Name : Mubeen Palh

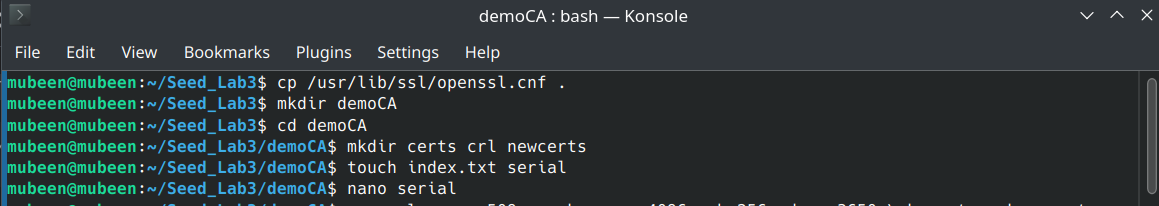
Roll No: 21K-3292

Name: Abdul Aziz

Roll No: 21K-4557

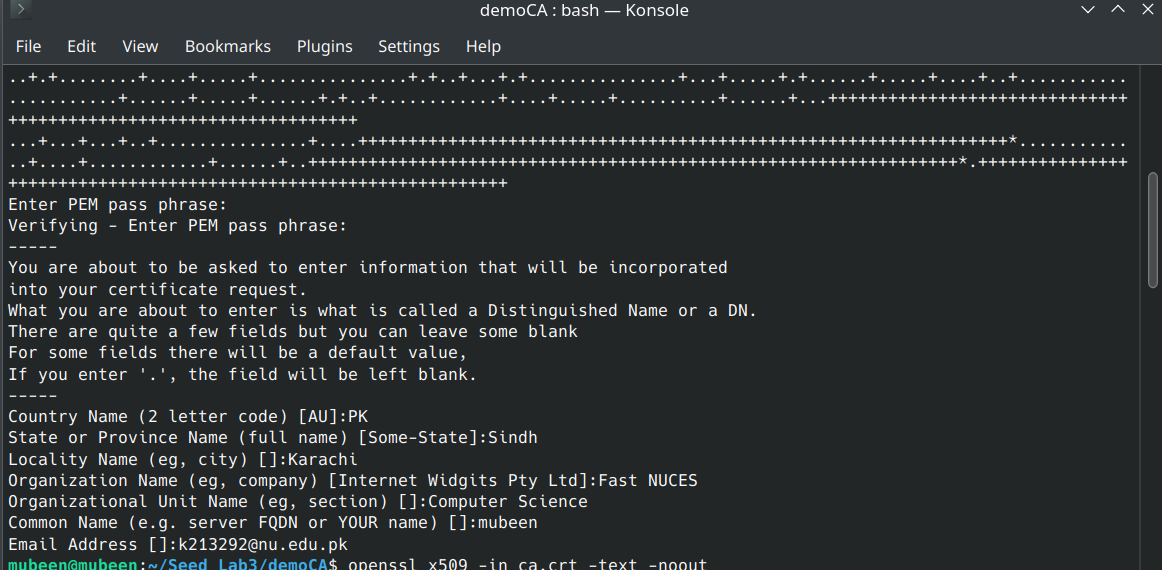
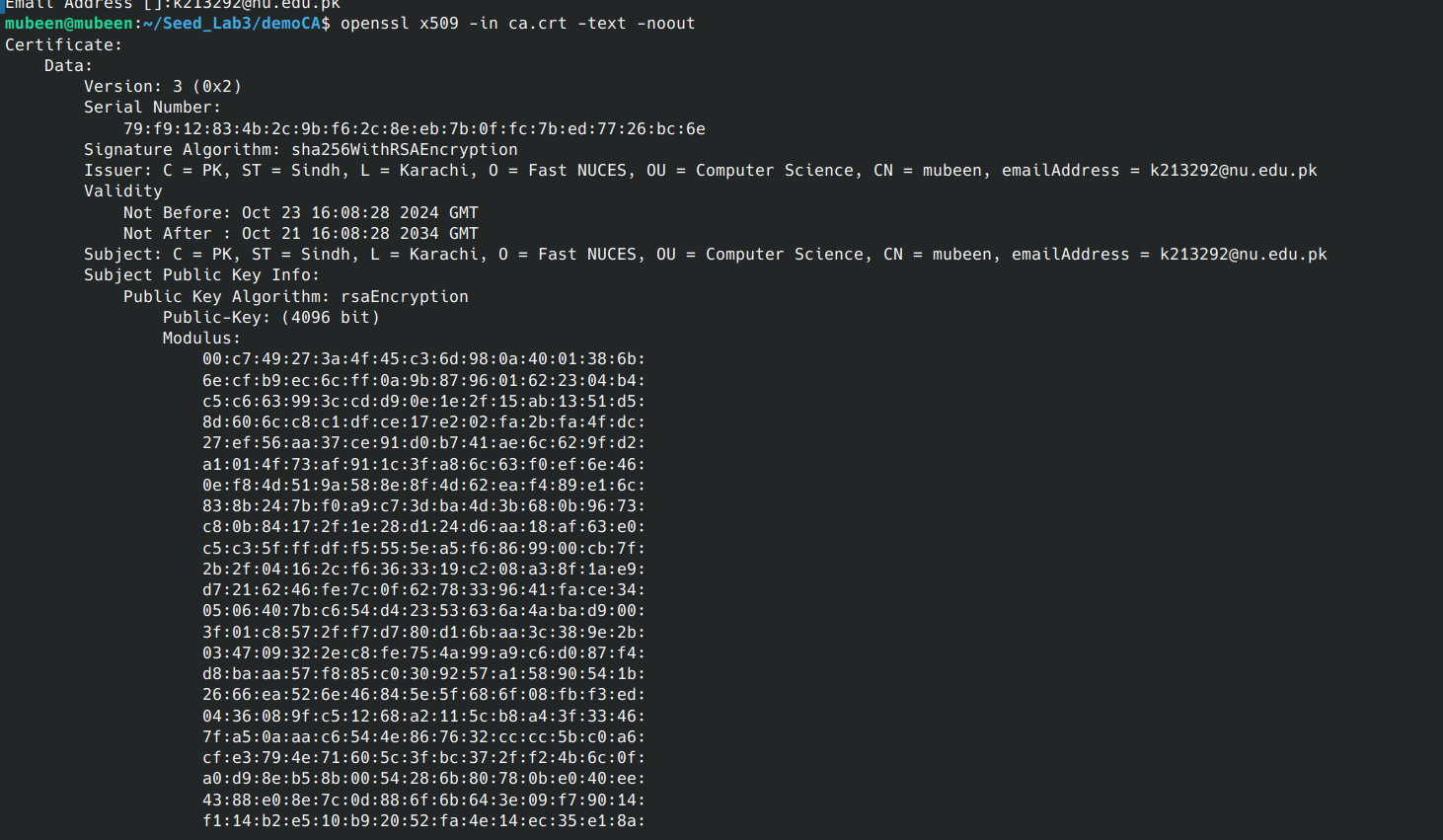
**Task 1 (Becoming a certificate Authority):**

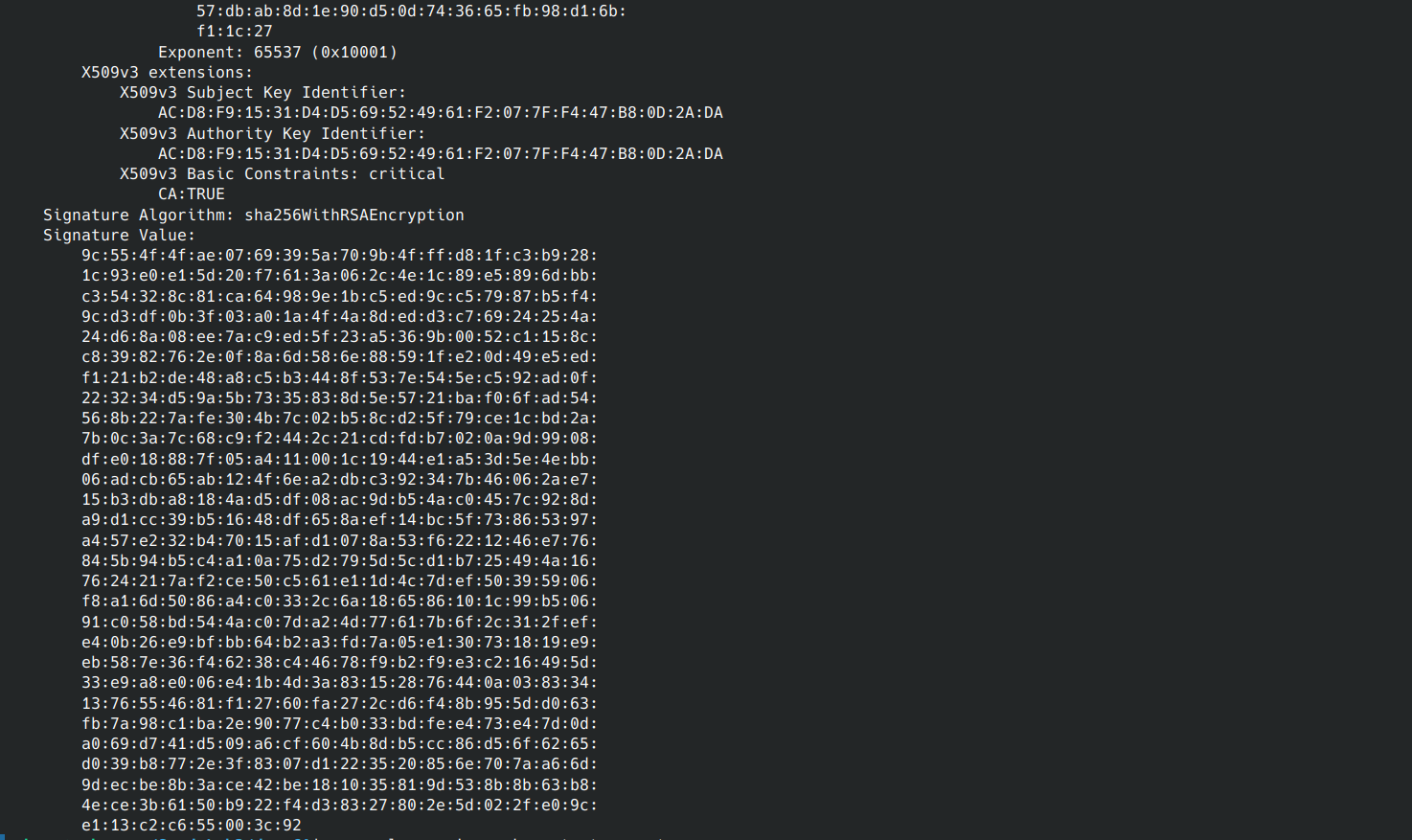
Creating sub directories and writing single line integer to serial file:





Entering the necessary information:

  
 **Certificate:  
**

****

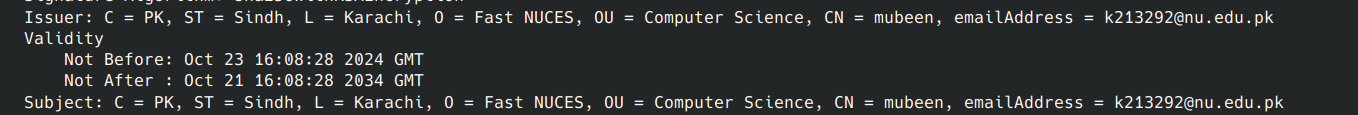
**What part of the certificate indicates this is a CA’s certificate?**

**Ans :** This field (Basic Constraints) defines whether the certificate is a CA certificate or an end-entity certificate. The value CA:TRUE explicitly states that this certificate can be used to sign other certificates, making it a CA certificate.

