Institiúid Teicneolaíochta Leitir Ceanainn
Letterkenny Institute of Technology

lyit | educating for life

Computer Services

Quick Guide on How to Use an Encrypted **Vera**Crypt Container

lyit | Institiúid Teicneolaíochta Leitir Ceanainn - Seirbhísí Ríomhaireachta
Letterkenny Institute of Technology - Computer Services

Introduction

This guide shows you how to use VeraCrypt to securely store confidential and sensitive data on an encrypted storage container (e.g. on USB pen drives, External hard drive etc.)

VearCrypt Container Encryption creates an encrypted area (container) on a disk. The size of the area can be defined by the user. Once files are moved to the area they are automatically encrypted.

This guide shows you how to:

- Download and install VeraCrypt
- Create an encrypted storage Container in VeraCrypt
- Mount the VeraCrypt container (to use as a normal drive)
- Add / Remove files to the encrypted drive.

You should read this document in its entirety before attempting this procedure.

By following the guidance in this document you are helping to improve compliance with the Institutes Information Security and Data Protection Policies.

What is encryption?

Encryption helps secure confidential and sensitive data by converting it into a form that cannot be understood by criminals.

Why use VearCrypt?

VeraCrypt creates an encrypted storage space, called a container, to securely store confidential and sensitive data. The container can be created on external drives, e.g. USB thumb drive, external hard drive etc. When you place your files into the VeraCrypt Container it automatically encrypts the data using encryption and your pre-determined password. You will be required to have VearCrypt installed on each device you wish to use to open the encrypted data.

When do I need to create an encrypted storage drive?

Encrypted storage drives need to be used for all confidential and sensitive data when:

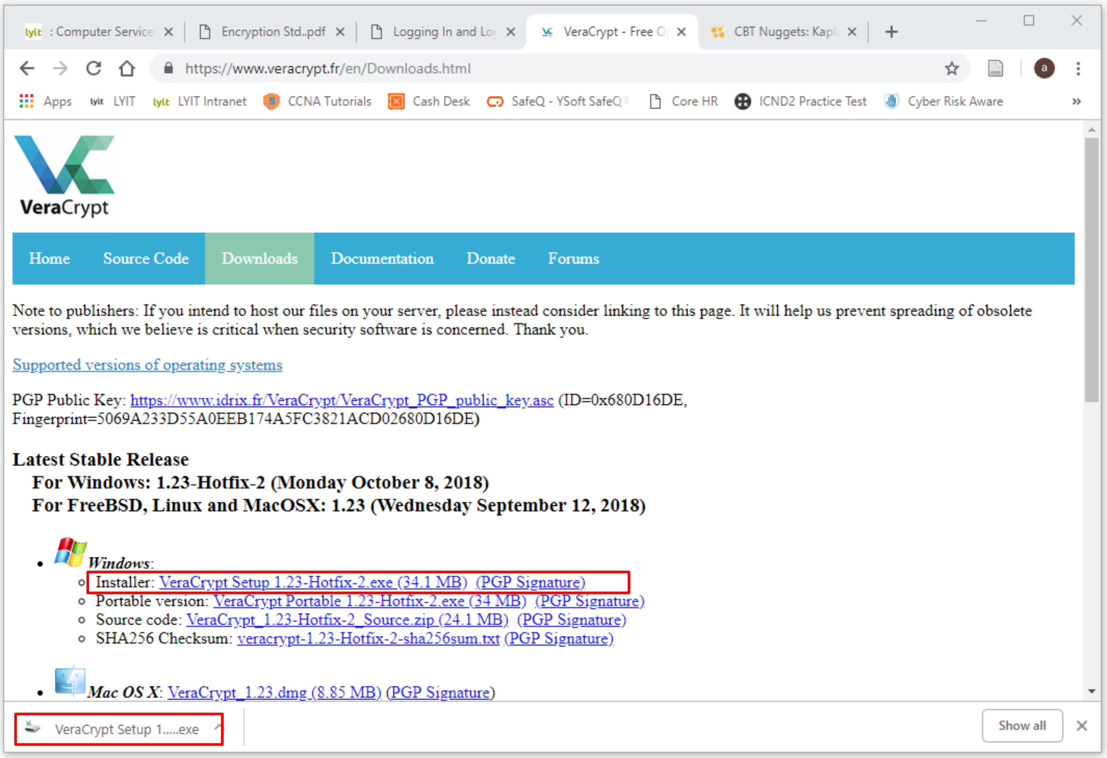
- It is not possible to store the data on secure Institute servers.
- It is kept on a portable storage device (e.g. USB thumb drive, External Hard Drive etc...)

1. Download and Install VeraCrypt

Go to https://www.veracrypt.fr/en/Downloads.html and download the version of VeraCrypt that is best suited to your operating system (typically Microsoft Windows).

VeraCrypt will automatically download after you have clicked on the appropriate link.

Click on the download in your browser to initiate the instillation (Fig 1). (Alternatively if installing at a later date, double click on the 'VeraCrypt Setup 1.23-Hotfix-2.exe' file in downloads VeraCrypt Setup 1.23-Hotfix-2.exe)



Note to publishers: If you intend to host our files on your server, please instead consider linking to this page. It will help us prevent spreading of obsolete versions, which we believe is critical when security software is concerned. Thank you.

Supported versions of operating systems

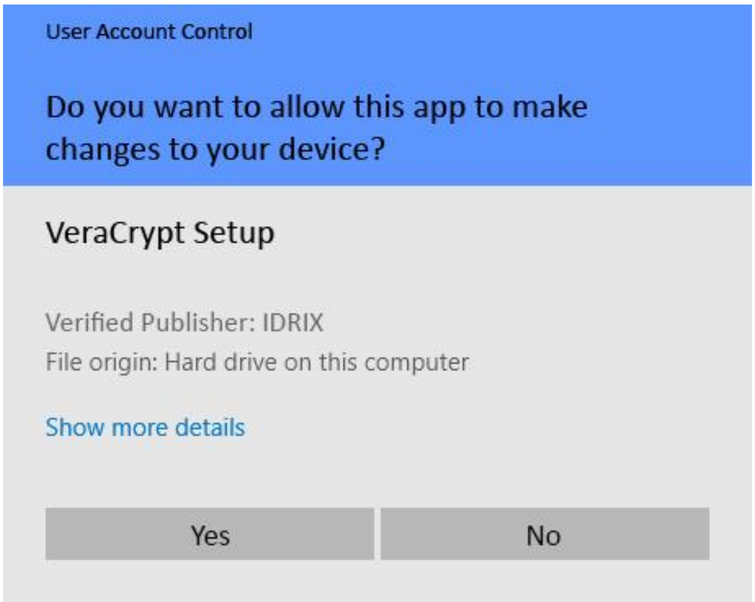
PGP Public Key: https://www.idrix.fr/VeraCrypt/VeraCrypt_PGP_public_key.asc (ID=0x680D16DE, Fingerprint=5069A233D55A0EEB174A5FC3821ACD02680D16DE)

Latest Stable Release
For Windows: 1.23-Hotfix-2 (Monday October 8, 2018)
For FreeBSD, Linux and MacOSX: 1.23 (Wednesday September 12, 2018)

- *Windows*:
  - Installer: VeraCrypt Setup 1.23-Hotfix-2.exe (34.1 MB) (PGP Signature)
  - Portable version: VeraCrypt Portable 1.23-Hotfix-2.exe (34 MB) (PGP Signature)
  - Source code: VeraCrypt_1.23-Hotfix-2_Source.zip (24.1 MB) (PGP Signature)
  - SHA256 Checksum: veracrypt-1.23-Hotfix-2-sha256sum.txt (PGP Signature)
- *Mac OS X*: VeraCrypt_1.23.dmg (8.85 MB) (PGP Signature)

(Fig 1 – browser window with VeraCrypt download)

Click **Yes** (Fig 2) to allow the instillation.



User Account Control

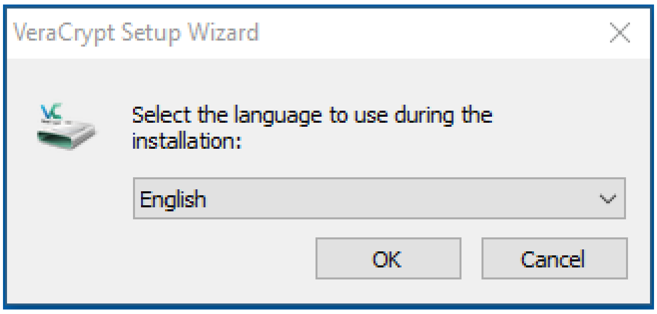
Do you want to allow this app to make changes to your device?

VeraCrypt Setup

Verified Publisher: IDRIX
File origin: Hard drive on this computer

(Fig 2 – User Account Control)

Select your language and click **OK** (Fig 3).

