**EXPOSE DE CRYPTOGRAPHIE**

**Groupe 2 :**

**Membres du groupe :**

* Kone Yaya
* Diakite Abdoul Junior
* Gbatto Loualou Flora Davila
* Bamba N’giantchan Alassane

**Présentation**

Contenu :

Dans cet expose nous traiterons de deux thèmes. Ces thèmes nous entretiendrons sur deux outils logiciels dans la pratique de cryptographie.

**Thème 1 :**

Veracrypt : présentation, fonctionnement, avantages et limites.

**Thème 2 :**

Hashacalc : présentation, fonctionnement, avantages et limites.

Objectif :

* Connaitre Veracrypt et Hashacalc
* Comprendre leurs fonctionnements
* Savoir les utiliser pour la sécurisation de l’information

Table des matières

**Thème 11**

Introduction2

I/ Présentation et fonctionnement de veracrypt2

1. Présentation de veracrypt 3
2. Fonctionnement de veracrypt 3

II/ Avantages et limites 2

1. Avantages de veracrypt 3
2. Limites de veracrypt 3

**III/ Pratique 2**

**IV/ Conclusion 2**

**Thème 24**

Introduction2

I/ Présentation et fonctionnement de Hashacalc 2

1. Présentation de Hashacalc 3
2. Fonctionnement de Hashacalc 3

II/ Avantages et limites de Hashacalc 2

1. Avantages de Hashacalc 3
2. Limites de Hashacalc3

**III/ Pratique 2**

**IV/ Conclusion 2**

**Thème 1 :**

**VERACRYPT : PRESENTATION, FONCTIONNEMENT, AVANTAGES ET LIMITES.**

Introduction

La cryptographie est une**méthode de protection des informations et des communications par l’utilisation de codes**, de sorte que seuls les destinataires des informations puissent les lire et les traiter. De nos jours, elle nous offre de nombreux outils de chiffrements, notamment les outils logiciel tels que veracrypt, qui fait l’objet de notre étude. Verrons qu’est ce que veracrypt, comment fonctionne ce logiciel et, quelles sont ses avantages et ses limites.

**I/ Présentation et fonctionnement de veraCrypt**

1. Présentation de veraCrypt

VeraCrypt est un logiciel de chiffrement instantané open source, il permet de chiffrer et déchiffrer les données. VeraCrypt offre la possibilité de crypter des disques durs ou clés USB entièrement, de créer des partitions chiffrées ou bien encore des "conteneurs" protégés. En créant un disque virtuel crypté, vous pouvez protéger les fichiers importants. Il est basé sur la même interface que **TrueCrypt** dont le projet a été abandonné courant de l'année 2014.

Par ailleurs, avec ses divers algorithmes de chiffrement, vous pouvez sécuriser les fichiers avec un fichier de clé.

Les systèmes de chiffrements supportés par VeraCrypt sont :

* AES
* Camellia
* Kuznyechik (en)
* Serpent et Twofish

En outre, cinq combinaisons différentes de chiffrements en cascades sont possibles :

* AES-Twofish,
* AES-Twofish-Serpent,
* Serpent-AES,
* Serpent-Twofish-AES et
* Twofish-Serpent.

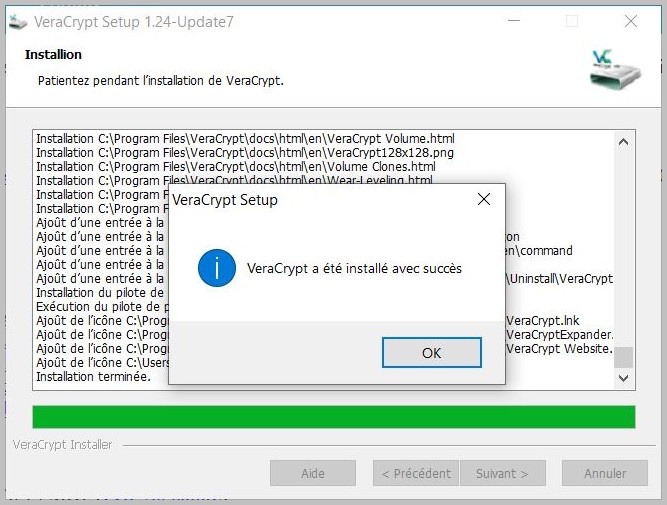
Les fonctions de hachage cryptographique disponibles pour une utilisation dans VeraCrypt sont **RipeMD-160, SHA-256, SHA-512, Streebog**et**Whirlpool**.

