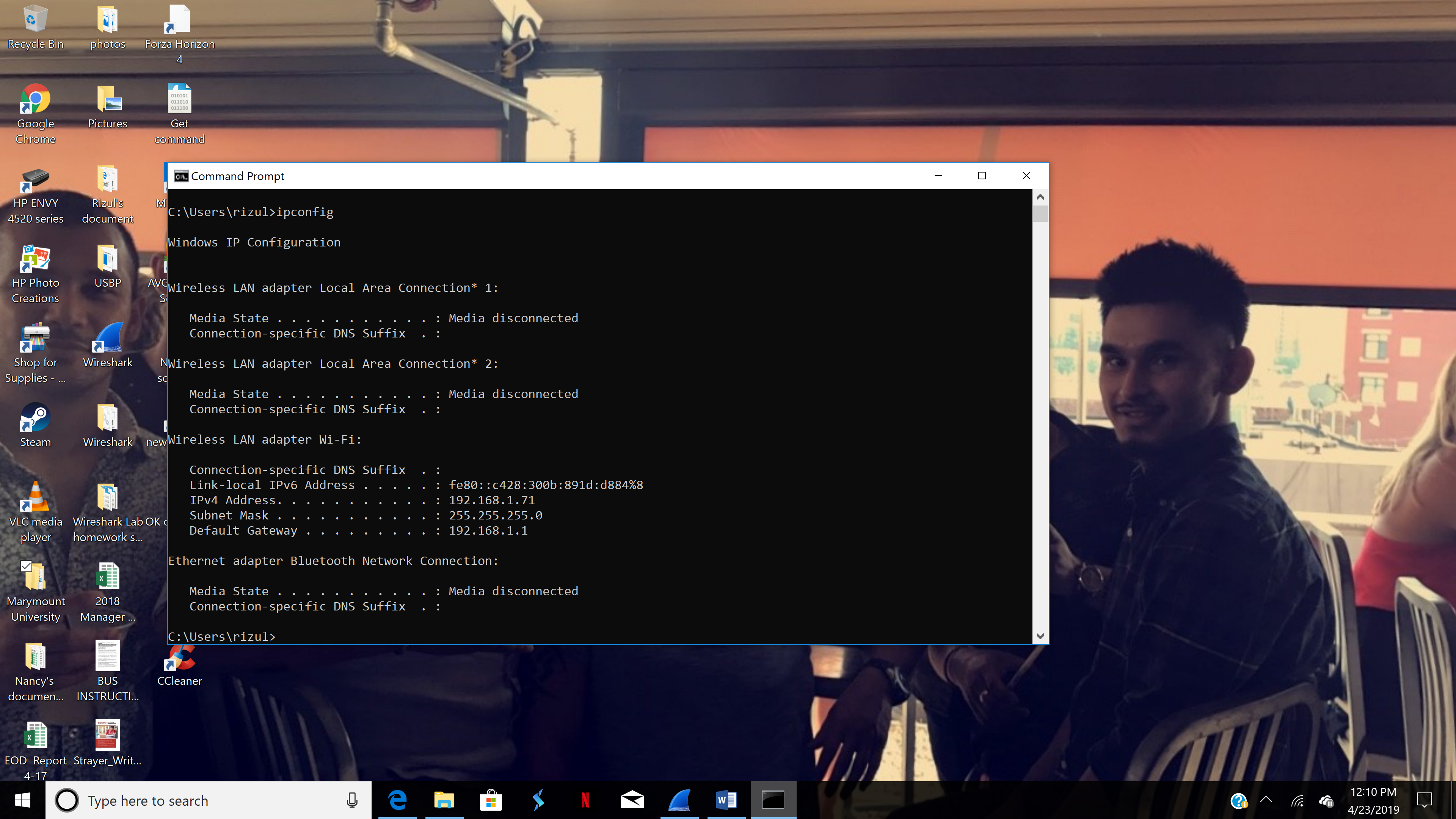
**Naincy Thapa**

**IT-520**

