

100%
PRATIQUE

[PIRATAGE]
Spécial Débutants

[ANONYMAT]
Devenez invisible

[SMARTPHONE]
Prenez le contrôle !

3⁵⁰€
seulement

LE GUIDE DU **Pirate**

🦴 **Anonymat** 🦴 **Hacking** 🦴 **Multimédia**

0%
PUBLICITÉ

HACKING de A à Z

→ **DOSSIER**

**Crack
de MOTS
DE PASSE**

avec
John The Ripper

**FICHES &
ASTUCES**

EN - DE **3 MN**
CHRONO !

SPÉCIAL FILMS & SÉRIES

» Téléchargement
» Sous-titres
» Encodage





SOMMAIRE

EN PARTENARIAT
AVEC

LES CAHIERS DU HACKER
PIRATE
[INFORMATIQUE]

MULTIMÉDIA

12

M4NG : la trousse à outils de l'encodage

16

Tout savoir sur les «**BOOTLEGS**»

20

TVSHOWTIME : vos séries le jour de leur sortie !

23

LE FORMAT MKV : lire et modifier

26

TORRENT À DISTANCE : toutes les solutions

28

Les sous-titres faciles avec **VLSUB**

MOTS DE PASSE

34

JOHN THE RIPPER : le logiciel ultime pour cracker

42

PASSWORD SAFE : un coffre fort à mot de passe

46

CRACKEZ le mot de passe de **WINDOWS** !

CRYPTAGE

49

AXCRYPT : un chiffrement simple et rapide

52

Cryptez le contenu de votre cloud avec **CRYPTSYNC**

55

TrueCrypt est mort, vive **VERACRYPT** !

ANONYMAT

62

FREEDOM IP : un VPN communautaire français

66

Des proxy à la demande avec **FOXYPROXY**

68

STREALTHY : soyez furtif sur le Net

71

Un **TOR** encore plus costaud !

74

SOFTETHER : le VPN du soleil levant

► MOBILE

81

«**ROOT**» Android, quels sont les avantages ?

84

WIFIKILL : soyez le maître de votre réseau

86

DSPLOIT :
testez et sécurisez
votre réseau local

88

Un mot de passe principale
avec **DASHLANE**

90

VPN1CLICK : chiffrez votre
connexion sur mobile

92

Cryptez vos conversations
avec **DISCRETIO**

94

GREENIFY : faites hiberner
vos applications

► MATOS

98

**NOTRE SÉLECTION
DE MATÉRIELS**

LE GUIDE DU Pirate

N°1 – Août/Oct. 2014

Une publication du groupe ID Presse.
27, bd Charles Moretti - 13014 Marseille
E-mail : redaction@idpresse.com

Directeur de la publication :

David Côme

Flam : Benoît Bailleul

Mala : Yann Peyrot

Crag : Sergueï Afanasiuk

Johann Landore : Karima Allali

Imprimé en France par

/ Printed in France by :

Aubin Imprimeur
Chemin des Deux Croix
CS 70005
86240 Ligugé

Distribution : MLP

Dépôt légal : à parution

Commission paritaire : en cours

ISSN : en cours

«Pirate» est édité par SARL ID Presse,
RCS : Marseille 491 497 665
Capital social : 2000,00 €
Parution : 4 numéros par an.

La reproduction, même partielle, des articles et illustrations parues dans «Pirate Informatique» est interdite. Copyrights et tous droits réservés ID Presse. La rédaction n'est pas responsable des textes et photos communiqués. Sauf accord particulier, les manuscrits, photos et dessins adressés à la rédaction ne sont ni rendus ni renvoyés. Les indications de prix et d'adresses figurant dans les pages rédactionnelles sont données à titre d'information, sans aucun but publicitaire.



QUAND UN SYSTÈME DE SÉCURITÉ SE TRANSFORME EN TROJAN

CONNAISSEZ-VOUS COMPUTRACE ? CE SYSTÈME DE SÉCURITÉ EST INTÉGRÉ DANS LE BIOS DE CENTAINES DE MILLIERS D'ORDINATEURS. LE PROBLÈME C'EST QUE CE COMPUTRACE EST PRESQUE INVISIBLE ET PEUT ÊTRE UTILISÉ PAR DES PERSONNES MALVEILLANTES POUR VOUS ESPIONNER OU PRENDRE LE CONTRÔLE DE VOTRE ORDINATEUR. COMMENT SAVOIR SI VOUS ÊTES CONCERNÉ ?

Absolute
COMPUTRACE

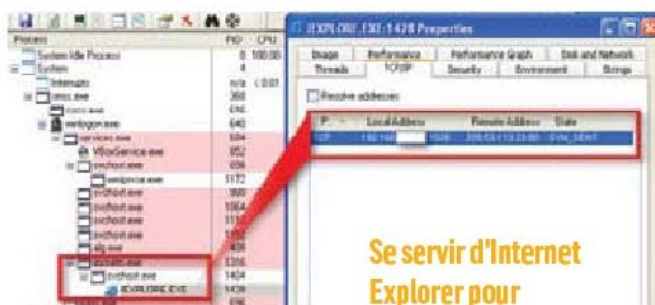


A la base Computrace part d'un bon sentiment. Il s'agit d'un système de sécurité intégré au BIOS permettant de géolocaliser un PC volé, de prendre le contrôle d'une machine pour faire des

mise à jour ou de lancer des diagnostics à distance. Les plus grandes marques font confiance à ce programme (Asus, Dell, HP, Lenovo, Toshiba, etc.) alors où se situe le problème ? Tout a commencé lorsque la femme d'un employé de Kaspersky a

COMMENT ÇA MARCHE ?

Lors du démarrage du PC, Computrace va s'octroyer un accès illimité à tous les fichiers du PC ainsi qu'à la base de registre pour installer ses DLL et son agent de contrôle. Computrace aura alors toute la liberté d'utiliser votre connexion pour envoyer et recevoir des données (via Internet Explorer). Le processus est transparent (à part quelques ralentissements) et permet au final pour un tiers de prendre le contrôle de votre machine. Le plus retors c'est que même si vous supprimez les éléments de votre disque dur ou que vous changez ce dernier, le BIOS vous les remettra au prochain reboot...



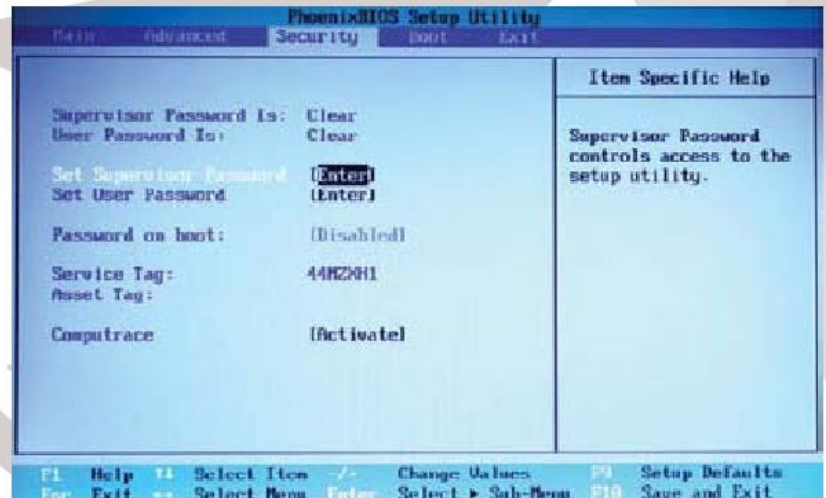
Se servir d'Internet Explorer pour communiquer sur Internet... vraiment une idée saugrenue !



rencontré des ralentissements inquiétants sur son PC. Ni une ni deux, son mari a donc analysé la machine pour se rendre compte que les processus incriminés appartenaient au logiciel Absolute Computrace. Certains antivirus détectaient un malware tandis que d'autres ne détectaient rien. En effet, Computrace agit comme un trojan mais figure sur les listes blanches d'antivirus car il s'agit d'un logiciel «respectable».

OÙ EST LE PROBLÈME ALORS ?

Le problème c'est que les gens qui ont acheté des PC avec cette technologie embarquée ne sont pas au courant que le logiciel fait tourner des processus sur leur machine. Kaspersky a contacté la société Absolute pour leur fournir des numéros de série de carte mère contenant Computrace dans le but de vérifier que les informations arrivaient «à bon port». Or Absolute n'a aucune trace de certains appareils dans sa base de données. Soit Absolute ment, soit Computrace a été utilisé de manière frauduleuse par des pirates...ou des services secrets. Le problème est très grave puisque 2 millions de postes seraient «infectés» par Computrace. On peut aussi se poser cette question toute simple : vous achetez un ordinateur avec un service de sécurité intégré. OK. Mais pourquoi la marque, le fabricant et le détaillant ne vous mettent-



ils pas au courant ? Pourquoi Computrace est-il activé d'office et est même masqué dans certains BIOS ? En d'autres termes Computrace est-il utilisé par des hackers ou des organismes gouvernementaux à l'insu de l'utilisateur ? Absolute est-il complice ?

Les BIOS affichent souvent la présence de Computrace dans leurs entrailles, mais parfois non. Pourquoi ?

ÊTES-VOUS INFECTÉ ?

Pour savoir si vous êtes concerné par la présence de Computrace, il existe un logiciel qui pourra vous le dire en deux clic : Phrozen Computrace Dectector 1.0. Il suffit de le lancer pour avoir une réponse en 5 secondes. Si jamais vous faites partie des malheureux, nous verrons dans le numéro 23 de Pirate Informatique comment changer de BIOS et désinfecter votre machine...

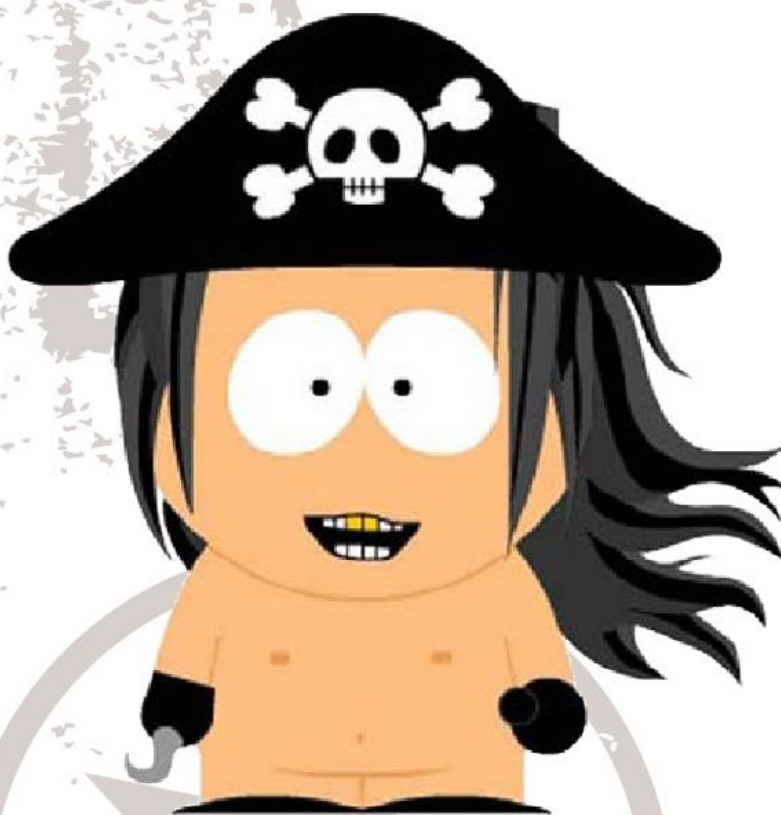
Lien : <http://goo.gl/xvbgau>





«RIEN À CACHER ?» BIEN SÛR QUE SI !

C'EST UNE EXPRESSION QUE L'ON ENTEND SOUVENT LORSQUE L'ON PARLE DE VIE PRIVÉE. LES SERVICES SECRETS SURVEILLENT VOS E-MAILS ? LES GROSSES SOCIÉTÉS D'INTERNET SONT COMPLICES DE CES AGISSEMENTS ? QU'À CELA NE TIENNE, CAR VOUS N'EST NI PÉDOPHILE NI TERRORISTE ET VOUS N'AVEZ «RIEN À CACHER». DANS LE CAS CONTRAIRE, VOUS SERIEZ COUPABLE N'EST-CE PAS ? CE RAISONNEMENT EST NON SEULEMENT FAUX, MAIS DANGEREUX. EXPLICATIONS...



Accepteriez-vous qu'on lise votre courrier, vos SMS ou vos conversations téléphoniques ? Accepteriez-vous qu'une caméra enregistre vos faits et gestes chez vous ? Bien sûr que non. Pourtant certains politiciens et autres PDG de grosses compagnies

vous assurent que «*si vous n'avez rien à cacher, vous n'avez rien à craindre*». Il faut en effet attraper les criminels, mais à quel prix ? Vous ne faites sans doute rien d'illégal, mais vous aimeriez quand même avoir le droit à une vie privée. Ne tirez-vous pas les rideaux le soir lorsque vous voulez être tranquille à



LA VIE PRIVÉE NE SERT PAS FORCEMENT À
CACHER DES COMPORTEMENTS ILLÉGAUX

la maison ? Racontez-vous les difficultés rencontrées dans votre vie à n'importe qui ?

QUAND ON CHERCHE, ON TROUVE !

Ne pensez pas « je suis un citoyen lambda mes informations n'intéressent personne » ou « je suis intégré dans la société, je paye mes infos et j'ai un casier vierge, la NSA peut bien perdre son temps à regarder mes e-mails ». Ceux qui utilisent cet argument du « je n'ai rien à cacher » partent du principe que la vie privée sert forcément à cacher des comportements illégaux ou répréhensibles. Peut-être ne voudriez-vous pas qu'en lisant vos e-mails ou en analysant vos recherches que l'on sache que vous avez contracté une MST en 2002, bien avant de rencontrer votre femme ou que l'on sache que votre cousin éloigné, qui porte le même nom que vous, a été condamné pour trafic de drogue ou violence conjugale. Avec l'abandon du projet des récépissés remis après un contrôle de police nous nous sommes rendu compte que même les policiers refusaient d'être « fliqués ».

LE CROISEMENT DE PLUSIEURS SOURCES

Il est important de comprendre que la vie privée est constituée de plusieurs éléments connectés entre eux. Le programme PRISM de la NSA agrège les informations issues des sites de Microsoft (Hotmail, OneDrive),

"Si vous faites quelque chose et que vous voulez que personne ne le sache, peut-être devriez-vous déjà commencer par ne pas le faire !"

- Eric Schmidt, PDG de Google



Apple, Google (YouTube, Google+, Gmail), Facebook, Dropbox, etc. Si vous achetez une cocotte minute sur Le Bon Coin et un sac d'engrais sur Amazon dans le même mois, vous pouvez très bien être suspecté de vouloir faire une bombe alors que vous voulez juste faire des soupes avec les légumes de votre jardin. Quand on cherche, on trouve. De même si vous faites une recherche sur le SIDA et que vous vous renseignez sur la trithérapie, on pourrait supposer que vous êtes malade. Vous auriez peut-être voulu garder ça secret d'autant que certains pays interdisent les visas aux personnes séropositives... Les informations sur vous qui circulent en ligne sont bien plus importantes qu'il y a 5 ou 10 ans. On a jamais su autant de choses sur les citoyens. Même la Stasi (police politique de l'Allemagne de l'Est) fait « petit joueur » à côté de la colossale collecte



d'information de la NSA (7 To par seconde). Et ce sont des informations que l'on donne la plupart du temps sans que les services secrets fassent d'efforts particuliers.

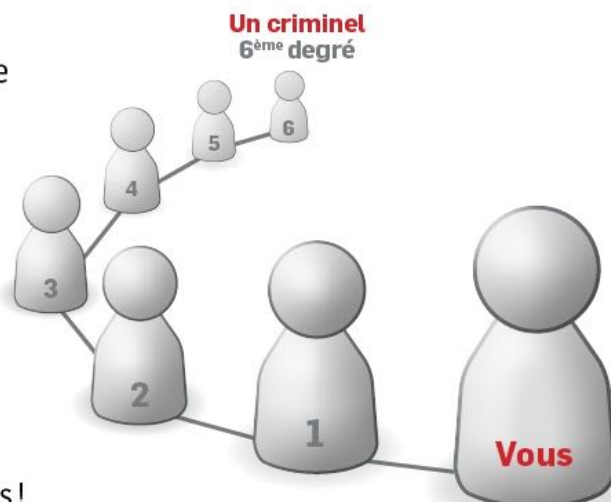
LES INFORMATIONS COLLECTÉES SONT-ELLES EN SÉCURITÉ ?

On peut se poser aussi la question de la sécurité des

informations qui transitent sur vous. Que la NSA sache que vous aimez le porno hardcore hongrois est déjà assez gênant, mais si cette information venait à se répandre sur un site public, votre vie professionnelle serait terminée. Toujours rien à cacher ? Peut-être avez-vous une clause de confidentialité dans votre contrat de travail ? Aimeriez-vous être licencié pour avoir, malgré vous, fourni des informations professionnelles ? Que vous soyez journaliste, employé dans une centrale nucléaire ou ingénieur chez Peugeot, cela peut arriver. Nicolas Sarkozy a été mis sur écoute et ses conversations avec son avocat ont été rendues publiques. Pourquoi pas vous ? Quand il s'agit de surveillance généralisée, on ne fait pas le tri.

6 DEGRÉS DE SÉPARATION ENTRE BARACK OBAMA...ET OUSSAMA BEN LADEN

N'oublions pas que 6 degrés de séparation entre deux individus sur la planète. Entre vous et un fauconnier kazakh ou un paysan péruvien, il n'y a que 5 maillons (le fauconnier connaît une personne, qui connaît une personne [etc.], qui vous connaît). Sur les réseaux sociaux, il n'y a que 4 degrés de séparation. Ce qui veut dire que vous êtes forcément ami, avec un ami qui connaît un terroriste ou un pédophile. Combien de temps avant que l'on vous pose des questions sur Jean-Claude, cette vague connaissance, qui vole des mobylettes ? Et n'y a-t-il jamais d'erreur dans la collecte des infos ? Des homonymes, des fautes de frappe, des erreurs de mise à jour ? Impossible de le savoir puisque vous n'avez pas accès à ces informations !



CHEZ VOTRE MARCHAND
DE JOURNAUX

seulement
3,00 €

SAMSUNG » NEXUS » HTC » LG » SONY » WIKO

Android MT

Mobiles & Tablettes

AVRIL - MAI 2014

+ DE 50 FICHES PRATIQUES & ASTUCES

LE GUIDE ANDROID 100% GRATUIT

+ DOSSIER SÉCURITÉ

- » Solutions antivol
- » Verrouillage à distance
- » Retrouver son smartphone



MINI PRIX
3,00 €
seulement

LE 1^{ER} MAGAZINE
100% ANDROID ET 100% PRATIQUE

TÉLÉCHARGER // STREAMING MAGAZINE INTERDIT



**DOWN
LOAD** N°8
TÉLÉCHARGEMENT & MULTIMÉDIA

**LES NOUVEAUX SERVICES
PIRATES**

TOUTBOX :
LA NOUVELLE
BOMBE POUR TOUT
PARTAGER

ACE PLAYER :
FICHIERS TORRENTS
EN STREAM DIRECT
SANS TÉLÉCHARGEMENT !

**FICHES
PRATIQUES :**
LES MEILLEURS SERVICES
ET LOGICIELS EXPLIQUÉS

GUIDE MOBILE
**APPSTORES
ALTERNATIFS**
Où télécharger des
APPLIS INTERDITES,
GRATUITES ou SEXY ?

**TV SHOW
TIME**
Toutes les SÉRIES
en ILLIMITÉ

+ DES DIZAINES DE TUTOS !

SAVEDO : Téléchargez le stream
DIRECT TORRENT : Seedbox gratuite !
YOUTUBE : Postez comme un pro

DEEZER : Le retour du gratuit
IPMAGNET : Vérifiez votre anonymat
MUSICPLAYR : Playlists inédites !

+ CD OFFERT !

**DOWN
LOAD** N°8
TÉLÉCHARGEMENT & MULTIMÉDIA

**341
LOGICIELS
& SERVICES**

DOWNLOAD
STREAMING
MOBILES
TROUSSE À OUTILS
ANONYMAT

**+100
APPLIS
MOBILES
GRATUITES !**

**13 TUTORIELS
EN VIDÉO !**
**2 MAGAZINES
COMPLETS OFFERTS**
**13 JEUX
GRATUITS**

CD OFFERT !

© 2014 - SUPPLÉMENT GRATUIT - CD POUR WINDOWS

CHEZ VOTRE MARCHAND DE JOURNAUX !

MULTIMEDIA

12

M4NG : la trousse à outils de l'encodage

16

Tout savoir sur les «**BOOTLEGS**»

20

TVSHOWTIME : vos séries le jour de leur sortie !

23

LE FORMAT MKV : lire et modifier

26

TORRENT À DISTANCE : toutes les solutions

28

Les sous-titres faciles avec **VLSUB**





INFOS [M4NG]

Où le trouver ? [www.m4ng.fr]

Difficulté :

DÉBUTANTS OU EXPERTS, **M4NG** LES MET TOUS D'ACCORD !

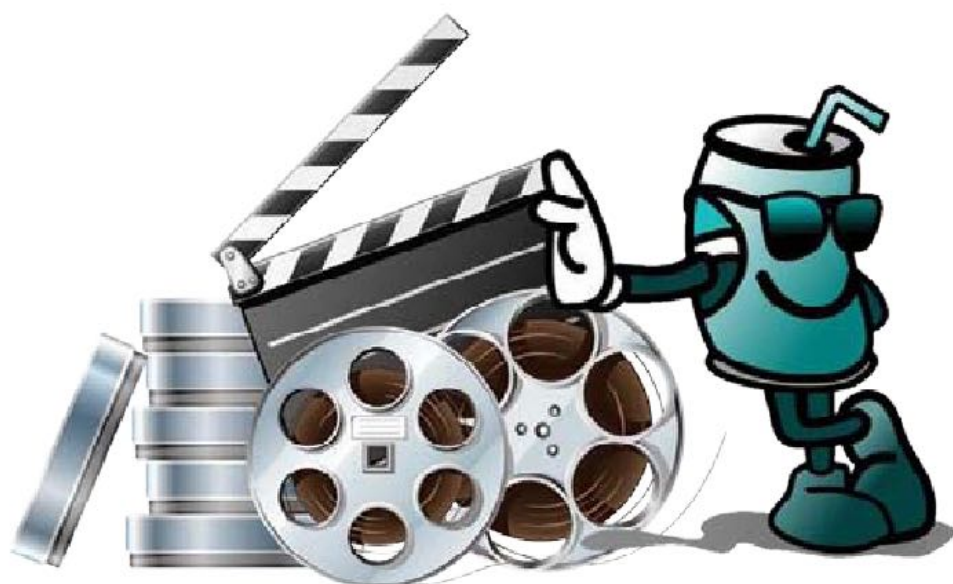
CONNU DEPUIS DES ANNÉES PAR LES AFICIONADOS DE L'ENCODAGE VIDÉO, M4NG EST UNE SOLUTION TOUT-EN-UN PERMETTANT DE FAIRE TOUT CE QUE VOUS POUVEZ IMAGINER AVEC UN PC ET DES FICHIERS VIDÉO. IL RÉUSSIT EN OUTRE LE TOUR DE FORCE D'ÊTRE ACCESSIBLE POUR LES DÉBUTANTS TOUT EN PROPOSANT DES RÉGLAGES TRÈS POUSSÉS POUR LES UTILISATEURS AVANCÉS.



Un outil très complet, en français et facile à prendre en main



Si vous voyez des côtés négatifs, faites-nous signe...



Medi4 next gen (abrégié en m4ng) est un logiciel permettant de faire énormément de manipulations avec vos précieuses vidéos. Vous avez un DVD ou un Blu-ray plein d'épisodes de votre série préférée et vous voudriez les lire sur votre iPad, PC, PSP ou smartphone Android ? Cette vidéo téléchargée ne fonctionne pas sur votre machine de prédilection ? Changer l'encodage du son uniquement

ou fusionner deux vidéos en une seule ? Pour toutes ces tâches, m4ng s'en sortira sans problème. Il est aussi possible de couper, coller, isoler le son, exécuter différents projets à la suite (batch), recréer les chapitres d'un DVD ou d'un Blu-ray, si vous avez un graveur de ce type. Un module permet même de couper les publicités issues d'un flux TNT ou satellite et les amoureux de sous-titres pourront éditer leur fichier SRT ou SUB avec SubsWay.



MULTIMÉDIA

Encodage Vidéo

DEUX MODES POUR TOUCHER LE PLUS GRAND NOMBRE D'UTILISATEURS

Le plus important, c'est que vous n'avez pas à être un expert en codecs ou jargon technique puisque le mode Débutant propose une interface claire sans réglages fastidieux. Vous pointez vers le fichier ou le disque, vous choisissez votre format de sortie (représenté par des icônes très claires) et c'est tout ! Le mode Expert propose

lui de choisir vos codecs audio et vidéo, la taille maximale de votre fichier, de régler le bitrate, d'ajouter des sous-titres, de prévisualiser ou de paramétrer un profil que vous utiliserez à chaque fois.



ENCODAGE, ASSEMBLAGE, SOUS-TITRES, RIP DVD/BLU-RAY, SÉRIES TV : M4NG EST UN VÉRITABLE COUTEAU SUISSE...

LE MODE DÉBUTANT

PRATIQUE



01 > Votre vidéo ne fonctionne pas avec votre appareil préféré ? Déposez cette dernière ici. S'il s'agit d'une vidéo sur DVD ou Blu-ray, cliquez sur le bouton du dessous. Le dernier bouton permet d'isoler des épisodes.



02 > Choisissez ici l'appareil sur lequel vous voulez faire fonctionner votre vidéo : home cinéma, iPad, Android, PSP, PC, etc.

03 > Choisissez la qualité et lancez la conversion !



LE MODE EXPERT

PRATIQUE



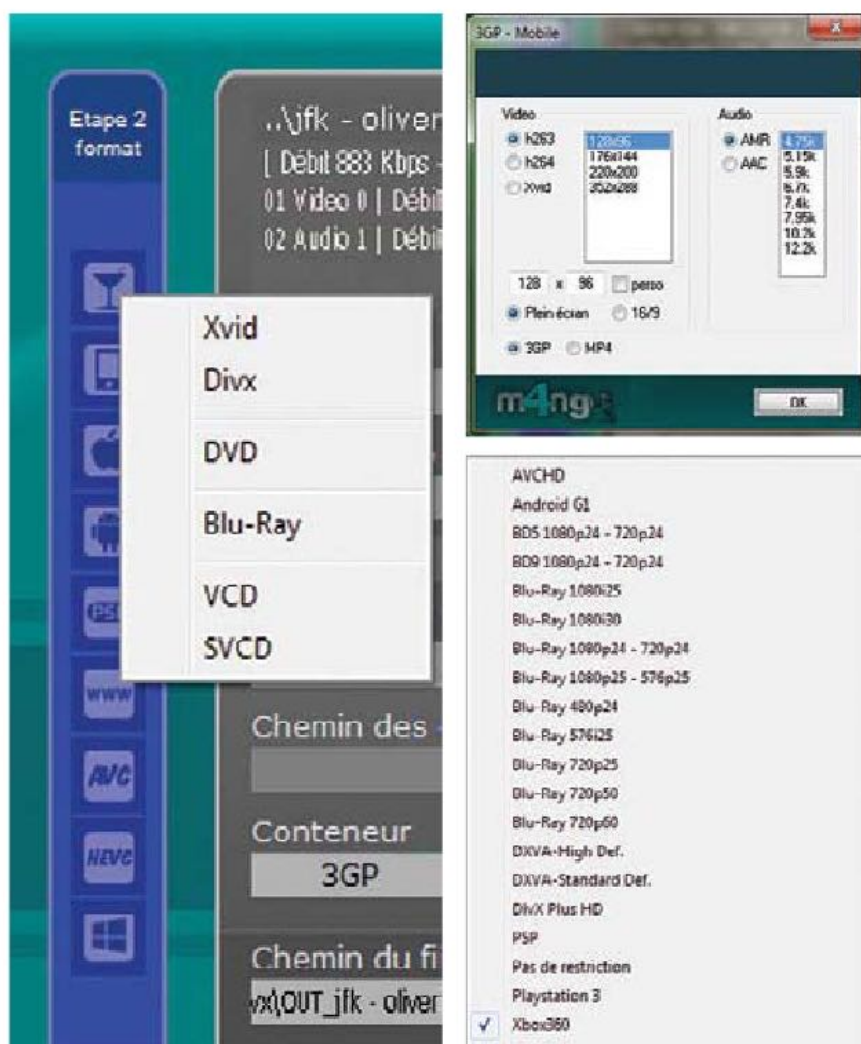
01 > VOTRE FICHIER

Comme pour le mode **Débutant**, il faudra pointer vers le fichier que vous voulez encoder ou vers votre lecteur de DVD/Blu-ray (vous pouvez aussi partir d'un fichier rippé IFO depuis ce menu). Notez que pour avoir accès aux outils de découpe, fusion ou mux/demux (séparation ou ajout de pistes audio), il faudra cliquer sur l'engrenage juste à côté de **Expert**.



02 > LE FORMAT DE SORTIE

Choisissez ensuite le format de sortie. Il suffit de cliquer sur l'icône correspondant à l'appareil sur lequel vous voulez lire votre vidéo. En fonction de votre choix, le logiciel vous donnera plusieurs choix de codec, de format, de résolution, etc. Chaque appareil dispose de ses propres propriétés.



UN MODE «AUTONOME» ?

m4ng est maintenant doté d'un mode **Autonome** lui permettant ainsi de fonctionner sans aucune installation de logiciel tiers et/ou codec externe. Si vous n'êtes pas sûr des versions de vos codecs ou si vous souhaitez encoder facilement une vidéo, c'est le mode le plus sûr.

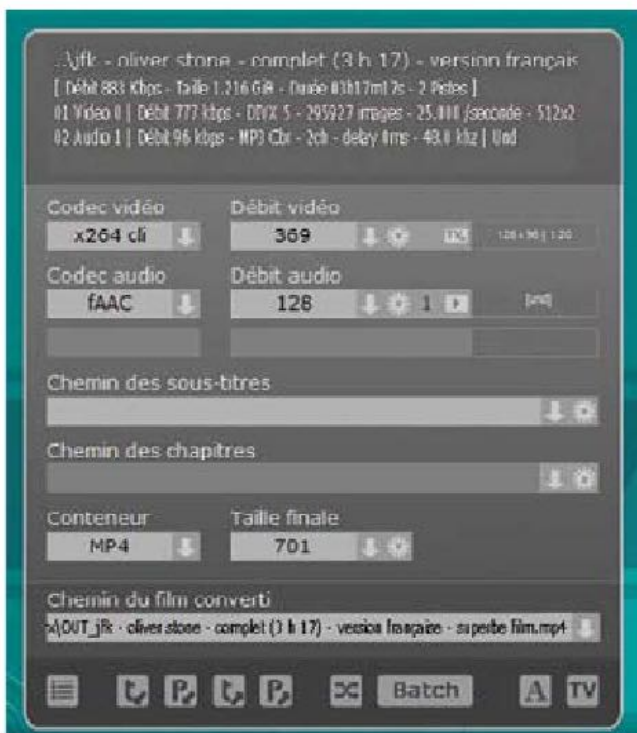


MULTIMÉDIA

Encodage Vidéo

03 > LES RÉGLAGES

Dans la fenêtre suivante, vous pouvez encore affiner vos réglages: le choix d'un codec, du bitrate, l'ajout de sous-titres (Le module **SubsWay** est accessible depuis le petit engrenage), la taille finale du fichier et tout ce qui concerne le type de conteneur (chapitrage MP4 ou MKV), si ce paramètre peut être appliqué.



04 > L'ENCODAGE

À la fin, il faudra choisir la qualité (encodage en1 ou 2passes) et éventuellement le ré-encodage de la piste audio ou vidéo uniquement (si votre film d'origine fonctionne, mais sans le son, pas besoin de ré-encoder la vidéo par exemple). **Multiplexage** permet de réunir différentes composantes de votre vidéo. Faites **Lancer la conversion** et ne fermer aucune des fenêtres qui vont s'afficher avant la fin du processus.



LES MODULES COMPLÉMENTAIRES

M4NG est plus qu'un logiciel. Il s'agit aussi d'une collection de modules permettant de réaliser différentes tâches sur des fichiers vidéo.

• LE PACK DE CODECS M4NG

Il s'agit d'un pack qui intègre tous les codecs vidéo et audio les plus courants. Aucun de ces derniers n'a été trafiqué et tous sont garantis pour une utilisation optimale de m4ng. Foncez l'installer !

• VIDEO ANALYSER

Il s'agit d'une espèce de widget qui permet d'avoir accès instantanément à plusieurs paramètres d'une vidéo : codecs utilisés, longueur, bitrate, etc. Il ne prend pas beaucoup de place et reste très utile.

• VIDEO ENHANCER

Video Enhancer est un module permettant d'améliorer le réencodage d'une vidéo grâce aux filtres AVIsynth. Vous pouvez bien sûr l'utiliser sans installer m4ng.



melodyne

INFOS [MIXMEISTER BPM ANALYZER] [<http://mixmeister-bpm-analyzer.softonic.fr>][MELODYNE EDITOR] Où le trouver ? [www.celemony.com/fr/trial]

Difficulté: ☠☠☠

TOUT SAVOIR SUR LES BOOTLEGS !

CONNAISSEZ-VOUS LES BOOTLEGS ? CES MORCEAUX DE MUSIQUE (APPELÉS AUSSI PARFOIS «MASHUPS») COMBINENT DEUX OU PLUSIEURS AUTRES MORCEAUX. EN CALANT LES TEMPOS, LES ARTISTES QUI RÉALISENT CE GENRE DE MIX ARRIVENT À FAIRE DE BELLES PROUESSES AU NIVEAU MUSICAL. DÉCOUVRENS ENSEMBLE CET UNIVERS ET COMMENT FAIRE SES PREMIERS PAS...

