h e g

Haute école de gestion
Genève

Étude et conception d'un service assurant l'anonymat

Travail de Bachelor réalisé en vue de l'obtention du Bachelor HES

par :

Artrit AJDINI

Conseiller au travail de Bachelor :

Bryce CIARAN

Genève, le 30 septembre 2019

Haute École de Gestion de Genève (HEG-GE)

Filière informatique de gestion

Hes·so GENÈVE
Haute Ecole Spécialisée
de Suisse occidentale

Déclaration

Ce travail de Bachelor est réalisé dans le cadre de l'examen final de la Haute école de gestion de Genève, en vue de l'obtention du titre de Bachelor of Science HES-SO en informatique de gestion.

L'étudiant a envoyé ce document par email à l'adresse remise par son conseiller au travail de Bachelor pour analyse par le logiciel de détection de plagiat URKUND, selon la procédure détaillée à l'URL suivante : http://www.urkund.fr/student_gorsahar.asp.

L'étudiant accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans le travail de Bachelor, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteur, ni celle du conseiller au travail de Bachelor, du juré et de la HEG.

« J'atteste avoir réalisé seul le présent travail, sans avoir utilisé des sources autres que celles citées dans la bibliographie. »

Fait à Genève, le 30 septembre 2019

Artrit Ajdini

Remerciements

Je tiens d'abord à sincèrement remercier monsieur Bryce Ciaran, qui a accepté de suivre mon travail de Bachelor mais qui s'est surtout montré très attentif et très à l'écoute tout au long de la réalisation, je le remercie également pour le temps qu'il m'a consacré, notamment quand je l'ai sollicité pendant son weekend.

Je remercie également ma conjointe et mon fils de m'avoir apporté du soutien malgré mes indisponibilités durant ce travail.

Résumé

Le droit à l'anonymat sur internet est devenu un enjeu majeur pour notre société, avec presque 4,5 milliards d'internautes[1], ce qui représente pratiquement 60% de la population mondiale, internet se retrouve aujourd'hui au cœur de notre système et son influence ne cesse de grandir.

La nature des infrastructures et technologies internet ne permet pas d'agir en tant qu'anonyme en les utilisant, en effet les moindres faits et gestes des utilisateurs sont aujourd'hui collectés, traités et analysés par les différentes entités constituant la toile, notamment les acteurs principaux du type GAFAM et leurs services très repandus, mais ce ne sont pas les seuls : les gouvernements, les services de renseignements, les services de police sont aussi de la partie, les scandales à répétition que vivent actuellement les internautes et leurs données personnelles sont là pour nous le prouver.

Il est impossible d'avoir le contrôle total des données que nous laissons chaque jour sur internet, données sensibles incluses, ce document vient démontrer comment, pourquoi et avec quelles outils les entités du web collectent les informations des internautes, il présente également des outils d'anonymisation et présente notamment un service web collaboratif utilisant certains de ses outils afin de rendre le traçage et l'identification des utilisateurs pratiquement impossibles de la part de quiconque.

[1] https://www.internetlivestats.com/

Table des matières

Liste des tableaux

Liste des figures

1. Introduction

Le monde interconnecté dans lequel nous vivons actuellement à ouvert de nouvelles perspectives en termes de communication et de partage d'informations. Communiquer à travers tous les continents en quelques clics et à une vitesse incroyable, faire ses achats sans bouger de sa chaise sont des exemples des avantages considérables qu'internet a créés.

Les technologies, qui ne cessent d'évoluer, ont permis de mettre en œuvre ces nouveaux moyens de communications mais aussi de mettre le monde face à des nouveaux défis. Ces mêmes technologies sont aujourd'hui au cœur de notre système à tous les niveaux, elles confrontent les individus à une situation délicate : comment préserver sa vie privée et faire confiance dans ce contexte, quand tout est mis en œuvre pour absorber un maximum d'informations ?

Les entités qui absorbent les données personnelles des internautes sont nombreuses et sont partout, parfois même cachées, c'est ici qu'entre le terme anonymat, ce droit à nécessairement besoin d'être appliqué sur internet comme il l'est dans la vie réel, les données personnelles que nous partageons tous les jours sur la toile sont des traces indélébiles et ce droit est donc violé. Comment ce droit est-il violé et comment peut-on s'en affranchir ? C'est ce que ce document tente de démontrer, il propose également un service collaboratif anonyme permettant d'éviter d'être retracé et identifié sur la toile.

2. L’anonymat

2.1 En générale

L’anonymat signifie globalement l’état de quelqu’un ou quelque chose qui choisit de rester inconnu, inaccessible, impossible à suivre : anonyme. Au cours de l’histoire l’anonymat a été utilisé à plusieurs fins et sous différentes formes, certains le considérant comme un côté obscure synonyme de manque de courage ou lâcheté et d’autres comme un moyen de protection, l’anonymat a traversé et évolué à travers les époques et a été directement influencé par l’avancée technique des moyens de communications et du droit en générale.

La technique la plus connu et la plus drastique consiste à rester anonyme en ne mentionnant aucun nom, la lettre manuscrite non signé en est l’exemple parfait, l’autre technique consiste à utiliser un pseudonyme derrière lequel l’identité réel est dissimulée, William Shakespeare est probablement un pseudonyme derrière lequel se cachait le vrai auteur des œuvres, les femmes artistes également durant l’histoire se sont cachées derrière des pseudonymes masculins pour éviter la répression et la censure. Les lois ont été aussi encouragées à favoriser l’anonymat dans certains cas de figures : les services fournis par les avocats et les médecins sont tenus au secret professionnel et donc une certaine forme d’anonymat, les articles de journaux et leurs sources le sont aussi, l’accouchement sous X, aller voter requiert l’anonymat également etc.

Les applications et les objectifs de l’anonymat sont autant nombreuses que variées et peuvent être utilisés à des fins positives ou négatives dépendant du contexte et du point de vue, dans la vie réel le droit à l’anonymat est donc un droit fondamental presque illimité, on peut penser ce que l’on veut mais certaines limites existent notamment quand il s’agit de les dire : incitation au crime, discrimination raciale etc., ces limites sont fixées par le code pénal. Dans la vie virtuelle, donc sur internet, ce droit est devenu la norme et sa régulation problématique. Donc forcément le principe d’anonymat sur internet fait couler beaucoup d’encre et est devenu une question hautement politique notamment autour de la question : faut-il garantir ou non l’anonymat sur internet ?

2.2 Sur internet

Être anonyme sur internet ne se résout pas à se cacher simplement derrière un pseudonyme, la tâche est bien plus complexe, l’anonymat réel requiert une non-traçabilité, et évidemment la nature des réseaux informatiques rend cela difficile.

Mais l’anonymat sur internet est un besoin et une liberté nécessaire pour beaucoup de monde, que ce soit pour affirmer sa différence sans craindre de représailles, parler de

problèmes personnels ou de santé ou dénoncer des faits graves comme le font les lanceurs d'alertes, les raisons sont ici également aussi nombreuses que variées.

De l'autre côté, vous avez les privées et les grands acteurs d'internet qui sont eux hostile à l'anonymat sur internet et préféreraient stocker dans leurs bases de données les identités réelles de leurs utilisateurs, cela paraît évident car leurs modèles économiques reposent sur les informations des utilisateurs. Les états d'une manière générale, la Suisse compris, sont favorable à la création d'une identité réel électronique et centralisé que tout citoyen devrait utiliser pour s'identifier sur les services que propose la toile. Les pays répressifs et autoritaires rêveraient quant à eux de suivre l'activité en ligne de leur population.

Donc, aujourd'hui l'anonymat sur internet représente un grand enjeu pour notre système et la vie privée d'une grande partie de la population de ce monde. A l'heure du web 2.0 où les internautes sont incités à partager un peu plus de leurs données personnelles, notamment à travers les réseaux sociaux, les forums de discussion, les messageries, les sites de rencontres et autres, les suspicions et craintes d'atteinte à la vie privée, à la liberté d'expression et la surveillance de masse, notamment mener par les gouvernements, sont des thèmes de plus en plus préoccupants.

Les traces laissées lors d'utilisation d'un service sur la toile sont considérables et compromettent l'anonymat, caché derrière un pseudo ne suffit plus, une action en justice permet généralement de récupérer les informations nécessaires à une identification, que ce soit auprès du service concerné ou des différents intermédiaires du type fournisseur d'accès à internet. L'anonymat réel ne peut donc pas être assuré au vu du caractère limité de cette protection juridique et c'est pourquoi de nombreux internautes ont choisis d'autres solutions techniques pour contourner cette problématique, la nécessité d'approfondir ses connaissances est requise et n'est donc pas accessible à tout le monde.

2.3 Pourquoi l'anonymat sur internet ?

Pour une grande majorité de personnes, la vie privée en ligne et la vie privée réelle sont différentes, on permet certaines choses qu'on n'oserait même pas imaginer dans la vie réelle, et pourtant on pourrait croire que les gens ne s'y intéressent pas vraiment, peut-être par manque de connaissance, et pourtant la confidentialité en ligne est très importante. Voici différentes raisons pour lesquelles il faut s'en soucier :

2.3.1 Vie privée – Données personnelles

Les données personnelles sont l'essence de l'économie numérique, les sociétés numériques s'enrichissent grâce aux données récoltés sur les internautes, malheureusement on a pu constater avec de nombreux scandales que les sociétés ne sont pas en mesures de garantir une sécurité à 100% pour les données des utilisateurs. Les gouvernements et les entreprises profilent les internautes et si ces informations finissent entre de mauvaises mains il deviendra théoriquement possible de manipuler ces derniers afin de modifier leurs façons de penser ou même de voté, on pense notamment à l'ingérence russe durant l'élection présidentielle américaine de 2016 qui a sans doute joué un rôle majeur dans l'orientation de l'opinion des internautes.

2.3.2 Protection de l'identité

Internet est disponible dans tous les pays du monde, néanmoins il ne peut être utilisé de la même manière partout, notamment à cause des régimes autoritaires ou la moindre action est surveillé et peut être réprimandée sévèrement si elle constitue une infraction. Protéger son identité sur la toile devient une obligation dans ces cas-là.

2.3.3 Censure

Certains pays pratiquent la censure ou l'accès à certains sites web sont bloqués, les réseaux sociaux comme Facebook, Twitter, Instagram et autres par exemple sont bloqués en chine.

2.3.4 Couvrir des actions illicites ou réprimées

Les lanceurs d'alertes et leurs actes, qui consistent à divulguer des informations qu'ils jugent menaçant pour l'intérêt général ou public, sont évidemment réprimées et lourdement sanctionner par ceux qui protègent ces informations surtout s'il s'agit d'un état, on pense notamment à l'affaire Snowden. Dans ce cas, la diffusion de ces informations, généralement vers les médias, nécessitent un canal de communication totalement anonymes pour échapper à une identification.

3. Pseudonymat

Le pseudonymat, qui signifie “faux-nom”, est un aspect de l’anonymat qui consiste à masquer son identité sans forcément chercher l’anonymat complet, cela dépend du contexte, on peut dire qu’il est à mi-chemin entre l’anonymat et l’identification précise. C’est concrètement reconnaître une personne qui porte un pseudonyme sans savoir qui elle est en tant que personne physique. Ce principe largement répandu sur la toile fonctionne dans des contextes aussi nombreux que variés : blogs, forums, jeux en ligne, réseaux sociaux etc.

Cette pratique consiste à, pour celui qui utilise un pseudonyme, se confier en toute discrétion et d’échanger des informations sur des sujets sensibles par exemple, l’avantage premier est donc d’assurer un minimum de confidentialité, toutefois le pseudonyme n’est pas toujours suffisant pour protéger sa vie privée et son anonymat.

En informatique, le pseudonymat se définit en plusieurs niveaux de confidentialité :

Tableau 1 : Les types de pseudonymes

Type	Description
Non associable	Le lien entre l’être humain et le pseudonyme ne peut être déterminé ni publiquement, ni par les administrateurs système.
Potentiellement associable	L’association entre l’être humain et le pseudonyme ne peut être établie que par les administrateurs système, c’est à dire qu’il n’est publiquement pas connu.
Associable	L’association entre l’être humain et le pseudonyme est facilement identifiable ou connu publiquement.

3.1 L’exemple Wikipédia

Les utilisateurs de la plateforme Wikipédia utilisent largement les pseudonymes, cependant les administrateurs des sites ont la possibilité d'associer un pseudonyme à une personne physique même si cette dernière ne divulgue pas de données personnelles, en effet les identifiants de connexion leurs permettent de retrouver son adresse IP et de potentiellement l’associé à un utilisateur enregistré. Toutefois, il est

possible de créer un pseudonyme sans pouvoir établir un lien en utilisant un proxy ouvert (service permettant de cacher son adresse IP réelle), mais Wikipédia gère et bloque indéfiniment (généralement 1 à 5 ans) les adresses IP de ses services proxy pour éviter qu'elles soient utilisées pour du vandalisme notamment et autres pratiques indésirables.

4. Traces numériques

Concrètement les traces numériques sont toutes les informations d'activités ou d'identités liés aux utilisateurs et qui sont enregistrés dans un dispositif numérique : tous les systèmes demandant une interaction ou identification est potentiellement susceptible d'enregistrer des données.

Chaque internaute laisse, volontairement ou involontairement, des centaines de traces chaque jour sur la toile, ces informations peuvent potentiellement constituer, une fois rassemblées, un profil très détaillé. Il devient donc difficile de maîtriser son identité sur la toile, les informations collectées peuvent également être rendues public par les moteurs de recherches et donc influencer la e-réputation d'un internaute, cette identité peut favorablement ou pas orienter une opinion par exemple.

4.1 Les traces volontaires

Les traces volontaires sont les informations données consciemment et délibérément par l'internaute, ces traces sont représentées, par exemple, par une inscription sur un réseau social, un commentaire laissé sur un forum, une photo publiée, un CV en ligne etc. Ces traces volontairement laissées sont la partie que l'internaute peut contrôler en les supprimant ou en les modifiant, à noter que les données supprimer ne le sont pas vraiment, prenons un exemple très simple : vous commandez en ligne des habits avec une certaine adresse de livraison, entre temps vous changez de domicile et décidez de supprimer l'ancienne adresse de livraison sur le site pour utiliser la nouvelle : l'ancienne adresse ne sera réellement pas supprimer sur le serveur du site de vente mais ne sera plus visible pour l'internaute : on parle de suppression logique, dans le contexte du site de vente il est évident que ce dernier à l'obligation légale de garder mémoire de ces adresses car elles sont directement liées à la facturation, mais d'une manière globale ce procédé est présent partout et pour toutes les données, on peut donc qualifier ces traces comme indélébiles.

4.2 Les traces involontaires

Les traces involontaires sont les informations collectées à l'insu de l'internaute, ces informations concernent l'usage d'internet par l'internaute depuis le moment où il se connecte au réseau.

Les données que peuvent récupérer les navigateurs et sites web que nous utilisons sont nombreuses et variées :

4.2.1 Eléments collectés par les moteurs de recherche

4.2.1.1 Environnement – Logiciels

Un navigateur connait des informations à propos de l'appareil utilisé mais également sur les logiciels qui sont installées sur ce dernier :

Logiciel :

- Nom et version du système d'exploitation
- Nom et version du navigateur
- Nom et version des plugins installés

Matériel :

- CPU – Détail sur le processeur
- GPU – Détail sur le processeur graphique
- Niveau de batterie

4.2.1.2 Connection

Un navigateur connait les informations concernant la connectivité au réseau web :

- Adresse IP publique

Une adresse IP est une adresse d'identification unique attribué à chaque terminal se connectant au réseau internet, cette adresse peut être attribuée de façon permanente ou provisoire, elle va essentiellement permettre de communiquer sur le réseau avec d'autres périphériques mais aussi d'être potentiellement géo-localisable. Le protocole Internet Protocol (IP) va donc fournir une adresse et permettre d'échanger des flux de données entre deux terminaux. C'est cette même adresse qui porte le plus préjudice à l'anonymat.

