Protégez vos fichiers avec le chiffrement de disque dur

Chiffrer les données d'un disque dur vous permet de vous assurer de la **confidentialité** de ces données, même dans le cas où un attaquant a un accès physique au disque dur, par exemple dans le cas d'un vol d'ordinateur portable. Pour cela, vous pouvez utiliser **VeraCrypt,** un logiciel open-source et gratuit de **chiffrement de données.** VeraCrypt permet de chiffrer et déchiffrer les données à la volée, c'est-à-dire de manière transparente pour l'utilisateur et le système. Dans ce chapitre, vous utiliserez VeraCrypt pour **chiffrer un fichier, une partition de disque puis l'ensemble d'un disque dur.**

> **Prérequis** : Ce tutoriel est basé sur **Windows 10**. Vous pouvez le réaliser sur Linux et macOS, mais certaines commandes peuvent différer selon le système. Je vous conseille d'utiliser une machine virtuelle avec VirtualBox ou VMware pour réaliser ce tutoriel, afin de pouvoir facilement revenir en arrière. Utilisez Windows avec un disque dur de 40 Go environ dans la machine virtuelle. Vous devez également avoir au moins 50 Go d'espace disque disponible sur l'ordinateur hébergeant la machine virtuelle, car le chiffrement du disque oblige à utiliser la totalité de l'espace disque de la machine virtuelle.

Installez VeraCrypt

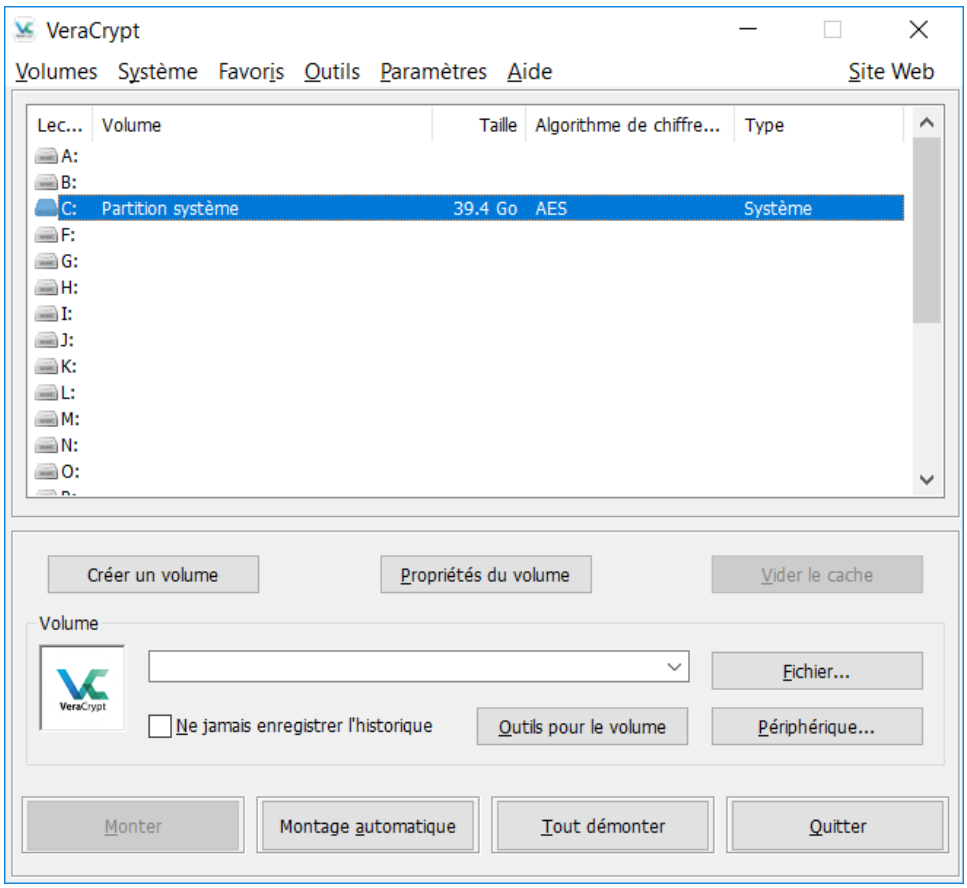
1. Allez sur le site officiel de VeraCrypt et téléchargez la dernière version de Veracrypt pour Windows (pour ce chapitre, la version est 1.23-Hotfix-2).
2. Effectuez l'installation en gardant les options par défaut et choisissez *Français* pour la langue d'installation.
3. À la fin de l'installation, VeraCrypt vous propose de lire la **documentation** (en anglais). Cette documentation est très complète et vous pourrez l'utiliser par la suite pour aller plus loin dans l'utilisation de VeraCrypt.

Chiffrez un fichier conteneur

C'est la méthode la plus simple pour créer un volume chiffré sur le disque dur. Vous allez créer un fichier avec VeraCrypt, que vous monterez ensuite comme une partition dans le système d'exploitation.

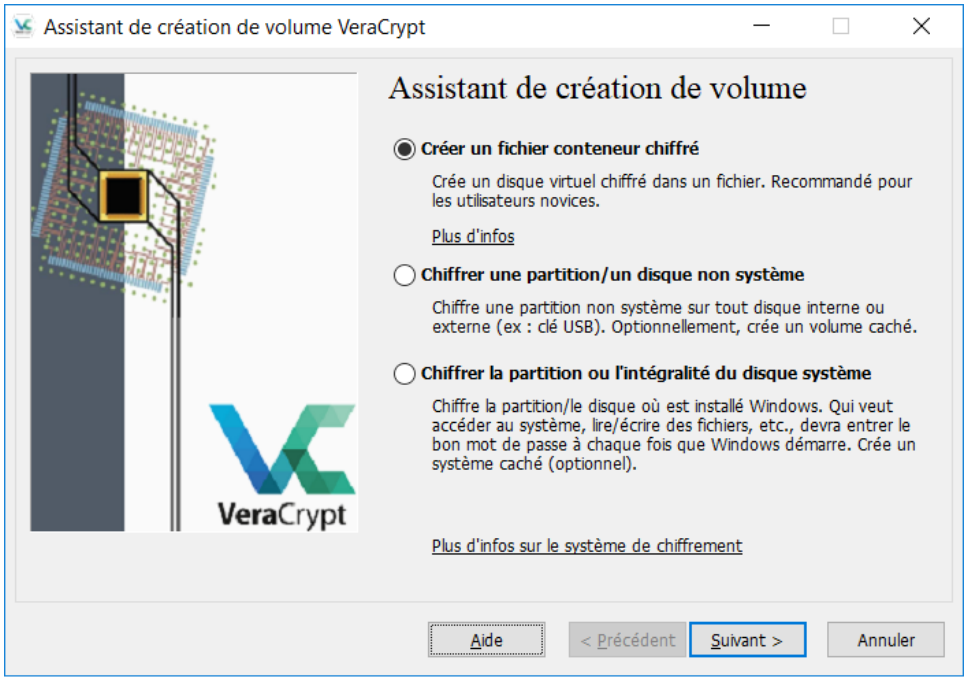
Créez un fichier conteneur

Ouvrez l'application VeraCrypt et cliquez sur `Créer un volume` .



Créer un volume

Sélectionnez `Créer un fichier conteneur` et cliquez sur `Suivant`. Choisissez l'emplacement du fichier conteneur et donnez-lui un nom. Cliquez sur `Suivant`.

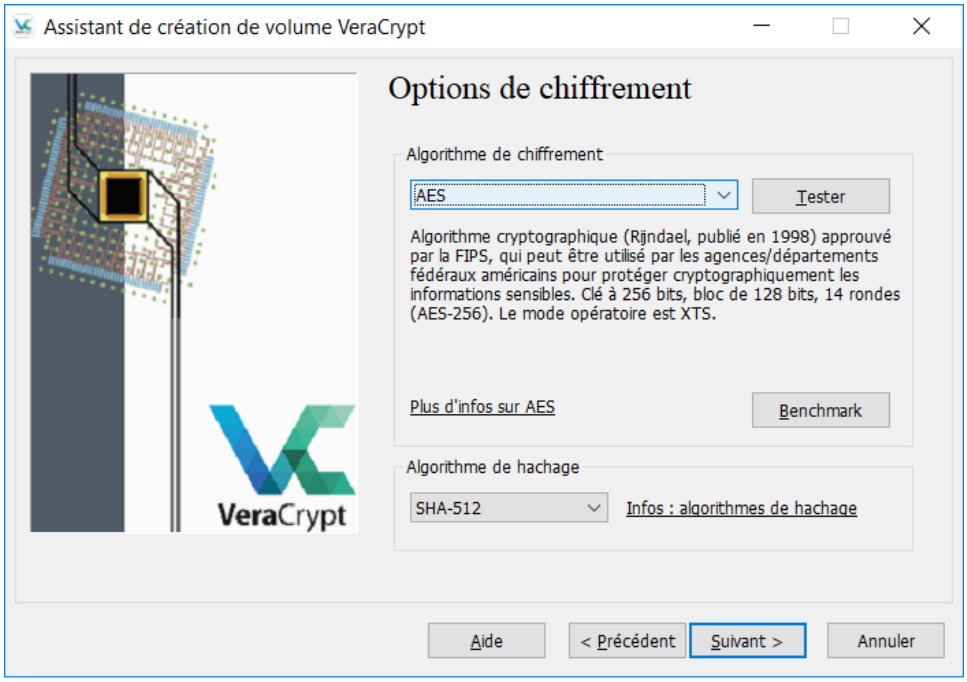


Création de volume

Vous arrivez sur la fenêtre des **options de chiffrement**. Vous pouvez choisir l'algorithme de chiffrement. Pour chaque algorithme, une description est donnée en dessous. Naviguez dans la

liste pour voir les différentes caractéristiques des algorithmes de chiffrement.

