Encrypt Your Flash Drive Using TrueCrypt

Note: Understand that to use TrueCrypt, you need to have administrative privileges [admin rights]. If you are a home user, then most likely, you are already running your PC as an administrator. At work, it might be a different story. Your system administrator has probably locked down your PC. The reason you need admin rights is because TrueCrypt loads a driver that enables the "on-the-fly" encryption. To load the driver, you need the administrative privileges. It does not matter that you are running TrueCrypt from your USB Flash Drive. It still loads the driver and you still need admin rights. So, if you are at work, on a PC that is locked down, then you'll need to have your system administrator install TrueCrypt on your PC in order for you to use your encrypted USB Flash Drive. If you plug your drive into a machine that requires administrative rights, and doesn't have TrueCrypt already installed, then you'll get a message stating "*In order to load the TrueCrypt driver, you need to be logged into an account with administrator privileges*". You can read about it on the TrueCrypt website here. Now that we got that out of the way, let's move on.

Introduction

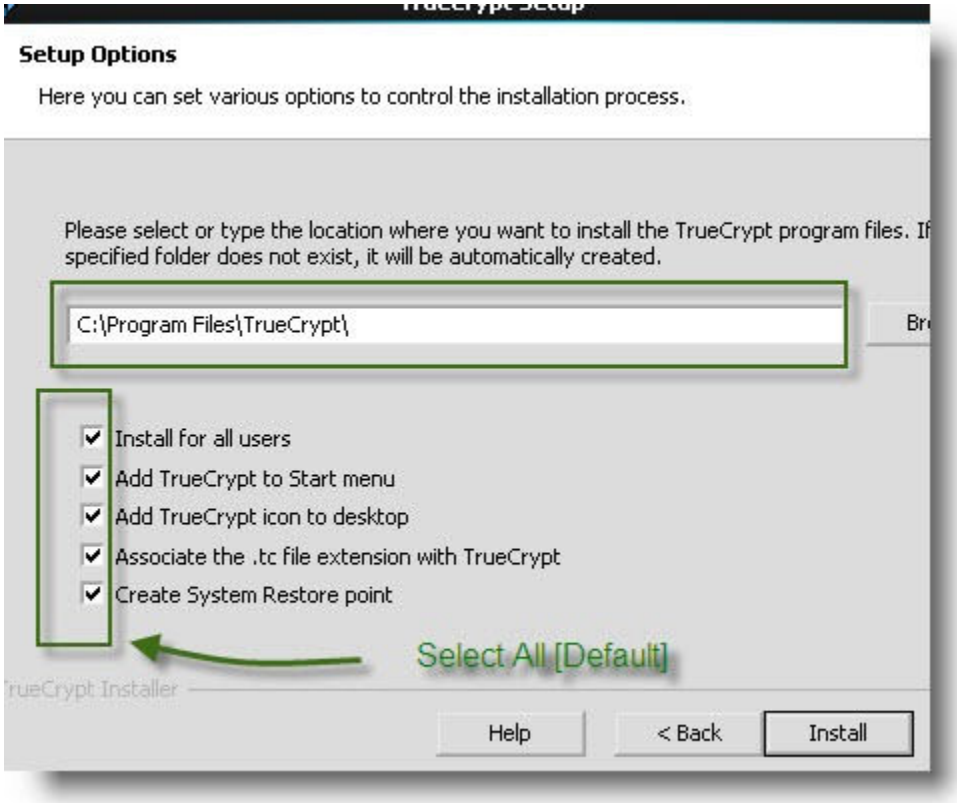
Portable USB flash drives are becoming cheaper and cheaper every day. Some companies are even giving them away. When they first arrived on the scene, most of the drives had a capacity of less than 1GB. But now, you can find 2GB to 4GB drives almost everywhere, including your local drugstore chain. At these sizes, they can actually be useful. You can use it to store your music, pictures, videos, or documents. Some even use it to store bootable operating systems like Linux. I use it to store a text file that contains the passwords for all of my online accounts, such as for my online bank accounts, my Amazon account, credit card accounts, etc. And since the flash drives are so portable, it makes sense to have one. However, since they *ARE* so portable, they can easily be lost, stolen, or misplaced. If you are like me, and store personal information on your flash drive, information that you don't want to fall into the wrong hands, then you need to encrypt your flash drive. By encrypting your flash drive, the files contained within it become password protected and can only be accessed by you or someone who knows your password. There are many different applications that help you encrypt your flash drive. Some drive manufacturers include encryption applications on the flash drive. In this tutorial, I will show you how to encrypt your portable USB flash drive using my favorite freeware application, TrueCrypt.

