SECURITY+ V4 LAB SERIES

Lab 16: Securing Data with Encryption Software

Document Version: 2022-04-29

Material in this Lab Aligns to the Following	
CompTIA Security+ (SY0-601) Exam Objectives	2.1: Explain the importance of security concepts in an enterprise environment 3.2: Given a scenario, implement host or application security solutions
All-In-One CompTIA Security+ Sixth Edition ISBN-13: 978-1260464009 Chapters	9: Enterprise Security Architecture 18: Host and Application Security

Contents

Introduction

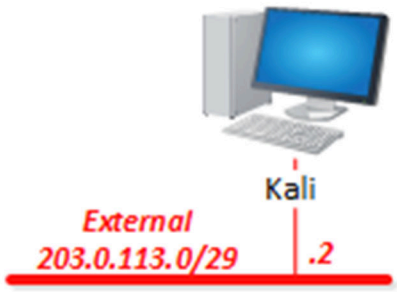
In this lab, you will be conducting data security practices using various tools.

Objective

In this lab, you will perform the following tasks:

- Practice the use of VeraCrypt for securing files.

Lab Topology



Lab Settings

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

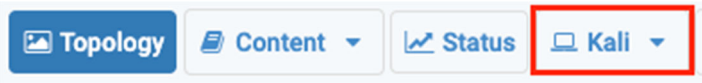
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Kali	203.0.113.2	kali	kali

1 Creating a VeraCrypt Container

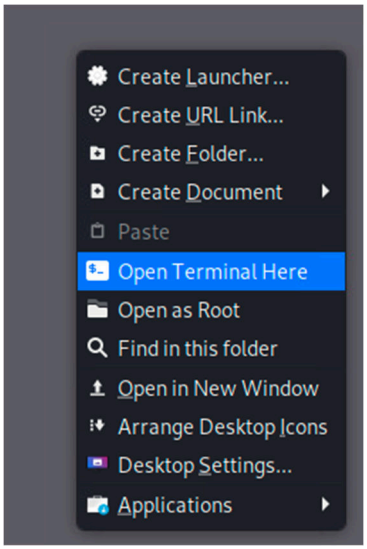
1.1 Creating a Container

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.

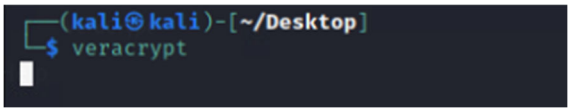


2. Log in as `kali` with `kali` as the password. Open the *Kali PC Viewer*.
3. Right-click on an empty space on the desktop, then select **Open Terminal Here**.

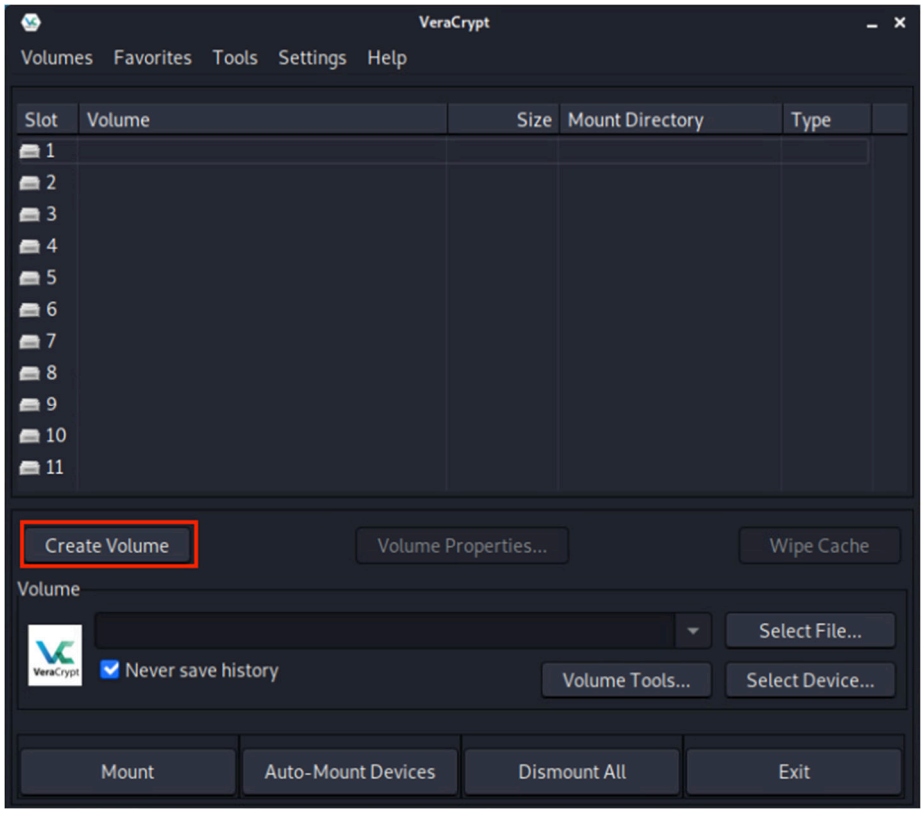


4. In the *Terminal* window, type `touch billing.txt` to create a text file.

5. Launch the *VeraCrypt* application by typing `veracrypt` in the *Terminal* window, followed by pressing the **Enter** key.

