

# Utiliser le navigateur Tor

Damien Belvèze

20210207

## Décharge

### cadre de l'intervention

Les contenus qui sont présentés lors de cet atelier ont été relus par le responsable de la sécurité informatique de l'Université mais ne représentent ni son point de vue, ni le point de vue global de l'Université pour qui l'usage de Tor sur le réseau Rennes 1 reste toléré mais comporte des risques pour la sécurité informatique de l'établissement. L'usage d'OnionShare notamment contrevient à la politique de sécurité de l'Université.

C'est la raison pour laquelle, nous vous demandons dans le cadre de cette activité de ne pas utiliser le réseau de Rennes 1 mais celui de votre fournisseur d'accès à internet. Si vous êtes chez vous, vous n'avez rien à faire de particulier. Si vous êtes à l'Université, merci d'utiliser votre smartphone comme hotspot pour utiliser Internet et de ne pas utiliser le réseau local.

La bibliothèque de l'Université de Rennes 1 propose cet atelier, en même temps qu'un autre sur la gestion des mots de passe, dans la suite des ateliers du FDLN qui ont eu lieu entre 2018 et 2020. Cette courte présentation de Tor a pour précédents à Rennes 1 les formations à cet outil d'étudiants qui se destinent au métier de journaliste, dans le cadre de la protection des sources. En vertu de la déclaration de l'IFLA (réunion internationale des organisations professionnelles de bibliothécaires) d'août 2015, les bibliothécaires doivent contribuer à protéger la vie privée de leurs utilisateurs en leur proposant d'une part un environnement autant que possible indemne de la surveillance de masse et d'autre part des formations aux outils qui leur permettront de protéger leur vie privée. C'est dans ce dernier cadre que nous intervenons aujourd'hui.

### Utiliser son smartphone comme relais internet.

Pour utiliser les données mobiles de son téléphone avec un ordinateur, voir le mode d'emploi : - Android - Iphone ou Ipad

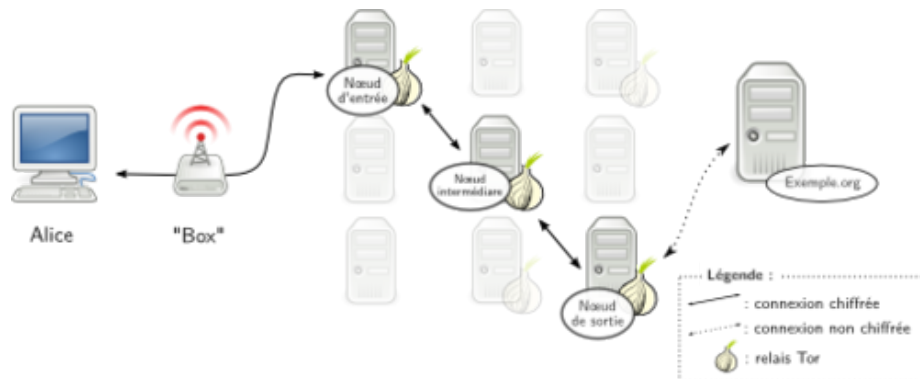
# Le circuit Tor

## histoire du réseau

De 1995 à 2003, Tor était un projet à la fois universitaire (MIT) et militaire (laboratoire de l'US Navy). L'Electronic Frontier Foundation (EFF), organisation à but non lucratif pour la protection des libertés numériques, a financé le projet à partir de 2004, deux ans après que le réseau soit devenu accessible à tous les internautes. Toutefois à l'époque la connexion aux relais Tor demandait des compétences un peu plus poussées. Pour faciliter cet accès au réseau et en démocratiser l'usage, le navigateur Tor (Tor Browser) a été conçu en 2008 ce qui a rendu le réseau populaire notamment lors des printemps arabes. En 2013, les révélations de Snowden ont encore accru le nombre d'utilisateurs réguliers. Pour en savoir plus, voir l'historique du projet sur le site du projet Tor.

