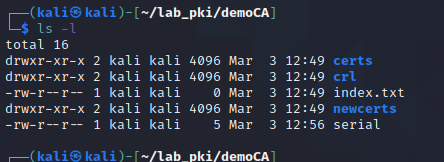
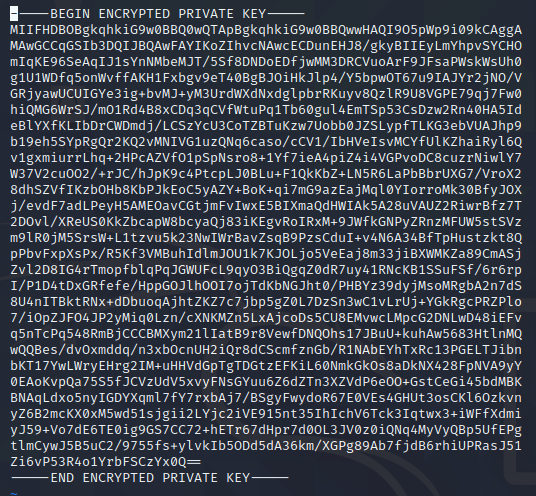
# IT666 - PKI Lab [Rjs1070@wildcats.unh.edu](mailto:Rjs1070@wildcats.unh.edu)

Ryan J. Skelly 3/3/21

Task 1.1 (5 points) Provide a screen shot of a detailed listing of the files in demoCA directory.



Task 1.2 (5 points) Provide the contents of ca.key and ca.crt.



