N°17 - Juil. / Sept. 2018

LES DOSSIERS DU

Pirate

3,50€ seulement

TROUSSE À OUTILS ULTIME

BEST-OF 2018
LE GUIDE DU PIRATE

HACKING
SAUVEGARDE
MULTIMÉDIA
ANONYMAT

LES 99 MEILLEURS LOGICIELS GRATUITS

100% PIRATE // 100% ESSENTIELS

PROTECTION
OS ALTERNATIFS

+ TUTOS & ASTUCES ÉTAPE PAR ÉTAPE

SOMMAIRE

EN PARTENARIAT AVEC LES CAHIERS DU HACKER PIRATE [INFORMATIQUE]

ANTIVIRUS

HACKING

SAUVEGARDE

OS ALTERNATIFS

CHIFFREMENT

MULTIMÉDIA

LES DOSSIERS DU **Pirate**

N°16 - Juil. / Sept. 2018

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

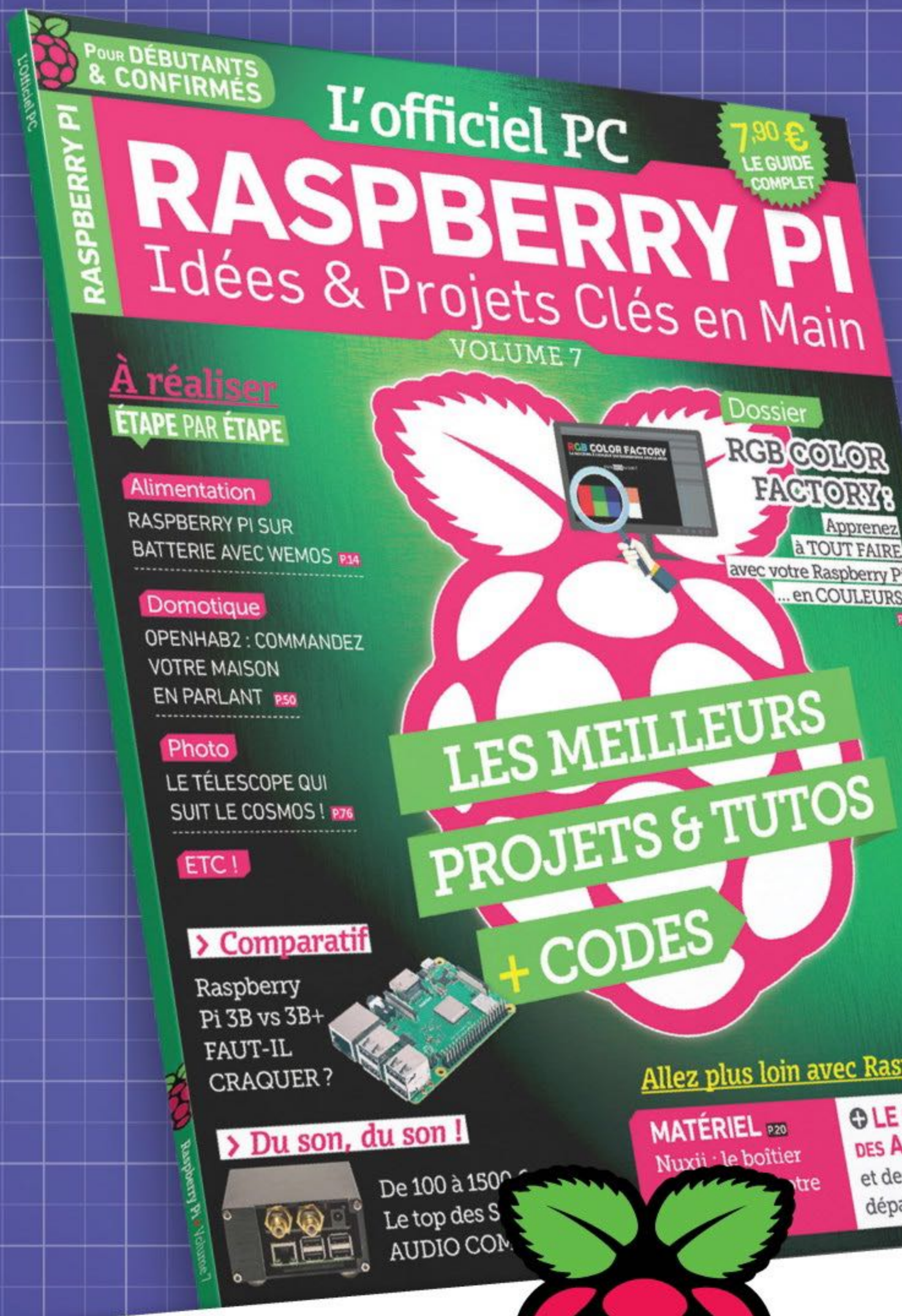
Directeur de la publication :
David Côme
Marlo : Benoît BAILLEUL
The corner kids : TP & YP
Snoop & Chris : Stéphanie Compain & Sergueï Afanasiuk
Correctrice :
Marie-Line Bailleul

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.

NOUVEAU !



Par l'équipe de *Pirate Informatique* !

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

GUIDE COMPLET

CHEZ VOTRE MARCHAND DE JOURNAUX

RGPD :
ATTENTION AUX MALINS !

No n non ne partez pas ! Nous savons que vous en avez un peu marre de ces 4 lettres (dans l'ordre ou dans le désordre), mais nous n'allons pas vous demander de cliquer sur quoi que ce soit. Nous souhaitons juste vous éclairer sur ces dizaines ou centaines d'e-mails que vous avez reçus récemment. Mais au fait, c'est quoi le RGPD ?

Alors oui vous en avez mangé pendant tous les mois d'avril et de mai, mais nous allons vous décrypter la chose. De quoi nous parlons ? Du RGPD bien sûr ! Le règlement général sur la protection des données (ou encore GDPR, de l'anglais General Data Protection Regulation) dans son nom complet. Car vous n'avez pas pu passer à côté de ces quantités d'e-mails vous invitant à renouveler votre confiance ici et là, et même à des sites donc vous ne vous souvenez plus : une boutique où vous avez acheté un jeu vidéo il y a deux ans, un institut de beauté où vous ne mettez plus les pieds, une chaîne de pizzeria où vous aviez participé à un concours en 2015, une salle de sport, le site où vous commandez le plein de fioul, etc. En bref tout un historique de vos habitudes de consommation sur Internet vient se rappeler à votre bon souvenir…

OPT-IN/OUT ? LES EXCEPTIONS

Le RGPD prévoit 2 exceptions pour lesquelles l'obtention du consentement n'est pas obligatoire.

1. Pour les contacts B2B, c'est à dire des adresses e-mails professionnelles et à condition que la prospection soit en rapport avec l'activité exercée par le destinataire
2. Pour vos clients existants, à condition que vos communications portent sur des produits ou services en rapport avec ce qu'ils ont déjà acheté précédemment

PETIT RAPPEL

OPT-OUT : pratique consistant à inscrire d'office un utilisateur à une liste après une inscription à un service, en lui laissant la charge de se désinscrire.

OPT-IN PASSIF : pratique consistant à obtenir le consentement d'un internaute de manière détournée, le plus souvent en pré-cochant la case correspondant au souhait de recevoir des e-mails de la part de l'entreprise.

OPT-IN : pratique consistant à laisser l'internaute exprimer librement son consentement par une action positive, généralement en cochant de lui-même une case correspondant au souhait de recevoir des e-mails de votre part.

DES TONNES D'INFORMATIONS

Eh oui, tous ces gens ont des informations sur vous : nom, âge, adresse, profession peut-être. Imaginez si une personne centralise ces différentes données… Mais ces e-mails, de quoi il s'agit ? Et surtout pourquoi on vous «spamme» depuis des semaines pour au final vous dire qu'on veut vous respecter et vous donner l'occasion de vous laisser tranquille ? Il s'agit d'une nouvelle réglementation appliquée depuis le 25 mai dernier afin de remplacer une ancienne directive française de 1995, qui a pour objectif de renforcer la protection des données. Il n'y aura donc plus de fragmentation des lois nationales en ce qui concerne la protection des données, mais une seule règle partout dans l'Union. Encore plus fort, ce règlement s'applique aux entreprises établies en dehors de l'Union européenne dès qu'elles proposent des biens et services à des résidents européens (voir notre encadré).

FAITES LE CYBER-MÉNAGE !

Concrètement cela veut dire que les sites que vous visitez devront vous octroyer un droit à l'effacement et bannir le profilage (ne pas faire l'objet d'une décision fondée sur un

traitement automatisé). Ils doivent en outre obtenir votre consentement «explicite» et «positif» pour une éventuelle collecte de données. Pour l'internaute, il faudra être patient et bien relire les conditions d'utilisation des données et surtout de les accepter...ou pas. Ces innombrables e-mails que vous recevez, ne les ignorez pas : si les boutiques ou services ne vous intéressent plus, faites le cyber-ménage ! La plupart du temps il suffit de cliquer sur un lien, de dire «non» ou de résilier votre partage de données personnelles. Notez que le RGPD est là pour mieux vous informer et non pas pour arrêter la collecte !

MAIS ATTENTION AUX FILOUS !

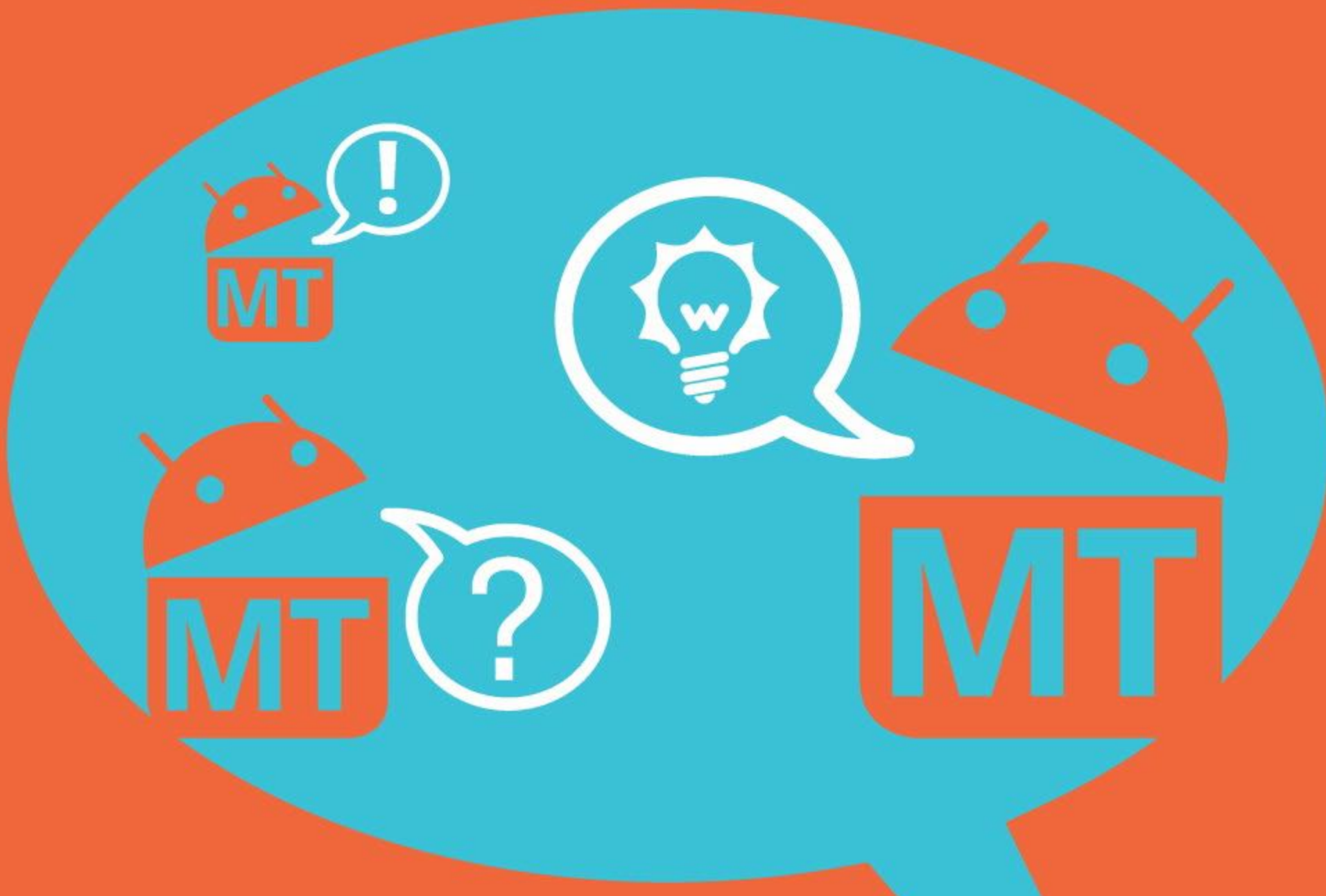
Mais attention, certains malins en profitent pour obtenir votre consentement alors qu'ils étaient dans l'illégalité ! En effet, le RGPD conserve tout consentement donné auparavant à une entreprise. Imaginons par exemple que vous vous soyez inscrit à une newsletter. Lors de votre inscription, vous avez dû confirmer votre adresse et donner votre consentement. Pour les responsables de cette newsletter, pas besoin d'obtenir à nouveau ce consentement si vous avez eu un contact avec eux durant

les 3 dernières années. Dans le cas contraire, les responsables, sans nouvelles de vous, doivent supprimer vos informations. Or, quand un vendeur de chaussures sur lequel vous avez acheté des baskets il y a 6 ans vous recontacte avec un mail de la RGPD, il s'agit d'une manœuvre pour à nouveau avoir le droit de vous solliciter sans craindre l'amende de l'UE (celles-ci pourront s'élever jusqu'à 4% du chiffre d'affaires mondial d'une société). En revanche, si elle a toujours respecté les règles européennes en matière de «traitement des données à caractère personnel», énoncées en 1995, elle n'a pas besoin de vous redemander votre accord. Le souci c'est que de nombreuses sociétés ne savent souvent pas comment elles ont obtenu ces informations vous concernant : changement de propriétaire, d'infrastructure, de responsable, etc. Dans le doute, elles demandent donc à nouveau votre consentement...

Libre à vous de dire oui, non ou de laisser couler.

UN MUR VIRTUEL POUR LES ~~MEXICAINS~~ EUROPÉENS !

Quand nous avons pris connaissance de ce service, nous avons cru à une blague, mais c'est au contraire très sérieux. Le problème avec la RGPD, c'est que si les grands groupes étrangers se sont préparés pour être «prêts» à se conformer à cette directive européenne, ce n'est pas le cas de millions de petites entreprises (qui utilisent souvent des outils pré-configurés pour collecter des informations à but commercial) qui ne veulent/peuvent pas se mettre en conformité. C'est ainsi que s'est créé le site **https://gdpr-shield.io**. Le but est simple : si votre site ne vise pas un public européen, pourquoi dépenser des sommes folles pour sa mise en conformité ou risquer une amende ? La solution : bloquer les internautes européens ! Se comporter comme un petit despote c'est facile avec GDPR Shield ! Bien sûr c'est ridicule, car on voit mal l'Europe porter plainte contre un site Web basé en Arizona qui vend des pendentifs à 5 dollars. Selon Isabelle Falque-Pierrotin, directrice de la CNIL, le but est d'«*accompagner la montée en apprentissage des acteurs pour que ceux-ci se mettent en conformité et non de gérer un tableau de chasse des sanctions*». Sauf que pour les gens mal renseignés et très pro-américains, GDPR Shield présente bien en proposant un service payant qui ne les force pas à réfléchir. Une sorte de mur virtuel pour les Mexicains d'Internet que nous sommes...



LE FORUM
DE LA COMMUNAUTÉ
Android MT

forum.android-mt.com

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

L'INFORMATIQUE FACILE POUR TOUS !

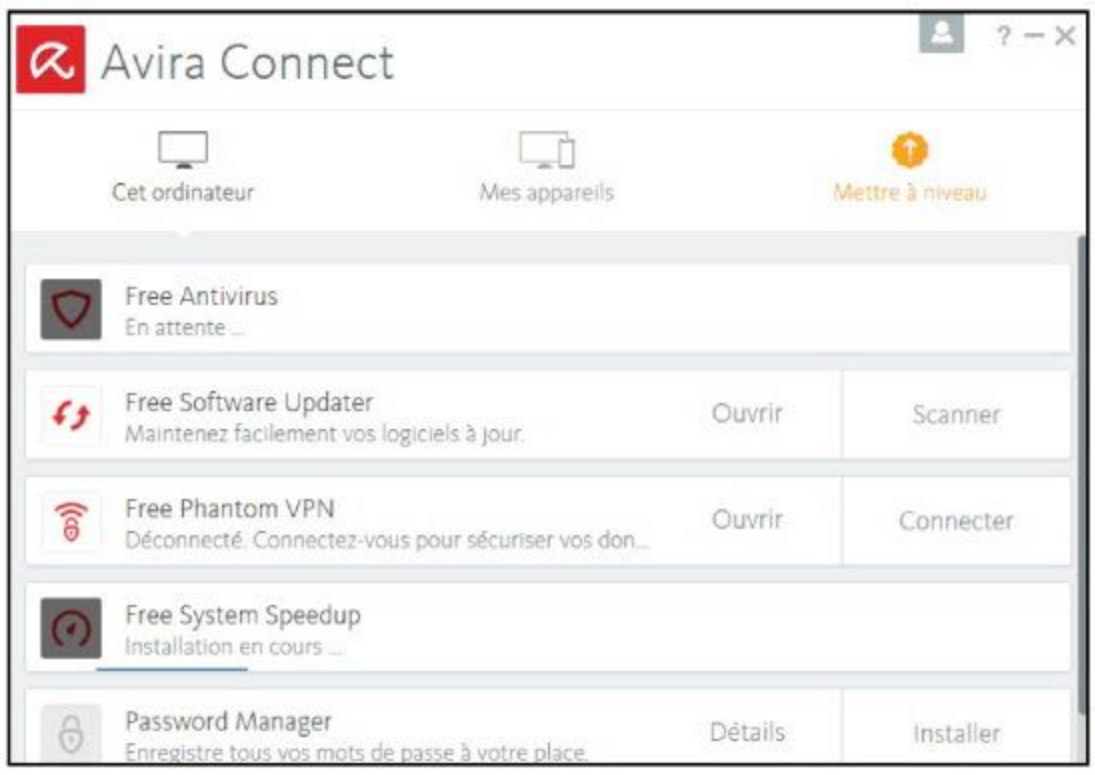
CHEZ VOTRE MARCHAND DE JOURNAUX

ANTIVIRUS

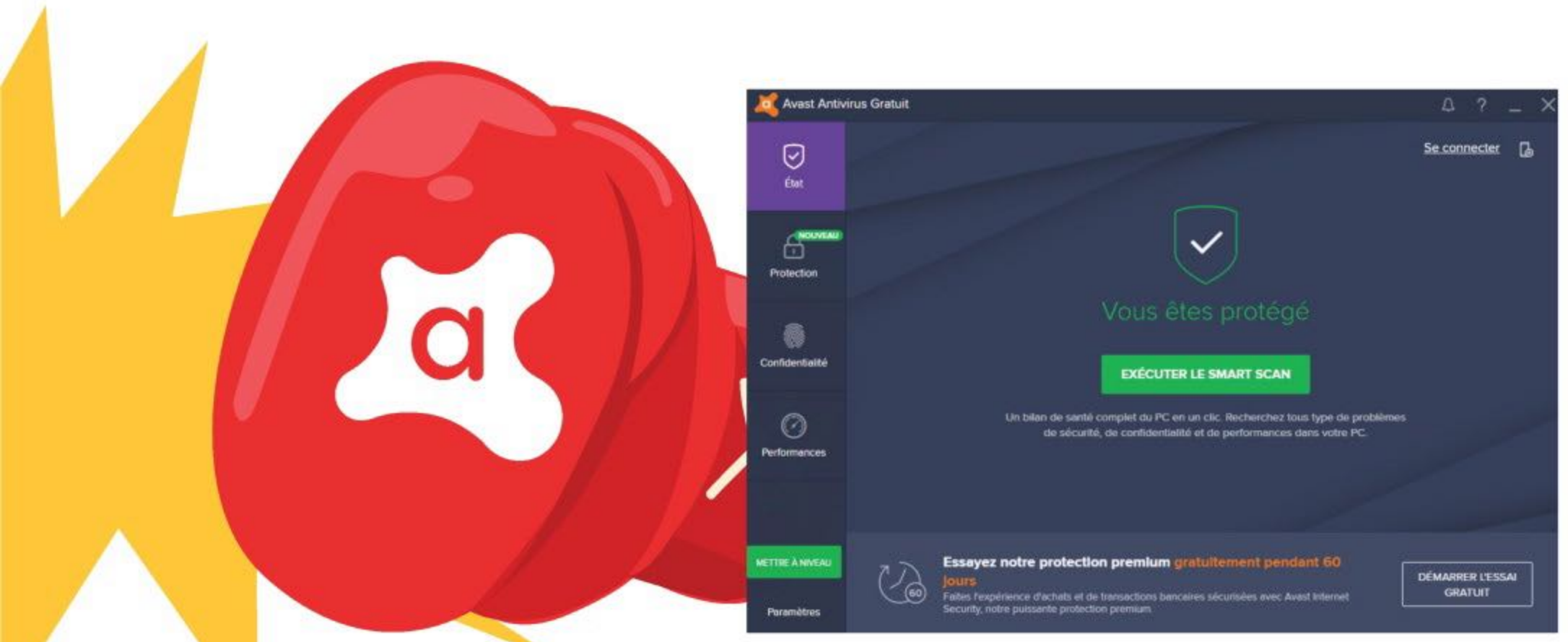
AVAST VS AVIRA : LEQUEL CHOISIR ?

Au royaume des antivirus gratuits, deux solutions surnagent. Avast et Avira sont les plus plébiscités par les utilisateurs qui souhaitent protéger leurs ordinateurs ou mobiles, le tout sans bourse déliée. On vous aide ici à choisir le plus adapté à votre machine et à vos habitudes de navigation sur la toile. Plus loin, nous verrons quelles solutions alternatives, autres que les antivirus, existent pour préserver vos bécanes des menaces.

Les deux antivirus seront comparés sur 5 critères au total. Premièrement leur facilité d'installation. Vient ensuite l'interface. Si cette dernière est complète, se laisse aisément apprivoiser. Le test se focalise ensuite sur l'impact du fonctionnement du logiciel antivirus sur les performances de votre bécane. Car oui un scan antivirus influence la réactivité de l'appareil. Enfin, dernier critère, et non des moindres, le niveau d'imperméabilité du soft face aux menaces.
Avast, pour commencer, est très facile à installer, il suffit de lancer l'exe pour débuter le processus. Seul hic ! Ce dernier propose quantité d'agents (nettoyeur de navigateur, extension de navigation, un VPN...) en plus de ses solutions antivirus habituelles (protection face aux



L'installation d'Avira se fait très facilement et nécessite moins de bidouille.



La simplicité d'Avast prend l'avantage par rapport au côté usine à gaz d'Avira.

fichiers, mails, sites frauduleux...). Mieux vaut passer par une installation personnalisée pour éviter de s'encombrer.
Avira de son côté vous propose en sus de ses services de protection, un VPN et un outil d'optimisation. Des services annexes qui s'activent/désactivent très facilement.
Du côté de l'interface, Avast offre un menu principal aéré, très visuel qui permet en un clic de lancer un scan ou de contrôler le niveau de protection. Les outils de scan et autres sur Avira sont un peu mieux cachés et présupposent l'ouverture d'une nouvelle fenêtre en plus de celle de base si vous souhaitez les lancer.
Sur le plan de la réactivité face aux menaces et de l'impact sur les ressources de votre bécane, Avast tire son épingle du jeu. Les mises à jour sont faites automatiquement. Si une menace est détectée, un simple pop-up vous le signale, l'antivirus fait alors son office, sans ralentir votre système. Il en est de même pour les scans manuels que vous effectuez. Le logiciel est beaucoup plus léger qu'à son lancement il y a de ça quelques années, mais aussi plus performant.
De son côté Avira jouit également d'une vitesse de détection des menaces record. Le principal écueil du soft reste qu'il demande beaucoup de ressources. Notamment lorsque vous lancez des scans profonds. Pour plus de réactivité, pensez à désactiver les modules qui vous sont inutiles (Password Manager, Safe Shopping...).
Pour l'impact sur les performances, sa simplicité d'utilisation ou encore sa réactivité face aux menaces, Avast se détache d'une courte tête dans ce comparatif. Il conviendra tant aux utilisateurs débutants qu'aux pros souhaitant protéger leur système efficacement. Avira de son côté reste une excellente alternative.

Configurez Avast ou Avira

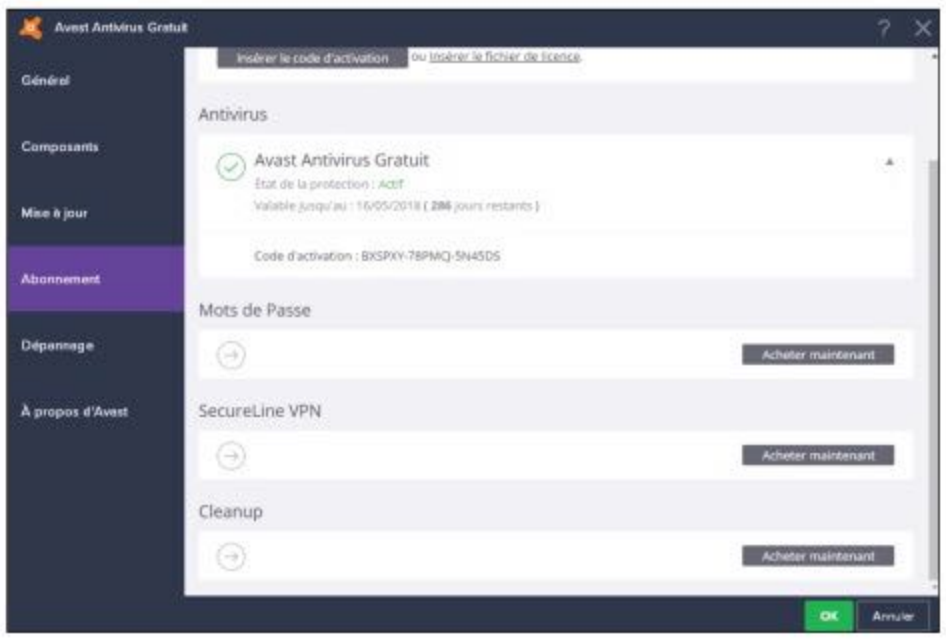
INFOS [AVAST & AVIRA]
Où le trouver ? [**www.avast.com ; www.avira.com**] Difficulté :
TUTO

01› INSTALLER AVAST

Lancez l'installation d'Avast et cliquez sur **Personnaliser**. Pour choisir vous-même les éléments désirés. Pour une protection efficace, mais peu envahissante, nous vous conseillons d'installer uniquement les quatre agents : **Agent des fichiers**, **Agent actions suspectes**, **Agent Web** ou encore **Agent de messagerie**. Vous pouvez ici **Changer** le dossier d'installation en pointant vers celui de votre choix. Validez avec **Installer**.

