

# SilexLabs - Reprenez le contrôle de votre vie privée sur Internet

Genma

December 21, 2015



This work is licensed under the *Creative Commons Attribution-NonCommercial-ShareAlike 3.0 License*.

SilexLabs



« Tous les Événements »

## REPRENEZ LE CONTRÔLE DE VOTRE VIE PRIVÉE SUR INTERNET

19 janvier 2016 @ 19:00 - 21:00 | Gratuit



**MARDI 19 JANVIER**

19H  
21H



**Vie privée & Internet**

**Vie privée**

**mozilla** 16 bis Boulevard Montmartre 75009 PARIS

Genma



# A propos de moi

## Où me trouver sur Internet?

- Le Blog de Genma :  
<http://genma.free.fr>
- Twitter :  
<http://twitter.com/genma>

## Mes projets-contributions

Plein de choses dont :

- Des conférences sur plein de thèmes différents

**Le Blog de Genma**

**Rencontre avec Genma IRL**

publié le 5 août 2013 par **Genma**

Si tu es un lecteur régulier de ce blog, que tu souhaites me voir autour d'un verre, pour manger dans un resto où tu pourrais simplement discuter, contacte moi que l'on se fixe un rendez-vous. En effet, je serai disponible du dimanche 11 août au mardi 20 août, en fin de journée ou le soir, à l'endroit que tu souhaites, sur Paris, France. Si tu es partant, fais signe... A la suite de cette rencontre, je pourrais faire (ou non), si tu es d'accord, un petit compte-rendu sur mon blog, ainsi que quelques (...)

**POUR LIRE LA SUITE...**

**Lifefacking - L'importance du matériel**

publié le 2 août 2013 par **Genma**

Un bon artisan doit avoir de bons outils pour faire du bon travail. Un meilleur musicien ne sera pas avec une basse si son instrument de musique n'est pas de qualité. Il en est de même pour l'informatique. Ça n'est pas la taille qui compte.

En fait, pendant deux ans, sur ma mission précédente, j'avais pour travailler du bricolage. Un écran 22" et un écran 15" (celui du portable), l'un sur l'autre de l'autre. Avec ma nouvelle mission, je suis passé sur un unique écran de 17", avec un PC plus lent (je (...))

**POUR LIRE LA SUITE...** TAGS : Lifefacking

**Syndication**

**rechercher**

**Cà lire**

Actualités GENMA de la semaine

Blog : tout et rien

# Programme

Pourquoi ne dit-on pas crypter ? Un peu de théorie

- Le principe du chiffrement
- Le chiffrement symétrique (Cesar)
- Le chiffrement asymétrique (les enveloppes)

Le chiffrement en pratique

- Connexion Internet httpS
- Le coffre-fort numérique avec TrueCrypt/Veracrypt

Comment est-on suivi à la trace sur Internet?

- Les publicités et le tracking par scripts (Le bouton j'aime de Facebook / Lightbeam)
- Comment les bloquer.

Aller plus loin? Tor et le TorBrowser

- Comment l'installer, comment ça marche...

