Sommaire :

Notes:

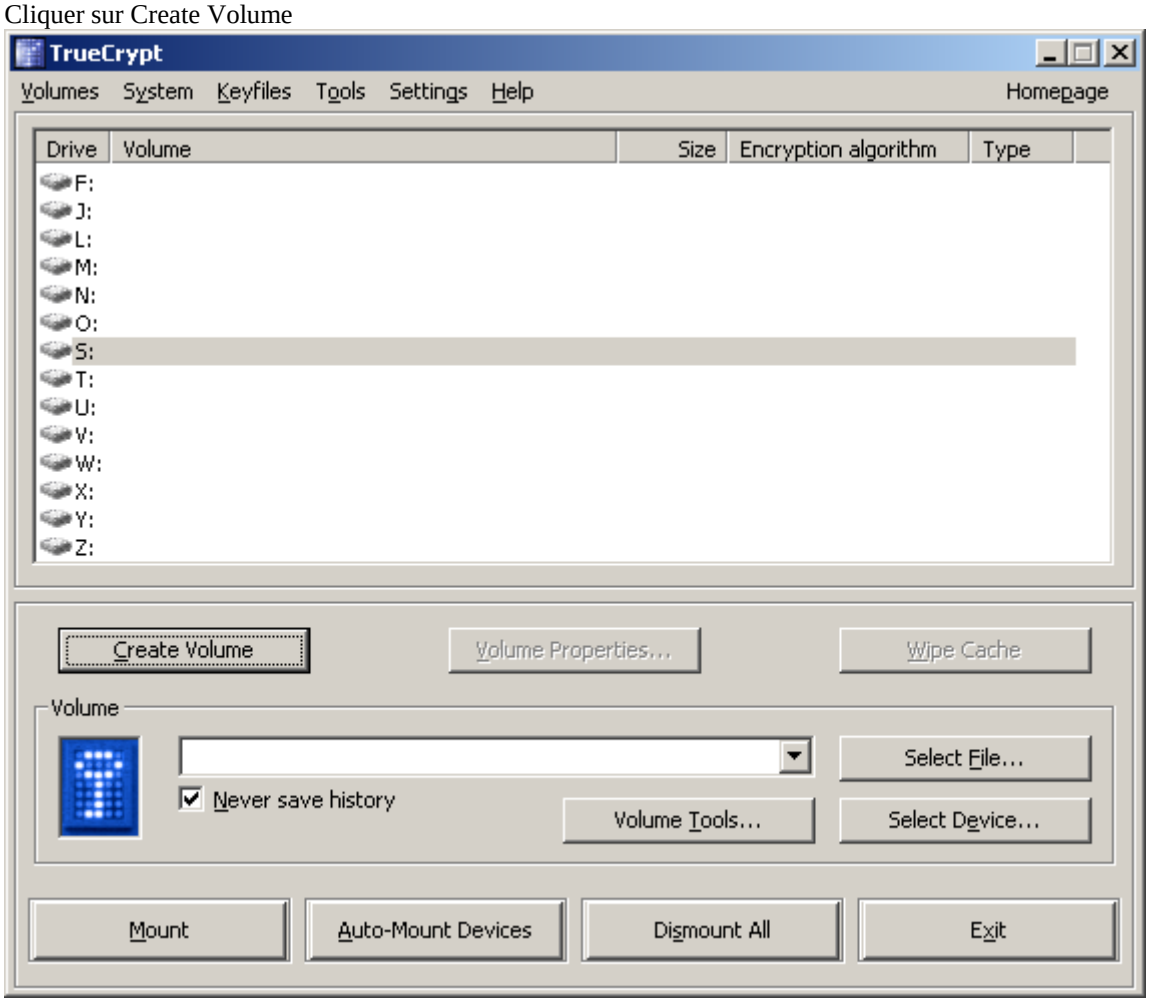
- Points de départ sur le web: http://www.framasoft.net/article3931.html et http://www.truecrypt.org
- Normalement, tout ce que je raconte plus bas figure dans la doc. Il suffit de la lire...
- TrueCrypt fonctionne sous plein de systèmes, mais je n'ai testé que Windows.
- La doc a été mise à jour en juin 2009, avec la version 6.2 de TrueCrypt. Depuis il y a de nouvelles versions, et il y a peut-être quelques nuances dans les menus

