



Security+ Lab Series

Lab 25: Securing Data with Encryption Software

Document Version: 2020-12-10

Copyright © 2020 Network Development Group, Inc.
www.netdevgroup.com

NETLAB Academy Edition, NETLAB Professional Edition, NETLAB+ Virtual Edition, and NETLAB+ are registered trademarks of Network Development Group, Inc.

Contents

Introduction	3
Objectives.....	3
Lab Topology	4
Lab Settings	5
1 Creating a TrueCrypt Container	6
1.1 Creating a Container	6
2 Opening and Viewing Data within a TrueCrypt Container	15
2.1 Using the TrueCrypt Container	15
3 Bruteforcing a TrueCrypt Container	21
3.1 Using TrueCrack.....	21

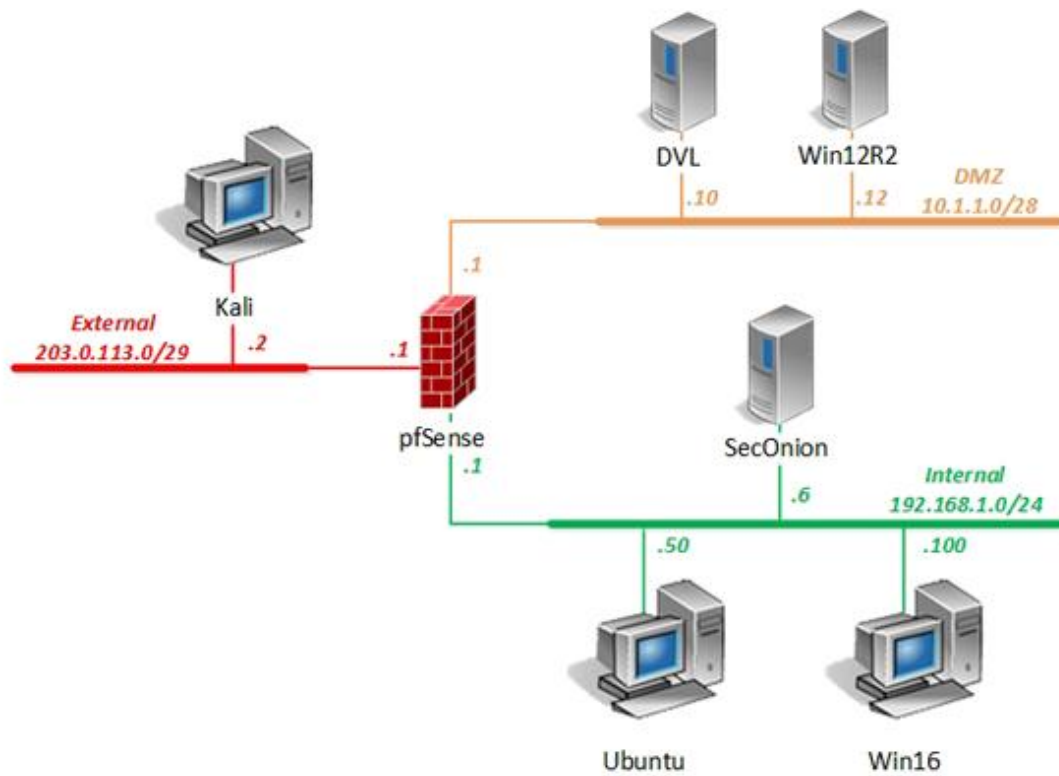
Introduction

In this lab, you will be conducting data security practices using various tools.

Objectives

-) Compare and contrast basic concepts of cryptography

Lab Topology



Lab Settings

The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account	Password
DVL	10.1.1.10 /28	root	toor
Kali	203.0.113.2 /29	root	toor
pfSense	eth0: 192.168.1.1 /24 eth1: 10.1.1.1 /28 eth2: 203.0.113.1 /29	admin	pfsense
SecOnion	eth0: 192.168.1.6 /24	soadmin	mypassword
		root	mypassword
Ubuntu	192.168.1.50 /24	student	securepassword
		root	securepassword
Win12R2	10.1.1.12 /28	administrator	Train1ng\$
Win16	192.168.1.100 /24	lab-user	Train1ng\$
		Administrator	Train1ng\$

1 Creating a TrueCrypt Container

1.1 Creating a Container

In this task, you will configure an encrypted volume container on the Kali Linux workstation.

1. Launch the **Kali** virtual machine to access the graphical login screen.
2. Log in as **root** with **toor** as the password. Open the **Kali PC Viewer**.
3. Click on the **terminal** icon located in the top menu bar.



4. In the *terminal* window, change to the **/tmp** directory.

```
root@Kali-Attacker:~# cd /tmp
```

```
root@Kali-Attacker:~# cd /tmp/  
root@Kali-Attacker:/tmp#
```

