

Berner l'espionnage de l'Internet avec Firefox



par Raymond Ouellette
pour LinuQ – JILL2018



LINUQ

<http://linuq.org>

PARLEZ EN et n'hésitez pas à utiliser cette
présentation, elle est libre de droit (à condition
d'y référer et de respecter les références des
emprunts que j'ai fait)



Pourquoi Firefox?



- Fureteur libre de la fondation Mozilla
- Respecte votre vie privée
- Mozilla promeut la neutralité de l'Internet
- La Free Software Foundation suggère plutôt l'utilisation de la version GNU de Firefox : IceCat



(basée sur Firefox Extended Support Release ou ESR). Voir <https://directory.fsf.org/wiki/IceCat>

Suis-je unique?



- Voir l'empreinte laissée par notre fureteur
<https://amiunique.org/>

Vue d'ensemble

Détails

Graphiques

Êtes-vous unique ?

Presque ! (Vous pouvez très probablement être tracé.)

42.18 % des navigateurs observés sont **Firefox**, comme le vôtre.

0.20 % des navigateurs observés sont **Firefox 62.0**, comme le vôtre.

14.12 % des navigateurs observés sont installés sur **Linux**, comme le vôtre.

9.88 % des navigateurs observés sont réglés en "**fr**", comme le vôtre.

5.18 % des navigateurs observés sont réglés sur le fuseau horaire **UTC-4**, comme le vôtre.

Mais **seulement 2** navigateurs parmi les 824006 observés (0.00 %) ont exactement la même empreinte que celle de votre navigateur.

Voir plus de détails

Voir graphiques

Suis-je unique? (Détails)



Am I Unique?

Accueil

Mon empreinte

Ma frise chronologique
Nouveau

Statistiques globales

FAQ

Politique de confidentialité

Outils pour limiter le traçage sur Internet

Liens MAJ

À propos

Voir sur GitHub

Vue d'ensemble Détails Graphiques

Mon empreinte <https://amiunique.org/>

Attribut	Ratio de similarité	Valeur
En-tête "User agent"	<0.1%	"Mozilla/5.0 (X11; Linux x86_64; rv:62.0) Gecko/20100101 Firefox/62.0"
En-tête "Accept"	54.29%	"text/html,application/xhtml+xml,application/xml;q=0.9;*/q=0.8"
En-tête "Content encoding"	50.85%	"gzip, deflate, br"
En-tête "Content language"	<0.1%	"fr-CA,fr;q=0.8,fr-FR;q=0.6,en-US;q=0.4,en;q=0.2"
Liste des plugins	<0.1%	"Plugin 0: Shockwave Flash; Shockwave Flash 31.0 r0; libflashplayer.so."
Détail des plugins		
	29.41 %	Shockwave Flash
Plateforme	10.51%	"Linux x86_64"
Utilisation des cookies	80.16%	"yes"
Utilisation du Do Not Track	32.02%	"yes"
Fuseau horaire	5.19%	"240"
Résolution de l'écran	3.54%	"1920x1200x24"
Utilisation du stockage local	77.61%	"yes"
Utilisation du stockage de session	77.61%	"yes"
Canvas	<0.1%	Cwm fjordbank glyphs vext quiz, ☺ Cwm fjordbank glyphs vext quiz, ☺
WebGL Vendor		"NVIDIA Corporation"
WebGL Renderer		"GeForce 9800 GT/PCIe/SSE2"
Liste des polices	13.44%	"Flash detected but not activated (click-to-play)"
Résolution d'écran	13.44%	"Flash detected but not activated (click-to-play)"
Langage	13.44%	"Flash detected but not activated (click-to-play)"
Plateforme	13.44%	"Flash detected but not activated (click-to-play)"
Utilisation d'AdBlock	33.87%	"yes"



Suis-je unique? (Données recueillies)



<https://amiunique.org/>

- l'agent utilisateur
- l'entête Accept
- l'entête Connection
- l'entête Encoding
- l'entête Language
- la liste des greffons (plugins)
- la plateforme
- la préférence des témoins (cookies) : allouée ou non
- la préférence du pistage (Track) : oui, non, non communiqué

- le fuseau horaire
- la résolution de l'écran et sa profondeur de couleur
- l'utilisation du cache locale
- l'utilisation du cache de session
- le rendu d'une image HTML Canvas
- le rendu d'une image WebGL
- la présence de Adblock
- la liste des polices

Être comme tout le monde...



