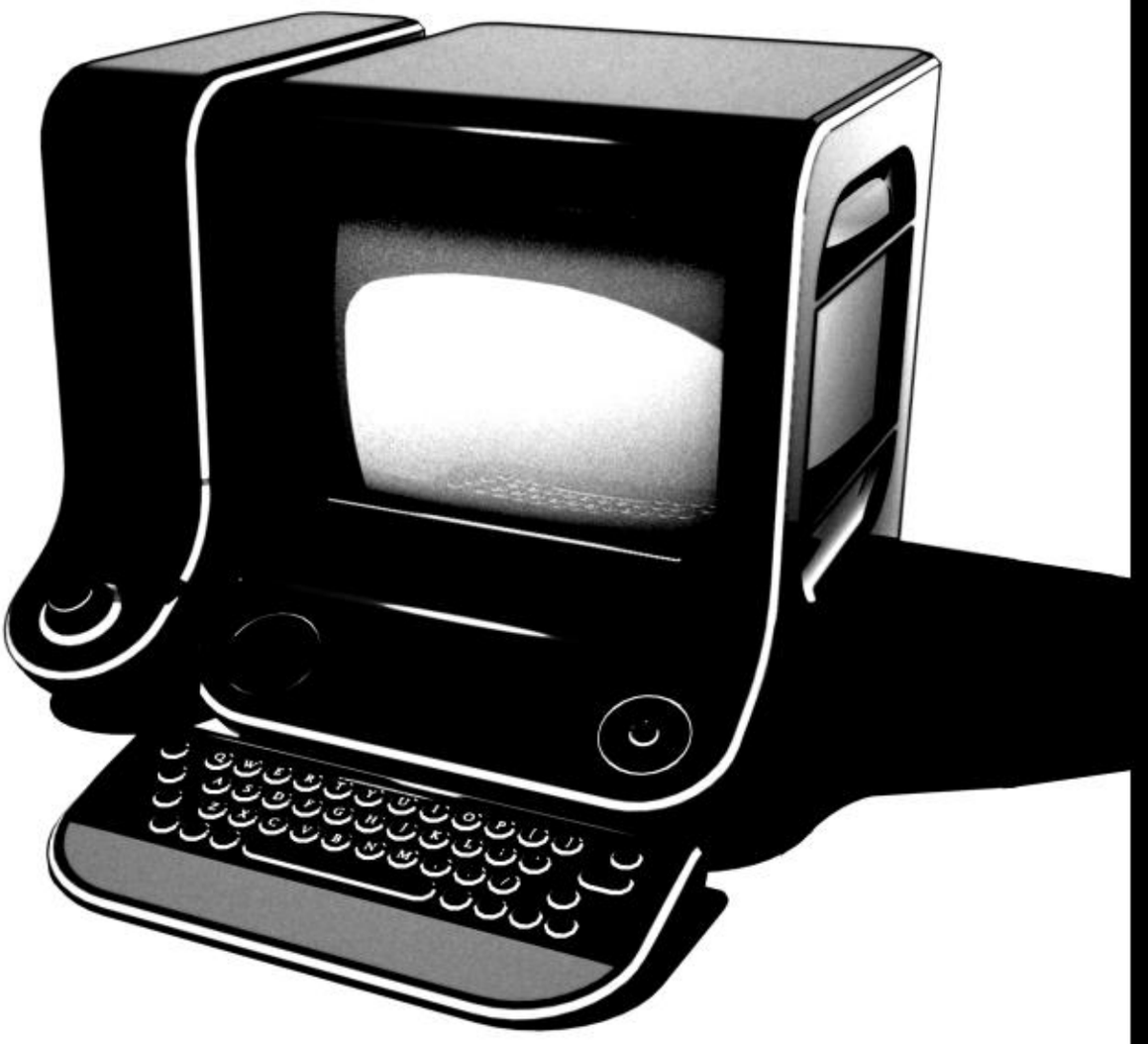
L'INFORMATIQUE
SE DÉFENDRE ET ATTAQUER



VERSION 3.0

L'INFORMATIQUE
SE DÉFENDRE ET ATTAQUER

VERSION 3.0

Juin 2015

ISBN 978-3-033-05128-7

Table des matières

1 Introduction: comprendre pour mieux se défendre et... attaquer

Ce livre a été écrit par désir de rassembler les connaissances théoriques et les outils pratiques actuellement les plus efficaces à nos yeux, pour utiliser l'informatique pour des activités sensibles, sans se faire avoir. Voir: 16.3
Concrètement, ça implique d'être en mesure d'agir de manière anonyme, confidentielle et en laissant le moins de traces possible derrière nous. Sans ces précautions, inutile d'espérer déjouer longtemps la surveillance et la répression employées par les États et leurs classes dirigeantes pour continuer à exercer tranquillement leur domination.

C'est dans cette optique, que ce texte se concentre sur un système d'exploitation précis: Tails. On va y puiser, au fil des chapitres, différents outils Voir: 3.1
partageant tous la même finalité: mettre des bâtons dans les roues de la surveillance informatique.
On ne va donc pas parler ici de tous les degrés possibles de précaution, ni de ce qui est partiellement possible de faire sous d'autres systèmes plus courants comme Windows, Mac ou Ubuntu, qui ont souvent autre chose en tête que nous aider à nous protéger des keufs. Ce n'est pas par manque de place, mais plutôt parce que faire les choses à moitié donne souvent une illusion de sécurité, qui peut avoir des conséquences plus que craignos.
Se réapproprier les outils informatiques, c'est comprendre pour mieux se défendre et... attaquer[1], mais c'est aussi se donner les moyens de pouvoir choisir en connaissance de cause, quand ne pas utiliser l'informatique.

Le texte est construit autour de chapitres théoriques, servant de base pour comprendre les problèmes soulevés par les traces informatiques qu'on laisse un peu partout, et auxquels répondent des chapitres pratiques proposant et discutant des outils informatiques sortis tout droit de Tails.
D'autre part, les différentes parties du texte se renvoient régulièrement la balle et regorgent de plein de références externes intéressantes, plus ou moins bien citées et dont certaines ne sont disponibles qu'en anglais.

De plus, comme en informatique les choses changent rapidement, il est plus que probable qu'au fil du temps, des éléments du texte ne soient plus à jour. Les informations manquantes seront alors à trouver en ligne, dans la docu-

[1] Une première note, le terme «attaquer» n'est pas utilisé ici dans le sens d'attaquer, hacker d'autres systèmes informatiques (désolé, si ça te déçoit). Ce mot a été employé pour appuyer notre envie de concevoir l'informatique aussi comme un outil offensif, de s'ouvrir les portes de l'illégalisme, et de ne pas se laisser enfermer dans une vision assez répandue de braves citoyen-ne-s traqué-e-s par Big Brother.

mentation officielle de Tails, qui est mise à jour très régulièrement, ainsi que dans les versions futures de ce texte et dans la véritable mine d'infos qu'est Internet. Voici donc, quelques sources de référence que l'on recommande à la lecture:

- La documentation officielle de Tails:
  [https://tails.boum.org/doc/index.fr.html]
- Le guide d'autodéfense numérique:
  [https://guide.boum.org]
- Infokiosques.net qui publie les dernières versions de ce texte:
  [https://infokiosques.net/]

Finalement, le but du format brochure et du mode de diffusion[2] qui va avec, c'est aussi de rendre plus accessibles ces savoirs techniques qui, comme l'a fait remarquer une copine, sont détenus dans les mains de quelques spécialistes, presque exclusivement des mecs cis-genres. À ça, il faut ajouter que la plupart du temps ce sont aussi des blancs, qui ont eu les moyens de faire des études. Bref, un petit concentré de privilèges bien ancrés et confortables et donc bien difficiles à enrayer...

2 Ordinateurs et mémoires numériques: des traces à tous les étages

2.1 Qu'est-ce qu'un ordinateur

Un ordinateur est une machine permettant de traiter, enregistrer, analyser, classer et transmettre des informations (des données) sous forme électrique. C'est un circuit électronique complexe rassemblant plusieurs composants aux rôles aussi nécessaires que différents:

- Carte mère:
  La carte mère est un grand circuit imprimé qui permet de brancher et de relier ainsi entre eux tous les autres éléments qui composent l'ordinateur (alimentation, processeur, mémoires, périphériques). Elle prend la forme d'une plaque de résine rectangulaire parcourue de l'équivalent de milliers de fils électriques de cuivre incrustés entre différentes fiches de branchement. C'est le système nerveux de l'ordinateur.

[2] Bien qu'existant aussi sous forme de livre, ce texte est à l'origine, destiné à être publié et mis à jour sur Internet, au format de brochure numérique. Ce qui permet de le copier ou de l'imprimer facilement avec les moyens du bord, et de le diffuser ensuite de manière décentralisée.

- Processeur:
  C'est la partie centrale de l'ordinateur, le cerveau qui réfléchit. En d'autres mots c'est réellement là que sont exécutés les programmes informatiques pour le traitement des données. Pour se représenter le travail d'un processeur, l'exemple le plus concret sur lequel se baser est la calculatrice. Tout d'abord, on y entre des données, les nombres (ici codés sous forme de nombres binaires qui sont constitués d'une succession de 0 et de 1). Ensuite, elle effectue des opérations qu'on lui dit de faire sur ces données; addition, multiplication ou autres (ici ces opérations sont des suites d'instructions contrôlées par les programmes informatiques). Finalement elle nous donne le résultat, qu'on peut éventuellement utiliser ensuite comme base pour d'autres calculs (tout comme l'ordinateur qui nous transmet directement les résultats à l'écran, mais qui peut aussi les mettre en mémoire).
  Le processeur est constitué d'une puce électronique, un micro-circuit branché directement sur la carte mère et qui contient des millions de composants électroniques aux dimensions infimes.

- Alimentation:
  C'est par là qu'est apportée l'énergie nécessaire à l'ordinateur sous forme d'électricité. C'est le système digestif de l'ordinateur.

- Mémoire vive:
  La mémoire vive (ou RAM, pour Random Access Memory), est l'équivalent de notre mémoire à court terme. Pour l'ordinateur, elle sert de mémoire temporaire de travail. En effet, c'est à cet endroit que sont stockées les données de tous les programmes et les documents ouverts. C'est là que le processeur va chercher les données à traiter et entreposer le résultat des opérations. C'est une mémoire dite volatile, c'est-à-dire une mémoire qui s'efface lorsque l'ordinateur n'est plus alimenté en électricité. C'est pourquoi ce type de mémoire est limité à son rôle de mémoire vive dans un ordinateur et ne peut servir au stockage d'informations au long terme. Néanmoins, quand on veut ne pas laisser de traces, cette propriété offre un avantages énorme par rapport à tous les autres types de mémoires qui sont non-volatiles ! On en reparlera à plusieurs reprises dans la suite du texte. Voir: 2.2.1
  Elle se présente souvent sous forme de barrettes qui se branchent directement sur la carte mère. Voir: 3.2.1

- Mémoire de stockage:
  Aussi appelée mémoire morte, elle correspondrait à notre mémoire à long terme. Elle sert à stocker des données même lorsque le support de mémoire n'est plus alimenté en électricité; c'est une mémoire non-

volatile ! Pourtant, et ceci est valable pour toute mémoire de stockage, cela n'exclut pas son usage en tant qu'extension de la mémoire vive, qui prend alors le nom de mémoire virtuelle (cf suite). Qui peut le plus peut le moins !
Elle se présente sous différents types de supports internes ou externes à l'ordi: mémoire magnétique (disque dur), mémoire flash (clés USB, cartes SD d'appareil photo ou de téléphone et barrettes SSD), mémoire optique (CD, DVD).

- Mémoire virtuelle:
  L'usage qui est fait dans ce texte du terme «mémoire virtuelle» est une simplification, qui réduit un concept informatique assez large à une seule de ses facettes. On parle de mémoire virtuelle (swap en anglais) quand un espace de mémoire de stockage est utilisé pour jouer un rôle de mémoire vive. Cette mémoire est fréquemment utilisée pour améliorer les performances des ordinateurs. Quand la mémoire vive est trop sollicitée, elle va relayer une partie de sa charge de travail à une mémoire de stockage interne de l'ordinateur (typiquement une partie de disque dur). En somme, c'est une mémoire vive qui laisse des traces non-volatiles. Les conséquences indésirables de ce fonctionnement sont approfondies dans la suite.

Voir: 2.2.2

- Périphériques:
  Les périphériques sont en quelque sorte les cinq sens de l'ordinateur qui lui permettent d'interagir avec l'extérieur sous une multitude de formes différentes (transmission et réception de données).
  Les périphériques vont venir se ficher dans différents connecteurs reliés à la carte mère. Ce sont le clavier, la souris, l'écran, les lecteurs et graveurs de CD/DVD, les prises (USB, firewire, jack, micro), la webcam, la carte réseau (wifi ou filaire), l'imprimante, les enceintes etc.

- Système d'exploitation:
  Le système d'exploitation est le programme de base qui permet de faire fonctionner les composantes de l'ordinateur avec les autres programmes. Il se trouve généralement sur le disque dur, mais peut aussi être enregistré sur des supports de mémoire transportables (clé USB, carte SD ou DVD). Tails est un système d'exploitation !

- Les autres programmes:
  Un programme informatique est une succession d'instructions exécutables par l'ordinateur dans le processeur. C'est la base de toute action sur un ordinateur qui, pour fonctionner, a besoin de milliers de programmes coordonnés par le système d'exploitation. Il y a différents

niveaux de programmation qui se passent le relais des instructions entre les programmes appelés «applications» qui sont destinés aux utilisatrices et utilisateurs (par exemple: Open Office) et les programmes interagissant directement avec le processeur.

2.2 Des traces dans toutes les mémoires

Un ordinateur, à moins qu'il ne fonctionne avec un système d'exploitation qui, comme Tails est spécifiquement conçu pour être discret, va laisser beaucoup de traces de tout ce que l'on fait dessus. Ceci même si on suppose, qu'il n'est pas connecté à l'Internet. En disant ça, on ne parle évidemment pas des données consciemment archivées sur un disque dur, mais bel et bien d'une multitude d'informations qui nous échappent, qu'on le veuille ou non. Ceci autant au niveau de leur éparpillement dans toutes les mémoires, que de la grande difficulté à les localiser et à les effacer vraiment. En fait, ces traces sont souvent nécessaires au bon fonctionnement de la plupart des systèmes d'exploitation !

Voir: 9.3

2.2.1 Traces dans la mémoire vive

Comme on l'a dit plus haut, tant que l'ordinateur est en marche, le rôle de cette mémoire est de stocker temporairement toutes les données dont le système d'exploitation a besoin pour tourner. Ça implique une grande panoplie d'informations dont certaines peuvent s'avérer très confidentielles et compromettantes. Cela va des textes tapés aux fichiers sauvegardés, en passant par les sites Internet visités, l'historique des clés USB connectées, les phrases de passe ou les clés de cryptage !
Heureusement pour nous, à moins d'une intrusion ciblée sur la mémoire vive pendant ou juste après l'utilisation de l'ordinateur, il devient rapidement impossible d'y récupérer une quelconque trace après la mise hors tension.

Voir: 3.2.1

2.2.2 Traces dans la mémoire virtuelle

Le système d'exploitation utilise, dans certains cas, une partie d'une mémoire de stockage pour venir en aide à sa mémoire vive. On constate ça si l'ordinateur est fortement sollicité, par exemple quand on travaille sur de gros fichiers ou quand on met le système en hibernation. Pourtant dans de nombreux autres cas, ça arrive de façon peu prévisible. La conséquence la plus chiante de ce fonctionnement, c'est que l'ordinateur va écrire sur une mémoire non-volatile des informations habituellement confinées à la mémoire vive, donc comme on l'a vu, potentiellement sensibles. Ces données resteront lisibles après avoir éteint l'ordinateur et ne seront pas si faciles à effacer.
Avec un ordinateur utilisé de façon standard, il est donc par exemple illusoire

de croire qu'un document ouvert puis refermé à partir d'une clé USB sans avoir été sauvegardé, ne laissera jamais de traces durables.

2.2.3 Traces dans les mémoires de stockage

Sur un ordinateur, la sauvegarde de données sur le long terme se fait dans deux situations bien distinctes. Soit c'est simplement nous qui faisons des sauvegardes, soit c'est l'oeuvre de l'ordinateur lui même qui compte sur l'archivage pour faire fonctionner correctement un système d'exploitation peu soucieux de discrétion.

- Journaux, sauvegardes automatiques et autres listes:
  La plupart des systèmes d'exploitation écrivent dans leur journal de bord un historique détaillé de ce l'on y fabrique. En plus de ces journaux, de nombreux programmes font régulièrement des sauvegardes automatiques. Cette pratique conduit à ce qu'un fichier, même parfaitement supprimé, continuera probablement, pendant un certain temps, à exister quelque part sur l'ordinateur, référencé ou stocké sous une forme différente (compressé par exemple).

- Sauvegardes volontaires et archivage de nos données:
  En fin de compte, on s'aperçoit que dans la masse de traces laissées, les moments où des traces sont conservées de manière délibérée de notre part font plutôt figure d'exception. Malgré tout, c'est quand même de façon régulière qu'on utilise un disque dur, une clé USB ou un CD pour archiver des documents ou sauvegarder un travail en cours. Et c'est tant mieux, car sans cette possibilité l'usage de l'informatique perdrait beaucoup de sens. Dans ce cas, on pourrait alors avoir l'impression de, pour une fois contrôler la destinée des traces qu'on laisse derrière nous. «Un tract est en cours d'écriture, je le sauvegarde avant de l'imprimer. Je n'en ai plus besoin, hop à la corbeille». Malheureusement les choses ne sont de nouveau pas aussi simples que ce que l'on pourrait croire au premier abord. Comme ça à été déjà plusieurs fois sous-entendu dans ce texte, l'effacement réel des données n'est pas forcément une mince affaire. C'est ce qu'on appelle le mythe de la corbeille.

Voir: 2.3

2.2.4 Traces dans les imprimantes, appareils photo et téléphones

Même si les mémoires numériques ont été initialement conçues pour les ordinateurs, elle sont actuellement très répandues dans un grand nombre d'autres appareils fonctionnant de manière tout à fait similaire pour traiter et stocker des informations (ce sont en fin de compte des sorte d'ordis). C'est notamment le cas des imprimantes, des appareils photo et des téléphones portables

dont le nombre dépasse de loin celui des ordinateurs à proprement parler. Aussi, c'est sans grande surprise que le problème des traces se repose. Ceci de manière souvent encore plus épineuse, puisque les outils (qui vont être présentés au point suivant) permettant d'éviter de laisser des traces sur les ordinateurs ne sont souvent pas disponibles sur d'autres machines.
Notons pour finir, qu'on parlera aussi à la fin du livre des traces laissées par, Voir:12.2.1
et non pas dans, les appareils photo numériques et les imprimantes.

- Traces dans les imprimantes:
  Les imprimante sont dotées d'une mémoire vive pour stocker temporairement les tâches qu'elles ont à accomplir. Jusqu'ici tout va bien puisque tout s'efface si on pense à éteindre l'imprimante entre deux utilisations. Là où ça se complique, c'est quand certains modèles d'imprimantes haut de gamme (comme ceux des centres de photocopies) disposent en plus d'une mémoire de stockage non-volatile sous la forme de disques durs internes. Celle-ci en plus d'être très difficilement accessible, va garder nos traces pendant un bon bout de temps.

- Traces dans les appareils photo et téléphones:
  La plupart du temps ces petits appareils utilisent des mémoires de stockage de type flash sous la forme de cartes mémoire. Si la carte peut être sortie de l'appareil photo ou du téléphone pour être branchée à un ordinateur, l'effacer devient équivalent à effacer une clé USB (avec les limites inhérentes à la technologie flash[3] soulevées au point suivant). Mais par contre, si l'appareil possède une mémoire interne (comme c'est souvent le cas avec les téléphones portables), il n'y a pas grand chose à faire.

2.3 Le mythe de la corbeille

Lorsqu'on «supprime» un fichier, en le plaçant dans la corbeille puis en la vidant, on ne fait que dire au système d'exploitation que le contenu de ce fichier ne nous intéresse plus. Il supprime alors son entrée dans l'index des fichiers existants. Il a ensuite le loisir de réutiliser l'espace de mémoire qu'occupaient ces données pour y inscrire autre chose. Mais il faudra peut-être des semaines, des mois voire des années avant que cet espace ne soit effectivement utilisé pour de nouveaux fichiers, et que les anciennes données soient recouvertes. En attendant, si on regarde directement ce qui est inscrit sur le disque dur, il est possible de retrouver le contenu des fichiers «effacés»

[3] On ne donnera pas de détails sur les différentes technologies utilisées pour faire des mémoires de stockage, mais il faut savoir qu'un disque dur s'efface différemment qu' une clé USB ou qu'un DVD. Pour plus d'infos: [http://etronics.free.fr/dossiers/num/num29/memoires.htm].

de cette manière. On peut noter qu'il se passe exactement la même chose quand on reformate un disque dur ou qu'on efface l'historique du navigateur Internet Firefox.
Ensuite, même si un fichier est recouvert, il n'est pas rare que certaines formes de traces puissent persister, par exemple sous forme de champs magnétiques résiduels sur les disques durs ou pire, à cause du fonctionnement parfois imprévisible des mémoire de type flash face à l'effacement[4] (clés USB, carte mémoires d'appareil photo ou téléphone et barrettes SSD). Ceci peut permettre à des raclures aussi répressives qu'oppressives, la recherche de nos données brutes sur les mémoires et leur récupération partielle ou complète par l'utilisation de matériel spécialisé.

2.4 Surveillance des ordinateurs et des mémoires numériques

La surveillance d'un ordinateur ou d'une autre machine hors-connexion implique que les flics ou d'autres collabos y accèdent physiquement pour y récupérer les traces de ce qui s'y est fait. Cela peut se faire par la ruse ou plus fréquemment par la force, lors de perquisitions ou d'arrestations. Si on n'applique aucune des précautions recommandées dans la suite du texte, la récupération et l'interprétation de nos données saisies de la sorte n'a rien de difficile. En fait, c'est aussi simple que de lire dans un livre ouvert (quand on sait lire).

Pourtant même quand on fait gaffe, des techniques de surveillance plus avancées existent. Elles seront décrites au fil des chapitres 3, 5 et 12, en lien avec les divers outils qu'on essaie de leur opposer.
De plus, on verra que la surveillance informatique et la répression qui peut l'accompagner s'appuient de plus en plus sur l'exploitation de traces laissées ou extirpées sur des ordinateurs connectés à des réseaux avec ou sans le recours aux logiciels malveillants et aux métadonnées. On en parle aux chapitres 3, 5, 9, 10 et 12.

2.5 Comment ne pas laisser ses traces dans les mémoires numériques

On renvoie ici en quelques mots aux chapitres pratiques présentant des outils qui peuvent aider à éviter de laisser trop de traces compromettantes dans les mémoires numériques:

- À moins de détruire physiquement le support de mémoire, il n'y a qu'une manière d'effacer ses traces d'une façon pouvant être considérée

[4] Pour plus d'infos en anglais: [https://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html], [https://tails.boum.org/todo/wiping_flash_media/] et [https://en.wikipedia.org/wiki/Secure_file_deletion#Data_on_solid-state_drives].

comme satisfaisante. Elle consiste à réinscrire de multiples fois l'ensemble de la partition[5] de mémoire avec des données aléatoires et des motifs choisis pour maximiser la destruction des données résiduelles. On verra comment faire ça avec la commande shred au chapitre 4.

- Dans une autre perspective, le recours au cryptage de nos données, à défaut de ne pas laisser de traces, va au moins rendre celles-ci très difficilement utilisables. Le concept et les applications du cryptage seront présentées aux chapitres 5, 6, 7 et 8.

- Finalement, l'utilisation d'un système d'exploitation discret, est peut-être l'outil à disposition le plus efficace pour empêcher que nos traces ne soient laissées ailleurs que dans la mémoire vive de l'ordinateur et autrement que de manière temporaire. Cela va être approfondi au chapitre 3, consacré au système d'exploitation Tails.

3 Utiliser un ordinateur sans laisser de traces avec Tails[6]

3.1 Qu'est-ce que Tails[7]

Comme on l'a vu au chapitre précédant, les systèmes d'exploitation classiques (Windows, Mac, Ubuntu, etc.) laissent, qu'on le veuille ou non, des traces sur les mémoires, notamment en sauvegardant à notre insu des données très difficiles à vraiment effacer.
TAILS (The Amnesic Incognito Live System) est un système d'exploitation assez révolutionnaire ! Il est conçu pour ne laisser, dans les mémoires de l'ordinateur aucune trace persistante de ce qu'on y fait, à moins que ça ne lui soit explicitement demandé. C'est pourquoi il est qualifié d'«amnésique». Cet exploit est rendu possible par le fait que ce système n'a pas besoin du disque dur de l'ordinateur pour fonctionner, ni même de la mémoire virtuelle. Tails ne laisse temporairement des traces que dans la mémoire vive, qui est effacée automatiquement à l'extinction de l'ordinateur.
Voir: 2.1
De plus, c'est un live-system. C'est-à-dire que le système d'exploitation est installé sur une clé USB, une carte SD ou un DVD, des supports de mémoire amovibles qui permettent de lancer Tails au démarrage de n'importe quel ordinateur, qu'on soit chez soi, chez un-e ami-e ou à la bibliothèque du coin ! Bien sûr, l'utilisation de Tails ne modifie pas le système d'exploitation en place sur l'ordinateur. Une fois le support de mémoire contenant Tails retiré de l'ordinateur, celui-ci peut redémarrer sur le système d'exploitation

[5] Une partition est la subdivision de base des mémoires de stockage.
[6] Du moins sans laisser de traces informatiques sur un ordinateur hors-connexion.
[7] Ce chapitre et les chapitres suivants ont été écrits à partir de la version de Tails 1.4 (printemps 2015). Certaines infos sont susceptibles de changer au fil des versions !

habituel. Cette conception a de nombreux avantages pratiques. Tout d'abord, ce système est facilement transportable et dissimulable puisqu'il tient dans une poche. Dans le même ordre d'idée, il est accessible et destructible à peu de frais. En effet, comme le système en lui même est gratuit il suffit de mettre la main sur un clé USB, une carte SD ou un DVD sans forcément posséder soi-même un ordinateur. Un dernier aspect intéressant et peu connu est que l'utilisation d'un live-system permet dans de nombreux cas de s'infiltrer sur un ordinateur ou un réseau sans nécessiter pour autant les codes d'accès et autres autorisations habituellement exigées par les systèmes d'exploitation traditionnels. On réussit par exemple souvent à utiliser le parc d'ordinateurs et la connexion Internet d'une administration sans en être membre !

Pour finir, il est important de relever qu'au delà de ces spécificités, Tails est un environnement informatique Linux complet et facile d'utilisation. Il est développé et fréquemment mis à jour par une équipe de personnes militantes et, comme c'est un logiciel libre[8], son code est ouvert à quiconque aurait l'envie et les connaissances techniques pour participer au projet ou juste jeter un œil. Il embarque de nombreux programmes minutieusement intégrés au système qui permettent de travailler sur tout type de document sensible (texte, image, son, vidéo), de communiquer et d'utiliser Internet en contrôlant les traces qu'on laisse, de manière confidentielle et... anonyme. C'est d'ailleurs cette démarche radicale en faveur de l'anonymat qui explique pourquoi il est qualifié d'«incognito». Ces outils vont constituer le fil rouge de tous les chapitres pratiques de la suite du texte.

3.2 Limites de Tails et parades

Rien, aucune défense n'est infaillible, c'est un processus en perpétuel ajustement face aux attaques, et le système Tails ne fait pas exception.

3.2.1 Attaques sur la mémoire vive

Comme ça a déjà été évoqué, environ tout ce qu'on fait durant la session de travail de Tails est stocké dans la mémoire vive. De là, deux types d'attaques sont envisageables:

- Dans le premier cas, un-e attaquant-e a accès à l'ordinateur en cours d'utilisation. Soit un accès physique qui peut être aussi simple qu'y brancher un smartphone trafiqué quand on a le dos tourné, soit un accès virtuel en infiltrant, à distance par le réseau Internet, un virus ou tout autre logiciel malveillant.

[8] Pour plus d'infos: [https://fr.wikipedia.org/wiki/Logiciel_libre].

- Deuxièmement, il a été démontré que des données présentes dans la mémoire vive peuvent être récupérées plusieurs secondes ou même minutes après extinction de l'ordinateur en utilisant une attaque dite «cold boot»[9].

Dans les deux cas, le contenu de la mémoire vive peut être récupéré, des textes tapés aux fichiers sauvegardés, sans oublier les mots de passe et clés de chiffrement. Ce qui peut se révéler être un véritable désastre !

Alors, qu'en est-il des stratégies de défense ?

- Le premier type d'attaque peut être difficile à parer. Dans le cas d'une intrusion physique ça va encore, puisqu'il s'agit de ne pas laisser la session de Tails sans surveillance. Mais comme on le verra par la suite, se prémunir de manière absolue contre l'attaque de logiciels malveillants s'avère être un vrai casse-tête.

- Pour ce qui est des attaques de type «cold boot», la stratégie de défense est quand même plus facile et des outils sont déjà en place. En effet, à chaque mise hors tension, Tails effectue l'effacement du contenu de la mémoire vive en la remplissant de données aléatoires, qui recouvrent tout ce qui s'y trouvait auparavant.
  Donc, un bon réflexe lorsqu'on a fini de travailler sur Tails ou qu'on entend les flics à la porte, consiste à simplement éteindre la session Tails (et donc l'ordinateur). De plus, quand on fait tourner Tails sur un ordinateur portable, il faut se rappeler d'enlever la batterie, qui garde sinon la mémoire vive sous tension ! Ensuite on a tout le loisir d'attendre, ou d'essayer de gagner un temps précieux en barricadant la porte. Finalement, on peut quand même relever que les attaques «cold boot» ne semblent pas (encore ?) être une procédure standard du coté des flics ou des agences gouvernementales répressives de par le monde.

3.2.2 Virus et autres logiciels malveillants

Même avec un système comme Tails, l'élaboration d'une ligne de défense contre les logiciels malveillants n'est pas chose facile, tant la diversité des stratégies et des angles d'attaque est grande. Les possibilités d'action et donc de nuisance des logiciels malveillants n'ont de limite que l'imagination de leur créateur-trice.
Voir:12.1.1
Les personnes impliquées dans le développement de Tails mettent une grande

[9] Pour plus d'infos: [https://tails.boum.org/doc/advanced_topics/cold_boot_attacks/index.fr.html].

énergie à prévenir et corriger des brèches de sécurité qui pourraient être exploitées par des adversaires malveillant-e-s et leurs logiciels. Mais on ne peut pas tout prévoir, aucun effort humain, antivirus ou pare-feu ne peut exclure l'éventualité d'avoir à un moment donné un temps de retard face à une nouvelle attaque. Sans parler du fait que de nombreux logiciels malveillants comptent sur des erreurs humaines et non pas matérielles pour infecter un système (par exemple par l'ouverture d'un fichier-joint accompagnant un e-mail piègeux). Comme on le verra plus tard, il n'y a pas beaucoup de souci à se faire à propos de la majorité des logiciels malveillants qui ont des buts commerciaux et ne ciblent que rarement les systèmes Linux (dont Tails fait partie). Par contre, ce qui plus inquiétant est le développement, par les gouvernements[10] du monde entier, de logiciels espions spécifiquement conçus à des fins de surveillance sur des personnes ou des groupes spécifiques, utilisant des outils spécifiques (dont Tails). C'est donc bien cette deuxième éventualité qui pourrait gravement compromettre la sécurité de Tails et des personnes qui l'utilisent. Le recours à ces moyens de surveillance est en nette augmentation depuis quelques années. Et ça risque bien de continuer, puisque avec la popularisation de technologies comme le cryptage, c'est souvent le seul moyen qui leur reste pour persister à surveiller les télécommunications. Pourtant, ça demande la mise en œuvre de moyens coûteux et demeure en général lié à une enquête poussée.

Voir: 5.1

Il y a principalement deux voies d'entrée sur Tails (avec des conséquences similaires) pour les attaques de logiciels malveillants:

- Présence dès le début dans une version corrompue de Tails:
  Cette attaque repose sur le fait de substituer à la version officielle et intègre de Tails qui est disponible en téléchargement, une version modifiée du système intégrant des logiciels espions cachés.

- Infiltration ultérieure dans Tails:
  L'enjeu de cette attaque consiste à réussir à infiltrer un logiciel espion de manière plus ou moins durable dans le système. Tout d'abord, ceci peut se faire via un accès physique au système. Des supports amovibles comme les clés USB, les disques durs externes, les appareils photo numériques et les téléphones servent de plus en plus souvent de

[10] Pour plus d'infos sur les moyens des keufs dans ce domaine notamment en France, aux USA et en Suisse: [https://www.pcinpact.com/news/51027-police-opj-cheval-troie-loppsi.htm], [http://www.bastamag.net/Logiciels-mouchards-metadonnees-reseaux-sociaux-et-profilage-comment-l-Etat], [http://www.wired.com/politics/law/news/2007/07/fbi_spy ware], [https://ntdroit.wordpress.com/2013/03/07/revision-de-la-lscpt-et-nouvelles-bases-legales-pour-les-logiciels-espions/], [http://www.ejpd.admin.ch/content/ejpd/fr/home/dokumentation/mi/2013/2013-02-271.html] et [http://www.itespresso.fr/chaos-computer-club-un-logiciel-espion-encombrant-pour-la-police-allemande-47218.html].

vecteurs de propagation pour des logiciels malveillants[11]. Il est possible que la connexion au système de ces périphériques infectés, soit due à une personne malveillante. Pourtant, malheureusement on le fait le plus souvent par nous-même. Mais au final, le plus grand risque est que l'infection se fasse à distance via une connexion à Internet. En effet, un réseau où de nombreux ordinateurs sont reliés est le milieux idéal pour accéder discrètement à un ordinateur. Sur Internet, de nombreuses possibilités d'intrusion s'offrent aux flics et suivent deux principales stratégies d'attaque. Premièrement, en essayant de tromper la personne qui utilise l'ordinateur afin d'installer le logiciel malveillant. Ça peut se faire via l'ouverture d'une page Internet, un téléchargement de fichier infecté, caché derrière l'installation d'un programme d'apparence inoffensif, ou par l'ouverture d'un pdf ou d'un fichier infecté accompagnant un e-mail. Deuxièmement, en exploitant des failles dans les programmes déjà installés sur l'ordinateur. De plus, afin de mieux cibler des individu-e-s ou des groupes, les attaques peuvent être très personnalisées. Voici deux exemples. Le logiciel malveillant peut être dissimulé dans un lien de téléchargement d'un site que les flics surveillent mais qui est géré et visité de manière anonyme. Encore plus tordu, l'identité d'un-e ami-e peut être usurpée (via sa boîte mail) pour envoyer un faux e-mail personnel contenant un fichier-joint malveillant.