5. Create a text file named **billing.txt**.

```
[root@Kali-Attacker:/tmp]# touch billing.txt
```

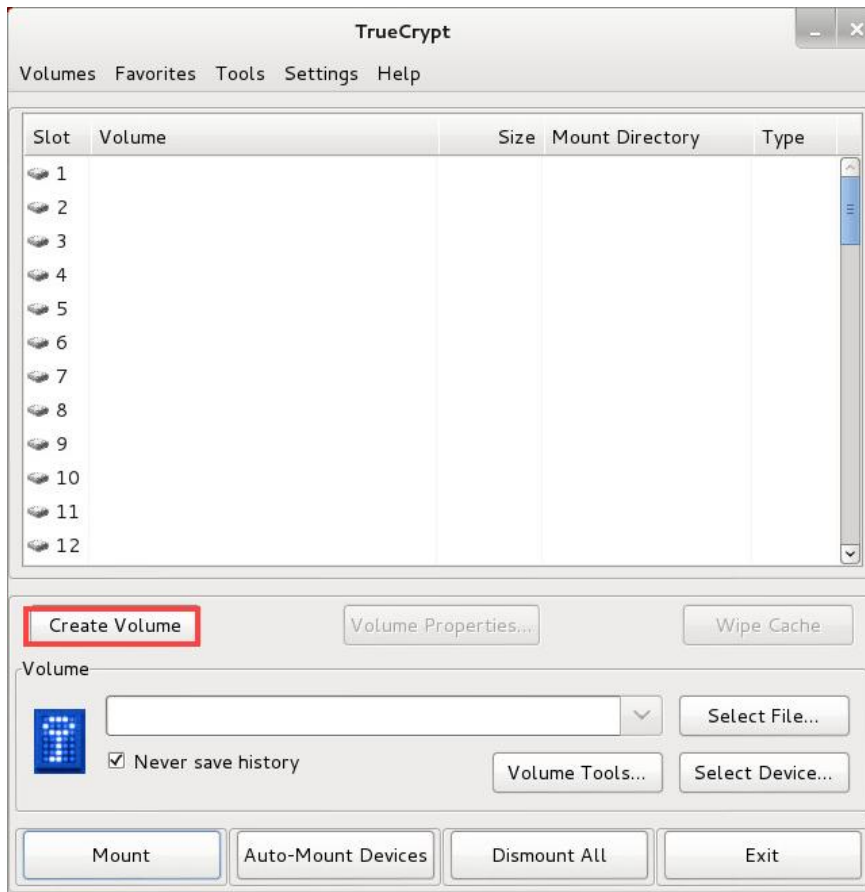
```
root@Kali-Attacker:/tmp# touch billing.txt  
root@Kali-Attacker:/tmp#
```

6. Launch the *TrueCrypt* application by typing **truecrypt** in the *terminal* window followed by pressing the **Enter** key.

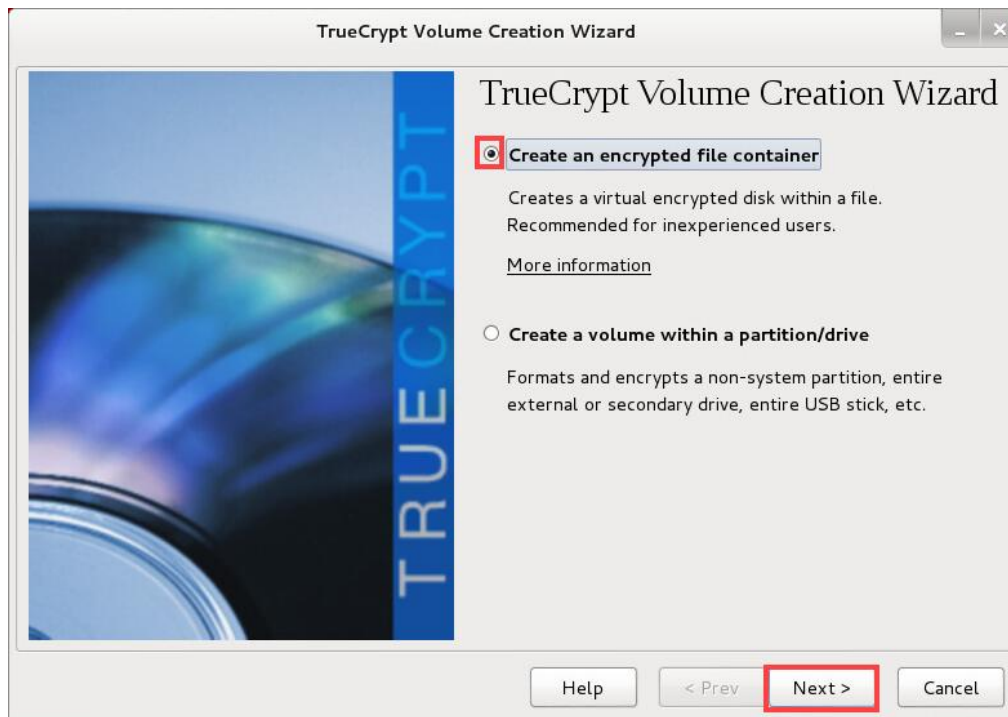
```
root@Kali-Attacker:/tmp# touch billing.txt
```

```
root@Kali-Attacker:/tmp# truecrypt  
█
```

7. In the *TrueCrypt* application window, click the **Create Volume** button.



8. Notice the *TrueCrypt Volume Creation Wizard* appears. Proceed with creating an encrypted file container by selecting the radio button for **Create an encrypted file container** and click **Next**.