Les principales caractéristiques de VeraCrypt sont :

* La création des disques virtuels chiffrés et le monter simplement sur le système comme n’importe quel disque physique.
* Le chiffrer d’une partition entière ou un périphérique de stockage tel qu’une clé USB ou un disque dur.

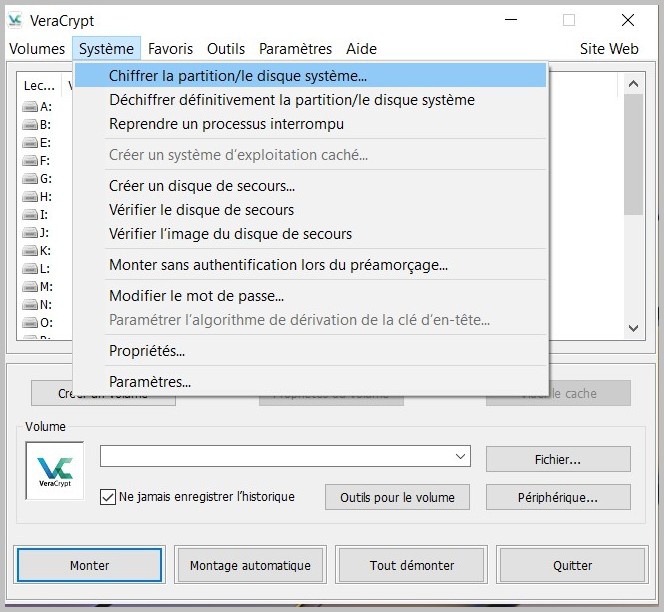
1. Fonctionnement de veraCrypt

D’abord pour Installer l’application sur votre ordinateur, rendez-vous sur <https://www.veracrypt.fr/en/Downloads.html> téléchargez la version qui convient à votre PC, puis installez la. Le logiciel vous demandera éventuellement de désactiver le démarrage rapide, ce qui nécessitera un redémarrage de la machine. Sur les ordinateurs récents qui utilisent le mode de démarrage UEFI, VeraCrypt ne peut pas chiffrer d’un coup la totalité du disque dur. Il faut donc d’abord chiffrer la partition système (C:), puis la partition qui stocke les données (D:). Si vous n’avez qu’une seule partition, cette seconde étape est évidemment superflue.



**Chiffrez la partition système**

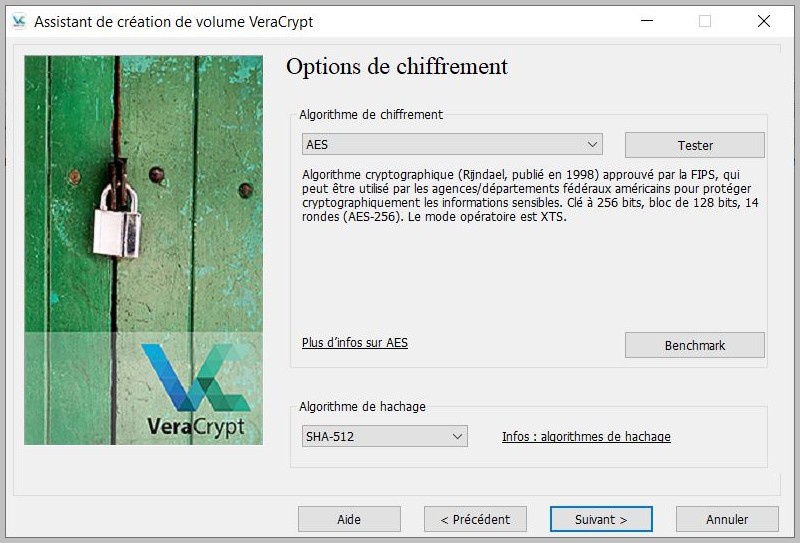
Lancez VeraCrypt, allez dans le menu « **Système** » et sélectionnez l’option ***Chiffrer la partition/le disque système***.

