TUTORIEL

TAILS FACILE POUR TOU-TE-S

TAILS / CLEFS de chiffrage GPG / RISEUP / ENIGMAIL

Introduction :

Ce tutoriel en construction se propose de donner une méthode « pas à pas » pour créer une clé TAILS (The Amnesic Incognito Live System) avec un volume de stockage persistant chiffré et de la configurer pour envoyer et recevoir des mails chiffrés au sein d'un groupe de confiance.
Il est considéré en préalable que l'on possède déjà dans le groupe de confiance une clé Tails vérifiée. Si non se référer à https://tails.boum.org/install/debian/usb/index.fr.html pour en créer une.
On peut retrouver ce tuto actualisé à l'adresse https://tailsfacile.blackblogs.org/ ou http://popfilesxuru7lsr.onion/~tailsfacile/Tails-facile.html et aussi et surtout http://torvps7kzis5ujfz.onion/~cisenma/index.php et **https://tails-facile.antirep.net/**

Pour toutes questions écrire à tails-facile@riseup.net, ou tails-facile@tails-facile.antirep.net .Les contributions sont bienvenues : ce sont elles qui font progresser ce tutoriel !
Notamment les traductions ‼ La référence reste https://tails.boum.org/index.fr.html
D'autres tutos : https://chouettecouetteblog.wordpress.com/

Disclaimer :
La sécurité complète n'existe pas, surtout en informatique ! Mais une culture et des bonnes pratiques peuvent fournir une sécurité acceptable.
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). Ici le choix s'est porté sur Riseup mais d'autres fournissent des services équivalents notamment https://www.autistici.org/fr/index.html . Il peut-être utile de ne pas compter QUE sur Riseup ;) …

Ce tutoriel est distribué sans aucune autre licence qu'un contrat moral interdisant l'utilisation de tout ou partie des connaissances puisées dans ce tuto dans des buts qu'ils soient capitalistes, racistes, spécistes, sexistes, homophobes, lesbophobes, transphobes, grossophobes, putophobes, validistes, capacitistes, psychophobes, addictophobes, agistes ou qu'ils soient liés à l'état ou une de ces ramifications…

Ce tuto est un peu désordonné parfois. Si un problème survient, lire la suite du tuto peut donner la solution. Parfois aussi la solution c'est de redémarrer… sinon : tails-facile@tails-facile.antirep.net
! Le point faible de la sécurité informatique se situe entre la chaise et le clavier !
C'est à dire TOI /MOI et/ou tes/mes correspondantEs.
Les outils de sécurité ne sont que des outils. Mal utilisés ils sont **inefficaces.** Et ils ont des limites à connaître (fails/bugs).

La recherche de la sécurité doit être pensée collectivement : si une personne se met en danger en négligeant la sécurité, elle met touTEs ses correspondantEs en danger. Soyons bienveillantEs : soignons notre sécurité collective.
La recherche de la sécurité implique la vérification systématique des informations. Pas de confiance sans vérification. La vérification valide et renforce la confiance (ex: fonctionnement des clés de chiffrage asymétriques qui seront utilisées dans ce tuto et de leur système de signatures) .
Ne facilitons pas le travail de la surveillance : restons Incognitos et Amnésiques.
La première des sécurités c'est d'accéder à ses données ; d'où l'importance des outils permettant des procédures de recouvrement de mots de passes » (cf « ssss » point I page 9)

 # Quelques bases :
La touche "majuscule" (touches avec une flèche vers le haut à droite du §! et à gauche du <>) permet d'utiliser les caractères écrit en haut des touches, exemple : ~1234567890°+
La touche AltGr (à droite de la barre d'espacement) permet d'utiliser les caractères à droite ou en bas des touches exemple: ¬¹~#{[|`\^@]}

Raccourcis :
Ctrl+a = sélectionner tout
Ctrl+c = copier
Ctrl+v = coller
Ctrl+z = annuler la dernière action
En mettant le curseur au milieu d'un mot le double clic gauche sélectionne le mot, le triple clic gauche sélectionne la ligne.
La plupart du temps TAILS garde dans une mémoire temporaire ce qui a été sélectionné en dernier et le colle en cliquant simultanément sur les 2 boutons de la souris ou du touchpad, ou sur le bouton du milieu sur les souris à 3 boutons. Parfois pour des raisons de sécurité cela ne fonctionnera pas.

Le navigateur Tor n'a le droit d'écrire que dans le dossier "Tor Browser". Il faut donc télécharger d'abord dans ce dossier pour ensuite, déplacer les fichiers ailleurs si besoin et les ouvrir hors-ligne (c'est à dire après avoir coupé les connexions réseaux wi-fi et/ou réseau Ethernet (filaire)). Tous les fichiers venant du net sont potentiellement dangereux. Il est nécessaire de vérifier les sommes de contrôle (MD5, SHA1, SHA256) avec GtkHash (applications,Accessoires,GtkHash. Cf point H) avant de les ouvrir hors-ligne. Les procédures de vérification sont pesantes mais sont le prix de l'anonymat voire de la liberté pour soi et ses correspondantes.

A / Insérer une clé TAILS vérifiée dans une prise USB.

B / Allumer l'ordinateur : 2 cas de figure :

1/ Si le démarrage se fait directement sur Tails : COOL !! Passer au point C.

2/ Si le démarrage se fait sur votre système d'exploitation habituel (Windows ou Mac ou autre système…), éteindre l'ordinateur : il va falloir, soit aller dans le Basic Input Output System (BIOS) pour « dire » au pc de toujours démarrer de préférence sur la clé USB si elle est insérée, soit changer l'ordre de démarrage uniquement pour cette session.

https://www.whonix.org/
http://kkkkkkkkkk63ava6.onion/wiki/Main_Page
Sécurité active :
Distributions de systèmes Linux sur cd ou clés USB et orientés sécurité et audit de réseaux et applications. (Attention : potentiellement considéré comme arme dans certains pays ou contextes)
kali linux
https://www.parrotsec.org/
https://packetstormsecurity.com/files/download/98831/torshammer.tgz

#/ Mises à jour :

Tails a un agenda de mises à jour :

https://labs.riseup.net/code/projects/tails/roadmap
https://tails.boum.org/contribute/calendar/
réf : https://tails.boum.org/doc/first_steps/upgrade/index.fr.html
la procédure de mise à jour est normalement simple : à la connexion à internet Tails vérifie les mises à jour ; si une mise à jour est nécessaire, une fenêtre apparaît . Suivre la procédure et patienter.
Si pour une raison quelconque la mise à jour échoue ou ne se lance pas taper dans un terminal : tails-upgrade-frontend-wrapper
Il est aussi possible de mettre à jour à partir d'une autre clé à jour (Applications/Tails/Programme d'installation de Tails/Upgrade by cloning)
Il est également possible de mettre à jour à partir d'un fichier iso téléchargé et vérifié https://tails.boum.org/install/download/index.fr.html.

DONS et soutiens :
Les dons serviront particulièrement à tirer des brochures et payer du matériel et des services informatiques mutualisées et autogérés (hébergements, VPN, VPS, Riseup, autistici, Tor, TAILS) pour contrer la censure et le contrôle de l'information et des populations, et faire avancer la liberté et la libération totale.
-En bitcoins :
5mBTC : 1NUc3nLZnmHuaeGdzL83faRaCBkCVb8Kg
1mBTC :19NtxSVFxik4NkAMebdxWcZ2Zr1dxz1CYW
10mBTC :1McM8ESWbnMRRP6YHN9CbmEZxAodmCNmop
montant libre :13xM9Rz4aazSxChFdqKz8ZvYng7NuuYT5Q
-Via recharge de cartes bancaires PCS anonymes (coupons recharge qui s'achètent en argent liquide dans les tabacs) -Virement (contact par mail pour infos sur les virements PCS)

X/ Chiffrer le contenu d'un fichier, le presse-papier :

Ouvrir le fichier, faire Ctrl+a pour tout sélectionner, Ctrl+c pour copier, cliquer sur l'icône de l'applet de chiffrement  signer/chiffrer le presse-papier avec une phrase de passe ou signer/chiffrer le presse-papier avec une clé publique
si dessous la phrase « Tant qu'il y aura des abattoirs il y aura des guerres ! » chiffrée avec le code «Tolstoï» sans les guillemets mais avec le ï ;) :

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

jA0ECQMCPfIq5dNwriFg0mEB9bC7P+2N4SUbzdwgah0o2AgL4/MkqFka963QW/Qw
ZN1TeSJWsDj2fiCIqbmQYFJXZAbpixMUjMr7Il1cfcgtn8PoIUsPZtGs6kVU0A9r
wxzNSNwIcLqrLqHputMKLlDF
=aiWf
-----END PGP MESSAGE-----

En sélectionnant depuis ------BEGIN jusqu'à END PGP MESSAGE----- puis en cliquant sur l'applet de chiffrement/déchiffrement, déchiffrer, entrer la phrase de passe, valider. Le presse-papier est déchiffré.
(attention aux espaces en début et fin de copier-coller ! Tous les tirets doivent être copiés. Il ne doit pas y avoir d'espace avant ou après les tirets copiés.)

