iMail Email Ingestion & Extraction – Hard Drive Encryption Guide

Email Encryption Guide

Purpose

The purpose of this document is to detail how to encrypt your disks when sending them to iMail for ingestion or extraction.

Software

iMail uses encryption software called VeraCrypt. You can download the software from the follow link https://www.veracrypt.fr/en/Downloads.html

Encrypting your disk

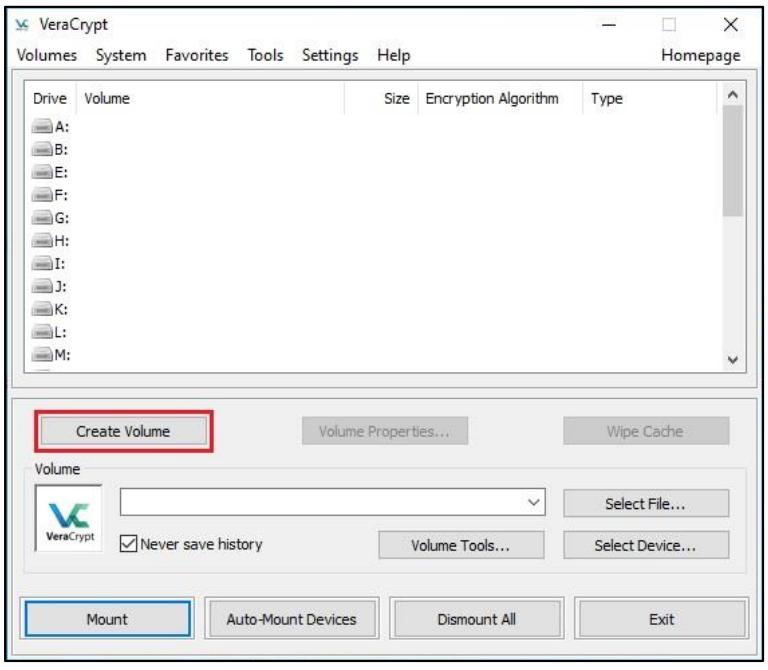
Windows

Below are the step-by-step instructions on how to create, mount, and use a VeraCrypt volume:

STEP 1:

- Download and install VeraCrypt. Then launch VeraCrypt by double-clicking the file VeraCrypt.exe or by clicking the VeraCrypt shortcut in your Windows Start menu.

STEP 2:



- The main VeraCrypt window should appear. Click **Create Volume** (marked with a red rectangle for clarity).

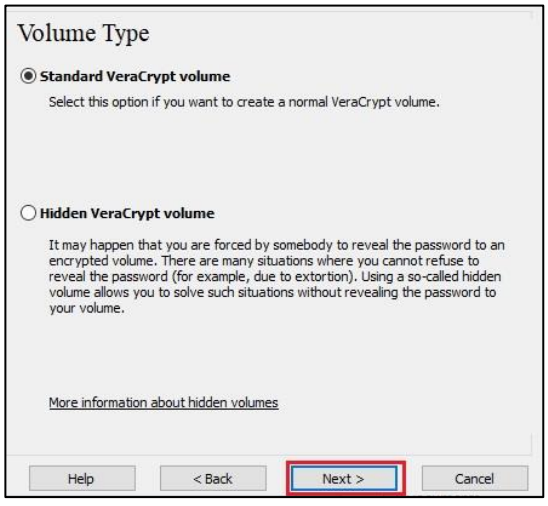
STEP 3:

The VeraCrypt Volume Creation Wizard window should appear. Choose where you wish the VeraCrypt volume to be created. A VeraCrypt volume can reside in a file, which is also called container, in a partition or drive. We will choose the first option and create a VeraCrypt volume within a file.

As the option is selected by default, you can just click **Next**.

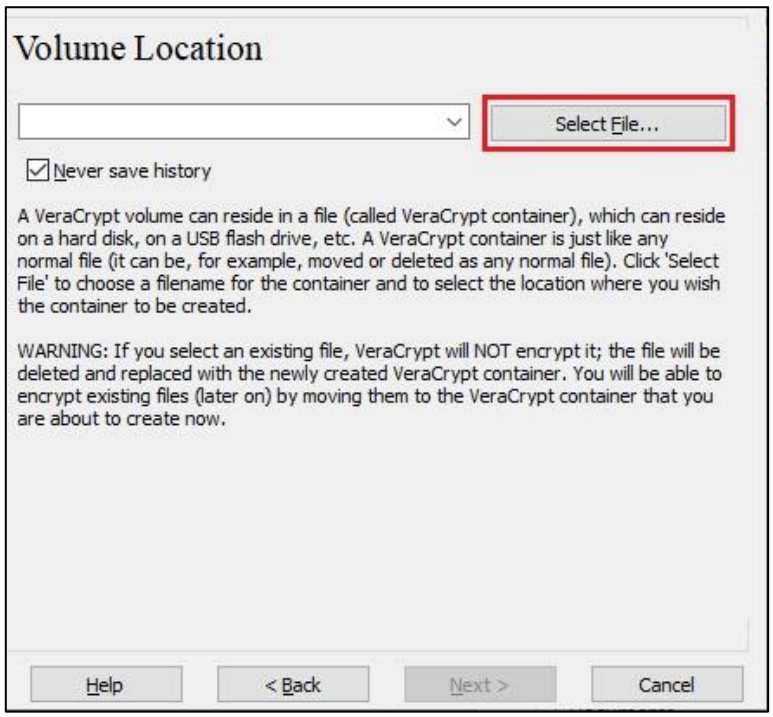
Note: In the following steps, the screenshots will show only the right-hand part of the Wizard window.

