N°40 **NOUVELLE FORMULE** + DE PAGES + DE HACKS + DE TUTOS

PIRATE INFORMATIQUE

Fév. / Avril 2019

TOP 8 **HACKING**
SPÉCIAL TECHNIQUES D'ATTAQUES

NUMÉRO SPÉCIAL
ANNIVERSAIRE 10 ANS

COMMENT PIRATER **SKYPE** EN MOINS DE 2 MINUTES ?

CRACKER LES **CARTES DE TRANSPORTS ?**
LES PIRATES S'ABONNENT !

LE GUIDE DU HACKER

PÊCHE AUX **GILETS JAUNES**
LE PARTI PIRATE LEUR TEND LE CROCHET

DÉCOUVREZ LES POUVOIRS DE **WINJA**
LA PROTECTION NOUVELLE GÉNÉRATION

BLACK DOSSIER // *Ne soyez plus esclave*

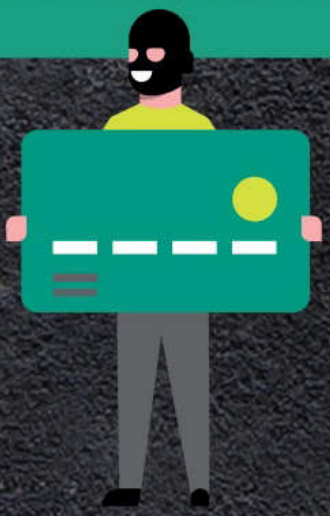
Virez-moi **GOOGLE** par dessus-bord !

TOP 22 DES SERVICES ALTERNATIFS

AU REVOIR!

SOMMAIRE

HACKING



ANONYMAT

SOUTENEZ-NOUS !

Vous découvrez ce magazine en l'ayant téléchargé illégalement ? C'est de bonne guerre, nous sommes pour le partage ! Merci de l'intérêt que vous portez à nos articles, mais pour que nous puissions continuer l'aventure, pensez à acheter le magazine : offrez-le, parlez-en autour de vous ! *Pirate Informatique* existe depuis 10 ans, sans publicité et sans hausse de prix depuis 7 ans.

PROTECTION

MULTIMÉDIA

PIRATE INFORMATIQUE
N°40

Fév. / Avril 2019

Une publication du groupe ID Presse.
Impasse de l'Espéron - Villa Miramar
13960 Sausset Les Pins
E-mail : redaction@idpresse.com

Directeur de la publication : David Côme

Snake : Benoît Bailleul

Raiden & Big Boss : The Lone Gunman & Etienne Sellan

Otacon : Sergueï Afanasiuk

Correctrice : Marie-Line Bailleul

Imprimé en France par / Printed in France by : Léonce Deprez
ZI Le Moulin 62620 Ruitz

Distribution : MLP

Dépôt légal : à parution

Commission paritaire : en cours

ISSN : 1969 - 8631

«Pirate Informatique» est édité par SARL ID Presse, RCS : Marseille 491 497 665
Parution : 4 numéros par an.

ÉDITO

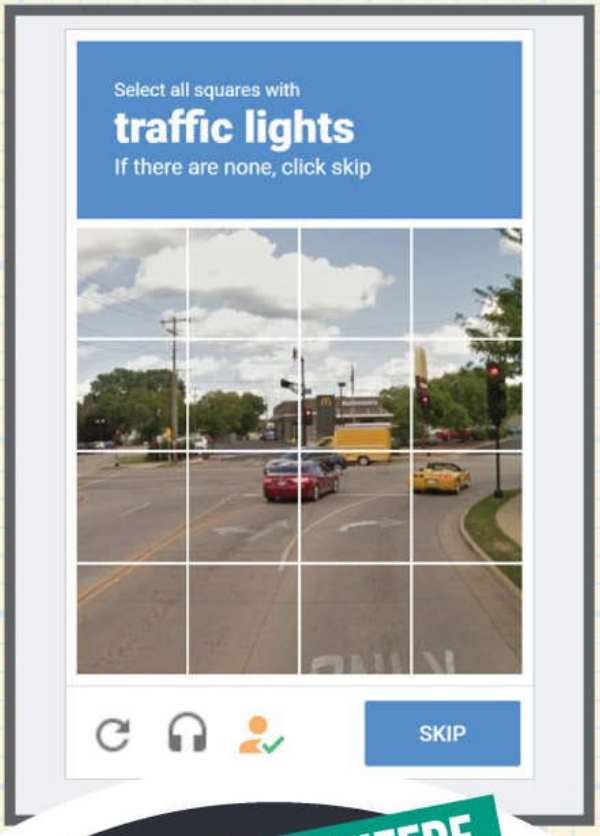
BONJOUR AUX HABITUÉS COMME AUX NOUVEAUX VENUS !

Cela faisait 7 ans que nous n'avions pas changé la formule de *Pirate Informatique*. Nous avons donc profité de l'anniversaire des 10 ans du magazine (qui correspond avec le quarantième numéro) pour faire un coup de propre. Les habitués auront remarqué que le CD n'est plus là. Il faut dire que même si ce dernier avait des adeptes (et même des collectionneurs), ce support est non seulement dépassé, mais presque inutile puisque les choses évoluent vite dans le hacking et qu'il est facile de trouver les logiciels à jour sur Internet en suivant nos liens. Pour compenser ce manque nous avons augmenté le nombre de pages et nous vous préparons une petite surprise que nous mettrons en place pour tous les lecteurs dès le prochain numéro. Outre les rubriques habituelles, vous trouverez chaque mois un grand dossier de plusieurs pages sur un sujet particulier alors n'hésitez pas à nous faire part de vos commentaires et de vos souhaits pour les prochaines éditions sur **benbailleul@idpresse.com**

Bonne lecture et merci pour ces dix dernières années... Vous avez fait de *Pirate Informatique* le seul magazine du genre dans le monde francophone.

Benoît BAILLEUL

EN FINIR AVEC LES CAPTCHAS



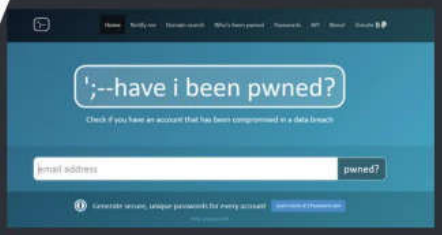
Captcha Solver for Humans est une extension de navigateur pour Mozilla Firefox et Google Chrome permettant de rendre les captchas moins frustrants sur Internet. Vous connaissez certainement ces procédés visant à vérifier que «vous n'êtes pas un robot». Le problème c'est qu'ils sont parfois tellement tordus que vous vous demandez vous-même si vous êtes bien humain. Peut-être avez-vous remarqué que ces captchas disposent d'une alternative sonore au cas où il s'affiche mal ou si la personne est handicapée. C'est là que Captcha Solver for Humans va agir : l'extension va simplement utiliser la reconnaissance vocale pour résoudre les captchas automatiquement afin que vous n'ayez pas à le faire.Il suffit de cliquer sur le bouton d'extension en bas du widget pour lui faire résoudre automatiquement le captcha audio. Facile, mais réservé aux humains !

Lien : **https://frama.link/XsxGTKMv** (Firefox)

Lien : **https://frama.link/csZ46y3H** (Chrome)

LE CHIFFRE

773 MILLIONS



C'est le nombre d'adresses mail contenu dans le fichier «Collection #1». Ce dernier qui a récemment fait son apparition dans les recoins les plus mal famés d'Internet fait beaucoup parler de lui, mais il ne s'agit en fait que d'une super-compilation de données glanées ça et là suite à des vols de données issues de gros sites. Outre ces 773 millions d'e-mails, on trouve aussi 21 millions de mots de passe : idéal pour se faire un petit dico !Même si les personnes les plus avisées ont changé leur mot de passe depuis les vols chez Adobe (2013), Dropbox (2012), Lastfm (2012) ou LinkedIn (2016), il y a fort à parier que les utilisateurs les moins renseignés n'auront rien changé. Imaginez qu'ils utilisent les mêmes mots de passe partout... Pour être sûr que votre e-mail ne se trouve pas dans ce panier de crabes, il suffit d'aller sur le site HaveIBeenPwned : **https://haveibeenpwned.com**. Pour éviter les problèmes avec les mots de passe, rappelons qu'il est possible de se choisir un mot de passe différent pour chaque compte que vous avez sans pour autant les mémoriser puisque Firefox dispose d'un mot de passe principal stocké en local. Vous allez me dire «*Oui, mais là il s'agit d'un vol en ligne*» et vous avez raison, mais commençons déjà par limiter les dégâts potentiels de votre côté. N'oubliez pas non plus de ne jamais utiliser un mot de passe qui veut dire quelque chose (ou qui se trouve dans un dictionnaire) : alternez les capitales, les minuscules, les chiffres et les caractères spéciaux. Activez aussi la double authentification lorsque cela est possible.

«Vous pouvez obtenir des données gratuites pour améliorer votre programme de reconnaissance faciale en créant le 10 years challenge». Pourquoi payer des gens quand vous avez 2 milliards de connards cobayes sous la main ?

LEXIQUE

DARK QUOI ? Il ne faut pas confondre Darknet, Dark Web et Deep Web. Le Deep Web est l'ensemble des sites et pages auxquelles on ne peut accéder par un moteur de recherche classique (sites non indexés), le Dark Net est un réseau parallèle à Internet garantissant l'anonymat et le Dark Web est l'ensemble des sites sur ce dernier.

En Bref...

PIRATAGE DE CRYPTOPIA EXCHANGE

Après MtGox, Bitfinex ou Coincheck, c'est la plate-forme d'échange de cryptomonnaies Cryptopia qui a annoncé avoir été victime d'un piratage informatique. Basé en Nouvelle-Zélande, ce site restera en maintenance, avec une suspension des transactions en attendant que la police fasse son enquête. J'en connais qui vont passer quelques mois au vert...

UNE FAILLE SUR FORTNITE

Le nombre de personnes qui dispose d'un compte au jeu Fortnite est de 200 millions. Un nombre qui attire forcément les pirates de tous bords d'autant qu'une faille a été récemment découverte. Il serait en effet possible de récupérer l'identifiant et le mot de passe des joueurs qui se connectent depuis une application tierce : Facebook, Xbox Live ou Google.

UNE TESLA MODEL 3 PRÊTE À HACKER !

Comme chaque année le concours de piratage Pwn2Own réunit les plus grands hackers de la planète. Cette année il faudra venir à bout du système de sécurité d'une Tesla Model 3, et de prendre le contrôle du véhicule. Le gagnant se verra tout simplement offrir la voiture d'une valeur de 44 000$.

TOP 10 SITES DE TÉLÉCHARGEMENT ILLÉGAUX

NEXTWAREZ.COM

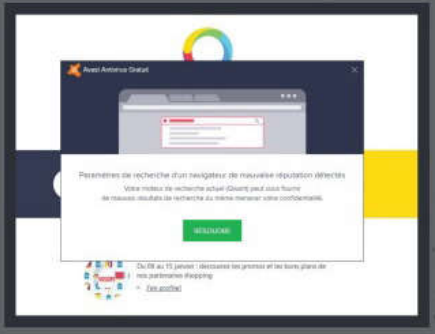
Tous les premiers vendredis du mois, le site NextWarez présente son classement des sites de téléchargement et de streaming les plus visités par les Français...

1.	Annuaire-Téléchargement	Site de DDL généraliste francophone	=
2.	YggTorrent	Tracker torrent francophone généraliste	+3
3.	LibertyVF	Site de streaming & DDL francophone	-1
4.	VoirFilms	Site de streaming généraliste francophone	=
5.	Torrent9	Tracker torrent francophone généraliste	-2
6.	Extreme-Down	Site de DDL généraliste francophone	=
7.	FilmComplet	Site de streaming généraliste francophone	+1
8.	FilmStreaming	Site de streaming généraliste francophone	+2
9.	StreamingDivx	Site de streaming généraliste francophone	RE
10.	FrenchStream	Site de streaming généraliste francophone	-1

Sources : NetxWarez.com

DOWN

L'antivirus gratuit Avast était efficace et discret, mais ce n'est plus le cas depuis longtemps. Dernier débordement en date : Il va regarder quel est le moteur de recherche par défaut et vous avertir d'une menace potentielle si ce dernier n'est pas Google. Normal. Le plus beau c'est que pour vous convaincre de changer, l'antivirus vous préviendra que Qwant (par exemple) peut «*menacer votre confidentialité*». On croit rêver.



Interview de Nicolas Petitdemange, secrétaire national du Parti Pirate français

Entre les prochaines élections européennes de mai 2019 et la main tendue aux Gilets Jaunes, nous avons voulu en savoir plus sur l'actualité du Parti Pirate français, ses ambitions et leur définition de la démocratie.

L'ÉCHÉANCE ÉLECTORALE DU 26 MAI ARRIVE À GRANDS PAS. POUVEZ-VOUS NOUS FAIRE UN ÉTAT DES LIEUX RAPIDE SUR LE NOMBRE DE CANDIDATS QUE VOUS ALLEZ PRÉSENTER ? QUELS SONT VOS OBJECTIFS ? ET EN CE QUI CONCERNE L'ÉTRANGER : A-T-ON UNE CHANCE DE VOIR PLUS D'UN ÉLU DU PP À STRASBOURG ?

Les élections européennes c'est la présentation d'une liste unique sur tout le territoire, donc nous prévoyons la constitution d'une liste paritaire de 75 noms. Notre objectif c'est d'avoir des élus, même si nous savons que ce sera compliqué puisqu'il faut atteindre 5% des votes pour en avoir, donc nous avons fixé un autre objectif, celui de faire une campagne de qualité pour rappeler notre existence et nos idées aux électeurs.

Au niveau européen, nous avons une chance d'avoir 4 à 5 élus, surtout en République tchèque où le Parti Pirate fait d'excellents scores depuis l'an dernier, et au Luxembourg. On espère qu'en Allemagne aussi le Parti Pirate réussira à obtenir un siège malgré la volonté de notre élue européenne Julia Reda de ne pas se présenter à sa succession, volonté que nous saluons puisque nous sommes assez défavorables au cumul des mandats et plutôt favorables au renouvellement de nos représentants. En effet, dans le modèle démocratique que nous défendons, la démocratie liquide, il n'y a pas de représentant. En France, c'est plus compliqué, notre parti n'est pas très connu et nous avons du mal à nous faire entendre, le modèle partisan que nous portons, sans leader, n'est pas un modèle traditionnel, cela fait peur, et cela n'intéresse pas les journalistes qui du coup ne parlent que très peu de nous.

EN QUELQUES LIGNES, POUVEZ-VOUS EXPLIQUER LE PRINCIPE DE DÉMOCRATIE LIQUIDE À NOS LECTEURS ET POURQUOI CE PRINCIPE VOUS TIENT TANT À CŒUR ?

Comme nous l'avons abordé précédemment, la démocratie liquide (ou fluide, ou délégative) est un modèle de démocratie que nous portons dans le débat public avec ardeur. Nous sommes convaincus qu'à l'heure d'Internet nous devons revoir nos schémas de prise de décision. La République et les institutions ont été créées à une époque où une petite partie de la population seulement était en capacité de lire et d'écrire, et donc avait besoin de représentants qui s'exprimeraient et prendraient les décisions en leur nom, à cette époque d'ailleurs, nos élus et les artisans de la République ne considéraient pas qu'elle était démocratique, le mot et le concept de «démocratie» étaient, pour eux, aussi dangereux que le mot et le concept d'»anarchie» l'est aujourd'hui pour la plupart des politiciens. Aussi, c'est assez étonnant de voir avec quelle facilité on prétend vivre dans une société démocratique de nos jours alors qu'il n'en était rien il y a quelques dizaines années.

Ce n'est que tardivement que, pour répondre à une volonté populaire, et pour des questions de communication purement politicienne, certains hommes politiques ont commencé à se revendiquer démocrates, mais dans les faits, le pouvoir n'appartient pas au peuple, et la démocratie ce n'est pas voter pour des gens, c'est voter pour des idées et donner une orientation à la société. Beaucoup de Pirates considèrent aujourd'hui que la République n'est pas démocratique, le pouvoir est confisqué au peuple, il est contraint de le donner à des représentants qui, bien trop souvent, ne représentent que leurs propres intérêts et pas ceux du plus grand nombre.

Aujourd'hui, notre société a bien évolué ce qui rend le modèle républicain tel qu'il a été conçu au départ complètement obsolète. La démocratie liquide est, selon nous et en l'état actuel de notre réflexion, la réponse la plus adaptée au besoin de démocratie émis par une grande partie de la population.

La démocratie liquide c'est un mélange entre la représentativité et la démocratie directe. Il s'agit de donner aux gens la possibilité de décider de participer à la prise de décision ou de déléguer à des personnes en qui ils ont confiance, et selon les sujets traités, cette prise de décision. Nous sommes conscients que tout le monde ne souhaite pas participer aux votes, que des personnes ont encore besoin aujourd'hui de laisser le soin à d'autres de choisir pour eux les orientations de la société dans laquelle ils vivent, c'est pourquoi nous pensons que la démocratie directe, soit l'appel au vote systématique de la population sur toutes les orientations, a ses limites. Il y a, parmi la population, beaucoup de personnes dont les connaissances dans certains domaines dépassent largement celles de leurs concitoyens, et ces personnes ne sont pas forcément celles qui prennent aujourd'hui les décisions.

Nous pensons qu'une personne ne peut pas être compétente dans tous les domaines, et si c'est le cas elle est rarement candidate aux élections, les élus que nous avons ne sont pas suffisamment compétents pour être en capacité de choisir pour nous tous la direction que va prendre notre société, et nous considérons que nous devons mettre fin à la confiscation du pouvoir par des élites.

Nous sommes, nous Pirates, aussi les victimes de ce système républicain ultra capitaliste qui ne laisse aujourd'hui que les riches accéder au pouvoir et qui leur permet de le conserver.
En effet, nous sommes un parti politique qui ne survit que grâce aux adhésions et aux dons, nous n'avons aucun élu et tant que nous n'avons pas d'élu nous n'avons aucun autre moyen de nous financer, car aujourd'hui, le système des partis politiques est tel que seuls les partis déjà au pouvoir, ou ceux qui ont suffisamment de moyens pour réaliser de bonnes campagnes de communication et donc d'obtenir suffisamment de voix aux élections, bénéficient de l'aide de l'état pour survivre. La démocratie liquide nécessite donc un engagement individuel quotidien, elle supprime toute notion de personne, de mandat, puisque si nous pouvons déléguer nos voix selon les sujets à n'importe quel moment à une ou plusieurs personnes, nous pouvons aussi choisir de retirer nos délégations à n'importe quel moment du processus.
Ainsi, personne n'est assuré de conserver ses voix toute sa vie ou sur un mandat d'une certaine durée. Ce système ne peut cependant fonctionner que si l'on accepte, dès le départ, de supprimer l'anonymat du vote. En effet, ce système ne peut fonctionner que grâce aux outils numériques ce qui implique une transparence totale du processus de décision. Mais comme dans ce modèle, il n'est plus question de vote sur des personnes, mais sur des idées, on perd la notion de représentativité et tout ce qui entoure cette notion, comme par exemple la possibilité qu'une seule personne détienne tous les pouvoirs, donc on perd par la même occasion la notion de mandat et toute pression individuelle sur le vote est retirée, la seule pression qui subsiste est celle de la société et de son bien-être, les citoyens devront donc assumer leurs choix. Nous estimons que même si cela implique une libération de beaucoup de paroles plus ou moins radicale, cette transparence de la prise de décision est une nécessité pour une société plus sereine.

LE SOUTIEN AUX GILETS JAUNES N'A PAS DÛ ÊTRE UNE CHOSE FACILE À DÉCIDER. QU'EST-CE QUI VOUS A POUSSÉ À LE FAIRE ? QUELS SONT LES POINTS QUE VOUS AVEZ EN COMMUN ? COMMENT COMPTEZ-VOUS LEUR APPORTER VOTRE AIDE ?

Nous avons été approchés par les Gilets Jaunes à plusieurs reprises et de différentes manières. Comme il s'agit d'un mouvement protéiforme sans leader, nous avons été approchés par des personnes qui ne se connaissaient pas les unes les autres, mais qui avaient visiblement un objectif commun, celui de pratiquer la démocratie. Nous avons en commun avec eux le fait de ne pas avoir de leader et de nous exprimer publiquement par le biais de porte-paroles, nous avons aussi en commun le fait de souhaiter de grandes modifications dans notre société pour une démocratie réelle, ouverte et transparente, et nous sommes d'accord pour dire que notre République française n'est pas démocratique, comme nous l'avons expliqué précédemment, et ne permet pas un débat ouvert et public ou chacun peut prendre la parole et s'exprimer.
Nous avons donc collectivement rédigé une proposition de motion que nous avons soumise à l'ensemble des Pirates par notre Assemblée Permanente de décembre et qui a été adoptée par une large majorité d'entre nous (87%).
Il nous a fallu pas moins d'un mois pour rédiger, amender et voter ce texte de manière à ce qu'il colle au plus près à notre positionnement, nous ne voulions pas apporter un soutien de forme comme d'autres partis populistes l'ont fait, nous souhaitions tendre la main aux Gilets Jaunes pour leur donner l'opportunité de tester notre organisation et nos outils de prise de décision, pas forcément en adhérant au Parti Pirate, mais en leur rappelant notre existence, en leur expliquant nos statuts et en leur mettant à disposition notre outil de démocratie interne développé sur mesure pour nous et par nous : Congressus. Nous avons peut-être été un peu maladroits dans notre communication, car beaucoup de ceux qui ont vu passer l'information se sont arrêtés au titre «le Parti Pirate soutient les Gilets Jaunes», et nous avons reçu un accueil plutôt positif bien que parfois assez brutale suite à cette publication, mais nous rappelons à nos détracteurs que nous prenons nos décisions collectivement et de manière réfléchie, et que si certains sont déçus par cette orientation, la porte du Parti Pirate est toujours ouverte, la seule manière d'influer sur l'orientation de notre parti politique c'est d'adhérer et de proposer des orientations au collectif, chez nous il n'y a personne qui a la main sur notre parti si ce n'est la totalité d'entre nous.
Donc pour résumer, nous n'appelons pas forcément nos adhérents à manifester, drapeau à la main, aux côtés des Gilets Jaunes, les Pirates sont libres de ne pas en avoir envie tout comme ils sont libres d'y aller, et nous n'avons pas envie que notre position soit prise pour une forme de récupération politique, ça n'est pas notre volonté, les Gilets Jaunes sont libres de nous rejoindre tout comme nous sommes libres de les rejoindre, mais même si ces deux mouvements ont énormément de points communs, nous ne nous envisageons pas comme le parti des Gilets Jaunes mais plutôt comme une organisation politique qui peut les aider à poser des mots sur leurs idées, à décider de leurs orientations et à se comprendre eux-mêmes. Nous envisageons notre soutien plutôt sous la forme d'une aide technique, d'un apport de connaissances, d'un partage d'expérience, car nous avons expérimenté plusieurs modèles et nous estimons aujourd'hui que le fonctionnement que nous avons adopté l'an dernier est le plus adapté aux revendications que nous portons depuis le début de notre existence, ainsi qu'aux revendications des Gilets Jaunes, c'est pourquoi nous nous tenons à leur disposition et nous espérons avoir la possibilité de travailler avec chacun d'entre eux en bonne intelligence.

LE PARTI PIRATE A BESOIN DE VOUS !

Fondé en 2006, Le Parti pirate est un parti politique créé sur le modèle de son homologue suédois. Sa devise est «*liberté, démocratie, partage*». Son programme se développe sur la base de la protection des droits et libertés fondamentales, aussi bien dans le domaine numérique qu'en dehors : légalisation du partage hors marché, la lutte contre le fichage abusif, l'indépendance de la justice, la transparence de la vie politique et l'ouverture des données publiques.
Si vous voulez adhérer : **https://adhesion.partipirate.org**
Si vous souhaitez faire un don : **https://don.partipirate.org**

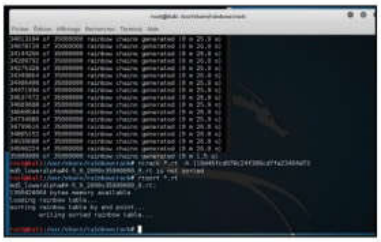
SÉLECTION

TOP 15 SÉLECTION DE LOGICIELS

Vous vous demandez quel logiciel choisir pour tel ou tel usage ? En cherchant sur le Net, vous vous retrouvez avec des produits incomplets ou payants ? Dans chaque numéro, retrouvez ici notre Top 5 dans 3 catégories. La crème de la crème !

TOP5 CRACK

RAINBOWCRACK



Au lieu de vérifier si tel mot de passe correspond au hash de départ, puis de refaire la même opération jusqu'à trouver le bon sésame, le principe de rainbow table diffère quelque peu. Il s'agit d'une technique de « compromis temps-mémoire » réduisant considérablement le temps nécessaire pour casser un mot de passe... Il faut pour cela télécharger ou se confectionner ses rainbow tables, mais les résultats sont là.

Lien : **http://project-rainbowcrack.com**

HASHCAT

Le meilleur logiciel pour cracker des mots de passe à partir de hash. 160 types de hash pris en compte, 5 différents types d'attaque et des options à n'en plus finir. Il est complexe, mais s'il ne faut en choisir qu'un...

Lien : **https://hashcat.net/hashcat**

CRARCK

Si vous avez oublié le mot de passe d'une archive créée avec 7-Zip, Crarck va vous aider ! Ce logiciel de brute force utilise toute la puissance de votre processeur graphique pour venir à bout des mots de passe les plus solides...

Lien : **www.crark.net/crark-7zip.html**

JOHN THE RIPPER

John the Ripper est un logiciel de cassage de mots de passe : un «crack» du crack. Plusieurs techniques sont à sa disposition. Le mode simple va essayer plusieurs mots de passe en fonction du nom d'utilisateur, le «brute force» et l'attaque par dictionnaire. Il dispose d'une version avec interface graphique disponible sous Linux et Windows appelée Johnny.

Lien : **www.openwall.com/john**

FCRACKZIP

fcrackzip permet de récupérer les mots de passe de fichiers ZIP. En plus d'être gratuit et open source,il a l'avantage de proposer l'attaque par dictionnaire en plus du brute force. C'est un logiciel assez vieux, mais qui fonctionne à merveille avec les archives utilisant le ZipCrypto (mais pas l'AES)

Lien : **http://goo.gl/y8Lbsx**

TOP5 SAUVEGARDE

COBIAN BACKUP

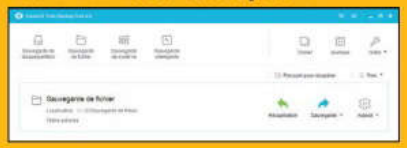
Gratuit et régulièrement mis à jour Cobian permet de faire des sauvegardes standards ou incrémentielles qui peuvent être chiffrées, compressées et surtout programmées. C'est le logiciel que nous conseillons aux débutants.

Lien : **www.cobiansoft.com**

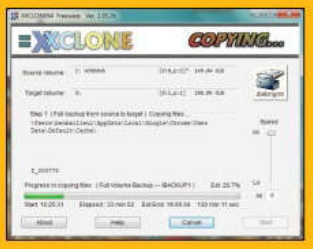
EASEUS TODO BACKUP

Un autre logiciel spécialisé dans les sauvegardes avec des tonnes d'options sympas. Il est gratuit, mais pas open source. Il est donc éliminé d'office si vous désirez stocker des données sensibles.

Lien : **www.todo-backup.com**



XXCLONE



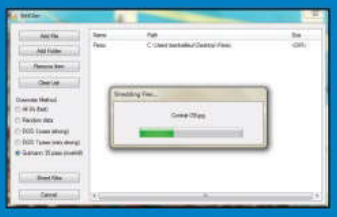
Pourquoi faire des sauvegardes alors que vous pouvez carrément cloner votre disque dur principal avec XXClone ? Le logiciel dispose de pas mal d'options et n'est jamais inutilement compliqué.

Lien : **www.xxclone.com**

TOP5 EFFACEMENT/RÉCUPÉRATION DE FICHIERS

BITKILLER

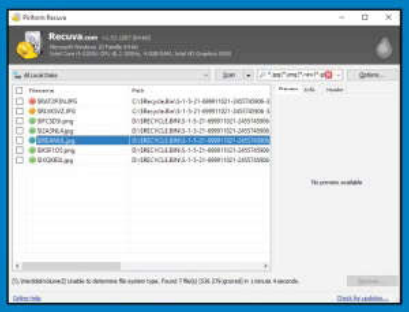
Si vous avez beaucoup de fichiers à effacer de manière sécurisée (vente d'un PC familial avec des photos, etc.), le mieux est d'utiliser un logiciel qui va non seulement effacer les données, mais réécrire plusieurs fois là où elles étaient stockées. BitKiller va réécrire sur votre fichier, réinitialiser la taille à 0 octet, le renommer de manière aléatoire jusqu'à 10 fois et l'effacer encore une fois. Avant cela, le logiciel propose plusieurs types d'effacement : placer des 0 en lieu et place de chaque bit, écrire des données aléatoires ou chiffrées jusqu'à 35 fois (méthode «Peter Gutman»). Pour Linux, vous avez Bleachbit.



Lien : **https://sourceforge.net/projects/bitkiller**

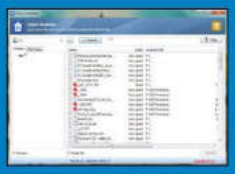
RECUVA

Vous avez vidé la corbeille de Windows alors que des documents importants s'y trouvaient ? Ce n'est pas bien grave si vous utilisez le logiciel Recuva. Faites un clic droit dans la Corbeille recherchez vos fichiers depuis le menu contextuel. Au bout de quelques secondes, le programme vous dressera la liste des fichiers qu'il a retrouvés. Les pastilles vertes indiquent que les fichiers sont encore «entiers». Attention, certains n'auront plus leur nom d'origine.



Lien : **www.recuva.fr**

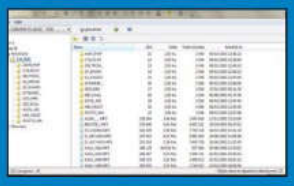
GLARY UNDELETE



Vous vous êtes trompé de lettre de lecteur au moment de formater, vous avez cliqué sur **Couper** ou lieu de **Copier** ou vous avez tout simplement écrasé les données sans faire attention ? Avec Glary Undelete, vous allez pouvoir récupérer les données de vos clés USB ou cartes mémoire. Cliquez sur les cases correspondantes aux fichiers que vous voulez restaurer et c'est tout !

Lien : **www.glarysoft.com/glary-undelete**

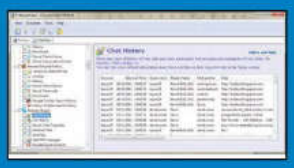
ISOBUSTER



Les CD, DVD ou Blu-ray que nous gravons avec notre matériel n'est pas aussi solide que ce que les fabricants ont voulu nous faire croire. En plus d'être fragiles, ils résistent mal au temps et aux UV. Il arrive souvent qu'une vieille galette refuse de se lancer ou de transférer certains fichiers (erreur de redondance cyclique, etc.). Après avoir bien nettoyé votre disque, lancez IsoBuster. Attention, certaines fonctions sont payantes.

Lien : **www.isobuster.com**

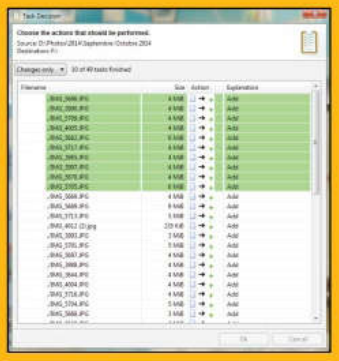
R-WIPE&CLEAN



Sans verser dans la paranoïa, il suffit de vendre votre PC pour que le nouvel acquéreur puisse déterrer beaucoup de données confidentielles. Dans le cas inverse, si vous êtes acquéreur d'un PC d'occasion, vous aimeriez sans doute effacer toutes traces de fichiers illégaux ou de consultation de sites louches. R-Wipe&Clean va effacer de manière irréversible vos activités en ligne et hors ligne avec des algorithmes très efficaces. Le logiciel est gratuit et complet pendant 30 jours.

