Chiffrer ses données avec VeraCrypt

Vincent GIRAUD

Jeudi 15 février 2018

Festival des Libertés Numériques

Document disponible à l'adresse https://www.giraud.eu/contenus/initiation-chiffrement.pdf

Qu’est-ce que le chiffrement ?

Chiffrement

\ʃi.fʁə.mɑ̃\ masculin

Procédé utilisé en cryptographie permettant de protéger un document en le rendant incompréhensible à toute personne ne possédant pas la clé.

(Selon Wiktionnaire)

Qu’est-ce que le chiffrement ?

Concrètement, quand je chiffre mes données :

Elles ne sont pas lisibles si l’on a pas le mot de passe…

Elles le deviennent après soumission du mot de passe…

Donc une application malicieuse peut simplement attendre que vous déchiffriez vos données pour les exploiter !

➡ Le chiffrement protège surtout vos données au repos, lorsque votre périphérique n’est pas utilisé ou éteint

Pourquoi chiffrer ses données ?

- Pour défendre ses libertés
- Pour préserver sa propriété intellectuelle
- Pour protéger ses sources et ses informations sensibles
- Pour se protéger des gouvernements

Pourquoi chiffrer ses données ?

Que deviendraient vos données si vous vous faisiez cambrioler ?

Si vos équipements sont contrôlés lors d’un passage de frontière ?

Si vous perdez votre ordinateur ou support ?

Un procédé de plus en plus répandu

- Maintenant souvent activé par défaut
  - Android 6 et plus
  - iOS 8 et plus
- Conseillé par l’ANSSI et promu par le parlement européen

Que chiffrer ?

On chiffre un périphérique de stockage.

Celui-ci peut-être amovible :

- Clé USB
- Disque dur externe
- Carte SD, microSD…

Ou non :

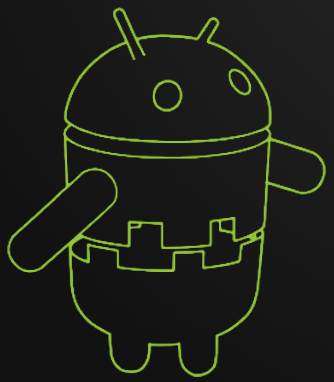
- Disque dur
- SSD, mémoire flash…

Avec quoi ?

DriveCrypt

VeraCrypt

DIGITALGUARDIAN®



Avec quoi ?

SILL 2018 : l'État actualise son référentiel de logiciels libres

Qu'est-il recommandé pour la conception et le développement logiciel cette année ?

Le 13 février 2018, par Michael Guilloux, Chroniqueur Actualités

developpez.com

Security

Brazilian banker's crypto baffles FBI

18 months of failure

By John Leyden 28 Jun 2010 at 11:49 97 SHARE ▼

Cryptographic locks guarding the secret files of a Brazilian banker suspected of financial crimes have defeated law enforcement officials.

Brazilian police seized five hard drives when they raided the Rio apartment of banker Daniel Dantas as part of Operation Satyagraha in July 2008. But subsequent efforts to decrypt files held on the hardware using a variety of dictionary-based attacks failed even after the South Americans called in the assistance of the FBI.

The files were encrypted using Truecrypt and an unnamed algorithm, reportedly based on the 256-bit AES standard. In the UK, Dantas would be compelled to reveal his passphrase under threat of imprisonment, but no such law exists in Brazil.

The Register

TrueCrypt a subi 2 audits de sécurité, et a eu deux versions certifiées par l'ANSSI.