Voir: 9.4.6

L'anticipation du premier type d'attaque, implique une attention portée à chaque nouvelle version de Tails. En effet, ce type d'attaque peut être contrecarré dans la plupart des cas par la vérification de l'authenticité de la version de Tails que l'on vient de télécharger. Cela permet de s'assurer que le système que l'on va utiliser n'a pas été modifié, depuis sa publication par des personnes de confiance impliquées dans son développement[12].

Voir: 3.4.1
Voir: 3.4.3

Maintenant, au sujet des parades possibles à l'infiltration de logiciels malveillants:

- Avant tout, voici trois pratiques de base permettant de limiter les infections ou leurs effets, que ce soit via un accès physique au système ou par Internet. Premièrement, il faut savoir qu'il est plus sûr d'utiliser un DVD non réinscriptible plutôt qu'une clé USB comme support pour Tails (les deux types d'installation sont quand même présentés dans le texte). En effet, un logiciel malveillant n'aura physiquement pas la possibilité de se cacher de manière permanente sur ce genre mémoire,

Voir: 3.4

[11] Un exemple: [http://www.itespresso.fr/les-malware-sur-cle-USB-ont-le-vent-en-poupe-21310.html].

[12] Une page intéressante sur la confiance que l'on peut avoir dans le travail des personnes qui font Tails: [https://tails.boum.org/doc/about/trust/index.fr.html].

ce qui n'est pas le cas pour les clés USB. Deuxièmement, il peut être assez sage de n'autoriser l'accès administrateur-trice au système que de manière exceptionnelle, si on veut par exemple installer des programmes supplémentaires. Cette décision se fait au démarrage de Tails. Enfin, il peut être préférable pour un usage collectif, dans une salle informatique par exemple, d'utiliser Tails sur un ordinateur dédié sur lequel on aura pris le soin de débrancher les supports de mémoire de stockage (disques durs internes, mémoire SSD). Ceci afin de diminuer les risques de contamination persistante.

Voir: 3.3.4

- Pour ce qui est spécifiquement de l'infiltration de logiciels espions par un accès physique au système, et comme on l'a déjà dit précédemment; il faut éviter de tourner le dos au système, tant qu'on ne peut avoir la certitude que seules des personnes de confiance peuvent y accéder. Ceci est valable que celui-ci soit allumé ou éteint et surtout s'il est installé sur une clé USB.

- Pour ce qui est spécifiquement des intrusions via Internet, on peut d'ores et déjà placer un petit mot à propos de l'inutilité des antivirus dans le cas de Tails. Premièrement du fait de la quasi inexistence d'épidémies ciblant Linux, les antivirus disponibles se contentent surtout de rechercher sur notre système Linux, des logiciels malveillants qui infectent Windows et Mac. Ce qui n'a que peu d'intérêt, si on garde à l'esprit qu'un virus Windows n'affectera quasiment jamais un système Linux ! Le second problème des antivirus sous Linux est que même si un nouveau virus est détecté sous Linux, il le sera bien moins rapidement que sous Windows. Linux n'étant pas le domaine de prédilection ni le marché numéro 1 des antivirus, il est quasiment certain que le virus ne sera déjà plus efficace quand la mise à jour permettant de s'en débarrasser sortira. Ceci est d'autant plus vrai que dans le cas qui nous concerne, on ne parle pas de virus largement diffusés mais de programmes espions taillés sur mesure dans le cadre de surveillances précises.
  Maintenant que c'est dit, on peut quand même évoquer quelques moyens concrets de limiter les risques d'infection via Internet: n'installer (ou n'utiliser) aucun logiciel propriétaire[13] ou de provenance inconnue, ne pas faire confiance au premier site web venu, faire preuve de méfiance en ce qui concerne les téléchargements et les fichiers-joints et toujours veiller à mettre à jour sa version de Tails.

Voir: 3.4

[13] Logiciel dont le code source (la recette), n'est pas librement disponible, vérifiable et modifiable.

Pourtant, même si on a bien en tête ces précautions de base, il est évident que c'est aussi le cas de nos ennemis. Et puis, à quoi bon utiliser Internet si c'est pour s'empêcher de visiter certains sites, de télécharger une brochure, d'ouvrir un pdf ou même de cliquer sur une image ? Il faut se rendre à l'évidence, l'utilisation d'Internet constitue de loin la principale source de vulnérabilité pour Tails; dans ce cas encore plus que dans d'autres, le risque zéro n'existe pas. Face à ce relatif constat d'échec, il nous reste néanmoins quelques ressources. Imaginons que l'on prenne pour acquis que le système puisse être infecté à notre insu par un logiciel malveillant, capable du pire. Disons transmettre par Internet notre adresse IP et des données personnelles contenues temporairement en mémoire vive. Quelles options nous reste-t-il ?

Voir: 9.3.2

- La méthode du Air Gap ou Trou d'Air:
  Si on veut en priorité protéger ses données confidentielles de l'attaque de logiciels espions, une pratique prudente est d'utiliser la méthode du Air Gap ou Trou d'Air qui consiste à sécuriser un système sensible en l'isolant du réseau Internet.

Voir: 15.1

- La méthode du squattage d'IP:
  Si, face à l'éventualité d'attaques de logiciels espions, on veut en priorité protéger son anonymat lors d'activités sensibles en réseau auxquelles ont aimerait en aucun cas être identifié-é via l'adresse IP, une bonne pratique consiste à utiliser Tails sur un ordinateur ne pouvant être relié à nous (par exemple: bibliothèques, écoles, Internet cafés). Comme ça, même si le logiciel espion trahit l'adresse IP de l'ordinateur malgré l'utilisation d'un réseau d'anonymisation comme Tor, il restera quand même difficile de faire le lien avec nous. À moins bien sûr d'une identification dûe à des citoyen-ne-s flics, à la vidéosurveillance, à une filature policière ou autre.

Voir: 10.1

La manière dont ces deux dernières pratiques ont été présentées peut donner l'impression qu'elles sont réservées à des cas de surveillance ou de parano extrêmes et donc à utiliser en dernier recours. Mais en fait, pas tant que ça, à en juger par les cas de répression informatique qu'elles auraient peut-être déjà permis d'éviter. Donc, on ne peut que recommander qu'elles fassent partie intégrante de notre usage de l'informatique au quotidien pour des activités sensibles.

3.3 Lancer et utiliser Tails

On va voir ici comment démarrer un ordinateur avec un système Tails sur une clé USB ou un DVD. La plupart du temps, c'est très simple. D'autres fois, c'est un peu à s'arracher les cheveux mais on y arrive. Dans de très rares

cas, tout se complique à cause d'une incompatibilité matérielle de certains modèles d'ordinateurs avec certaines clés USB, DVD ou même avec Tails tout court. Par exemple, certains anciens ordinateurs Macs ne peuvent faire fonctionner Tails qu'à partir d'un DVD. Si définitivement rien ne marche, il ne reste alors plus qu'à essayer sur un autre ordi ou à utiliser un autre support de mémoire pour Tails. Pas de bol.
Tout se joue au démarrage de l'ordinateur. Trois étapes sont présentées ici. Dans le meilleur des cas, le système démarre dès la première étape, mais il faut souvent passer à la deuxième et parfois à la troisième étape.

3.3.1 Première étape: essayer naïvement

Commencer par insérer la clé USB ou le DVD contenant Tails, puis démarrer l'ordinateur. Parfois, ça marche tout seul et Tails démarre alors automatiquement. Si c'est le cas, c'est gagné, lire la suite est inutile et on peut directement passer au point 3.3.4 !

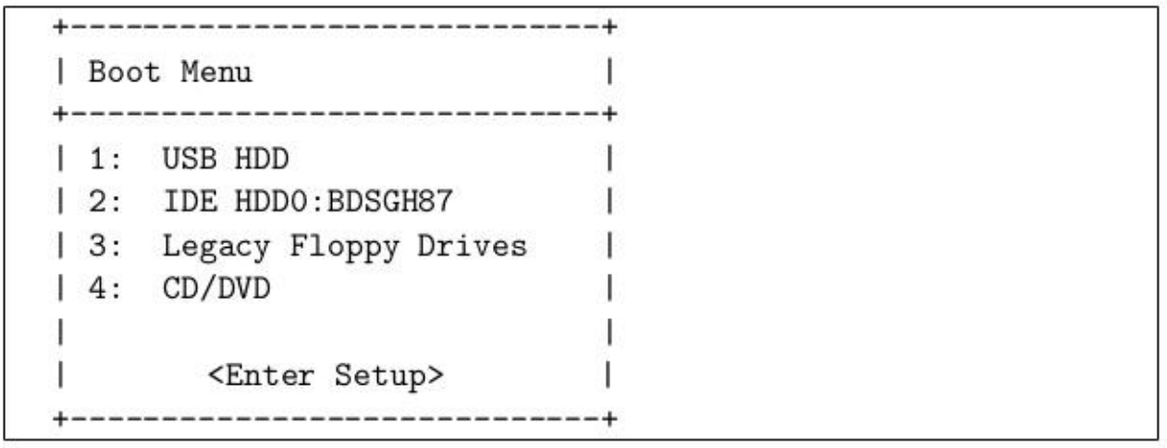
3.3.2 Deuxième étape: tenter de choisir le périphérique de démarrage

Si ton ordinateur ne démarre pas automatiquement à partir de la clé USB ou du DVD qui contient Tails, tu dois accéder au menu de démarrage (boot menu). Ce menu liste les différents périphériques de démarrage (par exemple: disque dur, CD, USB, DVD) qui peuvent contenir un système d'exploitation. Pour cela, redémarrer l'ordinateur (appuyer simplement sur le bouton d'allumage de l'ordi) en regardant attentivement les tout premiers messages qui s'affichent à l'écran. Chercher des messages en anglais qui ressembleraient à:

```
Press [KEY] to select temporary boot device [KEY] = Boot menu
```

```
[KEY] to enter MultiBoot Selection Menu
```

Ces messages disent d'utiliser une touche [**KEY**] pour choisir un périphérique de démarrage. Cette touche est souvent **F12**, **F10** ou **Esc**. Au bout d'un moment, on doit normalement voir apparaître le menu de démarrage. Mais souvent, on n'a pas le temps de lire le message, de le comprendre et d'appuyer sur la touche. Qu'à cela ne tienne, redémarrer l'ordinateur autant de fois que nécessaire et une fois la bonne touche identifiée, redémarrer une dernière fois la machine en appuyant sur la touche en question dès l'allumage de l'ordinateur. Il ne faut pas maintenir la touche enfoncée, mais la presser puis la relâcher plusieurs fois. Avec un peu de chance, un message comme celui-ci s'affiche:



Si ça marche, c'est gagné. Choisir la bonne entrée dans ce menu, en se déplaçant avec les flèches du clavier ↑ et ↓ , puis appuyer sur la touche **Entrée** du clavier. Par exemple, pour démarrer sur une clé USB, choisir USB HDD. Pour démarrer sur DVD, il faudrait choisir l'option mentionnant CD/DVD.

Sur les Macs récents, rien de tel n'apparaît à l'écran mais il existe un équivalent de cette possibilité. Immédiatement après le redémarrage de l'ordinateur, il faut appuyer de manière répétée sur la touche **alt** ou parfois **c**. Ensuite, il s'agit de sélectionner parmi icônes qui apparaissent, celle représentant un DVD et d'appuyer finalement sur la touche **Entrée** du clavier.

Si les manoeuvre présentées à cette étape fonctionnent, l'ordinateur va lancer Tails à partir du périphérique sélectionné et lire le prochain point est inutile !

3.3.3 Troisième étape: modifier les paramètres du menu démarrage

Si choisir un périphérique de démarrage ne fonctionne pas, il va falloir modifier les options du menu démarrage manuellement. Encore une fois, il s'agit de redémarrer l'ordinateur en regardant attentivement les premiers messages qui s'affichent à l'écran. Chercher des messages en anglais qui ressembleraient à:

```
Press [KEY] to enter setup Setup:  [KEY]
```

```
[KEY] = Setup Enter BIOS by pressing [KEY]
```

```
Press [KEY] to access BIOS Press [KEY]
```

```
to access system configuration For setup hit [KEY]
```

Ces messages disent d'utiliser la touche [**KEY**] pour entrer dans le BIOS[14]. Cette touche est souvent **Suppr**, **Delete**, **DEL** ou **F2**, parfois **F1**, **F10**, **F12**, **Échap**, **esc**, **Tab**, voire autre chose encore.
Souvent, comme pour l'étape précédente, on n'a pas le temps de lire le message, de le comprendre et d'appuyer sur la touche; il faut donc rallumer plusieurs fois l'ordinateur.
Une fois dans les options du menu démarrage, l'écran est souvent bleu ou noir et plein de sous-menus. En général, une zone en bas ou à droite de l'écran explique comment naviguer entre les options, et les modifier. Il faut s'y référer. L'idée, c'est de fouiller dans les menus jusqu'à trouver quelque chose qui contient «**Boot**», et qui ressemble par exemple à:

```
First Boot
```

```
Device Boot
```

```
Order Boot
```

```
Boot Management
```

```
Boot Sequence
```

Une fois la bonne entrée trouvée, il faut encore parfois entrer dans un sous-menu (par exemple, s'il y a un menu **Boot order**).
Il s'agit alors de trouver comment on modifie ce menu (toujours en se référant à la zone en bas ou à droite de l'écran). L'objectif est alors de mettre USB ou DVD en premier sur la liste (suivant si on veut démarrer sur DVD ou USB). Après avoir enregistré les modifications, redémarrer l'ordinateur et retourner à la deuxième étape.

Voir: 3.3.2

3.3.4 Ouverture et utilisation d'une session de travail de Tails

Maintenant qu'on a réussi à démarrer sur la clé USB ou le DVD voici comment faire ses premiers pas sur Tails:

1. Écran noir **Boot Tails**:
   Ne toucher à rien, à ce stade Tails démarre automatiquement en passant par une barre de chargement et plusieurs écrans successifs.

[14] Le Basic Input Output System (BIOS, en français: «système élémentaire d'entrée/sortie») est un petit programme intégré à la carte mère permettant d'effectuer les actions et les réglages de base au démarrage de l'ordinateur.

2. Écran bleu **Welcome to Tails**:

   2.1. Sur le menu déroulant en bas à gauche, choisir la langue.

   2.2. Sur le menu déroulant en bas à droite, choisir le type de clavier. Pour ça, cliquer sur **other** puis défiler jusqu'à la bonne entrée.

   2.3. Si on démarre Tails avec un **Stockage persistant** crypté et qu'on veut utiliser celui-ci pour la session à venir, il faut choisir **Oui** à la boîte de dialogue qui demande: **Activer la persistence ?** et taper ensuite la phrase de passe requise.

Voir: 6.3

3. À ce stade, deux autres options sont encore possibles:

   3.1. Soit une connexion avec droits d'administration (plus souple, mais moins sûr). Sur la fenêtre du milieu, répondre **Oui** à la question **Plus d'options ?** puis cliquer sur **Suivant**. Un écran apparaît permettant de choisir un mot de passe. Écrire à deux reprises le mot de passe d'administration de son choix (seulement valable pour cette session), puis cliquer sur **Connexion**.

Voir: 3.2.2

   3.2. Soit une connexion sans droits d'administration (plus sûr, mais moins souple). Sur la fenêtre du milieu, laisser l'option par défaut **Non** à la question **Plus d'options ?** puis cliquer sur **Connexion**.

4. Durant l'utilisation du live système:

   4.1. Une fois la session ouverte, il est possible d'utiliser les nombreux programmes contenus dans le menu **Applications** situé dans la barre d'icônes en haut à gauche de l'écran.

   4.2. Une fois la connexion à Internet faite, le branchement au réseau de navigation Internet anonyme Tor se fait automatiquement, un message indiquant quand **Tor est prêt** apparaissant alors dans le coin supérieur droit de l'écran. Le tout peut prendre plus de 30 secondes. On peut ensuite aller surfer sur Internet, en ouvrant une page de navigation du **Navigateur Tor** (équivalent de Firefox), via le menu **Applications** ▷ **Internet** ▷ **Démarre le Navigateur Tor**.

Voir:10.4.1

   4.3. Toute donnée qui n'est pas sauvegardée sur une mémoire persistante est irrémédiablement perdue à la fin de la session !

5. Pour éteindre l'ordi, cliquer sur le **bouton gris** situé dans la barre d'icônes en haut à droite de l'écran, puis sur **Éteindre immédiatement**. L'effacement de la mémoire et la mise hors tension sont automatiques.

3.4 Installer et mettre à jour Tails sur DVD ou clé USB[15]

Par souci de cohérence et de sécurité, et à l'image du reste du texte, les marches à suivre présentant ici comment installer et mettre à jour Tails, vont elles-même s'accomplir à partir d'un système Tails. Mais comment faire quand on veut justement installer Tails pour la toute première fois ? Une manière intéressante de remédier à cette situation apparemment paradoxale, est de demander de l'aide à une connaissance utilisant déjà Tails. On pourra ensuite participer à son tour à la diffusion de copies du système dans des cercles de confiance et à l'organisation d'ateliers où on découvre et installe Tails. Sinon, il est toujours possible et très facile de télécharger, authentifier et graver Tails sur un DVD, à partir de n'importe quel système d'exploitation autre que Tails. Cette manière de faire n'est pas détaillée dans ces pages, mais elle est très bien documentée[16] sur Internet.
Pour finir, on peut encore relever la grande importance de maintenir Tails à jour! Si on ne le fait pas, le système sera sujet à de nombreuses failles de sécurité. Mettre à jour implique de télécharger, authentifier et installer la nouvelle version de Tails dès sa sortie, qui a lieu toutes les six semaines. Pour nous tenir au courant, à chaque connexion à Internet, Tails affiche un avertissement s'il détecte qu'on utilise une ancienne version du système.

3.4.1 Installer et mettre à jour Tails sur un DVD

On va voir dans ce point comment télécharger, authentifier, installer et donc graver la dernière version de Tails sur un DVD. De là, mettre à jour Tails sur DVD reviendra à graver un nouveau DVD non-réinscriptible à chaque nouvelle version du système. Ce qui rend la mise à jour un peu plus contraignante que l'opération équivalente sur clé USB.

Voir: 3.4.4

On peut encore noter que la méthode d'authentification de Tails va utiliser le programme Open PGP, permettant entre autre la vérification de signatures cryptographiques. À ce stade, il n'est peut-être pas nécessaire de comprendre toutes les subtilités de son fonctionnement qui sera détaillé plus tard.

Voir: 5.1

Voir: 7.1

Bon, voici comment faire:

1. Télécharger la dernière version de Tails:
   1.1. Démarre Tails depuis une clé USB ou un DVD (si ton ordi a un lecteur DVD distinct du graveur).
   1.2. Une fois dans Tails, connecte-toi à Internet via **Tor**, va sur la page

Voir:10.4.1

[15] À noter que bien qu'on ne cite pas systématiquement dans le texte les cartes SD comme support d'installation pour Tails, elles sont pourtant, de manière équivalente aux clés USB, tout à fait adaptées à l'installation, la mise à jour et le démarrage de Tails.

[16] Pour plus d'infos: [https://tails.boum.org/download/index.fr.html] et [https://tails.boum.org/doc/first_steps/dvd/index.fr.html].

officielle de téléchargement [`https://tails.boum.org/download/index.fr.html`] et clique sur le rectangle vert contenant le lien de téléchargement de la dernière version de Tails. C'est un fichier au format **.iso**, enregistre-le dans le dossier de téléchargement du **Navigateur Tor**, appelé **Tor Browser**. C'est un gros fichier, c'est donc normal que le téléchargement dure longtemps (jusqu'à quelques heures).

2. Vérifier l'authenticité de la dernière version de Tails:

   2.1. Il faut maintenant télécharger la signature dite numérique, ou cryptographique, authentifiant le travail des personnes qui développent Tails. C'est un fichier **.sig** correspondant au fichier **.iso** de la version de Tails que tu souhaites vérifier. Pour ça, toujours sur la même page que précédemment, clique sur le rectangle vert contenant le lien de téléchargement de cette signature et qui est intitulé **Tails Signature**. Une fenêtre s'ouvre appelée **Ouverture de Tails...**, la case **Ouvrir avec: Vérifier la signature** est sélectionnée par défaut, clique sur **OK**.

   2.2. Une nouvelle fenêtre s'ouvre, intitulée **Choisissez un fichier original pour Tails**. Il s'agit donc maintenant, d'entrer dans le dossier ▷ **Tor Browser**, que l'on trouve dans la colonne gauche et où on a auparavant téléchargé la dernière version de Tails. Ensuite, il faut selectionner ce fichier reconnaissable par son extension **.iso** et cliquer sur **Ouvrir**.

   2.3. Là, une fenêtre apparaît, indiquant **Vérification**. La vérification de l'authenticité du fichier de Tails peut prendre jusqu'à une minute. Si à l'issue de ce processus, le fichier est reconnu comme intègre et authentique, une fenêtre s'ouvre en haut à droite de l'écran et annonce: **Signature valide**. Si à l'inverse, la version de Tails est reconnue comme corrompue, la même fenêtre annoncera: **Signature non valide**. Dans ce cas peu fréquent, il ne reste plus qu'à télécharger à nouveau le fichier **.iso** et à refaire l'authentification.

3. Graver Tails sur un DVD:

   3.1. Fais un clic droit avec la souris sur le fichier **.iso** de Tails que tu désires graver, choisis **Ouvrir avec Gravure de disque Brasero** dans le menu. Une fenêtre intitulée **Options de gravure d'une image** s'ouvre.

   3.2. Insère un DVD dans le graveur DVD de l'ordinateur. Ferme la fenêtre qui s'ouvre automatiquement à l'insertion du DVD. Clique

ensuite sur le bouton **Propriétés** et choisis la vitesse de gravure la plus lente possible pour diminuer le risque d'erreurs de gravure. Enfin, clique sur **Graver**. À la fin de la gravure, le DVD contient Tails et tu peux démarrer dessus.

Voir: 3.3

3.4.2 Installer Tails sur une clé USB

Que ce soit pour l'installation (duplication) ou la mise à jour manuelle des versions de Tails sur clé USB, la marche à suivre qu'on propose ici nécessite l'utilisation simultanée de deux supports de mémoire. L'un, une clé USB ou un DVD contenant déjà un système Tails, sur lequel on va démarrer et qu'on peut utiliser comme modèle; l'autre, la clé USB sur laquelle on a envie d'installer ou de mettre à jour Tails.

Attention, dans le cas de la duplication (pas de la mise à jour) l'intégralité du contenu de la nouvelle clé sera perdu durant l'opération !

1. Démarre Tails depuis une clé USB ou un DVD avec le système Tails à jour (ne branche pas encore la clé USB sur laquelle tu veux mettre Tails).

2. Une fois dans Tails, il s'agit maintenant d'installer le système sur une clé USB. Choisis **Applications ▷ Tails ▷ Programme d'installation de Tails** pour démarrer le **Programme d'installation de Tails**.

3. Pour installer Tails sur une nouvelle clé USB, clique sur le bouton **Cloner & Installer**.

4. Branche la clé USB sur laquelle tu souhaites installer Tails. Un nouveau périphérique, correspondant à la clé USB, apparaît alors dans le menu déroulant des **Périphériques Cibles**.

5. Sélectionne la clé USB dans le menu déroulant des **Périphériques Cibles**.

6. Pour démarrer l'installation, clique sur le bouton **Installer Tails**. Lis le message d'avertissement. Clique sur le bouton **Yes** pour confirmer. Une fois que l'installation est terminée, tu vas pouvoir immédiatement démarrer Tails depuis cette nouvelle clé USB.

Voir: 3.3

3.4.3 Mettre à jour automatiquement Tails sur une clé USB

Après le démarrage de Tails sur clé USB et la connexion à Internet via Tor, le **Tails Upgrader** vérifie automatiquement si des mises à jour sont disponibles et propose le cas échéant de mettre à jour Tails sur la clé USB.

Cette méthode comporte plusieurs avantages par rapport à une mise à jour manuelle sur DVD ou sur clé USB. Tout d'abord, on a uniquement besoin d'un seul périphérique avec Tails (au lieu de deux). En effet, la mise à jour est faite à la volée depuis le système Tails en cours d'utilisation. Ensuite, la mise à jour est beaucoup plus petite à télécharger qu'une image **.iso** complète. Pour finir, le mécanisme de mise à jour inclut une vérification cryptographique de la mise à jour. On n'a plus à vérifier l'authenticité du fichier **.iso** soi-même.

Voir: 3.4.1

Voici comment se passe une mise à jour automatique de Tails:

1. Démarre Tails depuis la clé USB que tu souhaites mettre à jour.

2. Dans Tails, il faut ensuite se connecter à Internet. Une fois que la connexion qui se fait via **Tor** est établie, un message disant: **Tor est prêt** apparaît dans le coin supérieur droit de l'écran. À partir de ce moment il faut attendre environ une minute, sans ouvrir aucun nouveau programme. Si une mise à jour est disponible, une fenêtre intitulée: **Upgrade available** s'ouvre alors et te propose de mettre à jour la clé USB. Si tu veux faire la mise à jour, clique sur **Mettre à jour maintenant**, et suis l'assistant à travers le processus de mise à jour.

3. Télécharger la mise à jour peut prendre du temps, de quelques minutes à plusieurs heures (suivant la rapidité de la connexion Internet). Il est recommandé de fermer toutes les applications ouvertes pendant la mise à jour.

4. La connexion réseau est désactivée après le téléchargement de la mise à jour. Une fois le processus terminé, il est nécessaire de redémarrer Tails pour activer la mise à jour. Si tu as plusieurs mises à jour de retard, chaque mise à jour sera installée l'une après l'autre. Par exemple, si tu as la version 1.3 de Tails installée et que la dernière version est la 1.3.2, alors la mise à jour vers la version 1.3.1 sera tout d'abord installée, puis après un redémarrage de Tails, ce sera ensuite au tour de la mise à jour vers la version 1.3.2 d'être installée.

3.4.4 Mettre à jour manuellement Tails sur une clé USB

Il n'est parfois pas possible de faire une mise à jour automatique de Tails sur sa clé USB comme décrit ci-dessus. Cela peut arriver dans diverses circonstances. Par exemple, lorsque la mise à jour automatique est impossible pour des raisons techniques (pas assez de mémoire vive disponible). Il peut aussi arriver que la mise à jour automatique soit interrompue en cours de

route et qu'on doive réparer, le système Tails à moitié installé. Il est aussi fréquent qu'on veuille mettre à jour depuis un autre périphérique Tails qui a déjà la dernière version installée, par exemple en travaillant hors connexion. Dans ces cas, on va se tourner vers une mise à jour manuelle du système Tails installé sur notre clé USB.
Tout comme lors de l'installation (duplication) sur clé USB, on a aussi besoin pour la mise à jour manuelle, de deux supports de mémoire. En effet, contrairement à la mise à jour automatique, le système en cours d'utilisation ne peut, dans ce cas, se mettre à jour lui-même à la volée. Il nous faut donc un système Tails sur clé USB ou DVD sur lequel on va démarrer, en plus de la clé USB contenant l'ancienne version de Tail que l'on va mettre à jour.

Voici comment mettre à jour Tails manuellement sur clé USB ou carte SD:

1. Démarre Tails depuis une clé USB ou un DVD (ne branche pas encore la clé USB sur laquelle tu veux mettre à jour Tails).

2. Soit mettre à jour la clé USB avec la dernière version de Tails trouvée sur Internet:

Voir: 3.4.1

   2.1. Dans Tails, télécharger et vérifier l'authenticité de la dernière version de Tails.

   2.2. Choisis **Applications ▷ Tails ▷ Programme d'installation de Tails** pour lancer le **Programme d'installation de Tails**.

   2.3. Choisis **Mettre à jour depuis une image ISO**.

   2.4. Branche la clé USB sur laquelle tu souhaites mettre à jour Tails. Un nouveau périphérique, qui correspond à la clé USB, apparaît alors dans le menu déroulant des **Périphériques Cibles**.

   2.5. Choisis la clé USB dans le menu déroulant des **Périphériques Cibles**.

   2.6. Clique sur le bouton **Parcourir** pour désigner l'emplacement du fichier **.iso** (préalablement enregistré). Enfin, pour démarrer la mise à jour, clique sur le bouton **Installer Tails**. Lis le message d'avertissement qui apparaît alors. Clique sur le bouton **Yes** pour confirmer et attends la fin de l'installation. Bravo c'est terminé !

3. Soit mettre à jour la clé USB avec la dernière version de Tails actuellement utilisée:

   3.1. Choisis **Applications ▷ Tails ▷ Programme d'installation de Tails** pour lancer le **Programme d'installation de Tails**.

   3.2. Choisis **Cloner et Mettre à jour**.

3.3. Branche la clé USB sur laquelle tu souhaites mettre à jour Tails. Un nouveau périphérique, qui correspond à la clé USB, apparaît alors dans le menu déroulant des **Périphériques Cibles**.

3.4. Choisis la clé USB dans le menu déroulant des **Périphériques Cibles**. Enfin, pour démarrer la mise à jour, clique sur le bouton **Installer Tails**. Lis le message d'avertissement qui apparaît alors. Clique sur le bouton **Yes** pour confirmer et attends la fin de l'installation. Bravo c'est terminé !

4 Effacer pour de vrai des mémoires numériques avec shred

4.1 Qu'est-ce que shred

Shred est un programme en ligne de commande disponible par défaut depuis le terminal[17] de nombreux systèmes d'exploitations de type Linux (dont Tails fait partie) et qui est utilisé pour effacer des données de manière suffisamment sûre pour qu'elles ne puissent être récupérées qu'au prix de grandes difficultés, si ce n'est pas du tout. Shred effectue la technique d'effacement évoquée précédemment qui consiste en de multiple réinscriptions de l'ensemble de la partition de mémoire[18] avec des données aléatoires et des motifs choisis pour maximiser la destruction des données résiduelles. Au fait, «to shred» en anglais veut dire déchiqueter, marrant non ?

Voir: 6.2.2

À ce stade, comme shred fait appel au terminal, une petite note concernant son utilisation est peut-être utile. En effet, si on ne s'est jamais servi du terminal on peut avoir l'impression d'un outil très complexe et élitiste. En fait, il faut savoir que derrière tous les boutons et menus des programmes employant une interface graphique (l'ensemble des logiciels d'usage courant, comme par exemple Open Office) se cache l'équivalent d'une commande de terminal adressée au système d'exploitation. Seulement voilà, certains programmes très utiles n'ont pas (encore ?) d'interface graphique, d'où l'intérêt de s'initier au b.a-ba du terminal. Donc, pas de souci, l'utilisation basique de cet outil est très simple: on ouvre le programme et au lieu de cliquer sur le bon bouton on y recopie la bonne commande, à la virgule et à l'espace près[19].

[17] Le terminal est un programme qui permet d'interagir avec le système d'exploitation en lançant d'autres programmes, les commandes, sous la forme de bouts de texte, entrés au clavier ou par copier/coller.

[18] Une partition est la subdivision de base de la mémoire pour les disques durs, les clés USB, les cartes SD, etc.

[19] Si on entre un espace de trop, ou une faute d'orthographe dans la commande elle ne fonctionnera pas. Donc concentration !

4.2 Limites de shred et parades

Au vu des difficultés que peut imposer l'effacement des données (surtout en ce qui concerne les mémoires flash (clés USB, cartes SD et mémoires SSD), l'effacement complet de la mémoire ne suffit pas. Pour des données sensibles, il est indispensable de l'associer au cryptage, sujet qui compose la matière des chapitres suivants.

Voir: 2.3
Voir: 5.1
Voir: 6.1

Et si on veut avoir la certitude que de données compromettantes stockées sur une clé USB de manière non-cryptée, ne puissent plus jamais être récupérées ? Dans le doute persistant face à l'effacement de ce genre de support, le mieux est peut-être de la détruire physiquement en la pulvérisant au marteau, non sans l'avoir soumise auparavant à l'action de shred.

4.3 Utiliser shred pour vraiment effacer une partition de mémoire

1. Identifier la partition de mémoire à effacer:

Voir: 3.3

   1.1. Démarrer l'ordinateur avec Tails. Dans l'écran de connexion au démarrage de la session Tails, répondre **Oui** à la question **Plus d'options ?** On va devoir choisir un mot de passe qui va nous permettre de disposer des droits d'administration, parfois nécessaires pour travailler sur certaines partitions.

   1.2. Dans Tails, ouvrir le programme **Utilitaire de disque** depuis le menu **Applications** ▷ **Accessoires** ▷ **Utilitaire de disque**.

   1.3. L'**Utilitaire de disque** liste tous les périphériques disponibles sur le côté gauche de l'écran. Branche le périphérique externe de mémoire (clé USB, carte SD ou disque dur externe) dont tu souhaites effacer une partition. Un nouveau périphérique devrait apparaître dans la liste. Sélectionne-le en cliquant dessus.

   1.4. Vérifie que la description du périphérique sur le côté droit de l'écran correspond à ton périphérique: sa marque, sa taille, etc.

   1.5. Clique sur la partition de mémoire que tu souhaites effacer (la ou les partitions sont représentées sous la forme d'une barre colorée en bleu ou en blanc sous l'intitulé **Volumes**). Tu peux maintenant identifier le nom de la partition après l'intitulé **Périphérique** à droite de l'écran. Le nom commence par **/dev/** suivi de trois lettres, les deux premières étant sd ou hd: par exemple, **/dev/sdd1**. Noter nom quelque part: il faudra l'écrire tout à l'heure dans la commande à la place de [**LE_NOM**]. Attention, à ce stade il faut bien s'assurer que l'on note le nom de la bonne partition, car l'issue de cette manœuvre aboutit à la perte irrémédiable des données.