**MixMeister Analyzer**

Fait le travail qui lui est confié

Melodyne Editor

Cette version limitée dans le temps n'est pas limitée au niveau des fonctionnalités

**MixMeister Analyzer**

Ne sert qu'à connaître le BPM dans notre cas

Melodyne Editor

Une version limitée à 30 jours seulement

Le bootleg faisait uniquement référence aux enregistrements audio ou vidéo live de concerts, voire à des inédits «échappés» des studios. Mais depuis presque dix ans, le terme «bootleg» fait surtout référence à un autre type de création. Il s'agit d'un détournement et du remix de deux chansons en vue d'en faire une seule et même troisième. La recette est «simple».

Il suffit de prendre d'un côté la version «a cappella» d'un titre, la version instrumentale du second et de mixer savamment le tout sur ordinateur. Certains DJ arrivent à agrémenter leur création d'éléments issus de 4 ou 5 morceaux différents.

BÉZU VS LED ZEPPELIN ?

Cela peut paraître simple, mais mixer Joey Starr avec la musique de Star Wars, Bruce



Springsteen et Katy Perry ou Daft Punk avec les Beatles est un vrai tour de force... Une foule de bidouilleurs, à la fois mélomanes et versés dans l'informatique, s'y mettent au fond de leurs garages. Des sites comme www.bootlegsfr.com se sont même spécialisés dans l'indexation de sources et proposent une sélection de titres toutes les semaines. On voit même apparaître des concours et certains artistes connus comme Madonna ou Nine Inch Nails facilitent la tâche des «bootleggers» en fournissant les pistes nécessaires à la création de mix. Hier réservé aux professionnels (il y a plus de 10 ans, c'est MTV qui avait fait connaître le genre), ces créations connaissent une seconde jeunesse grâce à Internet. Les bidouilleurs de génie peuvent réaliser leurs propres créations avec peu de moyens, même si la technique demande persévérance et pas mal de pratique. Une excellente oreille musicale est bien sûr



requis... Comme aucun logiciel n'est capable de désolidariser les pistes, il va falloir trouver des «packs remix» sur Internet (appelés aussi «multitrack», «raw tracks» ou «studio tracks»). Google est votre ami !



MIXER DU DAFT PUNK AVEC LES BEATLES EST UN VRAI TOUR DE FORCE !



NOS LIENS

- **LES RADIOS SUR INTERNET :**
www.mixcloud.com/tag/bootleg-mash-up
www.themashupradio.com
- **LE SITE RÉFÉRENCE :** www.bootlegsfr.com
- **UN EXCELLENT DOCUMENTAIRE :** <http://goo.gl/Lml1b>
- **UN SUPER SITE AVEC DES PISTES MULTITRACK AU FORMAT YOUTUBE :**
www.studiomultitracks.com



melodyne

INFOS [MIXMEISTER BPM ANALYZER] [<http://mixmeister-bpm-analyzer.softonic.fr>][MELODYNE EDITOR] Où le trouver ? [www.celemony.com/fr/trial]

Difficulté: ☠☠☠

CRÉER UN BOOTLEG

CONNAÎTRE LE BPM D'UN MORCEAU

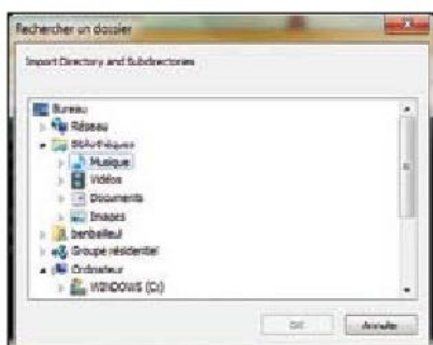
PRATIQUE



ÉTAPE 1

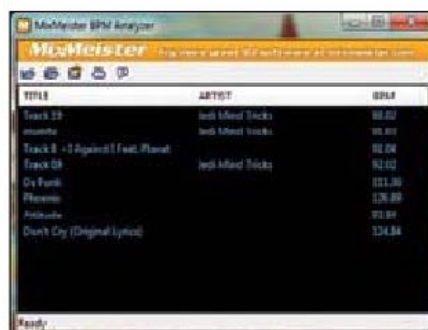
01 > BPM ?

MixMeister BPM Analyzer permet de connaître le nombre de BPM («beat per minute» ou «battement par minute» en français) d'un morceau de musique. Très utilisé pour ajuster au mieux le rythme une fois utilisé avec le logiciel Melodyne, ce programme est gratuit. Installez-le et lancez l'interface.



02 > L'ANALYSE

Pour connaître le BPM d'un MP3 ou d'un autre type de fichier musical, faites un glissé-déposé dans la fenêtre du logiciel et attendez d'avoir le nombre de BPM qui s'affiche. Il est possible de mettre plusieurs morceaux en même temps ou d'exporter les résultats dans un fichier TXT.



MELODYNE À VOTRE SERVICE

PRATIQUE

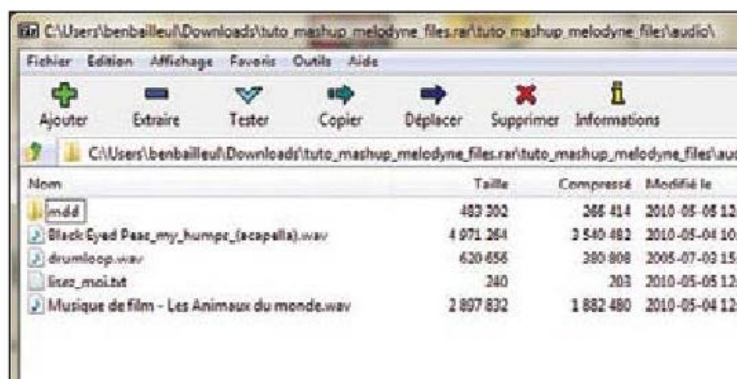


ÉTAPE 2

MELODYNE EST UN LOGICIEL PERMETTANT DE JOUER AVEC LES RYTHMES ET LA TONALITÉ DES MORCEAUX DE MUSIQUE. LES BOOTLEGGERS S'EN SERVENT AVANT TOUT POUR «CALER» LES TEMPOS DES DIFFÉRENTES COMPOSANTES DE LEUR CRÉATION. NOTRE PARTENAIRE FISSUNIX PROPOSE SUR SON SITE UNE VIDÉO QU'IL A LUI-MÊME RÉALISÉE POUR EXPLIQUER COMMENT UTILISER CE LOGICIEL ET FAIRE UN BOOTLEG DE A À Z. MALHEUREUSEMENT, ELLE DURE 25 MINUTES. NOUS ALLONS DONC PRÉSENTER DE MANIÈRE SUCCINCTE LES ÉTAPES. POUR PLUS DE PRÉCISION ET AVOIR EN MÊME TEMPS LES EXPLICATIONS DE L'ARTISTE, NOUS VOUS INVITONS À DÉCOUVRIR SA VIDÉO ICI : [HTTP://GOO.GL/EZxX3l](http://goo.gl/eZxX3l).

01 > LES ÉLÉMENTS

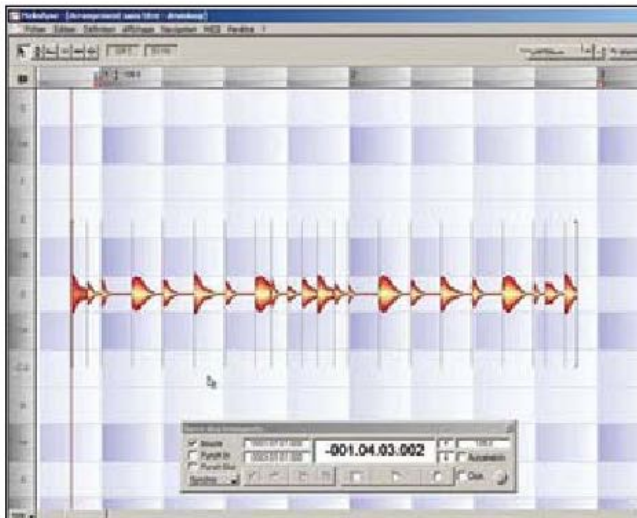
Commencez par télécharger la version démo de Melodyne ainsi que les morceaux nécessaires à la démonstration. Fissunix vous facilite la tâche puisque vous trouverez le pack à cette adresse: <http://goo.gl/n19q9>. Le fichier RAR contient une boucle de batterie, la version a capella d'un morceau des Black Eyed Peas et la musique des Animaux du monde.





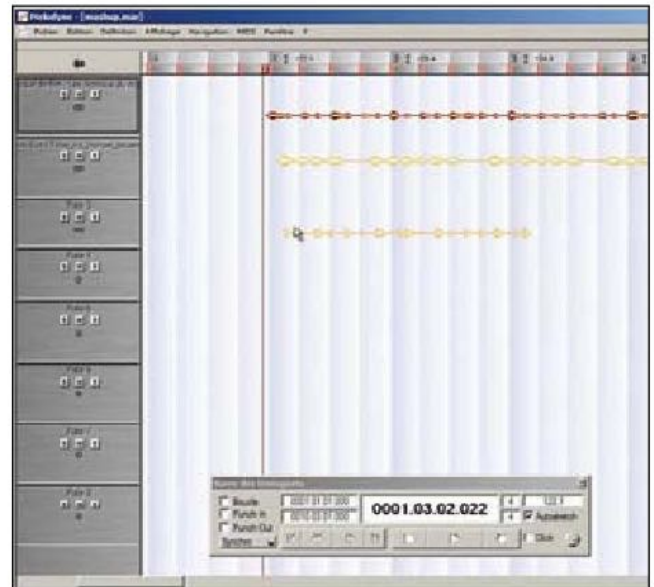
02 > LE FICHIER MDD

Après avoir glissé-déposé la boucle de batterie dans Melodyne, le logiciel va l'analyser et afficher une onde le représentant. Calez la boucle sur le début de la mesure et n'oubliez pas de sauvegarder le fichier MDD qui contient toutes les informations de votre projet. Faites de même avec la musique des Animaux du monde. Ici, il faudra utiliser le **Mode d'édition Tempo variable** (dans **Édition**), car ce morceau n'a pas été enregistré avec une boîte à rythmes. Suivez les instructions de la vidéo.



03 > LE FICHIER MAR

Sauvegardez une nouvelle fois le MDD et sauvegardez aussi cet arrangement. Ouvrez ce nouveau fichier MAR pour afficher une nouvelle



vue multipiste. Avant de mettre les 2 autres pistes, il faudra retravailler un peu l'a capella. C'est ici que vous aurez besoin de **MixMeister BPM Analyzer**. Une fois terminé, rouvrez le fichier MAR et placez votre a capella en piste2 et la batterie en3.

04 > LES DERNIERS RÉGLAGES

Calez le tout en suivant les instructions très détaillées de l'artiste. Dans **Fenêtre > Mixeur**, vous avez accès à la table de mixage pour augmenter ou baisser le son de certaines pistes. Toujours dans **Fenêtre**, choisissez **Offset Temps Réel de Lecture** et dans **Tempo**, réglez le rythme global de votre morceau. Dans **Fichier > Sauvegarder Audio...** sauvegardez votre expérience au format désiré.





INFOS [TVSHOWTIME]

Où le trouver ? [www.tvshowtime.com]

Difficulté :

TVShowTime : VOS SÉRIES LE JOUR DE LEUR SORTIE !

VOUS AIMEZ LES SÉRIES
TV, MAIS VOUS N'ARRIVEZ
JAMAIS À VOUS SOUVENIR
DE LA DATE DU PROCHAIN
ÉPISODE ? VOUS AVEZ
AUSSI DES DIFFICULTÉS
À TROUVER UN LIEN DE
TÉLÉCHARGEMENT OU
DES SOUS-TITRES ?
TVSHOWTIME VA VOUS
SIMPLIFIER LA VIE...



Organisation,
informations,
visionnage :
l'outil parfait
pour les fans de
série TV



L'obligation de
s'abonner à Put.
io (et de ne pas
pouvoir choisir
son service de
seedbox)

T

VShowTime
est un site
qui recense
et diffuse

les séries les plus
regardées. Il s'agit en
fait d'un concept hybride à mi-
chemin entre le stream et le P2P.
Le service utilise le site Put.io pour
diffuser en stream des Torrents
triés sur le volet. Attention, les deux
sites n'ont rien en commun. Non
seulement le choix et la qualité
sont au rendez-vous, mais le site
vous permet de rester au courant
de la diffusion des épisodes. Si
la VO ne vous fait pas peur, vous
pourrez donc regarder un épisode
le lendemain de sa diffusion aux
USA. Pour les sous-titres, il faudra
attendre quelques jours de plus
(parfois 24 h seulement !). Il existe
même une application pour les
appareils sous Android ou iOS !



UN SERVICE QUI FONCTIONNE DEPUIS UN AUTRE...

Le seul reproche que l'on peut faire
à ce site très bien conçu, c'est qu'il
faudra s'abonner à Put.io. Un mois
d'utilisation vous en coûtera 8 € mais
il existe une version d'essai de 24
heures pour moins d'un euro. Atten-
tion, ce Put.io est un service que vous
pouvez utiliser pour bien des choses.
Vous pourrez profiter d'une seedbox
pour télécharger des Torrents sans le
faire depuis votre ordinateur, stocker
des fichiers dans un Cloud et y avoir
accès depuis n'importe quel ordina-
teur. Un bon investissement si vous
êtes fan de séries...



PLUS BESOIN DE CHERCHER POUR
VOIR VOS SÉRIES TV, TVSHOWTIME
S'OCCUPE DE TOUT...



VOS SÉRIES À LA CARTE AVEC TVSHOWTIME

PRATIQUE



01 > LE COMPTE

Lorsque vous cliquez sur une série, vous verrez une fenêtre vous invitant à vous abonner au service de «cloud storage» [Put.io](https://put.io). Si vous cliquez sur



Create a Put.io account to watch my shows, cela ne fonctionnera que si vous avez un identifiant Facebook. Si vous n'avez pas de Facebook, il faudra aller sur le site <https://put.io> et vous inscrire de là-bas. Si vous avez déjà un compte de ce type, faites **Connect my Put.io account**.

02 > INSCRIPTION PUT.IO

Sur le site [Put.io](https://put.io), cliquez sur **Try It for 0,99\$** pour ne pas prendre de risque (on ne sait jamais, le service peut ne pas vous plaire). Entrez vos informations personnelles dans les champs et choisissez votre moyen de paiement (CB ou BitCoin). Lorsque c'est fait, vous êtes libre de découvrir Put.io (un très bon service à mi-chemin entre le Cloud et la seedbox), mais nous sommes là pour autre chose non ?



03 > VOS SÉRIES PRÉFÉRÉES

Une fois inscrit, vous pouvez revenir au site TVShowTime et vous inscrire aussi sur le site. Ici, c'est gratuit et très rapide. Pour vous accueillir, le site va vous demander de cliquer sur les séries



que vous avez l'habitude de regarder. Elles viendront s'ajouter en bas de la page. Si une manque à l'appel, vous pouvez toujours faire une recherche avec un mot clé. Faites **Next** lorsque vous avez fini.

04 > OÙ EN ÊTES-VOUS ?

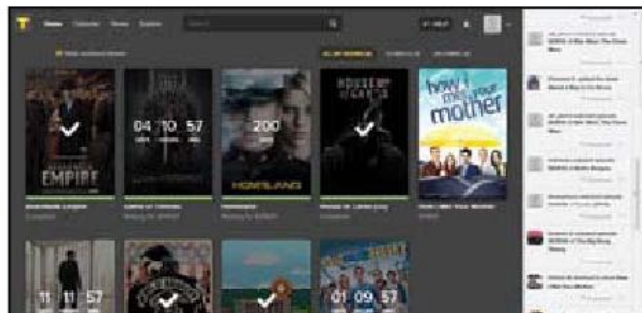
Pour chaque série, le site va alors vous demander quel est le dernier épisode que vous avez vu. Vous pouvez passer cette étape (**Skip this step**), mais nous le déconseillons. **I haven't start this show yet** signifie que vous n'avez vu encore aucun épisode et **The last aired** signifie que vous êtes «à jour». Faites **Next show** pour passer à la série suivante. À la fin, cliquez sur **Enter TVShowTime now!**





05 > VOTRE TABLEAU DE BORD

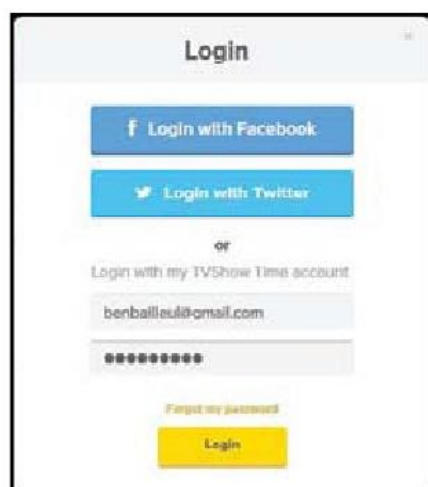
Vous verrez alors vos séries sur une seule page avec le temps restant pour le prochain épisode. Si la série est terminée ou que la date de diffusion est inconnue, vous verrez la mention **Complete**. Un peu plus bas, le site vous fera des



suggestions sur des séries que vous ne suivez pas, mais que vous pourriez aimer. Sur la droite, vous verrez ce que font les utilisateurs connectés au site. Vous pouvez commenter leur choix ou cliquer sur leurs séries pour les découvrir.

06 > MAIN DANS LA MAIN

Un peu plus haut dans **To Watch**, vous verrez les épisodes que vous avez en retard. Cliquez dessus et faites **Connect my Put.io**



account.

Entrez vos identifiants et quand le site vous demandera, cliquez sur **Authorize Application** pour que Put.io puisse «travailler» de concert avec TVShowTime.

On vous demandera ensuite de paramétrer les flux RSS pour que TVShowTime retrouve vos épisodes. Pas de souci, ici, puisque la communauté les aura déjà remplies pour vous. Faites juste **Submit RSS** à moins que vous n'ayez vos préférences.

07 > LE FICHER

TVShowTime va alors commencer à télécharger les épisodes (mis en cache). Vous pouvez en profiter pour vous découvrir les fonctionnalités du site (**Take a tour**). Une fois revenu l'interface, vous verrez le message **You will be able to watch your episode in a few minutes**. Un peu de patience! Une fois terminé, cliquez sur l'icône **Play**. Votre épisode va alors se lancer dans un player intégré au navigateur.



08 > TV SHOW TIME!

En bas à droite vous pourrez mettre la vidéo en plein écran, régler le son et surtout charger des sous-titres! Il suffit de cliquer sur **Subtles** et de choisir votre langue pour qu'ils



s'affichent immédiatement. Si l'épisode est trop récent, il faudra peut-être attendre un peu pour le français... Notez avec les touches **G** et **H**, vous pouvez décaler les sous-titres de quelques fractions de seconde. Si vous ne souhaitez pas voir l'épisode dans le navigateur, vous pourrez le télécharger (ainsi que les SUB) depuis le bouton **Download** un peu plus bas.



LIRE ET MODIFIER UN MKV



À l'inverse du Xvid ou du DivX, le MKV n'est pas un codec, mais bel et bien un format de fichier. Le nom MKV vient du russe Matroska qui désigne (lorsqu'il est bien orthographié) ces poupées russes de plus en plus petites et qui s'emboîtent. Il s'agit de montrer que ce format permet de renfermer (on dit «encapsuler»)

plusieurs fichiers. Mis à disposition gratuitement auprès du public depuis presque 10 ans, ce n'est que depuis quelques années seulement que ce format se répand sur la Toile et les réseaux P2P. Le MKV est capable d'encapsuler des contenus en HD, il est donc devenu un format privilégié pour la copie des Blu-Ray (comme l'AVI a été popularisé par les Rip DVD à son époque).

DE PLUS EN PLUS POPULAIRE SUR LES RÉSEAUX, LE FORMAT MKV EST, EN FAIT, UN CONTENEUR PERMETTANT DE REGROUPER PLUSIEURS FICHIERS DANS UN SEUL : VIDÉO, BANDE-SON, SOUS-TITRE, JAQUETTE, ETC. QUE VOUS VOULIEZ SÉPARER CES FICHIERS OU, AU CONTRAIRE, CRÉER VOS PROPRES MKV AVEC VOS SOURCES, IL EXISTE DES SOLUTIONS ADAPTÉES...

COMPATIBILITÉ AVEC LE MKV ?

Sur PC, le plus simple est de faire confiance à VLC Media Player qui gère ce format très simplement (allez dans **Audio>Piste audio** ou **Vidéo>Piste de sous-titres** pour changer la langue du doublage ou de sous-titrage). Le Media Center XBMC s'en sort aussi très bien. Au niveau des platines DVD, Blu-ray ou des disques durs multimédias, c'est un peu plus compliqué.

Si votre matériel date d'avant 2010, il faudra jeter un œil sur la notice ou tout simplement, faire l'essai. Attention, si votre appareil lit le MKV, il n'est pas obligé de lire les codecs qu'il contient !



Permet de jongler avec les MKV très facilement



Une interface un peu austère



Cet encapsulage permet de réunir tous les fichiers nécessaires à la lecture d'un film (sous-titres, éventuels doublages, etc.), mais aussi de chapitrer les séquences et de pouvoir contenir des fichiers encodés de différentes manières.

UN FORMAT, PLUSIEURS CODECS

En effet, un MKV peut très bien contenir un DivX avec une bande-son en MP3 et des sous-titres au format SUB comme il peut renfermer un H.264 (codec vidéo HD très à la mode) avec du son en AAC ou en FLAC. Certains

utilisateurs, qui n'ont pas de machine compatible (voir encadré) préféreront extraire les différents fichiers pour les utiliser tel quel alors que d'autres voudront faire leurs propres conteneurs MKV, car ils trouvent ce format plus facile à distribuer et à partager. Pour les deux, nous allons voir comment utiliser MKV Merge.



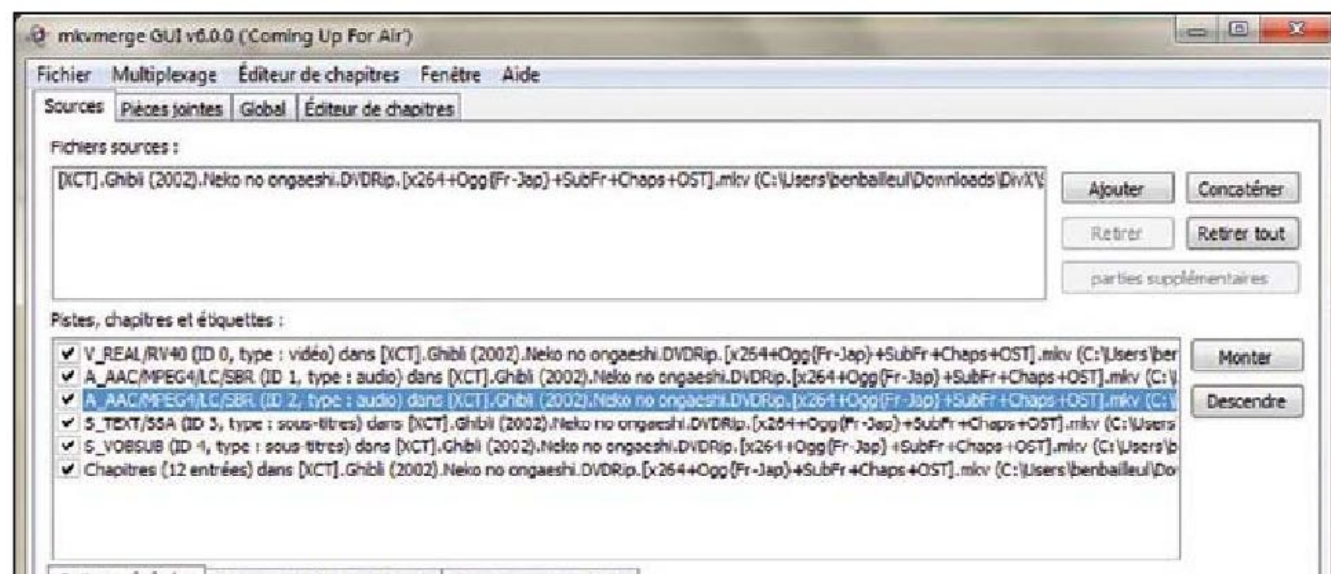
**PETIT À PETIT LE MKV
REMPLECE LE XVID ET LE
DIVX SUR LES RÉSEAUX P2P...**

PREMIERS PAS AVEC MKV MERGE

PRATIQUE


01 > LE CONTENU D'UN MKV

Téléchargez l'archive, décompactez-la et double-cliquez sur mmg.exe. Pour voir l'intérieur d'un MKV, faites **Ajouter** et sélectionnez votre fichier. Dans le cadre du dessous, vous verrez alors les différents éléments qui composent votre MKV. Les lignes qui commencent par **V** correspondent à une piste vidéo, **A** pour audio et **S** pour les sous-titres. En cliquant dans chaque piste, vous aurez les détails un peu plus bas.



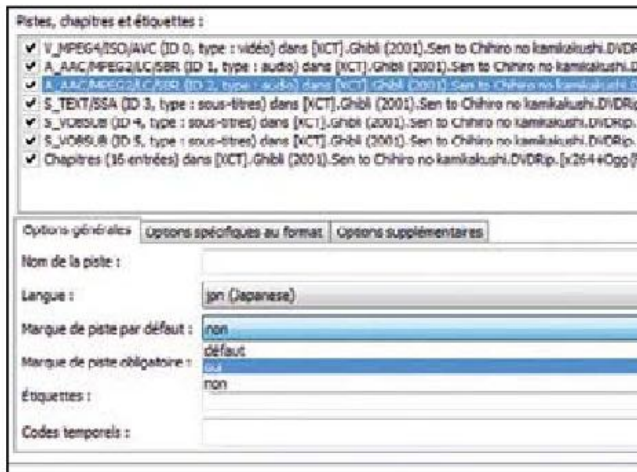


MULTIMÉDIA

Format Vidéo

02 > UNE MODIFICATION?

Imaginons que votre film se lance en VF, mais que vous voulez qu'il se lance en VOSTFR par



défaut. Il suffit de choisir la bande-son originale et de mettre **Oui** dans **Marque de piste par défaut**. Choisissez, ensuite, la piste de sous-titres français et faites de même. Notez que de cette manière les sous-titres ne sont pas incrustés, ils sont juste incorporés dans le même fichier.

03 > UN AJOUT?

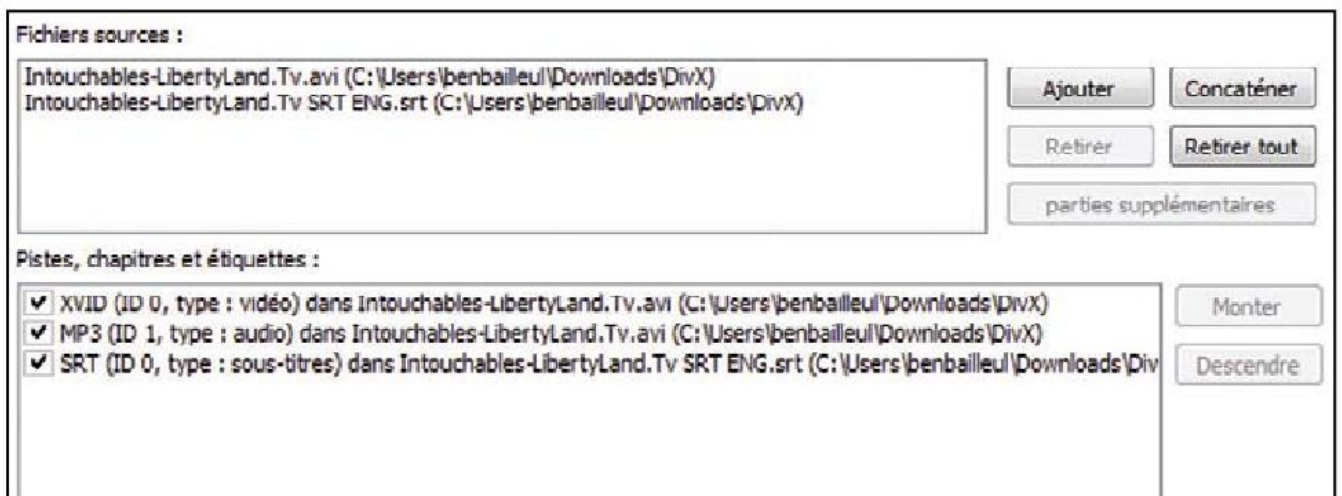
Pour être sûr du réglage, mettez toutes les autres **Marques de piste** par défaut sur **Non**. Elles seront présentes, mais ne démarreront pas au lancement. Notez qu'il est possible de décocher



une piste ou d'en rajouter une. Dans l'onglet **Pièce jointe**, vous pouvez ajouter la pochette ou d'autres éléments. Spécifiez le chemin du fichier final dans **Fichier cible** et faites **Démarrer le multiplexage**. Vous aurez alors votre MKV modifié à l'endroit spécifié.

04 > VOTRE MKV MAISON

Pour extraire les sous-titres, par exemple, ne cochez que cette case et faites encore **Démarrer le multiplexage**. Il est possible de renommer le fichier ainsi extrait. Pour ceux qui veulent se confectionner un MKV de toutes pièces, il suffit de faire **Ajouter** pour toutes les parties que vous voulez encapsuler (faites **Concaténer** pour réunir deux parties d'un film). Mettez de l'ordre dans vos pistes (voir étapes 2 et 3) et faites **Démarrer le multiplexage**.





INFOS [**PHROZEN DROPBOX TORRENT**] [www.phrozensoft.com/downloads.ps]

[**µTORRENT**] [www.utorrent.com] [**BitTorrent**] [www.bittorrent.com]

Difficulté:

Gérez vos Torrents À DISTANCE



IL N'EST PAS ÉVIDENT DE TÉLÉCHARGER DES TORRENTS LORSQU'ON TRAVAILLE OU QUE L'ON EST RAREMENT À LA MAISON. POUR AMORCER, SURVEILLER OU GÉRER SES TÉLÉCHARGEMENTS À DISTANCE, IL EXISTE CEPENDANT DES SOLUTIONS : CONTRÔLE À DISTANCE, SERVICE EN LIGNE OU LOGICIEL. SUIVEZ LE GUIDE...



Phrozen Dropbox

Un sorte de petite seedbox gratuite...

µTorrent

un des meilleurs logiciels pour vos .torrent avec la possibilité de gérer les téléchargements à distance.



Phrozen Dropbox

Pas le même puissance qu'une vraie seedbox

µTorrent

De la publicité dans la dernière version

Pour optimiser au mieux ses téléchargements, on était autrefois obligé de sauvegarder ses .torrent sur une clé USB pour les rapporter chez soi le soir et enfin commencer le rapatriement des fichiers. Rares sont en effet les jobs ou les bibliothèques universitaires où l'on peut télécharger sans être inquiété. Que vous soyez en vacances, au bureau ou tout simplement ailleurs, pourquoi attendre pour pouvoir profiter de vos fichiers multimédias ?

UNE SOLUTION POUR CHAQUE CAS DE FIGURE

Pour avoir ses fichiers prêts à l'emploi à l'heure de l'apéro ou tout simplement gérer ses

téléchargements lorsque vous n'êtes pas à la maison, il existe plusieurs solutions. La première consiste à paramétrer son client BitTorrent pour autoriser son contrôle à distance. Des logiciels comme xTorrent ou le client historique BitTorrent (qui propose la même interface) permettent ce genre de passe-passe. Si vous n'utilisez aucun de ces programmes, il existe enfin Phrozen Dropbox Torrent qui ira chercher les .torrent dans votre espace de stockage Dropbox pour commencer le téléchargement dès que vous les aurez placés dans votre répertoire dédié. Si vous n'avez pas accès à un PC, il est aussi possible de le faire depuis un mobile sous Android.

PUT.IO : IL TÉLÉCHARGE POUR VOUS !

Pour moins de 8 €/mois, Put.io vous propose un espace de stockage de 50 Go «intelligent» appelé «seedbox». Il permet en effet de télécharger pour vous n'importe quel fichier à votre place. Donnez-lui un .torrent à manger et il le rapatriera sur votre espace. Une fois chez vous, vous n'aurez qu'à le télécharger via HTTP (Direct Download) beaucoup plus rapidement. Notez que vous pourrez profiter d'une période d'essai de 24h pour moins d'un euro...

Lien : <https://put.io>



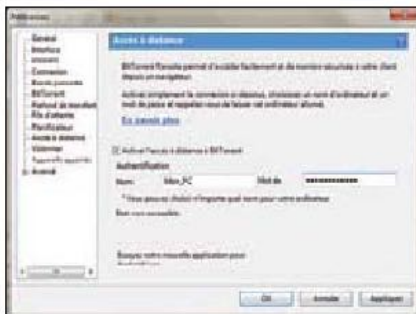
µTORRENT & BITTORRENT VIA L'INTERFACE WEB OU MOBILE

PRATIQUE



01 > SUR VOTRE PC

Commencez par télécharger la dernière version de µTorrent ou de BitTorrent et installez-la. Dans **Options > Préférences**, sélectionnez **Accès à distance** dans le



menu de gauche et cochez la case **Activer l'accès à distance µTorrent**.

Définissez un mot de passe, un identifiant

puis paramétrez une question de sécurité au cas où vous perdriez ces informations. Au bout d'un moment, le logiciel va vous avertir que l'inscription est terminée.

02 > SUR LE PC D'UN AMI OU AU BUREAU

Connectez-vous au site <https://remote.utorrent.com> ou <https://remote.bittorrent.com> en fonction du logiciel que vous utilisez et entrez vos identifiants.

