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 : pourquoi protéger sa vie privée ?

Vous vous dites certainement que vous n'avez rien à cacher, et que vous vous moquez qu'on puisse tout savoir sur vous via internet. Beaucoup de personnes pensent comme vous. Pourtant, que ce soit des agences étatiques ou des grandes compagnies de marketing, ainsi que les réseaux sociaux, les moindres petites miettes que vous semez sur la toile sont collectées et analysées. Pour la première catégorie, c'est la surveillance totale des citoyens. Pour les seconds, mieux vous manipuler et vous gaver de publicités. Bien sûr, il existe d'autres personnes, encore moins scrupuleuses, qui pourraient utiliser ces données personnelles contre vous, et les cas de piratage de comptes sur Internet sont fréquents. Il existe donc des tas de raisons de se protéger, et ce même si nous n'avons rien à se reprocher.

La mise à mal de la vie privée a éclaté au grand jour en juin 2013, lorsque Glenn Greenwald a voyagé vers Hong-Kong pour rencontrer un ancien agent de la NSA, Edward Snowden[1]. Celui-ci a quitté l'agence avec des milliers de documents démontrant l'absence totale d'éthique de la NSA, collectant appels téléphoniques, e-mails et activités sur les réseaux sociaux de millions d'individus sur la planète. Le simple fait d'être en relation avec une personne critiquant, par exemple, le gouvernement américain, vous met sur la liste des personnes suspectes et êtes, de facto, mis sous surveillance.

Nous avons découvert PRISM et XKEYSTORE, deux programmes permettant à un agent de pénétrer dans diverses infrastructure informatiques tels que Google, Facebook, Apple… afin de collecter toutes vos informations. Personne n'est à l'abri, même si vous n'êtes pas citoyen américain. Pourtant, la situation en Europe est sensiblement pareille. Les pays de l'Union Européenne prennent le même chemin. Suite à la série d'attentats de Paris, la France a opté pour une surveillance globale de toute personne vivant sous son territoire. La Belgique n'est guère mieux lotie : elle a instauré une loi demandant aux fournisseurs d'accès Internet d'enregistrer toute l'activité des internautes belges. Bien que cette loi ait été cassée par la CEDH, le projet de loi est en train de revenir, avec seulement quelques termes légaux qui ont été modifiés. Mais globalement, le texte reste le même.

La surveillance étatique n'est pas le seul problème posé pour notre vie privée. Les grandes compagnies informatiques, que l'on appelle généralement GAFAM (Google Apple Facebook Amazon et Microsoft) nous offrent une myriade de produits gratuitement. En fait, ce n'est pas tout à fait exact. Nous payons le service avec nos données personnelles, qui seront par exemple revendues à des annonceurs publicitaires. Microsoft, avec son nouveau système Windows 10, enregistre tout ce que vous faites avec votre ordinateur. Ce que vous recherchez sur internet, ce que vous tapez dans les barres de recherche, les sites que vous visitez sont précieusement collectés par Microsoft. Google, en plus de pratiquer des méthodes similaires, enregistre tous vos déplacements via votre smartphone. Facebook enregistre vos likes, les statuts et articles sur lesquels vous vous arrêtez. Avec son algorithme, il peut mieux vous cibler en publicité, mais surtout va censurer une grande partie du contenu posté sur le réseau social, en ne vous affichant que des statuts ou articles qu'il suppose que vous aimeriez.

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, une des meilleures solutions à la protection de sa vie privée est de s'auto-héberger pour tous les services à

1 https://fr.wikipedia.org/wiki/Edward_Snowden

l’aide de logiciels libres. Malheureusement, ce système comporte beaucoup de contraintes : il faut non seulement de très grandes connaissances en informatique, mais également un ordinateur que l’on transformera en serveur et qui ne sera dédié qu’à cela[2]. Le tout, bien sûr, dans le meilleur des mondes, où le matériel ne tombe jamais en panne. Des communautés d'informaticiens ont cependant créé des équivalents libres à nos Gmail,Outlook,Dropbox,... Certains proposent mêmes des solutions hébergées et que vous pouvez utiliser sans devoir passer par un apprentissage conséquent. Il est donc totalement possible d'abandonner des sociétés comme Twitter, Facebook ou Google pour garder le contrôle sur ses données.

Cependant, couper tous les services et réseaux sociaux propriétaires risquent, en cas de vie sociale numérique intense, de vous couper d’un grand nombre de vos contacts. C’est pourquoi une partie de ce document s’axera sur comment limiter la casse. Je vous proposerai dans ce document des bons réflexes à prendre pour mieux se protéger. Néanmoins, le sujet est extrêmement vaste, et la technologie évolue tous les jours. Il se peut donc qu’à l’heure où vous lirez ces lignes, certaines informations soient obsolètes. Dans cet ouvrage, je ne me lancerai pas dans des explications trop techniques comme, par exemple, la cryptographie et les méthodes de chiffrement. Le but de ce document est donc de vous donner des bases, mais aussi de vous donner des moyens de creuser le sujet de manière bien plus approfondie.

2 À l'heure actuelle, un collectif d'hébergeurs alternatifs a créé la brique internet, qui permet de palier ce problème. Vous trouverez plus d'informations par ici : https://labriqueinter.net/

1. Premiers réflexes, pour une bonne hygiène numérique

Préambule : erreurs courantes de langage

Vous avez très certainement entendu parler de cryptage, de méchants hackers qui ont piraté tel ou tel service sur internet. En réalité, ce sont des erreurs de langage. Je me permets donc, avant d'aller plus loin, de corriger ces petites erreurs. Simplement car j'utiliserai les termes corrects dans ce document.

L'utilisation du terme cryptage, en français, n'est pas correct. Dans le cas d'un document « crypté », on parle de document chiffré. Tout comme pour cryptage, nous dirons chiffrement. Un hacker n'est pas non plus un pirate informatique. En réalité, un hacker est un bidouilleur. Quelqu'un qui bidouille un système pour l'étudier et/ou l'améliorer. C'est pour cela que vous entendez également parfois l'expression « hacker le système ». Dans le cas de piratage informatique, il y a plusieurs termes : il y a cracker, blackhat, scriptkiddies[3]… Pour simplifier ce document, j'utiliserai simplement le mot « pirate ».

1.1 Les mots de passe

Les mots de passe sont la base de la sécurité informatique. Pourtant, peu de personnes ont conscience réellement que leur mot de passe est peu fiable et peu sécurisant. En faisant un peu de social engineering[4] auprès de mon entourage, on constate que la majorité des utilisateurs sur internet utilisent des mots de passe facilement devinables : en effet, ces derniers sont souvent des combinaisons de 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.

Le second réflexe est de ne pas également utiliser simplement un mot du dictionnaire : il existe des logiciels qui vont tester les mots de passe en testant tous les mots un par un, et donc ceci est à proscrire également !