What Is TrueCrypt?

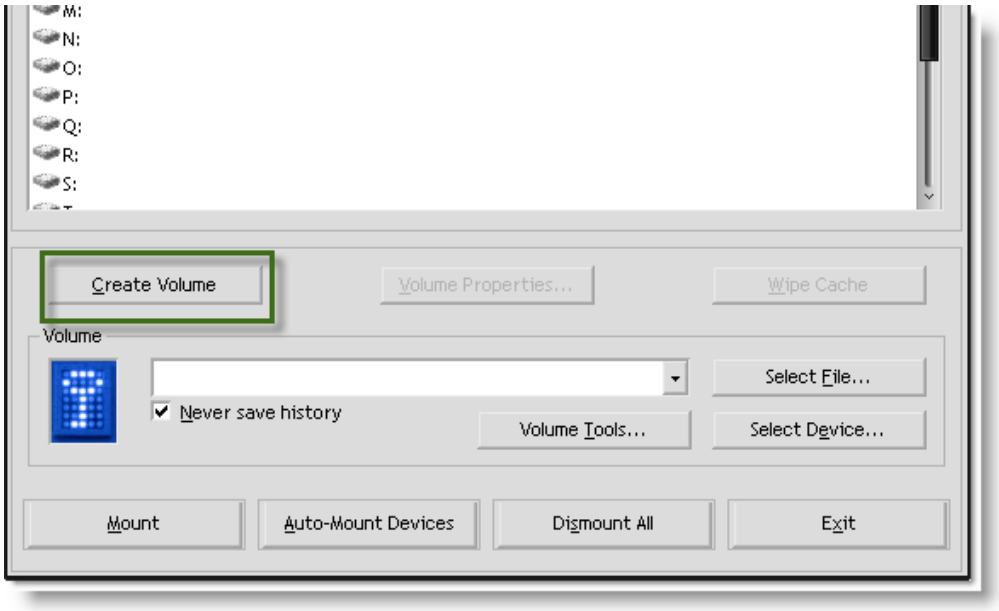
Using TrueCrypt, you create a password protected encrypted file that is stored on the flash drive. This encrypted file acts as a "container", within which all the files you want encrypted are stored. When you connect your flash drive into a PC, this "container" gets mounted as a separate hard drive (provided you enter the correct password). And now, everything you save into this separate hard drive is encrypted automatically. This is where TrueCrypt really shines, providing transparent, real-time encryption. Plus, you don't need TrueCrypt to be installed on the local computer [unless you don't have admin rights on your computer - see note above].

How To Encrypt Your Flash Drive Using TrueCrypt

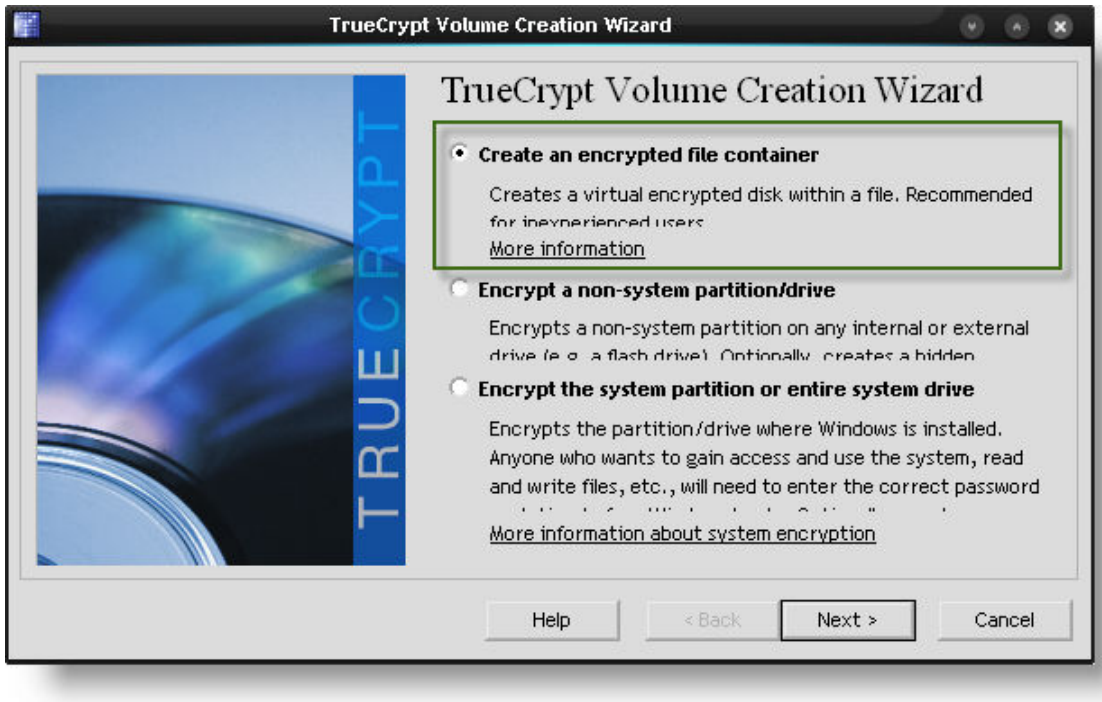
1. Download the latest stable version of TrueCrypt here: http://www.truecrypt.org/downloads.php
2. Install the software on your local computer (accepting all the default options)



