COMPRENDRE LA CYBERSÉCURITÉ !

Introduction à la cybersécurité

Une série de volumes pour comprendre les **techniques des cybercriminels.**

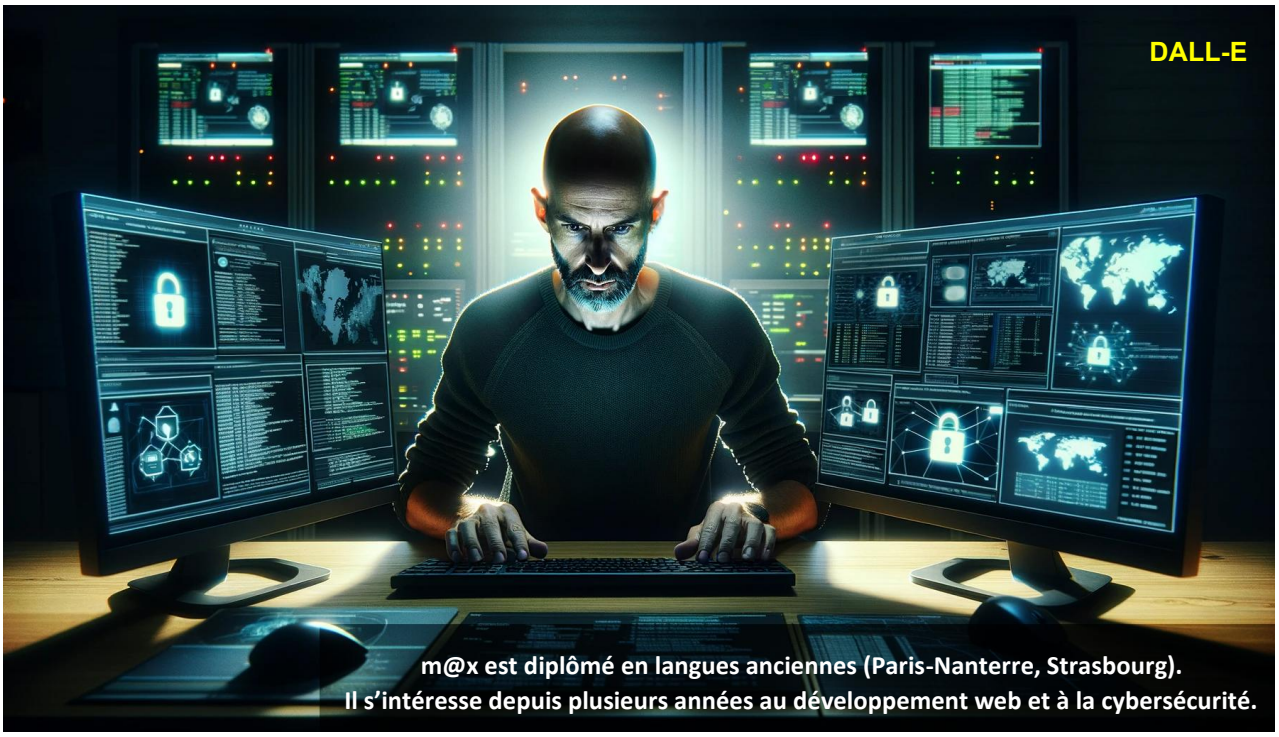
Anonymat & vie privée

m@x (contact@mgregoire.be)

CLAUSE DE NON-RESPONSABILITÉ (disclaimer)

WARNING

Il est illégal d'utiliser les techniques présentées dans cet ouvrage contre des cibles réelles sans avoir conclu au préalable un accord avec les responsables concernés. Ne pas tenir compte de cet avertissement vous expose à des poursuites judiciaires et éventuellement à des peines de prison. Le but de ce document est avant tout didactique et je ne pourrai en aucun cas être tenu pour responsable des actes commis par les lecteurs. Je ne serai pas là, le cas échéant, pour vous éviter de sérieux ennuis. La lecture de ce manuel et l'étude de la cybersécurité demandent un minimum de maturité ! Dans le cadre du hacking éthique, seules les cibles virtuelles (machines virtuelles) sont autorisées, ainsi que les cibles réelles qui en font la demande de manière contractuelle. Un accord oral n'a, en effet, pas de valeur légale. Soyez sensible à cet avertissement car la sécurité informatique est un domaine aussi captivant que glissant…



m@x est diplômé en langues anciennes (Paris-Nanterre, Strasbourg).
Il s'intéresse depuis plusieurs années au développement web et à la cybersécurité.

 Version 1.6

À A. M.

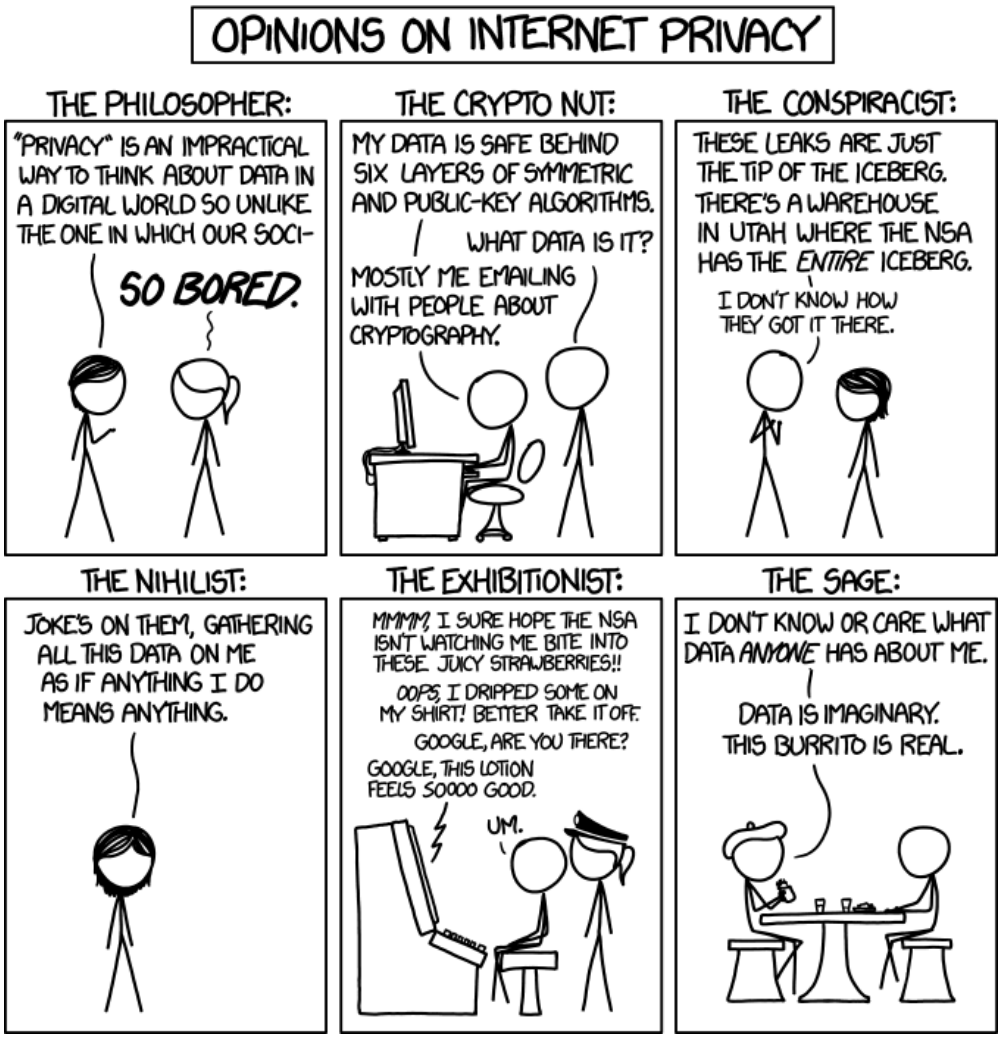
Un grand merci à toi.

Table des matières

Comment faire respecter votre vie privée et votre anonymat sur Internet :

	VOTRE IDENTITÉ EST :	VOTRE ACTIVITÉ EST :
RESPECT DE LA VIE PRIVEE	**NON SECRÈTE**	**SECRÈTE**
RESPECT DE L'ANONYMAT	**SECRÈTE**	**NON SECRÈTE**

Anonymat et vie privée sur Internet



https://xkcd.com/1269/ (Creative Commons BY-NC 2.5, auteur : Randall Munroe)

OPSEC (OPerations SECurity)

La sécurité opérationnelle est une technique qui permet de ne pas divulguer de l'information critique à des adversaires potentiels. L'OPSEC consiste à utiliser des contre-mesures comme le chiffrement des données, le compartimentage, …

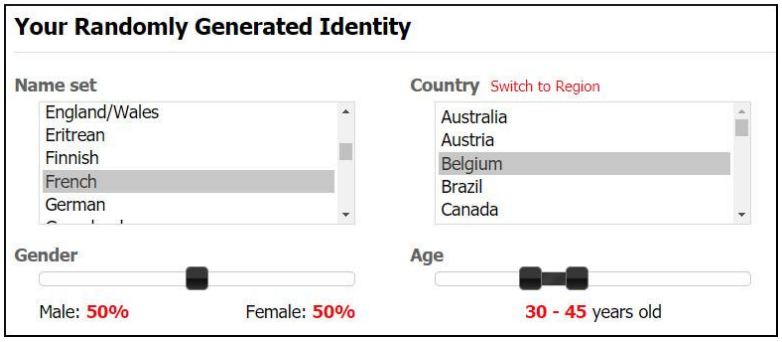
L'OPSEC permet d'assurer :

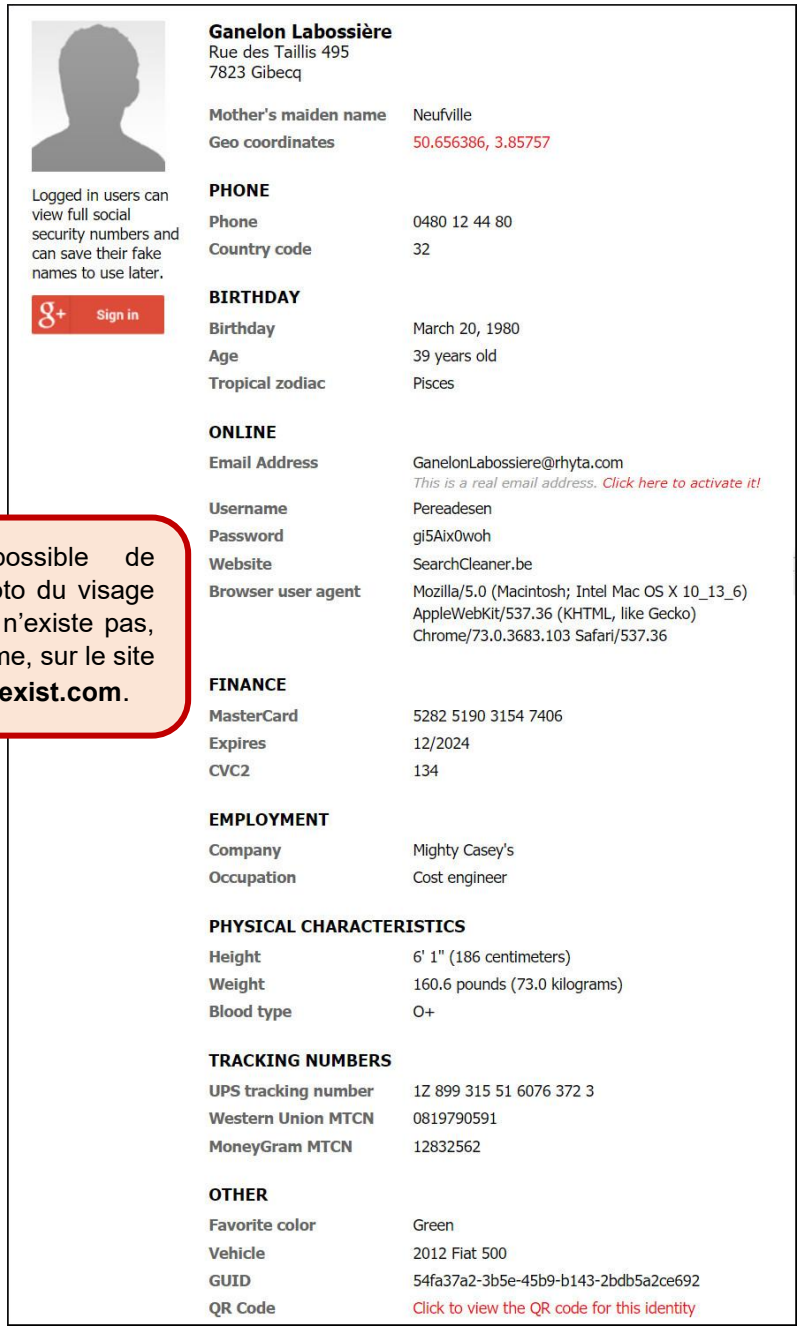
- **Le secret (privacy) : maintenir la confidentialité,**
- **L'anonymat : empêcher que vos actions vous soient attribuées,**
- **Le pseudonymat : faire en sorte que vos actions soient uniquement attribuées à un pseudonyme ou alias.**

L'attribution d'un acte sur Internet à une personne réelle est très souvent due à une erreur humaine, et donc à une violation d'OPSEC. Utiliser le réseau TOR ne sert à rien si vous commettez une erreur permettant de vous identifier (par exemple en vous connectant à votre compte Google). De nombreux cybercriminels s'en sont rendus compte à leurs dépens. Il faut, par exemple, toujours séparer sur Internet ses activités personnelle et professionnelle. Il est impératif d'avoir un laptop (smartphone, …) personnel et un laptop (smartphone, …) professionnel. La mode actuelle du BYOD (*Bring Your Own Device*), qui consiste à utiliser ses équipements personnels au travail est très dangereuse. Un hacker ayant piraté votre compte personnel aura également accès à vos documents professionnels. Une catastrophe pour votre carrière.

Une stratégie très efficace pour maintenir son anonymat est le compartimentage (compartmentalization). Il suffit d'avoir un alias différent pour chaque profil (un alias pour Facebook, un autre pour Linkedin, un autre encore pour jouer en ligne, …) Il faut bien évidemment éviter la contamination croisée des ses identités. Ross Ulbricht, le créateur du site caché Silk Road, en a fait les frais puisqu'il fut ainsi démasqué par le FBI. Un de ses alias fut relié à son identité réelle par une simple recherche sur Google ! Ross Ulbricht fut arrêté en octobre 2013, deux ans après l'ouverture de Silk Road.

Une personne désirant se créer une couverture afin de crédibiliser un alias peut se rendre sur le site www.fakenamegenerator.com :



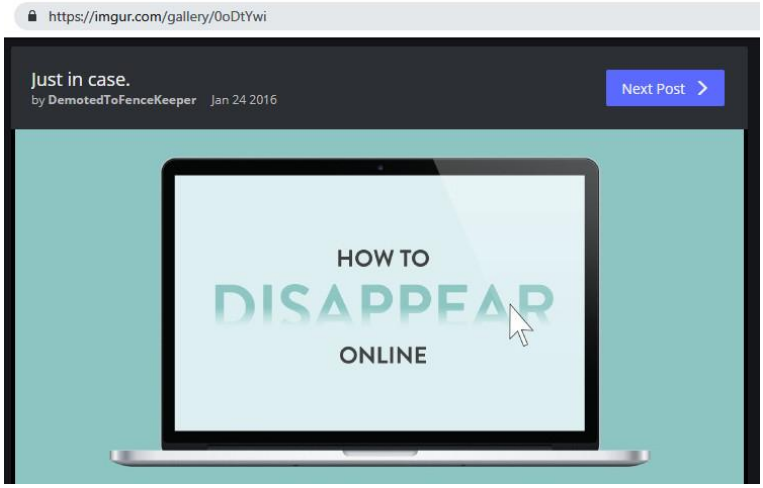


Il est même possible de télécharger une photo du visage d'une personne qui n'existe pas, créé par un algorithme, sur le site **thispersondoesnotexist.com**.

10 RÈGLES D'OPSEC

1. **Ne révélez jamais plus d'informations qu'il n'est nécessaire,**
2. **Ne faites confiance à personne sur Internet (zero trust model),**
3. **Evitez la contamination croisée de vos identités (par exemple : deux alias différents doivent se connecter à Internet à l'aide de deux appareils différents)**
4. **Soyez inintéressant pour vos ennemis afin de rester sous les radars,**
5. **Soyez constamment paranoïaque,**
6. **Ayez conscience de vos limitations (évitez d'utiliser le navigateur TOR si vous ne savez pas comment le configurer, évitez d'utiliser un VPN si vous ne savez pas ce qu'est le *kill switch*[1], …),**
7. **Minimisez les informations : les logs constituent un ennemi silencieux (il faut toujours effacer son historique dans le navigateur, …),**
8. **Utilisez des techniques d'anti-profilage : ne jamais révéler d'informations personnelles (aussi anodines soient-elles), toujours se connecter à des heures différentes et depuis des emplacements différents, (…),**
9. **Protégez vos biens : il ne faut jamais envoyer de données non chiffrées, …**
10. **Soyez professionnel : prenez les règles d'OPSEC très au sérieux. Soyez logique et systématique.**

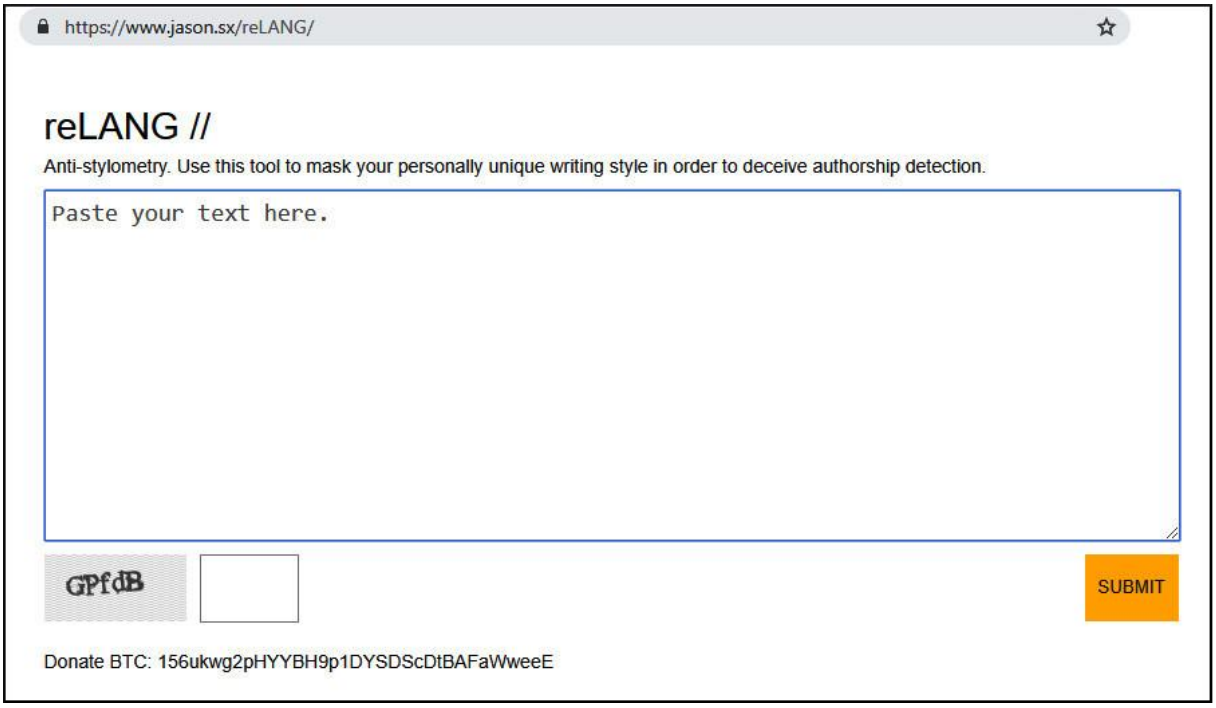
Si une contamination croisée survient, il faut faire disparaître les alias correspondants d'Internet. Vous pouvez, pour cela, suivre les conseils donnés à la page https://imgur.com/gallery/0oDtYwi [2] (cette page n'existe plus aujourd'hui) :



[1] Le kill switch est un service proposé par certains VPN (pas tous !) qui coupe totalement la communication Internet lorsque la connexion VPN ne fonctionne plus.
[2] Cette page est accessible sur la Wayback Machine (archive.org).

Il faut encore savoir qu'il est possible de relier différents alias grâce à la stylométrie (analyse statistique du style).

Un site anglais permet de contourner cette détection de paternité :



Quelques mesures d'anti-stylométrie :

1. **Utiliser des outils d'évasion comme le site ci-dessus,**
2. **Utiliser des alias multiples,**
3. **Ecrire le moins possible (plus le texte est long, plus son analyse sera probante),**
4. **Poster des textes écrits par d'autres personnes,**
5. **Imiter le style autre d'une personne,**
6. **Utiliser le *leet speak*.**

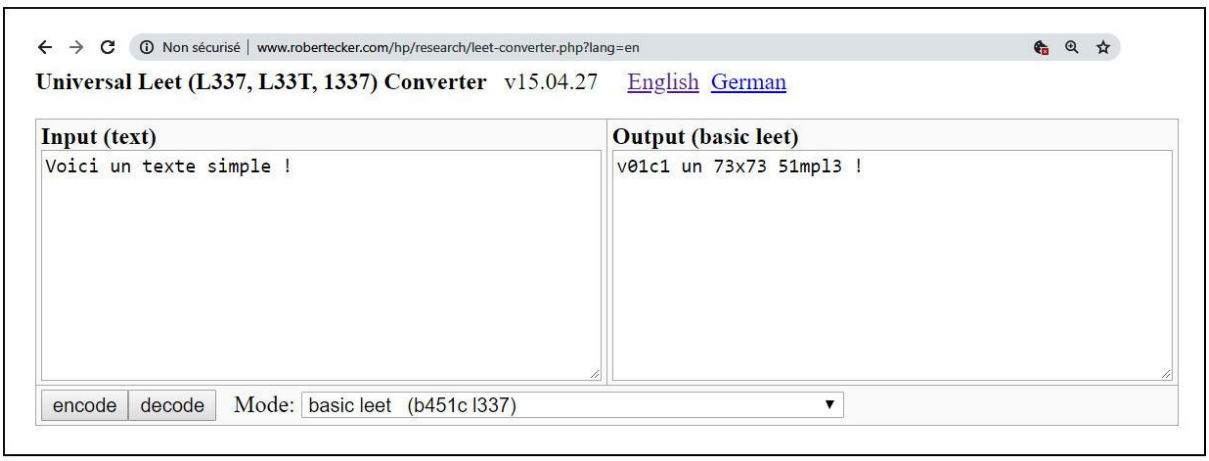
Le leet speak utilise les caractères alphanumériques de manière volontairement peu compréhensible. Par exemple, le mot SECRET pourra s'écrire $ € (Я € †.

Alphabet leet :

A	4 /\ @ ^ aye ∂ /-\ |-\ q
B	8 6 13 |3 ß P> |: !3 (3 /3)3
C	(¢ < [©
D	[) |o) I> |> ? T) |) 0 </
E	3 & € £ ɛ ë [- |=-
F	|= ƒ |# ph /=
G	6 & (_+ 9 C- gee (γ,
H	# /-/ [-]]-[ )-((-) :-: |~| |-|]~[}{]-[? }-{ hèch
I	1 ! |][eye 3y3] :
J	_| _/ ¿ </ (/ ɟ ;
K	X |< |{ ɮ < |\"
L	1 £ 1_ ℓ | |_][_,
M	|v| [V] {V} |\/| /\/\ (u) (V) (\/) /| ^^ /|/| //. .\\ /^^\ /// |^^|
N	^/ |V || /\/ [\] <\> {\}]\[// ^ [] /V ₪
O	0 () oh [] ¤ ° ([])
P	|* |o |° |^(o) |> |" 9 []D |˚ |7 ? /* ¶ /*
Q	(_,) ()_ 0_ °| <| 0.
R	2 |? /2 |^ lz ® [z 12 Я |2 ʁ |² .- ,- |°\ Я
S	5 $ z § ehs es _/¯
T	7 + -|- 1 '][' † |² ¯|¯
U	(_) |_| v L| µ J
V	\/ 1/ |/ o|o
W	\/\/ vv '// \\` \^/ (n) \V/ \X/ \\|/ \_|_/ \_:_/ Ш ɯ `^/ \./
X	>< Ж }{ ecks ×)(8
Y	7 j `/ Ψ φ ʌ ч ¥ '/
z	≥ 2 =/= 7_ ~/_ % >_ -_ '/_

Il est possible de trouver des *leet converters* en ligne :

www.robertecker.com/hp/research/leet-converter.php?lang=en

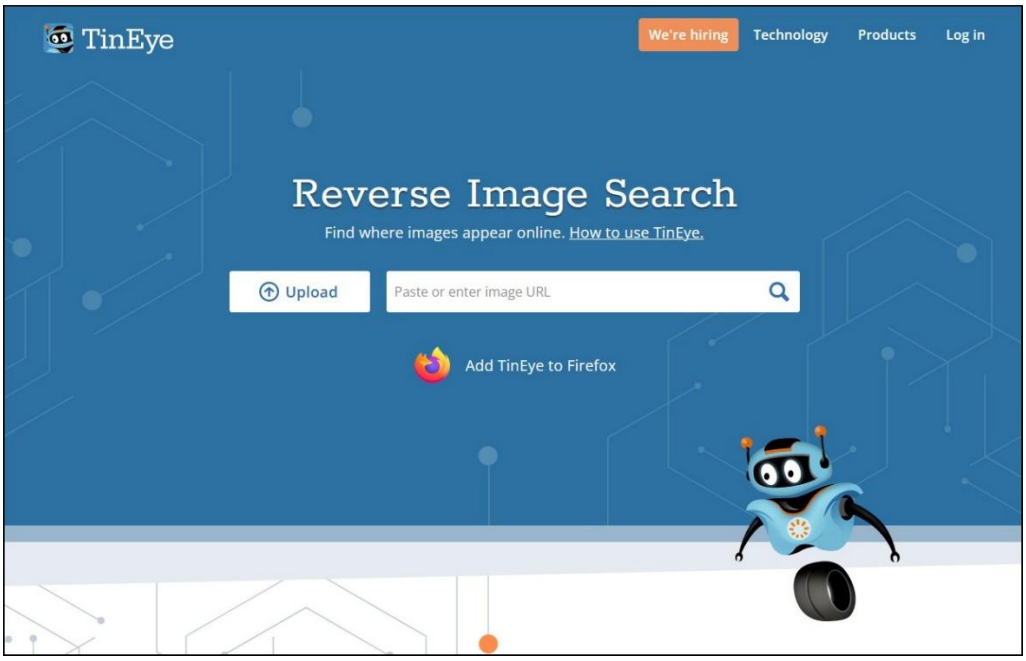


Détecter une fausse identité en ligne

Il est fréquent sur Internet de communiquer avec des personnes que vous n'avez jamais rencontrées dans la vraie vie. Ces personnes ont parfois une fausse identité et il existe des moyens de le découvrir.

Je vais vous présenter deux outils intéressants qui concernent les images que la personne est susceptible de vous envoyer :

https://tineye.com/	Ce site permet de réaliser une recherche inversée d'images. Si une personne vous envoie sa photo et que la recherche inversée dénombre des dizaines de sites hébergeant cette même photo, cela pourra vous alerter.
https://www.exiftool.org/	Ce site vous propose de télécharger un programme DOS qui permet d'examiner les métadonnées EXIF d'une image. Ces métadonnées peuvent comprendre des coordonnées GPS. Si une personne prétend habiter en Bretagne et vous envoie une photo dont les coordonnées GPS sont localisées en Amérique du Sud, il y a potentiellement un problème qui pourra ici aussi vous alerter.

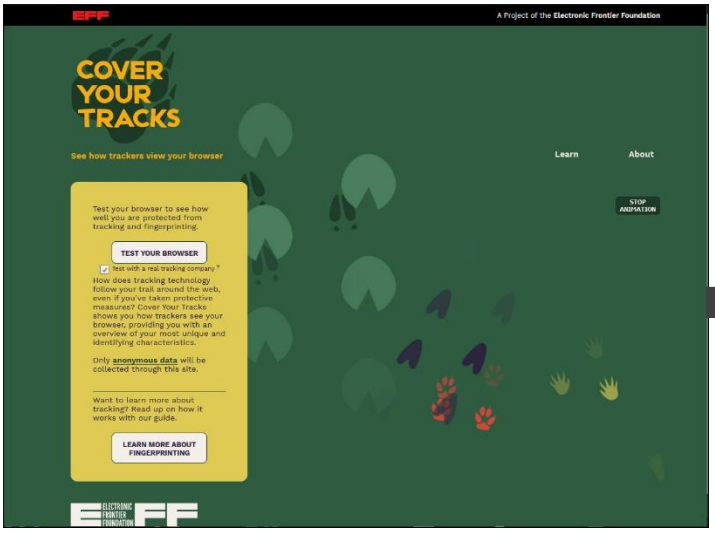


Théorie de l'information

- **La quantité d'information est mesurée en bits par l'entropie S.**
- **ΔS mesure le nombre de bits d'information que le fait x révèle**
- **Mathématiquement, $\Delta S = -\log_2 P(x)$ P(x) = probabilité de x**
- **La population terrestre est proche des 8 milliards d'individus, d'où $\Delta S = -\log_2(1/(8.000.000.000)) = 32,9$**
- **En conséquence, il est nécessaire d'obtenir 32,9 bits d'information pour identifier de façon certaine un individu.**

Voyons maintenant combien de bits d'information fuitent lors d'un surf sur Internet.

Nous allons pour cela nous servir du site https://coveryourtracks.eff.org/ **qui permet de vérifier si votre navigateur vous protège adéquatement des traceurs.**



NAVIGATEUR	FINGERPRINT
Chrome	18,1 bits
Edge	18,1 bits
Brave	18,1 bits
Firefox	18,1 bits
Tor Browser (Tails)	9,5 bits

Le navigateur TOR est le seul qui obtient un résultat honorable. Les autres transmettent, à votre insu, un nombre incalculable d'informations permettant de vous identifier.

Live Operating System

Un *Live Operating System* (live OS) est un système d'exploitation qui peut être démarré sur un CD (live CD), sur un DVD (live DVD), sur une carte SD (live SD) ou sur une clé USB (live USB), à la place du système d'exploitation installé sur le disque dur interne. Il faut configurer le BIOS (ou UEFI) pour que l'ordre de démarrage soit celui souhaité.

L'utilisation d'un live OS adéquat permet d'assurer la sécurité et le secret, mais aussi l'anonymat, si ce live OS supporte des services d'anonymisation.

Exemples de live OS		
- SÉCURITÉ +	Puppy linux	**N'est pas axé sur la sécurité.**
	Tiny core linux	**N'est pas axé sur la sécurité.**
	Knoppix	**Assure une sécurité raisonnable.**
	JonDo/Tor-Secure-Live-DVD [3]	**Assure une sécurité et un anonymat raisonnable (Tor proxy).**
	Tails [4]	**Assure une très bonne sécurité et un très bon anonymat (Tor proxy).**

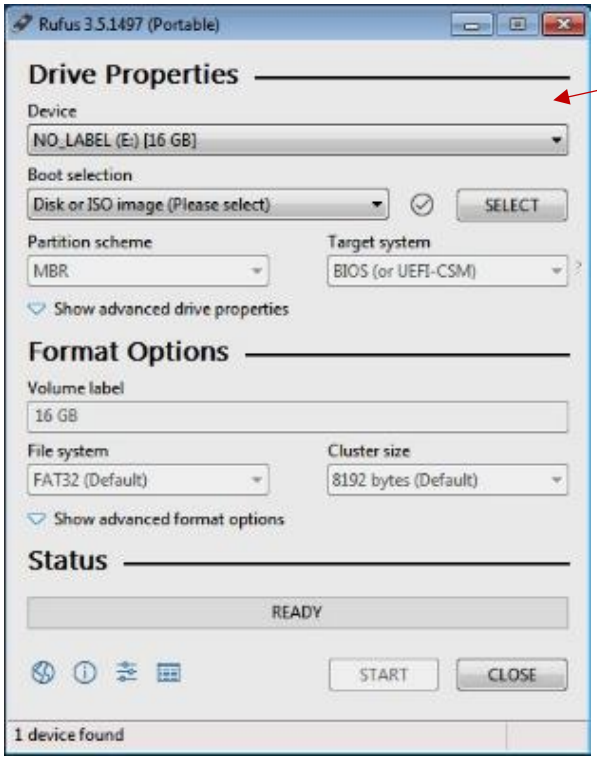
[3] **Ce live OS contient les navigateurs JonDoFox et Tor, qui permettent de surfer anonymement. La connexion réseau est inactive par défaut pour plus de sécurité. Il faut l'activer manuellement.**

[4] **Tails est le live OS sécurisé le plus utilisé pour préserver le secret et l'anonymat. Il n'est cependant pas infaillible : des failles existent. Tails ne protège évidemment pas des rootkits de firmware, il ne chiffre pas vos documents par défaut (il fournit les outils pour le faire : GnuPG pour les documents et LUKS pour les périphériques), il ne supprime pas les métadonnées de vos documents (il fournit MAT -*Metadata Anonymisation Toolkit*- pour le faire). Il faut encore utiliser des sessions différentes pour chaque alias utilisé, sinon vos différentes identités pourront être corrélées. Il faut aussi savoir que la recherche et le téléchargement de Tails sur Internet sont scrutés par la NSA et autres agences de renseignement. La désanonymisation d'un utilisateur du navigateur Tor sera plus difficile avec Tails qu'avec un autre système d'exploitation.**

Le live OS, en pratique, est un fichier .iso :

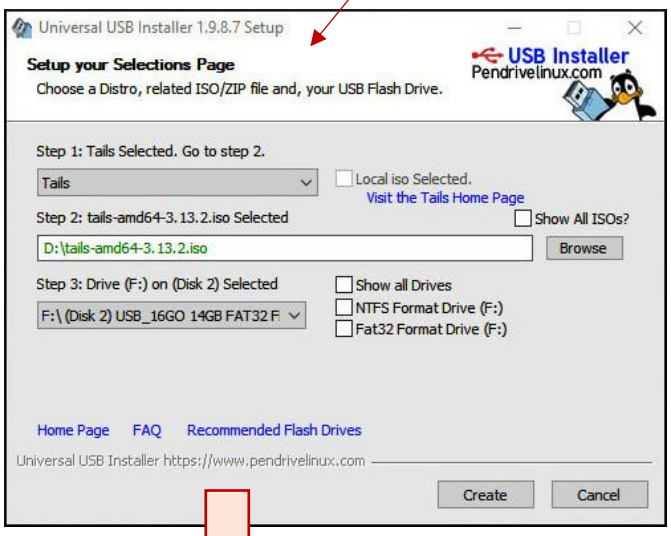
- **que l'on grave sur un CD ou DVD (le CD/DVD sera bootable)**
- **qui permet de créer un USB/SD bootable à l'aide d'un logiciel**

Pour créer l'USB bootable, on se sert de logiciels comme Rufus (https://rufus.ie), Universal USB Installer (https://www.pendrivelinux.com), ou encore Etcher :



Rufus

Universal USB Installer

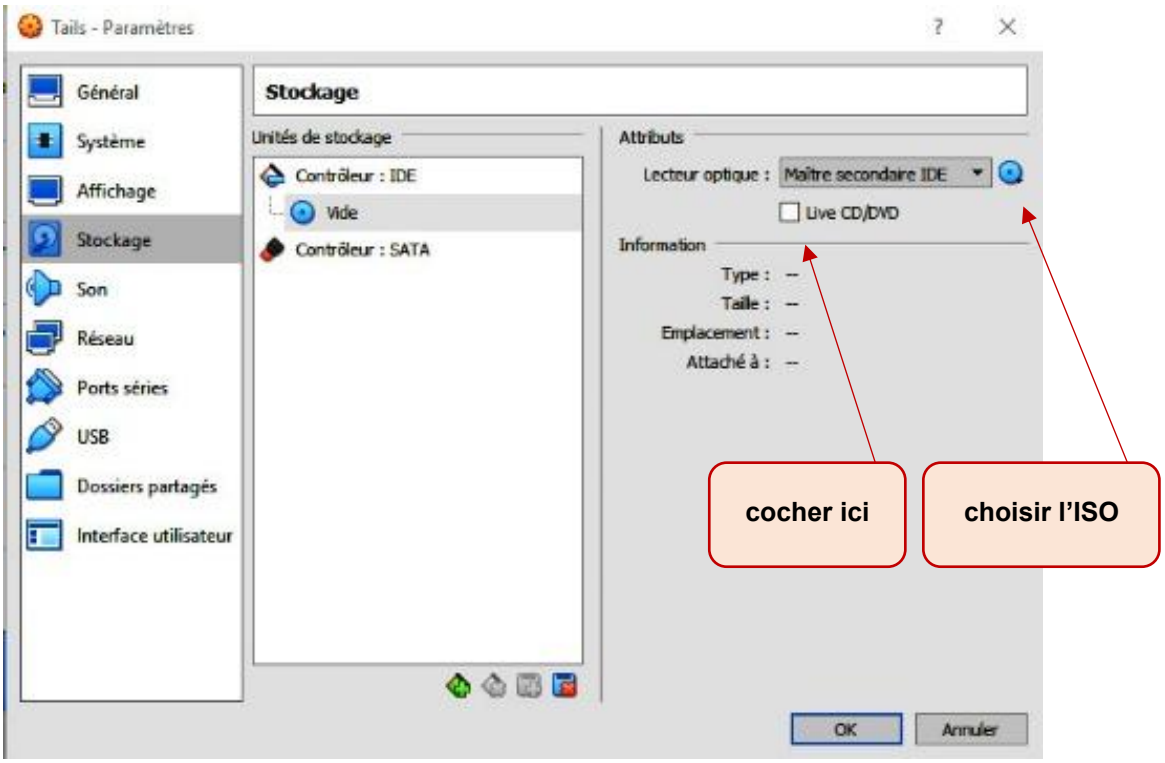


Etcher

En février 2025, Tails conseilla de remplacer balenaEtcher par Rufus pour résoudre des problèmes de confidentialité posé par l'installateur de balena.

