Créer un espace de stockage sécurisé avec VeraCrypt

Créer un espace de stockage sécurisé avec VeraCrypt

Modèle de menace :

>La police saisit une clé USB, un disque dur ou une carte SD pendant une perquisition, ou dans un sac à la frontière, ou pendant une action, etc. La clé USB ou assimilé est confiée à des spécialistes qui en extraient les données. Ces données sont utilisées plus tard pour incriminer le propriétaire et/ou d’autres rebelles et/ou compromettre la branche XR. La clé USB peut être rendue au rebelle arrêté sans aucune indication que ce processus a eu lieu.

Ce post est un complément à celui sur la [Sécurité de l'ordinateur : saisie par la Police](https://base.extinctionrebellion.fr/t/securite-de-lordinateur-1-saisie-par-la-police/52523) où il est conseillé de chiffrer le disque dur de son ordinateur s'il contient des données sensibles. Le modèle de menace est le même.

:arrow_right: Il ne s'agit pas ici d'apprendre à chiffrer son disque dur système (celui où est installé votre système d'exploitation) mais le logiciel est le même. Je vous conseille d'apprendre d'abord comment fonctionne VeraCrypt, puis à chiffrer quelque chose de léger comme une clé USB.

:arrow_right: Moins risqué pour votre ordinateur mais tout aussi amusant et utile, nous allons jouer ici avec une clé USB.

:arrow_right: Rappel : d'une manière générale, ne centralisez nulle part d'informations sensibles (noms, adresses, numéros de téléphones, tout ce qui peut permettre de casser le pseudonymat d'un.e rebelle et de l'identifer). Si vous le faites, il est conseillé d'avoir dans votre groupe local quelques clés USB sécurisées, achetées en liquide, si vous stockez des fichiers contenant des informations sensibles. N'oubliez pas de formatez les clés lorsque les données ne sont plus utiles.

Bonne lecture,

:blue_heart: & :zap:

Plan

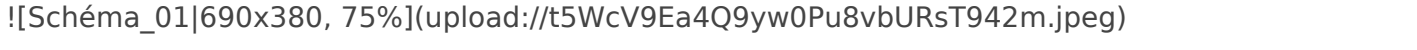
:bulb: Première partie théorique. Comprendre ce que nous allons apprendre à faire

:hammer_and_wrench: Seconde partie pratique. Créer un espace de stockage sécurisé

:bulb: Première partie : comprendre ce que nous allons apprendre à faire

Puisque de petits dessins sur Paint valent mieux que de longues prises de tête, en voici deux qui illustrent ce à quoi va nous servir le logiciel VeraCrypt.

Considérons ces trois espaces, de taille nécessairement décroissantes, qui représentent des volumes de stockage sur une clé USB.



VeraCrypt va nous permettre de créer dans notre clé USB ce qu'on appelle un conteneur, c'est-à-dire un volume de stockage sécurisé. C'est une fonction de base du logiciel. Après avoir créé votre "conteneur A", vous possédez sur votre clé USB un endroit protégé par un mot de passe que vous avez défini préalablement. Sur votre clé USB, le conteneur apparaît avec l'icône d'un simple fichier. C'est ce fichier qui sert de porte pour entrer dans le conteneur.

Une fonction plus avancée du logiciel permet de cacher un conteneur B dans le conteneur A. Le conteneur B est lui aussi protégé par un mot de passe qui lui est propre et, à la différence du conteneur A, il n'apparaît pas à l'écran. L'espace de stockage qu'il occupe est incorporé à celui du conteneur A, si bien qu'il n'apparaît pas individuellement dans la capacité de stockage (clic droit sur le disque, propriété). Il est invisible, ce qui lui donne un atout de poids : puisqu'il est impossible de prouver que vous cachez quelque chose, il est impossible d'exiger de vous que vous révéliez un mot de passe pour y accéder.

Voici, en image, comment fonctionne le cloisonnement entre les volumes de stockage.

Le logiciel VeraCrypt, après avoir servi à créer les conteneurs A et B, sert à y accéder. L'explorateur de fichiers ne les voit pas.

L'accès aux conteneurs fonctionne de la même manière que la salle sur demande d'Harry Potter : une seule porte pour plusieurs salles ; un seul fichier pour deux conteneurs. Cela signifie qu'il est impossible d'ouvrir en même temps les deux conteneurs : lorsque vous entrez un mot de passe, vous choisissez le conteneur qui se trouve derrière. Un fois le conteneur A ouvert, le conteneur B est inaccessible ; si le conteneur B est ouvert, le A est inaccessible. L'analogie s'arrête ici.

