Lab 3: Perform Disk Encryption

Lab Scenario

Disk encryption is a technology that protects the confidentiality of the data stored on a disk by converting it into an unreadable code using disk encryption software or hardware, thus preventing unauthorized users from accessing it. Disk encryption provides confidentiality and privacy using passphrases and hidden volumes. As a professional ethical hacker or pen tester, you should perform disk encryption in order to prevent sensitive information from unauthorized access.

Disk encryption works in a manner similar to text-message encryption and protects data even when the OS is not active. By using an encryption program for the user's disk (Blue Ray, DVD, USB flash drive, External HDD, and Backup), the user can safeguard any or all information burned onto the disk and thus prevent it from falling into the wrong hands. Disk-encryption software scrambles the information burned on the disk into an illegible code. It is only after decryption of the disk information that one can read and use it.

This lab will demonstrate the use of various disk encryption tools to perform this technique.

Lab Objectives

- Perform disk encryption using VeraCrypt

Overview of Disk Encryption

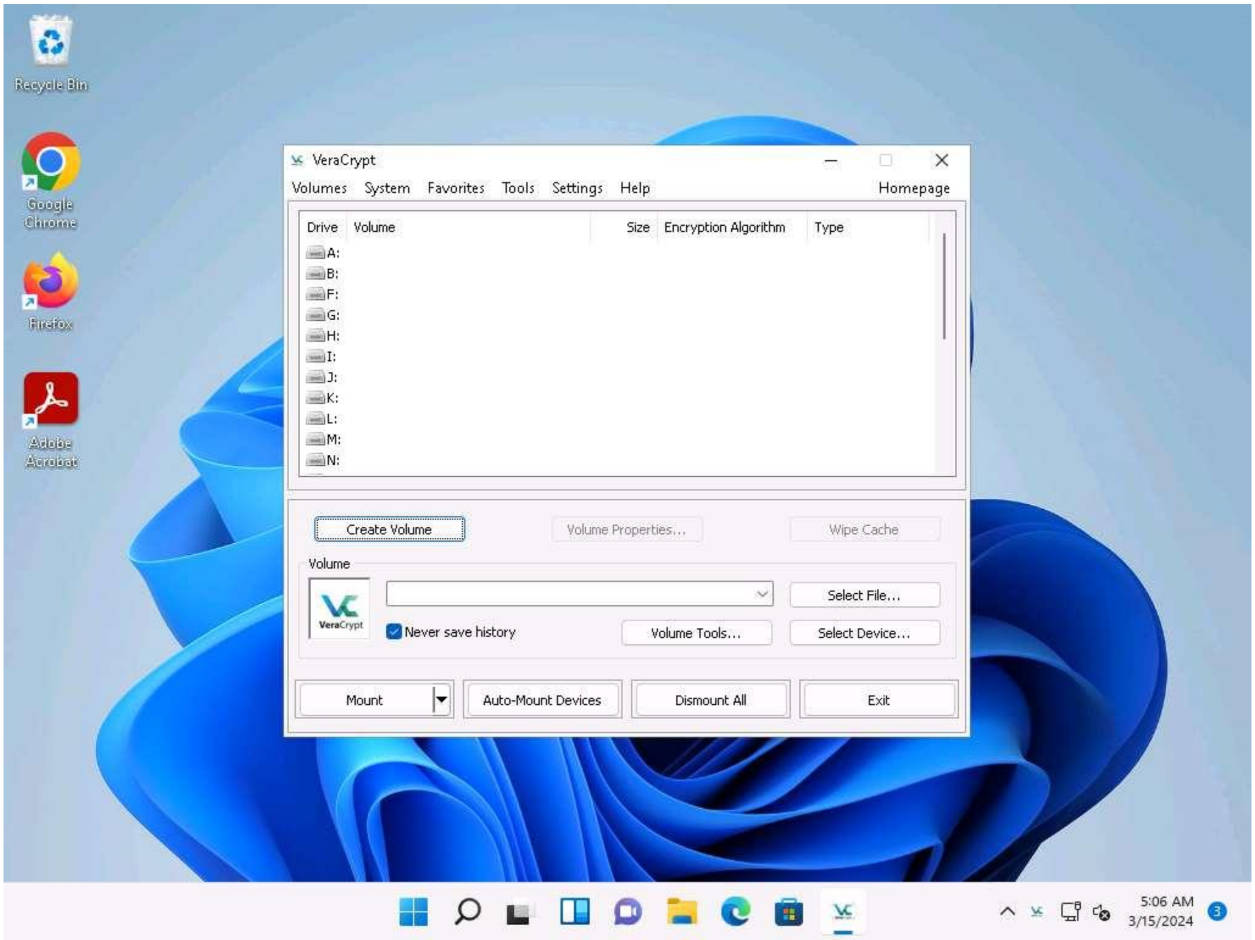
Disk encryption is useful when the user needs to send sensitive information through email. In addition, disk encryption can prevent the real-time exchange of information from threats. When users exchange encrypted information, it minimizes the chances of compromising the data; the only way an attacker could access the information is by decrypting the message. Furthermore, encryption software installed on a user's system ensures the security of the system. Install encryption software on any systems that hold valuable information or on those exposed to unlimited data transfer.

Task 1: Perform Disk Encryption using VeraCrypt

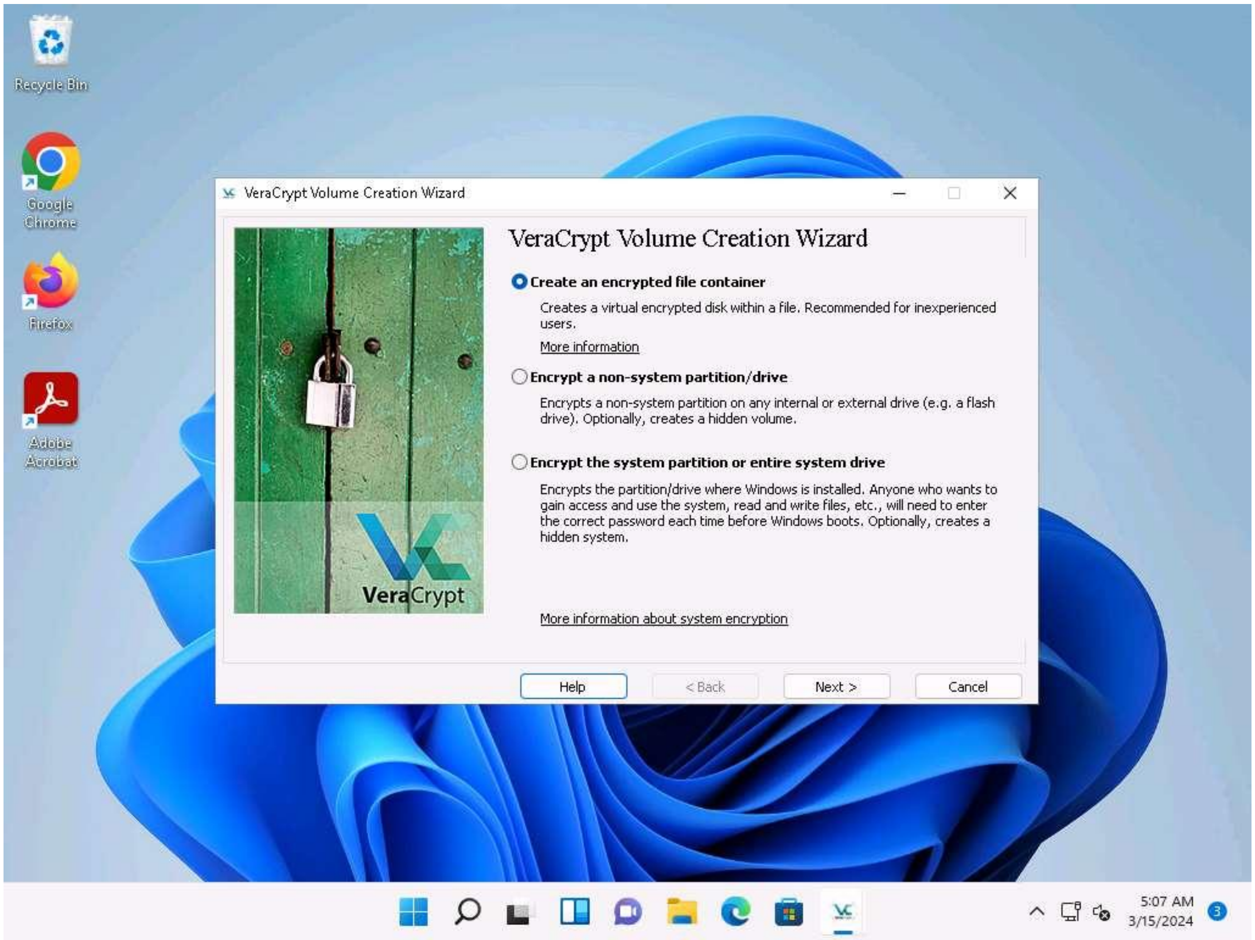
VeraCrypt is a software used for establishing and maintaining an on-the-fly-encrypted volume (data storage device). On-the-fly encryption means that data is automatically encrypted just before it is saved, and decrypted just after it is loaded, without any user intervention. No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys. The entire file system is encrypted (e.g., file names, folder names, free space, metadata, etc.).

Here, we will use the VeraCrypt tool to perform disk encryption.

1. Click Windows 11 to switch to the **Windows 11** machine.
2. Click **Search** icon (🔍) on the **Desktop**, search for **vera** in the search field, the **VeraCrypt** appears in the results, click **Open** to launch it.
3. The **VeraCrypt** main window appears; click the **Create Volume** button.



4. The **VeraCrypt Volume Creation Wizard** window appears. Ensure that the **Create an encrypted file container** radio-button is selected and click **Next** to proceed.