Pourquoi ne dit-on pas crypter  
? Un peu de théorie

# Le principe du 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 symétrique (Cesar)

## 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.

# Le chiffrement en pratique

# HttpsEverywhere

Avoir une connexion httpS dès que possible

 **ELECTRONIC FRONTIER FOUNDATION**  
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

HOMEABOUTOUR WORKDEEPLINKS BLOGPRESS ROOM



## HTTPS Everywhere

**HTTPS Everywhere**

FAQ

Report Bugs / Hack On The Code

Creating HTTPS Everywhere Rulesets

How to Deploy HTTPS Correctly

HTTPS Everywhere Atlas

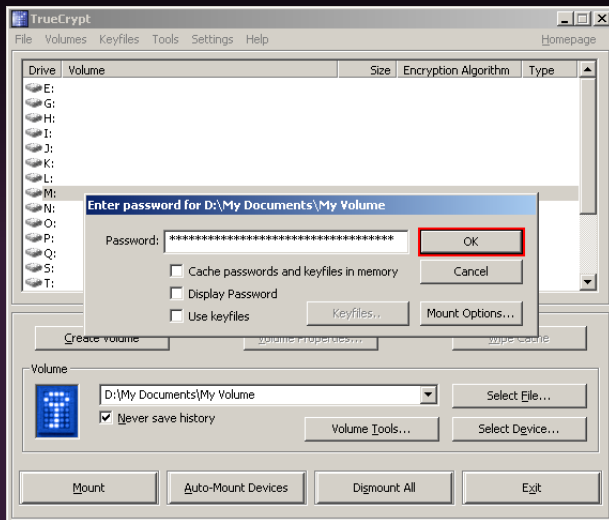
HTTPS Everywhere is a Firefox, Chrome, and Opera extension that encrypts your communications with many major websites, making your browsing more secure.

**Encrypt the web: Install HTTPS Everywhere today.**

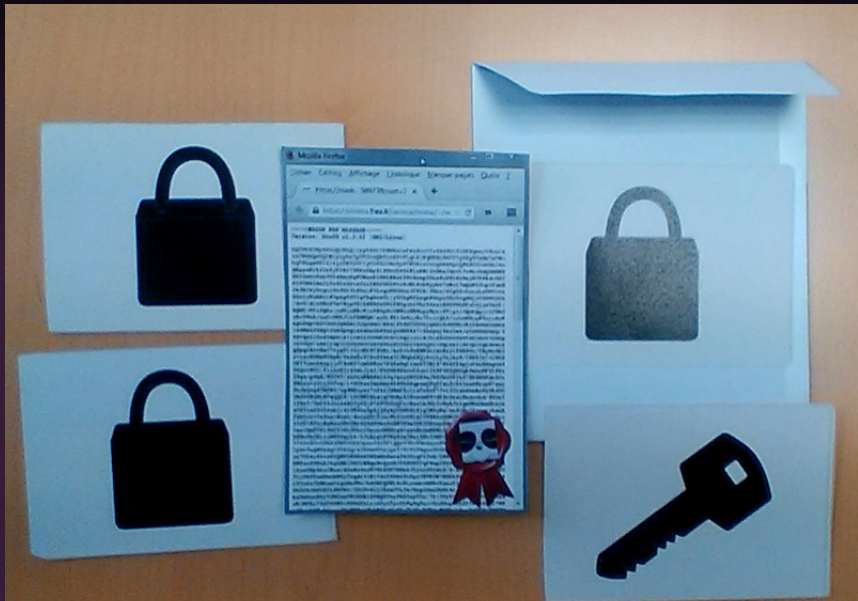


**Install in Firefox**

# Le coffre-fort numérique avec TrueCrypt/Veracrypt



# Les enveloppes



Comment est-on suivi à la  
trace sur Internet?



# Comment est-on pisté ?

## 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...

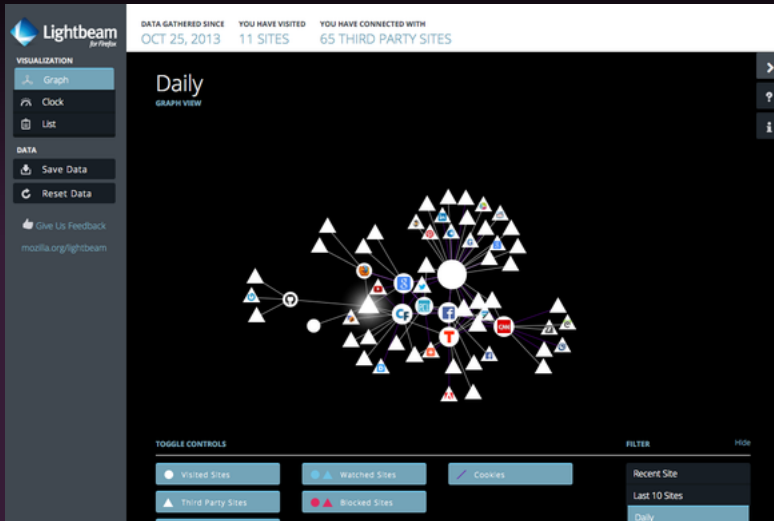


# Le tracking publicitaire

## 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.

# Lightbeam



# AdBlock - block 1/2


Page avec publicité :

