ENCRYPTION FOR RESEARCHERS

UNIVERSITEIT GENT

CONTENTS

This document was produced in collaboration with the following services:

- the Research Department, University Library - Data Steward Team
- the Research Department, Research Co-ordination Office
- the Department of Information and Communication Technology
- the Department of Administrative Affairs.

I. WHAT IS ENCRYPTION?

Encryption is a method that makes data unreadable using certain algorithms. These algorithms use a password to encrypt the data. The password is needed to be able to read the encrypted data.

This prevents third parties from viewing the encrypted data. But it also means that if you no longer have the password, you can no longer access the data.

Security naturally depends on choosing a good password. So think carefully about the password you set. The following are tips for creating a strong password: (1) the longer the better (min. 10 characters), (2) combine letters, numbers and special characters, (3) make sure you can remember the password (for example, use a passphrase). For more tips on choosing a strong password, see https://www.safeonweb.be/nl/gebruik-sterke-wachtwoorden.

Also remember that encryption of data does not replace a good backup. Encryption does not protect against (accidental) deletion of data. So encrypted data still needs to be backed up properly.

II. WHEN TO ENCRYPT?

> Tip: It is better not to keep confidential data on a local device (laptop, USB stick, …), but only on the central disk space managed by the Department of Information and Communication Technology. If this is not possible, it is recommended to encrypt.

It is advised to encrypt any confidential[1] data you collect and store as part of your research. To determine whether encryption is needed, consider whether there is an increased risk that the data you want to keep confidential could be read by unauthorised persons and what the impact could be (in a worst-case scenario).

As a rule of thumb, if the data leaves the 'walls' of Ghent University, there is an increased risk. So if you want to share confidential data with others via the cloud, via filesender or by email, you must encrypt it. If you have confidential data on your laptop or on an external medium that you take home (e.g. USB stick), encryption is also recommended. Also be aware that when you have to log in with a password on your laptop, it does not necessarily mean that the data on the laptop is protected from unwanted glances. The login password protects access to your account, but does not make the data you have saved illegible. Someone who knows what they are doing can easily retrieve data from your laptop. This can only be avoided by using encryption software such as BitLocker (Windows) or FileVault2 (MacOS) (Also see Scenario 1 – Encrypting an entire laptop).

When the confidential data is on a Ghent University network drive, it is in principle not necessary to encrypt it. For highly sensitive data, however, it is recommended to take extra security measures and still use encryption.

[1] For a classification of confidential data, see https://www.ugent.be/intranet/nl/op-het-werk/ict/informatieveiligheid/classificatie-data.pdf

III. HOW TO ENCRYPT?

> Tip: Do you store confidential data on your Ghent University laptop? The easiest way to secure it is to encrypt with BitLocker (Windows).

There is a wide choice of encryption software. Before giving an overview it is important to briefly discuss how these applications work.

Volumes and containers

Simply put, specialised software packages use two methods of encryption: container encryption and volume encryption.

With *container encryption*, a kind of container or box is made and the files you want to encrypt are placed in it. This is similar to a zip file. This box is locked with an encryption key (e.g. a password) and made illegible. Since this 'box' is really nothing but a file, it has the properties of a regular file. You can move the container file (e.g. from your disk to a USB stick) and copy it, but you can also easily delete the file. Deleting it naturally also poses a danger. A good backup therefore remains important.

With *volume encryption*, the entire medium on which the data is stored is encrypted. In practice, this usually concerns an external hard drive, a USB stick or the system disk on which your operating system is located. In technical terms, these are often referred to as 'volumes', hence the name volume encryption. With this type of encryption, the encrypted files are permanently attached to the medium, to the hardware. At first sight, this is less flexible (you can't just copy the encrypted volume anywhere), but it also has advantages. For example, the risk of accidentally removing the volume is much smaller. This is also a more convenient way to encrypt large amounts of data.

In addition to specialised encryption software, there are also other ways to encrypt. Some compression programmes can also encrypt a zip file. It is also possible in most office software packages to protect and encrypt a file with a password.

Multiplatform?

Every modern operating system has the necessary tools to perform encryption. These are useful and work well as long as you are sure that the encrypted medium will never be used on any other operating system. In other words, these programmes do not work cross-platform and are therefore not appropriate in settings where collaboration and data sharing are common.

Tables 1 and 2 provide a simplified overview of the different types of encryption software. The examples in Table 1 are programmes only used for encrypting data. The examples in Table 2, on the other hand, are programmes that provide encryption in addition to their other primary function.

Table 1 - Specialised encryption software

Programme	Encryption by
Bitlocker (Windows)	Volume (system disks and USB)
FileVault 2 (MacOS)	Volume (system disks and USB)
VeraCrypt	Volume and container
Cryptomator	Container

Table 2 - Non-specialised software with encryption functionality

Programme	Encryption by
7-Zip	Container
SPSS	File
Office (Microsoft, LibreOffice)	File

The list is much longer than this (for an overview see https://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software).

Hardware solutions

If you often exchange USB sticks with confidential information, you can also buy copies with 'built-in' encryption. This works well, but is relatively expensive.

IV. SCENARIOS

Because the choice of the right encryption tool often depends on the situation and the purpose, we examine a number of scenarios in this how-to. Detailed examples for each scenario will follow.

Scenario 1 – Encrypting an entire laptop

Suppose you store confidential data on the hard drive of your laptop that you take with you everywhere.

In this scenario it is best to encrypt the system disk on which the data is stored. For this you can use the encryption software of your operating system (BitLocker for Windows, Filevault2 for MacOS, dm-crypt for Linux).

Let's go!

Scenario 2 – Encrypting one or a few files

Suppose you want to share 1 or a few confidential files with a colleague (via email, filesender, cloud).

If the software you use to edit the file provides encryption, it is a good choice to use it. The advantage is that you do not need extra programmes. For example, most office programmes (e.g. Microsoft Office, LibreOffice), but also SPSS offer the possibility to encrypt files with a password.

If the software in which you edit the file does not provide encryption or if you want to quickly group some files in an encrypted whole, you can use 7-zip. 7-zip is compression software that also allows you to encrypt the zip file you create. It is also freely available for all major operating systems (http://www.7-zip.org/) and is installed as standard on Ghent University computers.

You can then share the encrypted zip file with your colleague however you want (e.g. by email, filesender, cloud). Of course you also have to share the password with your colleague. A safe way to do this is by phone or text message.

Let's go!

Scenario 3 – Encrypting a project folder

Suppose you want to work dynamically (collaboratively) with confidential data. This means you want to be able to easily add, edit and delete files within a secure data repository. For this scenario, it is recommended to create an 'encrypted file container' with specialised software.

For example, in this scenario you can use VeraCrypt. VeraCrypt is freely available for all major operating systems (https://VeraCrypt.codeplex.com/).

Another application is Cryptomator (https://cryptomator.org/). This package has the added benefit of being optimised for use with cloud storage. In addition, mobile versions of the software are also available for use on your smartphone and tablet. The mobile versions are not free.

Let's go!

Scenario 4 – Encrypting external devices

Suppose you have a large amount of data that you want to keep safe for yourself on an external hard drive or USB stick.

In this scenario, it is recommended to encrypt the entire disk with BitLocker (if you are using Windows) or Filevault2 (if you are using MacOS). If you want to be able to use the encrypted external hard drive on operating systems other than yours, you should opt for multiplatform software such as VeraCrypt.

Important! With long-term storage, it is important not to forget the password. Use a strong[2] password and keep it in a safe place. Also make sure that others who need to have access to the data later (e.g. your supervisor) also have the password. You can also store passwords in a password manager such as KeepassXC.

Let's go!

V. LET'S GO

Scenario 1 – Encrypting an entire laptop

If you keep confidential data on your laptop and you also use that laptop externally (i.e. outside Ghent University), it is strongly recommended to encrypt the hard drive. This can be done in most cases with tools that come with the operating system you use. For Windows this is BitLocker and for MacOS this is FileVault2.

Encryption of the system disk in Windows with BitLocker

Before you get started, it is important to check the following items.

- BitLocker is only available for the 'professional' editions of Windows (Enterprise, Ultimate). This is normally not a problem for laptops that have been provided by Ghent University, but for laptops purchased externally, this may be different because they often have the "lightest" Home edition installed.
- To encrypt your system disk you also need to work with a modern device that has a Trusted Platform Module (TPM). This is a special encryption chip installed in your laptop that is used to encrypt your system disk. If you don't have a TPM, you will be notified when activating BitLocker.

> Tip: When purchasing your laptop, check whether your PC is equipped with a Trusted Platform Module, and ensure that a professional version of Windows has been installed. In case of doubt, contact the Department of Information and Communication Technology helpdesk.

[2] http://helpdesk.ugent.be/account/wachtwoord.php

Find out how to check whether you have a TPM chip in your computer at the following website:
https://www.howtogeek.com/287737/how-to-check-if-your-computer-has-a-trusted-platform-module-tpm-chip/

The following website is a good guide on how to setup BitLocker on a Windows PC:
http://www.howtogeek.com/192894/how-to-set-up-bitlocker-encryption-on-windows/

For a full, highly technical explanation, you can also see:
https://technet.microsoft.com/en-us/library/c61f2a12-8ae6-4957-b031-97b4d762cf31

Encryption of the system disk in MacOS with FileVault 2

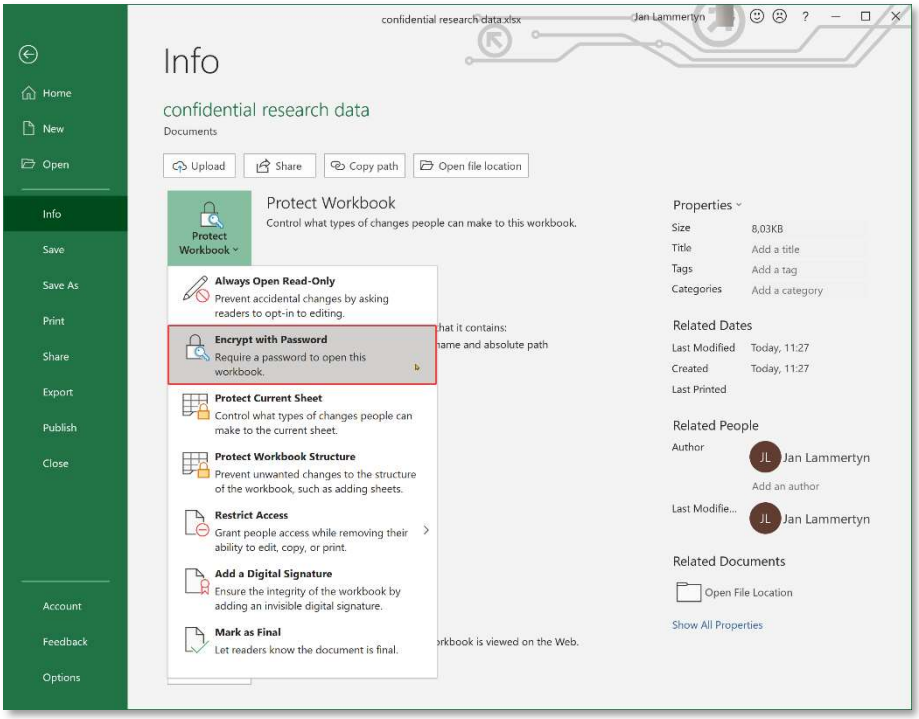
On the Apple website you will find a good manual on how to use FileVault 2 and encrypt your system disk:
https://support.apple.com/en-us/HT204837

Scenario 2 – Encrypting one or a few files

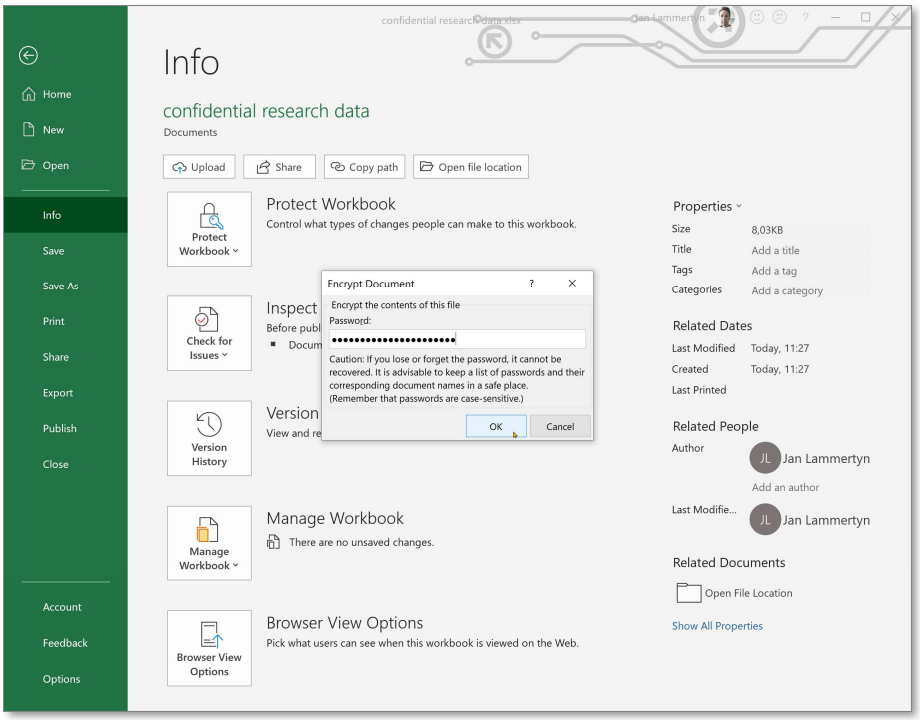
If you want to quickly encrypt one or a few files because you want to share them with a colleague, for example, in some cases you can use the software you use to edit the data (e.g. SPSS). If the software you use to edit the data files does not have this option, it is best to use 7-zip. Below we first go through some examples of software with built-in encryption. Then we discuss encryption with 7-zip.

