DEEP WEB (web Profond)

Le terme « **Deep Web** » fait référence à la partie du World Wide Web qui n'est pas indexée par les moteurs de recherche standard. Cela inclut tous les sites Web et contenus en ligne qui ne sont pas accessibles via un moteur de recherche car ils sont cachés derrière des pages de connexion protégées par mot de passe, du contenu généré dynamiquement ou des protocoles non standard. On estime que le Web profond est plusieurs fois plus grand que le Web de surface, qui est la partie du Web accessible via les moteurs de recherche. Le Deep Web est aussi parfois appelé le « Web invisible » ou le « Web caché ». Il est important de noter que le Deep Web n'est pas intrinsèquement illégal ou contraire à l'éthique ; il fait simplement référence à un contenu qui n'est pas facilement accessible via les moteurs de recherche standar

Le "web profond" fait référence à toute partie d'Internet qui n'est pas indexée par les moteurs de recherche traditionnels, tels que Google, Yahoo ou Bing. Cela inclut une variété de différents types de contenu, dont certains sont légaux et inoffensifs, tandis que d'autres peuvent être illégaux ou dangereux. Voici quelques exemples de différents types de contenus trouvés sur le web profond :

1. **Réseaux privés** : les réseaux privés tels que Tor, I2P et Freenet sont utilisés par les utilisateurs pour accéder au Web profond de manière anonyme. Ces réseaux sont souvent utilisés par des militants, des journalistes et d'autres personnes qui ont besoin de protéger leur vie privée et leur sécurité.

2. **Places de marché** : Le Web profond abrite également de nombreuses places de marché en ligne où les gens peuvent acheter et vendre des biens et services illégaux, tels que des drogues, des armes, de fausses pièces d'identité, des informations de carte de crédit volées, etc.

3. **Sites de dénonciation** : Certains sites Web profonds sont dédiés aux dénonciateurs, où les gens peuvent soumettre des conseils et des fuites anonymes. Ces sites sont souvent utilisés par des journalistes et des militants pour découvrir les actes répréhensibles des gouvernements et des entreprises.

4. **Forums et salons de discussion** : il existe également de nombreux forums et salons de discussion en ligne profonds où les gens peuvent discuter de sujets sensibles, tels que la politique, la religion et la sexualité, sans crainte de persécution ou de censure.
5. **Bases de données académiques et scientifiques** : de nombreuses bases de données académiques et scientifiques ne sont pas accessibles via les moteurs

de recherche traditionnels, de sorte que les chercheurs utilisent souvent le Web profond pour accéder à ces ressources.

6. **Contenu multimédia** : Enfin, le Web profond contient également une grande quantité de contenu multimédia, tel que des vidéos, de la musique et des images, qui n'est pas disponible via les moteurs de recherche traditionnels.

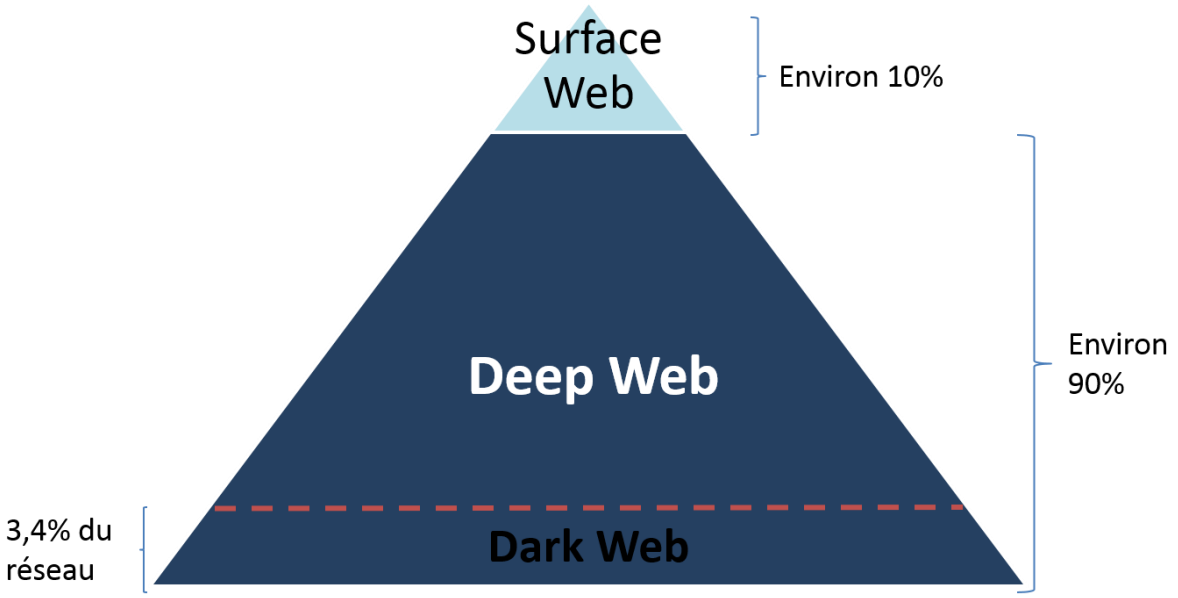
Le **Web profond**, également connu sous le nom de « **Web caché** », fait référence à la partie d'Internet qui n'est pas indexée par les moteurs de recherche et qui n'est pas accessible via les navigateurs Web traditionnels. Cela inclut les sites Web protégés par mot de passe, les bases de données en ligne et tout autre contenu qui n'est pas accessible au grand public.

Le Web profond suscite beaucoup d'intérêt car il est souvent associé à des activités illégales, telles que le trafic de drogue, la vente d'armes et le piratage de forums. Cependant, il est important de noter que tout le contenu du Web profond n'est pas illégal et qu'il existe également des utilisations légitimes pour y accéder.

Certaines personnes souhaitent explorer le Web profond pour trouver des informations qui ne sont pas disponibles sur le Web de surface, telles que des revues universitaires, des documents gouvernementaux et d'autres types de données qui peuvent être cachées derrière des murs payants ou d'autres restrictions.

D'autres s'intéressent au Web profond en raison de sa réputation de refuge pour la vie privée et l'anonymat. Tor, un navigateur Web populaire pour accéder au Web profond, est connu pour sa capacité à masquer les adresses IP des utilisateurs et à crypter leur trafic, ce qui rend plus difficile pour les agences gouvernementales et autres entités de suivre leurs activités en ligne.

Dans l'ensemble, le Web profond est une partie complexe et fascinante d'Internet qui peut être à la fois informative et dangereuse. Il est important de l'aborder avec prudence et de comprendre les risques potentiels liés à son accès.



Le **web visible**, également connu sous le nom de **surface web** ou **clearne**t, fait référence à la partie du World Wide Web qui peut être consultée et indexée par les moteurs de recherche. Il comprend tous les sites Web facilement accessibles et ne nécessitant aucune autorisation ou information d'identification spéciale pour y accéder. Les exemples de contenu Web visible comprennent les sites d'actualités, les plateformes de médias sociaux, les sites Web de commerce électronique et les blogs. En revanche, le Web profond fait référence aux parties d'Internet qui ne sont pas indexées par les moteurs de recherche et nécessitent des outils spéciaux ou une autorisation d'accès, tels que des forums en ligne privés, des sites Web protégés par mot de passe et des services par abonnement.

1 – Moteurs de recherche

1 – 1 – The internet archive – https://archive.org

Ce site consacré à l'archivage du Web est un projet créé par un organisme à but non lucratif. Il héberge et permet donc d'accéder à plusieurs types de ressources ayant parfois disparu du web. Celles-ci incluent des vidéos, audio, livres numérisés, des copies de jeux vidéo, de logiciels et même de systèmes d'exploitation n'existant plus depuis bien des années. Il vous permet par ailleurs de visiter les anciennes versions (archivées) des sites du Web. Ces versions « cache » se comptent par centaines de milliards.

