

Chiffrer vos données avec VeraCrypt

Le menu :

- 1 Intro.
- 2 Modes opératoires possibles avec TrueCrypt
- 3 Installation.
- 4 Configuration.
- 5 Montage automatique des volumes
- 6-Sauvegarde / Restauration.
- 7 Les KeyFiles pour une authentification renforcée
- 8 Cryptage du volume contenant le Système d'Exploitation.
- 9 Crypter ET cacher sa partition (système).
- 10 Détecter la présence de volume VeraCrypt

1 – Intro.

Sur la base de TrueCrypt, VeraCrypt est un logiciel qui permet le cryptage des fichiers et partitions sous forme de conteneur global ou fichier unique.

Dans la continuité de Truecrypt, sans les problèmes identifiés en 2014, une société Française Idrix a développé un produit similaire disponible sur SourceForge et CodePlex. VeraCrypt est sous licence TrueCrypt et surtout MS-PL (Licence Microsoft Public).

Qu'apporte VeraCrypt vis à vis de la version de TrueCrypt ? Les équipes de VeraCrypt ont tenu compte et corrigé un bon nombre de faiblesses/vulnérabilités identifiées par l'Open Crypto Audit Project sur TrueCrypt.

Le rapport d'origine sur l'audit de TrueCrypt : https://opencryptoaudit.org/reports/iSec_Final_Open_Crypto_Audit_Project_TrueCrypt_Security_ Assessment.pdf

La liste des corrections apportées suite à l'audit de TruceCrypt :

https://veracrypt.codeplex.com/discussions/569777#PostContent_1313325

Le document présente différentes utilisations possibles de VeraCrypt: un usage classique avec création d'un fichier(volume) crypté et protégé par un mot de passe, la même chose protégé par un

fichier clé (keyfile), le cryptage de tout votre PC ou portable y compris la partition système (!), et le cryptage d'un volume qui sera caché.

VeraCrypt effectue le cryptage/décryptage à la volée après lecture du fichier, avant enregistrement du fichier. C'est aussi ce qu'on appelle le cryptage OFT = On The Fly

La version 1.0f2 présente les fonctionnalités suivantes :

- Compatibilité Mac OS X 10.6 à 10.10
- Compatibilité Windows XP à 8.1 en 32 et 64 bits
- Compatibilité Linux kernel 2.6+ en 32 et 64 bits
- Montage automatique des volumes VeraCrypt. Si vous posséder un volume VeraCrypt sur un support amovible que vous connectez celui-ci sur votre PC, le volume *pourra* être monté automatiquement.
- Comptabilité entière des volumes TrueCrypt (merci Korben : http://korben.info/veracryptest-maintenant-compatible-avec-les-conteneurs-truecrypt.html)
- Les partitions supportent des secteurs de taille 1024 à 4096 octets.
- La gestion de Volumes Favoris présente de nombreuses options (montage lecture seule, ordre de montage, etc...)
- la possibilité de crypter une partition contenant des données, sans perdre le contenu (sous Vista/Windows 2008)
- le support des tokens et smart cards
- l'interopérabilité d'un volume crypté sous Windows et utilisable sous Linux/Mac

• ...

Cette dernière release intègre des corrections aux vulnérabilités identifiées dans la phase II de l'audit de TrueCrypt

(https://opencryptoaudit.org/reports/TrueCrypt_Phase_II_NCC_OCAP_final.pdf)

2 – Modes opératoires possibles avec VeraCrypt

Il existe plusieurs variantes à l'usage de VeraCrypt : certains ont la première utilité de crypter ses fichiers pour se protéger de tout vol alors que d'autres visent à masquer, voire leurrer l'hypothèse que vous puissiez crypter vos fichiers. En voici cinq :

Créer un conteneur VeraCrypt dans un fichier visible. Cette option basique vous permet de vous promener avec votre conteneur (fichier) sur une clé USB, votre disque externe, vos sauvegardes, etc avec un minimum de confidentialité. C'est ce qui est expliqué dans la <u>partie 3</u>

- **Dédier une partition (non système) en tant que conteneur VeraCrypt**. Option similaire à la précédente avec un conteneur qui fera la taille de votre partition ou de votre disque complet, donc particulièrement confortable pour les disques externes par exemple.

- **Mettre sa partition Système dans un conteneur VeraCrypt**. Cette fois-ci, votre système d'exploitation et tout l'environnement/paramètres/données qui se trouvent sur la partition système se trouvent cryptés, de manière transparente pour l'OS, hormis le **VeraCrypt** Boot Loader initial qui vous demandera un mot de passe pour lancer votre OS. <u>Partie 7.</u>

Déclarer un conteneur dans un fichier qui contiendra lui-même un autre conteneur caché. Imaginez un coffre-fort caché derrière un tableau de maitre, ce coffre-fort une fois découvert s'avère posséder quelques documents peu compromettants mais possède surtout un double fond

contenant vos véritables documents confidentiels. A ceci près qu'en fonction du mot de passe du conteneur initial, soit vous ouvrez le conteneur leurre, soit vous ouvrez le conteneur qui vous est cher.

 A l'image de l'option précédente, vous cryptez votre partition système, qui se trouve contenir également une autre partition systèmes chiffrée accessibles l'une comme l'autre selon le mot de passe saisi. Cet usage est détaillé en <u>partie 8</u>

Enfin, une fonctionnalité commune à tous les modes ci-dessus concerne la clé d'accès au conteneur chiffré : dans les cas les plus simples, la clé sera un mot de passe mais peut également être un fichier de votre choix.

3 – Installation

Parce que le parc de postes Windows est encore important, c'est cet OS qui est utilisé pour expliquer un peu plus comment çà s'installe.

Il vous faudrait donc :

Windows 7+

VeraCrypt 1.19 (<u>https://veracrypt.codeplex.com</u>) – le package d'installation fait environ 23 Mo Etre administrateur du poste (uniquement durant la phase d'installation)

Après avoir accepté la licence, un premier choix :



Vous pouvez choisir de poursuivre une installation classique ou d'extraire VeraCrypt: ce choix est utile si vous souhaitez utiliser VeraCryptponctuellement sans installer quoique soit sur l'ordinateur (utilisation dans un cadre mobile). Choisissons le cas le plus répandu : **install**



Rien de particulier dans cet écran sauf à noter la possibilité de forcer un point de restauration Windows.

L'installation finie



Vous aurez cette icône sur votre bureau :



Pour avoir une interface en langue autre qu'US :

Allez simplement dans Settings / Langages....

4 – Configuration

L'étape primordiale est ensuite de créer un volume (unité logique de type e, f, g,...) qui sera cryptée et qui contiendra l'ensemble de vos données protégées.

Allez dans le menu Volumes, Créer un Nouveau Volume ou cliquez sur le bouton « Creer un volume »



Trois choix s'offrent à vous :

1 – « *Créer un fichier conteneur* chiffré», créer un volume qui sera associé à un fichier unique de type *confidentiel.tc* qui contiendra les fichiers cryptés sur votre volume habituel (par exemple sur



2 – « *Chiffrer une partition/ un disque non système* », créer un volume complet sur un espace disque disponible tel que une clé USB, une partition de disque non-utilisée, un disque externe

3 – « *Chiffrer la partition ou l'intégralité du disque système* », modifier une partition actuelle pour la rendre cryptée en totalité. Cette partition peut-être la partition système ou le disque système.

Ces 3 choix définissent ce à quoi ressemblera le container crypté qui stockera les fichiers cryptés.

Choisissons la première option .

L'écran suivant vous propose deux options (disponibles également pour les autres choix précédents) :

Assistant de création de volu	me VeraCrypt
inning	Type de volume
	Olume VeraCrypt standard
	Sélectionnez cette option si vous voulez créer un volume VeraCrypt normal.
- management	O Volume VeraCrypt caché
	Il se peut que vous soyez forcé par quelqu'un de révéler votre mot de passe. Il y a des situations où vous ne pouvez pas refuser de divulguer le mot de passe (ex : par une extorsion). L'utilisation d'un volume caché vous permet de résoudre de telles situations sans donner le mot de passe de votre volume.
	Plus d'infos sur les volumes cachés
	Aide < Précédent Suivant > Annuler

– Standard TrueCrypt Volume : globalement, vous allez créer un espace (fichier ou partition) qui sera visible en tant qu'élément chiffré. Traditionnel...