- Nom du fournisseur d'accès à Internet
- Vitesse de téléchargement

4.2.1.3 Localisation

Le navigateur peut révéler votre position géographique d'après l'adresse IP, en réalité cette dernière indiquera l'adresse physique d'un des points de sortie de votre fournisseur d'accès (généralement un routeur), toutefois si votre appareil à le GPS activé, les différents services n'auront aucun mal à localiser précisément votre position.

4.2.1.4 Historique de navigation

L'historique de navigation est la liste des sites visités qui inclut les informations détaillées de ces derniers, on y retrouve notamment la date et l'heure, l'URL, le nom etc. Il a été révélé que Google gardait en mémoire l'historique des navigations même après

suppression de la liste sur le moteur de recherche Chrome, là aussi on parle de suppression logique.

4.2.1.5 Mouvement de souris

Aussi futile que ce soit, les navigateurs ont également les moyens de suivre les mouvements de souris.

4.2.1.6 Autres données collectées par les navigateurs

Données techniques en tout genre, cela comprend la taille de l'écran, la langue utilisée, les polices utilisés etc. et également les connexions aux médias sociaux établies pendant la session.

4.2.2 Eléments collectés par les sites web

Les sites web ont également l'habitude d'en savoir un maximum sur vous. En plus de certaines données techniques, l'outil principal de récolte de données est le cookie. Il permet notamment d'afficher des publicités ciblées ou améliorer l'expérience utilisateur. La plupart des données techniques lui sont directement fournis pour le navigateur lui-même.

Quelques données techniques pouvant être récoltés sans consentement :

- Adresse IP
- Date et heure de la demande
- Fuseau horaire
- Statut d'accès / code d'état HTTP
- Quantité de données transférées
- Site Internet à l'origine de la requête
- Nom et version du navigateur
- Nom et version du système d'exploitation

4.2.2.1 Démonstration

Afin d'avoir un aperçu des données qu'un site internet peut récolter, j'ai mis en place un page web qui liste certaines de ces données, ces dernières ne nécessitent aucune demande ni acceptation de la part du service ou de l'utilisateur, donc ses données et plus encore sont récoltées et stockées à chaque fois que vous visitez une page web

Le lien : http://ht54ixtuy.preview.infomaniak.website/UserInfomations.php

Capture d'écran depuis un PC de la HEG à Carouge :

Figure 1 : Exemples de données récoltées

(http://ht54ixtuy.preview.infomaniak.website/UserInfomations.php)

4.2.3 Eléments collectés par les intermédiaires

4.2.3.1 Fournisseurs d'accès à internet

S'il y a bien une entité capable de voir tous les faits et gestes d'un utilisateur, c'est bien le fournisseur d'accès à internet, en effet tout le trafic est acheminé via ce dernier avant d'arriver sur le réseau internet, chaque octet de données envoyés ou reçu passe physiquement via leur infrastructure et ils sont donc en mesure de conserver toutes les informations qui transitent.

- Identité et géolocalisation

Le FAI assigne à tous ses utilisateurs une adresse IP privé, cette adresse se situe dans les plages d'adresses IP non accessible depuis internet et ne permet également pas de se connecter à internet, elle fonctionne uniquement sur les réseaux privés (réseau wifi domestique, réseaux en entreprise etc.). Afin de connecter un utilisateur à internet avec une adresse IP valide, le FAI dispose d'une adresse IP publique qu'il fera correspondre

aux adresses IP privés de ses clients à l'aide de technologies de translation d'adresse (PAT-NAT par exemple), donc dans ce sens le FAI est capable de localiser un utilisateur très facilement et encore plus précisément si les services de localisation GPS sont activés sur l'appareil de ce dernier.

Pour aller plus loin, il est également possible pour le FAI de faire correspondre l'adresse MAC du support utilisé (notamment les boîtiers wifi pour les réseaux privés) avec sa base de client pour retrouver des informations précises sur ce dernier : adresse physique et facturation notamment.

Et évidemment ces informations recueillies peuvent également être consultés par les organisations externe comme les services de polices ou autre organisme gouvernemental.

- Journaux de navigation et de recherche

Les FAI tiennent des journaux de navigation et de recherche, chaque requête envoyée sur internet est enregistrée et répertoriée, voici quelques exemples de données que peuvent récoltés les FAI, elles seront souvent corrélées à d'autres informations (géolocalisation, contenu...) :

  - Les sites visités
  - L'URL complète avec le chemin d'accès (si la communication non crypté)
  - Applications utilisées
  - Habitudes en ligne et hors ligne
  - Temps passé sur un site

Même si la connexion est cryptée, le FAI aura besoin de certaines informations en clair pour pouvoir acheminer la demande, en effet lors d'une recherche de domaine via un navigateur ou simplement lors d'un clic sur un lien URL, l'ordinateur aura besoin de l'adresse IP du domaine en question pour pouvoir établir la connexion. Pour se faire, ce dernier va interroger un répertoire DNS pour traduire le nom de domaine en adresse IP et étant donné que les requêtes DNS peuvent ne pas être crypté, il devient facile de créer un historique de navigation pour chaque utilisateur. Ces informations intéressent particulièrement les organismes publicitaires et gouvernementales.

- Communication non cryptée

Les informations les plus détaillés que le FAI peut recueillir proviennent des pages web n'utilisant pas le protocole de chiffrement HTTPS (HyperText Transfer Protocol Secure). Cela veut dire qu'il est capable de voir en clair le contenu d'une page web que l'utilisateur

visite ainsi que l'URL complète, donc dans ce cas il lui est possible de suivre toutes les actions effectuées sur un site web et de voir le contenu, contenu sensible inclus :

- Données bancaires et autres informations de paiements
- Email
- Messages (commentaires, messages, chat)
- Nom d'utilisateur et mot de passe
- Transactions Bitcoin / bancaire

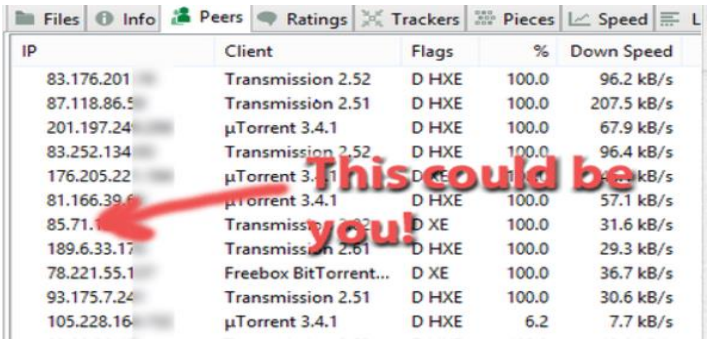
- Téléchargements

Les FAI sont en mesure de collecter vos activités liées aux téléchargements, néanmoins il ne s'intéresse pas vraiment au contenu qui est téléchargé, même s'ils en ont les capacités, mais plutôt à la bande passante nécessaire à ces téléchargements et par le fait de savoir si ces derniers ralentissent tout le monde, les actions menés par ces derniers se concentrent donc autour du type de trafic, ils peuvent voir quel trafic a été généré par des jeux en ligne, du courrier électronique, du vidéo chat, la navigation sur la toile ou BitTorrent(protocole de transfert de données pair à pair) par exemple, ils ralentissent une connexion s'il juge qu'il y a un abus d'usage de la bande passante.

Le vrai problème de confidentialité concernant les téléchargements ne vient pas directement des FAI mais des sociétés de médias qui protègent leurs produits des téléchargements illégaux. En effet lorsque qu'on télécharge du contenu via un client TORRENT (permet à un pc de devenir un nœud qui compose le réseau BItTorrent) par exemple, il devient possible pour ces sociétés de chercher des torrents de leur contenu et de voir avec quels utilisateurs ils sont connectés et entrain d'échanger du contenu, parmi les informations visibles se trouvent évidemment l'adresse IP des utilisateurs qui téléchargent du contenu illégal.

Voici un exemple avec un client BitTorrent, les sociétés de médias peuvent se balader sur ce type de programme et trouver des adresses IP de gens qui piratent leurs contenus :

Figure 2 : Adresse IP sur client BitTorrent



(https://www.best-bittorrent-vpn.com/how-to-use-utorrent-anonymously.html)

A partir de l'adresse IP, ces sociétés vont rechercher votre fournisseur d'accès et les contacter afin qu'il retrouve votre identité et ainsi vous envoyez une lettre disant que vous avez été pris à pirater du contenu protégé et ainsi être fiché en tant que pirate.

4.2.3.2 Services externes

Les services VPN et PROXY ont de plus en plus la côte et le nombre d'entre eux ne cesse d'augmenter, ces services agissent en tant qu'intermédiaire (en plus du fournisseur d'accès) afin de sécuriser et anonymiser une connexion, cependant tous les fournisseurs de ces services ne sont probablement pas digne de confiance, la plupart ont besoin du strict minimum pour pouvoir assurer le service : vrai adresse IP fournit par le FAI, IP interne du service, ID client, états de connexion, messages de contrôle et d'erreur.

Ce qui va les différencier sera la politique de confidentialité et je journalisation, certains ont l'obligation de garder en mémoire des informations sur les utilisateurs quand d'autres peuvent fournir ce service sans garder trace de l'utilisateur, ces différences sont notamment dues aux lois en vigueur dans les pays respectifs depuis lequel le service est fourni. Cela signifie pour l'utilisateur qu'il ne bénéficiera peut-être pas de l'anonymat qu'il espérait.

Voici les données qu'ils sont susceptibles de collecter :

- Journaux de connexion

Ces données sont généralement utiles pour optimiser et contrôler les services, on peut les appeler métadonnées, il s'agit notamment des dates et heures de connexion, de la bande passante utilisée et parfois de l'adresse IP, la plupart de ces données peuvent être récoltés sur une base globale ou bien individuel.

- Journaux d'adresses

Ces données sont le point pour lequel un service externe peut être considéré comme sûr ou non, en effet l'objectif est de dissimuler une adresse IP mais certains de ces services tiennent des journaux d’adresses IP qui peuvent potentiellement être liées à des individus. Dans ce cas, les journaux d’adresses IP mettent en péril l’anonymat, d’autant plus si ces données tombent entre les mains d'organisations gouvernementale.

- Journaux de trafic

Ce type de journaux contiennent généralement le contenu du trafic internet, les fichiers téléchargés, les logiciels utilisés, l’historique de navigation et d’autres informations liées à l’activité sur la toile. Si ce type de journaux est conservé c’est probablement pour générer du profit, les informations peuvent être vendu par exemple à des sociétés tierces, il est important pour l’utilisateur de se référer à la politique de confidentialité car ce type de journaux va à l’encontre de l’un des objectifs principaux de ces intermédiaires : la confidentialité.

Généralement utilisé pour confondre les traces laissés sur internet, ces services externes utilisent des protocoles des chiffrements pour éviter qu’un autre intermédiaire puisse lire les contenus, notamment le FAI qui ne pourra pas savoir ce que vous faites sur internet, toutefois ce dernier sera informé de quand est-ce que vous accédez à internet et quelle quantité de données a été échangé.

4.3 Cookies

Un cookie est concrètement un fichier texte installé sur le pc d'un utilisateur lorsqu'il visite un site web. L'objectif premier d'un cookie est de stocker des informations à propos de l'utilisateur dans le but d'optimiser l'expérience utilisateur, c'est notamment éviter de ressaisir les mêmes données plusieurs fois, conserver ses produits dans le panier virtuel même après quelques jours ou bien garder sa connexion active même après la fermeture du navigateur, ils opèrent donc comme des marqueurs pour identifier une personne et mémoriser la configuration du site web.

Toutefois comme ces fichiers sont largement utilisés pour récupérer des données, ils peuvent également être utilisés pour transporter des données liées aux publicités notamment pour le profilage comportemental et le re-ciblage, ils affectent donc la vie privée en ligne des utilisateurs.

D'un point de vue technique ils fonctionnent sur les mêmes principes, ce qui les différencies sont les objectifs pour lesquelles ils ont été créés et surtout la manière d'être crées et utilisées. En effet certains cookies suscitent des débats et de la confusion autour de la confidentialité et la vie privée et constituent actuellement le moyen le plus courant pour identifier un utilisateur et fournir un service personnalisé.

4.3.1 Structure

Les cookies ont une structure très précise, elle est constituée de plusieurs attributs (nom/valeur) qui stockent des informations diverses : certaines pour assurer le bon fonctionnement du cookie, d'autres pour la personnalisation du service. Voici une liste d'attributs principaux possibles :

Tableau 2 : Structure d'un cookie

Attributs	Description
Nom	Il s'agit du dom du cookie, il est le seul à être obligatoire
Expiration	Date limite à laquelle le fichier cookie ne doit plus être stocké sur le PC
Domaine	Nom de domaine de la page visité

Chemin d'accès	Représente le chemin de page ayant créée le cookie
Secure	Prend comme valeur "TRUE" ou "FALSE" pour savoir si le cookie sera envoyé via une connexion sécurisée ou non (HTTP ou HTTPS généralement)

A cela s'ajoute donc les données personnelles qui seront enregistré de la même manière : nom / valeur. L'expiration d'un cookie est variable et dépend du contexte, il peut être temporaire ou permanent.

4.3.2 Niveau de sécurité

Les cookies peuvent stocker des données de configuration comme vue au-dessus, des données dédiées aux analyses, à la pub, mais aussi des données personnelles qui peuvent être très sensibles : données bancaires pour une utilisation en ligne, orientations politiques, données concernant la santé, orientation sexuelle etc. Les données sensibles sont nombreuses et variées et il est nécessaire de protéger ces fichiers pour éviter toute utilisation frauduleuse. Il existe plusieurs techniques pour subtiliser des cookies afin d'en exploiter les données pour différentes raisons, les plus fréquentes sont pour obtenir des droits privilégiés ou récupérer des données d'authentification, voici quelques techniques :

- Vol par accès physique à la machine
- Vol par sniffing
- XSS, vol de session via les cookies
- CSRF, pour les requêtes falsifiées
- Vulnérabilité du navigateur

4.3.3 Types de cookies

Il existe deux grandes familles de cookies : les cookies propriétaires et les cookies tiers.

4.3.3.1 Les cookies propriétaires

Ces cookies sont créés sur votre machine par le domaine que vous visitez. Ils servent essentiellement à améliorer l'expérience utilisateur, comme en gardant une session ouverte, ou à récupérer des données analytiques. Ils sont considérés comme étant normaux pour l'utilisateur, ils ne contiennent pas de virus et ne compromettent pas

l'ordinateur et ont de nombreuses raisons d'être utilisés. Désactivé ce type de cookie impactera sérieusement l'expérience utilisateur, vous ne pourrez par exemple pas commander en ligne plusieurs produits en même temps, mais seulement un à la fois. Voici quelques applications de ce type de cookie :

- Connexion sur un site établi même après fermeture du navigateur
- Panier virtuel rempli d'articles même après fermeture de la session
- Publicités ciblées
- Paramètres de confidentialité de l'utilisateur

4.3.3.1.1 Comment sont-ils créés ?

Les cookies sont créés simplement en visitant un site web à l'aide d'un navigateur, le nom du cookie enregistré fera référence au domaine visité, par exemple si vous visitez www.ge.ch, alors vous aurez un cookie lié directement à ce nom de domaine enregistré sur votre machine pendant un temps définit.

4.3.3.1.2 Comment sont-ils intégrés ?

Lorsque vous visitez un site en particulier pour la première fois, alors un bout de code créer par les développeurs du site s'enclenche et créer un cookie sur votre navigateur, lorsque vous revisitez le site, un code se chargera de lire votre cookie lié au domaine et reprendra les différentes informations écrites dans le cookie, pour finalement vous assurez une expérience utilisateur convenable. Ce principe est totalement invisible pour l'utilisateur, mais n'est pas en soi problématique en matière d'anonymat et de confidentialité dans la mesure et vous avez accepté, souvent malgré vous, la création de ses cookies.

4.3.3.1.3 Qui peut y accéder ?

Les cookies propriétaires sont accessible uniquement par leurs créateurs, en aucun cas un autre domaine peut accéder aux cookies qui ne sont pas les siens, à moins de se les faire subtiliser comme énoncé plus haut.