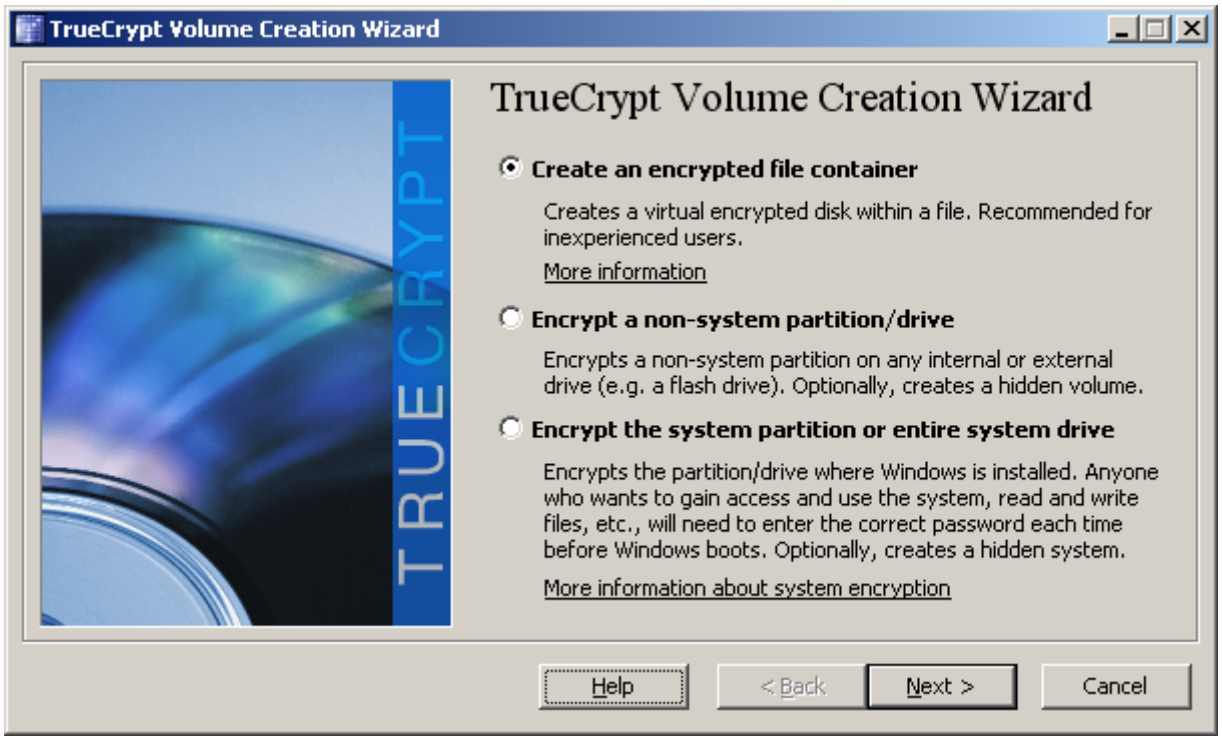
Principe de TrueCrypt

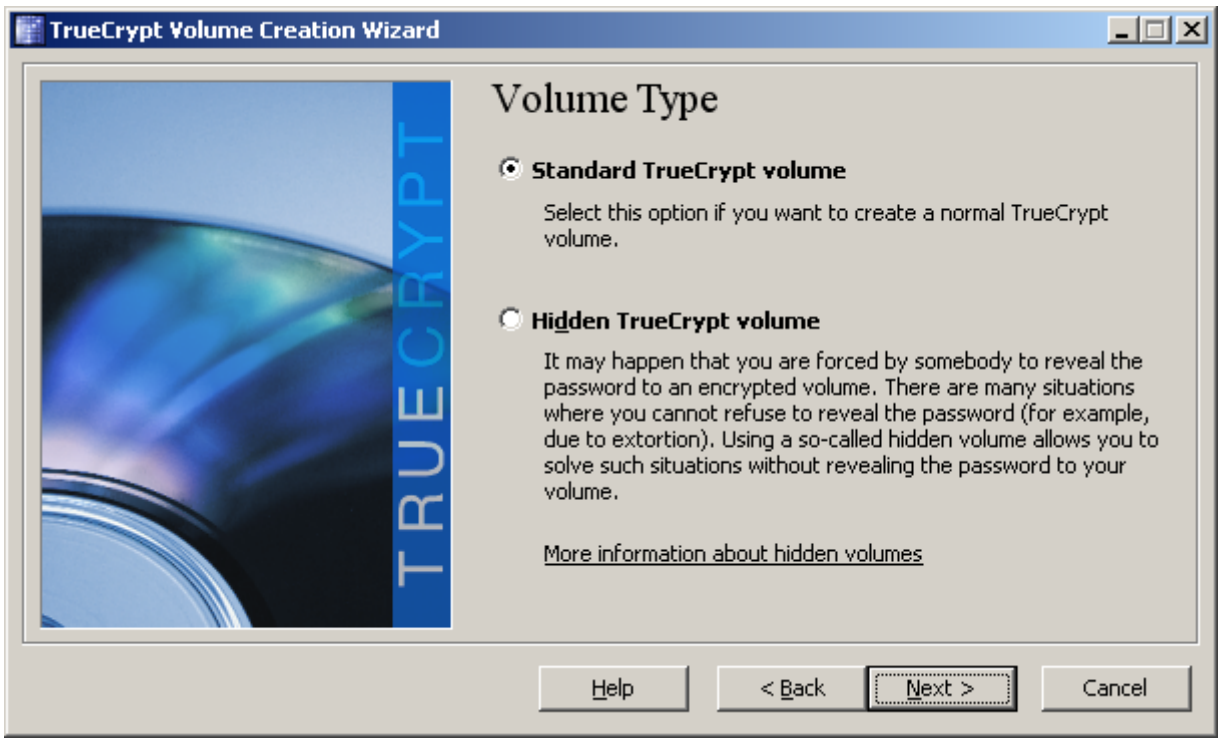
Les données cryptées sont stockées dans un fichier, à priori inutilisable par quiconque ne connait pas votre mot de passe (dans cette doc, le fichier est D:\GT\TrueCrypt\GT_TC).
En fournissant le mot de passe, le contenu de ce fichier est décrypté, et il est "monté" dans un volume (au même titre que C: ou toute autre unité de disque externe ou clef USB. Dans cette doc, le volume est S:). On peut travailler dans ce volume comme dans un volume ordinaire (créer des arborescences, des fichiers de toute sorte, etc...). Quand on "démonte" le volume, tout son contenu est réintégré dans le fichier crypté et redevient inaccessible.

