Fous ta cagoule sur le Net !

Petit guide d'initiation à *Tails*

deuxième édition – avril 2016

tails.boum.org

Tails

theamnesicincognitolivesystem

Beaucoup d'entre-nous utilisons un grand nombre d'outils informatiques créés par de grosses sociétés avec lesquelles l'État marche mains dans la main.

On le fait, on sait que c'est mal, que c'est le nouvel ordre capitaliste qui dirige internet et l'informatique, que les gouvernements s'en servent pour asseoir leur pouvoir, mais voilà, l'informatique c'est compliqué, ça prend du temps, etc. C'est vrai. Un ordinateur est une machine compliquée, et la comprendre de A à Z peut prendre une vie.

Par contre, pas besoin d'être ingénieur/euse en informatique pour protéger ses données, ni pour communiquer avec ses potes sans enrichir les fichiers des RG ou ceux d'une entreprise qui arrive à transformer nos données en euros.

L'objet de ce guide est de permettre, à celles et ceux qui n'y connaissent rien, d'utiliser un outil global efficace pour lutter contre le flicage du monde informatique et la centralisation d'internet. Il s'agit d'un système amnésique qui vous rend incognito. Rien que ça ! Et en plus, c'est à la portée de toutes et tous.

CONFIDENTIALITÉ ET ANONYMAT POUR TOU·TE·S ET PARTOUT !!

Concrètement, vous avez une clé USB dans la poche. Vous la branchez à n'importe quel ordi, vous démarrez, vous rentrez votre mot de passe. Vous pouvez maintenant travailler sur le tract de votre collectif prônant la lutte armée et l'assassinat de Donald Trump, l'envoyer par mail à votre pote qui a les flingues, et en discuter un peu avec elle/lui. Vous enregistrez ce tract et vous le publiez sur internet. Vous éteignez l'ordi, absolument aucune trace informatique n'y est laissée, et personne n'a pu intercepter vos données. Et même si c'était le cas, elle seraient illisibles. Et même si elles l'étaient, personne ne pourrait les relier ni à vous, ni à la personne propriétaire de l'ordi, ni à celle détentrice de la ligne internet. Pas mal non ?

Présenté comme ça, c'est magique et infaillible …

RIEN N'EST INFAILLIBLE ! SOYEZ TOUJOURS PRUDENT-E-S DANS VOTRE UTILISATION DE L'INFORMATIQUE ET MÊME DE *TAILS* !
DES FAILLES PEUVENT SUBSISTER
ET LA PLUPART DU TEMPS, ELLES SONT ENTRE LA CHAISE ET L'ECRAN !

Bon, cette brochure est un petit guide d'initiation, pas une encyclopédie. Vous n'y trouverez pas toutes les réponses à vos questions. Heureusement, la documentation de *Tails* en ligne est super bien faite : https://tails.boum.org/doc/

Sommaire pour une cagoule informatique !

Quelques explications préalables

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 ou 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***. Votre utilisation n'aura aucune influence sur l'ordinateur utilisé, et n'y laissera absolument aucune trace, nulle part.

>>> *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.

Il faut bien comprendre l'état d'esprit de *Tails* : tout y est fait pour être sécurisé au maximum. Par contre, **la manière dont vous l'utilisez peut comporter des failles**. Quelqu'un-e peut tout à fait être derrière votre épaule et surveiller votre écran, lire votre mot de passe sur le clavier quand vous le tapez, ou si vous l'écrivez dans votre agenda. L'inconvénient c'est que personne ne pourra vous redonner votre mot de passe si vous le perdez. La taille de votre clé USB aussi réduira vos possibilités de stockage… bref, y'a des inconvénients, qui découlent de la volonté d'être amnésique et incognito et des possibilités technologiques.

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* a été conçu par des gen-te-s comme nous, mais dingues d'informatique, qui se sont dit qu'il fallait un outil simple pour les parano-e-s et les gen-te-s qui ont raison de se cacher dans leur utilisation d'un ordi. Aucun gain d'argent (*Tails* est fait pour être gratos), aucune gloire, juste du bon sens et une volonté politique de **se réapproprier nos outils informatiques** !

Tout est une question de confiance. Les outils qui composent *Tails* ont fait leurs preuves[1]. Le fait que tout le monde puisse connaître la recette de *Tails* renforce cette confiance. Même si vous ne comprenez rien au code source de *Tails*, certain-e-s savent le lire, et les concepteurs-trices le savent bien : ils/elles n'ont pas intérêt à y cacher quoi que ce soit.

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 ça fait partie de l'installation. C'est parti !

1 Ils ont par exemple été utilisés par Edward Snowden, un des hommes les plus surveillés de la planète aujourd'hui.

Niveau : **Très facile** (solution 1)
ou **Difficile** (solution 2)

Installation

La partie la plus relou

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

Pour la clé USB, choisissez une clé de 4 Go minimum. Elle sera complètement effacée lors de l'installation de *Tails*, donc sauvegardez vos données avant de commencer.

Concernant la « source », deux solutions :

- **[SOLUTION 1]** Trouver un utilisateur de *Tails* (explications page 14)
- **[SOLUTION 2]** Utiliser le fichier d'installation de *Tails* téléchargeable sur internet

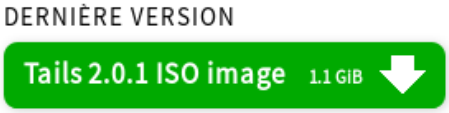
[SOLUTION 1] : La meilleure solution (et de très loin la plus simple) est de trouver un-e utilisateur/trice de *Tails* en qui on a confiance. Car dans *Tails*, un petit logiciel très simple permet de créer une nouvelle clé *Tails* en cinq minutes et trois clics (et je n'exagère même pas). La procédure est expliquée dans cette brochure, page 14 (« Répandre Tails »). En plus, ça permet d'en discuter avec quelqu'un-e, et de voir des vrais gen-te-s dans la vraie vie.

> Près de chez toi existe forcément 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 … 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
> À Toulouse, des « install partys *Tails* » sont régulièrement organisées, autour des associations *Tetaneutral* ou *Toulibre*

[SOLULTION 2] : Il faut commencer par télécharger le fichier d'installation de *Tails* depuis le site https://tails.boum.org/download/. Une fois téléchargé, nous vérifierons que le fichier téléchargé n'a pas subi d'altérations lors de son téléchargement. Et nous nous assurerons surtout que le fichier téléchargé est le bon ! Qu'il n'a pas été modifié par un-e méchant-e RG et replacé là l'air de rien. Ce(tte) RG pourrait par exemple modifier *Tails* pour que quand vous envoyez un mail à vos potes, il/elle en reçoive une copie. Ce serait moche... Une fois ces vérifications faites, il va falloir créer la clé USB de démarrage, puis booter dessus. Ces opérations sont un peu fastidieuses sous Linux, un peu plus compliquées encore sous Windows, et encore plus sous Mac… Donc, préférez vraiment l'aide d'un-e utilisateur/trice de *Tails*. Si vous n'avez aucune autre solution, les quelques pages suivantes vont vous aider à créer votre clé Tails, mais ne seront peut-être pas suffisantes. N'hésitez pas à chercher un peu plus loin sur le net, notamment sur le site officiel *tails.boum.org*. Soyez curieu-se-x.

Sur cette page (https://tails.boum.org/download/), il vous faut télécharger trois fichiers :

- **« L'image ISO » de *Tails* :** il s'agit du contenu de *Tails*. Le fichier se nomme *tails-i386-2.2.iso*, ou quelque chose s'en approchant (en fonction de la dernière version dispo). Téléchargez-le en cliquant sur le bouton :



- **La clé de signature de l'image ISO** : après l'avoir importée, cette clé vous permet de vous assurer que le fichier ISO n'a pas été « corrompu » lors de son téléchargement.

  Le fichier se nomme *tails-signing.key*, et vous pouvez le télécharger en cliquant sur le bouton :

- **La signature cryptographique** sert à s'assurer que c'est bien le Tails officiel que vous avez téléchargé et pas un autre. Le fichier s'appelle *tails-i386-2.2.iso.sig*, et le bouton :

Vous avez téléchargé tous les fichiers nécessaires à la vérification de cette satanée « image ISO ». Bien !

