Mieux gérer sa vie privée via les outils informatiques

Par Greg Siebrand

Avertissement

Ce document est toujours en cours de réalisation. Les informations de certains chapitres ne sont pas encore totalement finalisées et peuvent être donc incomplètes. Rédigeant ce document sur mon temps libre, il sera complété au fur et à mesure et régulièrement mis à jour. Vous pourrez toujours trouver une version plus récente du document à l'adresse suivante :

http://www.antredugreg.be/votre-vie-privee/

Licences, droits d'auteurs et tout le bazar touchant à ce domaine

Table des matières

Introduction

Suite au scandale prisme, je voulais partager ce genre de petites informations qui peuvent vous faciliter la protection de votre vie privée sur internet et sur votre ordinateur.

Existe-t-il une solution ultime pour se protéger ? Je dirais non, à moins d'être totalement déconnecté et que toutes vos données soient enfermées dans une chambre forte. Pour moi la meilleure solution à la protection de sa vie privée est de s'auto-héberger pour tous les services à l'aide de logiciels libres. Malheureusement, ce système comporte beaucoup de contraintes : il faut non seulement de plus grandes connaissances en informatique que la majorité des internautes possède, mais également un ordinateur que l'on transformera en serveur et qui ne sera dédié qu'à cela, et le tout bien sûr dans le meilleur des mondes, où le matériel ne tombe jamais en panne.

Je ne vais pas me lancer dans des explications techniques sur la cryptographie et les méthodes de chiffrement. Je vais vous expliquer des moyens simples à mettre en œuvre chez vous, ainsi que divers programmes à utiliser.

Ce document sera divisé en trois partie : la première consiste à de bons usages sur internet, que ce soit les mots de passe, les questions secrètes,... La seconde sera un peu plus focalisée sur les réseaux sociaux. En troisième partie, je parlerai des programmes à utiliser sur votre ordinateur ainsi qu'un petit paragraphe sur le cryptage de vos e-mails avec PGP. Vous pourrez aussi consulter en annexe des techniques un peu plus compliquées.

Et sinon pour me présenter en quelques lignes: je m'appelle Greg, 33 ans, et père d'un petit garçon de 14 mois maintenant. Je suis passionné par les technologies informatiques dès l'âge de 8 ans et je n'ai plus quitté mon clavier depuis. Je dispose d'une certification du Linux Professionnal Institute ainsi que la Novell CLA11. Et si, bien sûr, vous avez des questions suite à la lecture de ce document, n'hésitez pas à me contacter que ce soit par mail ou les réseaux sociaux. Car j'en conviens, l'informatique évolue de plus en plus vite, et il se peut que certaines informations soient déjà obsolètes à l'heure où vous lirez ces lignes.

1.Premiers réflexes :

1.1 Les mots de passe

En faisant un peu de social engineering[1] auprès de mon entourage, on constate que la majorité des utilisateurs sur internet utilisent des mots de passe facilement crackables : en effet, ces derniers sont souvent des dates de naissance, mariages, ou simplement les noms de leurs enfants et autres évidences que l'on peut facilement trouver. Donc mon premier conseil à ce propos, est de bannir ce genre de pratique.

Ne pas également utiliser des mots du dictionnaire : il existe des logiciels qui vont tester les mots de passe en utilisant tous les mots du dictionnaire, et donc ceci est à proscrire également !

Le mieux est d'utiliser des mots de passe complexe, assez longs avec des majuscules, minuscules, chiffres et caractères spéciaux. Il devient dès lors beaucoup plus difficile de « cracker » le mot de passe, et ce même avec un logiciel. On peut également faire des phrases, histoire de garder un moyen mnémotechnique pour le retenir. Par exemple :

> Je mange une tartine

Et vous le transformez comme ceci :

> j3!m@Ng3-Un3_t@Rt1n3

Et bien sûr, le dernier conseil à vous donner en mot de passe est de ne pas vous limiter à un mot de passe ! La pratique idéale serait de créer un mot de passe différent pour chaque service que vous utilisez sur internet (et d'autres personnes de mon entourage préconisent également une adresse mail différente par service que vous utilisez : c'est plus contraignant, mais beaucoup plus sécurisé).

A noter qu'il existe aussi des générateurs de mot de passe, qui permet de générer aléatoirement ces derniers. Un petit exemple à cette adresse :

http://strongpasswordgenerator.com/

Vous pouvez aussi choisir 3 mots du dictionnaire que vous mettez aléatoirement.

Vous allez me dire que finalement, c'est impossible de retenir ce genre de mot de passe. Alors voici ma petite technique, qui ne me permet de n'en retenir qu'un seul alors que j'utilise des mots de passe différents sur chacun de mes services en ligne :

Je vais avoir besoin de deux choses : un simple fichier texte ainsi que le logiciel TrueCrypt, présenté plus loin. Dans le fichier texte je mets les logins et mot de passe de chacun des services utilisés, et

1 Définition wikipedia :L'ingénierie sociale (ou social engineering en anglais) est une forme d'acquisition déloyale d'information et d'escroquerie, utilisée en informatique pour obtenir d'autrui, un bien, un service ou des informations clefs. Cette pratique exploite les failles humaines et sociales de la structure cible, à laquelle est lié le système informatique visé. Utilisant ses connaissances, son charisme, l'imposture ou le culot, l'attaquant abuse de la confiance, de l'ignorance ou de la crédulité des personnes possédant ce qu'il tente d'obtenir.

ensuite je mets ce fichier dans un container TrueCrypt, dont moi seul ai l'accès. Le seul mot de passe à retenir est donc le mot de passe de ce fameux container.

1.2. Les questions secrètes

On voit encore régulièrement l'utilisation de questions secrètes en cas d'oubli de mot de passe, même si ce système à tendance à tout doucement disparaître au profit d'envoi de SMS. La pratique que je conseille est bien sûr, de ne pas répondre exactement à la question. Je vous donne un petit exemple :

Si la question est quel est le nom de mon professeur de première primaire ? Je ne ne répondrais pas Madame Machin, mais par exemple un autre nom du style Gérard Menfroy.

1.3 Un navigateur libre et ses ajouts indispensables

Ceci pourrait être mis dans la section logicielle, mais je vais déjà en toucher un petit mot ici. En effet, abandonnez votre navigateur propriétaire tel qu'Internet Explorer, Safari ou Google Chrome au profit d'un navigateur libre tel que FireFox. Je privilégie ce dernier car il y a derrière une forte communauté, et beaucoup d'efforts sont faits pour préserver un maximum la vie privée de ses utilisateurs.

Mais un navigateur tout seul n'est pas suffisant. En effet, pour Firefox (et la majorité des navigateurs actuels), il est possible d'installer des petits ajouts au programme afin de faire telle ou telle chose. Il existe pour moi deux extensions indispensables pour se protéger : DoNotTrackMe et Adblock. Je vous conseille la lecture de ce petit article de blog de mon crû, qui vous parle de tous ces petits ajouts et comment les installer, sur mon blog personnel[2]. Vous pouvez rajouter à ces ajouts l'extension lightbeam[3], qui permet de voir tous les services entrain de traquer votre activité sur le site internet que vous visitez.

1.4 Fuyez la technologie Flash !!!

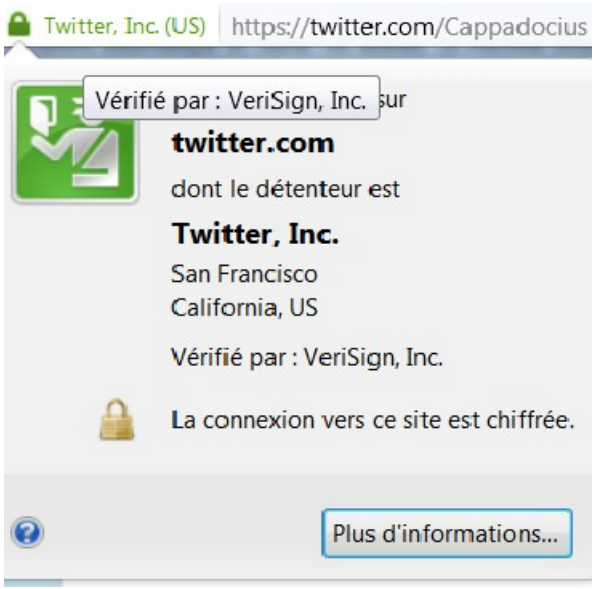
Tout site utilisant la technologie Flash est fermé, et donc il se pourrait qu'un programmeur malveillant ait mis une technologie permettant de renvoyer des informations de votre machine vers chez lui (un backdoor).