01net - informatique high-tech : actu, produits, téléchargement logiciels et jeux - Mozilla Firefox

Fichier Édition Affichage Historique Marque-pages Outils ?

01net - informatique high-tech : actu, produi... +

← → www.01net.com ☆ RSS ▼ W Wikipédia (fr)



DOSSIER  
**iPad 5**

**J'Y VAIS**

en partenariat avec  
**numericable**

**01net**

Rechercher un logiciel OK


**01net** Utilisez 01net pour 2,45 € / n° seulement.

Marre de payer votre CB ? N'hésitez plus, cliquez !

ACTUALITÉS COMPARATIFS ET TESTS JEUX ASTUCES VIDÉO **telecharger.com** BONS PLANS FORUM 01BUSINESS 01MEN

Retrouvez toutes les informations sur la conférence Apple

**J'Y VAIS**



Retrouvez toutes les informations sur la conférence Apple

**J'Y VAIS**

en partenariat avec  
**numericable**



**iPad Air et iPad mini Retina: les premières prises en main en vidéo**

Apple a dévoilé hier soir deux nouvelles tablettes: un iPad Air plus fin et plus léger, ainsi qu'un iPad mini avec écran Retina. 01net vous livre son impression, produits à l'appui.



**01net**

iPad Air et iPad mini Retina: les premières prises en main en vidéo

23/10/2013 à 08:30

Apple, Nokia, Microsoft : rendez-vous ce soir pour un grand show

# AdBlock - Microblock 2/2

Bloque les publicités. Allège les pages.

01net - informatique high-tech : actu, produits, téléchargement logiciels et jeux - Mozilla Firefox

Fichier Édition Affichage Historique Marque-pages Outils ?

01net - informatique high-tech : actu, produi... +

www.01net.com

W - Wikipédia (fr)

01net

Rechercher un logiciel OK

nos newsletters

nos magazines

01net Utilisez 01net pour 2,45 C / n° seulement

ACTUALITÉS COMPARATIFS ET TESTS JEUX ASTUCES VIDÉO **telecharger.com** BONNS PLANS FORUM 01BUSINESS 01MEN

**iPad Air et iPad mini Retina: les premières prises en main en vidéo**

Apple a dévoilé hier soir deux nouvelles tablettes: un iPad Air plus fin et plus léger, ainsi qu'un iPad mini avec écran Retina. 01net vous livre son impression, produits à l'appui.

**LA CHAÎNE TECHNO**

**01net**

iPad Air et iPad mini Retina: les premières prises en main en vidéo  
23/10/2013 à 08:30

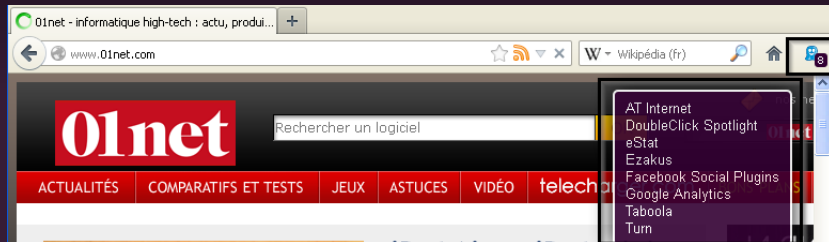
Apple, Nokia, Microsoft : rendez-vous ce soir pour un grand show live...  
23/10/2013 à 07:00

Découvrez la Nvidia Shield, une console "concept" sous Android qui...  
21/10/2013 à 07:00  
> Toutes les vidéos

**TOP TESTS**

# Ghostery

Bloque tous les trackers associés au site.