La vérification de l'intégrité de votre image iso

Sur Linux, vous devez d'abord installer *seahorse-nautilus* ainsi que *shared-mime-info*. Une fois fait, double-cliquez simplement sur chacun des deux fichiers de signature, et suivez les instructions, c'est assez simple. Voici les pages correspondantes de la doc de Tails :

https://tails.boum.org/doc/get/verify_the_iso_image_using_gnome/index.fr.html
ou
https://tails.boum.org/doc/get/verify_the_iso_image_using_the_command_line/index.fr.html

Sur Windows, il faut installer un logiciel qui se nomme *Gpg4win* (https://www.gpg4win.org/). La documentation de ce logiciel est en anglais. Concernant l'import de la clé de signature, vous trouverez de l'aide ici :
https://www.gpg4win.org/doc/en/gpg4win-compendium_15.html

Concernant la vérification de l'intégrité de l'image iso, vous trouverez de l'aide là :
https://www.gpg4win.org/doc/en/gpg4win-compendium_24.html#id4

Sur Mac, il vous faut le logiciel GPGTools que vous trouverez ici : https://gpgtools.org/. Peu d'aide est disponible malheureusement, mais c'est possible !

Votre fichier ISO est vérifié ? Très bien ! Maintenant, l'installation de la clé Tails !

Niveau : Moyen à Difficile

Créer une clé bootable !

Une clé « bootable », c'est une clé USB qui contient un système d'exploitation (comme *Tails*), et qui sera reconnue comme telle par n'importe quel ordinateur, qui pourra démarrer dessus.

Si vous êtes sur Linux, il va falloir utiliser la ligne de commande ! Mais ne soyez pas impressionné-e-s …

Il suffit de démarrer le logiciel appelé « Terminal », et de suivre la procédure décrite dans la documentation de *Tails* ici :
https://tails.boum.org/doc/first_steps/installation/manual/linux/index.fr.html

Si vous êtes sur Windaube, c'est un peu moins impressionnant, il vous faut installer un logiciel appelé « Universal USB Installer », un logiciel libre dispo ici :
http://www.pendrivelinux.com/

Dans ce petit logiciel, il suffit de sélectionner *T(A)ILS* dans *« Linux distribution »*, sélectionner l'image iso téléchargée précédemment, et sélectionner votre clé USB. Puis cliquer sur *« Create »* et attendre la fin de l'installation.

Si vous êtes sur MacCaca, il va falloir utiliser là aussi la ligne de commande. Vous trouverez la marche à suivre dans la doc de *Tails* ici :

https://tails.boum.org/doc/first_steps/installation/manual/mac/index.fr.html

Créer une clé bootable avec un autre moyen que ceux-ci est imprévisible, voire dangereux. Il se pourrait que l'install se passe mal et que votre *Tails* comporte des failles. Les logiciels comme *UnetBootin* ou le *Créateur de disque de démarrage* d'*Ubuntu* ne sont pas appropriés pour installer *Tails* ! Et même si vous y parvenez, vous ne pourrez pas être sûr-e-s du bon état de votre clé *Tails*.

On y est presque ! Il ne reste plus qu'un peu de config pour pouvoir redémarrer sur votre clé *Tails* !

Les trois précédentes pages d'install peuvent être évitées. Il vous suffit de trouver un-e utilisateur/trice de *Tails* pour vous créer une clé *Tails* bien plus facilement !!
(procédure en page 14)

Niveau : Aléatoirement chiant / Moyen

Booter sur votre clé Tails

Dernière étape avant d'être incognito

Là, c'est aléatoire. Ça peut être ultra simple, ça peut être chiant. Tout dépend du modèle de votre ordinateur. Et là, y'a beaucoup, beaucoup de possibilités !

La première chose simple à essayer est d'éteindre son ordi, de brancher la clé *Tails*, et de le rallumer. Le but est de tomber sur un écran noir ressemblant à :

Écran de démarrage de Tails. Prêt-e pour l'incognitotisme ?

Si votre système d'exploitation habituel démarre, il va falloir indiquer à votre ordinateur qu'il faut démarrer en priorité sur les clés USB, puisque ce n'est pas le cas. On le fait sur la plupart des ordis grâce au « Bios ». Sauf sur les Mac.

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), dont 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). Cliquez dessus, et vous devriez obtenir l'écran noir 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[2]). Au démarrage, appuyez simultanément sur quatre touches :

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 »*

Si t'as cet écran avec ton macCaca, Youpi Tralala !

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

Pour les autres ordinateurs, il va falloir configurer le « Bios » ! Le « Bios » est un logiciel qui gère notamment le démarrage de votre machine, en lui disant quel disque utiliser pour commencer à faire quelque chose. Pour le modifier, redémarrez votre ordi. Au démarrage, au bas d'un des premiers écrans, vous verrez un message du genre :

```
Press F11 to enter Bios setup
  ou
F2 for order boot
```

Vous savez ce qu'il vous reste à faire : appuyer sur cette touche (habituellement F2, F10, F11, F12, ou encore « Echap ») quand on vous le propose (toujours au démarrage).

Vous aurez alors un écran à dominance bleu et gris, en anglais, sans souris. C'est un peu flippant parce qu'on a l'impression de faire des trucs d'informaticien-ne, mais pas de panique, c'est à la portée de tou-te-s. Grâce au clavier (←,↑,→,↓, Entrée et Echap), naviguez dans les menus jusqu'à quelque chose qui ressemble à « Boot order » ou « Boot priority device ». Souvent, une liste dont on peut modifier l'ordre s'affiche. Il s'agit donc (grâce à l'aide textuelle la plupart du temps dans le volet de droite ou en bas) de mettre en première position de cette liste l'élément qui correspond à une clé USB (« USB device » ou « Storage device » ...). Il est possible que vous deviez brancher une clé sur votre ordi pour qu'il la reconnaisse et vous propose ce choix.

Chaque Bios est différent et il est difficile de donner une marche à suivre globale. Vous trouverez de l'aide sur internet en recherchant « Boot clé USB Bios » (avec le modèle de votre machine) dans votre moteur de recherche préféré (pas Google mais plutôt Framabee.org, Searx.me , DuckDuckGo.com, etc.)

Une fois la priorité de boot mise à jour, le moyen de quitter le Bios est souvent d'appuyer sur la touche F10. Un message vous demande si vous voulez sauvegarder les modifications, choisissez Oui. L'ordinateur redémarrera et, si vous avez bien configuré le Bios, démarrera sur votre clé USB *Tails* (si elle est branchée et bien installée bien sûr), et vous obtiendrez l'écran noir de *Tails* (cf. page précédente). Si ce n'est pas le cas, retournez dans le Bios, c'est que vous avez loupé un truc dans la configuration.

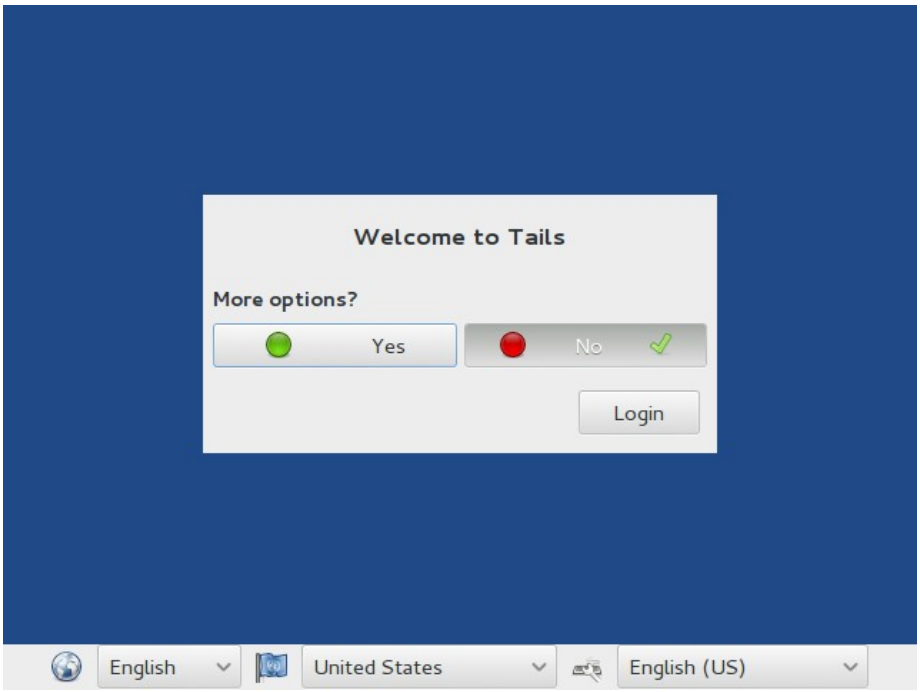
Toutes ces étapes sont relou, on est d'accords,
et je vous avais prévenu.
Si vous avez l'écran de démarrage de *Tails*, le gros est derrière vous, *Tails* est simple d'utilisation, vous verrez.

Niveau : Facile

Démarrer *Tails*, quelques détails

A l'écran noir de démarrage de *Tails*, choisissez l'option « Live ». L'option « Live (failsafe) » ne vous servira probablement jamais, mais vous pouvez l'utiliser si vous remarquez que votre système *Tails* ne fonctionne pas normalement.