1 – 2 -Yippy – (yippy .com)

Anciennement connu sous le nom Clusty, Yippy est un **méta moteur** de recherche qui mise sur le clustering, une méthode de classification des résultats de recherche dans des dossiers thématiques. Cette approche très différente de celle des moteurs de recherche classiques permet d'orienter l'internaute facilement vers les types de ressources et d'informations souhaitées : images, téléchargements, vidéos, blogs, boutiques, etc

1-3 – WorldCat – https://www.worldcat.org/fr

Il s'agit de la base de données bibliographique la plus large du web. Considérez-la comme un moteur de recherche référençant les catalogues de plus de 72 000 bibliothèques situées aux quatre coins du globe. Elle peut vous aider à trouver n'importe quel document, livre, thèse, vidéos, éléments multimédias, et même des objets de musée stockés quelque part dans le monde.

On retrouve cette base de données dans plusieurs bibliothèques, mais aussi sur les réseaux informatiques de certaines universités. Depuis 2006, elle est accessible librement sur le web via **worldCat.org.**

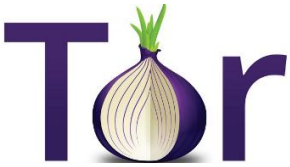
1 – 4 – World Wide Science – https://worldwidescience.org

C'est d'un moteur de recherche scientifique conçu pour accélérer la découverte et le partage de connaissances scientifiques. Il donne accès à une variété de ressources enfouies dans le deep web, et de surcroît dans plusieurs langues, y compris le français.

1 – 5 – DuckDuckGo – https://www.duckduckgo.com

C'est le moteur de recherche par excellence pour ceux qui veulent se passer de la domination de Google. C'est une parfaite alternative qui mise tout, de surcroit, sur votre vie privée. Beaucoup l'utilisent également sur le dark web pour ses fonctionnalités axées sur l'anonymat. C'est aussi le moteur de recherche par défaut du navigateur TOR. Cela en dit long sur sa réputation dans la communauté.

1 – 6 – moteur de recherche TOR



Il est impossible de parler du **deep web** ou même du **dark web** sans mentionner le fameux réseau Tor. Un navigateur éponyme qui permet de surfer en sécurité sur le web en substituant son adresse IP tout évitant d'être pisté. Cela étant dit, le réseau Tor donne également accès à un vaste univers de sites web souterrains portant l'extension .onion.

Ces services sont accessibles uniquement par le biais du navigateur Tor. Il existe de nombreux moteurs de recherche permettant de découvrir des contenus hébergés sur les sites du réseau. On peut citer parmi eux les moteurs :

- **Torch** (cnkj6nippubgycuj.onion)
- **notEvil** (hss3uro2hsxfogfq.onion)
- **Ahmia** (msydqstlz2kzerdg.onion) qui est lui accessible depuis le web surfacique (https://ahmia.fi). Mais vous aurez besoin de Tor pour ouvrir les sites référés.

2 – browsers pour web profond -navigateur

~~Les navigateurs Deep Web sont des navigateurs qui vous permettent d'accéder au Deep Web. Le Deep Web, comme son nom l'indique, est la partie « la plus profonde » d'Internet~~

ls vous permettent d'accéder au Deep Web, c'est la réponse au niveau de la surface, mais ce qui les rend spéciaux, pourquoi ne pouvez-vous pas utiliser les navigateurs généraux pour faire de même

- **Accès aux liens cachés**

  Le Deep Web n'est pas hébergé sur le « **World Wide Web** » (*WWW),* vous ne pouvez donc pas y accéder avec les navigateurs généraux car ils ne reconnaissent pas **le .onion** ou ne peuvent pas vous accorder l'accès aux opposés. Ces liens ne sont pas non plus disponibles sur les moteurs de recherche pour que vous puissiez simplement cliquer dessus et atterrir là-bas.

  Alors que les navigateurs Web profonds sont conçus spécifiquement pour faciliter l'accès à ces liens oignon, et en même temps vous permettent généralement de naviguer sur le **clearnet.**

- **Vie privée**

  Le Deep Web est généralement associé à un contenu « illicite » sinon illégal au mieux, même si ce n'est pas toujours vrai, je suis presque sûr que vous ne voudriez pas que d'autres jettent un coup d'œil sur votre historique de recherche, ou Identité sur le Deep Web, n'est-ce pas?

  Il ne s'agit pas seulement de l'historique de recherche, des cookies ou des activités de votre côté, même d'autres (*y compris des sites Web et des « tiers » intéressés de manière indépendante)* suivent et suivent votre emplacement, vos activités et d'autres données.

  Aucune information n'est envoyée des navigateurs Web profonds aux sites Web que vous parcourez, ce qui n'est pas le cas avec les navigateurs généraux que nous utilisons.

  Donc, fondamentalement, les navigateurs Web profonds sont spécifiquement armés de telle sorte que votre identité est protégée et gardée anonyme, de sorte que vous avez toujours une cape sur vous pendant que vous marchez dans les rues visqueuses du Web profond.

- **Meilleurs navigateurs**

  2 – 1 – Tor – https://www.torproject.org

Même s'il ne s'agit pas d'un « tableau de classement, **TOR** est littéralement « le meilleur navigateur Web profond » que vous rencontrerez jamais.

Le navigateur Tor est basé sur le réseau **Tor**, qui signifie "**The Onion Router**". Il offre l'anonymat et la confidentialité aux utilisateurs en cryptant et en acheminant leur trafic Internet via une série de relais, ce qui rend difficile le suivi de leurs activités en ligne. Le navigateur Tor peut être utilisé pour accéder à des sites Web avec le domaine .onion, qui ne sont accessibles que via le réseau Tor.

Voici quelques fonctionnalités clés du navigateur Tor :

1. **Anonymat** : Le navigateur Tor dissimule votre adresse IP et vos activités en ligne en acheminant votre trafic Internet via plusieurs relais, ce qui rend difficile l'identification de votre emplacement réel ou le suivi de vos habitudes de navigation.
2. **Cryptage :** Le navigateur crypte votre trafic Internet, garantissant que vos données restent sécurisées et privées lors de leur passage sur le réseau Tor.
3. **Accès aux sites Web .onion** : le navigateur Tor vous permet d'accéder à des sites Web avec le domaine .onion, qui sont hébergés sur le réseau Tor et ne sont pas accessibles via les navigateurs Web classiques.
4. **Anti-censure** : Le réseau Tor aide les utilisateurs à contourner la censure en ligne et à accéder aux informations qui peuvent être bloquées ou restreintes dans certains pays ou régions.

Il est important de noter que bien que le navigateur Tor offre l'anonymat et la confidentialité, il ne garantit pas une sécurité complète. Les utilisateurs doivent toujours faire preuve de prudence et suivre les meilleures pratiques pour protéger leur confidentialité et leur sécurité en ligne.

De plus, il convient de mentionner que si le Web profond comprend du contenu légitime et légal, il est également connu pour héberger des activités et des sites Web illégaux. Il est important d'utiliser le Web profond de manière responsable et de respecter les lois et réglementations de votre juridiction.

2-2 – TOR pour Android

Tor pour Android est un **navigateur mobile** qui permet aux utilisateurs de naviguer sur Internet de manière anonyme et d'accéder au réseau Tor. Le réseau Tor, également connu sous le nom de The Onion Router, est un réseau

décentralisé de serveurs gérés par des bénévoles qui aident les utilisateurs à protéger leur vie privée et leur anonymat en ligne.

