Tutoriel Tails

Août 2019 version TAILS 3.15

Table des matières

Quelques explications

The **A**mnesic & **I**ncognito **L**ive **S**ystem

>>> Tails est un ***Système*** d'exploitation. Tout le monde connaît les systèmes d'exploitation. Si je vous dis « Windows » ou « Mac », ça devrait vous parler. Je devrais préciser *Mac Os X* pour être exact, ou *Windows 8* pour préciser la version. D'autres systèmes d'exploitation existent. Peut-être avez-vous déjà entendu parler de *Linux* ou de *Ubuntu* ?

GNU/Linux (le nom complet de *Linux*) est en quelque sorte une famille de systèmes d'exploitation. Dans cette famille, on trouve une sous-famille qui s'appelle *Debian* (prononcez « débiane »). Et dans cette sous-famille, on trouve *Ubuntu* et *Tails*. *Tails* est une distribution (une version) de Linux.

Un système d'exploitation est une sorte de super-logiciel, qui fait tourner un ordinateur de manière compréhensible à un.e humain.e comme vous et moi.

➔ Tails est un système dit ***Live***. Ça veut dire qu'il ne s'installe pas sur un ordinateur. Il s'installe généralement sur une clé USB (ou une carte SD ou même un DVD). Lors de son utilisation, l'ordinateur fonctionne uniquement sur cette clé. D'ailleurs, cet ordi peut ne pas avoir de disque dur, son système d'exploitation habituel peut être complètement planté ou surchargé, peu importe, ça marchera pareil, il ne s'en servira pas.

➔ C'est ce qui lui permet d'être ***Amnésique***. Par défaut Tails est conçu pour ne pas laisser de traces sur l'ordinateur une fois que la session est terminée. La clef utilise uniquement la mémoire vive de l'ordinateur (mémoire plus volatile que le disque dur), qui est nettoyé à l'éteignage. Elle est faite aussi pour, par défaut ne pas installer de nouveaux logiciels (même si on verra que c'est possible) et revenir à son état initial après chaque redémarrage.

➔ *Tails* est aussi un système qui vous permet d'être ***Incognito***. Il cache les éléments qui pourraient révéler votre identité, votre localisation, le contenu de ce que vous échangez, etc.

➔ Tails est conçu pour faire de la sécurité informatique, elle est aussi bien utilisée pour des activistes, journalistes, toutes personnes souhaitant limiter ses traces numériques (pour des raisons politiques ou de protection), des mafieux, des militaires,… Un environnement minimal, fonctionnel et vérifié est déjà installé (avec de quoi faire un minimum de traitement de texte, traitement d'image, de son, de vidéos,…). Elle intègre des outils de chiffrements et de suppression de données qui se veulent simples et tout un tas de protections contre des types d'attaques sont pensées.

➔ La sécurité numérique d'aujourd'hui ne vaudra plus rien demain. **La protection des données personnelles passent par les mises à jour, il est important de les faire dans des délais raisonnables**. Il n'existe pas d'outils informatique de protection de données fiable s'ils ne sont jamais mis à jour, pour faire confiance dans le temps dans ces outils il est bien de vérifié que des équipes travaillent en continu dessus, sont réactives, et leur réputation sur le net.

Il faut bien comprendre l'état d'esprit de *Tails* : tout y est fait pour être sécurisé au maximum. Cependant en informatique il n'existe pas d'outil tout puissant, il y a toujours

des limites (on verra à la fin de la brochure quelques unes). Qui plus est **la manière dont vous utilisez Tails peut générer des failles**.

Des inconvénients existent, qui découlent de la volonté d'être amnésique et incognito : espérance de vie moindre d'une clef usb, possibilité de la perdre ou d'oublier sa phrase de passe (et toutes les données qui vont avec), difficulté d'utiliser certains outils non programmés par défaut, limites de la mémoire vive.

Tails est un « logiciel » libre. **Chacun peut en consulter le code source (la recette), le récupérer, le modifier, et le redistribuer tel quel ou modifié** …

Tails essaye de fonctionner au maximum par dons afin d'être indépendant et d'avoir des outils permettant d'améliorer la sécurité. Son coût est estimé à 5 euros par an et par utilisateurices. De la même manière il est possible d'aider de plein de manières possibles son fonctionnement (même sans être geek, par exemple la traduction)[1].
Les outils et services utilisés (Tails, TOR, Riseup, GPG,...) sont des services à prix libre, mutualisés, militants, accessibles à touTEs et qui ne vivent QUE par l'implication de touTEs (en temps, argent ou autre).[2]
Par contre, il faut absolument s'assurer que la version de *Tails* en votre possession est saine. C'est essentiel. Ne négligez pas les étapes de vérification. Heureusement, des outils existent pour ça, et sont bien vulgarisés sur le site de Tails.

Notion de modèle de menace

Tails n'est pas magique et comporte plein de limites. Internet et l'informatique sont un monde de truands qui ont leur économie et leur pouvoir basé sur le vol de données. Tails ne vous protège pas des failles humaines, de mouchards matériels directement intégrés à l'ordinateur, d'un mouchard logiciel sur le bios, d'être vérolé, ou de certains types d'attaques. Il n'existe pas de sécurité absolument parfaite sur internet, d'où l'intérêt de pouvoir faire un modèle de menace en informatique :
Contre qui je me défends, quelles sont ses moyens, quelles sont les conséquences s'ielle à accès à telles données, quels moyens je peux mettre en œuvre. En fonction de ça des réponses différentes peuvent être posées.

1 Pour cela on peut se référer à ce lien : https://Tails.boum.org/contribute/index.fr.html
2 Pour consulter des sites qui proposent des logiciels ou hébergements avec de la sécurité informatique vous pouvez fouiller par ici : https://riseup.net/en/security/resources/radical-servers, ou par ici : https://prism-break.org/fr/

I) Bases pour utiliser Tails

Préalable

Tails ne marche pas avec des ordinateurs en 32 bit (vieux ordis, la plupart sont en 64 bits). Il marche uniquement sur des clefs usb ou des cd de plus de 8 Go, si c'est un cd il n'est pas possible d'avoir de persistance. Les données seront complètement effacées à l'installation, donc sauvegarder avant tes données ailleurs, et si tu veux qu'on ne retrouve pas de traces de ce qu'il y avait avant consulte la partie « supprime vraiment tes données ».

Certains modèles d'ordinateurs ou de clef usb ne fonctionnent pas avec Tails, ou certaines fonctionnalités ne marche pas, ou il faut des astuces pour la faire marcher. Pour savoir cela n'hésite pas à consulter la documentation de Tails qui recense certaines de ces problématiques.

Si c'est trop lent, il est possible d'augmenter la RAM de ton ordinateur (mémoire vive), y en a pas mal sur le bon coin, n'hésite pas à y mettre 4 Go ou plus (ça marchera avec moins mais faudra pas que t'ouvres trop de logiciels en même temps).

Comment utiliser ce tuto ?

Ce tuto est en plusieurs parties : la première comporte plutôt les bases pour se lancer sur Tails, certaines parties abordent plus des cas spécifiques (à voir celui qui peut te concerner). La 2ème partie comporte des astuces, sur des logiciels intégrés dans Tails. Dedans il y a aussi des éléments qui sont plus complexes / moins nécessaires pour utiliser Tails. La 3ème porte plus sur des astuces et bug que tu risques de rencontrer avec ta clef Tails (pour éviter de la mettre de côté dès le 1er problème, le plus souvent la solution est simple), ainsi que les marches à suivre pour faire des sauvegardes de ta clef Tails.

Une partie de ce tuto vient de copier-coller d'autres tutos déjà existant un peu mis à jour.

Installation

Pour installer *Tails* sur une clé, il vous faut une « source » et … une clé USB supérieur à 8 Go.

Concernant la « source », deux solutions :

- **[SOLUTION 1]** Trouver un utilisateur de *Tails*
- **[SOLUTION 2]** Utiliser le fichier d'installation de *Tails* téléchargeable sur internet

[SOLUTION 1] : Ca consiste à trouver un-e utilisateur/trice de *Tails* en qui on a confiance. Car dans *Tails*, un petit logiciel très simple permet de créer une nouvelle clé *Tails* en quelques minutes et trois clics. La procédure est expliquée plus loin dans cette brochure. En plus, ça permet d'en discuter avec quelqu'un-e, et de voir des vrais gen-te-s dans la vraie vie. L'inconvénient de cette méthode c'est que si cette source n'a pas été vigilante elle peut diffuser une clef vérolée (cf partie clef vérolée)

Près de chez toi existe probablement un-e utilisateur-trice de Tails ! Rapproche-toi des assos qui défendent les logiciels libres, des fournisseurs d'accès à internet (FAI) associatifs, des hébergeurs militants, etc … (tou.tes ne font pas forcément de la sécurité informatique) Tu peux jeter un coup d'œil à l'agenda de l'asso *April*, avec des rendez-vous fréquents dans toute la France, ici :
https://www.april.org/aggregator/sources/1
Ou une petite listes de FAI associatifs là :
https://www.ffdn.org/fr/membres

[SOLUTION 2] : Il faut suivre le guide d'installation de *Tails* depuis le site *https://Tails.boum.org/install/index.fr.html*. A partir de là le site de Tails t'accompagnera pas à pas, il est important de suivre la totalité du tutoriel qui est très bien fait.

Booter sur ta clef Tails

Pour les Mac : la première chose à essayer est, tout de suite au démarrage, d'appuyer de manière continue sur la touche Alt (appelée touche options), ou le symbole est quelque chose comme : ⌥ . L'écran qui devrait suivre comportera deux icônes, dont l'une représente une sorte de clé USB et est sous-titrée *« EFI Boot »* (voir l'image ci-dessous, attention parfois ça a un autre nom, parfois ça s'appelle windows car mac croit qu'il n'existe pas d'autre système d'exploitation que lui même et windows). Cliquez dessus, et vous devriez obtenir l'écran de démarrage de *Tails*.
Si Mac OS démarre sans que vous n'ayez cet écran avec les deux icônes, il se peut que vous deviez effacer la mémoire NVRAM de votre mac (renseignez-vous avant de le faire[3]). Au démarrage, appuyez simultanément sur quatre touches :

3 Plus d'infos en français ici : https://support.apple.com/fr-fr/HT204063

Command (⌘) + Alt (⌥) + P + R , jusqu'à entendre une deuxième fois le son de démarrage de l'ordi. À partir de là, gardez uniquement la touche Alt (⌥) maintenue, et vous devriez arriver à l'écran qui vous permettra de choisir *« EFI boot »* (des fois ça s'appelle autrement, ça peut même s'appeler windows car mac croit qu'un autre système d'exploitation que lui est forcément un windows, des fois y a plus d'options)

Pour les PC: Il faut au démarrage configurer le bios. Le « Bios » (ou pour les ordis récents on va chercher « UEFI ») est un logiciel qui vient avant que l'ordi démarre sur le système d'exploitation, il gère notamment le démarrage de votre machine, en lui disant quel disque utiliser pour commencer à faire quelque chose.

Au moment ou tu démarres il faut appuyer la plupart du temps sur F2, ou F12, ou F6, ou suppr, ou echap, ou une touche spéciale, ou parfois une combinaison de touches…

Des fois il y a aussi un autre menu qui s'appelle le « boot order » ou «option de boot » c'est encore plus simple tu fais entrer sur ta clef ou tu montes ta clef en premier et lances le démarrage.

Bref les solutions sont multiples :

1) quand t'appuies sur démarrer tu fais des allés retour en appuyant sur toutes les touches F, ainsi que echap et supprimer. La plupart du temps ça marche mais faut bien aller vite. L'inconvénient c'est que des fois y a un autre truc inutile qui démarre sur un autre Fx du coup faut redémarrer et faire la même procédure sans ce F. Bon des fois ça lance un truc dans le bios en même temps, tu fais annuler.

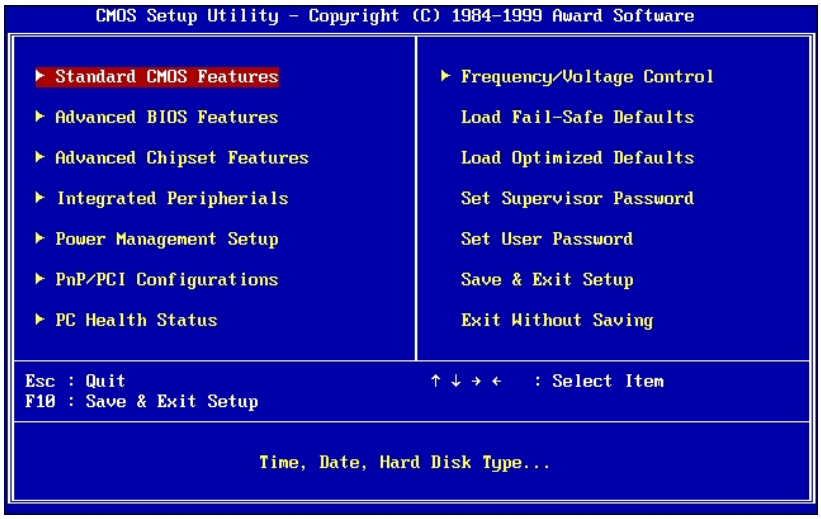
Manufacturer	Key
Acer	Esc, F12, F9
Asus	Esc, F8
Dell	F12
Fujitsu	F12, Esc
HP	Esc, F9
Lenovo	F12, Novo, F8, F10
Samsung	Esc, F12, F2
Sony	F11, Esc, F10
Toshiba	F12

2) Tu sais qu'il faut appuyer sur telle touche, parce que c'est marqué pendant 1 seconde au démarrage, ou parce que tu as tapé le modèle de ton ordi sur internet suivi de *bios*. C'est pas mal, la difficulté c'est qu'on ne sait pas toujours à quel moment exactement il faut appuyer sur la touche en démarrant. Donc à partir du moment ou tu démarres tu appuies plein de fois sur la touche spéciale jusqu'à arriver au bios. Des fois il y a une touche spécial pour aller sur le bios (si tu vois une touche bleue qui correspond à rien sur d'autres ordi) t'appuies dessus une fois éteint et ça fait démarrer sur le bios.

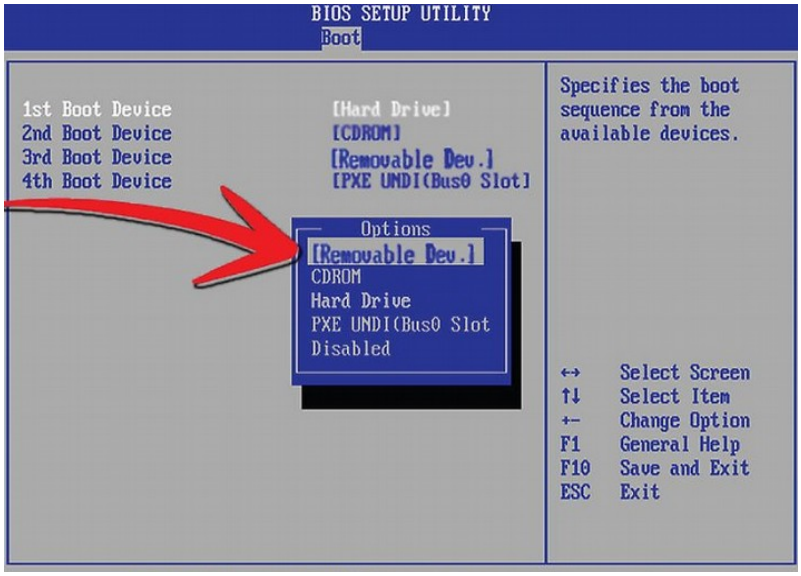
3) Ca peut parfois être plus compliqué si t'as un windows 10 ou 8 (cf plus loin).

=> Des fois il faut appuyer simultanément sur la touche Fn en même temps que la touche Fx pour pouvoir utiliser sa fonction

Réglage du bios / programme UEFI



Le bios ressemble à un écran bleu et gris, le plus souvent comme dans la 1ère capture écran, plus rarement comme la 3 ème. Pour naviguer dans le bios c'est marqué quelque part tout ce que tu peux faire. Souvent tu peux juste naviguer avec les flèches, faire F5 / F6 ou +/- (parfois d'autres touches) pour « monter / descendre » les options, ou faire Entrée pour aller dans un sous menu ou sélectionner quelque chose.



Une fois dans le bios il s'agit de chercher quelque chose qui s'appelle « boot », « boot order », « boot option » (ou si le bios est en français c'est donc « ordre de démarrage »). Faut soit chercher le nom de ta clef usb, soit chercher usb device ou quelque chose comme ça.