Hidden TrueCrypt Volume (ou mode paranoïa) : le container qui recevra les fichiers cryptés sera 'invisible', cet espace sera plus précisément sur un espace de disque non partitionné donc non visible sous Windows. Dans le détail, c'est un schéma de fonctionnement peu plus compliqué mais davantage sécurisé puisqu'une analyse rapide d'un ordinateur ne permettra pas de repérer l'existence d'un volume crypté.

Assistant de création de volume VeraCr	ypt
VERA CRYPT	Emplacement du volume d:\test\confidentiel.vc Fichier Ne jamais enregistrer l'historique Un volume VeraCrypt peut résider dans un fichier (appelé conteneur VeraCrypt), qui peut résider dans un fichier (appelé conteneur VeraCrypt), qui peut résider dans un disque dur, une dé USB, etc. Un conteneur VeraCrypt est comme un fichier normal (il peut par exemple être déplacé ou supprimé comme tout autre fichier). Cliquez sur "Fichier" pour choisir un nom de fichier pour le conteneur et pour sélectionner l'emplacement où vous souhaitez que le conteneur soit créé. ATTENTION : Si vous sélectionnez un fichier existant, VeraCrypt ne le chiffrera PAS ; le fichier sera supprimé et remplacé par le conteneur VeraCrypt nouvellement créé. Vous pourrez chiffrer des fichiers existants (par la suite) en les déplaçant dans le conteneur VeraCrypt que vous êtes sur le point de créer.
	Aide < Precedent Suivant > Annuler

Vous devez ensuite définir de l'emplacement de votre container (ou fichier global) qui contiendra vos éléments à protéger). Cet emplacement peut être vos disque local, externe, USB,... précisez un chemin, voir un nom de fichier. *Si celui-ci existe, il ne sera pas réutilisé mais écrasé par TrueCrypt*.

Assistant de création de volume Vera	Crypt	
	Options de chiffrement Algorithme de chiffrement AES AES	Tester
RYPT	Serpent Twofish AES(Twofish) AES(Twofish(Serpent)) Serpent(AES) Serpent(Twofish(AES)) Twofish(Serpent)	nces/départements raphiquement les de 128 bits, 14 XTS. <u>B</u> enchmark
VERA C	Algorithme de hachage SHA-512 Infos : algorit Aide < Précédent	hmes de hachage ivant > Annuler

L'étape suivante consiste à sélectionner en premier le **type de cryptage** que vous souhaitez utiliser. AES, Serpent ou TwoFish mais plus amusant encore, vous pouvez choisir d'additionner séquentiellement 1 ou 2 voire 3 de ces algorithmes déjà forts puissants utilisés de manière individuelle. Partons sur AES, un système de cryptage à clé symétrique très répandu dans maintes applications informatiques, système robuste et approuvé par le NIST, le FIPS et la NAS comme algorithme de cryptage fort. Pour l'anecdote qui n'en pas une, l'algorithme a été conçu par deux Belges Vincent Rijmen et Joan Daemen.

Le menu Outils / Banc de Test vous permettra d'évaluer le cryptage le plus rapide.

Sélectionnez aussi le **type de hachage** retenu. Le hachage étant l'algorithme qui permet de définir une empreinte « unique » pour un fichier donné. Si le contenu du fichier est modifié, le hachage ne sera plus vérifiable et confirmera que le fichier a été modifié.

Choisissez SHA-512, relativement répandu et très fiable (produit un condensat ou Hash de 512 bits, ce qui est assez important).

Assistant de création de volume Vera	Crypt
	Taille du volume
	560
VERA CRYPT	Please specify the size of the container you want to create. If you create a dynamic (sparse-file) container, this parameter will specify its maximum possible size. Note that the minimum possible size of a FAT volume is 292 KB. The minimum possible size of an NTFS volume is 3792 KB.
	Aide < Précédent Suivant > Annuler

Définissez le volume que fera votre conteneur (en Ko ou Mo ou Go). L'espace sera alors alloué dans son intégralité sur le disque mais comme une coquille vide.

Petit rappel : un Ko est Kilo Octet = 1000 octets et qu'il ne faut pas confondre avec un Kibi Octet = 1024 octets. Le CEI a normalisé tout ceci (le kibi octet, le mebioctet,...) en 1998.

Assistant de création de volume Vera	Crypt
	Mot de passe du volume
VERA CRYPT	Confirmer : Fichiers dés Fichiers dés Afficher mot de passe Fichiers dés Afficher mot de passe 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 < <u>P</u> récédent Suivant > Annuler

Sur le choix du mot de passe, inutile de préciser que plus c'est long plus c'est bon ... mais si c'est trop long et trop compliqué on est obligé de le noter sur un post-it... Cela n'empêche pas pour

autant d'y glisser quelques caractères exotiques, chiffres, majuscules, minuscules,...).

Le mot de passe est limité à 64 caractères. C'est ce mot de passe qui vous sera demander pour accéder au volume crypté.

Si vous cochez « Fichier Clé », vous devrez indiquer un fichier qui servira de « clé » supplémentaire au mot de passe. Ce fichier sera ensuite toujours nécessaire pour pouvoir ouvrir le fichier TrueCrypt. Cela peut-être un fichier mp3, avi, texte... <u>Mais un fichier qui ne soit plus</u> <u>modifié !</u>

En fonction de l'utilisation de votre conteneur (notamment si la taille des fichiers hébergés dans le volume sont > 4 Go), TrueCrypt utilisera le système de fichier adapté (exclusion de FAT).



L'étape suivante est de générer les clés nécessaires au cryptage du volume sur un modèle le plus aléatoire possible sans utiliser la fonction pseudo aléatoire de votre ordinateur. Plus le mouvement de la souris sera long, plus la clé sera difficile à reproduire.

Sélectionnez également le système de fichier retenu (FAT, NTFS)

L'option « Dynamique » permet de créer un conteneur de taille limité qui grossira au fur et à mesure des besoins (mais ne diminuera pas) : cette fonction mérite de ne pas occuper la totalité du volume spécifié au départ, en revanche cela a un impact sur les performances.

Vous devez donc bouger la souris puis faire « Formater »

Assistant de création de volume VeraCr	ypt
VERA CRYPT	Formatage du volume Options Système NTFS Obtions Dynamique Nb aléatoire : D1F8F270FDB01EDA2E02EF14F153501D Clé d'en-tête : 9CEE5B1EAD217635A53CE18C38138B30 Clé principale : 063B3640131216A9876B8051D4210FEE Important Arrêter Fait à 30.004% Vitesse 73.1 Mo/s Reste 48 s 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. Aide < Précédent Eormater

Le container sera formaté et l'espace chiffré

Assistant de création de volume VeraCrypt
Le volume VeraCrypt a été créé avec succès.
ОК

Vous pouvez ensuite quitter sans quoi l'assistant vous re-proposera de créer un nouveau volume...



Le conteneur créé (sous forme de fichier) avec l'extension que vous avez choisi.

5 – Montage automatique des volumes



Faites un double-click pour accéder à l'interface

🛐 VeraCrypt	x
<u>V</u> olumes Système Favor <u>i</u> s <u>O</u> utils <u>P</u> aramètres <u>A</u> ide <u>S</u> ite	Web
Le Volume Taille Algorithme de chiffr Type	
G:	-
E H:	=
	-
<u> </u>	
<u>ا</u> N:	
i <u>⇒</u> 0:	
	-
Créer un volume Vider le cache	
Volume	
E:\confidentiel.vc	
Ne jamais enregistrer l'historique	
Outils pour le volume Périphérique	
Monter Montage automatique Quitter Quitter	

- Sélectionnez la lettre de lecteur qui sera affectée au volume chiffré,
- Dans Volume, sélectionnez le fichier que vous avez généré.
- Cliquez sur « Monter »
- Saisissez votre mot de passe

Mot de passe :	•••••		ОК
PKCS-5 PRF :	Auto détection	Annuler	
	Mots de passe et fich	niers dés en cache	
	Afficher mot de pass	e	

 – l'option « Mode Truecrypt » vous permet de spécifier que le volume sélectionné a été créé par TrueCrypt.

