100% PRATIQUE

[TÉLÉCHARGER] T411 : Et après ?

[ANONYMAT] Best-of 2017

[CAMÉRAS] Qui vous espionne ?

LES DOSSIERS DU

Pirate

3,50 € seulement

Anonymat Hacking Multimédia

0% PUBLICITÉ

101 HACKS & ASTUCES GRATUITS

EN - DE 5 MN CHRONO !

ÉTAPE PAR ÉTAPE

DOSSIER PRATIQUE

LE GUIDE MOTS DE PASSE !

Les solutions des PROS pour ZÉRO EURO !

- Vie privée, fichiers & Web 100% SÉCURISÉS
- Contrôler un PC À DISTANCE
- HACKS : Skype, Wi-Fi, Windows, eMails, ...
- ETC !

SOMMAIRE

EN PARTENARIAT AVEC LES CAHIERS DU HACKER PIRATE [INFORMATIQUE]

PROTECTION

ANONYMAT

CRACK & MOTS DE PASSE

HACKING

MULTIMÉDIA

LES DOSSIERS DU **Pirate**

n°13 - Oct – Déc 2017

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

Directeur de la publication :
David Côme
El Patrón : Benoît BAILLEUL
Los sicarios :
Yann Peyrot & Thomas Povéda
El Chapo : Sergueï Afanasiuk
Correctrice : Marie-Line Bailleul
Conseil éditorial : Irina Oleshko SPD

Imprimé en France par / Printed in France by :
Aubin Imprimeur
Chemin des Deux Croix
CS 70005
86240 Ligugé

Distribution : MLP
Dépôt légal : à parution
Commission paritaire : en cours
ISSN : 2267-6295

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

YGGTORRENT, UN SUCCESSEUR DE T411

Pour la petite histoire, Ygg est un des fils d'Odin. Il faudra aller saisir les serveurs au Valhalla !

Juste après la fermeture de T411.ai en juin dernier, le petit monde des téléchargeurs était en deuil. D'ailleurs nous tenions à remercier les autorités d'avoir fermé le site juste le jour du bouclage des *Dossiers du Pirate* n°12 alors que nous avions préparé un article dessus : super timing les mecs ! Heureusement nous ne somme pas restés longtemps orphelins puisque quelques semaines après est né **YggTorrent.com**, un tracker semi-privé qui a vite fait l'unanimité auprès des anciens de T411. Il faut dire que la philosophie est loin d'être celle, toxique, de son prédécesseur. Même si nous n'avions rien contre les utilisateurs et les seeders (salut lolo !), YggTorrent c'est pas de pub, des admins sympas et accessibles, des news sur les nouveautés ou heures de maintenance sur Twitter et des super cadeaux en termes de ratio. Les téléchargeurs ne s'y sont pas trompés, la communauté est de 300 000 personnes à l'heure où nous écrivons ces lignes. L'engouement est tel qu'il a presque éclipsé le retour de T411 ! Enfin presque, puisque les serveurs ont été saisis : il s'agit en fait d'un clone, **https://t411.si**. Même si le catalogue de contenu est encore en construction, ce nouveau T411 a, lui, complètement abandonné l'idée de ratio et propose un tracker public comme on en connaissait dans le milieu des années 2000. Deux trackers francophones à la place d'un seul ? On peut presque remercier la police suédoise...

QUAND TU TE FAIS «BAN» PAR POUTINE...

Vladimir Poutine a dernièrement signé une loi bannissant l'utilisation des VPN, des proxies anonymes et...de Tor. Selon les autorités, il ne s'agirait pas d'imposer des restrictions aux citoyens respectant la loi (bah non, bien sûr quelle idée !), mais d'empêcher l'accès à des contenus prohibés comme la propagande djihadiste. On ne sait pas encore comment la Russie va bloquer Tor car c'est en pratique très difficile. Même en faisant la chasse aux «noeuds» (ce que fait la Chine depuis des années), Tor dispose de contre-mesures comme le Protocole Obfuscation ou les bridges qui permettent de brouiller les pistes. Réponse le 1er novembre prochain à la date de mise en application de la loi...

MESSAGE DE HAINE INCOMPATIBLE AVEC LA LIBERTÉ D'EXPRESSION. À TOR OU À RAISON ?

Le Daily Stormer, un site de la «droite radicale» américaine (doux euphémisme) a été chassé par tous les hébergeurs américains malgré le premier amendement de la constitution de Trump Land. C'est donc tout naturellement qu'il s'est tourné vers le darknet et les hidden services de Tor pour naviguer sous les radars. Même si nous ne partageons rien avec ce ramassis de redneck racistes, les hidden services (ou Tor sites) sont exactement faits pour cela : avoir le pouvoir de s'exprimer là où on vous en empêche. Le truc amusant c'est que Tor (que nous défendons bec et ongles) a trouvé le moyen de communiquer sur ce dossier suscitant l'indignation de la Toile.

On a retrouvé le site sur le Darknet. Il s'appelle maintenant Punished Stormer. Ils sont bêtes et méchants, mais quand ils se moquent de la facture de maquillage de notre président c'est rigolo quand même...

DEUX POIDS, DEUX MESURES

On peut en effet se demander pourquoi Tor a pris la parole sur le problème du racisme alors qu'ils n'ont jamais rien dit sur les trafics de drogue, le djihadisme ou les images pédopornographiques. Il faut tout de même préciser que même si c'est la première fois que Tor fait un commentaire sur l'utilisation qui est faite de son service et qu'il a pris position contre les suprémacistes blancs, les responsables ne souhaitent pas bloquer ou censurer qui que ce soit. En effet, si un site était bloqué, le réseau s'effondrerait de lui-même. Personne ne voudrait prendre le risque d'être mis au banc du réseau. Pas sûr non plus que Tor ait les moyens de la censure...

LE GILET JAUNE : ce vêtement au pouvoir surnaturel

David Allegri et son ami Sean ont tenté une expérience amusante qui se révèle être aussi un peu inquiétante... Équipés de vestes fluo de chantier, ils ont réussi à entrer gratuitement dans des lieux pourtant payants ou surveillés : un cinéma, un zoo et même un concert de Coldplay. Tout cela dans une ville de Melbourne pourtant aussi vigilante que les autres en ce qui concerne le terrorisme. En effet, personne ne vient demander des comptes à deux types avec des gilets jaunes et des talkies-walkies tant qu'ils ont l'air sûrs de l'endroit où ils vont. Les gens font naturellement confiance à l'uniforme et ce gilet jaune les incite naturellement à croire que ceux qui les portent sont «accrédités». Il s'agit d'un cas pratique de social engineering cher à Kevin Mitnick. Pas sûr cependant qu'un gilet jaune l'aurait sauvé de la prison...

ATTENTION À VOS SÉSAMES !

En 2003, Bill Burr (un ancien responsable un National Institute of Standards and Technology) avait suggéré de mettre au point des mots de passe complexes en utilisant des majuscules, des chiffres et des caractères spéciaux (&, £ ou @, par exemple). C'est aussi ce que nous conseillons et même si nous en parlons souvent dans *Les Dossiers du Pirate* ou *Pirate Informatique*, nous allons revenir dessus puisque c'est d'actualité. Car Bill regrette en effet d'avoir donné ce conseil, mal suivi par les utilisateurs. Quand ce dernier parlait d'utiliser plusieurs types de caractères dans un sésame il parlait de quelque chose de ce genre : **Rg56) l=Y14;#uJ8***. À l'inverse, **kEbAbLoVeR123**, **Gaulois69** ou **Kevin78Tuning** ne sont pas de bons mots de passe et laissent penser à une certaine solidité alors qu'il n'en est rien. Ces sésames sont sans doute présents dans certains dictionnaires accessibles sur le Net et le fait d'alterner les majuscules et les minuscules (tout comme d'ajouter 2 ou 3 chiffres) est très facilement contournable par les logiciels spécialisés dans le crack de mots de passe (Hydra, John The Ripper, etc.) Pour éviter d'oublier ses mots de passe trop compliqués, il y a plusieurs techniques de mémorisation, mais aussi les portefeuilles de mots de passe (voir notre article page 58)...

PROTECTION

AUTHENTIFIEZ-VOUS DE MANIÈRE SÉCURISÉE SUR FIREFOX

Inconditionnel de Firefox, que ce soit sur PC ou sur mobile, vous aimeriez automatiser les connexions à vos sites préférés ou profiter de vos mots de passe d'un appareil à un autre ? Voyons comment gagner du temps tout en se protégeant des pirates.

La mémorisation des mots de passe de Firefox est utile, tant que vous utilisez un mot de passe Windows pour blinder votre session, et surtout le mot de passe principal du navigateur pour protéger tous les autres. L'extension Secure Login vous simplifie encore plus la vie, en améliorant les fonctionnalités du gestionnaire de mots de passe de Firefox. Vous pourrez ainsi vous authentifier sur un site en un clic, même si vous disposez de plusieurs comptes. Secure Login fait aussi office de protection contre le phishing puisque les identifiants ne se chargeront pas s'il s'agit d'un site frauduleux.

IMPORT/EXPORT

Pour exporter vos duos identifiants/mots de passe, vous avez aussi plusieurs solutions. La première consiste à utiliser l'extension Password Exporter qui va chiffrer et exporter vos sésames dans un fichier XML pour pouvoir la transférer sur un autre PC ou les garder bien au chaud dans une clé USB en cas de panne. Mais vous pouvez aussi compter sur l'option de synchronisation de Firefox puisque cette dernière fonctionne très bien sur mobile ou sur PC.

STOCKEZ VOS MOTS DE PASSE EN LOCAL !

INFOS **[SECURE LOGIN]** Où le trouver ? [**https://goo.gl/xEVnqc**]
[PASSWORD EXPORTER] Où le trouver ? [**https://goo.gl/xEVnqc**]

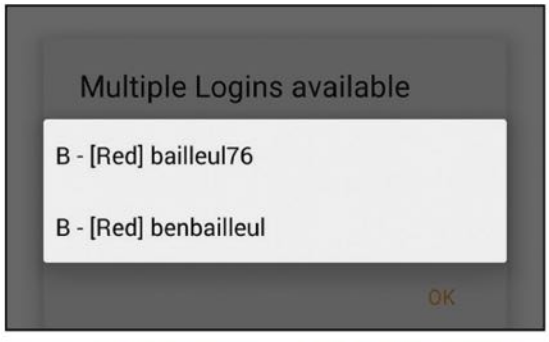
TUTO

01 › S'AUTHENTIFIER EN UN CLIC

Après installation de Secure Login, un nouveau bouton devrait apparaître dans la barre d'outils en haut à droite. Faites un clic droit sur ce dernier et choisissez **Options**. Si Firefox connaît les identifiants, vous verrez les champs des formulaires entourés d'orange par exemple. Lancez un service Internet sur lequel vous êtes enregistré. Faites un clic droit sur le bouton, et voilà, vous êtes loggé !

02 › EXPORTER OU SYNCHRONISER

Pour exporter vos mots de passe, vous pouvez installer Password Exporter et aller dans la partie **Sécurité** des options pour faire **Importer/ Exporter les mots de passe**. Si vous utilisez Firefox sur mobile (iOS et Android), vous pouvez utiliser la méthode de synchronisation. Sur le PC, cliquez sur les trois barres horizontales en haut à droite et faites **Se connecter à Sync**. Créez un compte et choisissez les éléments à synchroniser.



03 › TOUS VOS FIREFOX À L'UNISSON

Validez votre inscription depuis votre client de messagerie puis ouvrez la version Firefox sur votre mobile. Dans l'onglet Historique, faites **Démarrer** et entrez les identifiants de connexion que vous venez d'entrer. Tous vos identifiants et mots de passe sont transférés sur votre nouvel appareil. Sur Android, allez dans **Outils** > **Identifiants** pour les voir, domaine par domaine. Gérez les appareils connectés dans la partie **Sync** des **Options**.

04 › LOG ME IN = SECURE LOGIN

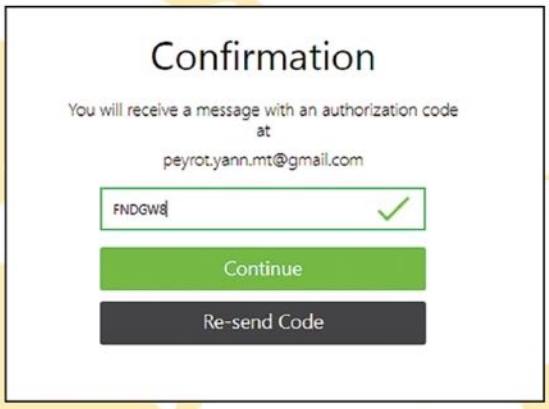
Maintenant que vos différents Firefox sont synchronisés, sachez que vous pouvez utiliser l'extension **Log Me In** pour mobile. Cette dernière agira exactement de la même manière que **Secure Login** (qui n'existe pas en version mobile pour le moment). Lorsque vous êtes sur un site connu et sur lequel vous avez un compte, une petite icône en forme apparaît. Cliquez dessus pour vous logger automatiquement, même si vous avez plusieurs compte pour le même site.

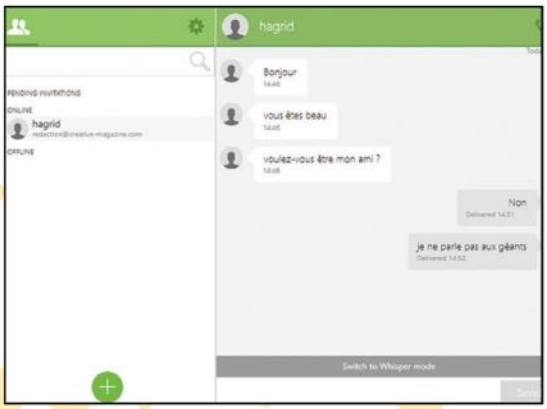
DISCUTEZ EN TOUTE DISCRÉTION

Ce service de messagerie gratuit chiffre tous vos échanges, qu'ils soient à l'oral ou à l'écrit. Créez un compte en suivant ce pas-à-pas.

INFOS [BLEEP BY BITTORRENT]
Où le trouver ? [**www.bleep.pm**] Difficulté :

TUTO





01 › SE CONNECTER

Suivez notre lien pour cliquer sur **Get Bleep**. Faites un double-clic sur le fichier **.exe** qui vient d'être téléchargé. Choisissez-vous un nom avant de créer le compte associé (**Create an Account**). Renseignez une adresse mail ou un numéro de téléphone, ils seront utilisés par les autres utilisateurs pour vous trouver sur Bleep. Validez en renseignant le code reçu par mail ou SMS.

02 › ÉCHANGER

Ajoutez des contacts avec le **+** et renseignez l'adresse des personnes à ajouter. Débutez l'échange en cliquant sur le nom de votre contact puis écrivez dans le champ **Send a message**. Pour l'envoyer pressez **Entrée**. **Switch to Whisper** mode sert à envoyer des messages qui s'autodétruisent au bout de 25 secondes. Il est possible d'envoyer des photos, mais uniquement depuis la version mobile de Bleep.

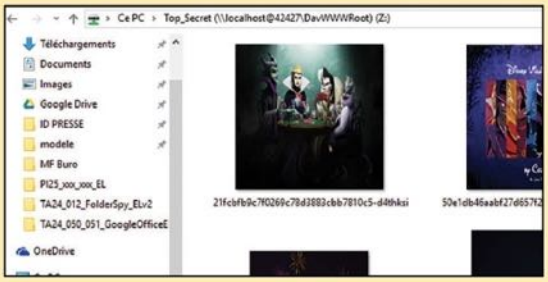
CRYPTEZ VOS FICHIERS STOCKÉS DANS LE CLOUD

INFOS [CRYPTOMATOR]
Où le trouver ? [https://cryptomator.org] Difficulté : ☠☠☠

TUTO

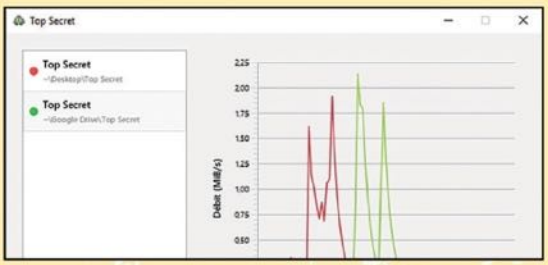
01› CRÉER L'ESPACE

Lancez le logiciel et cliquez sur le **+ créer un nouveau coffre** en bas à gauche. Sélectionnez le dossier de votre service de Cloud, Google Drive dans notre exemple, choisissez un nom pour votre coffre-fort et faites **Enregistrer**. Définissez un mot de passe sécurisé pour ne pas compromettre vos données puis cliquez sur **Créer le coffre.**



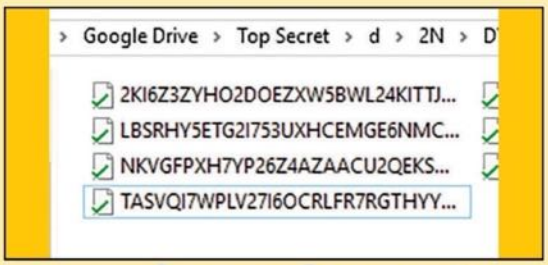
02› Y STOCKER SES FICHIERS

Votre coffre est verrouillé d'office. Entrez le mot de passe précédemment renseigné et cliquez sur **Déverrouiller le coffre**. Cryptomator ouvre automatiquement le dossier virtuel dans lequel vous pouvez placer tous vos fichiers.



03› VERROUILLER L'ESPACE

Le logiciel affiche également un graphique de débit de cryptage et décryptage. Pour surveiller qu'il fait bien son travail. Une fois que vos fichiers sont bien dans votre coffre, cliquez **sur Verrouiller le coffre**. Vous pouvez voir dans le poste de travail que le lecteur virtuel a disparu.



04› VÉRIFIER LA SÉCURITÉ

Le coffre verrouillé, personne ne peut y accéder. Allez dans le dossier de votre Cloud sur votre PC, il y a bien votre dossier, mais les fichiers sont illisibles. Idem sur le site du Cloud, si quelqu'un télécharge les fichiers, il ne pourra pas les lire. Vos fichiers sont définitivement à l'abri tant que le coffre est verrouillé. Si vous oubliez le mot de passe, vos fichiers sont définitivement perdus.

PROTÉGEZ VOTRE COMPTE GOOGLE

INFOS [GOOGLE]
Où le trouver ? [https://goo.gl/wpmOX0] Difficulté :

TUTO

01› SE CONNECTER

Suivez le lien que nous vous proposons puis identifiez-vous avec le compte Google pour lequel vous voulez activer la validation en deux étapes. Une fois connecté, cette dernière vous est proposée. Cliquez sur le bouton **Démarrer**. Le service vous demande d'abord de confirmer vos identifiants : ressaisissez-les.

02› INDIQUER SON NUMÉRO

Sur la page suivante, indiquez le numéro du téléphone (à côté du petit drapeau français) sur lequel sera envoyé le code unique, à chaque tentative de connexion à votre compte Google. Deux possibilités, recevoir un **SMS** où le code est écrit ou décrocher un **Appel téléphonique** où un robot vous le dictera. Faites votre choix et cliquez sur **Suivant**.

03› TESTER LA PROCÉDURE

La validation en deux étapes est ensuite testée. Vous recevez le code par SMS (ou par appel vocal). Entrez-le dans le champ **Saisissez le code** avant de valider avec **Suivant**. Si vous ne l'avez pas reçu, faites **Réenvoyer**. Le service vous demande de vous connecter, toujours avec votre adresse Gmail et le mot de passe associé.

04› ACTIVER LE CODE DE SECOURS

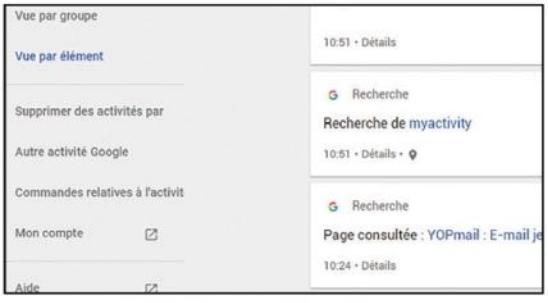
Vous n'avez plus qu'à cliquer sur **Valider** pour rendre effective la validation en deux étapes. Mieux vaut avoir un code de secours pour conserver l'accès à votre compte si vous égarez votre téléphone. Depuis la page **https://goo.gl/ulcvpw**, cliquez sur **Configurer > Codes de secours**. Téléchargez ou imprimez ces codes.

AJUSTEZ LES PARAMÈTRES DE CONFIDENTIALITÉ

INFOS [MON ACTIVITÉ]

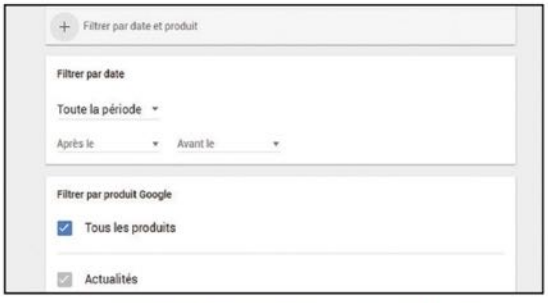
Où le trouver ? [https://goo.gl/CaJH5K] Difficulté : ☠☠☠

TUTO



01› VÉRIFIER YOUTUBE

Depuis la section **Mon compte** https://goo.gl/PmcrqS, allez dans **Vérification des paramètres de confidentialité**. Cochez/Décochez toutes les cases concernant **YouTube** (**Garder privées les vidéos que j'aime**, **Garder privées toutes mes playlists enregistrées**...). Cliquez sur **Suivant** lorsque vous avez fait le ménage dans les infos que partage YouTube.

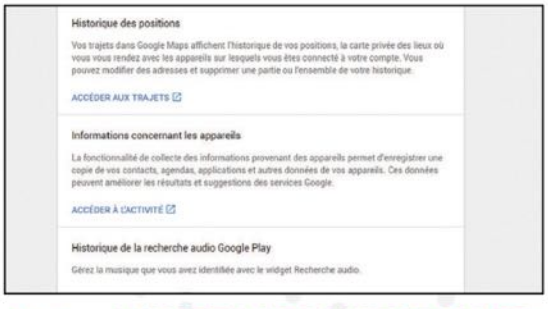


02› PROTÉGER SON NUMÉRO

Si vous avez renseigné votre numéro de téléphone, n'importe qui le connaissant peut s'en servir pour vous retrouver sur les services Google, et éventuellement découvrir votre nom, vos photos... Pour éviter cela, décochez les deux cases proposées. Cliquez sur **Modifier vos numéros de téléphone** pour supprimer votre numéro ou le mettre à jour.

03› CONTRÔLER GOOGLE +

Décochez la case **YouTube/vidéos** pour que les vidéos postées sur YouTube n'apparaissent pas sur votre profil Google+. Faites de même pour les **Photos**, les **Avis** et les **+1**. Vous rédigez des recommandations ? Cliquez sur **Modifier le paramètre relatif aux recommandations...** pour décocher **En fonction de mon activité Google peut afficher mon nom et ma photo...**



04› AJUSTER LES HISTORIQUES

Dans la section **Personnaliser votre expérience utilisateur Google**, vous avez accès à l'historique de toutes vos activités. Vous pouvez les désactiver en cliquant sur la flèche à l'extrémité de chaque ligne. Attention, cela va seulement couper l'enregistrement. Pour supprimer les éléments déjà enregistrés, cliquez sur le bouton **Gérer l'historique.**

ÉVITEZ LES PIÈGES DE FACEBOOK

INFOS [FACEBOOK]
Où le trouver ? [www.facebook.com] Difficulté :

TUTO

01 › LE CLONAGE DE COMPTE

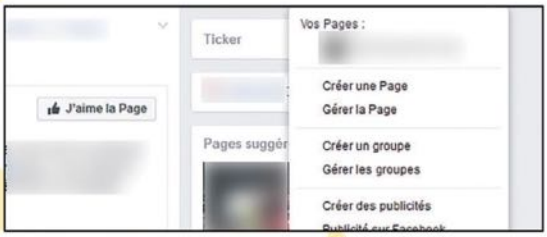
Choisissez bien vos amis et supprimez ceux que vous avez ajoutés uniquement parce que X ou Y les connaît. Ces comptes ont pu être piratés. Si vous êtes victime, postez un avertissement sur votre profil et envoyez des SMS à vos amis les plus proches et les moins sensibles au problème de sécurité. Le but est bien sûr d'éviter que vos amis ne quittent votre profil pour devenir amis avec le brigand. Demandez-leur de bloquer les invitations de cette personne et de signaler le compte comme étant un faux en suivant ce lien : **https://goo.gl/6UHCMT**.

02 › ACTIVER LA DOUBLE AUTHENTIFICATION

Il s'agit de recevoir un code par SMS ou directement sur l'application mobile pour valider les changements de mots de passe et autres manipulations délicates. Sur Facebook, cliquez sur la petite flèche vers le bas en haut à droite puis allez dans **Paramètres** > **Sécurité et connexion** > **Modifier** à droite d'**Utiliser l'authentification à deux facteurs** > **Configurer** à droite d'**Authentification à deux facteurs désactivée**. Plusieurs choix s'offrent à vous. Suivez la procédure, qui nécessitera de manipuler le smartphone également.

03 › CONFIDENTIALITÉ

Dans **Paramètres** > **Confidentialité** (ou depuis votre assistant de confidentialité), regardez de plus près vos réglages. Votre liste d'amis ne doit pas être publique puisqu'un pirate va l'utiliser pour les contacter après vous avoir bloqué. Dressez aussi une liste d'**Amis proches** et faites en sorte que seuls ces derniers puissent voir vos publications (vous pourrez donc accepter un nouvel ami sans craindre qu'il soit un pirate). Suivez ce lien pour savoir comment faire : **https://goo.gl/sN5aeT**.



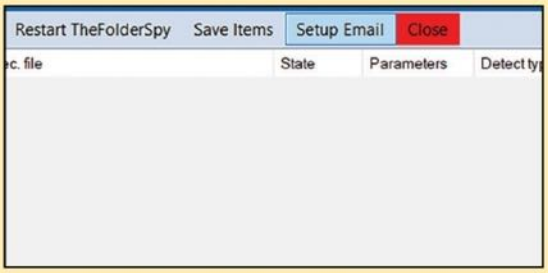
04 › ATTENTION AUX FAUX MAILS

Vos identifiants (couple nom d'utilisateur/mot de passe) sont précieux. Facebook ne vous demandera jamais de les saisir depuis un formulaire par e-mail. Le seul cas où vous devrez entrer votre sésame, c'est lors d'une nouvelle connexion ou lors d'un changement de mot de passe que vous aurez demandé. Choisissez un mot de passe solide et changez-le tous les 6 mois. N'oubliez pas non plus de vous déconnecter si vous êtes sur un ordinateur qui n'est pas le vôtre.

SURVEILLEZ LES CHANGEMENTS DANS VOS DOSSIERS

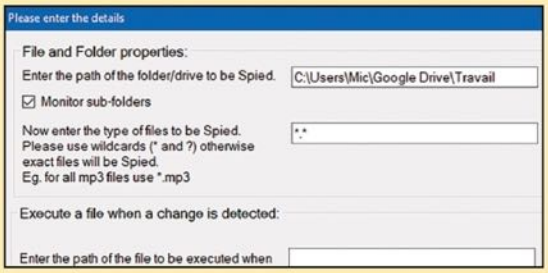
INFOS [THE FOLDER SPY]
Où le trouver ? [**https://goo.gl/Xz5LFy**] Difficulté :

TUTO



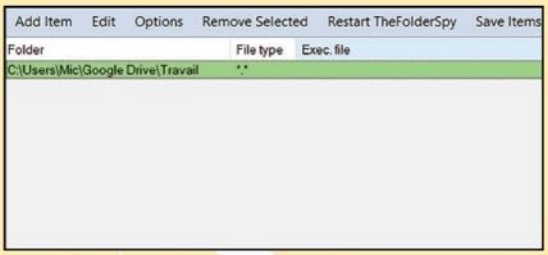
01› LANCER LE SOFT

Décompressez l'archive pour obtenir le fichier exécutable du logiciel. Il s'agit d'un programme portable, qui ne nécessite aucune installation. Via l'onglet **Setup Email**, vous renseignez la boîte mail qui recevra un avertissement en cas de modifications effectuées dans l'un de vos dossiers.



02› POINTER VERS LES DOSSIERS

Pour chaque dossier à surveiller, cliquez sur **Add Item**. Avec les trois petits points (...) dans **File and Folder properties**, vous définissez le chemin du dossier à surveiller. Pour être alerté des modifications (en plus de ce que vous avez fait en étape 1), cochez la case Send email if change detected, sur la droite de la fenêtre.



03› ACTIVER LA SURVEILLANCE

Une fois les dossiers sélectionnés via le programme, ces derniers sont surlignés en vert, cela signifie qu'ils sont placés sous surveillance. Vous mettez en pause la surveillance en double-cliquant sur le dossier concerné. Pour fermer la fenêtre des dossiers, cliquez sur Close puis faites Yes pour sauvegarder les réglages.

