

# How to take back you privacy?

Naam, Genma

EPITA / Gconfs  
*naam@riseup.net*  
*genma@riseup.net*

01/17/13

# Overview

## 1 Intro

- Why we do this talk ?
- The digital identity
- Questions ?

## 2 HOW TO : Encryption

- WTF is encryption ?
- What can I encrypt ? How ?
- Questions ?

## 3 HOW TO : Anonymity

- Why does it matter ?
- There is always a tool that fit your need
- Questions ?

## 4 Conclusion

- We're not in a XOXO word
- Cryptoparty
- Questions ?

# Sensitive data

## Definition

- a set of values of qualitative or quantitative variables
- individual pieces of information

Some of them are (important|critical)s, don't play with Mallory.

# The right to stay anonymous

The Convention for the Protection of Human Rights and Fundamental Freedoms states that :

## Article 8 - Right to respect for private and family life

- Everyone has the right to respect for his private and family life (...).
- There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society *in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

## You will also see

- Tons of softwares, distributions, techniques to defeat too inquisitive people and censorship.
- What's a Cryptoparty and what you could learn from it.

# L'identité numérique c'est quoi ?

## Définition

- L'identité numérique, c'est l'ensemble des données publiques que l'on peut trouver sur Internet et rattacher à une personne, en l'occurrence moi.
- C'est la fameuse e-reputation.

# L'image que je donne de moi

Googler "son nom".

- Les résultats apparaissant sont-ils bien ce que l'on souhaite ?

## [Le Blog de Genma ...](#)

[genma.free.fr/](http://genma.free.fr/) ▼

Interview de Skhaen, Telecomix et Cyphercat.eu. publié le 13 septembre 2013 par **Genma**.  
C'est via sa conférence à PSES2012, traitant de la cryptographie et ...

## [Genma \(genma\) on Twitter](#)

<https://twitter.com/genma> ▼

The latest from **Genma** (@genma). **Genma** - Compte Officiel ;-) - Un peu linuxien, un peu otaku mais surtout Geek et Blogueur sur Le Blog de **Genma**. Paris.

## [Genma Kun - France | LinkedIn](#)

[fr.linkedin.com/in/genma](http://fr.linkedin.com/in/genma) ▼

Région de Paris , France - Geek, Blogueur, Développeur, Lifehacker  
Voir le profil professionnel de **Genma** Kun (France) sur LinkedIn. Grâce à LinkedIn, le plus grand réseau professionnel au monde, les professionnels comme ...

## [Genma Kun | Facebook](#)

<https://www.facebook.com/genma> ▼

**Genma** Kun is on Facebook. Join Facebook to connect with **Genma** Kun and others you may know. Facebook gives people the power to share and makes the ...

# Adage

## Les paroles s'envolent, les écrits restent

- Cet adage est encore plus vrai avec Internet.
- Il faut partir du principe que ce que l'on dit sera toujours accessible, même des années après.
- Tout ce qui est sur Internet est public ou le sera (même si c'est "privé". Les conditions d'utilisation évoluent. Cf.Facebook).
- Il ne faut donc pas abuser de la liberté d'expression et rester respectueux des lois en vigueur.



# Le pseudonymat

## Définitions

- Contraction des termes pseudonyme et anonymat, le terme de pseudonymat reflète assez bien la volonté contradictoire d'être un personnage public et de rester anonyme...
- Avoir un pseudonyme ne veut pas dire faire et dire n'importe quoi.
- Il en va de l'image que je renvoie, que je donne de moi et de ma crédibilité présente et à venir.
- Un pseudonyme, c'est aussi une identité publique, qui est associée à un ensemble cohérent de compte qui forme un tout : mon blog, mon Twitter, mon compte Facebook.
- L'identité numérique est l'ensemble des données publiques associées à cette identité.