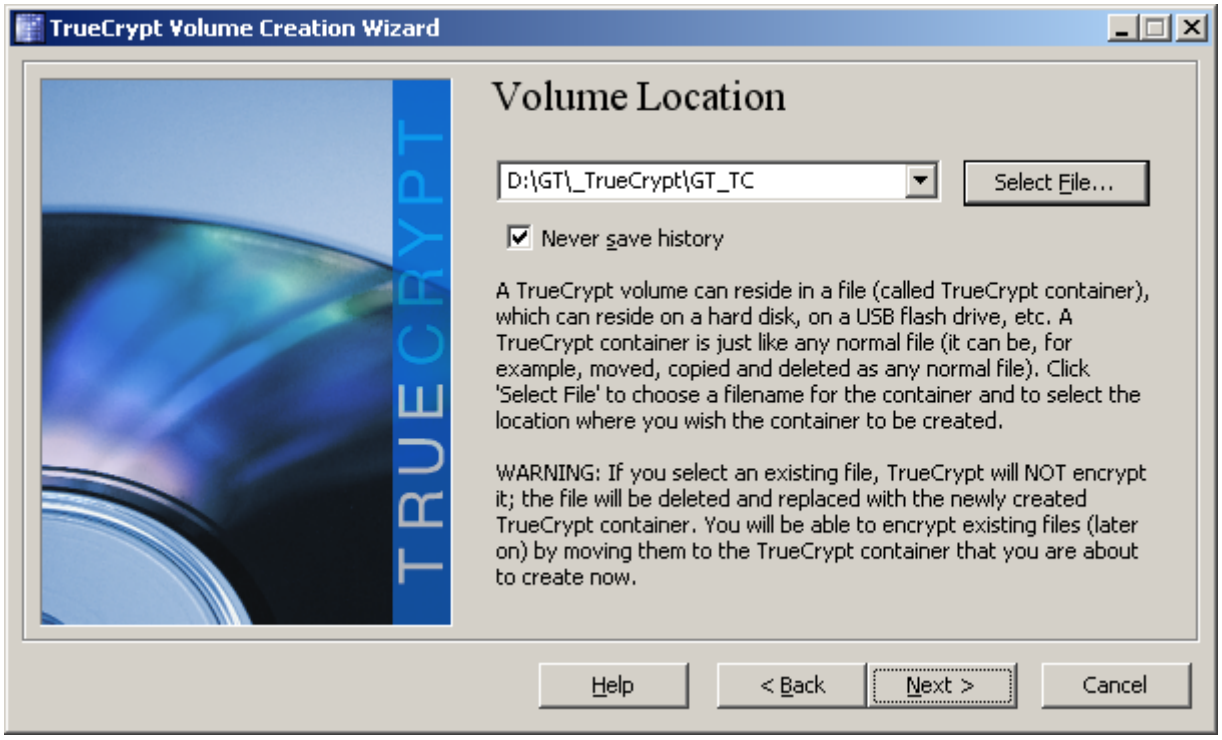
Créer un volume pour TrueCrypt

Cliquer sur Create Volume



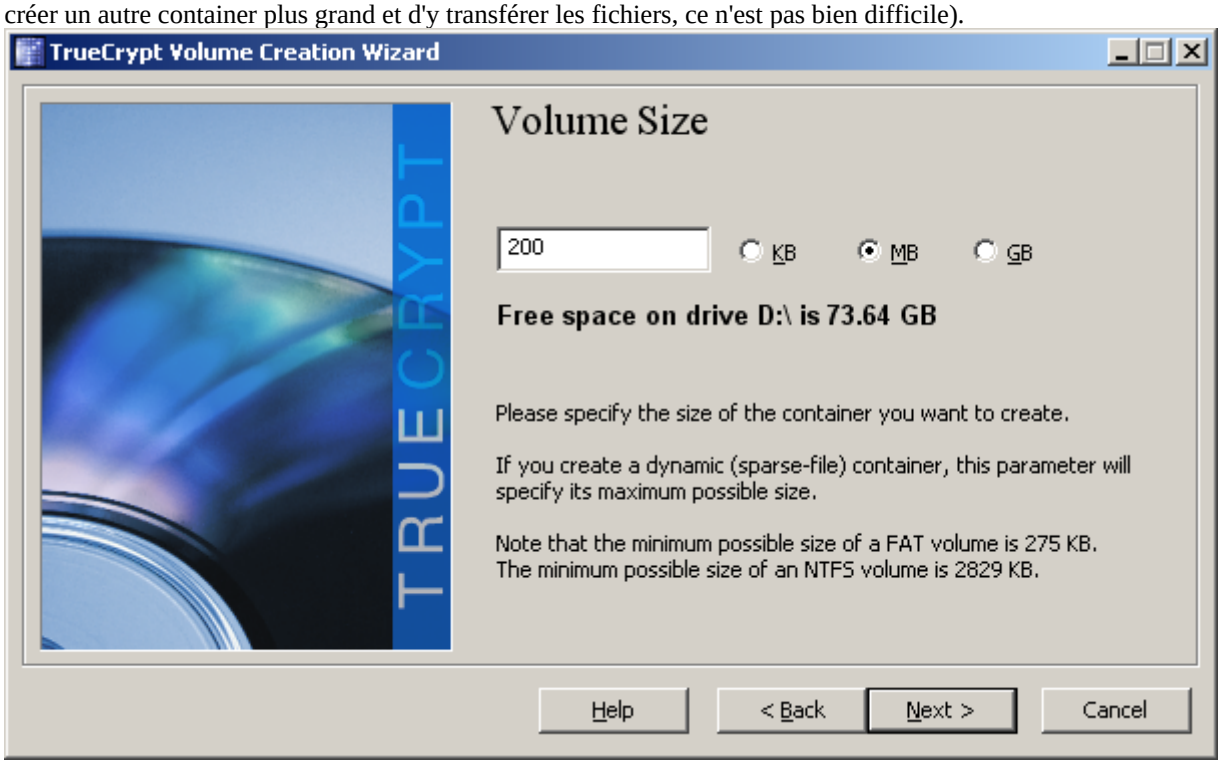

TrueCrypt Volume Creation Wizard
TrueCrypt Volume Creation Wizard
TRUECRYPT
Create an encrypted file container
Creates a virtual encrypted disk within a file. Recommended for inexperienced users.
More information
Encrypt a non-system partition/drive
Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume.
Encrypt the system partition or entire system drive
Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files, etc., will need to enter the correct password each time before Windows boots. Optionally, creates a hidden system.
More information about system encryption
Help
< Back
Next >
Cancel