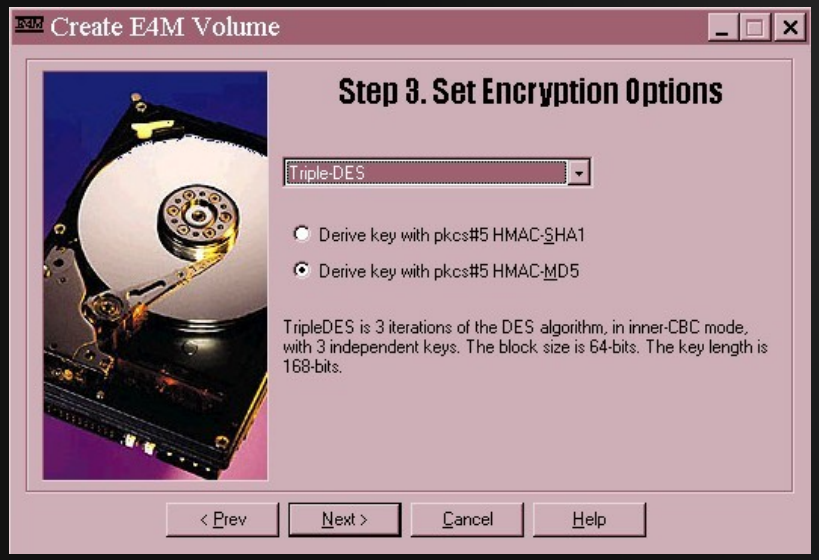
VeraCrypt a subi un audit de sécurité à ce jour.

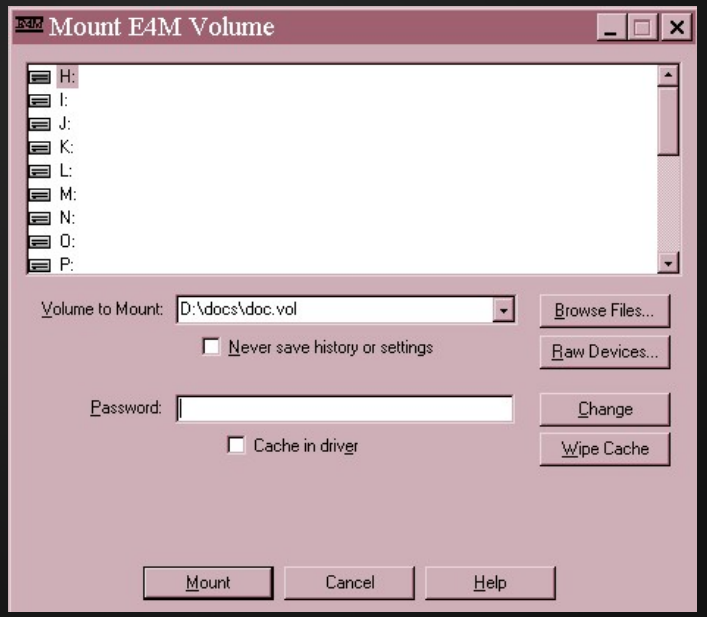
Le chiffrement n'est rien sans un bon mot de passe !