Encryption with Microsoft Office

For example, to encrypt files with Microsoft Excel, go to the 'File' menu. Then select 'Protect Workbook' and then 'Encrypt with Password'.



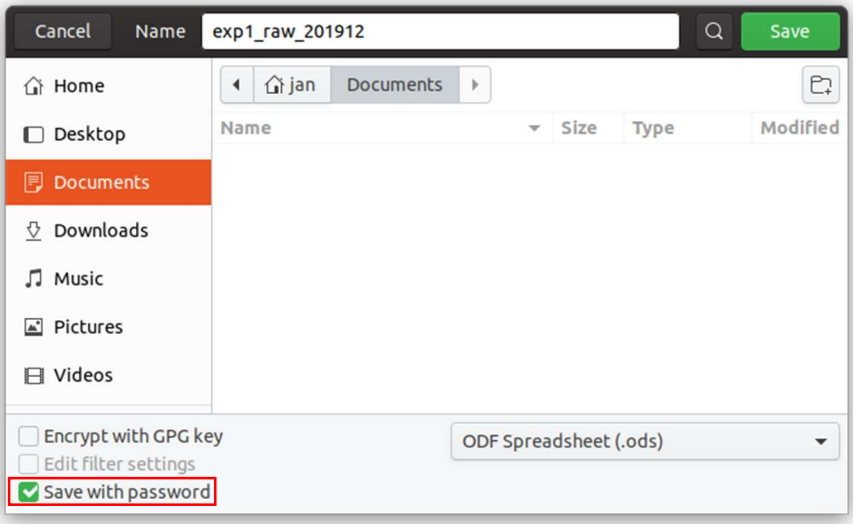
Then you enter a password.



Once the password has been entered, you still have to save the document. From that moment on, your file is protected. The next time you open the document you will be asked for the password.

Encryption with LibreOffice

For example, to encrypt files with LibreOffice Calc, save the file. In the save window select 'Save with password'.

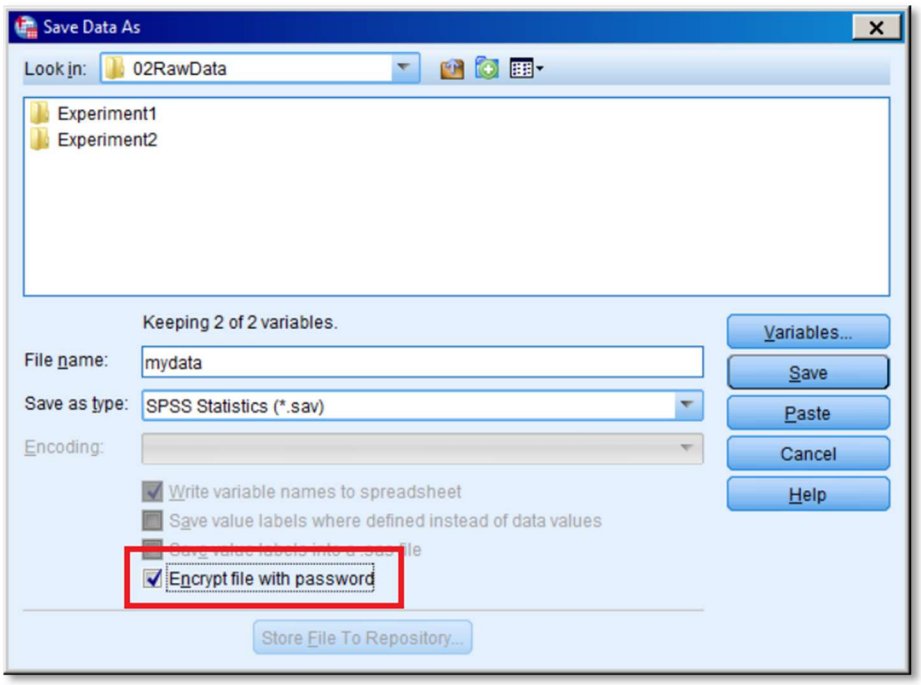


Then you enter a password.

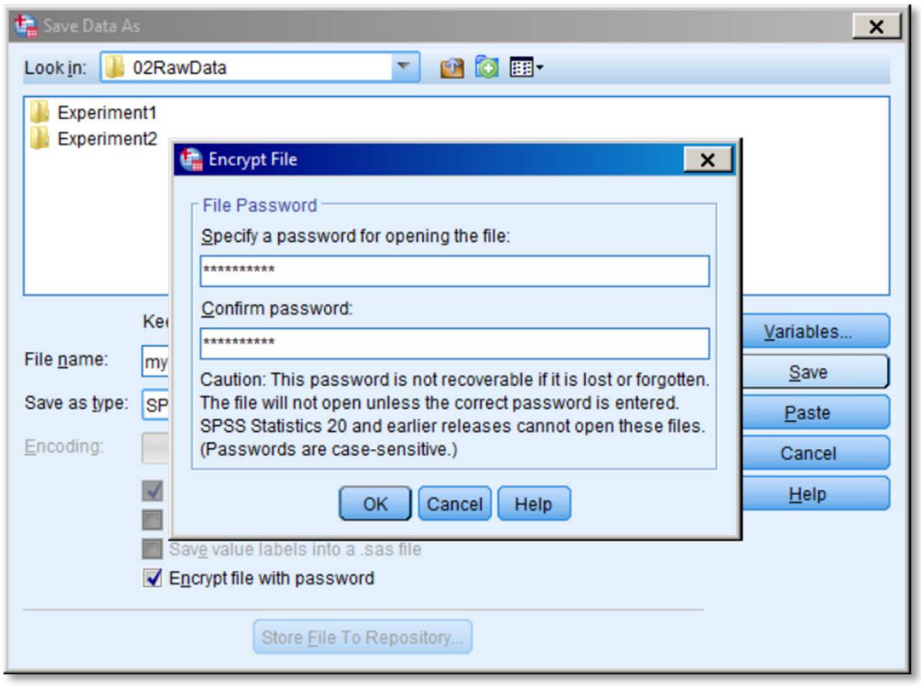
Once the password has been entered, the file is saved in encrypted form. The next time you open the document you will be asked for the password.

Encryption with SPSS

Save the file to encrypt SPSS files. In the save window select 'Encrypt file with password'.



Then you enter a password.



Once the password has been entered, the file is saved in encrypted form. The next time you open the document you will be asked for the password.

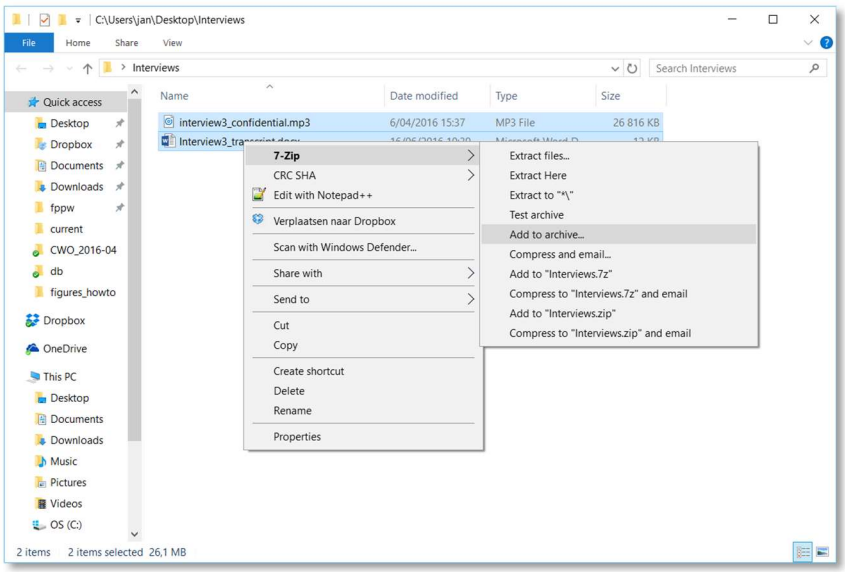
Encryption with 7-zip

7-zip is installed as standard on computers provided by Ghent University. If 7-zip is not already on your computer, go to http://www.7-zip.org to download the installation files. In this example we use the version for Windows.

Suppose you have some files that you want to put in an encrypted zip file.

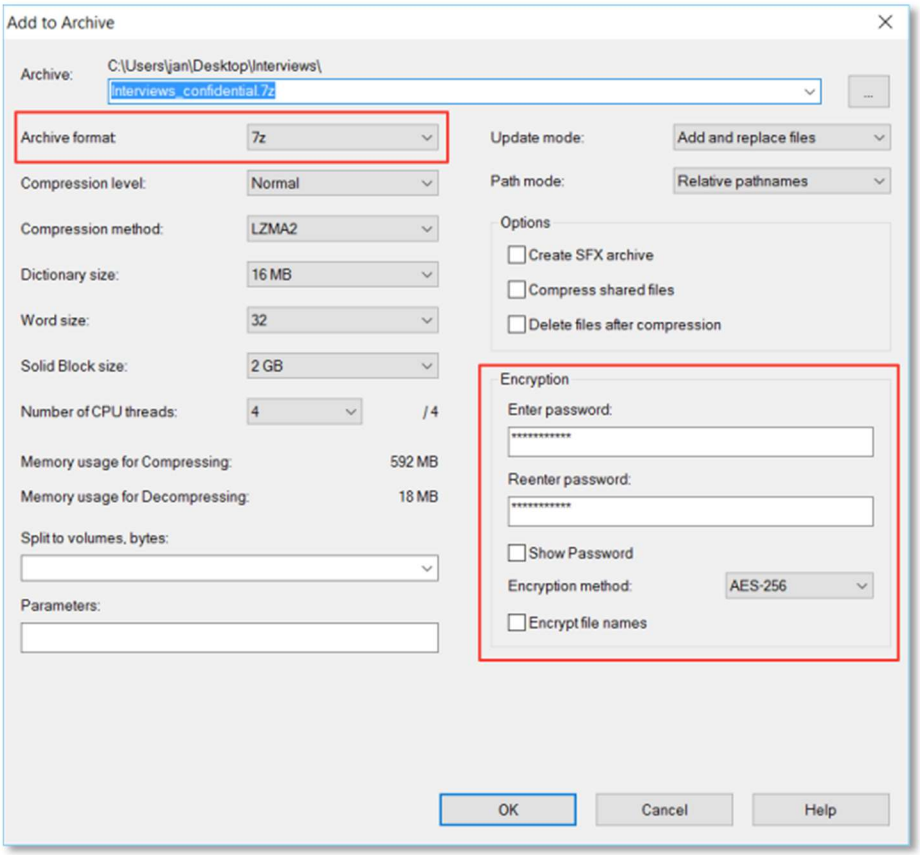
Step 1

Go to the folder where the files are located. Select the files and right-click. If the installation of 7-zip was successful, select '7-Zip' in the context menu and then 'Add to archive…'.



Step 2

You will see the following window



Make sure the 'Archive format' is set to 7z and leave the 'Encryption method' at AES-256. Once you have given an appropriate name to the zip file, you can enter a password. If you also want to make the names of the files in the zip file unreadable, select 'Encrypt file names'. This is only recommended if the file names themselves contain confidential information. Press 'OK' and the encrypted file will be created.

If you share this zip file with others, they will also need to install 7-zip to extract the files.

See how to create encrypted 7-zip files on MacOS and Linux at http://www.howtogeek.com/203590/how-to-create-secure-encrypted-zip-or-7z-archives-on-any-operating-system/.

Scenario 3 – Encrypting a project folder

In this dynamic scenario, we want to create a safe place where we can easily add and edit files. We do this by creating an 'encrypted file container'. This container can be easily shared, e.g. via the cloud[3].

Folders can be encrypted in different ways and with different software packages. We first go through how to use Cryptomator for this. We will then go deeper into the use of VeraCrypt.

[3] See also point 8 in Tips for working safely with IT tools

Cryptomator

In this example we are using the Windows version of Cryptomator. You can find the installation file for this encryption software at https://cryptomator.org under 'Download'.

In Cryptomator, the 'encrypted file container' is called a vault. This vault is actually a normal folder that serves as a secure 'safe' to store other files. Because the safe is a folder, it also means that you can use it just like a normal folder. This is very flexible: you can copy, move and rename the folder. However, there are hazards that you should take into account: you can easily delete the folder, for example.