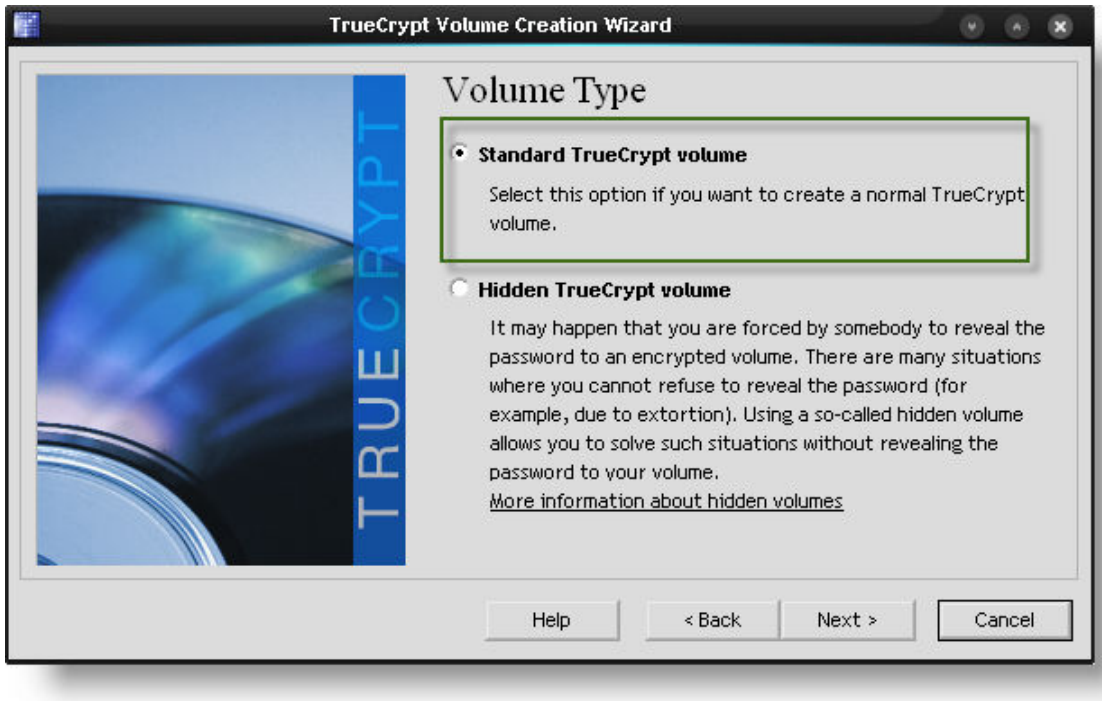
3. Connect your USB flash drive to your computer. For this tutorial, let's assume that it is assigned drive letter **G:**
4. Start the TrueCrypt application
5. Click on the **Create Volume** button to start the **TrueCrypt Volume Creation Wizard**. This is where you create the "container".