02› S'ENREGISTRER

Avast requiert un enregistrement (gratuit) pour fonctionner plus de 30 jours. Cliquez sur **Paramètres** en bas à gauche puis sur **Abonnement** et **Enregistrez-vous maintenant**. Cliquez sur le bouton **Sélectionner** de gauche (le gris) et entrez une adresse mail avant de valider. Choisissez **Non merci** sur le pop-up s'ouvrant juste après et fermez le tout avec **OK**. Vous voilà libre d'utiliser le soft gratuitement et de profiter de sa protection

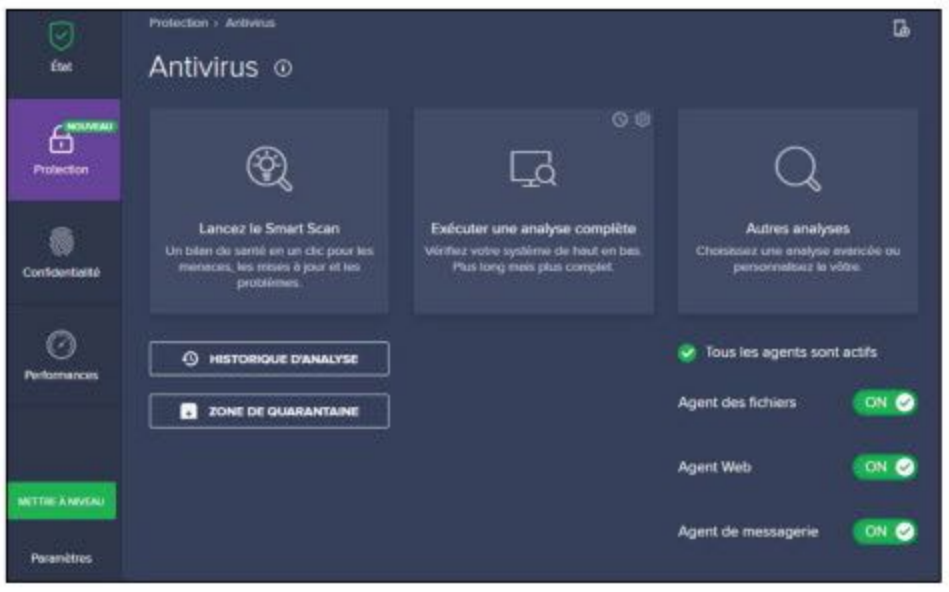


03› RENDRE AVAST DISCRET

Pour éviter qu'Avast ajoute une signature à vos mails, allez à **Paramètres** > **Général**, décochez **Activer la signature d'e-mail Avast**. Allez ensuite dans **Composants** et cliquez sur **Personnaliser** à droite d'**Agent Mail** puis **Autres paramètres**. Décochez les cases sous **Général**, sauf la dernière. Autre point : Avast parle, et c'est plutôt gênant. Cliquez sur **Paramètres** > **Général** > **Sons** pour décocher **Activer les sons Avast** pour faire taire l'antivirus.

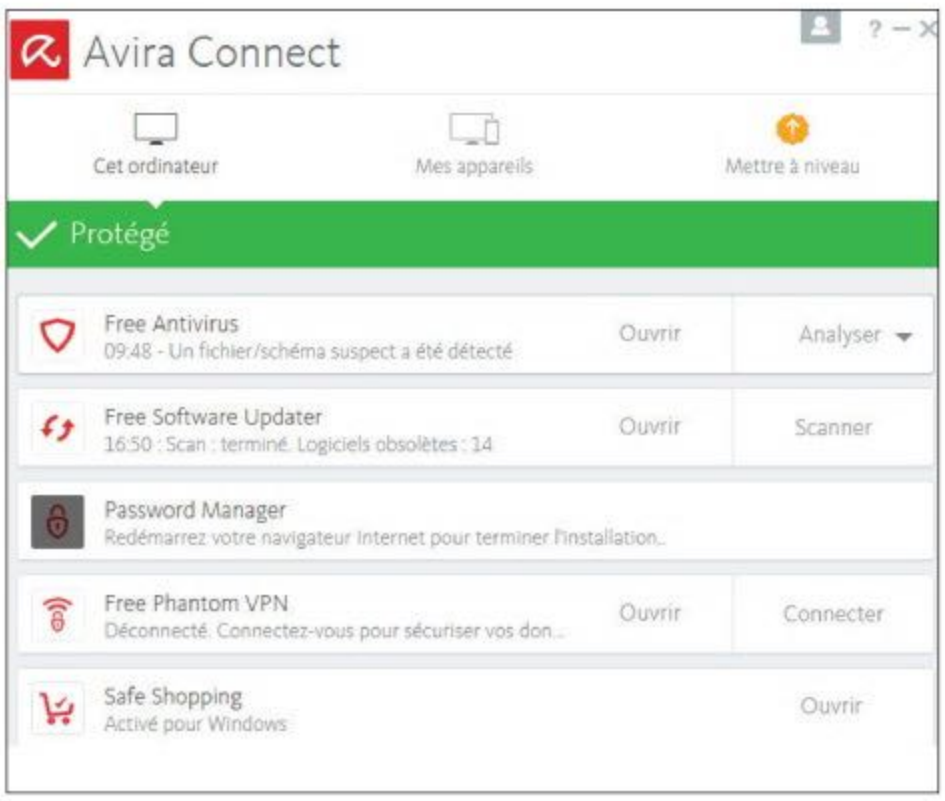
04› SCANNER

Depuis la fenêtre principale du logiciel, choisissez **Exécuter le Smart Scan** pour effectuer une analyse rapide de votre système. Si des menaces sont identifiées, elles sont automatiquement placées en quarantaine. Pour lancer des scans plus en profondeur, allez dans l'onglet **Protection** puis ouvrez le menu **Antivirus**. Choisissez d'**Exécuter** une analyse complète pour scanner les moindres recoins de votre bécane à la recherche de menaces.



05› CONFIGURER AVIRA

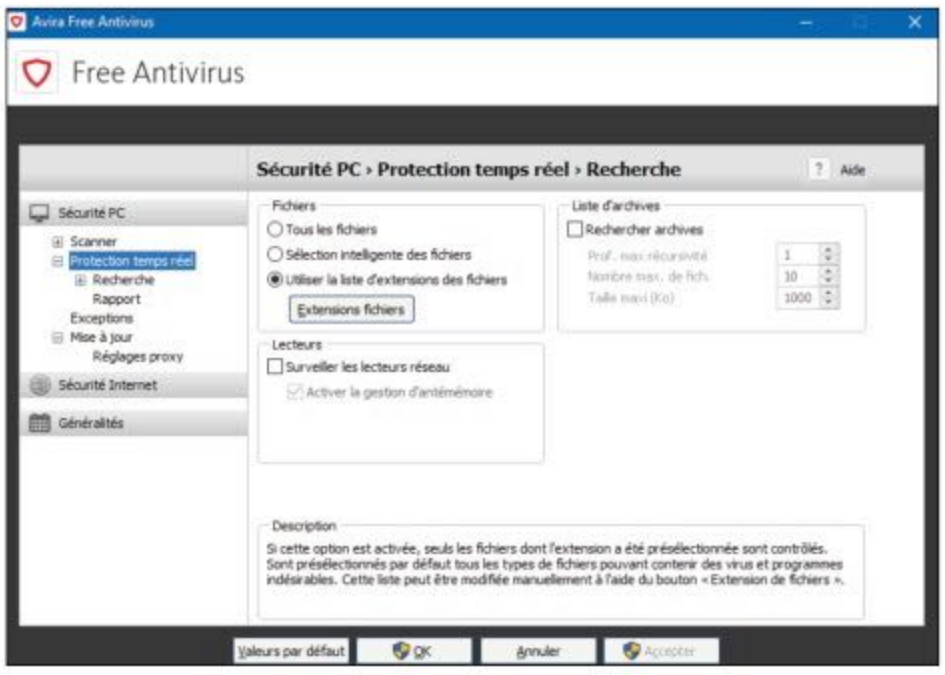
Qu'il s'agisse de la version gratuite ou d'une des payantes, faites attention de décocher la case correspondant à l'installation de l'inutile **SearchFree Toolbar**, une toolbar qui ne sert qu'à encombrer vos navigateurs Web. Dès le



premier lancement, Avira va chercher les dernières signatures de virus et faire une mise à jour. Lancez votre premier **scan** en choisissant **Analyser** sur la ligne **Free Antivirus**.

06› CONFIGURER

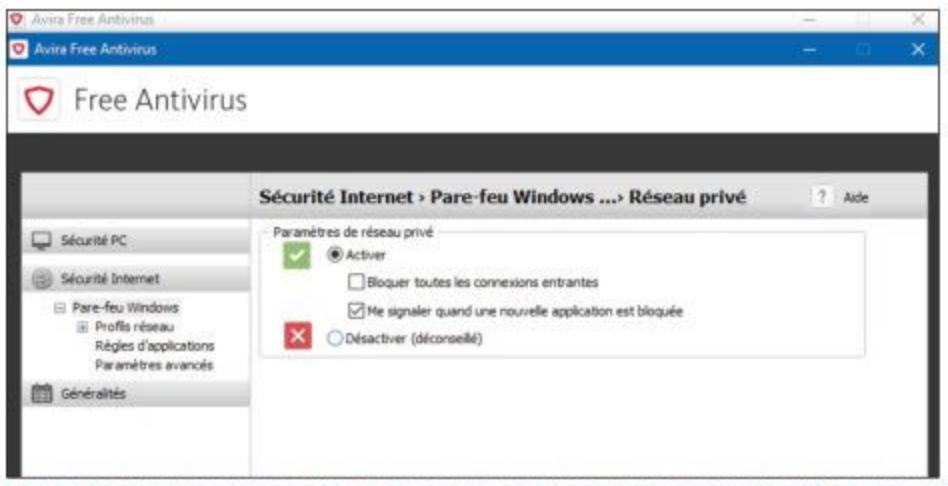
Vous accédez aux services fournis par les différents modules en choisissant **Ouvrir** sur celui à solliciter. Pour **Free Antivirus**, c'est ici que vous accédez aux paramètres et que vous ajustez les différents réglages. Cliquez sur les petits rouages pour accéder aux options avancées de chaque outil



du module. Par exemple pour Free Antivirus, c'est ici que vous réglez le rythme des mises à jour, que vous rajoutez des exceptions de dossier à ne pas scanner...

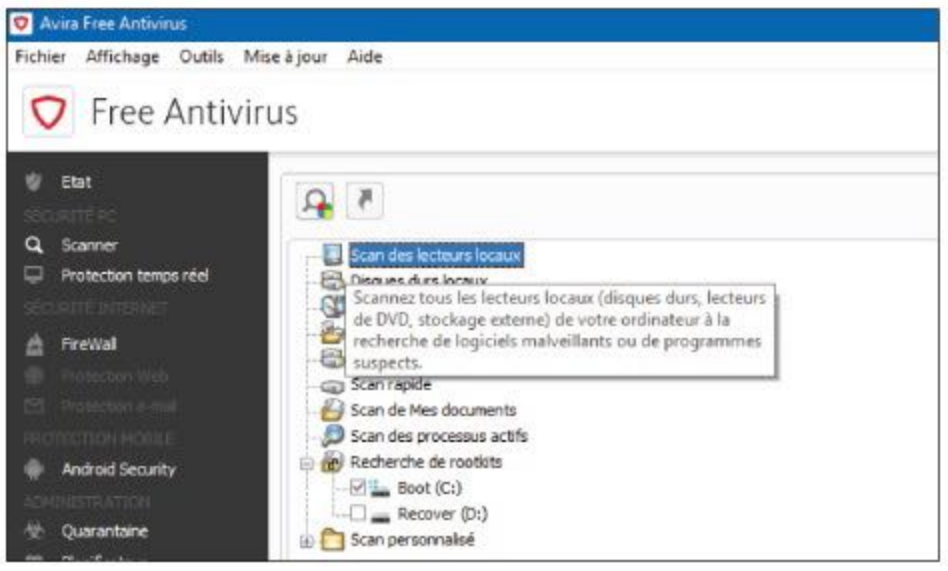
07› EXPLORER LES PARAMÈTRES AVANCÉS

La liste des options dans les paramètres est très longue. Il est par exemple possible de régler la priorité de la fonction scanner (par rapport aux autres processus), les actions à accomplir en cas d'infection, la spécification d'un mot de passe pour éviter que vos enfants ou un pirate ne désactivent vos protections, etc. Malgré tout, les débutants n'auront pas à s'arracher les cheveux puisque tout est facile à configurer.



08› CHANGER DE SCAN

Outre le scan principal abordé dans l'étape 1, Avira dispose de quantité d'autres outils pour rechercher les menaces sur votre appareil. Faites **Ouvrir** sur **Free Antivirus** pour aller dans **Scanner**. Présélectionnez un scan puis lancez-le avec l'icône de la loupe en haut. Patientez jusqu'à la fin du scan pour traiter les menaces éventuelles et les envoyer en quarantaine.



ANTIVIRUS

Virus Total
→ Un scan en ligne

Nous vous parlons souvent de sites qui permettent de scanner un ordinateur en ligne à la recherche de malwares. Le problème, c'est que la plupart du temps il faudra tout de même télécharger un module ce qui est impossible si vous n'êtes pas administrateur. Si vous n'êtes pas sur votre poste ou si vous êtes au travail (et que l'«informaticien» vous a recommandé d'utiliser un Norton jamais mis à jour), allez sur le site Virus Total. D'ici, vous pourrez scanner des pièces jointes (maximum 64 Mo), mais aussi demander l'analyse d'une URL (cliquez sur le lien en bas) ou directement chercher dans la base de données virales en cas de doute.

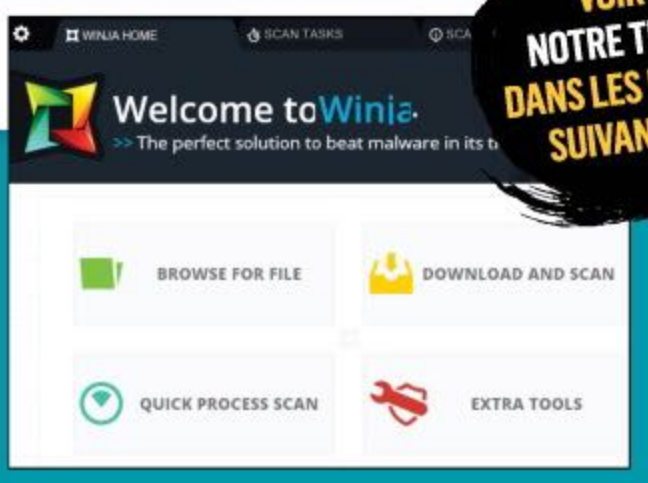
Difficulté : Lien : **www.virustotal.com**

Ransomware File Decryptor → Antidote

Le principe des ransomwares est simple, mais coquin. La plupart du temps, ces vils virus chiffrent vos documents et fichiers perso et vous promettent restitution de ces derniers en l'état... à condition de passer à la caisse. Le logiciel que nous vous proposons ici est l'antidote permettant de récupérer vos données en les déchiffrant. Vous piochez dans la liste le ransomware qui vous a contaminé puis vous le laissez travailler. Vous récupérez ainsi vos fichiers dans l'état où ils étaient avant la contamination.

Difficulté :
Lien : **https://goo.gl/th7Gxx**

Winja → Surveiller les contaminations



VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

Winja soumet le fichier louche de votre choix à une batterie de tests effectués par plus d'une cinquantaine d'antivirus en ligne. Le programme vérifie le niveau de dangerosité du fichier stocké sur votre bécane, ou d'un que vous vous apprêtez à télécharger. Si par ailleurs un processus inconnu venait à se lancer dans votre gestionnaire des tâches, Winja ira faire sa petite enquête en sondant sa base de données pour vous rassurer. D'autres outils sont de la partie : surveillance des tâches planifiées, des processus au démarrage...Ce logiciel édité par Phrozen est un complément à votre antivirus préféré.

Difficulté : Lien : **https://goo.gl/DSX9RA**

Surveillez les menaces avec Winja

INFOS [WINJA]
Où le trouver ? [**www.phrozensoft.com**] Difficulté :

TUTO

01› EXPLORER L'INTERFACE

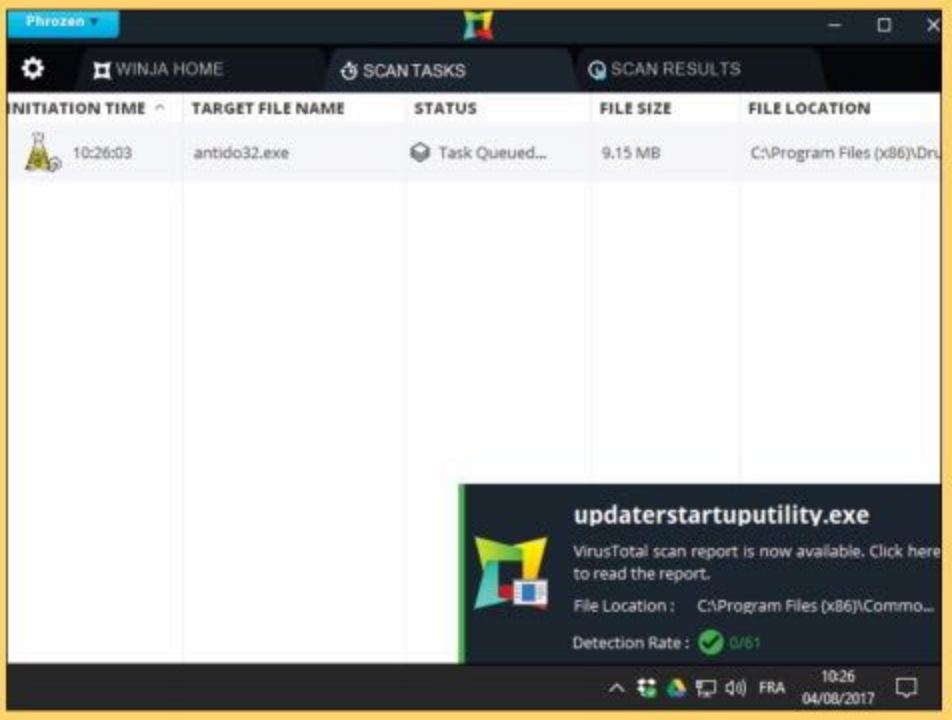
Procédez à l'installation du soft en suivant notre lien. Relancez Winja. L'interface s'affiche avec ses outils. En vert vous ouvrez le fichier déjà présent sur votre PC, en jaune vous scannez un fichier en ligne, en bleu vous sondez les processus actifs et le rouge ouvre les outils complémentaires. Ces derniers doivent être lancés en mode administrateur.

02› SCANNER AVANT DE TÉLÉCHARGER

Vous êtes sur un site de téléchargement légal et on vous propose de récupérer un fichier EXE ? Pourquoi prendre un risque ? Depuis votre navigateur préféré, faites un clic droit dans le bouton de téléchargement et faites **Copier l'adresse du lien** (ou équivalent). Dans Winja, allez dans **Download and Scan** puis copiez ce lien pour cliquer à nouveau sur **Donwnload and Scan**. Patientez jusqu'au verdict.

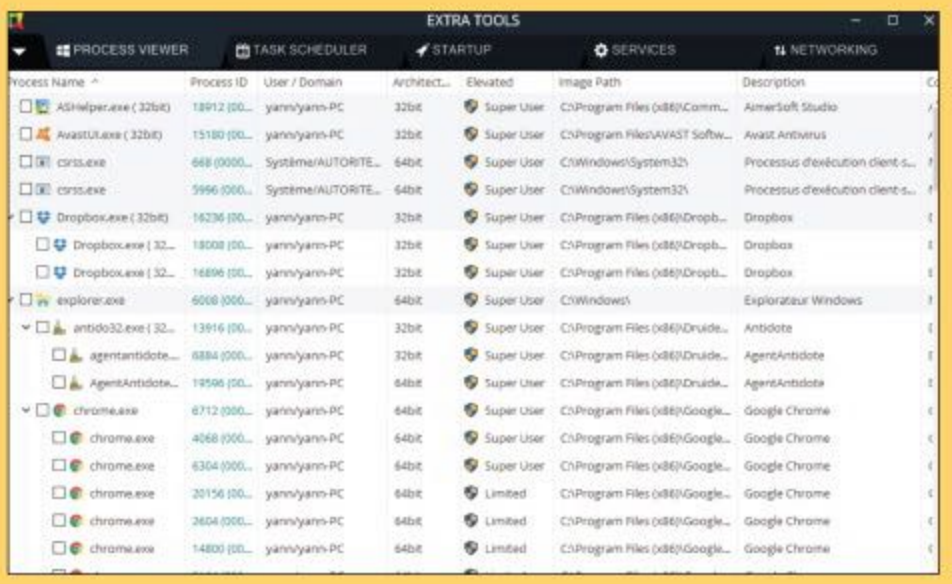
03› SCANNER LES PROCESSUS

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



04› UTILISER LES OUTILS

Explorez les **Outils supplémentaires** (**Extra Tools**) pour un scan plus précis des processus, des tâches planifiées de Windows (qui peuvent être utilisées par des virus), des programmes qui se lancent au démarrage de Windows, des services de Windows ou encore de votre réseau Internet.



ANTIVIRUS

LEXIQUE

MALWARE :

C'est le terme générique pour désigner les logiciels malveillants. Un malware peut être un virus, un vers, un trojan, un ransomware, etc.

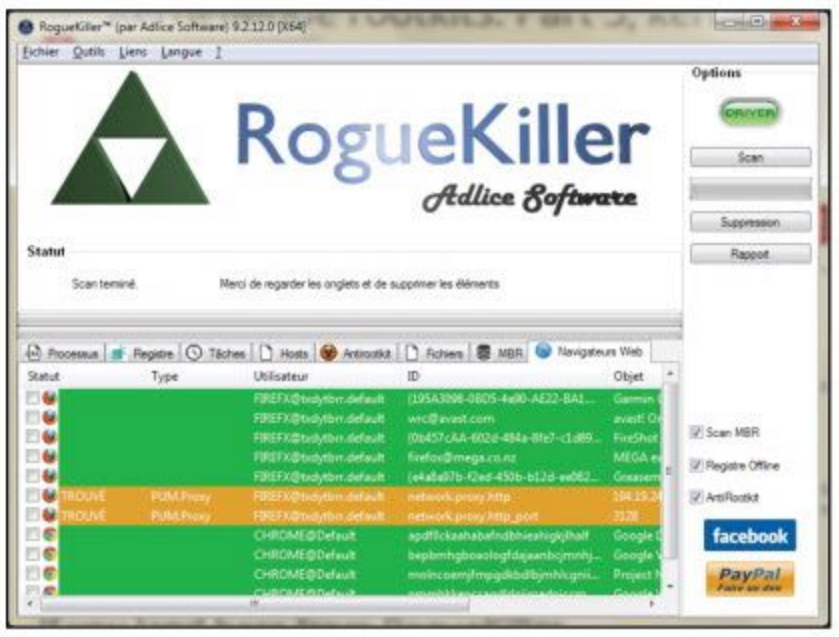
ROGUEWARE :

Les roguewares sont de faux antivirus créés par des petits filous pour faire de l'argent sur la crédulité des internautes. Tout commence par une infection bénigne, le rogue s'installe sur votre ordinateur, mais ne détruit rien du tout. Au bout de quelques minutes, vous verrez un pop-up qui vous indique qu'une menace est détectée sur votre ordinateur. Bien sûr cette menace est imaginaire et pour supprimer ces infections, vous devez passer à la caisse !

BOOT :

Ou "amorce" en français. Il s'agit du démarrage d'un ordinateur. Généralement, le PC "boot" sur le disque dur pour démarrer Windows, mais il est possible de démarrer un autre système depuis le lecteur de DVD ou un port USB. Un outil de désinfection comme AVG rescue CD par exemple...

RogueKiller → UN ANTI ROGUEWARE



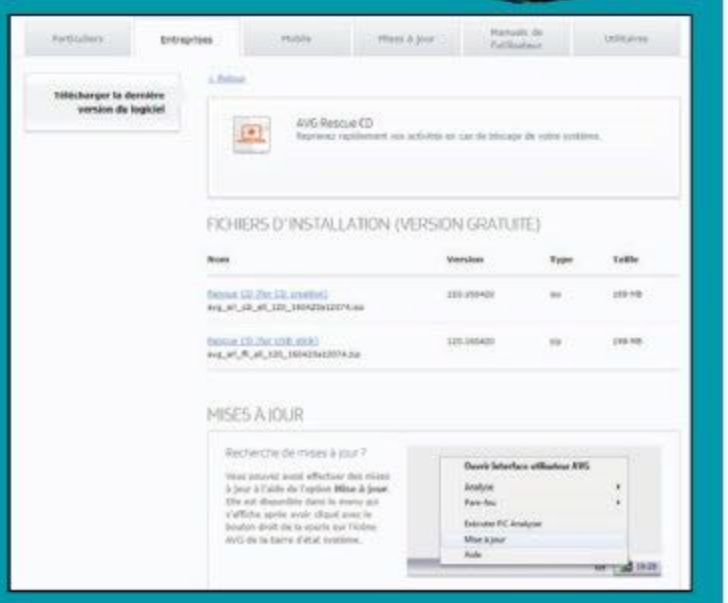
Les rogues sont de faux antivirus créés par des petits filous qui jouent sur la peur de la contamination pour vous soutirer de l'argent... RogueKiller est un logiciel spécialisé dans la lutte contre ce type de menace. Il est régulièrement mis à jour et pourra vous éviter bien des frayeurs.

Difficulté : ☠☠☠ Lien : **http://goo.gl/Qn6Jpk**

AVG Rescue CD

→ LE CD DE LA DERNIÈRE CHANCE

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES



Si votre PC est tellement infecté et que votre antivirus ne peut rien faire. Avant de formater ou de réinstaller un nouveau système, tentez de résoudre le problème avec cette solution d'AVG à graver ou à placer sur clef USB. Le CD de désinfection va se lancer avant même que l'OS se charge. Lorsque ce dernier n'est pas démarré, vous aurez le champ libre pour soigner en profondeur votre bécane. Analyse approfondie, nettoyage des cochonneries, récupération d'infos de démarrage supprimées... un utilitaire à garder bien précieusement.