4.3.3.2 Les cookies tiers

Ces cookies sont créés par un autre domaine que celui que vous visitez, ils servent au suivi inter site et notamment au ciblage publicitaire. D'un point de vue technique, il n'y pas de différence avec les cookies propriétaires, lorsque le cookie propriétaire est créé quand vous visitez un site, un ou plusieurs autres cookies peuvent être créé et porté un nom différent du domaine visité et donc pointé vers une URL différente : la raison pour laquelle on les nomme cookies tiers. Ce type de cookie pose énormément de problème en termes d'anonymat et de confidentialité, car les actions des utilisateurs sont traquées

à travers tous les sites web qui posent un cookie venant de la même source. Même si les nouvelles lois en matière de données personnelles poussent les sites à informer leurs utilisateurs de ces pratiques, ce type de cookie continue d'être une source importante de données sur les comportements des utilisateurs et s'apparente donc à une collecte de données silencieuse sans consentement de l'utilisateur.

Les cookies tiers collectent notamment les données pertinentes suivantes :

- Données personnelles telles que l'âge, le sexe
- Site visité via lequel le cookie a été généré
- Sous-pages visitées sur le site visité
- Temps passé sur le site
- Identifiant publicitaire

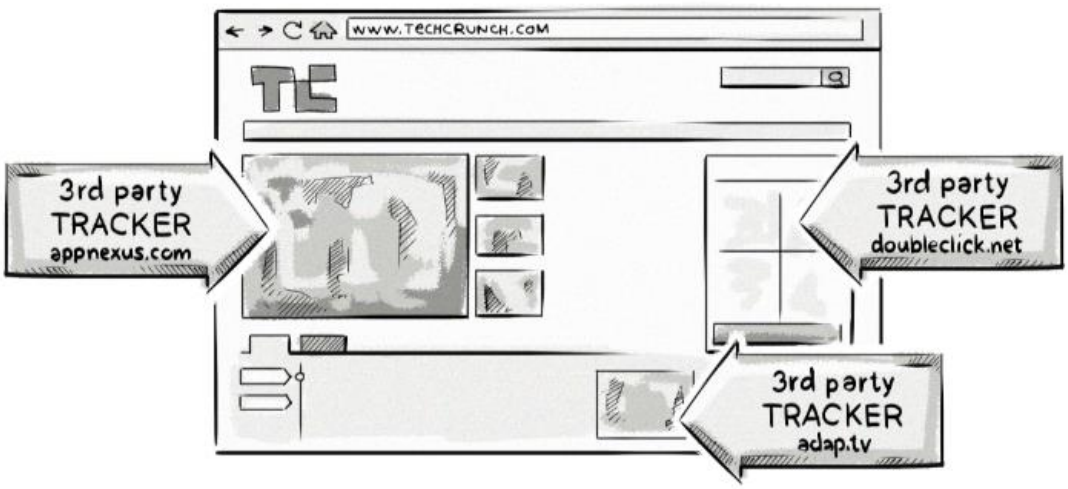
4.3.3.2.1 Comment sont-ils créés ?

Les cookies tiers sont donc créés par un domaine différent, en pratique cela signifie que lorsque vous visitez un site, vous serez susceptible et pour différentes raisons d'avoir des cookies provenant de domaines différents enregistrés sur la machine. Concrètement le propriétaire du site que vous visités incorpore des éléments de code qui ne lui sont pas propres, ces bouts ce code sont fournis par des sites partenaires, qui sont souvent des régies publicitaires, et permettent d'injecter un ou plusieurs cookies sur la machine de l'utilisateur.

Imaginons qu'un utilisateur visite, à l'aide d'un navigateur, le site 1. Le navigateur possède déjà un cookie provenant de ce site, ce cookie contient son identifiant. Maintenant, le site 1 a intégré une publicité partenaire qui doit être chargé en appelant le site 2. Lorsque l'appel vers 2 se fait, le site 1 lui transmet certaines informations en paramètre, notamment le nom de son propre site et l'identifiant de l'utilisateur. Le site 2 enregistre ces informations, renvoie la bannière publicitaire et enregistre un cookie sur le navigateur au passage. Se procéder permet au site 2 de suivre l'utilisateur sur tous les sites ou sa publicité sera visible en l'identifiant avec le cookie précédemment installer, il permet au final de proposer à l'utilisateur de la publicité pertinente, mais cela constitue une certaine forme de pistage.

4.3.3.2.2 Comment sont-ils intégrés ?

Figure 3 : Intégration des traqueurs (cookies tiers) sur une page web



(https://clearcode.cc/blog/difference-between-first-party-third-party-cookies/)

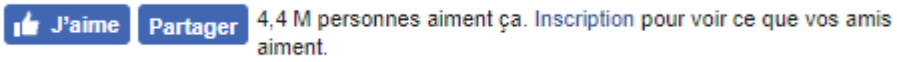
- Bannière publicitaire

Lorsqu'un site désire monétiser son contenu, la solution évidente est d'y placer de la publicité, l'annonceur fournira au propriétaire du site un élément de code à placer sur une ou plusieurs pages pour que l'utilisateur puisse voir les annonces. Concrètement, avant que la page ne soit chargée pour l'utilisateur, ces éléments de code vont faire appels au serveur de l'annonceur afin d'y charger le contenu publicitaire et par la même occasion de placer un cookie sur le navigateur du visiteur.

- Modules sociaux

Les modules sociaux sont proposés dans une grande majorité des sites web, ils sont ajoutés par les propriétaires des sites pour des faits évident de marketing, mais ces modules permettent aux différents médias sociaux de placer des cookies sur le navigateur des utilisateurs.

Figure 4 : Module sociaux : bouton J'aime



(https://developers.facebook.com/docs/plugins/like-button)

Figure 5 : Module sociaux : boutons sociaux

(https://mageewp.com/how-to-add-social-media-buttons-to-sidebar-or-menus.html)

Cette manière de faire permet aux médias sociaux d'où proviennent les cookies de suivre les sites sur lesquels l'utilisateur a visités puis une fois qu'il sera revenu sur un des sites des réseaux sociaux, alors de la publicité ciblée en lien avec ce qu'il a déjà visité lui sera proposé.

Ces modules sociaux peuvent être des boutons "J'aime", des commentaires intégrés, ou des publications intégrées, dans tous les cas ils chargent tous des cookies venant d'un autre domaine que celui que vous visitez.

4.3.3.2.3 Qui peut y accéder ?

Comme pour les cookies propriétaires, seul le domaine qui les aura installés sur le navigateur pourra y accéder.

4.3.3.2.4 Eléments de code pour l'intégration

Placer une bannière publicitaire ou des boutons "J'aime" sur une page web nécessite donc de faire appel à des ressources externes pour y afficher le contenu, pour ce faire il existe plusieurs balises HTML prévu à cet effet :

- <iframe> : ajout d'une page HTML
- <link> : ajout fichier type CSS
- <object> : ajout de fichier multimédia
- <script> : ajout fichier type Javascript

Ces balises pointent vers des domaines différents, lorsque l'appel vers le serveur du domaine en question sera établi et que la ressource demandée sera renvoyée, le serveur de ce domaine placera un cookie au passage sur le navigateur de l'utilisateur.

Voici un exemple de code proposé par Google pour intégrer une vidéo YouTube :

Figure 6 : Eléments de code pour intégration vidéo YouTube

```
<iframe width="560" height="315" src="https://www.youtube.com/embed/videoseries?
list=PLx0sYbCqOb8TBPRdmBHs5Iftvv9TPboYG" frameborder="0" allow="autoplay; encrypted-media"
allowfullscreen></iframe>
```

(https://support.google.com/youtube/answer/171780?hl=fr)

La balise <iframe> contient un attribut “src” qui signifie source, et c’est cette adresse/domaine-là qui placera un cookie (du même nom) sur le navigateur en même temps qu’il fournira la vidéo, en l’occurrence le domaine ici est : www.youtube.com.

4.4 Pixel transparent - mouchard

Le pixel transparent ou mouchard est en réalité une balise HTML placée sur un site ou un email utilisé pour surveiller l'activité des utilisateurs. Pixel de suivi, pixel 1X1 ou pixel tag est donc un graphique de taille 1 pixel sur 1 qui est chargé lors d'ouverture d'une page web ou d'un email. Ces graphiques sont conçus pour être totalement invisible pour l'utilisateur qui ne sont de toute façon pas censés les voir. Ces derniers restent plus fiables que les cookies car l'utilisation de cookies peut-être complètement bloqué par l'utilisateur et donc fournir des données imprécises, inexactes voir pas du tout de données, alors que le pixel transparent ne peut pas être bloqué par un navigateur standard (sauf ajout de plugins spéciaux pour navigateur).

Voici quelques données récoltées par ces mouchards transparents :

- Nom et version du navigateur / logiciel de messagerie
- Type de support
- Adresse IP
- Date - Heure
- Activités sur site en question (avec plusieurs mouchards)
- Nom et version du système d'information

Combiné aux cookies, cette technique devient une source importante de données, notamment avec l'utilisation du langage JavaScript qui permet d'en savoir beaucoup sur le navigateur et l'utilisateur, et généralement les outils d'analyses comme Google Analytics nécessitent l'implémentation de ce type de traqueur. Beaucoup contestent ces pratiques car en termes d'anonymat et de confidentialité, il est évident que ce droit est violé, car cela implique un transfert de données sans consentement.

4.4.1 Comment sont-ils créés et intégrés ?

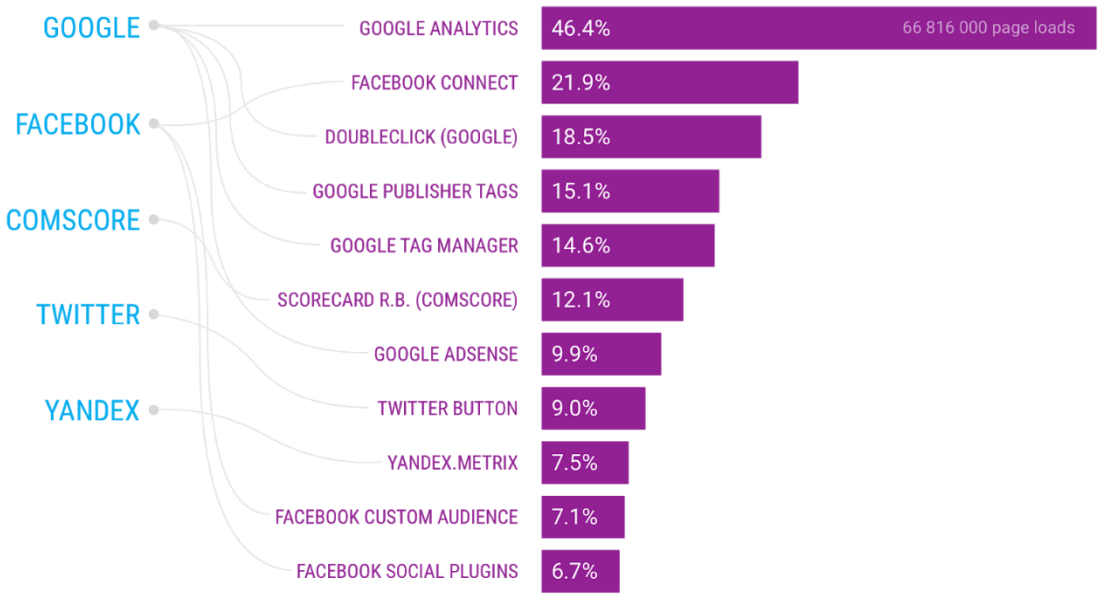
Tout d'abord ces mouchards sont camouflés et généralement directement implémentées dans le code des sites. La plupart des sites web ont besoin de statistiques et pour ce faire l'utilisation des outils d'analyse proposer par les géants du web sont primordiales, cela implique donc l'intégration de pixel transparent qui font office de de traqueur. D'autres les utilisent pour la publicité et là encore se sont les géants du web et leurs régis publicitaires qui proposent l'intégration de pixel transparent.

4.4.2 Qui peut y accéder ?

Les données récupérées par ces pixels transparents s'enregistrent directement sur les serveurs de ceux qui les ont créés, il s'agit très souvent de régies publicitaires gérer par les acteurs principaux d'Internet du type GAFAM.

Voici des statistiques intéressantes et surprenantes menées par Ghostery (bloqueur de traqueurs) en 2017 : l'étude de 144 millions de pages examinées dans plus de 12 pays dont la Suisse, a révélé qu'environ 77,4% des pages contenaient des traqueurs, parmi les traqueurs les plus en vue, la palme d'or revient à Google :

Figure 7 : Statistique sur les traqueurs



(https://www.ghostery.com/study/)

Ces traqueurs sont une réelle menace pour l'anonymat et la vie privée des internautes, en plus de pouvoir collecter des données ultra sensibles, c'est probablement la pratique la plus malhonnête vis-à-vis des utilisateurs. D'ailleurs, les opérateurs des sites également n'ont absolument pas la maîtrise de ces pratiques et ne savent donc pas quelles données ont été collectées ou non sur leurs utilisateurs.

Voici un exemple en vidéo poussé à l'extrême qui montre comment il est possible de suivre chaque faits et gestes de l'utilisateur avec cette pratique : https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/.

4.4.3 Eléments de code pour l'intégration

Généralement l'intégration de ce type de mouchard se fait à l'aide de la balise HTML suivante :

- <img> : ajout d'une ressource image

Figure 8 : Eléments de code intégration pixel transparent

```
<img height="1" width="1" style="display:none"
src="https://www.facebook.com/tr?id=<PIXEL_ID>&ev=<EVENT_NAME>"
 />
```

(Capture d'écran – Notepad++)

La balise <img> contient un attribut "src" qui signifie source, et c'est cette adresse/domaine-là qui va récupérer les données concernant l'utilisateur et les enregistrer sur son serveur.

5. Outils pour mettre en œuvre l'anonymat

La protection des données et l'anonymat sur internet plus généralement, font actuellement couler beaucoup d'encre : fuites de données personnelles, scandales à répétition, manipulation de l'opinion publique, pays répressif et autoritaires, surveillance de masse sont clairement des thèmes d'actualité.

Être anonyme sur internet requiert des connaissances et compétences qui sont loin d'être acquis pour la plupart des internautes. Voici quelques outils qui permettent de mettre en œuvre l'anonymat, chacun d'entre eux répond à un besoin bien spécifique et n'ont donc pas les mêmes objectifs, ce chapitre décrit les solutions des plus simples au plus complexes.

Il convient à chacun de choisir son degré d'anonymat selon ses besoins et son contexte, les outils décrits dans ce chapitre ne pourront pas, individuellement, vous garantir l'anonymat à 100%, toutefois ces outils sont complémentaires et vous permettront de vous rapprocher de l'anonymat complet.

5.1 Module d'extension navigateur

La plupart des navigateurs classiques proposent par défaut certaines options de confidentialités, notamment le blocage des cookies, toutefois dépendant du navigateur ils ne seront pas activés par défaut et leurs configurations difficile, les modules d'extension viennent faciliter cette configuration en prenant en charge plusieurs type de blocage et proposant des interfaces ludiques.

5.1.1 Protection contre les cookies tiers

- Privacy Badger

Ce module d'extension disponible sur Chrome et Firefox permet de bloquer les cookies tiers, en particulier les régies publicitaires qui cherchent à connaître l'historique des utilisateurs.

- Logiciel antipub

Les logiciels anti pub ont pour tâche principale de bloquer les contenus publicitaires, les plus performants de ces logiciels sont configurés, par défaut, pour également bloquer les cookies tiers qui agissent comme des dispositifs de suivi.

5.1.2 Protection contre les traqueurs (pixel transparent)

- Ghostery

Ghostery est un module axé sur la protection de la vie privée et est également capable de bloquer les cookies tiers mais surtout les traqueurs.

5.1.3 Protection des communications

HTTPS est un protocole de communication basé sur le protocole standard HTTP combiné avec une couche de chiffrement, c'est donc sa version sécurisée. En effet, le protocole HTTP ne chiffre pas les communications client-serveur et permet, à quiconque qui intercepte vos communications, de les lire, données sensibles comprises.

