I. OBJET ET DOMAINE D'APPLICATION

Le CHU AMIENS PICARDIE a mis en œuvre la présente procédure de cryptage pour chiffrer des données sur un répertoire ou un périphérique de stockage (clé USB, disque externe, …), recommandée par l'ANSSI, la CNIL et le RGPD.

II. DÉFINITIONS ET ABRÉVIATIONS

II.1 DEFINITIONS

AES : Advanced Encryption Standard, soit standard de chiffrement avancé en français

II.2 ABREVIATIONS

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information
CNIL : Commission Nationale Informatique et Libertés
RGPD : Règlement Général sur la Protection des Données à caractère personnel

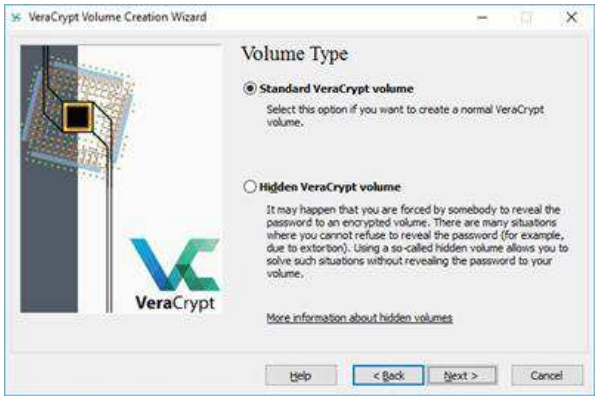
III. DESCRIPTION

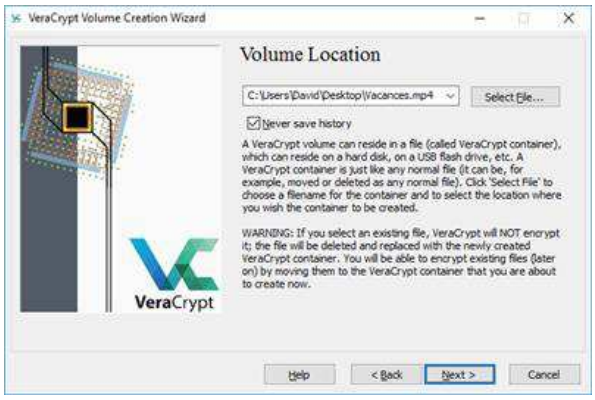
Veracrypt – logiciel de cryptage pour chiffrer des répertoires ou périphériques : clés USB, disques durs internes ou externes. VeraCrypt est un logiciel libre qui permet de chiffrer un répertoire sous Windows, Mac et GNU/Linux.

La création d'un conteneur :

Ici, il s'agit de protéger des fichiers et des répertoires qui seront placés dans un fichier, un peu comme lorsque l'on compresse des données avec un mot de passe avec des outils tels que 7-Zip, WinRAR ou WinZip. La différence ici, c'est qu'il sera possible de « monter » ce fichier qui apparaîtra alors comme un lecteur physique.

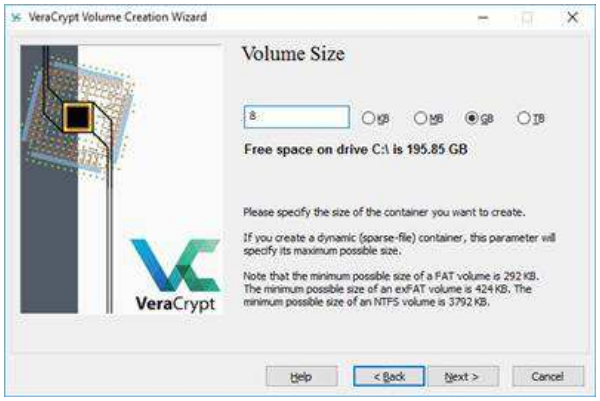
Pour procéder cliquez sur *Create Volume* puis *Create an encrypted file container*. Dans un premier temps nous opterons pour un volume standard. Sélectionnez ensuite un nom de fichier à créer et indiquez si vous voulez l'enregistrer dans l'historique ou non. Notez qu'il est possible d'utiliser n'importe quel nom de fichier et n'importe quelle extension. Cela permet de le rendre plus « discret » :





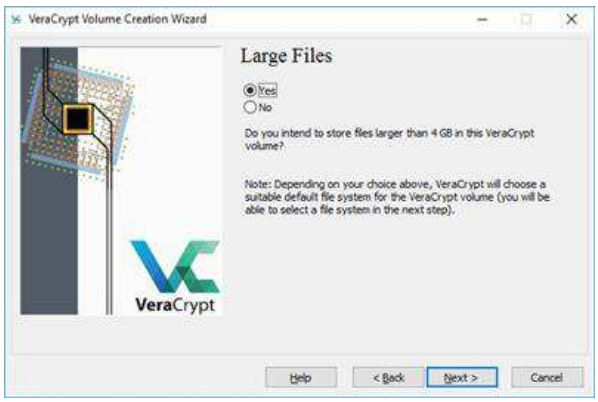
Il faudra ensuite choisir parmi les algorithmes de chiffrement et de hash. Notez que dans le cas des algorithmes de chiffrement, il est tout à fait possible d'en cumuler plusieurs, jusqu'à un maximum de trois. Ce sera le cas si *Serpent(Twofish(AES))* est sélectionné par exemple.