1.5 Https :

Utilisez les versions https des sites quand elles sont disponibles ! En effet, le https permet en réalité à ce que la communication entre votre ordinateur et le site que vous visitez soit sécurisée. Vous pouvez toujours en cas de doute sur le site que vous consultez, regarder qui est le propriétaire du site internet en cliquant sur le petit cadenas de la barre d'adresse de votre navigateur. Car en réalité, non seulement la communication est cryptée entre votre ordinateur et le site que vous visitez, mais la force de ce système est qu'elle est basée sur des certificats qui sont vérifiés par ce qu'on appelle une autorité de certification : je vais prendre l'exemple de Twitter pour vous expliquer comment ça fonctionne.

2 http://www.antredugreg.be/des-ajouts-indispensables-a-votre-navigateur-pour-proteger-votre-vie-privee/
3 http://www.mozilla.org/fr/lightbeam/

Twitter pour son site internet a émis un certificat, afin de faire fonctionner le protocole https. Il a donc demandé une autorité de certification, en l'occurrence Verisign, de vérifier qu'il est bien le propriétaire légitime du site twitter.com. Verisign, une fois qu'il a fait toutes ces vérifications, envoie un certificat signé, qui prouve bien que la société twitter est bien propriétaire de twitter.com. Vous pouvez toujours vérifier, comme expliqué un peu plus haut, la provenance du certificat, en cliquant simplement sur le petit cadenas dans la barre d'adresse de votre navigateur. Le résultat devrait donner ceci :



Vous apercevez bien sur l'image que vous êtes sur twitter.com, appartenant à la compagnie Twitter, et vérifié par la société Verisign.

1.6 Les moteurs de recherche :

Étant donné que Google enregistre toutes les requêtes que vous faites via son moteur de recherche, le mieux est d'utiliser un autre moteur, beaucoup plus respectueux de votre vie privée. Pour n'en citer qu'un, je vous propose DuckDuck GO, qui est d'ailleurs proposé comme moteur de recherche par défaut avec le logiciel TOR, détaillé un peu plus loin.

https://duckduckgo.com/

De plus, duckduckgo dispose d'énormément de paramètres, que ce soit pour faire des recherches à travers d'autres moteurs (Google, Yahoo, Bing,...) mais également dispose d'options pour protéger sa vie privée à travers les recherches qu'on effectue.

1.7 Prudence avec les produits Apple et Android

Ceci est peut être moins flagrant avec le système android de Google, mais soyez très prudent avec les smartphones et tablettes Apple. Le programme SIRI enregistre toutes vos interactions avec lui et stocke les données dans les data center de la firme à la pomme. De plus, vous ne possédez absolument pas le contrôle sur votre produit et ce pour deux raisons : La première est qu'Apple a

déposé une technologie permettant de bloquer certaines fonctionnalités de votre appareil quand ça lui chante[4]. De plus, jailbreaker[5] un appareil peut être passible de prison aux Etats-Unis[6].

Pour les produits Android, c'est quelque peu la même chose. Pour être sûr d'être tranquille, n'hésitez pas à « libérer » votre appareil en mettant une version modifiée de l'appareil, telle que Cyanogenmod. Mais attention, vous risquez de perdre la garantie de votre appareil en mettant une version modifiée.

Pour Android, il existe également des solutions logicielles libres (voir mes explications sur ce que c'est dans le chapitre suivant) et je vous invite fortement à découvrir le site internet http://fsfe.org/campaigns/android/android.html tout comme le site F-Droid[7], qui est un équivalent au google play store, et ne contenant que des logiciels libres. Malheureusement, n'ayant plus d'appareil mobile à la pomme depuis belle lurette, je ne saurais vous dire si de tels équivalents existent pour ces derniers, mais à mon avis cela devrait être le cas. Par ailleurs, il a été reporté que Google enregistre bien tous vos déplacements via les appareils Android, mais cette option est désactivable facilement.

1.8 Technologies sans fils

Lorsque vous n'en avez pas besoin, désactivez systématiquement les technologies sans fils de votre appareil mobile (je parle ici du WI-FI, Bluetooth et GPS). Je reviendrai un peu plus tard sur la géolocalisation dans la partie sur les réseaux sociaux. Laisser tous ces systèmes ouverts revient plus ou moins à dire : « rentrez, la porte est ouverte ! » De nombreux outils existent pour « sniffer » les appareils dont les connexions sont ouvertes et donc peut inciter une personne malveillante à s'introduire dans votre appareil. De plus, en coupant constamment les connexions que vous n'utilisez pas, vous aidez à ce que votre batterie se décharge moins vite, ce qui n'est pas non plus, négligeable, ces appareils étant extrêmement énergivores.

1.9 Historiques et caches

Nettoyez régulièrement l'historique ainsi que le cache de votre navigateur internet. Lorsque vous surfez sur la toile, une multitude de données s'enregistre dans votre ordinateur : les sites que vous avez visité, les documents que vous avez téléchargé sont gardés en mémoire par votre navigateur. Il est donc impératif que ce ce dernier oublie régulièrement ce que vous avez fait. Par ailleurs, chaque fois que vous naviguez sur internet, vous chargez sur votre ordinateur tout ce qui est contenu dans une page, et ce afin que le navigateur évite de re-télécharger des données lorsque vous revisitez ce site (c'est ce qu'on appelle le cache). Donc, nettoyez le régulièrement également !

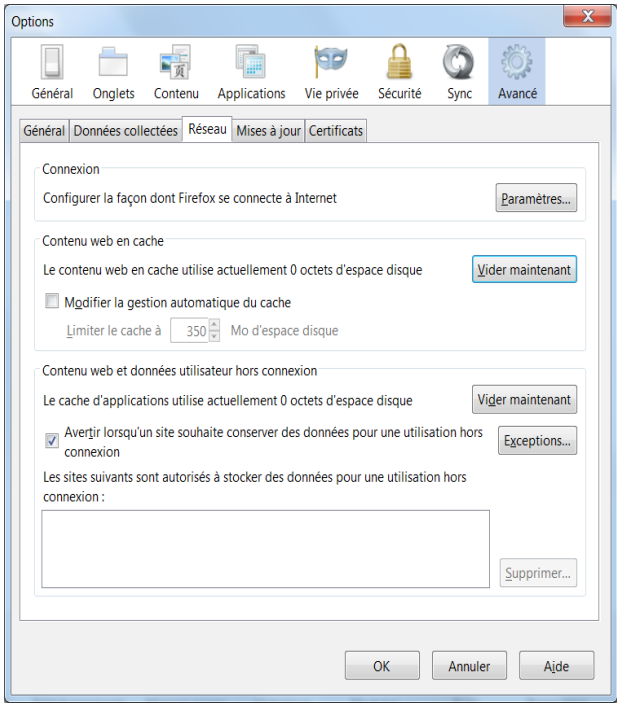
---

4 http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.htm&r=36&p=1&f=G&l=50&d=PTXT&S1=%2820120828.PD.+AND+Apple.ASNM.%29&OS=ISD/20120828+AND+AN/Apple&RS=%28ISD/20120828+AND+AN/Apple%29

