



Advanced Networking Security
CS/IS 196

LAB25 REPORT

4/15/2022

DAVID ARCHER

Table of Contents

1. Introduction	3
2. Lab Results	3

1. Introduction

In this lab, I will be conducting data security practices using various tools and compare basic concepts of cryptography

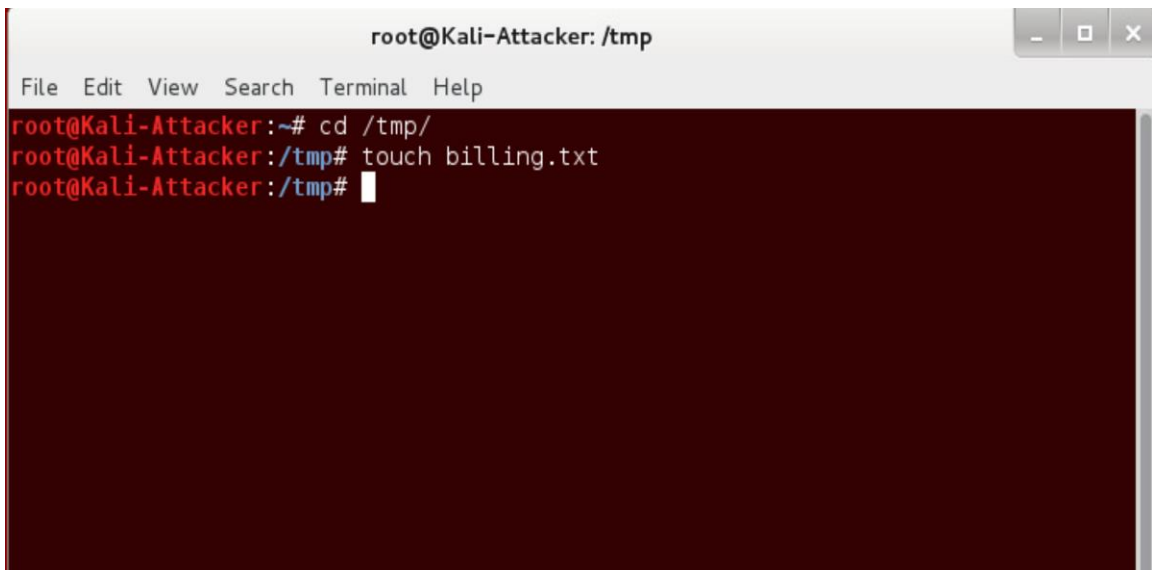
2. Lab Results

1 Creating a TrueCrypt Container

1.1 Creating a Container

4. Directory change

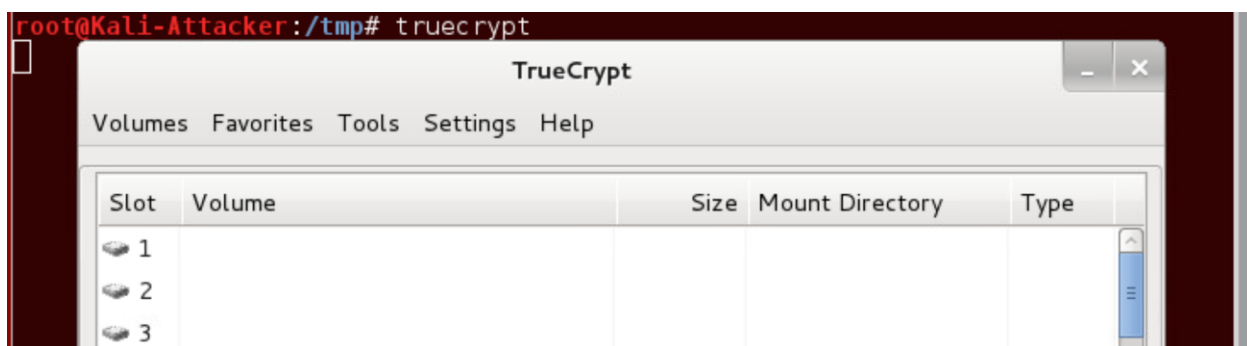
5. Creating a file.

A terminal window titled 'root@Kali-Attacker: /tmp' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

```
root@Kali-Attacker:~# cd /tmp/  
root@Kali-Attacker:/tmp# touch billing.txt  
root@Kali-Attacker:/tmp#
```

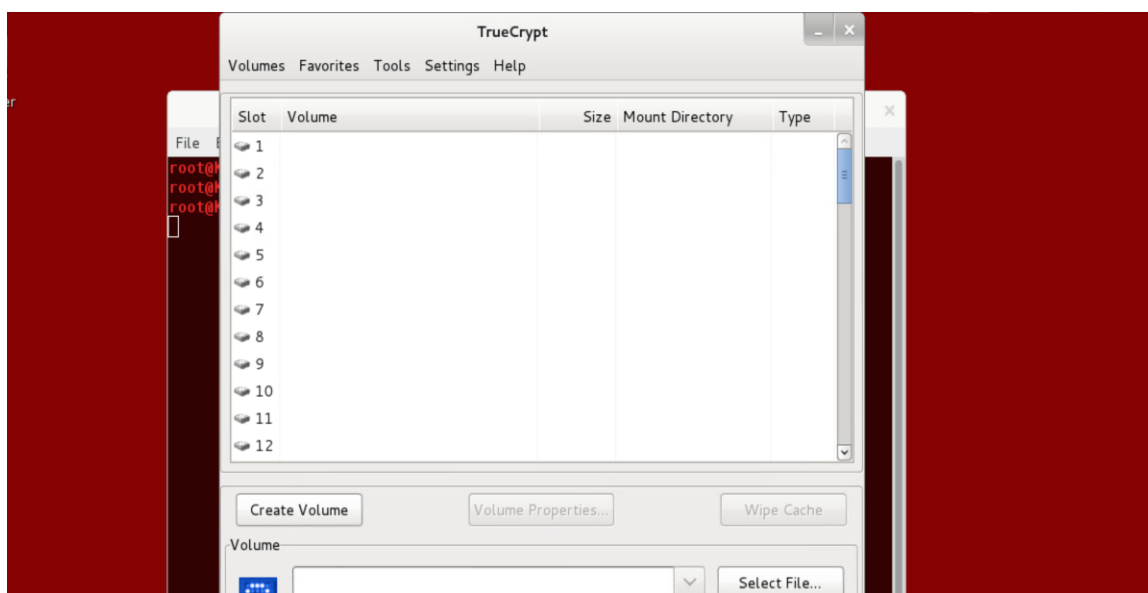
Changed to the **/tmp** directory.
Command used: **cd /tmp**
Created a text file named **billing.txt**.
Command used: **touch billing.txt**

6. TrueCrypt application.



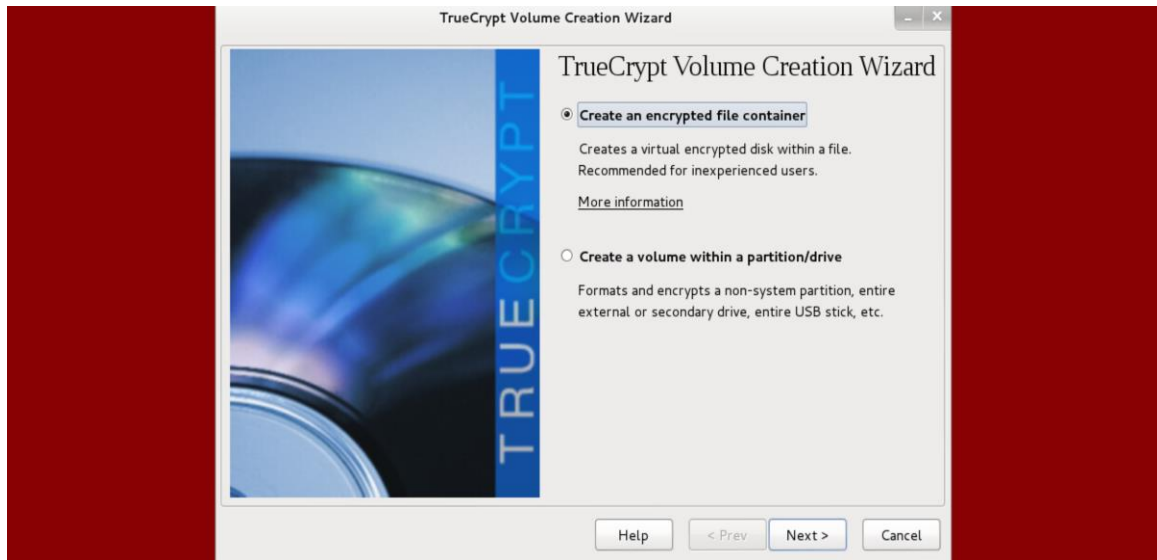
Launched the TrueCrypt application.
Command used: **truecrypt**

7. TrueCrypt application window.



Clicked on the **Create Volume** button.