Il est également possible de **mixer plusieurs algorithmes de chiffrement**. Ainsi, si un algorithme est vulnérable, l'autre algorithme conservera la confidentialité du chiffrement. Cependant, ces options ne sont possibles qu'entre certains algorithmes. Par ailleurs, chaque algorithme de chiffrement doit avoir sa propre clé secrète, pour éviter que la vulnérabilité d'un algorithme ne permette de retrouver toutes les clés de chiffrement.



Options de chiffrement

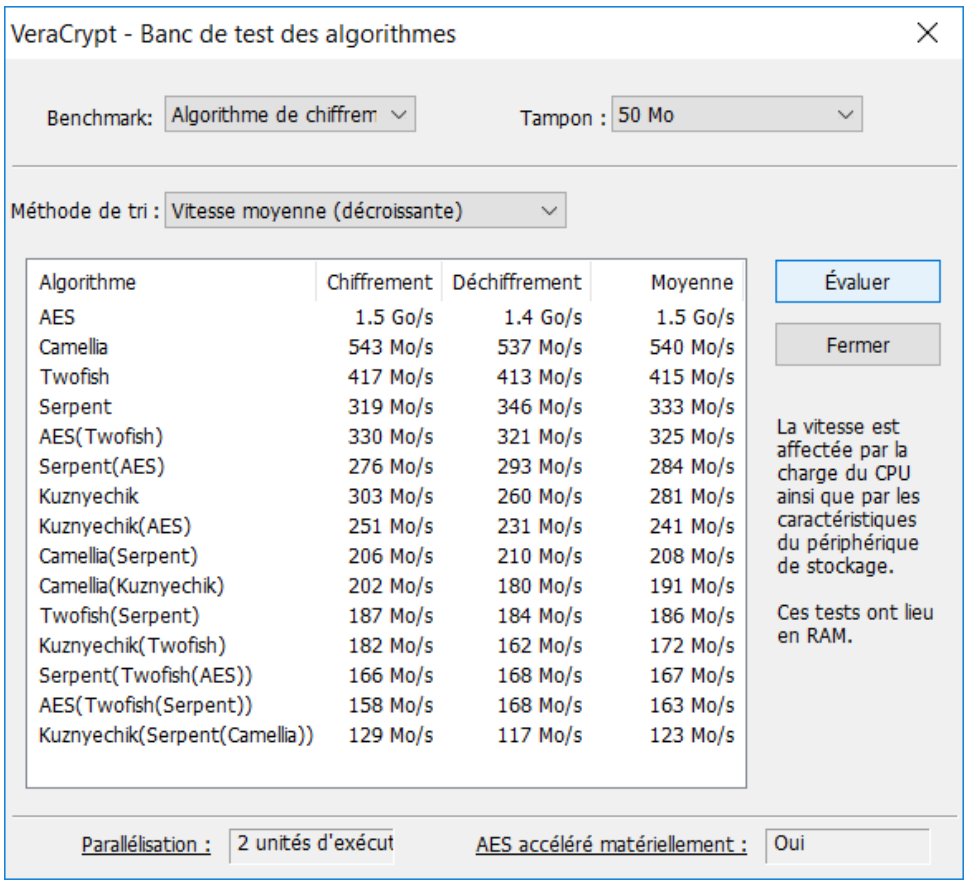
Vous pouvez cliquer sur `Benchmark` puis sur `Évaluer` pour voir la vitesse de chaque algorithme de chiffrement. Par défaut, le test prend quelques secondes.

Le chiffrement AES est bien plus rapide que les autres algorithmes de chiffrement. En effet, comme c'est un standard, les processeurs possèdent des instructions matérielles dédiées pour accélérer AES. Cliquez sur `Fermer` pour revenir à la fenêtre de choix de l'algorithme de chiffrement.

Choisissez l'algorithme AES dans la liste. VeraCrypt indique que c'est la version AES-256 qui est utilisée, c'est-à-dire avec une **clé de 256 bits,** des **blocs de 128 bits** et **14 tours**. Par ailleurs, le mode de chiffrement est **XTS**, qui est une variante du mode CBC.

L'algorithme de hachage est utilisé comme générateur de nombres pseudo-aléatoires déterministes pour générer les clés de chiffrement, ainsi que comme fonction de hachage de mot de passe. **SHA2** (SHA256 et SHA512) est le **standard actuel des fonctions de hachage** que

vous étudierez dans le prochain chapitre. Conservez l'algorithme de hachage par défaut et cliquez sur `Suivant` .



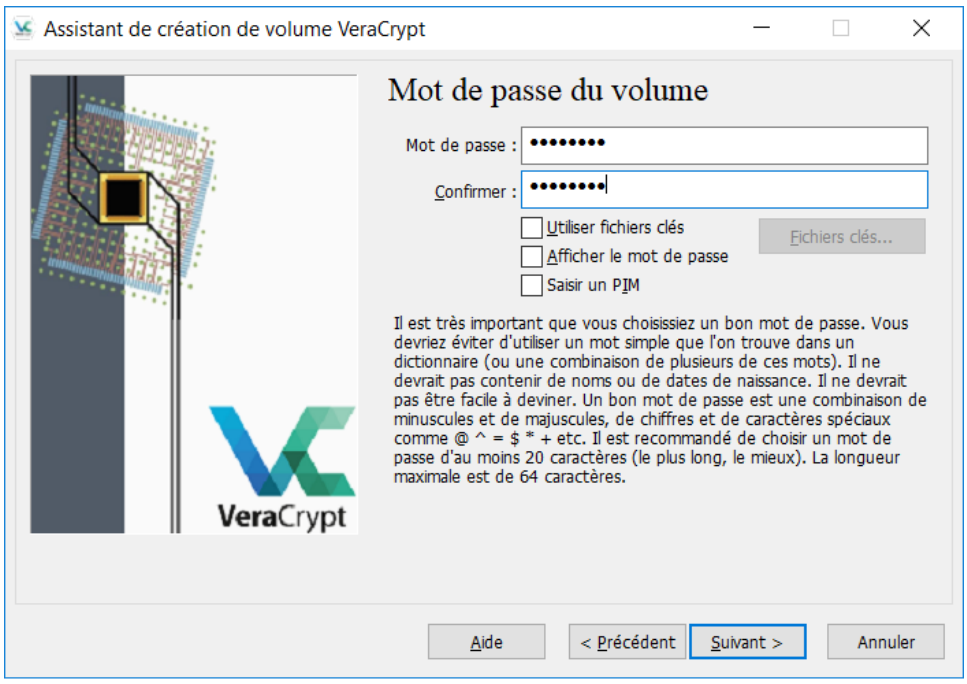
Tester l'algorithme

Choisissez une taille de volume, par exemple 50 Mo. C'est la taille maximale des fichiers que ce conteneur pourra contenir, il faut donc prévoir un peu plus large que nécessaire. Cliquez sur `Suivant` .

Choisissez le mot de passe du volume. Il est crucial de choisir un mot de passe **suffisamment long** pour éviter les attaques par force brute, mais aussi **suffisamment original** pour éviter les attaques par dictionnaire, c'est-à-dire que le mot de passe ne doit pas être uniquement composé de mots et de chiffres prédictibles. Voici un exemple de mot de passe à la fois difficile à deviner mais assez facile à retenir : 1l0v30p3nC!@55r0*m5

Attention, si vous oubliez votre mot de passe, il n'y aura pas de moyen de secours pour le récupérer !

Il est également possible d'utiliser un **fichier clé** en plus ou à la place du mot de passe. Cela est particulièrement utile en entreprise lorsque les utilisateurs possèdent une clé matérielle appelée ***token de sécurité***, qui est en général une clé USB ou une carte à puce Bluetooth.



Choix d'un mot de passe

La fenêtre suivante va vous permettre de choisir le système de fichiers utilisé. VeraCrypt va monter le conteneur chiffré comme un volume de données dans le système d'exploitation avec ce système de fichiers. Vous pouvez laisser **FAT**. Si vous devez stocker des fichiers de plus de 4 Go, choisissez **NTFS**, mais le conteneur ne pourra être lu que par un système Windows.