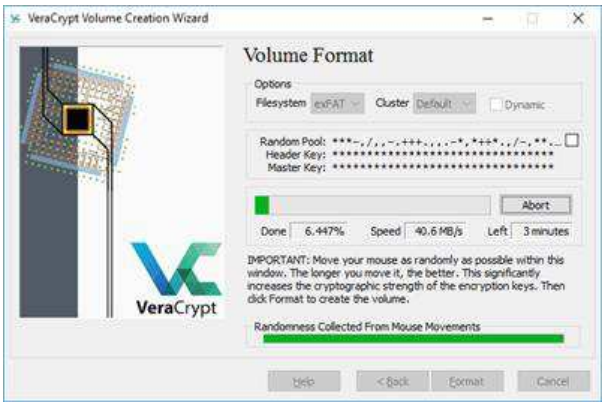
Il faudra ensuite choisir la taille du conteneur, ce qui représente l'espace qui sera disponible une fois qu'il sera monté, puis les éléments de sécurité qui permettront d'assurer le chiffrement/déchiffrement :



VeraCrypt demandera s'il est prévu de stocker des fichiers de plus de 4 Go, ce qui changera simplement le système de fichiers sélectionné par défaut pour le formatage. Il sera de toute façon possible de le modifier dans la fenêtre suivante, avec d'autres paramètres comme la taille des clusters ou le fait que le volume soit dynamique ou non.

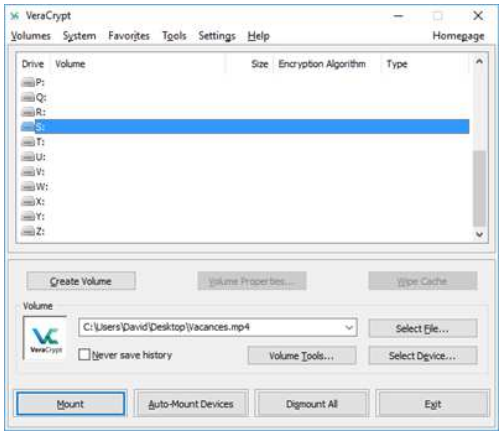
Il faudra ensuite bouger la souris au sein de la fenêtre pour générer assez de données aléatoires pour assurer une entropie suffisante pour les clefs de chiffrement. On pourra alors passer au formatage :

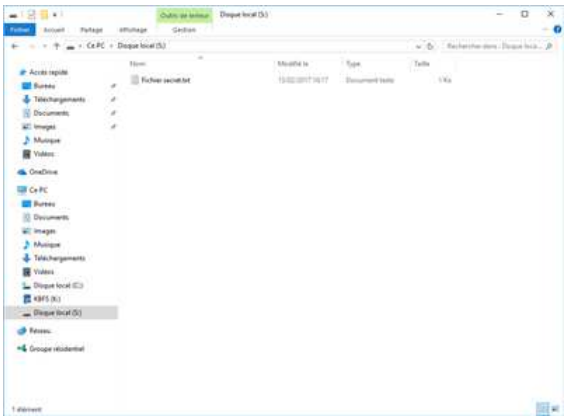




Une fois cette phase terminée il sera temps de quitter la procédure de création. L'interface principale permettra alors de sélectionner une lettre de lecteur disponible, votre fichier (*Select File...*) puis de le monter. Ici, il faudra entrer les différents éléments de sécurité (mot de passe, fichiers clef, PIM). Des options complémentaires permettront d'opter pour la mise en place d'un lecteur accessible uniquement en lecture, vu comme un périphérique externe, etc.

Un lecteur physique apparaîtra alors dans le gestionnaire de fichiers. On pourra y créer, supprimer ou déplacer des éléments comme s'il s'agissait d'un périphérique de stockage. Une fois que l'accès n'est plus nécessaire, il suffit de le démonter. Le conteneur sera alors vu comme un fichier lambda, de la taille définie lors de sa création.





IV. RÉFÉRENCES

Site de l'éditeur du logiciel
https://www.veracrypt.fr/en/Downloads.html

V. ÉVALUATION

Le logiciel VeraCrypt est validé et recommandé par l'ANSSI, ainsi que la CNIL et le RGPD
https://www.cnil.fr/fr/comment-chiffrer-ses-documents-et-ses-repertoires