# Exemples

## Twitter

The image shows a Twitter profile card for a user named Genma. The background of the card is a photograph of tall bamboo stalks. At the top center is a square profile picture of a panda's face with a hand cursor icon pointing at it. Below the picture, the name "Genma" is displayed in bold, followed by the handle "@genma". Underneath the handle is a bio: "Genma - Compte Officiel ;-) - Un peu linuxien, un peu otaku mais surtout Geek et Blogueur sur Le Blog de Genma". Below the bio, the location "Paris" and the website "genma.free.fr" are listed. At the bottom of the card, there are three statistics: "6 514 TWEETS", "350 ABONNEMENTS", and "820 ABONNÉS". To the right of these statistics is a button with the Twitter logo and the text "Suivre".

**Genma**  
@genma

Genma - Compte Officiel ;-) - Un peu linuxien, un peu otaku mais surtout  
Geek et Blogueur sur Le Blog de Genma  
Paris · genma.free.fr

6 514 TWEETS   350 ABONNEMENTS   820 ABONNÉS

Suivre

## Linkedin

The image shows a LinkedIn profile card for a user named Genma Kun. The background is a light gray. On the left is a square profile picture of a cartoon panda sitting and holding a small object. To the right of the picture, the name "Genma Kun" is displayed in bold. Below the name is the bio: "Geek, Blogueur, Développeur J2EE/.NET, Lifehacker". Below the bio, the location "Région de Paris , France" and the industry "Internet" are listed.

**Genma Kun**  
Geek, Blogueur, Développeur J2EE/.NET, Lifehacker  
Région de Paris , France | Internet

# Something unclear ?



Feel free to ask for questions now.

# Définitions - cryptage, crypter, chiffrement ?

## Le chiffrement

Le chiffrement consiste à chiffrer un document/un fichier à l'aide d'une clef de chiffrement. L'opération inverse étant le déchiffrement.

## Le cryptage

Le terme « cryptage » est un anglicisme, tiré de l'anglais encryption. Le décryptage existe : il s'agit de "casser" un document chiffré lorsqu'on n'en a pas la clef.

## La cryptographie

La science quant-à elle s'appelle la "cryptographie".

# Le chiffrement, comment ça se passe ?

## Le chiffrement symétrique

Cela consiste à chiffrer un message avec la même clef que celle qui sera utilisé pour le déchiffrement.

Exemple : le code de César avec un décalage de lettres. A->C, B->D etc.

Nous venons en paix -> Pqwu xgpqpu gp rckz

On applique le processus inverse pour avoir le message.

## Une clef de chiffrement c'est quoi ?

Une clef s'appelle une clef car elle ouvre/ferme le cadenas qu'est l'algorithme de chiffrement utilisé.

- Ici, l'algorithme est dans la notion de décalage.
- La clef est le nombre de lettre décallées (ici deux lettres).

# Le chiffrement asymétrique 1/2

## Clef publique - clef privée

Le chiffrement asymétrique repose sur le couple clef publique - clef privée.

⇒ Ce qu'il faut comprendre/retenir :

- Ma clef privée est secrète.
- Ma clef publique est distribuée à tous.

## L'algorithme de chiffrement

L'algorithme de chiffrement est bien plus complexe que le fait de décaler des lettres ; il repose sur des notions mathématiques (nombre premiers...)

# Le chiffrement asymétrique 2/2

## Le chiffrement

Avec la clef publique de mon correspondant, je chiffre un fichier.  
⇒ Le fichier ne peut plus être déchiffré que par la personne qui possède la clef privée correspondant à la clef publique que j'ai utilisée (donc mon correspondant).

## Le déchiffrement

Avec sa clef privée, mon correspondant déchiffre le fichier.  
⇒ Il peut alors lire le message.

## Cas concret

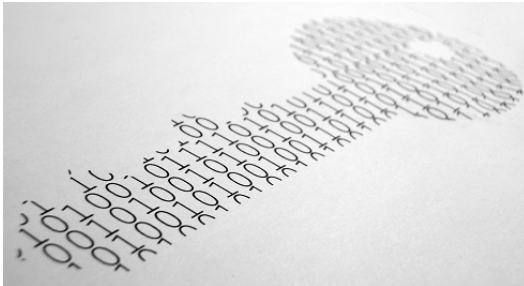
Le chiffrement de ses mails avec PGP.