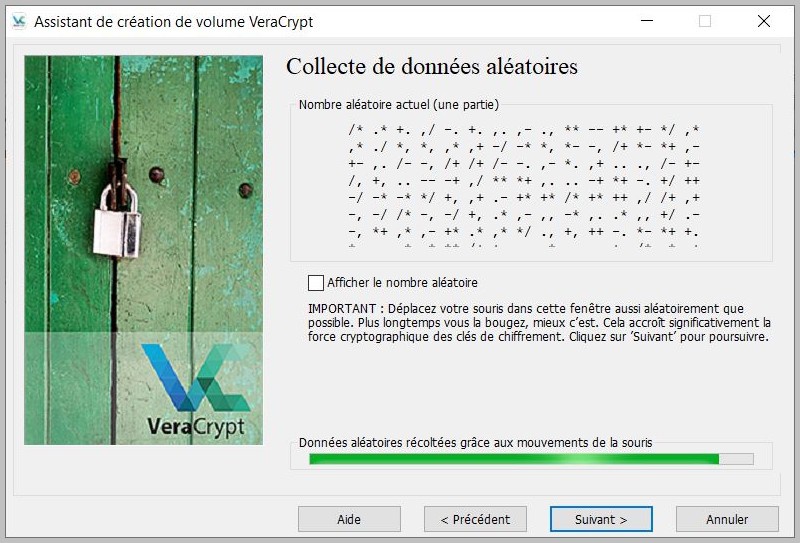


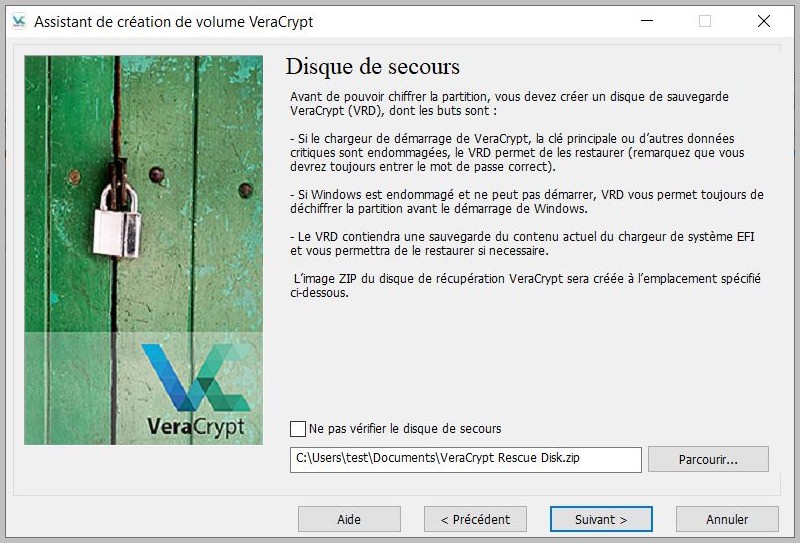
Après avoir validé un contrôle d’accès, vous pouvez choisir le type de chiffrement. Gardez l’option par défaut, à savoir « Normal ».

Pour la zone à chiffrer, vous n’avez pas le choix, c’est la « partition système Windows ».

Ensuite, choisissez « Amorçage » ou « Amorçage multiple », si vous avez respectivement un ou plusieurs systèmes d’exploitation installés sur votre machine.