Y/ Chiffrer un disque, une clé, une partition :

! Attention les données présentes sur le disque ou la partition seront perdues !
https://tails.boum.org/doc/encryption_and_privacy/encrypted_volumes/index.fr.html
Applications/ Utilitaires/ Disques. Sélectionner le disque ou la partition clic sur les engrenages/ formater. Écraser les données existantes avec des zéros (lent) / formater. Clic sur + . Dans la fenêtre de dialogue Créer une partition, pour le type choisir Chiffré, compatible avec les systèmes Linux (LUKS + Ext4), créer.

Z/ Pour aller plus loin :

ref install tails :
https://tails.boum.org
http://www.makery.info/2015/06/09/bricole-it-yourself-installer-tailsos-le-linux-anonyme-sur-cle/

Le kit de survie linux : http://www.commentcamarche.net/faq/8386-kit-de-survie-linux

virtualisation tails :
machine virtuelle : http://virt-tools.org/learning/start-install-with-virt-manager/
https://tails.boum.org/doc/advanced_topics/virtualization/virt-manager/index.fr.html
sudo apt-get install qemu virt-manager libvirt-daemon-system
Utiliser apt-get avec prudence. Ne Pas utiliser apt-get pendant des sessions à risque.
Qubes+whonix :

NB : il y a souvent au BOOT (= démarrage) une phrase éphémère précisant sur quelle(s) touche(s) appuyer pour accéder au BIOS (ou SETUP). Si non, faire une recherche sur Internet avec le modèle de l'ordinateur. Il y a aussi parfois une phrase indiquant sur quelle(s) touche(s) appuyer pour changer l'ordre de boot (souvent Echap ou F12).

Quelle touche pour bios/marque ?
http://assiste.com/BIOS.html
http://anima-ex-machina.fr/raccourci-bios-demarrage-restauration/

Pour les principales marques :

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
others...	F12, Esc

2.1/ Pour changer l'ordre de boot dans le BIOS **:** toujours avec la clé USB branchée, redémarrer l'ordinateur

2.2/ Appuyer *de suite* sur les touches nécessaires pour entrer dans le Setup du BIOS suivant la marque du bios (cf tableau).

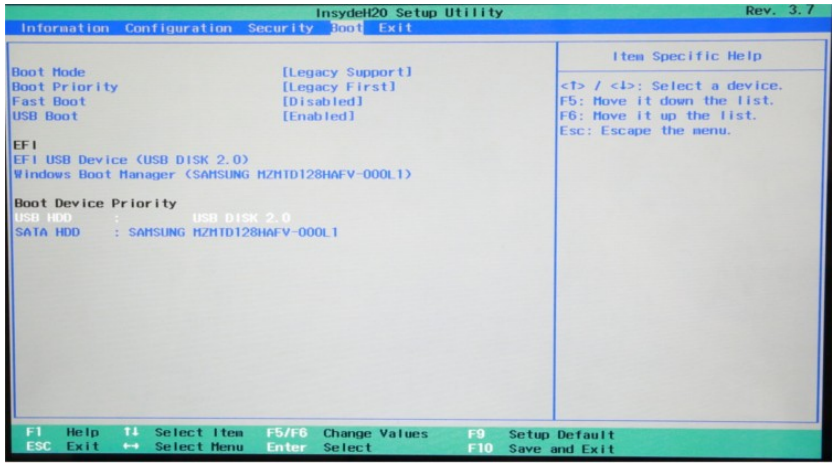
2.3/ Arrivée dans le BIOS (ou SETUP ou...).

2.4/ Rechercher dans le menu un onglet contenant « boot » ou « startup », à l'aide des flèches de direction du clavier, une ligne type « séquence de boot » « boot order », « boot priorities »....

2.5/ Remonter les lignes contenant USB en tête de liste (ligne contenant par exemple « usb disk », « Hard drive BBS priorities ») + faire entrée

NB : ces dénominations peuvent être différentes selon les ordinateurs. Souvent les touches F5 et F6 permettent de monter/descendre un périphérique dans l'ordre de boot.

Si doute pour trouver le nom de la clé : redémarrer une nouvelle fois l'ordinateur sans la clé tout en appuyant sur « échap »(ou la touche indiquée par le pc au boot), noter les noms des périphériques indiqués, éteindre, insérer la clé USB et redémarrer l'ordinateur (si besoin en appuyant sur « échap » ou la touche indiquée par le PC au boot). L'ordinateur doit repérer la clé et il est à présent possible de se positionner dessus (c'est le nouveau périphérique qui apparaît (cf première liste des périphériques) et d'accéder à Tails.

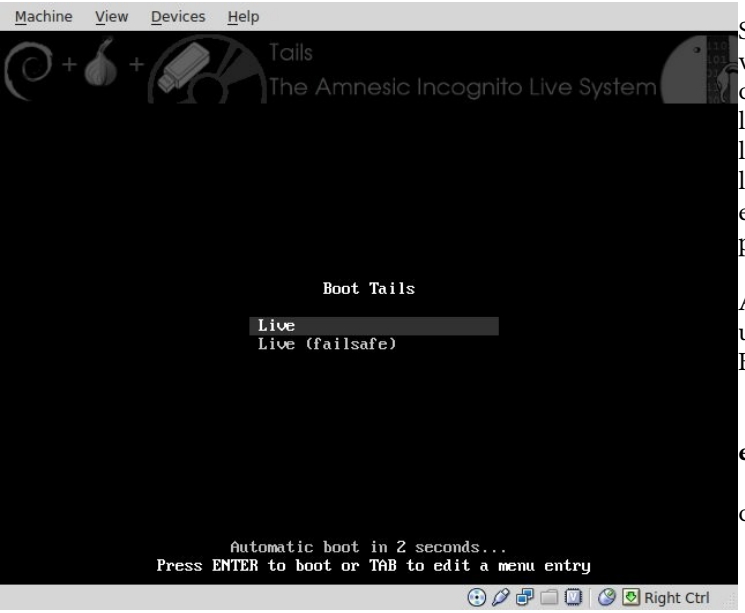


2.6/ Enregistrer et quitter (souvent F10).

NB : selon les ordinateurs, et après les modifications effectuées dans le BIOS comme précisé ci-dessus, il est possible (mais rare) que l'ordinateur ne démarre quand même pas systématiquement sur la clé USB. Dans ce cas, faire « échap » (ou la touche indiquée par le pc au boot) à chaque démarrage et lui indiquer de démarrer sur la clé.

C / «Bienvenue dans Tails » : un démarrage classique

NB : si la première partie du démarrage paraît trop longue et qu'il y a un doute sur l'activité réelle du système appuyer sur F1 permet de voir défiler les journaux relatant l'activité en cours.



Si le système TAILS passe en veille c'est la barre d'espacement qui le réveille. Pour verrouiller l'écran : touche logo (souvent le logo windows :/) +l (comme lock). Pour déverrouiller : touche espace puis entrer votre mot de passe de session.

Après avoir démarré le PC sur une clé Tails et passer l'écran Boot Tails live live (failsafe) :

1/ Sélectionner une langue en bas de page à droite

2/ Optionnel et seulement quand il y en a besoin : S'il y a un

-Dans Nautilus (le navigateur de fichiers) il est possible d'ouvrir un terminal dans le dossier en cours en cliquant droit dans la fenêtre puis « ouvrir dans un terminal »
- Pour relancer Tor : Dans un terminal taper : `sudo /etc/init.d/tor restart`

Programmer les sauvegardes automatiques dans LibreOffice

(Application, Bureautique, LibreOffice Writer, Outils, Options, Chargement/Enregistrement, général, ajuster le temps d'intervalle des sauvegardes : enregistrer les informations de récupération automatique toutes les X minutes).

V/ Utiliser un pad :

Exemple http://5jp7xtmox6jyoqd5.onion/p/Tails-facile_pour_TouTEs

➡ Comment commencer ?
Créer un nouveau pad http://5jp7xtmox6jyoqd5.onion/ choisir un nom pour le pad. Clic sur ok
• Renseigner un pseudo, en cliquant sur l'icône « utilisateur » en haut à droite.
• Choisir une couleur d'écriture au même endroit.
• écrire sur le pad !
• Les contributions de chacunEs se synchronisent « en temps réel » sous leur propre couleur.

➡ Comment partager / collaborer ?
• Sélectionner et copiez l'URL (l'adresse web dans la grande barre en haut à gauche du navigateur)
• Partager-là à vos collaborateurices
• Attention : toute personne ayant cette adresse d'accès peut modifier le pad .
• Utilisez l'onglet chat (en bas à gauche) pour séparer les discussions du texte sur lequel vous travaillez.