- Pour être anonyme...
- Mais notre empreinte nous rend presque à coup sûr unique :-)
- Berner l'acquisition de notre empreinte
 - En ajoutant quelques extensions à Firefox
 - En modifiant certains paramètres de la configuration par défaut de Firefox

5 extensions pour Firefox



Désactivation de Google Analytics

Indique au fichier Javascript Google Analytics (ga.js) de ne pas envoyer d'informations à Google Analytics.



HTTPS partout

Chiffrez le Web ! Utilisez automatiquement la sécurité HTTPS avec de nombreux sites.



Privacy Badger

Privacy Badger vous protège des traceurs lorsque vous surfez sur le web !



Suppression automatique des témoins

Contrôlez vos témoins ! Supprimez automatiquement les témoins non utilisés de vos onglets ferm...



uBlock Origin

Un bloqueur de nuisances efficace, qui ménagera votre processeur et votre mémoire vive.

- Des extensions de qualité et de confiance
 - ajoutent des fonctionnalités
 - ou simplifient le paramétrage

Plus de contrôle moins d'indiscrétion



- Ces 5 extensions

Désactivation de Google Analytics

HTTPS partout (HTTPS Everywhere)

Privacy Badger

Suppression automatique des témoins (cookie auto-delete)

uBlockOrigin

- sont complémentaires
- mais elles peuvent aussi se recouper
- elles améliorent votre vie privée

Désactivation de Google Analytics



- on la trouve évidemment chez Google puisqu'elle en désactive une fonction!
- <https://tools.google.com/dlpage/gaoptout?hl=FR>



Select a language ▼

Module complémentaire de navigateur pour la désactivation de Google Analytics

Nous souhaitons donner aux visiteurs d'un site Web la possibilité de bloquer l'utilisation de leurs données par les fichiers JavaScript de Google Analytics (ga.js, analytics.js, dc.js). C'est dans cette optique que nous avons développé le module pour la désactivation de Google Analytics.

Si vous ne souhaitez pas transmettre d'informations à Google Analytics, téléchargez et installez ce module dans votre navigateur Web. Il est compatible avec Chrome, Internet Explorer 11, Safari, Firefox et Opera. Pour fonctionner, ce module complémentaire doit pouvoir se charger et s'exécuter correctement dans votre navigateur. Pour Internet Explorer, vous devez activer les cookies tiers. Pour en savoir plus sur la désactivation de Google Analytics et l'installation du module complémentaire dans votre navigateur, veuillez [cliquer ici](#).

Télécharger le module
complémentaire de
navigateur pour la
désactivation de Google
Analytics

Ce module est disponible pour
Microsoft Internet Explorer 11,
Google Chrome, Mozilla Firefox,
Apple Safari et Opera.

[En savoir plus sur la confidentialité dans Google Analytics »](#)

©2018 Google - [Règles de confidentialité](#) - [Aide](#)

HTTPS partout (HTTPS Everywhere)



HTTPS partout 2018.8.22

Par [EFF Technologists](#)



Chiffrez le Web ! Utilisez automatiquement la sécurité HTTPS avec de nombreux sites.

Beaucoup de sites web offrent une prise en charge limitée pour le chiffrement via HTTPS, mais la rendent difficile à utiliser. Par exemple, ils peuvent utiliser une adresse par défaut non chiffrée avec HTTPS, ou proposer sur des pages chiffrées uniquement des liens qui retournent sur le site non chiffré.

L'extension HTTPS Everywhere résout le problème en redirigeant toutes les requêtes de ces sites vers HTTPS.

Mises à jour automatiques

Par défaut Activées Désactivées

Dernière mise à jour

1 septembre 2018

Page d'accueil

<https://www.eff.org/https-everywhere>

Appréciation

★★★★☆ 351 appréciations

Paramètres généraux

Paramètres avancés

Update Channels

Afficher le compteur

Ensembles de règles de mise à jour automatique

Privacy Badger



Musée de la civilisation - Québec : MCQ.org - Mozilla Firefox

Musée de la civilisation - x

Rechercher

Météo Québec OpenStreetMap RTC OpenTopoMap ArchW

MUSÉE DE LA CIVILISATION

LA ON

BILLETS E

POSITIONS ▾ ACTIVITÉS MLAB COLLECTIONS FO

APPLICATION MOBILE OFFICIELLE

—

MON MCQ

—

PRODUIT NUMÉRIQUE - MUSÉE DE LA CIVILISATION

POSITIONS EN COURS

Privacy Badger
version 2018.8.22

Privacy Badger a détecté 6 **traceurs** potentiels sur cette page. Ces curseurs vous permettent de modifier la façon dont ils sont gérés. Vous ne devriez pas avoir besoin de les modifier à moins d'un site non fonctionnel.