Historique du chiffrement libre

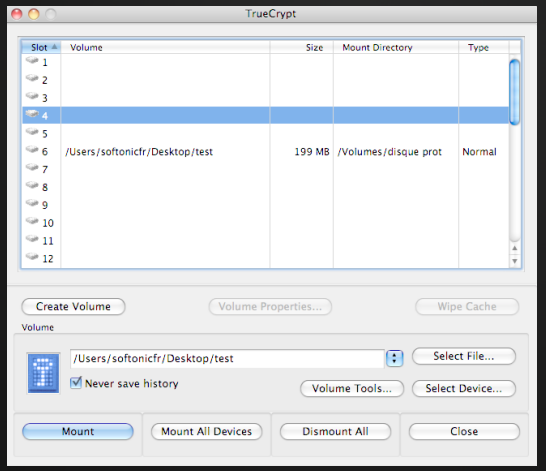
1997

E4M





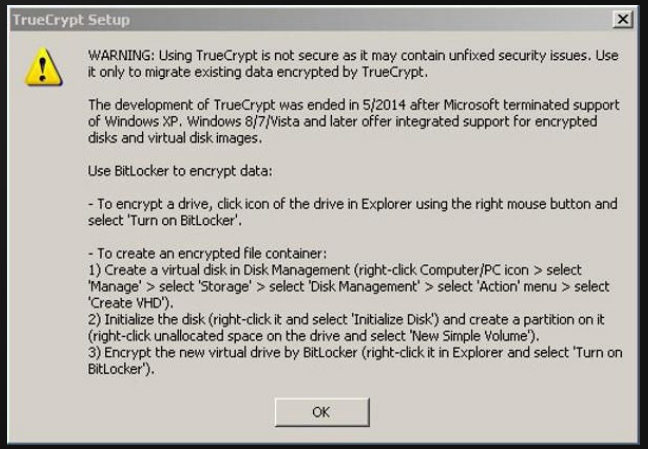
Historique du chiffrement libre



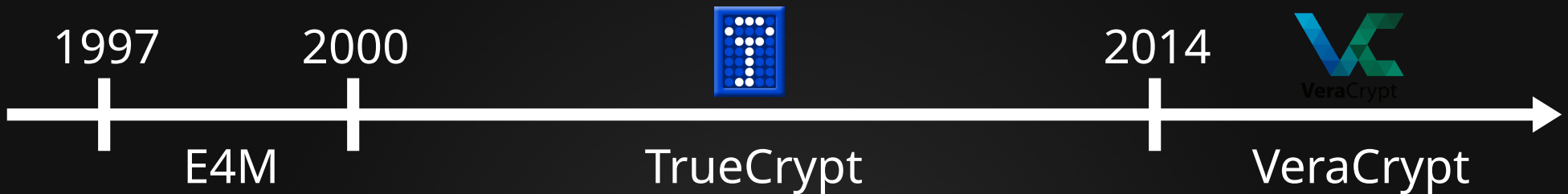
WARNING: Using TrueCrypt is not secure as it may contain unfixed security issues

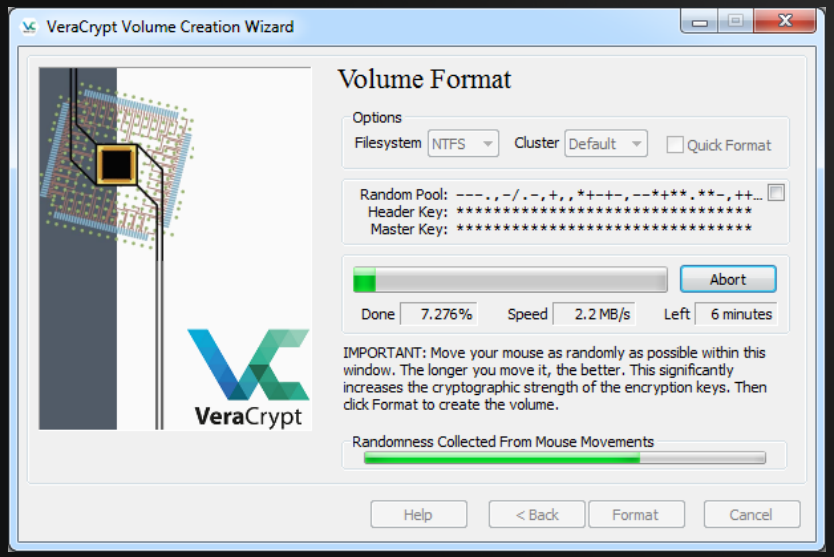
This page exists only to help migrate existing data encrypted by TrueCrypt.

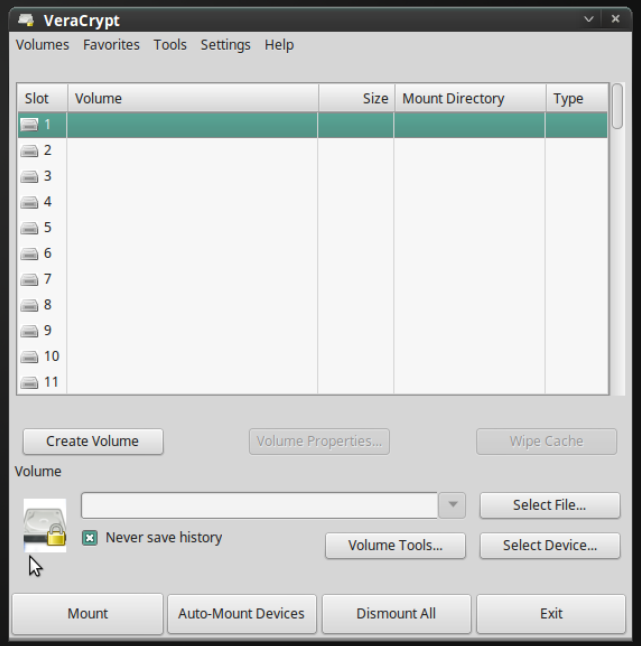
The development of TrueCrypt was ended in 5/2014 after Microsoft terminated support of Windows XP. Windows 8/7/Vista and later offer integrated support for encrypted disks and virtual disk images. Such integrated support is also available on other platforms (click here for more information). You should migrate any data encrypted by TrueCrypt to encrypted disks or virtual disk images supported on your platform.