Tails et Knoppix, une fois démarré, permettent en effet de créer directement un live USB sans devoir utiliser de logiciels.
Cela dit, il est fortement déconseillé, pour votre sécurité et votre anonymat, d'utiliser un live USB persistant.

Le live OS permet de diminuer la surface d'attaque exposée à un hacker potentiel.
Pour créer un live OS sur une machine virtuelle (ce qui n'est pas conseillé car le système d'exploitation et VirtualBox pourront voir ce que vous faites dans la machine virtuelle !), il suffit de créer une nouvelle machine (sans ajouter de disque dur virtuel pour un live OS non persistant), puis d'installer le fichier .iso comme disque optique (configuration/stockage) et de cocher l'option *Live CD/DVD* :



On peut aussi créer un live OS persistant qui sera un peu moins sécurisé puisqu'un attaquant pourra y installer une porte dérobée et que des logs seront conservés d'une session à l'autre.

Si vous souhaitez, pour une sécurité maximale, chiffrer votre live USB, je vous conseille l'Aegis Secure Key 3.0 (100€ à 400€).

<u>Une dernière mise en garde :</u>

Il est possible, pour un pirate, de récupérer via un malware le numéro de série de votre carte mère, même si vous utilisez un live OS. Ce numéro de série peut éventuellement permettre de remonter jusqu'à vous, si vous avez acheté votre ordinateur de façon non anonyme. Ceci est une faiblesse importante.

Une contre-mesure consiste à utiliser le live OS dans une machine virtuelle (sous Linux et surtout pas sous Windows) : cette dernière cache le numéro de série du hardware…

Navigateurs de JonDo/Tor-Secure-Live-DVD	
	JonDoFox
Tor	**JonDoFox**

Rester anonyme sur Internet

Il y a cinq techniques pour rester anonyme sur Internet. Aucune de ces méthodes n'est vraiment sûre à 100%, il faut le savoir. Il n'est donc pas question de se servir de cet anonymat pour avoir des agissements contraires à la loi.

L'anonymat dont on parle ici n'est valable que pour une personne qui désire ne pas être pistée sur les sites qu'elle fréquente, souvent dans un but commercial.

Méthodes pour surfer anonymement	
1	**Utiliser les services d'un cybercafé**
2	**Utiliser le navigateur TOR**
3	**Utiliser les services d'un VPN**
4	**Utiliser ProxyChains (serveurs proxy SOCKS)**
5	**Utiliser un anonymiseur gratuit (proxy web)[5]**

1) CYBERCAFÉ

Surfer sur Internet dans un cybercafé est une très mauvaise idée. Non seulement vous ne serez pas toujours anonyme (enregistrement vidéo par exemple) mais en plus, les ordinateurs de ces établissements contiennent souvent une quantité ahurissante de malwares. À éviter donc !

2) TOR

TOR est un réseau de serveurs appelés *nœuds*. Contrairement au VPN, TOR est décentralisé.
Le surf via le réseau TOR est très lent à cause du passage par les différents noeuds.
Le site visité ne verra pas l'adresse IP du visiteur mais celle du dernier nœud.
Cependant TOR n'est pas toujours recommandé car il y a beaucoup d'activités illégales qui transitent sur ce réseau. La cyberpolice surveille d'ailleurs particulièrement ce qui s'y passe.

[5] Le proxy web est un proxy dédié au web (HTTP et HTTPS)

3) VPN (Réseau Virtuel Privé)

Le VPN est un système centralisé qui vous permet de rester anonyme. Les données sont chiffrées (contrairement aux serveurs proxy) entre l'utilisateur et le serveur VPN. Le site visité ne verra que l'adresse IP du serveur VPN et pas la vôtre. Il existe des VPN gratuits et des VPN payants. Il est bon de savoir qu'un VPN gratuit est intégré au navigateur Opera.

L'intérêt des VPN est triple :

- **Les communications sont sécurisées car chiffrées.**
- **Dans les pays où sévit une dictature, le VPN permet de contourner la censure.**
- **Lorsque vous voulez accéder à certaines ressources (vidéos d'ARTE, vidéos NETFLIX, …), il faut parfois habiter un pays particulier, sinon l'accès vous est refusé. Le VPN permet d'accéder à ces ressources en vous servant d'un serveur VPN se trouvant dans le pays adéquat.**

Il est préférable d'utiliser un VPN payant pour avoir un service de qualité.

Il n'est bien sûr pas question de profiter de l'anonymat procuré par le VPN pour enfreindre la loi. En effet, le fournisseur VPN communiquera souvent votre identité à la justice en cas de requête de sa part. Personnellement, je me méfie plutôt des autoproclamés "VPN no logs" (en français : VPN sans registre d'activité).

EXEMPLES DE VPN PAYANTS (quelques dizaines d'euros par an)	
HIDE MY ASS!	NordVPN
ExpressVPN	CyberGhost
PrivateVPN	IPVANISH VPN

4) PROXYCHAINS (préinstallé sur Kali Linux) et les serveurs proxy SOCKS

ProxyChains est un logiciel qui permet de router le trafic d'une application à travers un tunnel SOCKS, il permet de socksifier d'autres applications. Le *proxy chaining* consiste à intercaler plusieurs proxys entre le client et le serveur. Il y a deux types de serveurs proxy SOCKS : SOCKS4 et SOCKS5. SOCKS4 ne supporte que TCP tandis que SOCKS5 supporte TCP, UDP et IPV6.

De nombreux serveurs proxy SOCKS4 et SOCKS5 sont gratuits, mais ils sont vraiment à déconseiller (ils sont très lents et vous pouvez être sûr qu'ils communiquent vos données personnelles, selon l'adage *: si le produit est gratuit, c'est que le produit c'est vous* !)

Il y a trois modes possibles pour ProxyChains :

1) **Mode STATIC**
   Le logiciel passe par tous les proxys de la liste. Si un proxy est non fonctionnel, la communication ne fonctionnera pas.

2) **Mode DYNAMIC**
   C'est le mode le plus utilisé. Si un proxy est non fonctionnel, le logiciel en choisit un autre.

3) **Mode RANDOM**
   Le logiciel choisit un proxy au hasard. S'il est non fonctionnel, le logiciel en choisit un autre. Le proxy change pour chaque URL.

Comment utiliser ProxyChains ?

- **Il faut éditer le fichier /etc/proxychains.conf et décommenter le mode choisi, par exemple on enlève le # de la ligne : #dynamic_chain**
- **On ajoute les proxys à la fin du même fichier, par exemple (exemple fictif) :**

```
socks4    94.180.123.89    33169
socks5    60.12.166.44     18060
socks5    77.173.17.70     1080
```

→ Ce sont les ports

- **On utilise finalement une application à travers proxychains, par exemple :**

```
proxychains firefox youtube.com
proxychains nmap -sT 156.54.78.0/24
(…)
```

→ A taper dans une console

<u>Bon à savoir</u> : se cacher derrière 20 serveurs proxy comme on le voit dans les films est totalement irréaliste : avec un seul proxy, le trafic est déjà fort ralenti !

5. ANONYMISEUR GRATUIT

L'anonymiseur (anonymizer) est un service qui permet de naviguer anonymement sur Internet. Derrière l'anonymiseur se cache un serveur proxy utilisé pour le Web (on parle alors de proxy web). Grâce à son interface web, l'anonymiseur est très simple à utiliser (pas besoin d'installation). Un anonymiseur fonctionne comme suit : il suffit de se rendre sur un site web et de taper l'adresse de la page que l'on souhaite visiter anonymement dans un champ de formulaire, et cette page s'affiche directement dans la page du site web précité. Dans la barre d'adresse du navigateur se trouve l'adresse de l'anonymiseur, pas celle de la page visitée.

EXEMPLES D'ANONYMISEURS GRATUITS	
Anonymouse.org	HIDEme
hidester	

Les inconvénients de ces anonymiseurs gratuits sont nombreux :

- **Avec certains d'entre eux, on ne peut pas visiter des sites comme Youtube, ni les sites en HTTPS.**
- **On ne peut pas toujours soumettre de formulaires ou effectuer de login.**
- **On ne peut pas télécharger de fichiers dont la taille dépasse une taille fixée.**
- **Parfois, on ne peut visiter qu'un nombre limité de pages par jour.**
- **Il y a souvent beaucoup de publicités affichées.**
- **Contrairement aux VPN, ils ne chiffrent généralement pas le trafic !**
- **Parfois, ces sites volent vos données personnelles.**

Bref, vous l'avez compris, je ne conseille vraiment pas l'utilisation de ce type de proxys pour protéger votre anonymat. A vous bien sûr de vous faire une idée.

Conclusion :

Si vous restez dans la légalité et désirez surfer anonymement sur Internet, la meilleure solution consiste, selon moi, à utiliser un VPN payant. Il faut bien sûr avoir confiance dans le fournisseur.

Les dix risques majeurs pour la vie privée

Source : https://owasp.org/www-project-top-10-privacy-risks/

1	Application avec vulnérabilités
2	Fuite de données par l'opérateur
3	Mauvaise réponse suite à une fuite de données
4	Suppression insuffisante des données personnelles
5	Conditions d'utilisation opaques
6	Collecte de données excessive
7	Partage de données
8	Données personnelles périmées
9	Expiration de session manquante ou insuffisante
10	Transmission de données non sécurisée

Extensions de navigateur qui améliorent le respect de la vie privée

Rôle	Extensions	Alternatives
Suppression des publicités	**AdBlock et Adblock Plus**	**uBlock**
Blocage des traceurs	**Privacy Badger**	**Disconnect.me**
Injection locale des librairies	**Decentraleyes**	**- - - - -**

➔ **Decentraleyes injecte localement les librairies et bibliothèques de code, ce qui protège du pistage et accélère la vitesse de navigation.**

➔ **AdBlock et Adblock Plus sont deux extensions concurrentes.**

		
AdBlock	Adblock Plus	uBlock Origin

		
Privacy Badger	Disconnect	Decentraleyes

Vérifier une application Android avec Exodus Privacy

Exodus Privacy est une association à but non lucratif qui analyse les applications Android gratuites dans le but d'y débusquer les pisteurs et permissions :

- ➔ Les pisteurs collectent diverses données sur l'utilisateur : ils peuvent être totalement justifiés (pour rapporter un plantage par exemple) ou plus intrusifs (pour effectuer un profilage ou déterminer une localisation). Ils sont contenus dans des SDK (Software development Kit) parfois même à l'insu du développeur.
- ➔ Les permissions donnent accès à vos données : localisation, photos et fichiers, micro, caméra, …

SMS Tracker

Exemple d'application Android peu problématique.

0 pisteur

4 permissions

Version 5.0.3 - voir les autres versions
Source : Google Play
Créée par VlaPo
Téléchargements : 50,000+
Rapport créé le 3 août 2018 14:02 et mis à jour le 29 avril 2022 14:53

TeamViewer

1 seul pisteur mais quand même 20 permissions demandées !

1 pisteur

20 permissions

Version 15.34.152 - voir les autres versions
Source : Google Play
Rapport créé le 18 octobre 2022 06:59

Voir sur Google Play >

CLEANit

Application à éviter à tout prix : 11 pisteurs et 159 permissions !

11 pisteurs

159 permissions

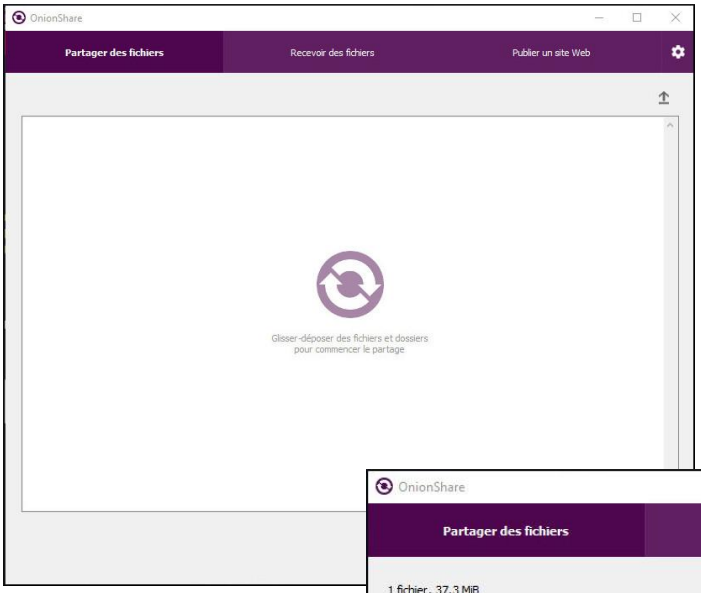
Version 1.9.28_ww - voir les autres versions
Source : Google Play
Rapport créé le 1 août 2021 10:02 et mis à jour le 28 avril 2022 02:45

Voir sur Google Play >

Échanger des fichiers de façon anonyme

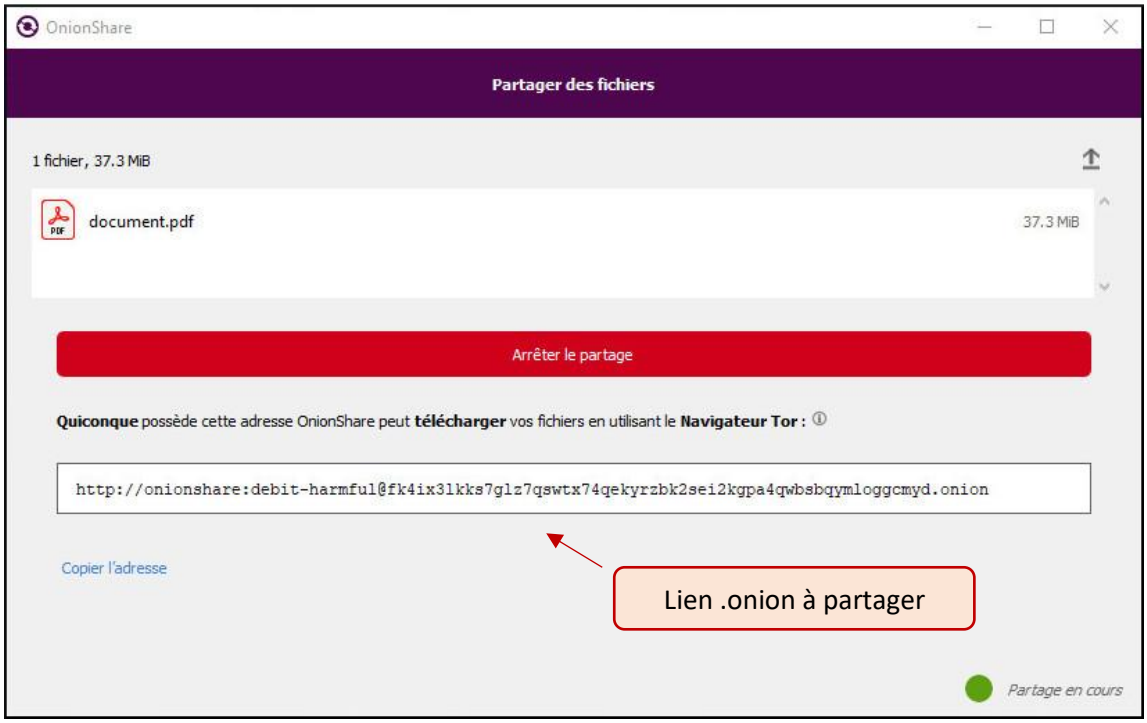
Échange de fichiers	Remarques
OnionShare	Outil open source pour Windows et MacOS : via Tor

Démonstration

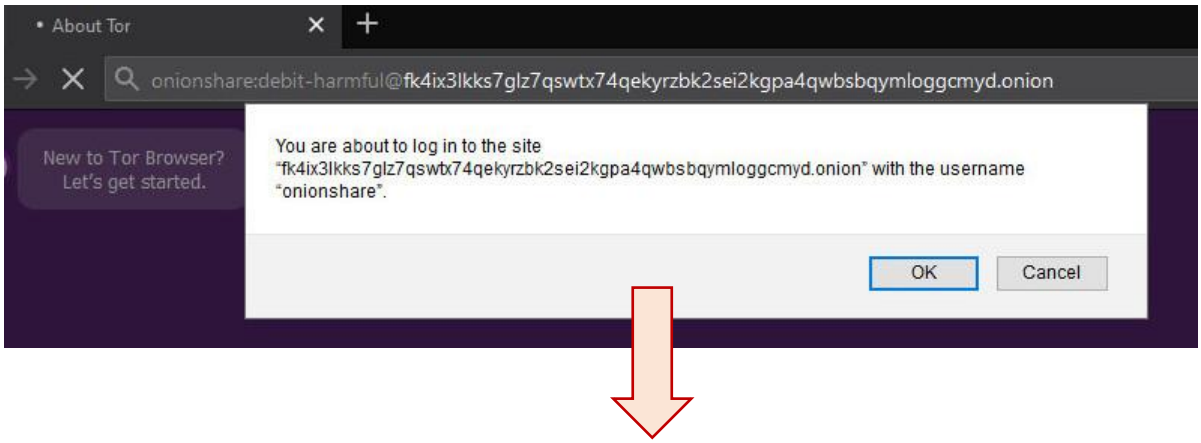


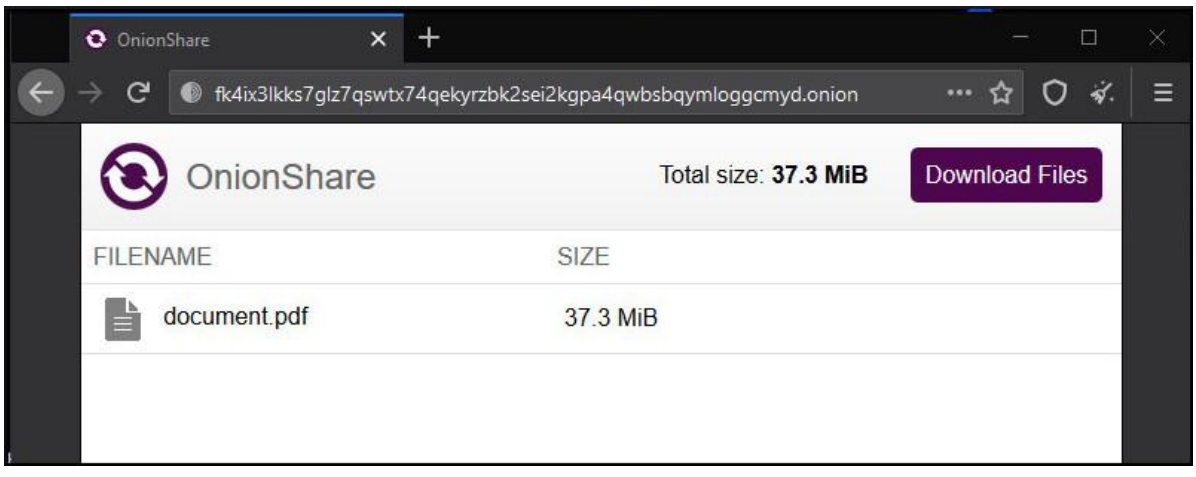
Après avoir installé le programme, on fait un glisser-déposer du fichier à échanger dans la fenêtre de l'outil.

Le fichier apparaît alors et il suffit de cliquer sur "**Commencer le partage**"



On peut alors, depuis n'importe quel ordinateur, et à l'aide du navigateur Tor, télécharger le document disponible sur un site en .onion :



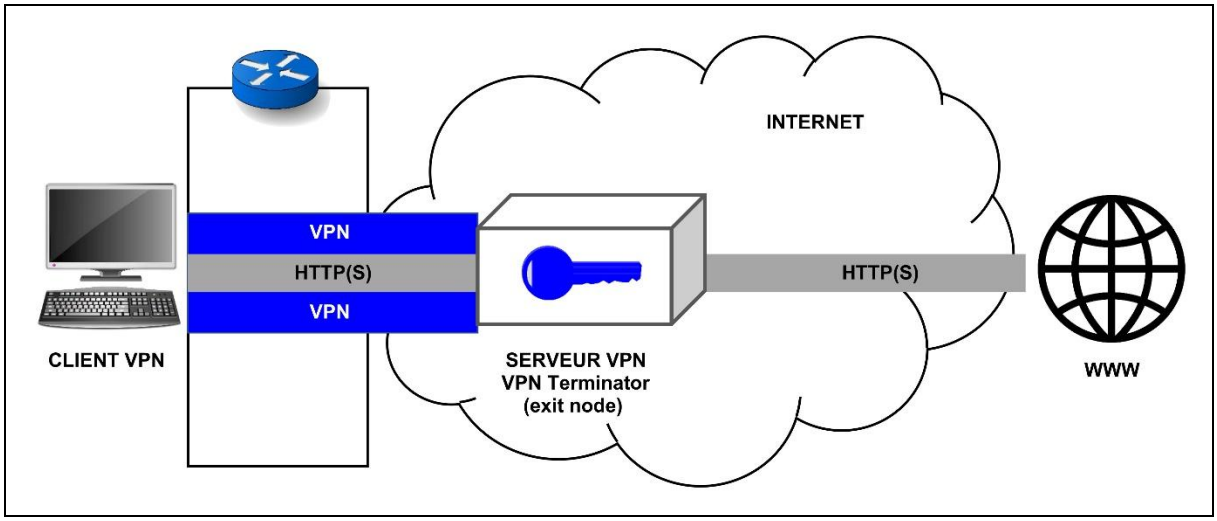


VPN (Virtual Private Network)

Il existe de nombreux services d'anonymisation :

- **Tor**
- **JonDoNym**
- **Tunnel SSH**
- **Proxys**
- **Freenet**
- **I2P [6]**
- **VPN**

Nous nous intéresserons dans ce chapitre au VPN, qui est le service le plus simple à utiliser. Il est simple mais d'une efficacité relative puisque les fournisseurs VPN communiquent vos données de connexion à la police, en cas de requête officielle, ce qui est un problème dans un régime totalitaire.



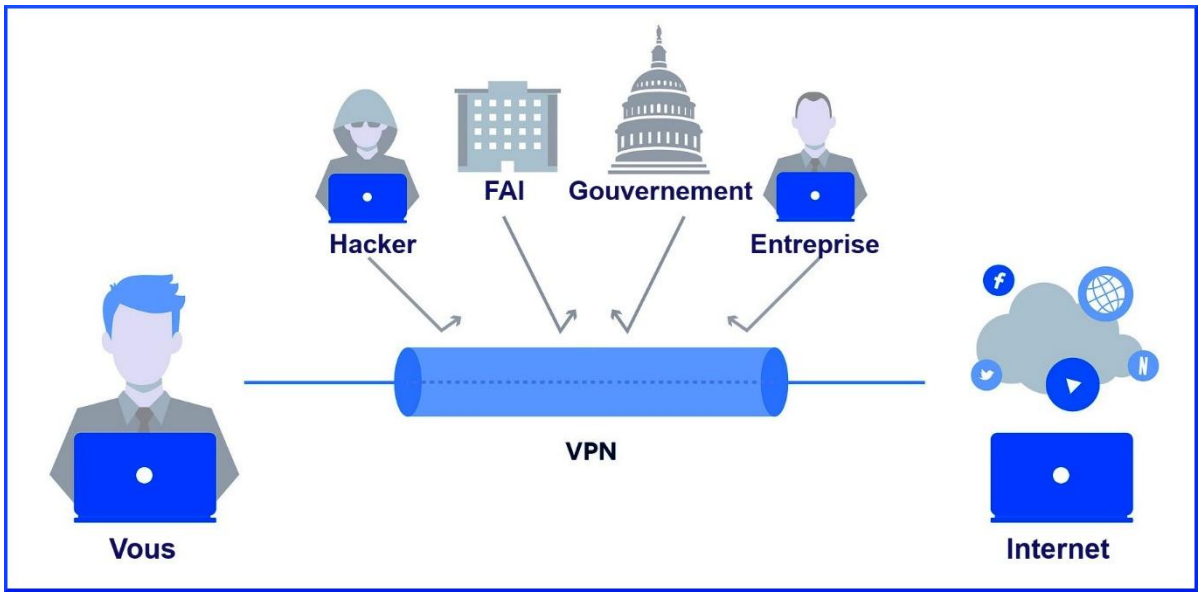
On peut bien évidemment installer également le client VPN sur le routeur d'une entreprise plutôt que sur chaque ordinateur du réseau interne.
On peut encore installer le VPN client sur une machine virtuelle. Cela est utile pour créer des VPN imbriqués (nested VPNs) : on installe un client VPN sur la machine virtuelle et un autre client VPN sur la machine hôte. Cela crée un double chiffrement des données. Les hackers se servent de ce type de configuration pour cacher leurs activités illégales.

[6] **I2P est un réseau anonyme qui permet de visiter les sites .i2p uniquement. On n'a pas accès à l'Internet classique avec I2P (sauf via un OutProxy, mais ce n'est pas conseillé). L'anonymat, à l'intérieur du réseau I2P est bon, mais n'est pas infaillible !**

Comme dit précédemment, les VPN ne protègent pas de la police, mais bien des hackers et trackers, qui ne pourront plus voir le trafic en clair. Le fournisseur d'accès à Internet (FAI ou, en anglais, ISP) ne pourra lui non plus lire le trafic en clair. Cela peut être utile. Un autre avantage des VPN est leur capacité à contourner la censure et les restrictions géographiques.

Une question vous taraude : pourquoi utiliser un VPN si le trafic est un trafic chiffré HTTPS ? Simplement pour la capacité des VPN à masquer votre IP et à vous procurer un certain anonymat, ce que n'assurent pas le seul chiffrement SSL/TLS.

De nombreuses personnes étant connectées en même temps à l'*exit node*, cela procure un certain degré d'anonymat.



Utilité des VPN :

Le VPN chiffre le trafic, comme pourrait le faire SSL/TLS (avec HTTPS), mais il permet en plus de masquer votre IP et de cacher les sites visités à votre fournisseur d'accès à Internet (FAI).

Il existe de nombreux protocoles VPN
(PPTP, OpenVPN, L2TP sur IPsec, SSTP, IKEv2, OpenConnect, …)

PPTP

Protocole propriétaire (Microsoft) qui n'est plus du tout recommandé aujourd'hui à cause de failles multiples.

SSTP

Il s'agit d'un autre protocole propriétaire (toujours Microsoft) qui est utilisé uniquement avec Windows et qui n'est pas toujours bien supporté par les fournisseurs VPN. Quand on sait avec quel dynamisme Microsoft collabore avec la NSA, cela ne nous rassure pas quant à l'utilité de ce protocole. Je ne le recommande pas du tout.

L2TP sur IPsec

IPsec fournit le chiffrement non disponible avec L2TP. Les systèmes d'exploitation récents supportent ce protocole. Il est de plus facile à installer. Malheureusement, ce protocole utilise des ports fixes, ce qui est un désavantage car les firewalls pourront bloquer facilement le trafic. Sinon, c'est un bon choix, si votre ennemi n'est pas une agence de renseignement (la NSA peut déchiffrer le trafic utilisant ce protocole). L2TP sur IPsec vous protègera des hackers et trackers. Il est conseillé d'utiliser l'algorithme de chiffrement AES 256.

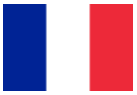
OpenVPN

OpenVPN est un protocole open source. Ses ports sont configurables (gros avantage). Ce protocole est plus rapide avec UDP qu'avec TCP. Il est ici aussi conseillé d'utiliser l'algorithme de chiffrement AES 256.
OpenVPN n'est pas supporté nativement par tous les systèmes d'exploitation, ce qui est son seul désavantage.
Si votre ennemi est une agence de renseignement, OpenVPN est le protocole à utiliser, avec prudence. Il s'agit du meilleur protocole VPN.

Faiblesses des VPN

1. **Ils ralentissent le trafic à cause du chiffrement. Les VPN sont malgré tout plus rapides que d'autres services d'anonymisation comme Tor, JonDoNym et I2P.**
2. **Ils ne cachent votre identité qu'aux hackers et pas à la police, ni aux agences de renseignement. Si vous souhaitez un anonymat renforcé, il faut utiliser Tor et les VPN imbriqués (nested VPNs). Le VPN n'est donc qu'un morceau de la solution pour vous anonymiser efficacement et totalement.**
3. **En Iran et en Chine, si un trafic VPN est détecté, il sera bloqué. On peut contourner cette détection avec des outils comme Stunnel ou encore obfsproxy (qui masque le trafic VPN en le transformant en trafic innocent, on parle d'obfuscation).**
4. **Les VPN gratuits sont lents. Pour un VPN rapide, il faudra payer (5 à 10 euros/mois). Il faut être prudent car le paiement des VPN peut permettre de remonter jusqu'à vous. Il faut, en cas de besoin, penser à payer en cash ou en bitcoins.**
5. **Plutôt que de tenter de déchiffrer le trafic VPN, une agence de renseignement peut utiliser une attaque de type *end-to-end correlation*. Dans ce type d'attaque, il est possible de désanonymiser un client VPN en observant la taille du trafic. Si un serveur envoie 10 Mo de données au terminateur VPN et qu'un trafic chiffré renvoyé par ce terminateur à un client VPN fait aussi 10 Mo, on aura identifié l'origine de la requête initiale. Ce type d'attaque est une faiblesse des VPN et de Tor.**
6. **Le VPN ne protège pas des attaques côté client (exploitation du navigateur, ingénierie sociale, phishing, XSS, …)**
7. **Si le contenu d'une page est connu par avance, une agence de renseignement pourra, grâce à la technique du *website fingerprinting*, connaître le contenu d'un trafic chiffré. Chaque page visitée possède en effet un *pattern* unique.**
8. **L'envoi de mails via SMTP est souvent bloqué par les fournisseurs VPN. En effet, les spammeurs se servent des VPN pour envoyer leurs pourriels, ce qui est un réel problème.**
9. **Netflix bloque aujourd'hui les trafics VPN.**
10. **Un compte peut être bloqué si vous utilisez un VPN car l'activité du compte sera jugée suspecte (connexions rapprochées provenant de multiples positions géographiques, …).**
11. **Pour assurer complètement votre anonymat, un VPN ne suffit pas. Il faut utiliser des VPN imbriqués (nested VPNs).**
12. **Certains fournisseurs VPN doivent être évités car ils se situent dans des pays où les agences de renseignement sont très actives et ont signé un traité d'alliance impliquant l'échange d'informations. C'est le cas des services VPN localisés dans les Five Eyes, et dans une moindre mesure de ceux situés dans les Nine Eyes ou Fourteen Eyes. Ces pays sont dangereux si vous désirez rester anonyme.**

FIVE / NINE / FOURTEEN EYES

Australie	
Canada	
Nouvelle-Zélande	
Royaume-Uni	
Etats-Unis	
Danemark	
France	
Hollande	
Norvège	
Allemagne	
Belgique	
Italie	
Suède	
Espagne	

5 EYES

9 EYES

14 EYES

Les VPN basés dans ces 14 pays doivent être évités si vous vous souciez de votre confidentialité en ligne !

Installer OpenVPN sur Windows

Il suffit d'utiliser le fichier d'installation proposé sur le site d'OpenVPN. Ensuite, il faut copier les fichiers .ovpn (par exemple France.ovpn) dans le répertoire Program Files/openVPN/config pour pouvoir se connecter aux VPN en question (on clique sur l'icône d'OpenVPN dans la barre des tâches et on clique ensuite sur *connecter*). Il faut lancer OpenVPN en administrateur. Il y a éventuellement un mot de passe à introduire.

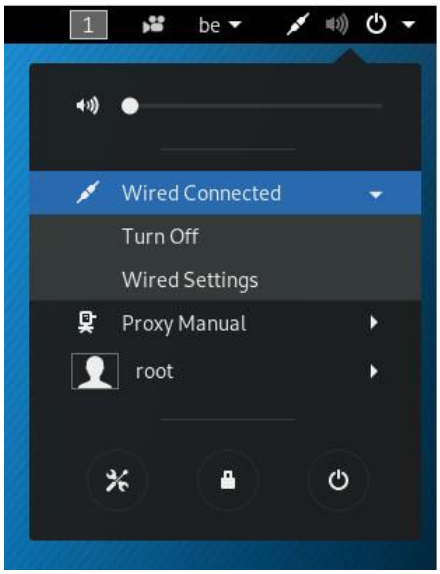
Installer OpenVPN sur Linux

OpenVPN est installé par défaut sur Kali Linux. Si ce n'est pas le cas, on tape dans un terminal :

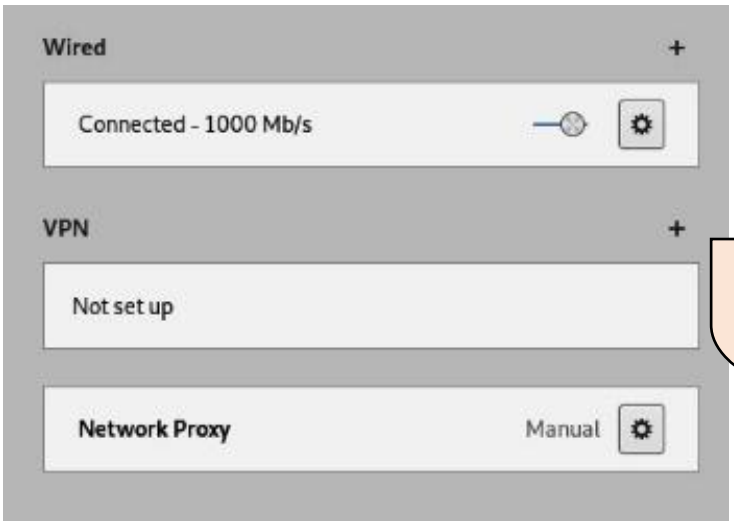
sudo apt-get install openvpn

Il faut ensuite installer le manager (il n'est pas installé par défaut sur Kali) :

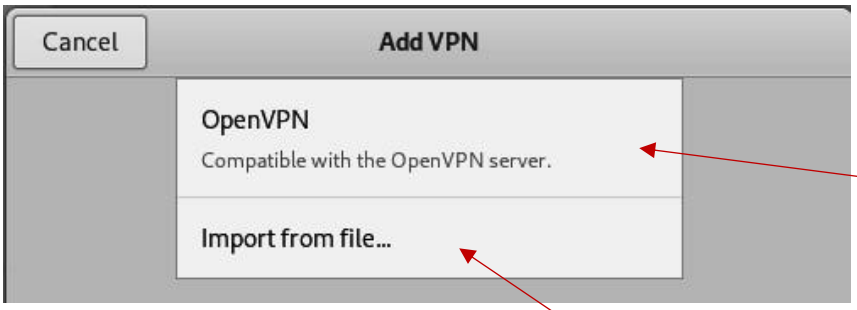
sudo apt-get install network-manager-openvpn-gnome



On clique maintenant sur Wired Connected/Wired Settings



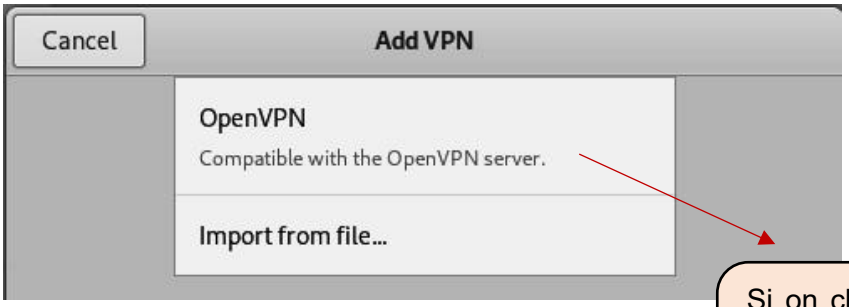
On clique ensuite sur le +



Cette option apparaît grâce à l'installation du manager

Cette deuxième option permet d'importer un fichier .ovpn présent sur le disque dur. Dans ce cas, le VPN sera configuré automatiquement.

Si cela ne fonctionne pas, il faudra extraire les certificats et la clé du fichier .ovpn et importer ces fichiers séparément, comme indiqué page suivante…



Si on clique sur cette option, on peut configurer manuellement son VPN.

Il faut indiquer l'emplacement :

- du certificat du serveur (ca.crt),
- du certificat du client (client.crt),
- de la clé privée du client (client.key)

Ici se trouvent les options avancées.

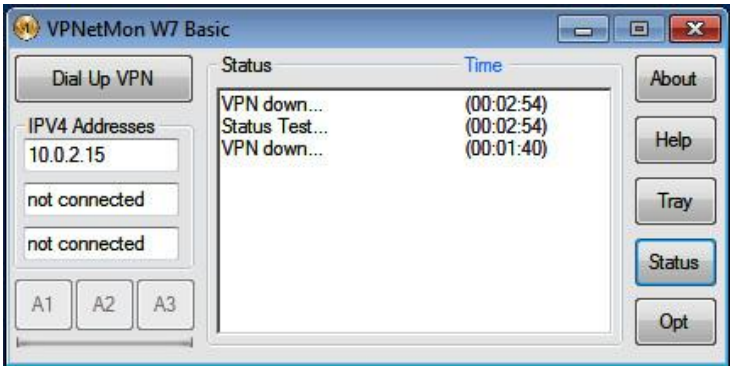
Problèmes causés par les VPN :

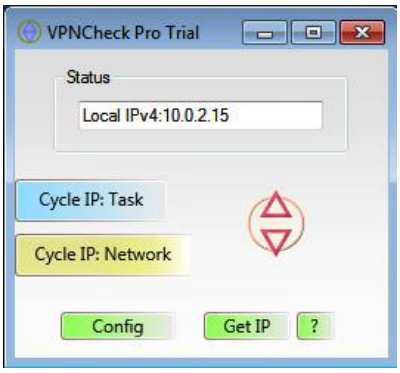
Si le VPN arrête de fonctionner, tout le trafic pourra être envoyé directement à sa destination finale. Vous serez totalement désanonymisé.

Un autre problème est celui des fuites DNS avec IPv6 qui permettent d'identifier le site que vous êtes en train de visiter. Une fuite DNS est une requête DNS envoyée en dehors du tunnel VPN encrypté. Cela arrive lorsque vous utilisez à la fois IPv4 et IPv6 avec un client VPN sans support IPv6. Cela arrive aussi avec Windows 8, 10 et 11 (il n'est pas toujours possible de désactiver la fonction *Smart Multi-Homed Name Resolution)*

Les contre-mesures sont :

- **On peut désactiver IPv6 via le système d'exploitation, ou via certains clients VPN (le choix du client est donc primordial).**
- **On peut choisir un client VPN doté du kill switch.**
- **On peut établir des règles firewall qui bloquent le trafic non VPN.**
- **Il existe des applications qui permettent de stopper instantanément un programme si le VPN se déconnecte. Par exemple : vpnetmon (gratuit) et vpncheckpro (payant).**





A RETENIR

Il est déconseillé d'installer un client VPN sur Windows 10 et 11 à cause des fuites DNS intempestives générées par ces systèmes d'exploitation.