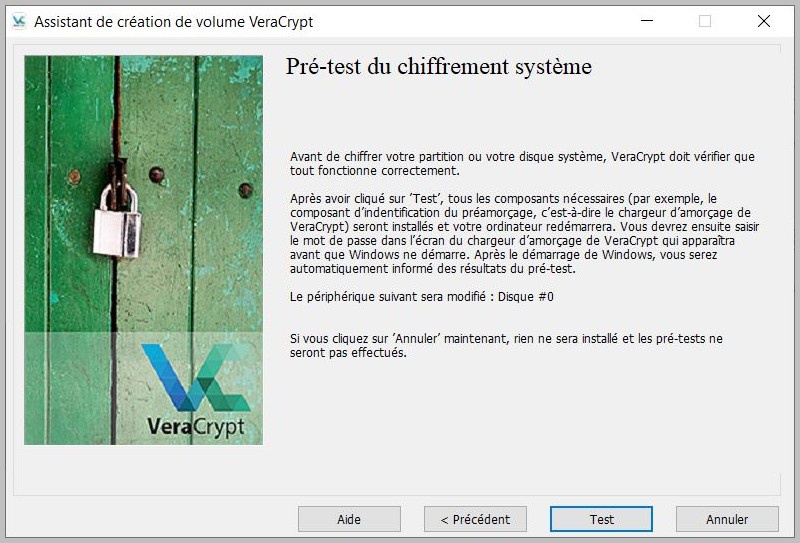
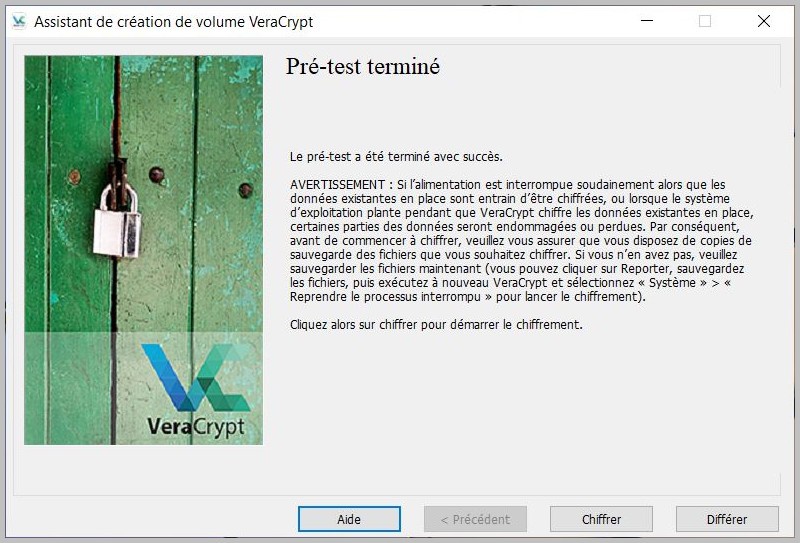
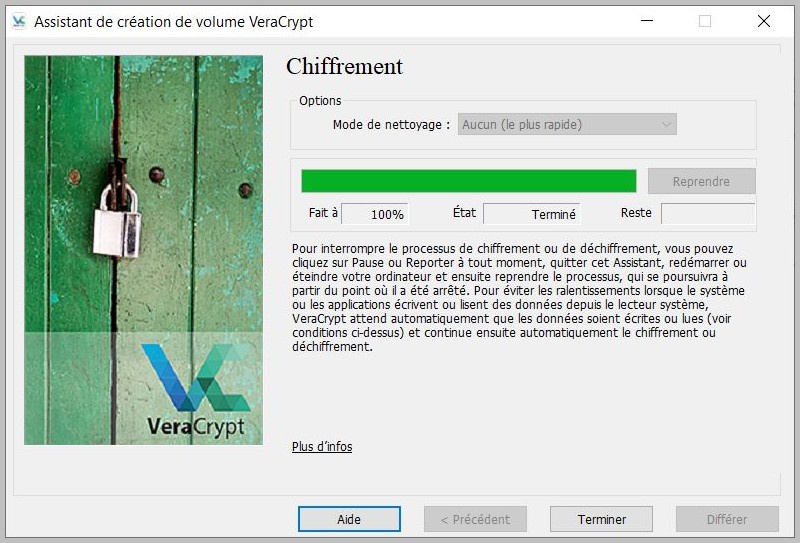
Dans les options de chiffrement, gardez les options par défaut, à savoir AES et SHA-512. C’est largement suffisant.