➡ Comment sauvegarder ?
• Il n'y a rien à faire : le texte est automatiquement sauvegardé, à chaque caractère tapé.
• Marquer une version (un état du pad) en cliquant sur l'icône « étoile ».
• Retrouver toute l'évolution du pad et les versions marquées d'une étoile dans l'historique (icône « horloge »).
• Importez et exportez le texte avec l'icône « double flèche » (formats HTML, texte brut, PDF, ODF…) ou avec un copier/coller.
Important ! N'oubliez pas de conserver quelque part l'adresse web (URL) de votre pad.

W/ Chiffrer un fichier, un dossier :

Dans Nautilus, le navigateur de fichier (Application, Accessoires, Fichiers) clic droit sur le fichier à chiffrer puis chiffrer, choisir le mode de chiffrement : soit avec une phrase de passe soit avec une clé gpg. Dans le cas d'une clé choisir la clé puis entrer le mot de passe de la clé. Valider. Un nouveau fichier est créé dans le même dossier avec le même nom plus une extension gpg.
Dans un terminal (Applications/Favoris/Terminal) taper ou copier/coller:
openssl bf -e < fichier-à-chiffrer > fichier.chiffré
ou
gpg -c < fichier-à-chiffrer> fichier.chiffré
ex : gpg -c <'Tuto_Tails-facile.pdf'> Tuto_Tails-facile.pdf.chiffré

https://tails.boum.org/blueprint/UEFI_boot_on_Mac_without_rEFInd/
Il faut appuyer sur Alt avant d'allumer l'ordinateur portable et maintenez enfoncé jusqu'à ce qu'un menu apparaisse et ensuite choisir l'entrée qui s' appelle Boot EFI (comme toutes les autres entrées) et ressemble à une clé USB.
Sinon, il faut sans doute installer rEFInd sur la machine http://www.rodsbooks.com/refind/
Dans mac : récupérez rEFInd (prenez la version "refind-bin"). Ouvrez un Terminal, puis depuis l'archive d'installation "refind", lancez e.g. "cd Downloads/refind-bin-0.7.7" puis "./install.sh". Le mot de passe est demandé.

- copiez le dossier "drivers_x64" depuis le dossier d'installation de rEFInd vers /EFI/refind avec "sudo cp -r refind/drivers_x64 /EFI/refind"
- Redémarrez. Le système TAILS doit maintenant être listé dans le menu rEFInd.

T/ Utiliser des bitcoins :

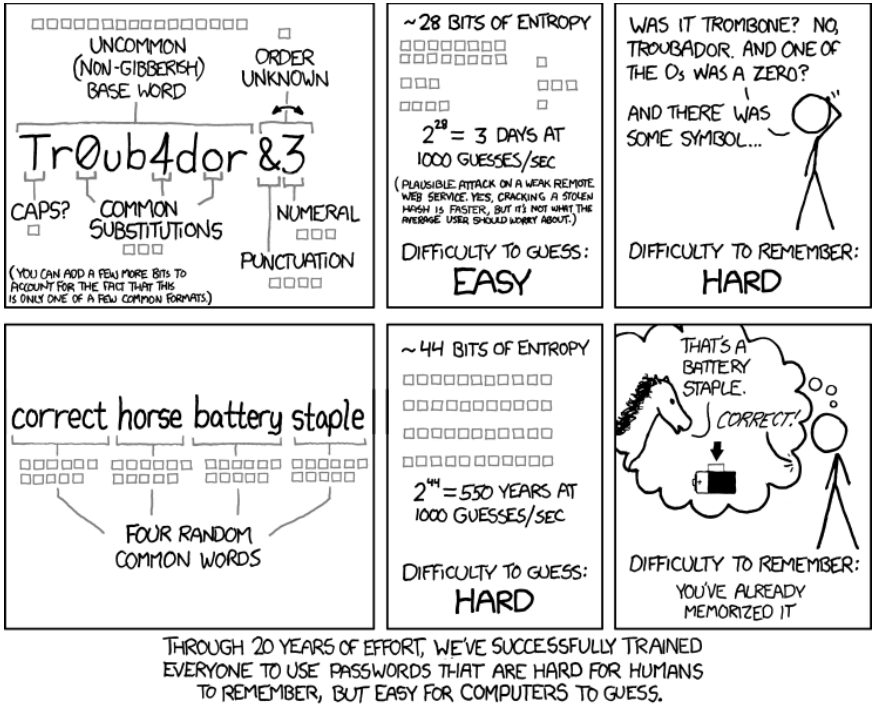
Applications / internet / electrum puis Fichier / nouveau. Entrer un nom pour ce portefeuille, create a new wallet, bien enregistrer les codes. Choisir une phrase de passe.
Pour acheter des bitcoins https://localbitcoins.com/ ou sur le darknet

U/ Commandes usuelles et astuces :

-Si pour une raison ou pour une autre l'écran se bloque, la souris ne répond plus pour exemples, faire Alt + F2 et taper r dans la fenêtre qui s'affiche puis entrée. Cela relance le serveur d'interface graphique et tout devrait s'arranger. Si le bug se reproduit utiliser Applications, Outils systèmes, WhisperBack pour faire un rapport de bug afin qu'un correctif soit trouvé.
-Si une application « plante », dans le terminal (applications, favoris, terminal) taper pkill « nom du programme » (cf I).
-Logo+l verrouille l'écran.
la touche avec le logo (windows ou mac souvent) permet d'accéder rapidement aux applications favorites et de voir toutes les fenêtres ouvertes et les différents bureaux.
-Pour lire des pages html téléchargées sur le stockage persistant,il faut les copier d'abord dans le dossier Tor Browser ou Tor Browser (persistant). Tor Browser n'a de droits de lecture et d'écriture que sur ces 2 répertoires pour des raisons de sécurité.
-Par sécurité NE PAS ouvrir de fichiers téléchargés en étant connecté en même temps.
-Pour savoir si le processeur est en 64 Bits, taper dans un terminal :
uname -r
si 64 dans les résultats c'est du 64 bits.
-Dans certains cas la carte wifi pose problème, la commande rfkill peut aider.
Taper dans un terminal :
rfkill block all
->bloque toutes les interfaces réseaux sans fil (les arguments (= »options ») de la commande rfkill peuvent être : "all", "wifi", "wlan", "bluetooth", "uwb", "ultrawide-band", "wimax", "wwan", "gps", "fm" or "nfc"
rfkill unblock wifi
->débloque les cartes wifi.
- La commande wget télécharge les url (adresse internet) dans le répertoire en cours. Dans un terminal : wget https://tails-facile.antirep.net/ téléchargera ce tuto dans le répertoire en cours .

volume persistant sur la clé « activer la persistance » : cliquer sur « OUI » et rentrer la phrase de passe de votre volume persistant (normalement dans le déroulé du tuto, il n'y a pas de persistant maintenant)

NB :phrase de passe « sécurisée » : minimum 20 caractères avec majuscules, minuscules, chiffres, caractères spéciaux... mais SANS accents (problèmes de compatibilité/bug? avec Riseup entre autre) !!phrase de passe à ne pas oublier, à ne pas communiquer. Il est conseillé de s'inspirer d'une phrase d'un livre/brochure... que l'on peut retrouver facilement là où l'on se trouve et noter sous forme codée (ex : page 5 , 2e phrase = 5,2). Penser à ssss (cf point I) pour protéger les mots de passe de l'oubli.(c'est à ce moment là, le point faible entre la chaise et le clavier ;))



3/ « plus d'option » : « OUI » ou « NON », cela dépend des travaux à exécuter. Il y a une encoche verte sur l'option sélectionnée. Le « OUI » permet l'installation (non recommandée) de logiciels et l'accès aux disques du pc et/ou externes par exemple. Par défaut et pour plus de sécurité ne pas prendre de mot de passe administrateur quand ce n'est pas nécessaire. Il y a moins de risques de faire des erreurs préjudiciables en tant qu'utilisateur simple. L'administrateur (appellé « root ») a tous les droits, y compris ceux de casser la sécurité et l'anonymat s'il est mal utilisé (pour une connexion sécurisée prendre « plus d'option » clic sur suivant. Pour une connexion Tor « simple », passer au point D).

4.a/ Apparition d'un nouvel écran. Indiquer une phrase de passe qui servira seulement pour cette session, la recopier pour confirmer.

4.b/ Pour plus de sécurité, cliquer sur "ma connexion est filtrée, censurée etc." / cliquer sur démarrer (en bas à droite).

5/ Arrivée sur le bureau Tails.

