

ELU 525:Exploration du web

**Cours sur le web profond**

TABLE DES MATIÈRES

[**INTRODUCTION**](#_rc1znfyb4fd7) **3**

[**I- Généralités sur le web:**](#_9iiozienzzpt) **3**

[I.1- Le web surfacique:](#_4gkcuihiplhr) 3

[I.2- Le web profond ou deep web](#_ethjgkuqodnu) 3

[I.3- Le web obscure ou dark web](#_8b05q04mgvw) 3

[**II- Le Deep web ou web profond:**](#_26rlfdj2sefn) **4**

[II.1- Comment accéder au deep web?](#_86su4vxkkc4l) 4

[II.1-1 Notion de proxy:](#_iog0lg1dkh9h) 4

[II.1-2 TOR( The Onion Router)](#_xczom04z8tzi) 4

[**III- Le contenu du Deep Web:**](#_qffwjbo0x3p4) **6**

# 

# INTRODUCTION

# I- Généralités sur le web:

## I.1- Le web surfacique:

Le web surfacique désigne la partie du web accessible au grand public.Il contient toutes les pages web indexées par les moteurs de recherche classiques.Néanmoins, il ne représente que 10% de l’information qu’on peut trouver sur Internet.Selon une statistique datée du 14 Juin 2015 , 14.5 milliards de pages web sont indexées par Google.[1]

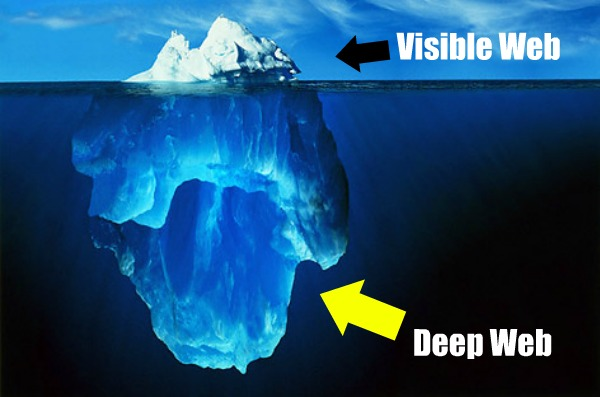
## I.2- Le web profond ou deep web

Le web profond est la partie du web inaccessible par les moteurs de recherche classiques, c’est-à-dire non indexée ou dont le contenu est d’accès limité,. On cite par exemple les sites web accessibles via une connexion sécurisée comme les transactions bancaires sur des comptes en ligne ou bien les vidéos à la demande sur Netflix.[2]

## I.3- Le web obscure ou dark web

Le dark web est le contenu du web qui existe sur des réseaux superposés appelés darknets. Ce sont des petits réseaux pair à pair en plus des réseaux Tor, I2P et autres gérés par des entités privées dont le partage est anonyme (les adresses IP ne sont pas partagées publiquement). Ces réseaux utilisent des protocoles spécifiques intégrant des fonctions d’anonymisation. Le dark web constitue une petite partie du web profond.Le contenu du dark web est divers mais souvent illégal: cybercrime,vente et achat de biens ou services illégaux,partage de fichiers confidentiels,...etc [3].

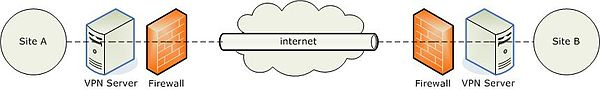
Il faut bien faire la différence entre le deux termes : le *Deep Web* (l’Internet non indexé) et le *Dark Web* (les bas fonds obscurs de l’Internet).



# II- Le Deep web ou web profond:

## II.1- Comment accéder au deEp web?

### II.1-1 Notion de vpn:

****

Un réseau privé virtuel, abrégé VPN – Virtual Private Network , est un système permettant de créer un lien direct entre des ordinateurs distants, en isolant ce trafic. Toutes les données que vont s’échanger les utilisateurs seront donc cryptées, à l’aide de différents protocoles(PPTP, L2TP, …) et passeront par un tunnel sécurisé reliant leurs machines.