We will first go through how to create a new vault. Then we will go deeper into daily use. In summary, you use Cryptomator as follows:

Preparation (only once):

1. Start Cryptomator
2. Choose location and name for vault
3. Set Password

At each use:

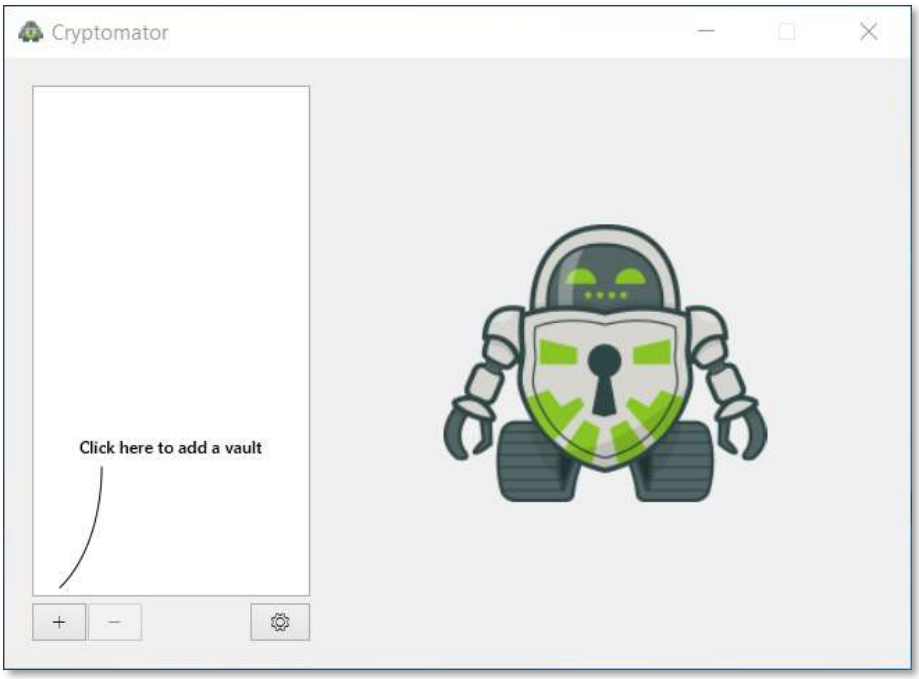
1. Start Cryptomator
2. Select and open Vault (Unlock)
3. Work
4. Close Vault (Lock)

Creating a new vault

Creating a vault is quite easy. In short, you have to choose where you want to place the vault and what it should be called. Then you also choose a password.

Let's go through the process step by step:

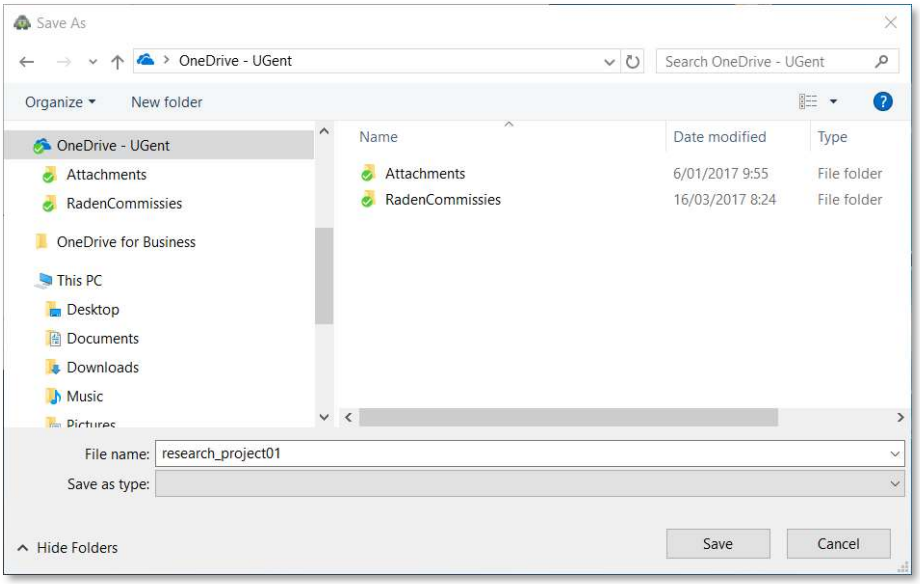
Step 1 – Open Cryptomator
First open Cryptomator. You will see the following screen.



To start, press '+' and select 'create new vault' to create a new vault.

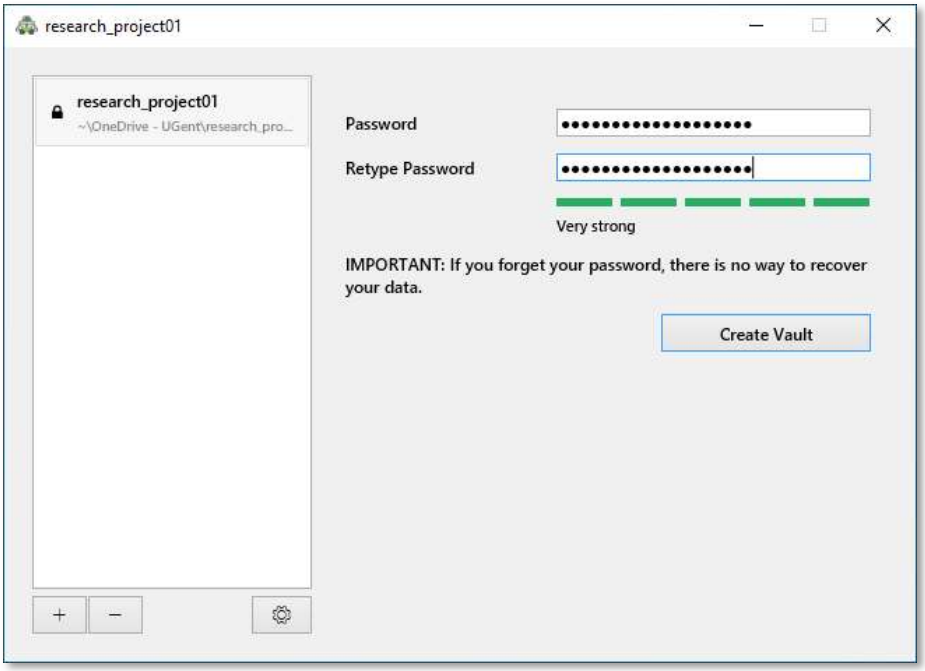
Step 2 – Choose location and name

In this example we want to create a new vault, so we select a location (here the OneDrive for Business folder) and choose an appropriate name (in the example 'research_project01'). Once you have done this, press save.



Step 3 – Set password

Once the location and name have been chosen, your vault will appear on the left in the selection window. Now you choose a strong password. Then press 'Create Vault' to create the safe.



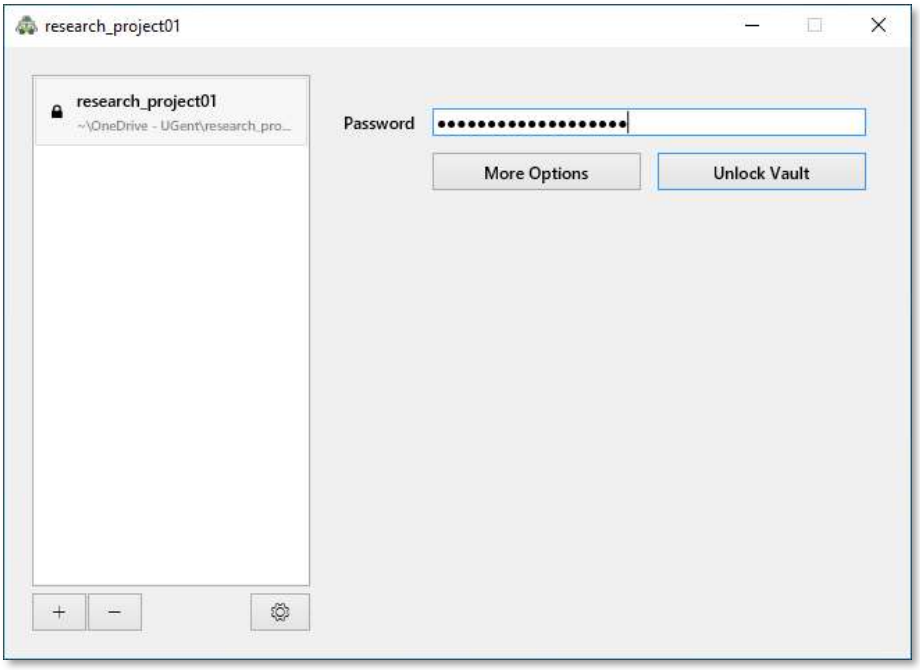
Using a vault on your PC

The procedure for using a vault is always the same. You always start by opening your vault in Cryptomator and you always close the safe again at the end. We will describe this in detail later.

To make the vault convenient to use, Cryptomator mounts it on a virtual disk. When the vault is mounted it looks like you have an extra disk on your computer. You can work on it just like on a normal disk. This also means that as long as this 'virtual' drive remains mounted, its contents are available to anyone who has access to your computer. Once you have finished working on the virtual disk you need to unmount it ('Lock vault'). If you forget this, the contents of the vault will remain accessible to anyone who has access to your computer until you turn your computer off.

Step 1 – Opening a Vault

Once you have opened Cryptomator, the first step is to open your vault. Do this by selecting the vault you want to open. Then enter the password and press 'Unlock vault'.



Note: If you want to open a vault that you have never used before on the computer you are working with, you will not see that vault in the list of available vaults (the left part of the window). This may happen, for example, if you have created a vault with your desktop PC on OneDrive and you want to open it on your laptop.

To add an existing vault to the selection list in Cryptomator, press + and select 'Open existing vault'. Then look for the folder containing the vault you want to open. That folder contains a file with the '.cryptomator' extension. If you select and open this file, the vault will be added to your list of available vaults.

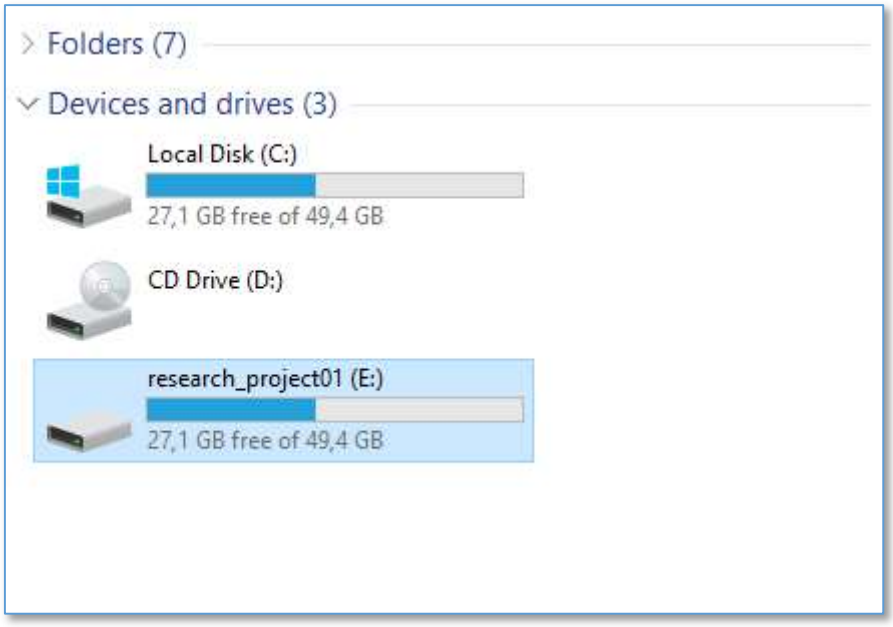
Once this is done, the vault will be opened and mounted on your system. If you want you can now reduce the Cryptomator programme window.

In this step there are also some additional options under 'more options'. The main ones are:

- *Drive Name:* Do you want the drive being created to have a different name than the name of your vault? Then you can set that here.
- *Save password:* do you want to not have to enter your password every time? Then you can also let Cryptomator store the password. This is not recommended.
- *Auto-Unlock on Start:* This option automatically mounts the selected vault when Windows starts. This is not recommended.
- *Custom Drive letter:* Do you not want Cryptomator to automatically choose a drive letter to mount the virtual disk? Then you can set here which drive letter should be used each time.

Step 2 – Use

You can now simply save files to this virtual disk via Windows Explorer as you would with a normal disk. Note that the capacity of the virtual disk is the same as the physical hard drive on which you created it. In this case, this is the C:/ drive because OneDrive stores a local copy of its files there.



Step 3 – Unmounting

Once you have completed the previous steps, you must close the vault. You need to do this because people who have access to your computer also have access to the mounted vault.

Proceed as follows: in Cryptomator select the disk you want to unmount and then press 'Lock vault'. After that, the virtual disk will be unmounted and it will disappear from your system. The contents of the vault will now not be accessible and a folder with (unreadable) encrypted files will remain.

VeraCrypt

First we go through how to create an 'encrypted file container' with VeraCrypt. We will then go deeper into the daily use of such a container.

In this example we are using the Windows version of VeraCrypt. You can find the installation file for this encryption software at https://www.veracrypt.fr.