Aller plus loin? Tor et le  
TorBrowser

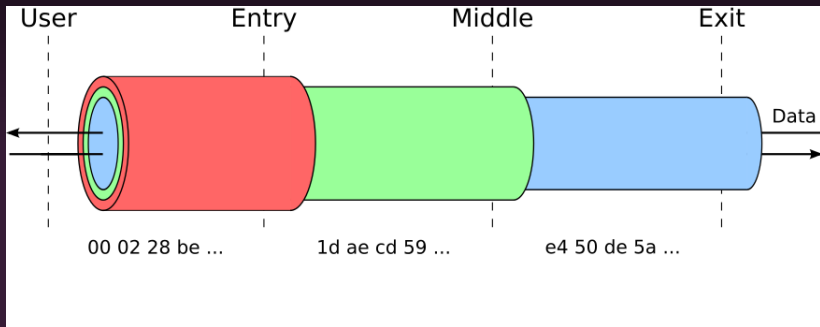
# Quelques mots sur Tor ?



Attention : la présentation *complète*  
dure une bonne heure et demie...



# Comment fonctionne Tor ?



# Tor et les enveloppes



# A quoi sert TOR?

## Ce que l'usage de Tor permet de faire

- d'échapper au fichage publicitaire,
- de publier des informations sous un pseudonyme,
- d'accéder à des informations en laissant moins de traces,
- de déjouer des dispositifs de filtrage (sur le réseau de son entreprise, de son Université, en Chine ou en France...),
- de communiquer en déjouant des dispositifs de surveillance,
- de tester son pare-feu,
- ... et sûrement encore d'autres choses.

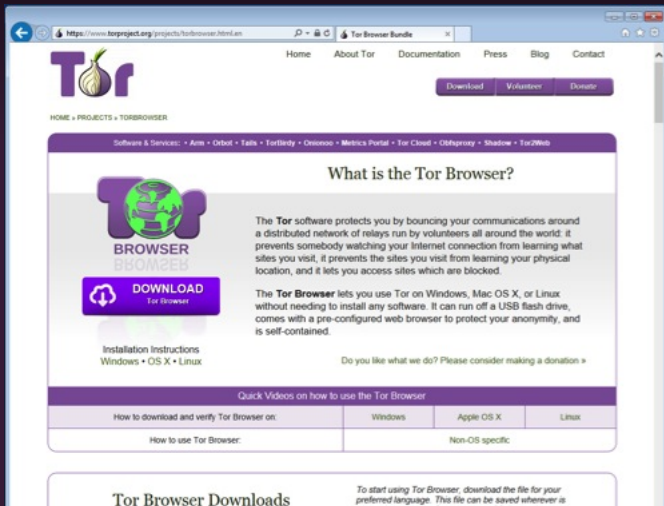
⇒ Tor dispose également d'un système de "services cachés" qui permet de fournir un service en cachant l'emplacement du serveur.

# Télécharger le Tor Browser

Toutes les versions (dans différentes langues, différents OS) sont disponibles sur le site du projet :

<https://www.torproject.org/>

Rq : Il existe la possibilité de le recevoir par mail...



The screenshot shows the Tor Browser project website. At the top, there's a navigation bar with links: Home, About Tor, Documentation, Press, Blog, and Contact. Below this is a large purple banner with the Tor logo (a purple onion) and the text "Tor Browser". To the right of the logo are buttons for "Download", "Volunteer", and "Donate". Below the banner, there's a section titled "What is the Tor Browser?". It contains a paragraph explaining that Tor software protects users by bouncing communications around a distributed network of relays. Below this paragraph is a "DOWNLOAD" button with a download icon. To the right of the button is a link to "Installation Instructions" for Windows, OS X, and Linux. Below the "DOWNLOAD" button is a link to "Quick Videos on how to use the Tor Browser". At the bottom, there's a table with two rows and three columns. The first row is titled "How to download and verify Tor Browser on:" and has columns for "Windows", "Apple OS X", and "Linux". The second row is titled "How to use Tor Browser:" and has a single column for "Non-OS specific".

