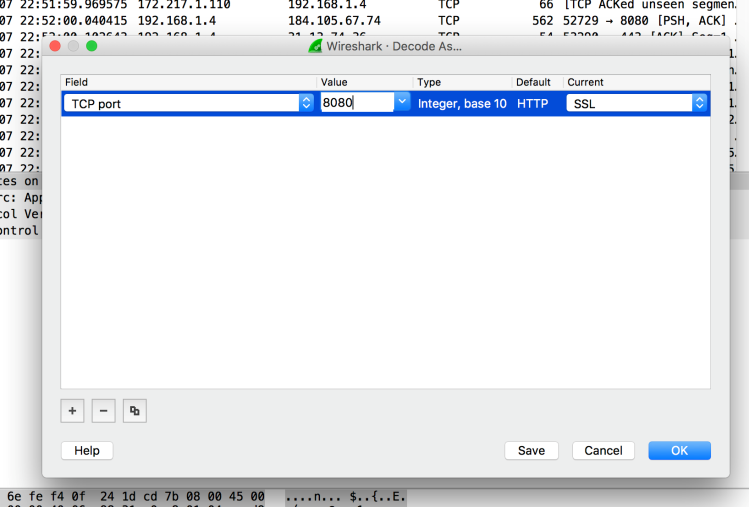


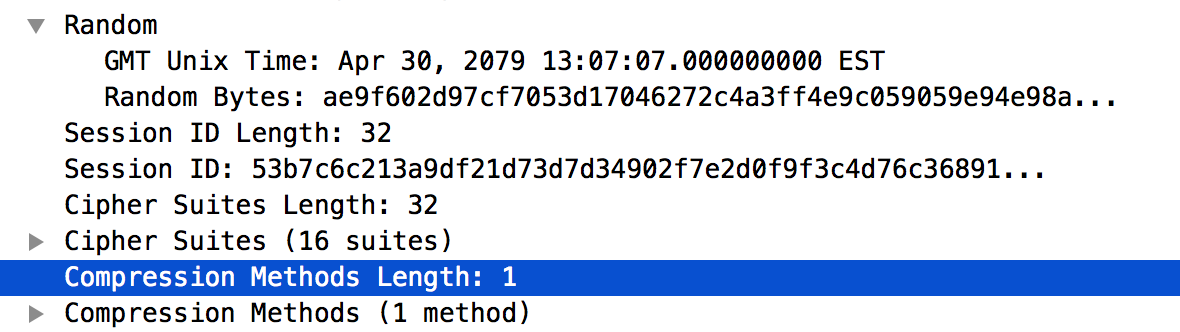
3b



3.c) Expand “cipher suites” in the “Client Hello” message.