04› ANALYSER LES CHANGEMENTS

Cliquez sur **Run in Background** pour faire disparaître la fenêtre du logiciel. Une notification apparaîtra dès qu'un changement sur un dossier est détecté. Si vous revenez sur votre PC après un petit moment, cliquez sur l'icône du logiciel, accessible depuis le volet système. Les changements opérés s'afficheront.

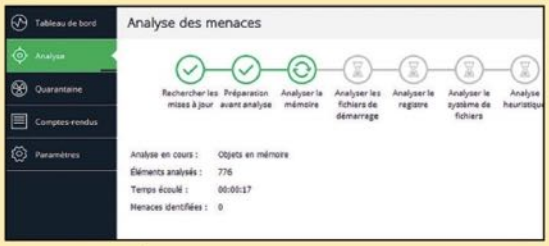
REPÉREZ ET ÉRADIQUEZ LES FAUX ANTIVIRUS

INFOS [MALWAREBYTES]
Où le trouver ? [https://fr.malwarebytes.com] Difficulté :

TUTO

01 › ANALYSER

Malwarebytes est un antivirus qui, dans sa version gratuite (celle qui nous intéresse), n'offre pas de protection en tâche de fond. Vous lancez vous-même l'analyse avec **Analyser maintenant**. Auparavant, n'oubliez pas d'**Installer les mises à jour d'application** depuis les **Paramètres** pour augmenter les chances de détection de logiciels suspects.

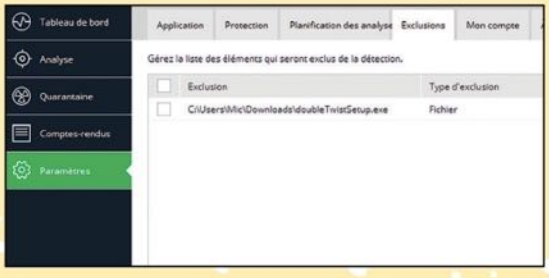


02 › DÉTECTER

Outre les éventuels rogues, Malwarebytes tente de déceler d'éventuelles anomalies dans le Registre, les tâches planifiées, certains fichiers système... La durée de l'analyse dépend évidemment de la quantité de données stockées sur votre PC. Patientez le temps nécessaire.

03 › GÉRER LA QUARANTAINE

Une fois le scan terminé, Malwarebytes place les menaces en quarantaine. Pour accéder à cette zone, cliquez sur l'onglet **Quarantaine**. Choisissez de **Supprimer tout** pour enlever définitivement toutes menaces. En revanche, si un logiciel placé ici est un faux positif (ce qui est rare), faites le choix de le **Restaurer**.



04 › AJOUTER DES EXCEPTIONS

Si vous savez qu'un de vos dossiers ne contient aucune menace (votre bibliothèque musicale), demandez au logiciel de ne pas le scanner. Allez dans l'onglet **Paramètres** > **Exclusion**, puis choisissez d'**Ajouter une exclusion**. Répétez l'opération pour l'ensemble des dossiers sans risque.

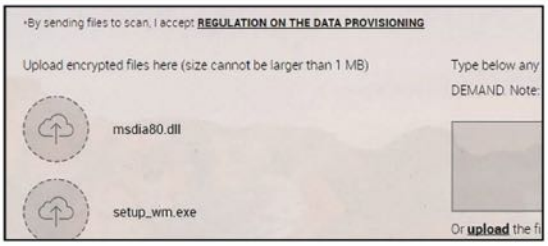
NE VOUS FAITES PLUS AVOIR PAR LES RANSOMWARES

NO MORE RANSOM!

INFOS [NO MORE RANSOM]

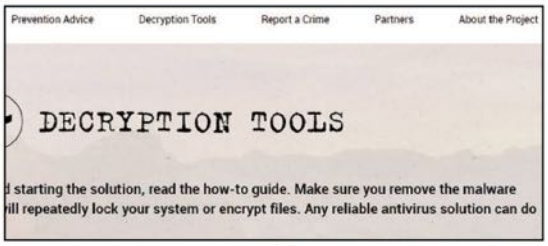
Où le trouver ? [**www.nomoreransom.org**] Difficulté : ☠☠☠

TUTO



01 › ANALYSER

Si vous avez été contaminé par un ransomware et que vous avez gardé vos fichiers, téléversons-les sur ce site. Il peut s'agir d'un fichier chiffré contre votre gré ou les « notices » qui vous expliquent comment payer les malfrats (qui se trouvent souvent en vrac dans **C:**). Cliquez sur **Yes** puis **Choose first file from PC** et éventuellement sur **Choose second file from PC** pour en ajouter un deuxième.



02 › VOIR LES RÉSULTATS

Dans notre cas, pas de chance, il s'agit de CryptoWall 3.0 un ransomware qui est pour l'instant hermétique à tous les outils de déchiffrement. Le site vous propose de faire une sauvegarde de vos fichiers inutilisables en attendant une éventuelle solution dans le futur. Explorez les solutions en allant dans l'onglet **Decryption Tools**.

03 › TROUVER UNE SOLUTION

Si vous avez de la chance, le site vous dirigera vers les logiciels permettant de déchiffrer quantité de ransomwares et leurs variantes. Pour chaque cas, il suffit d'installer le programme et de suivre les instructions pour récupérer vos précieux fichiers.

04 › SIGNALER

Si ce n'est pas déjà fait, vous pouvez aussi vous signaler à la police. Suivez le lien **Report a crime** après votre analyse puis, depuis le site d'Europol, choisissez **France**. Vous pourrez déposer une pré-plainte ou signaler le problème à la plate-forme Pharos qui gère les cybercrimes.

GARDEZ VOTRE HISTORIQUE EN NAVIGATION PRIVÉE

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 : ☠☠☠

TUTO

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.

TRANSMETTEZ DES DOCUMENTS SENSIBLES SANS SOUCI

INFOS [SECURESAFE]
Où le trouver ? [www.securesafe.com/fr] Difficulté :

TUTO

01› STOCKER

Créez un compte sur SecureSafe. Francisez l'interface via l'icône **Mon Compte**. Stockez tous documents que vous pourrez organiser par dossier via la fonction **Upload**. Rendez-vous dans **Héritage des Données**. Cliquez sur **Paramètres** puis sur **Ajouter un bénéficiaire.** Remplissez les champs, plus un petit mot que vos bénéficiaires recevront en même temps que le code d'accès.

02› ORGANISER LA SUCCESSION

SecureSafe vous permet de choisir le sort de chaque document. Dans la version gratuite, vous n'avez droit qu'à un seul bénéficiaire. Sélectionnez le document que vous souhaitez léguer et cliquez sur **Plus**. Cliquez ensuite sur **Affecter des bénéficiaires** et cochez votre héritier. Les documents sans bénéficiaire seront supprimés en toute sécurité s'il vous arrive quelque chose.

03› TRANSMETTRE LE CODE D'ACTIVATION

Rendez-vous dans **Héritage des Données** puis dans **Setup Wizard**. SecureSafe vous indique si vous avez rempli la procédure pour activer la transmission des données. Vous devrez imprimer le code d'activation qui devra être transmis à vos bénéficiaires via votre testament ou en mains propres au préalable.

04› DÉMARRER L'HÉRITAGE DES DONNÉES

Il vous est arrivé quelque chose et vos bénéficiaires veulent accéder à vos données. Ils doivent entrer le code d'activation sur **https://goo.gl/6oc92h**. Pour s'assurer qu'il peut déclencher la transmission de données, SecureSafe essaiera de vous contacter pendant 7 jours. Si vous ne vous manifestez pas, le service ouvrira le compte à vos bénéficiaires.

ÉVITEZ LES CONTAMINATIONS

INFOS [WINJA]
Où le trouver ? [**www.phrozen.io/freeware**] Difficulté :

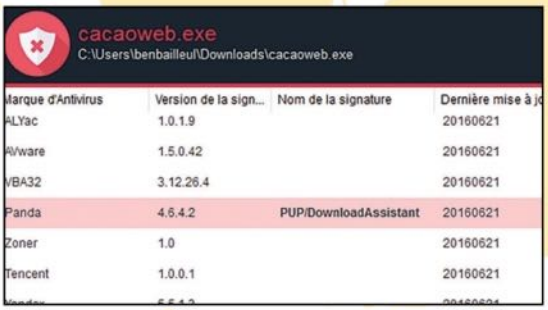
TUTO

01› APPRIVOISER L'INTERFACE

Après avoir choisi la langue de l'interface, celle-ci va s'afficher avec ses différents boutons. Utilisez les boutons de couleurs. Vert pour ouvrir un fichier déjà présent sur votre PC. Jaune pour scanner un fichier en ligne. Bleu pour les processus actifs et en rouge pour les outils complémentaires. Ces derniers doivent être lancés en mode administrateur.

02› TESTER

Pour tester, nous avons lancé un scan du controversé cacaoweb.exe. Le verdict est sans appel : infecté. En faisant un clic droit sur ce dernier dans **Résultat des Scans** il est possible d'ouvrir le rapport de Winja ou d'aller directement sur Virus Total. Vous pouvez aussi demander un nouveau scan ou voir les propriétés du fichier.



03› CONSULTER LES RÉSULTATS

En fait, un seul des antivirus de l'API Virus Total trouve que ce programme de stream contient un PUP (Potentially Unwanted Program) : pas un virus donc, mais un «download assistant», un petit adware. Pas dangereux, mais sans doute pénible à désinstaller. Il se peut aussi qu'il s'agisse d'un programme «à décocher» lors de l'installation de cacaoweb. À vous de voir !

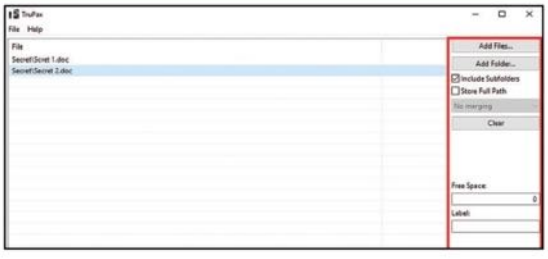
04› SCANNER AVANT DE TÉLÉCHARGER

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 **Télécharger et Scanner** puis copiez ce lien. Attendez le verdict. N'hésitez pas à utiliser les autres de Winja pour faire le ménage.

CHIFFREZ VOS FICHIERS SENSIBLES

INFOS [TRUPAX]
Où le trouver ? [https://coderslagoon.com] Difficulté : ☠☠☠

TUTO

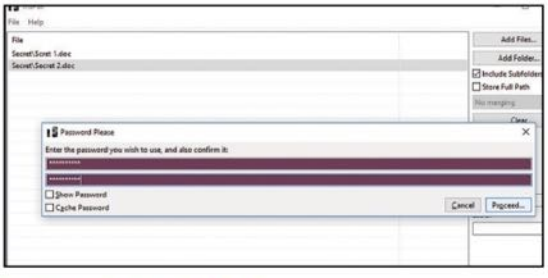


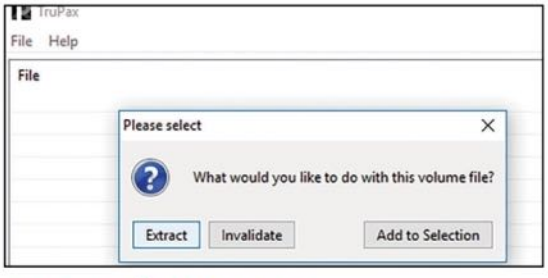
01 › CRÉER LE DOSSIER

Téléchargez TruPax, décompressez le dossier, et lancez **install**. Double-cliquez sur le raccourci créé sur le bureau et choisissez la langue anglaise (**English**). Faites un glisser-déposer des éléments à chiffrer dans la fenêtre principale ou cliquez sur **Add Files** (fichiers) ou **Add Folder** (dossier). Intégrez les sous-répertoires en cochant **Include Subfolders**.

02 › CONSULTER LES OPTIONS

No Merging signifie que les éléments ne seront pas combinés lors du chiffrement (dans le cas où les noms des dossiers seraient les mêmes par exemple). **Free Space** permet de garder un peu de place pour ajouter des fichiers ou pour des mises à jour. Cochez **Wipe Afterwards** pour effacer les éléments qui auront été chiffrés dans leur répertoire d'origine.





03 › CHIFFRER

Lorsque tout est près, cliquez sur **Make Volume**. Choisissez un dossier, tapez un nom pour le conteneur crypté et faites **Enregistrer**. Spécifiez un mot de passe et validez avec **Proceed**. Cocher **Cache Password** l'enregistre sur le PC pour ne pas avoir à le retaper (attention que personne d'autre n'y accède) et surtout gardez le mot de passe en cas de panne.

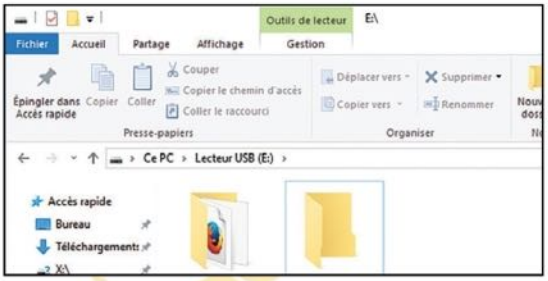
04 › DÉCHIFFRER

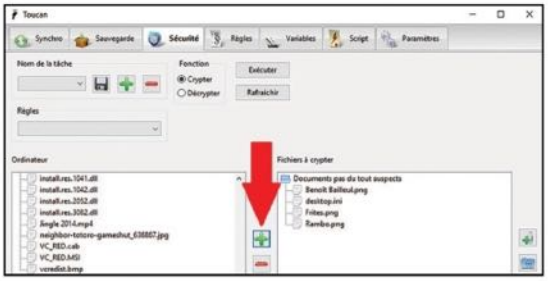
Vous obtenez un fichier en **.tc**. Pour le décrypter, cliquez sur **Clear** dans TruPax et glissez-déposez le fichier **.tc** dans la fenêtre. **Extract** extrait le tout, tandis que **Invalidate** détruit la clé, ce qui empêche quiconque (même vous) d'accéder au contenu. Utile en cas d'oubli du mot de passe. Faites **Extract**, spécifiez l'emplacement, tapez votre mot de passe et validez avec **Proceed**.

PROTÉGEZ LE CONTENU DE VOS CLÉS USB

INFOS [TOUCAN]
Où le trouver ? [https://goo.gl/XPA6Cy] Difficulté :

TUTO



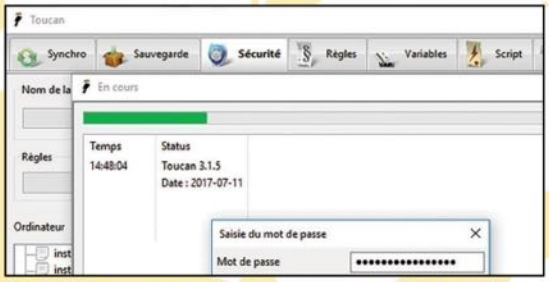


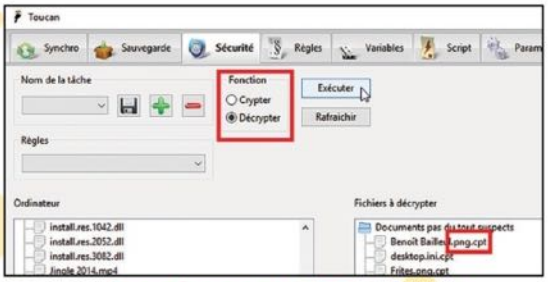
01› PRÉPARER LA CLÉ

Téléchargez Toucan via le lien fourni et installez le logiciel. Après l'installation, copiez le dossier **Toucan** créé directement à la racine de votre clé USB. Placez ensuite tous les fichiers à protéger dans un seul et même dossier, à part, que vous placerez également sur la clé (où vous voulez). Cette opération est utile pour tout chiffrer en même temps.

02› SÉLECTIONNER LE DOSSIER

Ouvrez le dossier **Toucan** présent sur la clé pour lancer le logiciel via le fichier .exe. Rendez-vous dans l'onglet **Sécurité**. Sélectionnez le dossier à crypter dans la colonne de gauche (cliquez sur Rafraîchir si vous ne le voyez pas) et cliquez sur le bouton « + ». Il passe dans la colonne de droite.





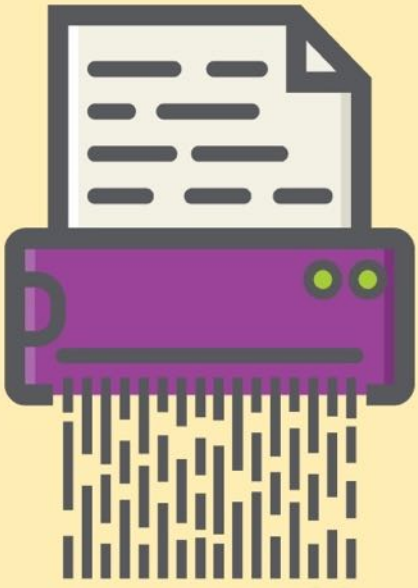
03› CRYPTER LES DONNÉES

En haut de la fenêtre, veillez à ce que la mention **Crypter** (sous **Fonction**) soit cochée. Cliquez sur **Exécuter**. C'est là qu'il faudra définir un **Mot de passe** solide, comprenant comme d'habitude (si possible) des caractères spéciaux, des chiffres, des majuscules et minuscules. Confirmez et validez par **OK**. Attention, si vous oubliez ce mot de passe, Toucan ne vous proposera pas de le récupérer.

04› ACCÉDER AU CONTENU

Les fichiers cryptés sont désormais impossibles à ouvrir (extension de fichiers **.cpt**). Pour les déchiffrer, lancez Toucan, allez dans l'onglet **Sécurité**, et répétez les étapes 2 et 3, mais cette fois-ci, cochez **Décrypter**, sous **Fonction**, avant de cliquer sur **Exécuter**. Tapez le mot de passe, puis cliquez sur **OK** pour rendre vos fichiers lisibles.

CHIFFREZ VOS MESSAGES

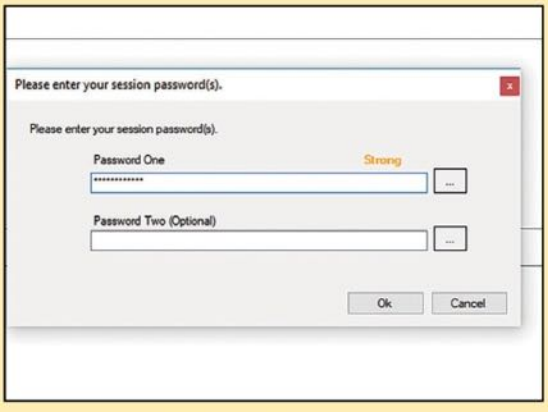


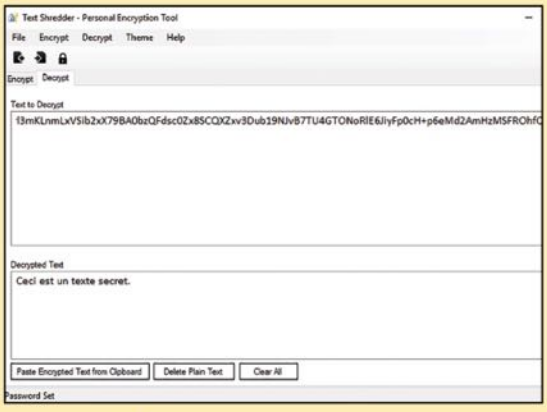
Le programme libre TextShredder transforme les textes que vous lui soumettez en une suite alphanumérique que seul le détenteur du mot de passe peut déchiffrer.

INFOS **[TEXT SHREDDER]**

Où le trouver ? [**https://textshredder.codeplex.com**] Difficulté :

TUTO





01› CHIFFREMENT

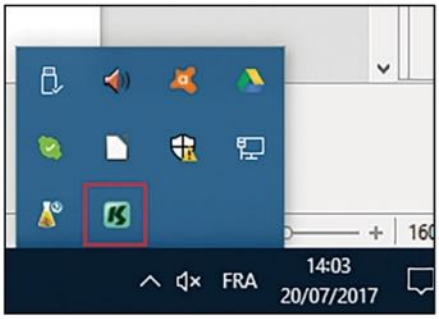
Lancez le programme et tapez un mot de passe (le deuxième est facultatif). TextShredder évalue son niveau de sécurité. Visez au moins le **Strong** avec la classique combinaison de majuscules, caractères spéciaux et chiffres. Validez avec **OK** puis entrez à nouveau votre mot de passe, toujours en validant avec **OK**. Tapez ensuite le message et cliquez sur **Encrypt**. Envoyez le **Encrypted text** à votre destinataire.

02› DÉCHIFFREMENT

Le destinataire doit ouvrir TextShredder et se rendre dans l'onglet **Decrypt** pour coller le message chiffré sous **Text to Decrypt**. Après un clic sur **Decrypt** en bas à droite, il sera invité à entrer le mot de passe, que vous lui aurez communiqué de manière sécurisée, pour enfin voir le message. TextShredder intègre même un clavier virtuel pour déjouer les keyloggers, ces enregistreurs de frappes au clavier.

01# Chiffrez vos frappes au clavier
→ AVEC KEYSCRAMBLER

Vous l'ignorez peut-être, sauf si vous êtes un lecteur assidu de Pirate Informatique, mais tout ce que vous tapez sur votre clavier peut être intercepté si votre PC est infecté par un keylogger. Pour contrer cela, nous vous proposons d'installer KeyScrambler. Installez le logiciel puis redémarrez votre bécane. Une petite barre verte s'affiche brièvement sur votre bureau, signe que KeyScrambler est actif. Une icône est également présente dans la barre des tâches. Toutes vos frappes au clavier sont désormais protégées contre les vils keyloggers.



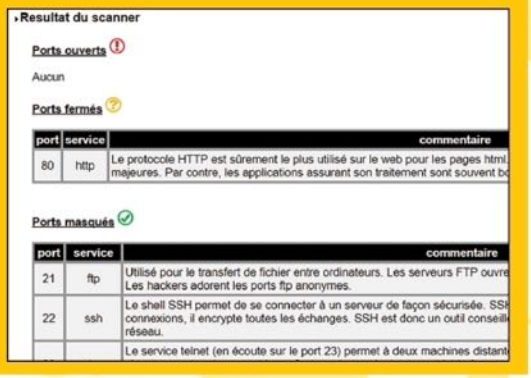
Difficulté : Lien : **https://goo.gl/vTt1gN**

02# Scannez les ports de votre PC → AVEC INOCULER

Vous avez l'impression que votre PC attrape tous les virus qui se promènent sur Internet ? Un pirate sino-russe profite certainement de la faiblesse liée à un port que vous avez laissé ouvert par inadvertance. Suivez notre lien pour effectuer un scan des ports en ligne. Depuis **Outils**, choisissez **Scanner de ports**. Démarrez l'opération avec **Scanner les ports de mon ordinateur maintenant**. Les ports ouverts sont notés en rouge, à vous de les fermer en agissant directement sur votre pare-feu.

Difficulté :

Lien : **www.inoculer.com**


Resultat du scanner

Ports ouverts

Aucun

Ports fermés

port	service	commentaire
80	http	Le protocole HTTP est sûrement le plus utilisé sur le web pour les pages html. majeures. Par contre, les applications assurant son traitement sont souvent b

Ports masqués

port	service	commentaire
21	ftp	Utilisé pour le transfert de fichier entre ordinateurs. Les serveurs FTP ouvre Les hackers adorent les ports ftp anonymes.
22	ssh	Le shell SSH permet de se connecter à un serveur de façon sécurisée. SS connexions, il encrypte toutes les échanges. SSH est donc un outil conseill réseau.
		Le service telnet (en écoute sur le port 23) permet à deux machines distant

03# Testez votre messagerie
→ AVEC EMAIL PRIVACY TESTER

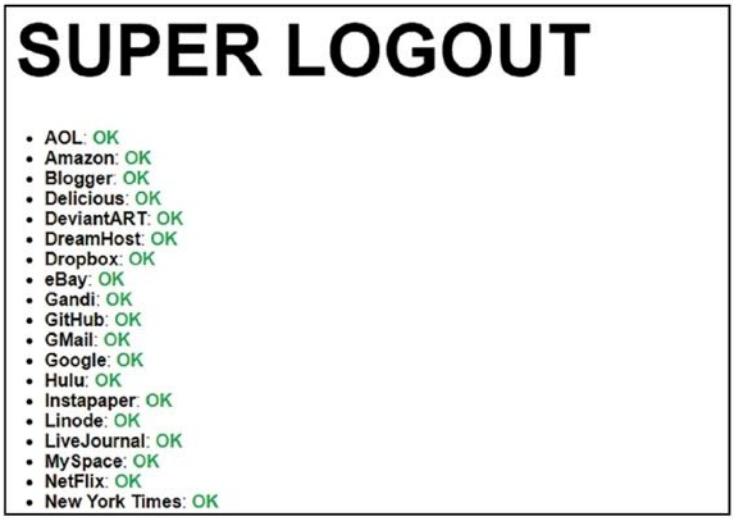
Malgré vos précautions, votre adresse IP peut se retrouver dans la nature, et pour les échanges de mails, votre client ou votre service Webmail ne sont pas forcément vos alliés. Pour identifier le type d'informations qui circulent sur Internet, lorsque vous envoyez des mails, rendez-vous sur ce site puis tapez votre adresse de messagerie dans le champ **Email Address** avant de cliquer sur **Submit**. Ouvrez l'email reçu sur votre boîte. Les éléments en rouge sont susceptibles d'apparaître chez vos correspondants. Réglez votre client en conséquence pour colmater les fuites.

Difficulté :

Lien : **www.emailprivacytester.com**

04# Vous déconnecter de plusieurs services automatiquement → avec Super Logout

Vous avez ouvert vos comptes Google, YouTube, eBay, Netflix, Wikipedia, AOL... dans différents onglets de votre navigateur et, en partant dans la précipitation, vous avez oublié de vous déconnecter. Une omission dangereuse sur un ordinateur partagé... Pour ne plus prendre de risques, suivez notre lien pour arriver sur Super Logout. Dès que le site s'affiche dans votre navigateur, les déconnexions commencent. Patientez jusqu'à ce que les **OK** verts apparaissent à la droite des services, signe que la déconnexion a été réalisée.

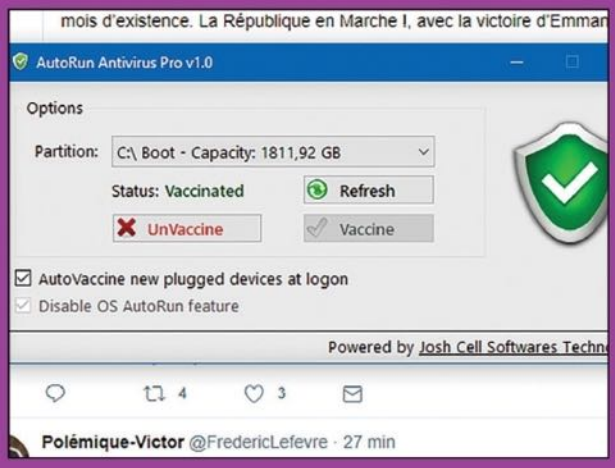


Difficulté : 💀💀💀

Lien : **http://superlogout.com**

05# Protégez votre système d'une infection USB → avec AutoRun Antivirus Pro

Les virus appelés «autorun» sont présents sur les clefs USB ou les disques durs externes. Dès que vous les connectez à votre PC, ils entrent en action et infectent votre machine. Suivez notre lien pour télécharger AutoRunAntivirus Pro. Définissez via le menu déroulant la **Partition** à vacciner puis cliquez sur **Vaccine** pour protéger votre système des indésirables présents sur les périphériques externes. Il est recommandé de réaliser l'opération sur vos appareils USB. Pour ce faire, cochez la case **AutoVaccine new plugged devices at logon**.



Difficulté : 💀💀💀

Lien : **https://goo.gl/iUb9zj**

06# Expulsez les squatteurs de réseau Wi-Fi

→ AVEC FING NETWORK TOOLS

Rien de plus rageant que de voir son réseau Wi-Fi complètement aux fraises, sans aucune raison. Impossible de regarder une vidéo en streaming, de faire une petite partie de DOOM en ligne ou de télécharger de la musique en toute légalité...
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 gratuite Fing Network Tools, disponible sur Android, vous dénichez les squatteurs et vous les expulsez par la même occasion. On ne peut pas s'emparer d'une connexion Wi-Fi impunément.

