**Tools**

*These links are for your use only, as sources of images used below if they are not high quality enough in this doc.*

1. Adium tool guide [– Link](https://ssd.eff.org/en/module/how-use-otr-mac)
2. Basic Security Setup for Android - [Link](https://securityinabox.org/android_basic)
3. ChatSecure tool guide - [Link](https://ssd.eff.org/en/module/how-install-and-use-chatsecure)
4. Cobian Backup Guide - [Link](https://securityinabox.org/cobian_main)
5. How to change your Facebook privacy settings - [Link](https://www.eff.org/deeplinks/2013/01/how-protect-your-privacy-facebooks-graph-search)
6. How to opt-out of Facebook's data broker relationships – [Link](https://www.eff.org/deeplinks/2013/02/howto-opt-out-databrokers-showing-your-targeted-advertisements-facebook)
7. How to opt-out of Twitter's data broker relationships – [Link](https://www.eff.org/deeplinks/2013/07/how-opt-out-twitters-tailored-advertisements-and-more)
8. Jitsi Tool guide – [Link](https://securityinabox.org/jitsi)
9. K9 & APG tool guide – [Link](https://securityinabox.org/k9_apg_main)
10. KeePassX tool guide – [Link](https://www.keepassx.org/screenshots/)
11. ObscuraCam Tool guide – [Link](https://securityinabox.org/obscuracam_main)
12. Orbot & Orweb tool guide – [Link](https://securityinabox.org/Orbot_main), [Link](https://securityinabox.org/orweb_main)
13. PGP for Linux tool guide – [Link](https://ssd.eff.org/en/module/how-use-pgp-linux)
14. PGP for Mac O SX tool guide – [Link](https://ssd.eff.org/en/module/how-use-pgp-mac-os-x)
15. PGP for Windows tool guide – [Link](https://ssd.eff.org/en/module/how-use-pgp-windows-pc)
16. Pidgin tool guide – [Link](https://ssd.eff.org/en/module/how-use-otr-windows)
17. Psiphon3 tool guide – [Link](https://www.level-up.cc/leading-trainings/training-curriculum/deepening/psiphon3)
18. Recuva – File Recovery Guide – [Link](https://securityinabox.org/recuva_main)
19. Redphone Tool guide – [Link](https://ssd.eff.org/en/module/how-use-redphone-android)
20. Signal Tool guide – [Link](https://ssd.eff.org/en/module/how-use-signal-%E2%80%93-private-messenger)
21. TextSecure tool guide – [Link](https://ssd.eff.org/en/module/how-use-textsecure-android)
22. Tor for Mac tool guide – [Link](https://www.torproject.org/projects/torbrowser.html.en#macosx)
23. Tor for Windows tool guide – [Link](https://ssd.eff.org/en/module/how-use-tor-windows#overlay=en/node/57/)
24. TrueCrypt Tool Guide – [Link](https://securityinabox.org/truecrypt_main)

**TOR FOR MAC TOOL GUIDE**

# ****Tor for Mac**** Tool Guide

**Lesson to read: The Internet**

**This guide outlines how to use the [Tor Browser Bundle](https://www.torproject.org/projects/torbrowser.html.en" \t "_blank) on Mac.**

**Computer requirements:** An internet connection, a computer running Mac OS X

**Version used in this guide:** Tor Browser Bundle: 3.6.2

**License:** Free Software; mix of Free Software licenses

**Level:**Intermediate

**Other reading**: <https://tor.stackexchange.com/>

**Time required:** 15-30 minutes

**Using Tor will give you**:

* The ability to get around internet censorship
* The ability to get online anonymously

**1.0 Before you start**

Tor is a volunteer-run service that provides both privacy and anonymity online by masking who you are and where you are connecting. The service also protects you from the Tor network itself.

For people who might need occasional anonymity and privacy when accessing websites, Tor Browser provides a quick and easy way to use the Tor network.

The easiest way to use the Tor network is to use the Tor Browser Bundle, which combines a web browser, the Tor software, and other helpful software that will give you a way of more securely accessing the web.

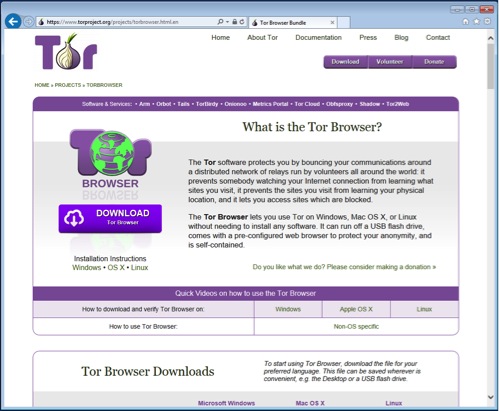
The Tor Browser works just like other web browsers, except that it sends your communications through Tor, making it harder for people who are monitoring you to know exactly what you're doing online, and harder for people monitoring the sites you use to know where you're connecting from. Keep in mind that only activities you do inside of Tor Browser itself will be anonymised. Having Tor Browser installed on your computer does not make things you do on the same computer using other software (such as your regular web browser) anonymous.

## 2.0 Getting Tor Browser Bundle

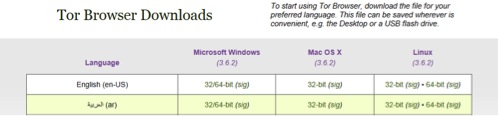
Open a browser like Mozilla Firefox or Internet Explorer and type: <https://www.torproject.org/projects/torbrowser.html.en> in the URL bar. If you are using a search engine to look for the Tor Browser Bundle, make sure that the URL is correct.

ow to Use Tor 1

Click the big purple download button to get the installation program for Tor Browser Bundle.



The website will have detected your operating system and you'll get the correct file for Windows. If, for any reason, you want a different installer file you can scroll down to the Tor Browser Downloads section.



Many browsers will ask you to confirm whether you want to download this file.

For any browser, it is best to save the file first before proceeding. So click the Save button.

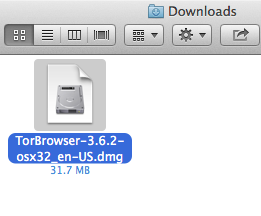
## 2.1 Installing Tor Browser Bundle

## After the download is complete, you might get an option to open the folder where the file was downloaded to. The default location is the Downloads folder.

Double-click on the Tor Browser installer. This opens the .dmg file.

(On recent versions of OS X, you might get a warning that it's from an "unidentified developer" — you can get around this complaint by control-clicking and selecting "open".)

Drag the included file into your Applications folder and you will have a Tor Browser application in your chosen language that you can pin on your Dock.

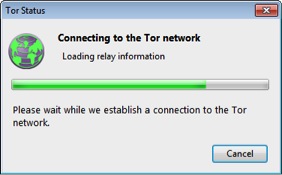


### Starting Tor Browser for the first time

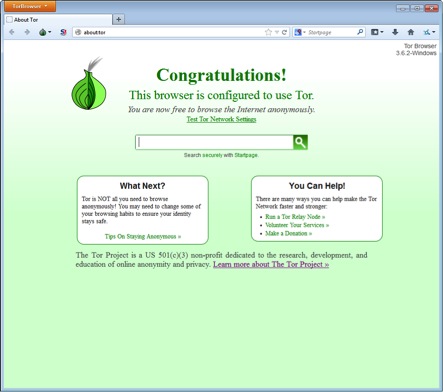
Open the Tor Browser folder from your Applications folder and double click on the file called Tor Browser.

The first time Tor Browser starts, you may get a window that allows you to modify some settings if necessary. You might have to come back and change some configuration settings, but go ahead and try to connect to the Tor network by clicking the Connect button.

After clicking the connect button, a new window will open with a green bar that will get longer as the Tor software starts up.



The first time Tor Browser starts it might take a bit longer than usual, but be patient, within a few minutes Tor Browser will be done and a web browser opens up congratulating you.



