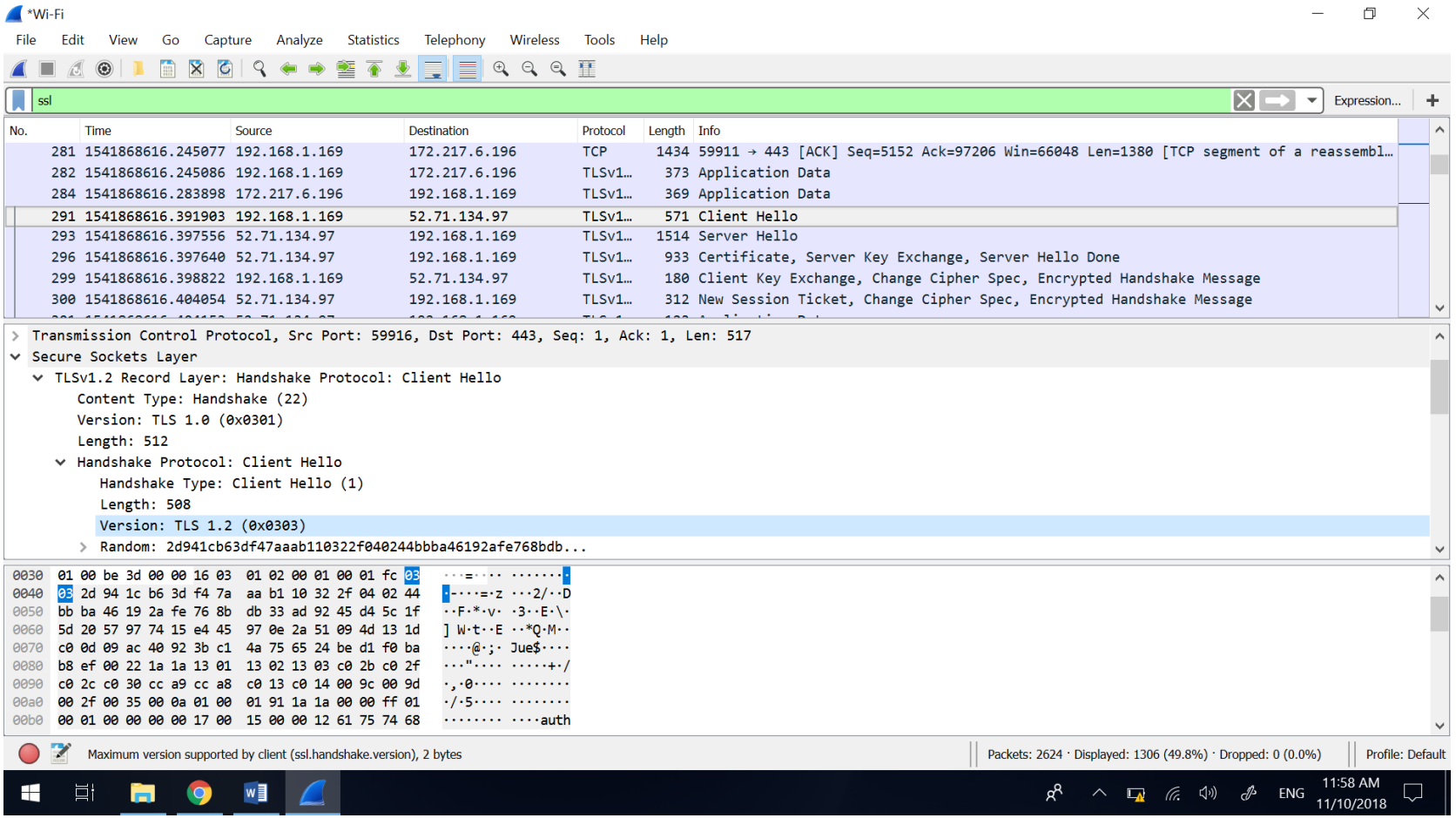
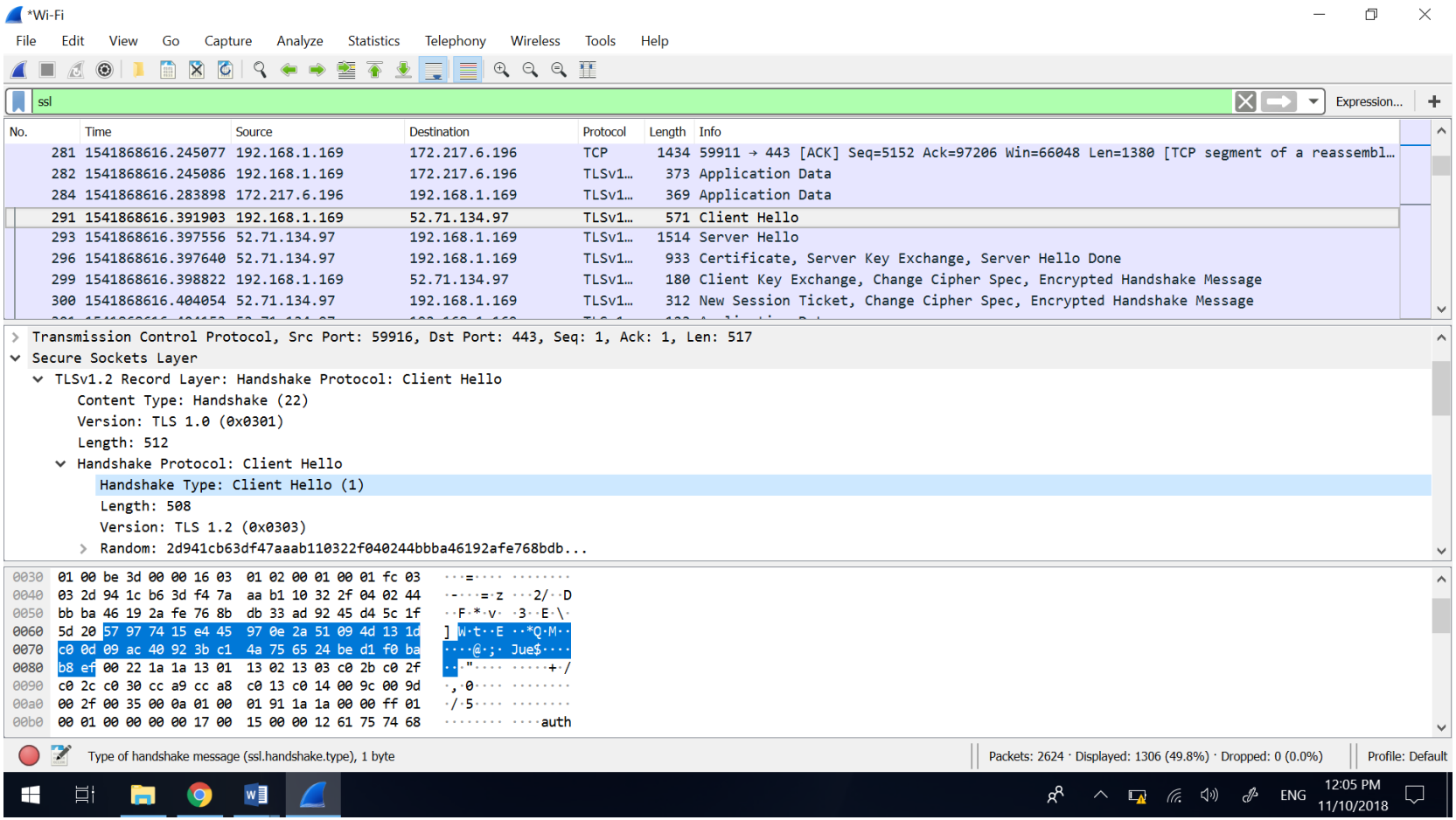
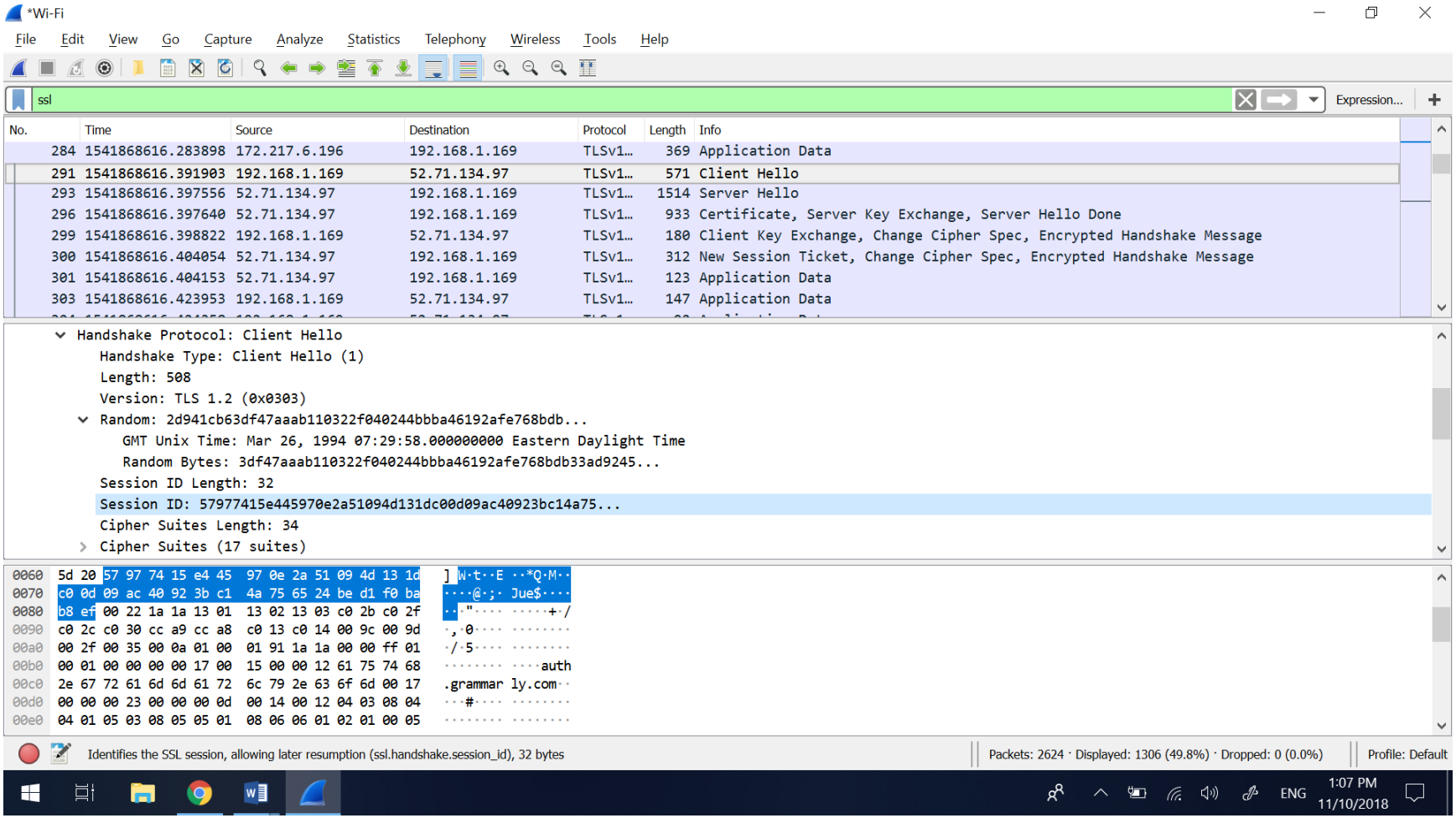
1. What is the SSL/TLS version of the of the Client Hello frame?
   Answer: Version: TLS 1.2 (0x0303)



2. Expand the ClientHello record. (If your trace contains multiple ClientHello records, expandthe frame that contains the first one.) What is the value of the content type?
