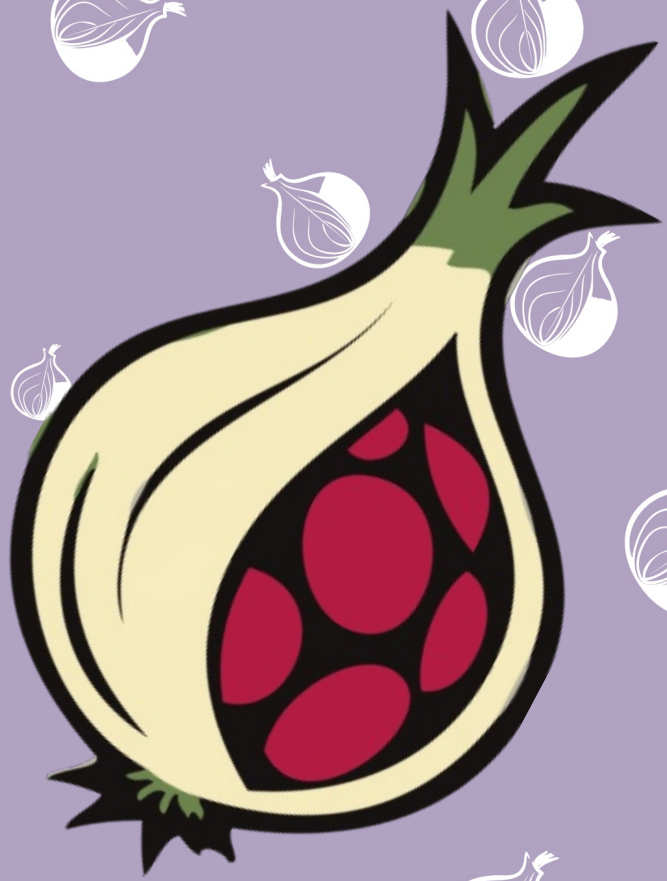


Initiation cosmico-féline à TOR en mode PiFi

A propos de Tor

Qu'est-ce qu'un routeur TOR?

Acronyme de The Onion Router ("le routeur oignon"), TOR est un réseau superposé décentralisé à l'échelle mondiale et qui repose sur le principe de réseau mélangé. Si l'oignon a été choisi comme emblème des faits d'armes de TOR sur la Toile, ce n'est pas parce que ses développeurs jouent à Monsieur-l'oignon-l'andouille, c'est parce qu'il est composé de routeurs organisés en couches, appelés nœuds de l'oignon, qui transmettent de manière anonyme des flux TCP (Transmission Control Protocol ou "protocole de contrôle de transmissions").

Si l'on fait abstraction des tactiques de noyautage mises en place par la NSA pour contrer cette particularité et d'autres subtilités à étudier sérieusement pour garantir une quasi-impossible intraçabilité totale sur les réseaux, le réseau TOR est supposé rendre anonymes tous les échanges Internet basés sur le protocole de communication TCP. TOR propose en effet à ses utilisateurs un ensemble de services cachés qui ont pour but de publier des sites internètiques ou de proposer d'autres services sur Internet en cachant l'identité du serveur qui les héberge. Ils permettent ainsi de cacher l'adresse IP, donc les coordonnées géographiques, de serveurs utilisant ce service caché.

De nombreuses ramifications

Plusieurs logiciels tirent parti du réseau TOR :

- TOR Browser : service phare du projet TOR, il inclut un proxy TOR, un navigateur web Mozilla Firefox ESR modifié ainsi que les extensions Firefox TORButton, TORLauncher, NoScript et HTTPS-Everywhere, préconfigurés pour protéger l'anonymat sans devoir installer aucun autre logiciel. Il peut être exécuté depuis des médias amovibles et il est disponible pour Windows, Mac OS X, et GNU/Linux ;
- Bitmessage : messagerie anonyme qui utilise le réseau I2P (similaire à I2P-Bote) ;
- Syndie : forums et blogs en architecture distribuée ;
- Vuze (ex Azureus) : client Bitorrent.