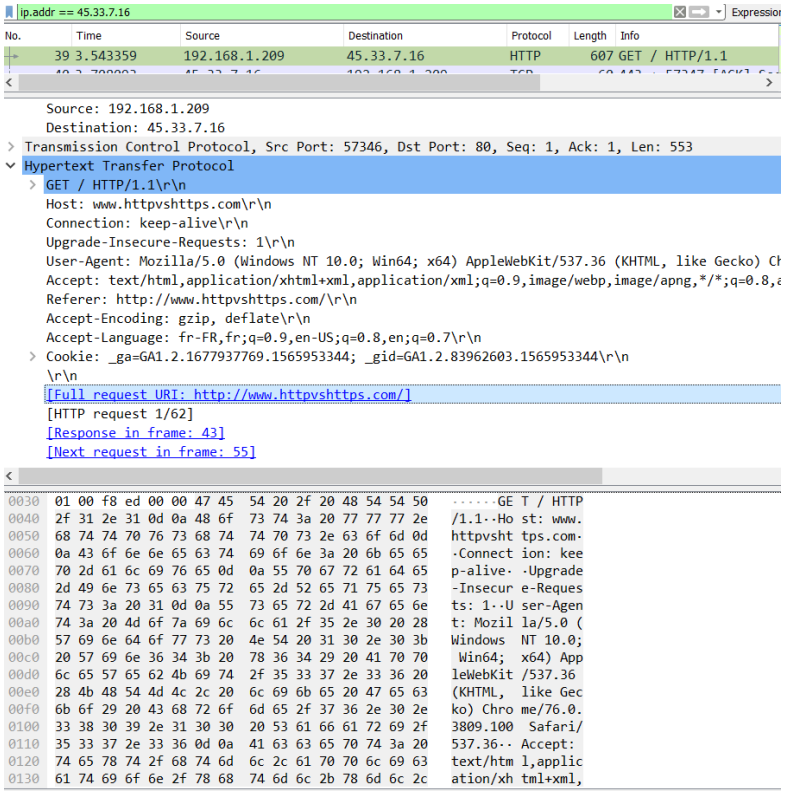
HTTPS rend illisible les communications en les chiffrant de bout en bout, elle permet donc d'échanger des données chiffrées mais également de confirmer l'identité des sites internet à l'aide de certificats HTTPS, toutefois tous les sites internet n'utilisent pas ce protocole sécurisé même s'il devient la norme.

- HTTPS Everywhere

Ce module permet d'appliquer le chiffrement pour le site qui ne le proposent pas, concrètement il réécrit les requêtes en utilisant une technologie intelligente pour les transformer en requêtes HTTPS. Une fois installer la navigation sur les sites se fera de manière sécurisée et le risque de se faire subtiliser des données devient pratiquement impossible.

Voici un exemple qui démontre la différence entre le protocole HTTP et HTTPS, le principe est simple, j'utilise WireShark qui est un analyseur de trafic et me place entre le client et le serveur, le client envoie deux requêtes, la première avec une connexion HTTP puis avec une connexion HTTPS :

Figure 9 : Analyse du trafic avec le protocole HTTP

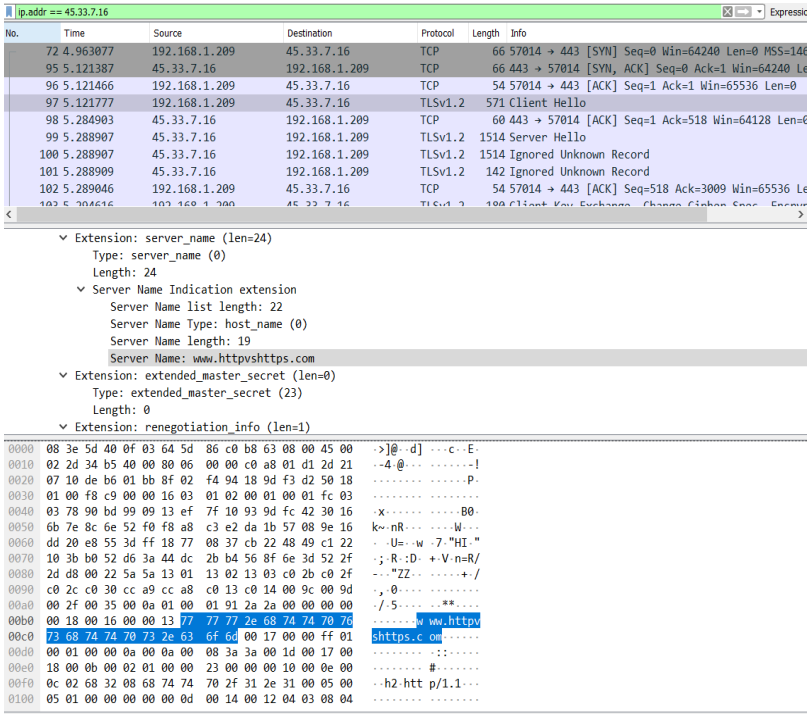


Requête vers http://www.httpvshttps.com/

La communication n'est pas cryptée, comme visible dans la section du bas.

(Capture d'écran - WireShark)

Figure 10 : Analyse du trafic avec le protocole HTTPS



Requête vers https://www.httpvshttps.com/

La communication est cryptée, comme visible dans la section du bas.

(Capture d'écran - WireShark)

5.2 Navigateurs anonymes

Ce n'est plus un secret, les navigateurs populaires tels que Google Chrome emmagasinent un maximum d'informations sur ses utilisateurs et rendent la navigation anonyme impossible malgré certaines extensions disponibles qui permettent de cacher certains aspects de l'identité. Ces navigateurs sont donc à éviter mais fort heureusement il en existe qui assure l'anonymat de l'utilisateur : pas de journalisation de l'historiques, pas de collecte d'adresse IP, aucunes données liées aux téléchargements, pas d'identifiant de suivi publicitaire etc. Ces navigateurs ont également pour vocation de rendre impossible la collecte de données en bloquant les cookies tiers et traqueurs, pour ce faire ils intègrent par défaut les modules d'extension cités dans la section "Module d'extension navigateur".

A noter que les navigateurs standards proposent un mode navigation privée ou incognito, ces mots sont trompeurs, ce mode ne cache en rien l'identité de l'utilisateur mais permet seulement le temps de son activation de surfer sur internet sans stocker de données localement, il s'agit notamment de ne pas enregistrer l'historique, les mots clés de recherches et le cookies, toutefois cela n'empêche en rien de continuer à être traquer à l'aide de pixel transparent ou tout simplement de la part du navigateur.

5.2.1 Tor Browser

Ce navigateur basé sur Firefox et embarque plusieurs extensions citées dans la section « module d'extension navigateur », il est à l'heure actuelle le navigateur fournissant le plus haut degré d'anonymat, aucune données propre au navigateur n'est collecté ni partager avec des services tiers, il a été spécialement conçu pour fonctionner sur le réseau Tor, il permet donc d'accéder aux services du réseau Tor mais également aux services présent dans le réseau internet, c'est à dire aux sites et services web classiques en passant par le réseau Tor, il est depuis peu également disponible sur Android.

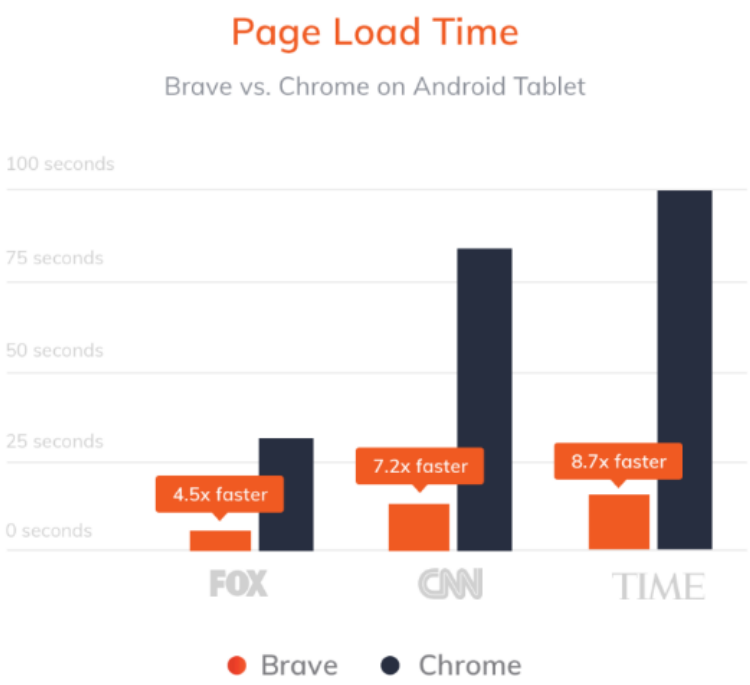
5.2.2 Epic

Epic Browser se est basée sur Chromium et permet donc des performances excellentes, il ne garde, ni ne partage de données propres aux navigateurs, en plus de bloquer les traqueurs et les cookies il propose un VPN gratuit en combinaison afin d'augmenter le degré d'anonymat.

5.2.3 Brave

Brave est également basé sur Chromium et protège ses utilisateurs contre les traqueurs et publicités en tout genre, il est donc principalement axé sur la confidentialité, mais se vente également d'être le plus rapide en termes de performance, voici une comparaison avec Chrome :

Figure 11 : Performance Brave navigateur



:

(https://brave.com/fr/)

5.3 Adresse mail jetable

Le courrier électronique est un aspect susceptible de compromettre l'anonymat. Heureusement il existe les adresses mail jetables qui ont pour objectif d'éviter de divulguer sa propre adresse email et donc potentiellement son identité pour des raisons de confidentialités et/ou éviter les mails indésirables de type pourriels. Elle permet concrètement à un utilisateur de recevoir un mail sur une adresse mail expirant après un certain délai, c'est à dire qu'elle sera supprimée après ce délai, ou à la décision de l'utilisateur. De nombreux sites fournissent ce type de service.

Lorsque vous souhaitez par exemple télécharger du contenu ou vous inscrire sur un réseau social votre adresse mail sera la plupart du temps requise pour confirmation et par la suite pour l'envoie de communications diverses, si vous transmettez votre adresse mail personnel, il est fort probable que vous compromettez votre identité d'une certaine manière, notamment si vous vous identifiez à l'aide de compte d'autres plateformes (Google, Facebook...).

5.3.1 Types d'adresse jetable

- Avec boîte de réception temporaire
- Possibilité de transférer les données vers une adresse principale (sous adressage)
- Possibilité de créer ou supprimer des alias

5.4 Systèmes d'exploitation

Actuellement les systèmes d'exploitation les plus utilisés sont Mac OS et Windows, et évidemment ils ne sont malheureusement pas connus pour leurs confidentialités, mais de plus en plus promettent une anonymisation vi leurs systèmes notamment l'aide de chiffrement matériel ou logiciel sécurisé et des mesures qui arrêtent le suivi en ligne.

La plupart des systèmes d'exploitation anonymes fonctionnent sous Linux et ont été créé par des passionnés d'anonymat, généralement ces systèmes s'installent à partir d'une clé USB ou un CD et permettent donc de posséder sur le même ordinateur, à la fois le système d'exploitation principal et le système anonyme, ce dernier inclut des outils de cryptage de communication, un navigateur anonyme et des programmes d'anonymat (I2P par exemple qui sera décrit plus bas).

Voici une liste des systèmes d'exploitation anonymes :

5.4.1 Tails

Tails est connu pour avoir été utilisé par Edward Snowden pour divulguer PRISM (un des programmes de surveillance de la NSA) dans le but d'échapper à la surveillance de la NSA. Tails est un système d'exploitation basé sur Debian.

5.4.2 Qubes OS

Le principe de ce système est, comme son nom l'indique, de garantir une sécurité maximale pour chaque activité réalisée sur l'ordinateur en les isolant dans des compartiments appelés Qubes.

5.4.3 Whonix

Le principe de Whonix est de faire fonctionner deux stations virtuelles, la première dédiée à l'utilisateur et la seconde est utilisé comme passerelle pour se connecter au réseau Tor (décrit plus bas), Whonix a donc pour objectif de préserver la sécurité et l'anonymat sur internet en utilisant le réseau Tor par défaut.

5.5 Réseaux privés virtuels - VPN

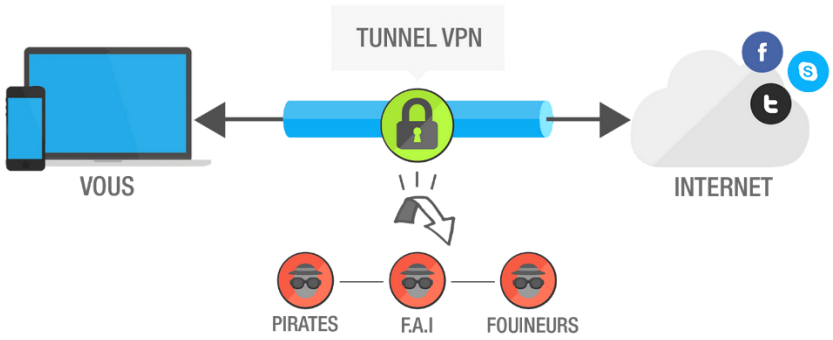
Les réseaux privés virtuels désignent un réseau crypté au sein du réseau internet, ce dernier garantie la confidentialité des données car elles circulent de manière cryptée afin que personne ne puisse les intercepter, ce procédé permet donc de créer un lien direct entre deux ordinateurs distants via la création d'un tunnel à l'aide d'un protocole d'encapsulation ce qui a pour conséquence de créer un réseau local virtuel, comme si ses deux ordinateurs de retrouvaient dans la même pièce.

Le VPN permet de contourner les contraintes géographiques liée aux contenus web, il va permettre à un utilisateur d'accéder à un réseau interne, comme celui d'une entreprise par exemple, ou simplement masquer son adresse IP en se connectant en dehors de son réseau local.

Tableau 3 : Avantages et inconvénients VPN

Avantages	Inconvénients
Masque l'adresse IP source sur tous les appareils et logiciels de l'utilisateur	Sécurité données personnelles : surveillance et contrôle de données de la part des sociétés VPN (notamment pour les service gratuit)
Chiffrement puissant des données à l'aide d'une clé 256 bits	Peut être difficile à configurer pour une personne lambda
Contournement de la géo-restriction	

Figure 12 : Principe du VPN



5.6 Proxy

Un Proxy est un programme qui sert d'intermédiaire entre un ordinateur et un réseau, le serveur proxy reçoit la requête du client puis la transfère vers le site cible avec sa propre adresse IP. Ce procédé crée un pont et transporte les requêtes via les chemins et routes demandés, dans la mesure où l'adresse IP source du client est masqué, la censure et les restrictions imposés par certains états peuvent être contournés par exemple.

Néanmoins ils sont discutables, car quiconque ayant accès au flux de données peut retrouver les informations en clairs vous concernant, on pense notamment aux fournisseurs d'accès, aux réseaux wifi publics aux sniffeurs et même aux gouvernements. Donc tous les proxys ne sont pas en mesure de chiffrer le trafic entre le client et le serveur Proxy.

A noter qu'il existe une multitude de proxy différents qui peuvent être très spécifique selon le contexte, les proxys lister ci-dessous n'assure pas tous un anonymat complet voir pas du tout, mais il est important de noter à quel type de proxy les utilisateurs peuvent être confrontés.

5.6.1 Proxy HTTP

Les proxy HTTP ont été créés spécialement pour les requêtes web, le proxy va donc jouer le rôle d'intermédiaire et lancer les requêtes HTTP vers les ressources demandées par le navigateur du client. Comme le trafic n'est pas chiffré, il est fortement recommandé de visiter des sites internet utilisant le protocole de sécurité SSL afin de créer un canal sécurisé.

5.6.2 Proxy transparent

Ce type de proxy fonctionne comme un routeur et filtre comme un serveur proxy, c'est à dire qu'il n'y aucune configuration à faire de la part de l'utilisateur, il s'intercale en réalité entre le périphérique et le modem routeur obligeant tout le trafic à passer par lui.

Il peut être très utile en entreprise que ce soit en termes de sécurité pour filtrer l'accès vers certaines applications web tel que des chat en ligne ou vers des échanges peer2peer ou bien en terme de performance en mettant en cache les pages déjà visités. Mais cette pratique force donc les utilisateurs à l'utiliser sans le savoir et évidemment elle peut être utilisé à des fins pas très morale comme pour les fliquer, l'anonymat n'est donc pas garanti avec ce type de proxy.

