**Certificates Assignment**

**Group Members:** Nina Onwuachi (10190678)

                     Sarah Kaunain Syeda (30220873)

                                 Abigail Brown (30214975)

**Exercise 1**

1. 04bd936cd506be6d93c6878d6a3d8af29832

2. DST Root CA X3

3. Wed, 27 Dec 2023 21:46:20 UTC

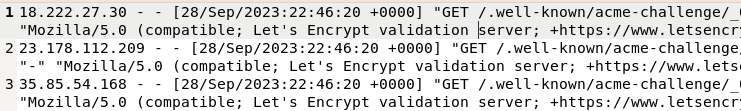
4. Line 4 is triggering all the secure HTTPS requests after that, hence line 4 corresponds to an access of the website using TLS.

**Exercise 2**

1. IP1: 18.222.27.30

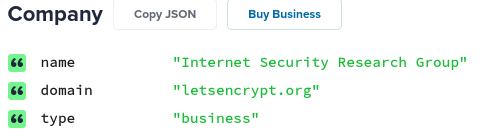
    IP2: 23.178.112.209

    IP3: 35.85.54.168

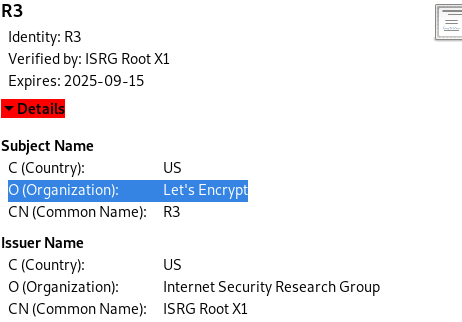


2. Yes

Domain of IP2 is:



The organization to issue the certificate is also Let’s encrypt:



Hence the IP address corresponds to our CA.

3. GET/.well-known/acme-challenge/\_0gAsUtno\_aSVmEPVvbSMnbXWguoLrsx\_OWIwqKmXQw

4.\_0gAsUtno\_aSVmEPVvbSMnbXWguoLrsx\_OWIwqKmXQw.Vr0qvc3vEW\_UDPp8yZqn3aCNh3XgSLGuAnADoBnXZUw

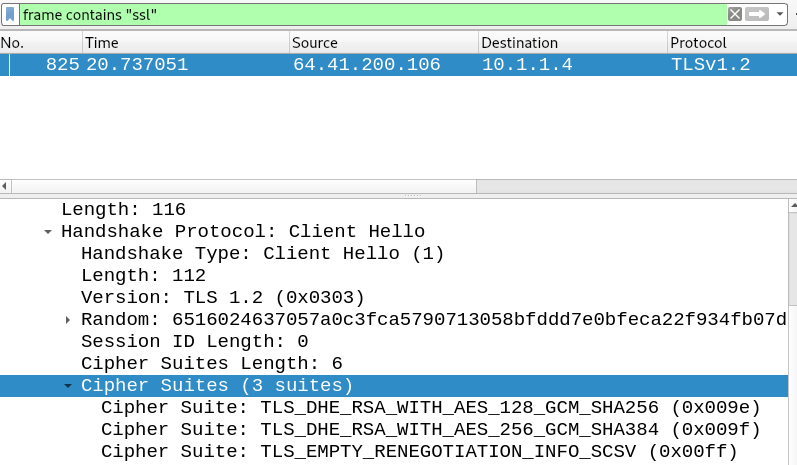
5. The data is retrieved over HTTP, since the validation is not yet completed. After the domain validation is successfully completed the CA issues the SSL/TLS certificate. The certificate is issued with the domain's details and the requirement to use HTTPS. Once the certificate is installed on the web server, it enforces HTTPS for secure data transmission.

6. We requested a certificate from Lets Encrypt. The request part is not captured however we receive a response from certbot. Therefore, the traffic from certbot is going to us, i.e the party that requested the certificate.

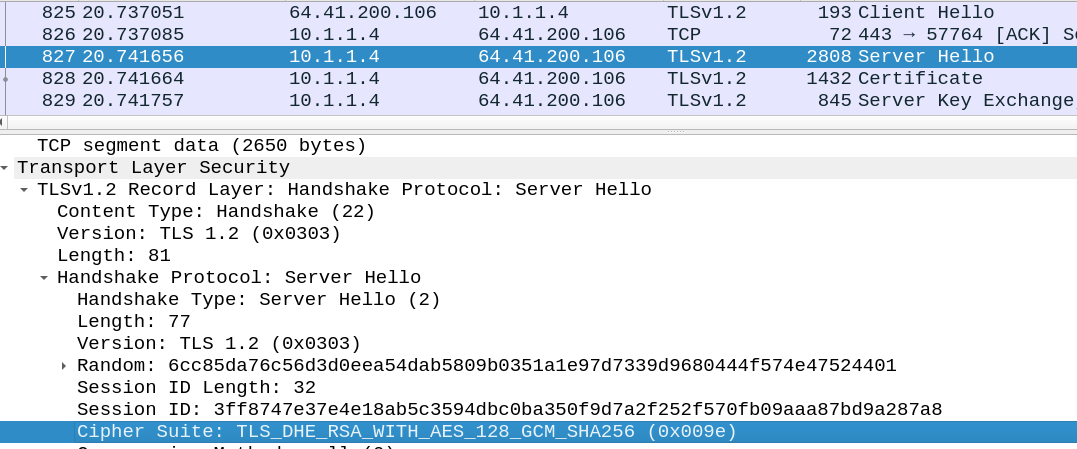
**Exercise 4**

1. The client sends a preferred cipher suite to the server in a TLS handshake. The server responds by saying if itself prefers that cipher suit or not.

2. This packet capture demonstrates the CLIENT HELLO, where the client sends 3 cipher suits to the server in order of preference.



In the next packet capture, the server sends a SERVER HELLO responding with the 1 cipher suite it prefers.



1. \*Michelle asked us to ignore this question, as the answer to the first question answers it\*

**Exercise 5**

1. 136.159.49.117

206.81.1.88

167.172.20.95

2. A screen shot of a computer code

Description automatically generated

3. YES

A screenshot of a computer

Description automatically generated

**Exercise 6**

1. 42746, 45241, 45242

2. We initially filtered to frame contains “linkedin” and then we verified the dstn ip with dig and confirmed that it was the same for linkedin.

3. TLS V1.2

4. TLS v1.2

5. TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384