In summary, VeraCrypt is used as follows:

Preparation (only once):

1. Open VeraCrypt
2. Create volume (encrypted file container)
3. Set Password

At each use:

1. Open VeraCrypt
2. Select encrypted container and mount to drive letter.
3. Work
4. Select encrypted container and unmount ('Dismount').
5. Exit VeraCrypt

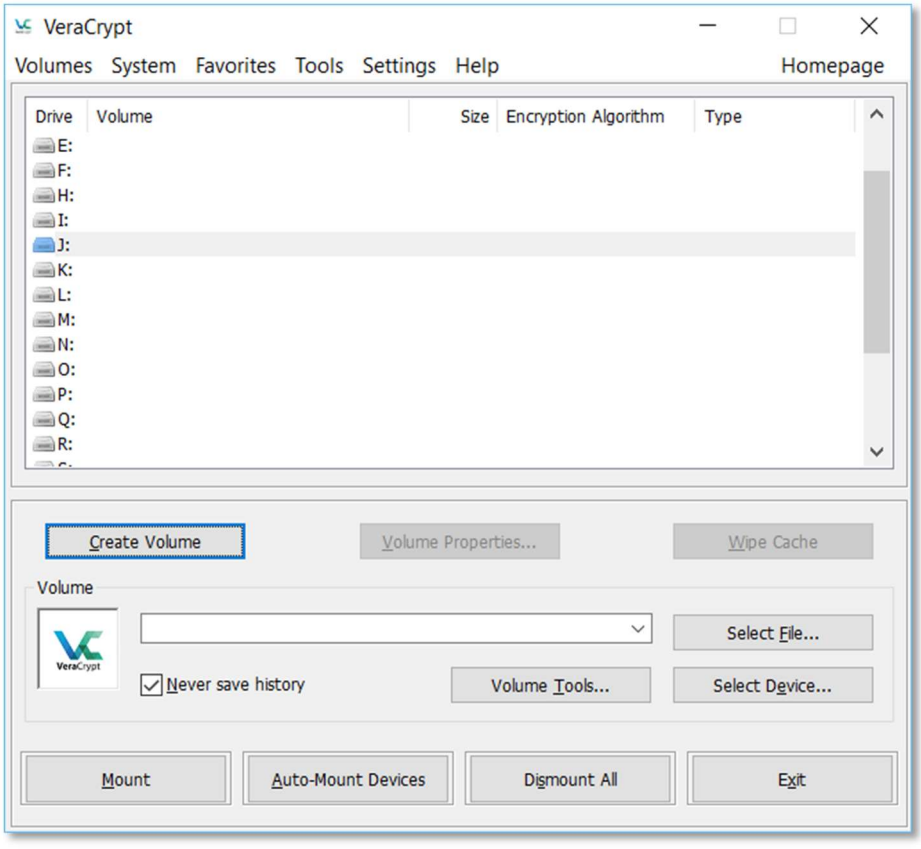
Creating an encrypted file container

An 'encrypted file container' is a file that serves as a secure 'box' to store other files. Because the result is a file, it also means that you can use it just like a normal file. This is very flexible: you can copy, move and rename the container. There are also hazards that you should take into account: you can easily delete the container.

Creating an 'encrypted file container' looks complicated due to the number of steps required, but the default settings are usually followed. In short, you have to choose where you want to place the 'encrypted file container', what it should be called and how big it should be. Then you also choose a password.

We now go through the process step by step:

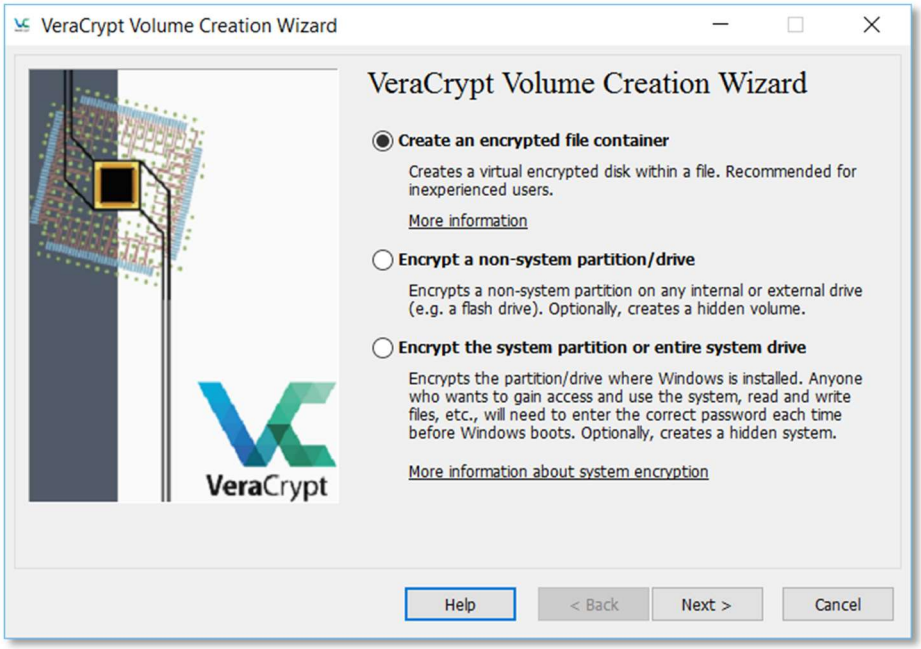
Step 1
First open VeraCrypt. You will see the following screen.



To start, press 'Create Volume'.

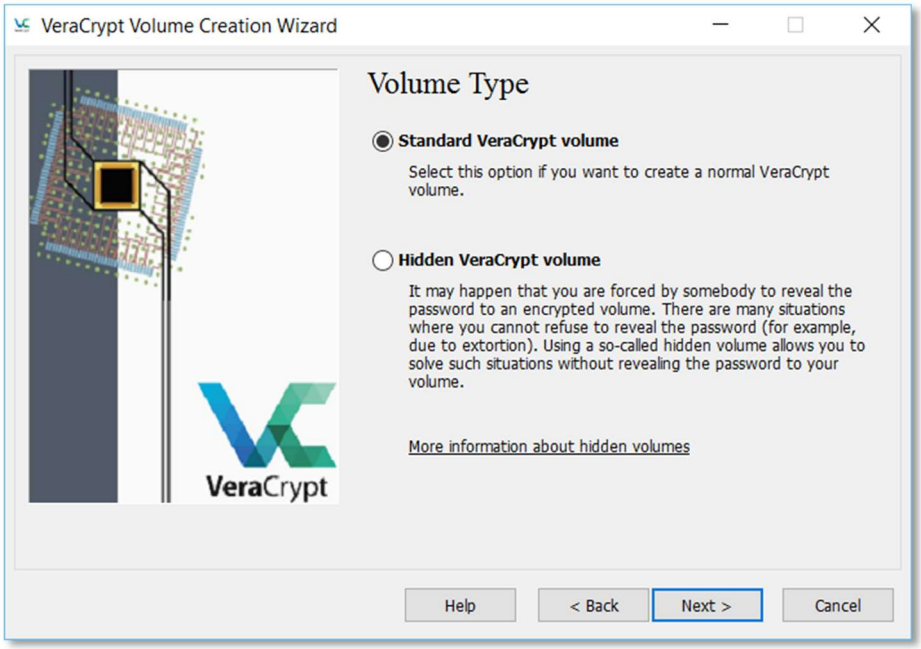
Step 2

By default, the option for an encrypted file container is checked. This is what we want, so click on 'Next'.



Step 3

In this step you will be asked what type of container you want to create. Again we choose the standard option. Click on

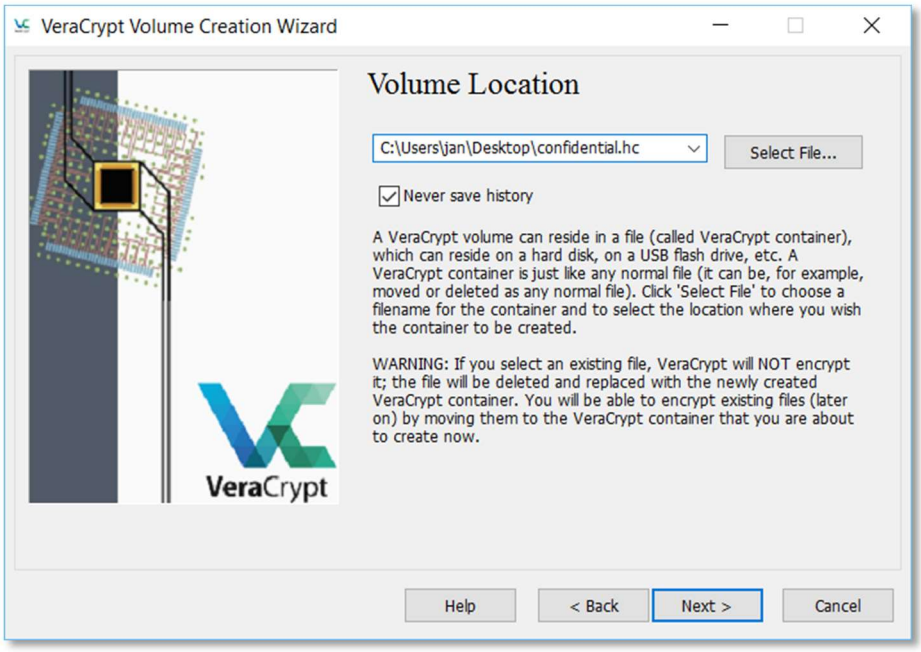


'Next'.

Step 4

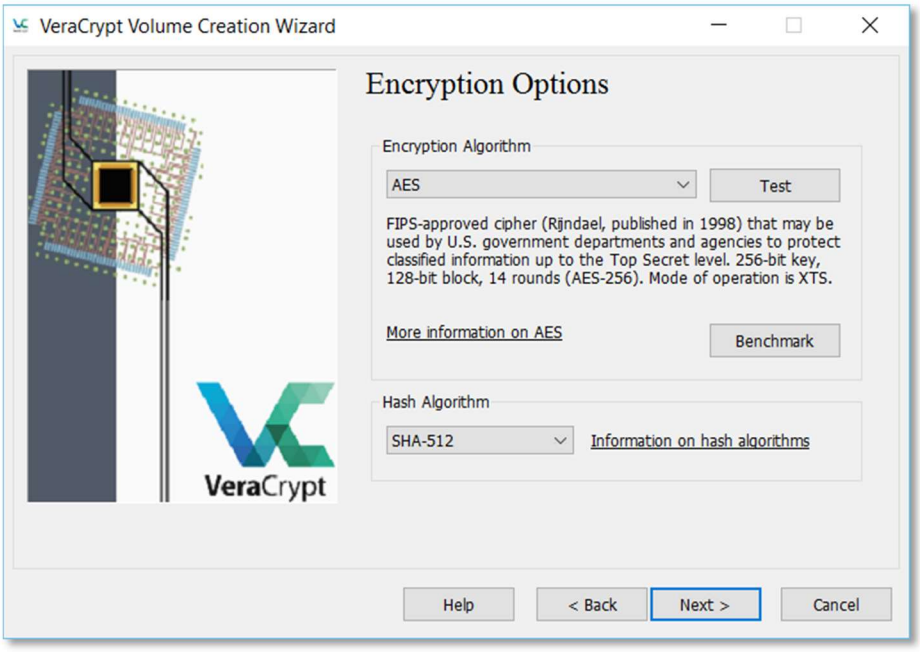
In the next step, you need to find a location for the container you want to create. Click on 'Select file' and navigate to where you want to place the container file and give it a name. In the example, a file called 'confidential.hc' will be created on the desktop. The .hc extension is often used for this type of file, but this is not mandatory (so you can also

omit the extension). If you want to move the file to a different location later, this is no problem. You can just move or copy it like a normal file.



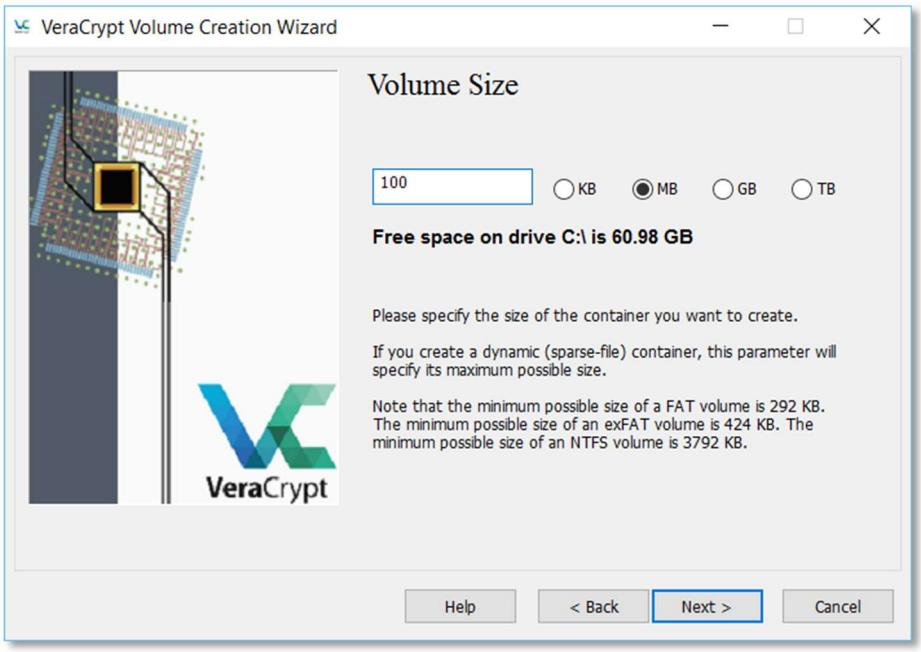
Step 5

The encryption options are set in the following step. Unless you're an expert and have good reasons for deviating from the default settings, just leave them as is. Click on 'Next'.