8. TrueCrypt Volume Creation Wizard.



Selected **Create an encrypted file container** option and clicked **Next**.

9. Volume Type



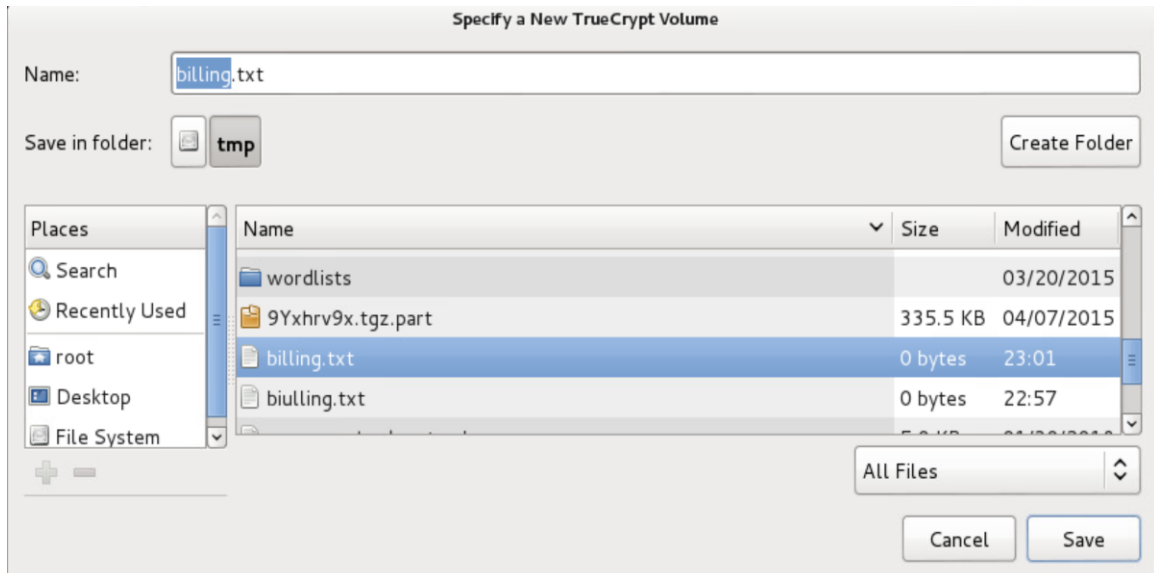
Selected the **Standard TrueCrypt volume** option and clicked **Next**

10. Volume Location



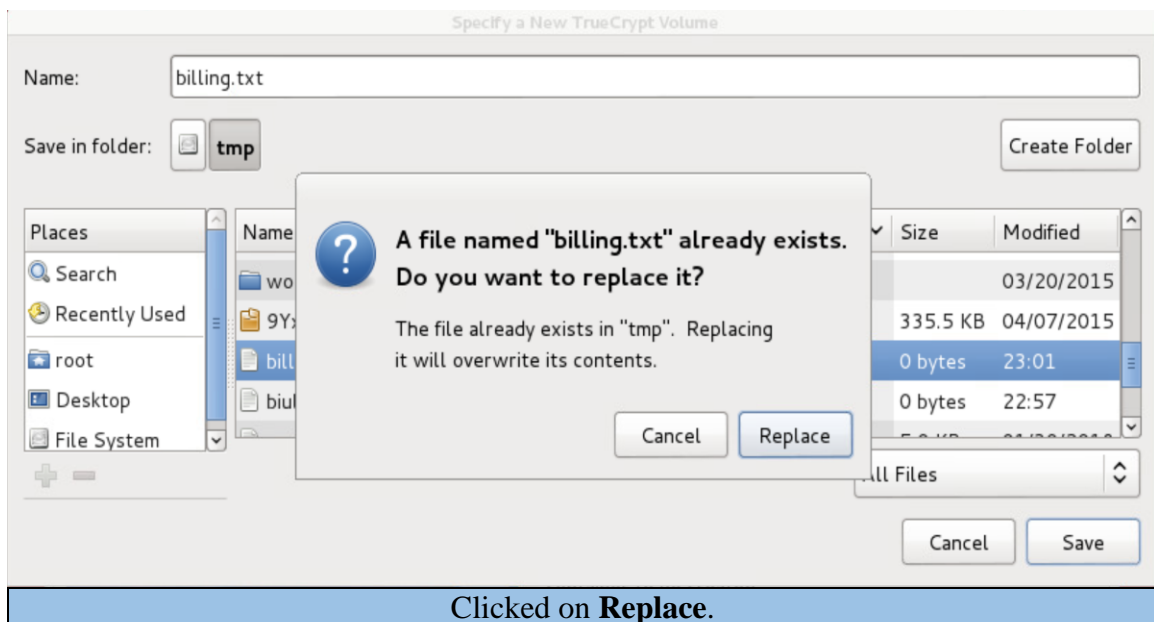
Clicked on the **Select File** button

11. File Manager window



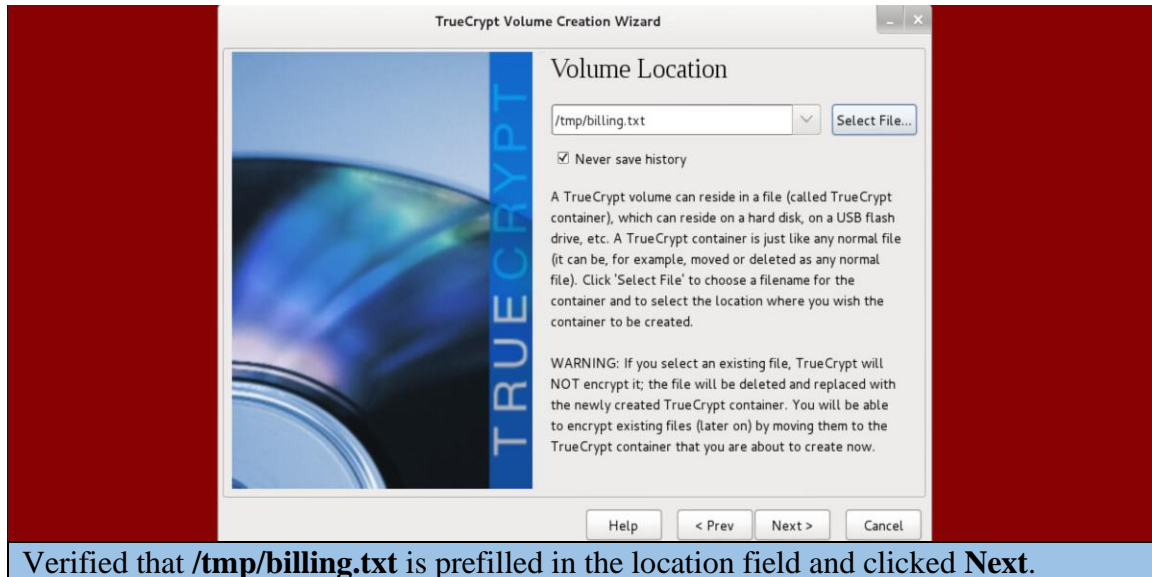
Navigated to **File System** > **tmp**. Select the **billing.txt** file and clicked **Save**.