Lien : **www.r-wipe.com**

FULLSYNC



Sauvegarde ou synchronisation entre tous vos appareils, FullSync s'occupe de tout ! FullSync est un outil universel de synchronisation et de sauvegarde de fichiers personnalisable et customisable. Créé spécialement pour les développeurs, il est tellement simple que n'importe qui peut l'utiliser.

Lien : **http://fullsync.sourceforge.net**

SYNCTHING

Syncthing permet de synchroniser vos fichiers depuis tous vos appareils sans passer par un serveur distant. Il s'agit en fait d'une solution de partage en local accessible à distance et chiffrée (AES+TLS). Il est possible de spécifier des répertoires sur plusieurs machines pour centraliser ses fichiers. Vous n'aurez plus à aller chercher ou transférer vos données pour en profiter sur la machine de votre choix.

Lien : **https://syncthing.net**

LES DOSSIERS DU Pirate

DES DOSSIERS THÉMATIQUES COMPLETS

À DÉCOUVRIR EN KIOSQUES

- PETIT FORMAT
- MINI PRIX
- CONCENTRÉ D'ASTUCES

100% Windows

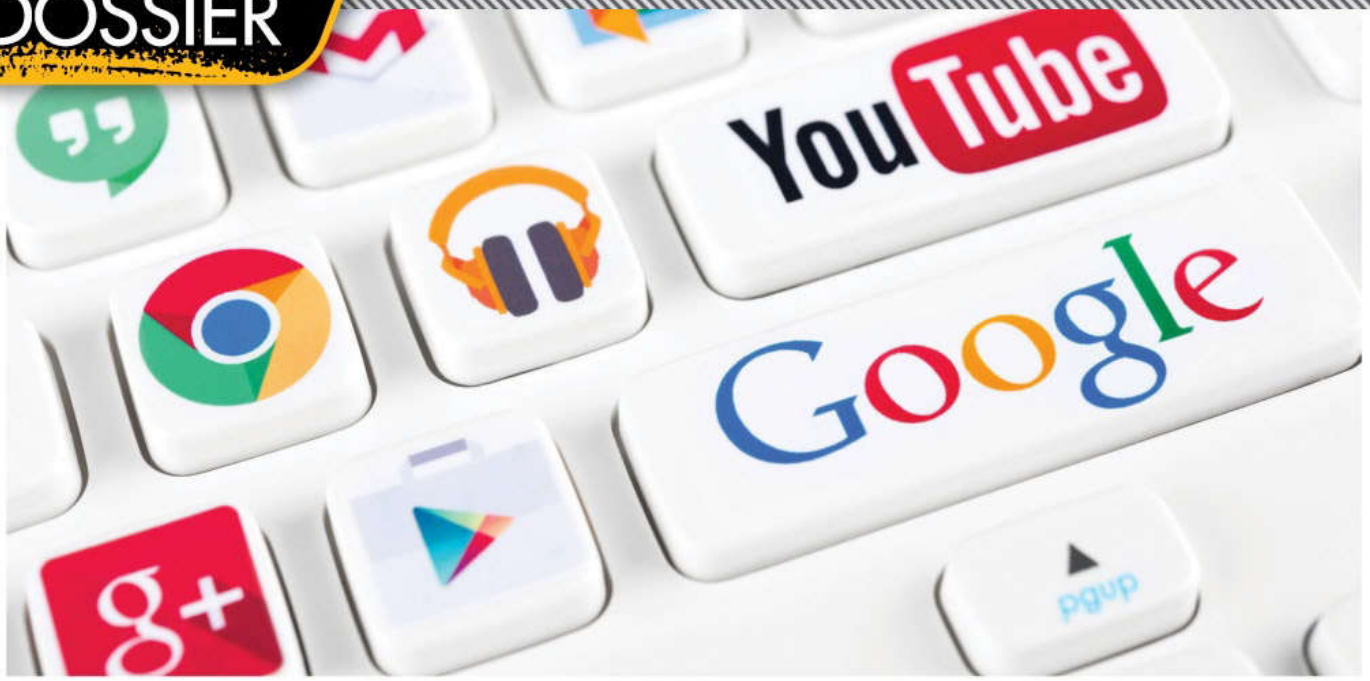
Actuellement #Guide pratique

BEST-OF HACKING 2019

VIREZ-MOI GOOGLE PAR DESSUS-BORD !

TOP 22 DES SERVICES ALTERNATIFS

Virer Google, d'accord, mais pour trouver des services moins efficaces, moins pratiques et peut-être tout aussi dangereux pour mes données et ma vie privée ? C'est toute la gageure de ce dossier : tous les services présentés ici sont gratuits, considèrent la sécurisation de vos données comme prioritaire... et sont vachement bien. Voilà.



Il y a cinq ans, Google vous connaissait déjà mieux que votre mère. Pourquoi pas. Mais depuis quelques mois, votre malaise grandit. Il commence même à deviner ce que vous ne savez pas encore de vous-même et vous révèle/suggère/impose régulièrement des désirs, idées et projets jusqu'alors insoupçonnés. Tiens, même de nouveaux amis.
Il semble vous entendre quand vous chuchotez à voix basse et il se comporte de plus en plus comme un majordome (excellent par ailleurs) directif et intrusif.
Raaâh, et cette manie de ne plus vous lâcher d'une semelle ! Il garde un œil par dessus votre épaule où que vous soyez. Pas un seul endroit où un appareil connecté ne vous suive. Qui est devenu le maître de qui ?

ÉTIQUETAGE, TRIAGE... ET LIBRE-ARBITRE ?

Une cure sans Google s'impose... ne serait-ce que pour retrouver ce qui vous définit : vous, et vous seul. Parce ce que se retrouver dans la case 87b74dd23 de l'algorithme du géant américain, on n'est pas sûr que ce soit très valorisant comme identité. Surtout quand on s'angoisse à l'idée qu'une fois étiqueté, la gare de triage automatisée ne soit jamais très loin...

Google nous offre à tous (et gratuitement!) un majordome d'exception pour nous aider au quotidien. Une relation maître-esclave typique… c'est à dire ambigüe

GOOGLE ENCORE CONDAMNÉ... MAIS PAS PRESSÉ

Droit européen, information de l'utilisateur et transparence : Google traîne les pieds... et se fait condamné en France.

Fin janvier, Google a été condamné à une amende record de 50 millions d'euros suite à la mise en cause, en France, de sa politique de gestion des données personnelles. Cette condamnation intervient après des plaintes collectives déposées devant la CNIL par les associations None of Your Business et La Quadrature du Net.

Traitements massifs et intrusifs

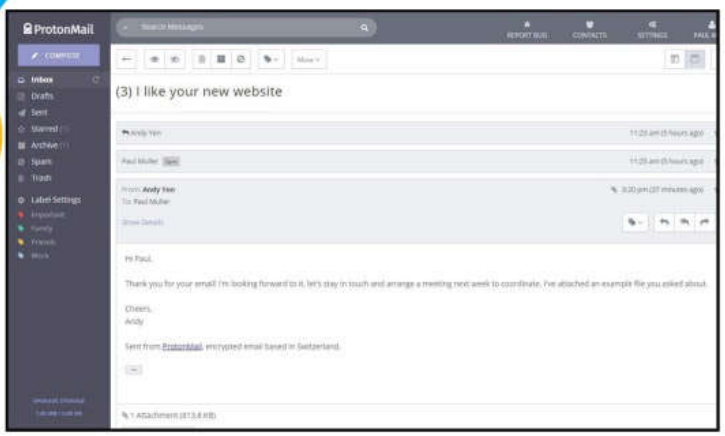
Malgré la mise en place de la RGPD en Europe, censée protéger les citoyens et leur vie privée sur Internet, la CNIL estime que Google a poursuivi une stratégie ne laissant que trop peu de place au consentement de ses utilisateurs quant à l'utilisation de leurs données personnelles. Les internautes français ne seraient ainsi « pas en mesure de comprendre l'ampleur des traitements mis en place par Google. Or, ces traitements sont particulièrement massifs et intrusifs », estime la CNIL, en référence à la galaxie des services proposés par le groupe : Google Search, YouTube, Google Maps, Play Store, Google Photos...

Par défaut, Google impose aussi le partage par lot d'un certain nombre de données, données dont les finalités restent obscures et inintelligibles pour le commun des mortels (voir pour tout le monde). La CNIL demande plus de transparence et de contrôle pour chacun. Les observateurs estiment qu'il s'agit là d'un premier fil tiré par la commission mais que cette victoire en appelle d'autres.

3 ALTERNATIVES À GMAIL

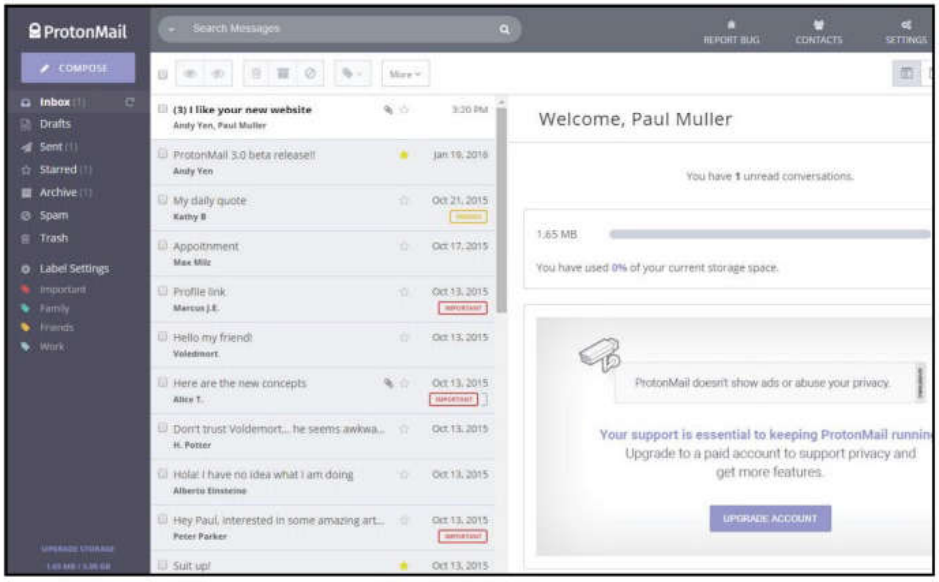
1# PROTONMAIL

LE CHOIX DE LA RÉDACTION

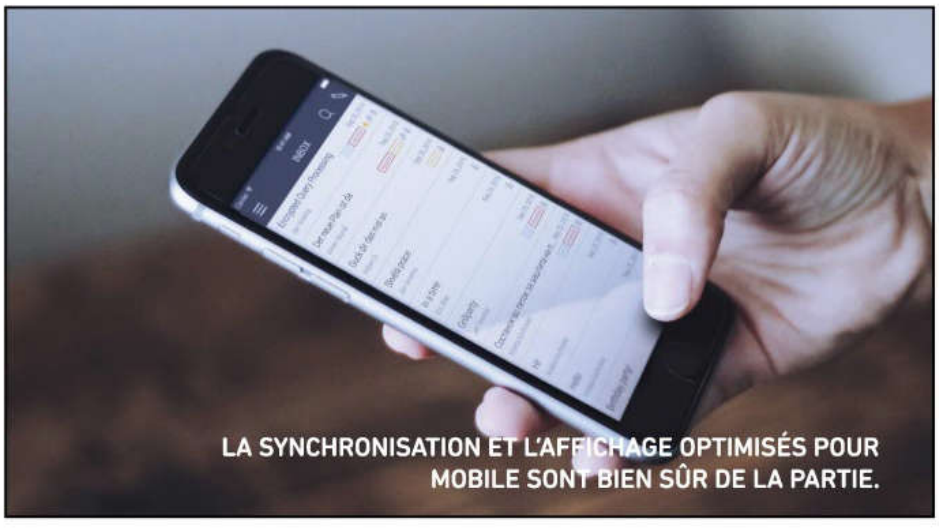


Développé par des chercheurs du CERN et du MIT, ProtonMail propose un chiffrement de vos échanges mails de bout-en-bout, sans que personne ne puisse y jeter un œil indiscret. Un plus grand respect de la vie privée et plus de sécurité comparé aux autres solutions de messagerie puisque la compagnie est incapable de lire les messages des utilisateurs. C'est la grande différence par rapport aux autres services de messagerie – comme Gmail donc. Depuis 2017, ProtonMail dispose de sa version 100 % francophone et de 5 Gb de stockage gratuits. Ajoutées à cela une ergonomie et des fonctionnalités proches de Gmail, une sécurisation de votre liste de contacts et un data center réputé inviolable sous les montagnes suisses : what else ?

Lien : **protonmail.com**



ProtonMail offre la meilleure offre de stockage gratuit (5 Gb) parmi les trois solutions proposées ici



2 DRIVES ALTERNATIFS

1# SYNC

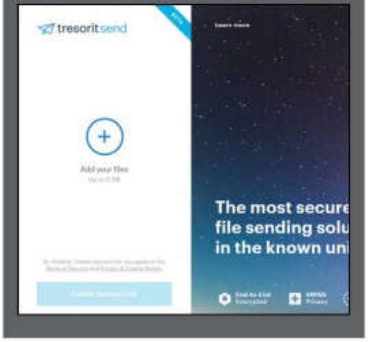
Encrypté de bout en bout, 5 Gb dans sa version gratuite. Partage et accès même sans compte Sync pour les invités : c'est simple et complet !

Lien : **www.sync.com**

2# TRESORIT

Tout pareil que Sync avec ses 5 Gb offerts et son encryption. Mais, par contre, pas de gestion collaborative, le service est principalement destiné à l'échange sécurisé de gros fichiers.

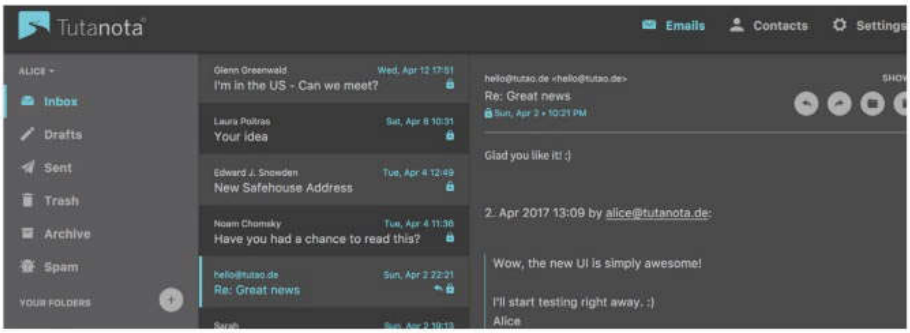
Lien : **send.tresorit.com**



2# TUTANOTA

Le mot Tutanota est dérivé du Latin et contient les mots «tuta» (sécurisé) et «nota» (message, note). Voici pour l'étymologie de cette messagerie gratuite et open source développée à Hanovre, en Allemagne. Tutanota est gratuite dans sa version « 1 Go de stockage » pour les particuliers. Avec le chiffrement de bout-en-bout et l'A2F, personne (y compris Tutanota) ne peut déchiffrer ou lire vos données. Des versions mobiles Android et iOS sont bien sûr disponibles.

Lien : **tutanota.com**



3# MAILFENCE

Pour Mailfence, « le respect de la vie privée, c'est un droit et pas une fonctionnalité ». La messagerie est complètement exempte de publicité et l'éditeur s'engage à n'envoyer aucun spams ni sollicitations, à ne jamais commercialiser sa base d'utilisateurs ou partager leurs données avec des tiers et précise que son certificat SSL/TLS ne comporte aucune autorité de certification américaine dans sa chaîne de certification. Créée et hébergée en Belgique, Mailfence insiste sur l'importance de cette domiciliation et ne pas être, comme ses confrères européens présentés ci-contre, sous la juridiction des «gag orders» ni des «National Security Letters» américains. La version gratuite de Mailfence propose 500 Mb de stockage.

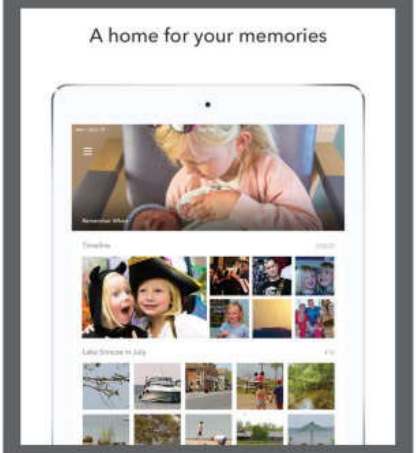
Lien : **mailfence.com**

2 GOOGLE PHOTOS ALTERNATIFS

1# SHOEBOX

Même dans version gratuite, Shoebox vous offre un stockage illimité pour vos photos... et le tout sécurisé par une bonne dose d'encryption. Accédez à vos clichés sur tous les supports puisque Shoebox est compatible Windows, Mac, iOS etAndroid.

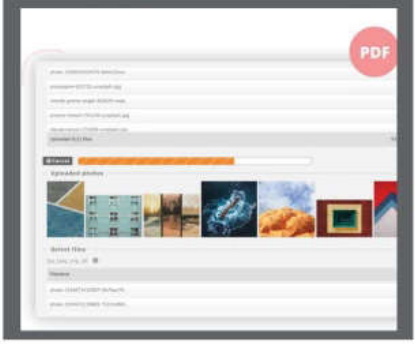
Lien : **shoeboxapp.com**



2# PIWIGO

Sans pub et open source, Piwigo présente l'avantage de proposer une version en français. Cet excellent gestionnaire de photothèque ne gère par contre pas le stockage (il vous faut un hébergement ailleurs) dans sa version gratuite pour particuliers.

Lien : **fr.piwigo.com**



GMAIL, VOTRE MEILLEUR ENNEMI

Gmail est le coeur de la stratégie Google, tous ses services passent par la création d'un compte idoine. C'est la porte d'entrée marketing la plus puissante du géant américain puisque tous vos messages et connexions sont scannés et les datas ainsi collectées alimentent ses outils à des fins pratiques mais aussi publicitaires. Et depuis que Google permet aux éditeurs de solutions tierces d'utiliser vos logins Gmail comme moyen d'identification, ces mêmes sociétés sont autorisées à accéder à une partie de vos données privées et de les mouliner dans leurs système d'apprentissage automatique.

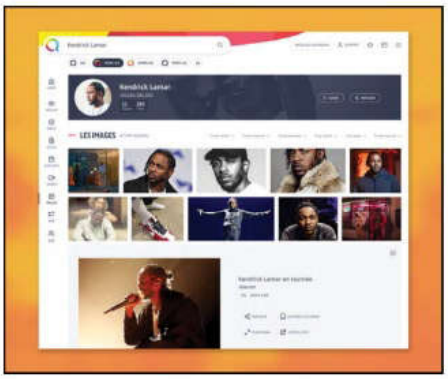
3 MOTEURS DE RECHERCHE ALTERNATIFS

1# QWANT

Vous le savez, Qwant est depuis quelques années le chouchou de la rédaction. Peut-être y-a-t-il ici quelque chauvinisme puisque Qwant est un moteur de recherche franco-européen. Mais c'est surtout l'esprit, l'ambition technique affichée et la qualité finale du search engine qui nous séduisent et en font un concurrent crédible à Google pour tous les amoureux de la protection des données. Entre 50 et 70 millions d'utilisateurs l'auraient déjà adopté selon des analyses indépendantes.

NEUTRALITÉ DES RECHERCHES

Preuve de sa maturité, Qwant est devenu le moteur de recherche par défaut du Ministère français des armées depuis octobre dernier. Qwant n'installe pas de cookies traceurs et ne piste pas ses utilisateurs, le seul cookie présent n'existe que durant la session et est supprimé immédiatement après. Les résultats affichés sont neutres et ne sont pas personnalisés d'après un historique de recherche comme pour Google, Qwant n'en possédant pas, mais dépendent uniquement des tendances du moment, en partie d'après les réseaux sociaux. Qwant ambitionne de devenir un véritable écosystème de services (comme Google) avec un module de paiement sécurisé intégré mais aussi d'autres outils grand public comme Qwant Junior, Qwant Music (partenariat avec Qobuz!), Qwant Boards ou le petit dernier Qwant Maps (toujours en mode test).

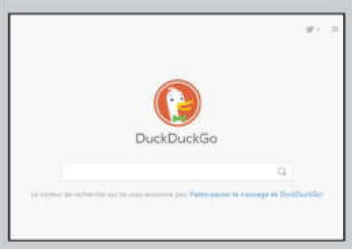


Lien : **www.qwant.com**

QWANT MUSIC DÉMONTRE QUE QWANT S'ATTAQUE À TOUS LES AXES DE RECHERCHE EN LIGNE, SURTOUT CEUX QUI SONT DEVENUS LE QUOTIDIEN DU GRAND PUBLIC. LES FONCTIONNALITÉS SONT MODERNES ET ERGONOMIQUES, À L'IMAGE DES AUTRES SERVICES DU MOTEUR DE RECHERCHE FRANÇAIS.

2# DUCKDUCKGO

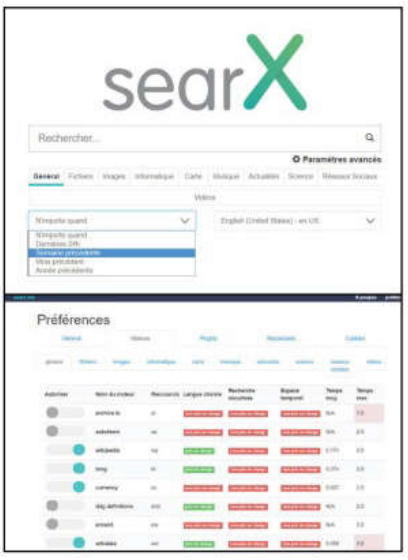
Au niveau mondial, DuckDuckGo est le principal concurrent sécurisé au moteur de recherche de Google. Très agréable à utiliser (pages Web, photos et vidéos), il ne profile pas ses utilisateurs et assure ne pas permettre aux sites tiers de le faire, ne collecte pas leur données de connexion et promet d'afficher pour tous les mêmes résultats de recherche, basés uniquement sur la pertinence et l'objectivité de son algorithme. N'ayant pas de fonctionnalités payantes, le moteur de recherche relaie cependant des liens sponsorisés. En installant sa version PC (ou mobile), vous intégrez aussi de façon sécurisée d'autres moteurs de recherche tels que Youtube, Amazon, Google Image ou encore Wikipedia.



Lien : **duckduckgo.com**

3# SEARX

Searx est un méta-moteur de recherche open source qui rassemble les résultats d'autres moteurs de recherche tout en respectant la confidentialité des utilisateurs. Searx est personnalisable en indiquant les sources de recherche que vous préférez et vous pourrez affiner les résultats via différentes catégories.



Lien : **searx.me**

LA FORCE DE SEARX, C'EST LA POSSIBILITÉ D'AFFINER LES RÉSULTATS PAR CATÉGORIE, DATE ET LANGUE DE RECHERCHE AINSI QUE VIA LES « PRÉFÉRENCES » QUI VOUS PERMETTENT DE CHOISIR LES SOURCES DE RECHERCHE À PRIVILÉGIER OU À BANNIR.

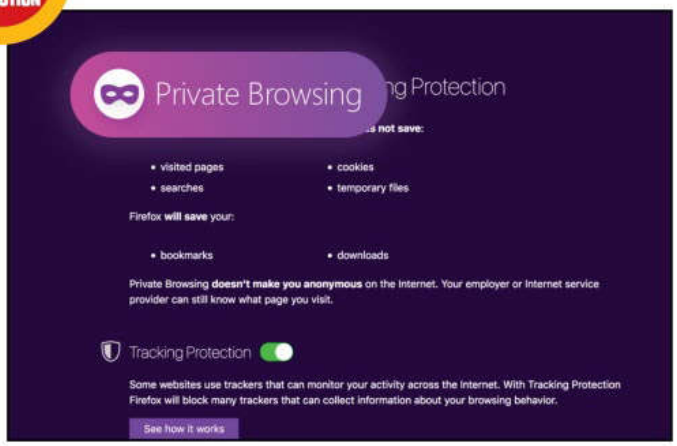
3 NAVIGATEURS ALTERNATIFS

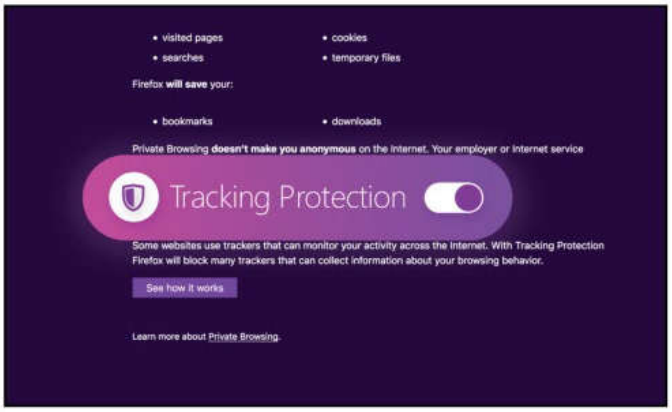
1# FIREFOX QUANTUM

LE CHOIX DE LA RÉDACTION

Il y a 10 ans, il était au coude à coude avec Chrome pour détrôner Microsoft Internet Explorer. Las, la puissance de feu de Google a relégué ce très bon navigateur au second rang. Mais l'esprit frondeur et libertaire des débuts (open source, non lucratif, protecteur) a perduré et s'est même accentué grâce à des moyens financiers importants et une communauté de développeurs de haut niveau parmi la Fondation Mozilla. Notamment sur la synchronisation PC et mobiles, Firefox est l'un des navigateurs les plus puissants et agréables.

EN NAVIGATION PRIVÉE, FIREFOX BLOQUE LES TRAQUEURS TANDIS QUE LA PROTECTION CONTRE LE PISTAGE POUR DÉSACTIVER LES MOUCHARDS DU WEB EST À ACTIVER EN UN CLIC.





NOYAU PROTECTEUR, PLUG-INS PUISSANTS

Aujourd'hui, un Firefox bien configuré reste le navigateur Internet le plus protecteur et le plus sécurisé de sa catégorie. Car au-delà de ses qualités intrinsèques et les dizaines de réglages dédiées à la protection de vos données, il existe aussi de nombreux plug-ins sécurisés qui vous permettront de personnaliser votre expérience sans rien sacrifier à la performance et à l'ergonomie (contrairement à Tor).
Pour être clair, vous devez mettre la main dans le moteur mais, contrairement à Google, Firefox favorise cette prise de contrôle et rend toutes ses options « Vie privée » très accessibles. Il nous faudrait plusieurs pages vous vous montrer l'étendue de ses possibilités alors, promis, nous vous guiderons pas à pas dans l'un de nos prochains numéros.

Lien : **www.mozilla.org**

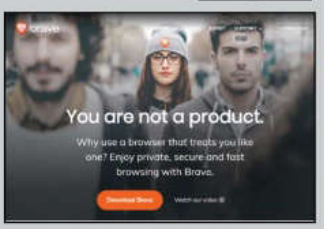
2# TOR BROWSER

Ici, l'objectif c'est la protection et l'anonymat les plus poussés possibles, certainement pas l'ergonomie. Le navigateur Tor Browser est moche, pas de services ou de menus novateurs : mais il fait le job ! Basé sur Firefox quand même, Tor Browser est conçu et configuré pour naviguer de façon anonyme et ultra sécurisée sur les réseaux Internet et Tor. Il bloque certains programmes JavaScript (quitte à bousiller certaines pages Web) et privilégie les connexions sécurisées. Moins de plaisir, plus de sécurité. Camarade, choisis ton camp.

Lien : **www.torproject.org**

3# BRAVE

Un petit gars tout ce qu'il y a de sympathique... qui annonce quand même des affichages de pages jusqu'à 8 fois plus rapides que Google Chrome sur mobile et jusqu'à 2 fois plus rapides sur PC. La raison ? Basé sur Chromium, Brave a poussé aussi loin que possible la suppression de toutes les collectes et injections de données, le plus souvent synonyme de traçage et d'espionnage marketing. Du coup, l'utilisateur retrouve un navigateur sécurisé et allégé, sans perdre ses habitudes de navigation.



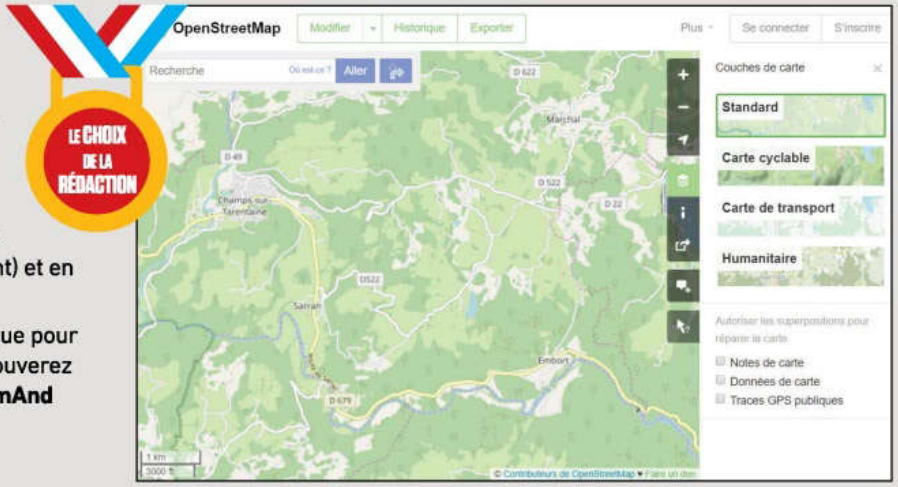
Lien : **brave.com**

2 MAPS ALTERNATIVES

1# OPENSTREETMAP

OpenStreetMap est un service de cartographie gratuit et open source, ce qui signifie que de nombreux développeurs se le sont approprié pour proposer leur propre outil personnalisé, pour plusieurs plateformes (PC, Mac, Android, iOS notamment) et en ajoutant des fonctionnalités bienvenues.

La base OpenStreetMap a cependant été conçue pour un environnement Windows/PC. Mais vous trouverez des variantes mobile comme l'application **OsmAnd** (Android et iOS).

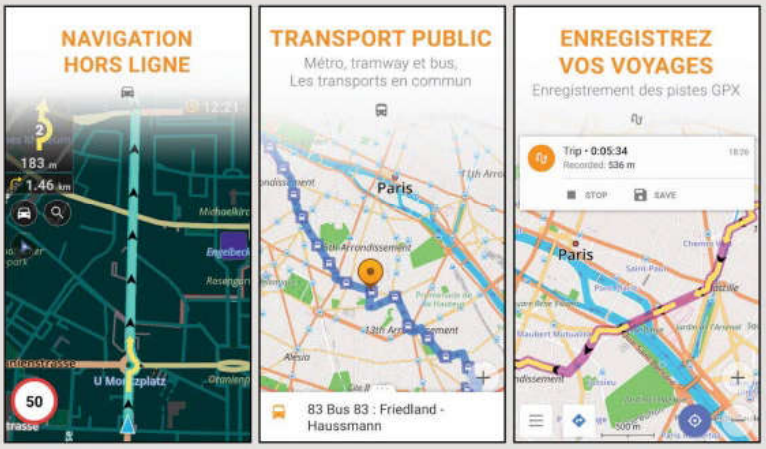


PAS DE COMPTE, PAS DE PUB

Le gros plus de OpenStreetMap et de ses déclinaisons, contrairement à Google Maps, c'est de pouvoir utiliser le services sans compte associé, c'est à dire en évitant le tracking centralisé même si la localisation GPS est bien sûr un impondérable la plupart du temps. La désactivation du GPS est cependant très simple et vos informations de localisations peuvent être maintenues complètement privées.

