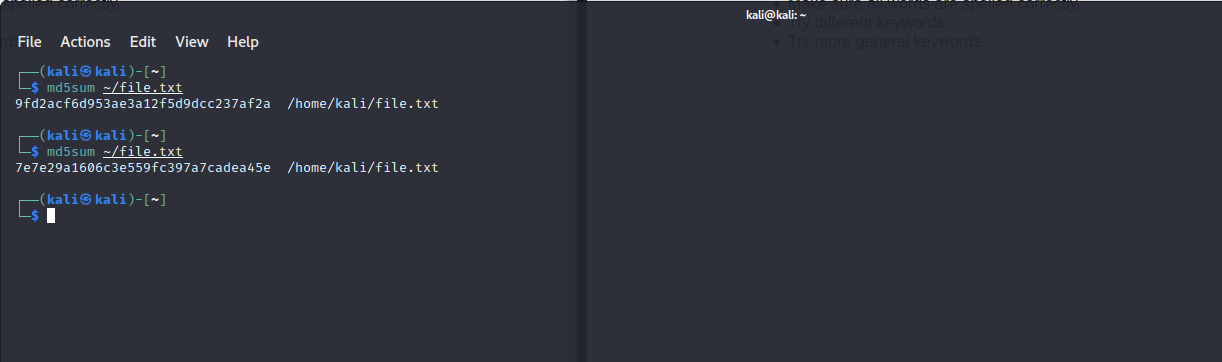
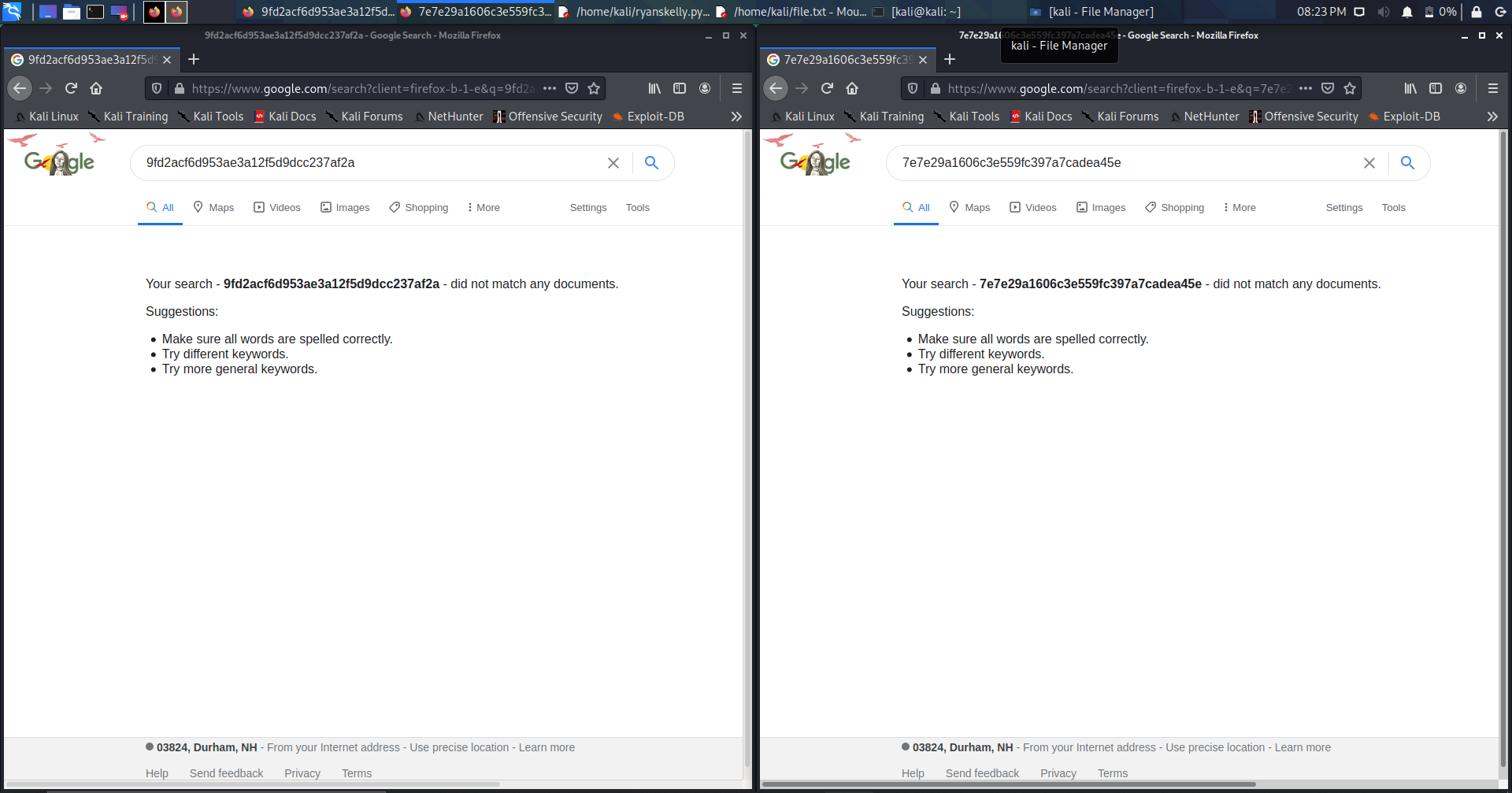
# IT666 – Password Cracking Lab