Cliquez sur OK

Volumes Système Favoris Qutils Paramètres Aide Site Web Le Volume Taille Algorithme de chiffr Type Image: Constraint of the second	🚐 VeraC	rypt							
Le Volume Taille Algorithme de chiffr Type F: G: I I I I: I: I I I I: I: I I I I: II II III IIII I: IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Volumes	S <u>y</u> stème	Favor <u>i</u> s	<u>O</u> utils	<u>P</u> aramè	tres <u>A</u> i	de		<u>S</u> ite Web
F: G: H: I: J: K: E: \confidentiel.vc 5.0 Go AES Normal L: M: N: O: Image: Créer un volume Propriétés du volume Vider le cache Volume E: \confidentiel.vc Fichier Fichier Volume E: \confidentiel.vc Fichier W: Ne jamais enregistrer l'historique Outils pour le volume Périphérique	Le	Volume				Taille	Algorithme de chiffr	Type	*
G: H: I: I: M: M: N: O: P: Créer un volume Propriétés du volume Vider le cache Volume E: \confidentiel.vc Fichier Fichier Fichier P: Volume Units pour le volume Périphérique	i i i i i i i i i i i i i i i i i i i								
H: I: J: M: N: O: P: Créer un volume Propriétés du volume Vider le cache Volume E:\confidentiel.vc Fichier P: Fichier Priphérique	📄 G:								
I: J: K: E: M: M: N: O: P: Volume Volume E: Créer un volume P: Vider le cache Volume E: Confidentiel.vc Fichier P: Volume Difference Fichier Volume Difference Volume Outils pour le volume Périphérique	i i i i i i i i i i i i i i i i i i i								E
image: State in the	i in the second								
K: E: \confidentiel.vc 5.0 Go AES Normal Image: L: Image: Mission Missio Mission Missio Mission Mission Mission Mi) 📄 J:								
Image: Second secon	K:	E:\confident	iel.vc			5.0 Go	AES	Normal	
M: N: O: P: Créer un volume Propriétés du volume Vider le cache Volume E:\confidentiel.vc Fichier Fichier Propriétés du volume Volume Units pour le volume Périphérique	E:								
N: O: P: Créer un volume Propriétés du volume Vider le cache Volume E:\confidentiel.vc Fichier Fichier Propriétés du volume Volume E:\confidentiel.vc Fichier Périphérique Périphérique	M:								
O: P: Créer un volume Propriétés du volume Vider le cache Volume E:\confidentiel.vc Fichier Fichier Propriétés du volume Volume E:\confidentiel.vc Fichier Périphérique Périphérique	-N:								
Créer un volume Propriétés du volume Vider le cache Volume E:\confidentiel.vc Fichier Image: Second	0: 0:								
Créer un volume Propriétés du volume Vider le cache Volume E:\confidentiel.vc Fichier Image: Second Secon									-
Créer un volume Propriétés du volume Vider le cache Volume Fichier E:\confidentiel.vc Fichier Image: Ne jamais enregistrer l'historique Outils pour le volume Périphérique									
Volume E:\confidentiel.vc Image: Ne jamais enregistrer l'historique Outils pour le volume Périphérique		réer un volum	e		Proprié	étés du vo	olume	Vider le	cache
E:\confidentiel.vc Fichier Ne jamais enregistrer l'historique Outils pour le volume Périphérique	Volume								
Image: Second state of the second s		E:\cor	nfidentiel.v	c			•	Fichie	r
Outils pour le volume Périphérique		Ne j	iamais enre	aistrer l'hi	storique				
						Out	ils pour le volume	Périphér	ique
Démonter Montage automatique Tout démonter Quitter		Démonter	M	ontage au	tomatique	•	Tout démonter	Q	uitter

Aller ensuite dans le menu *Favorites*, et sélectionnez « Add mounted volumes to Favorites...»

Le Label	Volume	
к:	E:\confidentiel.vc	
<u>M</u> onter De	escendre	Supprimer
Label du volume favoris	sélectionné :	
Documents Personnels		
Documents Personnels Monter le volume séle Monter le volume séle	ectionné en <u>l</u> ecture seule ectionné en tant que support amo <u>v</u> ible	
Documents Personnels Monter le volume séle Monter le volume séle Monter le volume séle	ectionné en <u>l</u> ecture seule ectionné en tant que support amo <u>v</u> ible ectionné à l' <u>o</u> uverture de session	
Documents Personnels Monter le volume séle Monter le volume séle Monter le volume séle Monter le volume séle	ectionné en lecture seule ectionné en tant que support amo <u>v</u> ible ectionné à l' <u>o</u> uverture de session ectionné quand son appareil hôte est <u>c</u> onnecté	
Documents Personnels Monter le volume séle Monter le volume séle Monter le volume séle Monter le volume séle Ouvrir une fenêtre de	ectionné en <u>l</u> ecture seule ectionné en tant que support amo <u>v</u> ible ectionné à l' <u>ouverture de session</u> ectionné quand son appareil hôte est <u>c</u> onnecté e l' <u>E</u> xplorateur pour le volume sélectionné quand il e	est monté avec succès

De nombreuses options associables au montage de ce volume favori :

- Mettre un label pour rendre le volume facile à identifier parmi d'autres.
- Monter le volume en lecture seule,
- Préciser que le volume est monté à partir d'un support amovible,
- Ne monter le volume que pendant que la session est ouverte,
- Préciser que le volume est monté à partir d'un lecteur réseau
- Ouvrir l'explorateur Windows dès que le volume est monté,
- Ne pas monter le volume favori quand la hot key est pressée.
- Choisir parmi plusieurs volumes, l'ordre de montage des volumes cryptés.

Validez par OK.

Vous trouverez alors l'unité logique montée comme une partition, tout ce que vous y mettrez sera chiffré et accessible uniquement avec VeraCrypt + votre mot de passe (ou votre fichier clé+mot de passe)

Particularités Windows

L'idéal est dans la plupart des cas, d'avoir VeraCrypt exécuté et initialisé à chaque démarrage de Windows.

Dans le menu Paramètres / Préférences des options sont à activer pour permettre cela :

VeraCrypt - Préférences
Options de montage par défaut Monter les volumes en lecture seule Monter les volumes comme des médias amovibles
Tâche de fond VeraCrypt Image: Activer Image: Quitter quand il n'y a aucun volume monté
Actions à effectuer à l'ouverture d'une session Windows Image: Start VeraCrypt Background Task Image: Monter tous les volumes VeraCrypt
Démontage automatique Tout démonter si : Démontage automatique est activé Démontage automatique quand aucune donnée n'a été lue/écrite durant 60 minutes
Windows Image: Ouvrir la fenêtre de l'Explorateur des volumes montés avec succès
 Utiliser une icône de barre des tâches différente quand il y a des volumes montés Preserve modification timestamp of file containers
Mots de passe en cache Mots de passe en cache Vider le cache des mots de passe en quittant Vider le cache des mots de passe au démontage
Plus de paramètres OK Annuler

Notamment « Start VeraCrypt Background Task »

Désormais, à chaque lancement de VeraCrypt , le (ou les) volumes sauvegardés dans les favoris seront montés automatiquement.

6 - Sauvegarde / Restauration

L'essentiel est maintenant d'envisager la situation suivante :

- que faites-vous si votre fichier conteneur est perdu, altéré, effacé ?

Il n'y a pas grand chose à faire dans le cas où le conteneur est un fichier stocké sur un volume windows : sauvegardez le fichier classiquement sur bande, média externe,...Restaurez, réinstallez VeraCrypt et voilà...

7 – Les KeyFiles pour une authentification renforcée

Dans l'étape 3, vous avez associé l'accès au conteneur à un mot de passe. Ce dernier est plus facilement vulnérable (exemple de BrutForce ou Keylogger,....)