Vous vous retrouverez alors avec exactement la même interface que votre logiciel. Si vous téléchargez des Torrents



à la maison et que votre PC est allumé, vous les retrouverez sans problème. Si vous disposez d'un mobile sous Android, les applications **BitTorrent Remote** et **µTorrent Remote** permettent aussi de faire le lien avec les mêmes identifiants.

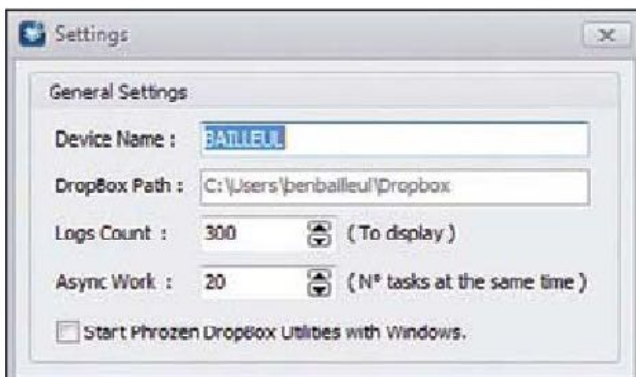
PHROZEN DROPBOX TORRENT : LA SOLUTION PASSE-PARTOUT

PRATIQUE



01 > LES RÉGLAGES

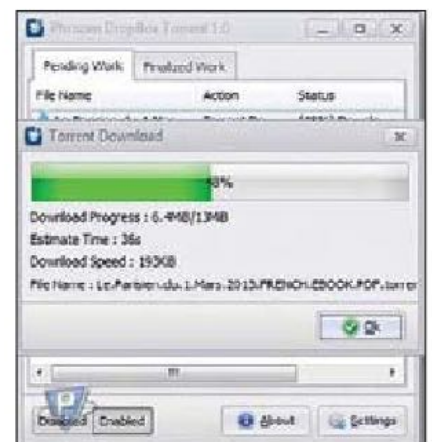
Si vous n'avez pas de client favori, il existe une autre solution. Phrozen Dropbox Torrent ira simplement chercher vos **.torrent** dans votre Dropbox. Après l'avoir installé, allez dans **Settings** pour vérifier que le chemin vers votre Dropbox est le bon. Ici, vous pourrez aussi cocher la case permettant de démarrer le programme avec Windows.



02 > LE TÉLÉCHARGEMENT

Après avoir mis votre **.torrent** dans la Dropbox, le fichier disparaîtra au bout de quelques secondes et il commencera à se télécharger sur votre PC. Vous retrouverez votre fichier dans le répertoire **Phrozen-Torrents** de votre Dropbox. Notez que si des erreurs apparaissent dans l'onglet

Finalized Work, il faudra peut-être régler une exception dans votre pare-feu...





INFOS [VLSUB]

Où le trouver ? [<https://github.com/exebetche/vlsub>]

Difficulté :

VLSUB :

LES SOUS-TITRES FACILES !

QUE DIRIEZ-VOUS D'OBTENIR TRÈS FACILEMENT LE SOUS-TITRE CORRESPONDANT À VOTRE VIDÉO SANS ALLER SUR UN SITE OU TÉLÉCHARGER UN FICHIER SUB OU SRT ? GRÂCE À L'EXTENSION VLSUB DE VLC MEDIA PLAYER, VOUS ALLEZ GAGNER DU TEMPS...

Simple, puissant et fonctionnant parfaitement avec tous types de fichier et de codecs, VLC Media Player est aussi très à l'aise avec les sous-titres. Pourtant, nous avons trouvé une extension qui améliore encore plus la prise en charge de ces derniers. Après avoir installé VLSUB, vous pourrez automatiquement récupérer les sous-titres du film que vous êtes en train de lire depuis la base de données OpenSubtitles. Plus besoin d'utiliser un logiciel séparé ou d'aller sur le site !



NE CHERCHEZ PLUS DES SOUS-TITRES COMPATIBLES PENDANT DES HEURES !



Terminées les laborieuses recherches de sous-titres !



Des difficultés d'installation en fonction de votre configuration (voir encadré)

EN CAS DE PROBLÈME...

Comme l'extension est encore en version bêta, vous pourriez rencontrer certains problèmes. Si tout ne fonctionne pas comme vous le voulez, faites un tour sur cette page qui dresse une liste de problèmes avec les solutions adéquates...

Lien : <http://goo.gl/vaHYdv>



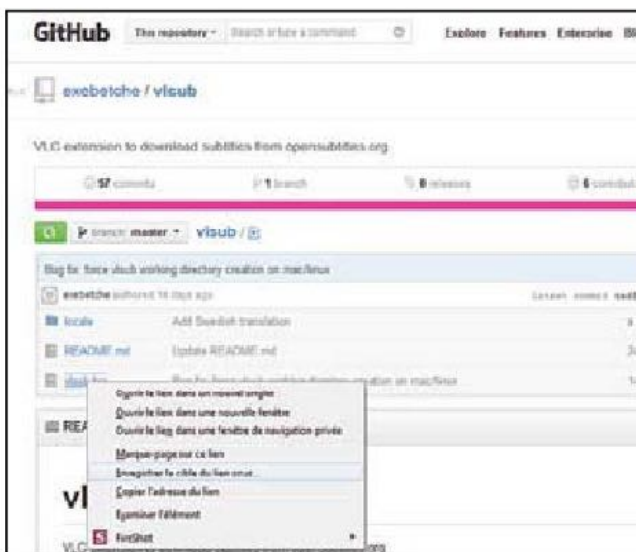
LES SOUS-TITRES, C'EST AUTOMATIQUE !

PRATIQUE



01 > RÉCUPÉRATION DU FICHIER LUA

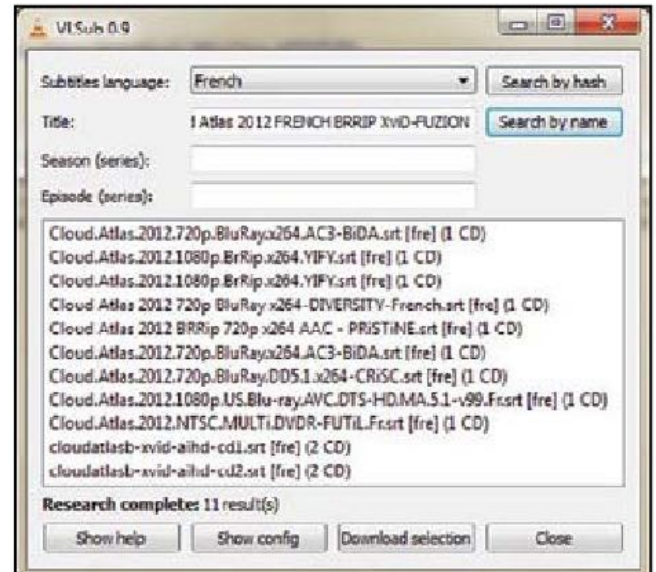
Le même fichier LUA vous servira quel que soit votre système d'exploitation (Windows, Mac, Linux). Sur la page du projet, faites un clic droit dans **vlsb.lua** puis **Enregistrer la cible du**



lien sous... avec Firefox ou **Enregistrer le lien sous avec Chrome**. Il faudra ensuite mettre le fichier dans un répertoire **extensions** que vous aurez créé pour l'occasion (si vous n'avez jamais utilisé ce type de fichiers). Ce dossier ira dans **ProgramFiles\VideoLAN\VLC\lua**. Si vous avez des difficultés ou si l'extension ne fonctionne pas sous Windows 7 & 8, il faudra utiliser l'installateur : <http://goo.gl/SXQrDL>.

02 > L'INTERFACE

Redémarrez éventuellement VLC et après avoir lancé une vidéo, allez dans le menu **Vue** et cliquez sur **VLSb 0.9.9** pour faire apparaître l'interface. Choisissez la langue des sous-titres et cliquez sur **Search by name** pour trouver un sous-titre correspondant au nom. **Search by hash** permet de trouver un sous-



titre correspondant directement à l'empreinte numérique de votre film même s'il est nommé n'importe comment.

03 > LE RÉSULTAT

Sélectionnez le sous-titre dans la liste et cliquez sur **Download selection**. Le sous-titre devrait s'afficher immédiatement dans votre fenêtre. Si ce dernier ne correspond pas à ce que vous recherchez, trouvez-en un autre ou si vous



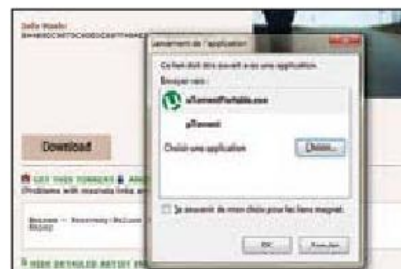
constatez un décalage entre la parole et les textes, vous pouvez corriger cela avec les touches **G** et **H** du clavier (retarder et avancer l'apparition des sous-titres).



VOS TORRENTS DANS UNE CLÉ USB

// AVEC TORRENT PORTABLE

µTorrent Portable est la version «prête à emporter» du célèbre client de téléchargement. Depuis votre PC, il suffit d'installer le logiciel sur une clé USB ou un disque dur externe pour le rendre opérationnel depuis ce périphérique. Si vous téléchargez à partir de liens magnet, il suffit de cliquer dessus et de spécifier que vous voulez télécharger à partir de votre version de µTorrent Portable (en recherchant le programme dans votre clé USB grâce au bouton **Choisir** qui va s'afficher). Si, au contraire, vous avez l'habitude de télécharger le fichier **.torrent**, placez ce dernier dans la clé et glissez-déposez-le dans la fenêtre principale du client. Lorsque le logiciel vous demandera l'emplacement où vous désirez stocker le fichier à télécharger, n'oubliez pas non plus de pointer vers votre clé USB ou votre disque dur externe. Une fois chez un ami ou sur votre autre poste, vous pourrez donc commencer ou continuer vos téléchargements rien qu'en branchant votre clé et en démarrant le programme.



    <http://utorrent-portable.softonic.fr>

SOYEZ MAÎTRE DE VOS SOUS-TITRES

// AVEC SUBTITLE EDIT

Si vous lisez *Pirate Informatique*, vous savez que nous faisons souvent la part belle à la gestion des sous-titres dans nos pages. Nous sommes en effet des amoureux de la VOST et nous aimons partager nos connaissances sur ce sujet avec nos lecteurs. Voici notre dernière trouvaille en ce qui concerne cet aspect de la vidéo: Subtitle Edit. Ce logiciel est à l'opposé de ses concurrents: interface conviviale et en français, rapidité d'exécution et tout terrain. Vous pourrez en effet corriger l'orthographe, les Time stamps, la traduction ou la synchronisation. Si vous avez un sous-titre qui n'est pas reconnu par votre appareil, il est aussi possible de convertir le fichier puisque Subtitle Edit prend en charge une centaine de formats et de sous-formats.

    www.nikse.dk/subtitleedit



RÉDUIRE LE POIDS D'UNE PHOTO

// AVEC IRFANVIEW OU JPEG EXPRESS

Avec les récents appareils photos numériques, le poids des images devient vite problématique: 4, 8 voire 16Mo pour un fichier! Si vous voulez mettre vos clichés sur Internet, les envoyer par e-mail ou les placer sur un cadre numérique,



pas besoin d'autant de données! Téléchargez et installez IrfanView, ouvrez votre photo et faites **File>Save as...** puis cochez la case **Show options dialog**. Grâce à la barre de réglages de cette nouvelle fenêtre, réglez la qualité. Vous pouvez faire de même avec le logiciel JPEG Express.

Attention, surtout ne nommez pas ces photos de la même manière que l'original, vous pourriez écraser vos précieuses photos en haute résolution!



www.irfanview.com ; <http://goo.gl/zQbuL>



TROUVEZ CE QUI PREND DE LA PLACE

// AVEC WINDIRSTAT

Le problème avec les disques durs de plus en plus gros, c'est qu'on y met tellement de fichiers qu'il est bien difficile de s'y retrouver. Entre les films, les photos de vacances ou les gigaoctets de MP3 que vous avez récupérés chez votre cousin, vous ne savez plus où sont ces dossiers qui vous prennent de la place pour rien. Heureusement avec WinDirStat vous allez pouvoir vous rendre compte graphiquement des endroits de votre disque dur qui sont surchargés. Passez la souris sur les éléments rectangulaires pour voir de quoi il s'agit. Plus l'élément est gros et plus il prend de place...



<http://windirstat.info>



VÉRIFIEZ L'INTÉGRITÉ DE VOS PHOTOS

// AVEC BAD PEGGY

Si vous aimez la photo et que vous prenez cliché sur cliché, vous vous êtes peut-être rendu compte de la fragilité du format JPEG. Lors d'un transfert ou d'une copie, il arrive parfois que vos précieuses photos deviennent illisibles: on dit qu'elles sont corrompues. Si le mal est déjà fait, vous pouvez toujours essayer les versions d'évaluation de Recover My Files ou de Best Image Repair. Si ses programmes vous ont plu, vous serez libre de payer pour obtenir une licence. Mais pour éviter d'en arriver là, il est possible de vérifier l'intégrité de vos JPEG avec Bad Peggy après chaque transfert! Le logiciel vous dira quel cliché a mal été transféré ou a été corrompu avant de vous proposer de les effacer. Vous pourrez donc supprimer vos photos de votre carte SD en toute tranquillité...



www.recovermyfiles.com ;

<http://goo.gl/J8dmt> ;

www.coderslagoon.com/#badpeggy



FAITES DES GIF ANIMÉS

// AVEC SCREENTOGIF OU QGIFER

Omniprésent dans les années 90 puis tombés en désuétude, les GIF animés reviennent à la mode! Il s'agit en fait d'images au format GIF qui, lues les unes à la suite des autres, se transforment en vidéo. Il est aussi possible de partager des «cinemagraphs», des tutoriels ou des diaporamas sans que vos amis aient de logiciel de lecture vidéo ou le codec adéquat. Screentogif est un logiciel qui vous propose d'enregistrer au format GIF ce qui se passe sur votre écran. Placez la fenêtre dans la zone que vous voulez enregistrer et vous n'aurez qu'à appuyer sur le bouton d'enregistrement! Et dans le cas où vous voudriez transformer une vidéo existante en GIF animé, le programme QGifer propose d'ajouter du texte, des éléments graphiques et d'éditer votre création...



<http://screentogif.codeplex.com> ;
<http://sourceforge.net/projects/qgifer>

SYNCHRONISEZ UN DOSSIER AVEC MEGA

// AVEC MEGASYNC

Vous aimez la manière dont fonctionne Dropbox, SkyDrive ou Google Drive avec leur «Cloud» et leurs dossiers Windows qui se synchronisent tout seuls? Le problème c'est que ces trois services proposent moins d'espace de stockage que MEGA qui lui, ne comporte pas de dossier synchronisé (respectivement 2, 7 et 15 Go contre 50 Go pour MEGA). Il suffisait donc d'en créer un! Installez MEGASync sur votre PC et vous pourrez paramétrer un ou plusieurs répertoires, réguler la bande passante des transferts et vérifier qu'il vous reste toujours de la place pour stocker tous vos fichiers en ligne...



Lien: <http://goo.gl/2El3af>

CHEZ VOTRE
MARCHAND DE JOURNAUX

LES PIRATES CRYPTENT, NOS LECTEURS DÉCRYPTENT!

WI-FI,
ANONYME,
MOBILES,
HACKING,
ENCODAGE,
ANTIVOL,
CRYPTAGE,
MOTS
DE PASSE,
SURVEILLANCE

+ EN CADEAU : 2 magazines complets offerts SUR LE CD

LES CAHIERS DU HACKER **PIRATE** [INFORMATIQUE] // 22

SIMPLES ET 100% EFFICACES
**LES MEILLEURES
RECETTES
& ASTUCES
SECRÈTES
DES HACKERS**

GUIDE
PRATIQUE!
avec CD GRATUIT
> Les meilleurs
logiciels avec
PAS À PAS!

SMS cryptés
Streaming
Mots de pas
Smartph
Anony
Web Inte
Prise de con

spécial MESSAGERIE
HACKER SKYPE :
jeu d'enfants

NAVIGATION
PACK DE GPS :
LÉgal ET
GRATUIT



MULTIMÉDIA
FILMS, VIDÉOS, MP3 :
TOUT TÉLÉCHARGER, TOUT
PARTAGER, TOUT STREAMER!

BRICOL'H
CRÉEZ VOTRE
ÉMETTEUR
RADIO PIRATE



+ CD GRATUIT **PACK 100% PIRATE**

MOTS DE PASSE



34

JOHN THE RIPPER :

le logiciel ultime pour cracker

42

PASSWORD SAFE :

un coffre fort à mot de passe

46

CRACKEZ le mot de passe de **WINDOWS !**



INFOS [JOHN THE RIPPER]

Où le trouver ? [www.openwall.com/john]

Difficulté :   

Crack de mots de passe AVEC JOHN THE RIPPER

LE CRACK DE MOTS DE PASSE EST UN SUJET TABOU DANS LA PRESSE INFORMATIQUE. EN EFFET, CETTE TECHNIQUE EST SOUVENT ASSOCIÉE AUX PIRATES ALORS QU'IL S'AGIT AUSSI DU SEUL MOYEN DE VÉRIFIER LA SÉCURITÉ DE SES SÉSAMES. À *PIRATE INFORMATIQUE*, NOUS AVONS DONC DÉCIDÉ DE VOUS MONTRER COMMENT UTILISER JOHN THE RIPPER, LE LOGICIEL SPÉCIALISÉ DANS CETTE DISCIPLINE.



Comment savoir si vos mots de passe sont sûrs ? Nous avons déjà abordé le sujet par le passé en expliquant qu'un sésame doit être à la fois long, ne rien vouloir dire (pas un mot du dictionnaire donc) et alterner les lettres majuscules, minuscules, chiffres et autres caractères spéciaux (\$, ^, ×, &, etc.). Ces précautions sont primordiales pour qu'une personne ne devine pas votre mot de passe trop facilement, mais aussi pour contrer le logiciel dont nous allons vous parler.



Un seul logiciel regroupant plusieurs techniques pour cracker les mots de passe



Demande un peu d'entraînement avant de maîtriser toutes les facettes du logiciel



UN LOGICIEL TRIPLE ACTION !

John the Ripper est un logiciel de cassage de mot de passe : un «crack» du crack. Plusieurs techniques sont à sa disposition. Le mode simple (single crack mode) va essayer plusieurs mots de passe en fonction du nom d'utilisateur. Pour un identifiant Jésus, il va essayer Jésus, Jésus123, Jésusazerty, etc. Inutile de dire que si votre mot de passe est de ce type, il faudra quelques secondes à John pour le découvrir. L'attaque par dictionnaire est aussi dans ses fonctions, donnez-lui une liste de mots dans un fichier (facilement trouvable sur le Net dans différentes langues) et il

les essaiera tous en alternant les majuscules et les minuscules si besoin est.

«SINGLE CRACK», «DICTIONARY» PUIS «BRUTE FORCE»

Il faudra garder en tête que tous les utilisateurs ne sont pas français et qu'il faudra avoir sous le coude plusieurs dicos dans plusieurs langues pour arriver à ses fins. Bien sûr, ces dictionnaires sont compilés par des hackers et ils couvrent plusieurs domaines, y compris l'argot, le langage technique ou des mots de passe très utilisés par les personnes négligentes : azerty, 123456, password, secret, etc. La bonne chose de cette

```
C:\ Invite de commandes

Copyright (c) 1996-2011 by Solar Designer
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single                "single crack" mode
--wordlist=FILE --stdin wordlist mode, read words from FILE or stdin
--rules                enable word mangling rules for wordlist mode
--incremental[=MODE]   "incremental" mode [using section MODE]
--external=MODE         external mode or word filter
--stdout[=LENGTH]      just output candidate passwords [cut at LENGTH]
--restore[=NAME]        restore an interrupted session [called NAME]
--session=NAME          give a new session the NAME
--status[=NAME]         print status of a session [called NAME]
--make-charset=FILE     make a charset, FILE will be overwritten
--show                 show cracked passwords
--test[=TIME]           run tests and benchmarks for TIME seconds each
--users=[-]LOGIN:UID[,..] [do not] load this <these> user(s) only
--groups=[-]GID[,..]    load users [not] of this <these> group(s) only
--shells=[-]SHELL[,..]  load users with[out] this <these> shell(s) on
--salts=[-]COUNT       load salts with[out] at least COUNT passwords
--save-memory=LEVEL     enable memory saving, at LEVEL 1..3
--format=NAME           force hash type NAME: des/bsd/md5/bf/afs/lm/dummy

C:\Users\benbailleul>
```

Comme tout logiciel puissant, John the Ripper est assez complexe. En faisant `C:\john\run\john.exe`, vous aurez une liste des commandes disponibles.



MOTS DE PASSE

Cracking

méthode, c'est que lorsque le logiciel a épuisé le dictionnaire, vous êtes sûr que le mot de passe ne se trouve pas dans le dico. Il faudra alors changer de dico ou passer à la méthode brute force... Avec cette technique, le logiciel va essayer tous les mots de passe possible en commençant par exemple par aaaaaa puis aaaaab, aaaaac, etc. Plus le mot de passe est long et plus il comporte de types de caractères différents et plus il sera difficile de le découvrir. D'un autre côté, avec la puissance des PC de maintenant et la possibilité d'utiliser plusieurs ordinateurs, les pirates font de véritables prouesses.



JOHN THE RIPPER PROPOSE TROIS TYPES DE MÉTHODES POUR CRACKER LES MOTS DE PASSE

DU HASH ?

Pour retrouver le mot de passe, John the Ripper aura besoin du «hash» correspondant. En effet, les mots de passe ne sont jamais écrits en clair dans une base de données ou un ordinateur, ils sont codés avec une fonction de hachage. Il en existe plusieurs : MD5, SHA256, NTLM, etc. Notez qu'un hash comme **721a9b52bfceacc503c056e3b9b93cfa** ne correspond qu'à un seul mot de passe. John the Ripper va analyser ces «hashs» et en déduire le mot de passe avec différentes méthodes. Pour savoir à quel type de «hash» vous avez affaire : <http://goo.gl/uQ5B4v>.

LEXIQUE

*CRACK :

Cracker un mot de passe c'est le «casser», réussir à l'obtenir en utilisant ses méninges et un logiciel (et oui, il faut les deux !)

*BRUTE FORCE :

La technique de bourrin pour retrouver un mot de passe. Le logiciel va essayer toutes les combinaisons de lettres, de chiffres et autres caractères pour arriver à ses fins. Un mot de passe comme coucou peut être retrouvé en quelques heures, mais pour **dJer7(ghSg(^#H54*DùDCµ,cj`/fd,c ç lcnb_**, c'est mission impossible (à moins d'avoir un super calculateur ou quelques siècles devant soi...)

*HASH :

Les mots de passe ne sont jamais écrits en clair dans une base de données ou un ordinateur, ils sont codés avec une fonction de hachage. Il en existe plusieurs : MD5, SHA256, NTLM, etc. Notez qu'un hash comme **721a9b52bfceacc503c056e3b9b93cfa** ne correspond qu'à un seul mot de passe. John the Ripper va analyser ces «hashs» et en déduire le mot de passe avec différentes méthodes.



LA MÉTHODE «DICTIONNAIRE»

PRATIQUE



01 > LES BASES

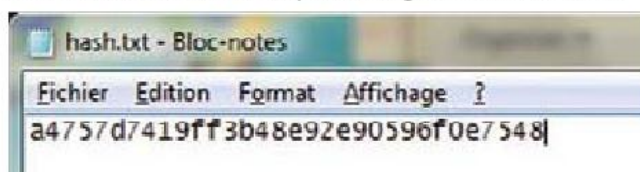
Commençons par télécharger la version Windows de John the Ripper en suivant notre lien. Pour notre démonstration, nous choisirons la version Jumbo qui contient des outils additionnels sélectionnés par la communauté. Pour plus de facilité, nous vous invitons à la décompresser dans votre disque dur **C:** en racine. Renommez alors le



dossier **John179J5w** en **John**. Ce dernier devrait contenir un dossier **run** et un dossier **doc**. Pour la démonstration, nous allons devoir générer un hash à partir d'un mot de passe très utilisé chez les Américains: **god** (dieu). Allez sur le site **www.md5.fr** et tapez **god** pour obtenir le hash **a4757d7419ff3b48e92e90596f0e7548**.

02 > PREMIER ESSAI

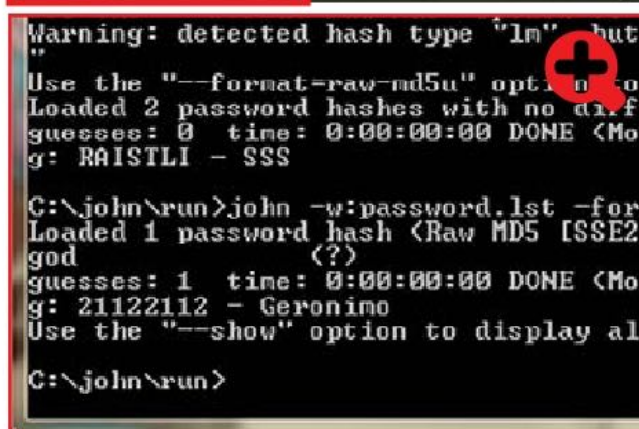
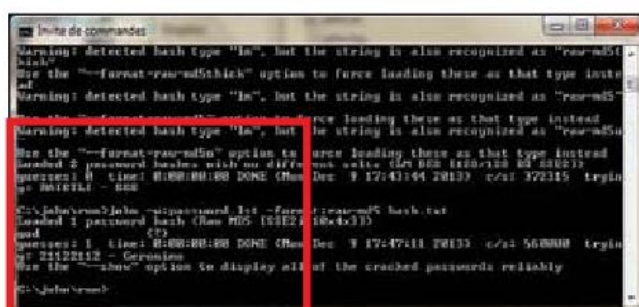
Collez ce hash dans un fichier **hash.txt** qui prendra place dans **C:\John\run**. Pour utiliser le logiciel, il faudra utiliser des lignes de commandes. Rien ne sert de double-cliquer sur le fichier **John.exe**, allez dans le champ **rechercher** du menu **Démarrer** et tapez **cmd** puis sélectionnez **cmd.exe**. Faites alors **cd C:\John\run**, validez puis tapez **John -w:password.lst hash.txt** avant de faire **Entrée**. **-w:password.lst** correspond au fichier **password.lst**, un dictionnaire basique en anglais contenu dans



le dossier **run**. John the Ripper ira piocher dans ce fichier pour trouver le bon mot de passe. Bien sûr, **hash.txt** est votre fichier renfermant le hash correspondant au mot de passe **god**.

03 > RÉSULTAT EN MOINS D'UNE SECONDE

Surprise, le logiciel ne trouvera rien et il vous dira que ce hash peut correspondre à plusieurs types: MD4, Lotus5, etc. Ici, nous savons qu'il s'agit de MD5 brut (raw en anglais) donc nous allons taper **John -w:password.lst -format:raw-md5 hash.txt** pour aider le logiciel. Ici, le mot de passe **god** est trouvé en moins d'une seconde! Bien sûr, la rapidité va dépendre de l'importance du dictionnaire, mais comme John the Ripper peut essayer des centaines de mots de passe à la seconde, cela est souvent rapide... Dans le cas où vous ne savez pas le type, il faudra tous les essayer ou utiliser HashTag (<http://goo.gl/uQ5B4v>).





Le fichier **password.lst** contient les mots les plus utilisés chez les Anglo-saxons mais il est assez pauvre (seulement 1000 mots). Pour de meilleurs résultats, il faudra utiliser un dictionnaire multilingue ou de préférence un dictionnaire bilingue français-anglais car il est possible de spécifier la langue de la liste de mots (il faudra placer ce fichier dans le dossier **dict** et changer son nom après **-w**). Allez sur <http://goo.gl/dQJxX> ou ici (<http://goo.gl/9B9BO>) pour profiter de deux fichiers de plus : un fichier de mots anglais et mots de passe les plus utilisés tandis qu'à cette adresse, <http://goo.gl/9B9BO>, vous trouverez une liste de mots en français (<http://goo.gl/9B9BO>). À vous d'en trouver d'autres qui vous conviennent.

Une dernière astuce consiste à essayer des variantes. Par exemple, si le mot de passe est **god123**, **GOD** ou encore **God!** et que le dico ne comprend que le mot **god**, le logiciel ne trouvera

rien. Il faudra encore une fois l'aider avec la commande **-rules** (règles). Vous trouverez une liste de règles à appliquer dans le dossier C:\john\doc et encore d'autres astuces pour parfaire votre recherche ici: <http://goo.gl/aeo0z8>.

39



LA MÉTHODE BRUTE FORCE

PRATIQUE



01 > LE «HASH» DE TEST

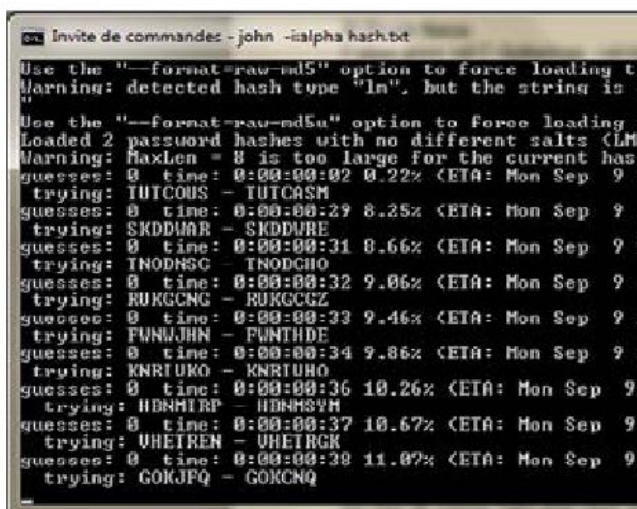
Pour cette démonstration nous partons du principe que vous avez déjà téléchargé John the Ripper (version Jumbo) et que le dossier **John** est bien en racine de **C:**. Si vous êtes perdu, regardez l'étape 1 du précédent pas à pas. Pour notre exercice, nous allons commencer par mettre



un hash MD5 dans un fichier texte pour que le logiciel retrouve le mot de passe associé. Allons sur **www.md5.fr** et notons le mot de passe **coucou** dans le champ (pour «chercher» un mot de passe de plus de 8 lettres, il faudra changer le fichier **john.ini**). Nous avons alors le hash suivant: **721a9b52bfceacc503c056e3b9b93cfa**. Dans une base de données MySQL, c'est ainsi qu'apparaîtrait votre mot de passe. Collez-le dans un fichier TXT que nous appellerons **hash.txt**. Placez ce fichier dans le dossier **run**.

02 > BRUTE FORCE

Faites alors **cd C:/John/run**, validez puis tapez **John hash.txt** après le **>**. Le logiciel va alors commencer le travail en essayant toutes les combinaisons de mots de passe. Si rien ne se passe à l'écran, c'est normal, le logiciel ne montre pas de barre de progression. Appuyez sur **Entrée** pour voir où il en est. **Guesses 0** signifie qu'il n'a encore rien trouvé (vous pouvez mettre plus d'un hash dans hash.txt). Ensuite, on peut voir le temps écoulé depuis le début du processus ainsi que son avancement en pourcentage puis à la fin les différentes plages de mot de passe qu'il essaye. Pour arrêter le processus, il faudra faire **Ctrl+C**.



UNE INTERFACE GRAPHIQUE ?

Si pour vous, utiliser John the Ripper sous Windows est un sacrilège, vous n'allez pas aimer Johnny ! Il s'agit d'une interface graphique pour John the Ripper. Au lieu d'entrer des lignes de commande, vous pourrez utiliser la plupart des options avec votre souris. Le problème, c'est que Johnny n'est pas encore disponible pour Windows. Choisissez ton camp camarade !





03 > OPTIMISEZ VOTRE «BRUTE FORCE»

Cela prend du temps, car le logiciel cherche dans toutes les directions. En effet, il existe plusieurs types de hash et il n'est pas aisé de les reconnaître. Ici comme nous savons qu'il s'agit d'un MD5 nous allons faire:

John -format:raw-md5 hash.txt

Dans ces conditions et sans même restreindre le champ des caractères, John the Ripper a mis 2 malheureuses secondes! Il faut dire que le mot de passe était très faible. Avec un mot de passe comme **Br7vcf,4**, au bout de 16 heures, nous n'avons pas encore exploré 0,02%



SI L'AVENTURE
BACKTRACK (KALI
LINUX) VOUS
TENTE, SACHEZ
QUE JOHN THE
RIPPER EST
INTÉGRÉ À CETTE
DISTRIBUTION...

```
CA Invite de commandes
c:\john\run>john -format:raw-md5 hash.txt
Loaded 1 password hash (Raw MD5 [SSE2i 10x4x3])
coucou (?)
guesses: 1 time: 0:00:00:02 DONE (Mon Sep 9 12:43:34 2013) c/s: 675
g: coftea - coupou
Use the "--show" option to display all of the cracked passwords reliably
c:\john\run>
```

des possibilités. Mais attention, non seulement il est possible d'améliorer ce résultat, mais le cassage n'est ici qu'une question de temps... 8 caractères, mêmes aléatoires ne sont pas suffisants pour une bonne protection.

04 > JOUEZ AVEC LES JEUX DE CARACTÈRES

Pour améliorer la rapidité, il est possible de réduire le champ de possibilité. Imaginons que vous avez oublié un mot de passe, mais que vous êtes sûr de n'avoir utilisé que des lettres, vous pouvez utiliser la commande **john -l:alpha hash.txt**. Tandis que **john -l:digits hash.txt** s'attaquera uniquement aux chiffres. On peut aussi utiliser d'autres types de restrictions pour gagner du temps comme ne chercher que des minuscules, des majuscules, cumuler les suites alphanumériques sans les espaces, etc. Il faudra pour cela ajouter d'autres fichiers **CHR** dans le dossier **run**.