Step 6

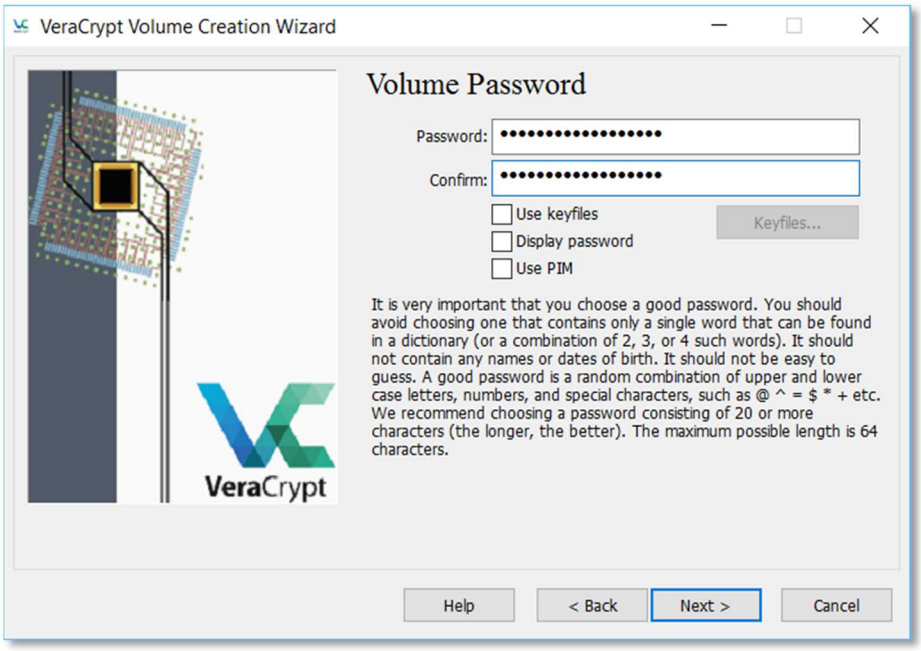
In the next step you choose the size of the container file. It is important to think about this carefully. Do not make the size too large if not necessary. The larger the file, the longer it will take to encrypt it.



Step 7

In step 7 you set the password.

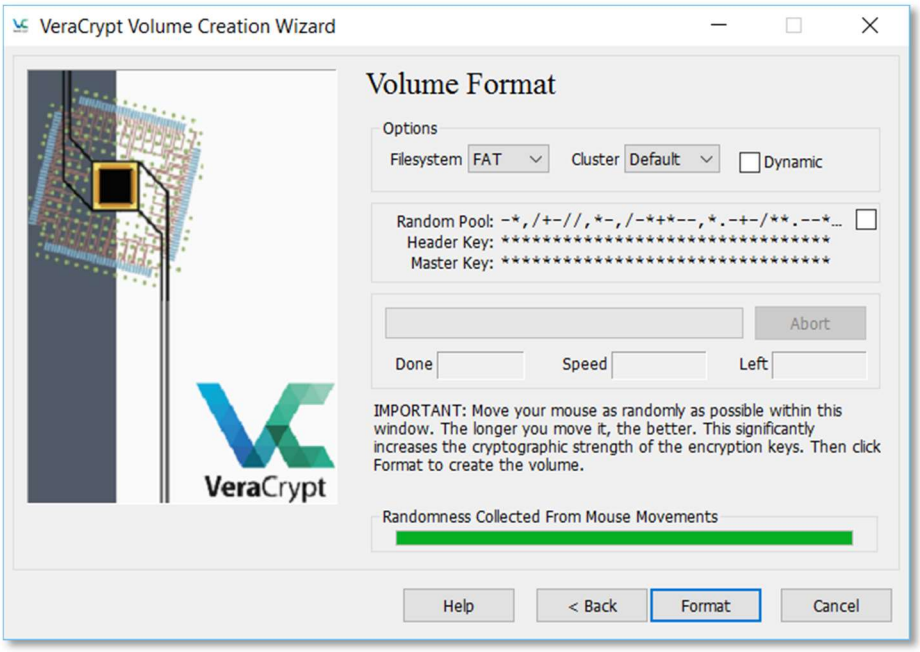
Note: In addition to a traditional password, you can also use so-called 'key files' for extra security. These are unique files that you must have to open the container. You can consider them as extra keys on the lock. These key files can be created with VeraCrypt, but you can also use your own files (e.g. a photo of your cat). Anyone who wants to open the container must have these files and know the password. In this example, we limit ourselves to encryption with a normal password, without using key files.



Step 8

In the last step, you are asked to strengthen the encryption by adding 'randomness' to the encryption algorithm. You do this by randomly moving your mouse cursor on the screen until the bottom bar is completely green.

Once this is done you can finalise your container by clicking on 'Format'.



This can take a while, especially if you want to create a large container. After formatting your container, you will find the file in the location you specified in Step 4.

Note: The 'Filesystem' option is set to 'FAT' by default at this step. This is usually sufficient and all operating systems can handle this. However, in some situations it may be better to use 'exFAT'. E.g. if you plan to save large files (>4GB) in your encrypted file container.

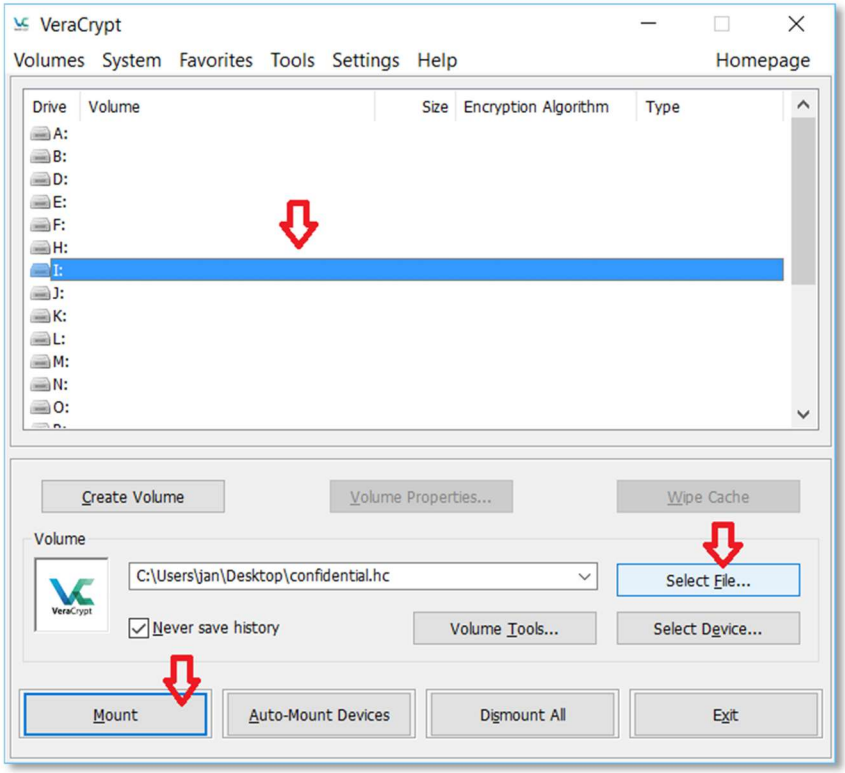
Using an encrypted file container

The procedure for using an encrypted file container is always the same: Open VeraCrypt, mount container, work, unmount container.

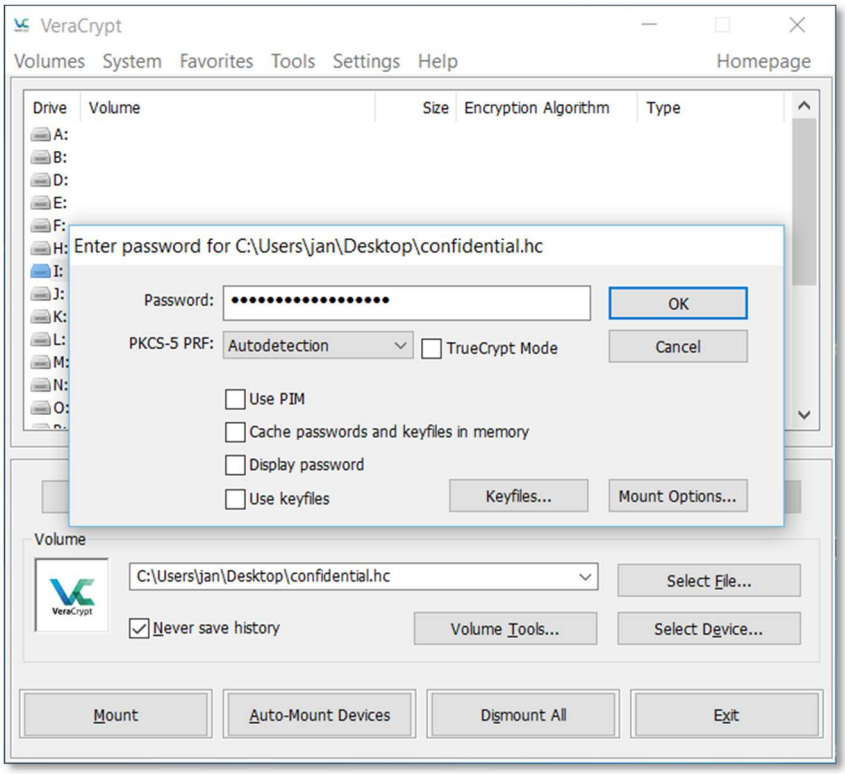
To make the container convenient to use, VeraCrypt mounts the file created on a virtual disk. When the container is mounted it looks like you have an extra hard drive on your computer. You can work on it just like on a normal hard drive. This also means that as long as this 'virtual' drive remains mounted, its contents are available to anyone who has access to your computer. When you have finished working on the virtual disk, you need to unmount it ('Dismount'). When the container is unmounted, the contents are encrypted. Did you forget to unmount before turning off your computer? In principle, this is not a problem because the container is automatically unmounted and encrypted when you turn off your computer.

Step 1 – Mounting

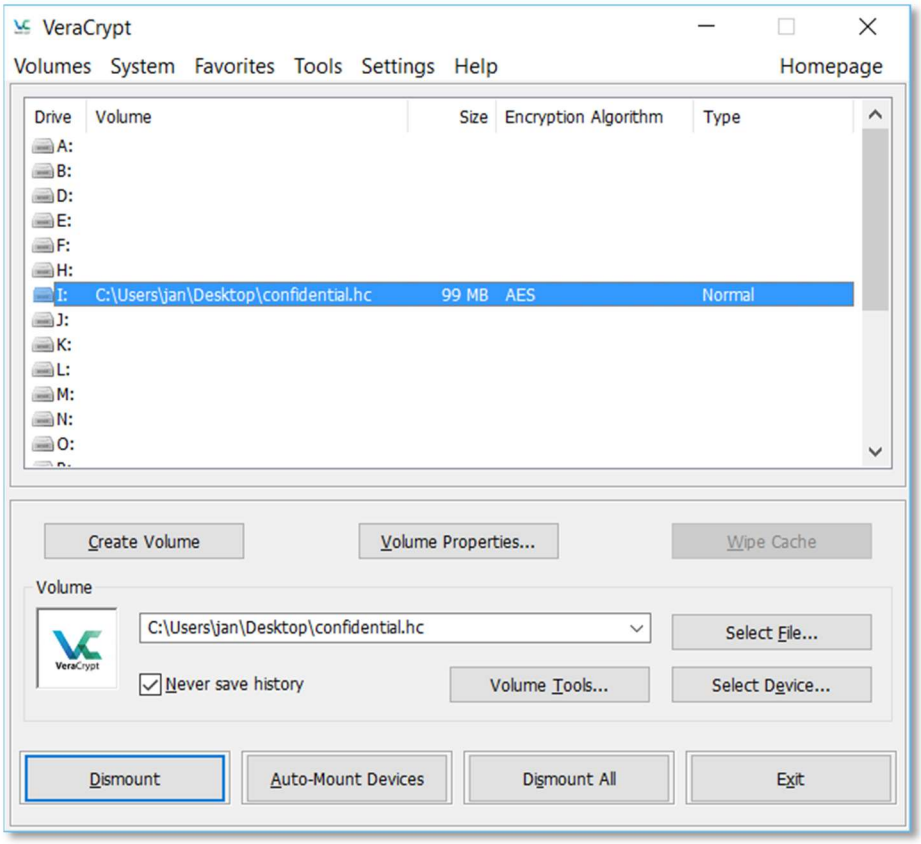
The first step is to mount your encrypted file container on a hard drive. In Windows this means that you select a drive letter you want to mount to as well as the container you want to mount. Then click on 'Mount'.



You will then be asked to enter the password.



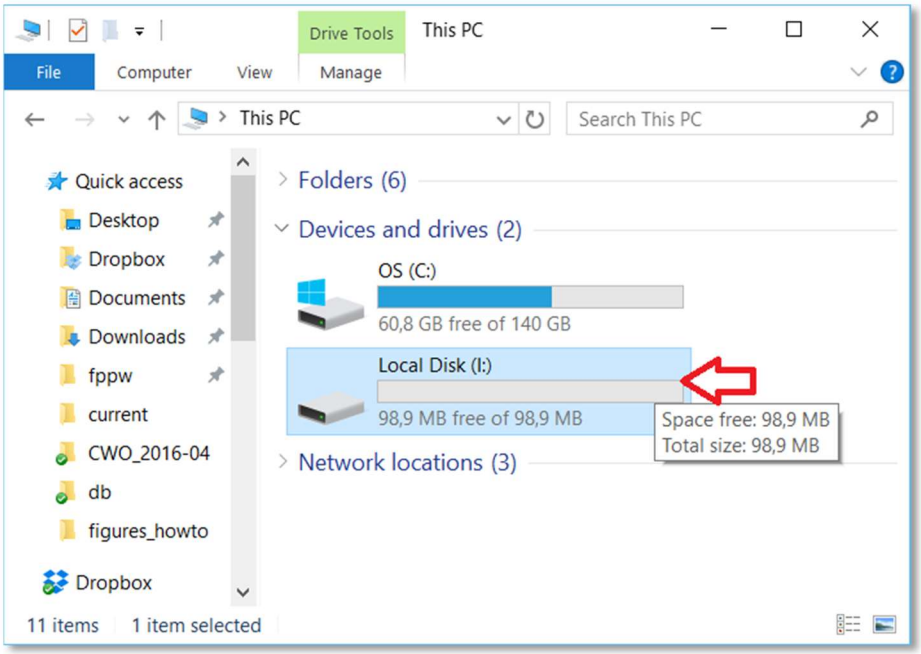
Once this is done, the encrypted file container will be unlocked and mounted on your system. As a result, a new local disk will be added to your computer (in this case under the disk letter I:\).



