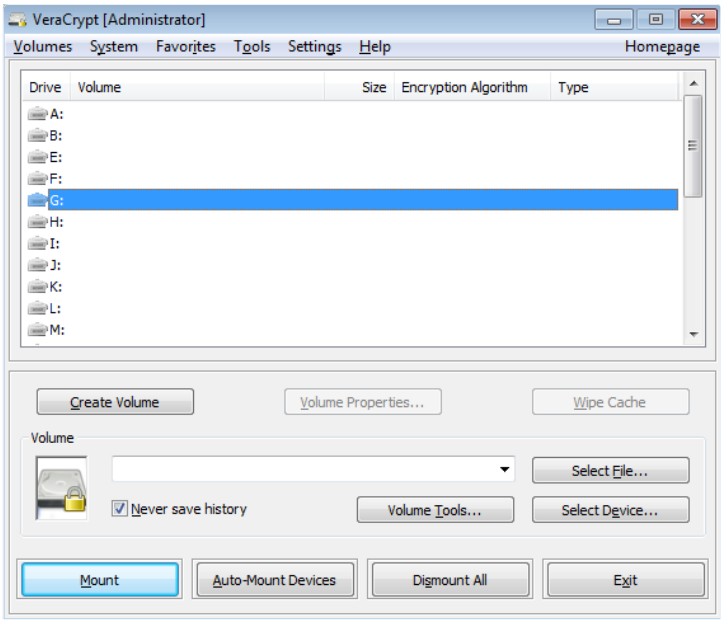
# Using VeraCrypt to protect your USB based drives

There has been considerable research done and also various newspaper articles about people leaving laptops or drives in public locations that contain sensitive data. There are numerous ways to protect data and one of the easiest and reliable ways we have found is a program called VeraCrypt. This is short guide to enable you to produce an encrypted drive to use and protect your data.

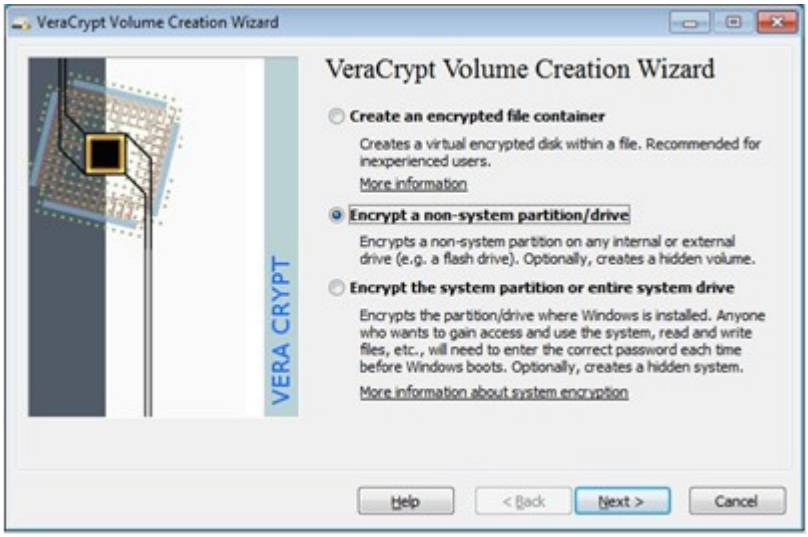
You obviously need VeraCrypt for this guide, the latest available is from https://veracrypt.codeplex.com/ Download and install the software as usual and start it afterwards. You will also need VeraCrypt on **all machines** you are using with this drive or media. VeraCrypt runs on all major platforms Linux, Windows and Mac OS and transparently so, we regularly use it between all three platforms.

The main VeraCrypt window will load and look like the following:

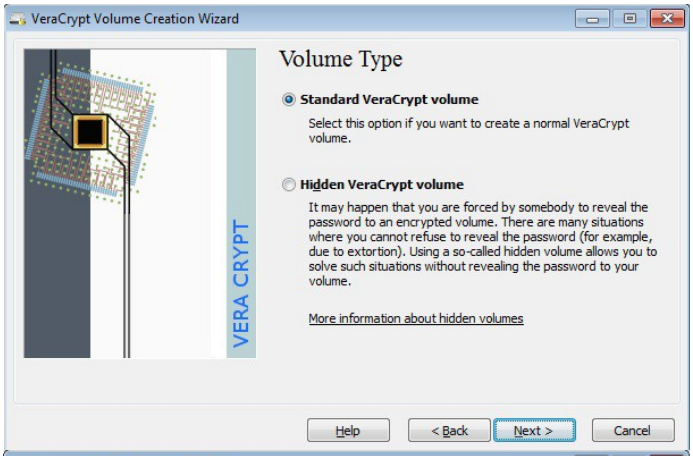



You obviously need to make some decisions before you continue. This guide will encrypt the full USB drive, erasing all of the existing contents in the process. WARNING Do not encrypt a drive that already has data on it. Copy the data off somewhere first and recopy back on after encrypting.