Voici quelques fonctionnalités et aspects clés de Tor pour Android :

1. **Anonymat et confidentialité** : Tor pour Android achemine votre trafic Internet à travers une série de couches cryptées, ce qui rend difficile pour quiconque de retracer vos activités en ligne jusqu'à vous. Il cache votre adresse IP et crypte votre connexion, offrant un haut niveau de confidentialité.
2. **Réseau Tor** : Le navigateur se connecte au réseau Tor, qui est un réseau de relais qui font rebondir votre connexion via différents serveurs, ce qui rend difficile le suivi de votre emplacement ou de vos habitudes de navigation.
3. **Accès aux sites Web .onion** : Tor pour Android vous permet d'accéder à des sites Web avec le domaine .onion, qui font partie du réseau Tor et ne sont pas accessibles via les navigateurs habituels. Ces sites Web hébergent souvent du contenu qui peut ne pas être indexé ou disponible sur le Web de surface.
4. **Sécurité** : Tor pour Android offre des fonctions de sécurité intégrées pour protéger votre navigation. Il empêche les sites Web de suivre votre comportement en ligne via des cookies et bloque certains éléments Web qui pourraient compromettre votre vie privée.
5. **Pas d'historique ni de cookies** : Par défaut, Tor pour Android ne stocke pas votre historique de navigation ni n'enregistre de cookies, garantissant que vos activités en ligne restent privées.
6. **Modules complémentaires et extensions** : Semblable à d'autres navigateurs, Tor pour Android prend en charge les modules complémentaires et les extensions pour améliorer votre expérience de navigation. Cependant, il est important de noter que toutes les extensions ne sont pas compatibles avec Tor et peuvent compromettre votre anonymat.
7. **Interface utilisateur** : L'interface utilisateur de Tor pour Android est conçue pour être conviviale et familière aux utilisateurs d'autres navigateurs mobiles. Il offre une expérience de navigation transparente tout en préservant votre confidentialité
8. **Limitations** : Il est important de connaître les limitations de Tor pour Android. Bien qu'il offre un anonymat et une confidentialité solides, l'expérience de navigation peut être plus lente que celle des navigateurs classiques en raison des couches de cryptage supplémentaires et du réacheminement du trafic. De plus, certains sites Web peuvent bloquer

l'accès des nœuds de sortie Tor, limitant votre capacité à accéder à certains contenus.

Lorsque vous utilisez **Tor pour Android** ou tout autre navigateur compatible Tor, il est essentiel de comprendre ses capacités et ses limites pour prendre des décisions éclairées concernant votre confidentialité et votre sécurité en ligne.

2 – 3 – Invisible Project Internet (I2P) – https://get.i2p.net/fr/

I2P (Invisible Internet Project) est un réseau anonyme permettant à deux applications distantes de communiquer au sein d'un environnement invisible et sécurisé.
Déployé comme surcouche réseau d'anonymisation (réseau dans le réseau), **I2P** protège les communications contre la surveillance globale (**dragnet**) et celle réalisée par des tiers (FAI par exemple). Conçu pour sécuriser au maximum les données personnelles de ses utilisateurs tout en les affranchissant de la censure imposée par la situation géographique, **I2P** vise à réduire au maximum les attaques pour garantir une anonymisation presque parfaite.
I2P fonctionne à la fois avec votre navigateur Internet et vos applications de chat pour une efficacité renforcée.

2 - 4 – Whonix - https://www.whonix.org

Ce système s'appuie sur Tor et un ensemble ingénieux de machines virtuelles pour assurer un niveau important de sécurité et d'anonymat. Ce projet open source s'installe sous la forme de deux machines virtuelles dans l'hyperviseur **Virtualbox**. La première est la station de travail que vous utiliserez pour naviguer sur le web, écrire des mails, faire des chats, etc. La seconde joue le rôle de passerelle réseau. Elle établit les circuits Tor sur lesquels transiteront les connexions de la station de travail. Autrement dit, avec Whonix, vous n'installez pas seulement un système d'exploitation, mais carrément un petit réseau virtuel. Avec Whonix, toutes les connexions passent par Tor, et pas seulement les connexions HTTP/HTTPS. De plus Whonix crée un circuit Tor différent pour chaque application qui sera lancée sur la station de travail. Pour un observateur extérieur, il sera donc beaucoup plus difficile de relier les différentes tâches les unes aux autres et de réaliser un profilage.

2 – 5 – Subgraph OS– https://subgraph.com/sgos/

SubGraph OS est un open-source et l'un des navigateurs les plus sécurisés que vous pouvez utiliser pour naviguer sur le Web profond.
Il est emballé avec GrSecurity pour commencer, tout ce que je peux dire, c'est que c'est « la meilleure » amélioration de la sécurité du noyau **Linux connue de l'homme !**
L'un de ses superpouvoirs est sa capacité à créer des « bacs à sable » autour de programmes généralement sujets aux attaques en ligne et aux fuites de sécurité. Cela signifie qu'il « contient » ces applications (*e-mail, fichiers PDF, applications de messagerie) en eux-mêmes*, donc même s'il y a une fuite ou une faille de sécurité, cela n'affecte pas l'ensemble du système et reste limité à l'application. Sans oublier que tout le trafic sortant est acheminé via le réseau TOR. C'est un programme complet, mais je suis presque sûr que les fonctionnalités ci-dessus peuvent vous brosser un tableau en ce qui concerne les capacités de Subgraph, n'est-ce pas ?

2 – 6 – Disconnect – https://disconnect.me

Disconnect est une extension développée par Brian Kennish, principalement connu pour avoir travaillé chez Google. Cette extension, accessible à la fois sur Google Chrome , Mozilla Firefox ou Safari pour ne citer que les navigateurs web les plus populaires, permet de bloquer les widgets et cookies permettant d'interagir avec les réseaux sociaux et moteurs de recherche. Le principe derrière Disconnect est particulièrement simple, sans compter que le logiciel ne nécessite aucune configuration de la part de l'utilisateur. Une fois l'extension installée, elle bloque immédiatement tous les cookies issus de divers services en ligne comme Google, Facebook , Twitter , Digg (entre autres), ainsi que tous les widgets et boutons sociaux tirés de ces sites en particulier. En plus des scripts, Disconnect s'occupe également des programmes malveillants de surveillance qui pourraient créer un profil de l'utilisateur pour utilisation commerciale. Mécaniquement, le chargement de pages web devient alors beaucoup plus rapide, puisque Disconnect supprime l'apparition de divers pop-ups.

2 – 7 – Tails – https://tails.boum.org/

Tails ou **The Amnesic Incognito Live System** est une distribution GNU/Linux axée sur la sécurité fondée sur Debian qui a pour but de préserver

la vie privée et l'anonymat. Toutes les connexions réseau transitent soit à travers le réseau Tor, soit sont bloquées. Le système est conçu pour être démarré à partir d'un live DVD ou d'un live USB, et ne pas laisser de trace numérique sur la machine à moins qu'il soit explicitement autorisé à le faire. Le projet Tor pourvoit (en partie) à son développement

T*ails* est reconnu comme étant un système d'exploitation particulièrement bien sécurisé, notamment grâce aux nombreuses précautions prises par le système du point de vue du hardware et du réseau. De surcroît, le code du système étant sous licence GPLv3+ (logiciel libre), celui-ci est entièrement ouvert au public et consultable en ligne. Cette pratique permet de réduire le risque de portes dérobées et/ou de code malveillant.

Cependant, la sécurité de *Tails* possède des faiblesses, souvent dues au hardware et non au logiciel à proprement parler. Par exemple *Tails* ne saurait protéger l'utilisateur si le matériel de l'ordinateur utilisé a été préalablement compromis, ou si son firmware l'a été. Enfin, certaines attaques comme les attaques par démarrage à froid parviennent à compromettre le système.

2 – 8 – EPIC – https://epicbrowser.com/

Epic Browser est un navigateur Web qui prétend donner la priorité aux fonctionnalités de confidentialité et de sécurité pour ses utilisateurs. Bien qu'il ne soit pas spécifiquement conçu pour accéder au Web profond , il intègre des fonctionnalités qui visent à améliorer la confidentialité et à protéger les données des utilisateurs.

Voici quelques fonctionnalités et aspects clés d'Epic Browser :

1. **Confidentialité et sécurité** : Epic Browser utilise diverses fonctionnalités axées sur la confidentialité pour protéger les informations des utilisateurs. Il bloque les cookies tiers, empêche le suivi par les moteurs de recherche et offre une protection contre les empreintes digitales, qui est une technique utilisée pour identifier et suivre les utilisateurs sur les sites Web.
2. **Connexion cryptée** : Epic Browser établit automatiquement des connexions cryptées (HTTPS) dans la mesure du possible, ce qui aide à protéger vos données pendant la transmission et empêche les écoutes clandestines.
3. **VPN intégré** : Epic Browser comprend un réseau privé virtuel (VPN) intégré qui vous permet de naviguer sur le Web de manière anonyme en acheminant votre trafic via différents serveurs, masquant ainsi votre adresse IP et votre emplacement. Cependant, veuillez noter que ce VPN n'est pas spécifiquement conçu pour accéder au Web profond.
4. **Bloqueur de publicités** : le navigateur intègre un bloqueur de publicités pour empêcher l'apparition de publicités intrusives sur les sites Web, améliorant à la fois la confidentialité et la vitesse de navigation.