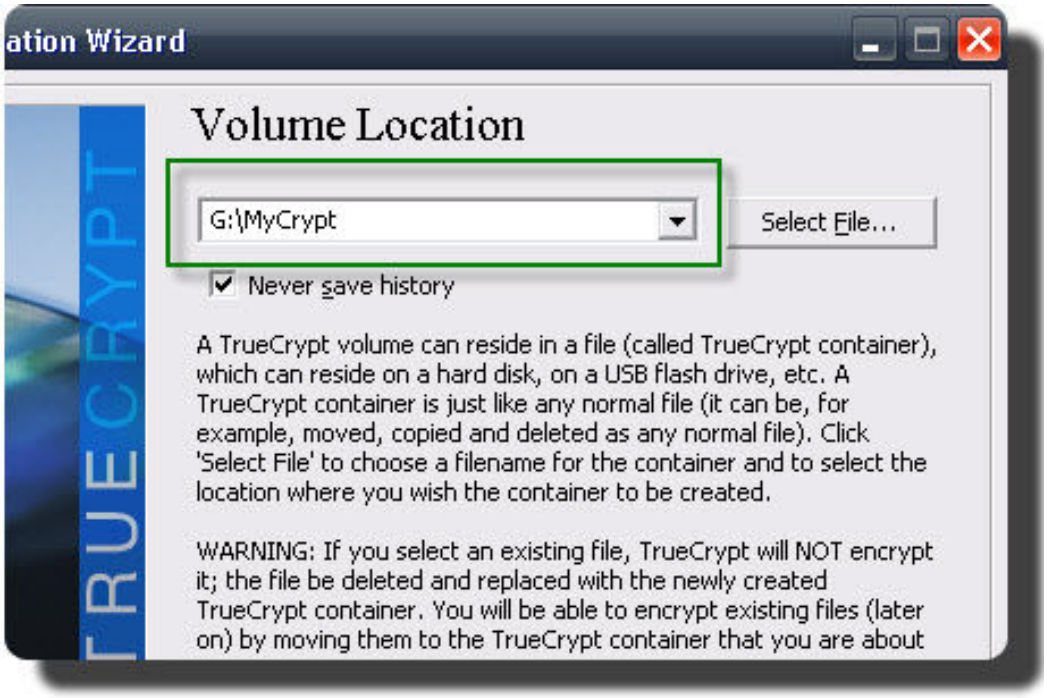
6. Select **Create an encrypted file container** (default option) and click on **Next**.



7. This brings you to the **Volume Type** window. Here you can specify if you want your "container" to be a standard, visible file or if you want to create a hidden "container" (essentially a "container" within a "container"). For this tutorial, we'll select the default option, **Standard TrueCrypt Volume**, and click on **Next**.

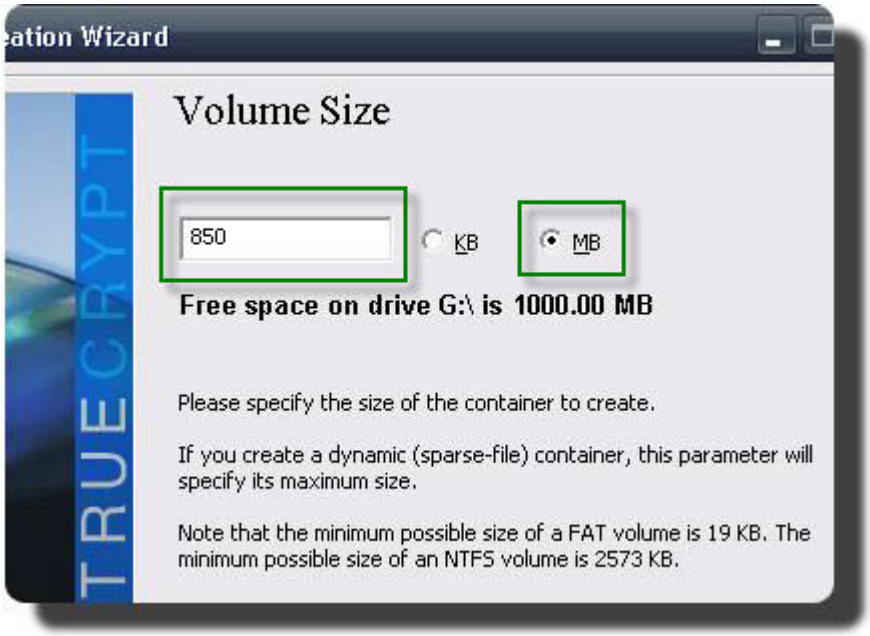


8. This brings you to the **Volume Location** window. Here you specify the filename and location of the "container". For this tutorial, let's call the container **MyCrypt**. And since your flash drive is mounted as the **G:** drive, specify your location and filename as **G:\MyCrypt**, placing the container in the root of the flash drive. Click **Next.**