**TOR FOR WINDOWS TOOL GUIDE**

# ****Tor for Windows**** Tool Guide

# Online Anonymity and Circumvention

**Lesson to read: The Internet**

**This guide outlines how to use the [Tor Browser Bundle](https://www.torproject.org/projects/torbrowser.html.en" \t "_blank) on Windows.**

**Computer requirements:** An internet connection, a computer running Windows

**Version used in this guide:** Windows: Windows 7 Ultimate; Tor Browser Bundle: 3.6.2

**License:** Free Software; mix of Free Software licenses

**Level:**Intermediate

**Other reading**: <https://tor.stackexchange.com/>

**Time required:** 15-30 minutes

**Using Tor will give you**:

* The ability to get around internet censorship
* The ability to get online anonymously

**1.0 Before you start**

Tor is a volunteer-run service that provides both privacy and anonymity online by masking who you are and where you are connecting. The service also protects you from the Tor network itself.

For people who might need occasional anonymity and privacy when accessing websites, Tor Browser provides a quick and easy way to use the Tor network.

The easiest way to use the Tor network is to use the Tor Browser Bundle, which combines a web browser, the Tor software, and other helpful software that will give you a way of more securely accessing the web.

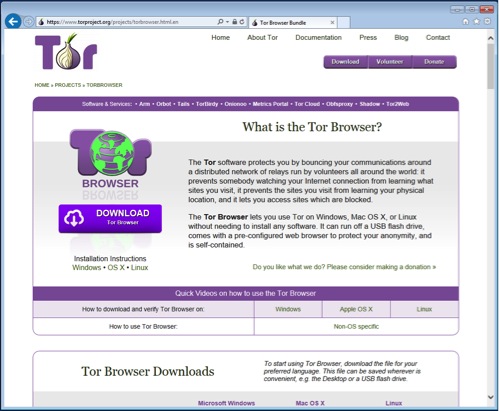
The Tor Browser works just like other web browsers, except that it sends your communications through Tor, making it harder for people who are monitoring you to know exactly what you're doing online, and harder for people monitoring the sites you use to know where you're connecting from. Keep in mind that only activities you do inside of Tor Browser itself will be anonymised. Having Tor Browser installed on your computer does not make things you do on the same computer using other software (such as your regular web browser) anonymous.

## 2.0 Getting Tor Browser Bundle

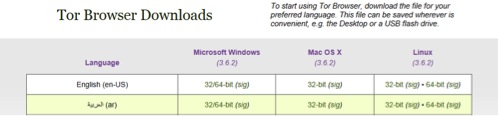
Open a browser like Mozilla Firefox or Internet Explorer and type: <https://www.torproject.org/projects/torbrowser.html.en> in the URL bar. If you are using a search engine to look for the Tor Browser Bundle, make sure that the URL is correct.

ow to Use Tor 1

Click the big purple download button to get the installation program for Tor Browser Bundle.



The website will have detected your operating system and you'll get the correct file for Windows. If, for any reason, you want a different installer file you can scroll down to the Tor Browser Downloads section.



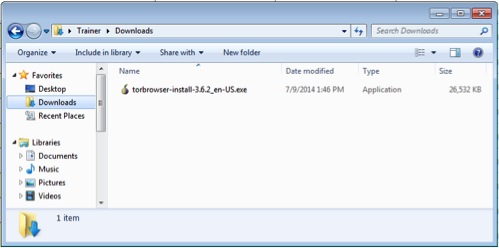
Many browsers will ask you to confirm whether you want to download this file. Internet Explorer 11 shows a bar at the bottom of the browser window with an orange border.

ow to Use Tor 4

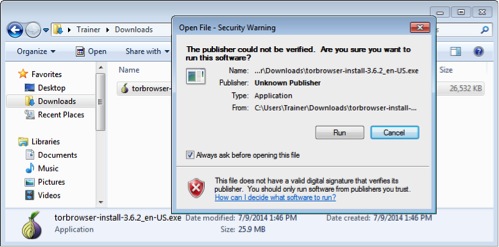
For any browser, it is best to save the file first before proceeding. So click the Save button. This example shows Tor Browser Bundle version 3.6.2, which was the current version at the time we wrote this. There will probably be a more recent version available for download by the time you read this.

## 2.1 Installing Tor Browser Bundle

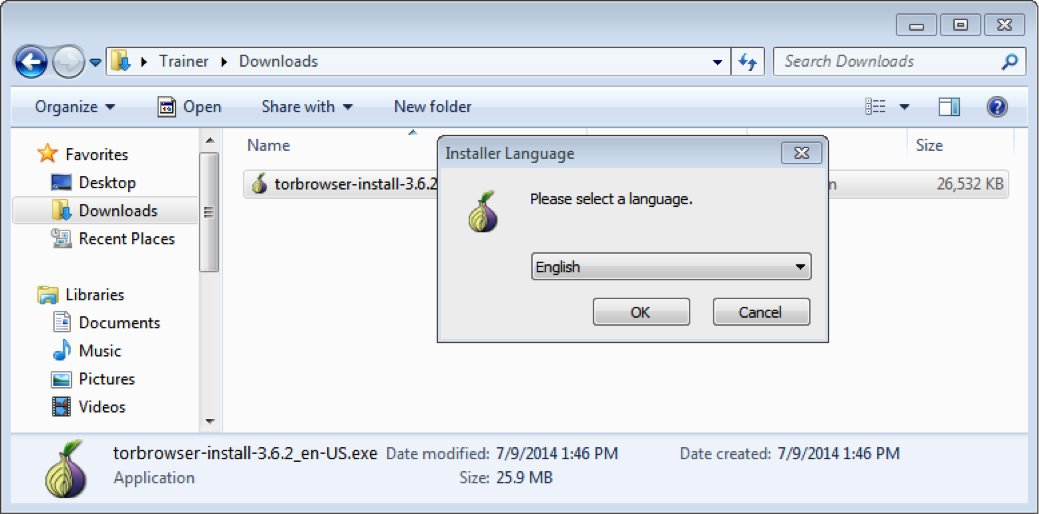
After the download is complete, you might get an option to open the folder where the file was downloaded to. The default location is the Downloads folder. Double-click on the file torbrowser-install-3.6.2\_en-US.exe



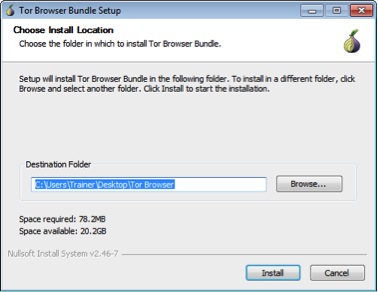
After double-clicking on the Tor Browser installer, a window will open with a warning about the origin of the software. You should always take these warnings seriously and make sure you trust the software you want to install and that you got an authentic copy from the official site over a secure connection. Since you know what you want, and you know where to get the software, and the download was from the Tor Project's secure HTTPS site, go ahead and click Run.



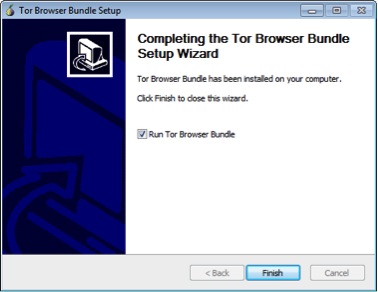
A small window will open asking what language you want to use for the Tor Browser Bundle. There are several to choose from. Pick the language you want and click the OK button.



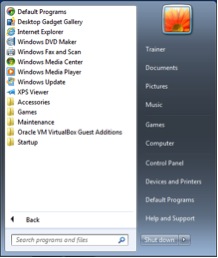
You'll find a new window that will tell you where the Tor Browser Bundle will be installed. The default location is your desktop. You can change this to be a different location if you want, but for now keep the default.



The installation process is complete when you see a window that says you have completed the installation process. If you click the Finish button, the Tor Browser will start immediately. For now, uncheck the box by “Run Tor Browser Bundle.” We'll come back to using Tor Browser Bundle in a bit. If you missed unchecking the checkbox and Tor Browser starts, just close the window for now.



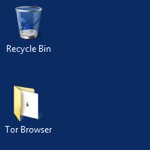
Tor Browser Bundle will not be installed with other programs and will not show up in your start menu.