5.6.3 Proxy anonyme

Ces types de proxy ne se présente pas comme un serveur proxy standard vers le site ou application finale, mais comme un ordinateur normal. Il permet de contourner les restrictions imposées par certains sites ou applications vis-à-vis de ces derniers, notamment en les bloquant. Il assure également l'anonymat en éliminant les cookies et autres traqueurs indésirables.

5.6.4 Proxy inverse

Ce type de proxy, au contraire des autres proxys, ne s'installe pas du côté client, mais du côté serveur, il agit notamment comme intermédiaire de sécurité. Cette technique empêche les interventions tierces sur une application en les redirigeant vers un serveur plus sur par exemple.

5.6.5 Proxy SOCKS

Ce type de proxy est considéré comme une application et permet d'utiliser les services d'un pare-feu dans un échange entre un client et un serveur, ce processus de sécurité permet d'une certaine manière d'être anonyme sur internet, ce type de proxy est notamment utilisé avec les services cachés que propose le réseau Tor.

Tableau 4 : Principales différences entre VPN et Proxy

VPN	Proxy
Adresse IP cachée	Adresse IP cachée
Toute la connexion internet sur le PC est crypté et sécurisé	Doit être configuré individuellement pour chaque application
Les données sont également cryptées pendant leurs transferts	Les données ne sont pas cryptées pendant leurs transferts
Plus lent	Plus rapide

5.7 Réseaux anonymes

Les réseaux anonymes sont des systèmes de communications anonymes caractérisés par des applications distribuées entre clients dans lesquelles toutes les parties sont anonymes, l'anonymat s'obtient à l'aide de technique de surcouche logicielle ou de réseau de superposition. L'intérêt de cet outil est d'empêcher l'analyse et la surveillance du trafic, ce sont des logiciels généralement open-source accessible au grand public et qui ont de plus en plus la côte auprès des utilisateurs préoccupés par la surveillance massive notamment.

Ces réseaux tentent de garder une connexion anonyme lors d'une navigation en dirigeant le trafic vers un réseau mondial de relais et de nœuds et agissent donc sur des technologies et infrastructures existantes (Internet).

5.7.1 Freenet

Freenet est un logiciel libre qui permet d'accéder au réseau du même nom qui est un réseau autonome anonyme distribué le plus ancien avec pour objectif d'assurer la sécurité et l'anonymat à chacun, sa première version a été publiée en mars 2000. Freenet est décentralisé afin de la rendre moins vulnérable aux attaques et permet d'utiliser de façon anonyme les différents services proposés au sein de son propre réseau, il n'est donc pas possible de se connecter à des services comme Facebook ou Google avec Freenet.

5.7.1.1 Historique

Freenet a vu le jour à l'université d'Edimbourg, en 1999 un étudiant nommée Ian Clarke proposa un rapport inédit qui a servi de base à la construction du projet Freenet, ce rapport intitulé "A distributed decentralized information storage and retrieval system" avait pour objectif d'offrir la liberté de parole et une forte anonymisation sur internet.

Freenet est en développement continue depuis 2000, il a toujours été un logiciel open source et de nombreuses versions continuent d'être publié pour l'améliorer. Sa mise à jour la plus célèbre consiste à avoir mis en place un mode darknet (réseau invisible) : transforme Freenet en un réseau privé réservé aux amis, c'est à dire que les utilisateurs se connectent seulement à leurs amis, ce qui devient difficilement détectable.

5.7.1.2 De quoi s'agit-il concrètement ?

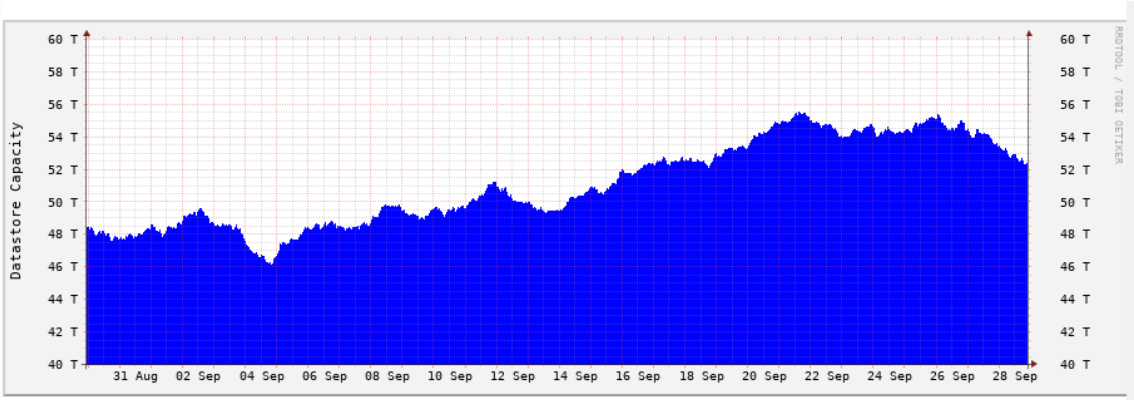
Le réseau est en réalité un espace de stockage partagé et distribué ou les ressources sont dispersés sur différentes machines à travers le monde, c'est fondamentalement un système de distribution de fichiers. Elle est utilisée pour la publication de sites web, la communication en ligne, le partage de fichiers, forums, courrier électronique, tout ceci

dans l'anonymat, en effet les communications sont chiffrées et acheminées via plusieurs nœuds dans le but de rendre difficile l'identification d'un utilisateur qui demande de l'information et du contenu.

Freenet est très différent des autres réseaux, plutôt que d'essayer de couvrir les flux de trafic entres les deux extrémités, un client et un serveur par exemple, les données sont-elles même découpées en blocs chiffrés et distribuées sur les magasins de données des autres utilisateurs afin d'en assurer la pérennité notamment. Les utilisateurs contribuent au réseau en donnant de la bande passante et une partie de la mémoire de leur disque dur, qui sera donc nommé magasin de données, afin de stocker des fichiers chiffrés, ils agissent donc tous comme des nœuds.

Donc pendant le processus de téléchargement, lorsqu'un utilisateur décide d'envoyer sur le réseau un fichier, ce fichier sera divisé en morceaux et stockés de manière chiffrés sur d'autres ordinateurs du réseau, et à l'inverse lorsqu'un utilisateur veut acquérir un fichier, les morceaux seront simplement trouvés et réassemblés. Contrairement aux systèmes de partage de fichier standard, pour l'utilisateur qui a envoyé sur le réseau un fichier il n'est pas nécessaire de rester connecter pour continuer de partager ce fichier. De cette manière, l'utilisateur qui veut télécharger un contenu spécifique n'aura pas besoin de se connecter directement au nœud qui l'a fourni à la base, la demande est donc acheminée sur plusieurs nœuds et donc de cette manière la liberté d'expression et l'anonymat sont garanties, car tout est décentralisé. Le contenu étant chiffré, il est impossible pour l'opérateur d'un nœud de déterminer ce qui est stocké sur son propre magasin de donnée, ce qui nous amène à une possibilité de refus plausible, c'est à dire qu'il est possible pour un nœud donc un utilisateur de nier l'existence d'un fichier chiffré sur son propre disque.

Tableau 5 : Capacité de stockage du réseau en TeraByte



(https://www.asksteved.com/stats/)

5.7.1.3 Darknet et Opennet

Pour se connecter au réseau Freenet, il existe deux façons définis par deux modes qui peuvent fonctionner simultanément ou individuellement, le premier mode est non sécurisé il ira automatiquement chercher les nœuds auxquels se connecter, on dit qu'il est non sécurisé car les nœuds sont étrangers et ne peuvent peut être pas être digne de confiance même si les données qui transitent sont cryptées, puis il y le mode invisible qui ira chercher des nœuds gérés par des utilisateurs connus, donc des amis, pour renforcer encore un peu plus cette sécurité il est préférable de réellement connaître ces personnes.

5.7.2 I2P (Invisible Internet Project)

I2P signifie "Le projet Internet invisible" dont l'objectif principale est l'anonymat, c'est un réseau isolé des autres réseaux et agit en tant que réseau superposé aux infrastructures internet existantes. Ce réseau anonyme peut donc être utilisé pour créer des services web anonymes : blog, forum, stockage de fichier décentralisé, courriel, SSH, proxys sortant…

Dans I2P, les utilisateurs peuvent contrôler le niveau de sécurité, l'anonymat, la bande passante pour répondre à leurs besoins spécifiques. Ce qui garantit l'anonymat avec I2P est le fait que l'expéditeur et le destinataire ne communiquent jamais directement, mais via plusieurs routeurs nommé tunnels.

5.7.2.1 Historique

Le projet a démarré en 2003 grâce à un groupe de volontaires, I2P est une version bêta depuis le début de son développement notamment à cause du manque d'utilisateurs, les développeurs ont affirmé être malheureusement encore à la recherche d'une version stable.

5.7.2.2 De quoi s'agit-il concrètement ?

C'est donc un réseau anonyme décentralisé, à la base le projet I2P a été conçu à partir du concept de Freenet, c'est à dire que c'est un réseau ou tous les ordinateurs se connecte entre eux et sont totalement isolés du reste du réseau internet standard, toutes les connexions passent à travers des tunnels chiffrés et plutôt que d'utiliser des adresse IP, ce sont en réalité des clés (à partir de clés asymétriques) qui seront utilisés pour la communications.

Tous les ordinateurs du réseau sont donc les nœuds et sont considérés comme des routeurs, de ce fait chacun envoie et reçoit une multitude de message, ces messages peuvent donc être dirigé vers ou en provenance de l'utilisateur qui gère le routeur en

question, mais dans la plupart des cas, les messages ne feront que transiter vers d'autres points qui seront finalement presque impossible à identifier.

Les principes pour la communication entre deux utilisateurs est plutôt complexe mais très efficace pour assurant un haut degré d'anonymat, pour ce faire I2P construit des tunnels temporaires virtuels passant par un multitude de routeurs, la longueur et donc le nombre de routeurs peut être défini par les clients I2P, le choix du nombre aura un effet important sur la latence, le débit, et l'anonymat, en effet moins il y a de routeurs dans le tunnel plus le risque de voir son anonymat brisé est grand car une attaque par analyse de trafic devient plus facile. Tous les clients (et routeurs en même temps) possèdent un tunnel sortant et un tunnel entrant, par exemple lorsqu'un utilisateur désire envoyer un message à un autre, il lui faudra d'abord l'envoyer à l'un de ses propres tunnels sortants avec des instructions sur le point final du tunnel fait de plusieurs routeurs, pour le transmettre ensuite au tunnel entrant de l'utilisateur destinataire. Dans les sens inverse le groupe de routeurs pour acheminer le message ne sera pas le même, les tunnels changent constamment pour éviter de se faire espionner. Pour contrer différentes attaques, les messages sont cryptés, et avec i2P le principe est de mettre dans un paquet plusieurs messages pour compliquer la tâche d'un observateur potentiel, cette technique se nomme "Garlic Routing".

Figure 13 : Fonctionnement du tunnel I2P

(https://geti2p.net/fr/docs/how/tunnel-routing)

A: Passerelle sortante (Alice)

B: Participant sortant

C: Point terminal sortant

D: Passerelle entrante

E: Participant entrant

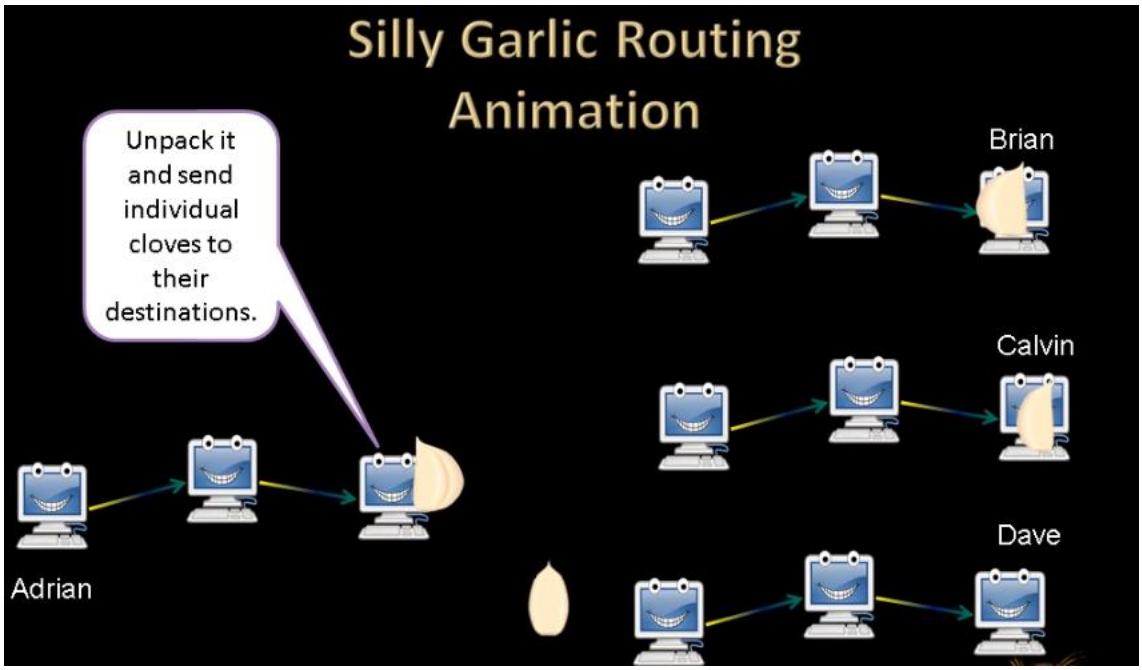
F: Point final entrant (Bob)

5.7.2.3 Garlic Routing – routage en ail

Le principe du routage en ail est de chiffrer plusieurs messages ensemble et de les faire circuler dans le même paquet, cela permet d'une part d'accélérer la vitesse de transfert mais également rendre plus difficile l'analyse du trafic, le routage en oignon qui sera décrit dans la section « Tor » permet de créer un tunnel ou chemin avec plusieurs routeurs, le routage en ail consiste à regrouper plusieurs message et leurs instructions en un seul block, ces messages ne seront exposés qu'une fois arrivé au bout du tunnel.

Voici le principe illustré, une fois arrivé au bout du tunnel (sortant dans l'exemple) la gousse d'ail se décompose pour que chaque message puisse rejoindre sa destination :

Figure 14 : Principe du routage en ail



(https://www.youtube.com/watch?v=NV90TRs_pGE)

5.7.3 Tor

Le réseau Tor est à l'origine un moyen de rendre anonyme sa connexion pour un accès sur les sites web standard ou ceux de son propre réseau : les services cachés. Fondamentalement, il agit comme un réseau superposé au réseau internet standard en utilisant des serveurs décentralisés appelés nœuds. Ce dernier a pour objectif de rendre confidentiel les applications basées TCP en anonymisant le flux, toutefois l'anonymisation total n'est pas garantie si l'application utilisés collecte des informations, c'est pourquoi il existe un navigateur dédié développé par le projet Tor.

5.7.3.1 Historique

Le principe du routage par couche ou routage en oignon fut inventée dans les années 1990 par des collaborateurs du laboratoire de recherche navale des Etats-Unis pour objectif de protéger les communications du renseignement américain. Plusieurs versions ont vu le jour avec à chaque fois des noms différents et la première publication publique aura lieu en 2003 sous le nom de Tor Project. En 2004, le laboratoire de recherche navale annonce qu'elle publiera dorénavant le code pour Tor sous licence libre. Dès ses débuts, le projet Tor trouve de nombreux partisans financiers décidé à financer le projet, notamment Human Rights Watch, l'université de Cambridge, Google et certains entités gouvernementales américaines.

