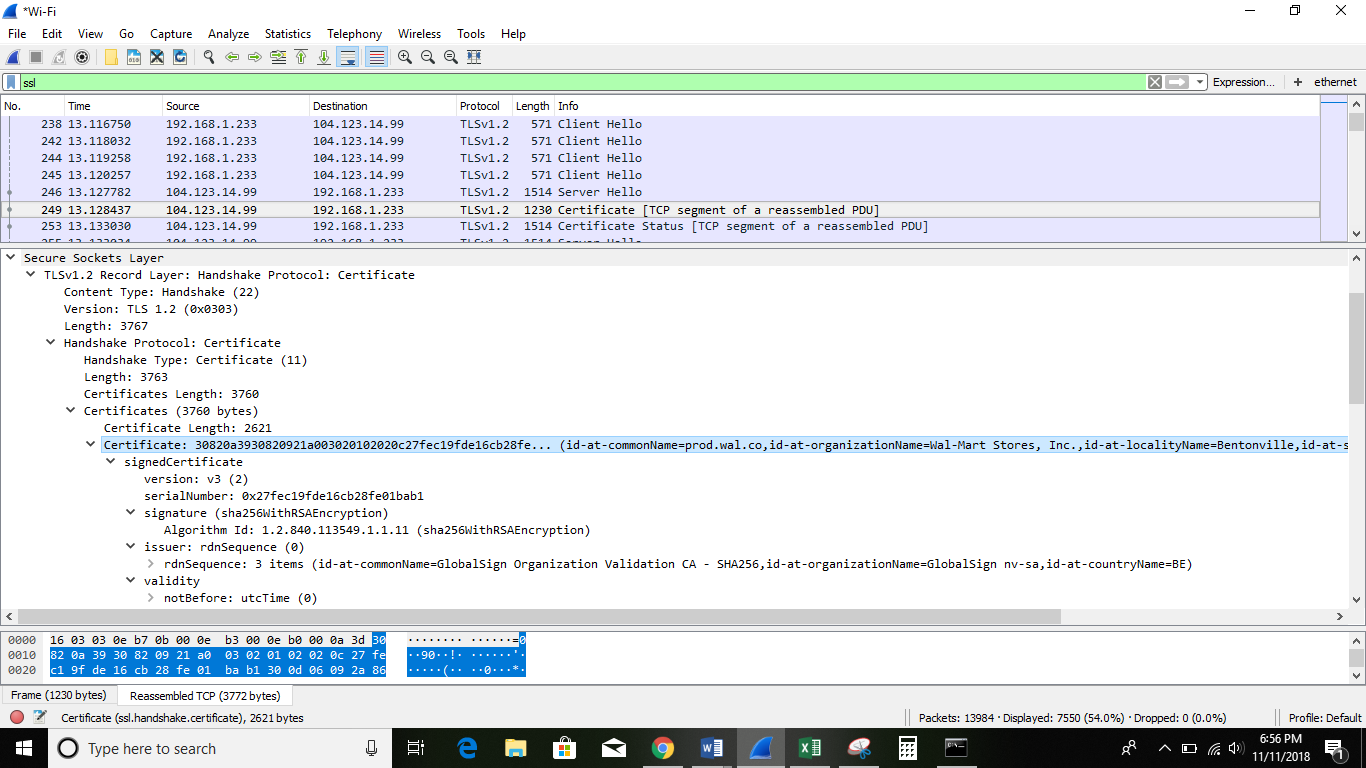
**Luz Deloria**

**Lab-8 – SSL/TLS**

**11/12/18**

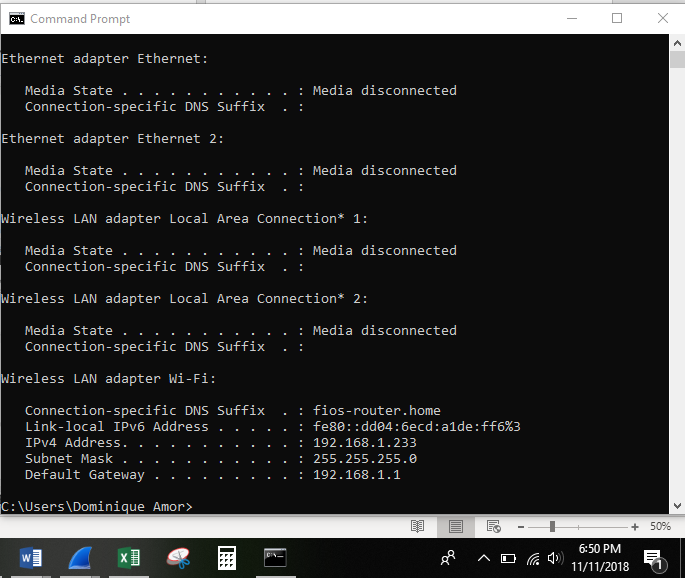
Capture your packets in an SSL session. To do this, you should go to your favorite e-commerce site and begin the process of purchasing an item (but terminating before making the actual purpose!).

* **Walmart.com**



• Take a screenshot of your computer’s IP address

IP address: 