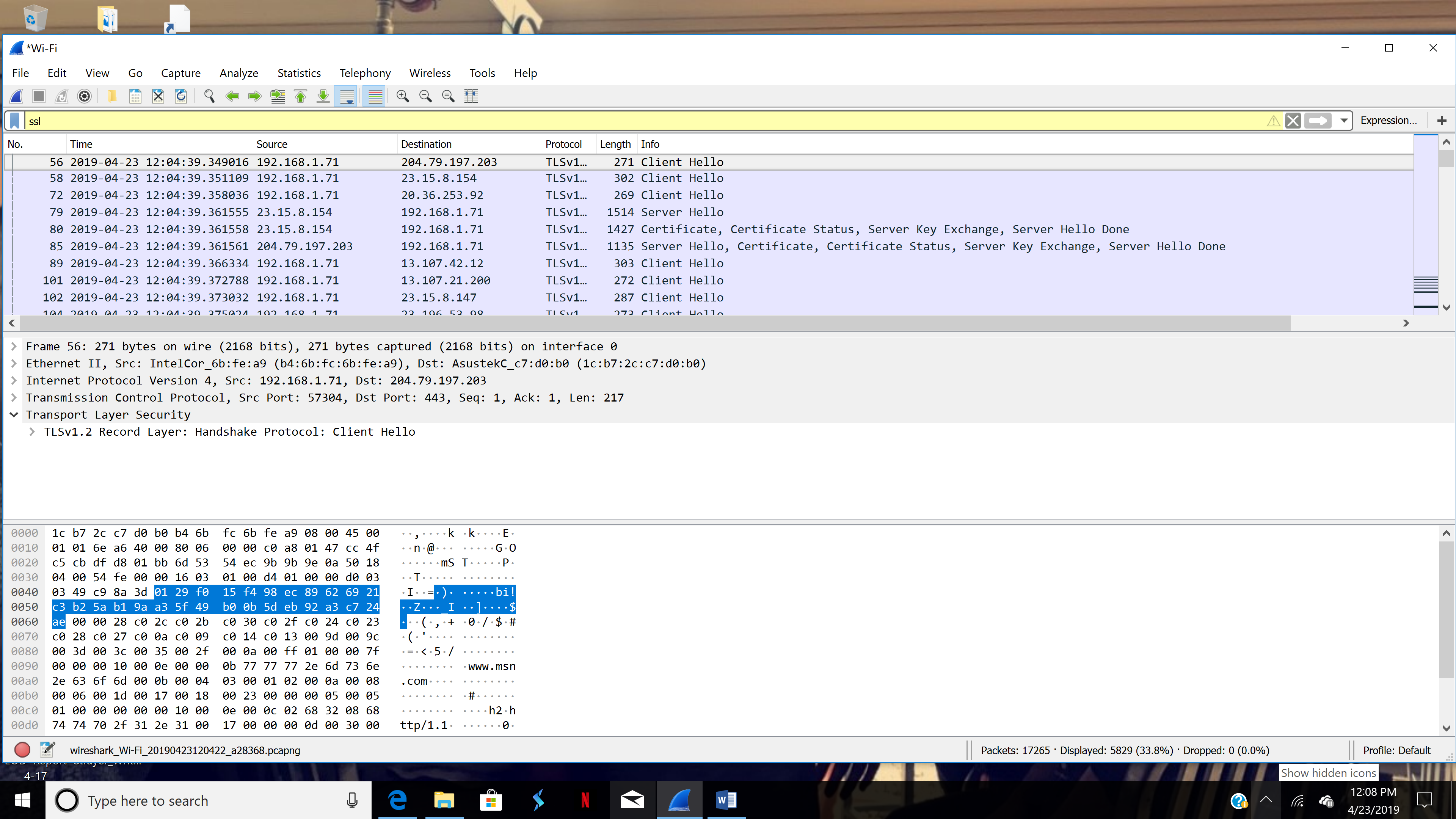
**Lab 8**

**April 23, 2019**



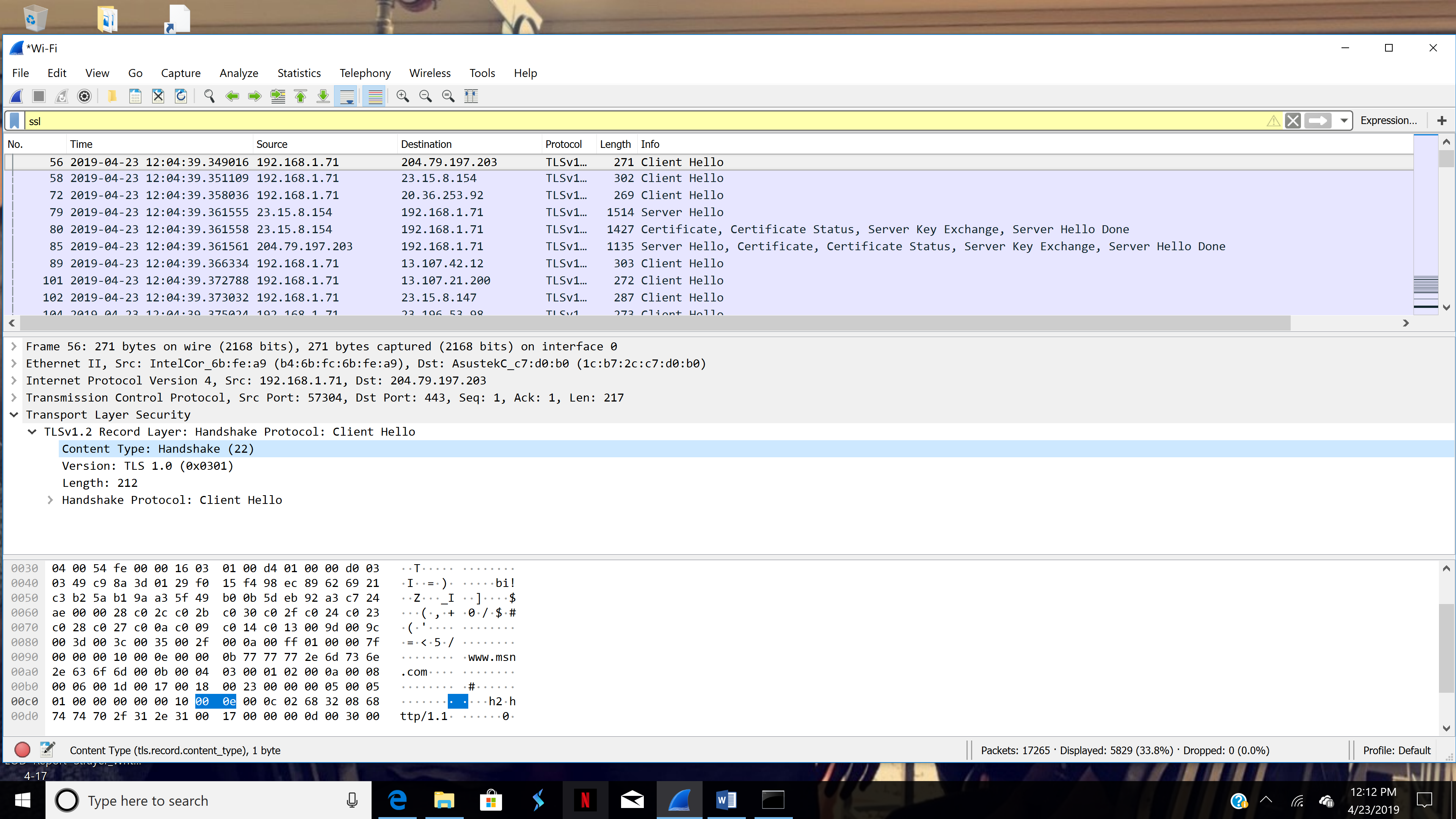
1. What is the SSL/TLS version of the of the Client Hello frame?

