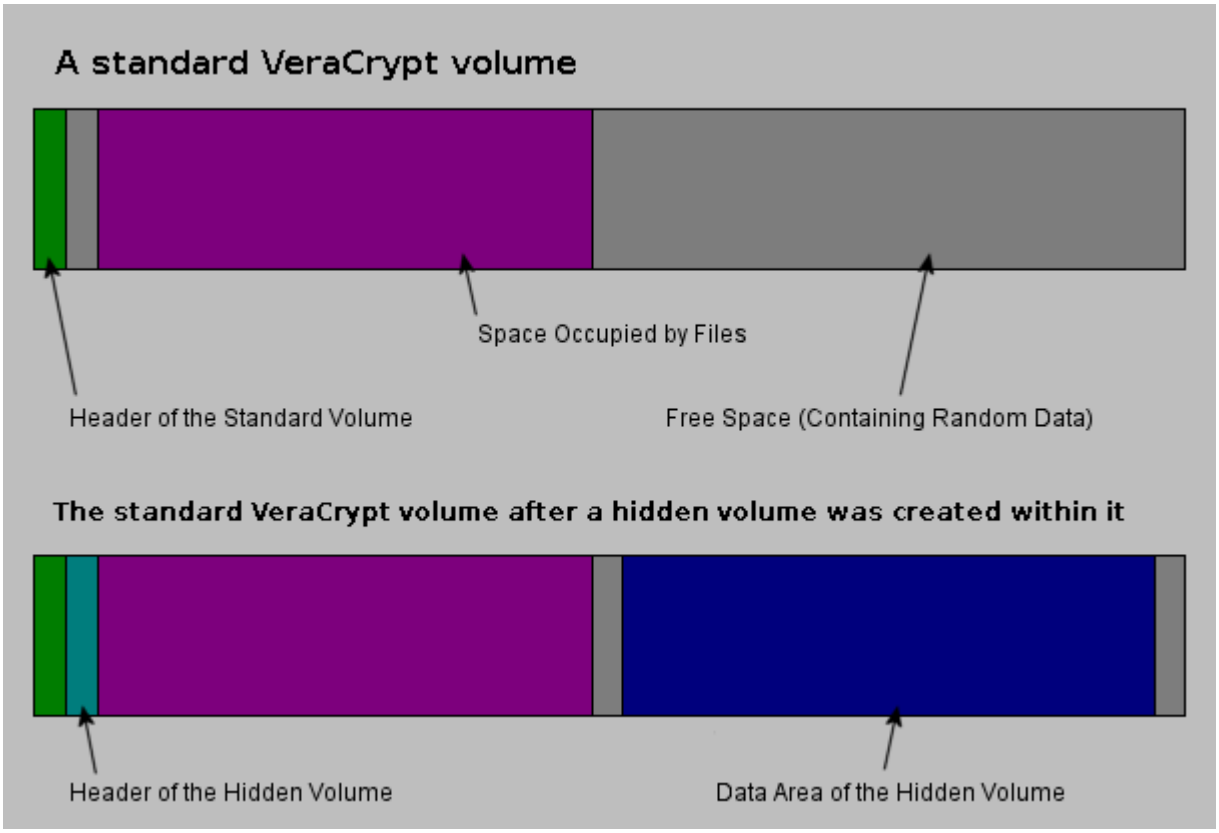
Hidden Volume

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.



The layout of a standard VeraCrypt volume before and after a hidden volume was created within it.

The principle is that a VeraCrypt volume is created within another VeraCrypt volume (within the free space on the volume). Even when the outer volume is mounted, it should be impossible to prove whether there is a hidden volume within it or not*, because free space on *any* VeraCrypt volume is always filled with random data when the volume is created** and no part of the (dismounted) hidden volume can be distinguished from random data. Note that VeraCrypt does not modify the file system (information about free space, etc.) within the outer volume in any way.

The password for the hidden volume must be substantially different from the password for the outer volume. To the outer volume, (before creating the hidden volume within it) you should copy some sensitive-looking files that you actually do NOT want to hide. These files will be there for anyone who would force you to

hand over the password. You will reveal only the password for the outer volume, not for the hidden one. Files that really are sensitive will be stored on the hidden volume.

A hidden volume can be mounted the same way as a standard VeraCrypt volume: Click *Select File* or *Select Device* to select the outer/host volume (important: make sure the volume is *not* mounted). Then click *Mount*, and enter the password for the hidden volume. Whether the hidden or the outer volume will be mounted is determined by the entered password (i.e., when you enter the password for the outer volume, then the outer volume will be mounted; when you enter the password for the hidden volume, the hidden volume will be mounted).

VeraCrypt first attempts to decrypt the standard volume header using the entered password. If it fails, it loads the area of the volume where a hidden volume header can be stored (i.e. bytes 65536–131071, which contain solely random data when there is no hidden volume within the volume) to RAM and attempts to decrypt it using the entered password. Note that hidden volume headers cannot be identified, as they appear to consist entirely of random data. If the header is successfully decrypted (for information on how VeraCrypt determines that it was successfully decrypted, see the section Encryption Scheme), the information about the size of the hidden volume is retrieved from the decrypted header (which is still stored in RAM), and the hidden volume is mounted (its size also determines its offset).

A hidden volume can be created within any type of VeraCrypt volume, i.e., within a file-hosted volume or partition/device-hosted volume (requires administrator privileges). To create a hidden VeraCrypt volume, click on *Create Volume* in the main program window and select *Create a hidden VeraCrypt volume*. The Wizard will provide help and all information necessary to successfully create a hidden VeraCrypt volume.

When creating a hidden volume, it may be very difficult or even impossible for an inexperienced user to set the size of the hidden volume such that the hidden volume does not overwrite data on the outer volume. Therefore, the Volume Creation Wizard automatically scans the cluster bitmap of the outer volume (before the hidden volume is created within it) and determines the maximum possible size of the hidden volume.***

If there are any problems when creating a hidden volume, refer to the chapter Troubleshooting for possible solutions.

Note that it is also possible to create and boot an operating system residing in a hidden volume (see the section Hidden Operating System in the chapter Plausible Deniability).

---

* Provided that all the instructions in the VeraCrypt Volume Creation Wizard have been followed and provided that the requirements and precautions listed in the subsection Security Requirements and Precautions Pertaining to Hidden Volumes are followed.
** Provided that the options *Quick Format* and *Dynamic* are disabled and provided that the volume does not contain a filesystem that has been encrypted in place (VeraCrypt does not allow the user to create a hidden volume within such a volume). For information on the method used to fill free volume space with random data, see chapter Technical Details, section VeraCrypt Volume Format Specification.
*** The wizard scans the cluster bitmap to determine the size of the uninterrupted area of free space (if there is any) whose end is aligned with the end of the outer volume. This area accommodates the hidden volume and therefore the size of this area limits the maximum possible size of the hidden volume. On Linux and Mac OS X, the wizard actually does not scan the cluster bitmap, but the driver detects any data written to the outer volume and uses their position as previously described.

Next Section >>