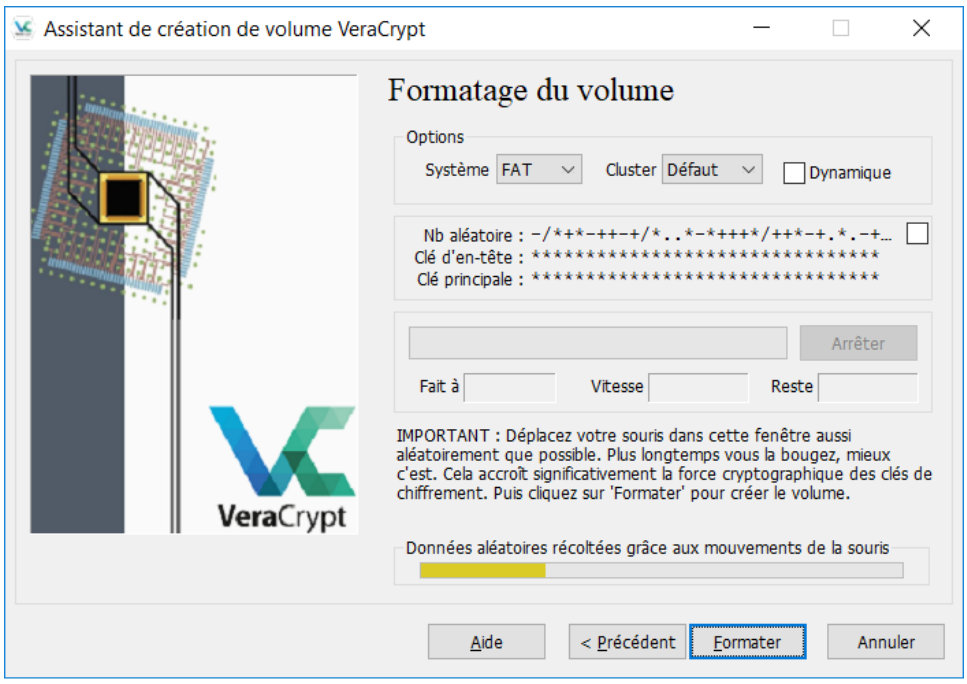
En dessous, vous pouvez voir une entrée appelée ***Nombre aléatoire*** qui défile. Il s'agit d'un générateur de nombres pseudo-aléatoires cryptographiques. Il utilise l'entropie fournie par Windows, mais aussi l'entropie provenant des mouvements de la souris.

Plus vous bougez la souris, plus l'entropie est grande et plus il est rapide de générer un nombre aléatoire.

Lorsque l'entropie est suffisante, le curseur de données aléatoires passe au vert et vous pouvez cliquer sur *Formater*.

Ce générateur va créer une clé de chiffrement aléatoire appelée ***Master Key***, qui sera la clé de chiffrement AES des fichiers stockés dans le volume chiffré que nous venons de créer. Cette clé est elle-même stockée sur le disque dur de manière chiffrée, avec comme clé de chiffrement le mot de passe que vous avez choisi.

Ainsi, si vous voulez changer de mot de passe, VeraCrypt n'aura pas besoin de chiffrer de nouveau toutes les données avec le nouveau mot de passe, mais seulement le fichier contenant la Master Key et chiffré avec votre mot de passe.



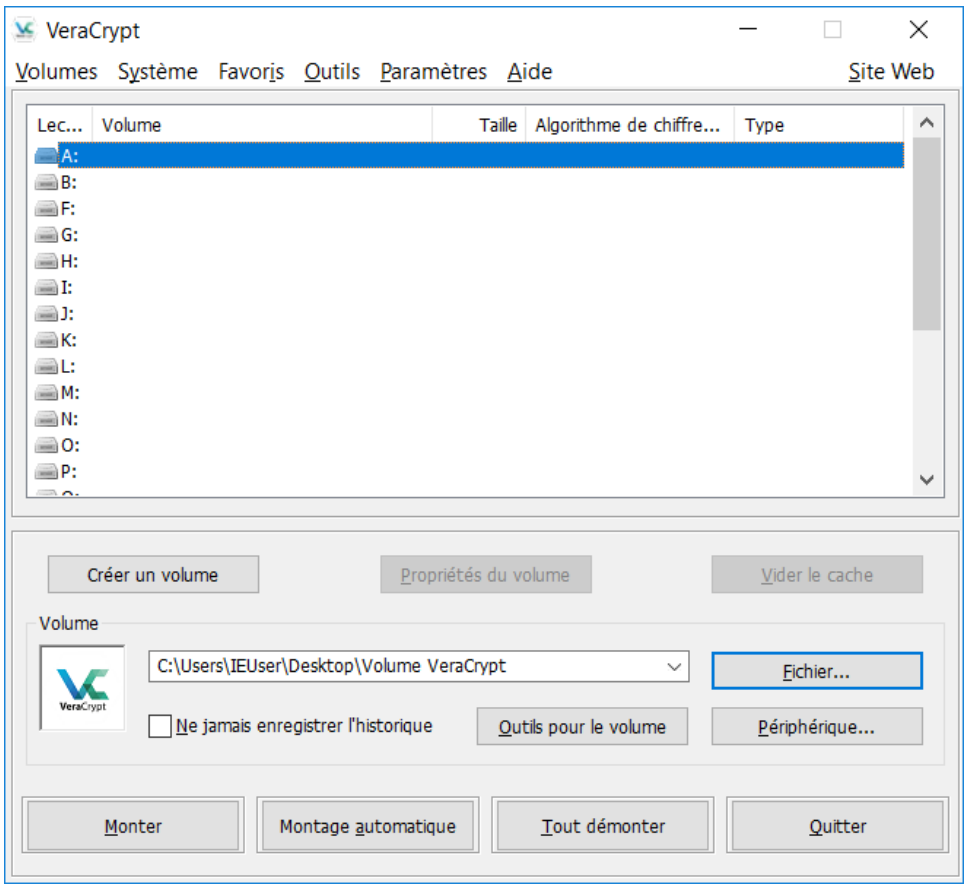
Formatage du volume

Lorsque la création du fichier conteneur est terminée, vous pouvez cliquer sur `Quitter` pour revenir à la fenêtre principale de VeraCrypt.

Montez votre conteneur chiffré dans le système d'exploitation

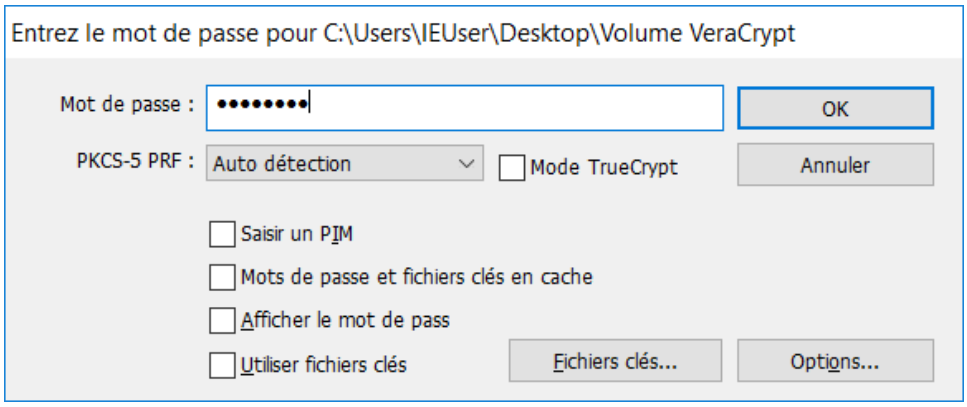
Une fois que le conteneur chiffré est créé, vous allez le monter dans le système d'exploitation. Sélectionnez la lettre à laquelle vous voulez associer le volume chiffré, par exemple `A:`

Cliquez sur *Fichier* et sélectionnez le fichier Veracrypt que vous venez de créer, puis cliquez sur `Monter` .



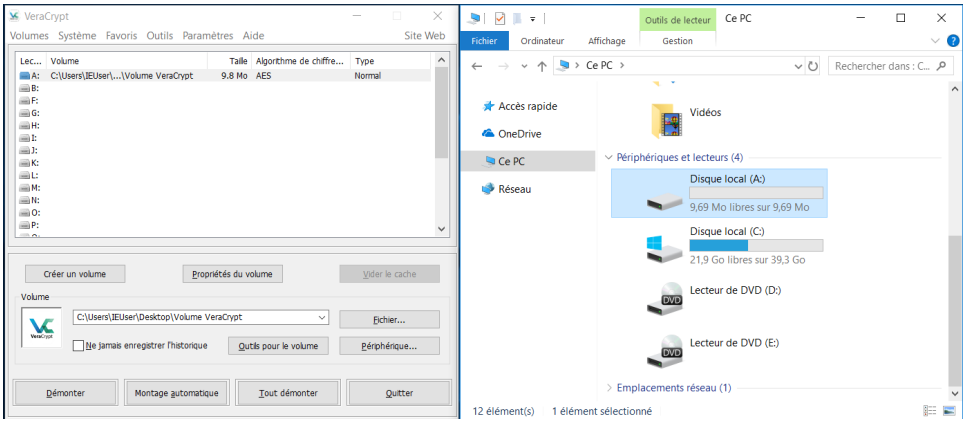
Montage du volume

Entrez le mot de passe et cliquez sur OK



Mot de passe

Le volume chiffré apparaît maintenant comme une partition dans l'explorateur. Vous pouvez y créer, modifier et supprimer des fichiers comme sur une partition normale. Les données enregistrées dans ce conteneur seront stockées sur le disque dur de manière chiffrée.



