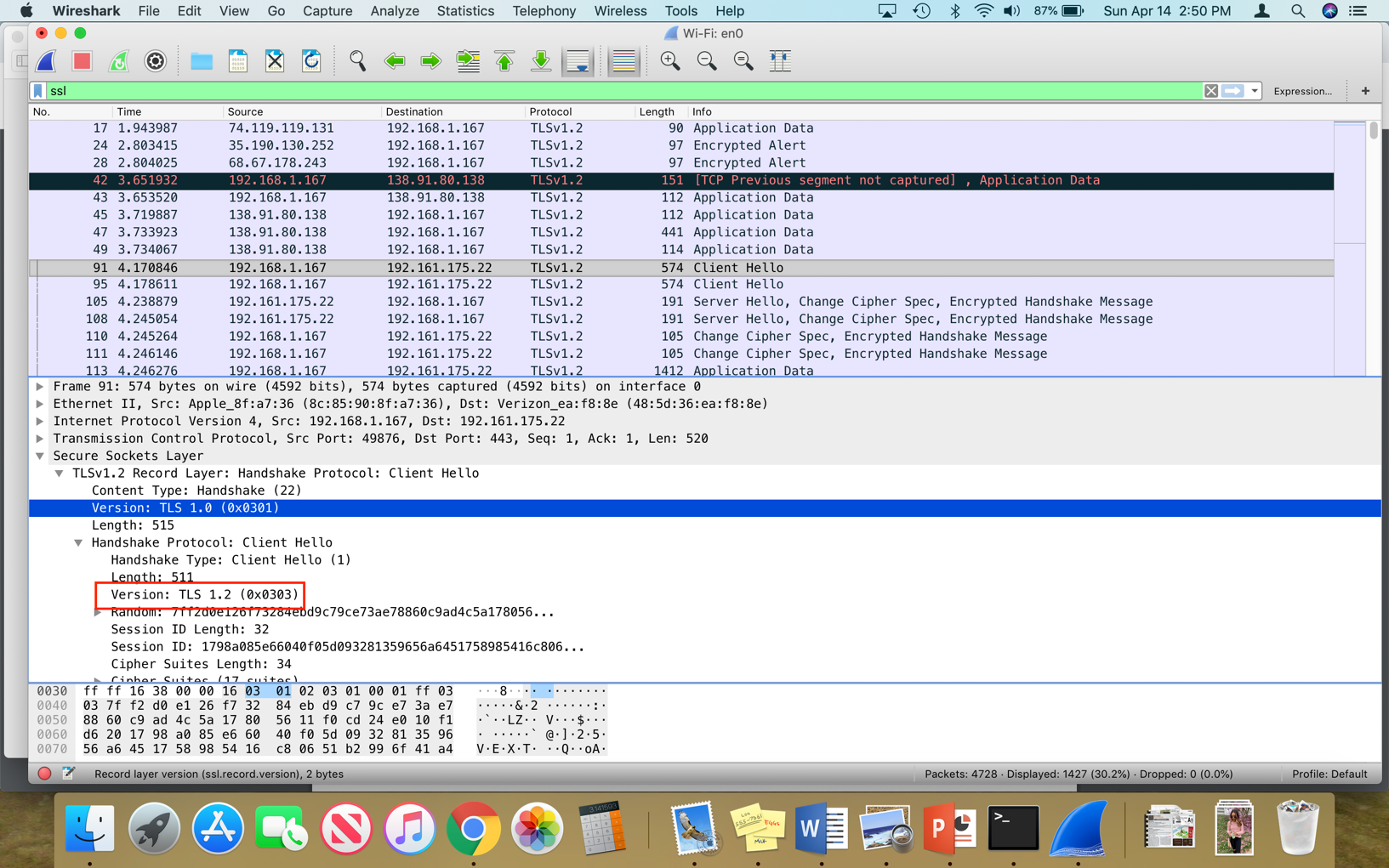