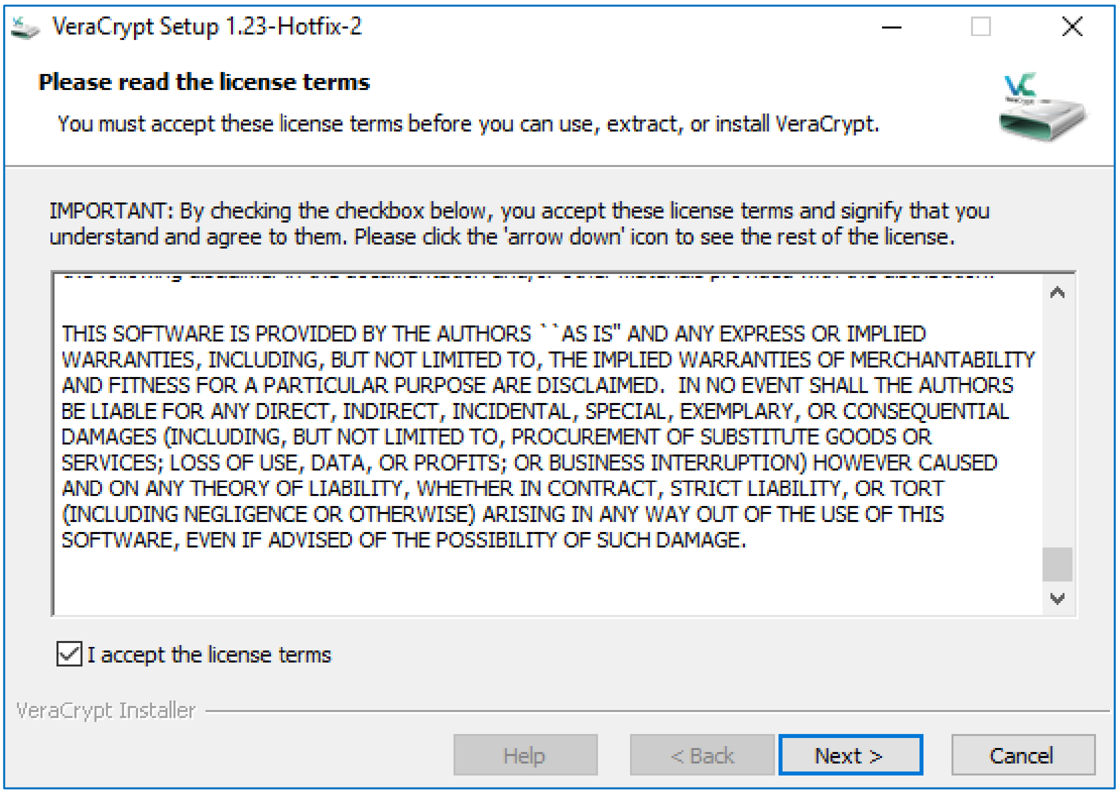


Select the language to use during the installation:

English

(Fig 3 – Language Selection)

Read and Accept the License Terms and click **Next** (Fig 4).



Please read the license terms

You must accept these license terms before you can use, extract, or install VeraCrypt.

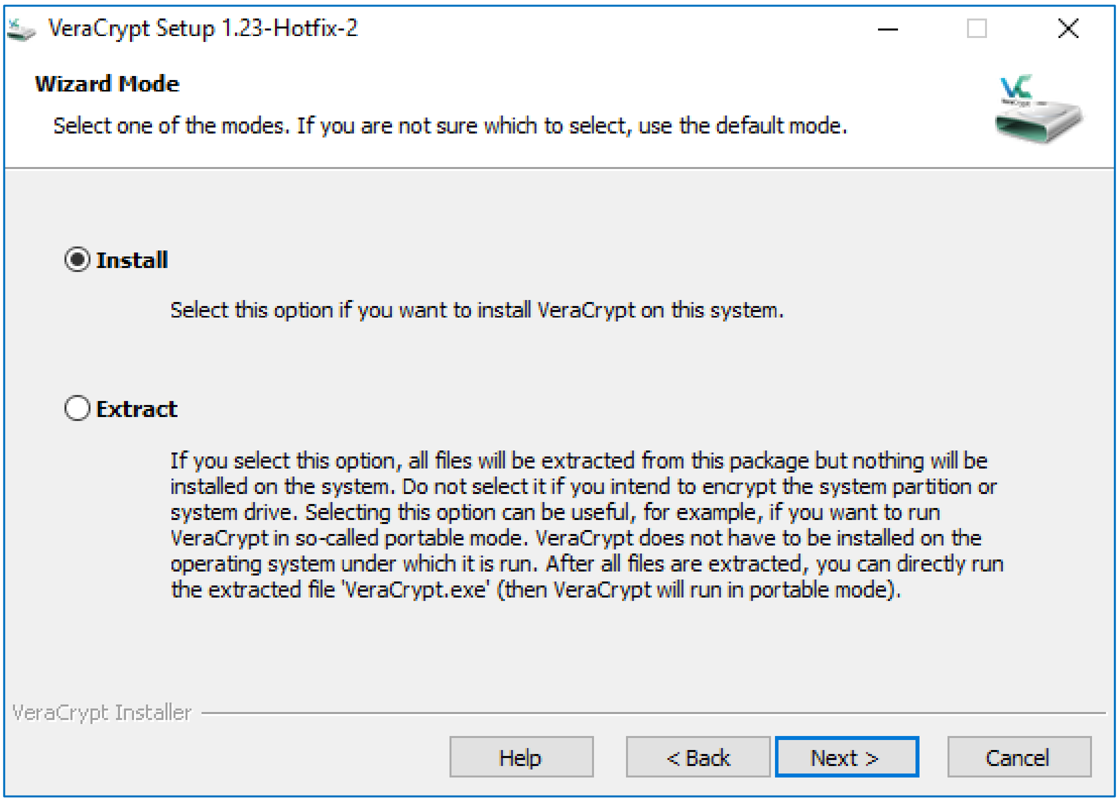
IMPORTANT: By checking the checkbox below, you accept these license terms and signify that you understand and agree to them. Please click the 'arrow down' icon to see the rest of the license.

THIS SOFTWARE IS PROVIDED BY THE AUTHORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

☑ I accept the license terms

(Fig 4 – The license terms)

Choose to Install (Fig 5) and click **Next**



VeraCrypt Setup 1.23-Hotfix-2

Wizard Mode

Select one of the modes. If you are not sure which to select, use the default mode.

● **Install**

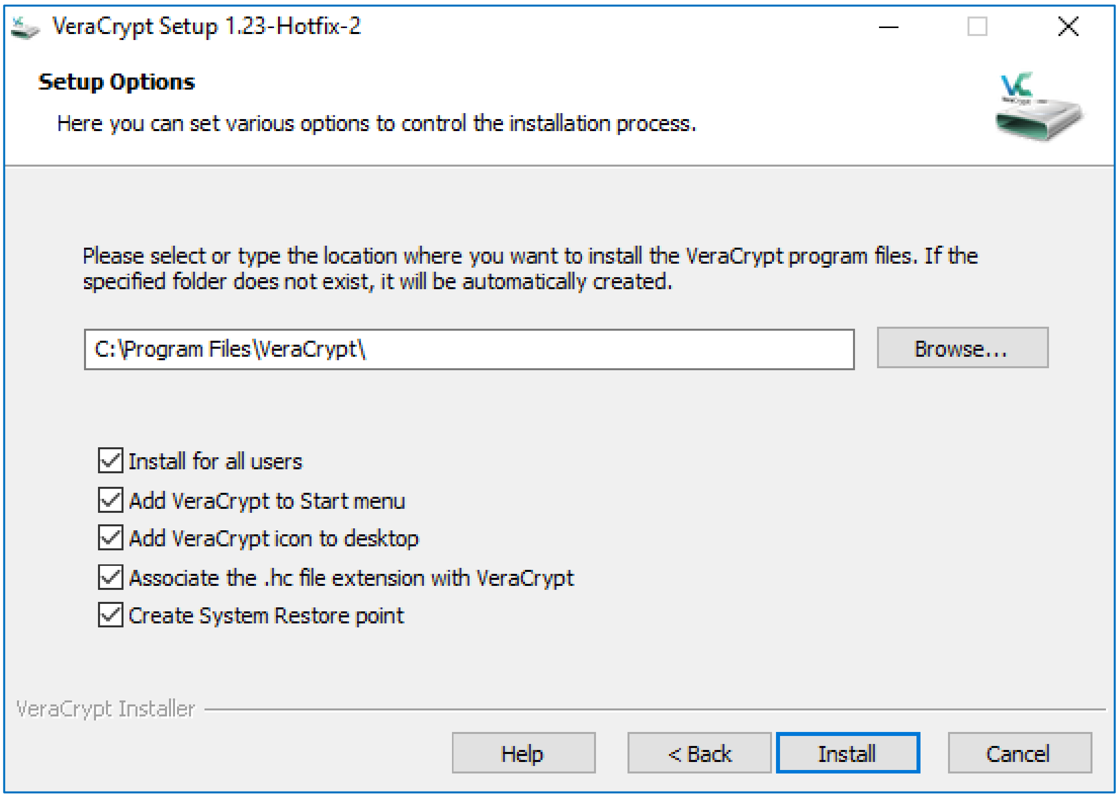
Select this option if you want to install VeraCrypt on this system.