Answer: Client Hello: Content Type: Handshake (22) – type 22. Handshake Type: Client Hello (1) - type 1

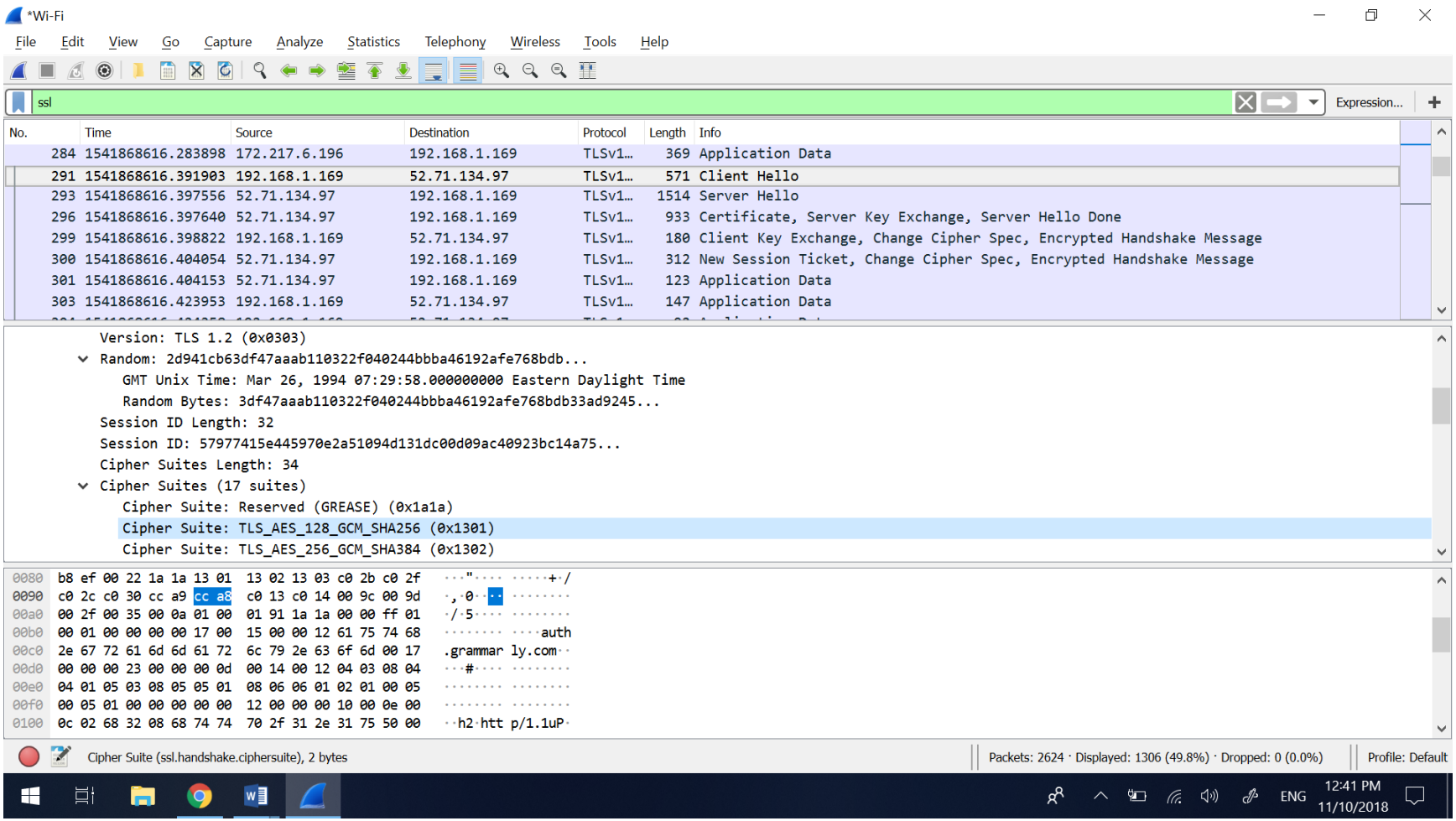


3. Does the ClientHello record containa nonce (also known as a “challenge”)? If so, what isthe value of the challenge in hexadecimal notation?
Answer: Then there is 'Random' field which contains a nonce or challenge (in hexadecimal)
3df47aaab110322f040244bbba46192afe768bdb33ad9245...



4.Does the ClientHello record advertise the cyber suites it supports? If so, in the first listedsuite, what are the public-key algorithm, the symmetric-key algorithm, and the hashalgorithm?