NB : si besoin de se connecter au net : après avoir activé le wifi ou le réseau (cf point F), cliquer sur « configurer » puis « oui », « next » puis copier-coller (ou recopier) dans la fenêtre qui s'ouvre, des adresses de bridges

(point d'accès permettant d'éviter, ou de rendre difficile, la censure ou le filtrage de Tor, le réseau utilisé par TAILS pour se connecter).
Ces adresses sont de différents types:
simple ou cachés. Les bridges cachés sont plus efficaces.
pour les bridges simples :

85.204.50.211:36849 A792C3143CC5E0E9F69D8E156BA7C93B5D92CB12
104.223.1.106:8443 6A6112BD94D2561E3A5DFB751B6F3833A8EDE6A3
68.45.52.117:443 3C89FB56CDEE23F0F16FDF86086866E33EAB24D8

ou

pour les bridges cachés (obfuscated)(plus sûrs dans les pays où l'usage de Tor est répréhensible) :

obfs4 194.132.208.62:64935 D400530F8ABD44175E7C833E2CBF679E7BF84A8B cert=tAeaCENFcvYDgImjDxulJjJ0oaSr8poSH5krsK+1+vm1IjXVdUlZ7gzK93GE68XFrBQhLA iat-mode=0
obfs4 158.69.204.189:5269 A4C09C00899047EB1E3F3D1DC873C3D490E00EBB cert=FOQL0Mqzq2g7qV5h9S/MJNXEPGdCrZUSplgiZMnIJk0Yok4i3oFNs7mNYuxcFTKFYwM0Aw iat-mode=0
obfs4 192.36.31.94:42612 FA166E93D6E7D89E021DA2B34ECB0914CA75BF0A cert=xOdYOq9IjPAAEtpH/dMgQs+ylePxYTirFyN5VZl+M2A+B5R00Y9FucWOrOH3BcRps/dIUA iat-mode=0

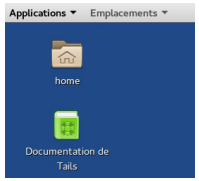
On trouve ces adresses ici: https://bridges.torproject.org/options *ou en envoyant un mail à* bridges@torproject.org
Il peut-être pratique de créer un fichier texte (Applications/Accessoires/Gedit) dans le persistant avec les adresses de bridges pour pouvoir les copier/coller. Taper les adresses de bridges, une par ligne, puis cliquer sur enregistrer, donner un nom au fichier (par exemple bridges.txt et indiquer un répertoire où enregistrer le fichier (dans le persistant!)
(les adresses données dans ce tuto sont disponibles sur un pad ici: 5jp7xtmox6jyoqd5.onion/p/bridges)

Dans la fenêtre configuration du proxy local clic sur non, puis « se connecter ».

6/ Valider.
7/ Attendre le message après avoir activé le wifi ,disant que Tor est prêt avant de démarrer Tor Browser (cf point F)

D / Créer une nouvelle clé TAILS à partir d'une clé existante et de confiance :

La solution la plus simple et sûre pour autant que les vérifications d'usage de l'image iso (= format de fichier contenant le système) ayant servi à créer la clé TAILS de confiance aient été faites.
(cf la référence : https://tails.boum.org/install/index.fr.html)



1/ Cliquer sur l'onglet « Applications » en haut à gauche. Puis « Tails » / « Programme d'installation de Tails » et ensuite cliquer sur « Install by cloning »

Créer un site ou heberger des fichiers sous TOR : http://popfilesxuru7lsr.onion/
French deep web : http://fdwocbsnity6vzwd.onion/ un forum francophone (créer un faux-profil puis s'identifier en bas de page)
Pierre par pierre (anti-répression) http://pppierreqdmdhrfm.onion/
Shell TorVPS : http://torvps7kzis5ujfz.onion/index.php/TorVPS (suivre les instructions.nom d'utilisateur de huit lettres maximum)
Freedom hosting http://fhostingesps6bly.onion/
Wordpress sous tor :http://torvps7kzis5ujfz.onion/index.php/WordPres
Cacher ses données : stéganographie http://data44v2jfxk46ma.onion/data.php?url=Planquez-vos-donn%C3%A9es-avec-toplip---st%C3%A9ganographie
Les services cachés Riseup :

riseup.net : nzh3fv6jc6jskki3.onion (port 80)
help.riseup.net : nzh3fv6jc6jskki3.onion (port 80)
imap.riseup.net : zsolxunfmbfuq7wf.onion (port 993)
lists.riseup.net : xpgylzydxykgdqyg.onion (port 80)
mail.riseup.net : zsolxunfmbfuq7wf.onion (ports 80, 465, 587)
pad.riseup.net : 5jp7xtmox6jyoqd5.onion (port 80), document collaboratif en ligne avec chat pour permettre de travailler à plusieurs sur un texte, en temps réel, à distance dans le temps et l'espace.
Exemple : http://5jp7xtmox6jyoqd5.onion/p/Tails-facile_pour_TouTEs
pop.riseup.net : zsolxunfmbfuq7wf.onion (port 995)

#Pour changer dans Icedove :

Applications/Favoris/Icedove
Sélectionner le compte mail à gauche puis à droite « voir les paramètres pour ce compte ». Dans «paramètres serveur » remplacer « pop.riseup.net » par « zsolxunfmbfuq7wf.onion » et en profiter pour changer quelques paramètres (cf image page suivante)
share.riseup.net : 6zc6sejeho3fwrd4.onion (port 80), partage de fichiers (toujours chiffrer les fichiers partagés)
smtp.riseup.net : zsolxunfmbfuq7wf.onion (ports 465, 587)
user.riseup.net : j6uhdvbhz74oefxf.onion (port 80) pour gérer le compte riseup.
we.riseup.net : 7lvd7fa5yfbdqaii.onion (port 443) Crabgrass des outils pour l'organisation des collectifs.
xmpp.riseup.net : 4cjw6cwpeaeppfqz.onion (ports 5222, 5269) compte de discussion instantanée (à utiliser avec Pidgin)
0xacab.org : vivmyccb3jdb7yij.onion (port 80) hébergement de code source logiciel.
black.riseup.net : cwoiopiifrlzcuos.onion (port 80)

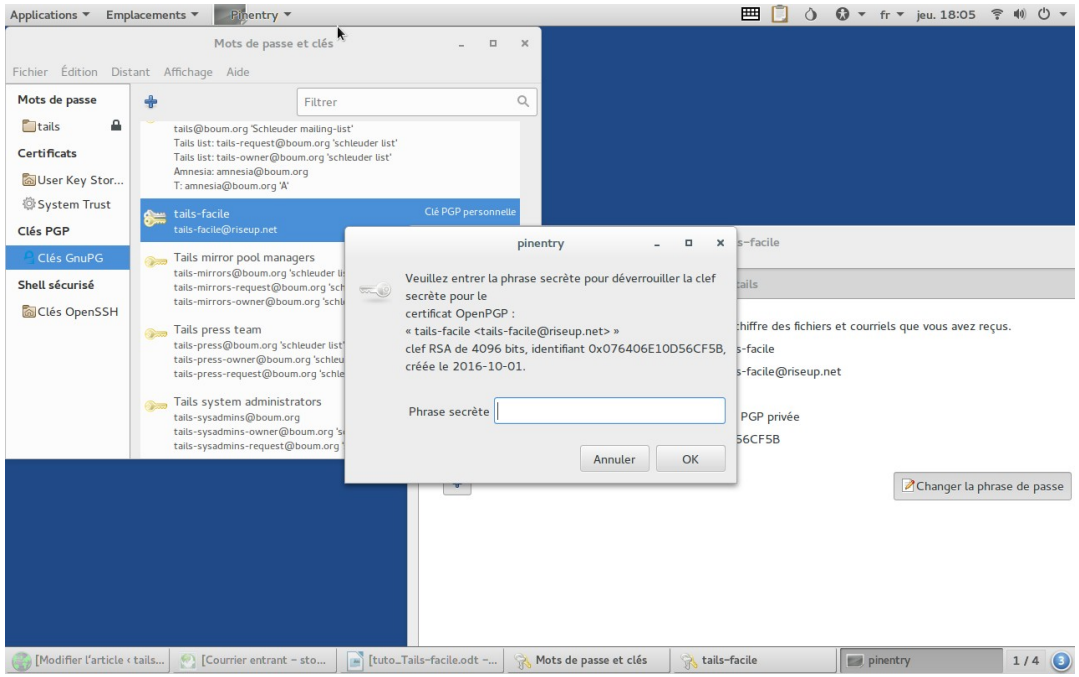
Sur le clearweb :
Services militant mutualisé : https://www.autistici.org/en/index.html
Génératrice de fausse identité : http://www.fakenamegenerator.com/gen-female-fr-fr.php
Courriel jetable : http://www.yopmail.com
recevoir des sms : https://www.freeonlinephone.org/#number

S/ TAILS et Mac :

rEFInd et boot mac :

P/ Changer la phrase de passe du trousseau de clés GPG :

Application/Utilitaires/mot de passe et clés/GnuPG puis clic droit sur la clé/propriétés/changer la phrase de passe.