○ **Extract**

If you select this option, all files will be extracted from this package but nothing will be installed on the system. Do not select it if you intend to encrypt the system partition or system drive. Selecting this option can be useful, for example, if you want to run VeraCrypt in so-called portable mode. VeraCrypt does not have to be installed on the operating system under which it is run. After all files are extracted, you can directly run the extracted file 'VeraCrypt.exe' (then VeraCrypt will run in portable mode).

(Fig 5 – Install VeraCrypt)

Select the location to install VeraCrypt (Fig 6) and click **Install**.



VeraCrypt Setup 1.23-Hotfix-2

Setup Options

Here you can set various options to control the installation process.

Please select or type the location where you want to install the VeraCrypt program files. If the specified folder does not exist, it will be automatically created.

C:\Program Files\VeraCrypt\

☑ Install for all users

☑ Add VeraCrypt to Start menu

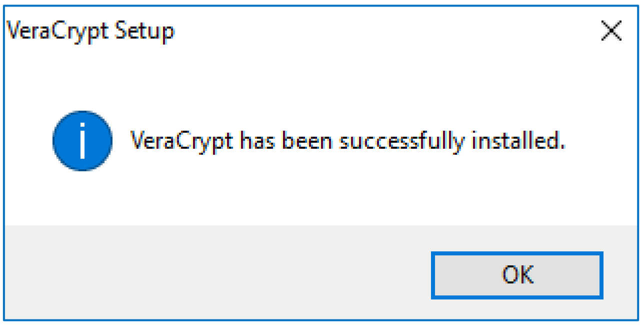
☑ Add VeraCrypt icon to desktop

☑ Associate the .hc file extension with VeraCrypt

☑ Create System Restore point

(Fig 6 – Select Default location)

Click **OK** (Fig 7) once the installation has completed.



VeraCrypt Setup

VeraCrypt has been successfully installed.

(Fig 7 – Instillation complete)

Once complete a Donation Page will pop up – Click ‘Finish’.

You will then be asked to read the VeraCrypt User Guide. You should read the Beginner’s Tutorial if this is your first time using VeraCrypt.

The Beginners Tutorial can be found at:
C:\Program Files\VeraCrypt\docs\html\en\Beginner's Tutorial.html (once instillation has completed and installed to the default location) or online at
https://www.veracrypt.fr/en/Beginner%27s%20Tutorial.html

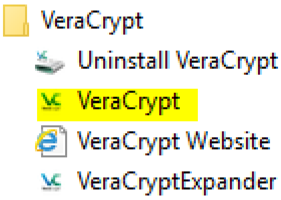
Now you will need to create a VeraCrypt Container to store your encrypted files.

2. How to Create a VeraCrypt Container

Step 1:

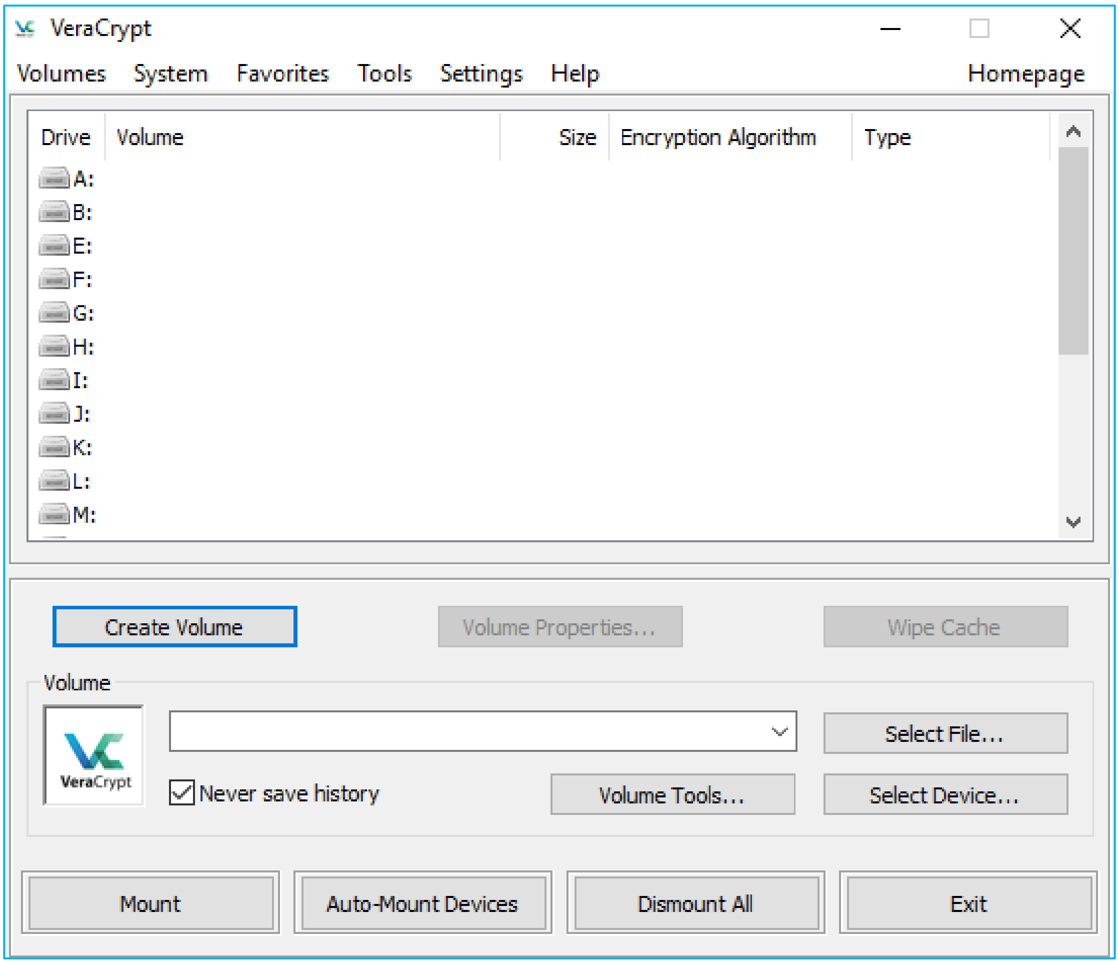
Open VeraCrypt by clicking on the VeraCrypt icon (Fig 8) located on your desktop or in your Windows Start Menu.

(Fig 8 – VeraCrypt)



Step 2:

The main VeraCrypt window (Fig 9) should appear. Click **Create Volume**



Drive	Volume	Size	Encryption Algorithm	Type
A:				
B:				
E:				
F:				
G:				
H:				
I:				
J:				
K:				
L:				
M:				

☑ Never save history

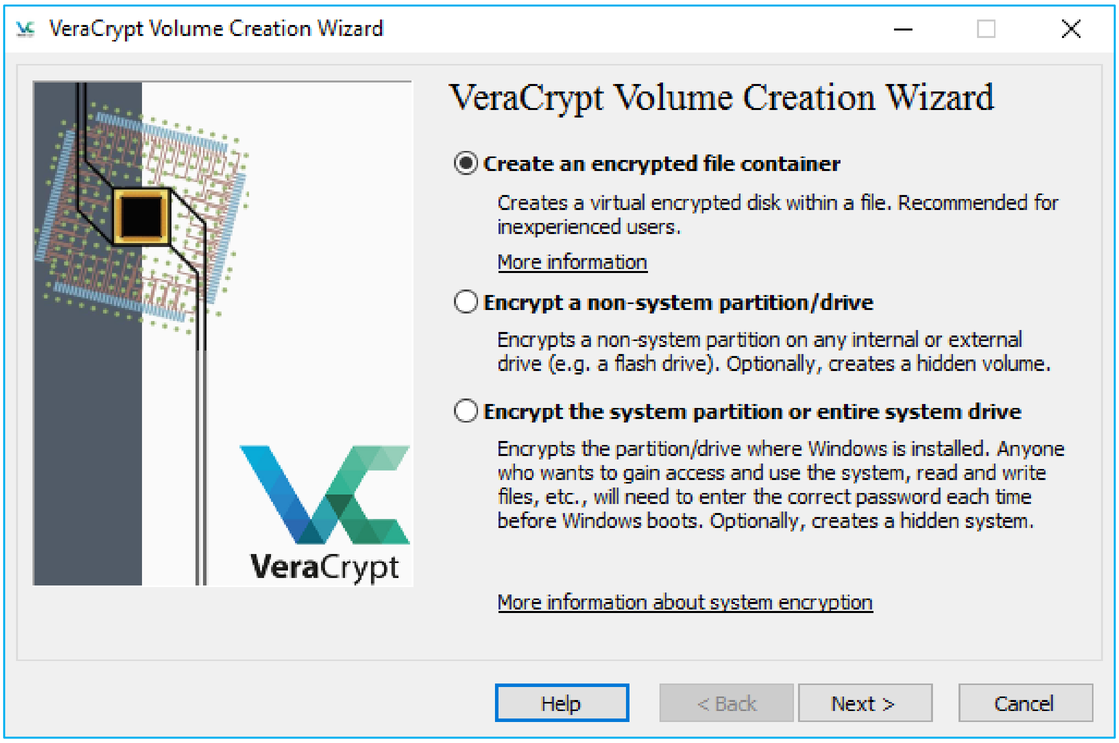
(Fig 9 - main VeraCrypt window)