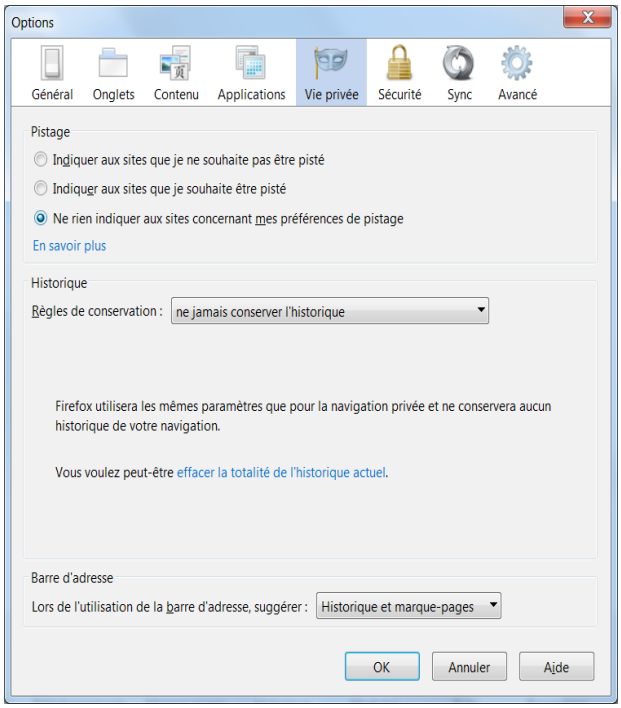
5 Définition wikipedia : Le jailbreak d'iOS également appelé débridage d'iOS, déverrouillage ou déplombage est un processus permettant aux appareils tournant sous le système d'exploitation mobile d'Apple iOS (tels que l'iPad, l'iPhone, l'iPod touch, et plus récemment, l'Apple TV) d'obtenir un accès complet pour déverrouiller toutes les fonctionnalités du système d'exploitation, éliminant ainsi les restrictions posées par Apple.

6 http://www.generation-nt.com/jailbreak-iphone-ipad-legalite-actualite-1646142.html

7 https://f-droid.org/



Le cache se vide via cette fenêtre



Et l'historique sur celle-ci

2.Utilisation des réseaux sociaux.

Attention, cette section est en cours d'écriture, et n'est donc pas encore complète ni détaillée.

Soyez prudent avec l'utilisation des réseaux sociaux ! Ces derniers sont une mine d'or que ce soit pour les agences de renseignements, les grandes compagnies de marketing et d'autres personnes malintentionnées. Voici mes quelques petits conseils :

1. Tout ce que vous postez est public

Le premier conseil que je donnerai, est selon moi, le plus important de tous. Gardez en tête que tout ce que tout élément que vous publierez sur un réseau social devient public. Même si vous cloisonnez correctement vos publications, que ce soit en paramétrant vos messages uniquement à votre cercle proche, la donnée que vous avez mise sur le réseau social ne vous appartient plus. Il existe cependant des réseaux sociaux nettement moins connus, qui sont libres au sens informatique du terme (voir le prochain chapitre sur les logiciels), et respectueux de votre privée[8].

2. Le moins d'informations personnelles possibles

-Dans le même genre, n'oubliez pas non plus qu'au moins d'informations personnelles vous mettez dans les réseaux sociaux, au mieux votre vie privée est protégée. Je dois dire que mon utilisation de ces derniers est majoritairement à vocation d'informations et de sensibilisation.

3. Cloisonnez vos publications.

Je ne vais pas vous donner un cours sur comment bien paramétrer vos publications par le reste du monde sur les réseaux sociaux, car je pense que ça ferait la taille d'un bon gros livre ! Au plus d'informations sont mises publiquement sur les réseaux sociaux, au plus on sait facilement les retrouver avec un moteur de recherche.

4. Ne jamais aimer une marque.

Premièrement, vous travaillez gratuitement pour cette dernière en leur faisant de la publicité. De plus, généralement il y a souvent des concours ou offres promotionnelles. Lisez bien les conditions générales d'utilisation de ces dernières, car souvent se cache derrière l'acceptation de se faire pourrir sa boite mail par la marque qui organise le concours. Et le plus important bien sûr, cela permet de mieux cerner toutes vos habitudes de consommation, et ceci est une mine d'or pour les « marketteurs » et agences de renseignements.

5. La géolocalisation.

La géolocalisation est un outil certes très pratique, néanmoins, elle comporte un grand danger pour votre privée. En utilisant des services tels que foursquare, vous indiquez au monde entier tout ce que vous faites. C'est encore une mine d'or pour tous les services de renseignements. Pensez également à la désactiver entièrement sur votre smartphone et de ne l'activer qu'en cas ou vous êtes réellement perdu et cherchez votre chemin ! (voir mon petit commentaire sur la géolocalisation dans le chapitre précédent, Premiers Réflexes.

8 http://www.antredugreg.be/et-si-vous-testiez-les-reseaux-sociaux-libres/

3.Logiciels

Je ne vais en toucher qu'un tout petit mot pour commencer, mais le premier principe est d'abandonner les systèmes d'exploitations propriétaires (Windows, Mac OS), pour des systèmes libres tels que GNU/Linux qui eux sont absents de backdoor[9]. Mais ce n'est néanmoins pas suffisant. Avant d'attaquer des logiciels bien particuliers, je vais toucher un petit mot sur les logiciels libres, ce que c'est, et pourquoi il est important d'utiliser ces logiciels plutôt que des logiciels que vous achetez ou téléchargez, et qui ne sont pas libres de droit.

Quelques mots sur le logiciel libre

Un logiciel libre, de base, est un logiciel qu'on peut acquérir librement et qu'on peut repartager sans restriction. Il y a quatre principes fondamentaux aux logiciels libres:

0. la liberté d'exécuter le programme, pour tous les usages ;
1. la liberté d'étudier le fonctionnement du programme et de l'adapter à ses besoins ;
2. la liberté de redistribuer des copies du programme (ce qui implique la possibilité aussi bien de donner que de vendre des copies) ;
3. la liberté d'améliorer le programme et de distribuer ces améliorations au public, pour en faire profiter toute la communauté.

Il va sans dire que vous avez donc accès au code source (le code du programme en lui-même) afin de pouvoir l'étudier ou le modifier par vous même. C'est totalement l'inverse des logiciels, dits propriétaires (celui que vous achetez en magasin). Si vous achetez un windows, un word, un photoshop,… vous êtes totalement contraint par le fabricant du dit logiciel et devez vous plier à ces propres désirs. De plus, vous n'avez aucun moyen de voir comment le programme propriétaire se comporte et s'il fait des choses dans votre dos (j'y reviendrai plus tard). Vous vous dites certainement en ayant lu ces lignes, que ça ne vous concerne pas trop, mais je vais maintenant souligner certains points, à mon sens éthiques, et démontrer les dérives que le logiciel propriétaire peut découler.

Les dérives et dangers des logiciels propriétaires

Je parle donc ici des logiciels que vous acquérez en magasin, et que pour pouvoir l'utiliser, vous devez accepter des conditions d'utilisation (qui font en moyenne une trentaine de pages) et qui bien sûr, ne sont jamais à votre avantage. Voici donc ces dérives en quelques points:

1. Vous payez pour vous cadenasser dans une certaine utilisation.

Comme je l'ai dit juste au-dessus, utiliser un logiciel propriétaire vous cloisonne dans une certaine utilisation. Vous ne pouvez pas faire ce que vous voulez avec le programme, vous devez faire comme le concepteur du programme a décidé. Bien sûr, le concepteur va mettre des nouveaux ajouts continuellement dans son programme et si vous voulez en profiter, il faudra de nouveau sortir son porte-monnaie. Un exemple flagrant me vient à l'esprit avec le logiciel word. Vous recevez un document word d'un ami,collègue,… qui dispose de la toute dernière version du logiciel. Et bien vous, qui disposez d'une version antérieure, ne savez

9 Définition de Wikipédia :Dans un logiciel, une porte dérobée (de l'anglais backdoor, littéralement porte de derrière) est une fonctionnalité inconnue de l'utilisateur légitime, qui donne un accès secret au logiciel.

absolument pas le lire! Afin de pouvoir lire le fichier correctement, il va vous falloir passer par la case achat de la nouvelle version.