Comment ça fonctionne :

L'ordinateur essaye de démarrer sur la 1ère option, s'il y a il démarre dessus, sinon il tente l'option d'en dessous. Ce qui veut dire que :

- si y a le nom de ta clef usb, une fois que tu la retires il rechangera l'ordre de démarrage pour aller sur ton ordi et il faudra aller à nouveaux sur le bios pour remettre dans l'ordre.
- Si y a « usb device » il va vouloir démarrer sur une clef usb quand y en aura une, sinon il ira sur ton ordi. Si ton ordi ne démarre pas, c'est peut être qu'une clef usb sans système d'exploitation est branchée et qu'il essaye désespérément de

démarrer dessus (dans ce cas redémarre en débranchant la clef usb ou change la configuration du bios)

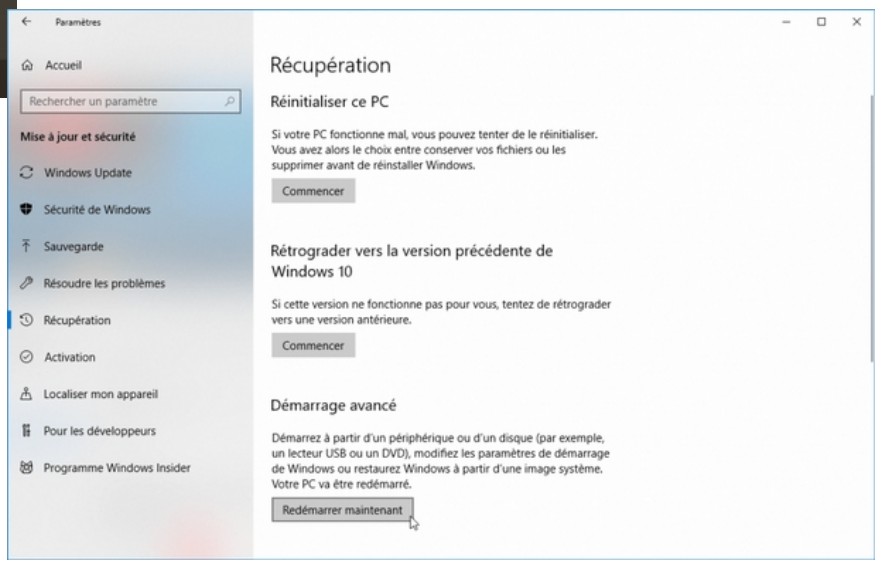
=> Des fois y a des options de boot dans le « exit » ou tu peux sélectionner ta clef directement et faire entrer.

Si tu ne trouves pas ta clef : C'est possible qu'elle soit cachée dans une autre option. Petite astuce : quand y a une petite flèche (⇒) devant une option, tu peux faire entrée et y a des sous options. Par exemple des fois il faut mettre ta clef en première option dans « hard drive » avant qu'elle apparaisse dans la page d'ordre de démarrage.

En cas de bug : Si ça ne démarre plus sur ton ordi (ce qui est rare), tu peux retourner dans ton bios pour voir l'ordre de démarrage ce qui se passe, si vraiment tu piges pas y a toujours une touche pour remettre ton bios dans les options initiales.

<u>Cas des windows 8 ou 10 (si c'est la première fois que tu démarres sur un autre système d'exploitation) :</u>

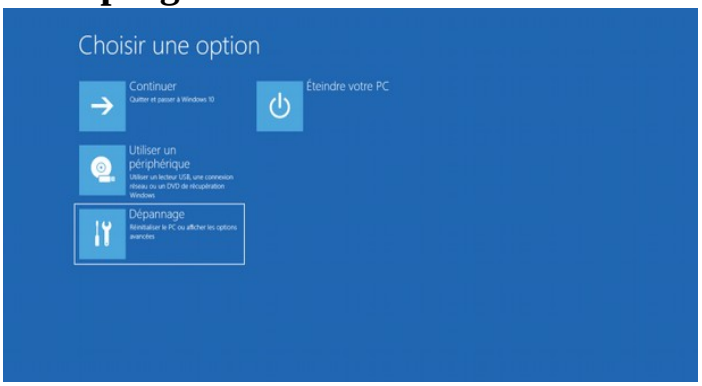
Ces petits systèmes d'exploitation ont tendance à mettre plusieurs pièges qu'il va falloir désactiver :
1) Ils peuvent empêcher ou rendre difficile de démarrer directement sur le bios au premier démarrage. Dans ce cas dans windows tu peux soit essayer :
Tu peux : soit essayer de cliquer sur le menu Démarrer puis sur le bouton **Marche/Arrêt** puis, **tout en restéant appuyé sur la touche Shift (⇑)**, clique sur **Redémarrer**.

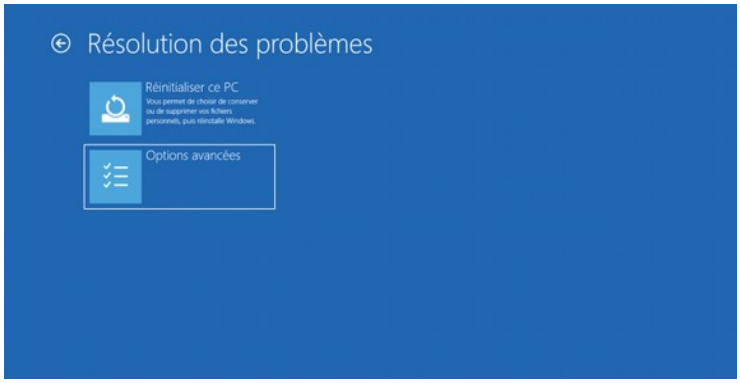


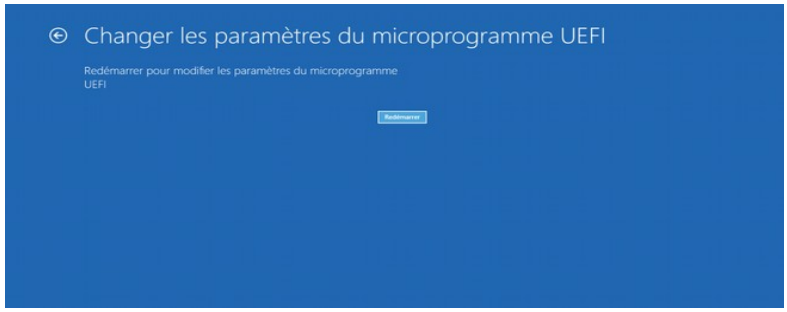
Soit tu vas, via le menu Démarrer, dans > **Paramètres** > **Mises à jour et sécurité** > **Récupération** en cliquant sur le bouton **Redémarrer maintenant** dans la section **Démarrage avancé**.

Le menu **Démarrage avancé** de Windows 10 va alors s'afficher.

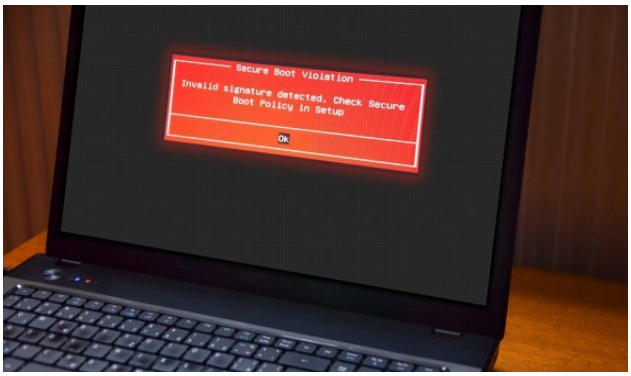
Clique sur le bouton **Dépannage => option avancée => Changer les paramètres du microprogramme UEFI. => Redémarrer** et tu devrais arriver sur le bios.







Pour la première fois c'est possible qu'il y ait certains paramètres qui t'empêchent de démarrer sur Tails.



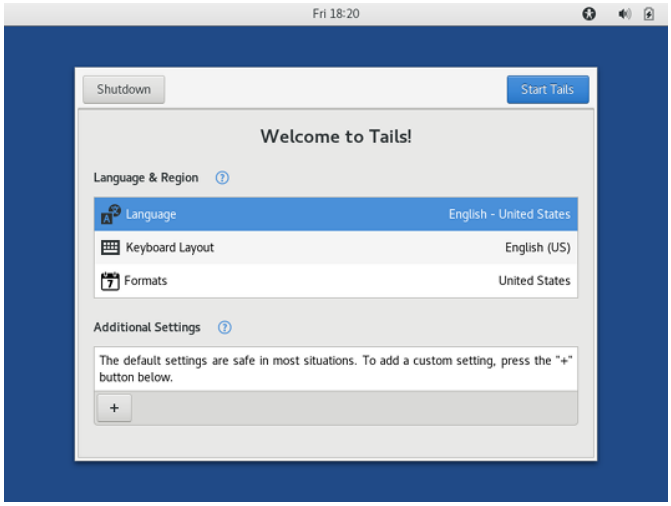
=> Dans security (ou dans boot ou quelque part dans le bios) il faut désactiver le « secure boot ». Celui-ci sert à vérifier sur quoi tu démarres et il peut refuser le démarrage de ton ordi sur un linux.
=> Des fois il peut être utile de désactiver « fast boot » (dans boot), qui peut au démarrage squizzer la possibilité d'aller sur le bios.

=> Parfois l'unique façon de désactiver le secure boot est d'enlever l'UEFI vers le legacy. Il faut alors aller dans boot trouver l'option « UEFI », quand tu fais « entrée » il te propose de le mettre en legacy, ce que tu fais. Attention !!: il faudra penser à remettre en UEFI pour redémarrer sur le système d'exploitation, sinon l'ordinateur ne reconnaîtra plus son système en place.

Démarrer sur Tails

Si l'ordinateur démarre sur Tails, le menu du chargeur d'amorçage apparaît et Tails démarre automatiquement après 4 secondes.

Après 30–60 secondes, un autre écran appelé Tails Greeter (Welcome to Tails!) apparaît.

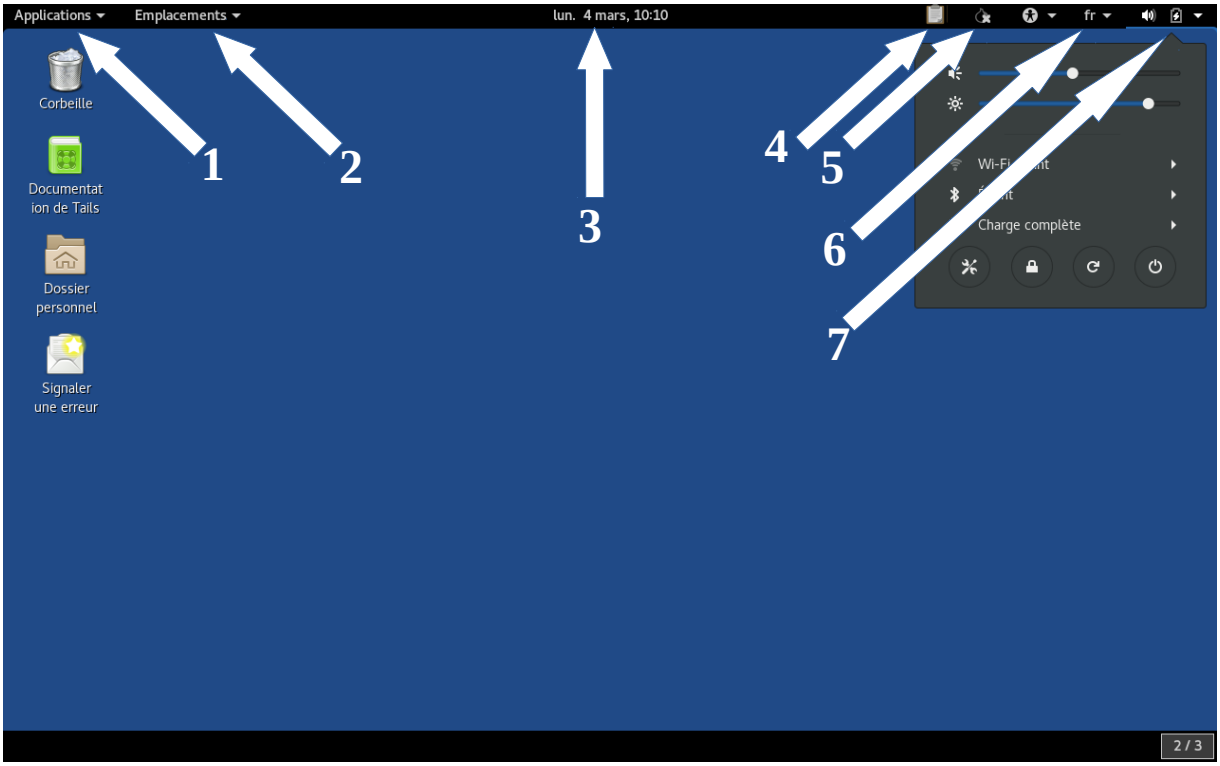


Dans le Tails Greeter, sélectionne ta langue et ta disposition de clavier dans la section Langue et région. Clique sur Démarrer Tails. Quand tu auras activé la persistance, le mot de passe pour l'activer apparaîtra sur cette fenêtre. En attendant tu ne pourras pas stocker de données sur ta clef Tails.

Après 15–30 secondes, le bureau de Tails apparaît.

Utiliser Tails

Le bureau de Tails ressemble à :



Tails est un système d'exploitation assez classique et simple d'utilisation. Dans la barre supérieure tu trouveras, de gauche à droite :

[1] Une liste classée par thème des applications (des logiciels) disponibles

[2] Accès aux principaux dossiers (où **apparaît le dossier persistent** lorsqu'il est connecté)

[3] Date et heure. Attention si t'es pas connecté.e à internet, Tails est à l'heure de l'ordi, une fois connecté.e, tous les Tails du monde ont la même heure (il y a un décalage horaire)

[4] Un outil pour chiffrer le presse papier, pour accéder à tes clefs de chiffrements (par exemple si t'utilise PGP), ouvrir un éditeur de texte

[5] Le témoin de l'état de Tor si tu es connecté.e au réseau Tor. Ce petit outil s'appelle « Oignon Circuits »

[6] choix des langues du clavier

[7] Le menu système, pour la luminosité de l'écran et le volume du son, la connexion wifi et Ethernet s'il est branché, l'état de la batterie, les paramètres, le bouton pour verrouiller l'écran avec un mot de passe créé sur le moment (pour quand tu pars et que tu ne veux pas que d'autres gens accèdent directement à ce que tu fais) les boutons de démarrage et d'extinction.

=> **si l'onglet wifi n'apparaît pas ici** c'est que tu ne pourras pas utiliser de wifi sur cet ordinateur (car certaines cartes wifi sont difficilement utilisables sur des linux). Dans ce cas soit t'as internet par cable Ethernet soit tu te procures une clef wifi (compatible avec les linux), soit si tu sais faire tu change ta carte wifi par une autre compatible à debian.

Configurer la persistance / stockage de donnée sur la clef Tails

Tails est totalement amnésique par défaut. Il oublie tout ce que vous avez fait entre deux sessions. Quand on veut travailler sur un document c'est un peu balot. Quand on veut paramétrer Tails c'est tout aussi chiant : on est obligé.e de le refaire après chaque démarrage. Heureusement, les créateur-trice-s de Tails y ont ajouté la persistance !
Le principe est de créer un « endroit » (appelé volume) sur ta clé, qui sera entièrement chiffré, sur lequel tu pourras stocker tes documents, et qui sera aussi utilisé par certains logiciels pour y stocker les données que tu auras autorisé. C'est techniquement très simple à faire, il faut juste faire un tout petit effort de compréhension.

Tu démarres ta clef Tails, tu vas dans *Applications => Tails => configurer le stockage… (persistant).* Là une fenêtre s'ouvre ou tu dois taper une phrase de passe et ensuite configurer ce que tu dois conserver dans la persistance. Ensuite, le stockage persistant peut être activé pour plusieurs types de données, en voici quelques détails / explications :

Données personnelles	Stocker des fichiers persos, que tu retrouveras dans le dossier **home>persistent** (sur le bureau ou via le raccourci « persistent »)
Marque-pages du navigateur	Tout est dans le titre
Connexions réseau	Pour se souvenir notamment des mots de passe wifi ou autres configurations de connexion
Logiciels additionnels	Pour pouvoir ajouter des logiciels à Tails (s'installeront automatiquement à chaque démarrage avec persistance)
Imprimantes	Il s'agit de sauvegarder les configurations des imprimantes
Thunderbird	C'est un client mail. Ça permet de garder tes configurations et tes mails en mémoire
GnuPG	Sers à chiffrer / signer. (Si tu veux chiffrer tes mails coche cette case et celle de Thunderbird)
Client Bitcoin	La configuration et le porte-monnaie Bitcoin sont sauvegardés. (Bitcoin est une monnaie cryptée décentralisée)
Pidgin	Pidgin sert à faire de la messagerie instantanée chiffrée. Activer cette option te permettra de garder les config des comptes, tes contacts, tes conversations …
Client SSH	SSH permet de se connecter à des serveurs à distance. Cette option permet de sauvegarder des config de connexion.
Dotfiles	Utile pour des configurations avancées, afin de dédoubler des fichiers de config dans le répertoire personnel. Option sensible concernant la confidentialité.

Si t’as un doute sur l'activation d'une des options, n'hésite pas à l'activer (sauf peut-être pour Dotfiles). Tes choix peuvent de toute façon être modifiés en revenant dans ce programme de « *configuration de volume persistant* ».
Pour prendre en compte les changements de configuration ou la création du volume persistant, il faut redémarrer *Tails*. Après le redémarrage, **le premier écran te propose maintenant de mettre un mot de passe de persistance**. Si tu ne le mets pas, la persistance ne sera pas activée mais tu peux tout de même démarrer Tails.