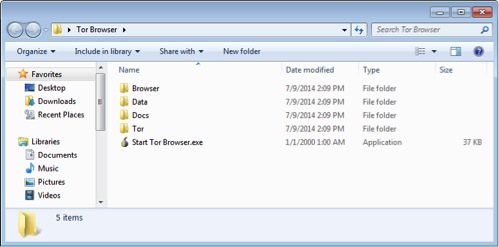
## 3.0 Using Tor Browser Bundle

### Starting Tor Browser for the first time

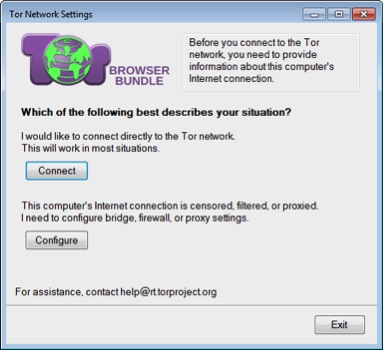
You chose not to start Tor Browser when you finished with the installer, so now go ahead and start Tor Browser for the first time. If you followed all the default settings from the installation you'll see a folder on your desktop called Tor Browser.



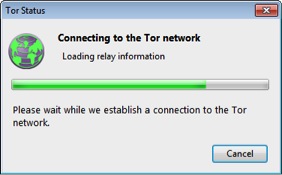
Open the Tor Browser folder and double click on the file called Start Tor Browser.



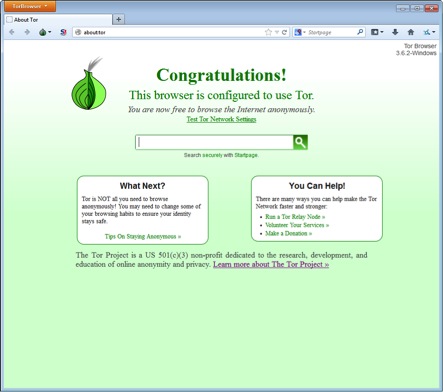
The first time Tor Browser starts, you'll get a window that allows you to modify some settings if necessary. You might have to come back and change some configuration settings, but go ahead and try to connect to the Tor network by clicking the Connect button.



After clicking the connect button, a new window will open with a green bar that will get longer as the Tor software starts up.



The first time Tor Browser starts it might take a bit longer than usual, but be patient, within a few minutes Tor Browser will be done and a web browser opens up congratulating you.



**TRUECRYPT TOOL GUIDE**

# ****TrueCrypt**** Tool Guide

# Secure File Storage

**Lesson to read: Protecting Files**

**Download Location:** <https://truecrypt.ch/downloads/>

**Computer requirements:**

* An internet connection, Windows 2000/XP/2003/Vista/7, Mac OS X or GNU Linux (This guide runs through Windows)
* Administrator rights required for installation or to create volumes but not to access existing volumes

**Version used in this guide:** 7.1a

***(The developers web page is offering a new version 7.2 of TrueCrypt with some functionality removed. Despite this new release we recommend that you continue to use older version 7.1a.)***

**License:** Free and Open-Source Software

**Level:**Advanced

**Other reading**: <http://andryou.com/truecrypt/docs/index.php>

**Time required:** 30-60 minutes

**Using TrueCrypt will give you**:

* The ability to effectively protect your files from intruders or unauthorized access
* The ability to easily and securely store copies of your important files

**NOTE: TrueCrypt is currently unmaintained, which might have security implications.**



**1.0 Before you start**

**Truecrypt**keeps your files secure by preventing anyone without the correct password from opening them. It works like an electronic safe, creating an encrypted container (called a volume) on your computer or hard drive, that you can put as many files as you like into. If you forget your password, you will lose access to your data!

Please bear in mind that the use of encryption is illegal in some countries.

TrueCrypt offers the ability to create a standard encrypted volume or a hidden volume. Either one will keep your files confidential, but a hidden volume allows you to hide your important information behind less sensitive data in order to protect it, even if you are forced to reveal your TrueCrypt volume. This guide explains both volumes in detail.

• How to Install TrueCrypt and Create Standard Volumes

• How to Mount the Standard Volume

• How to Back up your Volume

• Hidden Volumes

• Portable TrueCrypt

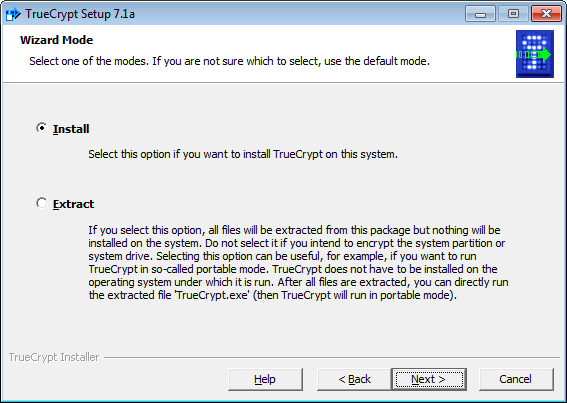
***NOTE: TrueCrypt is currently unmaintained, which might have security implications.***

# 2 How to Install TrueCrypt and Create Standard Volumes

## 2.0 How to Install TrueCryrpt

**Step 1**. **Double click***TrueCrypt Setup 7.1a.exe*; the Open File - Security Warning dialog box may appear. If it does, **click**“Next” to activate the **TrueCrypt**License screen.

**Step 2**. **Check**the I accept and agree to be bound by the license terms option to enable the Accept button; **click**“Accept” to activate the following screen:

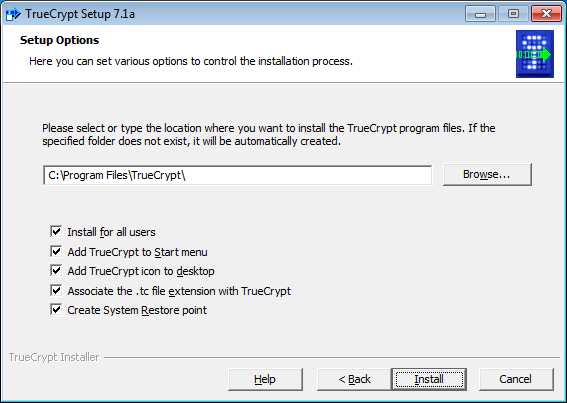


* Install mode: This option is for users who do not wish to hide the very fact that they use **TrueCrypt**on their computer.
* Extract mode: This option is for users who wish to carry a portable version of **TrueCrypt**on a USB memory stick and do not wish to have **TrueCrypt**installed on their computer.

**Note**: Some of the options (for example, entire partition and disk encryption) will not work when **TrueCrypt**is extracted only.

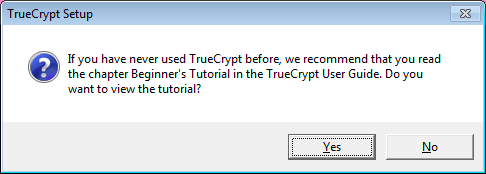
**Note**: Although the default Install mode is recommended here, you may still use **TrueCrypt**in portable mode later on.

**Step 3**. **Click** “Next” to activate the following screen:



**Step 4**. **Click**“Install” to activate the Installing screen to begin installing **TrueCrypt**on your system.

**Step 5**. **Click “**OK**”** and then “Finish” to activate the following screen:



**Step 6**. **Click**“Yes” to complete the **TrueCrypt**installation.

**Note**: All users are strongly encouraged to consult [**TrueCrypt** help documentation](http://andryou.com/truecrypt/docs/index.php) after completing this tutorial.

## 2.1 About TrueCrypt

**TrueCrypt**is a program which secures your files by preventing anyone without the correct password from accessing them. It functions like an electronic safe, letting you lock up your files so that only someone with the correct password can open them. **TrueCrypt**works by letting you set up volumes or sections on your computer where you can securely store files. When you create data in, or move data to these volumes, **TrueCrypt**will automatically encrypt that information. As you open or take your files out, it automatically decrypts them for use. This process is called on-the-fly encryption.

