

## Archivia e trasporta i Tuoi dati sensibili in sicurezza

---



Probabilmente anche tu come molti, trasporti giornalmente **PC portatili, chiavi USB, CD, DVD** o altri supporti contenenti tuoi dati personali o aziendali senza tenere molto in considerazione che la semplice perdita o furto comporta, oltre al valore dell' hardware, il fatto che le tue preziose informazioni riservate possono finire in mano a qualcuno che potrebbe farne un uso illecito con conseguenze imprevedibili a livello di privacy.

La soluzione é la Crittografia di tutti i dati sensibili contenuti nei tuoi archivi portatili ed eventualmente anche fissi, in modo che il nuovo proprietario sia costretto a riformattare l' archivio per limitare il danno alla sola perdita dell' hardware.

Io utilizzo da tempo l' ottimo **TrueCrypt** per rendere inaccessibili a terzi i miei dati sensibili.

Vediamo ora in pratica come puoi fare per rendere sicura una **chiave USB da 1GB**, ma la stessa procedura é sostanzialmente applicabile anche ad altri tipi di supporto, tenendo però presente che il programma consente di scegliere tutta una serie di opzioni da utilizzare a seconda delle specifiche necessità.

Inserisci la chiave USB nel PC, copia in una cartella temporanea gli eventuali archivi e poi cancella tutto il contenuto verificando la lettera dell' unità associata, che supponiamo sia **F:**

Dopo aver installato **TrueCrypt** sul PC, apri il programma e clicca "*Crea Volume*", si aprirà una nuova finestra con già selezionato "*Crea un volume standard di TrueCrypt*", clicca "*Avanti >*".

Clicca "*Seleziona file...*" e specifica il percorso e il nome del file che servirà a contenere il nuovo Volume TrueCrypt con i dati criptati, per esempio **F:\TrueCryptTEST** (al nome io aggiungo un codice **...\_XXX** che mi ricorda quale password ho utilizzato) poi clicca "*Avanti >*".

Ora puoi scegliere il tipo di algoritmi da utilizzare, lascia pure quelli preselezionati e clicca "*Avanti >*", inserisci come dimensione del volume **990MB** e clicca "*Avanti >*".

Adesso inserisci una buona password composta da minimo 20 caratteri e massimo 64 e clicca "*Avanti >*", lascia le opzioni Formato del Volume preselezionate e clicca "*Formatta*" per creare il volume criptato, poi "*OK*" e "*Esc*".

Ritornato nella finestra principale del programma, ora scegli la lettera di unità da utilizzare, ad esempio **M:**, e inserisci in basso il percorso del volume appena creato **F:\TrueCryptTEST**, poi clicca "*Monta*" e inserisci la password.

---

A questo punto il volume criptato é stato montato come unità **M:** di 990MB, ed é disponibile per qualsiasi normale operazione di lettura / scrittura.

Per poter utilizzare la chiave USB con il volume criptato anche in altri PC sprovvisti di TrueCrypt, devi solo copiare sulla chiave USB nei residui 10MB lasciati liberi, i seguenti 4 archivi da  
C:\Programmi\TrueCrypt\ :

**TrueCrypt.exe**, **Language.it.xml**, **truecrypt.sys** e **truecrypt-x64.sys**, in modo da poter eseguire TrueCrypt.exe direttamente dalla chiave USB.

Puoi seguire la stessa procedura per la copia o backup di dati su CD o DVD, l' unica differenza é che in questo caso il volume criptato va prima preparato sul disco rigido, e successivamente copiato su CD o DVD.

Gli archivi contenenti volumi criptati possono anche essere utilizzati per l'invio sicuro di allegati email.

---

[http://abtechno.org/index.php/2005/12/16/come\\_creare\\_password\\_sicure](http://abtechno.org/index.php/2005/12/16/come_creare_password_sicure)

---

## Come creare dischi rigidi virtuali criptati e invisibili

**TrueCrypt** é un programma gratuito con licenza **OpenSource** che permette di creare dischi virtuali criptati con lettura / scrittura dati trasparente e in tempo reale (on-the-fly) utilizzando alcuni tra i migliori algoritmi criptografici disponibili come l'AES-256, Blowfish, CAST5, Serpent, etc.

Il programma crea dischi virtuali dal contenuto criptato, inseriti all'interno di un normale file-archivio che viene visto dal sistema operativo come un nuovo disco rigido addizionale.

