How to Create and Use a TrueCrypt Container

This chapter contains step-by-step instructions on how to create, mount, and use a TrueCrypt volume.

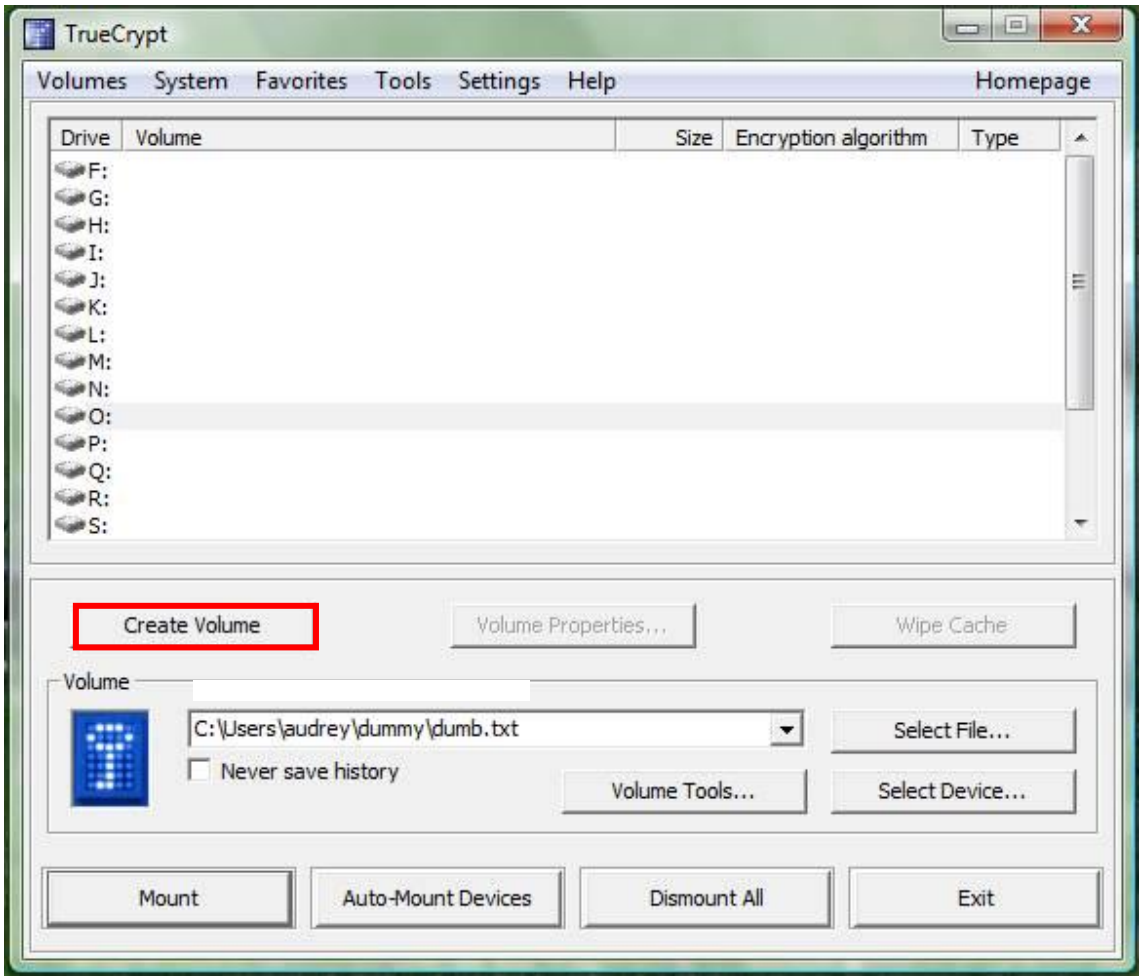
Step 1:

Download TrueCrypt from the ICT Security Portal (www.ictsecurity.sarawak.gov.my) under **Media > Downloads** tab. Download True Crypt (zip file) and extract the file.