ET SOUS LINUX ?

Nous avons conscience que proposer un tutoriel pour la version Windows de John the Ripper va hérisser les poils des puristes. En effet, le logiciel fonctionne à l'origine sous Linux (vous pouvez le retrouver sous BackTrack par exemple) et même si nous avons déjà parlé de la manière de faire tourner cette distribution sans installation, la version Windows permet aux néophytes de s'exercer sans se rajouter de difficultés.



INFOS

[PASSWORD SAFE] Où le trouver ? [<http://passwordsafe.sourceforge.net>][XCRETS] Où le trouver ? [www.axantum.com/Xcrets]Difficulté : 

Protégez VOS MOTS DE PASSE ! (EN LOCAL ET EN LIGNE)



VOUS CHERCHEZ UNE SOLUTION POUR SAUVEGARDER DE MANIÈRE SÉCURISÉE DES MOTS DE PASSE À LA FOIS EN LOCAL ET EN LIGNE ? AVEC **PASSWORD SAFE** ET LE SERVICE **XCRETS** VOUS NE PERDREZ PLUS JAMAIS VOS PRÉCIEUX SÉSAMES. ILS SERONT DISPONIBLES PARTOUT OÙ VOUS IREZ ET IMPOSSIBLES À VOLER GRÂCE À UN CHIFFREMENT AES 256 BITS...

Nous parlons souvent de services permettant de contourner les restrictions géographiques des sites de contenus multimédias : proxy, VPN, etc. UnoTelly propose, sans installation de logiciel, de faire

transiter votre trafic vers un hôte qui ne dévoilera pas votre véritable emplacement. Résultat : vous avez accès pour 3 €/mois à plus d'une centaine de sites de stream audio ou vidéo : Netflix, Hulu, Discovery Channel, les chaînes de la BBC, Pandora, MTV, CBS, HBO, Channel

**Password Safe**

Gratuit et très bien conçu

Xcrets

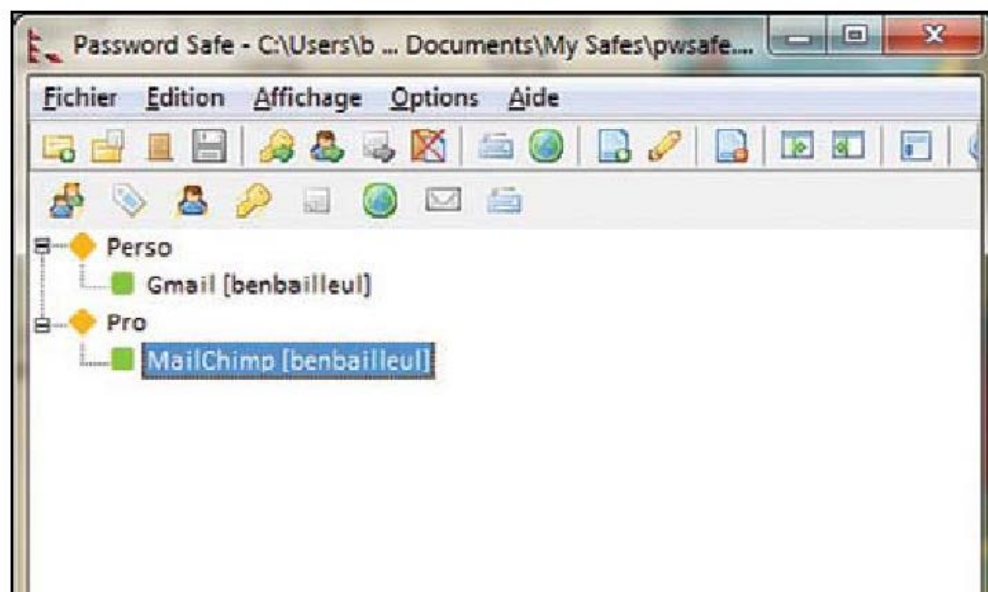
Même si vous ne souhaitez plus payer, vous aurez tout de même accès aux données.

**Password Safe**

Un peu laborieux si vous voulez entrer tous vos mots de passe mais c'est le prix de la tranquillité

Xcrets

Un service payant et une interface minimaliste.



Password Safe stocke de manière sécurisée tous vos mots de passe, mais vous pouvez aussi l'utiliser pour enregistrer vos codes PIN, numéro de carte bancaire, etc.



MOTS DE PASSE

Cracking

4, NBC, NBA TV, etc. La liste des chaînes est disponible sur le site et elle est dithyrambique ! Le service pense aussi aux Français expatriés ou en vacances puisque les chaînes françaises sont aussi présentes : TF1, Canal+, France Télévision, etc.

de logiciels à démarrer ou de mot de passe à entrer, tout est prêt directement. Sachez enfin que vous pourrez utiliser UnoTelly sur tous les appareils de votre maison : PC sous Windows ou Linux, Mac, iPad, console de salon, NAS, TV connectées, etc.

SANS PROXY NI VPN !

Même si la mise en place est un peu plus délicate que l'installation d'un logiciel, les avantages sont nombreux. Vous n'aurez pas à jongler avec 10 proxy différents, les flux audio et vidéo sont accessibles immédiatement et sans ralentissement. Les connexions sont aussi transparentes : pas



PASSWORD SAFE
SÉCURISE VOS MOTS
DE PASSE SUR VOTRE
DISQUE DUR ET
XECRET LE FAIT DANS
LE "CLOUD"

UTILISATION DE PASSWORD SAFE

PRATIQUE



01 > INSTALLATION ET FICHIER DE DONNÉES

Lors de l'installation, le logiciel vous demandera de choisir entre une utilisation sur un PC ou sur une clé USB (cette dernière n'utilise pas le registre). Dans la fenêtre qui vous invite à **Ouvrir le fichier de mots de passe**, faites **Nouveau**.



02 > VOTRE MOT DE PASSE GÉNÉRAL

Après avoir entré le nom de votre première base de mots de passe, le logiciel vous demandera de



choisir un sésame général qui déverrouillera tous les autres. Inutile de préciser qu'il faudra un mot de passe solide et à ne pas oublier. Validez pour afficher l'interface principale.



INFOS



[PASSWORD SAFE] Où le trouver ? [<http://passwordsafe.sourceforge.net>]

[XCRETS] Où le trouver ? [www.axantum.com/Xecrets]

Difficulté :

03 > LE PREMIER SÉSAME ENREGISTRÉ

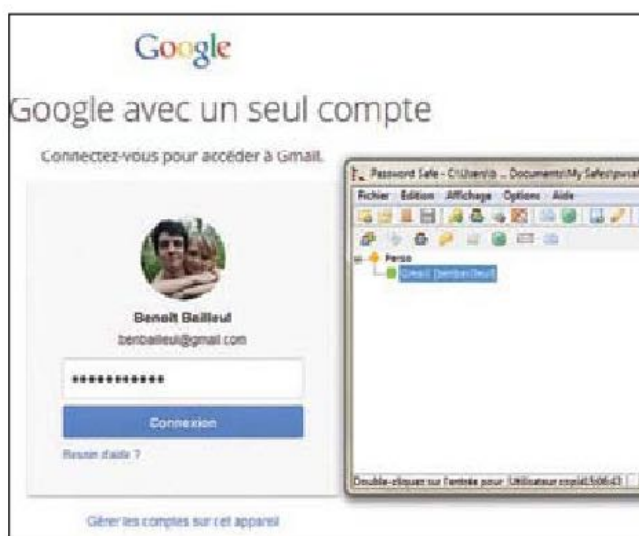
Faites ensuite **Édition > Ajouter** une entrée pour enregistrer votre premier mot de passe. Mettez un groupe (**Pro**, **Personnel**, etc.) puis un **Titre** (**Amazon** ou **Gmail** par exemple), un nom

d'utilisateur (login), une **URL** (pour avoir accès à la page directement depuis le logiciel) et votre

mot de passe. Dans **Heures et Dates** vous pouvez définir une date d'expiration pour votre mot de passe et dans **Stratégie** vous pourrez concevoir des mots de passe aléatoires.

04 > UTILISEZ VOTRE BASE DE DONNÉES

Après avoir validé, votre premier mot de passe enregistré apparaîtra dans la fenêtre principale. Vous pourrez accéder à la page en question avec un clic droit. Faites un double clic dans l'entrée et



le mot de passe sera intégré dans le presse-papier. Tout ce que vous aurez à faire sera de faire coller dans le champ adéquat. Pour copier l'identifiant (si celui-ci n'apparaît pas) il faudra faire **Maj** + double-clic. Il faudra reprendre l'**étape 3** avec tous vos autres mots de passe...

SUR MOBILE AUSSI !

Vous avez un smartphone ou une tablette sous Android ? Vous pourrez alors avoir accès à votre base de données stockée sur Xecrets ! Il suffit de télécharger l'application en suivant notre lien et de rentrer vos identifiants de connexion (ceux que vous avez utilisés pour ouvrir votre compte Xecrets). Vous aurez alors la liste des mots de passe que vous aurez importés. Vous pourrez faire Copy pour coller le sésame choisi dans une page internet ou un logiciel.

Lien: <http://goo.gl/BW7oHr>





TRANSFERT DES DONNÉES VERS XCRETS

PRATIQUE



01 > 90 JOURS GRATUITS

Xcrets est payant, mais si vous vous inscrivez (<http://goo.gl/HJDcrf>) vous pourrez l'utiliser gratuitement pendant 90 jours. Au-delà il vous en coûtera 3,30 € pour un trimestre. Notez que même si vous ne voulez plus payer après



cette période, vous aurez tout de même accès à vos mots de passe mais vous ne pourrez plus en ajouter d'autres. Après vous être inscrit, vous pourrez exporter toute la base de mot de passe depuis Password Safe à cette adresse: <http://goo.gl/6deQcx>.

02 > IMPORTER LA BASE DE MOTS DE PASSE

Cliquez sur le bouton **Parcourir** et retrouvez le fichier au format **.psafe3** normalement contenu dans **C:\Users\[nom d'utilisateur]\Documents\My Safes**. Attention, ce dernier ne devra pas faire plus de 500Ko. Si vous avez déjà uploadé un fichier



de ce type, le nouveau remplacera l'ancien. Dans le champ **Safe Combination**, tapez le mot de

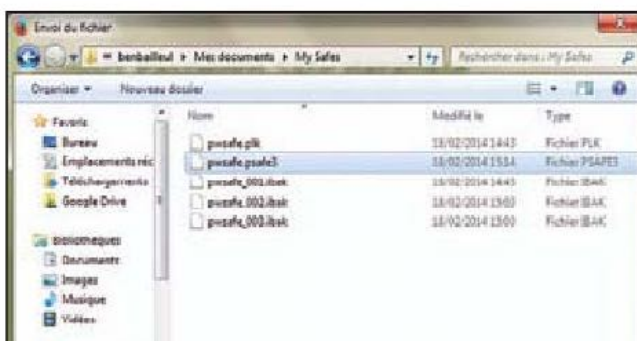
pas général que vous aurez choisi dans le logiciel Password Safe. Cliquez ensuite sur **Import!**

03 > RETROUVEZ VOS SÉSAMES!

Un message vous informant que vous avez envoyé avec succès X mots de passe vers Xcrets devait s'afficher. Pour récupérer vos mots de passe sur un autre PC, en vacances ou de votre travail, allez



sur le site <https://www.axantum.com> et cliquez sur le nuage. Dans le menu en colonne à gauche, repérez la partie sur **Xcrets**. Vous pouvez faire **Export** pour récupérer un document XML chiffré où figureront vos précieux sésames. Vous pouvez aussi aller dans **Search** pour taper le nom de votre entrée. Il s'agit de ce que vous avez tapé dans le champ **Titre** de Password Safe (par exemple **Amazon** ou **Gmail**). Notez qu'il existe une application pour mobile Android: <http://goo.gl/BW7oHr>.





Windows, OUVRE- TOI !



QUE VOUS AYEZ OUBLIÉ VOTRE MOT DE PASSE WINDOWS OU QUE VOUS NE LE CONNAISSIEZ PAS (ACHAT D'OCCASION, DÉPANNAGE CHEZ UN AMI, ETC.), IL EXISTE UNE SOLUTION POUR RÉINITIALISER CE DERNIER ET EN DÉFINIR UN AUTRE SI VOUS N'AVEZ PLUS LE DVD D'INSTALLATION.

Windows stocke les informations concernant l'utilisateur dans le fichier «sam» du répertoire **C:\Windows\system32\config**. Ce fichier contient notamment les mots de passe cryptés. Malheureusement, il n'est pas possible de changer le mot de passe si vous ne pouvez pas ouvrir une session avec les droits pour le faire. Si vous ne vous souvenez pas du mot de passe et que vous n'avez pas créé de clé USB permettant d'ouvrir votre session, vous êtes bloqué avec

un PC qui ne se lancera pas. La seule solution consiste alors à formater pour tout effacer. Heureusement, il y a Offline NT Password & Registry Editor. Il s'agit d'un logiciel permettant de réinitialiser le mot de passe des comptes utilisateurs de tous les Windows depuis XP. Nul besoin de connaître l'ancien mot de passe pour en définir un nouveau. Il suffit de graver l'image sur un disque (ou de le placer sur une clé USB) puis de «booter» dessus pour afficher l'interface.

RÉCUPÉRER LE MOT DE PASSE WINDOWS

PRATIQUE



Fonctionne sur toutes les versions de Windows, y compris la version 8.1



Un logiciel à l'interface un peu austère

01 > LE CD DE BOOT

Dézippez le fichier ZIP pour extraire le fichier ISO. Il s'agit d'une image de CD que vous pouvez graver avec n'importe quel logiciel de gravure comme CDBurnerXP (option **Graver une image ISO** au démarrage). Une fois que le disque est prêt, laissez-le dans le lecteur et redémarrez Windows.





MOTS DE PASSE

Windows

02 > BOOT SUR LE CD OU LA CLÉ USB

Si le programme ne se lance pas au démarrage du PC, c'est que l'ordre du boot n'est pas le bon. Faites **Suppr** ou **F1** (en fonction de votre carte mère) juste après avoir allumé le PC et entrez dans le BIOS (**Setup**). Trouvez l'option **Boot Sequence** et modifiez l'ordre en mettant en premier votre lecteur de CD/DVD.



03 > LE DÉMARRAGE

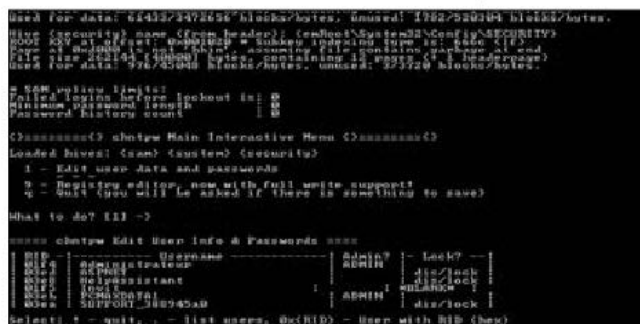
Lors du démarrage du logiciel, validez en tapant sur **Entrée**. Sélectionnez la version de boot. Laissez le choix **1** pour sélectionner la partition détec-



tée. Validez avec la touche **Entrée** du clavier. Laissez le choix du chemin du dossier de registre de Windows. Laissez le choix **1** pour changer le mot de passe et laissez encore le choix **1** pour éditer le compte.

04 > FAITES VOS COMPTES...

Laissez le compte **Administrateur** par défaut et validez encore. Il est bien sûr possible de



sélectionner d'autres comptes. Certains comptes peuvent être désactivés (**Dis**) ou verrouillés (**Lock**). Vous pourrez les réactiver ou les déverrouiller depuis cette interface.

05 > RÉINITIALISATION OU CHANGEMENT

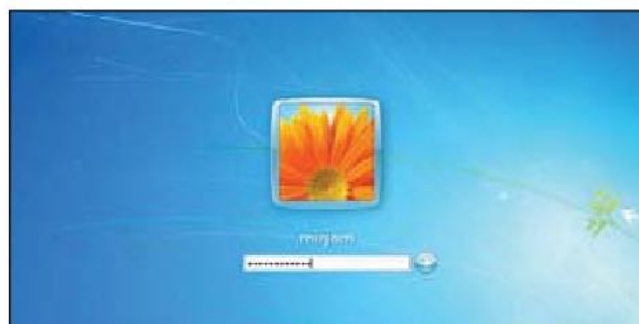
Tapez **1** (clavier numérique) pour réinitialiser le mot de passe et validez encore une fois. Vous pouvez



aussi ajouter un nouveau mot de passe avec l'option **2** (attention au type de clavier), faire en sorte de mettre un compte en administrateur (option **3**) ou activer un compte verrouillé (option **4**).

06 > RETOUR À WINDOWS!

Tapez **!** pour quitter (sur un clavier AZERTY, faites **Maj + &**) et validez. Tapez **Q** pour quitter (**A** sur un clavier AZERTY) et **Y** pour valider les changements. Lorsque l'on vous demande **New run?**, faites **N** et redémarrez la machine en faisant **Ctrl + Alt + Suppr** (sans oublier de retirer le CD. Vous pouvez maintenant entrer dans Windows en laissant le mot de passe en blanc!



CRYPTAGE



49

AXCRYPT : un chiffrement simple et rapide

52

Cryptez le contenu de votre cloud avec **CRYPTSYNC**

55

TrueCrypt est mort, vive **VERACRYPT** !



CHIFFREZ FACILE AVEC AXCRYPT



A lors que certains logiciels proposent tout un arsenal pour chiffrer vos données sensibles (création de conteneurs cachés, sauvegarde incrémentielle compactée, etc.), AxCrypt va au plus simple. Le logiciel ne comporte même pas d'interface graphique, toutes les fonctionnalités sont accessibles via le menu contextuel du clic droit. En effet, lors de l'installation, AxCrypt aura ajouté quelques entrées dans ce dernier. Il suffit de pointer un dossier ou un fichier puis de faire un clic droit pour voir apparaître : **Crypter**, **Crypter et créer** un exécutable et **Brouiller et supprimer**.

AES 128 BITS C'EST ASSEZ ? OUI DIT LA BALEINE !

La deuxième option permet d'envoyer un document à une personne qui ne possède pas le logiciel tandis que la troisième va effacer toute trace du fichier/dossier cible en réécrivant des données aléatoires à son emplacement d'origine. Notez que l'algorithme d'AxCrypt est de l'AES 128 d'où la nécessité de se choisir un mot de passe correct pour éviter le «brute force». Cet algo est suffisamment costaud pour protéger vos données en local, mais est un peu léger si vous voulez chiffrer des documents professionnels en ligne par exemple (eh oui, la NSA est là !). Pourquoi ne pas utiliser AxCrypt en seconde passe alors ?

LORSQUE L'ON PARLE DE CHIFFRAGE, ON PENSE TOUT DE SUITE À TRUECRYPT MAIS CE DERNIER N'EST PLUS SUR (VOIR PAGE 55).

IL EXISTE DES ALTERNATIVES, MAIS LES NOTIONS DE PARTITIONS OU DE CONTENEURS CHIFFRÉS SONT UN PEU COMPLEXES À COMPRENDRE POUR UN DÉBUTANT. POUR FAIRE SIMPLE ET RAPIDE, VOICI AXCRIPT.

UNE VERSION PORTABLE ?

Vous voulez utiliser AxCrypt sur un ordinateur qui n'est pas à vous ? Impossible de l'installer, car vous n'êtes pas Administrateur ? Pour vous, il existe AxCrypt2Go, une version «portable» du logiciel qui permet de profiter de ses fonctionnalités depuis une clé USB ou un disque dur externe. Attention de ne pas mettre le fichier clé sur le même périphérique, car si ce dernier tombe entre de mauvaises mains...



La manière la plus simple pour chiffrer vos fichiers sensibles



Moins puissant que VeraCrypt (page 55) et moins de choix au niveau des paramètres



LES FONCTIONNALITÉS DE AXCRIPT

PRATIQUE



01 > DEHORS LA BARRE!

Lors de l'installation, AxCrypt va vous demander d'installer une barre d'outils de chez

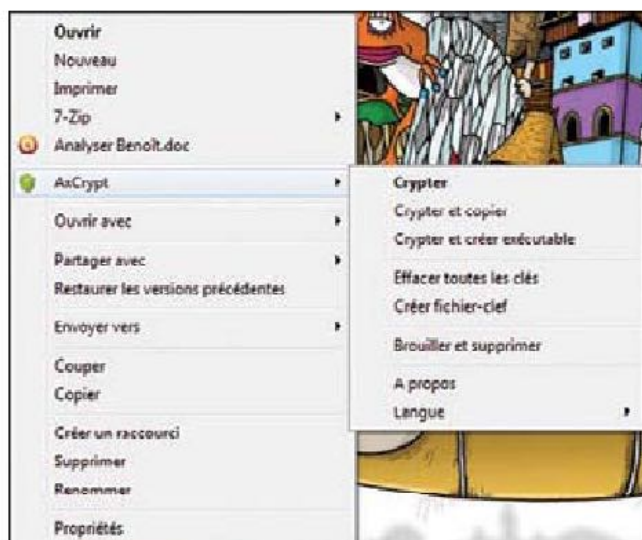


Softonic. Pour éviter d'avoir à la désinstaller plus tard, choisissez **Personnalisé** et décochez **Télécharger et installer**

Softonic Websearch Toolbar. Après l'installation, décochez aussi la case **Register** pour éviter d'envoyer les rapports d'erreur.

02 > LES OPTIONS PRINCIPALES

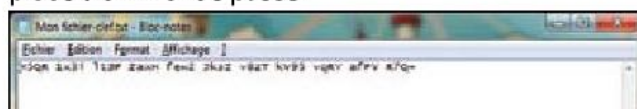
Comme nous l'avons vu, le logiciel est «invisible», il ne comporte pas d'interface ou de bouton. Pour chiffrer un document, un dossier ou un groupe de fichiers, il faudra le/les sélectionner et faire un clic droit dessus. Trouvez ensuite le menu **AxCrypt** et choisissez votre fonctionnalité. **Crypter** va simplement chiffrer la sélection (voir étape4), **Crypter et créer un exécutable** va permettre d'envoyer votre document/dossier sous forme de fichier **EXE**. De cette manière, votre



correspondant n'aura pas à installer AxCrypt pour déchiffrer votre document.

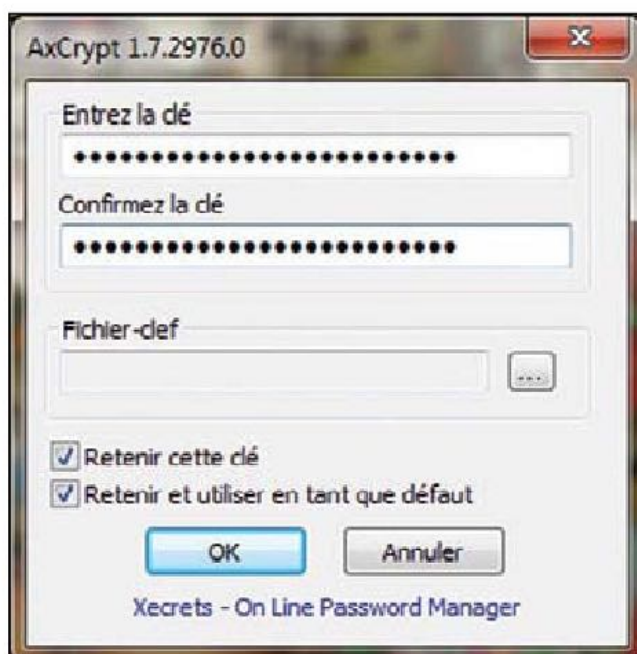
03 > LES OPTIONS COMPLÉMENTAIRES

Effacer toutes les clés va effacer du cache le ou les mots de passe que vous aurez utilisés. Attention, si vous cliquez sur cette option, assurez-vous d'avoir les sésames en têtes! **Créer un fichier clé** vous permettra de déchiffrer vos documents en utilisant, non pas un mot de passe, mais un fichier de décodage que vous pourrez mettre sur une clé USB. Une fois créé, ce dernier pourra être utilisé en lieu et place d'un mot de passe.



04 > CHIFFREZ!

Commençons par faire un clic droit dans un fichier et faire **AxCrypt > Crypter**. Vous pourrez soit entrer un mot de passe (puis une seconde fois pour confirmation) ou utiliser le fichier-clé





CRYPTAGE

Simple et rapide

que vous aurez déjà créé auparavant. Il s'agit d'un simple fichier **TXT** avec des caractères aléatoires à l'intérieur. Si vous cochez **Retenir cette clé**, vous n'aurez pas à entrer à nouveau le mot de passe. L'autre option permet d'utiliser le même sésame ou le même fichier-clé à chaque fois.

pouvez brouiller un peu plus les pistes en faisant **AxCrypt > Retitrer** pour renommer le fichier avec des caractères aléatoires. Pour retrouver votre fichier d'origine, faites un clic droit puis **AxCrypt > Decrypter**. Tapez votre mot de passe ou pointez vers le fichier-clé.

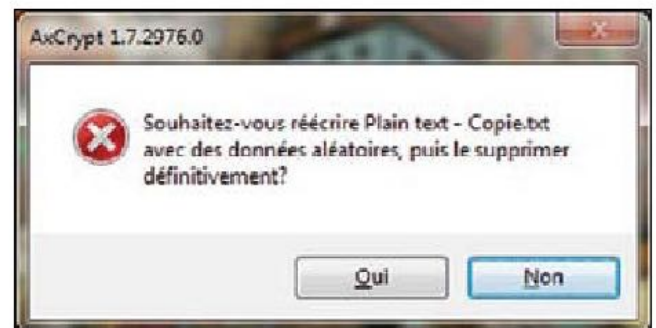
05 > DÉCHIFFREZ!

Après avoir validé, votre fichier prendra une extension **AXX** et changera d'icône. Vous



06 > ENTERREZ UN FICHIER!

Enfin, pour effacer un fichier complètement et éviter qu'une personne ne le retrouve sur votre disque dur (car même effacé, les fichiers peuvent être ressuscité), faites **AxCrypt > Brouiller et supprimer**. Cela restera

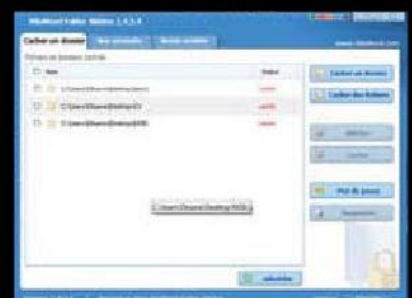


moins efficace que l'option «Peter Gutman» de R-Wipe & Clean (voir *Pirate Informatique* n°19), mais votre fichier sera enterré pour le commun des mortels!

POURQUOI CRYPTER QUAND ON PEUT CACHER ?

Vous avez des fichiers ou des dossiers dans votre disque dur ou sur votre bureau que vous ne voulez partager avec personne ? Qu'il s'agisse de votre comptabilité, de vos photos coquines ou de votre projet ultra-secret de domination du Monde, vous ne voulez pas qu'on puisse les trouver. WinMend Folder Hidden est fait pour vous ! Gratuit et peu gourmand en ressource, ce logiciel permet de dissimuler des fichiers ou des dossiers le plus simplement du monde. Il suffit de l'installer, de définir un mot de passe et de choisir quels éléments seront cachés à l'écran ou pas. Les fichiers cachés sont ensuite totalement invisibles dans l'explorateur de fichiers de Windows et les applications. Pour les faire apparaître à nouveau, il faut repasser par l'interface du programme et changer leur statut.

Lien : www.winmend.com





INFOS [CRYPTSYNC]

Où le trouver ? [<http://code.google.com/p/cryptsync>]

Difficulté : ☠☠☠

CryptSync : SÉCURISEZ VOTRE «CLOUD»

VOUS AVEZ NATURELLEMENT
SUCCOMBÉ À LA MODE DES
SERVICES DE STOCKAGE EN
LIGNE. DIFFICILE EN EFFET
DE RÉSISTER À 5, 7 OU
18 Go D'ESPACE GRATUIT
POUR Y PLACER CE QUE
VOUS VOULEZ. DE NATURE
PRUDENTE, VOUS ÉVITEZ DE
METTRE DES FICHIERS TROP
SENSIBLES DE PEUR DE VOUS
FAIRE PIRATER. POURTANT,
GRÂCE À CRYPTSYNC, VOUS
ALLEZ POUVOIR CHIFFRER
TOUT CE QUE VOUS PLACEZ
SUR CES SERVEURS SANS
VOUS PRENDRE LA TÊTE...



Cryptez vos
fichiers et
expédiez-les dans
le «cloud» en un
seul clic !



Le décryptage
demande
un logiciel
supplémentaire

Rien de plus pratique que
ces services gratuits
proposant de l'espace où
stocker tout et n'importe
quoi. De votre domicile, en voyage
ou au travail, vous avez accès
à vos fichiers qu'il s'agisse de
multimédia, de photo ou de texte.
Le problème, c'est qu'à part votre
mot de passe, rien n'est sécurisé.

Les noms de fichiers et leur contenu
apparaissent «en clair». On
imagine mal Google ou Microsoft
vous espionner (quoique...), mais
ces grosses compagnies ne sont
pas à l'abri d'un vol de données
informatiques et vous n'êtes pas
non plus à l'abri d'un piratage. Sans
compter les mauvaises habitudes
des services secrets...



CRYPTAGE

Chiffrement

LE CHIFFREMENT : INDISPENSABLE POUR PROTÉGER VOS DONNÉES

La solution consiste alors à chiffrer les données avant de les envoyer sur ces serveurs distants, mais le processus pourra décourager les adeptes du «tout, tout de suite». Pour chiffrer vos fichiers automatiquement et les envoyer «dans le cloud» en un seul clic, nous vous proposons de découvrir CryptSync. Compatible avec tous les services de type Dropbox (avec un répertoire en local sur votre PC), ce

programme va chiffrer tout ce que vous lui présenterez pour le placer directement dans votre espace de stockage. En cas d'indisponibilité, de maintenance ou de vols de données, vous aurez toujours un exemplaire de vos fichiers quelque part.



LA SOLUTION CONSISTE
ALORS À CHIFFRER LES
DONNÉES AVANT DE
LES ENVOYER SUR CES
SERVEURS DISTANTS

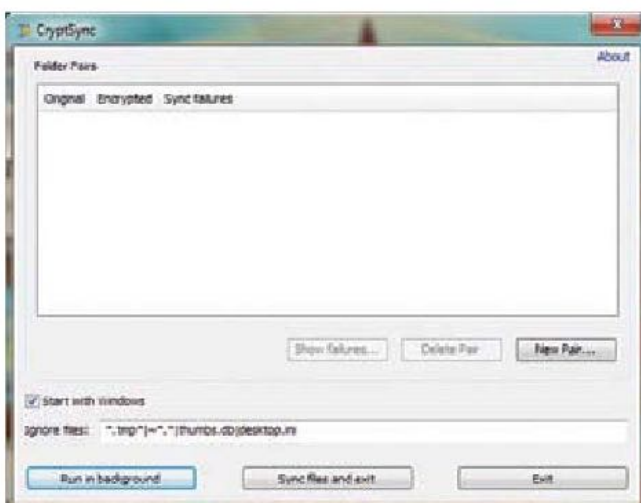
ENVOYEZ DES FICHIERS CHIFFRÉS «DANS LE CLOUD» !

PRATIQUE



01 > L'INSTALLATION

Dans la partie **Download** de notre lien, choisissez la version de CryptSync qui correspond à votre configuration: 32 ou 64bits. Pour être sûr de vous, faites un clic droit dans **Ordinateur** puis



Propriétés et enfin **Type du système**. L'installation ne pose aucun problème particulier. À la fin, cochez **Launch CryptSync** et cliquez sur **Finish**. L'interface graphique va alors s'afficher. Il est possible de cocher **Start with Windows** pour démarrer le programme en même temps que système.

02 > UN COMPTE AVEC UN DOSSIER LOCAL

Notons que pour utiliser CryptSync, il faudra non seulement avoir un compte chez un fournisseur d'espace de stockage, mais aussi télécharger le programme PC permettant de placer ses fichiers directement dans un répertoire. Par exemple pour Google Drive, il faudra se connecter à son compte et faire **Télécharger Google Drive pour PC**. Pour Dropbox, télécharger **Dropbox** depuis la page de connexion et pareil pour SkyDrive. L'accès à l'interface Web ne suffit pas.



Drive

CRÉER



Mon Drive

Partagés avec moi

Suivis

Récents

Plus ▾

Télécharger Google Drive
pour PC



Télécharger Skydrive
pour Windows 7, gratuit

Des applications SkyDrive existent aussi pour Windows 8,
Mac OS X, iPhone/iPad, Windows Phone et Android*

Pourquoi



03 > LA BONNE PAIRE

Commençons par cliquer sur **New Pair...** pour créer notre duo de dossier, l'un contenant des fichiers «normaux» en local et l'autre contenant les mêmes fichiers, mais chiffrés cette fois. Dans la première ligne, mettez le chemin d'accès à votre dossier

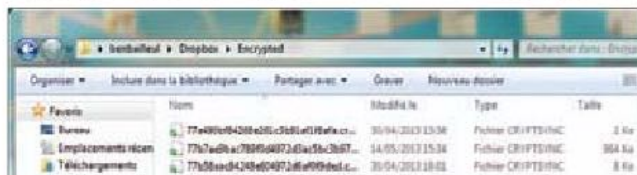


local où vous placerez votre fichier non chiffré. Pour ce faire, nous avons créé un dossier appelé **Local** sur le bureau. Sur la deuxième ligne, tapez ou collez le chemin d'accès vers le dossier où seront stockés les fichiers chiffrés: par exemple **C:\Users\[nom d'utilisateur]\Google Drive** ou **C:\Users\[nom d'utilisateur]\Dropbox**. Si vous ne voulez pas uniquement mettre des fichiers chiffrés, créez un dossier **Encrypted** sur votre espace.