Voici l'écran suivant :



Tails démarre toujours en anglais. C'est la langue par défaut, le système ne connaît pas votre localisation géographique (et ne cherchera pas à la connaître). Prenez le réflexe de choisir votre langue (case en bas à gauche), ce qui configure automatiquement votre clavier. C'est quand même plus pratique d'avoir un clavier français (surtout quand il va falloir taper un mot de passe !).

Si vous laissez *« non »* coché à *« Plus d'options ? »*, les options par défaut seront utilisées. Les options par défaut sont très safe. En cochant « oui » à « plus d'options », vous pourrez :

- **Définir un mot de passe administrateur/trice.** Ça permet d'installer des logiciels ou de réaliser des modifications importantes sur votre système. Par défaut, aucun mot de passe n'est défini, et ni vous ni personne d'autre ne pourra faire ce type de modifications système (c'est donc le mode le plus sécurisé). Si vous pensez devoir faire des modifs système, définissez ici le mot de passe qui vous sera demandé pour les faire.
- **Choisir d'usurper ou non les adresses Mac.** Rien à voir avec Macintosh ou Apple. Les adresse Mac sont des sortes de numéros d'identification de certaines parties physiques de votre ordinateur (les cartes réseau notamment). Ça peut être un moyen d'identifier une personne sur un réseau. *Tails* vous propose ici de les usurper, c'est à dire de les modifier délibérément pour en donner des mauvaises à qui serait trop curieu-se-x. Si vous êtes dans un cybercafé ou sur un ordinateur public, il se peut qu'usurper les adresses Mac rende suspecte voire impossible votre connexion au réseau.
- **Choisir des options concernant votre connexion au réseau.** Vous pouvez notamment ici la désactiver complètement pour les plus parano-e-s d'entre-nous, ou configurer une connexion via un proxy[3].

Après ces quelques explications, il ne vous reste plus qu'à accéder au bureau de *Tails* en cliquant sur **« Démarrer ».**

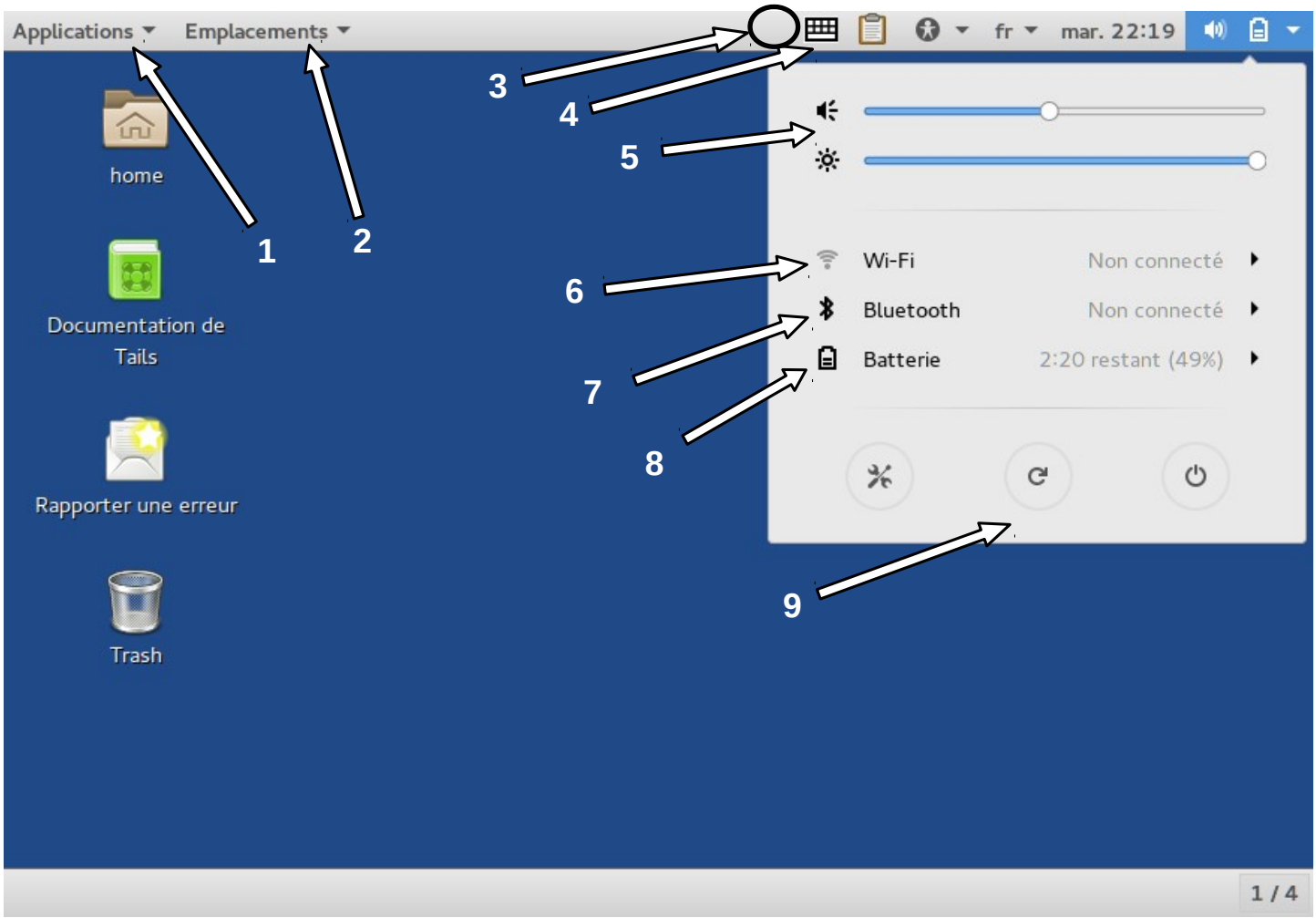
3 Un proxy est une sorte de machine-relai entre vous et internet, qui peut servir à déjouer des blocages du web (étatiques ou patronaux) ou à vous anonymiser.

Niveau : Très facile

Utiliser *Tails*

Le bureau de *Tails* en détails

Le bureau de *Tails* :



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

- [1] Une liste classée par thème des applications (des logiciels) disponibles
- [2] Quelques raccourcis pratiques
- [3] Le témoin de l'état de Tor si vous êtes connecté au réseau Tor. Ce petit outil s'appelle « Oignon Circuits » depuis la version 2.2 (mars 2016)
- [4] Un clavier virtuel, un outil pour crypter le « presse-papiers », des options d'accessibilité, le choix de la langue utilisée pour votre clavier, et la date et l'heure
- Le menu système, pour la luminosité de l'écran et le volume du son [5] , la connexion au réseau qui vous permet de vous connecter en wi-fi [6], la connectivité BlueTooth [7], l'état de la batterie [8] et les boutons de démarrage et d'extinction [9]

Sur le bureau vous avez notamment accès à votre « home », votre répertoire personnel. On en reparlera quand on voudra stocker des données (Voir la partie « Volume Persistant »).

Niveau : Facile

MAT

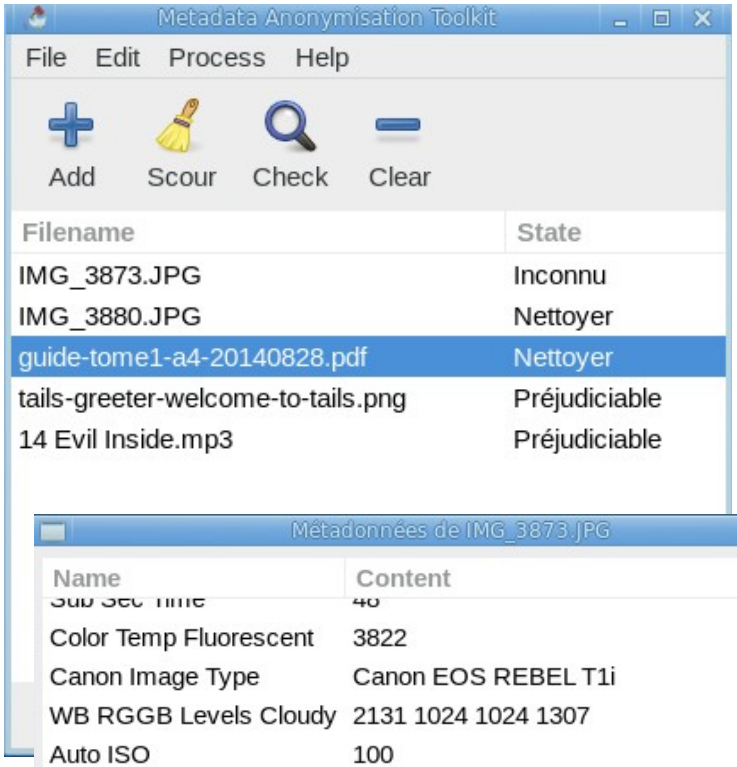
Anonymiser ses fichiers, suppression des métadonnées

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 celui 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, une photo peut comporter la taille de votre photo en pixels, la marque et le modèle de votre appareil, son numéro de série … Si la photo a été prise depuis un téléphone, on peut y ajouter votre 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 votre téléphone. Les métadonnées d'un fichier texte peuvent révéler le nom de votre ordinateur, le votre, et bien d'autres infos.