CA.KEY

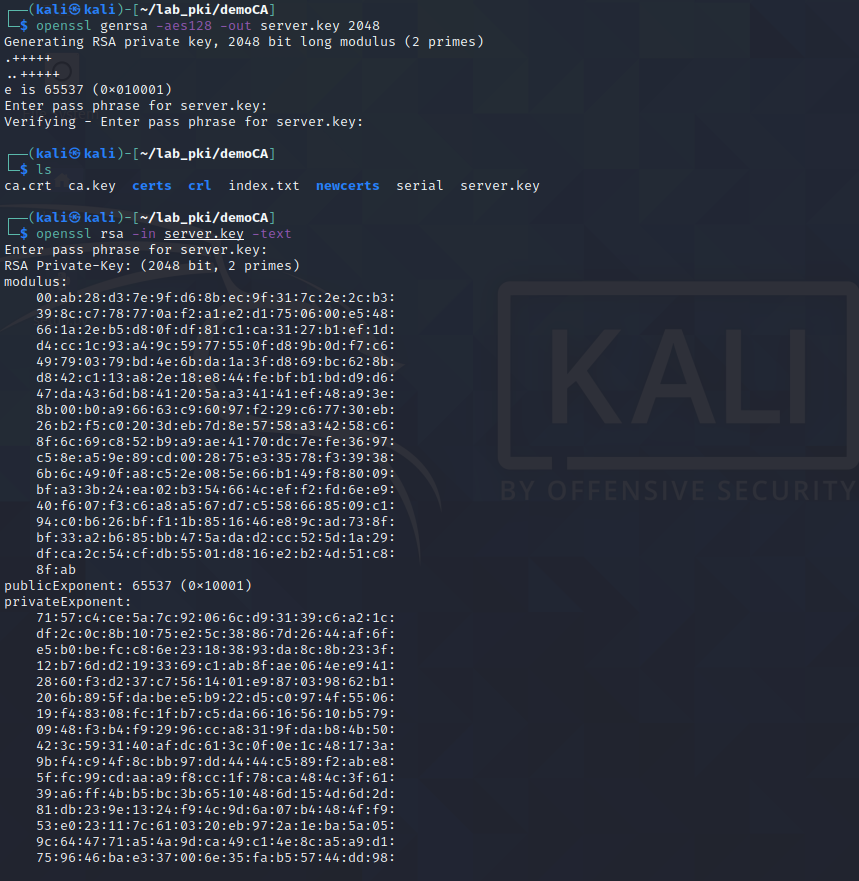
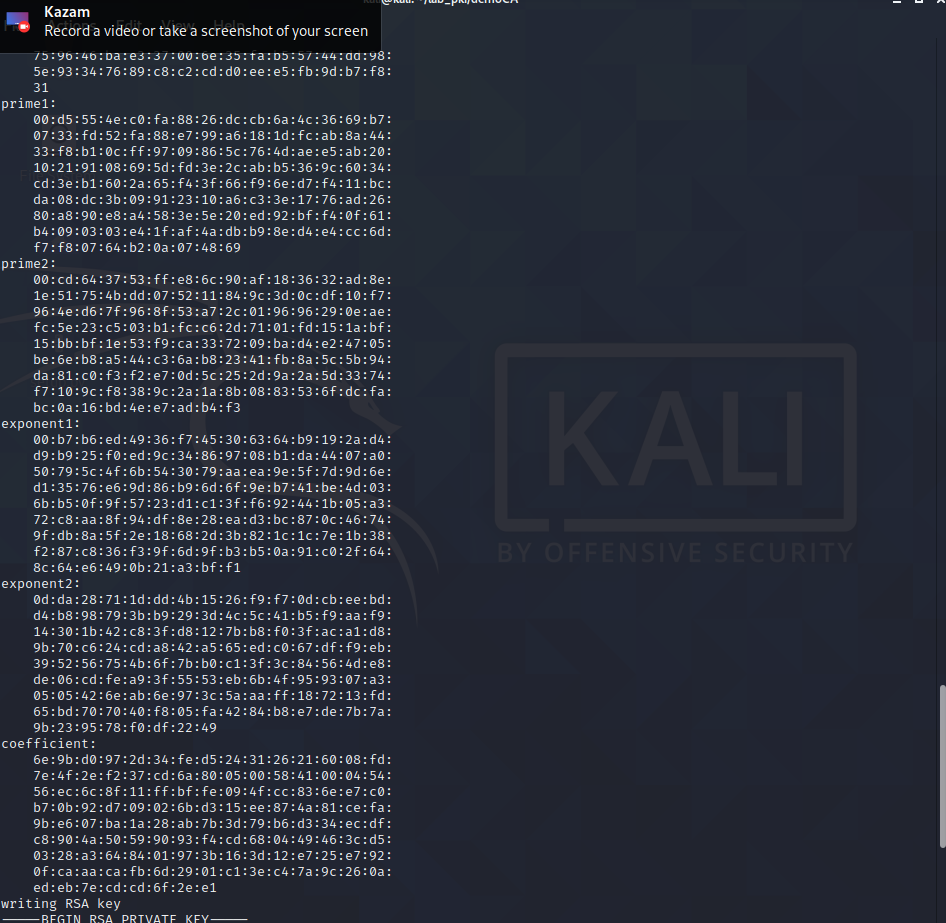


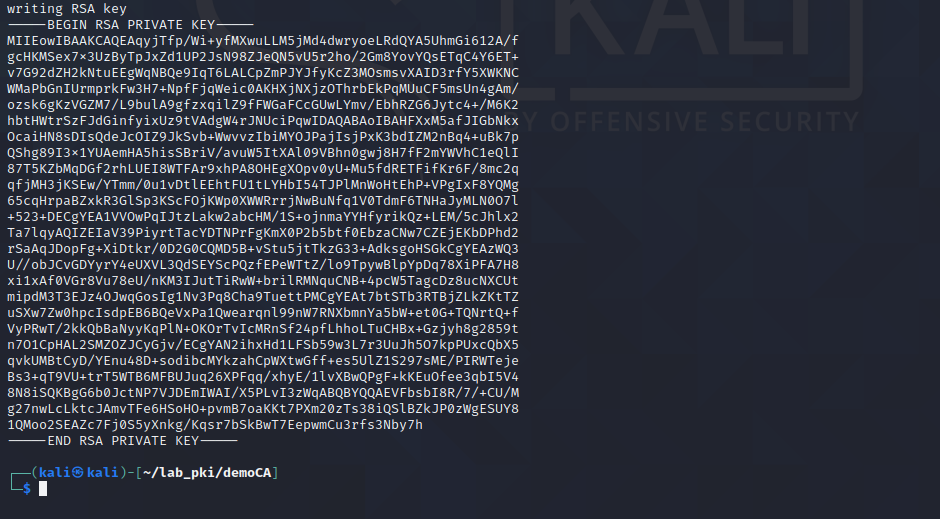
CA.CRT

Task 1.3 (5 points) True/False: Openssl can retrieve forgotten passwords in private key files?