Avec VeraCrypt, une utilisation plus sécurisée est possible. L'accès à une donnée confidentielle n'est plus dépendant de *ce que je sais*, mais **aussi** de *ce que je possède* : le keyfile

L'utilisation des keyfiles : c'est associer un fichier ou les fichier d'un répertoire (la clé) qui vous donnera accès au volume crypté à la condition initiale que le mot de passe fourni soit le bon.

Le fichier peut-être aussi bien un mp3, qu'un avi, qu'un fichier word,... Il doit faire au moins 30 octets et **ne doit plus être modifié**.

Pour basculer d'u simple « mot de passe » au mode « mot de passe + keyfile »

– Ouvrez l'interface VeraCrypt (ne montez pas le volume)

Cliquez sur Outils pour le Volume (ou dans le menu Volume / Modifier le mot de passe du volume)



Choisissez Change Volume Password...

ctuel		
Mot de passe :		OK
Hot de passe i		Annuler
PKCS-5 PRF	Auto détection 🔹 🦳 Mode TrueCrypt	
	Fichiers dés	
	Afficher mot de passe	
ouveau		
Mot de passe :		
Confirmer :		
	Fichiers dés	
	Afficher mot de passe	
PKCS-5 PRF:	Inchangé 🔹	
	Inchange	

- Dans la zone Actuel, saisissez votre mot de passe actuel
- Dans la zone Nouveau, saisissez avec confirmation votre nouveau mot de passe, puis
- Cliquez sur le bouton Fichiers clés
- Sélectionner le fichier (ou le répertoire) qui vous servira de clé

VeraCrypt - Fichiers clés	×
Fichier dé	ОК
E:\temp\drone\MOVI0010.avi	Annuler
	AVERTISSEMENT : Si vous perdez un fichier dé ou si tout bit de ses 1024 premiers kilooctets change, il sera impossible de monter les volumes utilisant ce fichier dé !
Ajouter fichiers Ajouter un chemin Add Token Files Supprimer	Tout supprimer
Tout type de fichier (par exemple .mp3, .jpg, .zip, .avi) peut être utilisé en tant q VeraCrypt. Notez que VeraCrypt ne modifie jamais le contenu du fichier clé. Vous sélectionner plus d'un fichier clé (l'ordre n'a pas d'importance). Si vous ajoutez un fichiers non cachés trouvés dans le dossier seront utilisés en tant que fichiers clés Token Files" pour sélectionner des fichiers clés stockés sur des jetons de sécurit	ue fichier clé pouvez dossier, tous les . Cliquez sur "Add té ou cartes à puce
✓ Fichiers dés Plus d'infos sur les fichiers dés Générer aléatoire	ement un fichier dé

Le fichier sélectionné ne sera pas modifié.

Actuel		OK
Mot de passe :	•••••	
PKCS-5 PRF :	Auto détection 🔹 🗖 Mode TrueCrypt	Annuler
	Fichiers dés	
	Afficher mot de passe	
Nouveau Mot de passe :	•••••	
Confirmer :	•••••	
	✓ Fichiers dés Fichiers dés ■ Afficher mot de passe	
PKCS-5 PRF:	Inchangé 🔻	
Mode de nettovage :	3 passages (US DoD 5220.2 V	

-Validez.

VeraCry	eraCrypt - Random Pool Enrichment						X												
IMPO you n 'Cont	IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases security. When done, click 'Continue'.																		
1	Mélange PRF : SHA-512 Afficher le nombre aléatoire																		
Rése	rve	de no	ombr	es a	léato	oires													
AA	3B	AA	0A	EC	5B	95	7A	28	E2	68	0C	1D	19	5F	8E	FC	5B	D7	25
9F	02	D8	D3	1F	7F	44	C3	7D	71	16	0B	14	C2	10	60	5F	77	3F	86
4D	1D	B8	59	15	C3	C5	73	11	59	Α2	86	69	09	BC	AA	0C	CB	5B	81
9A	7E	E6	77	72	FE	85	2A	FD	DF	05	22	E1	85	2F	2C	3C	3C	25	1D
94	E3	26	82	C5	83	E2	50	75	43	80	89	6A DE	B4	E6	31	E3	CF	AE	5B
01	46	E4	51	CF	19	14	AA	CD	E0 CD	50	41	DE	34	27	EE	23	50	27	01
47	58	25	46	14	55	36	5B	AD SF	45	CA	13	20	15	91	96	SF	20	60	27
29	04	60	5D	DD	5E	59	55	95	09	E8	02	76	8D	A6	B1	17	3D	6C	33
E8	5D	12	25	0B	27	ED	E7	1F	A9	FC	B9	2D	55	BB	34	42	BD	6E	D6
F1	64	A6	3B	18	79	E0	0C	9B	99	5E	CD	53	72	DE	D3	AA	DB	61	2C
87	Α2	DD	30	67	EE	5F	EE	33	E1	B7	8C	C8	СВ	9A	CA	E4	70	4A	D1
D3	31	2A	69	F7	FF	4F	52	2C	43	17	D4	3D	47	73	02	2A	1B	Α9	5E
DD	1B	97	43	26	41	04	92	B1	05	3A	78	C1	C2	86	4F	D8	6C	0B	77
40	9F	BA	3A	05	7F	E6	31	36	8D	54	27	53	1B	90	19	4A	68	25	61
90	F5	D8	97	3D	AO	3B	28	04	C2	B1	6F	8F	81	FF	48	E5	CD	91	80
							F	-	Con	tinue									
								_	2011	ande									
		_	_	_	_	_			_	_	-	-	_				-		

Bougez votre souris de manière aléatoire.

VeraCrypt	
1	Password and/or keyfile(s) successfully changed. IMPORTANT: Please make sure you have read the section 'Changing Passwords and Keyfiles' in the chapter 'Security Requirements and Precautions' in the VeraCrypt User Guide.
	ОК

Et c'est tout.

Pour monter le volume crypté, il vous restera à spécifier le fichier clé et le mot de passe comme auparavant.

Pensez à sauvegardez votre fichier clé car il devient désormais une clé essentielle pour l'ouverture de votre conteneur (ainsi que votre mot de passe).

8 – Cryptage du volume contenant le Système d'Exploitation

Plus délicat maintenant mais tellement plus efficace, la mise en place du cryptage au niveau du volume complet où se trouve le système d'exploitation.

Autrement dit, le système démarre au sein d'un conteneur chiffré.

Pour commencer, il faut avoir son OS et VeraCrypt installés normalement.

1 – aller ensuite dans le menu Système / Chiffrer la partition/le disque système...

Choisir « Normal »

Assistant de création de volume VeraC	rypt
	 Type du chiffrement du système Normal Choisir cette option si vous voulez simplement chiffrer la partition système ou l'intégralité du disque système. Caché It may happen that you are forced by somebody to decrypt the operating system. There are many situations where you cannot refuse to do so (for example, due to extortion). If you select this option, you will create a hidden operating system whose existence should be impossible to prove (provided that certain
VERA C	guidelines are followed). Thus, you will not have to decrypt or reveal the password to the hidden operating system. For a detailed explanation, please click the link below. <u>Plus d'infos</u> <u>Aide</u> < Précédent <u>Suivant ></u> <u>Annuler</u>

– Dans le choix suivant, soit vous décidez de crypter le volume système seulement, à l'exception de toutes les autres partitions présentes, soit « Chiffrer l'intégralité du disque », soit de « Chiffrer la partition système Windows ». Dans le premier cas vous décidez (et c'est sans doute le meilleur choix) de chiffrer le volume système et TOUTES les partitions présentes sur le disque physique ; dans ce dernier cas, un chargeur VeraCrypt sera installé : à chaque boot du système, le chargeur vous demandera le mot de passe Veracrypt et la séquence de boot système pourra démarrer ensuite.



Attention, si vous avez choisi l'option « Chiffrer l'intégralité du disque », VeraCrypt va alors crypter TOUS les volumes du disque physique, y compris les volumes contenant des utilitaires ou boot spécifiques ou systèmes de restauration etc... Donc si pensez être dans cette situation (vérifier avec les DiskManager de Windows), choisissez Yes. Veracrypt va alors détecter ces volumes spécifiques et les exclure.