Vision de l'explorateur

Lorsque vous n'avez plus besoin d'utiliser le volume chiffré, vous pouvez le démonter en sélectionnant le volume dans la liste sur la fenêtre de VeraCrypt, puis en cliquant sur `Démonter`, en bas.

> Lorsque vous éteignez l'ordinateur, VeraCrypt démonte automatiquement le volume, il n'est donc pas nécessaire de le faire manuellement.

VeraCrypt contient de nombreuses autres options comme le montage automatique, le changement de mot de passe ou le montage de partition en ligne de commande. N'hésitez pas à vous référer à sa documentation si vous avez des besoins complémentaires.

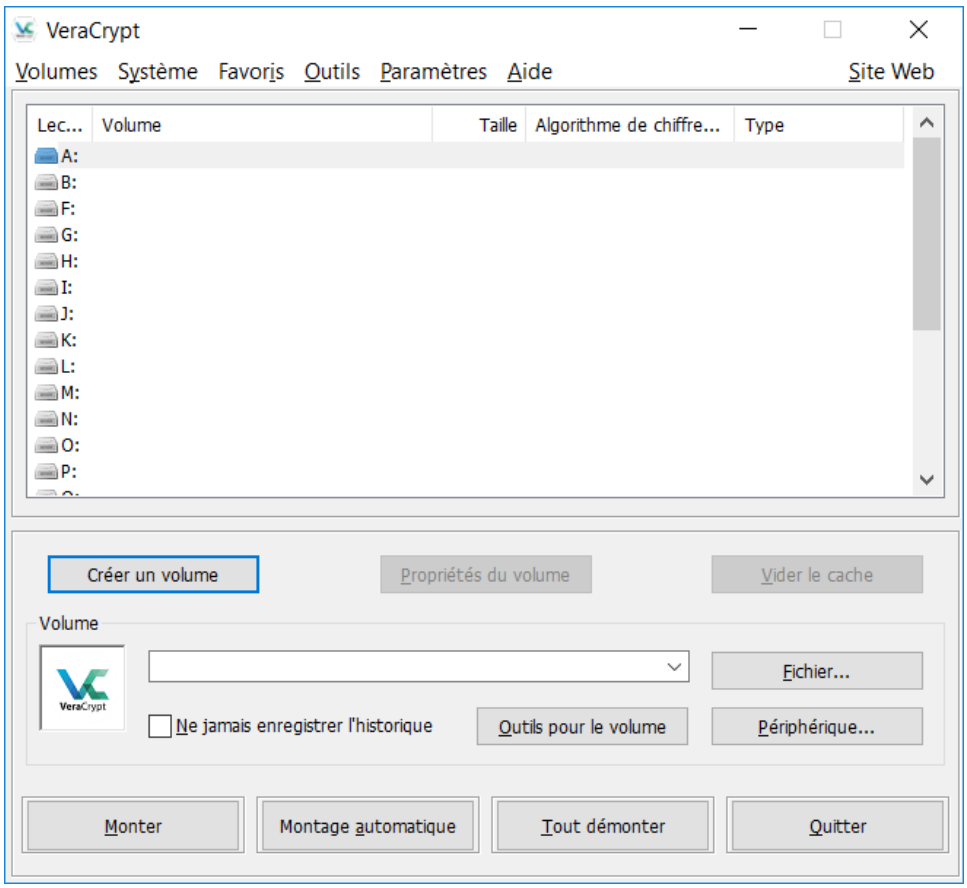
Créez une partition chiffrée

Une partition chiffrée est similaire à un fichier conteneur chiffré, mais en utilisant une partition de disque dur à la place d'un fichier conteneur. Cette solution est très pratique par exemple pour **chiffrer l'ensemble des données d'une clé USB ou d'un disque externe**. Dans cet exemple, vous allez chiffrer la partition d'une clé USB.

> Tout d'abord, assurez-vous que votre clé USB ne contienne aucune donnée, car elles seront supprimées durant la création de la partition chiffrée !

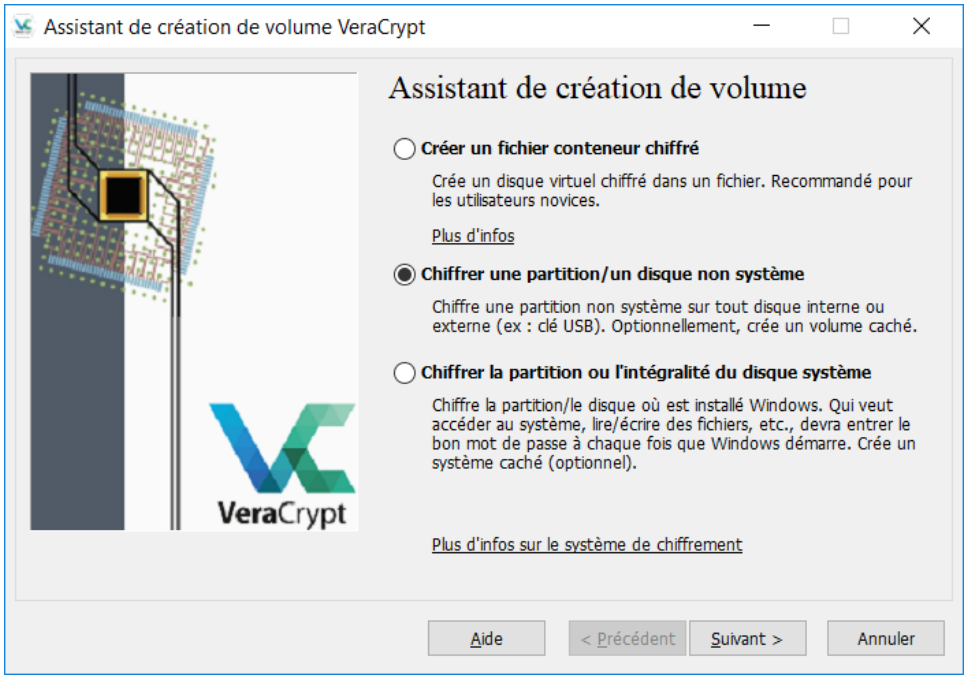
Branchez la clé USB sur votre ordinateur et assurez-vous qu'elle soit visible par la machine virtuelle sur laquelle vous travaillez.

Dans la fenêtre principale de VeraCrypt, cliquez de nouveau sur `Créer un volume`.



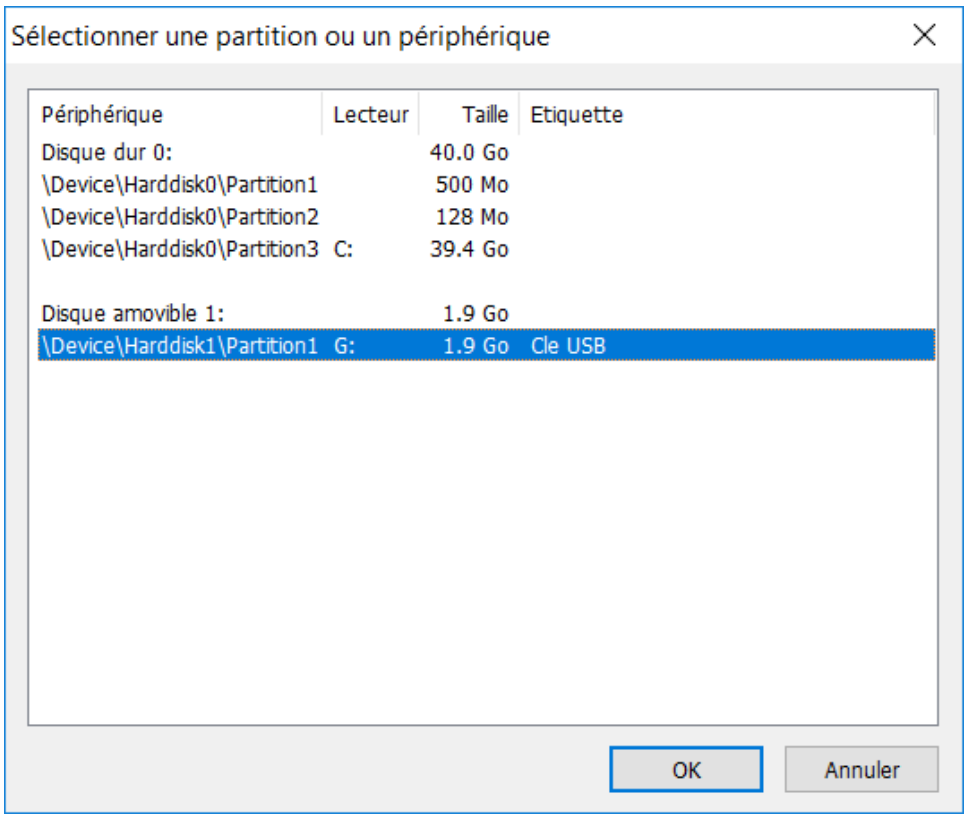
Créer un volume

Sélectionnez `Chiffrer une partition / un disque non système`, cliquez sur `Suivant` puis laissez l'option *Volume VeraCrypt standard* et cliquez sur `Suivant`



