

Utilisation de base du logiciel VeraCrypt.

L'objectif de ce document est de décrire étape par étape la création d'un fichier conteneur chiffré à l'aide du logiciel Veracrypt.

Postulat de départ : nous supposons que le logiciel VERACRYPT est déjà installé sur la machine avec laquelle vous souhaitez créer cette clef. Néanmoins, si ce n'était pas déjà le cas, vous pouvez télécharger le logiciel à l'adresse ci-dessous.

<https://www.veracrypt.fr>

Il existe une version « portable » de Veracrypt ne nécessitant aucune installation sur la machine. Néanmoins, nous recommandons d'utiliser la version installable sur le système d'exploitation. La version mobile sera éventuellement déposée sur un périphérique mobile et utilisée sur des machines n'appartenant pas au laboratoire et sur lesquelles toute installation est impossible.

Installez le logiciel ou demandez à l'administrateur de votre machine de le faire.

ATTENTION : ce fichier a vocation à être stocké sur les périphériques de stockage mobiles tels des clefs USB ou des disques durs externes. Stocker ce fichier sur un cloud synchronisé avec un dossier local peut entraîner des temps de synchronisation élevés ! Une modification, même minime, d'un fichier stocké dans le conteneur entraînera la synchronisation de l'intégralité du conteneur.

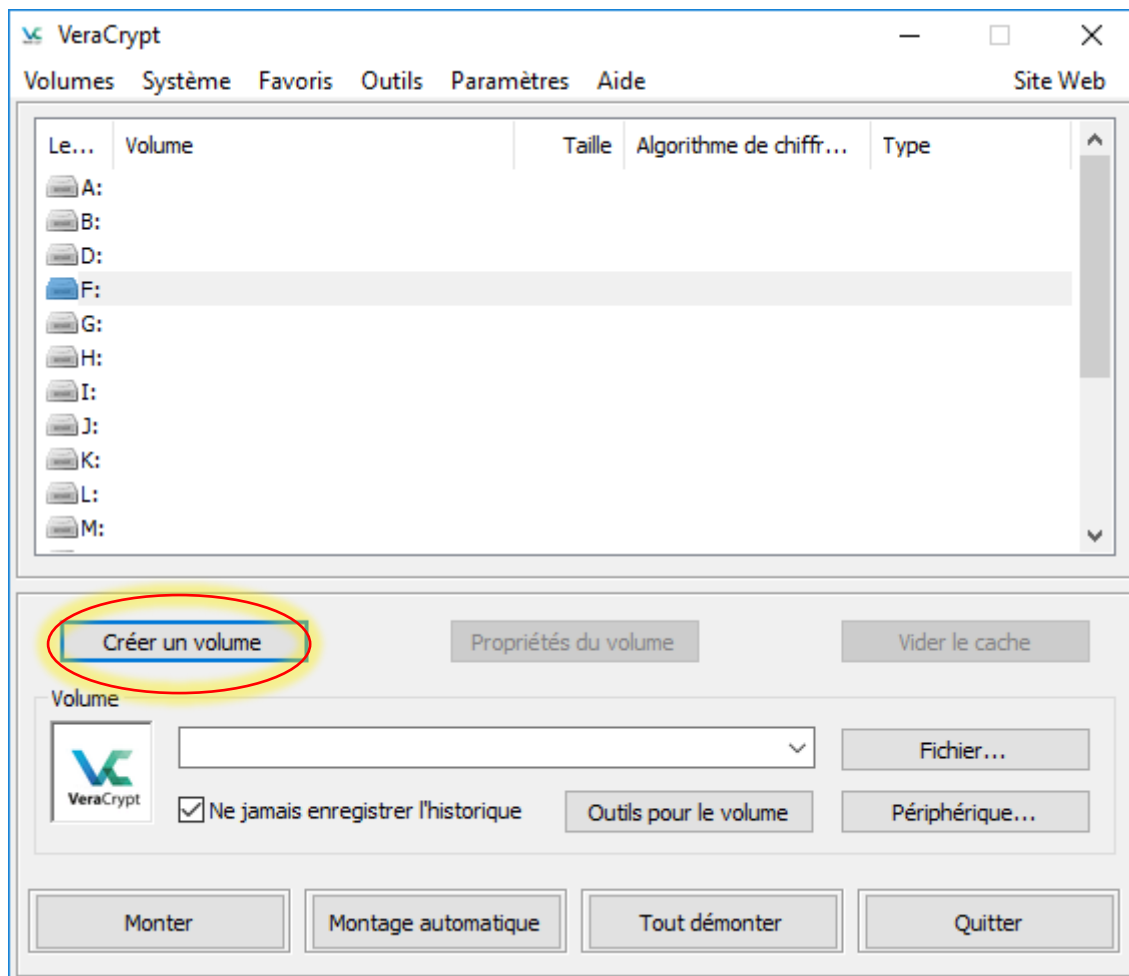


Université Clermont Auvergne

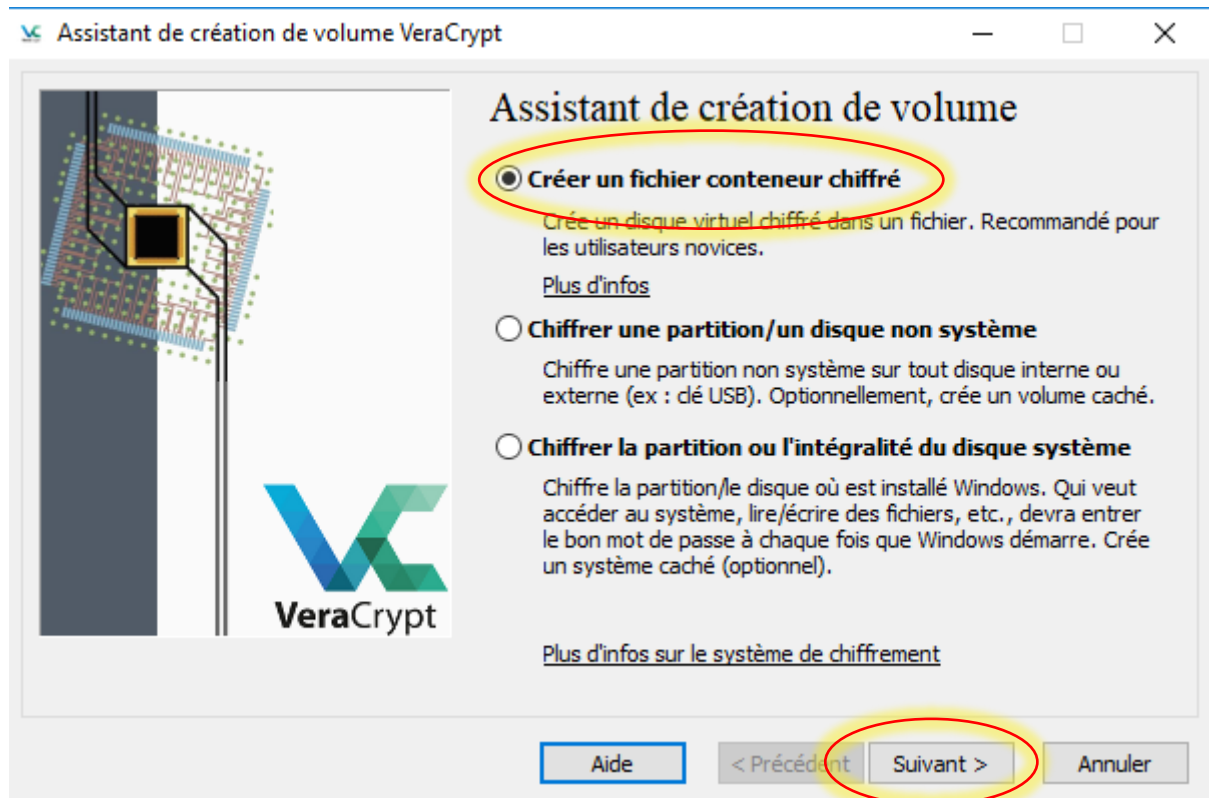
Direction Opérationnelle des Systèmes d'Information – Pôle proximité