🚫 🍪 ✅

googleads.g.doubleclick.net	🚫
connect.facebook.net	🟡
fonts.googleapis.com	🟡
www.google-analytics.com	🚫
www.googletagmanager.com	🚫
fonts.gstatic.com	🟡
Les domaines ci-dessous ne semblent pas vous tracer.	
acuityplatform.com	✅
cloud.typography.com	✅

Désactiver Privacy Badger pour ce site

Signaler un site non fonctionnel

Faire un don à l'EFF

Suppression automatique des témoins (cookie auto-delete)



Musée de la civilisation - Québec : MCQ.org - Mozilla Firefox

Musée de la civilisation - x +

Rechercher

Météo Québec OpenStre

Le nettoyage automatique est activé

Les notifications sont désactivées

Nettoyer

Paramètres

mcq.org

mcq.org + Liste grise + Liste blanche

*.mcq.org + Liste grise + Liste blanche

Aucune règle ne correspond à ce domaine

12/09/2018 à 23:12:32 - 1 témoins ont été supprimés pour : (Private)

12/09/2018 à 22:50:02 - 10 témoins ont été supprimés pour : , worldweather.wmo.int

12/09/2018 à 22:42:03 - 1 témoins ont été supprimés pour : (Private)

uBlockOrigin



Rechercher

efox Send

MUSÉE DE L'AMÉRIQUE FRANCOPHONE

uBlock Origin 1.16.20

Cliquez pour désactiver uBlocko pour ce site

Ctrl+Clic pour désactiver uBlocko uniquement pour cette page

421 756, soit 8%

Domaines connectés

5 sur un total de 9

Rechercher

efox Send

MUSÉE DE L'AMÉRIQUE FRANCOPHONE

uBlock Origin 1.16.20

Requêtes bloquées

sur cette page :
8, soit 10%

depuis toujours :
421 756, soit 8%

Domaines connectés

5 sur un total de 9

2 extensions à éviter

<https://linuxfr.org/news/protoger-sa-vie-privee-sur-le-web-exemple-avec-firefox>



Le site web LinuxFR.org a publié *Protéger sa vie privée sur le Web, exemple avec Firefox* le 26 février 2018;

le collectif qui a rédigé l'article ne recommande pas les deux extensions suivantes :

- le bloqueur de requêtes Ghostery
 - n'est pas un logiciel libre
 - il y aurait remontée d'informations depuis le fureteur
 - le modèle économique de l'éditeur peut être sujet à quelques questionnements
- Disconnect bloque principalement les requêtes vers Google, Facebook et Twitter
 - externalise le traitement de votre navigation

Configuration générale de Firefox

témoins et pistage



- Menu de Firefox ☰ → Préférences → Vie privée et sécurité (ou menu classique ponctuel avec la touche Alt)
 - Désactiver les témoins (cookies) tiers
 - Cocher Accepter les cookies et les données de sites (recommandé)*
 - Les conserver jusqu'à leur expiration
 - Accepter les cookies tiers et les données de sites tiers *jamais*
 - Protection contre le pistage
 - Cocher Toujours* dans Utiliser la protection contre le pistage pour bloquer les traqueurs connus.

Configuration générale de Firefox

moteur de recherche



- Menu de Firefox ☰ → Recherche
(ou cliquer sur la loupe 🔍 dans la barre de recherche)
 - Décocher les suggestions de recherche
 - Changer le moteur de recherche par défaut
On peut remplacer Google par un moteur qui respecte notre vie privée
 - Qwant <https://www.qwant.com>
- DuckDuckGo <https://duckduckgo.com>



Configuration générale de Firefox

polices de Google



- Menu de Firefox ☰ → Préférences → Vie privée et sécurité → Cookies et données de sites → Exceptions

(ou menu classique ponctuel avec la touche Alt)

– Bloquez les domaines suivants :