Création de volume

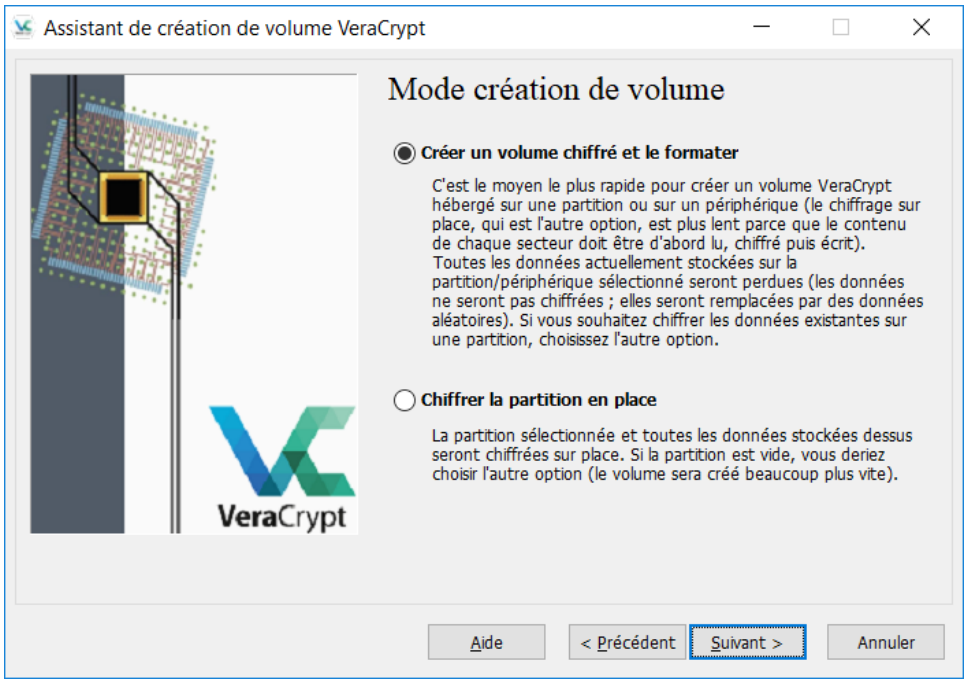
Cliquez sur `Périphérique` pour choisir l'emplacement du volume.



Partition

Sélectionnez la partition correspondant à votre clé USB. Pour moi, il s'agit de la partition située sur `G:` ; puis cliquez sur `OK` . Si vous ne trouvez pas la partition, assurez-vous que la clé USB soit bien visible par votre machine virtuelle.

Vous avez le choix entre créer un volume chiffré à la place de la partition actuelle, ce qui supprime toutes les données de la partition, **ou chiffrer la partition en place,** ce qui conserve et chiffre toutes les données de la partition actuelle, mais qui est plus long. Assurez-vous de sauvegarder toutes les données de votre clé USB, conservez *Créer un volume chiffré* et cliquez sur `Suivant`



Formater le volume

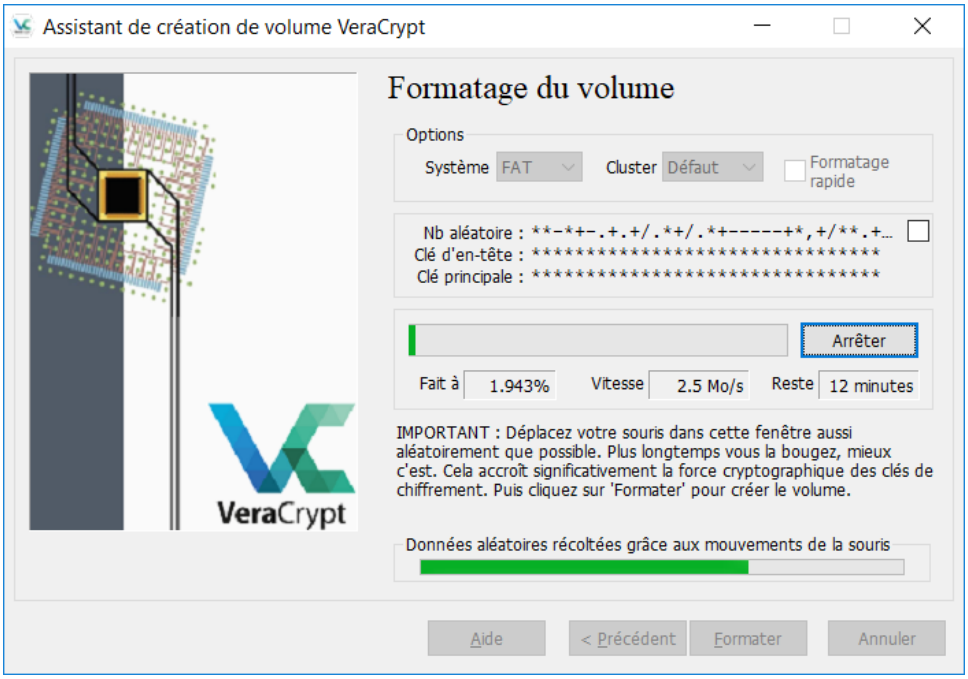
La taille du volume est fixée automatiquement à la taille de la clé USB, cliquez sur `Suivant` .

Le formatage du volume est similaire. Si vous n'avez jamais stocké de données confidentielles sur la clé USB, vous pouvez activer l'option ***Formatage rapide***. Dans ce cas, seuls les nouveaux fichiers qui seront écrits sur le volume chiffré seront chiffrés, c'est-à-dire que les anciennes données qui ont été écrites sur la clé USB et qui sont toujours présentes physiquement (même si les fichiers ont été supprimés) ne seront pas chiffrées. Cette option permet de formater le volume beaucoup plus rapidement.

Si vous avez stocké des données confidentielles sur la clé USB dans le passé, même si ces données sont supprimées, il ne faut pas activer cette option.

Générez suffisamment d'entropie avec la souris, puis cliquez sur `Formater` .

Lorsque le formatage est terminé, vous pouvez cliquer sur `Quitter`



Pour monter la partition chiffrée, il faut cliquer sur `Périphérique` dans la fenêtre principale de VeraCrypt et sélectionner la partition de la clé USB. Cliquez ensuite sur `OK` puis choisissez une lettre de disque dans la liste, et cliquez sur `Monter` . À partir de là, les opérations sont les mêmes qu'avec un fichier conteneur.

Les données que vous stockerez sur cette clé USB seront chiffrées et accessibles uniquement avec votre mot de passe. Vous pouvez utiliser cette clé USB sur n'importe quel ordinateur qui possède VeraCrypt.

Pour supprimer la partition chiffrée de la clé USB, il suffit de formater la clé avec un outil de gestion de partition normal.

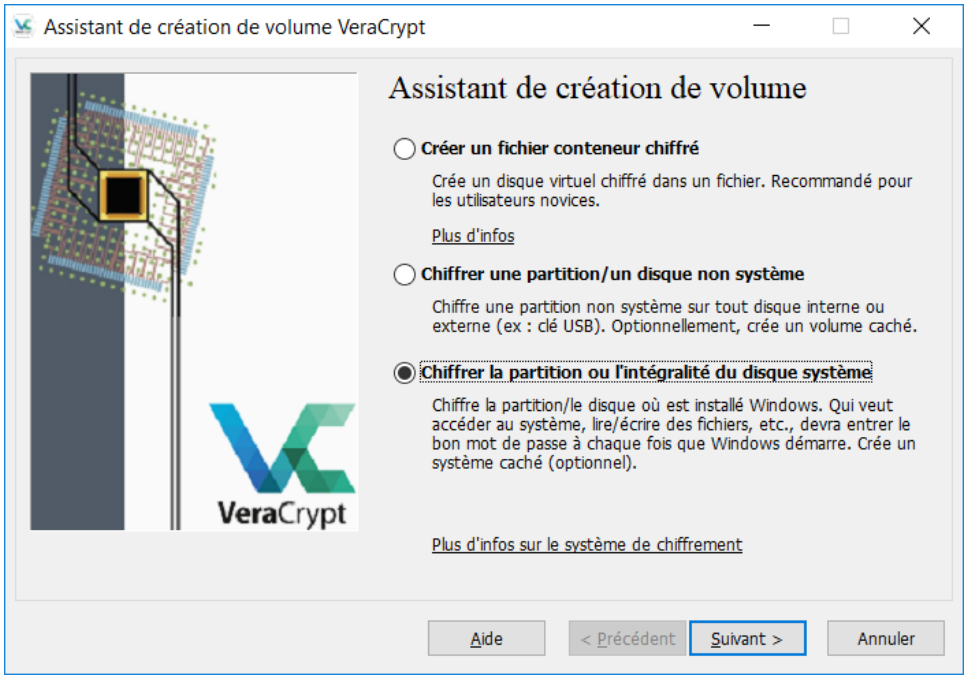
Créez une partition système chiffrée

Maintenant que vous êtes familier avec le chiffrement de disque dur, vous allez chiffrer la partition système de votre machine virtuelle. VeraCrypt ne propose pour le moment cette option qu'avec Windows.