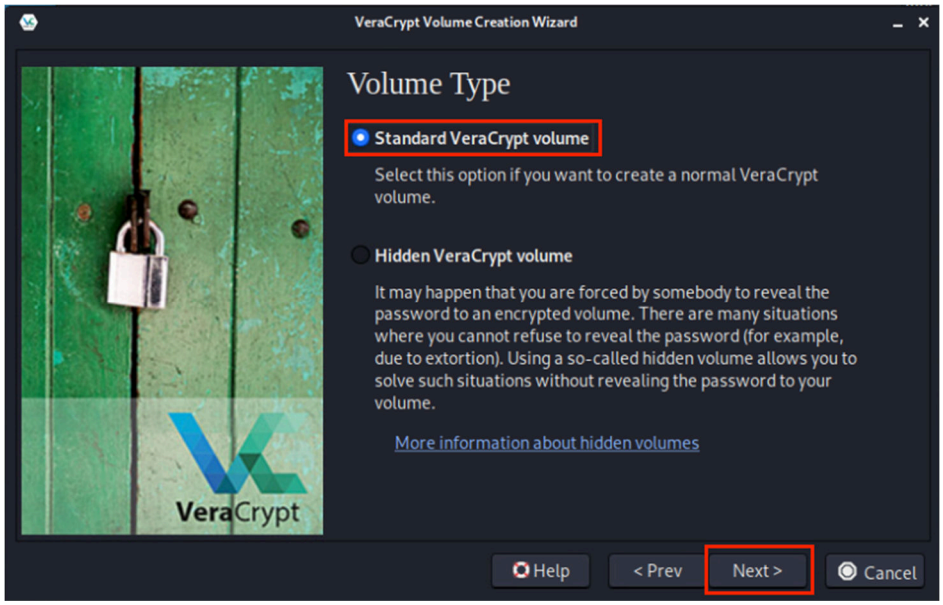


6. In the *VeraCrypt* application window, click the **Create Volume** button.



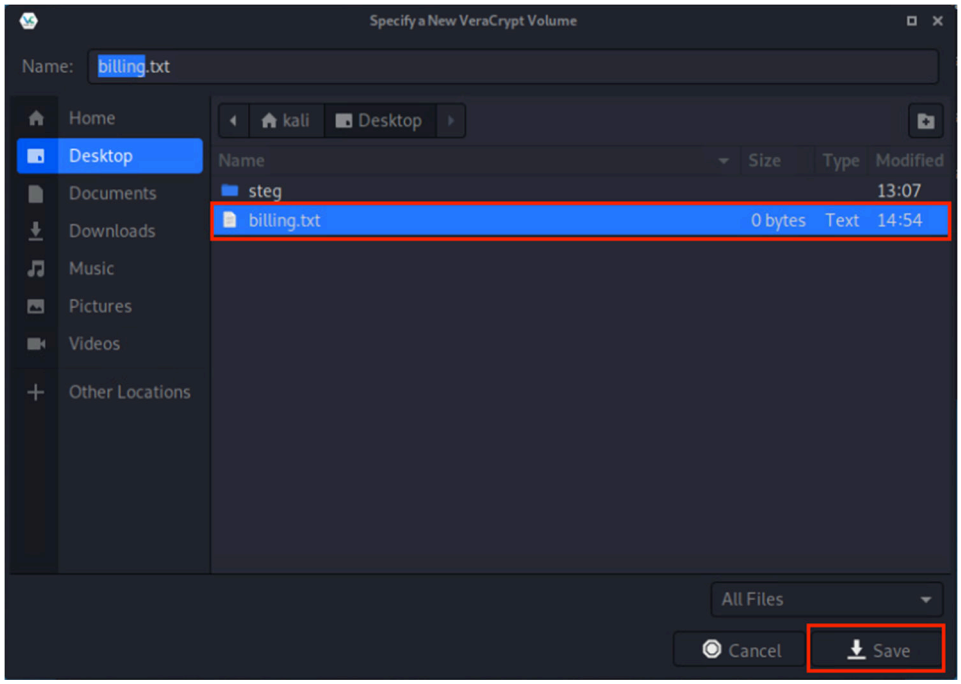
7. Notice the *VeraCrypt Volume Creation Wizard* appears. Proceed with creating an encrypted file container by selecting the radio button for **Create an encrypted file container** and clicking **Next.**