VERA CRYPT	Chiffrement de la zone protégée hôte Oui Non A la fin de nombreux disques, il y a une zone qui est normalement cachée du système d'exploitation (de telles zones sont généralement appelées 'Zones protégées hôtes' - Host Protected Area). Cependant certains programmes peuvent lire et écrire des données dans ces zones. AVERTISSEMENT : Certains constructeurs d'ordinateurs peuvent utiliser à dessein ces zones pour y stocker des outils et des données pour le RAID, des outils de récupération système, des outils de diagnostic, etc. Si de tels outils ou si des données doivent être accessibles avant l'amorçage, la zone cachée ne doit PAS être chiffrée (choisir 'Non' ci-dessus). Voulez-vous que VeraCrypt détecte et chiffre un telle zone cachée
	Aide < Précédent Suivant > Annuler

Dans le cas d'un volume sur un disque virtuel, sur certains portables également, on pourra choisir No.

L'écran suivant permet de spécifier si le module de boot doit intégrer la présence de 1 ou plusieurs

OS déjà installés en multi-boot.



Étapes suivantes, choisissez l'algorithme de cryptage :

Assistant de création de volume VeraCŋ	ypt
	Options de chiffrement Algorithme de chiffrement
	AES Tester
RYPT	Algorithme cryptographique (Rijndael, publié en 1998) approuvé par la FIPS, qui peut être utilisé par les agences/départements fédéraux américains pour protéger cryptographiquement les informations sensibles. Clé à 256 bits, bloc de 128 bits, 14 rondes (AES-256). Le mode opératoire est XTS. <u>Plus d'infos sur AES</u> Benchmark
VERA C	Algorithme de hachage SHA-256 Infos : algorithmes de hachage
	Aide < Précédent Suivant > Annuler

Spécifiez votre mot de passe suffisamment robuste, c'est à dire 20car min avec une complexité habituelle (vous pouvez le tester ici : http://www.passwordmeter.com/)

Assistant de création de volume VeraC	Mot de passe
VERA CRYPT	Confirmer : •••••••• Fichiers dés Fichiers dés 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

Puis se démarre les séquences de génération de clés :

man		Collecte de données aléatoires														
		Nom	bre a	aléat	toire	actu	iel (u	ine p	artie	:)						
		BF	36	D7	DO	BB	BF	BA	35	31	D3	D6	3B	DA	B7	DA
		C2	C9	8E	1F	F7	A9	92	15	CE	B6	EF	78	09	56	CO
		52	73	82	9D	35	88	F4	1A	80	2B	AC	DD	D3	65	25
		10	D1	29	BA	2C	58	OF	05	7D	36	F3	33	DE	E6	D9
annannan del 1		38	07	D1	70	9C	A4	73	D4	03	E9	8D	C7	88	54	77
and the second se		6E	A2	84	B8	FC	86	F8	1E	D2	AE	71	OD	CD	E6	9E
		96	DD	76	89	F8	F9	82	82	50	8B	1D	7B	6C	6C	92
	F	DO	OF	90	32	88	91	AA	56	EC	AA	A6	D4	B6	AO	E6
	VERA CRI	☑ Af IMPOI aléato c'est. de chi	fiche RTAI birem Cela	NT : I ent acc ment	Dépl que roît s	ore a acez poss signif quez	iléati voti ible. ficati sur	oire re so Plus veme 'Suiv	ouris long ent la ant'	dans tem a for pour	s cet ps vo ce ci pou	te fe ous l rypta irsuiv	enêtr a boi ograf vre.	e au ugez ohiqu	ssi :, mie Je de	eux es dés
			,	Aide) [< P	récé	dent		Suiv	ant	>		An	nuler



L'étape suivant consiste à créer un fichier ISO de secours – passage obligatoire.

Assistant de création de volume VeraC	Disque de secours Before you can encrypt the partition/drive, you must create a VeraCrypt Rescue Disk (TRD), which serves the following purposes: - If the VeraCrypt Boot Loader, master key, or other critical data gets damaged, the TRD allows you to restore it (note, however, that you will still have to enter the correct password then). - If Windows gets damaged and cannot start, the TRD allows you to permanently decrypt the partition/drive before Windows starts. - The TRD will contain a backup of the present content of the first drive track (which typically contains a system loader or boot manager) and will allow you to restore it if necessary. The VeraCrypt Rescue Disk ISO image will be created in the location specified below.
VERA C	The VeraCrypt Rescue Disk ISO image will be created in the location specified below. C:\Users\olivier\Documents\VeraCrypt Rescue Dis Parcourir Aide < Précédent

Ce fichier est stocké sur un autre CD ou DVD.

Il vous permettre de booter votre système, de déchiffrer votre partition et contient une sauvegarde des premiers secteurs de boot. Veracrypt vous invitera d'ailleurs à le graver sur un CD ou DVD immédiatement : condition nécessaire pour pouvoir lancer le cryptage de la ou des partitions.



Une fois, le CD gravé, vous devrez vérifier la bonne issue de l'opération.

Assistant de création de volume Vera	Disque de secours vérifié
VERA CRYPT	Le disque de secours de VeraCrypt a été vérifié avec succès. Enlevez-le du lecteur et stockez-le en lieu sûr. Cliquez 'Suivant' pour continuer.
	Aide < Précédent Suivant > Annuler

Dernière opération : VeraCrypt prévoit une passe simple ou complexe de nettoyage du volume afin de réduire toute récupération de donnée non chiffrée.

VERA CRYPT	Mode de Aucun (le plus rapide) Mode de Aucun (le plus rapide) Aucun (le plus rapide) On some types of s data, it may be pos techniques such as data that are overv 35-pass (random data) data that are overv 35-pass (Gutmann") when VeraCrypt initiany encrypts an unencrypted partuton or drive). According to some studies and governmental publications, recovery of overwritten data can be prevented (or made very difficult) by overwritting the data with pseudorandom and certain non-random data a certain number of times. Therefore, if you believe that an adversary might be able to use such techniques to recover the data you intend encrypt, you may want to select one of the wipe modes (existing data will NOT be lost). Note that wiping will NOT be performed after the partition/drive is encrypted. When the partition/drive is fully encrypted, no unencrypted data is written to it. Any data being written to it is first encrypted on the fly in memory and only then is the (encrypted) data written to the disk.
	Aide < Précédent Suivant > Annuler

Ensuite, VeraCrypt fera un premier test de chiffrement du système (au prochain reboot) :

Assistant de création de volume Vera	Crypt
. inining the second second	Pré-test du chiffrement système
	Avant de chiffrer votre partition ou votre disque système, VeraCrypt doit vérifier que tout fonctionne correctement.
RYPT	Après avoir cliqué sur 'Test', tous les composants nécessaires (par exemple, le composant d'indentification du pré-amorçage, c'est-à-dire le chargeur d'amorçage de VeraCrypt) seront installés et votre ordinateur redémarrera. Vous devrez ensuite saisir le mot de passe dans l'écran du chargeur d'amorçage de VeraCrypt qui apparaîtra avant que Windows ne démarre. Après le démarrage de Windows, vous serez automatiquement informé des résultats du pré-test. Le périphérique suivant sera modifié : Disque #0
VERA C	Si vous cliquez sur 'Annuler' maintenant, rien ne sera installé et les pré-tests ne seront pas effectués.
	Aide < Précédent Test Annuler

Un dernier click : le reboot de votre système est lancé

Au boot du système, VeraCrypt vous demandera votre mot de passe :



Il suffit de le saisir, et Windows démarrera (pour faire un premier test de boot).

Après ce premier reboot, VeraCrypt doit valider que le prétest est OK puis vous proposera de lancer le cryptage final des partitions.