04 > CHIFFREMENT, UPLOAD ET SYNCHRONISATION

Spécifiez un mot de passe et cochez les deux premières cases si vous voulez chiffrer les noms de fichiers et synchroniser automatiquement **Local** avec **Encrypted** (si ce sont les noms que vous avez choisis). La troisième case permet de directement déchiffrer les fichiers avec votre mot de passe depuis l'interface de 7Zip ou WinRAR: pratique. Vous n'avez plus qu'à placer

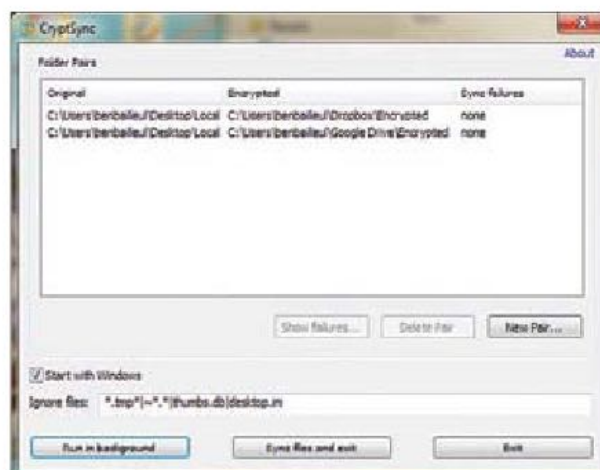
les fichiers que vous voulez chiffrer et envoyer dans **Local** et cliquer sur **Sync files and exit**. Vous pouvez



aussi faire **Run in background** pour que le logiciel travaille en arrière plan et synchronise les fichiers à la volée..

05 > ET POURQUOI PAS DEUX PAIRES?

Vous pourrez voir vos fichiers chiffrés dans votre dossier **Encrypted** en ligne. Une fois que cette paire a été créée pourquoi ne pas cumuler les sécurités? Si vous avez par exemple un compte Dropbox et un autre compte Google Drive, il suffit de les appairer pour que vos fichiers soient placés chez l'un et chez l'autre. Faites une nouvelle fois **New Pair...**, gardez le chemin vers **Local** et mettez votre deuxième répertoire chiffré sur la ligne suivante. Pour déchiffrer vos fichiers, il faudra utiliser 7Zip, par exemple...



LA CLÉ USB «PENSE-BÊTE»

Si vous n'avez pas envie de retenir votre mot de passe, il est possible de créer une clé USB qui fera office de «pense-bête» si vous oubliez votre mot de passe Windows. Dans le champ **Rechercher** du menu **Démarrer** de Windows, tapez **mot de passe** et sélectionnez **Modifier votre mot de passe Windows**. Sur la nouvelle fenêtre cliquez à gauche dans **Créer un disque de réinitialisation de mot de passe** en ayant pris soin de placer une clé USB. Faites deux fois **Suivant**, tapez votre mot de passe et laissez Windows opérer. Un fichier PSW sera présent sur votre support amovible. Mettez cette clé en lieu sûr...



TRUECRYPT EST MORT, VIVE VeraCrypt



Mais que se passe-t-il chez TrueCrypt ? Ce logiciel de chiffrement gratuit et open source n'est plus disponible au moment où nous rédigeons ces lignes. Le 31 mai dernier, le site a été remplacé par une page Web expliquant que le programme n'est plus sûr. Le plus bizarre dans cette histoire c'est que l'équipe en charge du développement conseille aux utilisateurs de se rabattre sur BitLocker, une immondice de chez Microsoft qui comporte potentiellement des backdoors...

RESTER À LA VERSION 7.1A OU OPTER POUR UN AUTRE LOGICIEL

On peut se poser alors plusieurs questions sur ce surprenant épisode. Un hack du site ? Impossible, car la page a été signée numériquement avec les clés des auteurs. Vrai problème au niveau

du programme ? Improbable, car la communauté est telle qu'il aurait été facile de patcher la faille. La seule explication qui semble possible réside dans une clause très spécifique du Patriot Act (une loi américaine antiterroriste, mais également liberticide) qui interdit à des tiers de parler d'une assignation. En d'autres termes il est possible que les développeurs de TrueCrypt aient été approchés par une agence gouvernementale pour interdire ou saboter le logiciel. Devant cette menace et ne pouvant le dire clairement sous peine de finir en prison, les développeurs ont alors imaginé une mise en garde sous forme de blague : « N'utilisez plus Truecrypt mais plutôt cette bouse de Microsoft, de toute façon ce sera bientôt la même chose ». Inquiétant non ? Heureusement d'autres équipes veulent reprendre le flambeau et il existe des alternatives...

NOUS AVIONS PRÉVU DE FAIRE UN RÉCAPITULATIF DES FONCTIONNALITÉS DE TRUECRYPT DANS CES QUELQUES PAGES, MAIS MALHEUREUSEMENT L'ACTUALITÉ NOUS A RATRAPÉS. TRUECRYPT N'EST PLUS SÛR ET CE SONT SES DÉVELOPPEURS QUI LE DISENT. RETOUR SUR UNE HISTOIRE SURPRENANTE...



Plus résistant aux attaques « brute force » que son prédécesseur



Pas compatible avec les conteneurs de TrueCrypt



INFOS [VERACRYPT]

Où le trouver ? [<http://sourceforge.net/projects/veracrypt>]

Difficulté :

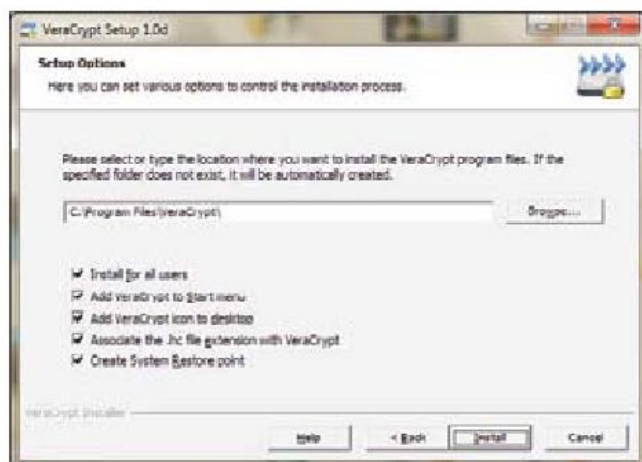
FONCTIONNEMENT DE VERACRYPT

PRATIQUE



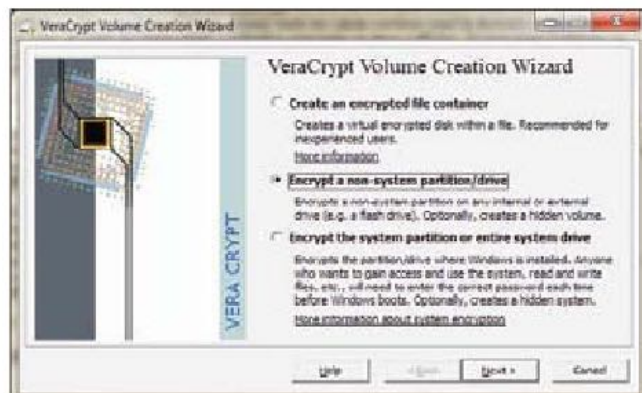
01 > L'INSTALLATION

Lors de l'installation, choisissez **Install** au lieu de **Extract**. Cette deuxième option permet de placer les fichiers nécessaires à l'exécution de TrueCrypt sur une clé USB pour l'utiliser chez un ami en mode «portable». Dans les **Setup Options**, laissez toutes les cases cochées (sauf la dernière si vous ne souhaitez pas créer de point de restauration). La fenêtre principale va alors s'afficher. Si vous avez l'habitude de TrueCrypt, vous ne serez pas dépaycé. Notez que vous pouvez changer la langue en allant dans **Settings > Langages...**



02 > LES TROIS OPTIONS

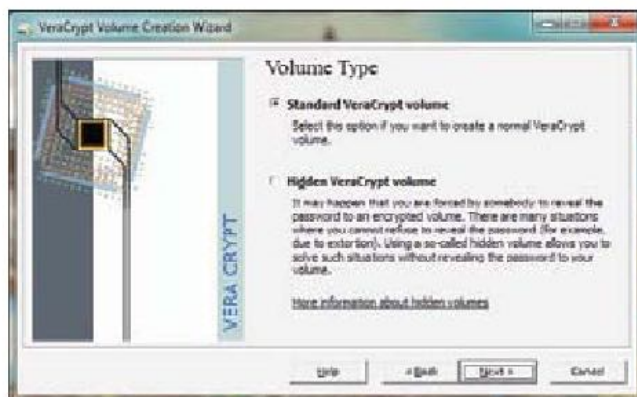
Dans la fenêtre principale du logiciel, cliquez sur **Create Volume**. Vous aurez, ici, trois options. La première consiste à créer un



volume chiffré dans un fichier. La deuxième permet de chiffrer toute une clé USB ou disque dur externe non-système (ne contenant pas Windows). La dernière permet de chiffrer tout le disque dur principal (contenant Windows). Avec cette option, il est même possible de créer un système caché.

03 > VOLUME STANDARD OU CACHÉ?

Nous choisissons la deuxième option pour chiffrer complètement une clé USB, par exemple. Après validation, le logiciel demande si nous souhaitons créer un volume chiffré standard ou un volume caché (pour utiliser le



«dénier plausible» en cas d'extorsion). Comme nous ne sommes pas du KGB et que notre clé ne contient que des informations non sensibles, nous allons choisir la première option...

04 > CRÉATION DU VOLUME

Sélectionnez ensuite une partition ou un périphérique. Le logiciel vous donne le choix entre créer le volume chiffré et le formater ou chiffrer les données qui sont déjà installées (ne fonctionne qu'en NTFS). Après avoir choisi la première option (plus simple, car notre clé est vide et en FAT32), le logiciel vous demandera quel algorithme vous désirez utiliser. Laissez AES dans le doute, mais



vous pouvez aussi opter pour un chiffrement en cascade avec pas moins de trois algorithmes les uns sur les autres.

05 > LE FORMATAGE

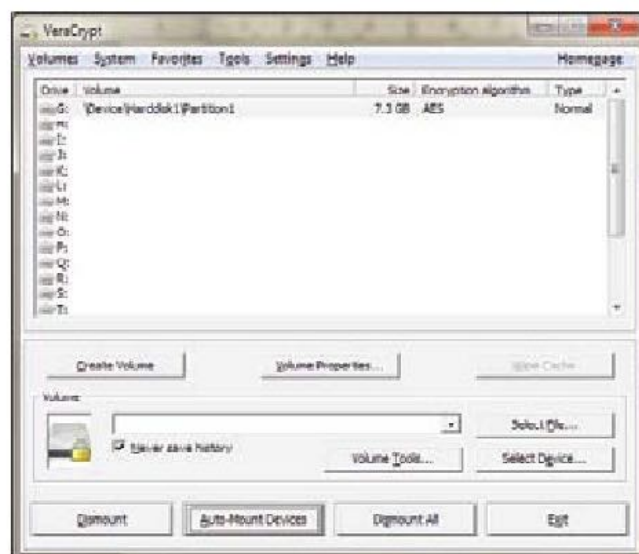
Validez encore deux fois et choisissez votre mot de passe. Il est possible de créer un fichier clé au cas où vous oublieriez votre mot de



passer. Ce dernier peut prendre la forme d'un MP3 ou de n'importe quel autre fichier (son contenu ne sera pas modifié). Après validation, TrueCrypt va vous demander si vous souhaitez mettre des fichiers de plus de 4Go. Dans ce cas, le logiciel choisira automatiquement un formatage NTFS au lieu du classique FAT32. Cliquez sur **Format** après avoir bougé la souris aléatoirement dans la fenêtre pour générer la clé de cryptage.

06 > LE MONTAGE

À la fin du processus (qui peut durer de longues minutes), faites **Exit** et, dans l'interface principale du logiciel, sélectionnez une lettre de lecteur, cliquez sur **Auto-Mount Device** et tapez votre mot de passe. Vous



verrez alors que votre clé USB a changé de lettre (ici G au lieu de F). L'ancienne lettre est toujours présente, mais ne sera plus active. Dans **Ordinateur**, vous avez accès au disque local G après insertion et validation du mot de passe. Mettez-y tous vos fichiers sensibles. Faites **Dismount All** pour les rendre inaccessibles.

POUR OUVRIR LES ANCIENS CONTENEURS

Vous avez des conteneurs chiffrés avec TrueCrypt et vous voudriez bien récupérer leur contenu ? Sous Linux, il existe des logiciels comme RealCrypt ou TcPlay qui sont compatibles avec le format de fichiers de TrueCrypt. Malheureusement il n'existe aucun logiciel de ce type sous Windows à l'heure où nous écrivons ces lignes. La seule solution consiste à récupérer les données «en clair» avec votre ancienne version de TrueCrypt (surtout, ne passez pas à la version 7.2 qui peut être vérolée) pour passer à une solution alternative comme AxCrypt, CypherShed ou VeraCrypt. Rappelons que la version 7.1a de TrueCrypt a récemment été analysée et qu'aucune faille n'a été détectée. Des développeurs suisses ont même commencé à reprendre le flambeau même si pour l'instant il s'agit encore d'un projet : <https://truecrypt.ch/downloads>.



CRYPTEZ VOS FRAPPES AU CLAVIER

// AVEC KEYSCRAMBLER

Nous vous avons parlé plusieurs fois des keyloggers, ces logiciels malveillants qui, une fois installés sur vos PC, vont récupérer tout ce que vous saisissez au clavier: mots de passe, informations bancaires, etc. Même si un antivirus est la meilleure arme contre ces malwares, il arrive que certains passent au travers du filet. Pour lutter contre cette menace, nous vous conseillons KeyScrambler un logiciel qui va crypter toutes les frappes directement au niveau du pilote de votre clavier pour ne le décrypter que dans votre navigateur Web (IE, Firefox ou Flock). Si un pirate essaye de lire vos frappes, il se retrouvera avec du texte inexploitable...



www.qfxsoftware.com



CHIFFREZ FACILE

// AVEC FILEWALL

Si vous avez toujours voulu chiffrer un fichier ou un dossier en un clic sans pour autant passer par de compliqués réglages, FileWall est la solution! Le logiciel s'intègre aux menus contextuels de Windows (via le clic droit) pour proposer le cryptage de l'élément sélectionné en AES 128bits... Après l'installation de FileWall, redémarrez l'ordinateur, faites un clic droit sur un fichier puis choisissez **Firewall>Encryption**. Dans cette nouvelle fenêtre, il suffira de choisir un mot de passe, de le confirmer puis de valider. L'option **Encrypt filename** n'est disponible que pour la version payante (25\$ soit 18,50€). Pour éviter de payer, à vous de vous creuser la tête pour qu'on ne devine pas à quoi correspondent vos fichiers... Validez pour chiffrer votre fichier ou votre dossier. Pour l'ouvrir, faites un clic droit puis **Firewall>Decryption**...



Lien : <http://hummerstudio.com/filewall>



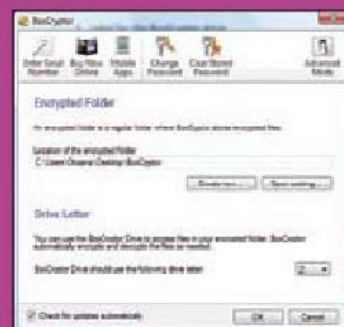
CRYPTEZ «DANS LE COUD»

// AVEC BOXCRYPTOR

Au lieu d'utiliser un conteneur TrueCrypt assez lourd et peu ergonomique, pourquoi ne pas se laisser séduire par BoxCryptor ? Cette application permettant de chiffrer à la volée vos documents et de les envoyer sur les services de stockage à distance Dropbox, Google Drive et SkyDrive. Personne ne pourra vous voler vos précieux fichiers, vous pourrez les récupérer de n'importe quel ordinateur et le service est même disponible pour les possesseurs de smartphones ou de tablettes! Une bonne alternative à CryptSync.



Lien: www.boxcryptor.com



UN COFFRE-FORT NUMÉRIQUE

// AVEC MY LOCKBOX

My Lockbox permet de protéger n'importe quel dossier de Windows avec un mot de passe. À des années-lumière des autres logiciels de ce type, il est doté d'une interface simple. Il suffit de sélectionner votre répertoire depuis l'interface et de spécifier votre sésame. Même après désinstallation (qui est elle-même sécurisée par mot de passe), il sera impossible de retrouver les informations protégées. La version payante ne limite pas le nombre de dossiers que vous pouvez chiffrer. Plus facile que de créer un conteneur TrueCrypt, mais aussi un peu plus limité au niveau des options, c'est une solution idéale pour les débutants.



Lien: <http://fspro.net>





UNE SOLUTION SIMPLE POUR CHIFFRER VOS E-MAILS

// AVEC SECURE GMAIL

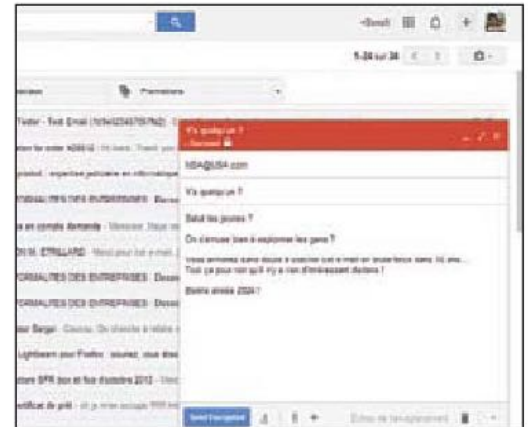
Si vous êtes lecteur de *Pirate Informatique*, vous savez que nous proposons souvent des solutions pour chiffrer vos e-mails. Le problème, c'est que la plupart du temps il s'agit de systèmes assez complexes avec plusieurs logiciels. Ici, il ne vous faudra qu'un compte Gmail et le navigateur Google Chrome. Après avoir téléchargé cette extension, vous verrez un petit cadenas à côté de l'icône **Nouveau message**. Cliquez dessus pour faire apparaître une fenêtre de rédaction. Rédigez votre message et faites **Send Encrypted**.

Choisissez-vous un mot de passe suffisamment compliqué et validez.

À la réception, votre ami devra cliquer sur **Decrypt message with password**. Il faudra bien sûr lui donner le sésame par un autre moyen... Pas besoin d'échanges de clés publiques entre intervenants, SecureGmail utilise la librairie JS crypto de l'université de Stanford. Le code est disponible sur le site... Pas de backdoor en vue!



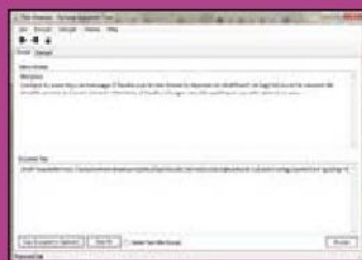
Lien: www.streak.com/securegmail



CRYPTER SES MESSAGES

// AVEC TEXTSHREDDER

Simple comme bonjour, Text Shredder permet de chiffrer des messages. Ne nécessitant aucune installation, le programme va en fait générer une suite alphanumérique depuis le texte que vous aurez tapé. Il suffira alors



d'envoyer ce texte illisible à votre ami (par e-mail ou une messagerie non chiffrée par exemple)

pour qu'il puisse lire le texte avec votre mot de passe. Bien sûr, il faudra trouver une manière sécurisée de lui faire parvenir. Sachez qu'un clavier virtuel qui permet de déjouer les keyloggers, que vous pourrez effacer le texte d'origine automatiquement après le chiffrement (**Encrypt**) et qu'il est possible d'importer ou d'exporter sous forme de fichier texte.



Lien: <https://textshredder.codeplex.com>

EFFACER DES DONNÉES SENSIBLES

// AVEC CCLEANER

Si vous lisez *Pirate Informatique*, vous utilisez peut-être CCleaner pour assainir la base de registre, désinstaller des programmes récalcitrants ou dégager vos cookies, mais vous

ne savez peut-être pas que ce programme permet aussi d'effacer le contenu d'une clé USB ou d'un disque dur externe en écrivant du contenu chiffré. En effet, même après un formatage, le contenu d'un support amovible peut être récupéré par des professionnels. Avant de prêter ou de vendre un disque ou une clé, il est conseillé de réécrire des données aléatoires sur vos propres données. Lancez CCleaner et cliquez sur **Outils** puis **Effaceur de disques**. Sélectionnez l'option **Effacer tout le lecteur** et déroulez la liste pour choisir le nombre de passages. Pour des données très sensibles, vous pouvez aller jusqu'à 35passes! Cochez alors la case devant le lecteur en question puis cliquez sur **Effacer**. Confirmez l'opération en saisissant le mot **ERASE** dans la fenêtre suivante. Attention, l'opération est assez longue même pour 7passes...



Lien: www.piriform.com/ccleaner



Le nouveau site
des utilisateurs
ANDROID



Des dizaines de tutoriels et
dossiers pratiques



Mobiles &
Tablettes :
des tests complets !



Sélection des
meilleures applis
+ des vidéos
et du fun !



Android

Solutions & Astuces

www.android-mt.com

Votre site

100% ANDROID
100% PRATIQUE



ANONYMAT

62

FREEDOM IP : un VPN communautaire français

66

Des proxy à la demande avec **FOXYPROXY**

68

STREALTHY :
soyez furtif sur le Net

71

Un **TOR** encore plus costaud !

74

SOFTETHER :
le VPN du soleil levant



INFOS [FREEDOM-IP]

Où le trouver ? [<http://freedom-ip.com>]

Difficulté :

Freedom IP : LE VPN COMMUNAUTAIRE

ALORS QUE TOUT LE MONDE SAVAIT QU'HADOPI SCRUTAIT NOS PETITES HABITUDES DE TÉLÉCHARGEMENT, LES INTERNUTES ONT DÉCOUVERT QUE LES SERVICES SECRETS LES ESPIONNAIENT. DÈS LORS, LES VPN (VIRTUAL PRIVATE NETWORK) SONT L'UNIQUE MOYEN DE PROTÉGER SA VIE PRIVÉE. SOUVENT PAYANT OU LIMITÉ, NOUS AVONS DÉCOUVERT FREEDOM IP, UN SERVICE COMMUNAUTAIRE GRATUIT.



Service francophone avec une forte communauté, une gratuité totale et sans pub dans le logiciel.



Il faudra montrer patte blanche à l'entrée ! Un peu plus compliqué à mettre en place que d'autres mais plus efficace

Un VPN est un service permettant de passer inaperçu sur le Net. Une fois qu'une connexion à Internet passe par ce réseau privé, tous les échanges de données sont chiffrés et l'ordinateur dispose même d'une nouvelle IP. La plupart de ces services sont payants, car difficiles à mettre en place, nécessitant beaucoup de ressources et des serveurs dans un pays plus clément (pas d'obligation de garder les journaux de connexion, etc.) Nous en avons pourtant trouvé quelques-uns gratuits (comme SecurityKISS que nous vous présentons dans ce numéro) mais limité.

CHOISISSEZ VOTRE PAYS D'ACCUEIL !

À l'inverse, Freedom-IP ne limite pas la quantité de données et propose une vitesse tout à fait honorable. Il propose de surcroît une connexion cryptée par une clé RSA 2048 bits, le top du chiffrement civil. Comme il s'agit du seul service gratuit de ce genre, les nouveaux inscrits se sont bousculés au portillon ces derniers temps. Il faut dire qu'à l'inverse

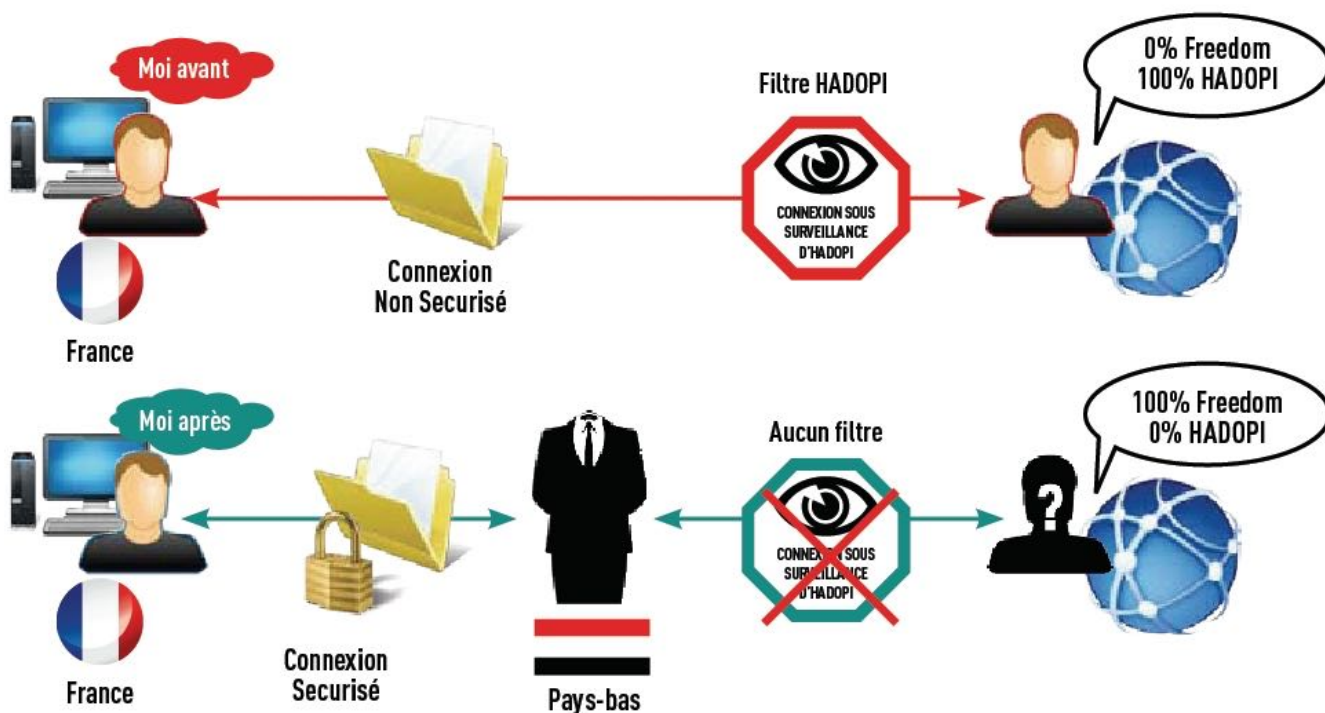


de nombreux VPN payant, l'esprit libertaire et la non recherche de profit constituent la philosophie du service. Devant la recrudescence des nouveaux arrivant, le service a dû revoir son système d'inscription. Le petit nouveau devra, en effet, poser sa candidature en répondant à certaines questions concernant ses motivations ou l'utilisation qu'il compte faire du service. Un parrain pouvant répondre de votre



sérieux ou le fait d'avoir fait un don sont aussi des petits plus... L'infrastructure est basée aux Pays-Bas, mais il est possible de choisir l'Allemagne, l'Espagne, la Pologne ou la République tchèque comme terre d'accueil

pour votre nouvelle IP. Bien sûr, tout cela est légal puisque Freedom-IP est considéré comme un fournisseur d'accès virtuel qui n'a pas de contrôle sur la responsabilité des contenus échangés.



VOTRE CONNEXION AVEC FREEDOM-IP

PRATIQUE



01 > L'INSCRIPTION

Sur le site du VPN, allez dans la rubrique inscription et remplissez les champs en suivant les instructions. Si les inscriptions sont fermées, faites une demande d'invitation ou cherchez un parrain sur le forum. Allez

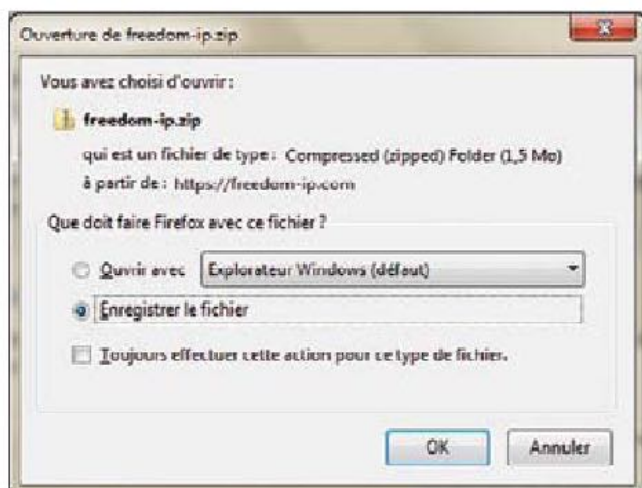


dans **Mon Compte** et téléchargez vos fichiers de configuration lorsque vous aurez été prévenu de votre inscription. Nous allons voir comment Freedom-IP fonctionne avec Windows mais sachez que ce dernier est compatible avec Linux, Mac OS, Android et iOS.



02 > INSTALLATION D'OPENVPN

Freedom-IP fonctionne de concert avec le logiciel OpenVPN (la version 2.2.3 patchée contre la faille heartbleed) qui permet de



configurer un réseau privé virtuel sécurisé. Dernièrement le VPN est aussi compatible avec PPTP. Dans le ZIP, vous trouverez le fichier `openvpn-2.3.3-install-freedom-ip.exe` permettant d'installer ce logiciel en plus de vos fichiers de configuration. Attention, il faudra toujours installer OpenVPN sur votre partition principale et le lancer avec les droits administrateurs (clic droit et **Exécuter en tant qu'administrateur**).

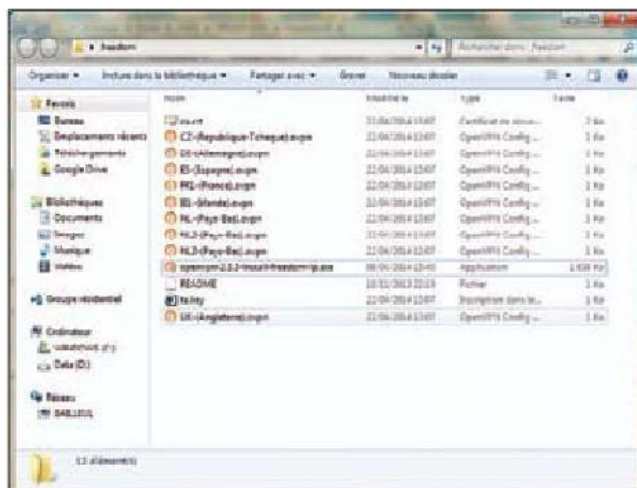
03 > LES FICHIERS DE CONFIGURATION

Après avoir installé OpenVPN, retournez alors dans le ZIP où vous trouverez tous les fichiers suivants:

ca.crt
ca.key
CZ_freedomip.ovpn
PL_freedomip.ovpn
NL_freedomip.ovpn
NL2_freedomip.ovpn
NL_rapide_freedomip.ovpn
ta.key

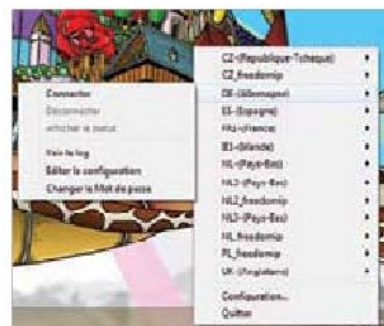
Tous devront être copiés dans le répertoire

C:\Program Files (x86)\Open VPN\Config. Les doublons devront être écrasés.



04 > LA CONNEXION

Connectez-vous au VPN en ouvrant OpenVPN en mode administrateur. En bas près de l'horloge vous aller voir une nouvelle icône. Choisissez votre serveur, cliquez sur **Connect** et entrez les identifiants qui vous ont été communiqués par email. Vous



êtes connecté! L'IP que vous allez voir n'est que la passerelle entre vous et le VPN. Pour être sûr que l'infrastructure fonctionne, allez sur **www.hostip.fr**. Sur le site, vous trouverez d'autres tutos pour exclure certaines IP de la connexion sécurisées (le choix se fait avant le téléchargement de l'archive), choisir ses DNS, etc.



L'INFORMATIQUE FACILE POUR TOUS !



**CHEZ
VOTRE
MARCHAND
DE JOURNAUX**



[FoxyProxy] Où le trouver ? : [http://goo.gl/EUTtC]

[ID Cloak Free Proxy Server List] Où le trouver ? : [http://goo.gl/EUTtC]

Difficulté :

Proxies à la demande... ET EN UN CLIC

VOUS UTILISEZ DES PROXIES, MAIS LES RÉGLAGES MANUELS VOUS FATIGUENT ? FoxyProxy EST UNE EXTENSION SOUS FIREFOX ET CHROME PERMETTANT DE PARAMÉTRER AUTANT DE PROXIES QUE VOUS VOULEZ POUR POUVOIR CHANGER D'IP À VOLONTÉ ET INSTANTANÉMENT. EN UTILISATION CONJOINTE AVEC LA LISTE ID CLOAK, VOUS AUREZ UN GRAND CHOIX DE PROXIES ACTIFS MIS À JOUR ET DÉTAILLÉS.

FoxyProxy est une extension pour Firefox et Chrome qui permet de mémoriser et de jongler entre plusieurs proxies de votre choix et pas d'une liste préétablie. Rappelons que ces serveurs mandataires permettent de faire le tampon entre votre ordinateur et Internet. Il existe des proxies permettant de masquer son IP ou de se protéger des attaques et des curieux. Si vous ne savez pas où trouver des proxies qui valent le détour, le site www.idcloak.com

propose une liste mise à jour des meilleurs serveurs en fonction de leur niveau d'anonymat, de leur vitesse et du protocole utilisé. Rien de mieux pour avoir accès aux sites géolocalisés, outrepasser les restrictions mises en place par une dictature ou rendre la tâche plus difficile aux espions qui sévissent sur le Net... Notez que FoxyProxy se connecte à certains proxies en fonction des sites que vous fréquentez (tel proxy pour tel site ou pas de proxy du tout).



Une interface conviviale et tout en français



Profitez-en avant qu'il ne devienne payant !