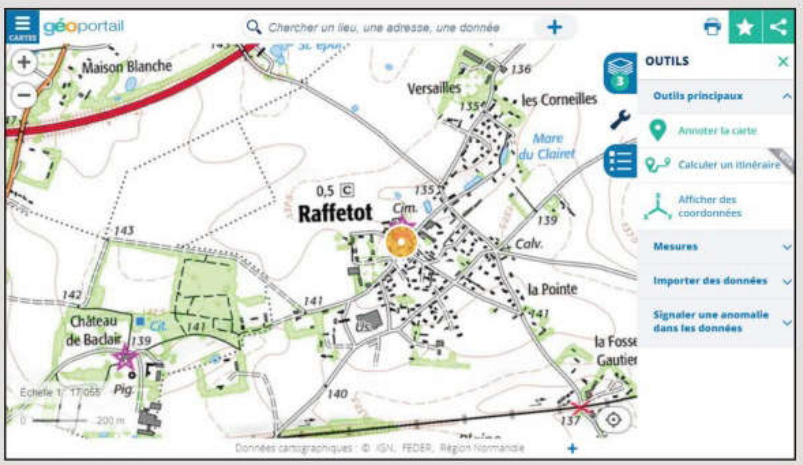
Lien : **www.openstreetmap.org**

OPENSTREETMAP EST UNE BASE LIBRE ET OPEN-SOURCE DONT DE NOMBREUX DÉVELOPPEURS SE SONT EMPARÉ POUR PROPOSER DES SERVICES DE CARTOGRAPHIE MULTIPLATEFORME, INCLUANT BIEN SÛR IOS ET ANDROID



2# GÉOPORTAIL

Alors les petits gars, cela vous ébouriffe le poil que nous vous proposions un service gouvernemental parmi notre sélection. Passez un peu d'huile de coco sur votre pelage velu et tout se passera bien. Géoportail est un excellent service qui exploite les données cartographiques publiques (IGN et BRGM) sur le territoire français. Pas de connexion obligatoire, pas de conservation de vos données privées, pas de publicité et une précision meilleure que Google Maps pour la France rurale. Le service public, ça a du bon, préservons-le et soutenons-le. Des applications mobiles (iOS et Android) complètent la version desktop. Cartographies 2D et 3D, cadastres, chemins de traverse, topographie, lieux-dits improbables, itinéraires bien sûr : l'essentiel et même plus est sur Géoportail. Le seul bémol, vous l'aurez sans doute compris, c'est que vous êtes limités au territoire français pour accéder à l'ensemble de ces fonctions.



Lien : **www.geoportail.gouv.fr**

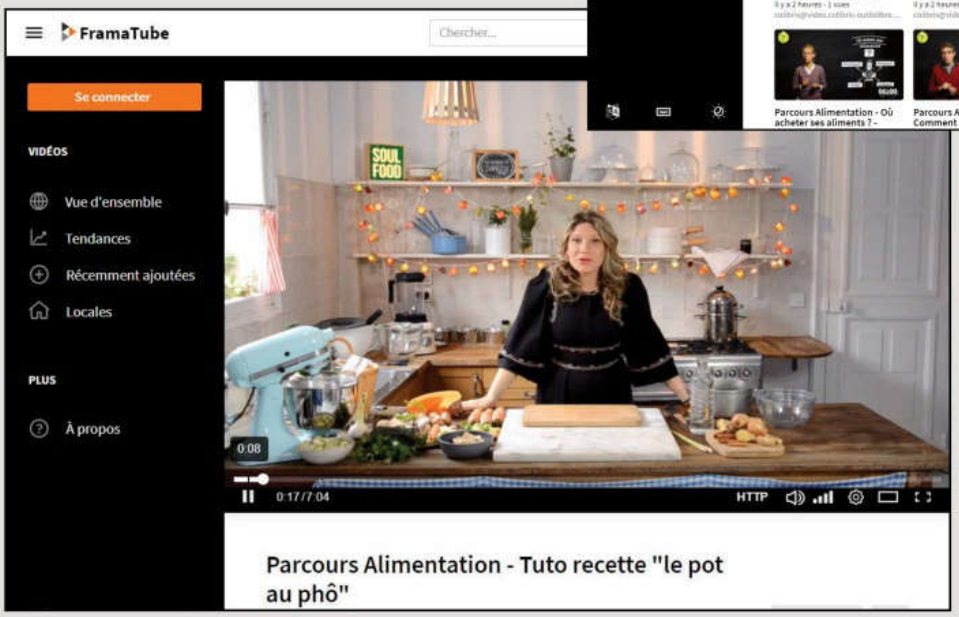
2 ALTERNATIVES À YOUTUBE

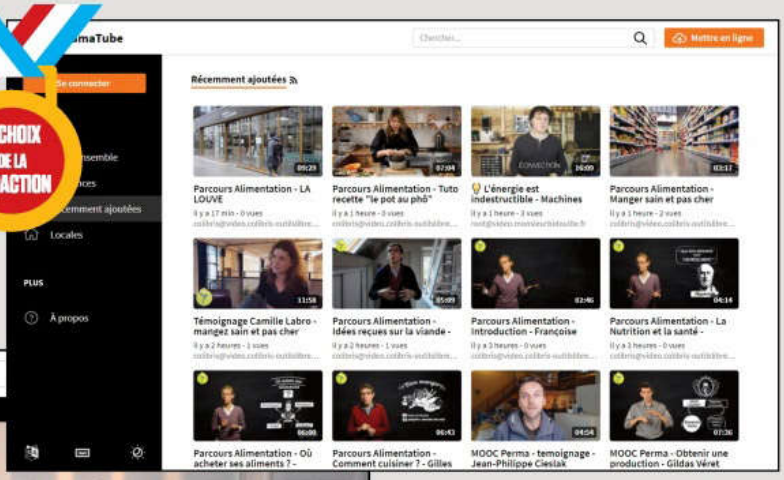
1# FRAMATUBE

Framasoft

Framatube, plateforme développée par Framasoft, héberge des milliers de vidéos et refuse tout tracking de ses utilisateurs. Ici, pas d'hébergement centralisé, ce sont les utilisateurs qui forment un réseau de type P2P pour mutualiser bande passante et espace de stockage grâce à leur propre PC ou serveur.

LE CHOIX DE LA RÉDACTION





Une économie de coût qui permet de se passer de publicité (mais pas de dons) et qui rompt avec la culture centralisée et propriétaire de YouTube. L'interface est une réussite et votre vie privée est garantie par Framasoft, l'un des piliers les plus anciens du logiciel libre en France. Même l'outil de mise en ligne obéit à cette logique et Framatube ne restreint pas le type de contenus publiés (contrairement à YouTube encore) tant que la loi est respectée.

Lien : **framatube.org**

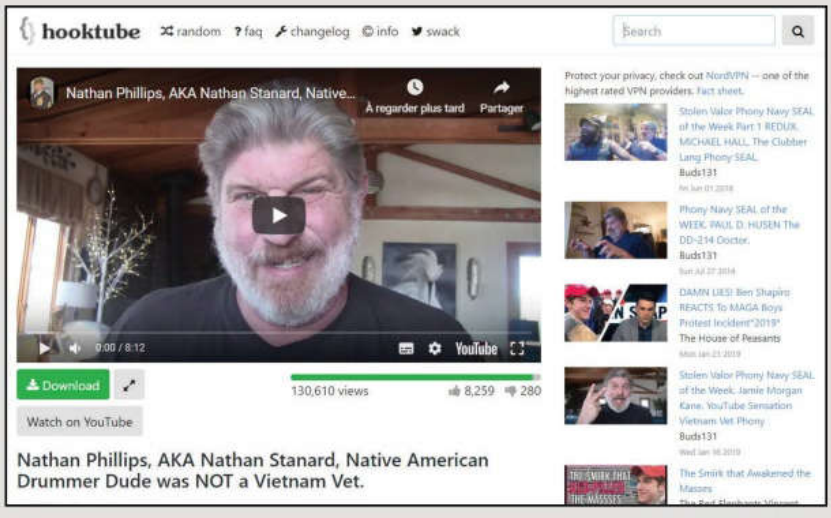
2# HOOKTUBE

hooktube

On ne va pas se mentir, l'hégémonie de YouTube signifie aussi que, côté contenus, il est impossible de trouver plus fourni et diversifié (même si certaines vidéos sont bannies selon le type de contenu ou la zone géographique de consultation). Difficile de s'en passer donc. Plutôt que de créer une concurrence illusoire, HookTube a eu une idée simple et géniale : pouvoir consulter n'importe quelle vidéo de YouTube... mais en bloquant toutes les pubs, requêtes de tracking et enregistrements de données de la plateforme américaine ! Pour ce faire, il vous suffit de remplacer la racine YouTube de n'importe quel lien par « hooktube.com ». Exemple :

« *https://youtube.com/watch?v=S6b0kFLrsAc* » devient « *https://hooktube.com/watch?v=S6b0kFLrsAc* ». Aussi simple que cela.

Lien : **hooktube.com**



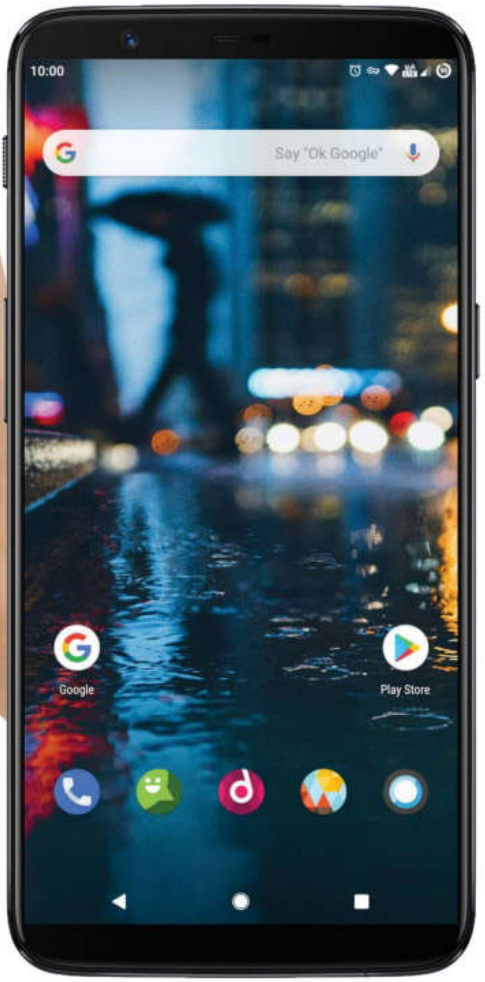
5 ALTERNATIVES À ANDROID

C'est la nouvelle bataille à mener pour les défenseurs de la vie privée : se réapproprier le contrôle sur leurs smartphones, tablettes, TV et objets connectés. Jamais la technologie n'aura permis une telle collecte croisée de données depuis la généralisation dans nos vies de ces nouveaux « assistants » (géolocalisation, recherches, échanges textes et vocaux, enregistrement de la voix, caméras, etc.). Le législateur peine à se faire entendre, voir se désintéresse de la question par manque de compréhension de cette révolution techno.

Pour l'écosystème Apple, il n'existe qu'une solution : ne pas acheter. iOs étant fermé et 100 % propriétaire, il n'y a rien à faire à part effectuer les maigres réglages autorisés par Apple sur ses appareils.

ANDROID : DISTRIBUTIONS ALTERNATIVES

Pour Android, c'est un peu différent car il faut se rappeler que le système d'exploitation de Google est basé sur une solution open source. Des développeurs s'échinent encore et toujours à produire des distributions alternatives (firmware alternatif, ROM alternative) du système d'exploitation Android et principalement basées sur l'Android Open Source Project (AOSP). Le plus connu est LineageOS, qui a pris la suite de CyanogenMod.
Mais attention, pour réussir à réinstaller sur vos appareils ce type de distribution, il faut rooter ces derniers et il peut y avoir de la casse. Vérifiez toujours que votre modèle est compatible avec telle ou telle distribution et suivez scrupuleusement les tutoriels en ligne qui vous guideront pas à pas en fonction de celui-ci.



UN SMARTPHONE ANDROID COMME UN AUTRE ? SAUF QU'IL TOURNE SOUS CRDROID !

VOICI NOTRE SÉLECTION DE CINQ DISTRIBUTIONS ALTERNATIVES :

	NOM	SITE	OPEN SOURCE	VERSION D'ANDROID	NOMBRE D'APPAREILS SUPPORTÉS
1	**LineageOS**	lineageos.org	Oui	9.0 Pie	183
2	**Resurrection Remix Team**	www.resurrectionremix.com	Oui	9.0 Pie	62
3	**Paranoid Android**	aospa.co	Oui	9.0 Pie	47
4	**Pixel Experience**	download.pixelexperience.org	Oui	9.0 Pie	38
5	**crDroid**	crdroid.net	Oui	9.0 Pie	37

TUTO

POUR QUI ?
Pour les curieux

POUR QUOI FAIRE ?
Pour en savoir plus sur les pistes magnétiques

RETRO ENGINEERING ET BIG DATA : JOUONS AVEC LES BANDES MAGNÉTIQUES !

LEXIQUE

***RETRO-ENGINEERING :**
La rétro-ingénierie, ou ingénierie inversée, consiste à étudier un objet pour en déterminer le fonctionnement interne ou la méthode de fabrication.

***BIG DATA :**
Le big data, littéralement «grosses données», désigne des ensembles de données extrêmement volumineux.

Vous avez toujours eu envie de savoir comment fonctionnaient les cartes magnétiques ? Nous allons prendre l'exemple des tickets Tisséo avec notre ami The Lone Gunman qui nous avait déjà montré comment il était possible de gruger les fontaines à soda chez KFC (voir notre n°35) ou de faire joujou avec les vignettes Crit'Air (n°36)... Et comme il est très sympa, il vous a mis tous les outils dans un lien unique à télécharger !

L'objectif de cet article n'est pas de faire de faux tickets de métro, mais de découvrir le lecteur de bande magnétique MSR605X, puis de «retro-engineerer» le contenu d'une bande magnétique sans faire d'effort grâce au «big data». Dans certaines villes les tickets de métro contiennent sur leur bande magnétique toutes les informations d'état du ticket, c'est-à-dire que les informations changent à chaque utilisation et qu'elles ne sont pas sur un serveur distant. Nous allons étudier ici les tickets Tisséo du réseau de transports en commun de Toulouse et sa région.

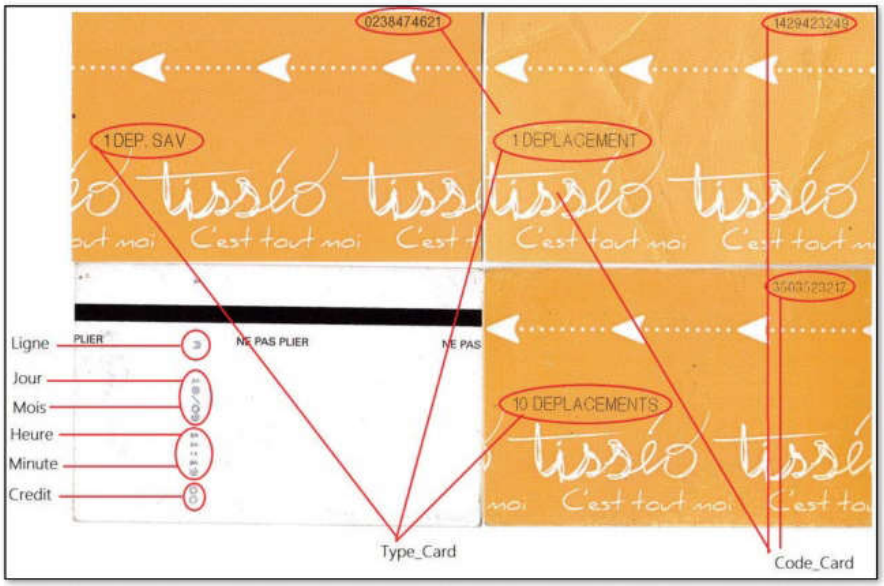
MSR605X EST UN APPAREIL QUI PERMET DE LIRE ET D'ÉCRIRE SUR DES CARTES À BANDE MAGNÉTIQUE. LA COMMUNICATION AVEC L'ORDINATEUR ET L'ALIMENTATION SE FONT VIA UN SEUL CÂBLE USB. IL EST LE PLUS SOUVENT AVEC UN LOGICIEL QUI PEUT LIRE, CLONER ET ÉCRIRE DES DONNÉES. ON EN TROUVE À MOINS DE 90 € SUR INTERNET.

ANALYSE DES CARTES MAGNÉTIQUES TISSÉO

PRATIQUE

01› CE QU'IL NOUS FAUT...

Pour cela il nous faut un lecteur de bande magnétique ! La partie écriture n'est pas nécessaire dans ce tuto, mais peut être utile pour faire ses propres tickets. Ainsi le lecteur/réécriveur polyvalent choisi ici est le MSR605X. Comme on va faire un peu de big data, il faut de la data dans notre cas : plein de cartes de métro !

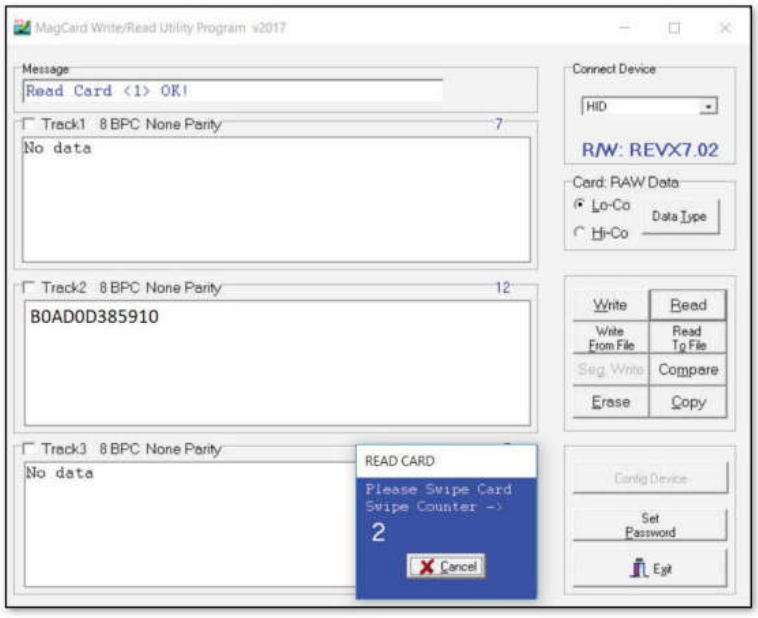


02› LES DONNÉES D'ENTRÉE ET DE SORTIE

Il faut mettre le maximum de données concernant nos cartes dans un fichier. Nous mettrons donc dans un fichier CSV les informations écrites sur le verso c'est-à-dire la ligne de métro/bus empruntée, le jour, le mois, l'heure, les minutes, le nombre de crédits restant et sur le recto le numéro de la carte. Cela constituera nos données d'entrée. Nos données de sortie à prédire correspondront donc au contenu de la bande magnétique.

03› PASSAGE D'UNE CARTE DANS LE LECTEUR ET RÉCUPÉRATION DU CODE DE LA BANDE MAGNÉTIQUE (MODE RAW)

Après avoir passé la carte dans la machine, il faudra transformer le code retourné par le MSR605X en binaire (conversion hexadécimal vers binaire). Ici, B0AD0D385910 se convertit en 48 bits 0 ou 1.
B0AD0D385910 = 101100001010110100001101001 1100001011001000100000
Le premier bit nous l'appellerons C1, le deuxième C2, le i ème bit Ci, et le dernier C48.
Nous recherchons donc la relation entre ces 48bits et nos variables d'entrée. On a donc une relation Sortie=Fonction(C1,C2,C3,...,C48)



INFOS [R ; Rstudio ; Le script Tisseo_ANALYSE.R
Un faux jeu de test représentant 1000 cartes Tisséo]
Où le trouver ? [https://frama.link/qYwXPaNE] Difficulté :

04 › LE LOGICIEL R

Nous allons utiliser le logiciel R pour faire l'analyse de notre lot de cartes (un lot d'entraînement contenant 80% des cartes et un lot de test pour valider le résultat de l'algorithme). R est un logiciel libre destiné aux «sciences des données « permettant d'analyser des données très facilement avec des algorithmes puissants et précodés. Pour cela, utilisons la capacité **Recursive Partitioning and Regression Trees** du logiciel pour trouver si le type de carte peut être déterminé avec les variables C1 à C48 (cette partie est réalisée dans le script en appelant l'algorithme sur notre jeu de données, voir ceci dans le script Tisseo_ANALYSE.R)

```
classifier = rpart(formula = Type_Card  ~
C1+C2+C3+C4+C5+C6+C7+C8+C9+C10+C11+C12+C13+C14+C15+C16+C17+C18+C19+C20+C21+C22+C23+C24+C25+C26+C27+C28+
C29+C30+C31+C32+C33+C34+C35+C36+C37+C38+C39+C40+C41+C42+C43+C44+C45+C46+C47+C48, data = training_set)
```

La matrice de confusion nous montre que le modèle a prédit à 100% le type de carte, aucun faux positif ni faux négatif, seule la diagonale est remplie.

> CONFUSION_MATRIX

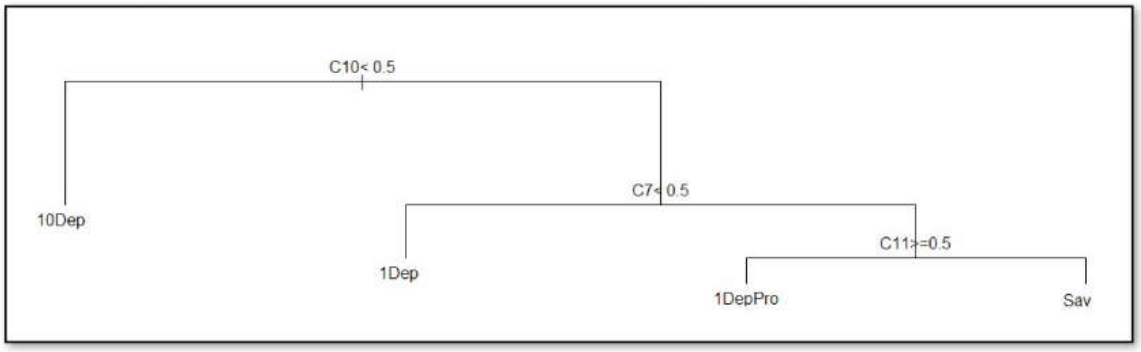
TYPE_CARD_PREDICT VERSUS REAL

	10Dep	1Dep	1DepPro	Sav
10Dep	**96**	**0**	0	0
1Dep	0	**100**	0	0
1DepPro	0	0	**3**	0
Sav	0	0	0	**1**

NOTA BENE : une matrice de confusion permet de voir à partir d'un jeu de test la capacité de l'algorithme à donner une bonne réponse. Dans l'exemple suivant, 96 cas de cartes avec 10 déplacements ont été détectés comme des cartes avec 10 déplacements. Si seulement la diagonale est remplie, l'algo trouve 100% de bonnes réponses. Sinon on aurait eu des faux positifs ou négatifs, par exemple une carte 10 déplacements serait détectée comme une carte 1 déplacement si on avait 1 dans la case en jaune.

05 › LE «CLASSIFIER»

La représentation graphique du «classifier» nous dit qu'il faut utiliser C10,C7,C11 pour déterminer le type de carte. Un classifier est un algorithme qui permet de classifier automatiquement des data en plusieurs groupes. Ici l'auteur a demandé à l'algo de lui classifier les cartes automatiquement en 4 groupes (10 déplacements, 1 déplacement, 1 déplacement pro, 1 Sav) à partir des variables d'entrée lues sur la bande magnétique (C1 à C48) et automatiquement il indique :



-Si C10 est égale à 0 alors c'est un ticket 10 dép
-Sinon si C7 est égale à 0 alors c'est un ticket 1 dép
-Sinon si C11 est égale à 0 alors c'est un ticket 1 dép pro
-Sinon c'est un ticket Sav

Cherchons maintenant si le **Code_Card** est présent dans la bande magnétique. Pour cela utilisons le **Fitting Linear Models** du logiciel R pour trouver si le type de carte peut être déterminé avec les variables C1 à C48.

```
regressor = lm(formula = Code_Card ~ C1+C2+C3+C4+C5+C6+C7+C8+C9+C10+C11+C12+C13+C14+C15+C16+C17+C18+C19
+C20+C21+C22+C23+C24+C25+C26+C27+C28+C29+C30+C31+C32+C33+C34+C35+C36+C37+C38+C39+C40+C41+C42+C43+C44+C4
5+C46+C47+C48, data = training_set)
summary(regressor)
```

06› LES RÉSULTATS

Le coefficient **Multiple R-squared = 1** nous montre que le modèle a prédit à 100% la détermination du numéro écrit sur le recto de la carte. Le test de la **PValue** sur chaque variable (ainsi que la petite étoile) nous indique les variables utilisées pour calculer le fameux numéro. Les **PValue** de C13 à C44 sont minimum avec des coefficients multiples de 2.

COEFFICIENTS: (13 NOT DEFINED BECAUSE OF SINGULARITIES)

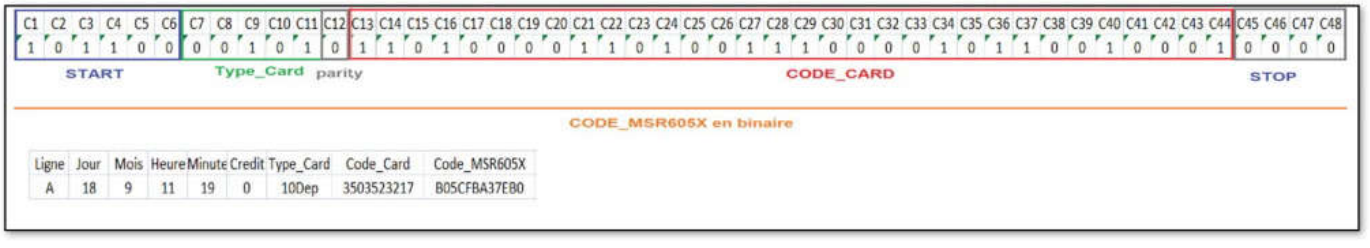
Estimate	Std.	Error	t	value	Pr(>|t|)	
(Intercept)	-5.127e-06	1.397e-06	-3.671e+00	0.000259	***	
C1	NA	NA	NA	NA		
C2	NA	NA	NA	NA		
C3	NA	NA	NA	NA		
C4	NA	NA	NA	NA		
C5	NA	NA	NA	NA		
C6	NA	NA	NA	NA		
C7	-5.486e-07	1.408e-06	-3.900e-01	0.696892		
C8	NA	NA	NA	NA		
C9	6.260e-06	1.955e-06	3.202e+00	0.001423	**	
C10	NA	NA	NA	NA		
C11	-6.537e-06	1.904e-06	-3.434e+00	0.000628	***	
C12	NA	NA	NA	NA		
C13	2.147e+09	4.840e-07	4.437e+15		<2e-16	***
C14	1.074e+09	4.782e-07	2.245e+15		<2e-16	***
C15	5.369e+08	4.440e-07	1.209e+15		<2e-16	***
C16	2.684e+08	4.437e-07	6.050e+14		<2e-16	***
C17	1.342e+08	4.374e-07	3.069e+14		<2e-16	***
C18	6.711e+07	4.371e-07	1.535e+14		<2e-16	***
C19	3.355e+07	4.365e-07	7.686e+13		<2e-16	***
C20	1.678e+07	4.371e-07	3.839e+13		<2e-16	***
C21	8.389e+06	4.367e-07	1.921e+13		<2e-16	***
C22	4.194e+06	4.376e-07	9.584e+12		<2e-16	***
...	...	...	...	...	...	...
C35	5.120e+02	4.363e-07	1.174e+09		<2e-16	***
C36	2.560e+02	4.450e-07	5.752e+08		<2e-16	***
C37	1.280e+02	4.451e-07	2.876e+08		<2e-16	***
C38	6.400e+01	4.407e-07	1.452e+08		<2e-16	***
C39	3.200e+01	4.400e-07	7.273e+07		<2e-16	***
C40	1.600e+01	4.366e-07	3.665e+07		<2e-16	***
C41	8.000e+00	4.340e-07	1.843e+07		<2e-16	***
C42	4.000e+00	4.418e-07	9.053e+06		<2e-16	***
C43	2.000e+00	4.357e-07	4.591e+06		<2e-16	***
C44	1.000e+00	4.349e-07	2.300e+06		<2e-16	***
C45	NA	NA	NA	NA		
C46	NA	NA	NA	NA		
C47	NA	NA	NA	NA		
C48	NA	NA	NA	NA		

*Signif. codes: 0 '***' - 0.001 '**' - 0.01 '*' - 0.05 '.' - 0.1 ' ' - 1*
Residual standard error: 6.043e-06 on 764 degrees of freedom
Multiple R-squared: 1, Adjusted R-squared: 1
F-statistic: 6.215e+29 on 35 and 764 DF, p-value: < 2.2e-16

07› CONCLUSION

Les autres informations comme le nombre de crédits ou autre date/heure n'étant pas présent sur le ticket, on en déduit que toutes les informations associées aux tickets sont sur des serveurs distants, on ne peut donc pas modifier le nombre de crédits en changeant une information de la bande magnétique. Les tickets Tisseo sont donc mieux protégés que la moyenne des tickets de métro/bus français. Félicitons l'équipe de développement ! Avec le MSR605X on peut explorer d'autres bandes magnétiques, voici par exemple une carte visa... Si vous désirez aller plus loin, l'auteur recommande le livre de Patrick Gueulle «*Cartes Magnétiques et PC*» ainsi que ce PDF : **https://frama.link/PPtK8X1w**

Les colonnes C1 à C6 ainsi que C45 à C48 sont à N/A car toutes les valeurs sont identiques (cela veut dire que les bits START et nos bits STOP ne changent jamais). Le bit C12 est à N/A alors que ses valeurs varient. Cela signifie qu'il peut être déterminé à partir des autres colonnes, l'utilisation d'une fonction de régression comme précédemment sur C12 nous montre sa dépendance avec les bits C7 à C11. Nous avons donc des bits de START de C1 à C6, l'encodage du type de carte de C7 à C11, un bit de parité en C12 calculé sur les bits de C7 à C11. Finalement le code écrit sur le recto du ticket codé sur un entier 32bits de C13 à C44 avec les bits de poids fort coté C13 et des bits de STOP de C45 à C48.



Ligne	Jour	Mois	Heure	Minute	Credit	Type_Card	Code_Card	Code_MSR605X
A	18	9	11	19	0	10Dep	3503523217	B05CFBA37EB0

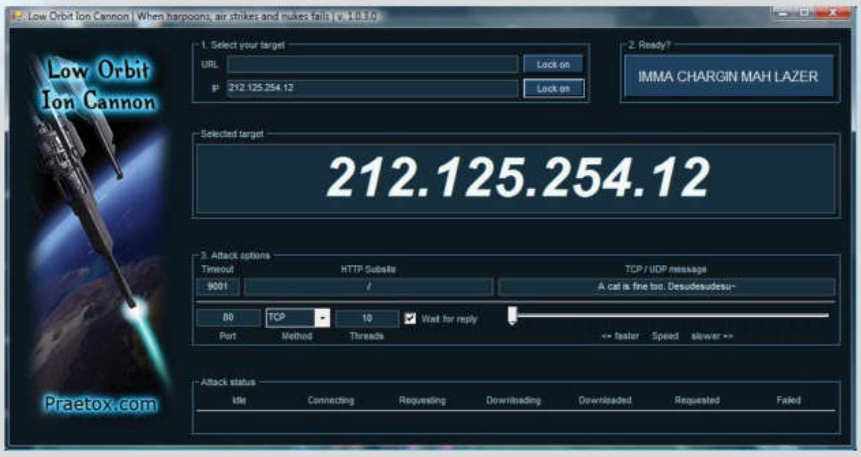
DECRYPTAGE

LE POINT SUR LES TECHNIQUES D'ATTAQUE DES HACKERS

On entend souvent parler de tel hacker ayant mis tel serveur à genou en utilisant une attaque DDoS ou une injection SQL sans vraiment savoir de quoi il retourne. Même si nous ne dévoilons rien de sensible dans ces techniques, voici une petite explication pour chaque cas.

DDOS

L'attaque DDoS (pour Distributed Denial of Service ou «déni de service» en français) vise à saturer de requêtes un site pour qu'il ne soit plus en mesure de répondre. Il y a quelques années, le groupe de hackers Anonymous l'a utilisée pour son projet Payback dont le but était de se venger des majors. Grâce au logiciel LOIC (comme le «Low Orbit Ion Cannon» de L'Empire contre-attaque) distribué gratuitement et avec la complicité d'une communauté d'internautes, Anonymous avait rendu inopérants les sites de la MPAA (Motion Picture Association of America), de la RIAA, etc. Mais ce genre d'attaque n'a pas toujours un but si «noble».