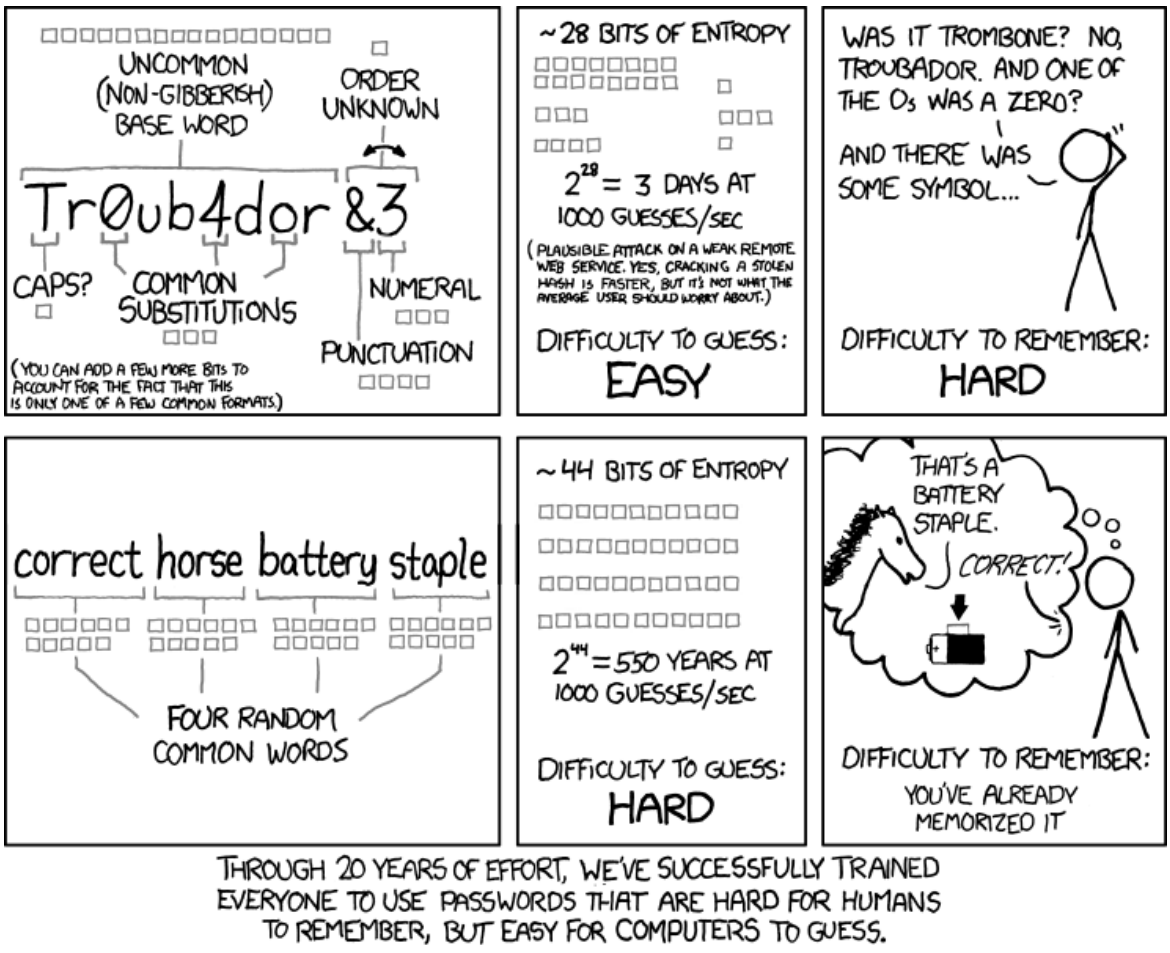
Changer sa phrase de passe :

Tu démarres Tails sans la persistance avec des droits d’aministrateur (cf partie *définir un mot de passe d’administration*), tu vas dans Applications => Utilitaires => Disques. Tu sélectionnes ta clef tails. Tu vas voir sur cette écran les partitions de ta clef tails. Tu sélectionne la partition *Tailsdata* avec un petit cadenas denté, tu cliques sur les roues dentées => Modifier la phrase de passe, on va d’abord demander ton mot de passe administrateur, puis tu tapes ton ancienne et nouvelle phrase.

J’ai oublié ma phrase de passe :

Tu perdras toutes tes données, mais tu peux démarrer Tails sans persistance, puis Applications => Tails => Supprimer le volume d… Et Applications => Tails => Configurer le stockage... (cf chapitre dessus au début du chapitre)

Configurer une bonne phrase de passe

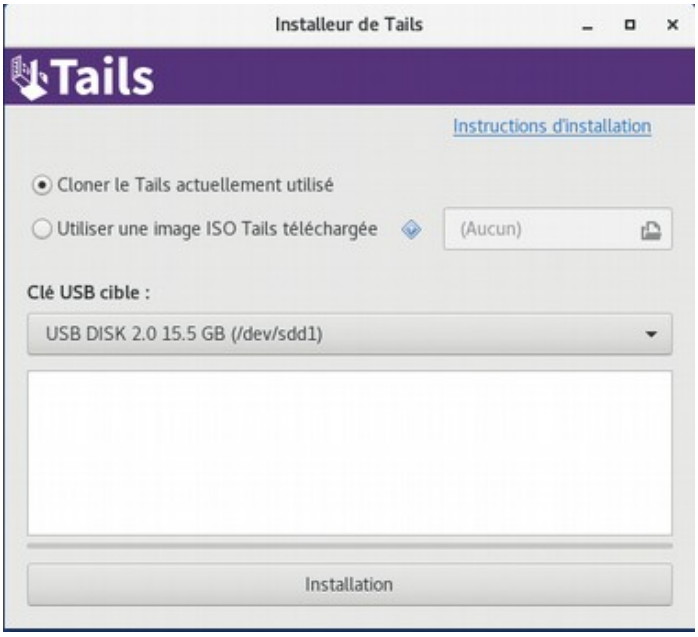


Il est plus recommandé un mot de passe long (20aine de caractère soit 4-5 mots) qui ne soit pas une citation, qu’un mot de passe court même avec des caractères compliqués.

Chaque personne détient sa façon de retenir ses phrases de passe. Des physionomistes vont se souvenir d'un tableau dans lequel y a des éléments dedans, d'autres vont coller un tout début d'une musique qui finit par une autre, d'autres peuvent prendre 4 mots aléatoirement dans un livre, d'autres mélanger des langues.
A toi de voir ta technique, attention à la sauvegarde de mot de passe écrite à la main ou sur un document texte qui traîne et que t'oublies ! Il est recommandé quand tu commences un nouveau mot de passe de le taper régulièrement la première semaine pour que ça s'ancre.
Il est important de ne pas utiliser le même mot de passe pour des services différents, ça évite de tout compromettre. Le niveau de sécurité n'est pas forcément le même entre logiciels. Sur internet, on ne peut pas faire confiance aux sites internets par lesquels on passe. Régulièrement on entend tel gros serveur qui a été hacké et des millions de mdp récupérés. Tu donnes aussi la possibilité à cette entreprise de pouvoir connaître tes mdp (ou ta façon de construire tes mdp).
Il existe aussi des coffres forts à phrase de passe. Par exemple keepassX (explication de l'outil plus loin dans ce document).

Installer une clef Tails (à partir d'une clef Tails)

Il te faut : Une clé avec déjà Tails. C'est la version qu'il y a sur cette clé qui sera mise. Si elle n'est pas à jour, ça mettra ta version Tails pas à jour, si elle est vérolée aussi (voir le chapitre suivant).
Une autre clé USB de plus de 8Go[4], attention elle sera formatée et toute les données y seront supprimées. S'il y avait des données auparavant sur cette clé usb, tu peux avoir envie qu'elle ne soit pas retrouvable à posteriori il peut être intéressant d'écraser plus correctement les données avant (cf chapitres suivant)
T'allumes ta clef Tails (avec ou sans persistance ça n'a pas d'importance). Tu vas dans *Applications => Tails => Programme d'installation.*



Si l'installeur de Tails voit une autre clef usb, elle va être mise en « clé USB cible ».
T'as juste à faire Installation, ça prend 5 à 20 min. Ta persistance ne sera pas clonée.
Si ça ne marche pas (ce qui n'arrive pas souvent) essaye de formater toi-même ta clef usb, de l'enlever / remettre et de relancer l'installation.

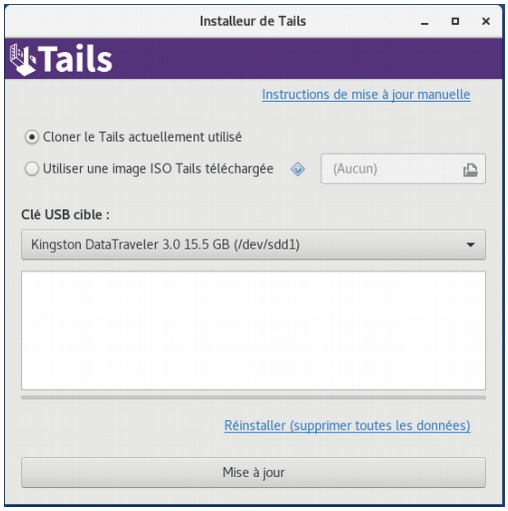
4 Si tu peux choisir ta clef, tu peux consulter avant la liste des clefs usb problématiques avec Tails pour ne pas tomber dessus : https://Tails.boum.org/support/known_issues/index.fr.html#index1h2

Eviter d'avoir une clef vérolée :

Une clef Tails vérolé, est une clef qui n'est pas le Tails d'origine (donc potentiellement avec des mouchards)
D'autant plus si tu diffuses souvent d'autres clefs Tails :
1) Évite de laisser traîner n'importe où ta clef (surtout dans les lieux surveillés), comme tu vois ça met 10 min à cloner, on pourrait très bien te cloner une autre version qui ressemblerait à Tails mais avec d'autres choses dedans comme des sniffeurs à mot de passe.
2) Ne branche pas ta clef dans des systèmes d'exploitations allumés (et donc avec ses processus allumés qui pourrait lancer en toile de fond de modification sur ta clef), éteins l'ordi avant de la brancher.
3) Fais gaffe aux clefs qui peuvent revenir du commissariat.

Mettre à jour une clef Tails

La sécurité sur Tails (et de manière plus générale sur linux), passe par le fait qu'il continue à être développé et que des mises à jour viennent trouver des solutions aux failles de sécurité apparaissant. La sécurité informatique d'aujourd'hui sera obsolète dans 5 ans. Il est très important de faire les mises à jour régulièrement (Tails en fait une par mois).
Les mises à jour correspondent à : mise à jour de Tails, et de tous les logiciels qui y sont utilisés (debian, Tor, thunderbird, …), ils permettent aussi de fixer des bugs, mais parfois de nouveaux peuvent apparaître (surtout sur les gros changements).
Il existe 2 types de mises à jour, t'en seras informé.e par un mot quand tu te connectes à internet, lis le bien :
1) La mise à jour automatique. T'as juste à lancer le téléchargement. Il faut se prévoir un peu de temps et bien attendre la fin, un moment ça va couper ton internet, c'est normal ! S'il y a un bug (éteignage avant la fin), pas de panique, tes données ne sont pas affectées par la mise à jour.



2) La mise à jour manuelle.

- Si t'as déjà une clef Tails avec la dernière version, tu démarres sur celle là, et comme pour l'installation *Applications => Tails => Programme d'installation.* Sauf que là, plutôt que de mettre « installation », on va te demander « mettre à jour », la différence c'est que ça ne formatera pas toute la clef usb, ça remplacera juste la partition de la Tails allumée par celle qui est mise à jour. (tu peux donc mettre à jour d'autres personnes, attention aux clefs Tails verolées !)

- Si tu ne connais personne, il te faudra une clef USB vierge ou une autre clef Tails (donc pas à jour), et tu pourras télécharger c'qu'il te faut en suivant le tuto Tails qui te suit pas à pas : *https://Tails.boum.org/upgrade/index.fr.html*

II) Pour aller plus loin quelques trucs et astuces supplémentaires

Supprimer vraiment des données d'une clef usb

Supprimer ou « mettre à la corbeille » ne supprime pas les données. … et ça peut être très facile de les retrouver.
En effet, lorsqu'on « supprime » un fichier — en le plaçant dans la *Corbeille* puis en la vidant — on ne fait que dire au système d'exploitation que le contenu de ce fichier ne nous intéresse plus. Il supprime alors son entrée dans l'index des fichiers existants. Il a ensuite le loisir de réutiliser l'espace que prenaient ces données pour y inscrire autre chose.
Mais il faudra peut-être des semaines, des mois ou des années avant que cet espace soit *effectivement* utilisé pour de nouveaux fichiers, et que les anciennes données disparaissent réellement. En attendant, si on regarde directement ce qui est inscrit sur le disque dur, on retrouve le contenu des fichiers. C'est une manipulation assez simple, automatisée par de nombreux logiciels permettant de « récupérer » ou de « restaurer » des données.
On ne peut pas réellement supprimer des données en informatique, cependant on peut « réécrire des données par dessus », ce qu'on appelle faire une passe. **S**ur Tails, tu peux faire clique droit sur un fichier, écraser les données (par défaut ça fait 2 passes), attention si c'est un fichier très gros ça va prendre du temps. Pour l'ensemble d'une clef usb, tu peux quand tu la formates faire « écraser les données existantes avec des zéros » (le faire à minima 2 fois). Attention si sur ta clef usb ou sur ton disque dur tu as des documents sensibles à supprimer pour de vrai, ces propositions ne sont pas les plus adéquates car il peut rester des traces notamment en cas d'accès physique au matériel. Il vaut mieux se référer à l'article : Effacer des données « pour de vrai » sur le guide d'autodéfense numérique[5].

Comment créer un disque dur ou une clef usb chiffrée (ouvrable sur des linux)

Dans Tails tu peux aller dans Applications => Utilitaires => Disques. Là tu sélectionnes le bon disque (c'est à dire ta clef usb ou ton disque dur souvent il y a marqué le poids de la clef suivi de Drive), tu formates tout le disque ainsi que ses partitions en faisant les 3 petits traits en haut à droite de l'écran (si y a des documents sensibles ou perso dedans cf chapitre supprimer vraiment des données). Quand c'est fini il n'y a plus rien du tout sur ton disque, tu cliques sur le « + » dans volumes, tu choisis la taille de ta partition (tout si tu n'en veux qu'une) et tu mets dans « type » => « chiffré, compatible avec les système linux » (= probablement tu ne pourras pas aller sur cette clef avec windows et mac) et tu mets ton mot de passe.

5 https://guide.boum.org/tomes/1_hors_connexions/3_outils/06_effacer_pour_de_vrai/

Chiffrer un fichier / un document / un message par une phrase de passe

Dans Tails tu peux très bien faire clique droit sur un fichier, faire « chiffrer » choisir « use passphrase only » ou par clef publique. Ca va créer un fichier en .pgp. Attention à supprimer les données non chiffrées pour de vrai auparavant (cf chapitre au dessus).
Si tu choisis l'option passphrase, il faudra ouvrir le fichier dans Tails et taper la phrase de passe. Si tu ne veux pas que les données non chiffrées soient marquées à l'emplacement où tu l'ouvres (par exemple sur une clef usb), il vaut mieux d'abord copier le fichier chiffré dans un dossier Tails qui est uniquement en mémoire vive (tout sauf la persistance) avant de l'ouvrir.
De la même manière tu peux envoyer des messages chiffrées par phrase de passe préalablement convenu. Tu ouvres un éditeur de texte (que tu n'enregistres pas), tapes ton message, tu le sélectionnes et le copies. Tu cliques sur le petit livret en haut à droite, « chiffrer le presse papier avec une phrase de passe », tu colles le nouveau message dans un mail par exemple. Ca ressemble à ça :

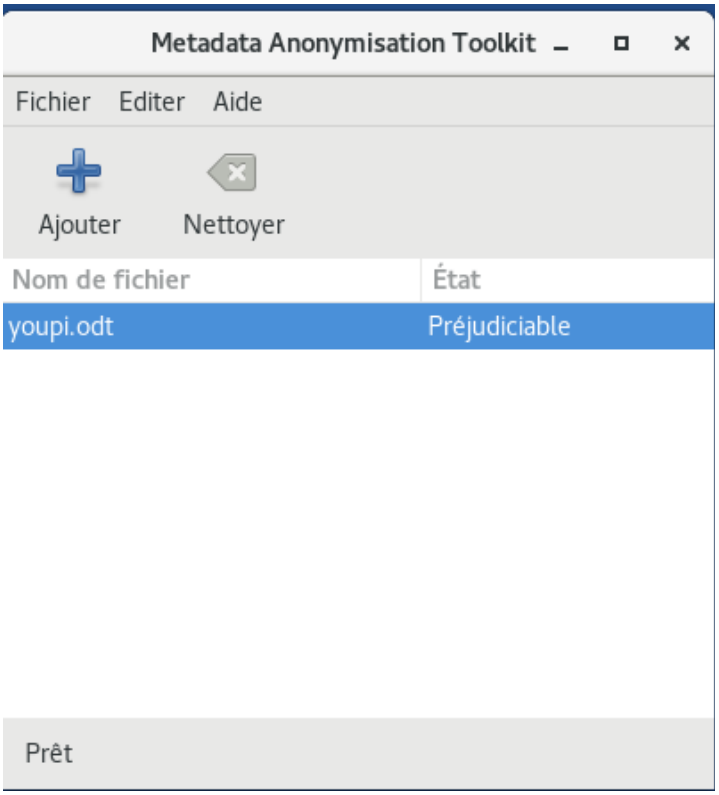
```
-----BEGIN PGP MESSAGE-----

jA0ECQMCKvDnnDLWYjXO0nABjBNyfM0NFJ5beMOJUGDEsDB0QdW+7ohxAgDVlO07
83ZJ8eoEpNlKV6NQ4IYx6YpIpjUsiv3FB5SZOVlTXAoTlNRQmhAi2pishDcMtBSk
9vXmpJ8LRKncAC3Cl4PEfLklY2CzHceUpGgRkoRS2/hd
=zT87
-----END PGP MESSAGE-----
```

Pour le déchiffrer, il suffit dans Tails de copier l'entièreté (à partir de petit « - » avant Begin PGP, jusqu'à la fin des « - » de END PGP MESSAGE). Là si tu ne t'es pas trompé un cadenas apparaît sur le livret, tu cliques dessus et « déchiffrer/vérifier le presse papier » et une phrase de passe te sera demandée. Si tu lis ce texte par ordi tu peux sélectionner le texte, faire l'opération et écrire la phrase de passe :« youpi ». Tu as réussi à déchiffrer le message.