# Bob envoie un message à Alice





# Pourquoi chiffrer ?



# Chiffrer - Les arguments contre

Personne ne le fait...

FAUX. Sans le savoir, vous le faites tous les jours.

Exemple 1 : "le cadenas" quand on se connecte

Exemple 2 : La clef du Wifi.

Je n'ai rien à cacher...

FAUX. Qui accepterait que le facteur lise son courrier médical ?

Le chiffrement, c'est pour les pédonazis de l'Internet...

FAUX. Cas des journalistes/blogueurs dissidents qui dénoncent des dictatures...

# Chiffrer - Les arguments pour

Le chiffrement, ce n'est pas si compliqué

Ce n'est pas plus compliqué que d'utiliser un "logiciel" ; i faut comprendre le principe et c'est du clickodrome.

Protection et sécurité

Mes données personnelles, sensibles sont protégées. Cf. PRISM, NSA...

Confidentialité

Seule la personne à qui est destiné le "message" est en mesure de le lire.

# Edward Snowden

Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on.



Le chiffrement fonctionne. Correctement mis en œuvre, les systèmes cryptographiques forts sont l'une des rares choses sur lesquelles vous pouvez compter.

## Limites du chiffrement

Ce qui est chiffré aujourd'hui pourra être déchiffré demain

Les ordinateurs de demain pourront permettre de décrypter les données chiffrées aujourd'hui.

Si on perd la clef

On n'a plus accès aux données.

Métadonnées, graphe social

**PGP ne protège pas contre l'analyse des métadonnée (serveurs de transit, adresses, headers, sujet).** Ne pas oublier de nettoyer les métas-données des fichiers (tag EXIF des photos, documents de bureautiques avec le suivi des modifications). DNS, cas du tracking Internet...

# Le chiffrement et la loi

En France, la loi considère donc que l'utilisation de moyens de cryptologie est libre (LCEN article 30-1) et il n'y a donc, actuellement pas de limite à la taille de la clef de chiffrement que l'on peut utiliser.

En cas de perquisition, le refus de remise de la clef de chiffrement peut entraîner 3 ans d'emprisonnement ainsi que 45000€ d'amende.

Cette peine est aggravée dans le cas où le chiffrement a été utilisé pour commettre un délit.

Il est donc recommandé de donner la clef de déchiffrement, sauf dans le cas où les données déchiffrées entrainerait une procédure judiciaire dont la peine finale serait supérieure à celle de l'entrave à l'enquête judiciaire.

# Le chiffrement

## En local - ses données

- Son disque dur
- Sa clef USB
- Son smartphone

## En réseau - ses communications

- Https : utilisation de l'extension HTTPSEveryWhere pour Firefox
- Ses e-mails : utilisation de GPG via Enigmail pour Thunderbird
- Sa connexion : utiliser un VPN, SSH, la clef "WIFI".

⇒ À chaque "usage", il y a une solution de chiffrement possible.

# Les mails - PGP, GPG ?

## PGP

Pretty Good Privacy - PGP est un logiciel de chiffrement et de déchiffrement cryptographique, créé par l'américain Phil Zimmermann en 1991.

## OpenPGP

Ce standard décrit le format des messages, signatures ou certificats que peuvent s'envoyer des logiciels comme GNU Privacy Guard. Ce n'est donc pas un logiciel, mais un format pour l'échange sécurisé de données, qui doit son nom au programme historique Pretty Good Privacy (PGP).

## GnuPG

GnuPG (ou GPG, de l'anglais GNU Privacy Guard) est l'implémentation GNU du standard OpenPGP.



# Chiffrer son disque dur

## Logiciels intégrés aux systèmes d'exploitations


- Windows 7/8 : Bitlocker (Backdor)
- MacOS : FileVault
- GNU/Linux : Encfs...


Peut-on faire confiance à autre chose du logiciel libre ?

## Indépendamment du système d'exploitation

⇒ Le logiciel TrueCrypt. Pour une clef USB/un disque dur externe.

