**TASK 2**

**HTTPS PACKET TRACING :**

**QUESTION 1 :**

What is the name of website?

**ANSWER 1 :**

The name of website is (mblock.cc)

**QUESTION 2 :**

Find the packet that contains the ClientHello message for the website you are accessing.

**ANSWER 2 :**

ClientHello message for the website I am accessing is (Packet No. 813 (Client Hello (SNI = mblock.cc)))

**QUESTION 3:**

List all the TLS extensions included in the ClientHello?

**ANSWER 3 :**

* The ClientHello includes the following TLS extensions:
* Reserved (GREASE)
* server\_name = mblock.cc
* Unknown type 17613
* status\_request
* ec\_point\_formats
* psk\_key\_exchange\_modes
* encrypted\_client\_hello
* supported\_versions = TLS 1.3, TLS 1.2
* extended\_master\_secret
* key\_share (X25519MLKEM768, x25519)
* supported\_groups
* signed\_certificate\_timestamp
* compress\_certificate
* signature\_algorithms
* renegotiation\_info
* application\_layer\_protocol\_negotiation (ALPN)
* session\_ticket
* Reserved (GREASE again)

**QUESTION 4 :**

Identify the ServerHello message. What cipher suite is chosen by the server?

**ANSWER 4 :**

The ServerHello is shown in Packet No. 8316 is:

**TLS version**: TLS 1.2 (0x0303)

**Cipher Suite chosen by the server**: **TLS\_AES\_128\_GCM\_SHA256 (0x1301)**

**QUESTION 5 :**

Locate the Certificate message. Extract the server’s certificate information (issuer, subject, validity dates).

**ANSWER 5 :**

**ISSUED TO** : mblock.cc

**ISSUED BY** : WE1 (Google trust service)

**ISSUE DATE**: Saturday,August2 ,2025 at 11:06pm

**EXPIRES ON** : Saturday,November1,2025,12:06am

**Subject:** CN = mblock.cc

**QUESTION 6 :**

After the TLS handshake, identify the first encrypted application data packet. Why can’t you directly see the HTTP headers in this packet?.

**ANSWER 6 :**

The first encrypted application data packet appears immediately after the TLS handshake (e.g., Packet No. 814). So we cannot directly see the HTTP headers in this packet because the HTTP data is encrypted inside TLS to ensure confidentiality and security.