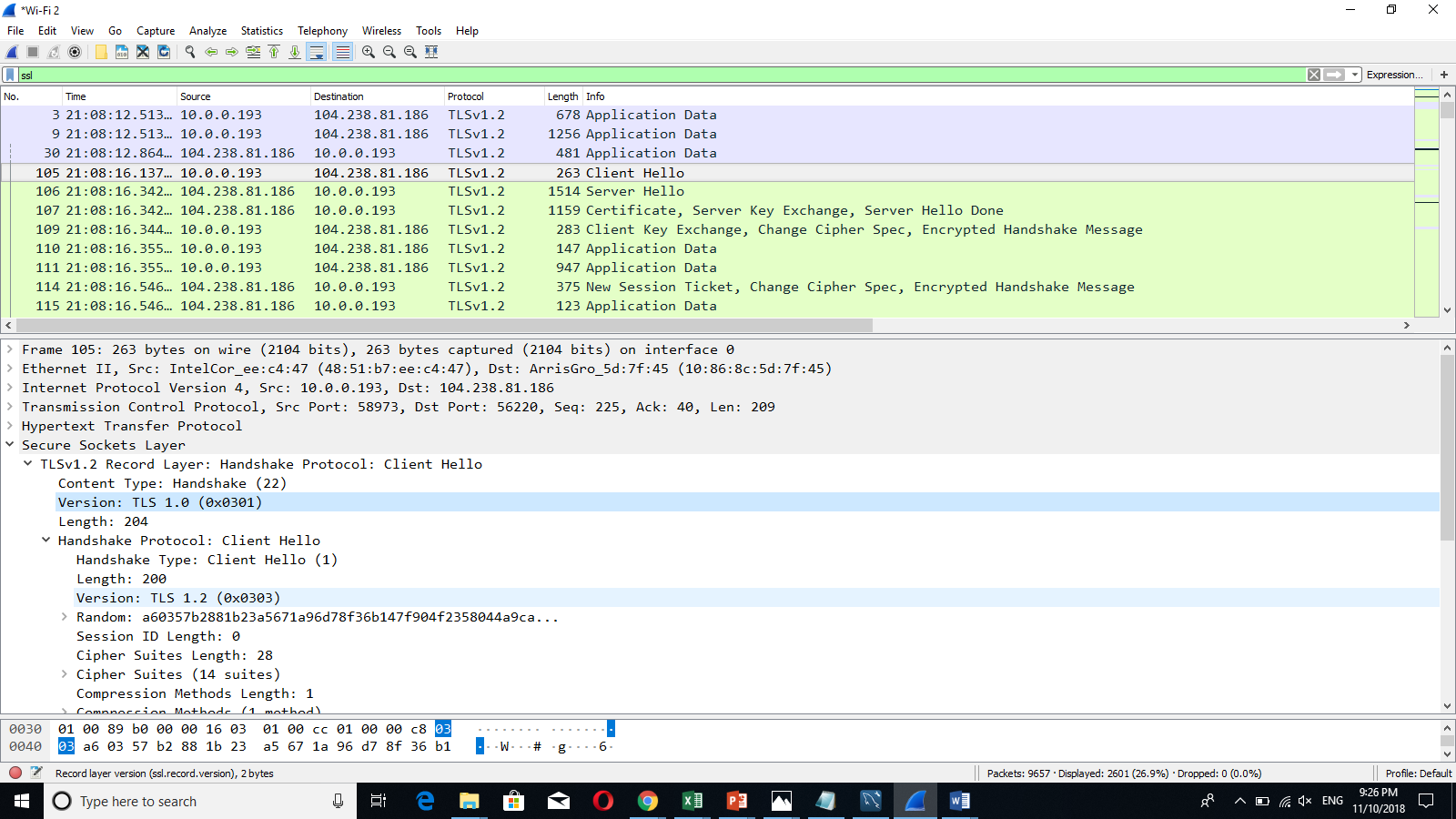
**Abdalrhman Abdalla Lab 8**