Q/ Révoquer une clé :

Application/Utilitaires/mot de passe et clés/GnuPG puis clic droit sur la clé/propriétés/onglet détails/révoquer.

R/ Les outils du deep-web/darknet :

TRIGGER WARNING : le deep web recèle tout ce qui est illégal y compris le Child Porn CP (pédopornographie), les snuffs movies (exécutions, viol ou meurtres filmés), les films « gores », le racisme, nazisme, etc.)
‼ Ne faites confiance à personne sur les markets du deepweb ‼

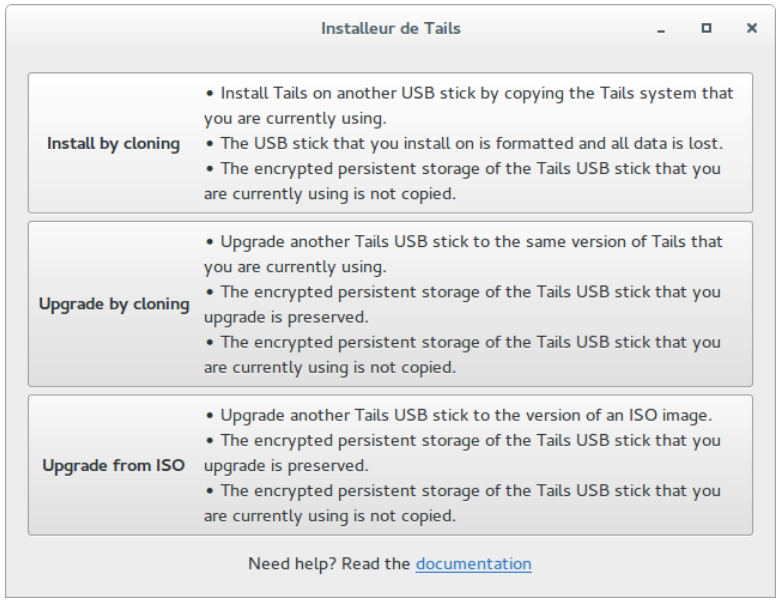
Débuter sur le deep-web : http://paste5e3na6bar5p.onion/0Z7RV9O1
Zerobin : http://zerobinqmdqd236y.onion/ pour envoyer des messages chiffrés éphémères et auto-destructibles.
Hidden wiki :http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page pour trouver des adresses de sites
Tor hidden wiki http://paste5e3na6bar5p.onion/0Z7RV9O1
Mail sous tor: http://sigaintevyh2rzvw.onion/mail/
Partage d'images :http://md4nx3btlhc525sk.onion/

2/ Ouverture d'une nouvelle fenêtre « Installateur de Tails, Target device »

3/ Insérer la nouvelle clé (votre clé apparaît dans Target device). Cliquer sur « Install Tails » en bas de la fenêtre.

4/ Confirmer la sélection du périphérique en cliquant sur « OUI ». Attendre le message : l'installation est terminée. Cela prend quelques minutes. Cliquer sur fermer

5/ Enlever la 1ère clé (celle qui a servi à la création). TAILS s'éteint.



Pas de panique c'est une fonction de sécurité de TAILS qui s'arrête et vide la mémoire vive (RAM) dès qu'on enlève la clé. Ce qui veut aussi dire que s'il y a un choc sur la clé qui provoque une micro-coupure pendant que TAILS tourne il peut s'arrêter en pensant 1 milliseconde que la clé a été enlevée : surveiller et protéger la clé TAILS quand elle est en action ‼
puis redémarrer avec seulement la nouvelle clé (si besoin en appuyant sur « échap » ou la touche indiquée par le pc au boot).

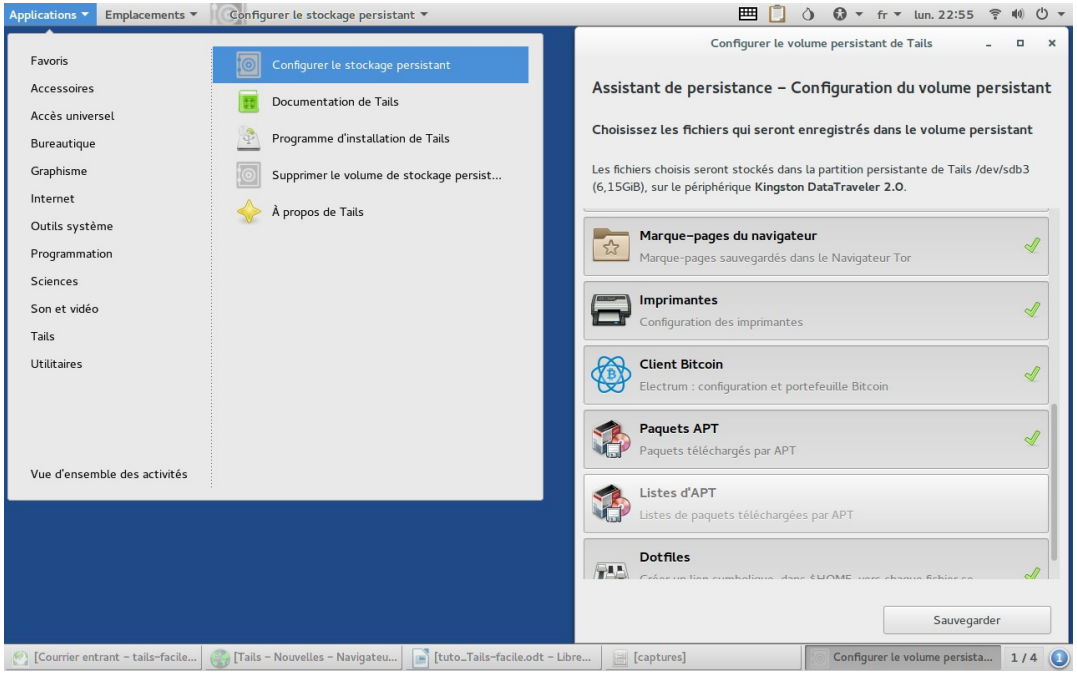
E / Créer le stockage persistant de la nouvelle clé TAILS :

Le stockage persistant permet de conserver ses documents mais aussi ses configurations (phrases de passe, trousseaux de clés, identifiants, logiciels installés, signets, préférences, etc...) .C'est pratique mais cela peut aussi être une faille de sécurité. Penser à faire des sauvegardes régulières du persistant.
Après avoir redémarré la nouvelle clé TAILS dans votre langue sans options :

1/ Cliquer sur les menus « Application » / « Tails » / « configurer le stockage persistant »
2/ Créer sa phrase de passe* persistant sécurisée. Clic sur création. Apparition d'une nouvelle fenêtre

NB : phrase de passe du persistant « sécurisée » : minimum 20 caractères avec majuscules, minuscules, chiffres, caractères spéciaux… (mais SANS accents problèmes de compatibilité/bug? avec Riseup entre autre) !! Phrase de passe à ne pas oublier, à ne pas communiquer. Il est conseillé de s'inspirer d'une phrase d'un livre/brochure... que l'on peut retrouver facilement là où l'on se trouve et noter sous forme codée (ex : page 5 , 2e phrase = 5,2). Il est possible de prendre la phrase à l'envers, ou un mot/lettre sur 2 ou 3, ou changer des lettres ou quoi que ce soit.En gardant en mémoire qu'il est

impératif de retrouver cette phrase de passe à l'exact identique !! Une bonne méthode pour s'assurer de bien taper la phrase de passe peut être d'ouvrir un éditeur de texte (application/accessoires/gedit), de taper la phrase de passe dedans et de la copier coller ensuite dans les champs mot de passe.



3/ Configuration du stockage/volume persistant :

4/ « Assistant de persistance » / « configuration du volume »

5/ Cocher toutes les lignes (**bien descendre en bas de page** en utilisant la barre de défilement sur la droite)

6/ Sauvegarder et fermer

7/ Redémarrer (flèche en haut à droite de l'écran puis clic sur le bouton avec la flèche qui s'enroule) avec cette clé toujours branchée. (voir point C)

NB : Si problèmes avec la phrase de passe : bien vérifier que le clavier est bien en français (ou autre mais le même que lors de la création de la phrase de passe).