12. File replace.

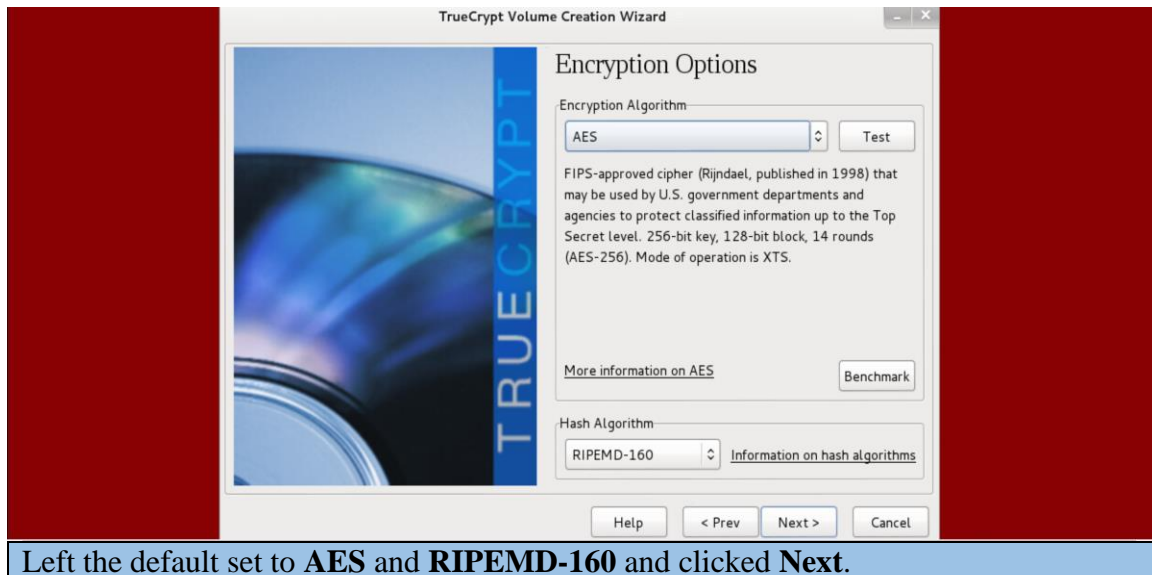


Clicked on **Replace**.

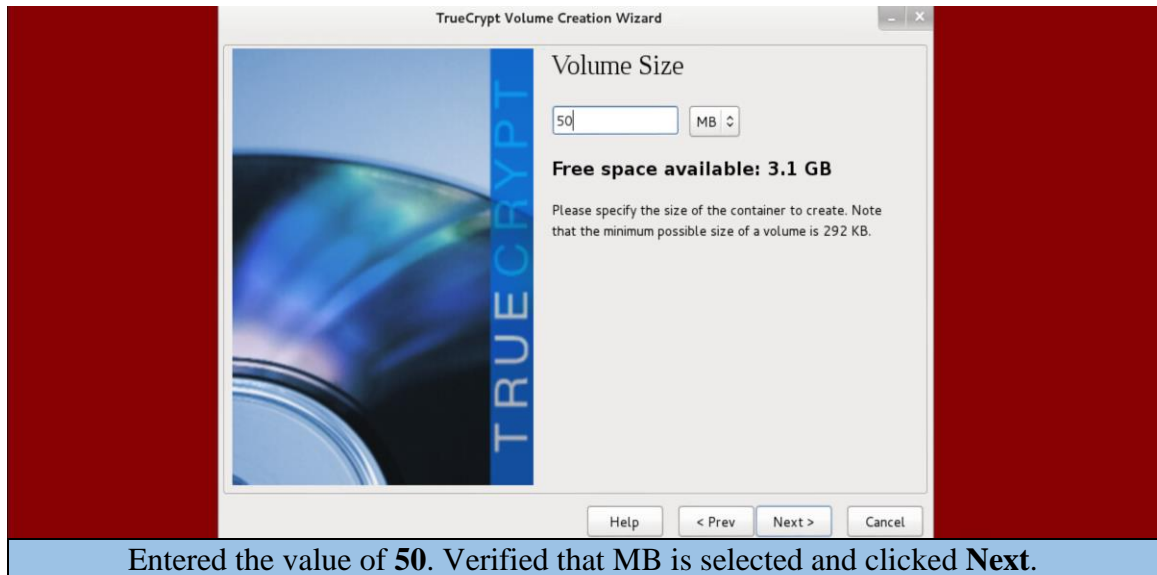
13. TrueCrypt Volume Creation Wizard window.



14. Encryption Options



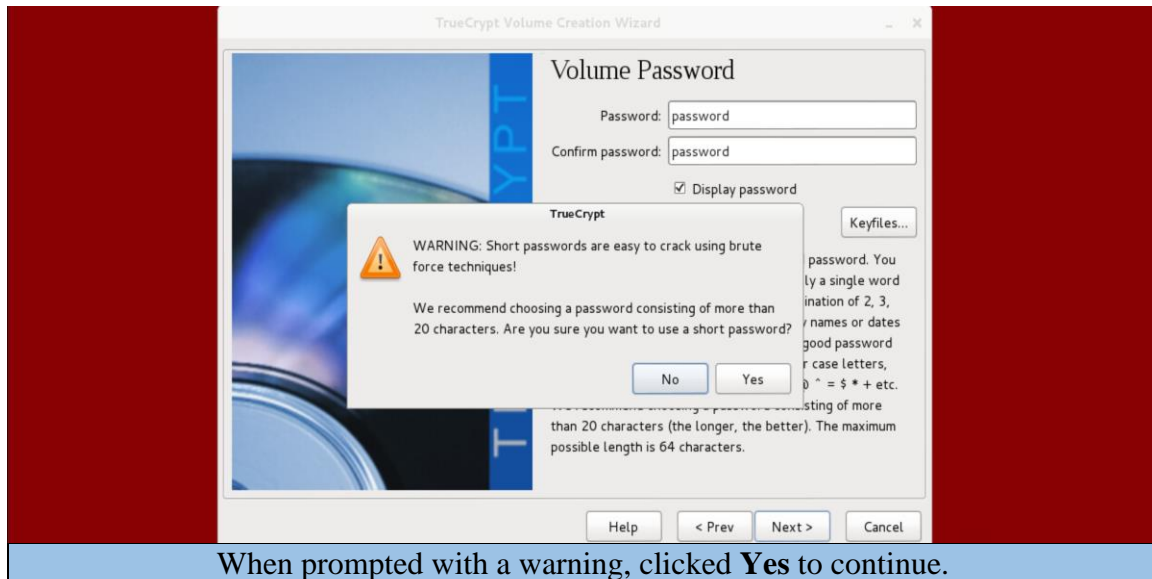
15. Volume Size



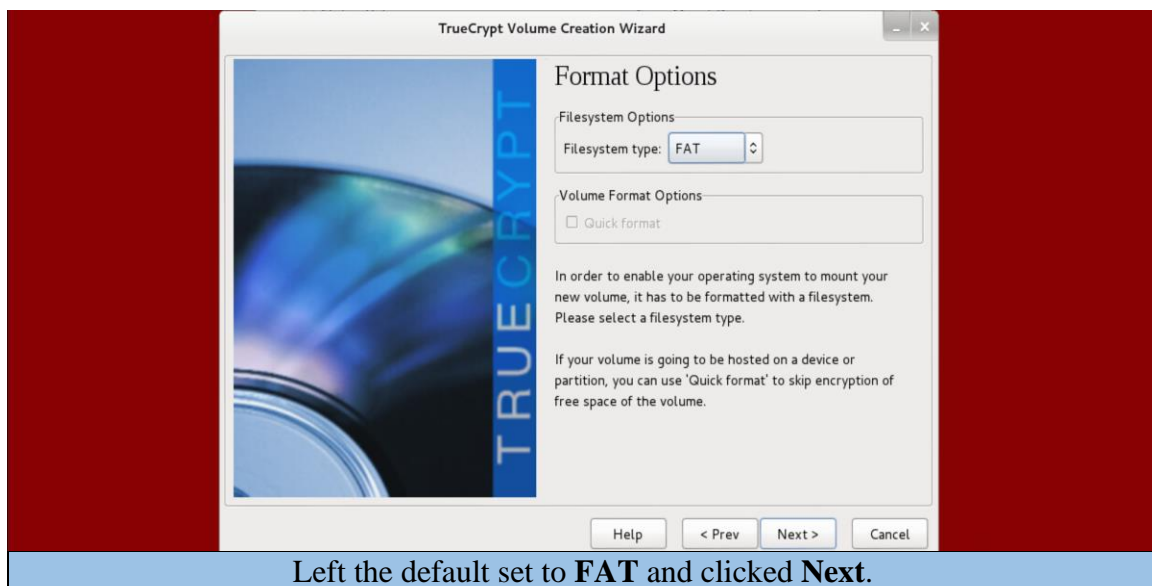
16. Volume Password.