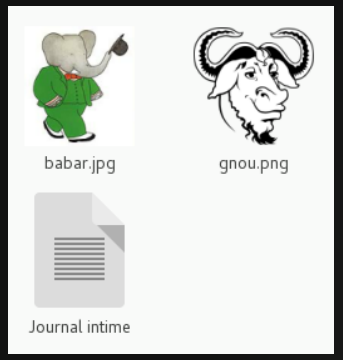
Historique du chiffrement libre







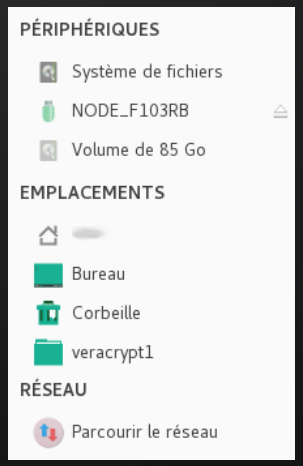
Utilisation en pratique

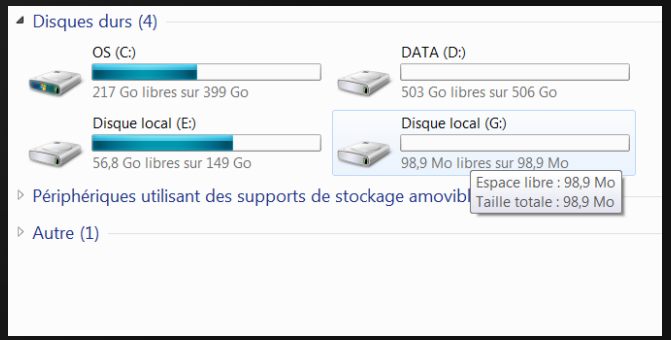


Je souhaite chiffrer des fichiers.

Quelles implications en pratique ?