Assistant de création de volume VeraCr	ypt
VERA CRYPT	Pré-test terminé The pretest has been successfully completed. WARNING: Please note that if power supply is suddenly interrupted while encrypting existing data in place, or when the operating system crashes due to a software error or hardware malfunction while VeraCrypt is encrypting existing data in place, portions of the data will be corrupted or lost. Therefore, before you start encrypting, please make sure that you have backup copies of the files you want to encrypt. If you do not, please back up the files now (you can click Defer, back up the files, then run VeraCrypt again anytime, and select 'System' > 'Resume Interrupted Process' to start encrypting). When ready, dick Encrypt to start encrypting.
	Aide Précédent Qhiffrer Différer

Appuyez juste sur « Chiffrer » et c'est parti pour le chiffrement des partitions.

Ci-dessous une progression ; environ 25 minutes pour 30 Go.

as Assistant de création de volume VeraCrypt		
VERA CRYPT	Options Mode de Aucun (le plus rapide) Fait à 1.265% État Chiffrement Reste 18 minutes You can dick Pause or Defer anytime to interrupt the process of encryption or decryption, exit this wizard, restart or shut down your computer, and then resume the process, which will continue from the point it was stopped. To prevent slowdown when the system or applications write or read data from the system drive, VeraCrypt automatically waits until the data is written or read (see Status above) and then automatically continues encrypting or decrypting. Plus d'infos	
	Aide < Précédent Chiffrer Différer	

A la fin :

Assistant d	e création de volume VeraCrypt
1	The system partition/drive has been successfully encrypted.
	Note: If there are non-system VeraCrypt volumes that you need to have mounted automatically every time Windows starts, you can set it up by mounting each of them and selecting 'Favorites' > 'Add Mounted Volume to System Favorites').
	ОК

Vos partitions sont chiffrées !

PS : si la partition est chiffrée, une fois l'OS démarré, les données sont bien entendues en clair accessible depuis l'explorateur, donc également à travers le réseau du PC...

9 - Crypter ET cacher sa partition (système) -

(partie non mise à jour pour VeraCrypt)

Cela peut s'avérer utile lorsque vous voyagez dans certains pays où on peut légalement vous demander votre portable à la douane : crypter un volume de données, ET le rendre non visible afin

de ne pas susciter d'attention particulière.

Cette méthode est sensiblement plus complexe que l'étape précédente.

Globalement cela consiste à mettre en œuvre un premier OS sur une partition cryptée dans lequel nous insérerons un second volume contenant l'OS final (et donc les données) crypté et caché. Le premier OS sera ensuite formaté et <u>vous devrez réinstaller un OS</u> sur cette première partition !



Voici ce à quoi va ressembler votre partitionnement final :

La partition 1 est celle qui reçoit l'OS crypté qui servira de leurre (c'est l'OS1).

La partition 2, juste après la partition 1 est celle qui reçoit l'OS crypté et caché (c'est l'OS2) : sa taille doit être de 2.1 fois la partition 1. La partition 2 doit être créée..

Sur l'OS1, vierge avec VeraCrypt installé :

1 - dans le menu Système, choisissez « Créer un systèmes d'exploitation caché»

📮 VeraCŋ	/pt	- • ×
Volumes	Système Favoris Outils Paramètres Aide	Site Web
Le E: F:	Chiffrer la partition/le disque système Déchiffrer définitivement la partition/le disque système Reprendre un processus interrompu	
	Créer un système d'exploitation caché	E
≡ I:	Créer un disque de secours Vérifier le disque de secours	
	Monter sans authentification lors du pré-amorçage	
	Modifier le mot de passe Paramétrer l'algorithme de dérivation de la clé d'en-tête	*
Cre	Propriétés Baramètres	er le cache
Volume	Parametres	
	▼ F ✓ Ne jamais enregistrer l'historique Outils pour le volume Périp	ichier
	Montage automatique Tout démonter	Quitter
VeraCrypt	×	
i	It may happen that you are forced by somebody to decrypt the operating system. There are many situations where you cannot refuse to do so (for example, due to extortion). Using this wizard, you can create a hidden operating system whose existence should be impossible to prove (provided that certain guidelines are followed). Thus, you will not have to decrypt or reveal the password for the hidden operating system.	
	ОК	

On vous prévient que vous DEVREZ réinstaller vos OS situé sur la première partition. Votre OS1 et le contenu entier de la partition 1 sera recopié sur la partition 2.



Dans la question suivante, VeraCrypt détecte que le fichier d'échange est sur votre partition system ce qui peut représenter le risque de dévoiler la présence de votre partition système cachée. Si vous répondez Yes, Veracrypt fera la modification nécessaire.

Assistant d	e création de volume VeraCrypt
<u>^</u>	There is/are paging file(s) on non-system partitions. Paging files may be located only on the system partition. Otherwise, plausible deniability of the hidden operating system might be adversely affected. Note: If an adversary analyzed the content of such files (residing on a non-system partition), he might find out that you used this wizard in the hidden-system-creation mode (which might indicate the existence of a hidden operating system on your computer). Also note that any such files stored on the system partition will be securely erased by VeraCrypt during the process of creation of the hidden operating system.
Do you want to configure Windows to create paging files only on the Windows partition now? Note that if you click 'Yes', the computer will be restarted. Then start VeraCrypt and try creating the hidden OS again.	
	Oui Non

Après le reboot éventuel pour suppression du Pagefile.sys, on peut relancer la séquence :



On vous rappelle que l'OS1 sera à réinstaller (donc supprimé)

Assistant d	e création de volume VeraCrypt
<u>^</u>	WARNING: During the process of creation of the hidden operating system, you will be required to fully reinstall the currently running system (in order to create a decoy system securely). Note: The currently running operating system and the entire content of the system partition will be copied to the hidden volume (in order to create the hidden system).
	Are you sure you will be able to install Windows using a Windows Setup medium (or using a service partition)?
	Oui Non

Attention, nombreux avertissements de sécurité qui visent à faire en sortie que l'usage d'un système crypté/caché reste « indétectable » : raison pour laquelle toute écriture en dehors de la partition 2 (typiquement sur la partition 1) ne sera pas possible.

Assistant de création de volume VeraCrypt		
	For security reasons, when a hidden operating system is running, local unencrypted filesystems and non-hidden VeraCrypt volumes are mounted as read-only (no data can be written to such filesystems or VeraCrypt volumes). Data is allowed to be written to any filesystem that resides within a hidden VeraCrypt volume (provided that the hidden volume is not located in a container stored on an unencrypted filesystem or on any other read-only filesystem). There are three main reasons why such countermeasures have been implemented: - It enables the creation of a secure platform for mounting of hidden VeraCrypt volumes. Note that we officially recommend that hidden volumes are mounted only when a hidden operating system is running. (For more information, see the subsection 'Security Requirements and Precautions Pertaining to Hidden Volumes' in the documentation.) - In some cases, it is possible to determine that, at a certain time, a particular filesystem was not mounted under (or that a particular instance of an operating system (e.g. by analyzing and comparing filesystem journals, file timestamps, application logs, error logs, etc). This might indicate that a hidden operating system is installed on the computer. The countermeasures prevent these issues. - It prevents data corruption and allows safe hibernation. When Windows resumes from hibernation, it assumes that all mounted filesystems are in the same state as when the system entered hibernation. VeraCrypt ensures this by write-protecting any filesystem accessible both from within the decoy and hidden systems. Without such protection, the filesystem could become corrupted when mounted by one system while the other system is hibernated.	
	ОК	

Page suivante : on retrouve l'installation du BootLoader qui sera adapté en fonction votre choix « avez-vous un seul OS ou bien avez-vous plusieurs OS distincts ? »

Assistant de création de volume Ver	aCrypt
minim	Nombre de système d'exploitation
	Amorçage Sélectionner cette option s'il n'y a qu'un seul système d'exploitation installé sur cette machine (même s'il y a plusieurs utilisateurs)
	Amorçage multiple Sélectionner cette option s'il y a au moins deux systèmes d'exploitation installés sur cet ordinateur.
A CRYP1	Par exemple : - Windows 2000 et Windows XP - Windows XP et Windows Vista - Windows et Mac OS X
VER	- Windows et Linux - Windows, Linux et Mac OS X
	Aide < Précédent Suivant > Annuler

Info importante : sous Windows, assurez-vous d'avoir activé votre système auprès de Microsoft avant de lancer la copie vers la Partition 2. Toujours pour éviter de faciliter la détection de l'existence de cet OS2...