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

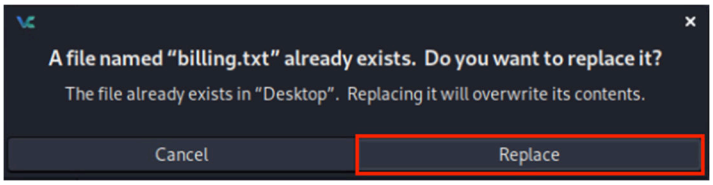


9. On the *Volume Location* step, click on the **Select File** button.

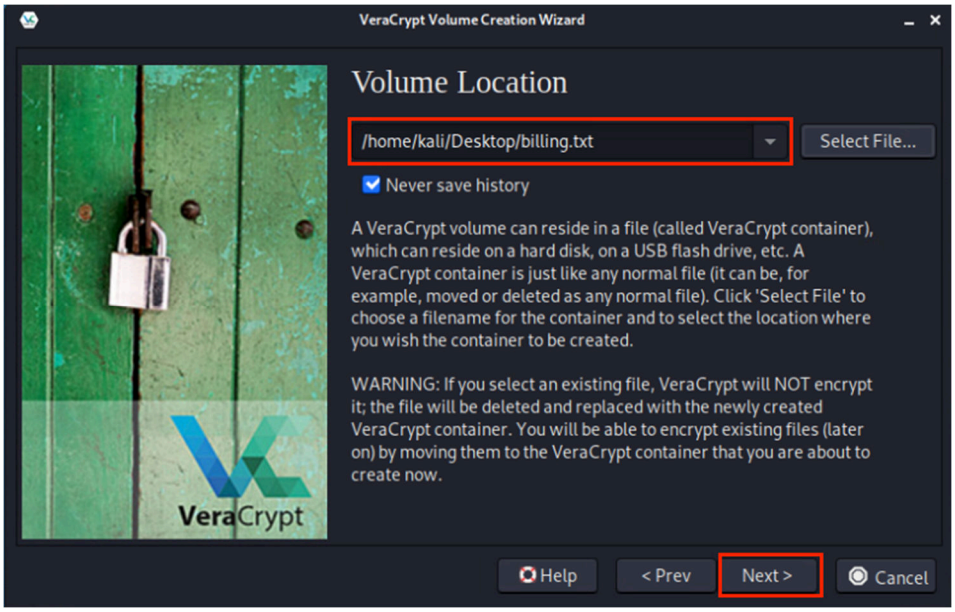
10. A new *File Manager* window appears. Navigate to **Desktop**. Select the **billing.txt** file and click **Save**.



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

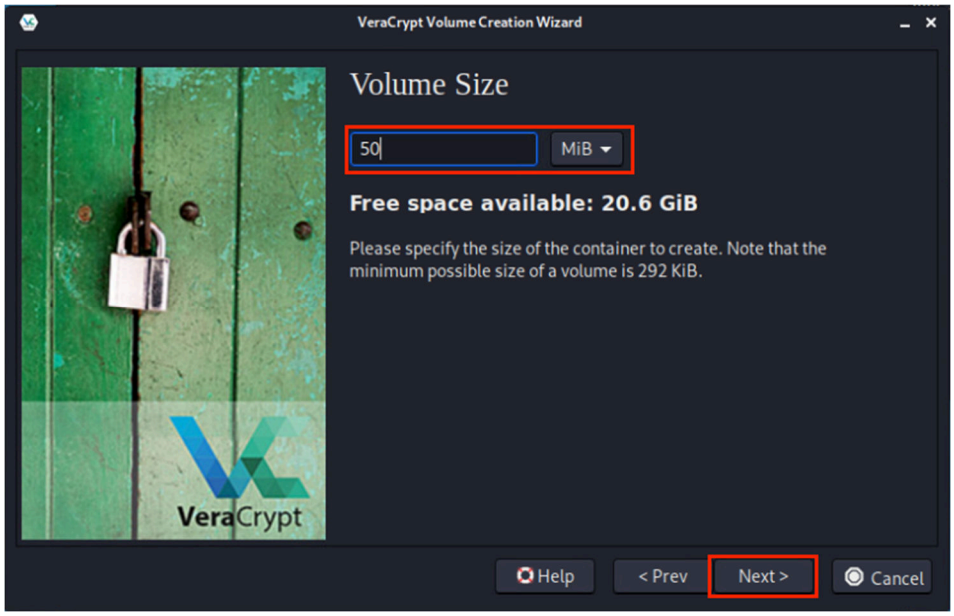


12. Back on the *VeraCrypt Volume Creation Wizard* window, verify that */home/kali/Deskop/billing.txt* is prefilled in the *Location* field and click **Next**.