Un des avantages du chiffrement de la partition système est que Windows et les programmes stockent fréquemment des fichiers sur le disque dur, notamment des fichiers temporaires. Lorsque vous ouvrez un fichier qui se trouve dans une partition chiffrée, il est possible qu'une copie de ce fichier soit écrite sur le disque dur dans la partition système. Si cette partition n'est pas chiffrée, un attaquant pourrait donc lire ce fichier.

> Il est très fortement conseillé de faire cette opération sur une **machine virtuelle** et de **sauvegarder ses données au préalable** par sécurité. En effet, la partition système du disque dur est particulière, car elle contient les instructions pour démarrer le système d'exploitation au démarrage de l'ordinateur. Or, ces instructions seront chiffrées par VeraCrypt. VeraCrypt doit donc modifier le secteur de démarrage de la partition système pour vous demander le mot de passe au démarrage de l'ordinateur, et déchiffrer les instructions pour démarrer le système d'exploitation.

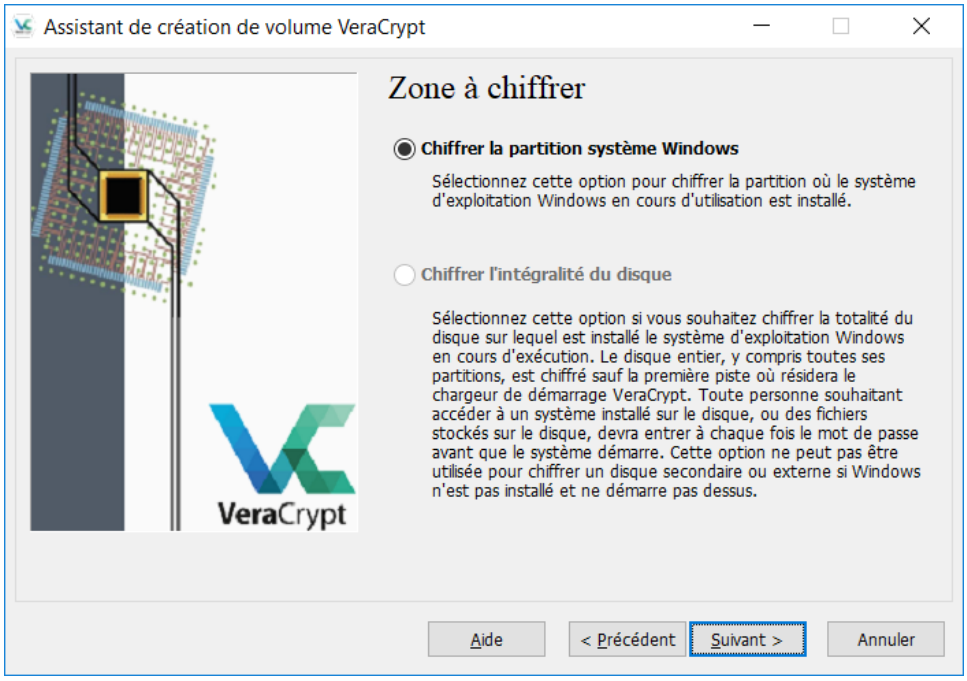
Sélectionnez `Chiffrer la partition système` puis cliquez sur `Suivant` . Laissez le type de chiffrement sur ***Normal*** et cliquez sur `Suivant` .



Chiffrer une partition système

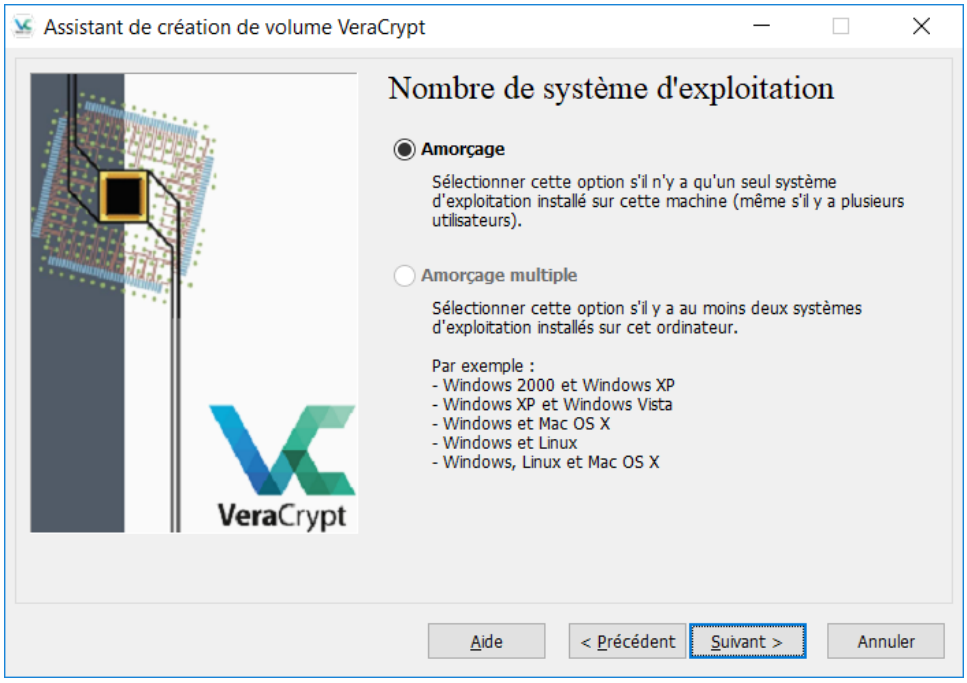
Laissez ***Chiffrer la partition système Windows*** et cliquez sur `Suivant` . Il est également possible de chiffrer l'intégralité du disque dur, mais uniquement si celui-ci est basé sur MBR (Master Boot Record) et non sur GPT (GUID Partition Table), qui est le système utilisé actuellement par la plupart des ordinateurs.

Cliquez sur `Suivant` .



Zone à chiffrer

Laissez l'option ***Amorçage*** puisque vous n'avez qu'un système d'exploitation, et cliquez sur `Suivant` . Les options de chiffrement, mot de passe et données aléatoires sont similaires ; vous pouvez donc les laisser par défaut et cliquer sur `Suivant` . VeraCrypt affiche les clés générées, cliquez sur `Suivant` .

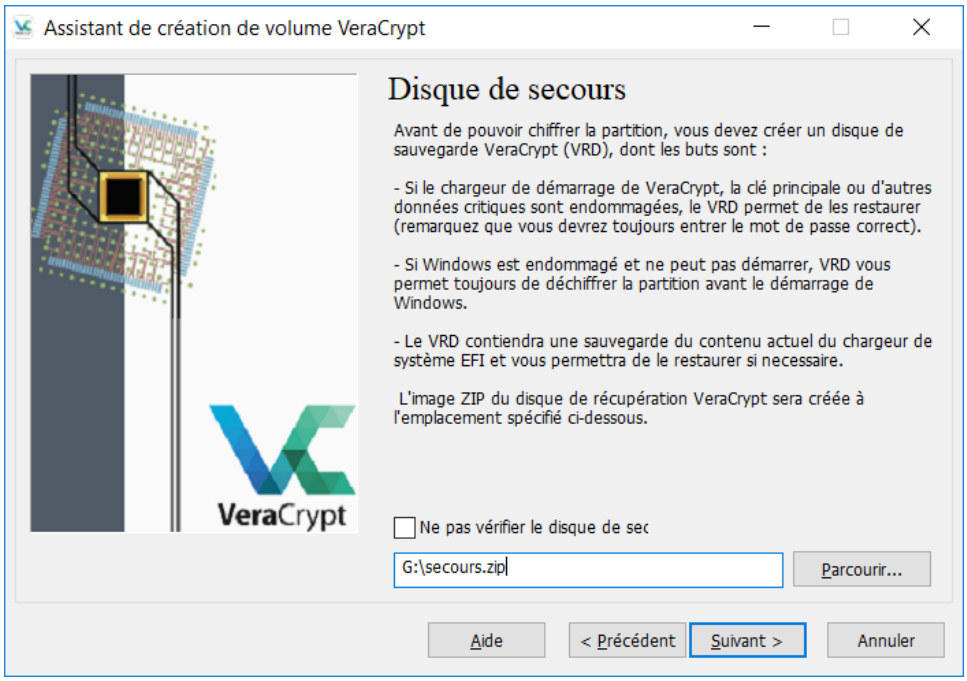


Option Amorçage

VeraCrypt vous propose de créer un **disque de secours**, dans le cas où un problème surviendrait, pour revenir en arrière. Il est fortement conseillé de stocker ce dossier en dehors du disque que l'on veut chiffrer. Vous pouvez le stocker sur la partition chiffrée de la clé USB utilisée précédemment (dans ce cas, il vous faudra la formater en FAT, et donc perdre la partition chiffrée créée précédemment).