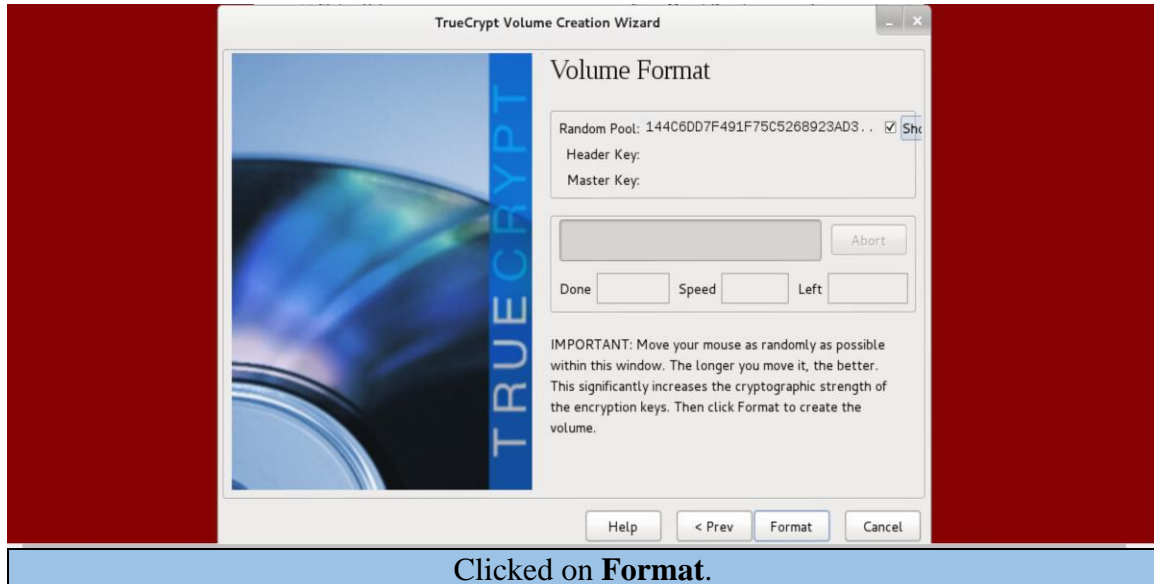
17. Warning prompt.