VeraCrypt Volume Creation Wizard

● Create an encrypted file container

Creates a virtual encrypted disk within a file. Recommended for inexperienced users.

More information

○ Encrypt a non-system partition/drive

Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume.

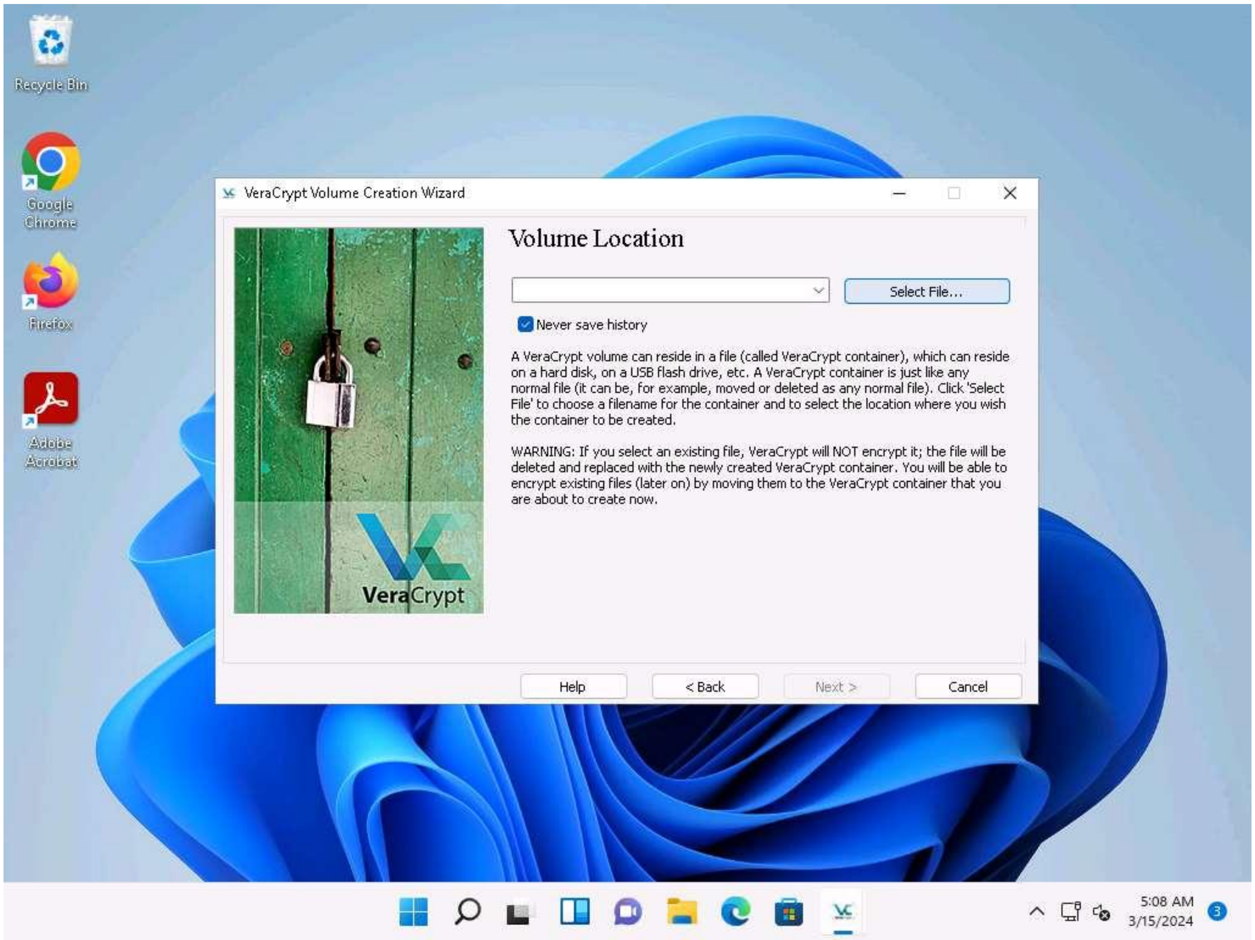
○ Encrypt the system partition or entire system drive

Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files, etc., will need to enter the correct password each time before Windows boots. Optionally, creates a hidden system.

More information about system encryption

5. In the **Volume Type** wizard, keep the default settings and click **Next**.

6. In the **Volume Location** wizard, click **Select File…**.



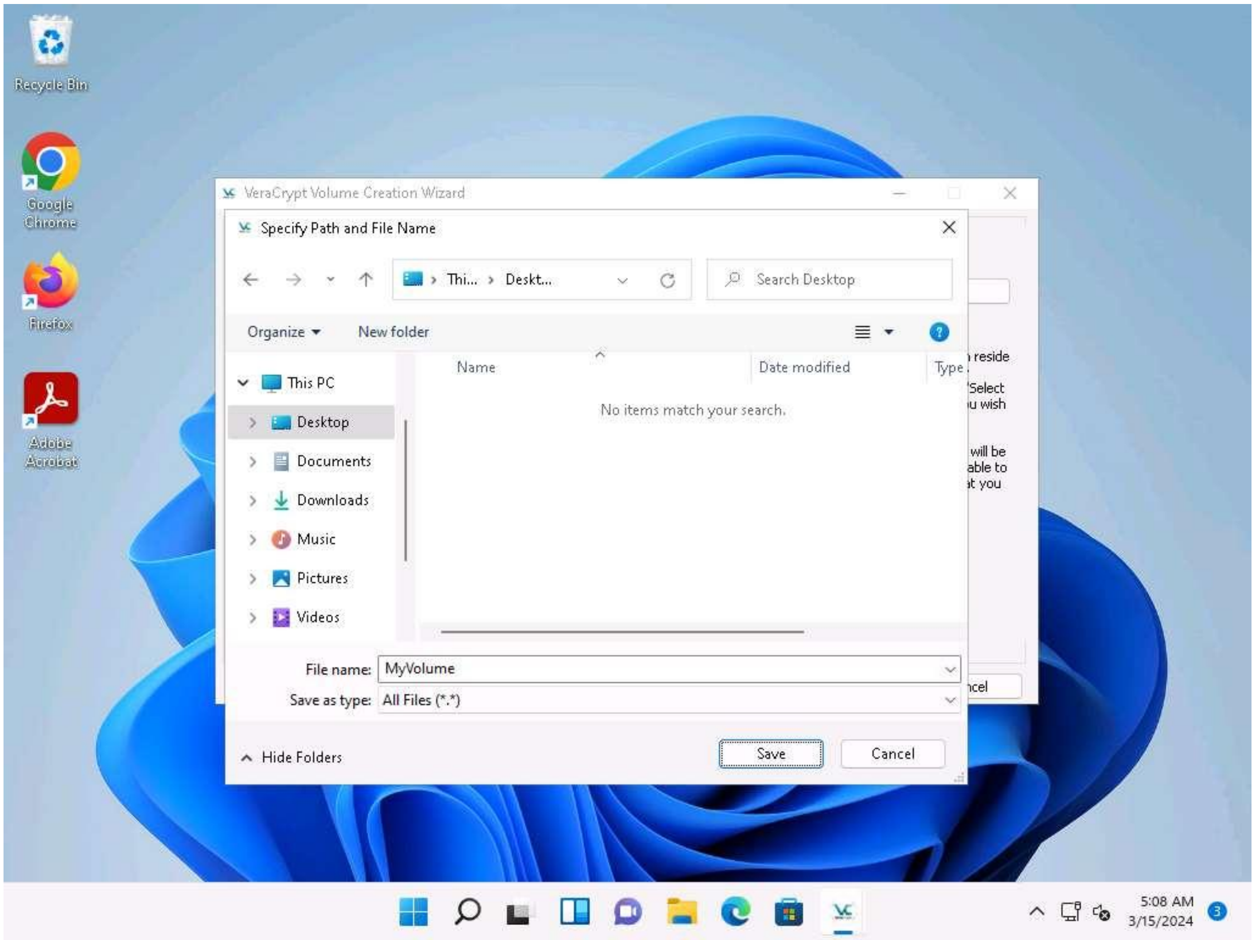
Volume Location

☑ Never save history

A VeraCrypt volume can reside in a file (called VeraCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A VeraCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.

WARNING: If you select an existing file, VeraCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created VeraCrypt container. You will be able to encrypt existing files (later on) by moving them to the VeraCrypt container that you are about to create now.

7. The **Specify Path and File Name** window appears; navigate to the desired location (here, **Desktop**), provide the **File name** as **MyVolume**, and click **Save**.