MAT - supprimer les métadonnées sur des fichiers

Beaucoup de fichiers que nous utilisons (images, sons, vidéos, documents texte, …) contiennent des méta-données. Ce sont des données inscrites dans le fichier, mais qui ne constituent pas le contenu du fichier. Les métadonnées sont à un fichier ce qu'est le générique de fin à un film grand public : quelque chose que personne ne regarde vraiment, mais pas caché pour autant, et qui livre des informations importantes. Et cellui qui veut avoir des infos sur le contenu de l'objet (votre fichier ou le film), auscultera les métadonnées de vos fichiers ou le générique avec attention.
Pour exemple, les métadonnées d'une photo peuvent comporter la taille de ta photo en pixels, la marque et le modèle de ton appareil, son numéro de série … Si la photo a été

prise depuis un téléphone, on peut y ajouter ton numéro de téléphone, le nom attribué à l'abonnement téléphonique, les coordonnées GPS du téléphone lors de la prise de vue, et de manière générale toutes les options définies dans ton téléphone. Et enfin le nom de ton ordi, les logiciels qui ont servis à la modifier, etc.



MAT (pour Metadata Anonymisation Toolkit) est un logiciel qui lit et supprime les méta-données de vos fichiers. À son démarrage une fenêtre s'ouvre, dans laquelle tu peux glisser-déposer les fichiers à analyser.
Pour ça dans Tails tu fais soit clique droit Clean metadata, soit tu ouvres MAT tu mets ton fichier et tu fais nettoyer. Si c'est marqué préjudiciable c'est qu'il y a des métadonnées, tu peux cliquer 2 fois sur le fichier pour voir un peu quoi.
Certains formats de fichiers ne fonctionnent pas avec MAT (dans *aide => information* t'auras indiqué tous les formats supportés), il faut alors se renseigner sur les techniques pour le faire.

Petit bug

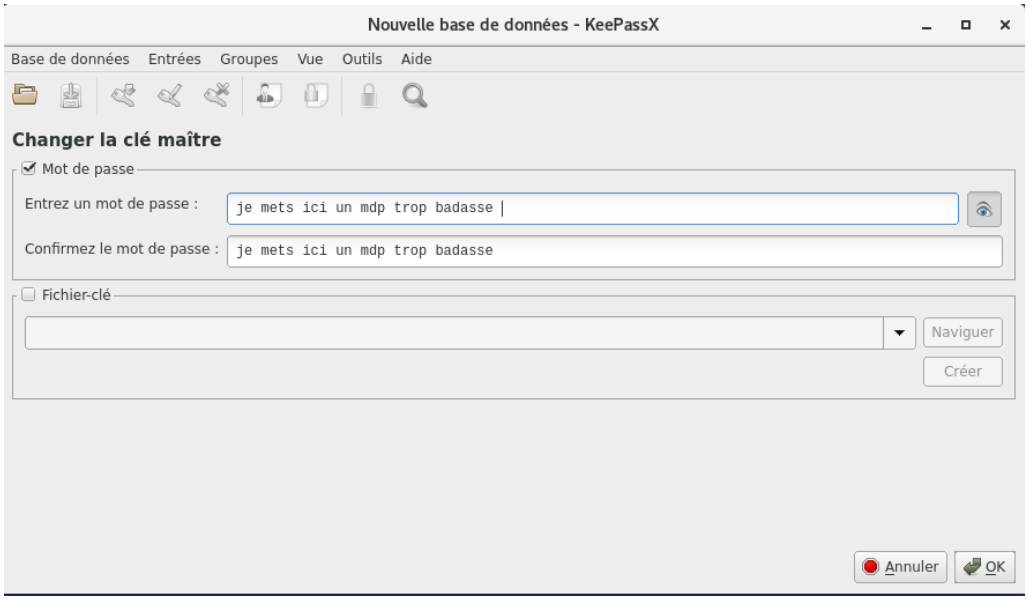
C'est possible qu'un / plein de fichiers apparaissent dans le dossier, il suffit de réactualiser le dossier pour les voir disparaître.

Supprimer les métadonnées d'un fichier pdf

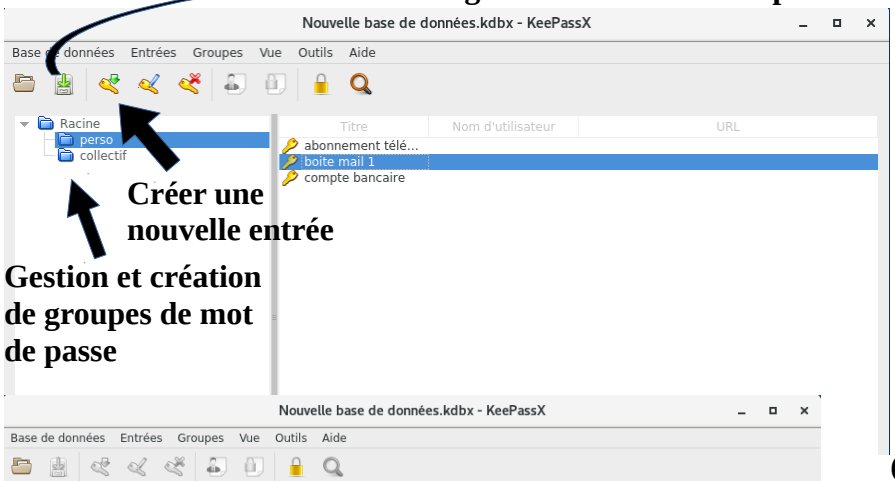
Pour les pdf (format trop compliqué), il vaut mieux repartir du fichier texte (qui passe dans MAT) avant de le convertir en pdf.
Si tu n'as que la version pdf, il faut d'abord le transformer en image, supprimer les métadonnées et le remettre en pdf. L'inconvénient c'est que tu ne pourras plus sélectionner le texte, que tu vas perdre en qualité et le document risque d'être plus lourd.
Dans Tails actuellement, pour faire ça, il faut installer des logiciels additionnels qui ne marchent que par ligne de commande. T'installes le logiciel mat2 (cf chapitre *installer des logiciels additionnels*). Tu dois ouvrir un simple terminal, taper la commande :
mat2 [chemin du document] Pour avoir le chemin du document, tu sélectionnes le document et restes appuyé avec ta souris, et le glisses dans le terminal. Ca donne quelque chose comme : amnesia@amnesia:~$ mat2 '/home/amnesia/Persistent/[chemin]/[ton-document].pdf', en appuyant sur entrée il va te produire le même document à côté qui fini par « cleaned ».

Coffre fort à mot de passe (KeepassX)

Si tu es amené.e à devoir connaître beaucoup de phrases de passe, il peut être bien d'avoir un moyen sécurisé de les stocker (et pas un bout de papier à côté de ton ordi).
Il existe KeepassX (*Application => Favoris => KeepassX)*.
Tu mets ta phrase de passe (tu peux aussi mettre un fichier clé en complément, ça veut dire qu'il faudra le mettre pour pouvoir ouvrir ton coffre fort à mdp), et là t'enregistres dans la persistance le fichier (sinon tu risques de perdre tous les mdp que tu vas mettre dedans, ce fichier s'appellera quelque chose comme keepassx.kdbx).
L'interface est simple d'usage.

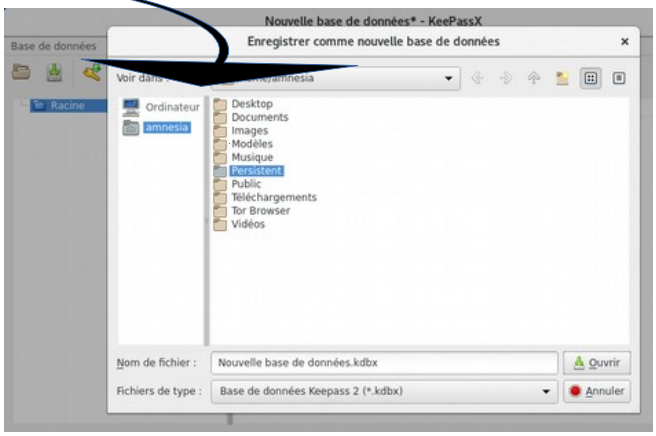


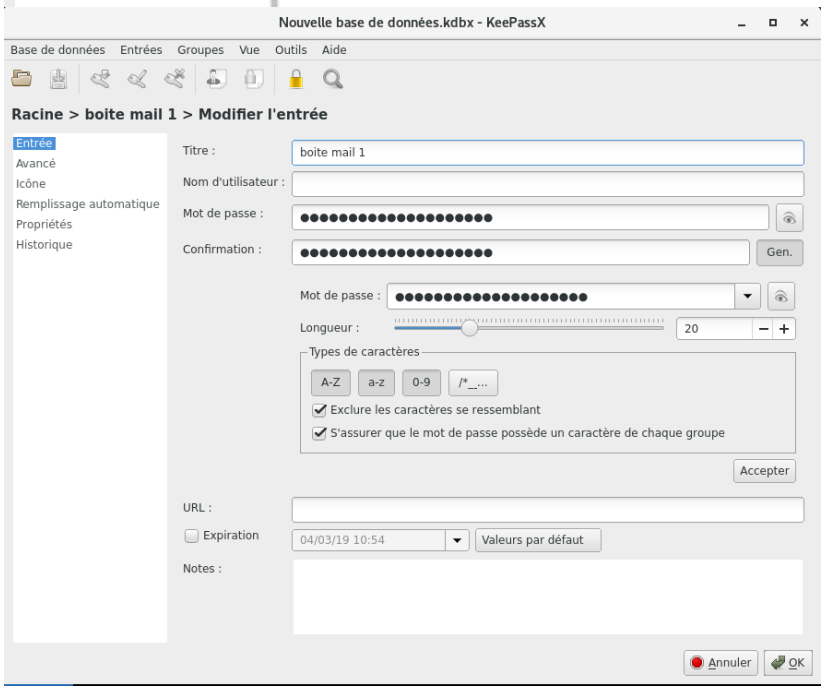
Pour enregistrer mon fichier keepassX



Créer une nouvelle entrée

Gestion et création de groupes de mot de passe



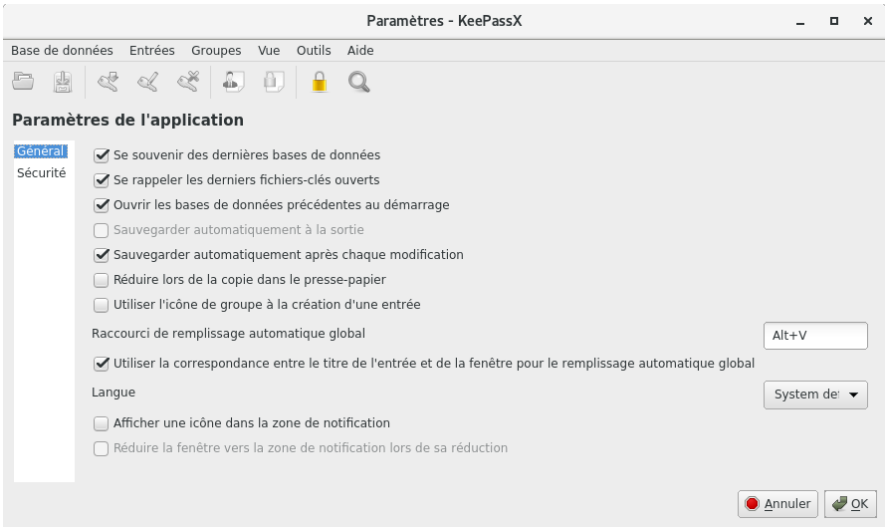


Grace à keepassX tu peux aussi générer des phrases de passe aléatoire que seul KeepassX retiendra. Tu cliques 2 fois sur une entrée, tu fais « Gen » et t'oublies pas de faire accepter (et non pas Ok tout en bas)

Dès que tu fermes KeepassX il se chiffre.

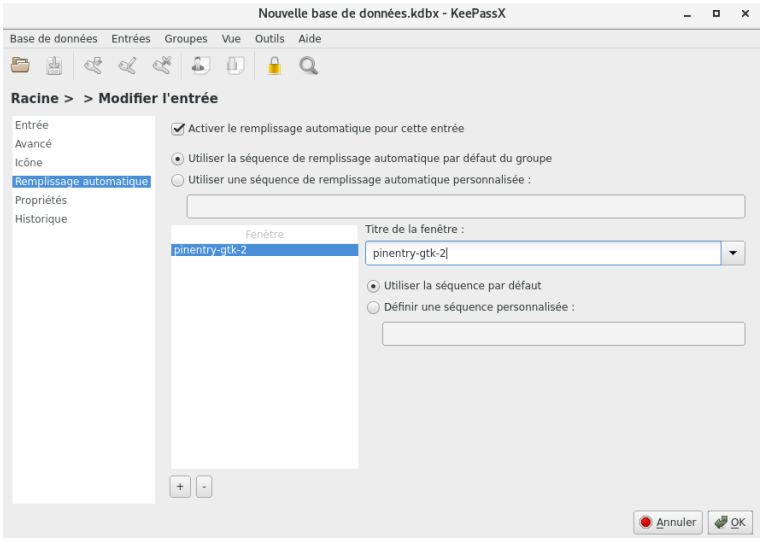
Utiliser les paramètres de remplissage automatique de keepassX

(Bonus si t'en as marre de copier-coller tout le temps tes phrases de passe)



1) Configurer les touches qui feront le remplissage automatique

Dans keepassX faire (en haut) outil => paramètre => mettre les touches qu'on veut dans « raccourci de remplissage automatique global » (genre alt+v par exemple, pas de raccourcis utilisés par d'autres fonctions comme Ctr+c). Ce paramètre ne s'enregistre pas sur Tails, il faudra le refaire à chaque démarrage de Tails



2) configurer le remplissage automatique de l'entrée

Revenir dans la fenêtre des mots de passe de keepassX. Faire clique droit sur l'entrée souhaitée puis Voir/modifier l'entrée puis à gauche « remplissage automatique » en bas le « + » et il suffit de rajouter le titre de la fenêtre. Pour savoir le nom de cette fenêtre, il suffit de regarder le nom de la fenêtre qui s'ouvre pour demander un mot de passe, et soit de la taper dans le titre précédemment dit, soit si cette fenêtre du mot de passe est ouverte en parallèle du keepassX il suffit de cocher la petite flèche à droite du titre de la fenêtre et de choisir le bon nom de fenêtre (moins vous aurez de fenêtre ouverte, moins y aura de nom de fenêtre)

3) Pour effectuer le remplissage automatique

Dans la fenêtre qui demande le mot de passe, tu appuie sur les touches choisies dans 1). Si y a plusieurs mots de passe qui ont le même nom de remplissage t'auras à choisir le bon. Des fois la fenêtre pour choisir s'affiche derrière la fenêtre qui demande le mdp, faut bouger la fenêtre.

Téléchargement / téléversement et le dossier tor browser

Une protection sur Tails existe qui fait qu'internet n'a pas accès à vos dossiers (persistance, clefs usb ou tout autre), ça évite qu'il fouine dans vos documents, ce qu'on appelle un *bac à sable*. Pour télécharger il faut donc télécharger dans le dossier Tor Browser puis mettre ensuite dans le dossier que vous souhaitez / dans la persistance. De la même manière, si vous voulez téléverser un document (=le mettre sur internet, l'envoyer sur un site ou en pj), il faut d'abord le copier dans le tor browser avant de le téléverser.

Conseil de rapidité (peu de ram)

Il existe 2 tor browser, un qui n'est pas persistant, l'autre qui l'est (qui s'allume que si tu as activé la persistance au demarrage). Celui qui n'est pas persistant enregistre dans la RAM. Attention donc si tu télécharges trop dessus ça va ralentir la clef Tails. De manière générale si trop de documents / trop d'onglets sont ouverts ou si trop de documents sont enregistrés sur autre chose que la persistance ça peut faire buguer ou ralentir.

