are the algorithms in the chosen cipher suite?



Public key algorithm: ECDHE\_ECDSA

Symmetric‐key algorithm: AES\_128\_GCM

Hash algorithm: SHA256