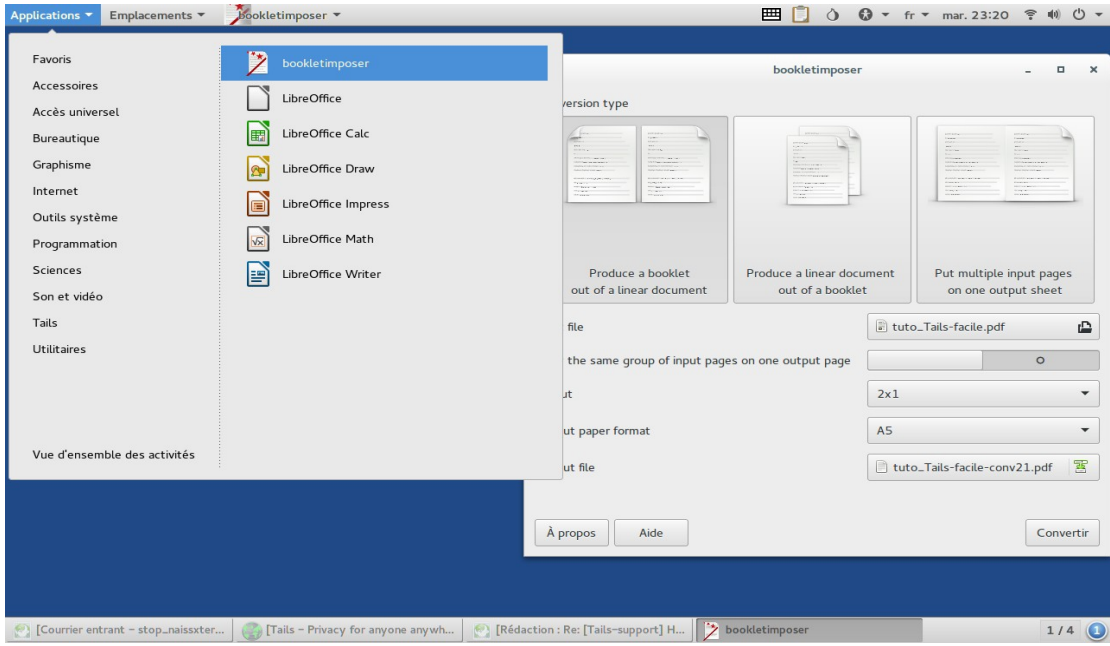
Le volume persistant est une partition chiffrée et peut donc être ouvert à partir de n'importe quel système d'exploitation (avec la phrase de passe bien sur). Avec Tails pour ouvrir un volume de stockage persistant sur une autre clé, ou sur une clé dont le persistant n'a pas été activé au démarrage: Applications/Utilitaires/Disques dans la partie gauche cliquer sur la clé contenant le volume de stockage persistant à ouvrir (si le volume chiffré est sur une autre clé, enlever et remettre la clé permet de s'assurer que l'on sélectionne la bonne clé avant de cliquer) puis dans la partie de droite clic sur la partition avec le petit cadenas. Taper le mot de passe, valider, une nouvelle partition apparaît. Cliquer dessus puis sur la petite flèche à coté des engrenages. Le volume persistant se trouve par Emplacements/TailsData.

pdfShuffler%202.3.3/pdfbooklet_2.3.3-2_all.deb/download

Pour installer taper dans un terminal :

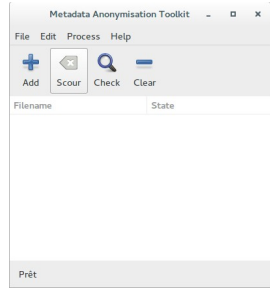
sudo dpkg -i '/home/amnesia/Persistent/pdfbooklet_2.3.3-2_all.deb'

Pour utiliser taper dans un terminal :pdfbooklet



N/ Enlever les métadonnées de certains fichiers (image, son) :

MAT (Metadata Anonimisation Toolkit)



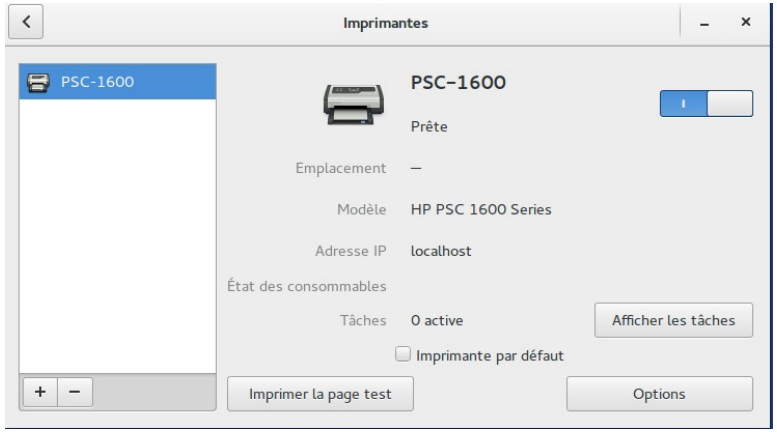
Les métadonnées peuvent identifier le matériel (appareils photo, cameras, imprimantes, etc...), géolocaliser un événement ou permettre de le situer dans le temps.
Applications/outils système/MAT
glisser/déposer les fichiers à nettoyer dans MAT
scour pour nettoyer (les fichiers ne changent pas de noms ni de dossier)

O/ Changer le mot de passe du persistant :

Application/Utilitaires/disques sélectionner la clé TAILS dans le cadre de gauche. Dans le cadre à droite sélectionner la partition Tailsdata avec le verrou, clic sur les engrenages, modifier la phrase de passe, taper le mot de passe actuel, puis 2 fois le nouveau. Clic sur modifier.

- n indique le nombre de codes de partage total.
Dans un terminal :
echo "My Secret ABCD" | ssss-split -t 3 -n 6
ou :
ssss-split -t 3 -n 6 (le terminal demande le secret et renvoie n codes de partages du secret)
Le secret réparti en pratique
https://linuxfr.org/users/gouttegd/journaux/gfsecret-le-secret-reparti-en-pratique

L/ Installer une imprimante :



Flèche coin droit / paramètres / imprimante / installer une nouvelle imprimante puis cliquer sur l'imprimante.

M/ Créer une brochure :

Avec Bookletimposer à partir d'un pdf : la solution la plus simple
Applications/Bureautique/bookletimposer
Avec html2pdf à partir d'une page html (avec un mot de passe administrateur) :
-Pour installer wkhtmltopdf, dans un terminal taper :
sudo apt-get update && sudo apt-get install wkhtmltopdf
(rentrer la phrase de passe définie pour cette session. Par sécurité rien ne s'affiche quand on tape les mots de passe. Ne pas utiliser apt-get pendant des sessions à risque.)
sudo ln -s /usr/bin/wkhtmltopdf /usr/local/bin/html2pdf
html2pdf « url de la page »
l'url est l'adresse de la page (que l'on copie dans la barre d'adresse du navigateur web, du navigateur de fichiers locaux, ou d'un lien dans une page web, puis qu'on colle dans le terminal après la commande html2pdf)

A partir d'un pdf :
taper (ou copier/coller) dans un terminal pour télécharger le logiciel:
cd ~/Persistent/ && sudo wget https://sourceforge.net/projects/pdfbooklet/files/pdfBooklet-

Récuperation de persistant :

`Il arrive que lors d'un démarrage le volume persistant ait disparu. Dans ce cas refaire la procédure de création de volume persistant et redémarrer. Le volume persistant et toutes ses données apparaissent de nouveau.`

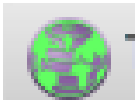
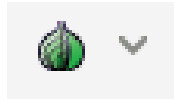
Utilisation du gestionnaire de mots de passe keepassX :

Créer un conteneur/porte-clé de phrases de passe (une base de donnée gérée par keepassX contenant les phrases de passe) :
Applications/Favoris/KeepassX puis fichier, nouvelle base de données, entrer une phrase de passe (et pour renforcer la sécurité il est possible de générer un fichier servant de complément à la phrase de passe), confirmer la phrase de passe puis entrée, Ajouter une nouvelle entée. Le bouton tools en bas à gauche permet d'automatiser le remplissage des phrases de passe .
https://tails.boum.org/doc/encryption_and_privacy/manage_passwords/index.fr.html
Il existe une version keepassX 2

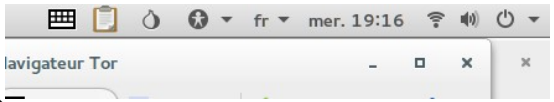
F / Se connecter à Tor & créer un compte et une adresse email RISEUP :

1/ Connexion à Tor :

Pour info : le navigateur Tor "Tor browser" est symbolisé par une planète. Tor est symbolisé par un oignon.

1.1.a/ Pour se connecter à un point d'accès Internet en wifi :
-Cliquer sur la petite flèche en haut tout à droite de l'écran.



- Cliquer sur « wifi »/« sélectionner un réseau »
- Choisir le réseau wifi auquel on veut se connecter et cliquer sur « se connecter » puis indiquer le code wifi, clic sur « se connecter ». - Attendre que le message « Tor est prêt » apparaisse au centre bas de page. La connexion est établie. (retour au NB du point C 4b pour connexion Tor par bridges).

1.1.b/ Pour se connecter en filaire (ethernet):
- Brancher le câble, la connexion se fait automatiquement. Attendre que le message « Tor est prêt » apparaisse au centre en bas de page. C'est une méthode plus sûre que le WIFI. La connexion est établie. (retour au NB du point C 4b pour connexion Tor par bridges).