Difficulté :

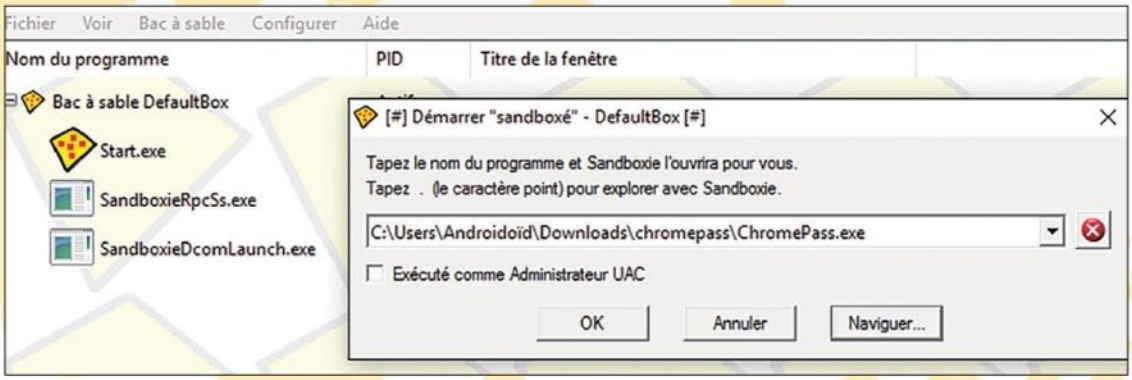
Lien : **https://goo.gl/rild3**

07# Testez un logiciel douteux avant de l'installer

→ AVEC SANDBOXIE

La sandbox sert quand vous souhaitez tester un logiciel, car vous doutez de son authenticité. Installez le programme Sandboxie en suivant notre lien. Lancez ensuite un soft puis suivez **Bac à sable** > **DefaultBox** > **Exécuter « sandboxé »** > **Exécuter un programme** > **Naviguer**. Dans l'explorateur qui s'ouvre, pointez vers le logiciel à tester puis validez avec **OK**. Si le cadre brille en jaune durant l'installation dans la sandbox, cela signifie que le programme est de confiance. En rouge, ce dernier est potentiellement dangereux.

Difficulté : Lien : **www.sandboxie.com**



08# Vaccinez vos clefs USB

→ AVEC USBFIX FREE

En complément d'AutoRun Antivirus Pro, qui se charge de protéger votre système d'une infection provoquée à cause d'une clef USB vérolée, utilisez USBFix. Le logiciel se charge de détruire les infections repérées sur le périphérique de stockage externe, de la vacciner et tente de restaurer les fichiers qui ont été endommagés. Si d'autres fichiers sont infectés, ils iront en **Quarantaine**. Commencez par faire **Recherche** et effectuez un **Nettoyage** si des menaces sont repérées.

Difficulté :

Lien : **www.usbfix.net**

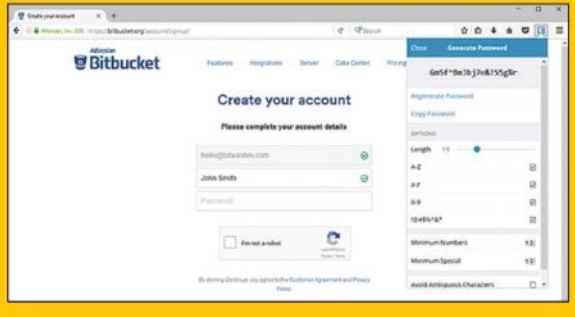
09# Désinfectez et réparez votre PC → AVEC WINDOWS REPAIR TOOLBOX

Windows Repair Toolbox est, comme son nom l'indique, une boîte à outils pour votre bon vieux Windows malade ou convalescent. Ce programme embarque quantité de logiciels de réparation (**FixWin**, **FreeFixer**, **Zoek**...), mais aussi des outils de désinfection ou encore de diagnostic (température de votre processeur, utilisation de la mémoire, espace de stockage disponible...). Passez votre souris au-dessus d'un outil pour en obtenir la description. Vous n'avez qu'à cliquer sur un outil pour le solliciter.

Difficulté : Lien : **https://goo.gl/XTrA3p**

10# Rapatriez tous vos mots de passe dans un gestionnaire Open Source → AVEC BITWARDEN

Parce que vous savez très bien qu'un mot de passe fort et différent pour chaque service est une étape nécessaire vers la sécurité, vous avez opté pour un gestionnaire de mot de passe. Mais parce que ce dernier ne vous plaît plus, vous aimeriez en changer, sans devoir tout refaire. Bitwarden est un gestionnaire Open Source qui permet de rapatrier simplement vos mots de passe en provenance de 1Password, Chrome, LastPass ou autre. Une application mobile est également de la partie, le tout gratuitement.



Difficulté : Lien : **https://bitwarden.com**

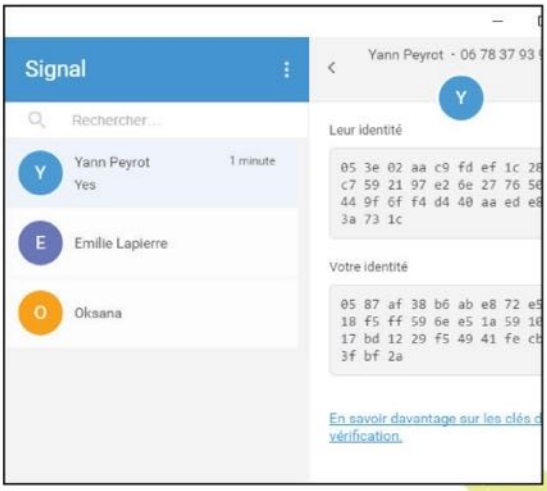
ANONYMAT

SYNCHRONISEZ SIGNAL AVEC VOTRE PC

L'application de messagerie chiffrée préférée d'Edward Snowden nécessite une petite manipulation pour être active dans votre navigateur Chrome.

INFOS [SIGNAL]
Où le trouver ? [**https://whispersystems.org**] Difficulté : ☠☠☠

TUTO



01› SYNCHRONISER

Une fois l'extension de navigateur **Signal Private Messenger** installée, utilisez votre smartphone pour scanner le QR Code et synchroniser le PC avec le mobile. Vous devriez voir votre numéro de téléphone s'afficher dans une fenêtre. Validez pour voir vos contacts et converser avec eux. Les messages seront aussi contenus dans votre mobile, avec un chiffrement de bout en bout.

02› VÉRIFIER L'IDENTITÉ DE VOTRE CORRESPONDANT

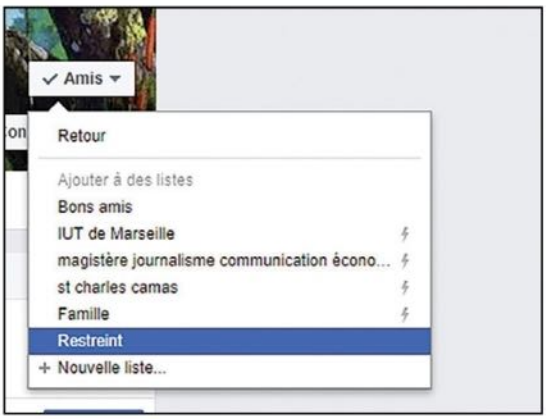
Libre à vous de vérifier l'identité de votre correspondant avec la clé publique. Sur mobile, initiez une conversation et faites **Préférences de conversation** > **Vérifier** l'identité. Sur PC, il faudra cliquer sur les trois petits point verticaux puis **Vérifier l'identité**. Vous obtenez une suite de lettres et de chiffres. Demandez à votre interlocuteur d'envoyer la sienne et comparez.

PROTÉGEZ VOS PUBLICATIONS FACEBOOK DES AMIS CURIEUX

Vous ne souhaitez plus qu'un « ami » accède à vos publications, mais vous ne voulez pas pour autant le retirer de votre liste d'amis, car il s'en apercevrait. Voici la solution.

INFOS [FACEBOOK]
Où le trouver ? [www.facebook.com] Difficulté : ☠☠☠

TUTO



01 › RESTREINDRE L'AMI

Connectez-vous sur votre compte Facebook puis allez sur la page de « l'ami » en question. Cliquez sur la flèche à droite d'**Amis** (celle pointant vers le bas) puis sélectionnez **Ajouter à une autre liste** > **Restreint**. Celui-ci pourra alors voir uniquement les publications que vous aurez rendues publiques.

02 › UTILISER LE MODE DE PUBLICATION PRIVÉE

Cliquez sur le point d'interrogation en haut à droite pour aller dans les **Raccourcis de confidentialité**. Là, si **Public** est affiché dans **Qui peut voir mes futures publications**, optez pour **Amis** à la place. Vos futures publications seront désormais invisibles aux personnes présentes dans la liste **Restreint**.

NOS GUIDES WINDOWS 100% PRATIQUES

POUR UN PC

+ Puissant
+ Beau
+ Pratique
+ Sûr

Mini Prix : 3,50 €

Chez votre marchand de journaux

LIMITER LES TRACES DE SA NAVIGATION

INFOS [ADBLOCK PLUS] [https://adblockplus.org/fr]
[GHOSTERY] [www.ghostery.com/fr] Difficulté : ☠☠☠

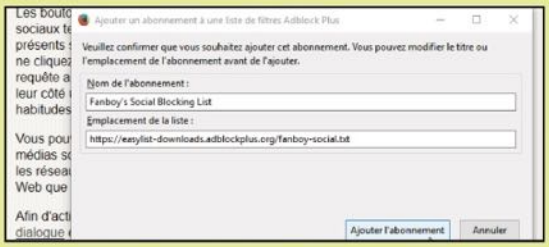
TUTO

01 › LIMITER LES COOKIES

Le cookie a plusieurs utilités, dont fournir des données sur vos habitudes de surf à des publicitaires... Dans Firefox, allez dans **Options > Vie privée** puis choisissez **Accepter les cookies tiers depuis les sites visités** et **Les conserver jusqu'à la fermeture de Firefox**. Sur Chrome, il faut passer par une extension comme **Click&Clean**.

02 › CHANGER DE MOTEUR DE RECHERCHE

Google est très efficace, mais aussi très indiscret, gardant traces de vos recherches et adresse IP, et créant une « bulle » orientant les résultats en fonction des précédents. Pour un anonymat respecté, essayez des moteurs comme **StartPage**, **Qwant**, ou **DuckDuckGo**, faciles à définir comme moteur par défaut. Exemple sur Qwant : cliquez sur **Installez Qwant**.



03 › BLOQUER LES BOUTONS DE RÉSEAUX SOCIAUX

Vous voyez ces boutons Facebook, Twitter ou Google+ sur certains sites Web ? Ils vous tracent que vous cliquiez dessus ou non, et même si vous n'avez pas de compte ! La célèbre extension Adblock Plus peut s'en occuper. Une fois installée, rendez-vous sur **https://adblockplus.org/fr/**features et, sous **Désactiver les boutons des médias sociaux**, cliquez sous **ouvrir cette boîte de dialogue** et **Ajouter l'abonnement**.

04 › BLOQUER LES MOUCHARDS

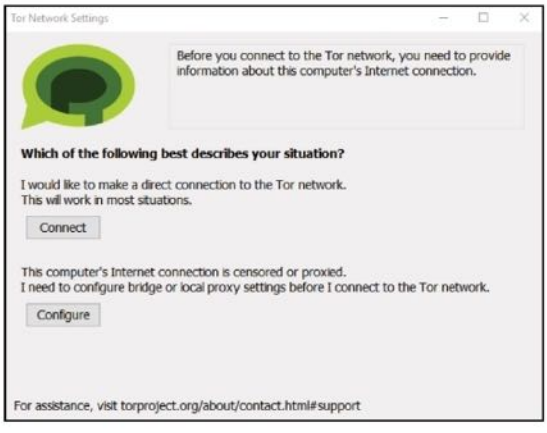
Chaque fois que vous visitez une page Web, un tas de programmes invisibles, des scripts, collectent des données sur vos activités et vos habitudes de surf. L'extension **Ghostery**, pour Firefox et Chrome, les bloque. Une fois installée, une page s'ouvre, sur laquelle vous devrez cocher les types de mouchards à bloquer. Attention, cela peut empêcher un site de fonctionner correctement.

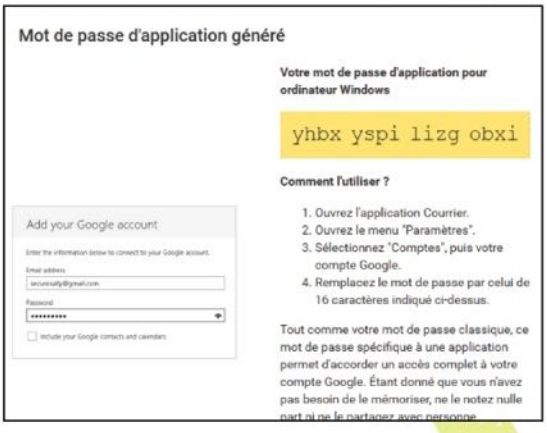
TOR MESSENGER : LE CHAT CHIFFRÉ

Compatible avec la plupart des protocoles de messagerie instantanée, Tor Messenger, bien qu'en bêta, est un service chiffré très prometteur.

INFOS [TOR MESSENGER BETA]
Où le trouver ? [**https://goo.gl/hb0AFr**] Difficulté : ☠☠☠

TUTO





01 › INSTALLER

Suivez le lien et choisissez **Get the lastest version**. Sous Windows 10, il faudra cliquer sur **Exécuter quand même** si vous avez Smartscreen d'activé. Si vous êtes dans un pays où les FAI scrutent les connexions Tor (Chine par exemple), ou si vous êtes derrière un proxy, choisissez **Configure**. Sinon, faites **Connect**. Sélectionnez ensuite le protocole de votre choix. Notez que XMPP n'est plus compatible avec Facebook depuis 2015.

02 › CONFIGURER

Nous avons choisi **Google Talk** (Gmail), car il requiert un peu plus de réglages que les autres. Google refuse une connexion directe avec vos identifiants « normaux ». Allez sur **https://myaccount.google.com** puis activez la **Validation en deux étapes** dans **Connexion et sécurité**. Ensuite, générez un **Mot de passe d'application** ici : **https://goo.gl/wJyqke**. Choisissez **Messagerie** puis **Ordinateur Windows** pour obtenir le sésame à rentrer dans Tor Messenger. Attention : pour chiffrer les messages, cliquez sur le petit cadenas rouge.

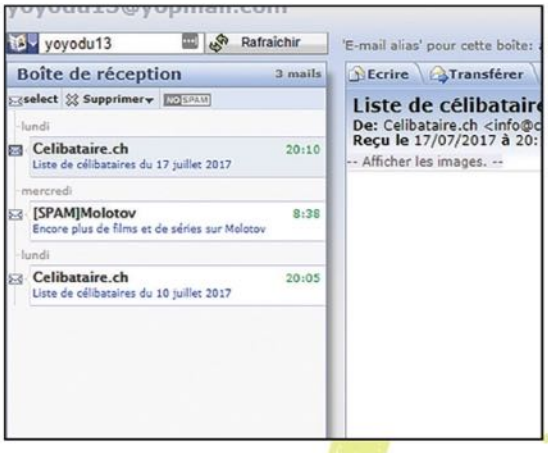
PROFITEZ D'UN MAIL JETABLE

1

Pour faire tampon entre votre véritable adresse mail et un service ou bien pour disposer d'une adresse temporaire, utilisez Yopmail.

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

TUTO



01 › SE CONNECTER

Inventez un nom pour votre boîte mail fictive. Par exemple : **yoyodu13**. Écrivez-le dans le champ **Saisissez le mail jetable de votre choix**. Cliquez ensuite sur **Vérifier les mails**. Vous accédez ensuite à votre boîte mail.

02 › UTILISER VOTRE ADRESSE

Vous voici dans la boîte de réception de votre mail. Pas d'inscription ou de mot de passe. Notez que tout le monde peut accéder aux boîtes Yopmail en tapant le même nom que vous (si l'utilisateur a la même idée). Veillez à ne pas l'utiliser pour des échanges importants ou pour recevoir des mails sensibles.

FLOUTEZ LES VISAGES

ObscuraCam sur Android est une appli qui reconnaît et brouille les visages sur les photos. Pour protéger l'identité des personnes.

INFOS [OBSCURACAM]
Où le trouver ? [**https://goo.gl/Ugnhhd**] Difficulté :

TUTO

01› EXPLORER LE MENU

L'application ne nécessite pas l'accès root. Dans le menu vous aurez le choix entre prendre une nouvelle photo avec **New Picture** (qui sera automatiquement traitée par ObscuraCam) ou ouvrir une photo/vidéo déjà existante via **Obscure Photo**.

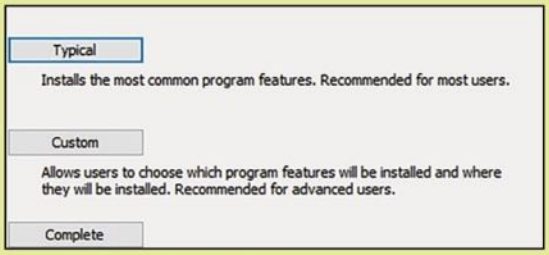
02› DÉTECTER LES VISAGES

L'appli va détecter les visages. Si elle a «oublié» quelqu'un, vous pouvez ajouter un masque ou en supprimer un. Lorsque vous sélectionnez un visage, vous avez le choix entre plusieurs effets : une pixellisation forcée, une sorte de postiche virtuel (lunette + gros nez) et quelques autres.

SUPPRIMEZ VOS DONNÉES SENSIBLES

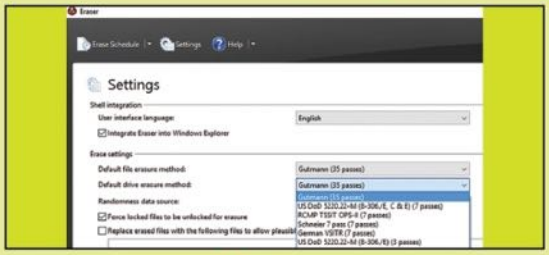
INFOS [ERASER]
Où le trouver ? [: https://eraser.heidi.ie] Difficulté :

TUTO



01 › INSTALLER

Eraser propose trois modes d'installation. Nous vous conseillons d'opter pour **Typical**, qui va installer les composants classiques du logiciel. **Custom** permet de choisir avec précision chaque élément, mais mieux vaut savoir ce que vous faites. Notez qu'Eraser ne contient pas de bloatware (logiciels additionnels indésirables). Cliquez sur **Install** pour confirmer votre choix.



02 › PARAMÉTRER

Eraser va non seulement supprimer vos fichiers, mais surtout réécrire sur l'espace laissé libre avec des données aléatoires. Vous pouvez opter pour des méthodes encore plus sûres. Lancez Eraser, allez dans **Settings** et choisissez **Gutman (35 passes)** pour les deux premières lignes sous **Erase Settings**. Validez avec **Save Settings**.

03 › EFFACER

Eraser s'intègre dans le menu contextuel de Windows pour une utilisation extrêmement simple : il suffit de faire un clic droit sur le fichier à effacer et d'aller sur **Eraser > Erase**. Une fenêtre vous demande si vous êtes sûr de vouloir faire cela, confirmez avec **Yes**. L'opération prend plus ou moins de temps suivant la méthode choisie (étape précédente).

04 › ESSAYER UNE ALTERNATIVE

Cherchez le programme **R-Wipe & Clean** dans Google. Il s'agit d'une alternative à Eraser. De la même manière, une fois installé, il se sollicite depuis le menu contextuel de Windows (lorsque vous faites un clic droit sur un fichier). Il permet de faire le ménage sur votre bécane, sans laisser aucune trace de vos données personnelles (pratique si vous souhaitez vendre votre PC).

OPENVPN sous WINDOWS

Le protocole OpenVPN est réputé pour être sûr mais pour l'utiliser, il faut passer par un prestataire qui s'ocupera du trafic. Pour ce test grandeur nature, nous avons choisi le service IPredator basé en Suède. Vous êtes libre d'en choisir un autre mais sachez que ce dernier est une création des 3 enfants terribles de Pirate Bay...

Espionnage, piratage de vos données personnelles, infection... Surfer sur Internet n'est pas sans danger, surtout avec la multiplication des points d'accès WiFi où il est compliqué de vérifier la sécurité. Une solution pour y remédier : passer par un VPN, ou Virtual Private Network. Le principe est simple : une fois le VPN activé, les données envoyées quand vous serez sur Internet passeront par un «tunnel» où elles seront chiffrées, rendant impossible l'espionnage ou l'interception de vos données. Vous aurez même le droit à une IP dans un autre pays pour brouiller les pistes. À part quelques rares exceptions, les VPN sont devenus des services commerciaux payants.

POURQUOI CHOISIR IPREDATOR ?

Pour cette démonstration nous avons choisi IPredator, car même s'il se situe dans un pays qui oblige à conserver les données, l'équipe a volontairement diversifié les zones géographiques pour chaque pièce du puzzle : conservation des données, propriété du service, du serveur, du réseau, etc. Le but est de rendre toute tentative de harcèlement juridique difficile, voire impossible. L'IP réelle du client est utilisée le temps de la connexion et c'est tout. Bien sûr, il faut les croire sur parole pour ce dernier détail, mais après tout, les personnes à

POURQUOI UTILISER UN VPN ?

- Éviter l'espionnage et les attaques (cela va des services secrets aux pirates en passant par HADOPI)
- Protéger son emplacement
- Se connecter en toute sécurité sur un point d'accès WiFi inconnu
- Rester anonyme sur Internet
- Contourner la géolocalisation de certains sites (avoir le Netflix US en France par exemple même s'il faudra en plus utiliser Tor, car IPredator ne propose qu'une IP suédoise que vous pouvez faire «rebondir» avec Tor)
- Contourner le bridage de certains sites ou services si un jour la neutralité du Net n'était pas respectée

l'origine du projet sont les créateurs de Pirate Bay : Gottfrid Svartholm, Fredrik Neij et Peter Sunde. On peut tomber plus mal comme caution. Le problème des VPN payants c'est...qu'il faut les payer ! Et l'argent laisse des traces. IPredator se plie en quatre pour proposer le plus de moyens de paiement possibles dont certains sont anonymes : carte de crédit prépayée (il suffit de l'acheter avec du liquide), BitCoin (même si le BitCoin n'est pas anonyme à la base, il est possible de passer par Tor et de réduire les risques).

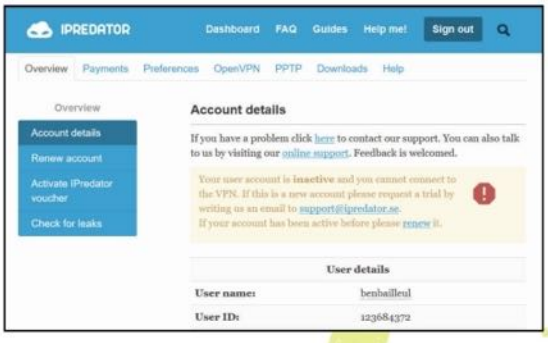
POURQUOI CHOISIR OPENVPN ?

Le protocole PPTP est disponible sur IPredator, mais il est fortement déconseillé, car considéré comme cassé. À l'inverse, OpenVPN propose un chiffrement solide. Seuls inconvénients : il reste gourmand en ressource (problématique sur mobile) et est un peu plus compliqué à mettre en place. Heureusement, Viscosity (un «fork» d'OpenVPN pour PC) simplifie les choses en proposant une interface intuitive et la gestion du fichier .ovpn contenant vos informations personnelles pour accéder au «tunnel». Le logiciel est gratuit 30 jours puis coûte 8,50 € à l'achat. Avec les 6 €/mois du service IPredator, cela fait un petit budget à prévoir au début de l'aventure, mais c'est le prix de la tranquillité. Sur mobile, le client OpenVPN for Android est gratuit.

PÉRIODE D'ESSAI ET INSCRIPTION

INFOS [IPREDATOR]
Où le trouver ? [**https://ipredator.se**] Difficulté : ☠☠☠

TUTO



01› TROIS JOURS D'ESSAI

Il est apparemment impossible de payer directement pour un mois ou plus, il faudra d'abord demander une période d'essai de 72 heures (sans doute font-ils cela pour éviter de rembourser les n00bs qui n'arriveront pas à faire fonctionner le VPN). Envoyez une demande en anglais à cette adresse : support@ipredator.se. Pas besoin de faire du Shakespeare, aidez-vous de Google Traduction. Au bout de trois heures nous avons reçu notre code pour une période d'essai. Pas de carte bancaire à sortir donc...

02› VOTRE COMPTE

Ouvrez un compte, identifiez-vous et sur la gauche, cliquez sur **Activate IPredator voucher** et entrez le code pour activer votre compte. Vous serez alors dirigé vers le **Dashboard** d'où vous aurez accès à vos données, vos fichiers de configuration, etc. Lorsque votre période d'essai sera terminée, c'est dans **Renew Account** qu'il faudra aller pour payer et **Check for Leak** permet de voir si votre VPN est bien étanche lorsqu'il sera installé. En haut, **Guides** vous propose des tutos pour tous les appareils compatibles.

INFOS [VISCOSITY (optionnel)]
Où le trouver ? [**www.sparklabs.com/viscosity**] Difficulté :

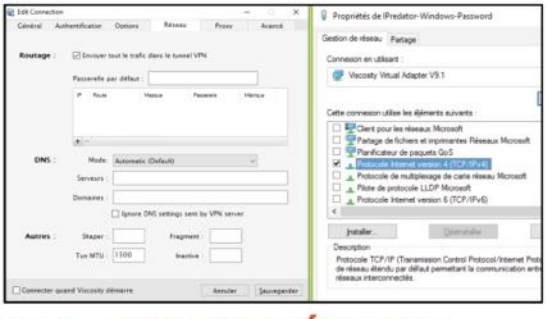
TUTO

01 › UNE OFFRE UNIQUE POUR TOUS LES SYSTÈMES

Sous Windows, on a le choix entre le client OpenVPN de base ou le client Viscosity, payant, mais plus simple et disposant d'une interface graphique et d'un très bon système d'import/export de configuration. Heureusement Viscosity dispose d'une version d'essai de 30 jours. À vous de voir ensuite si ce dernier vaut les 9 $ (8,50 €) que l'éditeur vous réclamera. Si vous pensez le contraire, le client historique est à peine plus compliqué et vous trouverez de l'aide dans **Guides**. Notez que IPredator fonctionne sous Linux, iOS, MacOS, Android, etc.

02 › VOTRE FICHIER .OVPN PERSONNEL

Téléchargez Viscosity, installez-le et dans votre **Dashboard**, téléchargez aussi le fichier **IPredator-Windows-Password.ovpn**. Lancez Viscosity puis dans la zone de notification, faites un clic droit dans l'icône correspondant au client et choisissez **Préférences**. Dans cette nouvelle fenêtre, faites **+** puis **Importer connexion** > **À partir du fichier** puis trouvez le fichier **.ovpn**. Vous devriez voir **Connexion importée** si tout se passe bien.



03 › QUELQUES RÉGLAGES...

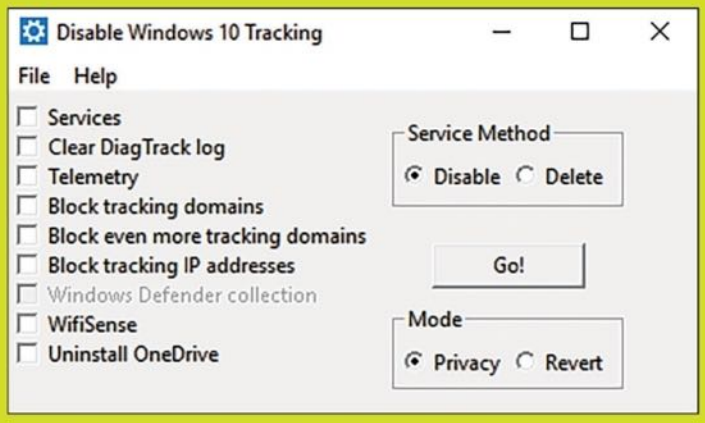
Sélectionnez maintenant **Éditer** et allez dans l'onglet **Réseau** pour cocher la case **Envoyer tout le trafic dans le tunnel VPN**. Vous n'avez pas besoin de faire autre chose. Cliquez sur **Sauvegarder**. Maintenant il va falloir désactiver des services dans la connexion en passant par Windows. Ouvrez le menu **Démarrer**, allez dans **Paramètres** > **Réseau et Internet** > **VPN** > **Modifier les options d'adaptateur**. Effectuez un clic droit sur **IPredator** et sélectionnez **Propriétés**. Décochez toutes les cases sauf **Protocole Internet version 4 (TCP/IPv4)**. Validez avec **OK**. Dans la zone de notification faites un clic droit dans l'icône de Viscosity, cliquez sur **Détails** et laissez cette fenêtre ouverte.

04 › CONNEXION, VÉRIFICATION ET RÉSULTAT

Toujours dans la zone de notification cliquez sur **Connecter IPredator**. Il ne vous reste qu'à rentrer les identifiants que vous avez utilisés pour l'inscription et vous pourrez voir dans la fenêtre **Détails** que vous êtes connecté. En faisant un test de bande passante, nous sommes passés de 10,15 à 7,62 Mbit/s en téléchargement. La différence est imperceptible par contre, le ping est passé de 28 à 227 : OpenVPN n'est pas vraiment l'ami des gamers. Vérifiez qu'il n'y a pas de fuite avec cette URL : https://check.ipredator.se. Et n'oubliez pas de passer par Tor en plus !