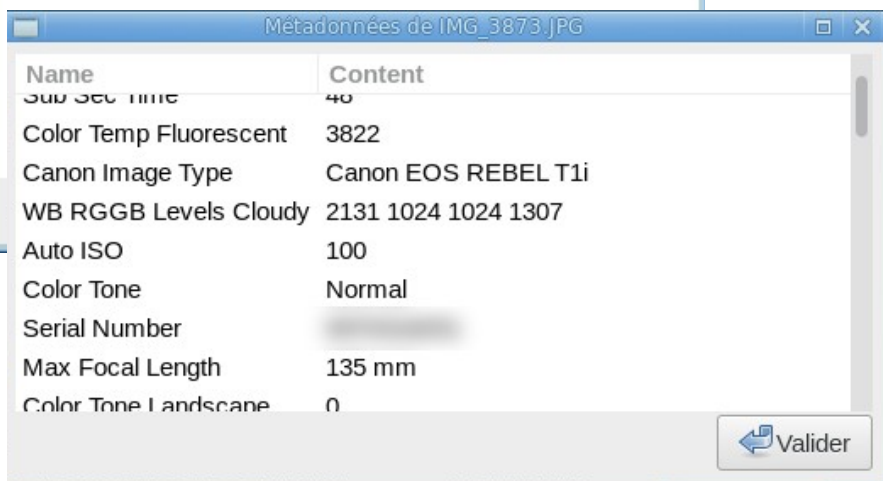
MAT (pour Metadata Anonymisation Toolkit) est un logiciel qui lit et supprime les méta-données de vos fichiers. **Il est disponible pour n'importe quelle version de Linux !** À son démarrage une fenêtre s'ouvre, dans laquelle vous pouvez glisser-déposer les fichiers à analyser.

Dans cet exemple j'y ai déposé cinq fichiers différents : sons, images, documents …



La colonne de gauche comporte le nom des fichiers, et celle de droite leur état, qui peut être « Inconnu » (pas encore analysé), « Préjudiciable » (fichier qui contient des métadonnées, quelles qu'elles soient), ou « Nettoyer » (vide de métadonnées, le terme est mal choisi, on est d'accord).

Ici, *IMG_3873.JPG* n'a pas encore été analysé. En cliquant sur « Check », l'analyse se lance. En double-cliquant sur un des fichiers de la liste, les méta-données qu'il contient s'affichent. Ça permet de les lire à l'écran dans une nouvelle fenêtre (cf. ci-contre).



Il suffit de fermer cette fenêtre et de cliquer sur « Scour » pour effacer les métadonnées du fichier sélectionné. Facile !

N'oubliez pas d'effacer les méta-données de votre tract anti-Trump avant de le diffuser sur internet !

Niveau : Très Facile

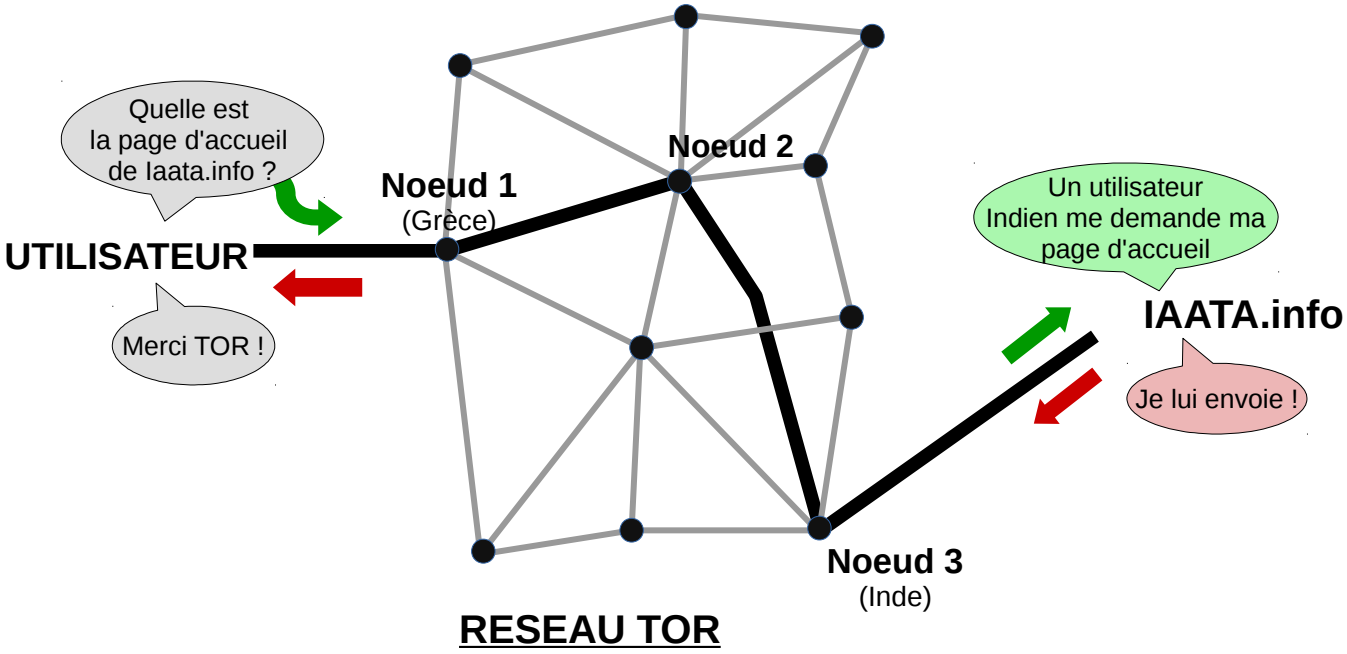
Tor

Naviguer sur internet anonymement

Tor est un réseau mondial de machines (environ 7000), mises gratuitement à disposition, et connectées entre-elles. Elles forment un maillage qui sépare votre ordinateur d'internet. Avec Tor, lorsque vous consultez internet, vous passez d'abord par ce maillage (mais sans vous en rendre compte)… et c'est le moyen connu le plus efficace pour être anonyme sur le web.

Tor ne chiffre pas vos communications sur internet. Il ne fait que cacher votre identité[4] ! Si vous vous connectez *via* Tor à votre compte Google qui comporte votre nom et prénom, Google pourra savoir ce que vous y faites, et pourra rattacher ces informations à votre nom.

En pratique, lorsque vous demandez à accéder au site www.iaata.info (par exemple) *via* Tor, cette demande passe par trois machines (des « nœuds Tor ») choisies sur le tas. Chaque machine connaît l'identité des machines avec qui elle communique. La première (qu'on imagine en Grèce) vous connaît, et sait à qui elle doit envoyer la demande de page web. L'info passe par la deuxième machine, puis la troisième (en Inde par exemple). Le site final (iaata) ne connaît que la troisième machine... Pour iaata.info (et les RG qui espionnent ce site), la personne qui demande la page est un ordi en Inde, et envoie la page d'accueil à cette machine, qui l'envoie à la seconde, puis à la première, puis à vous.



Concrètement, sous *Tails*, lorsque vous vous connectez à un réseau (par wifi ou par un câble physique), *Tails* lance automatiquement le logiciel Tor qui configure votre accès au réseau. Une fois fait, un petit message vous le signale, et l'oignon qui apparaît dans la barre du haut vous indique que Tor est prêt. En cliquant sur l'icône du navigateur Tor sur le bureau, vous accéderez à internet de manière complètement anonyme. Et pourrez diffuser vos tracts de « terroristes » sur iaata.info par exemple. Vous n'avez rien à configurer !

4 Tor cache en fait votre adresse IP. Cette adresse pourrait révéler le lieu physique dans lequel se trouve votre Box Internet ou votre modem.