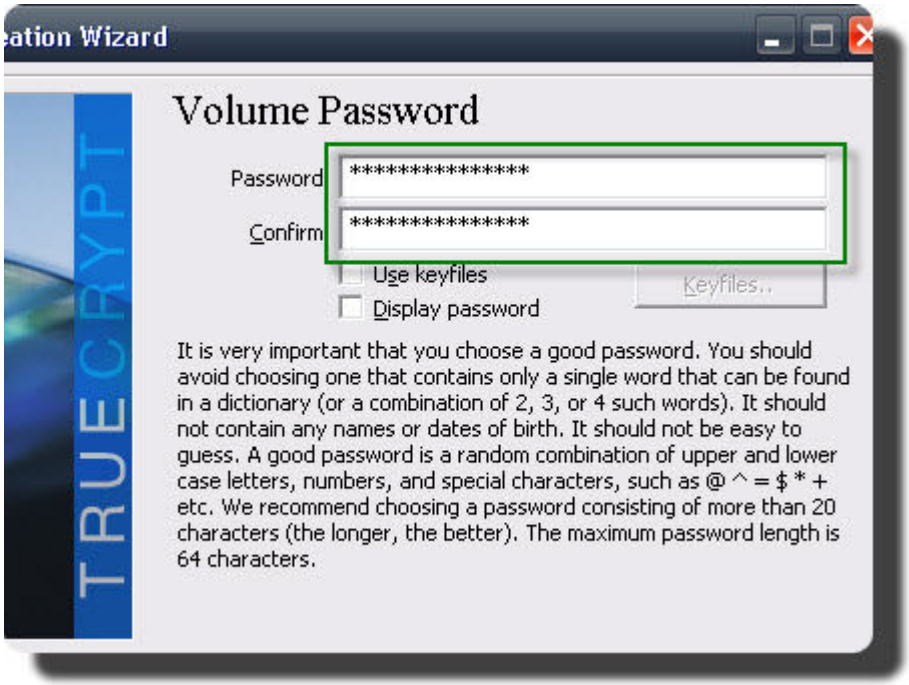


9. Next you need to select the **Encryption Algorithm** and **Hash Algorithm**. I won't go into the details of the differences between the different options, their pros and cons. That would turn this tutorial into a book. For this tutorial, we'll leave the defaults, as they should be sufficient. Click **Next.**

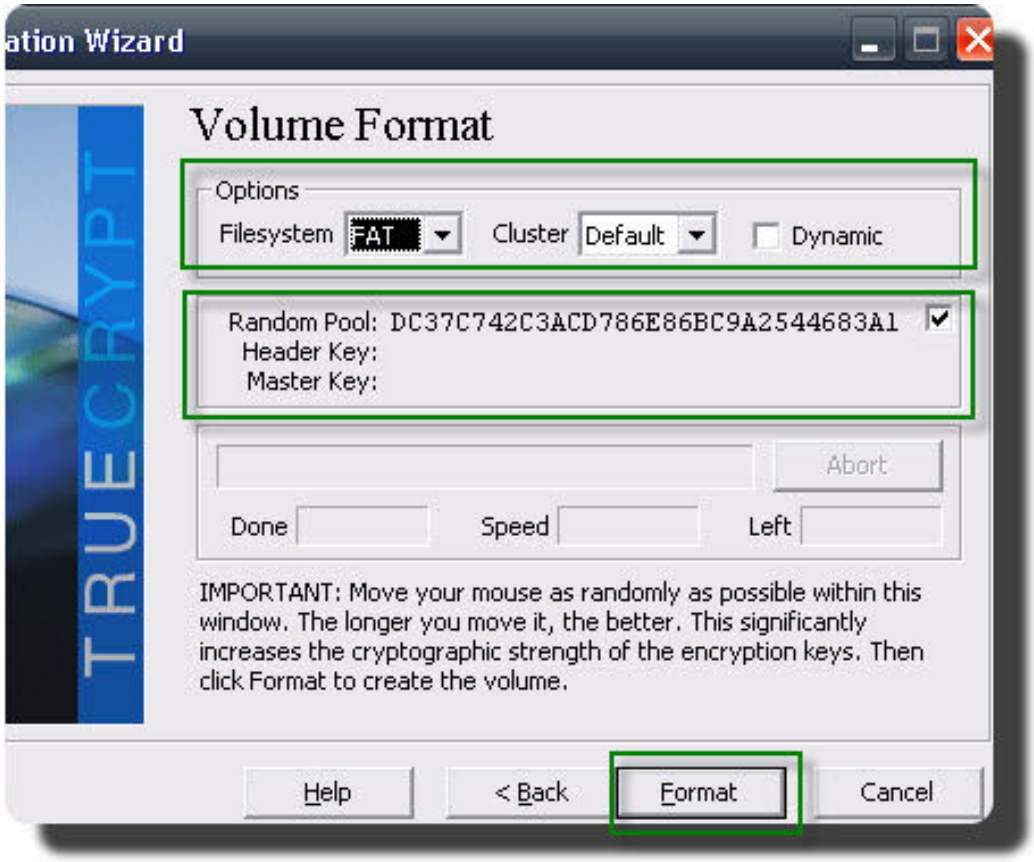
10. Next, you need to choose the size of the "container". This depends on the size of your flash drive and how much info you want to encrypt. Personally, I would suggest leaving anywhere between 10% to 20% of the drive unencrypted so that you have room for the TrueCrypt application files (about 6MB) as well as unimportant files that you might want to share or just don't need encrypted. For this tutorial, using a 1GB flash drive, we'll set the "container" to be 850MB. Click **Next.**