Step 3:

The VeraCrypt Volume Creation Wizard window (Fig 10) should appear.

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**.



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.

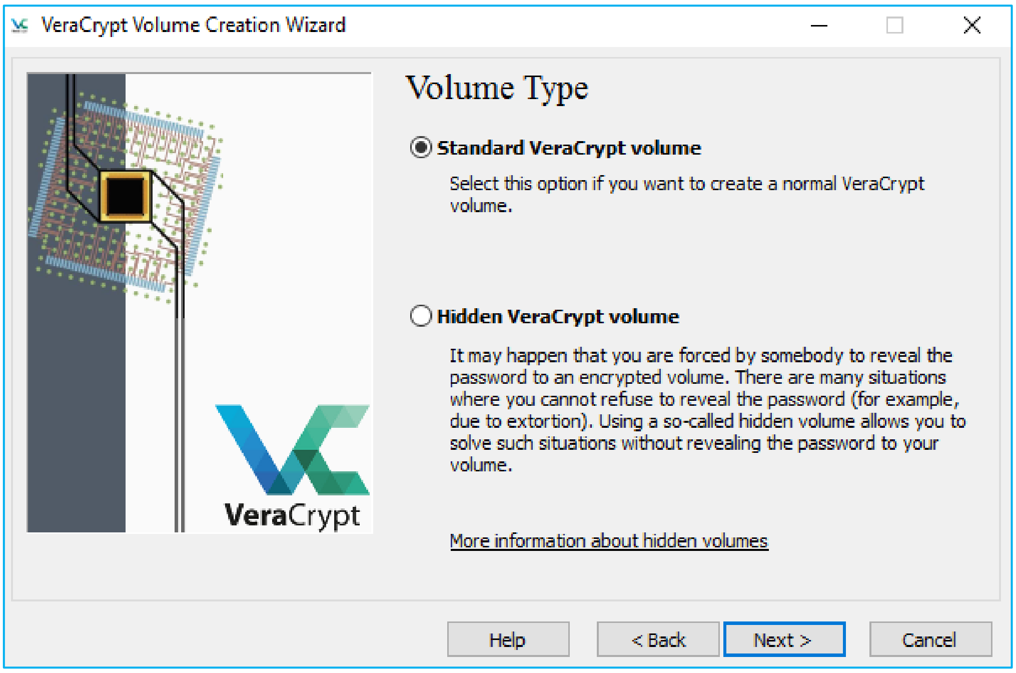
More information about system encryption

(Fig 10 - VeraCrypt Volume Creation Wizard window)

STEP 4:

In this step we will create a standard VeraCrypt volume (Fig 11).

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



Volume Type

● Standard VeraCrypt volume

Select this option if you want to create a normal VeraCrypt volume.

○ Hidden VeraCrypt volume

It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.

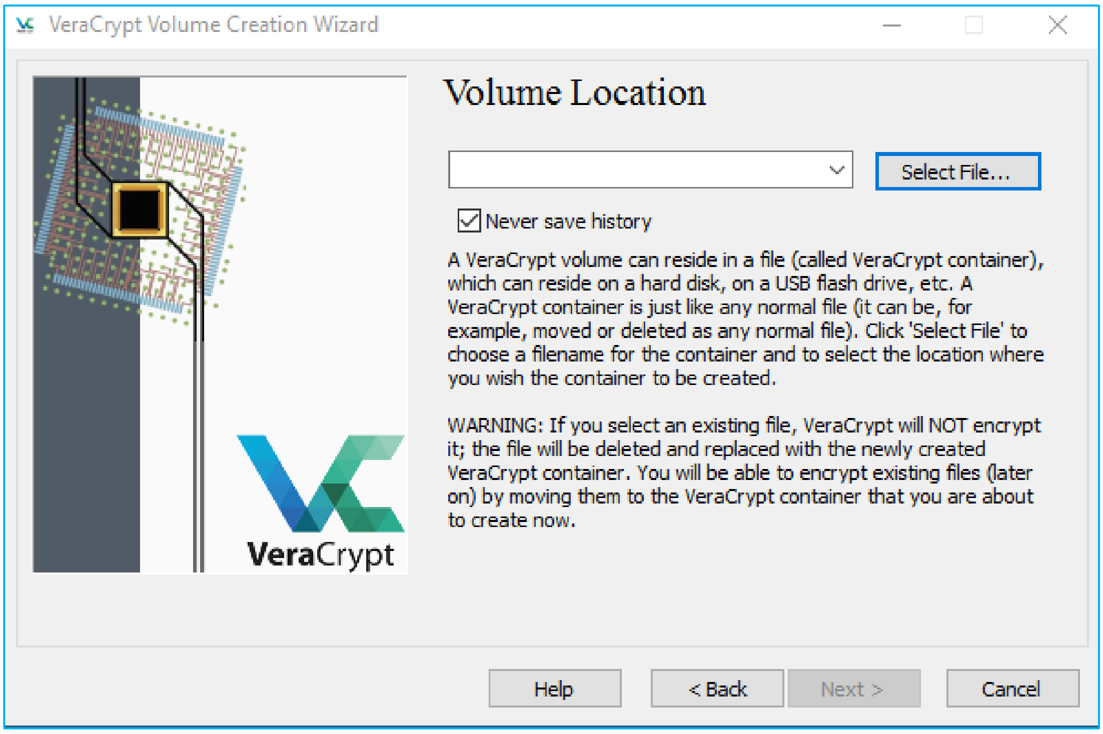
More information about hidden volumes

(Fig 11 – Create a standard VeraCrypt Volume)

Step 5:

In this step you have to specify where you wish the VeraCrypt volume (container) to be created (Fig 12). Note that a 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**.



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.

(Fig 12 – VeraCrypt Volume Location)

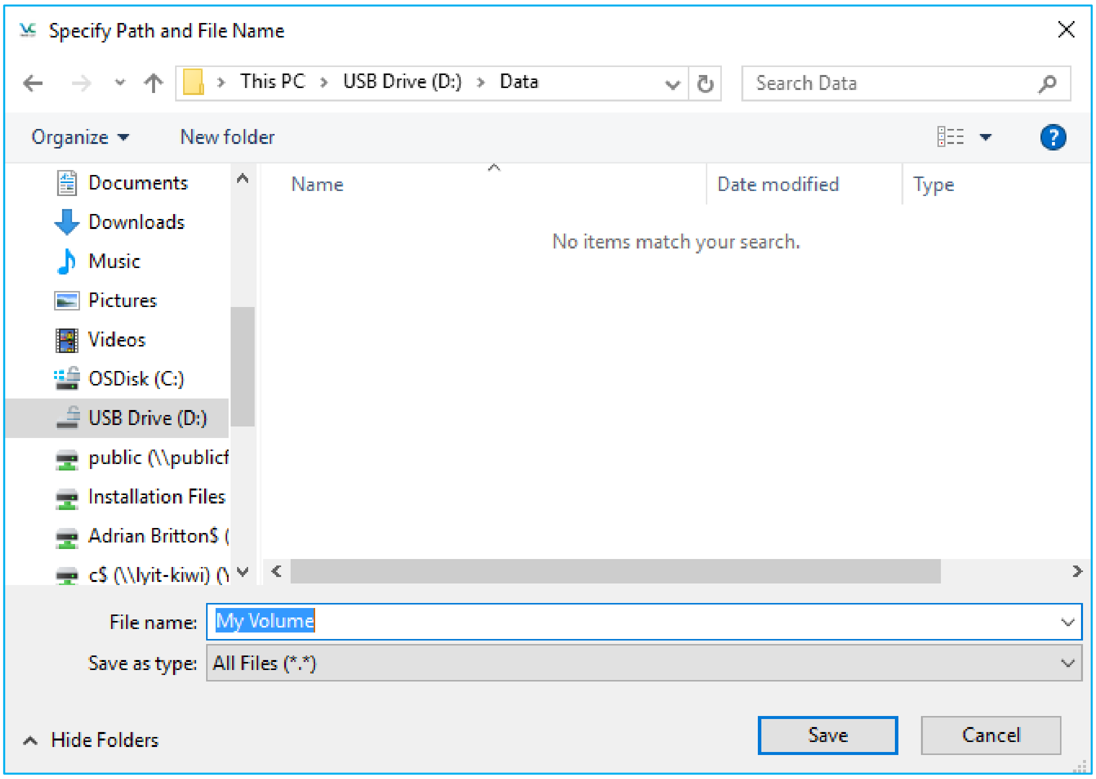
Step 6:

You now create your VeraCrypt volume (where your encrypted files will be stored) on your external drive and specify the filename of the volume (container) (Fig 13). (named *My Volume* in the screenshot below). You may, of course, choose any other filename and location you like. Note that the file *My Volume* does not exist yet – VeraCrypt will create it.

IMPORTANT: Note that 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 **File name:** box.

Click **Save**.



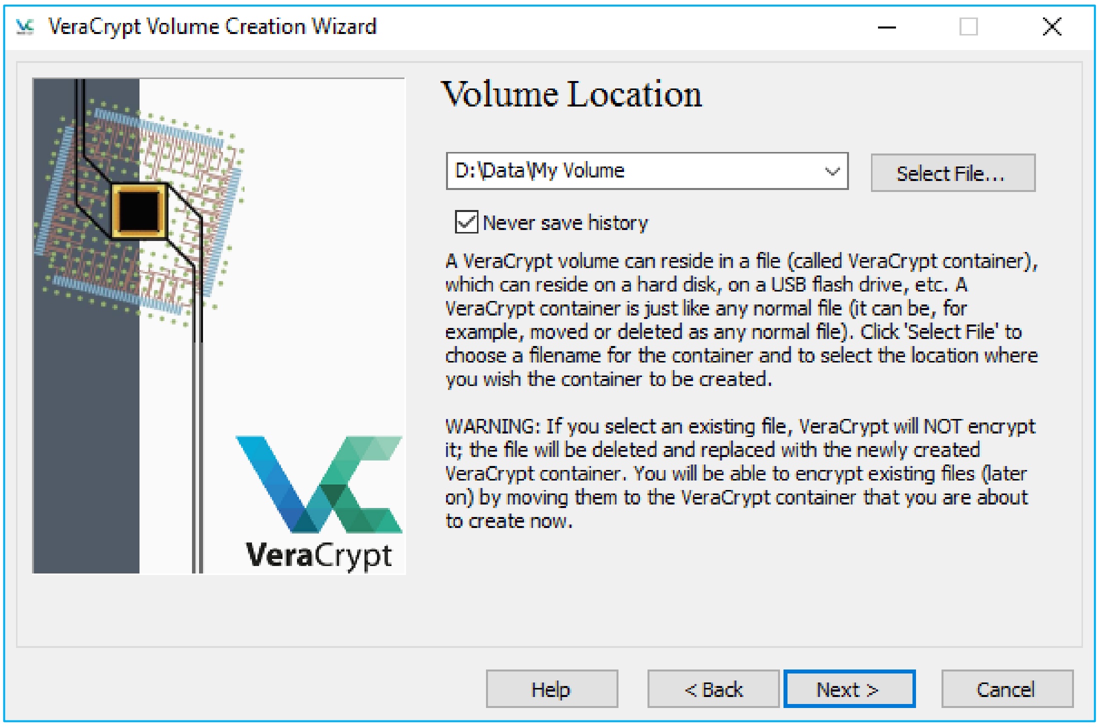
File name: My Volume

Save as type: All Files (*.*)

(Fig 13 – Specify Path and File Name)

STEP 7:

In the Volume Creation Wizard window (Fig 14), click **Next**.



Volume Location

D:\Data\My Volume

☑ Never save history

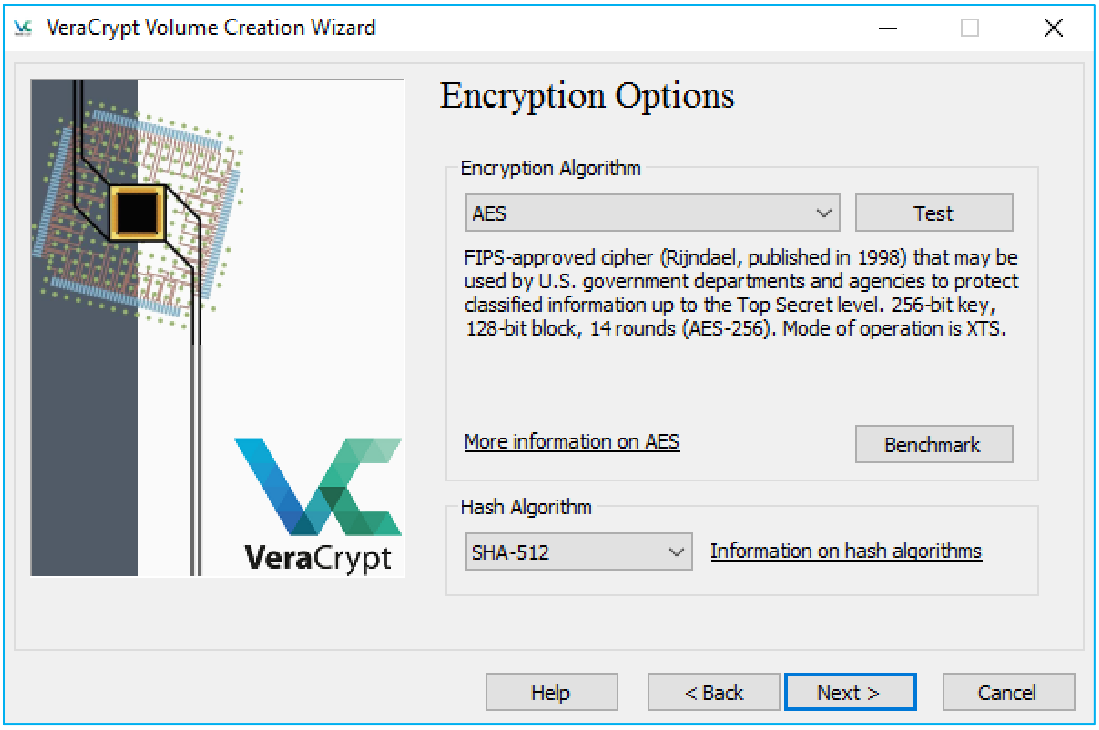
A VeraCrypt volume can reside in a file (called VeraCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A VeraCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Click 'Select File' to choose a filename for the container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

(Fig 14 – Volume Location)

STEP 8:

Here you can choose an encryption algorithm and a hash algorithm for the volume. If you are not sure what to select here, you can use the default settings and click **Next**.



VeraCrypt Volume Creation Wizard

Encryption Options

Encryption Algorithm: AES

FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.

More information on AES

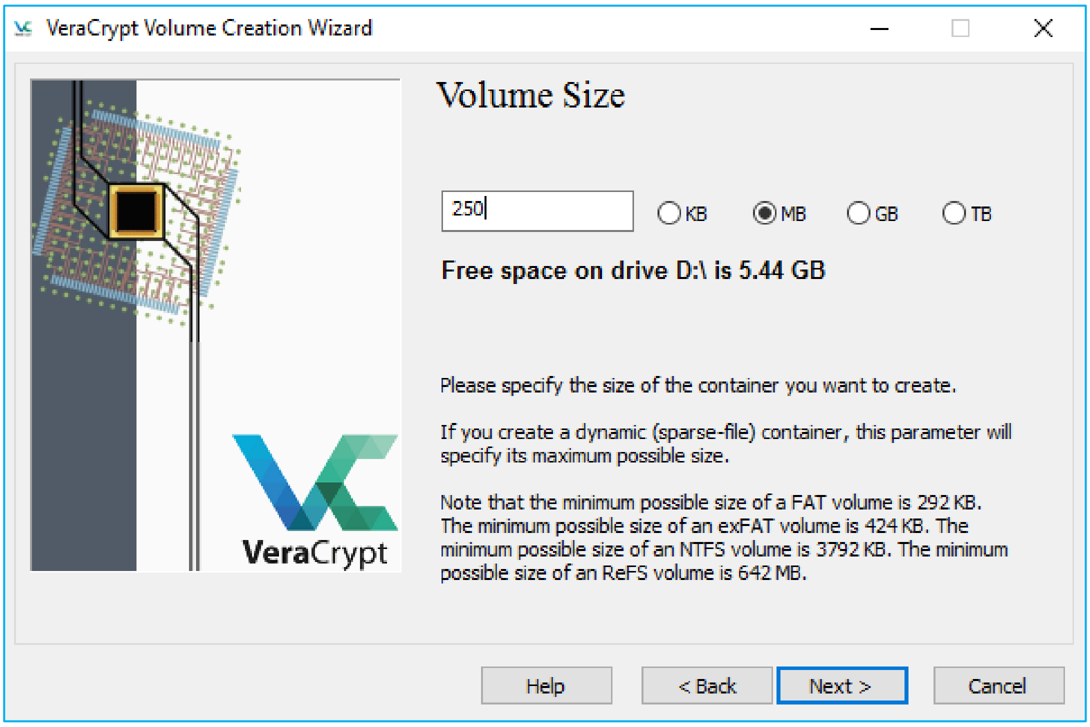
Hash Algorithm: SHA-512

Information on hash algorithms

(Fig 15 – Chose Encryption and Hash Algorithm)