Plusieurs systèmes d'exploitation axés sur la sécurité font un usage intensif de TOR : Tails (The Amnesic Incognito Live System), Anonym.OS, Hardened Linux From Scratch, Incognito, Liberté Linux, QubesOS, TOR-ramdisk ou encore Whonix. Des initiatives telles que The Guardian Project s'appuient également sur les ressources TOR anonymisantes.

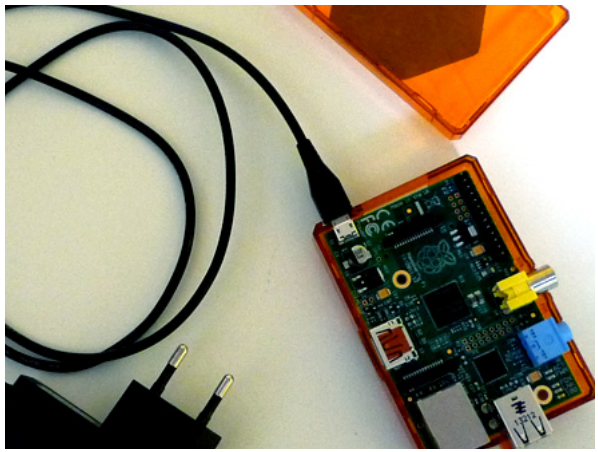
Source : Wikipédia

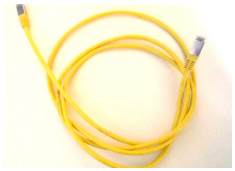
Pré-requis

Cet atelier est une adaptation des instructions listées par le tutoriel "*How to Bake an Onion Pi*" du magazine MAKE (également disponible à l'url suivante : http://makezine.com/projects/make-36-boards/how-to-bake-an-onion-pi).
Plusieurs outils et matériels sont nécessaires pour réaliser correctement l'initialisation d'un routeur TOR en mode PiFi.

- un RaspberryPi (modèle B 512 pour cet atelier) et tout ce qui va avec : alimentation, carte SD initialisée et distribution Linux adéquate (Raspbian dans notre cas),
- boîtier, moniteur de type écran PC ; clavier & souris USB peuvent s'avérer utiles,
- un câble HDMI,
- un câble Ethernet,
- **Et surtout :** Un routeur.

Les Chats Cosmiques ont opté pour un nano-adaptateur wifi-USB Edimax EW-7811UN (clé USB sans fil 150 Mbps) mais on vous recommande chaudement de consulter des ressources telles que http://elinux.org/RPi_USB_Wi-Fi_Adapters (en anglais only malheureusement) pour vérifier vous-mêmes la compatibilité des différents systèmes d'exploitation et services RaspberryPi avec la multitude de matériels disponibles (antennes, modems, etc).





Note préliminaire : commandes sur le RasPi

Pour cet atelier, on part du principe que le RaspberryPi a d'ores et déjà été initialisé de manière appropriée. Deux possibilités s'offrent à nous suite à l'initialisation du Rasppberry Pi (cf. atelier préliminaire) :

- Soit une session utilisateur est désormais ouverte via le serveur SSH sur le Rpi, auquel cas toutes les opérations qui suivent sont réalisées à travers la liaison SSH ouverte depuis un autre PC.
- Soit on réalise ces mêmes opérations directement sur le Rpi avec clavier/souris/écran, à condition qu'ils soient correctement reliés au Rpi.

Dans les deux cas, on est en mode invite de commande de la manière suivante :

```
pi@CosmiKats ~ $ _
```

Connexion à l'Ethernet / Wi-Fi

Lorsque cette ligne de commande apparaît, on connecte le RasPi à une box avec un câble Ethernet classique.