NB : pour accéder aux messages du système (faute de n'avoir pas eu le temps de les lire par exemple), cliquer sur le petit rond bleu en bas à droite de l'écran avec un nombre dedans, puis sur l'ampoule.

1.2/ Lancer le navigateur Tor (Applications/Favoris/ Navigateur Tor)

1.3/ Apparaît une fenêtre, cliquer sur le gros bouton vert dans la fenêtre « vérification de Tor » : « OK » (si le bouton de vérification Tor n'apparaît pas, aller sur

l'adresse :« https://check.torproject.org »)

1.4/ Test identité IP : se souvenir/noter l'adresse IP affichée, cliquer sur la flèche à droite de l'oignon en haut à gauche de l'écran, cliquer sur « nouvelle identité » : l'adresse IP a changé = TOR fonctionne !

1.5/ Régler Tor sur le max de sécurité : cliquer sur la flèche à coté de l'oignon vert puis "paramètres de confidentialité et de sécurité" mettre le curseur sur haut./OK

NB : si Tor rame, changer d'identité (cf point F 1.4 ci dessus) et relancer. Certaines connexions Tor peuvent être foireuses. Parfois sur certains pc, éteindre le réseau (flèche à droite en haut de l'écran, wifi (ou filaire),éteindre et le rallumer (flèche, mode avion, éteindre) améliore les choses.

2/ Riseup :

Riseup est un service militant mutualisé. Merci de participer aux frais (~1€ par compte mail/service) il en va de la pérennité de cette structure très utilisée. La disparition de Riseup entraînerait de grosses pertes de données pour les milieux militants et désorganiserait nombre de réseaux de communication. Merci de respecter le contrat social de Riseup. (même remarque pour TAILS et Tor).

NB : en haut à droite, changer la langue.

Pour créer un compte Riseup, il faut se procurer 2 codes provenant de 2 adresses Riseup différentes. Demander à des contacts de confiance de faire la manip 2.1 suivante :

2.1/ Récupération de codes :

2.1.1/ Taper « https://user.riseup.net » (sans les guillemets) dans la barre d'adresse + entrée.

2.1.2/ S'identifier (nom d'utilisateur email Riseup et phrase de passe Riseup).

2.1.3/ Arrivée sur la page d'accueil, dans le menu de gauche, cliquer sur « invites»

2.1.4/ Cliquer sur « créer un code d'invitation ».

2.1.5/ Le code apparaît dans la colonne" code". Il est valable 1 mois. Noter ce code. Il est aussi possible de générer d'autres codes.

2.2/ Création du compte et du mail Riseup :

2.2.1/ Taper « https://user.riseup.net » dans la barre d'adresse + entrée.

2.2.2/ Cliquer sur « request a new account », cliquer sur « suivant » puis encore sur « suivant ».

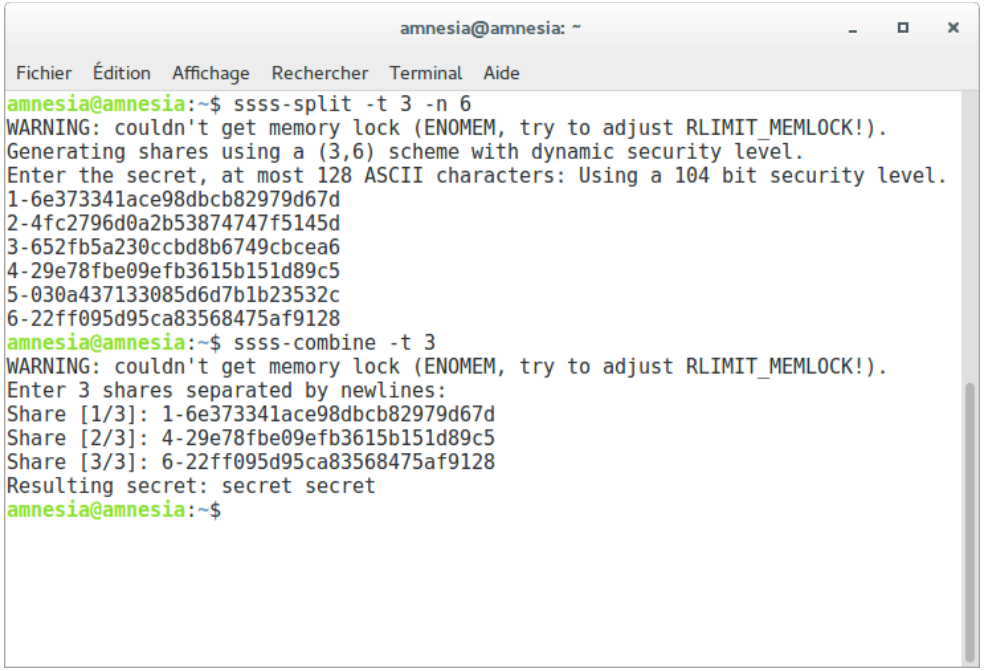
2.2.3/ Choisir un nom d'ultilisateurice. (rien qui puisse être relié à une vraie identité !!)

NB : Dans le paragraphe « Adresse de courriel de rechange », ne rien mettre sauf une autre adresse Riseup ***de confiance****, et seulement en cas de nécessité.*

2.2.4/ Choisir une phrase de passe. La ressaisir et cliquer sur « suivant ».

NB :phrase de passe « sécurisée » : minimum 20 caractères avec majuscules, minuscules, chiffres, caractères spéciaux… mais SANS accents (problèmes de compatibilité/bug? avec Riseup entre autre) !!phrase de passe à ne pas oublier, à ne pas communiquer. Il est conseillé de s'inspirer d'une phrase d'un

Tuer/forcer l'arrêt d'un programme : ouvrir un terminal Application/Favoris/Terminal et taper pkill <nom du programme à tuer> +entrée



ex : pkill icedove

Le partage de secret : Arrivé à ce stade nous sommes en possession de clefs de chiffrage que l'on peut vouloir garder « à diffusion restreinte » par exemple. Mais comment transmettre ma clé publique (ou autre chose : une phrase de passe importante, un numéro de carte ou une adresse de bridge caché, un lieu et une heure de rendez-vous) à unE correspondante sur un autre continent sans être en possession de sa clé publique…?

Dans ce cas ssss est très utile pour pouvoir disséminer des partages d'un secret (pour pouvoir le retrouver par exemple ou le partager) sans partager le secret lui-même.

Avec ssss, en choisissant le nombre de partages nécessaires pour reconstituer le secret, (maximum 128 caractères), on peut fixer des niveaux de confiance (par exemple).

S'il est question de partager un secret placé dans un dossier chiffré à n'ouvrir que si certaines conditions sont réunies ; dans cet exemple on créera avec ssss x partages de la phase de passe du dossier chiffré disons 6 avec la condition qu'il y ait, par exemple, 3 partages pour retrouver le passe. Il n'y a plus qu'à transmettre ces partages à lae correspondantE en utilisant plusieurs méthodes (mail, sms, téléphone, courrier postal, zerobin etc…(il est encore possible de donner plusieurs partages selon le degré de confiance).

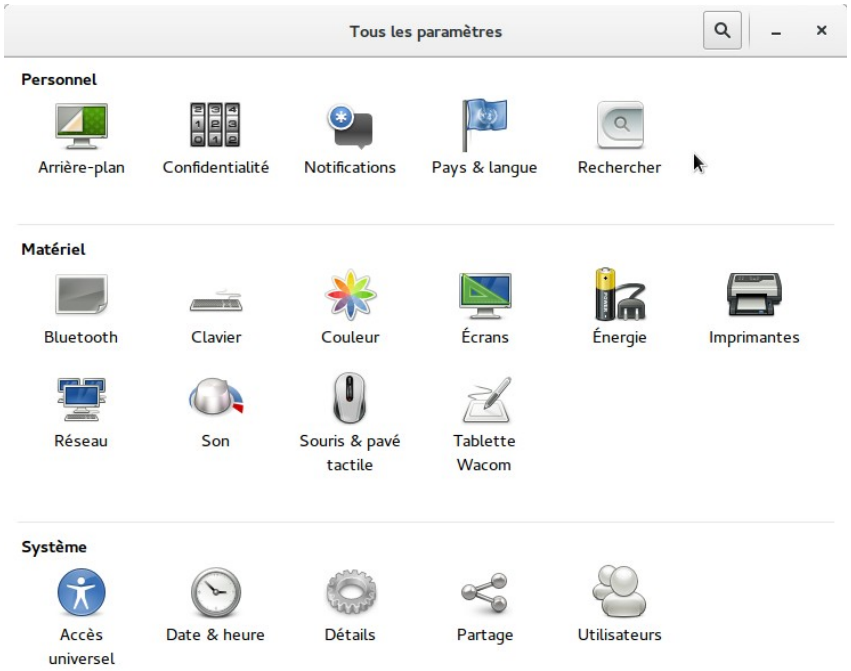
Utiliser ssss :

http://point-at-infinity.org/ssss/

http://linux.die.net/man/1/ssss-split

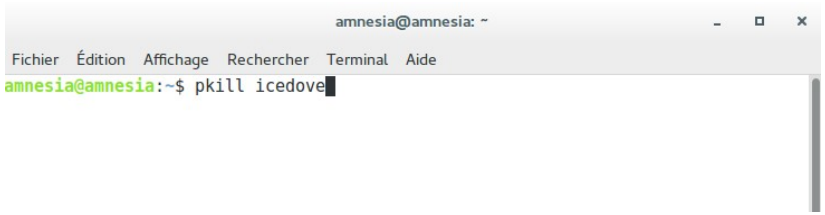
exemple :

- t indique le nombre de codes de partage nécessaires pour retrouver le secret.