**Lab report**:

Task 1.1: (10 points) Provide screen shots of both md5sum commands

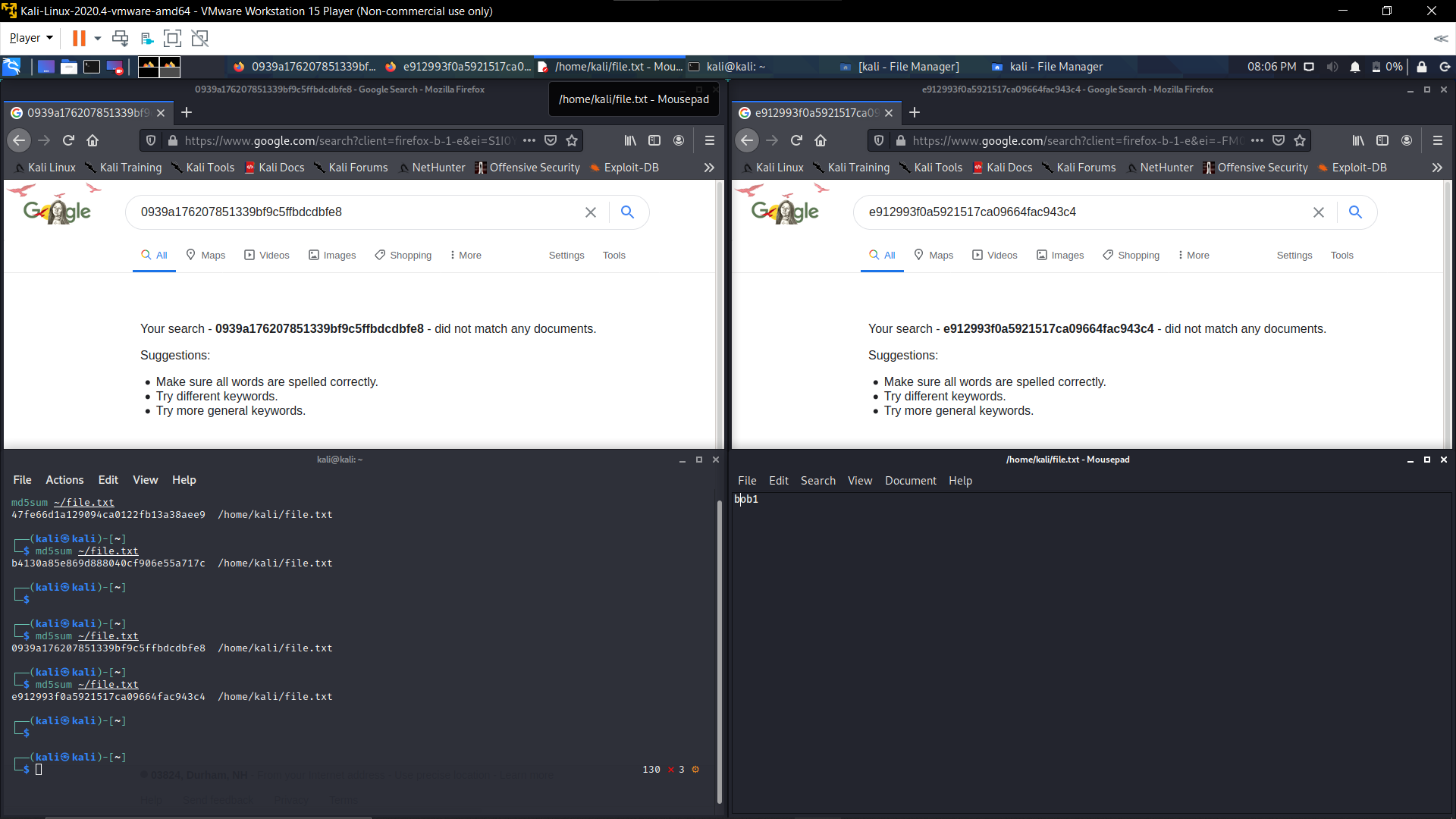


Task 1.2: (10 points) Provide