5. **Pas de prélecture DNS** : Epic Browser désactive la prélecture DNS, ce qui aide à réduire le risque de fuite d'informations involontaire.
6. **Prise en charge du proxy** : bien qu'Epic Browser ne fournisse pas d'accès direct au Web profond, vous pouvez le configurer pour utiliser des proxy pour accéder à des sites Web ou à des services spécifiques qui nécessitent des connexions proxy.
7. **Base d'utilisateurs limitée** : Epic Browser n'est pas aussi largement utilisé ou connu que les navigateurs grand public comme Chrome, Firefox ou Safari. Par conséquent, il peut ne pas recevoir de mises à jour ou de correctifs de sécurité aussi fréquemment, ce qui peut affecter sa sécurité globale.

Il est important de noter que l'accès au Web profond implique la visite de sites Web intentionnellement cachés ou non indexés par les moteurs de recherche. Bien qu'Epic Browser puisse fournir certaines fonctionnalités de confidentialité et de sécurité, l'accès au Web profond nécessite des précautions supplémentaires telles que l'utilisation de logiciels spécialisés comme Tor et la prudence quant au contenu et aux sites Web avec lesquels vous interagissez.

2 – 9 – IPREDIA – https://www.ipredia.org/os

iPredia Browser est un navigateur Web axé sur la confidentialité qui vise à protéger la confidentialité et l'anonymat en ligne des utilisateurs. Il est conçu pour offrir une expérience de navigation sécurisée en acheminant le trafic Internet via le réseau Tor anonyme.

Voici quelques fonctionnalités et caractéristiques clés du navigateur iPredia :

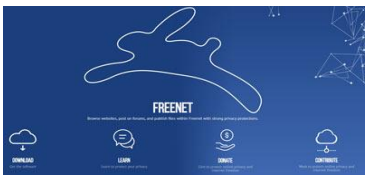
1. Basé sur le réseau Tor : le navigateur iPredia est construit sur le réseau Tor, qui est un réseau largement utilisé pour anonymiser les connexions Internet. Tor achemine votre trafic Internet via une série de relais, ce qui rend difficile le suivi de vos activités en ligne.
2. Anonymat et confidentialité : en utilisant le navigateur iPredia, votre adresse IP est dissimulée, ce qui rend difficile pour les sites Web ou les services en ligne de suivre votre position ou de vous identifier. Cela aide à protéger votre vie privée et à empêcher des entités tierces de surveiller vos habitudes de navigation.
3. Cryptage : le navigateur iPredia crypte votre trafic Internet, ce qui rend plus difficile pour quiconque d'intercepter et de lire vos données. Ce cryptage renforce la sécurité de vos communications en ligne.
4. Anti-Tracking : iPredia Browser inclut des fonctionnalités pour bloquer les mécanismes de suivi, tels que les cookies, que les sites Web et les annonceurs utilisent pour suivre votre comportement de navigation. Cela

aide à empêcher la publicité ciblée et minimise la collecte de données par les sites Web.

5. Résistant à la censure : le navigateur iPredia peut contourner la censure sur Internet et accéder à des sites Web et à des services en ligne qui peuvent être restreints ou bloqués dans certaines régions. Ceci est réalisé grâce à la capacité du réseau Tor à contourner ces restrictions.
6. Facile à utiliser : le navigateur iPredia offre une interface conviviale similaire à d'autres navigateurs Web populaires. Il permet aux utilisateurs de naviguer sur le Web sans avoir besoin de connaissances techniques approfondies.

Il est important de noter que si le navigateur iPredia offre une confidentialité et un anonymat améliorés, il présente certaines limites. En raison de la nature du réseau Tor, les vitesses de navigation peuvent être plus lentes que celles des navigateurs Web traditionnels. De plus, certains sites Web ou services peuvent avoir mis en place des mesures pour bloquer les nœuds de sortie Tor, ce qui peut affecter l'accès à certains sites.

2 – 10 – projet FreeNet – https://freenetproject.org



Freenet est un logiciel libre qui vous permet, de façon anonyme, de partager des fichiers, de parcourir et de publier des « sitesFree » (sites Web accessibles uniquement par Freenet), de clavarder sur des forums, le tout sans craindre la censure. Freenet est décentralisé afin de le rendre moins vulnérable aux attaques, et s'il est utilisé en mode « réseau invisible » qui implique que les utilisateurs se connectent seulement à leurs amis, il est très difficile à détecter.

Les communications des nœuds Freenet sont chiffrées et acheminées par d'autres nœuds afin qu'il soit extrêmement difficile de déterminer qui demande l'information et quel en est le contenu.

Les utilisateurs contribuent au réseau en donnant de la bande passante et une partie de leur disque dur (appelée « magasin de données ») pour le stockage de fichiers. Les fichiers sont automatiquement conservés ou supprimés suivant leur popularité, les moins populaires étant détruits pour faire place à du contenu plus récent ou plus populaire. Les fichiers sont chiffrés. L'utilisateur ne peut donc pas découvrir facilement ce que contient son magasin de données et, avec un peu de chance, ne peut pas en être tenu responsable. Les forums de discussion, les

sites Web et la fonction de recherche s'appuient sur ce magasin de données distribué.

2 – 11 – Psiphon – https://www.psiphon.com

Psiphon comme Whonix ou un certain nombre d'autres outils sur cette liste est un outil anti-censure. C'est un navigateur qui utilise VPN, SSH Tunnels et Proxy pour aider à contourner la censure sur Internet. Notez qu'il indique clairement qu'il n'augmente pas l'anonymat et ne doit pas être considéré comme un outil de sécurité en ligne.
En termes simples, lorsque nous utilisons Psiphon, nos FAI ne peuvent pas intercepter notre trafic. Ils ne peuvent pas non plus surveiller nos habitudes Internet, notre historique de navigation, nos messages ou quoi que ce soit d'autre. Sous Windows, Psiphon utilise les protocoles L2TP/IPSec pour se connecter à Internet, sans doute l'une des solutions les plus puissantes et les plus cryptées.
Il est actuellement disponible pour Windows, Android et iOS. Actuellement, Linux et MacOS ne sont pas pris en charge, mais l'équipe a déclaré que cela pourrait être une possibilité future.
Notez que Psiphon n'est ni une alternative à Tor ni un VPN. C'est simplement un « outil de contournement de la censure ». Il permet d'accéder au contenu que d'autres navigateurs ne peuvent pas. Mais il n'offre pas nécessairement l'anonymat ou la vie privée. De plus, contrairement à un VPN, il ne transmet que les proxys des activités menées explicitement via le navigateur Psiphon. Toutes les autres connexions Internet sont non cryptées et publiques.

2 – 12 – Yandex – https://browser.yandex.com

Yandex est un navigateur Web populaire développé par la société russe Yandex. Il est basé sur le projet open source Chromium, qui sert également de base à d'autres navigateurs bien connus comme Google Chrome et Microsoft Edge.

Voici quelques fonctionnalités et caractéristiques clés du navigateur Yandex :

1. **Interface utilisateur** : le navigateur Yandex présente une interface claire et conviviale. Il offre une page de démarrage personnalisable avec des widgets pour un accès rapide aux sites Web fréquemment visités, aux actualités, aux mises à jour météorologiques, etc.
2. **Mode Turbo** : le navigateur Yandex inclut une fonctionnalité appelée "Mode Turbo", qui permet d'optimiser les temps de chargement des pages Web, en particulier sur les connexions Internet plus lentes. Le mode Turbo compresse les données, réduit la quantité de données à transmettre et accélère par la suite la navigation.