If you want, you can now reduce or close the VeraCrypt window.

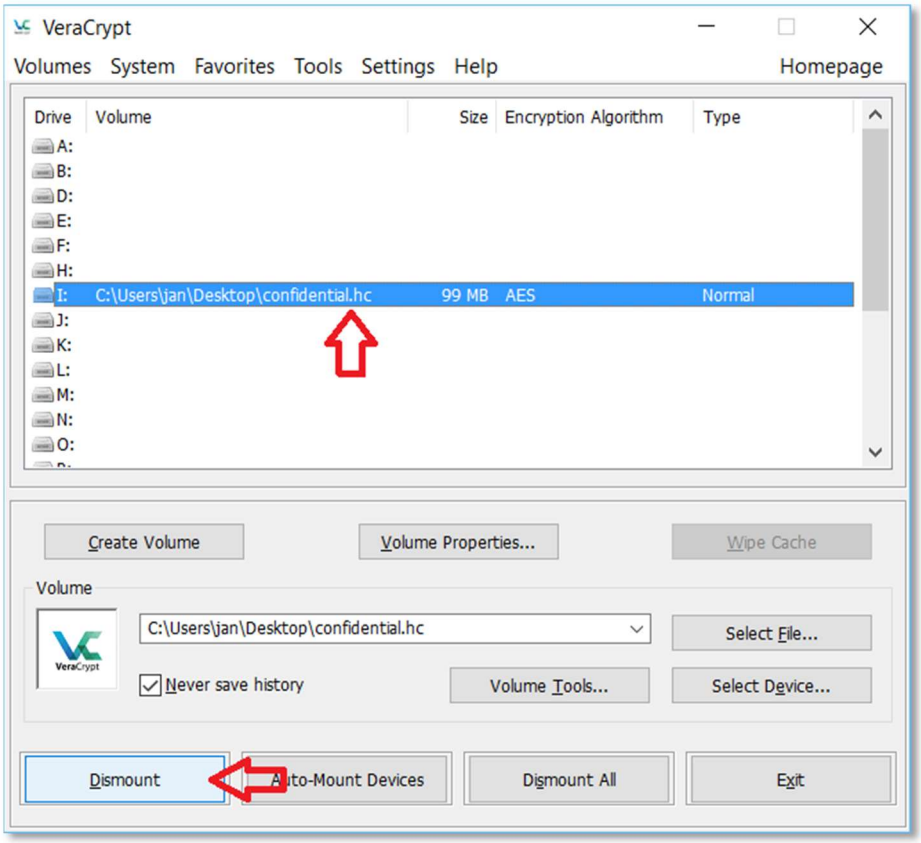
Step 2 – Use

You can now simply save files to this local disk via Windows Explorer as you would with a normal disk.



Step 3 – Unmounting

Once you've finished your work, you still have to unmount the file container. If you don't do this manually, the file container will be automatically unmounted when you turn off your computer. Be aware that as long as you have not done this, people who have access to your computer can also access the (confidential) files in the file container.



Proceed as follows: first select the disk you want to unmount in VeraCrypt and then press 'Dismount'. Then the virtual disk will be unmounted and disappear from your system. The file container is now encrypted and what remains is the (unreadable) encrypted file you started with in step 1.

Scenario 4 – Encrypting external devices

In this example we will go through how to encrypt an external hard drive or USB stick. This largely corresponds to creating an encrypted file container (see 'Scenario 3 – Encrypt project folder with VeraCrypt'), but instead of using an encrypted file, a physical disk or USB stick is used here.

The use of VeraCrypt in this scenario is especially appropriate when the encrypted medium will be used on different operating systems. Suppose you work with MacOS and your colleague uses Windows. If you want to make an encrypted USB stick to be read by both, you should use VeraCrypt. If you do not need to be able to use the medium on different operating systems, it is more convenient to use encryption software in your operating system (Bitlocker for Windows, FileVault2 for MacOS).

In summary, VeraCrypt is used as follows:

Preparation (only once):

1. Open VeraCrypt
2. Create Encrypted Volume
3. Set Password

At each use:

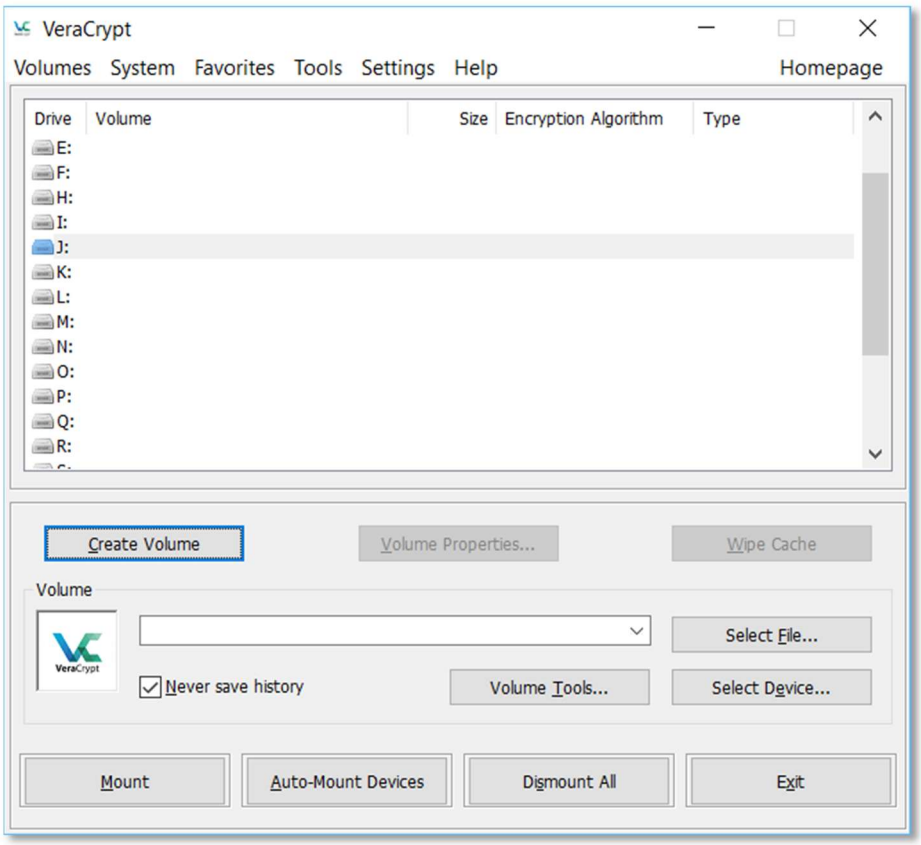
5. Open VeraCrypt
6. Select encrypted device and choose drive letter and 'Mount'.
7. Work
8. Select encrypted device in VeraCrypt and 'Dismount'.
9. Exit VeraCrypt

Preparing an encrypted disk

Before you can use an encrypted disk or USB stick, you must first prepare it. To do this, follow the steps below. You only need to do this once.

Step 1

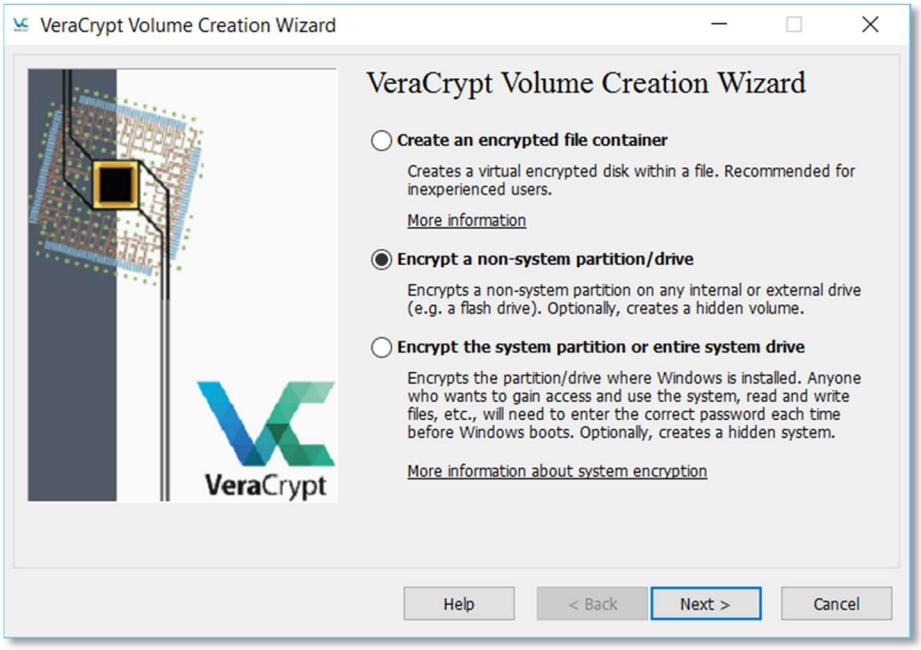
First open VeraCrypt. You will see the following screen.



To start, press 'Create Volume'.

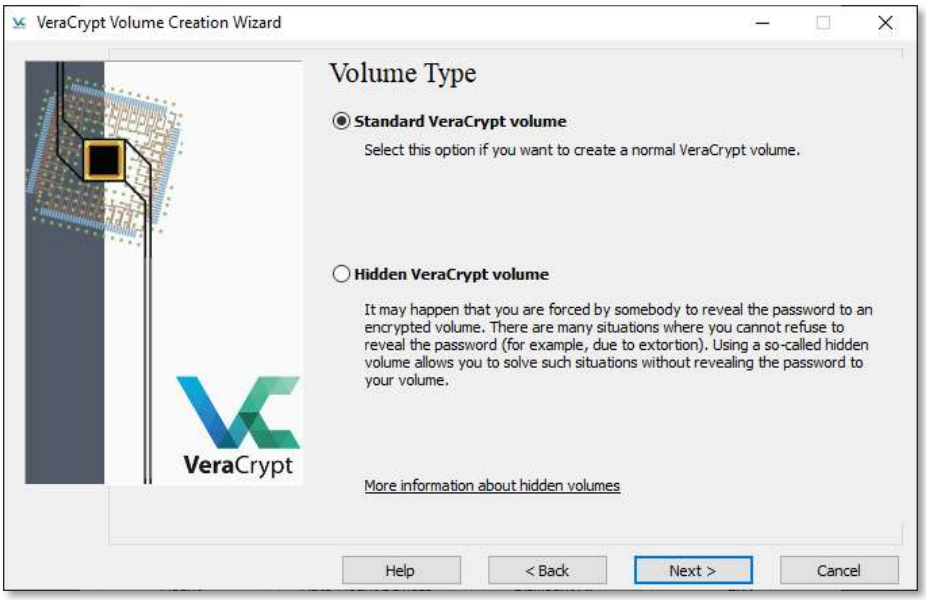
Step 2

By default, the option for an encrypted file container is checked. This is NOT what we want here. We want to encrypt a disk that is not the system disk (e.g. an external USB disk or a USB stick). To do this we select the second option 'Encrypt a non-system partition/drive' and then 'Next'.



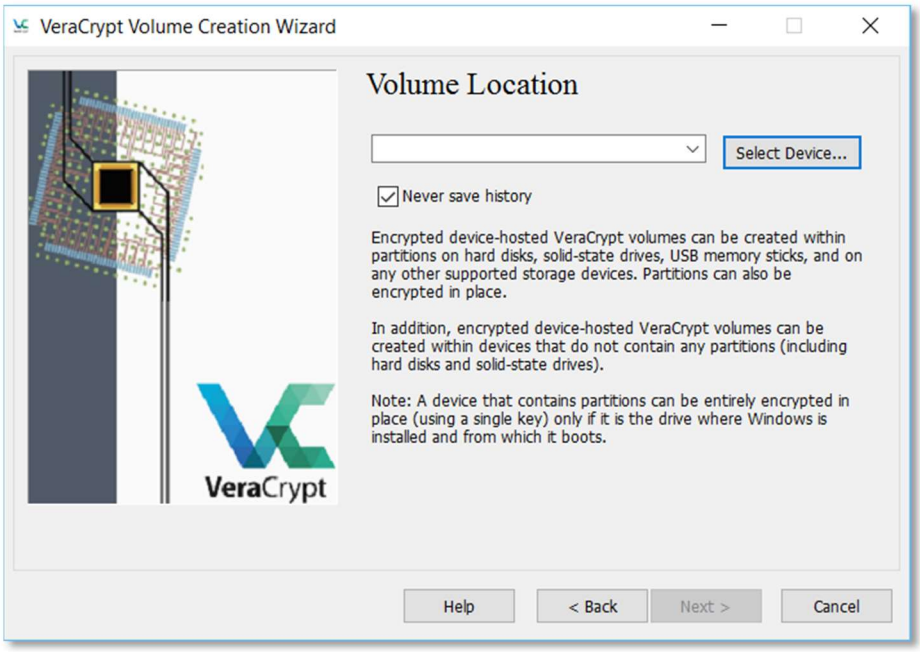
Step 3

Then you will be asked whether you want to create a normal VeraCrypt volume or a hidden volume. This second option can come in handy in very specific circumstances, but the standard option is usually sufficient.