Update time	Country	Connection Speed	Speed	Anonymity	Protocol	Port	IP Address
48s	RU			Low	HTTPS	8128	188.128.99.94
47s	CH			Low	HTTP	8084	65.54.104.84
47s	CH			Low	HTTPS	8080	248.22.78.128
53s	VE			Low	HTTPS	8080	200.18.30.70
1min 20s	BR			Medium	HTTP	8080	187.1.10.227
1min 41s	BR			Low	HTTPS	80	201.12.106.98
1min 54s	CH			Low	HTTPS	8080	154.597.87.3
2min 04s	CH			Low	HTTPS	8080	133.6.163.101
2min 20s	CH			High	HTTP	80	211.142.236.133
2min 20s	CH			Medium	HTTP	82	218.108.80.28
2min 50s	BR			Low	HTTPS	8080	88.85.100.18
2min 54s	CH			Low	HTTPS	80	65.552.106.187
4min 31s	CH			Low	HTTP	8080	58.67.147.185
5min 0s	CH			Low	HTTPS	8128	222.188.14.48
5min 0s	CH			Low	HTTPS	8128	212.144.254.123
5min 24s	US			Low	HTTP	83	64.79.85.68
5min 51s	BR			Low	HTTPS	8080	2.184.31.3
6min 30s	CH			High	HTTP	8080	211.142.236.133
7min 54s	RU			Low	HTTP	8080	222.124.11.120
8min 1s	BR			Low	HTTP	8080	194.143.96.1

Sur le site ID Cloak, vous trouvez une liste de proxies longue comme le bras avec moult détail technique : niveau d'anonymat, rapidité, protocole, port de connexion et adresse bien sûr !



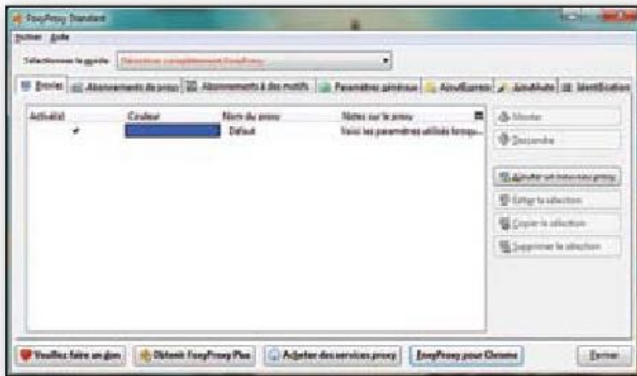
PREMIERS PAS AVEC FOXYPROXY

PRATIQUE



01 > L'INTERFACE

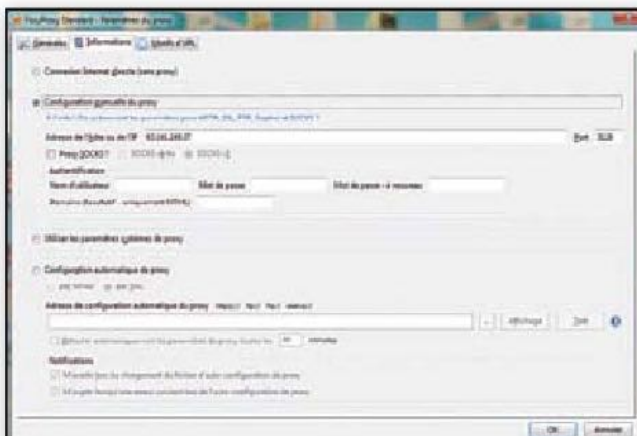
Après avoir installé l'extension, vous verrez alors une nouvelle icône en forme de renard à droite de la barre d'adresse. Celle-ci est barrée, car d'origine, aucun proxy n'est paramétré. Cliquez sur cette icône



pour afficher l'interface de paramétrage. Dans le premier onglet, cliquez sur **Ajouter un nouveau proxy** et entrez le maximum d'informations dans les trois onglets qui vous seront proposés.

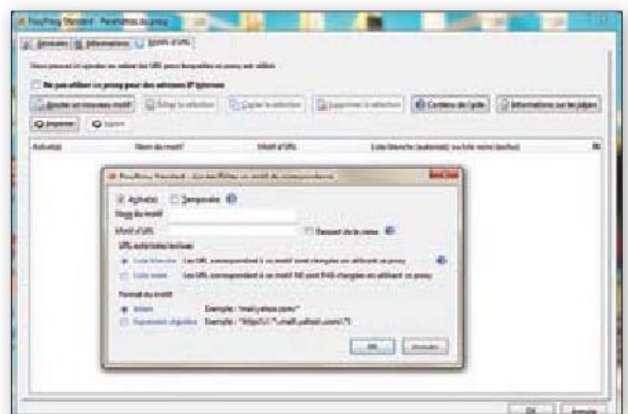
02 > LES RÉGLAGES

Pour avoir accès à ces données, allez sur le site ID Cloak (suivez notre lien). Donnez un nom à votre proxy, un code couleur et choisissez ou non de supprimer les cookies avant de l'utiliser (onglet **Générales**) et mettez le nom de l'hôte et son port de connexion depuis le second onglet (vous trouverez ces informations dans les deux dernières colonnes de la liste ID Cloak). Après avoir validé, votre premier proxy configuré sera sur la fenêtre principale.



03 > TROIS MODES DE FONCTIONNEMENT

Il est temps de l'activer. Tout en haut, à côté de **Sélectionner le mode**, vous aurez le choix entre **Désactiver complètement FoxyProxy**, **Utiliser le proxy «Default» pour toutes les URLs** et **Utiliser**



les proxies basés sur leurs motifs et propriétés prédéfinies. Cette option permettra, par exemple, de se passer de proxy pour certains sites n'en nécessitant pas tout en activant d'autres lorsque vous en aurez besoin (proxy français lorsque vous êtes à l'étranger ou proxy américain pour avoir accès à Pandora par exemple).

04 > LES EXCEPTIONS

Pour régler en amont ce type de configuration, il faudra aller dans l'onglet **Motifs d'URL** après avoir fait **Ajouter un nouveau proxy**. Il est possible de dresser une liste noire (les sites dans cette liste n'utiliseront jamais de proxy) et une liste blanche selon votre utilisation. Le site de stream Hulu sera donc disponible même de France. Nous vous conseillons de faire passer les autres sites sans utiliser de proxy pour éviter les ralentissements.





INFOS [STEALTHY]

Où le trouver ? [<http://goo.gl/4ulpi> (Firefox)] [<http://goo.gl/6xPDG> (Chrome)]

Difficulté :

Stealthy :

SOYEZ FURTIF SUR LE NET



POURQUOI PASSER PAR UN VPN SI VOUS NE TÉLÉCHARGEZ RIEN OU QUE VOUS NE VOUS CONNECTEZ JAMAIS À UN HOTSPOT NON SÉCURISÉ ? LES PROXY PERMETTENT DE MASQUER VOTRE IP LORSQUE VOUS SURFEZ, MAIS ILS SONT SOUVENT DIFFICILES À METTRE EN PLACE POUR LES DÉBUTANTS. AVEC STEALTHY, PLUS DE PROBLÈME...

Stealthy est une extension pour Google Chrome et Firefox qui va vous permettre de masquer votre IP lorsque vous êtes sur Internet. Plus précisément, vous «empruntez» une IP autre que la vôtre : celle de votre proxy. Une fois connecté à ce serveur, les sites de stream ou les services en

ligne qui excluent les internautes en fonction de leur position géographique ne pourront plus le faire puisque pour eux, vous



Le dernier épisode des Simpsons sur le site de la Fox. Sans Stealthy, un message vous avertit que vous devez être résident américain pour en profiter. Avec un proxy basé aux USA, pas de problème...



Très facile à mettre en place



Pas de chiffrement



serez résident américain. Vous pouvez aussi utiliser un proxy pour brouiller les pistes ou éviter le traçage des sites qui vous «flickent».

UN TRAFIC, «RE-ROUTÉ », MAIS PAS CHIFFRÉ

Il est assez fastidieux de saisir «à la main» les coordonnées d'un proxy à chaque fois que vous voulez vous connecter, mais heureusement Stealthy permet de réduire ces opérations à deux

ou trois clics. Après l'installation, il suffit de choisir la destination de votre proxy, de mettre en route l'extension et c'est tout ! Attention, ce type de connexion ne fait pas passer l'ensemble de votre trafic, mais uniquement le HTTP qui permet de surfer ou de télécharger en direct (sans passer par un réseau P2P donc). De même, ils ne chiffrent pas les informations comme avec un VPN, attention donc à ce que vous faites transiter dans les «tuyaux»...



AVEC STEALTHY VOUS CHOISISSEZ VOTRE PAYS DE DOMICILIATION

MISE EN PLACE DE STEALTHY

PRATIQUE



01 > INSTALLATION

Allez sur le lien correspondant à votre navigateur et faites **Ajouter à Firefox**, **Installer maintenant** puis **Redémarrer maintenant** ou **Add to Chrome** et **Ajouter**. Vous serez alors dirigé vers la page de Stealthy. Notez que le site propose un Webproxy

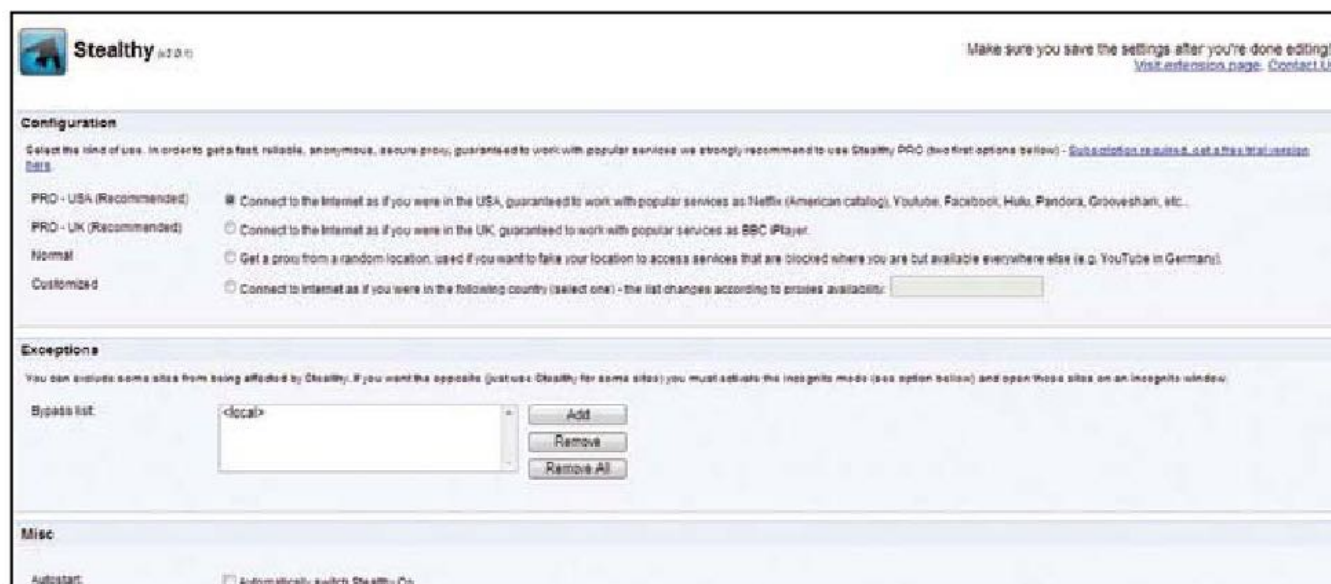


permettant de naviguer anonymement. Néanmoins, ce dernier ne fonctionnera pas avec le stream. De même à certaines heures, vous devrez passer par la version payante de l'extension pour certains proxy.



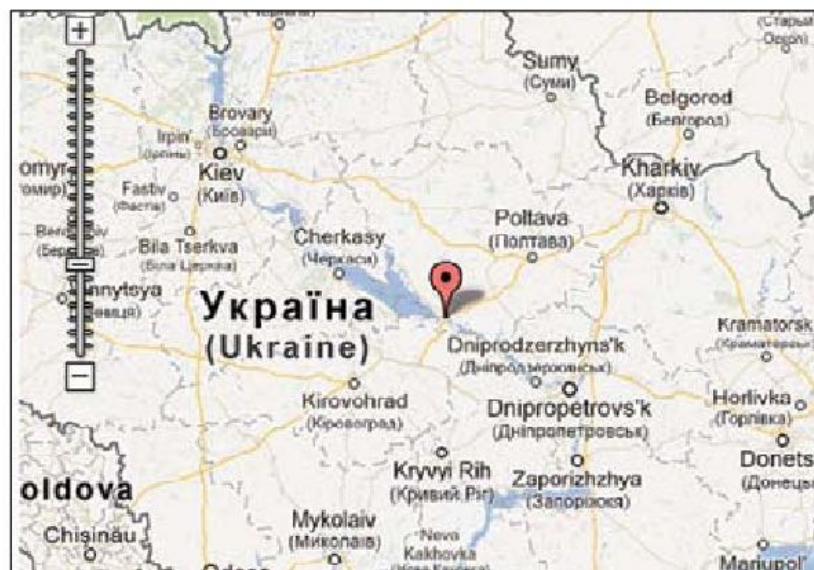
02 > LE CHOIX DU PROXY

Vous aurez alors une nouvelle icône en haut à droite de votre navigateur. Pour les réglages, cliquez dans la petite flèche à droite de l'icône puis faites **Préférences** (pour Firefox) ou cliquez sur l'icône avec les trois barres puis **Outils > Extensions** (dans Chrome). Vous aurez alors le choix de vous connecter à un proxy américain (pour éventuellement vous connecter à des services géolocalisés comme Hulu ou Netflix), un proxy anglais (pour le service de stream de la BBC) ou à un proxy complètement au hasard (si vous êtes au Royaume-Uni et que vous voulez vous connecter à The Pirate Bay, interdit chez les sujets de Sa Majesté).



03 > ACTIVATION

La dernière option permet de vous connecter à un proxy suivant le pays que vous désirez «emprunter». Tapez la première lettre de ce pays et choisissez-le dans la liste. Pour activer les réglages, il suffira de cliquer dans l'icône de Stealthy



en haut à droite pour qu'elle devienne verte. Cela signifiera que vous êtes bien connecté. Vérifiez votre nouvelle «nationalité» en allant sur le site **www.localiser-ip.com**.



Un TOR ENCORE PLUS FORT !



TOR et le gouvernement chinois, c'est une longue histoire de désamour !

Beaucoup plus agressif que de nombreuses autres dictatures, la République Populaire de Chine passe à la vitesse supérieure. Rappelons que TOR est un système permettant d'anonymiser les échanges de données sur Internet. Un dissident chinois pourra donc poster sur un blog ou un forum sans pour autant trahir son emplacement géographique ou son identité.

L'EMPIRE DU MILIEU CONTRE-ATTAQUE !

Bien sûr, le système connaissait des ratés, car il était possible de bloquer les adresses IP des nœuds TOR publics, mais les développeurs trouvaient des parades sous forme de mises à jour pour faire aléatoirement passer le flux de données par d'autres nœuds. Mais récemment, la Chine a trouvé une technique : scanner de grandes plages d'IP «suspectes» en essayant de communiquer avec chaque machine comme s'il s'agissait d'un nœud (public ou privé). Si la machine répondait correctement à la sollicitation, l'IP correspondante était bloquée !

UTILISÉ DANS LE MONDE ENTIER POUR SÉCURISER LES ACCÈS À INTERNET DE PERSONNES SURVEILLÉES PAR LES DICTATURES, TOR A POURTANT CONNU SES PREMIERS DÉBOIRES. LE GOUVERNEMENT CHINOIS A, EN EFFET, TROUVÉ LE MOYEN DE BLOQUER CE SYSTÈME POURTANT BIEN RODÉ. HEUREUSEMENT, *PIRATE INFORMATIQUE* VOUS LIVRE LA PARADE...

LE PETIT MONDE DE TOR

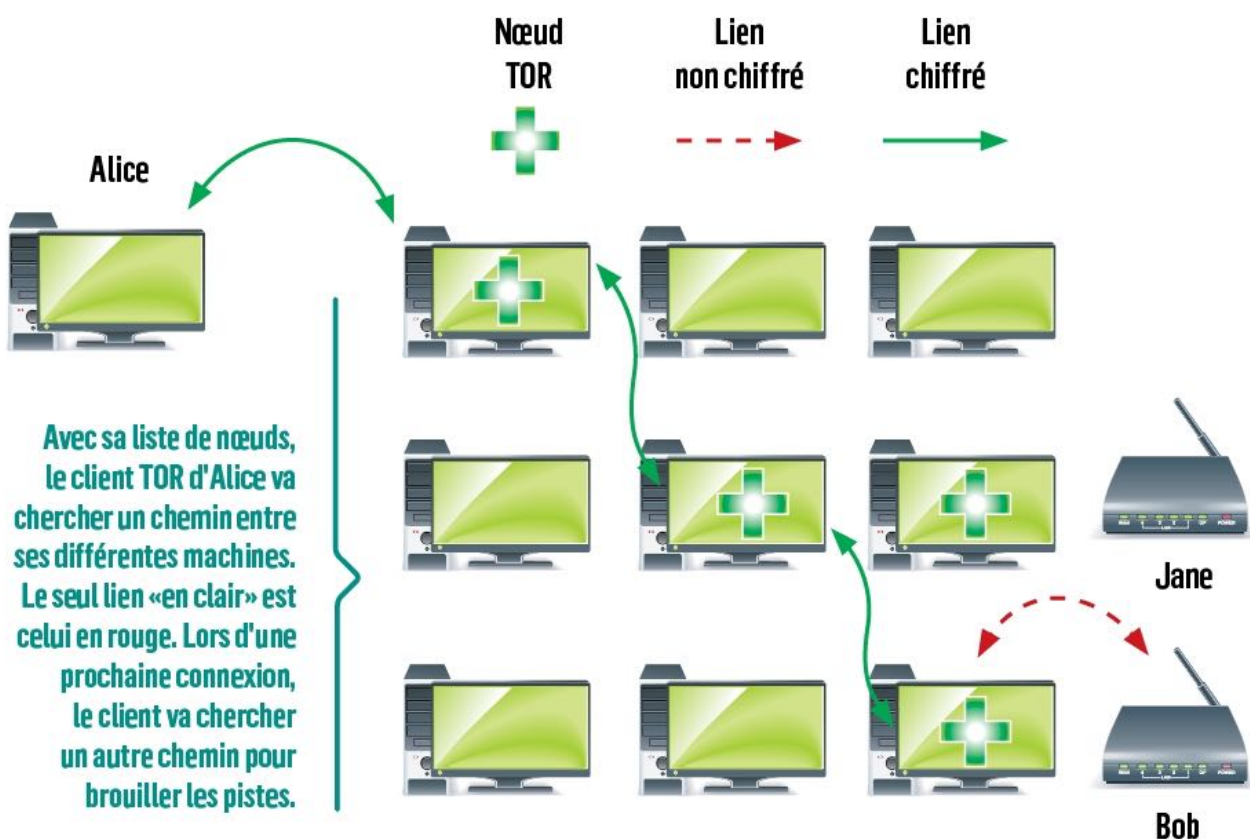
Tor est supporté par une grosse communauté de développeurs qui contribuent à le rendre impénétrable, mais aussi à le doter de divers services annexes. Parmi ces derniers on compte Orbot pour surfer anonyme depuis son smartphone sous Android, Tails qui est un OS 100% anonyme, TorBirdy qui permet de chiffrer ses e-mails sous Thunderbird et Tor2Web qui permet d'avoir un accès (non-anonyme) aux sites Tor depuis un simple navigateur.



Il s'agit du futur de Tor.



Encore en version bêta donc prudence...



CONTOURNEZ LA CENSURE AVEC TOR !

PRATIQUE

01 > LE RÉSEAU

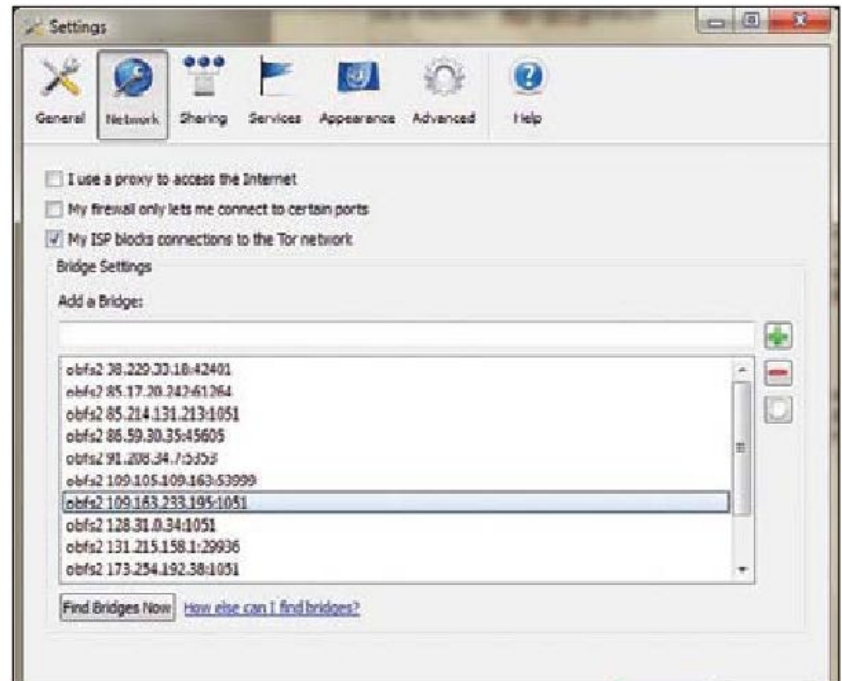
Après avoir téléchargé la version spéciale du **Tor Browser Bundle**, dézippez l'archive et double-cliquez sur **Start Tor Browser**. Notons au passage que cela fonctionne avec n'importe quel navigateur y compris la version portable de Firefox (faites un tour dans le répertoire idoine pour en profiter). Tor va chercher une liste de nœuds publics et chercher un chemin entre les différents éléments pour se connecter au réseau (voir notre schéma). Au bout d'un moment, vous devriez voir **Connected to the Tor network**





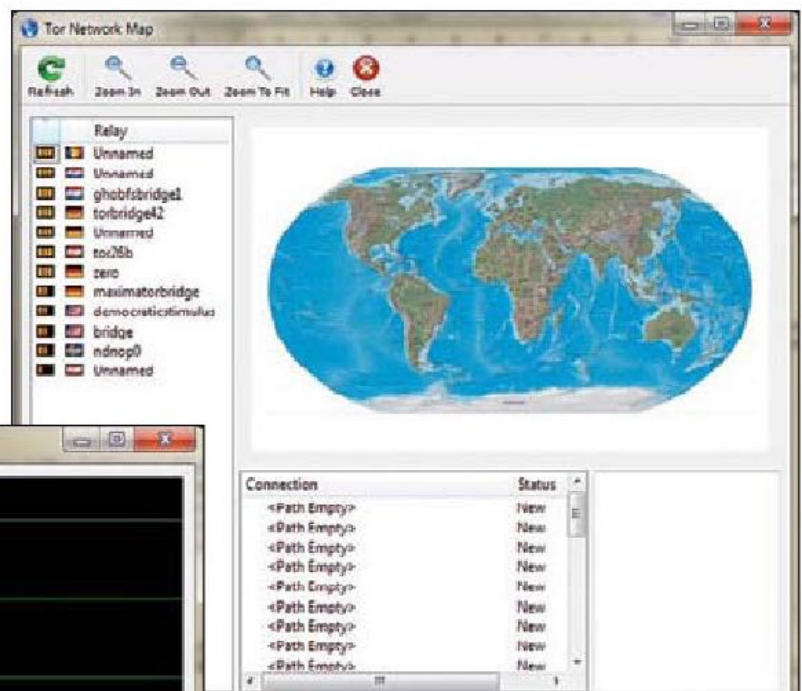
02 > LES PONTS

Dans **Vidalia shortcuts**, vous pourrez arrêter d'utiliser ce réseau (**Stop Tor**) ou **Setup Relaying** pour les options avancées. Dans l'onglet **Network**, vous pourrez ajouter des ponts (bridge) pour masquer le protocole. Pas de panique, vous n'aurez rien à faire au début! Il faudra simplement cliquer sur **Find Briges Now** pour en trouver de nouveaux si vous l'utilisez depuis quelque temps. En effet, certains peuvent devenir inopérants au bout d'un moment. Il est aussi possible d'en rajouter à la main.



03 > LES AUTRES OPTIONS

Notez que pour mieux maîtriser votre nouveau réseau, vous pouvez avoir un aperçu de votre bande passante dans **Bandwith Graph** et une représentation graphique des nœuds emprunté dans **View the Network**. Pour que Tor continue à fonctionner correctement, laissez ouverte la page



Internet qui s'est affichée au démarrage. Elle contient l'IP qui semble être la vôtre sur le réseau externe.



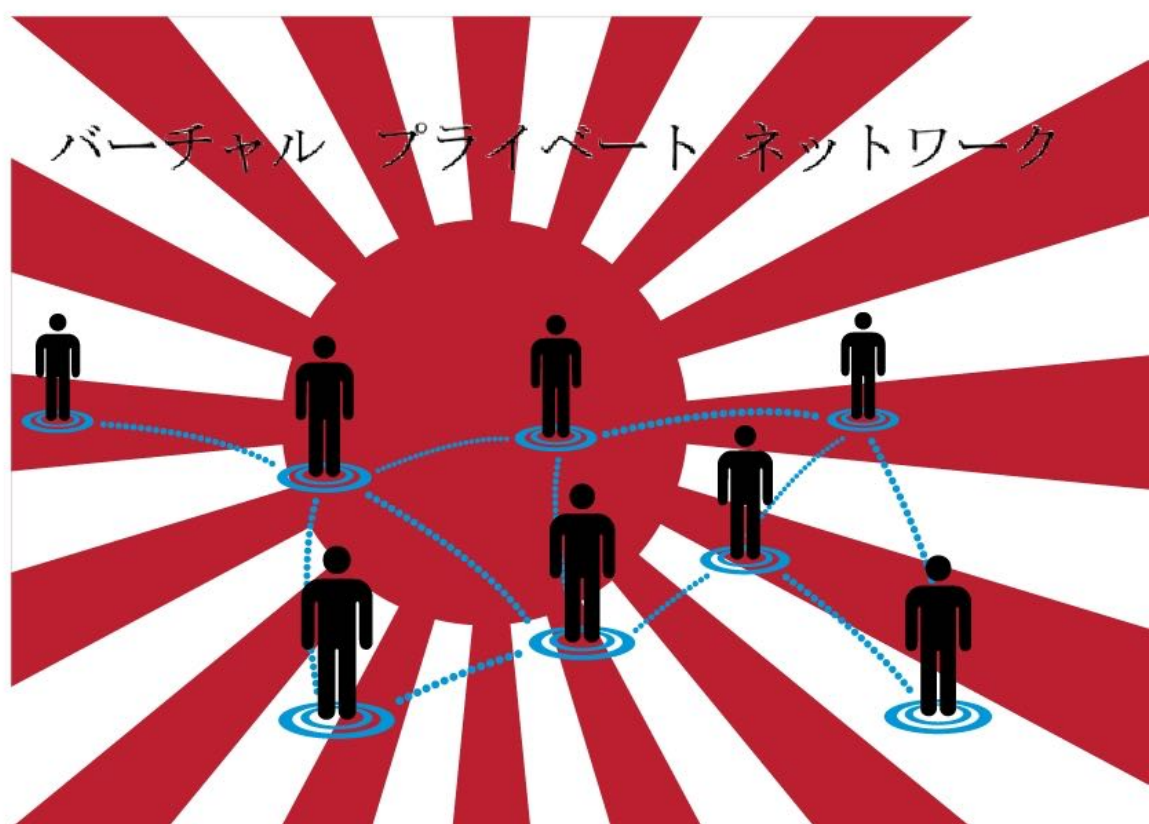
INFOS [SOFTETHER]

Où le trouver ? [<http://goo.gl/8bZB7>]

Difficulté : ☠☠☠

SoftEther : LE VPN DU SOLEIL LEVANT

À PART QUELQUES RARES EXCEPTIONS (COMME NOS AMIS DE FREEDOM-IP), LES VPN SONT DEVENUS DES SERVICES COMMERCIAUX PAYANTS. POUR GARDER UN CERTAIN ANONYMAT SUR INTERNET, IL EXISTE POUTANT DES SOLUTIONS. LE PROJET SOFTEETHER DE L'UNIVERSITÉ DE TSUKUBA AU JAPON PROPOSE UN RÉSEAU DE RELAIS CHIFFRÉS AUXQUELS CHACUN PEUT SE CONNECTER OU PARTICIPER À L'AGRANDISSEMENT...



Un VPN gratuit avec différents relais au quatre coins du monde...



Il faudra tâtonner avant de trouver un relais stable et rapide

Se connecter à un VPN peut devenir vital dans certains pays. C'est en pensant aux citoyens surveillés et brimés en Chine, en Iran ou en Biélorussie que le projet SoftEther a vu le jour. Il s'agit d'un VPN basé sur un réseau de serveur «volontaire».

Un internaute peut s'y connecter avec le logiciel client, mais aussi participer à l'agrandissement du réseau en devenant un serveur relais. Ces derniers ne pouvant pas être filtrés de manière efficace par les gouvernements censeurs proposent donc une «porte de sortie» aux citoyens pour consulter



Internet sans restrictions, mais aussi commenter sur les blogs, forums ou poster sur Twitter, YouTube, etc.

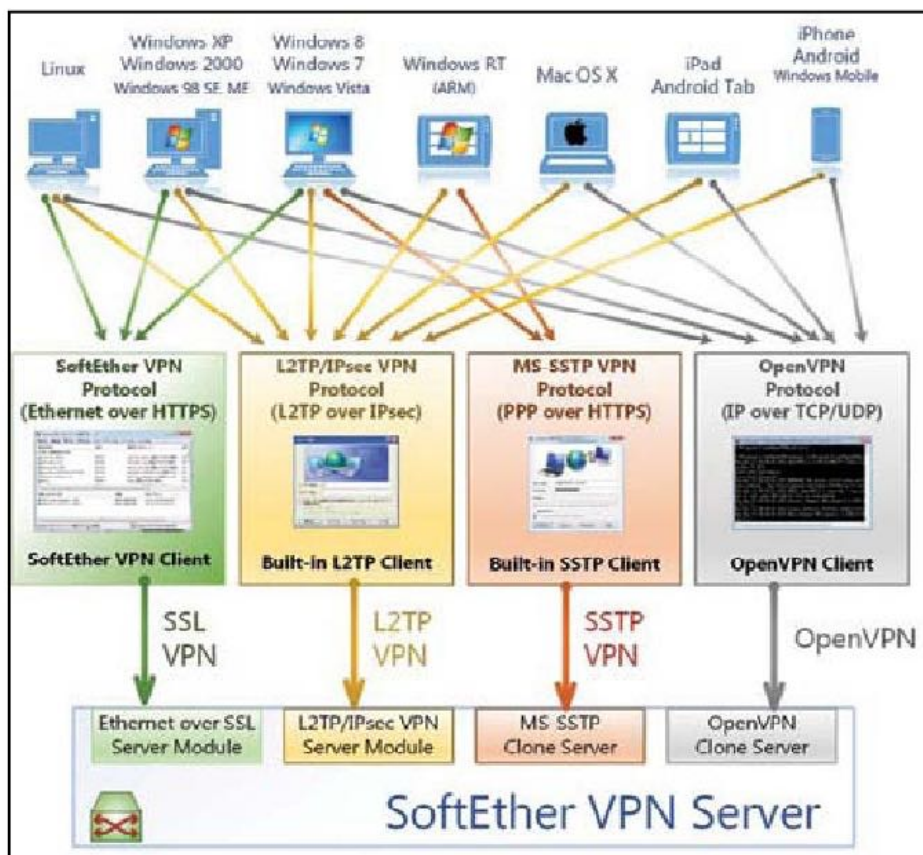
CHIFFRÉ DE BOUT EN BOUT

À l'intérieur de ce réseau, tout est chiffré, mais très simple à employer puisque vous n'aurez pas à toucher à vos réglages de pare-feu grâce au protocole SSL-VPN. En utilisant ce dernier, il est possible de se connecter, de se déconnecter ou de changer de relais en un seul clic sans aller dans les entrailles de Windows pour configurer un à un les serveurs. Pour ceux ayant leurs petites habitudes, pas moins de 6 protocoles sont acceptés (OpenVPN, IPsec, L2TP, MS-SSTP, L2TPv3 and

EtherIP) en plus du SSL-VPN.

ANTI-DICTATURE MAIS PAS QUE...

Sans avoir forcément quelque chose à cacher ou habiter dans un pays qui pratique la censure, vous pouvez vous aussi trouver une utilisation à SoftEther. Il est, par exemple, possible d'avoir accès à des services multimédias géolocalisés, mais aussi de pouvoir sécuriser sa connexion lorsque vous surfer depuis un hotspot inconnu. Pour le téléchargement via P2P ? Cela marche aussi sous certaines conditions... Enfin si vous trouvez votre démarche un peu égoïste, vous pouvez vous aussi faire office de serveur relais pour les autres participants.



Le programme client de SoftEther via SSL-VPN n'est disponible pour l'instant que pour Windows et Linux, mais le mode serveur est aussi ouvert à MacOS X, FreeBSD et Solaris. Notons qu'avec la compatibilité avec le protocole OpenVPN, tous les appareils (y compris sous iOS et Android) peuvent se connecter.