screen shots of both Google search results.

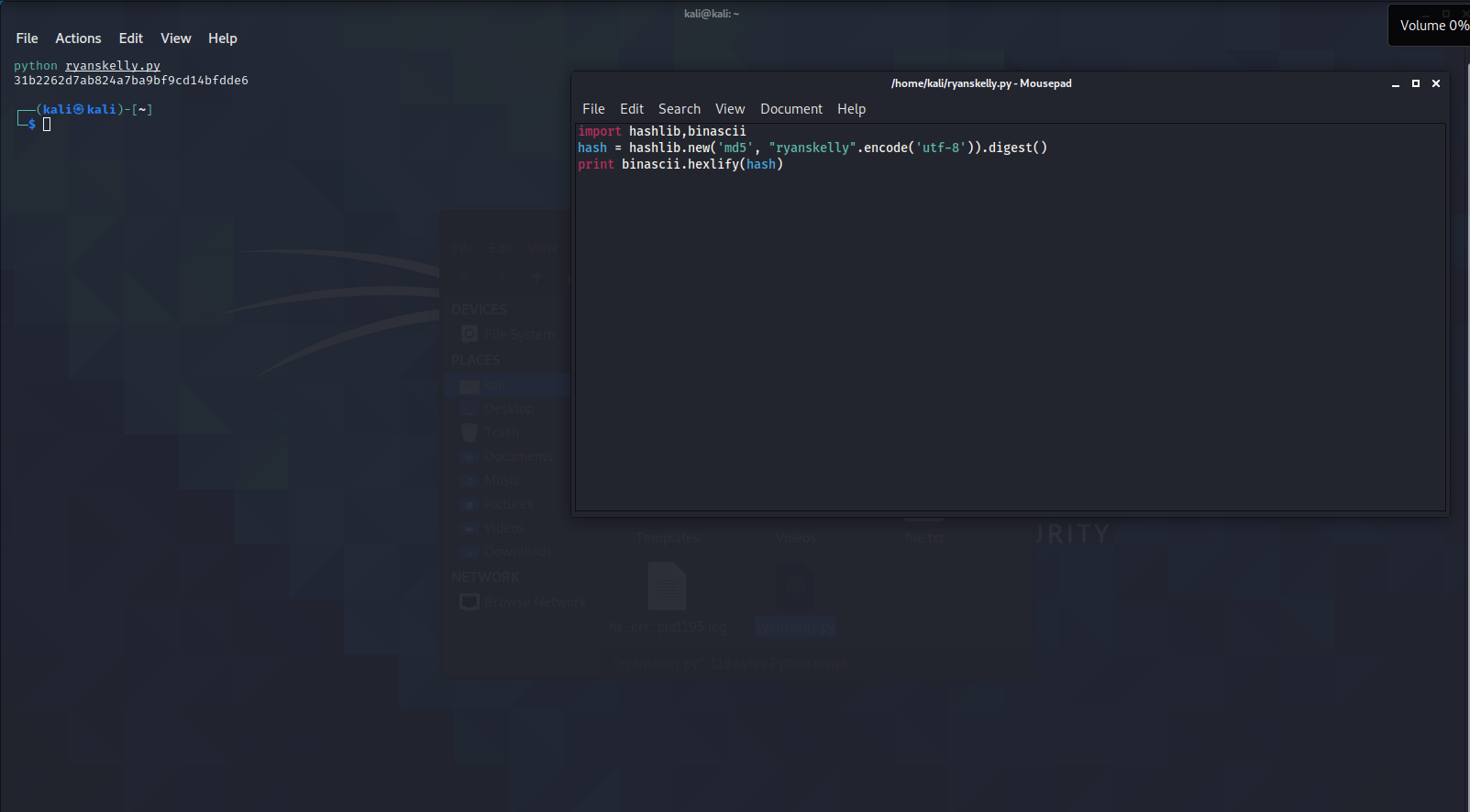


Task 1.3: (5 points) True/False: Does Google return the hash of "Bob1"