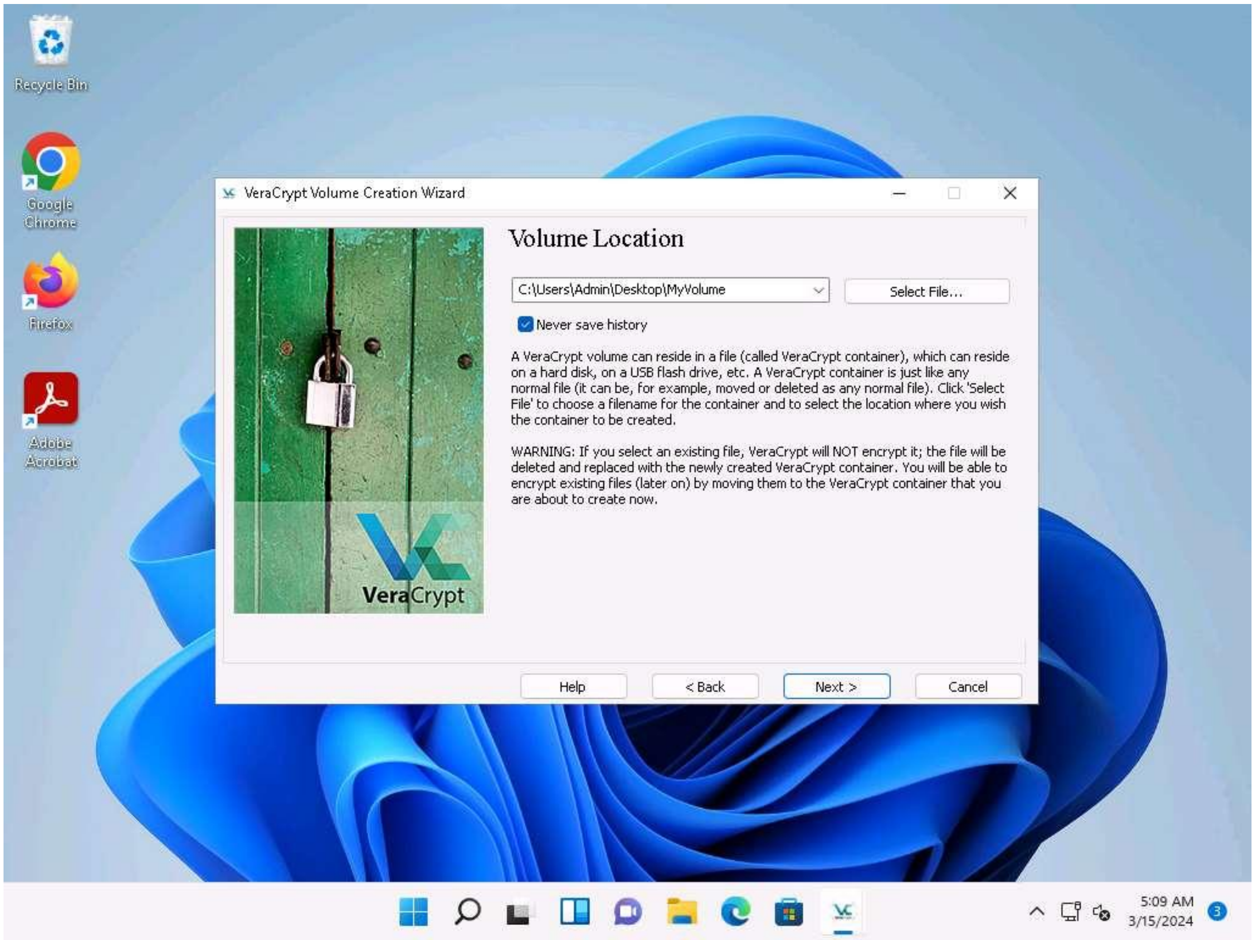


No items match your search.

File name: MyVolume

Save as type: All Files (*.*)

8. After saving the file, the location of a file containing the **VeraCrypt** volume appears under the **Volume Location** field; then, click **Next**.



Volume Location

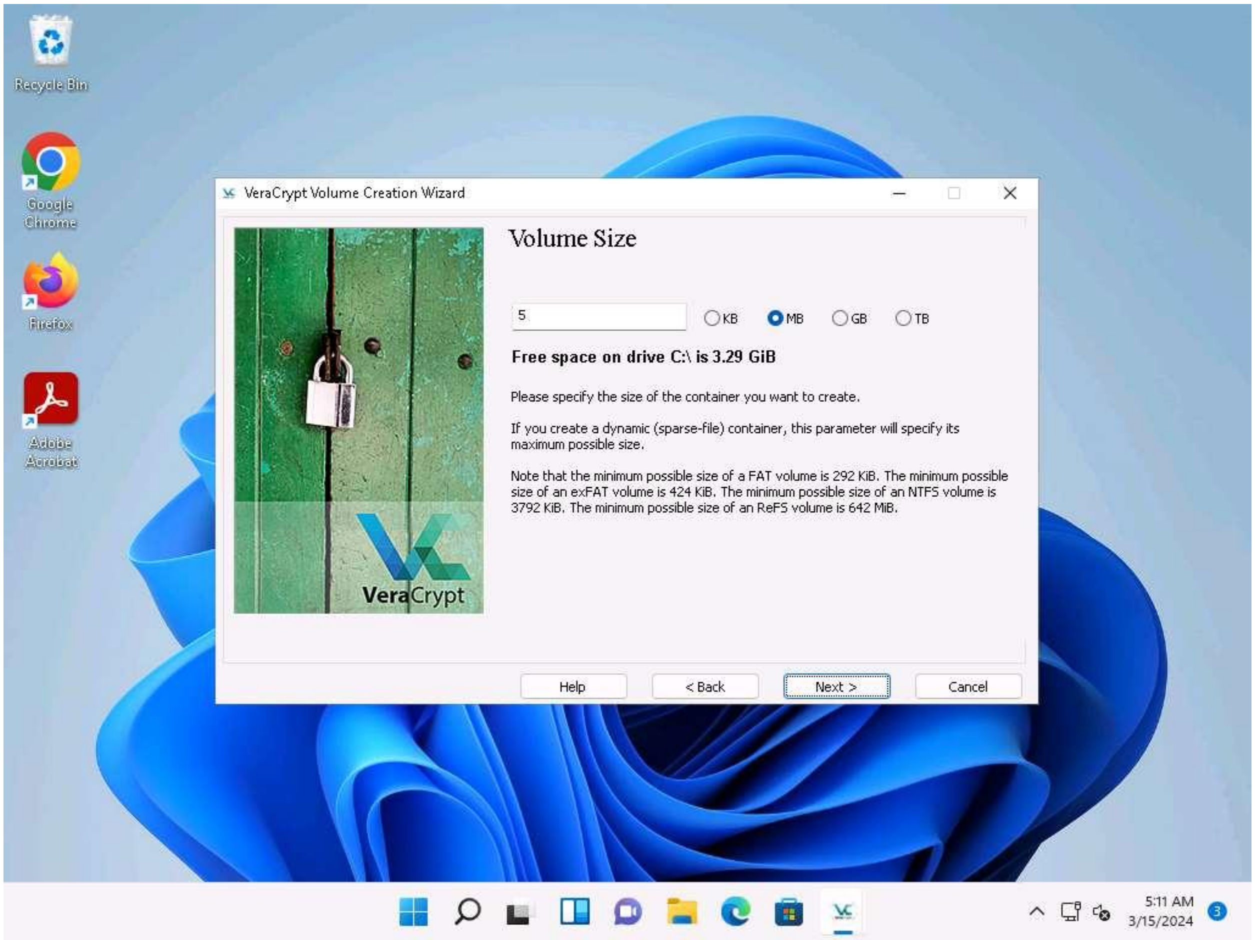
C:\Users\Admin\Desktop\MyVolume

☑ Never save history

A VeraCrypt volume can reside in a file (called VeraCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A VeraCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.

WARNING: If you select an existing file, VeraCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created VeraCrypt container. You will be able to encrypt existing files (later on) by moving them to the VeraCrypt container that you are about to create now.

9. In the **Encryption Options** wizard, keep the default settings and click **Next**.
10. In the **Volume Size** wizard, ensure that the **MB** radio-button is selected and specify the size of the VeraCrypt container as **5**; then, click **Next**.



VeraCrypt Volume Creation Wizard

Volume Size

5 ○KB ●MB ○GB ○TB

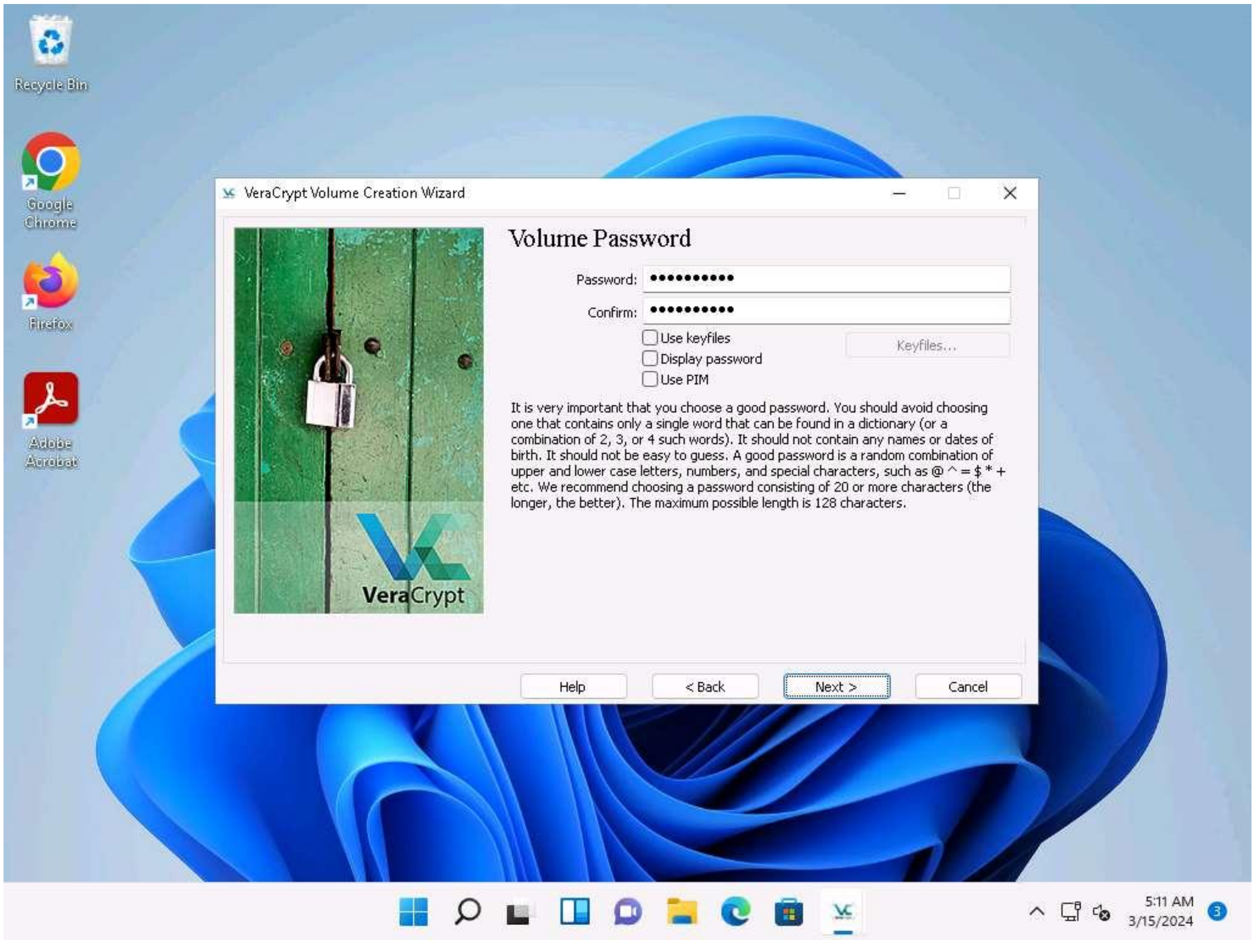
Free space on drive C:\ is 3.29 GiB

Please specify the size of the container you want to create.