3. **SmartBox** : le navigateur Yandex dispose d'une barre de recherche et de navigation appelée SmartBox, qui fournit des suggestions au fur et à mesure que vous tapez, similaire à l'omnibox des autres navigateurs. Il offre un accès rapide aux résultats de recherche, aux sites Web, aux signets et aux paramètres du navigateur.
4. **Sécurité et confidentialité** : le navigateur Yandex met l'accent sur les fonctionnalités de sécurité et de confidentialité. Il utilise le service de navigation sécurisée pour se protéger contre les sites Web malveillants et avertir les utilisateurs des menaces potentielles. Il dispose également d'une protection intégrée contre le phishing et d'un outil pour bloquer les cookies tiers.
5. **Extensions et thèmes** : Semblable à d'autres navigateurs, le navigateur Yandex prend en charge les extensions et les thèmes. Les utilisateurs peuvent améliorer leur expérience de navigation en ajoutant diverses extensions à partir de la galerie d'extensions Yandex. Ils peuvent également personnaliser l'apparence du navigateur en appliquant différents thèmes.
6. **Synchronisation** : le navigateur Yandex permet aux utilisateurs de synchroniser leurs paramètres, signets, historique et autres données sur plusieurs appareils. Cette fonctionnalité est bénéfique pour les utilisateurs qui souhaitent avoir une expérience de navigation cohérente sur différents appareils.
7. Services intégrés : le navigateur Yandex s'intègre à d'autres services fournis par Yandex, tels que Yandex.Mail, Yandex.Disk (stockage en nuage), Yandex.Translate et Yandex.Music. Cette intégration permet aux utilisateurs d'accéder à ces services directement depuis l'interface du navigateur.

Il convient de noter que la popularité du navigateur Yandex est principalement concentrée en Russie et dans d'autres régions russophones, où Yandex est un moteur de recherche et un fournisseur de services Internet bien établis et largement utilisés. Cependant, le navigateur est disponible pour téléchargement et utilisation dans le monde entier.

2 – 12 – Zero Net – https://zeronet.io

ZeroNet est un réseau peer-to-peer décentralisé qui permet aux utilisateurs de créer et d'héberger des sites Web sans dépendre de serveurs traditionnels ou d'une infrastructure centralisée. Il utilise la technologie blockchain et les protocoles BitTorrent pour distribuer les données du site Web aux utilisateurs participants, ce qui rend les sites Web résistants à la censure et capables de fonctionner même sans autorité centrale.

Voici un bref aperçu du fonctionnement de ZeroNet :

1. **Réseau peer-to-peer** : ZeroNet fonctionne comme un réseau de pairs, chaque utilisateur contribuant au stockage et à la bande passante pour héberger des sites Web et distribuer leur contenu.
2. **Cryptage cryptographique** : ZeroNet utilise le cryptage cryptographique pour sécuriser la transmission des données et assurer la confidentialité des utilisateurs accédant aux sites Web sur le réseau.
3. **Adressage de contenu** : les sites Web sur ZeroNet sont identifiés à l'aide de l'adressage de contenu au lieu des noms de domaine. Chaque site Web se voit attribuer une adresse cryptographique unique en fonction du contenu qu'il contient.
4. **Stockage de données distribué** : le contenu des sites Web ZeroNet est distribué sur plusieurs pairs, chaque pair stockant des parties des données du site Web. Cela rend les sites Web résistants aux tentatives de censure et leur permet d'être accessibles même si certains pairs se déconnectent.
5. **Technologie BitTorrent** : ZeroNet exploite la technologie BitTorrent pour distribuer les données du site Web entre pairs. Lorsqu'un utilisateur accède à un site Web ZeroNet, son client télécharge et partage automatiquement les fichiers nécessaires à partir d'autres pairs sur le réseau.
6. **Intégration de la blockchain Bitcoin** : ZeroNet utilise la blockchain Bitcoin à diverses fins, telles que la gestion d'un registre public des mises à jour du site Web, la gestion de l'authentification des utilisateurs et la facilitation des micropaiements facultatifs pour soutenir les créateurs de contenu.
7. **Interface conviviale** : ZeroNet fournit une interface conviviale, permettant aux utilisateurs de parcourir les sites Web sur le réseau à l'aide de navigateurs Web standard. Les sites Web sur ZeroNet peuvent avoir des fonctionnalités dynamiques telles que des forums, des salles de discussion et l'authentification des utilisateurs.

La nature décentralisée de ZeroNet offre plusieurs avantages, notamment la résistance à la censure, une confidentialité accrue et une meilleure tolérance aux pannes. Cependant, il convient de noter que bien que ZeroNet puisse fournir l'anonymat aux visiteurs du site Web, les opérateurs de site Web peuvent toujours avoir besoin de prendre des mesures supplémentaires pour protéger leur identité et garantir le respect des lois applicables.

3 – Différences entre TOR et I2P

TOR (The Onion Router) et I2P (Invisible Internet Project) sont tous deux des réseaux anonymisants qui visent à assurer la confidentialité et la sécurité des internautes. Bien qu'ils partagent certaines similitudes, il existe également des différences significatives entre les deux.

1. **Architecture de réseau** :
   - TOR : TOR est un réseau décentralisé qui fonctionne en acheminant le trafic Internet via une série de relais ou de nœuds gérés par des

bénévoles. Chaque nœud du réseau TOR ne connaît que les nœuds précédent et suivant de la route, ce qui aide à masquer l'origine et la destination du trafic.

- I2P : I2P est également un réseau décentralisé, mais il utilise une approche de routage différente. Il utilise une technique appelée "acheminement à l'ail", où les messages sont regroupés dans des couches de cryptage (appelées "gousse d'ail"). Chaque couche est décollée une à une par le destinataire, ce qui rend difficile la traçabilité de l'origine du message.

2. **Concentrez-vous sur l'anonymat** par rapport à la confidentialité :
   - **TOR** : TOR se concentre principalement sur l'anonymat en dissimulant l'identité et l'emplacement de l'utilisateur. Il y parvient en faisant rebondir le trafic de l'utilisateur à travers plusieurs nœuds TOR, ce qui rend difficile le traçage de la source de la communication.
   - **I2P** : Bien qu'I2P fournisse également l'anonymat, son objectif principal est la confidentialité. Il vise à créer un réseau sécurisé et privé où les utilisateurs peuvent communiquer et partager des informations sans exposer leur identité ou le contenu de leur communication.
3. **Services et demandes** :
   - **TOR** : TOR est largement utilisé pour accéder à l'Internet public de manière anonyme, parcourir des sites Web et accéder à des services cachés au sein du réseau TOR, tels que les places de marché basées sur TOR et les forums anonymes.
   - **I2P** : I2P est conçu pour héberger son propre écosystème de services et d'applications au sein du réseau. Il fournit des fonctionnalités telles que le partage de fichiers anonymes, la messagerie électronique, la navigation Web et l'hébergement de sites Web et de services au sein du réseau I2P lui-même.
4. **Performances et Vitesse** :
   - **TOR** : En raison de son approche de routage en couches, TOR peut parfois introduire une latence et réduire les vitesses de navigation, en particulier lorsque le trafic passe par plusieurs nœuds. Les performances peuvent varier en fonction du nombre d'utilisateurs et de la congestion du réseau.
   - I2P : L'approche de routage à l'ail d'I2P peut également introduire une latence supplémentaire, mais elle vise généralement à fournir une communication plus rapide en minimisant le nombre de sauts et en maintenant une taille de réseau plus petite par rapport à TOR.
5. **Accessibilité :**
   - TOR : TOR est plus largement connu et accessible au grand public. Il propose un navigateur convivial appelé Tor Browser, qui simplifie le processus de connexion au réseau TOR et d'accès aux services TOR.

- I2P : I2P, bien que moins populaire, est toujours accessible aux utilisateurs. Il nécessite que les utilisateurs installent le logiciel I2P et configurent leurs applications pour utiliser le proxy I2P pour se connecter au réseau.

En résumé, TOR et I2P sont des réseaux axés sur la confidentialité, mais TOR met l'accent sur l'anonymat et l'accès à l'Internet public, tandis qu'I2P se concentre sur la création d'un réseau autonome et sécurisé pour diverses applications au sein de son écosystème. Le choix entre TOR et I2P dépend des exigences spécifiques de confidentialité et de fonctionnalité de l'utilisateur.