Le projet Tor s'est retrouvé dans la tourmente plus d'une fois notamment en novembre 2014 après l'opération conjointe Onymous menée par le FBI et Europol, en effet un certain nombre de site ont été fermés, notamment des sites de contrebandes et de blanchiment d'argent, suite à ça, une spéculation selon laquelle une vulnérabilité 0-day aurait été exploitée vue le jour, néanmoins un représentant du projet a démenti ces spéculations en affirmant qu'elles étaient exagérées et que l'impression données par ces entités policières comme quoi le système fut "hacker" étaient fausses, cependant les vecteurs d'attaques utilisés ne sont pas encore clair pour la communauté Tor, certaines pistes affirment que certains relais Tor aurait été saisis et exploités par cette coalition gouvernementale, d'autres voient une désanonymisation Bitcoin qui aurait permis de lier les transactions et connaître les réelles identité des clients Bitcoin.

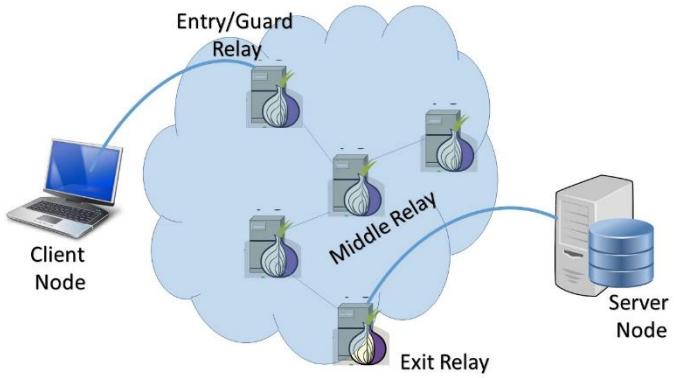
Aujourd'hui le réseau peut compter sur une grande communauté de développeurs, de chercheurs et d'utilisateurs qui luttent chaque jour pour la protection de la vie privée et la liberté en ligne, il est devenu plus qu'un simple logiciel.

5.7.3.2 De quoi s'agit-il concrètement ?

Concrètement, lorsqu'un utilisateur se connecte à un site web sur le réseau internet normal, il échange avec ce dernier des paquets TCP (Transmission Control Protocole), les données qui transitent via ces paquets peuvent ou non être chiffrées, notamment via les protocoles HTTP et HTTPS. Il est théoriquement possible de surveiller une connexion internet et lire le contenu des paquets TCP, soit par un intermédiaire soit par une attaque de type Man In The Middle, donc l'adresse IP , le site web visité et le port auquel la connexion est établie peuvent être révélés et subtilisés, si une connexion sécurisé via HTTPS est établie le contenu du site visité ne sera pas lisible, mais le nom de domaine visité et généralement l'adresse IP pourront toujours être lisible ce qui compromet toute confidentialité.

En utilisant Tor, le principe de base est de ne jamais établir une connexion directe entre un ordinateur et un serveur afin de préserver l'anonymat. Pour ce faire, les messages de routages sont encapsulés dans plusieurs couches de cryptage, d'où l'appellation routage en oignon, puis elles transitent jusqu'au destinataire.

Figure 15 : Circuit Tor standard



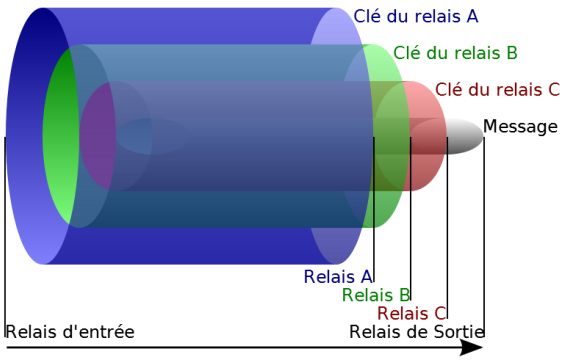
(https://medium.com/coinmonks/tor-nodes-explained-580808c29e2d)

5.7.3.3 Principe Routage Oignon

Le principe du routage oignon consiste à utiliser plusieurs relais pour acheminer une requête d'un point A jusqu'au point B, ce chemin est nommé circuit.

Lorsqu'une requête est envoyée à travers le circuit vers le destinataire, cette dernière est chiffrée autant de fois qu'il y a de nœuds dans le chemin grâce à un système cryptographique à clé symétrique, s'il y a 5 nœuds la requête aura alors 5 couches de cryptage au départ. Puis le message envoyé sera décodé au fur et à mesure qu'il passe entre les différents relais pour que finalement le destinataire puisse lire le message totalement déchiffré.

Figure 16 : Principe du routage Oignon



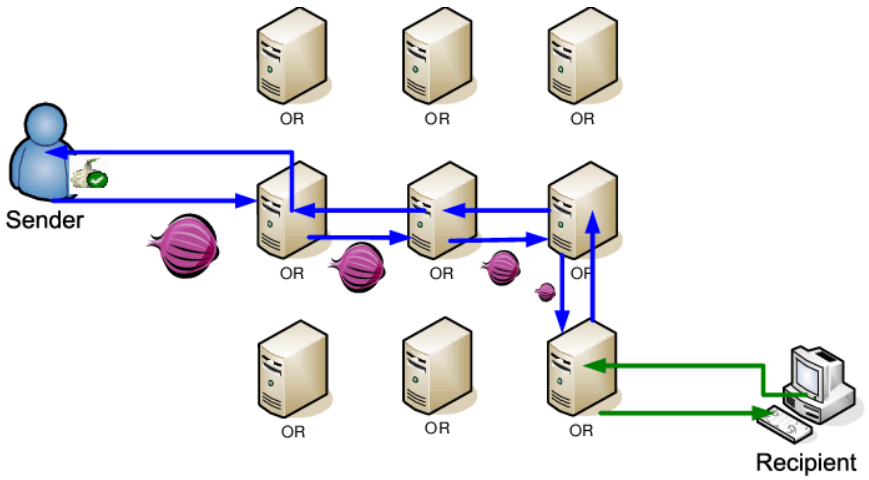
(https://openclassrooms.com/fr/courses/2939276-surfez-incognito-sur-internet-avec-le-reseau-tor/2955001-tor-et-le-routage-en-oignon)

Concrètement on peut comparer ce principe aux poupées russes ou à un coffre-fort, lorsqu'on désire envoyer un message à Bob en passant par plusieurs relais, le message sera placé dans plusieurs coffres selon le nombre de relais utilisé (donc chiffrez plusieurs fois), une fois arrivée au premier relais ce dernier supprimera la première couche avec sa clé de chiffrement que seul lui connait, à ce niveau-là il n'est toujours pas possible de lire le contenu du message étant donnée qu'il a encore autant de couches de chiffrement que de relais nécessaire pour arriver à destination, au fur et à mesure que le message se déplace les couches se retirent, les relais intermédiaires n'ont aucune connaissance du contenu du message, ils sont simplement en mesure de dire qui leurs a envoyé le message et à qui il faut le renvoyer.

Finalement le message lisible sera transféré vers le destinataire par le dernier nœud après avoir déchiffré la dernière couche, il connaît donc le destinataire et le contenu du message mais pas celui qui a envoyé le message ni le nombre de couches qui ont été nécessaire pour acheminer le message.

Dans le sens inverse, le destinataire renvoie la réponse au dernier relais qui se chargera d'ajouter la première couche de chiffrement, ce dernier nœud connaît uniquement le nœud auquel doit être acheminer la réponse, c'est à dire l'avant dernier nœud qui lui-même ajoutera une couche de chiffrement supplémentaire et ainsi de suite jusqu'à arriver au premier nœud, ce dernier étant le seul à connaître l'origine du message et donc celui à qui la réponse doit être livrée, à cette étape la réponse est entièrement chiffré et il ne reste plus qu'à utiliser les clés symétriques pour décrypter la réponse et la transmettre sans plus aucune couche de chiffrement.

Figure 17 : Empilement et dépilement des messages via le principe du routage en oignon



(https://www.researchgate.net/figure/An-overview-of-how-Tor-works-Client-establishes-a-path-of-onion-routers-and-sends_fig3_4377386)

5.7.3.4 Comment le circuit est créé ?

Le circuit que vont emprunter les paquets TCP sera définit par le client Tor pour chaque nouveau circuit, la première étape sera de choisir le nœud de sortie suivie des autres nœuds nécessaire dans le circuit, généralement les nœuds intermédiaires sont au nombre de 3, ajouter des nœuds supplémentaires n'augmente pas la sécurité, en effet si le premier et le dernier nœud sont contrôlés par des espions cela n'augmentera pas la sécurité, elle sera même compromise.

Lorsque Tor choisit le nœud de sortie, il se base sur certains principes :

- Tout d'abord Tor ira voir dans le fichier de configuration du client afin de consulter les paramètres de géolocalisation, il est possible pour l'utilisateur de créer une liste noire de géolocalisation qui empêchera d'utiliser un nœud de sortie pour un certain pays.
- Tor choisira uniquement un nœud de sorti permettant de sortir du réseau Tor, par exemple certains nœuds ne laissent passer que le trafic web (HTTP /port 80) ce qui n'est pas très utile quand on veut envoyer des mails (SMTP port 25).
- Le nœud de sortie doit avoir assez de ressources disponibles pour vous supporter.

Lorsque Tor choisit les nœuds d'entrées et les nœuds intermédiaires, il se base sur ces critères :

- Tor ne choisit pas le même routeur deux fois pour le même chemin
- Tor ne choisit qu'un seul routeur d'une même famille, deux routeurs sont de la même famille s'ils sont exploités et déclarés par le même opérateur
- Pas plus d'un routeur dans un sous-réseau
- Tor ne choisit pas de relais non-actif ou non-valide, non actif signifie que le routeur en question n'est pas en ligne, non valide signifie que la configuration du routeur est incorrecte
- Le premier nœud doit être un nœud de garde

5.7.3.4.1 Noeud de garde

Le nœud de garde est un nœud privilégié car il est un point d'entrée pour le réseau Tor, chaque client qui souhaite se connecter au réseau Tor doit passer par ce dernier, c'est un point sensible car il est capable de voir la véritable adresse IP de l'utilisateur (véritable

sauf utilisation de VPN ou Proxy en combinaison), si une organisation malveillante exploite un nœud d'entrée elle pourra observer la navigation de sa victime.

Il est possible de consulter la liste des relais d'entrée sur le site de Tor.

5.7.3.4.2 Noeud intermédiaire

Les nœuds intermédiaires représentent la majeure partie d'un circuit Tor, ils agissent simplement comme des relais et font transiter les données cryptées vers d'autres nœuds, ils ne connaissent que leur prédécesseur et leur descendant et ne sont pas tenu responsable s'il transmet du trafic malveillant, car il n'est ni la source ni la destination finale du trafic, ces nœuds sont donc entre les nœuds d'entrée et les nœuds de sorties.

5.7.3.4.3 Noeud de sortie

Le nœud de sortie est le dernier relais du réseau Tor, il agit en tant que point de sortie et envoie les données au destinataire, l'adresse IP de ce dernier est visible par le destinataire et est donc perçu comme étant à l'origine du trafic, si donc le trafic de sortie vers le destinataire n'est pas crypté il pourra être utilisé de manière abusive. Voici deux exemples simples :

- Si HTTPS n'est pas utilisé entre le nœud de sortie et le destinataire, le cookie, les identifiants, les messages, le contenu pourront être capturés.
- Si un email est envoyé en utilisant SMTP (pas de TLS), l'email pourrait être capturé.

5.7.3.4.4 Noeud d'annuaire

Ces nœuds gèrent une liste des relais en cours d'exécution, concrètement le réseau est suivi et rendu public par un groupe de serveurs appelés nœuds d'annuaire, chacun est contrôlé par une organisation, l'intégrité du réseau repose donc sur l'honnêteté et de ces listes. Ces listes sont maintenues quotidiennement, les différents nœuds publient un consensus : un document unique compilé et voté par chaque nœud du répertoire. Cela garantit l'exactitude des informations vis-à-vis des clients.

5.7.3.4.5 Noeud pont

Les nœuds pont sont destinées aux utilisateurs se trouvant dans un pays répressif ou internet est censuré, comme vu au-dessus et étant donné que la liste est publique, il suffit d'utiliser l'annuaire de nœuds pour bloquer l'accès à Tor, un état peut bloquer le trafic vers un nœud spécifique en utilisant son adresse IP. C'est pourquoi les nœuds de pont ont vus le jour, les utilisateurs envoie leur trafic vers ces ponts qui agissent comme

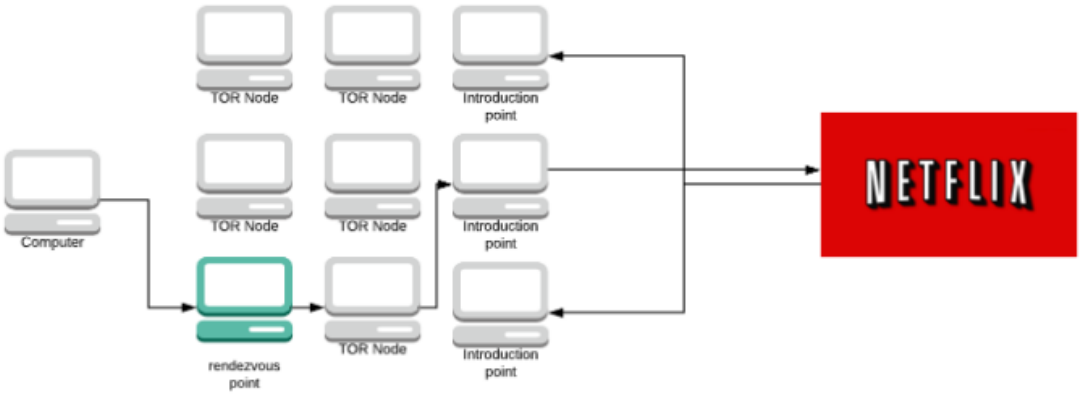
des proxys et transfèrent ensuite le trafic vers un nœud de garde. La liste des nœuds pont n'est pas publique ce qui empêche les états de les bloquer.

5.7.3.5 Services cachés

Les services cachés Tor sont les sites web accessible uniquement via le réseau Tor, ces sites web sont en réalité des serveurs ordinaires communiquant avec un client, toutefois ces services ont la particularité de communiquer sans que les deux parties connaissent l'identité de l'autre.

Pour ce faire, le serveur doit être déclaré en tant que service caché, ce dernier aura besoin de sélectionner d'autres routeurs pour qu'ils agissent en tant que point d'introduction au service caché. Les points d'introductions servent à présenter les utilisateurs au service, mais ne permettent pas d'accéder directement au service, en effet une fois le point d'introduction établie, Tor choisit un routeur au hasard qui fera office de point de rendez-vous et c'est par ce routeur que la communication entre le client et le serveur se fera. Voici un schéma qui illustre cela, ici NetFlix fait office de service caché pour l'exemple :

Figure 18 : Service caché



(https://skerritt.blog/how-does-tor-really-work/#tor-hidden-services-)

6. Service collaboratif anonyme sur Tor

6.1 Objectif

L'objectif premier est de proposer un outil collaboratif sur le réseau Tor afin de permettre aux potentielles utilisateurs de bénéficier d'un anonymat total vis-à-vis des différentes technologies. D'une part les utilisateurs ne pourront pas être suivi en utilisant ce service, de plus la garantie de contrôler leurs données est assurée. Il est ouvert à quiconque nécessitant une collaboration anonyme avec d'autres utilisateurs, il leurs assure un service libre respectueux de la vie privée/professionnel.

6.2 Motivations

Ma plus grande motivation est de créer un service assurant à ses utilisateurs un anonymat proche du 100%, pour ce faire le réseau Tor me semble être la meilleure option, il offre une solution très efficace en termes d'anonymat et de performance, il est surtout accessible par un plus large public, que ce soit en Chine en Turquie ou tout autre pays répressif, sa notoriété semble grandir. La compréhension des outils assurant l'anonymat sur internet et leurs applications sont des connaissances que tout internaute devrait maitriser au vu de la transformation de ce monde ou le contrôle de nos données personnelles semblent nous avoir échappé, et où tous les moindre fait et gestes semblent être surveillé.