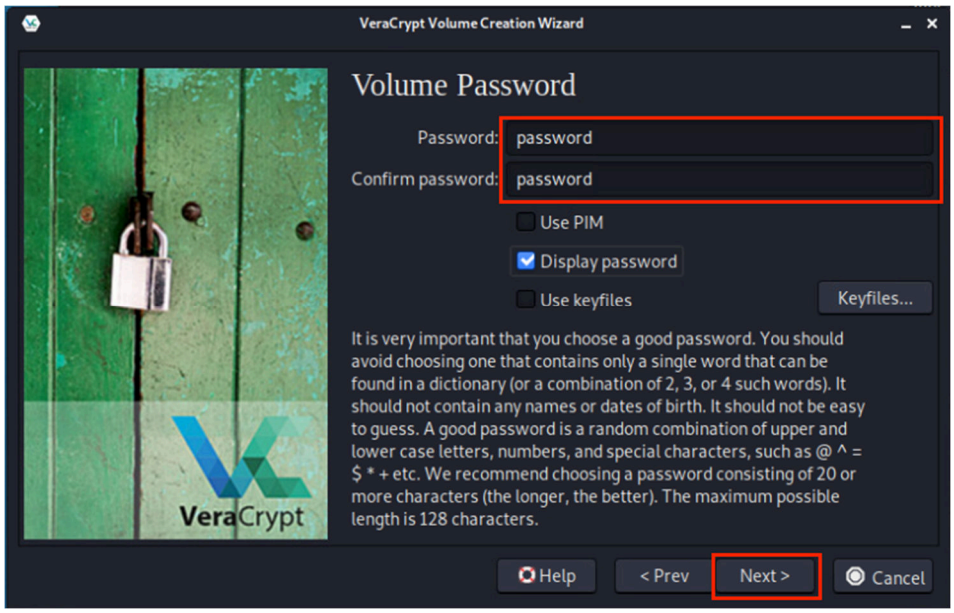


13. On the *Encryption Options* step, leave the default set to **AES** and **SHA-512**. Click **Next**.

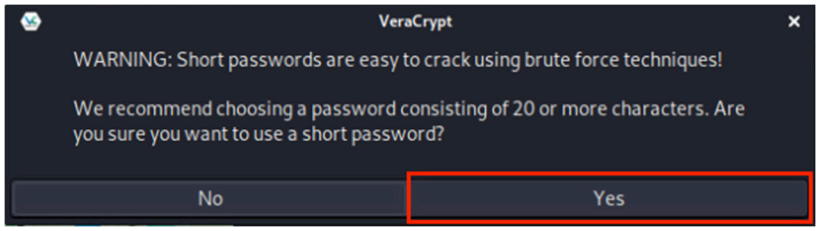
14. On the *Volume Size* step, enter the value of `50`. Verify **MB** is selected and click **Next.**



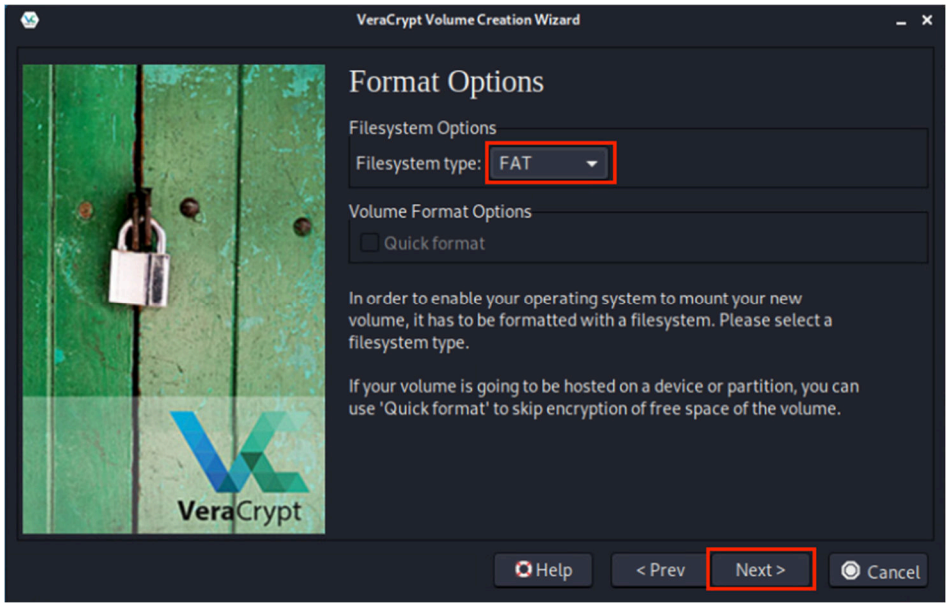
15. On the *Volume Password* step, type `password` and confirm the password of `password`. Click **Next**.



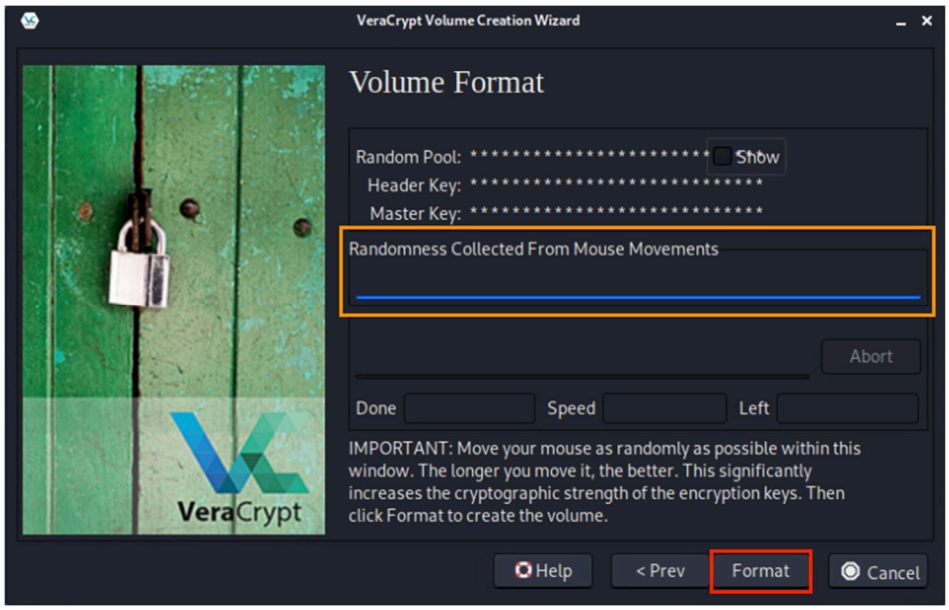
16. When prompted with a warning, click **Yes** to continue.