If you create a dynamic (sparse-file) container, this parameter will specify its maximum possible size.

Note that the minimum possible size of a FAT volume is 292 KiB. The minimum possible size of an exFAT volume is 424 KiB. The minimum possible size of an NTFS volume is 3792 KiB. The minimum possible size of an ReFS volume is 642 MiB.

11. The **Volume Password** wizard appears; provide a strong password in the **Password** field, retype in the **Confirm** field, and click **Next**. The password provided in this lab is **qwerty@123**.



VeraCrypt Volume Creation Wizard

Volume Password

Password: ••••••••••

Confirm: ••••••••••

□ Use keyfiles

□ Display password

□ Use PIM

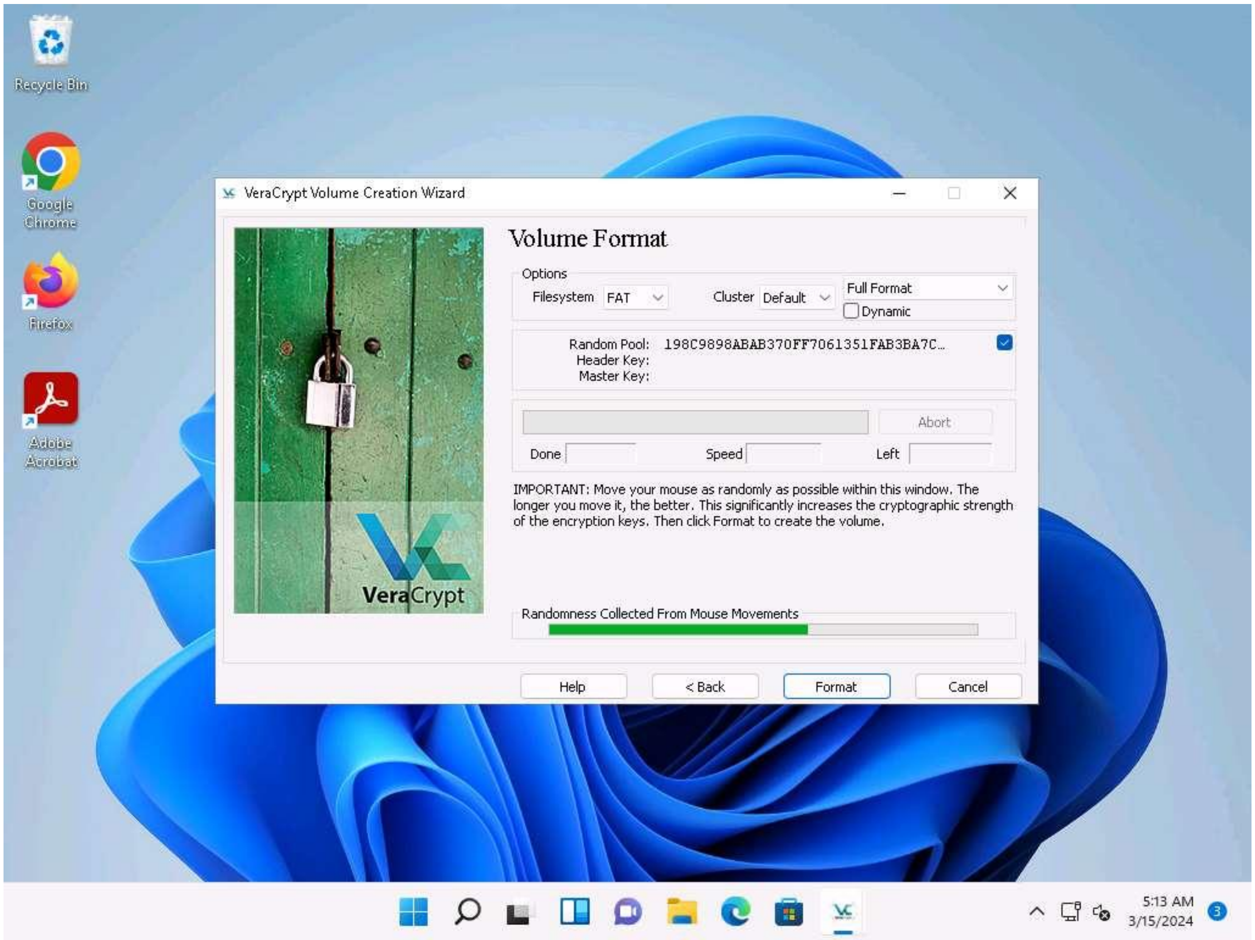
It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of 20 or more characters (the longer, the better). The maximum possible length is 128 characters.

A **VeraCrypt Volume Creation Wizard** warning pop-up appears; then, click **Yes**.

12. The **Volume Format** wizard appears; ensure that **FAT** is selected in the **Filesystem** option and **Default** is selected in **Cluster** option.

13. Check the checkbox under the **Random Pool, Header Key**, and **Master Key** section.

14. Move your mouse as randomly as possible within the **Volume Creation Wizard** window for at least **30 seconds** and click the **Format** button.



VeraCrypt Volume Creation Wizard

Volume Format

Options

Filesystem: FAT

Cluster: Default

Full Format

□ Dynamic

Random Pool: 198C9898ABAB370FF7061351FAB3BA7C… ☑

Header Key:

Master Key:

Done

Speed

Left

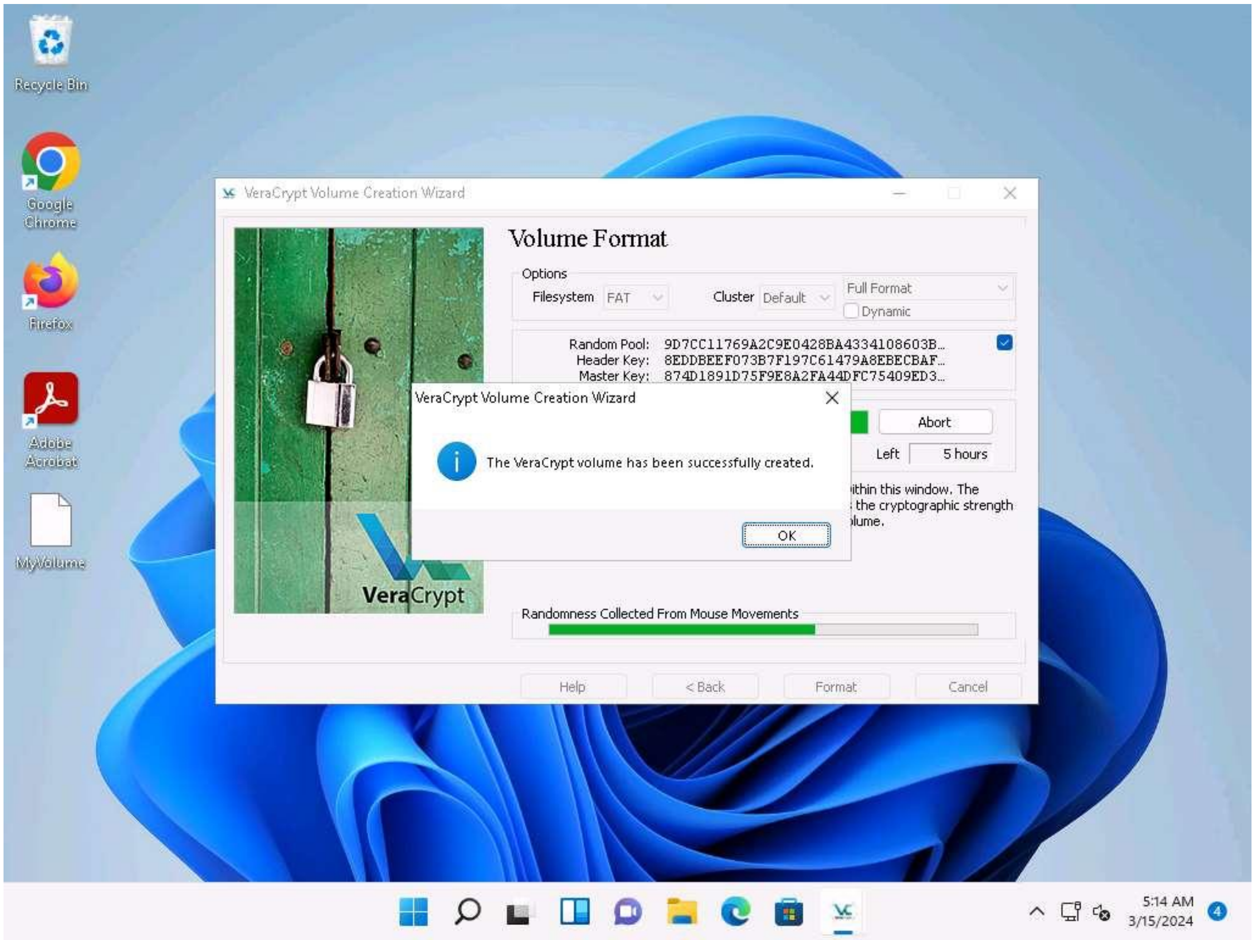
IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.

