

# VERACRYPT

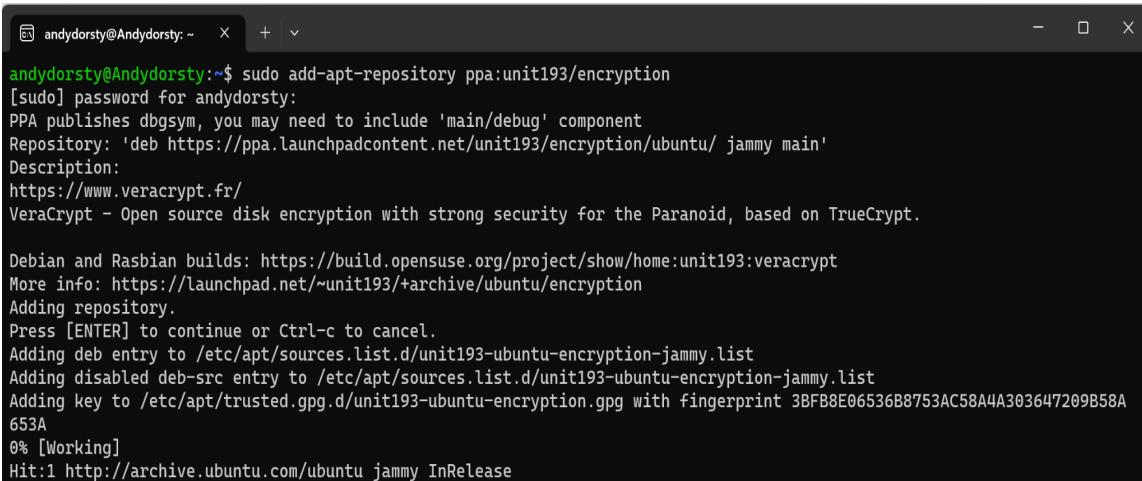
**VeraCrypt is an open source software that is used to encrypt files in a hard disk, encrypt hard disk partitions as well as the hard disks.**

## Installing VeraCrypt

1. Download the file and extract it.

```
andydorsty@Andydorsty:~$ tar -xvf 'veracrypt-1.25.9-setup (1).tar.bz2'  
veracrypt-1.25.9-setup-console-x64  
veracrypt-1.25.9-setup-console-x86  
veracrypt-1.25.9-setup-gtk3-console-x64  
veracrypt-1.25.9-setup-gtk3-gui-x64  
veracrypt-1.25.9-setup-gui-x64  
veracrypt-1.25.9-setup-gui-x86
```

2. Add the PPA.



```
andydorsty@Andydorsty:~$ sudo add-apt-repository ppa:unit193/encryption  
[sudo] password for andydorsty:  
PPA publishes dbgsym, you may need to include 'main/debug' component  
Repository: 'deb https://ppa.launchpadcontent.net/unit193/encryption/ubuntu/ jammy main'  
Description:  
https://www.veracrypt.fr/  
VeraCrypt - Open source disk encryption with strong security for the Paranoid, based on TrueCrypt.  
  
Debian and Rasbian builds: https://build.opensuse.org/project/show/home:unit193:veracrypt  
More info: https://launchpad.net/~unit193/+archive/ubuntu/encryption  
Adding repository.  
Press [ENTER] to continue or Ctrl-c to cancel.  
Adding deb entry to /etc/apt/sources.list.d/unit193-ubuntu-encryption-jammy.list  
Adding disabled deb-src entry to /etc/apt/sources.list.d/unit193-ubuntu-encryption-jammy.list  
Adding key to /etc/apt/trusted.gpg.d/unit193-ubuntu-encryption.gpg with fingerprint 3BF88E06536B8753AC58A4A303647209B58A  
653A  
0% [Working]  
Hit:1 http://archive.ubuntu.com/ubuntu jammy InRelease
```