Création d'un fichier conteneur chiffré :

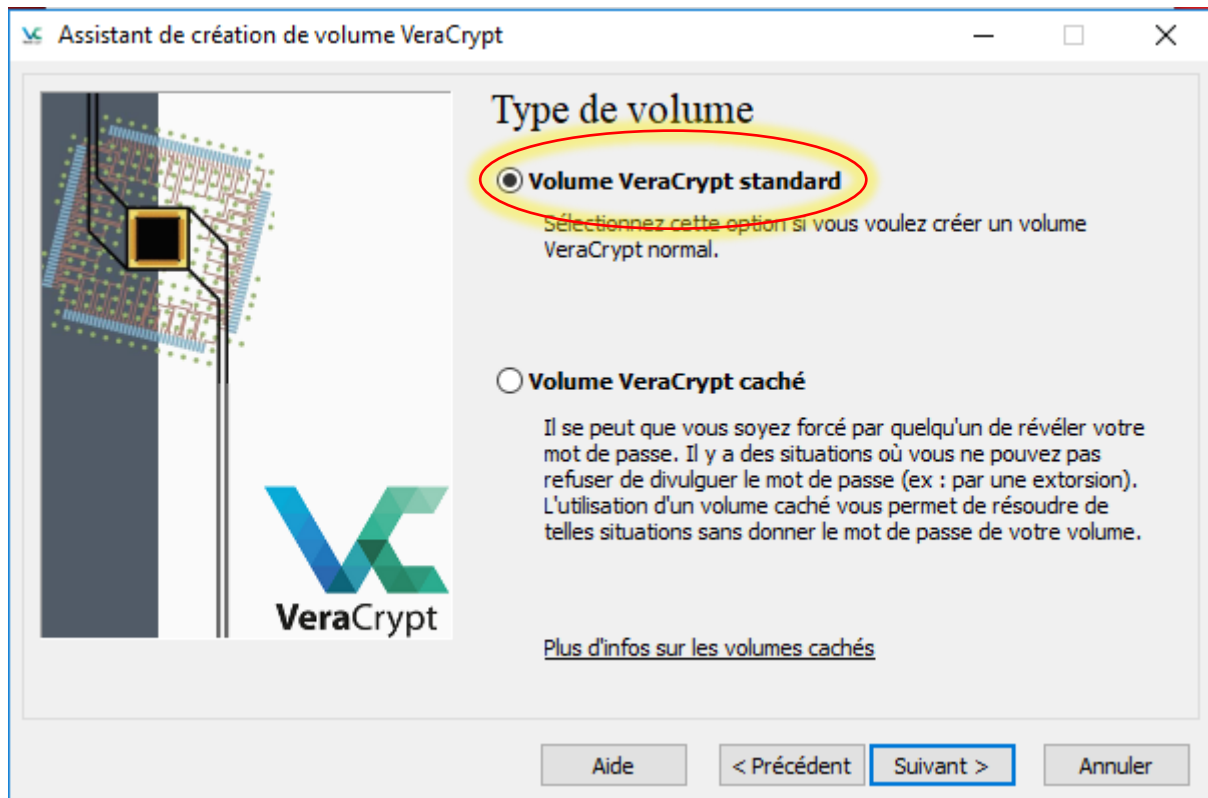
Etape 1 : Cliquez sur « créer un volume »



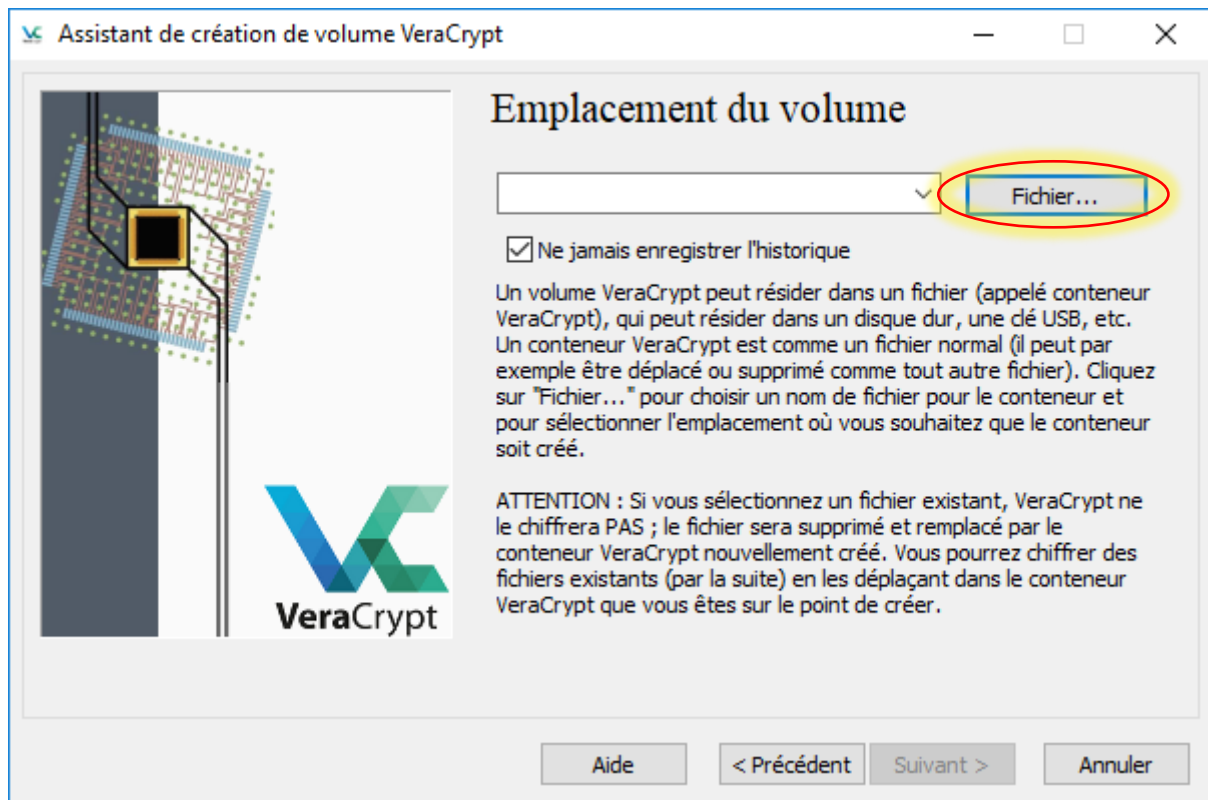
Etape 2 : Cochez « Créer un fichier conteneur chiffré » puis cliquez sur « Suivant »