6.3 Le service

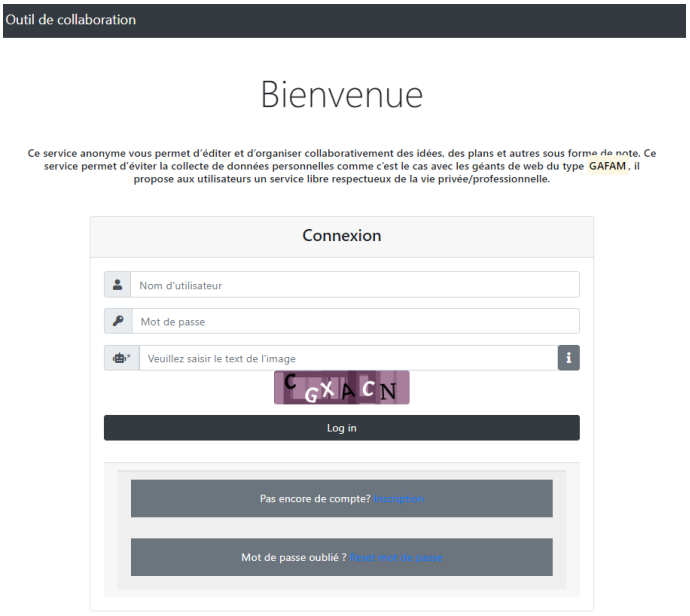
Dans sa première version, le service permet d'éditer et d'organiser collaborativement des idées, des plans et autres sous forme de note, il permet à un utilisateur enregistré d'inviter à collaborer d'autres utilisateurs pour partager un document, ce document peut s'apparenter à un document word comme on peut le faire en utilisant le service de GoogleWord par exemple. Le service ne garde en mémoire que le stricte nécessaire, il n'y a ni traqueurs, ni cookies et la nature du réseau Tor ne permet pas de tracer quiconque.

6.3.1 Description des pages et fonctionnalités

- Page d'accueil et identification utilisateur

L'identification des utilisateurs ne requiert pas d'adresse email, lors de l'inscription seul un nom d'utilisateur le mot de passe et un code PIN est demandé, le code PIN sert à modifier son mot de passe en cas d'oubli. Pour des raisons de sécurité, un captcha est également demandé.

Figure 19 : Service : page d'accueil et d'identification

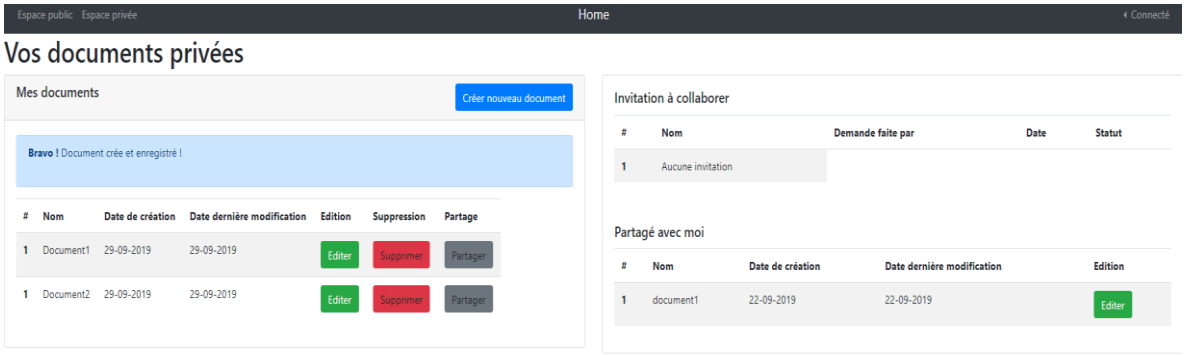


(nyuma6poeaiut43mp5a5l45av5uxhbxgj7dwmd5h5ueahnwyztiff2qd.onion)

- Espace privé

L'espace privée permet à chaque utilisateur d'avoir une vue globale sur ses documents, il a la possibilité de créer, éditer, supprimer un document et de le partager, il a également possibilité de gérer les invitations à collaborer qui lui sont soumises. Finalement une fois les invitations acceptées il sera invité à éditer des documents d'autres utilisateurs.

Figure 20 : Service : page espace privé

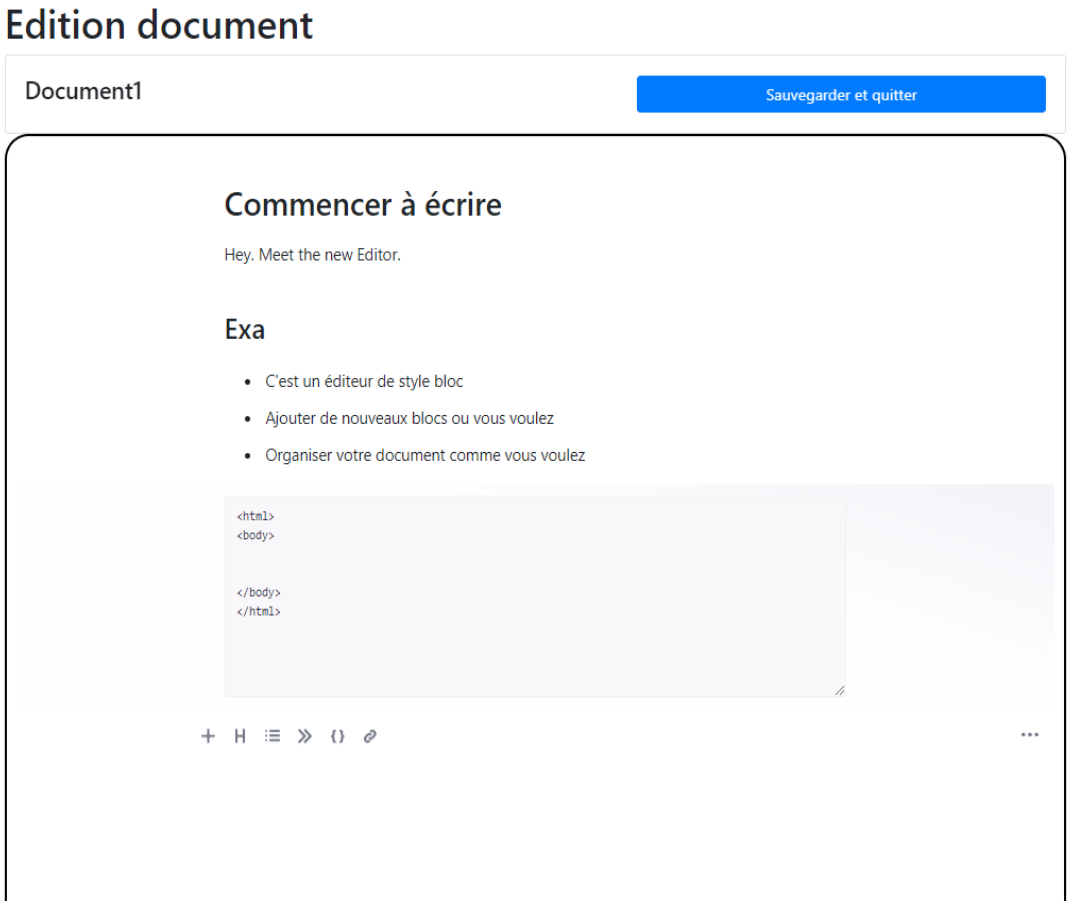


(nyuma6poeaiut43mp5a5l45av5uxhbxgj7dwmd5h5ueahnwyztiff2qd.onion)

- Edition de document

La fonction d'édition de document permet d'insérer plusieurs éléments pour former des notes, les éléments disponibles sont les liens, les paragraphes, les citations, les entêtes, les listes et des zones de texte avec un format particulier pour le code.

Figure 21 : Service : page édition de document

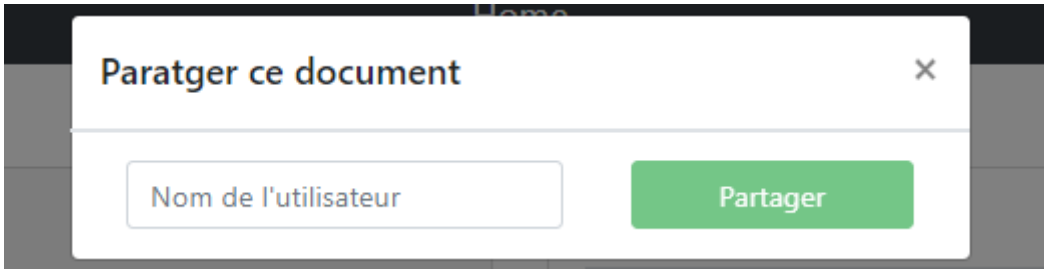


(nyuma6poeaiut43mp5a5l45av5uxhbxgj7dwmd5h5ueahnwyztiff2qd.onion)

- Invitation à collaborer

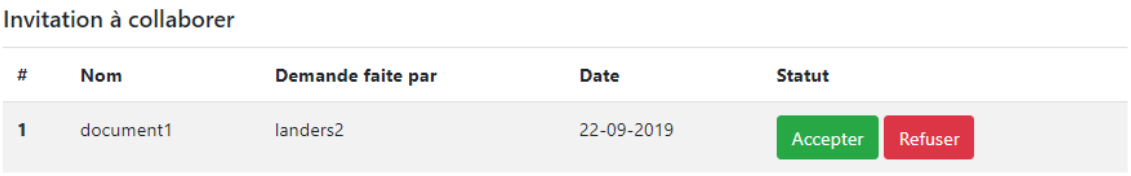
Pour qu'un utilisateur puisse inviter un autre utilisateur à collaborer sur un document, il doit impérativement connaitre son nom d'utilisateur, la collaboration ne pourra débuter qu'une fois l'invitation acceptée.

Figure 22 : Service : partager un document



(nyuma6poeaiut43mp5a5l45av5uxhbxgj7dwmd5h5ueahnwyztiff2qd.onion)

Figure 23 : Service : invitations à collaborer



(nyuma6poeaiut43mp5a5l45av5uxhbxgj7dwmd5h5ueahnwyztiff2qd.onion)

6.3.2 Caractéristiques techniques

6.3.2.1 Configuration et déploiement du service Tor

Les outils et technologies utilisés dans la conception du service sont tous open-source.

6.3.2.1.1 Configuration de service Tor

Tout d'abord il faut installer le logiciel Tor depuis le site officiel, ce dernier fonctionne en tant que proxy, son principe consiste à écouter le trafic dédié à Tor sur un port définit, ensuite le trafic est acheminé vers le port du service caché (serveur web local). Les adresses IP et les ports écoutés doivent être spécifiés dans le fichier de configuration de Tor.

Une fois le logiciel installé, il faut le configurer via son fichier de configuration nommé « torrc » afin d'activer le service. La configuration consiste d'abord à indiquer le chemin

d'accès sur site web local puis l'endroit vers ou les connexions venant de l'extérieur doivent être acheminées. Dans la configuration ci-dessous, les demandes venant de l'extérieure seront redirigé sur le port 80 (dédié au web) à l'adresse 127.0.0.1 :80

Figure 24 : Configuration service Tor

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

(Capture d'écran fichier torrc)

Jusqu'ici le service n'est pas encore activé, une fois que le fichier de configuration est enregistré il faut redémarrer Tor. Lorsque Tor démarre, il va créer deux fichiers dans le répertoire associé au service caché :

- private_key

Ce fichier contient la nouvelle clé privée du service, elle est liée mathématiquement à la clé publique, la clé publique consiste à chiffrer les données, la clé privée consiste à déchiffrer les données, ce qui signifie que je suis le seul à pouvoir déchiffrer les données pour mon service avec la clé privée et qu'il est important de la protéger.

- hostname

L'autre fichier nommé hostname contient la clé publique, dans mon cas la clé publique est la suivante : nyuma6poeaiut43mp5a5l45av5uxhbxgj7dwmd5h5ueahnwyztiff2qd. Cette clé publique devient également le nom d'hôte de mon service en y ajoutant à la fin « .onion ». Cette clé est à partager afin d'atteindre le service via le réseau Tor, dans mon cas, l'utilisation de la récente version de Tor a généré une clé de 56 caractères pour plus de sécurité, contrairement aux versions précédentes ou les clés faisaient 16 caractères.

6.3.2.1.2 Configuration serveur web apache

La configuration du serveur web nécessite de modifier le port d'écoute d'Apache, pour le service caché l'adresse se limite à 127.0.0.1. De plus il faut ajouter l'adresse du service à 56 caractères sous l'attribut « ServerName » du fichier de configuration pour qu'Apache puisse le reconnaitre.

Figure 25 : Port d'écoute du serveur web

```
Listen 127.0.0.1:80
```

(Capture d'écran fichier de configuration serveur apache)

Figure 26 : ServerName Apache

```
ServerName nyuma6poeaiut43mp5a5l45av5uxhbxgj7dwmd5h5ueahnwyztiff2qd.onion
```

(Capture d'écran fichier de configuration serveur apache)

Une fois ces étapes réalisées et le site par défaut activé, il est nécessaire de redémarrer le serveur. Une fois redémarré, le lien entre le service caché et le logiciel Tor sera établie et donc le service devient disponible via l'adresse publique et TorBrowser.

6.3.2.2 Environnement global

- OS : Linux Debian Strech – sur VMWare
- Serveur web : Apache 2.4.25
- Base de données : MariaDB 15.1
- Langage de programmation : PHP 7.0
- Tor 0.4.1.5

6.3.2.3 Code source

https://github.com/Aajdini/TDB_Anonymat

6.3.2.4 Nom de domaine

nyuma6poeaiut43mp5a5l45av5uxhbxgj7dwmd5h5ueahnwyztiff2qd.onion

QRcode, pratique si vous utilisez TorBrowser sur votre téléphone mobile :

Figure 27 : Service : QR code nom de domaine

7. Conclusion

7.1 Synthèse sur le travail

Dans ce document nous avons défini ce qu'est l'anonymat et ses enjeux dans notre société, le première chose mise en évidence est que les infrastructures internet ne permettent pas par nature d'assurer l'anonymat des internautes, les technologies et les protocoles qui font qu'internet est ce qu'il est, ne peuvent pas assurer la non traçabilité des internautes.

Les géants du web ont fait des données personnelles des internautes leurs business, c'est pourquoi ils cherchent absolument à collecter un maximum d'informations sur leurs utilisateurs, de plus internet est devenu une place très surveillée que ce soit par des états ou des services de renseignements, il est donc difficile d'utiliser son droit à l'anonymat dans ce contexte.

Nous explorons à travers ce document les outils et techniques qui mettent en danger l'anonymat, on constate qu'il y en beaucoup et qu'ils sont devenus légion. Se cacher derrière un pseudo sur internet par exemple, ne suffit pas à être anonyme, mais heureusement il existe de nombreux moyens qui permettent de cacher ses traces et de rendre l'identification des utilisateurs difficile voir presque impossible, ce document décrit donc également certains outils qui favorisent l'anonymat.

Finalement, la conception d'un service anonyme via des technologies permettant un très haut degré d'anonymat vient concrétiser ce travail en offrant une solution évitant à ses potentielles utilisateurs d'être identifiés.

7.2 Point de vue personnel

Internet s'est rapidement placé au cœur de notre système et à complétement changer la face de ce monde, il est devenu le moyen de communication par excellence, on peut dire qu'il a d'une certaine manière redéfinit les frontières en les supprimant.

Ses services en tout genre apportent des avantages considérables à notre société, malgré ça, internet et son emprise deviennent un réel danger pour le monde, les droits les plus élémentaires tels que la liberté d'expression, le droit à la vie privée sont bafoués, les données partagées par les internautes sont des traces indélébiles et leurs contrôles perdus.

L’idée de se protéger devient donc primordiale, malheureusement la majorité des internautes ne réalisent pas que les droits appliquer dans les vraies vies doivent également l’être sur internet, de plus le manque de connaissance joue également son rôle et il faut le préciser, à l’heure actuelle, être réellement anonyme et se protéger sur internet requiert des connaissances pointues.

L’anonymat sur internet est donc, à mes yeux, conditionnel, et n’est de toute façon jamais garantie à 100%, il est toutefois possible de s’en approcher de très près. Etant de nature discret et pas enregistré sur les réseaux sociaux, mes données personnelles sont précieuses et les partager devient une opération risquée, ce travail vient confirmer mes inquiétudes, mais heureusement de plus en plus de gens s’appliquent à rendre internet plus sûr en terme d’anonymat et de confidentialité.