3. Installing VeraCrypt on the Linux distribution.

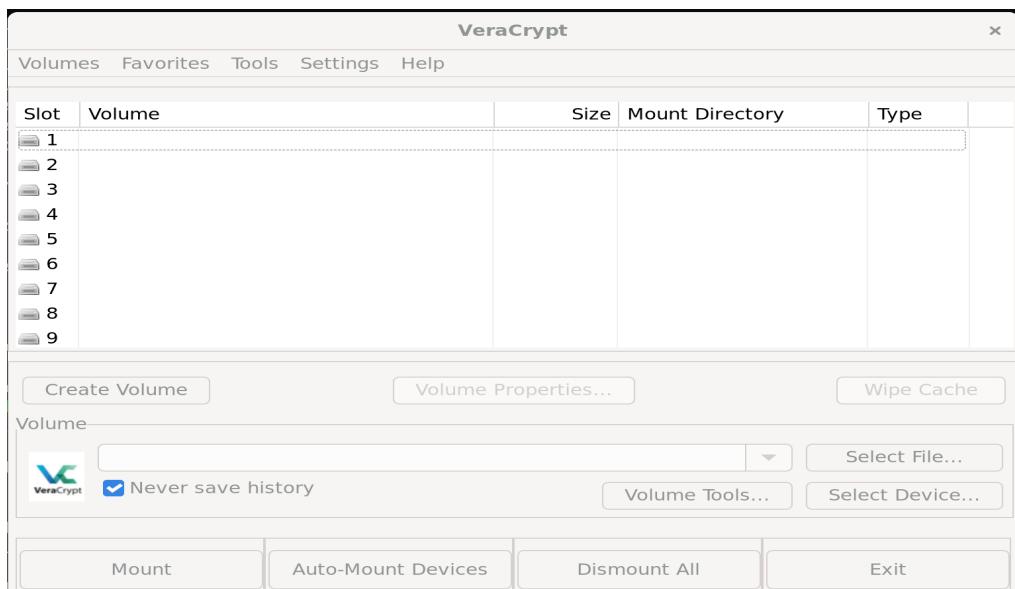
```
andydorsty@Andydorsty:~$ sudo apt update  
Hit:1 http://security.ubuntu.com/ubuntu jammy-security InRelease  
Hit:2 http://archive.ubuntu.com/ubuntu jammy InRelease  
Hit:3 http://archive.ubuntu.com/ubuntu jammy-updates InRelease  
Hit:4 http://archive.ubuntu.com/ubuntu jammy-backports InRelease  
Hit:5 https://ppa.launchpadcontent.net/unit193/encryption/ubuntu jammy InRelease  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
227 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

```

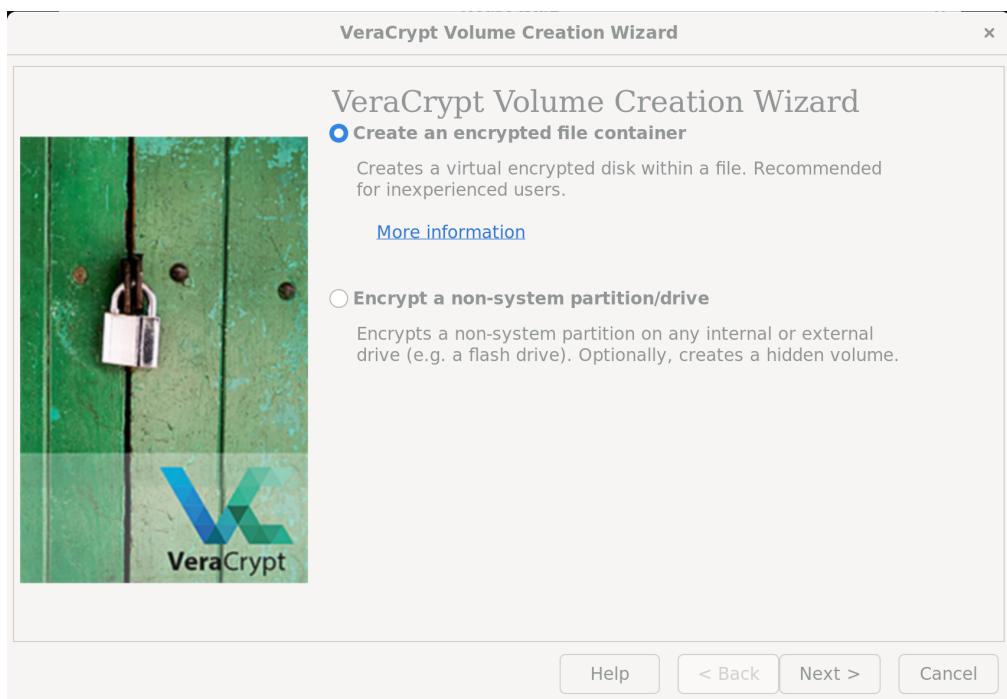
andydorsty@Andydorsty:~$ sudo apt install veracrypt
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
exfatprogs libauthen-sasl-perl libclone-perl libdata-dump-perl libencode-locale-perl libfile-basedir-perl
libfile-desktopentry-perl libfile-listing-perl libfile-mimeinfo-perl libfont-afm-perl libfontenc libgtkd-3-0
libhtml-form-perl libhtml-format-perl libhtml-parser-perl libhtml-tagset-perl libhtml-tree-perl libhttp-cookies-perl
libhttp-daemon-perl libhttp-message-perl libhttp-negotiate-perl libice6 libio-html-perl
libio-socket-ssl-perl libio-stringy-perl libipc-system-simple-perl liblvm1 liblwp-mediatypes-perl
liblwp-protocol-https-perl libmailtools-perl libnet-http-perl libnet-smtp-ssl-perl
libnet-ssleay-perl libnotify4 libphobos2-ldc-shared98 libsm6 libtbs-ixhash-perl libtimedate-perl libtry-tiny-perl
liburi-perl libvted-3-0 libwww-robotrules-perl libwxbase3.0-0v5 libwxgtk3.0-gtk3-0v5
libx11-protocol-perl libxaw7 libxcb-shape0 libxbfile1 libxml-parser-perl libxml-twig-perl libxml-xpathengine-perl
libxmu6 libxt6 libxxf86dg1 perl-openssl-defaults tilix tilix-common x11-utils x11-xserver-utils xdg-utils
Suggested packages:
libdigest-hmac-perl libgssapi-perl libcrypt-ssleay-perl gnome-shell | notification-daemon libsub-name-perl
libbusiness-isbn-perl libauthen-ntlm-perl libunicode-map8-perl libunicode-string-perl xml-twig-tools python-nautilus
mesa-utils nckle cairo-5c xorg-docs-core
The following NEW packages will be installed

```