:hammer_and_wrench: Seconde partie : créer un espace de stockage sécurisé

Tout d'abord, bien sûr, il faut [télécharger VeraCrypt](https://www.veracrypt.fr/en/Downloads.html) et l'installer sur votre ordinateur. Notez qu'une version dite "portable" est disponible : dans ce cas

le logiciel sera installé sur une clé USB, ce qui vous permet de l'avoir avec vous sans promener votre ordinateur.

Suivez les instructions pour installer VeraCrypt et, si cela peut vous aider, installez-le en français.

:arrow_right: Nous utilisons ici la version standard, installée sur ordinateur, en français.

Plan du didacticiel

* Dans la partie :one: nous allons d'abord montrer étape par étape comment créer un volume de stockage simple (le conteneur A),

* puis nous verrons dans la partie :two: comment ouvrir ce conteneur pour l'utiliser.

* Dans la partie :three: nous suivrons la création d'un volume caché (le conteneur B).

:one: Créer un volume VeraCrypt standard

[details="Cliquez pour dérouler"]

On se munit avant tout d'une simple clé USB (ici "disque amovible (G:)"), comportant quelques fichiers que vous ne craignez pas de perdre. Dans le doute, faites-en une copie avant de commencer la manipulation. Vous pouvez aussi trouver sur internet des générateurs de fichiers aléatoires, très utiles quand on tatônne.

La capacité de la clé utilisée pour le tutoriel est de 1 Gb.

Le fichier texte "_Pédago" nous sert de balise, en marquant que nous sommes à la racine de la clé : c'est l'espace que l'explorateur de fichiers nous permet de voir. J'utiliserai ce système de fichier texte pour bien distinguer les différents volumes de stockage.

Pour les besoin du tutoriel, j'ai enregistré des fichiers aléatoires sur la clé. Celui qui est entouré en rouge "dlN1WUfgf1zc" est celui qui va nous servir de porte d'entrée dans nos conteneurs. On le renommera "VolumeStockageChiffré" par la suite.

![1|690x473, 75%](upload://683WHg3pqEpyFtW7pcHMyhYtttl.jpeg)

La clé étant en place, j'ouvre VeraCrypt, en double cliquant sur l'icône comme tout logiciel. La boîte suivante apparaît.

![2|569x487, 75%](upload://zgnylQEobgmWhESKHIyh48oeWr.jpeg)

La longue colonne de gauche vous montre tous les disques sur lesquels vous pourrez "monter" vos conteneurs : ce sont, pour ainsi dire, les endroits dans votre ordinateur où vous pourrez poser vos conteneurs pour les voir apparaître à l'écran.

Mais ce qui nous intéresse pour l'instant, c'est le bouton "Créer un volume". Cliquons.

![3|679x433, 75%](upload://pJYKntwTt0IrKMBQeSm9cWMWpFV.jpeg)

L'assistant de création s'ouvre, qui vous propose trois possibilités. Je vous laisse lire les petites lignes : ne cliquez pas au hasard !

Nous nous contentons de la première option : nous allons créer un conteneur (notre conteneur A) qui se trouvera dans un fichier (la porte d'entrée du conteneur).

Cliquons sur "Suivant".

Il s'agit ensuite de déterminer quel type de volume nous souhaitons créer, c'est-à-dire choisir entre conteneur A et conteneur B (cf. plus haut, première partie théorique du didacticiel).

![4|679x433, 75%](upload://ilkDFDimsFmlzeACFW6DOUg9Plz.jpeg)

Le volume caché (un conteneur B) sera l'objet de la seconde partie pratique. Nous créons ici un volume standard (le conteneur A).

Sans surprise, il s'agit de choisir l'emplacement du fichier-conteneur A sur notre clé USB.

![4_01|676x431, 75%](upload://p6pzRaL8oghIv2jmebrJJBcmUYx.jpeg)

Et sans surprise je choisis mon fichier "dlN1WUfgf1zc", renommé pour l'occasion "VolumeStockageChiffré". La pédagogie avant tout.

![4_02|480x407, 75%](upload://9aHHA1fgdczAz9AYuADZyCo719M.jpeg)

Je clique sur "Suivant" et une boîte me préviens que le fichier que je cible existe déjà.

![5|367x130](upload://vvV6qHCwR1egcSIMGxVN8QxTvki.jpeg)

Je confirme : ce fichier sera la porte d'entrée de mon conteneur chiffré.