Randomness Collected From Mouse Movements

15. After clicking **Format**, VeraCrypt will create a file called **MyVolume** in the provided folder. This file depends on the VeraCrypt container (it will contain the encrypted VeraCrypt volume).

16. Depending on the size of the volume, volume creation may take some time.

17. Once the volume is created, a **VeraCrypt Volume Creation Wizard** dialog-box appears; click **OK**.



VeraCrypt Volume Creation Wizard

Volume Format

Options

Filesystem FAT   Cluster Default   Full Format   □ Dynamic

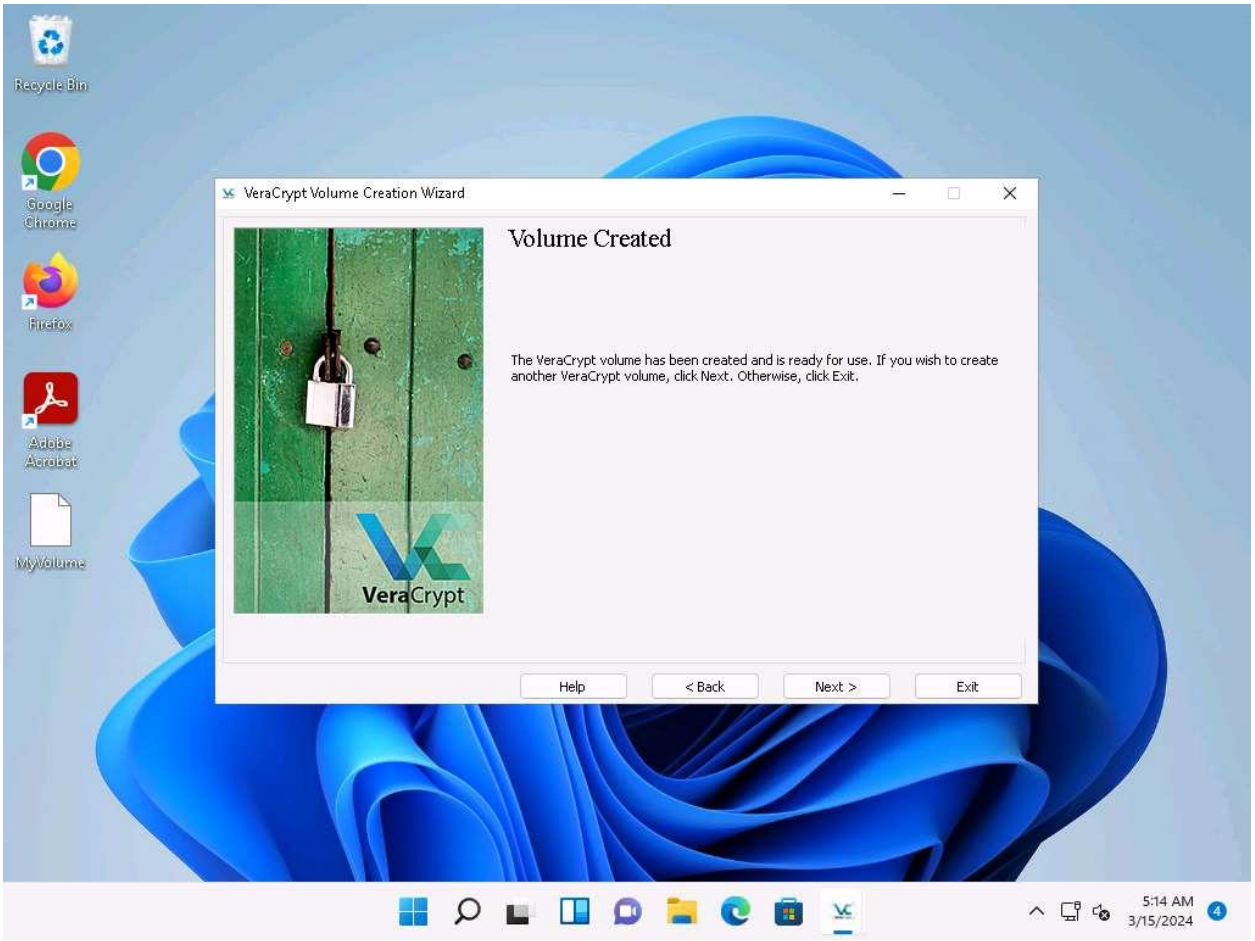
Random Pool: 9D7CC11769A2C9E0428BA4334108603B...
Header Key: 8EDDBEEF073B7F197C61479A8EBECBAF...
Master Key: 874D1891D75F9E8A2FA44DFC75409ED3...

Left 5 hours

VeraCrypt Volume Creation Wizard

The VeraCrypt volume has been successfully created.

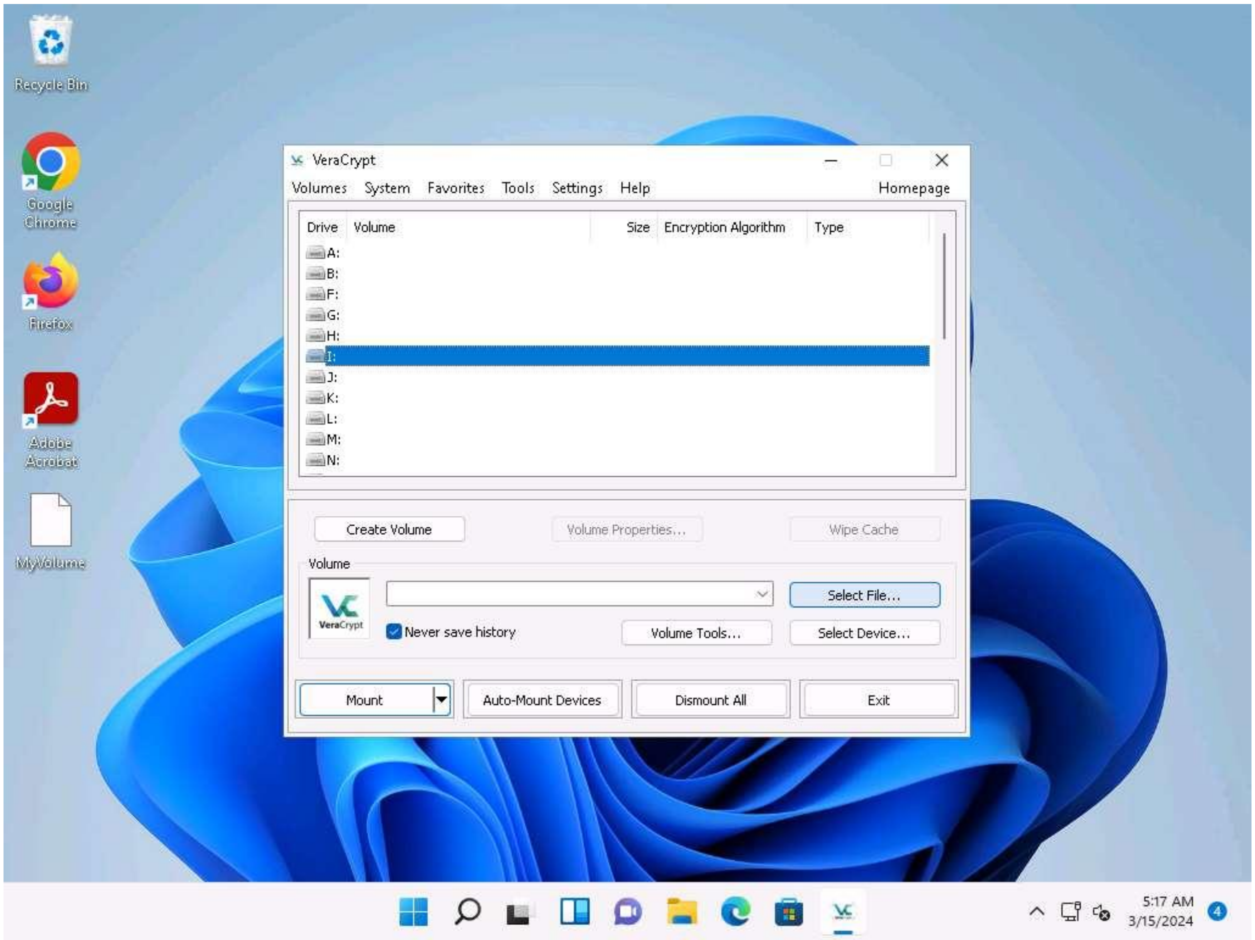
18. In the **VeraCrypt Volume Creation Wizard** window, a **Volume Created** message appears; then, click **Exit**.