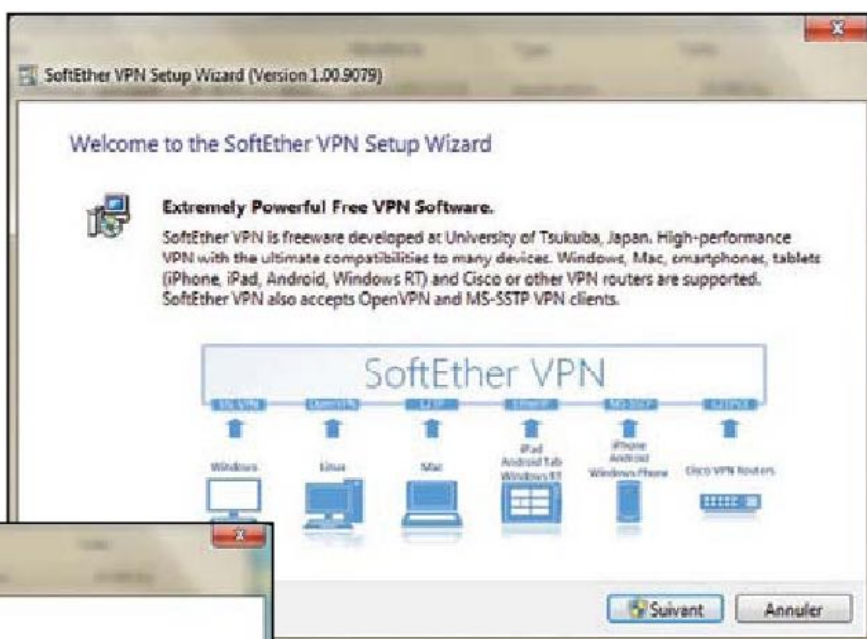
SE CONNECTER AVEC SFTETHER

PRATIQUE



01 > LA BONNE VERSION

Il faudra dans un premier temps télécharger la version de SoftEther qui comprend le plugin VPN Gate (suivez notre lien puis **Download SoftEther VPN Client + VPN Gate Client Plug-in**). VPN Gate est un projet annexe de SoftEther qui va vous permettre de vous connecter et de changer de VPN très



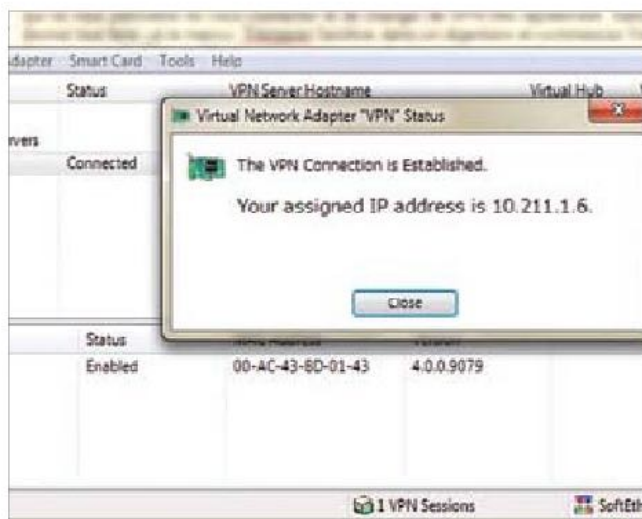
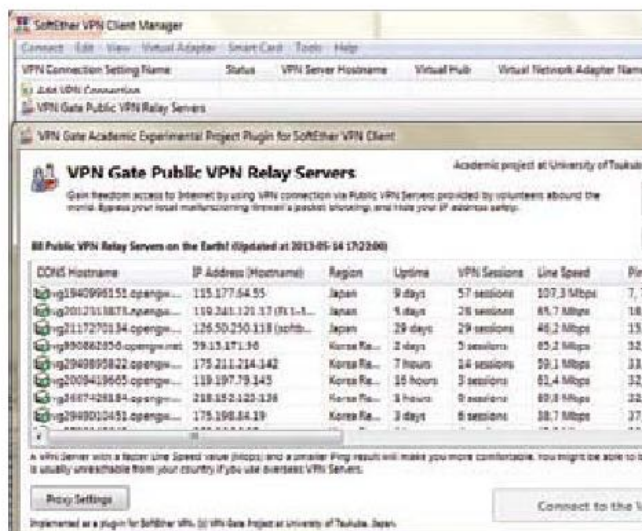
rapidement. Sans ce plugin, vous devrez tout faire «à la main». Dézippez l'archive dans un répertoire et commencez l'installation. Sélectionnez **SoftEther VPN Client** lorsqu'on vous le demandera, acceptez les termes de la licence et cliquez enfin sur **Terminer**. Vous devriez voir l'interface principale du client.





02 > LA LISTE DES SERVEURS «VOLONTAIRES»

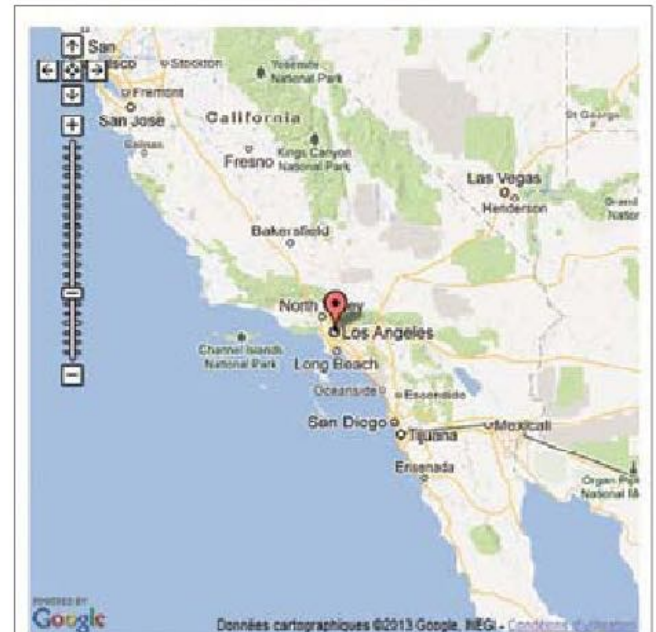
Double-cliquez sur **VPN Gate Public VPN Relay Server** puis faites **OK** pour avoir une liste des serveurs disponible sur le projet VPN Gate. Vous trouverez un descriptif détaillé pour chacun d'eux: pays, ping, transfert cumulé, rapidité, nombre de personnes connectées



et même une note finale pour faire son choix. N'habitant (pas encore) dans une dictature, mais voulant profiter de Hulu pour ses séries, nous allons choisir un VPN aux USA... Double-cliquez sur le serveur de votre choix. Faites **Agree** (après avoir coché **Do Not Show This Message Again**) et vous voici l'heureux propriétaire d'une nouvelle IP!

03 > NOUVELLE IP + ÉCHANGES CRYPTÉS

En faisant un clic droit dans l'icône de la barre de notification, vous pourrez vous connecter automatiquement au démarrage. Si le VPN vous le demande, choisissez toujours l'option **Use TCP Protocol**. À vous les séries sur Hulu ou la



Adresses IP à proximité de 108.252.17.38

possibilité d'avoir un compte Netflix. Et si vous êtes à l'étranger, on trouve aussi des serveurs français... Quant à la sécurisation d'un hotspot public, choisissez le VPN le plus proche et le plus rapide puisque de toute façon les échanges sont chiffrés. En allant sur www.localiser-ip.com, vous pourrez voir graphiquement votre nouvelle demeure virtuelle. Pour vérifier que le VPN masque aussi les échanges P2P, utilisez le site **Check my Torrent IP** que nous vous présentons à la page 79 !



ÉVITEZ LES PANNES DE VPN

// AVEC VPN LIFEGUARD

Passer pas un VPN pour protéger sa connexion c'est bien mais parfois le «réseau privé virtuel» flanche ou se déconnecte. Sans le savoir, vous n'êtes alors plus protégé et aucun outil de Windows ne viendra vous le dire! Il arrive parfois qu'on se rende compte d'une déconnexion de VPN après plusieurs jours (alors même que vous payez pour ce service!). La solution réside dans le logiciel gratuit VPN Lifeguard. Ce dernier doit être lancé en tant qu'administrateur. Dans **Gérer les connexions réseaux**, puis dans **Propriété VPN**, décochez **Rappeler si la ligne a été raccrochée**. Cochez aussi l'option concernant le mot de passe de connexion qui doit être retenu **pour tous les utilisateurs**.

    Lien: <http://vpnlifeguard.blogspot.com>

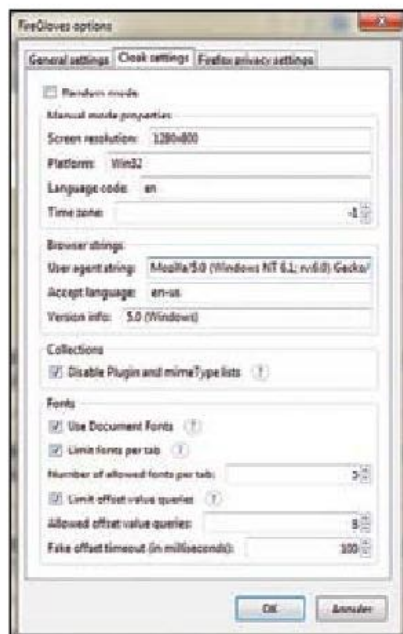


BROUILLEZ LES PISTES

// AVEC FIREGLOVES

Entre les proxys, les VPN, les clients mail et les espaces de stockage chiffrés, vous êtes parés à toutes les éventualités sauf une: l'empreinte unique de votre navigateur. Car quelque soit le logiciel utilisé ce dernier contient énormément d'informations permettant de vous tracer. Avec une simple requête, il est possible de connaître le nom de votre navigateur, sa version, le nombre et les noms des extensions, les polices installées, votre fuseau horaire, etc. En combinant ces différents éléments, les hackers peuvent dresser une empreinte unique: la vôtre. Même derrière un VPN vous voilà fiché! Firegloves est une extension sous Firefox qui va simplement donner de fausses informations aux curieux...

    Lien: <http://goo.gl/u50q9p>



DES PROXYS À LA DEMANDE

// AVEC CHRIS PC FREE ANONYMOUS PROXY

Après avoir téléchargé le logiciel, installez-le puis lancez l'interface. Difficile de faire plus simple ici puisqu'il suffit de choisir un pays dans le menu déroulant. Choisissez un proxy situé aux USA pour les sites de stream américain ou en France pour regarder vos émissions de l'étranger. Il est même possible de choisir un pays aléatoirement si vous êtes dans un pays où l'on censure Internet... Vous pouvez vous connecter automatiquement à un proxy au démarrage de l'application ou forcer l'anonymat même en cas de connexion lente. Cliquez sur **Connect to proxy** et au bout de quelques secondes, vous êtes connecté! Attention cette astuce ne fonctionne qu'avec votre navigateur et pas avec vos Torrents par exemple!

    Lien: www.chris-pc.com





ÊTRE SUR DE SON IP SÛR LES RÉSEAUX P2P

// AVEC CHECK MY TORRENT IP

Certains VPN ne redirigent que le protocole HTTP. Alors quand on veut être absolument sûr que son réseau privé virtuel fonctionne bien avec BitTorrent, il existe un moyen très simple: le site Check my Torrent IP. Ce dernier se charge de veiller à ce que vos sécurités soient bien actives... Allez sur le site de Check my Torrent IP et cliquez sur le bouton **FreeTorrent IP Checker**. Vous téléchargerez alors un Torrent test qui va indiquer au site votre IP toutes les 60 secondes. Placez ce Torrent dans votre client habituel et démarrez le «téléchargement». Au bout d'une minute, cliquez sur **Refresh** en bas du site pour voir les informations en sa possession.



    Lien: <http://goo.gl/MKHqU>

MOTEUR DE RECHERCHE ANONYME

// AVEC DUCK DUCK GO

Duck Duck Go est un moteur de recherche basé en Pennsylvanie et qui a pour philosophie de préserver la vie privée et de ne stocker aucune information personnelle concernant les utilisateurs. Pas de cookies intrusifs, d'adresse IP ou autres informations concernant la localisation, le navigateur et la configuration de l'Internaute. Comme le moteur ne cherche pas à savoir de quels pays vous venez, il faudra éventuellement lui dire. Après avoir fait une recherche, faites **More** (dans l'icône en haut à droite) puis **Setting**. Dans **Result**, choisissez votre région et votre langage.



     <https://duckduckgo.com>

ENCORE DES PROXY

// AVEC PROXY SWITCHER

Vous n'en avez pas encore assez? Voici encore un logiciel pour gérer vos serveurs mandataires. Proxy Switcher permet d'ajouter vos propres proxys, de les rechercher directement depuis l'interface et de tester leur rapidité. Il est même possible de paramétrer un changement automatique de proxy en cas de saturation de celui qui est utilisé. Après avoir testé ce logiciel, nous avons constaté qu'il est plus



rapide (moins de temps de latence pour le stream et le téléchargement) que Free Anonymous Proxy. Vous devrez néanmoins vous acquitter de 29,95\$ (soit 22€) pour profiter de la version standard après les 15 jours d'essai. À vous de voir, en fonction de votre utilisation, s'il est nécessaire de passer à un logiciel payant pour vos petites activités...

    <http://proxyswitcher.com>

CHANGEZ VOTRE ADRESSE MAC

// AVEC WIN7MACCHANGER

L'adresse MAC est un identifiant stocké dans votre carte réseau ou votre clé Wi-Fi. Il s'agit un peu d'un numéro d'identité sur un réseau sans fil et ces derniers s'en servent pour savoir qui est présent et depuis combien de temps. Si votre présence sur un hotspot est limitée à 20 minutes ou 1 heure, il suffit de changer votre adresse MAC et de se reconnecter pour passer inaperçu. Après tout, 20 minutes pour faire des recherches à la bibliothèque, c'est bien court (et un épisode de *South Park* dure un peu plus de vingt minutes non?). Sans connaissance particulière Win7MACChanger permet de changer votre adresse MAC.



    Lien: <http://soonware.blogspot.com>

MOBILE

81

«**ROOT**» Android, quels sont les avantages ?

84

WIFIKILL : soyez le maître de votre réseau

86

DSPLOIT : testez et sécurisez votre réseau local

88

Un mot de passe principale avec **DASHLANE**

90

VPN1CLICK : chiffrez votre connexion sur mobile

92

Cryptez vos conversations avec **DISCRETIO**

94

GREENIFY : faites hiberner vos applications





LE ROOT : POURQUOI ET COMMENT ?

Rooter son téléphone est une manipulation qui s'applique aux machines sous Android quelque soit leur marque (Samsung, HTC, Sony, etc.) Cette manipulation permet tout simplement d'élargir les droits d'accès des utilisateurs. Vous aurez alors le contrôle total sur votre machine. Au niveau de l'interface bien sûr puisqu'il est possible de télécharger des ROM spéciales permettant de se confectionner un «bureau» sur mesure : en 3D ou avec un thème qui vous tient à cœur par exemple. Mais aussi au niveau des logiciels qui s'autorisent des interventions plus en profondeur dans le système : capture d'écran, VPN, antiviol, suppression de la pub, etc. Par exemple la version mobile de l'antivirus Avast permet d'enregistrer votre SIM comme étant la seule à fonctionner pour qu'un voleur ne puisse pas l'utiliser. En mode root, cet enregistrement fonctionne même si le voleur

réinitialise le téléphone avec les réglages d'usine ! Vous aurez même accès à l'intégralité des données (ainsi que la localisation GPS) au nez et à la barbe de votre voleur...

COMMENT ?

En fonction de votre type de téléphone ou de tablette, la méthode sera différente et il existe même plusieurs méthodes pour un appareil donné. Il s'agit parfois d'un «toolkit» dédié (un logiciel qui réalise l'opération grâce à une connexion sur port USB) ou d'une manipulation avec le logiciel Odin. Ce dernier permet en effet de rooter plusieurs types de téléphones. Notez qu'il est même parfois de rooter son téléphone en plaçant une appli sur sa carte SD. Rares sont les appareils problématiques puisque Google encourage cette modification. Et de toute façon, Google est votre ami ! Vous pourrez sans problème trouver une méthode clé en main en tapant «Galaxy S5 root» ou «root HTC One X+».



SI VOUS AVEZ UN TÉLÉPHONE OU UNE TABLETTE SOUS ANDROID VOUS AVEZ SANS DOUTE DÉJÀ ENTENDU PARLÉ DE «ROOT» SUR INTERNET OU PAR UN AMI. CETTE MODIFICATION DU SYSTÈME PERMET D'INSTALLER DES APPLICATIONS SPÉCIALES OU D'ACCÉDER À DES FONCTIONNALITÉS INÉDITES. VOYONS CELA PLUS EN DÉTAIL...



LE "ROOT" PERMET UN CONTRÔLE TOTAL SUR VOTRE TÉLÉPHONE : SÉCURITÉ, PERSONALISATION, DÉINSTALLATION D'APPLIS INUTILES, ETC.



LE ROOT POUR QUOI FAIRE ?

PRATIQUE



01 > CHANGER LA ROM

Une fois que vous avez rooté votre téléphone, les programmes qui utilisent cette fonctionnalité pourront faire leur œuvre, mais les performances de votre appareil ne seront pas plus

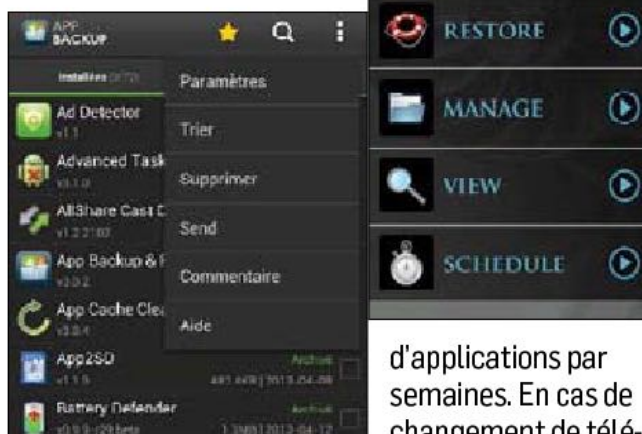


avancées. Pour un changement en profondeur, il faudra changer la ROM. Entre celles qui ajoutent de nouvelles fonctionnalités et celles qui permettent des bidouillages, vous avez le choix. La ROM alternative la plus plébiscitée du moment n'est autre que CyanogenMod.

<http://tinyurl.com/brdwuru>

02 > SAUVEGARDER SES APPLICATIONS

Pas facile de faire une sauvegarde de tous les éléments de votre téléphone surtout lorsque vous êtes habitué à installer des dizaines

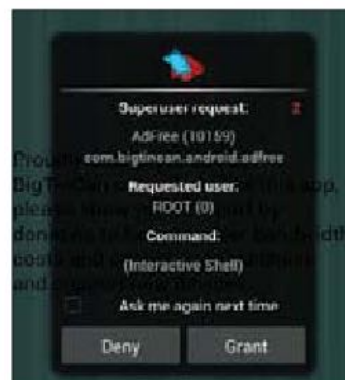


d'applications par semaines. En cas de changement de téléphone, il est possible de faire une sauvegarde avec un logiciel comme MyBackup par exemple.

<http://tinyurl.com/bno2wqk>

03 > SUPPRIMER LA PUB

La publicité sert à rémunérer les développeurs qui font le choix de proposer des applications gratuites. Le problème, c'est qu'avec les limitations des forfaits, vous devez sacrifier beaucoup de bande passante pour afficher ces pubs, même avec des applications ne nécessitant pas de connexion! Android Add Free supprime tout simplement la pub et les dépassements de forfait qui vont avec...



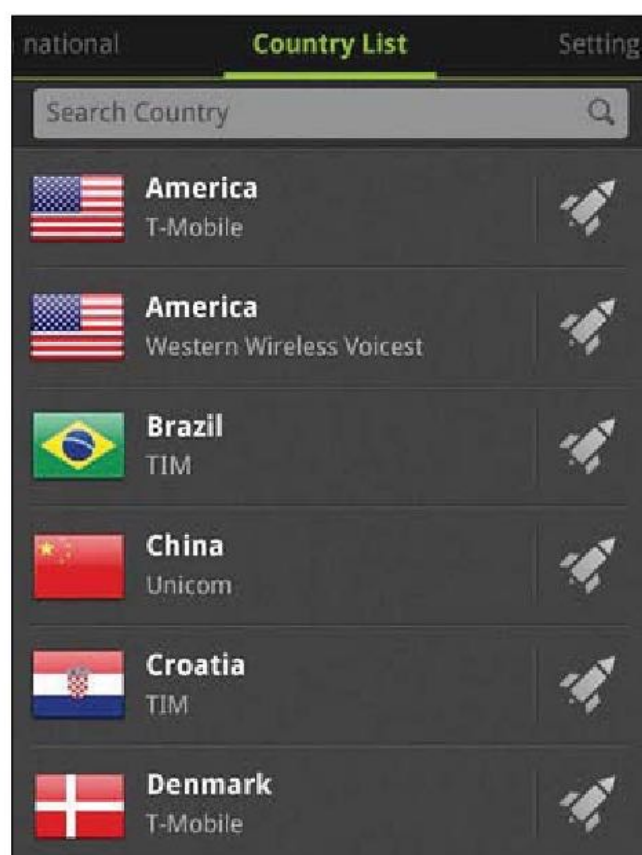
<http://tinyurl.com/nymzwwz>



04 > ACCÉDER À DES APPLICATIONS CENSURÉES

Saviez-vous que le GooglePlay disponible pour les utilisateurs français n'affiche pas l'intégralité des applications? Il semblerait, en effet, que certains opérateurs font pression sur Google pour que ce dernier ne propose pas les applications de tethering (pour partager sa connexion). Avec un téléphone rooté et Market Enabler, vous pouvez accéder à toutes les applis quelque soit votre pays...

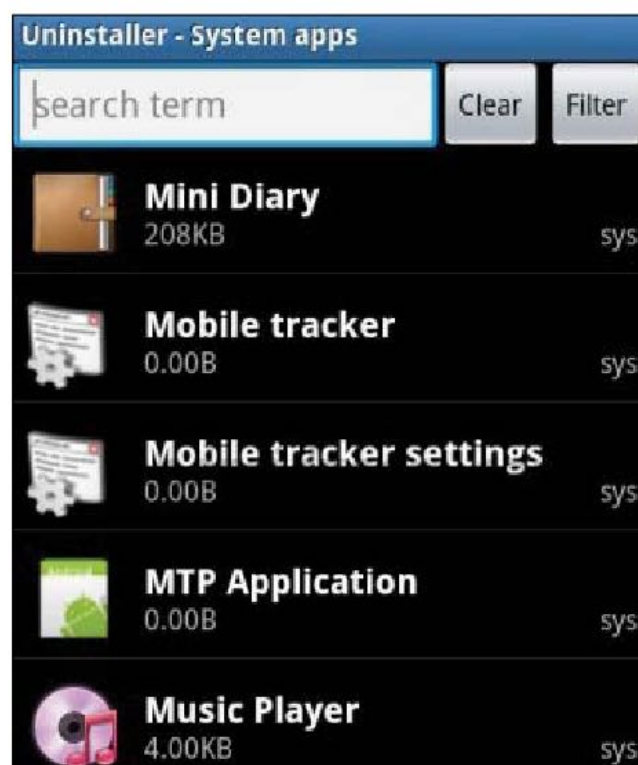
👤 <http://tinyurl.com/m4vbh7m>



05 > DES CENTAINES D'AUTRES FONCTIONNALITÉS...

Si vous n'utilisez jamais les applications du constructeur (Samsung Apps, etc.) ou de votre opérateur (achat en ligne, etc.) vous pouvez vous en débarrasser avec un téléphone rooté. Vous gagnerez de la place sur votre bureau et dans la mémoire de votre appareil. Pour plus d'exemples d'utilisation, nous vous invitons à lire la suite de cette rubrique. La plupart de nos astuces nécessitent un appareil rooté pour fonctionner: hibernation d'appli, sidejacking, récupération de fichier, overclock, chiffrement, récupération de mots de passe, etc.

👤 <http://tinyurl.com/c7mkfp5>



PEUT-ÊTRE PAS POUR VOUS...

Si vous utiliser votre téléphone pour...téléphoner (vous êtes né dans les années 60 ou quoi?) ou que vous utilisez les applications pour votre travail, vous n'avez peut-être pas besoin de rooter votre téléphone. Bien sûr vous pouvez tenter le coup par curiosité (c'est sans danger si vous faites une sauvegarde du contenu : contacts, fichier et applis) mais rares seront les occasions d'en tirer profit. Si par contre vous tombez sur une appli nécessitant le root, vous pourriez changer d'avis et rejoindre le clan des bidouilleurs...



INFOS [WIFIKILL]

Où le trouver ? [<http://goo.gl/QRH710>]

Difficulté : ☹️☹️☹️

WiFiKill, TUEZ L'ACCÈS AU RÉSEAU !

VOUS ÊTES EN COLLOCA-
TION, À LA BIBLIOTHÈQUE
OU DANS N'IMPORTE
QUEL ENDROIT AVEC UNE
CONNEXION Wi-Fi QUE
VOUS PARTAGEZ ? GRÂCE
À WiFiKill, VOUS POUVEZ
FAIRE EN SORTE DE BANNIR
LES AUTRES UTILISATEURS
POUR GARDER TOUTE LA
BANDE PASSANTE ! TERMINÉ
LES PETITES SŒURS QUI
SQUATTENT YouTube OU
LES NEUNEUS QUI LEECHENT
50 TORRENTS À LA FOIS...



Un outil d'ARP
poisoning facile
à utiliser et très
pratique



Le fichier
d'installation
APK est difficile à
trouver. Si notre
lien ne fonctionne
plus, tapez «WiFiKill
APK» sur Google



ue celui qui n'a
pas songé à
rétablir la peine
de mort pour
ceux qui abusent de la bande
passante nous jette la première
pierre ! Les «wesh wesh»
qui streament pendant que
vous travaillez, les noobs qui
engorgent la connexion avec leur
téléchargement et tous ceux qui
pensent qu'Internet fonctionne
par magie («c'est quoi la bande
passante ?»)... Vous avez tous
été dans une situation où vous ne
pouviez pas utiliser correctement
une connexion partagée à cause
d'égoïstes ou d'ignorants. WiFiKill
va changer votre vie ! Équipé d'un
téléphone Android rooté (avec
des droits Super Utilisateur) et
connecté au réseau partagé, vous
aller avoir le droit de vie et de mort
sur les connexions. Une fois en



LE RÉSEAU SUR LEQUEL VOUS
VOUS CONNECTEZ EST TROP
ENCOMBRÉ ? FAITES LE MÉNAGE
AVEC WIFIKILL !



action, le logiciel va trouver toutes
les machines qui sont connectées
au point d'accès. D'un mouvement
de doigt, vous allez alors pouvoir
«tuer» la connexion de votre voisin
ou toutes les connexions alentour,
sauf la vôtre, bien sûr !



MOBILE

ARP poisoning

TUEZ LA CONNEXION DE QUI VOUS VOULEZ !

PRATIQUE



01 > LES PRÉ-REQUIS

En premier lieu, il va vous falloir un téléphone sous Android (au moins 4.0) et rooté. Il s'agit d'une manipulation simple et qui ne risque pas d'endommager votre téléphone. Bien sûr, votre téléphone doit être connecté au réseau Wi-Fi ciblé. Ici, c'est le réseau domestique **ma_freebox**.



deux minutes au cas où un nouvel utilisateur débarque sur le réseau. Dans les réglages (**Setting** depuis le bouton **Menu**

à gauche), il est possible de faire vibrer votre téléphone à chaque nouvel «intrus».



02 > L'APPLI

Téléchargez l'application et installez-la.



Celle-ci n'est plus disponible sur l'Android Market, il faudra suivre notre lien pour l'obtenir. Le téléphone vous demandera si vous souhaitez utiliser les paramètres **Super User**. Validez. Si

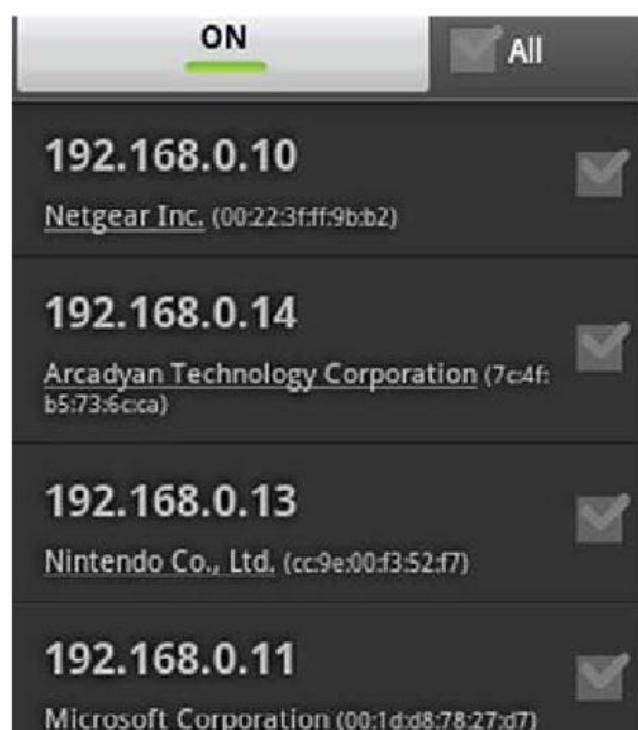
votre téléphone n'est pas rooté, il faudra trouver un tuto sur Google.

03 > TOUS LES APPAREILS CONNECTÉS

Cliquez alors sur **ON** et l'appli va chercher les appareils qui sont connectés sur le réseau Wi-Fi ciblé. Il répétera cette opération toutes les

04 > KILLING ET RESURRECTING

Chaque ligne correspond à une machine. Ici, on peut voir deux ordinateurs, une Nintendo 3DS et la Xbox360 du salon. Si vous appuyez sur une ligne, la connexion Internet est coupée! Un second clic rétablira la bande passante (**Resurrecting**). Faites **All** pour tuer toutes les connexions et utiliser le maximum de la bande passante avec votre téléphone ou recherchez votre PC dans la liste pour réactiver uniquement cette connexion.





INFOS

[DSPLOIT] Où le trouver ? [www.dsploit.net][BUSYBOX] Où le trouver ? [<http://goo.gl/hMLMve>]

Difficulté : ☠☠☠

TESTEZ & SÉCURISEZ VOTRE RÉSEAU LOCAL

VOUS VOULEZ VÉRIFIER LA SÉCURITÉ DU RÉSEAU WI-FI D'UN AMI ? AU LIEU DE VOUS DÉPLACER AVEC VOTRE MATÉRIEL, POURQUOI NE PAS UTILISER UN APPAREIL MOBILE. IL EXISTE DES OUTILS POUR «PENTESTER» (DE L'ANGLAIS «PENETRATION TEST») SOUS ANDROID. SUIVEZ LE GUIDE...



Couvre différents aspects et regorge de fonctionnalités sympathiques



Bien sûr l'application est moins puissante que Kali Linux (BackTrack) pour des tests de ce type mais quelle puissance dans une seule main !

Pour vérifier si votre réseau Wi-Fi et votre environnement informatique sont sécurisés de manière correcte, il existe plusieurs outils sous Windows ou Linux, mais lorsqu'il s'agit d'appareil mobile, les choix sont plus restreints. Les logiciels de ce type demandent, en effet, beaucoup de ressources et un téléphone, même puissant, ne pourra pas rivaliser avec un Intel Core i7. Pourtant, il existe des outils qui permettent de faire de vraies prouesses. dSploit est une application fonctionnant avec n'importe quel appareil rooté tournant minimum avec la version 2.3 du système Android. Cette

dernière permet de rechercher dans votre réseau les vulnérabilités matérielles et logicielles connues, de scanner les ports, de sniffer des mots de passe, de manipuler le trafic (ARP Poisoning) et de réaliser des attaques de type «man-in-the-middle». Une fois dans un réseau privé ou public, vous avez accès à tous les périphériques et êtes libre de scruter ses moindres faiblesses...



DSPLOIT PERMET DE SÉCURISER VOTRE RÉSEAU ET CELUI DES AUTRES DEPUIS VOTRE SMARTPHONE





INSTALLATION ET UTILISATION DE DSPLOIT

PRATIQUE



01 > INSTALLATION

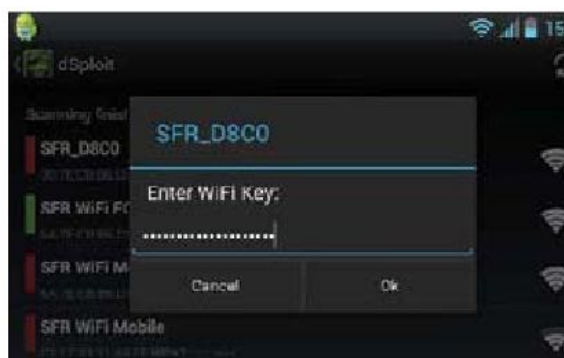
dSploit n'est pas disponible sur le Google Play Store, il faudra télécharger le fichier APK depuis notre adresse puis le transférer via le câble USB ou vous l'envoyer par mail. Pour pouvoir l'installer, il faudra autoriser les



sources inconnues. Allez dans **Paramètres > Sécurité** et cochez **Sources inconnues** dans **Administration du périphérique**.

02 > BUSYBOX ET MAPPAGE DU RÉSEAU

Telle quelle, l'application refusera de fonctionner, il faudra que vous installiez BusyBox. Pour cette dernière, pas de problème! Elle est disponible sur le Play Store. Lorsque vous la démarrerez, faites juste **Install** en bas et attendez la fin du processus. Retournez dans dSploit et tout devrait fonctionner. Après quelques secondes de paramétrage, vous verrez tous les périphériques qui sont connectés à votre réseau local (il faut bien sûr que votre appareil Android en fasse partie).