Difficulté : ☠☠☠ Lien : **https://goo.gl/H2aec7**

AVG Rescue CD : le mode d'emploi

INFOS [AVG RESCUE CD]
Où le trouver ? [**https://goo.gl/H2aec7**] Difficulté : ☠☠☠

TUTO

01› LE CHOIX DE LA VERSION

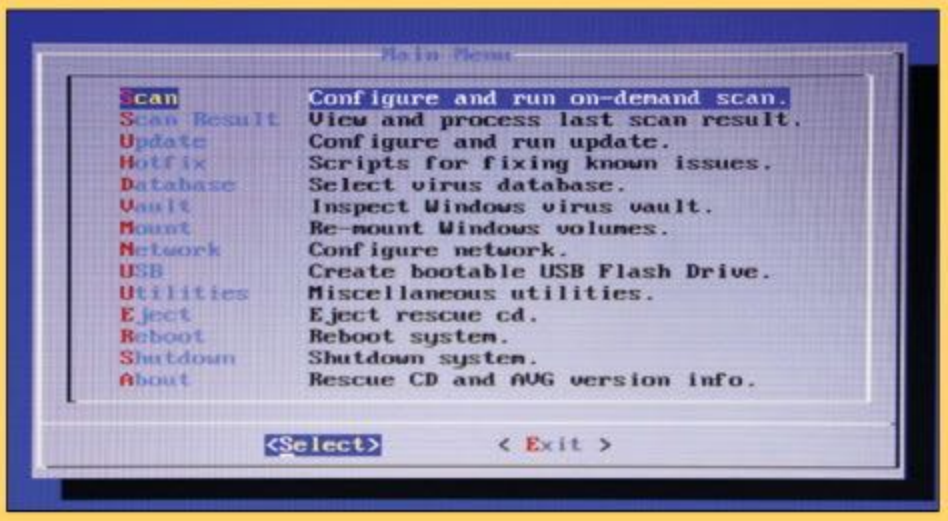
Sur la page d'AVG Rescue CD, cliquez sur **Téléchargement gratuit** et choisissez la version qui vous convient le mieux. Dans un logiciel gratuit comme CDBurner XP, gravez le fichier ISO en choisissant l'option **Image disque ISO**. Nous avons choisi le fichier ISO prêt à être gravé, mais vous pouvez aussi prendre une version à installer sur clé USB (vérifiez bien, auparavant, que votre BIOS autorise le boot sur port USB).

02› LE «BOOT»

Une fois gravé, il va falloir demander au PC «malade» de démarrer sur le CD. Faites **Suppr**, **F1**, **F2** ou **F8** (en fonction de votre modèle de carte mère) juste après avoir allumé le PC et entrez dans le BIOS (**Setup**). Trouvez l'option **Boot Sequence** (qui peut aussi être sélectionnable avant même l'entrée dans les menus) et modifiez l'ordre en mettant en premier votre lecteur de CD/DVD. Si vous avez des difficultés, consultez la notice de votre carte mère ou jetez un coup d'œil sur Google avec le nom de votre matériel.

03› LE LIVECD EN ACTION

Dans le menu qui s'affiche, choisissez **AVG Rescue CD** et attendez que le contenu du CD se charge dans la RAM. Vous devriez avoir le menu principal avec l'accès à la mise à jour de la base de données virales (**Update**) et aux **Utilities** (gestionnaire de fichiers pour sauver vos données, éditeur de registre, test du disque dur, etc.). Débutez par une mise à jour et pour commencer votre scan, montez les partitions Windows (**Mount**). Choisissez ensuite **Scan**.



04› LES OPTIONS DU SCAN

Il faudra alors sélectionner les éléments à scanner : volume, répertoire spécifique ou secteur d'amorçage. Vous aurez alors différents types d'options à votre disposition : scan des archives, des cookies, méthode heuristique, etc. À vous de faire vos choix. Si vous ne connaissez pas l'origine du problème, optez pour une recherche en profondeur en sélectionnant toutes les options possibles dans **Scan Options** (scan des cookies, des archives, etc.). Validez lorsque vous êtes prêt et patientez le temps que le processus se termine.

ANTIVIRUS

MediCat → Trousse à outils

Problème de fichier Windows, d'infection, de RAM, de disque dur, de partition ou de mot de passe ? Plus besoin d'avoir toute une collection de Live DVD sur vous lorsque vous partez réparer l'ordi de vos proches en détresse. MediCat propose une compilation d'outils fréquemment mise à jour... MediCat est également un Live CD, mais il permet de faire la chasse aux virus, de restaurer un Windows bancal, de sauvegarder des données en cas de problème physique ou de mettre un peu d'ordre dans vos partitions. Une vraie solution de secours complète.

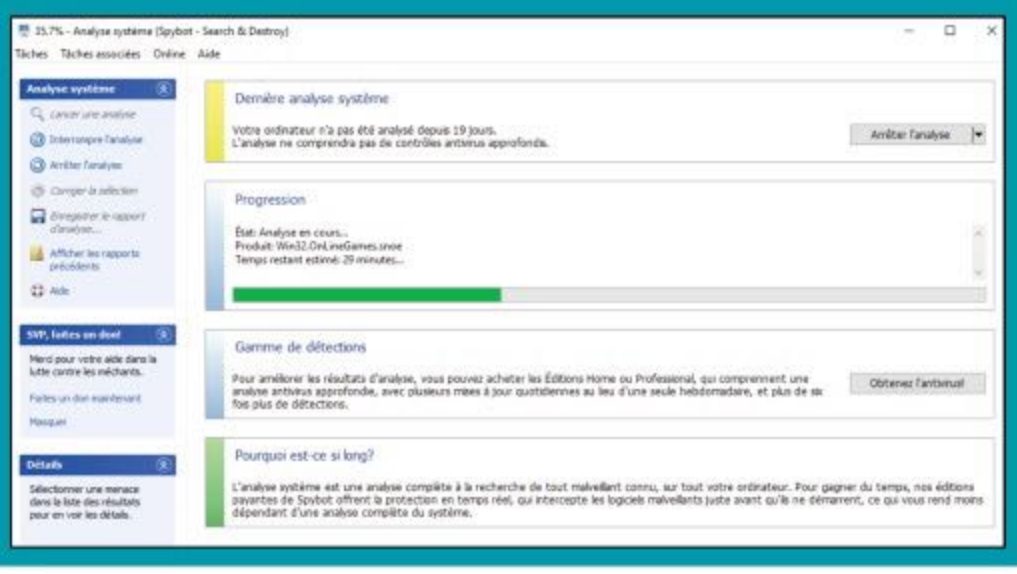
Difficulté : Lien : **https://goo.gl/Di4ht4**

Spybot Search & Destroy

→ Anti logiciels espions

Spybot Search & Destroy traque et supprime les spywares. Lancez le scan, un rapport vous informe des programmes suspects installés sur votre machine. En quelques clics, vous les supprimez. Les bases de données des logiciels espions sont régulièrement mises à jour. Il est recommandé de scanner votre ordinateur le plus souvent possible (toutes les semaines) pour repérer plus facilement les nouvelles menaces. Car s'ils ne sont pas aussi dangereux que les malwares pour la stabilité de votre système, ces programmes malveillants s'attaquent tout de même à votre vie privée et à vos données personnelles.

Difficulté : Lien : **https://goo.gl/4VXiPa**



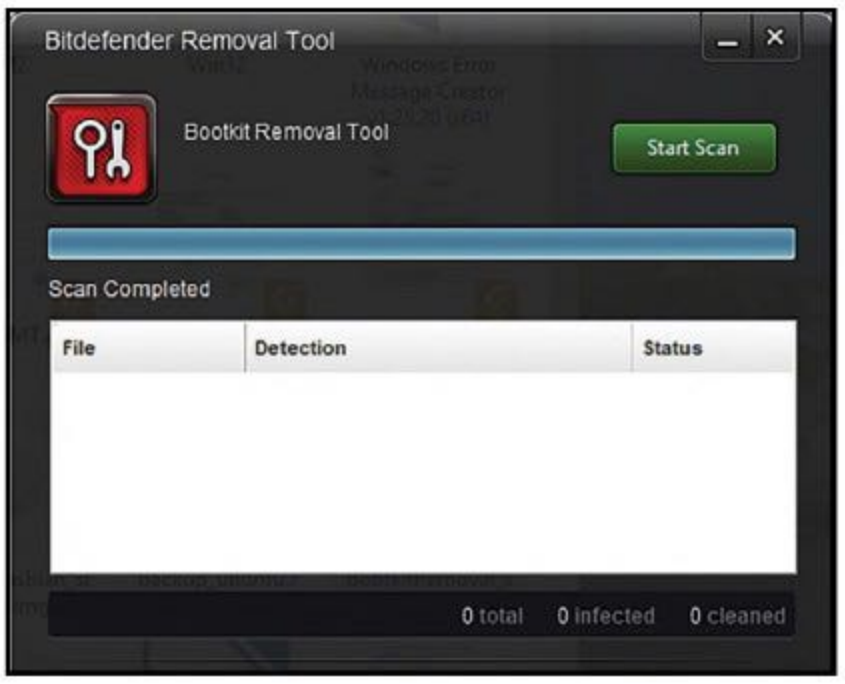
USB Immunizer

→ Protégez vos clés USB

Ce logiciel agit de deux manières. Il va en premier lieu vacciner votre système contre ces menaces en désactivant la fonction «autorun» de Windows. La version payante permet aussi d'immuniser vos clés USB/disques durs en créant à la racine du volume, un nouveau fichier Autorun.INF sain, mais surtout non modifiable par un programme quelconque. Vos périphériques seront donc immunisés lors de branchements sur des machines infectées.

Difficulté :

Lien : **http://labs.bitdefender.com**



NoMoreRansom → Sus au ransomwares !

Vous avez pu identifier le ransomware qui a attaqué votre système et qui maintenant réclame que vous passiez à la caisse ? Sur ce site, vous uploadez un fichier chiffré par le vil virus. NoMoreRansom sonde ensuite sa base de données pour vous proposer un antidote parmi quantité de logiciels. Notez que le site fourmille de pas-à-pas pour vous aider à vous débarrasser des ransomwares. Vous pouvez aussi signaler une menace identifiée sur votre bécane à l'équipe du site. Un moyen de lutter contre la propagation de ces cochonneries.

Difficulté : ☠☠☠

Lien : **www.nomoreransom.org**

Malwr → Analyse en ligne

Une alternative au scan de fichiers en ligne proposé par le logiciel Winja. De la même manière, depuis Malwr, vous interrogez la base de données du site pour savoir si le fichier Exe que vous vous apprêtez à installer est digne de confiance. Le site vous fournit ensuite un rapport détaillant le niveau de menace. Malwr utilise une sandbox à distance pour ouvrir et installer les malwares potentiels.

Difficulté : ☠☠☠

Lien : **https://malwr.com**

ZHP Cleaner → Contre le détournement de navigateur

Ce programme se concentre sur les menaces qui pourraient provenir de votre navigateur : les programmes pop-up affichant de la publicité intrusive, les pourriciels comme les toolbars ou autres qui viennent encombrer votre navigateur. ZHP Cleaner va rétablir les paramètres Proxy tout en supprimant les redirections de navigateurs. S'agissant d'un logiciel portable, vous pouvez l'emporter sur une clef USB pour l'utiliser sur une autre bécane. Lancez simplement le scan pour commencer à traiter les menaces éventuelles.

Difficulté : ☠☠☠

Lien : **https://goo.gl/Xvcvs4**

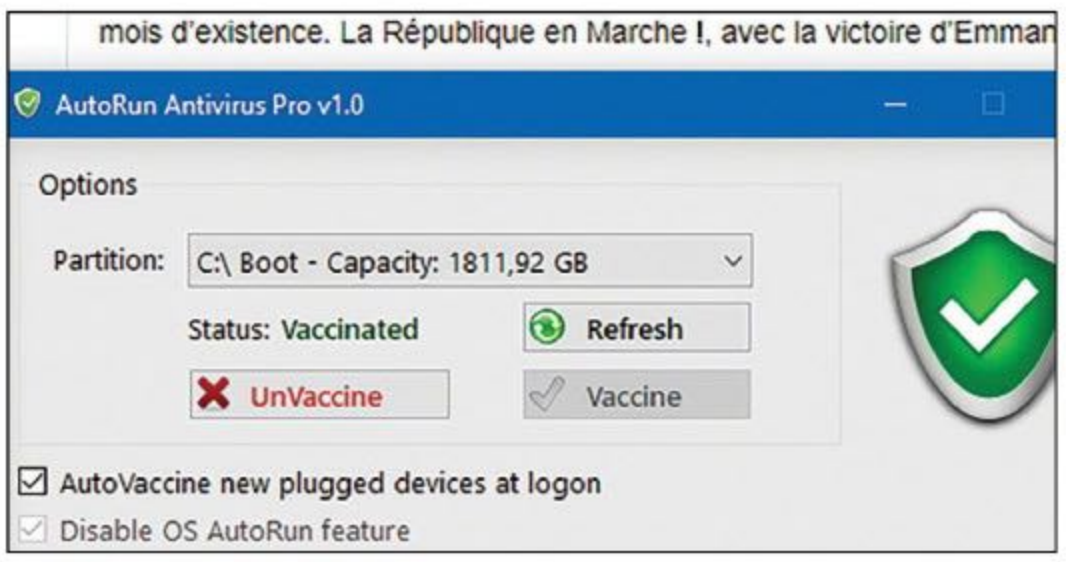
ANTIVIRUS

AutoRun Antivirus Pro

→ Bloquer les clés USB vérolées

Les virus appelés autorun s'invitent souvent dans les clefs USB ou les disques durs externes. Dès que vous connectez ces périphériques à votre bécane, ils entrent en action et contaminent votre système. La solution AutoRun Antivirus Pro permet de s'en protéger. Définissez le disque dur ou la partition à vacciner puis lancez l'opération. Notez qu'il est possible de régler la vaccination automatique de tout périphérique qui se connecte à votre PC. Pour vous protéger efficacement des appareils qui seraient branchés en votre absence.

Difficulté : Lien : **https://goo.gl/sR66QL**



LEXIQUE

ADWARE :
Programme malveillant qui va vous afficher de la publicité non désirée sur votre ordinateur. Ce type de logiciel n'est pas considéré comme un malware par votre antivirus, mais il ralentit le système et reste très pénible.

TROJAN :
Ou Cheval de Troie. Comme son nom l'indique, il s'agit d'un malware qui va s'inviter sur votre système en faisant le moins de vague possible. Il ouvrira cependant une porte dérobée sur votre ordinateur pouvant être utilisée par un pirate ou d'autre malwares.

AdwCleaner → Virer les toolbars et autres nuisibles

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

Ils polluent votre ordinateur, ralentissent vos navigateurs, se mêlent un peu trop de votre vie privée pour vous spammer de pubs. Ce sont les méchants adwares. AdwCleaner en fait son affaire. Ce logiciel gratuit les trouve et les supprime. Le tout en deux clics. Vous lancez un simple scan, le logiciel mouline avant de vous fournir une liste des indésirables installés sur votre machine. Vous les sélectionnez puis vous lancez la purge. Votre bécane redémarre et vous dresse ensuite un rapport détaillant les menaces éradiquées. Un programme très simple à utiliser qui ne nécessite aucune installation.

Difficulté : Lien : **https://goo.gl/3Gjk7p**

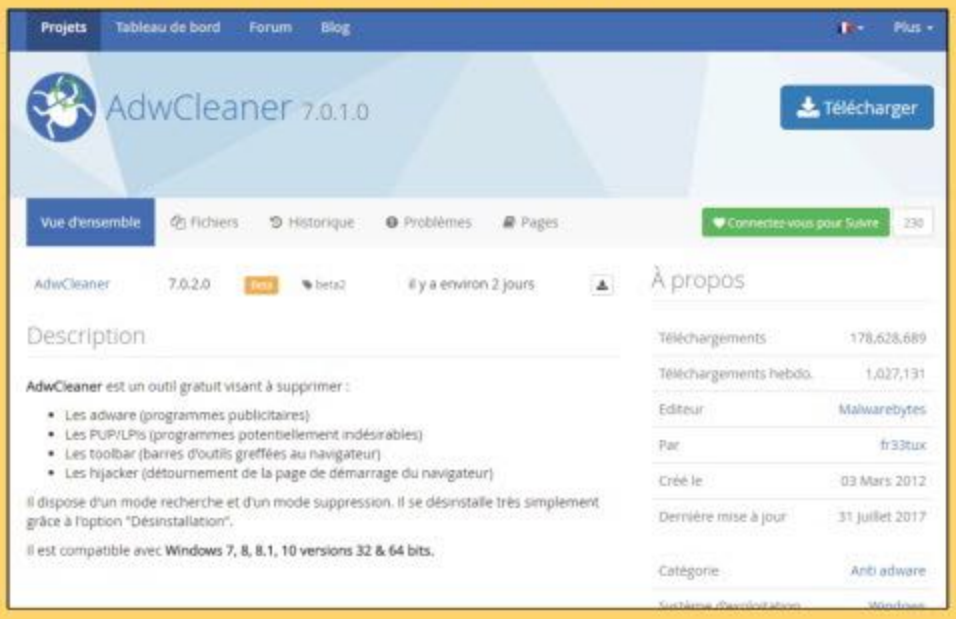
Éradiquez les adwares

INFOS [ADWCLEANER]
Où le trouver ? [**https://goo.gl/JNtBFZ**] Difficulté : ☠☠☠

TUTO

01› OBTENIR ADWCLEANER

Suivez le lien de téléchargement dans le bloc d'infos ci-dessus pour acquérir le soft. Choisissez **Télécharger** puis patientez jusqu'à obtenir le logiciel. Notez que le programme ne nécessite aucune installation. Placez le raccourci où bon vous semble (sur une clef USB, pour l'emporter partout avec vous). Faites un double-clic sur l'icône de raccourci pour lancer le logiciel.



02› SCANNER

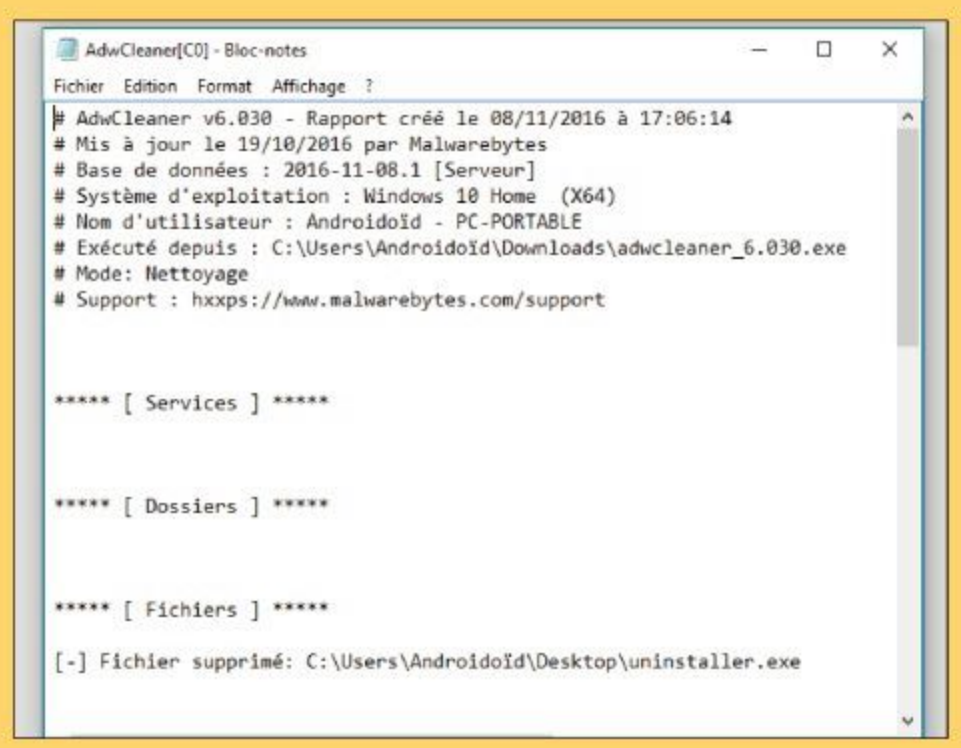
Faites **J'accepte** pour passer les conditions générales d'utilisation du logiciel. Pour préparer la suppression de tous les adwares, il faut d'abord les détecter. Cliquez sur **Analyser**. Patientez jusqu'à la fin du scan. Les menaces identifiées apparaissent dans les onglets **Fichiers** et **Registre**, dans le champ principal **Résultats**. Cochez les menaces que vous souhaitez éradiquer.

03› EFFACER

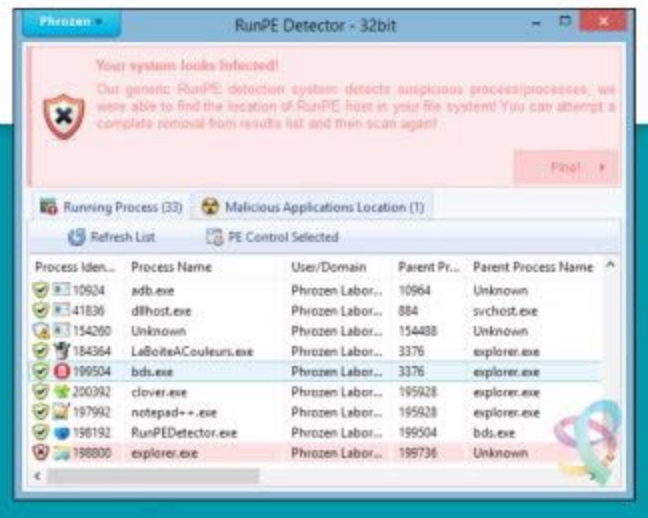
Cliquez maintenant sur **Nettoyer**. Le logiciel vous demande alors de fermer toutes les applications en cours et de redémarrer votre ordinateur. Sauvegardez tous vos travaux en cours puis faites **OK**. Il se peut que votre curseur disparaisse. Ne paniquez pas, pressez plusieurs fois la touche **Entrée** pour valider chaque fenêtre jusqu'au redémarrage du système.

04› APPRENDRE

Votre ordinateur est désormais tout propre comme en témoigne le fichier .txt qui s'ouvre au démarrage de Windows. Il ne vous reste plus qu'à appliquer les conseils prodigués par AdwCleaner : lisez bien les petits caractères lors de l'installation de chaque logiciel et, par précaution, décochez toutes les cases qui vous paraissent suspectes.



RunPE Detector → Un anti-RAT



RunPE Detector s'occupe de repérer la présence de malwares de type RAT (contrôle à distance, comme DarkComet). Ce type de logiciel malveillant va démarrer un processus légitime (souvent Firefox ou explorer.exe) pour le remplacer juste avant sa mise en mémoire par l'image mémoire du malware. Ce dernier profite de ces droits pour passer à travers les mailles du pare-feu. RunPE Detector va comparer l'empreinte du processus en mémoire avec son image physique. Si les différences sont avérées, l'alerte est donnée.

Difficulté : Lien : **www.phrozensoft.com**

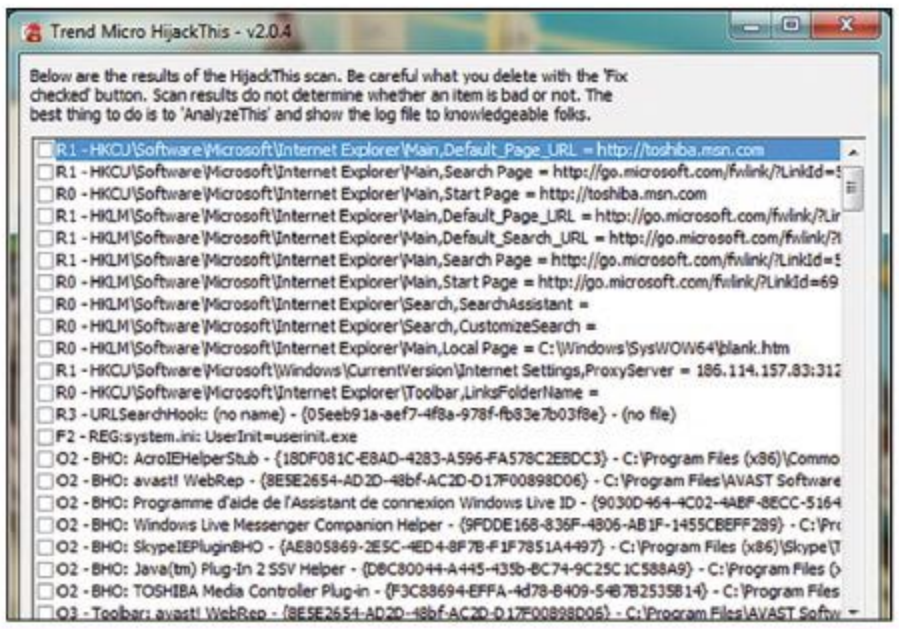
HijackThis

→ Contrôlez votre système

Ce logiciel s'adresse à tous ceux qui pensent (à tort ou à raison) être victimes d'attaque ou d'infection. HijackThis permet de localiser les programmes malintentionnés pour pouvoir ensuite les éliminer. Le logiciel ne nécessite aucune installation : il scanne votre machine puis rend son verdict sous forme de log (ou fichier journal). Attention, il ne s'agit pas d'un antivirus, mais d'un logiciel de contrôle.