Si tu as donc un gros téléchargement vaut mieux le faire sur le tor browser persistant. Mais ne laisse pas tout tes documents dedans si tu veux que le bac à sable soit efficace.

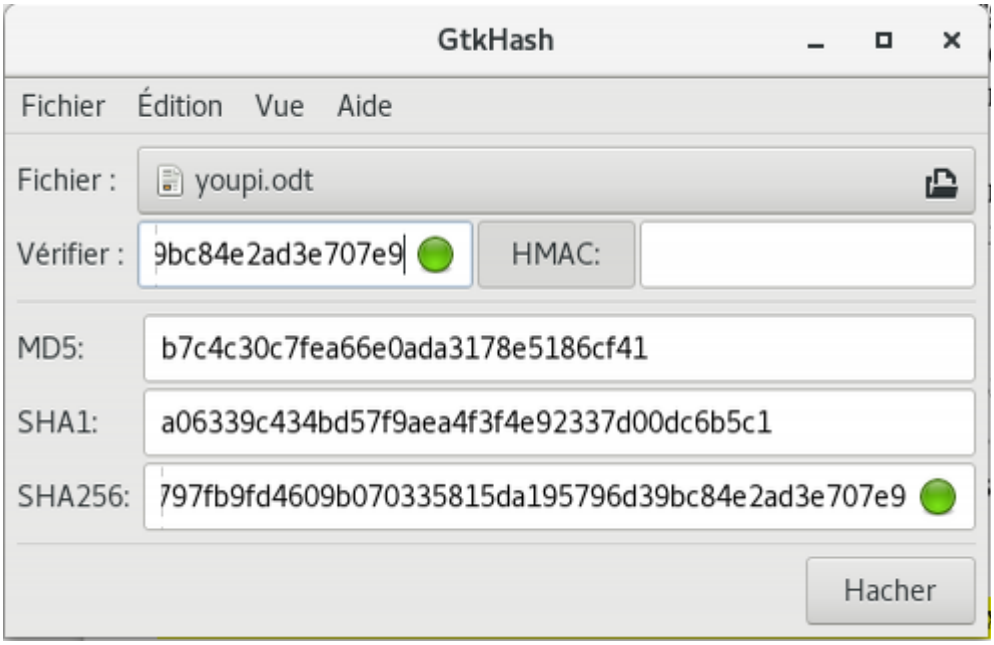
Format de fichier HTML

Les fichiers en html ne peuvent pas être ouverts sur la persistance (car le navigateur tor n'a que accès au tor browser), il faut donc les mettre dans le dossier tor browser avec le dossier de configuration (pour avoir les images) avant de l'ouvrir. Tu n'auras pas besoin d'internet pour l'ouvrir.

Document téléchargé et vérification :

Les fichiers téléchargés sur internet peuvent être dangereux. En fonction de ton modèle de menace / de la sensibilité / du type de document il peut s'avérer nécessaire de prendre plusieurs précaution :

1) Vérifier l'intégrité d'un document (important pour les logiciels / images iso), vérifier que ce qu'on a téléchargé est bien complet. Il existe pour cela « GTKhash ». C'est ce qu'on appelle « vérifier les sommes de contrôle (MD5, SHA1, SHA256) ». Cela permet de vérifier sur le document téléchargé que tu as la même somme de contrôle que la personne qui l'a mis sur le site, ainsi sur le site s'il y a la somme de contrôle SHA256, il suffit de le copier dans « vérifier », mettre le fichier télécharger, le « hacher » (opération qui ne peut pas altérer le fichier). En terme de vérification SHA256 > SHA1 > MD5.



Si y a le point vert, c'est que le fichier n'a pas été altéré pendant le téléchargement.

2) Vérifier l'origine du fichier.

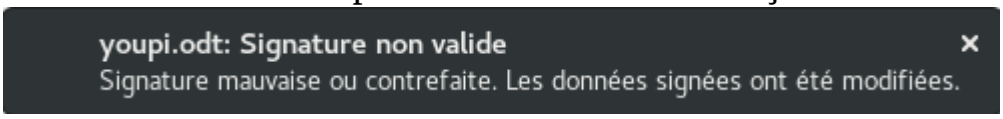
Avisé. Prérequis : connaître pgp, ce qu'est une signature de document et une clef publique

Pour être sûr que le fichier que tu viens de télécharger appartienne bien à X et pas à un intermédiaire Y, une possibilité de vérification par pgp existe, pour cela il faut que X ait *signé* son document et ait laissé la possibilité d'accéder à sa clef publique.

Si t'as une fenêtre comme cela dans ton navigateur (la signature du document des fois appelé *sig*) tu fais « enregistrer sous » et ça va te proposer d'enregistrer un fichier en *.asc*

En parallèle il te faut télécharger la clef publique du/ de la signateurice (par serveur de clef ou autre moyen proposé à disposition).

Si tu cliques 2 fois sur le fichier .asc obtenu, Tails va l'ouvrir avec le vérificateur de signature. Soit le fichier a le même nom et est dans le même dossier, soit tu devras indiquer ou se trouve le fichier à vérifier et alors l'opération se lance. Si t'as ça en haut qui apparaît, c'est pas bon, il y a possibilité d'usurpation (ou erreur de manip) :



Si c'est ça, c'est le document signé par la clef présenté. Mais c'est *untrusted*, ça veut dire que par contre tu n'as pas vérifier la clef publique, qu'elle ne soit pas elle même usurpée (là on rentre dans le domaine de pgp).

3) *Notion de confiance*

Malgré tout ça, se pose la question de la confiance qu'on peut avoir dans le groupe qui gère le fichier téléchargé : fait-il bien ce qu'il dit ? (attention aux véreux.ses qui traînent sur internet). Cela repose souvent sur ce qu'on appelle une toile de confiance.

S'il y a risque, en fonction du modèle de menace, une solution est de télécharger un fichier avec une clef Tails, de ne pas l'ouvrir et avoir par exemple une 2ème clef Tails que t'allumes en désactivant internet. Pour cela au démarrage, sur la page de mot de passe de persistance tu fais le petit + en bas, et tu peux mettre une option sans accès à internet. Et là seulement t'ouvres le document.

S'ajouter des droits d'administrateurices

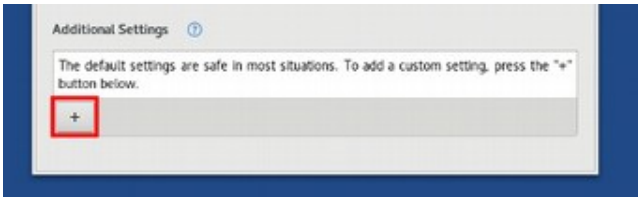
Dans Tails, un mot de passe d'administration (également appelé *mot de passe root* ou *mot de passe amnesia*) est nécessaire pour effectuer des tâches d'administration système. Par exemple :

- Pour installer des logiciels additionnels
- Pour accéder aux disques durs internes de l'ordinateur
- Pour lancer des commandes avec sudo
- Pour accéder à certains droits, notamment quand t’as une fenêtre qui demande une authentification avec écrit administrateur en orange.

Par défaut, le mot de passe d'administration est désactivé pour plus de sécurité. Ce qui peut empêcher un.e attaquant.e ayant un accès physique ou à distance à ton système Tails d'obtenir les droits d'administration et d'effectuer des tâches d'administration contre ta volonté.

Définir un mot de passe d'administration

Afin d'effectuer des tâches d'administration, tu dois choisir un mot de passe d'administration lors du démarrage de Tails, en utilisant Tails Greeter.



1. Lorsque Tails Greeter apparaît, clique sur le bouton +.
2. Lorsque la fenêtre Paramètres supplémentaires apparaît, clique sur « Mot de passe d'administration ».
3. Saisis un mot de passe de ton choix dans les zones de texte « Mot de passe d'administration » et confirme puis clique sur « Ajouter ».

Ce mot de passe ne dure que durant la cession. Tu peux avoir ces droits d’administration avec ou sans persistance.

Installer des logiciels additionnels

Attention : Si t’installes des nouveaux logiciels, c’est à toi de vérifier qu’il n’y a pas de faille de sécurité, de veiller à ses mises à jour sur le long terme et de le configurer pour passer par Tor s’il passe par internet. Si les logiciels utilisés dans Tails sont audités en terme de sécurité ça ne sera pas forcément le cas pour ce que tu installeras. C’est mieux avant d’installer un nouveau logiciel de vérifier qu’il n’y a pas déjà un logiciel dans Tails qui fait déjà le taffe que tu souhaites faire. Ici on va voir comment installer un logiciel parmi les paquets de debian.

En prérequis il faut que t’ais coché « logiciels additionnels » dans la configuration de ta persistance (cf chapitre associé). Il te faut démarrer Tails avec des droits d’administrateur.ices (cf au dessus), aller dans *applications => outil système => gestionnaire de paquets synaptic*. Là tu mets ton mot de passe admin (si c’est la première fois que tu fais ça ça va prendre du temps). Tu vas dans « Toutes » et tu choisis le logiciel que tu souhaites installer « sélectionner pour installation » puis « appliquer ». Une fois fait Tails te demandera, si ta persistance est ouverte, si tu veux l’installer une fois, où l’ajouter à ta persistance. Si tu fais le second choix, veille à l’évolution du logiciel au cours du temps (Tails ne le fera pas à ta place). Tu pourras accéder aux

logiciels additionnels que t'as installé dans *Applications => outils système => logiciels additionnels*.

Chiffrer ses mails (avec Thunderbird)

Nécessite d'avoir activé Thunderbird et PGP dans sa persistance

Note : cette méthode est intéressante sur tails, mais moins sur un système d'exploitation non chiffré car tous tes mails (dont les non chiffrés) seraient stockés dessus.

Si tu veux une vulgarisation de ce qu'est pgp, tu peux consulter l'article: « Une présentation approfondie du chiffrement de bout *en bout : comment les systèmes de chiffrement à clé publique fonctionnent-ils ?* » du site surveillance self défense[6].

Tu peux aussi consulter *Que devrais-je savoir au sujet du chiffrement ?* Sur le même site au sujet des différents types de chiffrements existant.

Quelques explications :

GNU Privacy Guard (GnuPG ou GPG) est un logiciel de *chiffrement* libre et gratuit développé par le GNU Project. Il est conforme aux standards **OpenPGP** et a été conçu pour interagir avec *Pretty Good Privacy (PGP)*, un équivalent commercial développé par Phil Zimmermann. **Enigmail** est un module complémentaire qui vous permet d'accéder au chiffrement GnuPG depuis Thunderbird.

GnuPG s'appuie sur une forme de *chiffrement à clé publique* qui nécessite que chaque utilisateurice génère sa propre paire de *clés*. Cette *paire de clés* peut être utilisée pour chiffrer, déchiffrer et signer du contenu numérique tel que des messages électroniques. Cela inclut une *clé privée* et une *clé publique* :

- Votre **clé privée** est une donnée extrêmement sensible. Quiconque réussi à obtenir une copie de cette clé sera capable, avec le mot de passe, de lire du contenu chiffré qui n'était destiné qu'à vous uniquement. Il pourrait aussi signer des messages *à votre place.* Votre *clé privée* est, elle-même, chiffrée par un mot de passe que vous choisirez lorsque vous générerez votre *paire de clés*. Vous devez choisir un mot de passe complexe et sûr de façon à ce que personne n'ait accès à votre *clé privée*. Vous utiliserez votre *clé privée* pour déchiffrer des messages qui vous sont envoyés par celleux qui ont une copie de votre *clé publique.*
- Votre **clé publique** est faite pour être partagée avec les autres et ne peut être utilisée pour lire un message chiffré ou contrefaire un message. Une fois que vous avez la clef publique de votre correspondante, vous pouvez commencer à lui envoyer des messages chiffrés. Elle seule sera capable de déchiffrer et lire ces messages parce qu'elle seule a accès à la *clé privée* qui correspond à la *clé publique* que vous utilisez pour les coder. De la même façon, pour que quelqu'un.e *vous* envoie un message chiffré, cette personne doit avoir une copie de votre *clé publique*. Il est important de vérifier que la *clé publique* que vous utilisez pour chiffrer les messages appartient effectivement à la personne avec qui vous essayer d'échanger. Si vous ou votre correspondant.e êtes dupés lors du chiffrement des messages avec la mauvaise clé publique, votre conversation ne sera pas sécurisée.

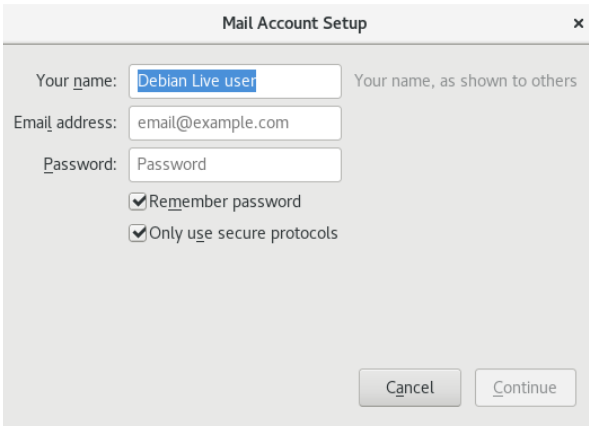
GnuPG et **Enigmail** vous permettent aussi d'attacher des **signatures numériques** à vos messages. Si vous *signez* un message en utilisant votre *clé privée*, chaque destinatairice ayant une copie de votre *clé publique* peut vérifier s'il a bien été envoyé par vous-même et que le contenu n'a pas été falsifié. De la même façon, si vous avez la *clé publique* d'un correspondant, vous pouvez vérifier ses signatures numériques

L'idée par la suite est de faire les configuration sur tails pour que thunderbird gére le chiffrement de bout en bout.

Pour démarrer Thunderbird choisis Applications ▸ Internet ▸ Messagerie Thunderbird.

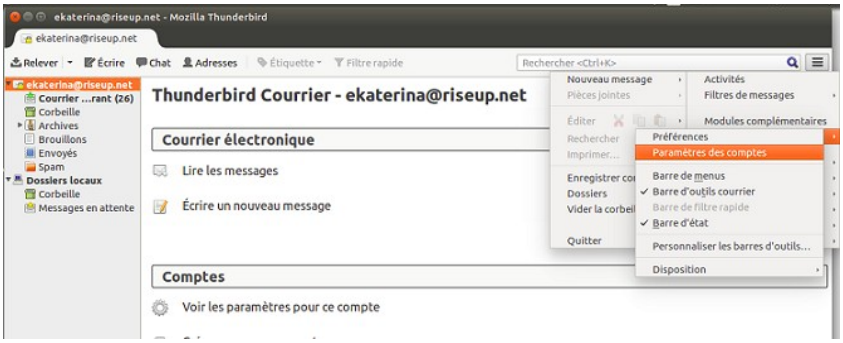
6 https://ssd.eff.org/fr/module/une-pr%C3%A9sentation-approfondie-du-chiffrement-de-bout-en-bout-comment-les-syst%C3%A8mes-de

Configurer un compte de messagerie électronique



Lorsque Thunderbird démarre pour la première fois, un assistant apparaît pour te guider à travers le processus de configuration de Thunderbird permettant d'accéder à ton compte de courrier électronique.

(Ne pas garder Debian live user comme nom, décocher se souvenir du mot de passe si tu ne veux pas qu'il soit sauvegarder dans thunderbird en clair)



Si tu n'as pas cette fenêtre, démarrer à nouveau l'assistant, depuis la fenêtre principale Thunderbird, choisir en haut à droite ☰ ► Préférences ► Paramètres des comptes et ensuite depuis la fenêtre Paramètres des comptes choisir Gestion des comptes ► Ajouter un compte de messagerie….

Entre le champ nom, ton adresse électronique et ton mot de passe (celui de ton e-mail)

Tu dois préciser quel protocole utiliser pour se connecter à ton fournisseur de courrier électronique, soit IMAP, soit POP. Si c'est tu démarre avec cet outil utilise IMAP.

Tableau récapitulatif de riseup.net entre pop et imap :

	POP	IMAP
Stockage	**Votre ordinateur**. En utilisant POP, vous téléchargez tous vos courriels sur votre ordinateur et les supprimez des serveurs de riseup.net. C'est à vous de gérer l'archivage des mails.	**Serveur Riseup**. IMAP laisse tous les messages sur le serveur. Une autre façon de voir cela est que le client courriel IMAP fournit une vue des données existantes stockées sur le serveur.
Mobilité	**Basse**. POP marche bien uniquement quand vous vérifiez vos courriels principalement depuis le même ordinateur.	**Haute**. IMAP vous permet d'utiliser différents clients et de les garder synchronisés.
Vitesse	**Plus rapide**, puisque tout est simplement téléchargé une fois sur votre ordinateur.	**Plus lent**, puisque le client courriel doit faire des requêtes au serveur de façon répété.
Quota	**Illimité**. Vous n'aurez jamais à vous inquiéter du quota si votre client est configuré pour supprimer les messages sur le serveur après téléchargement.	**Limité**. Vous aurez un quota limité.
Sécurité	**Haute**. Les messages ne sont pas stockés en permanence sur le serveur (*Note : c'est vrai que si vous faites confiance au serveur mail sur le fait qu'il ne fait pas de copie des mails*).	**Plus basse**. Vous devez vous fier à Riseup pour le stockage.