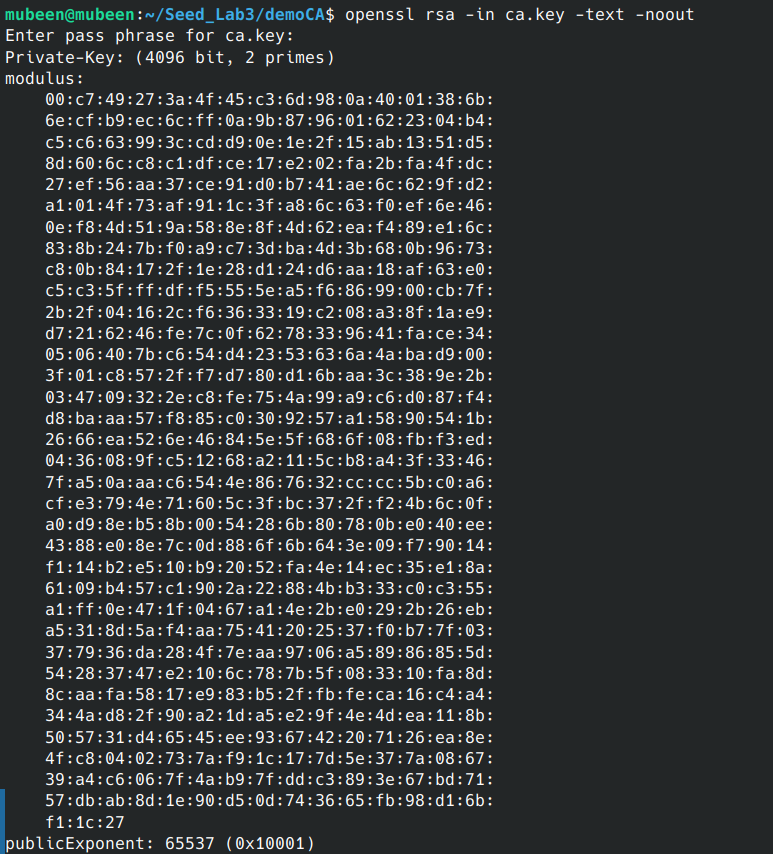


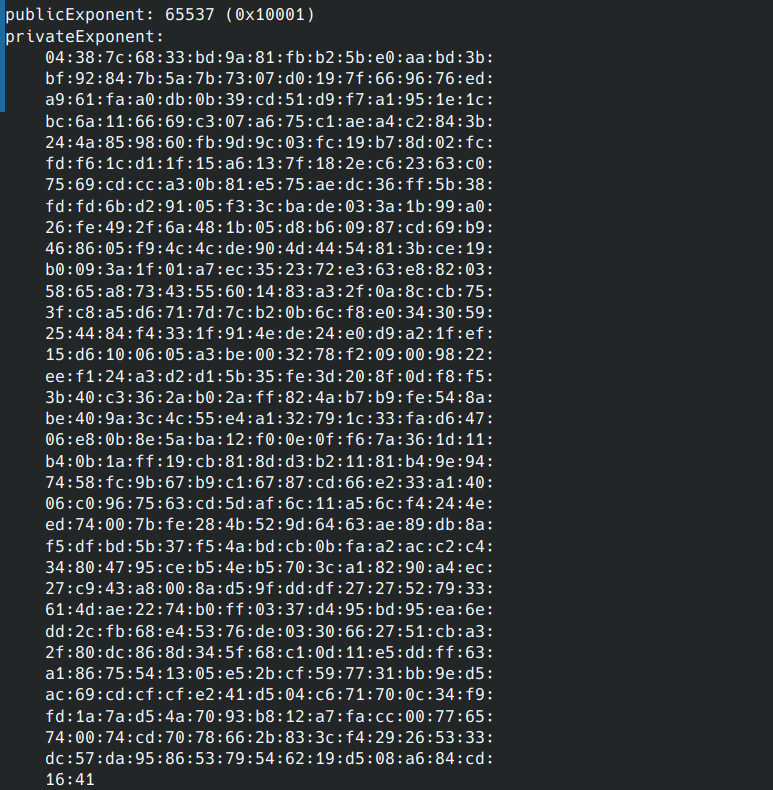
**What part of the certificate indicates this is a self-signed certificate?**

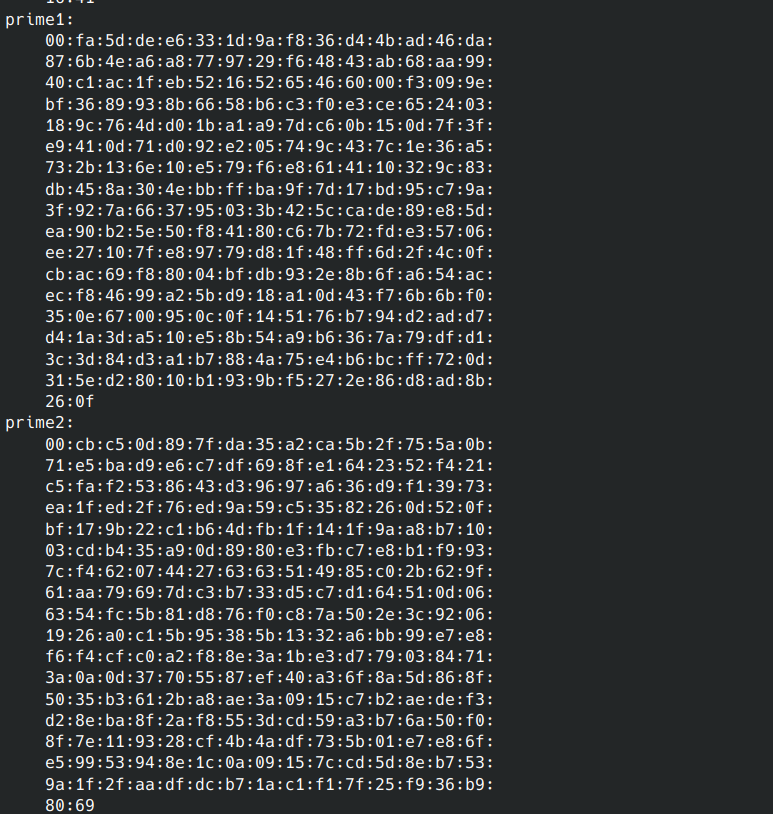
**Ans:** The field which specifies the issuer and the Subject indicates if it is a self-signed certificate or not. If the Issuer and subject fields are the same then it is a self-signed certificate (as shown in the picture above).

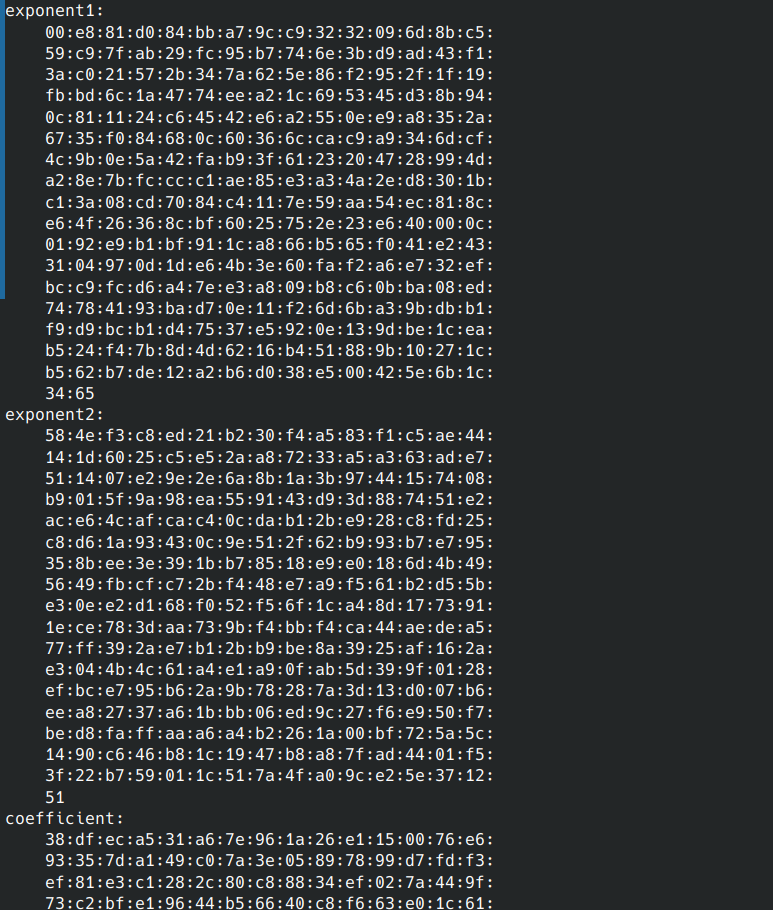


**Question: In the RSA algorithm, we have a public exponent e, a private exponent d, a modulus n, and two secret numbers p and q, such that n = pq. Please identify the values for these elements in your certificate and key files.**