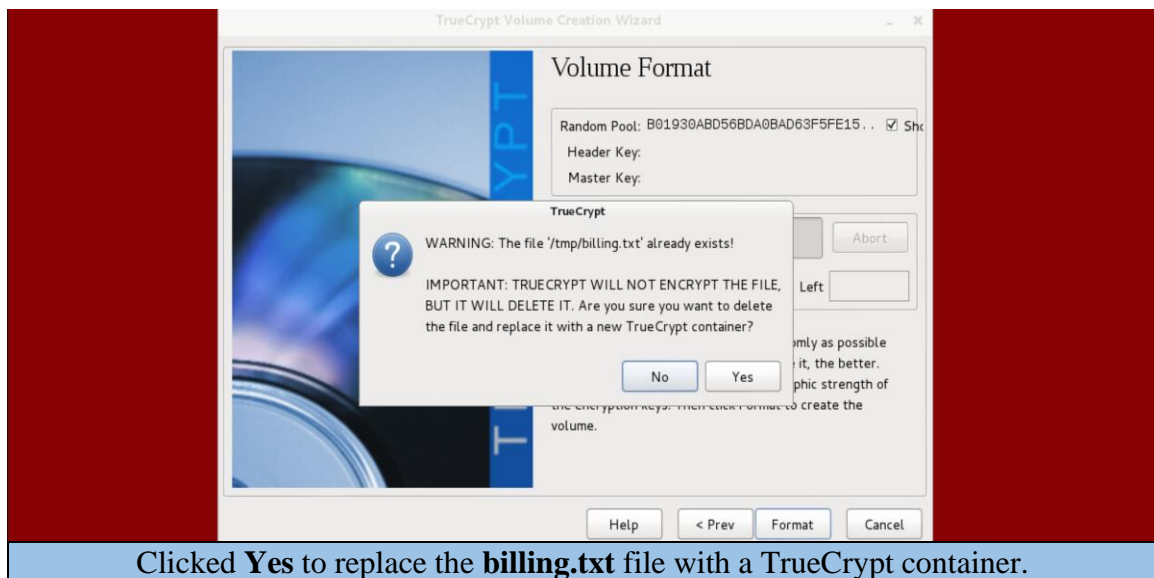
18. Format Options



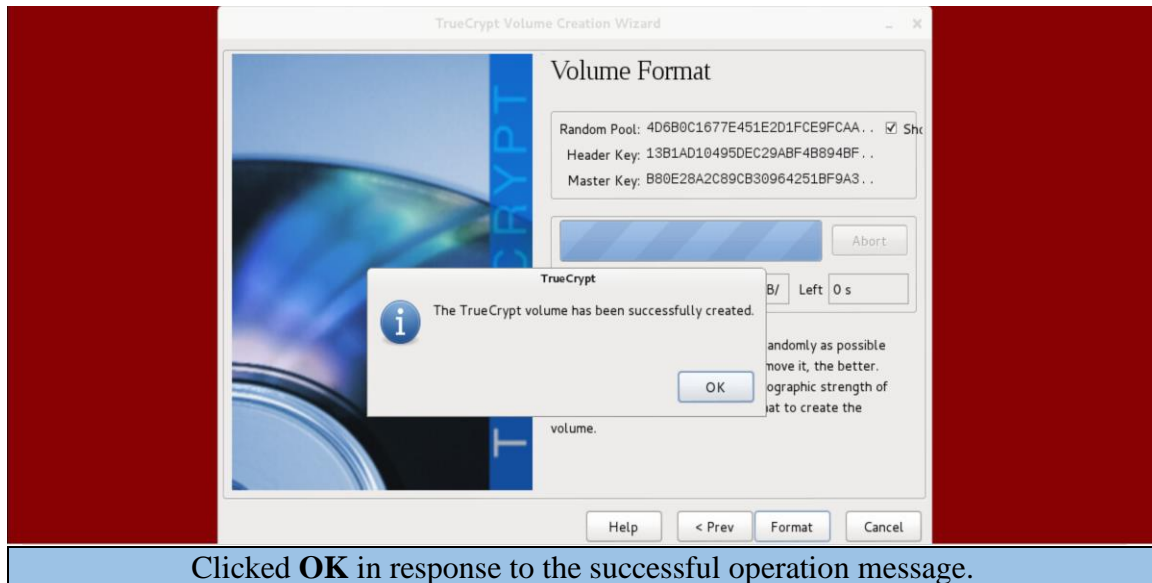
19. Volume Format



20. Warning prompt.



21. Success message.



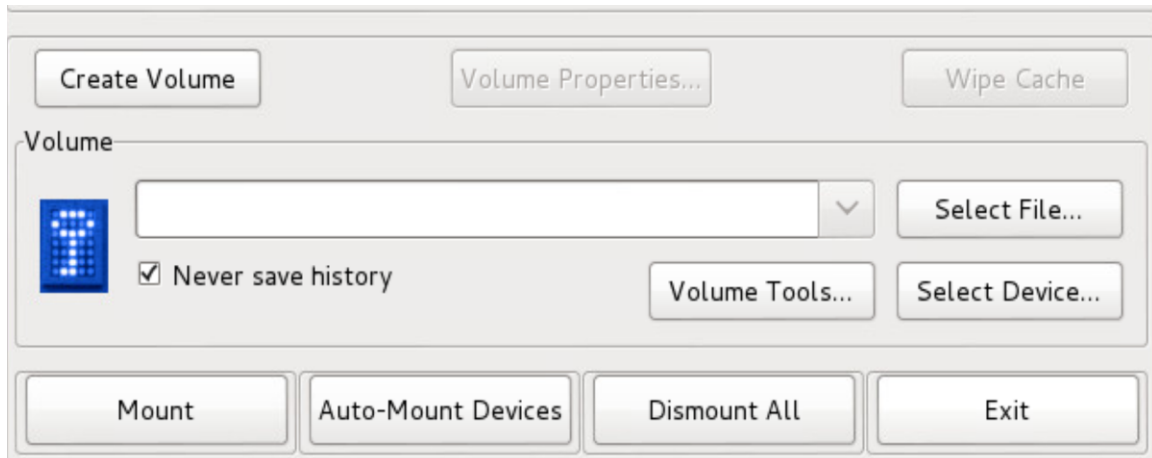
22. Volume Created



2. Opening and Viewing Data within a TrueCrypt Container

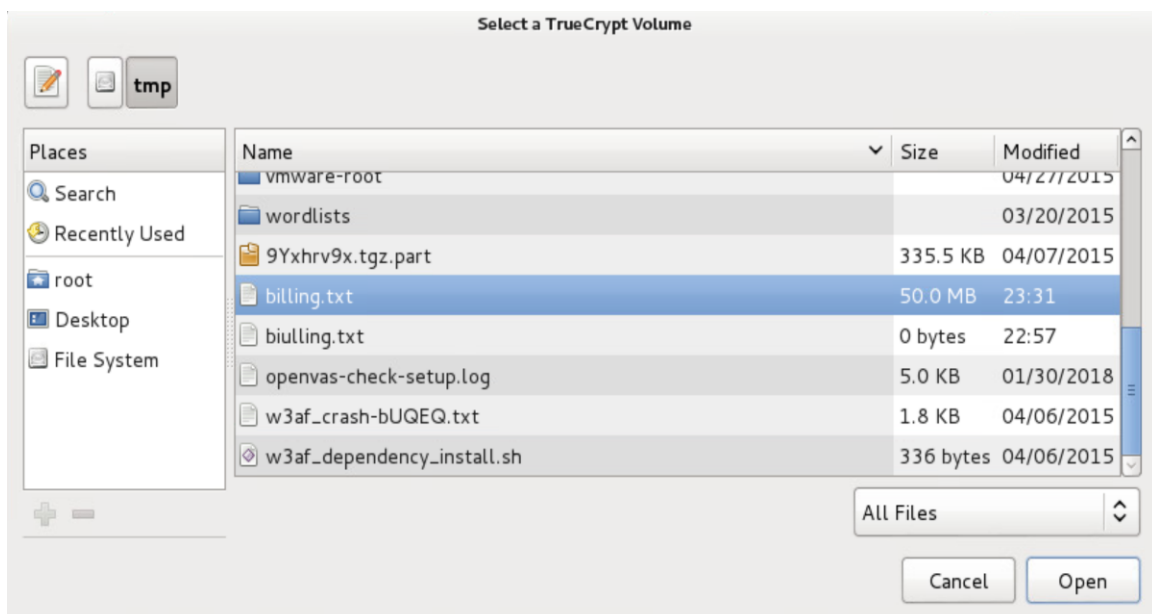
2.1 Using the TrueCrypt Container

1. Select File.



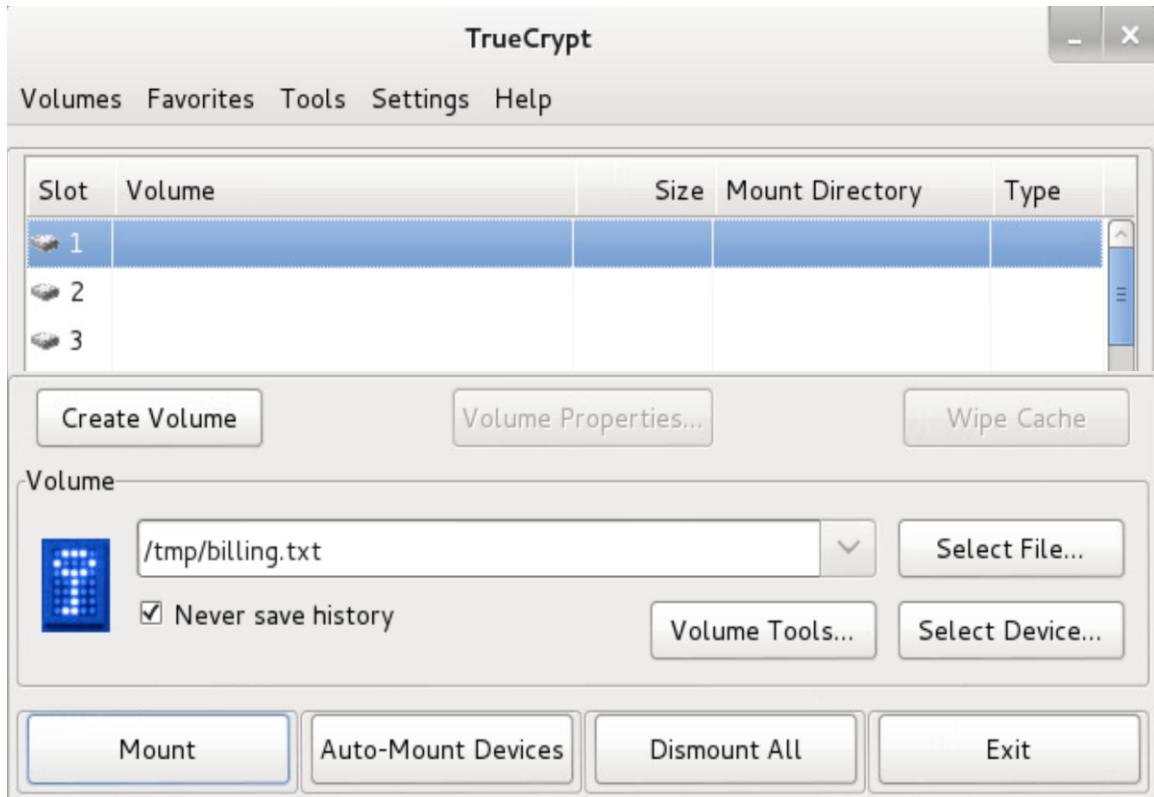
From the TrueCrypt application, clicked on the **Select File** button to locate my TrueCrypt container.

2. File Manager window



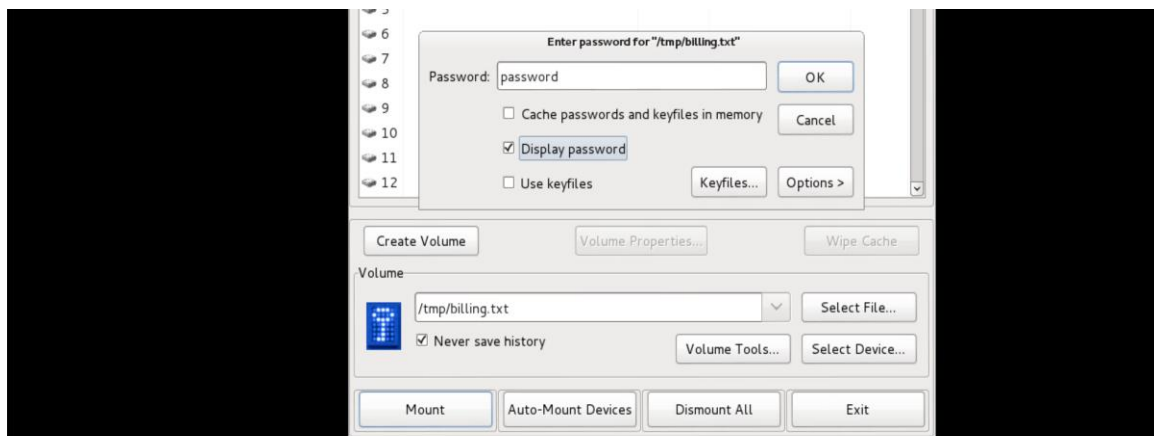
Navigated to **File System** > **tmp** and selected the **billing.txt** file. Clicked Open.