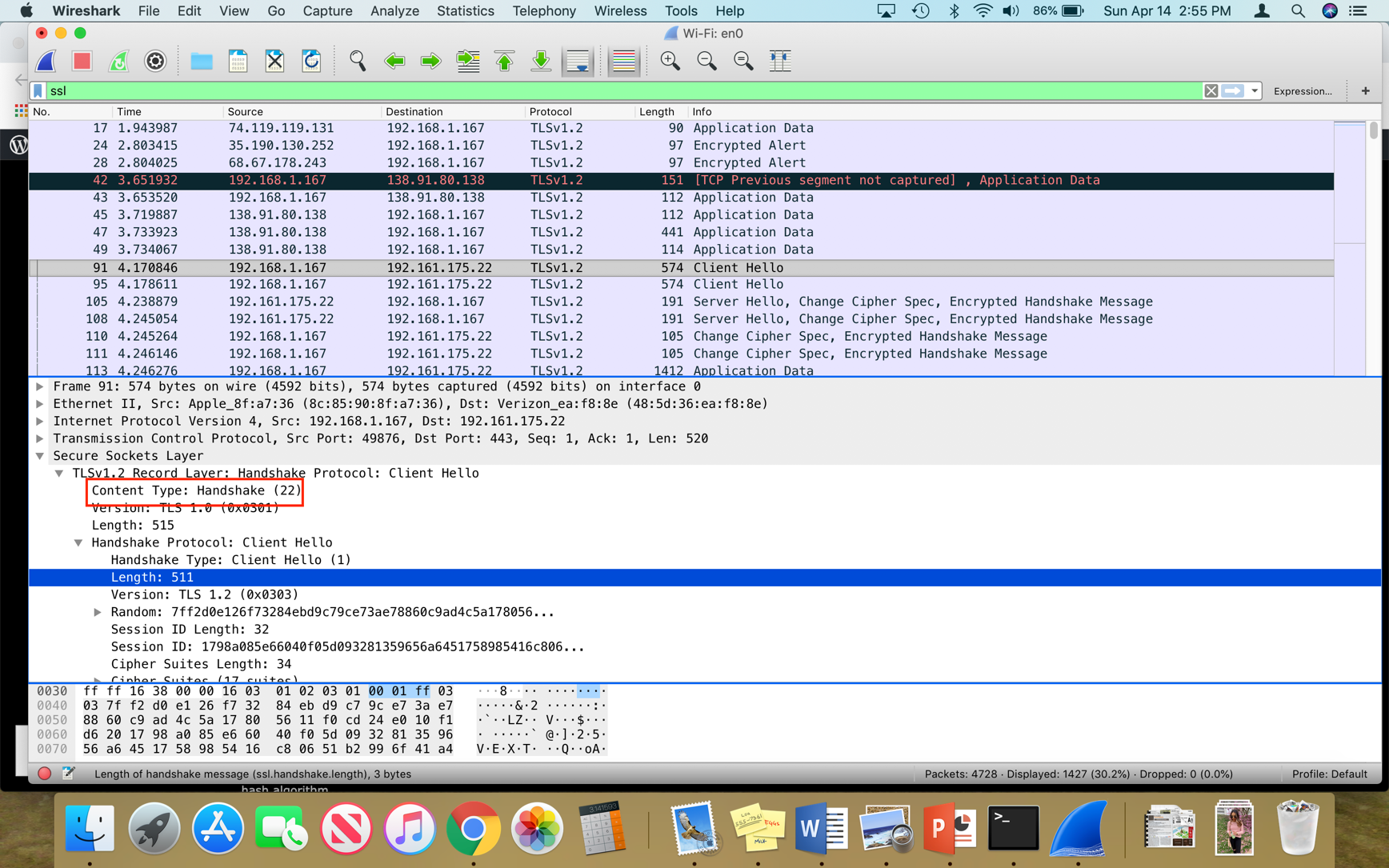