2. Vous payer un logiciel propriétaire pour avoir le droit de vous taire.

C'est malheureusement bien le cas. Lorsque vous acquérez un logiciel propriétaire, vous devez vous plier aux exigences du concepteur sous toutes ses formes. Vous donnez directement votre accord lorsque vous lancez ou installez ce programme pour la première fois. En effet, vous devez accepter les conditions d'utilisation du programme afin de pouvoir l'exécuter. Si vous n'êtes pas d'accord et que vous refusez les termes du contrat, et bien vous avez juste dépensé de l'argent pour rien. En effet, il n'est plus rare maintenant que les revendeurs refusent de reprendre le logiciel, simplement parce que la boite est ouverte. Dans ces conditions d'utilisation, il n'est pas rare de voir que vous renoncez à différents droits. Par exemple, dans le cas d'Apple, vous ne pouvez utilisez un logiciel que sur du matériel agréé par cette dernière (et donc bien sûr, que sur leurs appareils). Dans le cas de Windows, vous acceptez également que vous pouvez payer le logiciel et que Microsoft s'en lave les mains si cela ne fonctionne pas sur votre matériel.

3. Souriez, vous êtes espionné!

L'affaire a été révélée au grand jour ce mois de juin par Edward Snowden avec PRISM. En effet, comme vous ne savez pas comment le logiciel se comporte et celui-ci peut donc renvoyer des informations ailleurs. On appelle ce type de fonctions un backdoor, ou en français un porte dérobée. Comme le code d'un programme d'un logiciel libre est accessible à tous, une faille éventuelle de ce type est rapidement corrigée.

4. La technologie acquise ne vous appartient pas.

Je vais prendre ici les cas d'Apple, avec ses smartphones et tablettes. Vous n'avez aucun contrôle sur votre appareil, Apple a inventé une technologie appelée « Kill Switch[10] » . Le Kill Switch permet à Apple (ou à la personne/organisation à qui il a vendu la technologie) de couper quand ça lui chante diverses fonctions de l'appareil sans votre accord, ou même d'éteindre complètement l'appareil. Alors, pourquoi acheter un appareil lorsque celui-ci ne fait pas ce que vous demandez?

Le Logiciel libre proprement dit

Voila, je vais encore toucher un petit mot ici. Sauter le pas n'est pas difficile. Commencez par des petits programmes, comme par exemple, votre navigateur internet. Passez sous Firefox ou Chromium. Pensez à remplacer votre suite par LibreOffice ou Apache OpenOffice. Car oui, avec le logiciel libre, vous avez le choix de vos outils! La liberté commence par avoir le choix de vos outils, et de plus, ces derniers savent lire et modifier le document quel que ce soit le programme de départ!

Le communautaire est notion essentielle dans le logiciel libre. Rien de mieux pour échanger des informations, s'entraider si on n'arrive pas à telle ou telle chose avec un logiciel,.. vous avez une communauté derrière vous!

Ce dernier argument montre aussi un autre point essentiel: la sécurité. Avec une communauté réactive, le libre accès au code source, les failles de sécurité du logiciel sont plus vites corrigées que celles d'un logiciel propriétaire. Et ce n'est absolument pas négligeable!

Equivalences programmes propriétaires/ logiciels libres

10 http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.htm&r=36&p=1&f=G&l=50&d=PTXT&S1=%2820120828.PD.+AND+Apple.ASNM.%29&OS=ISD/20120828+AND+AN/Apple&RS=%28ISD/20120828+AND+AN/Apple%29

Voici un petit tableau résumé des applications les plus courantes et leur équivalent libre :

Logiciel propriétaire	Logiciel libre
Internet Explorer, Safari, Chrome	Mozilla Firefox, Chromium
M$ Office	Open Office, Libre Office
Photoshop	The Gimp
3DS MAX	Blender
Skype	LinPhone, Jabber,...
Mail, Outlook, Incredimail, Livemail,...	Mozilla Thunderbird
Android Devices	Firefox OS of Cyanogenmod
IOS devices en Mac OS 10.7+	Je suis très triste pour vous !
Windows en Mac OS	GNU/Linux of FreeBSD (Vrije Unix)
Nero , cd burner	Inutile dans une distribution linux qui grave les disques comme un grand
Win Media Player, WinAmp,...	VLC

Logiciels bien spécifiques

Voici une liste non exhaustive de logiciels que vous pouvez facilement utiliser et que vous pouvez installer sur tout système d'exploitation (si vous ne savez pas vous passez de votre Windows). Je ne vais pas détailler comment installer un programme, et pour installer certains de ces logiciels sous Linux, il faudra vous référer aux documentations fournies sur le site web du logiciel. Dans le cas d'un Windows ou d'un Mac, il suffit d'installer le logiciel comme vous le feriez pour n'importe quel autre programme.

1.TOR

TOR est un programme qui permet de surfer en toute tranquillité, en passant par un réseau de serveurs qui cryptent chaque transaction (pour essayer d'expliquer simplement). Il permet donc à l'utilisateur d'être anonyme. Je vous conseille avant de l'utiliser de bien lire les avertissements et les pratiques liées à ce programme. Vous pouvez le télécharger à l'adresse suivante :

https://www.torproject.org/

Je vais détailler TOR avec le TOR software bundle, qui est un outil tout en main pour surfer. Pour certains services que vous utilisez sur internet, il est également possible de faire passer vos applications par ce système, et vous pourrez trouver plus de détails à cette adresse. TOR n'est pas très compliqué d'utilisation. Vous le lancez, et l'utilisez comme si vous étiez sur firefox. A noter qu'il y a plusieurs choses à savoir sur son emploi :

- Respectez les consignes des premiers réflexes : évitez les sites avec Flash, et évitez les extensions de navigateur qui peuvent récupérer votre emplacement de départ (votre adresse IP). De plus, gardez toujours en mémoire de favoriser les sites en HTTPS (pour tous ces conseils, reportez-vous au précédent chapitre sur les bons réflexes à avoir.
- Ne pas vous identifier sur des sites pouvant ruiner votre anonymat : vous connecter sur des sites tels que Facebook, votre site de banque en ligne,... ruinerait votre effort d'anonymat

étant donné que vous insérez sur ces sites des informations personnelles (votre localisation, adresse,etc...)

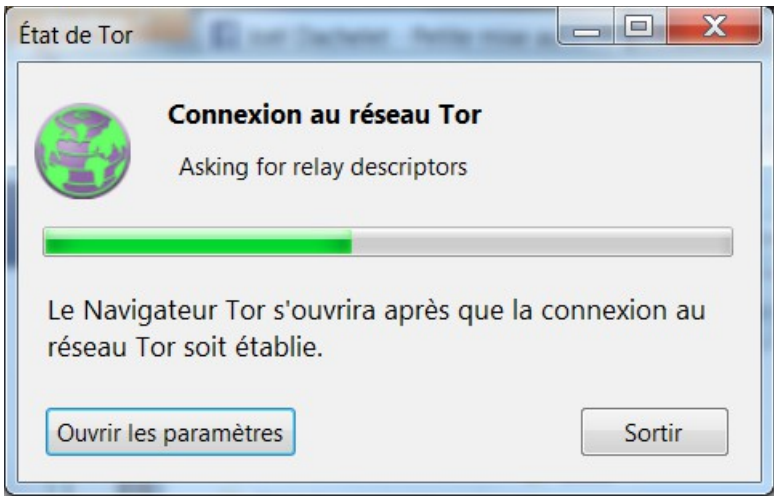
- Ne pas utiliser de Torrent avec TOR. De nouveau, les torrents permettent de se connecter à des des ordinateurs tiers, il y a donc un risque que l'ordinateur sur lequel vous vous connectez récupère votre adresse réelle, ce qui ruinerait également vos efforts d'anonymat.

Comment ça marche ?

Avant de commencer d'expliquer comment utiliser TOR, je vais tenter une explication sommaire de son fonctionnement. Lorsque vous êtes connecté à internet, vous disposez d'une adresse sur le réseau, un peu comme une adresse postale. En informatique, nous appelons cette adresse, adresse IP. Lorsque vous communiquez avec un site internet, vous donnez votre adresse IP à ce dernier, de manière à ce qu'il puisse vous répondre, lorsque vous lui demandez quelque chose. TOR est en fait tout un réseau d'ordinateur à travers le monde, dans lequel vous allez passer afin que le site internet que vous visitez n'ait pas votre adresse IP réelle. Chaque fois que vous passez dans TOR, à chaque passage par un des ordinateurs du réseau, que l'on appelle nœud, celui-ci rajoute une couche de cryptage supplémentaire, rendant la communication entre votre ordinateur et le site que vous visitez plus difficile à lire. A chaque couche rajoutée par un passage dans un nœud, vous devenez donc de plus en plus difficilement identifiable. C'est de cela que vient la signification de TOR (The Onion Router) : comme chaque passage dans un nœud rajoute une couche de cryptage, la communication ressemble à un oignon, caque couche de l'oignon étant une couche de cryptage.