Potete criptare un intero disco o una sua partizione, un CD/DVD o una chiave USB e il criptaggio/decriptaggio dei dati avviene completamente in automatico e in maniera invisibile per chi opera sugli archivi.

Volendo si possono creare i cosiddetti "volumi nascosti" (**steganografia**) totalmente invisibili, utili nel caso si venga costretti da qualcuno a rivelare la password di un volume protetto.

Il 25 Novembre 2005 é stata rilasciata la versione 4.1 del programma con nuove funzionalità e migliorie in linea con il futuro standard **IEEE** per la criptografia dati.

Download del programma :

<http://www.truecrypt.org/downloads.php>

Modulo lingua :

<http://www.truecrypt.org/localizations.php>

---

## 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. We strongly recommend that you also read the other sections of this manual, as they contain important information.

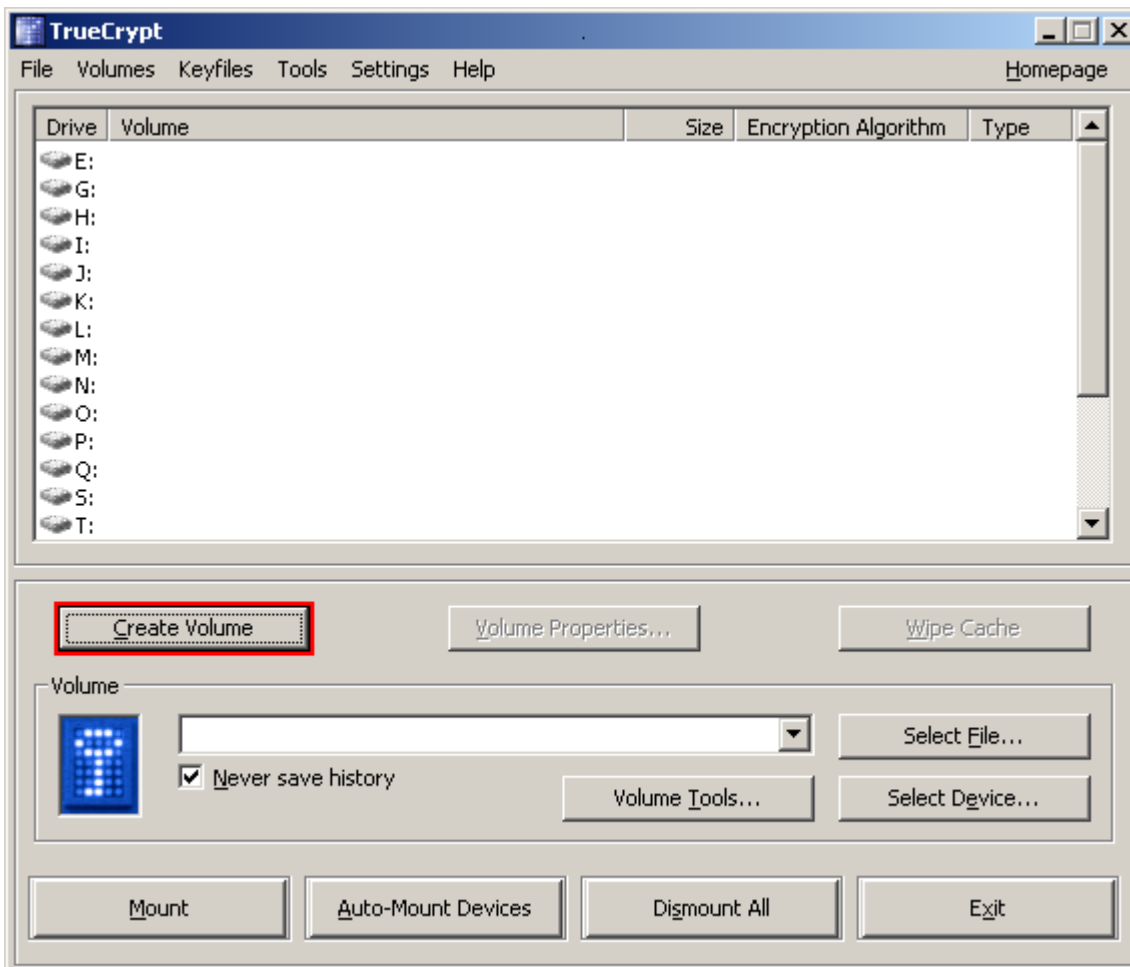
### Step 1:

If you have not done so, download, unpack, and install TrueCrypt (to do so, double-click *TrueCrypt Setup.exe* and then click **Install**).