Afin d'obtenir deux scripts nécessaires à l'installation du PiFi et généreusement mis à la disposition du grand public par MAKE, on saisit simplement la commande suivante :

```
pi@CosmiKats ~ $ wget makezine.com/go/onionpi
```

Puis on valide avec "Entrée" afin que le téléchargement des fichiers commence. Le RasPi nous avertit quand le téléchargement est complet et si la connexion au routeur fonctionne correctement. Dans le cas contraire, un message d'erreur de type "failed: Name or service not known" devrait apparaître. Pas d'autre choix alors que de vérifier que tout est bien branché, que le routeur est bien configuré en protocole "DHCP" et, si cela ne fonctionne toujours pas, on reprend à l'étape "Activation du service SSH" du tutoriel RaspberryPi :o).

Puis, pour extraire les scripts du fichier compressé qu'on vient de télécharger, il suffit alors de saisir la commande :

```
$ unzip onionpi
```

Une fois cette opération effectuée, on éteint le Rpi avec la commande suivante :

```
$ halt
```

Initialiser un point d'accès PiFi

Si vous ne maîtrisez pas du tout les commandes Linux, à partir d'ici c'est une question de confiance entre le site MAKE, les Chats Cosmiques et vous. Par contre, si vous le désirez, vous pouvez mettre directement votre truffe dans le code et modifier tous les détails de la configuration système fournie dans ces scripts pour l'adapter à vos propres objectifs.

Il s'agit de configurer le RaspberryPi afin qu'il mette en place un service WiFi et qu'il route un réseau sans fil connecté à Internet. Or **pifi.sh**, l'un des scripts que l'on vient de télécharger permet justement de mettre en place une telle configuration et la procédure pour exécuter ce script est relativement simple.

On commence avant tout par plugger notre nano-adaptateur USB-WiFi au Rpi éteint. Puis on le rallume en le débranchant / rebranchant.

Après avoir redémarré le RasPi, il est nécessaire de se relogger avec les identifiants utilisateur et mot de passe correctement renseignés auparavant dans le menu ***raspi-config*** (cf. tutoriel RaspberryPi). dans notre cas, on obtient de nouveau l'invite de commande suivante :

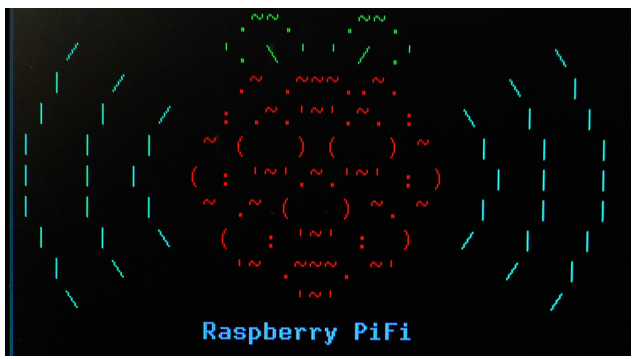
```
pi@CosmiKats ~ $ _
```

Il est alors juste nécessaire de saisir la commande suivante pour exécuter le premier script :

```
$ sudo bash pifi.sh
```

À moins qu'on ne souhaite interrompre la manip', on valide avec 2 fois "Entrée" et l'exécution du script envahit l'écran.

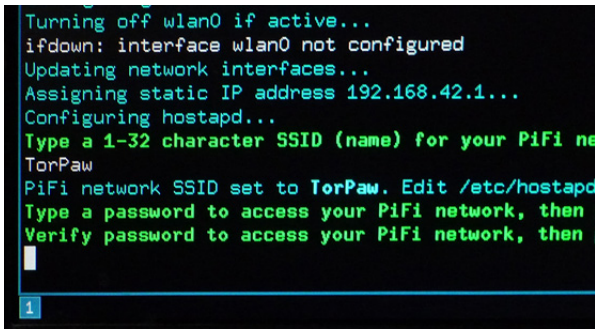
NB : Pour les chatons les plus téméraires et les moins paresseux, il est également possible d'ouvrir le script **pifi.sh** sur un autre moniteur puis de saisir ligne par ligne les commandes qui y sont compilées afin de mieux comprendre pas à pas les commandes mises en oeuvre et les réponses apportées par le système. Les lignes de code sont commentées (mais c'est en anglais dans le texte :oS).