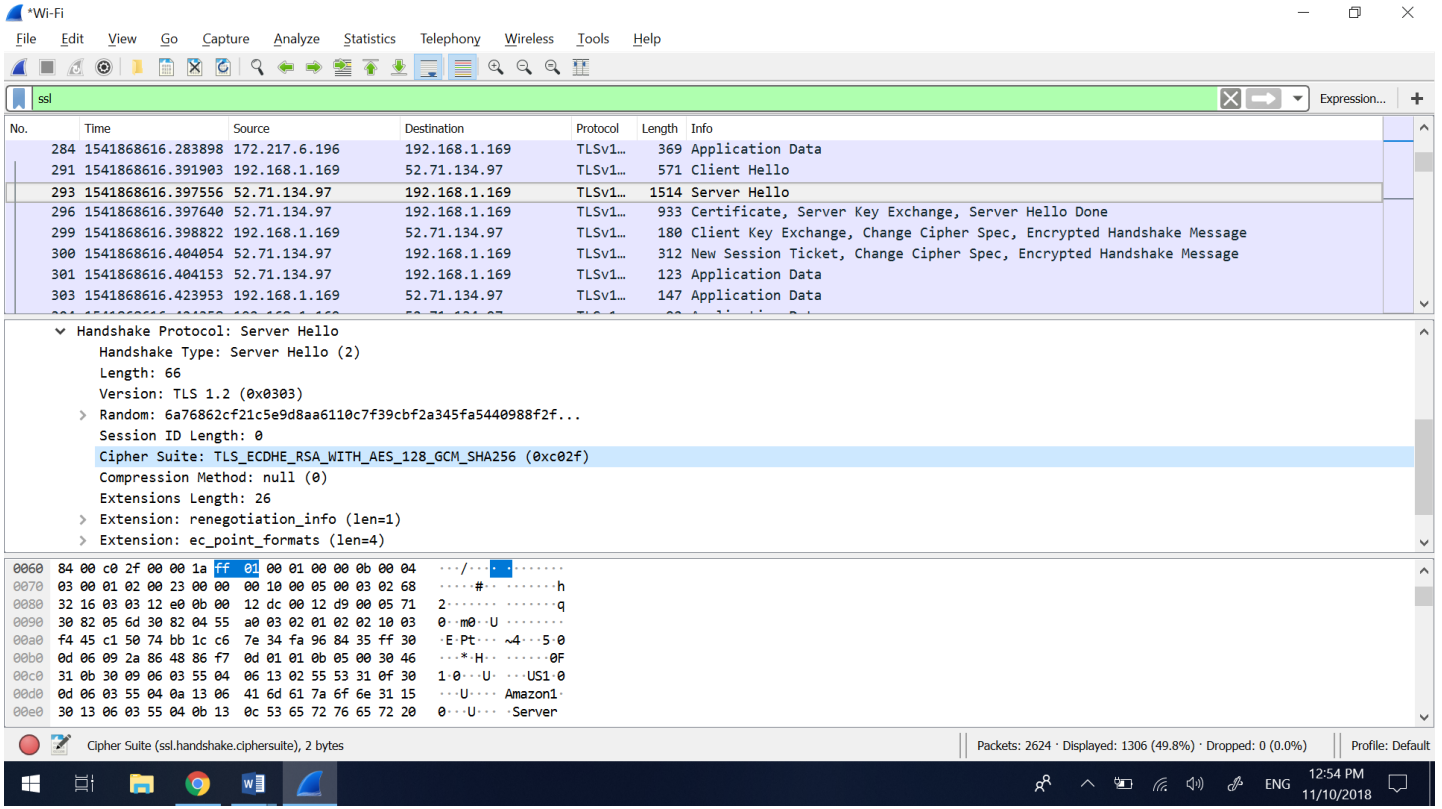
Answer: Yes. The first suite uses AES - symmetric algorithm, so it does not have public and private keys - only a shared secret., GCM 128 bites for the symmetric-key cipher and uses the SHA 256 bits hash algorithm.