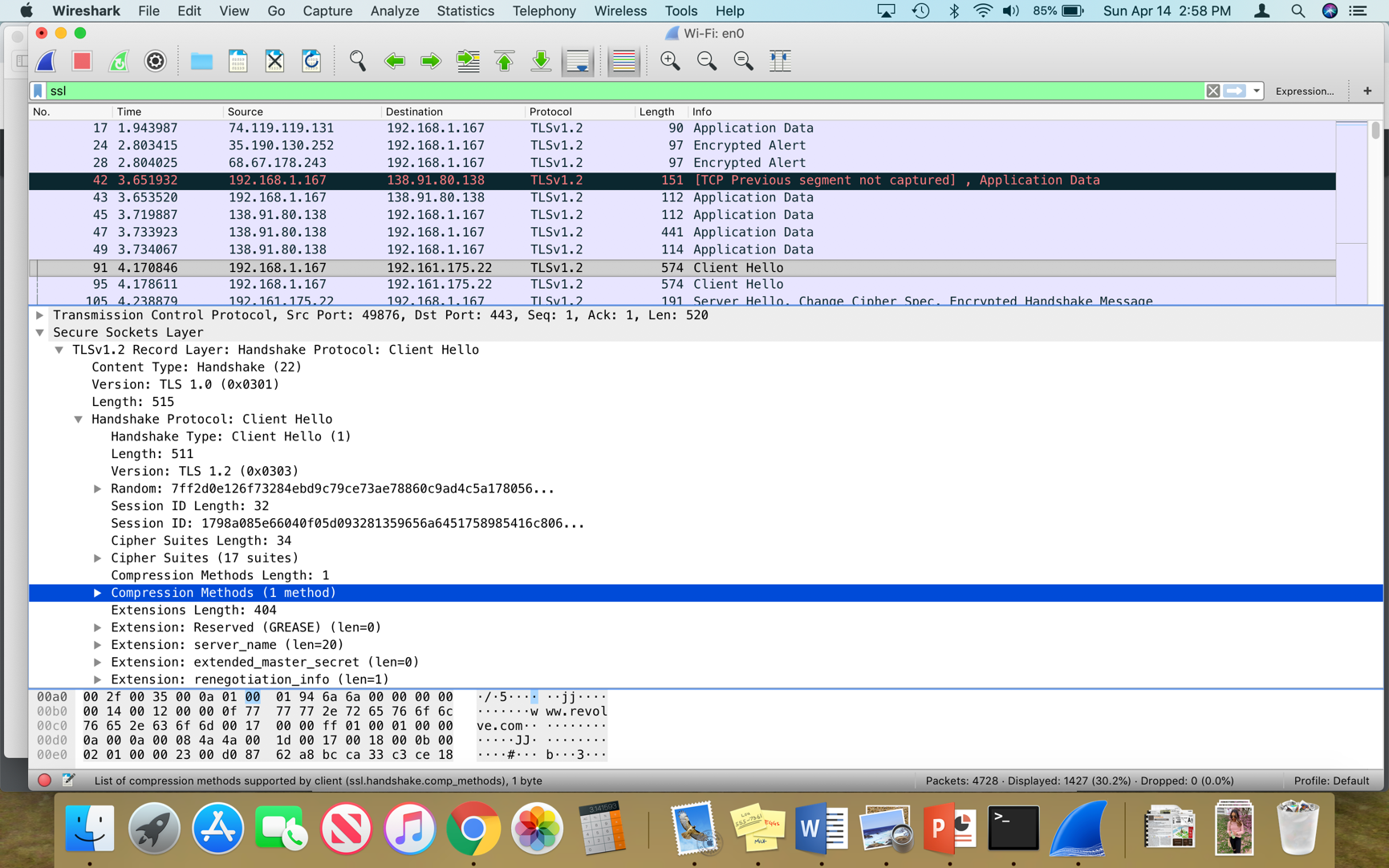
1. What is the SSL/TLS version of the of the Client Hello frame?