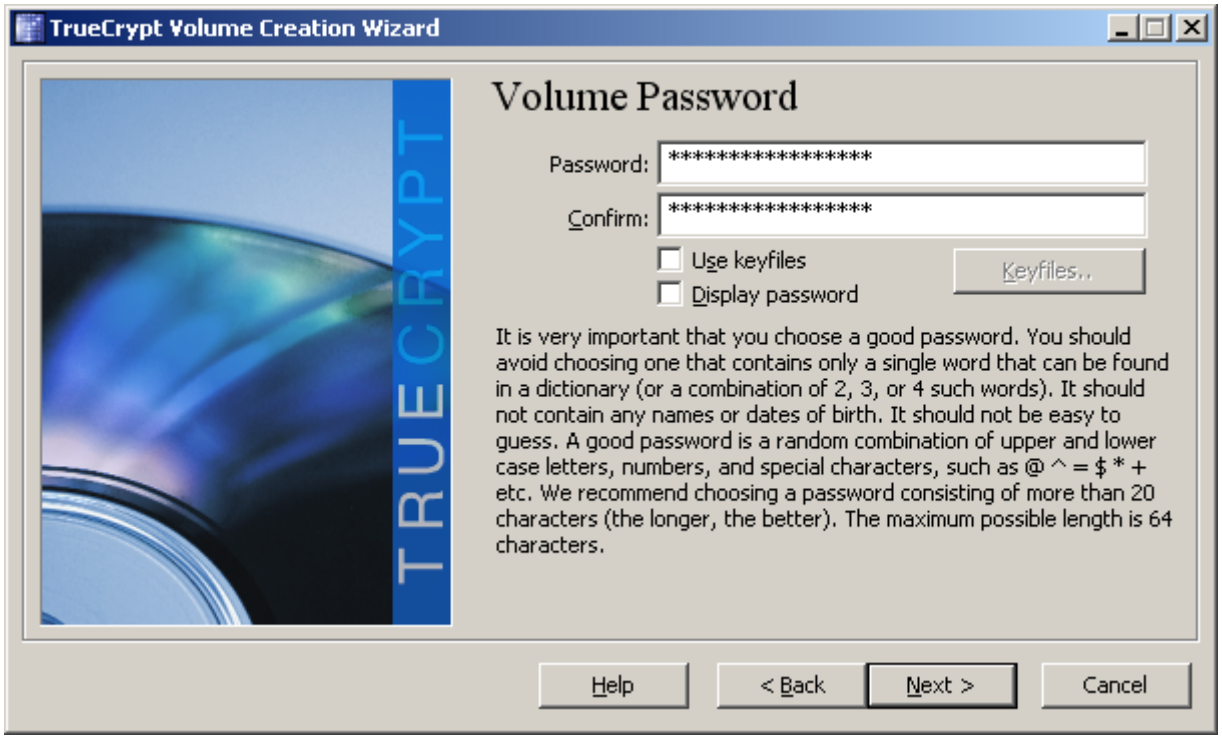

TrueCrypt Volume Creation Wizard
Volume Type
TRUECRYPT
Standard TrueCrypt volume
Select this option if you want to create a normal TrueCrypt volume.
Hidden TrueCrypt volume
It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you 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.
More information about hidden volumes
Help
< Back
Next >
Cancel


TrueCrypt Volume Creation Wizard
TRUECRYPT
Volume Location
D:\GT_TrueCrypt\GT_TC
Select File...
Never save history
A TrueCrypt volume can reside in a file (called TrueCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A TrueCrypt container is just like any normal file (it can be, for example, moved, copied and deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.
WARNING: If you select an existing file, TrueCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created TrueCrypt container. You will be able to encrypt existing files (later on) by moving them to the TrueCrypt container that you are about to create now.
Help
< Back
Next >
Cancel

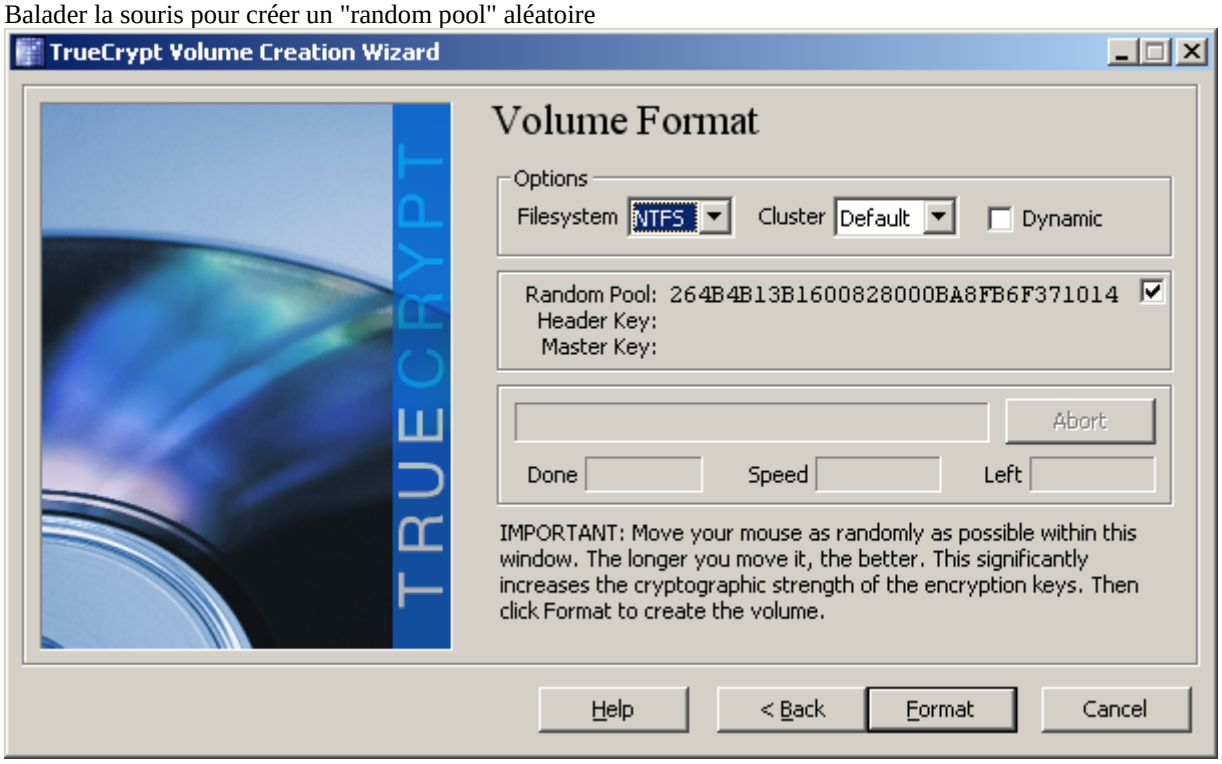
Personnellement, je garde les paramètres par défaut :

Donner la taille. On ne pourra pas la modifier ensuite, donc ne soyez pas trop chiche (mais si on veut l'agrandir, il suffira de créer un autre container plus grand et d'y transférer les fichiers, ce n'est pas bien difficile).