Le mieux est d'utiliser des mots de passe complexes, 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

3 Pour en savoir plus sur les hackers et pirates en tout genre : http://www.antredugreg.be/casser-le-mythe-du-mechant-hacker/

4 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.

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).

À 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/

Une autre méthode, très efficace, est de choisir quatre mots du dictionnaire que vous mettez aléatoirement. Bien sûr, ne prenez pas de phrases venant d'un livre par exemple. Il a été déjà démontré que bon nombre d'utilisateurs utilisaient des phrases des livres Harry Potter. Les pirates informatiques les ont rapidement intégrés à leur programme, rendant le mot de passe rapidement devinable. Essayez donc de mettre des mots qui n'ont rien à voir les uns avec les autres. Par exemple : chaussure manger constitution maison.

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 Veracrypt, présenté plus loin. Dans le fichier texte je mets les logins et mots de passe de chacun des services utilisés, et ensuite je mets ce fichier dans un container chiffré, dont moi seul ai l'accès. Le seul mot de passe à retenir est donc le mot de passe de ce fameux container. Il existe bien sûr des logiciels trousseaux permettant de stocker les mots de passe. Je conseille la prudence avec ces logiciels. Simplement parce que c'est une faille qui peut être exploitée. Dans le cas de Chrome, par exemple, le stockage de mot de passe est une invitation pour Google pour qu'il fouine dans tous vos services. Le cas du trousseau de MacOS est également à prendre avec des pincettes. Lors d'un de mes tests, j'ai pu avoir accès à tous les mots de passe stockés dans un trousseau en tapant quelques commandes.

1.2 Les questions secrètes

Beaucoup de systèmes proposent 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'envois de SMS (j'y viens juste après). La pratique que je conseille est bien sûr, de ne pas répondre exactement à la question. Une personne mal intentionnée, vous connaissant quelque peu, pourrait facilement prendre le contrôle de votre compte. Je vous donne un petit exemple :

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

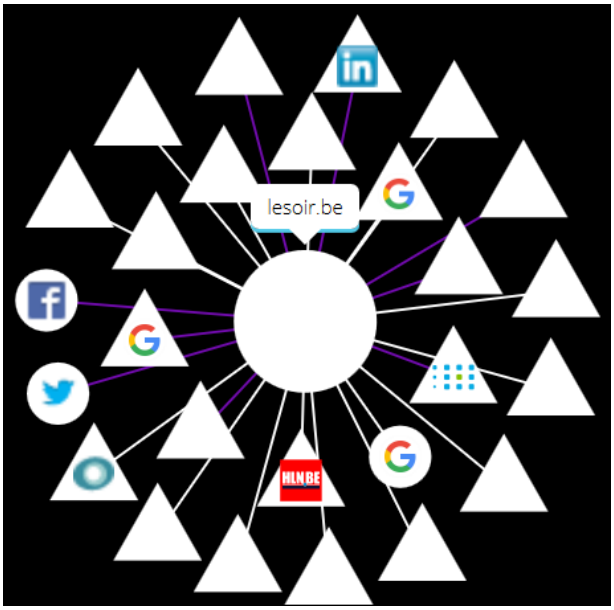
1.3 L'authentification à double facteur

Une solution de plus en plus fréquente pour protéger son compte est l'authentification à double facteurs. C'est-à-dire que lorsque vous vous connectez à un service, celui-ci peut envoyer un mail, un SMS ou demander un code spécifique via un appareil ou un logiciel. Cette solution est assez sécurisante. Il y a bien sûr un hic : vous devez dans le cas d'un SMS, donner votre numéro de téléphone. C'est une information supplémentaire sur vous-même que vous donnez à ce service. À

vous de voir si vous avez suffisamment confiance dans le service qui vous propose un tel système.

1.4 Vous êtes écoutés de toute part

Un des réflexes à prendre est de garder en mémoire que les sites que vous visitezOui, Facebook, Google, et bien d'autres compagnies connaissent toutes vos habitudes de surf. La majeure partie des sites que vous visitez contiennent des trackers qui enregistrent votre activité sur internet. Ils proviennent de bien d'outils différents : on analyse le temps et les pages que vous visitez, les régies publicitaires affichent des publicités selon vos habitudes de consommation, les réseaux sociaux analysent les articles que vous lisez pour mieux vous cibler ensuite (je reviendrai un peu plus en détails sur ce point plus tard). Par exemple, voici un petit schéma qui vous montre qu'une vingtaine de compagnies écoute ce que fait l'internaute sur le site du journal « Le Soir ».



Dans le même genre d'idées, votre smartphone n'est pas un ami qui vous veut que du bien. Les programmes d'assistance vocales, tels que SIRI sur Apple, enregistrent toute votre activité dans les centre de données de la firme. Pareil pour Android. Vos déplacements sont également enregistrés et analysés. Chaque fabricant dispose d'outils similaires : lifelog, par exemple de Sony, est un véritable petit espion sur ce que vous faites tous les jours.

Pour Apple, vous ne possédez absolument pas le contrôle sur votre produit et ce pour deux raisons : la firme a déposé une technologie permettant de bloquer certaines fonctionnalités de votre appareil quand ça lui chante[5]. De plus, jailbreaker[6] un appareil peut être passible de prison aux Etats-Unis[7]. Et nous avons vu dernièrement que toute personne faisant réparer son produit en dehors du circuit officiel ne pouvait plus utiliser son appareil[8].

Pour les produits Android, c'est quelque peu la même chose. Il y a cependant une alternative

5 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

6 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.

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

8 http://www.cnetfrance.fr/news/iphone-erreur-53-remplacement-ecran-bouton-home-bloque-iphone-39832476.htm

de taille. Vous pouvez « 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.

Toujours 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[9], 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.

1.5 Fuyez la technologie Flash !!!

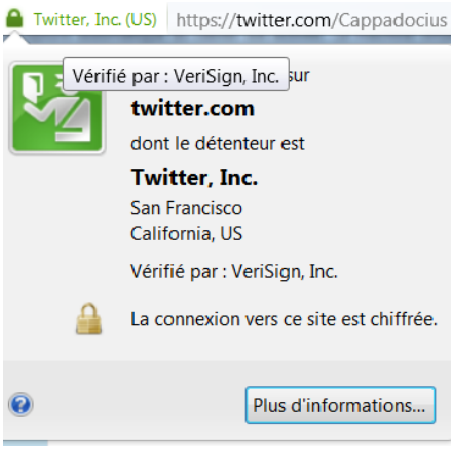
Tout site utilisant la technologie Flash est fermé, son code n'est pas analysable, et donc il se pourrait qu'un programmeur malveillant ait mis une technologie permettant de renvoyer des informations de votre machine vers chez lui (un backdoor). De plus, la technologie se fait de plus en plus vieille, et répond de moins en moins bien aux besoins actuels.