Intérêt des VPN : Utiliser un VPN permet aux utilisateurs de garder leur identité cachée. En effet, un VPN permet de ne pas dévoiler son adresse IP ainsi que ses informations personnelles, telles que les mots de passe, sur le Deep Web. Notre adresse IP va être remplacée par une adresse IP étrangère délivrée par un serveur situé à l’étranger. Ainsi, lorsque l’on surfe sur internet, seule cette adresse IP est visible. Un VPN peut également être utilisé d’un point de vue professionnel car il permet de réaliser du travail à distance, en accédant à un réseau interne depuis une autre machine.Toutefois, l’utilisation d’un VPN ne permet pas d’être totalement anonyme sur le Web, les fournisseurs de VPN pouvant toujours avoir accès à nos données personnelles.

<https://fr.wikipedia.org/wiki/R%C3%A9seau_priv%C3%A9_virtuel>

### II.1-1 Notion de proxy:

C’est un serveur qui fait les requêtes sur Internet. L’utilisation d’un service proxy permet de ne pas utiliser votre propre adresse IP et donc de ne pas vous identifier.

Si on établit une connexion à un proxy par un VPN , le contenu des paquets qu’on lui envoie est inexploitable par une personne qui décide de les intercepter puisque le VPN chiffre le contenu des paquets.

<https://openclassrooms.com/fr/courses/2939276-surfez-incognito-sur-internet-avec-le-reseau-tor/2954671-vers-un-debut-danonymat-notion-de-proxy>

### II.1-2 TOR( The Onion Router)

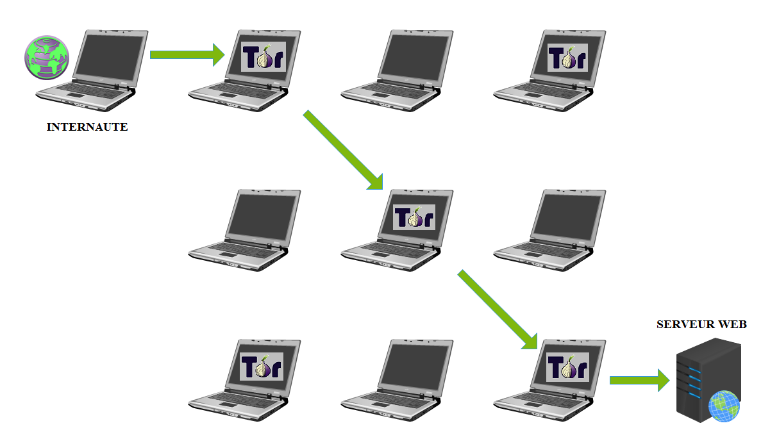
Tor est un réseau informatique superposé mondial et décentralisé. Il se compose d’un ensemble de **proxies,** appelés relais . Ce réseau permet d’**anonymiser les paquets TCP** .

Dans un réseau Tor, la requête d’un internaute quitte son ordinateur et passe par plusieurs autres ordinateurs présents dans le même réseau et utilisant Tor jusqu’au serveur à qui est adressé la requête. Il est le seul à pouvoir déchiffrer le contenu cette requête .C’est le principe du routage en oignon (qui donne son nom à Tor).Contrairement à un réseau normal, les paquets tor prennent un chemin aléatoire. Le client négocie un ensemble de clés de chiffrement pour chaque nœud emprunté par les paquets.Les figures ci-dessous schématisent le fonctionnement de Tor et le fonctionnement d’un réseau normal:

Réseau normal:



Réseau Tor:



Tous les échanges entre relais Tor sont sécurisés et cryptés. Tor propose également à ses utilisateurs un ensemble de services cachés sur internet en masquant l’identité (adresse IP, …) du serveur qui les héberge ; ce dernier recevra de Tor une adresse avec l’extension ".onion" (comme par exemple "nomdusite.onion") et ne pourra être accessible que par des internautes du réseau Tor. L’accès d’utilisateurs à un service web caché se fait selon un protocole défini par Tor.

Pour accéder au réseau Tor il faut utiliser le navigateur du même nom : Tor Browser. Le **logiciel Tor Browser** permet d’aller sur le réseau Tor, et donc de consulter les sites du deep web.