The version of SSL/TLS is 1.2.

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 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?

There is no challenge.

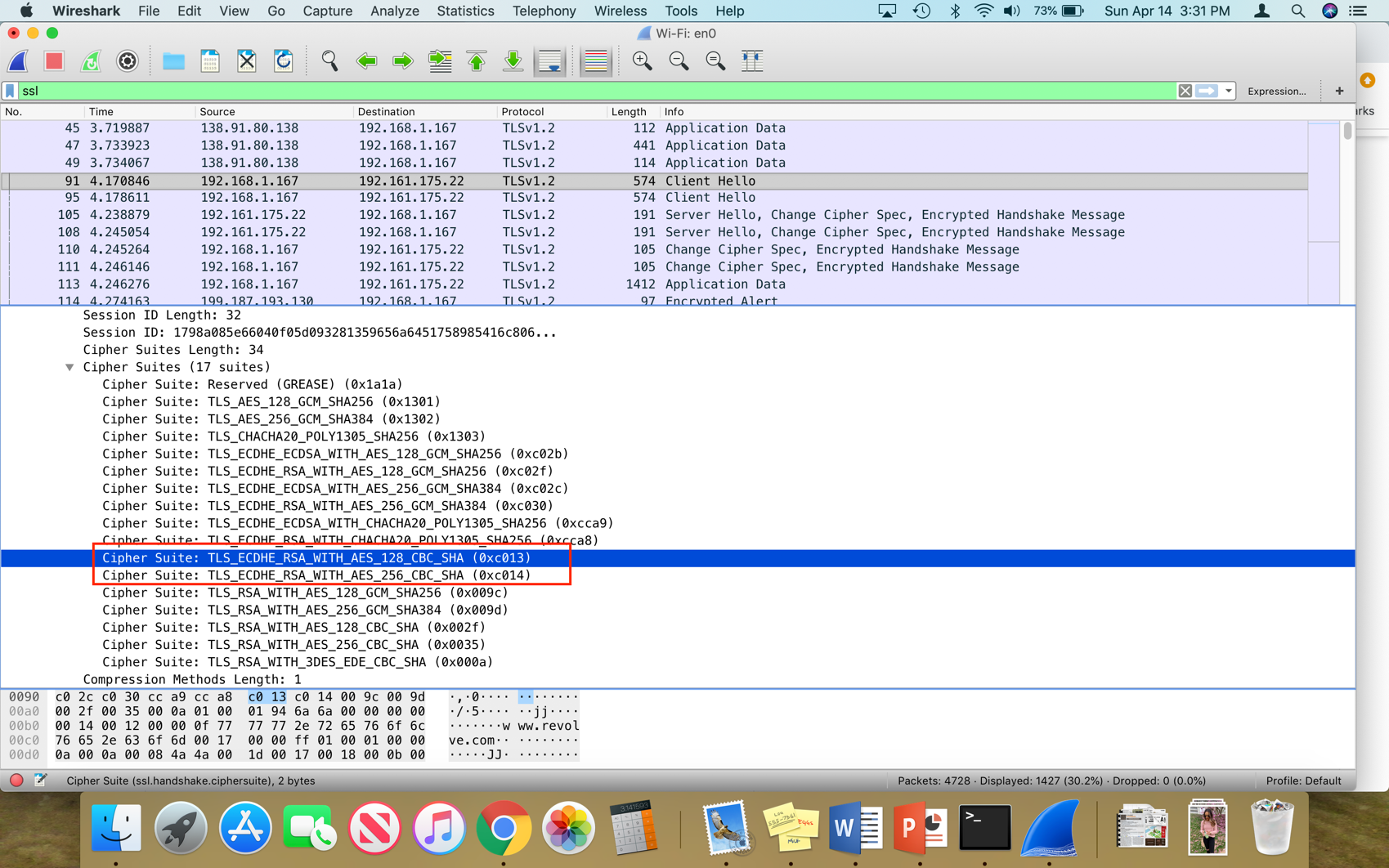
1. Does the ClientHello record advertise the cyber suites it supports? If so, in the first listed suite, what are the public-key algorithm, the symmetric-key algorithm, and the hash algorithm?

The ClientHello does record the cyber suites.

