# Qu'est-ce que TOR?

## Le Routeur Onion

### FAITS

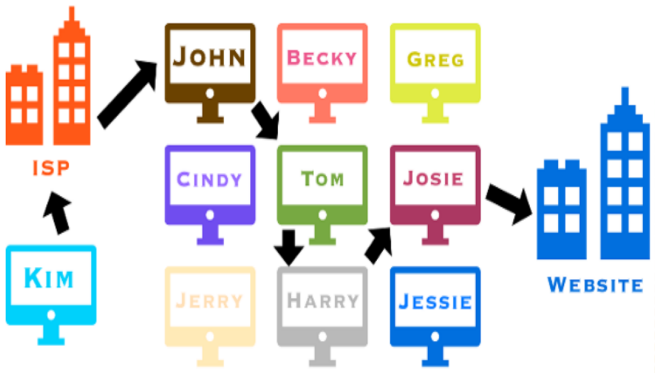
- TOR signifie en anglais The Onion Router, soit le Routeur Onion
- Le logiciel TOR fut développé par le Laboratoire de Recherches Navales des Etats Unies pour protéger la communication des renseignements
- TOR vise à cacher l'identité des utilisateurs et leurs activités en ligne de la surveillance et de l'analyse de trafic
- TOR a un usage légitime pour les utilisateurs souhaitant garantir leur vie privée ; contourner la censure ; ou se protéger de régimes répressifs ou du contrôle ciblé

## Comment ça marche?

TOR détourne le trafic à travers un réseau de manière à dissimuler la localisation d'un utilisateur ou son identité. Au lieu de transporter des trafics telles que des visites sur des sites web ou des messages instantanés par une route fixe prévisible [de l'utilisateur 'Kim' vers le site web], TOR passe par une route attribuée de façon dynamique qui devient introuvable.

La connexion TOR est cryptée. Un lien encrypté est exposé à la surveillance, permettant à quelqu'un de savoir quels sites web vous visitez en remontant jusqu'à votre adresse IP*.
Néanmoins, TOR utilise une connexion cryptée ce qui signifie qu'à n'importe quel point du parcours de l'utilisateur internet d'origine à la destination convenue, ce n'est pas clair d'où les données viennent et où elles vont.

** Une adresse IP reflète l'identité de l'utilisateur d'un appareil [voir fiche d'informations: Qu'est-ce qu'une adresse IP?]*




**Figure**

Lorsque Kim visite un site web à travers le réseau TOR, ses trafics prennent un chemin au hasard par les ordinateurs d'autres gens pour arriver au site web. A chaque point intermédiaire, les informations sur la source ou la destination sont retirées pour rendre l'identification de l'utilisateur extrêmement difficile. Par conséquent, les Fournisseurs de Services Internet ne peuvent pas trouver qui elle est et quels sites elle visite. Ou bien TOR présente de manière trompeuse le dernier nœud de sortie [Josie] comme source de communication.

## TOR appliqué à l'Exploitation

Les auteurs d'abus sexuels utilisent TOR pour parta des images d'abus sexuels d'enfants ou autres contenus facilitant et perpétuant une culture d'abus sexuel d'enfants. De plus, TOR leur permet de se connecter à des victimes potentielles de manière anonyme. En outre, les services cachés de TOR permettent à des délinquants de communiquer en secret les uns avec les autres. En utilisant TOR, les auteurs évitent de révéler leur localisation ou leur identité, évitant ainsi la détection par les Fournisseurs de Services Internet (FSI) et organismes d'application des lois. De cette manière, TOR complique l'identification des victimes et des auteurs.

TOR est le programme logiciel le plus populaire utilisé pour accéder à des parties d'Internet volontairement construites de manière à ne pas être vastement disponibles ni facile à utiliser. On s'y réfère également en tant que DeepWeb ou Darknet (ce dernier indiquant la nature [illégale] des comportements exécutés dedans). On ne peut accéder à ce réseau plus 'dissimulé' ou anonyme d'ordinateurs qu'en utilisant un logiciel spécial, tel que TOR.