FALSE

Task 2.1: (5 points) Include a screenshot of your command interaction.

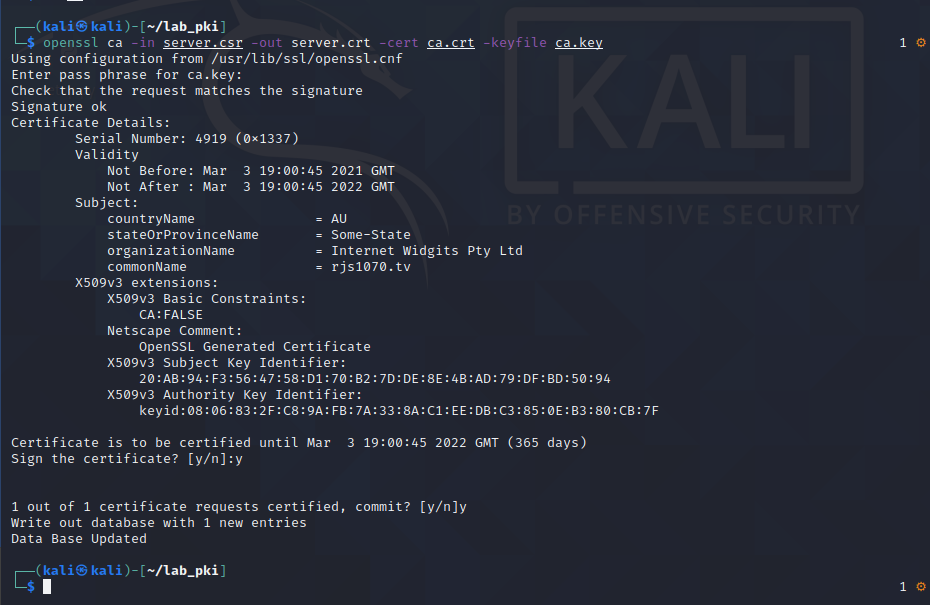
 



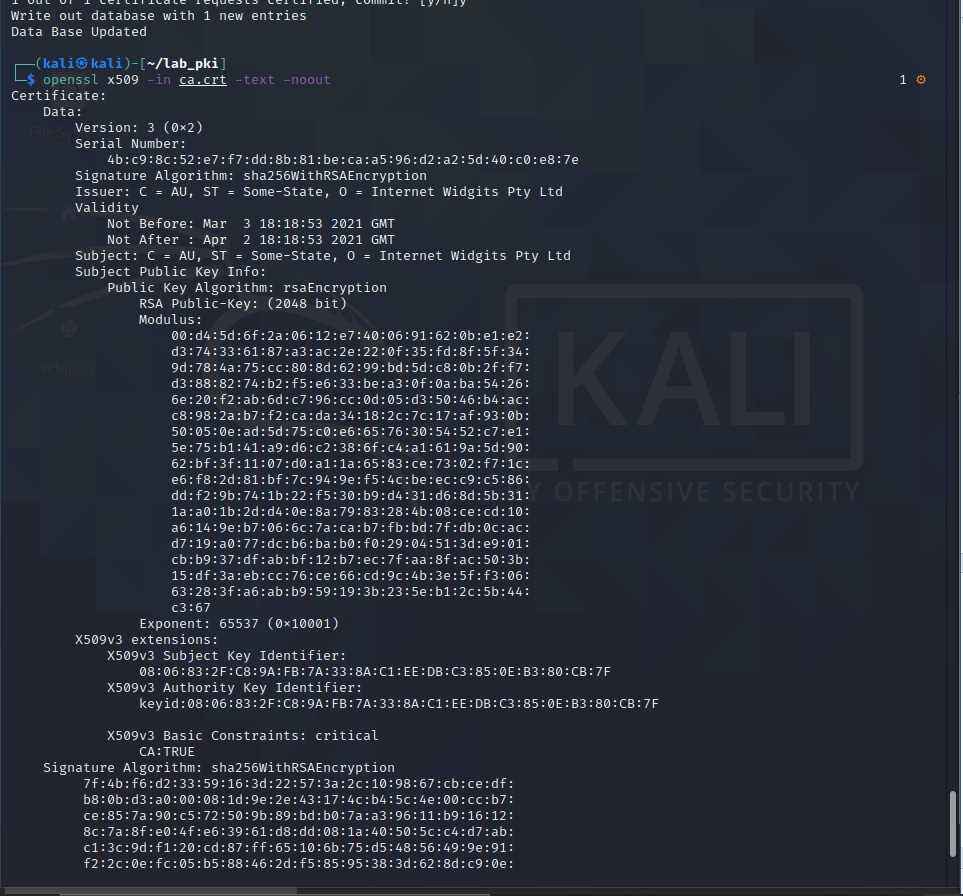
Task 2.2: (5 points) Include a screenshot of your command interaction.