**Answer:**The values are:  


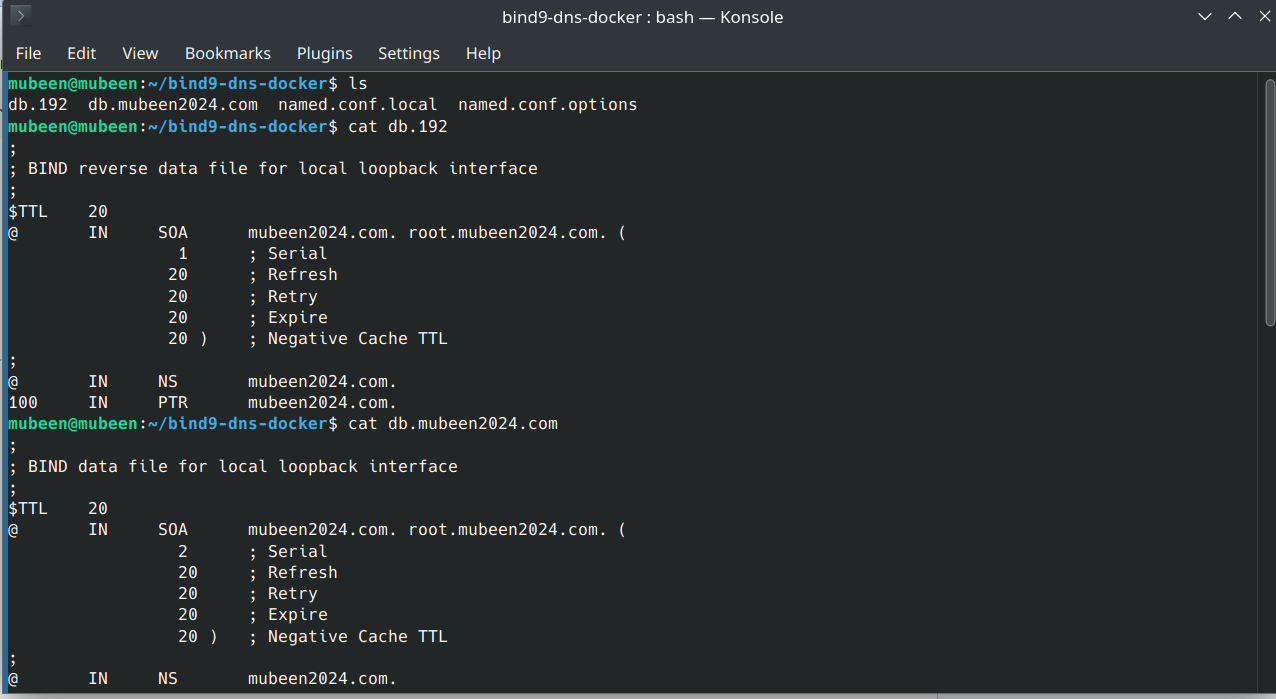


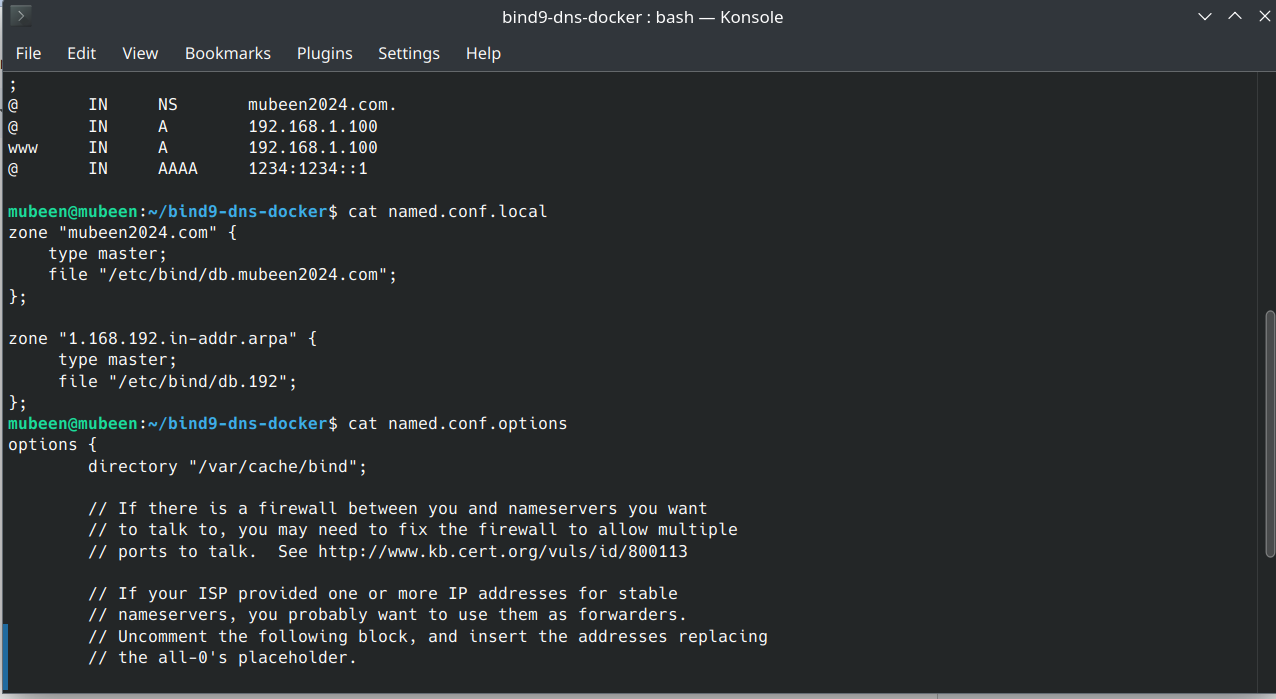


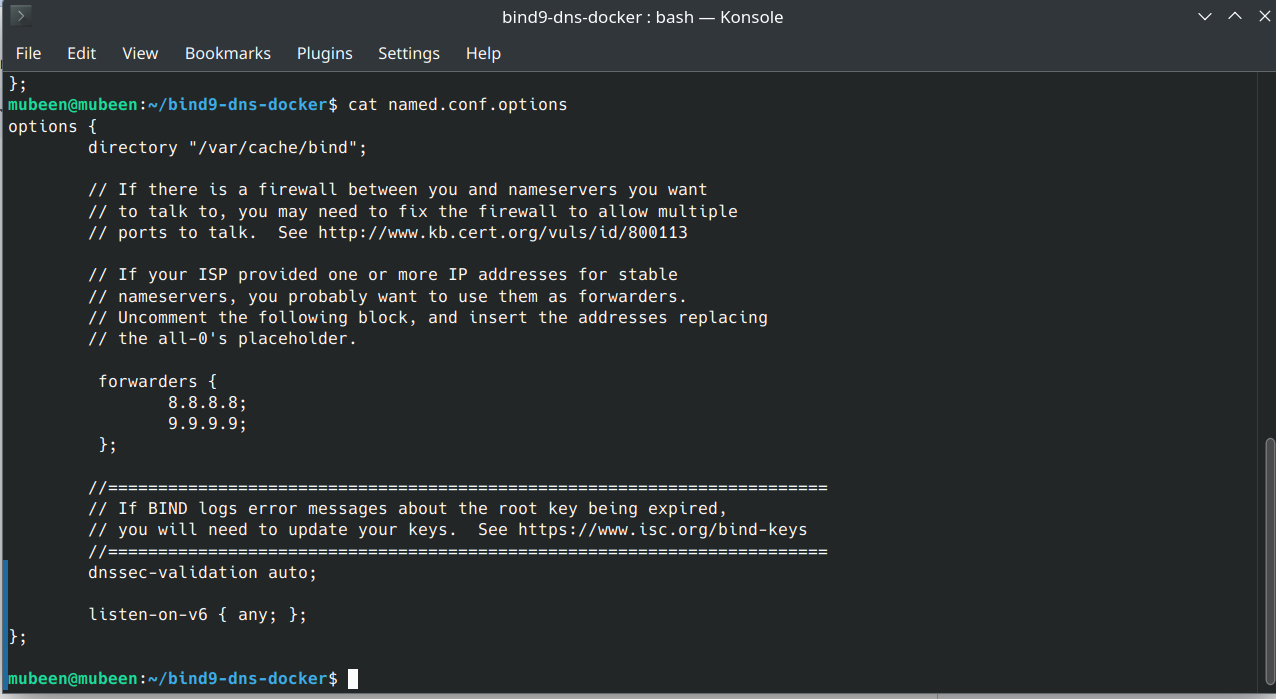


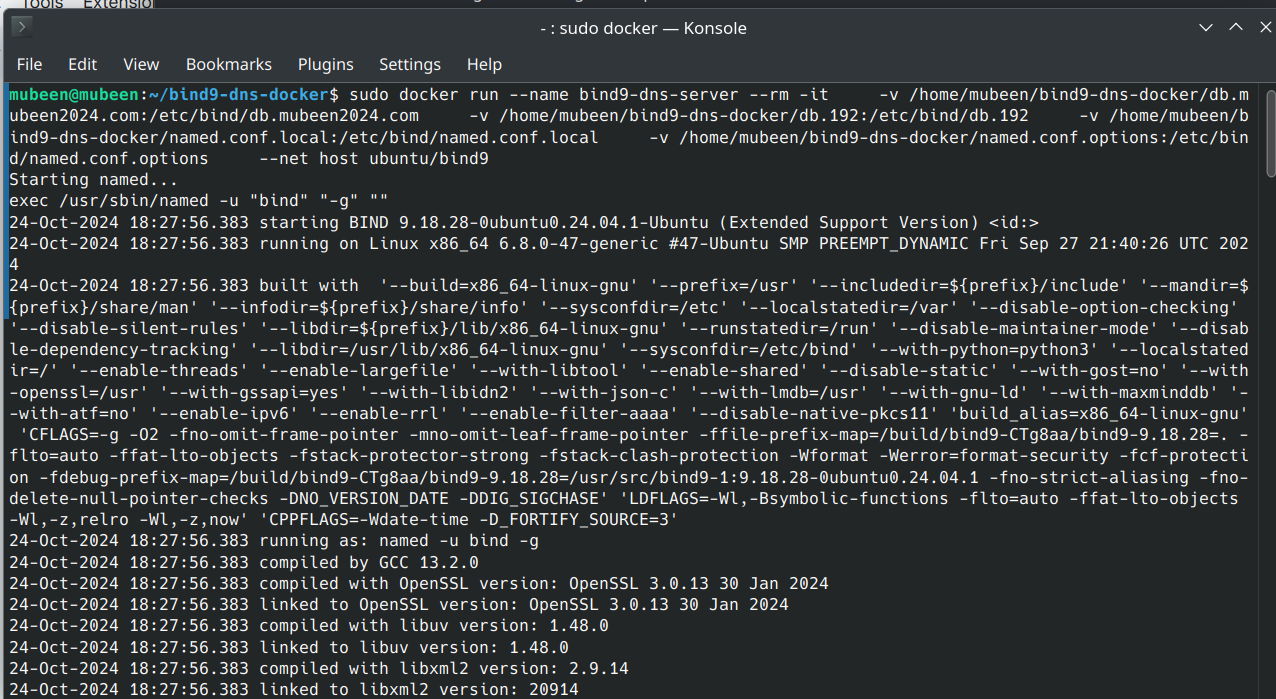
**Task 2:**

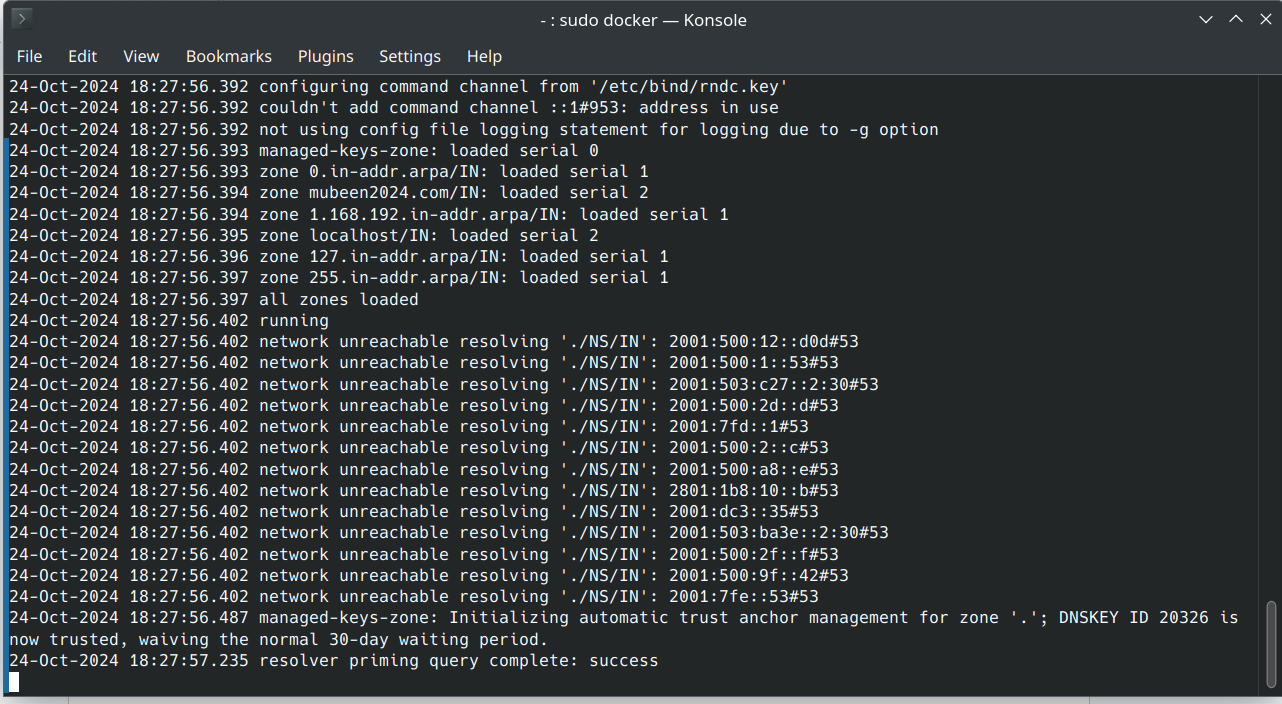
**(Setting Up the DNS Server using bind9 and docker)**

