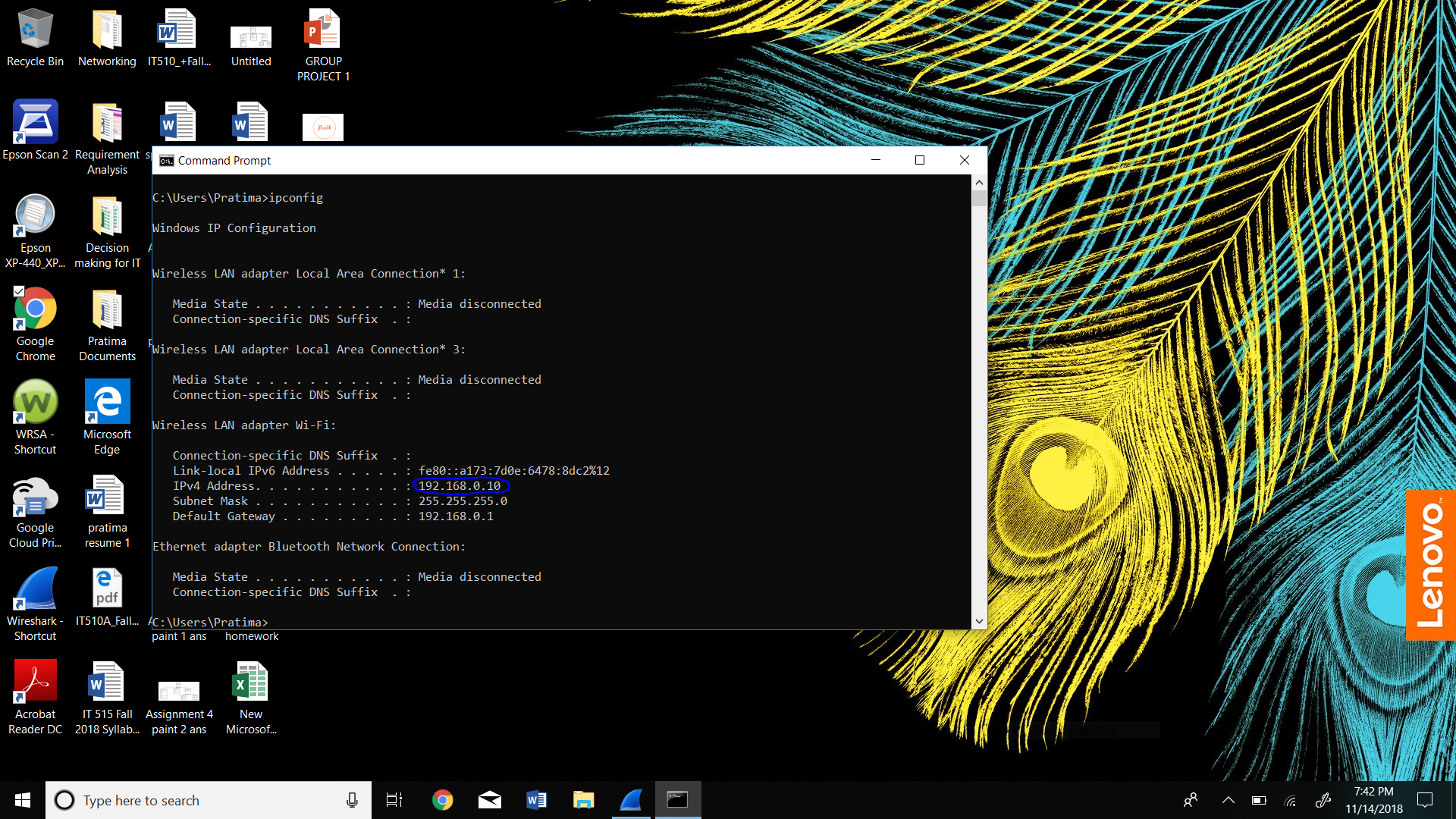