1.6 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 chiffrée 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.

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 :

9 https://f-droid.org/



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

1.7 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. Il existe aussi moyen d'installer un moteur de recherche personnel qui interrogera les autres moteurs pour vous. Il s'agit en l'occurrence de Sear-x, utilisé par Framasoft et son tontonroger.org, utilisé pour sa campagne « degooglisons internet », qui sera détaillée plus loin.

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 actives 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 visités, les documents que vous avez téléchargés sont gardés en mémoire par votre

navigateur. Il est donc impératif que 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, nettoye- le régulièrement également !

2. Utilisation des services web.

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

Les services Web propriétaires : une appropriation de vos données personnelles

La technologie a avancé très rapidement, et nous a facilité la vie. Des tas de services ont vu le jour, vous permettant de stocker, souvent gratuitement toutes vos données sur internet. Malheureusement, si c'est gratuit, c'est fait au détriment de vos données. Elles sont analysées, et de grands algorithmes étudient alors vos goûts, vos déplacements,... pour mieux vous cibler en publicité. On dit d'ailleurs généralement : « si c'est gratuit, c'est vous le produit ! » Prenons par exemple le cas de Facebook : tous vos « likes » sont analysés, et toutes les publicités sont affichées en conséquence. Si vous aimez le lait, Facebook vous affichera régulièrement des pubs Campina. Mais aussi, le réseau social décide pour vous ce que vous devez voir dans vos fils d'actualités. Si vous interagissez rarement avec une personne, vous ne verrez plus ce qu'elle fait sur le réseau. Vous n'êtes plus maître des informations que vous verrez.

Mais utiliser des services qui centralisent toutes vos données vous restreint également dans vos choix, car étant habitués à utiliser tel ou tel service, vous en devenez rapidement prisonnier et il devient de plus en plus difficile de s'en défaire. Vous n'êtes plus libre de choisir un concurrent, car migrer toutes vos données deviendrait aussi plus difficile.

Pour terminer, je soulignerai juste un dernier point : la surveillance. Comme je l'ai expliqué dans l'introduction, Edward Snowden a démontré que les services de renseignements avaient leurs portes d'entrées sur la majeure partie des services webs. Avant d'attaquer le gros morceau de ce chapitre, voici les règles d'or à appliquer sur les réseaux sociaux majeurs :

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 libres), et respectueux de votre privée[10].

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

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

retrouver avec un moteur de recherche. Limitez par exemple les photos de famille à votre sphère privée, les photos de guindaille avec les amis avec qui vous faites la fête, etc.

4. Ne jamais aimer une marque.

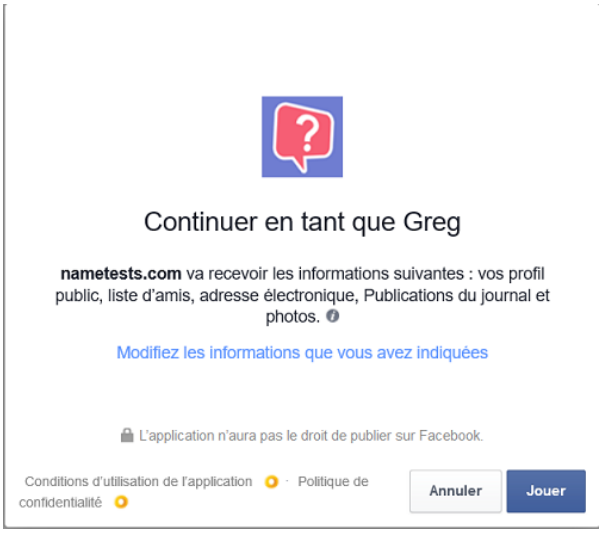
Aimer une marque, c'est indiquer vos habitudes de consommation, et ce type de renseignements est très précieux pour les annonceurs. Dans une autre mesure, on pourrait également dire que vous travaillez gratuitement pour cette dernière en leur faisant de la publicité. Vos amis verront que vous aimez la marque dans leur flux. 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 recevoir un multitude de mails publicitaires. Ces techniques de concours sont souvent utilisées également par des personnes peu scrupuleuses pour vous soutirer des informations personnelles, voire du phising pur et simple (spoliation de vos identifiants pour pirater votre compte). 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.

6. Les applications tierces sont des aspirateurs à données

Les réseaux sociaux majeurs utilisent pas mal d'applications tierces, que vous greffez à votre compte. Par exemple, si vous utilisez Facebook, vous avez certainement déjà vu des jeux gratuits, des petits quizz, des tests de personnalités, etc. Ces applications ne proviennent pas de Facebook, mais d'autres sociétés. Et chaque fois que vous connectez un de ces quizz, vous ouvrez la porte à une compagnie à scruter toutes vos données personnelles. Petit exemple par ici, avec le célèbre nametest.



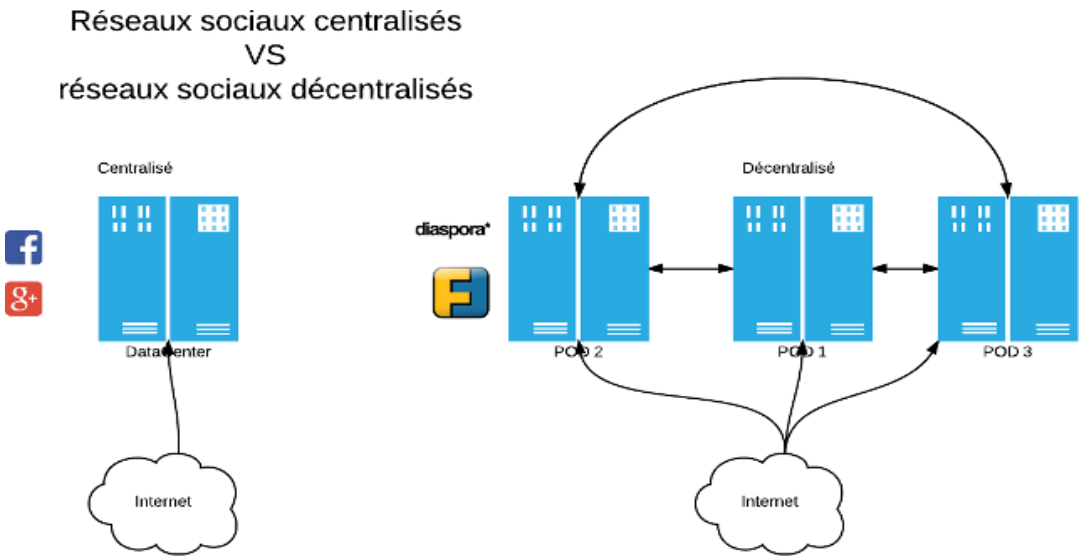
La liste des informations que vous données est plutôt impressionnante : toute information de profil public, mais aussi accès à votre liste d'amis, la liste de vos contacts, votre mail, vos photos,… Réfléchissez bien avant de donner de tels accès. Facebook permet de paramétrer les informations que vous fournissez à cette société (le lien que vous voyez en bleu sur la capture d'écran ci-dessus).

