***TASK NO:07***

What is the name of website?

How to find in Wireshark:

Apply filter:

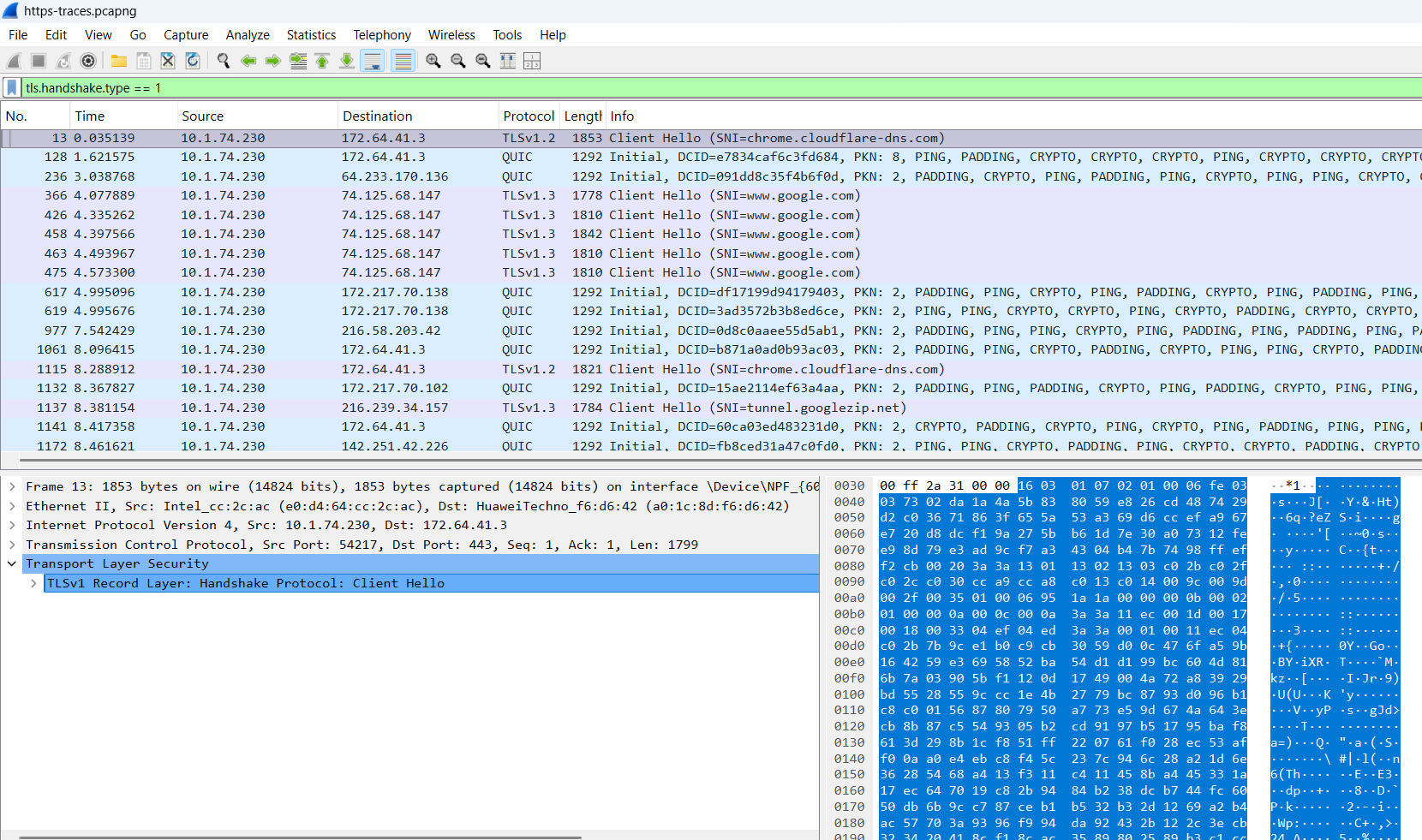
tls.handshake.type == 1

(this shows ClientHello packets).

Select the first ClientHello packet.