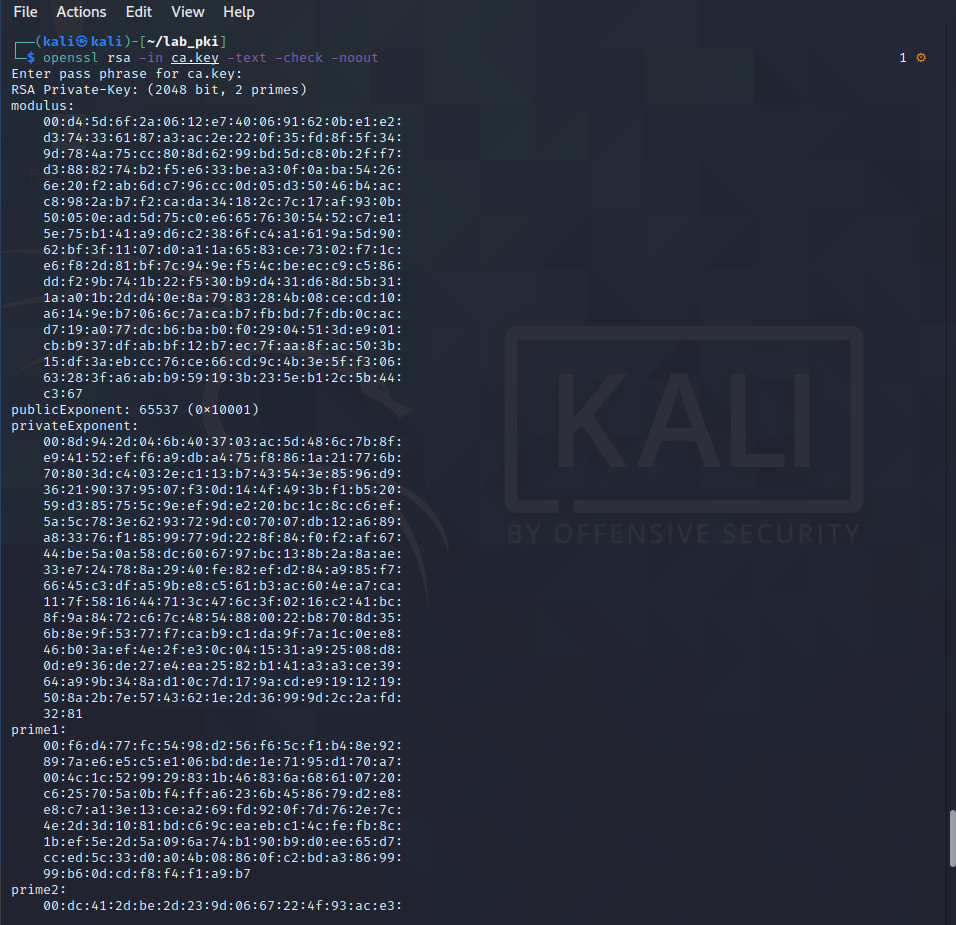
Task 2.3: (10 points) Include a screenshot of your command interaction.