Nommer le réseau PiFi

Le RasPi nous demande alors de renseigner une identification SSID pour ce nouveau réseau sans fil, ainsi que le mot de passe requis pour y accèder. Dans notre cas, il s'agit de TorPaw // Apollo11. Le Rpi nous demande de reconfirmer le mot de passe. On valide à chaque fois avec "Entrée" :

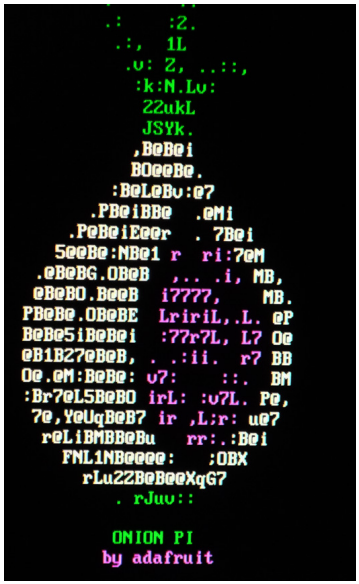
Une fois le script exécuté, le RasPi devrait redémarrer automatiquement et les terminaux alentours (PC, tablettes, smartphones, etc.) devraient voir apparaître dans leurs listes de réseaux sans fil le nom du réseau que l'on vient de créer. Une fois saisi le mot de passe, on devrait pouvoir accéder à n'importe quelle page web fonctionnelle. Et si l'on souhaitait uniquement configurer le Rpi en routeur de réseau sans fil sans les fonctionnalités TOR, on peut s'arrêter là.



Anonymiser le réseau avec TOR

Toujours sur la base de notre contrat de confiance avec MAKE, il est aussi très simple de passer à la seconde étape, à savoir anonymiser le réseau WiFi qui vient d'être créé avec un second script d'ores et déjà téléchargé et dézippé. Vu que le RasPi a automatiquement redémarré, on est de nouveau confronté à l'invite de commande et il suffit de saisir la commande suivante pour exécuter ce deuxième script :

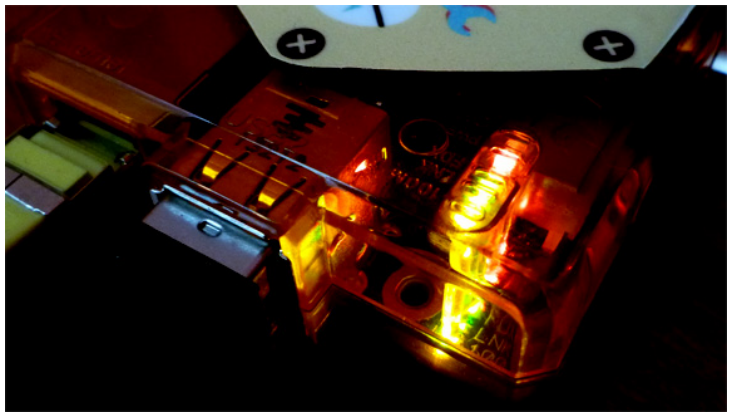
$ bash tor.sh



Again, à moins qu'on ne souhaite interrompre la manip', on valide deux fois avec "Entrée", et l'exécution du script qui envahit l'écran nous procure une vive émotion, à la vue de ce magnifique logo ASCII d'oignon qui n'attend que nous pour se joindre à la bande des joyeux pirates qui luttent mondialement contre le réchauffement climatique :o).

Si tout va bien, le Rpi reboote automatiquement et le proxy TOR ne sera pas fonctionnel avant ce redémarrage.

