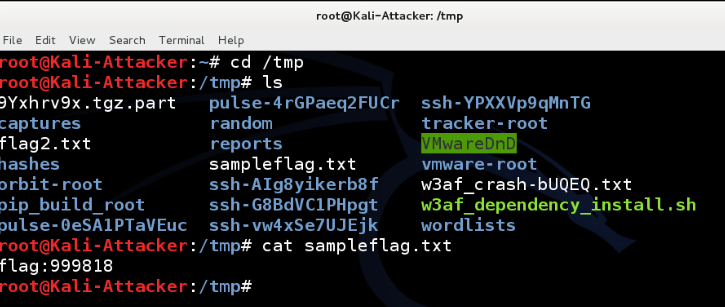
**ISEC 500 - Information Security Overview**

**Assignment 3 - Lab 3: Encrypting Data using TrueCrypt and Attacking the TrueCypt password using TrueCrack**

The requirements for this lab are to capture the screenshot of the below steps from given sections and submit in the word document.

**Part 1**

**challenge #1**



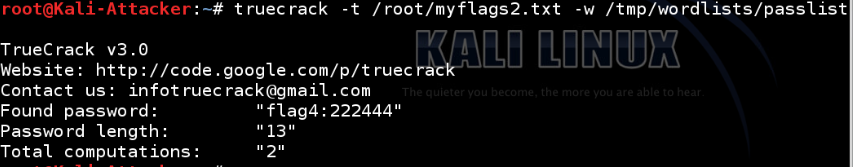
**challenge #2**



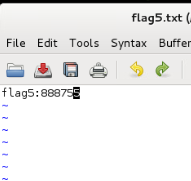
**challenge #3**



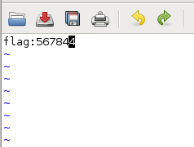
**challenge #4**



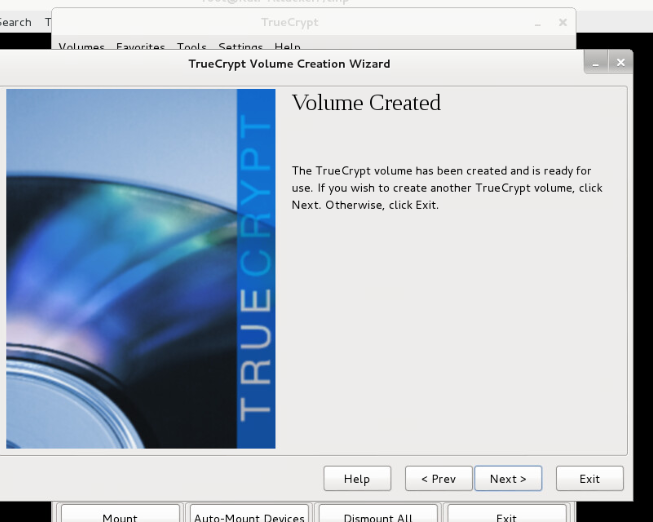
**challenge #5**

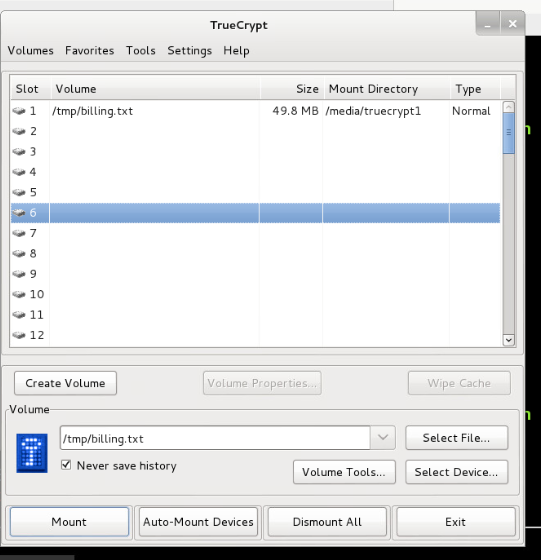


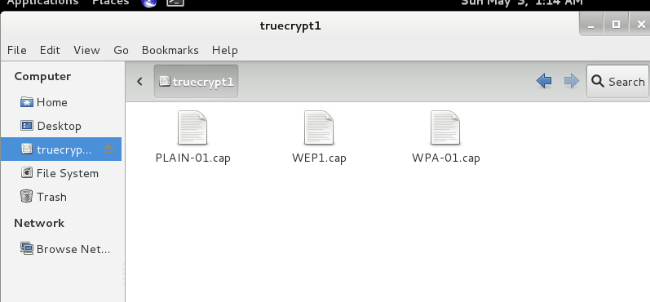
**challenge #6**

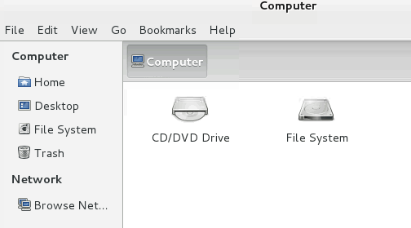


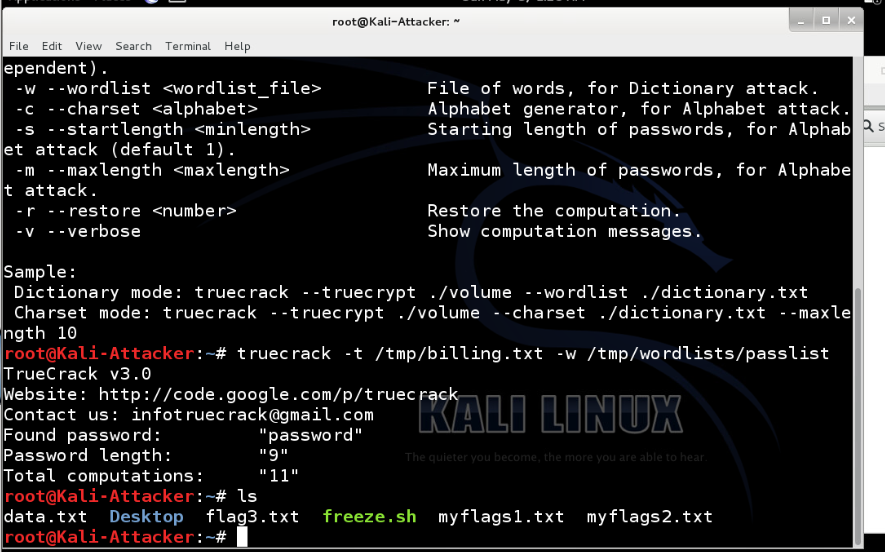
**Screenshots**

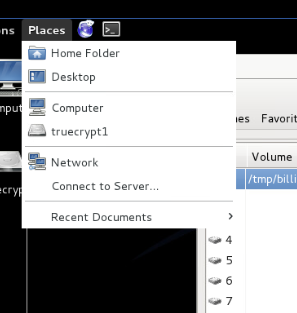












**PART 2**

I used veracrypt in the past. It looks identical to truecrypt. Apparently VeraCrypt is a fork of the discontinued TrueCrypt project. When I first used it, I really liked it and found it a very useful and easy to use encryption software.

[htps://www.veracrypt.fr/en/Beginner%27s%20Tutorial.html](https://www.veracrypt.fr/en/Beginner%27s%20Tutorial.html)

Computerphile and tom scott has some good videos on passwords.

<https://www.youtube.com/watch?v=7U-RbOKanYs>

<https://www.youtube.com/watch?v=3NjQ9b3pgIg>

<https://www.youtube.com/watch?v=8ZtInClXe1Q>

So basically, best passwords are long random collections of characters because they are hard to brute force and they are also hard to crack with dictionary attack. But these passwords are hard to remember. The solution is using few random words in a row. It will still be hard to brute force, and it will be hard to crack with dictionary attack because there are tons of wordsi n english. Trying every single combination ends up being hard even for computers.