Que peut-on contourner avec un VPN ?	Que ne peut-on pas contourner ?
• **La surveillance passive du trafic,** • **Certaines attaques de hackers,** • **Les dangers liés aux Wi-Fi publics gratuits (hôtels, aéroports, …),** • **Le monitoring du FAI (ISP),** • **Une restriction géographique (attention : Netflix, par exemple, bloque les VPN),** • **La censure (dictatures),** • **Le blocage DNS qui bloque les requêtes DNS associées à certains domaines. Une entreprise peut, par exemple, bloquer toutes les requêtes pour les réseaux sociaux…**	• **La surveillance de la police,** • **La surveillance du gouvernement,** • **La surveillance des agences de renseignement.**

Que peut-on faire d'autre avec un VPN ?	Les fausses promesses des opérateurs VPN
• **Cacher son IP aux serveurs visités,** • **Surfer anonymement sur Internet,** • **Joindre des hôtes ou des réseaux distants en un seul réseau privé sécurisé,** • **Permettre l'accès distant sécurisé pour les employés d'une entreprise en télétravail,** • **Protéger les utilisateurs contre le suivi en ligne.**	• **Nous protégeons votre ordinateur des menaces d'Internet : c'est faux car les VPN ne protègent que les connexions non sécurisées (HTTP) via un Wi-Fi public, ce qui ne correspond qu'à un type d'attaques parmi toutes celles possibles !** • **Nous protégeons vos données personnelles : c'est faux car un service VPN dont le siège social est situé dans un paradis fiscal est potentiellement plus dangereux que le FAI national respectant les lois européennes !** • **Nous garantissons la non-conservation des logs : c'est en fait impossible à vérifier et c'est souvent faux pour des raisons de législation !**

Quelques conseils pour choisir un fournisseur VPN

- **Pas de VPN situé dans la sphère d'influence de votre adversaire,**
- **Pas de journalisation (politique no-logs) : seulement si la juridiction le permet,**
- **Paiement anonyme autorisé (cash ou bitcoins),**
- **Logiciel VPN client prévenant les fuites (DNS, IPv6, kill switch),**
- **Serveurs DNS propres au fournisseur,**
- **Serveurs VPN physiquement sous le contrôle du fournisseur,**
- **Lecture attentive des conditions d'utilisation et de la politique de confidentialité,**
- **Fournisseur offrant OpenVPN avec un bon chiffrement,**
- **Le mot de passe doit pouvoir être changé,**
- **Le service doit permettre le port forwarding.**

Quel VPN peut-on conseiller ?

Le VPN qui possède ma préférence est Proton VPN, dont le siège social est situé en Suisse, pays où la protection des données est très stricte.

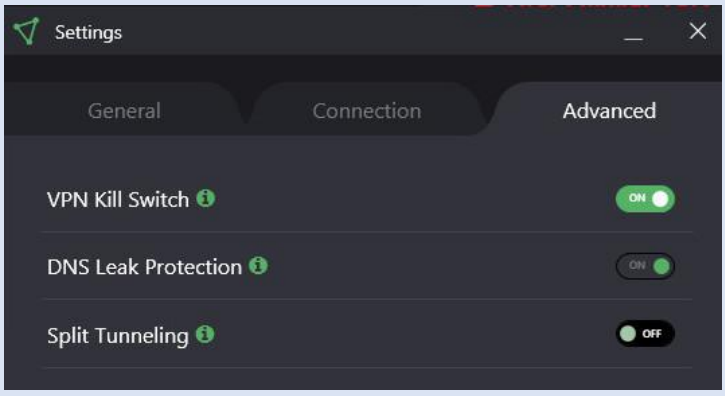
Proton VPN possède deux fonctionnalités très intéressantes :

- ➔ **Kill Switch : votre connexion est bloquée si le VPN a une défaillance**
- ➔ **Secure Core : le trafic passe par plusieurs serveurs pour augmenter votre sécurité (si, par exemple, un serveur spécifique est compromis)**

Voyons cela :

ProtonVPN

ProtonVPN est un VPN proposé par la même firme suisse qui gère le célèbre service mail sécurisé ProtonMail.

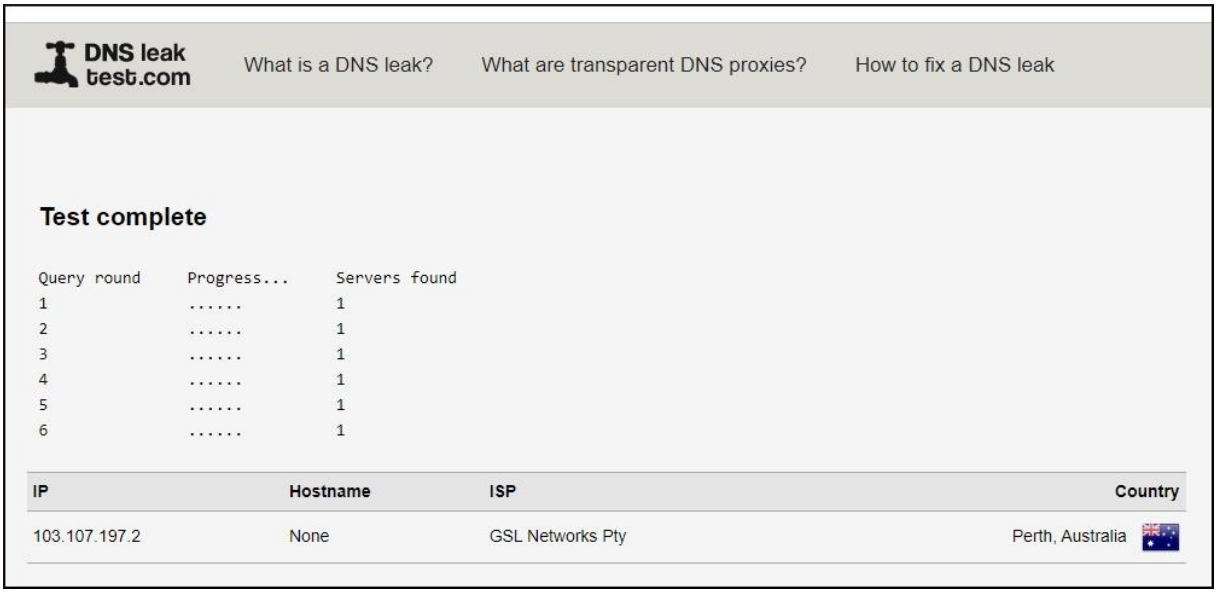


Ce VPN est doté du Kill Switch et d'une protection contre les fuites DNS. Génial !

L'option Secure Core permet d'utiliser un VPN multiple dont le premier nœud est situé dans un pays qui respecte l'anonymat (Suisse, Islande ou Suède)

VPN/TOR : rechercher des fuites IPv6 & DNS

Lors de l'utilisation d'un VPN, il est possible de constater une fuite DNS qui permet de retrouver votre véritable adresse IP. Si vous voulez vérifier que votre VPN n'a pas de telle fuite, vous pouvez visiter le site **https://dnsleaktest.com/** :



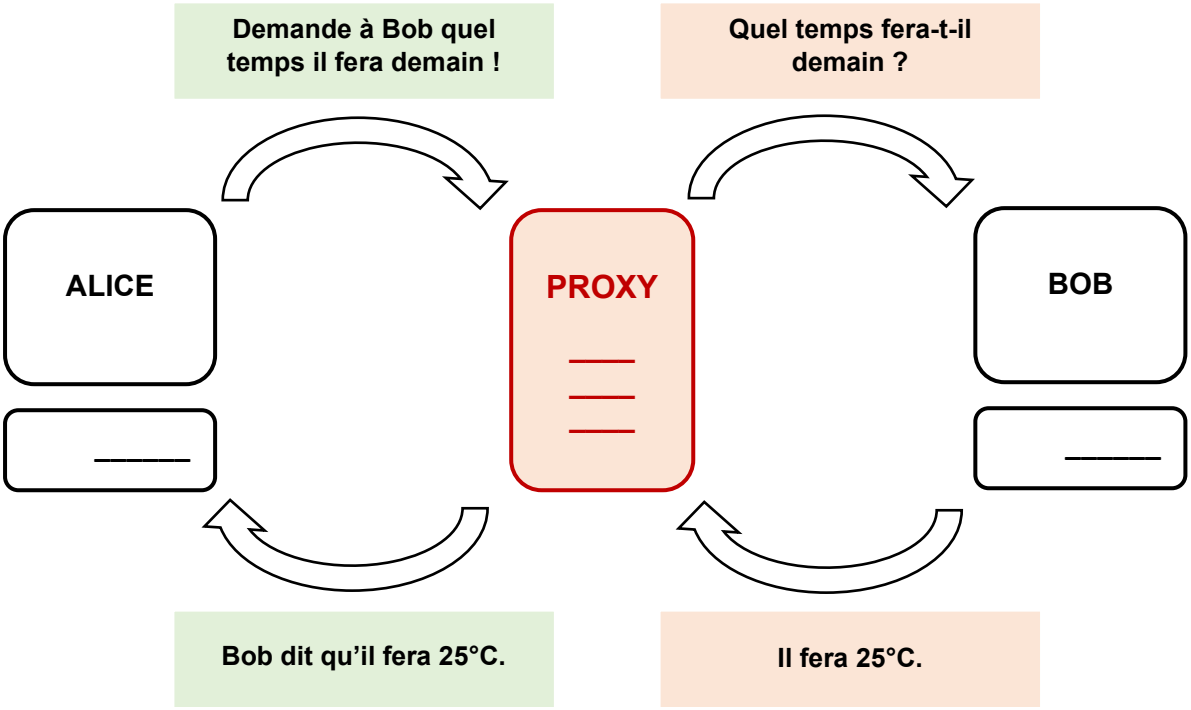
Cette recherche ne montre qu'un serveur étranger : ce VPN n'a donc pas de fuites DNS !

Pour les fuites IPv6, vous pouvez visiter le site **https://www.ipv6leak.com/** :

Les serveurs proxy

Un proxy est un serveur servant d'intermédiaire entre deux hôtes, facilitant ou surveillant les échanges.

Schématiquement, voici le fonctionnement d'un serveur proxy :



Il existe différents types de serveurs proxy :

- **proxys web :**
  - **proxys HTTP : pour les pages web**
  - **proxys HTTPS : pour les pages web sécurisées**
- **proxys FTP**
- **proxys SOCKS4 et SOCKS5[7] : fonctionne au niveau TCP/IP**

Les proxys peuvent permettre de surfer sur Internet en cachant son IP réelle, un peu comme les VPN, mais sans le chiffrement. Il n'y a donc aucun programme à installer, il faut juste configurer les applications afin qu'elles utilisent le proxy.

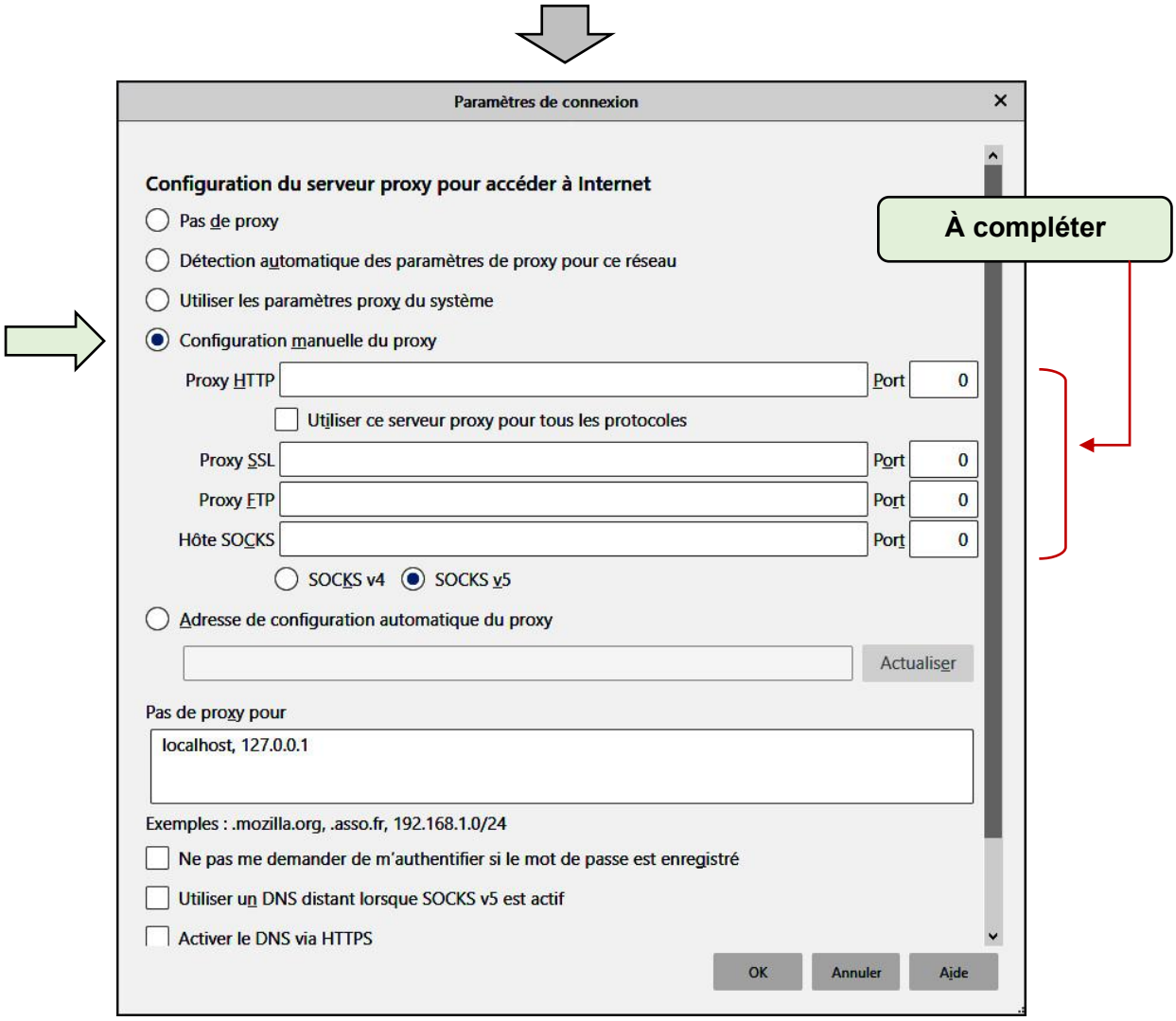
[7] Les proxys SOCKS4 n'autorisent pas les DNS distants ni UDP, contrairement aux proxys SOCKS5 (qui supportent aussi IPv6).

TYPES DE SERVEURS PROXY

Selon leur fonction	**On distingue :** ➔ **Le proxy direct (Forward Proxy)** **Il permet à des clients de demander des ressources sur Internet. Il peut être transparent, anonyme, …** ➔ **Le proxy inverse (Reverse Proxy)** **Il permet de filtrer le trafic provenant d'Internet et destiné à des serveurs internes. Il est utilisé par exemple pour la répartition de charge (Load Balancing).**
Selon l'anonymat	**On distingue :** ➔ **Le proxy transparent** **Il ne cache pas votre IP.** ➔ **Le proxy anonyme** **Il cache votre IP mais il s'identifie comme serveur proxy.** ➔ **Le proxy à haut anonymat (Elite)** **Il cache votre IP et aussi son statut de proxy.**
Selon le protocole	**On distingue :** ➔ **Le proxy web (le plus courant)** **Il utilise soit HTTP, soit HTTPS. Permet la navigation sur Internet, la mise en cache (pour accélérer l'accès aux sites fort sollicités) et le filtrage d'URL dans une école ou une entreprise (interdiction d'accès aux réseaux sociaux, …).** ➔ **Le proxy FTP** **Plus rare, il permet le transfert de fichiers.** ➔ **Le proxy SOCKS4 et surtout SOCKS5** **Proxy avancé, il ne se limite pas à un seul protocole. Presque tous les trafics possibles via TCP ou UDP sont autorisés.**
Selon l'accessibilité	**On distingue le proxy public ou ouvert (lent et peu fiable) et le proxy dédié ou privé (plus rapide et moins blacklisté).**

Par exemple, on peut configurer Firefox afin qu'il utilise un proxy :

Options / Paramètres réseau / Paramètres de connexion



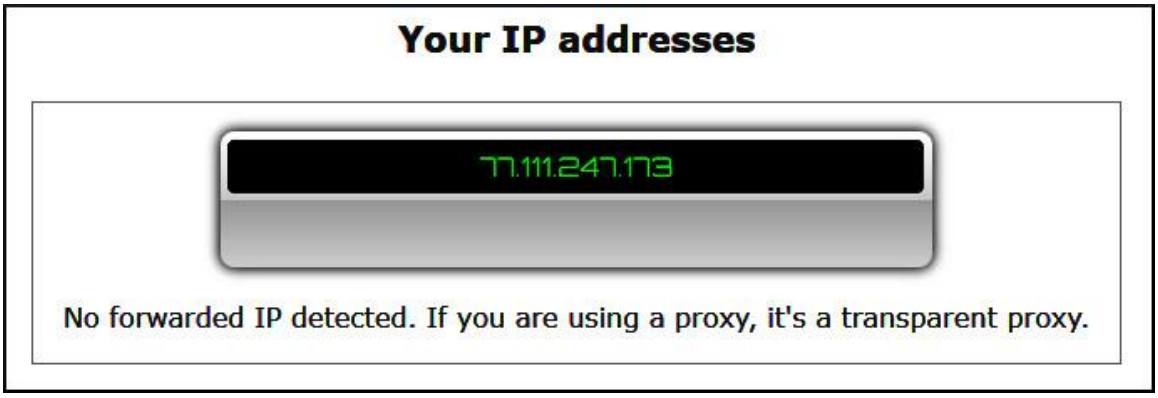
Les proxys sont plus rapides que les VPN à cause de l'absence de chiffrement. En contrepartie, l'anonymat qu'ils procurent est moins solide.

Pour une gestion aisée de vos proxys, il est conseillé d'installer l'extension FoxyProxy pour Firefox.

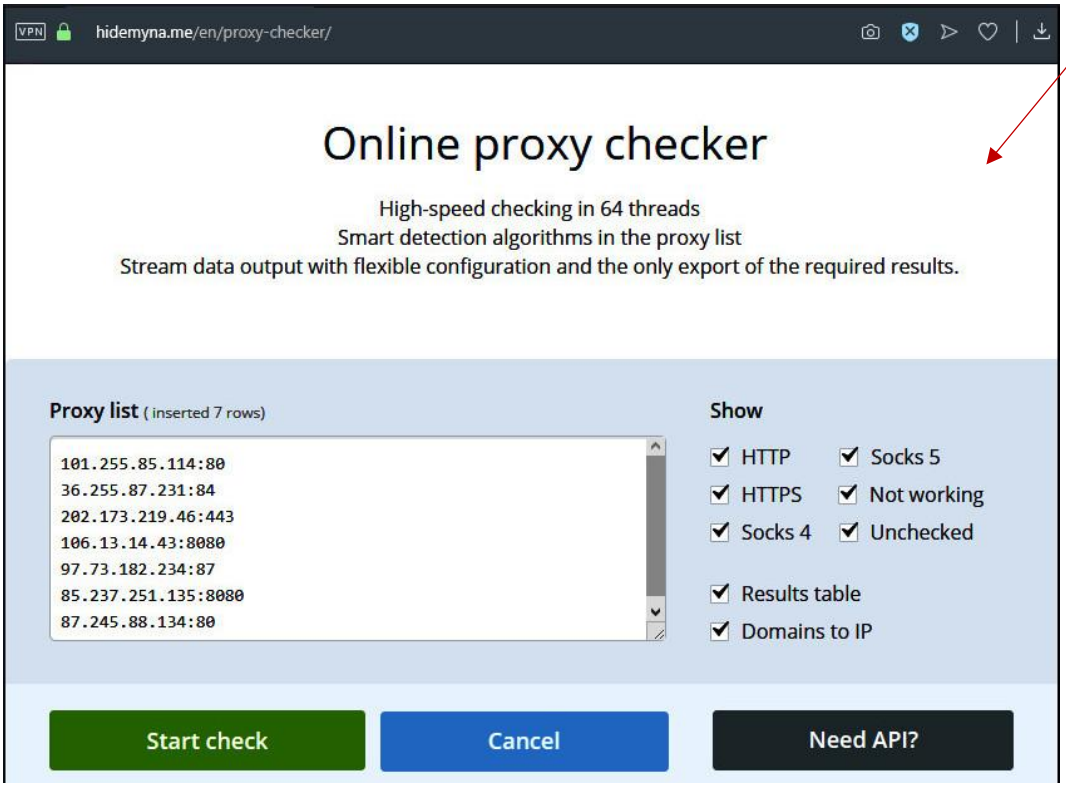
Il existe des listes de proxys gratuits sur Internet (ils sont à éviter absolument à cause du risque de vol de données ou même d'attaque de votre navigateur) et des proxys payants, qui sont moins chers cependant que les VPN. Comme pour ces derniers, vous n'avez jamais la garantie que le propriétaire du proxy ne journalise pas vos connexions. Il faut à l'évidence être extrêmement prudent.

Il existe des proxys transparents, anonymes (anonymous proxies) et hautement anonymes (high anonymous proxies ou elite proxies). Pour en savoir plus, vous pouvez consulter le chapitre : *Serveurs proxy HTTP en entreprise*.

Pour savoir si l'utilisation d'un proxy est visible ou non par le site que vous visitez, vous pouvez vous servir d'un proxy-test en ligne. Par exemple : ipleak.net



Si vous trouvez sur le web une liste de proxys dont vous voulez vérifier la disponibilité, vous pouvez utiliser un proxy-checker. Par exemple : hidemyna.me/en/proxy-checker/.



Résultat fourni par le proxy-checker de la page précédente :

Checked 7 of 7 (100%) **0** rows does not contain proxy **0** Repetitions, **4** Works, **3** Failed

Results: download as .txt èëè or .scv or open in new window

IP-address	Port	Country, city	Speed	Type	Anonymity
101.255.85.114	80	Indonesia Jakarta	1991 ms	HTTP	No
36.255.87.231	84	India Bengaluru	1278 ms	HTTP	No
202.173.219.46	443	Thailand	1197 ms	HTTP	No
106.13.14.43	8080	China		Failed	
97.73.182.234	87	United States Pacific	8195 ms	HTTP	No
85.237.251.135	8080	Slovakia		Failed	
87.245.88.134	80	Switzerland Schaffhausen		Failed	

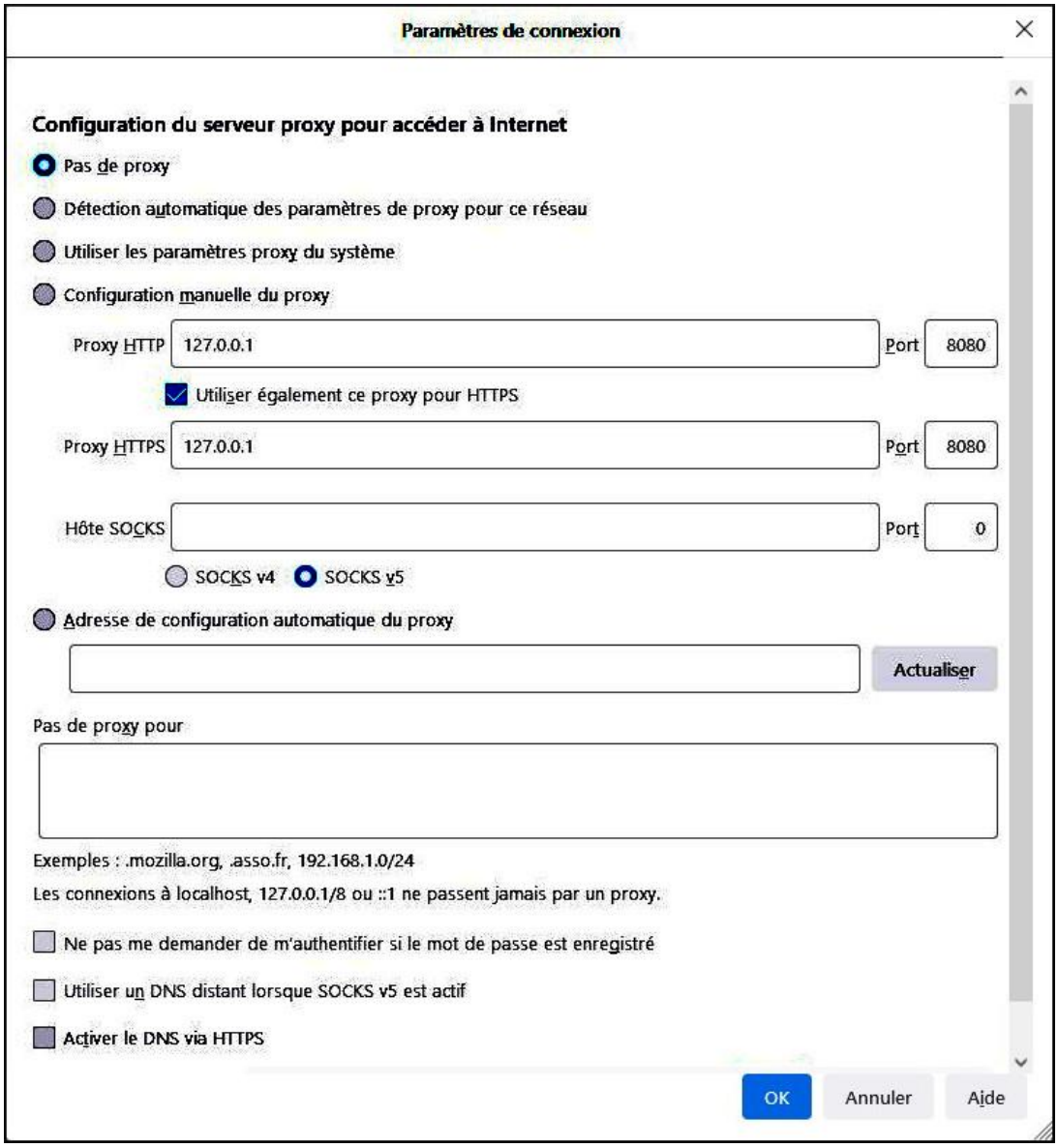
Anonymiseurs gratuits

Il existe un type de proxys web (HTTP & HTTPS) gratuits, moins puissants que les proxys normaux, sont parfois appelés Anonymizers (anonymouse.org, hide.me, hidester.com, …). En pratique, vous entrez l'adresse que vous désirez visiter dans le formulaire d'un site proposant ce service, et la page désirée s'affichera dans celle du site en question. Votre adresse IP sera cachée et seule celle du proxy sera communiquée à votre destinataire. Les liens contenus dans les pages visitées seront modifiés à la volée afin de toujours vous faire passer par le proxy.

Les proxys web sont souvent gratuits, mais il faut les éviter. Il s'agit d'un outil d'anonymisation vraiment basique et peu sûr (ils peuvent laisser fuiter votre adresse réelle, en plus de voler dans certains cas vos données).
Pour en savoir plus, vous pouvez consulter le chapitre : *Rester anonyme sur Internet*.

Utilisation d'un proxy avec Windows

Si vous désirez uniquement faire passer le trafic de votre navigateur via un proxy, vous devez régler les paramètres de connexion de ce dernier (ici : Firefox) :



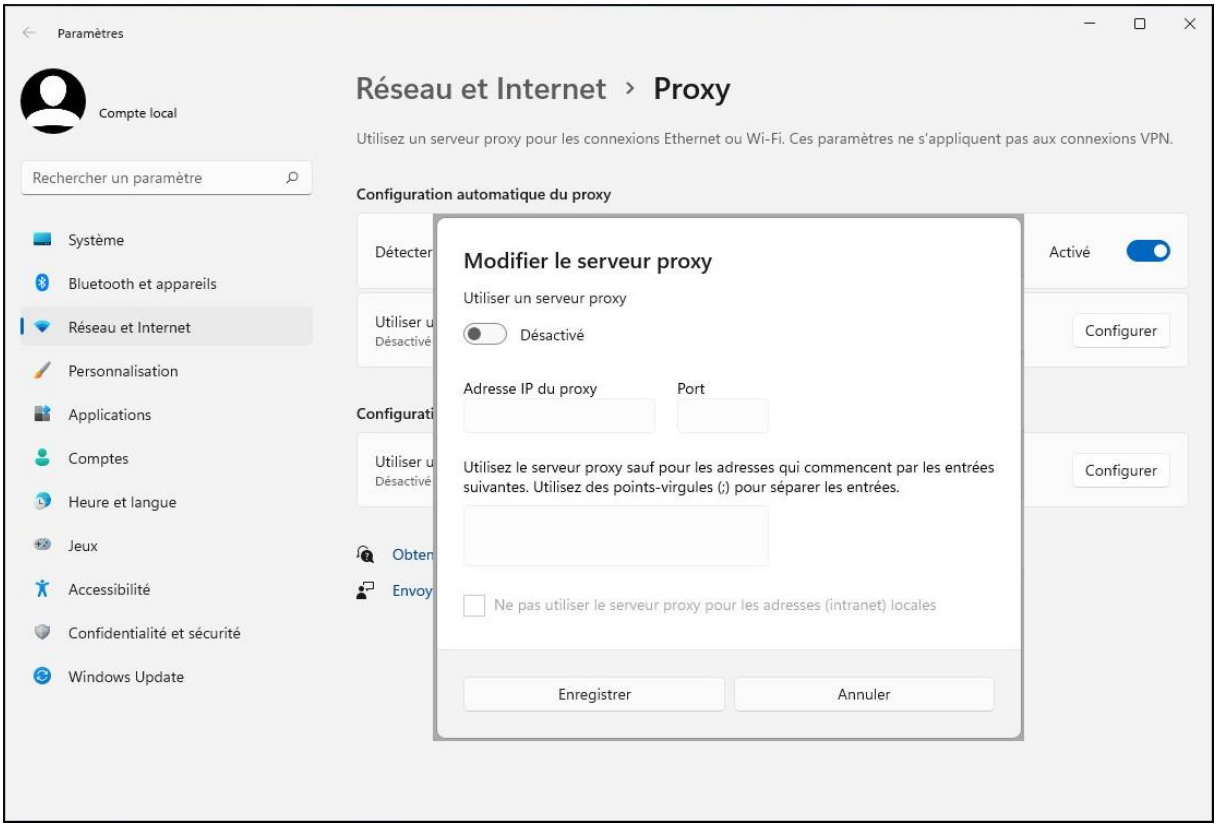
Il faut juste spécifier :

➔ le type de proxy (HTTP ou SOCKS)

➔ L'adresse IP du proxy

➔ Le port utilisé par le proxy

Si vous désirez faire passer tout le trafic Internet issu de votre ordinateur via le proxy, vous devez régler les paramètres proxy de Windows :



Il suffit ici aussi d'indiquer l'adresse IP du proxy et le port utilisé.

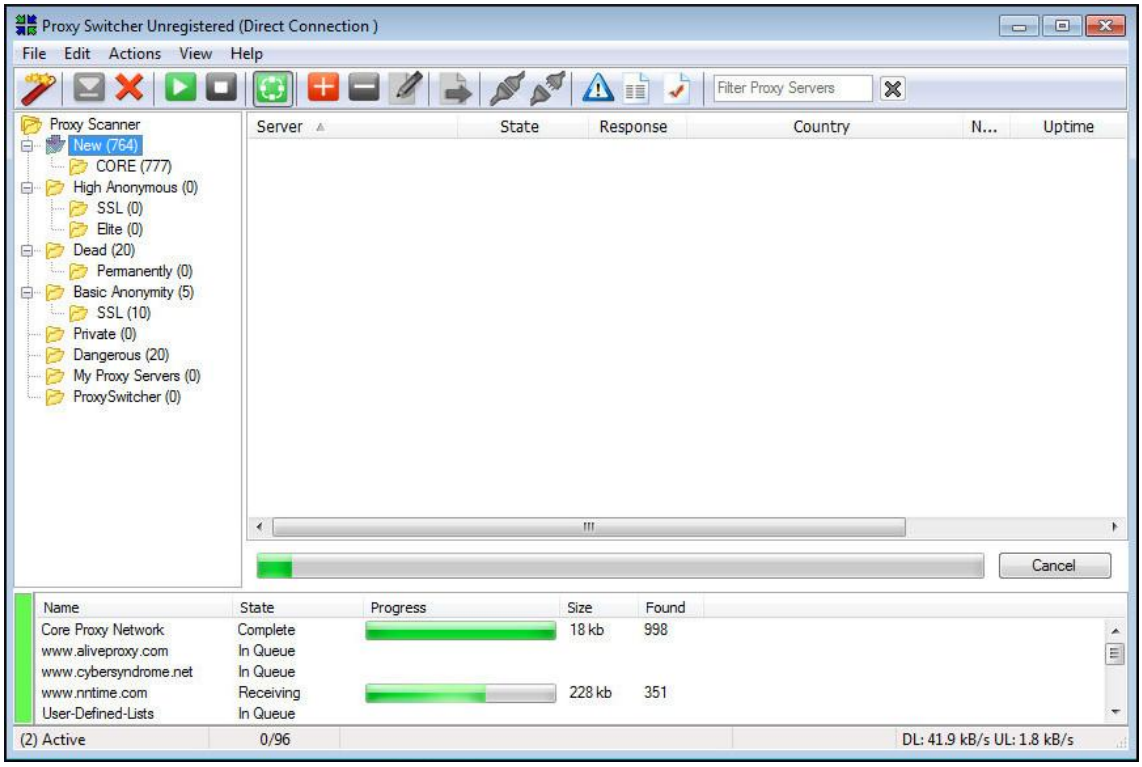
Surfer anonymement avec Proxy Switcher

Proxy Switcher est un programme qui permet de naviguer sur le web anonymement grâce à l'utilisation de serveurs proxy. La version *Standard* coûte environ 30 dollars et la version *Pro* coûte environ 50 dollars. Il y a une version gratuite limitée.

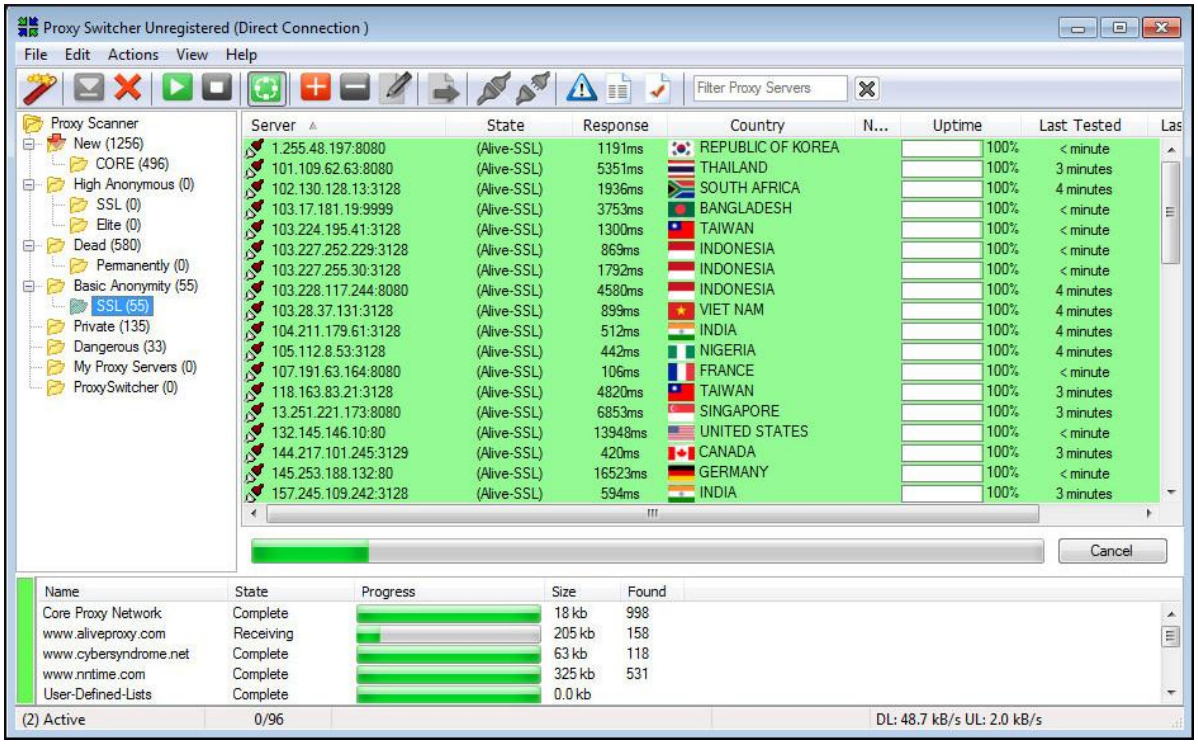
Proxy Switcher permet :

- ➔ **de masquer votre adresse IP lors de votre navigation sur le web,**
- ➔ **de contourner des restrictions géographiques,**
- ➔ **de contourner la censure,**
- ➔ **de changer automatiquement de serveur proxy pour une navigation anonyme encore plus sûre,**
- ➔ **de faire des recherches Google depuis différents pays (google.fr, google.ca, google.us, …),**
- ➔ **de prendre en charge complètement les serveurs SOCKS5 et Elite, …**

Lancement de Proxy Switcher :

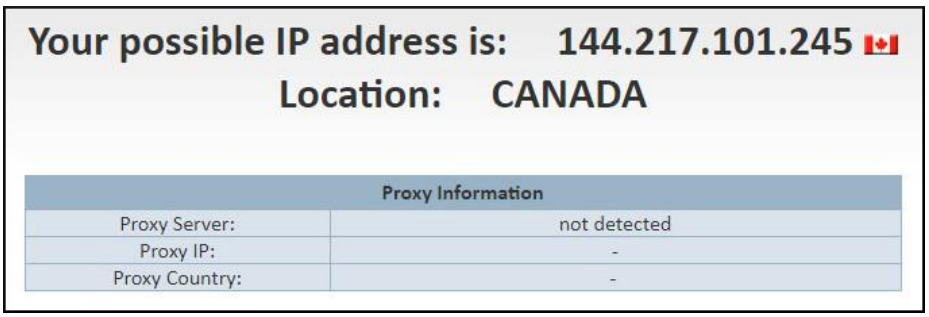


Les serveurs proxy se chargent automatiquement :



Il me suffit de double-cliquer sur le proxy de mon choix (ici un proxy canadien avec SSL) pour que ma navigation devienne anonyme.