HOME • PROJECTS • TORBROWSER

Software & Services: • Arm • Orbit • Tails • Tortirely • Onionoo • Metrics Portal • Tor Cloud • Obfsproxy • Shadow • Tor2Web

## What is the Tor Browser?

The **Tor** software protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, it prevents the sites you visit from learning your physical location, and it lets you access sites which are blocked.

The **Tor Browser** lets you use Tor on Windows, Mac OS X, or Linux without needing to install any software. It can run off a USB flash drive, comes with a pre-configured web browser to protect your anonymity, and is self-contained.

Do you like what we do? Please consider making a donation »

### Quick Videos on how to use the Tor Browser

How to download and verify Tor Browser on:	Windows	Apple OS X	Linux
How to use Tor Browser:	Non-OS specific		

## Tor Browser Downloads

To start using Tor Browser, download the file for your preferred language. This file can be saved wherever is

# Lancer le Tor Browser

A propos de Tor - Navigateur Tor

A propos de Tor

Saisir un terme à rechercher ou une adresse

Google

Le menu de l'oignon vert a maintenant un curseur de sécurité qui vous laisse ajuster votre niveau de sécurité. Découvrez le !

Ouvrir préférences de sécurité

Navigateur Tor 4.5



## Félicitations !

Ce navigateur est configuré pour utiliser Tor.

*Vous pouvez maintenant naviguer sur Internet de manière anonyme.*

[Tester les paramètres du réseau Tor](#)

### Que faire ensuite ?

Tor n'est PAS tout ce dont vous avez besoin pour assurer votre anonymat ! Vous devrez peut-être changer certaines de vos habitudes de navigation pour garder votre identité en sécurité.

[Conseils pour rester anonyme »](#)

### Vous pouvez aider !

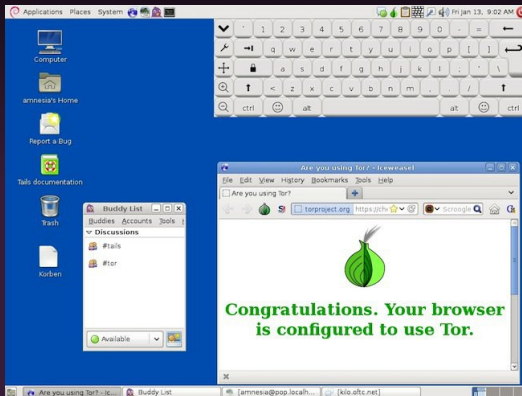
Vous pouvez aider à rendre le réseau Tor plus rapide et plus puissant de plusieurs manières :

- [Faire fonctionner un relai Tor »](#)
- [Devenir bénévole »](#)
- [Faire un don »](#)

Le projet Tor est une organisation à but non lucratif (US 501(c)(3)) dédiée à la recherche, le développement et l'éducation sur l'anonymat et la vie privée en ligne. [En savoir plus sur le projet Tor »](#)

# Utiliser Tor - Tails

Tails (The Amnesic Incognito Live System) est un système d'exploitation complet basé sur Linux et Debian, en live.



<https://tails.boom.org>

Merci de votre attention.  
Place aux questions.



Me contacter?