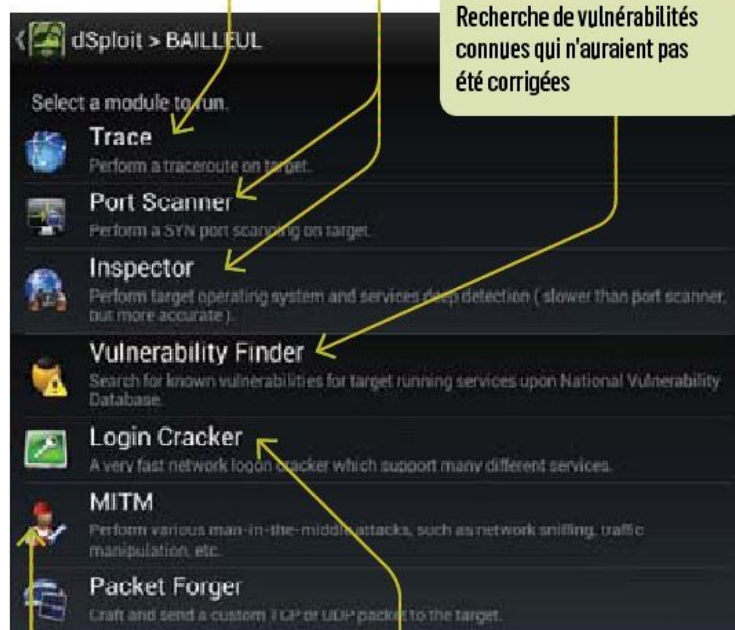
03 > LES FONCTIONNALITÉS

Traceroute permettant de suivre les paquets d'informations sur le réseau

Scan de port standard et poussé



Recherche de vulnérabilités connues qui n'auraient pas été corrigées



Un petit logiciel de crack «brute force» pas très puissant mais pouvant se révéler utile

Attaques Man-in-the-Middle : sniffer de mot de passe, ARP poisoning (couper le Wi-Fi sur un périphérique, sidejacking, injection de script, remplacer des images, des vidéos, etc.)



INFOS [DASHLANE]

Où le trouver ? [<http://goo.gl/ECcmX> (Android)] [<http://goo.gl/zHFOA> (iOS)]

Difficulté : 

Dashlane : VOTRE MOT DE PASSE PRINCIPAL

VOUS CONNAISSEZ DÉJÀ
LE PRINCIPE DE MOT DE
PASSE PRINCIPAL SUR PC :
UN SÉSAME QUI DÉBLOQUE
TOUS VOS AUTRES MOTS
DE PASSE SANS AVOIR À
LES MÉMORISER OU LES
TAPER. NON SEULEMENT
DASHLANE S'ACQUITTE
DE CETTE TÂCHE, MAIS IL
PROPOSE BIEN D'AUTRES
FONCTIONNALITÉS...



Un chiffrement
local solide et
la possibilité
de sauvegarder
d'autres données
confidentielles



Il faudra passer
à la caisse
pour pouvoir
exporter vos
mots de passe

Si vous recyclez le même
mot de passe à chaque fois
que vous vous inscrivez sur
un nouveau site, Dashlane
est fait pour vous. En effet rien de
plus risqué que de reprendre le
même mot de passe ou presque. Si
un hacker découvre votre sésame
«toto» valable pour le site A, il
découvrira ceux des sites B, C et
D si vous avez choisi «toto75»,
«ToTo», «Totobogoss», etc. La
solution pour éviter de tout retenir
est de choisir un mot de passe
principal qui débloquera tous les
autres. Dashlane propose en effet
de saisir vos mots de passe vers
Facebook, Gmail ou Instagram puis
de les retenir en local dans un coffre
fort numérique crypté.

LES PETITS PLUS

Dashlane fait encore plus
puisqu'il permet de remplir

automatiquement des formulaires
d'inscription, d'enregistrer des
documents confidentiels comme
votre carte de sécurité social,
passeport, carte d'identité, numéro
de carte bancaire, etc. Pas de risque
au niveau de la sécurité puisque
le mot de passe qui déverrouillera
tout ça doit obligatoirement
comporter 8 caractères avec
chiffres, minuscules et majuscules.
Petite précision : tout est stocké
en local, votre mot de passe ne se
baladera pas dans un «cloud» ou un
serveur distant...



DASHLANE STOCKE ET SÉCURISE VOS
MOTS DE PASSE MAIS REMPLIT AUSSI
LES FORMULAIRES AUTOMATIQUEMENT



**SUR ANDROID
ET IOS**





MOBILE

Mots de passe

ENREGISTREZ VOS SÉSAMES

PRATIQUE



01 > VOTRE MOT DE PASSE «MAÎTRE»



Après avoir installé et démarré l'appli, passez la présentation et appuyez sur **Continuer**. Faites **Créer un compte** et choisissez un **Mot de passe maître**. Ce dernier devra comporter 8 caractères,

au moins une lettre et un chiffre, au moins une majuscule, etc. Si un critère n'est pas rempli, vous ne pourrez pas sauver vos mots de passe. En effet ce mot de passe maître servira à déverrouiller tous les autres!

02 > VOS SITES PRÉFÉRÉS

Lorsque l'appli affichera que le compte a bien été créé, faites **Démarrer** et commencez

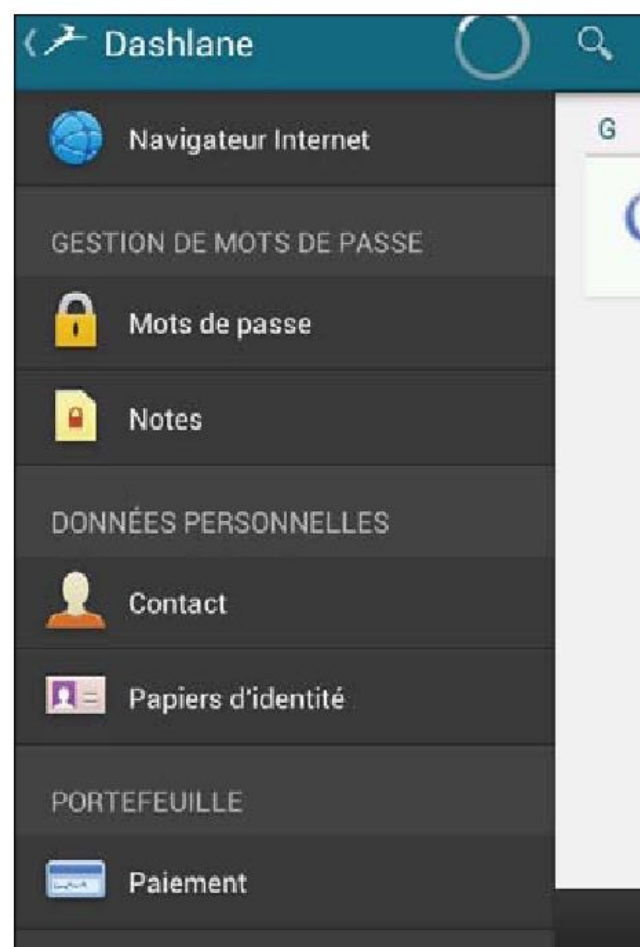


à sélectionner un des sites auquel vous êtes habitué dans la liste. Si un de vos sites ne figure pas dans la liste, vous pourrez rentrer l'URL à la main plus tard. Faites **Terminer** et remplissez les champs **Identifiant** et **Mot de passe**. À l'avenir, si Dashlane est

activé sur votre appareil vous n'aurez pas à rentrer cet identifiant. Continuez avec vos autres sites favoris...

03 > LES AUTRES FONCTIONNALITÉS

Dashlane fait aussi office de coffre fort numérique. En effet vous pourrez mettre les informations concernant votre passeport, votre carte vitale, votre compte Paypal ou les numéros de votre carte bancaire. Tout sera déblocable avec votre mot de passe maître. Heureusement tout cela est chiffré en AES 256 bits. Allez dans le menu déroulant de gauche et faites **Papiers d'identité** ou **Paiement**.





INFOS [VPN ONE CLICK]

Où le trouver ? [<http://goo.gl/gwmvq> (Android)] [<http://goo.gl/JQ4nSF> (iOS)]

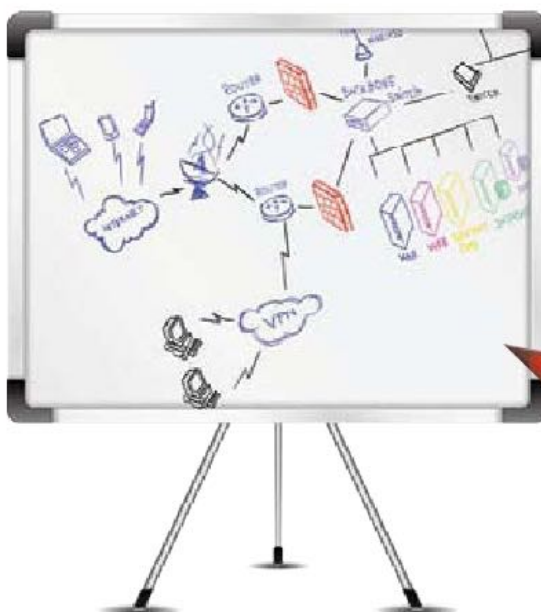
Difficulté : ☹️☹️☹️

Un VPN SUR SON SMARTPHONE



SUR ANDROID
ET IOS

UTILISER UN VPN SUR PC EST PRESQUE OBLIGATOIRE LORSQUE L'ON SE CONNECTE SUR UN POINT D'ACCÈS WiFi INCONNU OU NON SÉCURISÉ. SUR MOBILE C'EST UNE NÉCESSITÉ ! EN EFFET, LE CÔTÉ NOMADE DE VOTRE APPAREIL INCITE À SE CONNECTER DÈS QUE L'ON PEUT ET MALHEUREUSEMENT LES ANTIVIRUS NE SONT PAS UN RÉFLEXE POUR TOUT LE MONDE...



Si vous êtes un habitué de *Pirate informatique*, vous savez qu'un VPN est un logiciel qui permet d'établir un tunnel chiffré entre votre appareil et Internet. Imaginons que vous soyez connecté vers un hotspot non sécurisé. Les menaces sont alors multiples : sidejacking, vol de données, infections, etc. Des hackers peuvent, par exemple, récupérer des mots de passe ou usurper votre identité. Les modes de communication nomades sont tout particulièrement concernés. Parce qu'il est simple à utiliser et

stable, nous avons choisi de vous présenter Vpn One Click. Le logiciel est payant, mais il dispose d'une période d'essai gratuite où vous ne pourrez pas choisir l'intégralité des «domiciliations» qu'il propose. En effet, en choisissant de payer 5 \$ (3,70 €) pour un trimestre ou 10 \$ (7,40 €) pour un an, vous pourrez choisir votre IP parmi 29 pays différents ! Si vous décidez de ne pas payer pour ce service, vous serez de toute façon protégé sur les hotspots inconnus (dans ce cas, seul le bouton proposant une IP aléatoire sera disponible).



Un tunnelisation pour se protéger des faux points d'accès ou des hotspots non sécurisés



Il faudra passer à la caisse au bout de la période d'essai !



VOTRE CONNEXION AVEC FREEDOM-IP

PRATIQUE



01 > L'INSTALLATION

Pas besoin d'avoir un téléphone «rooté»



secondes, vous verrez votre IP.

pour profiter de Vpn One Click, il suffit de l'installer depuis le Google Play ou le store d'Apple. Ouvrez l'appli et commencez par regarder votre IP actuelle en choisissant **Check IP Address** en bas du menu déroulant. Au bout de quelques

qui nous intéresse n'est pas la localisation de l'IP, mais bien le chiffrement des communications, cette solution est idéale. Attention, le cryptage est très gourmand en ressource. Votre batterie va s'en souvenir...



02 > VOTRE PAYS DE RÉSIDENCE...

Il est temps de trouver un pays de résidence (c'est la mode). Vous avez le choix entre 29 pays: USA, Canada, Australie, Royaume-Uni, Allemagne, France, Pays-Bas, Suisse, Italie, Inde, Singapour, Russie, Égypte, Suède, Espagne, Turquie, Hong Kong, etc. Attention, certains pays ne sont disponibles qu'avec la version payante.



03 > ... AU HASARD!

Cependant, pendant la période d'essai, vous ne pourrez utiliser que le bouton **Connect Random** qui permet de prendre n'importe quel serveur disponible de manière aléatoire. Comme ce

04 > UNE CONNEXION SÉCURISÉE

Une fois que votre VPN est activé, vous devriez voir une clé apparaître dans la barre du haut. Retournez sur **Check IP Address** pour constater que votre adresse a changé. Si vous voulez basculer de protocole, allez sur **Change Vpn Protocol**. Vous pouvez surfer en toute sécurité sur n'importe quel réseau sans fil...





INFOS [DISCRETIO]

Où le trouver ? [<http://goo.gl/ZE9vR>]

Difficulté : ☠☠☠

CRYPTTEZ VOS CONVERSATIONS !

VOUS VOULEZ PROTÉGER VOS CONVERSATIONS TÉLÉPHONIQUES, CAR VOUS ÊTES AVOCAT, HOMME D'AFFAIRES OU TOUT SIMPLEMENT PARCE QUE VOUS VOULEZ PROTÉGER VOTRE VIE PRIVÉE ? DISCRETIO PERMET D'ÉVITER LES INTERCEPTIONS D'INFORMATIONS EN CHIFFRANT TOUT CE QUE VOUS DITES SUR MOBILE ANDROID.

Vous ne le savez peut-être pas, mais les conversations téléphoniques par GSM peuvent être interceptées avec un matériel relativement bon marché. Normalement, le chiffrement spécifique du GSM devrait interdire ces piratages, mais il n'est pas actif sur toutes les antennes qui équipent nos villes. Les opérateurs devraient signaler l'absence de chiffrement lorsqu'il n'est pas disponible, mais ils ne le font pas... Il suffit alors pour un pirate de se confectionner une antenne plus puissante que celle des environs pour que les téléphones se connectent directement dessus. Discretio est une application gratuite qui va permettre une communication via Wi-Fi ou 3G

entre deux téléphones équipés. L'authentification comme le contenu de la conversation seront chiffrés et même une analyse poussée des paquets ne révélera rien.



Un chiffrement complexe, mais une mise en place très facile



Il faut que vos correspondants utilisent aussi Discretio pour un anonymat complet



Quand il ne torture personne au nom de la liberté, Jack Bauer utilise Discretio...



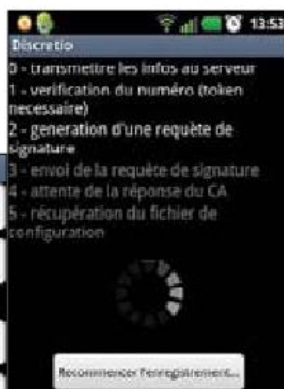
UN APPEL CRYPTÉ AVEC DISCRETIO

PRATIQUE



01 > PREMIERS PAS

Dès le lancement, l'appli vous demandera de remplir un formulaire avec nom, prénom, pays, e-mail et numéro de téléphone. Mettez



aussi un mot de passe et faites **OK**. L'enregistrement va alors commencer puis Discretio va

générer la clé privée et le certificat.

02 > LE TOKEN

Vous allez recevoir un SMS avec le token. Copiez ce code (un appui long sur le SMS puis **Copier le texte du message**) dans le champ idoine. Attention, il faudra supprimer le début du texte. Le token commence par **discretio://**. Si l'appli bugge, recommencez l'opération depuis le remplissage du formulaire (désinstallez et réinstallez)

03 > L'ACTIVATION

Lorsque toutes ces étapes se sont déroulées sans problème, on vous demandera le mot de passe que vous avez défini puis l'interface va se charger. Ici, vous pourrez paramétrer une sonnerie spéciale pour les interlocuteurs qui vous appelleront avec Discretio (vous saurez alors que la conversation est sécurisée). Il est aussi possible d'**Activer le Tunnel**, une sorte de VPN qui trompera les opérateurs qui bloquent ou brident la VoIP en 3G...



04 > VOTRE PREMIER APPEL!

En sortant de Discretio, vous verrez un voyant vert dans votre barre de notification en haut. S'il devient rouge attention, le logiciel ne peut pas se connecter au serveur et vos appels ne seront pas chiffrés. Utilisez alors votre téléphone comme d'habitude. Si vous essayez de joindre un numéro qui n'est pas enregistré comme appartenant à un utilisateur de Discretio, l'appli vous le signale. Lorsque vous



êtes en conversation avec un utilisateur de Discretio, vous verrez un cadenas fermé montrant que le système fonctionne. Bien sûr, ces conversations ne seront pas décomptées de votre forfait «appel», mais attention à l'utilisation en 3G!



Faites hiberner VOS APPLICATIONS



SI VOUS ÊTES SOUS ANDROID, VOUS SAVEZ QUE LA BATTERIE FOND COMME NEIGE AU SOLEIL LORSQUE LES APPLICATIONS SE METTENT À FONCTIONNER SANS VOTRE CONSENTEMENT. GREENIFY PERMET DE LES «FIGER» POUR ÉCONOMISER DE LA BATTERIE ET GAGNER EN PUISSANCE...



Doublez l'autonomie de votre téléphone avec cette application gratuite



Il vous faudra un appareil rooté pour utiliser toute les fonctionnalités

GREENIFY EN 3 ÉTAPES

PRATIQUE



01 > LA LISTE DES APPLIS

Téléchargez et installez Greenify sur



votre appareil rooté. Démarrez l'appli et autorisez les privilèges **Super-Utilisateur**. Faites + en bas de la page de présentation. Greenify va ensuite analyser les applications présentes sur

votre appareil et les classer en fonction de leur consommation et de leur utilisation. Parcourez la liste (faites éventuellement **Afficher plus**) et sélectionnez une ou plusieurs applications.

bouton +. Une fois hibernées, vos applications n'iront plus chercher de mises à jour ou s'allumer de manière intempestive pour aller fureter sur le réseau.



03 > UN RÉVEIL FACILE

Vous économiser votre batterie et le processeur sera plus réactif puisqu'il ne sera pas embêté avec des processus qui se lancent constamment. Ce qui est formidable c'est que vous n'aurez pas à aller à nouveau dans le

menu de Greenify pour réveiller vos applications. Il suffira de les lancer normalement. Attention de ne pas faire hiberner les alarmes et les messageries instantanées...

02 > FAITES HIBERNER LES APPLIS GOURMANDES

En haut à droite, appuyez sur l'icône en forme de curseur pour valider leur hibernation. Vous verrez **l'application a été greenifiée avec succès**. Vous pouvez rajouter d'autres applications avec le

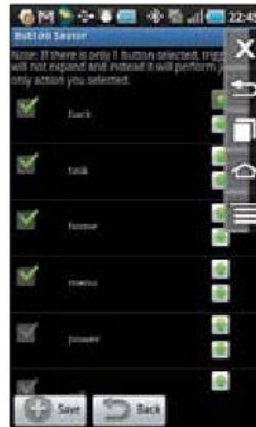




VIRTUALISER LES BOUTONS

// AVEC BUTTON SAVIOR

Votre téléphone a fait une chute ou est passé sous un vélo? Il a l'air de fonctionner, mais malheureusement les boutons physiques **Home**, **Menu** et **Retour** ne fonctionnent plus à cause du choc. Si votre téléphone est rooté, pourquoi ne pas utiliser Button Savior? Vous pourrez alors avoir les mêmes fonctionnalités que vos boutons cassés transposés sur des icônes de votre écran tactile. Notez que même sans casse, Button Savior permet de se créer des boutons sur mesure selon vos besoins!



<http://goo.gl/IHCmLJ>

ENREGISTREZ VOS MANIPULATIONS

// AVEC REPETITOUCH FREE

Vous avez des tâches répétitives à effectuer avec votre téléphone? Vous en avez assez de chercher dans les menus pour utiliser telle ou telle fonction? RepetiTouch Free est une appli pour smartphones Android «rootés» qui va enregistrer vos manipulations (touché d'écran, mouvements, «clic», etc.) et les reproduira à la demande. Faites **Start** pour commencer et afficher dans votre bureau une suite d'icônes. Une pression sur le rond rouge va enregistrer toutes les manipulations que vous souhaitez. Il suffira de faire **Play** (la flèche verte) pour les répéter à l'envi. L'étoile bleue affiche un menu où vous pourrez gérer et nommer les différentes manipulations («Accès direct vers menu applications» ou «Installer les applis hors Google Store»).

<http://goo.gl/lfWLMF>

DÉ-«ROOTER» VOTRE MOBILE

// AVEC UNIVERSAL UNROOT



Il arrive parfois que l'on veuille retirer les fonctions «super user» sur un téléphone rooté: problème durant le root qui fait bugger l'appareil, revente, renvoi au service après-vente, etc. Le problème c'est qu'on trouve plein de tutos sur Internet pour rooter un smartphone mais il y a peu d'information pour faire machine arrière! Avec Universal Unroot vous n'avez qu'à appuyer

sur un bouton pour défaire ce qui a été fait. Après un redémarrage, votre téléphone sera comme à la sortie d'usine... Fonctionne avec les versions d'Android de 2.2 à la 4.2.2.

Lien: <http://goo.gl/slsT7b>

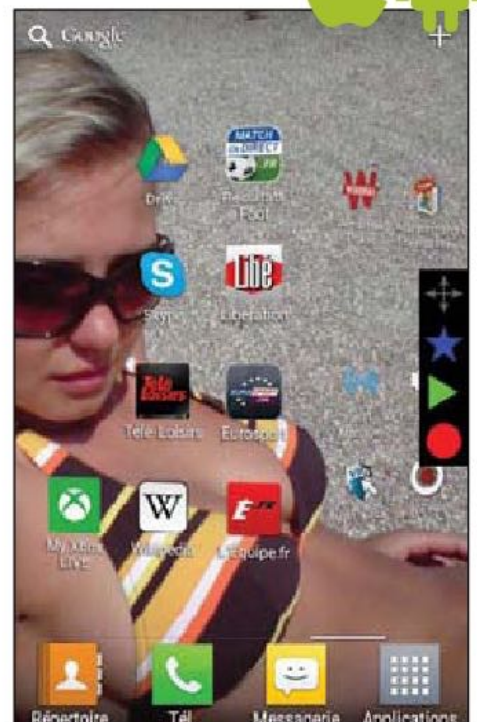
RÉCUPÉRER VOTRE MOT DE PASSE WIFI

// AVEC GESTIONNAIRE DE FICHIERS

Si vous n'avez pas le mot de passe Wi-Fi ou que vous ne l'avez plus en tête, il est possible de le récupérer en clair avec un téléphone rooté et l'appli Gestionnaire de fichiers. Allez dans les options et cochez **Root Explorer**. Rendez vous ensuite dans le dossier **/data/misc/wifi** (utiliser la flèche verte pour remonter) et ouvrez **wpa_supplicant.conf** avec l'éditeur de texte inclus dans l'appli. Vos mots de passe Wi-Fi apparaissent en clair...



<http://goo.gl/Kbjw0>





SIDEJACKER UN COMPTE

// AVEC DROIDSHEEP

Le sidejacking est une technique qui permet à un attaquant de se connecter à votre session (Facebook, Amazon, Google, etc.) pendant que vous êtes connectés sur le même réseau. Un vrai malheur sur un réseau Wi-Fi de bibliothèque ou de McDo! Attention, ce logiciel a pour but de mettre en évidence les vulnérabilités et pas de pirater quelqu'un. Pour éviter de tomber dans ce type de piège, passez par un VPN ou utilisez DroidSheep Guard du même auteur.



Lien : <http://goo.gl/y6uCB1>



ASPIRER LES MOTS DE PASSE

// AVEC USBCLEAVER

USBCleaver est un aspirateur de mots de passe assez intéressant. Une fois que l'application a été installée, il suffit de télécharger les fichiers supplémentaires et de sélectionner les mots de passe qui vous intéressent depuis **Enable/Disabled Payloads** (réseau Wi-Fi, mot de passe Firefox, système, etc.). Connectez alors le téléphone sur le port USB du PC cible et allez dans la carte SD depuis Windows pour lancer le fichier **Go.bat**. Ce dernier va transférer les données sur le téléphone! Attention, il faudra peut-être désactiver l'antivirus et le pare-feu de la cible, mais cela fonctionne très bien...



Lien : <http://goo.gl/Laf1xt>



TEST DE PÉNÉTRATION

// AVEC DROIDSQLi

Une injection SQL est un type d'attaque permettant de hacker un site. Il s'agit en fait de taper du code SQL dans un champ «mot de passe» pour obtenir des droits de manière frauduleuse. DroidSQLi est une application qui permet de réaliser ce genre d'attaque pour tester votre propre site et corriger les vulnérabilités. Il s'agit donc de Penetration Test ou «pentest». L'appli gère l'automatisme des injections et réalise différents tests: injection à l'aveugle, erreur de base MySQL, etc.



<http://goo.gl/Y1G39>



RÉCUPÉRER DES FICHIERS EFFACÉS

// AVEC DISKDIGGER

DiskDigger permet simplement de retrouver des photos malencontreusement effacées de votre mémoire interne ou de votre carte SD. Qu'il s'agisse d'une erreur de manipulation ou d'un formatage, cette appli va retrouver vos Jpeg, Png ou vidéos Mp4 tant que la perte est récente. En effet il faudra agir vite pour que le système n'enregistre aucune information sur les zones où étaient stockées vos précieux fichiers. Le mieux est encore d'installer DiskDigger avant toute tentative de récupération. Ne fonctionne qu'avec un appareil rooté.



<http://goo.gl/zLY3mC>

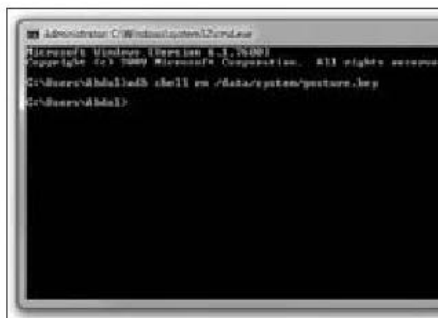




DÉVERROUILLER UN APPAREIL

// AVEC LE ANDROID SDK

Vous avez opté pour un verrouillage par pattern (le schéma graphique à reproduire sur votre écran tactile) pour interdire l'accès à votre mobile ou votre tablette? Le problème



c'est que vous l'avez oublié ou alors un ami vous a fait une blague pas drôle? Pour déverrouiller le téléphone, il va falloir télécharger le kit de développement Android (SDK) et connecter votre appareil au PC en mode **Débugage USB**. Lancez ensuite **cmd.exe** et tapez **adb shell rm /data/system/gesture.key**. Rebootez ensuite le téléphone. Si cela ne fonctionna pas, faites

```
adb shell
cd /data/data/com.android.providers.settings/databases
sqlite3 settings.db
update system set value=0 where name='lock_pattern_autolock';
update system set value=0 where name='lockscreen.lockedoutpermanently';
.quit
```

Vous pourrez alors débloquent le portable avec n'importe quel schéma.



Lien: <http://goo.gl/qmZmvE>

ANONYMISER VOS TÉLÉCHARGEMENTS

// AVEC CYANOGENMOD OU XPRIVACY

Lorsque vous installez une application sur votre mobile, le Play Store dresse une liste des «permissions». Il s'agit des informations que l'application aura le droit d'aller chercher dans votre mobile ou dans vos autres applications: coordonnées GPS, contacts, SMS, calendrier, historique, etc. Si on essaye d'interdire ces mauvaises manières, il se peut que l'application refuse de fonctionner. L'astuce est donc de «montrer» à l'application curieuse un calendrier vide, des coordonnées GPS



invalides, etc. Pour éviter de dévoiler votre vie privée à n'importe qui, nous vous proposons donc deux solutions. La première est contenue dans les dernières versions de la ROM Cyanogen (à partir de la 10.1). Il s'agit du mode Privacy Guard (ou Incognito Mode). La seconde option est l'application Xprivacy (3€) qui réalise la même chose à la différence qu'ici, toutes les ROMs sont compatibles.



Lien: www.cyanogenmod.org ; <http://goo.gl/7xLhU>

OVERCLOCKER VOTRE APPAREIL

// AVEC ANTuTu CPU MASTER

L'overclock est une technique qui permet d'accélérer le processeur d'une machine. AnTuTu CPU Master va automatiquement reconnaître votre processeur et vous proposer d'augmenter sa cadence pour gagner en puissance et donc en rapidité. Attention, il n'autorisera pas de mettre en danger votre appareil (un overclock trop élevé peut faire chauffer la machine et la détériorer). Vous ne pourrez qu'augmenter la valeur minimale. Les tâches courantes seront donc expédiées plus rapidement, mais vous pourrez aussi baisser la cadence pour économiser de la batterie. La version payante (3€) va vous proposer différents profils en fonction de votre utilisation.



Lien: <http://goo.gl/VENB7d>

Matériel

Un tracker GPS

QUI ENREGISTRE AUSSI LES SONS

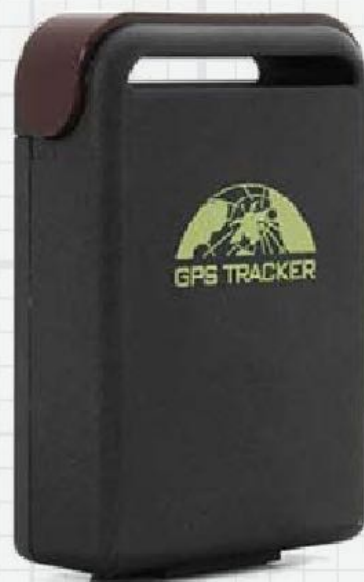
Voici un tracker GPS tout terrain et très bon marché. L'appareil est, en effet, idéal pour connaître la position de votre voiture, de votre valise, de vos enfants ou de votre animal de compagnie. Il suffit de



placer une carte SIM à l'intérieur pour être immédiatement au courant de son emplacement lorsque vous enverrez un SMS. L'appareil dispose aussi d'un bouton alerte qui enverra un SMS au téléphone enregistré. Discret, il est aussi équipé d'un micro

pour entendre ce qui se passe autour du dispositif à distance depuis son téléphone. La fonction GeoFence permet, quant à elle, d'être prévenue lorsque l'appareil sort d'une zone que vous aurez délimitée. L'appareil est aimanté et la boîte contient deux batteries pour ne jamais être à court.

Prix: 76 € Lien: <http://goo.gl/qfxlYU>



Call Recorder for mobile phone, ENREGISTREZ VOS CONVERSATIONS MOBILES

Dans notre numéro14, nous avons testé un dictaphone faisant aussi office d'enregistreur de conversation téléphonique. Grâce à un adaptateur filaire, il était en effet possible d'enregistrer vos appels passés sur téléphones fixes. Ce nouvel appareil fait la même chose avec votre téléphone portable. Une fois couplé à votre appareil via Bluetooth, vous pourrez sauvegarder plusieurs heures de conversation sur les 8Go de mémoire interne (extensible via carte Micro-SD). Attention, selon la loi française, votre interlocuteur doit être prévenu d'un éventuel enregistrement de sa voix.

Prix: 35 € Lien: www.chinavasion.com/dg4i



KeyGrabber ENREGISTRE LES FRAPPES AU CLAVIER

Dans le petit monde des keyloggers (enregistreur de frappe), vous pouvez trouver des logiciels, mais aussi des keyloggers «matériels». Ce sont de petits dispositifs placés entre la prise du clavier et l'ordinateur. Ils ressemblent à des adaptateurs et sont tout à fait discrets, mais attention, ils enregistrent tout sur une mémoire interne! Pour lire le contenu, il suffit de placer le dispositif sur votre PC et de taper un mot de passe. Le transfert des données récoltées se fait automatiquement. Ce keylogger est disponible pour les claviers USB et PS/2 (les prises rondes et violettes). Il est équipé d'une mémoire de 16Mo (de quoi enregistrer 8000 pages de texte), mais n'est malheureusement pas compatible avec les claviers sans fil.

Prix: 35 € Lien: www.keelog.com



DataLocker Sentry, LA CLÉ USB BLINDÉE

Saviez-vous que chaque année dans le monde près de 20 millions de clés USB disparaissent parce qu'elles sont perdues ou volées? Il suffit que la vôtre se retrouve dans ce cas et cela pourrait être l'enfer: photos compromettantes, documents sensibles, adresses, etc. Pour éviter les problèmes, il existe des logiciels de chiffrements, mais ils sont loin d'être très conviviaux. D'autres clés USB misent sur un lecteur d'empreintes digitales, mais ce genre de gadget peut être facilement contourné. DataLocker Sentry est la solution à tous vos problèmes. Le produit se présente sous une forme classique de clé USB à l'extérieur, cependant, c'est à l'intérieur que se fait la vraie différence. En effet, la clé DataLocker Sentry possède un système de cryptage des données de type matériel qui ne perturbe aucunement la lecture et l'écriture. Contrairement aux systèmes de cryptage à base de logiciel. Cela rend la clé totalement plug-and-play avec un cryptage de niveau militaire (FIPS 140-2) et une capacité de stockage de 4, 8 ou 16Go. Notez aussi que la clé possède un revêtement époxy protégeant la puce et la mémoire flash contre les intrusions physiques, l'eau et les poussières.

Prix: entre 60 et 140€ Lien: <http://goo.gl/jVG8Bb>



ESPION

Une multiprise POUR SURVEILLER SON DOMICILE

Quoi de plus anodin qu'une multiprise ? Attention cette dernière est équipée d'un micro-espion fonctionnant sur le réseau GSM ! Il suffit de mettre une carte SIM prépayée et de composer le numéro pour entendre les sons autour de celle-ci. Vous allez pouvoir écouter tout ce qui se passe dans une pièce dans un rayon de 15 à 20 mètres. Il est aussi possible de choisir le mode de détection de bruit. Si un bruit est détecté par ses capteurs, la souris vous alerte via un SMS afin que vous puissiez écouter les sons environnants. Autoalimenté, il n'est même pas nécessaire de la recharger ou de mettre des piles ! Et bien sûr, elle sert aussi de multiprise...

Prix: 80 € Lien: <http://goo.gl/bgBfik>



LE GUIDE DU

Pirate

"LE MAGAZINE
QUI VIENT D'UNE
AUTRE PLANÈTE"

L 14376 - 1 - F: 3,50 € - RD