Lancer TOR :

Une fois le programme installé, rendez vous à l'emplacement où vous avez demandé d'installer le programme et lancez-le. Vous devriez avoir une petite fenêtre de ce genre qui se lance :



Une fois cette opération terminée, un nouveau navigateur va se lancer. C'est en réalité une version de Firefox modifiée spécialement pour tourner avec TOR. Il se peut que vous ayez cette fenêtre au démarrage, si c'est le cas, n'hésitez pas à faire ce qui y est demandé ! Car un logiciel à jour est un logiciel moins vulnérable. A savoir aussi que si vous avez téléchargé la dernière version, vous risquez aussi d'avoir ce message, alors n'hésitez pas à vérifier la version affichée dans votre programme avec celle disponible sur le site de TOR. Si les deux numéros de version sont identiques, c'est que vous avez bien la dernière version sur votre ordinateur.

Maintenant, nous allons nous arrêter sur la barre d'outil de TOR. Bien qu'elle ressemble en tout point à celle de firefox, de nouveaux boutons sont apparus et vous pouvez donc jouer avec plusieurs paramètres.

Le bouton oignon : 

Ce petit bouton est le bouton principal, et qui nécessite le plus d'explications. Il est la pièce maîtresse du programme. L'option qui doit retenir toute notre attention est la **Nouvelle identité** : Cette option vous permet de vous refaire une autre identité sur internet. En réalité, votre navigateur va ouvrir une nouvelle fenêtre et passera par un autre chemin du réseau TOR. Vous pouvez faire le test à la maison :

1. Dans TOR, surfez sur whatismyipadress.com. Sur cette page, vous verrez que vous allez provenir d'une certaine région, avec une certaine adresse IP (voir mes explications sur les adresses IP)
2. cliquez maintenant sur nouvelle identité. Une nouvelle fenêtre va s'ouvrir, et répétez l'opération. Vous constatez directement que votre adresse IP, et éventuellement la région de sa provenance, a changé. Vous ne venez plus du même endroit !

Le bouton no script : 

Il se trouve juste à droite de l'icône du petit oignon. Ce bouton permet de désactiver l'éxécution d'un code Javascript fourni par le site internet que vous visitez. Pour ma part je le laisse activer, beaucoup de sites internet ne fonctionnant pas correctement sans l'utilisation de celui-ci.

Le bouton Https Everywhere : 

Https everywhere est une extension très utile également. Elle permet de, pour les sites qui le supportent, de faire une communicaton cryptée en https alors qu'elle ne se met pas en place par défaut. Par exemple, vous tapez sur votre ordinateur http://google.be, l'extension permettra d'aller automatiquement sur sa page sécurisée, à savoir https://google.be. La grande force est que

l'extension possède des tas de règles prédéfinies, mais vous pouvez en rajouter vous-même[11]. Vous trouvez ce bouton ainsi que ses options à droite de l'écran.

Voilà pour une prise en main rapide de TOR, mais sachez qu'il est possible d'installer uniquement TOR sans son navigateur internet, et de configurer tout comme bon vous semble. Vous pouvez toujours consulter la documentation de la communauté Ubuntu[12], qui est très bien détaillé à ce propos. Il doit cependant exister des tutoriels dans ce domaine pour Windows ou Mac, un peu de recherche sur le net devrait faire le bonheur de personnes un peu plus expérimentées.

2.Truecrypt

Truecrypt est un petit programme compatible tout système d'exploitation permettant de créer des disques durs et containers entièrement cryptés, que vous déverrouillez avec un mot de passe unique. Son utilisation est rapide à prendre en main. Vous pouvez le télécharger à l'adresse suivante :

http://www.truecrypt.org/

TrueCrypt est, par défaut, en anglais. Bien que j'utilise la version anglaise à la maison, il existe un moyen de le mettre en français, pour les utilisateurs de Windows. La traduction ne semble pas par contre, annoncée comme complète. Je conseille TrueCrypt aux autres méthodes de cryptage pour deux raisons : la première est que TrueCrypt est un logiciel libre, et en deuxième lieu, il fonctionne sur la majeure partie des systèmes (Windows, Linux, Mac,..) et les données sont donc facilement transportables d'un ordinateur à un autre, quelque soit le système d'exploitation.

Créer et utiliser un volume crypté:

Dans l'interface principale, cliquez sur Create Volume (créer un Volume). Vous allez avoir trois options qui s'offrent à vous :

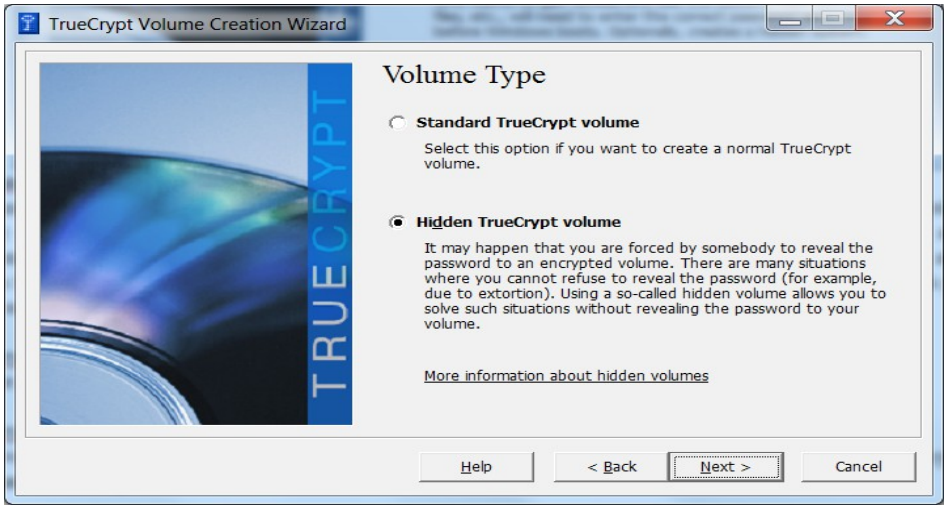
Create an encrypted file container :
Comme expliqué quelques lignes plus haut, True Crypt va en fait créer un dossier crypté où vous

11 https://www.eff.org/https-everywhere/rulesets (en anglais)
12 http://doc.ubuntu-fr.org/tor

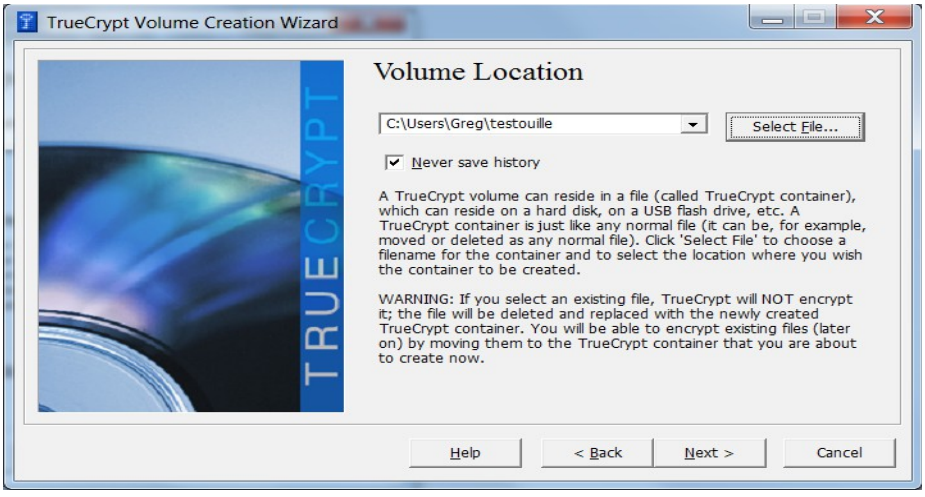
allez stocker tout sorte de données. Pour y accéder, il créera un lecteur virtuel, et on y accède comme si on accédait à une clé USB, disque dur,... Je m'attarderai sur la première option, afin de vous faire découvrir le programme, et une fois que vous aurez l'outil en main n'hésitez pas à passer aux suivantes.