11. Next, specify the password you want to use to access and mount this "container". Select a strong password, that would be easy for you to remember and hard for anyone else to figure out. A strong password usually consists of at least 20 characters, and uses a combination of letters (both lower and upper case), and numbers. But at a minimum, it should consist of 8 characters. Click **Next** after you enter your password.

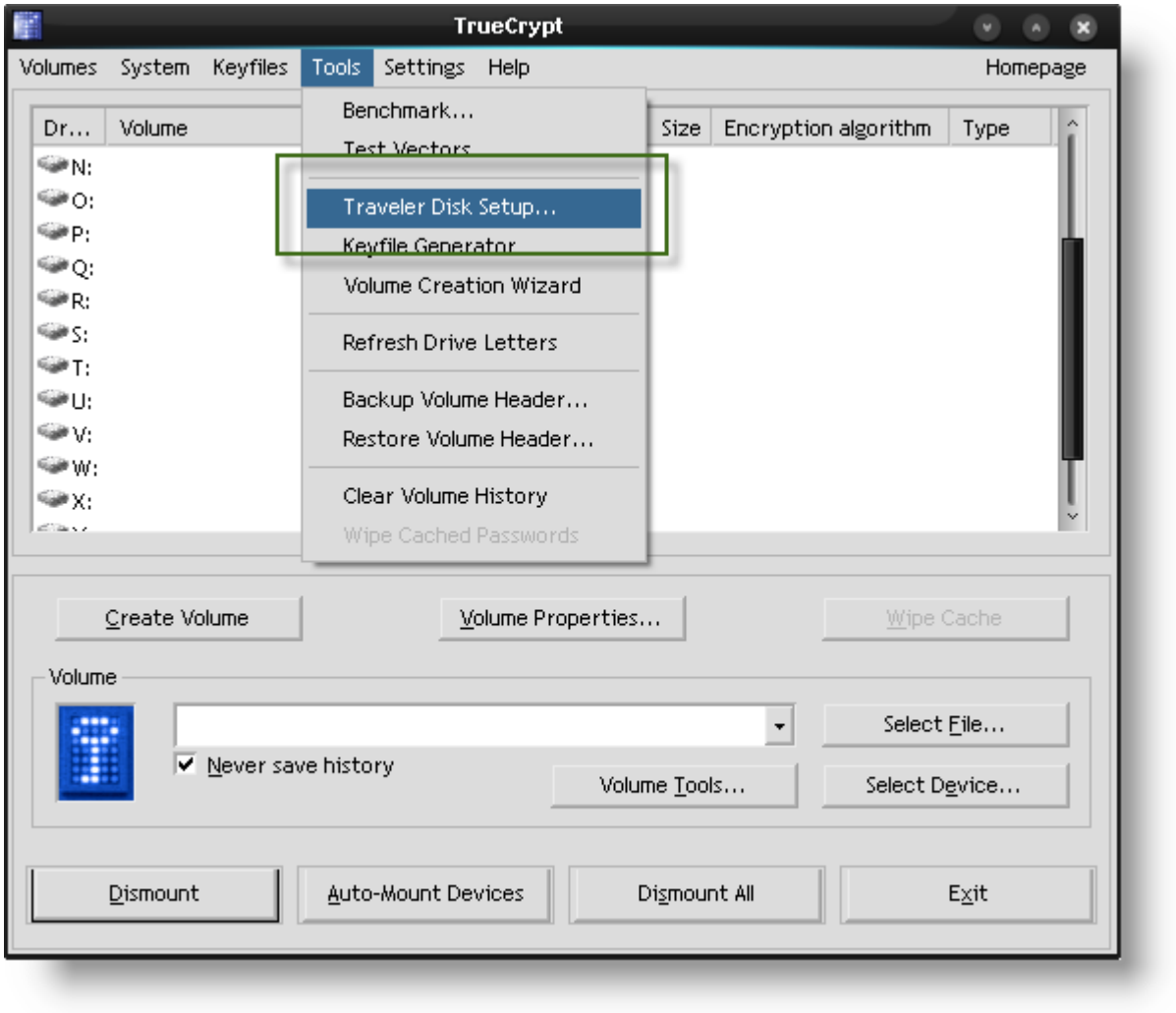


12. Next, you are ready to format the container. You can select the type of **File System** and **Cluster**. For this tutorial, leave the default values. Move your mouse randomly within the Volume Format window to generate the encryption keys. Don't worry; you are not going to have to remember these keys. When ready, click on **Format** to start. Depending on the size of the "container" (chosen in step 8), this may take up to 5 minutes.