Une fois déverrouillés, ceux-ci apparaissent dans un lecteur virtuel



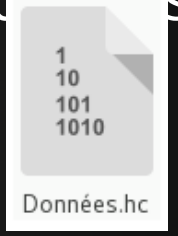


Utilisation en pratique

Deux possibilités

Chiffrer une partition du périphérique

Créer une archive chiffrée avec ses fichiers dedans

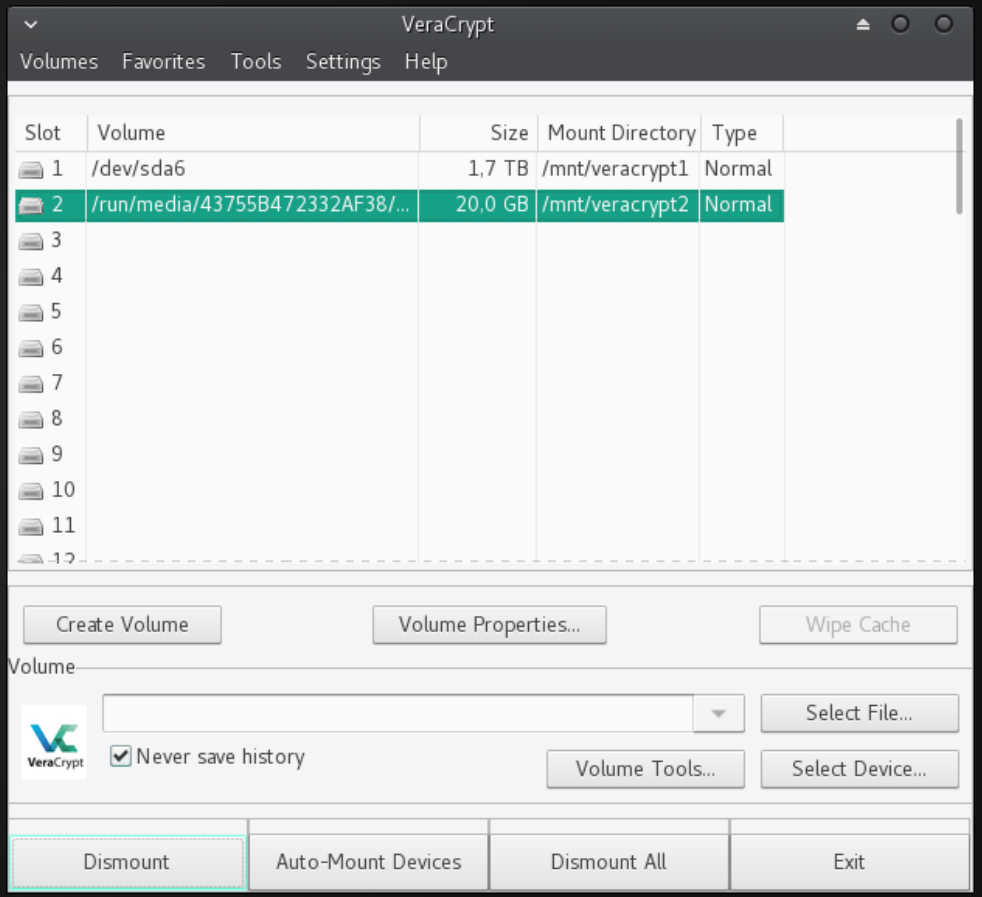


Le fichier ou la partition restera de taille fixe quelle que soit la quantité de données à l'intérieur.

Le temps nécessaire pour déverrouiller ne dépend pas de la taille du volume chiffré.

Utilisation en pratique

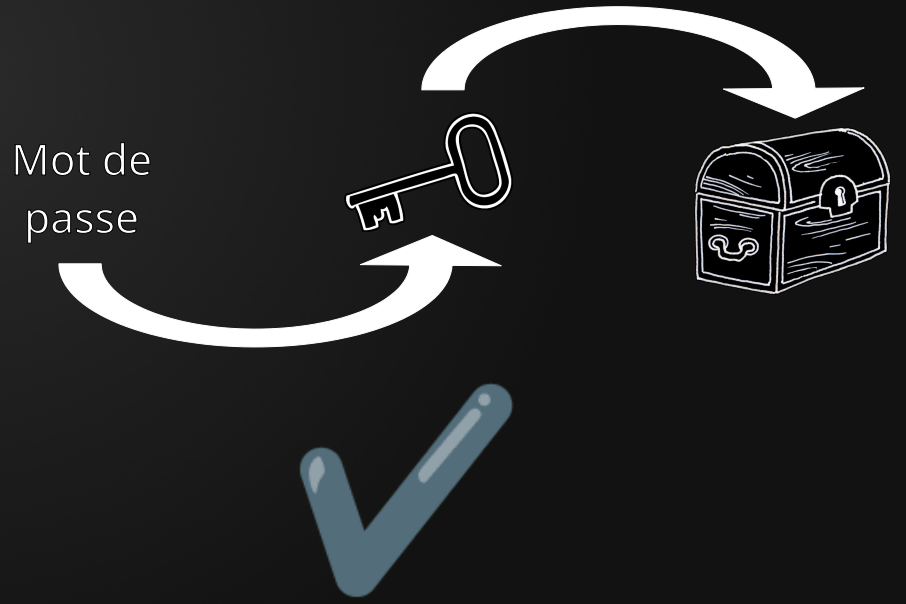
Fenêtre principale de VeraCrypt



Une fois déchiffrés, volumes et archives fonctionnent exactement de la même manière