Difficulté :

Lien : **www.hijackthis.de**

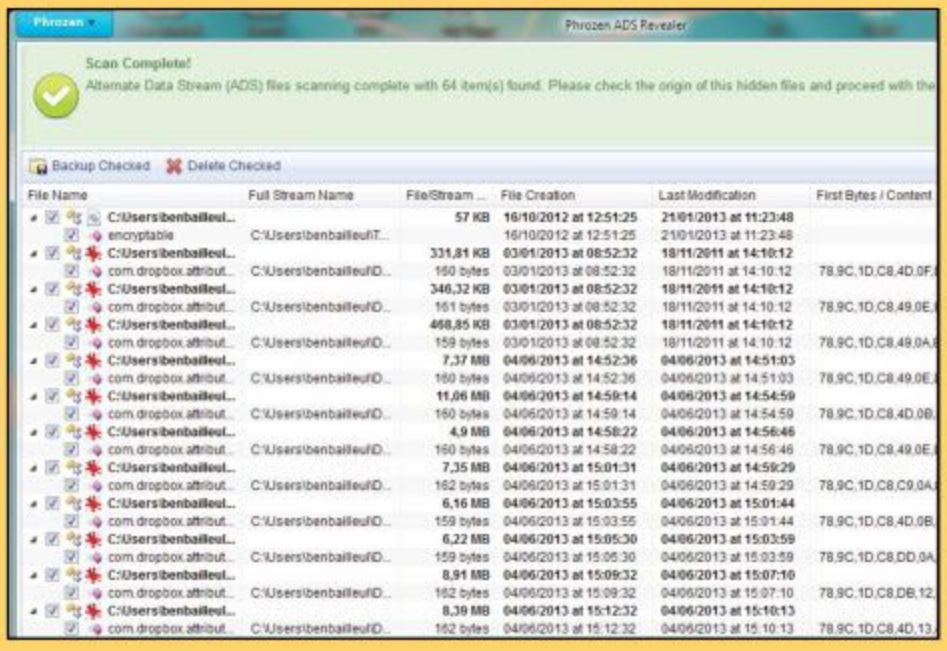


ADS Revealer → Contre les fichiers ADS frauduleux

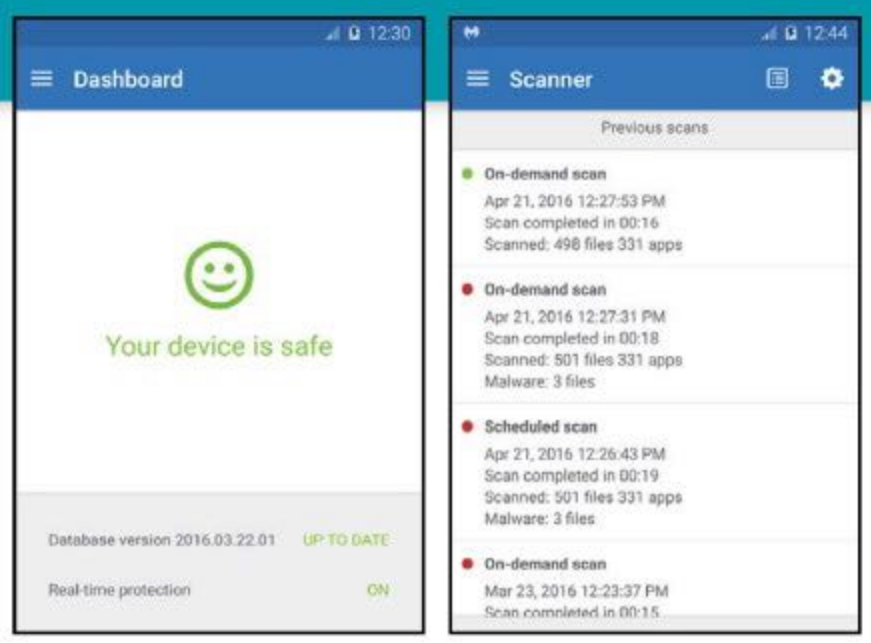
Phrozen ADS Revealer détecte la présence de fichiers cachés pouvant être des malwares sur les volumes NTFS : les fichiers ADS. Ces derniers, bien qu'invisibles depuis l'explorateur de fichiers Windows, ont un contenu bien physique et peuvent pulluler sans éveiller les soupçons de l'utilisateur. Le développeur du logiciel a même prouvé que malgré les restrictions de Microsoft, il est toujours possible d'exécuter du code directement à partir d'un emplacement ADS...

Difficulté :

Lien : **www.phrozensoft.com**



Malwarebytes → Antimalwares



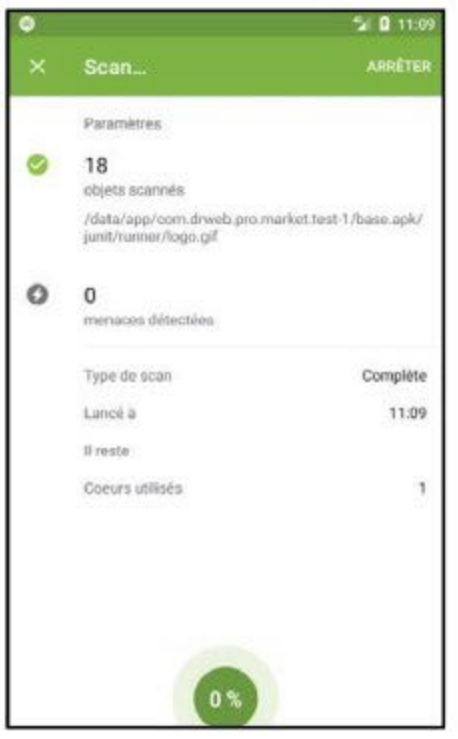
Bien connu des utilisateurs PC, l'antimalwares Malwarebytes se décline également en version pour terminaux mobiles Android. Gratuit à l'installation et à l'utilisation, il offre tout un panel d'outils pour se protéger des éventuelles menaces liées à vos activités sur le Web, depuis votre smartphone ou votre tablette. Détecteur de spywares et de trojans, scan pour détecter des applications potentiellement nuisibles, détecteur de failles de sécurité, contrôle des permissions des applications, scans de carte SD... très complet.

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

Anti-virus Dr.Web Light → Antivirus léger

Les antivirus ont la fâcheuse tendance d'utiliser beaucoup de ressources. Dr Web a le mérite de tourner sans solliciter à outrance votre mémoire vive. La navigation reste fluide, vous profitez de votre Androphone plus longtemps. De plus, tous les outils indispensables sont là (protection en temps réel, scan, antivirus, antimalwares, détection de fichiers suspects sur votre carte SD...). Efficace et économique.

Difficulté : Lien : **https://goo.gl/8NBMpv**



F-Secure Mobile Security → Antivirus et contrôle parental

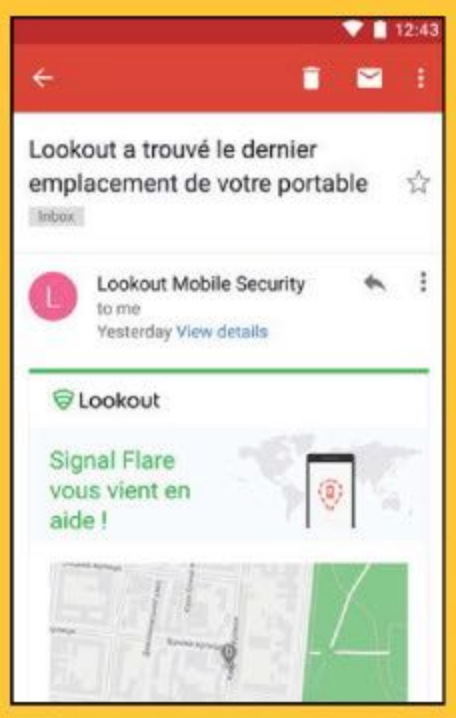
F-Secure est sans doute l'une des solutions de protection les plus complètes disponibles sur le Google Play Store. En plus d'une protection résidentielle pour lutter contre les malwares, elle vous offre un filtre parental pour le Web. Vous éviterez ainsi à vos enfants d'aller sur des sites au contenu inapproprié. Très facile à paramétrer et complètement gratuite, elle offre une protection efficace contre les fichiers vérolés que vous pouvez rencontrer en surfant sur le Web, depuis votre mobile.

Difficulté :

Lien : **https://goo.gl/3SPDJA**

Lookout

→ Antivirus et antivol



LookOut est un antivirus avec une partie dédiée aux applications qui ont accès à vos données personnelles (contacts, messages et localisation). Il permet aussi de sauvegarder les données de votre téléphone sur un serveur distant (contacts e-mail, photos, numéro de téléphone, etc.) Plus fort, il sait où votre téléphone se trouve si vous le perdez, fait émettre une sirène (depuis votre ordinateur, en se connectant au service) et en cas de vol il permet de bloquer le contenu ou de le supprimer d'un seul clic.

Difficulté : ☠☠☠

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

Mobile Security & Antivirus → Protection pour Android

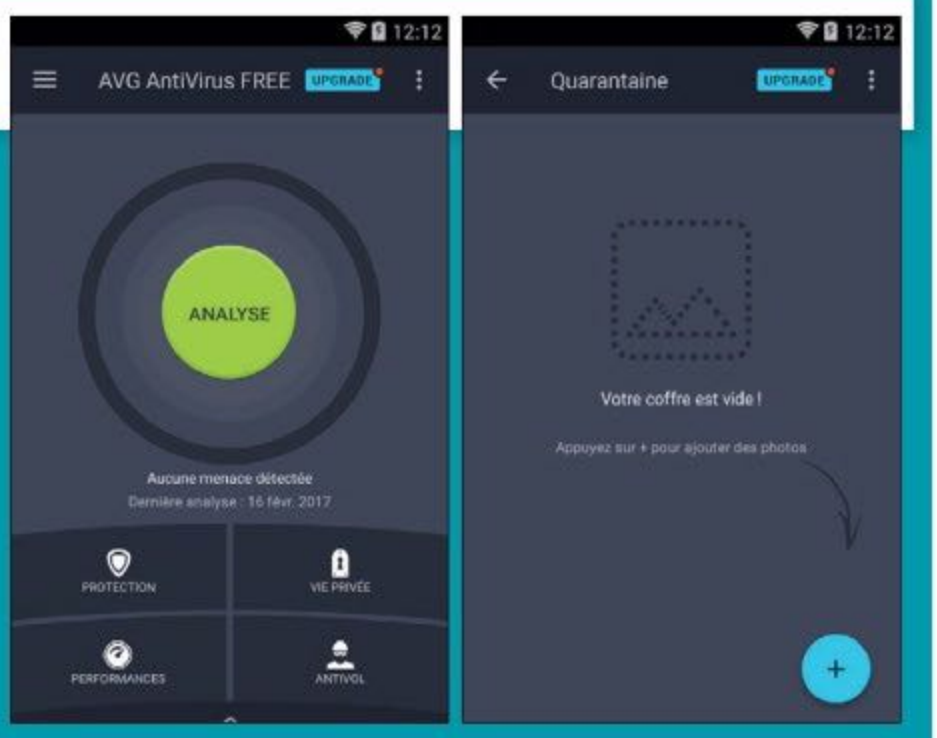
Votre PC est équipé de l'antivirus Bitdefender ? Vous en êtes satisfait ? Pourquoi ne pas essayer la protection pour mobiles et tablettes que propose la marque Bitdefender ? Vous retrouverez l'essentiel des outils indispensables (antimalwares, antivol, protection en temps réel) pour rendre votre appareil sûr à 100 %. Une version Premium (et donc payante) permet d'accéder à d'autres fonctionnalités (comme le contrôle de données).

Difficulté : ☠☠☠

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

AVG → Antivirus complet

La solution d'antivirus AVG pour les appareils Android permet de se protéger efficacement de toutes les menaces potentielles. En plus de la protection classique (virus, malwares, trojan...), l'application bloque les appels ou les messages suspects et propose même un tueur de tâches. À noter qu'un antivol est aussi de la partie. Pratique pour localiser et bloquer son mobile à distance (en cas de vol).



Difficulté : ☠☠☠ Lien : **https://goo.gl/C5cipe**

Le nouveau site
des utilisateurs
ANDROID

- Des dizaines de tutoriels et dossiers pratiques
- Mobiles & Tablettes : des tests complets !
- Sélection des meilleures applis + des vidéos et du fun !

Android MT

Solutions & Astuces

www.android-mt.com

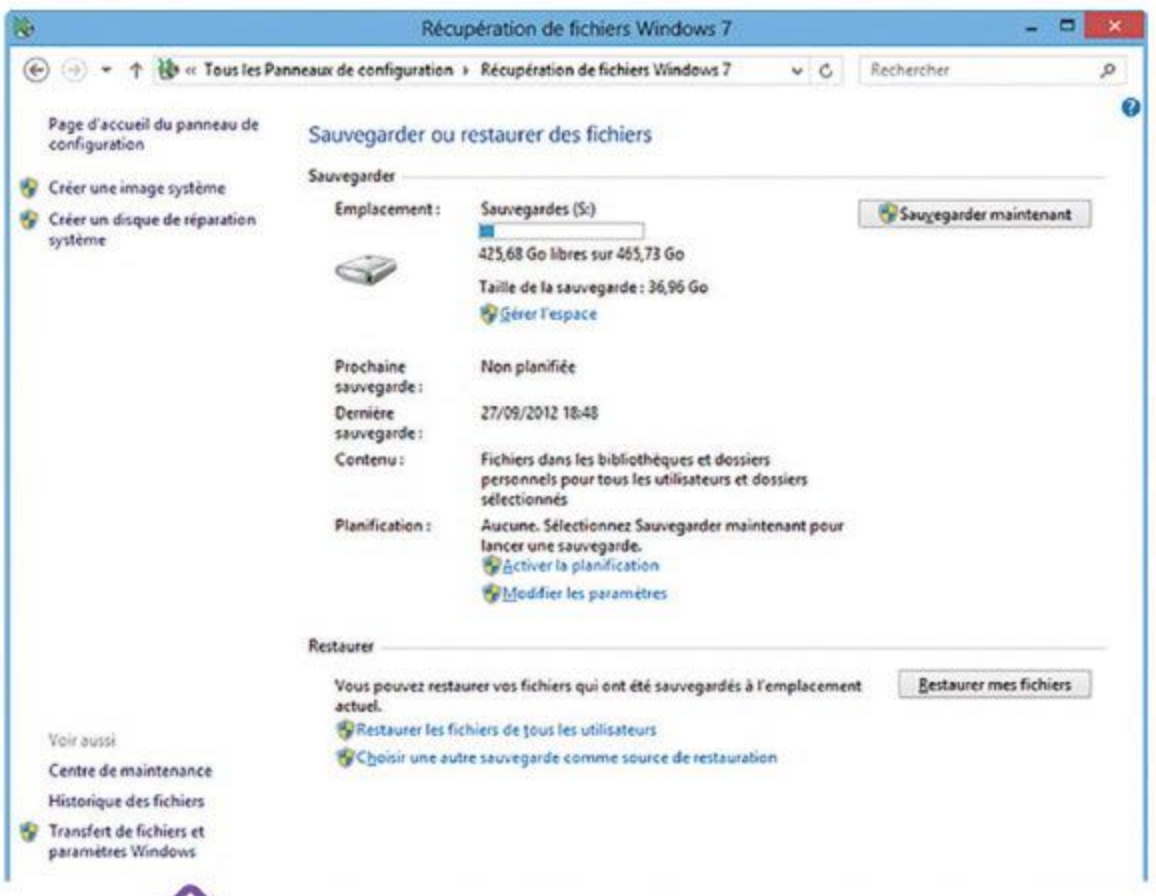
IL REVIENT !

SAUVEGARDE

TOUT POUR SAUVEGARDER VOTRE SYSTÈME

Avec la quantité de données et de souvenirs présente sur nos ordinateurs et nos smartphones, il faut aimer le goût du risque pour ne pas sauvegarder ses fichiers. Si vous avec une partition de libre, une clé USB ou un disque dur de grande capacité, pourquoi ne pas automatiser cette tâche ?

Même si Microsoft a fait des progrès depuis Vista, le module de sauvegarde de Windows manque encore un peu d'options et d'ergonomie pour les utilisateurs pointilleux que nous sommes : pas de chiffrement et pas de clonage de disque au programme. Si l'on compte aussi l'impossibilité d'accéder aux détails des fichiers, le module de Microsoft est un peu à la traîne. Ici, nous parlons de sauvegardes sécurisées, chiffrées, et paramétrables (tout le système, certains dossiers, quelques fichiers...). N'occultons pas complètement l'outil Windows, qui reste une solution simple et efficace, mais sachez que les outils présentés dans les pages suivantes sont beaucoup plus puissants, pour peu que vous acceptiez de changer un peu vos habitudes. Deux sortent particulièrement du lot : EaseUS Todo Backup et Cobian Backup, son concurrent direct. Après vous avoir expliqué leur fonctionnement, nous vous présenterons d'autres programmes intéressants, puis nous nous occuperons de la sauvegarde sur mobile Android.



L'outil de sauvegarde de Windows est clair et pratique mais pour les utilisateurs pointilleux que nous sommes, il existe des solutions gratuites proposant plus de fonctionnalités... Notez que même sous Windows 10, c'est le programme de Windows 7 qui vous sera proposé. Étrange, non ?

SAUVEGARDE

EaseUS Todo Backup → La référence

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

Même dans sa version Free, EaseUS Todo Backup est complet : sauvegarde d'un disque ou d'une partition, d'un groupe de dossiers, du système, planification, sauvegarde sur le réseau, sur un NAS ou un cloud (Google Drive, OneDrive ou Dropbox) et clonage complet de vos disques. Le logiciel permet aussi de créer un disque bootable pour restaurer les données préalablement sauvegardées. Si vous désirez stocker sur des CD ou des DVD, Todo Backup va fractionner votre sauvegarde en paquets de 650 Mo, 700 Mo ou 4,7 Go. Mais ce n'est pas tout. Todo Backup peut aussi effacer de manière sécurisée une partition, créer un disque d'urgence en cas de crash (Linux ou WinPE) et vérifier l'intégrité des différentes images de disque que vous aurez créées.

Difficulté : ☠☠☠ Lien : **goo.gl/7VvNFt Difficulté**

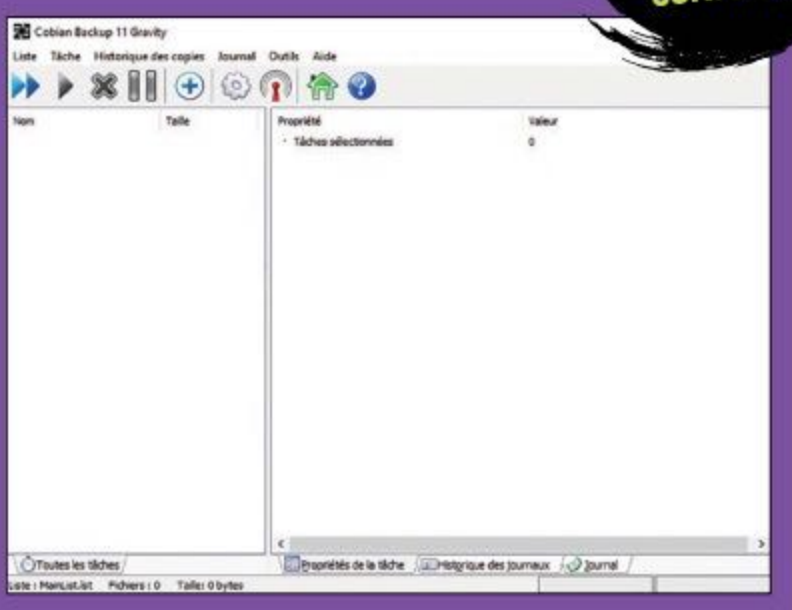
LEXIQUE

SAUVEGARDE INCRÉMENTIELLE : Une sauvegarde en mode incrémentiel permet de ne sauvegarder que le contenu modifié depuis la dernière sauvegarde. C'est un gain de temps et de place sur le disque dur.

CHIFFREMENT AES : Advanced Encryption Standard (standard de chiffrement avancé) est un algorithme de chiffrement qui a été choisi en 2000 par le gouvernement des USA pour remplacer l'obsolète DES (qui utilisait des clés de 56 bits facilement «crackable»). AES utilise, quant à lui, des clés de 128, 192 ou 256 bits.

Cobian Backup → Le challenger

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES



Cobian Backup est un autre poids lourd de la sauvegarde. Gratuit et régulièrement mis à jour, il permet presque autant de choses que Todo : sauvegardes standards ou incrémentielles, compression, planification, transfert vers FTP ou un volume disponible sur votre réseau local. Il lui manque cependant le clonage de disque et toutes les petites choses qui font de Todo un cador (disque d'urgence, fractionnement, effacement et sauvegarde du système). Du côté des points forts, on compte un chiffrement AES « complet » et une compatibilité avec la technologie Shadow Copy de Microsoft (création de sauvegardes même si le volume est en activité).

Difficulté : ☠☠☠ Lien : **cobiansoft.com**

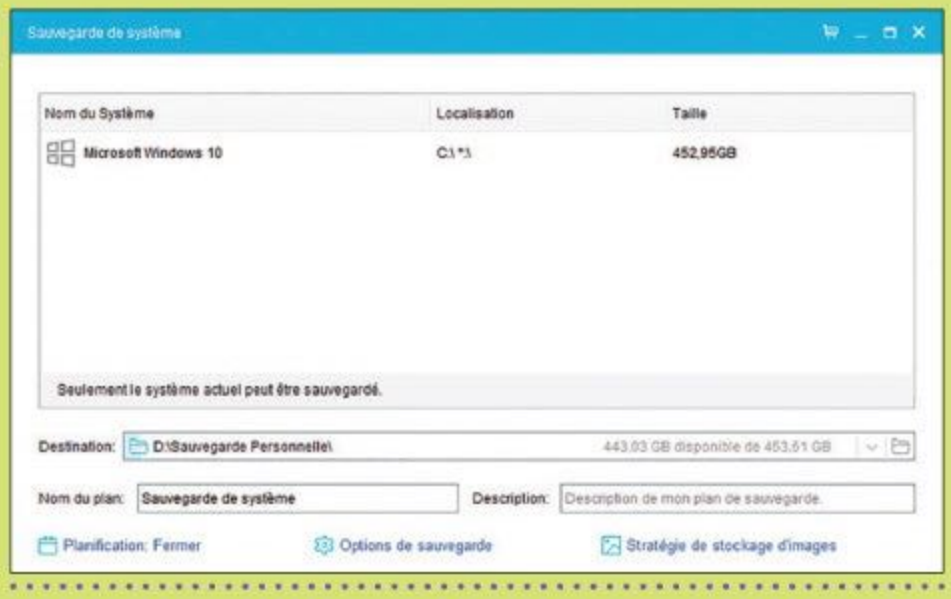
Sauvegarder avec EaseUS Todo Backup

INFOS [EASEUS TODO BACKUP]
Où le trouver ? [**goo.gl/7VvNFt**] Difficulté : ☠☠☠

TUTO

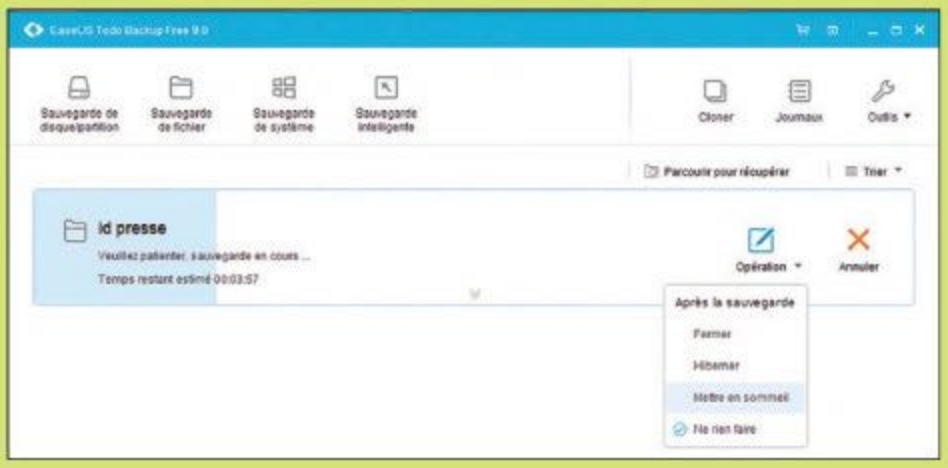
01› LES TYPES DE SAUVEGARDE

Sauvegarder un disque entier, un fichier ou un dossier précis, ou encore tout le système, EaseUS Todo Backup donne l'embarras du choix. La Sauvegarde intelligente laisse le choix au logiciel de sauvegarder ce qu'il estime essentiel. Chaque fonctionnalité propose un planificateur et des options spécifiques (emplacement, compression, chiffrement et priorité du processus).



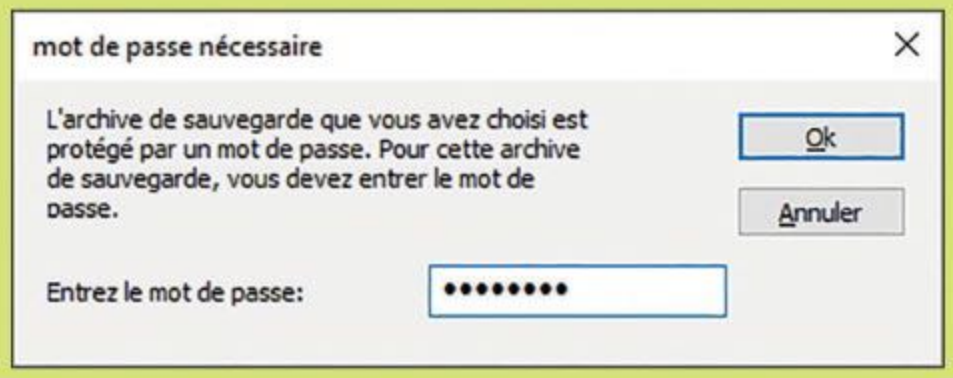
02› SAUVEGARDER

Après avoir tout paramétré, il suffit de cliquer sur **Procéder**. Durant la sauvegarde, il est possible de demander au logiciel de réaliser une tâche lorsque le processus sera terminé : hiberner, fermer ou mise en veille. C'est sur cette même fenêtre que l'icône de restauration apparaîtra lorsque la sauvegarde sera terminée.



03› EXPLORER UN FICHIER .PBD

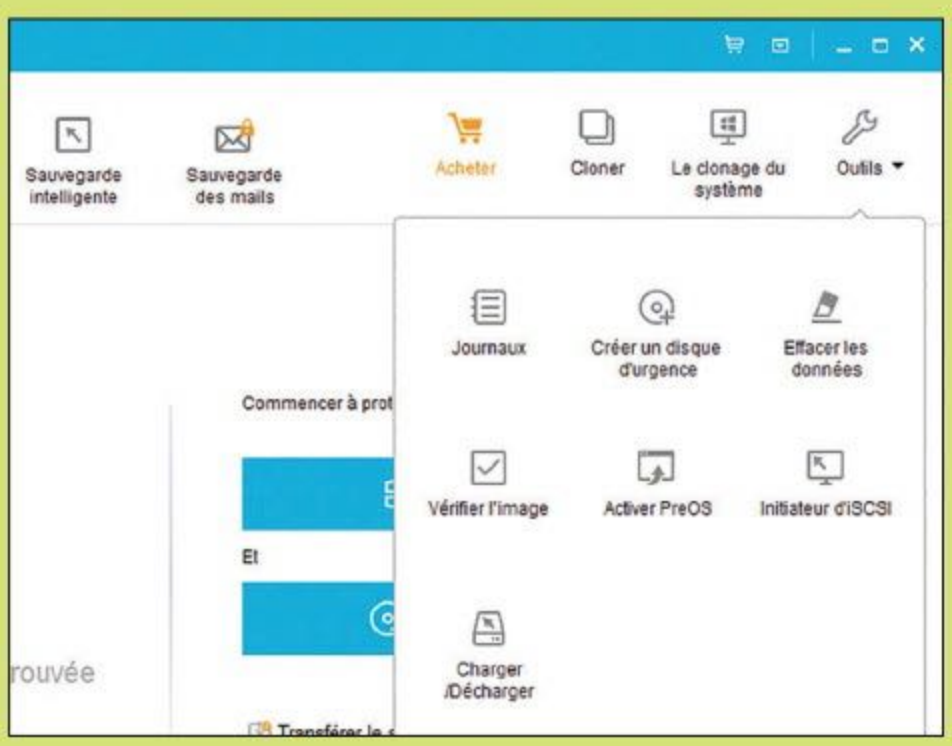
Si vous avez chiffré votre sauvegarde, vous pourrez tout de même explorer son contenu depuis



l'explorateur de fichiers Windows, à condition d'avoir installé Todo Backup et d'entrer le mot de passe lorsque vous ouvrez le fichier **.pbd**.