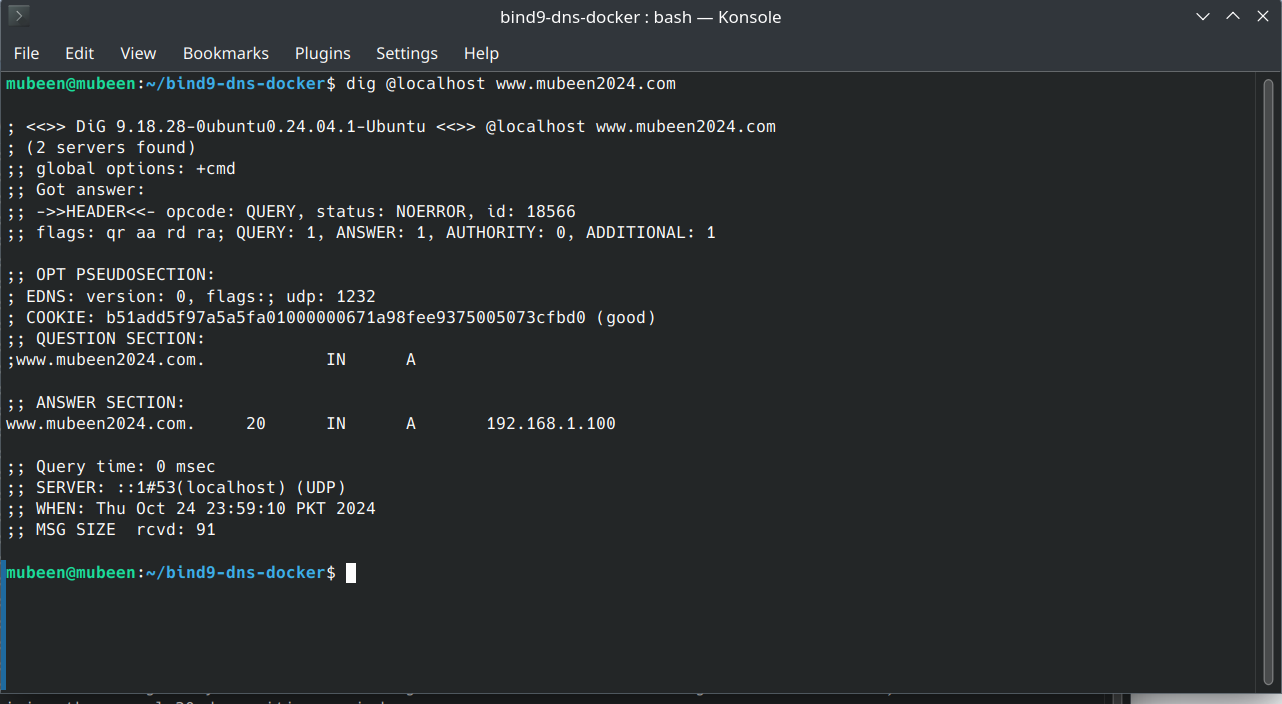
****

****

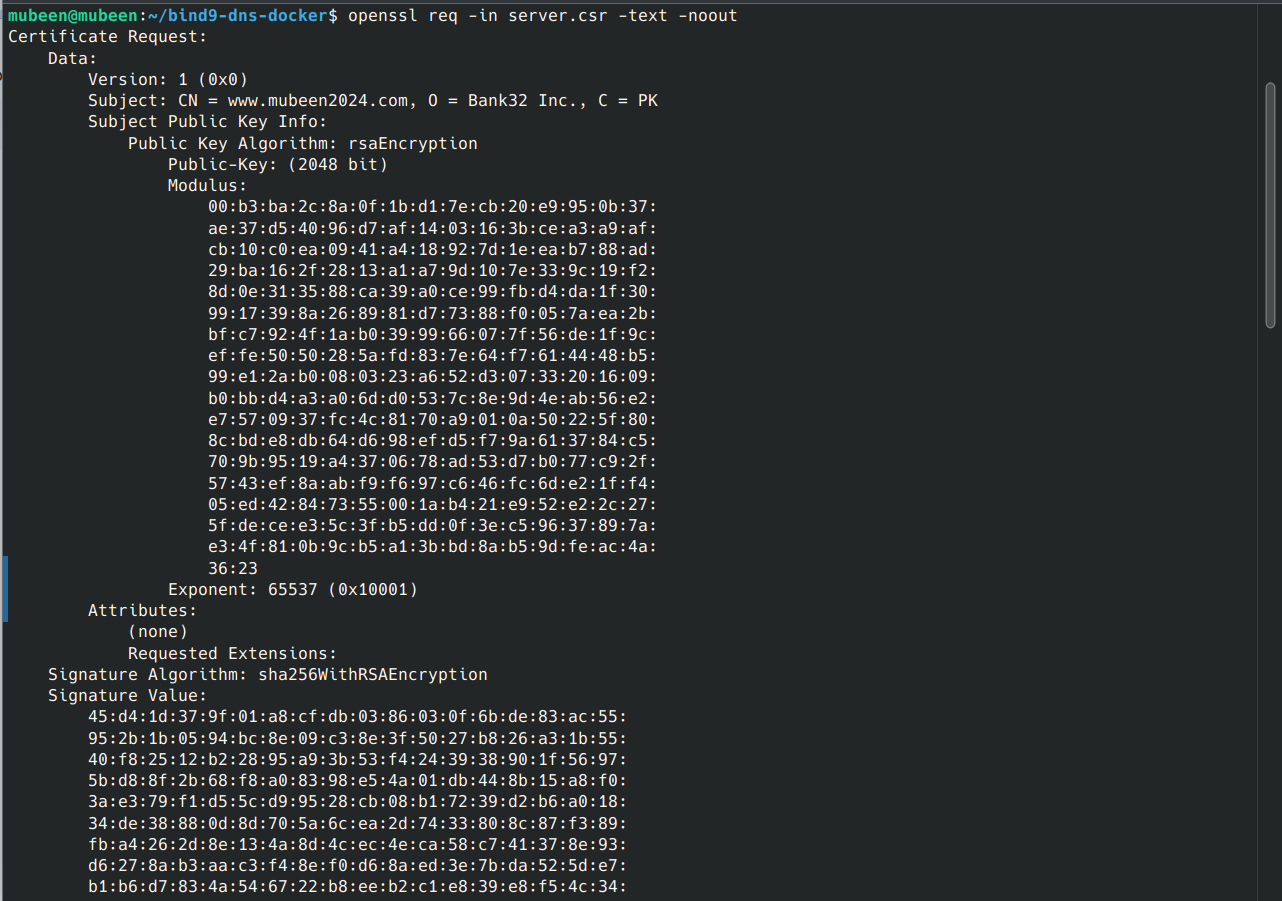
****

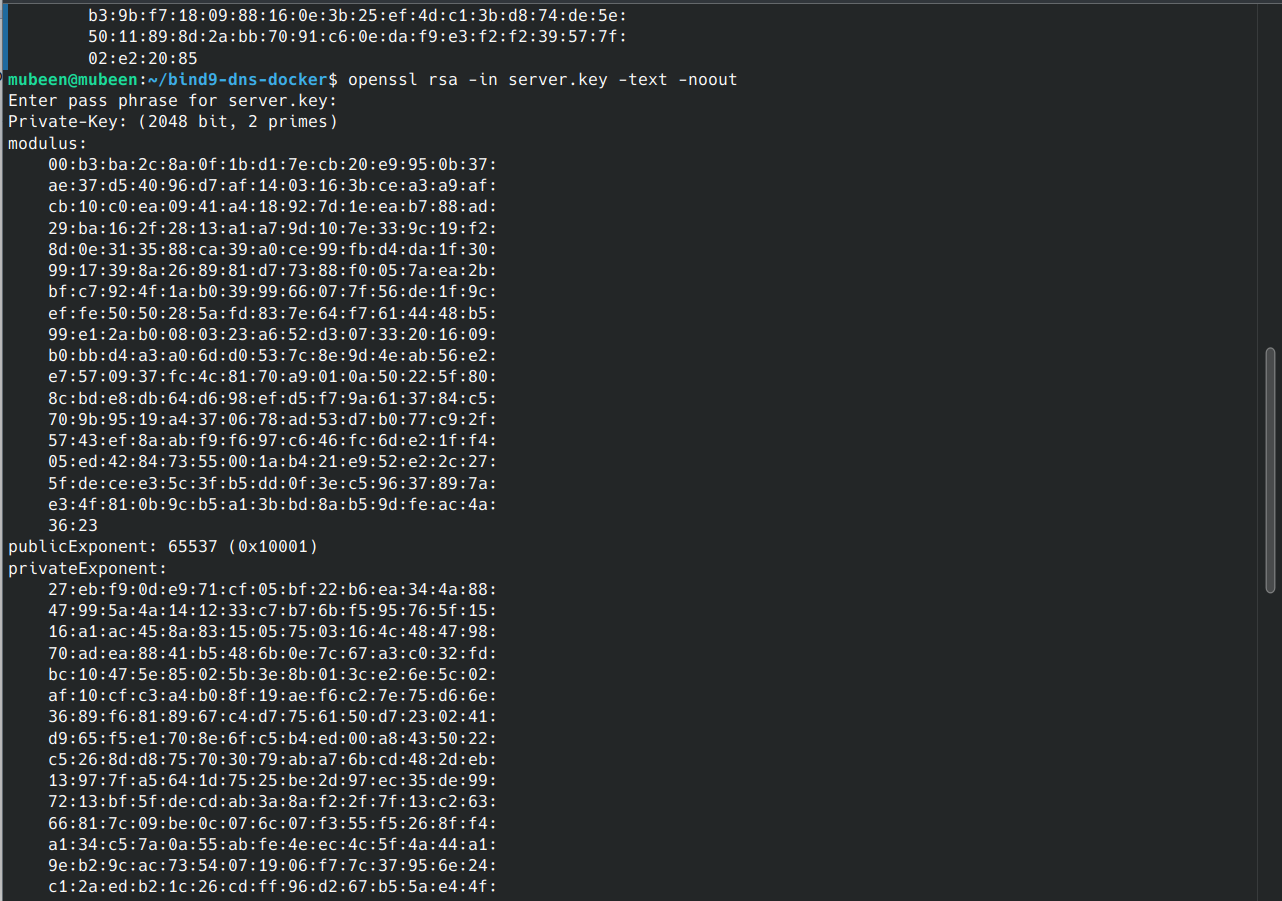
**Running docker container with bind9:  
**