01# Désactiver les derniers mouchards de Windows 10 → Avec Disable Win Tracking

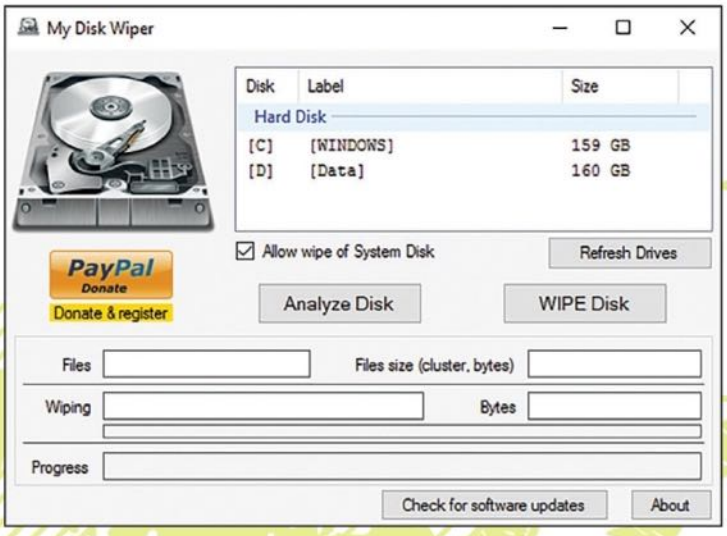
Si Windows 10 permet de désactiver certains de ses mouchards dans **Paramètres du PC > Confidentialité**, d'autres existent , cachés, impossibles à supprimer depuis l'interface. Téléchargez **Disable Win Tracking**, faites un clic droit sur le fichier **.exe** et **Exécuter en tant qu'administrateur**. Cochez toutes les cases de gauche, sauf si vous craignez des problèmes avec certains services et logiciels (le programme vous en avertira) et cliquez sur **Get privacy**. Redémarrez le PC une fois l'opération terminée.



Difficulté : Lien : **goo.gl/oVBdwZ**

02# Effacer les données compromettantes ou confidentielles → Avec My Disk Wiper

Envie de faire le grand ménage dans votre PC sans pour autant formater et tout réinstaller ? My Disk Wiper va effacer toute trace de données sur un disque dur ou une clé USB, sans espoir de récupérer quoi que ce soit. Que vous vouliez vendre ou acheter un ordinateur d'occasion, vous éviterez de voir vos données personnelles dans la nature ou, au contraire, vous effacerez les informations compromettantes de votre nouvelle acquisition.

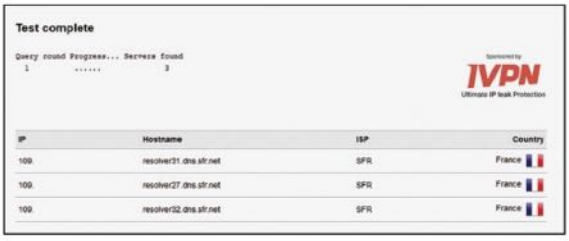


Difficulté :

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

03# Vérifier son VPN → Avec DNS Leak

Vous utilisez un VPN ? Sachez que vous n'êtes pas à l'abri des fuites de DNS, l'envoi accidentel de paquets d'informations utilisant le DNS de votre fournisseur d'accès Internet au lieu de celui proposé par votre VPN. Un réel problème d'anonymat. Lancez un test sur DNS Leak et vérifiez que les serveurs sont les mêmes que ceux de votre VPN. Sinon, vous êtes potentiellement vulnérable.



Difficulté : ☠☠☠ Lien : **dnsleaktest.com**

04# Brouiller votre empreinte Internet → Avec Random Agent

Entre les proxies, les VPN, les clients mail et les espaces de stockage chiffrés, vous êtes paré à toutes les éventualités sauf une : l'empreinte unique de votre navigateur. Avec une simple requête, il est possible de connaître son nom, sa version, le nombre et les noms des extensions, les polices installées, votre fuseau horaire, votre version de Windows, la résolution de votre écran, etc. En combinant ces différents éléments, les hackers peuvent dresser une empreinte unique : la vôtre. Random Agent Spoofer propose de brouiller encore plus les pistes sur Internet en générant de manière aléatoire des informations bidons. Vérifiez vos données sur https://panopticlick.eff.org ! Pour Chrome, essayez User-Agent Switcher.

Difficulté : ☠☠☠

Lien : **https://goo.gl/7rwHkH**

05# Un VPN Gratuit → Avec Opera

Il n'y a pas que Firefox et Chrome dans la vie (qui a dit Edge?). Et côté anonymat, le navigateur Opera est le seul à embarquer un VPN. Pour en profiter il faudra aller dans **Menu** > **Réglages** > **Vie privée & sécurité** puis cocher la case **Activer le VPN**. Vous aurez alors un bouton **VPN** dans la barre d'adresse d'où vous aurez accès à vos statistiques

et aux 5 pays « d'emprunt ». Ce VPN gratuit (fourni par SurfEasy) ne couvrira bien sûr que les données transitant par le navigateur...et c'est déjà pas mal.

Difficulté : ☠☠☠

Lien : **opera.com/fr/computer/windows**

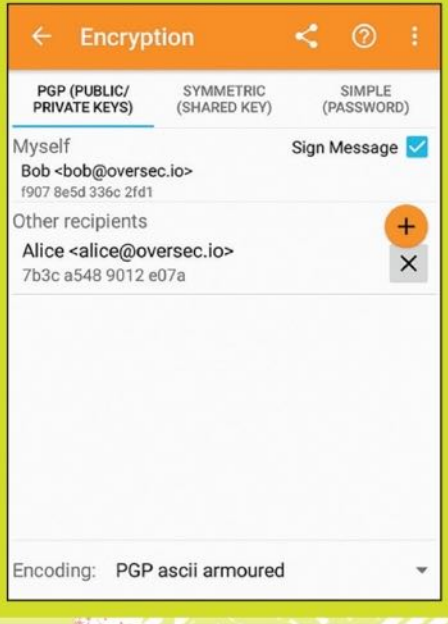
06# Du chiffrement natif sur Android

→ Avec Oversec

Lorsqu'il s'agit de chiffrer des communications, il faut que les correspondants utilisent le même logiciel/protocole. Décourageant, puisqu'il faudra « convertir » vos amis et contacts à tel ou tel service. Sur Android, la solution pourrait s'appeler Oversec : une application qui ajoute une couche de chiffrement de bout en bout à toutes les autres applications. À vous les SMS, Facebook, Twitter, Skype, ou Gmail entièrement chiffrés ! Alors certes, ici aussi vos correspondants devront posséder Oversec, mais ils pourront l'utiliser avec toutes les applications en leur possession. Il est même possible d'avoir de faux textes qui s'afficheront en clair sur le réseau pour détourner l'attention des espions/pirates !

Difficulté :

Lien : **oversec.io**



07# Une messagerie auto destructible → Avec Confide

Encore une messagerie sécurisée ? Oui, mais Confide a la particularité de détruire chaque message ou fichier échangé sitôt lu, sur les appareils bien sûr, mais aussi sur les serveurs. Pas de transfert ou de copie possible, et pas de capture d'écran non plus : vous obtiendrez juste un fond gris. Disponible sur PC, Mac, Android et iOS, Confide propose une interface très claire pour vous permettre de vous focaliser sur l'essentiel : discuter du plan de domination mondiale des Reptiliens Illuminati.

Difficulté :

Lien : **getconfide.com**

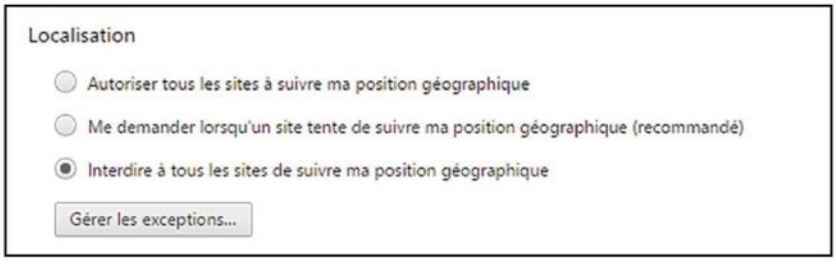
08# Être anonyme sur Internet

→ Avec Tor Browser

Vous utilisez Tor pour masquer vos activités sur le Net ou éviter les curieux ? Vous avez bien raison. N'oubliez cependant pas de mettre à jour votre **Tor Browser** pour disposer des dernières fonctionnalités ! C'est le moment où jamais avec cette version 7 qui reprend les bases de Firefox 52 et ajoute de nouvelles fonctionnalités, tout en corrigeant les dernières failles et quelques bugs. N'oubliez pas de n'installer aucune extension supplémentaire sur ce navigateur !

Difficulté : Lien : **torproject.org**

09# Bloquer les demandes de localisation dans les navigateurs → Avec Chrome, Firefox et Edge

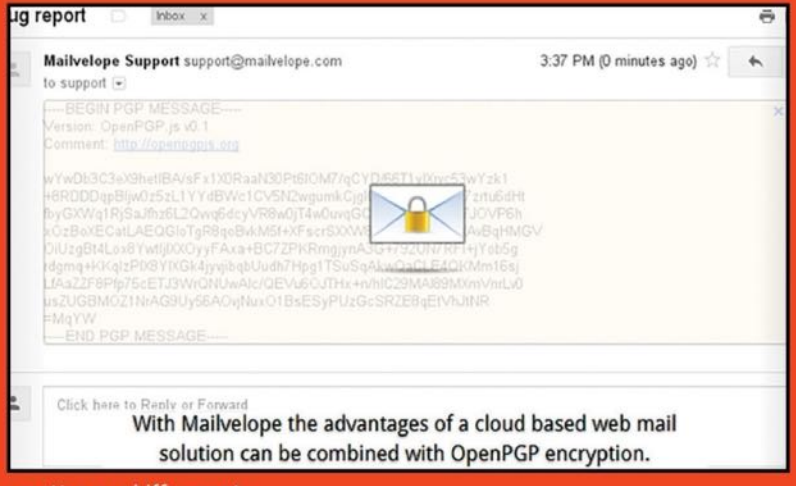


Les navigateurs demandent parfois votre localisation. Ça peut se comprendre sur Google Maps (et encore), mais dans la majorité des cas, c'est une indiscrétion inutile. Dans Chrome, allez dans les **Paramètres**, cliquez sur **Afficher les paramètres avancés** puis sur **Paramètres de contenu** (sous **Confidentialité**) et cochez **Interdire à tous les sites de suivre ma position géographique**. Sous Firefox, tapez **about:config** dans la barre d'adresse, passez l'avertissement, tapez **geo.enabled** et double-cliquez sur la valeur pour qu'elle bascule sur **false**. Enfin, si vous utilisez Edge (on ne juge pas), allez dans les **Paramètres du PC > Confidentialité > Localisation** et décochez **Microsoft Edge** sous **Choisir les applications autorisées à utiliser votre emplacement exact**.

Difficulté :

10# Un webmail chiffré

→ Avec Mailvelope



With Mailvelope the advantages of a cloud based web mail solution can be combined with OpenPGP encryption.

Compatible avec des services comme Gmail, Yahoo ou Outlook.com, Mailvelope est une extension pour Chrome ou Firefox permettant de chiffrer le contenu de vos e-mails avec OpenPGP. Une fois installée, Mailvelope va faire apparaître des menus dans votre interface Web pour gérer vos clés publiques et privées : génération, import/export, stockage, etc. Le moyen le plus simple si vous voulez vous mettre au chiffrement.

Difficulté :

Lien : **mailvelope.com**

NOUVEAU !

Par l'équipe de *Pirate Informatique* !

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

GUIDE COMPLET

CHEZ VOTRE MARCHAND DE JOURNAUX

CRACK & MOTS DE PASSE

OUTREPASSEZ LE MOT DE PASSE DE WINDOWS

Que vous ayez oublié votre mot de passe Windows ou que vous ne le connaissiez pas (achat d'occasion, dépannage chez un ami...), il existe une solution pour réinitialiser ce dernier et en définir un autre. Ce n'est pas vraiment un « crack », mais l'effet est le même.

Windows stocke les informations concernant l'utilisateur dans le fichier **SAM** d'un répertoire de C:Windows. Ce fichier contient entre autres le mot de passe (chiffré) de votre session Windows. Pratique, sauf que si vous ne pouvez pas ouvrir une session avec les droits adéquats, impossible de changer le mot de passe à partir de ce fichier. Il va donc falloir contourner le problème.

DÉBLOQUER VOTRE WINDOWS

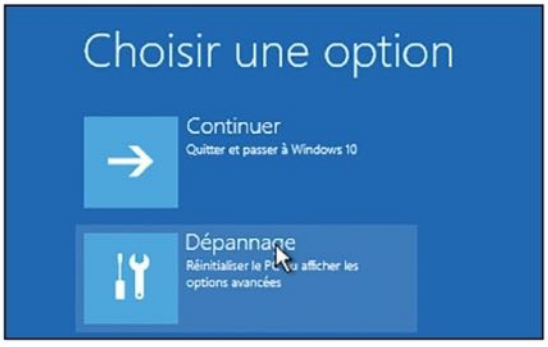
Peut-être connaissez-vous le logiciel Offline NT Password & Registry Editor, pour réinitialiser le mot de passe des comptes utilisateurs de tous les Windows de NT jusqu'à 10 en passant par XP. Plutôt rugueux à prendre en main, voici une astuce plus simple. Attention, elle ne fonctionne qu'avec un compte local, et pas avec le mot de passe du compte Microsoft (solution que nous déconseillons).

KON-BOOT, L'ALTERNATIVE

Ce logiciel s'installe sur une clé USB pour la rendre bootable. Kon-Boot pourra alors contourner la vérification du mot de passe Windows pour vous faire atterrir directement sur la session. Discret (il ne change pas le mot de passe), il peut aussi être utilisé à votre insu... La solution : crypter sa partition Windows, avec VeraCrypt par exemple.

INFOS [LE CD D'INSTALLATION DE WINDOWS]
Où le trouver ? [**www.microsoft.com**] Difficulté : ☠☠

TUTO

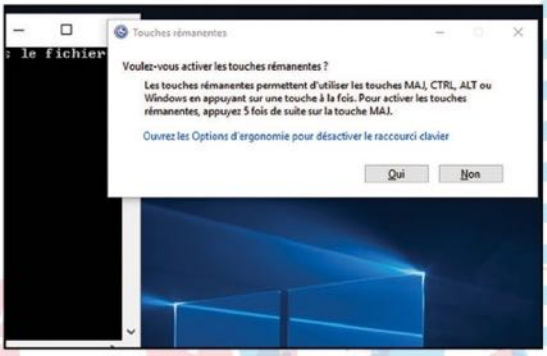


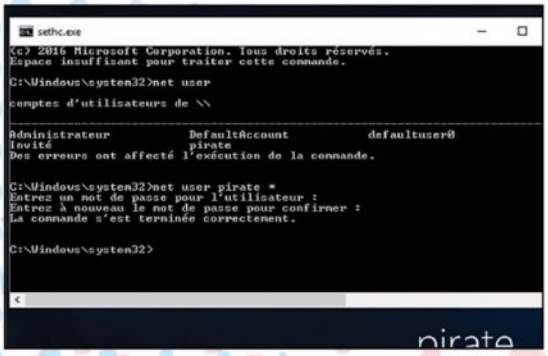
01 › UTILISER LE DVD D'INSTALLATION

Vous pouvez faire cette manipulation avec tous les Windows récents. Munissez-vous du CD d'installation de Windows. Si vous ne l'avez pas (version OEM), téléchargez une version « pirate » de Windows puisque vous l'avez acheté, mais vous pouvez aussi créer un DVD de réparation depuis un Windows identique au vôtre. Bootez votre PC depuis le lecteur optique en modifiant les paramètres de votre BIOS.

02 › COPIER LE FICHIER

Choisissez la langue du système et optez pour **Réparer l'ordinateur** (et non pas **Installer maintenant**). Dans **Dépannage**, sélectionnez **Options avancées** puis **Invite de commande**. L'objectif est de copier le fichier des touches rémanentes (sethc) qui se trouve dans **C :** (l'emplacement de Windows). Tapez la commande suivante : **copy c:\windows\system32\sethc.exe c:**





03 › LE REMPLACER

Remplacez le fichier copié par celui contenant l'invite de commande en faisant **c : \windows\system32\cmd.exe c : \windows\syetem32\sethc.exe**. Validez et tapez **Oui** (ou **y** si c'est en anglais). Redémarrez le PC jusqu'à voir votre session (si vous ne voyez pas de bouton, tapez **exit**). Lorsque votre nom et le mot de passe s'affichent, martelez la touche **Maj** pour accéder à l'invite de commande.

04 › CHANGER LE SÉSAME

Tapez la commande suivante pour enregistrer votre nouveau mot de passe : net user [votre nom de session] [votre nouveau mot de passe], exemple : **net user pirate Fh8&Pjk56n@p^**. Validez et faites **exit** pour fermer la console. Vous n'avez plus qu'à entrer votre nouveau mot de passe pour accéder à votre session. Bravo, vous récupérez votre environnement sans aucune perte de fichiers.

CRACKEZ VOTRE Z(L)IP !

Qui n'a jamais fait son malin en protégeant un fichier ZIP ou RAR avec un mot de passe, pour se rendre compte deux ans plus tard qu'il a oublié le sésame ? Nous allons y remédier...

Le problème avec les logiciels qui offrent de cracker les archives ZIP, RAR ou autres, c'est qu'ils proposent monts et merveilles, sans pour autant donner satisfaction : souvent lents, parfois obsolètes, certains fonctionnent, mais vous demanderont de passer à la caisse au moment de vous révéler le mot de passe.

Nous allons voir ici comment compresser une archive en spécifiant un mot de passe d'ouverture (pour ceux qui ne savent pas comment faire), puis nous concentrer sur le format ZIP avec le logiciel fcrackzip sous Windows. Ce dernier, en plus d'être gratuit et open source, a l'avantage de proposer l'attaque par dictionnaire en plus du brute force. Il n'est malheureusement pas compatible avec d'autres types d'archives comme le RAR ou le 7Z.

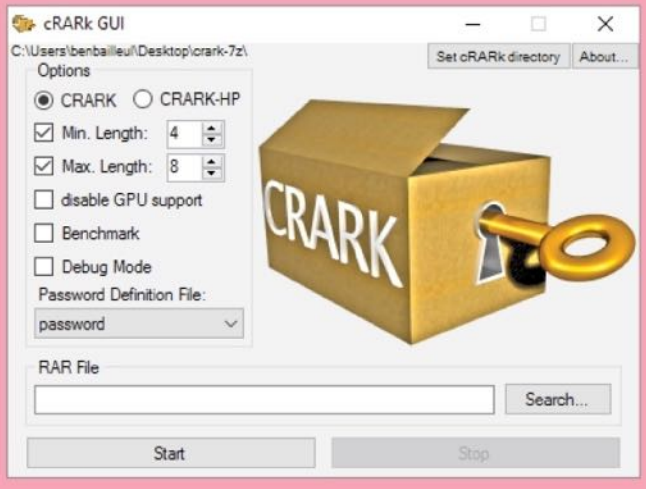
NOS ZIP DE TEST

Pour nos démonstrations, nous avons créé des fichiers compressés que nous allons tenter de cracker. Test1, 2, 3 et 4 sont des ZIP avec pour mot de passe **toto**, j**esus**, **delopa** et **H4j^p*U%J4s** (soit du plus facile au plus complexe à cracker). Notons que la méthode AES parfois utilisée par certains logiciels pour interdire l'accès au contenu du ZIP n'est pas prise en charge par fcrackzip. Ne vous inquiétez pas, car la vieille méthode ZipCrypto est toujours la plus utilisée. Si vous devez protéger vos propres archives ZIP, le cryptage ZipCrypto est à bannir, car beaucoup moins sûr que l'AES-256 par exemple.

ATTAQUE PAR DICTIONNAIRE OU "BRUTE FORCE"

CRACKEZ AVEC VOTRE CARTE GRAPHIQUE

Autre méthode : utilisez le logiciel **cRARk**. Avec celui-ci, vous tentez d'outrepasser les mots de passe d'une archive RAR ou 7z en exploitant la puissance du GPU de votre carte graphique. Le soft attaque en brute force le chiffrement AES-256 des fichiers RAR et 7z. Pour l'utiliser, vérifiez que votre carte graphique est compatible avec CUDA de nVidia ou OpenCL de AMD/ATI.

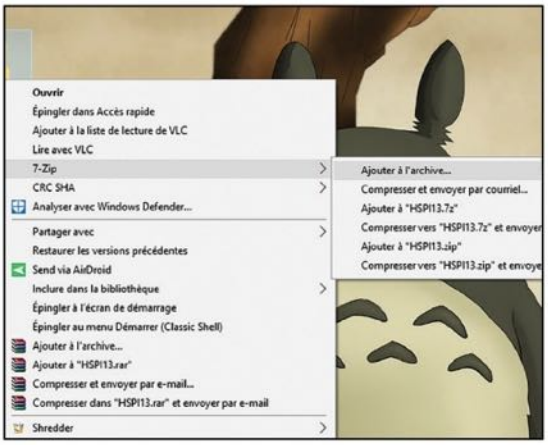


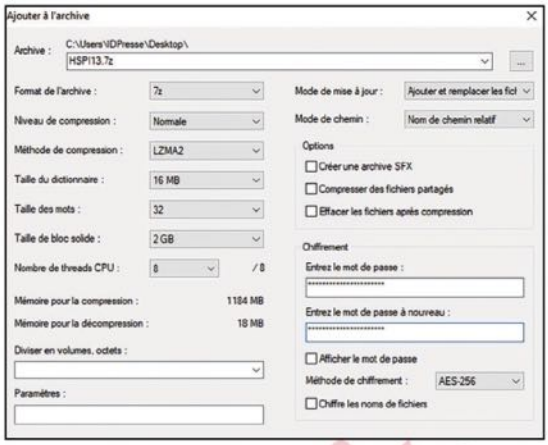
PROTÉGEZ PUIS CRACKEZ UNE ARCHIVE ZIP

Empêcher l'accès à une archive ZIP via un mot de passe prend quelques secondes. Pour cracker le sésame, c'est une autre paire de manches... Démonstration.

7ZIP **INFOS [7-ZIP]**
Où le trouver ? [**www.7-zip.org**] Difficulté : ☠☠☠

TUTO





01 › NOTRE LOGICIEL

Pour interdire l'ouverture d'une archive, nous allons utiliser le logiciel gratuit 7-Zip. Il permet de créer des fichiers ZIP, TAR, WIM, etc. Il dispose en plus de son propre format très performant, le 7Z. Téléchargez ce logiciel en fonction de votre système d'exploitation (32 ou 64 bits). Après avoir choisi un dossier, un fichier ou un groupe de fichiers, faites un clic droit puis dans le menu contextuel, sélectionnez **7-Zip** > **Ajouter à l'archive...**

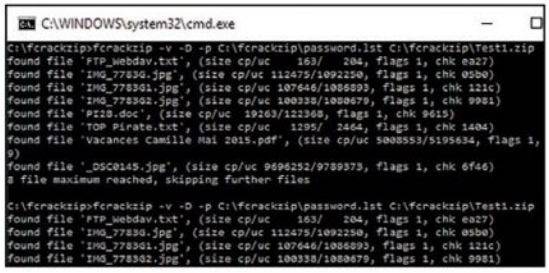
02 › LE CHIFFREMENT

Laissez par défaut le format, le niveau de compression et les autres données techniques. Dans la partie **Cryptage**, entrez votre mot de passe (sans caractères accentués). Notez que, selon le format d'archives choisi, vous pouvez changer la **Méthode de chiffrement**. Restez sur l'**AES-256**, plus sûr, mais attention, la version Windows de **fcrackzip** ne peut que retrouver des mots de passe chiffrés en **ZipCrypto**. Mieux vaut utiliser cette méthode très répandue si vous voulez vous amuser (cf. page suivante).

INFOS [FCRACKZIP]

Où le trouver ? [https://goo.gl/ZjZR4q] Difficulté : ☠☠☠

TUTO



03 › METTRE EN PLACE

Dézippez le contenu téléchargé dans un dossier **fcrackzip** à placer dans **C:**. Pour la méthode par dictionnaire, il faut une liste de mots de passe. Cherchez ici en version gratuite **https://goo.gl/rSwCMv**. Pour des dictionnaires en français, c'est ici : **http://goo.gl/gEbEss**. Mettez le dico au format LST (**password.lst**) dans le même dossier que le programme et vos fichiers de test. Attention, les entrées doivent être organisées : un mot de passe par ligne !

04 › ATTAQUE PAR DICTIONNAIRE

Maintenez la pression sur la touche **Maj** et faites un clic droit dans le dossier **fcrackzip**. Sélectionnez **Ouvrir une fenêtre de commandes ici**. Tapez **fcrackzip -v -D -p C:\fcrackzip\password.lst C:\fcrackzip\Test1.zip**. **-v** donne plus d'explications pendant le processus, **-D** spécifie l'attaque par dictionnaire et **-p** montre le chemin du fichier contenant les mots de passe potentiels. Pour **Test1.zip**, rien ne se passe ! En effet, **toto** n'est pas dans le dico... Essayons avec **Test2.zip**.

```
found file 'PI28.doc', (size cp/uc 19263/122368,
found file 'TOP Pirate.txt', (size cp/uc 1295/
found file 'Vacances Camille Mai 2015.pdf', (size
found file '_DSC0145.jpg', (size cp/uc 9696252/97
8 file maximum reached, skipping further files
possible pw found: jesus ()

C:\fcrackzip>fcrackzip -v -D -p C:\fcrackzip\pass
found file 'FTP_Webdav.txt', (size cp/uc 163/
found file 'IMG_7783G.jpg', (size cp/uc 112475/10
found file 'IMG_7783G1.jpg', (size cp/uc 107646/1
found file 'IMG_7783G2.jpg', (size cp/uc 100338/1
found file 'PI28.doc', (size cp/uc 19263/122368,
found file 'TOP Pirate.txt', (size cp/uc 1295/
```

```
found file 'IMG_7783G.jpg', (size cp/uc 1
found file 'IMG_7783G1.jpg', (size cp/uc
found file 'IMG_7783G2.jpg', (size cp/uc
found file 'PI28.doc', (size cp/uc 19263
found file 'TOP Pirate.txt', (size cp/uc
found file 'Vacances Camille Mai 2015.pdf
, chk f5e9)
found file '_DSC0145.jpg', (size cp/uc 96
8 file maximum reached, skipping further
possible pw found: delopa ()
checking pw lvvbjj
```

05 › SECONDE TENTATIVE

Tapez **fcrackzip -v -D -p C:\fcrackzip\password.lst C:\fcrackzip\Test2.zip** et validez. Le logiciel trouve **jesus !** Pour **delopa**, une attaque par dictionnaire ne fonctionne pas. Il faut la méthode brute force. Comme nous ne sommes pas censés savoir le mot de passe, nous allons essayer toutes les suites de caractères minuscules. Nous pouvons aussi tenter de définir une longueur minimale et maximale. La plupart des mots de passe choisis « à la va-vite » font entre 4 et 8 caractères. Nous allons donc taper **fcrackzip –v –c a -l 4-8 C:\fcrackzip\Test3.zip**

06 › LA MÉTHODE BRUTE FORCE

Ici, le switch **-c** suivi de **a** montre que nous ne recherchons que des caractères minuscules. Il faudrait mettre **-c aA1!** pour chercher en plus les majuscules, les chiffres et les caractères spéciaux. Enfin, **-l** (un L minuscule) permet de spécifier la longueur. Au bout de 12 secondes, **delopa** est découvert ! fcrackzip continuera la recherche à cause d'une marge d'erreur de 0,4 % causée par la structure de certains fichiers ZIP. Inutile de faire l'essai avec **Test4.zip,** car, vous l'aurez compris, le temps de calcul serait trop long. Il faudrait un super calculateur.

TABLES ARC-EN-CIEL : LE CRACK INTELLIGENT

Au lieu de tenter de cracker un mot de passe «à l'ancienne», il existe une méthode plus puissante : les rainbow tables. Il s'agit de chaînes de mots de passe «prémâchées» permettant d'accélérer le processus. Voyons comment cela fonctionne...

Lorsque vous possédez le hash d'un mot de passe et que vous voulez retrouver le sésame, il existe plusieurs méthodes. La première consiste à regarder sur des bases de données comme **https://crackstation.net** ou **https://hashkiller.co.uk**, si le hash n'est pas déjà connu ou se réfère à un mot de passe tellement facile qu'il est connu comme le loup blanc (**ab4f63f9ac65152575886860dde480a1** pour **azerty** en MD5 par exemple). La seconde solution consiste à attaquer par « dictionnaire » en essayant des millions de mots issus d'un fichier texte (par exemple **nirvana**, **Windows** ou **Porsche911** ont de grandes chances de s'y trouver). Lorsque cela échoue, il reste encore le « brute force » : essayer des combinaisons de caractères plus ou moins longs en espérant glaner des indices permettant de gagner du temps. On peut par exemple tenter d'en savoir plus sur les dates de naissance de la personne qui a créé le mot de passe.