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

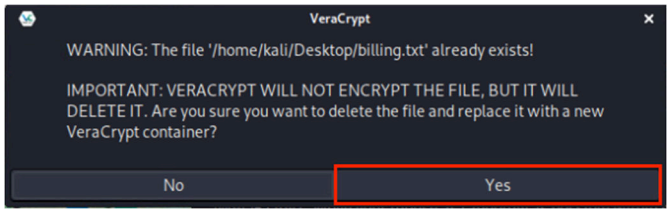


18. On the *Volume Format* step, the VeraCrypt software will collect the mouse movement as a factor for generating the encryption key, so keep moving your mouse at this screen until you are satisfied with the *Randomness* level (shown in blue). Then, click **Format.**

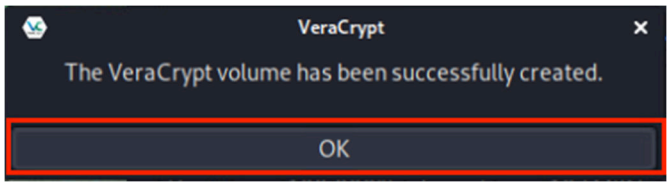


The higher the randomness, the securer the encryption.

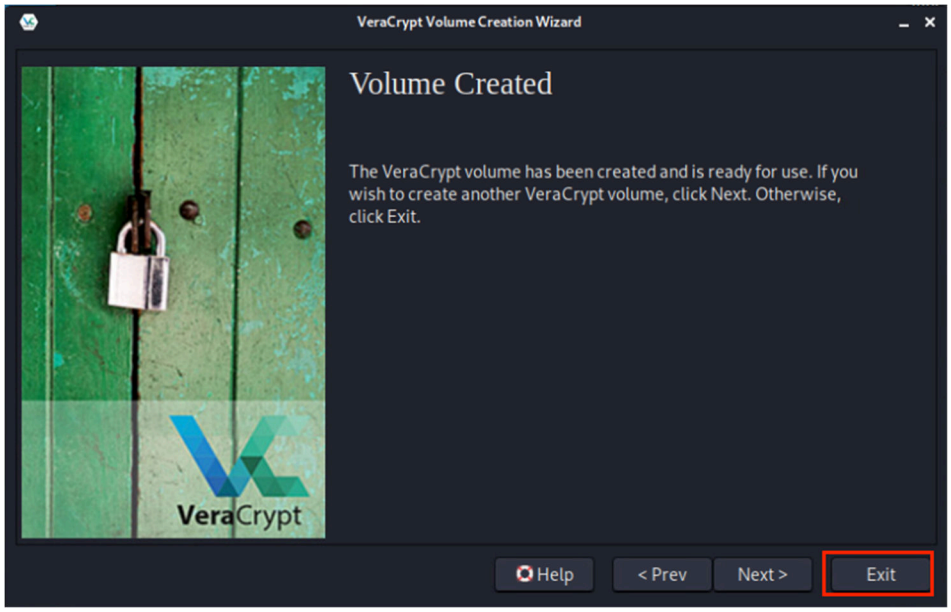
19. When prompted with a warning message, click **Yes** to replace the *billing.txt* file with a *Veracrypt container.*



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



21. Click **Exit** on the *Volume Created* screen to exit the *VeraCrypt Volume Creation Wizard* window.

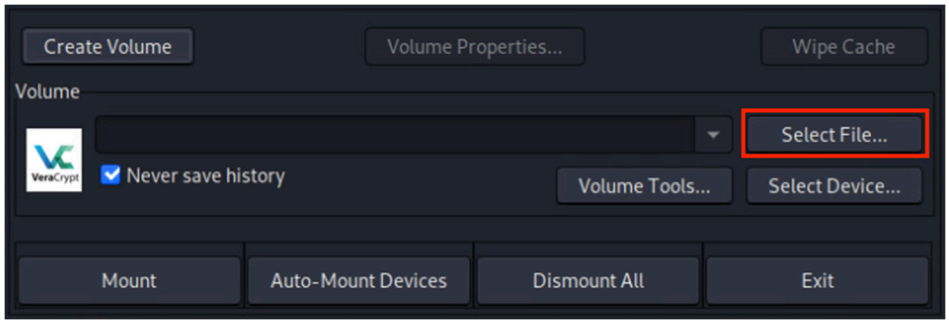


22. Leave the *VeraCrypt* application open to continue with the next task

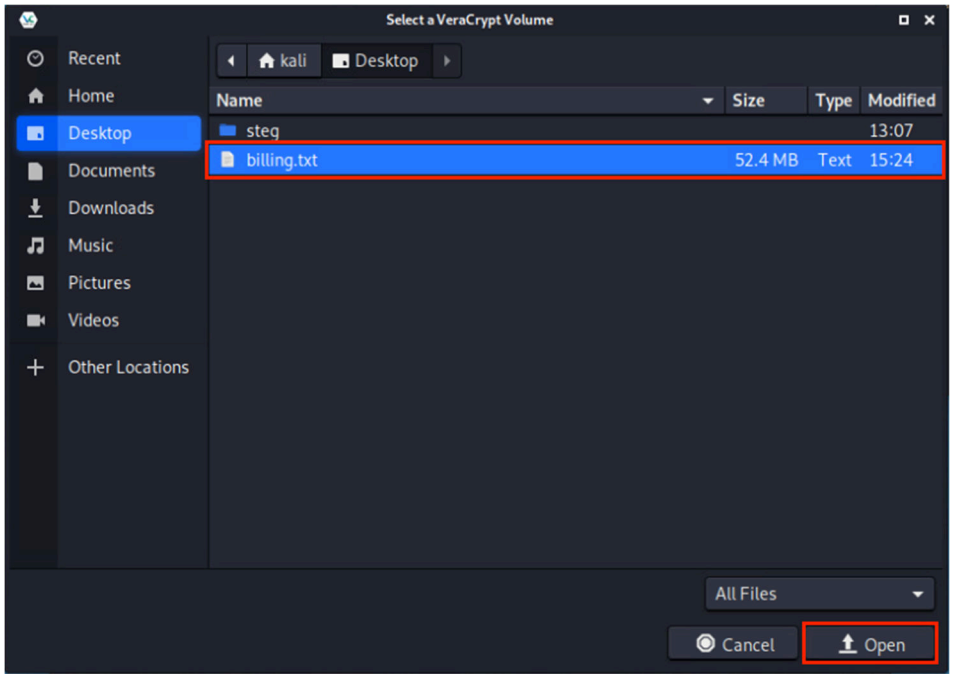
2 Opening and Viewing Data within a VeraCrypt Container