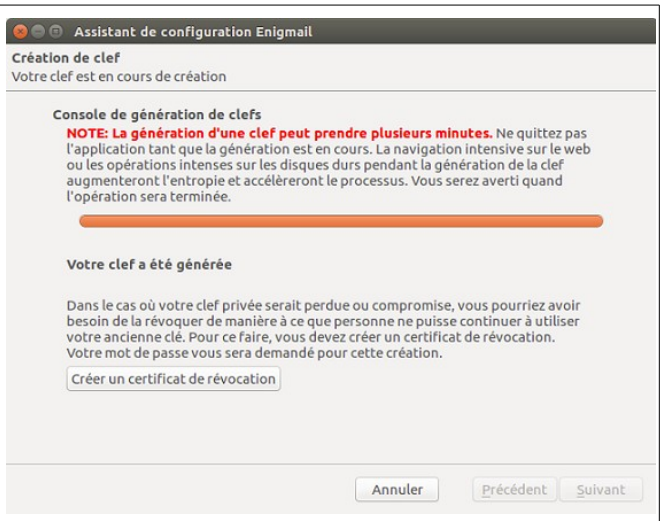
Configuration de la clef OpenPGP avec Enigmail

Si tu veux plus d'imprim' écrans sur ces démarches, tu peux en trouver beaucoup ici : https://securityinabox.org/fr/guide/thunderbird/linux/ (seulement après le chapitre 4.2)

Thunderbird dans Tails inclut Enigmail une extension pour chiffrer et authentifier les messages électroniques en utilisant OpenPGP.

Pour configurer Enigmail pour ton compte de messagerie, tu peux démarrer l'Assistant de configuration Enigmail en choisissant ☰ ▸ Enigmail ▸ Assistant de configuration et suivre pas à pas ce qui est demandé, il te faudra une nouvelle phrase de passe pour ta clef pgp (choisir novice, et enigmail configurera à la fois thunderbird et ta clef pgp). Si t'as plusieurs comptes mails dans ton thunderbird, il te sera demander à quelle adresse mail tu veux faire ta clef pgp.

A propos du certificat de révocation :



Vous devriez générer un *certificat de révocation* pour avertir les autres lorsqu'une clef n'est plus valide. Il faut faire cela si :

- vous arrêtez d'utiliser une paire de clés
- vous perdez une clé privée
- vous oubliez le mot de passe d'une clé privée
- vous pensez qu'une clé privée est compromise ou partagée avec d'autres

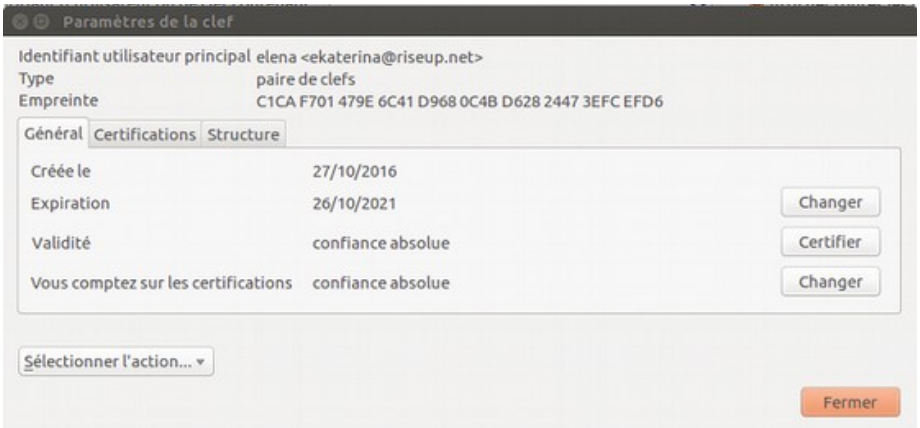
Il est particulièrement important de générer un certificat de révocation si vous prévoyez de charger vos clés publiques sur un serveur de clés. Il n'y a aucun autre moyen de "supprimer" une clé une fois qu'elle est chargée, de plus il n'est pas recommandé d'avoir des clés compromises ou anciennes conservées sur un serveur de clés. Cela peut être déroutant.

Ce certificat ne contient pas de données sensibles et ne peut être utilisé pour connaître votre clé privée, mais quelqu'un.e pourrait la charger sur un serveur clé et invalider votre paire de clé actuelle, donc laissez la dans un endroit sûr.

Afficher et gérer les paramètres des clefs :

Une fois que tu as généré ta paire de clés *GnuPG* et configuré ton compte de messagerie pour travailler avec **Enigmail,** tu pourras voir et gérer les paramètres de votre trousseau de clés (privées et publique) en suivant les étapes ci-dessous.

Clique sur ☰ pour afficher le menu Thunderbird puis sélectionne Enigmail > Gestion de clefs.



Si tu doubles-clique sur la clef qui t'intéresse tu pourras accéder à ces paramètres.

Ces fenêtres affichent, entre autres choses, l'ID de ta clé publique et son empreinte.

Par exemple, l'*ID de la clé publique* pour *ekaterina@riseup.net* est **0x3EFCD6** tandis que l'**empreinte** complète est **C1CA F701 479E 6C41 D968 0C4B D628 2447 3EFC EFD6**. Cette fenêtre affiche également la date d'expiration de ta clé (26 octobre 2021 dans ce cas).

Tu dois partager ta clé publique avec les autres pour qu'iels puissent t'envoyer des messages chiffrés. Tu dois aussi partager ton empreinte complète, via un canal différent, pour que ton/ta correspondant.e puisse vérifier que la clé publique que t'as envoyée t'appartient réellement. Tu ne dois jamais partager ta clé privée, car quiconque en a une copie peut déchiffrer les messages qui te sont envoyés et signer les messages pour qu'ils apparaissent comme provenant de toi.

Si tu souhaites modifier le mot de passe qui protège ta clé privée, **clique** sur **[Sélectionner action...]** et **sélectionne Modifier mot de passe**. Ton mot de passe actuel t'es demandé et tu dois en choisir un nouveau. Pour révoquer votre clé, **clique** sur **[Sélectionner action...]** et **sélectionne Révoquer la clef**.

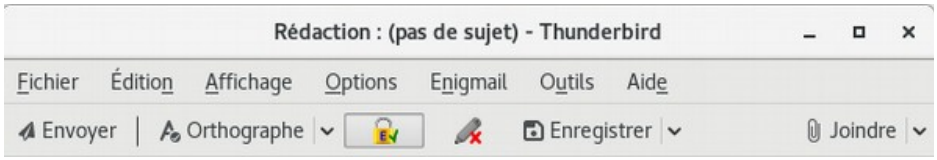
Envoyer sa clef publique

Dans Thunderbird : Ecrire => Enigmail => joindre ma clef publique (ou joindre une clef publique si tu veux en mettre plusieurs). *Ne jamais envoyer sa clef privée !*

Récupérer une clef publique / chiffrer un message

Si on t'as envoyé une clef publique, c'est un fichier qui ressemble à Ox[chiffresetlettres].asc, tu enregistre temporairement le fichier dans un endroit qui sera supprimé à la fin de session (genre le bureau), et tu cliques 2 fois sur le fichier (ça va faire automatiquement « ouvrir avec l'importeur de clef »)

Maintenant tu peux chiffrer tes mails avec la personne qui vient de t'envoyer sa clef.



Quand tu écris un message et que tu tapes le nom d'un.e correspondant.e dont tu possèdes la clef publique, automatiquement tu devrais avoir le  . Si le cadenas est encore barré en rouge, clique dessus pour forcer le chiffrement. Si en envoyant le message tu reçois une fenêtre « Sélection de clé d'Enigmail » avec marqué « aucune clé valide », dans cette fenêtre fais «actualiser la liste des clefs ». Si la clef publique n'apparaît pas cochée c'est que tu n'as pas téléchargé la clef publique.

Voilà maintenant le corps du message et les pièces jointes sont chiffrés de bout en bout (si t'as bien le ), mais pas les destinataires du message (le serveur sait à qui tu envoie les messages chiffrés), ni l'objet du message (attention à ne pas écrire un objet trop explicite)

Joindre sa clef publique en pièce jointe par défaut

Bonus pratique

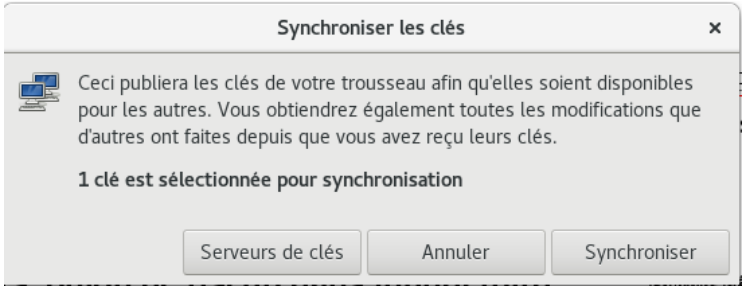
Dans thunderbird, tu fais ☰ => préférence => paramètre de compte => sécurité openpgp => Préférences d'enigmail => général => afficher les menus et paramètres pour expert => ok => ok (de la page paramètre de compte). Puis ☰ => préférence => paramètre de compte => sécurité openpgp => avancée => joindre ma clef publique au message => ok
Parfois faudra expliquer à certaines personnes c'est quoi cette pièce jointe...

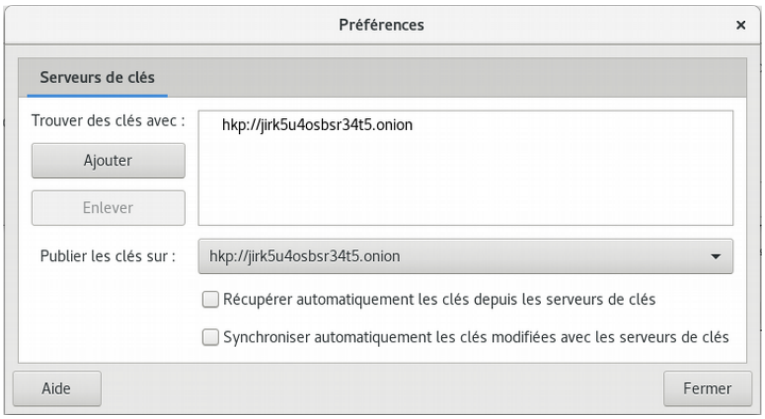
Bonus pratique

Mettre sa clef publique sur un serveur de clef

Quiconque tapera ton adresse mail dans un serveur de clef pourra trouver ta clef publique.

Dans Tails, tu vas dans  (outil 4 de la page 11) => Gérer les Clefs (ouverture de la fenêtre mot de passe et clef) => Clés GNUPG, tu sélectionnes ta clef personnelle, tu cliques sur Distant => Synchroniser et publier des clefs => Serveurs de clés => publier les clefs sur : là tu sélectionne ce qu'il y a => Fermer => Synchroniser.





De la même façon pour télécharger une clef potentiellement présente sur un serveur de clef tu reviens dans la fenêtre Mot de passe et clef => Clés Gnupg => Distant => chercher des clés distantes (attention à vérifier l'emprunte par cette méthode, n'importe qui pourrait avoir mis cette clef)

Mettre les serveurs .onion de riseup dans thunderbird

Bonus sécurité

Dans thunderbird, ☰ => préférence => paramètre de compte. Aller dans le paramètre serveur de chaque boite mail à modifier, remplacer pop.riseup.net ou imap.riseup.net par 5gdvpfoh6kb2iqbizb37lzk2ddzrwa47m6rpdueg2m656fovmbhoptqd.onion (actuellement)

Aller dans serveur sortant (smtp), tout en bas à gauche, cliquer 2 fois sur l'adresse mail, remplacer le nom du serveur (mail.riseup.net) 5gdvpfoh6kb2iqbizb37lzk2ddzrwa47m6rpdueg2m656fovmbhoptqd.onion
Pour vérifier l'adresse du serveur (qui peut changer ou que ce document peut ne pas mériter cette confiance), il faut aller sur le site de riseup, à la page tor : https://riseup.net/fr/security/network-security/tor

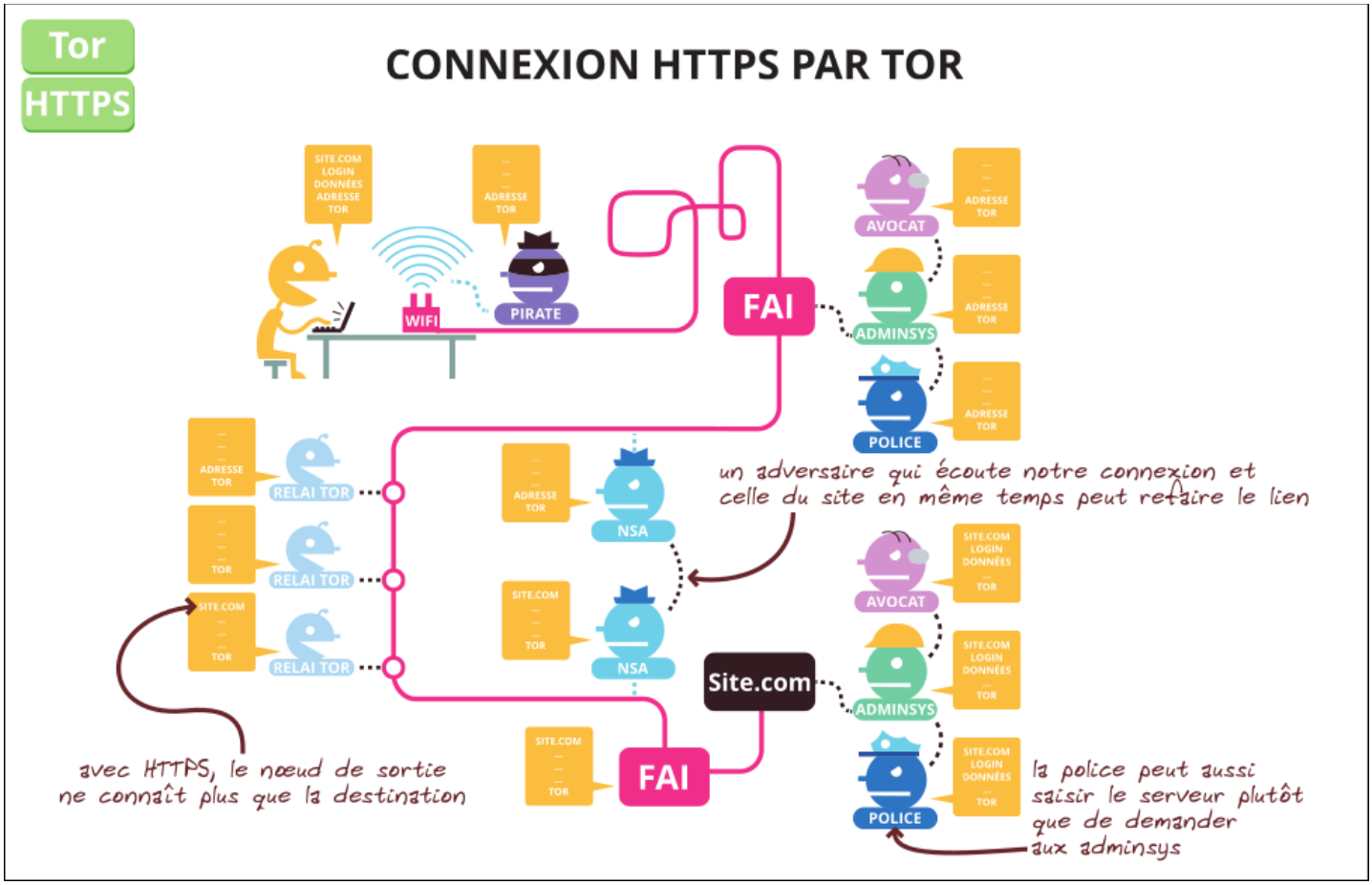
Pour le premier mail, et à chaque mise à jour des serveurs .onion de riseup, il faudra ajouter une exception de sécurité pour des questions de certificat la première fois que tu vas aller relever tes mails, et la première fois que tu vas envoyer un mail (après c'est bon). Il peut être important de faire « view » avant de confirmer le certificat de sécurité, et de vérifier le SHA-256 fingerprint. (procédure complète ici : https://riseup.net/fr/security/network-security/certificates)

Tor

Qu'est-ce que TOR?

Tor est un logiciel libre associé à un réseau public de plusieurs milliers de serveurs (aussi appelés nœud ou relais). Tor signifie The Onion Router, il va choisir en avance 3 relais sur le réseau de manière pseudo-aléatoire. Les données recherchées sur internet vont être chiffrées sur le relais 3, ces données chiffrées vont être elles mêmes chiffrées sur le relais 2, elles mêmes chiffrées sur le relais 1. Chaque relais sait seulement d'où ça vient avant, et où elles vont juste après (le relais 3 sait que ça vient de relais 2 et que ça va sur tel site internet après, mais ne connais pas le relais 1). D'où l'image de l'oignon, le relais déchiffre une première fois mais n'a toujours qu'accès qu'à des données chiffrées, relais 2 pareille, et le relais 3 déchiffre la dernière partie.