2. Effacer la partition de mémoire dans le **Terminal** avec **shred**:

   2.1. Toujours dans Tails, ouvrir le programme **Terminal** depuis le menu **Applications** ▷ **Accessoires** ▷ **Terminal**.

   2.2. Un écran blanc apparaît avec l'invite de commande:

```
amnesia@amnesia:~$
```

   À la suite de ça, entrer la commande **shred** avec les droits d'administration **sudo**:

```
sudo shred -n7 -v [LE_NOM]
```

   Veiller à remplacer [**LE_NOM**] par le nom de la partition à effacer déterminé précédemment. Attention de bien respecter les espaces dans le texte.

   Au final ça doit donner quelque chose comme ça:

```
shred -n7 -v /dev/sdd1
```

   Le nombre situé dans la commande après le **-n** correspond au nombre de réinscriptions qui vont être effectuées, dans ce cas 7 réinscriptions. Plus il y a de passages, plus sûr sera l'effacement mais il faut savoir que suivant la taille de la partition et le nombre de passages, cette procédure peut prendre beaucoup de temps (plusieurs jours pour des gros disques durs !).
   Le nombre 7 est donné ici comme un compromis entre rapidité et efficacité. Pour changer le nombre de passages il faut remplacer **-n7** par **-n25** dans la ligne de commande si on veut par exemple 25 réinscriptions.

   2.3. Après vérification de la commande, appuie sur la touche **Entrée** du clavier. Le **Terminal** nous renvoie un message qui demande le mot de passe administrateur choisi à l'étape 1.1 de cette marche à suivre:

```
[sudo] password for amnesia:
```

   Écris ton mot de passe (il n'apparaît pas à l'écran c'est normal) et appuie sur la touche **Entrée** du clavier.

   2.4. La commande **shred** va alors détailler dans le **Terminal** ce qu'elle fait et à quel stade en est l'effacement (ainsi qu'on lui a demandé

de le faire en ajoutant à la commande **shred** l'option **-v**, qui signifie, dans le cadre de cette commande, que l'ordinateur doit être «verbeux», c'est-à-dire «bavard»). Ça donne quelque chose comme:

```
shred:  /dev/sdd1:  passe 1/7 (random)...
shred:  /dev/sdd1:  passe 2/7 (333333)...
shred:  /dev/sdd1:  passe 3/7 (492492)...
shred:  /dev/sdd1:  passe 4/7 (000000)...
```

À la fin de la procédure, le **Terminal** affiche à nouveau l'invite de commande vue à l'étape 2.2 de cette marche à suivre. Tu peux alors fermer le **Terminal**.

3. Cette procédure peut être répétée quasiment à l'infini, sans risque pour le support de mémoire. Cependant, avant d'être réutilisée pour stocker des données, la partition doit être repartitionnée.

Voir: 6.4
Voir: 6.5

5 Brouiller ses traces grâce au cryptage

5.1 Qu'est-ce que le cryptage

Le cryptage aussi appelé chiffrement, recouvre trois aspects importants:

- Premièrement, c'est le procédé grâce auquel on rend une donnée (texte, image, e-mail etc.) confidentielle. C'est-à-dire, impossible à comprendre pour toute personne qui n'est pas dans le secret, parce qu'elle n'a pas la clé de déchiffrement.
- La deuxième propriété issue du cryptage est le fait d'assurer l'intégrité d'une information. C'est-à-dire, rendre impossible sa modification par toute personne n'ayant pas la clé de déchiffrement.
- Finalement, par le biais du principe de signature qui sera détaillé par la suite, le cryptage permet la vérification de l'authenticité d'une donnée ou d'un message.

5.2 Précisions théoriques sur le cryptage

Les précisions données dans ce point ne sont de loin pas nécessaires à l'utilisation du cryptage, elles pourront intéresser les personnes qui voudraient mieux cerner certaines limites de cette technique ou qui sont attirées par un peu de maths[20]. Si c'est pas ton cas, tu peux directement passer au point suivant.

[20]Pour plus d'infos: [https://fr.wikipedia.org/wiki/Chiffrement_RSA].

Les bases mathématiques permettant le cryptage sont les mêmes pour les trois programmes présentés dans ce manuel. La force de cette méthode de cryptage se base sur la grande difficulté mathématique (à l'heure actuelle) de factoriser des nombres entiers en produit de facteurs (nombres) premiers[21].
De manière plus claire, il est relativement facile pour un ordinateur de fabriquer deux grands nombres premiers p et q aléatoires et de les faire correspondre à une clé secrète de cryptage. Ensuite, le cryptage en lui même repose sur le résultat du produit (multiplication) p x q de ces deux nombres premiers qui donne un nombre entier n = p x q.
Pour le décryptage, il n'existe par contre aucune méthode mathématique directe, facile et rapide pour retrouver les facteurs p et q correspondant à la clé secrète à partir du résultat du cryptage: n (qui répétons le est le produit des facteurs p et q).
Il est d'importance vitale pour la solidité de la clé qu'elle soit générée en utilisant des nombres premiers (pseudo)aléatoires[22] (c'est-à-dire sans corrélation entre nombres successifs). Le contraire pourrait créer dans les données cryptées une logique détectable qui permettrait à l'adversaire de deviner p et q de manière beaucoup plus simple qu'en devant essayer toutes les possibilités pour p et q.

En 2015, le seul moyen pour tenter de décrypter mathématiquement des données chiffrées de la sorte est d'utiliser de puissants ordinateurs essayant consécutivement l'ensemble des combinaisons possibles pour la clé. Avec la puissance de calcul limitée des ordinateurs actuels, ça n'est pratiquement pas imaginable[23] d'espérer y arriver rapidement...
La difficulté technique de casser le cryptage PGP est discutée lors d'un procès aux USA[24]:
"Steven Russel, expert à la police de Portland fut prié d'expliquer ce qu'il signifiait en disant qu'il n'était pas «calculatoirement faisable» de casser le code. «Cela signifie qu'au vu de la technologie et des ordinateurs actuels, vous ne pouvez pas mettre ensemble suffisamment d'ordinateurs pour espérer

[21] Un nombre premier n'est divisible que par deux nombres entiers; il est n'est divisible que par 1 et par lui même. Par exemple 3 est un nombre premier.
[22] Pour plus d'infos: [https://freedom-to-tinker.com/blog/nadiah/new-research-theres-no-need-panic-over-factorable-keys-just-mind-your-ps-and-qs/].
[23] À moins d'arriver à obtenir la clé par des moyens de surveillance ou de contrainte ! Ce qui constitue la principale faille du cryptage, que l'on va donc approfondir au point suivant. Pour plus d'infos: [https://web.archive.org/web/20121014210015/http://www.pcworld.com/article/110841/article.html] et [htt ps://fr.wikipedia.org/wiki/Cryptographie_symétrique].
[24] Ce procès se passe en 1999, mais la difficulté du décryptage est encore plus grande aujourd'hui. Pour plus d'infos: [https://web.archive.org/web/20121014210015/http://www.pcworld.com/article/110841/article.html].

décrypter un message de ce type en une durée de temps raisonnable», dit-il à la cour. Il fut demandé à Russel s'il parlait de quelques années ou plus. «Nous parlons de millions d'années», répondit-il."

5.3 Limites du cryptage et parades

C'est un fait, le problème mathématique à la base des méthodes de cryptage actuelles est étudié depuis l'antiquité sans qu'aucune solution simple n'y ait été apportée. Il en découle que les meilleures techniques de cryptage sont hors de portée des meilleures techniques de décryptage. Pourtant tout pourrait changer. En effet, on ne peut pas exclure qu'un jour le problème mathématique soit résolu simplement ou que la puissance de calcul des ordinateurs devienne suffisante pour que des données cryptées présentement indéchiffrables le deviennent en un temps raisonnable.

Donc, étant donnée la grande facilité d'accès à des systèmes de cryptages d'une très haute solidité, des sbires du pouvoir ayant l'intention de décrypter des données espionnées vont probablement utiliser des méthodes beaucoup plus simples que le décryptage traditionnel. Les deux principaux axes empruntés pour tenter de contourner les systèmes de cryptage plutôt que de les attaquer directement sont: d'une part la surveillance (essayer d'intercepter les phrases et clés de passe) et d'autre part les mesures de contraintes (juridiques et/ou physiques):

- Pour ce qui est de la surveillance, les moyens mis en œuvre sont principalement de type informatique, avec des logiciels espions utilisés par les flics pour infecter un système d'exploitation ciblé. Ces chevaux de Troie (troyens) et enregistreurs de frappe permettent alors, au minimum, de capturer les clés de cryptage et les phrases de passe, mais une «perquisition en ligne» de l'ensemble de l'ordinateur est techniquement possible. La surveillance et la répression doivent s'adapter afin de ne pas être mises en échec par l'utilisation de nouvelles technologies comme le cryptage. C'est ce qui arrive aux USA au début des années 2000 et, en 2015, l'utilisation de ce genre de surveillance est de plus en plus homogène pour l'ensemble des pays riches, qui ont les moyens de se donner les moyens. Au début, ces pratiques policières étaient assez obscures et exceptionnelles, maintenant elles sont instituées par des lois dans de nombreuses juridictions comme en France (LOPPSI 2, 2012), en Suisse (LSCPT, SWS 2013) ou par des directives de police (notamment émises par Interpol).

Voir: 3.2.2
Voir: 12
Voir: 3.2.2

- Au sujet des contraintes légales visant à obtenir des personnes leur phrase de passe et clé de cryptage, la situation est plus contrastée selon

Voir: 5.4

les pays. En Angleterre, Belgique, France, Italie, USA et bien d'autres, des lois ou des jurisprudences peuvent exposer les personnes refusant de livrer leur secret à des amendes ou des peines de prison. De plus, l'utilisation du cryptage peut être considérée par certaines juridictions comme une circonstance aggravante. D'autre pays comme la Grèce, le Kenya, le Kirghizstan, la Suisse ou l'Uruguay ne disposent pas du tout de ce genre mesures de contraintes légales[25]. On peut encore noter que même en l'absence de lois répressives dans ce domaine, dans pas mal d'endroits du monde, le recours à des contraintes physiques[26] (torture ou d'autres types de menaces) est tout a fait envisageable pour faire cracher la phrase de passe.

Pour conclure, quelles que soient les juridictions ou les pratiques répressives qui nous sont imposées il est assez clair que ces types d'attaques représentent une menace bien plus grande à la sécurité du cryptage que les attaques mathématiques.

Maintenant, on peut envisager des stratégies de défense face à ces voies détournées d'attaquer le cryptage. Voici quelques idées:

- De manière générale, certaines pratiques de base peuvent permettre d'éviter l'impasse, même dans des cas de surveillance et de répression avancées. On peut tout d'abord rappeler ici qu'il est fondamental d'utiliser ses mémoires et communications cryptées uniquement sur des systèmes d'exploitation amnésiques et anonymes comme Tails, sous peine de vraiment laisser traîner ses petits secrets partout, jusqu'aux oreilles les plus indiscrètes.
  Ensuite, malgré l'utilisation du cryptage pour stocker des informations ou communiquer, il est important de restreindre les informations au strict minimum. Par exemple, on peut imaginer communiquer voire s'organiser à distance par des e-mails cryptés sans pour autant y inclure des informations comportant des noms, des lieux, des dates ou trop de détails.
  Une troisième pratique prudente consiste à effacer consciencieusement des documents ou des messages une fois qu'on n'en a plus l'usage, c'est-à-dire régulièrement. Un fichier qui n'existe plus ne peut être déchiffré !
  Finalement, il s'agit d'utiliser ses phrases de passe et clés de cryptages de manière réfléchie.

Voir: 4.1

[25] Pour plus d'infos, un excellent site web recense les lois relatives à la cryptographie suivant les pays: [http://www.cryptolaw.org/], quelques cas précis de répression sont donnés ici: [https://en.wikipedia.org/wiki/Pretty_Good_Privacy#Criminal_investigation].

[26] Pour plus d'infos: [https://en.wikipedia.org/wiki/Rubber-hose_cryptanalysis].

- Pour ce qui est spécifiquement des parades à la surveillance informatique, il faut se référer aux stratégies pour limiter les risques d'infection de logiciels malveillants, qui ont été détaillées précédemment et à l'usage du clavier virtuel qui sera vu à la fin de ce chapitre.

Voir: 3.2.2

Voir: 5.6

- Pour ce qui est des contraintes légales, on peut réfléchir à un panel de tactiques de défense à adapter selon chaque cas, juridiction et jurisprudence. Tout d'abord, il est intéressant d'introduire le concept de «déniabilité»[27] (deniability ou repudiability en anglais). En effet, suivant le contexte il est plus ou moins facile de dénier (refuser de reconnaître) son implication dans un fait dont on nous accuse. Dans ce cas, d'être à l'origine du cryptage ou que le cryptage existe tout court. Par exemple, il est toujours plus aisé de dénier être à l'origine de données cryptées planquées dans un espace collectif ou dans des e-mails anonymes que si elles étaient retrouvées dans sa chambre ou sur un compte e-mail personnalisé.
  Mais parfois, cette option tombe à l'eau devant l'intime conviction d'un juge l'amenant à faire endosser à quelqu'un-e la responsabilité de données cryptées. Il reste alors encore possible de prétendre que l'on a oublié la phrase de passe ou donner un faux code et ne pas comprendre pourquoi ça ne marche pas. Finalement, même dos au mur, le cryptage libère encore une marge de manœuvre:
  " Si la preuve que j'avais préparé quelque chose de lourdement punissable se trouvait dans un message que la justice m'ordonnerait de déchiffrer, il est probable que je préfère payer une lourde amende pour avoir refusé de donner la clé, que de passer une grande partie de ma vie en taule pour avoir préparé ce quelque chose[28]*."*

5.4 Principaux types de cryptages

5.4.1 Cryptage symétrique

La cryptage symétrique, également dit «à clé secrète» (par opposition à la cryptographie à clé publique), est la plus ancienne forme de chiffrement.
Le cryptage est dit symétrique quand il utilise la même clé pour chiffrer et déchiffrer. Une clé est la donnée qui, au travers d'un calcul, permet de chiffrer et de déchiffrer un message.

[27] La déniabilité est utilisée ici dans un sens assez large, pour plus d'infos: [www.cypherpunks.ca/otr/otr-wpes.pdf] et [https://en.wikipedia.org/wiki/Deniable_encryption].

[28] Extrait modifié de la deuxième séance du Cycle d'Ateliers Internet et Vie Privée: [https://caivp.poivron.org/].

C'est le mode de cryptage employé pour crypter des mémoires (avec LUKS), et il est aussi utilisé pour crypter des connexions Internet (avec Tor) et des e-mails confidentiels (avec PGP).

Voir: 6.1
Voir: 10.1
Voir: 7.2

5.4.2 Cryptage asymétrique

Le cryptage asymétrique, ou à clé publique, est une méthode de chiffrement qui est passablement différente du cryptage symétrique. Le cryptage est dit asymétrique quand chaque personne utilise deux clés différentes, en fait une paire de clés complémentaires composée:

- D'une clé publique (qui est diffusée publiquement).
- D'une clé privée (qui est gardée secrète).

La première permettant de coder le message et l'autre de le décoder. Ainsi, l'expéditeur-trice peut utiliser la clé publique d'un-e destinataire pour coder un message que seul-e ce-tte destinataire (en possession de la clé privée) pourra décoder, garantissant la confidentialité du contenu.
Ce mode de cryptage est utilisé pour crypter des connexions Internet (avec Tor), pour authentifier des fichiers téléchargés (téléchargement de Tails) et c'est le plus utilisé pour crypter des e-mails confidentiels (avec PGP) ou bien des messages instantanés confidentiels (avec OTR).

Voir: 3.4.1
Voir: 7.3
Voir: 8.1

L'utilisation d'un système symétrique ou asymétrique dépend des tâches à accomplir. La cryptographie asymétrique présente deux intérêts majeurs. Premièrement, l'utilisation d'une clef publique permet l'échange de messages confidentiels entre deux personnes sans devoir mettre en place au préalable une rencontre physique entre elles, ni un canal de transmission protégé, pour échanger une phrase de passe secrète. De plus, cette technique permet de limiter le nombre de phrases de passe à mémoriser, contrairement à ce qui prévaut pour le cryptage symétriques où, pour espérer la confidentialité, il faut inventer une nouvelle phrase de passe pour chaque personne avec qui on correspond. Enfin, elle permet la signature électronique.

Voir: 5.4.3

Pour mieux comprendre la logique du cryptage asymétrique (par exemple pour des e-mails) on peut s'aider d'une image.
Disons que que je veuille faire passer des messages confidentiels, mais qu'il m'est parfaitement impossible de les remettre en main propre à la personne destinataire. Comment donc les laisser quelque part, dans un lieu public (comme peut l'être le cyberespace), sans risquer que l'info soit interceptée par quelqu'un-e de mal-intentionné-e ?
On pourrait donc imaginer que l'on dispose de petits coffrets blindés très solides (aussi solides que le cryptage PGP) et comportant deux digicodes

différents. Le premier permet à mes ami-e-s d'entrer le code public que je leur ai confié afin d'ouvrir une fente dans le coffret pour y glisser des lettres à mon intention. Ce code est l'équivalent de la clé PGP publique dont je peux donner un exemplaire à quiconque souhaite m'envoyer des messages secrets. L'autre digicode permet d'entrer un code privé que je suis seul-e à posséder et avec lequel je peux ouvrir le coffret pour consulter mon courrier confidentiel. C'est l'équivalent de la clé PGP privée.
Enfin, il est important de se rappeler qu'à chaque clé privée personnelle correspond une clé publique car c'est à la base de ce qui fait la particularité de ces coffrets. Lorsque on y utilise le digicode d'un côté avec un code public, seul le code privé correspondant permettra la réouverture de la boîte !
Reprenons notre exemple: j'aimerais communiquer avec ma pote E.T. et nos contraintes spatiotemporelles font que nous ne nous croisons jamais... J'ai confié à E.T. mon code public et j'ai mon code privé avec moi et E.T., de son côté a fait exactement la même chose. De plus, nous possédons tou-te-s les deux quelques exemplaires de ces coffrets solides dans lesquels on se passe nos messages, si bien qu'on a toujours avec nous: notre propre code privé, le code public de l'autre et au moins un petit coffret.
Si je désire envoyer un message secret à E.T., je prend un coffret, y place le message par la fente à l'aide de son code public et je vais mettre le petit objet dans un endroit qu'E.T visite habituellement. Par exemple, sa boîte aux lettres (équivalent à sa boite mail). Je repars tranquille et serein-e en sachant que seule la détentrice du bon code privé permettant d'accéder à l'autre serrure, E.T en l'occurrence, sera en mesure de rouvrir le coffret.
Plus tard, E.T. trouvera le coffret secret disposé à son intention, et n'aura qu'à dégainer son code privé pour savoir ce que je voulais lui dire. Lorsqu'à mon tour je trouverai dans ma boîte aux lettres un message laissé par E.T, je n'aurai qu'à le lire avec mon propre code privé...

Avant de passer à la suite, on peut encore clarifier une chose. Un échange d'e-mails cryptés de manière asymétrique nécessite que les deux protagonistes se soient auparavant échangés leur clé publique, par un échange d'e-mails non-cryptés par exemple. De telles copies de sa propre clé publique peuvent être mises à la disposition de toute personne dont on souhaite recevoir des e-mails cryptés, tandis que la clé privée, dont dérive la clé publique, n'existe elle qu'à un seul exemplaire.

5.4.3 Signature

Inversement au cryptage asymétrique, l'expéditeur-trice peut utiliser sa propre clé privée pour signer (crypter) un message, signature qu'un-e destinataire pourra vérifier (décrypter) avec la clé publique qu'on lui a confié.

C'est le mécanisme utilisé par la signature numérique[29] pour authentifier l'auteur-e d'un message. En effet, seule la personne connaissant la clé privée est en mesure de signer.
Donc, contrairement à ce que son nom peut laisser penser, une signature numérique est bien plus que le pendant numérique de la signature manuscrite. En effet, la signature numérique est fonction de l'expéditeur et du contenu du message. Une signature témoigne donc simultanément de l'authenticité de l'origine d'un message et de son intégrité. Concrètement, si elle est systématiquement employée entre deux correspondant-e-s cela permet par exemple, d'éviter que des flics qui auraient piraté la boîte mail de l'un-e, puissent envoyer des e-mails crédibles à l'autre.

De plus, on peut encore ajouter que comme les autres formes de cryptage, la signature numérique peut aussi être appliquée à toutes sortes de fichiers et pas uniquement à des messages de texte. C'est cette propriété qui est notamment utilisée, pour authentifier que les versions de Tails téléchargeables sur Internet, proviennent bien de l'équipe de développement de Tails et, pas de n'importe quel imposteur.

Voir: 3.4.1
Voir: 3.4.3

Malheureusement, l'usage de la signature numérique amène un inconvénient, qui est la non-déniabilité (le contraire du concept de déniabilité vu auparavant). En effet, quand on signe un message ou un document avec sa clé privée, il va être beaucoup plus difficile de nier en être l'auteur-e ultérieurement. C'est bien d'avoir ça à l'esprit avant d'y avoir recours.

Voir: 5.3

5.5 Le bon mot de passe est une phrase de passe

À ce stade, attention à bien faire la distinction entre phrase de passe et clef de cryptage !
Comme on l'a vu avant, la clé de cryptage, générée par l'ordinateur, est ce qui sert à crypter/décrypter nos données. Comme elle est trop longue et complexe pour pouvoir être gardée en tête, de nombreux types de cryptage la font dériver d'une phrase de passe. Tout ça peut paraître compliqué, mais pas tant que ça une fois qu'on a compris à quoi sert une phrase de passe.

La phrase de passe, choisie par nous, est ce qui permet à l'ordinateur d'accéder à la clé de cryptage proprement dite. Suivant les méthodes, cet accès se fait via une fonction mathématique ou même en décryptant la clé de cryptage. Eh oui, les clés de cryptages sont elles-même souvent cryptées ! Ainsi même si la phrase de passe ne sert pas directement à crypter nos données, elle est quand même, pour nous, le secret qui les protège indirectement, et qui est

[29] Pour plus d'infos: [le chapitre 6.3 du tome 2 du Guide d'autodéfense numérique].

beaucoup plus facile à mémoriser. En résumé, la confidentialité des données repose sur une clé secrète, qui elle même repose sur une phrase secrète.
De plus, dans le cas notamment du cryptage asymétrique, elle permet une deuxième sécurité. En effet, un flic mettant la main sur notre clé privée ne pourra pas faire grand chose sans la phrase de passe, et inversement.

Qu'est-ce qui fait une bonne phrase de passe[30]:

- Longueur:
  Tout d'abord, une phrase de passe doit comporter au moins 10 mots (50 à 60 caractères, espaces compris). Elle est beaucoup plus résistante qu'un mot de passe même très compliqué de 9 signes (par exemple: Zx0p%Xn§3). Au vu des techniques actuelles, un mot de passe de 5 caractères peut être décrypté en quelques minutes[31], tandis qu'une phrase de passe demande un temps supérieur à des centaines d'années (si elle est bien faite).

- Mémorisation:
  Deuxièmement, une phrase de passe doit être facile à garder en mémoire. Ça évite de devoir conserver une trace écrite en clair (c'est-à-dire non cryptée) quelque part, pratique qui peut gravement remettre en question toute la démarche de confidentialité. Un bon truc consiste à choisir un passage de chanson, un vers de poésie ou une phrase de roman qu'on a déjà en tête. Un exemple de phrase:
  «Suffit d'abattre Etat et Capital ? Ça n'est pas ma révolution !»

- Non Lisibilité:
  Troisièmement, la phrase de passe ne doit pas être facilement lisible, que ce soit par dessus notre épaule quand on la tape ou avec un logiciel qui essaie de casser le mot de passe en utilisant prioritairement les mots du dico[32]. C'est pourquoi les substitutions de caractères et/ou les fautes d'orthographes renforcent considérablement la phrase de passe. On peut aussi y inclure des espaces supplémentaires et/ou en exclure d'autres, afin d'augmenter encore sa robustesse.
  «5uffi dabattr3 3tat 3tQapital ? Ca n3st pa5 mar3voluttyoN !»

[30] Pour plus d'infos: [http://www.cryptup.com/fr/help/html/password_vs_passphrase.htm], [https://en.wikipedia.org/wiki/Password_strength] et [p. 91 du tome 1 du Guide d'autodéfense numérique].
[31] Pour plus d'infos: [https://www.auscert.org.au/render.html?it=2260].
[32] Ça s'appelle une «attaque par dictionnire». Pour plus d'infos: [https://fr.wikipedia.org/wiki/Attaque_par_dictionnaire].

- Caractères spéciaux:
  Enfin, mélanger majuscules, minuscules et inclure des caractères spéciaux (§=+:¨*#!?$ etc.), est essentiel. Ceci parce que ça fait exploser le nombre de combinaisons possible à partir du jeu de caractères disponible sur un clavier. Il est peut-être quand même judicieux d'éviter certains caractères accentués qui n'existent pas sur tous les types de claviers.
  «+5uff: dabattr3 3tat 3tQap:taL ? Ca n3st pa5 mar3voluttyoN !+»

Encore quelques conseils concernant un usage prudent des phrases de passe et clés de cryptage[33].
Tout d'abord, il n'est pas très prudent d'utiliser toujours la même clé et phrase de passe pour des applications très différentes. Si l'une d'elles était un jour compromise, toutes les autres le seraient aussi ! Au contraire, c'est mieux de compartimenter, ce qui nous donne au minimum: une clé pour les e-mails cryptés, une autre pour les mémoires cryptées.
De plus, il ne faut jamais reprendre ses phrases de passe pour des utilisations non sécurisées.
Enfin, le fait de changer fréquemment les phrases de passe et clés de cryptage permet de limiter les dégâts si le cryptage venait à être percé (par n'importe quel moyen). Mais, que veut dire fréquemment ? Comme c'est une pratique assez contraignante, sa fréquence peut être déterminée par des moments où on a l'impression d'avoir fait les choses moins prudemment ou d'avoir pris des risques (par exemple avoir ouvert un fichier-joint bizarre). C'est assez vague et subjectif, mais voilà, c'est à chacun-e de voir.

5.6 Le clavier virtuel pour taper des phrases de passe de manière sûre sur un ordinateur qui ne l'est pas

Si un-e attaquant-e a accès physiquement à l'ordinateur sur lequel on utilise Tails, il ou elle peut y avoir installé un matériel malveillant qui enregistre chaque touche du clavier que l'on frappe. Il s'agit d'un enregistreur de frappe matériel (keylogger). Ce type de matériel est assez commun, et connu pour avoir déjà été utilisé, par exemple sur des ordinateurs publics dans des bibliothèques.
Voir:12.1.2
Quand on ne peut exclure la présence d'un keylogger matériel et pour éviter d'offrir à ce type de mouchards une phrase de passe servant au cryptage, on peut vouloir les «taper» en utilisant la souris, sur un clavier virtuel affiché à l'écran. Le **Clavier virtuel Florence** démarre automatiquement avec Tails et est accessible via l'icône d'un clavier dans la barre d'icônes en haut à droite de l'écran.

[33]Pour plus d'infos: [http://www.bugbrother.com/security.tao.ca/pswdhygn.html].

6 Crypter des mémoires numériques avec LUKS

6.1 Qu'est-ce que LUKS

LUKS (Linux Unified Key Setup) est une méthode standard de cryptage et de décryptage de partition de mémoire, qui est utilisée par de nombreux programmes fonctionnant avec des systèmes d'exploitation de type Linux (dont le système Tails fait partie).

Voir: 6.2.2

Le moyen le plus simple de transporter et de stocker des documents que tu souhaites utiliser avec Tails et d'être sûr-e qu'ils n'ont pas été consultés ou modifiés, est de les conserver sur un support de mémoire crypté amovible: une partition dédiée sur une clé USB, une carte SD ou un disque dur externe. Les deux outils de Tails présentés dans ce chapitre, que sont l'option de Stockage persistant ou le programme Utilitaire de disque, utilisent tout deux le cryptage LUKS et permettent de faire cela.

Notons encore que les mémoires cryptées que l'on va apprendre à créer ici ne seront ouvrables que dans des systèmes d'exploitation Linux (comme Tails ou Ubuntu par exemple).

6.2 Préparer le cryptage d'un support de mémoire

6.2.1 Effacement de la mémoire

Avant de crypter un support de mémoire, vierge ou ayant déjà servi à stocker des données, il est très important de l'effacer en le remplissant de données aléatoires. En effet, cela permet de cacher l'endroit où on va stocker nos propres données cryptées, et rend donc toute tentative de déchiffrement beaucoup plus ardue.

Voir: 4.1

Pour faire cela, on a vu précédemment la commande shred qui permet l'effacement sécurisé de toutes sortes de mémoires.

6.2.2 Partitionnement de la mémoire

Une partition est la subdivision de base de l'espace de stockage des mémoires numériques. Une mémoire numérique de stockage peut contenir plusieurs partitions et il existe différents formats de partitionnement qui vont déterminer la manière d'organiser les fichiers dans la mémoire. Le partitionnement est donc le fractionnement d'une mémoire numérique réelle (matérielle) en plusieurs espaces de mémoire virtuels indépendants, qui seront reconnus par l'ordinateur comme des supports de mémoire distincts. C'est-à-dire que, si par exemple on branche une clé USB divisée en deux partitions, l'ordinateur va reconnaître l'équivalent de deux clés USB ! C'est bien pratique car une seule clé USB va nous permettre de faire deux choses très distinctes sur chacune de ses partitions ! Comme par exemple, supporter le système Tails sur

la première partition et une mémoire cryptée sur l'autre. On pourrait aussi imaginer, une première partition avec un espace de mémoire cryptée pour du stockage sur le long terme (archivage) et une deuxième partition comportant un espace crypté de stockage à court terme, pour des données que l'on souhaite effacer régulièrement.

Voir: 6.3

Attention, en travaillant sur des partitions de mémoire il est très facile de perdre des données. Il suffit d'une fausse manipulation qui prend trois secondes ! C'est pas mal de bien regarder à deux fois ce qu'on fait et une petite sauvegarde des données importantes ne fait jamais de mal (à condition qu'elle soit faite sur un autre support crypté).

6.3 Utiliser le Stockage persistant qui intègre une partition cryptée dans Tails afin de stocker des données sensibles

Le Stockage persistant est une partition cryptée, protégée par une phrase de passe et qui est spécifiquement conçue pour être intégrée dans Tails. Avoir recours au Stockage persistant crypté conjointement à Tails, est probablement la manière la plus pratique qui soit d'utiliser ce système d'exploitation au meilleur de ses possibilités. En effet, le fait qu'il soit proposé automatiquement, d'activer, ou non, le volume persistant à chaque démarrage de Tails, permet un accès très facile à ses documents cryptés. De plus, cette méthode permet de garder en mémoire de manière confidentielle des données bien plus variées que les seuls documents de travail. Ainsi, on peut par exemple décider de sauvegarder la configuration de certains logiciels, ou d'avoir ses clés de cryptage toujours importées et prêtes à servir. Pour finir, le dernier avantage notable dans l'emploi du Stockage persistant crypté, est d'avoir le système Tails et ses données cryptées qui tiennent sur une seule et même clé USB ! Voyons maintenant comment installer et utiliser le Stockage persistant crypté de Tails:

1. Créer le **Stockage persistant**:

    1.1. Démarrer Tails à partir d'une clé USB ou d'une carte SD, sur laquelle on veut aussi installer le **Stockage persistant**. À noter qu'il est ici techniquement nécessaire que le support de mémoire sur lequel on utilise Tails, ait suffisamment de mémoire totale, c'est-à-dire au minimum 4 gigas et que Tails y ait été installé via le **Programme d'installation de Tails**.

    Voir: 3.4.2

    1.2. Dans Tails, lancer l'assistant de persistance depuis le menu **Applications ▷ Tails ▷ Configurer le stockage persistant**. Comme l'assistant est lancé pour la première fois, il propose de créer un nouveau volume persistant sur le périphérique USB depuis lequel

on utilise Tails. Il faut à ce stade choisir et inscrire, dans les zones de texte: **Phrase de passe** et **Vérification de la phrase de passe**, une phrase de passe qui va protéger la future partition cryptée du **Stockage persistant**. Ensuite, cliquer sur le bouton **Création**. L'opération de création peut durer de quelques secondes à quelques minutes, durant lesquelles il faut patienter, en prenant garde à pas fermer la fenêtre **Configurer le stockage persistant** ou à ne pas débrancher la clé USB.

Voir: 5.5

1.3. Une fois que c'est fait, la nouvelle fenêtre qui apparaît, présente une liste d'options qu'il est possible de sélectionner, par un clic de souris. Chacune des options sélectionnées correspond à un ensemble de fichiers qui seront sauvegardés sur le volume persistant. L'option: **Données personnelles** est sélectionnée par défaut. Pour en savoir plus sur l'utilité de cocher ou pas différentes options il faut se référer à la documentation[34] de Tails, sans oublier que certaines options posent des enjeux de sécurité.

1.4. Quand on est satisfait-e du choix des options, il s'agit maintenant de cliquer sur le bouton: **Sauvegarder**. La nouvelle fenêtre qui apparaît nous indique: **Assistant de persistance - Terminé**. Les modifications effectuées ne seront effectives qu'après un redémarrage du système. Il sera toujours possible de revenir, par la suite, modifier ces options. Cela se fera toujours via le menu **Applications ▷ Tails ▷ Configurer le stockage persistant**.

2. Activer et utiliser le **Stockage persistant**:

2.1. À partir de là, à chaque démarrage de Tails sur cette clé USB, on va avoir le choix d'activer le **Stockage persistant** et donc de pouvoir y lire et y inscrire des données. Dans l'écran de connexion intitulé: **Welcome to Tails**, une boîte de dialogue demande: **Activer la persistence ?**. Choisir **Oui**, pour activer le volume persistant pour la présente session de travail. Taper ensuite, dans la boîte de texte: **Phrase de passe**, la phrase de passe choisie au point 1.2 de cette marche à suivre, pour décrypter le **Stockage persistant**.

Voir: 3.3

2.2. Dans une session de Tails pour laquelle on a activé la persistance, les fichiers personnels et les documents de travail sont stockés dans le dossier **Persistent** (écrit à l'anglaise), accessible via le menu **Raccourcis ▷ Persistent**.

[34] Pour plus d'infos: [https://tails.boum.org/doc/first_steps/persistence/configure/index.fr.html] et [https://tails.boum.org/doc/first_steps/persistence/warnings/index.fr.html].