2.1 Using the VeraCrypt Container

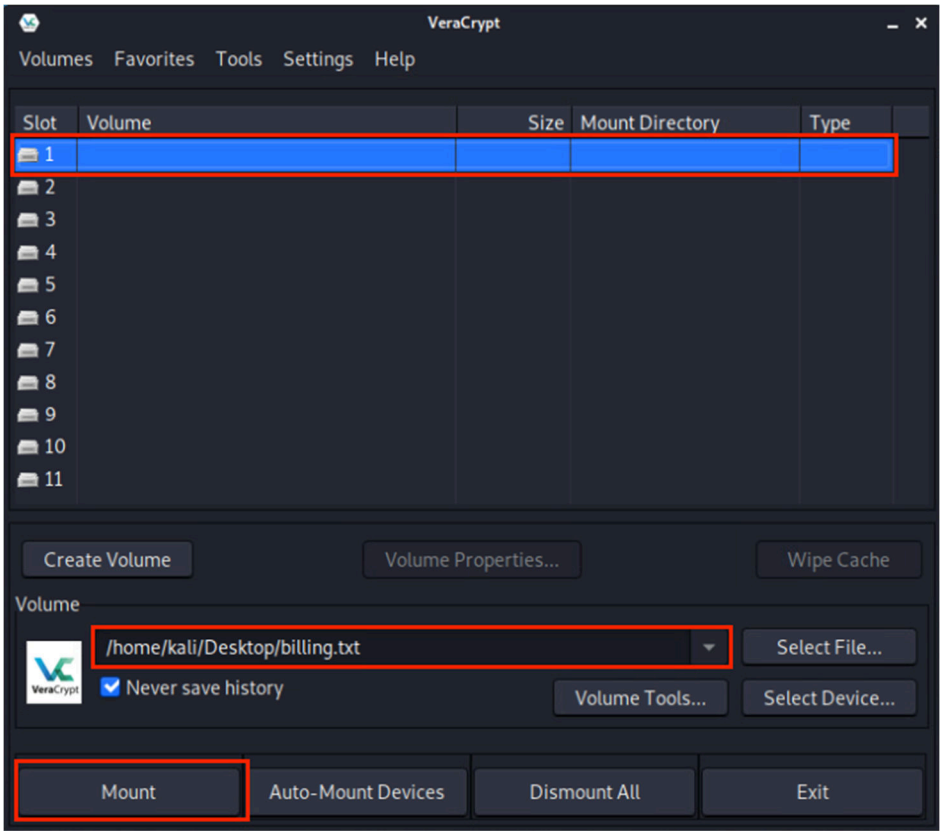
1. While on the *Kali* system with the *VeraCrypt* application opened, click on the **Select File** button to locate your *VeraCrypt* container.



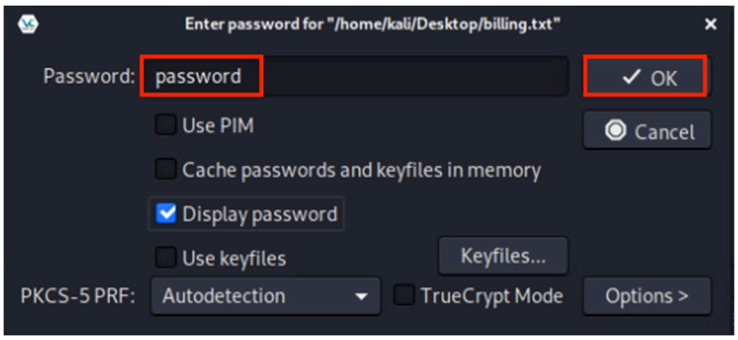
2. A new *File Manager* window appears. Navigate to **Desktop** and select the **billing.txt** file. Click **Open**.



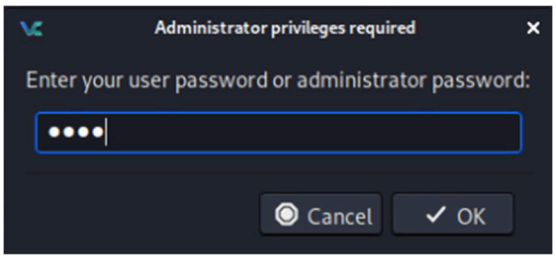
3. Select **one available drive slot** from the list and then click on the **Mount** button.