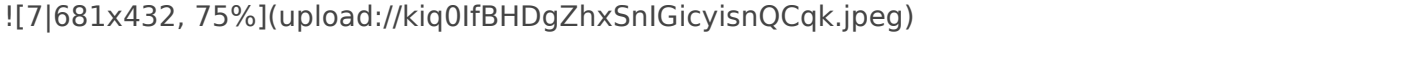
:warning: Attention : on ne vous le dit pas encore mais cela signifie que le contenu du fichier sera écrasé. Choisissez soigneusement votre fichier-conteneur (et ne l'appelez pas "VolumeStockageChiffré").

Je passe les options de chiffrement : si vous ne comprenez pas ce que vous dit cette boîte de dialogue, souriez-lui par politesse et cliquez sur "Suivant".

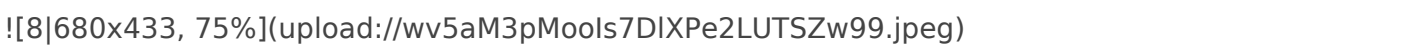
![6|678x432, 75%](upload://rBMHUL7VE1eZWNSTea77Bf0k4Cy.jpeg)

Vient ensuite un paramétrage essentiel : la taille du volume de stockage que vous allez créer. Vous ne pourrez pas la réajuster ensuite.
Considérez vos besoins de stockage : plus votre conteneur est volumineux, plus l'espace de stockage "normal" de votre clé USB sera faible. Demandez-vous si vous voulez protéger des fichiers textes (qui sont souvent légers) ou des vidéos (qui sont lourdes). L'assistant vous donne

clairement l'espace disponible sur votre clé USB (dans mon cas : 675, 09 Mo).



Je choisis de créer un conteneur de 500 Méga Octets et je passe au paramétrage essentiel suivant : le mot de passe.

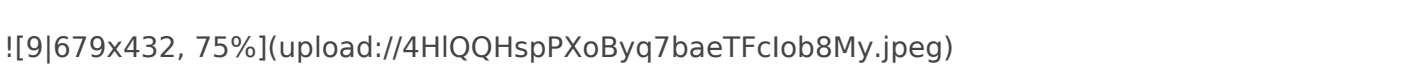


L'assistant ne vous encadrera pas aussi joliement les conseils sur le choix du mot de passe mais lisez-les attentivement quand même. Prenez le temps de réfléchir et d'aller voir notre [Foire au Questions spéciale sécurité numérique](https://base.extinctionrebellion.fr/t/securite-numerique-operationnelle-foire-aux-questions/54864). On vous propose une méthode pour vous créer un bon mot de passe.

Par sécurité, affichez le mot de passe, juste le temps de le relire, pour être sûr.e.

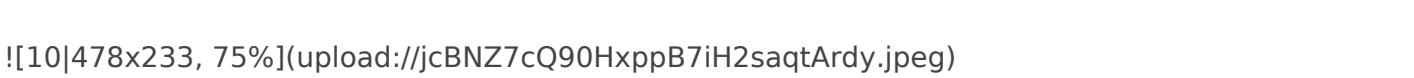
Et "Suivant".

Les choses se précisent. Lisez les petites lignes et bougez frénétiquement votre souris.



Lorsque la barre de chargement est pleine, soufflez et cliquez sur "Formater".

La boîte suivante apparaît : VeraCrypt vous signifie en majuscule que le fichier qui nous sert de porte pour entrer dans notre conteneur A sera SUPPRIMÉ. Mais comme on suit un tuto, on est sûr : "Oui".





Bravo :tada:

L'assistant est content de nous, on est content, on clique sur "Ok", on quitte l'assistant d'un air entendu et on va voir l'explorateur de fichier pour savoir ce qu'il pense de tout ça.

Le voici.



Du point de vue de l'interface, rien n'a changé. On est toujours sous (G:), on reconnait la balise "_Pédago", le fichier "VolumeStockageChiffré" est toujours là.

Ce qui a changé, c'est sa taille. Il a grossit, puisqu'on a créé dans ce fichier un conteneur de 500 Mo.

Reste que le fichier paraît corrompu ou cassé quand on essaie de l'ouvrir de manière traditionnelle, en lui cliquant dessus. Il faut utiliser le logiciel VeraCrypt pour ouvrir votre conteneur.

Voyons comment.

[/details]

:two: Ouvrir un conteneur sous VeraCrypt

[details="Cliquez pour dérouler"]

Retournons à la fenêtre basique de VeraCrypt.

