**L’écosystème Tor**

<https://www.team-azerty.com/html/articles/article-54-le-reseau-tor.html>

<https://framablog.org/2016/05/06/anonymat-en-ligne-nos-oignons/>

<https://korben.info/tor-messenger-discutez-anonymement-en-passant-par-tor.html>

<http://www.lemondenumerique.com/article-32422-les-10-meilleures-applications-de-securite-et-de-protection-de-la-vie-privee-en-2018.html>

<https://blog.torproject.org/tor-messenger-beta-chat-over-tor-easily>

<http://www.lemonde.fr/pixels/article/2016/01/19/ricochet-une-messagerie-securisee-qui-cache-aussi-les-metadonnees_4849970_4408996.html>

<https://www.eff.org/https-everywhere>

<https://tails.boum.org/about/index.fr.html>

Il existe une liste assez importante de projets connexes à Tor. Ces projets ont pour vocation d’améliorer encore un peu plus l’anonymat offert par Tor. Nous allons voir quelques-uns de ces projets en détails.

* Comment utiliser le réseau Tor ?
  + Le Tor Browser (méthode simple) :

Le logiciel Tor vous protège en faisant rebondir vos communications autour d'un réseau de relais distribué par des volontaires du monde entier : il empêche toute personne d'apprendre quels sites vous visitez en espionnant votre connexion, il empêche les sites que vous visitez d'apprendre votre emplacement physique et il vous permet d'accéder aux sites bloqués.

Tor Browser vous permet d'utiliser Tor sur Microsoft Windows, Apple MacOS ou GNU / Linux sans avoir besoin d'installer de logiciel. Il est livré avec un navigateur Web préconfiguré pour protéger votre anonymat, et est autonome (portable).

Il s'agit d'un bundle comprenant une version modifiée de Firefox avec un programme TOR embarqué. L’installation est très simple :  
- Téléchargez l'installeur [sur le site officiel](https://www.torproject.org/download/download-easy.html.en)   
- Exécutez le.   
- Demandez à TOR de se connecter au réseau lors du premier lancement

* + Le Proxy personnel (méthode plus complexe) :

Tout le monde ne dispose pas du matériel ou des connaissances pour monter son propre proxy TOR. Si la partie matérielle peut être facilement éludée à l'aide d'une machine virtuelle (VirtualBox par exemple) la mise en place nécessite quelques lignes de commandes et l'installation d'une distribution linux (par exemple Debian).

Il faut récupérer l'image ISO de Debian sur le site officiel puis créer une nouvelle machine virtuelle sur VirtualBox en la démarrant sur cet ISO. Une fois celle-ci installée il faut suivre le pas à pas décrit sur le site officiel de TOR. Ceci fait, il ne vous restera qu'à indiquer dans les paramètres de votre navigateur un serveur mandataire / Proxy en saisissant l'IP de votre machine virtuelle.

* Communiquer sur Tor
  + Tor Messenger :

Tor Messenger est un programme de discussion multiplateforme qui vise à être sécurisé par défaut. Il est basé sur Instantbird de Mozilla. Cette plateforme est instantanée, décentralisée et 100% sécurisée, alors que l’ensemble du trafic transite via Tor pour l’anonymat des utilisateurs.

Il prend en charge une grande variété de réseaux de transport, y compris Google Talk, Facebook Chat, Twitter, Yahoo et autres. Il possède une interface utilisateur graphique facile à utiliser disponible dans plusieurs langues.

Cela permet également l’échange de messages Off-The-Record (OTR) - un moyen sûr et crypté pour avoir des conversations privées.

Off-the-Record Messaging, appelé communément OTR, est un protocole cryptographique. Il utilise une combinaison d'un algorithme de clés symétriques AES, du protocole d'échange de clés Diffie-Hellman et de la fonction de hachage SHA-1. OTR permet d'avoir des conversations privées sur de multiples protocoles de messagerie instantanée. Instantbird à été choisi notamment pour sa communauté de développeurs de logiciels actifs.