Avec l'augmentation des échanges commerciaux sur Internet, le nombre de «chantage au déni de service» est apparu. Il s'agit pour un pirate de lancer une attaque DDoS contre une entreprise et de lui demander une rançon pour la faire cesser. Pas très sport.

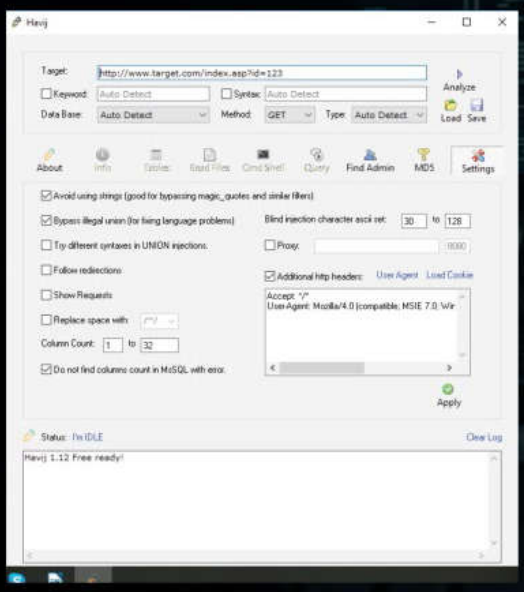
LE LOGICIEL LOIC PERMETTANT DES ATTAQUES DDOS PLANIFIÉES À L'AVANCE

BUFFER OVERFLOW

Un «débordement de tampon» (non, ce n'est pas sale !) consiste à écraser les informations nécessaires au fonctionnement d'un programme pour le faire exécuter du code malicieux. Lorsqu'un processus est en cours, il écrit des informations dans une zone de la mémoire appelée «tampon». Un bug peut alors être utilisé (ou provoqué par le pirate) pour faire déborder ce tampon. Tout le code qui sera injecté par un brigand sera alors exécuté comme s'il émanait d'une source sûre. Ensuite, toutes les horreurs sont imaginables, y compris l'accès au système par le pirate. Cette technique requiert une connaissance très approfondie des processus et du fonctionnement des programmes, mais comme souvent, il existe quantité d'outils «clé-en-main», heureusement souvent obsolètes au moment de leur distribution.

INJECTION SQL

Il existe plusieurs types d'injection SQL, mais toutes fonctionnent sur un modèle comportant une application interagissant avec une base de données. Prenons l'exemple d'un site programmé en PHP et qui communique avec une base SQL. Si le formulaire de connexion de ce site présente une faiblesse, il sera possible de se connecter à l'interface du webmaster en tapant une requête SQL non prévue par le système directement dans le champ «mot de passe». Bref, au lieu de taper le mot de passe, vous envoyez quelques bouts de code qui seront interprétés comme un sésame valide. Il existe des outils permettant d'automatiser ce type d'attaque (pour éviter d'avoir à les faire «à la main») qui servent aussi bien aux webmasters voulant tester la sécurité de leur site qu'aux scripts kiddies...



HAVIJ, UN LOGICIEL IRANIEN DONT NOUS VOUS AVIONS DÉJÀ PARLÉ PERMET D'AUTOMATISER DES INJECTIONS SQL...

LEXIQUE

LE PHISHING

Il s'agit plus d'un piège tendu que d'une attaque. Le phishing (ou hameçonnage) est donc un traquenard qui vise à récupérer les données confidentielles d'un internaute. Le pirate, se faisant passer par e-mail pour sa banque ou une autre institution (la CAF, son FAI, etc.) lui propose de cliquer sur un lien renvoyant à une page qui a exactement la même apparence. Une fois sur cette fausse page, il devra entrer son mot de passe qui tombera directement dans escarcelle du brigand.

ARP POISONING

L'ARP Spoofing ou ARP Poisoning permet de détourner des flux de communication sur un réseau local. Le pirate doit pour cela être connecté au réseau (un Wi-Fi public, par exemple). Cela permet à l'attaquant d'écouter, de corrompre, de couper l'accès au réseau mais aussi d'usurper une adresse IP ou de bloquer le trafic.

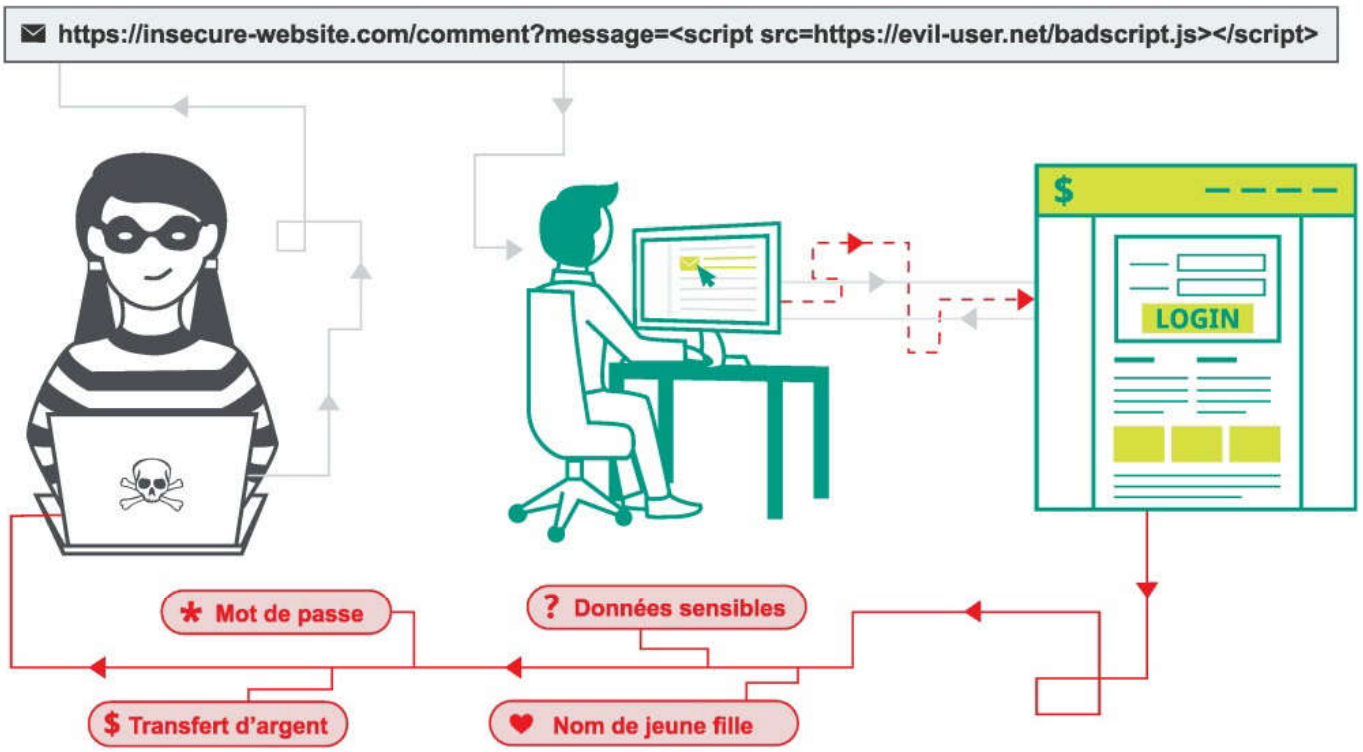
AVEC DE L'ARP POISONING, IL EST POSSIBLE D'INJECTER DE FAUSSES INFOS OU DES IMAGES DANS UN SITE SI VOUS ÊTES SUR LE MÊME RÉSEAU

SNIFFING

Le sniffing permet, grâce à un logiciel adapté, de lire ou d'enregistrer des paquets de données qui transitent par un réseau. Si ces données circulent en «clair» (non chiffrées), ces techniques donnent l'opportunité de récupérer des informations très facilement (mots de passe, etc.). Et dans le cas contraire, il est aussi possible d'analyser le contenu et même d'avoir accès à certaines données en décodant les paquets à la volée.

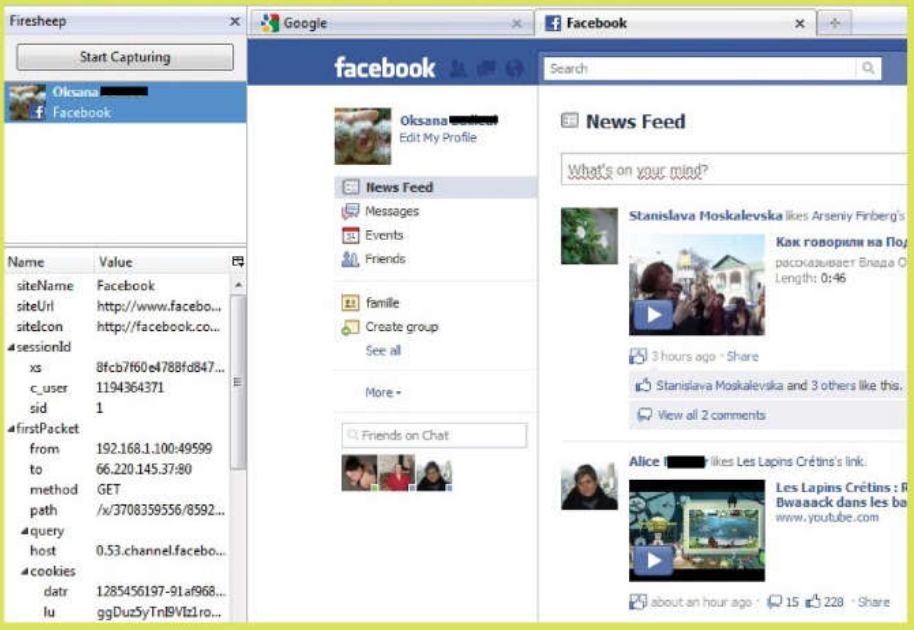
XSS : CROSS-SITE SCRIPTING

Il s'agit, ici, de polluer un site avec des bouts de code malicieux (dans un forum, des commentaires, etc.) pour que le navigateur de l'utilisateur interprète ce code. Il peut s'agir d'un site «complice» ou d'un site «victime». Les possibilités des attaques XSS sont très larges puisque le pirate peut utiliser tous les langages supportés par le navigateur (le plus souvent JavaScript). Généralement, ce type d'attaque permet de rediriger l'utilisateur vers une autre page (phishing ou hameçonnage en français) ou de voler la session en usurpant des cookies.



SIDEJACKING

Lorsque vous vous connectez à un site en entrant nom d'utilisateur et mot de passe, le serveur vérifie si un compte correspondant existe et place un «cookie» (un petit fichier qui contient vos identifiants) sur votre ordinateur pour ne pas avoir à vous ré-identifier pour toutes les autres requêtes suivantes. La plupart des sites protègent votre mot de passe en chiffrant votre identification initiale, mais il est plus rare qu'ils chiffrent autre chose. Si un tiers récupère ce cookie, il détourne la session HTTP et devient alors légitime pour le site : à lui l'envoi d'e-mails, la récupération d'informations ou le piratage de votre site... C'est ce qu'on appelle le «sidejacking». Et sur un réseau sans fil mal sécurisé (ou pas sécurisé du tout comme le hotspot d'un hôtel ou chez MacDo), il suffit de les intercepter à la volée...



L'INFORMATIQUE FACILE
POUR TOUS !

CHEZ VOTRE MARCHAND DE JOURNAUX

TUTO

POUR QUI ?
Pour tout le monde !

POUR QUOI FAIRE ?
Supprimer les publicités et le tracking des sites Internet

TRACKING ET PUBLICITÉS : COMMENT LES BLOQUER EN AMONT ?

Bien que la publicité soit un très bon moyen de rémunérer les créateurs de contenus, les abus de certaines régies publicitaires sont exaspérants et gâchent la lecture. En plus de cela, le tracking par les GAFAM est maintenant omniprésent sur le Web. Nous allons voir comment y faire face...

Merci à Etienne Sellan pour l'article et son serveur DNS !

LEXIQUE

***DNS :** Accronyme de "Domain Name System" que l'on peut traduire par "système de noms de domaine". Il s'agit d'un service informatique qui est utilisé pour traduire les noms de domaine Internet en adresse IP. Mis en place vers 1985 pour remplacer le système à base de fichier HOSTS.TXT et pallier la multiplication des sites, il reste un des composants essentiels du développement d'Internet.

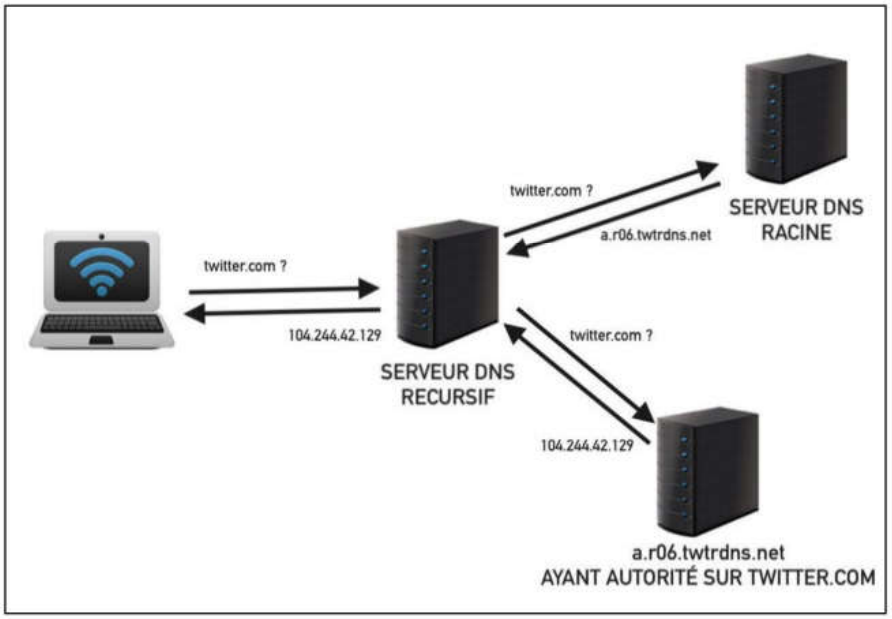
Lorsque vous naviguez sur le Web et que vous accédez à une page quelconque, il se passe beaucoup de choses dans votre navigateur. Ce dernier va commencer par télécharger le fichier principal de page. Il va ensuite lire ce fichier qui va définir la structure de la page, mais surtout lister les liens vers les fichiers annexes. Les fichiers annexes peuvent être les images, les feuilles de style, mais aussi de petits scripts chargés de gérer la publicité sur cette page. Mais ces scripts ne se contentent pas d'afficher une publicité, ils analysent votre comportement sur la page : Combien de temps vous y passez? Quelle partie de cette page vous a le plus attiré ? Ils transmettent ces informations aux serveurs de la régie publicitaire qui va ajouter ces données à votre identité publicitaire. Cela permet de retracer votre parcours sur Web, les sites que vous visitez le plus, à quel moment de la journée, où vous habitez... L'analyse des données étant de plus en plus poussée, on peut maintenant deviner des informations personnelles sur vous. Par exemple : les différents membres de votre famille, si vous avez des enfants ou des animaux, votre tranche de revenu, votre lieu de travail, de vacances... Et ce, avec un faible échantillon de données récolté

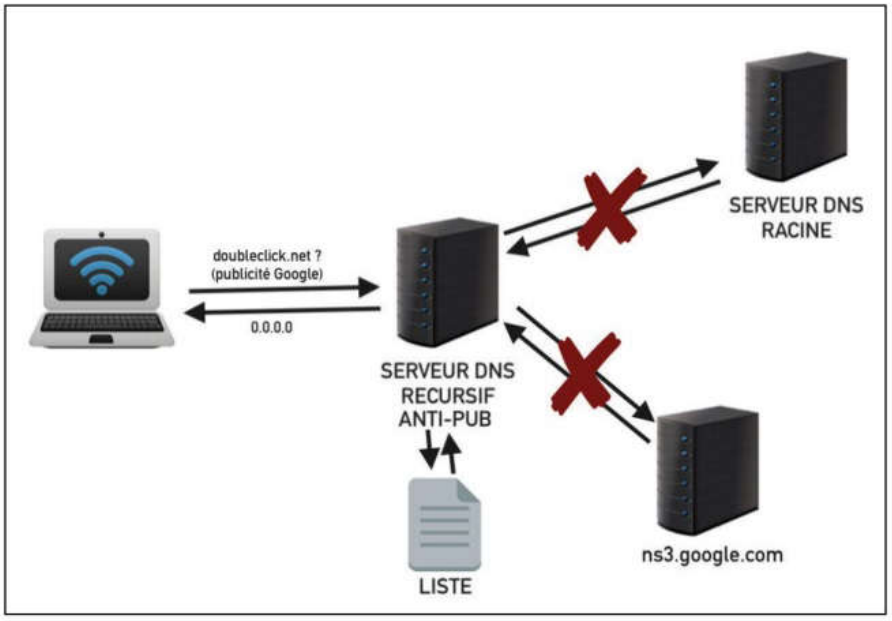
durant la navigation. En admettant une seconde (et seulement une seconde) que l'on fasse confiance aux GAFAM pour récolter, conserver et analyser ces données, que se passera-t-il quand ces données se retrouveront dans la nature suite à une énième faille de sécurité ? Pour en savoir plus sur les données que Google collecte, nous vous invitons à lire ce PDF : **https://frama.link/_1Nma9eb.**

> Faites «une pierre, deux coups» : virez les pubs et empêchez le tracking !

COMMENT BLOQUER CE TRACKING ?

Lorsque vous tentez d'accéder à une ressource en ligne, avant de télécharger les fichiers, votre ordinateur doit d'abord se connecter au serveur, il lui faut donc l'adresse IP. Évidemment vous n'utilisez pas d'adresse IP pour naviguer sur le Web, vous utilisez des noms de domaine, comme twitter.com. Pour résoudre ces noms de domaine, votre ordinateur va consulter un serveur DNS (Domain Name System) qui ira chercher l'adresse IP du site auprès des serveurs ayant autorité sur ce domaine, puis vous renverra l'adresse. Par défaut, le serveur DNS récursif utilisé sur votre ordinateur ou smartphone est celui de votre fournisseur d'accès Internet. Une méthode simple pour bloquer certaines ressources comme les scripts de tracking est d'empêcher la résolution des domaines correspondant à des régies publicitaires. Ainsi, votre navigateur ne pourra même pas télécharger ces scripts et publicités, et encore moins leur envoyer des données personnelles. Le fait de bloquer les publicités et les scripts de tracking à ce niveau permet une économie notable de bande passante en évitant le téléchargement de ressources et d'images inutiles.





VOICI UN SCHÉMA SIMPLIFIÉ D'UNE RÉSOLUTION DE NOM DE DOMAINE NORMALE ET UNE RÉSOLUTION AVEC LE SERVEUR D'ETIENNE...

COMMENT UTILISER CE SERVEUR DNS ?

PRATIQUE

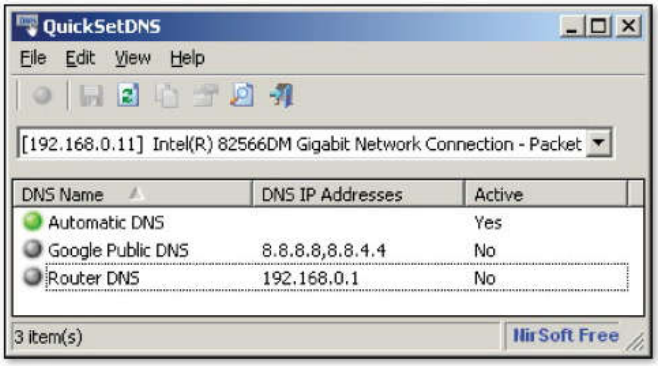
01› UN PROJET UNIVERSITAIRE

Ce service est un projet étudiant que j'ai développé au sein du campus Ynov Bordeaux, il est à but non lucratif, sans inscription, sans installation et sans collecte de données. Pour utiliser ce service, il suffit de se rendre sur le site du projet dns.sellan.fr. Copiez l'adresse IP du serveur présente sur la page d'accueil puis insérez la dans les paramètres de votre appareil à la place du

réglage par défaut. Si vous ne savez pas comment faire, suivez ce lien : **https://frama.link/zyPdLUxN**. Si par la suite vous voyez une publicité ou un tracker qui n'a pas été bloqué, vous pouvez retourner sur le site Web du projet, et signaler l'adresse de la page via le formulaire prévu à cet effet en bas de la page. Après validation, tous les utilisateurs bénéficieront de votre signalement.

02› SUR PC SOUS WINDOWS

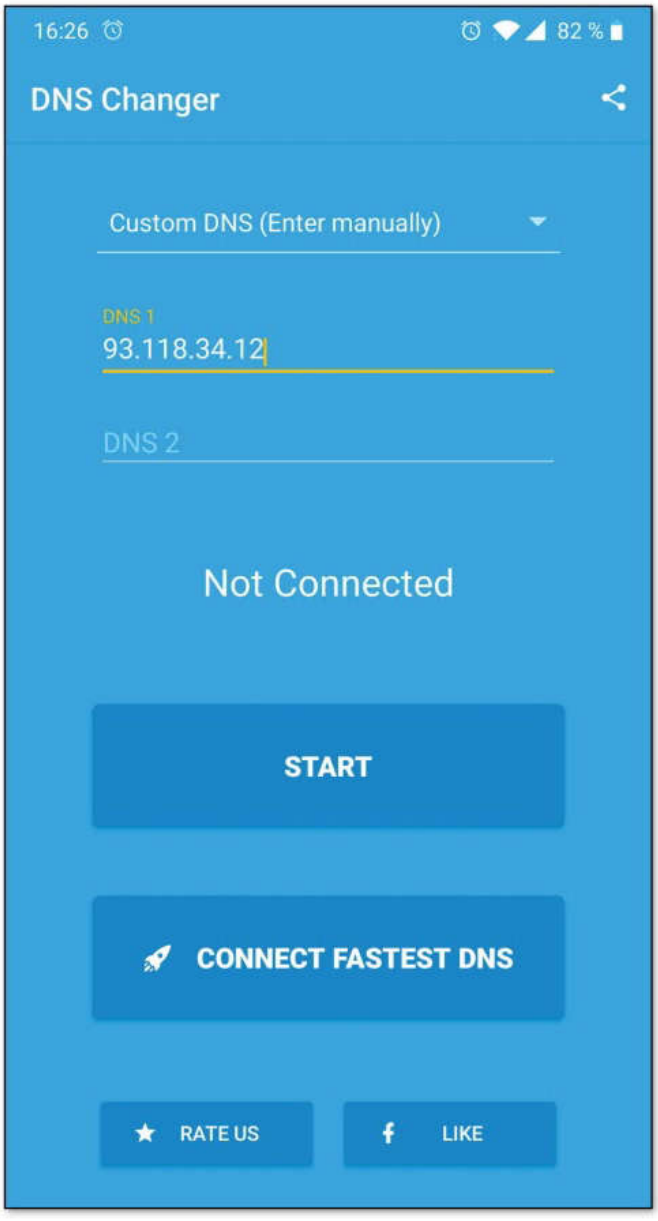
Vous n'avez pas envie de passer par 36 fenêtres pour changer vos DNS ? Nir Sofer propose



un outil pour cela ! QuickSetDNS vous permet de changer facilement les serveurs DNS utilisés pour votre connexion Internet. Vous pouvez définir les serveurs DNS souhaités à partir de l'interface utilisateur, en choisissant dans une liste de serveurs DNS que vous avez définie ou en ligne de commande, sans afficher d'interface utilisateur.
Lien : **https://frama.link/7P5YX3tQ**

03› SUR MOBILE ANDROID

Si vous n'avez pas envie d'aller dans les paramètres de votre mobile Android pour changer vos DNS, il est possible d'utiliser une application. Avec DNS Changer, pas besoin d'avoir un mobile rooté et cela fonctionne en 3G et en WiFi.
Lien : **https://frama.link/_TocPBj4**

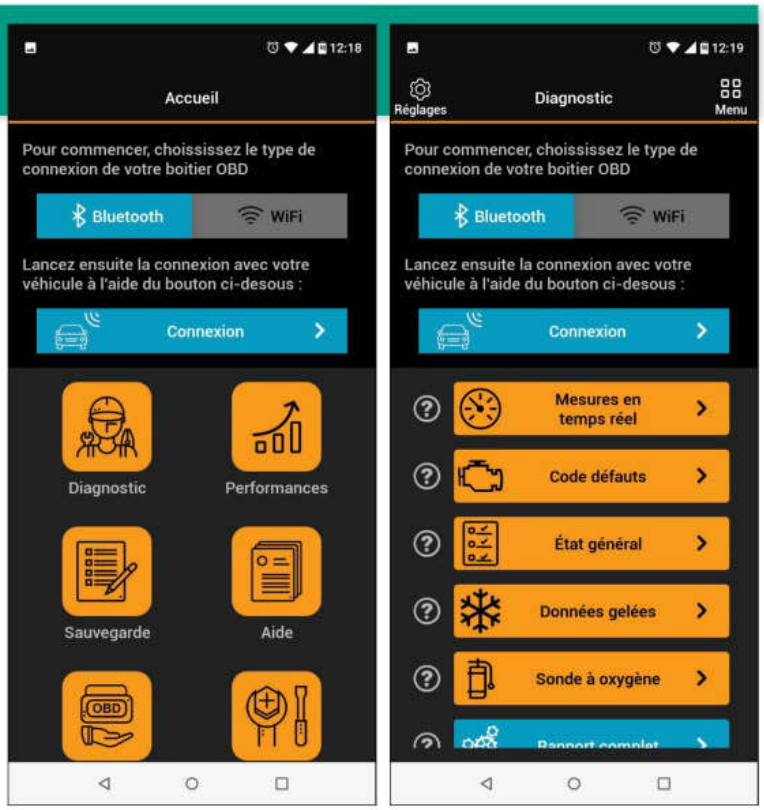


Comme dans une série américaine, le papier peut revenir pendant plusieurs saisons.

La force de tous les papiers, c'est de pouvoir être recyclés
au moins cinq fois en papier. Cela dépend de chacun de nous.
www.recyclons-les-papiers.fr

Tous les papiers ont droit à plusieurs vies.
Trions mieux, pour recycler plus !

Réglez et réparez votre voiture
> AVEC OBDCLICK



Nous vous avions déjà parlé de l'interface OBD2 qui équipe toutes les voitures depuis le début des années 2000. Il s'agit d'une prise qui peut être dissimulée dans la boîte à gants ou sous le tableau de bord et qui permet de traiter et d'analyser différents types d'informations : la température du liquide de refroidissement, l'état du système de carburant du véhicule et d'autres données concernant la vitesse et la puissance. Il est même possible d'effacer des voyants d'alerte et de monitorer certains paramètres moteur. L'application Android OBDclick se charge d'analyser les données issues de ces prises magiques. Il faudra juste s'équiper d'un récepteur compatible. Si vous n'en avez pas, l'appli se propose de vous en faire livrer un pour moins de 30 €. Notez que ce dernier devra être «sans fil» : WiFi ou Bluetooth. En effet les prises USB ne sont pas compatibles avec l'appli pour d'évidentes raisons de connectiques. Une fois que vous avez trouvé la prise sur votre véhicule (l'appli vous y aidera), il faudra juste appairer l'adaptateur avec OBDclick. Ensuite, vous pourrez à votre aise diagnostiquer votre auto : codes d'erreur, suppression de voyants, sonde à oxygène, régime moteur, système d'injection, débit d'air, pression du carburant, admission, etc. Plutôt que de laisser un garagiste vous expliquer les choses, soyez maître de votre destrier de métal (ou de plastoc, pour ma Dacia). C'est aussi un bon moyen de détecter les failles d'une voiture d'occasion ou d'anticiper les pannes même si vous n'êtes pas un professionnel, car grâce au code d'erreur que vous pouvez taper sur Google, vous trouverez le bon tuto en ligne pour parer à tout problème. Bien sûr, l'appli est compatible avec les plus grandes marques d'automobiles, Dacia y compris alors ?

Lien : **https://frama.link/K0Zu_Ch5**

Savoir si vous êtes victime de piratage
> AVEC SPYBOT IDENTITY MONITOR

Spybot Identity Monitor est un programme qui va vérifier si vos données personnelles sont entre les mains de pirates. Ce logiciel sous Windows va tout simplement faire la liste de vos noms d'utilisateur et vérifier qu'ils ne figurent pas dans la base de données du site Have I Been Pwned. Gratuit, Spybot Identity Monitor

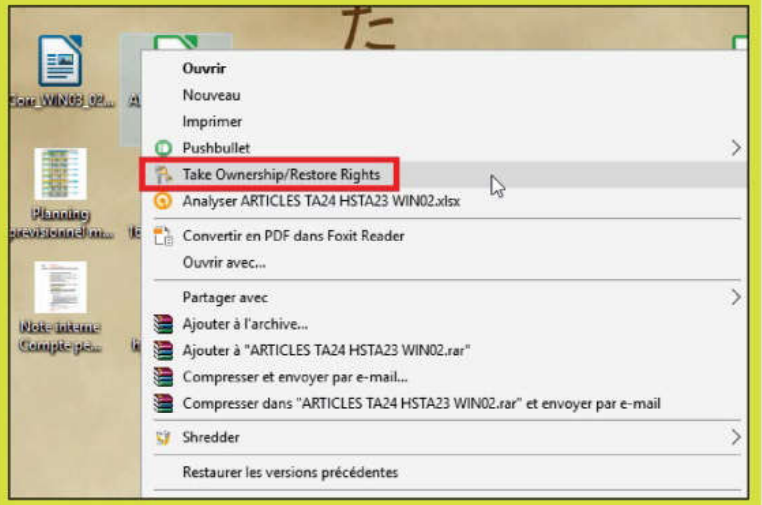
recherchera vos traces parmi les leaks les plus médiatiques de ces dernières années : Linkedin, Tumblr, Disqus, Dropbox, Ashley Madison, Dailymotion, VTech, etc. Le logiciel n'ira pas fouiller dans vos identifiants enregistrés, vous devrez entrer vos emails ou noms d'utilisateur à la main. Si votre trace a été repérée sur un des 340 sites qui ont été victime de vol de données, il faudra vite changer votre mot de passe et penser à l'identification à double facteur !

Lien : **https://frama.link/J-ZwBYRo**

Prendre le contrôle total d'un fichier
> avec TakeOwnershipEx

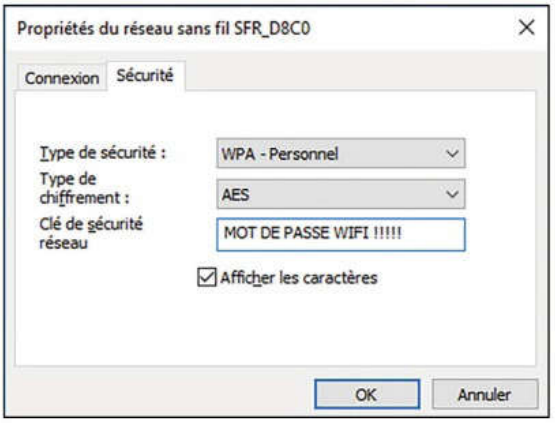
Windows verrouille vos possibilités sur la plupart des fichiers système (interdiction de modification, de copie, de déplacement, etc.) Pour passer outre, téléchargez et installez TakeOwnershipEx. Désormais, faites un clic droit sur le fichier concerné et gauche sur **Take Ownership/Restore Rights**. Un message indique que vous avez désormais tous les droits dessus. Refaites la manipulation pour restaurer les protections.