STEP 9:

Specify the size of your VeraCrypt container. You may specify any size (up to the free space available). After you type the desired size in the input field (250MB in this example) click **Next**.



VeraCrypt Volume Creation Wizard

Volume Size

250 ○ KB ● MB ○ GB ○ TB

Free space on drive D:\ is 5.44 GB

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.

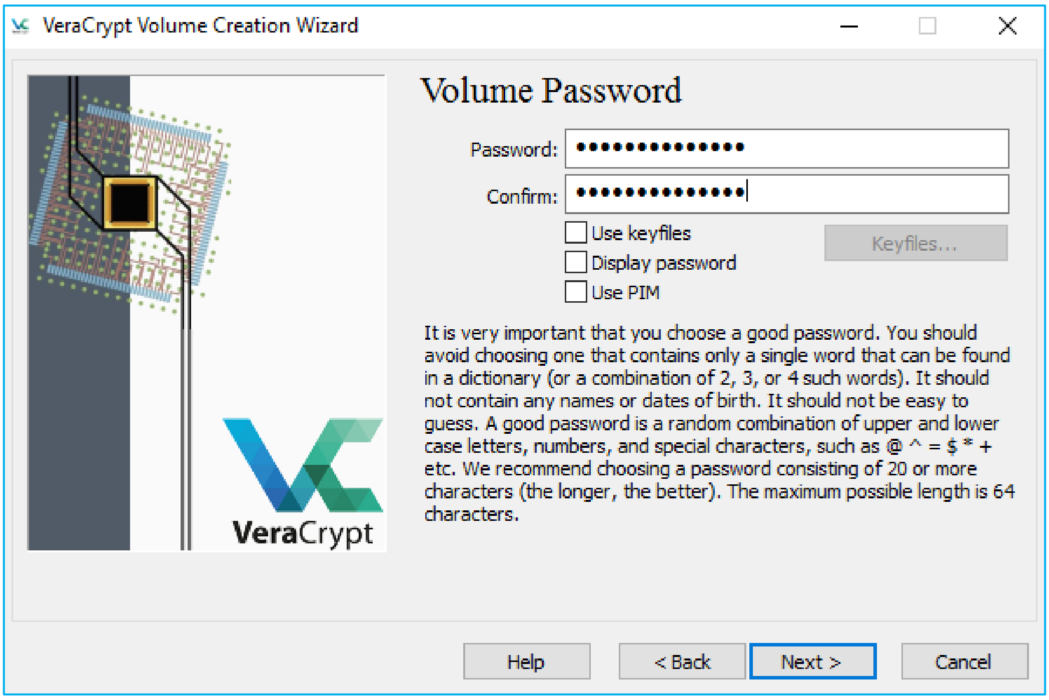
Note that the minimum possible size of a FAT volume is 292 KB. The minimum possible size of an exFAT volume is 424 KB. The minimum possible size of an NTFS volume is 3792 KB. The minimum possible size of an ReFS volume is 642 MB.

(Fig 16 – Specify the size of the encryption container)

STEP 10:

Choose a volume password. Read carefully the information displayed in the Wizard window about what is considered a good password.

Type your password in the Password field, then re-type it in the Confirm field. The **Next** button will be disabled until passwords in both input fields are the same.



VeraCrypt Volume Creation Wizard

Volume Password

Password: ••••••••••••••

Confirm: ••••••••••••••

□ Use keyfiles

□ Display password

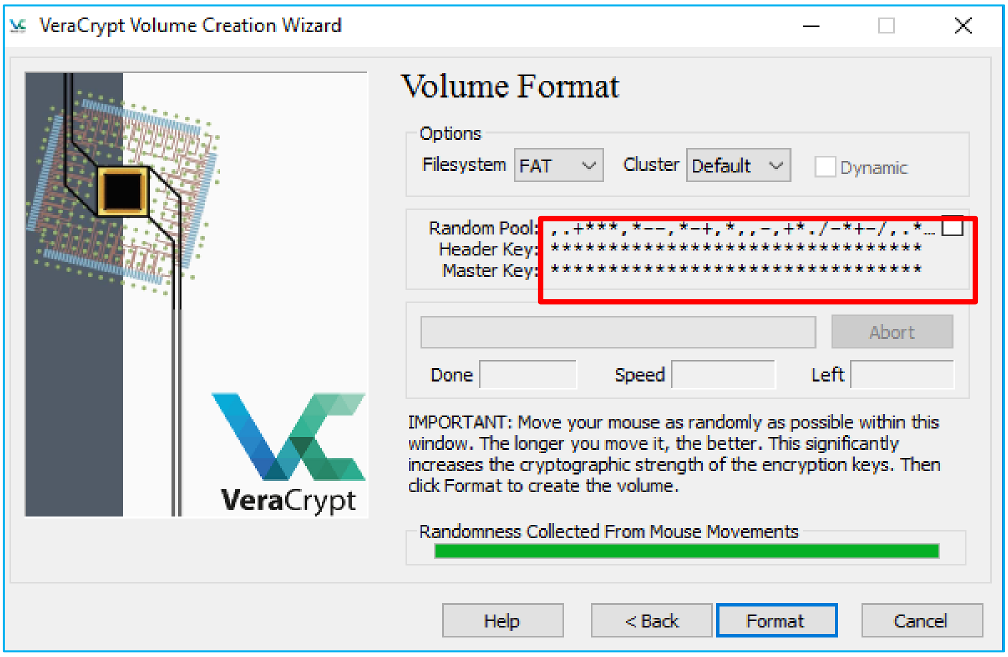
□ Use PIM

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 64 characters.

(Fig 17 – Create Password)

STEP 11:

Move your mouse randomly inside the Volume Creation Wizard window (inside the red square) 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).
Click **Format**.



VeraCrypt Volume Creation Wizard

Volume Format

Options

Filesystem: FAT

Cluster: Default

□ Dynamic

```
Random Pool: , . +***, *--, *-+, *, , -, +*. /-*+-/, . *...
 Header Key: ********************************
 Master Key: ********************************
```

Done

Speed

Left

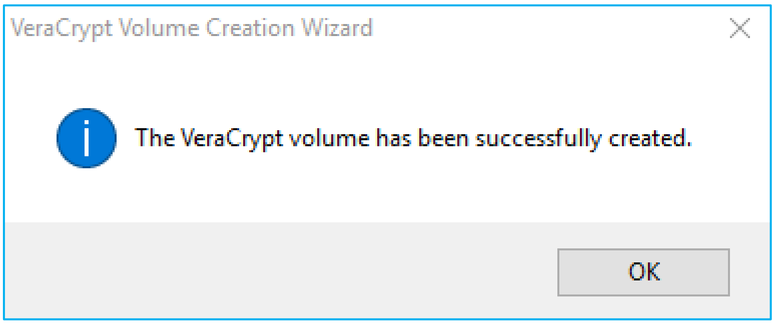
IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.