Centralisation des données VS décentralisation des données

Qu'est-ce-que ces termes chinois, me direz-vous? En fait, ce n'est pas bien compliqué. Je vais expliquer le tout grossièrement, sans terme technique, histoire de ne pas vous perdre dans les explications. Je lance cette explication ici, avant de rentrer dans les détails, parce que les services libres sont, à l'inverse des sociétés telles que Google et cie, décentralisés.

Imaginez un instant que Facebook est un gros silo à grains, les grains étant les données que vous y mettez. Bien que vous y mettiez vos grains, seul Facebook détient la clé de la porte du silo, décidant seul de ce qu'il va faire des grains. À l'inverse, un réseau décentralisé est une multitude de silos, plus petits, que l'on appelle pod. Vous pouvez décider de mettre vos grains dans un silo existant, au quel cas vous recevez une clé qui permettra d'aller dans l'espace où vous les stockez. Mais vous pouvez aussi décider de construire votre propre silo, et de le rajouter dans un parc qui en contient des tas, et qui communiquent entre eux. Ainsi les utilisateurs des silos extérieurs peuvent consulter votre réserve de graines. Bien sûr, comme vous avez accès à vos grains, ou si vous retirez votre silo du réseau, ces derniers ne seront plus visibles par personne. Vous restez le maître de vos semences, donc dans ce cas-ci de vos données.

Voici un petit schéma simplifié (parce qu'en réalité c'est un peu plus compliqué) qui explique la différence entre les deux systèmes.



Les alternatives :

Bien sûr, la majorité des services dans le « cloud » dispose de son équivalent libre. Que ce soit votre agenda, vos feuilles de calcul, vos outils de note... Il existe toujours un équivalent que vous pouvez installer chez vous ou sur un ordinateur (en l'occurrence on l'appelle un serveur) connecté à internet. Si je devrais n'en citer qu'un, je dirai Yunohost, qui est un équivalent à presque tout ce que propose Google : espace de stockage, serveur de mails, partage de fichiers, calendrier... Le tout dans une seule distribution Linux. Tout est prévu pour le débutant, les seuls prérequis étant d'avoir un ordinateur disponible (généralement un serveur dédié), ainsi qu'un nom de domaine[11]. Il existe également la brique internet, fournie par la FDN, association des fournisseurs internet indépendants.

Mettre tous ces outils en place peut cependant demander du temps et beaucoup d'apprentissage. C'est pourquoi Framasoft a mis en place une initiative qui vous montre comment cela fonctionne et met à disposition pléthore d'outils pour le néophyte.

Degooglisons internet !

Framasoft, une association qui promeut le logiciel libre s'est lancé dans une grande campagne appelée Degooglisons internet et propose une multitude de services libres, pour sensibiliser tous les internautes. Framasoft vous montre comment cela fonctionne, et vous propose des tutoriels pour chaque outil, afin que vous puissiez les installer sur votre machine. Quelques exemples :

Service propriétaire	Service Framasoft	Logiciel utilisé
Doodle	Framadate	Studs
Google Style sheets	Framacalc	Ethercalc
Google docs, Word Online	Framapad	Etherpad
Pocket	Framabag	Wallabag

11 Un nom de domaine équivaut à une adresse. Par exemple, google.be est un nom de domaine (c'est expliqué grossièrement, mais c'est pour vous faire une idée). Plus d'infos : http://fr.wikipedia.org/wiki/Nom_de_domaine

Ce tableau n'est pas exhaustif, et Framasoft projette de rajouter une multitude de services au cours des prochaines années.

Les réseaux sociaux libres

Bien sûr, il existe aussi des réseaux sociaux libres. Basés sur le principe de décentralisation, comme expliqué précédemment et dont le code source est librement accessible. Il en existe plusieurs, certains à stade très avancé de développement, comme Diaspora ou Friendica. Framasoft propose, pour son projet « degooglisons » une instance de Diaspora, la framasphere. Lister tous ces projets risque d'être long et fastidieux, car il existe des tas d'alternatives ! Je vais seulement vous en présenter quelques-uns, qui sont pour moi les plus avancés.

Diaspora

Diaspora est mon coup de coeur dans les réseaux sociaux alternatifs, et c'est aussi le plus actif. La communauté décide des futures fonctionnalités à implémenter.

Friendica

Friendica est aussi un énorme réseau social. Vous pouvez d'ailleurs facilement le tester chez vous à l'aide d'une machine virtuelle[12]. Néanmoins, l'interface dispose de tellement d'options que paramétrer correctement la confidentialité de ses données peut devenir fastidieux. A noter également qu'il existe Red Matrix, qui est un projet dérivé de Friendica

Twister

Twister est un dérivé de Twitter, entièrement décentralisé. Il est basé sur la technologie de la crypto-monnaie Bitcoin, et donc chaque message envoyé est crypté. Néanmoins, tous les messages échangés doivent être téléchargés sur votre ordinateur pour pouvoir utiliser correctement le logiciel. Il est toujours en développement mais est très prometteur.

12 http://fr.wikipedia.org/wiki/Machine_virtuelle

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[13]. 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 absolument pas le lire ! Afin de pouvoir lire le fichier correctement, il va vous falloir passer

13 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.

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[14] » . 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 ?+ modifier avec ceci : http://www.cnetfrance.fr/news/iphone-erreur-53-remplacement-ecran-bouton-home-bloque-iphone-39832476.htm

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 !

14 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

Equivalences programmes propriétaires/ logiciels libres

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 ou Cyanogenmod
IOS devices et Mac OS 10.7+	Je suis très triste pour vous !
Windows et Mac OS	GNU/Linux of FreeBSD (Unix libre)
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. Firefox, et ses ajouts indispensables :

Je conseille Firefox comme navigateur, en place et lieu des Chrome, Internet Explorer et consort. Chrome enregistrant toute l'activité, il vaut mieux s'en passer. Firefox est un logiciel libre, entièrement modulable. Bien sûr, utiliser Firefox a lui seul ne résoudra pas tous les problèmes. Voici quelques modules à installer, en complément.

Privacy Badger : cet outil, conçu par l'Electronic Frontier Fundation permet de bloquer tous les traqueurs sur un site internet. Il est entièrement modulable, et vous pouvez réactiver un traqueur ou un bouton si vous estimez qu'il est digne de confiance.

Mblock Origin : La publicité est omniprésente sur internet, et les régies publicitaires sont à elles seules des traqueurs, repèrent vos habitudes de consommation. Ublock origin permet de bloquer les publicités et de ne plus les afficher.

