Task 5:

For the HTTPS based website access, answer the following::

1. **What is the name of website?**
   wikipedia.org

2. **Find the packet that contains the ClientHello message for the website you are accessing.**
   First TLS message from client after TCP handshake (Client Hello).

3. **List all the TLS extensions included in the ClientHello.**
   SNI (wikipedia.org), supported versions, key share, signature algorithms, ALPN, etc.

4. **Identify the ServerHello message. What cipher suite is chosen by the server?**
   Server chooses TLS version and cipher suite (e.g., TLS_AES_128_GCM_SHA256).

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

   Issuer: trusted CA (like DigiCert), Subject: wikipedia.org, validity dates (Not Before/Not After).

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

   First Application Data packet after handshake. HTTP headers are not visible because they are encrypted.