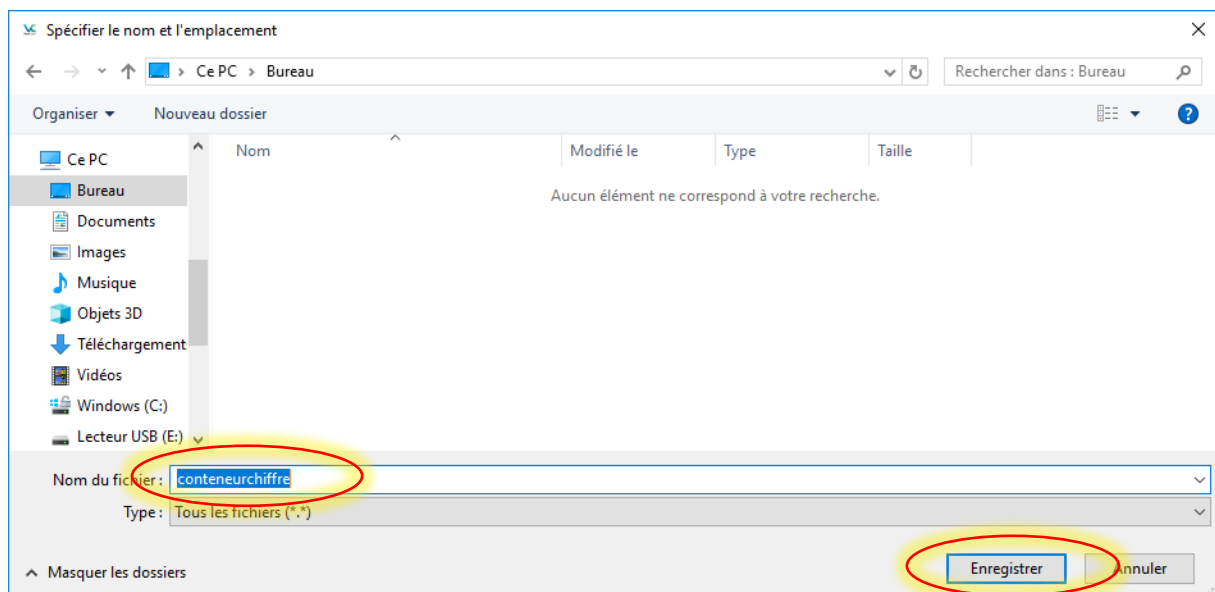
Etape 3 : Cochez « Volume VeraCrypt standard » puis cliquez sur « Suivant »

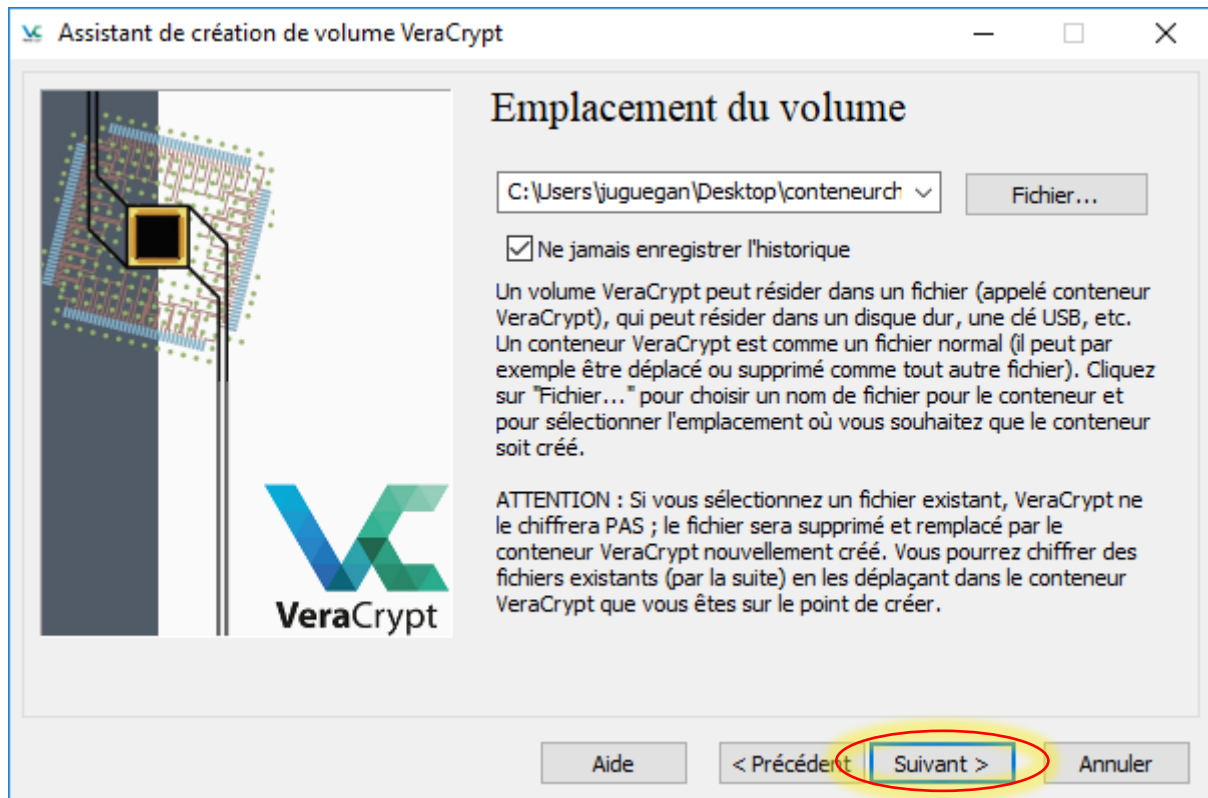


Etape 4 : Cliquez sur « Fichier ... » pour définir l'emplacement où vous souhaitez enregistrer le fichier