Lightbeam : Lightbeam est un outil qui permet de créer des graphiques de tous les traqueurs sur une page internet.

Web Of Trust : Web of trust est un outil communautaire qui permet de vérifier la qualité d'un

site internet, que ce soit au niveau de l'information mais aussi de dire si le site est créé à des fins frauduleuses. Comme l'outil est communautaire, c'est à tout un chacun de de donner son avis sur les sites visités, sinon les informations ne seront ni pertinentes ni abondantes.

Il y a bien sûr des tas d'autres outils utiles. Nous en verrons certains dans la partie suivante, qui sont utilisés avec le logiciel TOR, comme noscript, htttpseverywhere, qui sont directement intégrés. Vous pouvez aussi installer des outils qui permettent d'avoir des informations sur le serveur et/ou le site (adresse IP, propriétaire, etc).

2. 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.

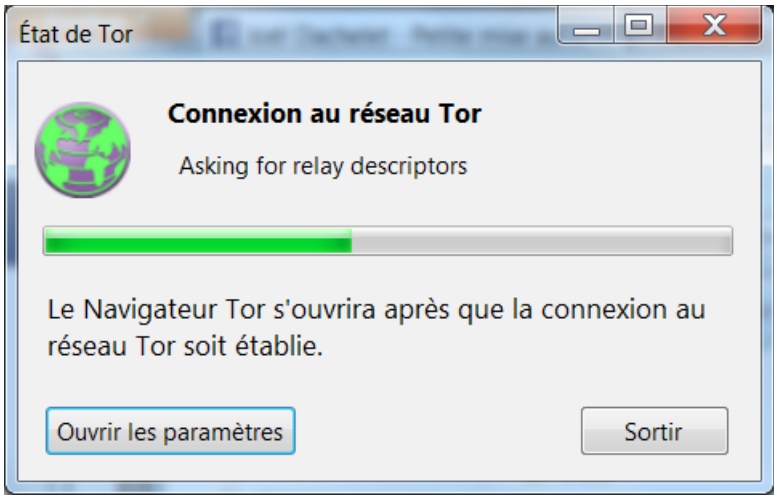
Comment ça marche ?

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.

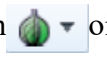
Lancer TOR :

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 chiffrée 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[15]. 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[16], 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.

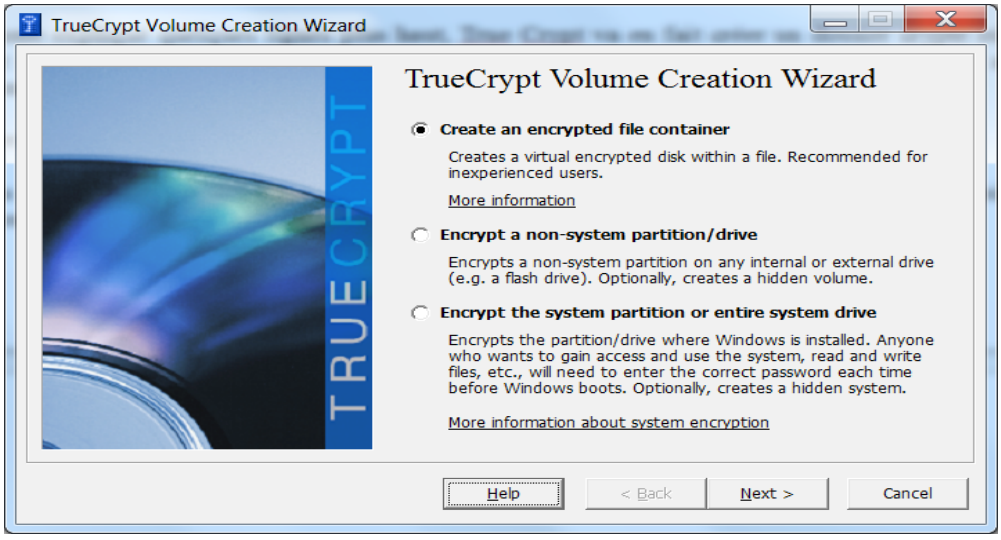
3. Veracrypt

Veracrypt est un petit programme compatible tout système d'exploitation permettant de créer des disques durs et containers entièrement chiffrés, 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://veracrypt.codeplex.com/

Veracrypt 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 Veracrypt aux autres méthodes de cryptage pour deux raisons : la première est que Veracrypt 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. Les captures d'écran suivantes, pour vous aider à créer un container chiffré sont basés sur un ancien logiciel appelé Truecrypt, mais les informations et fenêtres restent les mêmes.

Créer et utiliser un volume chiffré :



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

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

Create an encrypted file container :

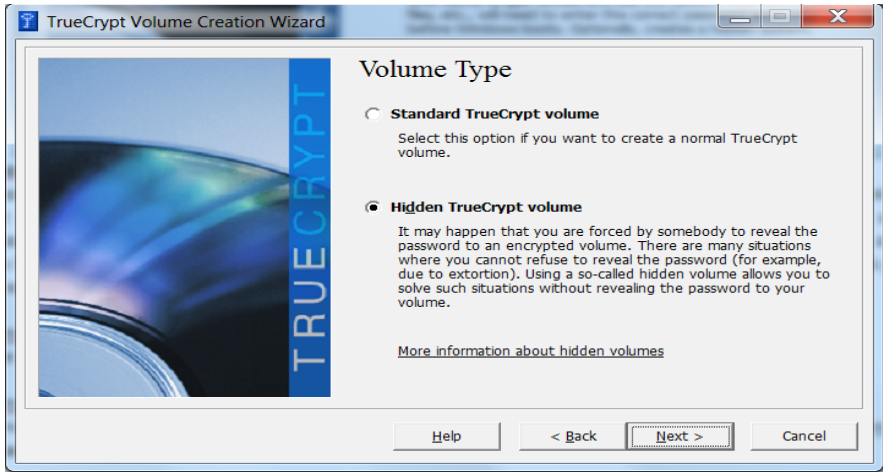
Comme expliqué quelques lignes plus haut, True Crypt va en fait créer un dossier chiffré où vous allez stocker tout sorte de données. Pour y accéder, il créera un lecteur virtuel, et on y accède comme si on accédait à une clé USB, disque dur,… Je m'attarderai sur la première option, afin de vous faire 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