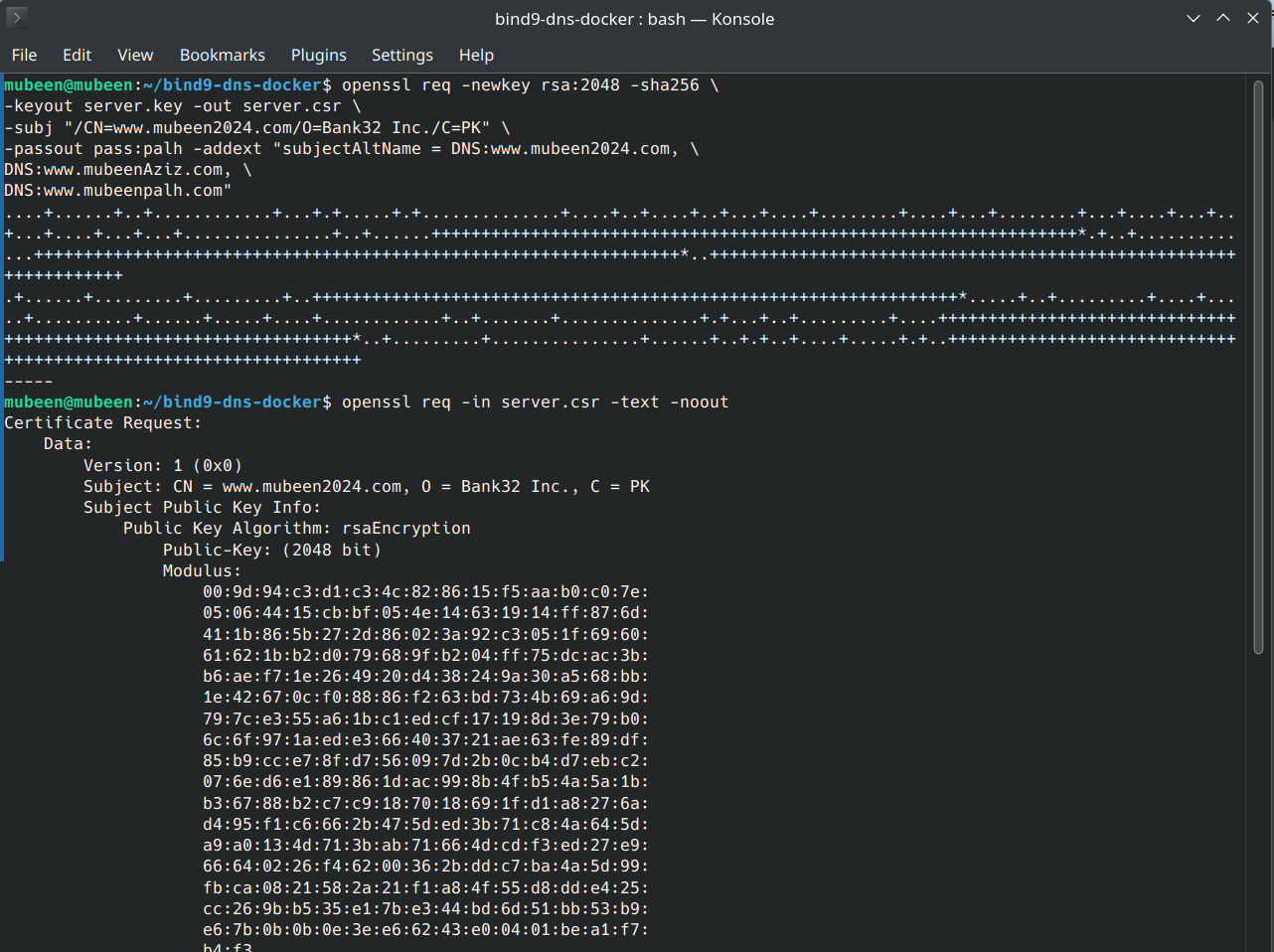
****

**After all configuration setup, checking the response on “**[**www.mubeen2024.com**](http://www.mubeen2024.com)**”  
**

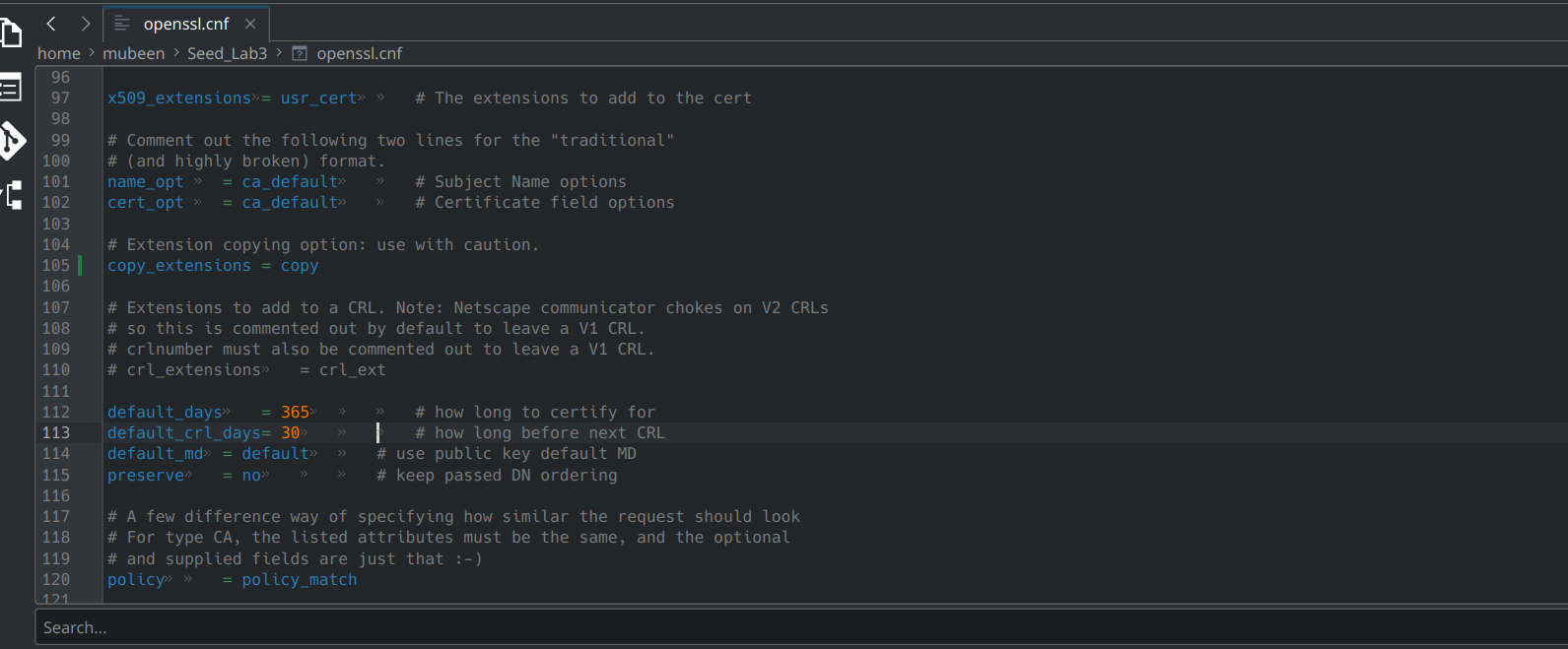
**Running the command to generate CSR:  
**

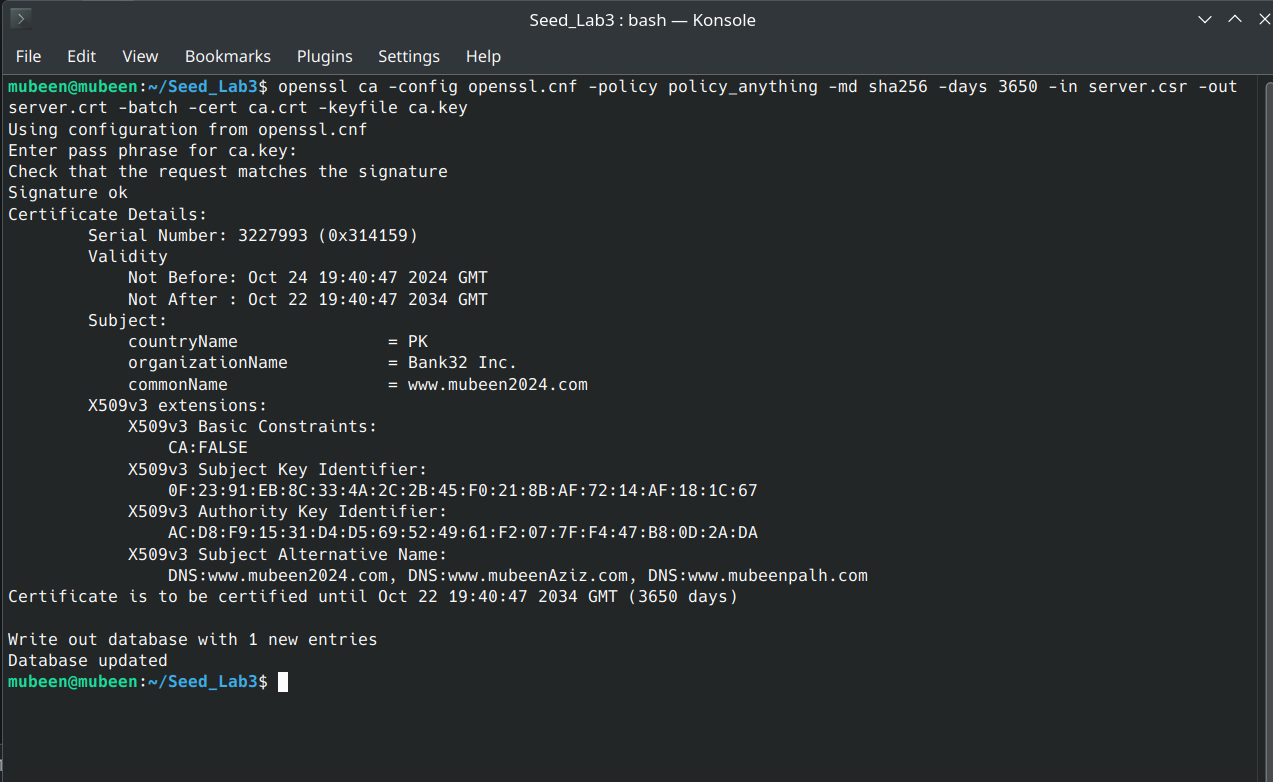
**Viewing the contents of file:  
  
**

****

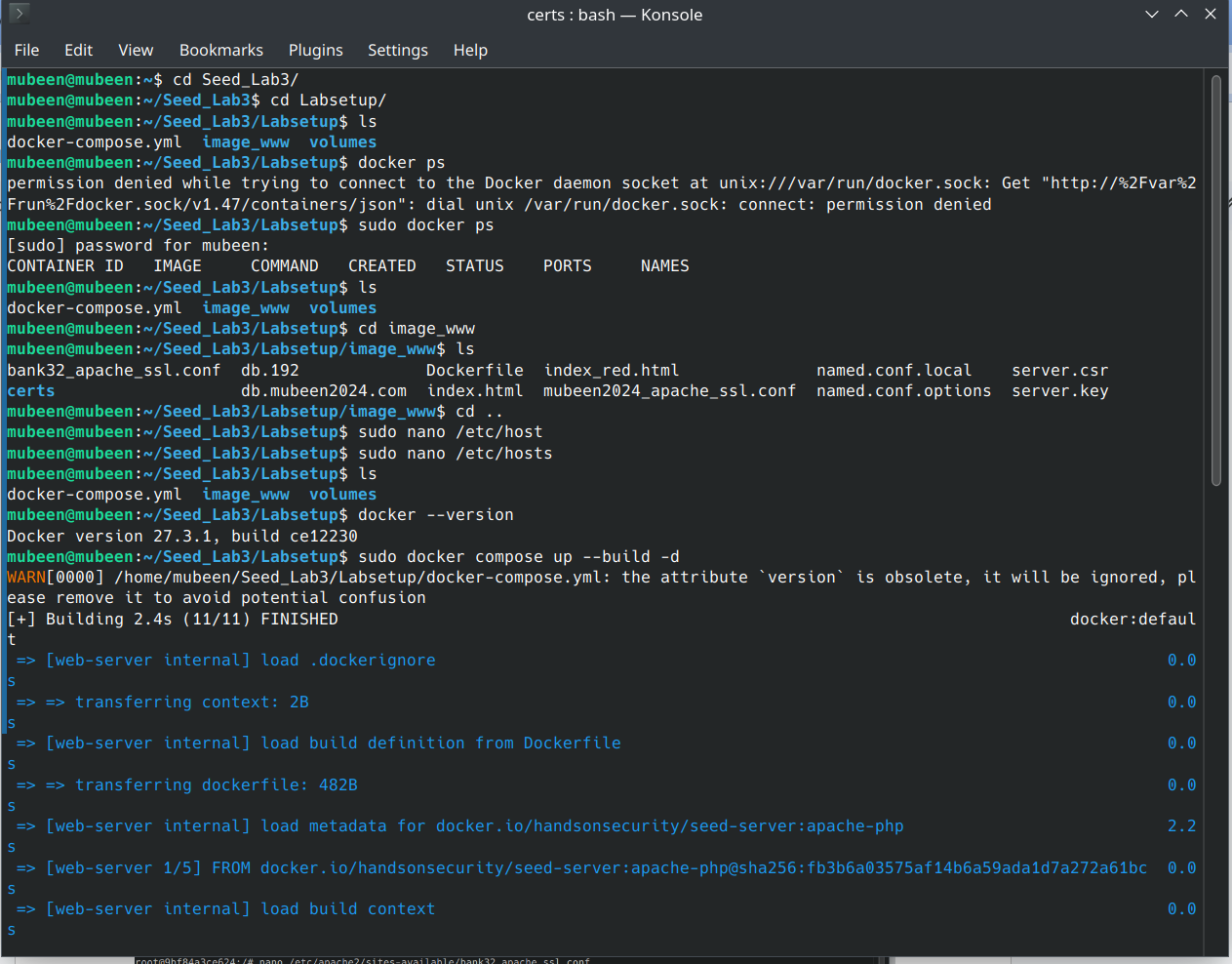
**Task:**Adding alternative names to certificate signing request:  
****