2.3. Dans certains cas, on peut vouloir décrypter le **Stockage persistant** même si ça n'a pas été fait au démarrage. Par exemple si Tails est lancé depuis un autre support que celui contenant le **Stockage persistant**, disons depuis un DVD. Pour faire ça, ouvrir le programme **Utilitaire de Disque** depuis le menu **Applications ▷ Accessoires ▷ Utilitaire de disque**. La fenêtre qui s'ouvre présente sur sa colonne de gauche, la liste de tous les périphériques disponibles. Branche la clé USB ou la carte SD sur laquelle se trouve le **Stockage Persistant**. Un nouveau périphérique devrait apparaître dans la liste, sélectionne-le en cliquant dessus. Ensuite, sur le schéma des partitions au milieu de l'écran, il faut sélectionner avec la souris, la partition cryptée du **Stockage persistant**. C'est la partition appelée **Chiffré** qui se trouve juste après celle appelée **Tails**. Une fois que c'est fait, il faut cliquer sur la petite icône représentant un cadenas et intitulée: **Déverrouiller le volume**. Là, une fenêtre s'ouvre où il est demandé de saisir la phrase de passe. Un fois que la bonne phrase de passe est donnée, il faut encore sélectionner avec la souris la partition intitulée: **TailsData** qui vient d'apparaître en dessous de la partition **Chiffré**, puis cliquer sur la petite icône intitulée **Monter le volume**. La partition décryptée est maintenant disponible sous l'intitulé **TailsData**, dans la colonne de gauche du menu **Raccourcis ▷ Dossier personnel**.

6.4 Utiliser l'Utilitaire de disque pour créer une partition cryptée afin de stocker des données sensibles

Il y a des situations, où on aimerait stocker des données de manière cryptée plus simplement et plus rapidement que ce que fait le Stockage persistant, de manière très ergonomique, mais parfois inutilement perfectionnée. Par exemple, quand on voudrait juste transmettre à une pote des données sensibles sur une clé USB, indépendamment de Tails. Ou bien quand on veut stocker sur une partition cryptée de petite taille, et donc rapide à effacer, des données très sensibles, dont on veut faire disparaître les traces à court terme. L'Utilitaire de disque est alors l'outil qu'il nous faut ! Voici comment l'utiliser:

Voir: 6.3

Voir: 4

1. Dans Tails, ouvrir le programme **Utilitaire de Disque** depuis le menu **Applications ▷ Accessoires ▷ Utilitaire de disque**.

2. Identifier le périphérique de stockage:
   L'**Utilitaire de disque** liste tous les périphériques disponibles sur le côté gauche de l'écran: branche le périphérique de stockage que tu

souhaites utiliser. Un nouveau périphérique devrait apparaître dans la liste. Sélectionne-le en cliquant dessus et vérifie que la description du périphérique sur le côté droit de l'écran correspond à ton périphérique: sa marque, sa taille, etc.

3. À ce stade, deux options sont possibles:

   3.1. Soit ta mémoire est vide, ou contient des données sur une ou plusieurs partitions que tu ne veux pas conserver:
   Il faut alors formater tout le périphérique. Clique sur **Formater le disque** pour effacer toutes les partitions sur le périphérique. Laisse l'option par défaut: **Master Boot Record**. Une confirmation te sera demandée. Maintenant, le schéma des partitions au milieu de l'écran présente une mémoire vide sous la forme d'une barre grise intitulée **Libre**. Sélectionne-la avec la souris.

   3.2. Soit ta mémoire contient des données stockées sur une ou plusieurs partitions que tu veux conserver:
   Il faut alors sélectionner l'espace vide à partitionner. Pour faire cela, sur le schéma des partitions au milieu de l'écran, sélectionne avec la souris l'espace mémoire vide sous la forme d'une barre blanche intitulé **Libre**.

4. Créer une nouvelle partition cryptée:
   Clique sur **Créer une partition**. Une fenêtre avec des options de configuration va apparaître. Coche la case: **Chiffrer le périphérique correspondant**. Tu peux donner un nom à la partition (en lettres, sans espaces ni caractères spéciaux, sinon ça risque de ne pas marcher) et décider de sa taille (par défaut elle occupe tout l'espace disponible). Ne pas modifier les autres options, à moins de bien savoir ce qu'on fait. Quand c'est bon, clique sur **Créer**. Il te sera demandé de saisir
Voir: 5.5
   à deux reprises la phrase de passe de ton choix pour la nouvelle partition. Clique sur **Créer**. La création de la partition devrait prendre de quelques secondes à quelques minutes (suivant sa taille), après quoi le schéma représentant le périphérique affiche la nouvelle partition chiffrée (petit cadenas). Dès lors, en allant dans le menu **Raccourcis ▷ Dossier personnel** dans la barre d'icônes en haut à gauche de l'écran, elle apparaît sous son nom dans la colonne de gauche.

5. S'il reste encore de l'espace libre sur la mémoire et que tu aimerais créer une partition cryptée supplémentaire, retourne à l'étape 3.2 de cette marche à suivre.

6. Lorsque tu branches un périphérique contenant une partition chiffrée, Tails ne l'ouvrira pas automatiquement mais elle apparaîtra dans le

menu **Raccourcis** ▷ **Dossier personnel**, dans la colonne de gauche. Tant que tu n'as pas entré le mot de passe, le nom que tu lui as donné n'apparaît pas, la partition chiffrée est alors seulement identifiée par la taille de sa mémoire. Après l'avoir identifiée selon sa taille et double-cliqué dessus, une fenêtre s'ouvre où il te sera demandé de saisir la phrase de passe pour déverrouiller la partition. En cas d'erreur, un message d'erreur **Impossible de monter le volume chiffré** apparaît. Tu peux essayer à nouveau d'ouvrir la partition aussi souvent que tu le souhaites. Si la phrase de passe est correcte, la partition sera ouverte dans le navigateur de fichiers. Pour retirer la clé USB cryptée, aller dans **Raccourcis** ▷ **Dossier personnel** et dans la colonne de gauche faire un clic droit sur la clé et choisir **Retirer le volume sans risque**. Un message d'erreur apparaît souvent, mais il est sans conséquence.

6.5 Utiliser l'Utilitaire de disque pour créer une partition non-cryptée afin de stocker des données pas sensibles

Ce point est un peu hors sujet dans ce chapitre, mais faire une partition non cryptée (même si c'est pour l'effacer juste après) peut être bien utile dans certains cas.

1. Dans Tails, ouvrir le programme **Utilitaire de Disque** depuis le menu **Applications** ▷ **Accessoires** ▷ **Utilitaire de disque**.

2. Identifier le périphérique de stockage:
   L'**Utilitaire de disque** liste tous les périphériques disponibles sur le côté gauche de l'écran: branche le périphérique de stockage que tu souhaites utiliser. Un nouveau périphérique devrait apparaître dans la liste. Sélectionne-le en cliquant dessus et vérifie que la description du périphérique sur le côté droit de l'écran correspond à ton périphérique: sa marque, sa taille, etc.

3. À ce stade, deux options sont possibles:

   3.1. Soit ta mémoire est vide, ou contient des données sur une ou plusieurs partitions que tu ne veux pas conserver:
   Il faut alors formater tout le périphérique. Clique sur **Formater le disque** pour effacer toutes les partitions sur le périphérique. Laisse l'option par défaut: **Master Boot Record**. Une confirmation te sera demandée. Maintenant, le schéma des partitions au milieu de l'écran présente une mémoire vide sous la forme d'une barre grise intitulée **Libre**. Sélectionne-la avec la souris.

   3.2. Soit ta mémoire contient des données stockées sur une ou plusieurs partitions que tu veux conserver:
   Il faut alors sélectionner l'espace vide à partitionner. Pour faire

cela, sur le schéma des partitions au milieu de l'écran, sélectionne avec la souris l'espace mémoire vide sous la forme d'une barre blanche intitulé **Libre**.

4. Créer une nouvelle partition non-cryptée:
   Clique sur **Créer une partition**. Une fenêtre avec des options de configuration va apparaître. Ne coche pas la case: **Chiffrer le périphérique correspondant**. Tu peux donner un nom à la partition (en lettres, sans espaces ni caractères spéciaux, sinon ça risque de ne pas marcher) et décider de sa taille (par défaut elle occupe tout l'espace disponible). De plus, dans le menu déroulant **Type** choisir le format de partition **FAT**, qui est lisible par tous les systèmes. Ne pas modifier les autres options, à moins de bien savoir ce qu'on fait. Quand c'est bon, clique sur **Créer**. La création de la partition devrait prendre de quelques secondes à quelques minutes (suivant sa taille), après quoi le schéma représentant le périphérique affiche la nouvelle partition. Dès lors, en allant dans le menu **Raccourcis** ▷ **Dossier personnel** dans la barre d'icônes en haut à gauche de l'écran, elle apparaît sous son nom dans la colonne de gauche.

5. S'il reste encore de l'espace libre sur la mémoire et que tu aimerais créer une partition supplémentaire, retourner l'étape 3.2 de cette marche à suivre.

7 Crypter et décrypter des e-mails et des fichiers avec PGP

7.1 Qu'est-ce que PGP

PGP, Pretty Good Privacy («Assez Bonne Intimité»), est un protocole de
Voir: 5.4 cryptage et décryptage (symétrique ou asymétrique) et d'authentification (signature) pour la communication de données comme des e-mails, des textes ou n'importe quel type de fichiers à envoyer en fichier-joint.
Dans ce chapitre, on va utiliser Open PGP (la variante la plus répandue du protocole PGP) au moyen d'un programme présent dans Tails nommé Applet de chiffrement OpenPGP.

Cette manière de crypter des e-mails est de loin préférable à l'utilisation de fonctionnalités PGP incluses dans de nombreuses messageries e-mail. En effet, écrire un texte confidentiel dans un navigateur web n'est pas prudent

car des attaques dirigées contre le site de messagerie[35] permettent d'accéder au texte en clair (c'est-à-dire non-crypté). Pour éviter cela, après avoir écrit le texte hors-ligne dans l'éditeur de texte, il s'agit comme on va le voir, de le crypter et seulement là, de coller le texte crypté dans la messagerie en ligne.

7.2 Utiliser OpenPGP pour crypter et décrypter des e-mails de manière symétrique

7.2.1 Création de la clé et cryptage symétrique d'e-mails

1. Dans Tails, ouvre l'**Éditeur de texte gedit** depuis **Applications** ▷ **Accessoires** ▷ **Éditeur de texte gedit**. Écris ton texte confidentiel à l'abri des regards. Ne l'écris pas dans le navigateur web !

2. Sélectionne tout le texte avec la souris (ou bien en appuyant simultanément les touches **Ctrl** et **a** du clavier).

3. Clique sur l'**Applet de chiffrement OpenPGP** dont l'icône a la forme d'un bloc-note dans la barre d'icônes en haut à droite de l'écran. Choisis dans le menu, l'option **Chiffrer le presse-papier avec une Phrase de passe**.

4. Dans la fenêtre qui s'est ouverte, tape la phrase de passe de ton choix et clique sur **OK**. Tape de nouveau cette phrase de passe dans la seconde boîte de dialogue pour confirmer.

Voir: 5.5

5. L'**Applet de chiffrement OpenPGP** de Tails affiche désormais un cadenas, signifiant que le programme a copié le texte crypté dans le presse-papier[36].

6. Tu peux maintenant coller (clic droit avec la souris et choisis **Coller** dans le menu) le texte crypté dans un nouveau message de ta messagerie e-mail.

7.2.2 Décryptage symétrique d'e-mails

1. Dans Tails, sélectionne avec la souris le texte chiffré que tu veux déchiffrer. En y incluant les lignes «**-----BEGIN PGP MESSAGE-----**» et «**-----END PGP MESSAGE-----**», du premier au dernier tiret. L'**Applet de chiffrement Open PGP** de Tails affiche désormais un cadenas, signifiant que le presse-papier contient du texte chiffré.

[35] Pour plus d'infos: [https://tails.boum.org/doc/encryption_and_privacy/gpgapplet/index.fr.html].

[36] Le presse-papier est l'espace temporaire où l'ordinateur stocke les données, notamment au moment d'un copier/coller.

2. Clique sur L'**Applet de chiffrement OpenPGP** de Tails et choisis **Déchiffrer/Vérifier le presse-papier** dans le menu. Une fenêtre **Phrase de passe** apparaît. Entre la phrase de passe qui a été utilisée pour chiffrer le texte et clique sur **OK**.

   2.1. Si la phrase de passe est correcte, une fenêtre intitulée **Résultat de GnuPG** apparaît. Le texte déchiffré est écrit en clair dans une boîte de texte **Voici la sortie de GnuPG**.

   2.2. Si la phrase de passe est incorrecte, une fenêtre intitulée une **Erreur de GnuPG** apparaît, mentionnant **échec du déchiffrement: mauvaise clé**. Il faut alors réessayer.

7.3 Utiliser OpenPGP pour crypter et décrypter, signer et authentifier des e-mails de manière asymétrique

7.3.1 Création et export d'une paire de clés de cryptage asymétrique

1. Création de la paire de clés de cryptage:

   1.1. Dans Tails, clique sur **l'Applet de chiffrement OpenPGP** dont l'icône a la forme d'un bloc-note dans la barre d'icônes en haut à droite de l'écran. Choisis **Gérer les Clés** dans le menu.

   1.2. Une fenêtre s'ouvre: **Mots de passe et clés**. Cliquer sur: **Fichier** ▷ **Nouveau**.

   1.3. Une fenêtre s'ouvre: **Sélectionnez le type d'élément à créer** et propose une liste d'éléments à créer. Sélectionner **Clé PGP utilisée pour chiffrer les courriels et les fichiers**. Ensuite, il faut cliquer sur **Continuer**.

   1.4. Une nouvelle fenêtre s'ouvre. Elle comporte plusieurs champs à compléter. Remplir les champs **Nom complet** et **Adresse électronique** avec l'adresse e-mail de sa messagerie cryptée. C'est cette adresse, qui servira par la suite à identifier la clé publique et privée dans le trousseau de clés OpenPGP.

   1.5. Afficher les **Options avancées de clé** et pousser la **Force de la clé** au maximum (**4096**). Il est conseillé de décocher l'option **N'expire jamais** et de choisir une **Date d'expiration** pour la clé[37] de, par exemple, deux ans. Ce choix nous imposera cependant de ne pas oublier de faire la transition vers une nouvelle paire

[37] Le fait de donner une date d'expiration à une paire de clés PGP est une bonne soupape de sécurité si la clé privée est compromise ou perdue. En effet, ça permet de limiter les dégâts dans ce genre de situations, puisque automatiquement, au bout d'un certain temps prédéfini, plus personne ne pourra crypter des messages à destination de cette clé que l'on ne contrôle plus.

de clés, à chaque fois que la précédante est sur le point d'expirer. Voir: 7.3.6 Ne pas modifier les autres options, à moins de bien savoir ce qu'on fait. Passer à l'étape suivante en appuyant sur **Créer**.

1.6. Une nouvelle fenêtre s'ouvre intitulée: **Phrase de passe pour la nouvelle clé PGP**. Là, il faut se creuser la tête pour pondre la plus belle phrase secrète possible, et la taper deux fois de suite Voir: 5.5 dans les champs adéquats. Cliquer sur **Valider**. Une fenêtre s'ouvre appelée **Génération de la clé** avec une barre de progression qui nous indique qu'il faut patienter. La génération de la paire de clés peut nécessiter plusieurs minutes ! Pendant ce temps, il peut être utile d'aider le générateur de nombres pseudo-aléatoires Voir: 5.2 à assembler un très grand nombre de données aléatoires en faisant des mouvements au hasard[38] avec la souris.

2. Export de la paire de clés vers une mémoire de stockage cryptée:

2.1. Retourne dans la fenêtre: **Mots de passe et clés** précédemment ouverte et clique sur l'onglet **Clés GnuPG**, dans la barre latérale gauche. On retrouve maintenant au centre de la fenêtre, une liste d'icônes en forme de clés dans laquelle on va en trouver une, qui porte le même nom que la paire de clés que l'on vient de générer.

2.2. Pour exporter sa clé privée (aussi appelée «clé complète»), afin d'être en mesure de l'importer dans une prochaine session: clic droit avec la souris sur l'icône contenant sa paire de clés, puis aller dans le menu **Propriétés** ▷ **Détails** ▷ **Exporter**. Nommer le fichier et l'enregistrer dans une partition de mémoire cryptée (seul moyen pour garder cette clé confidentielle). Attention de bien conserver l'extension de fichier **.asc** !

2.3. Pour exporter sa clé publique, afin d'être en mesure de la faire tourner à tou-te-s ses potes: s'assurer que la clé est bien sélectionnée, puis aller dans le menu **Fichier** ▷ **Exporter**. Dans la nouvelle fenêtre, ouvrir le petit menu déroulant en bas à droite intitulé: **Clés PGP** et choisir l'option: **Clés blindées PGP**. Pour finir, comme l'application donne par défaut le même nom aux deux clés, c'est pas mal de modifier un des noms à l'exportation, pour pouvoir distinguer la publique de la privée. Donc, choisis un nom explicite pour le ficher, l'endroit où tu veux l'enregistrer, puis clique sur le bouton **Exporter**. Attention à bien conserver l'extension de fichier **.asc** !

[38] Pour plus d'infos: [http://www.cyphercat.eu/tuto_gpg.php].

7.3.2 Échange de clés publiques entre ami-e-s

Avant de pouvoir échanger des e-mails cryptés avec ses ami-e-s, il faut tout d'abord avoir fait un échange des clés publiques. À ce stade, il est très important de ne jamais commettre l'erreur d'envoyer sa clé privée à un contact, au lieu de sa clé publique. Sous peine de mettre en danger la confidentialité de tous les messages qu'on a reçu par le passé et de devoir changer sa paire de clés PGP !

1. Transmission de sa clé publique à un-e amie-e:
   1.1. Soit transmets lui la clé directement sous le format **.asc** (format par défaut lors de son exportation), dans le fichier-joint d'un e-mail ou via une clé USB.
   1.2. Soit fais un clic droit sur le fichier de la clé au format **.asc** et choisis **Ouvrir avec** ▷ **Éditeur de texte gedit** dans le menu. Dans **gedit**, sélectionne ensuite le texte de la clé en y incluant les lignes «**-----BEGIN PGP PUBLIC KEY BLOCK-----**» et «**-----END PGP PUBLIC KEY BLOCK-----**», du premier au dernier tiret. Copie-le et colle-le dans le texte d'un e-mail à envoyer.
2. Enregistrement de la clé publique transmise par un-e ami-e:
   2.1. Si le fichier de la clé a été transmis au format **.asc** via le fichier-joint d'un e-mail ou via une une clé USB, enregistre-le directement le répertoire **Tor Browser** de Tails.
   2.2. Si la clé a été transmise dans le texte d'un e-mail, alors sélectionne et copie l'ensemble du texte composant la clé, en y incluant les lignes «**-----BEGIN PGP PUBLIC KEY BLOCK-----**» et «**-----END PGP PUBLIC KEY BLOCK-----**», du premier au dernier tiret. Ensuite, ouvre l'**Éditeur de texte gedit** depuis **Applications** ▷ **Accessoires** ▷ **Éditeur de texte gedit** et colle le texte dans le nouveau document qui s'est ouvert. Va ensuite dans **Fichier** ▷ **Enregistrer sous** et enregistre la clé en la nommant comme tu veux mais sans oublier de lui rajouter l'extension de fichier **.asc** à la fin du nom. Clique enfin sur **Enregistrer**.

7.3.3 Vérification de l'authenticité de clés publiques

Cette étape n'est pas obligatoire pour pouvoir utiliser le cryptage de données de manière asymétrique (on peut donc s'en passer). C'est juste une sécurité de plus, qui permet de vérifier que la clé publique transmise n'a

pas été modifiée par une tierce personne à des fins malveillantes. Alors que la clé publique est très longue (facilement plusieurs milliers de caractères !), l'empreinte dérivée de cette clé publique (public key fingerprint[39]) ne comporte elle, par contre, que quelques dizaines de caractères, facilement recopiables à la main sur un bout de papier et comparables à l'oeil nu. Ce sont ces propriétés qui vont être utilisées pour l'authentification.

1. Avant de pouvoir être en mesure de visualiser l'empreinte de sa clé publique, il faut tout d'abord que cette dernière soit importée dans l'**Applet de chiffrement OpenPGP**. Si tu n'en es pas sûr-e, il faut se rendre à l'endroit où elle est enregistrée dans la partition de mémoire cryptée (fichier de type **.asc**), puis il suffit de double-cliquer dessus. À ce moment là, une fenêtre s'ouvre, intitulée **Key imported**.

Voir: 7.3.1

2. Visualisation de l'empreinte de sa clé publique:
   Pour savoir quelle est l'empreinte de sa clé publique, il faut cliquer sur l'**Applet de chiffrement OpenPGP** dont l'icône a la forme d'un bloc-note dans la barre d'icônes en haut à droite de l'écran et choisir **Gérer les Clés** dans le menu. Clique sur l'onglet **Clés GnuPG**, dans la barre latérale gauche, de la nouvelle fenêtre qui s'est ouverte. On voit maintenant au centre de la fenêtre, une liste d'icônes en forme de clés, dans laquelle on va trouver celle qui nous intéresse. Faire un clic droit sur l'icône représentant la clé, puis aller dans le menu **Propriétés** ▷ **Détails** ▷ **Empreinte**. Cette empreinte prend la forme d'une suite de caractères groupés, qui pourrait par exemple ressembler à: **1F56 EDD3 0741 0480 35DA C1C5 EC57 B56E F0C4 1312**. Note cette empreinte sur un bout de papier ou mémorise-la, si tu as une bonne mémoire.

3. L'échange de l'empreinte des clés publiques peut se faire à n'importe quel moment après et même avant l'échange des clés publiques par voie numérique. L'échange de l'empreinte des clés publiques se doit par contre d'être fait par la voie la plus sûre qui soit. C'est-à-dire, à l'occasion d'une rencontre physique avec son ami-e, par un échange de main à main des petits bouts de papiers sur lesquels on a inscrit l'empreinte de sa propre clé publique.

4. Comparaison des empreintes:
   Une fois de retour chez soi avec le petit bout de papier, il suffit de comparer l'empreinte manuscrite à celle dérivée de la clé publique que notre ami-e doit nous avoir transmise par voie numérique. Pour visualiser cette dernière, il faut procéder de manière similaire aux étapes

Voir: 7.3.2

[39]Pour plus d'infos: [https://en.wikipedia.org/wiki/Public_key_fingerprint].

1 et 2 de cette marche à suivre, en important cette fois non pas sa propre clé publique mais celle de son ami-e. Si à la comparaison, les deux empreintes concordent, c'est ok !

7.3.4 Cryptage asymétrique et signature d'e-mails

1. Dans Tails, avant de pouvoir utiliser l'**Applet de chiffrement OpenPGP** en mode asymétrique, il faut tout d'abord que les clés publiques et privées dont on va avoir besoin, y soient bien importées. Si tu n'en es pas sûr-e, il faut se rendre à l'endroit où elles sont enregistrées dans la partition de mémoire cryptée (fichiers de type **.asc**), puis il suffit de double-cliquer dessus. À ce moment là, une fenêtre s'ouvre, intitulée **Key imported**.

Voir: 7.3.1

2. Ouvre l'**Éditeur de texte gedit** depuis le menu **Applications** ▷ **Accessoires** ▷ **Éditeur de texte gedit**. Écris ton texte confidentiel à l'abri des regards. Ne l'écris pas dans le navigateur web !

3. Sélectionne tout le texte avec la souris (ou bien en appuyant les touches **Ctrl** et **a** du clavier).

4. Clique sur l'**Applet de chiffrement OpenPGP** dont l'icône a la forme d'un bloc-note dans la barre d'icônes en haut à droite de l'écran. Choisis **Signer/Chiffrer le presse-papier avec une clé publique** dans le menu. Une fenêtre intitulée **Choisir les clés** s'ouvre.

   4.1. Si tu veux crypter le texte, sélectionne dans la boîte de dialogue **Choisir les clés des destinataires**, une ou plusieurs clés publiques pour les destinataires du texte. Pour sélectionner une clé publique, double-cliquer sur la ligne correspondante dans la liste.

   4.2. Si en plus de le crypter, tu veux signer le texte, sélectionne la clé privée avec laquelle tu veux signer, dans le menu déroulant **Signer le message en tant que**.

   4.3. Si tu veux masquer les destinataires du texte chiffré, coche **Cacher les destinataires**. Sans quoi n'importe qui voyant le texte chiffré peut savoir qui en sont les destinataires.

5. Clique sur le bouton **Valider**. Si tu obtiens l'avertissement **Faites-vous confiance à ces clés ?**, réponds-y en conséquence.

   5.1. Si tu as choisi de signer le texte avec ta clé privée et que la phrase de passe n'est pas déjà stockée en mémoire, une fenêtre s'ouvre avec le message suivant: **Une phrase de passe est nécessaire pour déverrouiller la clé secrète de l'utilisateur**. Tape la phrase de passe pour cette clé privée et clique sur **Valider**.

6. L'**Applet de chiffrement OpenPGP** de Tails affiche désormais un cadenas, signifiant que le programme a copié le texte crypté dans le presse-papier[40].

7. Tu peux maintenant coller (fais clic droit avec la souris et choisis **Coller** dans le menu) le texte crypté dans un nouveau message de ta messagerie e-mail.

7.3.5 Décryptage asymétrique et authentification de signature d'e-mails

1. Dans Tails, avant de pouvoir utiliser l'**Applet de chiffrement OpenPGP** en mode asymétrique, il faut tout d'abord que les clés publiques et privées dont on va avoir besoin, y soient bien importées. Si tu n'en es pas sûr-e, il faut se rendre à l'endroit où elles sont enregistrées dans la partition de mémoire cryptée (fichiers de type **.asc**), puis il suffit de double-cliquer dessus. À ce moment là, une fenêtre s'ouvre, intitulée **Key imported**.

Voir: 7.3.1

2. Sélectionne avec la souris l'ensemble du texte chiffré que tu veux déchiffrer, en y incluant les lignes «**-----BEGIN PGP MESSAGE-----**» et «**-----END PGP MESSAGE-----**», du premier tiret au dernier tiret. L'**Applet de chiffrement OpenPGP** de Tails affiche désormais un cadenas, signifiant que le presse-papier contient du texte chiffré.

3. Clique sur l'**Applet de chiffrement OpenPGP** de Tails et choisis **Déchiffrer/Vérifier le presse-papier** dans le menu.

4. Si le texte est signé et que la signature est invalide, un message **Erreur de GnuPG** mentionne **MAUVAISE signature de...**

5. Comme le texte a été crypté avec une clé publique, trois boîtes de dialogue différentes peuvent apparaître:

   5.1. Si la phrase de passe pour la clé privée correspondante n'est pas déjà stockée en mémoire, une boîte de dialogue apparaît avec le message suivant: **Une phrase de passe est nécessaire pour déverrouiller la clé secrète de l'utilisateur**. Tape la phrase de passe qui protège cette clé privée et clique sur **Valider**.

   5.2. Si la phrase de passe pour la clé privée correspondante est déjà stockée en mémoire, elle est automatiquement reconnue.

[40] Le presse-papier est l'espace temporaire où l'ordinateur stocke les données, notamment au moment d'un copier/coller.

5.3. Si aucune clé privée pour laquelle le texte est chiffré n'est disponible dans ton trousseau, un message **Erreur de GnuPG** apparaît, mentionnant **échec du déchiffrement: la clé secrète n'est pas disponible**. Il faut recommencer, en s'assurant d'avoir au préalable importé la bonne clé privée.

6. Si la phrase de passe est incorrecte, un message **Erreur GnuPG** apparaît, mentionnant **Phrase de passe incorrecte; veuillez réessayer**.

7. Si la phrase de passe est correcte, ou si la signature du texte est valide, ou les deux, une fenêtre **Résultat de GnuPG** apparaît. Le texte déchiffré est écrit en clair dans une boîte de texte **Voici la sortie de GnuPG**. Dans la partie **Autres messages de GnuPG** de la fenêtre, le message **Bonne signature de...**, confirme que la signature du texte est valide (si le texte a été signé).

7.3.6 Migrer vers une nouvelle paire de clés

Voir: 7.3.1

Quelques mois avant qu'une paire de clés n'expire, il est temps de se créer une nouvelle paire de clés PGP puis de transmettre et d'authentifier sa nouvelle clé publique auprès de tous ses contacts.
C'est important de ne pas rater le coche, car une fois qu'une paire de clés a expiré plus personne ne sera en mesure de l'utiliser. Et il est justement indispensable, que nos différents contacts PGP puissent encore vérifier l'authenticité de notre nouvelle clé publique, qu'on aura signée...avec notre ancienne clé privée.

En effet, une manière simple d'authentifier la nouvelle clé publique auprès de ses contacts, est de copier/coller celle-ci dans le corps du texte des e-

Voir: 7.3.4

mails qu'on leur enverra et qu'il faudra surtout signer avec notre ancienne clé privée. À noter que bien qu'on ne les présente pas ici, il existe d'autres méthodes[41] plus spécifiques pour authentifier une nouvelle clé avec une ancienne et même pour révoquer des clés immédiatement.

7.4 Utiliser OpenPGP pour crypter et décrypter, signer et authentifier des fichiers de manière asymétrique

OpenPGP permet de crypter individuellement n'importe quel type de fichier et pas seulement du texte ! C'est bien pratique quand ont veut par exemple transmettre ou recevoir de manière confidentielle une image ou un pdf dans le fichier joint d'un e-mail. On peut noter en passant, que tous les préalables

[41] Pour plus d'infos sur ces différentes méthodes: [le chapitre 18 du tome 2 du Guide d'autodéfense numérique].

au cryptage vus au chapitre précédant et en particulier les points traitants de la création et de l'échange de clés asymétriques sont à lire avant d'aborder cette partie.

Voir: 7.3.1
Voir: 7.3.2

7.4.1 Cryptage asymétrique et signature de fichiers

1. Dans Tails, avant de pouvoir utiliser l'**Applet de chiffrement OpenPGP** en mode asymétrique, il faut tout d'abord que les clés publiques et privées dont on va avoir besoin, y soient bien importées. Si tu n'en es pas sûr-e, il faut se rendre à l'endroit où elles sont enregistrées dans la partition de mémoire cryptée (fichiers de type **.asc**), puis il suffit de double-cliquer dessus. À ce moment là, une fenêtre s'ouvre, intitulée **Key imported**.

Voir: 7.3.1

2. Fais un clic droit sur le fichier que tu désires crypter, choisis ▷ **Chiffrer** dans le menu. Une fenêtre intitulée **Choisir les destinataires** s'ouvre:

    2.1. Si tu veux crypter le fichier, sélectionne dans le menu déroulant, une ou plusieurs clés publiques pour les destinataires du fichier. Pour sélectionner une clé publique, double-clique sur la ligne correspondante dans la liste.

    2.2. Si en plus de le crypter, tu veux signer le fichier, sélectionne la clé privée avec laquelle tu veux signer, dans le menu déroulant **Signer le message comme**.

3. Cliquer sur le bouton **Valider**. Si tu obtiens l'avertissement **Faites-vous confiance à ces clés ?**, réponds-y en conséquence.

    3.1. Si tu as choisi de signer le fichier avec ta clé privée et si la phrase de passe n'est pas déjà stockée en mémoire, une fenêtre s'ouvre avec le message suivant: **Une phrase de passe est nécessaire pour déverrouiller la clé secrète de l'utilisateur**. Tape la phrase de passe pour cette clé privée et clique sur **Valider**.

4. Le fichier crypté apparaît maintenant dans le même dossier que son homologue non-crypté. Il est reconnaissable par son extension **.pgp**. Si tu veux le renommer, fais un clic droit dessus et choisis ▷ **Renommer...** en ayant à l'esprit que le nom apparaîtra en clair. Donc, arrange-toi pour qu'il ne donne pas d'infos sur le contenu du fichier. N'oublie pas de conserver l'extension du fichier **.pgp** à la fin du nom.

5. Tu peux maintenant transmettre le fichier crypté dans le fichier-joint d'un e-mail, par exemple.

7.4.2 Décryptage asymétrique et authentification de signature de fichiers

1. Dans Tails, avant de pouvoir utiliser l'**Applet de chiffrement OpenPGP** en mode asymétrique, il faut tout d'abord que les clés publiques et privées dont on va avoir besoin, y soient bien importées. Si tu n'en es pas sûr-e, il faut se rendre à l'endroit où elles sont enregistrées dans la partition de mémoire cryptée (fichiers de type **.asc**), puis il suffit de double-cliquer dessus. À ce moment là, une fenêtre s'ouvre, intitulée **Key imported**.

Voir: 7.3.1

2. Ensuite, fais un clic droit sur le fichier que tu veux décrypter et choisis ▷ **Ouvrir avec Déchiffrer le fichier** dans le menu.

3. Si le fichier est signé et que la signature est invalide, un message **Erreur de GnuPG** apparaît, qui dit **MAUVAISE signature de...**

4. Comme le fichier a été chiffré avec une clé publique, trois boîtes de dialogue différentes peuvent apparaître:

   4.1. Si la phrase de passe pour la clé privée correspondante n'est pas déjà stockée en mémoire, une boîte de dialogue apparaît avec le message suivant: **Une phrase de passe est nécessaire pour déverrouiller la clé secrète de l'utilisateur**. Tape la phrase de passe qui protège cette clé privée et clique sur **Valider**.

   4.2. Si la phrase de passe pour la clé privée correspondante est déjà stockée en mémoire, elle est automatiquement reconnue.

   4.3. Si aucune clé privée pour laquelle le texte est chiffré n'est disponible dans ton trousseau, un message **Erreur de GnuPG** apparaît, mentionnant **échec du chiffrement: la clé secrète n'est pas disponible**. Il faut recommencer en s'assurant d'avoir au préalable importé la bonne clé privée.

5. Si la phrase de passe est incorrecte, un message **Erreur de GnuPG** apparaît, mentionnant **Phrase de passe incorrecte; veuillez réessayer**.

6. Si la phrase de passe est correcte, alors le fichier décrypté apparaît par défaut dans le même dossier et sous le même nom que le fichier crypté ou dans un autre fichier et sous un autre nom si ça a été spécifié.