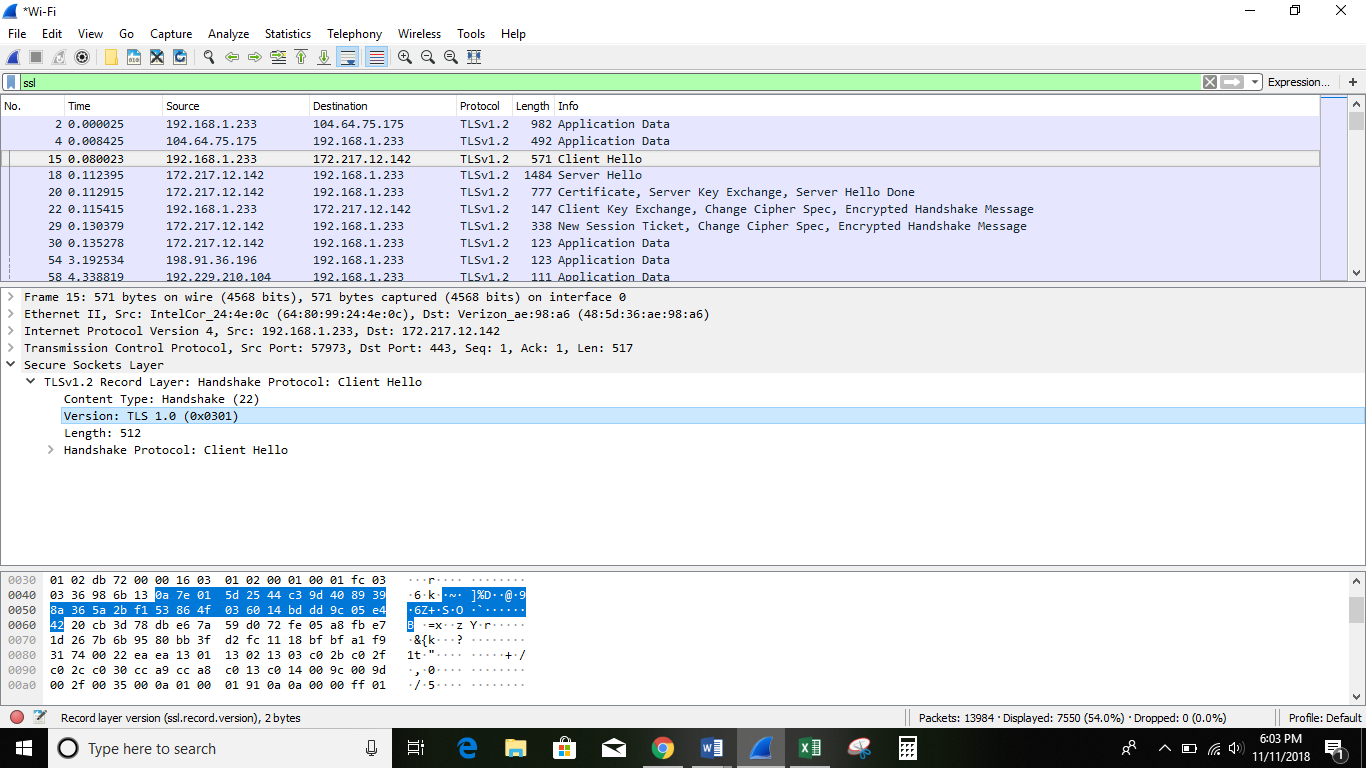


**Questions:**

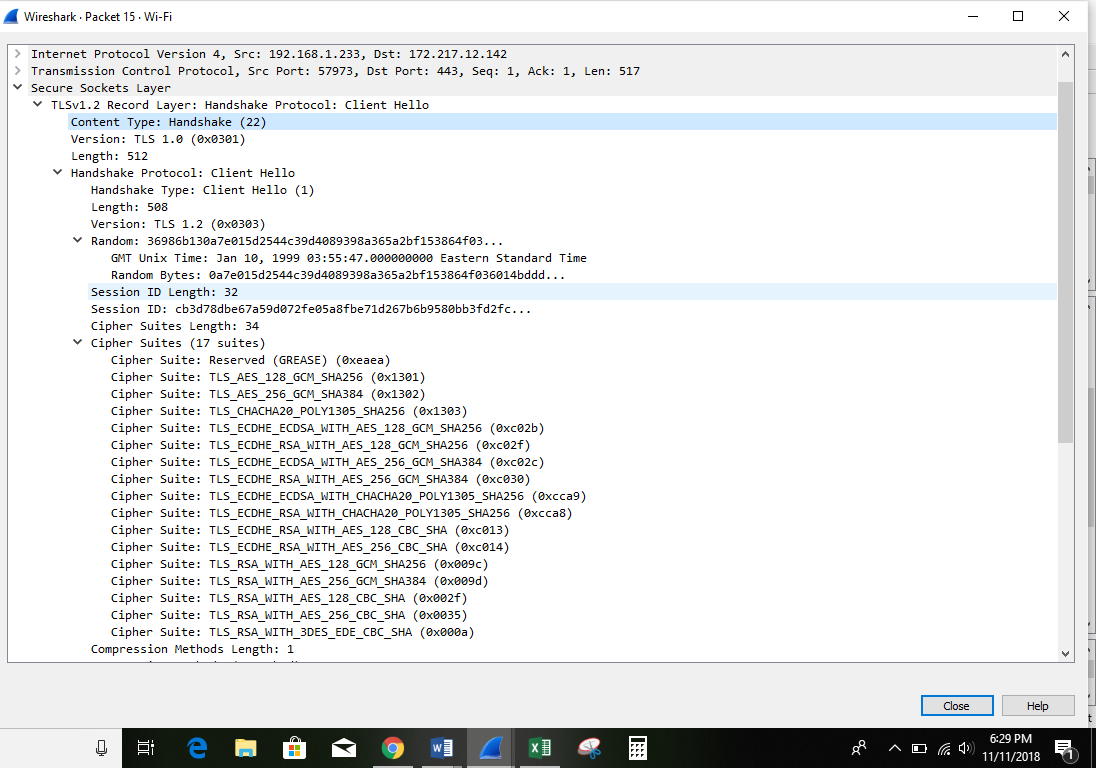
Client Hello Record:

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

* The SSL/TLS version of the Client Hello Frame is:

