

**Computer Network**

**Task No 02**

Submitted by: **Umair Tariq**

Registration No: **B23F0662AI103**

Submitted to:**Dr. Adnan Iqbal**

Date:**22-09-2025**

https://lh7-rt.googleusercontent.com/docsz/AD_4nXdVQ8OUBR_dhCrOWV1vxlqoLBzyJs70xCYbzvgAIFmfaWpFIdo2pXDaYOKmtp_vrwUYfft8dgX6ZR4ULRPnkssCqn40PP5czpDoNF8Wv8rX95d9oFefvexKWheM6s0jgWZ-dZ4C1u_sld56EN9HgaXiiTc?key=Wa7SeqjkZKC1QT8VhWH50Q **Assignment N0 01**

**Task NO 02:**

**For HTTPs:**

For the HTTPS based website access, answer the following:

7. What is the name of website?

**Solution:**

**Name of the Website:**

The name of the Website is  **google.com**.

**Explanation:**  
 From the TLS trace, the server IP address (for example 34.223.124.45) resolves to Google’s servers. In the ClientHello “Server Name Indication (SNI)” extension you can see the hostname sent by the browser, which is **google.com**.

**Conclusion:**  
 We can concluded that HTTPS website accessed is **google.com**.

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

**Solution:**

**Packet Containing the ClientHello Message:**

**Explanation:**  
 The ClientHello message is the first step of the TLS handshake. In Wireshark you can identify it by the “Info” column showing “TLSv1.2 Client Hello” or “TLSv1.3 Client Hello” sent from your client IP (10.1.77.141) to the server IP (34.223.124.45).

**Conclusion:** We can concluded that earliest packet labelled Client Hello from 10.1.77.141 to 34.223.124.45 is the ClientHello message for google.com.

9. List all the TLS extensions included in the ClientHello.

**Solution:**

**TLS Extensions in the ClientHello:**

**Explanation:**  
 By expanding the ClientHello in Wireshark you can list all extensions proposed by your browser. Common ones you will see for Google include:

* Server Name Indication (SNI = google.com)
* Supported Versions (TLS 1.2, TLS 1.3)
* Supported Cipher Suites
* Signature Algorithms
* Key Share (TLS 1.3)
* ALPN (h2, http/1.1)

**Conclusion:**  
 We can concluded that Open the “Extensions” section under the ClientHello packet to view each extension and its values.

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

**Solution:**

**ServerHello Message and Cipher Suite:**

**Explanation:**  
 The server responds with a ServerHello selecting one cipher suite from the list offered by the client. For Google you typically see something like:  
TLS\_AES\_256\_GCM\_SHA384 (TLS 1.3) or TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (TLS 1.2).

**Conclusion:**  
 We can concluded that ServerHello from 34.223.124.45 to 10.1.77.141 contains the chosen cipher suite for the connection to google.com.

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

**Solution:**

**Certificate Message and Server Certificate Details:**

**Explanation:**  
 After the ServerHello, the server sends its certificate. Expanding “Handshake Protocol: Certificate” in Wireshark shows:

* **Subject:**

CN=\*.google.com

* **Issuer:**

Google Trust Services / GlobalSign (or similar)

* **Validity:**

Start and End dates (for example, valid from 15-Aug-2025 to 15-Nov-2025).

**Conclusion:**  
 We can concluded that certificate message confirms the server’s identity as google.com and shows its issuer and validity period.

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

**Solution:**

**First Encrypted Application Data Packet:**

**Explanation:**  
 After the TLS handshake is complete, packets labelled “TLS Application Data” appear. These packets contain the encrypted HTTP requests and responses. You cannot view HTTP headers directly because TLS encrypts them to provide confidentiality.

**Conclusion:**  
 We can concluded that first “TLS Application Data” packet after the handshake is your first encrypted application data. Its contents are unreadable because HTTPS hides HTTP headers and body inside TLS encryption.

**CONCLUSION:**

By concluding the TLS handshake in Wireshark we can determine that:

* The accessed site is google.com.
* The ClientHello shows SNI and extensions.
* The ServerHello indicates the chosen cipher suite.
* The Certificate reveals issuer, subject, and validity.
* After the handshake, “TLS Application Data” appears where HTTP headers are encrypted.

**Thank You**