Vérifions-le à l'adresse www.proxyswitcher.com/check.php :



Le serveur proxy n'est pas détecté (il est bien anonyme) et mon adresse IP est bien localisée au Canada !

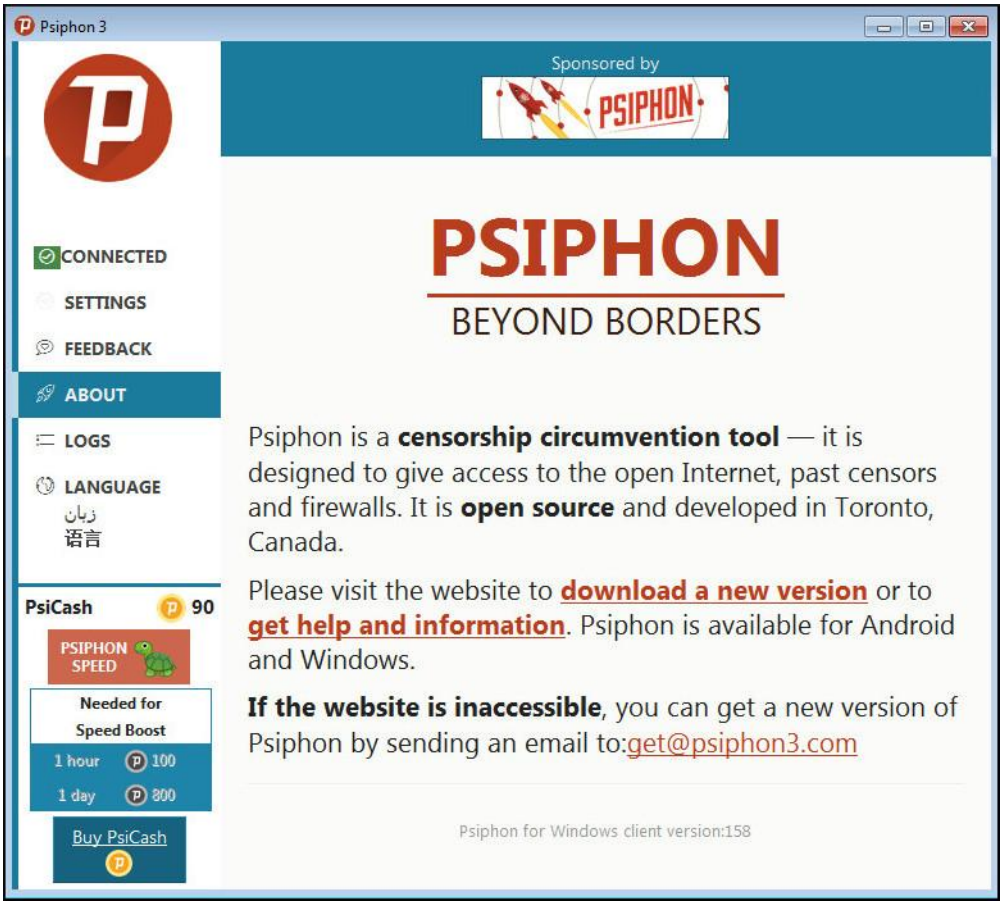
Contourner la censure avec Psiphon

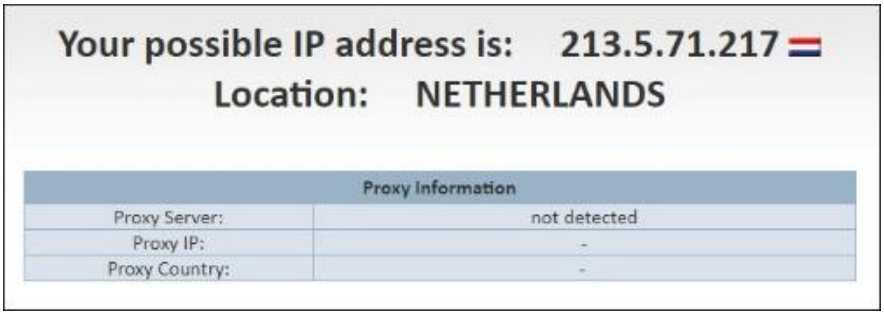
Psiphon est un outil canadien et open source (GNU General Public License) permettant de contourner depuis 2006 la censure et les firewalls. Il permet de naviguer anonymement et de façon sécurisée sur le web.
Psiphon combine plusieurs technologies pour arriver à ses fins :

- ➔ **Serveurs proxy HTTP**
- ➔ **SSH**
- ➔ **VPN**

La première version de Psiphon a été développée à l'Université de Toronto. Psiphon est disponible pour Windows et Android.

Lançons Psiphon :



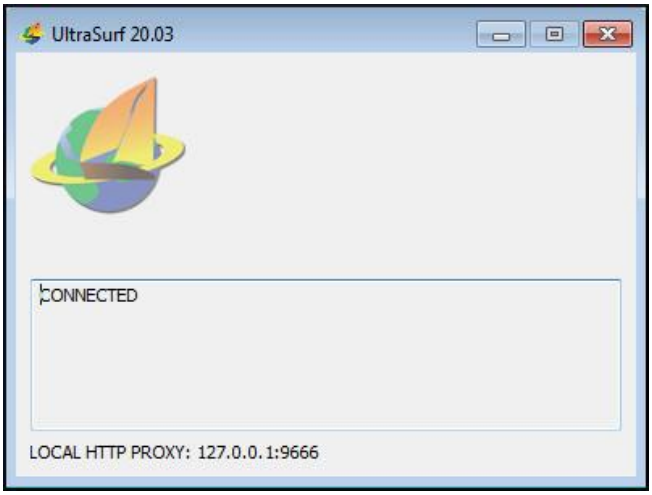


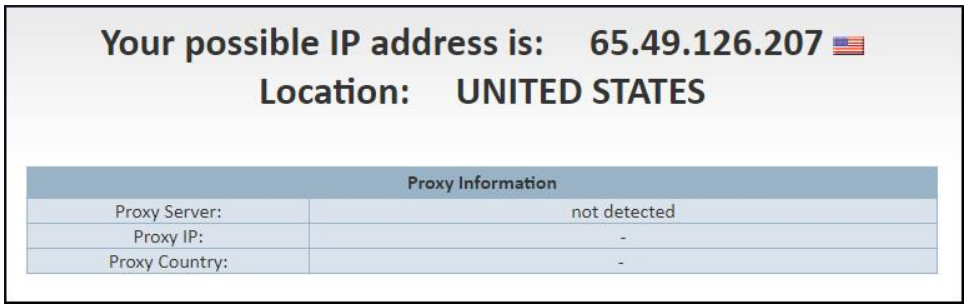
Mon adresse IP est bien masquée !

Contourner la censure avec Ultrasurf

Ultrasurf est un logiciel propriétaire qui permet, depuis 2002, de contourner la censure, mais il ne permet pas toujours d'être anonyme car des fuites d'informations sont possibles. De plus, UltraReach, qui développe cet outil, a accès à toutes vos données. Ce logiciel est très utilisé dans les régimes totalitaires pour bypasser les blocages IP et DNS, ainsi que le filtrage de mots-clés. Dix millions de personnes l'utilisent dans le monde, particulièrement en Chine.

Il suffit de télécharger le programme (ultrasurf.us) et de double-cliquer dessus pour être protégé :





Mon adresse IP est bien masquée !

Comparaison Proxy Switcher / Psiphon / Ultrasurf

	Proxy Switcher	Psiphon	Ultrasurf
Open source	Non	Oui	Non
Prix	Payant pour les versions STD (30$) et PRO (50$) Version gratuite limitée	Gratuit	Gratuit
Type de chiffrement	Variable	VPN, SSH, HTTP Proxy	SSL/TLS
Performance	Variable	Bonne mais parfois lente	Rapide mais instable
Objectif principal	Surfer anonymement avec un proxy	Contournement de la censure	Contournement de la censure
Niveau de confidentialité	Variable	Moyen	Bas

LUTTE CONTRE LA CENSURE

Psiphon et Ultrasurf sont plutôt utilisés dans des pays à censure très importante (Chine, Iran, Myanmar et Arabie Saoudite), mais aussi à censure moins élevée (Turquie, Venezuela et Inde).

Dans les pays à forte censure, il sera cependant conseillé d'utiliser Tor ou un bon VPN.

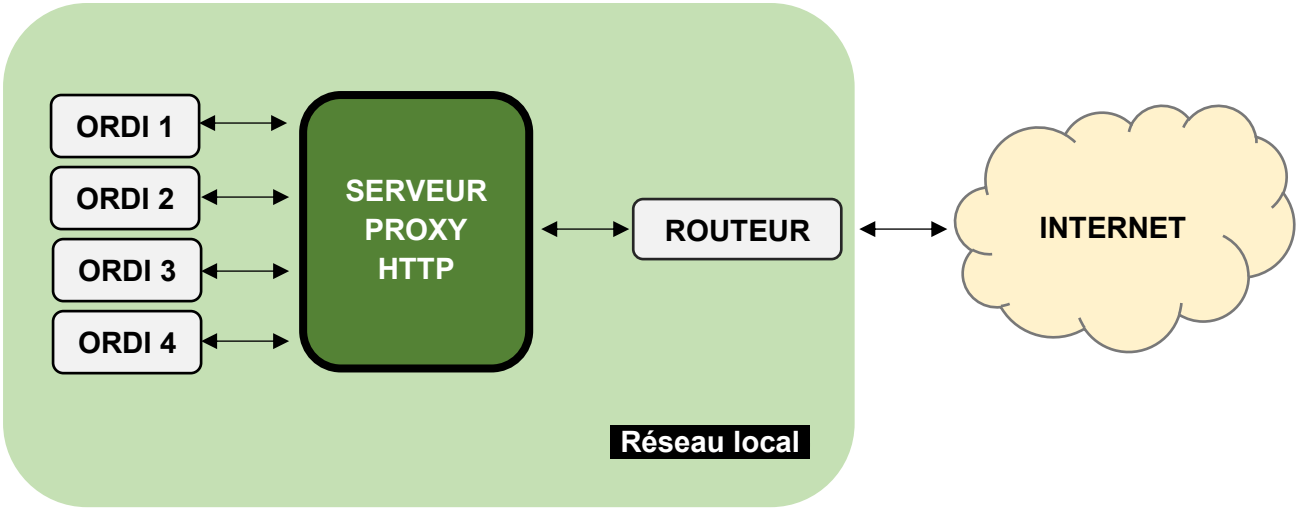
Serveurs proxy HTTP en entreprise

Les serveurs proxy HTTP sont des intermédiaires entre un ou plusieurs ordinateurs et les sites web présents sur le réseau Internet.

Pour utiliser un serveur proxy HTTP, il faut donc configurer le navigateur en lui communiquant l'adresse IP du serveur proxy ainsi qu'un numéro de port.

<u>Utilisation d'un proxy HTTP dans une entreprise :</u>

Il est possible d'installer, dans une entreprise, un serveur proxy HTTP entre les ordinateurs des employés et le routeur qui les relie à Internet :



Cela a cinq avantages majeurs :

1. **La protection des ordinateurs qui ne sont plus directement reliés à Internet (masquage des IP internes).**
2. **Le cache : si plusieurs ordinateurs téléchargent les mêmes données volumineuses depuis Internet, le cache permettra dès le deuxième téléchargement de fournir directement les données depuis le proxy sans devoir passer par Internet. Ceci constitue un gain de temps appréciable pour l'entreprise.**
3. **Blacklisting ou Withelisting : le filtrage des communications via l'ACL (Access Control List) : le patron de l'entreprise peut décider ce qu'il autorise à sortir ou à entrer du réseau local. Un exemple est l'interdiction pour les employés de visiter un site donné (Facebook, Youtube, …)**
4. **Centralisation de la journalisation (logging).**
5. **Blocage aisé du trafic malicieux.**

Il y a aussi, en contrepartie, trois inconvénients à considérer :

1. **Le proxy peut enregistrer tout ce qui transite entre les ordinateurs et le Web. Le patron peut donc avoir théoriquement accès à tout votre historique de navigation.**
2. **Si de nombreux ordinateurs sont connectés au même moment au proxy, cela peut ralentir le trafic.**
3. **L'accès à certains sites n'est parfois pas possible via un proxy à cause des technologies utilisées par les sites en question.**

<u>Utilisation d'un proxy HTTP par un particulier :</u>

Il est possible évidemment pour un particulier de se servir également d'un serveur proxy HTTP pour différentes raisons :

1. **Le proxy HTTP permet de surfer anonymement : ce n'est plus votre adresse IP qui est communiquée aux sites que vous visitez, mais celle du proxy.**
2. **Le contournement du filtrage dans votre entreprise évoqué précédemment : un employé peut visiter un site "interdit" en passant par un proxy HTTP externe à l'entreprise.**
3. **Le contournement d'une restriction géographique : si une ressource sur Internet n'est possible que pour les habitants d'un pays donné, il suffit à une personne étrangère de se connecter à la ressource via un proxy situé dans le pays adéquat.**

<u>Comment installer un serveur proxy HTTP sur un ordinateur</u>

1. **Il est possible pour un particulier d'installer un serveur proxy HTTP très facilement, par exemple sur le serveur qui héberge son domaine personnel, en utilisant des scripts PHP que l'on trouve gratuitement sur Internet. Exemple de tels scripts : PHP-Proxy, miniProxy, …**
2. **Un serveur proxy HTTP très performant utilisé dans les entreprises est le logiciel libre Squid. Pour installer le serveur Squid sur Linux, il suffit de taper dans une console : "sudo apt-get install squid". Pour lancer le service, il suffit de taper : "sudo service squid3 start". Le fichier de configuration est /etc/squid3/squid.conf (il faut remplacer "http_access deny all" par "http_access allow all" si nécessaire).**

Point de vue anonymat, il y a trois sortes de proxys HTTP :

1. **<u>High Anonymous Proxies (ou Elite Proxies)</u> : ces proxys ne changent pas les champs des requêtes qui semblent donc provenir d'une vraie adresse IP. L'adresse IP réelle est cachée.**

2. **<u>Anonymous Proxies</u> : L'adresse IP réelle est ici aussi cachée, mais les champs des requêtes sont modifiés. On peut donc deviner l'utilisation d'un proxy !**

3. **<u>Transparent Proxies</u> : aucun anonymat car l'IP réelle est transmise dans chaque requête via les champs modifiés.**

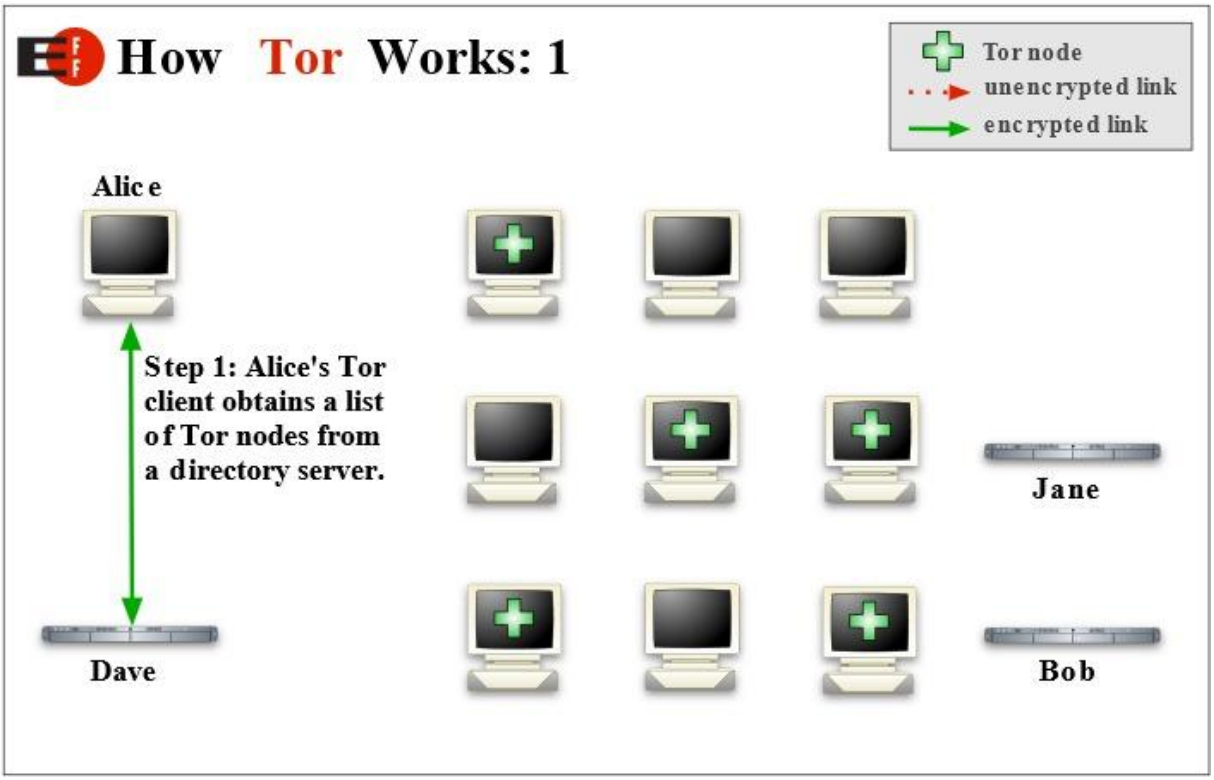
SERVEUR PROXY : CHAMPS DES REQUÊTES
Dans une requête originale émise par l'utilisateur, ainsi que dans une requête émanant d'un serveur proxy HIGH ANONYMOUS, les trois champs suivants apparaissent comme suit : ➢ **REMOTE_ADDR = <IP>** ➢ **HTTP_VIA = blank** ➢ **HTTP_X_FORWARDED_FOR = blank** **L'adresse IP <IP> sera celle de l'utilisateur dans la requête originale et celle du proxy dans le cas du proxy HIGH ANONYMOUS. Il est impossible de deviner qu'un proxy est utilisé et l'adresse réelle reste donc secrète !**
Dans une requête émanant d'un serveur proxy ANONYMOUS, les trois champs en question apparaissent comme suit : ➢ **REMOTE_ADDR = <PROXY IP>** ➢ **HTTP_VIA = <PROXY IP>** ➢ **HTTP_X_FORWARDED_FOR = blank** **L'adresse IP du proxy apparaît dans le champ HTTP_VIA, il est donc possible de deviner qu'un proxy est utilisé ! L'adresse réelle reste cependant cachée.**
Dans une requête émanant d'un serveur proxy TRANSPARENT, les trois champs apparaissent comme suit : ➢ **REMOTE_ADDR = <PROXY IP>** ➢ **HTTP_VIA = <PROXY IP>** ➢ **HTTP_X_FORWARDED_FOR = <USER IP>** **L'adresse IP du proxy apparaît dans les deux premiers champs et l'adresse IP réelle <USER IP> apparaît dans le troisième champ. Vous n'êtes donc plus anonyme !**

Le réseau Tor et le navigateur Tor

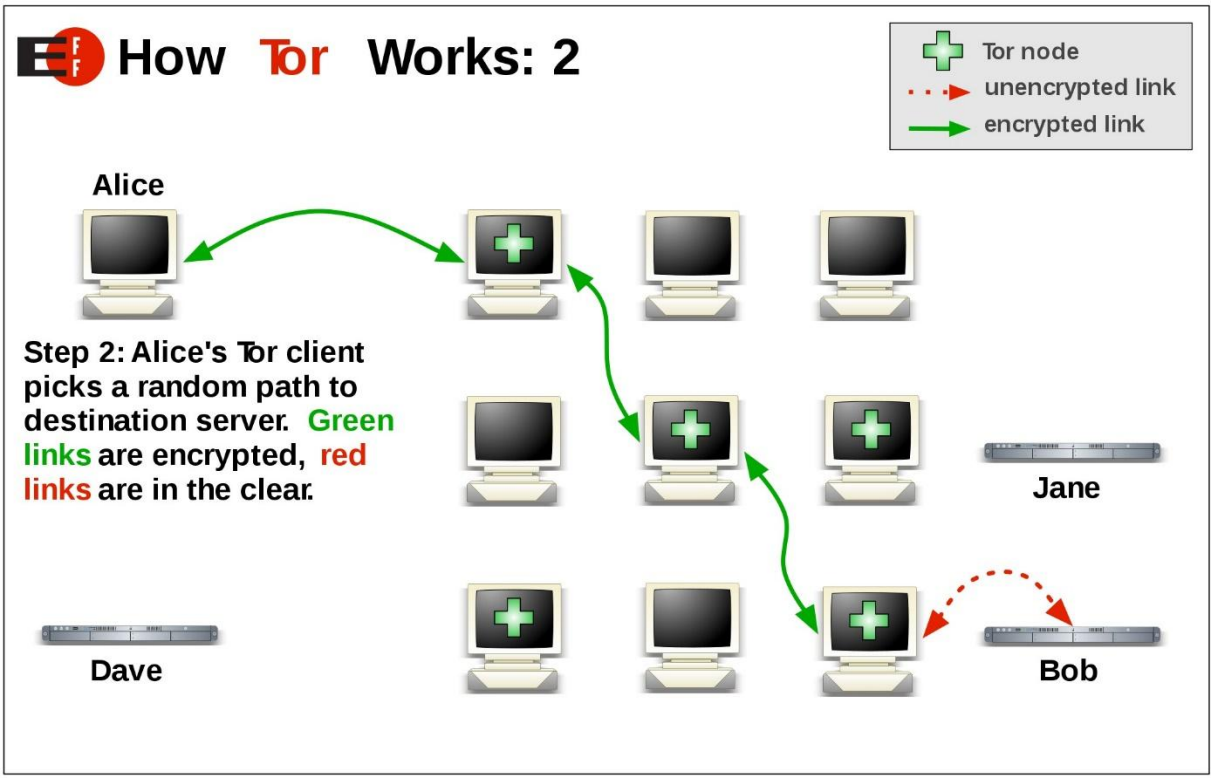
Tor (The Onion Router) est un réseau informatique décentralisé se composant de serveurs appelés nœuds (il y en a environ 7000 dans le monde) et permettant de surfer, dans une certaine mesure tout au moins, de manière anonyme grâce au routage en onion. Il existe un navigateur basé sur Firefox, Tor browser, qui permet d'utiliser le réseau Tor de manière plus sécurisée. Tor est d'origine académique.

Tor permet d'éviter l'analyse du trafic, de contourner la censure, d'accéder à des sites bloqués par le FAI (ISP), de visiter les sites cachés en .onion du Darknet. Tor est malheureusement également utilisé par des cybercriminels soucieux d'agir de façon anonyme.

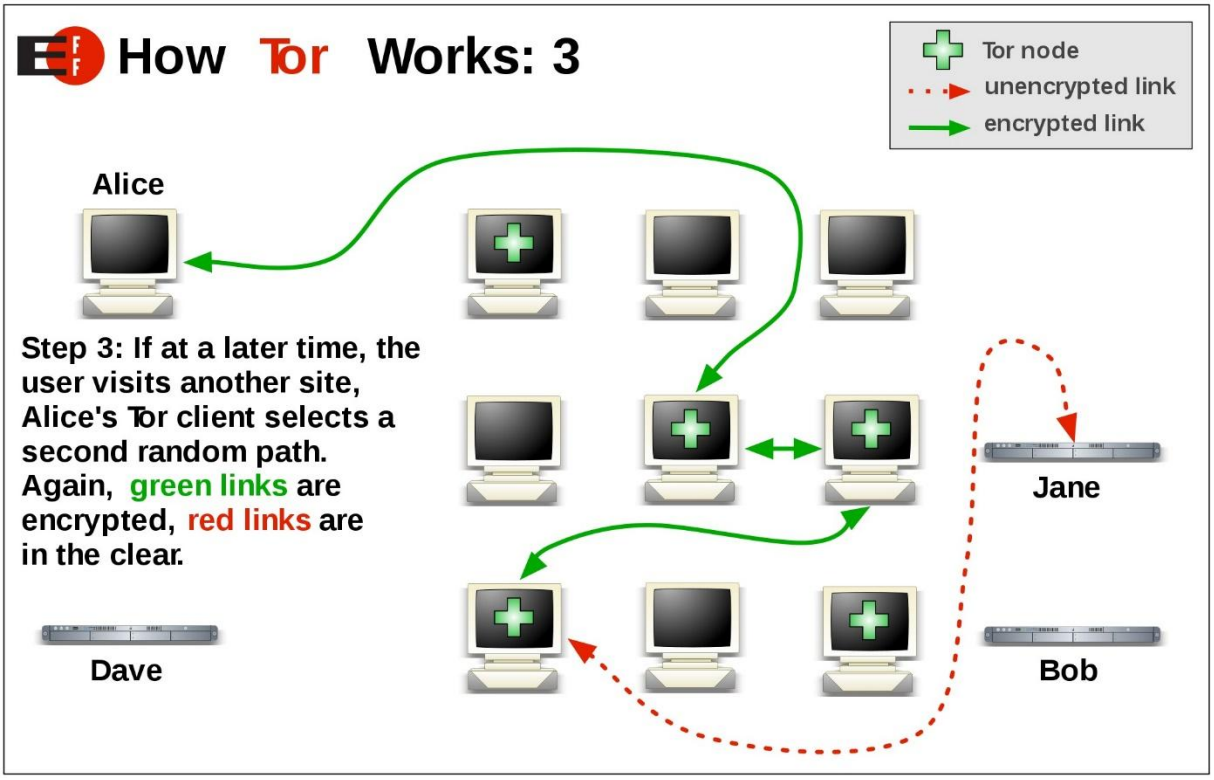
Fonctionnement du réseau Tor :



Electronic Frontier Foundation, CC BY 3.0



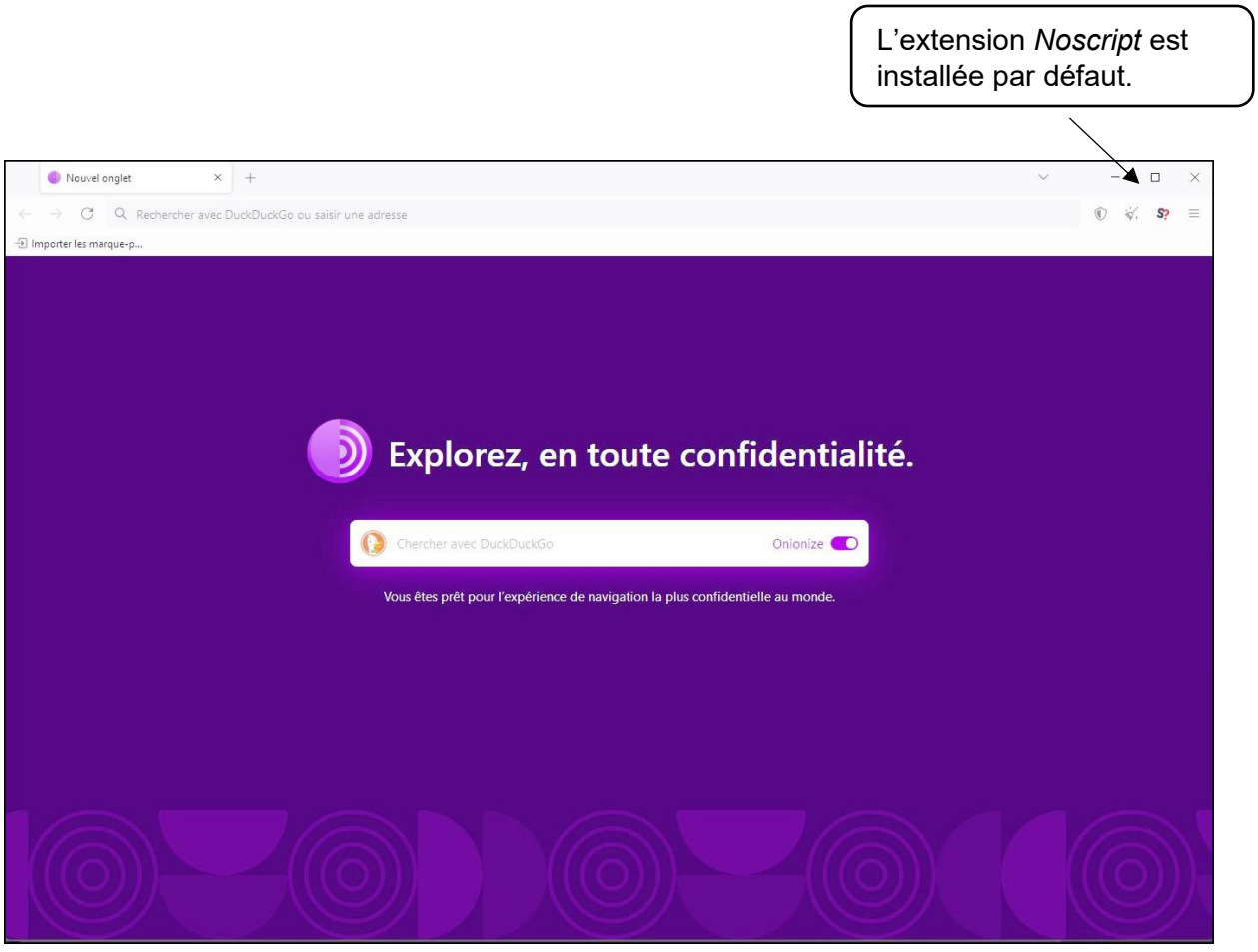
Electronic Frontier Foundation, CC BY 3.0



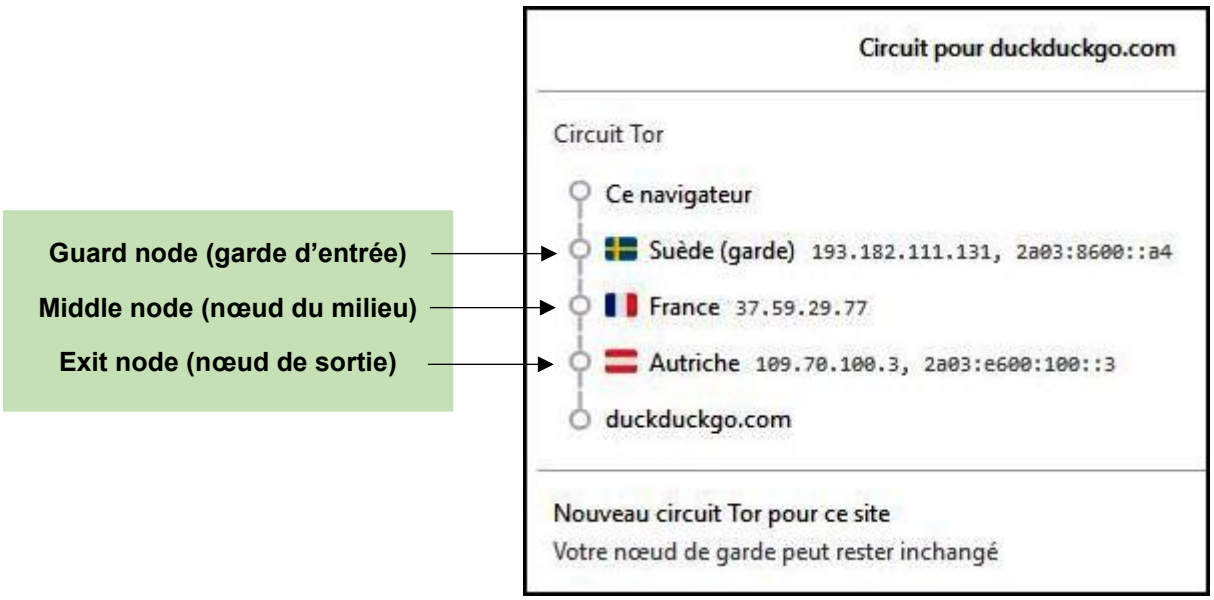
Electronic Frontier Foundation, CC BY 3.0

Le navigateur Tor

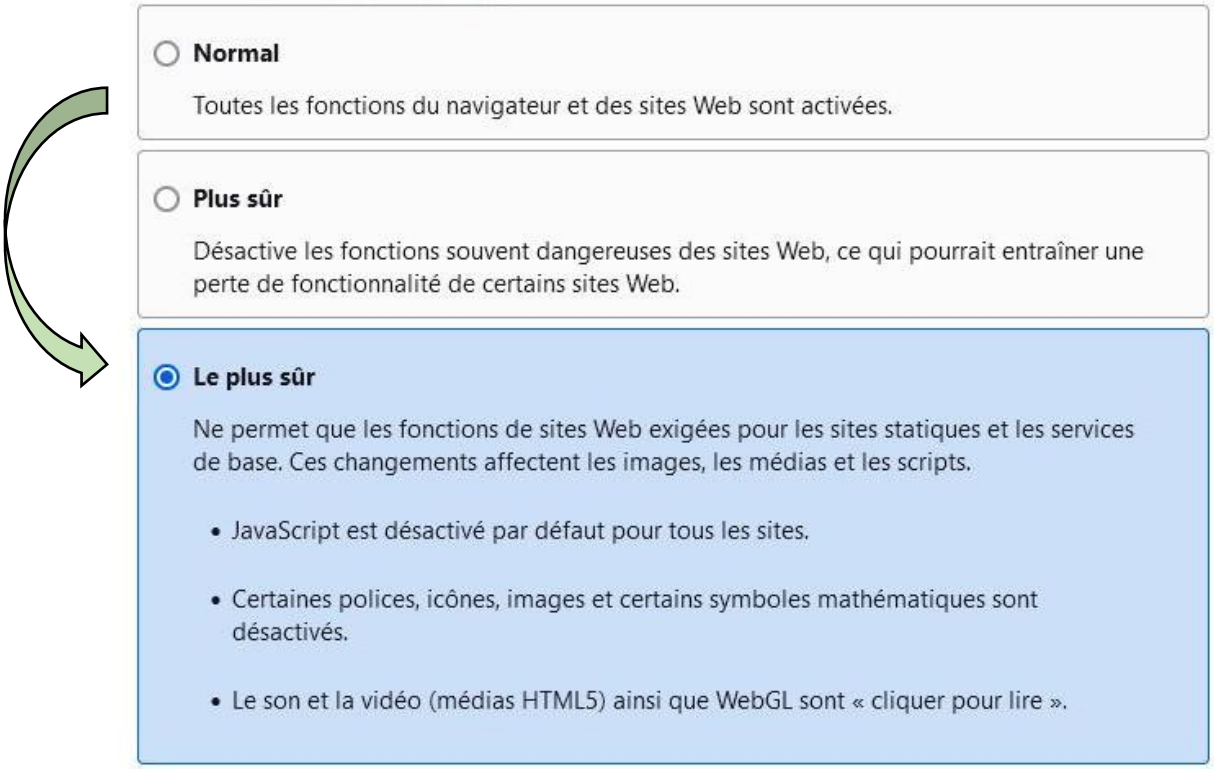
On peut le télécharger à la page : https://www.torproject.org/download/.



On peut afficher et même modifier, pour chaque page visitée le circuit Tor emprunté :



Il faut, par prudence, changer les paramètres de sécurité :



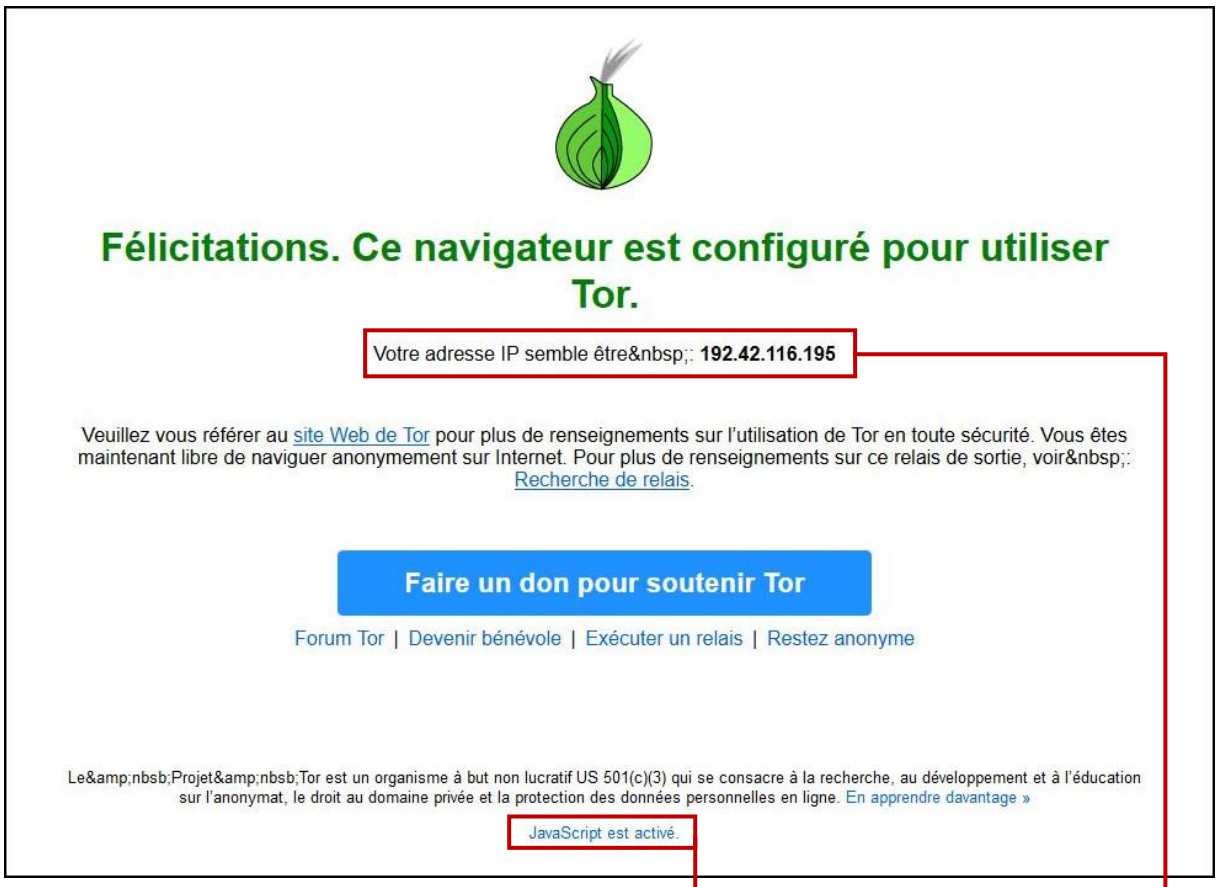
Que peut-on faire avec le navigateur Tor ?