False



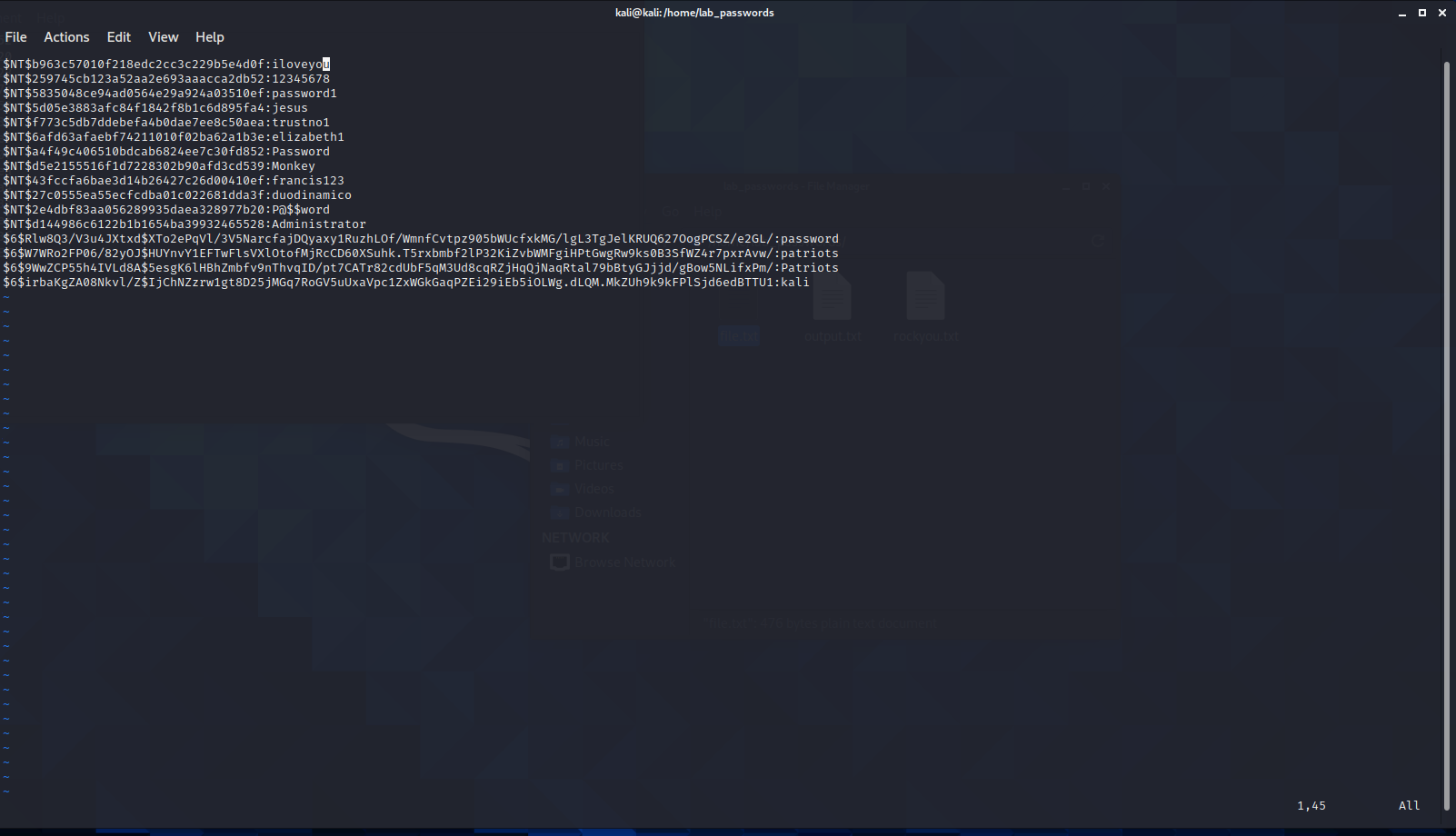
Task 2.1 (10 points) Include a screenshot of your command interaction.