La collecte de données aléatoires permet de créer une clé de chiffrement avec un bon niveau d’entropie. Faites bouger la souris jusqu’à ce que la barre soit totalement remplie. Le logiciel vous annoncera ensuite que les clés ont été bien générées.

 La dernière étape avant le chiffrement est cruciale. Il s’agit de créer un disque de secours, qui vous permettra d’accéder au système même si le chargeur de démarrage est endommagé, ce qui peut arriver suite à une mise à jour Windows. Pour ce faire, logiciel va créer dans votre répertoire « Documents » un fichier ZIP qu’il faudra extraire à la racine d’une clé USB formatée FAT ou FAT32.

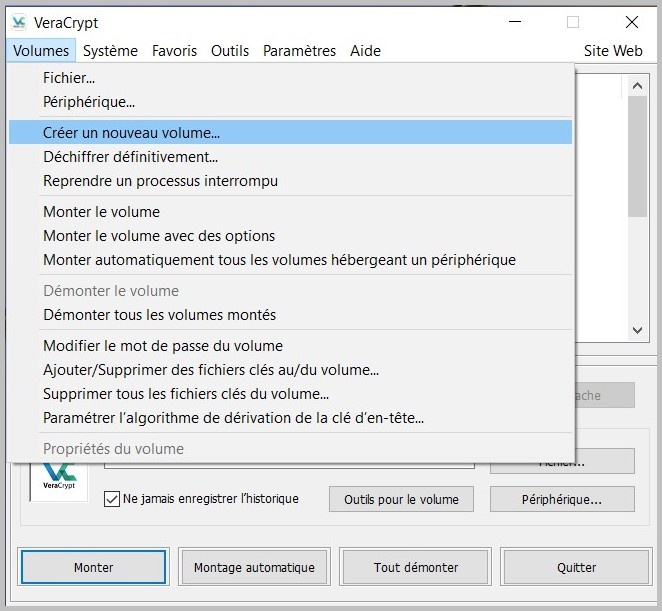
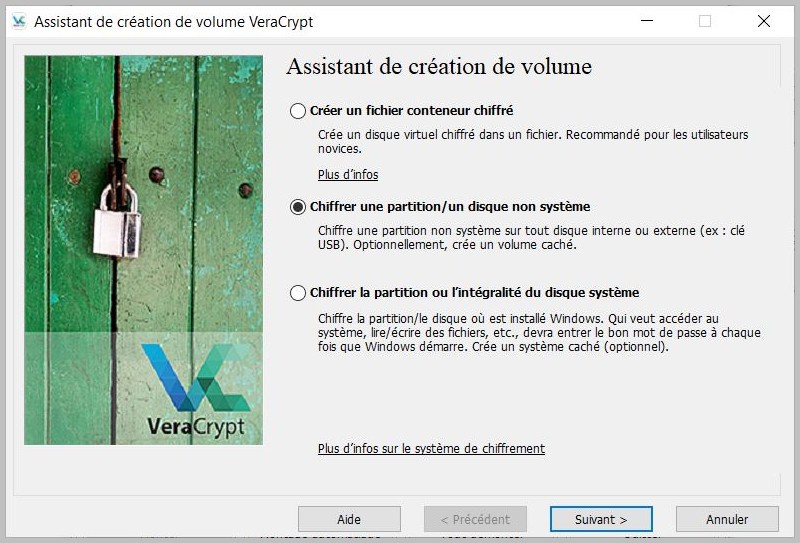