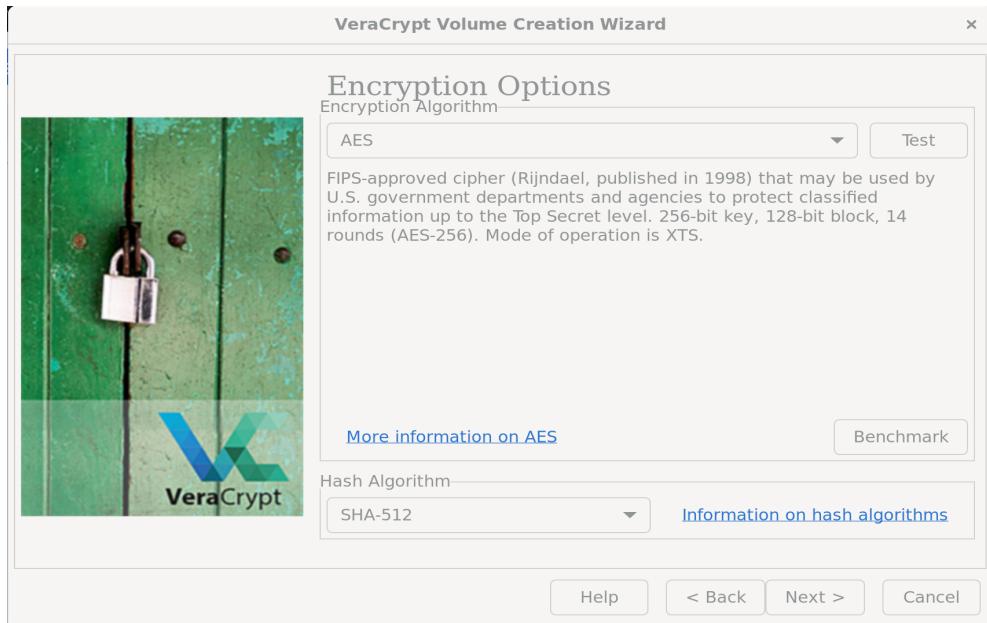
#### 4. Start VeraCrypt by entering “VeraCrypt”.