04› LES AUTRES OUTILS

EaseUS Todo Backup est très complet, même dans sa version gratuite. En cliquant sur **Outils**, vous accédez à plusieurs fonctions intéressantes qui vous épargneront l'installation d'autres logiciels : vérification des images disque, effacement sécurisé, création d'un disque d'urgence, etc. Difficile de ne pas trouver ce que l'on cherche !



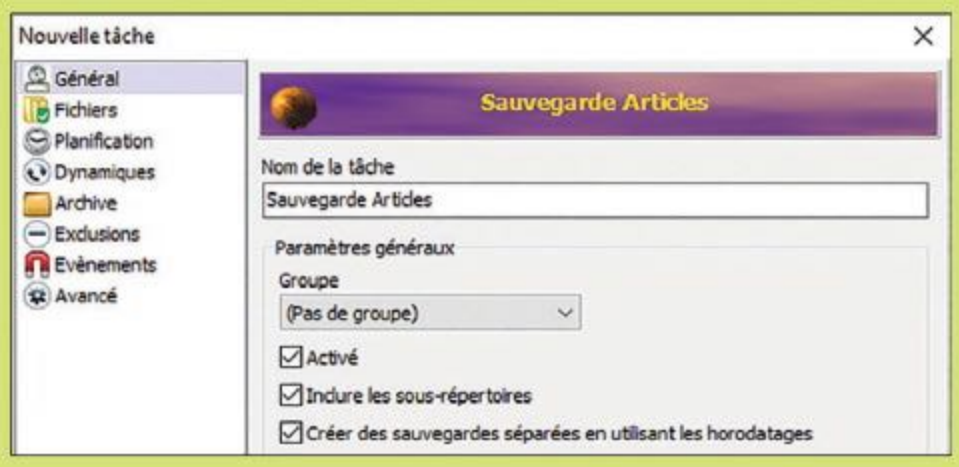
Sauvegarder avec Cobian Backup

INFOS **[COBIAN BACKUP]**
Où le trouver ? [**cobiansoft.com**] Difficulté : ☠☠☠

TUTO

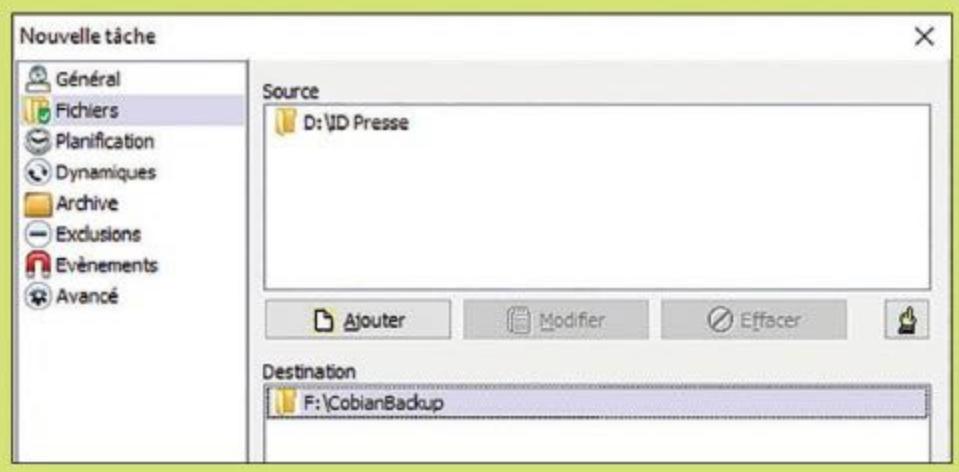
01› PARAMÉTRER

Après avoir installé le programme en mode **Application**, cliquez sur l'icône de la barre de notifications pour afficher l'interface (en bas à droite). Pour paramétrer une sauvegarde, cliquez sur **Tâche** puis **Nouvelle tâche**. Donnez lui un nom et décochez **Créer des sauvegardes séparées en utilisant les horodatages**. Dans **Type**, choisissez **Incrémentielle** et faites **OK** deux fois.



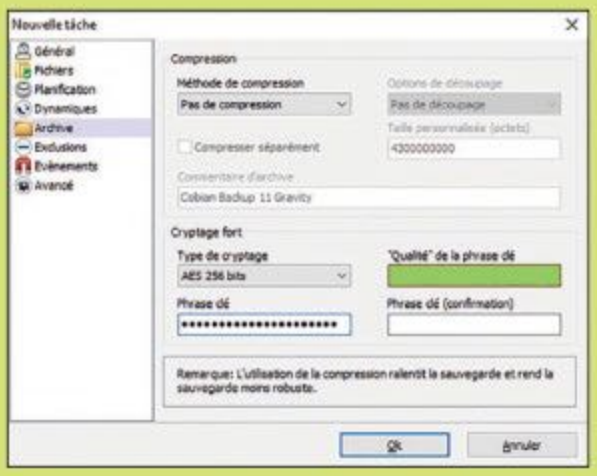
02› SÉLECTIONNER

Dans **Ajouter**, choisissez **Répertoire** pour sauvegarder un dossier entier et retrouvez-le dans l'arborescence. Il est possible de sauvegarder un simple fichier ou plusieurs dossiers, avec **Ajouter**. Dans le cadre de destination, spécifiez un emplacement pour votre sauvegarde avec **Ajouter**. Choisissez un répertoire dans un support externe ou un FTP pour éviter les problèmes matériels.



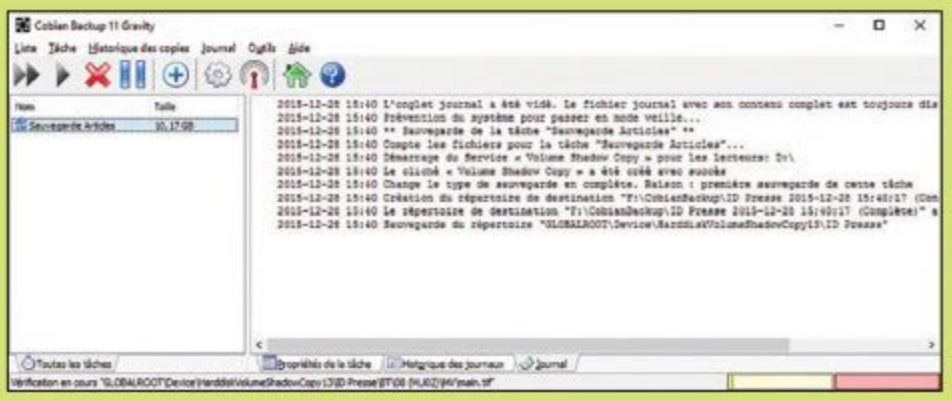
03› ARCHIVER ET CHIFFRER

Dans **Archive**, il est possible de compresser la sauvegarde pour gagner de la place sur le support de destination. Nous avons opté pour le format **7-Zip,** mais le **Zip** standard est aussi au menu. Vous pouvez définir un découpage précis si vous voulez placer votre sauvegarde sur CD ou DVD. Dans **Cryptage fort**, mettez de l'**AES 256 bits** si vos données sont sensibles et choisissez un mot de passe. Dans **Exclusions**, vous pouvez inclure ou exclure certains dossiers ou fichiers à votre sauvegarde.



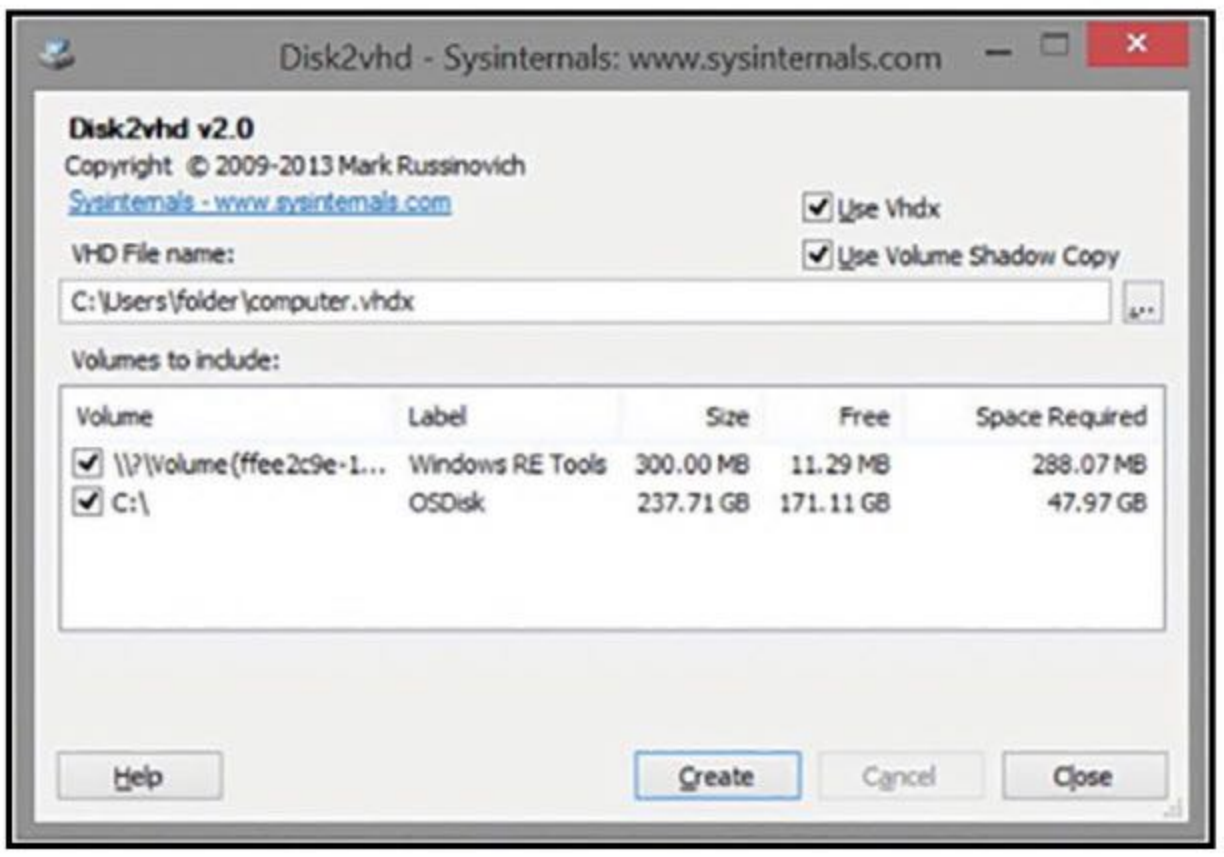
04› SAUVEGARDER

Événements sert à demander au logiciel de réaliser certaines tâches avant (fermer le programme, faire une pause...) ou après la création de la sauvegarde (redémarrer l'ordinateur, démarrer un service...). Une fois les paramétrages terminés, cliquez sur l'icône **Play** (en bleu) pour commencer la compression, le chiffrement et le transfert. L'onglet **Journal** (en bas), permet de suivre les étapes et de savoir lorsque la sauvegarde est terminée.



Disk2vhd → Disque dur virtuel

Disk2vhd va créer une image virtuelle d'un disque dur physique. L'image est lue par n'importe quelle machine virtuelle (via Microsoft Virtual PC par exemple, ou d'autres logiciels du genre). L'intérêt est que la sauvegarde peut se faire même pendant l'utilisation du disque (Shadow Copy). Seul l'espace occupé est copié : si votre disque dur de 500 Go contient 5 Go de données, le backup fera 5 Go. Disk2vhd est très simple d'utilisation, ce qui ne gâche rien.



Difficulté : ☠☠☠

Lien : **https://goo.gl/J2ajnN**

TestDisk → Récupération

TestDisk est un logiciel français de récupération de données. Il permet de restaurer des partitions perdues et de réparer la table des partitions si celle-ci a été endommagée par un virus ou une erreur de manipulation. Gratuit et open source, TestDisk permet aussi de reconstruire le secteur de boot d'un système de fichiers FAT ou NTFS, de récupérer des fichiers sur presque tout type de partition (FAT, NTFS ou ext) et de copier les fichiers depuis une partition FAT, NTFS, ext2/ext3/ext4 même si elle est effacée. Parfait pour les cas extrêmes où créer une sauvegarde de vos fichiers est devenu difficile.

Difficulté : ☠☠☠ Lien : **cgsecurity.org/wiki/TestDisk_Download**

SAUVEGARDE

Windows → La base

Windows intègre un système de sauvegarde depuis plusieurs années. La dernière mouture en date, Windows 10, est assez décevante en la matière puisqu'elle ne fait que reprendre l'outil introduit dans Windows 7. Vous pouvez donc soit programmer la sauvegarde automatique de vos fichiers sur un périphérique externe (ou un deuxième disque interne), soit créer une image de votre système. C'est basique, efficace, mais le manque d'options (notamment le chiffrement) vous fera préférer Windows uniquement pour un PC n'abritant aucune donnée sensible.

Difficulté :

CrashPlan → Pour les données

Réservé à la sauvegarde de vos données (fichiers, photos...), CrashPlan, dans sa version gratuite, s'occupe de mettre tout ça sur un périphérique externe, ou sur un autre PC, même si ce dernier n'est pas connecté au même réseau. Les données sont chiffrées avant transmission, qui est elle-même chiffrée. Les sauvegardes incrémentielles et différentielles sont supportées, mais vous ne pouvez programmer qu'une sauvegarde par jour.

Difficulté :

Lien : **crashplan.com**

XXclone → Clonage facile

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

XXClone propose de faire une copie intégrale de votre disque dur avec les fichiers systèmes et ceux de Windows. Le logiciel peut ensuite rendre bootable cette partition de sauvegarde et lui attribuer les mêmes empreintes d'identification que votre partition d'origine. En cas de problème, il faudra brancher votre nouveau disque (si votre sauvegarde réside dans un disque dur externe, il faudra booter en USB) ou démarrer sur la nouvelle partition depuis le BIOS. La version Freeware de XXClone fonctionne très bien, mais la version payante (Home) propose des options étendues comme la sauvegarde incrémentielle ou la compression des données, pour 30 € environ.

Difficulté : Lien : **xxclone.com**

Clonez votre disque dur avec XXClone

INFOS **[XXCLONE]**
Où le trouver ? [**gxxclone.com**] Difficulté : ☠☠☠

TUTO

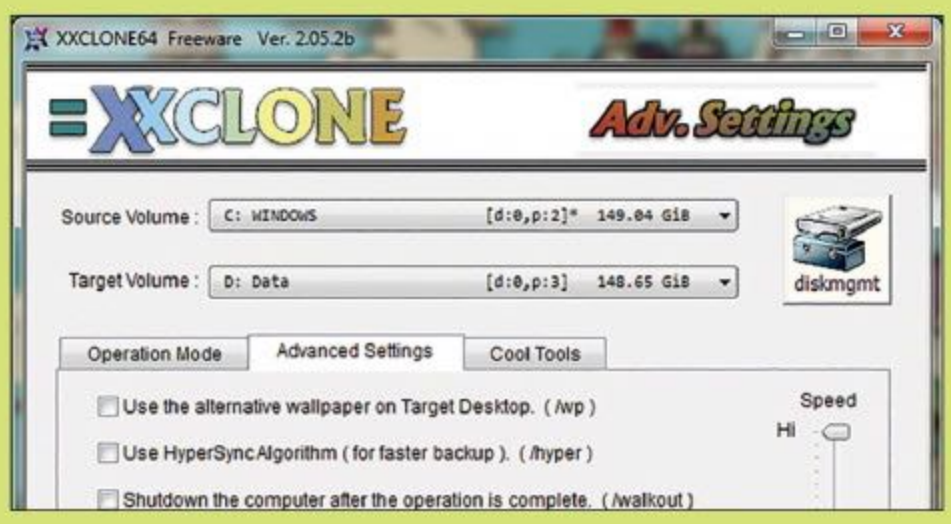
01 › LE MODE OPÉRATOIRE

Après avoir téléchargé, décompacté et installé XXClone, lancez le programme. Sélectionnez

le volume à sauvegarder dans **Source Volume** puis le disque où sera stockée votre sauvegarde dans **Target Volume**. Attention, il faudra qu'il y ait assez de place dans ce dernier et qu'une partition entière soit dédiée à la sauvegarde. Dans l'onglet **Operation Mode**, choisissez la première option.

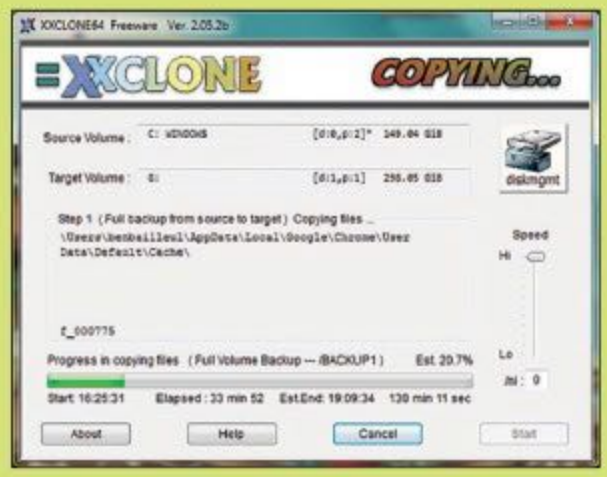
02 › LES OPTIONS

Faites ensuite un tour dans l'onglet **Advanced Settings**. Ici, il est possible d'éditer un journal ou un fichier debug pour en savoir plus sur les problèmes rencontrés pendant le processus. Notez que le **HyperSync Algorithm** permettant «d'oublier» volontairement des sous-dossiers ne fonctionne que pour la version payante. Sachez aussi qu'en cliquant sur l'icône **diskmgmt**, vous aurez accès à l'utilitaire de gestion des disques de Windows.



03 › LANCEMENT DE LA SAUVEGARDE

Avant de cliquer sur **Start** pour commencer le clonage, prenez bien note que toutes les données



présentes sur la partition de sauvegarde (**Target**) seront effacées. Il faudra un disque dur vierge ou une partition que vous aurez créée. Pour cela, vous pouvez utiliser **diskmgmt** ou **MiniTool Partition Wizard**. Faites attention à ce que vous faites ! Lorsque vous aurez fini vos réglages, faites **Start** et attendez la fin du processus (ou cochez **Shutdown the computer after the operation is complete** pour fermer le PC à la fin).

02 › LES OPTIONS COMPLÉMENTAIRES

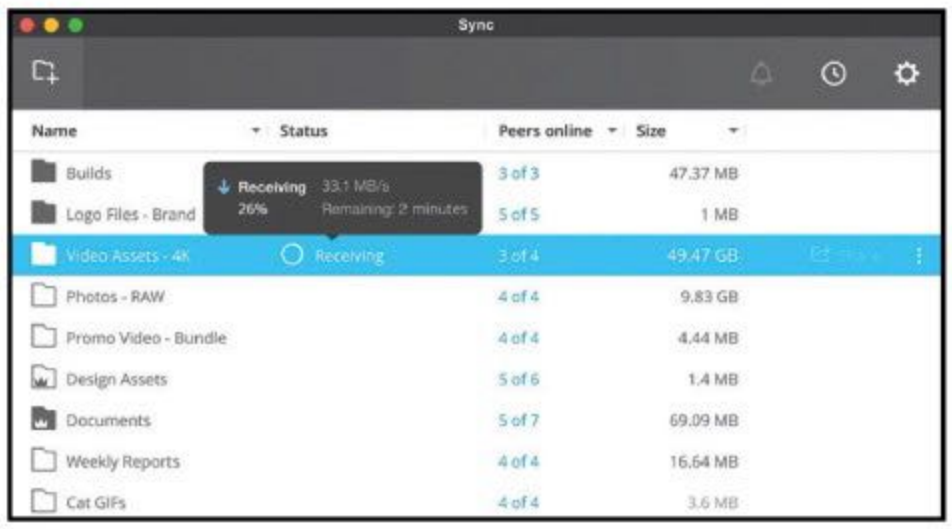
Une fois que votre sauvegarde est faite, vous pouvez ajouter des options dans **Cool Tools**. D'ici, vous pourrez créer un point de sauvegarde de votre système actuel pour pouvoir récupérer une configuration stable en cas de problème avec XXClone. Dans **Schedule Task,** vous pourrez faire en sorte d'automatiser certaines tâches depuis le planificateur de Windows. **Make Batch File** permet de sauvegarder vos réglages dans un fichier pour les utiliser ultérieurement.

Resilio Sync Home → Partage et synchronisation

Celui qui s'appelait encore BitTorrent Sync il y a quelques mois a trois casquettes : il permet de sauvegarder, de synchroniser vos données et de partager du contenu avec vos amis. Comme le système est décentralisé (vos fichiers ne sont pas sur un serveur), la seule limite est celle de la taille de votre disque dur. Grâce à la technologie P2P de BitTorrent, vous synchronisez un ou plusieurs dossiers avec vos amis en leur communiquant une clé secrète unique. Vos amis n'auront qu'à installer le programme et taper votre clé.C'est aussi un très bon moyen pour avoir accès à tous vos fichiers depuis tous vos appareils (Windows, MacOS, iOS, Android, Windows mobile, Kindle Fire, FreeBSD ainsi que les NAS Netgear). Il faudra juste que votre ordinateur soit allumé pour que vos contacts aient accès aux dossiers.

Difficulté :

Lien : **www.resilio.com/individuals**



LEXIQUE

P2P : Le peer-to-peer, ou «pair-à-pair» en français, est un modèle de réseau informatique où chaque client peut aussi faire office de serveur. Le protocole BitTorrent, très efficace dans le domaine du partage de fichiers est un système P2P.

FulSync

→ Sauvegarde et synchronisation

FullSync est aussi à l'aise avec des sauvegardes simples, incrémentielles ou avec de la synchronisation de fichiers (dans un ou deux sens). Le logiciel autorise aussi l'automatisation des sauvegardes depuis et vers des répertoires locaux, du FTP, du SFTP ou des partages Windows (SMB). Le mode Publish/Update vous permettra même de mettre à jour un site Web à partir d'une copie locale. Bien sûr, tout est paramétrable dans le temps (un oubli est si vite arrivé) et vous disposerez aussi de filtre pour exclure certains fichiers.

Difficulté :

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

CHEZ VOTRE MARCHAND DE JOURNAUX

LES PIRATES CRYPTENT, NOS LECTEURS DÉCRYPTENT !

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

HACKING
ANONYMAT
PROTECTION MULTIMÉDIA
BEST OF LOGICIELS & SERVICES 100% GRATUITS
LA TROUSSE À OUTILS DU PIRATE
N°37
GRATUIT # POUR WINDOWS

+ EN CADEAU : 2 magazines complets offerts SUR LE CD

LES CAHIERS DU HACKER

PIRATE [INFORMATIQUE] // 37

+DE 40 FICHES PRATIQUES AVEC CD GRATUIT

LE GUIDE PRATIQUE

HACKING

PRENDRE LE CONTRÔLE EST UN JEU D'ENFANTS

ANONYMAT
TOR : hébergez votre site sur le "DARKNET"

DÉCRYPTAGE
Usurpation de votre e-mail : Comment ça marche ?

INCOGNITO
USB Capture : Récupérez tout le contenu d'un clé USB !

MATÉRIEL
Tout savoir sur le Raspberry P

+ CD GRATUIT PACK 100% PIRATE

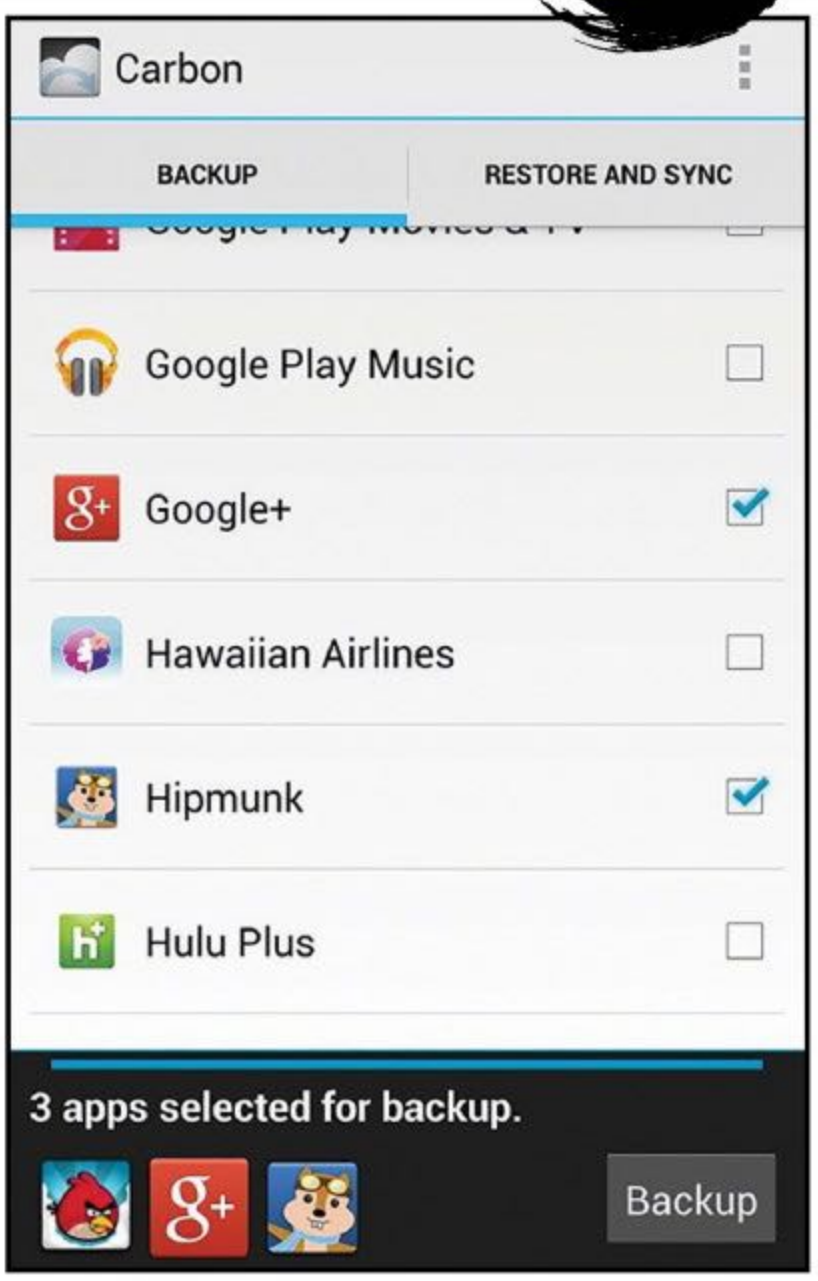
SAUVEGARDE

Helium → Sans root

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

Helium sauvegarde les applications, (et leurs données), les contacts, les SMS... Pour résumer, tout ce que contient votre appareil Android. Ainsi en cas de pépin (perte ou vol de ce dernier), vous pourrez tout restaurer depuis votre PC, vers votre nouvel Androphone. Cerise sur le gâteau, Helium est très facile à utiliser et vous n'êtes pas obligé de rooter votre téléphone pour en profiter.