   6.1. Si le fichier était signé et que la signature est valide, une fenêtre apparaît avec le message **Signature valide**, confirmant ainsi l'authenticité du fichier.

8 Crypter des messages instantanés avec Pidgin et OTR

8.1 Qu'est-ce que Pidgin et OTR

Pidgin est un programme de messagerie instantanée qui est disponible par défaut dans Tails. Il permet d'utiliser les protocoles de messagerie instantanée les plus courants, comme Jabber (XMPP) et IRC.
OTR[42] (Off The Record Messaging) est un protocole de cryptage des messages instantanés qui est utilisable avec Pidgin. OTR utilise le mode de cryptage asymétrique et comme il génère automatiquement les clés de cryptage, son utilisation est plus facile que le cryptage des e-mails avec PGP.
Voir: 5.4
Pour faire bref, en utilisant Pidgin et OTR sur un ordinateur allumé sous Tails et connecté à Internet via Tor, on va pouvoir contacter des potes instantanément, de manière anonyme (Tor cache l'origine et la destination des communications) et confidentielle (le cryptage d'OTR cache le contenu des communications aux personnes indiscrètes). En plus, si on dédie un vieil ordinateur à cet usage (avec ses supports de mémoire de stockage débranchés) et qu'il reste allumé en permanence, ces outils peuvent en grande partie se substituer avantageusement au téléphone fixe (pour peu que cette pratique se répande).
Voir: 10.1
Voir: 3.2.2

Pour finir, en voyant la simplicité d'utilisation de cet outil, on pourrait être amené-e à douter de l'utilité des e-mails cryptés avec PGP. En fait messagerie instantanée et e-mails sont deux moyens de communication complémentaires. Les messages instantanés sont conçus comme le téléphone pour communiquer dans l'instant, quand l'info doit circuler vite. Les e-mails par contre ne sont pas très efficaces dans ce domaine (à part pour les gens qui visitent leur messagerie 8 fois par jour...), mais permettent une communication beaucoup plus fiable sur le long terme. Tout comme le courrier postal, ils rendent possible le fait de se déconnecter une semaine et de reprendre facilement le fil à son retour, sans perte d'informations.

8.2 Utiliser Pidgin et OTR pour échanger des messages instantanés cryptés

8.2.1 Création du compte de messagerie instantanée

1. Allumer un ordi sous Tails et se connecter à Internet via **Tor**.
Voir:10.4.1

2. Aller sur la page Internet: [`https://user.riseup.net/forms/new_user/first`]. Le serveur militant riseup.net permet, pour l'inscription d'une seule adresse (un seul identifiant et mot de passe), de disposer à
Voir: 9.3.2

[42] Pour plus d'infos sur OTR: [`www.cypherpunks.ca/otr/otr-wpes.pdf`].

la fois d'un compte de messagerie e-mail et d'un compte de messagerie instantanée Jabber[43] (protocole XMPP). Dans ce cas, c'est la deuxième chose qui nous intéresse, mais une adresse e-mail riseup sécurisée est loin d'être inutile (parfaite pour l'échange d'e-mails cryptés).

3. Il va donc s'agir de suivre le formulaire d'inscription proposé. Il faut se choisir un nom d'utilisateur-trice, et un mot de passe dont il faudra se souvenir. À la fin de la marche à suivre, avant de valider l'inscription, on nous propose deux options. Soit on bénéficie d'un code de cooptation de deux ami-e-s déjà inscrit-e-s sur le serveur, ce qui permet l'activation immédiate du compte. Soit il suffit d'écrire quelques phrases de présentation, rassurant les personnes de riseup sur nos intentions militantes, non commerciales et non réactionnaires, ce qui repousse la validation du compte de deux à trois jours.

8.2.2 Communiquer avec Pidgin et OTR de manière ponctuelle

Avec cette méthode, la messagerie n'est pas allumée 24/24, on l'utilise alors plus pour contacter des potes (ayant un ordi connecté à **Pidgin** en permanence) que pour être soi-même contacté-e. Dans cette configuration, comme il faut rallumer un ordi sous Tails à chaque fois, il faut compter trois minutes avant de pouvoir appeler.

1. Chaque utilisation nécessite de disposer d'un ordi sous **Tails** et connecté à Internet via **Tor**.

2. Enregistrement dans **Pidgin** du compte créé précédemment:
   Ouvrir **Pidgin** en allant dans le menu en haut à gauche de l'écran **Applications** ▷ **Internet** ▷ **Messagerie internet Pidgin**. Dans la fenêtre active intitulée **Comptes**, il faut cliquer sur le bouton **Ajouter**. Une autre fenêtre s'ouvre appelée **Ajouter un compte**; dans l'onglet **Essentiel**, sélectionner: **XMPP** dans le menu déroulant **Protocole**;
Voir: 8.2.1
   dans le champ **Utilisateur**, mettre le nom d'utilisateur-trice choisi précédemment; dans le champ **Domaine**, mettre: **riseup.net**; dans le champ **Ressource**, mettre: **riseup**; dans le champ **Mot de passe** indiquer le mot de passe choisi précédemment et cocher l'option **Mémoriser le mot de passe**. Ensuite dans la même fenêtre, aller dans l'onglet **Avancé**[44] et dans le champ **Serveur de connexion**, indiquer

[43] Il existe de nombreux autres serveurs non-commerciaux proposant gratuitement des services de messagerie instantanée Jabber, mais très peu sont aussi exigeants que riseup.net. De toute façon, depuis un serveur Jabber donné, on peut discuter avec toutes les personnes connectées à n'importe quel autre serveur utilisant le même protocole. Pour plus d'infos: [http://wiki.jabberfr.org/Serveurs].

[44] À noter que les réglages présentés dans cet onglet sont spécifiques à riseup.net et ne seront pas nécessaires pour d'autres serveurs de messagerie instantanée.

l'adresse suivante: **4cjw6cwpeaeppfqz.onion**; enfin dans le champ **Proxy pour le transfert de fichiers**, mettre: **proxy.riseup.net** et cliquer sur **Ajouter**[45]. Si une fenêtre intitulée **Vérification de certificat SSL** apparaît, cliquer sur **Accepter**.

3. Paramétrer **Pidgin** pour qu'il utilise toujours le cryptage **OTR**:
   Aller dans **Outils** ▷ **Plugins** ▷ **Messagerie confidentielle Off the Record** et cliquer sur **Configurer le plugin**. Là, sélectionner le compte utilisé et cocher les options: **Permettre messagerie privée**, **Commencer messagerie privée automatiquement**, **Exiger une messagerie privée** et **ne pas Archiver les conversations d'OTR**. Il faut encore cliquer sur le bouton **Produire** qui va produire une clé de cryptage pour le compte. Finalement, laisser les autres options par défaut et cliquer sur **Fermer**.

4. Enregistrement de nouveaux contacts:
   Aller dans le menu **Contacts** ▷ **+Ajouter un contact** et il suffit d'écrire le nom du contact avec le nom de domaine, par exemple: **user@riseup.net** et cliquer sur **Ajouter**. Il faut encore aller dans le menu **Contacts** ▷ **Afficher** et cocher l'option **Contacts déconnectés**. Les contacts seront tout d'abord affichés comme **Non autorisé**, c'est pas grave (ça n'empêche pas d'appeler) et le contact pourra nous donner son autorisation dès le premier échange de messages.

5. Contacter ses contacts:
   Faire un clic droit avec la souris sur le contact enregistré à l'étape précédente et cliquer sur **Message**. Là, une fenêtre s'ouvre, aller dans le menu **OTR** ▷ **Commencer une conversation privée**, il faut ensuite attendre que le message: **Une conversation (...) a commencé** s'affiche et on peut après commencer à envoyer des messages. Si c'est la première fois qu'on communique avec un contact, il est mentionné : **Conversation non-vérifiée**. C'est pas très grave, ça ne signifie pas que les messages ne sont pas cryptés, mais seulement qu'il est possible de mieux vérifier (authentifier) que son contact est bien la personne avec qui on veut parler. Pour faire ça, on peut aller dans le menu en haut à droite de la fenêtre de conversation **OTR** ▷ **Authentifier contact**. Là, plusieurs méthodes d'authentification sont possibles, dont la plus simple est peut-être de poser une question dont seul le contact connaîtra la réponse.
   À noter que parfois, si on n'a pas de réponse au premier message envoyé, il vaut la peine de renvoyer quelques messages à intervalle régulier (environ toutes les 20 secondes). En effet, en l'absence de réponse chaque

[45] Pour plus d'infos sur ces réglages: [https://help.riseup.net/en/pidgin].

message envoyé va déclencher une sonnerie de quelques secondes, donc si on veut que la sonnerie continue il faut envoyer des messages dans le vide du genre «Houhou, réponds», «Y'a quelqun-e ?».
Pour mettre fin à la conversation de manière sécure, aller dans le menu **OTR ▷ Terminer la conversation privée**. Cela permet d'éviter qu'un ou une adversaire qui obtiendrait les clés de chiffrement puisse déchiffrer la conversation par la suite.

8.2.3 Communiquer avec Pidgin et OTR sur un ordinateur connecté en permanence

Avec cette méthode, la messagerie est allumée 24/24, on l'utilise alors à la fois pour contacter des potes (qui ont aussi un ordi connecté en permanence) que pour être soi-même contacté-e. Dans cette configuration, comme l'ordi sous Tails est tout le temps actif, c'est aussi rapide, voire plus rapide que de lancer un coup de fil.

1. L'installation nécessite de disposer d'un ordi sous **Tails** et connecté à Internet via **Tor**.

2. Enregistrement dans **Pidgin** du compte créé précédemment:
   Ouvrir **Pidgin** en allant dans le menu en haut à gauche de l'écran **Applications ▷ Internet ▷ Messagerie internet Pidgin**. Dans la fenêtre active intitulée **Comptes** il faut cliquer sur le bouton **Ajouter**. Une autre fenêtre s'ouvre appelée **Ajouter un compte**; dans l'onglet **Essentiel**, sélectionner: **XMPP** dans le menu déroulant **Protocole**;
Voir: 8.2.1
   dans le champ **Utilisateur**, mettre le nom d'utilisateur-trice choisi précédemment; dans le champ **Domaine**, mettre: **riseup.net**; dans le champ **Ressource**, mettre: **riseup**; dans le champ **Mot de passe** indiquer le mot de passe choisi précédemment et cocher l'option **Mémoriser le mot de passe**. Ensuite dans la même fenêtre, aller dans l'onglet **Avancé**[46] et dans le champ **Serveur de connexion**, indiquer l'adresse suivante: **4cjw6cwpeaeppfqz.onion**; enfin dans le champ **Proxy pour le transfert de fichiers**, mettre: **proxy.riseup.net** et cliquer sur **Ajouter**[47]. Si une fenêtre intitulée **Vérification de certificat SSL** apparaît, cliquer sur **Accepter**.

3. Paramétrer **Pidgin** pour qu'il utilise toujours le cryptage **OTR**:
   Aller dans **Outils ▷ Plugins ▷ Messagerie confidentielle Off the Record** et cliquer sur **Configurer le plugin**. Là, sélectionner le

[46] À noter que les réglages présentés dans cet onglet sont spécifiques à riseup.net et ne seront pas nécessaires pour d'autres serveurs de messagerie instantanée.
[47] Pour plus d'infos sur ces réglages: [`https://help.riseup.net/en/pidgin`].

compte utilisé et cocher les options: **Permettre messagerie privée**, **Commencer messagerie privée automatiquement**, **Exiger une messagerie privée** et **ne pas Archiver les conversations d'OTR**. Il faut encore cliquer sur le bouton **Produire** qui va produire une clé de cryptage pour le compte. Finalement, laisser les autres options par défaut et cliquer sur **Fermer**.

4. Paramétrer **Pidgin** pour avoir une sonnerie continue tant que l'on ne répond pas à un appel (comme un téléphone):
   Aller sur Internet, télécharger une sonnerie qui sonne bien et l'enregistrer dans le dossier appelé **Tor Browser**, puis couper/coller ce fichier dans le répertoire **Raccourcis ▷ Bureau**. Ensuite dans **Pidgin**, aller dans le menu **Outils ▷ Préférences ▷ État/Inactivité** et à l'option **Rapporter le temps d'inactivité**, répondre: **Depuis le dernier message envoyé**; à l'option **Minutes avant de passer inactif**, répondre: **3**; cocher l'option: **Changer vers cet état quand inactif** et choisir: **Absent**. Aller ensuite dans **Outils ▷ Préférences ▷ Sons** et dans le menu **Méthode**, choisir **Automatique**; cocher l'option **Jouer les sons quand la conversation est en avant plan**; à l'option **Activer les sons**, répondre: **Seulement quand je ne suis pas disponible**; mettre le volume au max; dans le menu **Événements sonores**, vérifier que **Réception d'un message** est la seule option cochée. Finalement, après s'être assuré-e que l'option **Réception d'un message** est bien sélectionnée (le nom de l'option doit être mis en évidence dans une barre bleue), naviguer dans les fichiers pour choisir la sonnerie précédemment placée sur le **Bureau**, avant de cliquer sur **Fermer**.
   Pour mettre en fonction ce dispositif, il faut encore rapidement réinitialiser **Pidgin**. Pour cela, aller dans le menu **Contacts ▷ Quitter**, puis redémarrer le programme en allant dans le menu en haut à gauche de l'écran **Applications ▷ Internet ▷ Messagerie internet Pidgin**. Parfois après quelques temps d'utilisation, il arrive que la sonnerie continue, même après que l'on ait répondu à un appel. Ce petit problème se résout facilement en se rendant dans le menu **Outils ▷ Préférences ▷ État/Inactivité** et en s'assurant qu'à l'option **État utilisé au démarrage**, il soit bien spécifié: **Disponible** et non pas **Absent**. Finalement, il faut encore réinitialiser **Pidgin** comme indiqué au paragraphe précédant.

5. Enregistrement de nouveaux contacts:
   Aller dans le menu **Contacts ▷ +Ajouter un contact** et il suffit d'écrire le nom du contact avec le nom de domaine, par exemple: **user@riseup.net** et cliquer sur **Ajouter**. Il faut encore aller dans le

menu **Contacts ▷ Afficher** et cocher l'option **Contacts déconnectés**. Les contacts seront tout d'abord affichés comme **Non autorisé**, c'est pas grave (ça n'empêche pas d'appeler) et le contact pourra nous donner son autorisation dès le premier échange de messages.

6. Contacter ses contacts:
   Faire un clic droit avec la souris sur le contact enregistré à l'étape précédente et cliquer sur **Message**. Là, une fenêtre s'ouvre, aller dans le menu **OTR ▷ Commencer une conversation privée**, il faut ensuite attendre que le message: **Une conversation (...) a commencé** s'affiche et on peut après commencer à envoyer des messages. Si c'est la première fois qu'on communique avec un contact, il est mentionné : **Conversation non-vérifiée**. C'est pas très grave, ça ne signifie pas que les messages ne sont pas cryptés, mais seulement qu'il est possible de mieux vérifier (authentifier) que son contact est bien la personne avec qui on veut parler. Pour faire ça, on peut aller dans le menu en haut à droite de la fenêtre de conversation **OTR ▷ Authentifier contact**. Là, plusieurs méthodes d'authentification sont possibles, dont la plus simple est peut-être de poser une question dont seul le contact connaîtra la réponse.
   À noter que parfois si on n'a pas de réponse au premier message envoyé, il vaut la peine de renvoyer quelques messages à intervalle régulier (environ toutes les 20 secondes). En effet, en l'absence de réponse chaque message envoyé va déclencher une sonnerie de quelques secondes, donc si on veut que la sonnerie continue il faut envoyer des messages dans le vide du genre «Houhou, réponds», «Y'a quelqun-e ?».
   Pour mettre fin à la conversation de manière sécure, aller dans le menu **OTR ▷ Terminer la conversation privée**. Cela permet d'éviter qu'un ou une adversaire qui obtiendrait les clés de chiffrement puisse déchiffrer la conversation par la suite.

9 Internet et les réseaux: des traces et encore des traces

9.1 Qu'est-ce qu'Internet

Un réseau informatique est un ensemble d'appareils (souvent des ordinateurs, mais pas seulement !) reliés entre eux pour échanger des informations.
Partant de là, on peut dire qu'Internet est un réseau de réseaux. En fait, c'est même de là qu'Internet tire son nom. C'est un système mondial d'**int**erconnexion non centralisé de millions de réseaux informatiques (**net**works en anglais) qui sont reliés de manière locale et globale par une véritable toile d'araignée de connexions, qui utilisent les mêmes langages informatiques: les protocoles de communication.

Maintenant, pour comprendre plus précisément le fonctionnement et les dangers d'Internet, il peut être utile de décortiquer tour à tour ses deux composantes principales: l'infrastructure matérielle d'un côté, et les protocoles informatiques de l'autre.

9.1.1 Infrastructure matérielle d'Internet

On va tout d'abord voir suivant quelle architecture sont organisées les différentes machines et connexions qui constituent la base matérielle du réseau. On pourra ensuite se faire une petite idée de ce qui se cache derrière nos navigations quotidiennes sur Internet.

Les machines faisant partie du réseau Internet peuvent être approximativement divisées en trois types. Clients, serveurs, routeurs:

- Tout d'abord, les clients sont tous les appareils profitant d'un accès au réseau, et qui obtiennent des serveurs les nombreux services disponibles sur Internet. Les clients sont généralement des ordinateurs personnels ordinaires, et plus récemment des smartphones.

- Ensuite, les ordinateurs qui répondent aux demandes des clients en stockant et rendant disponibles toutes les informations que l'on peut trouver sur Internet sont les serveurs (ou hébergeurs). Sans eux, pas de sites web, de vidéos en streaming ou de stockage de nos e-mails (pour ne citer que quelques exemples). La plupart des serveurs sont supportés par des entreprises commerciales, mais certains serveurs sont issus de personnes ou de collectifs qui hébergent des sites et offrent des services de manière souvent plus autonome, fiable et avec autre chose que le fric en tête.

Voir: 9.3.2

- Finalement, il y a les routeurs. Ce sont des machines spécialisées qui servent de relais intermédiaires entre clients et serveurs. Comme Internet est un immense réseau composé d'innombrables plus petits réseaux, l'utilisation des routeurs est une nécessité. Ils font le lien entre différents réseaux; en faisant transiter les données échangées des uns vers les autres, ils permettent à celles-ci d'atteindre leur destination à travers des milliers de connexions possibles. Notons aussi en passant que le modem, qui est le petit boitier servant souvent de relais entre l'ordinateur et l'accès à Internet dans les maisons, est une forme simple de routeur.

Les connexions constituent l'autre partie essentielle de l'infrastructure du réseau Internet. Elles matérialisent l'ensemble des voies de transmission reliant toutes les machines en un grand réseau. Ces connexions prennent principalement deux formes: soit des câbles électriques ou fibres optiques, soit

des connexions sans fil via les antennes téléphoniques terrestres, les satellites ou même le wifi domestique.
On peut encore relever l'existence des dorsales Internet (Internet backbone). Ce terme se réfère aux voies principales empruntées par les données, entre les plus grands réseaux interconnectés. Le fait qu'on ne considère pas Internet comme un réseau centralisé, signifie qu'il n'a pas un point central unique d'organisation, mais cela n'exclut pas le fait qu'en de nombreux endroits du globe, le trafic Internet soit localement extrêmement concentré. C'est le cas pour les connexions se faisant entre pays, continents et pour les lignes passant sous les océans. Ainsi, quand on sait que par exemple en l'an 2000, 95% des communications Internet en Allemagne étaient routées en un point unique à Francfort[48], on peut commencer à s'imaginer le grand impact que cette «centralisation décentralisée» peut avoir en matière de surveillance et de gouvernance d'Internet.

Voir: 9.2

Pour mettre un peu en contexte tous ces éléments, on peut essayer de suivre le(s) chemin(s) emprunté(s) par les flux de données lors de la visite d'un site web depuis un ordinateur personnel.
Pour faire simple, on a vu que le fonctionnement d'Internet repose sur la transmission d'informations d'un point à un autre, du client au serveur mais aussi inversement du serveur au client, sans manquer de passer par des relais, les routeurs, qui guident les données à travers la complexité du réseau. Le fait que l'information aille dans les deux sens entre le client et le serveur est essentiel, c'est la base même de la communication. Si le client effectue une demande au serveur (par exemple ouvrir une nouvelle page d'un site web), cette action n'aurait pas beaucoup de sens si le client n'est pas en mesure de recevoir de réponse (les données contenues sur la nouvelle page). En l'absence de réponse, le client ne sait même pas s'il a réussi à joindre le serveur. Autant parler à une pierre !
Donc, quand depuis son ordinateur connecté à Internet, on clique sur un lien ouvrant un site web, notre requête électronique (traduite en données numériques) va, dans l'ordre: tout d'abord passer de l'ordinateur, soit au routeur d'un éventuel réseau local[49], soit directement au modem central du bâtiment (par exemple via wifi), puis par le câble du téléphone ou la fibre optique rejoindre le routeur du fournisseur d'accès à Internet[50] du quartier, qui va relayer notre demande à d'autres routeurs plus loin dans le réseau (via des fibres optiques haut débit), jusqu'au final atteindre le serveur hébergeant

[48] Pour plus d'infos: [https://en.wikipedia.org/wiki/ECHELON].
[49] Les réseaux locaux sont fréquents dans les grandes institutions, mais pas chez les particuliers.
[50] Le fournisseur d'accès est généralement une entreprise qui permet la connexion au réseau Internet contre de l'argent.

le site que l'on aimerait visiter. Des données peuvent ainsi quitter un ordinateur, voyager à travers la moitié de la terre et arriver à un autre ordinateur, en une fraction de secondes seulement.
Ensuite, à partir du moment où le serveur reçoit la demande d'informations, il va renvoyer une réponse. Mais la particularité de cette structure en réseau, fait que les données vont dans ce cas peut-être voyager par un chemin totalement différent pour retourner à nous. Cette manière flexible de transférer les données est une caractéristique importante qui contribue à faire d'Internet un outil aussi puissant. En effet, comme les données peuvent suivre de multiples voies, même si des parties entières du réseau sont surchargées, voire hors d'usage, l'information arrivera quand même à destination (avec peut-être un peu de retard). Ce grand avantage de l'Internet par rapport à d'autres moyens de (télé)communications (comme le téléphone) comporte aussi ses inconvénients. La surveillance des informations transitant par un point donné du réseau est ainsi grandement facilitée, puisqu'elle peut se faire aussi bien depuis l'immeuble d'à côté que depuis l'autre bout du monde.

9.1.2 Protocoles informatiques d'Internet

L'ensemble de l'infrastructure matérielle ne pourrait faire fonctionner un réseau à elle toute seule sans la deuxième composante de base d'Internet: les protocoles informatiques. Les protocoles sont des sortes de langages, un ensemble de règles décrivant comment des machines doivent communiquer et se comprendre dans un réseau informatique et comment les informations doivent transiter sur Internet. Sans des protocoles communs aux différentes machines interconnectées, elles ne seraient pas capables de se comprendre ou même d'envoyer des données de manière compréhensible.

Il existe divers protocoles sur Internet. Chaque protocole a des fonctions propres et, ensemble, ils fournissent un éventail de moyens permettant de répondre à la multiplicité des besoins du réseau.
Le langage de base partagé par tous les ordinateurs est l'Internet Protocol (IP). Voir: 9.3.2
Chaque machine connectée à Internet se voit attribuer une adresse IP unique, c'est comme ça qu'elle (et les flics) retrouve(nt) les autres machines à travers ce réseau massif.

Des protocoles réseau plus sophistiqués peuvent être superposés au protocole IP, en permettant différents types de communications sur Internet. Ces protocoles utilisent leur propre type d'adresse, distinctes des adresses IP.
Par exemple, les sites web dont on a déjà parlé plusieurs fois, utilisent un protocole spécifique appelé le HyperText Transfer Protocol (HTTP), littéralement «Protocole de Transfert HyperTexte». Pour ouvrir une page web en

HTTP, l'adresse du site web commencera par les lettres http, suivies de www (pour World Wide Web) comme dans: http://www.siteweb.net. Internet ayant été popularisé par l'apparition du World Wide Web, les deux sont parfois confondus par le public non averti. Le World Wide Web n'est pourtant que l'une des applications d'Internet.
Pour ce qui est des e-mails, c'est le protocole Simple Mail Transport Protocol (SMTP) qui est utilisé et les adresses e-mails correspondantes ressemblent à ça: MonAdresse@BoîteMail.net.
Pour finir, on peut encore citer le protocole sécurisé HTTPS (pour Hyper-Text Transfer Protocol Secure). C'est la combinaison du HTTP, avec une couche de cryptage. Par ce biais, il garantit théoriquement la confidentialité et l'intégrité des données envoyées et reçues. Il permet également (pas tout le temps !), de vérifier l'identité du site auquel on accède grâce à un certificat d'authentification émis par des organisations réputées fiables qui garantissent qu'on n'est pas tombé sur une fausse page web[51] malveillante. Généralement utilisé pour les transactions financières en ligne, il est aussi utilisé pour la consultation d'autres données confidentielles qui nous intéressent plus, comme le contenu des sites que l'on visite par exemple. Une fois de plus, la boîte à outils de Tails est bien fournie et propose cette fonctionnalité qui est même intégrée par défaut dans le Navigateur Tor via l'extension HTTPS Everywhere[52]. Cette extension permet pour de nombreux sites web, un cryptage bout-à-bout qui est un bon complément au cryptage partiel offert par Tor.

Voir: 9.4.5
Voir:10.3.1

9.2 Neutralité et gouvernance du Net

La neutralité du Net ou la neutralité du réseau décrit une politique égalitaire qui a beaucoup imprégné la popularisation d'Internet et qui vise à exclure toute discrimination à l'égard de la source, de la destination ou du contenu de l'information transmise sur le réseau. Mais de plus en plus, les manœuvres des pouvoirs en place tendent à mettre fin à cette ouverture caractéristique d'Internet.

C'est ce constat qui nous amène à parler de la gouvernance de l'Internet. En effet, même si ce réseau mondial n'est pas contrôlé par une seule entité, il n'en reste pas moins clair qu'à tous les niveaux, les classes dirigeantes se confrontent ou s'accordent pour s'octroyer une part du gâteau ou empêcher qu'on la leur reprenne. Le fait que les riches et les puissant-e-s tentent à tout prix de faire dominer leurs intérêts n'est en général pas nouveau. Mais

[51] On verra aussi que cette fonctionnalité est assez utile face au risque d'attaque du type «attaque de l'homme-du-milieu».

[52] Pour plus d'infos: [https://tails.boum.org/doc/anonymous_internet/Tor_Browser/index.fr.html].

dans le cas précis d'Internet, après des années de relative stagnation (ajustements ?), cette emprise sur l'évolution et l'usage d'un outil aussi profitable mais potentiellement dangereux qu'Internet, semble s'accélérer. Ça concerne en premier lieu la distribution inégalitaire des ressources Internet mais aussi des mesures comme la surveillance, le contrôle, jusqu'à la censure pure et simple de ce qui se passe sur ce réseau. Certaines de ces mesures sont abordées plus concrètement dans la suite du chapitre.

9.3 Des traces dans tous les réseaux

Naviguer sur Internet est probablement l'usage le plus risqué que l'on peut faire d'un ordinateur. Pratiquement chaque clic que l'on fait est enregistré, archivé et analysé par des ordinateurs quelque part dans le réseau afin de prévoir nos comportements de consommation ou de faire régner l'ordre établi. À propos des traces laissées en connexion par des ordinateurs en réseau, on peut dire que les problèmes rencontrés (éparpillement et difficulté d'effacement des traces) sont à peu près les mêmes que ceux détaillés précédemment pour un ordinateur hors-connexion, mais en pire. Dans ce cas, le nombre de traces risquant d'être laissées de manière persistante est démultiplié, d'un côté par le grand nombre de machines impliquées dans le traitement de nos données et de l'autre, par l'inaccessibilité de la plupart de ces machines.

Voir: 2.2

De plus, il est important d'introduire ici le concept d'identité numérique, qui prend beaucoup de sens quand on parle de réseaux mais dont l'influence dépasse largement ce contexte précis, comme le rappellera son utilisation régulière dans les chapitres à venir.
L'identité numérique peut être définie comme un lien technologique[53] entre une entité réelle (la personne) et une entité virtuelle (sa ou ses représentation(s) numérique(s), via des données numériques).

9.3.1 Historique, cache et cookies; des traces des réseaux sur son ordinateur

Avant d'aborder les différents types de traces qui vont demeurer sur des ordinateurs distants au fil des connexions, on va tout d'abord voir celles qui peuvent polluer la première machine concernée: l'ordinateur avec lequel on surfe. En effet, les réglages par défaut de nombreux navigateurs Internet, vont amener ces derniers à stocker sur le disque dur de nombreux souvenirs de leurs voyages comme: des cookies, des fichiers temporaires (cache), mais

[53] Une petite expérience intéressante en rapport à l'identité numérique: [http://www.anonymat.org/vostraces/index.php]. À tester avec et sans Tails et Tor.

aussi l'historique des pages consultées.
Comme nous le verrons à la fin du chapitre et, contrairement aux traces laissées en réseau, dans ce cas le problème est facilement évitable dans sa totalité. Il est possible d'essayer d'effacer ces traces mais le plus simple est de désactiver ou d'utiliser Tails qui désactive par défaut ce genre de comportement dangereux dans l'ordinateur.

Voyons maintenant plus en détail ce qu'il y a derrière ces termes:

- Premièrement, l'historique de navigation consiste en une liste chronologique des adresses des sites visités, qui est souvent conservée à notre intention par le navigateur.

- Souvent, le navigateur conserve également sur le disque dur une copie des pages visualisées récemment sous la forme de fichiers dits «temporaires»: c'est ce qu'on appelle le cache. La mémoire cache est un moyen utilisé pour optimiser les temps de chargement et désengorger le réseau. Si cette fonctionnalité est présente sur le navigateur et qu'elle n'est pas désactivée, lorsqu'on lance une requête, celui-ci effectue la requête mais lorsque son résultat arrive, il l'enregistre sur le disque en même temps qu'il le présente à l'écran. La fois suivante, si la même requête est lancée à nouveau, il ira simplement la lire là où elle est stockée sur le disque. On verra alors le résultat s'afficher beaucoup plus vite que s'il avait parcouru la distance réelle qui nous sépare du serveur. Bien pratique, mais salissant...

- Finalement, un cookie est un enregistrement d'informations effectué par le serveur dans de petits fichiers texte situés sur l'ordinateur client, informations que ce même serveur peut aller relire et modifier ultérieurement, pour en exploiter leur contenu. Les sites web utilisent la technique du cookie pour faire un suivi des internautes qui les consultent, le terme «suivi» pouvant aussi bien signifier «apporter une aide» (par exemple, pour éviter à l'internaute d'avoir à taper ses identifiants de messagerie à chaque fois), que du traçage (permettant au site web de savoir qu'il a affaire à un-e même internaute malgré des consultations espacées dans le temps) ou un profilage de l'internaute à des fins commerciales.
  Un cookie contient au minimum un identifiant unique, reconnu dans une base de données au niveau du serveur et qui permet à un site web de reconnaître un ordinateur à chaque visite. Cependant, le contenu de ces cookies peut être très complet et il est susceptible d'être enrichi à notre insu avec des données parfois très indiscrètes.

9.3.2 Adresses IP et autres logs; des traces laissées à tous les intermédiaires, depuis le réseau local et le fournisseur d'accès jusqu'aux routeurs et aux serveurs

L'adresse Internet ou adresse IP (Internet Protocol), est un des moyens les plus directs (mais on en verra malheureusement beaucoup d'autres) d'établir une identité numérique. Dans ce cas, d'établir via l'adresse IP, un lien entre une activité en réseau et un-e internaute.
Comme on l'a vu précédemment, l'adresse IP permet d'identifier de manière unique un ordinateur sur le réseau. Elle ne dépend pas de la machine connectée mais plutôt du lieu de connexion. Ainsi, un ordinateur portable se connectant depuis différents points d'accès se verra typiquement attribuer des adresses IP différentes. Cette attribution se fait de diverses manières, selon le type d'abonnement Internet. Pour une connexion de maison, l'ordinateur se verra souvent attribuer par le fournisseur d'accès une adresse différente à chaque connexion. On parle alors d'adresse IP dynamique. Pour une entreprise ou un organisme plus important (université), il est attribué des adresses IP fixes. Mais au final, ces différences importent peu, car de toute façon, le fournisseur d'accès Internet est tenu de conserver pour une durée d'un an (un minimum pour la plupart des pays) un registre des adresses IP qu'il a attribuées à chaque instant. De là, rien de plus facile pour des flics que d'accéder à ces données, pour ensuite identifier l'adresse précise du lieu de connexion et peut-être même l'internaute.

Quand on navigue sur Internet, chacun de nos faits et gestes, chacune de nos connexions est traduite en requêtes numériques qui sont transmises à travers tous les intermédiaires du réseau. Ok, ça on le savait, mais ce qui est plus troublant c'est qu'à chacune de ces étapes, des traces sont méticuleusement conservées dans un journal de bord des connexions, appelé aussi fichier de log ou tout simplement logs.

Pour comprendre le pourquoi du comment du fichage quasi systématique de nos activités sur Internet, il faut se rappeler une chose. Derrière chacune des machines relayant nos flux de données (depuis le routeur du fournisseur d'accès Internet, aux serveurs qui hébergent les données, en passant par la flopée de routeurs aux mains des opérateurs de réseaux), il y a des personnes bien réelles. Ce sont souvent les employé-e-s d'entreprises qui entretiennent ces machines et logiciels allumés et connectés 24 heures sur 24 à Internet et qui veillent à la bonne circulation sur le réseau. Le fait de faire des relevés de données relatives au trafic, peut être très utile à ces personnes pour pouvoir gérer ce trafic et réagir à la survenue d'éventuels problèmes. Par contre, le fait de stocker au long terme et à l'attention des flics, des milliards de logs

contenant plus d'informations que celles nécessaires à l'entretien purement technique du réseau, est une contrainte légale sous de nombreuses juridictions. C'est là que commence le fichage.

Le délai durant lequel les divers intermédiaires du réseau sont légalement tenus d'être en mesure de balancer nos logs aux autorités, varie selon les pays et leurs lois. Par exemple: République tchèque 2 mois, Allemagne 3 mois, Suisse 6 mois, France 1 an. De plus, il faut savoir que la plupart du temps ces mêmes lois interdisent d'informer les personnes concernées par ces procédures, ce qui est assez logique quand on parle de surveillance.