- **On peut utiliser le réseau Tor pour surfer anonymement sur Internet,**
- **On peut empêcher le FAI de savoir quel site vous visitez,**
- **On peut empêcher le site visité de connaître votre adresse IP réelle,**
- **On peut empêcher le tracking,**
- **On peut contourner la censure,**
- **On peut visiter les sites cachés en .onion du Darknet.**

Que ne peut-on pas faire avec le navigateur Tor ?

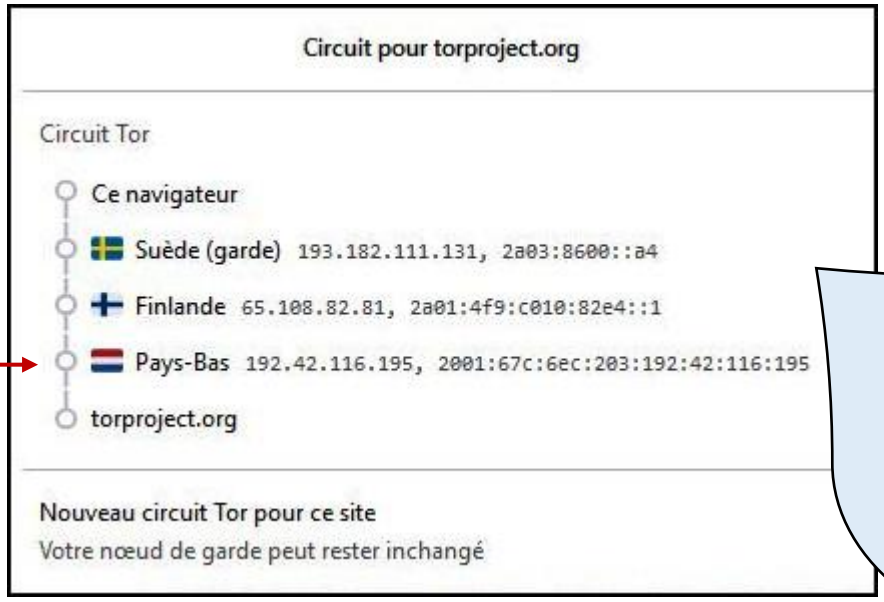
- **On ne peut pas utiliser le réseau Tor avec d'autres applications sans une configuration préalable,**
- **On ne peut pas empêcher le FAI de savoir que vous utilisez le réseau Tor,**
- **On ne peut pas empêcher le site visité de savoir que vous utilisez le réseau Tor,**
- **On n'est pas à l'abri d'une faille présente dans le navigateur,**
- **On n'est pas protégé des dangers liés aux contenus actifs (notamment JavaScript),**
- **On n'est pas à l'abri des dangers liés aux extensions que vous êtes susceptible d'installer (absolument à éviter),**
- **On n'est pas à l'abri des malwares éventuellement présents sur un site visité ou sur votre ordinateur,**
- **On n'est pas à l'abri d'un OS ou d'un hardware compromis,**
- **On n'est pas à l'abri d'une attaque de l'homme du milieu (MITM),**
- **Le navigateur Tor ne supprime pas les métadonnées éventuellement présentes dans les documents que vous uploadez,**
- **Tor ne supporte pas le protocole UDP,**
- **On ne peut pas utiliser un client BitTorrent avec Tor. Si on le fait, votre adresse IP ne sera plus cachée,**
- **On ne peut pas visiter certains sites avec Tor. Ceux-ci sont bloqués,**
- **Si vous avez un compte sur un site web, ce compte pourra être bloqué car son activité sera jugée anormale.**

Pour vérifier que vous êtes bien connecté au réseau Tor, il suffit de visiter la page : https://check.torproject.org. Vous pouvez même savoir si JavaScript est actif ou non :



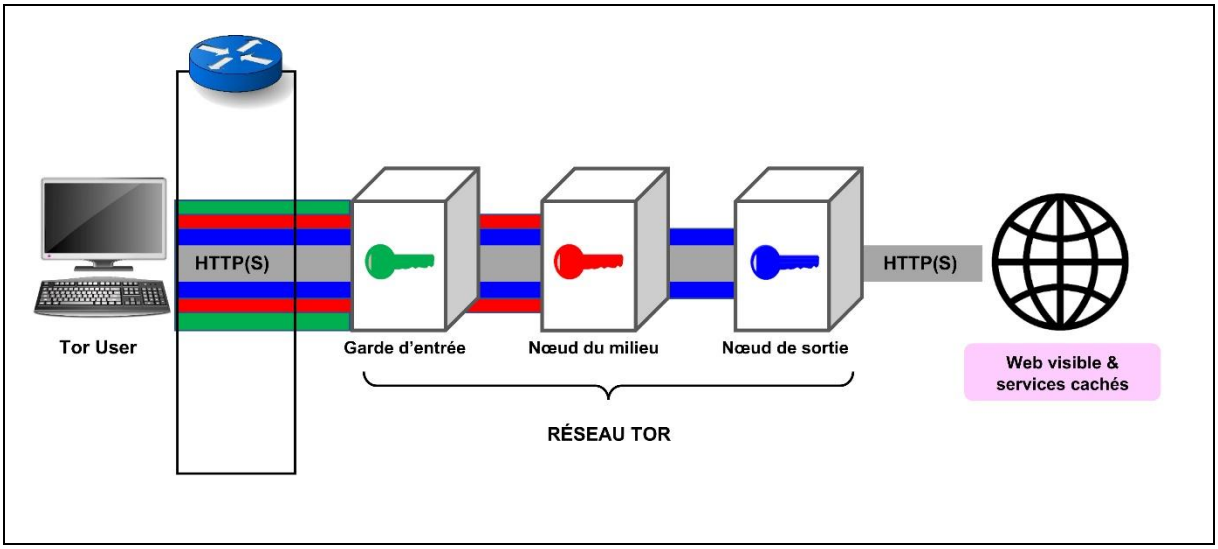
JavaScript est activé.

Votre adresse IP semble être : 192.42.116.195



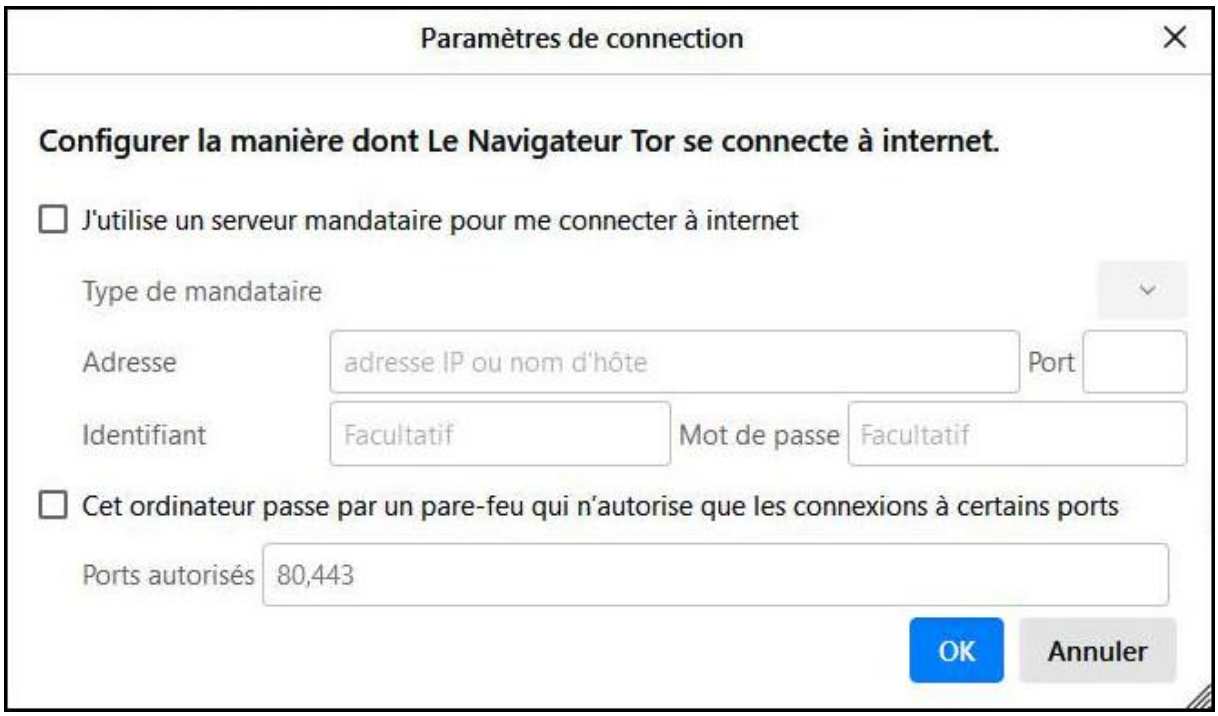
On est effectivement connecté au réseau Tor, cette adresse IP étant celle d'un nœud de sortie (*exit node*) situé aux Pays-Bas !

Le fonctionnement de Tor est donc simple :



Quoi de neuf dans les régimes totalitaires ?

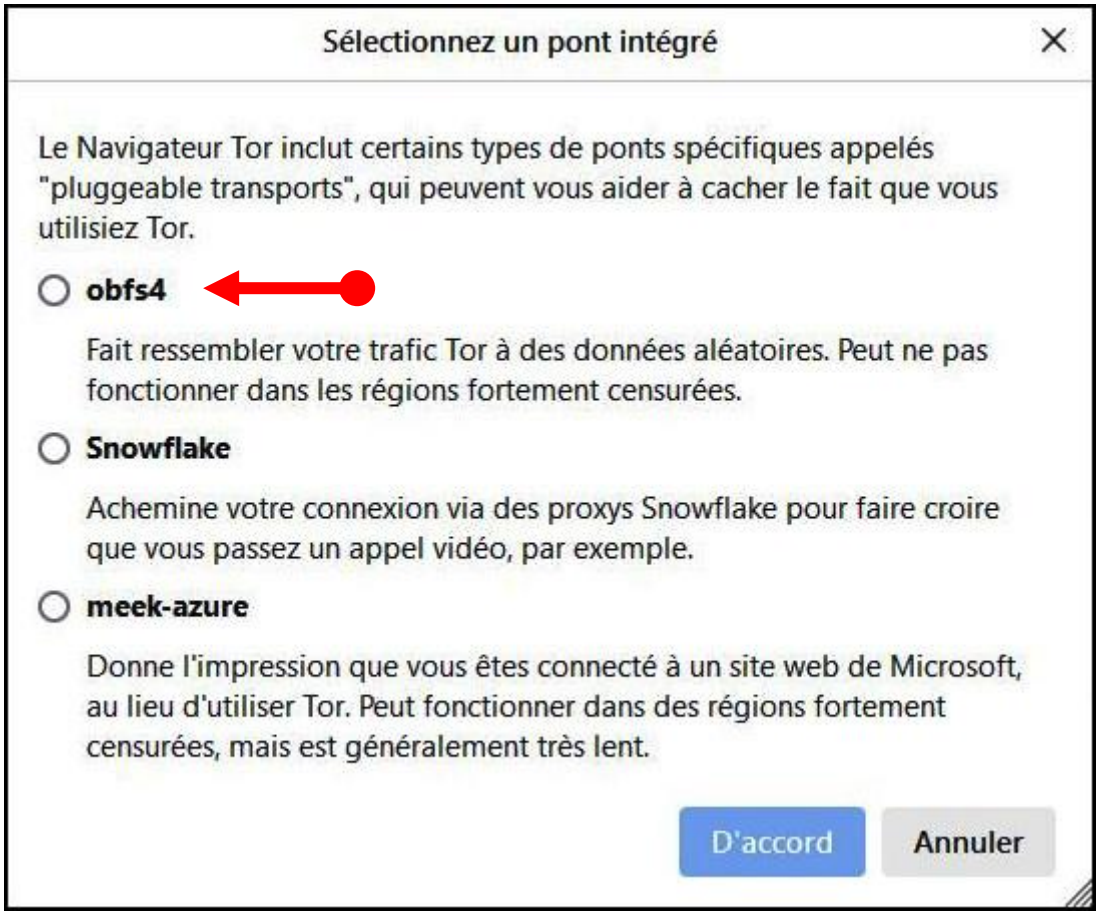
Pour empêcher les utilisateurs de contourner la censure en utilisant le routage en oignon, un État peut installer un pare-feu qui bloque certains ports utilisés par Tor. Dans ce cas, la contre-mesure est simple. On indique au navigateur Tor les ports autorisés par ce pare-feu dans les paramètres du réseau :



Il est encore possible pour les gouvernements ou les FAI de bloquer les nœuds du réseau Tor puisque ceux-ci sont connus de tous (ils sont listés dans des annuaires publics). La contre-mesure consiste alors à utiliser un pont (bridge). Les ponts sont des relais (nœuds) non listés dans ces annuaires.

Malheureusement, les oppresseurs ne s'avouent pas vite vaincus. Ils ont donc imaginé un autre moyen de bloquer les utilisateurs de Tor : le DPI. Le DPI (*Deep Packet Inspection*, en français *Inspection Profonde des Paquets*) recherche des signatures (grâce à des expressions régulière -RegEx-) dans les paquets transitant sur Internet. Dans ce cas, il y a encore une contre-mesure : l'obfuscation.

L'obfuscation consiste à modifier les paquets afin de les rendre innocents aux yeux des censeurs. L'utilisateur pourra donc continuer à contourner la censure en choisissant, par exemple, un pont obfs4.



Si vous désirez utiliser le réseau Tor avec d'autres applications, il faut être extrêmement prudent à cause des fuites possibles (fuites DNS par exemple). Il n'est pas garanti que l'application enverra tout le trafic via Tor ! On peut le vérifier grâce à Wireshark (analyseur de paquets libre et gratuit). Il est bien sûr toujours possible de stopper le trafic non Tor avec des règles de firewall. On peut aussi utiliser le proxy web *Privoxy* si on désire utiliser sereinement une application via le réseau Tor, mais cela est réservé aux utilisateurs avancés.

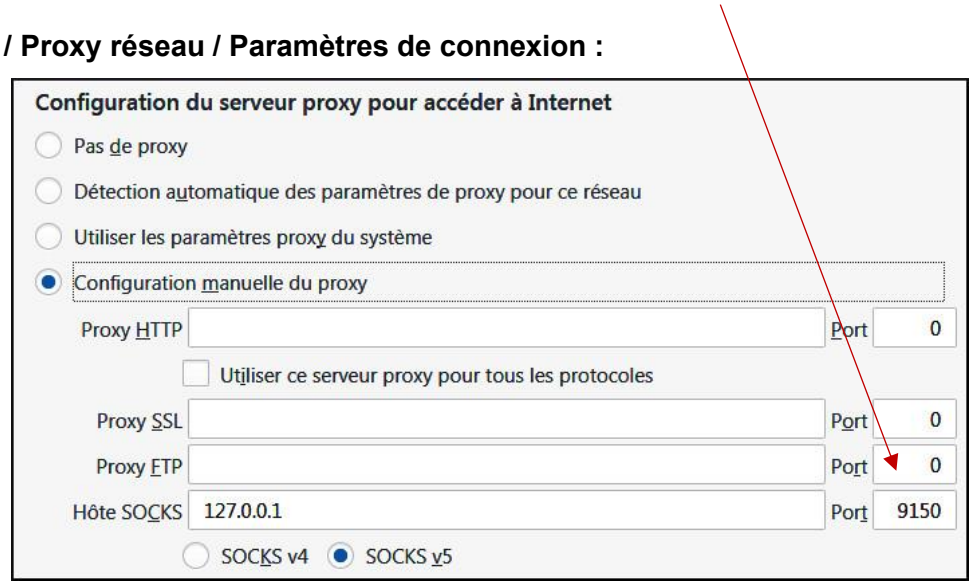
On peut encore utiliser Whonix : ce système est constitué de deux machines virtuelles (Linux), une passerelle (Gateway) reliée au réseau Tor et une station de travail (Workstation) avec les applications de l'utilisateur. La station de travail ne peut communiquer qu'avec la passerelle. Tout le trafic doit donc obligatoirement passer par le réseau Tor. Whonix est une façon très sécurisée d'utiliser une application quelconque avec le réseau Tor !

Pour surfer sur Internet avec le navigateur Tor de manière extrêmement sécurisée, le mieux est d'installer Tails (Linux) sur une clé USB bootable (sans volume de persistance, la persistance étant dangereuse). Vous pouvez installer Tails sur une clé USB avec le programme Rufus depuis un fichier .iso, ou simplement depuis un autre Tails installé sur une autre clé USB. Seul le Tails installé depuis un autre Tails pourra être rendu persistant.

<u>Bon à savoir</u>

Il faut savoir que Tor écoute généralement les connexions SOCKS sur le port 9050 et le navigateur Tor écoute les mêmes connexions sur le port 9150.

Options / Proxy réseau / Paramètres de connexion :



Faiblesses du réseau Tor

1. **On considère généralement qu'environ 2,5 % des nœuds de sortie (les nœuds du réseau Tor sont mis à disposition des internautes par des personnes volontaires) sont fournis par des personnes malveillantes. Vos communications peuvent donc être lues dans une certaine mesure (avec HTTP) par ces personnes à votre insu : MITM possible.**
2. **De nombreux pays et agences (FBI, NSA, GCHQ, …) développent des exploits destinés au navigateur Tor. Ces exploits permettent de vous désanonymiser. La NSA, par exemple, utilise une technique appelée EgotisticalGiraffe qui permet de désanonymiser certains utilisateurs de Tor en utilisant des failles présentes dans des applications présentes sur l'ordinateur des utilisateurs.**
3. **Tout utilisateur du réseau Tor est susceptible d'être étiqueté comme extrémiste ou comme personne d'intérêt par les agences de renseignement. Pensez-y !**
4. **Le navigateur Tor ne purge pas automatiquement les logs à sa fermeture (historique, cookies, cache, …). Il est donc recommandé d'utiliser un live OS (live CD ou live USB) afin de bénéficier d'un système non persistant.**
5. **Un autre défaut du navigateur Tor est qu'il possède un fingerprint unique, ce qui rend ses utilisateurs facilement repérables.**
6. **Un dernier danger de Tor est la possibilité de fuites (DNS, …).**
7. **Tor est un service plus lent qu'un service VPN.**
8. **Une attaque possible de Tor réside en la corrélation end-to-end associée à une attaque Sybil (voir : https://fr.wikipedia.org/wiki/Attaque_Sybil) ou DDoS.**
9. **Une autre attaque possible est le *website traffic fingerprinting* : si vous connaissez à l'avance le contenu d'une page (qui possède un pattern unique), vous pourrez la repérer une fois chiffrée dans le trafic grâce à son fingerprint.**

Qu'en est-il des smartphones ?

Il existe bien sûr des navigateurs pour smartphones utilisant le réseau Tor :

- **Orfox (Android)**
- **Onion Browser (IOS)**

Conclusion :

Il est vivement conseillé, si vous désirez que vos connexions sortantes vers Internet passent obligatoirement par le réseau Tor, d'installer le système d'exploitation Tails sur une clé USB bootable et d'utiliser ce système d'exploitation pour lancer le navigateur Tor. Tails a pour but de protéger votre vie privée et votre anonymat. Il faut absolument éviter d'utiliser le navigateur Tor avec Windows, et certainement pas avec Windows 10 ou 11, qui sont très problématiques quant au respect de votre vie privée et de votre anonymat !

TAILS (the amnesic incognito live system) :

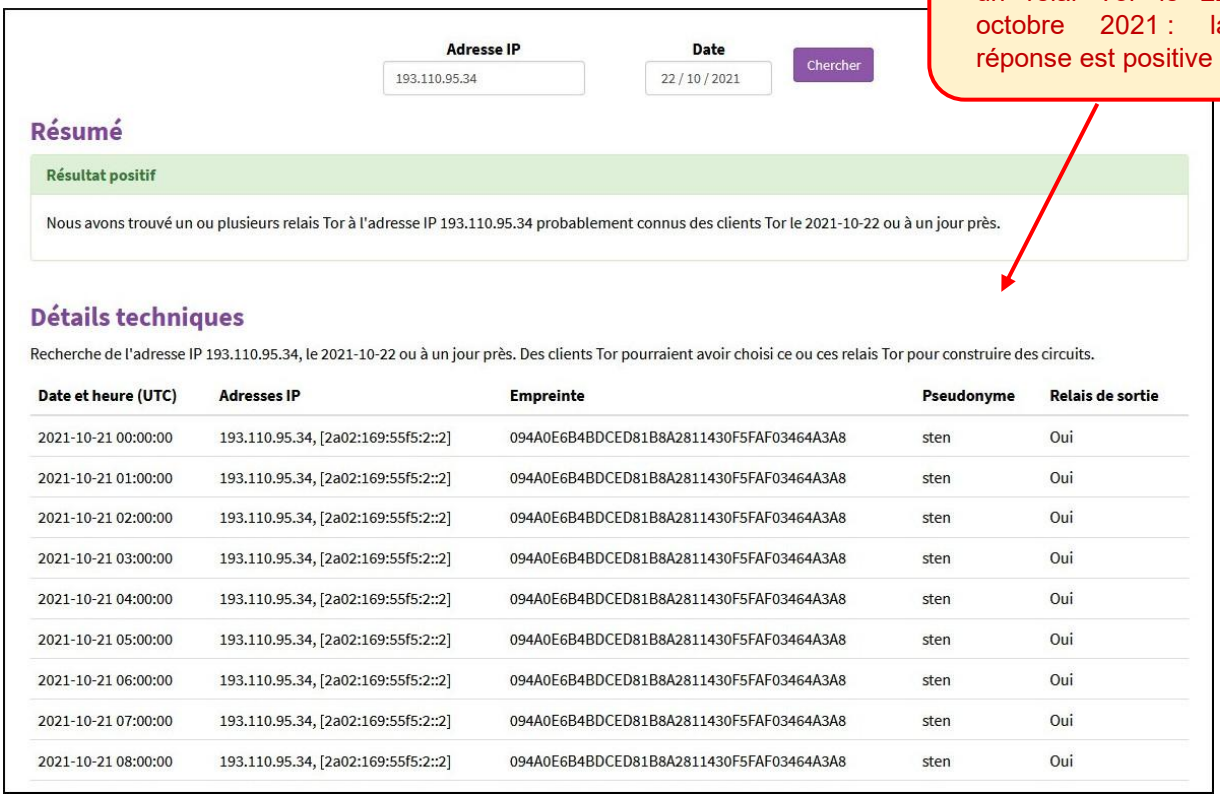
- ***Amnesic* car il ne laisse aucune trace sur votre disque dur**
- ***Incognito* car il est privé et anonyme**
- ***Live* car il fonctionne entièrement sur une clé USB ou un DVD (Live USB / Live DVD)**

Comment utiliser le navigateur TOR	
En l'installant sur son système d'exploitation (Windows, MacOS ou Linux)	**SOLUTION SIMPLE**
En utilisant Tails sur un Live-USB	**TRÈS BONNE SOLUTION**
En utilisant Qubes avec Whonix	**EXCELLENTE SOLUTION**

ExoneraTor

L'outil ExoneraTor (**https://metrics.torproject.org/exonerator.html**) permet de savoir si une connexion est issue du réseau Tor : il suffit de fournir une adresse IP et une date pour obtenir l'information souhaitée. Ce service est très utilisé par les autorités judiciaires.

Recherchons si l'IP 193.110.95.34 était un relai Tor le 22 octobre 2021 : la réponse est positive !



Date et heure (UTC)	Adresses IP	Empreinte	Pseudonyme	Relais de sortie
2021-10-21 00:00:00	193.110.95.34, [2a02:169:55f5:2::2]	094A0E6B4BDCED81B8A2811430F5FAF03464A3A8	sten	Oui
2021-10-21 01:00:00	193.110.95.34, [2a02:169:55f5:2::2]	094A0E6B4BDCED81B8A2811430F5FAF03464A3A8	sten	Oui
2021-10-21 02:00:00	193.110.95.34, [2a02:169:55f5:2::2]	094A0E6B4BDCED81B8A2811430F5FAF03464A3A8	sten	Oui
2021-10-21 03:00:00	193.110.95.34, [2a02:169:55f5:2::2]	094A0E6B4BDCED81B8A2811430F5FAF03464A3A8	sten	Oui
2021-10-21 04:00:00	193.110.95.34, [2a02:169:55f5:2::2]	094A0E6B4BDCED81B8A2811430F5FAF03464A3A8	sten	Oui
2021-10-21 05:00:00	193.110.95.34, [2a02:169:55f5:2::2]	094A0E6B4BDCED81B8A2811430F5FAF03464A3A8	sten	Oui
2021-10-21 06:00:00	193.110.95.34, [2a02:169:55f5:2::2]	094A0E6B4BDCED81B8A2811430F5FAF03464A3A8	sten	Oui
2021-10-21 07:00:00	193.110.95.34, [2a02:169:55f5:2::2]	094A0E6B4BDCED81B8A2811430F5FAF03464A3A8	sten	Oui
2021-10-21 08:00:00	193.110.95.34, [2a02:169:55f5:2::2]	094A0E6B4BDCED81B8A2811430F5FAF03464A3A8	sten	Oui

En résumé

<table>
<tr><td colspan="2">Un anonymiseur rend votre activité sur Internet intraçable</td></tr>
<tr><td rowspan="2">Anonymiseur à point unique
(Single Point Anonymizer)</td><td>Serveur proxy

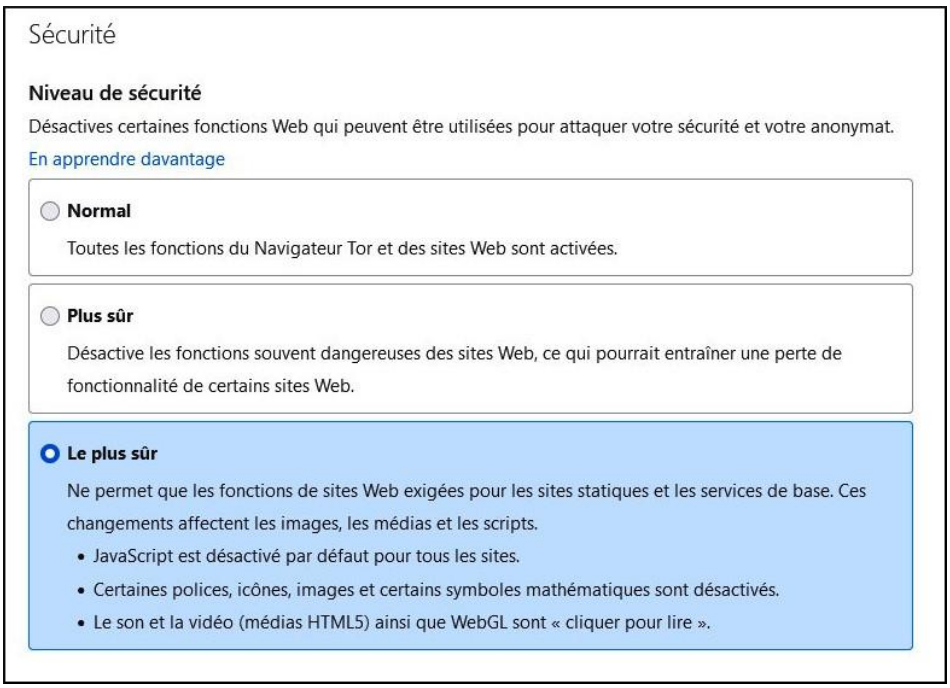
Le trafic n’est pas chiffré.</td></tr>
<tr><td>VPN

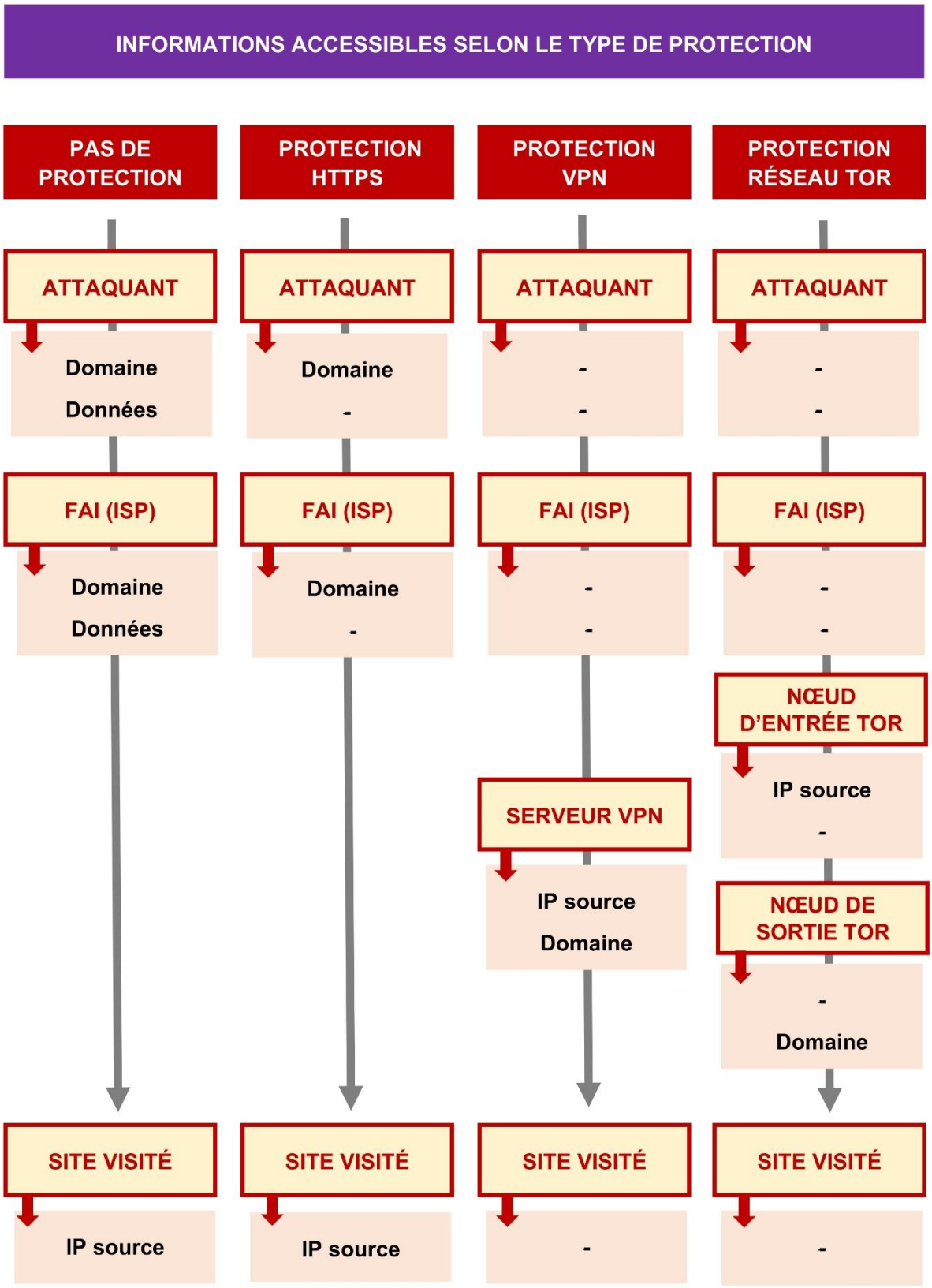
Le trafic est chiffré.

Les VPNs sont très utilisés pour accéder à l’Intranet d’une entreprise.</td></tr>
<tr><td>Anonymiseur en réseau
(Networked Anonymizer)</td><td>Tor</td></tr>
</table>

Conseil important

Lorsque vous utilisez Tor, vous devez placer le niveau de sécurité (dans les paramètres) à PLUS SÛR ou LE PLUS SÛR, pour éviter d’être l’objet d’une attaque. Un tas de personnages équivoques flânent en effet sur le darkweb…




INFORMATIONS ACCESSIBLES SELON LE TYPE DE PROTECTION
PAS DE PROTECTION
PROTECTION HTTPS
PROTECTION VPN
PROTECTION RÉSEAU TOR
ATTAQUANT
ATTAQUANT
ATTAQUANT
ATTAQUANT
Domaine
Données
Domaine
-
-
-
-
-
FAI (ISP)
FAI (ISP)
FAI (ISP)
FAI (ISP)
Domaine
Données
Domaine
-
-
-
-
-
NŒUD D'ENTRÉE TOR
IP source
-
SERVEUR VPN
IP source
Domaine
NŒUD DE SORTIE TOR
-
Domaine
SITE VISITÉ
SITE VISITÉ
SITE VISITÉ
SITE VISITÉ
IP source
IP source
-
-

Comment héberger un service caché sur votre ordinateur

Procédure sur Kali Linux

➔ **On installe Tor :**
- **sudo apt-get update**
- **sudo apt-get install tor torbrowser-launcher**

➔ **On crée le répertoire contenant le service caché sur le bureau :**
- **mkdir tor_service**

➔ **On se place dans ce répertoire et on lance un serveur web :**
- **cd tor_service**
- **python3 -m http.server --bind 127.0.0.1 8080**

➔ **On crée un fichier HTML simple (pour notre test) dans le répertoire tor_service**

➔ **On recherche et modifie le fichier torrc :**
- **whereis tor**
- **cd /etc/tor**
- **sudo nano torrc**
- **On décommente les deux lignes suivantes :**
  - **HiddenServiceDir /var/lib/tor/hidden_service**
  - **HiddenServicePort 80 127.0.0.1:8080**

On modifie le port qui suit les deux points : il doit valoir 8080.

➔ **On lance tor :**
- **sudo tor**

➔ **On recherche l'adresse de notre service caché :**
- **sudo -i**
- **cd /var/lib/tor/hidden_service**
- **cat hostname**

➔ **On vérifie l'adresse obtenue dans le navigateur Tor !**

```
 GNU nano 4.5                          torrc                          Modifié
#HashedControlPassword 16:872860B76453A77D60CA2BB8C1A7042072093276A3D701AD684053EC4C
#CookieAuthentication 1

############### This section is just for location-hidden services ###

## Once you have configured a hidden service, you can look at the
## contents of the file ".../hidden_service/hostname" for the address
## to tell people.
##
## HiddenServicePort x y:z says to redirect requests on port x to the
## address y:z.

#HiddenServiceDir /var/lib/tor/hidden_service/
#HiddenServicePort 80 127.0.0.1:80

HiddenServiceDir /var/lib/tor/hidden_service/
HiddenServicePort 80 127.0.0.1:8080
#HiddenServicePort 22 127.0.0.1:22

################ This section is just for relays #####################

^G Aide       ^O Écrire     ^W Chercher   ^K Couper     ^J Justifier  ^C Pos. cur.
^X Quitter    ^R Lire fich. ^\ Remplacer  ^U Coller     ^T Orthograp. ^_ Aller ligne
```

On décommente ces deux lignes et on modifie le port qui suit les deux points (il doit valoir 8080)

On recherche l'adresse du service caché :

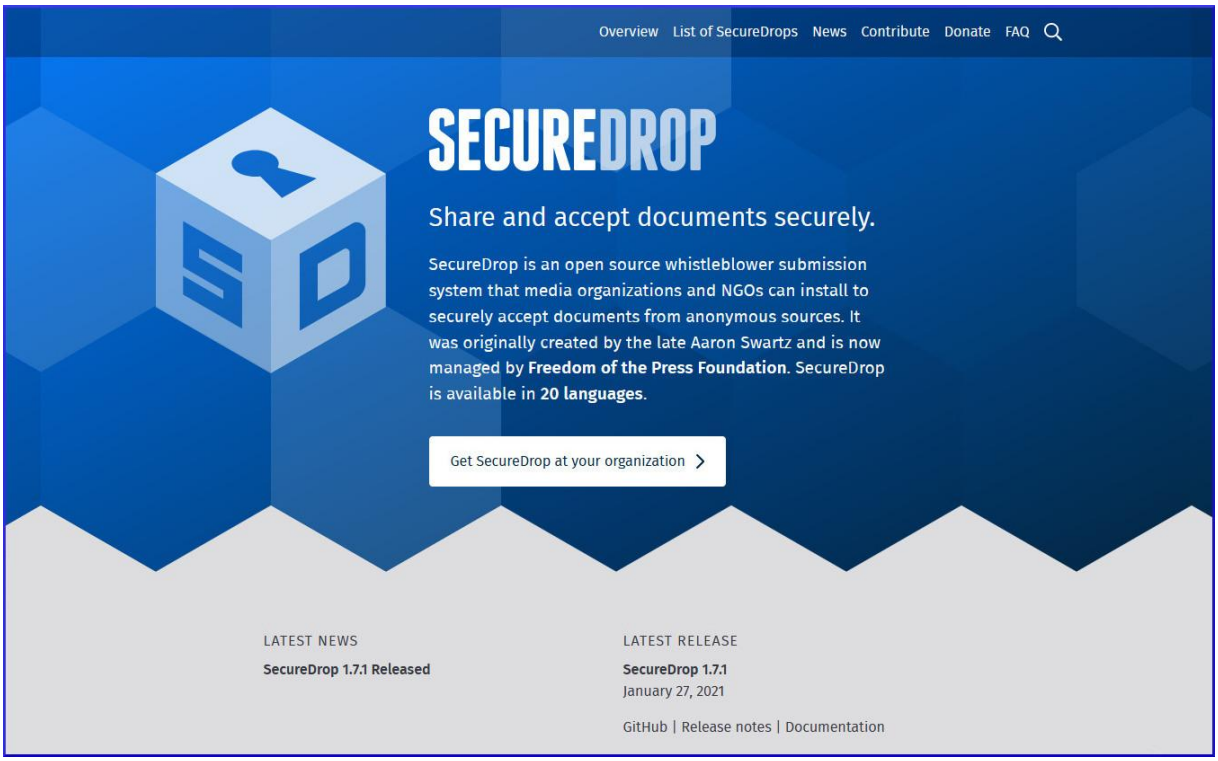
```
root@kali:~# cd /var/lib/tor
root@kali:/var/lib/tor# ls
hidden_service
root@kali:/var/lib/tor# cd hidden_service/
root@kali:/var/lib/tor/hidden_service# ls
authorized_clients  hostname  hs_ed25519_public_key  hs_ed25519_secret_key
root@kali:/var/lib/tor/hidden_service# cat hostname
eudtpz67znrnptoooddaweihhqlqa6mm4gngmjeuf2ji6e36odbzqfyd.onion
root@kali:/var/lib/tor/hidden_service#
```

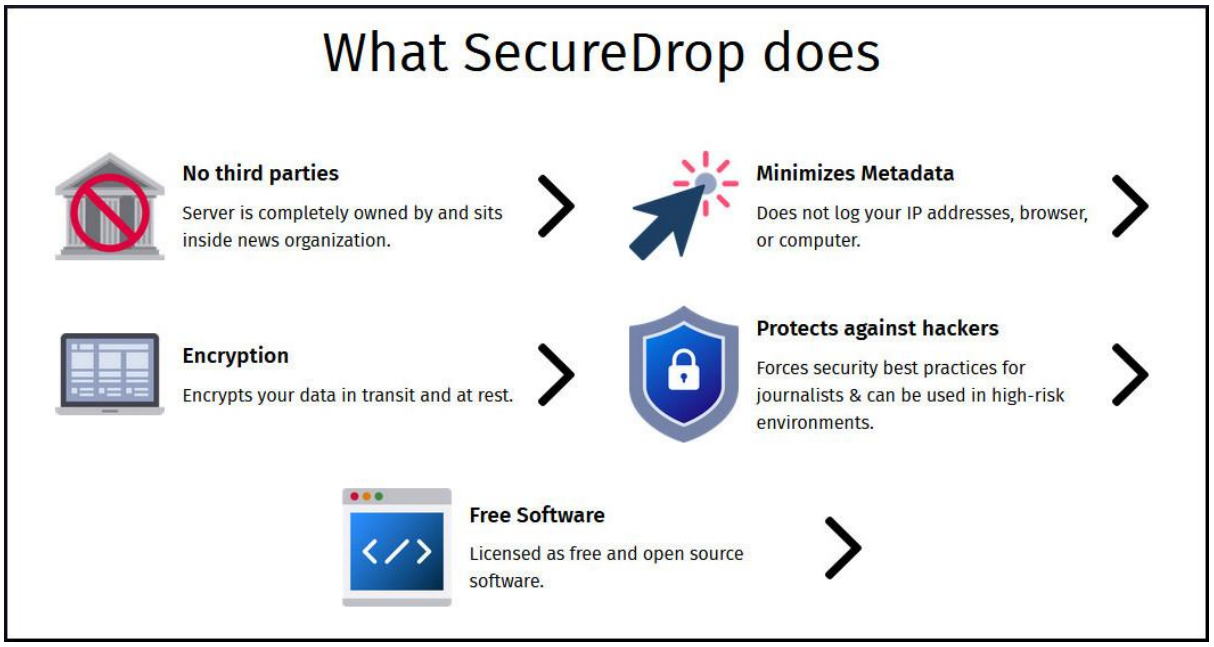
Notre service caché Tor est bien accessible !