3. Drives.



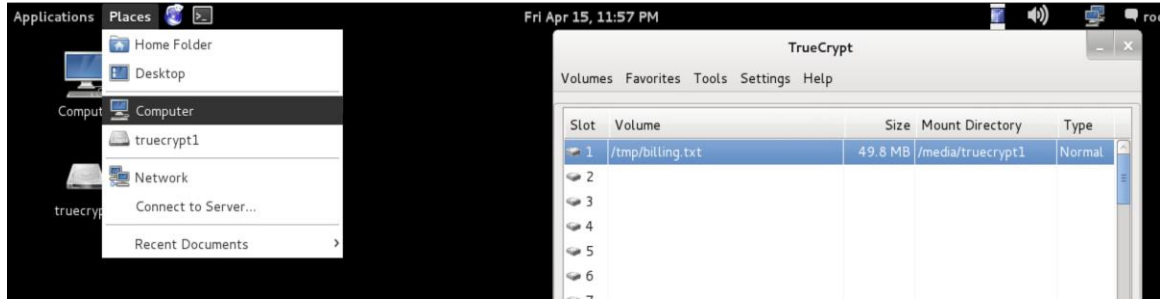
Selected one available drive slot from the list and then clicked on the Mount button.

4. Password prompt.



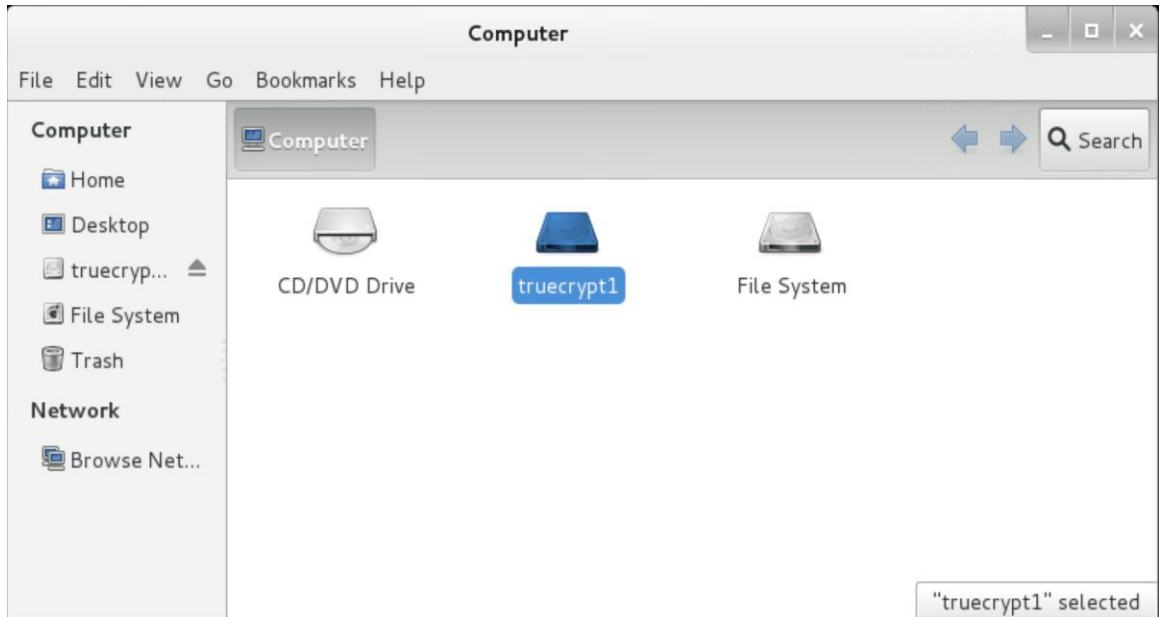
Typed **password** when prompted for a password and clicked **OK**.

5. Successful mount.



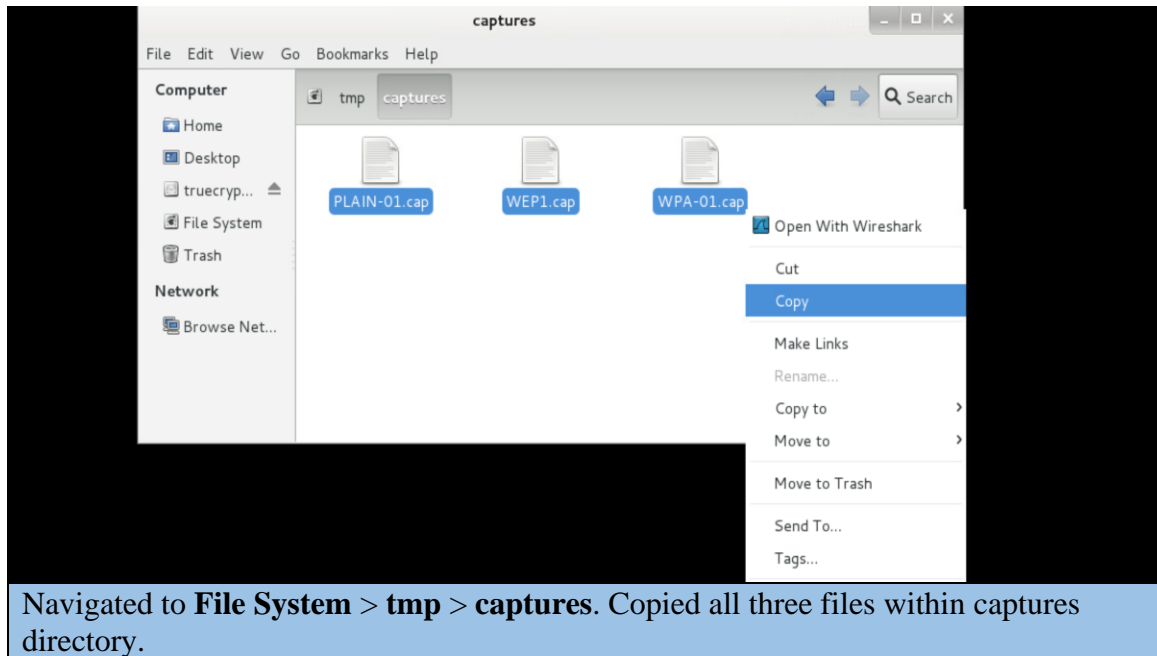
Selected the **Places** menu option located on the top menu pane and clicked on the **Computer** entry.

6. File Manager window.

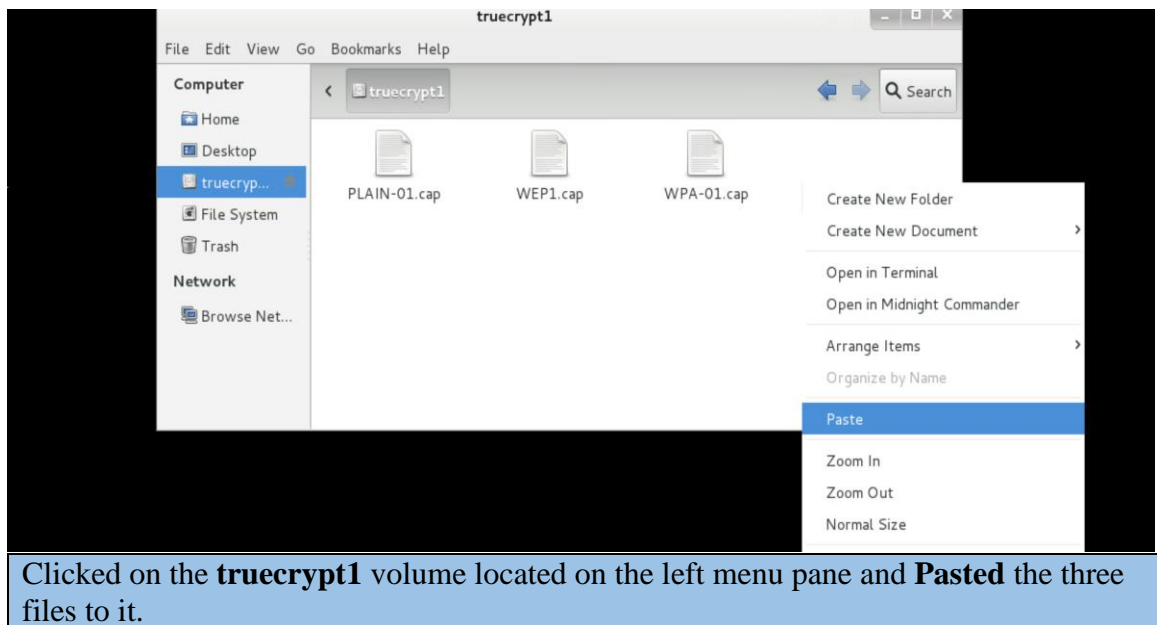


truecrypt1 is mounted to the system.