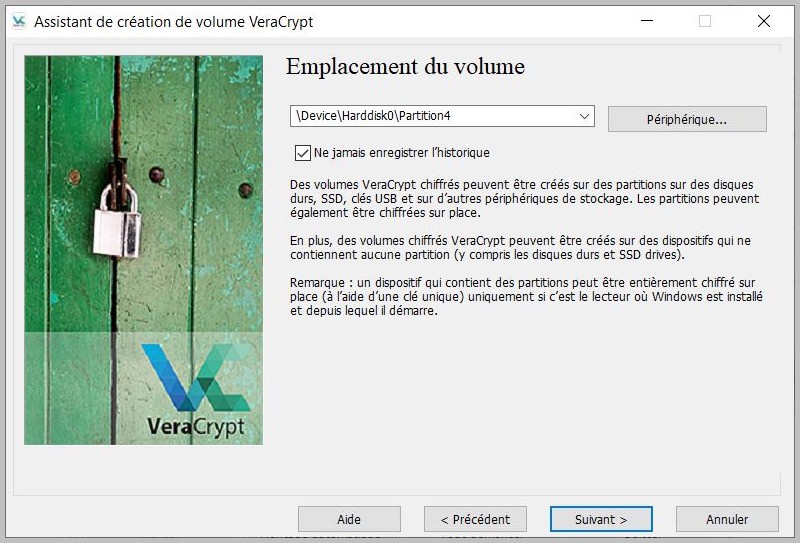
Après avoir choisi le mode « Aucun nettoyage », vous pourrez réaliser un pré-test de chiffrement. Le système va redémarrer et vous demander votre fameux mot de passe. Si le test est réussi, vous pourrez alors passer au véritable chiffrement. Pour notre disque SSD, il nous a fallu une dizaine de minutes. La partition chiffrée figurera ensuite sur l’écran principal de VeraCrypt.

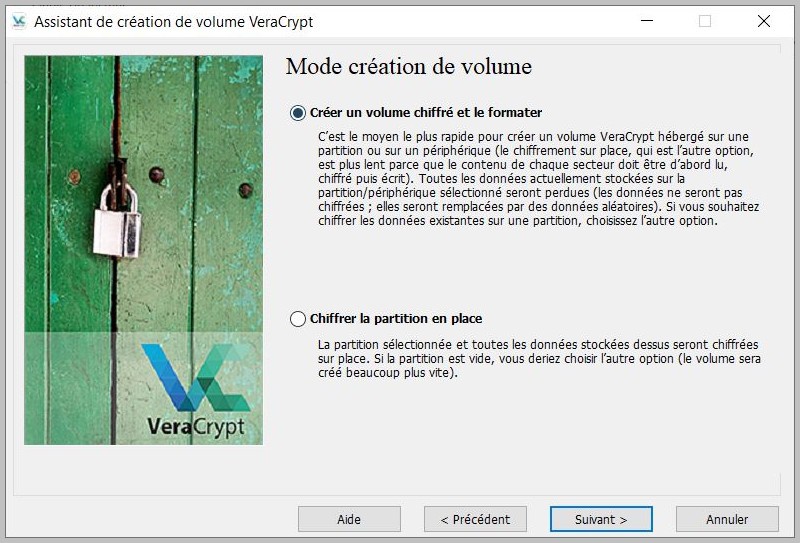


**Chiffrez la partition de données**

Lancez VeraCrypt, allez dans le menu « Volumes » et sélectionnez « Créer un nouveau volume… ». Dans l’assistant de création de volume, choisissez « Chiffrer une partition/un disque non système ». Après avoir validé un contrôle d’accès, vous pouvez choisir le type de volume. Gardez le choix par défaut (« standard »).