Pour les lanceurs d'alerte : la solution SecureDrop

SecureDrop est un système de communication chiffré (utilisant le réseau Tor) qui permet à ses utilisateurs d'envoyer des informations anonymement (hackers éthiques, journalistes, lanceurs d'alerte, vous ou moi…) Le journal britannique *The Guardian,* notamment, permet aujourd'hui l'envoi de documents via SecureDrop.

Vous pouvez en savoir plus sur le site : https://securedrop.org/





Les moteurs de recherche qui ne vous espionnent pas

De nombreuses personnes ne désirent plus utiliser les moteurs de recherche Google et Bing[8] qui possèdent une très mauvaise réputation quant au respect de votre vie privée et de votre anonymat.

Heureusement, il existe des alternatives vraiment intéressantes. Je vais en citer trois principales :

1. **Startpage**
2. **Qwant**
3. **DuckDuckGo**

→

Ces trois moteurs de recherche :

- **N'enregistrent pas votre adresse IP**
- **Ne vous tracent pas (pas de cookies traceurs)**
- **N'enregistrent pas la signature de votre navigateur**

Je parlerai, pour terminer, d'un moteur de recherche un peu à part : YaCy.

Startpage [www.startpage.com]

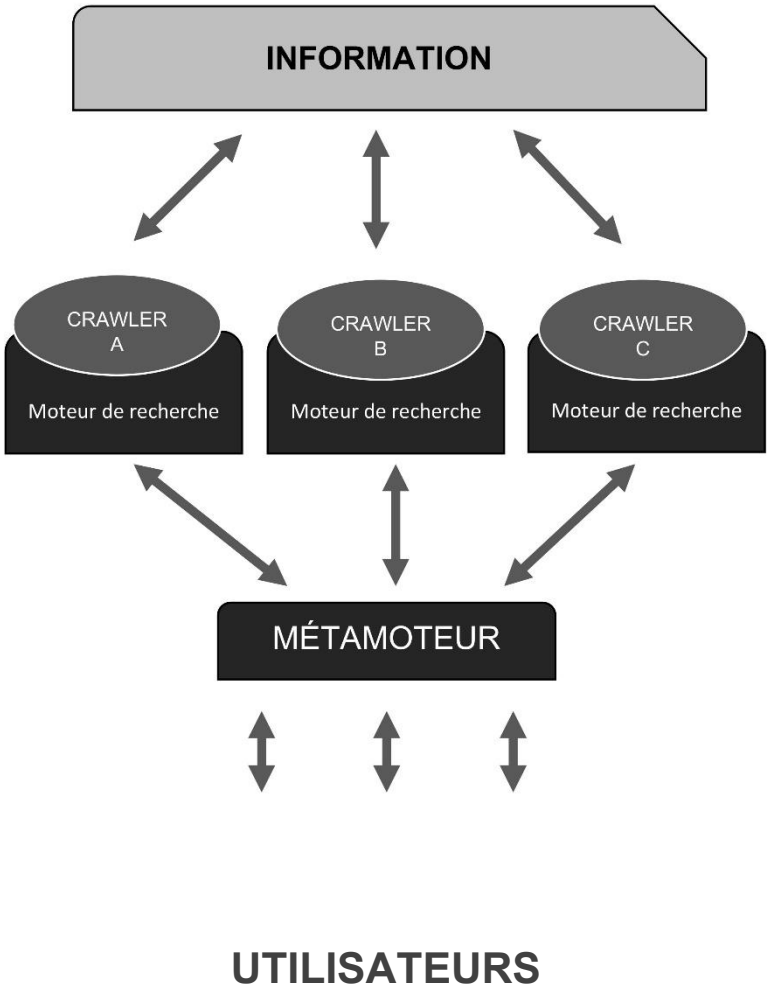
Startpage, qui était connu jusqu' en 2016 sous le nom d'Ixquick, se base sur les résultats de Google. Il ne trace pas les utilisateurs et ne génère donc pas de cookies traceurs. Startpage affirme ne livrer aucune donnée concernant les

[8] **Bing est un moteur de recherche semblable à Google et produit par Microsoft.**

utilisateurs à son partenaire Google. Le financement de Startpage est réalisé via des publicités non personnalisées.
Startpage est un métamoteur de recherche. Un métamoteur est un moteur qui puise ses informations à travers plusieurs autres moteurs de recherche (comme Google, Yahoo, …) L'avantage pour l'utilisateur est d'obtenir les résultats combinés de plusieurs moteurs en n'en utilisant qu'un seul.

Le moteur de recherche, quant à lui, collecte l'information sur le Web grâce à des robots d'indexation. Le robot d'indexation est encore appelé web crawler ou web spider.

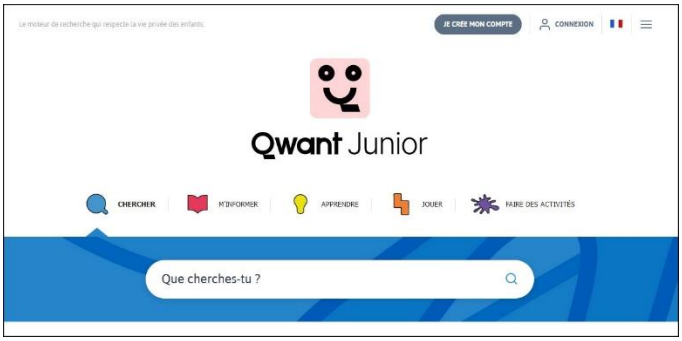
Schématiquement :



Qwant [www.qwant.com/]

Qwant est un moteur de recherche français qui existe depuis 2013. Comme Startpage, il affirme ne pas journaliser les adresses IP des utilisateurs ni faire commerce de leurs données personnelles. Qwant n'installe pas de cookies traceurs et ne piste pas ses utilisateurs. Les seuls cookies utilisés sont temporaires et les cookies commerciaux sont bloqués. Qwant est un moteur de recherche qui indexe lui-même les pages web via des robots d'indexation. Ce n'est donc pas un métamoteur comme Startpage. Le financement de Qwant se fait par la location de ses technologies de recherche aux entreprises.

Le nombre d'utilisateurs de Qwant est passé de 10 millions en 2015 à près de 80 millions en 2019.



Qwant Junior est un moteur de recherche adapté pour les enfants de 6 à 13 ans.

DuckDuckGo [https://duckduckgo.com/]

Avec un nom plutôt original, DuckDuckGo est un métamoteur (comme Startpage), situé aux USA, mais qui utilise également ses propres robots d'indexation (cette méthode hybride est intéressante). Le financement se fait par de la publicité non personnalisée. Le gros problème pour DuckDuckGo, en tant que moteur de recherche qui respecte l'anonymat, est que ses serveurs sont localisés aux USA. Il tombe donc sous la loi américaine qui oblige le partage des données (cf. le scandale PRISM dénoncé par Edward Snowden).

EN RÉSUMÉ :

MOTEURS	AVANTAGES	INCONVÉNIENTS
STARTPAGE	**Recherche anonyme** **Serveurs européens**	**Utilise les données de Google**
QWANT	**Recherche anonyme** **Serveurs européens** **Robots d'indexations propres**	**Résultats parfois moins pertinents**
DUCKDUCKGO	**Recherche anonyme** **Méthode hybride**	**Serveurs localisés aux USA**

POUR CLORE CE CHAPITRE : YaCy, un moteur de recherche décentralisé

Voici un dernier moteur de recherche original : YaCy. YaCy est un moteur de recherche libre et non centralisé qui existe depuis 2003 : c'est un moteur de recherche distribué écrit en Java, et fonctionnant sur le principe des réseaux peer-to-peer (P2P). Aucune entreprise ne contrôle donc ce moteur de recherche original, ni aucun individu. Les machines du réseau hébergent l'index de résultats et partagent les informations.

Ses principaux avantages sont les suivants : il ne possède pas de serveur central, il protège la vie privée des utilisateurs et il n'est pas censuré.

YaCy est disponible pour Windows, Linux et Mac.

Vous pouvez l'installer sur votre ordinateur à partir du site officiel : https://yacy.net.

```
root@kali:/opt/yacy# ./startYACY.sh
****************** YaCy Web Crawler/Indexer & Search Engine ******************
**** (C) by Michael Peter Christen, usage granted under the GPL Version 2  ****
****   USE AT YOUR OWN RISK! Project home and releases: http://yacy.net/   ****
**  LOG of       YaCy: DATA/LOG/yacy00.log (and yacy<xx>.log)                **
**  STOP         YaCy: execute stopYACY.sh and wait some seconds             **
**  GET HELP for YaCy: join our community at https://searchlab.eu            **
******************************************************************************
 >> YaCy started as daemon process. Administration at http://localhost:8090 <<
root@kali:/opt/yacy#
```

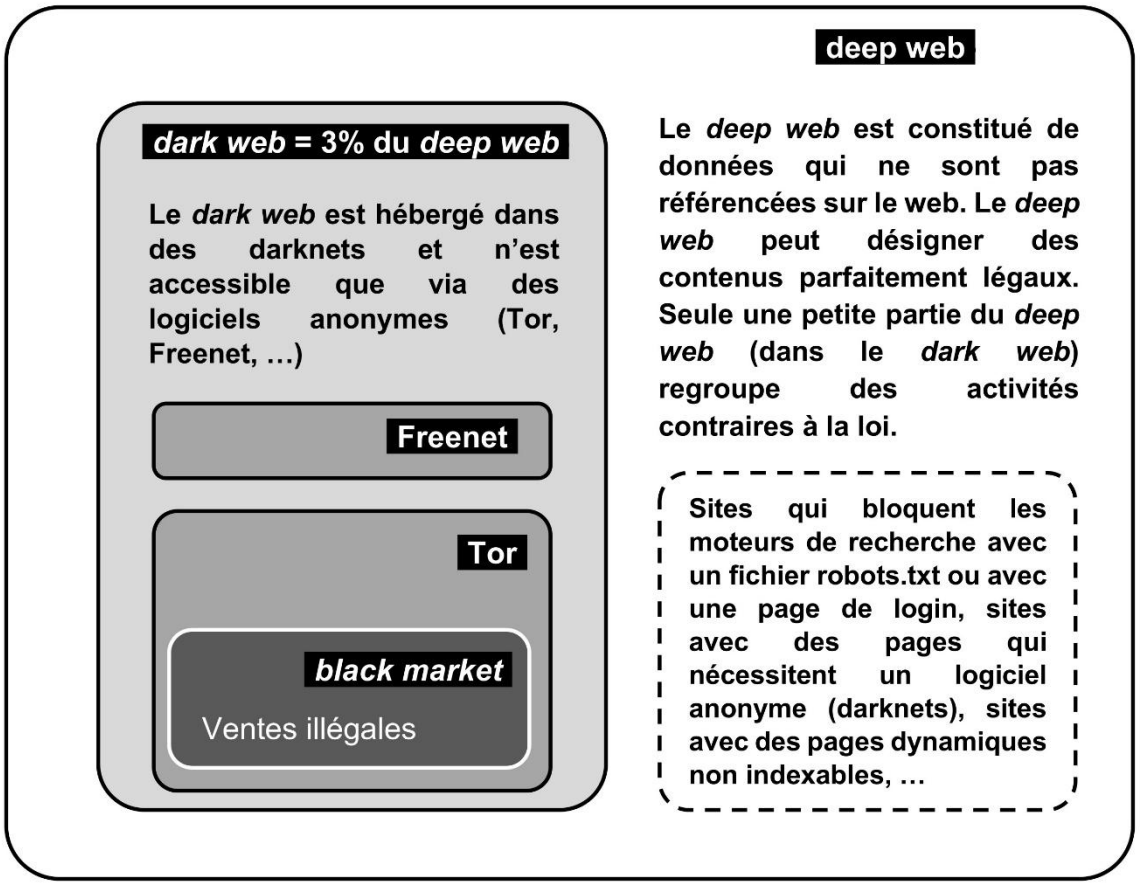
J'ai ici installé très facilement YaCy sur Kali Linux.

Le seul petit inconvénient de YaCy est qu'il fournit souvent des résultats moins pertinents que les moteurs plus célèbres. Je vous laisse tester YaCy et vous faire votre propre avis…

Deep Web / Dark Web / Black Market

Définitions :

Web = web visible (10%) + *deep web* (90%)



Le *deep web* contient des bases de données académiques, des enregistrements médicaux, des documents gouvernementaux, des données bancaires, … Vous allez tous les jours sur le *deep web* sans le savoir (connexion à votre banque, …) !

Le *dark web*, web clandestin ou web caché (constitué de sites web cachés), est accessible seulement via des logiciels comme Tor (ou Freenet) et est hébergé sur des réseaux appelés darknets.

Freenet est un réseau anonyme qui permet la liberté d'expression (politique).

Tor est un réseau anonyme et décentralisé. TOR est l'abréviation de The Onion Router. Les sites de ce réseau ont un nom .onion. Pour cette raison, le Dark Web TOR est souvent appelé ONIONLAND. Le navigateur Tor permet de visiter les sites en .onion.

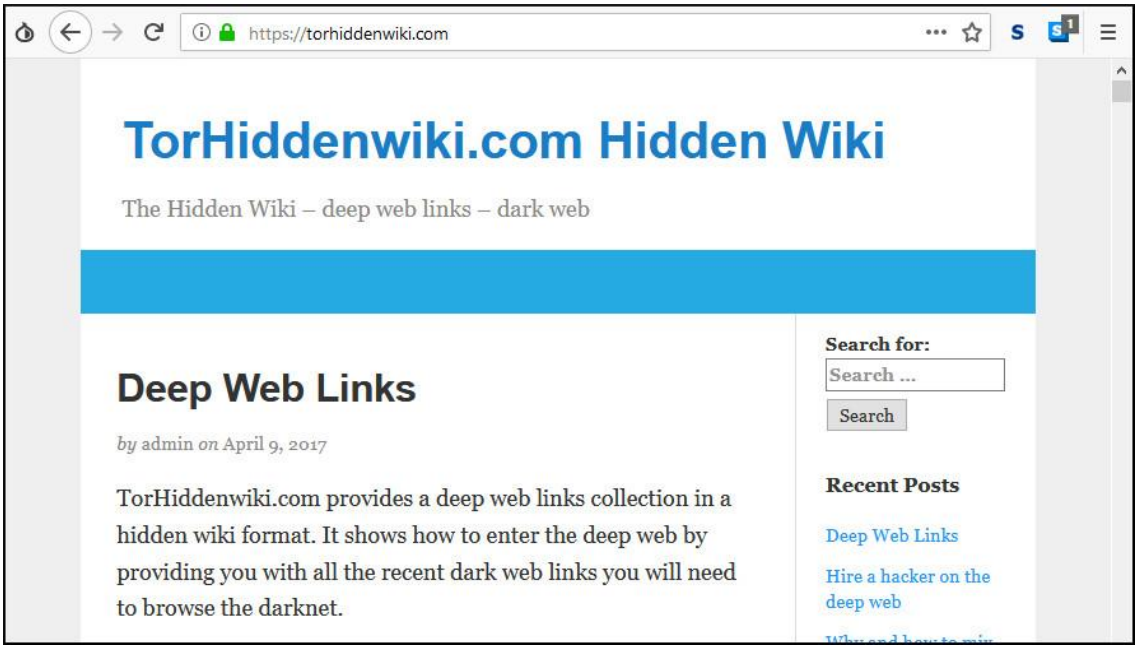
Dans les boutiques du *black market*, le paiement se fait souvent en monnaie virtuelle (Bitcoin, …) Les sites de ces boutiques ont des adresses en .onion qui ne sont donc

accessibles que via le réseau Tor. On y trouve des faux-papiers, de la drogue, des coordonnées bancaires, des armes, bref tout ce qui est illégal…

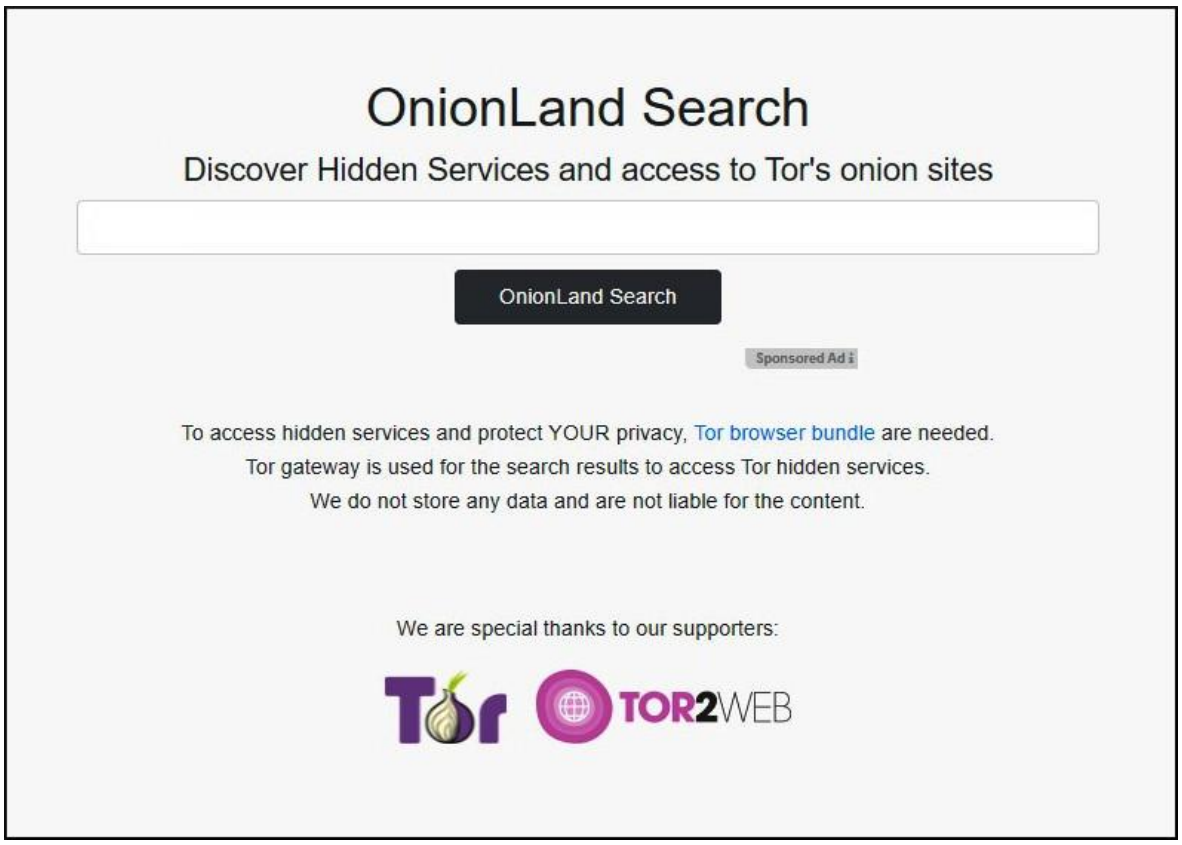
Un exemple célèbre de boutique du *black market* est Silk Road. Ce site a été plusieurs fois fermé par le FBI.

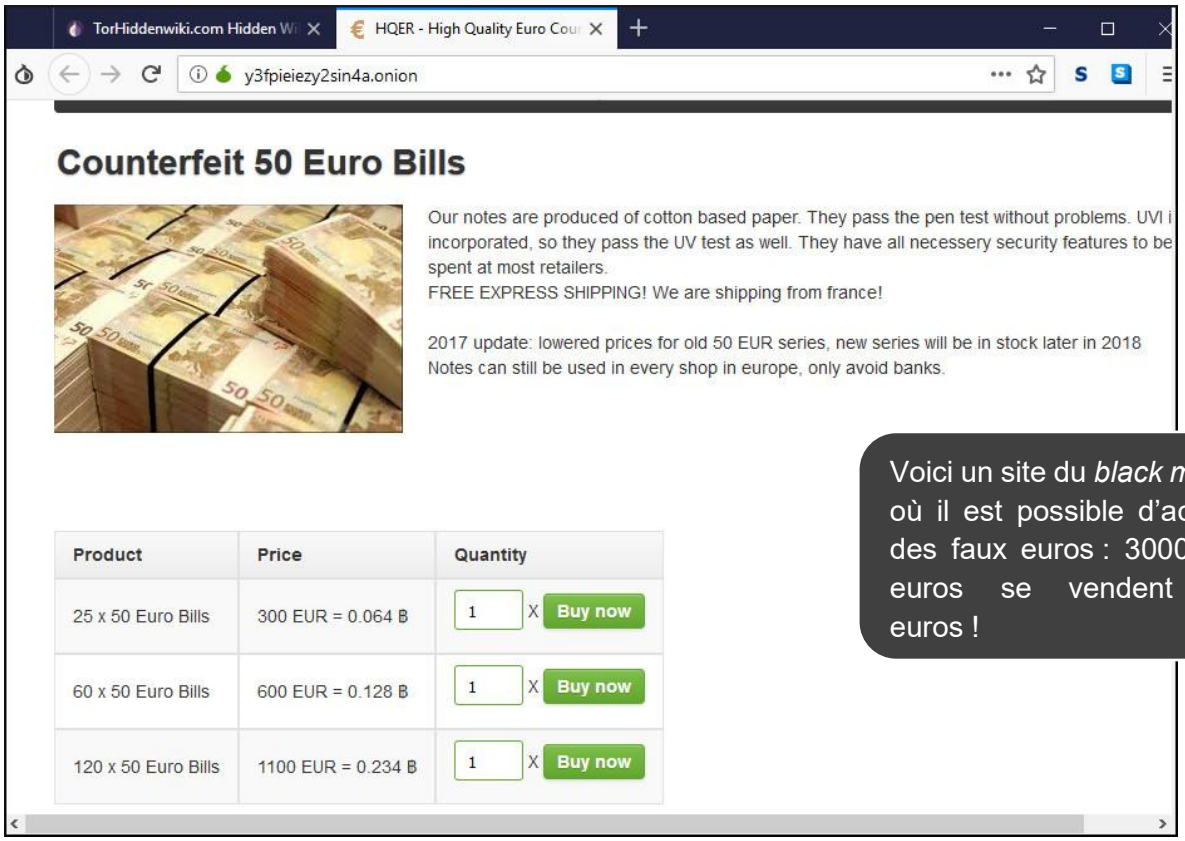
Voici le message affiché par le FBI sur le site *Silk Road*, après sa saisie en 2013 :

On peut trouver des liens pour le *deep web* sur TorHiddenwiki.com :

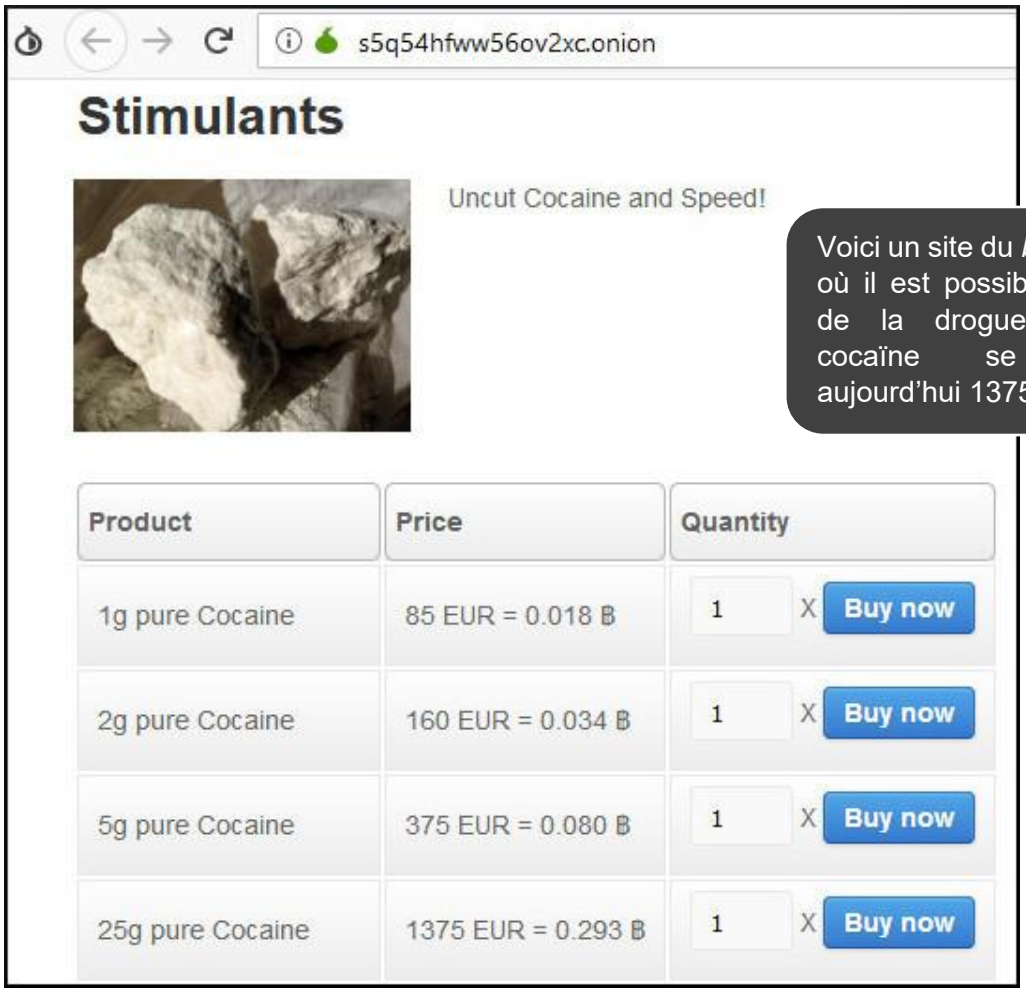


L'ancien site https://onionlandsearchengine.com/ **(lien obsolète) permettait de trouver avec votre navigateur classique des liens en .onion sur le *dark web* :**

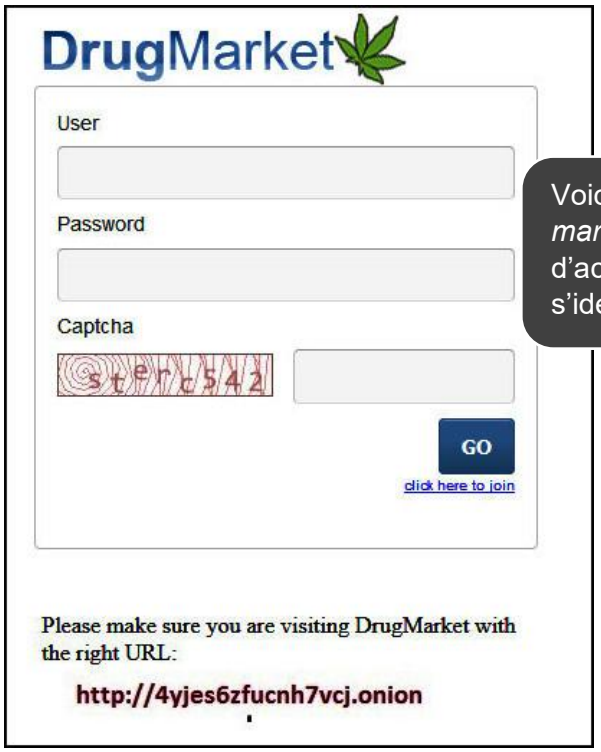




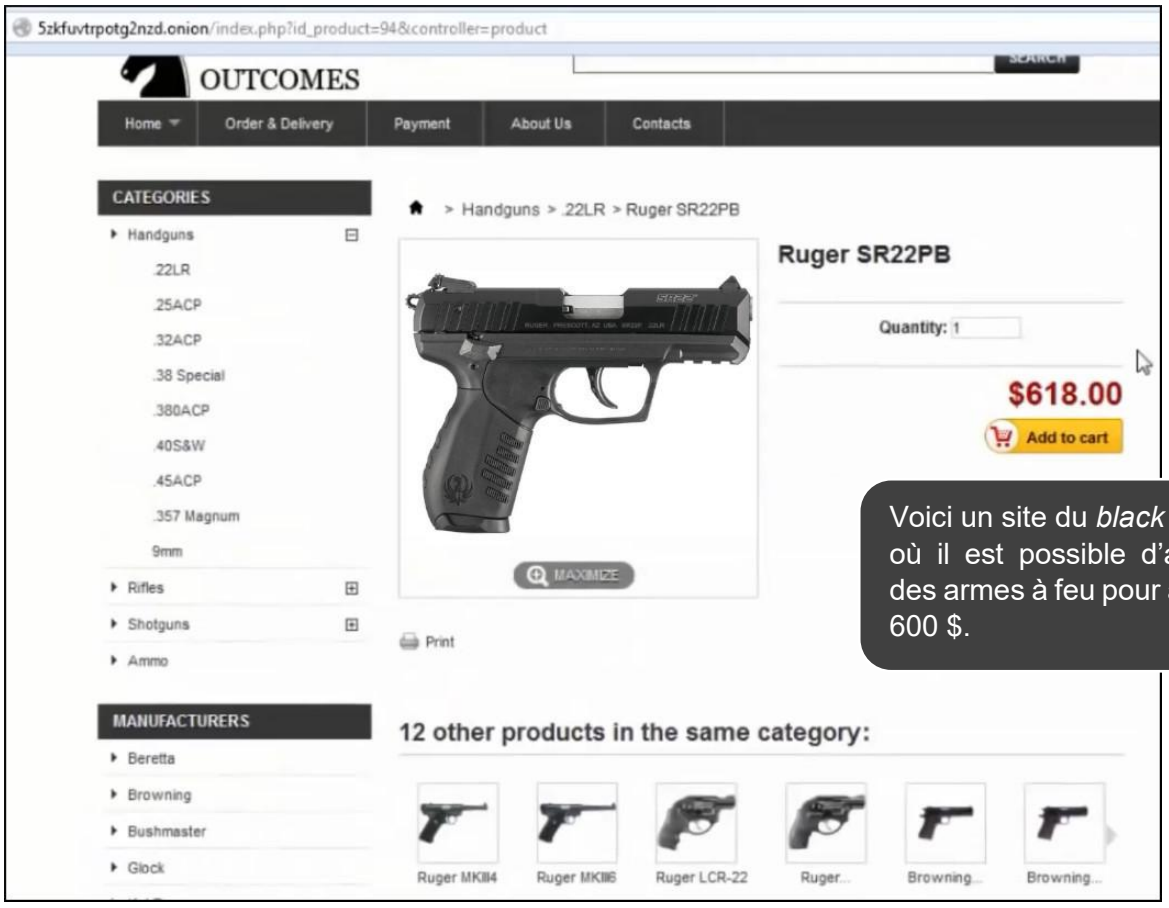
Voici un site du *black market* où il est possible d'acheter des faux euros : 3000 faux euros se vendent 600 euros !



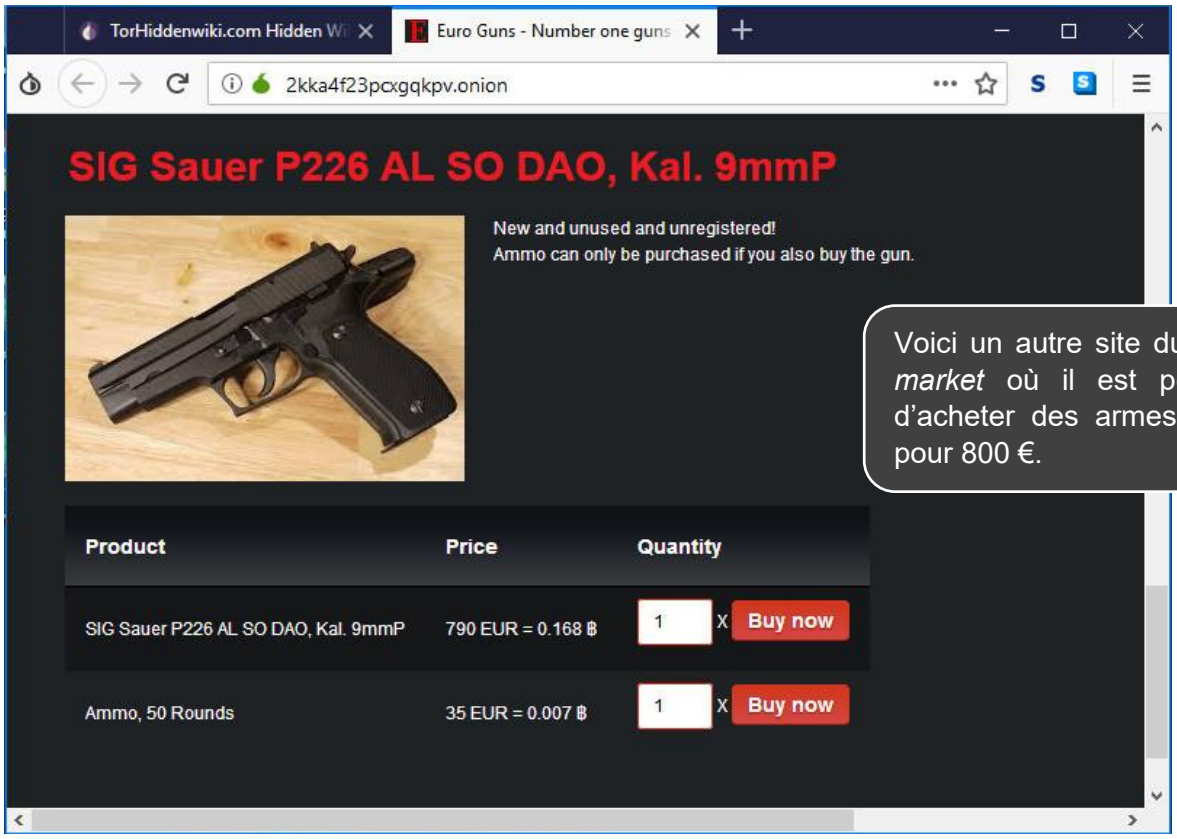
Voici un site du *black market* où il est possible d'acheter de la drogue : 25g de cocaïne se vendent aujourd'hui 1375 euros !



Voici un autre site du *black market* où il est possible d'acheter de la drogue en s'identifiant au préalable.

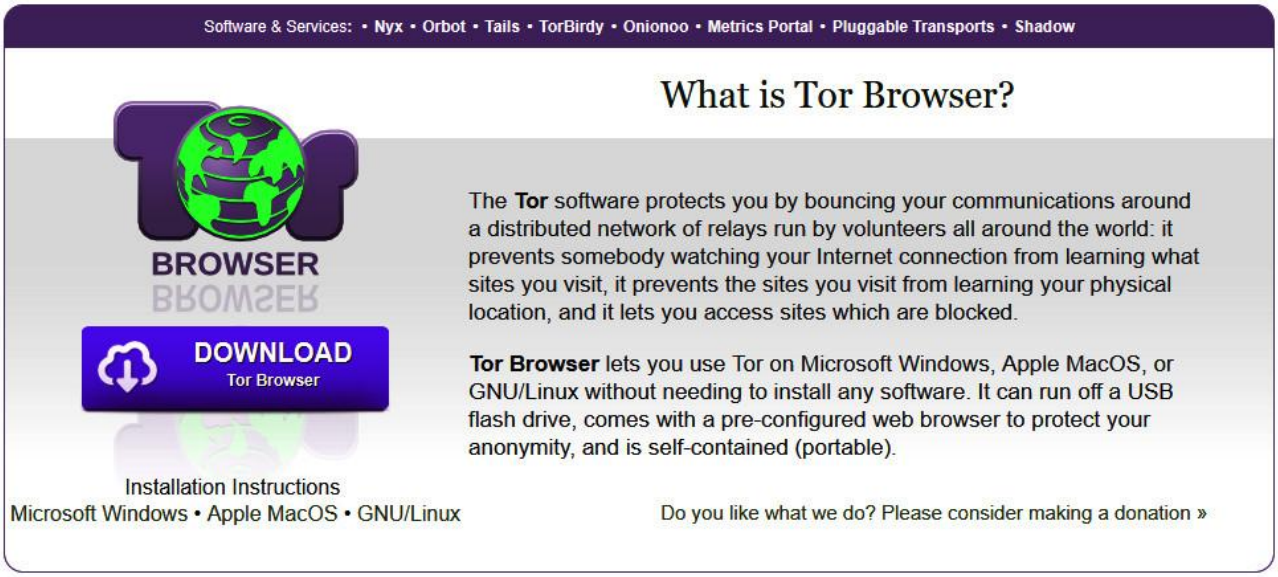


Voici un site du *black market* où il est possible d'acheter des armes à feu pour à peine 600 $.