## principe d'un circuit tor (ou "roulage en oignon")

Tor est donc le réseau, et nous allons vous présenter l'outil qui permet de le parcourir, le navigateur Tor. Ce navigateur (à télécharger sur le site de Tor Project) permet de consulter des sites web en préservant le plus possible son anonymat. Le principe général est que le serveur auquel se connecte la machine client qui utilise le navigateur Tor ne retient pas l'[[IP]] de cette machine mais celui du dernier routeur par lequel passe la communication, autrement appelé noeud de sortie.



Source: [[@anonymeGuideautodefensenumerique2017]]

Le circuit Tor est constitué de trois relais ou "noeuds" qui constituent trois couches [[cryptographie|cryptographiques]] (d'où l'image de l'oignon). Ces différents noeuds ignorent l'IP de la machine qui le suit ou le précède. Seul le serveur peut conserver l'IP du noeud de sortie. Mais il lui est impossible de remonter à l'IP de la machine client.

Tor complète le https pour rendre votre navigation la plus confidentielle possible (voir à ce sujet l'animation sur le site de l'EFF à ce sujet qui permet de visualiser ce que fait chaque protocole https et Tor)

## hébergement des noeuds de sortie

Du fait qu'en cas de trafic illicite, celui-ci peut être intercepté au niveau du noeud de sortie, ce sont plus souvent des associations loi 1901 qui en France maintiennent ces noeuds particuliers (par exemple l'association Nos Oignons). On peut en revanche, héberger des noeuds intermédiaires avec une simple machine (le débit minimal requis est de 16 Mbits/seconde, voir les autres requis sur le site du Tor Project)

## changer le circuit Tor

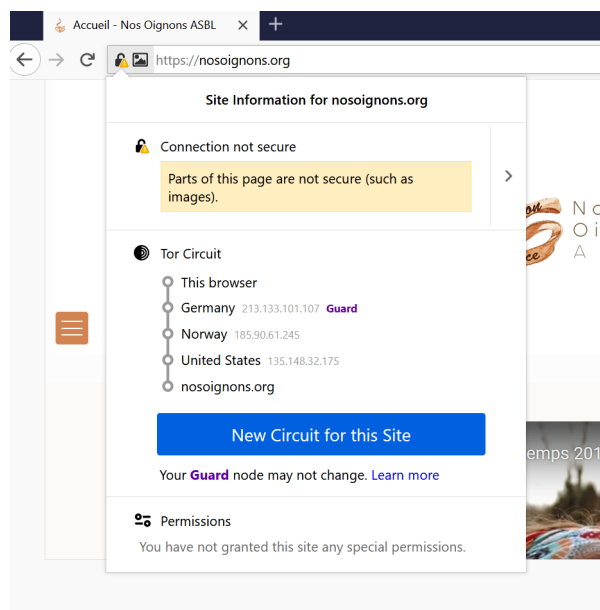


Figure 1: changement de circuit

Cliquer sur le cadenas > ‘new circuit for this site’ tous les circuits ne sont pas également rapides (certains relais ont plus de bande passante que d’autres). Il peut parfois être avantageux de changer le circuit pour cette raison. Le noeud d’entrée (guard) en revanche ne change que tous les deux ou trois mois et de manière automatisée afin de réduire le risque de certaines attaques

## Tor réduit la signature électronique de votre ordinateur.

Le [[fingerprinting]] consiste à repérer la singularité d’une machine connectée sur le réseau à partir de ses différents paramètres, notamment la configuration du navigateur, des caractéristiques du système d’exploitation, les polices disponibles dans certains logiciels. . . Pour se faire une idée de la manière dont votre machine

est repérable sur le web, vous pouvez consulter avec profit le site Am I Unique qui a été réalisé par Pierre Laperdrix, un ancien étudiant de l'IRISA (Rennes).