Le Blog de Genma  
<http://genma.free.fr>

Twitter : @genma



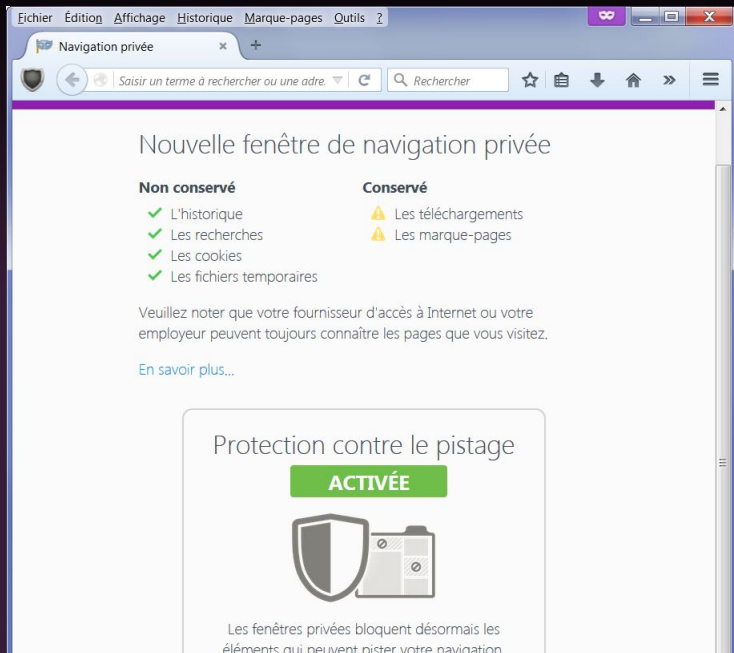
# ANNEXES

# La navigation en mode privée 1/2

Quelles données ne sont pas enregistrées durant la navigation privée ?

- pages visitées ;
- saisies dans les formulaires et la barre de recherche ;
- mots de passe ;
- liste des téléchargements ;
- cookies ;
- fichiers temporaires ou tampons.

# La navigation en mode privé 2/2



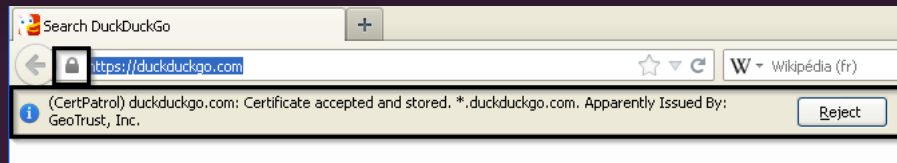
# Comment vérifier rapidement la sécurité d'un site ?

## La check-liste

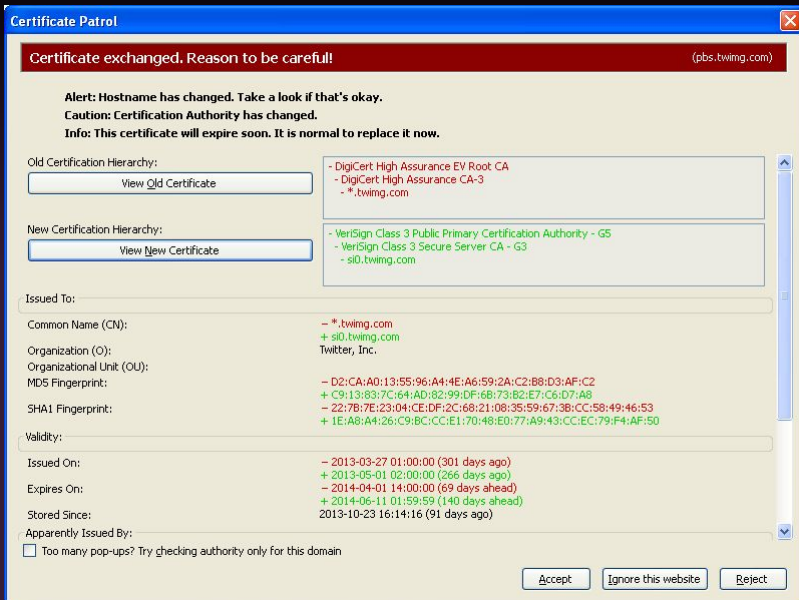
- Le site a-t-il une connexion en https ? (SSL).
- Y-a-t-il intégration d'éléments extérieurs au site en lui-même ?
- Le site utilise-t-il Google Analytics ?
- Le site utilise-t-il Google Fonts ?
- Le site utilise-t-il des régies publicitaires ?
- Le site utilise-t-il Cloudflare ?
- Le DNS est-il géré par Cloudflare ?
- Le site présente-t-il une politique de confidentialité ?
- Le site utilise-t-il les cookies ?
- Le site utilise-t-il des scripts javascript ?