Difficulté : ☠☠☠ Lien : **https://goo.gl/cwPSV**



LEXIQUE

ROOT : Le root est une manipulation issue du monde Unix permettant d'avoir les «pleins pouvoirs» sur votre mobile Android. Une fois que votre mobile est rooté, il y est même après un redémarrage. Pour en savoir plus : **www.android-mt.com !**

Sauvegarde Facile

→ Tout est dans le titre

Easy Backup & Restore (son nom d'origine) est une application idéale pour sauvegarder et restaurer votre mobile. Créez une copie du contenu du smartphone tel qu'il est à un instant T (ou instant I si vous préférez). Sans root, sauvegardez SMS, MMS, journal d'appels, agenda, dictionnaire personnel et contacts, ainsi que des versions APK de vos applications. Le root ajoute la possibilité de sauvegarder les données des applis (ce qu'Helium fait de base). Easy Backup & Restore peut s'utiliser même si vous activez la sauvegarde de votre compte sur les serveurs de Google. Cela permet de conserver un fichier « en dur », au cas où.

Difficulté : ☠☠☠ Lien : **https://goo.gl/QEaJ4**

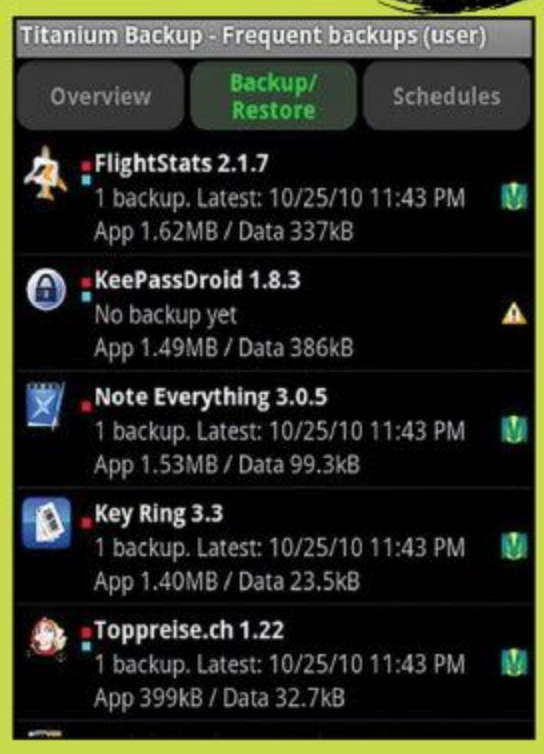
SMS Backup & restore → Messages et appels

L'application gratuite SMS Backup & Restore vous permet d'effectuer une sauvegarde facile de vos SMS et de votre journal d'appels. De plus, en cas de changement de téléphone, de vol ou d'erreur fatale, cette dernière vous donne la possibilité de réimporter ces données sur un nouvel appareil grâce à la sauvegarde effectuée par vos soins. Plus aucune raison de paniquer, vos SMS sont en sécurité.

Difficulté : ☠☠☠ Lien : **https://goo.gl/Kn4Vp**

Titanium Backup → Complet

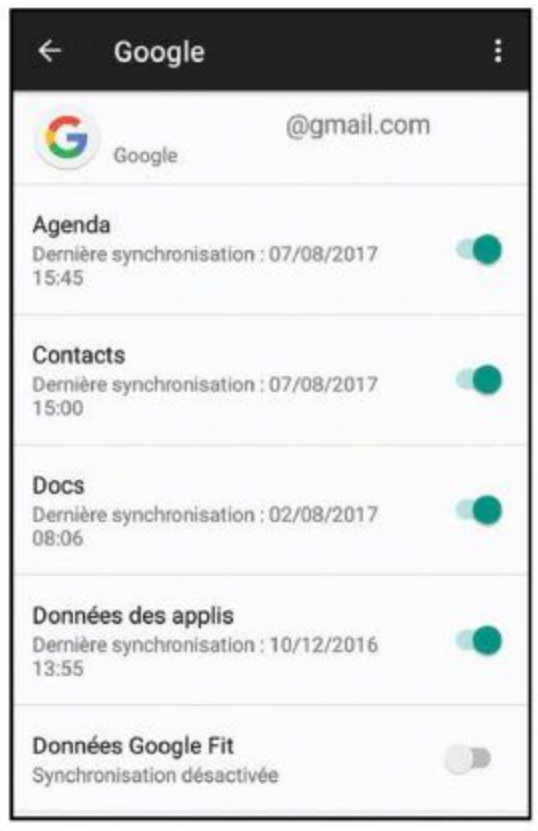
VOIR NOTRE TUTO DANS LES PAGES SUIVANTES



La version gratuite de Titanium Backup assure l'essentiel des fonctions attendues : sauvegarde de votre appareil et restauration ultérieure. La sauvegarde comprend les applications (applis systèmes inclues), leurs données (les sauvegardes de jeux par exemple), et bien sûr vos médias (photos, vidéos, musiques...). Si vous souhaitez effectuer une sauvegarde d'une appli et/ou de ses données sur une carte SD, Titanium Backup le permet. Son interface austère peut intimider de prime abord, mais ne vous inquiétez pas : pour une utilisation basique, elle est très facile à prendre en main.

Difficulté : ☠☠☠
Lien : **https://goo.gl/nb4q9**

Google → Par défaut



Pour peu que vous utilisiez les applications Google (Gmail, Hangouts, Agenda Google, Google Play Jeux/Films/Musique, etc.), il est très facile de synchroniser toutes vos données dans le Cloud (sur les serveurs Google, pas sur votre propre espace de stockage). Rendez-vous dans les **Paramètres** de votre appareil, puis **Sauvegarder et réinitialiser**. Cochez **Sauvegarder mes données** et **Restaurer automatiquement** pour activer les deux options. Toujours dans les **Paramètres**, mais dans la rubrique **Comptes** cette fois, touchez **Google** puis votre adresse mail. Activez ou désactivez les données que vous souhaitez sauvegarder et le tour est joué.

Difficulté : ☠☠☠

SAUVEGARDE

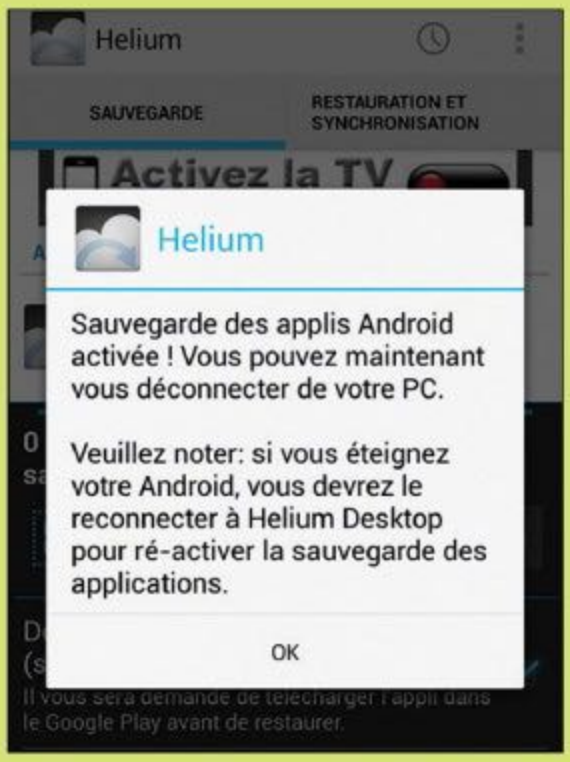
Sauvegarder son mobile avec Helium

INFOS **[HELIUM]**
Où le trouver ? [**https://goo.gl/cwPSV**] Difficulté :

TUTO

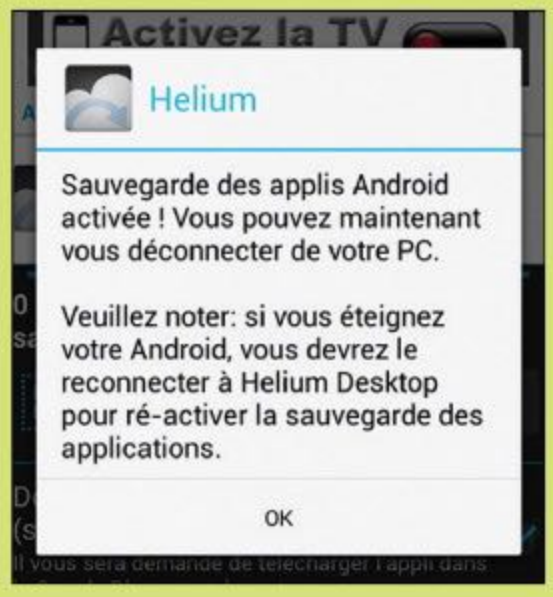
01 › LES INSTALLATIONS

Installez Helium sur votre appareil Android et lancez-le. L'appli vous propose d'envoyer le lien de téléchargement pour le programme Windows via Skype, Gmail, Google Drive... Vous pouvez aussi recopier le lien. Installez le programme sur PC (si votre téléphone est rooté, ce n'est pas nécessaire) et branchez l'appareil avec votre câble USB lorsque Helium vous le demandera.



02 › LE BRANCHEMENT

Activez le mode **Débogage USB** pour que la synchronisation fonctionne (il faudra peut-être débrancher le câble pour avoir accès à ce paramètre). Android vous demandera aussi d'activer le mode **PTP (Logiciel PC)**, mais sur certains modèles, ce ne sera pas nécessaire. Si vous n'avez jamais branché votre appareil de cette manière, laissez les pilotes s'installer automatiquement.



03 › LE SUPPORT

En cas de pépin, n'hésitez pas à redémarrer PC et téléphone puis à réessayer la connexion une fois les pilotes et programmes installés. Si tout se passe bien, vous devriez pouvoir sélectionner les applications que vous voulez sauvegarder. Appuyer sur **Tout** pour sélectionner la totalité de vos applis et validez. Helium vous demandera alors sur quel support vous voulez faire la sauvegarde. Notez que les messages et les contacts seront sauvegardés automatiquement.

04 › LES SAUVEGARDES

Il est possible de faire cette sauvegarde sur une carte SD, dans la mémoire même du téléphone (même si nous ne voyons pas l'utilité) ou dans le Cloud : Dropbox, Google Drive, etc. Attention, il faut souscrire à l'offre Premium pour cette dernière option (5 dollars, soit moins de 4 €). Pour restaurer vos applis sur un autre appareil, refaites un branchement et sélectionnez **Restauration et synchronisation**.

Sauvegarder avec Titanium Backup

INFOS [TITANIUM BACKUP]
Où le trouver ? [**https://goo.gl/nb4q9**] Difficulté : ☠☠☠

TUTO

01› FAIRE LA PREMIÈRE SAUVEGARDE

Ouvrez Titanium Backup et lisez les différents messages/avertissement. Touchez l'icône en forme de feuille de papier en haut à droite puis, sous **Sauvegarder**, appuyez sur **GO** à gauche de **Sauvegarder toutes applis utilisateur + données système** et sur le « ✓ » en haut à droite sur la page suivante. Le processus peut prendre du temps.

02› SAUVEGARDER AU CAS PAR CAS

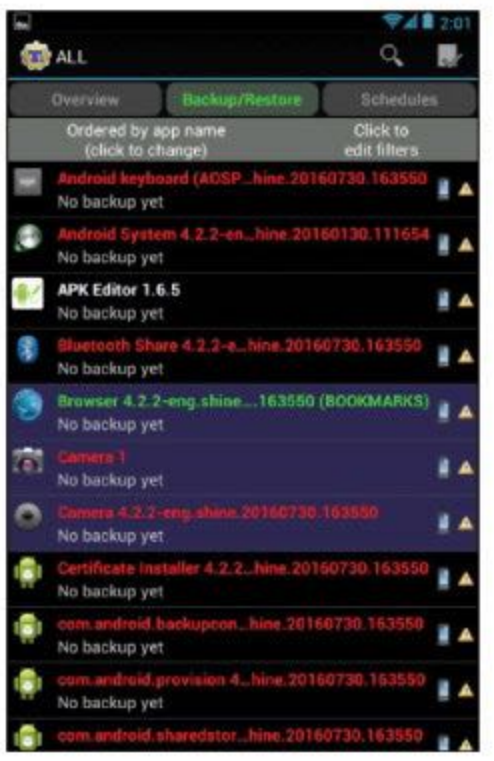
Dans l'onglet **Sauver/Restaurer**, touchez l'application ou le paramètre que vous souhaitez

03› PLANIFIER UNE SAUVEGARDE

Via l'onglet **Planifications**, cochez la case **Activé** à droite de **Sauvegarder nouvelles applis utilisateur+système & nouvelles versions**. Appuyez sur **Editer** et choisissez quoi sauvegarder avec la première flèche pointant vers le bas, un éventuel filtrage avec la deuxième, sous quelles conditions avec la troisième, une heure et **Sauver le tout**.

04› RESTAURER

Sur l'appareil qui vient de subir un « wipe », réinstallez Titanium Backup depuis le Google Play Store. Touchez à nouveau l'icône en forme de feuille de papier puis, sous **Restaurer**, appuyez sur **Restaurer applis manquantes + toutes les données système**.



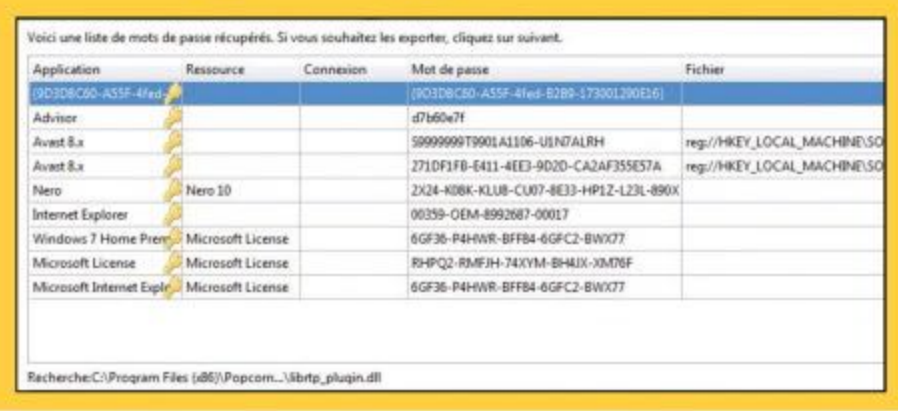
HACKING

recALL → Récupération de mots de passe en local

Après l'avoir installé, recALL ira chercher des mots de passe, des codes d'accès ou des numéros de licence dans des endroits de votre Windows dont vous ne soupçonniez même pas l'existence (dossier d'installation, base de registre, etc.) Ces emplacements sont préenregistrés et toutes sortes de logiciels sont passés au crible : Windows, Office, antivirus, client mail, tous les mots de passe mémorisés par une vingtaine de navigateurs, client FTP, messagerie instantanée, logiciels commerciaux, jeux vidéo, etc. Bien sûr, les codes d'accès Wi-Fi sont compris dans le lot.

Difficulté : ☠☠☠

Lien : **http://keit.co/p/recall**

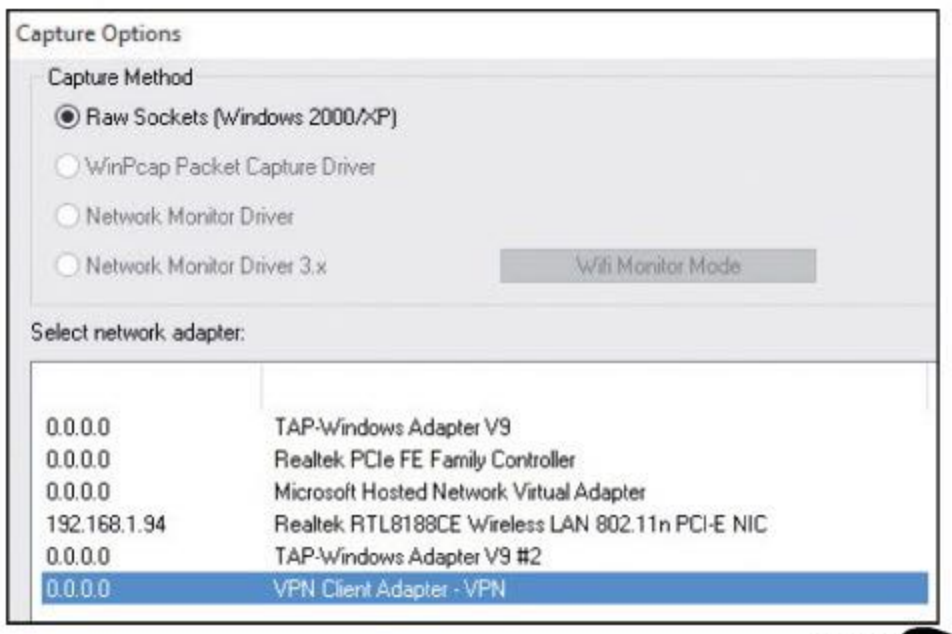


SniffPass → Un logiciel de NirSoft

Lancé en 2001 par Nir Sofer, NirSoft est un site très austère où vous trouverez plus de 180 logiciels programmés en C++. L'avantage de ce langage ? Des programmes très légers comme SniffPass. Ce dernier va «sniffer» votre réseau à la recherche de mots de passe POP3, IMAP4, SMTP, FTP et HTTP. Si vous avez une connexion, mais que vous avez perdu le mot de passe, lancez le logiciel et SniffPass le retrouvera pour vous.

Difficulté : ☠☠☠

Lien : **www.nirsoft.net/utils/password_sniffer.html**



LaZagne → Il récupère tout ce qui passe

Dans le même genre que RecALL (voir cette sélection), ce programme en ligne de commande va pomper les sésames contenus dans vos navigateurs et plusieurs autres logiciels. Il est légèrement moins complet que RecALL et un peu plus âpre au niveau de son interface, mais est beaucoup plus discret et rapide. Pour accélérer la manœuvre, il est possible de cibler ce que vous voulez récupérer. À essayer d'urgence !

Difficulté : ☠☠☠

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

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

Récupération de mots de passe avec LaZagne

Si vous avez physiquement accès à un ordinateur, LaZagne va analyser le contenu de la base de registre et des dossiers pour afficher tous les mots de passe qui traîne en clair : navigateurs, logiciels, bases de données, réseaux WiFi, etc.

laZagne

INFOS [LaZagne]

Où le trouver ? [**https://github.com/AlessandroZ/LaZagne**]

Difficulté : ☠☠☠

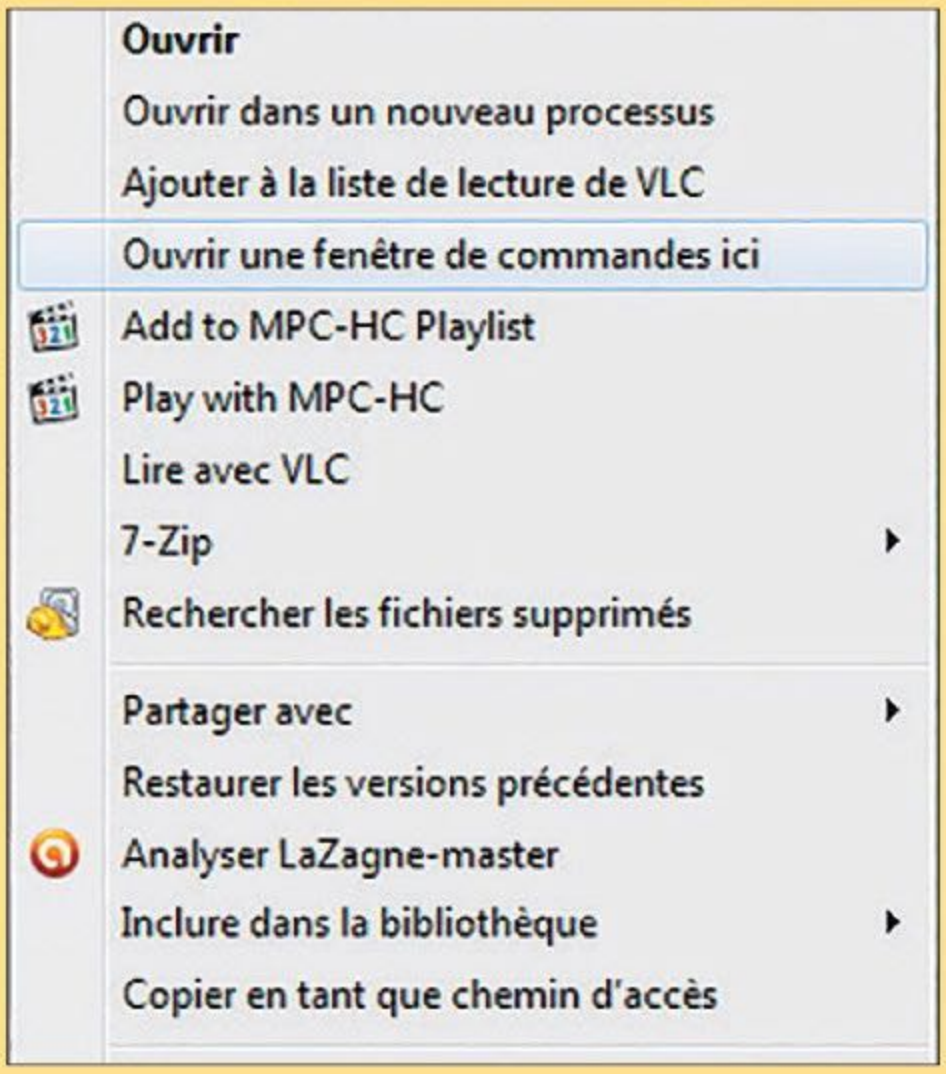
TUTO

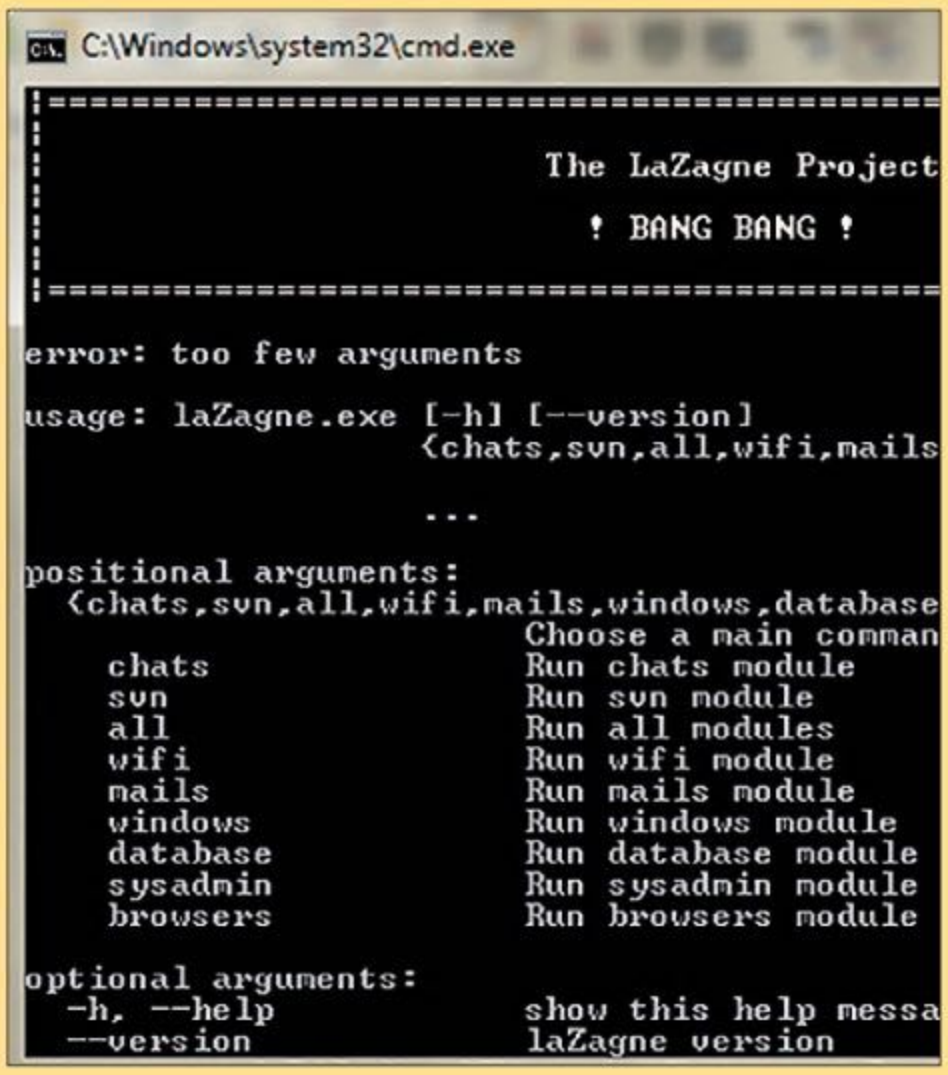
01› EN LIGNE DE COMMANDE

Décompactez le fichier ZIP et placez le contenu où vous le souhaitez. 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**. Pour connaître la liste des commandes, faites **lazagne.exe** puis tapez sur **Entrée**.

02› À L'ACTION !

Vous pouvez constater qu'il suffit de taper **lazagne.exe browsers** pour récupérer les mots de passe contenus dans les navigateurs ou **lazagne.exe mails** pour les clients POP/IMAP/SMTP. Pour obtenir absolument tous les mots de passe contenus dans le PC, il suffit de taper **lazagne.exe all**. Magique !





John the Ripper
→ Le pluri-disciplinaire

John the Ripper est un logiciel de cassage de mot de passe: un «crack» du crack. Plusieurs techniques sont à sa disposition. Le mode simple va essayer plusieurs mots de passe en fonction du nom d'utilisateur, le «brute force» et l'attaque par dictionnaire. Pour cette dernière méthode, il faudra trouver ou vous confectionner un fichier contenant des millions de mots courants ou de sésames connus. Quelques pistes sont disponibles ici : **www.openwall.com/passwords/wordlists**. Notons que pour que ce logiciel puisse travailler, il faudra mettre la main sur les hash présents dans les bases MySQL par exemple.