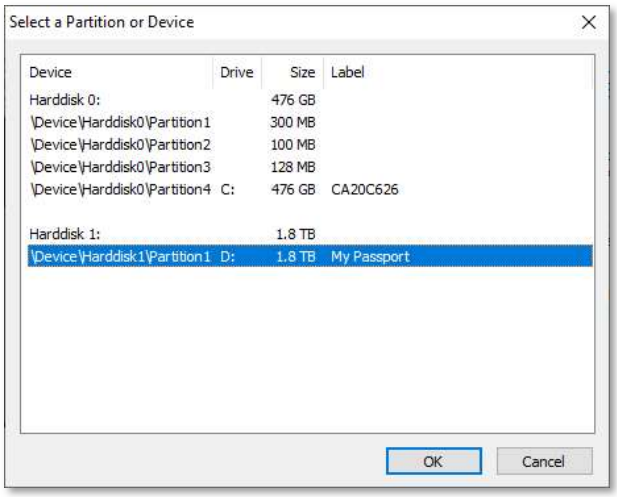


Step 4

In the next step you need to specify the location of the hard drive you want to encrypt. To do this click on 'Select device'.



You will see the following window.

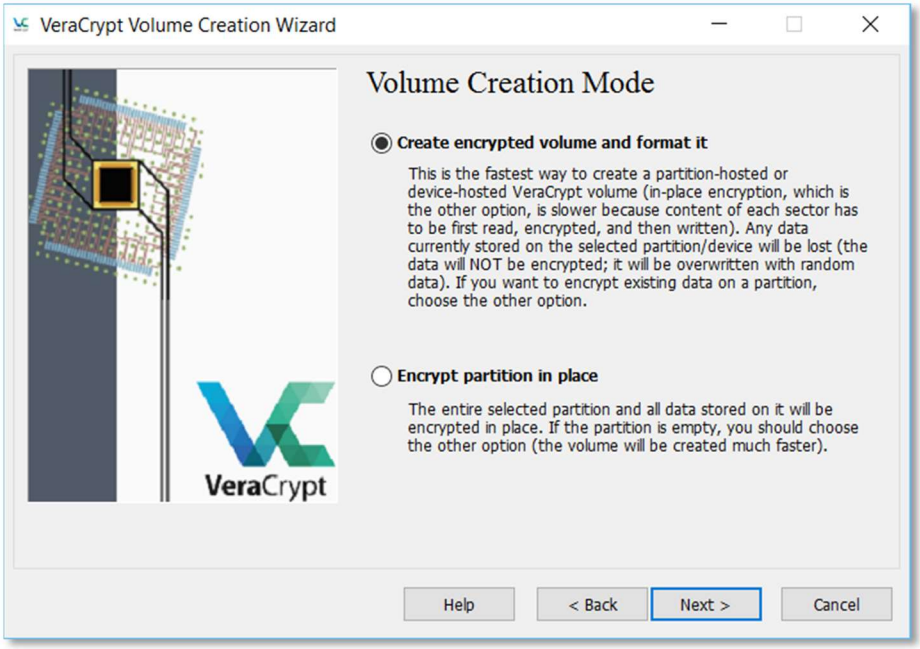


In this example, the removable hard drive we want to encrypt is mounted on the drive letter D:. We select this disk and press 'OK'.

Note: Caution! It is very important that you select the correct disk. If you know how large the external hard drive is, you can compare it with the specified size in the 'Size' column. Keep in mind that the real size of a disk is always slightly smaller than the size indicated on the package. In this example we use a 2TB disk. However, it's size is only listed as 1.8TB. If you don't know how big your disk is, open Windows Explorer before you connect the hard drive to your computer. Then connect the hard drive and see which disk letter is added. If you still have doubts, ask for help from your IT manager, for example.

Step 5

In the next step you choose what will happen to any data that may already be on the hard drive. If the disk is empty, or if it contains data that you no longer wish to keep, select the first option 'Create encrypted volume and format it'. Selecting this option will delete all data on the disk before it is encrypted. This is the fastest option.

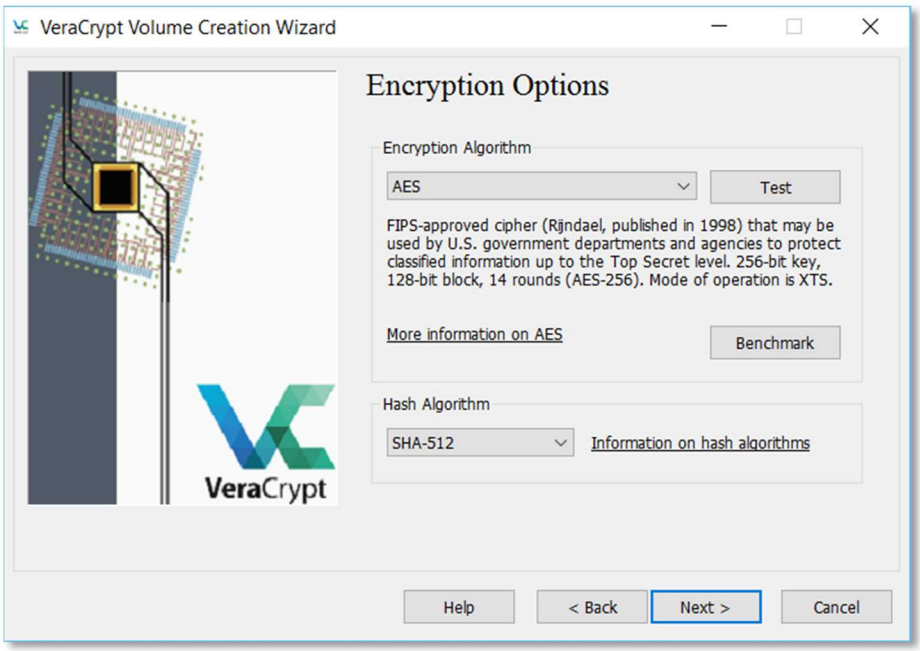


If you want to save and encrypt the data that is already on the disk, you need to select the second option ('Encrypt partition in place'). Because here the process does not start with a blank disk, choosing this option will take longer.

Once you have made your choice, click on 'Next'.

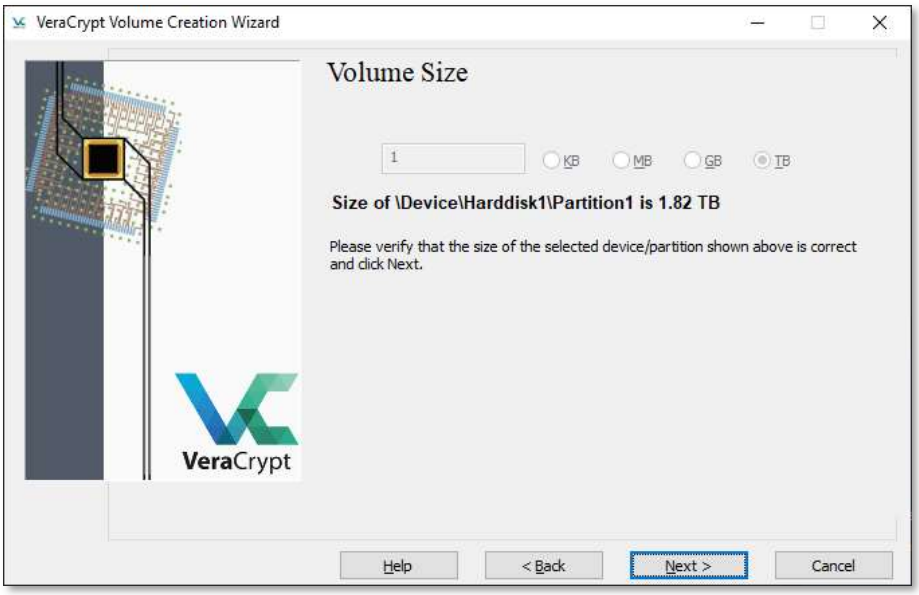
Step 6

The encryption options are set in the following step. Unless you're an expert and have good reasons for deviating from the default settings, just leave them as is. Press on 'Next'.



Step 7

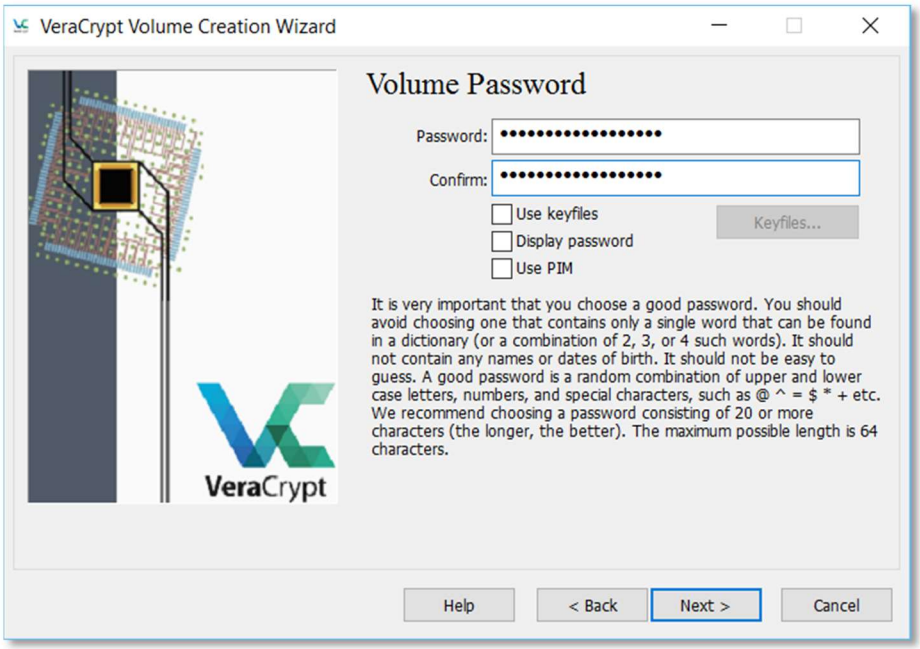
In the next step, the size of the volume is shown again. Since we are encrypting the entire hard drive, this step is purely informative and you cannot change anything. Press on 'Next'.



Step 8

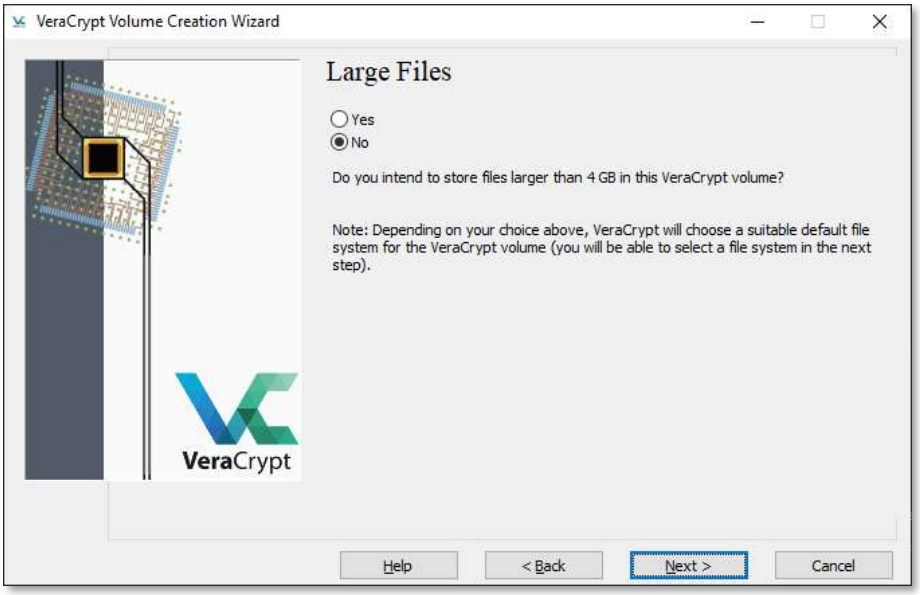
In step 8 you set the password.

Note: In addition to a traditional password, so-called key files can also be used for extra security. These are unique files that you must have to open the container. You can consider them as extra keys on the lock. These key files can be created with VeraCrypt, but you can also use your own files (e.g. a photo of your cat). Anyone who wants to open the container must have these files and know the password. In this example, we limit ourselves to encryption with a normal password, without using key files.



Step 9

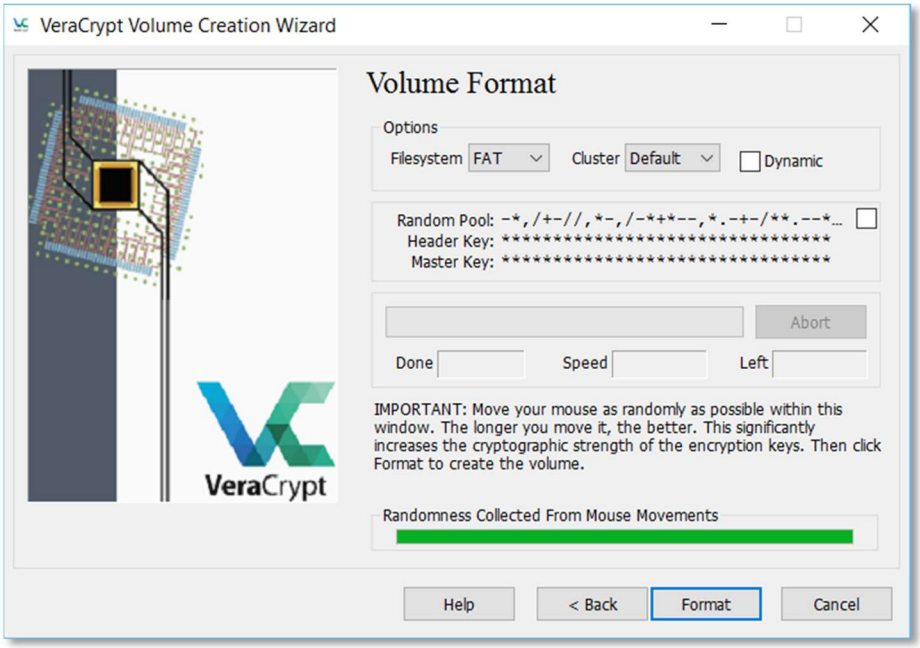
If you want to use large files (>4GB) on the encrypted disk, you can indicate this in this step.