I realized after the fact that all of my ca and server files were in the wrong directory, I mv’ed everything up one dir and it worked, Im not sure if itd change any of my output, just I had a bit of trouble here

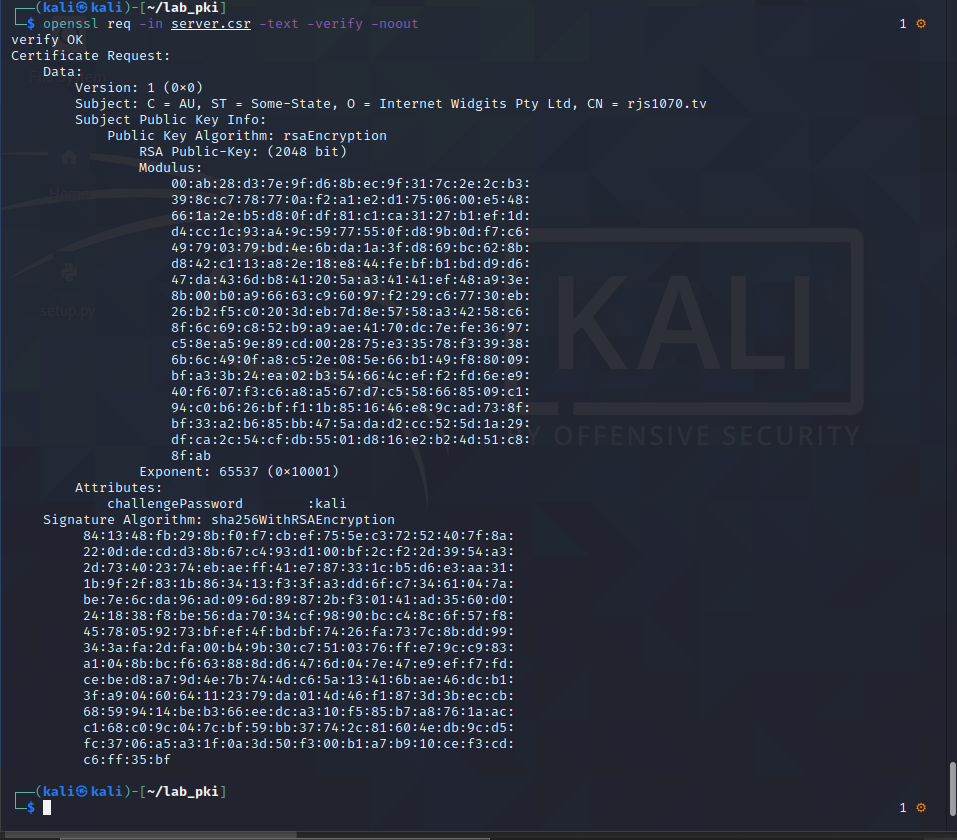
Task 3.1: (5 points) Include the command output in your lab report.



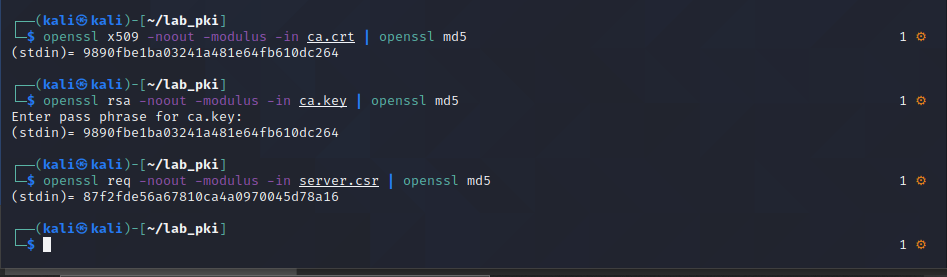
Task 3.2: (5 points) Include the command output in your lab report.