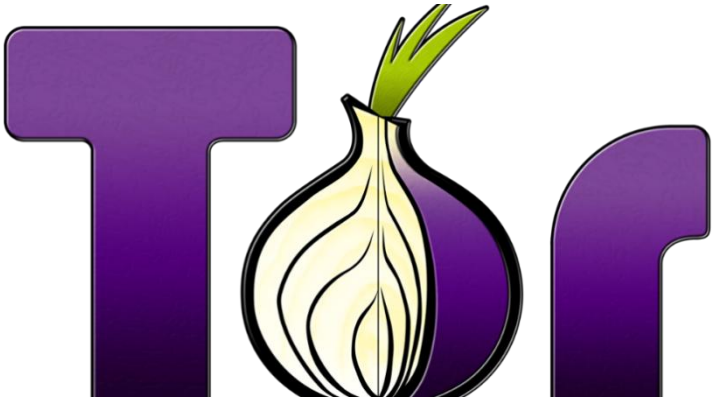


Voici un autre site du *black market* où il est possible d'acheter des armes à feu pour 800 €.

Il n'est pas recommandé d'utiliser le navigateur Tor avec Windows. L'idéal est d'utiliser le réseau Tor avec le système d'exploitation Linux, par exemple Tails (live USB).



Vous pouvez visiter les sites du *black market* par simple curiosité, mais je vous déconseille vivement d'y acheter des produits illégaux. L'expert en cybersécurité se doit de respecter la loi, en toutes circonstances. Pour en savoir plus sur le sujet, vous pouvez lire le chapitre suivant intitulé *Comment surfer sur le Darknet*.



Comment surfer sur le Darknet

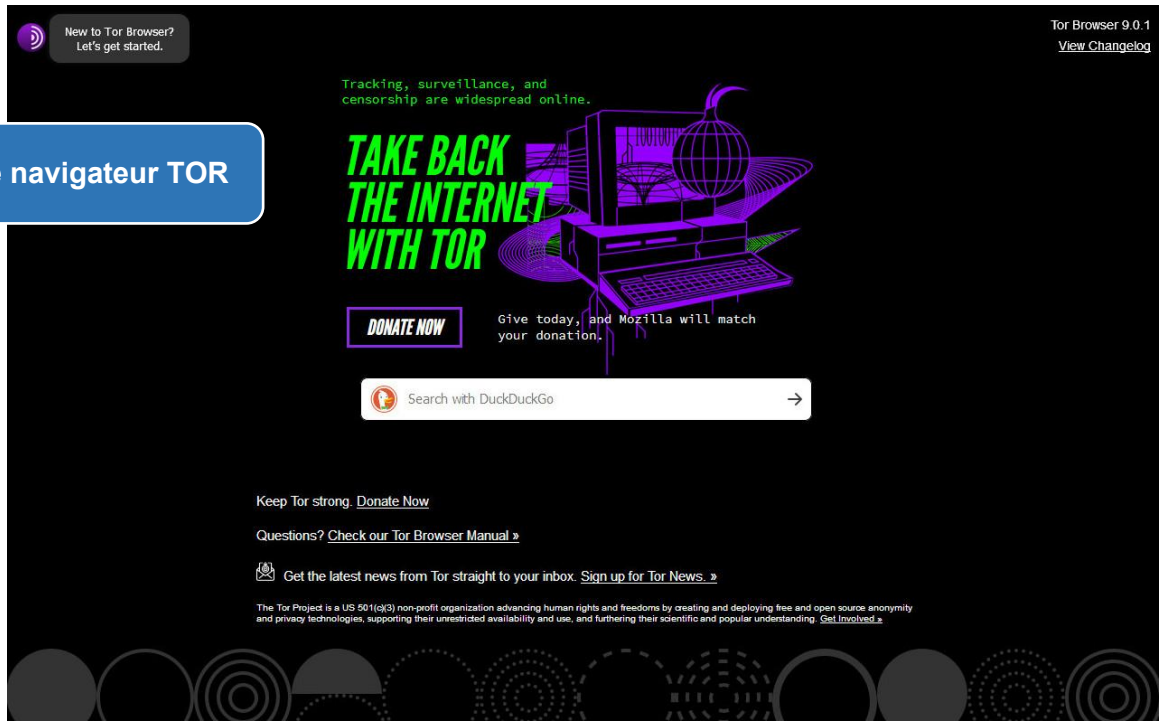
Les adresses dans le Darknet (adresses en .onion) changent régulièrement. Pour pouvoir les retrouver, voici comment faire :

On utilise le navigateur Tor et le moteur de recherche DuckDuckGo (qui ne collecte, contrairement à Google, aucune donnée sur ses utilisateurs), de préférence avec son adresse en .onion, de façon à obtenir l'adresse d'autres moteurs de recherche spécialisés sur le Darknet (comme notevil, torch ou ahmia)

Au moment où j'écris ces lignes, les adresses sont les suivantes (ce sera peut-être différent pour vous) :

MOTEUR DE RECHERCHE	ADRESSE
duckduckgo	**duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion**
Tor66	**http://tor66sewebgixwhcqfnp5inzp5x5uohhdy3kvtnyfxc2e5mxiuh34iid.onion/**
torch	**xmh57jrknzkhv6y3ls3ubitzfqnkrwxhopf5aygthi7d6rplyvk3noyd.onion**
ahmia	**http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion/**
Excavator	**http://2fd6cemt4gmccflhm6imvdfvli3nf7zn6rfrwpsy7uhxrgbypvwf5fad.onion/**

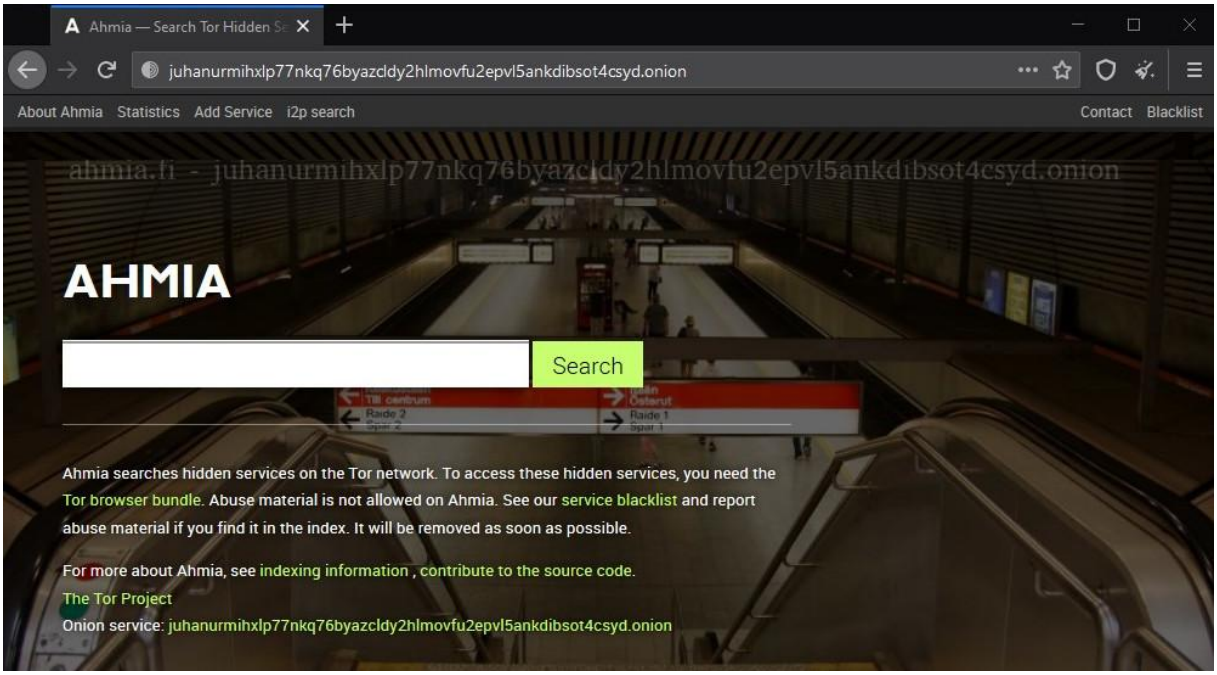
Le navigateur TOR



Le moteur de recherche excavator :

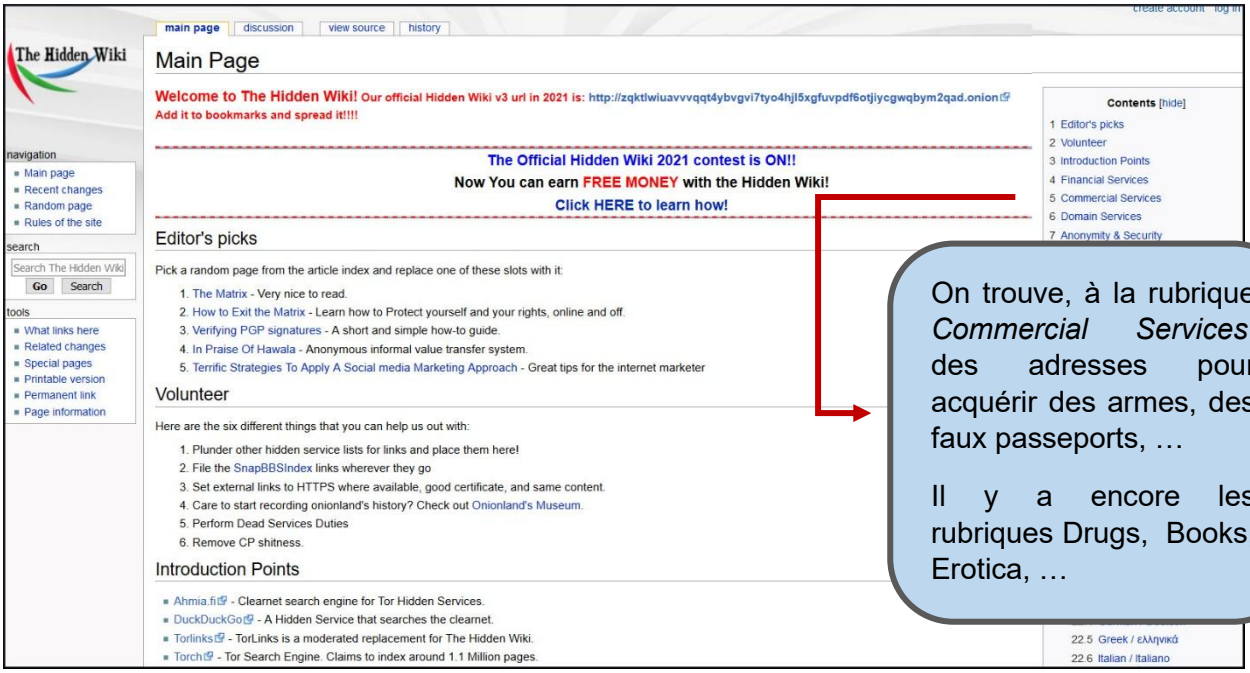
Le moteur de recherche torch (qui est moins conseillé car il affiche beaucoup de publicités et il ralentit la navigation) :

Le dernier moteur de recherche permet uniquement de trouver des sites en .onion :



Il est maintenant possible de trouver l'adresse des services du Darknet, comme le Hidden Wiki :

zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/wiki/index.php/Main_Page



On trouve, à la rubrique *Commercial Services*, des adresses pour acquérir des armes, des faux passeports, …

Il y a encore les rubriques Drugs, Books, Erotica, …

Le moteur de recherche VormWeb

VormWeb (https://vormweb.de/en/) est un moteur de recherche dédié au Darknet, mais accessible aussi bien depuis le DarkNet que depuis le ClearNet (web classique). Il est donc accessible avec Chrome ou Firefox. Tor Browser n'est pas obligatoire.

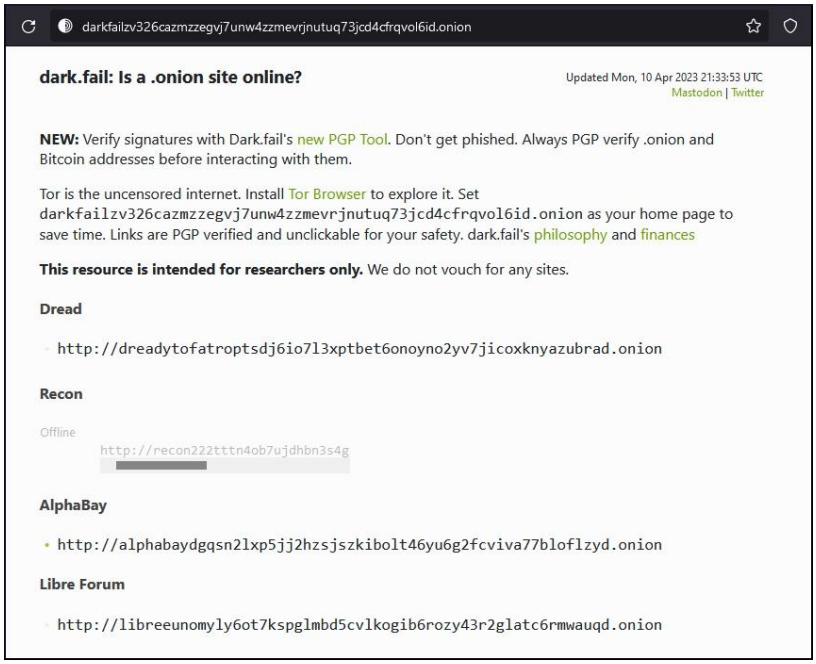
Ce moteur diffère de ses concurrents (comme Ahmia) par son système de classement des résultats :

➔ en vert		sites fiables
➔ en jaune		sites à consulter avec prudence
➔ en rouge		sites dangereux

Ce site, créé en 2021 par le Vormrodian Projects, n'utilise pas de trackers et préserve votre anonymat.

Il est même possible de trouver des adresses plus actualisées de services cachés (par rapport à celles du Hidden Wiki) à l'adresse de dark.fail :

http://darkfailzv326cazmzzegvj7unw4zzmevrjnutuq73jcd4cfrqvol6id.onion



Voici, sur un de ces sites, les prix pour de fausses cartes d'identité.

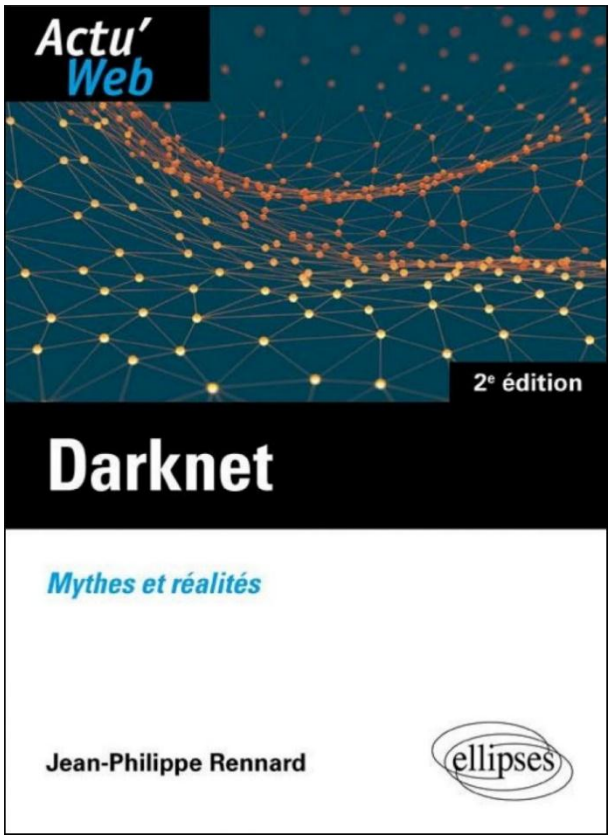
Product	Price	Quantity
Czech ID Card	500 EUR = 0.080 ฿	1 X Buy now
Netherlands ID Card	550 EUR = 0.088 ฿	1 X Buy now
Denmark ID Card	550 EUR = 0.088 ฿	1 X Buy now
French ID Card	550 EUR = 0.088 ฿	1 X Buy now
Lithuanian ID Card	550 EUR = 0.088 ฿	1 X Buy now

Product	Price	Quantity
Lithuanian Passport	1350 EUR = 0.215 ฿	1 X Buy now
Netherlands Passport	1500 EUR = 0.239 ฿	1 X Buy now
Denmark Passport	1500 EUR = 0.239 ฿	1 X Buy now
Great Britain Passport	1800 EUR = 0.287 ฿	1 X Buy now
Canada Passport	1250 EUR = 0.199 ฿	1 X Buy now

Et, sur le même site, le prix pour de faux passeports, qui sont un peu plus onéreux.

Darknet : mythes et réalités

Je vous conseille vivement l'achat et la lecture du livre ci-dessous :

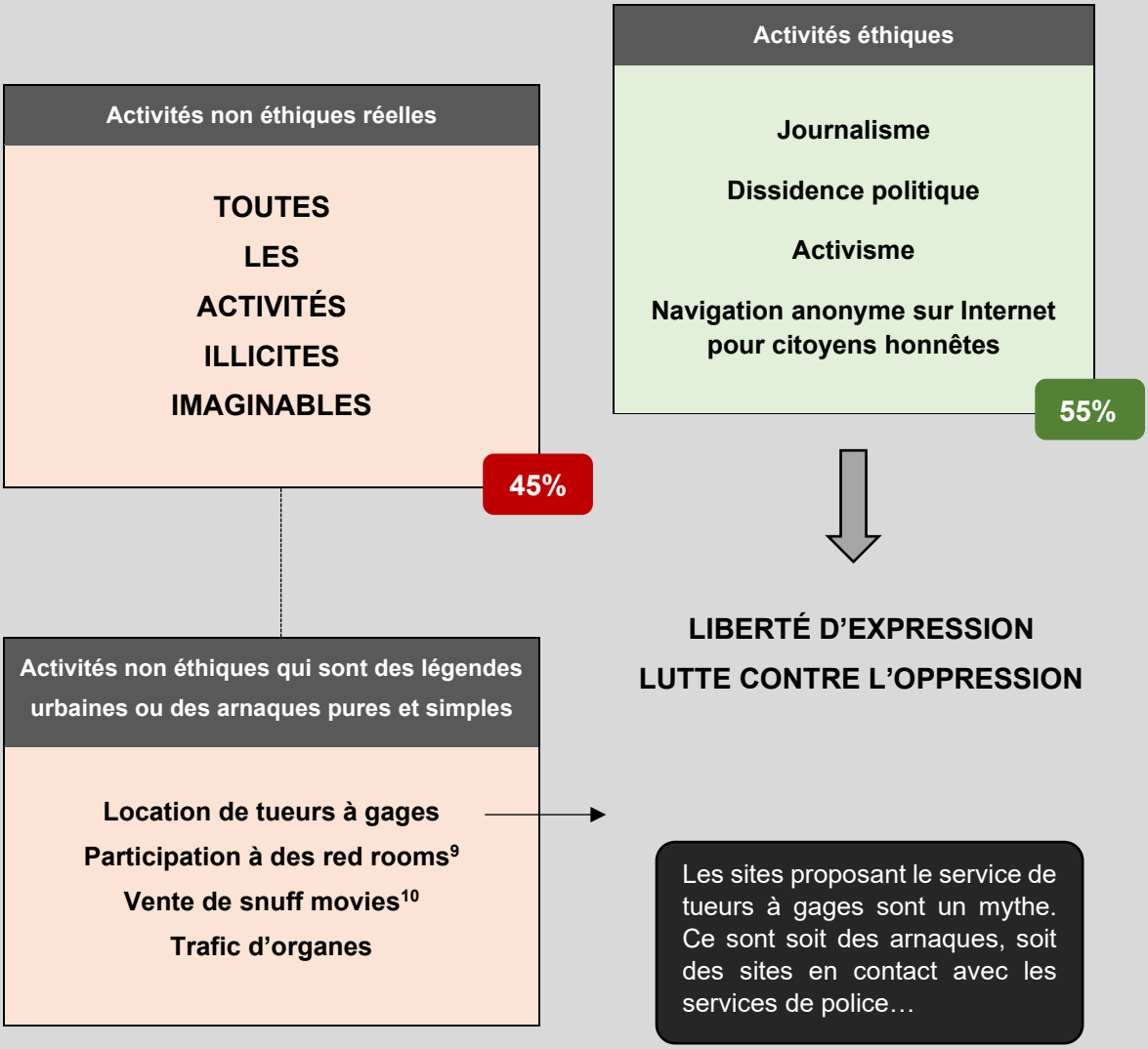


L'Internet classique auquel on oppose le Darknet est aussi appelé Clearnet. Le Darknet est quant à lui formé de différents darknets qui sont des sous-réseaux pair-à-pair utilisant des protocoles spécifiques et procurant un certain anonymat. Il n'y a pas vraiment d'anonymat sur le Clearnet.

Si vous désirez naviguer sur Internet avec un bon anonymat, quatre outils sont à considérer :

- **Tails** **(https://tails.net/)**
- **Heads** **(https://heads.dyne.org/)**
- **Whonix** **(https://www.whonix.org/)**
- **Subgraph OS** **(https://subgraph.com/sgos/)**

TABLEAU : LE DARKNET



D'après Guitton (cité par J.-P. Rennard), les activités non éthiques représentent 45% du Darknet (dont 18% pour la pédopornographie) et les activités éthiques 55%. Il ne faut donc pas jeter le bébé avec l'eau du bain : le Darknet ne se résume pas à *Silk Road*… Les gouvernements, qui veulent tout contrôler, trompent la population sur le sujet car le Darknet est aussi le dernier espace de liberté dans l'Internet d'aujourd'hui.

[9] Les red rooms sont des plateformes où il serait possible d'assister et participer à des séances de torture en temps réel. Il s'agit d'une légende urbaine.
[10] Les snuff movies sont des vidéos de torture, viol ou meurtre. Il s'agit d'une autre légende urbaine.

Imbrication de plusieurs services d'anonymisation

Il est possible d'imbriquer plusieurs services d'anonymisation afin d'accroître votre sécurité. On parle en anglais de *nested VPN*, *nested SSH*, …

On peut appliquer cette méthode (nesting) aux services suivants :

- **proxys**
- **VPN**
- **Tunnels SSH**
- **JonDoNym**
- **I2P (*Invisible Internet Project*)**
- **Tor**

Quelques exemples d'imbrications

Nested VPN

(UTILISATEUR) ► VPN ► VPN ► (INTERNET)

Nested SSH

(UTILISATEUR) ► SSH ► SSH ► (INTERNET)

(SSH / VPN / JonDoNym comme premier hop) & (Tor comme dernier hop) **(- sécurisé)**

(UTILISATEUR) ► VPN ► Tor ► (INTERNET)

(UTILISATEUR) ► SSH ► Tor ► (INTERNET)

(UTILISATEUR) ► JonDoNym ► Tor ► (INTERNET)

(Tor comme premier hop) & (SSH / VPN / JonDoNym comme dernier hop) **(+ sécurisé)**

(UTILISATEUR) ► Tor ► JonDoNym ► (INTERNET)

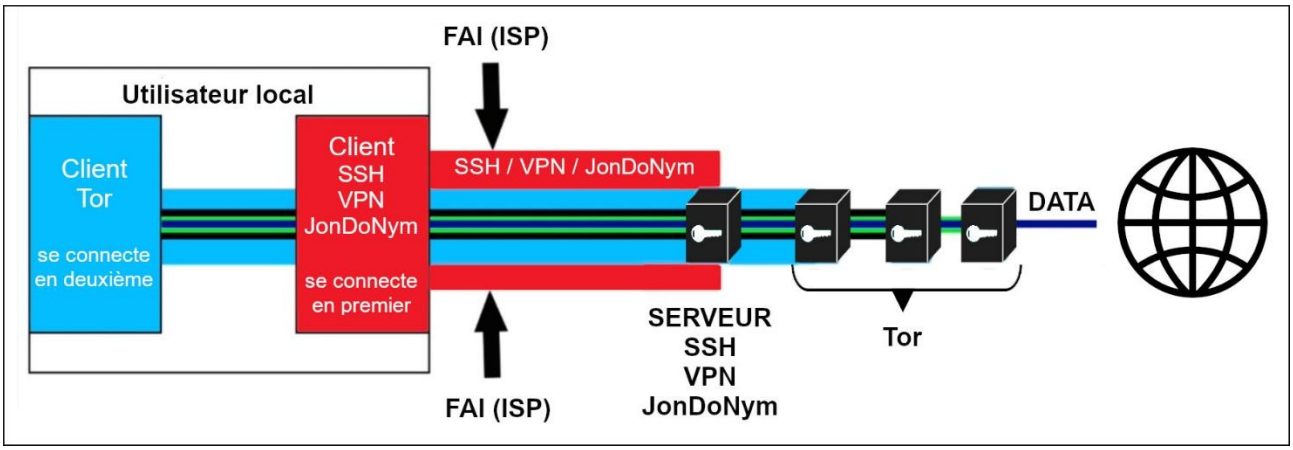
(UTILISATEUR) ► Tor ► SSH ► (INTERNET)

(UTILISATEUR) ► Tor ► VPN ► (INTERNET)

Avantage du double VPN : le premier VPN connaît votre adresse IP réelle et celle du deuxième VPN tandis que le second VPN connaît l'adresse finale et celle du premier VPN. Aucun des deux VPN ne connaît donc à la fois d'adresse finale et votre IP réelle !

Exemple 1

(UTILISATEUR) ► SSH / VPN / JonDoNym ► Tor ► (INTERNET)



Avantages

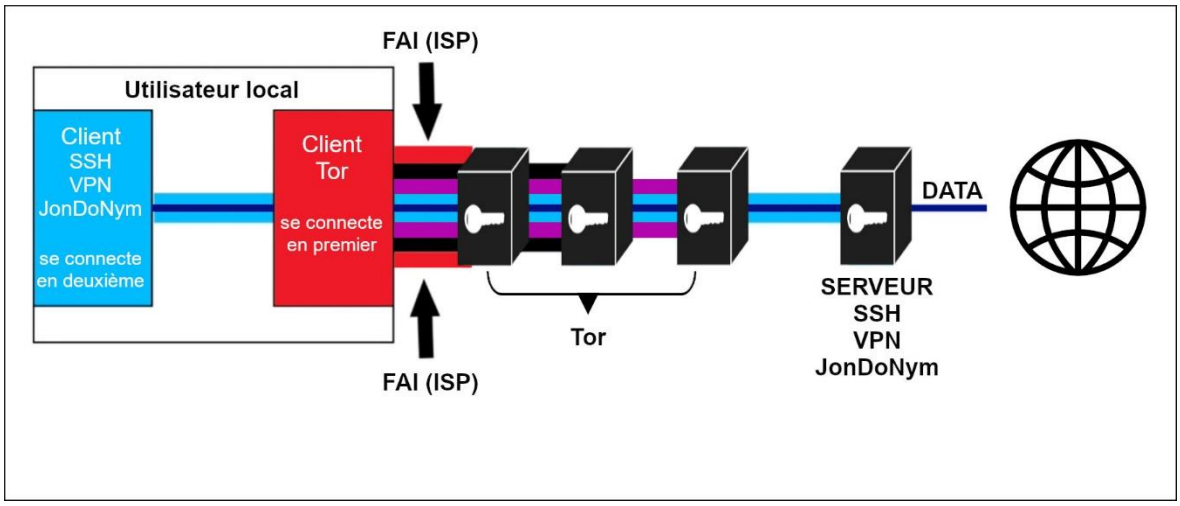
- **Peut être utilisé si la censure ou le FAI bloquent Tor et pas SSH / VPN / JonDoNym,**
- **Tor en deuxième hop permet un accès aux sites cachés en .onion (hidden services),**
- **Peut être utilisé si vous avez peur d'une attaque sur le réseau Tor (attaque par corrélation, …), Le premier hop procure une sécurité supplémentaire.**

Inconvénients

- **Avec SSH ou VPN en premier hop, il peut y avoir des fuites DNS ou IPv6 en cas de mauvaise configuration. Le trafic sera également envoyé en clair en cas de déconnexion,**
- **Si la destination finale bannit les exit nodes de Tor, vous serez bloqué,**
- **Si vous oubliez de créer manuellement le tunnel du premier hop, le FAI verra que vous utilisez Tor, ce qui peut être un problème dans certains pays.**

Exemple 2

(UTILISATEUR) ► Tor ► SSH / VPN / JonDoNym ► (INTERNET)



Avantages

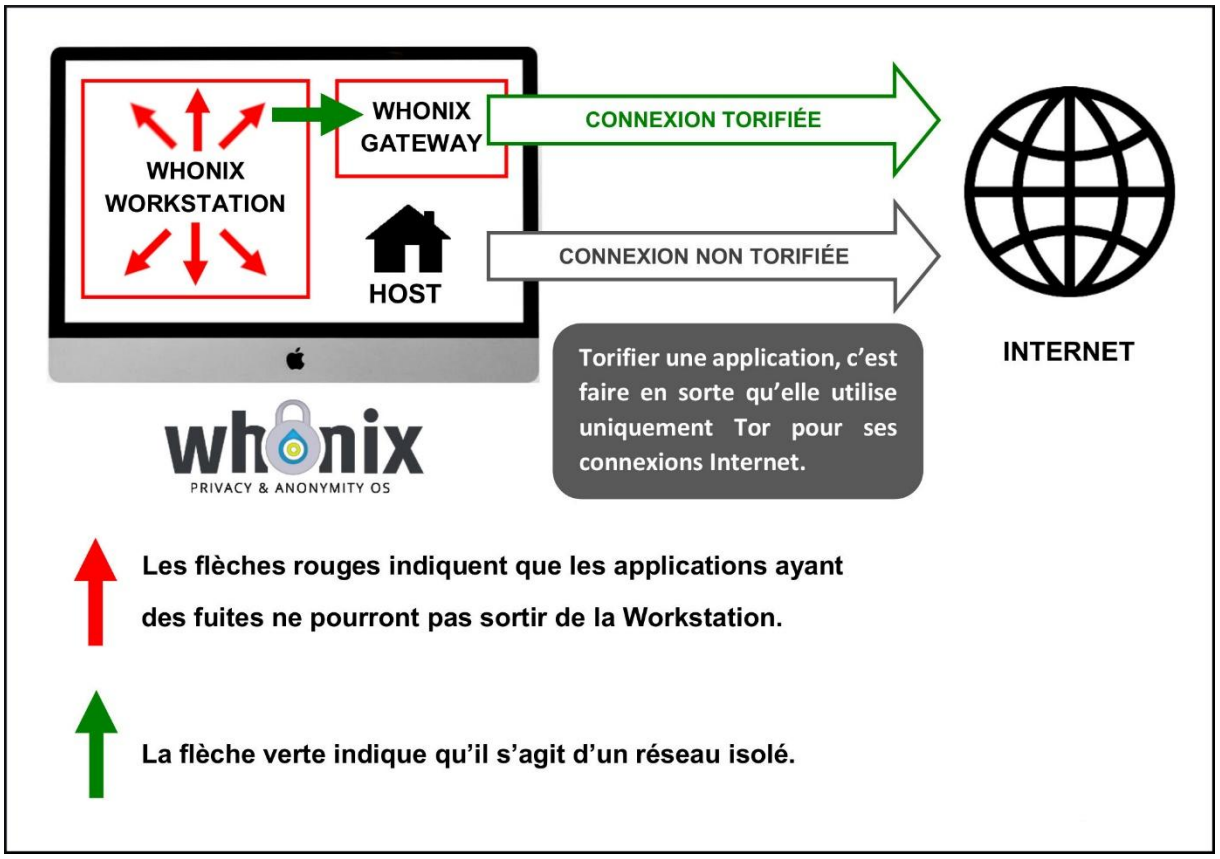
- **Il est impossible de manipuler le trafic qui provient de l'exit node de Tor,**
- **Il n'y aura pas de problème si la destination finale bloque le trafic Tor,**
- **SSH / VPN / JonDoNym ne connaîtra pas votre IP réelle mais uniquement celle de l'exit node de Tor,**
- **Si le deuxième hop est JonDoNym, il fournira un anonymat qui s'ajoute à celui de Tor.**

Inconvénients

- **Il faut être certain du deuxième hop si vous ne voulez pas être désanonymisé. Il est facile au fournisseur VPN de compromettre votre identité. Si vous vous êtes connecté avec votre email réel au fournisseur VPN, le premier hop ne sert plus à rien. Il faut être absolument anonyme vis-à-vis du deuxième hop !**
- **Votre FAI verra que vous utilisez Tor. Cela peut être un problème,**
- **Si la censure de votre pays bloque Tor, vous serez coincé.**

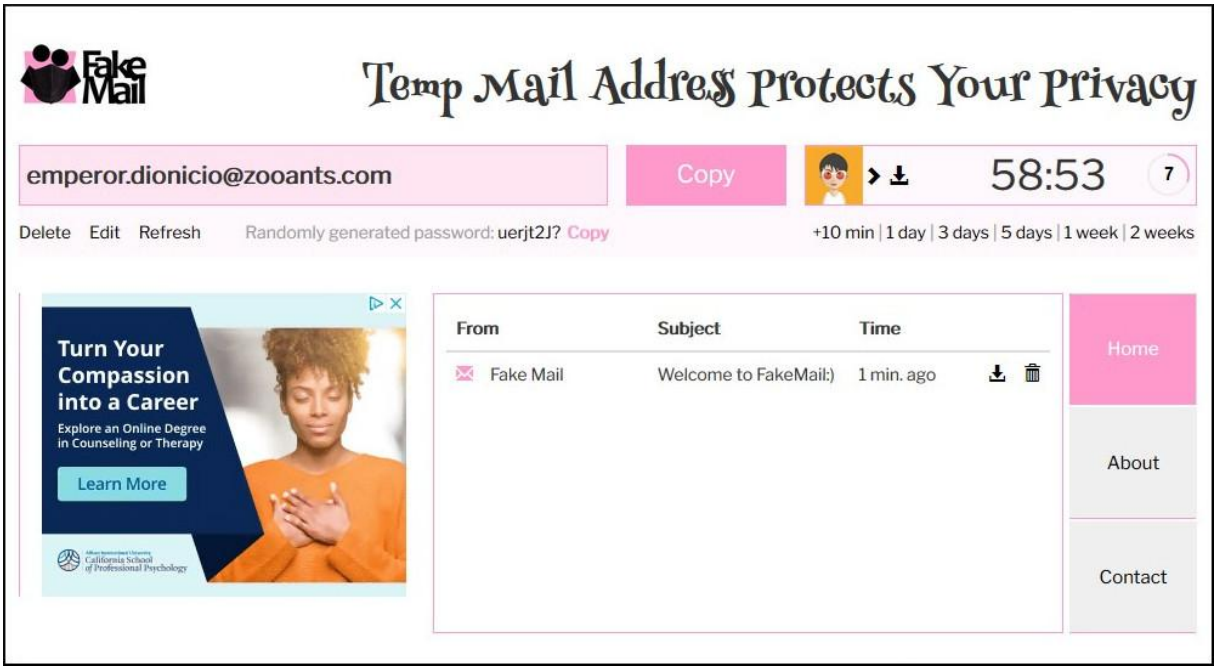
Comment réaliser techniquement ces imbrications ?		
	Premier hop	Dernier hop
(USER) ► VPN ► VPN ► INTERNET	Machine hôte	Machine virtuelle
	Routeur	Ordinateur
(USER) ► VPN ► TOR ► INTERNET (USER) ► SSH ►TOR ► INTERNET (USER) ► JonDoNym ►TOR ► INTERNET	Machine hôte	Machine virtuelle
	Routeur	Ordinateur
	Whonix Gateway	Whonix Workstation

Fonctionnement de Whonix (distribution Linux orientée sécurité et préservant vie privée et anonymat, fonctionnant sur deux machines virtuelles) :



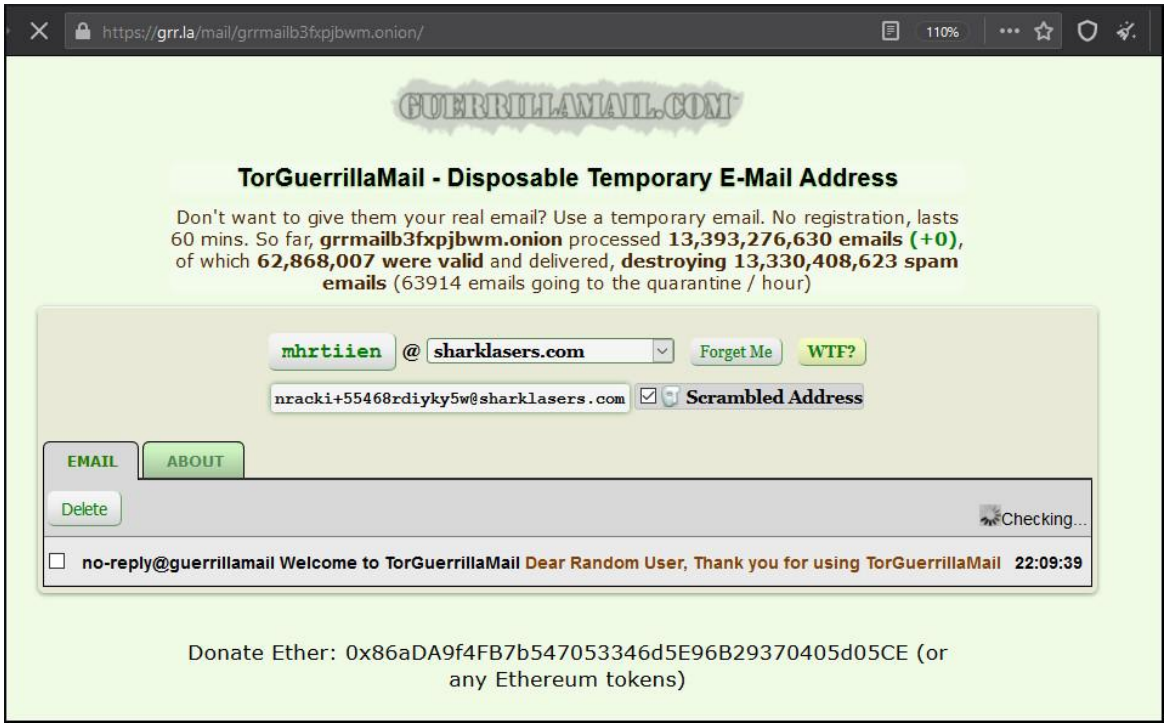
Courriels anonymes et services de messagerie

Il existe de nombreux services de courriels anonymes et temporaires, dans le Clearnet (comme yopmail.com et fakemail.net) et dans le Darknet (comme guerrillamail).



https://www.fakemail.net/

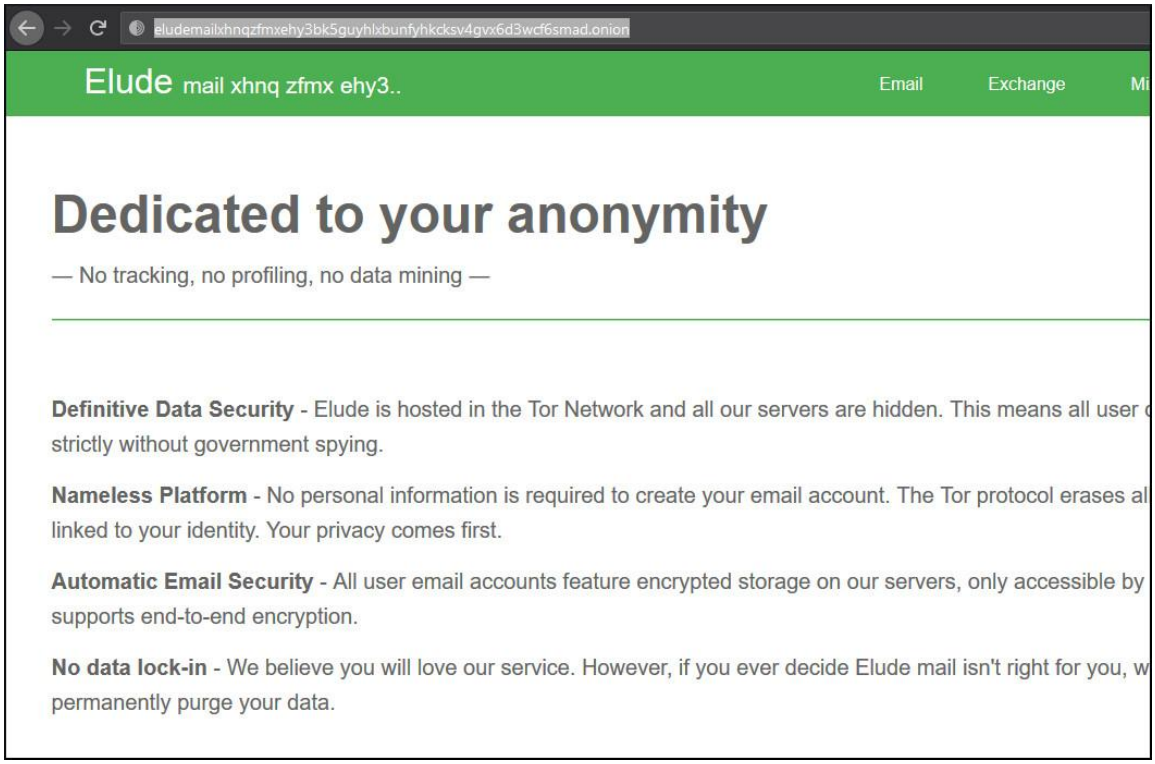
grr.la/mail/grrmailb3fxpjbwm.onion/



Les courriels jetables de la page précédente permettent juste de recevoir des emails et de les lire. Mais il est encore possible de trouver, dans le Darknet de véritables services de messagerie comparables à Gmail, mais beaucoup plus anonymes.

