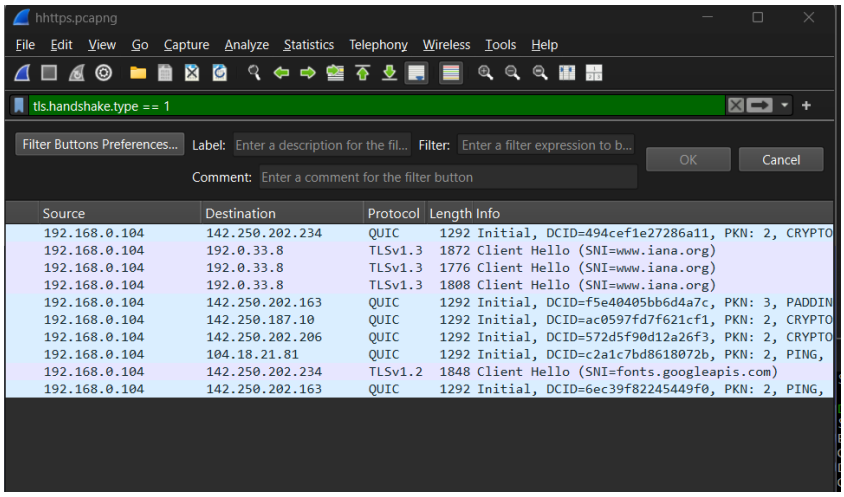
Task 5: HTTPS Traffic Analysis

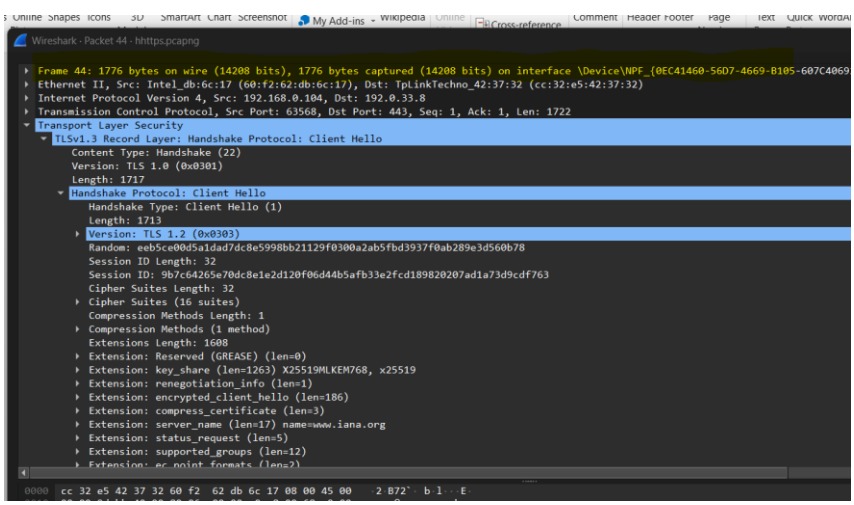
Q1. Identify the website to which the client is connecting.

The client is connecting to the website: **www.iana.org**
This was identified from the TLS Client Hello message (SNI extension).



Q2. Find the Client Hello message in the capture. Which frame contains it?