# L'audit de TrueCrypt

 browse | learn | create Sign Up | Log In




## The TrueCrypt Audit

People, businesses, and governments all over the world use TrueCrypt to protect their privacy. We need help making it better and more secure.

Technology – Research Triangle, North Carolina, United States

[Campaign Home](#) | [Updates / 0](#) | [Comments / 24](#) | [Funders / 1166](#)



**\$41,890** USD

Raised of \$25,000 Goal

**29** days left

**CONTRIBUTE NOW**

**Flexible Funding**  
This campaign will receive all funds raised even if it does not reach its goal. Funding duration: October 14, 2013 - December 13, 2013 (11:59pm PT).

Share This Campaign: <http://igg.me/at/truecryptaudit/csbw> [★ Follow](#)

Select a Perk for your contribution



# Something unclear ?



Feel free to ask for questions now.



# TOR - The Onion Router

# Présentation du réseau TOR

Tor est un logiciel libre,

- grâce auquel existe le réseau d'anonymisation Tor
- soutenu par l'organisation The Tor Project.

⇒ Techniquement, Tor nous permet de se connecter à des machines sur Internet via des relais.

⇒ Et cela de façon à ce qu'elles ne puissent pas identifier notre connexion (et donc de nous localiser).

# A quoi sert TOR ?

Concrètement, ça sert pour :

- échapper au fichage publicitaire,
- publier des informations sous un pseudonyme,
- accéder à des informations en laissant moins de traces,
- déjouer des dispositifs de filtrage (dans sa fac, en Chine ou en Iran...),
- communiquer en déjouant des dispositifs de surveillances,
- tester son pare-feu,
- ... et sûrement encore d'autres choses.

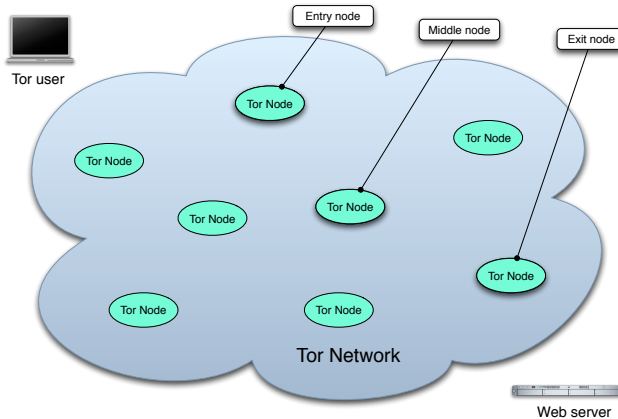
⇒ Tor dispose également d'un système de « services cachés » qui permet de fournir un service en cachant l'emplacement du serveur.



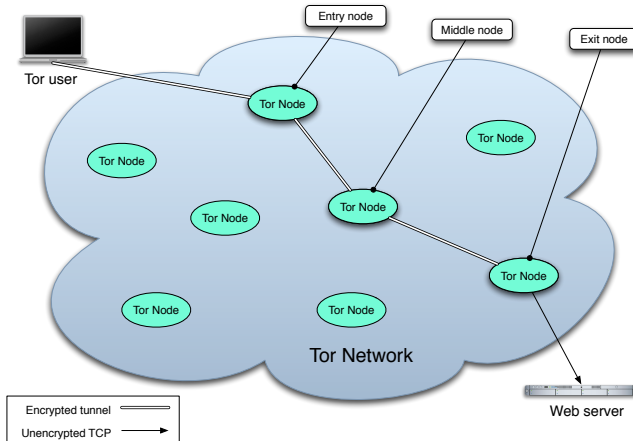
# A quoi sert TOR ?

Tor est un réseau d'anonymisation, donc par définition, c'est difficile de faire un compte précis. Tor ne fait rien pour cacher que nous utilisons Tor. Donc quand en utilisant Tor, nous nous mettons au milieu de la foule des gens qui utilisent Tor. Plus cette foule est grande, meilleur est l'anonymat.