UNE NOUVELLE TECHNIQUE

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. 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

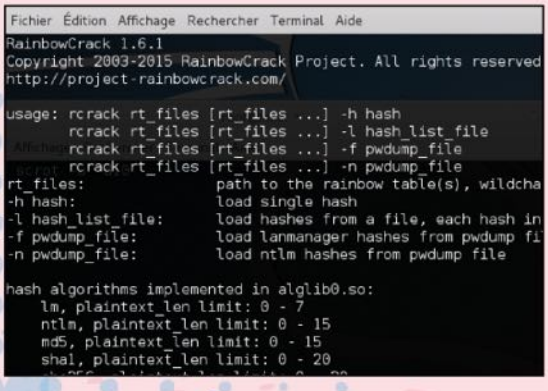
force : https://goo.gl/N1MNBx. L'inconvénient, c'est qu'il vous faut générer ces fichiers rainbow tables en amont. En fonction de la complexité du mot de passe que vous souhaitez retrouver ces derniers peuvent peser de 500 Mo à plus d'un To ! Il faut donc de la place sur un disque dur et beaucoup de temps pour les générer (comptez 3 heures pour 1 Go avec un PC standard). Heureusement, vous pouvez télécharger ces tables, les acheter et bien sûr les garder pour d'autres tentatives de crackage si vous avez eu le courage de les générer vous même. Nous allons donc voir comment générer ces tables et les utiliser avec RainbowCrack, un logiciel qui en plus d'être compatible avec un grand nombre de hash, supporte le multicoeur et l'accélération graphique (le CUDA de nVidia ou le OpenCL de ATI/AMD). Pas de jaloux pour cette démonstration puisque RainbowCrack est disponible sur Windows et Linux.

GÉNÉREZ VOTRE TABLE ARC-EN-CIEL

INFOS [RAINBOWCRACK]

Où le trouver ? [**http://project-rainbowcrack.com**] Difficulté : ☠☠☠

TUTO

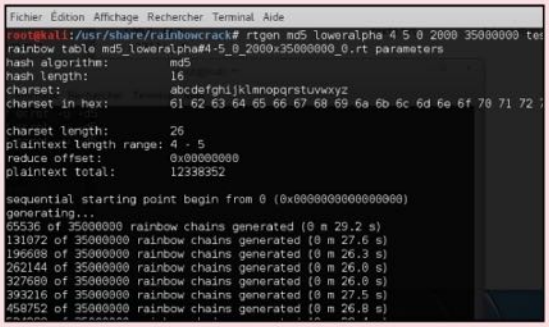


01 › OÙ TROUVER LE LOGICIEL ?

Sous Kali Linux, RainbowCrack est installé d'office. Sous d'autres distributions ou sous Windows, suivez notre lien pour le télécharger. Allez dans le menu **Applications** puis **Attaques de mots de passe** pour trouver le logiciel. Dans la fenêtre, vous verrez comment doivent être organisées les lignes de commandes ainsi que les limites pour les longueurs de mots de passe (de 0 à 15 pour le MD5, 0 à 20 pour le SHA1, etc.)

02 › PREMIÈRE TABLE

Comme nous avons vu que les fichiers peuvent peser plusieurs Go, nous allons commencer léger et créer un « set » de 6 rainbow tables. Supposons que nous cherchions un mot de passe à partir d'un hash MD5 et que nous sommes sûrs que ce dernier fait entre 4 et 7 caractères tout en minuscules. Nous allons d'abord taper **cd /usr/share/rainbowcrack** pour aller dans le répertoire de destination puis : **rtgen md5 loweralpha 4 7 0 2000 35000000 test** puis **Entrée**.



03 › LES DÉCLINAISONS

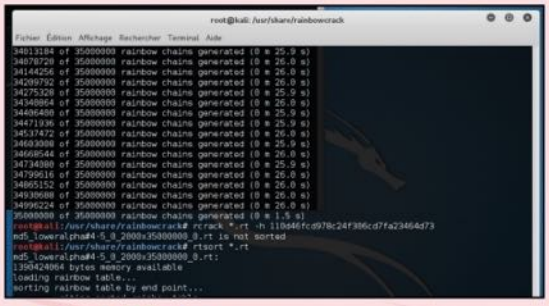
Le 0 correspond au numéro d'index. Si l'index change, la fonction de réduction aussi. 2000 correspond à la longueur de la chaîne. Plus elle est grande, plus la table contient de mots de passe, mais plus elle sera longue à générer. Enfin, 35000000 se rapporte au nombre de chaînes (les lignes du tableau). Comme chaque ligne fait 16 bits, on peut savoir combien pèsera la table en faisant 35 000 000x16 = 560 000 000 bits. Environ 560 Mo par table donc. Nous allons ensuite taper :

rtgen md5 loweralpha 4 7 1 2000 35000000 test

rtgen md5 loweralpha 4 7 2 2000 35000000 test

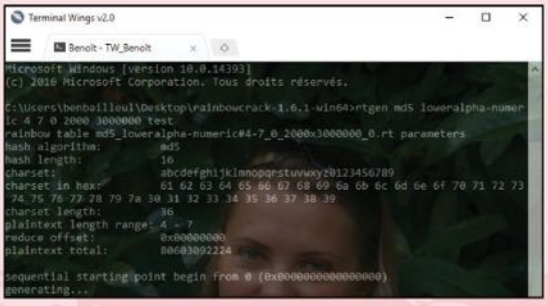
04 › NOM ET EMPLACEMENT

Continuez jusqu'à l'index **5** ce qui nous fera 6 tables en tout appelées **md5_loweralpha #3-7_0_2000x80000_test.rt**, etc. Ces opérations vont prendre énormément de temps alors, imaginez si nous prenions en compte les mots de passe mixtes (voir le fichier **charset.txt** pour changer le paramètre **loweralpha**) de 3 à 15 caractères ! Vous comprenez maintenant pourquoi certaines tables font plus de 1 To. L'avantage, c'est que cette technique va vous faire gagner des heures, des jours et même des années !



05 › LE TRI

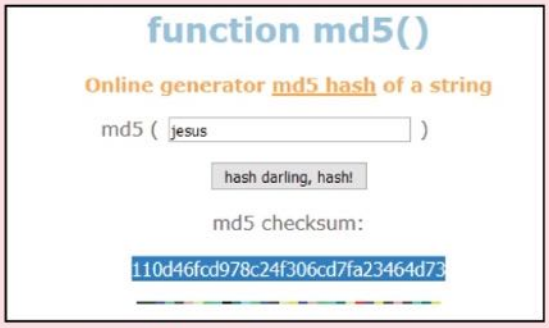
Une fois vos tables générées, il va falloir encore faire une opération pour les rendre exploitables : c'est le tri. La commande rtsort va « retourner » la table pour commencer la recherche par la dernière empreinte et donc remonter le fil de la table (voir notre schéma). Toujours dans **/usr/share/rainbowcrack**, faites **rtsort *.rt** pour trier vos 6 tables qui se trouvent dans le dossier de travail. N'interrompez surtout pas le processus !



06 › ET SOUS WINDOWS ?

Sous Windows, RainbowCrack s'opère en ligne de commande lorsqu'il s'agit de générer et trier les tables. Pour plus de confort, nous avons choisi d'utiliser le logiciel Terminal Wings (www.phrozensoft.com). L'avantage de ce dernier réside dans la gestion d'un profil avec un répertoire d'usage. Si vous ne souhaitez pas l'utiliser, restez appuyé sur **Shift** (ou **Maj**), faites un clic droit dans le dossier de RainbowCrack faites **Ouvrir une fenêtre de commande ici**. Au niveau des commandes, c'est exactement la même chose.

CRACKEZ AVEC VOTRE TABLE



01› PRÉPARATIFS

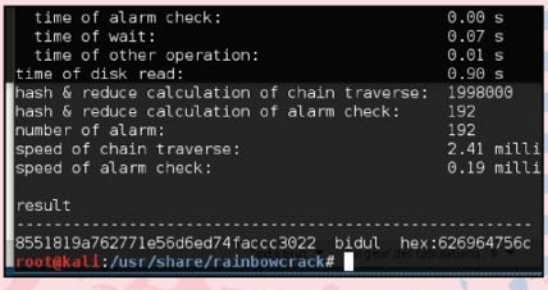
Votre belle rainbow table est prête ? Il est temps de l'utiliser ! N'oubliez pas que dans notre exemple, nous avons choisi de créer une table permettant de cracker un mot de passe hashé en MD5 de 4 à 7 caractères de long uniquement constitué de minuscules. Allons sur **www.md5.cz** et notons les hash correspondant à **0000**, **jesus** (vous avez appris la bonne nouvelle ? Il est ressuscité !) et **bidul**. Bien sûr, ces mots de passe sont très faibles, mais avec la table que nous avons générée il ne faut pas s'attendre à des miracles

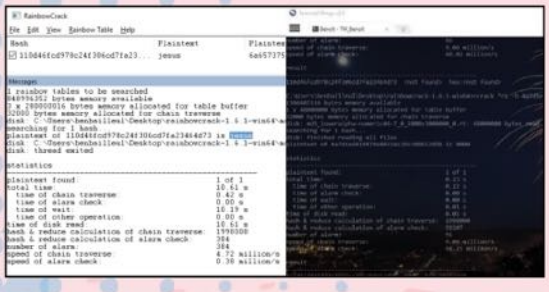
02› CRACK !

Depuis le répertoire de travail, tapez : **rcrack *.rt -h 110d46fcd978c24f306cd7fa23464d73**

Ce hash est celui correspondant au sésame **jesus**. Si vous en avez plusieurs, mettez-les dans un fichier TXT (toujours dans le même répertoire) et faites **rcrack *.rt -l hash.txt**

L'argument ***.rt** va prendre en compte toutes les tables dans le dossier de travail, faites donc attention si vous en avez plusieurs (rangez-les dans des dossiers séparés).





03› AVANTAGES ET LIMITES

En fonction de différents paramètres (taille du mot de passe, de la table, puissance du PC, etc.), le processus peut prendre longtemps, mais rien de comparable avec le brute force. **00000**, **jesus** et **bidul** ont été trouvés en quelques secondes (le résultat s'affiche en bas avec l'équivalent hexadécimal du mot de passe (c'est important pour les caractères accentués, voir notre encadré). N'espérez pas des résultats aussi rapides avec un sésame comme **Tf5Jç5d_cc23dx^$** par exemple. Mais avec les rainbow tables, vous avez une chance. Avec le brute force... aucune.

04› ET SOUS WINDOWS ?

Sous Windows, la partie « crack » peut s'effectuer en ligne de commande ou via une interface graphique (GUI). Notez qu'il est possible de tirer parti des accélérateurs graphiques CUDA ou OpenCL. Si cela ne fonctionne pas avec votre matériel, utilisez simplement **rcrack_gui.exe**, allez dans **File** puis **Add Hashes...** pour coller votre hash. Dans le menu **Rainbow Table**, allez dans **Search Rainbow Table...** pour choisir votre table. Les calculs commencent immédiatement.

KALI LINUX : HAIL HYDRA !

Hydra c'est bien sûr une organisation ennemie jurée de Captain America, mais c'est aussi un redoutable logiciel qui peut cracker du mot de passe en ligne. Pour cela, il nous faudra compter sur un dictionnaire de mots de passe et d'un peu de chance...

Nous vous mettons souvent en garde sur l'importance du choix de vos mots de passe et ce n'est pas pour rien ! Avec très peu de connaissances en informatique, un pirate à la petite semaine pourrait faire de votre vie un enfer (usurpation d'identité, défaçage de votre site, vol de données, etc.) Car on utilise des mots de passe tellement souvent sur Internet que certains utilisateurs font l'erreur de choisir le même partout. C'est bien sûr une chose à éviter, car il suffit qu'un seul de vos comptes se fasse pirater pour que les autres ne tombent comme des dominos. De même, n'utilisez pas de mots de passe permettant de deviner les autres (kiki75, kikiPaname, TheKiKidu75, etc.) ou faciles à deviner.

NE VOUS CROYEZ PAS À L'ABRI !

Car avec les réseaux sociaux il est facile de connaître des éléments sur vous : date de naissance de vos enfants, séries, sports ou parti politique préférés, etc. Si vous pensez que **MélenchonPSG9698** est solide, vous avez tort... Mais ce qui nous intéresse ici c'est la méthode par dictionnaire. À la différence de nos précédentes démonstrations sur les mots de passe, Hydra fonctionne en ligne. Alors que nous devions auparavant avoir un hash en main pour tenter de cracker le mot de passe correspondant, ce n'est pas le cas ici...

DES VERSIONS POUR TOUT LE MONDE !

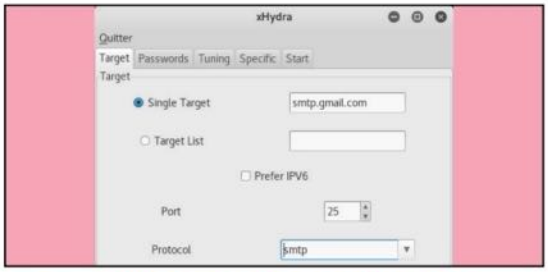
Si vous n'avez pas envie d'installer ou d'utiliser Kali Linux, il existe aussi une version Windows appelée THC-Hydra que vous trouverez ici : **www.thc.org/thc-hydra**. Attention, votre navigateur et votre antivirus ne vont pas aimer...

INFOS [KALI LINUX]
Où le trouver ? [www.kali.org] Difficulté : ☠☠☠

TUTO

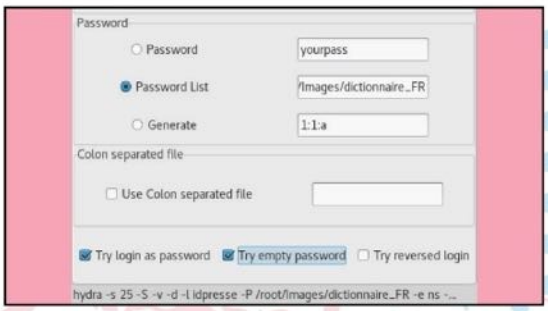
01 › XHYDRA DANS KALI LINUX

Nous ne reviendrons pas sur la mise en place de Kali Linux puisque nous avons vu plusieurs fois que vous pouviez l'installer, l'utiliser depuis un Live CD ou une virtualisation. xHydra est l'interface graphique du logiciel Hydra et vous la trouverez dans le menu **Applications** > **Attaques de Mots de Passe** > **Les Attaques en Ligne** > **hydra-gtk**.



02 › ONGLET TARGET (CIBLE)

Dans le premier champ vous devrez taper l'adresse IP ou l'URL de la cible. Si vous avez plusieurs cibles, vous pouvez en faire une liste au format TXT ou LST et spécifier l'emplacement. En dessous, vous devez spécifier le protocole et le port d'écoute. Chaque protocole a un ou plusieurs ports d'écoute habituels (21 pour le FTP, 22 pour le SSH, etc.) Hydra permet d'attaquer une cinquantaine de protocoles ou bases de données : Telnet, FTP, HTTP, HTTPS, IRC, VNC, SSH, SMTP, etc. Pour être sûr que vous ne donnez pas des coups d'épée dans l'eau, vous pouvez scanner les ports d'une cible avec le logiciel Nmap, inclus aussi dans Kali.



03 › ONGLET PASSWORD

Nom d'utilisateur de la cible, comme pour le précédent onglet, vous pouvez dresser la liste des Usernames potentiels... Cochez la première case si vous désirez que la liste revienne sur elle même en cas d'échec et cochez la deuxième si vous n'avez pas besoin de nom d'utilisateur. Si vous avez votre mot de passe mais que vous cherchez votre identifiant, entrez le sésame dans le premier champ. Si vous avez l'identifiant mais pas le mot de passe, vous pouvez spécifier une liste de mots de passe que l'on appelle dictionnaire au format TXT ou LST. Vous trouverez des exemples de dicos dans le dossier **usr/share/wordlists**.

04 › ONGLETS TUNING & SPECIFIC

En bas, vous trouverez des cases à cocher pour essayer d'utiliser l'identifiant comme mot de passe, un mot de passe vide ou inverser le mot de passe et l'identifiant. Cochez les trois. Les deux onglets suivants permettent moult autres réglages ou paramétrages : nombre de threads, comportement à adopter en cas de succès (continuer sur d'autres tâches ou s'arrêter), utilisation d'un proxy, etc. Bien sûr, le dernier onglet va démarrer le processus. Cliquez sur **Start** en bas lorsque vous êtes sûr de vos réglages.

GESTIONNAIRE DE MOTS DE PASSE : TROUVEZ CELUI QUI VOUS CORRESPOND

Xecrets, Enpass, Dashlane, LastPass... l'offre de solutions pour mettre à l'abri vos mots de passe est pléthorique, et ce sur toutes les plateformes. Voici les critères à prendre en compte pour choisir l'utilitaire le plus adapté à vos usages et à votre porte-monnaie.

Mettre de côté vos sésames pour les retrouver plus tard sur un autre appareil, en générer de nouveau plus « safe », vous en faciliter l'utilisation depuis le Web... Bien que se rapprochant du point de vue des fonctionnalités, les gestionnaires de mots de passe ne s'appréhendent pas tous de la même manière. KeePass, gratuit, open-source et considéré comme le plus sécurisé (labellisé par l'Agence Nationale de la sécurité des systèmes d'information), demande du temps avant d'être complètement apprivoisé. La synchronisation entre vos appareils nécessite

LES GESTIONNAIRES

	LastPass **** LastPass www.lastpass.com/fr
Prix	Gratuit, version premium à 12 € par an
Type de client	Extension de navigation
Compatibilité	Windows, Mac, Linux, Android, iOS et Windows Phone
Stockage des données	Local
Synchronisation appareils	Oui et gratuite
Open source	Non
Fonctionnalités premium	Mot de passe pour vos applis, plusieurs utilisateurs sur un même compte, double authentification...

de passer par différents plugins et manipulations fastidieuses pour un utilisateur débutant.

DES COMPROMIS À FAIRE

Si KeePass est la solution la plus sécurisée, son interface « old-school » en rebutera plus d'un. Ces mêmes utilisateurs se tourneront vers les alternatives qui se configurent en trois clics. Dashlane, par exemple, propose une ergonomie bien pensée qui facilite l'enregistrement des mots de passe et l'appel de ceux-ci lorsque vous surfez sur le Web. C'est en revanche une solution loin d'être parfaite : elle est payante si vous comptez synchroniser vos mots de passe entre différents appareils. De plus, bien que chiffrés, vos sésames transitent via le service en ligne et le client est lui même connecté. À contrario de KeePass qui fonctionne totalement en « offline ». Pour allier confort d'utilisation et protection de vos mots de passe, nous vous conseillons d'opter pour LastPass. Gratuit, jouissant d'une interface facile à appréhender et stockant les mots de passe directement sur votre bécane... vous n'aurez aucun mal à synchroniser vos mots de passe entre vos appareils. Si jamais c'est le cas, on vous explique comment le configurer plus loin.

DE MOTS DE PASSE À LA LOUPE

Dashlane www.dashlane.com/fr	Enpass www.enpass.io	Keepass http://keepass.info	Password Safe https://pwsafe.org
Gratuit, version premium à 3,33 € par mois	Gratuit, application à 9,62 €	Gratuit	Gratuit
Logiciel et extension de navigation	Logiciel	Logiciel	Logiciel
Windows, Mac, Android et iOS	Windows, Mac, Linux, Android, iOS, BlackBerry et Windows Phone	Windows, Mac, Linux, Android, iOS, BlackBerry et Windows Phone	Windows et Android
Local et en ligne	Local	Local	Local
Oui, mais en version premium	Oui, mais limitée à 20 mots de passe dans l'appli	Oui	Oui
Non	Non	Oui	Oui
Synchronisation entre tous vos appareils, sauvegarde sur le Cloud de vos mots de passe, double authentification...	Nombre de mots de passe illimité sur l'application	X	X

ENREGISTREZ ET SYNCHRONISEZ vos MOTS DE PASSE

Remplissage automatique des formulaires, générateur de mots de passe sécurisés, enregistrement de ceux que vous utilisez, synchronisation avec tous vos appareils... LastPass est un gestionnaire de mots de passe très complet.

Solution non limitée dans sa version gratuite, LastPass est certainement le gestionnaire de mots de passe le plus facile à prendre en main. Rendez-vous sur le site puis installez l'extension de navigateur compatible avec celui que vous utilisez (Chrome ou Firefox). Pour l'utiliser sur mobile ou tablette, téléchargez l'appli en rapport avec votre OS (Android, iOS ou Windows Phone).

Une fois connecté, vous créez un mot de passe maître, gardien de tous les autres. Ne le perdez surtout pas où vous n'aurez plus accès au coffre-fort à mots de passe. Pour enregistrer des mots de passe : ajoutez-les directement dans le coffre-fort comme nous vous le montrons ou authentifiez-vous sur un site de votre choix. Avec cette seconde option, LastPass vous souffle un mot de passe sécurisé et vous propose de le retenir... à votre place.

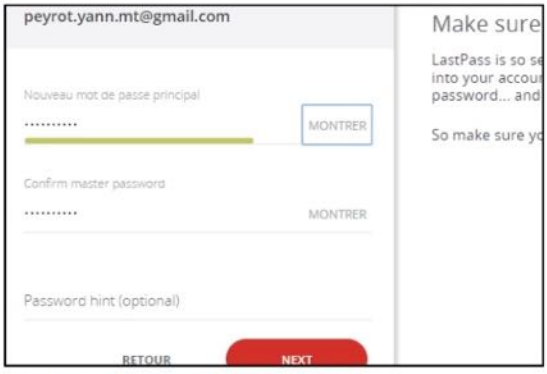
Ainsi à la prochaine connexion à ce même site, vous cliquez sur l'icône LastPass dans les emplacements réservés au mot de passe et à l'identifiant. Les champs sont automatiquement remplis, vous voilà connecté.

Une fois sur mobile, une simple connexion à votre compte (et un petit paramétrage comme expliqué ci-contre) permet de retrouver tous ses mots de passe. Facile !

LastPass **** INFOS [LASTPASS]

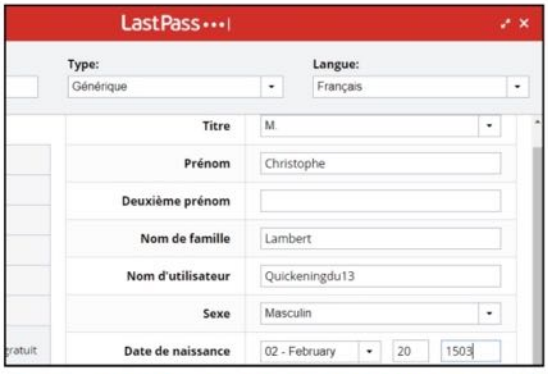
Où le trouver ? [www.lastpass.com/fr] Difficulté :

TUTO



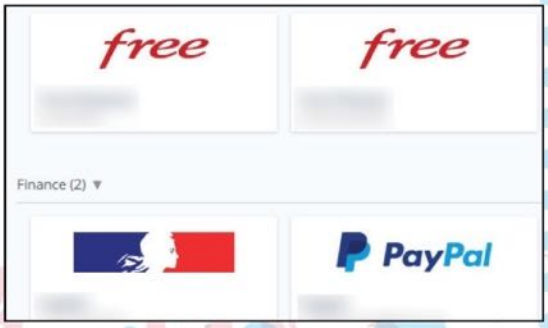
01 › RETENIR SES IDENTIFIANTS

Installez l'extension sur votre navigateur (Firefox ou Chrome). LastPass demande de créer un mot de passe maître déverrouillant l'accès aux mots de passe enregistrés. Attention : il n'existe aucun moyen de le récupérer si vous l'oubliez. Ensuite, cliquez sur **Ajouter un site** pour remplir la fiche correspondant à un site, avec identifiant et mot de passe. Faites cela pour tous vos comptes.



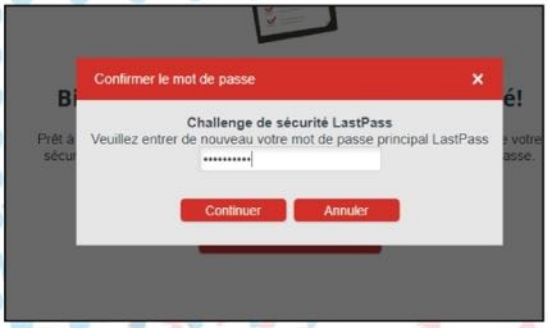
02 › REMPLIR LES FORMULAIRES

Dans **Formulaires**, cliquez sur **Add Form Fill** en bas à droite. Sauvegardez les informations communément demandées lors du remplissage d'un formulaire pour ne plus avoir à les retaper. Lorsque le cas se présentera, une petite icône LastPass apparaîtra dans chaque champ. Cliquez dessus pour choisir la bonne entrée.



03 SYNCHRONISER VOS APPAREILS

Ouvrez l'application mobile LastPass, connectez-vous, pressez les trois traits parallèles en haut à gauche pour aller dans **Réglages** puis **Remplissage d'application**. Cochez **Remplir les identifiants de connexion dans les autres applications** puis suivez les instructions qui s'affichent à l'écran pour finaliser la synchronisation.



04 › RENFORCER SES MOTS DE PASSE

Sur PC, dans LastPass, cliquez sur **Challenge de sécurité** (le bouclier sur le menu latéral). Une page Web s'ouvre, sur laquelle vous devez vous reconnecter à votre compte LastPass avant de valider avec **Voir mon score**. Vos mots de passe sont analysés, et le service vous indiquera si certains devraient être changés (trop faciles à deviner...) en vous accompagnant dans la marche à suivre.

01# Générer un mot de passe solide

→ Avec SafePasswd

Vous le savez maintenant : les mots de passe les plus sécurisés sont ceux qui combinent caractères spéciaux, chiffres, lettres majuscules et minuscules. Plus ils sont longs, plus ils sont difficiles à décoder. Ce service vous aide à élaborer un mot de passe solide. Via le menu déroulant, sélectionnez **All Characters**, cochez **Use UpperCase and LowerCase** et définissez le nombre de caractères avec **Length**. Validez la création du nouveau mot de passe solide avec **New Password**.

Difficulté :

Lien : **safepasswd.com**

02# Créer un support de réinitialisation du mot de passe Windows → Avec Windows

Vous avez peur d'oublier votre mot de passe Windows ? Toutes les versions de l'OS permettent de créer une clé à stocker sur un support amovible. Appuyez sur **Ctrl + Alt + Suppr** pour avoir accès au menu **Modifier un mot de passe** puis **Créer un disque de réinitialisation de mot de passe**. Insérez un périphérique USB et choisissez-le dans la liste. Tapez ensuite votre mot de passe actuel et laissez Windows s'occuper de placer le fichier **userkey.psw** sur la clé. Faites un essai en pressant **Win + L**. Votre session sera verrouillée. Tapez un mauvais sésame, validez et choisissez **Réinitialiser le mot de passe**. Connectez alors le périphérique contenant le fichier sus-nommé.

Difficulté :

03# Vérifier la solidité d'un mot de passe

→ Avec How Secure is my Password

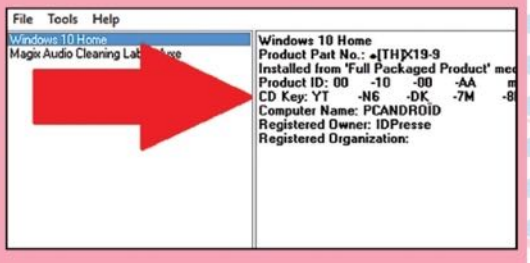
Ce site permet de savoir si votre mot de passe est suffisamment solide. Il suffit de taper votre mot de passe pour voir immédiatement si ce dernier remplit les critères basiques de sécurité. Vous pourrez même savoir combien de temps il faudrait aux meilleurs ordinateurs pour arriver à le cracker. Quelle que soit la solidité du sésame, le site vous donnera des conseils pour l'améliorer. Le site a beau être sponsorisé par le gestionnaire de mot de passe Dashlane, il reste très utile.

Difficulté : Lien : **howsecureismypassword.net**

04# Retrouver sa clé Windows

→ Avec Keyfinder

Sur le site de KeyFinder, cliquez sur **Download** en dessous de **Free** pour télécharger la version gratuite du logiciel. Ne vous inquiétez pas : pour ce qui nous intéresse ici, elle est amplement suffisante. Après avoir installé KeyFinder, il vous suffit de



lancer le programme pour voir s'afficher votre clé Windows, à droite de **CD KEY**. Notez-la précieusement et conservez-la dans un endroit sûr en cas de besoin.

Difficulté :

Lien : **magicaljellybean.com/keyfinder**

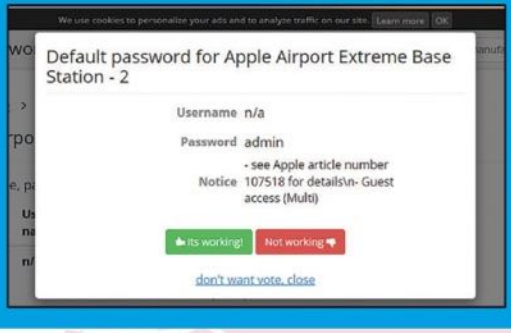
05# Retrouver le mot de passe par défaut

→ Avec Default Password

Les box, modems ou tout autre appareil de ce genre sont souvent livrés avec un couple identifiant/mot de passe défini en usine. Et si vous n'avez pas pris la peine de le changer, vous vous retrouvez bien embêté le jour où vous en avez besoin. Le site DefaultPassword recense de très nombreux modèles. Une fois trouvé le vôtre, cliquez sur **show me !** pour afficher identifiant et mot de passe.