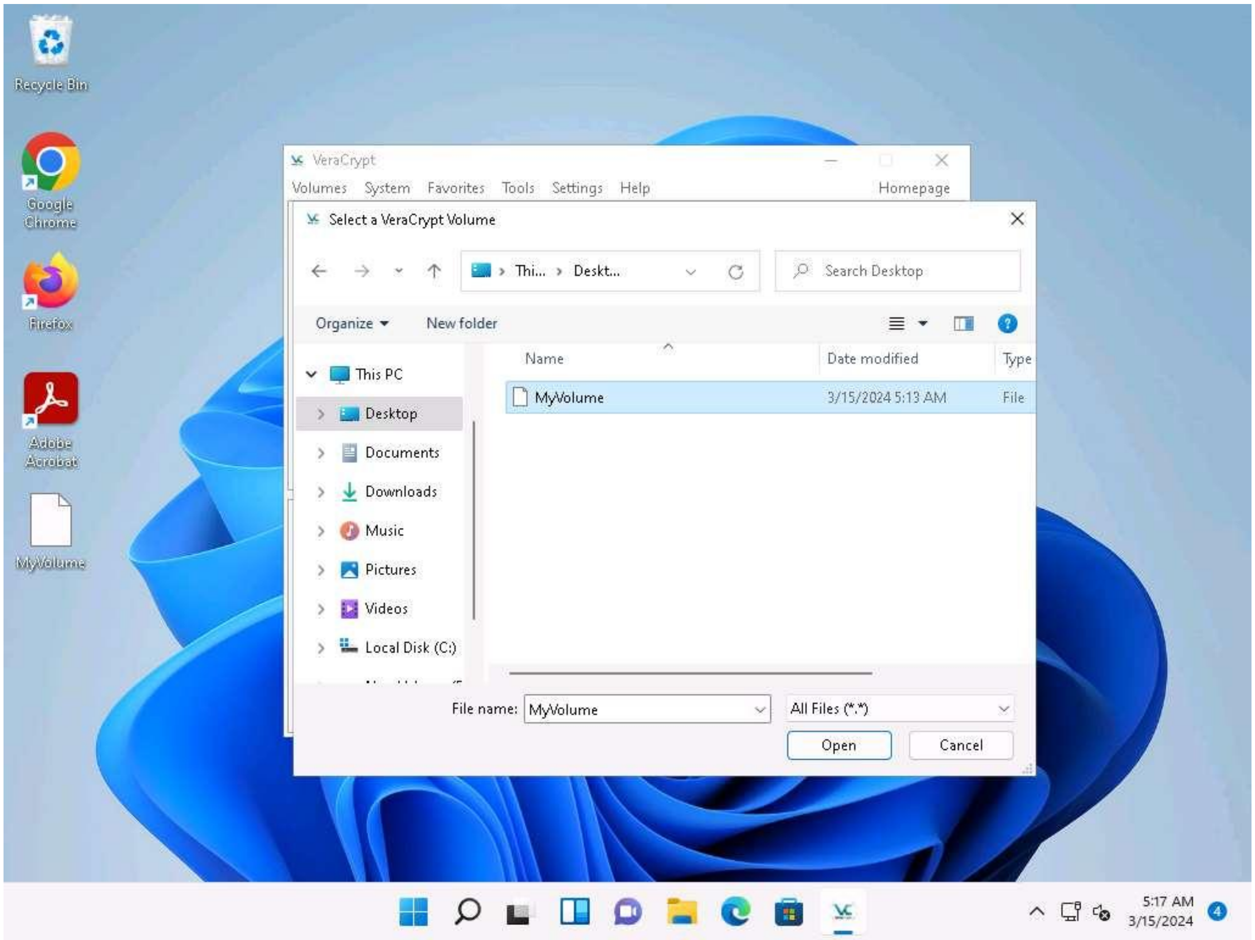
Volume Created

The VeraCrypt volume has been created and is ready for use. If you wish to create another VeraCrypt volume, click Next. Otherwise, click Exit.

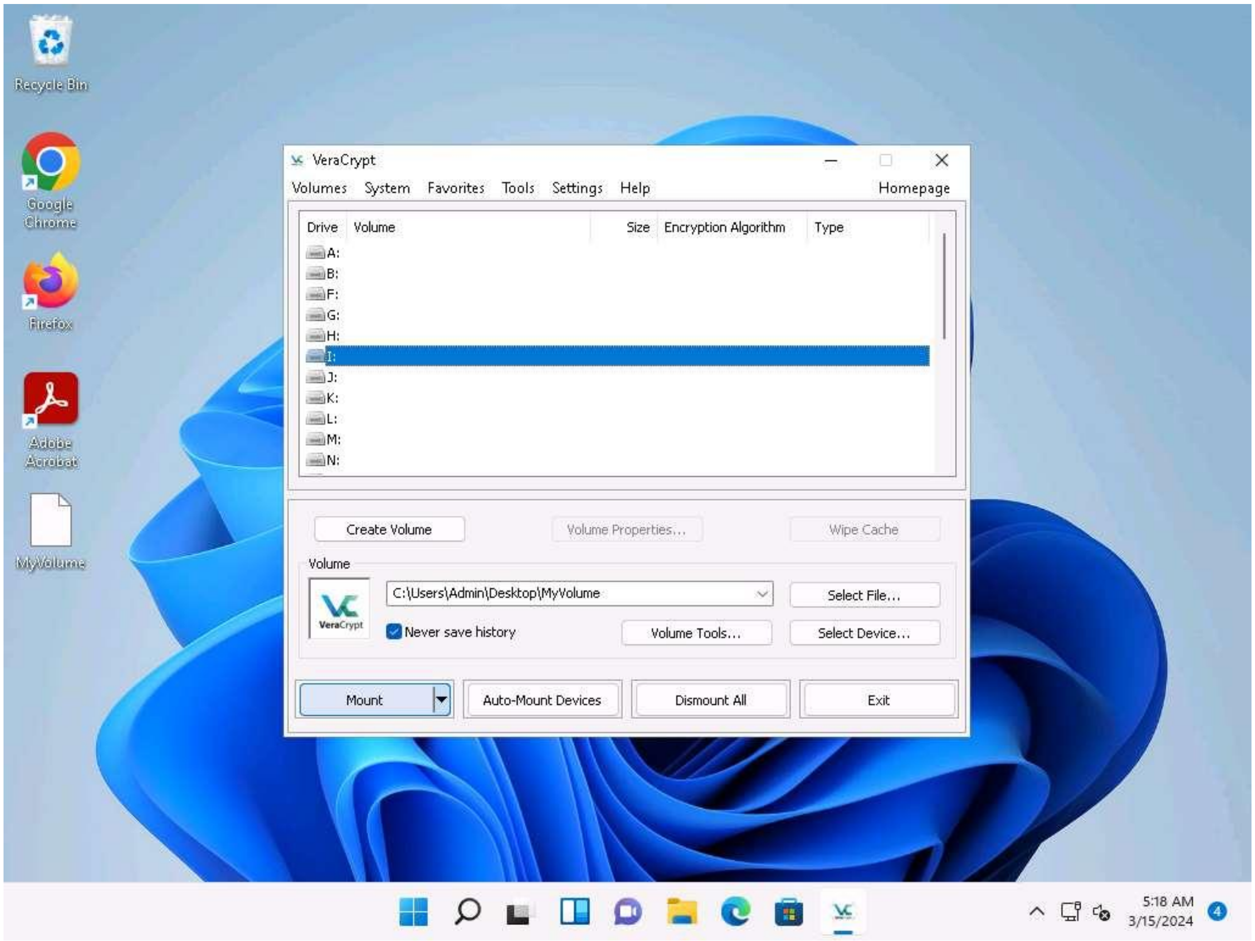
19. The **VeraCrypt** main window appears; select a drive (here, **I:**) and click **Select File…**.



20. The **Select a VeraCrypt Volume** window appears; navigate to **Desktop**, click **MyVolume**, and click **Open**.



21. The window closes, and the **VeraCrypt** window appears displaying the location of selected **volume** under the Volume field; then, click **Mount**.