Donc, de manière similaire aux cookies, ces logs permettent d'établir à notre insu des profils de navigation. Leur contenu varie, mais une chose est claire: quel que soit le type d'infos retenues contre nous dans ce contexte, toutes visent à rendre possible l'établissement d'une correspondance entre nous (nos cordonnées réelles d'abonnement) et nos activités sur Internet. Leur utilisation et leur conservation sont par conséquent utiles voire essentielles dans un nombre croissant de cas de répression s'appuyant typiquement sur les informations suivantes:

Voir: 9.3.3

- Un historique des logs permettant d'identifier l'internaute (adresse IP, adresse MAC ou adresse de courrier électronique par exemple).
- Un historique des sites auxquels chaque adresse IP s'est connectée ou des adresses e-mails qu'elle a contactées (pour les fournisseurs d'accès) et un historique des pages auxquelles chaque adresse IP a accédé (pour les serveurs), un historique de nos recherches associé à chaque adresse IP (nombreux moteurs de recherches).
- Les caractéristiques techniques de l'utilisation des services comme: la date, l'heure, la durée et le volume de chaque communication, ainsi que les informations relatives au routage comme: le protocole informatique utilisé, l'origine et la destination des données transitant par les machines au début et la fin de l'échange.

En pratique, quelques zones de flou subsistent parfois sur le contenu précis des logs qui est légalement exigé. Mais en général, on constate que ces directives sont appliquées très docilement par la majorité des fournisseur d'accès, serveurs et autres routeurs, dont les intérêts sont avant tout commerciaux. Collaborer avec les keufs ne pose évidement pas beaucoup de soucis à ces baltringues, dont la préoccupation principale est de pouvoir continuer leur exploitation à l'abri des amendes et des éventuelles interdictions d'exercer, en cas de non-respect de la réglementation.

Heureusement, il existe une poignée de serveurs qui résistent à cette logique et ont une position radicale par rapport à l'anonymat et la confidentialité des personnes sur Internet. Les logs ne sont pas conservés et les autres données personnelles hébergées sur le serveur ne sont pas livrées aux flics, quoi qu'en disent les lois.

Voir: 9.3.4

On peut notamment citer des collectifs anarchistes très partageurs comme riseup.net, boum.org, autistici.org ou immerda.ch[54] qui n'ont de cesse de révolutionner des outils essentiels d'Internet. Ils offrent par exemple des possibilités de messageries e-mail et d'hébergement de sites web dans un esprit clair d'opposition à toute surveillance informatique et récupération commerciale. D'ailleurs, la plupart de ces serveurs ne doivent leur survie qu'à des dons et des caisses de soutien qu'il est assez cool d'alimenter si on veut que ça continue.

Voir: 8.2.1

Pour finir, un petit extrait[55] de ce que le collectif riseup.net dit à propos de son projet:

"Peut-on compter sur des serveurs e-mail commerciaux pour défendre la confidentialité de nos communications par e-mail ? Non seulement, ces derniers scannent et enregistrent systématiquement le contenu des messages pour variété d'usages, mais ils répondent aussi aux attentes des gouvernements qui répriment les libertés numériques et font l'impasse sur une politique stricte à propos de l'intimité de leur client-e-s. Nous pensons qu'il est vital que les infrastructures essentielles de communication soient contrôlées par en bas et non pas, par des grosses sociétés et les gouvernements."

9.3.3 L'adresse MAC; une trace spécifiquement laissée sur le réseau local et chez le fournisseur d'accès

Chaque appareil disposant d'une interface réseau (ordinateur, smartphone, console, tablette, etc.) possède un numéro d'identification unique au monde qui est la seule donnée qui identifie complètement le matériel se connectant au réseau Internet. Ce numéro de série qui est défini pour chaque interface réseau depuis l'usine, est appelé adresse Ethernet ou adresse MAC (Media Access Control, rien à voir avec Macintosh).

Donc, de manière similaire à l'adresse IP, l'adresse MAC permet l'établissement d'une identité numérique. Mais contrairement à l'adresse IP, qui identifie sur Internet l'endroit par où se fait la connexion, l'adresse MAC identifie sur le réseau local la machine par laquelle se fait la connexion. Ainsi, un ordinateur portable se connectant à Internet depuis différents points d'accès, se verra typiquement attribuer des adresses IP différentes, mais donnera à

Voir: 9.3.2

[54] En fait, il en existe plein d'autres aux quatre coins du monde. Pour plus d'infos: [https://www.riseup.net/en/radical-servers].

[55] Pour plus d'infos: [https://www.riseup.net/en/about-us].

chaque fois la même adresse MAC. Cette adresse sert donc uniquement à identifier les ordinateurs de manière locale. Comme on l'a vu dans le point précédent, elle fait partie des logs fréquents à cette échelle du réseau. Elle ne transite pas sur Internet, car au pire elle est transmise jusqu'au fournisseur d'accès Internet, mais habituellement elle ne va pas au delà des intermédiaires présents dans le réseau local (par exemple le modem wifi domestique ou le routeur principal dans une bibliothèque). Cependant, il faut savoir que lors de l'utilisation du wifi, n'importe qui dans le périmètre de l'interface wifi peut voir notre adresse MAC, sans pour cela avoir besoin de se connecter au même réseau !
L'unicité de cette adresse est problématique pour deux raisons principales:

- Elle peut être utilisée pour surveiller un ordinateur se connectant à un réseau donné[56] (quand, pendant combien de temps, à quelle fréquence). Et de là, éventuellement identifier un-e propriétaire (sauf si l'ordi a été volé en magasin), si l'adversaire est en mesure de faire correspondre l'adresse MAC avec des registres de ventes (un lien est souvent possible entre le fabriquant du matériel et la vente au détail).

- Elle peut aussi servir à établir un historique et une carte d'utilisation d'une machine donnée s'étant connectée depuis plusieurs lieux (un peu comme la géolocalisation des téléphones portables). Ce scénario demande une investigation de grande envergure, mais peut en dire long sur les personnes qui utilisent la machine en question.

Heureusement, l'adresse MAC va nous poser moins de soucis que l'adresse IP car contrairement à cette dernière, elle ne voyage d'une part pas sur le net au delà de l'échelle locale et d'autre part, on verra qu'il est possible de
Voir: 11.1 la falsifier avec le logiciel MAC Changer !

9.3.4 Données client-e-s et variables d'environnement; des traces spécifiquement laissées dans les serveurs

Les données client-e-s comprennent toutes les informations qui, contrairement aux logs sont laissées de manière consciente sur des serveurs à partir d'un ordinateur client. Pourtant, de manière similaire aux logs, ces données peuvent être retenues contre nous en faisant l'objet d'une surveillance étatique, bénéficiant de la collaboration de nombreux serveurs.
Ainsi, en plus de tous les logs, les serveurs sont souvent légalement tenus de conserver pour une durée minimale (par exemple 1 an en fRance[57]) des

[56] Un cas intéressant d'exploitation d'adresses MAC par les flics: [http://www.theregister.co.uk/2010/06/29/spy_ring_tech/].
[57] Plus d'infos sur la législation française: [http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023646013&categorieLien=id].

éléments comme: les fichiers stockés par les client-e-s (e-mails, images, documents en tout genre), les mots de passe et les données d'inscriptions. Même les données d'un compte fermé sur un site web, doivent souvent être conservées pour la même durée à partir de la demande de résiliation.
De plus, il est possible que des copies de nos e-mails soient éparpillées dans les mémoires des ordinateurs de certain-e-s de nos correspondant-e-s moins prudent-e-s que nous. Finalement, il est bon de garder à l'esprit le problème récurrent que représente l'effacement réel des données et qui fait, qu'il est tout à fait imaginable que des données puissent être récupérées par des flics, même longtemps après leur «effacement» par le serveur.
Heureusement comme on l'a déjà vu précédemment, les mêmes serveurs radicaux qui faisaient de la résistance concernant la conservation des logs, appliquent souvent une politique de confidentialité très stricte à propos des données client-e-s (cryptage, effacement réel). Encore une chose à ce propos: bien qu'il existe souvent des collectifs tenant des serveurs très fiables proche de chez soi, le fait d'utiliser des serveurs géographiquement très éloignés (autre continent, autres juridictions), rend l'accès aux données plus difficile pour les flics locaux souvent tentés par une perquisition.

Parlons maintenant des variables d'environnement, qui sont un autre type de traces laissées sur les serveurs pouvant être exploitées pour nous identifier. Les navigateurs Internet (Firefox, Safari, Internet Explorer et même le Navigateur Tor) ont par défaut accès à certaines informations concernant la configuration de l'ordinateur sur lequel ils fonctionnent. On appelle ces informations les variables d'environnement. Les navigateurs Internet transmettent ces informations aux serveurs des sites que l'on visite, qui les utilisent de manière standard pour adapter leur contenu à leur visiteurs-euses en prenant en compte les éléments propres à chaque configuration. Bref, on pourrait aller jusqu'à dire qu'elles sont, jusqu'à un certain point, nécessaires au bon fonctionnement d'Internet.
Voir:10.3.2
Aucune de ces données, prise séparément, n'est suffisante pour nous identifier. Par contre, ce qui est problématique c'est que, prises ensemble, des données comme: la version du navigateur, la langue, le système d'exploitation, le fuseau horaire, la police d'écriture ou la liste des extensions (plugins), permettent de faire émerger une image plus claire. Si claire, qu'elle peut carrément constituer un portrait unique, une empreinte de chaque internaute et contribuer ainsi à l'établissement de son identité numérique[58]. Cela signifie que nombre d'internautes prenant des précautions basiques comme désac-

[58]Des expériences très instructives à ce propos: [https://panopticlick.eff.org/], [https://www.eff.org/press/archives/2010/05/13], [http://assiste.com.free.fr/p/qui_etes_vous/qui_etes_vous_vos_traces.php] et [http://ip-check.info/?lang=fr].

tiver les cookies, ou nettoyer l'historique de navigation régulièrement, sont beaucoup moins anonymes qu'ils ou elles peuvent le croire.
Alors, que peut-on faire pour se rendre moins identifiable ? Eh bien, le fait de désactiver les cookies et de rendre son navigateur Internet le moins personnalisé possible en désinstallant toutes extensions et autres polices d'écriture spéciales est déjà un bon début. Mais ce qui joue le plus grand rôle, est d'empêcher l'action des scripts. Dans le contexte du web, un script est un programme informatique intégré à la page web et exécuté par le navigateur. Ces scripts, dont les plus dangereux sont le Javascript et le Flash, portent la responsabilité de la transmission aux serveurs de l'essentiel des variables d'environnement !

9.4 Surveillance des ordinateurs en réseau

Au delà des nombreuses traces qu'on laisse inévitablement par nous-même dans les réseaux, le fait que leur récupération voire leur interception en toute discrétion soient grandement facilitées par l'organisation en réseau, n'est pas pour arranger les choses. On va donc voir ici les principaux pièges qui peuvent être tendus au détour des réseaux par divers ennemis de la liberté.

9.4.1 Données récupérées à postériori chez tous les intermédiaires du réseau

On l'a vu dans le point précédant, quasiment tous les intermédiaires d'Internet sont légalement tenus de conserver et de livrer aux flics des traces de nos activités en réseau. Ainsi, l'exploitation des mines d'informations que représentent les logs ou les données client-e-s est à la portée de nombreux services de police, après quelques formalités administratives (demande à des instances judiciaires). Comme ce sera aussi le cas pour la surveillance en temps réel, les choses se compliquent un peu quand les données sont détenues dans d'autres pays, avec d'autres juridictions. Mais avec le renforcement constant de la collaboration policière, une surveillance informatique au niveau international est tout à fait envisageable.

9.4.2 Données interceptées en temps réel par la surveillance de messageries e-mail

Dans certains cas, la flicaille se permet d'intercepter durant leur transmission, les échanges d'e-mails d'une adresse donnée. Depuis le début des années 2000, il y une grande recrudescence de ce type de mesures, qui restent cependant encore moins fréquentes que les interceptions téléphoniques. On peut aussi relever qu'en général, la surveillance des télécommunications en temps réel est plus coûteuse, plus difficile à obtenir d'un juge et donc réservée à des

affaires jugées prioritaires.
Finalement, on ne répétera jamais assez que pour nos communications confidentielles, il est préférable dans tous les cas d'utiliser une messagerie comme riseup.net qui est plus fiable et moins vénale que des merdes style gmail.

Voir: 8.2.1
Voir: 9.3.2

9.4.3 Données interceptées en temps réel par la surveillance d'un accès Internet

Une des techniques de surveillance informatique les plus efficaces qui soient, consiste à surveiller, au niveau du fournisseur d'accès, tous les flux Internet qui entrent et sortent d'une maison. Cela comporte tout: des sites visités aux échanges d'e-mails, en passant par les téléchargements, les conversations chat ou la téléphonie par Internet. Cette mesure, proche de la mise sous écoute d'une ligne téléphonique, est parfois appelée interception IP.
De manière similaire, il est aussi possible d'intercepter des données transitant localement par wifi. Cependant, cette mesure est moins fréquente car elle demande de dissimuler un récepteur à proximité du lieu surveillé.

9.4.4 Données interceptées en temps réel par une surveillance large du trafic sur les réseaux

Des moyens considérables sont mis en œuvre, par les gouvernements des pays les plus riches et puissants, pour mettre sur pied des programmes de surveillance à large échelle des télécommunications.
L'existence de tels programmes est avérée[59] depuis quelques années, le plus connu est le réseau Echelon qui est un système mondial d'interception des communications privées et publiques élaboré par les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande. Cependant, des structures plus modestes prolifèrent à des échelles nationales comme le nouveau projet de loi relatif au renseignement en France ou le programme Onyx en Suisse.
Contrairement aux mesures de surveillance vues précédemment, il ne s'agit dans ce cas pas du tout d'investigations ciblées mais au contraire de la tentative de détecter des cibles potentielles au milieu du flot monstrueux et continuel d'informations qui caractérise nos sociétés. Les portions du réseau parmi les plus visées par ce type de surveillance sont sans aucun doute les dorsales Internet vues précédemment. Ce sont des points d'observation privilégiés, puisqu'ils concentrent le trafic d'informations de régions entières. Comme la quantité de données à traiter est beaucoup trop grande pour être analysée par des humain-e-s, ce sont des ordinateurs automatisés qui se chargent de ce

Voir: 9.1.1

[59] La fuite de plus de 10'000 documents secrets du gouvernement étasunien occasionnée, en 2013, par Edward Snowden, en est une confirmation récente. Pour plus d'infos: [https://fr.wikipedia.org/wiki/Révélations_d'Edward_Snowden].

travail. Ils interceptent le trafic et le filtrent afin de rapporter à des personnes indiscrètes les morceaux choisis concernant des mots, phrases, fréquentations de sites et communications d'individus ou de groupes considérés du coup comme suspects.

9.4.5 Données interceptées en temps réel par une «attaque de l'homme-du-milieu»

Une «attaque de l'homme-du-milieu» (man in the middle) est une forme d'écoute active durant laquelle l'attaquant-e se positionne entre l'ordinateur client et le serveur et relaie le trafic entre eux, en laissant traîner ses oreilles. Il est par exemple ainsi possible, de détourner et surveiller une communication à l'origine sécurisée avec le protocole HTTPS. Il suffit de rediriger l'internaute vers une copie de la page web visitée où les liens https: ont étés discrètement changés en http:. Si la combine n'est pas détectée, l'internaute continuera à croire qu'il ou elle utilise une connexion cryptée HTTPS, alors qu'en fait, ses informations voyageront en clair via le protocole surveillé HTTP. Ce type d'attaque reposant sur le trucage du protocole informatique est assez fréquent, car il permet de rendre vulnérable à une attaque de l'homme-du-milieu à peu près n'importe quel type de communication sur Internet. Pour éviter ce risque, le protocole HTTPS effectue souvent l'authentification des pages web visitées, ce qui rend beaucoup plus difficile leur falsification.

9.4.6 Données interceptées en temps réel et à postériori par une surveillance due à l'utilisation de logiciels espions

Les logiciels espions comptent parmi les moyens de surveillance les plus difficiles à contrer. La menace qu'ils représentent et les différentes défenses qu'on peut leur opposer sont abordées à plusieurs endroits de ce texte.

Voir: 3.2.2
Voir: 12.1
Voir: 15.1

9.5 Comment ne pas laisser ses traces dans les réseaux

On renvoie ici en quelques mots aux chapitres pratiques présentant des outils qui peuvent aider à éviter de se faire trop avoir sur les réseaux:

- Échapper aux impasses dues aux cookies, au cache et aux variables d'environnement dangereusement transmises par divers scripts, est assez facile dans Tails grâce à la préconfiguration du Navigateur Tor et de son extension Torbutton. Plus de détails au point 10.3.2.

- Pour protéger son anonymat, en ne divulguant pas son adresse IP à tout va, l'utilisation du réseau anonymisé Tor peut être d'une grande utilité. Voir le chapitre 10.

- Pour protéger son anonymat, en ne divulguant pas son adresse MAC, il y a le logiciel MAC Changer qui est présenté au chapitre 11.

- Pour protéger la confidentialité de ses données sur Internet, on peut conseiller l'utilisation de l'extension HTTPS Everywhere présentée au point 10.3.1, le cryptage d'e-mails avec PGP vu au chapitre 7 et le recours à une messagerie instantanée cryptée vue au chapitre 8.

10 Surfer sur Internet de manière anonyme et confidentielle avec Tor

10.1 Qu'est-ce que Tor

TOR, The Onion Router (littéralement: le routage en oignon) est un réseau mondial décentralisé de relais Internet (routeurs), organisés en couches appelées nœuds (proxy) de l'oignon. Ils transmettent de manière anonyme (notre adresse IP n'est pas transmise) et confidentielle (cryptée) des flux d'information sur Internet.
Voir: 9.1.1
Donc, au lieu d'une connexion quasi directe entre un ordinateur et les sites que l'on visite, Tor fait rebondir nos communications sur un réseau crypté de relais maintenus par des volontaires partout dans le monde. Ceci nous protège doublement des pourritures avides de surveillance et de contrôle. Il empêche tout d'abord qu'une tierce personne scrutant notre connexion Internet connaisse les sites que l'on visite. Réciproquement, à partir des sites que l'on visite, il empêche de connaître notre position géographique, puisque l'adresse IP identifiable sur les serveurs ne sera pas la nôtre mais celle du dernier relais. Finalement, comme les nœuds sont localisés dans le monde entier, alors même qu'une législation à l'échelle d'un seul pays est déjà difficile à mettre en œuvre, certaines personnes qualifient ce système de «réseaux d'impunité». D'où ce genre de sorties sur Wikipedia[60]:
"(...)on ne saurait ignorer le risque que des actes illicites soient, à l'aide de Tor, commis sans qu'aucune archive ne permette d'identifier les éventuels auteurs d'infractions."

Pour finir, précisons que dans Tails tous les programmes sont configurés par défaut pour effectuer leur connexion Internet via le réseau Tor en utilisant le programme de liaison Vidalia. De plus, toutes les tentatives de connexion contournant Tor sont bloquées.

[60]Pour plus d'infos: [https://fr.wikipedia.org/wiki/Tor_(réseau)].

10.2 Précisions sur le fonctionnement d'un circuit Tor

Comme on l'a vu avant, l'intérêt du réseau Tor réside principalement dans son mode de routage et dans sa méthode de chiffrement. On va approfondir ces deux aspects[61]:
Tout d'abord le routage. C'est le mécanisme par lequel des chemins sont sélectionnés dans un réseau afin de construire un circuit qui va acheminer les données d'un-e expéditeur-trice jusqu'à un-e ou plusieurs destinataires.
À chaque connexion à Internet au travers du réseau Tor, un chemin aléatoire est constitué à partir de la liste des nœuds Tor disponibles. Au sein de ce circuit chacun des trois nœuds empruntés par les données transitant via le réseau Tor connaît uniquement le nœud précédent et le nœud suivant, sans en savoir plus. Le premier nœud du circuit connaîtra notre adresse IP. Mais celle-ci disparaît dès le deuxième nœud, qui ne connaîtra que l'adresse IP du premier nœud et du troisième, qui lui, se connectera finalement au serveur visité par l'internaute. Pour brouiller encore plus les traces, les différents nœuds de transit utilisés sont changés régulièrement et automatiquement, au cours d'une même connexion à Tor. En résumé, du fait que le circuit Tor emprunte un chemin aléatoire au travers de plusieurs relais perdant notre trace au fur et à mesure, aucune personne espionnant en un point unique du circuit n'est en mesure de dire d'où viennent les données et où elles vont. De là, connaître le chemin complet emprunté par l'internaute malgré cette traçabilité des connexions extrêmement difficile, demanderait des moyens gigantesques[62].
On peut encore noter que, puisque Tor repose sur une communauté d'internautes engagé-e-s qui offre des machines capables de relayer le trafic des autres personnes, tout le monde peut donc:

- Profiter des relais installés par les autres utilisateurs-trices.
- Mais aussi installer un nœud sur sa machine et participer au développement du réseau Tor.

Maintenant attaquons l'aspect du cryptage. Les données échangées, ainsi que les infos indiquant le chemin entre chaque nœud, sont cryptées en une succession de couches (d'où l'image de l'oignon). Elles sont alors décryptées au fur et à mesure du circuit, en fournissant à chaque nœud l'info nécessaire pour la connexion au relais suivant. Par contre, cette succession de couches ne permet à aucun nœud du circuit, à l'exception du dernier, de déchiffrer les données transmises en elles-mêmes. C'est donc le dernier maillon de la

[61] Les compléments théoriques qui suivent, bien qu'intéressants pour comprendre les limites de Tor, ne sont pas nécessaires pour une utilisation basique de cet outil. Pour plus d'infos: [`http://tor.hermetix.org/overview.html.fr`].

[62] Des failles sont néamoins imaginables, comme nous le verrons au prochain point.

chaîne qui déchiffre les données en clair avant de les envoyer au serveur ciblé par l'internaute.
Donc le fait qu'avec Tor, les données de même que les infos du circuit, soient cryptées à partir du moment où elles sortent de l'ordinateur peut se révéler bien pratique, si on pense par exemple à la surveillance de l'accès Internet d'une maison. Le flic indiscret ne sera ni en mesure de lire les données, ni même de savoir quel est le premier nœud. Par contre, il pourra savoir qu'on utilise Tor !

10.3 Limites de Tor et parades

10.3.1 Failles possibles de Tor

Comme on l'a déjà vu pour Tails, il est probable, voire même avéré que les flics mettent en œuvre des attaques spécifiques ciblant des outils de défense spécifiques, dont Tor est un bel exemple. À ce stade, il peut donc être intéressant d'avoir une petite idée de ces attaques et des erreurs qui pourraient menacer l'anonymat visé par Tor[63].

- Attaques du type «corrélation bout-à-bout»:
  Tor nous protège quand un-e adversaire essaye de déterminer notre adresse IP à partir d'un site qu'on a visité, mais ne protège pas contre des attaques dites de confirmation de trafic (aussi connues sous le nom de corrélation bout-à-bout). Celles-ci ont lieu lorsqu'un-e adversaire essaye de confirmer une hypothèse en surveillant aux bons endroits dans le réseau, puis en faisant la corrélation.
  Pour cette attaque, l'adversaire doit être capable de mesurer le trafic qui entre et qui sort des nombreux ordinateurs du réseau Tor. En étudiant, par exemple, le timing et le volume d'informations des différentes communications à travers ce réseau, il serait statistiquement possible d'identifier n'importe quel circuit Tor et du coup de relier la personne qui utilise Tor à son serveur destinataire.
  Maintenant, est-ce qu'une telle surveillance globale est envisageable ? Difficile à dire, mais on ne peut pas exclure qu'une ou plusieurs institutions de surveillance dans le monde ne soient pas si loin d'en avoir les moyens. Quoi qu'il en soit et sans aller aussi loin, une version plus ciblée et moins exigeante de cette attaque est d'ores et déjà à la portée d'organisations répressives plus modestes. En effet, des flics surveillant l'accès Internet d'une maison pourraient, malgré l'utilisation de Tor, établir un lien entre des données cryptées sortant et ces mêmes données entrant dans un site Internet, à condition qu'il soit lui aussi surveillé.

[63] Pour plus d'infos: [https://tails.boum.org/doc/about/warning/index.fr.html#identities].

Un moyen permettant de déjouer ce type de surveillance, est d'accéder à Internet via un ordinateur anonyme dans un lieu public (avec toutes les précautions supplémentaires que cela impose). Donc, malgré Tor, il faut rigoureusement éviter de publier, de rendre publiques, des choses compromettantes sur Internet depuis sa maison, si on pense qu'elle est susceptible d'être surveillée !

Voir: 3.2.2

- Attaque de type «attaque de l'homme-du-milieu»:
  D'un côté, en procurant l'anonymat, Tor rend compliquée une attaque du type homme-du-milieu qui vise quelqu'un-e en particulier. Mais d'un autre côté, Tor rend plus facile pour des gens ou des organisations qui font tourner des nœuds de sortie, d'effectuer des attaques de ce type à grande échelle, ou qui ciblent un serveur spécifique, et par là les utilisateurs-trices de Tor en particulier.
  Pour se protéger de telles attaques, on peut utiliser le protocole HTTPS.

Voir: 9.4.5
Voir: 9.1.2

- Attaque par identification des variables d'environnement:
  Dans Tails, le programme par défaut de navigation sur Internet, appelé Navigateur Tor est configuré par défaut pour surfer sur le réseau Tor en laissant le minimum d'informations, voire de fausses informations. Cependant, en voyant les résultats d'un site dont on a déjà parlé[64] et qui analyse les variables d'environnement de Tails depuis Tor, on pourrait faussement conclure que Tor est inefficace pour protéger notre anonymat par ce biais. Mais la situation n'est pas aussi mauvaise qu'on pourrait le croire car, en fait, il n'y a rien de surprenant à ce que les internautes utilisant Tor se distinguent du reste du web[65]. Comme on le verra, Tor est conçu pour faire que les internautes utilisant Tor semblent indistinguables entre eux, mais pas pour les faire ressembler au reste du web.
  En faisant ça, Tor ne trahit aucunement une identité numérique particulière. Au contraire, il arrive à instaurer un anonymat collectif, en nous dissimulant parmi les centaines de milliers d'autres membres de son réseau. Et c'est déjà pas mal !

Voir: 9.3.4
Voir:10.3.2

- Attaque par un logiciel espion:
  Une telle attaque ciblée serait en mesure de trahir notre vraie adresse IP, quel que soit le labyrinthe de rebonds et de cryptage présents entre l'attaquant-e et le système tentant de surfer anonymement. La seule parade véritablement efficace contre ce genre de péril est d'utiliser Tor depuis un ordinateur anonyme.

Voir: 3.2.2

[64] Pour plus d'infos: [https://panopticlick.eff.org/].

[65] Pour plus d'infos: [https://blog.torproject.org/blog/effs-panopticlick-and-tor button].

Pour finir, il peut être utile d'avoir à l'esprit certaines erreurs que l'on peut facilement faire si l'on comprend mal le fonctionnement de Tor. Notamment si on croit à tort que Tor fait certaines choses qu'en réalité il ne fait pas.

- Erreur d'identification contextuelle:
  Derrière le terme d'identification ou d'identité contextuelle, il y a l'idée selon laquelle l'identification d'une personne peut se faire sans passer par une adresse IP (si on parle d'informatique) mais en prenant en compte un faisceau d'indices fournis par le contexte dans lequel on utilise Internet. L'identité contextuelle est au sens large, une sorte d'identité numérique. Ainsi, il est généralement déconseillé d'utiliser la même session de Tor pour effectuer deux tâches, ou pour endosser deux identités contextuelles, qu'on désire conserver séparées l'une de l'autre. Par exemple se connecter à une adresse e-mail d'habitude visitée sans Tor (ou pire... à son nom) et ensuite espérer publier anonymement un communiqué sur le web.
  Voir: 9.3
  Comme détaillé par la suite, la solution à ce problème est d'éteindre et de redémarrer Tails (et pas seulement Tor !), à chaque fois qu'on utilise une nouvelle identité que l'on veut réellement séparer des autres. De plus, il est très important de ne pas laisser sa session de Tails ouverte après utilisation, afin que personne ne soit tenté-e de la réutiliser pour d'autres usages auxquels on n'aimerait pas être relié-e. Réciproquement, il faut éviter d'utiliser pour des activités en réseau que l'on veut anonymes, une session ouverte par une autre personne afin d'y faire on ne sait trop quoi (par exemple visiter une messagerie personnelle).
  Voir:10.4.2

- Erreur d'identification textuelle:
  On l'a vu, Tor empêche de savoir où on est, mais ne crypte pas complètement les communications. En effet, puisque les nœuds de sortie Tor transmettent les données en clair sur la dernière partie du circuit, Tor ne garantit pas la confidentialité des donnée par cryptage sur l'ensemble du circuit ! Si ces nœuds de sortie sont aux mains de personnes malveillantes, ils permettent donc de jeter un œil au contenu des communications. D'où l'idée d'identification textuelle; si on commet l'erreur de se contenter de Tor pour transmettre des données identifiables en elles-mêmes (par exemple des e-mails non cryptés contenant des noms de personnes ou de lieux).
  Voir: 10.2
  Pour dépasser cela et transmettre des données de manière confidentielle tout au long du circuit, en plus de Tor, on doit utiliser un programme de chiffrement bout-à-bout. Tails comprend plusieurs logiciels qui permettent cela, pour la navigation sur des sites web (HTTPS Everywhere), envoyer des e-mails (OpenPGP), ou bien pour communiquer avec une messagerie instantanée (Pidgin et OTR).
  Voir:10.3.2
  Voir: 7.1
  Voir: 8.1

- Finalement, Tor ne cache absolument pas le fait qu'on est en train de l'utiliser (et probablement Tails). Le fournisseur d'accès à Internet ou l'administrateur-trice du réseau local peut donc voir qu'on se connecte à un relais Tor, et pas à un serveur web normal par exemple. Du coup, utiliser Tor fait qu'on ne ressemble pas à un-e utilisateur-trice lambda d'Internet. C'est un peu la même problématique que celle qui est soulevée par le fait de se masquer à certaine occasions; *«est-ce qu'il est préférable qu'on puisse reconnaître mon visage, plutôt qu'on puisse reconnaître que je porte un masque ?»*
  Cela dépend des cas. Mieux vaut peut-être s'abstenir d'utiliser Tor et Internet tout court, dans certains États qui vont jusqu'à réprimer leur utilisation même, ou dans le scénario vu précédemment qui imagine que de gros moyens puissent être mis en oeuvre pour viser un contrôle global du réseau Tor.
  Mais en dehors de ces contextes on peut considérer le fait que Tor trahisse sa présence comme un moindre mal, car c'est bien une des seules informations qu'il laisse filtrer.

10.3.2 Limitations d'utilisation de Tor et du Navigateur Tor

Dans ce point, il est question de certaines limitations d'utilisation qui peuvent être perçues par rapport à la navigation traditionnelle sur Internet. Ces désagréments ne sont rien d'autre que les conséquences découlant des nombreux avantages apportés par un accès à l'Internet plus anonyme et confidentiel. Les changements les plus flagrants sont:

- Vitesse:
  La navigation Internet sous Tor est un peu plus lente que d'habitude. Ceci est dû à l'architecture spéciale du réseau Tor.

- Filtrage des pages visitées par Torbutton:
  Tor seul, n'est pas suffisant pour protéger l'anonymat et la confidentialité lorsqu'on surfe sur le web. La plupart des navigateurs Internet, tels que Firefox utilisent des fonctionnalités comme JavaScript, Adobe Flash, ou des cookies qui ont montré qu'ils pouvaient briser l'anonymat visé par le réseau Tor. Dans Tails, la désactivation par défaut de toutes ces fonctionnalités dangereuses au sein du Navigateur Tor, est contrôlée par une extension nommée Torbutton. Mais cela a un prix: certains sites peuvent ne pas fonctionner comme d'habitude. Le blocage partiel de JavaScript (NoScript)[66] peut altérer l'affichage des pages, le blocage

Voir: 9.3

[66] Pour plus d'infos: [https://tails.boum.org/doc/anonymous_internet/Tor_Browser/index.fr.html].

d'Adobe Flash (Flashblock)[67] empêche la lecture online de certaines vidéos en streaming.

- Blocage de Tor:
  Il arrive que certains points d'accès Internet publics (principalement accessibles en wifi) comme des cybercafés, bibliothèques, aéroports, hôtels, ou universités, nécessitent de s'identifier pour accéder à Internet et rendent ainsi impossible l'utilisation du réseau Tor. Le fait de trouver un moyen de se connecter à ces accès Internet par le câble, permet souvent de contourner ce problème.
  De plus, de rares sites web refusent certaines demandes venant d'un nœud Tor. Par exemple Wikipédia, n'accepte plus de publications anonymes venant de Tor... Aberrant.

10.4 Utiliser Tor pour surfer sur Internet de manière anonyme et confidentielle

Dans Tails, Tor est installé et correctement configuré par défaut. Il est important d'utiliser la dernière version de Tails, qui elle-même utilise la dernière version de Tor.

Voir: 3.4

10.4.1 Lancer Tor

Dans Tails, le lancement de Tor, se fait automatiquement dès que l'ordinateur se connecte à un accès Internet. La connexion à Internet se fait par l'**Applet NetworkManager**, qui est disponible via une icône représentant deux écrans d'ordinateur, dans la barre d'icônes en haut à droite de l'écran. Ensuite, l'établissement du circuit Tor peut prendre entre 30 secondes et 2 minutes. Une fois que la connexion est établie, Tails ouvre automatiquement une fenêtre indiquant **Tor est prêt** et on peut voir apparaître dans la barre d'icônes en haut à droite de l'écran, le petit oignon jaune, puis vert du panneau de contrôle de Tor, appelé **Vidalia**.
Ensuite, pour surfer sur Internet via Tor, il faut ouvrir le **Navigateur Tor**, qui est accessible via le menu **Applications ▷ Internet ▷ Démarre le navigateur Tor**.

10.4.2 Changer «d'identité» en cours d'utilisation

Actuellement, la seule manière satisfaisante de changer d'identité contextuelle en cours d'utilisation, consiste à éteindre et redémarrer Tails (et pas seulement Tor !).