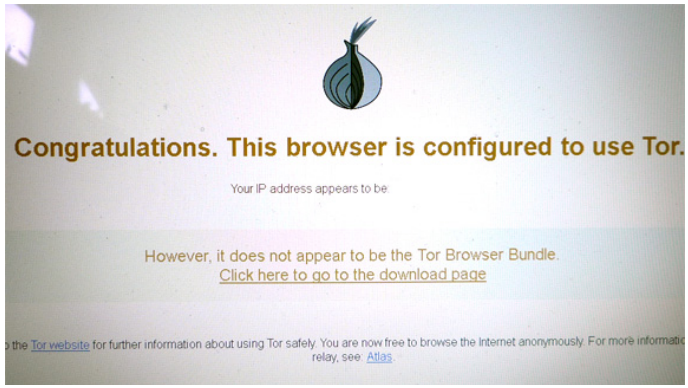
NB : On le dira jamais assez : ça peut valoir la peine d'examiner plus en détail le fichier source du script et les commandes, relativement simples, qui permettent cette installation du logiciel TOR et l'actualisation de l'iptables Linux afin que toutes vos actions soient automatiquement reroutées via TOR.



Arborez fièrement le pavillon TOR...

Désormais, votre RaspberryPi génère une réseau "PiFi" sans fil auquel vous pouvez accèder depuis n'importe quel PC, smartphone, tablette, etc. À chaque fois que vous l'allumez, vous contribuez également aux reroutages anonymisateurs du réseau mixte TOR à l'échelle mondiale.

Rendez-vous sur check.torproject.org. Si votre PiOnion fonctionne correctement, vous devriez voir apparaître un écran ressemblant à l'image ci-contre :



VOIR TOUJOURS PLUS LOIN, VISER TOUJOURS PLUS HAUT

La connexion Ethernet est la plus rapide et la plus simple pour obtenir le protocole DHCP mais vous pouvez également configurer un proxy WiFi à WiFi. Pour cela, vous aurez besoin de deux nano-adaptateurs USB wifi connectés sur le RaspberryPi et d'éditer les paramètres dans le menu /etc/networks/interfaces afin d'ajouter une interface wlan1 en renseignant la SSID et le mot de passe correspondant à votre fournisseur d'accès à Internet.
Il est aussi possible de configurer TOR afin d'obtenir une IP qui semblerait provenir d'un pays de votre choix.

Si vous êtes passionné de TOR, vous pouvez également le rendre plus rapide et plus efficace en devenant un noeud de sortie TOR. Enfin, vous pouvez également envisager de faire des dons au projet TOR.
Pour en savoir plus sur toutes des actions complémentaires, consultez TorProject.org ainsi que le site https://learn.adafruit.com/onion-pi/do-more-dot-dot-dot.

...Mais restez vigilants !

Utiliser TOR, c'est bien. Redoubler d'attention, c'est mieux.

Si les connexions sont chiffrées jusqu'aux nœuds de sortie, une fois sorti de ces derniers, la seule manière d'empêcher quelqu'un de savoir quelles informations transitent est de passer en https. Si vous ne le faites pas, il est possible de savoir ce que vous lisez, écrivez, consultez, mot-de-passez... D'une, évitez donc de vous connecter à TOR si c'est pour vous précipiter sur vos sites habituels et vous identifier illico. De deux, évitez vraiment de vous connecter à TOR si c'est pour vous précipiter sur vos sites habituels et vous identifier illico.

De même, vous serez identifiés en ligne comme un utilisateur de TOR et donc vous pouvez vous retrouver bloqués sur certains sites qui refusent l'anonymat (par exemple Wikipédia).

Vous risquez même d'être par défaut considérés comme potentiellement suspects et cibles "légitimes" de surveillance accrûe de la part d'organismes bien intentionnés. Les révélations d'Edward Snowden ont ainsi suggéré que TOR est la cible privilégiée d'attaques malveillantes de la part de la NSA, qui estime que "TOR pue" et que toute recherche d'anonymat en ligne est suspecte, donc mérite d'être sapée.

TOR vous donne donc de meilleures chances de ne pas être tracé, mais nul n'est jamais certain d'être invisible à 100%.

Licence