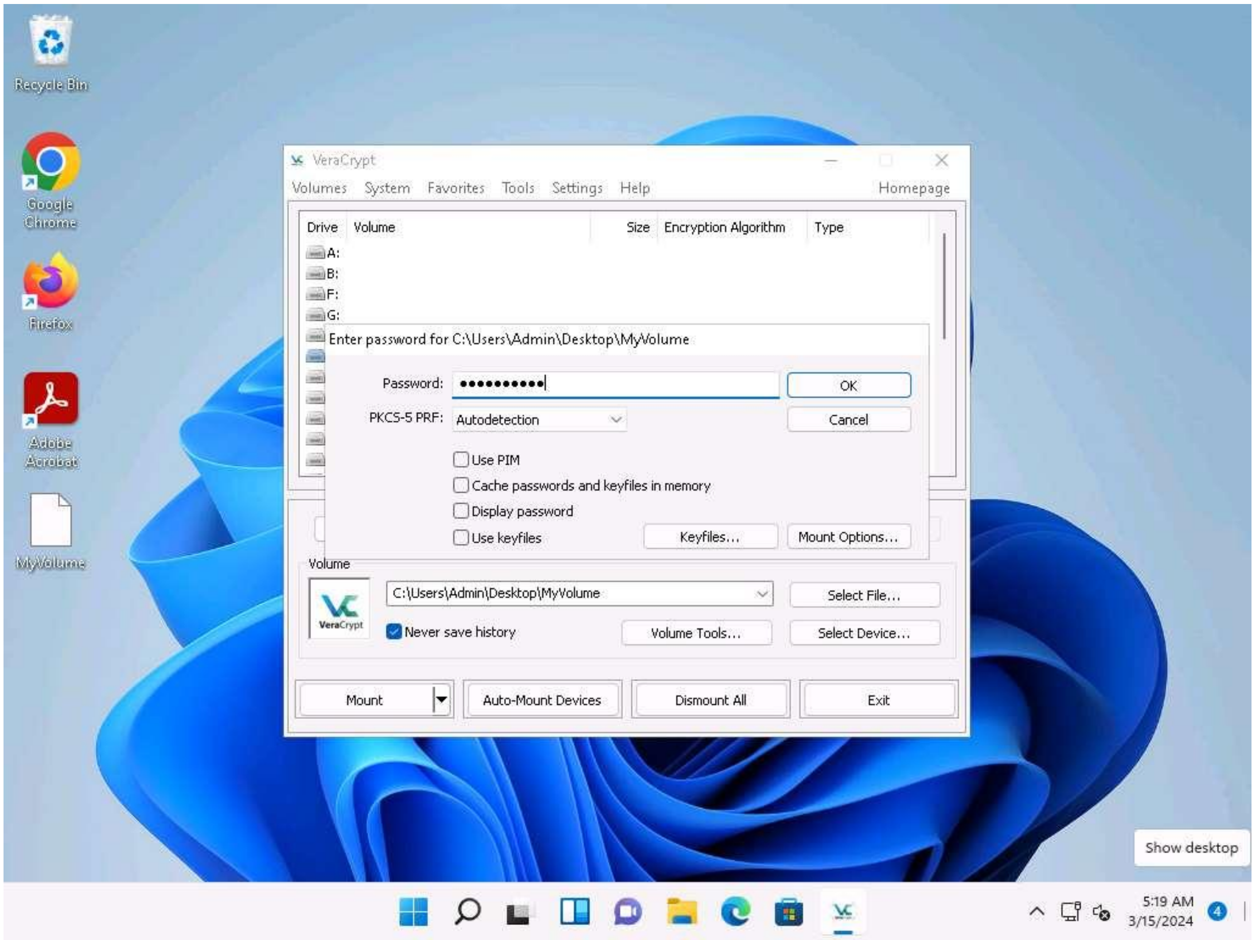


C:\Users\Admin\Desktop\MyVolume

☑ Never save history

22. The **Enter password** dialog-box appears; type the password you specified in **Step#11** into the **Password** field and click **OK**.

The password specified in this task is **qwerty@123**.



Enter password for C:\Users\Admin\Desktop\MyVolume

Password: ●●●●●●●●●●●

PKCS-5 PRF: Autodetection

□ Use PIM

□ Cache passwords and keyfiles in memory

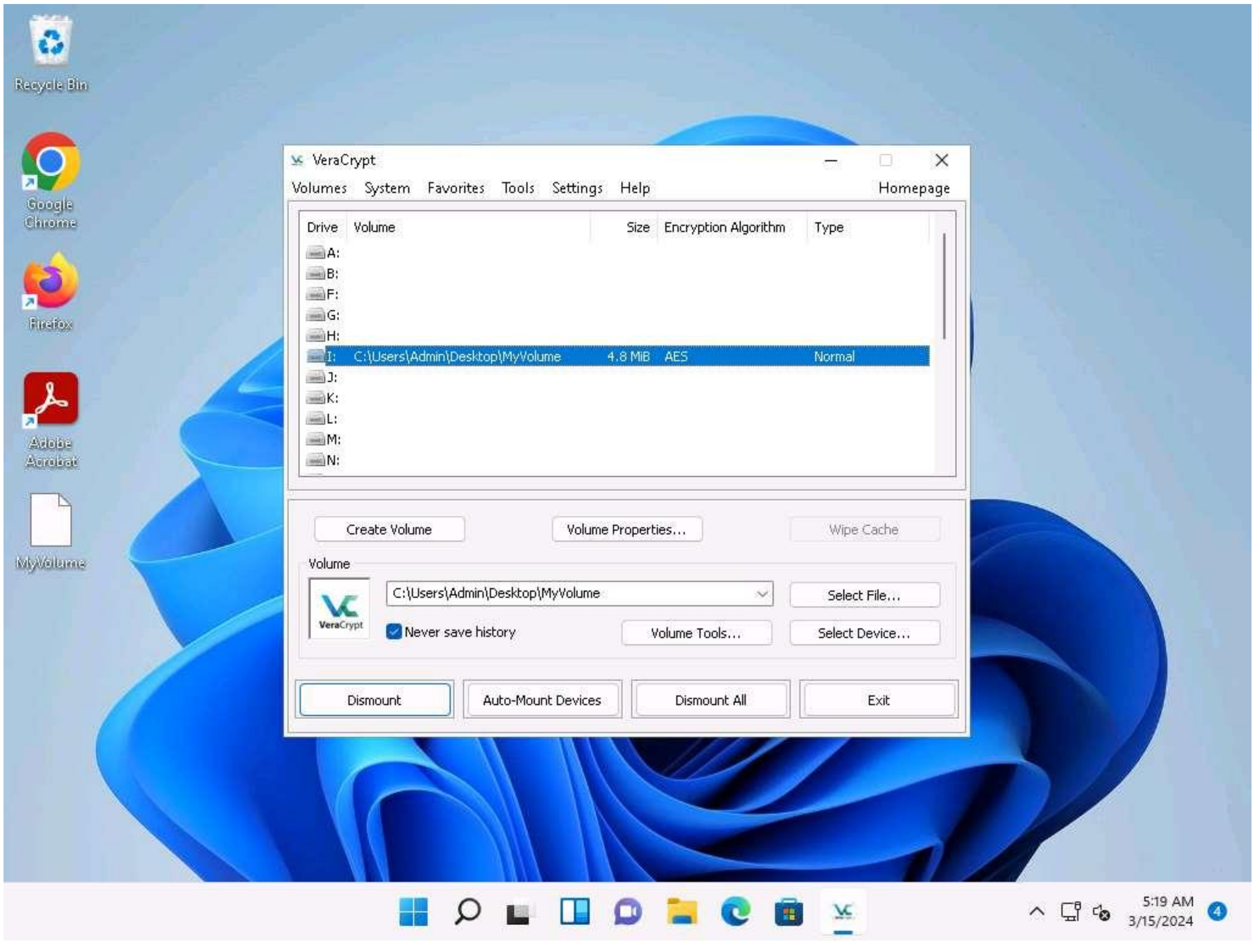
□ Display password

□ Use keyfiles

Volume: C:\Users\Admin\Desktop\MyVolume

☑ Never save history

23. After the password is verified, **VeraCrypt** will mount the volume in **I:** drive, as shown in the screenshot.



Drive	Volume	Size	Encryption Algorithm	Type
A:				
B:				
F:				
G:				
H:				
I:	C:\Users\Admin\Desktop\MyVolume	4.8 MiB	AES	Normal
J:				
K:				
L:				
M:				
N:				

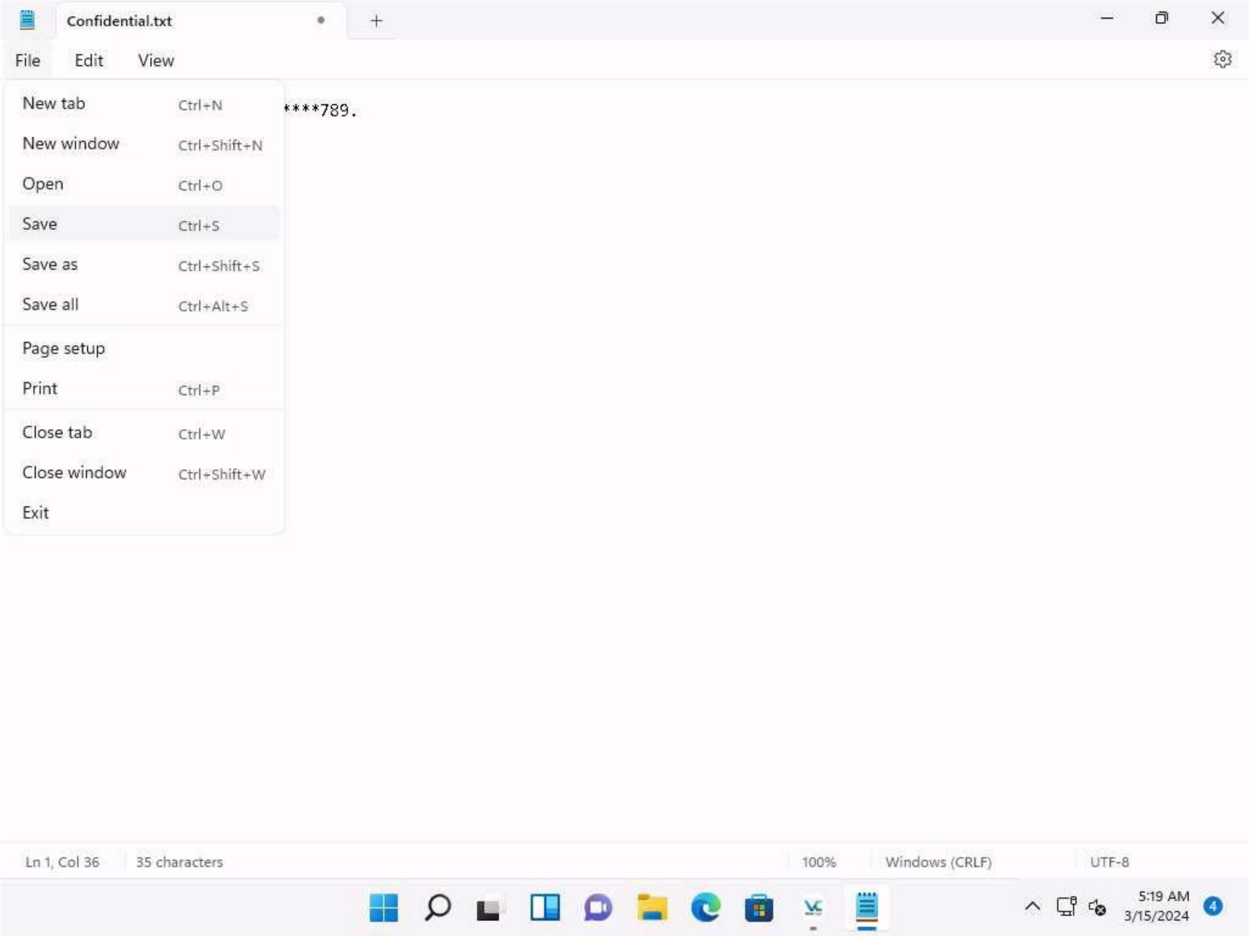
Volume: C:\Users\Admin\Desktop\MyVolume

☑ Never save history

24. **MyVolume** has successfully mounted the container as a virtual disk (**I:**). The virtual disk is entirely encrypted (including file names, allocation tables, free space, etc.) and behaves similarly to a real disk. You can copy or move files to this virtual disk to encrypt them.