4 – Aspects légaux

4 – 1 web profond

Le web profond fait référence à la partie d'Internet qui n'est pas indexée par les moteurs de recherche et qui nécessite un logiciel, des configurations ou une autorisation d'accès spécifiques. Il comprend différents types de contenus, légaux et illégaux. Lors de l'examen des aspects juridiques du Web profond, il est important de faire la différence entre le Web profond lui-même et les activités qui s'y déroulent.

1. **Web profond et légalité** : Le Web profond, en tant que concept, n'est pas intrinsèquement illégal. Il se compose principalement de contenu légitime tel que des bases de données privées, des services par abonnement, des ressources académiques et d'autres matériaux qui ne sont pas destinés à l'indexation publique. Il est important de noter que l'accès au Web profond est légal, mais que s'y engager dans des activités illégales ne l'est pas.
2. **Activités illégales** : le Web profond est connu pour héberger des marchés illicites, où des biens et services illégaux sont achetés et vendus. Ces activités peuvent inclure le trafic de drogue, la vente d'armes, les outils de piratage, la contrefaçon, le vol de données et d'autres transactions illégales. S'engager dans de telles activités est contraire à la loi dans la plupart des juridictions.
3. **Anonymat et confidentialité** : le Web profond est souvent associé à l'anonymat et à la confidentialité. Bien que la confidentialité en soi ne soit pas illégale, des individus peuvent exploiter ces fonctionnalités pour se livrer à des activités illégales ou échapper aux forces de l'ordre. Cependant, il convient de noter que les forces de l'ordre ont développé des techniques et des outils pour enquêter et poursuivre les activités criminelles sur le Web profond.
4. Efforts d'application de la loi : les gouvernements et les organismes d'application de la loi du monde entier surveillent activement le Web profond pour identifier et poursuivre les personnes impliquées dans des activités illégales. Ils emploient diverses méthodes telles que des opérations d'infiltration, l'infiltration de réseaux criminels et des technologies avancées pour traquer les criminels et faire respecter la loi.
5. Cryptage et Tor : le Web profond s'appuie sur des technologies de cryptage et d'anonymisation telles que le réseau Tor pour garantir la confidentialité et protéger l'identité des utilisateurs. Bien que ces technologies aient des utilisations légitimes, elles peuvent également être exploitées à des fins illégales. Cependant, l'utilisation

du cryptage et de Tor pour la confidentialité et la sécurité est généralement considérée comme légale et légitime.

En résumé, le web profond lui-même **n'est pas illégal**, mais il peut héberger des activités illégales. S'engager dans des activités illégales sur le Web profond, comme participer à des marchés illicites ou s'engager dans des transactions criminelles, est contraire à la loi. Les gouvernements et les forces de l'ordre surveillent activement le Web profond pour identifier et poursuivre les personnes impliquées dans des activités illégales.

4 -2 – Dark Web

Le dark web, également connu sous le nom de darknet, est une partie d'Internet qui est intentionnellement cachée et accessible uniquement via des logiciels ou des configurations spécifiques. Il offre aux utilisateurs l'anonymat et la confidentialité, ce qui rend difficile le suivi de leurs activités. Bien que le dark web lui-même ne soit pas illégal, il est important de comprendre que s'engager dans des activités illégales sur le dark web est contraire à la loi dans la plupart des juridictions.

Voici quelques aspects juridiques liés au dark web :

1. **Activités illégales** : Le dark web a acquis la réputation de faciliter les activités illégales telles que le trafic de drogue, le commerce d'armes, les services de piratage, les produits contrefaits, les données volées, etc. S'engager dans ces activités est illégal et puni par la loi.
2. **Application de la loi** : les gouvernements et les organismes chargés de l'application de la loi du monde entier surveillent activement le dark web pour identifier et appréhender les individus impliqués dans des activités illégales. Ils peuvent utiliser des outils et des techniques spécialisés pour traquer les criminels sur le dark web.
3. **Problèmes d'anonymat** : bien que le dark web offre un certain niveau d'anonymat, il n'est pas infaillible. Les organismes chargés de l'application de la loi utilisent diverses méthodes pour anonymiser les individus et suivre leurs activités, notamment en analysant les transactions, en infiltrant les marchés et en utilisant une technologie de pointe.
4. **Réseau Tor** : Le réseau Tor est un moyen populaire d'accéder au dark web, car il permet aux utilisateurs de parcourir les sites Web de manière anonyme. Cependant, il convient de noter que le réseau Tor lui-même est légal et que de nombreuses personnes et organisations l'utilisent à des fins légitimes telles que la protection de leur vie privée et le contournement de la censure.
5. **Utilisations légitimes** : Toutes les activités sur le dark web ne sont pas illégales. Les journalistes, les militants et les individus vivant sous des régimes oppressifs peuvent utiliser le dark web pour communiquer en toute sécurité et accéder aux informations sans crainte de surveillance ou de censure.
6. **Complexités juridictionnelles** : le dark web opère au-delà des frontières internationales, ce qui peut créer des problèmes juridictionnels pour les forces de l'ordre. La coopération entre les différents pays est essentielle pour lutter efficacement contre les activités illégales sur le dark web.

Il est crucial de comprendre que la participation à des activités illégales sur le dark web peut avoir de graves conséquences juridiques. S'engager dans de telles activités viole non seulement la loi, mais expose également les individus à des risques importants,

notamment des poursuites, des pertes financières et des préjudices personnels. **il est toujours illégal d'y faire des choses illégales**

5 – Avantages d'un VPN.

Un VPN (réseau privé virtuel) est indispensable si vous avez besoin d'une connexion Internet sécurisée et privée pour chiffrer vos données et vos informations personnelles. Un VPN masque votre adresse IP réelle, votre emplacement et vos activités en ligne, des éléments d'information importants à dissimuler pour accéder à des contenus bloqués ou trouver les meilleures offres en ligne.

Au-delà du chiffrement des données, la configuration d'un VPN présente de nombreux autres avantages en matière de confidentialité. Lisez la suite pour découvrir pourquoi un VPN est une pièce incontournable de votre boîte à outils de sécurité.

Les avantages d'un VPN

Les raisons pour lesquelles vous avez besoin d'un VPN sont nombreuses : dissimuler votre activité sur Internet, accéder librement à certains contenus et protéger vos données des espions et des cybercriminels ne constituent que quelques-uns des avantages.

Voici les principaux avantages de l'utilisation d'un VPN :

Contourner les blocages de contenu et éviter la censure

Parmi les principaux avantages des VPN figure leur capacité à débrider les sites web et à contourner les restrictions géographiques qui peuvent limiter l'accès à certains contenus en fonction de votre emplacement. Lorsque vous voyagez, certains contenus en streaming auxquels vous accédez régulièrement chez vous peuvent être soudainement indisponibles à l'étranger. L'utilisation d'un VPN peut vous aider à accéder à toutes vos séries et à tous vos films préférés.

Certains pays limitent ou interdisent également les réseaux sociaux et certains sites web afin d'empêcher leurs citoyens d'accéder librement à l'information sur Internet. Les journalistes et les militants qui opèrent dans des pays fortement censurés, du moins ceux où les VPN sont légaux, comptent sur ces outils pour préserver la confidentialité de leurs communications, accéder aux informations dont ils ont besoin et éviter la surveillance gouvernementale.

Un VPN masque votre adresse IP et utilise l'adresse d'un autre serveur VPN situé ailleurs pour se connecter à Internet. Il semble alors que vous naviguez en ligne à partir de là où se trouve *le serveur*, plutôt que depuis votre emplacement réel. C'est pourquoi les VPN sont si utiles pour regarder la télévision en ligne, accéder à des contenus géographiquement bloqués ou bénéficier d'un service de streaming.