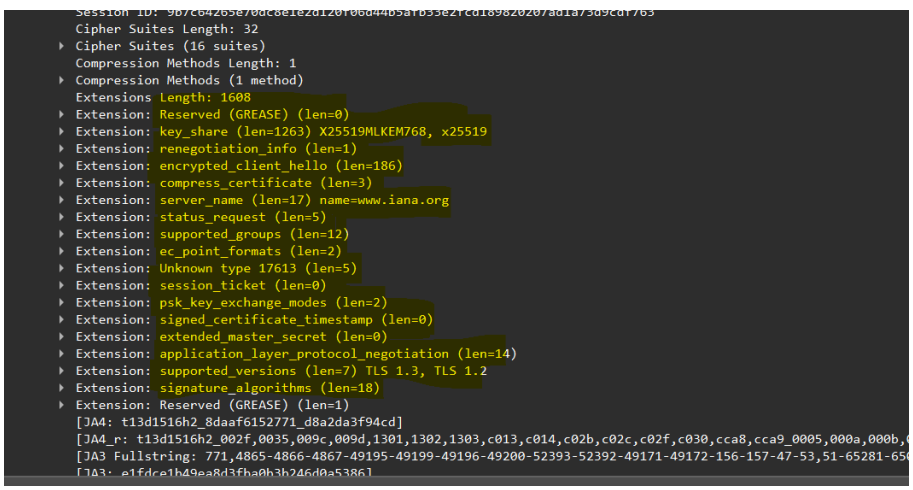
The Client Hello message is found in Frame 44.
This marks the beginning of the TLS handshake initiated by the client.



Q3. List the extensions present in the Client Hello message.

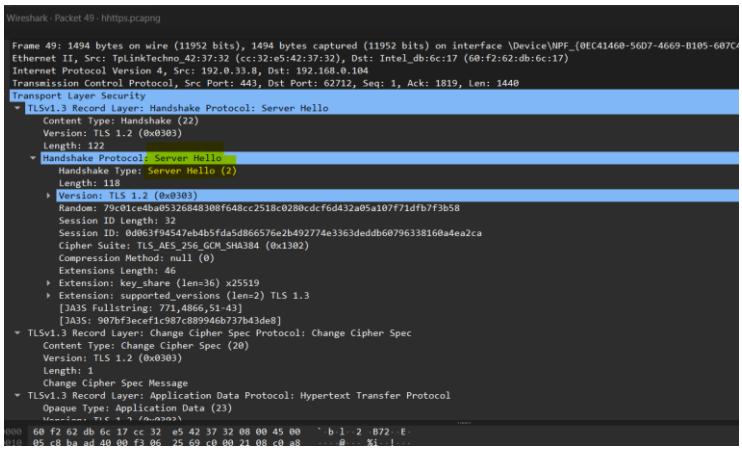
The Client Hello message (Frame 44) includes several extensions, such as:

- Reserved (GREASE)
- key_share (X25519MLKEM768, x25519)
- renegotiation_info
- encrypted_client_hello
- compress_certificate
- server_name (www.iana.org)
- status_request
- supported_groups
- ec_point_formats
- Unknown type 17613
- session_ticket
- psk_key_exchange_modes
- signed_certificate_timestamp
- extended_master_secret
- application_layer_protocol_negotiation
- supported_versions (TLS 1.3, TLS 1.2)
- signature_algorithms
- Reserved (GREASE)



Q4. Find the Server Hello message in the capture. Which frame contains it, and which cipher suite is selected?

The Server Hello message is found in Frame 49.
The selected cipher suite is: TLS_AES_256_GCM_SHA384.



Q5. Examine the Certificate message. Provide details of the certificate.

In TLS 1.3, the Certificate message is encrypted after the ServerHello, so Wireshark does not display it in the capture.
Therefore, we retrieved the certificate directly from the server using OpenSSL.

Details of the certificate for www.iana.org:
- Subject: C = US, ST = California, O = Internet Corporation For Assigned Names and Numbers, CN = *.iana.org
- Issuer: C = GB, ST = Greater Manchester, L = Salford, O = Sectigo Limited, CN = Sectigo RSA Organization Validation Secure Server CA
- Validity:
  - Not Before: Dec 6, 2024
  - Not After: Jan 5, 2026
- Public Key Algorithm: RSA 4096-bit
- Signature Algorithm: RSA-SHA256

Q6. Find the first packet containing encrypted application data. Which frame is it, and why can't you see the HTTP headers?

The first encrypted Application Data is found in Frame 49.
The HTTP headers are not visible because in HTTPS, all HTTP payloads are encrypted inside TLS Application Data records. Without the decryption keys, Wireshark cannot reveal the actual HTTP hedars