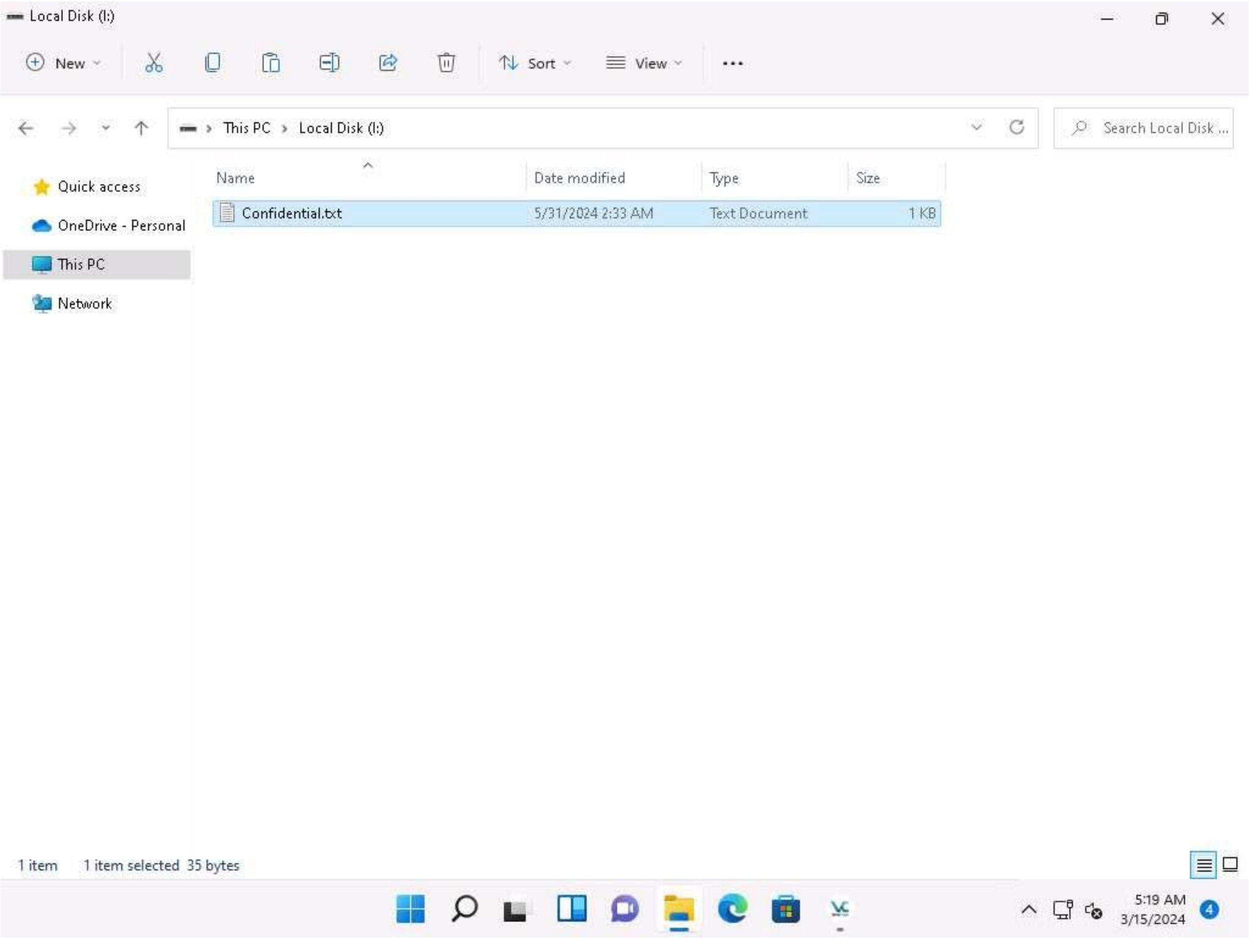
25. Create a text file on **Desktop** and name it **Test**. Open the text file and insert text.

26. Click **File** in the menu bar and click **Save**.



```
****789.
```

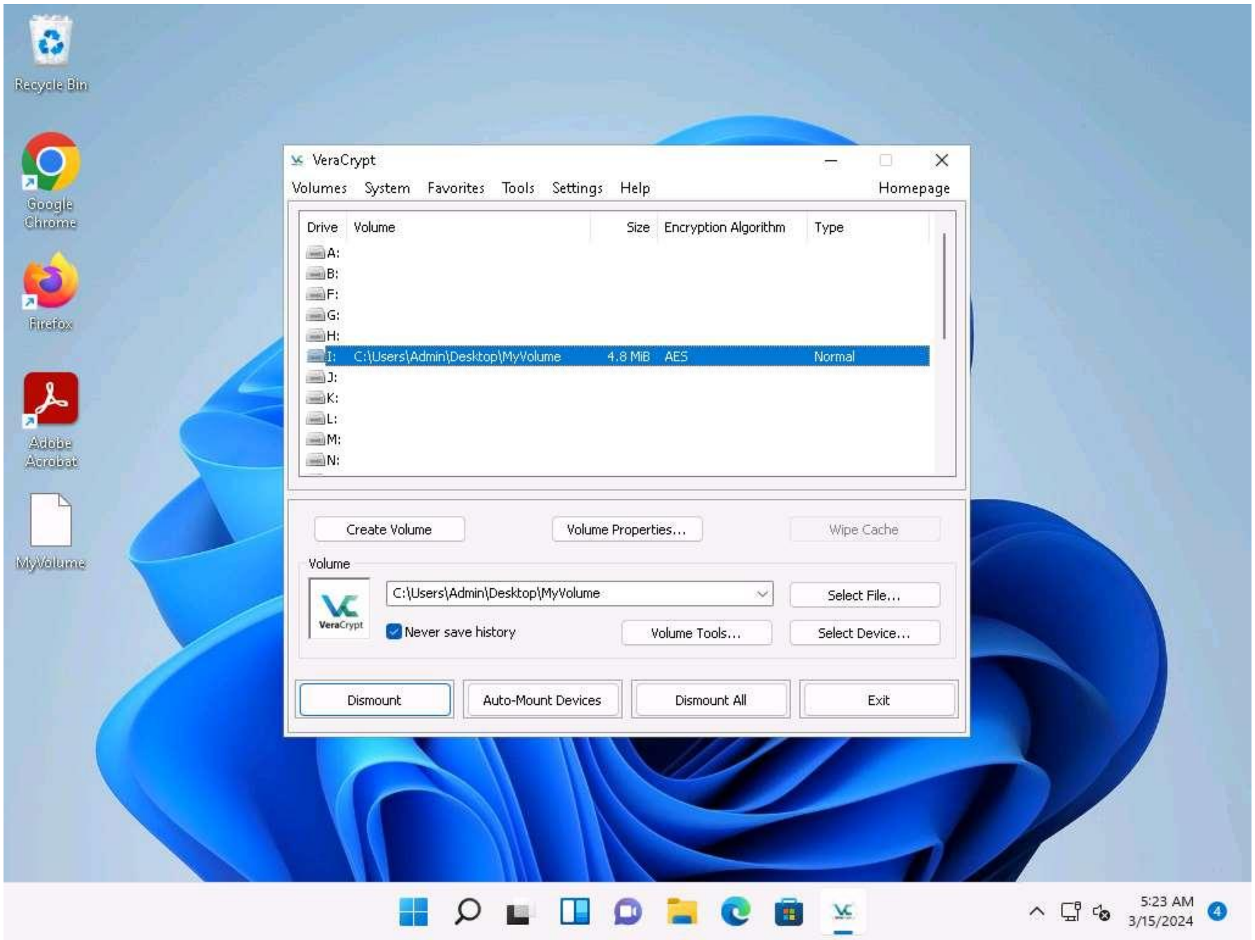
27. Copy the file from **Desktop** and paste it into **Local Disk** (**I:**). Close the window.



Name	Date modified	Type	Size
Confidential.txt	5/31/2024 2:33 AM	Text Document	1 KB

1 item   1 item selected 35 bytes

28. Switch to the **VeraCrypt** window, click **Dismount**, and then click **Exit**.



Drive	Volume	Size	Encryption Algorithm	Type
A:				
B:				
F:				
G:				
H:				
I:	C:\Users\Admin\Desktop\MyVolume	4.8 MiB	AES	Normal
J:				
K:				
L:				
M:				
N:				

Volume: C:\Users\Admin\Desktop\MyVolume

☑ Never save history

29. The **I:** drive located in **This PC** disappears.

This lab is used to demonstrate that, in cases of system hacks, if an attacker manages to gain remote access or complete access to the machine, he/she will not be able to find the encrypted volume-including its files-unless he/she is able to obtain the password. Thus, all sensitive information located on the encrypted volume is safeguarded.

30. This concludes the demonstration of performing disk encryption using VeraCrypt.

31. Close all open windows and document all the acquired information.

Question 20.3.1.1

Use VeraCrypt to create an encrypted volume. The block size of encryption algorithm used to encrypt the volume is 128-bit block. Name the encryption algorithm used in this task.