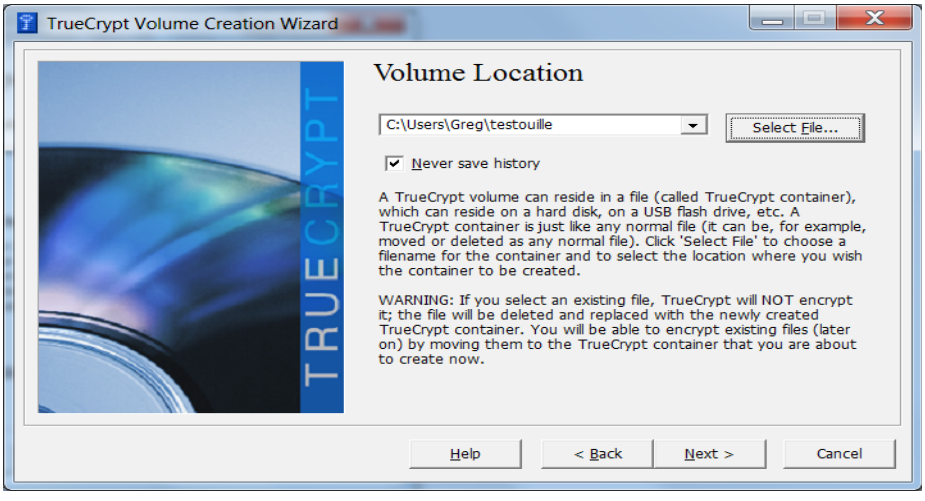
Cette option sert à faire de même, mais à l'échelle d'un disque dur, d'une clé usb,…

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.

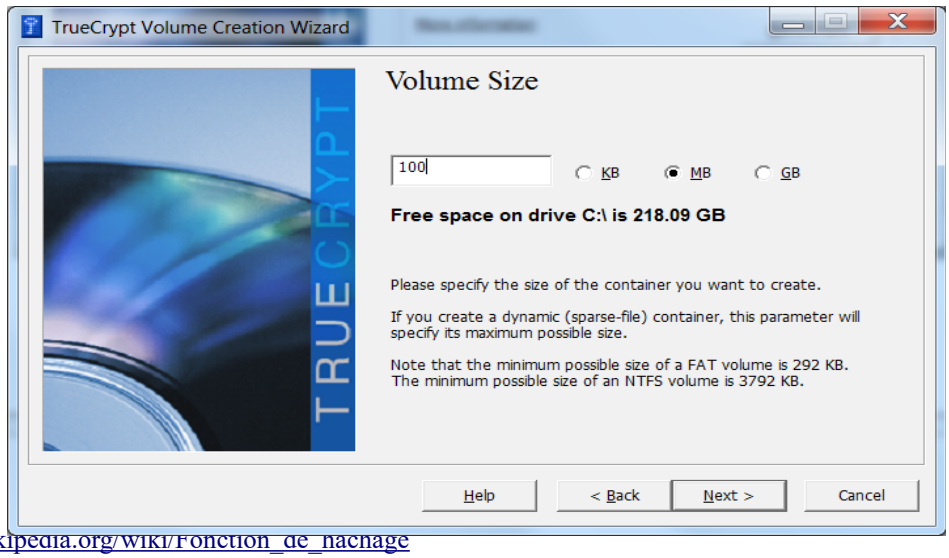


Ici, j'ai donc cliqué sur la première option, à savoir « Create an encrypted file container ». J'ai donc accès à deux options : le volume standard, ou le volume caché (Hidden). Ce dernier permet de faire un container caché dans un premier container. Personnellement je ne l'ai jamais utilisé, mais si 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 Veracrypt, si vous sélectionnez un de vos fichiers à ce moment du processus, le supprimera et créera un container chiffré au nom de celui-ci.

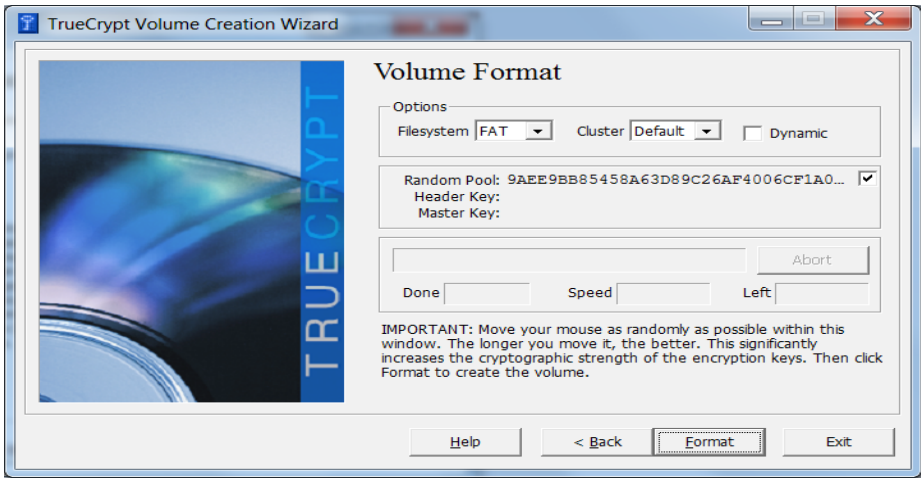
Nous en voici au choix de la méthode de cryptage. Je ne vais pas donner une explication détaillée sur les méthodes d'encryptage, mais si vous êtes intéressé par le sujet, pléthore de sites internet en parle, et vous pouvez déjà avoir un bref aperçu sur le site de Veracrypt. Pour ma part j'utilise la méthode que vous voyez à l'écran qui crypte les données plusieurs fois avec plusieurs protocoles différents. De même, pour les algorithmes de hashage[17] (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.



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

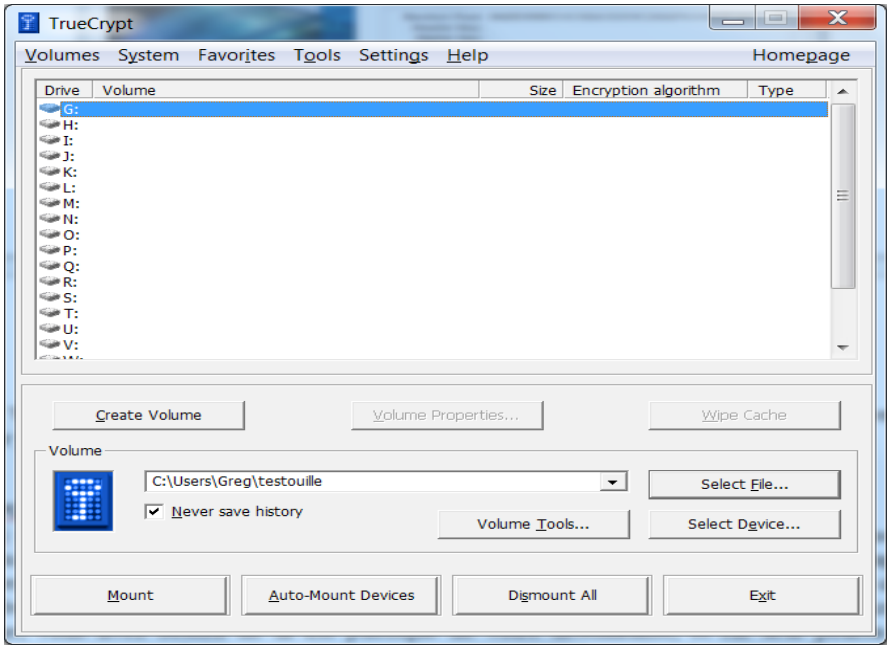
Cette étape-ci consiste à spécifier la tailler de votre dossier chiffré. Dans l'exemple que vous voyez, je viens d'allouer 100 MO d'espace à mon dossier "testouille". Dans la capture d'écran suivante vous arrivez à l'étape du mot de passe. Ici, vous trouverez une option supplémentaire : use key file. 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 !