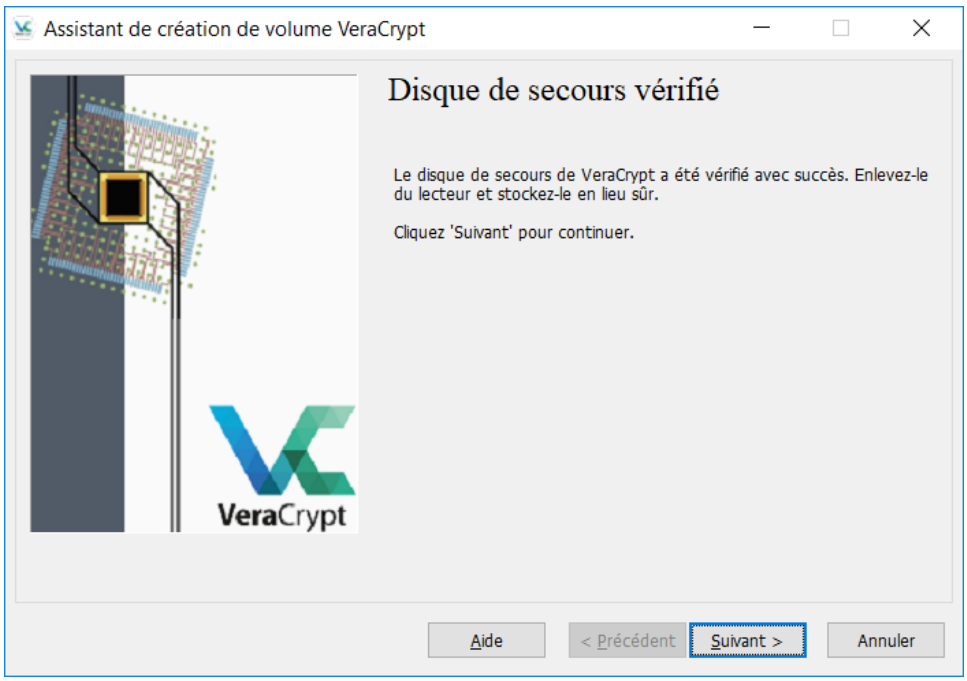
Pour créer le disque de secours, vous allez d'abord enregistrer le fichier en le nommant `secours.zip` par exemple, dans votre clé USB, puis il vous restera à ouvrir ce fichier et à extraire le dossier EFI à la racine de la clé USB.

Si vous ne souhaitez pas créer de disque de secours, il faut activer ***Ne pas vérifier le disque de secours***, sinon vous ne pourrez pas continuer la procédure.



Disque de secours

Cliquez ensuite sur `Suivant` pour vérifier le disque de secours.



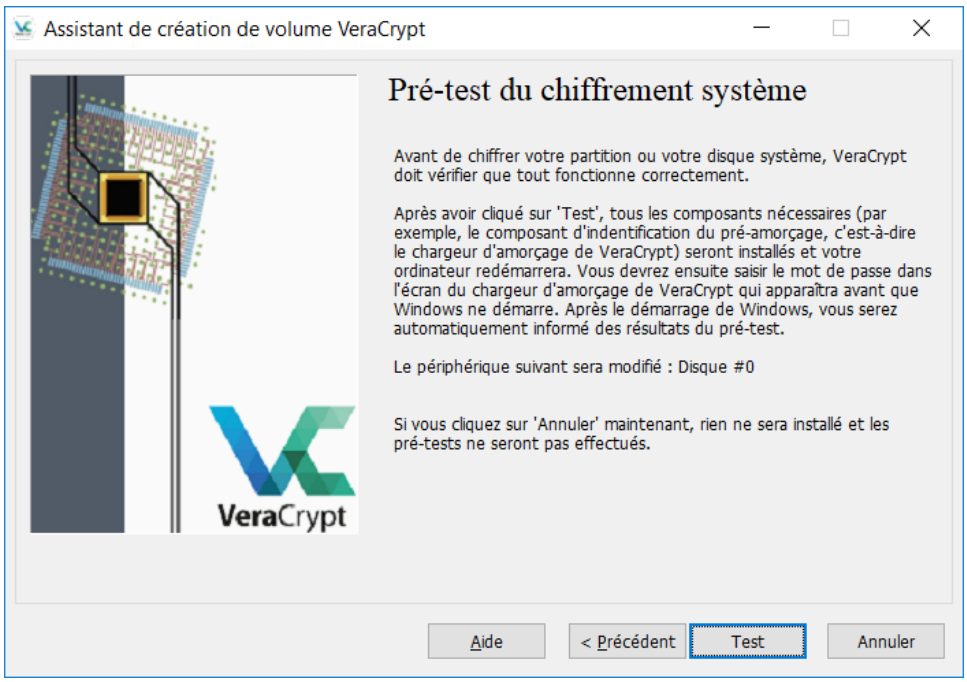
Disque vérifié

Si le disque de secours a bien été vérifié, vous pouvez cliquer sur `Suivant` . Sinon, vous ne pourrez pas continuer la procédure et il faudra la recommencer en vous assurant d'utiliser une clé USB formatée en FAT, et de bien extraire le dossier EFI à la racine de la clé USB.

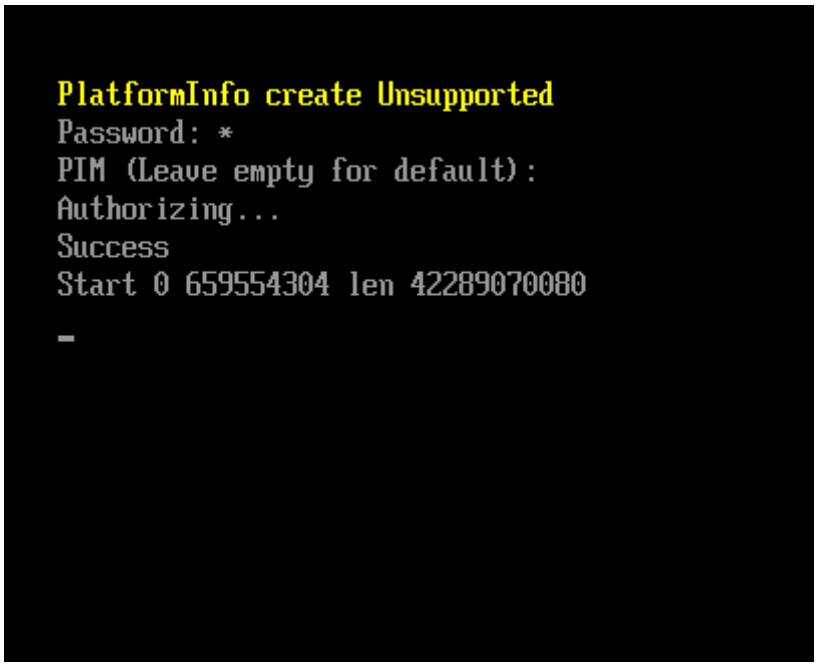
VeraCrypt vous demande ensuite quel **Mode de nettoyage** utiliser. Si le disque a contenu des informations confidentielles non chiffrées par le passé, il faudra sélectionner 3 passages, mais cela multipliera par 3 la durée du chiffrement. Pour ce test, vous pouvez laisser ***Aucun*** et cliquer sur `Suivant` .

Mode de nettoyage

VeraCrypt va alors redémarrer l'ordinateur pour tester si le démarrage avec mot de passe fonctionne bien. Cliquez sur `Test` puis validez *Redémarrer* pour redémarrer.



Prétest



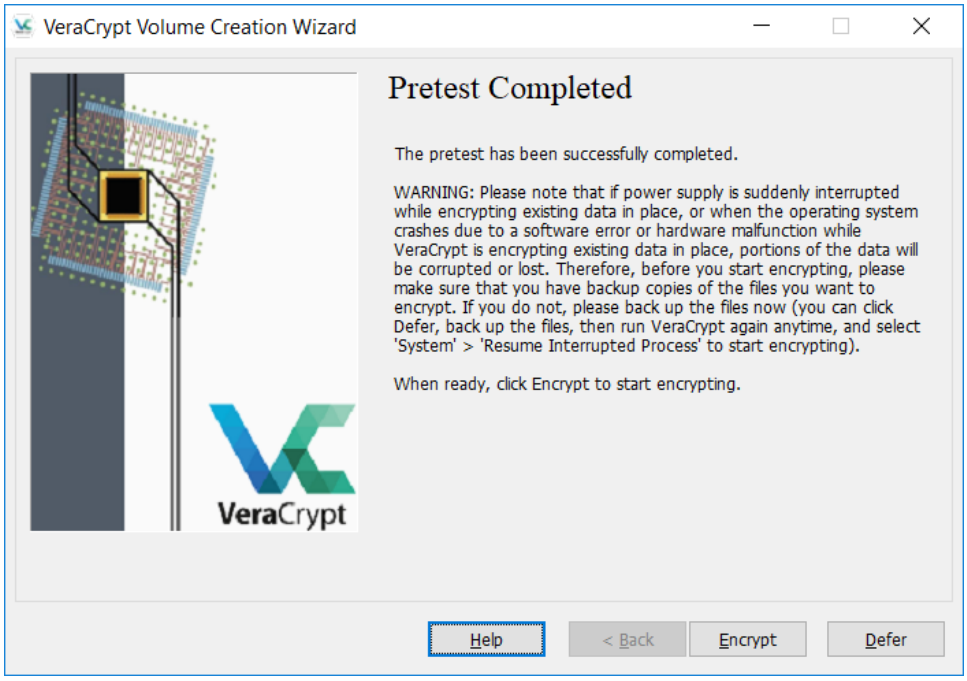
Mot de passe

Au démarrage, VeraCrypt vous demande votre mot de passe de chiffrement. Entrez-le et appuyez deux fois sur `Entrée` . Si le mot de passe est correct, l'ordinateur va démarrer normalement.