Step 2:

Run and install TrueCrypt. Then launch TrueCrypt by double-clicking the file *TrueCrypt.exe* or by clicking the TrueCrypt shortcut in your Windows Start menu.

Step 3:



The main TrueCrypt window should appear. Click **Create Volume** (marked with a red rectangle for clarity).

Step 4:

The TrueCrypt Volume Creation Wizard window should appear.

In this step you need to choose where you wish the TrueCrypt volume to be created. A TrueCrypt volume can reside in a file, which is also called container, in a partition or drive. In this tutorial, we will choose the first option and create a TrueCrypt volume within a file.

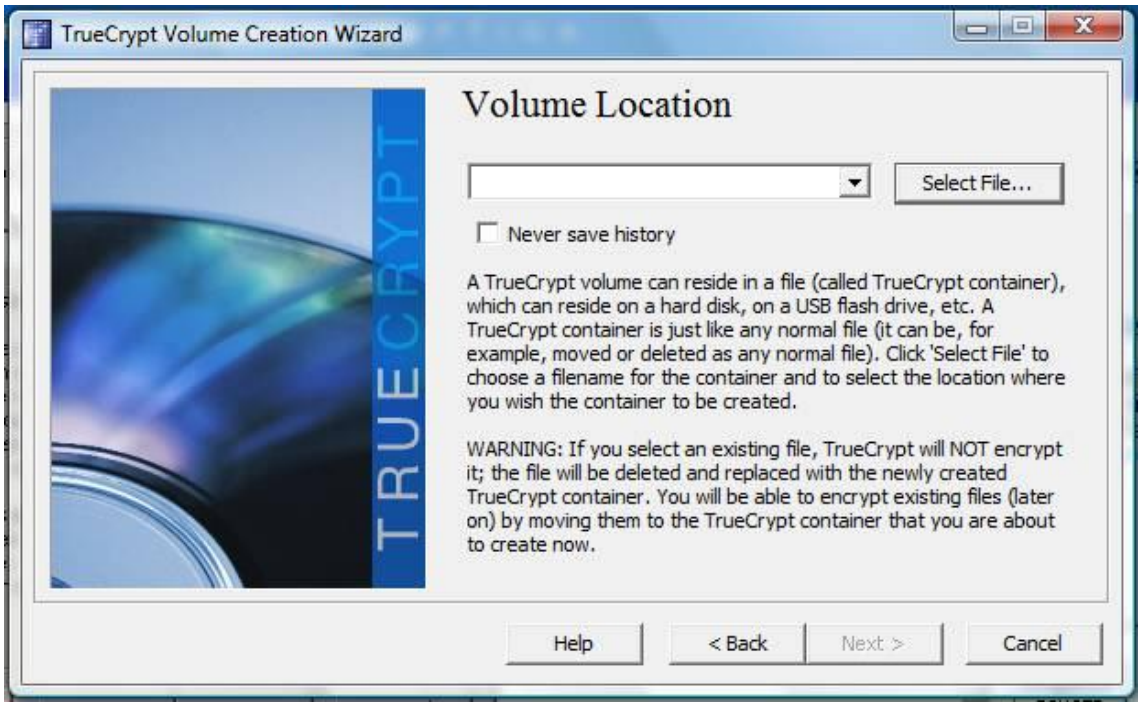
As the option is selected by default, you can just click **Next**.

Step 5:

In this step you need to choose whether to create a standard or hidden TrueCrypt volume. In this tutorial, we will choose the former option and create a standard TrueCrypt volume.

As the option is selected by default, you can just click **Next**.