- googleapis.com
- gstatic.com
- apis.google.com

ATTENTION : Cette méthode est radicale et elle peut vous empêcher d'utiliser des services de Google comme Maps ou des sites tiers qui utilisent les API de Google (comme le site du RTC)

Les témoins (cookies) Flash



- Manipulation sous Linux seulement...
- Ouvrir un terminal et taper (ou copier/coller) les 3 commandes suivantes :

```
rm -rf ~/.adobe ~/.macromedia
```

```
ln -s /dev/null ~/.adobe
```

```
ln -s /dev/null ~/.macromedia
```

DoH ou DNS over HTTPS

Firefox version 62 et + seulement



voir <https://blog.nightly.mozilla.org/2018/06/01/improving-dns-privacy-in-firefox/>

- Tapez `about:config` dans la barre d'adresse de Firefox 62+ (éditeur de configuration avancée)
- Tapez (pour rechercher) `network.trr` (qui signifie Trusted Recursive Resolver)
- Changez la valeur de `network.trr.mode` à 2 pour activer le DoH
- Renseignez la variable `network.trr.uri` de l'adresse du serveur DoH que vous utiliserez. Celle (suggérée) de Cloudflare est <https://mozilla.cloudflare-dns.com/dns-query>

Configuration fine de Firefox

about:config (dans la barre d'adresse)



- Suppression du référent en changeant la valeur de 4 variables :
 - `network.http.sendRefererHeader` → 1
 - `network.http.referer.XOriginPolicy` → 1
 - `network.http.referer.spoofSource` → true
 - `network.http.referer.trimmingPolicy` → 2

Configuration fine de Firefox

about:config (dans la barre d'adresse)



- Désactiver la connexion silencieuse lors du survol d'un lien
 - `network.http.speculative-parallel-limit` → 1
- Désactiver le préchargement des liens
 - `network.prefetch-next` → false
- Désactiver les suggestions de recherches
 - `browser.search.suggest.enabled` → false
- Ne pas divulguer où vous collez...
 - `dom.event.clipboardevents.enabled` → false

Fausse protections



- L'option Firefox « Ne pas me pister »
 - une demande aux sites de ne pas être pisté
 - la traçabilité est au bon vouloir du site
- Le mode de navigation privée
 - n'empêche pas le pistage
 - pas de trace pour l'utilisateur postérieur
 - n'empêche pas le partage d'informations avec les autres sites des autres onglets qui seraient accédés dans la même session – les témoins (cookies) restent communs

Conclusion



- D'autres actions sont aussi possibles
 - D'abord notre manière de naviguer dans l'Internet
 - Les sites que nous fréquentons!
- Firefox est un fureteur qui est très paramétrable
 - Ajoutez seulement des extensions de qualité et de confiance
 - about:config → bien se renseigner chez mozilla.org
http://kb.mozillazine.org/Editing_configuration

Références



- Protéger sa vie privée sur le Web, exemple avec Firefox, LinuxFR.org, collectif, 2018-02-26, <https://linuxfr.org/news/protoger-sa-vie-privee-sur-le-web-exemple-avec-firefox>
- The Complete Firefox Privacy and Security Guide, Douglas Crawford, 2018-01-18, <https://www.bestvpn.com/guides/firefox-privacy-security-guide/>
- Improving DNS Privacy in Firefox, Patrick McManus, 2018-06-01, <https://blog.nightly.mozilla.org/2018/06/01/improving-dns-privacy-in-firefox/>
- Firefox Nightly Secure DNS Experimental Results, Patrick McManus, 2018-08-28, <https://blog.nightly.mozilla.org/2018/08/28/firefox-nightly-secure-dns-experimental-results>
- Better security, privacy and anonymity in Firefox, 2016-07-17, <https://b.agilob.net/better-security-privacy-and-anonymity-in-firefox>
- <https://tools.google.com/dlpage/gaoptout?hl=FR> pour désactiver Google Analytics
- <https://amiunique.org/> Informations et test de l'empreinte du fureteur
- Cookieless Monster: Exploring the Ecosystem of Web-based Device Fingerprinting, 2013 http://cs.ucsb.edu/~vigna/publications/2013_SP_cookieless.pdf
- IceCat, le fureteur GNU basé sur Firefox <https://directory.fsf.org/wiki/IceCat>
- about:config → bien se renseigner chez mozilla.org http://kb.mozillazine.org/Editing_configuration