Sécuriser vos achats et vos transactions bancaires en ligne

Dans la mesure où les VPN chiffrent votre connexion Internet, ils sont essentiels pour protéger vos informations personnelles ou financières lorsque vous faites des achats en ligne. Pour la plupart, nous saisissons nos données de paiement ou

accédons à nos comptes bancaires sans y réfléchir à deux fois. Mais si vous utilisez une connexion non protégée, vous pouvez involontairement exposer votre numéro de carte de crédit, les détails de votre compte bancaire, vos mots de passe ou d'autres données personnelles à quelqu'un qui cherche à usurper votre identité. Les pirates informatiques ont plus d'un tour dans leur sac pour obtenir des informations sur les sites web, et même les banques ne peuvent pas garantir une protection totale contre les escroqueries en ligne. C'est pourquoi vous devriez éviter les achats ou les transactions bancaires sur des réseaux non protégés et toujours sécuriser votre propre connexion à l'aide d'un VPN.

Afficher des tarifs stables

La discrimination par les prix en ligne (parfois appelée tarification dynamique) désigne les cas où un site web utilise des algorithmes automatisés pour augmenter dynamiquement les prix. Ces ajustements de prix peuvent être basés sur les forces du marché ou sur des informations recueillies à votre sujet, notamment votre emplacement, votre historique de navigation, vos préférences linguistiques, vos cookies ou même vos revenus.

Vous est-il déjà arrivé de rechercher un jour des billets d'avion et de constater, en revenant plus tard, que les billets étaient plus chers ? Le site web de la compagnie aérienne vous avait en effet indiqué le prix destiné aux nouveaux visiteurs. Lorsque vous revenez, le site web vous reconnaît et vous propose un prix différent, souvent majoré, pour les billets que vous

Établir une connexion sécurisée

Le chiffrement de votre connexion Internet avec une sécurité de niveau militaire est l'un des plus grands avantages de l'utilisation d'un VPN. De nombreuses connexions Wi-Fi publiques gratuites et de nombreux sites non sécurisés (comme les pages http) pullulent sur le web. La connexion à travers un VPN garantit que votre connexion est protégée, même si vous n'avez pas le temps de vérifier le réseau.

Chez vous, pensez à laisser votre VPN activé en permanence. Même s'il est peu probable que quelqu'un tente de pénétrer dans votre réseau domestique, les VPN offrent un niveau de confidentialité supplémentaire pour empêcher votre fournisseur d'accès de voir ce que vous faites. Il existe également des moyens d'améliorer la vitesse de votre VPN pour que vous remarquiez à peine sa présence.

des prix plus élevés en fonction du pays du client et du pouvoir d'achat d'un marché particulier.

La navigation privée et la suppression des cookies de votre navigateur peuvent vous éviter la hausse des prix des vols en fonction de vos visites

Garantir votre anonymat

Si vous cherchez à protéger votre identité sur le web, l'utilisation d'un VPN peut vous assurer une navigation anonyme. En mode VPN, votre activité en ligne et votre identité restent masquées, vous évitant ainsi d'être pisté et de recevoir des publicités ciblées.

À l’instar des serveurs proxy ou de Tor, les VPN dissimulent votre adresse IP et votre emplacement afin de protéger l’endroit où vous vous trouvez physiquement. Cependant, contrairement aux proxies et à Tor, les VPN chiffrent vos données, masquant ainsi votre historique de navigation et garantissant un anonymat en ligne sans faille.
fonction de votre localisation. En masquant votre adresse IP et en rendant presque impossible le suivi de votre parcours, les VPN vous évitent les augmentations de prix et déjouent de nombreuses formes de discrimination tarifaire.

Empêcher le suivi par les FAI et protéger vos données

Votre fournisseur d’accès Internet (FAI) recueille de nombreuses informations sur votre activité en ligne. Les FAI peuvent ralentir la transmission des données sur votre téléphone si vous dépassez votre limite mensuelle ou réduire votre vitesse de connexion si votre activité consomme beaucoup de bande passante, comme avec les jeux ou le streaming.
Mais les FAI peuvent également partager vos données avec des annonceurs, des courtiers en données ou des agences gouvernementales, sans que vous en soyez informé et sans votre consentement. Parmi les avantages majeurs de l’utilisation d’un VPN, notons qu’il empêche votre fournisseur d’accès Internet de surveiller vos activités en ligne, ce qui exclut le partage ou la vente de vos données. Les VPN bloquent également d’autres types de pistage sur le web et vous aident à éviter les plafonnements de données qui ralentissent votre vitesse d’accès à Internet.

Annexe 1

1 - siur le site

- Technologie ! 2009 – VPN por les niuls
- Technologie : 2023 - VPN 2003 – Classemzent etbdescription des produits
- Technologie : 2023 – Architecture VPN (réseaux)

2 : bibliographie

- https://papergeek.fr/deep-web-7-meilleurs-recherche-exploter-face-cachee-web-56526
- 10 navigateurs Web profonds pour accéder au Web profond (techlazy.com)
- 191 liens Web profonds toujours actifs [Mai 2023] (deepwebsiteslinks.com)
- 2000+ Deep Web Links et Dark Web Link [Mise à jour 2023] (deepwebsiteslinks.com)
- Comment accéder au Deep Web (Dark Web) - Guide complet (deepwebsiteslinks.com)
- Comment utiliser TOR pour protéger votre vie privée en ligne (deepwebsiteslinks.com)

- Réseau TOR : principe de fonctionnement (open-freax.fr)

- https://www.avast.com/fr-fr/c-benefits-of-a-vpn#:~:text=Contourner%20les%20blocages%20de%20contenu,en%20fonction%20de%20votre%20emplacement.

Annexe 2 : comment accéder aux sites Web Profond

Si vous ne souhaitez pas lire le guide en entier (annexe1), voici l'essentiel. Les étapes exactes sous une forme plus simple:

1. Si vous êtes un utilisateur Windows, sachez que Windows 10 vous suit intensément. Voici un guide sur la façon de réparer la confidentialité de Windows 10: cliquez ici.
2. Si vous avez corrigé votre confidentialité Windows 10, fermez toutes les applications en cours d'exécution sur votre système.
3. Si votre PC est équipé d'un appareil photo, débranchez-le ou masquez-le à l'aide d'un ruban noir.
4. Téléchargez NordVPN et installez-le sur votre ordinateur, vous pouvez utiliser n'importe quel autre service VPN, mais NordVPN est un VPN avec une politique « Pas de journaux » auditée de manière indépendante. C'est aussi, à mon avis, le plus rapide de l'industrie.
5. Vous pouvez connecter votre NordVPN à n'importe lequel des serveurs disponibles. Mais, alors que vous essayez d'explorer le Web profond, l'une des fonctionnalités exclusives de NordVPN - « Onion Over VPN server » sera le meilleur choix.
6. Une fois NordVPN téléchargé et connecté, téléchargez le bundle du navigateur Tor et installez-le.
7. Lancez le navigateur Tor en cliquant sur l'icône Tor sur votre bureau.
8. Allez dans les paramètres TOR et modifiez les paramètres de sécurité sur « le plus sûr ». (*Voici un guide étape par étape sur Comment utiliser Tor pour protéger votre vie privée en ligne).*
9. Si les étapes 1 à 8 ont été effectuées avec succès, vous êtes prêt à explorer ces liens Web profonds.
10. Si l'un de ces sites sur le Web profond nécessite des informations personnelles, telles que l'e-mail, le nom, l'adresse D.O.B., etc. Utilisez toujours de faux alias sans rapport. Si et quand le chiffrement de la clé PGP est disponible, assurez-vous de l'utiliser. Pour les e-mails anonymes, vous devriez essayer protonmail.

NordVPN est un exemple

Annexe3 : principe de fonctionnement de TOR

TOR, c'est à la base un réseau mondial, comme l'Internet. Il l'utilise pour véhiculer ses données. Sauf qu'au lieu d'emprunter les chemins habituels, vos données se baladent dans une infrastructure différente : d'abord un nœud d'entrée, ensuite tout un tas de relais, et finalement un nœud de sortie.