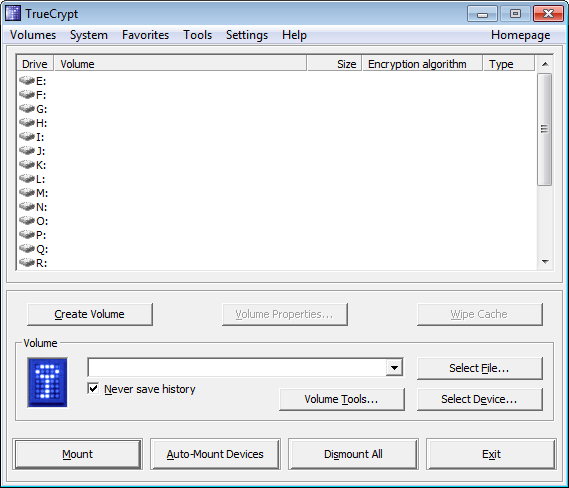
## 2.2 How to Create a Standard Volume

**TrueCrypt**lets you create two kinds of volumes: Hidden and Standard. In this section, you will learn how to create a Standard Volume in which to store your files.

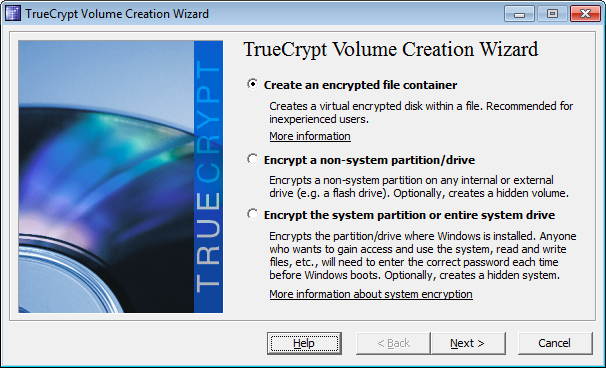
To begin using **TrueCrypt**to create a Standard Volume, perform the following steps:

**Step 1**. **Double click on**the TrueCrypt icon or **Select Start > Programs > TrueCrypt > TrueCrypt** to open **TrueCrypt**.

**Step 2**. **Select**a drive from the list in the **TrueCrypt**pane as follows:

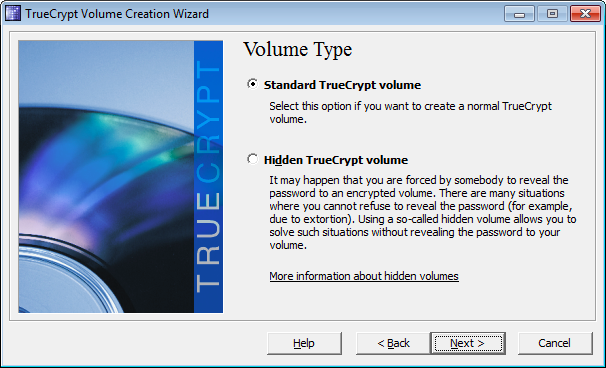


**Step 3**. **Click “**Create Volume**”** to activate the TrueCrypt Volume Creation Wizard as follows:



There are three options for encrypting a Standard Volume. In this guide, we will use the Create an encrypted file container option. Please refer to the [**TrueCrypt**](http://www.truecrypt.org/docs/) documentation for the description of other two options.

**Step 4**. **Click**“Next” to activate the following screen:

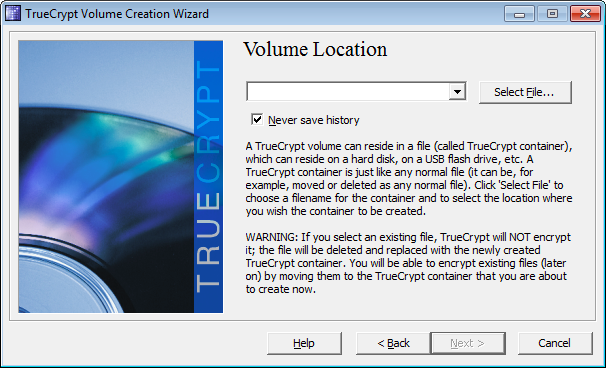


The TrueCrypt Volume Creation Wizard Volume Type window lets you specify whether you would prefer to create a Standard or Hidden **TrueCrypt** volume.

For more information about How to Create a Hidden Volume, please refer to the Hidden Volumes section further down.

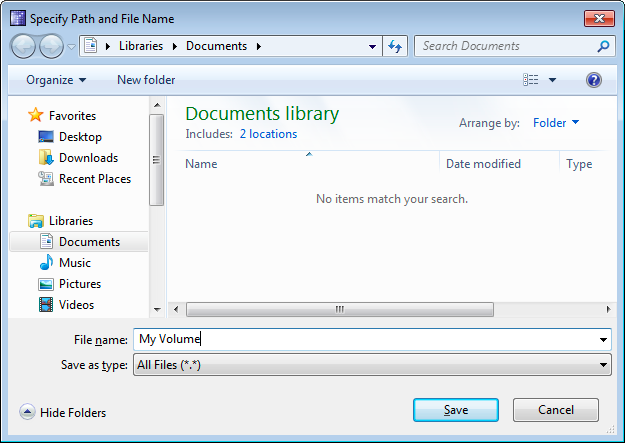
**Step 5**. **Check**the Standard TrueCrypt Volume option.

**Step 6**. **Click**“Next” to activate the following screen:



You can specify where you would like to store your Standard Volume in the Volume Creation Wizard - Volume Location screen. This file can be stored like any other file.

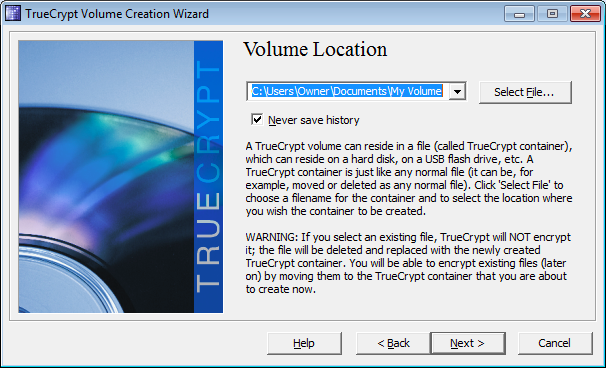
**Step 7**. Either **type**in the name of the file into the text field, or **click**“Select File” to activate the following screen:



**Note**: A **TrueCrypt**Volume is contained inside a normal file. This means that it can be moved, copied or even deleted! You need to remember both the location and name of the file. However, you must choose new file name for the volume you create. In this tutorial, we will create our Standard Volume in the **My Documents** folder, and name the file My Volume as shown in figure 8 above.

**Tip**: You can use any file name and file extension. For example, you can name your Standard Volume recipes.doc, so that it will look like a Word document, or holidays.mpg, so it will look like a movie file. This is one way you can help disguise the existence of your Standard Volume.

**Step 8**. **Click**“Save” to close the Specify Path and File Name window and return to the Volume Creation Wizard window as follows:



**Step 9**. **Click**“Next”.

## 2.3 How to Create a Standard Volume on a USB Memory Stick

To create a **TrueCrypt**Standard Volume on a USB memory stick, perform steps 1 to 7 in section 2.2 How to Create a Standard Volume, where you activate the Select a TrueCrypt Volume screen. Instead of choosing My Documents as your file location, **navigate**to and then **choose** your USB memory stick. Then, **enter** a file name and create the Standard Volume there.

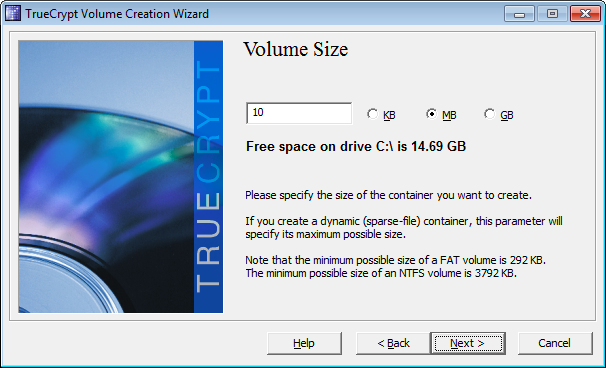
## 2.4 How to Create a Standard Volume (continued)

At this stage, you are ready to choose a specific encryption method (or algorithm as it is referred to on the screen) to encode the data that will be stored in your Standard Volume.