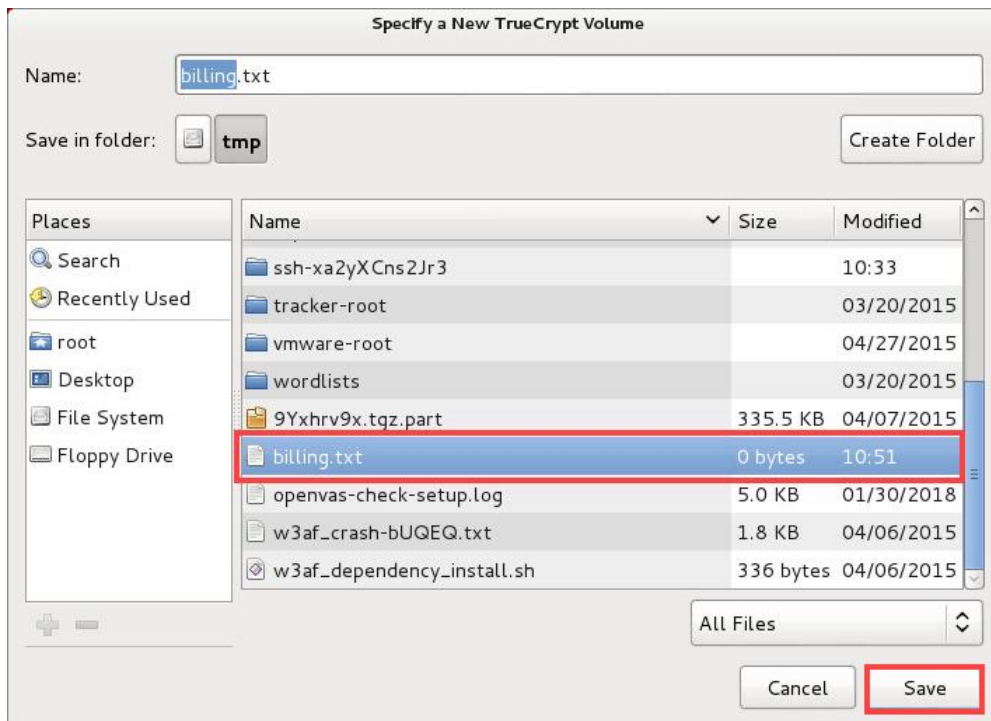
9. On the *Volume Type* step, select the radio button for **Standard TrueCrypt volume** and click **Next**.



10. On the *Volume Location* step, click on the **Select File** button.



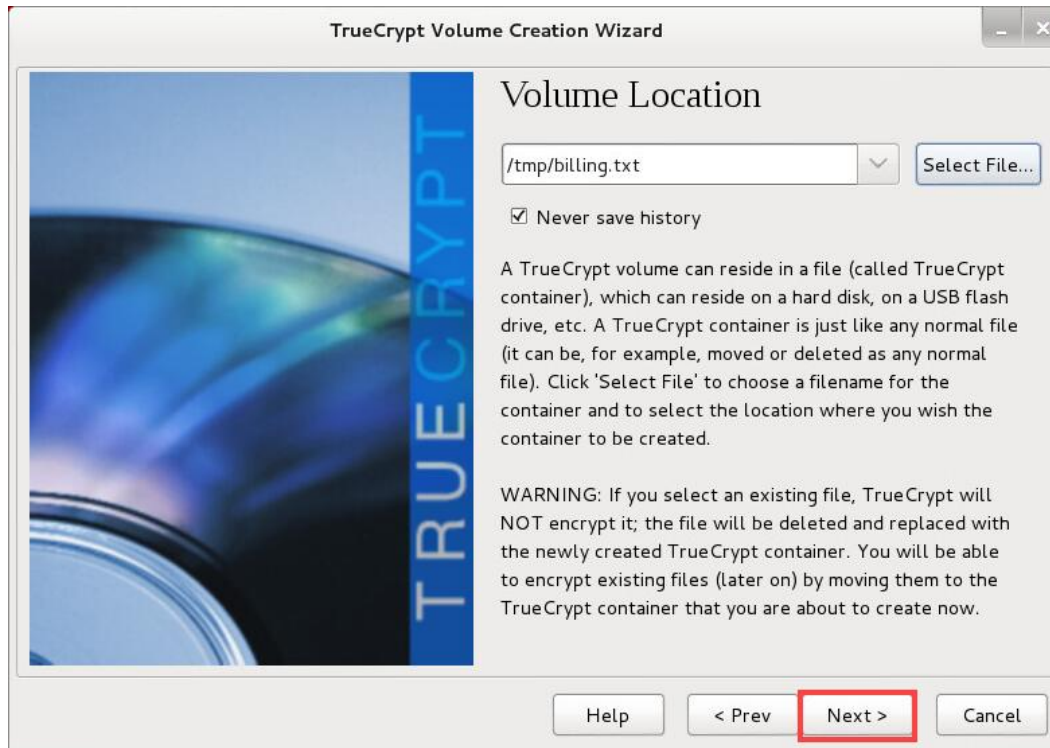
11. A new *File Manager* window appears. Navigate to **File System > tmp**. Select the **billing.txt** file and click **Save**.



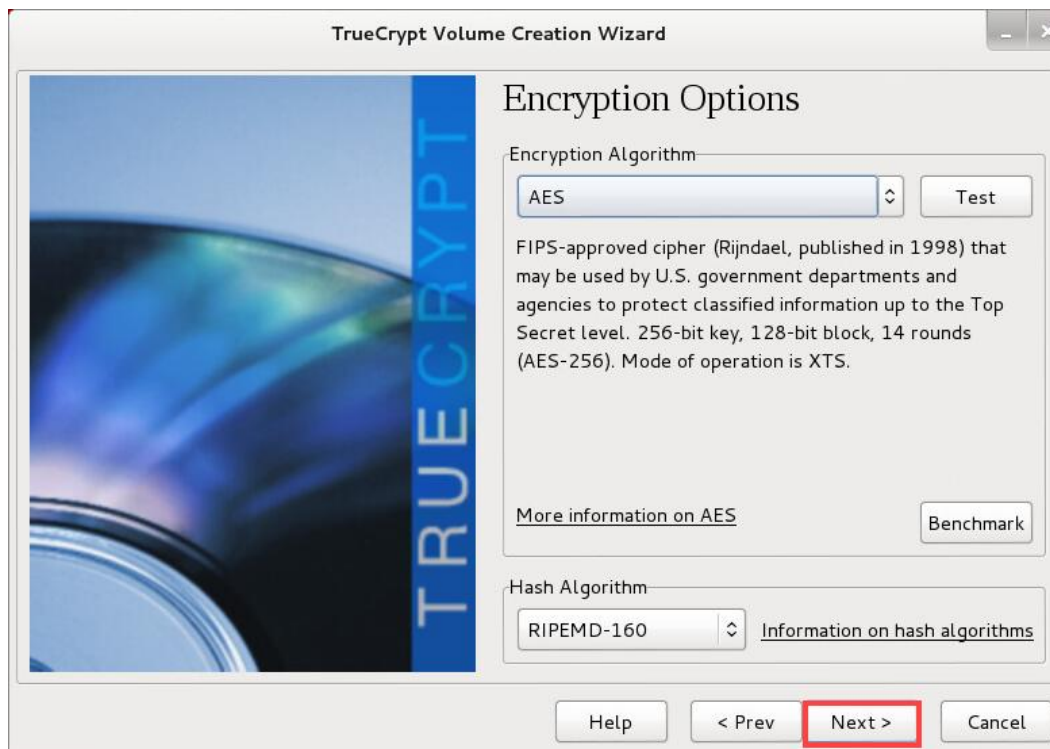
12. When asked to replace the file, click on **Replace**.