Randomness Collected From Mouse Movements

(Fig 18 – Randomness collected to specify encryption strength)

Volume creation should begin. VeraCrypt will now create a file called My Volume in the folder we specified in Step 6. This file will be a VeraCrypt container. Once it finishes, the following dialog box will appear:

Click **OK**



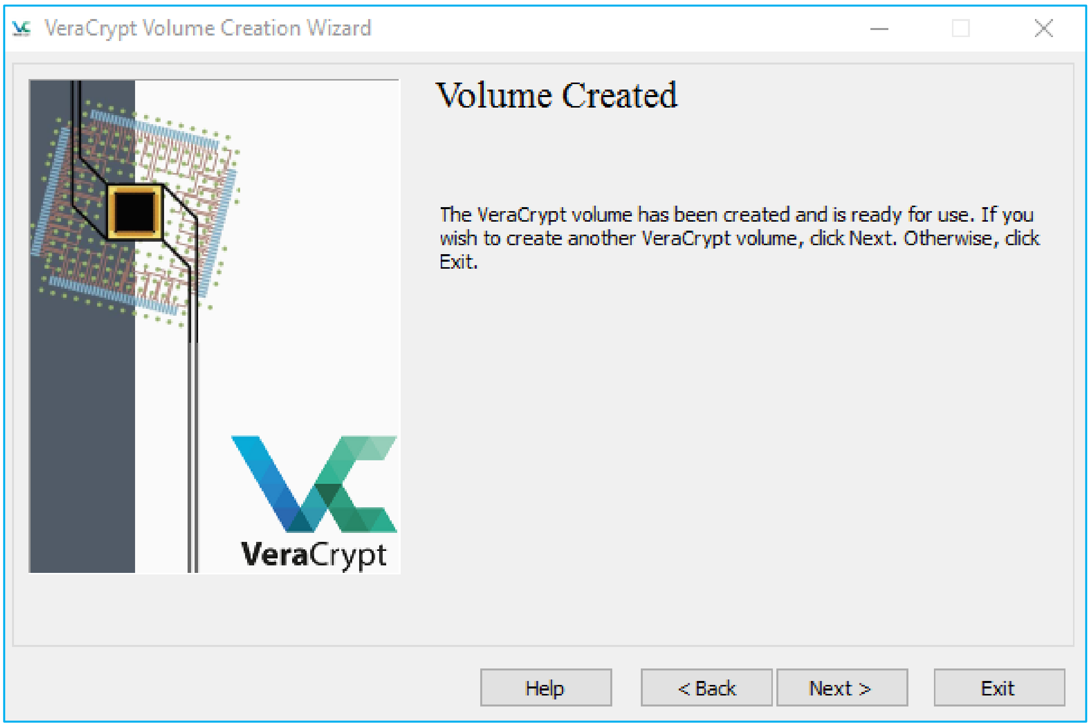
VeraCrypt Volume Creation Wizard

The VeraCrypt volume has been successfully created.

(Fig 19 – Volume Created)

STEP 12:

A VeraCrypt volume (file container) has successfully created. In the VeraCrypt Volume Creation Wizard window, click **Exit**.



VeraCrypt Volume Creation Wizard

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.

(Fig 20 – Volume Created – Exit the program)

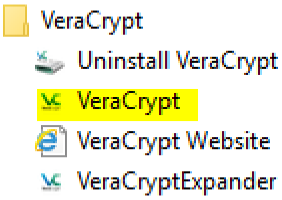
The Wizard window should disappear.

We have now created an encrypted container. To add or remove files to the container we will need to mount the container to use it as a normal drive.

3. How to mount the VeraCrypt container

Step 13:

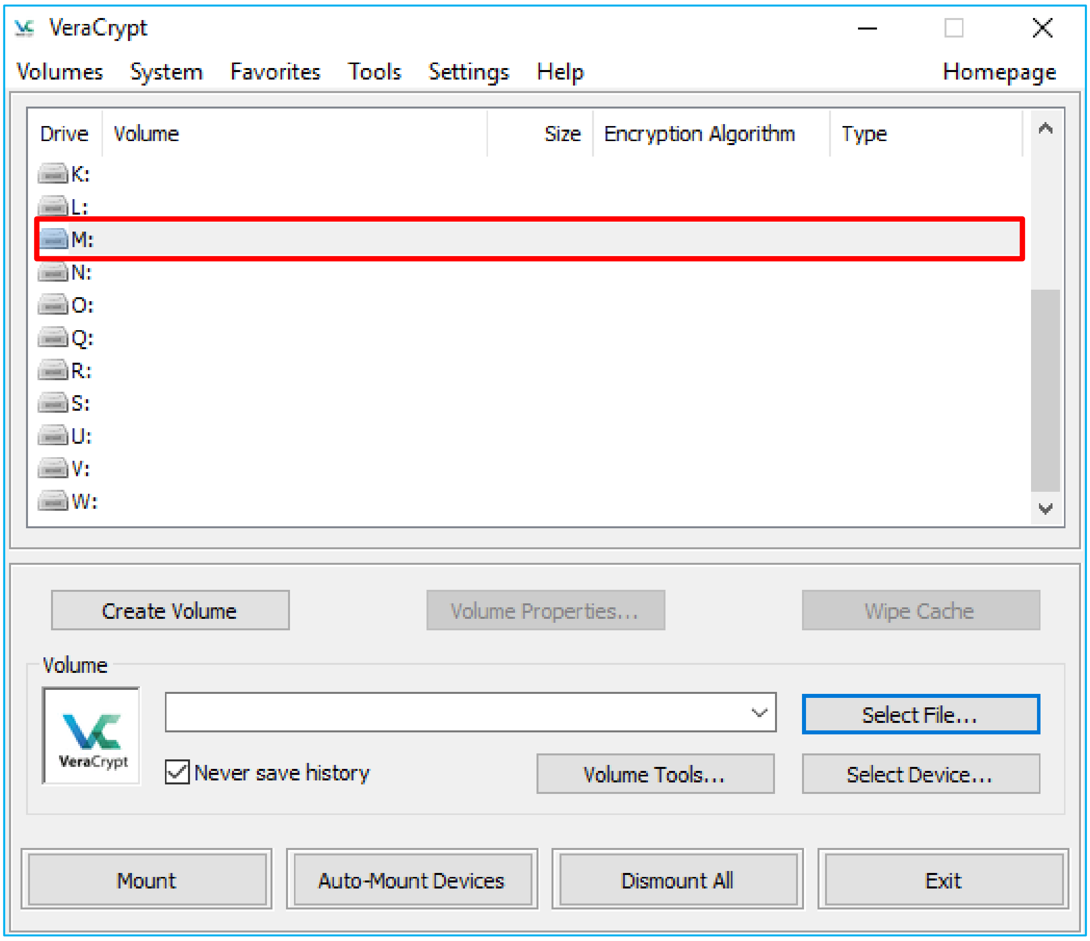
Open VeraCrypt by clicking on the VeraCrypt icon located on your desktop or in your Windows Start Menu.



STEP 14:

Select a drive letter from the list. This will be the drive letter to which the VeraCrypt container will be mounted. (You may choose any available drive letter)

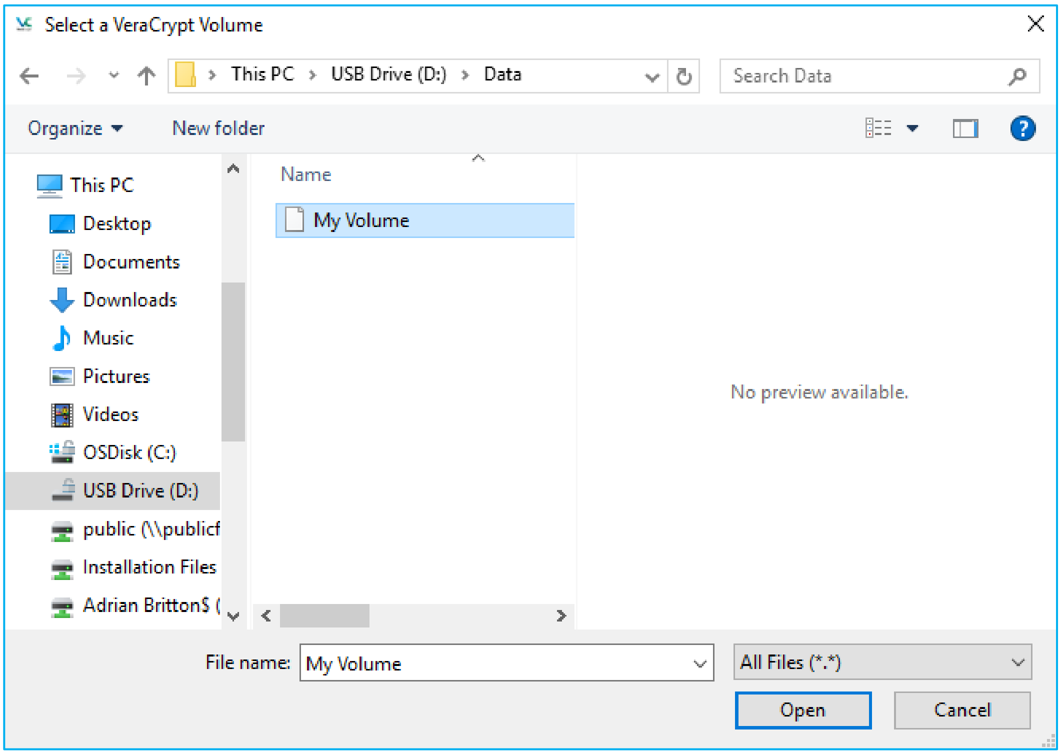
Click **Select File**



☑ Never save history

STEP 15:

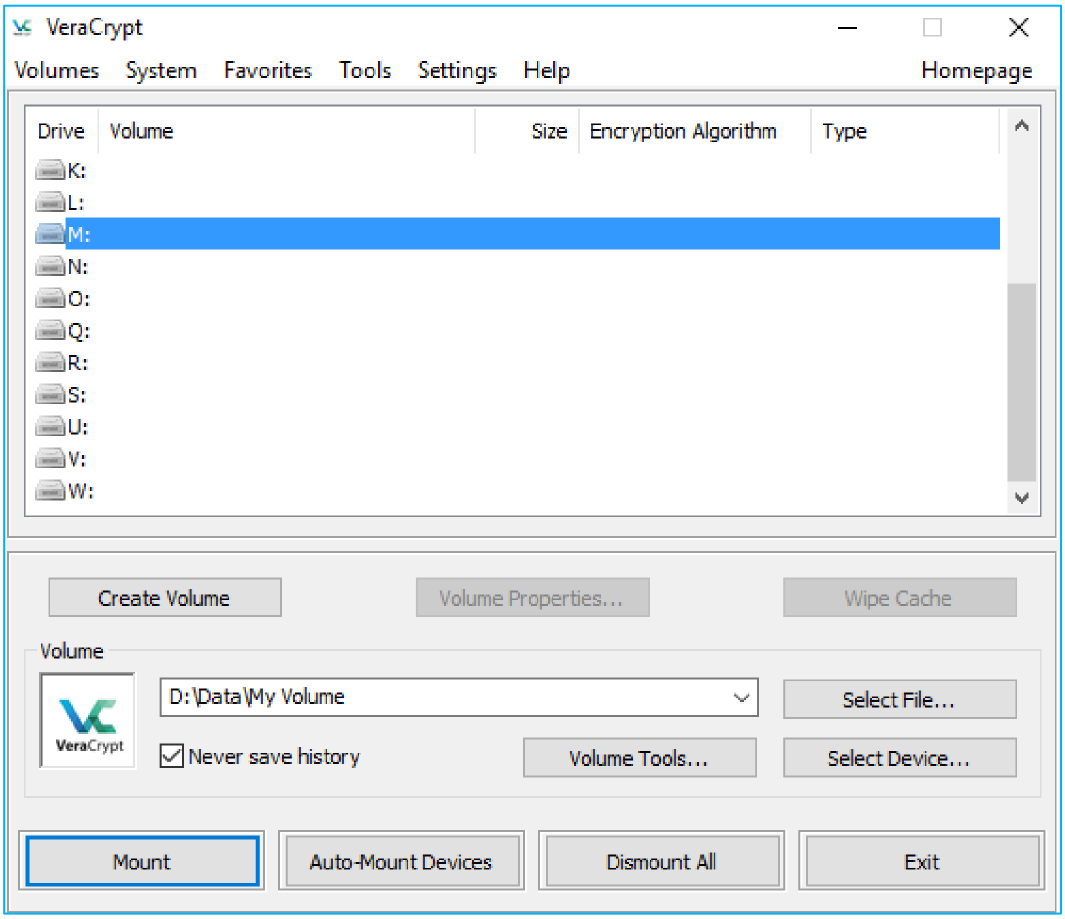
In the file selector, browse to the container file (which we created in Steps 6-12) and select it. Click **Open**.



File name: My Volume

STEP 16:

In the main VeraCrypt window, click **Mount**.

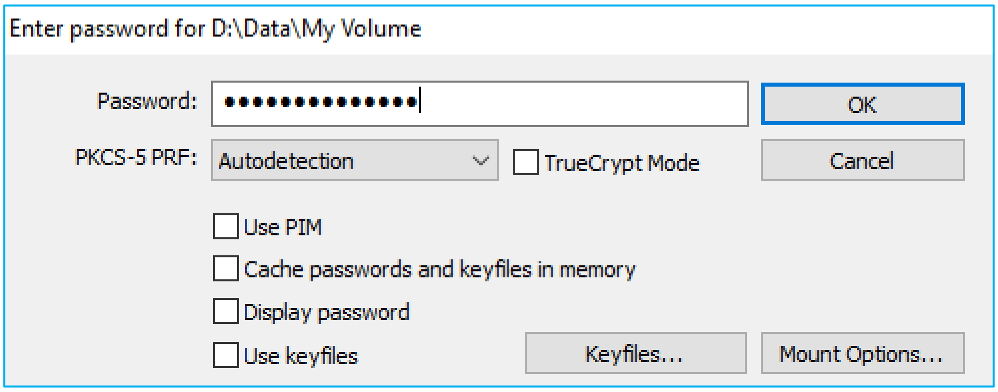


Volume: D:\Data\My Volume

☑ Never save history

STEP 18:

Enter your password (created in Step 10) and click **OK.**



Enter password for D:\Data\My Volume

Password: ••••••••••••••

PKCS-5 PRF: Autodetection

□ TrueCrypt Mode

□ Use PIM

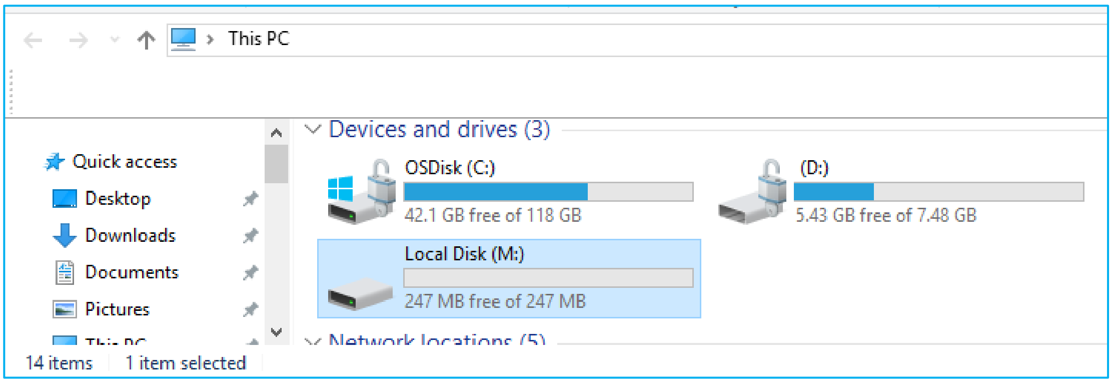
□ Cache passwords and keyfiles in memory

□ Display password

□ Use keyfiles

VeraCrypt will now attempt to mount the volume. This may take some time.
If this step fails, you may be required to repeat this step and reenter your password.

Once mounted, the container will appear as a virtual disk M:. It can be moved or deleted as any normal file.



Devices and drives (3)

OSDisk (C:) 42.1 GB free of 118 GB

(D:) 5.43 GB free of 7.48 GB

Local Disk (M:) 247 MB free of 247 MB

Network locations (5)

14 items 1 item selected

4. Add / Remove files to the encrypted drive

The virtual disk container 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 as they are being written.

You can copy files (or folders) to and from the VeraCrypt volume just as you would copy them to any normal disk (for example, by simple drag-and-drop operations).

If you open a file stored on a VeraCrypt volume, for example, in media player, the file will be automatically decrypted while it is being read.

Important: Note that 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.

If you want to close the volume and make files stored on it inaccessible, either restart your operating system or dismount the volume. The volume will have to be remounted (entering your password) to access the data on the volume again.

5. Protecting your encryption password / passphrase

Your password / passphrase is the only thing that stops a criminal from accessing the contents of your encrypted drive if it falls into the wrong hands.

Do not forget your password / passphrase. It is not possible for us to recover your data if you forget your password / passphrase.

6. Information security incidents

If you discover an incident that places sensitive or confidential information at risk, then you must notify the Computer Services Team through the Helpdesk by email (helpdesk@lyit.ie) or by telephone (0749186050).

7. Information Security checklist

Ref	**Requirement**	
1	Have you familiarised yourself with the prerequisites for using VeraCrypt?	
2	Have you downloaded and installed VeraCrypt?	
3	Do you know how to create a VeraCrypt container?	
4	Do you know how to mount the VeraCrypt container?	
5	Do you know how to add / remove files to the encrypted drive?	
6	Do you know how to protect your passphrase?	
7	Do you know how to report an information security incident?	
8	Have you read the Institutes Information Security and Data Protection Policies?	