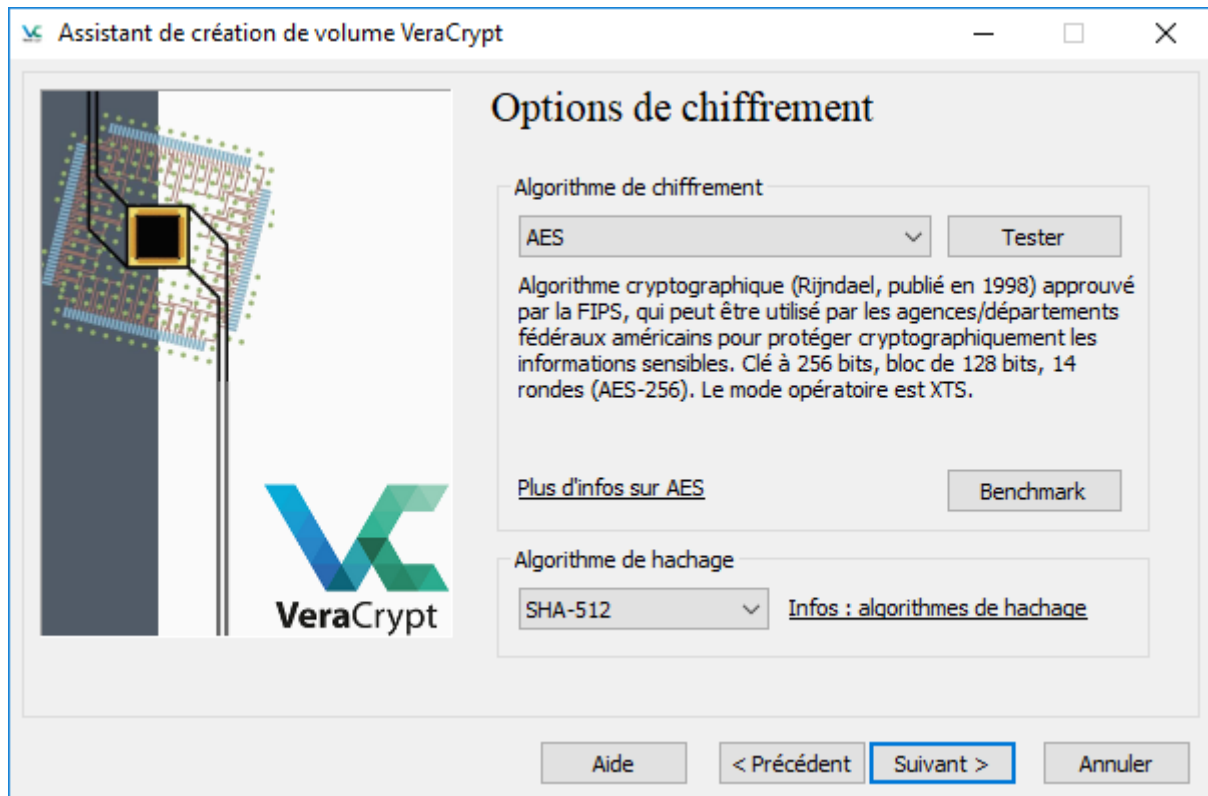
Donnez un nom au fichier, puis cliquez sur « Enregistrer »





Etape 5 : Options de chiffrement.

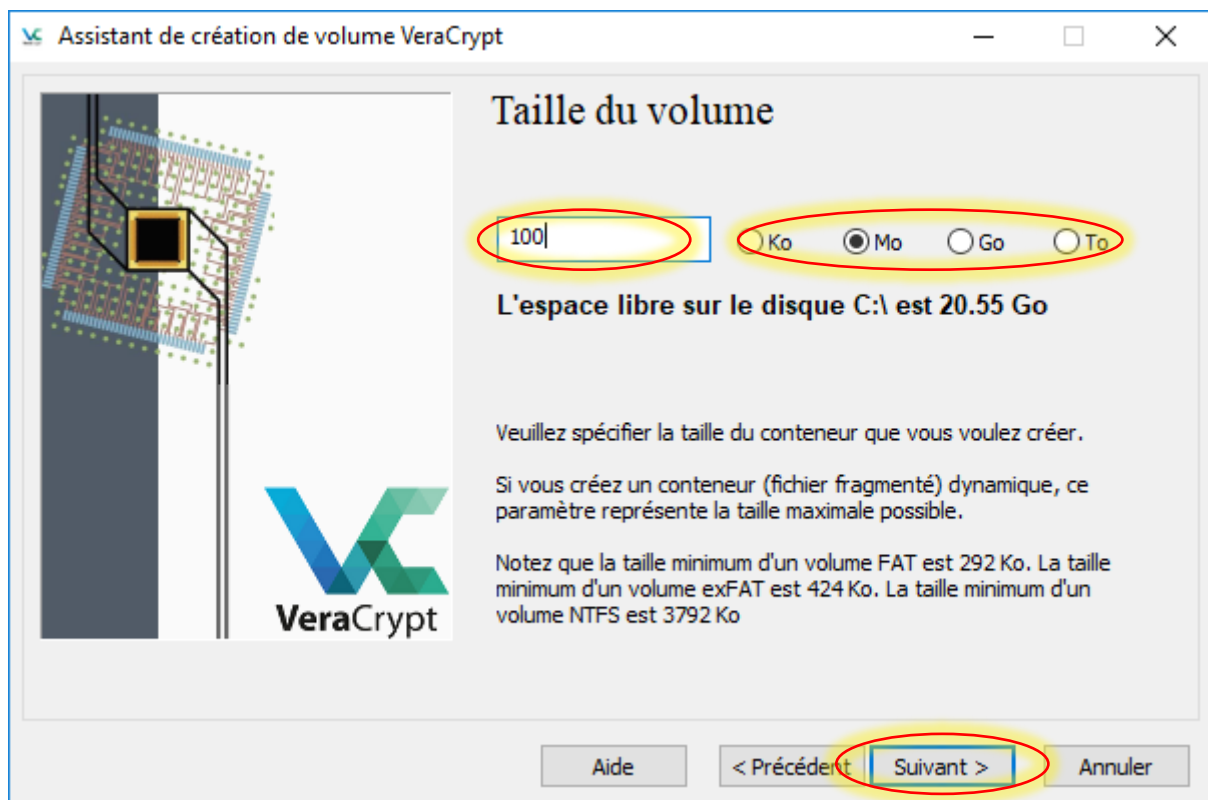
Cliquez sur « Suivant »



Etape 6 : Taille du volume.

Choisissez la taille que vous souhaitez allouer à votre fichier conteneur.

Attention : la taille du fichier sera fixe ; un fichier défini à 100Mo, même vide, fera 100Mo.



Etape 7 : Mot de passe du volume.

Définissez un mot de passe pour votre fichier puis cliquez sur « Suivant ».

Assistant de création de volume VeraCrypt

Mot de passe du volume

Mot de passe :

Confirmer :

☐ Utiliser fichiers clés Fichiers clés...

☐ Afficher le mot de passe

☐ Saisir un PIM

Il est très important que vous choisissiez un bon mot de passe. Vous devriez éviter d'utiliser un mot simple que l'on trouve dans un dictionnaire (ou une combinaison de plusieurs de ces mots). Il ne devrait pas contenir de noms ou de dates de naissance. Il ne devrait pas être facile à deviner. Un bon mot de passe est une combinaison de minuscules et de majuscules, de chiffres et de caractères spéciaux comme @ ^ = \$ * + etc. Il est recommandé de choisir un mot de passe d'au moins 20 caractères (le plus long, le mieux). La longueur maximale est de 64 caractères.