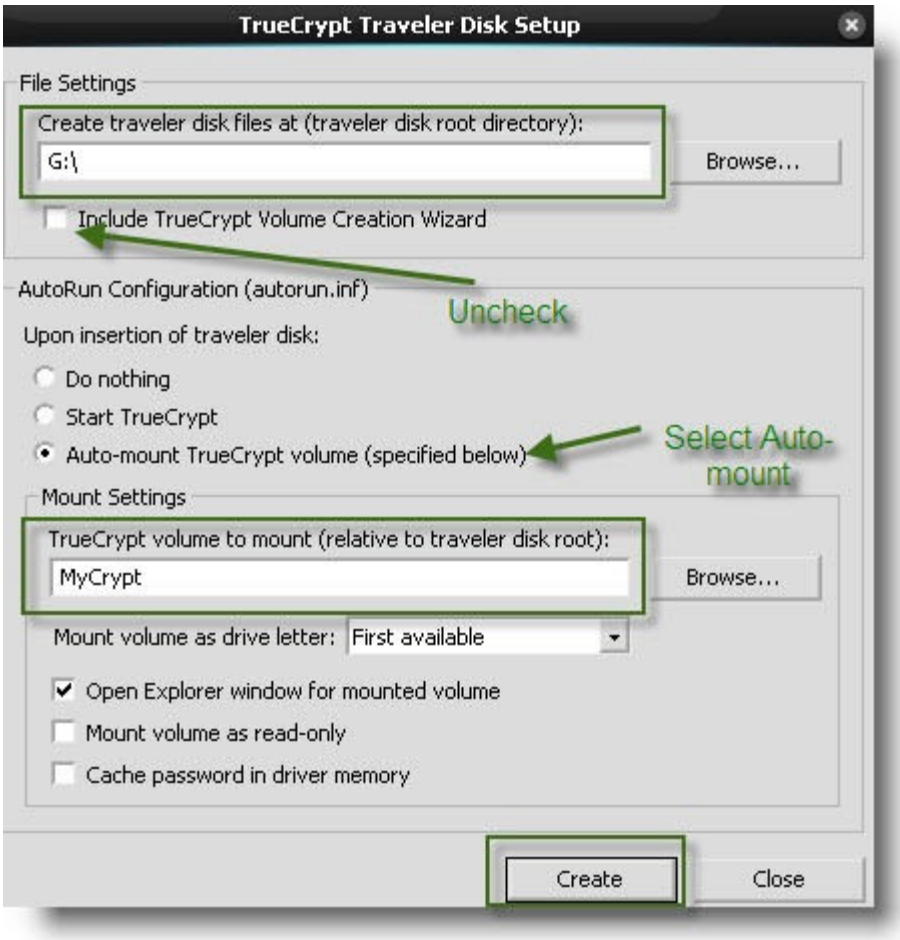


13. Once the format successfully completes, you will get a pop up indicating that the "container" has been created. Click **OK** then **Exit**.

