Assignment 3 of ELEC 473

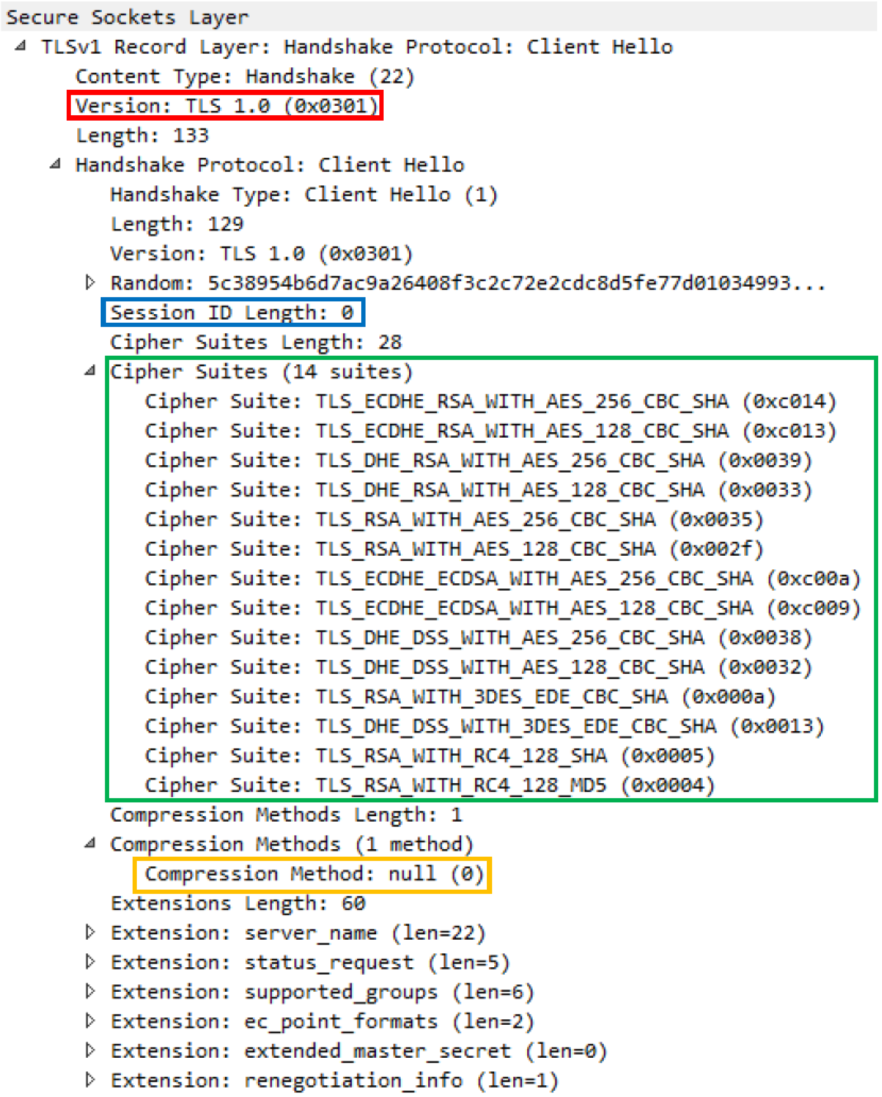
1. Give the flow diagram of TLS 1.3 and explain the information in each message of TLS 1.3 handshake protocol (e.g., Pages 15-22 in Lecture Note C10)

2. Use Wireshark to capture TLS 1.3 handshake messages for analysis.

   a. Give the screenshot of Wireshark for every message of TLS 1.3 handshake protocol and TLS 1.3 record protocol

   b. Identify the key information in each message and interpret them.

   Example:



```
Secure Sockets Layer
 ◢ TLSv1 Record Layer: Handshake Protocol: Client Hello
     Content Type: Handshake (22)
     Version: TLS 1.0 (0x0301)
     Length: 133
   ◢ Handshake Protocol: Client Hello
       Handshake Type: Client Hello (1)
       Length: 129
       Version: TLS 1.0 (0x0301)
     ▷ Random: 5c38954b6d7ac9a26408f3c2c72e2cdc8d5fe77d01034993...
       Session ID Length: 0
       Cipher Suites Length: 28
     ◢ Cipher Suites (14 suites)
         Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
         Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
         Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
         Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
         Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
         Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
         Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
         Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
         Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
         Cipher Suite: TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)
         Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
         Cipher Suite: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)
         Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
         Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
       Compression Methods Length: 1
     ◢ Compression Methods (1 method)
         Compression Method: null (0)
       Extensions Length: 60
     ▷ Extension: server_name (len=22)
     ▷ Extension: status_request (len=5)
     ▷ Extension: supported_groups (len=6)
     ▷ Extension: ec_point_formats (len=2)
     ▷ Extension: extended_master_secret (len=0)
     ▷ Extension: renegotiation_info (len=1)
```

Interpreting: xxx