Difficulté :

Lien : **default-password.info**



06# Cracker des mots de passe Wi-Fi

→ Avec Wibr+

Wibr+, appli bannie du Google Play Store, propose de casser le mot de passe d'un réseau Wi-Fi pour y pénétrer. Bien sûr, nous présentons cette appli pour tester votre propre réseau et aussi pour vous montrer comment s'y prennent les pirates pour accéder à votre réseau et réaliser tout un tas de méfaits (téléchargement illégal, attaque DdoS...). Très complète pour une appli mobile, Wibr+ propose 2 types d'attaques : dictionnaire et brute force.

Difficulté :

Lien : **auradesign.cz/android/wibrplus.apk**

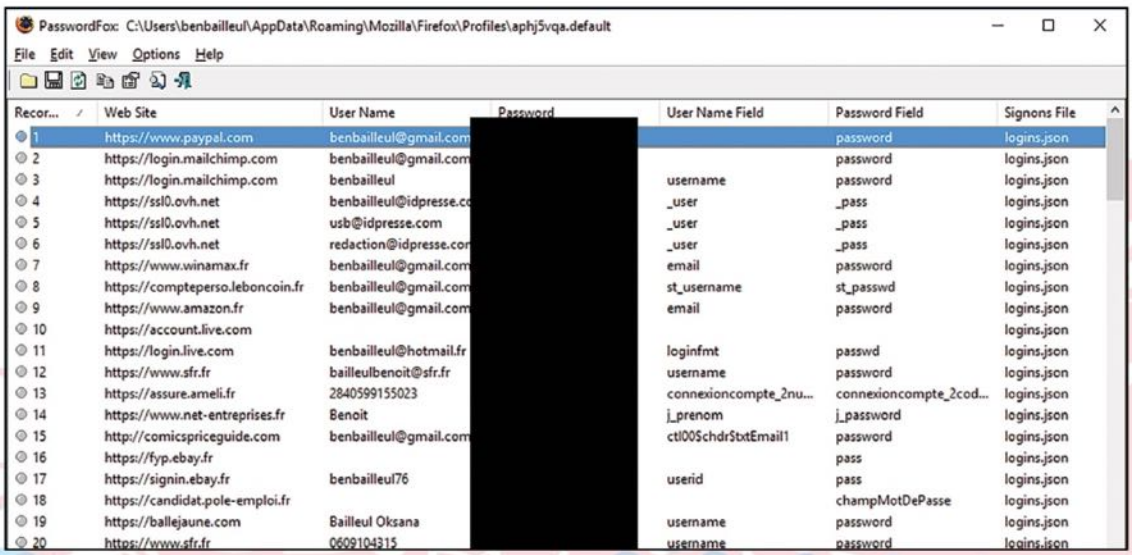
07# Récupérer les mots de passe de vos navigateurs

→ Avec les outils de Nir Sofer

Besoin de récupérer les identifiants/mots de passe de vos navigateurs ? C'est facile avec les outils de Nir Sofer ! Ce programmeur très consciencieux propose des logiciels sains : la plupart de ses produits ne nécessiteront aucune installation et pourront se loger sur une clé USB sans laisser de traces dans la base de registre de votre ordinateur. Avec PasswordFox, ChromePass et IE PassView (jusqu'à la version 8) vous pourrez récupérer vos sésames pour les transférer ou les sauvegarder en cas de problème.

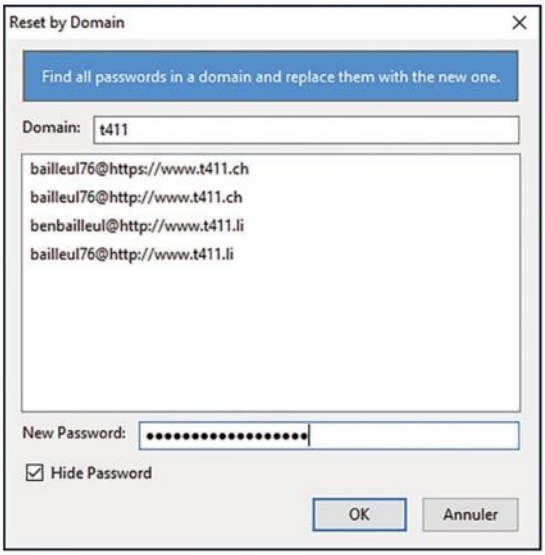
Difficulté :

Lien : **nirsoft.net/password_recovery_tools.html**



08# Changez tous les mots de passe enregistrés dans Firefox → Avec Mass Password Reset

Nous vous mettons souvent en garde contre la possibilité d'enregistrer vos mots de passe d'accès vers sites et services dans Firefox (ou n'importe quel autre navigateur), mais il faut bien se rendre à l'évidence : tout le monde le fait ! Pour éviter les problèmes, vous souhaitez changer vos mots de passe le plus souvent possible, mais le navigateur n'est pas très à l'aise avec cette fonction (redondance des mots passe, réenregistrement pas pratique, etc.). Pour vous sortir du pétrin, nous vous présentons Mass Password Reset un plugin qui vous dressera la liste de vos identifiants pour les changer le plus naturellement du monde et de façon groupée.



Difficulté : ☠☠☠

Lien : **http://tinyurl.com/6987lac**

09# Être sûr de taper le bon mot de passe → Avec UnicornPass

Vous n'êtes pas sûr de saisir le bon mot de passe lorsque vous remplissez un formulaire d'authentification ? Soit vous tentez la connexion quitte à vous prendre un vent, soit vous effacez tout pour retaper le sésame en grommelant... Avec UnicornPass, vous ne pourrez plus vous tromper. Cette extension Firefox va colorer le champ en se basant sur le hash du mot de passe. Si les couleurs vous sont étrangères, c'est que vous avez dû faire une faute de frappe... Astucieux et sécurisé ! Les utilisateurs de Chrome peuvent utiliser le script **UnicornPass.user.js** avec **TamperMonkey** (https://github.com/carmebar/unicornpass).

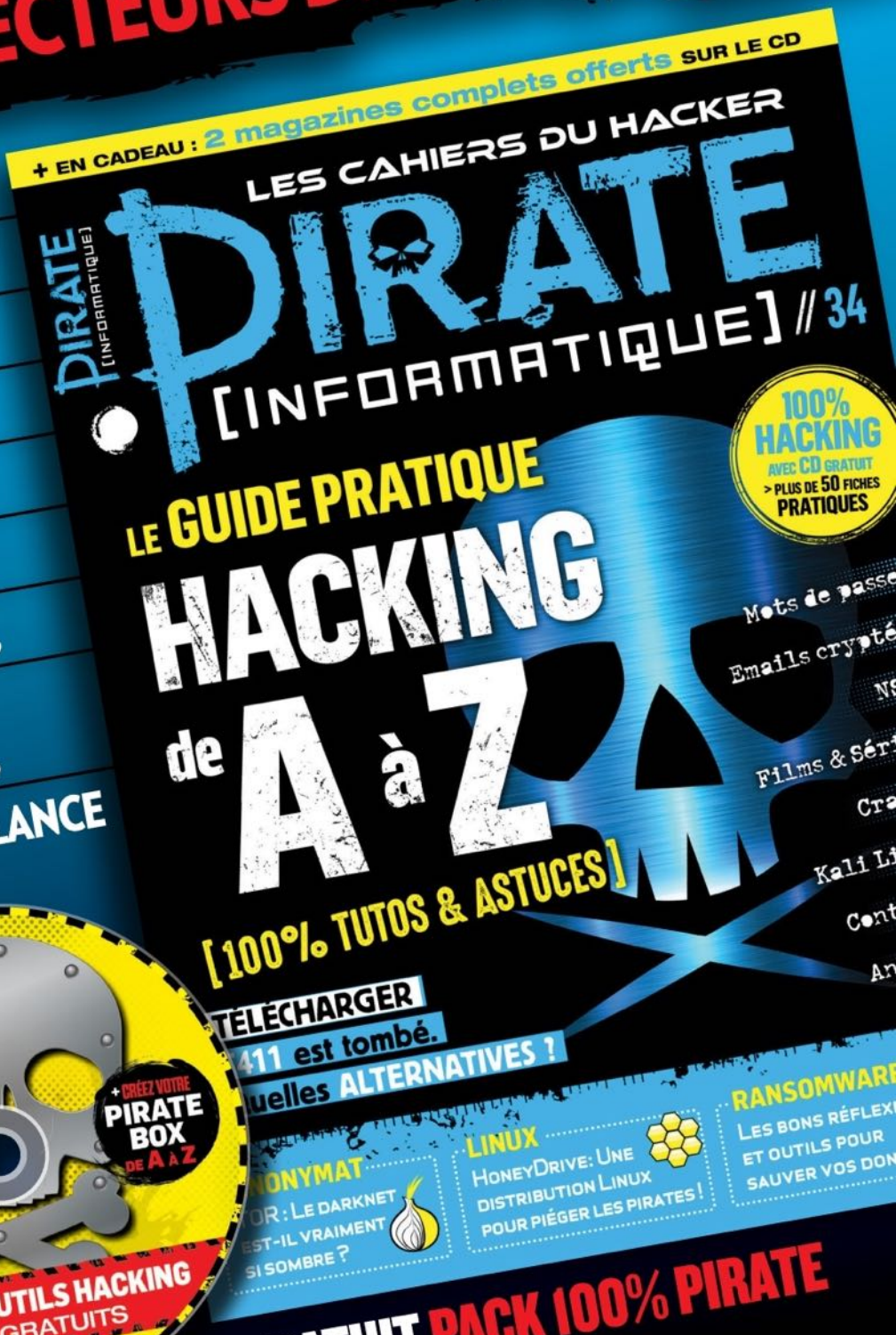
Difficulté : ☠☠☠

Lien : **goo.gl/6xaT5a**

CHEZ VOTRE MARCHAND DE JOURNAUX

LES PIRATES CRYPTENT, NOS LECTEURS DÉCRYPTENT !

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

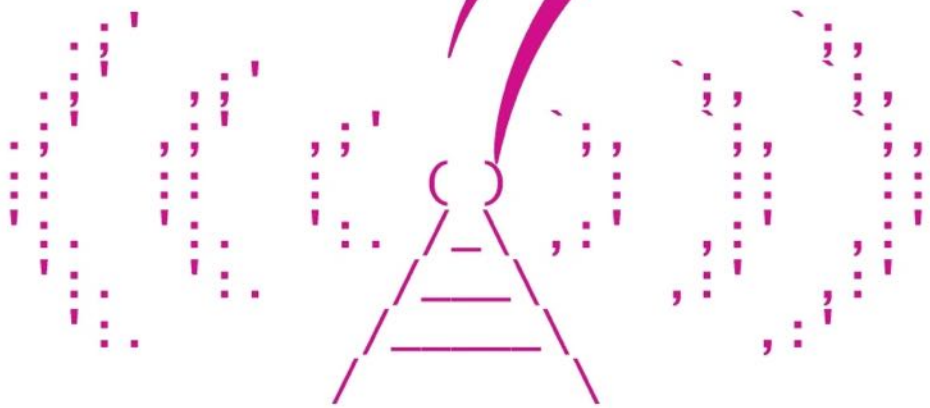


+ CD GRATUIT PACK 100% PIRATE

HACKING

WIFITE : PÉNÉTREZ LES RÉSEAUX SANS FIL

Intégré à la distribution Kali Linux 2.0, WiFit est un script particulièrement malin qui va tenter de pénétrer dans n'importe quel réseau à portée de Wi-Fi...

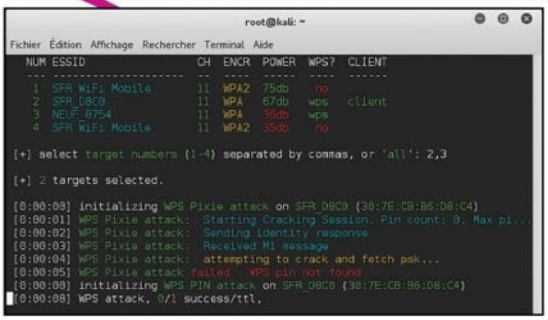


Le moins que l'on puisse dire, c'est que WiFite ne fait pas de détails. Bon point : il automatise les tests de pénétration. Sous réserve d'avoir une carte Wi-Fi compatible avec l'injection de paquet, WiFite va tester les réseaux des environs et tenter de s'y introduire, qu'ils soient protégés en WEP ou WPA. Plus fort, il va même essayer de forcer l'entrée des box ou routeurs protégés par WPS. Les puristes diront que c'est un logiciel de « script kiddies » (des pirates amateurs qui utilisent des outils clés en main, sans comprendre ce qu'ils font), mais il s'agit ici de vérifier la sécurité de son réseau. Si ce dernier est perméable à WiFite, c'est que n'importe qui peut y avoir accès. Il serait donc temps de blinder la sécurité !

LES FAILLES WPS SONT PLUS QUE JAMAIS D'ACTUALITÉ !

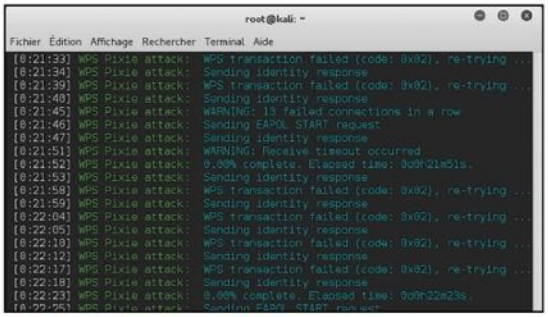
INFOS [KALI LINUX 2.0]
Où le trouver ? [www.kali.org] Difficulté : ☠☠☠

TUTO



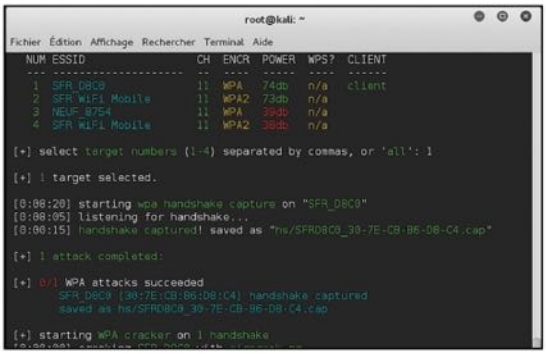
01 › LES BASES

Dans un terminal, stoppez le service network-manager pour éviter les conflits en tapant **service network-manager stop**. Faites ensuite **wifite** puis **Entrée**. Le logiciel scanne les réseaux alentour. Tapez **Ctrl+C** pour choisir les SSID à attaquer. Attention, si vous faites **all,** il ira frapper à toutes les portes ! Tapez le numéro de votre propre réseau (**Maj** + chiffre du haut du clavier) et validez. WiFite utilise Aircrack et Reaver pour pénétrer votre réseau par tous les moyens. Affinez avec les arguments.



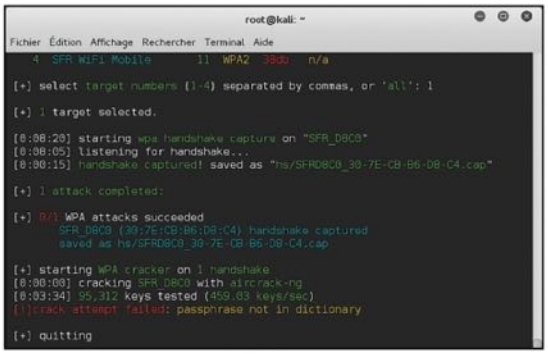
02 › WEP ET WPS

Laissons de côté le WPS, dépassé (la commande est **wifite – wep**, si jamais). Côté WPS, les points d'accès disposent de mesures de protection anti « brute force » en autorisant la saisie d'un seul PIN toutes les 60 secondes. Pas de solution miracle : il faut emprunter une adresse Mac « amie ». Cette technique étant plus complexe (Google est votre ami), nous irons au plus simple en tapant **wifite -wps -mac**. Comme plus haut, faites **Ctrl+C** pour choisir les SSID à attaquer.



03 › CAPTURER LE HANDSHAKE WPA

L'intrusion d'un réseau protégé par WPA ou WPA2 est plus compliquée. Il faut capturer le « handshake », le moment où un appareil et un point d'accès Wi-Fi vont tenter de s'authentifier mutuellement. Dans le handshake se trouve le mot de passe chiffré. Une fois capturé, il prend place dans **root/hs** (regardez **Dossier Personnel**). Il faut ensuite le cracker, soit par brute force, soit par une attaque dictionnaire. Kali Linux dispose de tous les outils nécessaires.



04 › ATTAQUER LE HANDSHAKE

Nous pouvons aussi demander à Aircrack d'essayer de cracker le mot de passe contenu dans le handshake, en tapant simplement **wifite -wpa -aircrack**. Ici, l'attaque a échoué. Même si le handshake a été capturé, Aircrack n'a pas réussi à découvrir le mot de passe « en clair ». Il faut dire que notre point d'accès est bien protégé ! Rien ne vous empêche d'utiliser à nouveau le handshake avec un meilleur dictionnaire ou avec un logiciel de brute force comme **John The Ripper**...

DÉSACTIVEZ LES PUCES NFC DE VOS CB

Le NFC est une technologie sans fil et sans contact. Elle nous entoure alors que nous n'avions rien demandé. Car comme le WiFi ou le Bluetooth, le NFC ajoute sans doute du confort dans nos habitudes, mais aussi de l'insécurité... surtout au niveau de votre porte-monnaie.

Le NFC est une technologie de communication permettant des échanges sans fil à courte portée. Lorsqu'il s'agit de lire des infos (prix en magasin, caractéristiques d'un produit), de les synchroniser ou de faire joujou avec votre console de jeux, cela ne pose pas de problème. Mais lorsque les industriels commencent à trouver d'autres applications un peu plus sensibles, cela ouvre les portes aux malfaiteurs. Les banques par exemple se sont engouffrées dans la brèche. Tout contents de pouvoir proposer à leurs clients des paiements simplifiés en dessous des 20 €, les deux géants du marché des cartes bancaires (Mastercard et Visa) ont implanté des puces NFC dans leur produit depuis quelques années. Ces cartes sont depuis majoritaires et peut-être en avez-vous une sans le savoir. La banque ne vous dit rien, et vous la propose d'office ! On vous montre ici comment désactiver cette puce qui, une fois piratée, peut révéler bon nombre d'infos sensibles vous concernant (type de carte, numéro, historique des paiements...). Attention, cette technique est périlleuse et ne doit être envisagée que dans un cas de force majeure : refus de désactiver la puce de la part de la banque, etc. N'oubliez pas que la carte appartient à la banque alors si vous l'endommagez volontairement, cette dernière peut bien sûr vous demander de la repayer...

L'APPLI QUI BALANCE TOUT !

Lecteur de carte bancaire NFC disponible sur le Google Play Store peut sans problème accéder à diverses informations : type de carte, numéro, date d'expiration et historique des paiements. Il ne manque que le cryptogramme visuel au dos. Notons quand même que dans certains pays (États-Unis, Russie, etc.), ces infos sont suffisantes pour effectuer des achats par Internet.

INFOS [LECTEUR DE CARTE BANCAIRE NFC]

Où le trouver ? [**https://goo.gl/zgRQcw**] Difficulté : ☠☠

TUTO

01 › SCANNER LA PUCE NFC

Vous avez une carte bancaire avec la technologie NFC ? Si c'est le cas, vous devriez avoir un petit logo en forme d'onde à côté de la puce électronique (on dirait le logo WiFi de travers !). Pour lire le contenu, installez l'appli **Lecteur de carte bancaire NFC** sur votre smartphone Android et posez votre carte bancaire au dos de votre téléphone. Patientez jusqu'à ce que la CB soit lue par votre appareil mobile.

02 › LIRE LES INFOS

Outre le numéro complet, le **Type de carte** (Visa ou Mastercard) et la date d'expiration, on trouve le numéro **AID**. Ce dernier permet de savoir le type de carte et le pays d'émission (vous trouverez une liste ici : **https://goo.gl/1HlbaS**)

Dans l'onglet **Transactions**, vous retrouverez la liste complète de vos derniers achats. En lisant le contenu de cette carte, on peut donc savoir tout ce qui a été acheté dernièrement et pour combien.

03 › REPÉRER LA BOBINE MAGNÉTIQUE

La puce NFC est trop près de la puce «normale» pour intervenir sans endommager la carte. Il faut opérer sur la bobine qui interagit avec les champs magnétiques. Cette dernière est un fil très fin qui parcourt la carte. Suivant les modèles, le «chemin» emprunté sera différent. Essayez de trouver ce fil en vous mettant dans le noir. Avec une lampe torche puissante (ou un flash de mobile) orientée sur le recto de la carte, vous trouverez une partie de la bobine.

04 › LA DÉTRUIRE

Une fois repérée, marquez l'endroit avec un stylo bille. Suivant l'emplacement de la bobine, vous pouvez percer ou couper avec une paire de ciseaux bien aiguisée pour détruire la fonctionnalité de paiement sans contact. Attention ne coupez/percez pas dans la bande magnétique ! Vérifiez que vous avez réussi en utilisant l'appli **Lecteur de carte bancaire NFC**. Tentez un retrait au guichet automatique pour être sûr que vous n'avez pas endommagé la carte.

LE FORUM

DE LA COMMUNAUTÉ

Android MT

forum.android-mt.com

Tutoriels · Conseils & astuces · **Tests** · Avis ·
Dépannage · **Hacking** · Découverte d'applications...

HASHCAT

UN CRACK DU CRACK

Pour le crack de mots de passe Hashcat est le meilleur. Très complet, mais aussi un peu difficile à prendre en main, ce logiciel travaille à partir de n'importe quel type de hash...

Compatible avec les technologies de GPU OpenCL et CUDA, Hashcat profite de la puissance des cartes graphiques en matière de calcul. Disponible sur Windows, utilisé ici, et Linux (mais pas Raspian), il prend en compte plus de 160 hash (normaux ou salés). Parmi eux, ceux spécifiques à de nombreux logiciels : Veracrypt, Truecrypt et Axcrypt, mais aussi Wordpress, WinZip, PDF (jusqu'à la version 11 d'Acrobat) ou Office 2013. Les types d'attaque sont légion : brute force, dictionnaire, attaque par masque, par combinaison, hybride (dictionnaire + brute force) et « rule-based attack ». C'est la plus compliquée, car il s'agit de programmer des règles précises en fonction de votre cas de figure (duplication, inversement, omission, remplacement des caractères, etc).

DES OPTIONS TRÈS POINTUES

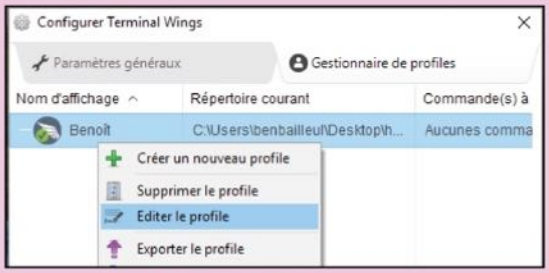
Pour accélérer les recherches, Hashcat permet de séparer le travail entre plusieurs ordinateurs sur un réseau local ou par Internet. On peut aussi imaginer commencer le travail sur un PC pour le terminer sur un autre sans perdre le temps de calcul. Quatre types d'occupation du système sont disponibles : **low**, **default**, **high** ou nightmare. Dernier point intéressant, Hashcat contient un garde-fou au niveau de la température du CPU ou du GPU, ainsi qu'un benchmark pour savoir à quoi s'attendre sur certains projets au niveau du temps de calcul.

HASHCAT

INFOS [HASHCAT]

Où le trouver ? [**http://hashcat.net**] Difficulté : ☠☠☠

TUTO

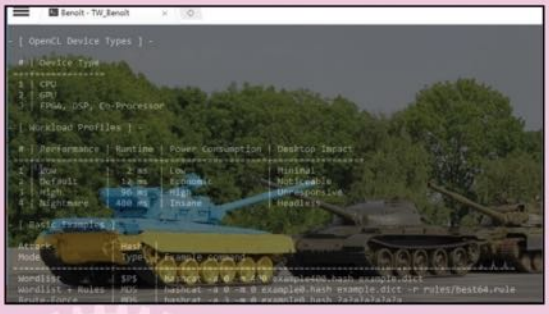


01› AVANT D'ATTAQUER

Avant de commencer, notons que si vous vous amusez avec ce logiciel, vous pouvez faire un tour sur **http://hashgenerator.de** pour avoir des hash que vous pourrez essayer de cracker. Sur **https://crackstation.net** vous pourrez voir si le hash correspondant à votre mot de passe est déjà connu et si votre mot de passe est à l'abri d'une attaque brute-force sur **https://howsecureismypassword.net**.

02› LE TERMINAL

Hashcat s'opère en ligne de commande. Pour plus de confort, nous utilisons le logiciel Windows Terminal Wings (**www.phrozensoft.com**), mais ce n'est pas une obligation. L'avantage réside dans la gestion d'un profil avec un répertoire d'usage. Allez dans le menu avec les trois barres horizontales à gauche puis **Configuration**. Créez un profil et pointez vers le répertoire de Hashcat. Si vous ne souhaitez pas utiliser Terminal Wings, restez appuyé sur **Maj**, faites un clic droit dans le dossier de Hashcat puis **Ouvrir une fenêtre de commande ici**.

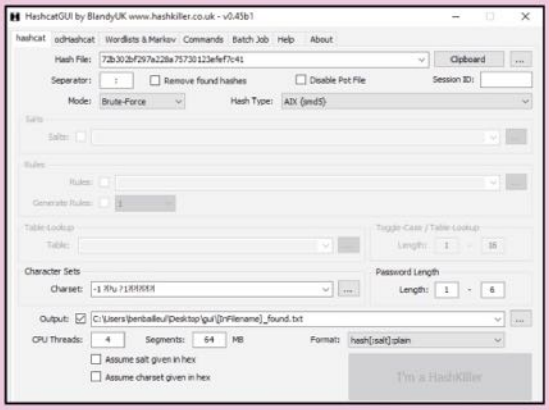


03› HELP !

Pour nos démonstrations, nous allons utiliser des mots de passe caractéristiques : **jesus** (facile à trouver), **delopa** (moins facile) et **H4j^p*U%J4s** (très difficile). Tapez **hashcat64 --help** pour en savoir plus sur les options du logiciel. Toutes les options principales sont ici. Mettez les hash correspondants à vos mots de passe dans un fichier **hash.txt** (un hash par ligne ou un par fichier si vous souhaitez faire des tests) et placez ce dernier dans le dossier de Hashcat.

04› BRUTE FORCE

Imaginons que nous savons que notre mot de passe soit un hash SHA-1 (pour mieux cibler le hash, utilisez le script Python hashtag.py). Créons un fichier **cracked.txt** dans le dossier et attaquons avec un brute force (**-a 3**). Dans le **--help,** nous voyons que le code pour le SHA-1 est **100** (**23** correspond à Skype, **2500** au WPA2, etc.) Nous allons donc taper : **hashcat64 -m 100 -a 3 -o cracked.txt hash.txt**. Le sésame correspondant à un hash se trouve dans le fichier **cracked.txt**, après le caractère « **:** ».

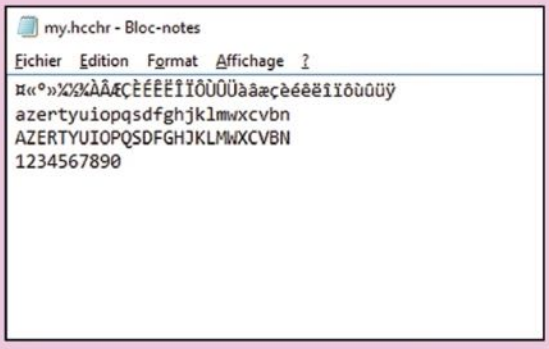


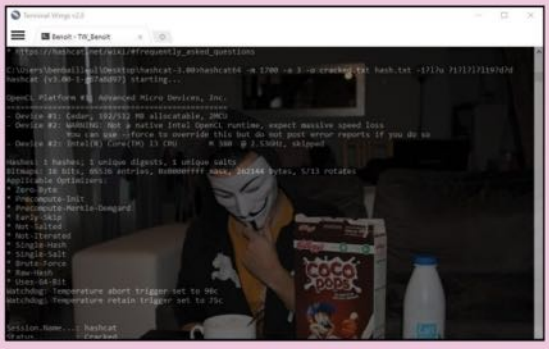
05› PLUS D'OPTIONS

Allez dans **charsets\special\French\fr_ISO-8859-16-special.hcchr**, copiez/collez le fichier dans la racine du dossier Hashcat et ajoutez les caractères que Hashcat doit chercher, avec un éditeur de texte (même s'il est possible d'ajouter **?l?u?d** à la commande pour tous les caractères classiques). Essayons maintenant : **hashcat64 -m 100 -1 my.hcchr -a 3 -o cracked.txt hash.txt**.

06› DICTIONNAIRE

Pour les attaques par dictionnaire vous pouvez utiliser le fichier **example.dict,** mais ce dernier est très léger et incomplet (pour trouver des dictionnaires, Google est votre ami). Essayons : **hashcat64 -m 0 -a 0 -o cracked.txt hash.txt exemple.dict**. On peut aussi tenter une attaque hybride ou par combinaison en ajoutant plusieurs dictionnaires à la suite à la fin de la ligne de commande.