### Step 2:

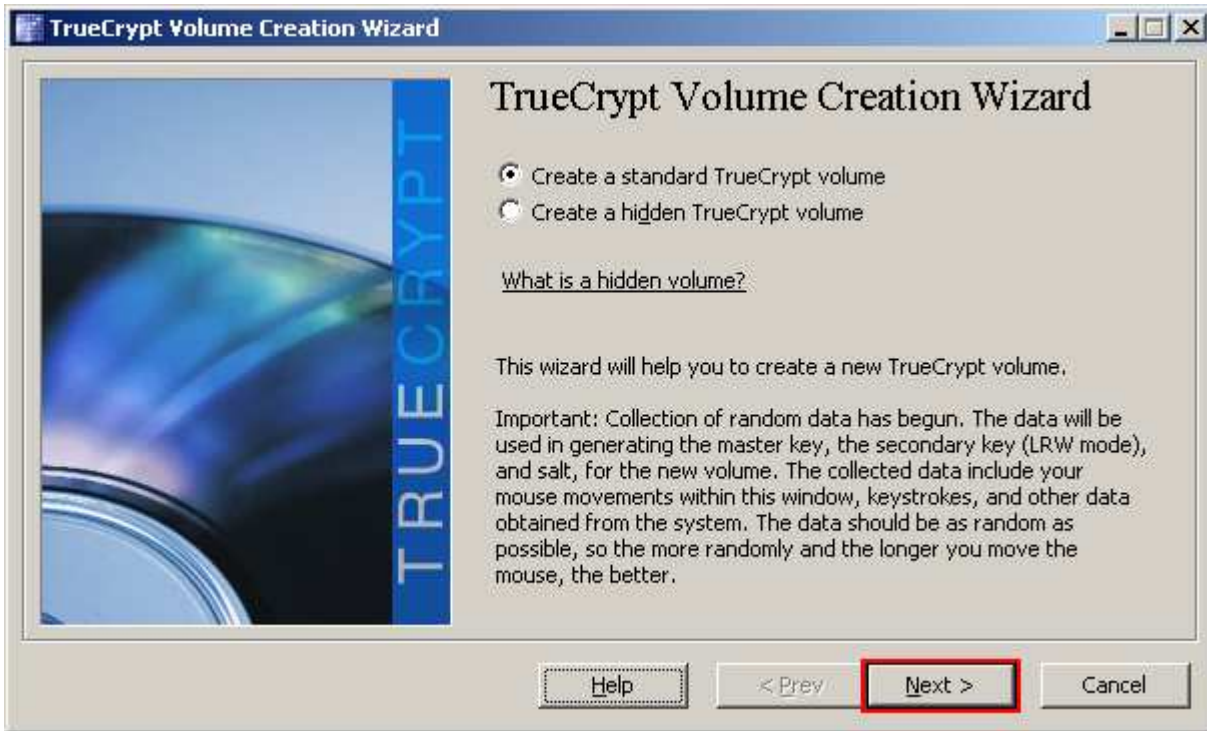
Launch TrueCrypt by double-clicking the file *TrueCrypt.exe* or by clicking the TrueCrypt shortcut in your Windows Start menu.

### Step 3:



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

### Step 4:

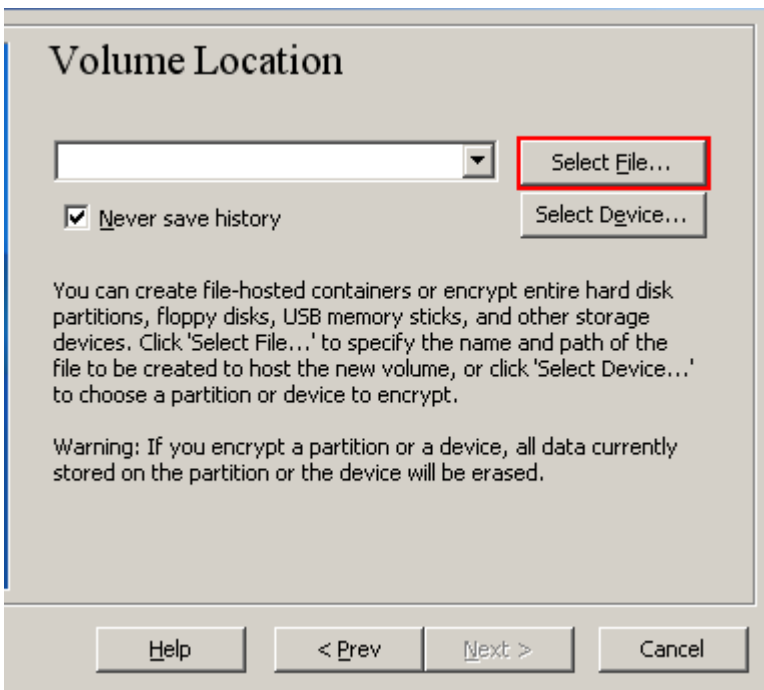


The TrueCrypt Volume Creation Wizard window should appear.

