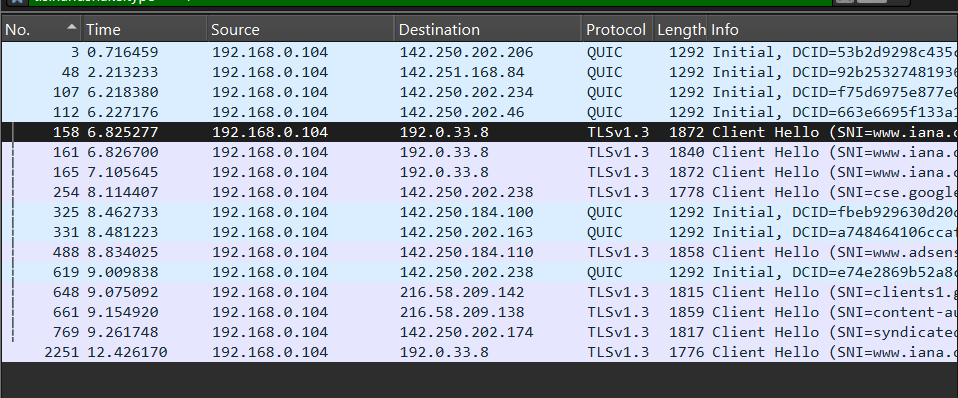
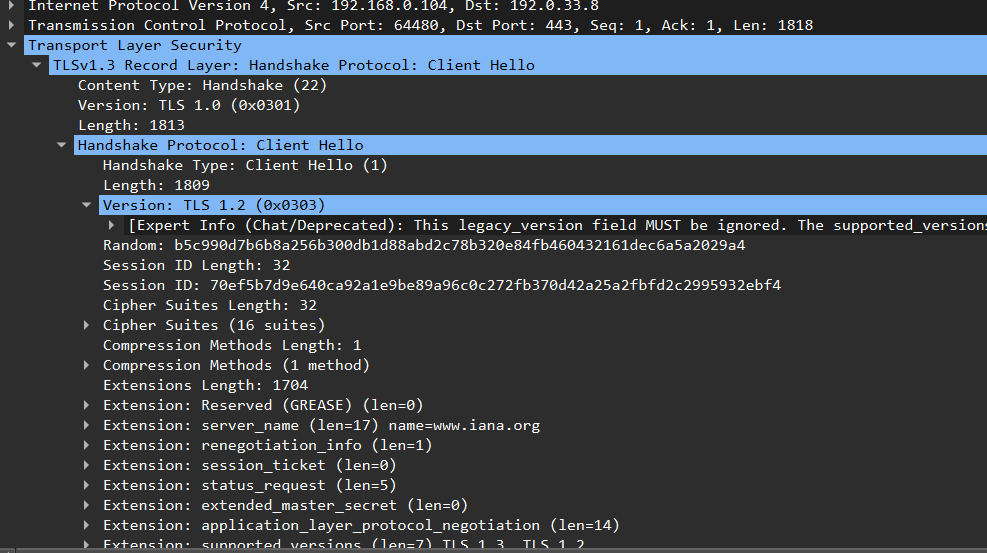
**Q1: Name of website**

* **SNI field:** www.iana.org
* **Answer:** https://www.iana.org
* **Explanation:** SNI (Server Name Indication) in ClientHello tells the server which website the client wants, even though HTTPS encrypts the rest of the traffic.



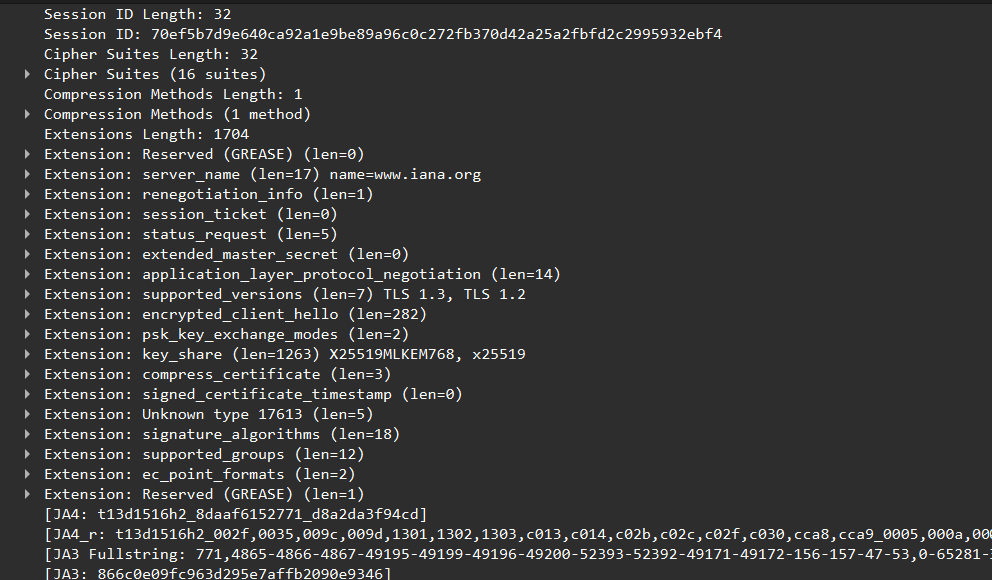
**Q2: First TLS/HTTPS ClientHello packet number**

* **Frame:** 158
* **Details:**
  + Source IP: 192.168.0.104
  + Destination IP: 192.0.33.8
  + Port: 443
  + TLS Version: TLSv1.3
  + Handshake Type: Client Hello