En termes techniques, nous allons monter un volume sur un lecteur. Comme nous l'avons vu plus haut, la colonne alphabétique à gauche vous propose tous les lecteurs disponibles sur votre ordinateur pour accueillir le conteneur que vous voulez ouvrir. Si vous regardez attentivement, vous voyez sur l'image que, par exemple, les lecteurs C: et D: n'apparaîssent pas. Ce sont des lecteurs que mon ordinateur utilisent pour d'autres disques : je ne peux pas y poser mon conteneur. Vous observerez le même phénomène chez vous.

Je décide de choisir le lecteur A:.

![14|564x483, 75%](upload://cjvWhOKvujwBAdHuDLEQoM3SDpG.jpeg)

Dans la partie notée "Volume" (deuxième ellipse rouge), je sélectionne le fichier dont je sais qu'il s'agit de la porte vers mon conteneur A. On reconnaît le nom subtil du fichier : "VolumeStockageChiffré", toujours sur ma clé USB qui occupe le lecteur G: (qui, vous l'avez vu, n'est pas dans la liste des lecteurs disponibles. Tout fait sens).

La cible étant acquise, je clique sur le bouton pour "Monter" mon conteneur sur le lecteur A:.

Le logiciel demande bien sûr le mot de passe.

![15|499x194, 75%](upload://bkj82k3uUhT9K57dfUmB1l8LemF.jpeg)

Lorsque le chargement du conteneur est effectué, la fenêtre VeraCrypt montre que le conteneur a bien été monté sur le lecteur A:. Le volume de stockage est de 499 Mo.

![16|564x482, 75%](upload://6JnJQYDULxPycVOQdl85s9MKrqW.jpeg)

Remarquez la mention : "Type : Normal". Elle signifie qu'il s'agit d'un conteneur standard, chiffré mais pas caché. Si je reprends notre typologie maison, cela montre qu'il s'agit d'un conteneur A et non d'un conteneur B. Un conteneur B serait noté "Type : Caché".

Pour ouvrir votre conteneur et y enregistré vos fichiers secret-défense, faites un clic droit sur la ligne, puis "Ouvrir".

![17|568x484, 75%](upload://1b2053zUiTRJxvCDHGblT9jmx5q.jpeg)

Une nouvelle fenêtre apparaît, qui vous montre l'intérieur du conteneur, tel qu'ici :

![18|532x500, 75%](upload://egezr7mRNkSpdIbDr2HR2jgSBnp.jpeg)

Comme demandé, le conteneur est bien monté sur le lecteur A:.

Pour la démonstration, j'ai placé un fichier texte, comme sous la racine de la clé USB, qui nous sert de balise pour reconnaître l'espace de stockage de mon conteneur A. Dans la dernière partie du didacticiel, je créerai une balise similaire pour marquer mon volume caché, le conteneur B.

Après avoir enregistré les fichiers souhaités et fermé la fenêtre, je peux laisser mon conteneur monté sur le lecteur A:. Dans ce cas, il reste ouvert et je peux y accéder sans avoir à redonner le mot de passe. Pratique tant que je travaille sur l'ordinateur mais c'est une faille de sécurité absurde si je ne suis pas vissé devant l'écran.

Pour refermer le conteneur, je dois le démonter. Un bouton est prévu à cet effet, joie : les développeurs sont des gens prévoyants.

![19|564x482, 75%](upload://8TVDKHbfrIcEkBTXUm0wBePLEFT.jpeg)

Cliquez et attendez que VeraCrypt fasse le travail. Lorsque le volume est démonté, son nom disparait de la fenêtre et il faudra de nouveau le monter sur un lecteur pour y accéder de nouveau.

>On prend une pause et on respire.

Si vous avez suivi toutes les étapes jusqu'ici, vous êtes sans doute parvenu à créer un conteneur chiffré sur votre clé USB et à y placer des documents confidentiels.

Cela étant, ne perdons pas de vue que vos documents, pour protégés qu'ils soient, ne sont pas cachés. Si, d'une manière ou d'une autre, un opposant peut vous forcer à donner votre mot de passe, vos documents sont compromis. Cela peut arriver en garde à vue, suite à une perquisition etc. La pression que vous pouvez subir ne doit pas être minimisée ni négligée.

Pour s'en protéger, on cache un conteneur B, invisible, dans un coin sombre du conteneur A.

Allez, go.