Step 6:

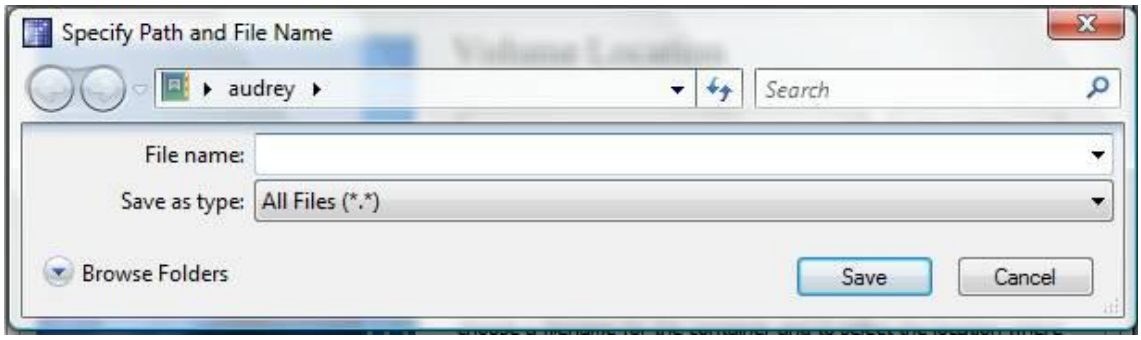


In this step you have to specify where you wish the TrueCrypt volume (file container) to be created. Note that a TrueCrypt container is just like any normal file. It can be, for example, moved or deleted as any normal file. It also needs a filename, which you will choose in the next step.

Click **Select File**.

The standard Windows file selector should appear (while the window of the TrueCrypt Volume Creation Wizard remains open in the background).

Step 7:



In this tutorial, we will create our TrueCrypt volume in the folder *D:\My Documents*\ and the filename of the volume (container) will be *My Volume* (as can be seen in the screenshot above). You may, of course, choose any other filename and location you like (for example, on a USB memory stick). Note that the file *My Volume* does not exist yet – TrueCrypt will create it.

IMPORTANT: **Note that TrueCrypt will *not* encrypt any existing files (when creating a TrueCrypt file container). If you select an existing file in this step, it will be overwritten and replaced by the newly created volume (so the overwritten file will be *lost*, *not* encrypted). You will be able to encrypt existing files (later on) by moving them to the TrueCrypt volume that we are creating now.***

Select the desired path (where you wish the container to be created) in the file selector.

Type the desired container filename in the **File name** box.

Click **Save**.

The file selector window should disappear.

Step 8:

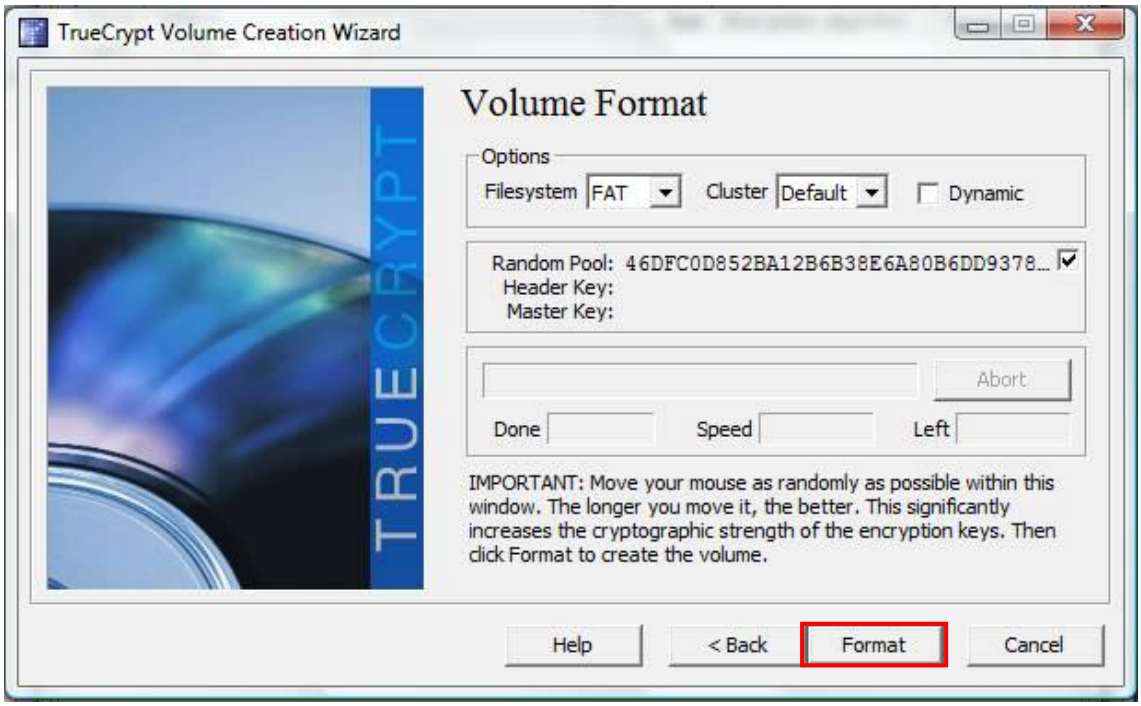
Accept the default setting, set the **Volume Size** of the file container, and set the **Volume Password** to access the file container once it is created.