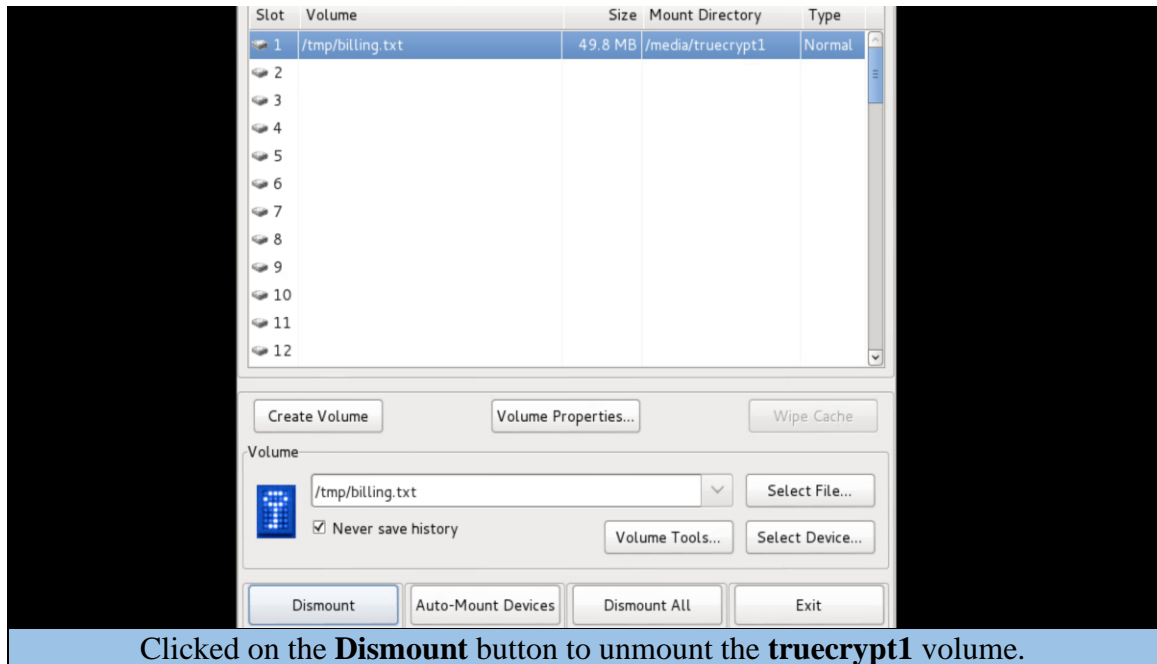
7. File Explorer window.



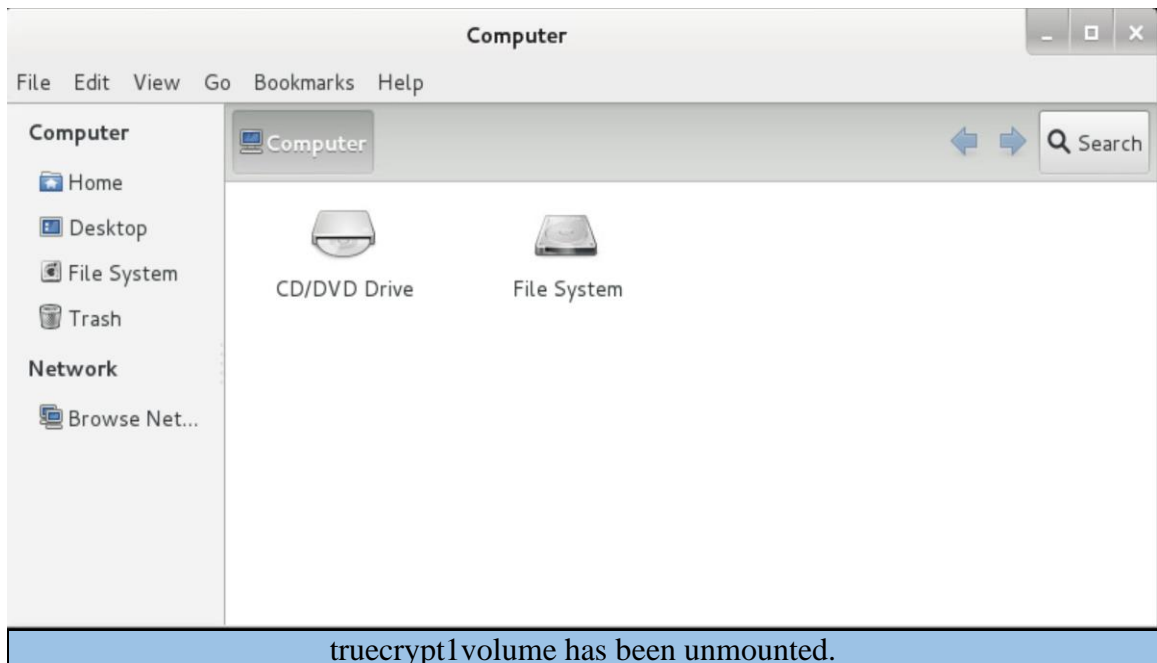
9. truecrypt1 volume



11. Dismount



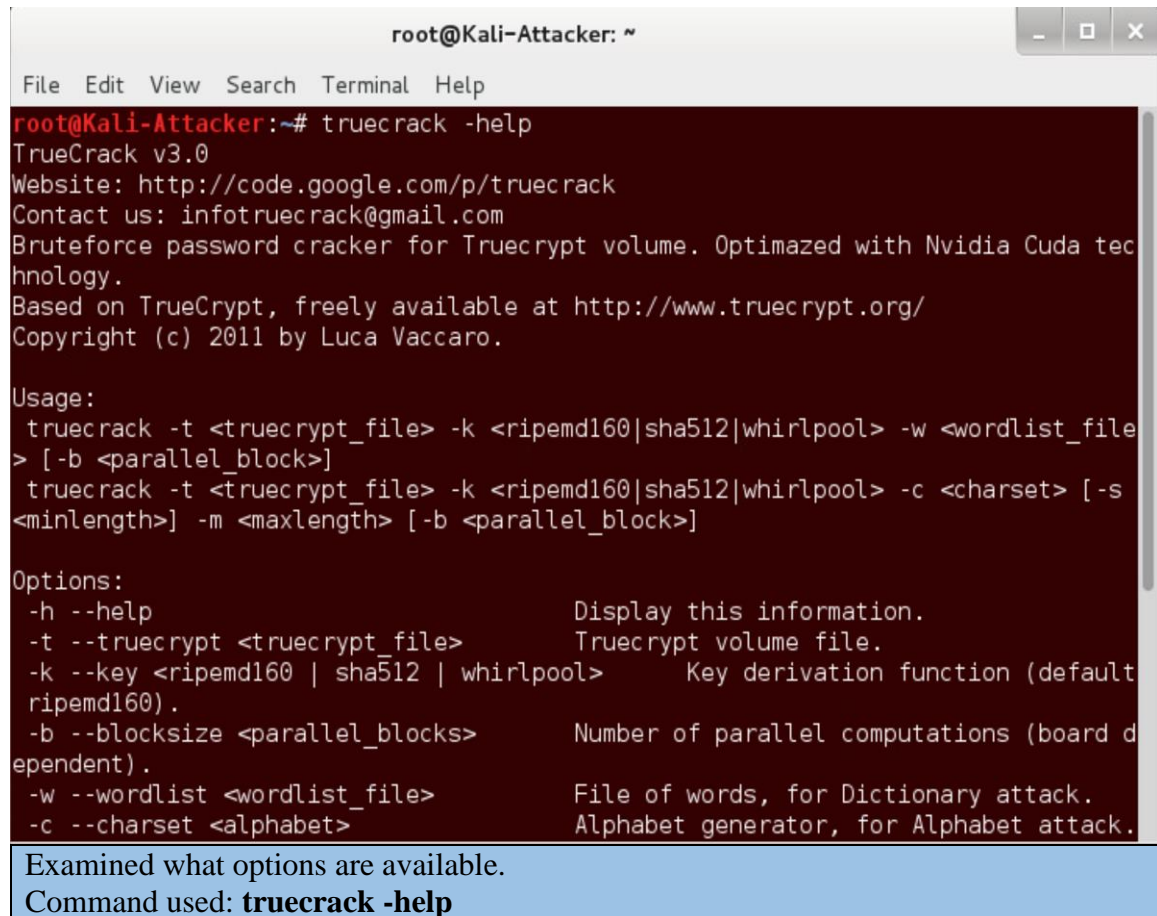
13. truecrypt1volume.