Lien : **https://frama.link/jetC3HCs**

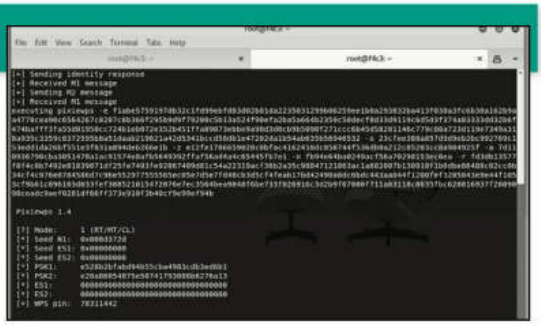


Retrouver votre mot de passe Wi-Fi
> avec Windows

Besoin de partager le mot de passe du Wi-Fi, mais aucune envie de retourner la box pour le récupérer ? Dans la barre des tâches, faites un clic droit sur l'icône du Wi-Fi puis sélectionnez **Ouvrir le Centre Réseau et partage**. Cliquez sur le nom de votre réseau Wi-Fi (à droite de **Connexions**). Dans la nouvelle fenêtre, cliquez sur **Propriétés sans fil** et allez dans **Sécurité**. Cochez la case **Afficher les caractères** pour voir le mot de passe.



Casser un PIN WPS > avec PixieWPS



Commençons par rappeler que le système WPS équipé par certains routeurs ou box permet de facilement se connecter à un réseau sans fil sans avoir à taper une longue clé d'authentification. En fonction des réglages par défaut (que vous pouvez bien entendu changer), le propriétaire du matériel doit parfois appuyer sur un bouton pour autoriser un invité à se connecter (limité dans le temps) et parfois il s'agit d'un code PIN. Même s'il existe des moyens pour court-circuiter la protection du bouton (nous y reviendrons dans un prochain numéro), la vulnérabilité la plus répandue concerne ce code PIN. En effet, certains constructeurs utilisent le même PIN, mais il est aussi très possible de cracker ce code bien plus facilement qu'une clé WPA. PixieWPS est un outil écrit en C que vous pouvez utiliser pour tenter une méthode «brute force» sur un code PIN WPS. Pour cela, il utilise l'attaque «Pixie-dust» qui fonctionne en exploitant des faiblesses au niveau logiciel, mais permet aussi de récupérer une clé WPA-PSK à partir d'une capture passive complète. Il vous faudra bien sûr un adaptateur WiFi compatible avec le Monotor Mode. Pour l'installer sous Linux, il faudra faire :

apt-get -y install build-essential
wget https://github.com/wiire/pixiewps/archive/master.zip && unzip master.zip
cd pixiewps * /
sudo make installer

Il n'existe pas de version Windows pour le moment, mais nous allons nous pencher sur la question pour le prochain numéro et vous proposer des alternatives.

Lien : **https://github.com/wiire-a/pixiewps/releases**

TUTO

QUE RENFERME VOTRE SKYPE ?

Avec son identification requise, on pourrait penser que vos informations Skype (messages, appels, contacts, etc.) sont bien précautionneusement chiffrées sur votre machine. Il n'en est rien. Un pirate ayant accès à votre machine peut tout récupérer en deux minutes. Et c'est encore pire, si vous vous connectez depuis une autre machine.

Tout votre univers Skype tient en 7 caractères : main.db. Ce fichier, caché dans les méandres de votre disque dur, contient le nom de vos contacts, les informations de votre profil, les dates de vos appels et même le contenu de vos messages. Avec toutes ces données sensibles, vous vous dites que l'accès à ce fichier est restreint, mais c'est tout le contraire ! Non seulement il est très aisé d'y avoir accès depuis une machine, mais vous pouvez facilement le récupérer sur une clé USB pour le consulter tranquillement chez vous. Aucun mot de passe n'est demandé et en ce qui concerne l'identifiant, ce dernier est inscrit en toutes lettres sur le dossier qui contient le fameux fichier main.db...

UN HISTORIQUE DES CONVERSATIONS EN MODE «OPEN-BAR»

Mais le plus grave c'est la possibilité pour une personne de récupérer une partie de vos données confidentielles. En vous connectant depuis une autre machine que la vôtre (cybercafé, PC d'un ami, université, etc.), vous laissez un fichier main.db sur celle-ci. N'importe qui peut donc avoir accès à vos messages échangés sur cette machine. Dans cet article, nous verrons comment accéder à vos données et accessoirement à celle des autres...

POUR SE PROTÉGER

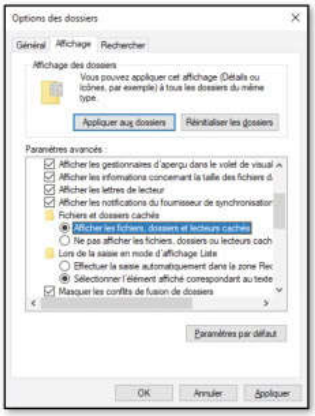
Pour éviter de voir vos données personnelles dans la nature, effacez systématiquement ce fichier main.db du PC étranger sur lequel vous vous connectez. Chez vous, optez pour un chiffrement du disque dur avec VeraCrypt par exemple.

LOCALISEZ ET TRANSFÉREZ VOTRE HISTORIQUE SKYPE

PRATIQUE

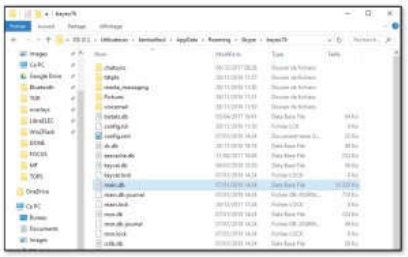
01› AFFICHEZ LES DOSSIERS CACHÉS

S'il est possible de transférer tout l'historique de vos communications Skype, il s'agit de pouvoir y accéder depuis un autre PC en cas de panne ou de changement de matériel. Dans un premier temps, il faudra afficher les dossiers cachés. Dans les paramètres d'Affichages d'un dossier, cliquez sur Options puis Modifier les options des dossiers et de recherche. Sélectionnez l'onglet **Affichage**. Ici, cochez la case **Afficher les fichiers, dossiers, et lecteurs cachés**. N'oubliez pas de valider.



02› LE FICHIER MAIN.DB

Il faudra ensuite vous rendre dans **C:\Utilisateur\[nom d'utilisateur]\AppData\Roaming\Skype\[pseudo Skype]**. Dans ce répertoire, vous trouverez le fichier **main.db**. Pour transférer vos conversations, il suffira de sauvegarder ce fichier puis le transférer dans votre nouvel ordinateur au même endroit. Si d'autres personnes se connectent à Skype depuis le PC cible, vous verrez aussi leur pseudo dans le dossier **Roaming/Skype**. Chacun d'eux comporte un fichier **main.db**...



Bien sûr pour utiliser SkypeFreak depuis votre PC, vous n'aurez pas besoin d'aller le chercher ou de le transférer.

ANALYSE DES DONNÉES AVEC SKYPEFREAK

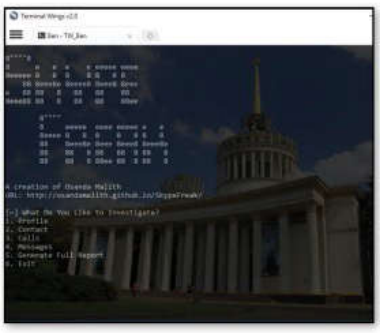
PRATIQUE

01› PYTHON ?

SkypeFreak est un script Python qui fonctionne en mode «stand alone» ce qui signifie que vous n'aurez pas besoin d'installer ce langage. Mais si vous avez vos petites habitudes, vous pouvez lancer le script **SkypeFreak.py** depuis une console Python. Si vous voulez analyser votre propre fichier **main.db** ou celui d'un ami qui se connecte depuis votre PC, vous n'aurez rien à faire de particulier.

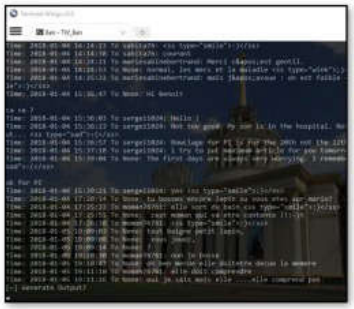
02› PRÉPARATIFS

Si vous voulez analyser des données qui viennent d'un autre PC, il faudra mettre tout le dossier «pseudo» contenu dans **C:\Utilisateur\[nom d'utilisateur]\AppData\Roaming\Skype** à ce même emplacement sur votre PC. Suivez notre lien, cliquez sur **Download ZIP** sur la droite et décompactez l'archive. Si votre antivirus donne l'alerte pendant cette phase, désactivez-le momentanément. Lancez **SkypeFreak.exe**. Ici aussi, notre antivirus a commencé à paniquer. Il a même mis l'EXE en quarantaine sans nous demander notre avis. Désactivez-le pour un peu plus de temps.



03› LE PROGRAMME

Le programme vous demandera le pseudo du compte à analyser. Pas difficile puisque c'est le même nom que le dossier contenant main.db. En tapant sur **Entrée**, vous aurez alors un menu vous proposant de vous renseigner sur le profil, les contacts, les appels ou les messages. Tapez le chiffre qui vous intéresse et faites **Entrée**. Si la fenêtre se ferme ou si le programme plante, réessayez. N'oubliez pas que SkypeFreak est encore en version bêta. Il nous a fallu quelques essais...



04› LE RAPPORT

À la fin du processus, le programme va vous demander si vous voulez éditer un journal. Pratique si vous êtes sur une machine étrangère et que vous voulez récupérer les infos rapidement. Tapez **y** (pour yes), validez et tapez un nom. Ce journal sera sauvegardé au format TXT dans le dossier SkypeFreak.
Sans le mot de passe de votre «victime», vous aurez donc accès à ses conversations écrites, à qui elle a parlé au téléphone, quels sont ses contacts, etc.

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 MT

Solutions & Astuces

www.android-mt.com

NOUVEAU SITE !

GARDEZ VOTRE HISTORIQUE EN NAVIGATION PRIVÉE

PRATIQUE

Le mode navigation privée de Chrome ne laisse pas de traces sur votre PC. Mais, il vous prive de l'historique, parfois bien pratique. Sauf si vous installez l'extension Off the record.

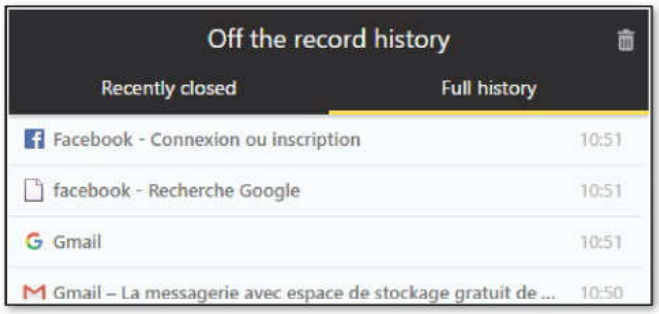
INFOS [Off The Record History]
Où le trouver ? [https://goo.gl/vRYDOR]
Difficulté :

01› ACTIVER L'EXTENSION

Après avoir installé l'extension, cliquez sur les trois points en haut à droite de votre navigateur. Cliquez sur **Plus d'outils** et **Extensions**. Cherchez **Off the record** et cochez **Autoriser en mode navigation privée**. Sans cela, l'extension ne marchera pas.

02› CONSULTER L'HISTORIQUE

Pour voir votre historique, cliquez sur l'icône de l'extension. Vous aurez accès à vos onglets fermés (**Recently closed**) et votre historique depuis le début de la session privée (**Full History**). Une fois la fenêtre de navigation fermée, votre historique disparaît définitivement.



CRÉER UNE ADRESSE MAIL JETABLE

PRATIQUE

Marre de devoir entrer votre mail personnel pour vous inscrire à un service que vous n'utiliserez qu'une seule fois ? Utilisez plutôt une adresse mail temporaire à la place.

INFOS [YOPMAIL]
Où le trouver ? [www.yopmail.com]
Difficulté :

01› CRÉER LA BOÎTE MAIL

Sur la page d'accueil de Yopmail, sous **Saisissez le mail jetable de votre choix**, entrez le nom souhaité (cela peut être n'importe quoi : « chien », « Albert », « fdghbgtrfgykayur »...) et validez avec **Vérifier les mails**.

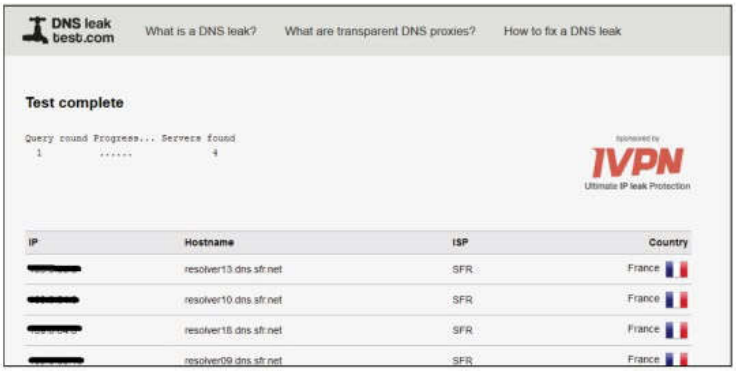
02› CONSULTEZ LES MAILS

Rien de plus simple : entrez le nom choisi dans le même champ qu'à l'étape précédente et validez à nouveau avec **Vérifier les mails**. Pas de mot de passe ou autre. Les messages sont automatiquement effacés au bout de 8 jours.

Vérifier son VPN > avec DNS Leak

Les fuites de DNS, c'est-à-dire l'envoi accidentel de paquets d'informations utilisant le DNS de votre fournisseur d'accès Internet au lieu de celui utilisé par votre VPN, posent un réel problème d'anonymat. Lancez un test sur DNS Leak. Si les serveurs affichés ne sont pas ceux de votre VPN, c'est que vous êtes potentiellement vulnérable.

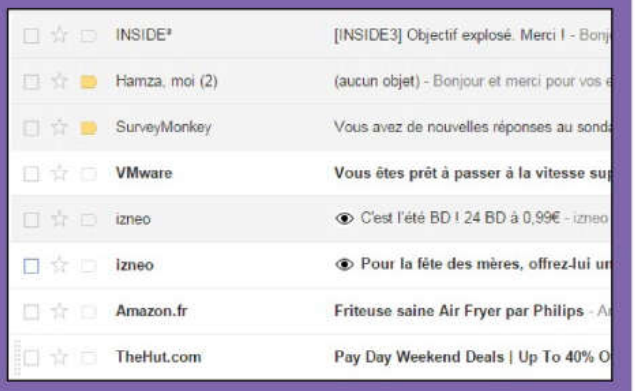
Lien : **www.dnsleaktest.com**



Éviter le pistage par mail > avec Ugly Mail

Disponible pour Chrome, l'extension Ugly Mail permet de savoir avant l'ouverture d'un mail si ce dernier sera utilisé pour vous pister : heure d'ouverture, navigateur utilisé... Une fois installé, Ugly Mail va afficher un œil ouvert à côté des mails intégrant des «trackers», tandis qu'un œil fermé indique leur absence. Notez qu'une demande d'accusé de réception est considérée comme un tracker et que les mailing-lists (dont la nôtre) disposent aussi de ces petites bêtes pour savoir si vous l'avez bien reçu ou si vous avez cliqué dessus.

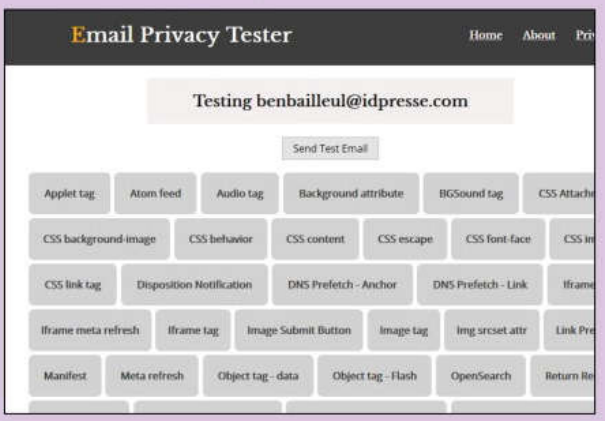
Lien : **https://uglyemail.com**



Tester sa messagerie > avec Email Privacy Tester

Malgré vos précautions, votre IP peut se retrouver dans la nature, et pour les échanges de messages électroniques, votre client ou votre service Webmail ne sont pas forcément vos alliés. Pour vérifier quelles informations transitent par Internet lorsque vous envoyez des e-mails, tapez votre adresse dans le champ prévu et validez. Ouvrez l'e-mail envoyé par le site. Les éléments en rouge sont susceptibles d'apparaître chez vos correspondants. À vous de régler votre client ou votre messagerie en ligne pour colmater les fuites.

Lien : **www.emailprivacytester.com**

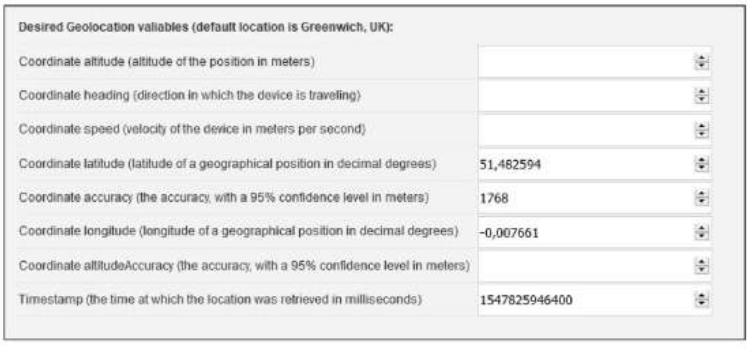


Empêcher la géolocalisation > avec Location Guard

Même si vous n'utilisez pas de VPN ou de solution d'anonymat, vous n'avez pas forcément envie que les sites sur lesquels vous vous connectez sachent où vous vous trouvez. L'extension Location Guard évite d'avoir à refuser manuellement le partage de sa localisation. Vous pouvez paramétrer pour chaque site un refus permanent, l'envoi d'une localisation aléatoire, voire fantaisiste. La localisation par défaut est Greenwich au Royaume-Uni. Attention, cela ne change pas votre IP...

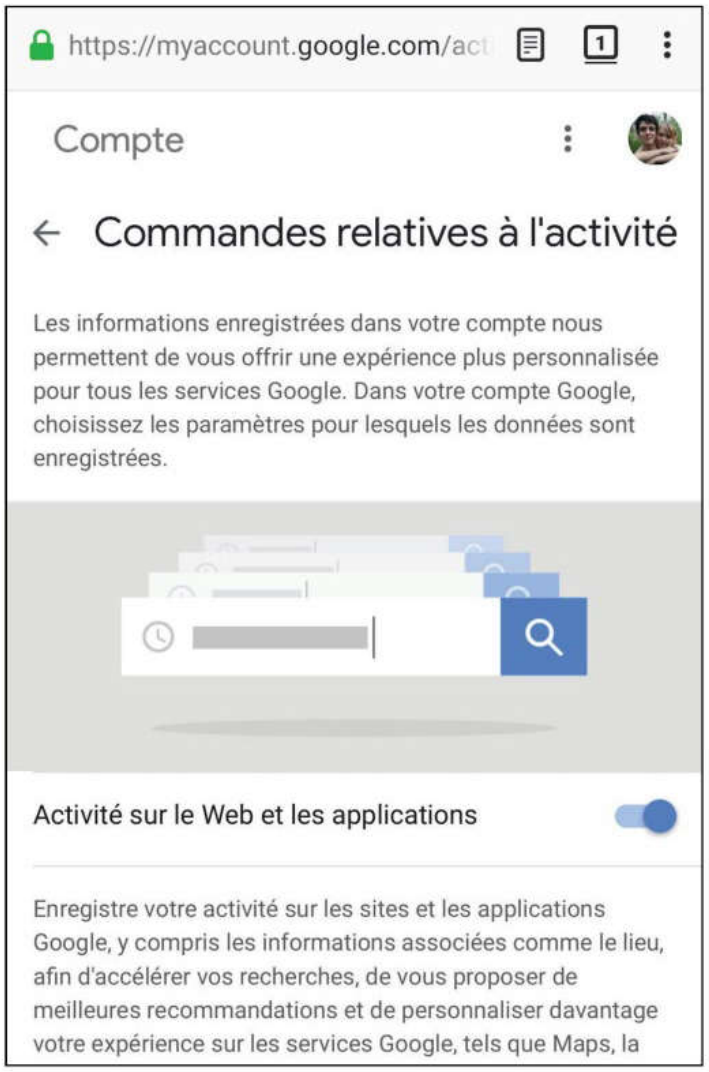
Lien : **https://frama.link/6Lb6n2cz** (Firefox)

Lien : **https://frama.link/h78heo3s** (Chrome)



Interdisez à Google de vous suivre !
> AVEC LES PARAMÈTRES DE VOTRE COMPTE GOOGLE

Nous sommes habitués aux mensonges ou aux omissions des GAFAM, mais il faut reconnaître que ça commence à devenir lourd. Selon une enquête Associated Press, Google enregistre la position de ses clients alors même que l'historique des positions est désactivé. Activé par défaut et destiné à vous traquer pour vous proposer des publicités ciblées, il existe une fonctionnalité cachée au fin fond de vos paramètres de compte. Il s'agit bien sûr d'un nouveau scandale, mais tant que personne ne les condamnera, Facebook, Google et les autres continueront de vous espionner et de vous traquer. Ce nouveau « flagrant délit » touche potentiellement un quart de l'humanité puisqu'il s'agit d'un problème propre aux utilisateurs Android, mais aussi des clients Apple qui utilisent des applis Google. Pour faire le ménage et définitivement vous débarrasser de ce fil à la patte, il faudra entrer cet URL : **https://myaccount.google.com/activitycontrols**. Tapez ensuite vos identifiants et allez dans la partie **Activité sur le web et les applications** puis désactivez cette option. Vous pouvez le faire depuis un PC ou votre mobile. N'oubliez pas de le faire sur tous vos comptes si vous en avez plusieurs !

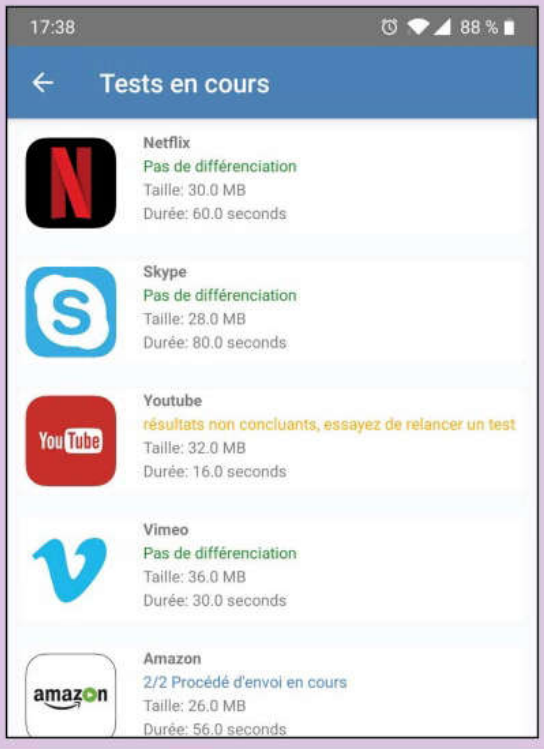


Testez le respect de la neutralité du Net > AVEC WEHE

Il existe pas mal d'outils en ligne ou sur PC pour tester la neutralité du Net. En France, les dégâts sont limités (mais pour combien de temps encore?), mais dans d'autres pays c'est loin d'être le cas : entre les censures, les services à deux vitesses, les points d'accès louches et les interventions des gouvernements sur le réseau des réseaux, il y a de quoi dénoncer. Pour pouvoir faire des tests plus facilement, vous pouvez essayer l'application Wehe. Disponible sur Android et iOS, cette dernière a été mise au point par une université américaine avec l'aide de notre ARCEP (cocorico !) Il suffit de faire **Lancer les tests** pour que diverses applications soient évaluées : Netflix, Skype, YouTube, Spotify, Amazon, etc. Pour mener à bien sa mission, Wehe va se connecter au site de deux manières : une fois en chiffrant les données et une autre fois en ne chiffrant rien. Si l'application trouve une différence de traitement entre les deux, c'est qu'il y a quelque chose de louche ! En cas de doute on peut pousser les tests jusqu'à tenter de déceler du Deep Packet Inspection (un procédé utilisé par les services secrets, les pirates et les gouvernements pas très cool). Attention, nous vous déconseillons d'utiliser cet outil dans un pays où la vie humaine n'a pas beaucoup de valeur...

Lien : **https://frama.link/33Bz5bKv (iOS)**

Lien : **https://frama.link/j_th8yrb (Android)**



TUTO

POUR QUI ?

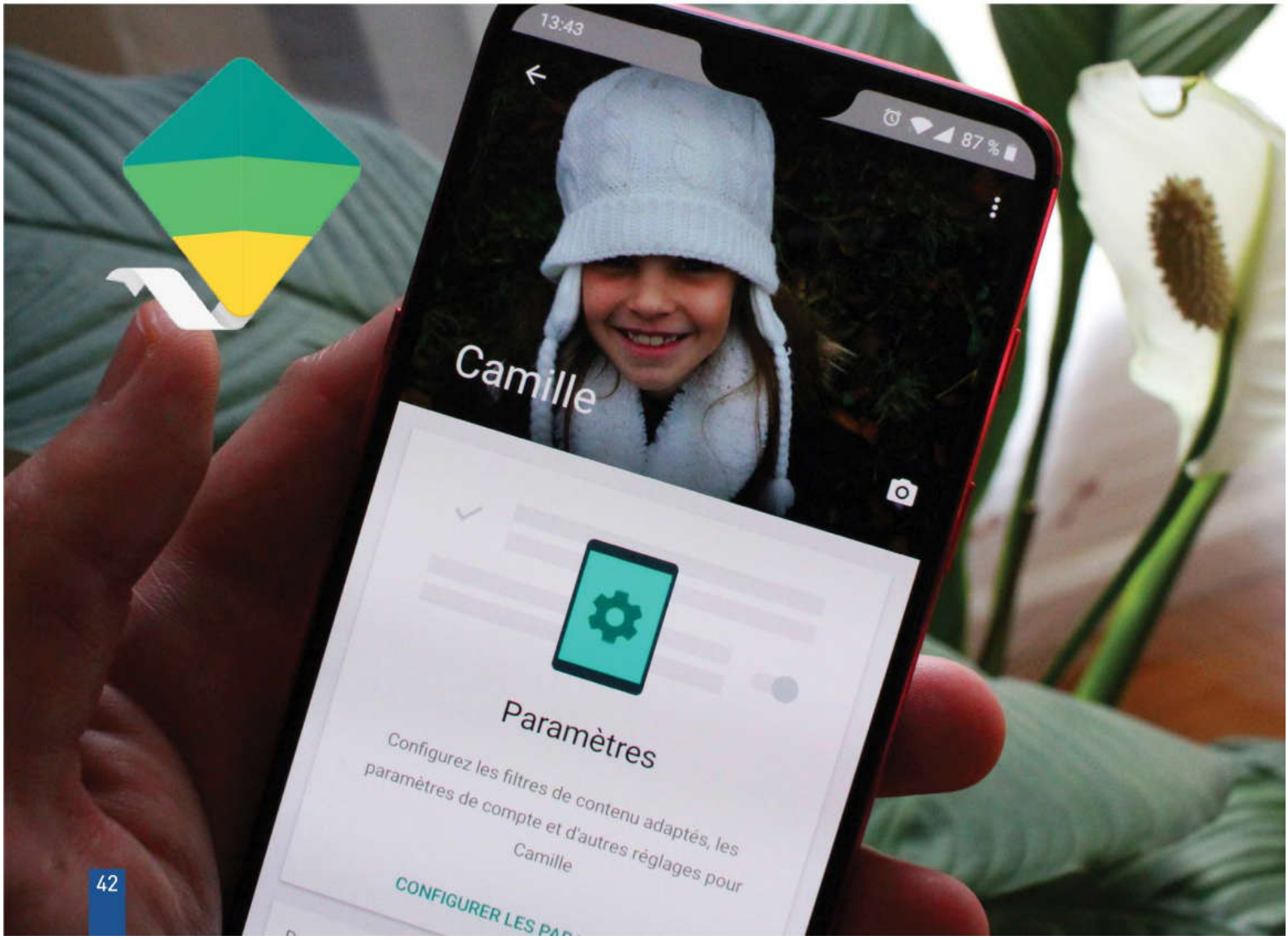
Pour les parents inquiets de voir leurs enfants sans surveillance sur leur tablette ou smartphone

POUR QUOI FAIRE ?

Installer un système d'approbation pour les applis, filtrer les recherches Internet et savoir ce que font vos enfants

FAMILY LINK : UN CONTRÔLE PARENTAL SIMPLE ET GRATUIT !

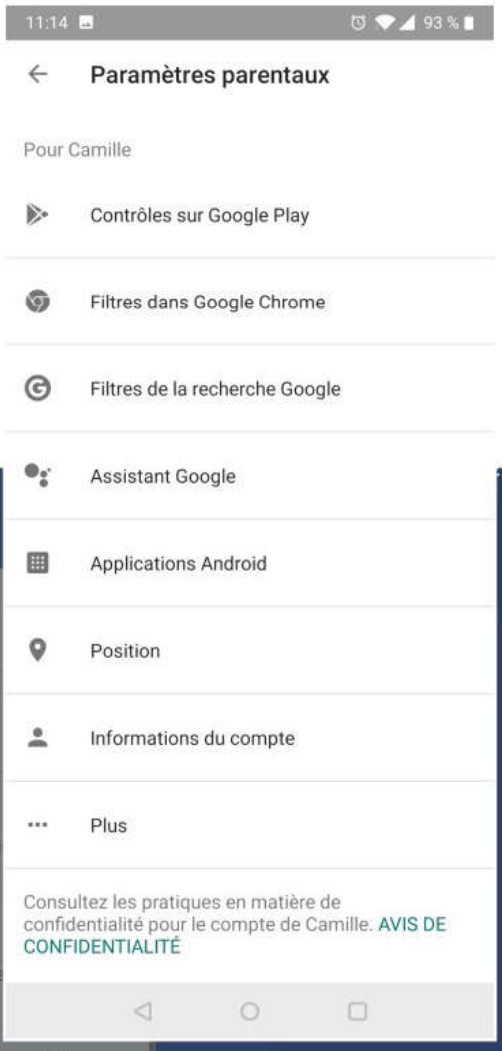
Noël est passé et il y a fort à parier que des tablettes ou des smartphones se sont retrouvés au pied du sapin pour les enfants sages. Le problème se pose alors pour les parents : comment contrôler les activités de votre enfant sans le brider ? Google propose l'application Family Link. Un contrôle parental qui permet de protéger vos enfants en associant son compte au vôtre et de gérer tout ça depuis l'appareil de papa ou maman...



Pour disposer d'un compte Google, il faut avoir 13 ans. Or les enfants sont de plus en plus jeunes à posséder un smartphone ou une tablette avant cet âge et comme vous le savez, il faut absolument avoir un compte de ce type pour accéder au Google Play Store, YouTube, etc. La société américaine a donc pensé aux parents qui veulent offrir un appareil Android tout en surveillant leur activité et actionner des garde-fous. Il s'agit d'une appli à installer sur la tablette de l'enfant et parallèlement sur un mobile parental. Pour les parents qui prêtent leur propre mobile à leurs enfants, c'est aussi possible... Le compte parent aura un parfait contrôle sur celui de l'enfant : applis bloquées ou en attente d'approbation, filtres de navigation, contrôle du temps passé avec la possibilité de définir des horaires d'utilisation, etc. Les parents disposent même d'une option permettant de géolocaliser leur progéniture. Voyons comment cela fonctionne...

> Même en éduquant bien ses enfants et en leur expliquant les dangers d'Internet, un contrôle parental n'est jamais superflu.

DEPUIS LES PARAMÈTRES, VOUS POURREZ ACTIVER LE FILTRE CHROME POUR ÉVITER LES CONTENUS POUR ADULTE. CELA FONCTIONNE PLUTÔT BIEN, MAIS VOUS POUVEZ AUSSI DRESSER UNE LISTE BLANCHE VOUS-MÊME.