Bibliographie

ANON., 2012a. DOSSIER – L'ANONYMAT DANS L'HISTOIRE. In : [en ligne]. 23 juin 2012. [Consulté le 8 juillet 2019]. Disponible à l'adresse : https://voxlemag.wordpress.com/numero-2-lanonymat-dans-lhistoire/dossier-lanonymat-dans-lhistoire/

ANON., 2012b. What are Tracking Pixels Used For and How do They Work? In : *Skillcrush* [en ligne]. 19 juillet 2012. [Consulté le 15 août 2019]. Disponible à l'adresse : https://skillcrush.com/2012/07/19/tracking-pixel/

ANON., 2014. Comment maîtriser ses traces numériques ? In : *Reputation VIP* [en ligne]. 5 mai 2014. [Consulté le 29 juillet 2019]. Disponible à l'adresse : https://www.reputationvip.com/fr/blog/comment-maitriser-ses-traces-numeriques

ANON., 2016. Je suis anonyme quand j'utilise un VPN - 10 mythes réduits en miettes | Golden Frog. In : *Golden Frog Blog* [en ligne]. 13 juin 2016. [Consulté le 20 août 2019]. Disponible à l'adresse : https://www.goldenfrog.com/blog/fr/myths-about-vpn-logging-and-anonymity

ANON., 2018a. 51 Best Privacy Tools for Complete Digital Privacy Online and Offline. In : *Deep web links | Deep web sites | The Deepweb 2018* [en ligne]. 16 février 2018. [Consulté le 25 août 2019]. Disponible à l'adresse : https://www.deepwebsiteslinks.com/best-privacy-tools/

ANON., 2018b. Cookies, mouchards : comment vous êtes suivis sur Internet. In : *Le Monde.fr* [en ligne]. 30 mars 2018. [Consulté le 30 juillet 2019]. Disponible à l'adresse : https://www.lemonde.fr/les-decodeurs/article/2018/03/30/cookies-mouchards-comment-vous-etes-suivis-sur-internet_5278722_4355770.html

ANON., 2018c. First-Party & Third-Party Cookies: What's the Difference? - Clearcode Blog. In : *Clearcode | Custom AdTech and MarTech Development* [en ligne]. 2 novembre 2018. [Consulté le 25 juillet 2019]. Disponible à l'adresse : https://clearcode.cc/blog/difference-between-first-party-third-party-cookies/

ANON., 2018d. *Réseau superposé* [en ligne]. S.l. : s.n. [Consulté le 26 août 2019]. Disponible à l'adresse : https://fr.wikipedia.org/w/index.php?title=R%C3%A9seau_superpos%C3%A9&oldid=144268370

ANON., 2018e. Serveur Proxy : Présentation de 5 types de serveurs proxy. In : *Routeur-Wifi* [en ligne]. 29 novembre 2018. [Consulté le 30 septembre 2019]. Disponible à l'adresse : https://le-routeur-wifi.com/types-serveurs-proxy/

ANON., 2018f. Surfer anonymement - VPN, TOR, proxy | VPNconnexion.fr. In : *VPN Connexion* [en ligne]. 6 juillet 2018. [Consulté le 1 septembre 2019]. Disponible à l'adresse : https://www.vpnconnexion.fr/meilleur-vpn/surfer-anonymement/

ANON., 2018g. *Trace numérique* [en ligne]. S.l. : s.n. [Consulté le 12 juillet 2019]. Disponible à l'adresse : https://fr.wikipedia.org/w/index.php?title=Trace_num%C3%A9rique&oldid=154244047

ANON., 2019a. *Anonymat sur Internet* [en ligne]. S.l. : s.n. [Consulté le 8 juillet 2019]. Disponible à l'adresse : https://fr.wikipedia.org/w/index.php?title=Anonymat_sur_Internet&oldid=159313531

ANON., 2019b. *Anonymity* [en ligne]. S.l. : s.n. [Consulté le 8 juillet 2019]. Disponible à l'adresse : https://en.wikipedia.org/w/index.php?title=Anonymity&oldid=915234602

ANON., 2019c. *Cookie (informatique)* [en ligne]. S.l. : s.n. [Consulté le 18 juillet 2019]. Disponible à l'adresse : https://fr.wikipedia.org/w/index.php?title=Cookie_(informatique)&oldid=160229946

ANON., 2019d. *Disposable email address* [en ligne]. S.l. : s.n. [Consulté le 1 septembre 2019]. Disponible à l'adresse : https://en.wikipedia.org/w/index.php?title=Disposable_email_address&oldid=906431362

ANON., 2019e. *Freenet* [en ligne]. S.l. : s.n. [Consulté le 30 août 2019]. Disponible à l'adresse : https://fr.wikipedia.org/w/index.php?title=Freenet&oldid=157126703

ANON., 2019f. *P2P anonyme* [en ligne]. S.l. : s.n. [Consulté le 30 août 2019]. Disponible à l'adresse : https://fr.wikipedia.org/w/index.php?title=P2P_anonyme&oldid=160876023

ANON., 2019g. *Paternité des œuvres de Shakespeare* [en ligne]. S.l. : s.n. [Consulté le 15 septembre 2019]. Disponible à l'adresse : https://fr.wikipedia.org/w/index.php?title=Paternit%C3%A9_des_%C5%93uvres_de_Shakespeare&oldid=161619021

ANON., 2019h. *Proxy* [en ligne]. S.l. : s.n. [Consulté le 2 septembre 2019]. Disponible à l'adresse : https://fr.wikipedia.org/w/index.php?title=Proxy&oldid=163002799

ANON., 2019i. *Pseudonymat* [en ligne]. S.l. : s.n. [Consulté le 20 juillet 2019]. Disponible à l'adresse : https://fr.wikipedia.org/w/index.php?title=Pseudonymat&oldid=158034383

ANON., 2019j. Third-Party Cookies Vs First-Party Cookies. In : *Opentracker* [en ligne]. 1 mai 2019. [Consulté le 27 juillet 2019]. Disponible à l'adresse : https://www.opentracker.net/article/third-party-cookies-vs-first-party-cookies

ANON., 2019k. *Tor (réseau)* [en ligne]. S.l. : s.n. [Consulté le 2 septembre 2019]. Disponible à l'adresse : https://fr.wikipedia.org/w/index.php?title=Tor_(r%C3%A9seau)&oldid=162808478

ANON., [sans date]. 3 Undeniable Reasons Why You Need Online Anonymity. In : *MakeUseOf* [en ligne]. [Consulté le 11 juillet 2019 a]. Disponible à l'adresse : https://www.makeuseof.com/tag/3-undeniable-reasons-need-online-anonymity/

ANON., [sans date]. Anonymity on the Internet. In : [en ligne]. [Consulté le 9 juillet 2019 b]. Disponible à l'adresse : https://people.dsv.su.se/~jpalme/society/anonymity.html

ANON., [sans date]. Anonymity on the Internet Must be Protected. In : [en ligne]. [Consulté le 12 juillet 2019 c]. Disponible à l'adresse : http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall95-papers/rigby-anonymity.html

ANON., [sans date]. Anonymous Network - an overview | ScienceDirect Topics. In : [en ligne]. [Consulté le 12 juillet 2019 d]. Disponible à l'adresse : https://www.sciencedirect.com/topics/computer-science/anonymous-network

ANON., [sans date]. Best Anonymous Browsers For Private Web Browsing. In : [en ligne]. [Consulté le 2 septembre 2019 e]. Disponible à l'adresse : https://hackernoon.com/best-anonymous-browsers-for-private-web-browsing-27e8798607e2

ANON., [sans date]. Best Operating Systems for Anonymity: Comparing Titans. In : [en ligne]. [Consulté le 2 septembre 2019 f]. Disponible à l'adresse : https://hackernoon.com/best-operating-systems-for-anonymity-comparing-titans-3501fd5cba3b

ANON., [sans date]. Cookies Internet | Que sont-ils et que font-ils ? | Cookiebot. In : [en ligne]. [Consulté le 25 juillet 2019 g]. Disponible à l'adresse : https://www.cookiebot.com/fr/cookies-internet/

ANON., [sans date]. Cookies (internet). In : *CommentCaMarche* [en ligne]. [Consulté le 25 juillet 2019 h]. Disponible à l'adresse : https://www.commentcamarche.net/contents/1041-cookies-internet

ANON., [sans date]. Cookies, Tags and Pixels: Tracking Customer Engagement – Visual IQ. In : [en ligne]. [Consulté le 10 août 2019 i]. Disponible à l'adresse : https://www.visualiq.com/resources/marketing-attribution-newsletter-articles/cookies-tags-and-pixels-tracking-customer-engagement

ANON., [sans date]. Freenet. In : [en ligne]. [Consulté le 29 juillet 2019 j]. Disponible à l'adresse : https://freenetproject.org/fr/index.html

ANON., [sans date]. I2P Anonymous Network. In : [en ligne]. [Consulté le 29 juillet 2019 k]. Disponible à l'adresse : http://geti2p.net/en/

ANON., [sans date]. Que sont les cookies tiers ? In : *IONOS Digitalguide* [en ligne]. [Consulté le 30 juillet 2019 l]. Disponible à l'adresse : https://www.ionos.fr/digitalguide/hebergement/aspects-techniques/que-sont-les-cookies-tiers/

ANON., [sans date]. Tails - Privacy for anyone anywhere. In : [en ligne]. [Consulté le 16 juillet 2019 m]. Disponible à l'adresse : https://tails.boum.org/index.fr.html

ANON., [sans date]. Traces numériques, de quoi s'agit-il? | Me and my Shadow. In : [en ligne]. [Consulté le 12 juillet 2019 n]. Disponible à l'adresse : https://myshadow.org/

ANON., [sans date]. [Tuto] Déployez un hidden service avec Tor en 30 secondes ! - mondedie.fr. In : [en ligne]. [Consulté le 30 septembre 2019 o]. Disponible à l'adresse : https://mondedie.fr/d/7428-tuto-deployez-un-hidden-service-avec-tor-en-30-secondes

ANON., [sans date]. Types of Proxy HTTP, HTTPS, Socks. In : [en ligne]. [Consulté le 30 août 2019 p]. Disponible à l'adresse : https://thesafety.us/http-socks-proxy

ANON., [sans date]. Using the Internet to Collect Data. In : [en ligne]. [Consulté le 15 juillet 2019 q]. Disponible à l'adresse : https://www2.virginia.edu/vpr/irb/sbs/resources_guide_data_tools_internet_collect.html

ANON., [sans date]. What Data Is Collected About You Online and How to Stop It. In : [en ligne]. [Consulté le 25 août 2019 r]. Disponible à l'adresse : https://www.globalsign.com/en/blog/what-data-is-collected-about-you-online

ANON., [sans date]. What every Browser knows about you. In : [en ligne]. [Consulté le 22 juillet 2019 s]. Disponible à l'adresse : http://webkay.robinlinus.com/

COLLECTIVE, Welance com-a Freelancers, [sans date]. Rethinking Anonymity for the Information Age. In : [en ligne]. [Consulté le 30 septembre 2019]. Disponible à l'adresse : https://www.gppi.net/2017/03/09/rethinking-anonymity-for-the-information-age

COMMUNICATION, D. G., [sans date]. Traces numériques. In : *Publictionnaire* [en ligne]. [Consulté le 22 juillet 2019]. Disponible à l'adresse : http://publictionnaire.huma-num.fr/notice/traces-numeriques/

ENCRYPT, Search, 2019. The Best Internet Privacy Tools for 2019. In : *Search Encrypt Blog* [en ligne]. 5 juin 2019. [Consulté le 20 août 2019]. Disponible à l'adresse : https://choosetoencrypt.com/privacy/the-best-internet-privacy-tools-for-2019/

GEORGES, Fanny, SEILLES, Antoine et SALLANTIN, Jean, 2010a. Des illusions de l'anonymat. Les stratégies de préservation des données personnelles à l'épreuve du Web 2.0. In : *Terminal. Technologie de l'information, culture & société* [en ligne]. 1 octobre 2010. n° 105. [Consulté le 10 septembre 2019]. DOI 10.4000/terminal.1876. Disponible à l'adresse : http://journals.openedition.org/terminal/1876

GEORGES, Fanny, SEILLES, Antoine et SALLANTIN, Jean, 2010b. Des illusions de l'anonymat. Les stratégies de préservation des données personnelles à l'épreuve du Web 2.0. In : *Terminal. Technologie de l'information, culture & société* [en ligne]. 1 octobre 2010. n° 105. [Consulté le 10 septembre 2019]. DOI 10.4000/terminal.1876. Disponible à l'adresse : http://journals.openedition.org/terminal/1876

INC, The Tor Project, [sans date]. Tor: Linux Install Instructions. In : [en ligne]. [Consulté le 9 septembre 2019 a]. Disponible à l'adresse : https://2019.www.torproject.org/docs/tor-doc-unix.html.en

INC, The Tor Project, [sans date]. Tor: Onion Service Protocol. In : [en ligne]. [Consulté le 9 septembre 2019 b]. Disponible à l'adresse : https://2019.www.torproject.org/docs/onion-services.html.en

LECOMTE, Romain, 2010. L'anonymat comme « art de résistance ». Le cas du cyberespace tunisien. In : *Terminal. Technologie de l'information, culture & société* [en ligne]. 1 octobre 2010. n° 105. [Consulté le 10 juillet 2019]. DOI 10.4000/terminal.1862. Disponible à l'adresse : http://journals.openedition.org/terminal/1862

MEZZOFIORE, Gianluca, [sans date]. Dear Prince William, this is why anonymity online is important. In : *Mashable* [en ligne]. [Consulté le 11 juillet 2019]. Disponible à l'adresse : https://mashable.com/2017/11/17/prince-william-anonymity-online-important-cyberbullying/

MICHEL, 2018. Être anonyme sur Internet. In : *Le Blog du Hacker* [en ligne]. 2 février 2018. [Consulté le 12 juillet 2019]. Disponible à l'adresse : https://www.leblogduhacker.fr/etre-anonyme-sur-internet/

MORRIS, A. J., 2019. What's a Tracking Pixel and How Can I Install and Use It on My WooCommerce Store? In : *Liquid Web* [en ligne]. 14 janvier 2019. [Consulté le 2 août 2019]. Disponible à l'adresse : https://www.liquidweb.com/blog/what-is-a-tracking-pixel/

NIELD, David, [sans date]. Here's All the Data Collected From You as You Browse the Web. In : *Gizmodo* [en ligne]. [Consulté le 18 juillet 2019]. Disponible à l'adresse : https://gizmodo.com/heres-all-the-data-collected-from-you-as-you-browse-the-1820779304

NIOUTY, 2018. Bien choisir son Tracking ? Qu'est ce qu'un Pixel ? In : *SemSeo Consulting | Expert en Visibilité* [en ligne]. 3 août 2018. [Consulté le 2 août 2019]. Disponible à l'adresse : https://www.sem-seo-consulting.fr/referencement/pixel-iframe-postback-cest-quoi-au-juste-le-tracking/

PÉLISSIER, Daniel, [sans date]. De quoi les traces numériques sont-elles le nom ? In : *Présence numérique des organisations* [en ligne]. [Consulté le 3 août 2019]. Disponible à l'adresse : https://presnumorg.hypotheses.org/94

PROGRAMS, Heinz Tschabitscher An independent writer who has reviewed hundreds of email et SINCE 1997, Services, [sans date]. These Are the 6 Best Disposable Email Services. In : *Lifewire* [en ligne]. [Consulté le 3 septembre 2019]. Disponible à l'adresse : https://www.lifewire.com/best-disposable-email-address-services-1171097

RESERVED, VTNV Solutions Limited https://www le-vpn com/fr/ Sitemap XML © 2019 Le VPN All rights, 2018. Qu'est-ce qu'un proxy ? Quand utiliser un proxy vs. VPN ? In : *Le VPN France* [en ligne]. 12 février 2018. [Consulté le 17 août 2019]. Disponible à l'adresse : https://www.le-vpn.com/fr/quest-ce-quun-proxy/