# Certificate Patrol

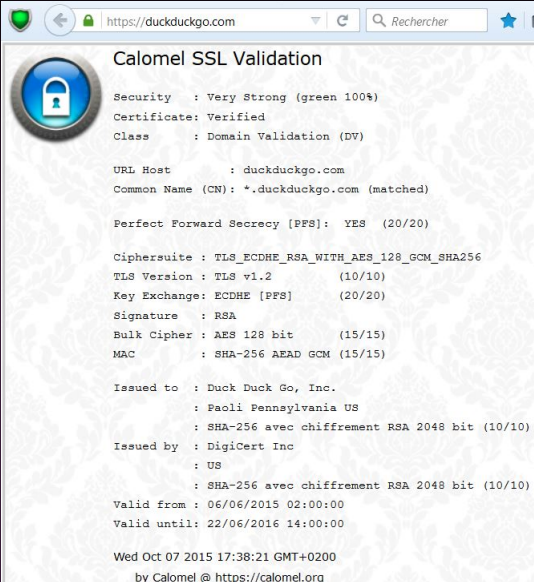
Permet de valider les certificats d'un site (lié à https).



# Certificate Patrol



# Calomel SSL



The image shows a web browser window with the address bar displaying `https://duckduckgo.com`. The page title is "Calomel SSL Validation". On the left, there is a circular icon with a blue padlock. The main content area displays the following information:

Security : Very Strong (green 100%)  
Certificate: Verified  
Class : Domain Validation (DV)

URL Host : duckduckgo.com  
Common Name (CN): \*.duckduckgo.com (matched)

Perfect Forward Secrecy [PFS]: YES (20/20)

Ciphersuite : TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256  
TLS Version : TLS v1.2 (10/10)  
Key Exchange: ECDHE [PFS] (20/20)  
Signature : RSA  
Bulk Cipher : AES 128 bit (15/15)  
MAC : SHA-256 AEAD GCM (15/15)

Issued to : Duck Duck Go, Inc.  
: Paoli Pennsylvania US  
: SHA-256 avec chiffrement RSA 2048 bit (10/10)

Issued by : DigiCert Inc  
: US  
: SHA-256 avec chiffrement RSA 2048 bit (10/10)

Valid from : 06/06/2015 02:00:00  
Valid until: 22/06/2016 14:00:00

Wed Oct 07 2015 17:38:21 GMT+0200  
by Calomel @ <https://calomel.org>

# L'authentification forte



# L'authentification forte

Différents termes, un même usage

Double authentification, Connexion en deux étapes, 2-Step Verification

## Exemple avec Google

Google permet aux utilisateurs d'utiliser un processus de vérification en deux étapes.

- La première étape consiste à se connecter en utilisant le nom d'utilisateur et mot de passe. Il s'agit d'une application du facteur de connaissance.
- Au moment de la connexion Google envoie par SMS un nouveau code unique. Ce nombre doit être entré pour compléter le processus de connexion.

Il y a aussi une application à installer qui génère un nouveau code toutes les 30 secondes.

# L'authentification forte

## Autres services implémentant cette fonctionnalité

- Web : Facebook, Twitter, Linkedin, Paypal
- Banque : envoi d'un code par SMS