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 chiffré !

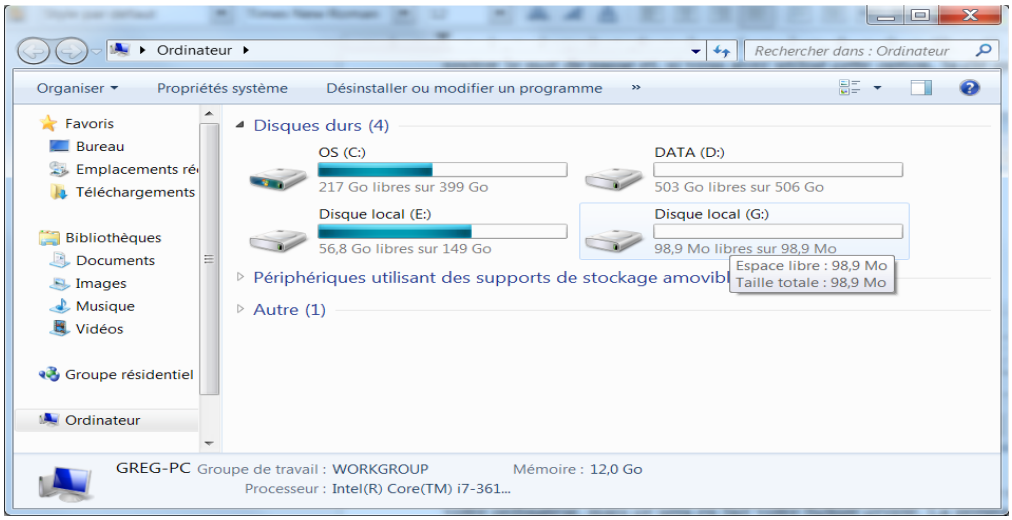


Voilà ! Votre dossier est créé et prêt à être utilisé ! Nous allons donc maintenant l'activer afin de pouvoir y mettre des fichiers dedans. Dans la fenêtre d'accueil, Sélectionnez la première lettre de lecteur disponible, puis en bas sur select file. Dans la fenêtre qui s'ouvre, choisissez votre dossier chiffré 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 chiffré 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 chiffré. La preuve en image :



Comme la première lettre de lecteur dans Veracrypt était G, mon dossier chiffré 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 chiffrer 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 chiffré, 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 (ce que nous appelons les méta-données).

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[18] (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[19] qui remplace totalement les skype et consort, en proposant la vidéo en plus, et Linphone[20] 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[21].

18 http://fr.wikipedia.org/wiki/Extensible_Messaging_and_Presence_Protocol
19 http://tox.im/
20 http://www.linphone.org/
21 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 réseaux (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 chiffré. 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[22] pour plus de renseignements.

SSH

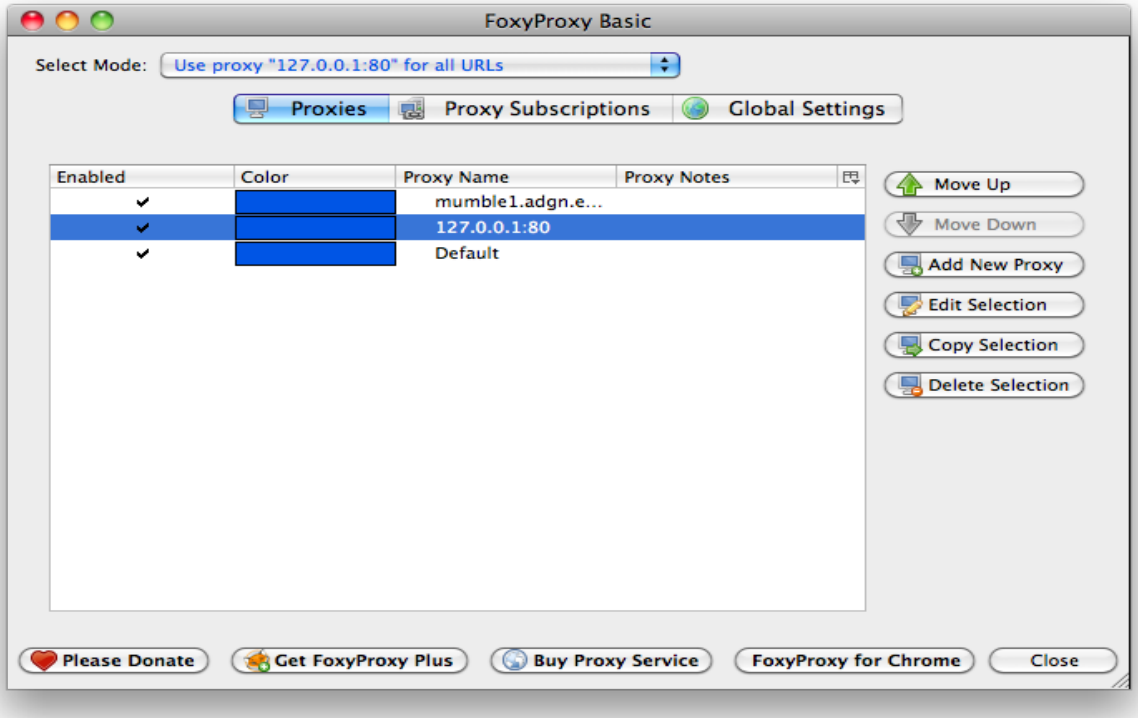
Le SSH est un protocole qui permet de contrôler une machine distante de manière sécurisée. Je vais mettre ici une petite explication pour surfer sur internet avec l'aide d'un plugin pour FireFox et ce protocole, dans le cas ou vous ne voulez pas utiliser TOR. Ce système est quelque peu plus contraignant 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.