Ce qui signifie dans la théorie que tous les intermédiaires jusqu'au relais 1 savent que tu vas sur Tor mais ne sait pas sur quel site tu vas, tous les intermédiaires après le relais 3, savent que quelqu'un.e dans le monde va sur tel site, le site te voit arriver de l'adresse IP du relais Tor.



Qu'est-ce que HTPPS ?

Quand dans l'URL (l'adresse du site) tu vois HTTP://, cela signifie que la totalité des intermédiaires après le relais 3 de TOR savent ce que tu demandes exactement au site internet (dont tes login, tes mots de passe si on t'en demande). La plupart des sites ont

une version « HTTPS », le S est pour « sécurisé ». Cela signifie que ce qu'on fait sur le site sur lequel on va est chiffré par une clef de chiffrement qui appartient au site. A partir du relais 3, les intermédiaires sur la ligne sauront qu'on va sur riseup.net, mais n'auront pas accès à nos mails et à nos mots de passe ni ne sauront si on consulte nos mails ou si on lit une page aléatoirement sur le site.
Cette sécurisation est essentielle à la fois pour limiter notre emprunte, mais aussi pour éviter qu'un intermédiaire modifie le contenu de ce que nous envoie un site (puisque l'intermédiaire n'a pas accès au contenu des données, il ne peut pas les modifier)
Ca c'est la théorie, en pratique plusieurs éléments peuvent donner des données sur ce que l'on fait sur le site internet (tracker, éléments d'autres sites sur la page qui peuvent ne pas être sécurisés,...). De plus cette sécurité peut comporter plusieurs limites : la question de comment le site gère ce chiffrement, certains chiffrements ne sont pas assez robustes, et comment il gère ses clefs de déchiffrement, si on peut lui faire confiance ou non. Ca c'est côté confiance lié au serveur du site.
Il y a aussi la confiance lié au transport des données. C'est la limite des autorités de certification, qui peut entraîner l'écoute / la modification du trafique internet (dit *attaque de l'homme du milieu*). Les *autorités de certification* sont des tiers qui ont la capacité de nous certifier que le site sur lequel on va est bien le bon site, d*'authentifier l'identité de ce site / correspondant*.

- Un site peut soit être auto-certifié, ou avoir une certification non reconnu par le navigateur, dans ce cas un message te demandera de rajouter une exception, de reconnaître cet inconnu qui dit être lui-même.
- Soit le site est certifié par une autorité reconnu par le navigateur (154 autorités reconnues par Firefox). Cette autorité peut être des entreprises, des organisations, des gouvernements, des banques,… Elle peut délivrer des faux certificats (ce qui veut dire qu'on pense être sur tel site, mais qu'on est en fait ailleurs). Elle peut être usurpée. Et enfin il y a beaucoup d'autorité reconnu par un navigateur, une autre autorité pourrait certifier un faux site, le cadenas vert apparaîtra.

Tor présente l'avantage de te protéger jusqu'au 3ème relais de *l'attaque de l'homme du milieu*, rendant plus compliqué une attaque ciblée, mais cette attaque est possible à partir du 3ème relais. On ne développera pas plus sur ce sujet, on a juste introduit que HTTPS ne te protège pas de tout, n'est pas un chiffrement parfait et ne doit pas t'empêcher de faire attention à ce que tu fais sur internet / à réfléchir à d'autres types de protection. Par exemple utiliser PGP pour chiffrer tes mails, le HTTPS de riseup ne protégera pas le contenu de tes mails de tout, comme dit sur leur site[7]. Pour un chiffrement de bout en bout, il est important que la clef privée de PGP soit stockée en local, et pas sur un

7 https://riseup.net/en/security/network-security/secure-connections

serveur distant (comme peut le proposer protonmail, attention à leur propagande qui est partiellement mensongère), signifiant que tu te connectes à protonmail par https.

Darkweb / deepweb, qu'est-ce que le .onion ?

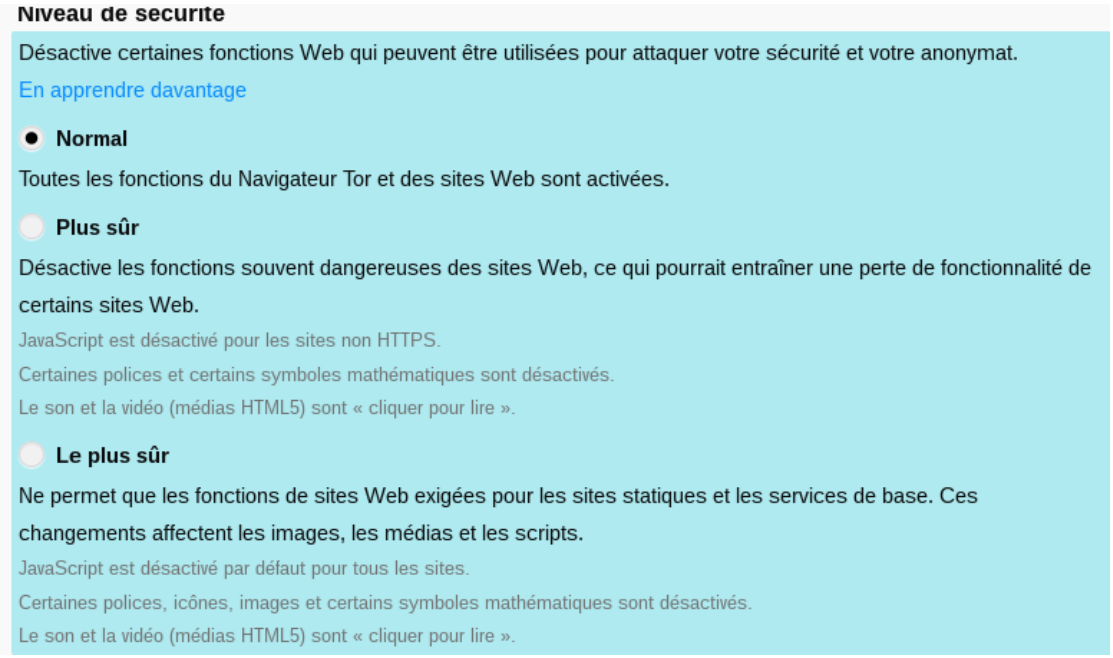
Quelques notions : le « deepweb » et le « darkweb » sont des termes inventés par les médias. Le *deepweb*, ce sont des sites qui ne sont pas répertorié par les moteurs de recherche. Pour y accéder il faut connaître directement l'URL (l'adresse du site), des sites en recensent un certain nombre.
Le *darkweb* concerne les sites qui sont accessibles uniquement par le réseau TOR et ne sont pas non plus répertoriés par un moteur de recherche. Ces sites finissent par .onion.
N'importe qui peut mettre un site en .onion. Quand tu sors du 3ème relais tor, tu rentres alors dans le 3ème relais tor du site, puis le 2ème puis le 1er. On a donc 6 relais tor entre nous et le site, nous on connaît les 3 premiers relais, le site les 3 derniers, et chaque nœud tor connaît juste le relais d'avant et celui d'après.
Une fois le 6ème relais passé, on a alors le chiffrement proposé par le site. Contrairement au chiffrement de HTTPS, les adresses de sites en .onion sont souvent long et compliqués car ils proposent l'emprunte partielle (pour l'ancien adressage) voir complète. On n'a pas besoin de certificats (même si quelques rares sites ont obtenu des certifications sur leur .onion), la sécurité passe par le fait de connaître l'emprunte du site.
Pour connaître ces sites, il faut soit l'avoir de bouche à bouche, soit par site internet qui recense d'autres sites.
Il est important de bien vérifier qui propose quoi, car n'importe qui peut proposer n'importe quoi. Attention donc aux arnaqueureuses qui vous proposent des choses.

Quelques exemples de sites en .onion :
Créer un site ou heberger des fichiers sous TOR : http://popfilesxuru7lsr.onion/
Site pierre par pierre sur l'antirepression: http://pppierreqdmdhrfm.onion/
Mettre en place un serveur en .onion (tor) : https://hack2g2.fr/articles/hiddenservice
Zerobin : http://zerobinqmdqd236y.onion/ pour envoyer des messages chiffrés éphémères et auto-destructibles.
La plupart des sites du réseau mutu en ont un.

Paramètres de sécurité de Tor

Tor a de multiples limites. Par exemple une entité avec un peu de moyens techniques / juridiques peut, si elle présume que tu te connectes de telle box pour publier sur tel site, essayer de faire des correspondances entre ce qui sors de ta box et entre sur le site. Si le besoin s'en ressent, il peut être intéressant de ne pas passer par des box qui nous sont attribuées pour certaines publications.
Il est bien plus compliqué de se défendre d'une entité plus puissante qui mesurerait tout ce qui entre et sort du réseau tor.
Il existe aussi sur internet des scripts avec certains failles qui peuvent révélés ton adresse IP malgré Tor. Pour limiter cela, il est important de tenir Tails à jour, il est aussi possible d'augmenter les paramètres de sécurité du navigateur Tor : Tu cliques sur  puis

« Paramètres de sécurité avancée ». Par défaut il est en normal, ce qui correspond à une qualité de navigation qui ne change quasiment pas d'un navigateur normal. Il est possible d'augmenter ce niveau pendant la session, ça enlèvera certains scripts réputés pouvant avoir régulièrement des failles de sécurité. La mise en page de certains sites peuvent être modifiés, parfois certains contenus ne seront plus téléchargés (images, vidéos,…), ou certains sites ne marcheront pas sans leur donner des autorisations temporaires si on pense pouvoir leur faire confiance.



Sites qui censurent tor

Il existe plusieurs types de censure du réseau tor, qui vont de l'image capcha (espèce de jeu pour pouvoir vérifier que tu « n'es pas un robot »), à l'obligation de données des données personnelles supplémentaires (carte d'identité, numéro de téléphone...) jusqu'à l'impossibilité d'accéder au site.

Cette censure peut cibler **certains nœuds tor**. Dans ce cas tu peux changer de nœuds de sortie tor pour ce site (ça ne le fera que sur l'onglet sur lequel tu fais ça). Il faut parfois le faire plusieurs fois si on a la malchance de tomber sur plusieurs nœuds qui se sont vus interdits.

Pour ça dans la barre URL, tu cliques sur le cadenas  . Puis « nouveau circuit pour ce site ».

Cette **censure peut cibler la totalité du réseau tor**. Ce qui n'est pas si compliqué à cibler pour les sites car tous les nœuds tor sont publics. Dans ce cas tu peux essayer de passer par un proxy pour aller sur le site tel que : (attention uniquement si tu n'as pas à saisir de données personnelles -login, mot de passe-, le proxy pouvant récupérer ces données). Tu peux de préférence passer par des alternatives à ce site : alternative libre (cf liens sur la dernière page de cette brochure), certains sites censurent d'un côté tor mais

proposent des services en .onion pour les gens qui sont dans des pays où leur site est censuré. (par exemple facebook : https://facebookcorewwwi.onion/[8]).
Autre utilité : Ca peut parfois **permettre d'aller un peu plus vite dans la navigation** (on peut passer par des nœuds avec une bande passante plus rapide) ou encore limiter les liens entre 2 travaux sur le navigateur (**Il est recommandé de redémarrer complètement Tails pour séparer 2 identités virtuelles et de ne pas se limiter à changer de circuit**)

Bridge et internet

Prérequis : Nécessite de connaître un Bridge

Si tu ne veux pas qu'au niveau de ton fournisseur d'accès internet on sache que t'utilises TOR (par exemple lorsque tu es dans un pays où TOR est interdit ou suspect – dans ce cas là c'est bien de se renseigner de manière plus approfondi), il est possible d'utiliser un « bridge ». Il s'agit d'un nœud in-officiel de TOR, donc moins connu.
Dans le Tails greeter (page Bienvenue dans Tails!), faire le « petit plus » => « connexion réseau » => configurer un bridger Tor ou un proxy local. Démarrer Tails (avec ou sans la persistance)
Là tu te connectes à internet. On te présente une page « se connecter à Tor », il faut faire « configurer ».

Ouvrir la persistance d'une clef Tails dans une autre

Tu souhaites ouvrir la persistance d'une clef Tails 2, sur une clef Tails 1 allumée.
Si tu n'y arrives pas par la procédure classique. Clef Tails 2 étant branchée, tu vas dans Applications => Utilitaires => Disques, tu sélectionnes la clef Tails n2, dans Volumes tu sélectionnes la partition avec un cadenas, tu appuies sur le cadenas ouvert, tape ta phrase de passe. La partition se sépare en 2 (Luks et ext4), tu sélectionnes celle d'en dessous (ext4) et tu appuies sur ▸. Tu peux ouvrir n'importe quelle dossier et voir ta clef apparaître.

8 Cf texte « Si tu dois tout de même utiliser facebook », quelques conseils d'indymedia nantes https://nantes.indymedia.org/articles/37002. A priori pour créer un compte il faut que tu valides avec un numéro de téléphone (à toi de trouver un moyen d'avoir un téléphone non relié à toi).

III) Astuces / bug récurrent sur Tails

L'ordi essaye de démarrer sur la clef mais ça ne marche pas

Vérifie les messages d'erreurs affichés (si ça ne marche pas à cause du sécure boot, ou parce que t'as un vieil ordi en architecture 32 bit). S'il y a marqué Error starting GDM with your graphics card, ça vient de la carte graphique, consulte la page « Problèmes connus avec des cartes graphiques » du site de Tails.
Si t'as la page d'amorçage de Tails, essaye de démarrer sur le « mode sans échecs » (*Tails troubleshooting mode*). Tu peux aussi consulter la liste des problèmes connus du site de Tails si des solutions ne sont pas proposées en cherchant le modèle de ton ordi.

Ma clef Tails ne veut plus démarrer ! (alors qu'elle démarrait avant sur l'ordi)

Suite à une mise à jour, mauvaise manip, ou autre Tails ne démarre plus sur mon ordi. 3 possibilités sont toujours là :
1) Je vais voir la documentation de Tails par exemple sur la page qui parle des problèmes de la mise à jour effectuée.
2) Je fais une mise à jour manuelle (plus haut dans le document), par exemple dans le cas ou la clef a été éteinte avant la fin de la mise à jour.
3) Rien à faire, les 2 premières solutions ne marchent pas (cas par exemple de clef usb trop vielle, de mauvaises qualité ou qui a été malmené). Je créé une nouvelle clef Tails et je clone mon ancienne. (chapitre sauvegarder sa clef Tails).
Cas particulier : La dernière version de Tails ne marche pas ou à un bug chez moi (à cause de l'ordi ou de la clef). Ca arrive, remets la version Tails d'avant ou va voir la page des nouveautés de Tails[9] souvent iels parlent de la dernière mise à jour, des bugs qui ont été remontés.

Je configure un logiciel (comme thunderbird), mais au redémarrage je perds tout

Soit t'as oublié d'activer ta persistance avant de faire les configuration. Sinon va voir dans *Applications => Configurer le stockage persistant* et regarde si ton logiciel est coché.

Trouver rapidement un logiciel

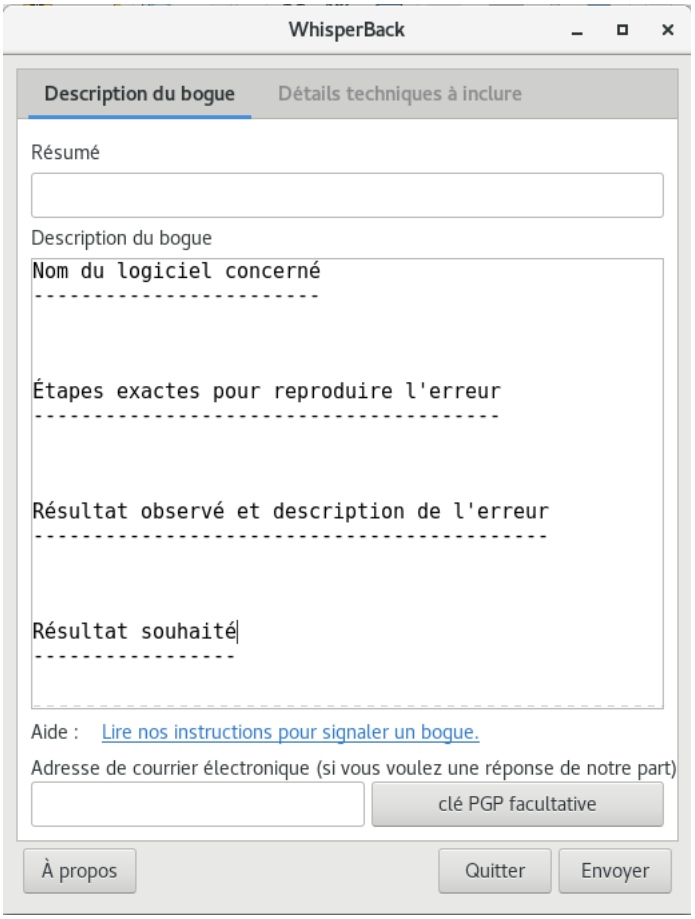
Si tu tapes ta souris contre le bord tout en haut tout à gauche une barre de recherche apparaît pour trouver un logiciel.