Encrypt a non-system partition/Drive
Cette option sert à faire de même, mais à l'échelle d'un disque dur, d'une clé usb,...

Encrypt the system partition or entire system drive
Ici, vous cryptez votre système en entier. Vous devrez rentrer un mot de passe lorsque votre système démarrera lorsque vous allumerez votre ordinateur.

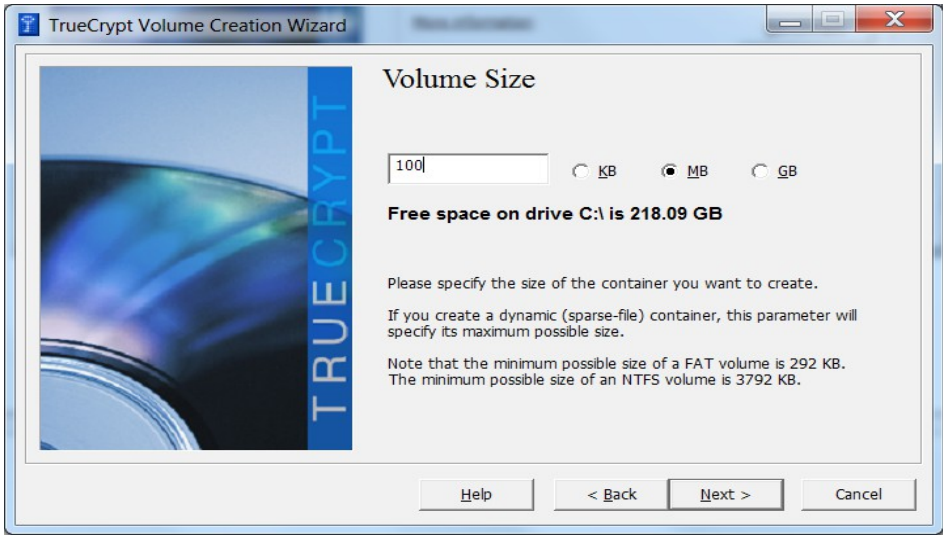


Ici, j'ai donc cliqué sur la première option, à savoir « Create an encrypted file container ». J'ai donc accès à deux options : le volume standard, ou le volume caché (Hidden). Ce dernier permet de faire un container caché dans un premier container. Personnellement je ne l'ai jamais utilisé, mais si vous possédez des données extrêmement sensibles, cela pourrait peut être vous être utile. Je vais rester sur la première option.



Ici, vous allez décider de l'emplacement ou vous allez stocker votre container. Par défaut, il se mettra dans votre dossier utilisateur. J'ai nommé mon fichier, pour l'exemple, testouille. A savoir que Truecrypt, si vous sélectionnez un de vos fichiers à ce moment du processus, le supprimera et créera un container crypté au nom de celui-ci.

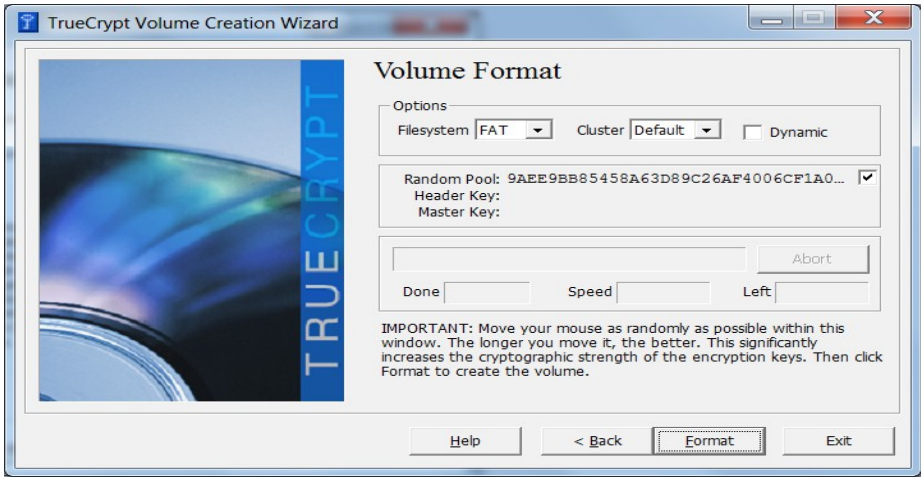
Nous en voici au choix de la méthode de cryptage. Je ne vais pas donner une explication détaillée sur les méthodes d'encryptage, mais si vous êtes intéressé par le sujet, pléthore de sites internet en parle, et vous pouvez déjà avoir un bref aperçu sur le site de TrueCrypt. Pour ma part j'utilise la méthode que vous voyez à l'écran qui crypte les données plusieurs fois avec plusieurs protocoles différents. De même, pour les algorithmes de hashage[13] (en gros cela permet de vérifier l'intégrité de votre fichier, par exemple si le hash ne correspond pas à ce qui est annoncé, c'est que le fichier a été modifié), j'utilise toujours SHA.



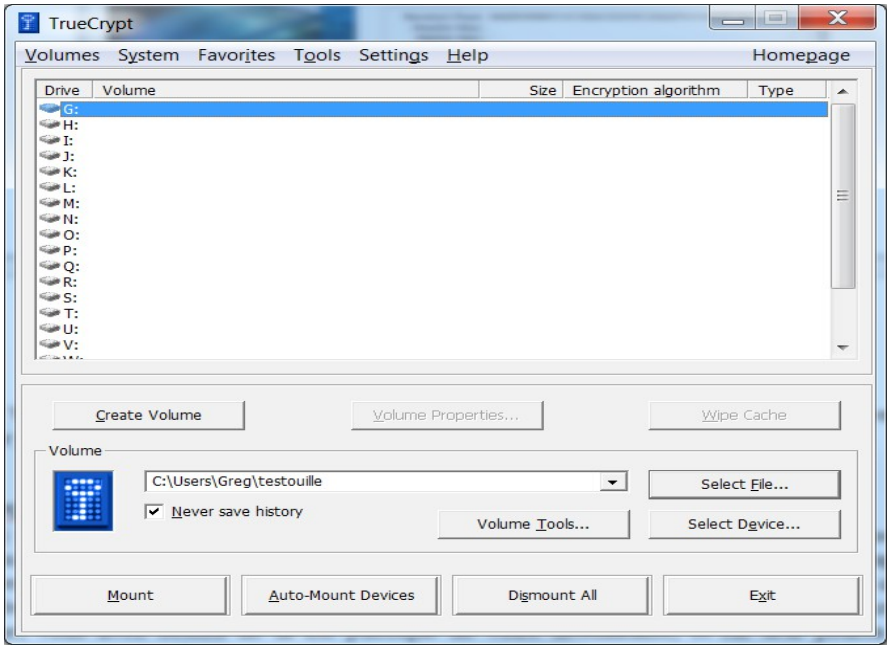
Cette étape-ci consiste à spécifier la tailler de votre dossier crypté. Dans l'exemple que vous voyez, je viens d'allouer 100 MO d'espace à mon dossier 'testouille'. Dans la capture d'écran suivante vous arrivez à l'étape du mot de passe. Ici, vous trouverez une option supplémentaire : use key file. Cette option permet en fait d'utiliser un fichier comme clé supplémentaire pour ouvrir votre container. Vous pouvez utiliser un fichier existant ou un créer un fichier aléatoire à cette fin. Mais attention, si vous supprimez ou perdez ce fichier, votre container ne sera plus utilisable, donc faites en une sauvegarde en lieu sûr !