Voir:10.3.1

Pour finir ce point, une petite mise en garde face à un outil assez foireux: le

[67] Pour plus d'infos: [https://tails.boum.org/support/faq/index.en.html#index].

bouton **Utiliser une nouvelle identité**, qui est disponible dans le panneau de contrôle de Tor (**Vidalia**), en double-cliquant sur le petit oignon vert, dans la barre d'icônes en haut à droite de l'écran. Il oblige Tor à utiliser un nouveau parcours mais uniquement pour les nouvelles connexions, les connexions déjà existantes peuvent rester ouvertes[68]. Cette fonctionnalité de **Vidalia** n'est donc pas une solution pour effectivement séparer différentes identités contextuelles !

11 Modifier son adresse MAC avec MAC Changer

11.1 Qu'est-ce que MAC Changer

MAC Changer est un programme présent par défaut dans Tails et qui permet de remplacer, uniquement pour la durée d'une session de travail (rien de définitif), l'adresse MAC des interfaces réseau de son ordinateur par des valeurs aléatoires.

Voir: 9.3.3

Donc dans Tails, à moins de le demander spécifiquement, les adresses MAC de l'ensemble des interfaces réseau (filaire ou wifi) sont toujours falsifiées, et ceci avant même qu'elles ne soient activées et puissent être communiquées dans le réseau. C'est pourquoi MAC Changer agit aussi bien sur les interfaces réseau déjà présentes à l'ouverture de la session de travail de Tails (par exemple une carte réseau pour la connexion par câble interne à l'ordinateur), que sur celles qui sont rajoutées en cours de session (par exemple quand on branche une antenne wifi USB).

Cette falsification des adresses MAC effectuée par MAC Changer, en dissimulant les numéros de série des nos interfaces réseau, permet jusqu'à un certain point, de dissimuler aussi notre identité dans un réseau local !
Par conséquent modifier ainsi son adresse MAC, peut s'avérer très pertinent à chaque fois que l'on se connecte depuis un ordinateur personnel à un réseau auquel on ne fait pas confiance ou auquel on ne veut pas être relié via une adresse MAC. Voici trois exemples plus précis où ça vaut le coup:

- Changer son adresse MAC peut être utile quand on se connecte avec son ordi portable à n'importe quel réseau public ouvert (par exemple une connexion wifi de bibliothèque). En faisant ça, on ne pourra pas nous identifier par le biais de notre ordinateur comme étant une personne utilisant Tails et Tor. En allant plus loin, si Tor foire ou qu'il arrive n'importe quoi qui révèle l'adresse IP, un éventuel adversaire sachant dès lors l'origine de la connexion ne pourra pas en apprendre plus sur

[68] Pour plus d'infos: [https://tails.boum.org/doc/about/warning/index.fr.html#index7h1].

nous. En tout cas, pas en demandant à l'administration du réseau local ou au fournisseur d'accès, la liste des adresses MAC enregistrées. C'est déjà pas mal, mais il ne faut pas oublier qu'il y a beaucoup d'autres façons d'identifier une personne dans un lieu public !

- Cette falsification peut aussi servir quand on utilise son ordinateur dans différents lieux potentiellement surveillés (par exemple chez des ami-e-s) et qu'on ne souhaite pas être géographiquement traçable via son adresse MAC.

- On pourrait finalement douter du sens de cette pratique quand on utilise sa connexion Internet domestique, puisque si l'adresse IP est trahie, l'identification de la maison qui s'ensuivra est déjà pleinement compromettante. Pourtant, il peut être très utile de laisser planer le doute sur quel ordinateur précis a servi quand on pirate un wifi du voisinage, ou dans le cas d'une perquisition, quand des ordis persos sont saisis.

11.2 Limites de MAC Changer et parades

L'usurpation des adresses MAC est activée par défaut dans Tails, car elle est généralement bénéfique. Mais dans certaines situations, cette fonctionnalité peut aussi conduire à des problèmes de connexion ou à donner un air inutilement suspect à une activité en réseau. La suite de ce point présente les cas dans lesquels il peut être préférable de désactiver MAC Changer.

- Utilisation d'un ordinateur public sur un réseau public, par exemple dans un cybercafé ou une bibliothèque. Cet ordinateur est régulièrement utilisé sur ce réseau local et son adresse MAC n'est pas associée avec notre identité. Dans ces circonstances, il se peut que l'usurpation d'adresse MAC rende impossible la connexion (voir le dernier exemple de cette liste). Même si ça n'est pas le cas, il peut tout de même paraître suspect à l'administrateur réseau de voir une adresse MAC inconnue être utilisée sur ce réseau.

- Sur certaines interfaces réseau, l'usurpation d'adresse MAC est impossible à cause de limitations matérielles ou d'incompatibilités avec le système d'exploitation. Tails bloque alors temporairement ces interfaces réseau et il faut donc désactiver l'usurpation d'adresse MAC pour être en mesure de les utiliser.

Voir: 2.1

- Utilisation de son ordinateur portable ou d'un ordinateur public, sur un réseau public restrictif. Certains réseaux ne permettent des connexions que depuis une liste précise d'adresses MAC autorisées. Dans ce cas,

falsifier son adresse MAC rend impossible la connexion, même à partir d'un ordinateur précédemment autorisé.

Pour finir, il est encore important de relever un point. Lors de la connexion à Internet via des téléphones portables utilisant les technologies 3G, 4G ou GSM, l'identifiant de votre carte SIM (IMSI) et le numéro de série du téléphone (IMEI) sont toujours envoyés à l'opérateur du téléphone. C'est le cas même si la connexion se fait au travers de Tails et que ces identifiants uniques (IMSI, IMEI) fonctionnent selon une logique très proche de celle des adresses MAC. Pour l'instant, ni MAC Changer, ni aucun autre programme de Tails ne sont en mesure de remédier à ça.

11.3 Utiliser MAC Changer pour modifier ou conserver son adresse MAC

Comme on l'a vu précédemment, l'usurpation d'adresse MAC est activée par défaut dans Tails et cependant dans certains cas, il peut être préférable de désactiver cette fonctionnalité. Que l'on choisisse l'une ou l'autre option, tout va se passer dans l'écran de connexion, au démarrage de la session Tails.

1. Démarrer l'ordinateur avec Tails:
Voir: 3.3
Dans l'écran de connexion au début de la session Tails intitulé: **Welcome to Tails**, choisir les options de langue et de configuration de clavier désirées pour le reste de la session. Une fois que c'est fait, deux options s'offrent à nous.

2. Soit désactiver **MAC Changer**:

   2.1. Répondre **Oui** à la question **Plus d'options ?** et cliquer sur **Suivant**.

   2.2. On va alors devoir choisir un mot de passe qui va nous permettre de disposer des droits d'administration pour le temps de la session.

   2.3. Dans la section **Usurpation d'adresse MAC**, désélectionner l'option **Usurper toutes les adresses MAC**.

3. Soit laisser **MAC Changer** activé par défaut:

   3.1. Pour que **MAC Changer** reste activé, peut importe si on décide de répondre **Oui** ou **Non** à la question **Plus d'options ?**. Il suffit de ne pas désélectionner l'option **Usurper toutes les adresses MAC**, si on a répondu **Oui** à la question **Plus d'options ?**.

12 Logiciels malveillants, matériels malveillants et métadonnées: des traces qu'on nous arrache

12.1 Logiciels et matériels malveillants

Il existe un grand nombre de logiciels ou de matériels malveillants pouvant être installés à notre insu quelque part sur l'ordinateur. Ils sont la plupart du temps conçus pour ne pas trahir de signes visibles de leur présence, qui peut donc être très difficile à détecter. Les actions qu'ils accomplissent peuvent être diverses et variées. Dans un certain nombre de cas, il s'agit de surveillance. C'est sur cet aspect précis que se focalise ce livre qui ne va pas s'attarder à l'ensemble de ce vaste sujet en perpétuelle évolution. Ainsi, au-delà des traces pouvant être laissées sur les ordinateurs par une utilisation plus ou moins prudente des systèmes d'exploitation et de l'Internet, certains logiciels ou matériels malveillants fonctionnent comme espions ou mouchards et peuvent nous arracher des informations parmi les plus sensibles qui soient. Ceci est fait avec des intentions et des conséquences parfois très différentes, suivant à qui profite la surveillance. On peut principalement distinguer trois situations.
Premièrement, des données personnelles peuvent être extraites par des pirates informatiques, soit par défi, soit pour prendre l'argent là où il est (dans le cas d'un détournement du n°de compte bancaire par exemple). Ensuite, il y a le cas des produits informatiques propriétaires (logiciels ou matériels) qui incluent des fonctions malveillantes afin de récolter des données à leur profit ou d'essayer d'empêcher le piratage. Finalement, des mouchards sont utilisés à des fins de surveillance par les États, veillant aux intérêts et aux pouvoirs en place. Ce troisième cas, de loin le moins fréquent, est néanmoins celui qui nous préoccupe le plus.

On peut encore noter que la portée de ces dispositifs augmente fortement dès que l'ordinateur est connecté à Internet. Leur installation est alors grandement facilitée (pour les logiciels), et la récupération des données collectées se fait à distance.

12.1.1 Logiciels malveillants, logiciels espions

Le terme «logiciel malveillant» (malware en anglais), est un terme générique utilisé pour parler d'une grande diversité de programmes malveillants aux fonctionnements distincts. Les virus nous viennent en premier à l'esprit, mais il en existe bien d'autres tels que les vers, les chevaux de Troie (troyens), les rootkits ou les enregistreurs de frappe (keyloggers). Les particularités de chaque type ne seront pas détaillées ici, mais tous peuvent potentiellement inclure des fonctions de surveillance et donc servir de logiciels espions. Notons

quand même, que les troyens qui permettent de prendre, à distance, le contrôle de l'ordinateur sont particulièrement utilisés à cette fin.
Il faut aussi savoir qu'un logiciel espion donné ne peut pas faire tout et n'importe quoi. Il est confectionné avec des capacités d'infection et d'action précises et limitées. Par exemple, un troyen pouvant infecter des systèmes Windows sera totalement inopérant sur Linux ou Mac. En allant plus loin, il n'est même pas sûr qu'il puisse agir sur l'ensemble des différentes versions de Windows.

Avant d'aller plus loin, une clarification est nécessaire. On entend souvent dire et à juste titre, qu'il y a très peu de logiciels malveillants ciblant des systèmes Linux, dont Tails fait partie. Cela s'explique par le fait que, Linux étant un système d'exploitation minoritaire, le développement de logiciels spécifiques est quantitativement et économiquement moins rentable. Ceci est valable pour l'écrasante majorité des logiciels espions ou plus généralement pour les logiciels malveillants conventionnels, qui ne sont pas intéressés dans une cible particulière mais qui au contraire, veulent des milliers de numéros bancaires ou d'ordinateurs zombies. La notion de défense à l'encontre de ce type d'attaque est relative. Aussi longtemps qu'on utilise un système plus sécurisé (Linux) que la plupart des autres personnes, les attaques vont toucher d'autres personnes que nous.

Voir: 3.2.2 Par contre, tout se corse quand on parle des logiciels espions de la flicaille[69], qui surveillent à plus ou moins long terme et à des fins répressives des personnes ou des groupe spécifiques. Dans ce cas, les adversaires se foutent de toucher aléatoirement le plus grand nombre. Au contraire, ils auront potentiellement de gros moyens et des sbires qualifiés pour tenter de déjouer les défenses d'un système ciblé quel qu'il soit. Quitte à essayer plusieurs voies d'attaque différentes pour y arriver. Dans ce genre de situation, ce qui est en jeu est le niveau absolu de sécurité du système. La comparaison de son niveau de précautions par rapport aux autres systèmes largement moins sécures n'a pas d'importance, tout ce qui compte est d'avoir une longueur d'avance sur la répression.

Maintenant, voyons de quoi sont capables les logiciels espions et à quels dangers ils peuvent nous exposer, suivant leur conception. Ils peuvent être à la base de fuites dramatiques d'informations en tout genre, se faisant par une surveillance en temps réel (via Internet) de toutes les activités imaginables sur un ordinateur. En vrac: adresse IP (et donc géolocalisation), contenu

[69] Ce type d'attaque déjà mentionné précédemment s'appelle en anglais une APT (Advanced Persistent Threat). Pour plus d'infos théoriques à ce sujet: [https://fr.wikipedia.org/wiki/Advanced_Persistent_Threat] et [https://www.schneier.com/blog/archives/2011/11/advanced_persis.html].

de la mémoire vive (dont les clés de cryptage et phrases de passe), captures d'écran, accès à l'ensemble des fichiers stockés, enregistrement des frappes au clavier, liste des programmes ouverts et des sites visités, interception des communications par e-mail, par messagerie instantanée et Skype. lls peuvent encore parfois utiliser le micro, la webcam ou d'autres périphériques de l'ordinateur et même installer de nouveaux programmes malveillants...

12.1.2 Matériels malveillants, matériels espions

Ces dispositifs sont clairement beaucoup moins fréquents que les logiciels malveillants, d'autant plus si on parle de surveillance répressive. Le fait que leur installation sur un ordinateur donné demande d'y avoir accès physiquement y est clairement pour quelque chose. Pourquoi se compliquer la vie, alors que quasi tous les ordis sont connectés à l'Internet ?
Les plus connus des matériels malveillants sont de manière très probable les enregistreurs de frappe[70] (keyloggers). Mais finalement, les cas où les mouchards matériels sont peut-être le plus souvent employés dépasse le cadre strictement informatique. En effet, c'est quand la surveillance ne peut avoir recours à Internet que des micros cachés et des balises de géolocalisation GPS prennent tout leur sens. Mais ça va au delà du champ de ce texte.

Voir: 5.6

12.2 Métadonnées

Les métadonnées sont des «données sur les données». Cela veut dire que ces données peuvent permettre d'apporter des précisions sur une autre donnée, à laquelle elles sont rattachées. Bien que la plupart des métadonnées accompagnent des données numériques comme des images, des fichiers textes ou des vidéos, certaines sont sur d'autres supports comme du texte papier ou des photos.
À ce stade, il est important de noter qu'il va être question ici de métadonnées dans un sens plus large que celui qui est généralement utilisé. En effet, l'usage du terme métadonnée est souvent limité à des données ajoutées volontairement par un ordinateur, une imprimante, un scanner, une caméra numérique ou tout autre appareil permettant de créer des données. Ces métadonnées peuvent, par exemple, comporter les dates de création et de modification d'un document ou le modèle et le numéro de série de l'appareil photo. Par «volontairement», on veut dire que l'ajout de ces informations supplémentaires est prémédité (bien que souvent à notre insu et sans notre consentement explicite) et donc qu'il est dans une certaine mesure évitable. Mais ici, on va aussi appeler métadonnées des informations aléatoires qui se rajoutent qu'on le veuille ou non durant de nombreux processus de création

[70] Pour plus d'infos: [http://www.bugbrother.com/security.tao.ca/keylog.html].

de données. Leur présence n'est pas volontaire, dans le sens où elle n'est pas préméditée, mais il reste quand même que l'ajout de ce type de métadonnées est prévisible et dans un certain nombre de cas, carrément inévitable. Ce fait est expliqué par la marge incompressible de hasard et d'aléatoire qu'implique parfois la création ou la retranscription de données. Deux exemples de ce phénomène qui seront décortiqués plus loin dans le texte, portent sur les légers défauts ou décalages systématiquement présents dans les têtes d'impression des imprimantes ou les capteurs des appareils photo.

Voir: 12.2.2

Pour finir cette intro sur les métadonnées, il est essentiel de comprendre qu'une métadonnée, qu'elle soit générée avec un but préalable ou au contraire aléatoirement, pourra vraisemblablement dans les deux cas, être utilisée en tant qu'identité numérique pour identifier des données qu'elle accompagne et de là, servir à des fins de surveillance et de contrôle. Cette perche tendue à la répression par la présence de métadonnées, est assez clairement illustrée en prenant l'exemple d'une photo prise par un appareil photo numérique et postée sur Internet de manière supposément anonyme. Dans ce cas, si une attention particulière n'a pas été consacrée à l'effacement des métadonnées il est plus que probable que l'anonymat recherché soit dangereusement remis en cause par la trahison d'informations comme le numéro de série et de petits défauts d'optique propres à l'appareil ayant pris la photo, ou même les coordonnées GPS au moment de la photo[71].

Voir: 9.3

12.2.1 Métadonnées laissées volontairement par les ordinateurs, les appareils photo numériques et les imprimantes

On va survoler ici la grande variété[72] des métadonnées, pouvant accompagner de manière préméditée et souvent très discrète la création de fichiers ou de documents. Avant de se lancer, on peut encore se demander quelles raisons et intérêts se cachent derrière l'utilisation volontaire des métadonnées. La plupart du temps, ces données sont conçues comme des informations supplémentaires et facultatives à propos des fichiers et documents et sont destinées à faciliter leur utilisation (par exemple pour classer des photos). Comme souvent, ça part d'une bonne intention mais le problème apparaît quand ces informations tombent entre de mauvaises mains. À l'inverse, les deux autres principales sources d'injection de métadonnées dans nos données sont

[71] Voici la petite histoire d'un hacker stupide qui s'est fait serrer par les flics à cause des métadonnées GPS qui accompagnaient les photos qu'il avait prises avec son smartphone: [http://www.csoonline.com/article/705170/embedded-data-not-breasts-brought-down-hacker].

[72] Pour plus d'infos: [http://www.arxiv.org/pdf/1212.3648], [p. 21 et 27-28 du tome 1 du Guide d'autodéfense numérique] et [http://33bits.org/2011/10/18/printer-dotspervasive-tracking-and-the-transparent-society/].

pourries dès le départ. Il s'agit d'un coté de mesures censées lutter contre le piratage et protéger la propriété intellectuelle, et de l'autre, de mesures destinées à permettre une traçabilité des données, ceci parfois explicitement en faveur des flics[73].
Voici les principales sources de métadonnées assaisonnant nos fichiers et documents de manière préméditée:

- Les ordinateurs:
  Les métadonnées apportées par les ordinateurs dépendent de quel format de données est créé et par quel logiciel, mais elles contiennent typiquement: le nom de l'utilisateur-trice de la session, la date et l'heure de création et de modification, la langue, le programme et le système d'exploitation utilisés et parfois même l'historique des dernières modifications.

- Les appareils photo numériques:
  La palme revient probablement aux formats d'images comme .tiff ou .jpeg. Ces fichiers de photo créés par un appareil numérique ou un téléphone portable contiennent un standard de métadonnées appelé EXIF. Ce dernier peut contenir la date, l'heure et parfois les coordonnées géographiques de la prise de vue, ainsi que la marque, le modèle et le numéro de série de l'appareil utilisé, sans oublier une version miniature de l'image. Toutes ces informations ont tendance à rester accrochées à nos photos, même après que celles-ci soient passées par un logiciel de retouche photo.
  Il ne faut pas confondre ce type de métadonnées accompagnant les fichiers et donc relativement facilement isolables, avec un autre type de métadonnées utilisant la technique du tatouage numérique[74] (watermarking). Cette technique de marquage, consiste à insérer une signature invisible et permanente à l'intérieur même des images numériques. Dans chaque image est inséré un code d'identification imperceptible et indétectable par tout système ignorant son mode d'insertion. Il permet notamment de garantir la preuve de propriété intellectuelle d'une œuvre numérique transitant par les réseaux, tel Internet, afin d'essayer de lutter contre la fraude et le piratage. Il tente de dissuader les pirates dans la mesure où cette «signature» peut être retrouvée dans chaque copie de l'image originellement marquée. De plus, cette signature est sensée pouvoir résister aux différentes techniques de traitement

[73] C'est le cas notamment pour des imprimantes laissant des traces spécifiquement destinées à aider les flics à coincer les faussaires et les braves personnes faisant de la fausse-monnaie. Pour plus d'infos: [https://www.eff.org/press/archives/2005/10/16].

[74] Pour plus d'infos: [https://fr.wikipedia.org/wiki/Tatouage_numérique] et [https://www.journaldunet.com/encyclopedie/definition/389/32/20/watermarking.shtml].

de l'image (compression, lissage, rotation, etc.). Ces métadonnées très difficiles à détecter et donc à supprimer, sont heureusement la plupart du temps restreintes à quelques appareils photo haut de gamme ou à des programmes spécifiques. Donc, il n'y a pour l'instant pas trop de soucis à se faire concernant le détournement de cette technique par les flics dans le domaine des appareils photo (on verra que ce n'est pas le cas concernant les imprimantes). Dans ce cas, le principal danger est que l'usage du tatouage numérique se généralise à l'ensemble des appareils photo numériques.

- Les imprimantes:
  Contrairement à la situation qui prévaut pour les appareils photo numériques, l'utilisation du tatouage numérique est déjà largement répandue pour les imprimantes laser haut de gamme[75] (typiquement les grosses imprimantes des centres de photocopie). De manière similaire à ce qu'on vient de voir, ces imprimantes identifient leur travail en dissimulant[76] au sein de chaque texte ou image imprimée une signature reposant sur de très légers détails d'impression, souvent invisibles à l'œil nu (typiquement de minuscules pixels jaunes). Ils permettent d'identifier de manière certaine la marque, le modèle et dans certains cas, le numéro de série de la machine qui a servi à imprimer un document. Ce qui est bien pratique pour des flics voulant pister les faussaires qui ont trouvé un bon moyen pour rembourser leur photocopieuse...

Pour avoir une idée des métadonnées cachées dans nos fichiers numériques, il existe divers outils faciles d'utilisation, dont un programme qui est présenté au chapitre suivant. Cependant, il faut quand même garder à l'esprit que les métadonnées utilisant le watermarking ne seront sûrement pas atteignables et qu'il est possible que certains formats de fichiers propriétaires ne livrent que partiellement le secret de leurs métadonnées.

Voir: 13.1

12.2.2 Métadonnées laissées involontairement par les imprimantes, les appareils photo numériques et autres scanners

Comme on l'a déjà évoqué, deux appareils électroniques permettant la création de données numériques et supposés identiques puisque du même modèle, comporteront tout de même une part certaine de variabilité indétectable à

[75] Pour une liste des marques et modèles d'imprimantes collabos: [https://www.eff.org/pages/list-printers-which-do-or-do-not-display-tracking-dots].

[76] Cela s'appelle de la stéganographie. Pour plus d'infos: [https://fr.wikipedia.org/wiki/Stéganographie].

l'œil nu, mais qui, si elle est analysée de manière adéquate, permet l'établissement d'un équivalent machine de l'empreinte digitale, sensée être unique pour chaque individu-e[77].
De là, tout comme l'empreinte digitale permet d'identifier la main qui l'a laissée ou la balistique permet d'identifier une arme à feu à partir d'une balle, il est possible d'utiliser la variabilité de certains petits défauts pour identifier une imprimante à partir d'une page qui en est sortie ou un appareil photo numérique à partir d'une image qu'il a générée.
Cependant, la technique permettant de caractériser l'empreinte unique d'un appareil photo ou d'une imprimante comporte des limites. Pouvoir prouver qu'une image donnée est bien issue d'une machine précise, requiert d'avoir à disposition, soit de multiples images issues de la même machine, soit la machine elle-même (capturée lors d'une perquisition par exemple).
Pour finir, on peut encore constater que le développement de ces techniques d'identification numérique est récent et qu'elles sont encore en cours d'homologation chez les flics[78]. Mais il y a clairement moyen qu'elles puissent bientôt représenter un réel danger pour l'anonymat des personnes qui aiment mettre leur grain de sable dans les rouages biens huilés de ce(ux) qui nous écrase(nt).
Petit passage en revue de ce type de traces laissées par certains de nos appareils électroniques:

- Les appareils photo numériques:
  L'établissement de l'empreinte d'un appareil photo numérique se base sur de légères irrégularités de construction et d'usure des capteurs, qui sont propres à chaque appareil et qui aboutissent à d'infimes défauts reproduits dans chaque image. Ces particularités se mesurent à l'échelle de quelques pixels.

- Les scanners:
  Puisque les scanners capturent des images via un processus similaire à celui mis en jeu pour les appareils photo numériques, il n'est pas surprenant que le principe sur lequel se base leur identification soit aussi analogue.

- Les imprimantes:
  En plus du recours à la technologie du tatouage numérique vue auparavant, l'établissement de l'empreinte d'une imprimante peut aussi se

Voir:12.2.1

[77]Pour plus d'infos: [http://33bits.org/2011/10/11/everything-has-a-fingerprint---dont-forget-scanners-and-printers/], [http://33bits.org/2011/09/19/digital-camera-fingerprinting/] et [https://phys.org/news64638499.html].
[78]Pour plus d'infos: [https://www.forensicmag.com/article/calling-shots-new-technique-links-digital-images-exact-camera?page=0,2].

baser sur l'observation de traces liées à de subtiles variations dans la construction et l'usure de la machine. Avec l'âge, les têtes d'impression se décalent, de légères erreurs apparaissent, les pièces s'usent, et tout cela constitue au fur et à mesure une signature propre à l'imprimante. De plus, cette fois-ci les risques de traçage ne sont plus réservés aux seules imprimantes laser haut de gamme, la première jet-d'encre de bureau est aussi concernée...

12.3 Surveillance basée sur les logiciels et matériels malveillants ou les métadonnées

On l'aura compris, les dispositifs vus dans ce chapitre sont peut-être ce que la surveillance informatique fait de plus agressif et de difficile à contrer, puisqu'ils sont conçus spécifiquement pour nous espionner ou, en tout cas pour ce qui est des métadonnées, pour mieux nous tracer.

12.4 Comment ne pas y laisser des traces

On renvoie ici en quelques mots aux chapitres pratiques présentant des outils qui peuvent aider à éviter de laisser trop de traces à des logiciels malveillants ou dans des métadonnées:

- Des solutions pour limiter notre vulnérabilité aux logiciels malveillants sont proposées de manière large au point 3.2.2 et plus spécifiquement au chapitre 15 qui traite de la technique du Trou d'Air.

- L'usage du clavier virtuel permettant de déjouer l'action des enregistreurs de frappe matériels est détaillé au point 5.6.

- ExifTool, un outil permettant de visualiser les métadonnées disposées volontairement dans les fichiers est proposé juste après, au chapitre 13.

- MAT, un outil pour l'effacement de nombreuses métadonnées disposées volontairement dans les fichiers, ainsi que diverses astuces permettant de contourner les traces laissées aléatoirement ou par la techniques du tatouage numérique sont présentées au chapitre 14.

13 Visualiser les métadonnées d'un fichier avec ExifTool

13.1 Qu'est-ce qu'ExifTool

ExifTool est un programme en ligne de commande disponible par défaut depuis le terminal de nombreux systèmes d'exploitation de type Linux (dont

Voir: 4.1

Tails fait partie) et qui permet de visualiser les métadonnées laissées volontairement dans beaucoup de formats de fichiers[79] (image, video, audio, pdf).

13.2 Limites d'ExifTool et parades

Les limites d'ExifTool sont similaires à celles qui seront décrites pour le programme d'effacement des métadonnées MAT. Tout d'abord, bien qu'ExifTool supporte un grand nombre de formats de fichiers, il est toujours possible que l'accès complet à des métadonnées contenues dans certains formats de fichiers propriétaires ne soit pas garanti. Ensuite, il ne faut pas compter sur ExifTool pour détecter les métadonnées issues de la technique du tatouage numérique et encore moins celles générées de manière non préméditée par des processus aléatoires. Le logiciel n'est tout simplement pas conçu pour ça !

Voir: 12.2
Voir: 14.1

En connaissant ces limites, il peut être parfois préférable de se référer à d'autres sources pour s'assurer de la présence de métadonnées non supportées par ExifTool. Il peut s'agir par exemple, de rechercher sur Internet si un modèle particulier d'imprimante ou d'appareil photo numérique utilise la technique du tatouage numérique. Ça ne va peut-être pas nous aider à visualiser ces métadonnées en elles-même, mais nous permettra au moins de savoir à quoi s'en tenir à propos de leur existence.

13.3 Utiliser ExifTool pour visualiser les métadonnées d'un fichier

1. Démarrer une session Tails.

2. Dans Tails, ouvrir le programme **Terminal** depuis le menu **Applications ▷ Accessoires ▷ Terminal**.

3. Un écran blanc apparaît avec l'invite de commande:

   ```
   amnesia@amnesia:~$
   ```

   À la suite de ça, entrer la commande:

   ```
   exiftool [le chemin du fichier]
   ```

   En veillant à remplacer la partie de la commande entre crochets: [**le chemin du fichier**] par le chemin du fichier dont on désire visualiser les métadonnées. Le plus simple pour faire cela est d'aller dans le menu **Raccourcis ▷ Dossier personnel**, de voyager dans les dossiers jusqu'à atteindre celui contenant le fichier à analyser, de sélectionner

[79] Pour plus d'infos: [http://www.sno.phy.queensu.ca/~phil/exiftool/].

ce dernier avec la souris et de le faire glisser dans la fenêtre du **Terminal** juste après le début de la commande **exiftool** (insérer quand même un espace après **exiftool**). Au final, la commande doit donner quelque chose comme ça:

```
exiftool '/home/amnesia/Dossier/MonFichier.pdf'
```

Une fois que c'est fait, appuyer sur la touche **Entrée** du clavier.

4. Le **Terminal** doit maintenant nous renvoyer un message qui liste à l'écran les informations obtenues à partir des métadonnées contenues dans le fichier.
   Cette énumération peut contenir une grande variété d'éléments et être plus ou moins longue, suivant le fichier soumis à l'analyse et son format. Même si une partie des informations est assez explicite (comme le numéro de série d'un appareil photo par exemple), de nombreux résultats de cette liste sont, de prime abord, difficiles à comprendre car ils utilisent un langage très technique. Pour une interprétation plus détaillée, il faut alors se référer à la documentation d'ExifTool[80] qui est très complète et disponible en-ligne.

14 Effacer des métadonnées avec MAT

14.1 Qu'est-ce que MAT

MAT (Metadata Anonymisation Toolkit) est un petit logiciel disponible par défaut dans Tails et qui permet d'anonymiser des données en supprimant
Voir: 12.2 les métadonnées qui y sont volontairement rattachées, dans de nombreux formats de fichiers.
Pour l'instant, MAT prend en charge les formats suivants:

- Formats de textes:
  Portable Document Format (.pdf)
  Documents type Open Office (.odt, .opt)
  Documents Microsoft Office(.docx, .pptx)

- Format d'images:
  Jpeg (.jpg, .jpeg)
  Portable Network Graphics (.png)

[80] Pour plus d'infos: [http://www.sno.phy.queensu.ca/~phil/exiftool/TagNames/index.html].

- Formats compressés:
  Zip (.zip)
  TApe aRchiver (.tar.gz, .tar.bz2, .tar)

- Formats multimédias:
  MPEG Audio (.mp3, .mp2, .mpa)
  Ogg Vorbis (.ogg)
  Free Lossless Audio Codec (.flac)
  Torrent (.torrent)

14.2 Limites de MAT et parades

Tout d'abord, parlons du fait que MAT efface les métadonnées mais sans donner plus de détails sur ce qu'elles contenaient. Ce fonctionnement assez minimaliste n'a pas trop d'importance au niveau de la sécurité mais peut s'avérer passablement frustrant. Pour avoir une idée du contenu d'un fichier en métadonnées ou, de manière plus prudente, pour vérifier l'efficacité de leur effacement par MAT, il existe comme on l'a déjà vu, un outil très simple d'utilisation; ExifTool. Voir: 13.1
Attaquons maintenant les réelles limites de ce logiciel et les manières de les dépasser. Il faut tout d'abord savoir que le logiciel MAT n'est pas la solution ultime. Il permet l'effacement des métadonnées de quelques formats de fichiers couramment utilisés, mais pas l'anonymisation de leur contenu (sans blague !). Et surtout, il ne comprend que de manière incomplète si ce n'est pas du tout, de contremesures pour des métadonnées issues de formats de fichiers propriétaires[81] trop complexes, de techniques comme le tatouage numérique ou pour toute la diversité de traces qui sont déposées de manière non préméditée et aléatoire par les appareils photo et imprimantes. Donc, Voir: 12.2
pour ces derniers cas, en plus de l'utilisation de MAT, il faut avoir recours à d'autres techniques pour essayer de ne pas se faire avoir:

- Se protéger des traces identifiables laissées par les appareils photo numériques:
  Comme on l'a vu, l'identification des appareils photo d'après les traces qu'ils laissent aléatoirement suit exactement la même logique que la balistique, sauf qu'il est très difficile de contrefaire des traces qui vont être laissées sur une balle, alors que modifier une photo numérique est à la portée de beaucoup de monde.
  Voici une défense simple qui combine deux stratégies. D'une part en compressant l'image, on perd de la résolution et donc de l'information,

[81] Il semble par exemple que MAT ne gère pas très bien l'anonymisation des fichiers EXIF de certains modèles d'appareils photo de marque Canon ou bien du format propriétaire de compression de fichier .zip.

de laquelle l'identification d'une empreinte dépend de manière cruciale (eh oui cela se passe au pixel près). Pour que cela marche, il faut noter que cette perte de résolution devra être bien plus agressive que celle proposée par défaut dans les réglages standards. Par exemple, diminuer le facteur de qualité d'un fichier .jpg à 50% au lieu des 95% habituels. D'autre part, il peut être pertinent de procéder en plus, à une transformation, un brouillage de l'information, en forçant un décalage dans la façon dont l'image était encodée. Cela peut être fait en redimensionnant l'image et en lui faisant subir une légère rotation (quelques degrés suffisent). Cette défense n'est pas infaillible, mais pour espérer la contourner, une tentative d'identification devra être beaucoup plus sophistiquée et aura un taux d'erreur beaucoup plus grand.

- Se protéger des traces identifiables laissées par les imprimantes:
  Il est intéressant de savoir que les détails d'impression ne résistent pas à la photocopie répétée. Dans ce cas aussi, le but visé est la perte de résolution, et donc d'information, qui a lieu à chaque copie. Photocopier la page imprimée sur une autre machine, puis photocopier la photocopie obtenue trois fois d'affilée, suffit la plupart du temps à faire disparaître des détails qui permettraient d'identifier une imprimante. Par contre, on en laissera sûrement d'autres, les photocopieuses présentant aussi des défauts, et parfois des signatures stéganographiques de type tatouage numérique. Bref on tourne en rond, et le problème devient surtout de choisir quelles traces on veut laisser...