07› CHOISIR LA LONGUEUR

Affinez la recherche n'essayant que des sésames d'une longueur déterminée. Par exemple, en utilisant le masque **?l?l?l?l?l?l?l?l**, vous ne vous attaquerez qu'à des mots de passe de 8 caractères minuscules de long (pour choisir des caractères, direction **https://goo.gl/Wy2Qdc**, sous **Built-in charsets**). Dans ce cas, un mot de passe de 7 caractères ne sera jamais trouvé. Au lieu de lancer plusieurs attaques sur le même mot de passe, utilisez l'argument **--increment**.

08› UN PEU DE PRATIQUE

Vous avez récupéré un hash correspondant à un mot de passe. C'est celui de votre maman Huguette, 62 ans, qui l'a oublié. Comment le retrouver ? Huguette se souvient avoir peut-être mis une majuscule au début et une année à la fin. En utilisant Hashtag.py, vous découvrez que le mot de passe est un hash SHA-512 (code **1700**). Pour le retrouver, nous allons taper : **hashcat64 -m 1700 -a 3 -o cracked.txt hash.txt -1?l?u ?1?l?l?l19?d?d**. Avec cette commande, le programme tentera tous les mots de passe de **aaaa1900** à **Zzzz1999**.

RÉCUPÉREZ TOUTES LES ADRESSES MAIL D'UN DOMAINE

Vous désirez récupérer toutes les adresses d'un domaine Internet ? EmailHarvester automatise la tâche et recherche des e-mails en utilisant une dizaine de ressources et moteurs de recherche.

EmailHarvester est une sorte de web crawler, il explore automatiquement Internet à la recherche de contenu ciblé. Souvent utilisé par les spammeurs pour collecter des adresses à qui envoyer du pourriel, ce type de logiciel peut aussi être utilisé pour des tâches plus nobles. Par exemple : récupérer les adresses d'une société pour l'envoi de CV ou pour trouver une personne particulière.

LES MOTEURS DE RECHERCHE SONDÉS

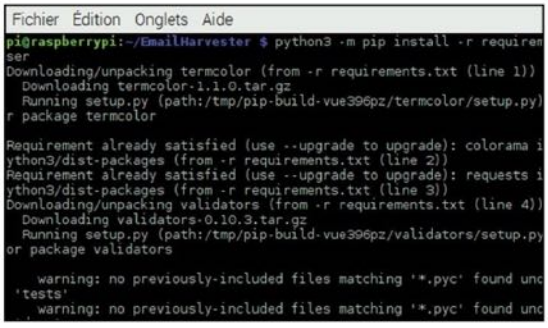
Ce type d'outil peut aussi être utilisé pour du footprinting avec Maltego (abordé dans *Pirate Informatique n°23*). Une technique qui consiste à glaner le plus d'infos sur un individu, une société ou un site et de dresser une liste de toutes les entités auxquelles ils sont rattachés. Vous pouvez aussi tester votre propre nom de domaine pour vous prémunir du spam ou du mail bombing. EmailHarvester va chercher des adresses e-mail laissées «en clair» sur le Net en questionnant les moteurs de recherche les plus connus (Google, Bing, Yahoo...) ainsi que les moteurs de Twitter, Reddit ou Instagram.

INFOS [PYTHON 3] [www.python.org]
[EMAILHARVESTER] [https://goo.gl/W8oJRW] Difficulté : ☠☠☠

TUTO

01 › L'UTILISER SOUS LINUX

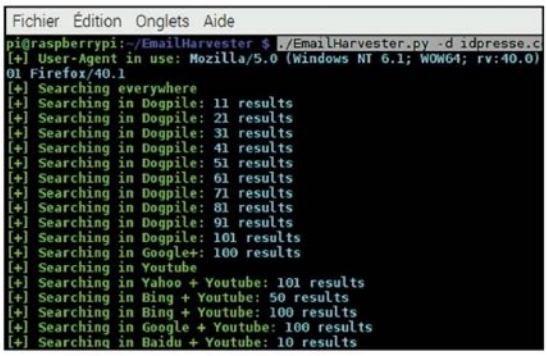
Sur un Raspberry Pi, nous utilisons ici Raspbian, une version spéciale de la distribution Linux Debian. Lancez un terminal et tapez : **sudo apt-get update && uggrade** Vous mettez alors à jour vos paquets et le système puis : **git clone https://github.com/maldevel/EmailHarvester**. Cela copie les fichiers dans un dossier **EmailHarvester**.



02 › INSTALLER

Pointez vers ce dossier avec **cd EmailHarvester**. Il faut ensuite ensuite ajouter les librairies nécessaires pour la version de Python que nous devons utiliser : **python3 -m pip install -r requirements.txt –user**. Rendez le script exécutable avec :

chmod +x EmailHarvester.py



03 › TAPER LES COMMANDES

Lancez cette commande : **./EmailHarvester.py -d idpresse.com -e all** Cette dernière va chercher les adresses du domaine idpresse.com sur tous les moteurs de recherche connus par EmailHarvester. Vous pouvez changer cette commande : **./EmailHarvester.py -d toyota.fr -e google**. Libre à vous de changer le code Python pour ajouter vos propres moteurs de recherche...

```
$ pip install scrapy
$ cat > myspider.py <<EOF
import scrapy

class BlogSpider(scrapy.Spider):
    name = 'blogspider'
    start_urls = ['https://blog.scrapinghub.com']

    def parse(self, response):
        for title in response.css('h2.entry-title'
            yield {'title': title.css('a ::text').

        for next_page in response.css('div.prev-pc
```

04 › ALLER PLUS LOIN

Email Harvester ne va pas assez loin ? Vous voudriez récupérer d'autres informations automatiquement à partir du Web ? Scrapy est un framework, téléchargeable depuis ce lien : https://scrapy.org, qui permet de créer des web crawlers sur-mesure. Pour récupérer toutes sortes d'informations (les liens d'une page Web, le contenu éditorial...).

PRENEZ LE CONTRÔLE D'UN PC À DISTANCE

INFOS [TIGHTVNC]
Où le trouver ? [**www.tightvnc.com**] Difficulté : ☠☠☠

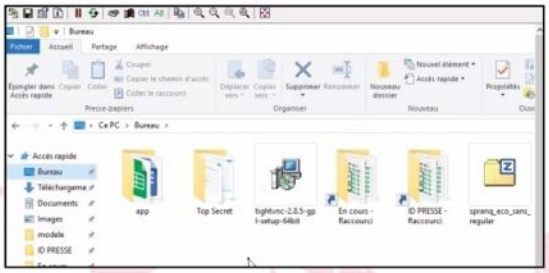
TUTO

01 › CHOISIR UN MOT DE PASSE

À la fin de l'installation de TightVNC, définissez un mot de passe pour protéger le contrôle à distance (**Password for Remote Access**). Cette opération est fortement recommandée. Pour une protection accrue, entrez également un mot de passe administrateur (**Administrative Password**). Utile en cas d'utilisateurs multiples.

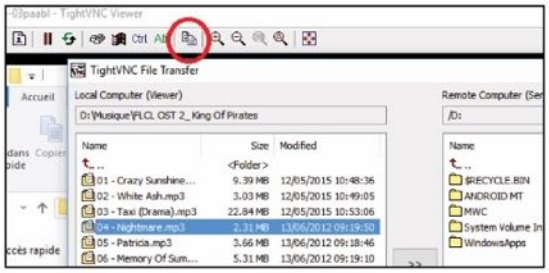
02 › CONNECTER

Lancez TightVNC Viewer sur le PC « maître » et TightVNC Server sur le PC « cible » (dans le dossier **TightVNC Server (Service Mode) > Start TightVNC Service**). Sur le PC « maître », entrez le nom du PC à contrôler dans le champ à droite de **Remote Host** et validez avec **Connect**. Le nom du PC est visible dans **Paramètres du PC > Système > Informations système**.



03 › CONTRÔLER

Une fenêtre s'ouvre et affiche le bureau du PC dont vous avez maintenant le contrôle. Vous pouvez naviguer dessus exactement comme si vous étiez en face de l'écran. Attention : pendant ce temps, un utilisateur peut agir sur le PC contrôlé, même si vos actions prévalent. Indiquez bien à la personne concernée de ne pas toucher au clavier ou à la souris.



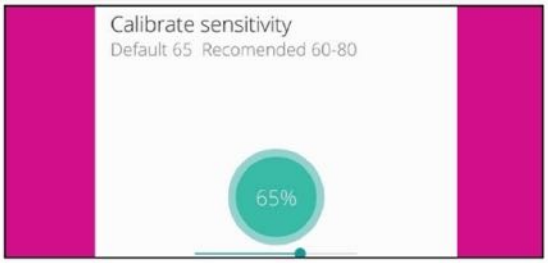
04 › TRANSFÉRER

Il n'est pas possible de glisser/déposer des fichiers d'un PC à l'autre avec la souris. Pour cela, cliquez sur l'icône de transfert des fichiers (entourée en rouge ci-dessus). À gauche se trouve l'arborescence du PC « maître », à droite celle du PC « cible ». Sélectionnez les fichiers et leur destination avant de démarrer le transfert avec les flèches, dans un sens ou dans l'autre.

DÉTECTEZ LES CAMÉRAS ESPIONS !

INFOS [DÉTECTEUR DE CAMÉRA CACHÉE]
Où le trouver ? [https://goo.gl/7MrBC8] Difficulté : ☠☠☠

TUTO



01 › COMPRENDRE LES CHIFFRES

L'appli ne vous dit pas si oui ou non une caméra est détectée. **Detect camera by radiation meter** transforme votre smartphone en détecteur de champs magnétiques pour appareils électroniques. Les données sont donc toutes relatives. Dans une chambre d'hôtel, si vous passez votre téléphone devant une lampe et que l'appli vous indique **50**, la lampe identique de l'autre côté du lit doit vous indiquer la même chose. Si l'indice s'envole à **280**, il y a quelque chose de louche.

02 › RÉGLER LE FONCTIONNEMENT

L'appareil est monté jusqu'à plus de **500** en le mettant au contact d'une caméra IP par exemple. Par contre, si votre miroir, votre portemanteau ou une peluche se met à biper, c'est qu'une caméra y est cachée ! Vous pouvez arrêter les « bip bip » en appuyant sur l'icône en forme de haut-parleur. Il est aussi possible d'ajuster la sensibilité de l'appareil en fonction de l'endroit où vous vous trouvez.

03 › OBTENIR DES CONSEILS

Tips and Tricks vous donne des indications en fonction de l'endroit où vous êtes. Dans une cabine d'essayage (**Changing room**), les caméras cachées sont souvent au même endroit. Dans un hôtel, elles seront dans les endroits les moins visibles. Touchez le miroir qui vous pose problème. Vous constatez un « trou » entre votre doigt et sa réflexion ? Si la réponse est non, une caméra est peut-être présente. En cas de doute, pourquoi ne pas mettre un linge dessus pour se cacher ?

04 › DÉTECTER EN INFRAROUGE

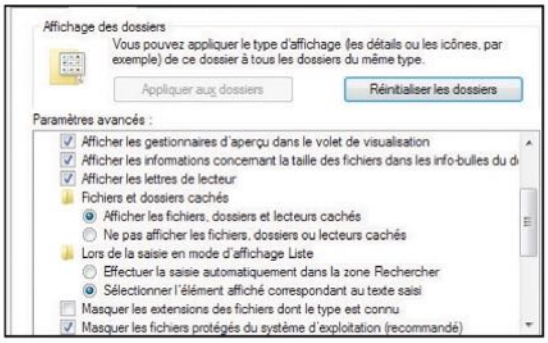
Detect infrared camera sert à repérer les caméras infrarouges. Testez avec une télécommande par exemple. Si vous voyez une lumière blanche (non visible à l'œil nu), c'est sûrement une caméra. Comme vous pouvez le constater, notre lapin en peluche a l'air bien curieux ! Vous pouvez cumuler les deux outils (détection des champs magnétiques et infrarouge) pour recouper les résultats.

LOCALISEZ ET TRANSFÉREZ VOTRE HISTORIQUE SKYPE

Si vous voulez transférer votre historique Skype sur un nouveau PC, c'est possible ! Même s'il est bien caché ce fichier n'est pas chiffré ! Prudence donc si vous devez laisser votre PC sans surveillance...

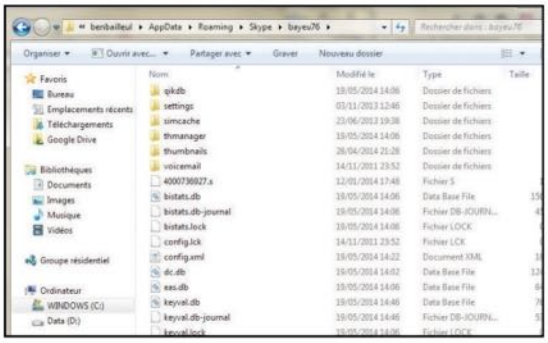
INFOS [SKYPE]
Où le trouver ? [**www.skype.com**] Difficulté : ☠☠☠

TUTO



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 le **Panneau de configuration**, faites **Apparence et personnalisation**, **Options des dossiers** et 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:\Utilisateurs\[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**...

ANALYSE DES DONNÉES DE SKYPE

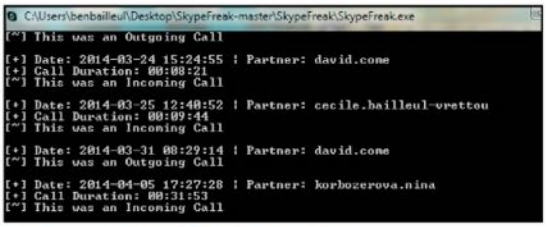
INFOS INFOS [SKYPEFREAK]
Où le trouver ? [https://github.com/yasoob/SkypeFreak] Difficulté : ☠☠☠
TUTO

01 › PYTHON ?

SkypeFreak est un script Python qui fonctionne sans avoir besoin d'installer le langage. Vous pouvez néanmoins lancer 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 (voir page précédente).

02 › PRÉPARATIFS

Si vous voulez analyser des données qui viennent d'un autre PC, il faudra mettre tout le dossier «pseudo» contenu dans **C:\Utilisateurs\[nom d'utilisateur]\AppData\Roaming\Skype** à ce même emplacement sur votre PC. Suivez notre lien et cliquez sur **Download ZIP**. Lancez **SkypeFreak.exe**. Ici, 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. Si la fenêtre se ferme ou si le programme plante, réessayez. N'oubliez pas que SkypeFreak est encore en version bêta...

04 › LE RAPPORT

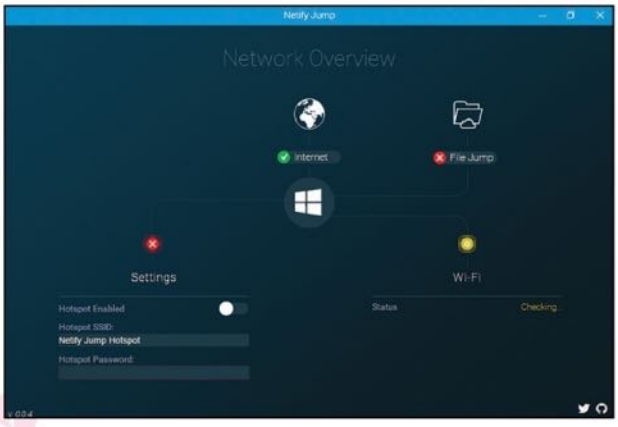
À la fin du processus, le programme va vous demander si vous voulez éditer un journal. Pratique si vous êtes sur une machine étrangère et que vous voulez récupérer les infos rapidement. Tapez **y** (pour yes), validez et tapez un nom. Ce journal sera sauvegardé au format TXT dans le dossier SkypeFreak. Sans le mot de passe de votre «victime», vous aurez donc accès à pleins d'informations.

01# Devenez lanceur d'alerte → avec SecureDrop

Nous aurions bien fait un article complet sur SecureDrop, mais il faut bien reconnaître que les gens concernés par le projet sont peu nombreux. Imaginons que vous ayez des informations à transmettre à un journaliste, mais que vous voudriez éviter d'avoir affaire avec lui (un journaliste est censé avoir le droit de protéger ses sources, mais dans les faits, il vaut mieux rester prudent). En bon whistleblower, vous devrez vous connecter au site Tor du journal puis laisser un message. En retour, SecureDrop vous donnera une clé permettant de lire les messages du journaliste. Ce dernier doit se connecter depuis Tor à son compte SecureDrop pour récupérer messages et documents. Pour l'instant seuls des médias anglo-saxons se sont intéressés au projet mais il existe une FAQ pour les journalistes, quels qu'ils soient.

Difficulté : ☠☠☠ Lien : **https://securedrop.org**

02# Faites «rebondir» votre signal WiFi → avec Netify Jump



Votre maison est trop grande, vous voulez vous connecter depuis votre piscine, mais vous n'avez malheureusement pas assez de sous pour vous acheter un répéteur WiFi (bizarre non?). Avec Netify Jump et un simple PC sous Windows vous pouvez très bien faire rebondir votre signal WiFi pour agrandir votre zone de couverture. Ce PC qui fera office de relais peut bien sûr être utilisé «normalement».

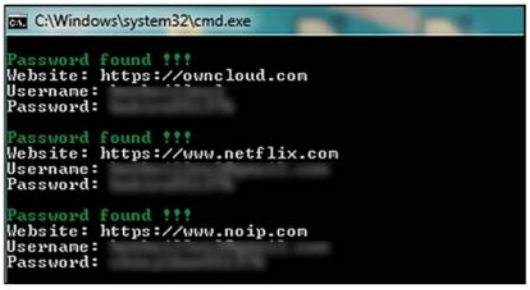
Téléchargez ce logiciel en fonction de votre système d'exploitation (32 ou 64 bits). Si vous ne le savez pas, faites un clic droit dans **Ordinateur** ou **Ce PC** (menu **Démarrer**) et cliquez sur **Propriétés**. Si Windows vous empêche d'installer le logiciel, faites **Afficher les détails** puis **Exécuter quand même**. Cliquez sur le bouton **Hotspot Enabled** et choisissez un mot de passe. C'est ce mot de passe qui devra être entré sur les appareils désirant se connecter à ce nouveau hotspot de fortune. Si un message d'erreur s'affiche c'est que votre dongle/carte WiFi n'est pas compatible avec l'hébergement d'infrastructure WiFi ce qui est parfois le cas sur des PC bas de gamme ou portables. Tentez le coup !

Difficulté : ☠☠☠

Lien : **https://goo.gl/UChTcU**

03# Récupérez des mots de passe
→ AVEC LAZAGNE

Dans le même genre que RecALL, LaZagne va pomper les sésames contenus dans vos navigateurs et plusieurs autres logiciels. Il est légèrement moins complet que RecALL, mais est beaucoup plus discret et rapide. Décompactez le fichier ZIP et rendez-vous dans le dossier **LaZagne-master\Windows**. Maintenez la touche **Maj** du clavier, faites un clic droit dans **Standalone** puis cliquez sur **Ouvrir une fenêtre de commande ici**. Tapez ensuite **lazagne.exe all**. Magique !



Difficulté : Lien : **https://github.com/AlessandroZ/LaZagne**

04# Cachez des fichiers dans des images
→ AVEC STEGANO

Pour dissimuler message ou fichier dans une photo, il suffit de jouer avec les octets qui codent pour la couleur de l'image. La méthode la plus courante consiste à modifier les «bits de poids faible» (ou «least significant bit» en anglais). Même modifiés, ces derniers n'altèrent que très peu le rendu final d'une photographie, mais correspondent à une suite suffisamment conséquente de bits pour qu'elle puisse constituer un message. Le logiciel Stegano, tout en français, permet de réaliser facilement ce tour de force...

Difficulté :

Lien : **http://tinyurl.com/3vggnxt**

05# Limitez la bande passante de vos applications → AVEC NETBALANCER

NetBalancer est un petit logiciel qui va devenir indispensable à tous les «control freak» de la bande passante. Une fois installé, il va non seulement vous afficher toute votre activité réseau (comme GlassWire, par exemple), mais il permet aussi de mettre des garde-fous. En cliquant sur l'icône en haut à droite à côté du petit nuage, vous pourrez contrôler la priorité de download/upload de chaque processus. Pratique, pour éviter d'engorger sa bande passante lorsque vous travaillez. Il est possible d'éditer des règles précises, de couper complètement le trafic vers certaines applications : le contrôle total quoi...

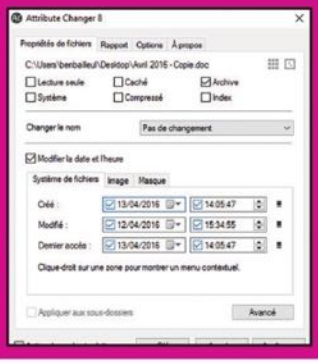
Difficulté :

Lien : **https://netbalancer.com**

06# Trafiquez les métadonnées de vos fichiers

→ AVEC ATTRIBUTE CHANGER

Attribute Changer est un logiciel qui va changer le menu contextuel, lorsque vous faites un clic droit sur un fichier. Vous serez libre alors de changer différents attributs et métadonnées comme l'heure de création ou de modification du fichier (pratique pour rendre un devoir en retard ou changer la date de prise de vue d'une photo). Vous pourrez aussi changer les privilèges comme choisir de mettre un fichier en lecture seule pour éviter que votre famille ne puisse modifier le contenu ou le camoufler comme un fichier caché ou un élément du système. Vous pourrez même garder une trace des modifications pour revenir en arrière en cas de besoin...



Difficulté : Lien : **www.petges.lu**

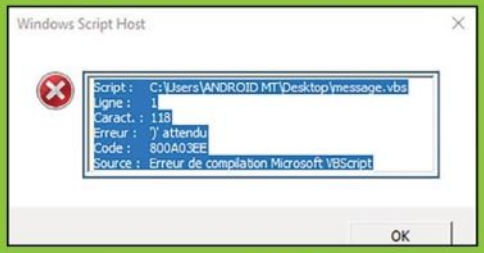
07# Copier un texte non sélectionnable

→ AVEC TEXTIFY

Si vous tombez sur un texte (message d'erreur Windows par exemple) qui n'est pas sélectionnable, mais que vous avez besoin de copier, Textify outrepasse cette restriction. Dans les options du logiciel, sélectionnez la combinaison que vous souhaitez : ici, nous avons choisi d'appuyer en même temps sur le bouton droit de la souris et de maintenir la touche **Maj**. Utilisez cette combinaison sur le texte et il deviendra sélectionnable. Cela fonctionne avec tout texte non sélectionnable dans Windows.

Difficulté :

Lien : **http://rammichael.com/textify**



08# Trouvez les failles WPS

→ AVEC WPS CONNECT

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. Le propriétaire 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. Et c'est là, que la vulnérabilité existe. Certains constructeurs utilisent le même PIN pour tous leurs produits et il est même parfois impossible de le changer sans modifier le firmware. WPS Connect est une application pour appareil Android rooté qui va tenter de se connecter sur les routeurs alentours pour voir s'ils sont vulnérables. Attention, il s'agit bien sûr de vérifier votre matériel et pas de se connecter chez le voisin !

Difficulté : Lien : **https://goo.gl/NZOAJ8**

09# Du pentesting sur mobile

→ AVEC CSPLOIT ANDROID

Vous voulez vérifier la sécurité du réseau Wi-Fi d'un ami ? Pas besoin de vous déplacer avec un PC sous Kali Linux puisqu' avec un mobile sous Android et cSploit, vous pourrez lancer toute une batterie de tests : sniffing, sidejacking, crack de mots de passe, scan de ports, manipuler le trafic (ARP poisoning) et réaliser des attaques de type « man-in-the-middle ». Si vous connaissiez dSploit, vous ne serez pas dépaysé avec son successeur. L'interface est légèrement plus agréable et certains menus sont en français. Pour le reste, c'est la même chose avec des mises à jour au niveau des exploits disponibles et des failles connues...

Difficulté :

Lien : **http://www.csploit.org**

10# Coller du texte sur les sites qui le refusent

→ AVEC FIREFOX

Sur certains sites, il est impossible de coller du texte dans un champ de saisie, il faut obligatoirement taper au clavier. Mais avec Firefox, une petite astuce permet de contourner ce blocage. Ouvrez une fenêtre ou un onglet vierge et tapez **about:config**. Cochez le **Je prends le risque**. Tapez ensuite **dom.event.cl** dans le champ **Rechercher**. Double-cliquez sur **dom.event.clipboardevents.enabled** pour que sa valeur passe à **False**. Fermez l'onglet, c'est effectif immédiatement.

Difficulté :

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.

MULTIMÉDIA

FORMAT FACTORY : LE CONVERTISSEUR UNIVERSEL

Nous vous parlons souvent de logiciels d'encodage ou de conversion dans nos pages, mais la plupart du temps, il s'agit de programmes spécialisés dans tel ou tel domaine. Si vous n'avez pas de besoin particulier, mais qu'il vous arrive fréquemment de convertir divers types de fichiers, Format Factory (FF) est le logiciel qu'il vous faut...

FF 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, mais aussi pour n'importe quel document (image, photo, ebook, etc.) 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.

LES FORMATS SUPPORTÉS

VIDÉO : MP4, AVI, 3GP, RMVB, WebM, GIF, WMV, MKV, MPG, VOB, MOV, FLV et SWF.

AUDIO : MP3, WMA, APE, FLAC, AAC, MMF, AMR, M4A, M4R, OGG, MP2, WavPack et WAV.

PHOTO : WebP, JPG, PNG, ICO, BMP, GIF, TIF, PCX et TGA.

DOCUMENT : PDF, Mobi, Epub, AZW3

IMAGE DE DISQUE : ISO, CSO

POUR LES SPÉCIALISTES... OU PAS

Et même si vous n'êtes pas un spécialiste des codecs et des formats de fichier, vous allez vous en sortir comme un chef grâce à l'assistant. Notez aussi que FF supporte le multicore, qu'il rippe des DVD ou des Blu-ray vers le format MKV et dispose aussi d'un éditeur pour couper, muxer/démuxer, extraire, etc.

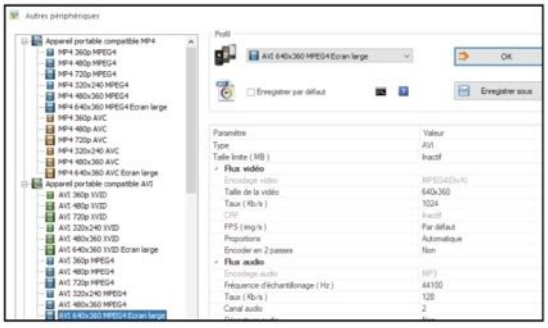
INFOS [FORMAT FACTORY]

Où le trouver ? [**www.formatoz.com**] Difficulté : ☠☠☠

TUTO

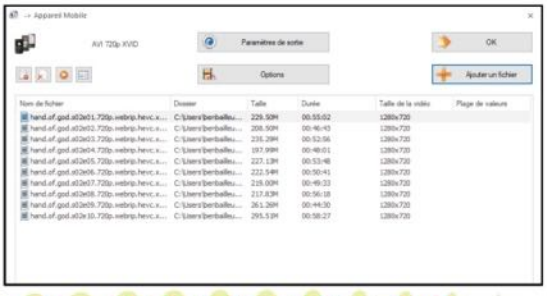
01 › LES CODECS

Après avoir installé FF, n'oubliez pas de laisser le logiciel copier les codecs dont il a besoin pour fonctionner (laissez la case **Install inside codecs** cochée) puis cliquez sur **Finish**. Au moment de l'installation, faites juste attention à ne pas installer aussi des «poubellewares». Soyez attentif et décochez les cases qui ne vous conviennent pas. Imaginons que vous vouliez encoder un fichier vidéo pour votre téléphone ou tablette...



02 › UN EXEMPLE...

Dans l'onglet **Vidéo**, cliquez sur **Appareil Mobile**. Dans la colonne de gauche, vous verrez une liste de formats longue comme le bras. Vous trouverez sans doute celui qu'il faut pour votre machine. Si ce n'est pas le cas, laissez celui par défaut et peaufinez vos réglages dans la partie de droite (résolution, bitrate, etc.)



03 › PARMI TANT D'AUTRES !

Pour les fichiers audio ou les photos, c'est à peu près la même chose. Dans l'onglet adéquat, cliquez sur **-> [format que vous désirez]** et faites **Ajouter un fichier** (en haut) ou **Ajouter un dossier** si vous voulez traiter toute une série de fichiers. Dans **Paramètres de destination**, il est même possible de paramétrer vos fichiers finaux (résolution max pour les photos, qualité de conversion audio, etc.) Faites **OK** puis, une fois revenu à la fenêtre principale, cliquez sur **Démarrer**. À la fin du processus, sélectionnez **Dossier de destination** pour aller voir vos fichiers finaux. Dans **Option,** vous pourrez changer ce dossier bien sûr...