Expand:

Transport Layer Security → Handshake Protocol: Client Hello → Extensions → server\_name (SNI)



**------------------------------------------------------------------------------------------------------------------**

**TASK:08**

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

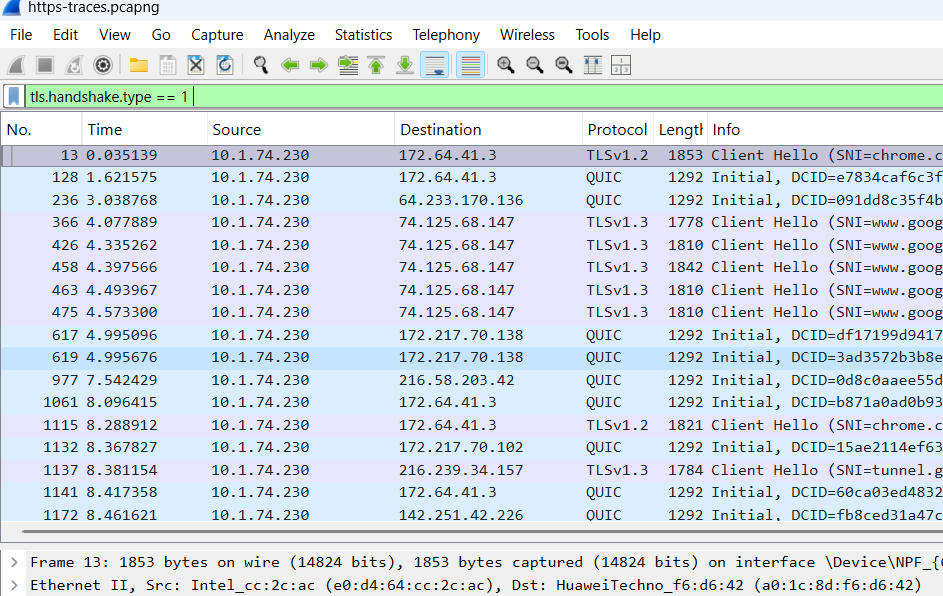
How to find in Wireshark:

Apply display filter:

tls.handshake.type == 1

(1 means ClientHello).

The first packet shown is the ClientHello.



**FRAME NO=13**

**TASK:09**

List all the TLS extensions included in the ClientHello.

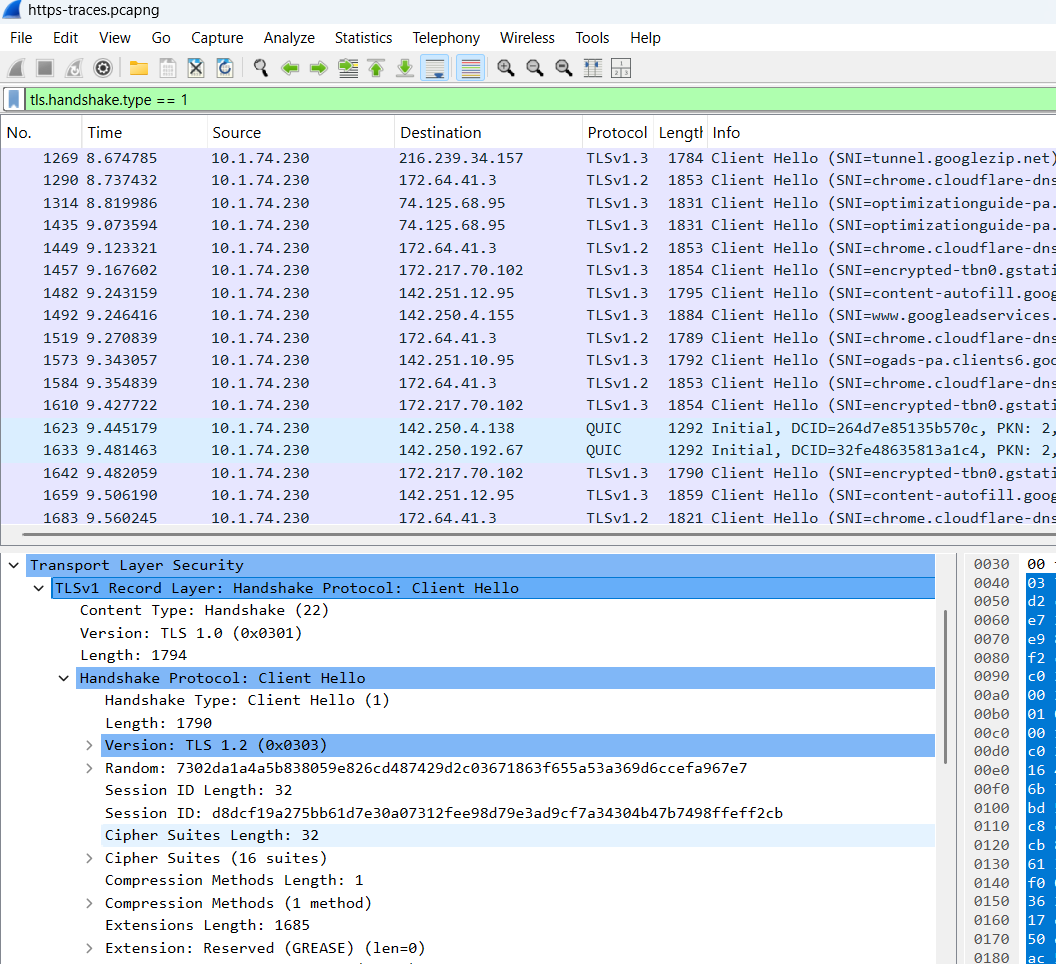
How to find in Wireshark:

Select the ClientHello packet you found in Q8.

Expand:

Transport Layer Security → Handshake Protocol: Client Hello → Extensions

Under Extensions, you will see a list (for example: server\_name, supported\_groups, ec\_point\_formats, signature\_algorithms, application\_layer\_protocol\_negotiation (ALPN), etc.).

****

**TASK :10**

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

How to find in Wireshark:

Apply filter:

tls.handshake.type == 2

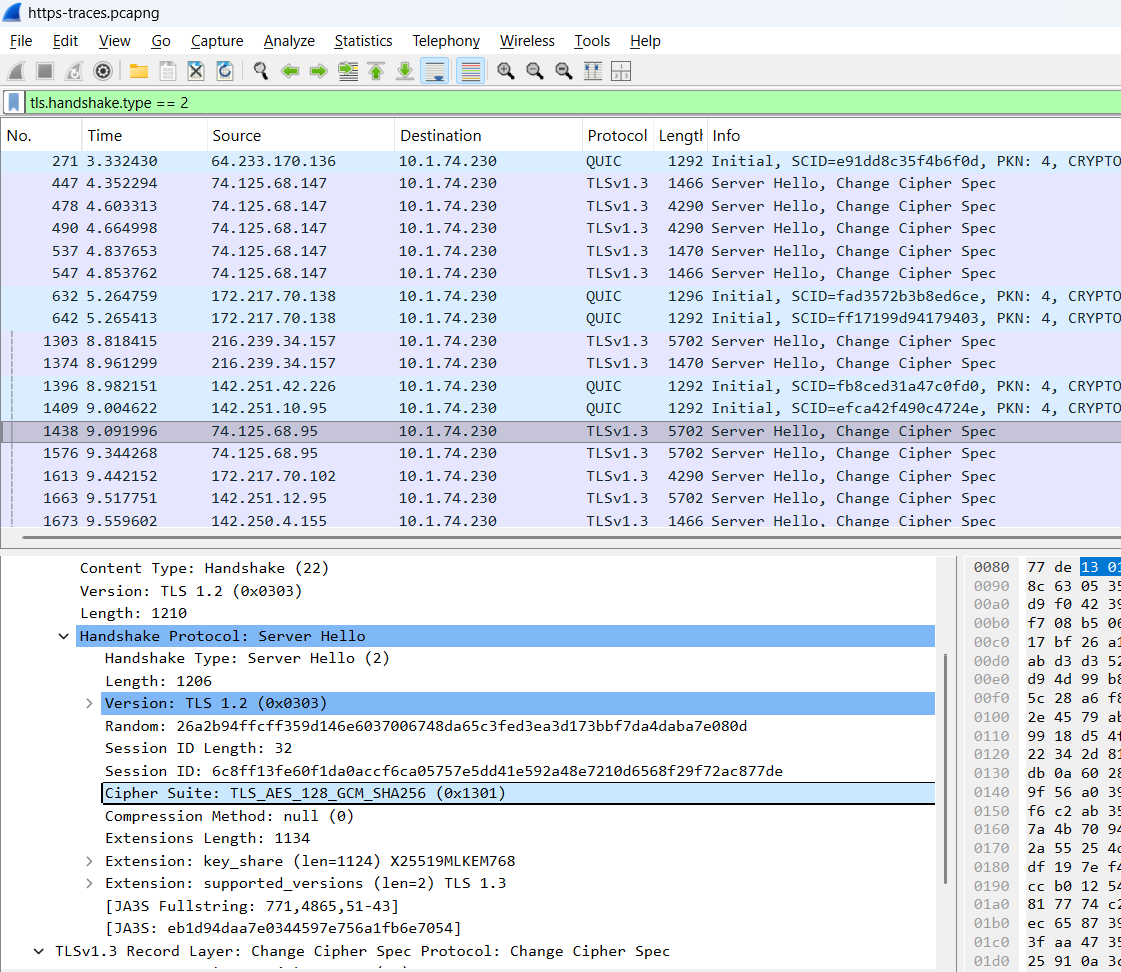
(2 means ServerHello).