3 Bruteforcing a TrueCrypt Container

3.1 Using TrueCrack

1. New terminal.
2. TrueCrack application.



The screenshot shows a terminal window titled 'root@Kali-Attacker: ~'. The terminal displays the output of the command 'truecrack -help'. The output includes the version 'TrueCrack v3.0', website 'http://code.google.com/p/truecrack', contact 'infotruecrack@gmail.com', and a description: 'Bruteforce password cracker for Truecrypt volume. Optimized with Nvidia Cuda technology. Based on TrueCrypt, freely available at http://www.truecrypt.org/ Copyright (c) 2011 by Luca Vaccaro.' It also shows the usage and options for the tool.

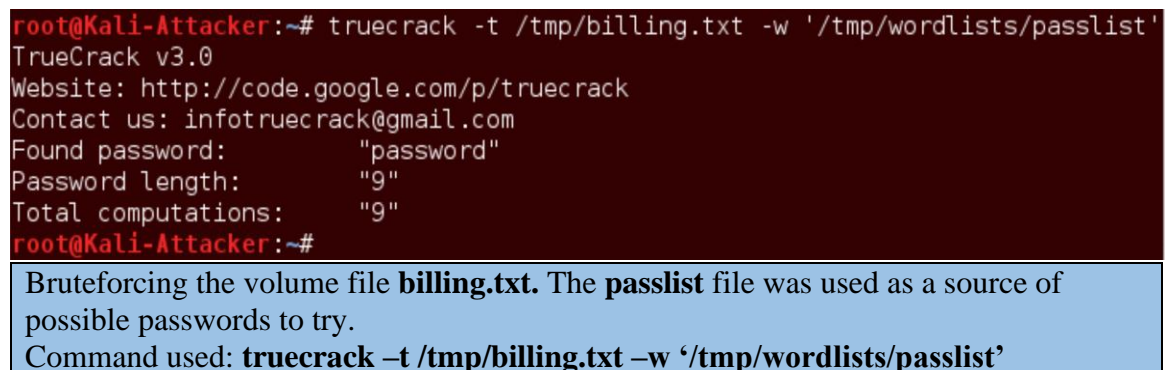
```
root@Kali-Attacker: ~
File Edit View Search Terminal Help
root@Kali-Attacker:~# truecrack -help
TrueCrack v3.0
Website: http://code.google.com/p/truecrack
Contact us: infotruecrack@gmail.com
Bruteforce password cracker for Truecrypt volume. Optimized with Nvidia Cuda technology.
Based on TrueCrypt, freely available at http://www.truecrypt.org/
Copyright (c) 2011 by Luca Vaccaro.

Usage:
truecrack -t <truecrypt_file> -k <ripemd160|sha512|whirlpool> -w <wordlist_file> [-b <parallel_block>]
truecrack -t <truecrypt_file> -k <ripemd160|sha512|whirlpool> -c <charset> [-s <minlength>] -m <maxlength> [-b <parallel_block>]

Options:
-h --help                                Display this information.
-t --truecrypt <truecrypt_file>          Truecrypt volume file.
-k --key <ripemd160 | sha512 | whirlpool> Key derivation function (default ripemd160).
-b --blocksize <parallel_blocks>         Number of parallel computations (board dependent).
-w --wordlist <wordlist_file>            File of words, for Dictionary attack.
-c --charset <alphabet>                  Alphabet generator, for Alphabet attack.
```

Examined what options are available.
Command used: **truecrack -help**

3. TrueCrypt volume file



The screenshot shows a terminal window titled 'root@Kali-Attacker: ~'. The terminal displays the output of the command 'truecrack -t /tmp/billing.txt -w '/tmp/wordlists/passlist''. The output shows the version 'TrueCrack v3.0', website 'http://code.google.com/p/truecrack', contact 'infotruecrack@gmail.com', and the results of the bruteforce attack: 'Found password: "password"', 'Password length: "9"', and 'Total computations: "9"'. The prompt returns to 'root@Kali-Attacker:~#'.

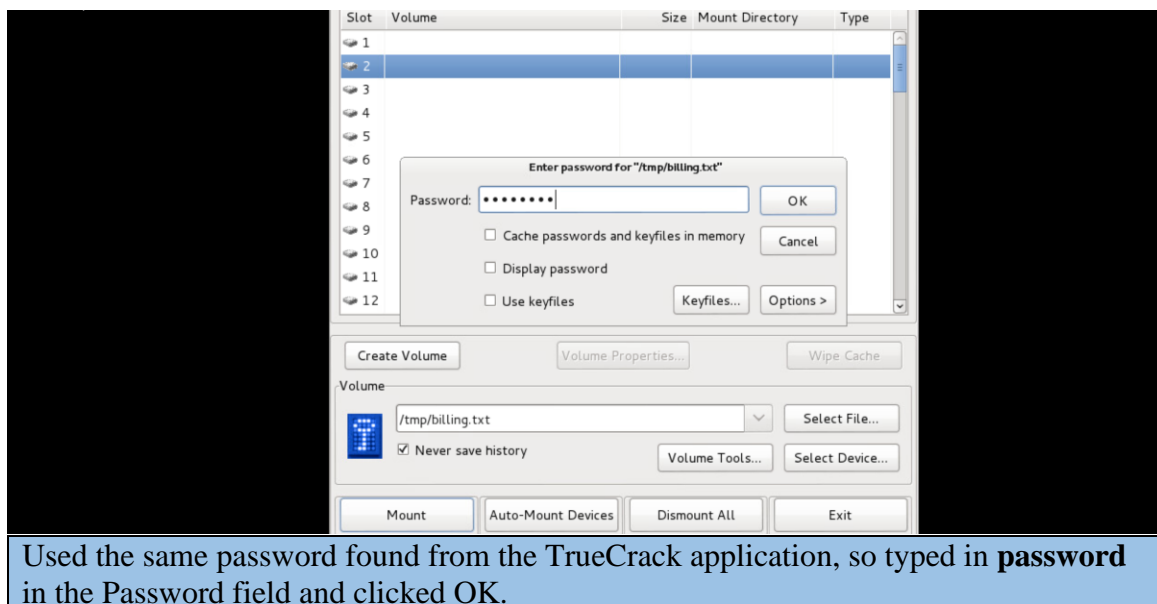
```
root@Kali-Attacker:~# truecrack -t /tmp/billing.txt -w '/tmp/wordlists/passlist'
TrueCrack v3.0
Website: http://code.google.com/p/truecrack
Contact us: infotruecrack@gmail.com
Found password: "password"
Password length: "9"
Total computations: "9"
root@Kali-Attacker:~#
```

Bruteforcing the volume file **billing.txt**. The **passlist** file was used as a source of possible passwords to try.
Command used: **truecrack -t /tmp/billing.txt -w '/tmp/wordlists/passlist'**

4. TrueCrypt application.



5. Password prompt



6. Successful mount.