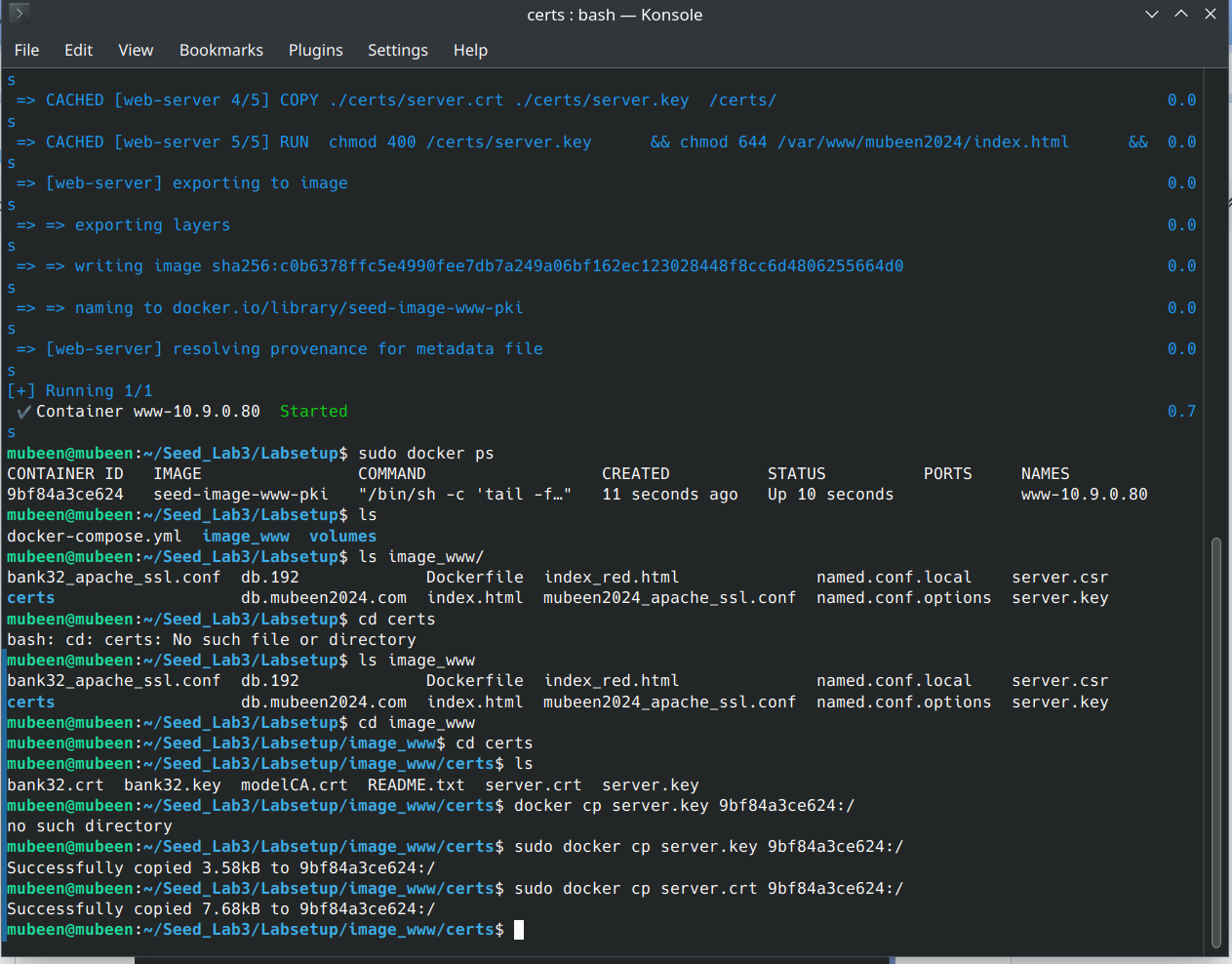
****

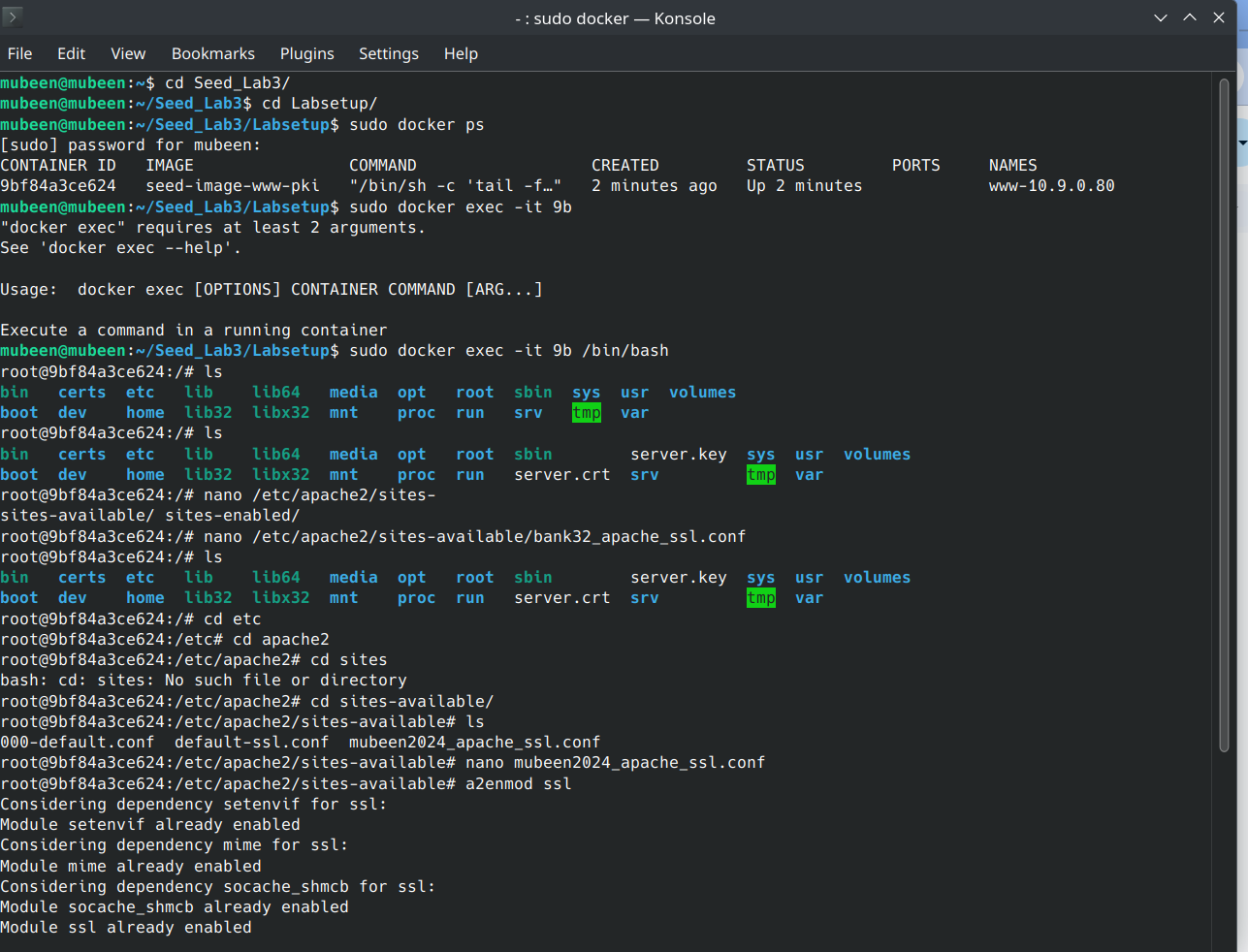
**Task 3 (Generating a Certificate for your server):**Uncommenting the field in openssl.conf file:  
****

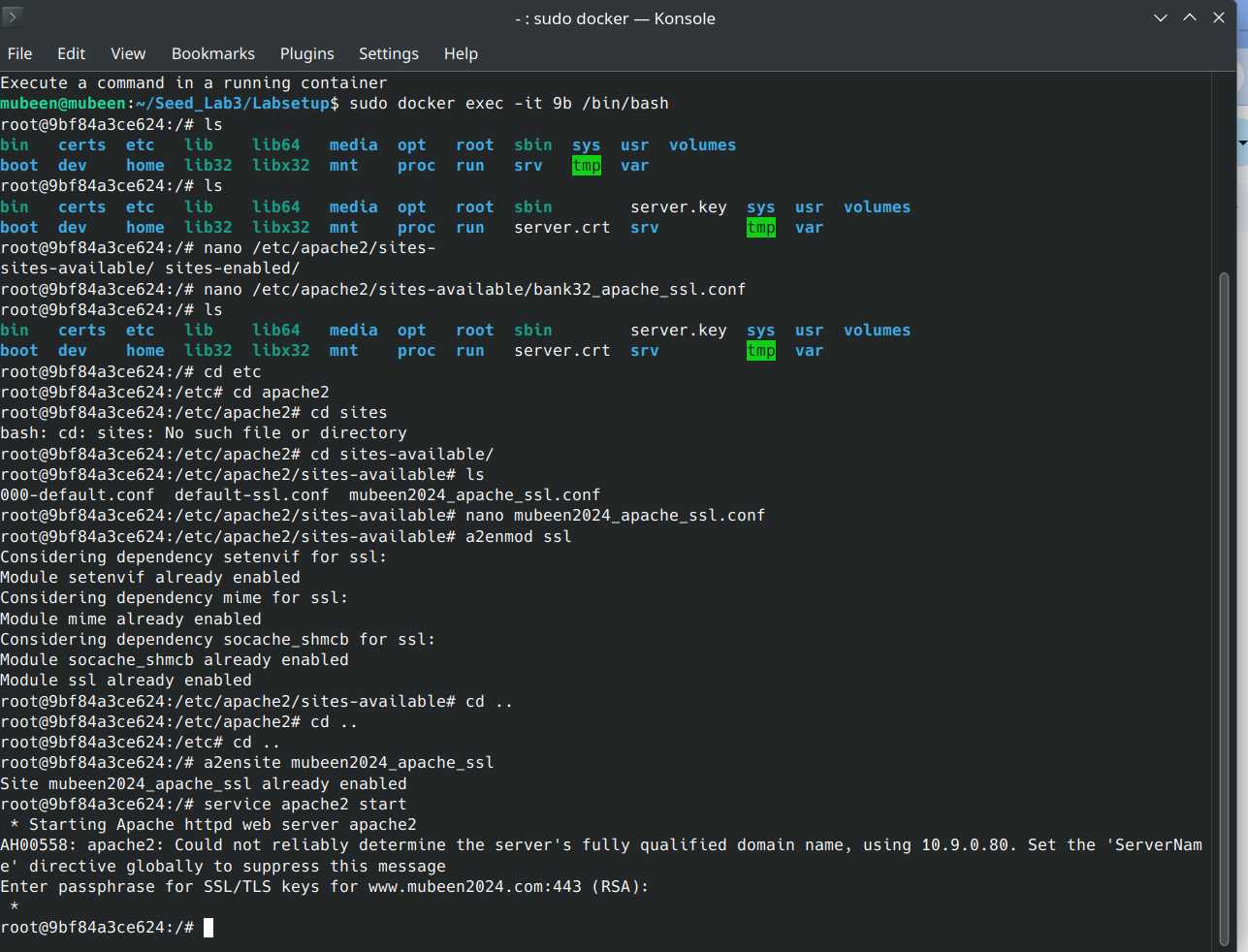
**Running the command again and checking all the subject alternatives exists or not:  
**