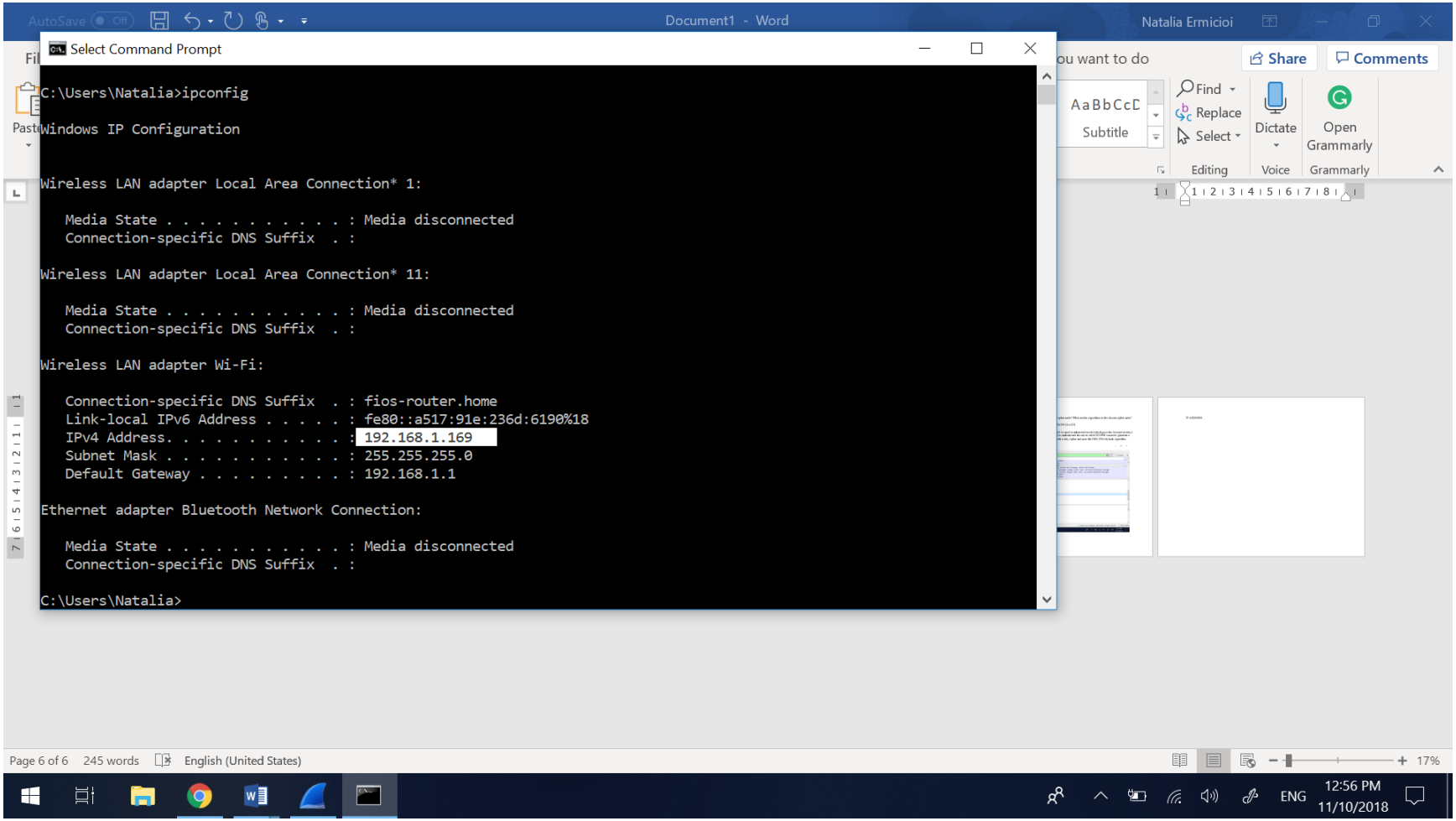
1.Locate the ServerHello SSL record. Does this record specify a chosen cipher suite? What are the algorithms in the chosen cipher suite?

Answer: Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

In our case elliptic curve diffie-hellman key exchange (ECDHE_RSA) will be used in ephemeral mode (which provides forward secrecy) and this exchange will be authenticated with RSA signature. RSA is used to authenticate the server while ECDHE is used to generate a shared secret between the client and server. GCM 128 bites for the symmetric-key cipher and uses the SHA 256 bits hash algorithm.



IP ADDRESS


Document1 - Word
Natalia Ermicioi
Select Command Prompt
C:\Users\Natalia>ipconfig
Windows IP Configuration
Wireless LAN adapter Local Area Connection* 1:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Local Area Connection* 11:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . : fios-router.home
Link-local IPv6 Address . . . . . : fe80::a517:91e:236d:6190%18
IPv4 Address. . . . . : 192.168.1.169
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
Ethernet adapter Bluetooth Network Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
C:\Users\Natalia>
Share
Comments
Find
Replace
Select
Dictate
Open Grammarly
Editing
Voice
Grammarly
Page 6 of 6
245 words
English (United States)
17%
ENG
12:56 PM
11/10/2018