13 http://fr.wikipedia.org/wiki/Fonction_de_hachage

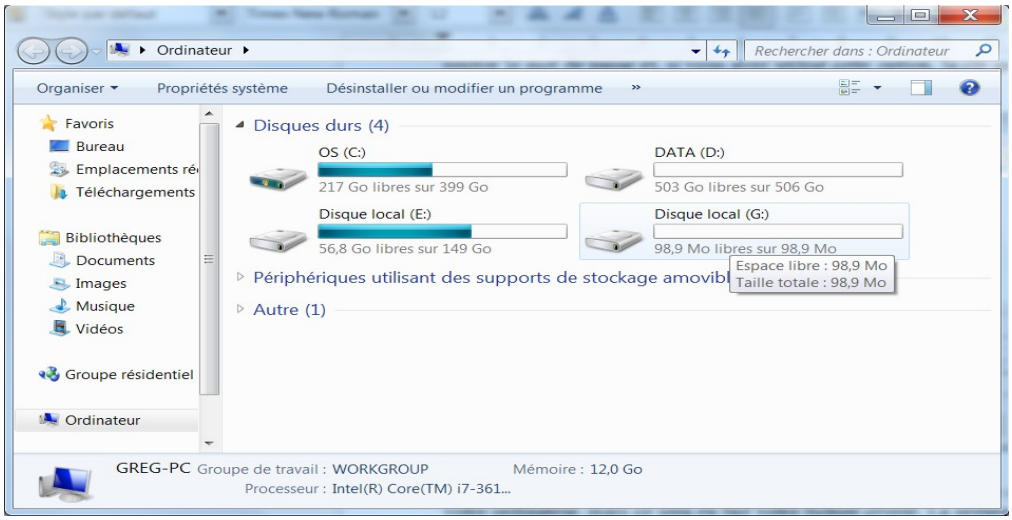
La dernière étape, avant la création de votre container, est de rajouter un peu d'entropie dans votre clé de cryptage. Pour se faire, sur la capture suivante, un endroit nommé 'random pool'. Passez dans cette zone avec votre souris, et vous verrez toute une série de chiffres et de lettre qui se mettront à changer. Cela permet de rajouter un peu d'aléatoire dans votre cryptage et donc rend votre dossier plus difficile à décrypter. Une fois que vous avez joué un peu avec, cliqué sur 'format' et le processus de création finalise votre dossier crypté !



Voilà ! Votre dossier est créé et prêt à être utilisé ! Nous allons donc maintenant l'activer afin de pouvoir y mettre des fichiers dedans. Dans la fenêtre d'accueil, Sélectionnez la première lettre de lecteur disponible, puis en bas sur select file. Dans la fenêtre qui s'ouvre, choisissez votre dossier crypté et puis une fois bien sélectionné, cliquez sur mount. La le programme vous demandera de rentrer le mot de passe et, si vous avez utilisé cette option, la clé que vous avez créée pour décrypter votre dossier. Votre dossier crypté est prêt l'emploi !



Pour votre ordinateur, le fait de cliquer sur ce bouton fera comme si vous branchiez une clé USB dans votre ordinateur, mais ce sera en fait votre fichier crypté. La preuve en image :



Comme la première lettre de lecteur dans TrueCrypt était G, mon dossier crypté s'est placé là. Je peux l'utiliser comme si c'était une clé USB normale ! Ensuite, quand vous avez fini de l'utiliser, il suffit de cliquer sur dismount, dans le programme (à la place du bouton mount, sur lequel vous avez cliqué pour monter votre dossier).

3.GnuPG

GnuPG est l'équivalent libre de PGP (Pretty Good Privacy) Il permet de chiffrer un message et d'être lu par le destinataire de votre choix à l'aide de clés. Pour expliquer de manière simple, vous disposer de deux clés : une privée, qui vous est personnelle et que vous avez besoin pour chiffrer et déchiffrer un message, et une clé publique que vous donnez à vos contacts. Lorsque vous cryptez un

message, vous avez besoin de la clé publique de votre destinataire, et lui seul pourra dès lors déchiffrer le message à l'aide de sa clé privée. Le parti pirate français a fait un excellent tutoriel que vous pouvez suivre pas à pas à l'adresse suivante :

http://wiki.partipirate.org/wiki/Tutoriel:PGP

Je ne vais pas expliquer en détail son fonctionnement dans ce document, car je trouve l'intérêt de ce système limité. Il est vrai que crypter un message peut être utile, mais ce système ne fonctionnerait correctement que si l'ensemble des internautes l'utilise, ce qui limite déjà fortement son utilisation, faute d'un grand nombre de personnes utilisant ce système. De plus, un autre problème notoire est que certaines données collectées par divers organismes rendent ce système caduque. En effet, seul le contenu de votre message est crypté, il est donc possible de retrouver des informations telles que les destinataires, destinateurs, le sujet du message ainsi que les heures et lieux d'envois.

4. Alternatives à Skype, Google Hangout, What'sapp...

Pour vos discussions instantanées, abandonnez les services comme Google Talk/Hangout ou skype. Il existe des multitudes de services libres, tels que Jabber. Par contre, recenser l'entièreté de ces services pourrait relever du parcours du combattant !

Je tiens néanmoins à relever certains projets, qui sont réellement dignes d'intérêt ! Tout d'abord, il y a n'importe quel serveur XMPP/Jabber[14] (et vous pouvez,si vous avez un minimum de connaissances en informatique, installer le vôtre), qui est le mastodonte de la messagerie instantanée libre. Il existe également Tox[15] qui remplace totalement les skype et consort, en proposant la vidéo en plus, et Linphone[16] si vous avez besoin d'un téléphone sur IP. Pour une alternative sécurisée au chats de type IRC, vous pouvez aussi essayer le projet cryptocat[17].

14 http://fr.wikipedia.org/wiki/Extensible_Messaging_and_Presence_Protocol
15 http://tox.im/
16 http://www.linphone.org/
17 https://crypto.cat/ ou mon article sur le sujet : http://www.antredugreg.be/discutez-en-toute-securite-avec-cryptocat/

ANNEXES

Ces annexes sont destinées aux plus paranoïaques ou aux personnes qui ont un bagage informatique un peu plus conséquent.

L'adresse MAC :

Vous pouvez également changer votre adresse MAC. Une adresse MAC est en réalité un identifiant unique attachée à une carte réseau. On peut donc avec un peu de recherche vous retrouver. Les manipulations que je vais vous montrer sont à faire à chaque démarrage de l'ordinateur, mais peuvent facilement être mise dans un script au démarrage de votre ordinateur. Pour Linux et Mac OS, vous devrez lancer un terminal :

Sous Linux

```
ifconfig eth0 down
ifconfig eth0 hw ether 01:FF:23:FF:45:FF
ifconfig eth0 up
```

-Explication à fournir sur les interfaces réseaus (à écrire)

Sous MAC OS

Le principe reste le même :

```
ifconfig en1 ether 01:FF:23:FF:45:FF
```

Sous Windows

Il existe un logiciel qui permet de changer son adresse MAC, mais personnellement, je ne l'ai pas testé :
http://www.softpedia.com/get/Network-Tools/Misc-Networking-Tools/Win7-MAC-Changer.shtml

Netfilter et fail2ban

Netfilter, faussement appelé iptables à cause de la commande qui permet de le gérer, est le firewall de Linux. Pensez par défaut à bloquer toutes les interactions sur ce dernier et de n'ouvrir que les ports dont vous ayez besoin. Rajoutez à ce dernier le petit programme fail2ban qui permet de bloquer les tentatives de connexions pendant un certain temps (que vous définissez vous même dans le fichier de configuration). Vous pouvez également changez les ports par défaut des logiciels que vous utilisez, et ce afin de rendre plus difficile les tentatives d'intrusion (par exemple en changeant le port de SSH qui est le port 22 par un port quelconque tel que 61329).

Les VPN

Au lieu d'utiliser TOR, vous pouvez aussi utiliser la technologie VPN (Virtual Private Network, ou réseau privé virtuel). Bien qu'il existe de nombreux VPNS gratuits, si vous possédez un serveur quelque part, vous pouvez toujours installer Open VPN dessus. Le trafic entre votre machine et le serveur abritant le VPN sera aussi entièrement crypté. N'ayant pas réinstallé Open VPN depuis un petit temps, je ne couvrirai pas son installation tout de suite, mais je pense le faire sous peu, afin de

vous montrer comment ça fonctionne. Vous pouvez déjà consulter le site d'Open VPN[18] pour plus de renseignements.