This is one of the most important steps. Here you have to choose a good volume password.
Read carefully the information displayed in the Wizard window about what is considered a good password.

After you choose a good password, type it in the first input field. Then re-type it in the input field below the first one and click **Next**.

Note: The button **Next** will be disabled until passwords in both input fields are the same.

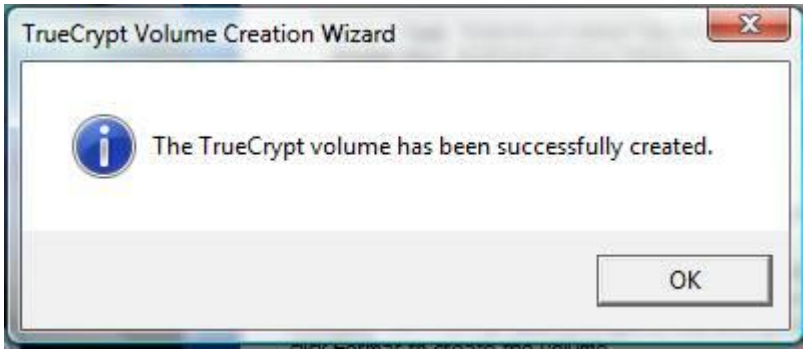
Step 9:



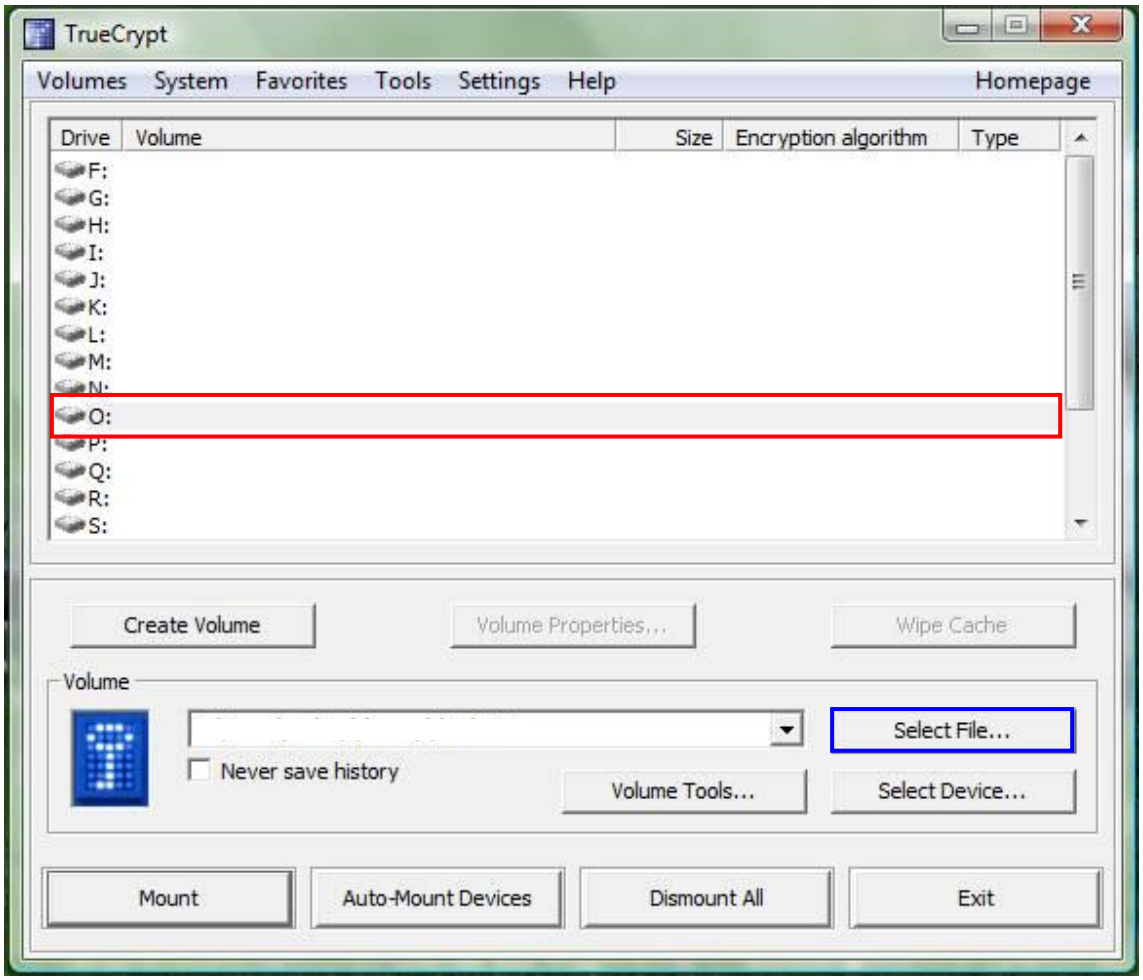
Move your mouse as randomly as possible within the Volume Creation Wizard window at least for 30 seconds. The longer you move the mouse, the better. This significantly increases the cryptographic strength of the encryption keys (which increases security).

Click **Format**.

Volume creation should begin. TrueCrypt will now create a file called *My Volume* in the folder *D:\My Documents*\ (as we specified in Step 6). This file will be a TrueCrypt container (it will contain the encrypted TrueCrypt volume). Depending on the size of the volume, the volume creation may take a long time. After it finishes, the following dialog box will appear:

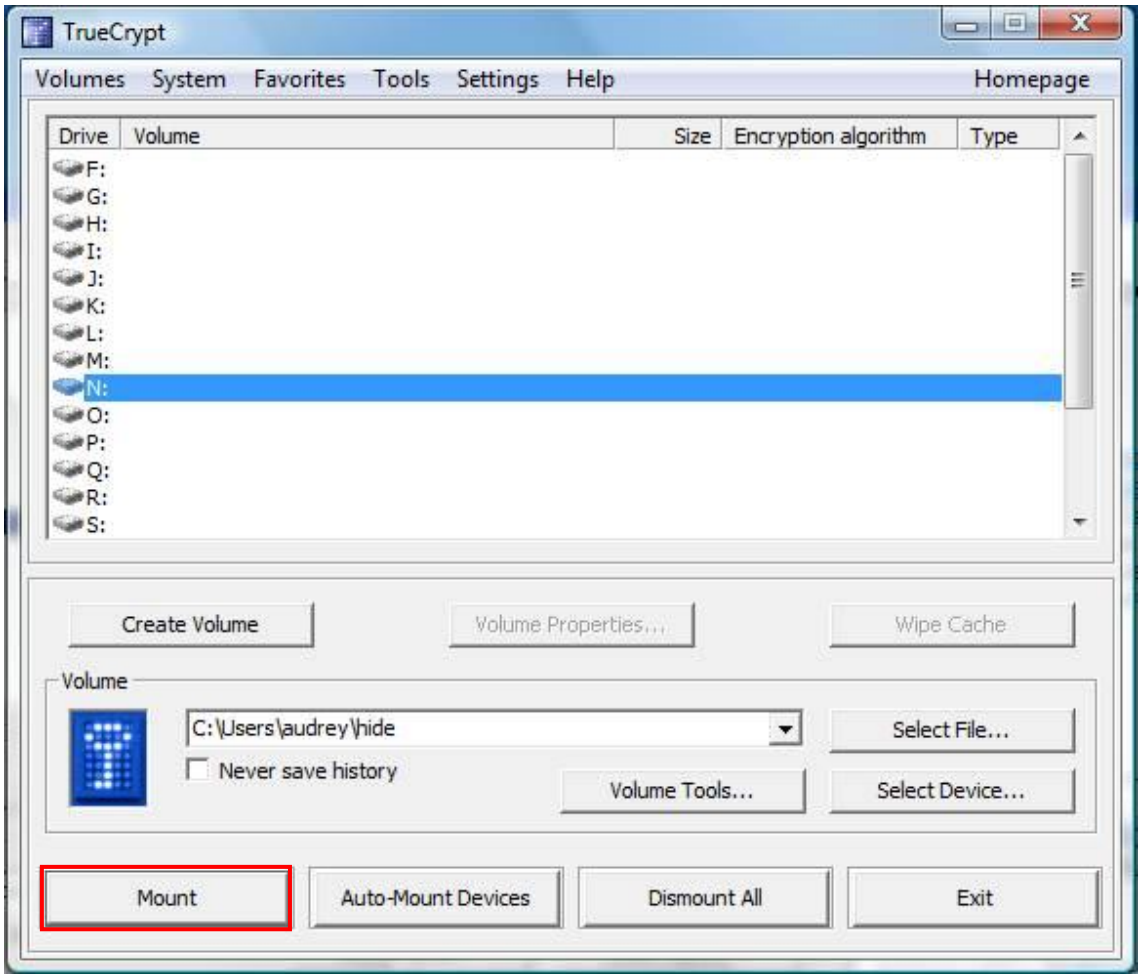


Step 10:



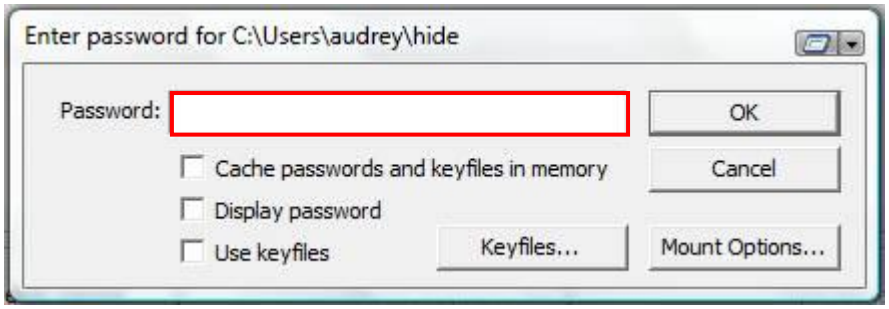
Select a drive letter from the list (marked with a red rectangle). This will be the drive letter to which the TrueCrypt container will be mounted. After select a drive letter, click on **Select File** (marked with blue rectangle) to select the file that was created on **Step 6**.