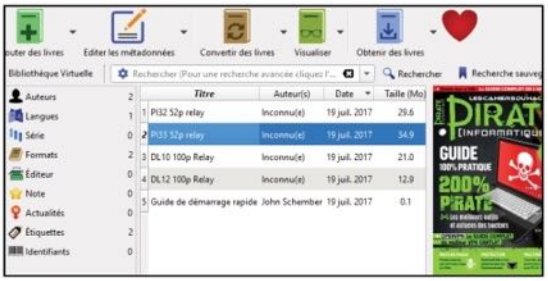
04 › EXTRACTION AUDIO OU VIDÉO

Enfin, sachez que FF permet aussi d'extraire le contenu d'un CD, d'un DVD ou d'un Blu-ray pour en faire des fichiers exploitables par votre PC (MKV, ISO, WAV). Allez dans **Périphérique ROM/DVD/CD/ISO** et laissez-vous guider par les menus. Ici aussi, vous pourrez choisir différents paramètres d'encodage sur la droite (codec, bitrate, etc.)

GÉREZ VOTRE BIBLIOTHÈQUE D'EBOOKS

INFOS [CALIBRE]
Où le trouver ? [https://calibre-ebook.com] Difficulté :

TUTO

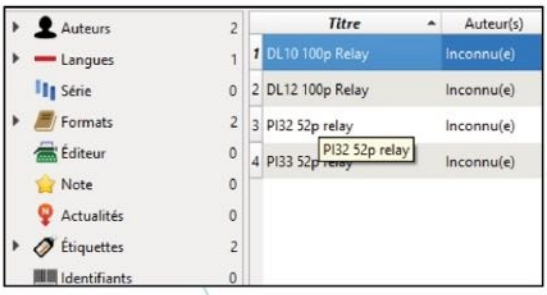


01 › AJOUTER DES LIVRES

Cliquez sur l'icône **Ajouter des livres** pour choisir les livres à ajouter sur Calibre. Si vous avez vos livres déjà organisés sur votre ordinateur, cliquez sur la petite flèche juste à côté de l'icône pour choisir l'option adéquate. Patientez quelques instants, le temps que les livres se chargent dans le logiciel.

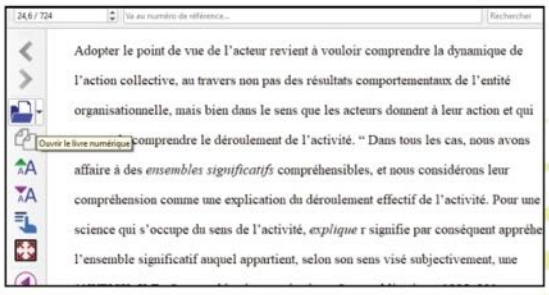
02 › RÉCUPÉRER DES INFOS

Pour ajouter des infos comme la couverture, l'auteur ou un petit résumé de l'œuvre, sélectionnez les livres concernés et cliquez sur la petite flèche de l'icône **Editer les métadonnées.** Choisissez **Télécharger les métadonnées**. Faites votre choix et patientez le temps que les données soient rapatriées. Validez avec **Ok**.



03 › TRIER

Une fois votre collection à jour, ajoutez des notes ou classez-la comme vous le désirez : par **Titre**, **Auteur**, **Note** (à éditer via l'icône **Editer les métadonnées**), par **Étiquette** (le genre) ou encore par éditeur. Via la colonne de gauche, vous pouvez par exemple choisir d'afficher seulement les livres classés 5 étoiles (**Note**).



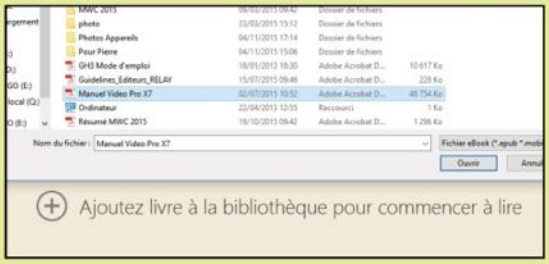
04 › LIRE DES LIVRES

Calibre vous permet de lire vos livres numériques sur l'écran de votre ordinateur. Présélectionnez l'ouvrage de votre choix puis cliquez sur la petite flèche à côté de visualiser pour choisir **Afficher avec la visionneuse de livre numérique calibre**. Vous pouvez ici changer la police, sa taille ou sauter des chapitres via les icônes placées à gauche.

LISEZ TOUS LES FORMATS D'EBOOKS

INFOS [EBOOK READER]
Où le trouver ? [**https://icecreamapps.com/fr**] Difficulté :

TUTO



01 › IMPORTER UN LIVRE

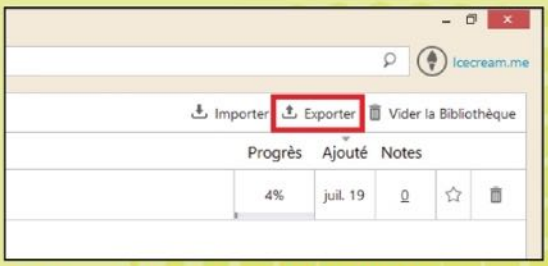
Installez Ebook Reader, ouvrez-le et cliquez sur **Ajouter livre à la bibliothèque pour commencer à lire**. Parcourez votre ordinateur pour pointer vers le fichier que vous souhaitez importer et cliquez sur **Ouvrir**. Lorsque l'opération est terminée, cliquez sur **OK** dans la fenêtre confirmant son succès.

02 › LIRE

Double-cliquez sur un ouvrage de l'onglet **Bibliothèque** pour commencer la lecture. Double-cliquez à nouveau pour passer en plein écran si besoin. Les options de lecture se trouvent dans la colonne de droite. La deuxième en partant du haut ouvre la table des matières, tandis que la cinquième en partant du haut toujours (au-dessus du mode « nuit ») affiche une ou deux pages en même temps.

03 › PLACER UN SIGNET

Avant de quitter le logiciel de lecture, n'oubliez pas de placer un marque-page virtuel en cliquant sur le troisième symbole en partant du haut (cf. image d'illustration). Une fenêtre de confirmation s'ouvre, cliquez sur **OK**. Pour reprendre la lecture là où vous l'aviez laissée, il suffit d'ouvrir le livre comme à l'étape 1. La page marquée s'affiche automatiquement.



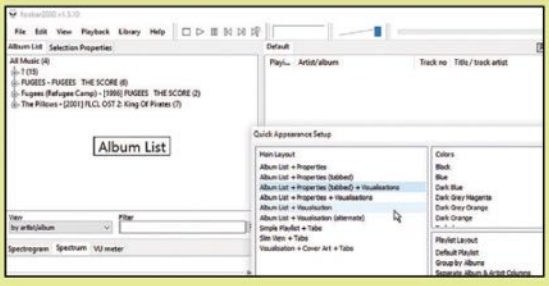
04 › EXPORTER UN LIVRE

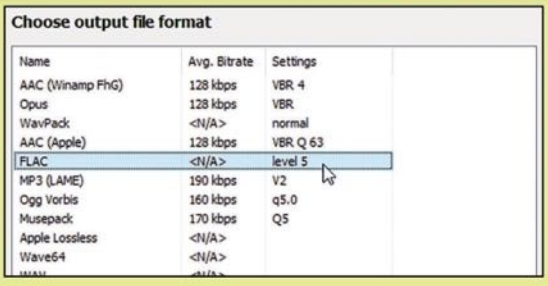
Si vous souhaitez récupérer un ebook depuis le logiciel, sélectionnez-le dans votre Bibliothèque et cliquez sur Exporter. Choisissez un emplacement et validez avec Enregistrer. Notez que le fichier est en **.ebr**. Vous pouvez l'ouvrir avec Ebook Reader d'Icecream uniquement. La démarche est surtout utile pour transférer un livre sur un autre appareil équipé du lecteur.

NUMÉRISEZ VOTRE MUSIQUE EN QUALITÉ CD

INFOS [FOOBAR2000]
Où le trouver ? [www.foobar2000.org] Difficulté :

TUTO



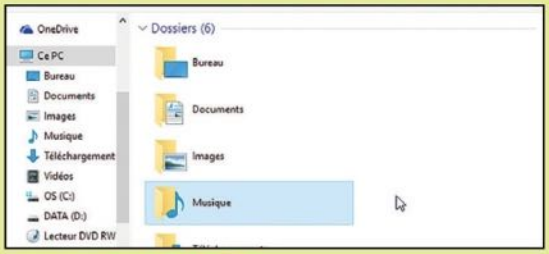


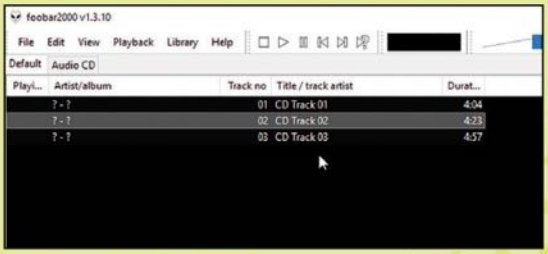
01 › INSTALLER

Téléchargez et installez Foobar2000 (suivez les étapes et ne changez rien). Faites de même avec le **Free Encoder Pack** (**www.foobar2000.org/encoderpack**). Puis insérez dans le lecteur du PC le CD à encoder. Ouvrez ensuite Foobar2000, cliquez sur **File > Open Audio CD >** le lecteur contenant le **CD > Rip > Proceed to the converter**. Dans **Output Format**, choisissez **Flac, level 5**.

02 › CHOISIR LE FORMAT

Vous pouvez choisir un autre format d'encodage, supérieur au **Flac, level 5**, mais sachez que ce dernier n'altère en rien la qualité du morceau, tout en divisant le poids du fichier initial par 2. Le format FLAC étant assez volumineux, nous vous conseillons de rester sur le niveau 5. Bien sûr, si le résultat ne vous satisfait pas, vous pourrez toujours recommencer l'opération avec un autre format.





03 › ENCODER

Vous n'avez plus qu'à choisir un dossier de destination où seront enregistrés les fichiers FLAC, avec **Destination**. Lancez le processus avec le bouton **Convert**. En fonction du nombre de pistes à extraire, l'opération peut prendre plus ou moins de temps. N'oubliez pas que vous pouvez choisir le nombre de morceaux traités lors de l'étape 1, si vous souhaitez en enlever certains.

04 › PROFITER

Vos morceaux sont désormais encodés au format FLAC. Vous pouvez les lire avec n'importe quel lecteur compatible, dont Foobar2000 bien sûr, avec la même qualité que si vous écoutiez le CD d'origine. Attention, si vous souhaitez mettre ces titres sur votre lecteur MP3, vérifiez que celui-ci lit bien le format FLAC, ce n'est pas le cas de tous.

DISCUTEZ PENDANT VOS JEUX EN LIGNE

INFOS [DISCORD]
Où le trouver ? [https://discordapp.com] Difficulté :

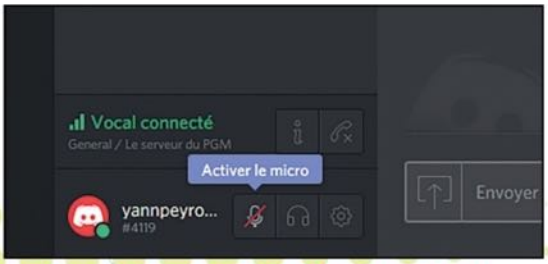
TUTO

01 › LANCER UN SERVEUR

Après avoir créé un compte Discord (facilite grandement la gestion de vos futurs serveurs) Cliquez sur **Commencer** pour accéder à l'interface principale. Donnez un nom à votre serveur de communication avant de choisir le pays (avec **Modifier**). Avec **Changer l'icône**, ajoutez une photo de profil, afin que vos amis identifient facilement le serveur. Faites **Terminé**.

02 › INVITER DES PERSONNES

Sur l'interface principale, cliquez sur **Inviter des gens**, en haut à gauche puis partagez le lien qui s'affiche avec vos amis (via mail, Facebook ou autre) pour qu'ils rejoignent votre serveur. Cochez **Faire en sorte que ce lien n'expire jamais** si vous voulez que le même lien soit réutilisable à l'avenir.



03 › ACTIVER LA DISCUSSION VOCALE

Vos contacts accèdent à un salon de discussion nommé **#general**. Vous échangez au départ en tapant au clavier. Pour utiliser la voix, cliquez sur **Activer le micro**, en bas de page, puis autorisez la détection. Vos contacts doivent faire de même, au besoin, expliquez-leur la manœuvre via le chat textuel.

04 › PASSER AU LOGICIEL

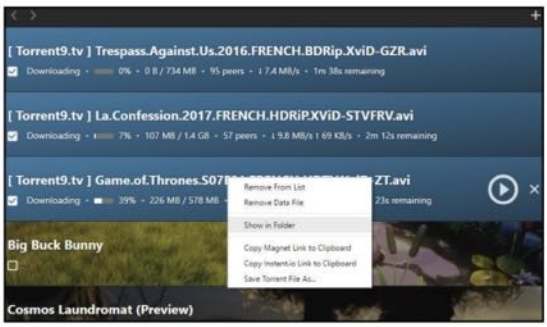
Le logiciel Discord offre plus de possibilités que le service en ligne, comme le Push-to-talk (maintenir une touche enfoncée pour activer le micro temporairement) ou l'Overlay (une fenêtre Discord toujours affichée, même en jeu). Pour vous le procurer, cliquez sur **Télécharger...** sur la page d'accueil du site.

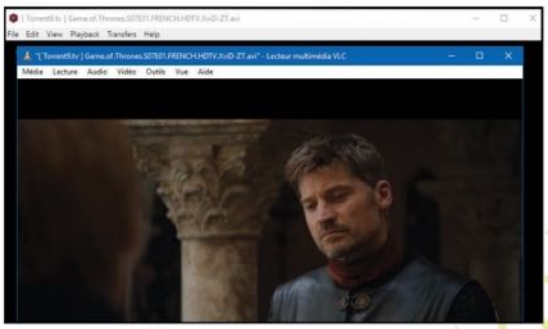
TÉLÉCHARGEZ OU STREAMEZ DES CONTENUS MULTIMÉDIAS

WebTorrent Desktop réunit à la fois streaming et téléchargement. Comprenez que pendant que vous téléchargez un film, un morceau de musique ou un ebook, vous pouvez en débuter la lecture.

INFOS [WEBTORRENT DESKTOP]
Où le trouver ? [**https://webtorrent.io/desktop**] Difficulté :

TUTO





01› TÉLÉCHARGEZ ET STREAMEZ

WebTorrent récupère les fichiers torrent et magnet. Faites glisser le fichier sur la fenêtre et le téléchargement débute. Vous commencez immédiatement à seeder. Vous pouvez supprimer le torrent via la petite croix qui apparaît en passant la souris sur ledit torrent. Le clic droit apporte d'autres options comme afficher le dossier de destination du torrent (**Show in Folder**).

02› PRÉVISUALISEZ

Dès que le téléchargement commence, vous pouvez le lire. Cliquez sur l'icône Play. Le soft échoue à lire nos vidéos, il nous bascule sur VLC (cliquez s**ur Play in VLC**). Naviguez à loisir dans la vidéo même si ce n'est pas téléchargé. Le logiciel télécharge la partie que vous voulez voir. Pour les musiques, aucun souci : WebTorrent fonctionne, tout comme le changement de morceaux.

L'INFORMATIQUE FACILE
POUR TOUS !

CHEZ VOTRE MARCHAND DE JOURNAUX

01# Encodez vos musiques et vidéos → AVEC SUPER

Super est une alternative sérieuse au logiciel d'encodage m4ng. Il a cependant l'avantage de posséder une interface simple, facile à appréhender et proposant quantité de réglages pointus. Faites un glisser-déposer des fichiers à encoder dans le champ **Drop a valid multimedia file here**. Ajustez les différents réglages proposés dans les rubriques **Video** et **Audio**. Choisissez le format de fichier désiré avec **Select the Output Container** et lancez l'opération d'encodage avec **Encode (Active Files)**

Difficulté : Lien : **http://www.erightsoft.com/SUPER.html**

02# Enregistrez vos parties de jeux → AVEC OBS

Vous rêvez de devenir le nouveau streamer roi de Twitch ? Ou simplement vous souhaitez mettre de côté vos parties épiques de The Elder Scrolls 2 daggerfall pour les montrer dans deux ans à vos petits enfants ? Le logiciel OBS est celui qui est le plus plébiscité chez les gamers. Il se configure facilement et, en quelques clics, le flux vidéo de votre partie est directement envoyé sur la plateforme Twitch ou enregistré en local, sur votre bécane. Dès le démarrage, choisissez **Optimiser pour l'enregistrement, je ne diffuse pas** et choisissez une **Résolution** d'image. Validez avec **Appliquer les paramètres**. Lancez votre jeu puis optez pour **Démarrez l'enregistrement**.

Difficulté :

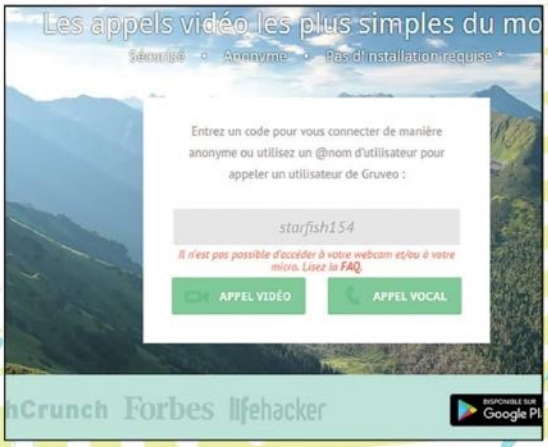
Lien : **https://obsproject.com**

03# Débutez une conversation VoIP facilement → AVEC GRUVEO

Compatible avec la plupart des navigateurs du marché et fonctionnant sur n'importe quel système capable d'afficher une page Web, Gruveo est la solution VoIP facile d'accès. Exploitant le protocole WebRTC, vous allez pouvoir converser avec la personne de votre choix en lui communiquant juste un code que vous aurez défini sur la page du service. La qualité est au rendez-vous et comme il n'y a rien à installer, c'est pratique.

Difficulté :

Lien : **www.gruveo.com**



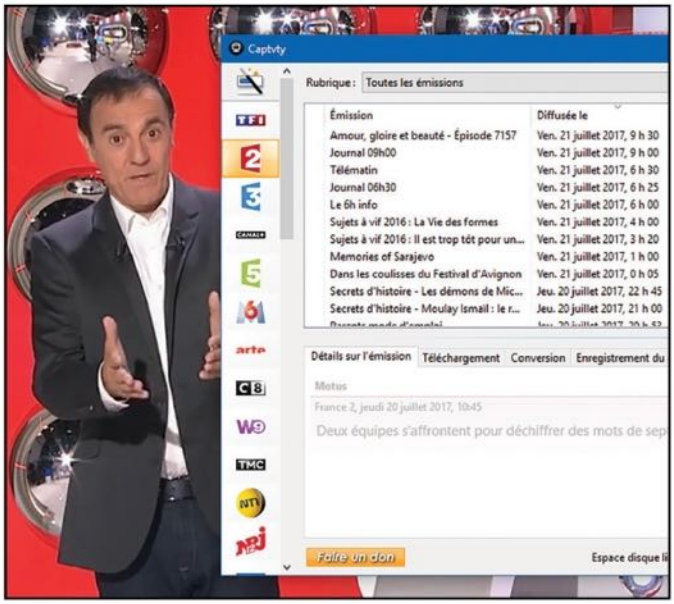
04# Enregistrez la TV

→ AVEC CAPTVTY

Captvty est l'outil idéal pour les amateurs de programmes TV. Il est capable d'enregistrer les émissions proposées sur les chaînes de la TNT pour les regarder quand bon vous semble. Choisissez votre chaîne, puis lancez la lecture. Faites un clic droit pour choisir Télécharger la vidéo. Selon les chaînes, vous aurez la possibilité de retrouver des émissions datant de plusieurs jours. En haut, dans **Rubrique**, vous triez. S'il n'y a que Motus et D'art D'art qui vous intéressent, vous récupérerez facilement tous les fichiers d'un coup. Les fichiers téléchargés sont accessibles dans un dossier l'onglet **Téléchargement**.

Difficulté :

Lien : **https://captvty.fr**



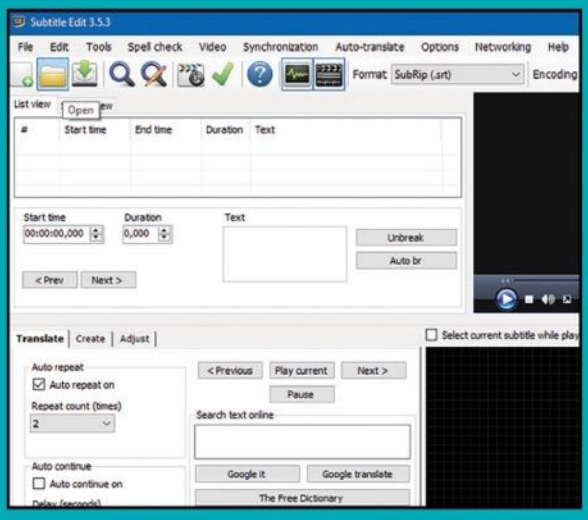
05# Modifiez les sous-titres

→ AVEC SUBTITLE EDIT

Les amateurs impatients de séries que vous êtes sont sans doute déjà tombés sur des épisodes où les sous-titres étaient en roue libre. Avec Subtitle Edit, vous corrigez ces derniers en un rien de temps. Une fois le logiciel installé, vous pouvez corriger les fautes d'orthographe, les time stamps ou encore la synchronisation. Vous avez la possibilité de diviser les lignes trop courtes ou celles qui s'étalent en longueur (pour éviter les hors cadre). Notez que Subtitle Edit prend en charge quantité de formats et les convertit facilement. Choisissez le sous-titre à traiter avec **Open** puis débutez le traitement.

Difficulté :

Lien : **www.nikse.dk/subtitleedit**



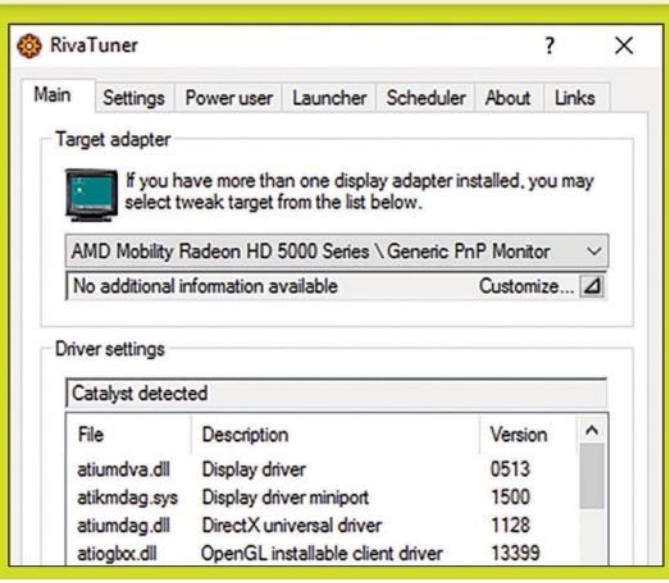
06# Overclockez votre carte graphique

→ AVEC RIVA TUNER

Eh oui, croyez-le ou non, mais la plupart des gens utilisent leur GeForce ou Radeon pour jouer et pas pour cracker des mots de passe ! RivaTuner ne se limite pas aux cartes nVidia et permet aussi d'overclocker les cartes AMD. Le logiciel permet d'outrepasser les fréquences normales et de modifier indépendamment le cadencement des shaders et celle du GPU. De l'overclocking pour les utilisateurs exigeants...

Difficulté :

Lien : **www.guru3d.com**



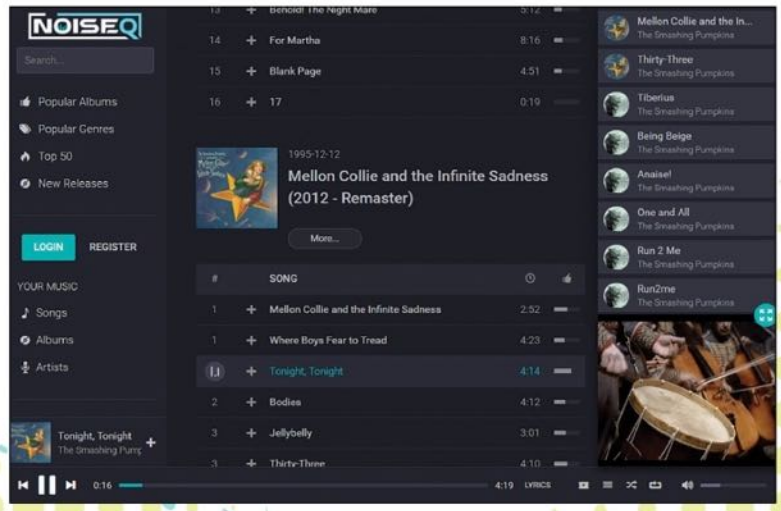
07# Écoutez de la musique gratuitement

→ AVEC NOISEQ

Dans la longue liste des « clones de Spotify gratuits qui vont se servir dans les vidéos de YouTube », voici NoiseQ. Ce service en ligne va chercher les chansons et les clips de votre choix dans les différentes bases de données dont il dispose. Vous pouvez paramétrer des playlists, avoir accès à des radios ou à des artistes similaires à ceux que vous aimez. L'interface est jolie et réactive. Le sans-faute pour les mélomanes. Créez un compte puis identifiez-vous pour créer des playlists.

Difficulté :

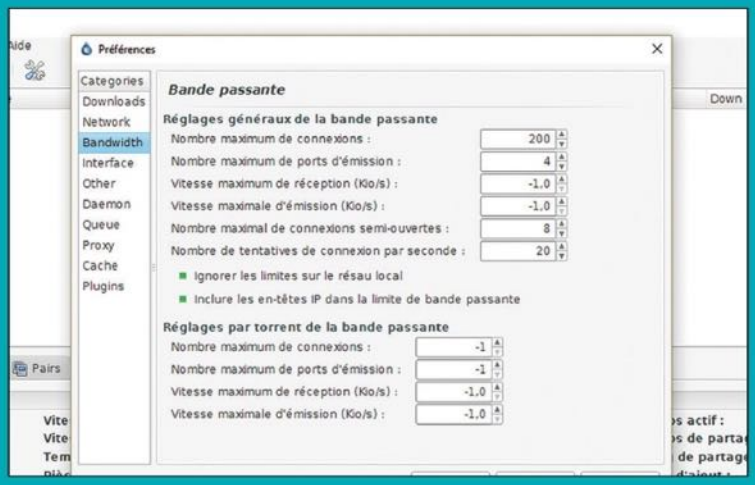
Lien : **www.noiseq.com**



08# Profitez d'un client Torrent intuitif

→ AVEC DELUGE

Très populaire auprès des utilisateurs de seedbox, Deluge conviendra parfaitement à ceux qui sont devenus allergiques à µTorrent ou qBitorrent. Il propose aussi un grand nombre de plugins permettant d'ajouter des fonctionnalités et d'automatiser de nombreuses opérations (renommer, récupérer des métadonnées, copier...). Depuis le menu **Daemon** des **Paramètres**, il est possible de régler un port de connexion pour pouvoir agir à distance sur vos Torrents avec un navigateur et NoIP ou avec l'application Android Transdroid (www.transdroid.org).



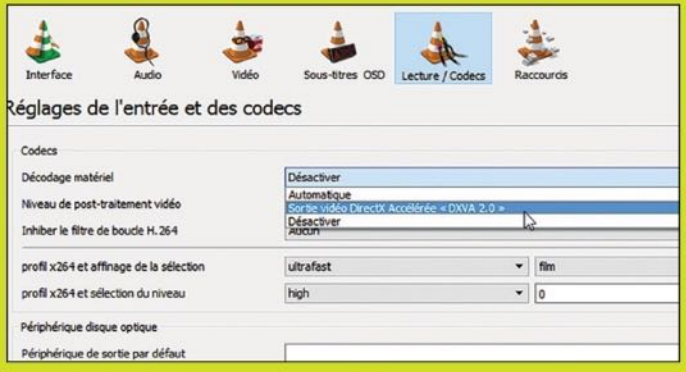
Difficulté : ☠☠☠

Lien : **http://deluge-torrent.org**

09# Regardez des vidéos en H.265

→ AVEC VLC

Le format vidéo H.265 propose une meilleure qualité d'image et de son. Pour lire un fichier de ce type avec VLC, assurez-vous d'abord d'en posséder la dernière version (**Aide > Vérifier les mises à jour**). Allez ensuite dans **Outils > Préférences > Lecture/Codecs** et cliquez dans la boîte de texte à droite de **Décodage matériel** pour choisir **Sortie vidéo DirectX Accélérée «DXVA 2.0»**. Validez avec **Enregistrer** et le tour est joué.



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

HACKING ALERT !

101 HACKS & ASTUCES
faciles détectés. Compatibles Windows.
Efficacité garantie.
Attention aux contrefaçons.

IDPRESSE id presse

L 14376 - 13 - F: 3,50 € - RD

BEL/LUX : 4,60 € - DOM : 4,70 € - PORT. CONT. : 4,60 € - CH : 6 FS - CAN : 6,99 $ CAD -
MAR : 43 MAD – TUN : 6,4 TND - NCAL/S : 650 CFP - POL/S : 660 CFP