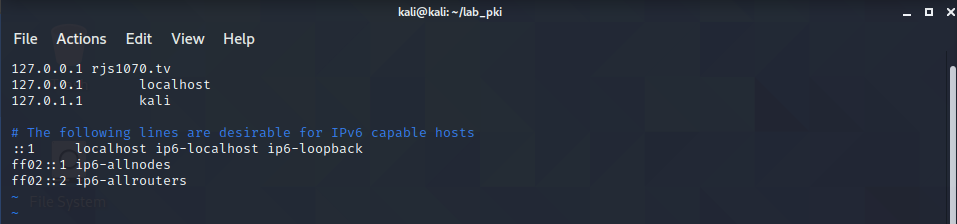
Task 3.3: (5 points) Include the command output in your lab report.



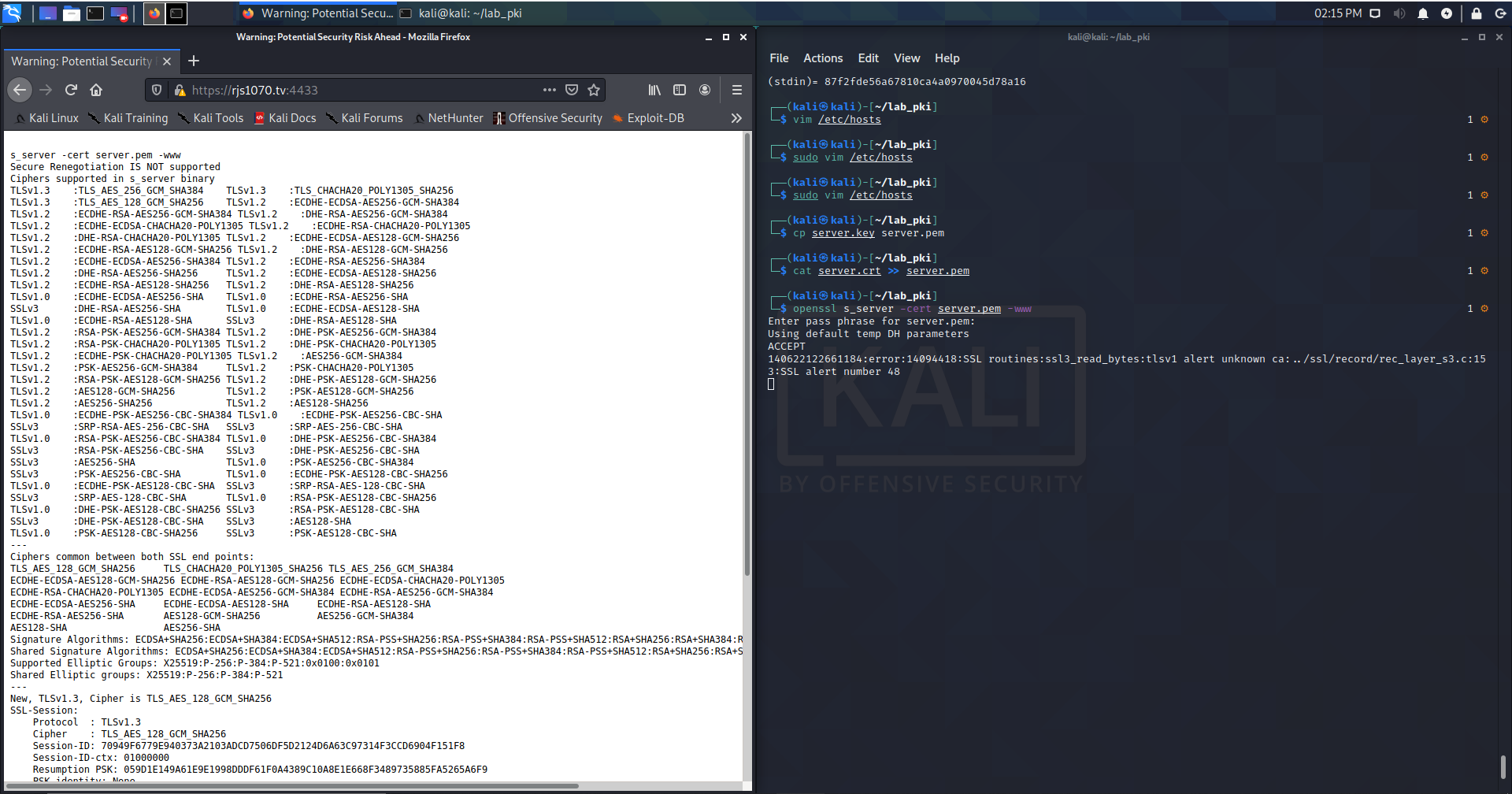
Task 3.4: (5 points) Include the command output in your lab report.