Step 11:



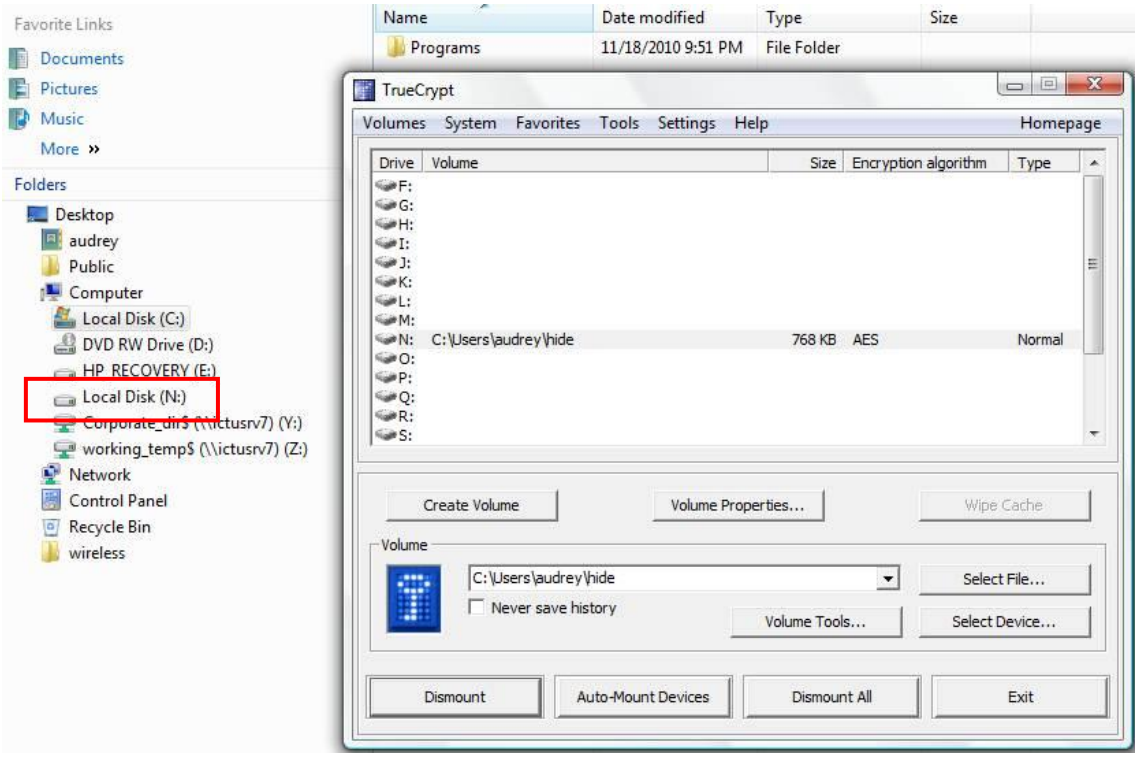
In the main TrueCrypt window, click **Mount**.

Password prompt dialog window should appear.



Type the password (which you specified in **Step 7**) in the password input field (marked with a red rectangle).

Step 12:

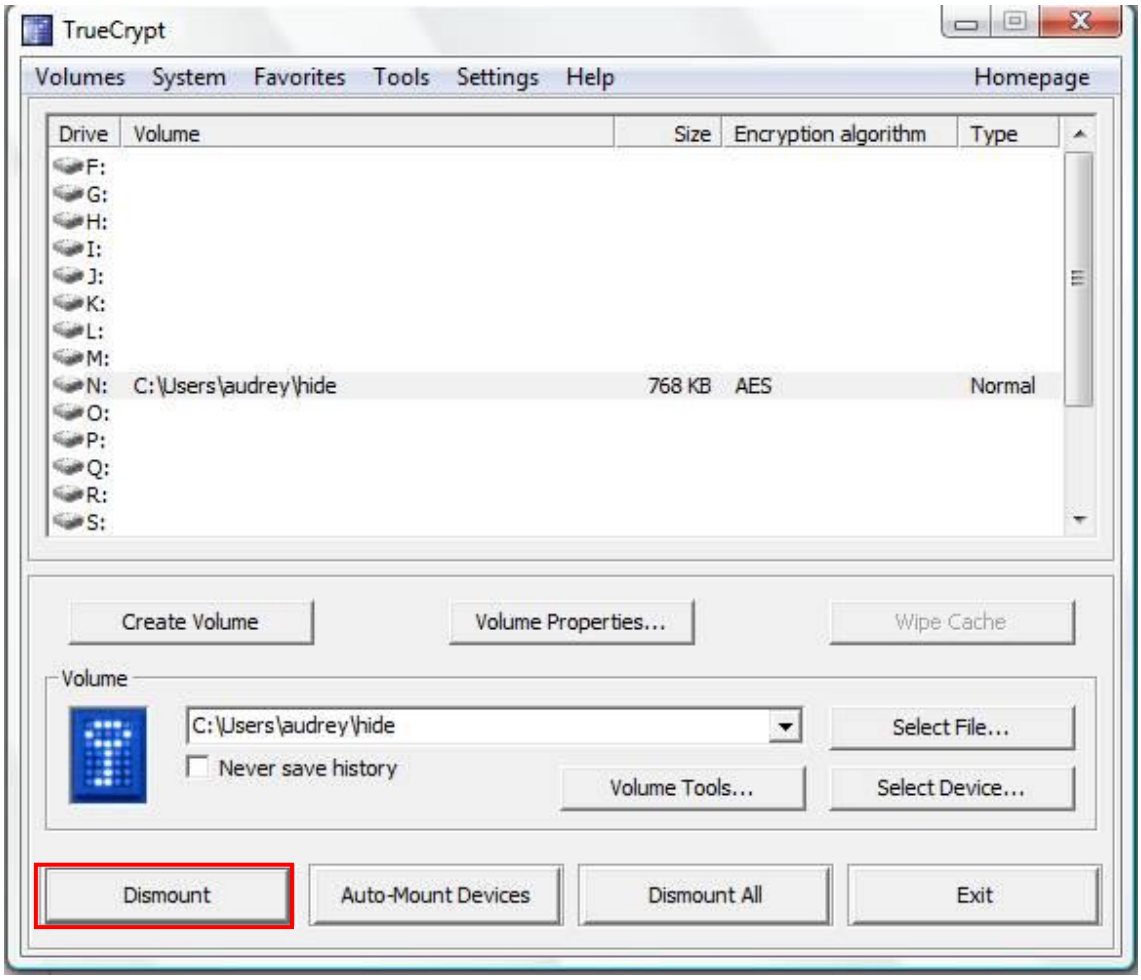


You can copy files to and from the TrueCrypt volume just as you would copy them to any normal disk (for example, by simple drag-and-drop operations). Files that are being read or copied from the encrypted TrueCrypt volume are automatically decrypted on the fly (in memory/RAM). Similarly, files that are being written or copied to the encrypted TrueCrypt volume are automatically encrypted on the fly (right before they are written to the disk) in RAM.

Note that TrueCrypt never saves any decrypted data to a disk – it only stores them temporarily in RAM (memory). Even when the volume is mounted, data stored in the volume is still encrypted. When you restart Windows or turn off your computer, the volume will be dismounted and all files stored on it will be inaccessible (and encrypted). Even when power supply is suddenly interrupted (without proper system shut down), all files stored on the volume will be inaccessible (and encrypted). To make them accessible again, you have to mount the volume. To do so, repeat Steps 9-10

Step 13:

If you want to close the volume and make files stored on it inaccessible, either restart your operating system or dismount the volume. To do so, follow these steps:



Select the volume from the list of mounted volumes in the main TrueCrypt window (marked with a red rectangle in the screenshot above) and then click **Dismount** (also marked with a red rectangle in the screenshot above). To make files stored on the volume accessible again, you will have to mount the volume. To do so, repeat Steps 9-10.