13. Back on the *TrueCrypt Volume Creation Wizard* window, verify that `/tmp/billing.txt` is prefilled in the location field and click **Next**.



14. On the *Encryption Options* step, leave the default set to **AES** and **RIPEMD-160**. Click **Next**.




15. On the *Volume Size* step, enter the value of 50. Verify **MB** is selected and click **Next**.



The screenshot shows the 'Volume Size' step of the TrueCrypt Volume Creation Wizard. On the left is a vertical banner with the word 'TRUECRYPT' and a blue abstract image. The main area is titled 'Volume Size'. It contains a text input field with '50' and a dropdown menu set to 'MB'. Below this, it says 'Free space available: 3.1 GB' and provides instructions: 'Please specify the size of the container to create. Note that the minimum possible size of a volume is 292 KB.' At the bottom are buttons for 'Help', '< Prev', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red box.

16. On the *Volume Password* step, type **password** and confirm the password of **password**. Click **Next**.

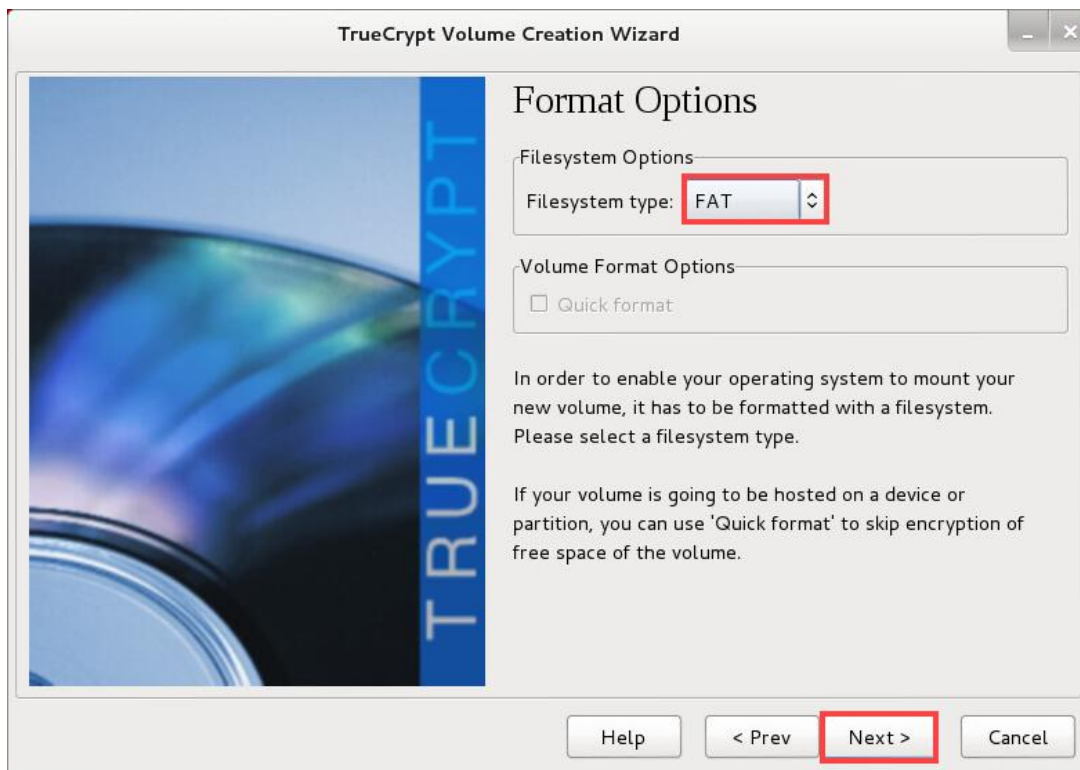


The screenshot shows the 'Volume Password' step of the TrueCrypt Volume Creation Wizard. On the left is the same 'TRUECRYPT' banner. The main area is titled 'Volume Password'. It has two text input fields: 'Password:' and 'Confirm password:', both containing the word 'password'. Below these are checkboxes for 'Display password' (checked) and 'Use keyfiles' (unchecked), with a 'Keyfiles...' button next to the second checkbox. A paragraph of text provides guidance on choosing a strong password. At the bottom are buttons for 'Help', '< Prev', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red box.

17. When prompted with a warning, click **Yes** to continue.



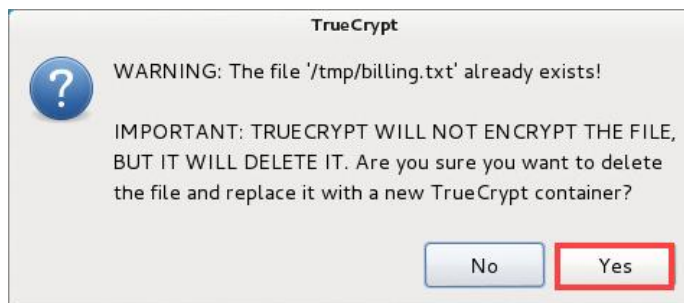
18. On the *Format Options* step, leave the default set to **FAT** and click **Next**.