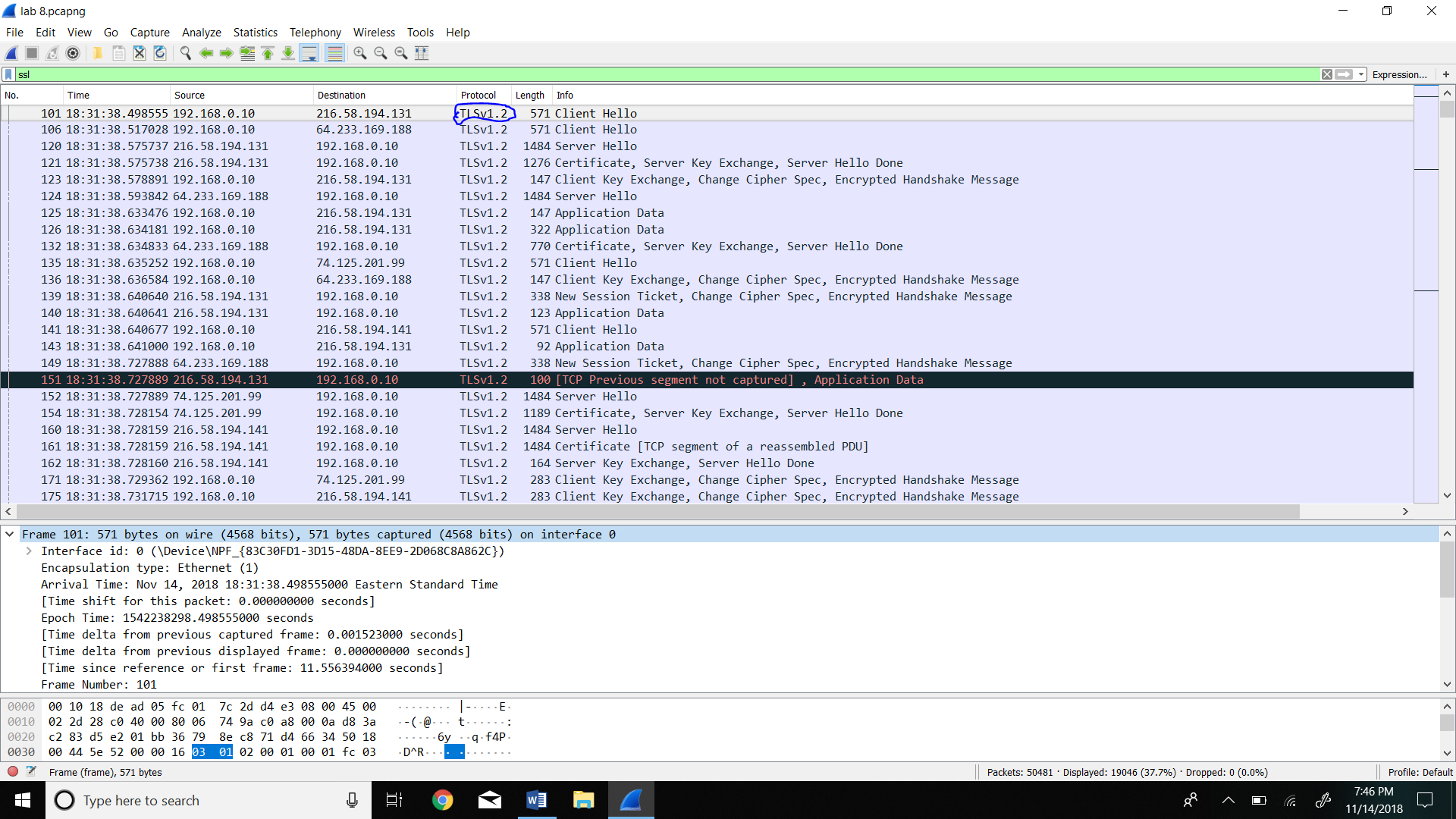
Lab – 8