INFOS [Family Link]
Où le trouver ? [https://frama.link/TM8A_wmE]
Difficulté : ☠☠☠

UN COMPTE GOOGLE SÉCURISÉ POUR VOTRE ENFANT

PRATIQUE

01› UN COMPTE INVITÉ POUR L'ENFANT

Pour commencer il faut ajouter un compte **Invité** dans votre appareil (dans **Paramètres>Comptes>Ajouter un compte**). Cette étape n'est pas nécessaire si c'est l'appareil de votre enfant par contre, si deux enfants partagent le même appareil, il faudra créer un compte pour chacun et bien leur dire de s'y connecter lorsqu'ils utilisent la tablette. Pour éviter les confusions, faites-leur mettre un fond d'écran différent pour chaque compte. Lorsqu'on vous le demandera, cliquez sur **Pour mon enfant** lorsque vous choisirez **Créer un compte**.

02› CRÉATION DU COMPTE ENFANT

Faites **Continuer** et suivez la procédure : entrez le nom, prénom et connectez votre propre compte lorsqu'on vous le demandera. Votre enfant va alors rejoindre votre groupe familial. Bien sûr vous pouvez le faire pour vos autres «Pokémons».

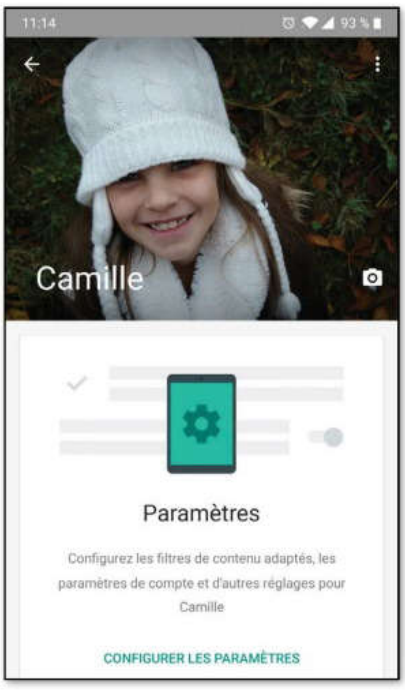
03› L'APPLI FAMILY LINK

Directement après l'appairage de vos comptes, vous pouvez déjà paramétrer quelques restrictions : filtres Chrome, navigation, téléchargement sur le Store, etc. Il

s'agit du cas où votre enfant serait amené à utiliser votre appareil, mais s'il s'agit de deux appareils distincts, l'appli de création de comptes vous suggérera de télécharger l'appli Family Link qui offre plus d'options.

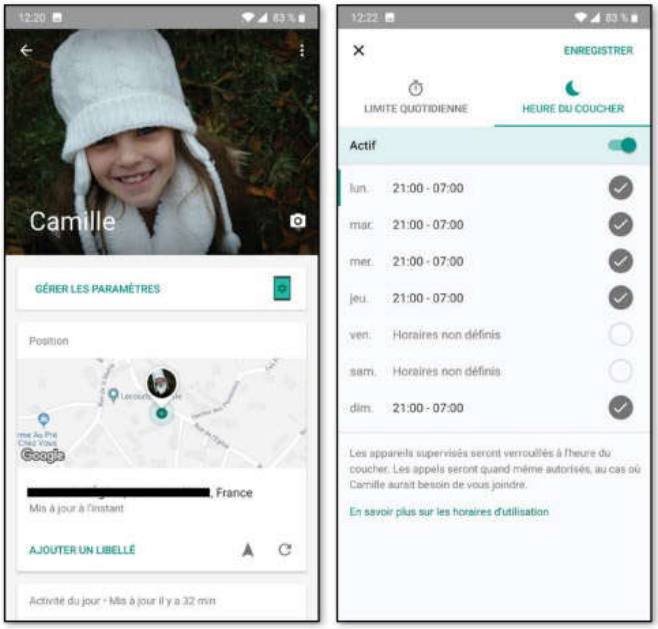
04› C'EST VOUS L'ADMINISTRATEUR !

Téléchargez l'application sur votre mobile et suivez les indications jusqu'à être considéré comme l'**Administrateur de famille**. Connectez le compte de l'enfant sur votre mobile. C'est terminé ! Il va falloir maintenant paramétrer vos restrictions...



05› PARAMÉTREZ LES RESTRICTIONS

Il n'y a rien de plus simple. Dans **Paramètres**, vous pouvez appliquer des contrôles sur le Play Store, Chrome, les recherches, etc. Mais vous pouvez aussi connaître la position de l'enfant, vérifier son activité (les recherches



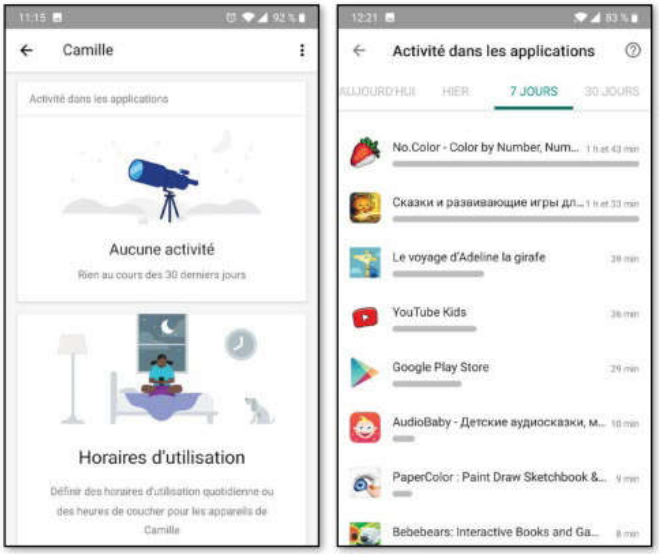
Internet, les applis utilisées, les heures de connexion, etc.), mais aussi définir des plages horaires d'utilisation. Tout cela est bien sûr paramétrable en fonction de l'âge de l'enfant et de ses besoins...

06› BIBLIOTHÈQUE FAMILIALE

La bibliothèque familiale permet de mettre en commun les applications que vous téléchargez. Pas besoin d'acheter 2 ou 3 fois une application éducative, un jeu ou un film si vous avez plusieurs enfants. En ouvrant cette bibliothèque, vous pourrez aussi y associer un moyen de paiement et contrôler les transactions bien sûr.

07› UN PETIT COUP D'ŒIL SUR LES ACTIVITÉS

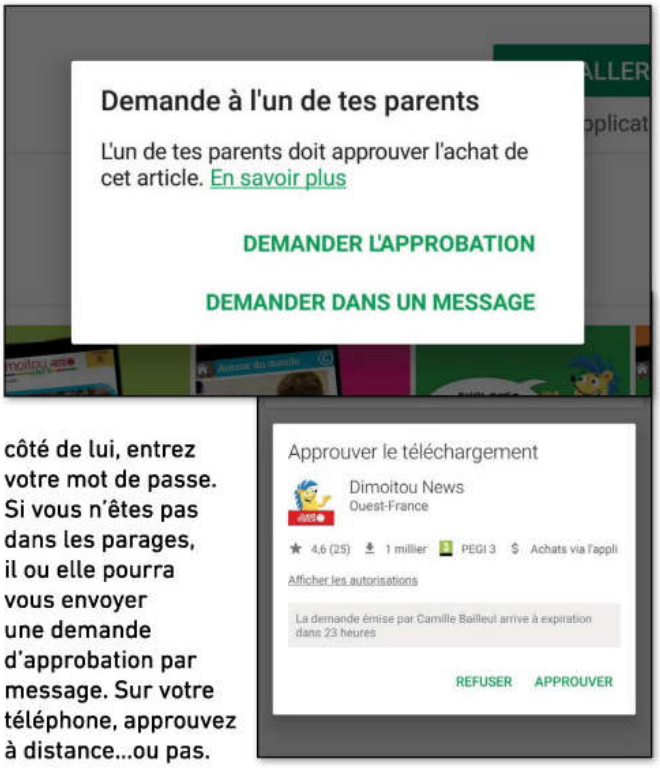
D'un seul coup d'œil vous pourrez voir le temps qu'ont passé vos enfants sur telle ou telle appli : hier, dans la semaine ou le mois en cours. Vous pourrez voir les autorisations accordées à cette appli et la bloquer si elle



vous semble inappropriée ou si vous jugez que votre rejeton passe trop de temps dessus.

08› APPROUVER UNE APPLICATION

Mais il est aussi possible de bloquer les installations d'appli pour les plus jeunes. Si votre enfant veut en télécharger une, il devra vous demander. Si vous êtes à



côté de lui, entrez votre mot de passe. Si vous n'êtes pas dans les parages, il ou elle pourra vous envoyer une demande d'approbation par message. Sur votre téléphone, approuvez à distance...ou pas.

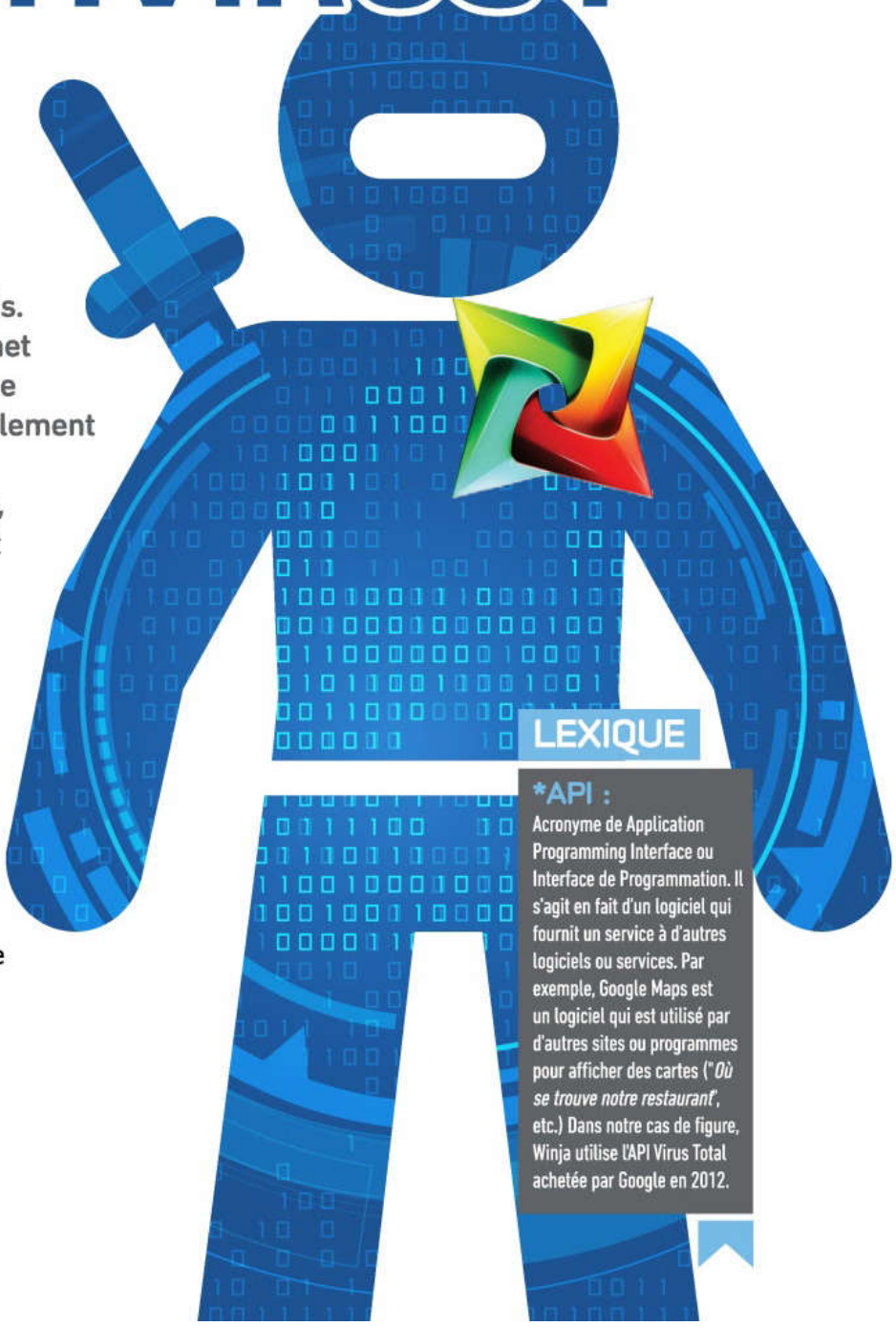
TUTO

POUR QUI ?
Pour tout le monde !

POUR QUOI FAIRE ?
Pour analyser des fichiers, des processus et des URLs

WINJA : LE PARTENAIRE DE VOTRE ANTIVIRUS !

Nous vous avions déjà parlé de Winja lorsque le logiciel est sorti il y a plusieurs mois déjà. Nous revenons dessus pour ce numéro car la société française Phrozen vient de lui ajouter certaines fonctionnalités. Rappelons que ce dernier permet d'éviter les contaminations et de surveiller un système potentiellement infecté. Un outil très complet permettant de scanner fichiers, URLs, services, programmes et tâches planifiées...



Phrozen SAS est une société française qui édite de nombreux logiciels de sécurité informatique : Who Stalks My Webcam pour surveiller l'activité de sa webcam, Windows Privacy Tweaker pour supprimer les mouchards de Windows 10, ADS Revealer qui se concentre sur une faille spécifique du système NTFS, RunPE Detector pour l'analyse de certains processus frauduleux et Shortcut Scanner pour surveiller les raccourcis Windows. Mais dans cet article, nous allons nous intéresser à Winja qui constitue le complément idéal à votre antivirus.

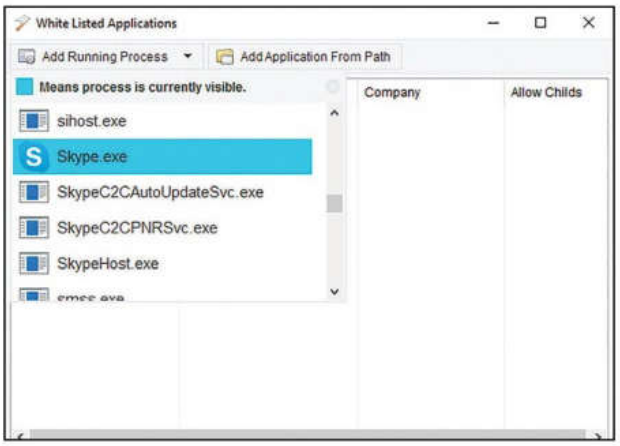
LEXIQUE

***API :**
Acronyme de Application Programming Interface ou Interface de Programmation. Il s'agit en fait d'un logiciel qui fournit un service à d'autres logiciels ou services. Par exemple, Google Maps est un logiciel qui est utilisé par d'autres sites ou programmes pour afficher des cartes (*"Où se trouve notre restaurant"*, etc.) Dans notre cas de figure, Winja utilise l'API Virus Total achetée par Google en 2012.

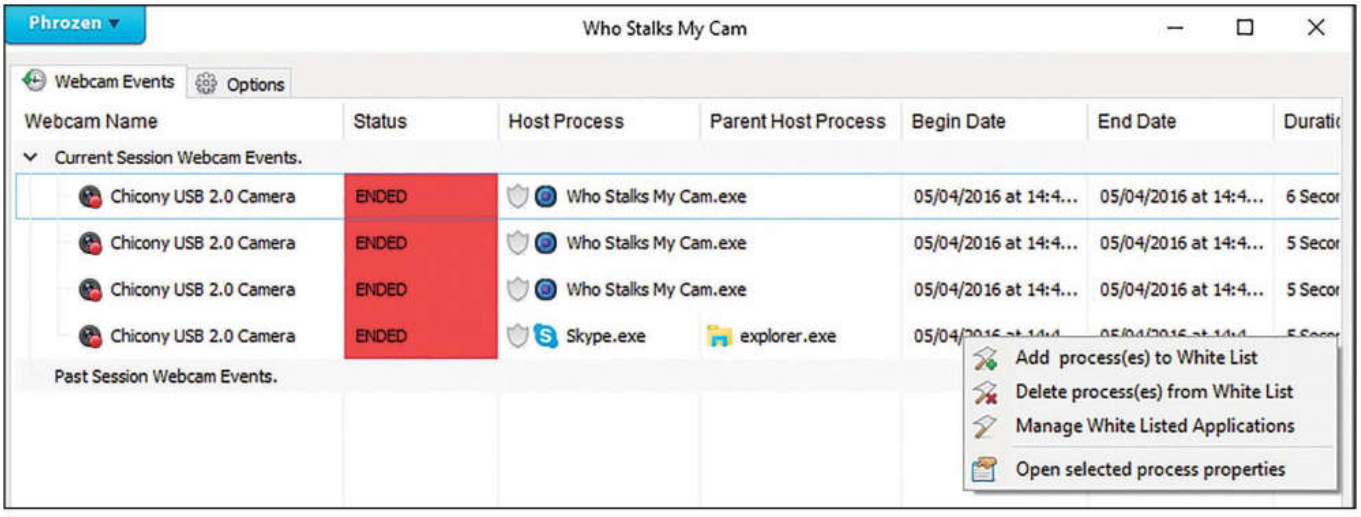
UN NINJA DANS VOTRE WINDOWS

Basé sur l'API Google Virus Total et développé de concert avec la firme américaine, Winja propose de soumettre n'importe quel fichier louche à une cinquantaine d'antivirus en ligne différents. Un doute sur un fichier avant de le télécharger ? Le logiciel va vérifier sa dangerosité avant même qu'il ne soit rapatrié sur votre ordinateur. Si « processus inconnu » vient apparaître dans votre gestionnaire des tâches, Winja ira se renseigner dans son immense base de données pour vous rassurer. Enfin d'autres outils vous permettront de mieux surveiller les planifications de tâches, les logiciels qui démarrent avec le système ou les services Windows qui peuvent aussi renfermer des saletés. Notez tout de même que Winja ne remplace pas un antivirus avec une protection d'arrière-plan. Par contre avoir les deux en même temps sur votre système ne causera aucun conflit… Bien sûr, tous les logiciels de chez Phrozen sont gratuits et sans publicité.

> *«Une fois que nous acceptons nos limites, nous les dépassons»*
>
> Albert Einstein



DANS LA PROCHAINE VERSION DE WINJA, LA SOCIÉTÉ PHROZEN VA AJOUTER LES FONCTIONNALITÉS DE WHO STALKS MY WEBCAM. LES DEUX LOGICIELS NE FERONT ALORS PLUS QU'UN !



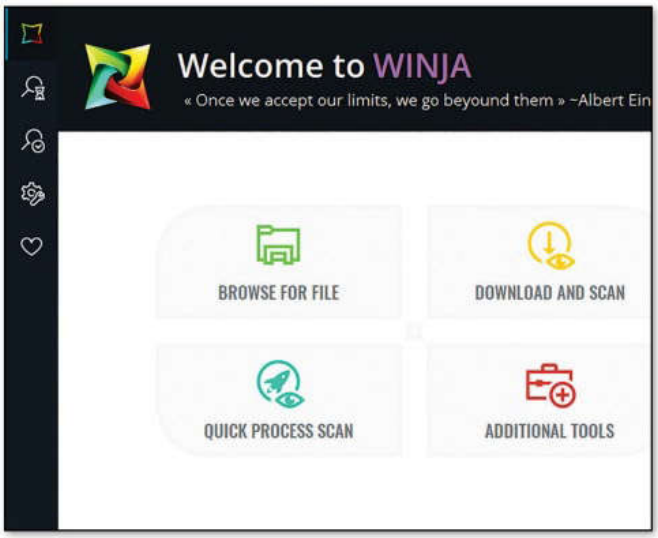
INFOS [Winja 5.1]
Où le trouver ? [www.phrozen.io/freeware/winja]
Difficulté :

LES FONCTIONNALITÉS DE WINJA

PRATIQUE

01› L'INTERFACE

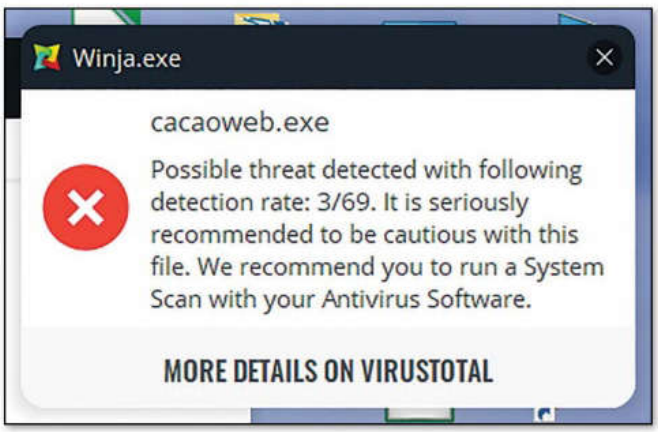
Après l'installation, l'interface va s'afficher avec ses différents boutons. Notez qu'il existe une version portable 32 ou 64 bits dans le ZIP où se trouve le fichier EXE. En vert vous



trouverez l'option pour ouvrir un fichier déjà présent sur votre PC, en jaune pour scanner un fichier en ligne, en bleu pour les processus actifs et en rouge pour les outils complémentaires. Ces derniers doivent être lancés en mode administrateur (en faisant un clic droit sur l'icône de Winja).

02› NOTRE TEST

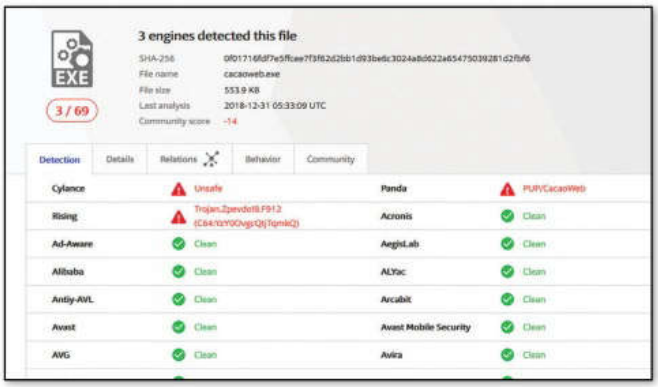
Pour tester, nous avons lancé un scan du controversé cacaoweb.exe. Le verdict est sans appel : infecté. Dès la fin du scan, une fenêtre vous



proposera d'aller directement sur le site Virus Total. Vous pouvez aussi demander un nouveau scan ou voir les propriétés du fichier.

03› 69 ANTIVIRUS À LA CARTE

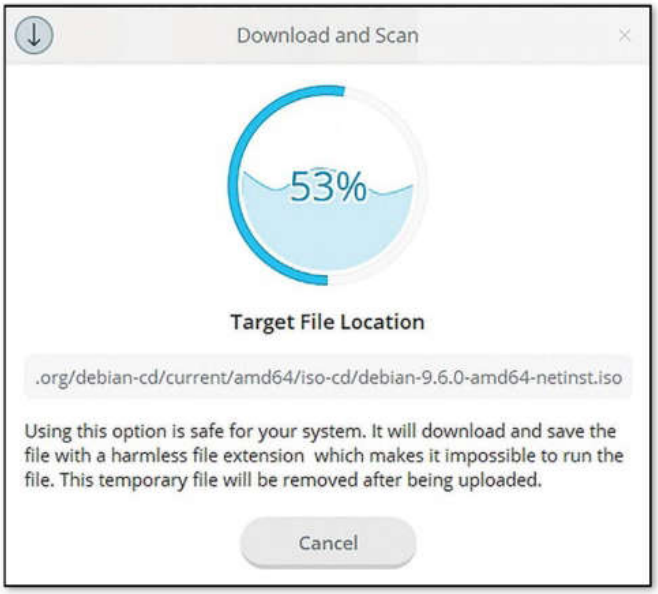
En fait, 3 des antivirus de l'API Virus Total sur les 69 trouvent que ce programme de stream contient un PUP (Potentially Unwanted Program) ou un trojan : pas un virus ou un ver donc, mais une crotte de nez au mieux



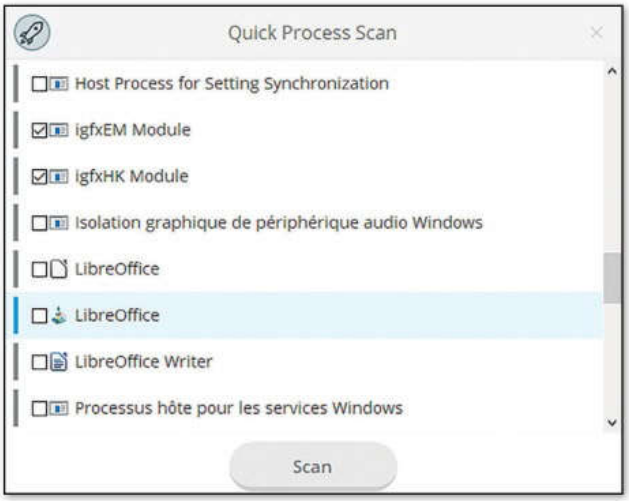
ou une belle saleté au pire. Même si la grosse majorité ne trouve rien à dire, il faudra se méfier. D'ailleurs Winja vous conseillera de lancer un scan avec votre antivirus. Notons qu'il peut aussi s'agir d'un programme «à décocher» lors de l'installation de cacaoweb. À vous de voir !

04› SCANNER AVANT DE TÉLÉCHARGER

Vous êtes sur un site et on vous propose de télécharger un fichier EXE ? Pourquoi prendre un risque ? Depuis votre navigateur, faites un clic droit dans le bouton de



téléchargement et faites **Copier l'adresse du lien** (ou équivalent). Dans Winja, allez dans **Download & Scan** puis copiez ce lien. Attendez le verdict.

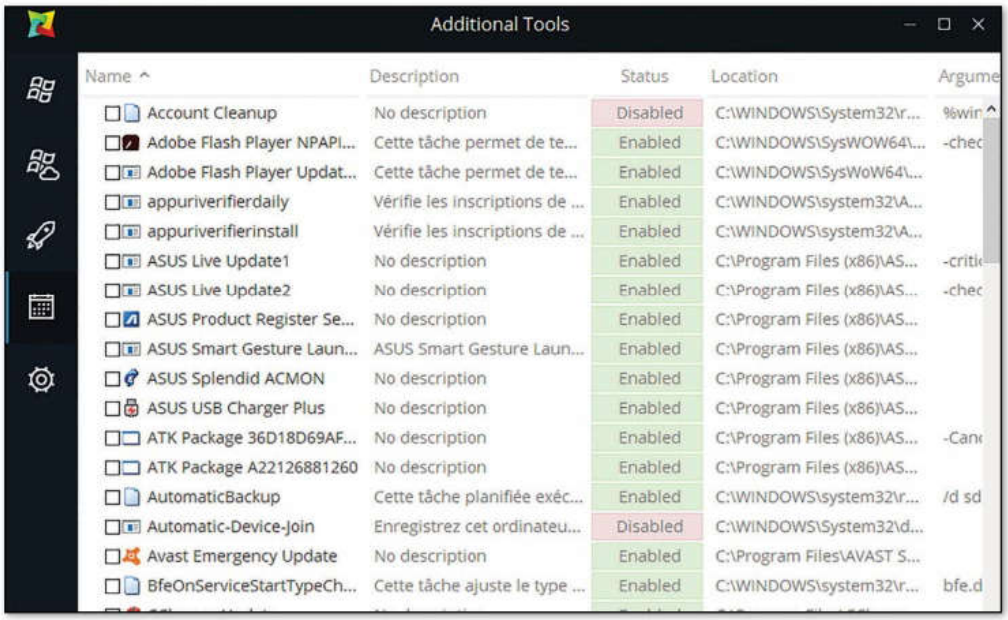


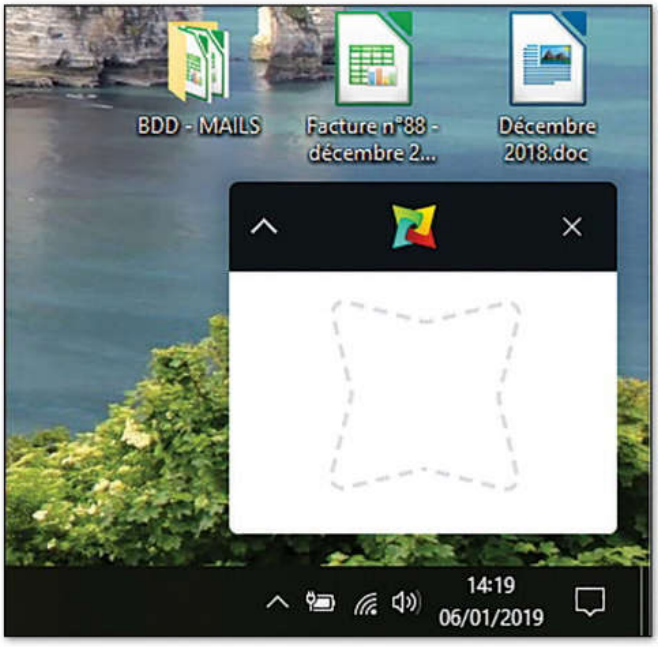
05› RAPIDE !

Dans **Quick Process Scan**, sélectionnez les programmes qui tournent en arrière-plan sans pourtant se manifester. Vous pourriez avoir des surprises : des noms méconnus sont parfois parfaitement légitimes tandis que d'autres aux noms «passe-partout» sont des malwares. Notez que Winja est très rapide, car il se base sur les précédentes recherches des internautes en se fiant à l'empreinte unique de votre fichier (hash MD5 et SHA-1)

06› DES OUTILS EN SUS

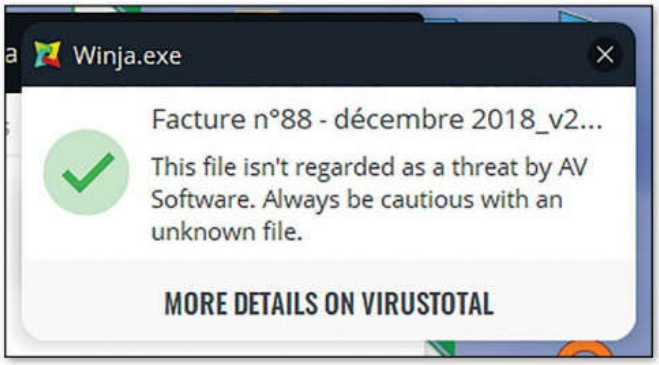
Enfin les **Outils supplémentaires** proposent un scan plus précis des processus, des tâches planifiées de Windows (qui peuvent être utilisées par des virus), des programmes qui se lancent au démarrage de Windows, et des services de Windows. Pour y accéder, il faudra juste accepter la proposition consistant à le lancer en mode administrateur.





07› UN WIDGET SUR LE BUREAU

En réduisant le logiciel, un petit widget va s'afficher sur le bureau. Il s'agit d'une zone où vous pouvez glisser-déposer vos fichiers pour les analyser.



VERROUILLEZ VOTRE PC AVEC UNE CLÉ USB

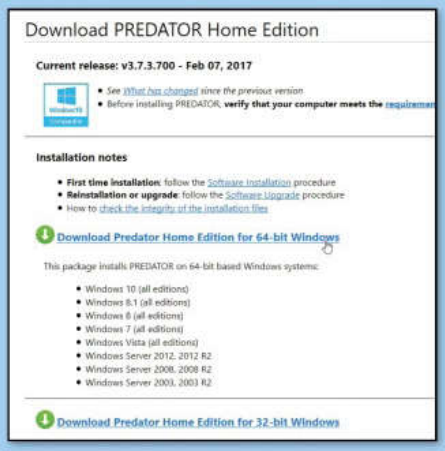
INFOS [Predator]
Où le trouver ?
[www.predator-usb.com]
Difficulté :

TUTO

Pour protéger l'accès à votre PC, il est possible d'utiliser une clé USB qui agira comme une vraie clé : sans elle, Windows ne démarrera pas. Attention, Predator Home Edition est utilisable gratuitement pendant 10 jours, à l'issue desquels il vous faudra vous acquitter d'une somme de 10 dollars (8,80 €) si vous voulez continuer à l'utiliser.