Aide < Précédent **Suivant >** Annuler

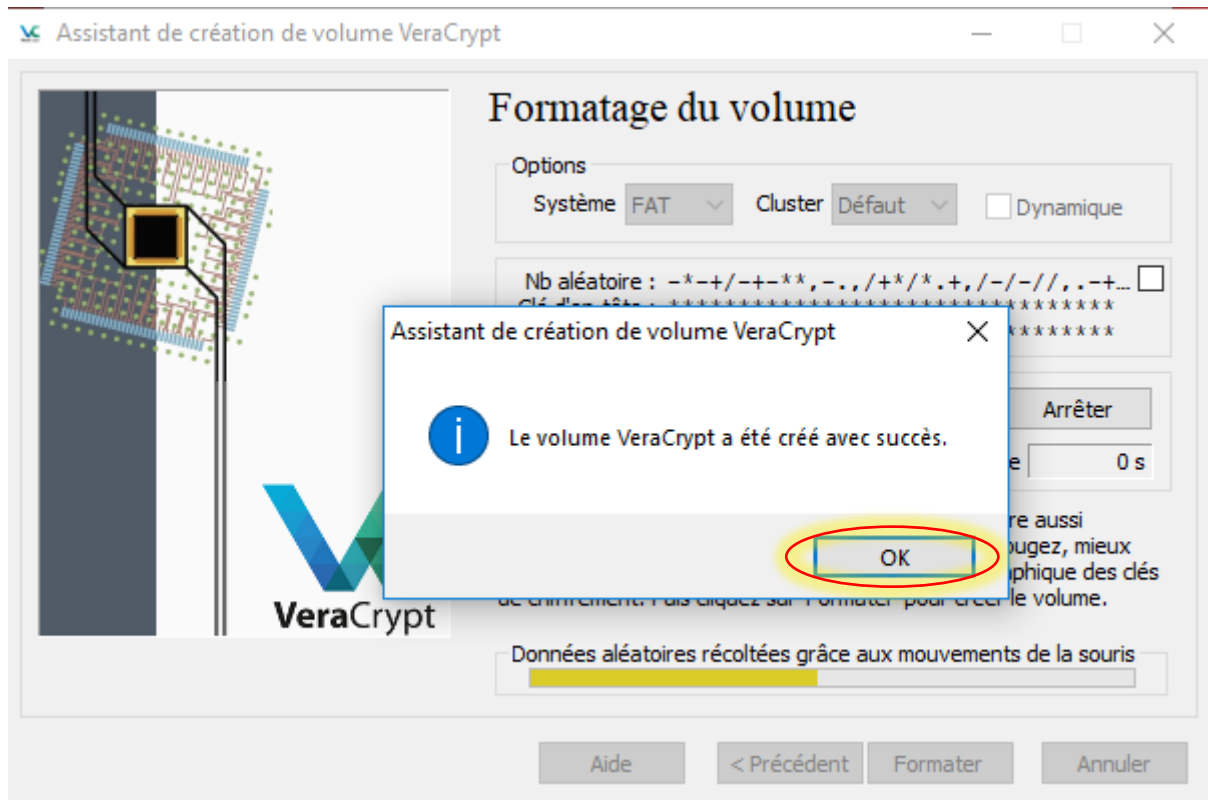
Etape 8 : Formatage du volume.

Cliquez sur « Formater ».

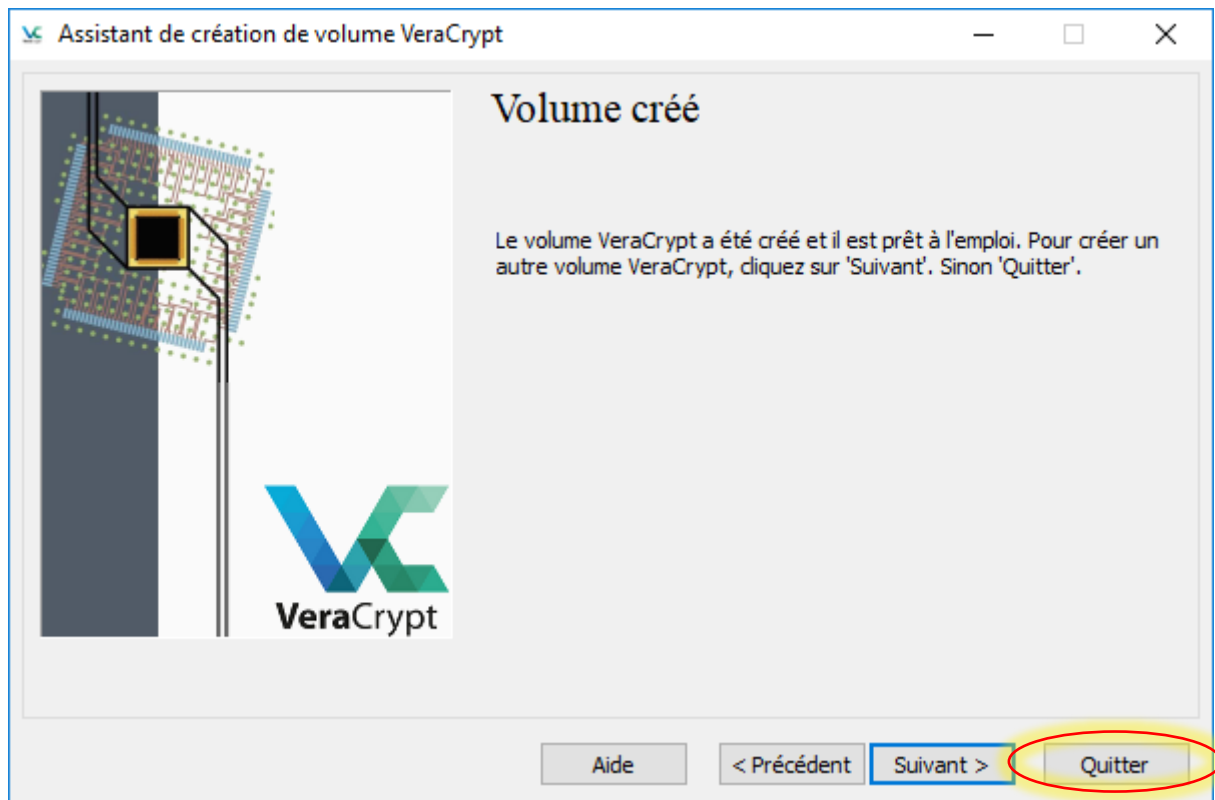
Vous pouvez aussi choisir le système de fichier de votre fichier. Ici « FAT » est choisi, mais vous pouvez sélectionner un autre système de fichier plus adapté à vos besoins.