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

LEXIQUE

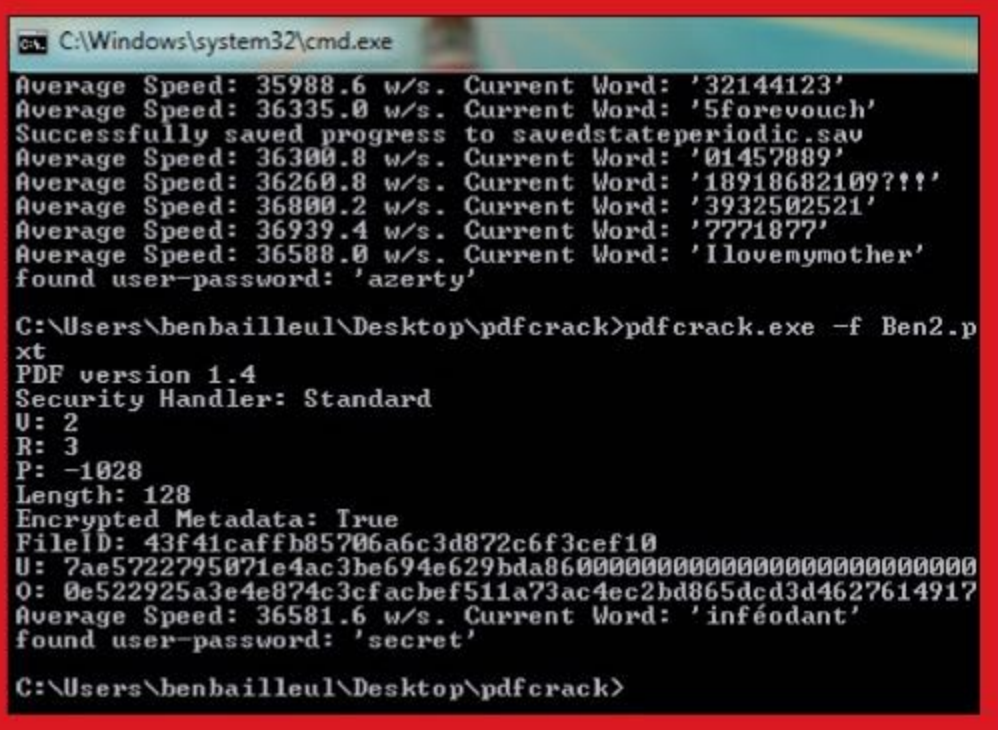
CRACK : Cracker un mot de passe c'est le "casser", réussir à l'obtenir en utilisant ses méninges et un logiciel (eh oui, il faut les deux !)

DICTIONNAIRE : Il s'agit d'une liste de mots dont le logiciel va se servir en espérant trouver son bonheur dedans. Il existe de nombreux dictionnaires sur Internet dans toutes les langues.

BRUTE FORCE : La technique de bourrin pour retrouver un mot de passe. Le logiciel va essayer toutes les combinaisons de lettres, de chiffres et autres caractères pour arriver à ses fins.

PDFCrack → Et crack, le PDF !

PDFCrack est un logiciel destiné à fonctionner sur système Linux, mais il existe une version pour Windows. Il permet de tirer profit des processeurs multicœurs et de la puissance de plusieurs ordinateurs (cluster) pour attaquer les mots de passe d'ouverture et d'autorisation. La progression est automatiquement sauvegardée pour reprendre un projet en cours. Sur notre PC de test, PDFCrack a été capable de passer en revue 37 500 mots de passe à la seconde.



Difficulté : ☠☠☠

Lien : **http://andi.flowrider.ch/research/pdfcrack.html**

RainbowCrack → Un compromis «temps-mémoire»

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

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. 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 plusieurs 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 crack 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.

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

Hashcat → Très exhaustif !

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, 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'attaques 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.)

Difficulté : ☠☠☠ Lien : **http://hashcat.net**

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**.N'interrompez surtout pas le processus !

```
RainbowCrack 1.6.1
Copyright 2003-2015 RainbowCrack Project. All rights reserved.
http://project-rainbowcrack.com/

usage: rcrack rt_files [rt_files ...] -h hash
       rcrack rt_files [rt_files ...] -l hash_list_file
       rcrack rt_files [rt_files ...] -f pwdump_file
       rcrack rt_files [rt_files ...] -n pwdump_file
rt_files:              path to the rainbow table(s), wildchar(*, ?) supported
-h hash:               load single hash
-l hash_list_file:     load hashes from a file, each hash in a line
-f pwdump_file:        load lanmanager hashes from pwdump file
-n pwdump_file:        load ntlm hashes from pwdump file
```

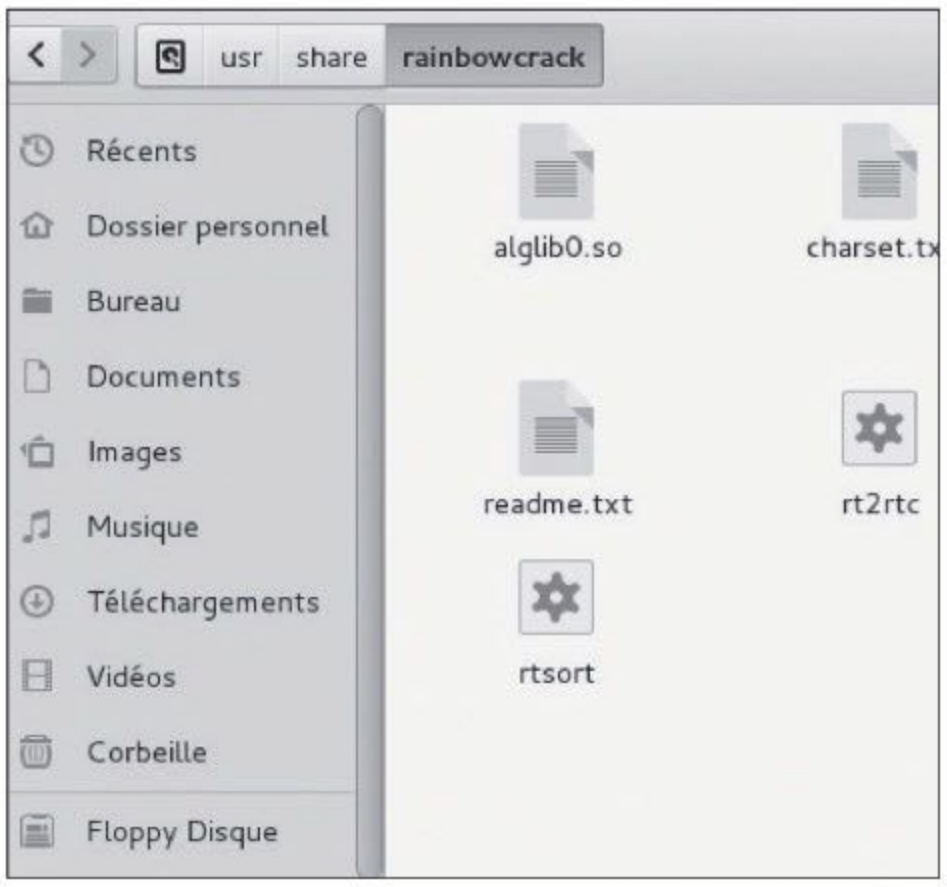
03› LES DÉCLINAISONS

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=560000000 bits. Environ 560Mo 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

```
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
root@kali:/usr/share/rainbowcrack# rtgen md5 loweralph
rainbow table md5_loweralpha#4-5_0_2000x35000000_0.rt
hash algorithm:         md5
hash length:            16
charset:                abcdefghijklmnopqrstuvwxyz
charset in hex:         61 62 63 64 65 66 67 68 69 6a

charset length:         26
plaintext length range: 4 - 5
reduce offset:          0x00000000
plaintext total:        12338352

sequential starting point begin from 0 (0x000000000000
generating...
65536 of 35000000 rainbow chains generated (0 m 29.2 s
131072 of 35000000 rainbow chains generated (0 m 27.6
196608 of 35000000 rainbow chains generated (0 m 26.3
262144 of 35000000 rainbow chains generated (0 m 26.0
327680 of 35000000 rainbow chains generated (0 m 26.0
393216 of 35000000 rainbow chains generated (0 m 27.5
458752 of 35000000 rainbow chains generated (0 m 26.8
524288 of 35000000 rainbow chains generated (0 m 28.4
```

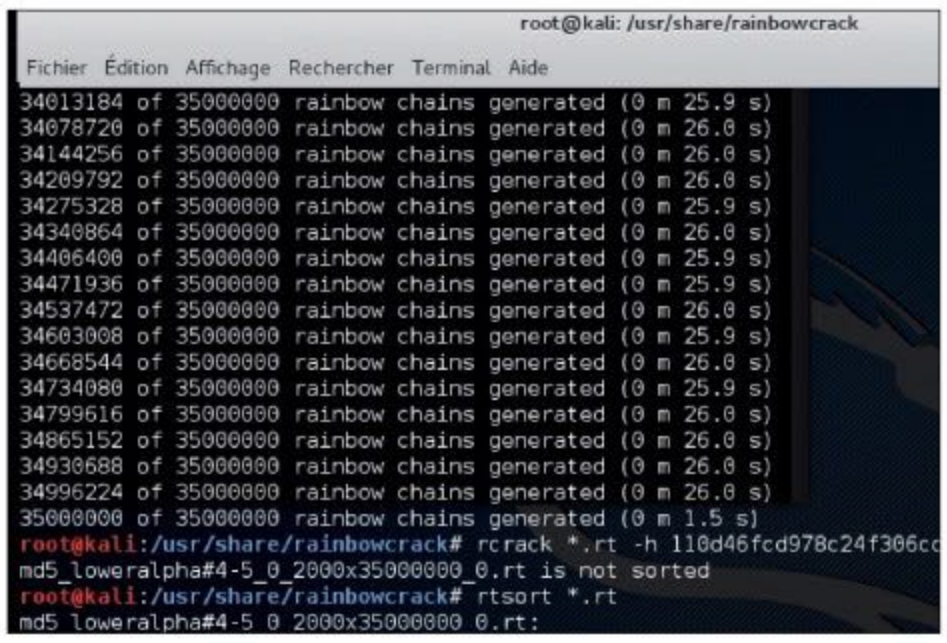
04› NOM ET EMPLACEMENT

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 !



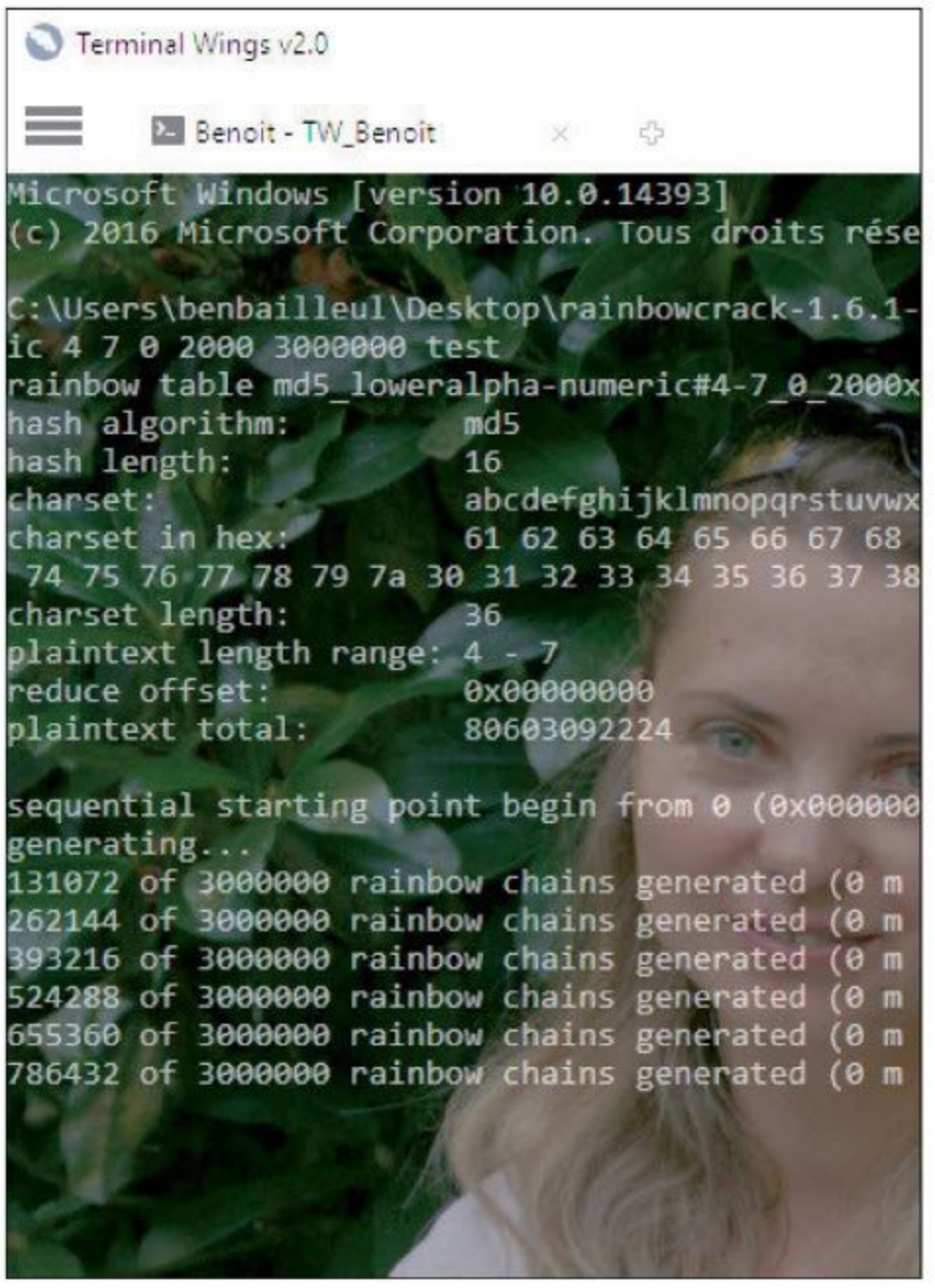
05› LE TRI

Une fois vos tables générées, il va falloir encore faire une opération pour les rendre exploitables : c'est le tri. La commande **rtsort**



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.phrozen.io**). 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.



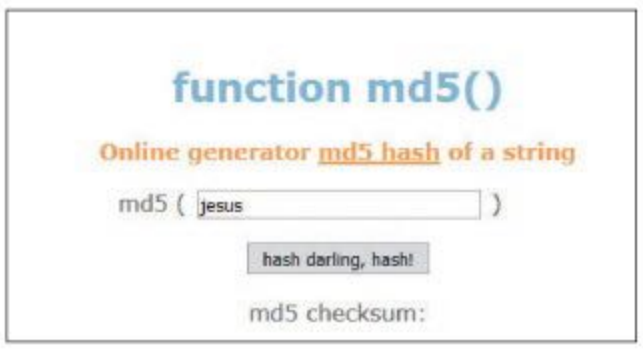
Crackez avec votre table

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

TUTO

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).

```
  time of other operation:                    0.01 s
time of disk read:                            0.92 s
hash & reduce calculation of chain traverse:  1998000
hash & reduce calculation of alarm check:     320
number of alarm:                              320
speed of chain traverse:                      2.38 milli
speed of alarm check:                         0.32 milli

result
---------------------------------------------------------
110d46fcd978c24f306cd7fa23464d73  jesus  hex:6a65737573
root@kali:/usr/share/rainbowcrack#
```

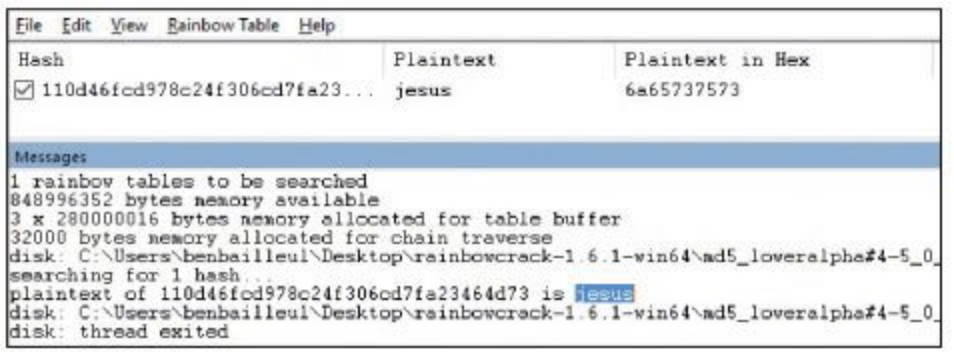
03› AVANTAGES ET LIMITES

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.

```
hash & reduce calculation of alarm check:     192
number of alarm:                              192
speed of chain traverse:                      2.41 milli
speed of alarm check:                         0.19 milli

result
---------------------------------------------------------
8551819a762771e56d6ed74faccc3022  bidul  hex:626964756c
root@kali:/usr/share/rainbowcrack#
```

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.



cRarck → Crackez avec votre carte graphique !

```
C:\WINDOWS\system32\cmd.exe
.ticks of #0__ ASM        = 122355389
.ticks of #2__ SSSE3      = 109428176
-- 4 pswd:
.ticks of #1__ SSE2       = 45626078
-- 8 pswd:
.ticks of #1__ SSE2       = 46548723

Chosen: SSSE3, SSE2, SSE2 (-f211)
Clock cycles per password expected = 46548723 (SIMD)/109428176 (x64) (*
Calculating pure SHA-256 clock cycles...
-- 1 pswd:
ticks of #2__ SSSE3       = 94635582
-- 4 pswd:
ticks of #1__ SSE2        = 45208151
-- 8 pswd:
ticks of #1__ SSE2        = 42848821
Pure SHA-256 clock cycles per byte expected = 5.9 (SIMD)/12.9 (x64) (*)
Intel(R) Core(TM) i3 CPU M 380 @ 2.53GHz found, CPU rate = 1.64 (*)
(*) May be inaccurate if Turbo Boost is on

Brute-force benchmark. Please wait about 10-20 s...
Device #0, Block size is: 32 x 128 (-m32), step = 1/16 (-d5)
1296 4-chars passwords in 11.80 seconds, rate = 110 p/s

C:\Users\benbailleul\Desktop\crark-7z>_
```

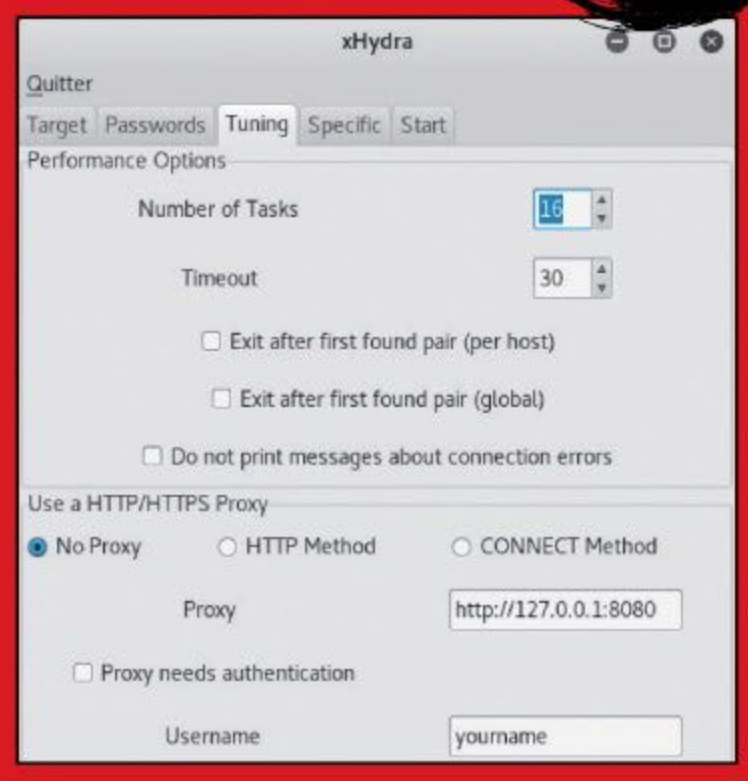
Si vous avez oublié le mot de passe d'une archive créée avec 7-Zip, cRarck va vous aider ! Ce logiciel de brute force utilise toute la puissance de votre processeur graphique (GPU OpenCL et CUDA) pour venir à bout des mots de passe les plus solides... Attention, car les cartes graphiques intégrées ou bas de gamme se montreront parfois moins puissantes que le CPU. Et comme cRARk ne supporte pas le multicœur, il faudra d'abord savoir quel processeur utiliser.

Difficulté : ☠☠☠

Lien : **www.crark.net**

Hydra → Du crack en ligne !

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES



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. 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. 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.

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 avec Hydra. Notez que si vous n'avez pas envie d'installer ou d'utiliser Kali Linux, il existe aussi une version Windows appelée THC-Hydra.

Difficulté : ☠☠☠ Lien : **www.thc.org/thc-hydra**

xHydra sous Kali

INFOS [HYDRA]
Où le trouver ? [**www.thc.org/thc-hydra**] Difficulté : ☠☠☠

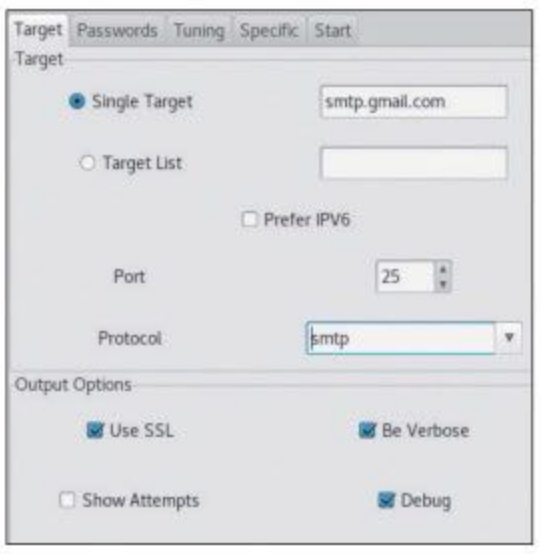
TUTO

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.

FindMyHash → Un script Python pour trouver du hash !

Le script Python FindMyHash permet de savoir à quel type de hash vous avez affaire. Pour les pirates, il suffit d'intercepter un hash dans un site Web ou une base de données pour obtenir un mot de passe valide presque à chaque coup! Pour vous, il s'agit, bien sûr, de vérifier que votre mot de passe ne figure pas dans ces bases pour éviter les surprises... En dehors du MD5, très répandu, FindMyHash permet de trouver des hash CISCO7, LM, MYSQL, NTLM, RMD160, SHA1, SHA224, SHA256, SHA384, SHA512, etc.

Difficulté : Lien : **http://code.google.com/p/findmyhash**

CrackStation → Une base de données gigantesque

Avant de vous lancer dans des recherches compliquées lorsque vous voulez trouver un mot de passe à partir d'un hash, pourquoi ne pas essayer CrackStation ? Ce site permet de retrouver le mot de passe correspondant à un hash en consultant des bases de données gigantesques où sont stockés des hash de tous types avec leur équivalent «en clair». Un mot de passe simple comme azerty été trouvé en quelques secondes. Lorsque vous avez un hash entre les mains, la consultation de ce genre de site doit être l'étape numéro 1.

Difficulté :

Lien : **https://crackstation.net**

Hash_ID → Une bonne alternative

Si Hashtag ou FindMyHash ne vous ont pas séduit et que vous cherchez un autre logiciel de ce type pour comparer, voici Hash-identifier, ou Hash_ID pour les intimes. Comme les concurrents, il va analyser les suites alphanumériques pour identifier à quel type de hash vous avez affaire. Compatible avec plus de 50sortes de hash (et leurs variantes), Hash_ID vous fera gagner un temps précieux lorsqu'il faudra lancer une attaque brute force ou dictionnaire avec John The Ripper ou Hashcat (voir les pages précédentes)...

Difficulté :

Lien : **https://code.google.com/p/hash-identifier**

Hashtag → Le plus efficace

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

Pour cibler directement la recherche du mot de passe sur un type de hash précis, nous utilisons le script Python HashTag. Ce dernier va reconnaître l'empreinte d'un hash pour vous désigner son type : MD5, SHA, MySQL, etc. Parfois HashTag ne trouvera pas précisément le type utilisé, mais vous donnera un panel de possibilité (car certains hash sont très proches au niveau de leurs structures). C'est largement suffisant pour gagner du temps et éliminer une bonne centaine de fonctions...

