**Task 5: HTTPS Website Analysis**

**7. What is the name of the website?**

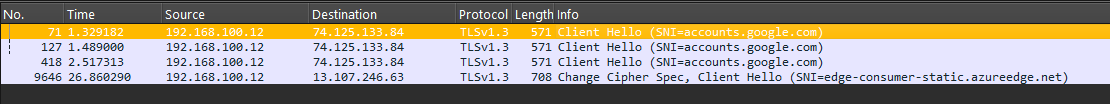
The website accessed is **accounts.google.com**

A screenshot of a computer

AI-generated content may be incorrect.

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

The **ClientHello** message is found at **Packet Number 71 .**



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

The following TLS extensions were included in the **ClientHello** message:

* Server Name Indication (SNI): [accounts.google.com]
* Supported Groups: [x25519, secp256r1,x448]
* Signature Algorithms: [ecdsa\_secp256r1\_sha256]
* Key Share: [x25519]
* Supported Versions: [TLS 1.2, TLS 1.3 , TLS 1.1 , TLS 1,0]

A screenshot of a computer

AI-generated content may be incorrect.

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

The **ServerHello** message is found at **Packet Number 47**

* **TLS Version:** [ TLS 1.3]
* **Cipher Suite chosen by server:** [TLS\_AES\_128\_GCM\_SHA256]

A screenshot of a computer

AI-generated content may be incorrect.

A computer screen shot of a computer

AI-generated content may be incorrect.

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

The website uses **TLS 1.3** and the certificate message is encrypted in Wireshark. So, it is not visible in the recorder packets.

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

The first **Application Data** packet is found at **Packet Number 72 .**  
This packet contains encrypted data.

* **Observation:** The actual HTTP request/response headers are not visible.
* **Reason:** After TLS handshake completes, all HTTP traffic is encrypted inside TLS records for confidentiality and security. Without decryption keys, Wireshark cannot display the HTTP headers or content.

A screenshot of a computer

AI-generated content may be incorrect.