19. On the *Volume Format* step, click **Format**.



20. When prompted with a warning message, click **Yes** to replace the *billing.txt* file with a *TrueCrypt container*.



21. Click **OK** in response to the successful operation message.



22. Click **Exit** on the *Volume Created* screen to exit the *TrueCrypt Volume Creation Wizard* window.



23. Leave the *TrueCrypt* application open to continue with the next task.

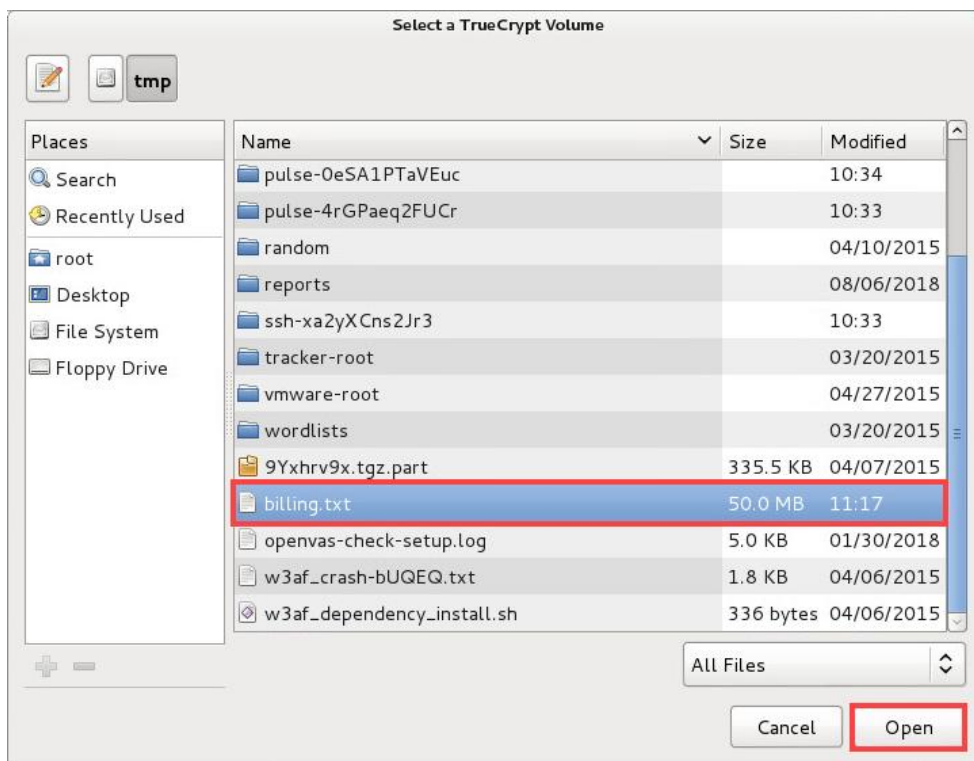
2 Opening and Viewing Data within a TrueCrypt Container

2.1 Using the TrueCrypt Container

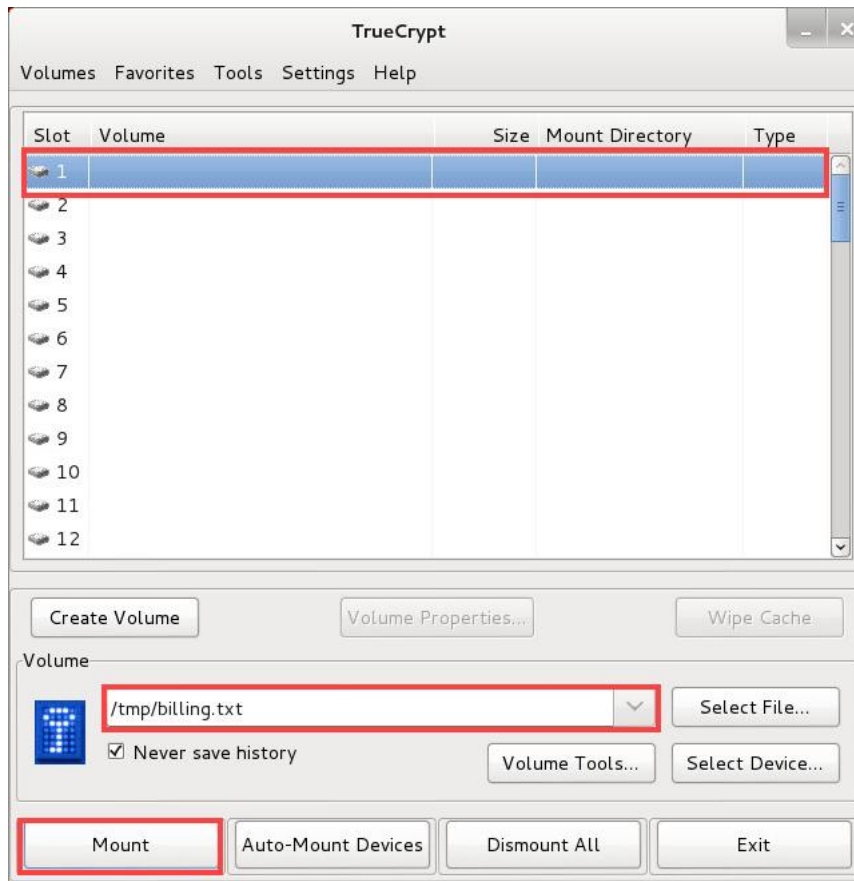
1. While on the *Kali* system with the *TrueCrypt* application opened, click on the Select File button to locate your *TrueCrypt* container.



2. A new *File Manager* window appears. Navigate to **File System > tmp** and select the **billing.txt** file. Click **Open**.