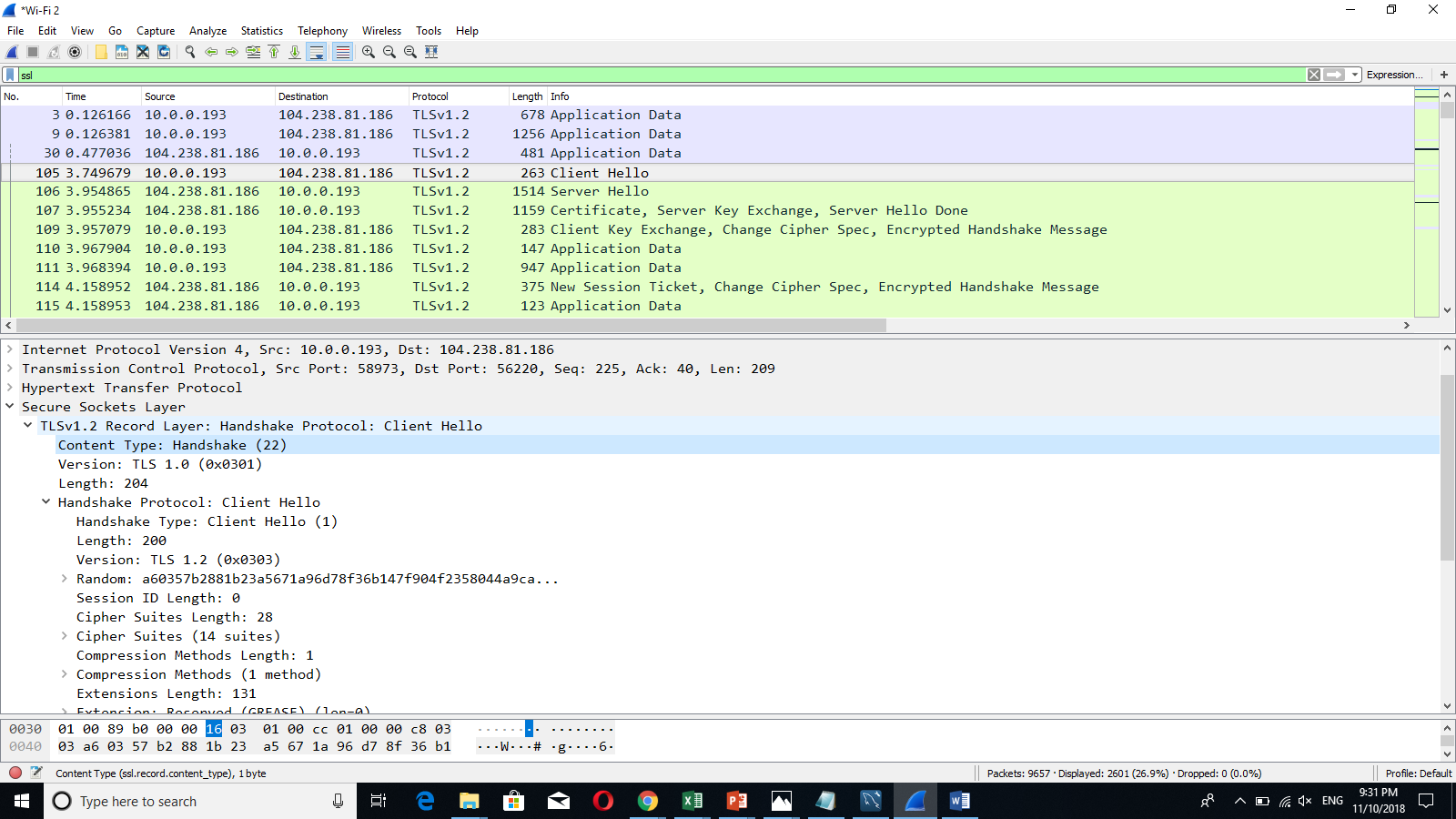
1. What is the SSL/TLS version of the of the Client Hello frame?