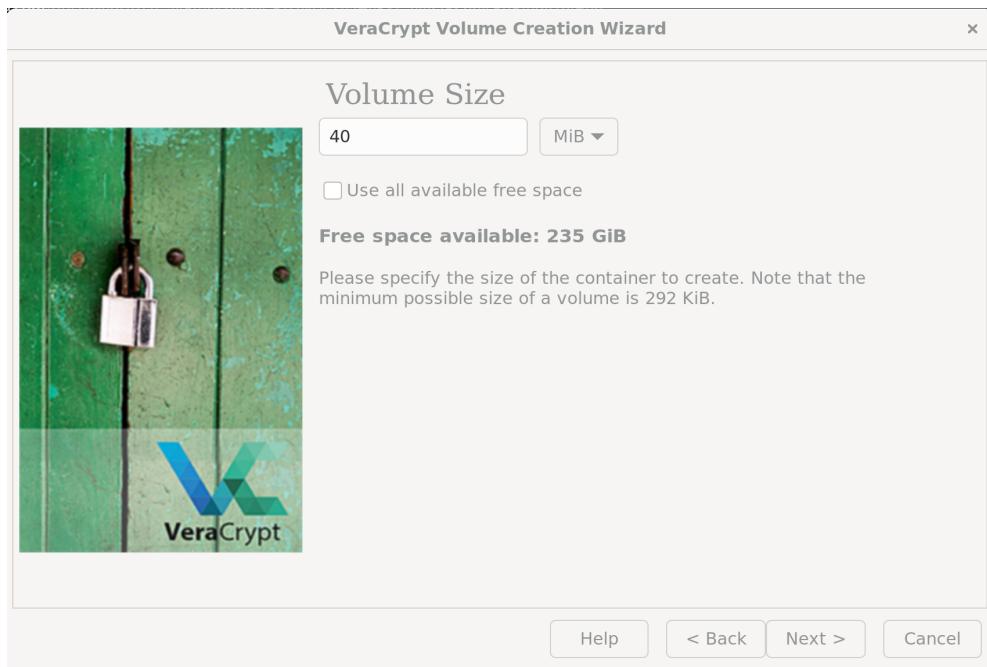
#### 5. Click on Create Volume.



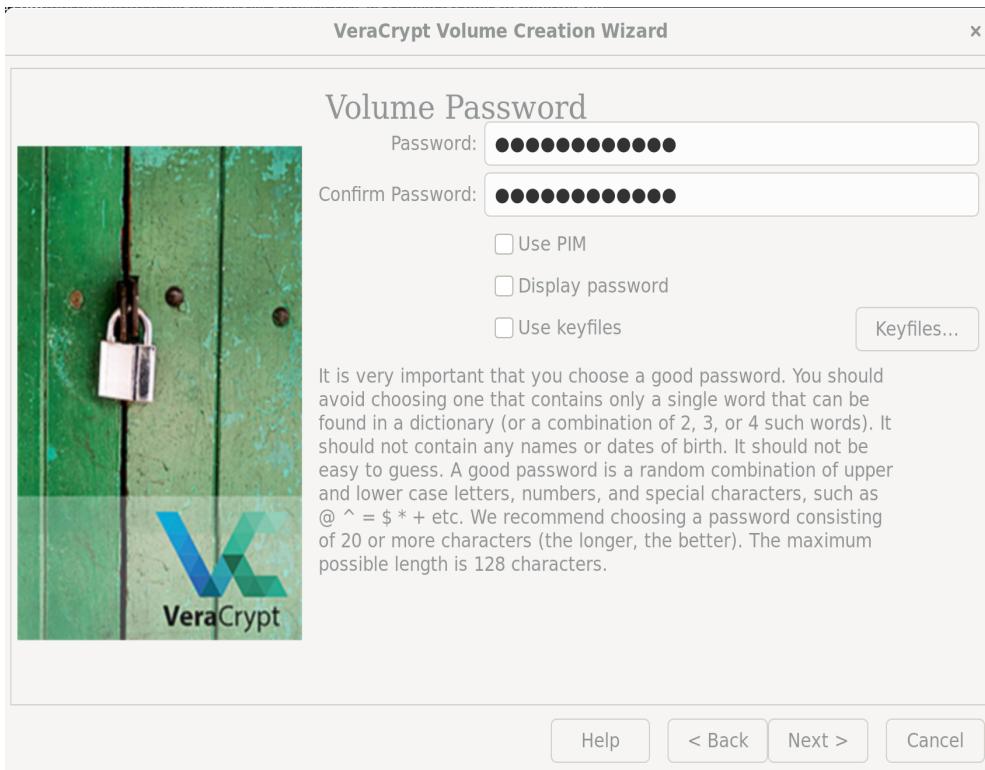
6. Choose Encryption Algorithm type.



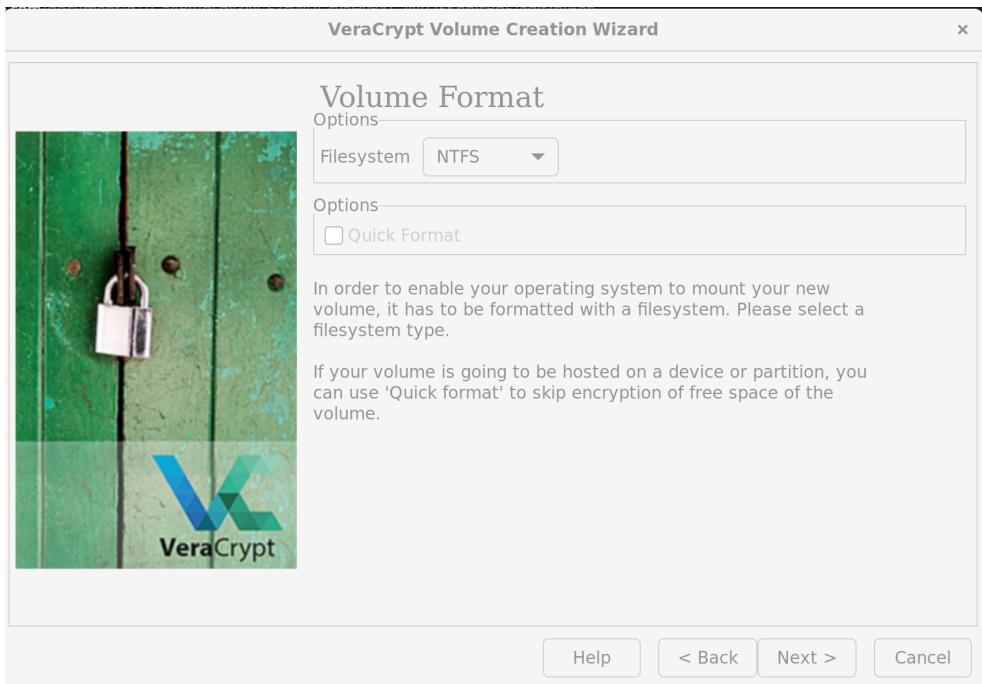