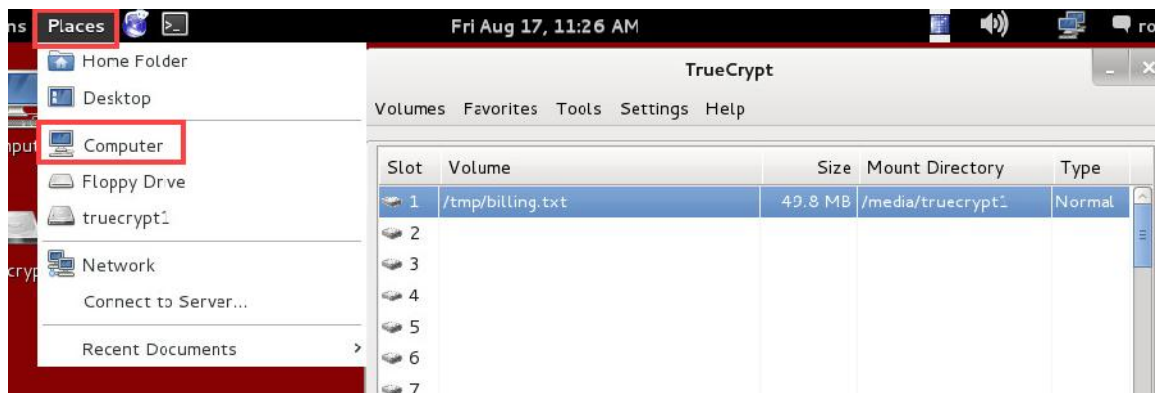
3. Select **one available drive slot** from the list and then click on the **Mount** button.



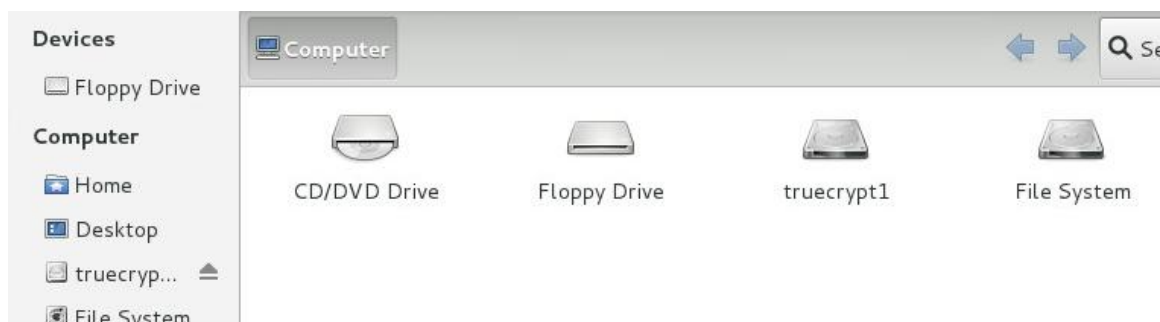
4. When prompted for a password, type **password** and click **OK**.



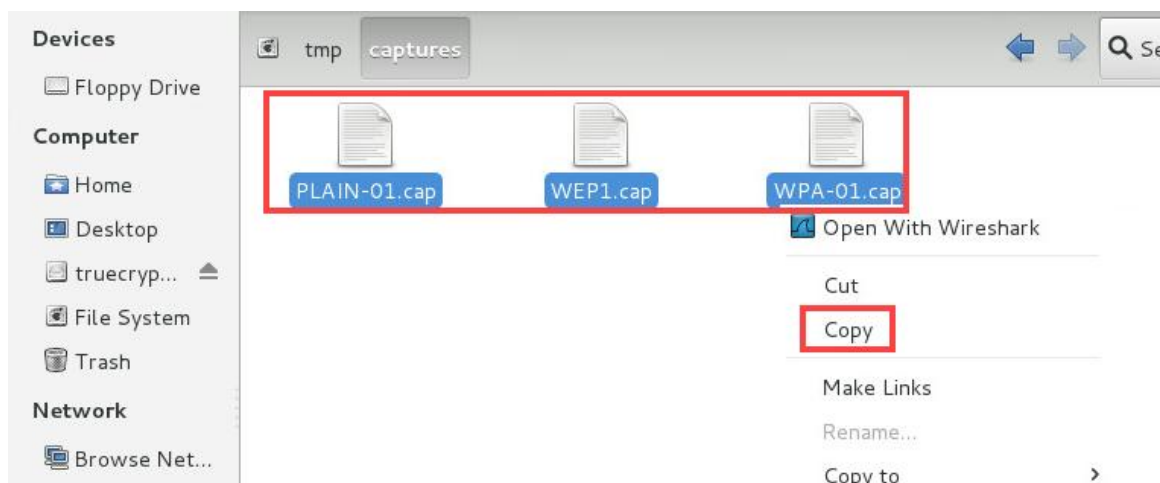
5. Notice that the drive is now successfully mounted when looking at the *TrueCrypt* window with the mount directory information presented as */media/truecrypt1*. Select the **Places** menu option located on the top menu pane and click on the **Computer** entry.



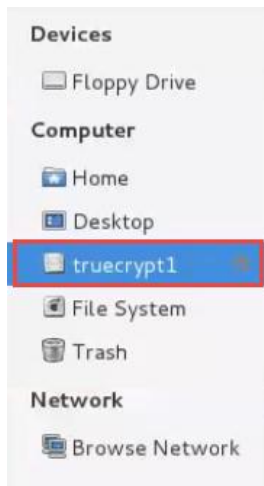
6. In the new *File Manager* window, notice a mount entry for *truecrypt1*. Notice that the drive is mounted to the system.