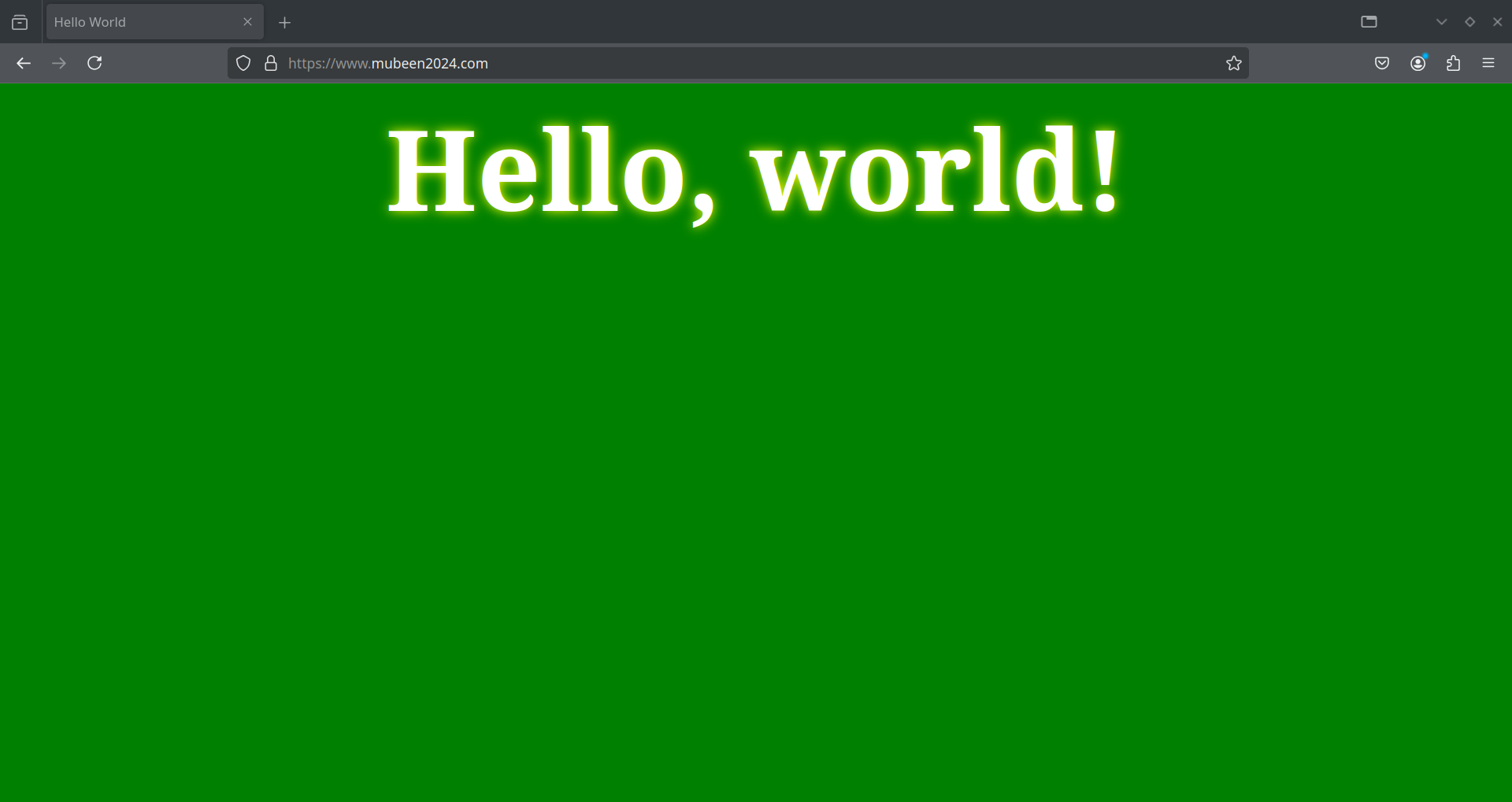
**The subject alternatives also exist as shown in the above screen shot.**