Niveau : Très Facile

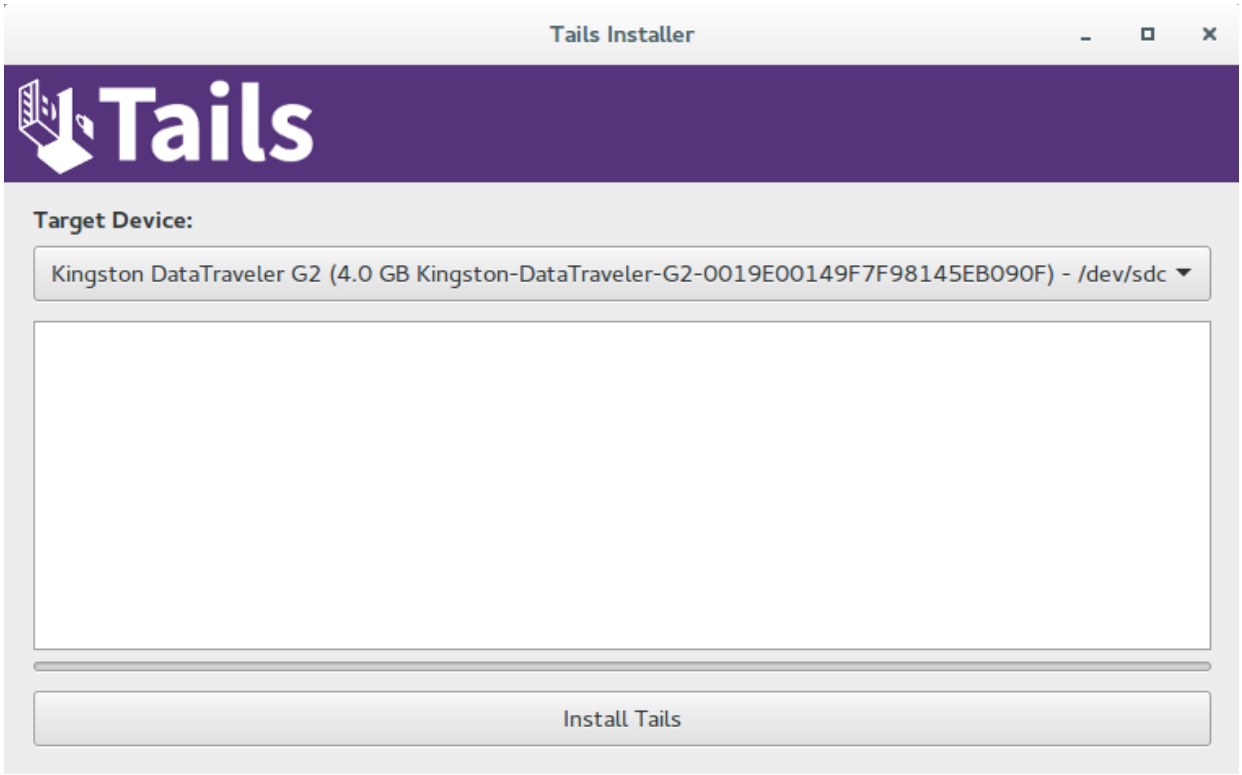
Répandre Tails

Créer facilement des clés Tails pour les potos !

Comme c'est vraiment easy et que vous aurez peut-être besoin par la suite de savoir le faire, voyons tout de suite comment créer très facilement une clé *Tails*, avec *Tails.*

Convertissez vos potes à *Tails*[5] !

Vous êtes sur votre bureau *Tails*. Branchez une clé USB de 4Go au moins. Puis, allez dans « *Applications* », puis « *Tails* », puis « *Programme d'installation de* Tails ». Dans la fenêtre qui s'ouvre, choisissez « *Install by cloning* ». Vous arrivez à la fenêtre suivante :



Choisissez ensuite dans la liste sous « *Target Device* » la clé USB sur laquelle vous voulez installer le nouveau *Tails* (on le voit sur cet écran, la mienne s'appelle *« Kingston-DataTraveler »*), puis cliquez sur *« Install Tails »*. Attendez bien la fin de l'install (ça bloque souvent un peu vers 95 %, mais soyez patient-e-s).

C'est fait ! Vous pouvez redémarrer sur cette nouvelle clé.

Bien sûr (et heureusement), l'installeur ne fait qu'installer *Tails*. Si vous avez déjà configuré un volume persistant (voir page suivante), la nouvelle clé en sera dépourvue. Ce sera une clé *Tails* vierge, prête à l'emploi !

5 Et n'hésitez pas à photocopiller cette brochure si besoin !

Niveau : Intermédiaire

Volume Persistant

Comment stocker des données sur ma clé *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 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 votre clé, qui sera entièrement chiffré, sur lequel vous pourrez stocker vos documents, et qui sera aussi utilisé par certains logiciels pour y stocker les données que vous aurez autorisé. C'est techniquement très simple à faire, il faut juste faire un tout petit effort de compréhension.

La création d'un volume persistant n'est disponible que pour les clés *Tails* créées via l'installateur présent dans *Tails*. Si vous avez installé *Tails* sur votre clé USB en téléchargeant les fichiers depuis le site de *Tails*, vous ne pourrez pas créer de volume persistant sur cette clé. Il vous suffit alors de créer une nouvelle clé *Tails* depuis celle que vous avez déjà (voir instructions page précédente), et le tour est joué. On est d'accord, c'est chiant …

Remarques et Mise en garde

- **Un tel volume persistant est une technologie assez complexe. Soyez vigilant-e-s sur votre manière de l'utiliser. Certaines modifications peuvent mettre en péril votre système *Tails* ou votre anonymat.**
- **Le volume persistant n'est pas caché. Son contenu l'est. N'importe qui peut savoir qu'une clé *Tails* contient un volume persistant (sans pour autant pouvoir le lire).**
- **Utilisez le volume persistant le moins possible. N'activez le volume persistant au démarrage que si vous êtes sûr de devoir l'utiliser. Sinon, ne l'activez pas.**
- **Installer de nouveaux logiciels ou modifier les configurations par défaut des logiciels présents peut mettre en péril votre anonymat. Soyez prudent-e-s.**

Pour créer le volume persistant, allez dans « *Application* », puis « *Tails* » puis « *Configurer le stockage persistent* ».

La première chose qu'il vous sera demandé est de créer un mot de passe de chiffrement. Ce mot de passe doit rester dans votre tête et nulle part ailleurs ! Ne l'écrivez nulle part et ne le confiez à personne (vraiment). Ce mot de passe doit être suffisamment complexe pour assurer la sécurité de vos données. Huit caractères comportant des majuscules et minuscules, des caractères spéciaux ET des chiffres, c'est vraiment la limite basse pour un mot de passe sécurisé.

Ensuite, le stockage persistant peut être activé pour plusieurs types de données, en voici quelques détails / explications :

Données personnelles		Stocker des fichiers persos, que vous retrouverez dans le dossier **home>persistent** (sur le bureau ou via le raccourci « persistent »)
GnuPG		Cela vous servira pour envoyer et recevoir des mails cryptés grâce à *Icedove* et *Enigmail* (pages 18 et suivantes)
Client SSH		SSH permet de se connecter à des serveurs à distance. Cette option permet de sauvegarder des config de connexion.
Pidgin		Pidgin est une messagerie. Activer cette option vous permettra de garder les config des comptes, vos contacts, vos conversations …
Icedove		C'est votre messagerie mail (cf page 18). Vous garderez votre configuration et vos mail en mémoire
Trousseau de clés de Gnome		Un outil de gestion des clés de chiffrement, de mots de passe, de certificats
Connexions réseau		Pour se souvenir notamment des mots de passe wifi ou autres configurations de connexion
Marque-pages du navigateur		Tout est dans le titre
Imprimantes		Il s'agit de sauvegarder les configurations des imprimantes
Client Bitcoin		La configuration et le porte-monnaie Bitcoin sont sauvegardés. (Bitcoin est une monnaie cryptée décentralisée)
Paquets APT & Listes d'APT		Si vous voulez installer d'autres logiciels sous *Tails*, vous les retrouverez plus facilement d'une session à une autre avec ces deux options activées[6]
Dotfiles		Utile pour des configurations avancées, afin de dédoubler des fichiers de config dans le répertoire personnel. Option sensible concernant la confidentialité.

Si vous avez un doute sur l'activation d'une des options, n'hésitez pas à l'activer (sauf peut-être pour Dotfiles). Vos 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 (cf page 10) vous proposera d'activer la persistance (« non » par défaut). Pour l'activer, cliquez sur « oui » et entrez le mot de passe qui vous avait été demandé lors de la création du volume.

Vous pourrez alors, une fois le système démarré, stocker vos fichier entre deux utilisations, dans le dossier Home > Persistent . Vous pouvez y accéder par le menu des raccourcis « Emplacement », dans la barre supérieure de *Tails*.

Les fichiers sauvegardés ailleurs seront effacés à l'extinction de votre machine !