i) How many cipher suites are supported? Ans: 16

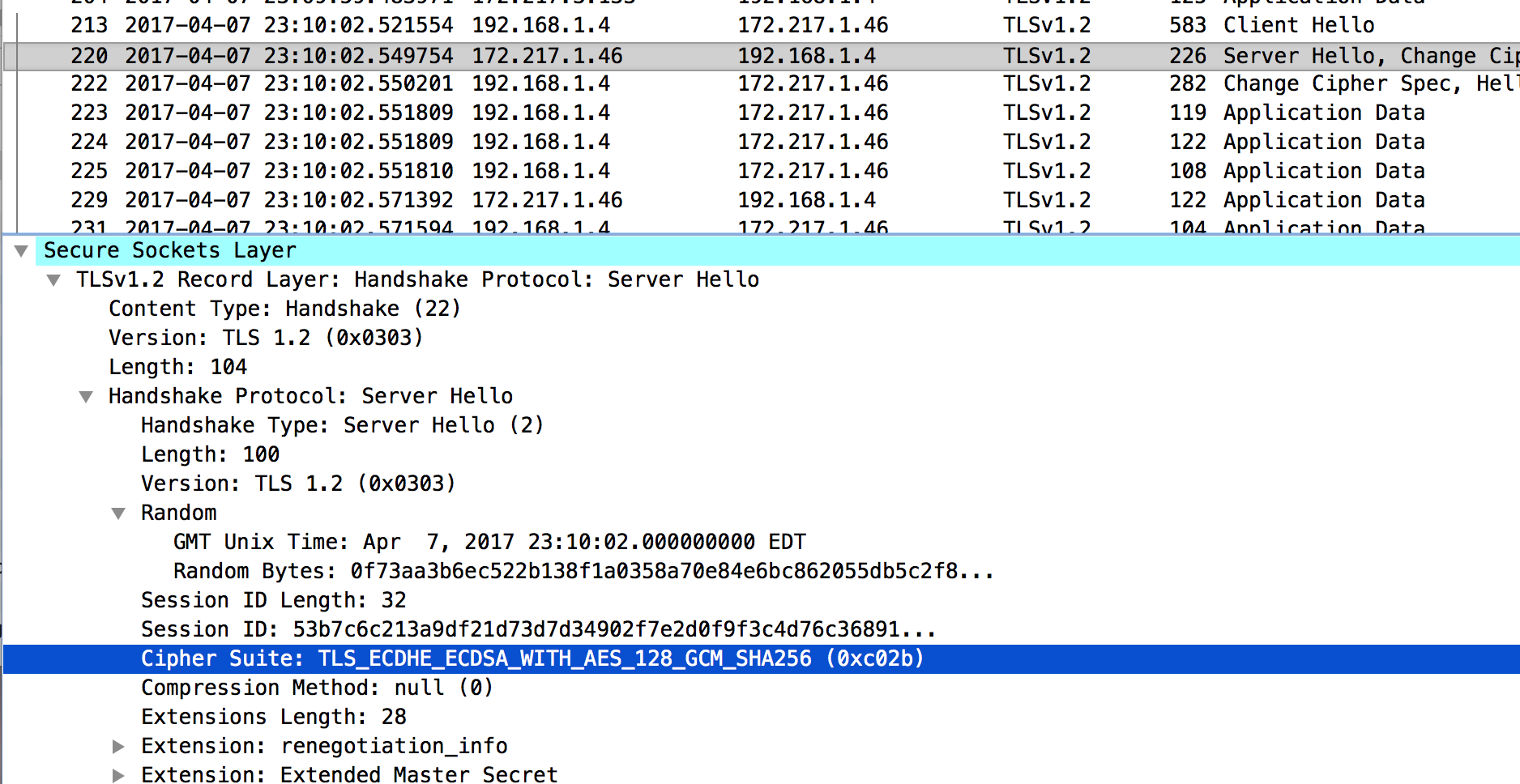
ii) what is the 28-byte nonce? AS: the 28-byte nonce is: ae9f602d97cf7053d17046272c4a



3.d) Highlight “Server Hello” message and expand the respective fields.

i) What is the cipher suite chosen by server?

ii) what is the 28-byte nonce (hint: Random -> random\_bytes)?

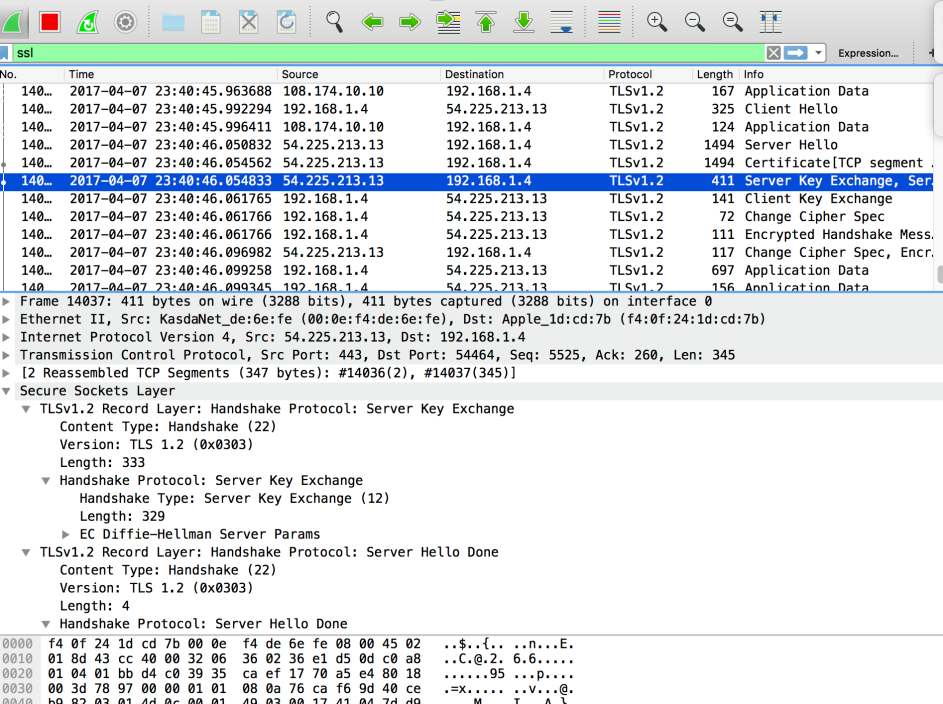


Ans:

The cipher suite chosen by server is: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 (0XC02B)

and the 28-byte nonce is: 0f73aa3b6ec522b138f1a0358a70e84e6bc

3e:



ANS: we now can see the exchange of the key and no it does not apply because it has to be http.