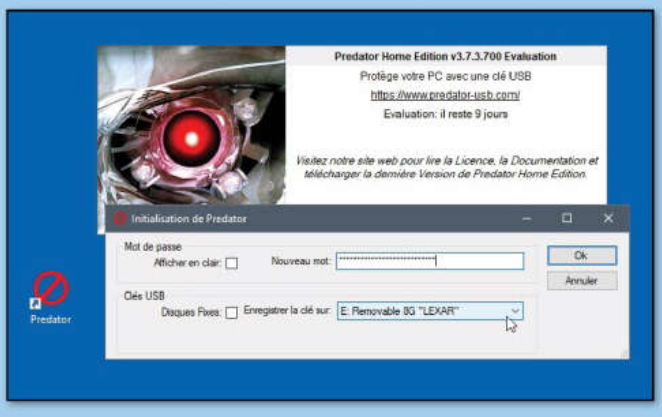
01 › INSTALLER LE LOGICIEL

Téléchargez le logiciel en suivant notre lien. A la section **Download**, choisissez la version Home compatible avec votre type de Windows (32 ou 64 bits). Pour le connaître, faites un clic droit dans **Ordinateur** puis sélectionnez **Propriétés** (Windows 7) ou allez dans les **Paramètres**, section **Système** puis **Informations Système**. Décompressez l'archive et lancez **InstallPredator**.



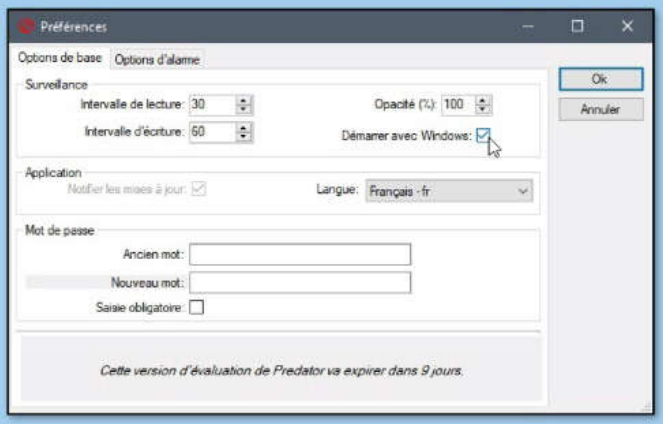
02 › DÉFINIR UN MOT DE PASSE

Lancez le programme, et validez par **OK**. Définissez un mot de passe, de préférence assez long : c'est plus sûr, et il ne sera utilisé qu'au cas où vous n'auriez pas votre clé sous la main. Dans **Clés USB**, sélectionnez votre clé après l'avoir branchée. N'importe quelle clé fera l'affaire, et vous pourrez toujours l'utiliser pour stocker des données. Validez.



03 › ACTIVER AU DÉMARRAGE

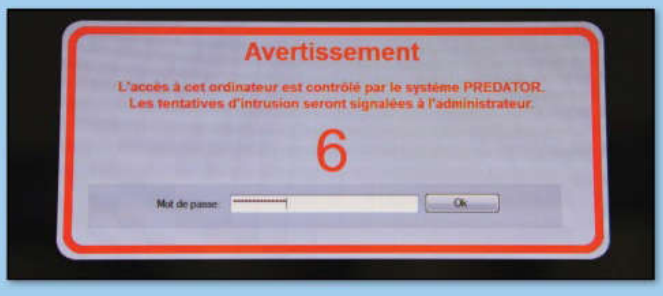
Laissez le programme faire son travail (préparer la clé). Puis allez dans la zone de notification (en bas à droite près de l'horloge) pour trouver les **Préférences** du programme



avec un clic droit dans la nouvelle icône verte. Cochez la case **Démarrer avec Windows** afin que Predator soit activé à chaque démarrage de l'ordinateur.

04 › UTILISER LA CLÉ

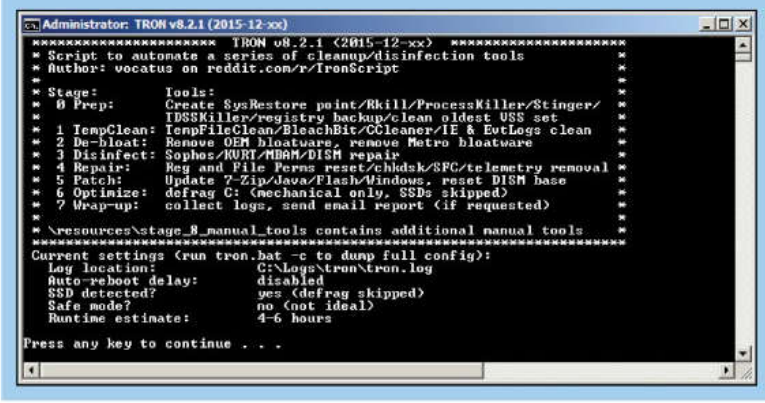
Lorsque vous quittez votre ordinateur, retirez la clé de son port USB. Au bout de 30 secondes, l'écran devient noir. Si vous tapez sur le clavier, Predator vous invite à remettre la clé USB ou à saisir votre mot de passe de secours. Chaque tentative d'intrusion sera répertoriée dans un journal et il est même possible de déclencher une alarme afin de décourager les indélicats.



Désinfectez et réparez
> avec Tron

Tron n'a rien à voir avec le Maître Control Principal, des motos futuristes ou Jeff Bridges. Il s'agit d'un script qui va vous permettre de récupérer un PC (de XP à Windows 10) en pleine santé. Il automatise des tâches bien connues des réparateurs de PC en herbe tout en proposant des outils bien utiles. C'est donc un total de 698 Mo de solutions de réparation/désinfection/optimisation/nettoyage qui vous est proposé : antivirus, patch, anti-bloatware, tueur de processus, récupération d'un registre sain, etc. Vous devrez lancer l'EXE en mode sans échec à condition d'être en mode administrateur. Attention, comme la plupart des actions sont automatiques, veillez à bien sauvegarder vos documents. Si ce n'est pas possible, Tron créera un point de restauration pour ne pas partir de plus bas que vous ne l'étiez...

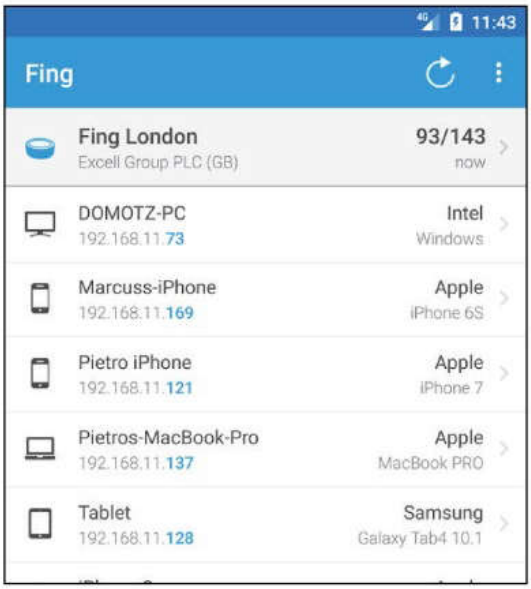
Lien : **www.bmrf.org/repos/tron**



Expulsez les squatteurs de Wi-Fi
> avec Fing Network Tools

Rien de plus rageant que de voir son réseau Wi-Fi complètement aux fraises, sans aucune raison. Vous ne le savez peut-être pas, mais il est possible que certains voisins mal intentionnés ne se privent pas d'utiliser votre connexion. Avec l'application Android Fing Network Tools, dénichez les squatteurs et expulsez-les par la même occasion. Il est aussi possible de « signer » vos appareils domestiques pour être immédiatement averti d'une intrusion.

Lien : **https://goo.gl/0MRB3p**



Récupérez vos données malgré une infection par PyLocky
> avec PyLocky Decryptor

Le ransomware PyLocky fait des ravages en France, mais heureusement il existe une solution ! Rappelons qu'un ransomware est une belle saleté qui va cibler les types de fichiers ayant une valeur sentimentale ou pratique (photo, vidéo, DOC, XLS, etc.) et les chiffrer avec une double clé très solide. Au bout de quelques minutes, vos fichiers deviennent inaccessibles et un message s'affiche sur votre écran. Ce dernier vous invite à payer une somme d'argent pour récupérer la clé privée ayant servi au chiffrement et ainsi retrouver vos données. Bien sûr, nous vous déconseillons de payer, car cela encourage la pratique sans vous donner la garantie de revoir vos précieuses photos par exemple. En cas d'infection par un ransommawe, nous vous conseillons d'éradiquer le mal à la base (désinfection complète du PC) et de garder vos données malencontreusement chiffrées dans une clé USB ou un disque dur externe en attendant une éventuelle solution. Les victimes de PyLocky vont exulter puisqu'il existe une parade depuis peu. La seule contrainte c'est d'avoir conservé le fichier PCAP de votre PC infecté. Si vous avez formaté C, c'est peu probable, mais vous trouverez les explications ici : **https://github.com/Cisco-Talos/pylocky_decryptor.** Et si vous êtes victime d'un autre ransomware, faites un tour ici pour potentiellement trouver des ressources : **www.nomoreransom.org**

TUTO

POUR QUI ?

Pour les utilisateurs qui veulent manipuler leurs fichiers vidéo

POUR QUOI FAIRE ?

Pour encoder, couper, scinder, muxer, convertir ou synchroniser des vidéos !

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

Connu depuis des années par les aficionados de l'encodage vidéo, m4ng (anciennement Ri4m) 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.

LEXIQUE

***RIP :** Les vidéos sur un DVD ou un Blu-ray ne peuvent être transférées sur votre disque dur avec un simple "copier-coller". Il faut les extraire avant l'encodage. C'est ce qu'on appelle le "Rip".

***CODEC :** Mot-valise pour «codeur-décodeur». Il s'agit d'un petit programme capable de compresser et/ou de décompresser un signal numérique : audio ou vidéo. Il ne faut pas confondre le codec (Xvid ou x.264 par exemple) avec le format de fichier (.mkv, .mp4, etc.)

***ENCODAGE :** L'encodage est le fait de modifier une vidéo avec un codec. Il s'agit la plupart du temps de gagner de l'espace (compression du fichier initial) ou de modifier la vidéo pour qu'elle fonctionne sur un appareil particulier.

Medi4 next gen (abrégé 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, console portable 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.

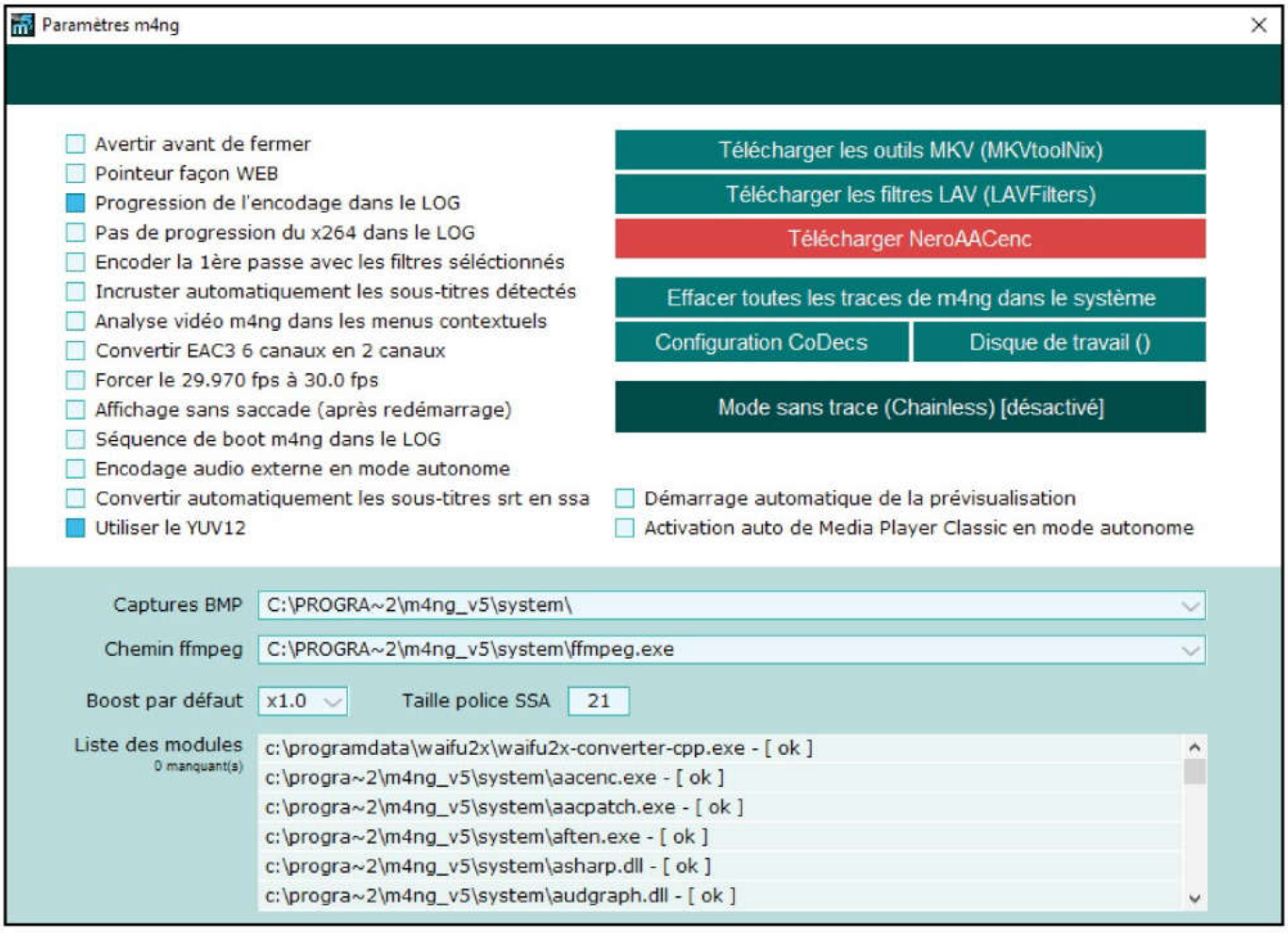
DEUX MODES POUR TOUCHER LE PLUS GRAND NOMBRE D'UTILISATEURS

Le plus important, c'est que vous n'avez pas à être un expert en codecs ou en jargon technique puisque le mode **Simplifié** 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 **Avancé** 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.

PLUS D'UN TOUR DANS SON SAC !

m4ng permet d'encoder ou de réencoder tous vos fichiers vidéo. Il comprend les formats AVI, OGM, MKV, MPEG, MP4, WMV, 3GP, smartphone Android et iPhone/iPad et permet de les convertir en DivX, Xvid, x264, x265 (à l'essai dans cette version 5), MPEG1, MPEG2, VP8, XMV, etc. Un boulot extraordinaire a été fait au niveau de la gestion audio : AC3, DTS, AAC, MP3, MP2 et OGG (en stéréo et 5.1). Rares sont les codecs absents de la liste.

DANS LES PARAMÈTRES DU LOGICIEL, LES PLUS EXIGEANTS TROUVERONT MOULT FONCTIONNALITÉS EN PLUS DE CELLES QUI SONT DISPONIBLES DANS LES MENUS...

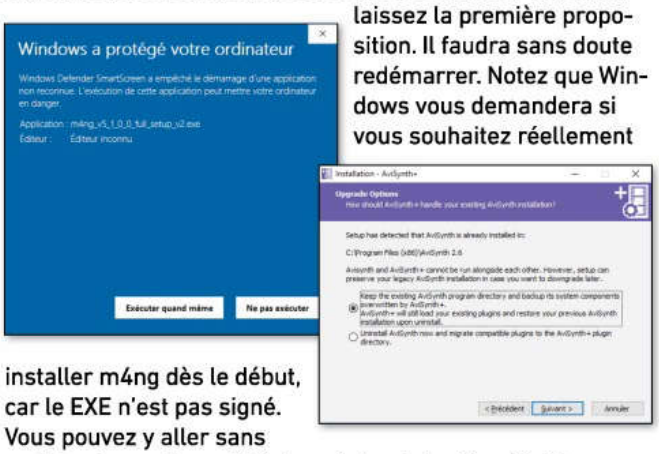


COMMENT UTILISER M4NG ?

PRATIQUE

01 › PREMIERS PAS

Lors de l'installation, n'oubliez pas de valider pour intégrer **AVIsynth** et **LAME**, deux logiciels indispensables au bon fonctionnement de m4ng. Si vous ne savez pas quoi répondre lorsqu'on vous posera une question sur AVIsynth, laissez la première proposition. Il faudra sans doute redémarrer. Notez que Windows vous demandera si vous souhaitez réellement



installer m4ng dès le début, car le EXE n'est pas signé. Vous pouvez y aller sans crainte si vous l'avez téléchargé depuis le site officiel.

02 › L'INTERFACE

L'interface n'a rien de bien sorcier. Sur la gauche, on a la fenêtre du m4ng **Video Analyser** qui va afficher les codecs présents sur votre machine. Notez en haut la présence d'un bouton pour utiliser le mode **Autonome** permettant de fonctionner sans aucune installation de logiciels tiers et/ou codecs externes. 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. Au centre, on trouvera la partie qui concerne la vidéo en elle-même. Pour commencer à travailler avec le logiciel, il faudra glisser-déposer un ou plusieurs fichiers ici.

03 › LE MODE SIMPLIFIÉ

Comme nous vous l'expliquions plus haut, m4ng est conçu pour les débutants avec un mode simplifié sans fonctionnalités compliquées. Imaginons que vous voulez utiliser un ou plusieurs fichiers vidéo très lourds sur une tablette ou un smartphone limité à 32 Go de stockage par exemple. Après avoir placé la vidéo dans l'interface, vous verrez le détail du fichier sur la gauche (codec, débit, nombre d'images par seconde, etc.) Vous pourrez alors choisir 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. Pour un smartphone Android par exemple ce sera le codec x264 qui sera sélectionné d'office, à vous de choisir ensuite la résolution et la qualité souhaitées. Tout le reste sera géré par m4ng. Pour les iPhone/iPad, il faudra choisir votre modèle pour que m4ng sache quels paramètres choisir...

DEUX CONCURRENTS À M4NG...

Format Factory

Format Factory est un logiciel très simple qui permet de convertir tous les types de fichiers les plus courants dans le domaine de la vidéo, de l'audio et de la photo. Il gère même les fichiers images (virtualisation d'un CD ou DVD) que vous pouvez télécharger sur Internet ou extraire à partir d'une galette. Là où certains programmes sont spécialisés dans un seul domaine, FF gère sans problème de nombreux formats et ne vous laissera jamais sur le bord de la route. Il suffit de choisir son fichier de départ et de choisir son format de sortie dans la liste. Une bonne alternative à m4ng pour les débutants...

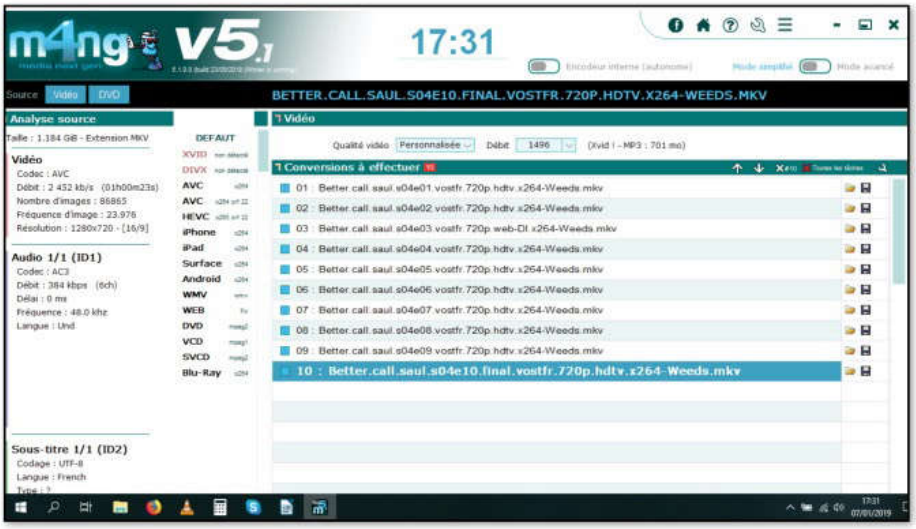
Lien : **https://format-factory.fr.softonic.com**

SUPER©

Malgré son interface un peu rude, ce dernier propose d'encoder et de convertir tous les fichiers multimédias que vous voulez. Comme m4ng, SUPER apporte une interface graphique unifiée à divers programmes et librairies d'encodage (x264, FFmpeg, Mplayer, etc.) dans le but de proposer un outil ultime. Il suffit de prendre un ou plusieurs fichiers et de choisir le conteneur et les codecs de votre choix pour lancer la machine. Les plus exigeants pourront bien sûr choisir le bitrate, la résolution, le ratio de l'image, etc. Les débutants, eux, auront à disposition des préréglages pour différents appareils : consoles, produits Apple, Android, etc. Attention, ce logiciel n'est pas vraiment conseillé pour les débutants !

Lien : **www.erightsoft.com**

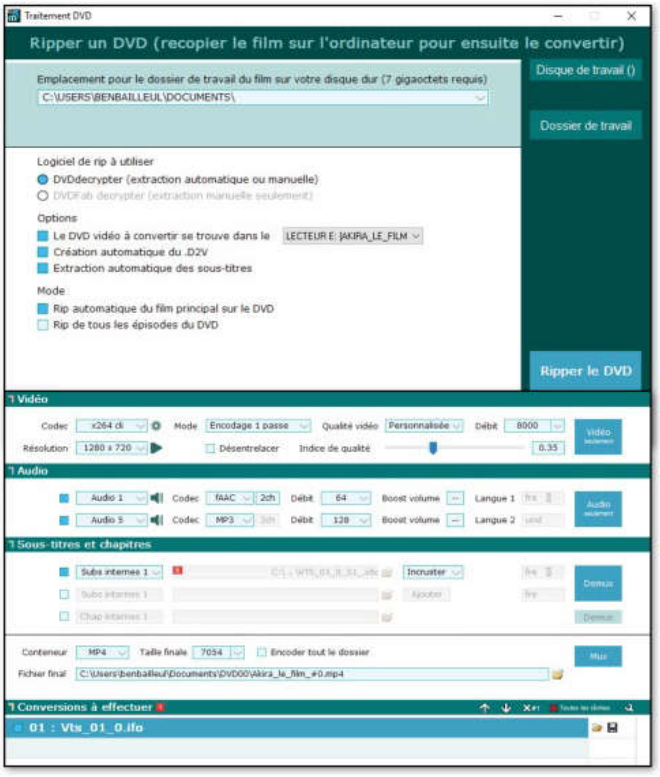
04 LE MODE AVANCÉ



Dans le mode **Avancé**, vous aurez aussi à choisir le format de sortie, mais les options seront bien plus nombreuses : réglage interne du codec, résolution, débit (bitrate), désentrelacement, encodage en 2 passes (plus long, mais de meilleure qualité), encodage de son, ajout ou incrustation de sous-titres, type de conteneur, taille finale, etc. Juste au-dessus de la liste des fichiers vous pourrez enregistrer la liste des tâches ou éteindre le PC une fois terminé en cliquant sur l'icône en forme de clé (pas celle de tout en haut !). Ce mode permet le réencodage de la piste audio ou vidéo uniquement (si votre film d'origine fonctionne, mais sans le son, pas besoin de réencoder la vidéo par exemple). Faites **Convertir** ou optez pour un déclenchement différé (en bas à droite).

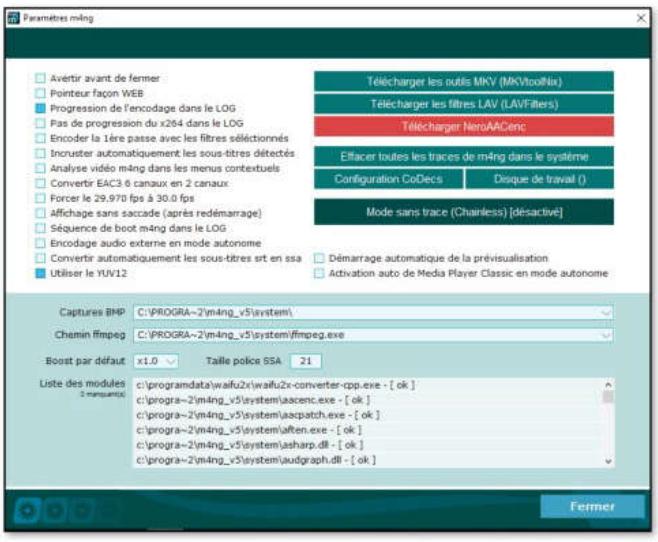
05 RIP D'UN DVD OU D'UN BLU-RAY

Si vous désirez ripper et encoder un DVD ou un Blu-ray, il faudra d'abord installer DVD Decrypter par exemple (**www.dvddecrypter.org.uk**) et aller dans le menu DVD en haut à gauche. Sans prise de tête et sans passer par les menus parfois compliqués de DVD Decrypter, vous pourrez ripper un film, des épisodes avec les différentes pistes audio et les sous-titres. Une fois que le rip est terminé, m4ng reprend la main et vous propose de faire votre petit marché : choisissez le codec vidéo, les nombres de pistes audio et ajoutez des sous-titres si vous n'êtes toujours pas à l'aise avec le japonais malgré le visionnage des 867 épisodes de One Piece...



06 LES AUTRES FONCTIONNALITÉS

M4ng est plein de surprises puisque le développeur a ajouté d'autres fonctionnalités pour jongler avec vos vidéos. Dans le menu avec le bouton en forme de clé (en haut à droite cette fois !), vous aurez accès aux outils de découpe, fusion ou mux/demux (séparation ou ajout de pistes audio), d'upscale HD, de corrections de décalage (audio/vidéo et vidéo/sous-titres), de création de structure DVD, etc.



TUTO

ROMSTATION
LA MACHINE À REMONTER LE TEMPS

RomStation est un logiciel d'émulation relié à une gigantesque base de données. Il est donc possible de télécharger des jeux consoles, PC et d'arcade puis de les lancer depuis la même interface. Compatible avec une vingtaine de machines, RomStation permet aussi de jouer en ligne avec des adversaires humains.

LES SYSTÈMES ÉMULÉS

NINTENDO : Game Boy (standard, Color et Advance), NES, Super Nintendo, N64, GameCube et Wii.

SEGA : Game Gear, Master System, Mega Drive, Mega-CD, 32X, Saturn et Dreamcast.

SONY : PlayStation et PlayStation 2

AUTRES : PC, 3DO, PC-Engine et Arcade (MAME, NeoGeo, etc.)

Pour jouer à de vieux jeux, il fallait jusqu'à présent télécharger un émulateur, des ROMs ou des ISOs (les jeux au format numérique) et lancer le tout sur votre ordinateur. Il fallait faire la même chose pour chaque système que vous vouliez émuler en cherchant des jeux sur Internet. Avec RomStation, tout va changer !

Depuis la même interface, vous choisissez, téléchargez et jouez à des milliers de jeux sans chercher, décompacter ou bidouiller quoi que ce soit. Il suffit de cliquer sur un bouton et cela fonctionne puisque tous les émulateurs ainsi que les BIOS nécessaires au fonctionnement sont intégrés dans les 188 Mo du programme. Attention, n'espérez pas émuler de la Wii avec un PC vieux de 5 ans tout de même...

MULTI-JOUEURS !

Une des fonctionnalités intéressantes du logiciel, c'est la possibilité de mettre en relation d'autres utilisateurs pour jouer à des jeux qui normalement ne permettent le multijoueur qu'en local. Il est donc possible de jouer à GoldenEye 64, Mario 64 ou Monster Hunter avec des joueurs distants.

> RomStation agit comme une fontaine de jouvence. C'est un plaisir de retrouver les jeux de sa jeunesse...

RECALBOX : UN OS DÉDIÉ AU RÉTOGRAMING...

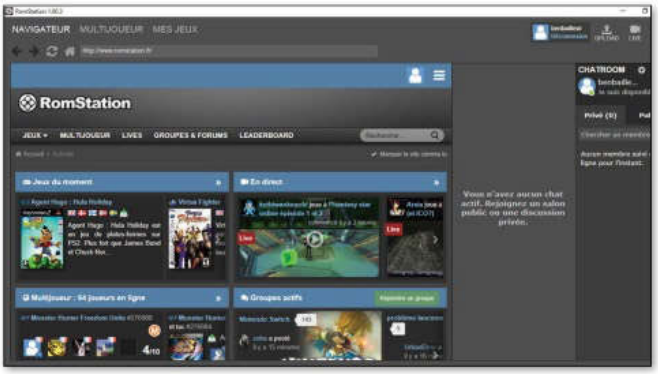
Recalbox est un OS gratuit et libre dédié au rétrogaming. Installable facilement sur Raspberry Pi, il est aussi compatible avec les cartes Odroid. Vous n'avez rien de tout ça ? Pas de problème puisque la dernière version 4.1 permet d'installer le système entier sur un PC, même de configuration modeste. Mais ce n'est pas la seule nouveauté puisque la liste des émulateurs s'est dernièrement agrandie avec la présence de la Sony PSP, du Commodore 64, de l'Apple II et... de la Dreamcast. La dernière console de Sega fait figure de Graal pour certains gamers qui pourront s'adonner à *SoulCalibur*, *Crazy Taxi*, *Ikaruga*, *Marvel VS Capcom 2*, ou *Shenmue*, ce magnifique jeu qui a plombé les comptes de Sega jusqu'à faire disparaître la société. Au final ce sont plus de 50 machines et 40 000 jeux qui sont supportés par Recalbox. Outre l'ajout de ces nouvelles machines, Recalbox intègre un paquet d'autres nouveautés : overclock et gestion du Bluetooth interne du Raspberry Pi 3, gestion des NAS, clavier virtuel, gestion via interface Web, un nouveau scrappeur pour les métadonnées (jaquettes, descriptions, etc.), des achievements/trophées, un démarrage personnalisé et encore plein d'autres choses. Car même si ces fonctionnalités ne font pas partie des nouveautés, notons qu'en plus des «savestates» (des sauvegardes à la demande dans n'importe quel jeu), Recalbox propose une option de rembobinage. Si votre plombier italien a la mauvaise idée de tomber dans un trou, il suffit de «rembobiner» pour éviter de perdre une vie ! Le logiciel PrBoom permet de jouer à *Doom* et à toutes les cartes amateurs au format .wad, quant à ScummVM il permet d'émuler les point'n click de LucasArts (*Day of the Tentacle*, etc.) ou Sierra (*Les Chevaliers de Baphomet*, etc.) Cela vous semble limité et vous voudriez d'autres jeux PC ? C'est possible avec l'intégration de DOSBox même s'il faudra un peu lutter. Enfin, et pour parfaire le système, Recalbox contient le media center Kodi !

COMMENT JOUER AVEC ROMSTATION ?

PRATIQUE

01 INSTALLATION

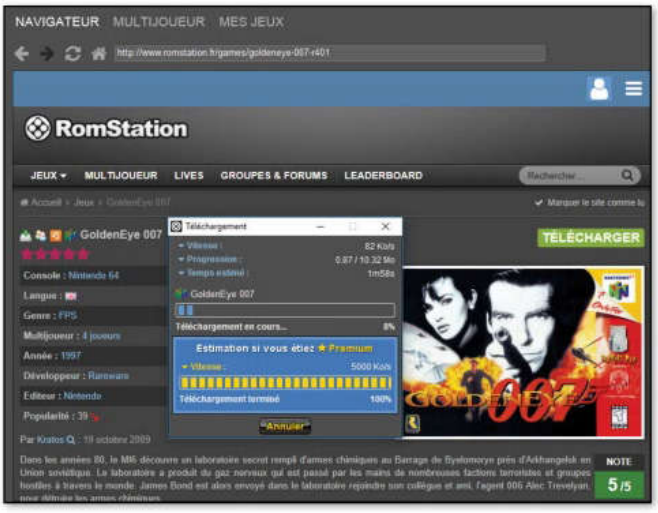
Sur la page principale du site, cliquez sur **Installer RomStation** en haut à gauche et lancez le fichier EXE. Vous devrez sans doute installer des composants additionnels comme DirectX, mais tout se fait de manière automatique.



Inscrivez-vous sur le site et validez cette inscription sur votre boîte aux lettres avant de rentrer vos identifiants dans l'application RomStation.