STEP 4:



- In this step you need to choose whether to create a standard or hidden VeraCrypt volume.
- We will choose the former option and create a standard VeraCrypt volume. As the option is selected by default, you can just click **Next**.

STEP 5:



- In this step you have to specify where you wish the VeraCrypt volume (file container) to be created.

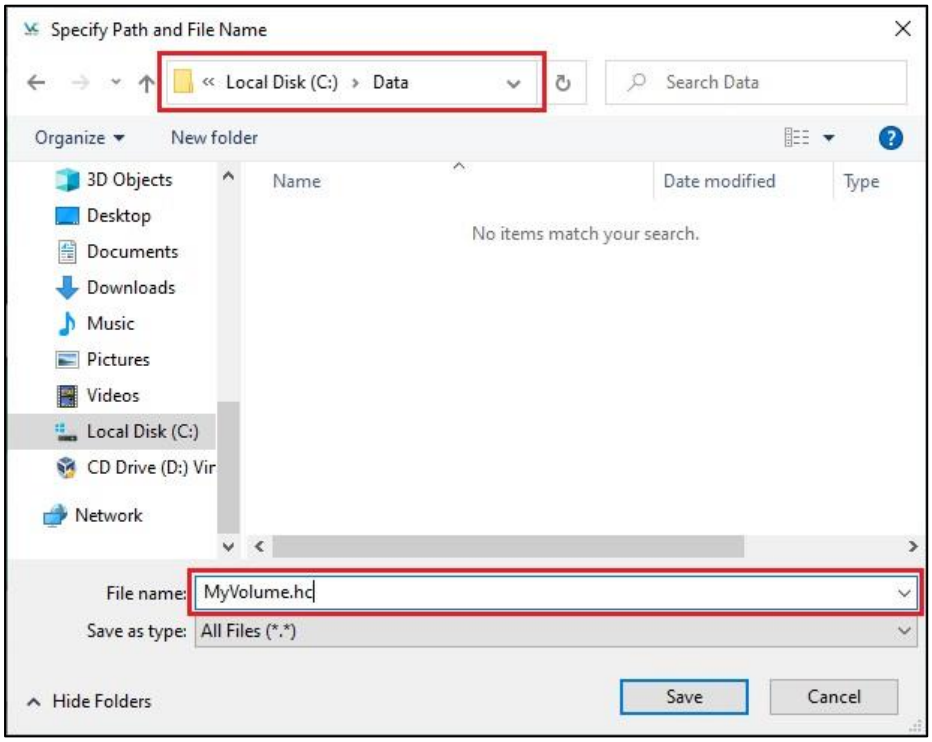
  Please Note: Aa VeraCrypt container is just like any normal file. It can be, for example, moved or deleted as any normal file. It also needs a filename, which you will choose in the next step.

- Click **Select File**. The standard Windows file selector should appear (while the window of the VeraCrypt Volume Creation Wizard remains open in the background).

STEP 6:

We will create our VeraCrypt volume in the folder F:*Data*\ and the filename of the volume (container) will be *MyVolume.hc* (as can be seen in the screenshot above). You may, of course, choose any other filename and location you like (for example, on a USB memory stick).

- Note that the file *MyVolume.hc* does not exist yet – VeraCrypt will create it.