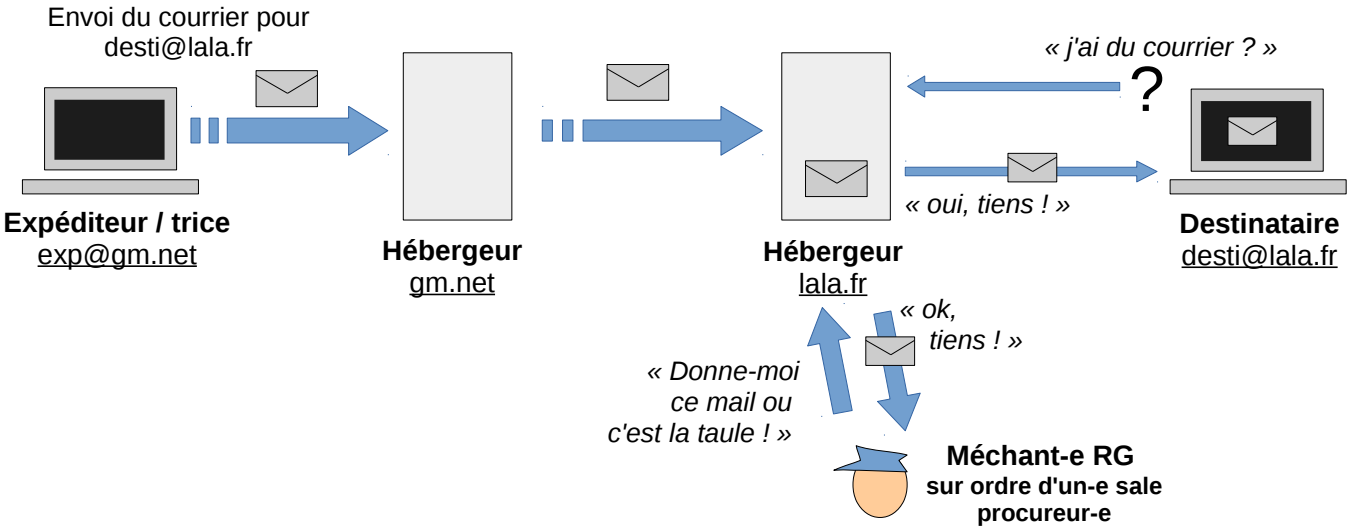
6 C'est pas si simple que ça. Vous trouverez plus d'infos dans la doc en ligne de *Tails* sur https://tails.boum.org/ . Sachez, avant de vous intéresser à comment installer des logiciels sous *Tails*, que tout ou presque est faisable avec les logiciels installés par défaut sous *Tails.* Essayez d'approfondir vos connaissances de ces logiciels en faisant par exemple des recherches sur le net. Cette brochure n'expliquera pas comment installer de nouveaux logiciels …

Icedove & Enigmail

Envoyer des mails intelligemment

Là, il va falloir faire un peu de théorie, car comprendre le fonctionnement d'un échange de mails est nécessaire.

Pour envoyer un mail, vous devez avoir une adresse mail, que vous fournit un hébergeur mail (gmail, laposte, riseup, no-log, …). Pour envoyer un mail, l'expéditeur-trice se connecte à son hébergeur, et lui transmet le mail qu'il/elle veut envoyer. L'hébergeur transmettra le courrier électronique à l'hébergeur mail du / de la destinataire qui le stocke. Lorsque le / la destinataire se connecte à son hébergeur mail, il lui délivre le courrier e-mail.



Chacune des machines dans la chaîne a accès au contenu du mail, peut en faire une copie et le stocker. Un-e méchant-e RG (ou un-e pirate quelconque) peut également intercepter votre e-mail sur le réseau, et même en réclamer légalement une copie à un des deux hébergeurs, sur ordre d'un-e procureur-e.

L'objet de ce chapitre est justement de communiquer par mail de manière sécurisée.

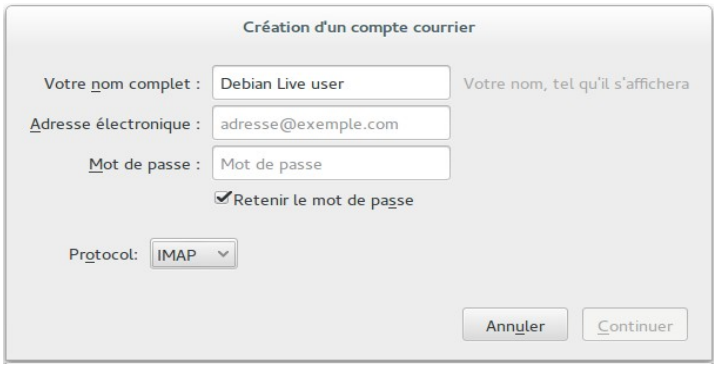
Je vous invite dès maintenant (si ce n'est pas déjà le cas) à vous créer une adresse mail chez un hébergeur non-commercial, qui protège vos données (voyez Autistici.org, Riseup.net, ou d'autres).

Vous aurez donc besoin d'utiliser et de configurer les logiciels *Icedove* et *Enigmail* (qui sont déjà installés sur *Tails*) :

- *Icedove* est un logiciel de messagerie qui vous permet de lire et d'envoyer vos mails. Plusieurs boites e-mails sont utilisables et vos courriers sont accessibles hors-connexion.
- *Enigmail* est un plugin, un logiciel associé à *Icedove*, qui permet de chiffrer et/ou signer ses mails, et lire des mails chiffrés (casser ce type de chiffrement mettrait plusieurs mois / années de calcul pour les machines les plus puissantes de la planète).

Configurer et utiliser Icedove

Lire et écrire des mails simplement

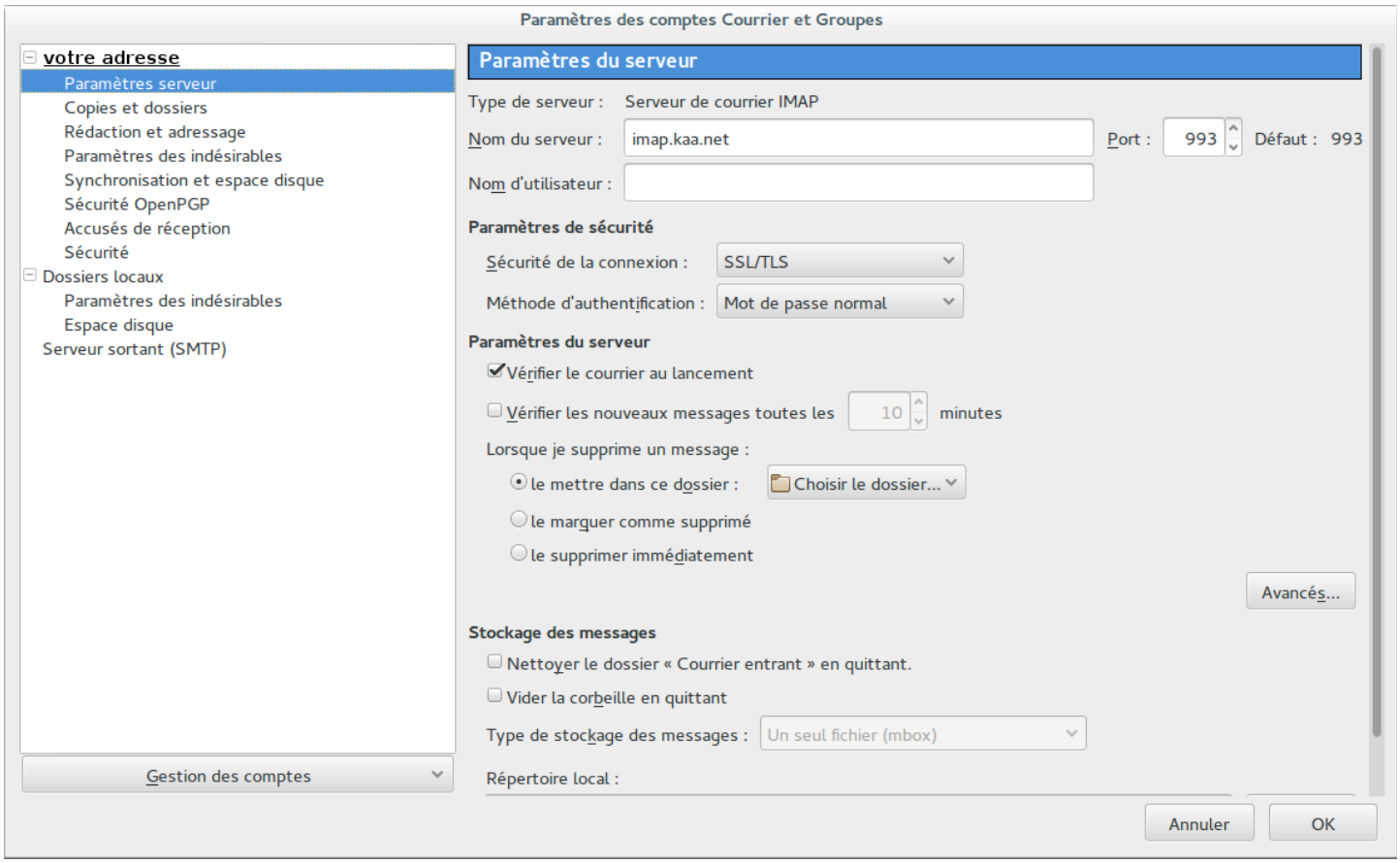


Au démarrage de *Icedove*, une fenêtre de configuration s'ouvre pour configurer votre première adresse e-mail… *« Nom complet »* c'est le nom qui s'affiche à vos destinataires. Rentrez ensuite votre adresse électronique, ainsi que le mot de passe d'accès à votre boite mail.