Il est possible que votre clavier passe en QWERTY au démarrage, ou que le clavier numérique soit désactivé à cette étape. Dans ce cas, le mot de passe pourrait éventuellement échouer. Pour éviter ces problèmes, VeraCrypt transforme

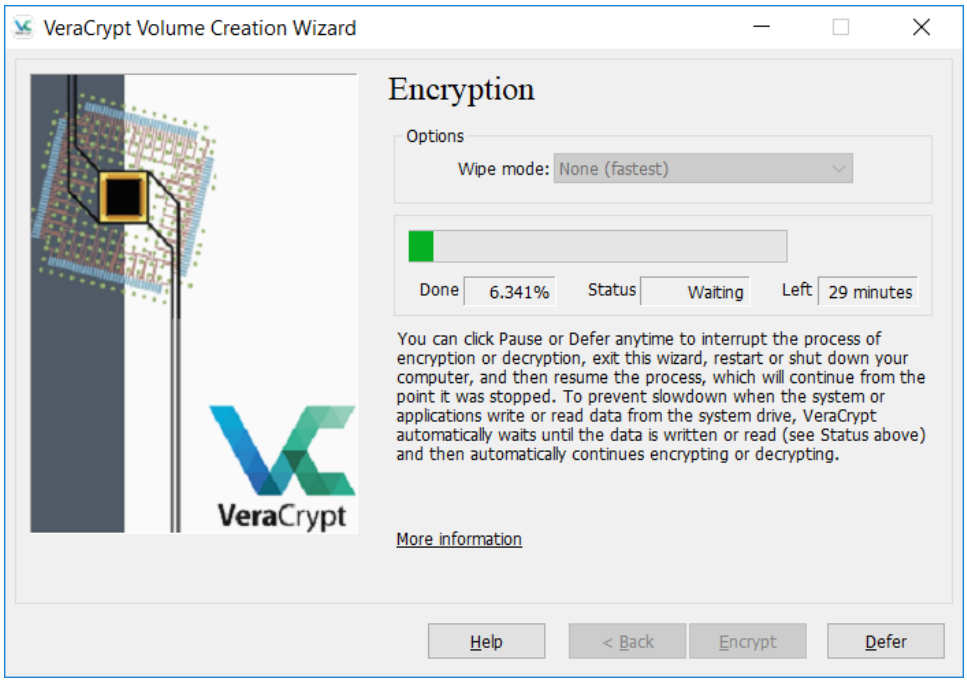
automatiquement votre mot de passe en QWERTY. Il vous faut donc entrer votre mot de passe normalement, même si le clavier passe en QWERTY.

Au démarrage de Windows, VeraCrypt confirme que le test a réussi et vous propose de commencer le chiffrement de la partition système. Cliquez sur `Encrypt` pour commencer.



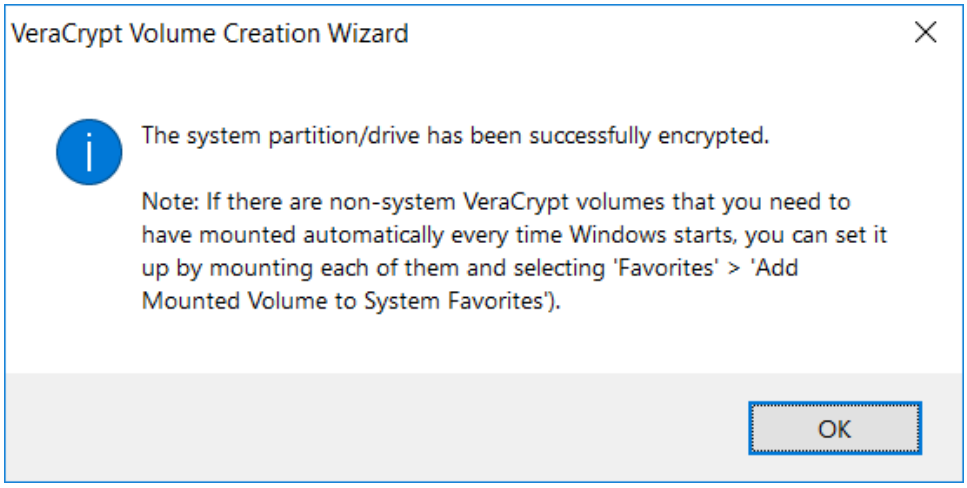
Test complet

Le processus prend environ 30 minutes pour un disque dur de 40 Go.



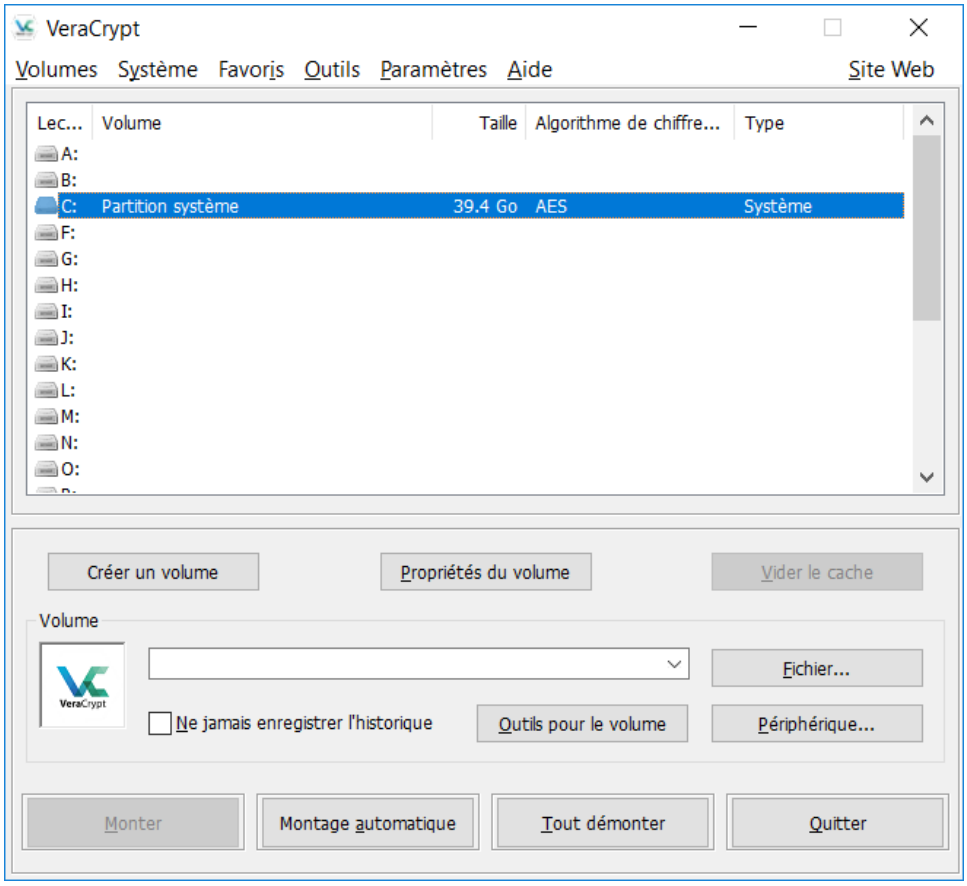
Encryption

Lorsque le chiffrement est terminé, vous pouvez cliquer sur `OK` pour fermer la fenêtre. La partition système est maintenant entièrement chiffrée et vous devez entrer le mot de passe au démarrage de l'ordinateur.



Validation

Vous pouvez vérifier dans VeraCrypt que la partition système est bien chiffrée.



Vérification

En résumé

- Le logiciel VeraCrypt permet de **chiffrer un disque dur à la volée**, c'est-à-dire de manière transparente pour l'utilisateur ;

- Veracrypt utilise par défaut le **chiffrement AES-256** en **modeXTS** ;
- Veracrypt génère une **clé secrète aléatoire**, qui est stockée sur le disque de manière chiffrée avec un mot de passe ;
- vous pouvez chiffrer un **fichier conteneur**, une **partition disque**, ou la **partition système** ;
- si vous chiffrez la partition système, vous aurez besoin du mot de passe pour démarrer la machine. Dans les autres cas, vous aurez besoin du mot de passe pour déchiffrer le volume chiffré.

Le professeur

Engue Gillier

Ingénieur Sécurité chez Facebook, anciennement Bug Bounty hunter notamment pour Google