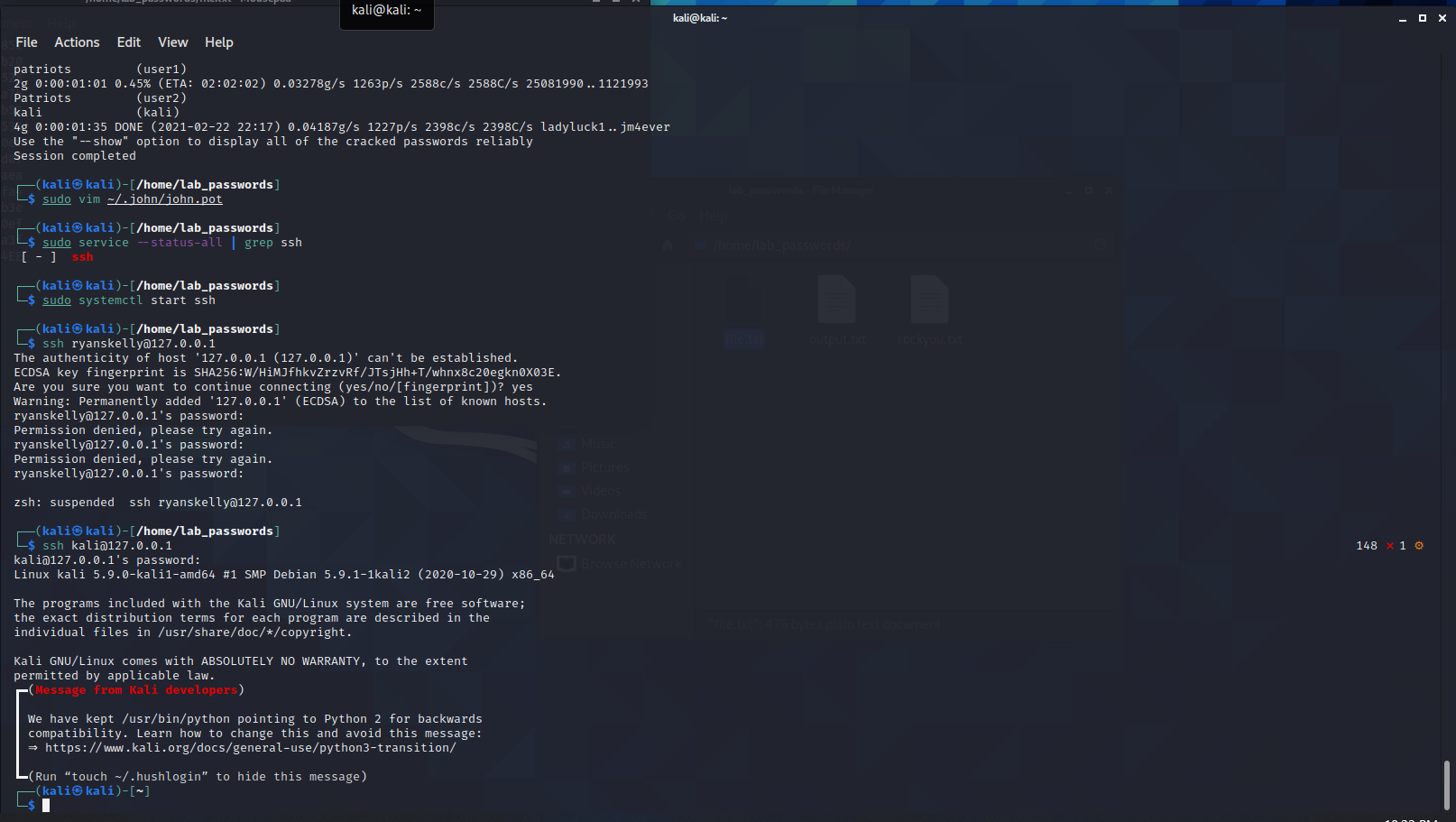
Task 3.1: (10 points) Provide the results stored in ~/.john/john.pot