Prenons un cas concret. Vous voulez visiter ce blog, de façon « classique ». Schématiquement, et en sautant l'étape de résolution du nom (les fameux DNS, qui convertissent un nom « humainement intelligible » comme open-freax.fr en l'adresse IP du serveur qui l'héberge), votre navigateur va envoyer une requête à mon serveur, pour lui demander s'il est « vivant » et lui demander de lui fournir le contenu demandé, la page d'accueil par exemple. Vous comprendrez bien que pour pouvoir vous servir le contenu, il faut que le serveur ait connaissance de votre IP. Et en plus, le chemin que parcourent les « paquets » entre vous et le serveur est généralement fonction de tout un tas de paramètres qui le rendent globalement statique, et donc facile à suivre

Maintenant, vous avez installé TOR, et vous voulez visiter le même site, mais pour des raisons qui ne regardent que vous, vous ne voulez pas que j'aie connaissance de votre IP réelle. En installant TOR, vous aurez déployé sur votre machine un proxy local qui va intercepter les requêtes de votre navigateur, et les re-router au travers de TOR. Mais à la différence du cas précédent, l'itinéraire emprunté par les paquets est aléatoire, et va se perdre entre tous les relais répartis autour du globe. Notez en passant que n'importe qui peut décider d'installer un relais TOR sur son serveur

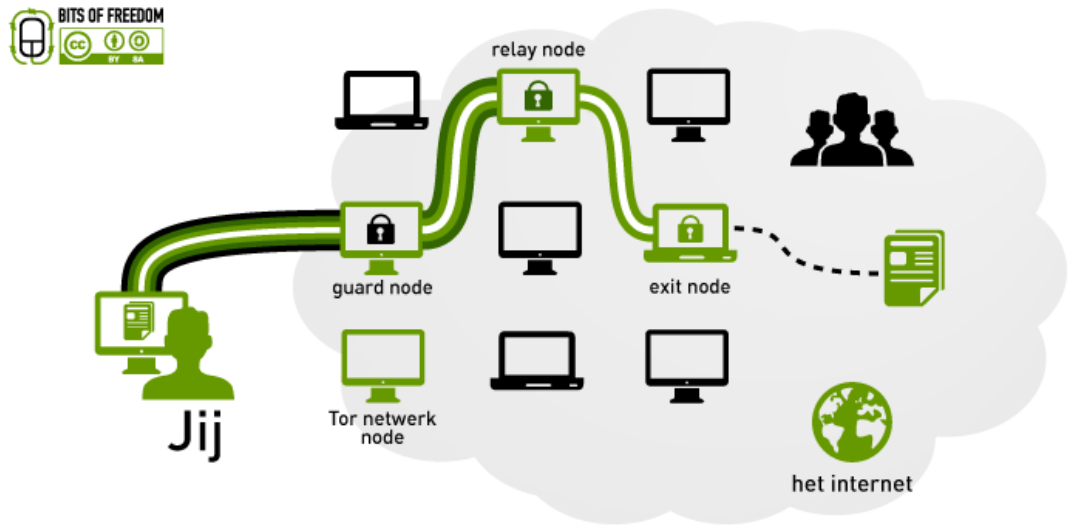
Résultat : pour votre fournisseur d'accès, la communication visible n'est plus directement celle entre vous et mon serveur, mais entre vous et le nœud d'entrée, qui en plus change régulièrement de façon transparente pour vous. Et pour le serveur, eh bien… même principe : pour lui, l'ordinateur qui demande à accéder à une page, c'est le nœud de sortie. Qui change aussi de temps en temps.

Et au milieu de tout ça, il y a les relais, qui n'ont que faire de votre IP, et ne gardent normalement aucune trace de ce qui transite par eux.

Un peu plus en détail…

Où l'on comprend l'analogie avec l'oignon

Pour les plus curieux d'entre vous, on va voir un peu plus précisément ce qu'il se passe lorsque vous utilisez TOR. On se détend, c'est plus compliqué pour les paquets IP que pour vous



Routage

C'est la première des particularités de TOR : le mode de routage (le fait de recevoir et transmettre des paquets) favorise l'anonymisation des flux. On parle ici de « circuit » : votre proxy va établir un chemin international par lequel transiteront vos connexions. Pour chacun des relais, c'est simple : un relais donné n'a connaissance que du relais précédent, et du relais suivant. Un relais n'est donc pas capable de retracer le chemin complet d'un paquet qui lui parviendrait. C'est essentiel !

Chiffrement

C'est l'autre grosse particularité, celle qui évoque le plus les couches de l'oignon. Avant d'êtres transmises par le proxy au nœud d'entrée, vos données sont chiffrées. Plusieurs fois, en plus. Explications :
votre proxy calcule l'itinéraire de vos paquets et établit un circuit. Il va donc choisir des points d'entrée/sortie, et des relais. Chacune de ces machines a sa propre clé publique.
vos paquets sont chiffrés une première fois, avec la clé du dernier nœud du circuit.
le résultat obtenu est chiffré avec la clé de l'avant-dernier nœud du circuit.
et ainsi de suite…
jusqu'à chiffrer le « truc » obtenu par ces chiffrement successifs avec la clé publique du nœud d'entrée.
Vous savez maintenant pourquoi on parle de couches

Pourquoi est-ce qu'on s'embête comme ça ? Simplissime : on chiffre avec des clés publiques, et donc seule la clé privée associée permet de déchiffrer le message. Dans notre cas, le fait que plusieurs chiffrements successifs soient effectués fait qu'aucun des relais n'est capable de déchiffrer entièrement les paquets et de prendre connaissance de leur contenu. Sauf le nœud de sortie, mais c'est normal : il faut que les données soient en clair pour être envoyées au destinataire final !

Résumons

En gros : sur votre machine, le proxy TOR calcule un itinéraire, récupère les clés publiques des nœuds associés, et chiffre vos données avec ces clés publiques, tour à tour. Les données sont chiffrées entre votre ordinateur et le nœud d'entrée, qui déchiffre « sa partie » et transmet au suivant, qui fait de même, et ainsi de suite. Le paquet chiffré perd une « couche » de chiffrement à chaque saut, jusqu'au moment où il va atteindre le nœud de sortie : ce dernier va faire sauter la dernière couche de chiffrement, et transmettre le paquet en clair à son destinataire final.

Comment ça « en clair »

Eh oui. C'est le seul « hic » : TOR ne peut pas assurer (au sens strict du terme) la confidentialité des échanges, puisque le dernier maillon de la chaîne est en clair. Autrement dit, dans le cas d'une confidentialité stricte, seuls vous et le serveur final auriez connaissance du contenu du paquet. Dans le cas de TOR, il faut y ajouter le nœud de sortie, même s'il est incapable de dire d'où provient le paquet.

Vous pouvez donc théoriquement être « écoutés » entre le nœud de sortie et le destinataire final de la communication. Et donc, utiliser TOR ne doit en rien vous dissuader de chiffrer vos fichiers, mails, communications… et d'utiliser le « https » lorsque cela est possible. D'ailleurs, l'extension HTTPS Everywhere dont je parlais rapidement ici est intégrée au navigateur TOR.

Et pour le retour ?

Très juste : on a causé du trajet « aller », mais pas du retour, or si les relais ne peuvent pas déterminer l'itinéraire complet, comment peuvent-ils amener la réponse du serveur destinataire jusqu'à vous, qui demandez à consulter une ressource donnée ?

C'est là que ça se complique. Bien sûr, les tunnels établis au fur et à mesure dans le circuit sont bi-directionnels. Mais encore faut-il que le relais sache si le paquet qu'il reçoit fait partie d'une trame qui vous est destinée, ou si elle est pour quelqu'un d'autre qui aurait une portion de circuit commune avec vous.

Eh bien, les relais ajoutent à tout un tas de mécanismes ce qu'on appelle un *time pattern* (motif temporel) Pour faire simple, on va faire une analogie avec un message échangé en morse : vous envoyez des signaux lumineux, puis attendez un certain laps de temps, puis transmettez la lettre suivante, et ainsi de suite. Cela forme un motif, par définition régulier et répétitif. C'est le même système qui est utilisé entre les relais de TOR. Système qui peut par ailleurs être détourné par un attaquant pour identifier des flux et les séparer, afin de les écouter… Mais c'est hors de notre propos.