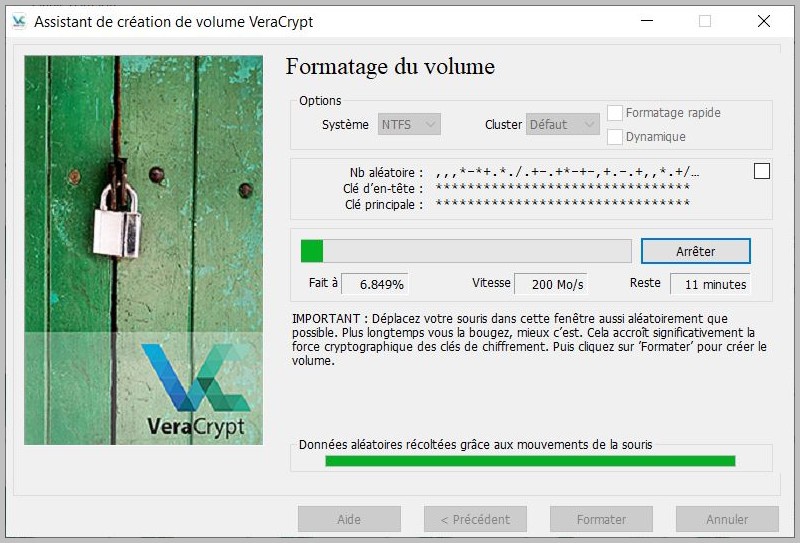


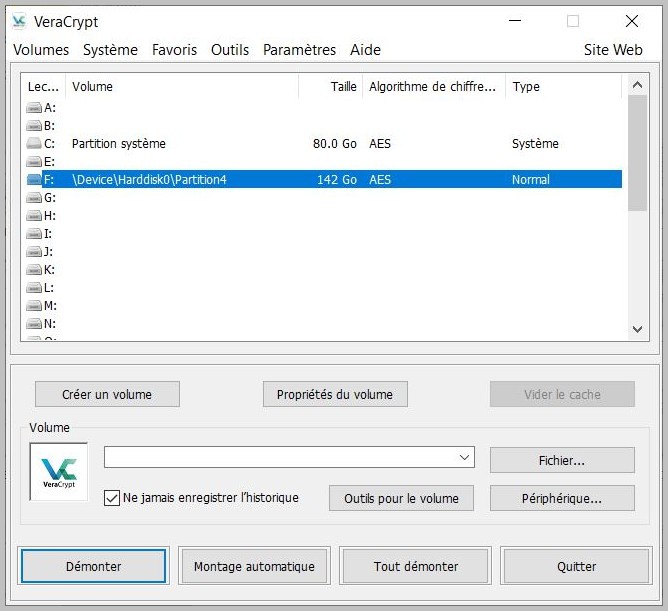
Il faut ensuite définir l’emplacement du volume à chiffrer. Cliquez sur « Périphérique… » et sélectionnez la partition qui stocke vos données. Généralement, c’est la lettre D. Pour le mode de création du volume, sélectionnez « Créer un volume chiffré et le formater » si vous n’avez aucune donnée dans votre partition. Sinon, il faut prendre « Chiffrer la partition en place », ce qui sera plus lent plus lent.

Par la suite, le logiciel vous demande les options de chiffrement. Comme précédemment, gardez les choix par défaut. Après une vérification de la taille du volume, il faudra choisir un bon mot de passe. Par simplicité, vous pouvez reprendre le même que tout à l’heure.



Si vous avez opté pour le formatage, vous devenez maintenant sélectionner un système de fichiers. Dans un premier temps, choisissez « Oui » à la question des « Grands fichiers », car qui peut le plus peut le moins. Le logiciel vous proposera ensuite une sélection de systèmes de fichiers. Comme il s’agit d’un disque interne, le mieux est de prendre NTFS. Puis, comme avant, faites bouger la souris pour récolter des données aléatoires et cliquez sur « Formater ». Le formatage nous a pris une dizaine de minutes.



 Votre nouvelle partition chiffrée est désormais prête à l’emploi. Mais pour l’utiliser, il faudra d’abord la monter. Pour cela, il faut retourner dans l’écran principal de VeraCrypt, sélectionner une lettre de lecteur logique (par exemple F) et cliquer sur « Montage automatique ». Une fenêtre pop-up vous demandera le mot de passe et quelques secondes plus tard, vous pourrez accéder au volume de stockage. Cette manipulation devra être répétée à chaque redémarrage.

II/ Avantages et limites

1. Avantages de veracrypt

Quelques avantages de veraCrypt sont :

* Il est open source
* C’est un logiciel de chiffrement de stokage simple d’utilisation

1. Limites de veracrypt

**Quels sont les problèmes de sécurité de VeraCrypt ?**

* VeraCrypt est vulnérable à diverses attaques connues qui affectent également d'autres logiciels de chiffrement de disque basé sur ce type de logiciel tels que BitLocker.
* Pour atténuer ces attaques, la documentation distribuée avec VeraCrypt incite les utilisateurs à suivre diverses précautions de sécurité.

**III/ Pratique**

**IV/ Conclusion**

**En résumé, nous retenons que la sécurisation de données avec veracrypt est plus simple.**