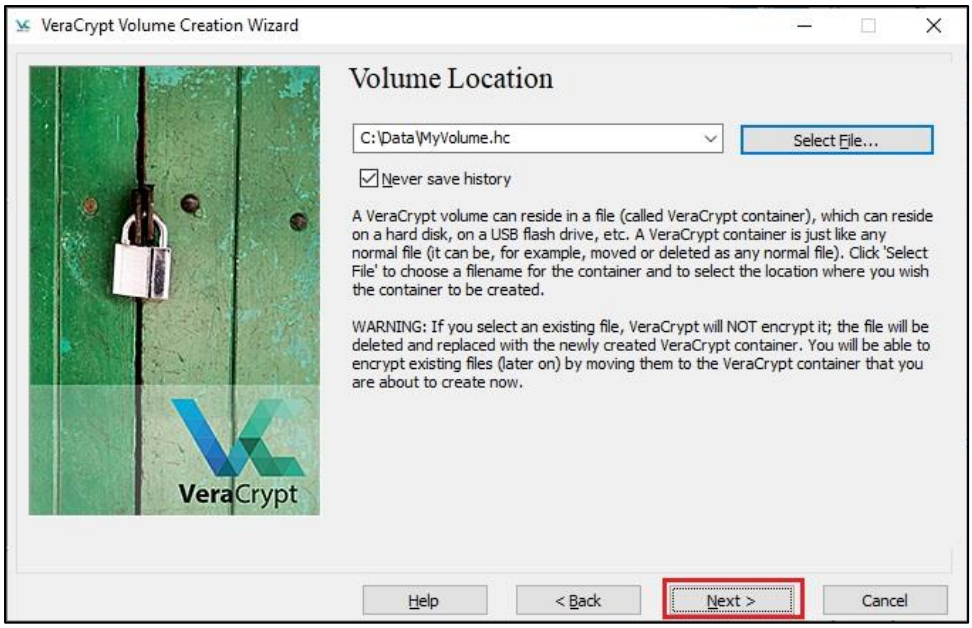


Please Note: VeraCrypt will not encrypt any existing files (when creating a VeraCrypt file container). If you select an existing file in this step, it will be overwritten and replaced by the newly created volume (so the overwritten file will be lost, not encrypted).

You will be able to encrypt existing files (later on) by moving them to the VeraCrypt volume that we are creating now.

- Select the desired path (where you wish the container to be created) in the file selector.
- Type the desired container file name in the **Filename** box.
- Click **Save**.
- The file selector window should disappear.
- In the following steps, we will return to the VeraCrypt Volume Creation Wizard.

STEP 7:

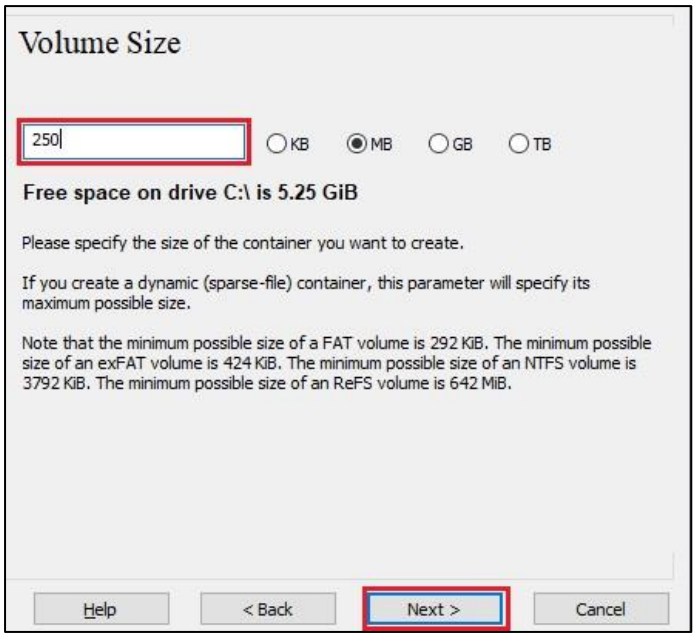


- In the Volume Creation Wizard window, click **Next**.

STEP 8:

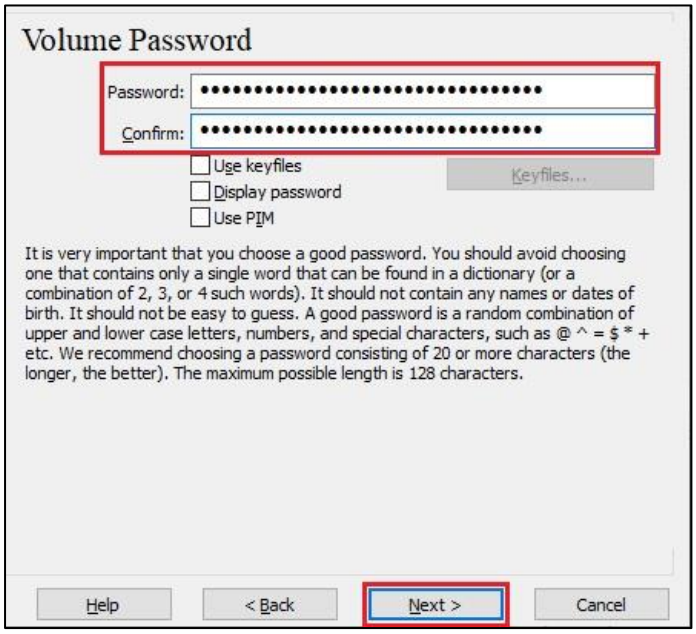
- Here you can choose an encryption algorithm and a hash algorithm for the volume. Please use the default settings and click **Next.**

STEP 9:



- Here we specify that we wish the size of our VeraCrypt container to be 250MB. You may, of course, specify a different size. After you type the desired size in the input field (marked with a red rectangle), click **Next**.