Tor depuis la version 10 permet de redimensionner la fenêtre de navigation à l'écran sans que cette information ne puisse être utilisée pour contribuer à identifier la machine. De même Tor complète renforce l'[[obfuscation]] de ses utilisateurs en chargeant des polices additionnelles

## Les services cachés

Tor on l'a vu permet d'assurer dans une large mesure l'anonymat de l'internaute. Le réseau permet également de se connecter à des **services cachés** (hidden services). Il s'agit de serveurs dont l'emplacement géographique est caché. Ces sites ne peuvent être atteints qu'avec le navigateur Tor. Les services cachés sont accessibles au moyen d'adresses en .onion

### des services peu utilisés par les internautes qui choisissent Tor

Les services cachés sur Tor ne génèrent d'après une étude récente que **6,7%** des usages du navigateur Tor[[@JardinepotentialharmsTor2020]]. Cela signifie que la plupart des utilisateurs de Tor utilisent le réseau pour accéder à des sites qui le sont depuis d'autres navigateurs mais en tirant profit de l'anonymat que leur confère le réseau en oignons et en sachant que les extensions pour navigateur du CleanNet sont contournées par la majorité des sites (cf. ce billet sur Do Not Track)

Bien sûr parmi ces sites en onion existent des sites non seulement illégaux mais criminels (pédopornographie, vente de drogue, virus informatiques, contenus haineux), mais plusieurs institutions de presse et de savoir ont aussi développé des sites cachés pour être lus dans les pays où leurs sites sont censurés.

### Liste de sites utiles pour la presse, la communication et la sécurisation des données.

Voici une liste de sites en .onion (Mise à jour : Mathieu Goessens)

Activité : Ouvrir le navigateur Tor, aller sur <http://liqr2cbsjzxmpw6savgh274tuzl34x6cd56h7m7ceatnrokveffm66ad.onion/> qui permet de supprimer les métadonnées rattachées à un document (une photo par exemple)

Télécharger cette photo supprimer les métadonnées du fichier. Testez avec <http://exif.regex.info/exif.cgi> que ni la date ni les coordonnées géographiques ne sont plus visibles.

## Le partage de fichiers avec OnionShare

Logiciel mis au point par Micah Lee et une communauté de développeurs de Tor Project pour permettre de partager et de recevoir facilement des documents sur le réseau Tor. Onionshare est facile à utiliser: il suffit de lancer le logiciel qui se connecte immédiatement au réseau en onion, de glisser déposer les fichiers qu'on veut partager, de copier l'adresse générée par le logiciel (adresse en .onion) et de l'envoyer de manière sécurisée au destinataire (remise en main propre ou mail chiffré). Ce dernier n'aura qu'à utiliser cette adresse dans son navigateur Tor pour accéder au document partagé. Il est également possible d'utiliser Onionshare avec une adresse pérenne afin de publier un site sur le réseau Tor (cf. billet de Micah Lee sur le blog de Tor Project).

Activité :

- charger OnionShare sur sa machine
- charger un document dans OnionShare (photo, poème, bout de code)
- obtenir le lien vers le document
- l'envoyer à un autre participant via le chat de Jitsi (préciser le @destinataire dans la conversation)
- Sur OnionShare, cliquer sur "recevoir des fichiers", envoyer le lien créé à un seul destinataire (un autre) en le nommant comme la première fois. Charge à ce participant de vous envoyer un document du même type que tout à l'heure.

## Les limites de Tor

### Le FAI sait qu'on utilise Tor

Le Fournisseur d'Accès à Internet ([[FAI]]) sait qu'on utilise Tor (il peut avoir l'IP du noeud de sortie, la liste des IP de ces noeuds est disponible sur le net)

Plus il y aura de personnes à utiliser Tor pour des raisons diverses (souvent bénines) et moins le fait d'utiliser Tor aura la valeur de vouloir cacher quelque chose de fondamentalement compromettant.

### Pas de confidentialité entre le noeud de sortie et le serveur visité

Les noeuds de sortie gérés par des personnes malveillantes (selon le principe de l'attaque par l'[[homme du milieu]]) peuvent leur permettre d'écouter des conversations : si les IP des expéditeurs ne sont pas décelés, le contenu peut parfois révéler d'où elles proviennent (à moins que ces communications ne soient chiffrées)

N'importe qui peut gérer un relais Tor, ce qui fait que beaucoup de relais Tor sont compromis.

### **Attaque par flux temporel**

Les paquets d'information sont envoyés selon un certain rythme d'une machine client et sortent du noeud de sortie avec le même rythme. Le poids du signal envoyé au premier relais et celui qui sort du relais de sortie peut être mesuré (ainsi que le rythme de l'envoi). Si les quantités sont les mêmes, il est possible d'affirmer que l'ordinateur A a envoyé une requête au serveur B.