<https://www.supinfo.com/articles/single/3109-deep-web>

## Fonctionnalités de TOR:

Tor propose à ses utilisateurs des fonctions axées sur la vie privée:

* **Suppression des cookies après chaque session** – Tor supprime tous les cookies d’une session juste après sa fermeture.Cette suppression s’assure de ne laisser aucune trace de vos navigations.
* **Des niveaux de sécurité**: Différents niveaux de sécurité sont conçus afin de neutraliser les attaques contre votre navigateur.
* **Une nouvelle identité** :Il est possible de changer totalement votre session de navigateur. Si vous utilisez d’utiliser cette fonction, le navigateur TOR va redémarrer en effaçant toutes les informations de votre navigation.
* **Accéder à des sites en .onion** :C’est l’une des particularités de TOR. Il propose des sites avec une adresse en .onion accessibles uniquement via le navigateur TOR.

<https://meilleurvpn.net/19119/navigateur-tor/>

### 

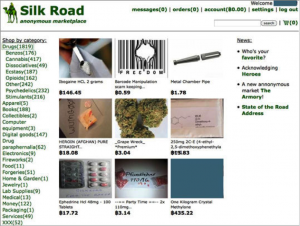
### 

# III- Le contenu du Deep Web:

Cette couche internet, possède sa propre monnaie(les Bitcoins), ses propres codes(Confiance) et ses propres modes d’accès (TOR).

Afin d’atteindre la majorité des sites non référencés, il faut également passer par TOR, un navigateur anonyme. Aussi, il faut connaître à l’avance les adresses que l’on souhaite visiter qui ressemblent souvent à cela :kpvz7kizv5agwt35.onion .

Tout au long de la recherche on peut souvent tomber sur des plateformes de e-commerce comme Silkroad.

Tout comme Amazon Marketplace, il suffit de créer un compte sans informations personnelles, ensuite laisser le moteur de recherche remuer la base de données des différents produits mis en ligne par les vendeurs. On pourra facilement repérer le produit qui nous intéresse.  
Par exemple, il est possible de choisir parmi les quelques milliers de drogues proposées : hash, héroïne, cocaïne ou LSD… Tout d’abord il faut se mettre en relation avec le vendeur, ensuite, lui envoyer l’adresse de livraison cryptée, il sera la seule personne en mesure de lire et enfin lui payer en Bitcoins : une monnaie 100% virtuelle développée par un japonais « Satoshi Nakamoto ».  
****

****

Silkroad une plateforme d’e-commerce appartenant au Deep Web pose un gros problème aux forces de l’ordre vue que premièrement il n’y a pas de trace postale : adresse cryptée connue que par le marchand, deuxièmement il n’y a pas de trace digitale : Tor presque intraçable et enfin et surtout il n’y a pas de trace de transaction monétaire : les bitcoins passent de compte en compte sans arrêt et sont impossible à suivre.

Les fondateurs de Silkroad ont décidé d’ouvrir the Armory, car comme bons entrepreneurs, ils cherchent à se diversifier. Mêmes principes les vendeurs proposent dans cette plateforme des biens qui sont des armes.

On peut donc selon les stocks acheter un AK-47, que l’on pourra se faire livrer par la poste, ou en dead-drop (on donne des références GPS et le vendeur pose/enterre/cache le produit aux coordonnées).

Le deep Web ne se limite pas uniquement sur Silkroad, mais on fait assez de découvertes en passant de lien en lien.

on peut également trouver de petites annonces de tueurs avec des tarifs différenciés selon les tâches demandées et selon le type de personne : prenons comme exemple 10 000 euros pour une personne normale, 50 000 pour les politiciens...



de plus, on peut acheter des numéros de cartes bancaires ou de “clones” avec le code PIN dans le but de l’utiliser en magasin ou pour des retraits.

En outre, on peut également acheter un diplôme: avec inscription dans la base de données de l’école concernée, faire des faux papiers, faire disparaître une personne de tout base de donnée (de son compte en banque, de la sécurité sociale)...

**Références Bibliographiques**

[1]Article sur Wikipédia: <https://en.wikipedia.org/wiki/Surface_web>

[2] Article sur Investopedia: <https://www.investopedia.com/terms/d/deep-web.asp>

[3] Article sur Wikipédia: <https://en.wikipedia.org/wiki/Darknet#Uses>