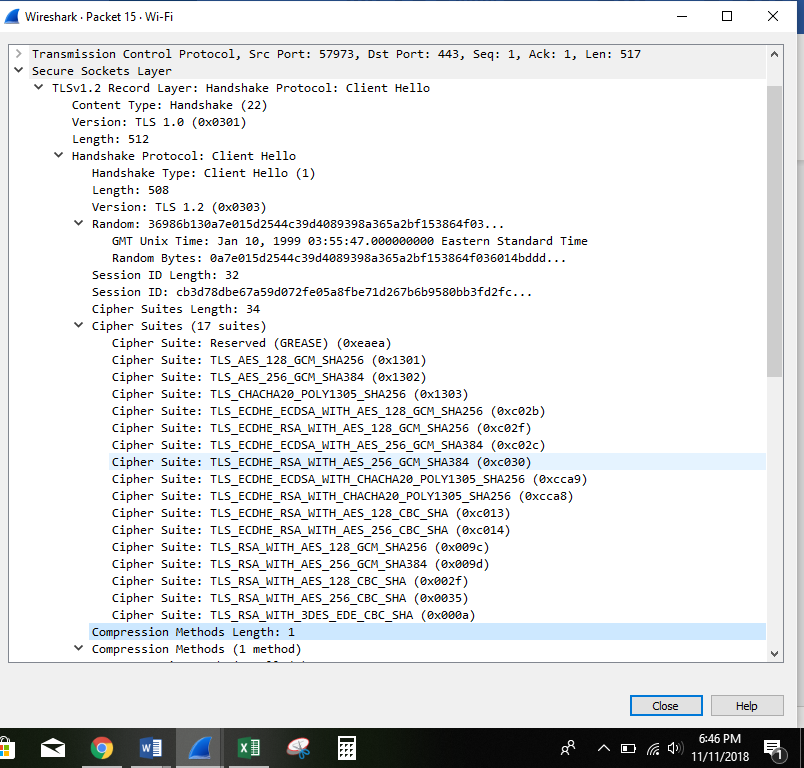


2. Expand the ClientHello record. (If your trace contains multiple ClientHello records, expand the frame that contains the first one.) What is the value of the content type?

* The value of

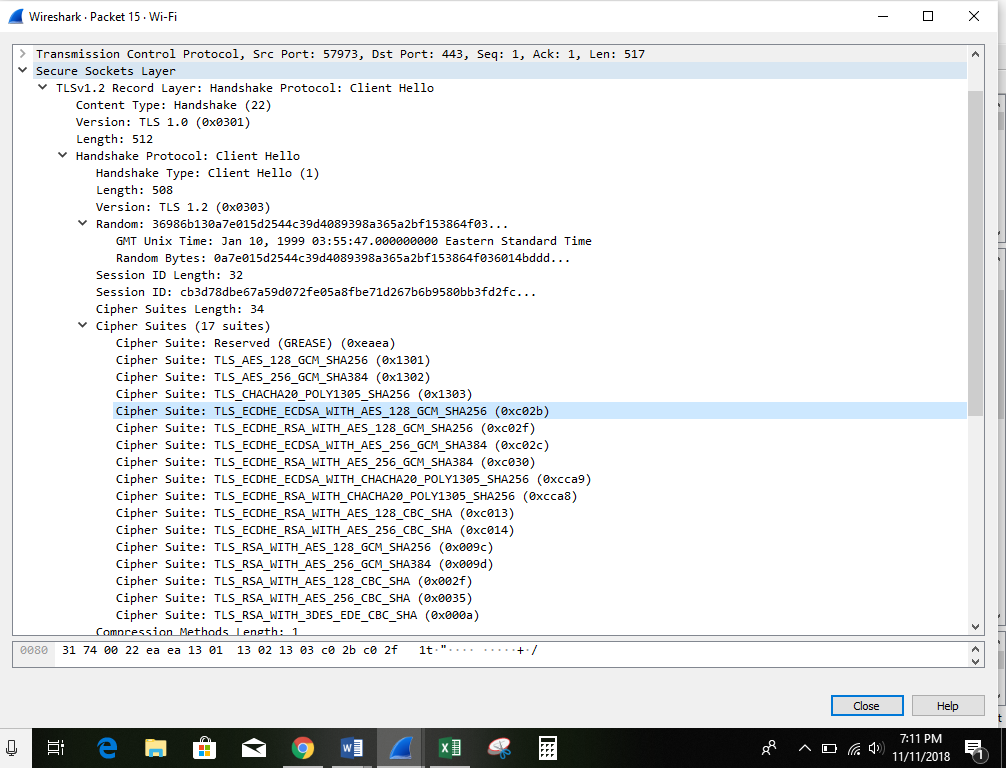
3. Does the ClientHello record contain a nonce (also known as a “challenge”)? If so, what is the value of the challenge in hexadecimal notation?

* none



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?

* Public key algorithm: TLS
* Symmetric‐key algorithm: AES128
* Hash algorithm: 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, it specifies a chosen cipher suite.
* The algorithms in the chosen cipher suite are:



* Public key algorithm: TLS
* Symmetric‐key algorithm: AES128
* Hash algorithm: SHA256