The screenshot shows the 'Assistant de création de volume VeraCrypt' window, specifically the 'Formatage du volume' (Volume Formatting) step. On the left is a graphic with the VeraCrypt logo. The main area contains the following options:

- Options:**
 - Système: **FAT** (dropdown menu)
 - Cluster: **Défaut** (dropdown menu)
 - ☐ Dynamique
- Nb aléatoire: **+*-, -/.+*, +.**, */-+, *+ -*+-. , , , , , ...** (checkbox)
- Clé d'en-tête: *********
- Clé principale: *********
- A progress bar for 'Données aléatoires récoltées grâce aux mouvements de la souris' is partially filled with yellow.
- Buttons: **Arrêter**, **Fait à**, **Vitesse**, **Reste**.
- Important note: 'IMPORTANT : Déplacez votre souris dans cette fenêtre aussi aléatoirement que possible. Plus longtemps vous la bougez, mieux c'est. Cela accroît significativement la force cryptographique des clés de chiffrement. Puis cliquez sur 'Formater' pour créer le volume.'
- Bottom navigation: **Aide**, **< Précédent**, **Formater** (highlighted with a red circle), **Annuler**.



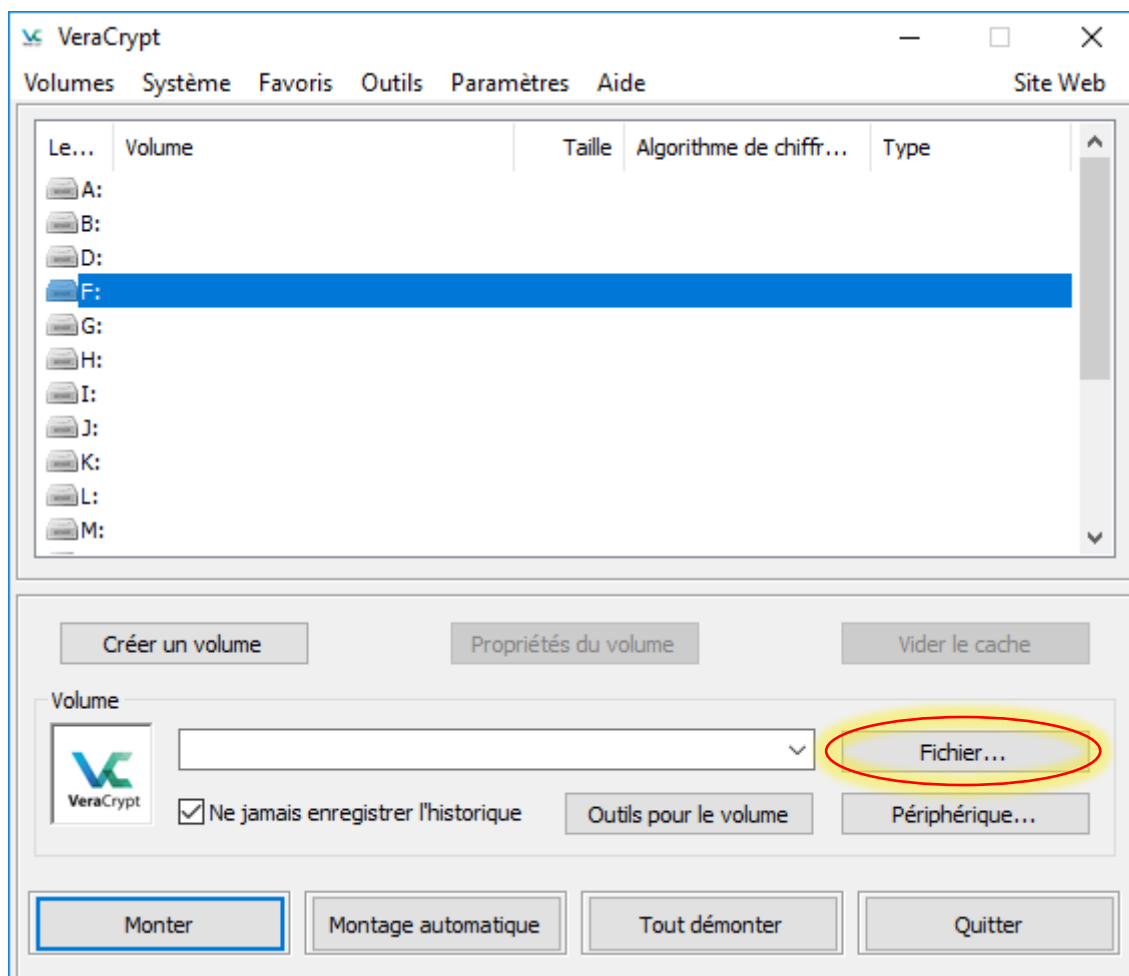
Etape9 : Le fichier est créé à l'emplacement que vous avez défini précédemment. Cliquez sur « Quitter ».



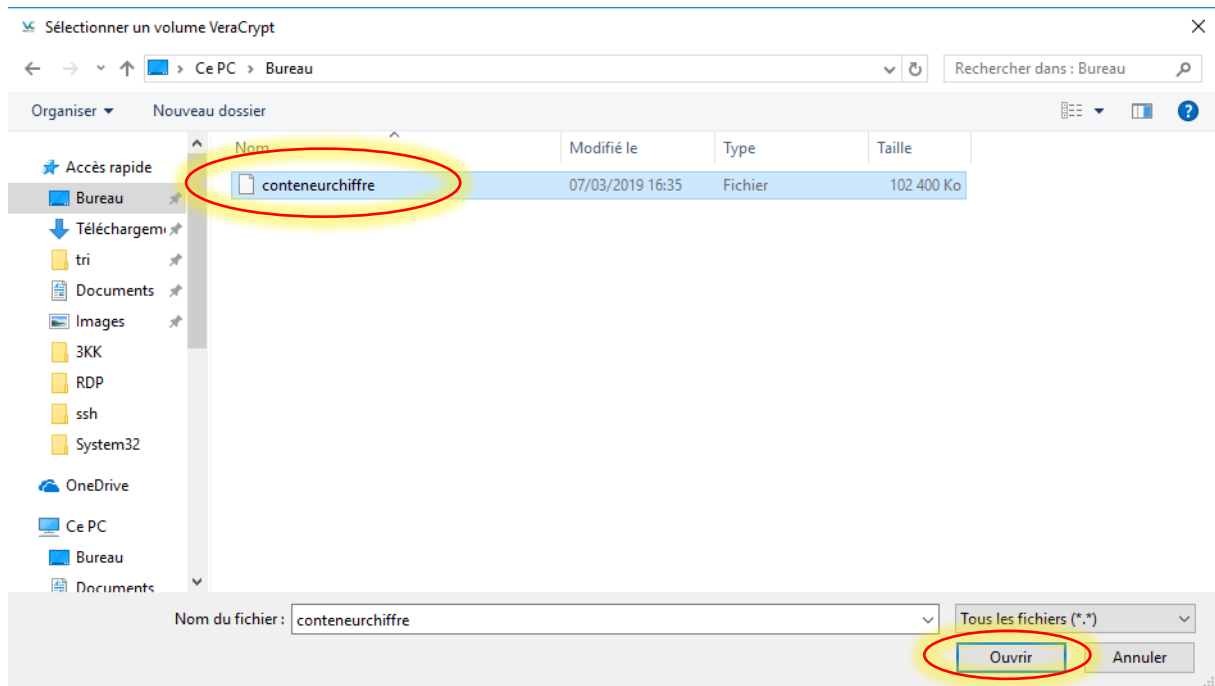
Lire le contenu d'un fichier chiffré.