**Note**: You may leave the default options here as they appear. All algorithms presented in the two options here are considered secure.

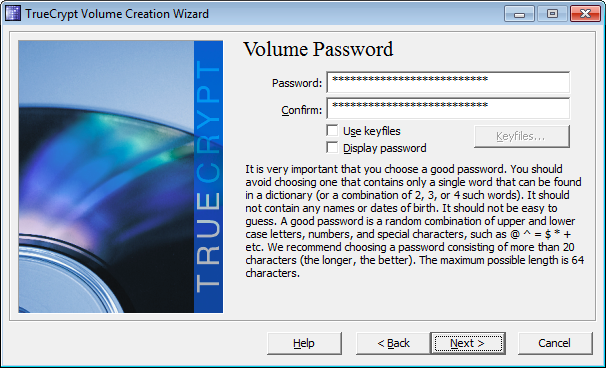
**Step 10**. **Click**“Next” to activate the TrueCrypt Volume Creation Wizard screen as follows:



The Volume Size pane lets you specify the size of the Standard Volume. In this example, it is set at 10 megabytes. However, you may specify a different size. Consider the size of the documents and file types you would like to store, and then set an appropriate volume size for them.

**Tip**: If you would like to backup your Standard Volume to a CD later on, then you should set the size to 700MB or less.

**Step 11**. **Type**in your specific volume size into the text field, and then **click**“Next” to activate the following screen:

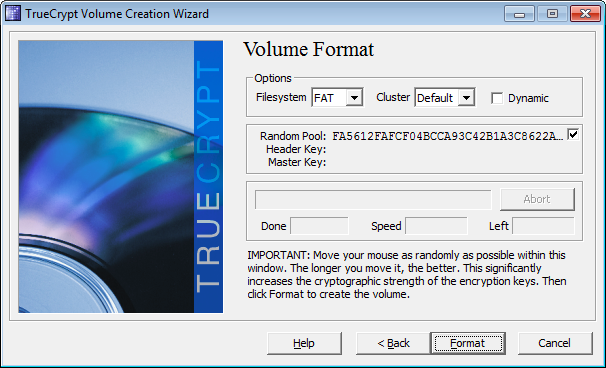


**Important**: Choosing a secure and strong password is among the most important tasks you will perform when creating a Standard Volume. A good password will protect your encrypted volume, and the stronger the password you choose, the better. You don't have to create your own passwords, or even remember them, if you use a password generation program like KeePass. Please refer to the **KeePass lesson**, to learn more information about password creation and storage.

**Step 12**. Type your password and then re-type your password into the Confirm text fields.

**Important**: The Next button will remain disabled until passwords in both text fields match. If your password is not particularly safe or secure, you will see a warning advising you of this. Consider changing it! Although **TrueCrypt** will still work with any password you have chosen, your data may not be very secure.

**Step 13**. **Click**“Next” to activate the following screen:

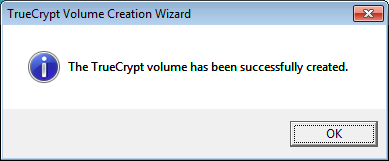


**TrueCrypt**is now ready to create a Standard Volume. Move your mouse randomly within the TrueCrypt Volume Creation Wizard window for few seconds. The longer you move the mouse, the better the quality of the encryption key.

**Step 14**. **Click**“Format” to begin creating your standard volume.

**TrueCrypt**will now create a file named My Volume in the My Documents folder as earlier specified. This file will contain a **TrueCrypt**Standard Volume, 10 Megabytes in size, that you can use to securely store your files.

After a Standard Volume has been successfully created, the following dialog box will appear:



**Step 15**. **Click**“OK” to complete creating your Standard Volume and return to the **TrueCrypt**console.

**Step 16**. **Click**“Exit” to close TrueCrypt Volume Creation Wizard.

# 3 How to Mount the Standard Volume

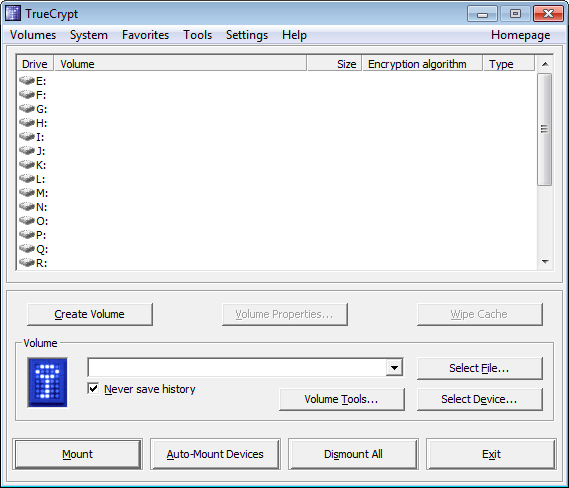
## 3.0 How to Mount a Standard Volume

In **TrueCrypt**, to mount a Standard Volume refers to making the standard volume available for use. In this section, you will learn how to mount your newly created standard volume.

To begin mounting your standard volume, perform the following steps:

**Step 1**. **Double click**on the TrueCrypt icon or **Select Start > Programs > TrueCrypt > TrueCrypt** to open **TrueCrypt**.

**Step 2**. **Select**any drive from the list as follows:

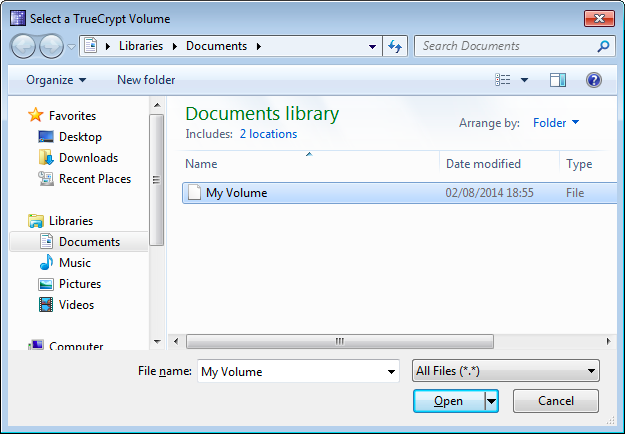


In this example the Standard Volume will be mounted as the M: drive.

**Note**: In the image above, the M: drive has been selected for mounting the standard volume; however, you may choose another listed drive.

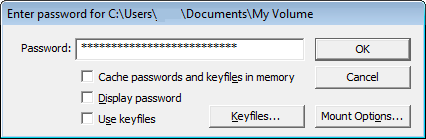
**Step 3**. **Click**“Select File…”

The Select a TrueCrypt Volume screen will appear as follows:



**Step 4**. **Select**the standard volume file that you created, then **click “**Open**”** to close figure 2 and return to the **TrueCrypt** console.

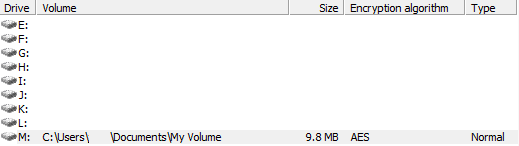
**Step 5**. **Click**“Mount” to activate the Enter password for prompt screen as follows:



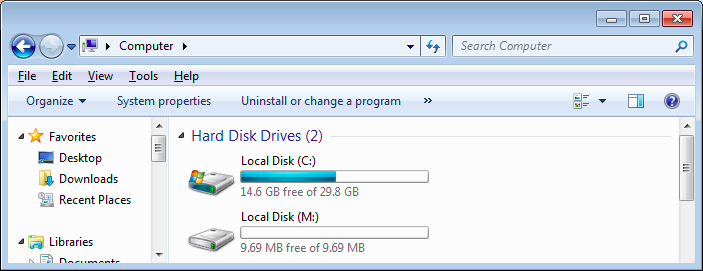
**Step 6**. **Type**the password in the Password: text field.