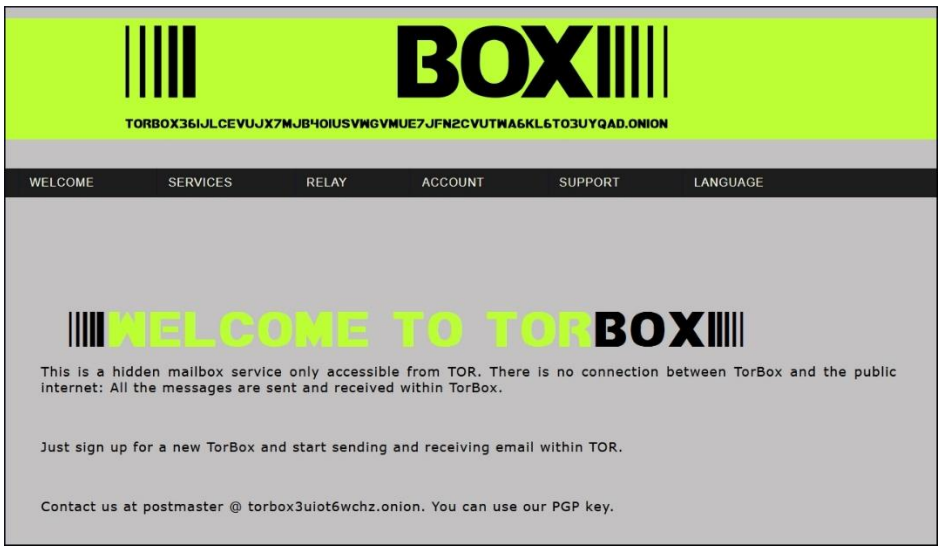
Un exemple : Elude (ancien site, lien obsolète)

(adresse : ~~eludemailxhnqzfmxehy3bk5guyhlxbunfyhkcksv4gvx6d3wcf6smad.onion/~~)

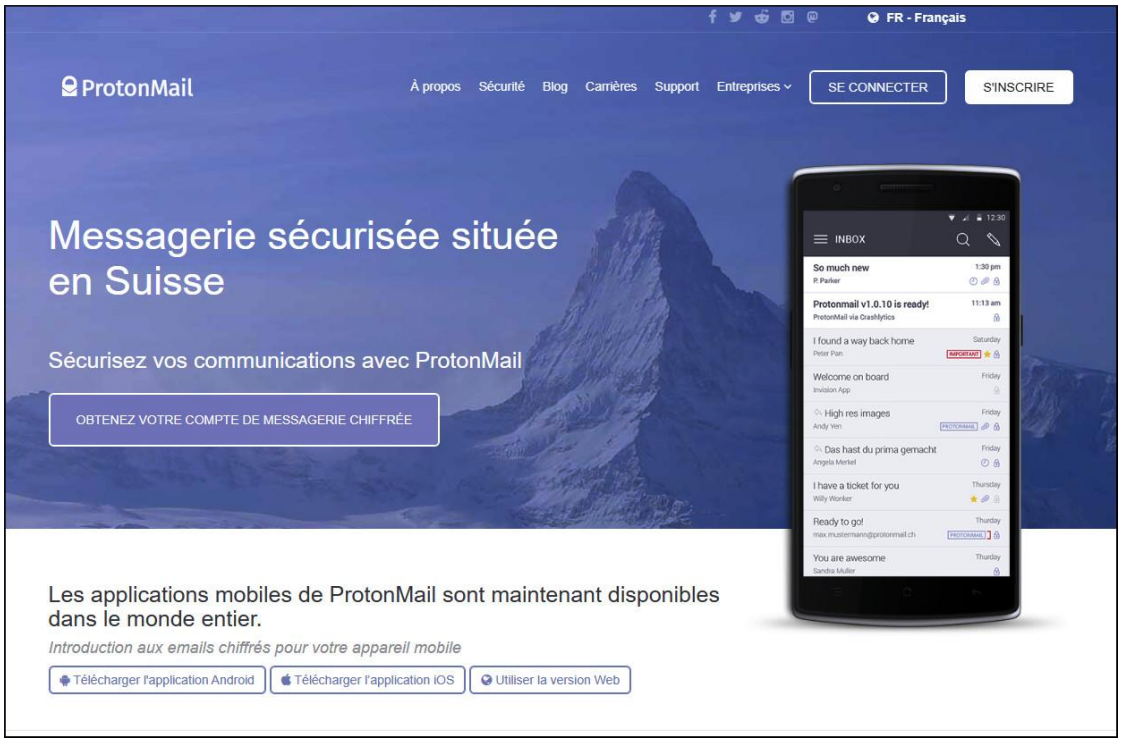


Un autre exemple : TorBox

(adresse : http://torbox36ijlcevujx7mjb4oiusvwgvmue7jfn2cvutwa6kl6to3uyqad.onion/)



Il existe aussi un très bon service de messagerie sécurisé dans le Clearnet, Protonmail. Les serveurs de ProtonMail sont tous situés en Suisse. Ce service est payant si vous voulez bénéficier de toutes ses options :



Les quatre services de messagerie du Clearnet recommandé dans le cadre du respect de la vie privée sont :

\+ ↑
- ➔ **Mailbox** (Allemagne)
- ➔ **ProtonMail** (Suisse)
- ➔ **Mailfence** (Belgique)
- ➔ **OpenMailbox** (France)

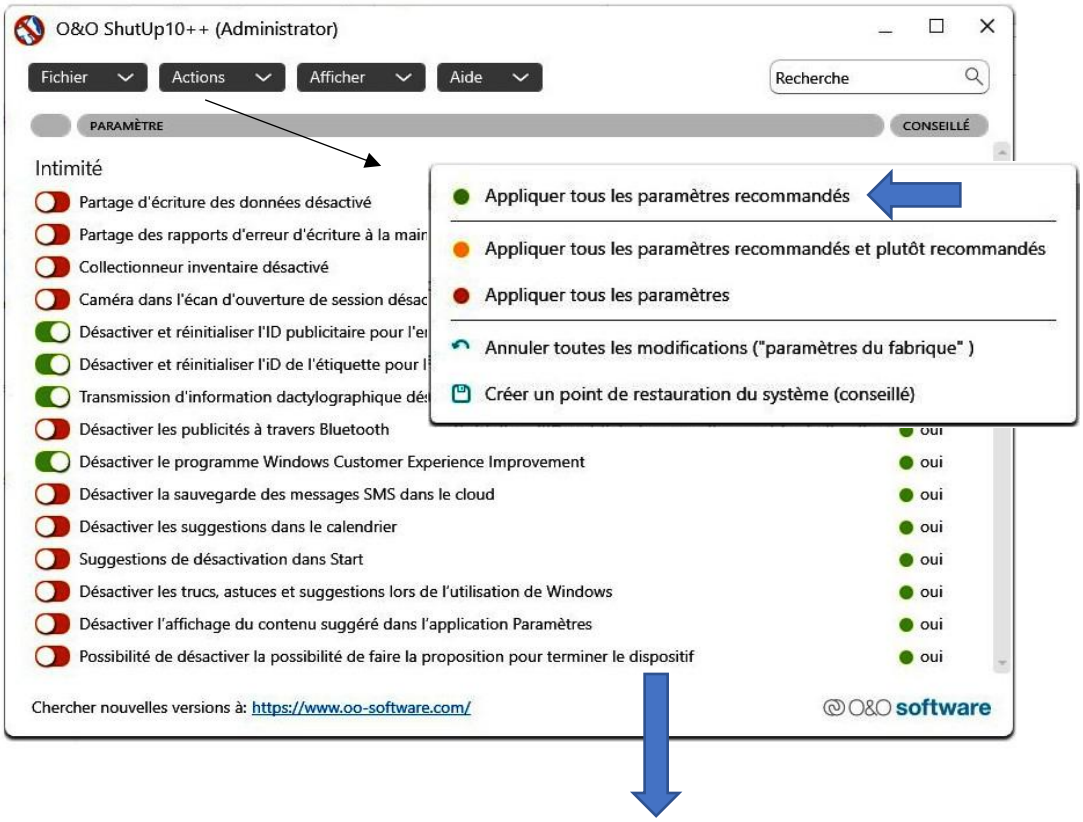
Les services de messagerie ProtonMail et Mailfence proposent le chiffrement de bout en bout (E2EE, end-to-end encryption) qui permet aux seules personnes qui communiquent la lecture des messages. Ni le FAI (ISP) ni même le fournisseur du service de messagerie ne peuvent déchiffrer les messages. Les autorités, impuissantes, accusent les services proposant l'E2EE, notamment la messagerie instantanée *Telegram*, de servir les intérêts des cybercriminels et terroristes.

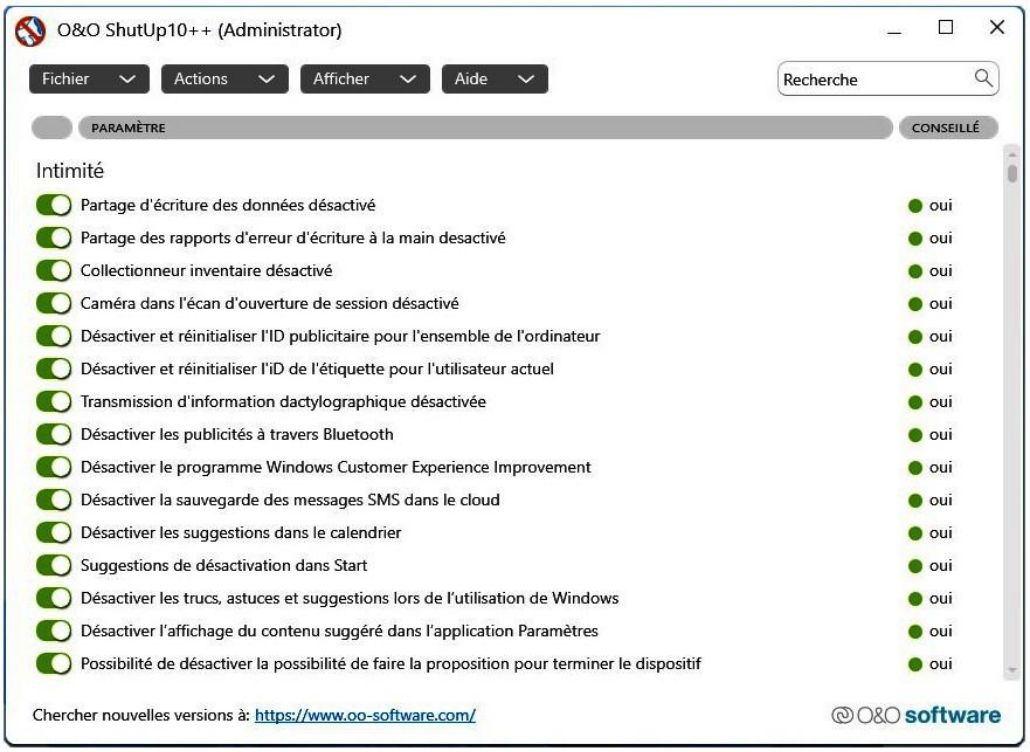
Pour tester le respect de la vie privée par votre messagerie :

https://www.emailprivacytester.com/

Rendre Windows 10 et 11 plus respectueux de la vie privée … si c'est encore possible !

Nous allons nous servir du programme gratuit O&O ShutUp10++ **(oo-software.com) :**



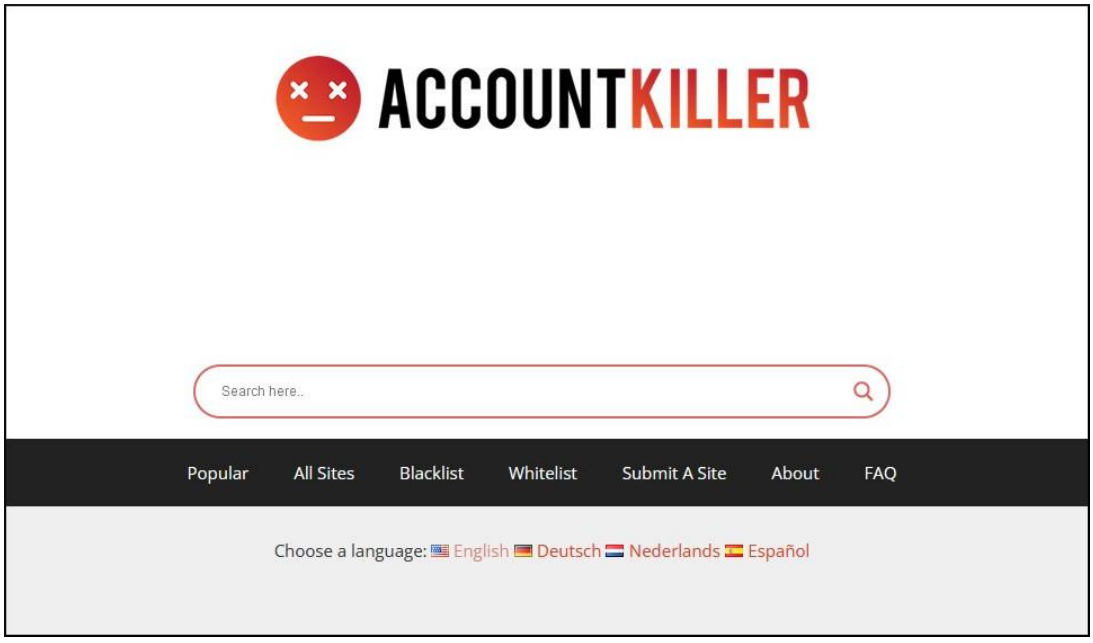


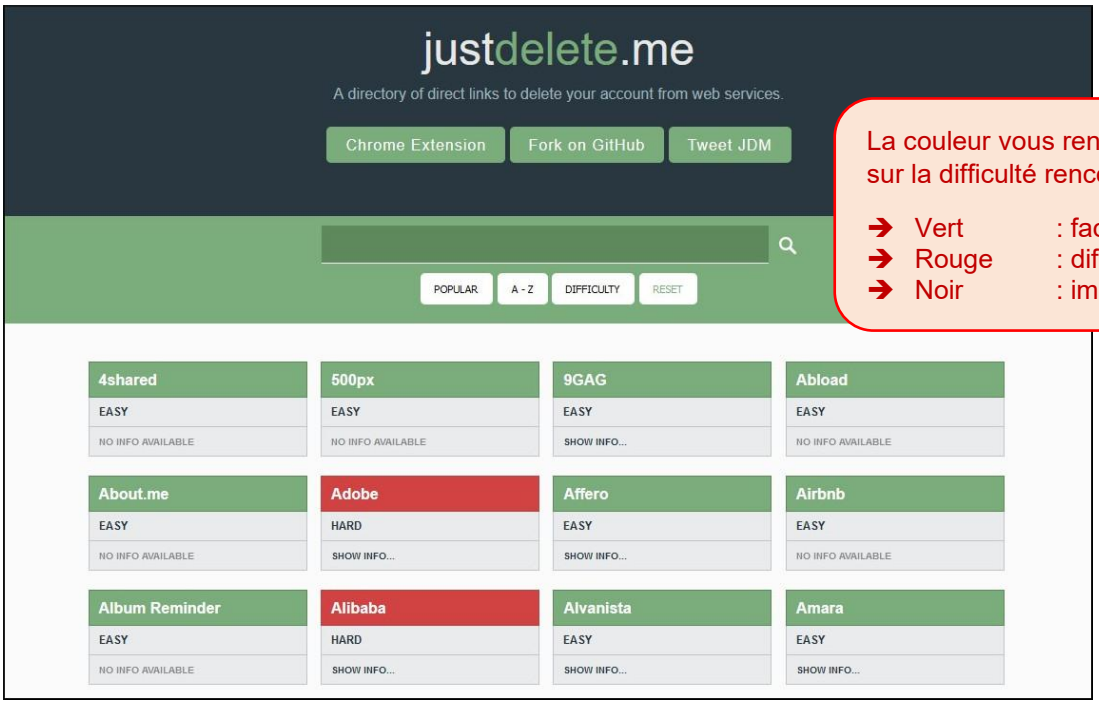
Supprimer un compte en ligne

Il peut parfois être fastidieux voire impossible de supprimer un compte en ligne. Pour vous aider dans cette tâche, deux sites ont vu le jour :

- ➔ https://www.accountkiller.com/en/home
- ➔ https://backgroundchecks.org/justdeleteme/

Je vous conseille vivement de les consulter si vous en éprouvez le besoin.





La couleur vous renseigne sur la difficulté rencontrée :

- ➔ Vert : facile
- ➔ Rouge : difficile
- ➔ Noir : impossible

Personnaliser les réglages de Firefox pour plus de sécurité

Les règlages avancés de Firefox se situent à la page about:config :

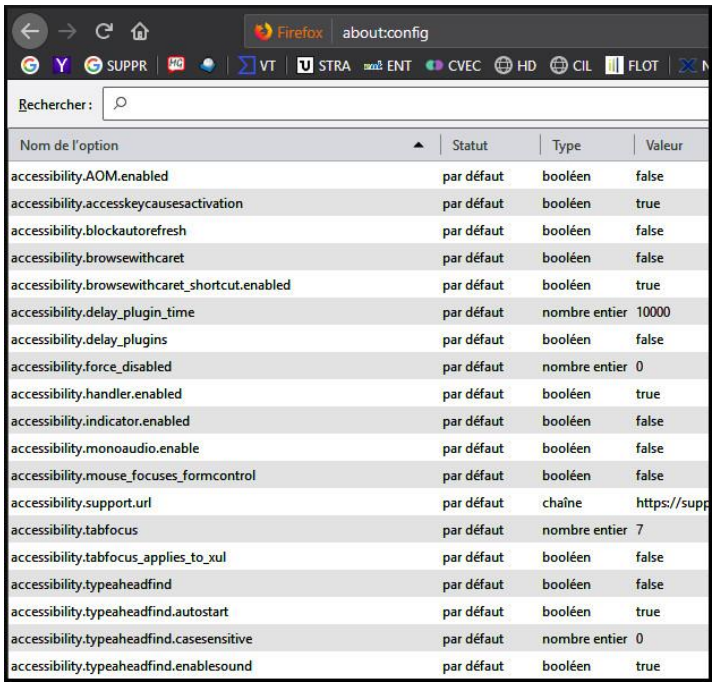
Voyons ce qu'en dit le site de Mozilla :

« L'éditeur de configuration (c'est la page *about:config*) donne la liste des paramètres de Firefox. Ce sont des *préférences* modifiables qui sont lues dans les fichiers prefs.js et user.js du profil de Firefox et dans les paramètres par défaut des applications. La plupart de ces préférences ou paramètres avancés ne sont pas accessibles dans le panneau des Options. (…)

Attention : la modification de ces paramètres avancés pourrait entraîner de sérieux dysfonctionnements de votre Firefox. N'opérez de modification que si vous savez ce que vous faites ou suivez des conseils de source fiable. »

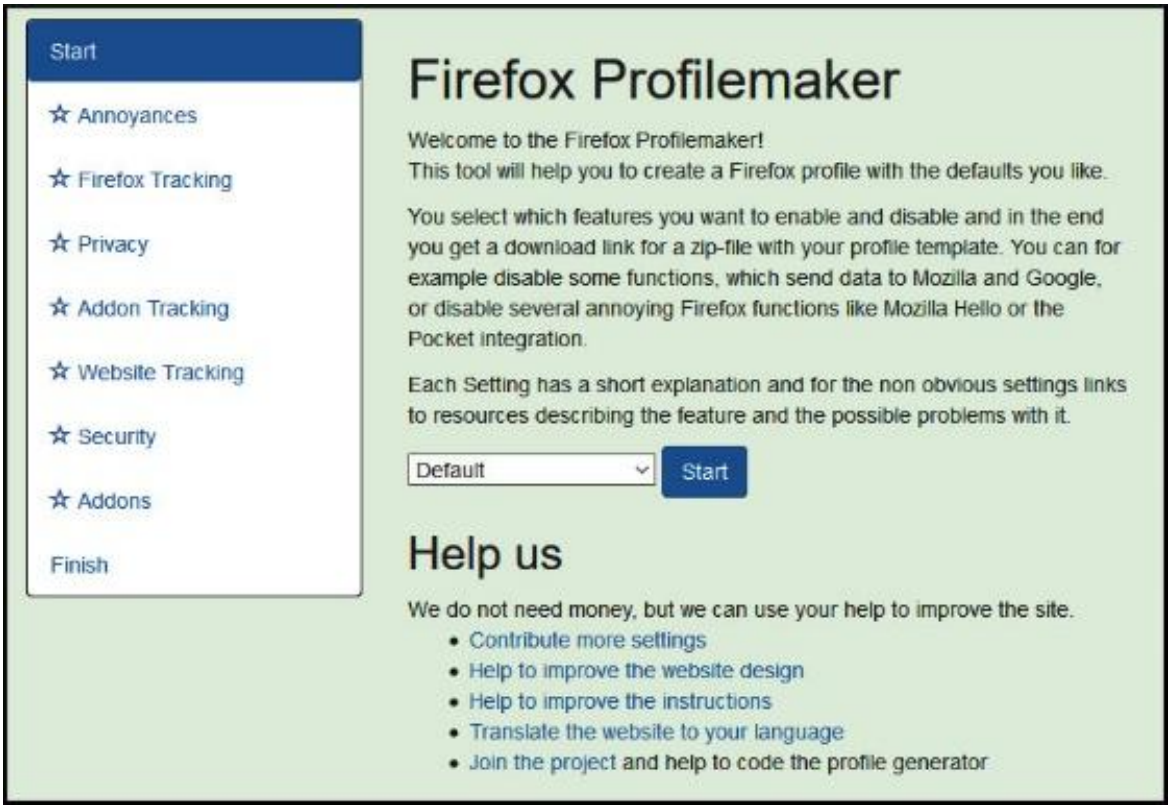
Source : https://support.mozilla.org/fr/kb/editeur-de-configuration-pour-firefox

Un avertissement s'affiche si on essaye d'afficher la page about:config :

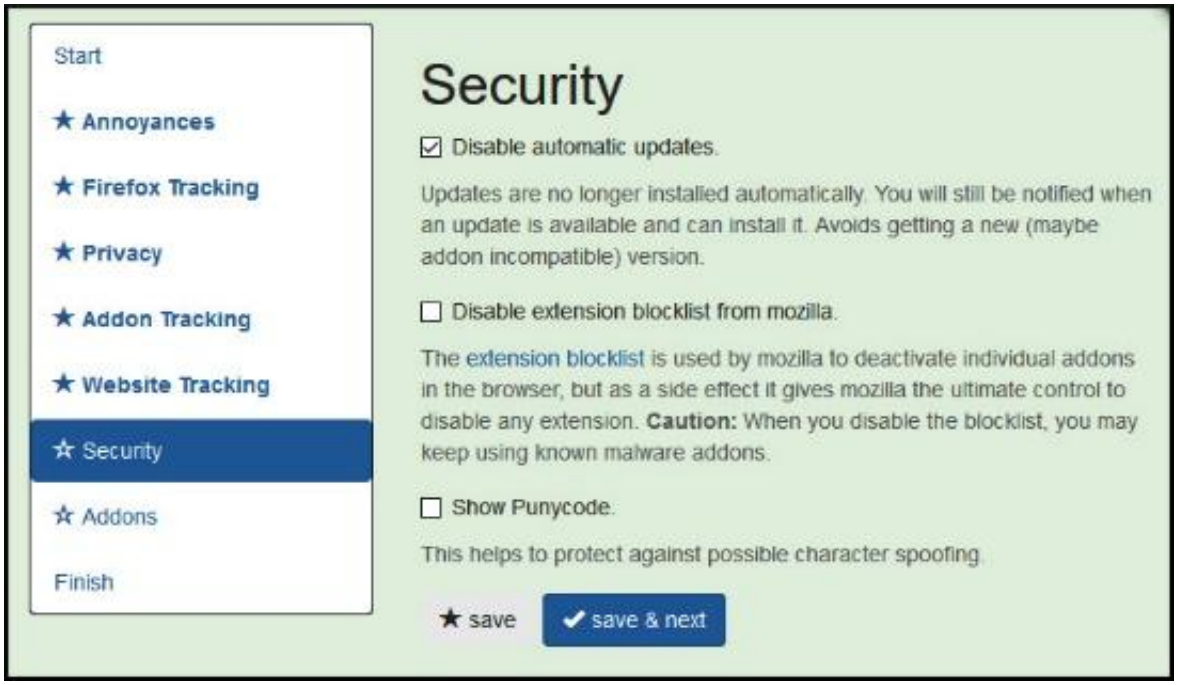


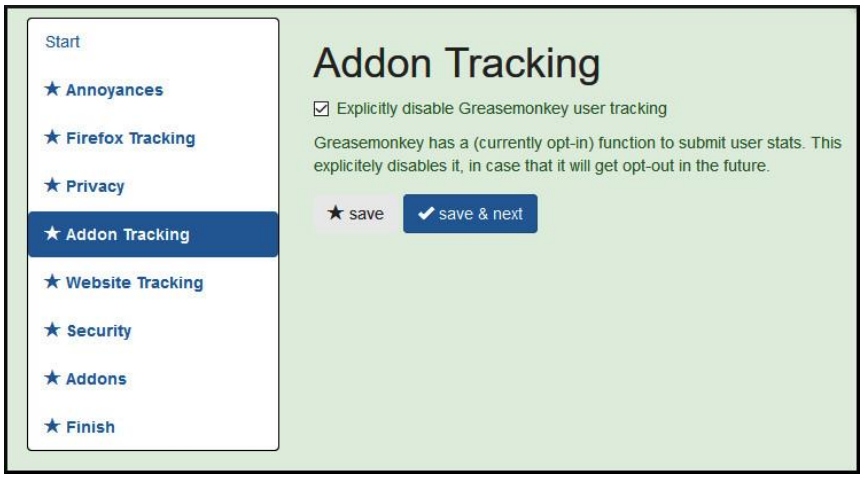
Liste des réglages disponibles.

Un site (https://ffprofile.com) vous permet de générer le fichier prefs.js (ou un fichier profile.zip qui le contient) :

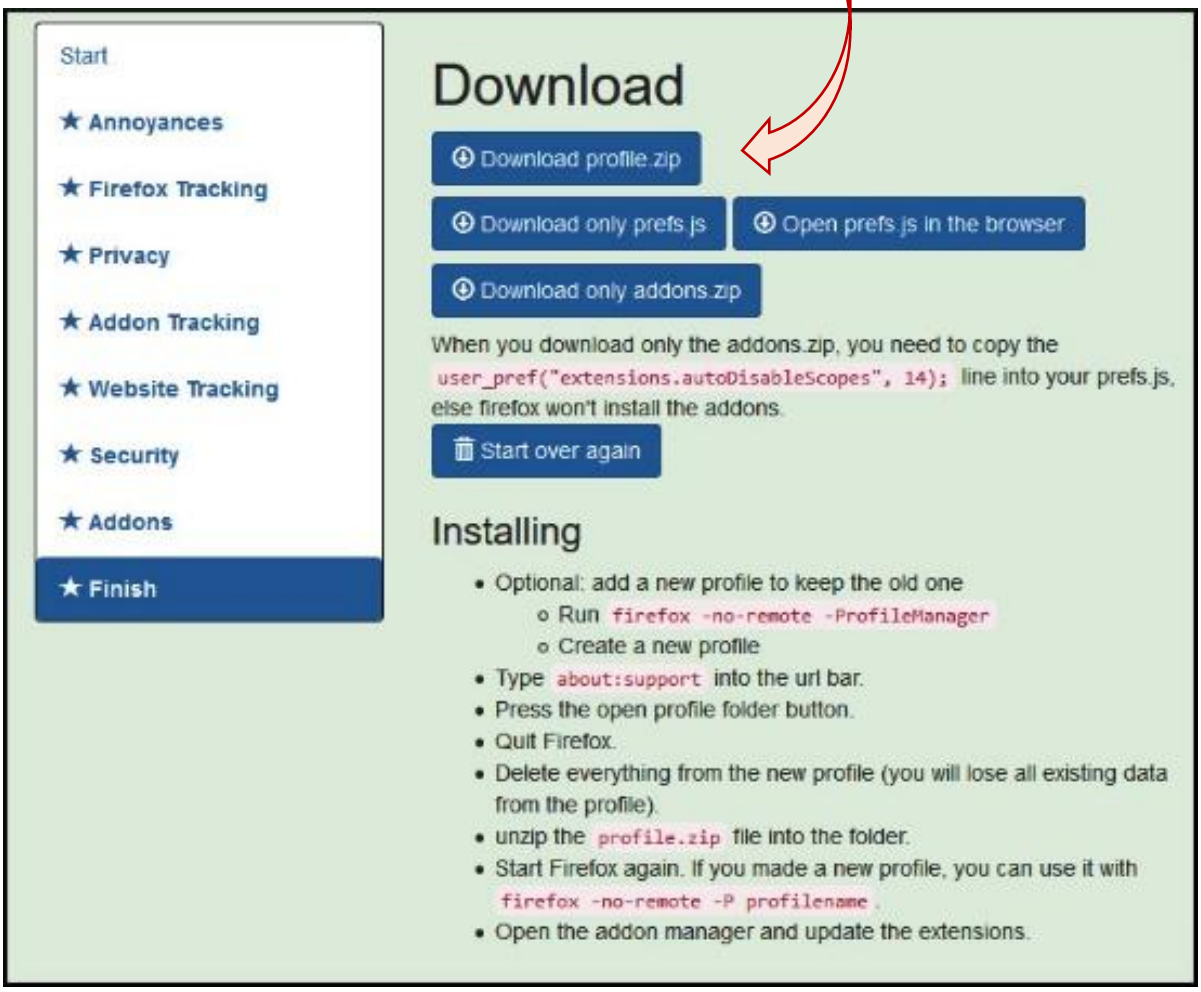


On active ou désactive les réglages, puis on clique sur ***✓ save & next*** **:**



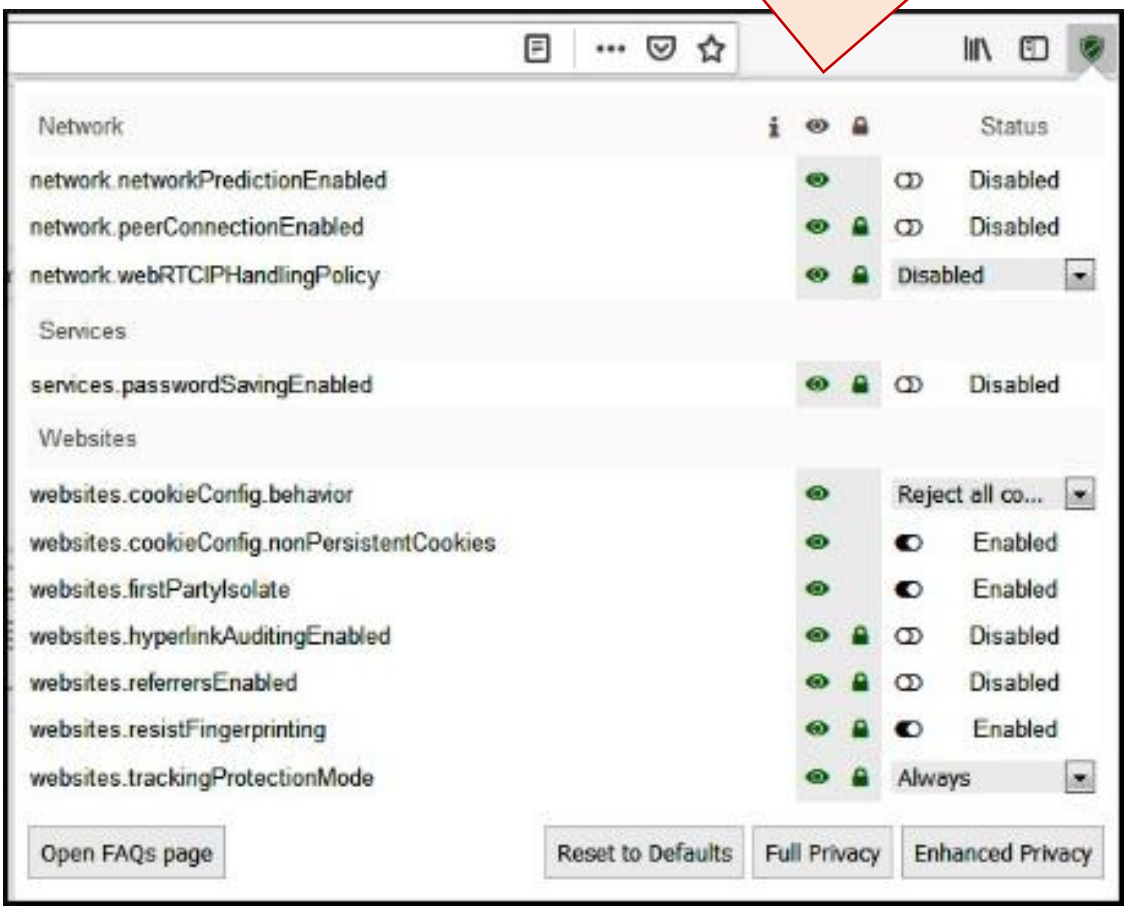


Il suffit maintenant de télécharger le fichier prefs.js ou le fichier profile.zip puis d'installer le nouveau profil.



Il existe encore un dernier outil dont je voudrais vous parler : l'extension pour Firefox Privacy-Settings. Cette extension permet très simplement d'activer ou désactiver certains réglages du fichiers about:config :

L'œil vert signifie que votre confidentialité est protégée tandis que le cadenas vert signifie que votre sécurité est assurée. Parfois seul l'un des deux paramètres est assuré : cela signifie que l'autre est non pertinent pour ce réglage.



Notes :

Des sites intéressants		
	Site	**Alternative**
permet de vérifier si vos adresses de courriel ont été compromises sur Internet.	**haveibeenpwned.com/**	**monitor.firefox.com/**
permet de recevoir des alertes lorsque des informations qui vous intéressent sont publiées sur Internet.	**google.com/alerts**	**talkwalker.com/fr** (payant)

.....

.....

.....

.....

.....

.....

.....

.....

.....

Notes :

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

INTRODUCTION À LA CYBERSÉCURITÉ