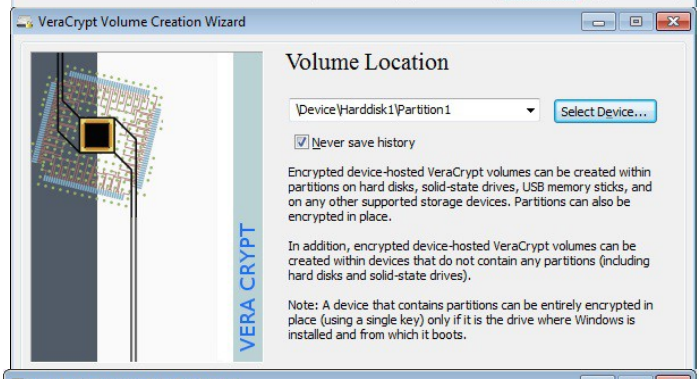
Click on the Tools menu then select Volume Creation Wizard.
A window will appear asking about the type of volume that you want to create.



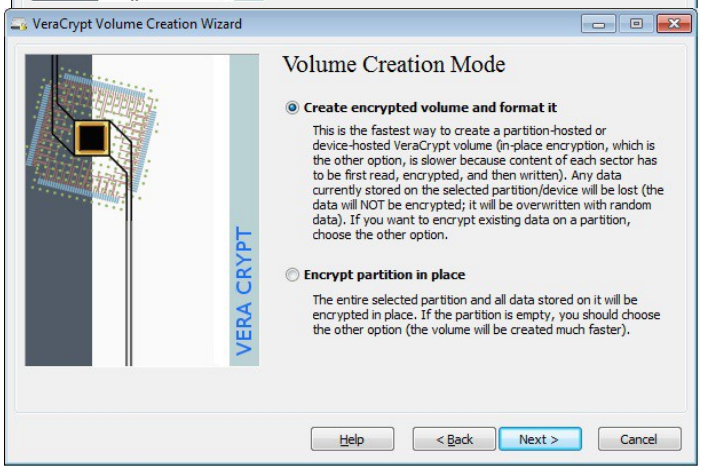

The choices are to create an encrypted container, encrypt a partition / drive or encrypt the system partition (the one running Windows). We are going to create a volume within a non-system device and check the second option in that screen. The next window gives us the choice to create a standard or hidden VeraCrypt volume.



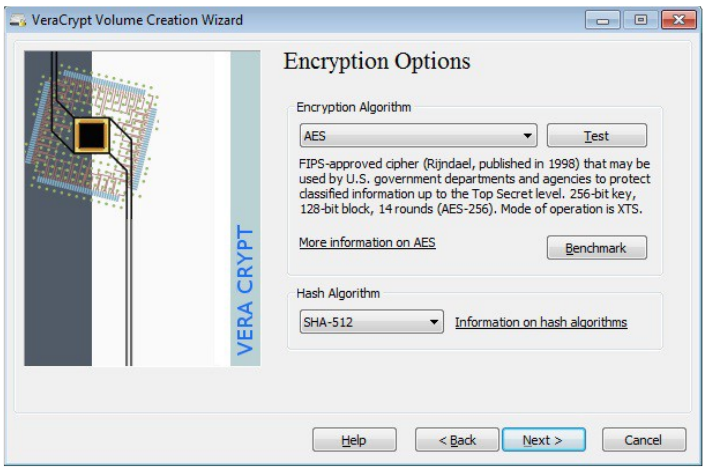

Hidden volumes are created in standard volumes. Hidden volumes and allow a decoy volume to exist with a separate password. If under duress, you can supply the standard password and not the password for the hidden volume. We are creating a standard volume therefore.



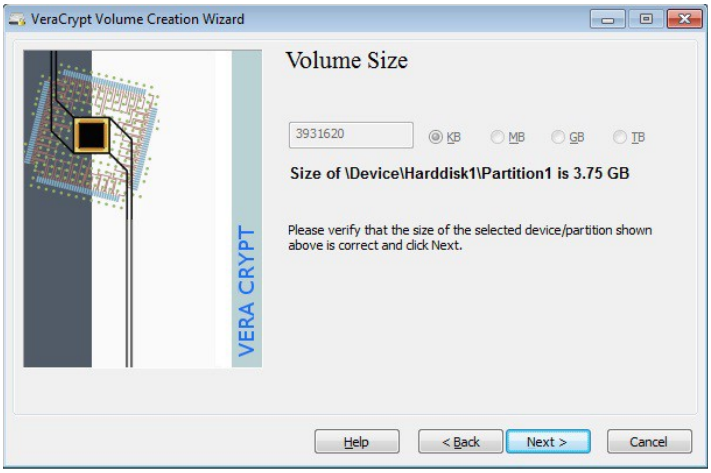

Now we are selecting the device that we want to encrypt, in our case the new USB drive.