**Step 7**. **Click “**OK**”** to begin mounting the Standard Volume.

**Note**: If the password you typed is incorrect, **TrueCrypt**will prompt you to re-type your password and **click**“OK”. If the password is correct, the Standard Volume will be mounted as follows:



**Step 8**. **Double click** the highlighted entry in **TrueCrypt** or **double click**the corresponding drive letter in the My Computerscreen to access the Standard Volume (now mounted on drive M: on your computer).



**Note**: We have just successfully mounted the My Volume standard volume on a virtual disk M:. This virtual disk behaves like a real disk, except that it is entirely encrypted. Any files will be automatically encrypted when you copy, move or save them to this virtual disk (a process known as on-the-fly encryption).

You can copy files to and from the Standard Volume just as you would copy them to any normal disk (for example, by dragging-and-dropping them). When you move a file out of the Standard Volume, it is automatically decrypted. Conversely if you move a file onto the Standard Volume, **TrueCrypt**automatically encrypts it. If your computer crashes or is suddenly switched off, **TrueCrypt**will immediately close the Standard Volume.

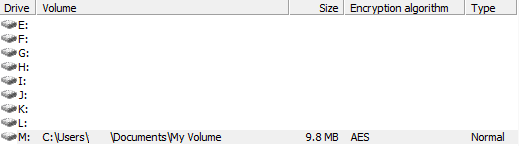
**Important**: After transferring files to the **TrueCrypt**volume, make sure that no traces of the files are left behind on the computer or USB memory stick that they came from. Please refer to the **Safe Deleting lesson**.

## 3.1 How to Dismount the Standard Volume

In **TrueCrypt**, to dismount a Standard Volume simply means to make a volume unavailable for use.

To close or dismount a Standard Volume and make its files accessible only to someone with a password, perform the following steps:

**Step 1**. **Select**the volume from the list of mounted volumes in the main **TrueCrypt**window as follows:

****

**Step 2**. **Click**“Dismount” to dismount or close your **TrueCrypt**standard volume.

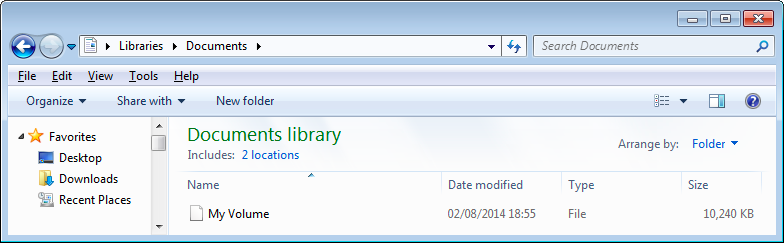
**Important**: Make sure to dismount your **TrueCrypt**volume before putting your computer to Standby or Hibernate mode. Better yet, always shut-down your computer or laptop if you plan on leaving it unattended. This will prevent anyone from being able to gain your volume password.

To retrieve a file stored in your standard volume once you have closed or dismounted it, you will have to mount it again.

**4.0 How to Back up your Volume**

Backing up your documents, files and folders on a regular basis is critical. Backing up your TrueCrypt volume is vital, and (fortunately) easy to do. Don't forget that your volume must be dismounted before you back it up.

**Step 1**. Navigate to your *Standard Volume* file (in the image below, it is located in the *My Documents* folder).



**Step 2**. Save the file to an external memory device, like a CD, DVD or a USB memory stick.

**Tip**: If you have large amounts of data that you want to encrypt and archive repeatedly, why not create a new *Standard Volume* which is the same size as a CD or DVD? This could be used as a secure storage technique.

Before you back up the standard volume to a removable device, make sure that the device size corresponds to the size of your volume.

|  |  |
| --- | --- |
| Backup Medium | Suggested TrueCrypt Volume Size |
| CD | 700mb |
| DVD | 3900mb |
| USB memory stick | Suggested 25% of total capacity (e.g. For 128MB USB stick, use 30MB for your Standard Volume) |

## 

## 5.0 About Hidden Volumes

In **TrueCrypt**, a Hidden Volume is stored within your encrypted Standard Volume, but its existence is concealed. Even when you 'mount' or open your standard volume, it is not possible either to find or to prove the existence of the hidden volume. If you are forced to reveal your password and the location of your standard volume, then its content may be revealed, but **not** the existence of the hidden volume within.

Imagine a briefcase with a secret compartment. You keep files that you do not mind having confiscated or losing in the normal section of your briefcase, and you keep the important and private files in the secret compartment. The point of the secret compartment (especially a well-designed one), is to hide its own existence and therefore, the documents within it.

## 5.1 How to a Create a Hidden Volume

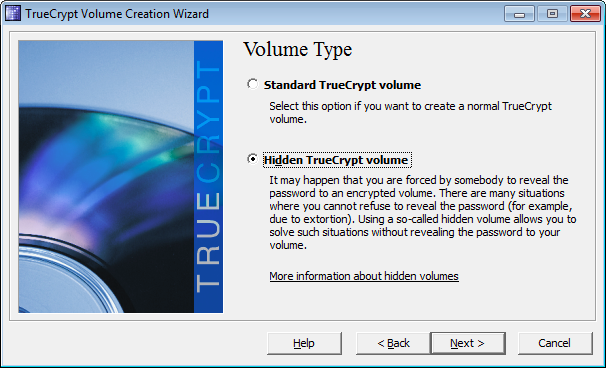
The creation of a **TrueCrypt**Hidden Volume is similar to creating a **TrueCrypt**Standard Volume: Some of the panes, screens and windows are even the same.

**Step 1**. **Open TrueCrypt.**

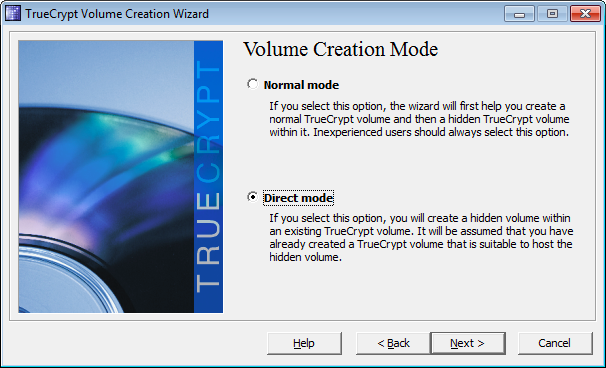
**Step 2**. **Click**“Create Volume” to activate the TrueCrypt Volume Creation Wizard.

**Step 3**. **Click**“Next” to accept the default Create an encrypted file container option.

**Step 4**. **Check**the Hidden TrueCrypt volume option as follows:



**Step 5**. **Click**“Next” to activate the following screen:



* Direct mode: This option lets you create the Hidden Volume within an existing Standard Volume.
* Normal mode: This option lets you create a completely new Standard Volume in which to store the Hidden Volume.

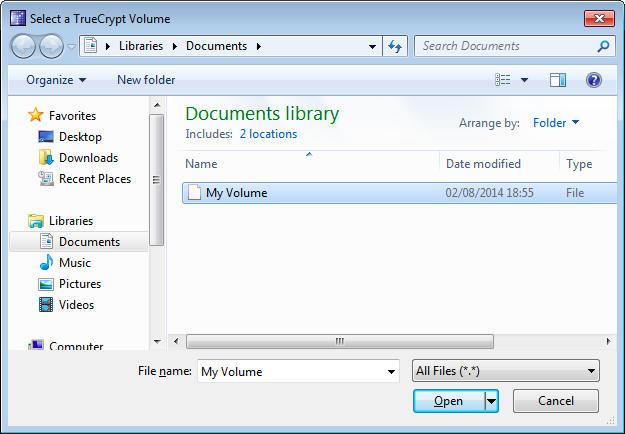
In this example, we will use the Direct mode.

**Note**: If you would rather start a new Standard Volume, please repeat the process from section 2.2 How to Create a Standard Volume.

**Step 6**. **Check**the Direct Mode option and then **click**“Next” to activate the TrueCrypt Volume Creation - Volume Location window.