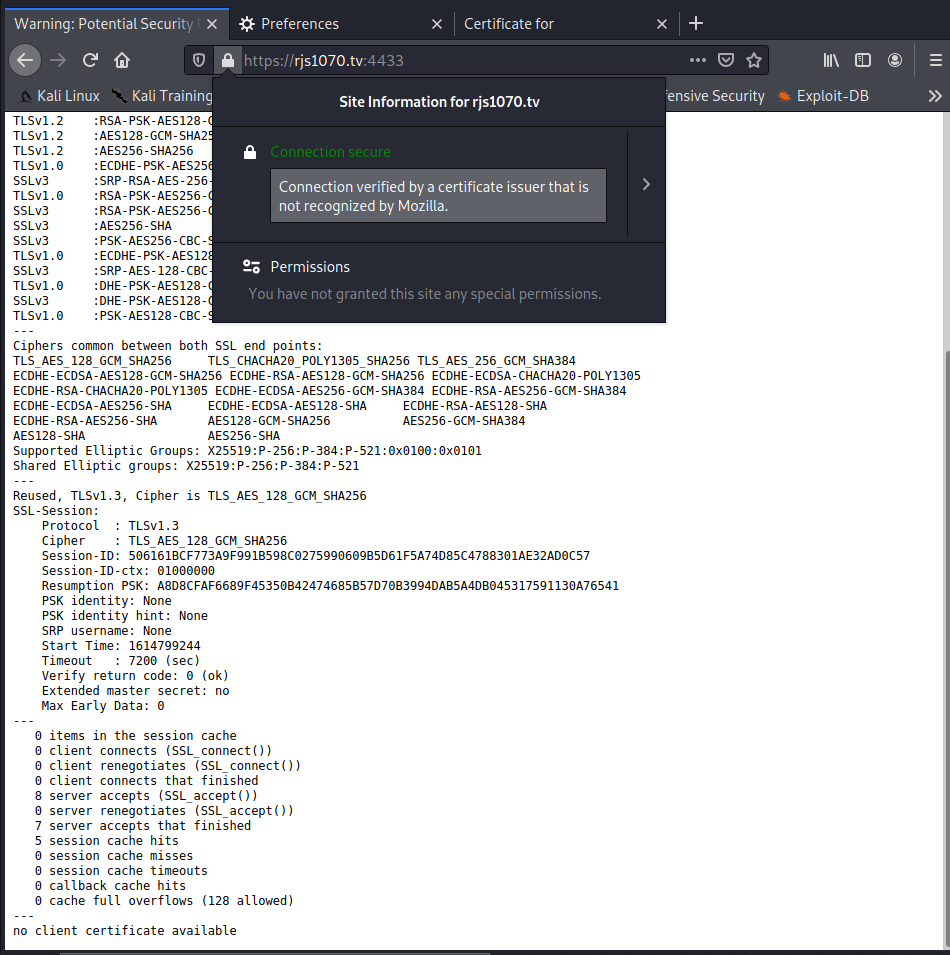
Task 4.1: (5 points) Provide the contents of your /etc/hosts file.



4.2: (5 points) Provide screenshots of your command and browser interaction.



Task 4.3: (10 points) Take a screenshot of the browser with the SSL lock turned green.



Task 5.1 (5 points) Sign the SHA256 hash of example.txt; save the output in example.signed.

Task 5.2 (5 points) Verify the digital signature in example.signed.

Task 5.3 (10 points) Slightly modify example.txt, and verify the digital signature again.

Nysize -> Nyside

Task 5.4: (5 points) Explain how binary data is in represented in the certificates created in this lab?

The binary data files are encoded and represented using base64

