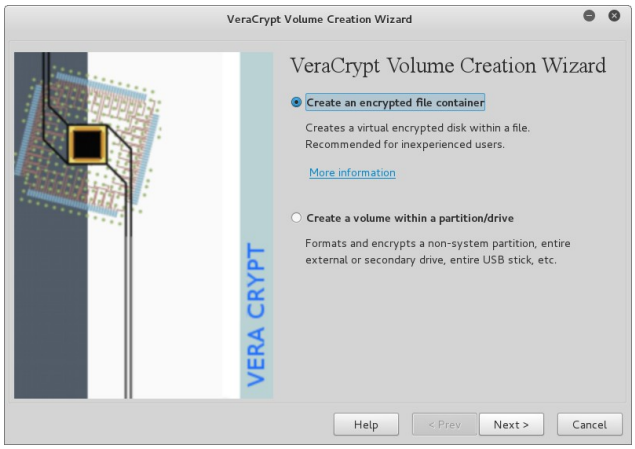
Using VeraCrypt to protect your files in a VeraCrypt container

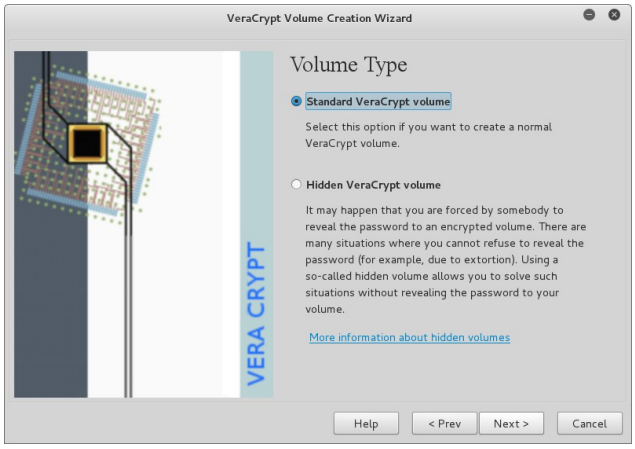
There are numerous ways to protect data and one of the easiest and reliable ways we have found is a program called VeraCrypt. This is short guide to enable you to produce an encrypted file (container) to use and protect your data storing it on your conventional drive as a file. You can create series of containers and use these to securely send files across the Internet via email or file transfer (FTP, HTTP, WEBDAV). All you need share with the receiving end is the password preferably via an alternate channel e.g SMS or a phone call, and of course they must have VeraCrypt installed.

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.

Volumes | Create New Volume

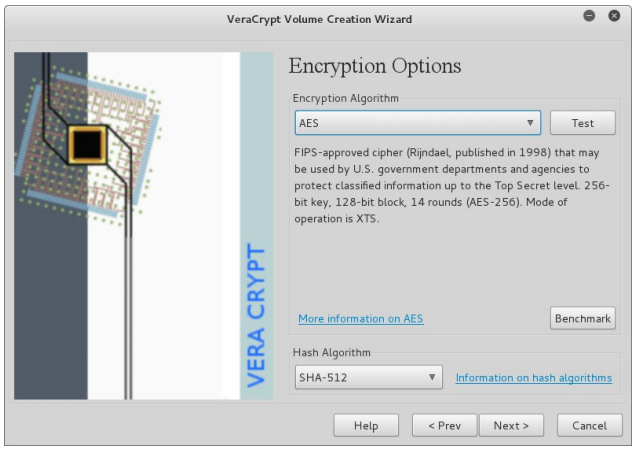


We need to create a Standard VeraCrypt Volume



Now select a place/folder where you are going to store these files and give it a meaningful name.

AES encryption is enough for most instances. But you can use any of the encryption algrorithms or combinations with confidence



Chose a realistic size for the container for emailing purposes <10MB typically. For file transfers have an idea of file size and typically add 5% safety in the size.

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

We chose FAT as its universal unless your have a 2GB or larger file then you should chose NTFS or if on Linux platforms ext3

Then we need to format the file. Move the mouse randomly over screen for at least 20-30 seconds, longer the better. Then click format and the container is produced.

The final is to load your newly produced container and assign it a drive letter. This allows you to copy your files to the new “drive”, once they have finished copying you can then “dismount the drive”. The files are now inside your container. Now you can email or upload with confidence your container to its final destination.