**TLS 1.2**



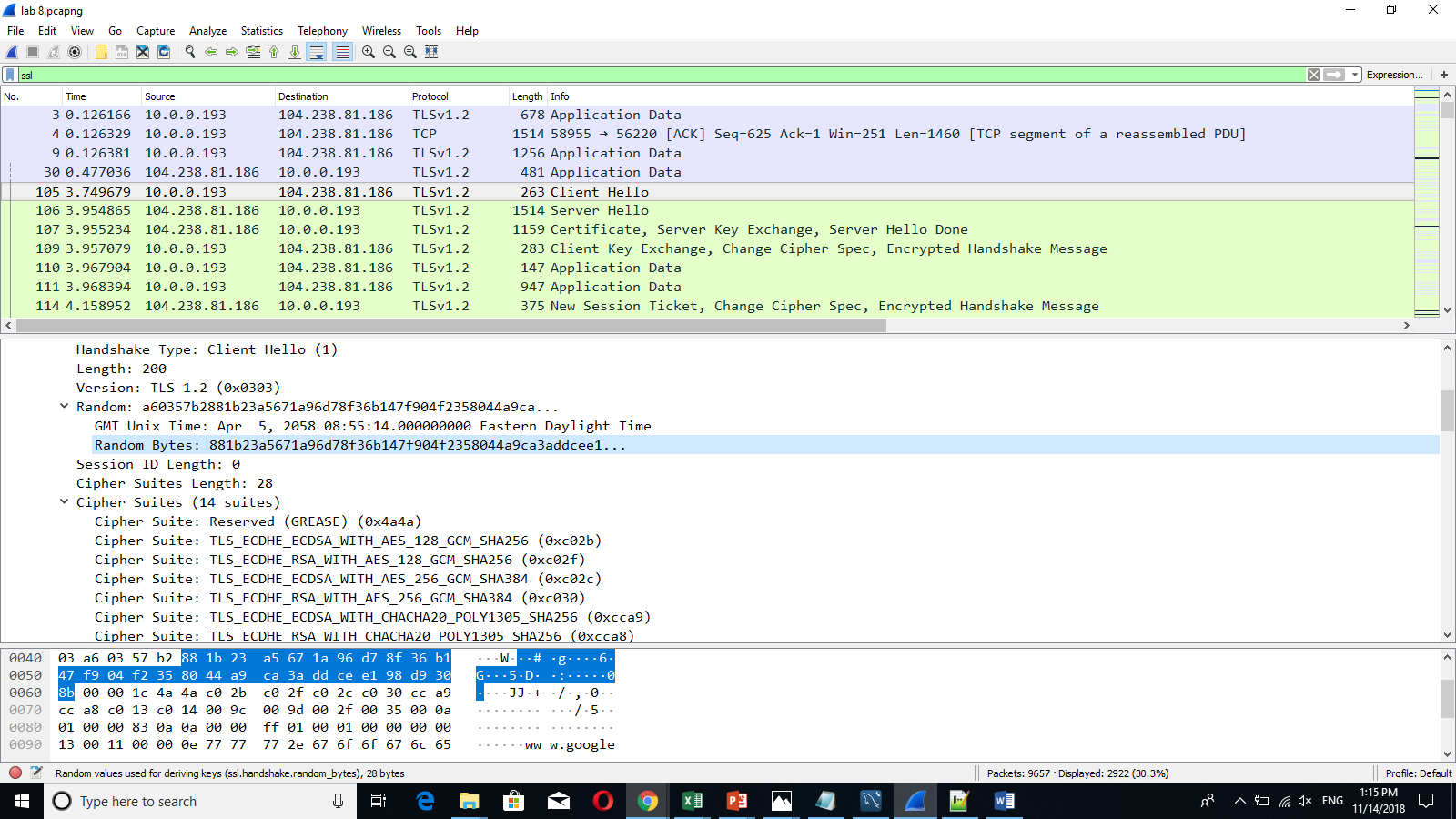
1. Expand the ClientHello record. (If your trace contains multiple ClientHello records, expand the frame that contains the first one.) What is the value of the content type?