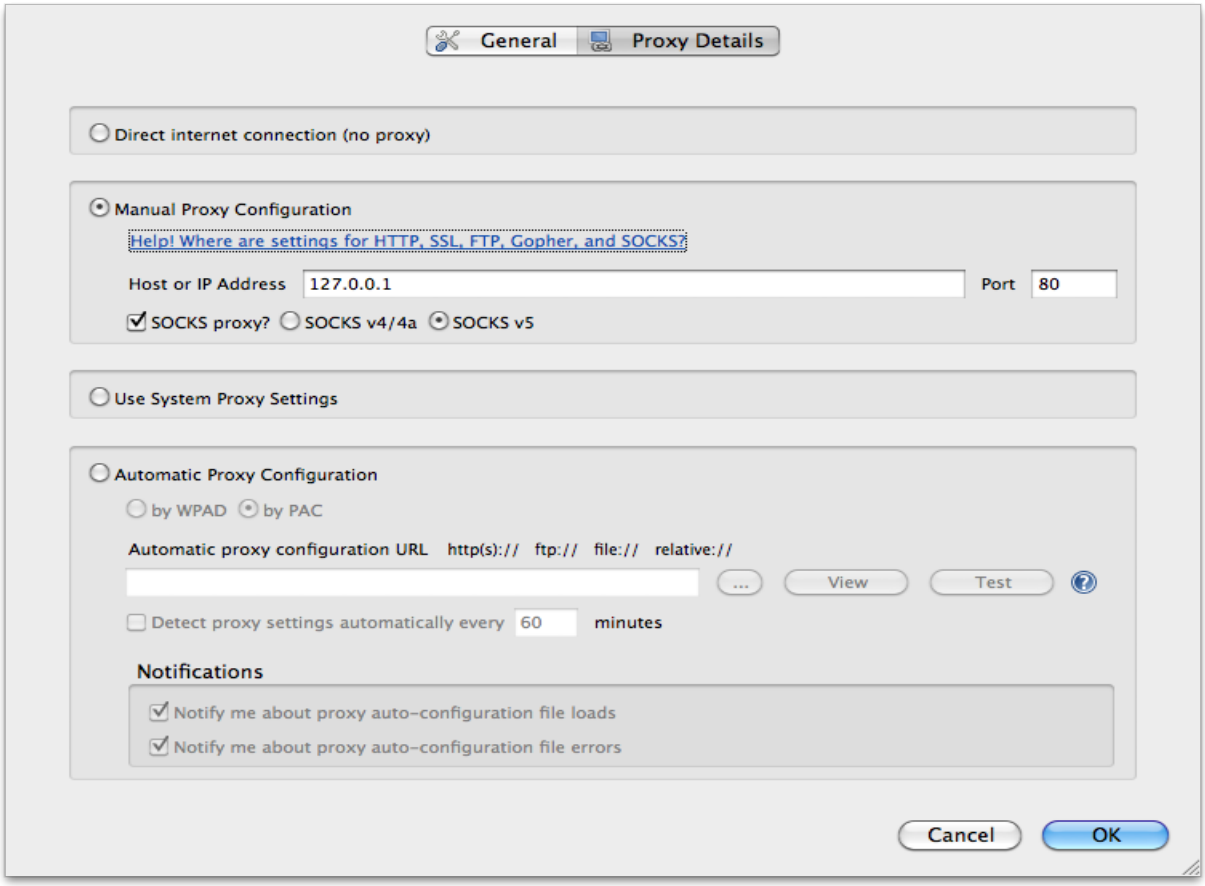
Comme vous avez installé FoxyProxy, à côté de votre barre d'adresse se trouve un petit renard bleu. Cliquez dessus et vous aurez accès au menu de FoxyProxy. Vous devriez arriver à cette fenêtre :



Ne faites pas attention aux règles qui sont déjà présentes, vu que je le fais à partir d'un de mes

22 http://openvpn.net/

ordinateurs. Cliquez juste sur Add New Proxy. Vous devriez arriver à la fenêtre suivante, complétez



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

Quelques sites et associations pour creuser le sujet :

Le logiciel libre

La Free Software Fundation

Site de la fondation, fondée par Richard Stallman. Il existe un site européen, dont la majeure partie est en français : http://fsfe.org/

Sourceforge

Sourceforge est une grande logithèque de logiciels libres ou Open Source. Elle dispose de milliers d'applications. http://sourceforge.net/

Github

Github est également une grande logithèque, un peu plus particulière. Elle est utilisée principalement par les développeurs qui peuvent y mettre du code en quelques clics. Framasoft dispose d'un équivalent plus libre dans les services qu'elle propose. https://github.com/

F-Droid

F-Droid est un répertoire de logiciels libres pour Android, un peu comme le Google Play Store. https://f-droid.org/

La Quadrature du Net

La quadrature est une association qui défend principalement la neutralité d'internet, mais aussi les droits des internautes. http://www.laquadrature.net/

April

April est une des plus grosses associations française faisant la promotion du logiciel libre. http://www.april.org/

Nurpa

La Nurpa est une association belge qui est similaire à la Quadrature du Net, mais plus axée sur la Belgique. Son objectif est de défendre les droits et libertés des citoyens sur internet. Http://www.nurpa.be

Framasoft

Framasoft est une association qui promeut les alternatives libres dans tous les sens. Elle ne se limite pas aux logiciels, mais aussi à la culture. Elle propose également énormément d'outils pour que l'on puisse reprendre son informatique en main. http://framasoft.net/

DoudouLinux

La distribution Linux pour les enfants: http://www.doudoulinux.org/web/francais/index.html

Les réseaux et services web

Degooglisons internet

Initiative de Framasoft pour sensibiliser les internautes sur les dangers de la centralisation de nos données, et propose des alternatives libres : http://degooglisons-internet.org/

The Diaspora Project

Site expliquant le projet Diaspora : https://diasporafoundation.org/

Twister
Twister est un équivalent de Twitter, entièrement décentralisé. http://twister.net.co/

Yunohost
Yunohost est un système Linux qui propose une alternative de taille pour héberger tout ses services web, que ce soit le mail, l'agenda ou le stockage des données. https://yunohost.org/#/

La brique internet
La brique internet est une petite boite qui permet d'installer vos services en quelques clics et sans grandes connaissances informatiques. Elle vous permet de vous affranchir de la majeure partie des services webs fermés. https://labriqueinter.net/

La FFDN
Cette association est un rassemblement des fournisseurs d'internet associatifs. Ils fournissent généralement des briques internet et des accès au réseau, dans une optique associatives et non commerciales. https://www.ffdn.org/ A noter qu'il existe bien un fournisseur d'accès internet belge fonctionnant sur ce modèle : neutrinet (http://www.neutrinet.be).

Informations et contact :

Vous pouvez trouver d'autres articles ou une version plus récente de ce manuel via mon site personnel. N'hésitez pas à me contacter, en cas de questions !

- Site : http://www.antredugreg.be
- Twitter : https://twitter.com/Le__Greg
- Facebook : https://facebook.com/antredugreg
- Diaspora : https://framasphere.org/u/legreg