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



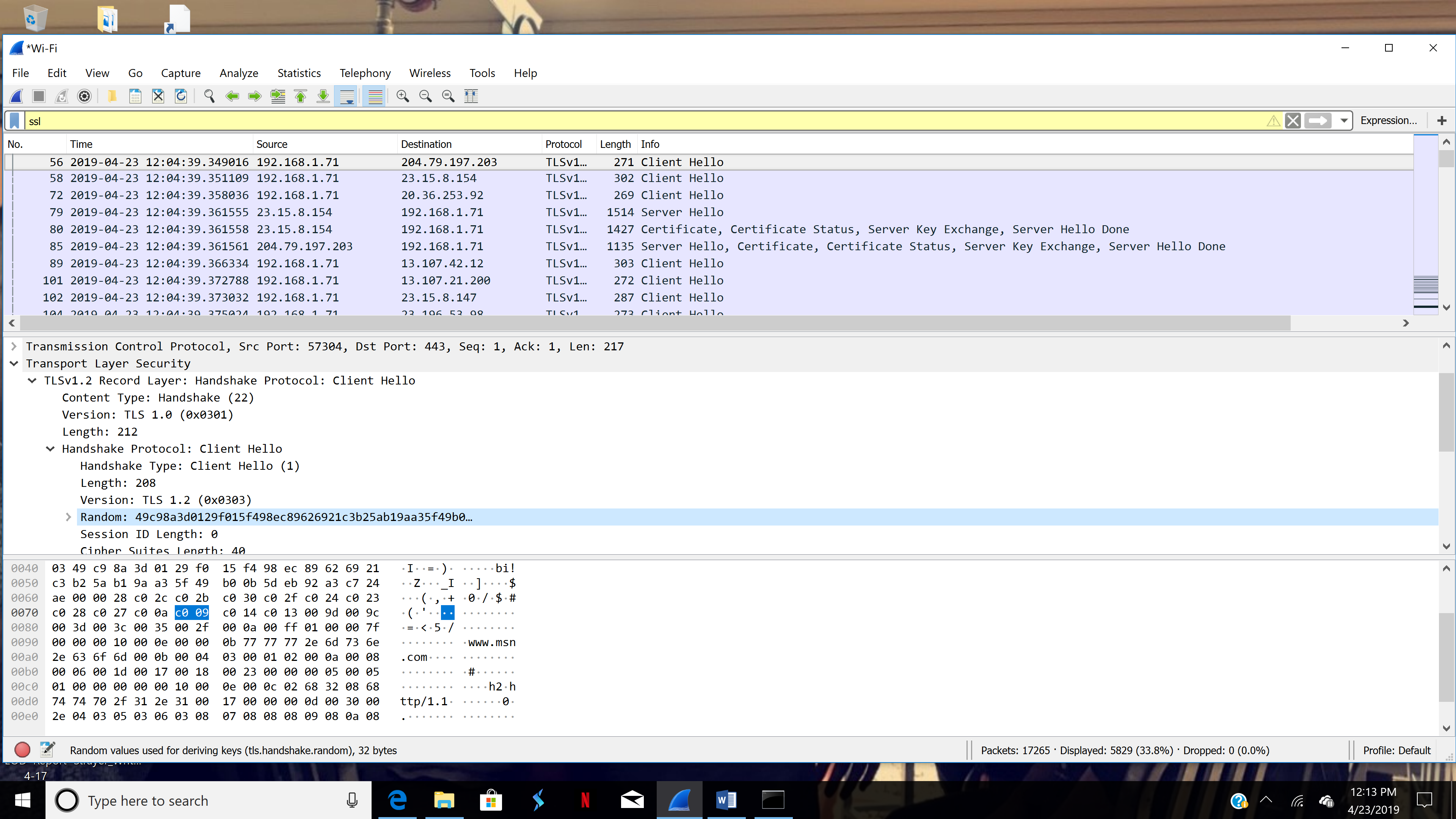
2. Expand the ClientHello record. (If your trace contains multiple ClientHello records, expand the frame that contains the first one.) What is the value of the content type?