STEP 10:

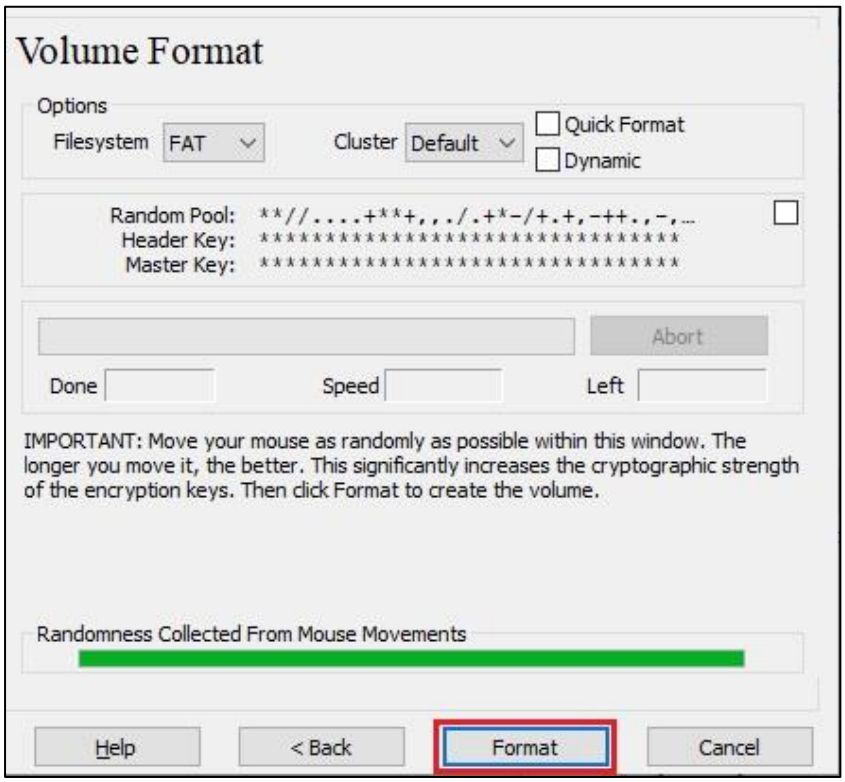


- NB: Here you have to choose a good volume password. Read carefully the information displayed in the Wizard window about what is considered a good password.

- After you choose a good password, type it in the first input field. Then re-type it in the input field below the first one and click **Next**.

*Please Note: The button **Next** will be disabled until passwords in both input fields are the same.*

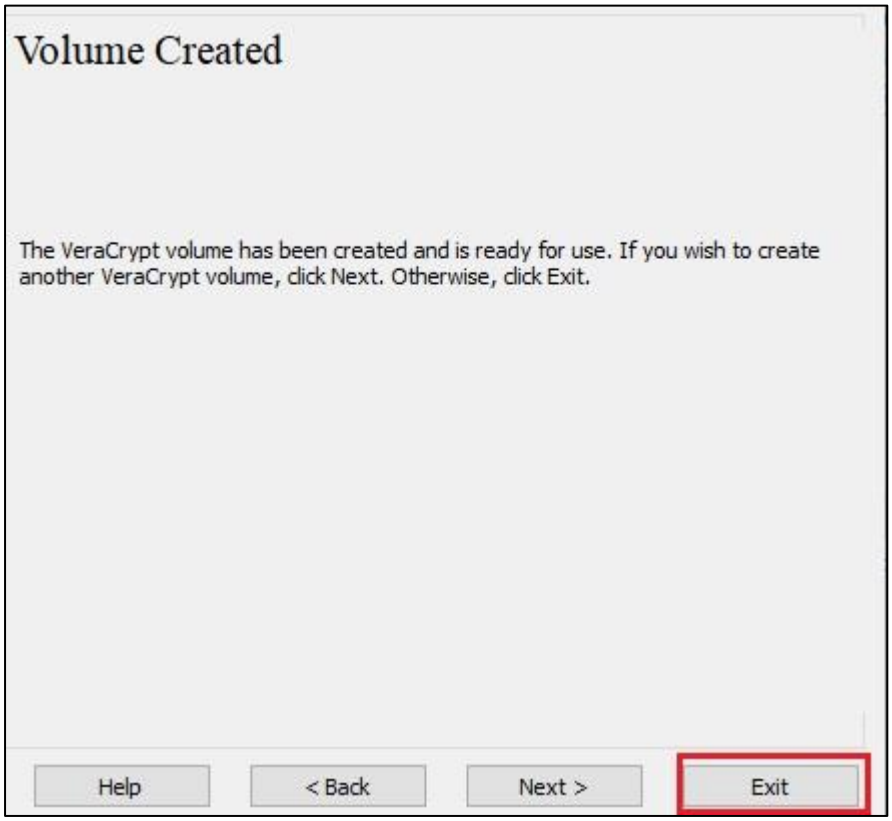
STEP 11:



- Move your mouse as randomly as possible within the Volume Creation Wizard window at least until the randomness indicator becomes green. The longer you move the mouse, the better (moving the mouse for at least 30 seconds is recommended). This significantly increases the cryptographic strength of the encryption keys (which increases security).
- Select the Quick Format option.
- Click **Format**.
- Volume creation should begin. VeraCrypt will now create a file called *MyVolume.hc* in the folder F*:\Data*\ (as we specified in Step 6).
- This file will be a VeraCrypt container (it will contain the encrypted VeraCrypt volume). Depending on the size of the volume, the volume creation may take a long time.
- Once it finishes, the following dialog box will appear:

- Click **OK** to close the dialog box.

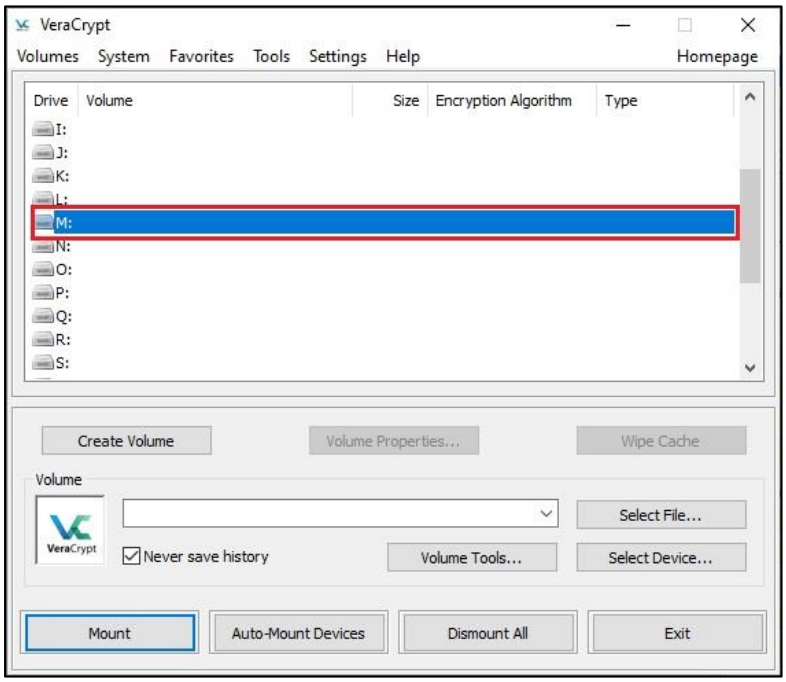
STEP 12:



- We have just successfully created a VeraCrypt volume (file container). In the VeraCrypt Volume Creation Wizard window, click **Exit**. The Wizard window should disappear.

  In the remaining steps, we will mount the volume we just created. We will return to the main VeraCrypt window (which should still be open, but if it is not, repeat Step 1 to launch VeraCrypt and then continue from Step 13.)

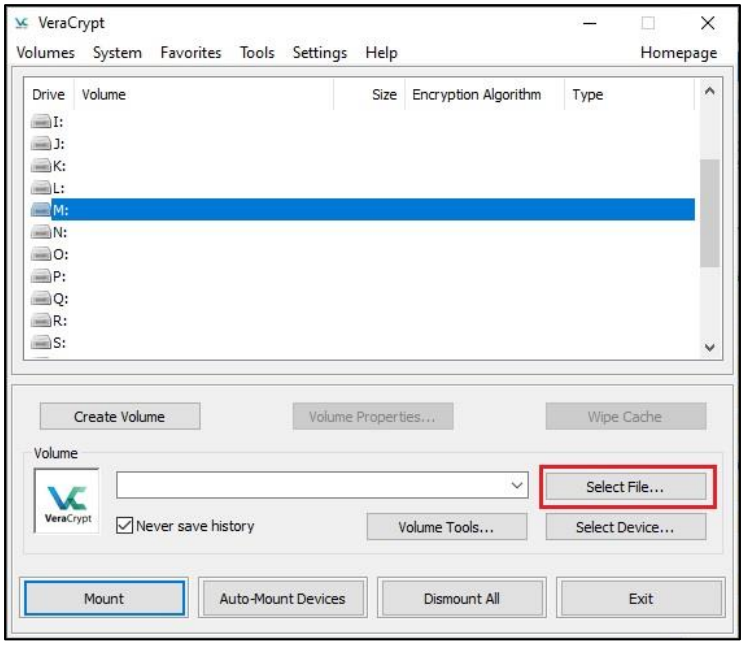
STEP 13:



- Select a drive letter from the list (marked with a red rectangle). This will be the drive letter to which the VeraCrypt container will be mounted.