**Note**: Make sure the Standard Volume is unmounted before selecting it.

**Step 7**. **Click**“Select File” to activate the following screen:

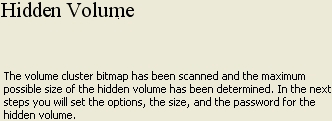


**Step 8**. **Locate**the volume file using the Select a TrueCrypt Volume window as shown above.

**Step 9**. **Click**“Open” to return to the TrueCrypt Volume Creation Wizard.

**Step 10**. **Click**“Next” to activate the Enter password screen.

**Step 11**. **Type**in password you used when creating the Standard Volume into the Password text field to activate the following screen:



**Step 12**. **Click**“Next” after you have read the message to activate the Hidden Volume Encryptions Options screen.

**Note**: Leave both the default Encryption Algorithm and Hash Algorithm settings for the Hidden Volume as they are.

**Step 13**. **Click**“Next” to activate the following screen:



You will be prompted to specify the size of the Hidden Volume.

**Note**: Consider the kind of documents, their quantity and size that need to be stored. Do leave some space for the Standard Volume. If you select the maximum size available for the Hidden Volume, you will not be able to put any more new files into the original Standard Volume.

If your Standard Volume is 10 Megabytes(MB) in size and you specify a Hidden Volume size of 5MB (as shown in figure 6 above), you will have two volumes (one hidden and one standard volume) of approximately 5MB each.

Ensure that the information you store in the Standard Volume does not exceed the 5MB you have set. This is because the **TrueCrypt**program itself does not automatically detect the existence of the Hidden Volume, and it could accidentally overwrite it. You may risk losing all files stored in the hidden volume if you exceed your previously established size.

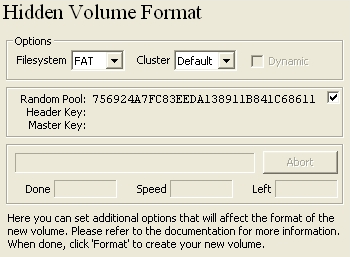
**Step 14**. **Type**in the desired hidden volume size into the corresponding text box as shown in the image below.

**Step 15**. **Click**“Next” to activate the Hidden Volume Password window.

You must now create a different password for the hidden volume from the one used to protect your standard volume. Again, remember to choose a strong password. Please refer to the **KeePass Tool Guide** to learn more about creating strong passwords.

**Tip**: If you anticipate being forced to reveal the contents of your **TrueCrypt**volumes, then store your password for the standard volume in **KeePass**, and create a strong password that you only have to remember for hidden volume. This will help you to conceal your hidden volume, as you will not leave any trace of its existence.

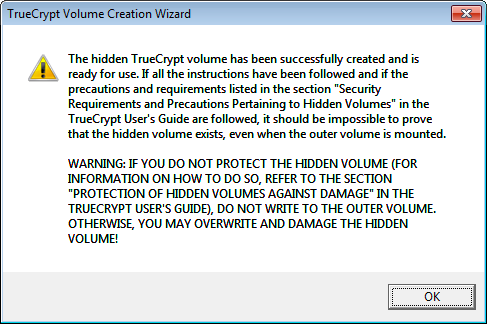
**Step 16**. **Create**a password and **type**it in twice, and then **click**“Next” to activate the following screen:



Leave the default File System and Cluster options as they are.

**Step 17**. **Move**the mouse cursor around the screen to increase the cryptographic strength of the encryption and then **click**“Format” to format the hidden volume.

After the hidden volume has been formatted, the following screen appears:



**Note**: Figure 8 both confirms that you have successfully created a hidden volume, as well as warning you against the dangers of overwriting files in the hidden volume when storing files in the standard volume.

**Step 18**. **Click**“OK” to activate the Hidden Volume Created window, and then **click**“Exit” and return to the **TrueCrypt**console.

The hidden volume has now been created inside your standard volume. You may now store documents in the hidden volume, which remain invisible even to someone who has obtained the password for that particular standard volume.

## 

## 5.2 How to Mount the Hidden Volume

The method for mounting or making a Hidden Volume accessible for use is exactly the same as that for a Standard Volume; the only difference is you will use the password that you have just created for the Hidden Volume.

To mount or open the Hidden Volume, perform the following steps:

**Step 1**. **Select**a drive from the list (in this example, drive K):

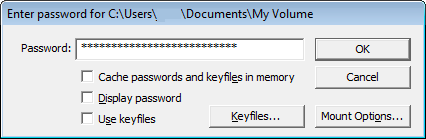


**Step 2**. **Click**“Select File…” to activate the Select a TrueCrypt Volume window.

**Step 3**. **Navigate**to and then **select**your TrueCrypt volume file (same file as for the standard volume).

**Step 4**. **Click**“Open” to return to the **TrueCrypt**console.

**Step 5**. **Click**“Mount” to activate the Enter Password for prompt screen as follows:



**Step 6**. **Type**the password you used to create the hidden volume, and then **click “**OK**”**.

Your hidden volume is now mounted (or opened) as follows:



**Step 7**. **Double click**on above entry or access it through the My Computer window.

## 

## 5.3 Tips on How to Use the Hidden Disk Feature Securely

The purpose of the hidden disk feature is to escape a potentially dangerous situation by appearing to hand over your encrypted files, when someone in a position of power demands to see them, without actually being forced to reveal your most sensitive information. In addition to protecting your data, this may allow you to avoid further jeopardizing your own safety or exposing your colleagues and partners. For this technique to be effective, you must create a situation where the person demanding to see your files will be satisfied by what you show them and let you go.

To do this, you may want to implement some of the following suggestions:

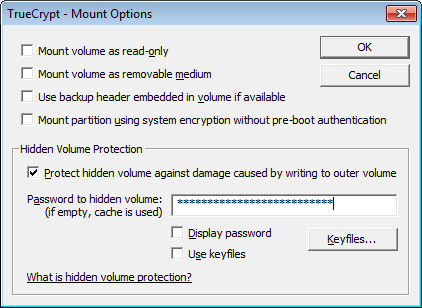
* Put some confidential documents that you do not mind having exposed in the standard volume. This information must be sensitive enough that it would make sense for you to keep it in an encrypted volume.
* Be aware that someone demanding to see your files may know about hidden volumes. If you are using **TrueCrypt**correctly, however, this person will not be able to prove that your hidden volume exists, which will make your denial more believable.
* Update the files in the standard volume on a weekly basis. This will create the impression that you really are using those files.

Whenever you mount a **TrueCrypt**volume, you can choose enable the Protect hidden volume against damage caused by writing to outer volume feature. A very important feature, it lets you add new 'decoy' files to your standard volume without the risk of you accidentally deleting or overwriting the encrypted contents of your hidden volume.

As mentioned earlier, exceeding the storage limit on your standard volume may otherwise destroy your hidden files. Do not enable the Protect hidden volume feature when forced to mount a **TrueCrypt**volume, because doing so requires you to enter the secret password to your hidden volume and will clearly reveal that volume's existence. When you are updating your decoy files in private, however, you should always enable this option.

To use the Protect hidden volume feature, perform the following steps:

**Step 1**. **Click**“Mount Options…” on the Enter Password prompt shown in the image above. This will activate the Mount Options window as follows:



**Step 2**. **Check**the Protect hidden volume against damage caused by writing to outer volume option.

**Step 3**. **Type**in in your Hidden Volume password, and then **click**“OK”.

**Step 4**. **Click**“Mount” to mount your standard volume. After you have successfully mounted it, you will be able to add decoy files without damaging your hidden volume.

**Step 5**. **Click**“Dismount” to dismount, or your make your standard volume unavailable for use, when you have finished modifying its contents.

**Remember**: You only need to do this when you are updating the files in your standard volume. If forced to reveal your standard volume to someone else, you should not use the Protect hidden volume feature.

# 6. Portable TrueCrypt



**Truecrypt**keeps your files secure by preventing anyone without the correct password from opening your hidden documents and files. It works like an electronic safe, which you can use to securely lock up your files.

## 6.1 Differences between the Installed and Portable versions of TrueCrypt

Given that portable tools are not installed on a local computer, their existence and use may remain undetected. However, keep in mind that your external device or USB memory stick, and portable tools are only as safe as the computer you are using, and may risk being exposed to adware, malware, spyware and viruses.