Step 10

In the last step, you are asked to strengthen the encryption by adding 'randomness' to the encryption process. You do this by randomly moving your mouse cursor on the screen until the bottom bar is completely green.

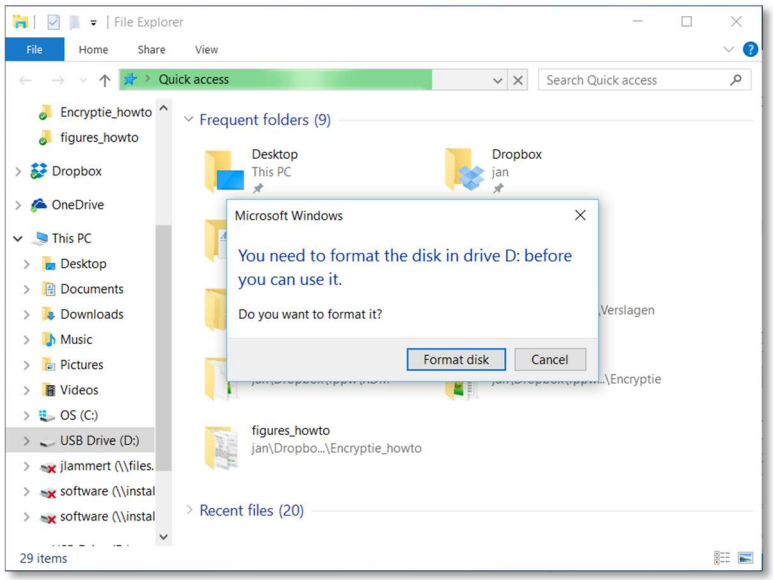
Once this is done you can finalise the encryption of the disk by clicking on 'Format'.



This can take a while, especially if you want to encrypt a large disk. After formatting and encrypting your hard drive, you will not find it on your system yet. You will need to mount it first.

Using the encrypted hard drive

Important! The contents of an encrypted disk are basically unreadable for a computer. When you mount the encrypted disk or USB stick on your computer, Windows will ask you if you want to 'format' the disk or USB stick. Do not do this as it will erase the contents of the encrypted disk! Click on 'Cancel'. To mount the encrypted disk we again use VeraCrypt.



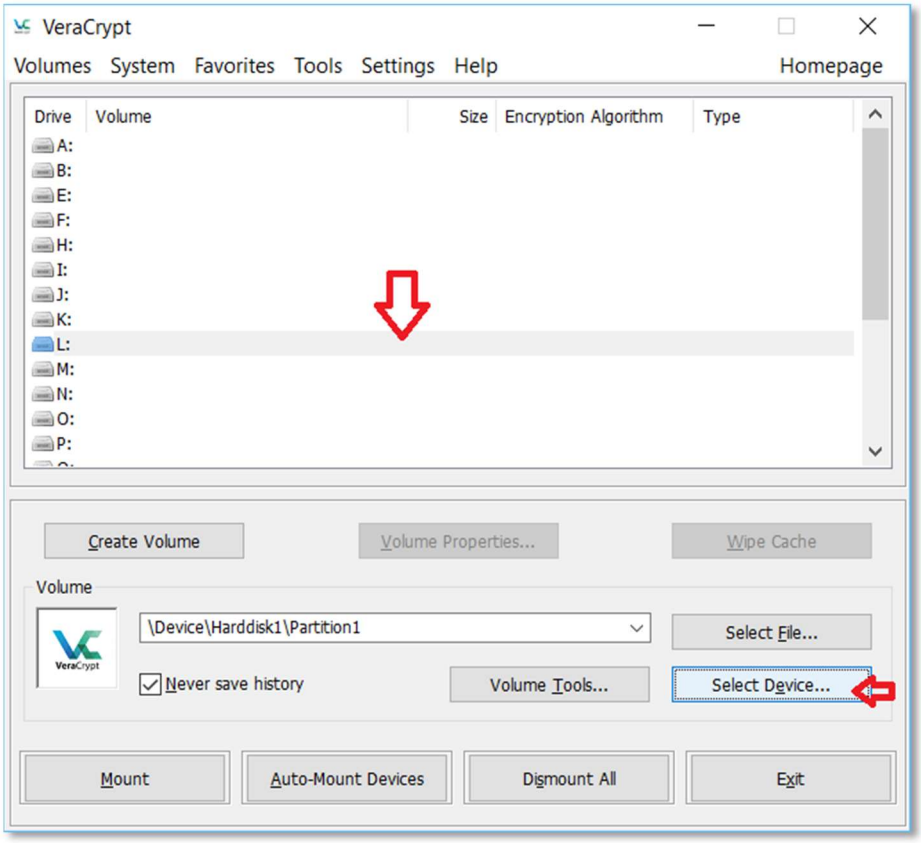
The procedure for using an encrypted hard drive is always the same: Open VeraCrypt, mount device, work, unmount device.

To make the encrypted hard drive convenient to use, VeraCrypt mounts it on a virtual disk. When the encrypted hard drive is mounted it looks like you have an extra hard drive. You can work on it just like on a normal hard drive. This can be confusing because the (unreadable) hard drive was already assigned a drive letter when mounting it on your Windows computer (in the example this is letter D:). Activating the hard drive with VeraCrypt will therefore add an extra hard drive (letter L: in the example, see below). It is the latter that can be used to work on.

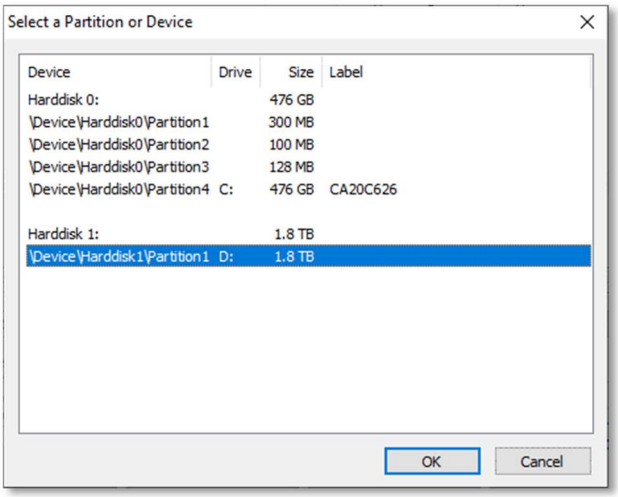
As long as the 'virtual' disk is mounted, its contents remain available to anyone who has access to your computer. Therefore, it is a good idea to unmount the virtual disk ('Dismount') when you no longer need it. If you do not manually unmount the drive, this will happen automatically when you turn off your computer.

Step 1 – Mounting

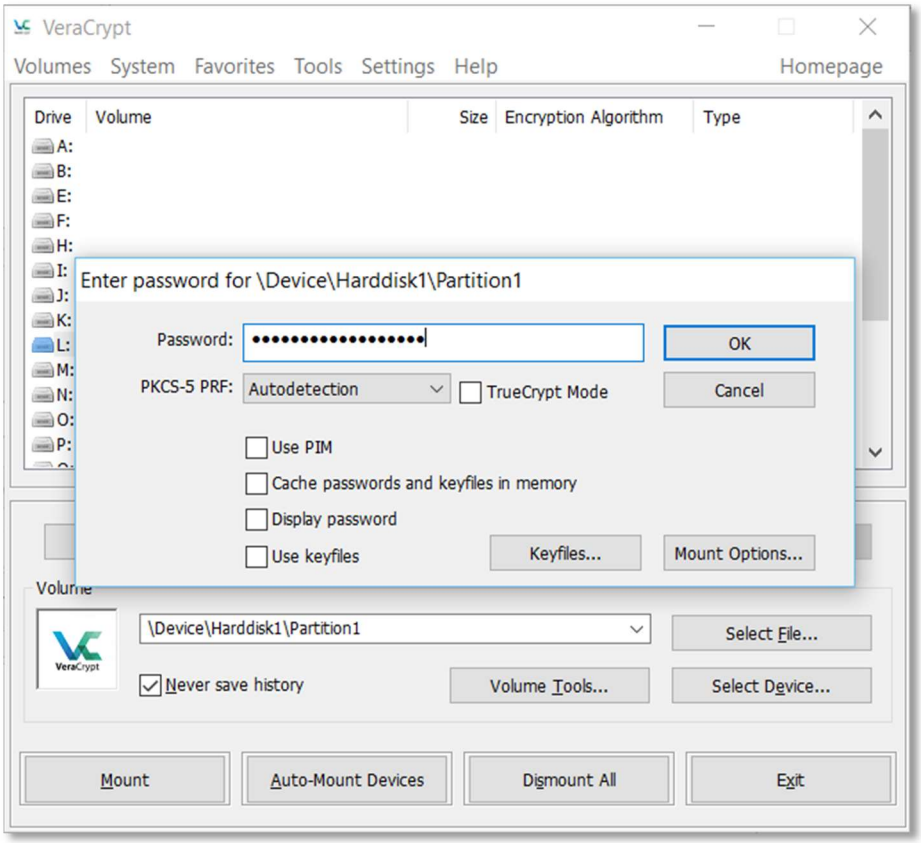
The first step is to mount your encrypted hard drive. In Windows this means that you select a drive letter to which you want to mount as well as the 'device' you want to mount.



In the overview of the available disk letters, first select a disk letter to which you want to mount the encrypted disk. Then select 'Select device' to choose the encrypted disk you want to mount.



Select the encrypted disk and press 'OK'. You have now selected your encrypted drive and the letter you want to mount it to. Then press 'Mount'. Because the disk is encrypted, you will be asked to enter the password.



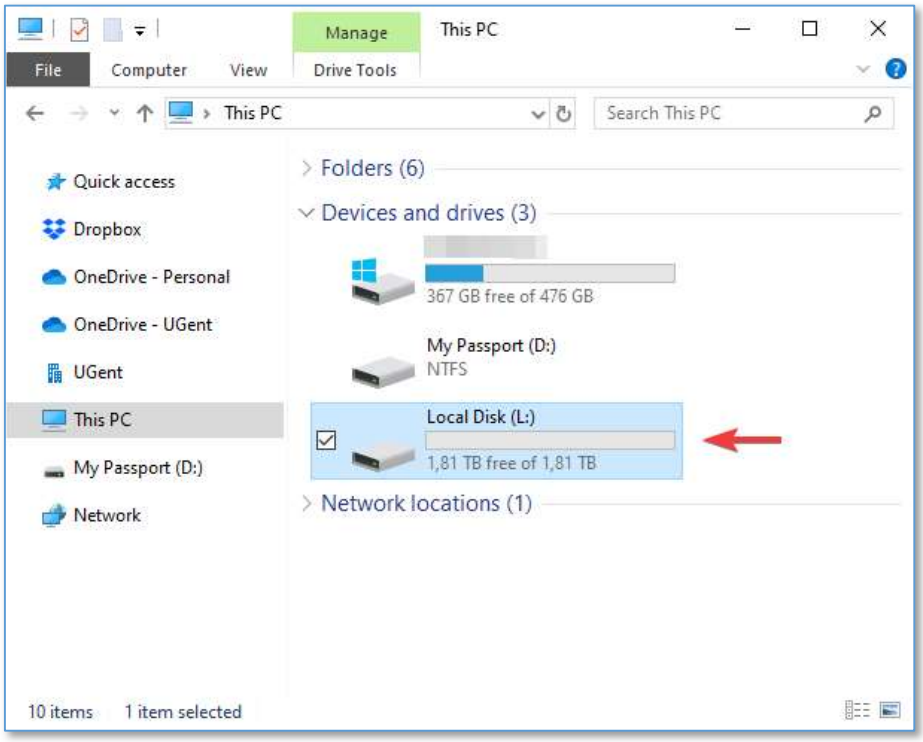
Enter the password and press 'OK'.

Once this is done, the encrypted disk will be unlocked and mounted on your system. As a result, a new local disk will be added to your computer (in this case under the disk letter L:\).

If you want, you can now reduce or close the VeraCrypt window.

Step 2 – Use

You can now simply save files to this local disk via Windows Explorer as you would with a normal disk.



In the screenshot above you can see that in Windows Explorer there are two disk letters for the mounted encrypted disk. The first is D: which cannot be written to, and the second is L: a virtual disk created by VeraCrypt to allow you to access the encrypted disk.

Step 3 – Unmounting

Once you are done with the above, you still need to unmount the virtual disk. If you do not do this manually, the virtual disk will be automatically unmounted when you turn off your computer. Be aware that until you have done this, people who have access to your computer can also access the (confidential) files on the virtual disk.

Proceed as follows: first select the disk you want to unmount in VeraCrypt and then press 'Dismount'. The disk will be unmounted and disappear from your system.

LICENSE