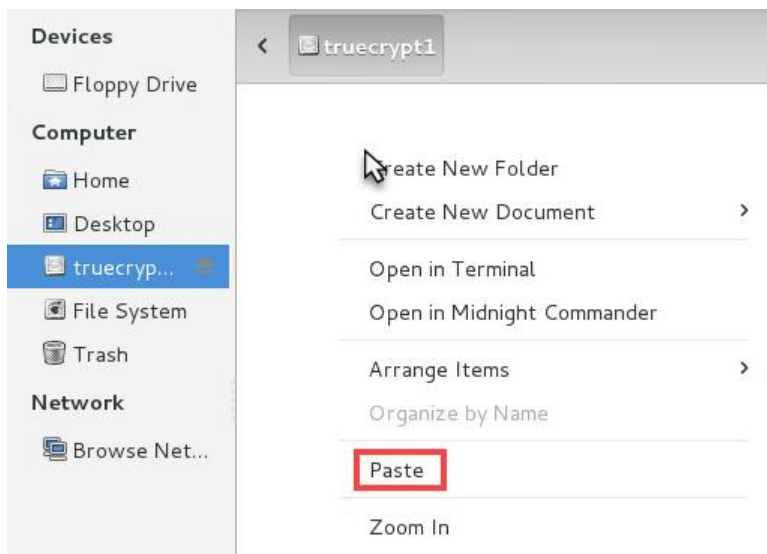
7. Within the *File Explorer* window, navigate to **File System > tmp > captures**. Notice the three files available. Press **CTRL+A** to select all files within this directory. Right-click on one of the files and select **Copy** to copy all three files.



8. Click on the **truecrypt1** volume located on the left menu pane.



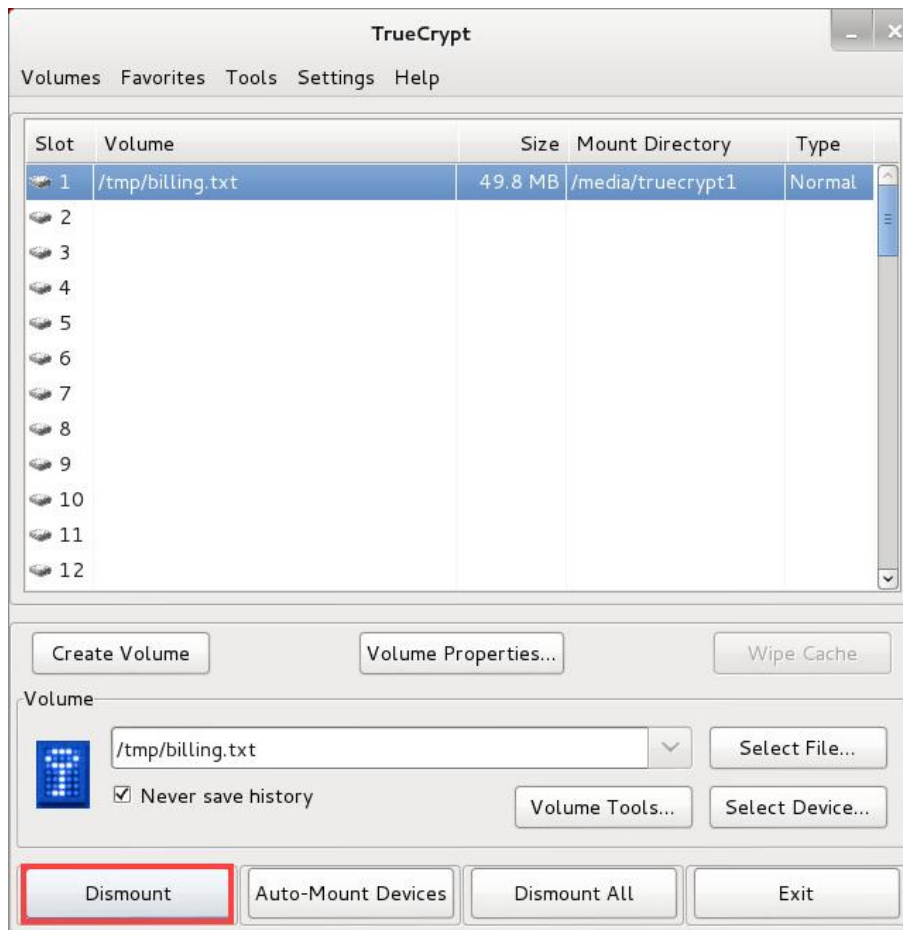
9. Right-click in the white space and select **Paste**.



The files should now all be in the *TrueCrypt* container.

10. Close the **File Manager** window.

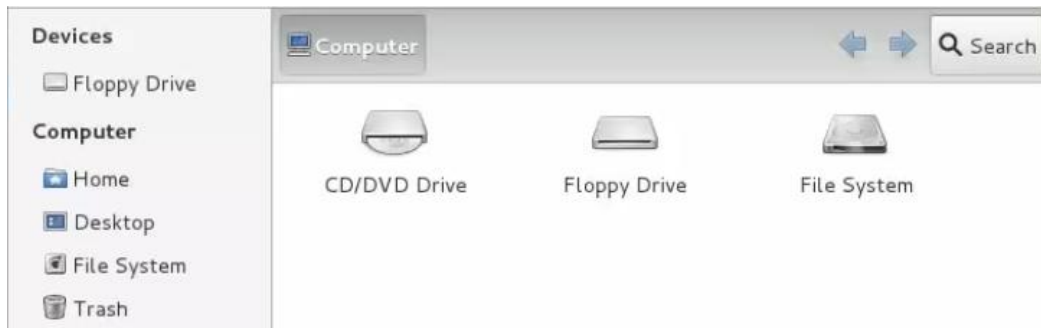
11. Change focus back to the *TrueCrypt* application window. Click on the **Dismount** button to unmount the *truecrypt1* volume.