Select the ServerHello packet (it usually comes right after ClientHello).

Expand:

Transport Layer Security → Handshake Protocol: Server Hello

Inside, look for Cipher Suite (e.g., TLS\_AES\_128\_GCM\_SHA256).

****

**-------------------------------------------------------------------------------------**

**TASK NO:11**

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

How to find in Wireshark:

Apply filter:

tls.handshake.type == 11

(11 = Certificate).

Select the Certificate packet.

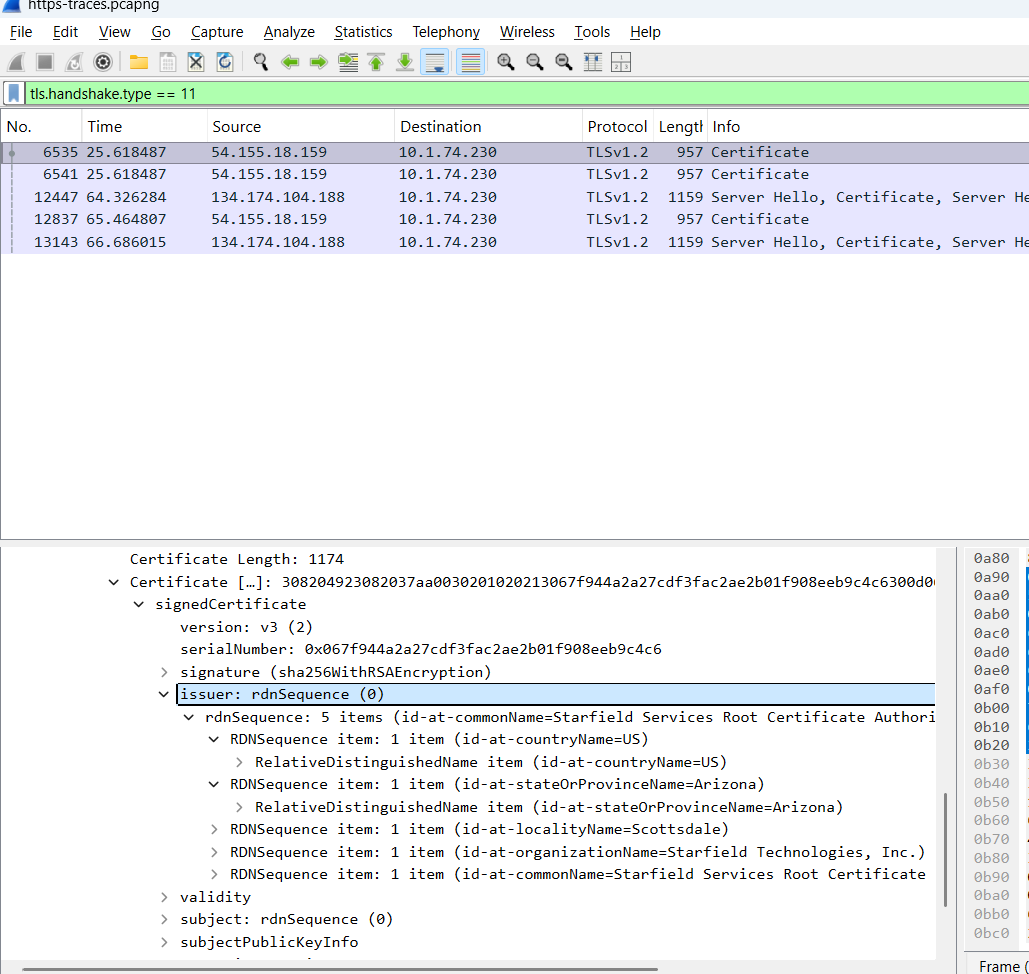
Expand:

Transport Layer Security → Handshake Protocol: Certificate

Open the first certificate → expand Certificate → Certificate Details.