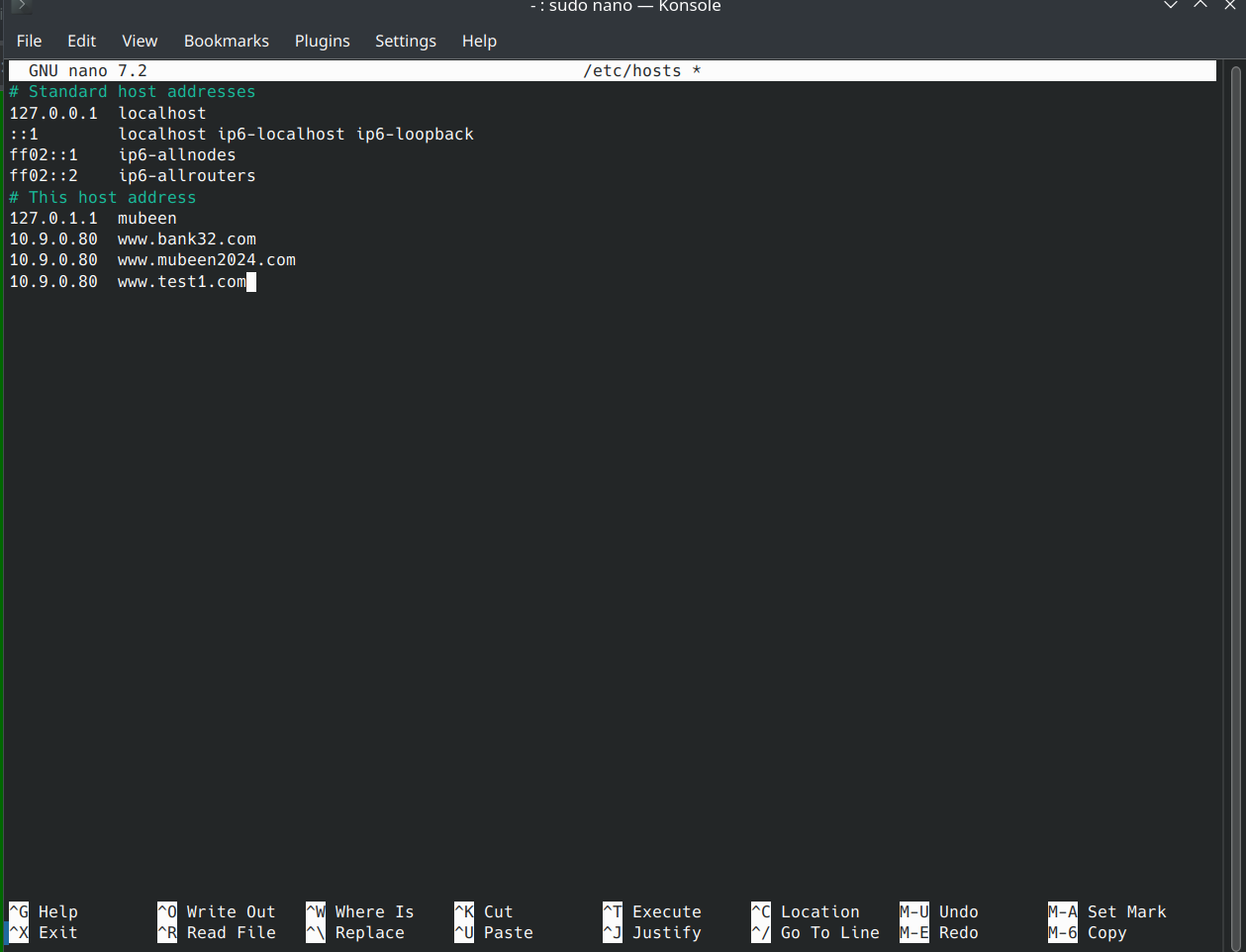
**Task 4:  
**

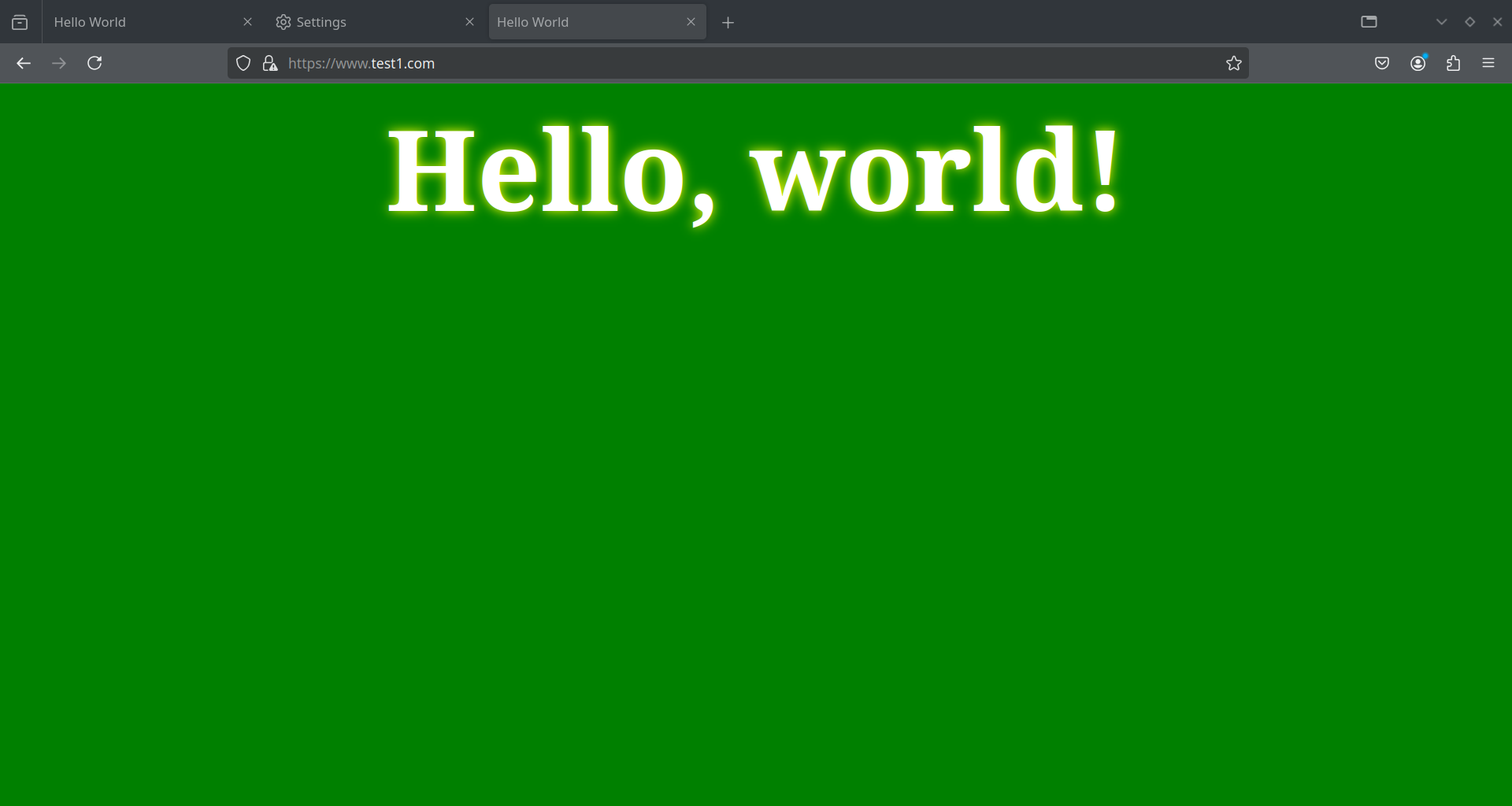
****

****

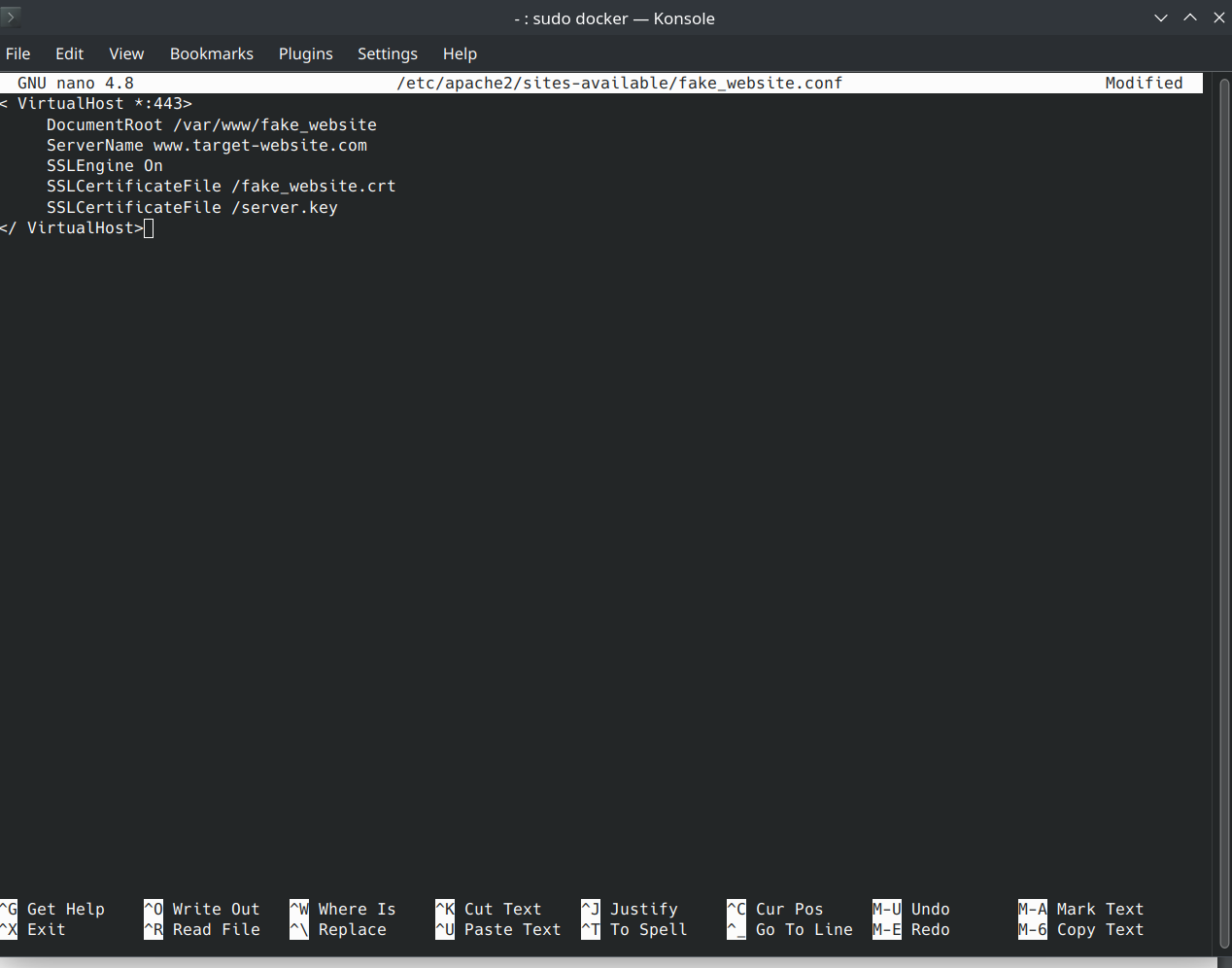
****

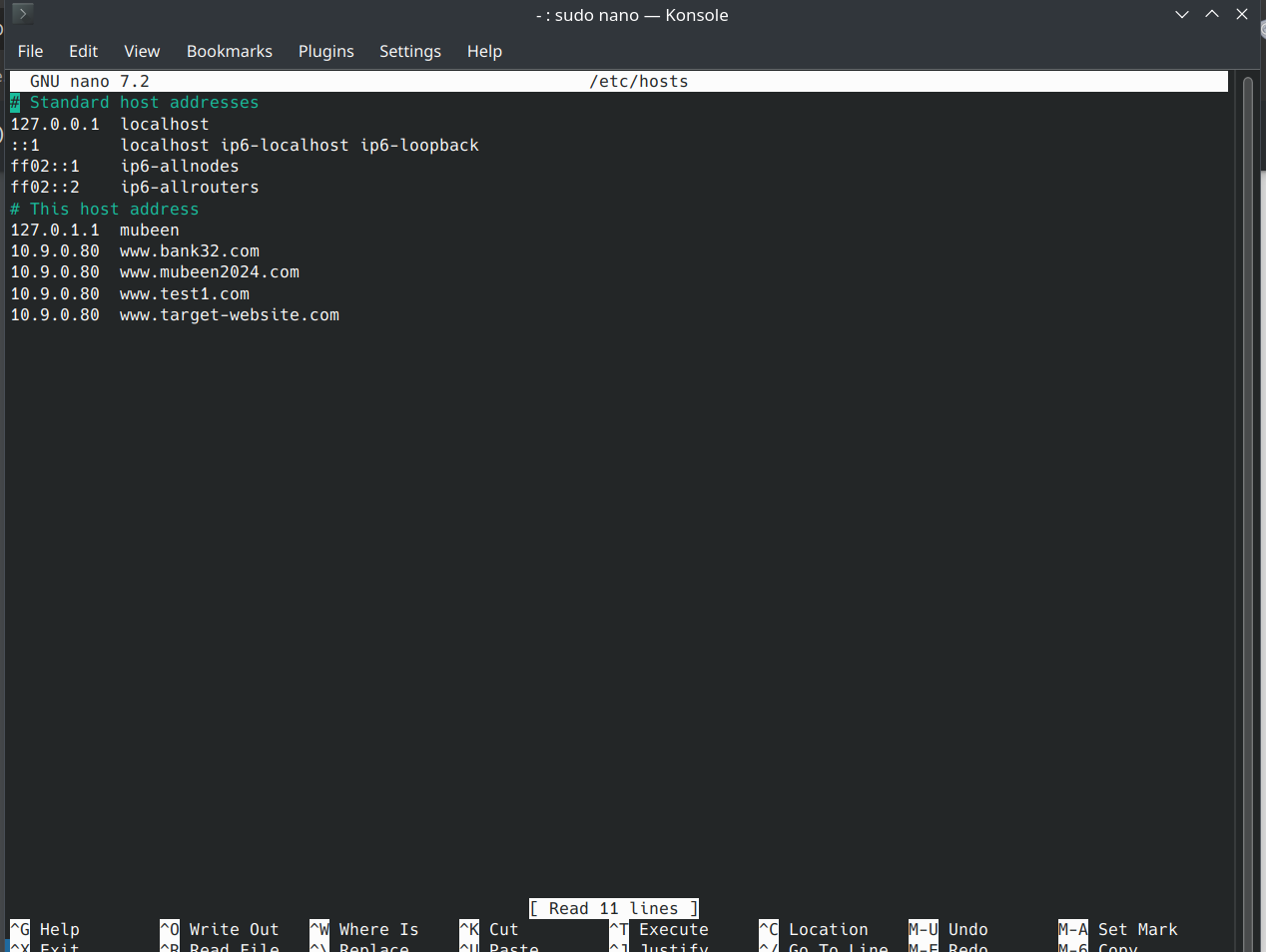
****

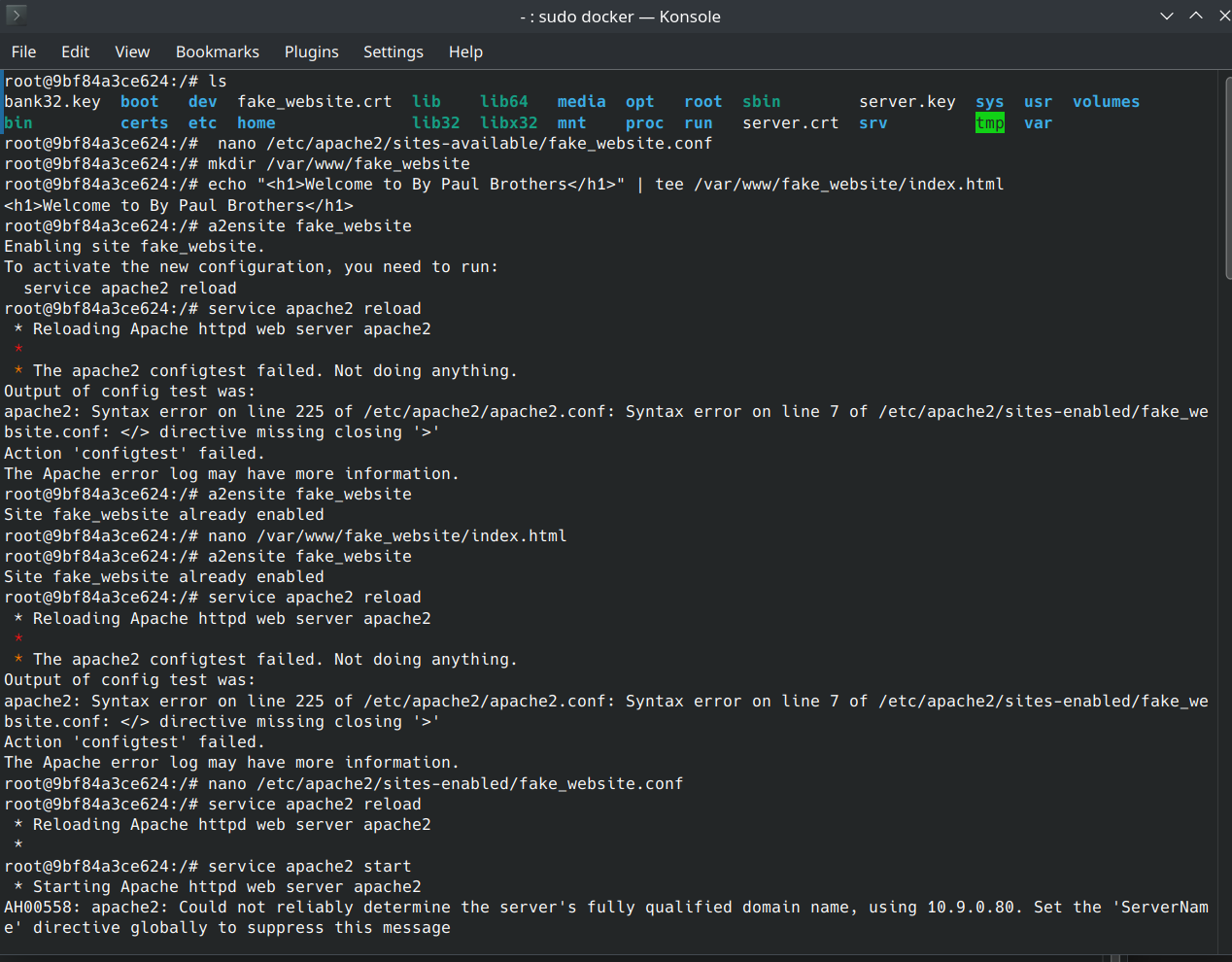
**Task 5:  
**

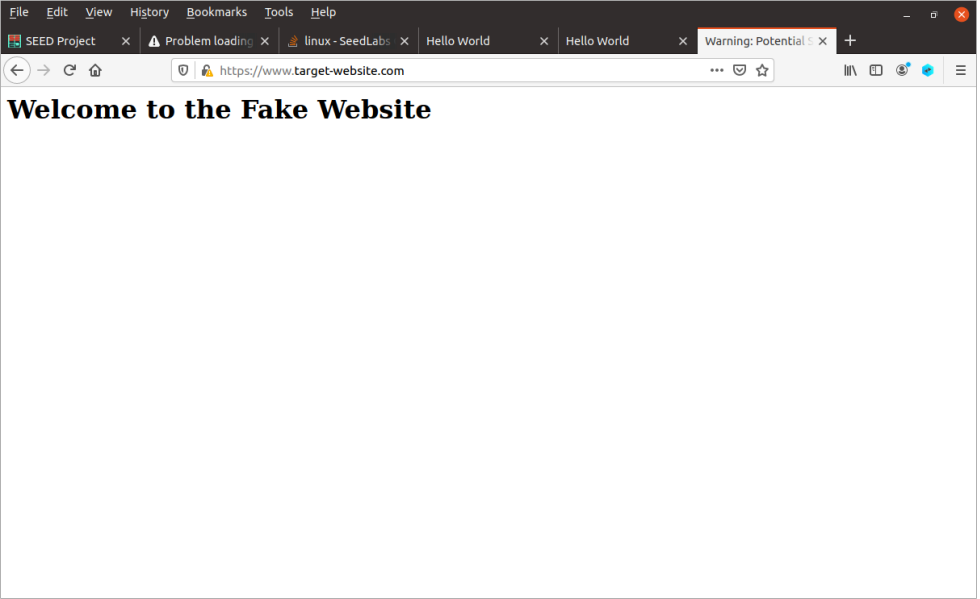
****

**Task 6:**

****

****

****

****