As with many of the portable software tools documented here, **Portable TrueCrypt**allows you to use a powerful and simple file encryption tool without being detected. Having **Portable TrueCrypt**on removable device or USB memory stick lets you use it from different workstations.

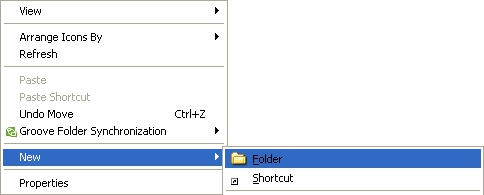
There are very few differences between both the installed and portable versions of **Portable TrueCrypt**, the main one being that **Portable TrueCrypt**does not permit the encryption of the entire disk or system disk.

## 6.2 Downloading, Extracting and Using Portable TrueCrypt

**Note**: The folder into which **Portable TrueCrypt**is to be extracted must be created manually on the removable device, USB memory stick or computer disk before the extraction process.

**Step 1**. **Navigate**to chosen destination where you would like to extract the **Portable TrueCrypt** program to, and then **right-click**to activate its associated menu.

**Step 2**. **Select**the New item to activate its sub-folder, and then **select**the Folder sub-menu item, as shown below:



**Step 3**. **Enter**the name of the folder.

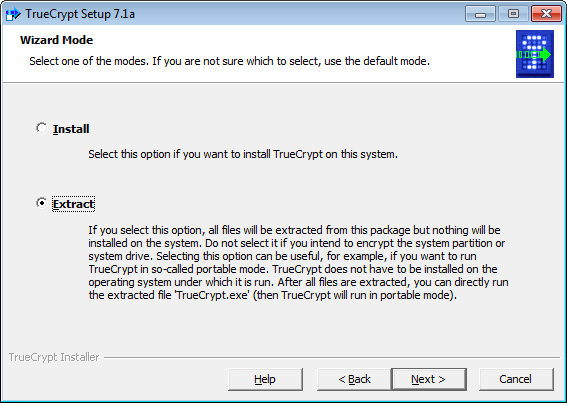
**Note**: You may give this folder a less obvious name to conceal the existence of the **Portable TrueCrypt**program.

**Portable TrueCrypt**can be extracted from the same archive as installation version:

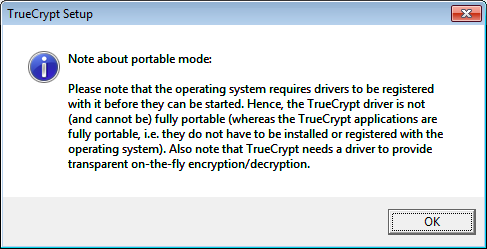
**Step 1**. **Navigate**to **TrueCrypt**installation file on your computer.

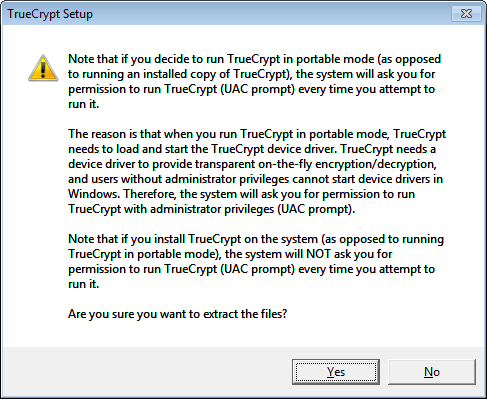
**Step 2**. **Double click***TrueCryptSetup7.1.a.exe*; the Open File - Security Warning dialog box may appear; if it does, **click**“Yes” to activate the **TrueCrypt**installation wizard.

**Step 5**. **Check**the **Extract**option to extract **TrueCrypt**portable to a removable drive or USB device as shown below:

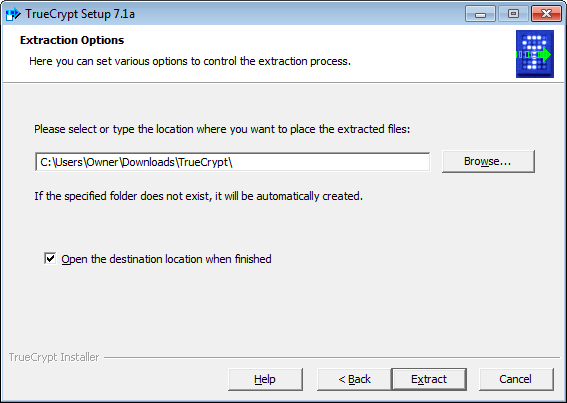


**Step 6**. **Click**“Next” to activate following two screens:





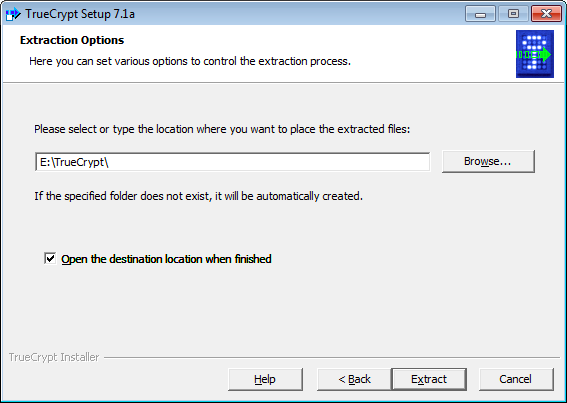
**Click** “OK” and “Yes” respectively to activate the **Extraction Options** window as follows:



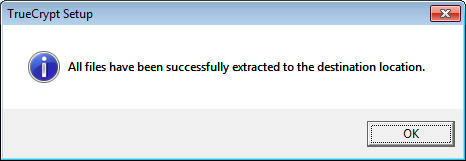
**Step 7**. **Click**“Browse” to activate the Browse for Folders window as follows:



**Step 8**. **Navigate**to your destination folder on either the external drive or USB memory stick, and then **click**“OK”, to return the Extraction Options window as follows:

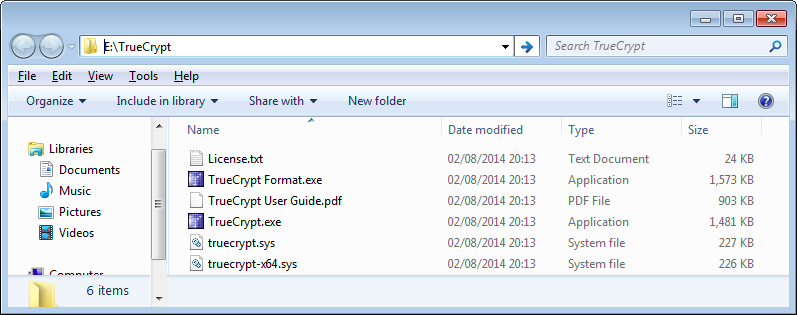


**Step 9**. **Click**“Extract” to begin extracting **TrueCrypt**to your removable drive or USB memory stick; a few seconds later, the following windows will appear:



**Step 10**. **Click**“OK” and then **click**“Finish” to complete the installation process.

If the*“Open the destination location when fininshed”*option was enabled (as it usually is by default), the following screen will appear:



**Step 11**. **Navigate**to and then **double click***TrueCrypt.exe*to run **Portable TrueCrypt**.

Please refer to the instructions for regular TrueCrypt above from this point onwards, for more on how to use **TrueCrypt**.

## 6.3 How to Eliminate All Traces of Having Extracted Portable TrueCrypt

**Important**: After you have successfully extracted **Portable TrueCrypt**to your external/removable device, you must **delete**the installation file from your computer to further eliminate any traces of you having downloaded and installed **Portable TrueCrypt**.

**Step 1**. **Navigate**to the folder in which **Portable TrueCrypt**was downloaded, and then **right click**the *TrueCryptSetup7.1.a.exe*installation file to activate the **Windows**pop-up menu; then, **select**the “**Delete”**command to move it to your **Recycle Bin**.

**Step 2**. **Double click**the Recycle Bin to open its associated window, and then **select**and **delete**the file.

**Note**: If you have either CCleaner or Eraser installed, you can use either of them to eliminate all traces of your having ever downloaded and installed **Portable TrueCrypt**. See the **Safe Deleting lesson** for more information on how to do this.