Assistant d	le création de volume VeraCrypt
	For security reasons, if the currently running operating system requires activation, it must be activated before proceeding. Note that the hidden operating system will be created by copying the content of the system partition to a hidden volume (so if this operating system is not activated, the hidden operating system will not be activated either). For more information, see the section "Security Requirements and Precautions Pertaining to Hidden Volumes" in the VeraCrypt User's Guide. Important: Before proceeding, please make sure you have read the section "Security Requirements and Precautions Pertaining to Hidden Volumes" in the VeraCrypt User's Guide. Does the currently running operating system meet the above condition?
	Oui Non

Le « Volume de Chiffrement externe » sera par défaut, la totalité de votre partition 1 (officielle) et partition 2 (cachée).

Assistant de création de volume VeraCr	ypt
	Algorithme de chiffrement Algorithme de chiffrement AES Algorithme cryptographique (Rijndael, publié en 1998) approuvé par la FIPS, qui peut être utilisé par les agences/départements fédéraux américains pour protéger cryptographiquement les
RYPT	informations sensibles. Clé à 256 bits, bloc de 128 bits, 14 rondes (AES-256). Le mode opératoire est XTS. <u>Plus d'infos sur AES</u> Benchmark
VERA C	Algorithme de hachage SHA-512 Infos : algorithmes de hachage
	Aide < Précédent Suivant > Annuler

Assistant de création de volume VeraC	rypt
	Taille du volume externe
	30 No O Mo O GB Size of \Device\Harddisk0\Partition2 is 30.22 GB
VERA CRYPT	Le volume externe et le volume caché (contenant le système d'exploitation caché) résidera dans la partition ci-dessus. Ce devrait être la première partition qui suit la partition système. Vérifiez que la taille de la partition et que les chiffres affichés plus haut sont corrects et s'ils le sont, cliquez sur 'Suivant'.
	Aide < Précédent Suivant > Annuler

Spécifiez un mot de mot de passe spécifique pour l'accès à ce volume.

Assistant de création de volume VeraC	rypt
VERA CRYPT	Mot de passe du volume externe Mot de passe : Confirmer : Fichiers dés Fichiers dés Afficher mot de passe Choisissez un mot de passe pour le volume externe. Ce sera le mot de passe que vous pourrez divulguer à toute personne vous forçant à révéler le mot de passe de la première partition après la partition système, où résideront le volume externe et le volume caché (contenant le système d'exploitation caché). L'existence du volume caché restera secrète. Notez que ce mot de passe n'est pas pour le système d'exploitation leurre. IMPORTANT : Le mot de passe doit être différent de celui que vous choisirez pour le volume caché (i.e. pour le système d'exploitation caché).
	Aide < Précédent Suivant > Annuler

Rappel que tout ce qui se trouve sur votre seconde partition sera effacé.

		ÉCRASÉS ET PERDUS (ILS NE SERONT PAS CHIFFRÉS) ! Êtes-vous sûr de vouloir procéder au formatage ?
--	--	--

On lance le formatage de la partition dès que vous avez généré assez de mouvement aléatoire avec votre souris.

Assistant de création de volume VeraCry	/pt
VERA CRYPT	Options Système FAT Cluster Défaut Pormatage Nb aléatoire : 2826CBB864318D5219E47847D275377F Clé d'en-tête : 0CF8E674DF2CD6B646BAE0EFBC5B71AE Clé principale : A91D8C8FB31BB165332796EBA085E296 Image: Fait à 1.219% Vitesse 15.7 Mo/s Reste 32 minutes Cliquez sur 'Formater' pour créer le volume externe. Pour plus d'infos, consultez la documentation.
	Aide < Précédent Formater Annuler

Maintenant que le volume externe est créé est accessible (par d »faut monté sous Z:), on passe à la création du volume caché de la partition 2.

Assistant de création de volume VeraC	rypt
	Volume caché
	In the following steps, you will set the options and password for the hidden volume, which will contain the hidden operating system.
VERA CRYPT	Remark: The cluster bitmap of the outer volume has been scanned in order to determine the size of uninterrupted area of free space whose end is aligned with the end of the outer volume. This area will accommodate the hidden volume, so it limits its maximum possible size. The maximum possible size of the hidden volume has been determined and confirmed to be greater than the size of the system partition (which is required, because the entire content of the system partition will need to be copied to the hidden volume). This ensures that no data currently stored on the outer volume will be overwritten by data written to the area of the hidden volume.
	Aide < Précédent Suivant > Annuler

Attention : l'algorithme de cryptage de la partition 2 devra être le même que celui de la partition 1.



Spécifiez un mot de passe (un3ème) disctinct des 2 autres.

Assistant de création de volume	: VeraCr	Mot de pa Mot de passe : Confirmer :	sse du systèm	e d'exploitation
	VERA CRYPT	Choisissez un mo pour le volume ca bon mot de passa trouve dans un c mots). Il ne devr ne devrait pas ét combinaison de n caractères spécia choisir un mot de mieux). La longu	Fichiers dés t de passe pour le syst aché). Il est très import e. Vous devriez éviter c lictionnaire (ou une com ait pas contenir de nom tre facile à deviner. Un ninuscules et de majusc aux comme @ ^ = \$ * passe d'au moins 20 ca eur maximale est de 64	Fichiers dés ième d'exploitation caché (i.e. tant que vous choisissiez un d'utiliser un mot simple que l'on nbinaison de plusieurs de ces ns ou de dates de naissance. Il bon mot de passe est une cules, de chiffres et de + etc. Il est recommandé de aractères (le plus long, le caractères.
		Aide	<pre> < Précédent</pre>	Suivant > Annuler

Formattage de la partition 2.

Assistant de création de volume Vera	Crypt
	Options Système Aucun ♥ Cluster Défaut ♥ ✔ Formatage rapide Nb aléatoire : 5618D2D8B7DDE616F4B6414DD07623D2 ✔ Clé d'en-tête : 121E510620F65392AEAD27C4035CA251 Clé principale : FD20B4E01F42CB383DB08130DAAE9CE2
VERA CRYPT	Fait à 100% Vitesse 1.8 Go/s Reste 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 dés de chiffrement. Puis cliquez sur 'Formater' pour créer le volume.
	Aide < Précédent Formater Annuler

Reboot du système.



Saisissez le dernier mot de passe saisi (celui fourni pour la mise en œuvre du système caché)

L'opération de recopie du premier système vers le second système en version cachée commence. (clonage de la partition 1 vers Partition 2.)



Et là, il faut s'armer de patience....

VeraCrypt Boot Loader 1.0f-1

•••

Copying system to hidden volume. To abort, press Esc. Copying completed. Enter password for hidden system: -

Quand la copie est terminée, ressaisissez à nouveau votre mot de passe (le dernier créé, celui de votre partition cachée).

Votre système caché démarre.

A l'ouverture de session Windows, un nouvel avertissement fort sur les recommandations :

VeraCrypt



Ensuite démarre la procédure d'effacement de l'OS1 :

X



Assistant de création de volume VeraContraction de volume VeraContraction	rypt
VERA CRYPT	Original System Windows creates (typically, without your knowledge or consent) various log files, temporary files, etc., on the system partition. It also saves the content of RAM to hibernation and paging files located on the system partition. Therefore, if an adversary analyzed files stored on the partition where the original system (of which the hidden system is a clone) resides, he might find out, for example, that you used the VeraCrypt wizard in the hidden-system-creation mode (which might indicate the existence of a hidden operating system on your computer). To prevent such issues, VeraCrypt will, in the next steps, securely erase the entire content of the partition where the original system resides. Afterwards, in order to achieve plausible deniability, you will need to install a new system on the partition and encrypt it. Thus you will create the decoy system and the whole process of creation of the hidden operating system will be completed.
	Aide < Précédent Suivant > Différer

Une fois démarré, TrueCrypt va vous proposer d'effacer le plus efficacement possible le contenu de la partition 1.