Votre mot de passe sera retenu dans le volume persistant, donc crypté. Pas d'inquiétude. Protocole : IMAP par défaut, c'est très bien[7].

En cliquant « continuer », un message assez mal rédigé et un peu obscur s'affiche :
« `TorBirdy a désactivé la configration automatique de Thunderbird pour protéger votre anonymat. Les paramètres de sécurité recommandé pour [votre adresse] on été selectionné. Vous pouvez maintenant configurer les paramètres de l'autre compte manuellement.` »[8]

Les « paramètres de l'autre compte » sont en fait les paramètres de ce compte. Vous arrivez alors sur une fenêtre de configuration que l'on va détailler :



7 Le protocole IMAP consiste à copier vos mails sur votre machine, en les laissant chez votre hébergeur mail (ce qui vous servira si vous voulez y accéder par un autre moyen que *Icedove* sous *Tails*).

8 TorBirdy, c'est Tor pour les mails. Non seulement vos mails seront chiffrés, mais les hébergeurs ne pourront pas connaître votre adresse IP.

Le volet de gauche permet de sélectionner les paramètres à définir, par « thème ». Voici des détails qui vous guideront, concernant les options délicates, importantes, ou intéressantes :

Paramètres serveur	> Le **nom de votre serveur** a été défini automatiquement. Cela suffit souvent. Si vous rencontrez des difficultés, cherchez sur internet le nom et le port du serveur IMAP de votre hébergeur mail. > Vous pouvez définir un délai pour vérifier les mails (toutes les 10 ou 5 minutes paraît judicieux). > Les autres options sont explicites et peuvent être laissées par défaut
Synchronisation et espace disque	Vous pouvez choisir de supprimer les plus vieux mails stockés automatiquement afin de ne pas encombrer votre clé *Tails*. Ils resteront dispo dans votre boite mais pas sous *Tails*.
Sécurité OpenPGP	Il s'agit des options de chiffrement de vos mails. Cochez ici la case « Activer OpenPGP pour cette identité », ainsi que « Utiliser l'adresse électronique pour identifier la clé PGP ». Nous y reviendrons plus tard
Serveur sortant (SMTP)	Il s'agit ici des options du serveur pour envoyer vos mails (le serveur SMTP). À droite, votre adresse apparaît, surlignée en bleu. Cliquez sur le bouton « Modifier ». Le nom du serveur est « smtp.[votre hébergeur] ». Si vous rencontrez des difficultés à l'envoi de mails, c'est que votre serveur smtp ne vous aime pas (à cause de *Tails* ou du chiffrement). Vous pouvez le remplacer par un serveur pratiquant l'amour inconditionnel, celui de Autistici (smtp.autistici.org) ou Riseup (smtp.riseup.net) par exemple. Cliquez sur OK, ça marchera avec n'importe quelle adresse !

Cliquez sur OK dans cette fenêtre de configuration. Vous pourrez la retrouver en faisant un clic droit sur votre adresse dans le volet de gauche de *Icedove*, puis en cliquant sur *« paramètres »*. Icedove se met alors à charger vos mails que vous pourrez gérer, lire, et envoyer, mais pas encore en chiffré … ça va venir.

Configurer Enigmail

Créer des clés GPG et chiffrer ses mails

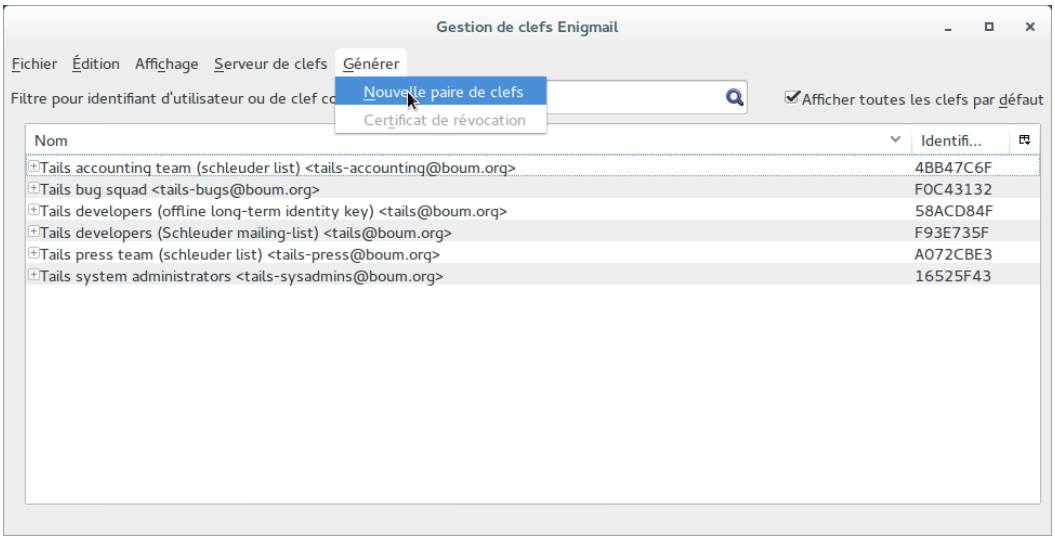
Le principe du chiffrement des mails est un peu compliqué : chaque utilisateur-trice possède une paire de deux clés (deux méga-mots-de-passe stockés dans deux fichiers).

La clé publique porte bien son nom, elle doit être diffusée à celles et ceux qui vous enverront des mails. Elle sert à chiffrer des mails qui vous sont destinés. N'importe qui peut l'avoir, elle ne sert qu'à chiffrer des mails pour vous.

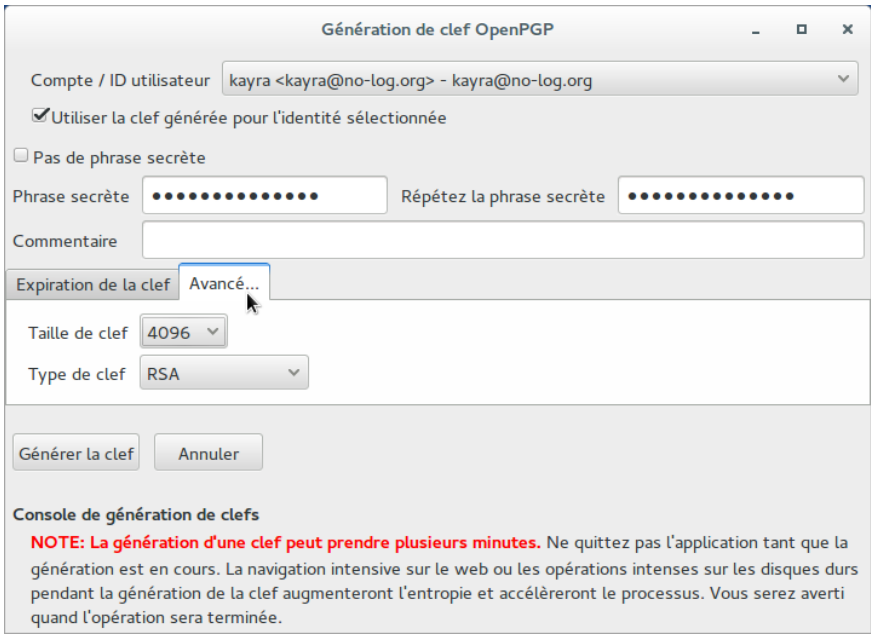
La clé privée vous sert à déchiffrer les mails qui vous seront envoyés. Personne ne doit pouvoir s'en emparer ! On la stocke souvent dans un dossier chiffré (comme sous *Tails*).

Chiffrer un e-mail le rend lisible uniquement à sa/son destinataire. La totalité d'un mail (même les pièces-jointes) peut être chiffrée, sauf son « en-tête ». L'en-tête d'un mail contient souvent le sujet du mail, les adresses des correspondant-e-s, leurs adresses IP (cachées sous *Tails*), la date et l'heure de l'envoi du mail, et quelques autres infos moins importantes. Soyez donc prudent-e-s sur l'objet notamment.