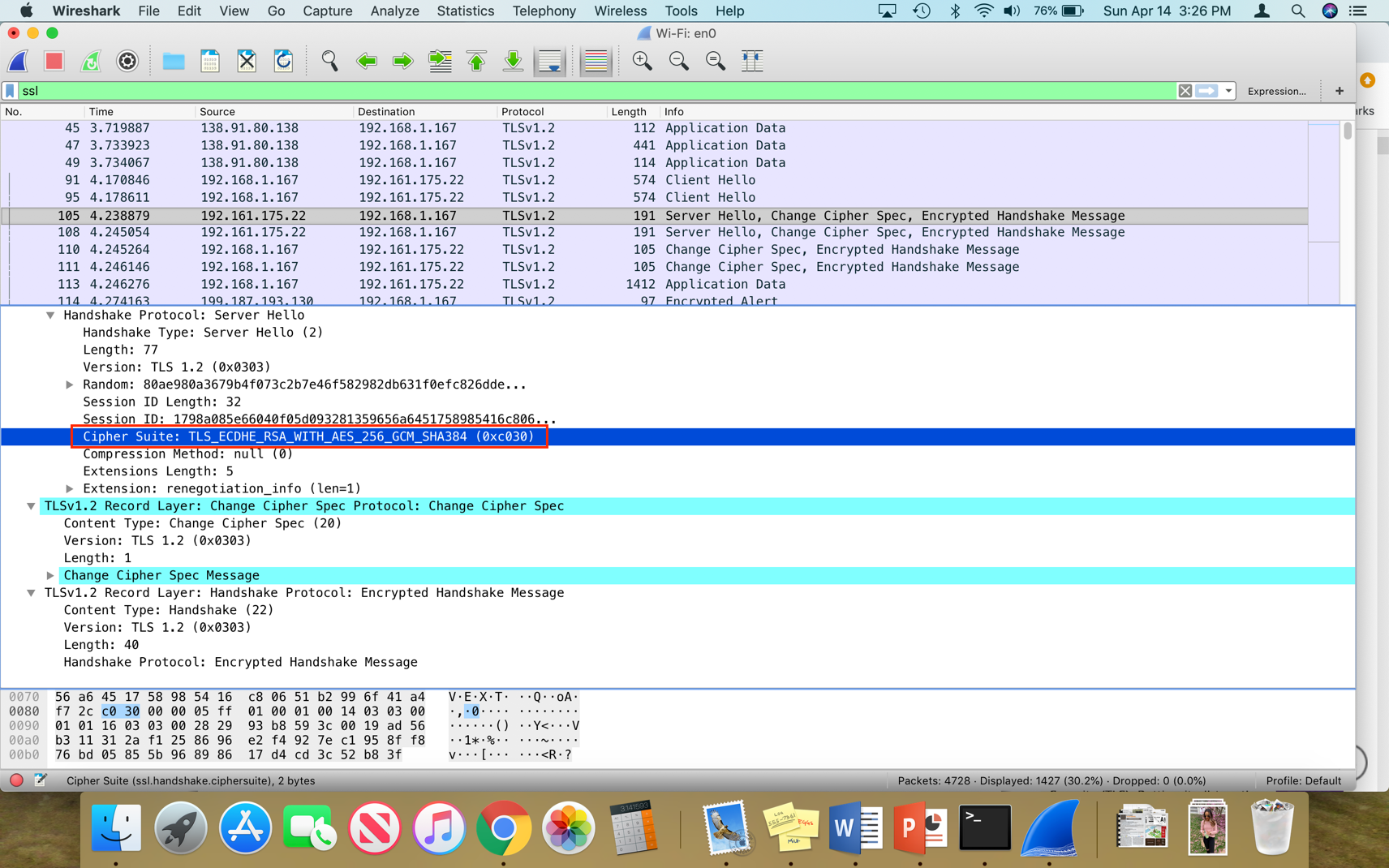
Public-key: RSA

Symmetric-Key: AES128 and AES 256

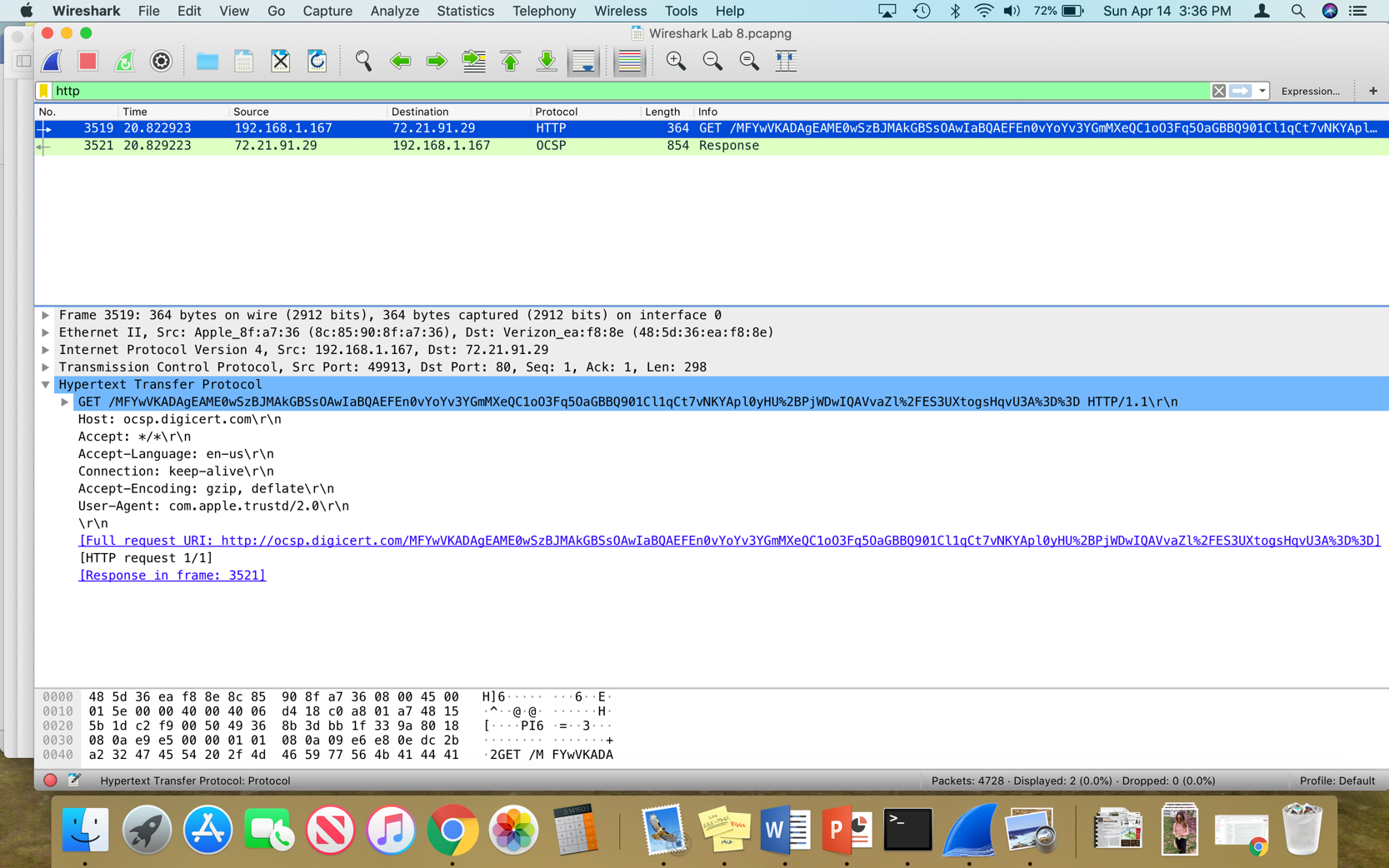
Hash: SHA



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

Yes, it does. It uses RSA for public key, AES for symmetric key, and SHA for hash.

HTTP OK Message:

I didn’t have a HTTP ok message, so I am including a screenshot of that.