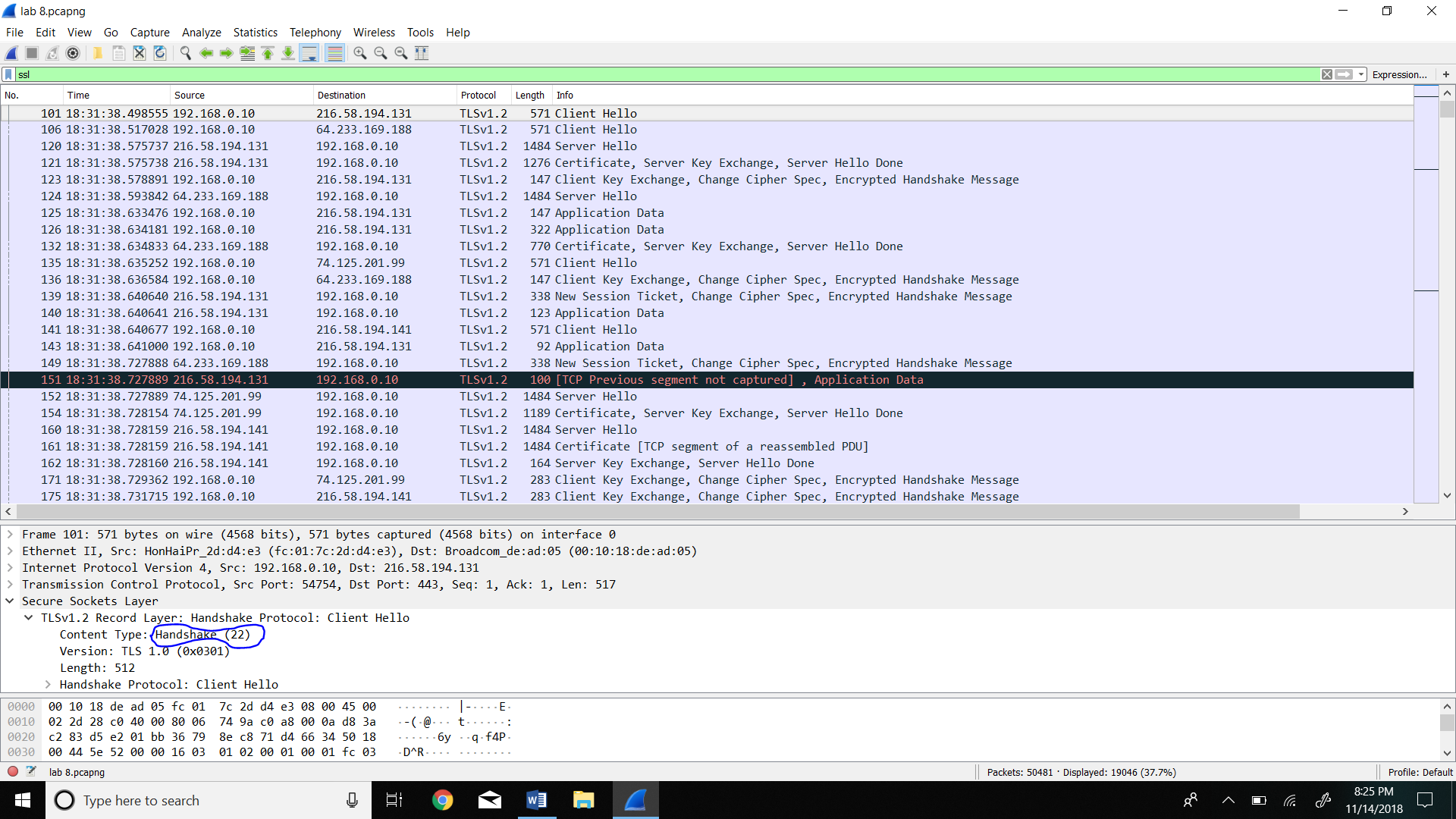
Pratima Bhattarai



Questions:

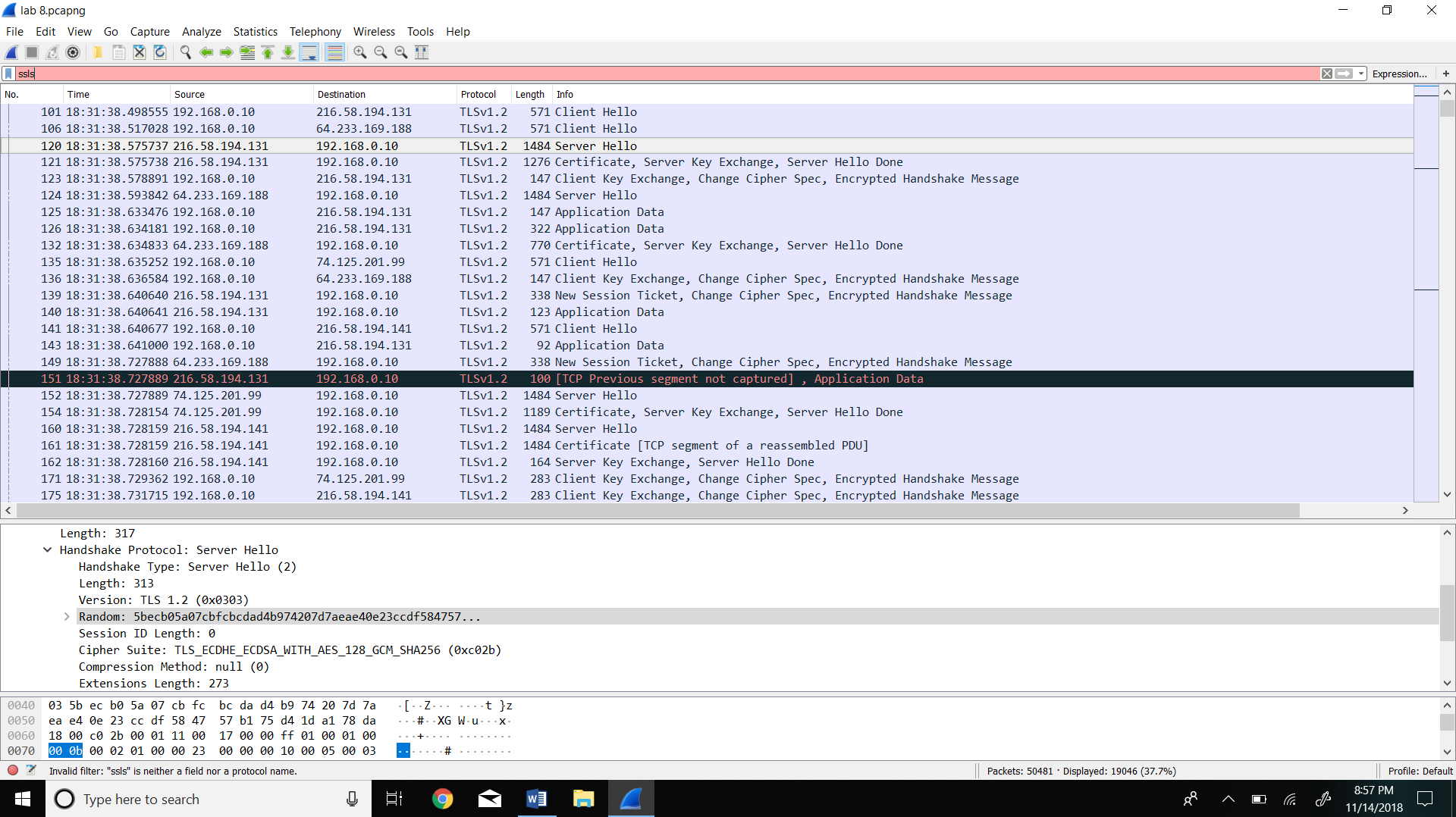
Client Hello Record: 1. What is the SSL/TLS version of the of the Client Hello frame?

The SSL/TLS version of the Client Hello frame is TSLv1.2. 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?