Etape 1 : Lancez VeraCrypt.

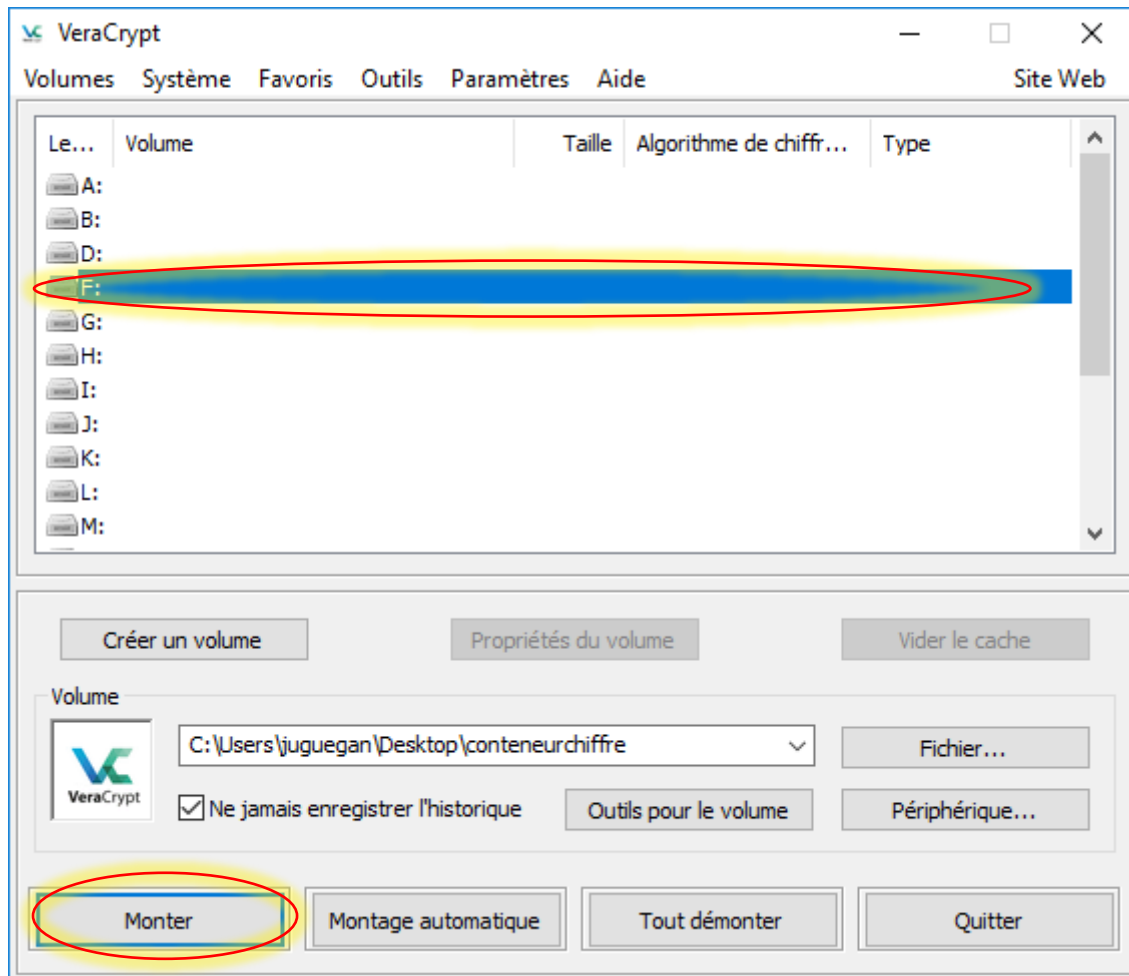
Etape 2 : Cliquez sur « Fichier... »



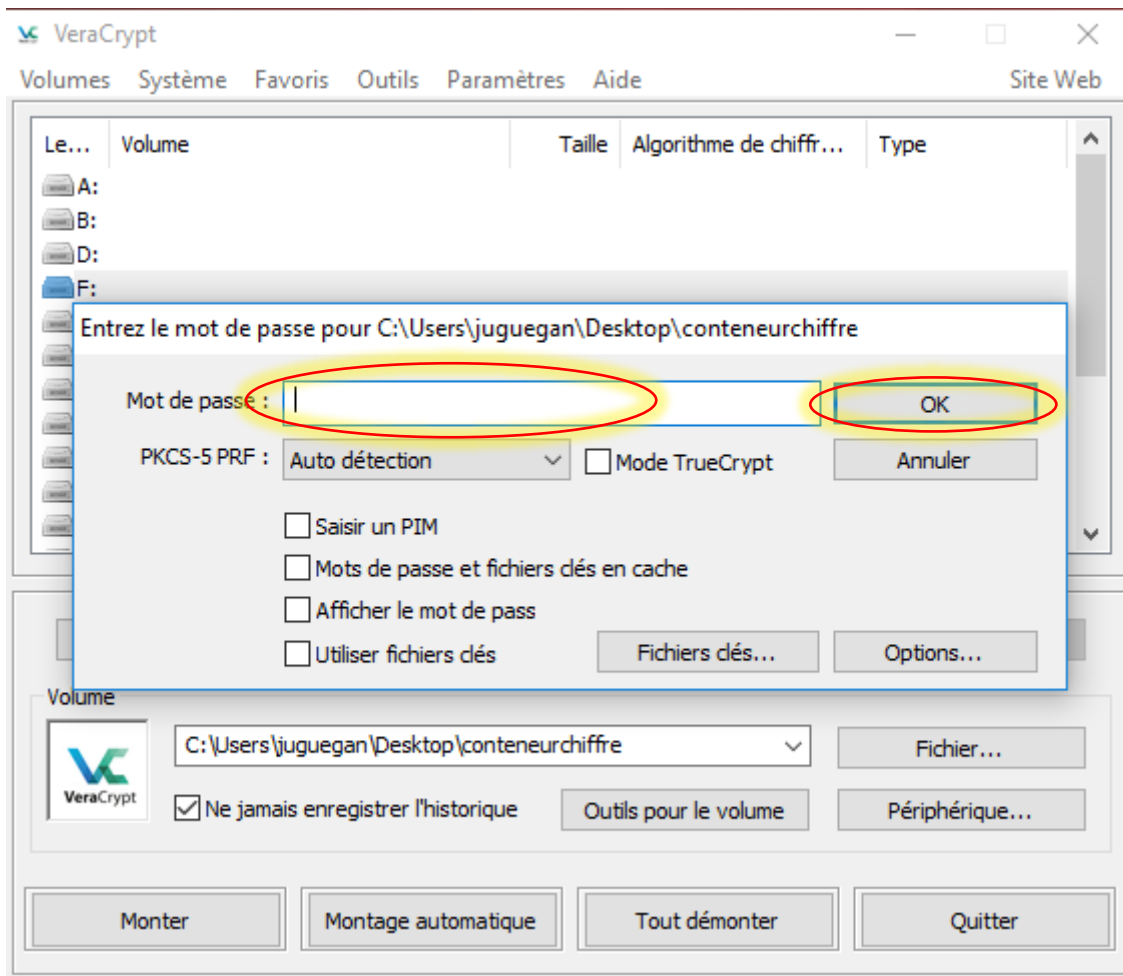
Etape 3 : Sélectionnez le conteneur que vous avez créé précédemment, puis cliquez sur « Ouvrir ».