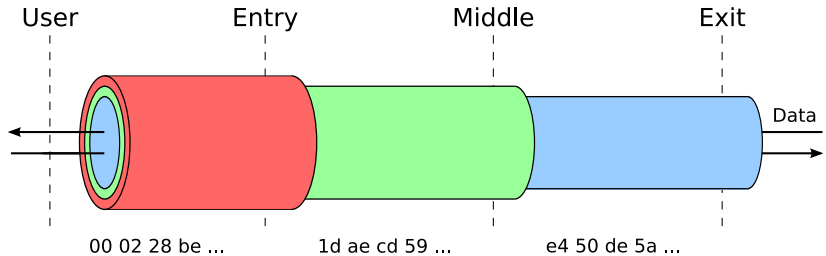
# Comment fonctionne Tor ?



# Comment fonctionne Tor ?



# Comment fonctionne Tor ?



# Comment fonctionne Tor ?

Ce tunnels se fait « en oignon » avec des couches de chiffrement empilées. Il y a une première clé de chiffrement vers le nœud d'entrée, une seconde clé vers le nœud du milieu et une dernière pour le nœud de sortie.

Il faut noter que Tor ne s'occupe pas de chiffrer après le nœud de sortie. Comme n'importe qui peut mettre en place un nœud de sortie, c'est une bonne idée de chiffrer sa communication en plus (par exemple en se connectant aux sites web que l'on visite en HTTPS). Après, se déroule tout un processus pour établir un tunnel chiffré jusqu'au nœud de sortie.

## Utiliser Tor - Le Tor Browser

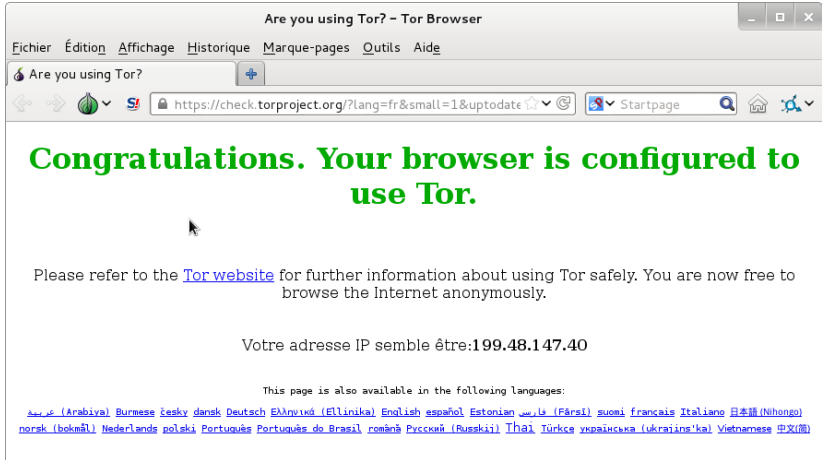
Le Tor Browser est une version Extended Support de Firefox, auxquelles sont ajoutée les extensions préconfigurées permettant qu'au lancement du navigateur, celui-ci se connecte à Tor.

⇒ Ainsi, toute la navigation qui se fait via ce navigateur est faite au travers du réseau Tor.

⇒ C'est simplissime.

Toutes les versions (dans différentes langues, différents OS) sont disponibles sur le site du projet : <https://www.torproject.org/projects/torbrowser>

# Le Tor Browser



# Tor Browser Launcher

Pour avoir un Tor Browser toujours à jour, on peut installer le Tor Browser Launcher. <https://github.com/micahflee/torbrowser-launcher>

Il gère :

- le téléchargement de la version la plus récente de TBB, dans votre langue et pour votre architecture
- la mise à jour automatique (tout en conservant vos signets et préférences) manuel
- la vérification de la signature GnuPG du TBB (pour être sûr de l'intégrité des fichiers)
- ajoute un lanceur d'application "Tor Browser" dans le menu de votre environnement de bureau.



# Utiliser Tor - Tails

Tails est un système d'exploitation complet basé sur Linux et Debian, en live.