[/details]

:three: Créer un volume VeraCrypt caché

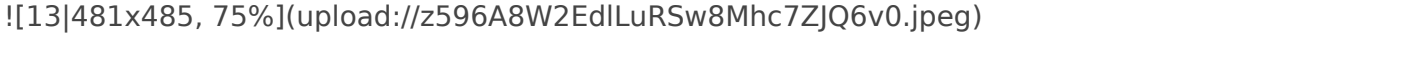
[details="Cliquez pour dérouler"]

Dans le modèle de menace qui nous occupe ici, lorsque la Police branche ma clé USB sur un ordinateur, elle voit ceci :

Le contenu à la racine de la clé :



Et, bien sûr, les propriétés de la clé :



Au-delà de l'évidence qu'une liste aussi bizarre de fichiers peut être suspecte (je passe sur le nom de mon fichier le plus coupable..), c'est l'espace utilisé par vos fichier sur la clé qui peut trahir la présence d'un conteneur.

Imaginez que mon fichier "VolumeStockageChiffré" s'appelle "Recette tarte aux fraises.txt" : rien de plus suspect qu'un fichier texte aussi anodin qui pèse près de 500 Mo. D'autant que lorsque l'agent de police clique dessus, le fichier est inutilisable.

L'opposant (celui qui veut récupérer les infos sensibles) essaye alors de nous faire craquer. C'est là qu'un conteneur caché est utile. Il vous permet de donner le mot de passe du conteneur A, qui ne doit contenir que des fichiers pseudo-sensibles. Comme on l'a vu dans la partie théorique du didacticiel, une fois révélé le conteneur A, le conteneur B est inaccessible. Et, puisque l'opposant ne peut pas prouver qu'il existe, il ne peut pas vous forcer à en révéler le mot de passe.

Invisible, me direz-vous ? Oui. Vous ne le saviez pas mais les 791 Mo utilisés, qui apparaissent en bleu sur l'image précédente, sont en fait occupés non seulement par notre conteneur A mais aussi par un conteneur B (et oui, je vais plus vite que le tuto). Invisible donc, parce que la porte d'entrée dans le conteneur B est le même fichier que pour le conteneur A : sa présence n'est pas trahit par l'interface.

Reprenons. Créons donc ce conteneur B, à l'intérieur du conteneur A.





Les deux étapes précédentes sont les mêmes que pour un conteneur A (volume standard). C'est à la troisième que l'on bifurque.

Puisque j'ai déjà créé mon conteneur A, je choisis "Volume VeraCrypt caché", puis "Mode direct".

Si vous n'avez pas déjà créé de conteneur sur votre périphérique de stockage, utilisez le "Mode normal" et suivez les étapes précédentes du didacticiel.

Je cible le fichier-conteneur qui sert de porte d'entrée au conteneur A, puisque c'est à l'intérieur de celui-ci que je vais construire le B.

"Suivant".

Même remarque que plus haut : dans le doute, ne touchez à aucun de ces paramètres de chiffrement. "Suivant".

Vous allez pouvoir choisir la taille du volume de stockage de votre conteneur B. Vous remarquez que, sur ma clé de 1 Go, seuls près de 500 Mo sont disponibles. Si vous avez suivis la partie :one: sur la création du conteneur A, vous avez que c'est la taille que j'ai alloué à ce conteneur A. Le B, qui se trouve dans le A, est nécessairement plus petit que lui.

"Suivant".

Choisissez un mot de passe puissant : inutile de prendre des risques.

Créez le volume caché, selon la même méthode que le conteneur A.

Et voilà !

J'ai dorénavant sur ma clé USB deux conteneurs, tels que décrit dans la partie théorique, tout en haut.

Nous allons voir que c'est bien le même fichier "VolumeStockageChiffré" qui sert à y entrer. J'utilise la même manipulation pour ouvrir le conteneur B que celle utilisée pour ouvrir le conteneur A.

Je cible le fichier, pour le monter sur le lecteur A:.

Remarquez que le mot de passe que je rentre ici est plus long que celui que j'ai créé pour le conteneur A. Il s'agit bien du mot de passe qui me donne accès au conteneur B.

On le voit ici :



Tout paraît identique, sauf que la taille du volume est bien de 299 Mo (pour les 300 demandés) et ce conteneur porte la mention "Type : Caché". Le conteneur A portait la mention "Type : Normal".

Je fait un clic droit sur la ligne pour ouvrir le conteneur.



Le même fichier m'a bien amené vers le conteneur B, comme en témoigne le fichier balise que j'y ai posé pour les besoins de la démonstration. C'est le mot de passe entré lors du "montage" du volume sur un lecteur qui détermine quel conteneur je vais ouvrir. Si vous avez créé un volume caché sur votre clé USB, le volume standard (conteneur A) est fait pour être révélé : c'est un leurre qui vous permet de nier l'existence d'un volume caché (conteneur B).

Ça va ?

[/details]

Créé 2023-09-08 20:19:16 CEST par mollusque
Mis à jour 2025-02-23 12:53:24 CET par mollusque