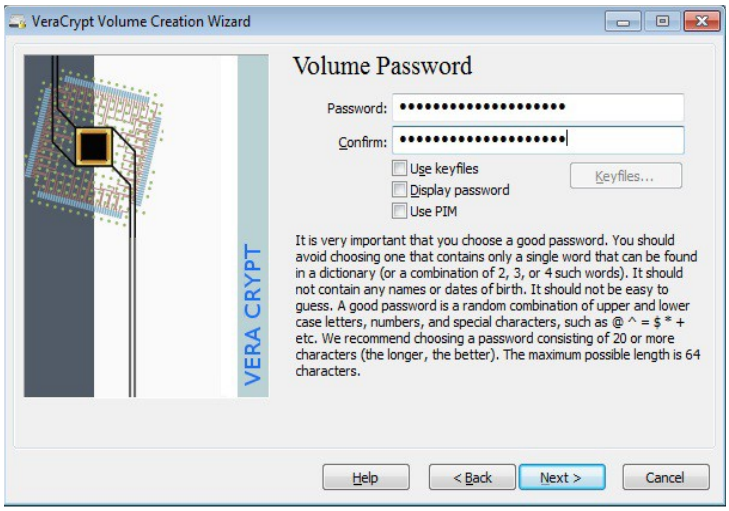

Select Create encrypted volume and format it




This screen details the encryption and hash algorithms that can be used. My selection was AES and SHA-512, which should be reasonably secure. You can run benchmarks in that window and get additional information about each algorithm. All algorithms are secure (unless someone proves otherwise, which has not happened yet).

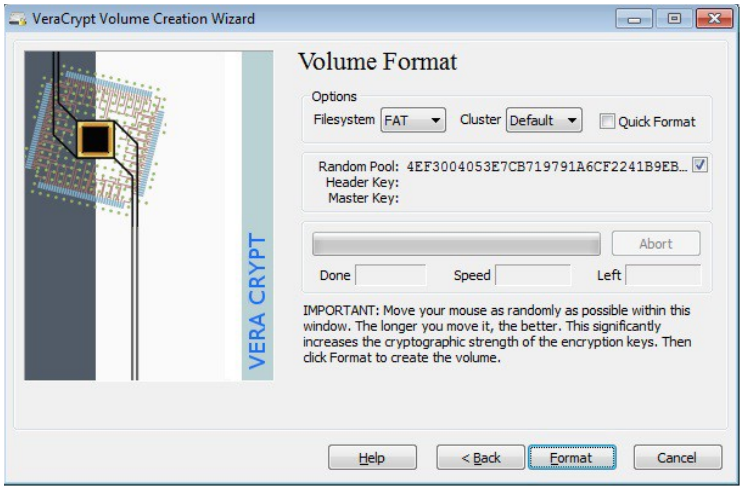



Next screen shows us the volume size we are using. We are encrypting the entire thumb drive, so simply hit next.




The Volume Password is the most important part of the process. You access your files with it and if you happen to forget it your files are lost.

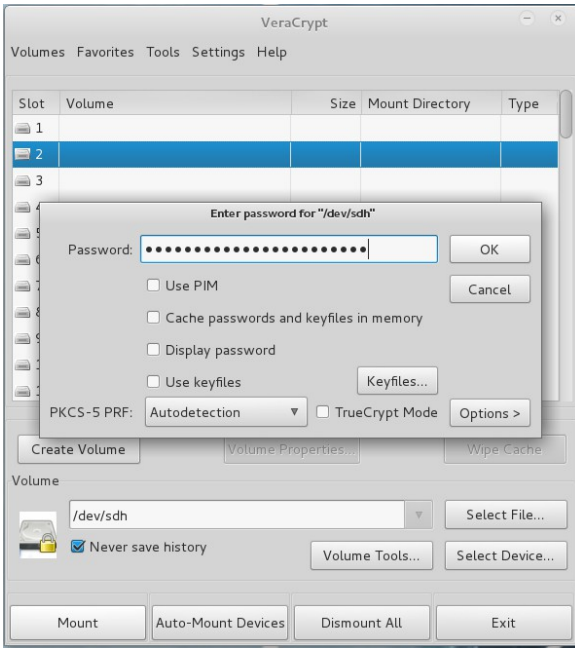
Make sure you use a large password, something that is not a dictionary word and not a combination of them. A password should be at least made of 20 characters and be made of upper and lower case chars, numbers and special chars. The maximum amount of chars is 64. A keyfile can be created as well which then works in combination with the password. Store this password somewhere safe (envelope in a safe) should you forget it




The drive will be **formatted** in the end. You need to move your mouse randomly around the screen for some time to improve the quality of the encryption keys. The file system and cluster size can remain as is unless you need them to be different. Using Quick Format since there have not been any files on the USB drive previously. The process is finished after this step. You need to mount the drive now to be able to use it.

## Mounting your encrypted USB drive

Select a drive letter currently not assigned and click on Select Device afterwards in the main menu. Now select the partition or drive that you have encrypted and click on ok.




Now click on Mount which opens up a password box where you have to enter the password that you have selected during setup. Click ok afterwards and work with the hard drive normally from there on if the password was correct

**IMPORTANT NOTE If you place a VeraCrypt encrypted drive in a normal machine it appears as a drive that needs formatting...and asks you to do so don't format it... otherwise..**
**...☺....▯**