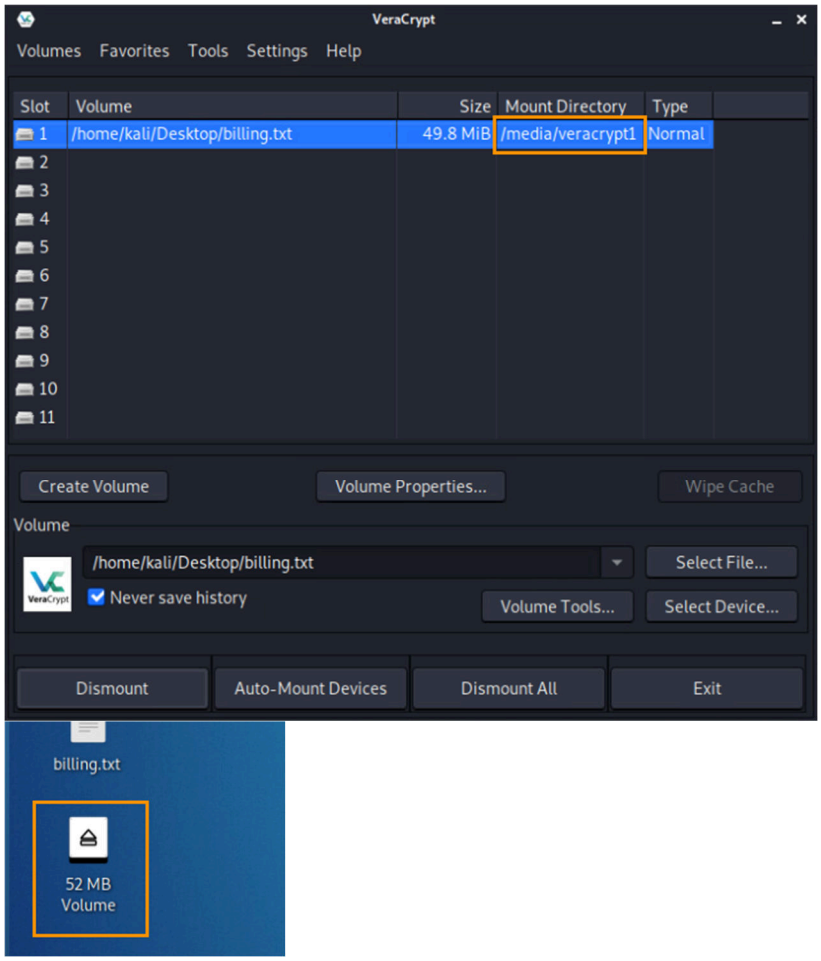
4. When prompted for a password, type **`password`** and click **OK.**



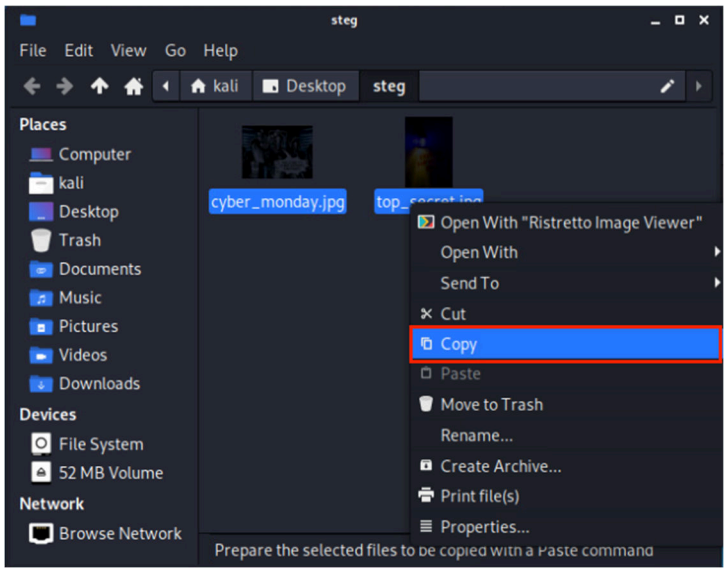
5. When prompted for *Administrative privilege* enter **`kali`**. Then click **OK**.



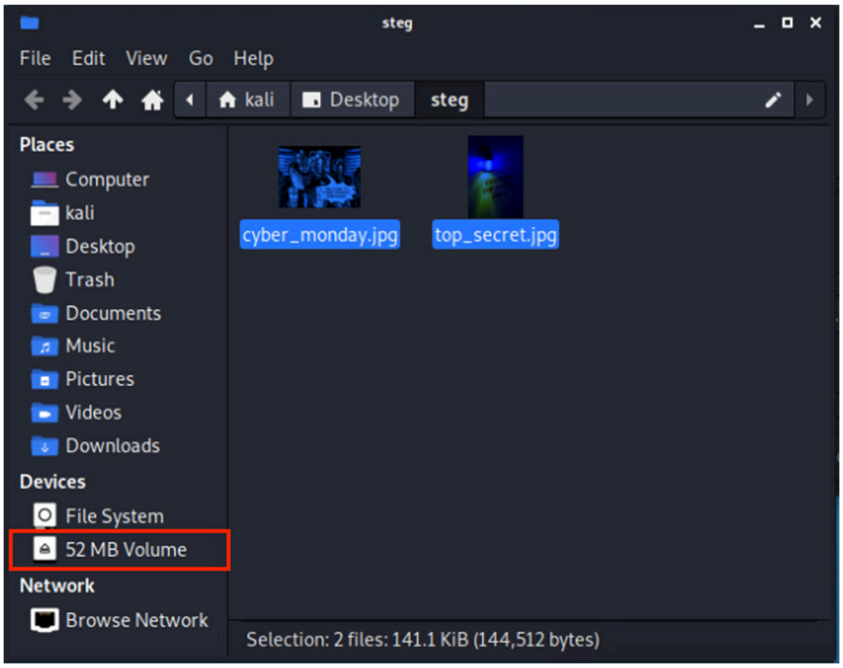
6. Notice that the drive is now successfully mounted when looking at the *VeraCrypt* window with the mount directory information presented as */media/varecypt1*. There should be a drive appearing on the desktop.