**The value of the content type is handshake 22.**



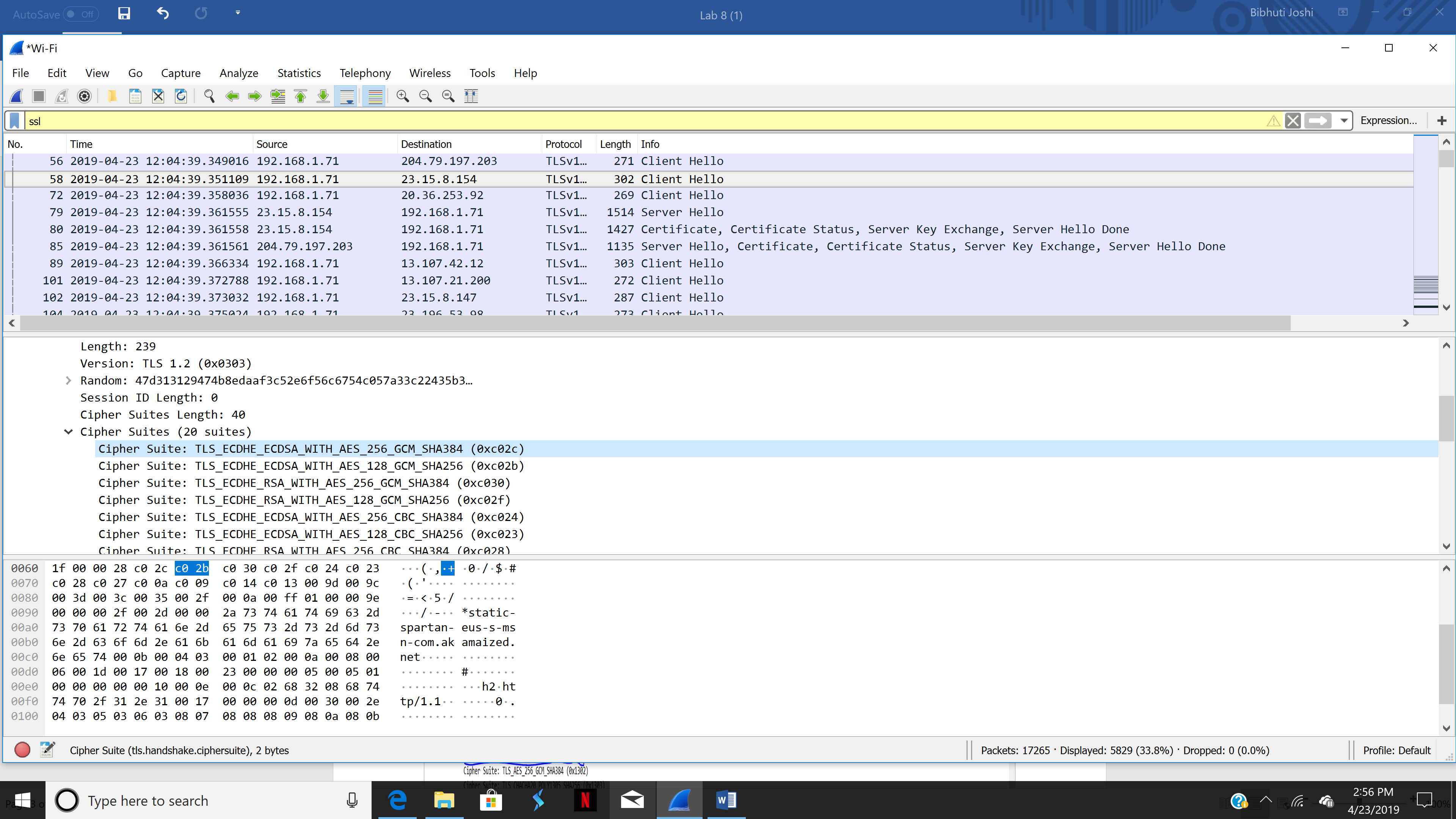
3. Does the ClientHello record contain a nonce (also known as a “challenge”)? If so, what is the value of the challenge in hexadecimal notation?

**Value: 49c98a3d0129f015f498ec89626921c3b25ab19aa35f49b0**



4. 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?

**Yes. The symmetric-key algorithm is AES, public -key algorithm is GCM and hash algorithm is SHA384.**



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?

**Yes. The algorithms in the chosen cipher suite are Private key algorithm is ECDHE whereas asymmetric key algorithm is ECDSA.**

