1. Client Hello

Server Hello

Certificate Status, Server Key Exchange, Serve Hello Done

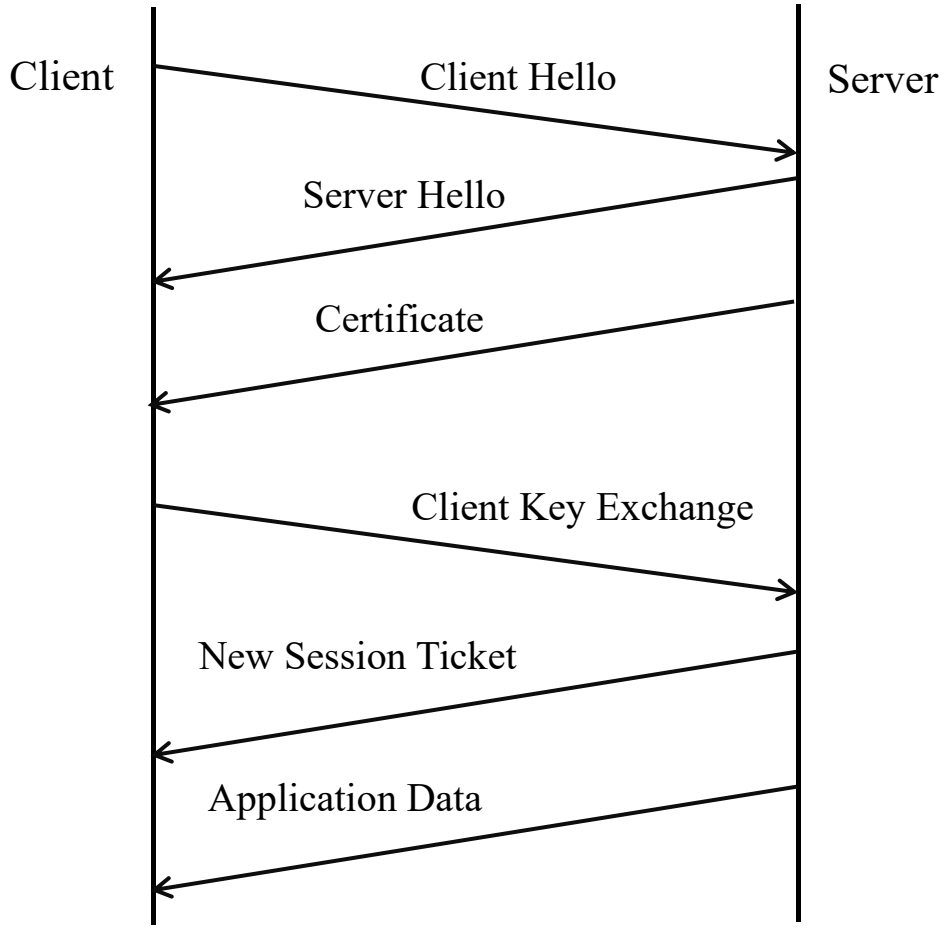
Application Data, Application Data

Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message

Application Data

New Session Ticket, Change Cipher Spec, Encrypted Handshake Message

Application Data



2. Content Type : 1 byte

   Version : 2 bytes

   Length : 2 bytes

```
TLSv1.2 Record Layer: Handshake Protocol: Client Hello
   Content Type: Handshake (22)
   Version: TLS 1.0 (0x0301)
   Length: 512
```

3. Content Type: Handshake (22)

4. Yes.

   41f4bda20d2d9e5cc14b9cd9bc5d97ff70737fbbf3bf1078...

```
Random: efe1e78aa84781e65523e6252e984a52b6fc2238e3b52c34…
   GMT Unix Time: Jul 13, 2097 21:11:38.000000000 中国标准时间
   Random Bytes: a84781e65523e6252e984a52b6fc2238e3b52c347ca56802…
```

5. Yes.

   ECDSA

   AES_128_GCM

   SHA_256

6. Yes.

   TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

```
Session ID Length: 0
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
```

7. Yes.

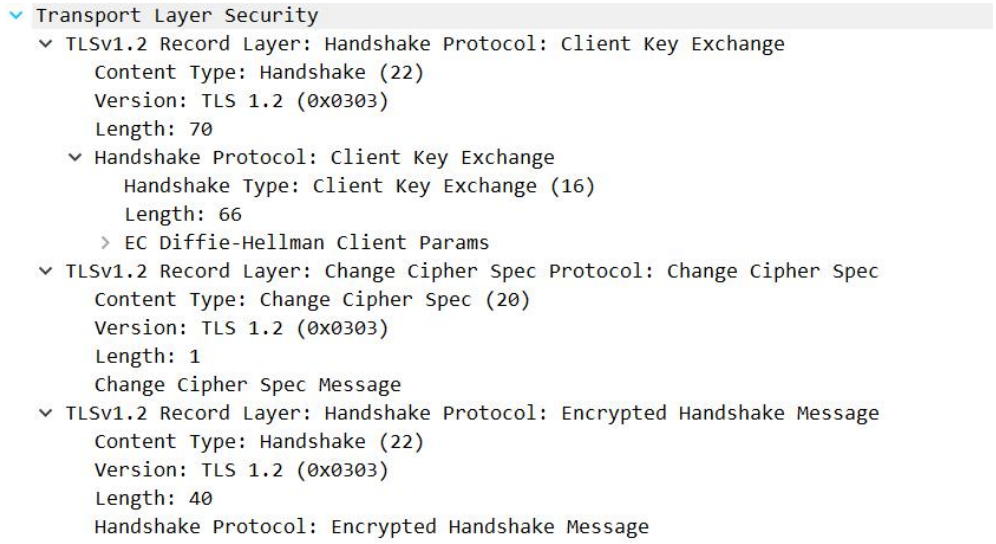
   32 bytes. Random value is used for deriving keys.

8. No ID for the first ServerHello record and Yes later.

   Session ID identifies SSL session, allowing the later resumption.

9. Certificate in a separate record, combined with Server Key Exchange.

10. Yes. It's used for generating symmetric key. It's not encrypted and is 65 bytes.
11. Show that following transmission will use the new suites and key. 1 byte.



12. Yes. By encrypted handshake message sent by client.
13. Server sent a New Session Ticket, Change Cipher Spec, Encrypted Handshake Message record. Encrypted by handshaking.
14. Encrypted by handshaking. Yes. No.
15. Client and Server use multiple conversations to make sure the transmission is secured.