

Forum:[Hack Forums](#)

Thread: [\[VERACRYPT\] \(FDE\) Fully encrypt External HDD / Hidden Partition \(2K20\) \[EVADE L.E.A\]](#)

SIM-4581439 - April 6, 2020, 8:28 am

This tutorial will show you how to fully encrypt an external drive, specifically with a hidden volume. This process will be carried out by Veracrypt which can be found for download [here](#). A hidden volume works when a main volume is encrypted, but contains another volume inside of it, hidden in junk data. A hidden volume will contain two headers, one for the outer/dummy partition, and one for the inner/hidden partition. There are many benefits of using encrypted drives. One for basic privacy. If you house files on a USB or external HDD and you lose it (its easy to do, belive me) anyone could plug it in and snoop through your information. Encryption will make sure those files don't get into the wrong hands. Also, this works nicely in criminal investigations. Anyone who specializes in Digital Forensics can tell if a drive is encrypted. Hidden volumes in a drive work nicely in a court of law. You get caught doing something you weren't supposed to, you get taken to court, and you will be charged with obstruction (and most likely hit with the proceeding charges anyway) if you don't unlock the device. The dummy partition is used to store bogus files. Things that look innocent. Songs, family pictures, games, pornography, videos, whatever. The real 'hidden' volume is the drive containing all the spooky 1337 haX0r files. There is no way to tell if a drive contains a hidden partition by simply looking at it, virtually of course. So far this stands as a full-proof technology. So without further ado, let's begin...

Spoiler ([Click to View](#))

If you haven't already, download Veracrypt. Make sure it matches your system's architecture either x86 or x64. You will also want to install Veracrypt rather than to use the portable version as it has minor limitations. When done, open up Veracrypt.exe. You will see a button towards the left/middle of the program labeled "Create Volume;" click it. A window should open up asking you if you want to...Create an encrypted file container

Encrypt a non-system partition/drive

Encrypt the system partition or entire system drive

You will want to choose the Encrypt a non-system partition/drive option, and click NEXT.

Next you will see a two more options to create either a [i]Standard[/i] or Hidden Veracrypt volume. Clearly, you will want to select HIDDEN. Finally, you will be asked if you want to utilize Direct or Normal mode. Unless you already know what you're doing (you most likely wouldn't be reading this thread) select NORMAL MODE. So far, it should look like this:

At this point you will see a button labeled SELECT DEVICE, click this and find your external drive. You may see smaller listings underneath, however click on the topmost one (main partition). NOTE: If you have files on the drive you want to keep, you will need to back them up elsewhere until this process is complete. Here is an example:

Following this step you will begin the process of constructing the outer volume. You will have the choice of choosing two encryption algorithms, one for encryption, and one for hashing. For all intensive purposes, TWOFISH was chosen for encryption and WHIRLPOOL for hashing. Choose whichever encryption algorithm you put the most trust in. When in doubt, leave them at their defaults. Yours may look something like this:

You will be brought to a screen to choose the size of your outer volume. This is sort of redundant but the option to choose to size will be disabled since this is a 'full drive encryption' (FDE) and your not making just a volume container or single partition encryption. The following screen is where you will set the password for your outer/dummy volume. Make this something simple that you will remember. Again, this wont be where you place your sensitive files at. Something as simple as "password" will even do. There will be check boxes underneath the password fields. Leave these at their default.

The screen following will ask you if you want to store large files in your outer volume. In this tutorial, the option NO was left at default. If you want to store 4GB+ files and over in your dummy volume, then enable YES. This option is up to you. Finally, the next screen is where you will format and begin to encrypt your outer volume. You will be asked to move your mouse cursor around to generate a random encryption pool. When the progress bar is filled completely, click FORMAT. This may take a while depending on the size of your drive. So far, you should have this:

At this time you will need to wait for the outer volume to format and setup. This takes the most absorbent amount of time. You may be waiting over an hour depending on the drive size. In this tutorial, the USB being encrypted was 64GB and took roughly an hour to two hours. Be patient. Once its done formatting you will be ushered to another screen. Here the outer volume is complete and you will be asked to drop some dummy files in the directory by clicking the OPEN OUTER VOLUME button. Put in whatever you deem fit. You can always go back in and change these files later.

After this point it will be a rinse and repeat of the outer volume. You will move onto the hidden volume. You will be asked to choose an encryption and hashing algorithm. In this tutorial the algorithms for the hidden were the same as the outer volume. Next you will be asked to specify how much in size you want the hidden volume to be. If your entire drive is 60GB and you choose 50GB for your hidden volume, that means you only have 10GBs left in the outer volume even though it will say you have the whole 60GB free. If you go over this amount you can damage or overwrite your hidden files. Be mindful of this! Choose whatever size you want then continue. You will be asked after that to choose the password for your hidden volume. Make it complex, yet something you can definitely remember. Following this step you will be asked to choose if you want to store large files over 4GB in size. For all intensive purposes, in this tutorial I chose YES. Finally, you will be allowed to format your hidden volume. This will take less than half of the time the outer did. Here should be your process:

...and then once your drive is completely encrypted, you will see this message:

So there you go! You're all set. To access this drive, you open Veracrypt, click a random drive letter from the queue, then click the MOUNT button. A prompt will come up. To access the outer volume, enter in the outer volume passwords. The same logic applies for accessing the hidden volume. Cheers!

PS: I mentioned at the beginning of this thread that there is no way anyone would be able to truly know if you have a hidden volume. This is true...however, due to the nature of most operating systems, especially Windows OS, they hold data and leave traces. Certain Windows OS components like prefetch cache, icon cache, thumbs DB, shells bags, and windows event logs can severely work against you and let an oversight know that you've been accessing files from certain other components. I will be dropping a thread on anti-forensics and evasion soon, however it would behoove you to do independent research on these topics to better secure yourself.