02 VOTRE PREMIER JEU

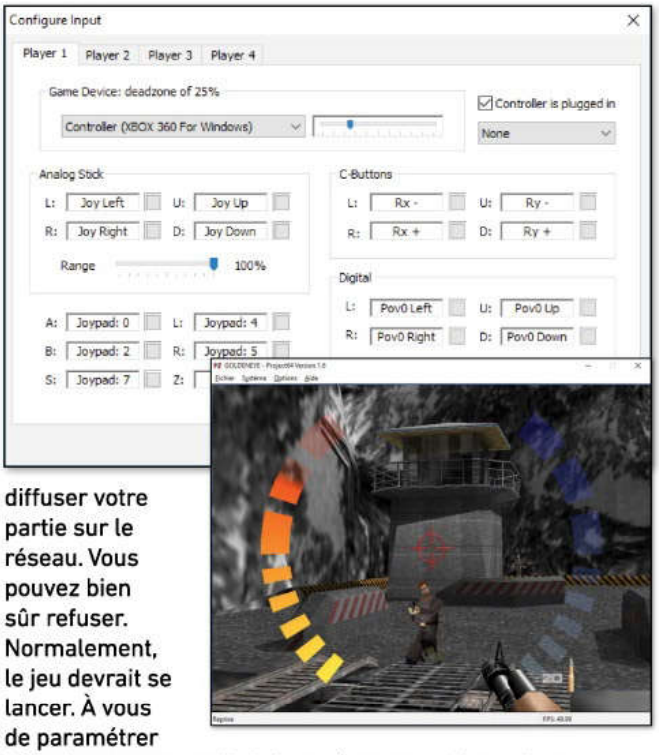
Choisissez votre système en cliquant sur l'icône adéquate puis recherchez un jeu. Dans notre exemple, nous allons jouer à GoldenEye 64, ce chef-d'œuvre du multijoueur local sur la N64 de Nintendo. Cliquez sur **Télécharger** et



lorsque le processus sera fini, faites **Jouer**. Notez qu'il existe des versions de jeux modifiées comme le mode coopératif à 4 joueurs de Zelda : Ocarina of Time.

03 LE BON ÉMULATEUR

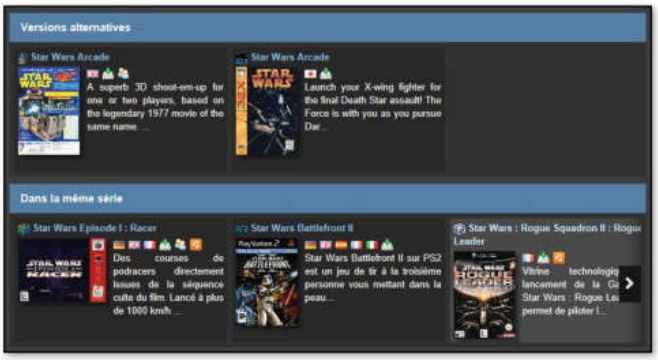
Si le système comporte différents émulateurs, le logiciel vous proposera de choisir celui que vous voulez utiliser. Après avoir validé, RomStation vous propose de



diffuser votre partie sur le réseau. Vous pouvez bien sûr refuser. Normalement, le jeu devrait se lancer. À vous de paramétrer l'émulateur pour qu'il s'adapte à votre configuration : manette ou clavier, qualité de la vidéo, du son, etc. Chaque émulateur propose ses propres réglages.

04 LE MULTI

Vous retrouverez les jeux que vous avez déjà téléchargés dans l'onglet **Mes Jeux**. Si le cœur vous en dit,



faites un tour dans **Multijoueur**. Cliquez sur **Rejoindre** pour accéder à la partie. Notez aussi que si vous sélectionnez un jeu Star Wars par exemple, le logiciel vous proposera des jeux en rapport avec cet univers.

NOUVEAU !

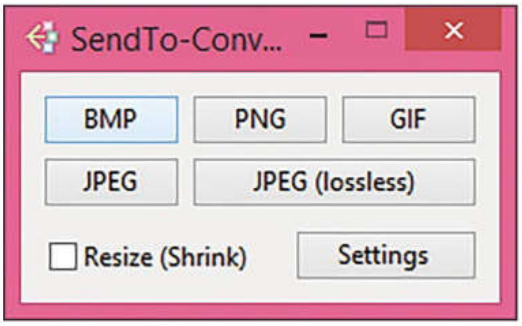
Par l'équipe de *Pirate Informatique* !

L'officiel PC
RASPBERRY PI
Idées & Projets Clés en Main

GUIDE COMPLET

CHEZ VOTRE MARCHAND DE JOURNAUX

Convertir des images depuis le menu contextuel > Avec SendTo-Convert



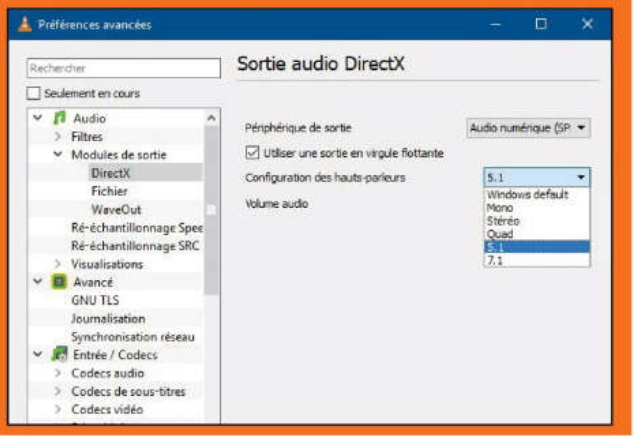
Vous avez fréquemment besoin de convertir des images, pour illustrer un blog ou vos posts sur Facebook ? Téléchargez et installez SendTo-Convert, puis lancez le logiciel et cochez la case **Add to Send To menu** (si vous ne la voyez pas, cliquez sur le bouton **Settings**). Une nouvelle entrée apparaît dans le menu contextuel, lorsque vous faites clic droit > **Envoyer vers** sur l'image à convertir. Plusieurs options de format s'affichent (**BMP**, **PNG**, **GIF**...). Le fichier converti se place dans le même dossier que celui de départ.

Lien : **http://goo.gl/F933fK**

Forcer le son Surround > avec VLC

Vous voulez exploiter à fond votre équipement audio ? Pour bénéficier du meilleur son sur le lecteur multimédia VLC, ouvrez le menu **Outils** > **Préférences**. Choisissez d'afficher **Tous** les paramètres, en bas à gauche, puis déroulez **Audio** > **Modules de sortie** > **DirectX**. Sélectionnez votre matériel audio dans **Périphérique de sortie** et choisissez le format de son supporté par votre appareil dans **Configuration des hauts-parleurs**. Pour le son Surround, optez pour **5.1** ou **7.1**. N'oubliez pas d'**Enregistrer** les modifications.

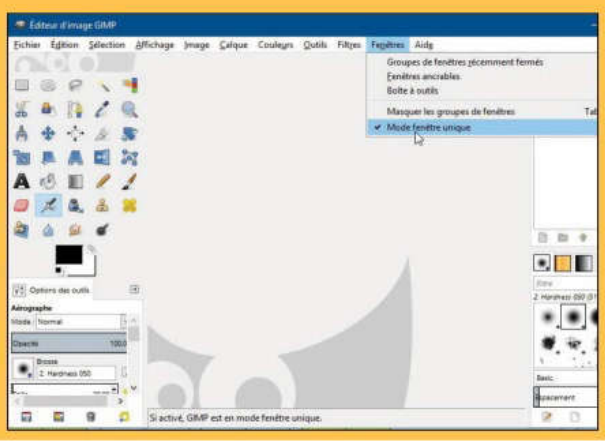
Lien : **www.videolan.org/vlc**



Simplifier l'interface du logiciel > Avec Gimp

Gimp est le logiciel gratuit de référence en matière de retouche d'image. À adopter si ce n'est déjà fait ! Mais sa prise en main est un peu délicate, et son mode multi-fenêtres ne facilite pas les choses. Pour simplifier, déroulez le menu **Fenêtres** et cochez **Mode fenêtre unique**. L'espace de travail et les différentes palettes d'outils sont alors rassemblés dans la même fenêtre, comme c'est généralement le cas pour la plupart des logiciels.

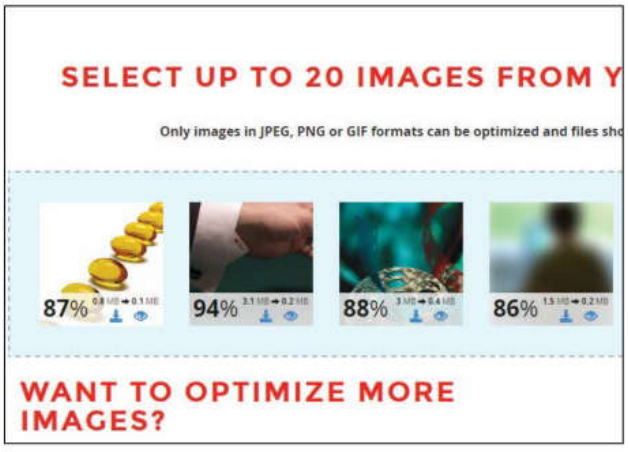
Lien : **www.gimp.org**



Optimiser ses images pour le Web > avec Short Pixel

Cette application en ligne réduit le poids de vos clichés sans en dégrader outre mesure la qualité. Commencez par vous enregistrer (**Sign Up**) puis sélectionnez la première ligne pour essayer l'outil gratuitement (**Free Plan**). Rendez-vous dans l'onglet **Compress** puis faites glisser les photos à compresser dans le champ principal (**Drog up...**). La compression des images téléversées est mentionnée en **%**. Cliquez sur l'icône avec la flèche pour rapatrier votre cliché compressé.

Lien : **https://shortpixel.com**

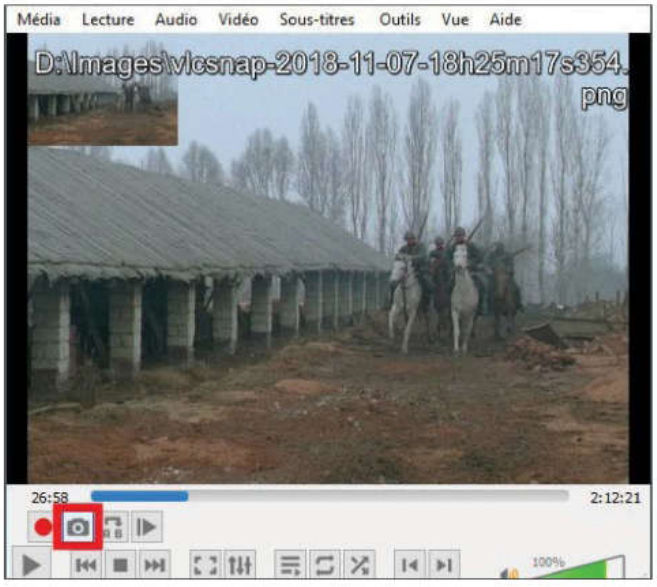


Éviter les saccades > Avec VLC

VLC est l'un des lecteurs multimédias les plus complets et les plus ergonomiques. Cependant, ce n'est pas celui qui économise au mieux les ressources de votre PC, et des saccades peuvent parfois apparaître à la lecture d'une vidéo sur un ordinateur peu puissant. Si cela vous arrive, ouvrez **Outils** > **Préférences** > **Entrée/Codecs**. Pour l'option **Décodage matériel** optez pour **Automatique**. Réglez ensuite l'option **Inhiber le filtre de boucle H.264** sur **Tous**.

Capturer une image d'un film > Avec VLC

Ouvrez le film ou la vidéo dont vous souhaitez capturer une vue, et mettez en pause sur l'image que vous désirez capturer. Au besoin, revenez très légèrement en arrière avec le curseur de temps, puis utilisez le bouton **Image par image** pour ajuster précisément (4e icône, juste sous la barre temporelle). Lorsque vous êtes sur la vue désirée, cliquez sur **Prendre une capture d'écran** (2e icône). La vue est enregistrée dans votre dossier **Images**.



Enregistrer le son d'une vidéo YouTube > avec YouTube-mp3.org

Les outils pour capter le son d'une vidéo YouTube, cela ne manque pas. Ces derniers sont en revanche souvent bourrés de pubs bien envahissantes. YouTube-mp3.org a le mérite d'être rapide et de n'arborer aucune pub. Nul besoin de créer de compte ici. Faites un copier-coller de la vidéo qui vous intéresse dans le champ principal puis faites **Convertir la vidéo**. Rapatriez le son avec **Télécharger**.

Lien : **www.youtube-mp3.org/fr**

PORTABLE IMSI/IMEI/TMSI CATCHER

Connaissez-vous les IMSI Catcher ? Il s'agit d'appareils tenant dans une petite valise permettant à la police ou aux services secrets de faire croire aux téléphones mobiles des environs qu'il s'agit d'une antenne relais de confiance. La portée est variable et dépend du type d'appareil, mais une fois que le téléphone cible accepte le IMSI-catcher en tant qu'antenne, le chiffrement GSM peut être tout simplement désactivé ! Bien sûr l'utilisateur n'est prévenu de rien et voilà que ses conversations ont aussi publiques que s'il parlait dans un talkie-walkie à 10 €. Alors que ces appareils étaient réservés à des entités gouvernementales ou des pirates très fortunés, les prix sont en train de se démocratiser. La plupart du temps ces appareils sont vendus comme des passerelles GoIP (comme sur Alibaba.com), mais il faudra quand même débourser pas loin de 1500 € pour en acquérir un. On trouve même des versions miniatures avec écran LCD. Rappelons qu'il est possible de se protéger (ou au moins de détecter) ces appareils grâce à une application Android «IMSI Catcher» que vous pourrez trouver ici : **http://goo.gl/loZ1ws**

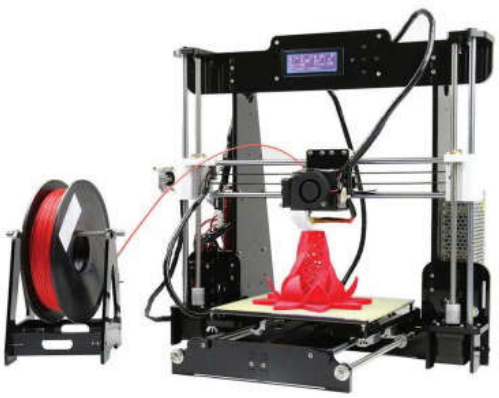
Prix : **NC**
Lien : **https://frama.link/v8PdvPCH**

HDD RAINBOW TABLE, DU CRACK PRÊT À L'EMPLOI !

Voilà un disque dur Wesrtern Digital USB 3.0 de 2 To un peu spécial. Celui-ci est en effet rempli de rainbow tables en tout genre ! Rappelons que le principe de rainbow table est une technique de « compromis temps-mémoire » réduisant considérablement le temps nécessaire pour casser un mot de passe. Une rainbow table, c'est une sorte de tableau avec un mot de passe de départ dans la première colonne et un mot de passe d'arrivée dans la dernière. Dans les colonnes du milieu, on va trouver des mots de passe intermédiaires qui sont obtenus avec des calculs appelés fonction de réduction. Une fonction de réduction transforme une empreinte de mot de passe en un nouveau mot de passe. Au final, on ne va garder que le premier et le dernier mot de passe générés puisque le reste de la chaîne (les colonnes du milieu) peut être retrouvé en refaisant des calculs beaucoup plus rapides que tout le processus d'un brute force. L'inconvénient, c'est qu'il vous faut générer ces fichiers rainbow tables en amont et que c'est souvent lent et fastidieux. Ici, vous avez donc un disque plein de sortes de tables différentes : MD5, A5/1, WPA-PSK, etc.

Prix : **132 €** Lien : **https://frama.link/-09NRvCd**

IMRIMANTE 3D ANET A8 : IDÉAL POUR COMMENCER L'IMPRESSION 3D !



L'impression 3D est le nouveau passe-temps des « makers ». Alors qu'il fallait craquer son PEL pour faire ses propres objets en 3D il y a encore 1 ou 2 ans, vous pouvez maintenant vous faire la main avec cette technique pour une somme très modique. L'appareil est compatible avec plusieurs types de filaments d'impression (ABS / PLA / nylon PVA / PP), il intègre une base en aluminium, une buse de diamètre de 0,4 mm et permet de faire des couches d'une épaisseur allant de 0,1 à 0,3 mm. Pas besoin d'être en ligne pour effectuer une impression puisqu'il est possible de commander le processus depuis une carte micro-SD. Le volume d'impression maximal est de 220 x 220 x 240 mm ce qui est impeccable pour commencer à faire des objets de bonne taille et vous faire la main. Le logiciel d'impression est compatible avec Windows, Linux et Mac et il fonctionne avec les principaux systèmes de fichiers d'impression : .code-G, OBJ et STL. Attention, pour ce prix, il faudra la monter soi-même, mais cela n'a rien d'insurmontable.

Prix : **129 €** Lien : **https://frama.link/GkhttkFN**

LE MINI PC BEELINK GEMINI X45

Les ordinateurs de type singleboard computer comme le Raspberry Pi, les cartes Odroid ou le Tinkerboard d'ASUS manquent un peu de puissance pour ce que vous désirez faire ? Il existe des PC comme ce Beelink Gemini X45 qui, en plus d'être faciles à transporter (115x102x43 mm pour 730 g), embarquent tout ce qu'il vous faut pour travailler ou jouer : processeur Intel Gemini Lake Celeron J4105 (4 cœurs 64 bits) cadencé entre 1,5GHz et 2,3GHz, processeur graphique Intel HD Graphics 600, 4 Go de RAM LPDDR4, WiFi bibande 2,4GHz + 5GHz et Ethernet 1000 Mbps. L'appareil dispose d'une connectique complète avec 4 ports USB 3.0, une prise jack et 2 ports HDMI. Les 64 ou 128 Go de stockage internes sont un peu justes, mais il est possible d'ajouter un disque dur SATA 2,5 pouces ou un SSD à l'intérieur.

Prix : **192 €** Lien : **https://frama.link/fC1QbEXd**

ADAPTATEUR WIFI ALFA AWUS036NHA AVEC MONITOR MODE

Lors de nos démonstrations sur l'interception de paquets ou le crack de clé WiFi, nous parlons souvent du monitor mode des antennes WiFi. C'est souvent compliqué de trouver du matériel de ce type, car la plupart sont illégales en France à cause de leur amplification trop forte ou juste parce que c'est rarement spécifié par les fabricants. Pas de surprise ici avec cet Alfa AWUS036NHA qui comporte un chip Atheros AR9271 et une antenne avec un gain de 5dBi (décibel isotrope). Si vous cherchez le partenaire de votre Kali Linux, nous l'avons trouvé pour vous !

Prix : **36 €** Lien : **https://frama.link/VUNN1faJ**

OBD II MINI GPS TRACKER, POUR SUIVRE VOTRE VOITURE À LA TRACE

Si vous nous lisez depuis longtemps vous connaissez les prises OBDII (ou OBD2)qui sont utilisées dans les automobiles pour brancher des sondes électroniques ou des ordinateurs et contrôler ou corriger tout un tas de choses. Cette prise est souvent bien cachée sous le tableau de bord ou au fond de la boîte à gants : il existe même des personnes qui n'ont même pas idée qu'une telle prise existe. C'est donc une idée de génie d'avoir inventé un tracker GPS à brancher sur cette prise ! Alimenté en énergie et discret (53x45x22 mm pour 130 g), l'appareil permet aussi de brancher une carte SIM pour pouvoir suivre en temps réel votre voiture via le réseau GPRS, mais on peut aussi l'utiliser sans. Il faudra alors l'extraire pour consulter les données grâce au port USB intégré

Prix : **24 €** Lien : **https://frama.link/N2qcJMjX**

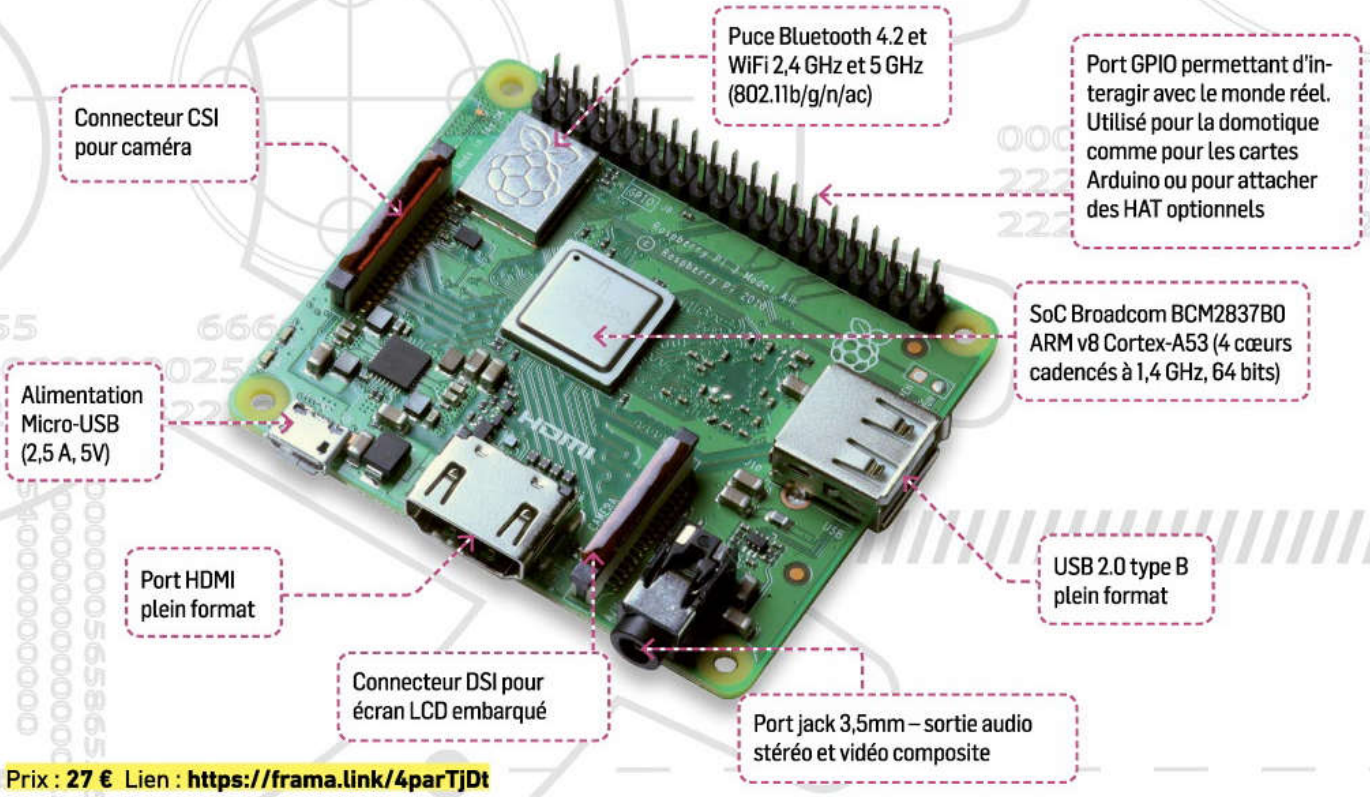
RASPBERRY PI 3A+, LA FRAMBOISE NOUVELLE EST ARRIVÉE !

Le Raspberry Pi est un nano-ordinateur à base de processeur ARM qui permet de faire tout un tas de projets pour une somme dérisoire : PC de bureau, robotique, domotique, media center, etc. La fondation en charge de la production de cette machine a récemment sorti une nouvelle version baptisée 3A+ : sorte de version « light » de la 3B+ sortie en mars 2018. Vu sa taille réduite, ce nouveau modèle 3A+ est moins fourni en RAM (512 Mo au lieu de 1 Go), embarque moins de ports USB (1 au lieu de 4) et un port HDMI «normal» (à l'inverse du micro-HDMI équipant le Zero). De même, le port GPIO est bien à 40 broches ce qui garantit la compatibilité avec les HAT des versions B. Par contre l'absence de port Ethernet RJ45 en frustrera certainement plus d'un même s'il est possible de «gruger» avec un adaptateur USB. Et bien sûr, sans RJ45, pas de PoE (Power over Ethernet) qui a été une des grosses évolutions, sinon la seule pour certains, du 3B+ sorti il y a 10 mois.

COMME ON PEUT LE VOIR SUR CETTE IMAGE, LE RASPBERRY PI 3A+ EST PLUS COMPACT QUE SON GRAND FRÈRE LE 3B+ SANS POUR AUTANT ÊTRE AUSSI COMPACT QUE LE ZERO.

Une Framboise intermédiaire à tout point de vue

Pour les ports CSI et DSI qui gèrent les modules caméra et écran d'appoint, il s'agit du même format que celui de ses grands frères et pas la nappe réduite des Zero. Cette version, un peu à cheval entre les «grands» et les Zero la destine aux systèmes embarqués, à la robotique et un peu à la domotique. La différence de poids et de prix la place également entre les deux puisque le 3B+ est affiché à 37 € et le Zero WH coûte 15 € tandis qu'il faudra débourser 27 € pour cette «nouveauté». Bien sûr pour les amoureux de la Framboise que nous sommes, il s'agit d'une petite déception, car, même si la 3A+ trouvera forcément son public, nous attendons toujours la version 4 de notre SBC (Single Board Computer) préférée.



Prix : **27 €** Lien : **https://frama.link/4parTjDt**

NOS GUIDES WINDOWS 100% PRATIQUES

POUR UN PC

+ Puissant
+ Beau
+ Pratique
+ Sûr

Mini Prix : 3,50 €

Chez votre marchand de journaux

SÉLECTION

WORLD HACK WEB

Lors de nos recherches ou au détour d'une discussion, nous faisons connaissance avec des sites ou des services intéressants. Au lieu de les garder pour nous, nous les partageons dorénavant sur cette page... N'hésitez pas à nous envoyer vos sites de prédilection à cette adresse : benbailleul@idpresse.com

PROTOCOLE D'ALERTE ZATAZ

> ALERTE VULNÉRABILITÉ

Crée par le journaliste Damien Bancal, le protocole d'alerte Zataz a pour but de prévenir de manière anonyme le propriétaire d'un site qui connaîtrait une faille, une vulnérabilité ou une fuite de données. Il s'agit d'une aide bénévole qui a déjà permis de prévenir de nombreux piratages.

Lien : **www.zataz.com/protocole-alerte-zataz**

UNDERNEWS

> ACTUALITÉS EN FRANÇAIS

Un très bon site d'information sur le hacking avec des actualités, des explications sur les méthodes utilisées par les pirates et encore beaucoup d'autres choses.

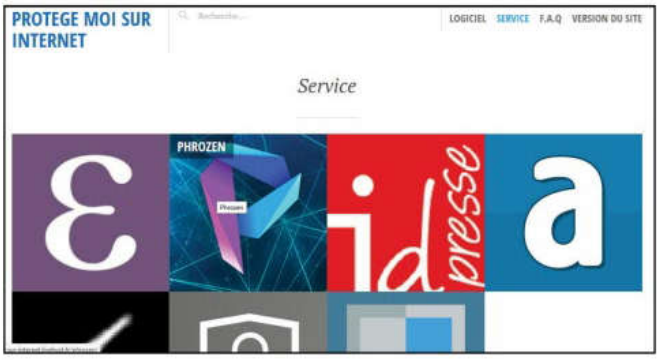
Lien : **www.undernews.fr**

PROTÈGE-MOI SUR INTERNET

> TROUSSE À OUTILS

Ce site créé par notre ami Yann vous donne tout un tas de pistes pour protéger votre vie privée sur Internet. Vous trouverez des logiciels, des services et des tutos dans différents domaines : VPN, messageries chiffrées, changement de DNS, sites incontournables, etc.

Lien : **http://protege-moi-sur-internet.livehost.fr**



CONTRÔLES TES DONNÉES > VIE PRIVÉE

Un site proposé par la Quadrature du Net proposant des solutions pour la réappropriation de ses données personnelles : pourquoi contrôler ses données, ce que les GAFAM savent sur vous, comment la loi peut changer la donne, etc. À lire absolument !

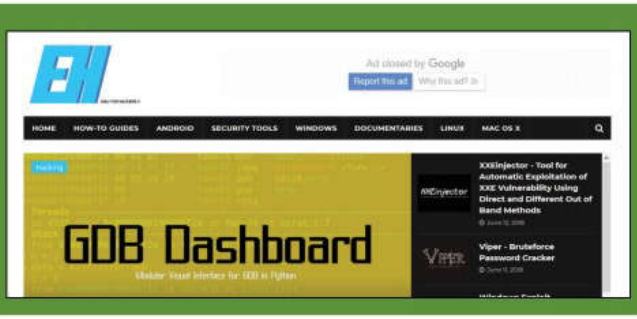
Lien : **https://controle-tes-donnees.net**

EFFECT HACKING

> ACTUALITÉS EN ANGLAIS

Un très bon site d'information sur le hacking avec des tutos, des documentaires, de l'actualité sur plusieurs plates-formes : Windows, Linux, MacOS et Android. Il est malheureusement réservé aux anglophones.

Lien : **www.effecthacking.com**



LE MAILING-LIST OFFICIELLE de

Pirate Informatique et des *Dossiers du Pirate*

INSCRIVEZ-VOUS GRATUITEMENT !

De nombreux lecteurs nous demandent chaque jour s'il est possible de s'abonner. La réponse est non et ce n'est malheureusement pas de notre faute. En effet, nos magazines respectent la loi, traitent d'informations liées au monde du hacking au sens premier, celui qui est synonyme d'innovation, de créativité et de liberté. Depuis les débuts de l'ère informatique, les hackers sont en première ligne pour faire avancer notre réflexion, nos standards et nos usages quotidiens.

Mais cela n'a pas empêché notre administration de référence, la «Commission paritaire des publications et agences de presse» (CPPAP) de refuser nos demandes d'inscription sur ses registres. En bref, l'administration considère que ce que nous écrivons n'intéresse personne et ne traite pas de sujets méritant débat et pédagogie auprès du grand public. Entre autres conséquences pour la vie de nos magazines : pas d'abonnements possibles, car nous ne pouvons pas bénéficier des tarifs presse de la Poste. Sans ce tarif spécial, nous serions obligés de faire payer les abonnés plus cher ! Le monde à l'envers...

La seule solution que nous avons trouvée est de proposer à nos lecteurs de s'abonner à une mailing-list pour les prévenir de la sortie de nos publications. Il s'agit juste d'un e-mail envoyé à tous ceux intéressés par nos magazines et qui ne veulent le rater sous aucun prétexte.

Pour en profiter, il suffit de s'abonner directement sur ce site

http://eepurl.com/FlOOD

(le L de «FlOOD» est en minuscule)

ou de scanner ce QR Code avec votre smartphone...

NOUVEAU !

La rédaction se dote d'un compte Twitter !

twitter.com/ben_IDPresse

Vous trouverez des news inédites, des liens exclusifs vers des articles au format PDF et nous vous tiendrons aussi au courant de la sortie des publications. Rejoignez-nous !

TROIS BONNES RAISONS DE S'INSCRIRE :

1. Soyez averti de la sortie de *Pirate Informatique* et des *Dossiers du Pirate* en kiosques. Ne ratez plus un numéro !
2. Vous ne recevrez qu'un seul e-mail par mois pour vous prévenir des dates de parutions et de l'avancement du magazine.
3. Votre adresse e-mail reste confidentielle et vous pouvez vous désabonner très facilement. Notre crédibilité est en jeu.

Votre marchand de journaux n'a pas *Pirate Informatique* ou *Les Dossiers du Pirate* ?

Si votre marchand de journaux n'a pas le magazine en kiosque, il suffit de lui demander (gentiment) de vous commander l'exemplaire auprès de son dépositaire. Pour cela, munissez-vous du numéro de codification L12730 pour *Pirate Informatique* ou L14376 pour *Les Dossiers du Pirate*.

Conformément à la loi «informatique et libertés» du 6 janvier 1978 modifiée, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent.

PIRATE INFORMATIQUE

N°40

Numéro spécial anniversaire

Nouvelle formule !

Merci à tous nos lecteurs.

IDPRESSE id presse

L 12730 - 40 - F: 4,90 € - RD

France METRO : 4,90 € - BEL/LUX : 6 € - DOM : 6,10 € - PORT.CONT. : 6 € - CAN : 7,99 $ cad – POL/S : 750 CFP – NCAL/A : 950 CFP - MAR : 50 mad - TUN : 9,8 tnd