Utilisation en pratique

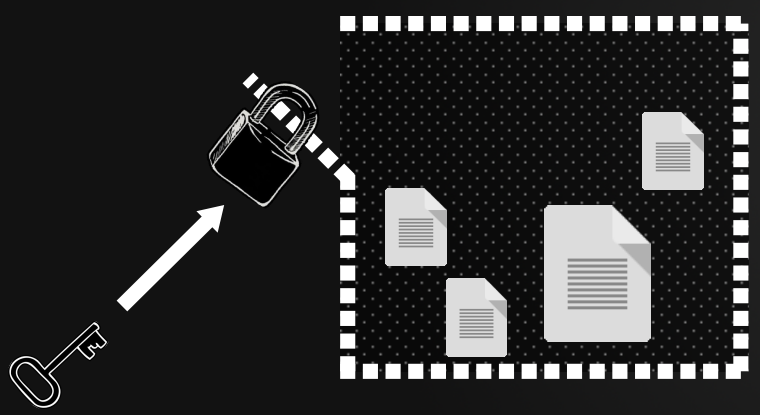
VeraCrypt ne chiffre pas les données directement avec le mot de passe



Utilisation en pratique

Déni plausible

VeraCrypt supporte le déni plausible, utile en cas d'extorsion (chantage, violences...)



En temps normal...

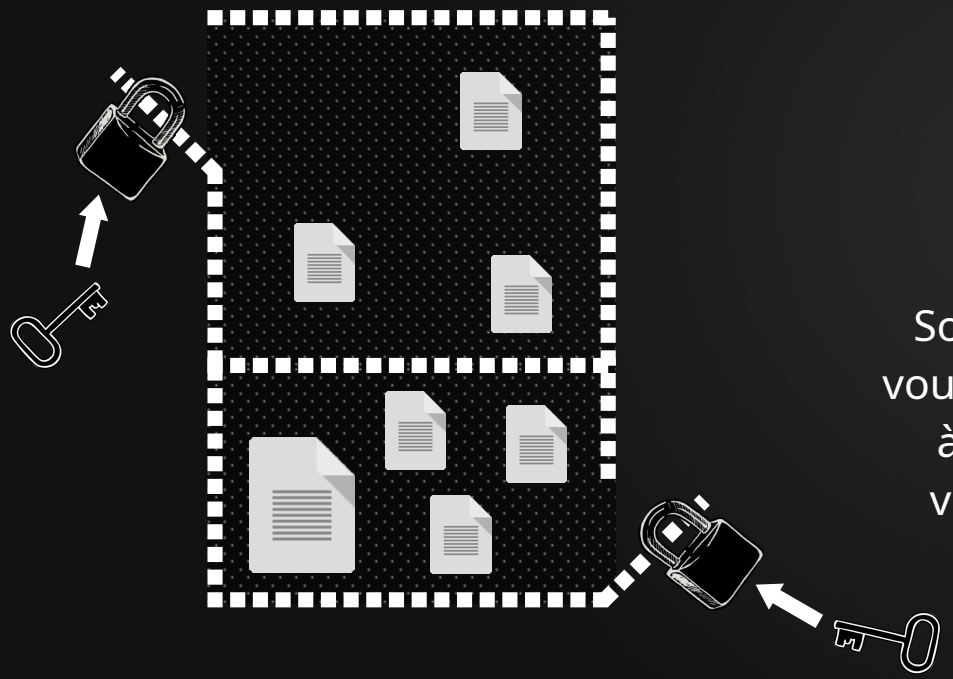
Sous pression, vous êtes forcé(e) à soumettre votre mot de passe.

L'attaquant obtient l'accès, vos données sont compromises.

Utilisation en pratique

Déni plausible

VeraCrypt supporte le déni plausible, utile en cas d'extorsion (chantage, violences...)



Avec le déni plausible...

Sous pression, vous êtes forcé(e) à soumettre votre mot de passe.

Vous donnez le faux mot de passe, l'attaquant accède à la première couche de chiffrement. Rien n'indique la présence d'une seconde couche.

Lorsque vous êtes en sécurité, taper le vrai mot de passe vous amène directement à la seconde couche : la vraie

Utilisation en pratique

Deux contraintes :

- Les droits administrateurs sont nécessaires

- Sans VeraCrypt, impossible de déchiffrer

Utilisation en pratique

Je veux chiffrer ma clé USB de 16 Go, pour pouvoir la garder avec moi malgré les fichiers sensibles dessus. Je souhaite pouvoir l'utiliser sur d'autres ordinateurs que le mien.

Meilleur compromis : chiffrer quasiment toute la clé, en laissant un peu d'espace libre pour avoir le logiciel VeraCrypt en clair !

Données chiffrées