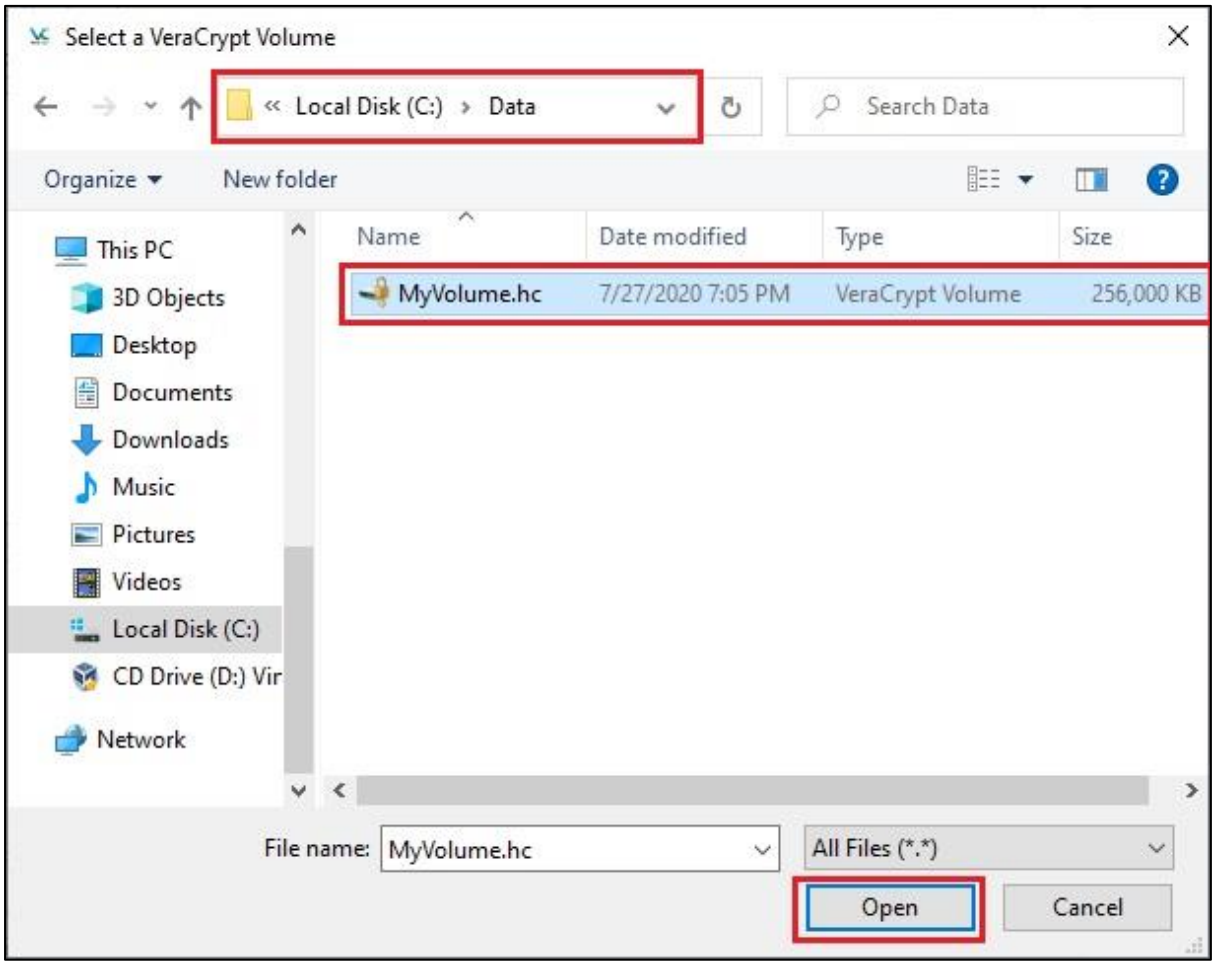
  Please Note: We chose the drive letter M, but you may of course choose any other available drive letter.