Y a des choses qui ne marchent pas avec ma Tails / signaler un problème

Ca peut venir de ton ordi, de ta clef ou de ce que t'as installé. Ca peut venir de ta clef Tails (bug de thunderbird,...), tu peux essayer de la réinstaller.

9 https://Tails.boum.org/home/index.fr.html

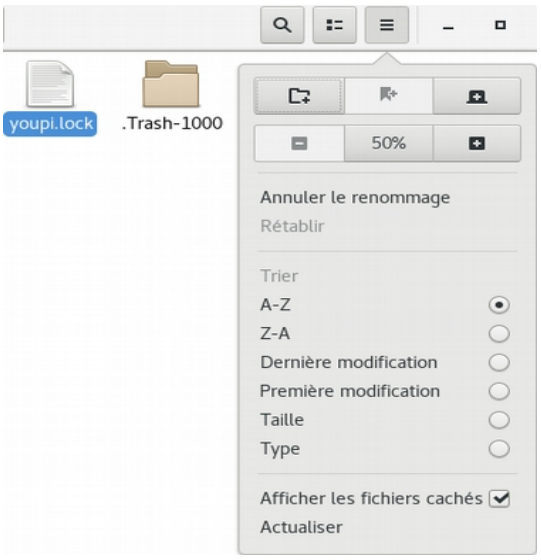
Ca peut venir des ordis qui ne sont pas tout à fait adaptés à Tails. Par exemple certains modèles d'ordi n'active pas la wifi avec Tails.
Regarde à la page problèmes connus s'ils n'en font pas état (avec parfois des solutions). s'il n'y a pas, tu peux utiliser l'outil pour signaler une erreur. S'il ne faut pas l'utiliser à la légère pour ne pas surcharger les personnes qui travaillent sur Tails, c'est aussi une manière de contribuer à Tails car iels peuvent à partir de ces données soit proposer une solution s'il y a, soit rajouter à la liste des problèmes connus et essayer de trouver une solution pour les prochaines versions de Tails. Tu vas dans *Applications => Outils système => WhisperBack Error Reporting*
Il est important d'être aussi précis.e que possible dans l'énonciation du problème, et, si c'est possible, de traduire en anglais.



Après une mise à jour, subitement j'ai pas accès à toute ma persistance malgré le fait qu'elle soit activée

Alors sache d'abord que ta persistance est toujours accessible à partir d'un autre système d'exploitation (de préférence une autre clef Tails). Tes données sont là, ça doit être le lien vers ceux-ci qui n'existent plus. Démarre avec la persistance, va voir dans *Applications => Configurer le stockage persistant.* Si ça te propose de mettre un mot de passe, mets le même qu'avant et recoche les cases, redémarre ça devrait être bon.

Plus d'espace libre ?



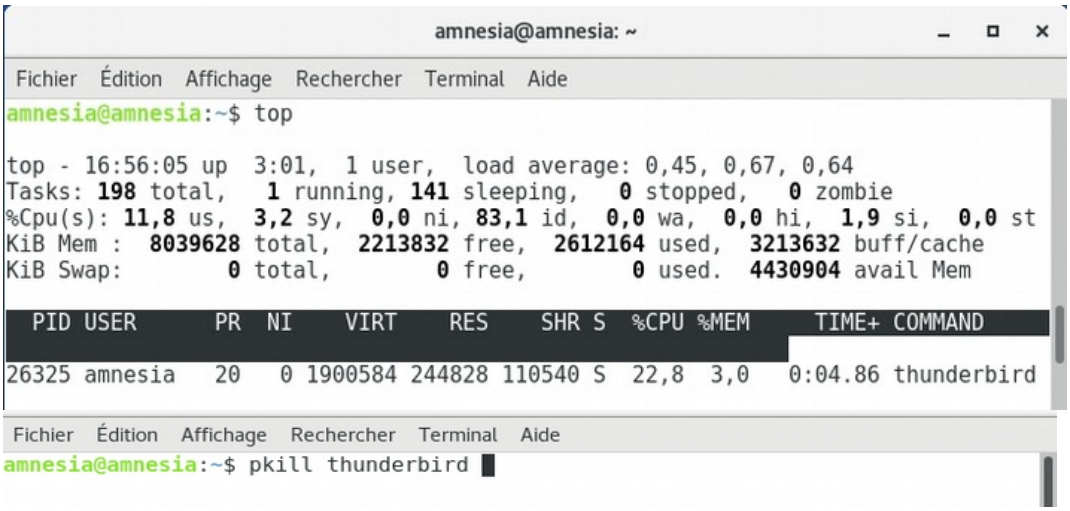
Si tu n'as plus de place dans ta persistance ou si y a plus de données indiquées que réellement présentes, pas de panique, dans ton dossier persistant tu cliques en haut sur 3 traits horizontaux, « afficher les fichiers cachés ». Là tu vas avoir de nouveaux fichiers en *.Quelquechose.* Ces fichiers (dans le dossier persistant) ne sont à priori pas importantes et sont supprimables. En particulier : *.Trash-1000*, c'est ta corbeille (et si tu mets à la corbeille ta corbeille elle va être complètement enlevée).

Un fichier s'ouvre toujours en lecture seule ou ne s'ouvre pas ?

… alors qu'il n'y a pas déjà le même fichier d'ouvert et qu'avant ça marchait. Même astuce que le paragraphe d'au-dessus. Tu fais *Afficher les fichiers cachés.* Un fichier en *.lock* avec avant le même nom que le fichier qui te pose soucis. Supprime ce fichier, il indique à la persistance qu'il serait déjà ouvert ailleurs. Si c'est pas ça, il faut changer les droits de permissions du document.

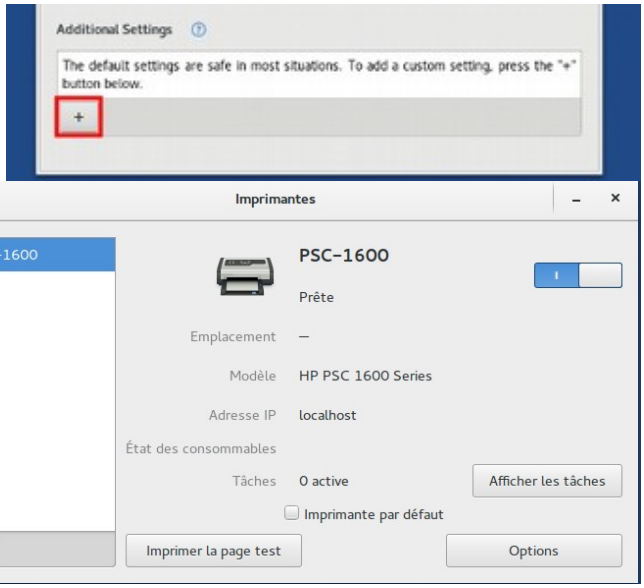
Un logiciel fait ramer Tails?

Ouvre un terminal (simple), tap *top* pour lister les processus actif. Il y a une colonne *command*, ça correspond au nom à mettre pour détruire ce processus. Pour avoir à nouveau accès au terminal appuies sur *q* (pour finir la commande *top*). Pour détruire le processus fais *pkill nomduprocessus.*
Exemple pour thunderbird :



Je n'arrive pas à avoir internet dans certains lieux ou j'avais identifier mon ordinateur

… comme la fac, certains lieux publics. Si ton ordinateur était identifié pour ouvrir internet à cet endroit pour pouvoir y utiliser le wifi, il faut que Tails arrête d'usurper l'adresse mac (c'est en gros l'identité de ton ordi, Tails l'usurpe automatiquement pour te protéger). Pour cela au démarrage, dans la fenêtre du Tails Greeter il faut faire le petit + et enlever l'usurpation de l'adresse mac.



Ajouter une imprimante :

Tu vas dans : Applications => Outils système => Paramètres => Imprimantes => « + » => Ajouter une imprimante.
Certains modèles d'imprimante peuvent ne pas fonctionner (ou difficilement) avec Tails.

Toutes tes clefs pgp publiques et privées ont disparu subitement

Ne télécharge pas de clefs publiques / ne créé pas une nouvelle clef pgp. Dans un dossier tu vas dans « + autres emplacements » => ordinateur => live => persistence =>

TailsData_unlocked => gnupg. Si le fichier pubring.kbx fait 0 octet, tu cliques alors sur ≡ coche « Afficher les fichiers cachés ». Là tu vérifies que le fichier « pubring.kbx~ » (c'est le backup qui s'enregistre avant chaque modification dans les clefs, le ~ indique qu'il est en fichier caché) n'est pas vide. Faut supprimer "pubring.gpg" puis renommé manuellement "pubring.gpg~" en "pubring.gpg", et là tu devrais trouver toutes tes clés dans le trousseau de clés de Tails.

Impossible de télécharger un document par le navigateur Tor

Si t'as un message d'erreur de type « *n'a pu être enregistré car vous ne pouvez changer le contenu de ce répertoire. Changez les propriétés du répertoire et essayez à nouveau, ou essayez d'enregistrer ailleurs.* » quand tu télécharges un document, tu copies l'url, quitte le navigateur Tor, tu le redémarre, colles ton url et tu vas pouvoir faire ton téléchargement.
Ce message semble arriver lorsque par exemple dans un mail thunderbird tu clique sur un lien alors que le navigateur n'est pas allumé, là un message nous dit que Tor n'est pas prêt et si tu fais démarrer le navigateur tor la bonne page va s'allumer, mais il sera impossible de télécharger quoique ce soit avec ce navigateur ainsi allumer. Dans ce cas il est mieux de d'abord ouvrir le navigateur Tor puis de cliquer sur le lien (ou de le copier coller).

Penser à faire des sauvegardes :

Une clef Tails ça se perd facilement, ça se fait piquer et les clefs usb ont une durée de vie bien moindre qu'un disque dur (surtout les premiers prix). Si t'y mets des données importantes, pense à y faire des sauvegardes régulièrement.
Si c'est seulement sauvegarder ton dossier persistant, c'est simple, tu peux copier sur une autre clef chiffrée tes documents. Tu peux aussi t'amuser à exporter manuellement tes clefs publiques/ privées, pour sauvegarder les quelques infos que tu veux sauvegarder etc etc.
Si tu veux sauvegarder toutes tes configurations enregistrées dans la persistance (pgp, thunderbird, pidgin, …) pour retrouver ta clef Tails à l'identique, il faut savoir utiliser un terminal. T'as ici une tuto pour *copier manuellement vos données persistantes vers une nouvelle clé Tails* : https://Tails.boum.org/doc/first_steps/persistence/copy/index.fr.html
Ici des indications si tu veux faire une sauvegarde complète avec une clef usb chiffrée intermédiaire :

Avisée : Attention à ce que tu fais dans cette partie et de ne pas se tromper
Pour sauvegarder toutes les données persistantes d'une clé Tails "A" sur une clé USB "B" munie d'une simple partition chiffrée :
1) Booter sur la clé Tails "A" avec la persistance activée et avec un mot de passe administrateur
2) Brancher la clé USB chiffré "B" (de taille suffisante pour tout sauvegarder), la monter en la déchiffrant (tu vas dessus normalement et tape ta phrase de passe).

3) Depuis n’importe quel dossier, tu vas dans + autres emplacements => ordinateur => live => persistence => TailsData_unlocked et ici tu copies les fichiers que tu souhaite sauvegarder. Tu peux avoir :
Le dossier apt et le fichier live-additional-software.conf correspondent aux options de persistance des [[Logiciels additionnels|configure#additional_software]. Mais il est nécessaire d'avoir les droits d'administration pour les importer, et cela sort du domaine couvert par ces instructions. À noter que ce dossier ne contient pas de données personnelles.

- Le dossier bookmarks correspond à l'option de persistance Marque-pages du navigateur.
- Le dossier cups-configuration correspond à l'option de persistance Imprimantes.
- Le dossier dotfiles correspond à l'option de persistance Dotfiles.
- Le dossier electrum correspond à l'option de persistance Client Bitcoin.
- Le dossier gnupg correspond à l'option de persistance GnuPG.
- Le dossier thunderbird correspond à l'option de persistance Thunderbird.
- Le dossier nm-connections correspond à l'option de persistance Connexions Réseaux.
- Le dossier openssh-client correspond à l'option de persistance Client SSH.
- Le dossier Persistent correspond à l'option de persistance Données personnelles.
- Le dossier pidgin correspond à l'option de persistance Pidgin.

S’il n’y a pas certains de ces dossiers c’est que tu ne les as pas activé dans la persistance la fonction.
3) Ouvrir le terminal administrateur, ton mdp administrateur taper :
nautilus
Attention à ce moment tu peux maintenant accéder à tes dossiers en mode administrateurice. Il est important de ne pas s’en servir à la légère et de le fermer une fois l’opération terminée.
Tu vas sur ta clef usb (sur le côté sûrement y aura plein de chiffres et de lettres en dessous de la corbeille, vérifie que c’est bien elle). Elle se situe aussi dans + autres emplacements => media => amnesia => dossier de ta clef
Tu colles les éléments
Ta sauvegarde est prête à être mise dans un coin pour le jour ou t’as besoin de refaire ta clef Tails à l’identique.

Pour restaurer les données sauvegardées sur la clé Tails d'origine ou sur une nouvelle clé Tails :
1) Booter sur la nouvelle clé Tails "C" avec la persistance activée et les droits d’aministrateurices. (vérifie d’avoir préalablement cocher dans Application => Tails => configurer le stockage… tous les éléments que tu souhaite activer)
2) Brancher la clé chiffrée USB "B", la déchiffrer, copier tous les dossiers de sauvegarde
3) Ouvrir un terminal administrateur, ton mdp administrateur, puis tape dedans *nautilus*
Attention à ce moment tu peux maintenant accéder à tes dossiers en mode administrateurice. Il est important de ne pas s’en servir à la légère et de le fermer une fois l’opération terminée.
Va dans + autres emplacements => Ordinateur => live => Persistence => TailsData_unlocked.
Colle les dossiers qui normalement devrait avoir les mêmes noms mais vide– sinon tu t’es trompé.e quelque part. Faire « fusionner » après avoir cocher « Appliquer cette action pour tous les fichiers et dossiers » puis remplacer en ayant cocher cette même case.
5) Toujours dans le terminal administrateur, rétablir les bons droits d'accès sur "A" avec :
find /live/persistence/TailsData_unlocked/ -uid 1000 -exec chown -R 1000:1000 '{}' \;
Laisser tourner jusqu’à avoir une nouvelle ligne root@amnesia:~# , c’est bon vous pouvez accéder à toutes tes fonctionnalités sur ta nouvelle clef tails.

Pour aller plus loin quelques sites :

- Le **guide d'autodéfense numérique**, par ici : https://guide.boum.org/
  Ce guide a été fait à destination des militant.es, il pose à la fois les problématiques politiques ainsi que des réponses techniques et des tutoriels à faire sur Tails et sur debian.
- Pages de riseup sur la sécurité (humaine, matériel, réseau), tout n'est pas traduit : https://riseup.net/fr/security
- Sur le site de Tails, il y a une page de documentation très bien faite : https://tails.boum.org/doc/index.fr.html
- A destination plus associative, il existe aussi les fiches informatiques pour réduire les risques liés à la surveillance du Cecil : https://www.lececil.org/fiches/
  Ce dernier vulgarise pas mal d'éléments, en cas de doutes de sécurité, mieux vaux se référer au guide d'autodéfense numérique.
- Les articles y sont principalement en anglais : Security-in-a-box est un guide de sécurité numérique destiné aux activistes et défenseureuses des droits humains dans le monde entier (version française existe mais moins de pages dedans) https://securityinabox.org/en/

Listes de logiciels et de services alternatifs :

- Une liste de sites militants qui font de l'hébergement, des vpn, des adresses mail ou tout un tas d'autres services basés pour faire de la sécurité informatique et la non récolte des données (riseup) : https://riseup.net/fr/security/resources/radical-servers
- Listes logiciels libres alternatifs (les liste proposée comporte des logiciels qui ne sont pas forcément pour faire de la sécurité informatique, mais plus basée sur le fait que ces sites ne sont pas fait pour récolter vos données personnelles) :

- https://prism-break.org/fr/
- https://degooglisons-internet.org/liste

Site d'info et d'analyse :

- Informations sur les lois de surveillance numérique : https://www.laquadrature.net/

Outils pédagogiques

- Outil visuel pour savoir qui nous traque sur un certain nombre de sites : https://trackography.org/
- Outils pédagogiques sur ce qu'on peut récolter à partir de notre navigation : http://ip-check.info/?lang=en et https://panopticlick.eff.org/
- Outil pédagogique sur les infos virtuelles piquées au quotidien à balthasar : https://www.digitale-gesellschaft.ch/dr.html
- Au sujet des données laissées sur internet : https://myshadow.org/fr

Autre

- Si tu veux payer des choses de manière anonyme (bitcoin et autres). Un article publié à ce sujet par ici: https://rebellyon.info/Comment-payer-de-maniere-anonyme-sur-le.html
- Faire sa propre carte interactive : https://umap.openstreetmap.fr/fr/

Contact : des questions ? Des critiques ? Des remarques ? souslaplage@riseup.net