**Handshake(22)**

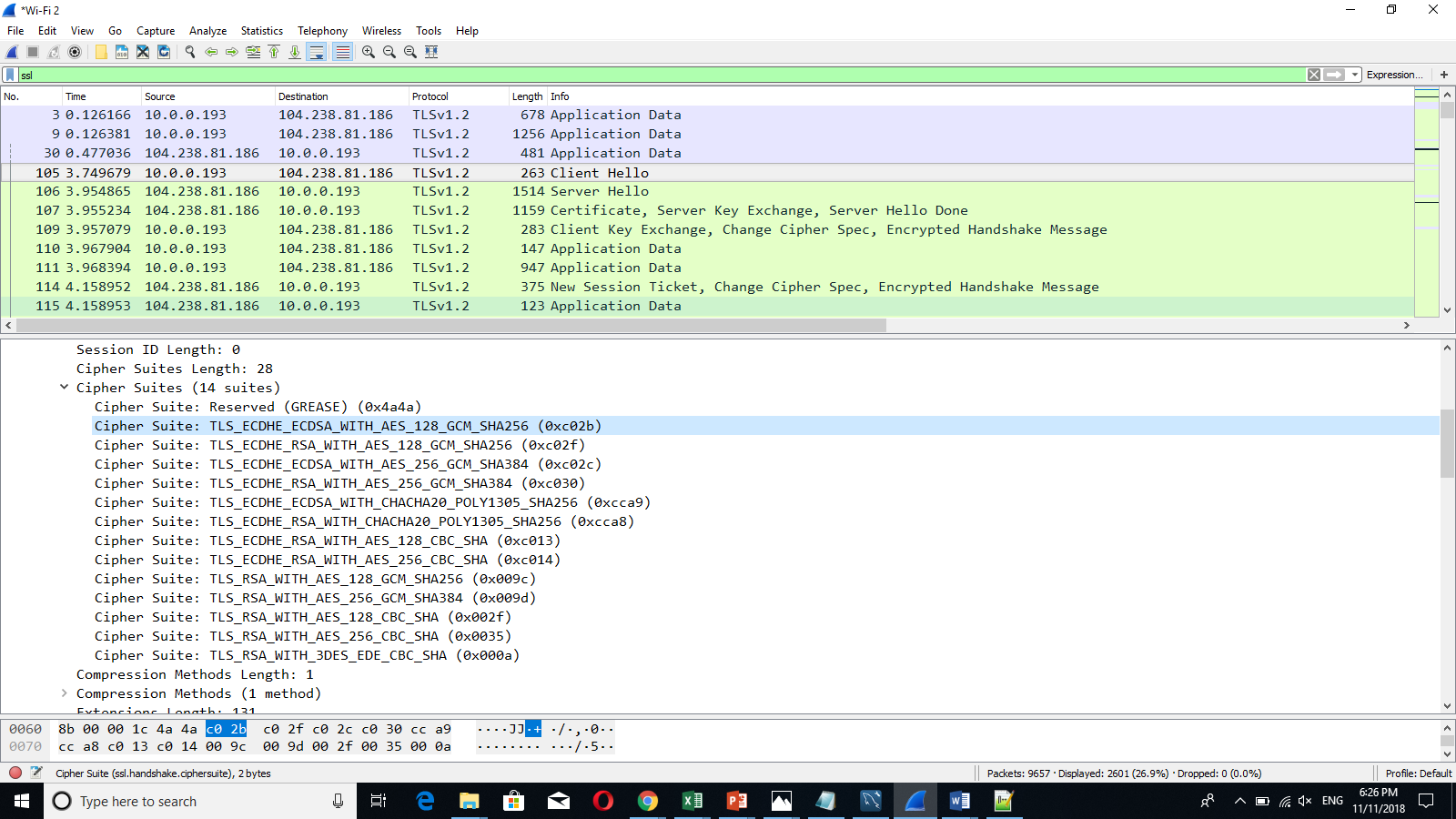


1. Does the ClientHello record contain a nonce (also known as a “challenge”)? If so, what is the value of the challenge in hexadecimal notation?

**88:1b:23:a5:67:1a:96:d7:8f:36:b1:47:f9:04:f2:35:80:44:a9:ca:3a:dd:ce:e1:98:d9:30:8b**



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 it does, ECDSA for public key, AES for symmetric key, SHA256 for hash** 

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 , Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02b)**