STEP 14:



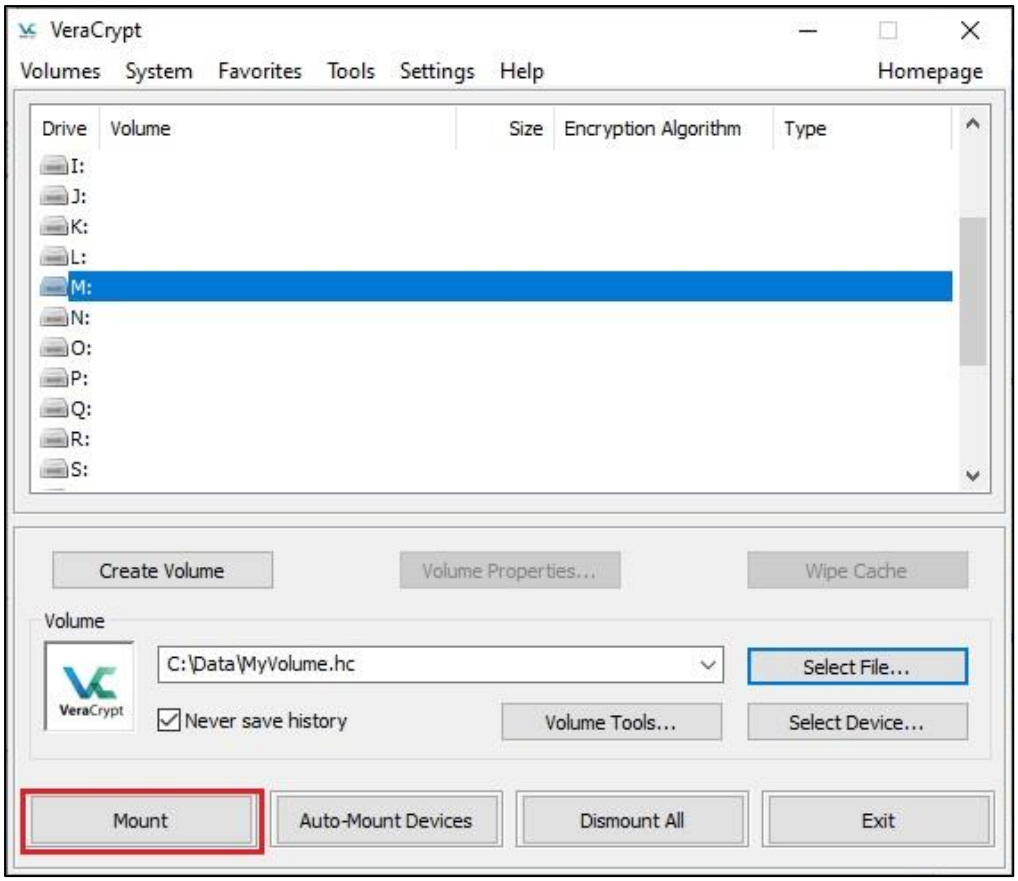
- Click **Select File**.
- The standard file selector window should appear.

STEP 15:



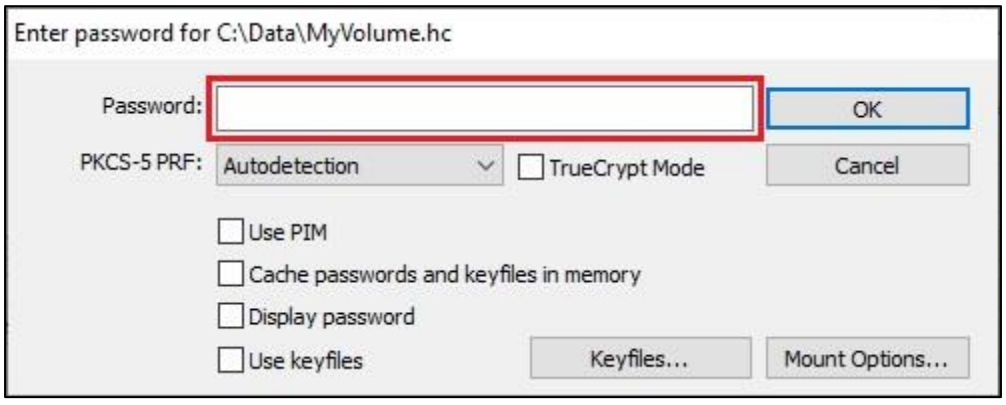
- In the file selector, browse to the container file (which we created in Steps 6-12) and select it.
- Click **Open** (in the file selector window).
- The file selector window should disappear.
- In the following steps, we will return to the main VeraCrypt window.

