Questions

1.

1. From Client / Client Hello
2. From Server / Server Hello
3. From Server / Certificate
4. From Client / Client Key Exchange
5. From Client / Application Data Protocol: http-over-tls
6. From Server / New Session Ticket

2.

Content Type (length): 1Byte

Version (length): 2 Bytes

Length (length): 2 Bytes

3.

The value of the content type is: 1

4.

ECDHE – public key

ECDSA – Private key

AES – hash algo

5.

Length: 70

6.

They use a symmetric key algo

7.

Yes, they do

8.

No, they don’t