Read the instructions displayed in the Wizard window and click **Next**.

Note: In the following steps the screenshots will show only the right-hand part of the Wizard window.

#### Step 5:



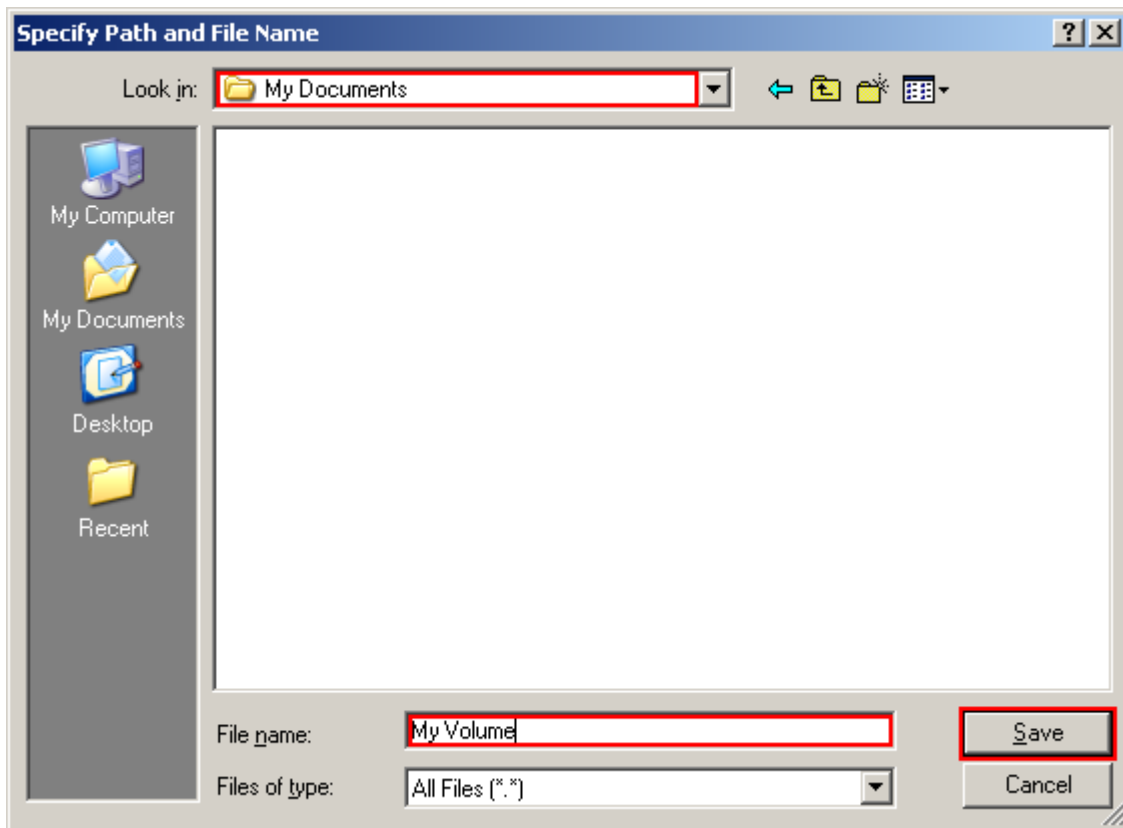
In this step you have to specify where you wish the TrueCrypt volume to be created. A TrueCrypt volume can reside either in a file, which is also called *container*, or in a partition (device). In this tutorial, we will choose the former option and create a TrueCrypt volume within a file.

Note that a TrueCrypt container is just like any normal file. It can be moved, copied and 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 6:**



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. If you select an existing file, 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.

In the following steps, we will return to the TrueCrypt Volume Creation Wizard.

**Note**

TrueCrypt is a software system for establishing and maintaining an on-the-fly-encrypted volume (data storage device). On-the-fly encryption means that data are automatically encrypted or decrypted right before they are loaded or saved, without any user intervention. *No* data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys. Entire file system is encrypted (e.g., file names, folder names, contents of every file, free space, meta data, etc).