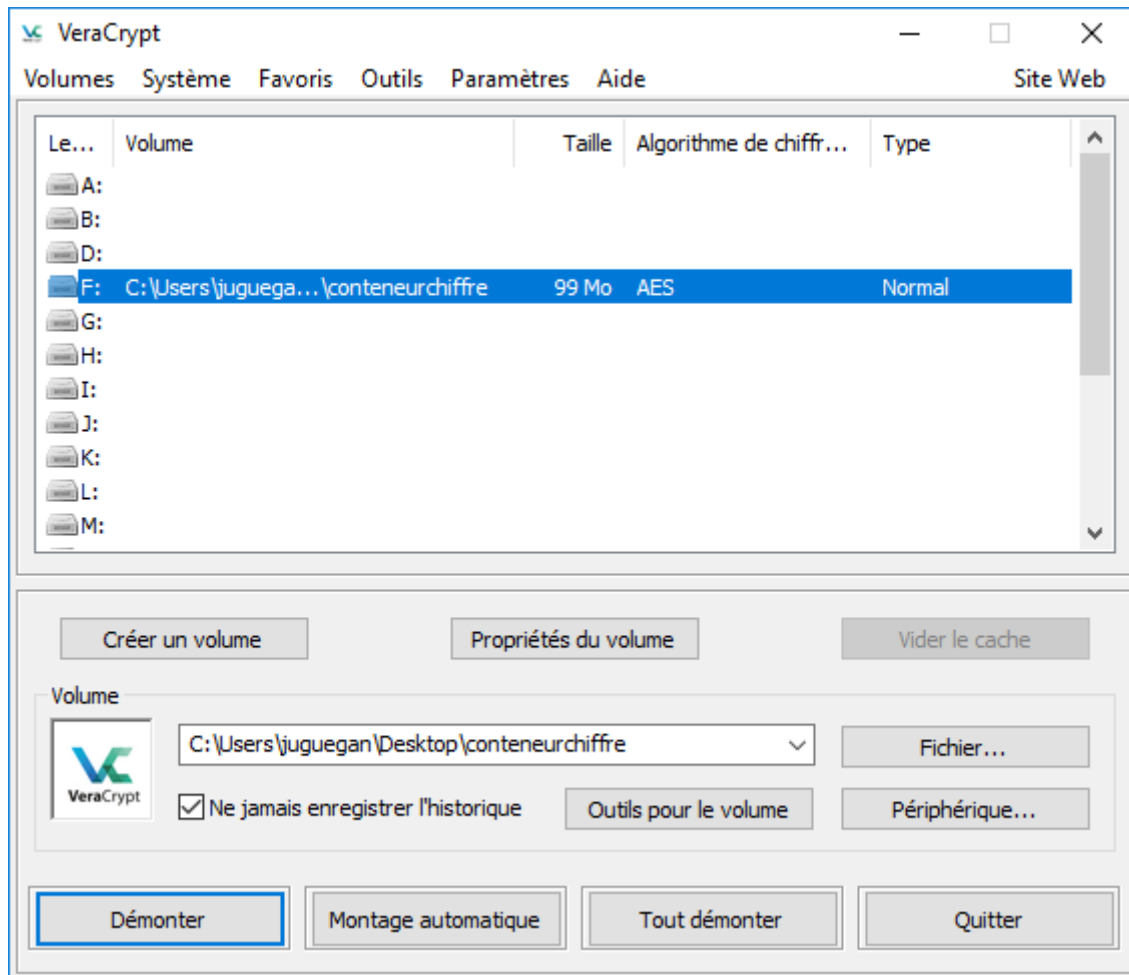
Etape 4 : Sélectionnez une lettre de lecteur, puis cliquez sur « Monter ».



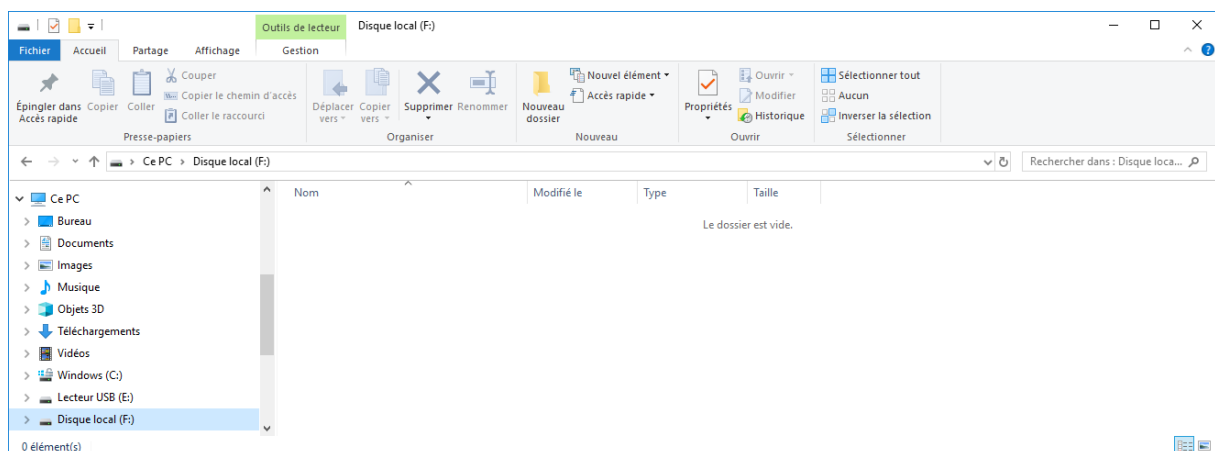
Etape 5 : Saisissez le mot de passe que vous avez défini précédemment pour votre conteneur, puis cliquez sur « OK ».



Etape 6 : votre fichier apparait désormais dans l'interface de VeraCrypt...



... et est utilisable via l'explorateur de fichiers de Windows, de la même manière qu'une clef USB.



Déconnecter un fichier conteneur chiffré.

Pour arrêter d'utiliser un fichier conteneur chiffré, vous ne devez pas l'éjecter comme vous pourriez le faire avec une clef USB, mais vous devez passer par les étapes suivantes.

Etape 1 : Lancez VeraCrypt

Etape 2 : Sélectionnez la lettre de lecteur attribuée à votre fichier puis cliquez sur « Démonter ».