12. Select the **Places** menu option located on the top menu pane and click on **Computer** to open a new *File Manager* window.



13. Once the *File Explorer* window appears, notice that the *truecrypt1* volume is now not visible (unmounted).



14. Leave the *Kali* window open to continue with the next task.

3 Bruteforcing a TrueCrypt Container

3.1 Using TrueCrack

1. While on the *Kali* system, open a new **terminal** window by clicking on the **Terminal** icon located on the top menu pane.



2. Before using the *TrueCrack* application, examine what options are available.

```
root@Kali-Attacker:~# truecrack -help
```

```
root@Kali-Attacker:~# truecrack -help
TrueCrack v3.0
Website: http://code.google.com/p/truecrack
Contact us: info@truecrack@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 is 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.
```

3. To use the *TrueCrack* application, we must know what the *TrueCrypt* volume file is. Since we already know the *TrueCrypt* volume file is *billing.txt*, type the command below to begin bruteforcing the volume file. Use the **passlist** file as a source of possible passwords to try.

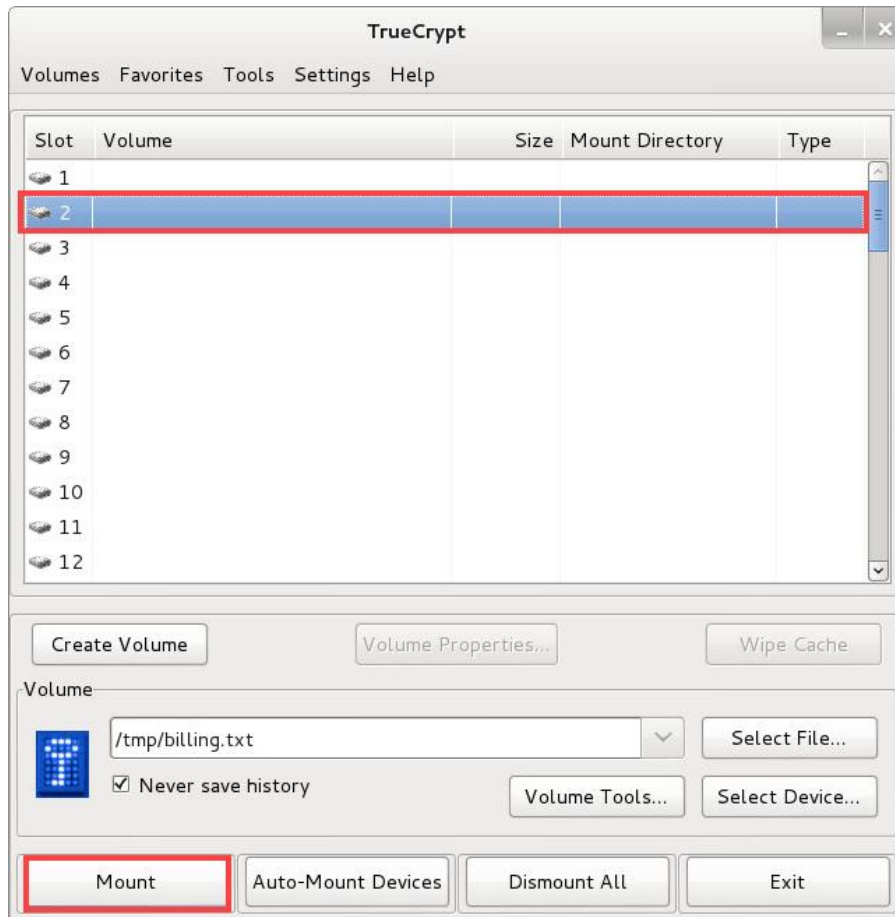
```
root@Kali-Attacker:~# truecrack -t /tmp/billing.txt -w '/tmp/wordlists/passlist'
```

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

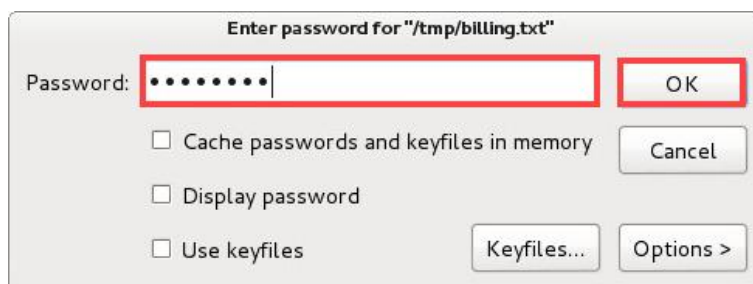


Notice after a few seconds, the *TrueCrack* application has found the password. This is accurate as we had created the encrypted container using a weak password of *password*.

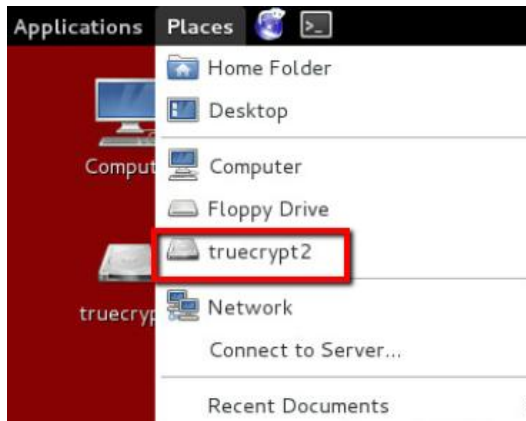
4. Change focus back to the **TrueCrypt** application. Select any available **drive slot** and click the **Mount** button.



5. When prompted for a password, use the same password found from the *TrueCrack* application. Type in **password** and click **OK**.



6. A successful mount has been established. Verify by selecting **Places** from the menu pane.



Notice the *truecrypt2* mounted volume entry.

7. The lab is now complete; you may end the reservation.