Files can be copied to and from a mounted TrueCrypt volume just like they are copied to/from any normal disk (for example, by simple drag-and-drop operations). Files are automatically being decrypted on-the-fly (in memory/RAM) while they are being read or copied from an encrypted TrueCrypt volume. Similarly, files that are being written or copied to the TrueCrypt volume are automatically being encrypted on-the-fly (right before they are written to the disk) in RAM. Note that this does *not* mean that the *whole* file that is to be encrypted/decrypted must be stored in RAM before it can be encrypted/decrypted. There are no extra memory (RAM) requirements for TrueCrypt. For an illustration of how this is accomplished, see the following paragraph.

Let's suppose that there is an .avi video file stored on a TrueCrypt volume (therefore, the video file is entirely encrypted). The user provides the correct password (and/or keyfile) and mounts (opens) the TrueCrypt volume. When the user double clicks the icon of the video file, the operating system launches the application associated with the file type – typically a media player. The media player then begins loading a small initial portion of the video file from the TrueCrypt-encrypted volume to RAM (memory) in order to play it. While the portion is being loaded, TrueCrypt is automatically decrypting it (in RAM). The decrypted portion of the video (stored in RAM) is then played by the media player. While this portion is being played, the media player begins loading next small portion of the video file from the TrueCrypt-encrypted volume to RAM (memory) and the process repeats. This process is called on-the-fly encryption/decryption and it works for all file types, not only for video files.

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 dismantled and files stored in it will be inaccessible (and encrypted). Even when power supply is suddenly interrupted (without proper system shut down), files stored in the volume are inaccessible (and encrypted). To make them accessible again, you have to mount the volume (and provide the correct password and/or keyfile).

In case an adversary forces you to reveal your password, TrueCrypt provides and supports two kinds of plausible deniability:

1. Hidden volumes (for more information, see the section [Hidden Volume](#)).
2. It is impossible to identify a TrueCrypt volume. Until decrypted, a TrueCrypt volume appears to consist of nothing more than random data (it does not contain any kind of "signature"). Therefore, it is impossible to *prove* that a file, a partition or a device is a TrueCrypt volume or that it has been encrypted.

TrueCrypt containers (file-hosted volumes) can have any file extension you like (for example, .raw, .iso, .bin, .img, .dat, .rnd, .tc) or they can have no file extension at all. TrueCrypt ignores file extensions. If you need plausible deniability, make sure your TrueCrypt volumes do not have the .tc file extension (this file extension is 'officially' associated with TrueCrypt).

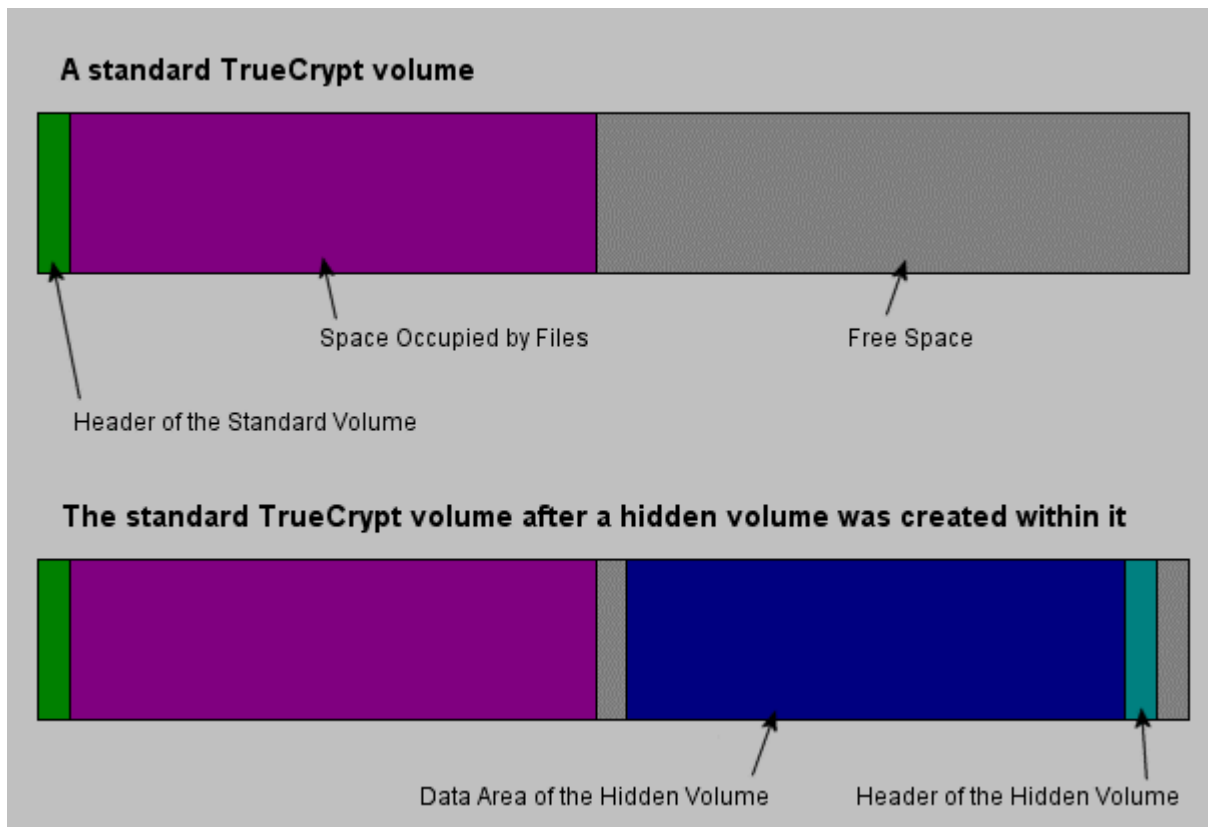
When formatting a hard disk partition as a TrueCrypt volume, the partition table (including the partition type) is *never* modified (no TrueCrypt "signature" or "ID" is written to the partition table).