14. From the main TrueCrypt window, select **Tools -> Traveler Disk Setup** to start the **Traveler Disk Setup Wizard**.

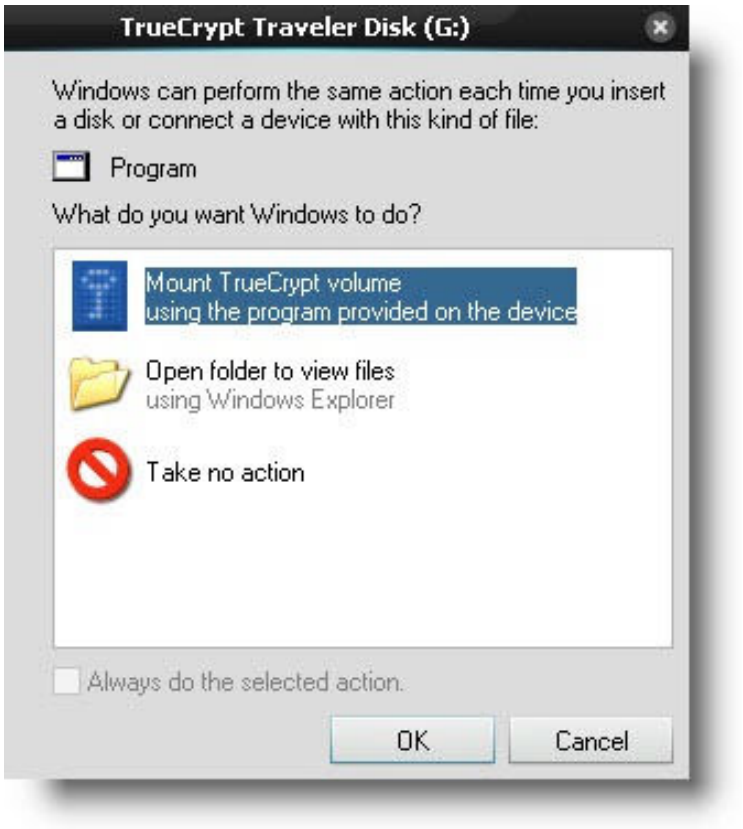


15. In the **Traveler Disk Setup Wizard**, we need to set several things. First, specify the root directory of the removable drive, in our case **G:**. Uncheck the "**Include TrueCrypt Volume Creation Wizard**" (we've already created the "container" called **MyCrypt** so we don't need the wizard). Next, select the "**Auto-mount TrueCrypt Volume**" button. This will allow you to be automatically prompted to mount the encrypted "container" when you insert your removable drive. Next, specify the name of the encrypted "container", in our case it's **MyCrypt**. Finally, click on **Create.**



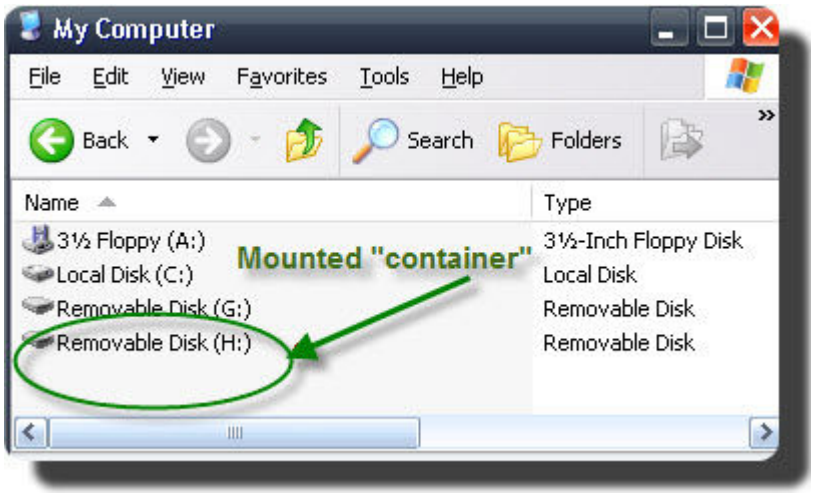
16. Once the Traveler Disk Setup is complete, you will get a confirmation popup:

17. Click **OK,** Close out of the **Traveler Disk Setup Wizard** and Exit the TrueCrypt application. That's it! Now, every time you connect your flash drive, you will be asked if you want to mount your encrypted "container". Select Mount TrueCrypt volume and click **OK.**

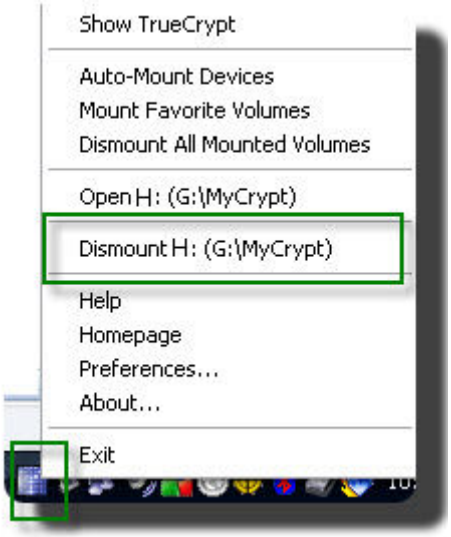


18. Next, you will be prompted to enter in the password you created for your encrypted "container". Enter your password and click **OK.**

19. Your encrypted “container” will be mounted as a drive using the next available drive letter. In this case, it is the H:\ drive.



20. Now, every time you put a file into the H:\ drive, it will be encrypted automatically. To “disconnect” the drive, right-click on the TrueCrypt icon in your taskbar and select Dismount:



Hopefully, I made the steps to create an encrypted drive easy. Having an encrypted drive will give you the assurance that if you lost your flash drive, the personal information stored in the encrypted drive will never be exposed.

Comments for this tutorial are welcomed!