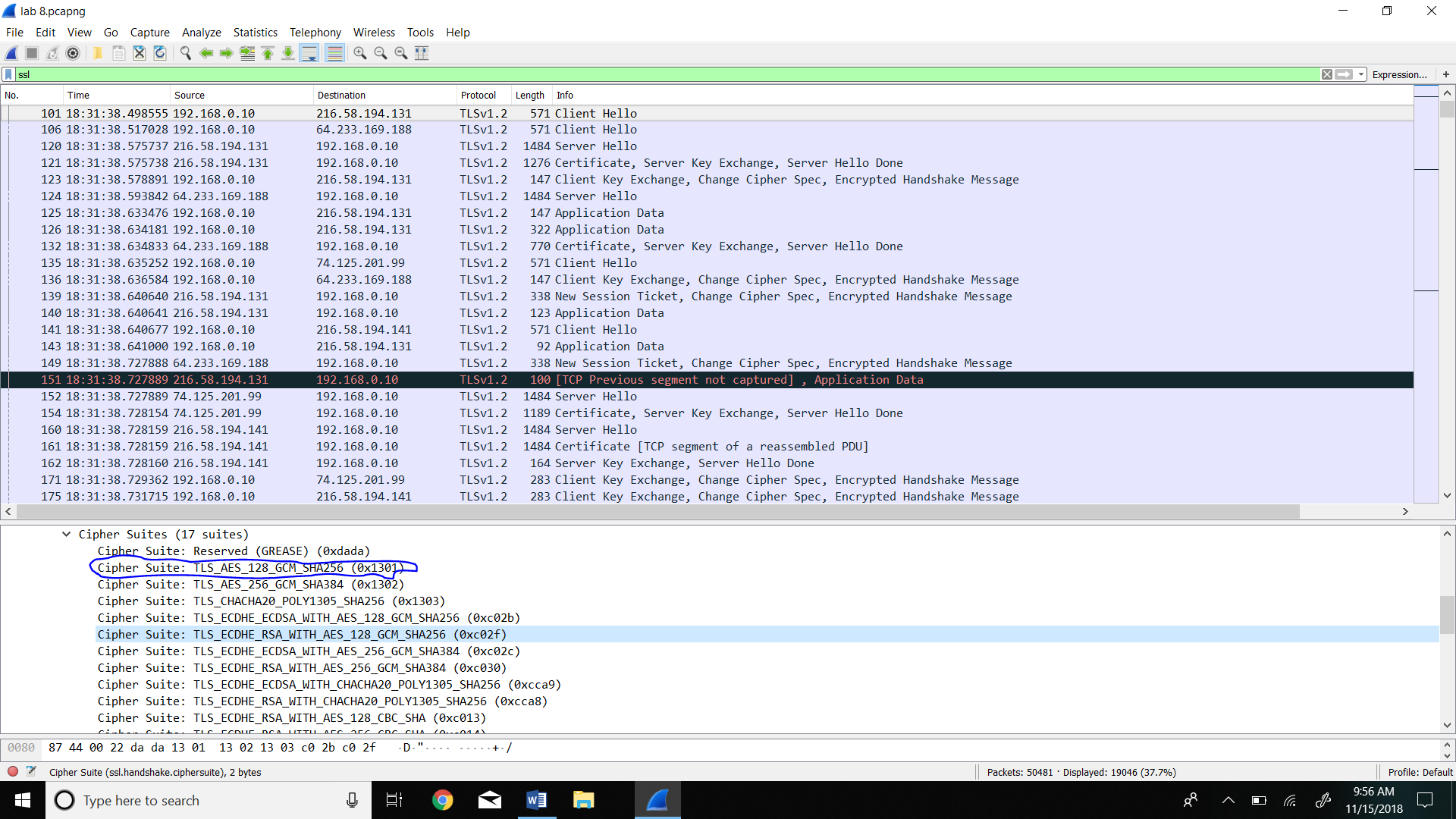
The value of the content type is handshake 22.

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

The value is 51 99 66 9f be 27 27 d7 f3 66 8c d7 e3 d1 61 c2 10 ad 15 87 86 3d fd fb 7f b1 87 fa ec a5 80 80 65



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 Clienthellow advertise the cyber suites it supports. The sysmmetric-key algorithm is AES, public -key algorithm is GCM and hash algorithm is SHA256. 

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 this record specify a chosen cipher suite. The algorithms in the chosen cipher suite are Private key algorithm is ECDHE wherease asymmetric key algorithm is ECDSA.