Whenever TrueCrypt accesses a file-hosted volume (e.g., when dismantling, attempting to mount, changing or attempting to change the password, creating a hidden volume within it, etc.) or a keyfile, it preserves the timestamp of the container/keyfile (i.e., date and time that the container/keyfile was last accessed\* or last modified), unless this behaviour is disabled in the preferences.

\* Note that if you use the Windows 'File Properties' tool to view a container/keyfile timestamp (e.g., by right-clicking the container/keyfile and selecting 'Properties'), you will alter the date and time that the container/keyfile was last *accessed*. Also note that if you view thumbnails of files in the Windows file selector (for instance, when selecting a container or keyfile in the Thumbnail file selector mode), Windows may modify the timestamps of the files (date and time that the files were last accessed).

## 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 TrueCrypt volume before and after a hidden volume was created within it.*

The principle is that a TrueCrypt volume is created within another TrueCrypt volume (within the free space on the volume). Even when the outer volume is mounted, it is impossible to prove whether there is a hidden volume within it or not, because free space on *any* TrueCrypt 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 TrueCrypt 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 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 TrueCrypt 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).

TrueCrypt first attempts to decrypt the standard volume header using the entered password. If it fails, it loads the sector of the volume where hidden volume headers are normally stored (the third sector from the end of the

volume) to RAM and attempts to decrypt it using the entered password. Note that the hidden volume header cannot be identified, as it appears to consist entirely of random data. If the header is successfully decrypted (for information on how TrueCrypt 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 TrueCrypt volume, i.e., within a file-hosted volume or within a partition/device (requires administrator privileges). To create a hidden TrueCrypt volume, click on *Create Volume* in the main program window and select *Create a hidden TrueCrypt volume*. The Wizard will provide help and all information necessary to successfully create a hidden TrueCrypt 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.\*\*

A hidden volume can only be created within a FAT TrueCrypt volume (i.e., the file system of the outer volume must either be FAT12, FAT16, or FAT32). NTFS file system stores various data throughout the entire volume (as opposed to FAT) leaving little room for the hidden volume. Therefore, the Volume Creation Wizard prevents the user from selecting NTFS as the file system for the outer volume. The hidden volume can contain any file system you like. Note that the outer volume (when file-hosted) can be stored on any file system.

Note: Should you be asked why the file system of the outer volume is FAT, you can answer that you left all settings at default (FAT is the default file system for all TrueCrypt volumes). There are also other reasons to use FAT instead of NTFS (for example, FAT is faster and tends to get less fragmented).

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

\* Provided that the options *Quick Format* and *Dynamic* are disabled. For information on the method used to fill free volume space with random data, see chapter [Technical Details](#), section [TrueCrypt Volume Format Specification](#).

\*\* This feature is implemented only in the Windows versions of TrueCrypt. 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.