* + Ricochet :

Ricochet utilise le réseau Tor pour atteindre vos contacts sans utiliser les serveurs de messagerie. Le programme permettant aux utilisateurs de Ricochet de se retrouver et de s’identifier est distribué sur différents serveurs, qui changent de façon aléatoire. Lors de l’inscription, chaque utilisateur se voit attribuer un identifiant unique généré automatiquement, ressemblant à cela : rs7ce36jsj24ogfw, qui servira à la fois d’adresse et d’identifiant de connexion. Puis chaque connexion est authentifiée grâce à un mot de passe temporaire. Il crée un service caché, qui est utilisé pour rencontrer vos contacts sans révéler votre position ou votre adresse IP. Vous pouvez voir quand vos contacts sont en ligne, et leur envoyer des messages. Votre liste de contacts n'est connue que de votre ordinateur : elle n'est jamais exposée aux serveurs ni à la surveillance du trafic réseau. Tout est crypté de bout en bout, donc seul le destinataire peut le décrypter et l'anonymiser, donc personne ne sait où il va et d'où il vient.

Le point fort de Ricochet est de cacher les métadonnées. Ce sont les informations techniques dont les routeurs ont besoin pour acheminer les messages : expéditeur, destinataire, date d’envoi, parfois taille du document.

* + Pond :

Pond est une application de messagerie asynchrone, chiffrée et sécurisée écrite par Adam Langley dans le langage de programmation Go. L'interface graphique de Pond est minimaliste, mais sous la surface, elle fait du bon travail en protégeant la communication de bout en bout. Pond possède des propriétés comme la sécurité par défaut fournie par l'usage obligatoire de Tor et des messages de longueur fixe. Il existe également plusieurs façons d'échanger le premier ensemble de clés entre les parties de communication. Le seul problème réside dans la complexité d'installation.

* Forcer l’utilisation de HTTPS

HTTPS Everywhere est une extension Firefox, Chrome et Opera qui chiffre vos communications avec de nombreux sites Web majeurs, rendant votre navigation plus sécurisée. HTTPS Everywhere est produit par le Tor Project et Electronic Frontier Foundation. L'EFF (Electronic Frontier Fundation) est la plus grande association de défense des droits de l'internaute et de la neutralité des réseaux. Basée aux USA, elle milite sensiblement pour les mêmes causes que La Quadrature du Net en France, mais dispose d'une envergure bien plus importante.

De nombreux sites sur le Web offrent un support limité pour le chiffrement sur HTTPS, mais ils sont difficiles à utiliser. Par exemple, ils peuvent utiliser par défaut le protocole HTTP non chiffré, ou remplir des pages chiffrées avec des liens renvoyant vers le site non chiffré. L'extension HTTPS Everywhere résout ces problèmes en utilisant une technologie intelligente pour réécrire les requêtes sur ces sites vers HTTPS. L’extension ne fonctionne que pour les sites qui prennent en charge HTTPS.

**TAILS**

Tails est un système live (système d'exploitation complet destiné à être utilisé depuis une clef USB ou un DVD indépendamment du système installé sur l'ordinateur) dont le but est de préserver votre vie privée et votre anonymat. Il vous permet d'utiliser Internet de manière anonyme et de contourner la censure quasiment partout où vous allez et sur n'importe quel ordinateur. Tails ne laisse aucune trace de ce que vous avez fait, sauf si vous le demandez explicitement.

Tails est livré avec de nombreuses applications, configurées avec une attention particulière accordée à la sécurité : navigateur web, client de messagerie instantanée, client email, suite bureautique, éditeur d'image et de son, etc.

Tails est spécialement configuré pour ne pas utiliser le disque dur de l'ordinateur. Le seul espace de stockage utilisé par Tails est la mémoire RAM, qui est effacée automatiquement à l'extinction de l'ordinateur.

TOR ne propose qu'un anonymat relatif, anonymat qui dépend principalement de votre propre comportement sur internet.