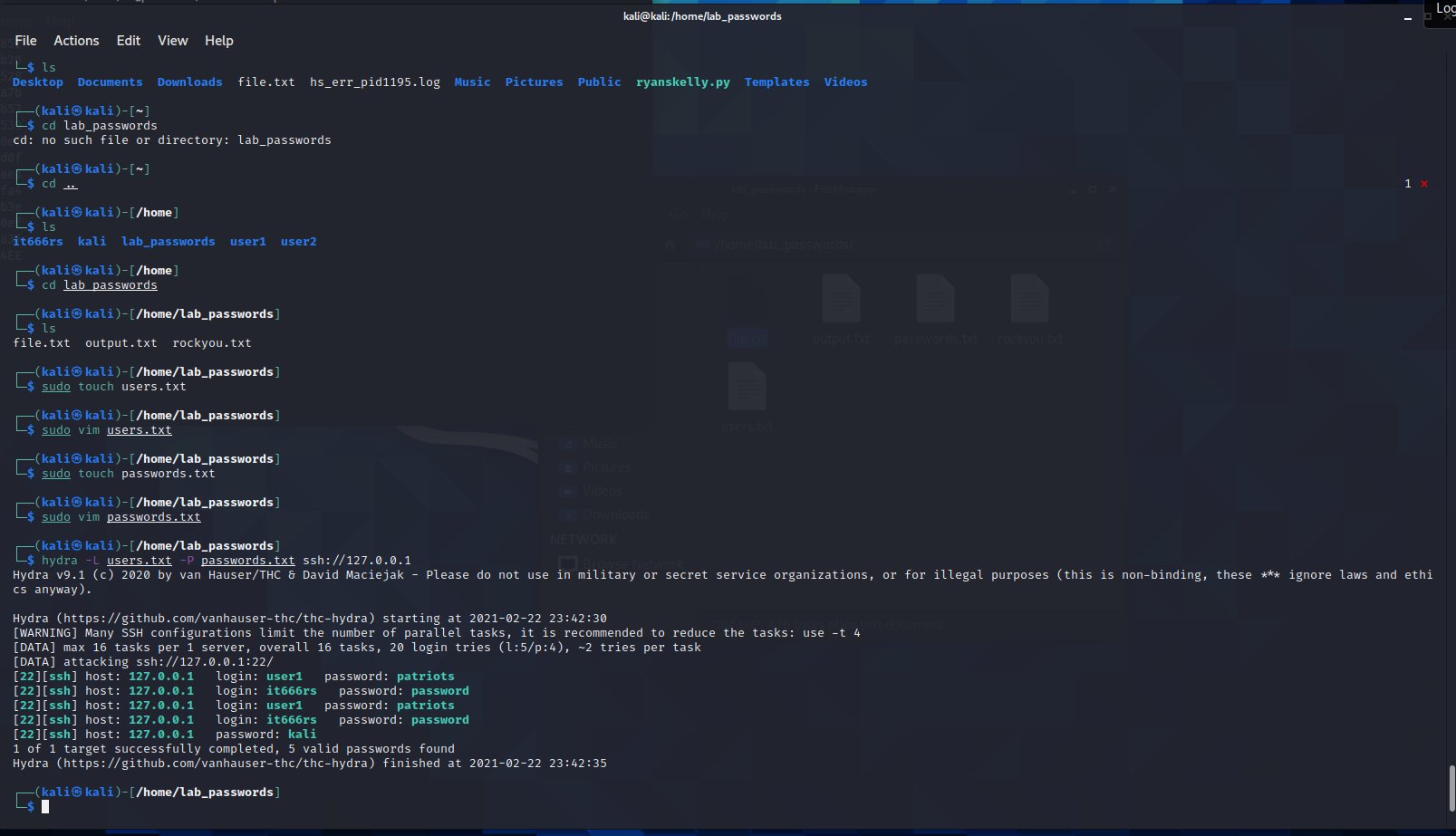
Task 3.2: (10 points) Provide the results stored in ~/.john/john.pot



Task 4.1: (10 points) Provide a screenshot showing you work.



Task 5.1: (15 points) Show your work to successfully run hydra



Task 5.2: (10 points) Explain what hydra did.

Hydra set up fake terminal/login instances and tried the logins in the text file, listed with the -L flag, paired with a password from the password file. The ssh in the command indicated what the system login type was and the IP was the IPv4 loopback addr, which is how this system can echo to itself.

Task 5.3: (10 points) True/False: Can you use hydra for attacking WWW and email logins?

True