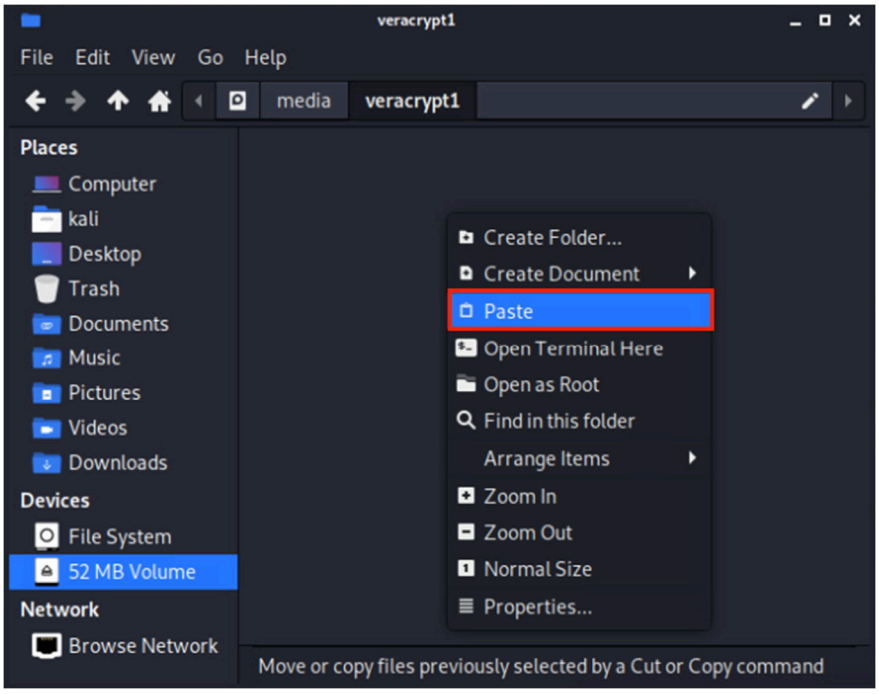
7. Notice the **steg** folder on the desktop; double-click to open it. You should see two pictures. Press **Ctrl** + **A** to select them, then right-click on the file and select **Copy** (or simply **Ctrl** + **C**).



8. Click on the veracrypt1 **52MB Volume** located on the left menu pane.



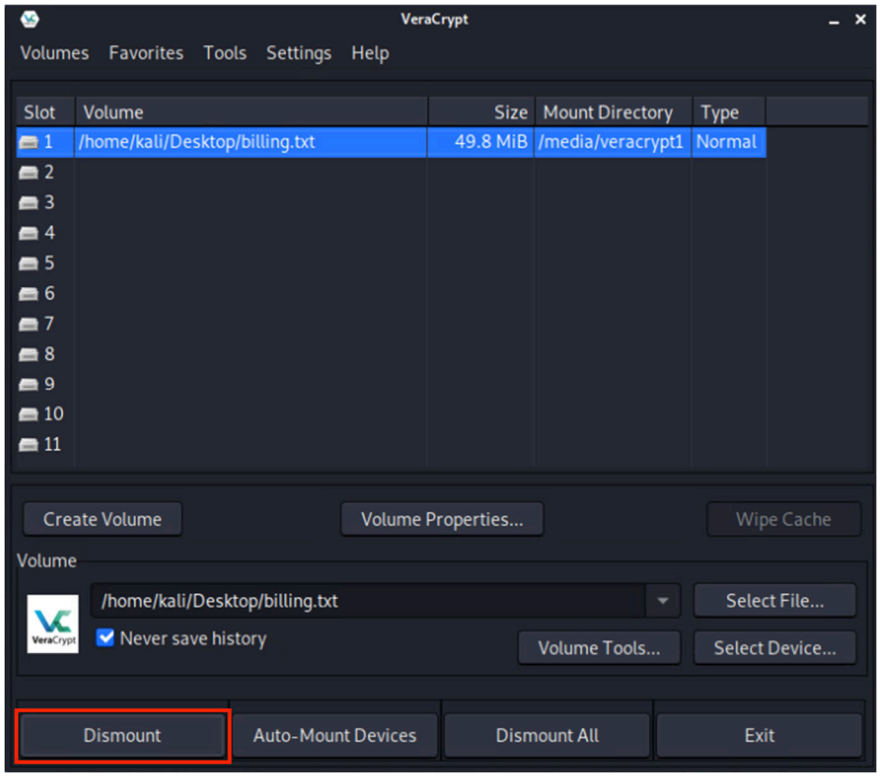
9. Right-click in the white space and select **Paste.** (or **Ctrl** + **V** to paste)



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

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

11. Change focus back to the *VeraCrypt* application window. Click on the **Dismount** button to unmount the *veracrypt1* volume



12. The mounted drive should disappear from the desktop.
13. The lab is now complete; you may end your reservation.