STEP 16:



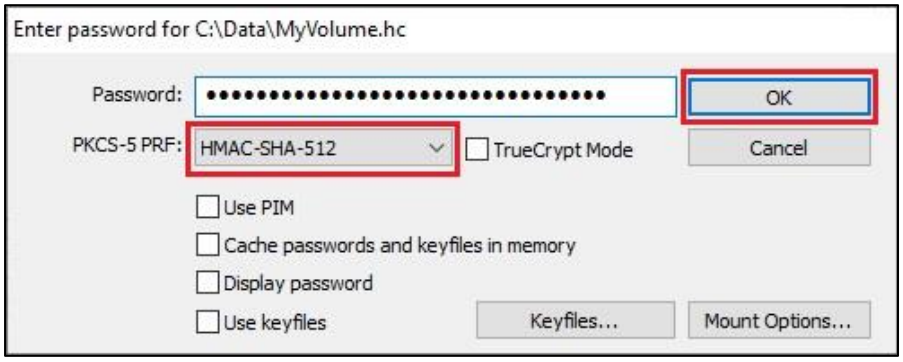
- In the main VeraCrypt window, click **Mount**. Password prompt dialog window should appear.

STEP 17:



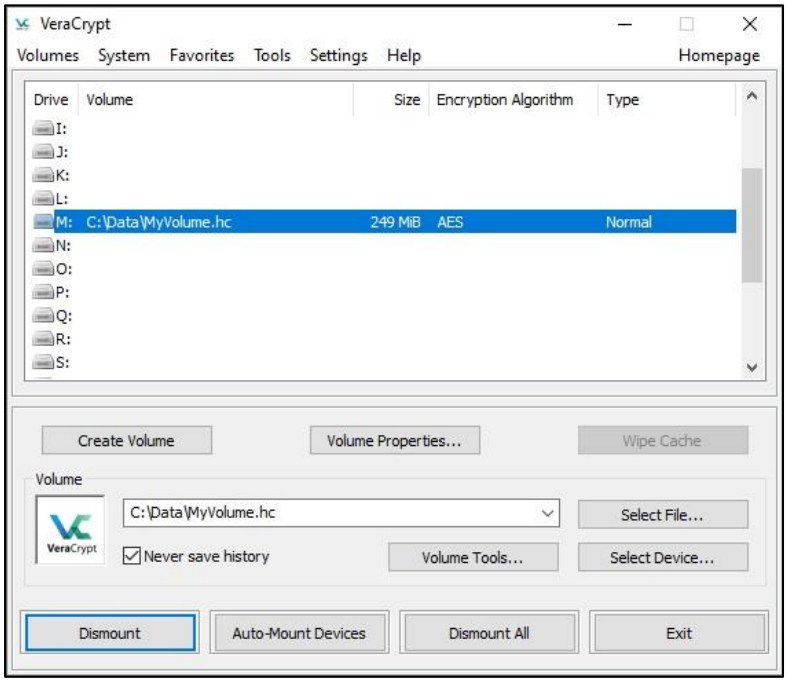
- Type the password (which you specified in Step 10) in the password input field (marked with a red rectangle).

STEP 18:



- Select the PRF algorithm that was used during the creation of the volume (SHA-512 is the default PRF used by VeraCrypt). If you don't remember which PRF was used, just leave it set to "autodetection" but the mounting process will take more time. Click OK after entering the password.
- VeraCrypt will now attempt to mount the volume. If the password is incorrect (for example, if you typed it incorrectly), VeraCrypt will notify you and you will need to repeat the previous step (type the password again and click OK). If the password is correct, the volume will be mounted.

FINAL STEP:



- We have just successfully mounted the container as a virtual disk M:

- The virtual disk is entirely encrypted (including file names, allocation tables, free space, etc.) and behaves like a real disk. You can save (or copy, move, etc.) files to this virtual disk and they will be encrypted on the fly as they are being written.

Please Note: When you open a file stored on a VeraCrypt volume (or when you write/copy a file to/from the VeraCrypt volume) you will not be asked to enter the password again. You need to enter the correct password only when mounting the volume.

- You can open the mounted volume, for example, by selecting it on the list as shown in the screenshot above (blue selection) and then double-clicking on the selected item.

- You can also browse to the mounted volume the way you normally browse to any other types of volumes. For example, by opening the '*Computer*' (or '*My Computer*') list and double clicking the corresponding drive letter (in this case, it is the letter M).

Linux

Below are the step-by-step instructions on how to create, mount, and use a VeraCrypt volume for Linux.

STEP 1:

Format:

Veracrypt --text --create --size=size[K|M|GT] --quick --volume-type=normal /dev/sd[xx] --encryption=aes --hash=sha-512 --filesystem=ext4 --password=[password] --pim=0 --keyfiles="" --random-source=/dev/urandom

STEP 2:

Mount:

veracrypt --text --pim=0 --protect-hidden=no --filesystem=ext4 --volume-type=normal --password=[password] --filesystem=ext4 --keyfiles="" /dev/sd[xx] /mnt/temp

- If you receive a complaint saying "kernel version not supported" you can add **m=nokernelcrypto** to the above mount command.