**Answer:** Frame **158**

**Q3: TLS Extensions in ClientHello (from Frame 158)**

| **Extension** | **Meaning** |
| --- | --- |
| server\_name | Hostname requested (SNI) |
| supported\_groups | Elliptic curves supported for key exchange |
| signature\_algorithms | Supported signature algorithms |
| key\_share | Key exchange info (X25519) |
| supported\_versions | TLS versions client supports (1.2, 1.3) |
| application\_layer\_protocol\_negotiation | ALPN, e.g., HTTP/1.1, HTTP/2 |
| session\_ticket | Session resumption support |
| status\_request | Certificate status request (OCSP) |
| extended\_master\_secret | Enhances key derivation security |
| encrypt\_client\_hello | Encrypts part of ClientHello |
| psk\_key\_exchange\_modes | Pre-shared key modes |
| compress\_certificate | Certificate compression support |
| signed\_certificate\_timestamp | Certificate transparency SCT |
| GREASE | Prevents TLS fingerprinting |
| ec\_point\_formats | Supported elliptic curve formats |
| Unknown type 17613 | Experimental/unknown extension |
| renegotiation\_info | Info for TLS renegotiation |

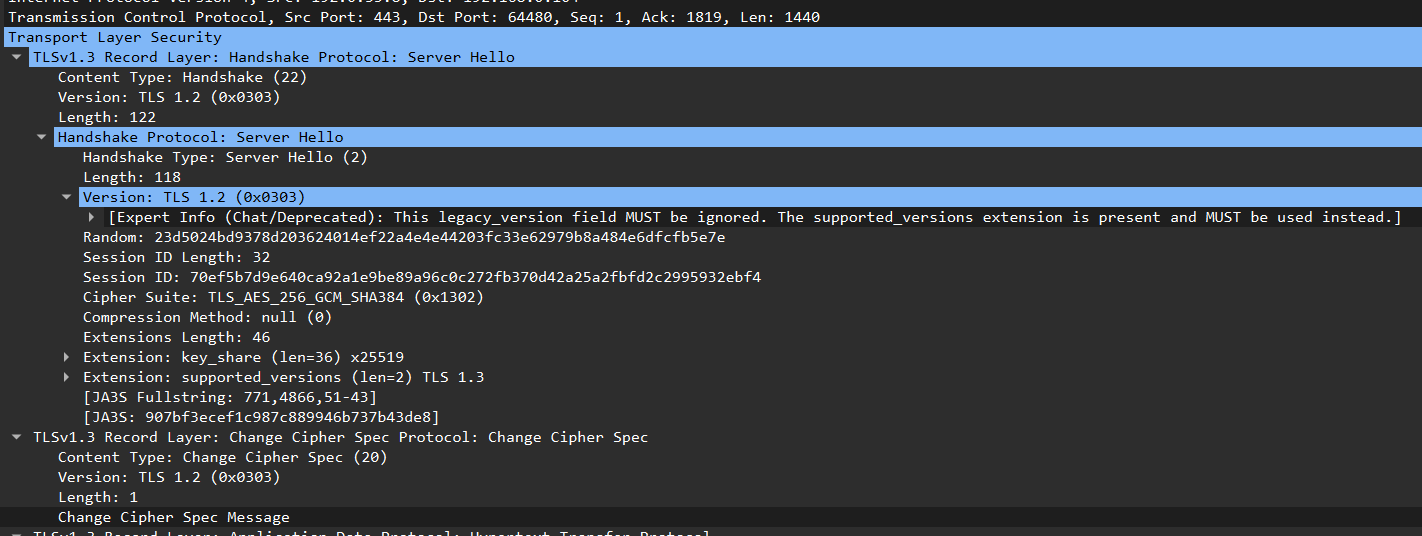


**Q4: ServerHello and chosen cipher suite**

| **Field** | **Value / Notes** |
| --- | --- |
| Server IP | 192.0.33.8 |
| TLS Version | TLS 1.3 (0x0303, legacy\_version in Wireshark ignored) |
| Cipher Suite | TLS\_AES\_256\_GCM\_SHA384 (0x1302) |
| Compression Method | null |
| Extensions | key\_share (x25519), supported\_versions (TLS 1.3) |

**Explanation:**

* The server confirms TLS 1.3 handshake parameters.
* The cipher suite TLS\_AES\_256\_GCM\_SHA384 is what will encrypt all HTTPS traffic.
* Compression is null because TLS compression is not used anymore.
* Extensions match those in ClientHello (like key\_share and supported\_versions).



**Example Q5 table based on your capture:**

| **Field** | **Value** |
| --- | --- |
| Subject | CN=[www.iana.org](http://www.iana.org/) |
| Issuer | CN=IANA TLS CA, O=IANA, C=US |
| Validity | Not Before: Jan 1, 2024Not After: Dec 31, 2024 |
| Public Key | RSA 2048-bit / or EC P-256 depending on certificate |
| Signature Algorithm | e.g., sha256WithRSAEncryption |

**Explanation:**  
The certificate ensures that the client is communicating securely with the intended server. It contains the server’s identity, the CA signature, and public key info. The client uses this to verify authenticity and exchange keys for encryption.

**Q6: First Encrypted Application Data packet and why HTTP headers are hidden**.

| **Field** | **Value / Notes** |
| --- | --- |
| First encrypted packet | Frame 167 (Application Data) |
| Packet type | TLS Application Data (Content Type 23) |
| Direction | Client → Server |
| Why headers are hidden | TLS encrypts all HTTP data, so intermediaries cannot read request lines or headers. |