SSH

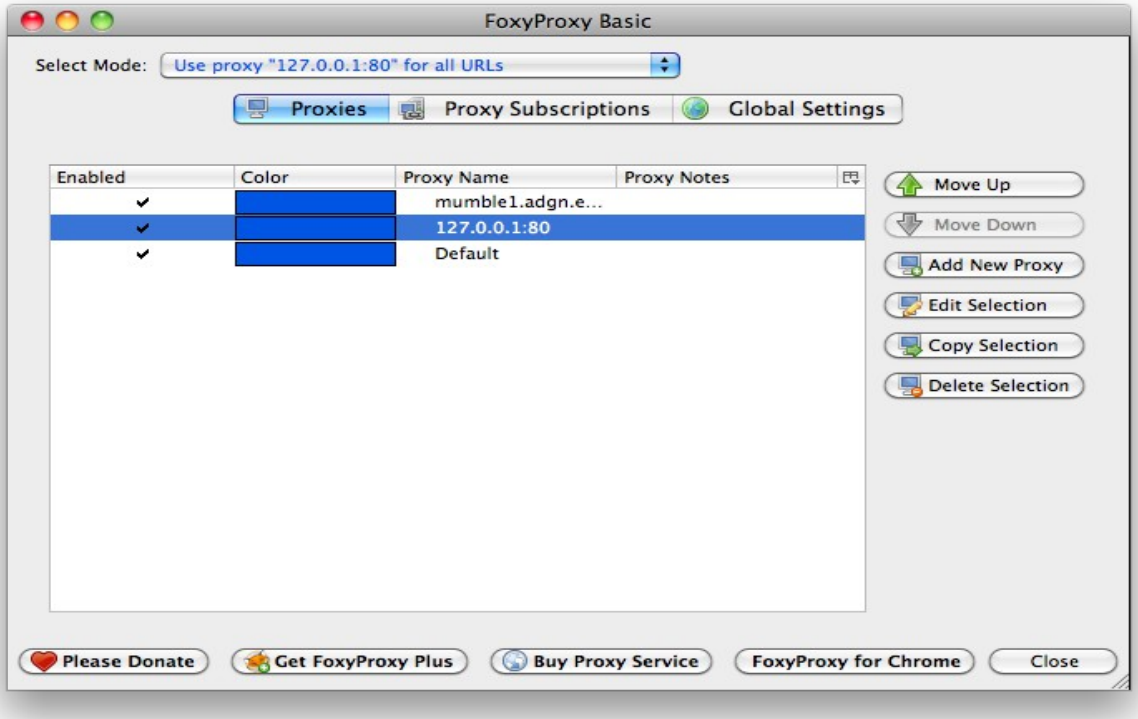
Le SSH est un protocole qui permet de contrôler une machine distante de manière sécurisée. Je vais mettre ici une petite explication pour surfer sur internet avec l'aide d'un plugin pour FireFox et ce protocole, dans le cas ou vous ne voulez pas utiliser TOR. Ce système est quelque peu plus contraignant car il nécessite l'accès à un serveur distant, mais permet de crypter entièrement votre surf si par exemple vous ne voulez pas que votre fournisseur d'accès internet voie les pages que vous consultez. Je ne vais pas rentrer en détail sur le fonctionnement de SSH (il faudrait plusieurs pages d'explication), mais je vais uniquement m'attarder sur cette petite technique. Il existe d'autres manières de faire, mais celle-ci est relativement simple.

Pour commencer, télécharger le plugin FoxyProxy Basic pour FireFox. Nous verrons comment le configurer par après. Dans un terminal (ou avec Putty si vous êtes sous Windows), rentrez la commande suivante :

ssh -D 80 utilisateur@mon.adresse.ip

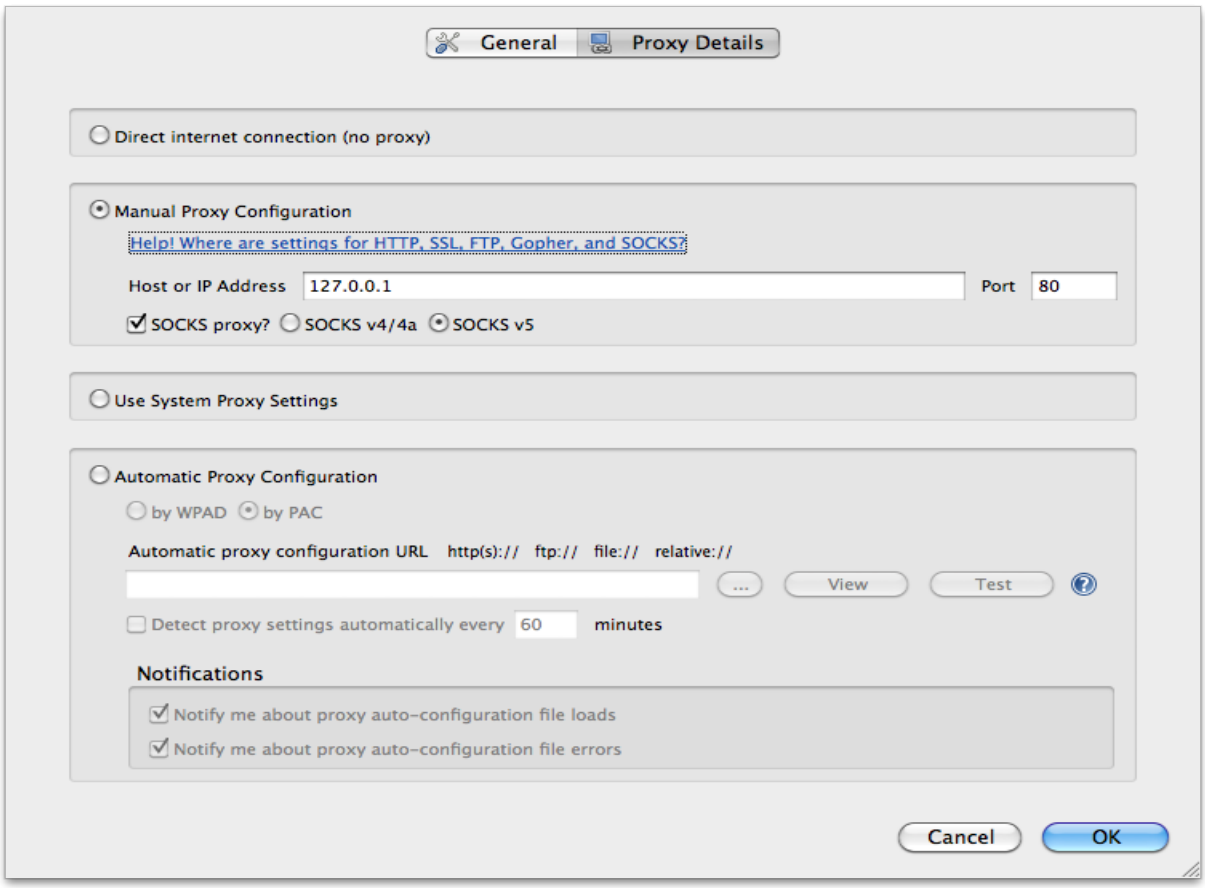
Laissez le terminal ouvert, n'y touchez plus jusqu'à ce que vous arrêtiez de surfer.

Comme vous avez installé FoxyProxy, à côté de votre barre d'adresse se trouve un petit renard bleu. Cliquez dessus et vous aurez accès au menu de FoxyProxy. Vous devriez arriver à cette fenêtre :



Ne faites pas attention aux règles qui sont déjà présentes, vu que je le fais à partir d'un de mes ordinateurs. Cliquez juste sur Add New Proxy. Vous devriez arriver à la fenêtre suivante, complétez

18 http://openvpn.net/



le tout comme indiqué sur l'image ci-dessous et cliquez sur OK.