7. Select Volume size



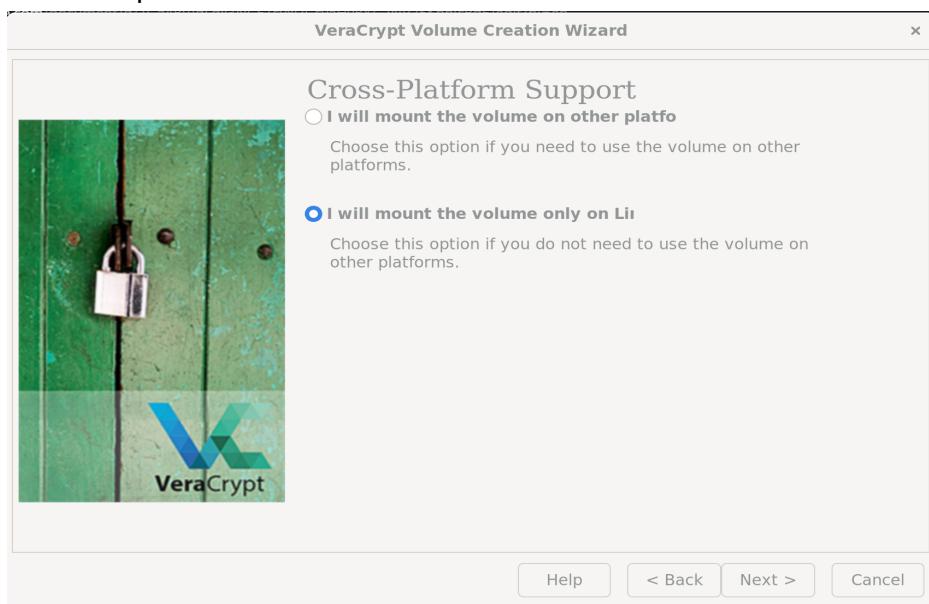
8. Create a password for the volume.



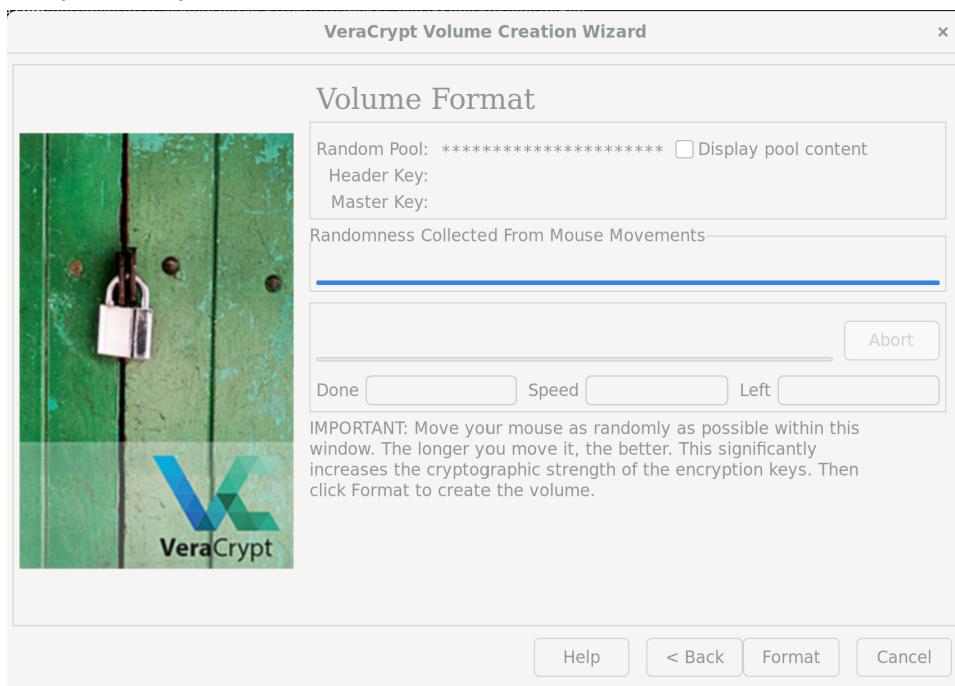
9. Select Volume format.



10. Choose a platform to mount the volume.



11. Randomly move the mouse pointer to increase the Cryptographic strength of the encryption key.



12. Enter password to authenticate the format request.