Voir:12.2.1

- Se protéger du tatouage numérique des imprimantes:
  Faire disparaître un tatouage numérique présent sur une impression, implique exactement la même procédure que celle vue dans le point précédent. Pourtant, la technique la plus simple pour éviter l'impasse des tatouages numériques, reste peut-être d'éviter les imprimantes laser haut de gamme. Mais parfois, on n'a pas le choix, surtout pour les gros tirages.

14.3 Utiliser MAT pour effacer les métadonnées d'un fichier

1. Dans Tails, lance le logiciel **MAT** en allant dans **Applications** ▷ **Outils système** ▷ **MAT**. La fenêtre du programme s'ouvre.

2. Pour sélectionner un fichier dont on aimerait effacer les métadonnées, cliquer sur l'îcone en forme de +. Une fenêtre s'ouvre intitulée **Sélectionner des fichiers**. Navigue dans les dossiers jusqu'à ton fichier, clique dessus et choisis **Valider**. Le nom du fichier apparaît maintenant dans la fenêtre principale du programme.

3. Pour effacer les métadonnées du fichier sélectionné, cliquer sur l'îcone en forme petit balais. Au bout de quelques secondes, **MAT** annonce **Nettoyer**, sous la colonne **État**. En fait il y a une erreur de traduction, le programme devrait indiquer Nettoyé et non pas Nettoyer...

4. Pour nettoyer un nouveau fichier, retourne à l'étape 2 de cette marche à suivre.

15 Se protéger des logiciels espions par la création d'un Trou d'Air

15.1 Qu'est-ce qu'un Trou d'Air

Un «Trou d'Air» ou «Air Gap», est une mesure de sécurité informatique souvent utilisée pour des ordinateurs ou des réseaux d'ordinateurs qui demandent un niveau de sécurité et de confidentialité maximale[82]. Cela consiste à s'assurer qu'un support informatique sensible soit isolé de toute connexion directe à des réseaux et leurs nombreux périls, notamment en matière d'infection par des logiciels espions. C'est la méthode fournissant à nos données confidentielles la protection la plus crédible contre ce type de surveillance informatique ciblée. Précisons quand même que la plupart du temps, le Trou d'Air n'est pas absolu, dans le sens où le système isolé est quand même indirectement relié au réseau par l'intermédiaire de supports de mémoire cryptés, étroitement contrôlés.

En pratique, la mise en place d'un Trou d'Air destiné à protéger des données confidentielles de l'attaque des logiciels espions, peut consister à utiliser deux systèmes Tails en parallèle, sur deux ordinateurs côte à côte. L'un connecté à Internet (par exemple pour aller sur sa boîte mail anonyme), l'autre, uniquement utilisé hors-connexion, sur lequel on travaille avec les données confidentielles (comme les très secrètes clés privées de cryptage de ses e-mails et de ses mémoires numériques). La liaison entre système en-connexion et système hors-connexion se fait ensuite par le biais d'une clé USB cryptée. Comme les données confidentielles ne doivent pas filtrer vers Internet, elles ne doivent jamais avoir la possibilité d'être transférées vers le système en-connexion. C'est pour ça que la clé USB de liaison potentiellement infectée par un logiciel espion, doit absolument être effacée et cryptée dans sa totalité à chaque fois qu'elle a été au contact de données confidentielles sur le système hors-connexion. Pour plus de sécurité encore, il est aussi envisageable de faire la liaison entre les deux systèmes par le biais de CDs au

[82] Comme par exemple les systèmes informatiques de contrôle des centrales nucléaires... Pour plus d'infos: [https://en.wikipedia.org/wiki/Air_gap_(networking)].

contenu crypté, qui au lieu d'être effacés et réinscrits à chaque voyage, sont purement et simplement détruits. La destruction permet en effet moins de failles de sécurité que le reformatage, mais elle quand même passablement plus exigeante en ressources (il faut avoir des CDs vierges à disposition). L'exemple d'utilisation d'un Trou d'Air présenté au point suivant, se base exclusivement sur l'utilisation de clés USB, mais la même procédure est tout à fait envisageable en utilisant des CDs comme supports de liaison.
En plus de la pratique de l'effacement (ou de la destruction) systématique, on verra que seul un timing réfléchi pour le branchement des supports de stockages, permettra d'éviter une infection persistante de logiciels malveillants sur le système hors-connexion.

Ainsi, même si cette méthode ne permet pas d'éviter l'infection temporaire de la mémoire vive de l'un et l'autre système par certains logiciels malveillants (eh oui nombre d'entre eux ont la capacité de s'infiltrer dans les clés USB), elle permet au moins de garantir que ceux-ci n'auront aucun moyen de s'installer durablement ou de faire des retours à l'ordinateur connecté, des informations confidentielles auxquelles ils auront eu accès. Le système qui serait susceptible d'être espionné, car relié à Internet n'est jamais au contact de données confidentielles. Les e-mails cryptés, par exemple, qu'on y télécharge ne sont en l'état plus confidentiels car illisibles pour qui n'est pas dans le secret du cryptage et c'est seulement une fois transférés sur le système isolé d'Internet, qu'ils seront déchiffrés en clair.
Pour permettre de mieux comprendre le fonctionnement de cette technique exigeante, on va donner dans la suite un exemple détaillé d'une manière de créer un Trou d'Air pour échanger des e-mails cryptés.

15.2 Limites de la technique du Trou d'Air

L'excellent effet défensif apporté par cette méthode, comprend aussi son lot d'inconvénients. Ainsi, l'application d'un tel système semi-clos rend passablement laborieux le transfert de données entre le monde extérieur des réseaux et la machine située au delà du Trou d'Air.

15.3 Comment créer un Trou d'Air pour échanger des e-mails cryptés en toute confidentialité

Comme on l'a vu, l'enjeu principal de cette technique est d'essayer de barrer tout chemin possible de retour vers le réseau pour un logiciel espion essayant de nous soutirer des données confidentielles traitées hors-connexion. On aura donc besoin pour ça, de disposer de deux ordinateurs avec Tails (celui hors-connexion doit avoir Tails sur DVD) et de deux supports de mémoire cryptés

Voir: 6.4

(clé USB, carte SD ou disque dur externe). Une des deux mémoires sert de liaison entre les deux ordinateurs et sera effacée à chaque utilisation, l'autre sert à stocker les clés de cryptage publiques de nos acolytes et notre clé privée confidentielle.

Voir: 7.3

Avant de se lancer, on peut encore préciser qu'au delà du cas précis du maintien de la confidentialité des communications cryptées, des procédures semblables à celle qu'on va voir, sont aussi valables pour assurer le secret de toutes sortes de données pouvant être stockées et utilisées à partir d'un support de mémoire crypté. Par exemple, un tract subversif en cours d'écriture et destiné à être publié sur Internet.

1. Démarrer deux ordinateurs sous Tails, l'un qui sera destiné à se connecter à Internet, l'autre avec Tails sur DVD, uniquement utilisé hors-connexion. Pour s'assurer que le deuxième ordinateur soit vraiment hors-connexion, il peut être bien de déconnecter (si possible) le câble de réseau et l'antenne Wifi.

2. Récupérer les messages reçus:
   Sur le premier ordinateur, se connecter à Internet via **Tor**, consulter sa messagerie e-mail anonyme et copier/coller dans un fichier texte (par exemple dans **Applications ▷ Accessoires ▷ Éditeur de texte gedit**) les e-mails cryptés qu'on a reçus. Sauvegarder ensuite ce fichier texte dans le premier support de mémoire crypté, qui va servir à faire le lien entre les deux ordis et débrancher ce support de mémoire.

Voir: 10.1

3. Décrypter les messages reçus:
   Sur l'ordinateur hors-connexion, il faut tout d'abord brancher et ouvrir le deuxième support de mémoire crypté servant au stockage des clés de cryptage, puis charger sa clé de cryptage privée dans l'**Applet de chiffrement OpenPGP**. Finalement, il est très important de débrancher ce support de mémoire avant de passer à la suite, afin de lui éviter tout risque d'infection.
   Ensuite, brancher et ouvrir le premier support de mémoire crypté sur l'ordinateur pour pouvoir décrypter les messages qui y ont été transportés. Une fois que l'on a décrypté nos messages et pris connaissance de leur contenu, débrancher le support de mémoire et redémarrer l'ordinateur. Cette dernière action permet d'effacer un éventuel logiciel malveillant qui se serait caché temporairement en mémoire vive depuis le support de mémoire de liaison et qui pourrait attendre qu'on l'ait effacé et réinitialisé pour, discrètement y transférer nos informations confidentielles.

Voir: 7.3

4. Effacement du support de liaison et cryptage des messages à envoyer:
   Une fois que la session Tails de l'ordinateur hors-connexion à été redémarrée, il faut tout d'abord rebrancher et ouvrir le deuxième support de mémoire crypté servant au stockage des clés de cryptage, puis charger dans l'**Applet de chiffrement OpenPGP** les clés de cryptage publiques des personnes avec qui on veut correspondre. Ensuite, il est très important de débrancher ce support de mémoire avant de passer à la suite afin de lui éviter tout risque d'infection.
   Il va s'agir alors de rebrancher le support de mémoire de liaison et, sans ouvrir la partition cryptée, de le reformater afin d'y créer une nouvelle partition cryptée. Il est important que le reformatage ait lieu sans ouvrir la partition cryptée initiale, afin de parer au risque d'infection de la mémoire vive vu au point précédant.
   Voir: 6.4
   Toujours sur la nouvelle session Tails de l'ordinateur hors-connexion, on peut maintenant écrire les messages à renvoyer et les sauver dans un fichier texte après les avoir cryptés avec les clés publiques correspondantes. Finalement, on peut copier/coller ces fichiers texte dans le support de mémoire crypté de liaison fraîchement reformaté et débrancher celui-ci.

5. Envoyer les e-mails en réponse:
   De retour sur la session Tails de l'ordinateur connecté à Internet, il faut tout d'abord brancher et ouvrir le support de mémoire crypté servant au transfert des messages. Ensuite, il s'agit d'ouvrir les fichiers texte stockés sur la partition cryptée, qu'il peut être intéressant d'avoir identifiés par un titre en rapport avec l'adresse du ou de la destinataire. En effet, rien ne ressemble plus à un message crypté qu'un autre message crypté. Pour finir, il suffit de copier/coller les messages cryptés contenus dans les fichiers textes et de les envoyer depuis sa messagerie e-mail.

16 Réflexions sur des stratégies face à la répression et aux limites des outils informatiques

16.1 Connaître son ennemi

Dès qu'on réfléchit à la répression dans le but de la contourner, on est amené-e à constater que comme dans tout rapport de force, on ne contrôle qu'une partie des paramètres. L'autre partie ne dépend pas de nous mais du hasard, dans une certaine mesure, et surtout de l'ennemi. D'où l'intérêt d'apprendre à le connaître.

Dans un contexte donné, disons l'Allemagne en 2015, il important d'essayer de faire la différence entre: ce que la répression a les moyens de faire et ce qu'elle fait, entre ce qu'elle aura les moyens de faire et ce qu'elle fera dans le futur. Ce n'est pas parce que la National Security Agency étasunienne a déjà utilisé certains moyens de surveillance informatique dans son arsenal anti-terroriste qu'ils seront d'usage en Allemagne.
De plus, il est fréquent que des techniques de surveillance matériellement disponibles et légalement bien établies soient peu, voire pas utilisées. C'est le cas par exemple, d'une loi française[83] punissant de trois ans d'emprisonnement et de 45000 euros d'amende, toute personne refusant de livrer ses clés de cryptage à la demande de la justice. Depuis plus de 10 ans qu'elle existe, cette menace n'a encore jamais été mise à exécution.

Pour finir, ça peut paraître évident, mais il n'est peut-être pas inutile de rappeler l'existence de grandes disparités, entre les différents niveaux de surveillance envisageables au sein d'une même juridiction. Dans la majorité des cas, le gendarme du coin ne va pas savoir faire plus que fouiller un ordi perquisitionné du bout de sa souris. Mais parfois, de manière pas très prévisible, la répression met les petits plats dans les grands et se paie un crackage de moyens. Sur quel niveau se calquer ? «Mieux vaut être parano que grillé-e» ? Un équilibre à trouver.

16.2 Méfiance et prudence face aux outils informatiques et leurs limites

À l'issue de ce texte, s'il y a des choses à ne pas perdre de vue, ce sont bien les limites inhérentes à tous les outils informatiques présentés ici. Aucune tentative de se protéger, aucune défense n'est infaillible, ni absolue. C'est un processus en perpétuel ajustement face aux attaques, que celles-ci exploitent des failles existantes, ou qu'elles créent de nouvelles brèches en rendant nos défenses obsolètes. Cette réalité a été illustrée de nombreuses fois au fil du texte, et l'exemple du cryptage est sûrement un des plus parlants.
En effet, on ne peut pas exclure qu'un cryptage incassable en 2015 sera peut-être facilement décrypté en 2020 et que des e-mails cryptés, soient interceptés et archivés par les flics et puissent ainsi facilement être lus seulement 5 ans après leur écriture. En allant plus loin, il est peu probable mais pas impossible que des sbires du pouvoir exploitent déjà de manière cachée des failles nouvellement découvertes dans l'algorithme de cryptage PGP. Bien sûr, si une entité quelconque a réussi à casser PGP, il est vraisemblable que

[83] Pour plus d'infos voir l'article 434–15–2 du Code Pénal réformé en 2003 dans le cadre de la Loi sur la Sécurité Intérieure.

cela reste un secret bien gardé[84] et qu'elle réfléchisse à deux fois avant de l'annoncer publiquement, sous peine de voir la faille rapidement comblée.

Au final, avoir trop confiance en soi et en ces outils peut être aussi dangereux que faire les choses à moitié. Si on pense avoir trouvé la parade absolue à la surveillance, qui va nous permettre de faire n'importe quoi avec l'informatique, c'est clair qu'on va vraiment faire n'importe quoi ! En matière d'informatique, un proverbe dit que la principale faille de sécurité se trouve entre la chaise et le clavier... C'est un peu ce dont parle le prochain point.

16.2.1 Des illusions de sécurité

Le plus souvent, les failles de sécurité viennent de nous et pas des outils qui, pour être fiables, doivent être bien utilisés ou utilisés tout court. Comme on l'a déjà dit dans l'introduction, faire les choses à moité peut donner une illusion de sécurité lourde de conséquences. Rien ne sert, par exemple, d'installer une porte blindée si on laisse la fenêtre ouverte. La sécurité informatique est avant tout une démarche, pas un produit fini. C'est une chaîne dont la solidité est égale à celle de son plus faible maillon (dans ce cas, la fenêtre restée ouverte). Souvent, le manque de précautions dans une étape de l'utilisation des outils informatiques peut compromettre grandement le processus dans son ensemble. Quelques exemples concrets :

- Il ne sert pas à grand chose de faire un tract sous Tails, si c'est pour utiliser son ordi normal au moment de l'impression.

- Inutile de recourir à un algorithme de cryptage dernier cri, si c'est pour l'utiliser sur un système d'exploitation normal (qui contrairement à Tails n'est pas amnésique), ou pour conserver sa phrase secrète sur un post-it, dans un tiroir de sa chambre.

- Il ne sert pas à grand chose d'essayer de cacher son identité en utilisant Tor, si c'est pour griller son identité contextuelle en envoyant des e-mails compromettants depuis une adresse e-mail à son nom, en se connectant à un compte e-mail identifiable, puis à un compte anonyme, ou en recevant sur une messagerie sensée être anonyme des e-mails de personnes identifiables (par exemple de sa famille).

[84] En attendant, dans les documents rendus publiques par Edward Snowden, des outils comme PGP, Tails et Tor, sont de l'aveu même de la NSA des obstacles majeurs à la surveillance. C'est d'ailleurs en les utilisant que Snowden a pu communiquer avec les journalistes sans se faire repérer: [http://www.computerworld.com/article/2863937/snowden-docs-show-tor-truecrypt-tails-topped-nsas-most-wanted-list-in-12.html] et [http://www.wired.com/2014/04/tails/].

- Il ne sert pas à grand chose de mettre en place un Trou d'Air, sans prendre la peine d'effacer scrupuleusement la clé USB de liaison à chaque transfert d'infos.

- Il ne sert pas à grand chose de flouter des visages sur des photos diffusées sur Internet, si c'est pour omettre d'effacer les métadonnées de l'image (qui contiennent souvent une miniature de l'image avant modification).

- Pour aller plus loin dans les considérations antirep, le fait d'être au taquet sur l'autodéfense informatique pourrait parfois nous faire oublier des fondamentaux de la répression. Comme par exemple, qu'il existe bien d'autres moyens que l'adresse IP ou l'adresse MAC, pour nous identifier quand on utilise un ordinateur public à des fins illégales. Cette identification peut se faire notamment en exploitant des données issues de la vidéosurveillance, de l'activité des téléphones portables[85] et des cartes bancaires, ou tout simplement à cause d'un témoignage. Mais heureusement, faire des efforts dans un domaine n'empêche pas de prendre des précautions dans un autre, bien au contraire !

Le risque zéro qui n'était déjà pas à la portée des machines, l'est encore moins des personnes qui les utilisent. Même si on est à fond, il arrive fatalement un moment où l'on se trahit, où l'on commet une erreur, ou plus simplement, où l'on tombe sur quelqu'un-e de plus fort-e que soi. D'une manière simpliste et pessimiste, on pourrait dire que tout ce qu'on peut faire, c'est limiter la casse. C'est pas spécifique à l'informatique, c'est comme ça, c'est pas mal d'avoir ça à l'esprit, sans non plus que ça nous bloque. Sinon on ne fait rien.

16.2.2 Proposition d'une stratégie d'utilisation des outils présentés ici

En résumé, ce texte a pris comme fil conducteur le système d'exploitation Tails, à partir duquel il est allé puiser, au fil des chapitres, différents outils qui y sont intégrés afin d'utiliser au mieux l'informatique pour des activités sensibles.
Au delà de la problématique des traces qui structure la partie théorique du texte, on peut relever deux grands axes qui ont peut-être plus de sens d'un point de vue pratique:

- Activités hors-connexion:
  Pouvoir travailler sur différents types de documents sensibles (texte, image, son, vidéo) avec **Tails**, sans laisser de traces de manière im-

Voir: 3.1

[85] Dans de nombreux cas de répression, les flics se contentent d'utiliser des données prélevées à postériori de l'utilisation des téléphones portables, comme la géolocalisation et les textos (même pas des écoutes téléphoniques). Ils y trouvent déjà assez d'éléments pour incriminer des gens et ne prennent pas la peine d'aller plus loin.

prévisible sur l'ordinateur.
Crypter des espaces de mémoire avec le standard de cryptage **LUKS** utilisé par le **Stockage persitant** ou l'**Utilitaire de disques** et y laisser volontairement des traces de manière plus ou moins durable, dans un espace clairement délimité et à l'accès contrôlé.
Réciproquement, pouvoir effacer vraiment des données quand on a envie avec **shred**.
Pouvoir imprimer des documents sensibles, tout en prenant les mesures nécessaires pour limiter les traces identifiables de l'imprimante.

Voir: 6.3
Voir: 6.4
Voir: 4.1
Voir: 14.2

- Activités en-connexion:
  Pouvoir se connecter à Internet avec **Tor** et **MAC Changer** pour y laisser des traces de manière anonyme et confidentielle en visitant des sites web, y publier des documents dont les métadonnées ont été au préalable identifiées avec **ExifTool** et anonymisées avec **MAT**, ou pour communiquer de manière confidentielle en envoyant des e-mails préalablement cryptés avec **PGP** ou avec la messagerie instantanée **Pidgin** cryptée par **OTR**.
  Pour contrer le risque de surveillance depuis les réseaux par l'infection des logiciels malveillants, il est possible d'établir un **Trou d'Air** à l'interface des systèmes hors-connexion et en-connexion, permettant un filtre précis de l'accès aux données confidentielles.

Voir: 10.1
Voir: 11.1
Voir: 13.1
Voir: 14.1
Voir: 7.1
Voir: 8.1
Voir: 15.1

Après cette vue d'ensemble, on peut essayer de faire la liste du matos dont il faut disposer pour faire tourner tout ça :

- Un ordinateur au minimum, deux si on veut être joignable en permanence via **Pidgin et OTR** sur un ordinateur dédié. Pas besoin de machines récentes, Tails n'étant pas trop exigeant. Rappelons que le fait de disposer d'ordinateurs dédiés à une utilisation sur Tails, dont les supports de mémoire de stockage (disques durs internes, mémoire SSD) sont débranchés, procure un net avantage en matière de protection contre les infections persistantes par des logiciels espions. Ainsi, pour équiper une salle informatique dans un lieu collectif, il suffit de trouver quelques vieilles machines, leur débrancher le disque dur et les mettre à jour régulièrement en leur gravant la dernière version de Tails sur DVD.

- Un support de mémoire (USB, SD ou DVD) contenant la dernière version de Tails. Rappelons quand même que dans le cas où l'on désire utiliser Tails seulement sur clé USB, deux clés peuvent alors être nécessaires au moment de l'installation, ou si on veut faire une mise à jour manuelle du système.
  Pour une utilisation personnelle de Tails c'est l'installation de Tails sur

Voir: 3.4.2
Voir: 3.4.4

clé USB ou carte SD, qui semble être l'option la plus pratique. Tandis que pour un usage collectif, par exemple dans une salle informatique on préférera l'utilisation de DVDs comme supports pour le système.

- Une clé USB ou une carte SD, pour servir de support à au moins deux partitions de mémoire, cryptées avec **LUKS**. La première, doit être suffisament grande pour pouvoir archiver des données sensibles dont on veut stocker des traces au long terme (comme par exemple ses clés de cryptage **PGP**). Celle-ci peut correspondre au **Stockage persistant** crypté de Tails, qui est alors installé sur le même support de mémoire que celui qui contient le système, ou bien elle peut être crée avec l'**Utilitaire de disques** sur un support annexe pour être indépendante de Tails. La deuxième partition cryptée, elle aussi faite à partir de l'**Utilitaire de disques**, aura un espace mémoire volontairement petit[86] (maximum 1 giga), qui servira d'espace de stockage éphémère pour des données particulièrement sensibles (comme par exemple un communiqué d'action en cours d'écriture), dont on voudrait pouvoir effacer les traces rapidement avec **shred**.

- L'accès à une connexion Internet peut se révéler assez pratique, si on veut faire des trucs sur Internet, comme par exemple télécommuniquer avec des e-mails cryptés ou mettre à jour le système.

Pour intégrer un peu toutes ces infos, il peut être utile à ce stade de proposer un cas pratique illustrant les différentes étapes d'une façon typique d'utiliser Tails et ses outils. Prenons par exemple une lutte donnée, dans laquelle on aimerait tout d'abord créer et diffuser une brochure imprimée présentant une analyse de la situation, puis dans la lancée, écrirer et publier sur Internet un communiqué à la suite d'une action illégale. C'est un exemple parmi d'autres, c'est clair que suivant le contexte, et le niveau de sécurité espéré il faut largement réadapter à sa sauce.

1. Création et impression de la brochure:

   1.1. La première étape consiste à écrire et mettre en page la brochure. On part du présuposé qu'il s'agit ici d'un document sensible mais qu'il peut être intéressant d'archiver sur le long terme, pour des retouches ou une publication ultérieure. L'utilisation de Tails sur clé USB, accompagné de son **Stockage persitant** crypté, permettant de sauvegarder le texte de manière confidentielle entre deux sessions d'écriture, est tout à fait indiqué à cet usage. On travaille alors tranquillement sur un ordi domestique tournant sous Tails.

[86] Le fait que cette partition soit petite a toute son importance, car il permet d'envisager une procédure d'effacement avec shred sans que ça nous prenne la journée.

1.2. Le texte peut donc être écrit dans le logiciel de traitement de texte **Open Office** (inclus dans Tails). Des infos peuvent être prises sur Internet via **Tor**. Pour plus de précautions, on peut utiliser deux ordis sous Tails pour créer un **Trou d'Air** entre le système en lien avec Internet et le système traitant nos données confidentielles cryptées.

1.3. Une fois la brochure terminée, on peut la sauver au format .pdf, visualiser les métadonnées du fichier avec **ExifTool** et les effacer avec **MAT**.

1.4. À partir de ce fichier, on peut vouloir faire des impressions sur l'imprimante de la maison, branchée sur l'ordinateur avec Tails, pour ensuite tirer le texte à des centaines d'exemplaires dans un centre de photocopies. À ce stade, il ne faut pas oublier, au préalable, de brouiller les traces de son imprimante en faisant plusieurs photocopies de photocopies avant de lancer l'impression en nombre.

1.5. On peut aussi avoir besoin de transmettre ce fichier de texte à des contacts distants, à qui on a pas d'autres moyens plus sûrs de transmettre le document rapidement. Cela peut se faire en cryptant le fichier (renommé sous un nom anodin) avec **PGP** et en l'envoyant dans le fichier joint d'un e-mail.

2. Publication du communiqué sur Internet:

2.1. Suivant l'action à laquelle il se réfère, un communiqué peut être considéré comme un document hautement sensible qui, si on est retrouvé en sa possession, peut nous amener au devant de lourds ennuis. C'est pour ça qu'on peut vouloir en garder des traces (même cryptées !) durant le moins de temps possible et l'effacer une fois qu'il a été rendu public. Dans cette perspective, il peut donc être malin, durant la création du document avec Tails, de faire l'effort de ne pas utiliser le **Stockage persistant** ou toute autre partition cryptée qu'on utilise pour garder des données au long terme. Les sauvegardes de travail pour ce type de documents sont plutôt enregistrées sur la petite partition cryptée de la clé USB servant au stockage à court terme. Elles pourront ainsi être effacées facilement et de manière plus efficace.

2.2. Comme avant, le texte peut être écrit dans le logiciel de traitement de texte **Open Office**. On peut aussi par exemple y intégrer des photos, nettoyées de leur métadonnées avec l'utilisation de **MAT**

et redimensionnées avec le logiciel de traitement d'image **Gimp** (inclus dans Tails). Un suivi de la présence de métadonnées peut, de surcroît, être effectué en utilisant **ExifTool**.

2.3. Il s'agit maintenant de publier le texte sur Internet. Le mieux est peut-être de faire cela via Tails lancé sur un ordinateur anonyme d'un réseau public (école, bibliothèque etc.). Il suffit d'amener avec soi un système Tails et son support de mémoire crypté. Si on veut pour ça utiliser son ordinateur personnel, l'utilisation de **MAC Changer** peut s'avérer très importante.
Dans ces lieux publics, ne pas trop traîner, checker les caméras, veiller à n'être pas trop reconnaissable par des citoyen-ne-s flics et à ne pas avoir été filé-e, sont des bonnes habitudes à adopter.

2.4. On peut relever l'importance de bien éteindre l'ordinateur (et enlever la batterie des portables) entre chaque session de travail. Cela évite que des données confidentielles soient récupérables par un accès direct à la machine (perquise) ou que des personnes de l'entourage compromettent notre anonymat ou le leur en faisant des recherches Internet après nous (malgré Tor !).

2.5. Une fois de retour à la maison, quand on n'a plus besoin du fichier (si jamais il est dispo sur Internet), on efface toute la partition avec **shred**, on la reformate, on la recrypte avec l'**Utilitaire de disques** et c'est reparti pour de nouvelles aventures !

Pour finir, on peut soulever la grande importance de la composante collective dans les pratiques adoptées face au danger de la surveillance et de la répression. À partir du moment où il y a des projets collectifs, ces enjeux deviennent collectifs et dépassent le seul cadre du positionnement individuel. Il devient important de discuter pour trouver des bases claires, des consensus sur les précautions à adopter, des stratégies collectives.
Par exemple, l'utilisation de moyens de communications pas du tout safe par une personne d'un groupe (par exemple: facebook, adresse e-mail ultragrillée, non-utilisation de Tails ou Tor, pas de cryptage), peut vraiment mettre en danger toutes les autres personnes, même si celles-ci sont très précautionneuses. Il suffit d'imaginer que des traces d'e-mails confidentiels qu'on lui a envoyés cryptés soient retrouvées en clair sur son ordi utilisant un système non-sécurisé. De plus, qui n'a jamais confié son adresse personnelle à quelqun-e pour au final recevoir des e-mails comme: «Hé t'as des infos pour le truc (illégal) mardi soir ?».
C'est pour ça qu'il peut être pas mal de porter rapidement le débat sur ce genre de points, avec des personnes avec qui on pourrait fonctionner et s'organiser. Ça permet aussi de savoir si on veut vraiment fonctionner avec certaine personnes. «Tu veux pas faire gaffe, ok mais sans moi». Dans cette

optique, ça pourrait par exemple être de se poser l'exigence à soi même et de faire la demande aux autres de n'utiliser que des boîtes e-mail PGP-only, Tor-only et Tails-only pour des télécommunications visant à être confidentielles et anonymes. Il faut entendre par là, une messagerie uniquement utilisée via Tails et Tor pour envoyer des e-mails cryptés. Ça permet d'éviter pas mal de plans à la con.

16.3 Quand prendre des précautions ? Quand se passer de l'informatique ?

L'informatique dans son utilisation la plus répandue, offre à la gouvernance des moyens de surveillance et de contrôle social jusque-là inégalés pour continuer à nous écraser. Des keufs faisant main basse sur un disque dur peuvent potentiellement obtenir en quelques clics des infos qui n'auraient pu être arrachées que sous la torture en d'autres endroits et époques... sans l'utilisation de l'informatique.

Mais cette technologie est-elle toujours aliénante et asservissante, ou est-elle parfois aussi émancipatrice et libératrice ? On pourrait étendre cette question à de nombreuses technologies qui envahissent nos vies. On peut se demander pourquoi on utilise l'informatique. Comment pourrait-on s'en passer pour: produire un tract, communiquer et s'organiser à distance, éditer des textes, diffuser largement des infos etc. ? Des personnes s'organisaient bien avant l'informatique et le téléphone, non ?

La question n'est peut-être pas de savoir si dans l'absolu d'un monde rêvé, on désire ou pas ces technologies dans nos vie. On est face au constat qu'elles existent, et qu'on ne peut pas tout faire disparaître d'un claquement de doigts. C'est à double tranchant. Dans ce monde où l'informatique est omniprésente, et tellement souvent au service de l'oppression et de la domination, serait-il pertinent de s'en passer ? N'est-il pas nécessaire de se donner les moyens de se la réapproprier comme, justement, un outil de lutte contre ces structures de domination ? Outil à utiliser du mieux possible si le besoin s'en fait ressentir. Ce qui n'implique pas de l'utiliser tout le temps.
À partir de là, qu'est-ce qui va nous aider à déterminer quand nous passer totalement de l'informatique ou, au contraire, quand nous conforter dans son utilisation ? Et, qu'est-ce qui dans cette utilisation, va nous pousser à prendre de nombreuses précautions, plutôt que d'en profiter de manière insouciante ? On s'aperçoit assez vite de l'impossibilité de résoudre ces interrogations de manière générale, une bonne fois pour toutes. C'est peut-être dû au fait que la notion d'activité ou de donnée sensible, qui a servi de point de départ et de repère régulier à ce texte, est elle-même passablement difficile

à expliquer. Est-ce-que sensible est synonyme de compromettant ? De confidentiel ? D'illégal ? De dangereux ? Peut-être tout ça à la fois ? À partir de quand une action informatique peut-elle être considérée comme sensible ? C'est relatif et très dépendant du contexte dans lequel on se trouve, de ce qu'on fait. C'est tantôt basé sur des sensations diffuses, des hypothèses, tantôt cela semble être une évidence largement partagée. Parfois on s'impose des précautions, juste au cas où, parfois une vague de répression met certaines choses au point (sans forcément mettre tout le monde d'accord).
Après ce tourbillon de points d'interrogation, on pourrait avoir l'impression que puisque qu'on a dit «tout dépend», alors ça veut dire «tout se vaut». En fait non, il y a quand même des pratiques qui sont et resteront pourries. Et inversement, s'il y a bien une généralité qu'on peut faire c'est que plus on fait gaffe, plus on fait gaffe... et plus on fait gaffe, moins on prend de risques. Voici deux manières d'utiliser l'informatique assez répandues parmi des personnes agissant en 2015 avec des idées politiques subversives pour ne pas dire renversantes et qui peuvent peut-être servir de base de réflexion sur ses propres pratiques:

- Certaines personnes peuvent se dire qu'elles placent le seuil de l'activité informatique sensible, dès qu'elles font autre chose que regarder sur le net le dernier clip à la mode ou les horaires de bus. Au delà, elles s'efforcent d'utiliser systématiquement Tails et tout le reste. Ça a l'air assez prudent, mais dans certains cas de surveillance policière ciblée, même aller regarder des horaires de bus sur Internet cesse d'être quelque chose d'anodin.

- Sur un autre plan, il peut être décidé de n'utiliser l'informatique comme moyen de communication qu'en dernier recours et pour se dire le minimum vital. Les e-mails cryptés servent à confirmer ou annuler des rencards pris par des acolytes distant-e-s qui n'ont pas les moyens de se chopper du jour au lendemain. Pour ce qui est par contre d'échange d'infos et d'organisation plus détaillée, l'informatique est bannie, on se bouge le cul pour se voir car rien ne vaut une discussion de vive voix dans un endroit calme.

Bref, qu'on se retrouve ou pas dans ces exemples, il n'en reste pas moins que c'est à chacun-e seul-e et collectivement de voir en fonction de ses besoins, ses possibilités, ses exigences, et des contraintes qu'elles impliquent, afin de pouvoir se décider en connaissance de cause.

Cette brochure a été faite par désir de rassembler les connaissances théoriques et les outils pratiques actuellement les plus efficaces à nos yeux, pour utiliser l'informatique pour des activités sensibles, sans se faire avoir. Concrètement, ça implique d'être en mesure d'agir de manière anonyme, confidentielle et en laissant le moins de traces possible derrière nous. Sans ces précautions, inutile d'espérer déjouer longtemps la surveillance et la répression employées par les États et leurs classes dirigeantes pour continuer à exercer tranquillement leur domination.

Se réapproprier les outils informatiques, c'est comprendre pour mieux se défendre et... attaquer, mais c'est aussi se donner les moyens de pouvoir choisir en connaissance de cause, quand ne pas utiliser l'informatique.

ISBN 978-3-033-05128-7