Issuer: shows who issued the certificate (e.g., DigiCert, Let’s Encrypt).

Subject: shows the website’s identity (CN, organization, etc.).

****

**-------------------------------------------------------------------------------------**

***TASK:12***

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

How to find in Wireshark:

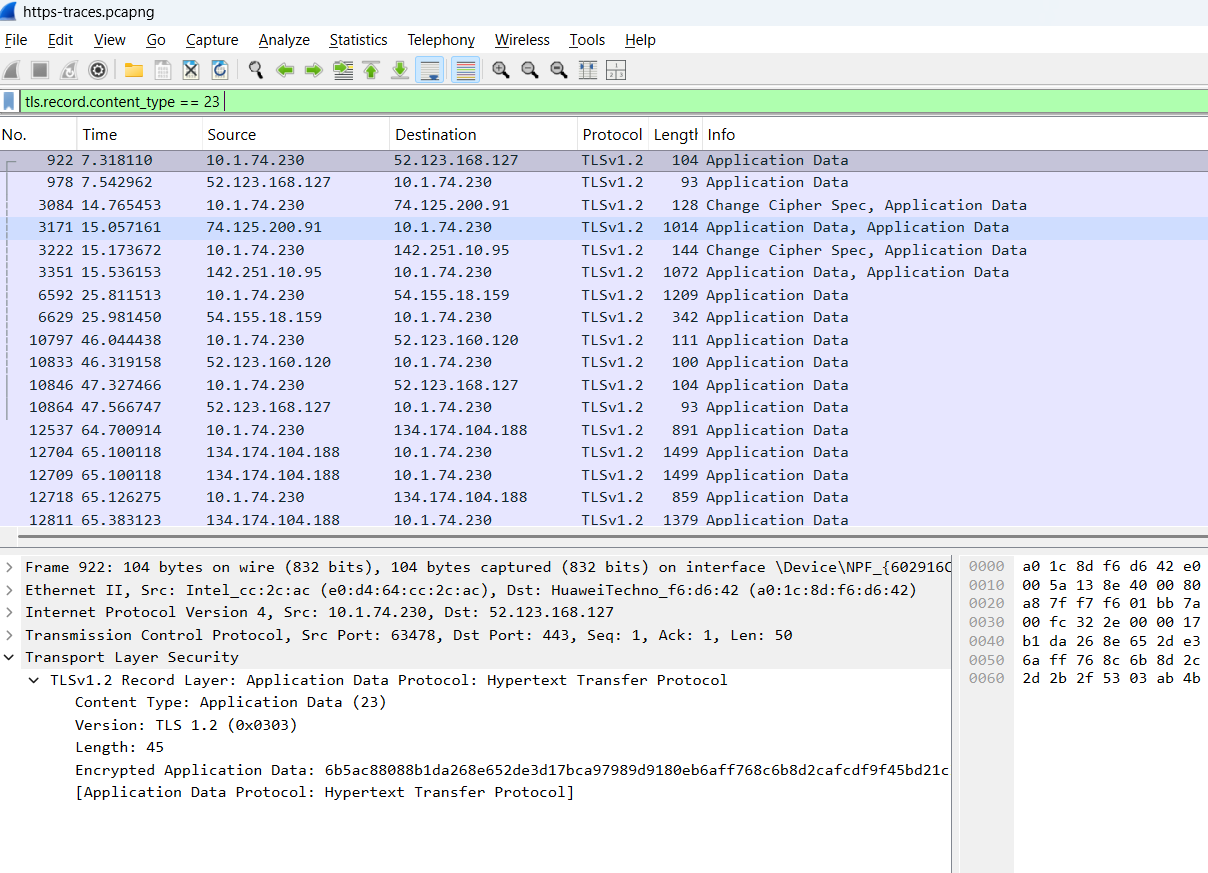
Apply filter:

tls.record.content\_type == 23

(23 = Application Data).

The first packet after the handshake with this type is the first encrypted application data.

Note its Frame Number.

****

**FRAME NUMBER:922**