J/ Changer la phrase de passe du persistant :

‼ Avant de toucher au persistant, en faire une sauvegarde ‼ Application/Utilitaires/disques. Sélectionner la clé usb puis la partition TailsData Luks, clic sur les 2 engrenages, modifier la phrase de passe, taper la phrase de passe actuelle et 2 fois la nouvelle, clic sur modifier.



K/ Bonus plus :

livre/brochure... que l'on peut retrouver facilement là où l'on se trouve et noter les références sous forme codée (ex : page 5 , 2e phrase = 5,2); et d'utiliser ssss (cf point I).

2.2.5/ Mettre le 1er code invité, puis le 2e

2.2.6/ S'il y a un cadre « Parlez nous un peu de vous » (il est conseillé de juste copier/coller du texte genre « je n'ai rien à déclarer ! ». Aucune informations personnelles). Cliquer sur « valider ». La création du compte et de l'adresse mail Riseup est faite.

G / Configurer la messagerie Icedove & créer un trousseau de clés GPG (clés de chiffrage) :

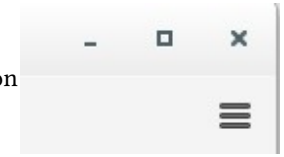
1/ Configurer la messagerie Icedove :

1.1/ Lancer Icedove (icône timbre vert) : applications/favoris/Icedove.

1.2/ Inscrire son pseudo, indiquer son adresse mail Riseup (ex : exemple@riseup.net), sa phrase de passe sécurisée du compte Riseup, valider et terminer. Il est conseillé de configurer Icedove pour utiliser les services cachés Riseup (cf point Q)

2/ Créer un trousseau de clés de chiffrage :

NB : Tails a besoin d'événements aléatoires pour générer une clé aléatoire forte. L'entropie se crée en utilisant le système. N'hésitez donc pas à taper du texte, regarder un film, écouter de la musique ou faire du montage vidéo avant et pendant la création de la clé.



2.2/ Dans la fenêtre « Accueil-Icedove », cliquer sur le bouton en haut à droite avec les trois barres horizontales qui indique, lorsque l'on passe la souris dessus, « afficher le menu de Icedove »

2.3/ Cliquer sur « Enigmail » / « assistant de configuration » / sélectionner la ligne « I prefer an extended configuration » / « suivant »

2.4/ Cliquer sur « je veux créer une nouvelle paire de clés pour signer et chiffrer des messages » / « suivant »

2.5/ Rentrer la phrase de passe sécurisée et la retaper (prohiber les diacritiques, c'est à dire les accents, les trémas , les tildés~,¤£$µ ...), c'est sa longueur qui fait la force de la phrase de passe ,/ « suivant »

2.6/ A la fin du processus de génération, l'indication « your key is generated » apparaît / cliquer sur « create revocation certificate » / retaper la phrase secrète /,« OK » / enregistrer dans le persistant / « enregistrer » / « terminer » / « OK ».

! Attention de ne pas perdre le certificat de révocation, ni les clés... Le certificat de révocation servira dans le cas où la clé privée est corrompue, perdue, volée... Stocker le certificat de révocation sur un support sûr et différent de celui de la clé privée . Différents stratégies existent concernant la gestion des clés (durée de validité,signature, publication) !

2.7/ « suivant » / « terminer ».

3/ Publier la clé publique sur un serveur de clés (pour que vos correspondantEs puissent

directement trouver votre clé publique pour vous envoyer des mails chiffrés) :
NB : Il est aussi possible de choisir de ne pas divulguer sa clé publique sauf à quelques correspondantEs pour augmenter le niveau de sécurité et de confiance (dans ce cas passer au point 4).

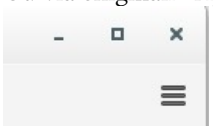
3.1/ Dans le menu de Icedove (en haut de la fenêtre à droite le bouton avec les 3 traits horizontaux), sélectionner "enigmail" puis "gestion de clés"

3.2.a/ Dans la fenêtre qui apparaît, sélectionner votre clé puis clic droit "envoyer les clés publiques vers un serveur de clés" + validez

3.2.b/ Pour exporter la clé publique vers un fichier: même manipulation sauf "exporter les clés vers un fichier" "exporter uniquement les clés publiques" enregistrer la clé dans le persistant.

Où sont mes clés GPG ? Cliquer sur application/utilitaires/mots de passe et clés/clé GnuPG.
Ou sur puis « gérer les clés »

Ou via enigmail : Application /Favoris/ Icedove / menu icedove / Enigmail / gestion de clefs



4/ Paramétrer Icedove pour qu'il utilise le chiffrage :

4.1/ Ouvrir Icedove, Application /Favoris/ Icedove / « voir les paramètres pour ce compte » / sur la partie de gauche, cliquer sur « Sécurité open PGP » / sur la partie de droite, cliquer sur «choisir une clé » / sélectionner la clé qui apparaît / cocher « chiffrer les messages par défaut » et « signer les messages par défaut »

4.2/ Dans la partie de gauche, cliquer sur « accusé de réception » / sur la partie de droite, cliquer sur « préférences globales » / cocher « lors de l'envoie d'un message, toujours demander l'accuser de réception » / « OK » / « fermer ». (c'est nécessaire pour pouvoir savoir si un message important est arrivé dans la boite du/de la destinataire sauf si ielle refuse d'envoyer l'accusé de réception)

4.3/ Cliquer sur « OK ».

H/ Envoyer un mail chiffré :

1/ Sur la page d'accueil de votre adresse mail dans Icedove, Application /Favoris/ Icedove , cliquer sur « écrire un nouveau message » / dans la fenêtre rédaction, cliquer sur « attacher ma clé publique »

2/ Entrer votre destinataire, le sujet/objet, écrire son mail

*NB : le sujet/objet et les pièces jointes **NE sont PAS chiffré.e.s.** Ne pas mettre d'info dans l'objet. chiffrer les pièces jointes AVANT de les joindre/envoyer.*
Toujours envoyer les fichiers chiffrés avec leurs hachage :

3 / Cliquer sur « envoyer ».

4/ Si apparaît une fenêtre précisant que le destinataire est invalide, alors cliquer sur le bouton « télécharger les clés manquantes » / « OK » / si la clé du destinataire a été publié sur le serveur de clés, elle apparaît (vérifier que c'est la bonne adresse mail), la cocher et cliquer sur « OK »

/ « OK ». Si la clé de la personne destinatrice du message n'apparaît pas alors il n'est pas possible de chiffrer le mail. Dans ce cas décocher l'option « chiffrer le mail » pour demander par mail à la personne sa clé publique puis importer celle-ci en faisant un double clic droit sur le fichier... (pour les échanges de secrets cf ssss, point I).

5/ Recevoir et déchiffrer un mail :

5.1/ Sur la page d'accueil de votre adresse mail dans Icedove (Application /Favoris/ Icedove) cliquez sur "Relever"

5.2/ Cliquer sur le mail reçu

5.3/ Taper la phrase de passe du trousseau de clés de chiffrage + entrée.

Générer ou vérifier les sommes de contrôles (hash) avec gtkhash :

Applications/Accessoires/Gtkhash puis cliquer sur le bouton (aucun) situé après « fichier », sélectionner le fichier à hacher puis cliquer sur le bouton hacher. Ensuite clic sur fichier/enregistrer sous, donner un nom au fichier et choisir un emplacement où l'enregistrer). Clic sur le bouton enregistrer. Fermer Gtkhash en cliquant sur le bouton avec la petite croix en haut à droite de la fenêtre.
Ou clic droit sur le fichier chiffré puis propriétés puis résumé et enfin hachage. Copier chaque hachage et les coller avec leurs référence (MD5, SHA1,SHA256...) dans un fichier texte. chiffrer et signer ce fichier texte et le joindre au fichier principal chiffré.

I/ Désactiver le micro :

En haut à droite de l'écran, cliquer sur la flèche puis sur le symbole paramètres (une clé et un tournevis croisés) puis sur « son » puis onglet « entrée »mettre l'interrupteur sur 0.