Assistant de création de volume VeraCr	ypt
VERA CRYPT	Mode de 1-pass (random data) On some types of storage media, when data is overwritten with other data (e.g. when the data is erased), it may be possible to recover the overwritten data using techniques such as magnetic force microscopy. According to some studies and governmental publications, recovery of overwritten data can be prevented (or made very difficult) by overwritting the data with pseudorandom and certain non-random data a certain number of times. Therefore, if you believe that an adversary might be able to use such techniques to recover the data that is to be erased, you may want to select one of the multi-pass wipe modes. Note: The more wipe passes you use, the longer it takes to erase the data.
	Aide < Précédent Suivant > Annuler

Générer une clé supplémentaire aléatoire pour renforcer l'effacement :

Ver	aCry	pt -	Ran	don	n Po	ol E	nric	hme	nt										l	x
	IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases security. When done, click 'Continue'.																			
	Mélange PRF : SHA-512 Afficher le nombre aléatoire									oire										
ſ	Rése	rve (de no	ombr	es a	léato	oires													
	Α7	96	F5	3B	AC	CD	0A	DF	1A	80	74	BE	2D	92	74	13	DO	8B	85	7D
	F4	3E	1E	1E	2A	90	AO	D9	43	9A	2D	7 F	F5	15	BD	BA	91	3E	00	05
	BA	E3	6B	35	07	A1	43	24	07	7F	93	F7	C3	32	E8	54	2E	C4	C 8	64
	8E	66	7D	4C	3D	68	94	8D	34	69	B9	BF	81	16	2A	CD	C9	FE	FE	1A
	B4	5C	4B	91	D7	48	1D	43	F8	7D	46	8F	7B	61	81	00	D7	DC	9C	07
	Α4	DC	86	Α2	EE	78	15	90	C6	Β4	02	36	47	F3	B6	9F	1C	C9	7A	10
	75	C2	65	83	E1	74	04	F9	C8	5B	29	2B	52	D5	EΒ	5A	64	03	3F	59
	CD	BD	31	14	C7	DO	92	97	D7	Β4	5E	D1	6E	A1	85	46	AF	36	CC	8B
	9A	3D	C5	23	9C	B0	93	B0	DD	43	2F	38	99	BC	F0	FC	DC	3A	F7	A3
	1B	9B	77	2B	D8	E8	BA	6A	9D	Α5	15	47	44	EΒ	6B	36	1B	86	75	0E
	15	42	E7	D2	68	3E	0F	3C	39	F2	6D	06	E0	1E	74	2B	Α2	0B	0C	E7
	72	C4	50	Α9	3D	38	19	E8	87	8C	25	27	OF	4E	22	77	48	7A	BD	65
	82	52	66	99	32	FD	D5	CD	7D	C4	8A	62	9E	0E	A6	DC	64	2B	94	07
	D1	9A	B4	8E	A6	D9	E9	30	33	48	AF	58	ED	55	7F	60	AB	8D	1E	41
	96	F8	AF	53	8A	D9	2B	F8	00	81	cc	C8	A3	69	D9	45	24	ED	FC	E5
	E5	AB	0E	D5	42	E4	CF	25	66	22	1F	41	04	45	C3	F6	80	7B	81	DE
								ſ		Con	tinue	2								

Attention, toutes les données de la partition 1 seront effacées (sachant que c'est une copie de cette première partition qui actuellement sur la partition 2).

Assistant de création de volume VeraCr	ypt
VERA CRYPT	Wiping Options Mode de 1-pass (random data) Fait à 0.222% Reste 22 minutes Note: You can interrupt the process of wiping, shut down your computer, start the hidden system again and then resume the process (this wizard will be launched automatically). However, if you interrupt it, the entire process of wiping will have to start from the beginning.
	Aide Précédent Wipe Annuler

Quand c'est terminé :

Assistant o	de création de volume VeraCrypt	3
i	The content of the partition where the original system (of which the hidden system is a clone) resided has been successfully erased.	
	ОК	

Vous devez éteindre vos ordinateur (histoire de vider autant que possible toute rémanence de mémoire).

Redémarrez votre ordinateur et installez votre OS : ne bootez pas sur le disque contenant le système caché = donc démarrez sur votre média d'installation (DVD/USB/WDS).

... ... Installation de votre OS

Une fois votre OS installé, bien sûr vous ne pouvez plus booter sur votre système caché.

Installez VeraCrypt sur le système fraichement réinstallé et lancez la fonction de cryptage de votre

partition système (comme au chapitre 7 précédent), c'est-à-dire :

- menu Système / Chiffrer la partition, le disque système,
- Choisissez « Normal » et non « Caché »
- Choisissez « Chiffrer la partition Sysème Windows »
- Si votre PC n'a qu'un seul système (hors celui est caché), choisissez Amorçage (simple),

– Dans l'étape Options de Chiffrement : choisissez impérativement le même cryptage que celui utilisé pour votre système crypté ET caché.

Spécifiez un mot de passe (différent de celui qui vous permet de booter sur votre OS cyrpté et caché)

 Laissez VeraCrypt vous graver un CD de récupération d'urgence (si vous en avez déjà, mettez le CD pour que VeraCrypt en fasse la vérification)

- Sélectionnez le mode de nettoyage qui vous convienne,
- Lancez le pré-test de chiffrement du système => un reboot sera proposé.

- Au reboot, saissez votre password créé dernièrement (pas encore celui de la partition chiffrée/cachée)

– Lancement de votre OS crypté (non caché), VeraCrypt vous propose vous confirme que le prétest est terminé et lance le chiffrage de votre partition.

– Quand c'est terminé, rebootez votre OS.

Maintenant, le process est terminé :

- Au boot de votre PC, le loader VeraCrypt vous demande un mot de passe

VeraCrypt Boot Loader 1.0f-1 Keyboard Controls: [Esc] Boot Non-Hidden System (Boot Manager) Enter password for hidden system: *** -

Si vous mettez le password de votre partition système cryptée ET cachée, vous booterez sur cet OS (l'OS2).

Si vous mettez le password de votre partition système chiffrée (la partition leurre), vous booterez sur l'OS normal .

Le troisième password vous permet d'accès à la partition externe.

10 – Détecter la présence de Conteneurs TrueCrypt

(partie non mise à jour pour VeraCrypt)

Utiliser TrueCrypt est sans doute indispensable lorsqu'on manipule des données confidentielles mais lorsqu'il s'agit à l'inverse de détecter si une personne abuse utilise TrueCrypt. Il existe à minima quelques pistes, outils et traces laissées par TrueCrypt.

TCHunt (TC pour TrueCrypt et Hunt pour...) : cet outil permet de détecter les fichiers TrueCrypt sur un ordinateur, pas seulement si ils ont l'extension .TC => <u>http://16s.us/TCHunt</u> A cette heure, TCHunt ne détectait pas encore les partitions. La dernière version était la 1.6, voici son usage :

TCHUNT -d C:\temp -v

-d pour Detect

C:\temp ou autre répertoire

-v pour mode verbeux.

Si vous lancez cette commande (surtout à la racine d'une partition), tous les fichiers seront analysés à la chaine, avec un résultat difficile à exploiter.

Préférez alors : tchunt -d c:\ 2>nul

TChunt vous renverra alors les éventuels fichiers ayant 1 conteneur TrueCrypt.

Attention : TChunt permet de suspecter la présence d'un fichier TrueCrypt. Le taux de faux négatifs et faux positifs peut être déroutant.

Traces locales :

Dans le cadre de conteneurs cachés (de second niveau), il reste deux arguments systématiques pour détecter la présence de ces conteneurs : 1 – le conteneur premier ne pourra jamais contenir ou stocker la totalité de l'espace qui lui est alloué, 2 – les fichiers leurres du premier conteneur sont rarement mis à jour et donc souvent obsolètes.

Le système d'exploitation laisse apparaitre également la présence de fichiers tels que truecrypt (- x64).sys dans system32\drivers

Le registre laisse entrevoir quelques associations de fichiers : .TC par défaut

Etc ...