The screenshot shows the Tails website interface. At the top, there's a navigation bar with 'news' and 'Appel à tester Tails 0.19-rc1'. The main heading is 'Appel à tester Tails 0.19-rc1'. Below it, a paragraph explains the purpose of the test version. A list of links is provided: 'Comment tester Tails 0.19-rc1 ?', 'Quoi de neuf depuis la 0.18 ?', and 'Problèmes connus dans la version 0.19-rc1'. A green button 'Télécharger Tails Tails 0.18' is visible on the right. Below the heading, a section 'Comment tester Tails 0.19-rc1 ?' contains a list of instructions. The first instruction is to download the ISO and signature, with corresponding green buttons. The second instruction is to verify the ISO. The third instruction is to check for problems, with links to 'problèmes connus de cette version' and 'problèmes connus de longue date'. The fourth instruction is to test the system. The fifth instruction is to report problems, with links to 'rapporter', 'points bonus si vous vérifiez que ce n'est pas un problème connu de cette version', and 'problème connu de longue date'. A sidebar on the right contains links: 'À propos', 'Premiers pas...', 'Documentation', 'Aide & Support', and 'Participer'. At the bottom, there's a section 'Quoi de neuf depuis la 0.18 ?' with a link to 'Nouvelles fonctionnalités' and a version number 'Linux 3.9.5-1'.

Tails  
The Amnesic Incognito Live System

news Appel à tester Tails 0.19-rc1

Français (63 %) EN DE ES PT

## Appel à tester Tails 0.19-rc1

Vous pouvez aider Tails ! La première (et on espère seule) version candidate pour la version 0.19 à venir est sortie. Merci de la tester et de voir si tout fonctionne pour vous.

- 1. [Comment tester Tails 0.19-rc1 ?](#)
- 2. [Quoi de neuf depuis la 0.18 ?](#)
- 3. [Problèmes connus dans la version 0.19-rc1](#)

### Comment tester Tails 0.19-rc1 ?

1. Gardez à l'esprit que c'est une image de test. Nous nous sommes assurés qu'elle n'est pas corrompue d'une manière évidente, mais elle peut toujours contenir des problèmes non découverts.
2. Téléchargez l'image ISO et sa signature :
  - [Image ISO de Tails 0.19-rc1](#)
  - [Signature de Tails 0.19-rc1](#)
3. Vérifiez l'image ISO.
4. Jetez un oeil à la liste des [problèmes connus de cette version](#) et à la liste des [problèmes connus de longue date](#).
5. Testez à volonté !

Si vous découvrez quelque chose qui ne fonctionne pas comme prévu, merci de [nous le rapporter](#) ! Points bonus si vous vérifiez que ce n'est pas un [problème connu de cette version](#) ou un [problème connu de longue date](#).

### Quoi de neuf depuis la 0.18 ?

- Nouvelles fonctionnalités
  - » Linux 3.9.5-1.

[Télécharger Tails Tails 0.18](#)  
Dernière version : 18 mai 2013

À propos  
Premiers pas...  
Documentation  
Aide & Support  
Participer

## Tor hidden service - les services cachés de TOR

Tor permet aux clients et aux relais d'offrir des services cachés. Il est possible d'offrir un serveur web, un serveur SSH, etc, sans révéler son adresse IP aux utilisateurs.

- Tous ces sites ne sont accessibles que via le réseau Tor.
- Ils portent une adresse qui se termine par .onion.
- Des wikis et moteurs de recherches référencient ces services.

# Soutenir Tor

Il existe l'association NosOignons.net, qui propose des nœuds de sortie Tor financés par la communauté. <https://nos-oignons.net>

- En parler
- Faire un don
- Mettre en place un relais

Sur Internet, si c'est gratuit,  
c'est vous le produit

# Qu'est-ce que le pistage ?

## Le pistage sur Internet

- Le pistage est un terme qui comprend des méthodes aussi nombreuses et variées que les sites web, les annonceurs et d'autres utilisent pour connaître vos habitudes de navigation sur le Web.
- Cela comprend des informations sur les sites que vous visitez, les choses que vous aimez, n'aimez pas et achetez.
- Ils utilisent souvent ces données pour afficher des pubs, des produits ou services spécialement ciblés pour vous.