Nous allons commencer par générer une paire de clé de chiffrement GPG. Démarrez *Icedove* si ce n'est pas déjà fait. Dans le menu de *Icedove* (icône ☰ en haut à droite de la fenêtre), allez dans *Enigmail* puis *Gestion des clefs*. Les clés qui s'affichent dans la liste ci-contre sont présentes par défaut dans *Tails*, pour envoyer des mails chiffrés à l'équipe de *Tails* (classe nan ?!).



Cliquez sur le menu *Générer* puis *Nouvelle paire de clefs*. Vous arriverez sur la fenêtre suivante.



Entrez une phrase secrète[9] complexe (et souvenez-vous-en!), et une date d'expiration de la clé[10]. La taille de la clé à 4096 vous assure le chiffrement le plus sûr. Puis cliquez sur *« générer la clef ».* L'opération peut prendre plusieurs minutes, et ne doit pas être interrompue. Soyez patient-e-s.

Après un message de confirmation de la création de la clé, on vous propose la création d'un certificat de révocation, que je vous conseille d'accepter[11]. Une fois accepté, enregistrez le fichier dans votre dossier *Persistent*, et on vous demande la passphrase de votre clé récemment créée (encore heureux!). Puis on vous invite à stocker ce fichier dans un endroit sûr. Il l'est, puisqu'il est dans votre dossier *Persistent* chiffré.

9 Elle vous sera demandée lorsque vous voudrez déchiffrer un mail. Si quelqu'un vous vole votre clé privée, il lui sera demandé cette phrase, sans laquelle il ne peut rien faire.

10 Pas obligatoire mais c'est mieux d'en définir une : ça permet d'avoir une sécurité en plus. Changer de mot de passe ou de clé de chiffrement de temps en temps est une bonne pratique.

11 Si vous oubliez votre mot de passe, ou si votre clé privée est compromise (volée) ou perdue, ce certificat de révocation peut être publié pour notifier aux monde que votre clé publique ne doit plus être utilisée.

Publier sa clé publique

Pour que quelqu'un-e puisse vous envoyer un mail chiffré, il/elle a besoin de votre clé publique. Et pour envoyer un mail à quelqu'un-e, vous avez besoin de sa clé publique. Heureusement, des endroits existent pour **se partager des clés publiques : les key signing parties**[12] **!**

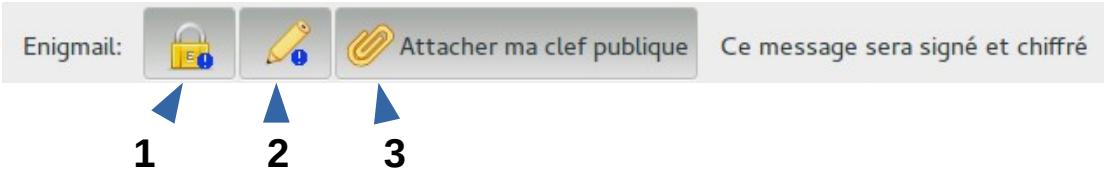
Il existe aussi des serveurs de partage de clés publiques, ce qui est nettement moins fun, et aussi moins sûr : n'importe qui peut mettre sur un serveur une clé associée à n'importe quelle adresse mail (au pire vous enverrez à François un mail qu'il n'arrivera pas à déchiffrer …)

Vous êtes certainement toujours dans le gestionnaire de clés *Enigmail* (sinon ≡ *Menu* > *Enigmail* > *gestion de clés*). Dans le menu *Serveur de clefs* vous trouverez *« Envoyer les clés publiques ».* Un serveur est déjà renseigné dans le menu déroulant, y'a plus qu'à valider.

Cherchez les clés de vos potos, et importez-les ! Menu *Serveur de clés* > *chercher des clés*. Vous rentrez un morceau d'adresse mail et le serveur vous renverra des résultats. Vous cochez et cliquez sur OK pour importer les clés cochées. Elles apparaissent dans la liste … Easy !!

Envoyer un mail chiffré ! Wouhou !

Désormais, rien de plus simple. Dans *Icedove*, cliquez sur l'icône « Écrire » (un mail). Dans la fenêtre de rédaction du mail, vous trouverez une barre d'outils qui vous propose trois choses :



1 – Chiffrer le mail
2 – Signer le mail : on peut signer sans chiffrer. La / le destinataire sera sûr-e de l'expéditrice/teur, c'est pas plus compliqué que ça. Par contre le message peut être envoyé « lisible » sur internet
3 – Attacher sa clé publique : envoyer sa clé en pièce-jointe pour que son/sa destinataire puisse vous envoyer des mails chiffrés par la suite.

Il faut que vous ayez importé la clé publique de votre destinataire pour pouvoir lui envoyer un mail chiffré ! Y'a pas à tortiller !

Écrivez votre mail, cliquez sur « envoyer ». On vous demande le mot de passe de vos clés. Hop ! Le tour est joué !

12 Les « teufs de clés de signatures ». On fait la fête en échangeant sa clé publique avec celles des potos ! Héhé !

Quelques conseils d'utilisation d'ordre général

En vrac et parce qu'il nous restait un peu de place

La sécurité n'est pas un produit mais un processus

Les moyens de communication électronique comportent toujours des failles de sécurité (au moins potentielles)

Votre utilisation de *Tails* peut altérer votre anonymat,

installer de nouveaux logiciels, accéder au(x) disque(s) dur(s) de la machine, un système pas à jour, sont des risques pris

A défaut de pouvoir se passer d'intermédiaires techniques, la sécurité des communications est basée sur la confiance qu'on a dans ces intermédiaires. Il faut toujours se demander quelles bonnes raisons vous avez (ou pas) de faire confiance dans tel ou tel intermédiaire technique (logiciels, services, matériel ...).

Éteins ton ordi, sors dans la rue, fais des trucs avec des gens !

Ne configurez et n'utilisez la persistance de *Tails* que si vous en avez vraiment besoin !

N'écrivez vos mots de passe nulle part

Utilisez le plus souvent possible les outils sécurisés, et pas uniquement lorsque vous travaillez sur des données sensibles !

Rejoignez les groupes de personnes qui défendent les logiciels libres, la neutralité et l'autogestion sur le net, ...

Beaucoup plus d'infos concernant la sécurité informatique dans le guide d'autodéfense numérique : https://guide.boum.org

----

You can now close this instructions book ...

Your memory is going to be fixed in a few seconds...

Display might be corrupted during this operation.

If your eyes do power off automatically in a few seconds,

it may mean the memory fixing has failed.

Loading, please wait...

Starting fixing the memory, press Control-C to abort earlier

++

++

++

++

++

++

++

++

++

++

++

++

++

++

++

*

* Ces messages (à deux ou trois détails près…) s'affichent à l'extinction de Tails. Voici le premier message exact : « `You can now remove the boot DVD or USB stick... The system memory is going to be wiped in a few seconds... Display might be corrupted during this operation. If the system does not power off automatically in a few seconds, it may mean the memory wiping has failed.` » Traduction non-officielle : *« Vous pouvez retirer la clé USB ou le DVD de boot … La mémoire système va être écrasée dans quelques secondes… L'affichage peut être défaillant pendant cette opération. Si le système ne s'éteint pas automatiquement dans quelques secondes, cela peut vouloir dire que l'écrasement de la mémoire a échoué »*

La succession de +++++ qui suit correspond en fait à une sorte de barre de progression de l'effacement de la mémoire vive de votre ordinateur. Juste avant l'extinction, *Tails* écrase le contenu de cette mémoire pour ne laisser aucune trace après votre passage. La clé USB peut être retirée avant cette opération. Il semblerait que certains modèles d'ordis (notamment des Mac) ne permettent pas l'écrasement de la mémoire vive à l'extinction.

≡ AVERTISSEMENT ! ≡

PRIERE DE PHOTOCOPILLER !!

* * * * * * * * * * * * *

CETTE BROCHURE EST RÉSERVÉE AUX PARANO(E)S DE L'INFORMATIQUE ET QUI N'Y CONNAISSENT PAS GRAND CHOSE. ET À CELLES ET CEUX QUI ONT PROBABLEMENT RAISON DE L' ÊTRE…

* * * * * *

ET À CELLES ET CEUX QUI ONT TOUT À CACHER. PUISQUE LA SURVEILLANCE EST PARTOUT. PUISQUE L'ANTICIPATION N'EST PLUS !

* * * * * *

BIG BROTER IS WATCHING US ! ! !

* * * * *

ET SI VOUS N'AVEZ RIEN À CACHER, CACHEZ QUAND MÊME ! ÇA VOUS PRÉPARERA À LE FAIRE, ET ÇA PROT ÉGERA LES PARANO(E)S PAR LE NOMBRE.

* * * * *

INTERNET EST À NOUS !
LE MONDE EST À NOUS !

* * * * * * * * * * * * *

21 Avril 2016