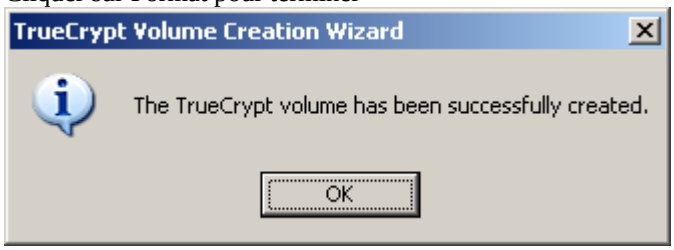




Personnellement, je choisis le format NTFS qui est plus sûr.
Balader la souris pour créer un "random pool" aléatoire

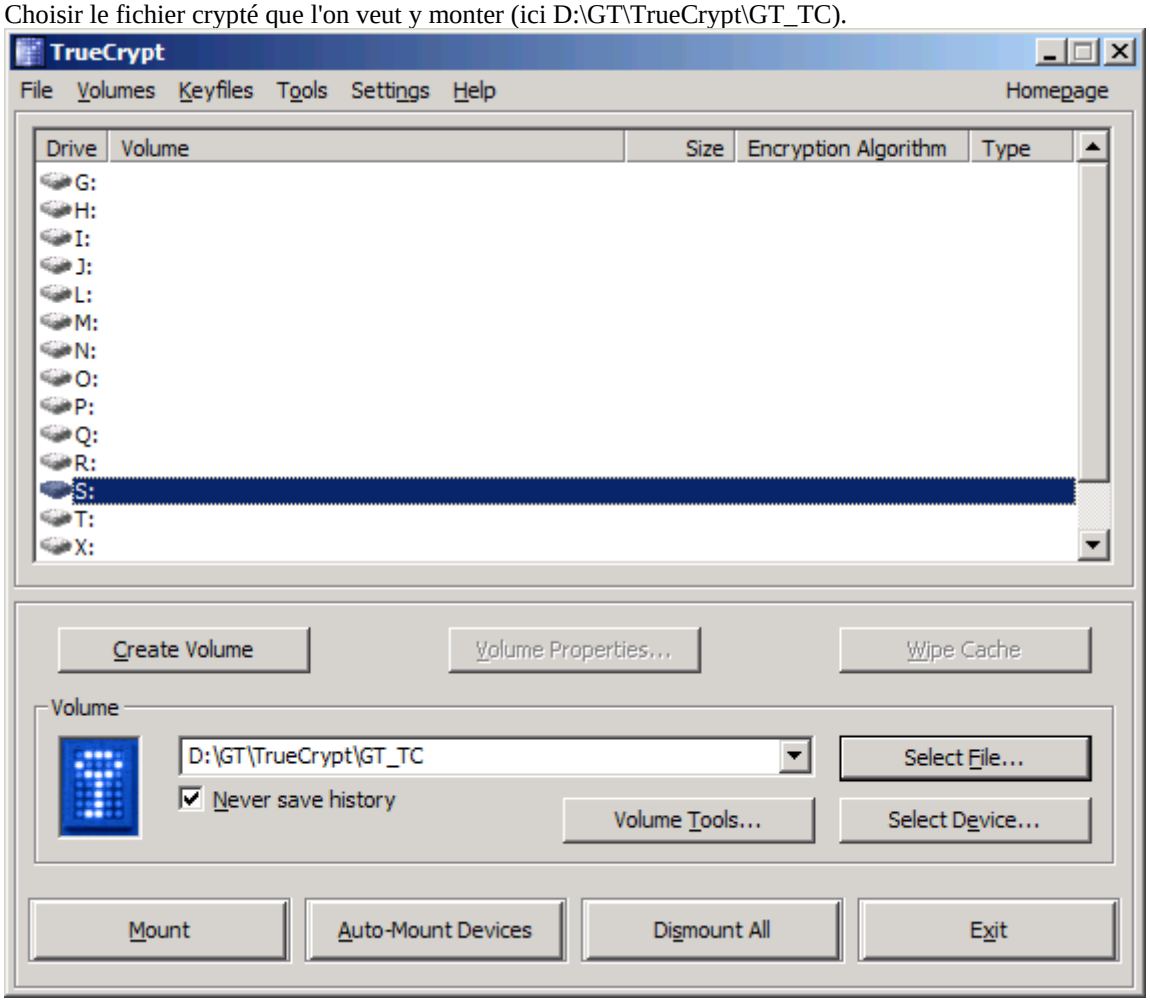


Cliquer sur Format pour terminer

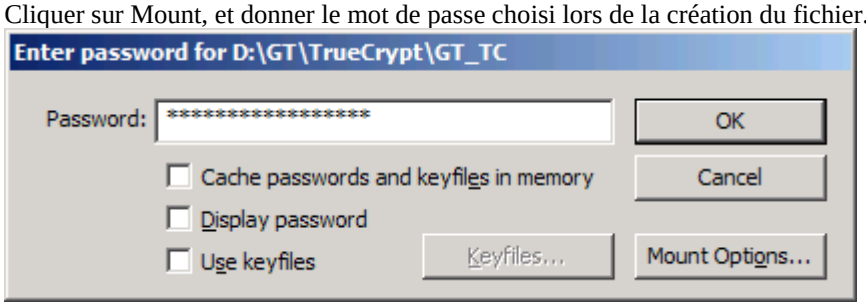


Premier montage

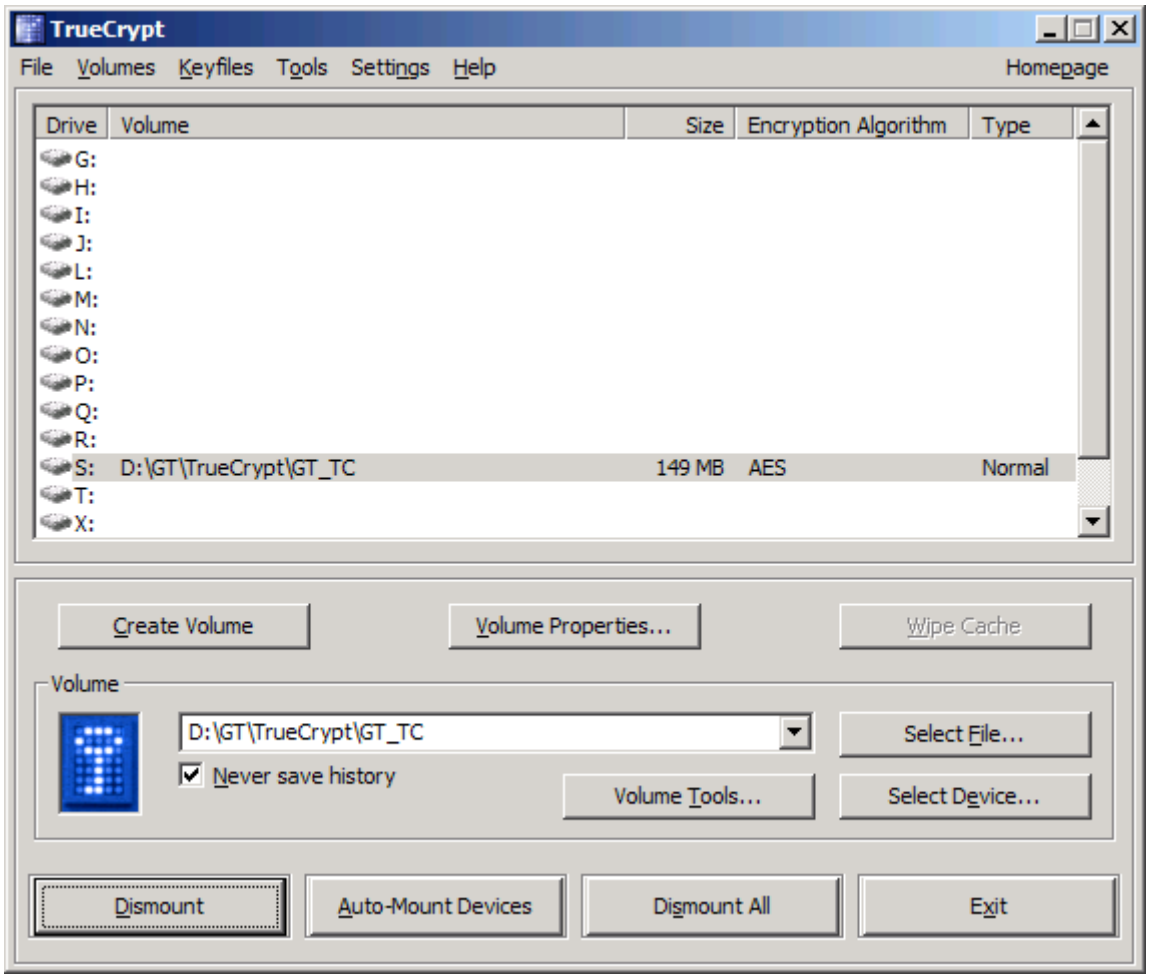
Choisir la lettre de l'unité (Drive) dans laquelle on veut monter les données cryptées (ici S:).
Choisir le fichier crypté que l'on veut y monter (ici D:\GT\TrueCrypt\GT_TC).



Cliquer sur Mount, et donner le mot de passe choisi lors de la création du fichier.



et le fichier est monté dans S:



On peut maintenant utiliser l'unité S:

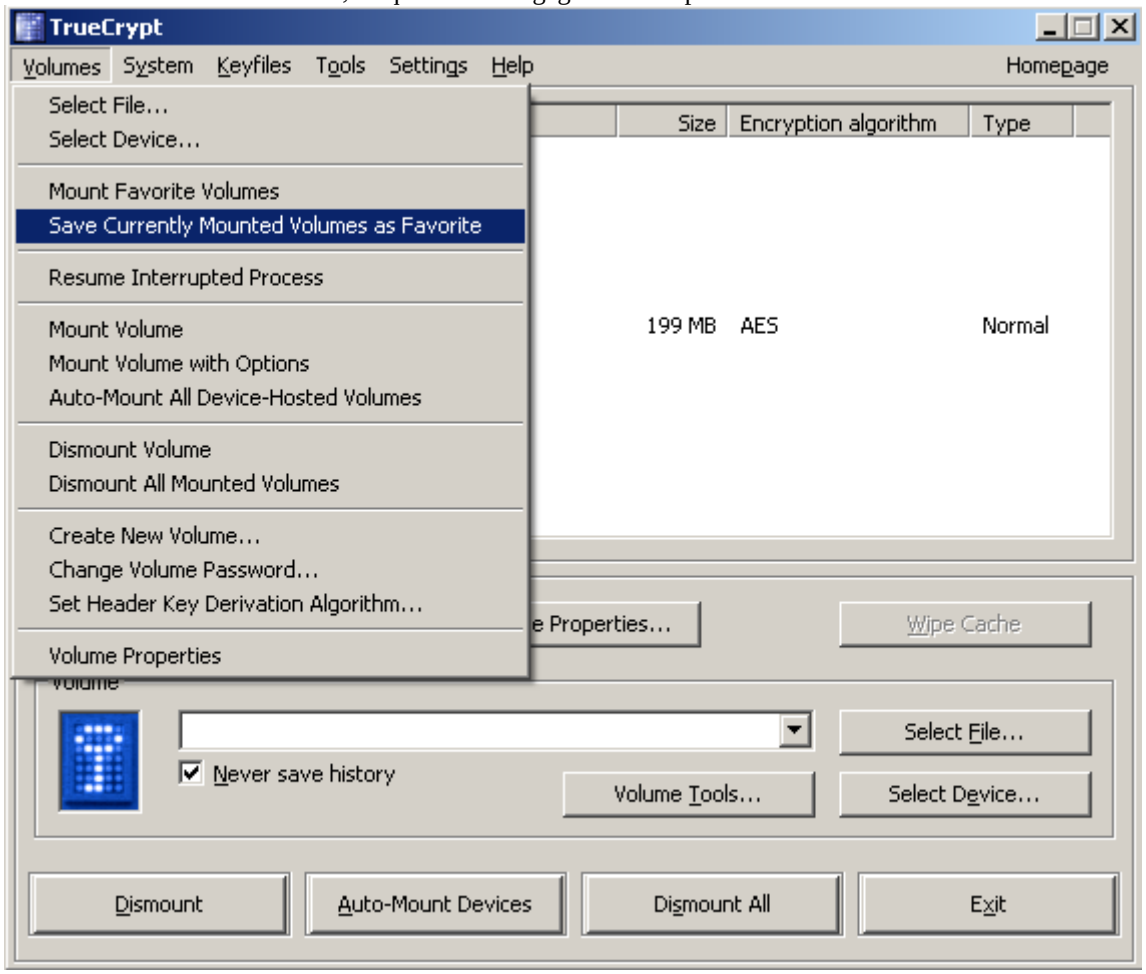
Réglages

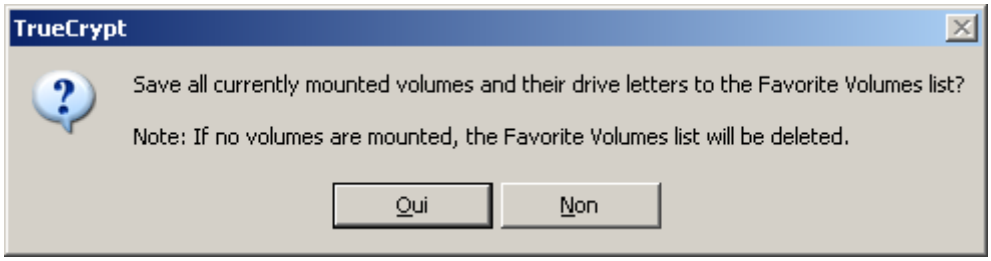
Save Currently Mounted Volumes as Favorite

NOTA: les menus ont changé depuis que j'ai fait la doc ci-dessous. Voir http://www.truecrypt.org/docs/?s=favorites
Pour faire bref:

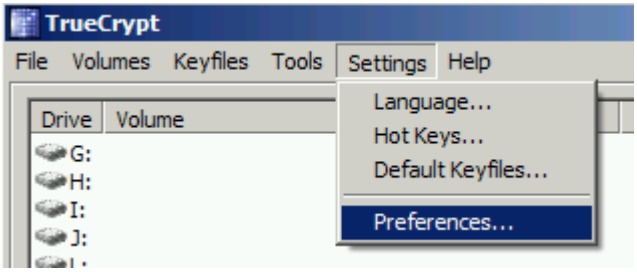
- il y a un nouveau menu "Favorites" dans la barre d'outils
- Pour sauver un volume monté comme favori, faire un clic-droit dessus

Après avoir monté votre volume, faire "Save Currently Mounted Volumes as Favorite". TrueCrypt va mémoriser les fichiers à monter et l'unité où il les monte, ce qui vous fera gagner du temps.

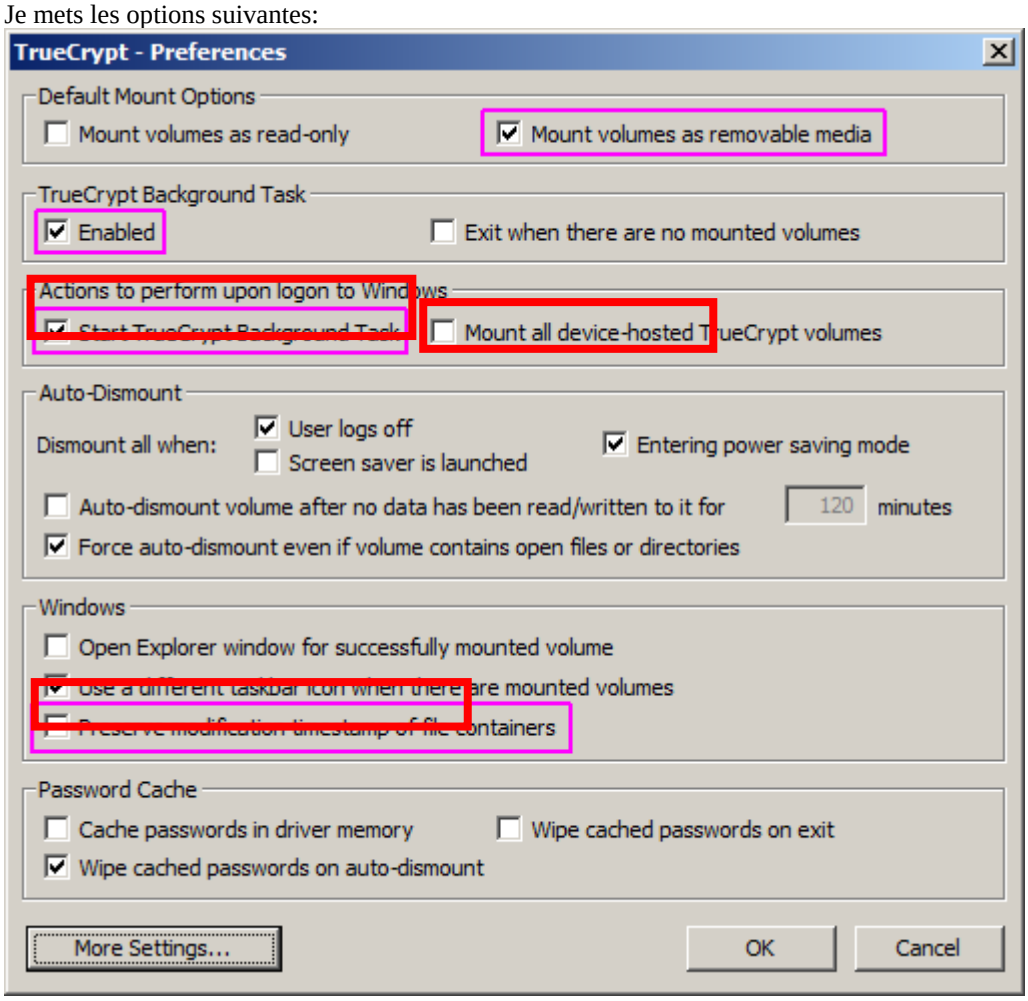




Settings > Preferences



Je mets les options suivantes:



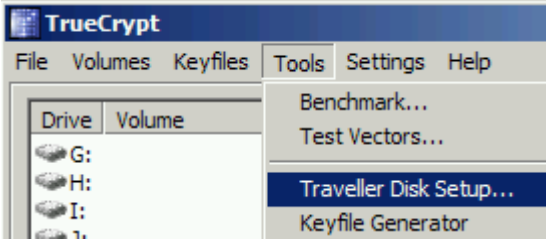
Avec ces réglages, TrueCrypt démarre automatiquement à chaque Session Windows. Il n'y a plus que le mot de passe à donner, ou bien il suffit d'ignorer si on ne veut pas décrypter les données.

"Preserve modification timestamp of file containers" est une option cochée par défaut. Il en résulte que le fichier contenant les données cryptées ne change jamais de date. C'est mieux pour la confidentialité, mais personnellement ça me gène d'avoir des données récentes et importantes dans un fichier qui conserve une date ancienne. Pour mes synchronisations et sauvegardes, je préfère décocher l'option.

"Mount volumes as removable media" a plusieurs avantages (à mon sens), décrits ici:
http://www.truecrypt.org/docs/?s=volume-mounted-as-removable-medium

TrueCrypt Traveller pour clef USB, disque externe,...

Il existe une option bien pratique qui configure un disque amovible ou une clef USB de manière à posséder une version de TrueCrypt autonome (à la fois le logiciel et les données cryptées sont sur la clef).



On peut ainsi trimbaler sa clef USB avec des données confidentielles sans aucun risque.
Si on a réglé convenablement les options, on branche la clef dans l'ordinateur hôte, on donne le mot de passe, et hop, les données cryptées sont montées.

Notes, FAQ,...

Quelques remarques en vrac

Peut-on perdre des données ?

Oui, quand le PC plante brusquement sans prévenir (écran bleu de Windows par exemple). Dans ce cas, si un volume TrueCrypt est monté, les données sont en RAM et n'ont pas le temps d'être réintégrées dans le volume. L'expérience montre qu'on peut perdre alors toutes les données de cette session TrueCrypt.

Par contre, dans le mode de fonctionnement normal, TrueCrypt ferme proprement le volume quand on quitte Windows, et il n'est pas nécessaire de démonter le volume avant de quitter Windows (bien que je vous le conseille fortement).

> http://www.truecrypt.org/faq
> **Do I have to dismount TrueCrypt volumes before shutting down or restarting Windows?**
> No. TrueCrypt automatically dismounts all mounted TrueCrypt volumes on system shutdown/restart.

J'ai réalisé ensuite qu'il existe une option "Mount volumes as removable media". Il semblerait qu'en l'activant, on gagne en sécurité. Mais ce n'est pas très clair...
http://www.truecrypt.org/docs/?s=volume-mounted-as-removable-medium

> **Volume Mounted as Removable Medium**
> This section applies to TrueCrypt volumes mounted when one of the following options is enabled (as applicable):
> - Tools > Preferences > Mount volumes as removable media
> - Mount Options > Mount volume as removable medium
> - Favorites > Organize Favorite Volumes > Mount selected volume as removable medium
> - Favorites > Organize System Favorite Volumes > Mount selected volume as removable medium
>
> TrueCrypt Volumes that are mounted as removable media have the following advantages and disadvantages:
> - Windows is prevented from automatically creating the 'Recycled' and/or the 'System Volume Information' folders on TrueCrypt volumes (in Windows, these folders are used by the Recycle Bin and System Restore features).
> - Windows may use caching methods and write delays that are normally used for removable media (for example, USB flash drives). This might slightly decrease the performance but at the same increase the likelihood that it will be possible to dismount the volume quickly without having to force the dismount.
> - The operating system may tend to keep the number of handles it opens to such a volume to a minimum. Hence, volumes mounted as removable media might require fewer forced dismounts than other volumes.
> - Under Windows Vista and earlier, the 'Computer' (or 'My Computer') list does not show the amount of free space on volumes mounted as removable (note that this is a Windows limitation, not a bug in TrueCrypt).
> - Under desktop editions of Windows Vista or later, sectors of a volume mounted as removable medium may be accessible to all users (including users without administrator privileges; see section Multi-User Environment).

Et aussi :

> http://www.truecrypt.org/faq
> **Can I unplug or turn off a hot-plug device (for example, a USB flash drive or USB hard drive) when there is a mounted TrueCrypt volume on it?**
> Before you unplug or turn off the device, you should always dismount the TrueCrypt volume in TrueCrypt first, and then perform the 'Eject' operation if available (right-click the device in the 'Computer' or 'My Computer' list), or use the 'Safely Remove Hardware' function (built in Windows, accessible via the taskbar notification area). Otherwise, data loss may occur.

> http://www.truecrypt.org/faq
> **What will happen when a part of a TrueCrypt volume becomes corrupted?**
> In encrypted data, one corrupted bit usually corrupts the whole ciphertext block in which it occurred. The ciphertext block size used by TrueCrypt is 16 bytes (i.e., 128 bits). The mode of operation used by TrueCrypt ensures that if data corruption occurs within a block, the remaining blocks are not affected. See also the question 'What do I do when the encrypted filesystem on my TrueCrypt volume is corrupted?

> http://www.truecrypt.org/faq
> **What do I do when the encrypted filesystem on my TrueCrypt volume is corrupted?**
> File system within a TrueCrypt volume may become corrupted in the same way as any normal unencrypted file system. When that happens, you can use filesystem repair tools supplied with your operating system to fix it. In Windows, it is the 'chkdsk' tool. TrueCrypt provides an easy way to use this tool on a TrueCrypt volume: Right-click

the mounted volume in the main TrueCrypt window (in the drive list) and from the context menu select 'Repair Filesystem'.