# Comment est-on tracké ?

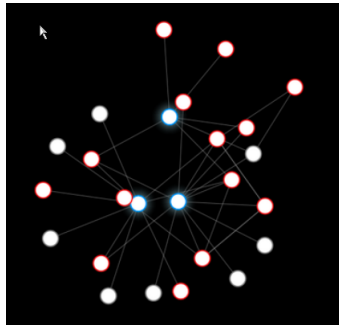
## Toutes les publicités nous espionnent

- Le bouton Like de Facebook : il permet à FaceBook de savoir que vous avez visité ce site, même si vous n'avez pas cliqué sur ce bouton.
- Même si vous vous êtes correctement déconnecté de Facebook.
- De même pour le bouton le +1 de Google, les scripts de Google Analytics,
- Tous les publicité, Amazon...



# L'extension Firefox LightBeam (ex Collusion)

Cette extension permet de voir en temps réel qui nous traque et les interconnexions qu'a le site actuellement visité avec d'autres sites.



# Anonymat et extensions pour Firefox

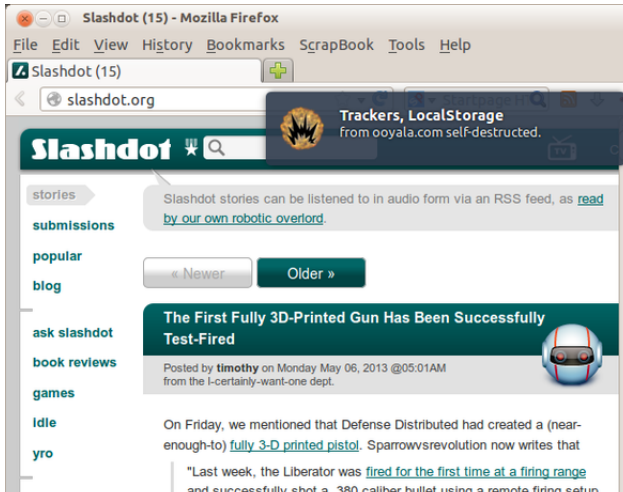


# Noscript

Bloque tous les trackers associés au site.

# Self destructing cookie

Suppression automatisée des cookies



# Changer de moteur de recherche

# Duckduckgo - Google tracks you. We don't.

`https://duckduckgo.com/`



# Et pour plus de sécurité ?

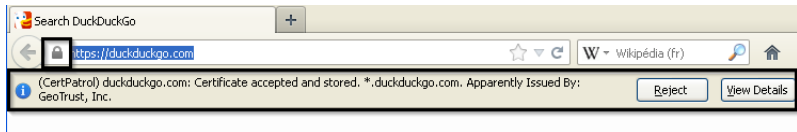
# HTTPSEverywhere

Force le passage en https quand celui-ci est proposé par le site.



# Certificate Patrol

Permet de valider les certificats d'un site (lié à https).



## Something unclear?



Feel free to ask for questions now.



# Le crypto-anarchisme

Tout le monde chiffre et ce qui est vraiment important est chiffré et noyé dans la masse.

On crée du bruit ce qui empêche la surveillance de masse (Affaire PRISM...)

Attention, à l'heure actuel, le chiffrement étant peu répandu, toute personne qui chiffre ses e-mails pourra être considérée comme suspecte.

# Relativité de l'anonymat de nos jours

## Analyse sur les éléments de langage

- On peut identifier quelqu'un à sa typographie, son style, son vocabulaire, sa culture, ses idées..
- La fréquence des mots utilisés, la tournure de phrase, le genre...
- Techniques utilisées pour déterminer qui se cachent derrière des Anonymous...

## Attention aux Logs

- Les horaires de connexions et l'estimation du fuseau horaire donnent également des informations...





# Something unclear?



Feel free to ask for questions now.

# Rendez vous at the Cryptoparty

CRYPTOPARTY