Difficulté : ☠☠☠ Lien : **http://goo.gl/vQx8E9**

```
C:\Python27>python hashtag.py -sh df6b9fb15cfdbb7527be5a8a(
79a943438e9d3d85ebfc2ccf9e0eccd9346026c0b6876e0e01556fe56f:
5a

Hash: df6b9fb15cfdbb7527be5a8a6e39f39e572c8ddb943fbc79a943·
ccd9346026c0b6876e0e01556fe56f135582c05fbdbb505d46755a

[*] Keccak-512
[*] Skein-1024(512)
[*] Skein-512
[*] SHA512 - Hashcat Mode 1700
[*] sha512($pass.$salt) - Hashcat Mode 1710
[*] sha512($salt.$pass) - Hashcat Mode 1720
[*] SHA-512(HMAC)
[*] Whirlpool - Hashcat Mode 6100
[*] Whirlpool(HMAC)
[*] sha512(unicode($pass).$salt) - Hashcat Mode 1730
[*] sha512($salt.unicode($pass)) - Hashcat Mode 1740
[*] HMAC-SHA512 (key = $pass) - Hashcat Mode 1750

C:\Python27>_
```

LEXIQUE

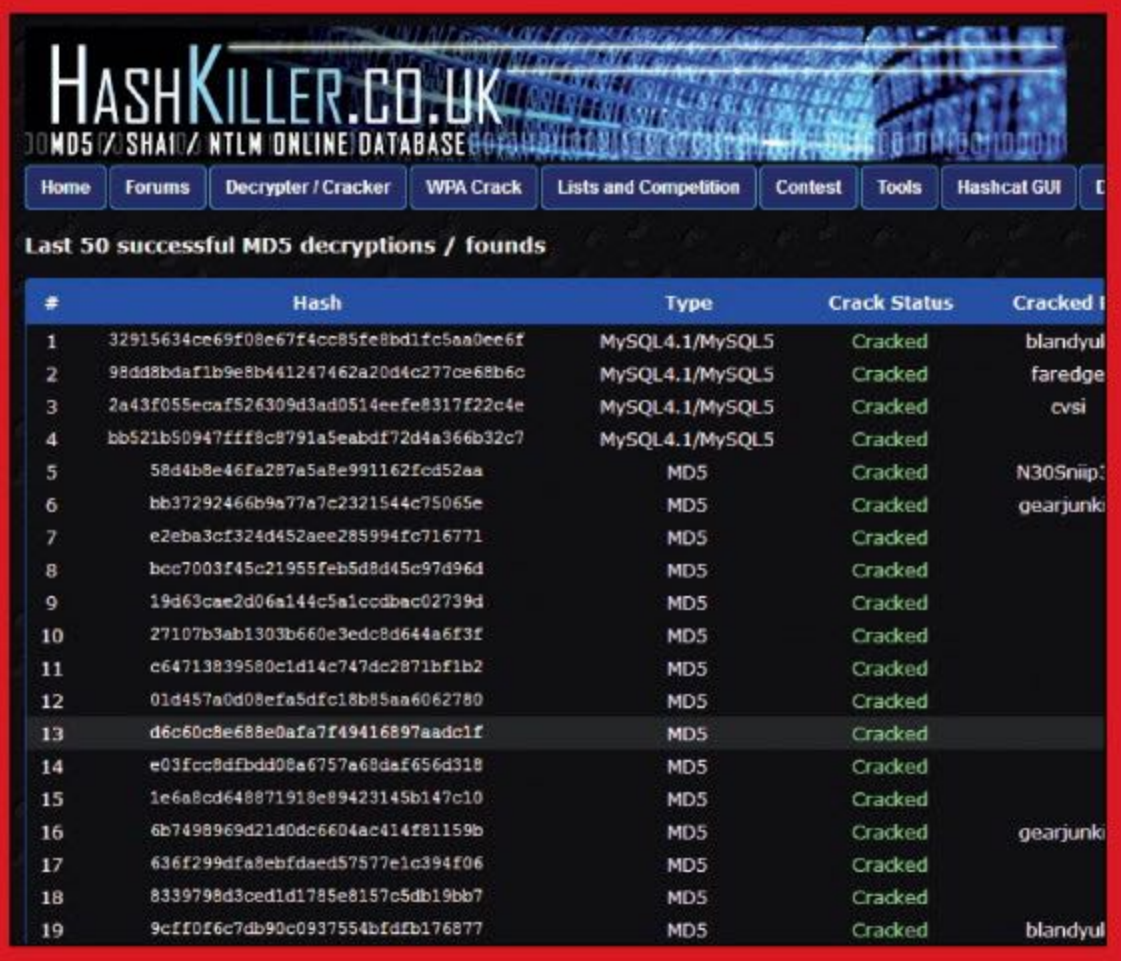
HASH : Les mots de passe ne sont jamais écrits en clair dans une base de données ou un ordinateur, ils sont codés avec une fonction de hachage. Il en existe plusieurs : MD5, SHA256, NTML, etc. Une fois ces hash interceptés, il faudra les faire "parler" et tenter de découvrir quel sésame se cache derrière avec des logiciels comme John The Ripper ou Hashcat. Notez qu'un hash comme **721a9b52bfceacc503c0 56e3b9b93cfa** ne correspond qu'à un seul mot de passe.

HashKiller → En savoir plus...

Vous voulez en savoir plus sur les hash ? HashKiller est un site qui contient une mine d'informations et d'outils sur ce sujet: des logiciels, des décrypteurs, des dictionnaires de mots et des tutos. Le site propose aussi parfois des concours et si vous ne savez pas par où commencer, vous pouvez aller sur le forum pour poser vos questions.

Difficulté : ☠☠☠

Lien : **www.hashkiller.co.uk**



#	Hash	Type	Crack Status	Cracked
1	32915634ce69f08e67f4cc85fe8bd1fc5aa0ee6f	MySQL4.1/MySQL5	Cracked	blandyul
2	98dd8bdaf1b9e8b441247462a20d4c277ce68b6c	MySQL4.1/MySQL5	Cracked	faredge
3	2a43f055ecaf526309d3ad0514eefe8317f22c4e	MySQL4.1/MySQL5	Cracked	cvsi
4	bb521b50947fff8c8791a5eabdf72d4a366b32c7	MySQL4.1/MySQL5	Cracked	
5	58d4b8e46fa287a5a8e991162fcd52aa	MD5	Cracked	N30Sniip:
6	bb37292466b9a77a7c2321544c75065e	MD5	Cracked	gearjunk
7	e2eba3cf324d452aee285994fc716771	MD5	Cracked	
8	bcc7003f45c21955feb5d8d45c97d96d	MD5	Cracked	
9	19d63cae2d06a144c5a1ccdbac02739d	MD5	Cracked	
10	27107b3ab1303b660e3edc8d644a6f3f	MD5	Cracked	
11	c64713839580c1d14c747dc2871bf1b2	MD5	Cracked	
12	01d457a0d08efa5dfc18b85aa6062780	MD5	Cracked	
13	d6c60c8e688e0afa7f49416897aadc1f	MD5	Cracked	
14	e03fcc8dfbdd08a6757a68daf656d318	MD5	Cracked	
15	1e6a8cd648871918e89423145b147c10	MD5	Cracked	
16	6b7498969d21d0dc6604ac414f81159b	MD5	Cracked	gearjunk
17	636f299dfa8ebfdaed57577e1c394f06	MD5	Cracked	
18	8339798d3ced1d1785e8157c5db19bb7	MD5	Cracked	
19	9cff0f6c7db90c0937554bfdfb176877	MD5	Cracked	blandyul

Utilisation de HashTag.py

Notre but est de connaître le type d'un hash pour qu'il soit plus rapide avec Hashcat ou John The Ripper de trouver le mot de passe correspondant. En effet ce genre de logiciels ne peut cracker différents types de hash en même temps. En sachant «où regarder», vous gagnerez un temps fou !

TUTO

INFOS [HashTag.py]

Où le trouver ? [**http://goo.gl/vQx8E9**]

Difficulté :

01› INSTALLATION

Avant de commencer, il va falloir installer le langage Python sur votre machine. Préférez la version2.7 et ne changez pas le répertoire d'installation par défaut. Téléchargez ensuite HashTag.py en suivant notre lien. En bas de la page, faites un clic droit dans le lien et faites **Enregistrer la cible du lien sous**. Placez-le ensuite dans le répertoire **C:\Python27**. Avec tout ça, vous êtes prêt ! Faites **Maj + clic droit** dans le répertoire **C:\Python27** et choisissez **Ouvrir une fenêtre de commandes ici**. Il faudra alors taper **python hashtag.py -sh [votre hash]**.

02› LA RECHERCHE

Lors de notre premier essai, nous n'avons pas eu de chance, car le hash choisi pouvait potentiellement être d'une vingtaine de types différents. Dans ce cas, il vaudra mieux commencer la recherche par les plus fréquents. Notre deuxième essai a été plus concluant puisqu'en excluant les variantes, HashTag nous a permis de réduire le champ de recherche à 4 types de hash différents! Nous savons ici que cette suite alphanumérique a de grandes chances d'être un SHA-512.

```
#!/usr/bin/python
"""
Name:           HashTag: Parse and Identify Password Hashes
Version:        0.41
Date:           11/05/2013
Author:         Smeege
Contact:        SmeegeSec@gmail.com

Description:    HashTag.py is a python script written to parse and ide
                which consist of identifying a single hash type (-sh),
                file (-f), and traversing subdirectories to locate fi
                Many common hash types are supported by the CPU and GP
                argument (-hc) hashcat modes will be included in the o

Copyright (c) 2013, Smeege Sec (http://www.smeegesec.com)
All rights reserved.
Please see the attached LICENSE file for additional licensing informat
"""
import argparse
import mimetypes
import os
import shutil
import string

parser = argparse.ArgumentParser(prog='HashTag.py', usage='%(prog)s [-
argGroup = parser.add_mutually_exclusive_group(required=True)
argGroup.add_argument("-sh", "--singleHash", type=str, help="Identify
argGroup.add_argument("-f", "--file", type=str, help="Parse a single f
argGroup.add_argument("-d", "--directory", type=str, help="Parse, iden
parser.add_argument("-o", "--output", type=str, help="Filename to outp
parser.add_argument("-hc", "--hashcatOutput", action='store_true', def
parser.add_argument("-n", "--notFound", action='store_true', default=F
args = parser.parse_args()

hashDict = dict()

hashcatDict = { \
'MD5': '0', 'md5($pass.$salt)': '10', 'Joomla': '11', 'md5($salt.$pass
```

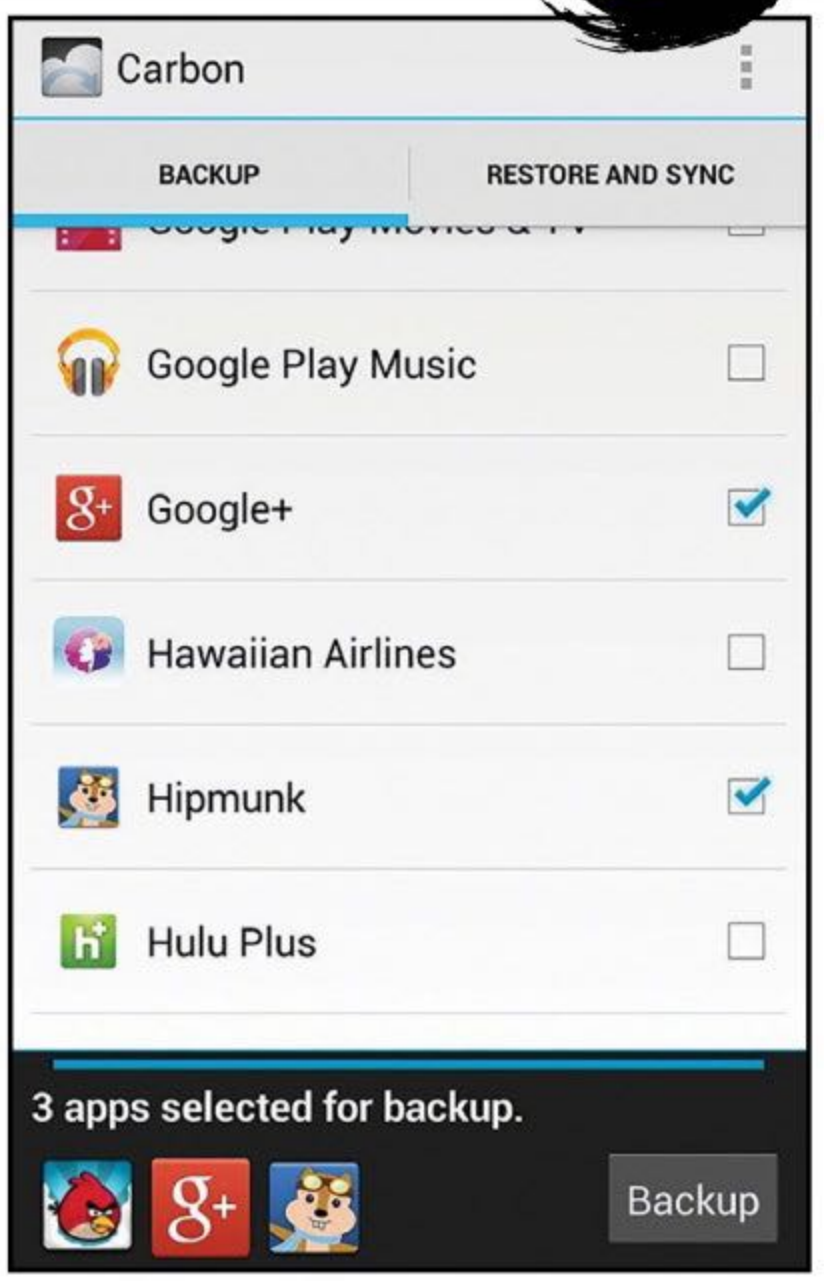
```
C:\Windows\system32\cmd.exe

C:\Python27>python hashtag.py -sh 721a9

Hash: 721a9b52bfceacc503c056e3b9b93cfa

[*] MD5 - Hashcat Mode 0
[*] NTLM - Hashcat Mode 1000
[*] MD4 - Hashcat Mode 900
[*] LM - Hashcat Mode 3000
[*] RAdmin v2.x
[*] Haval-128
[*] MD2
[*] RipeMD-128
[*] Tiger-128
[*] Snefru-128
[*] MD5(HMAC)
[*] MD4(HMAC)
[*] Haval-128(HMAC)
[*] RipeMD-128(HMAC)
[*] Tiger-128(HMAC)
[*] Snefru-128(HMAC)
[*] MD2(HMAC)
[*] MD5(ZipMonster)
[*] MD5(HMAC(Wordpress))
[*] Skein-256(128)
```

Helium → Sans root

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

Helium sauvegarde les applications, (et leurs données), les contacts, les SMS... Pour résumer, tout ce que contient votre appareil Android. Ainsi en cas de pépin (perte ou vol de ce dernier), vous pourrez tout restaurer depuis votre PC, vers votre nouvel Androphone. Cerise sur le gâteau, Helium est très facile à utiliser et vous n'êtes pas obligé de rooter votre téléphone pour en profiter.

Difficulté : ☠☠☠ Lien : **https://goo.gl/cwPSV**



LEXIQUE

ROOT : Le root est une manipulation issue du monde Unix permettant d'avoir les «pleins pouvoirs» sur votre mobile Android. Une fois que votre mobile est rooté, il y est même après un redémarrage. Pour en savoir plus : **www.android-mt.com !**

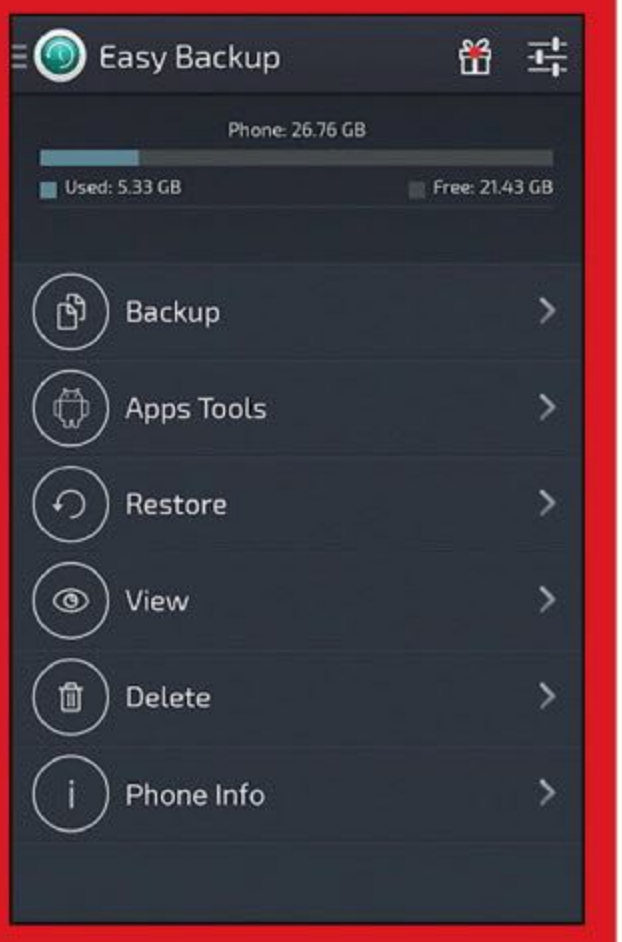
Hash_ID

→ Une bonne alternative

Si Hashtag ou FindMyHash ne vous ont pas séduit et que vous cherchez un autre logiciel de ce type pour comparer, voici Hash-identifier, ou Hash_ID pour les intimes. Comme les concurrents, il va analyser les suites alphanumériques pour identifier à quel type de hash vous avez affaire. Compatible avec plus de 50sortes de hash (et leurs variantes), Hash_ID vous fera gagner un temps précieux lorsqu'il faudra lancer une attaque brute force ou dictionnaire avec John The Ripper ou Hashcat (voir les pages précédentes)...

Difficulté : ☠☠☠

Lien : **https://code.google.com/p/hash-identifier**



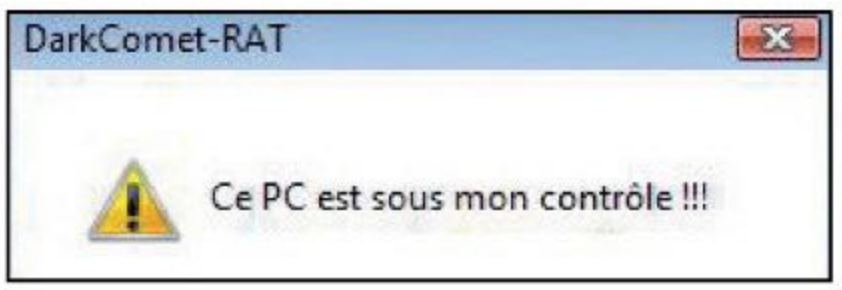
DarkComet RAT

→ Un vrai RAT underground

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

DarkComet est un RAT : un logiciel permettant de prendre le contrôle d'une machine. Pour dépanner un ami ou surveiller ce qui se passe sur votre second PC, pas de problème ! Mais en utilisant certaines options, il est possible de manipuler un ordinateur sans le consentement de son propriétaire. DarkComet fonctionne selon le modèle client/serveur. Le client est installé sur votre machine et le serveur (ou stub) est créé sur mesure par l'utilisateur. Il prendra la forme d'un fichier EXE que votre ami devra lancer. Même si les intentions du développeur n'ont jamais été de faire un logiciel malveillant, il faut reconnaître que les options pour camoufler ce fichier EXE et le rendre persistant sur une machine sont assez puissantes.

Difficulté : Lien : **http://goo.gl/MSTKbs**

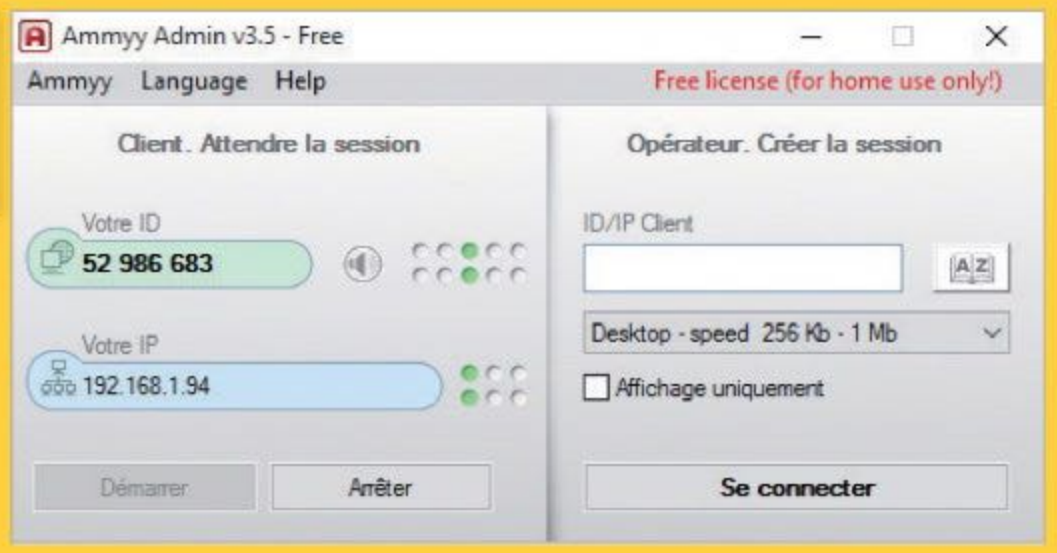


LEXIQUE

RAT : Abréviation de Remote Administration Tool ou Outil d'administration à distance en français. Il ne s'agit pas d'un malware, mais d'un programme permettant d'avoir accès au contenu d'un PC sans être physiquement présent (dépannage, accès à des fichiers, etc.). Ce type de logiciel peut bien sûr être utilisé à des fins malhonnêtes pour s'introduire sur l'ordinateur d'un tiers sans son consentement.

AMMYY Admin

→ La solution la plus simple



AMMYY Admin est un logiciel de contrôle à distance très simple. À la différence de DarkComet, celui-ci est destiné aux utilisateurs débutants et ne présente pas d'options «sans consentement». Ce mini-programme de 400 Ko n'a pas besoin d'être installé et fonctionne autant comme un client que comme un serveur. Il suffit de le lancer et d'obtenir l'ID de la machine auquel vous voulez vous connecter. Vous pourrez alors dépanner un ami, avoir accès à vos fichiers sur un autre PC...

Difficulté : Lien : **www.ammyy.com**

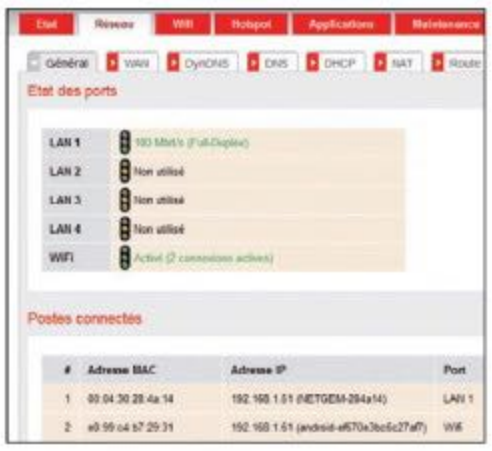
Paramétrage de DarkComet RAT

INFOS [DARKCOMET RAT]
Où le trouver ? [**http://goo.gl/MSTKbs**] Difficulté : ☠☠☠

TUTO

01› RÉGLAGE SUR LA BOX

Avant de commencer à bidouiller avec DarkComet, il faudra d'abord ouvrir le port **1604** sur votre box puisque c'est le port qui sera en écoute sur le logiciel. Ouvrez votre navigateur et tapez **192.168.1.1** (pour les abonnés Free, il faudra aller sur free.fr et pour d'autres FAI sur **192.168.0.1**) pour avoir accès aux réglages de votre box. Après avoir rentré vos identifiants d'abonnés, vous pourrez avoir la liste des appareils connectés à votre box ainsi que leurs IP.

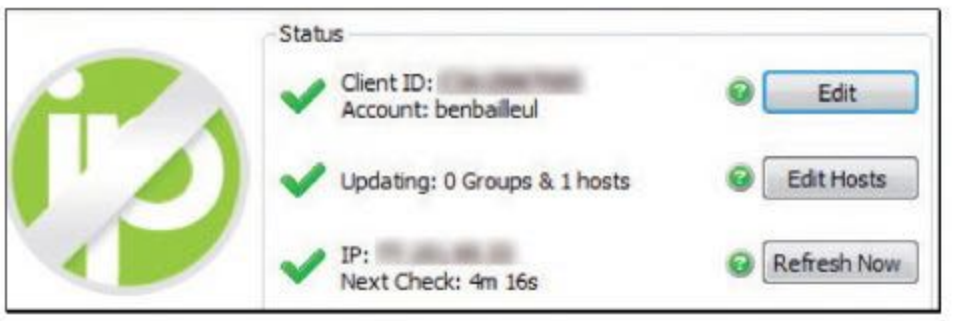


02› OUVERTURE DU PORT 1604

Notez l'IP locale de votre PC puis dirigez-vous vers un menu du type **Translation de ports** ou **NAT** (les noms des réglages peuvent varier suivant les box des FAI). Mettez l'IP de votre PC dans l'IP de destination ainsi que le numéro de port 1604 en externe et en destination. Choisissez **TCP** comme protocole, validez et refaites la même chose avec **UDP**. Votre port 1604 est libéré !
Il faudra aussi paramétrer une redirection de DNS pour que le serveur (le logiciel installé sur l'ordinateur «victime») puisse communiquer avec le client (la partie du logiciel installé sur votre PC) quels que soient les changements d'IP opérés par votre FAI. Heureusement, nous avons sous la main le service gratuit No-IP !

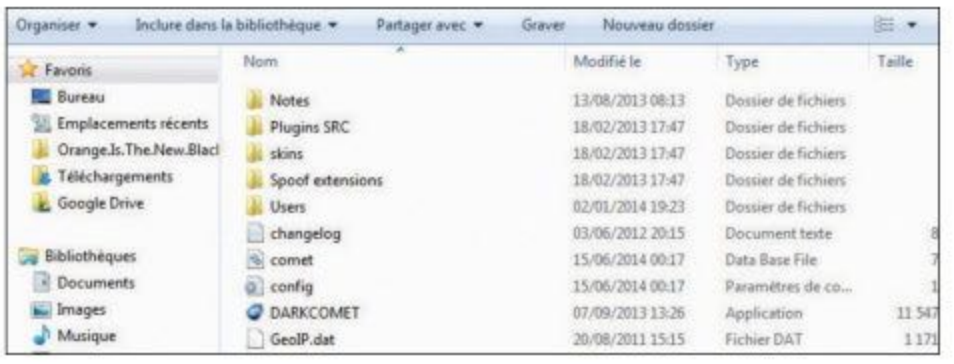
03› CHANGEMENT DE DNS

Sur la page principale du site, faites **Sign Up** et créez votre compte. Choisissez votre nom de domaine et optez pour la solution gratuite. Faites ensuite **Add a Host** et choisissez-vous un nom de domaine. Ne touchez à rien d'autre et validez en bas du formulaire. Faites **Download Update Client** et installez ce petit logiciel permettant de retrouver votre IP même si cette dernière est dynamique. Lancez le DUC et entrez vos identifiants. Cliquez sur **Edit Hosts**, cochez votre nom de domaine et faites **Save**. À partir de là, le nom de domaine que vous avez choisi va rediriger vers l'IP de PC.



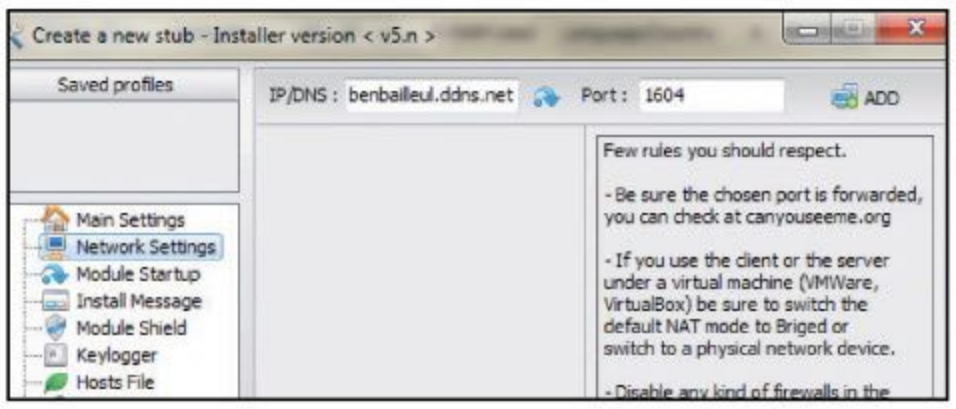
04› DARKCOMET (ENFIN !)

Il est temps de lancer DarkComet. Suivez notre lien et désactivez temporairement votre antivirus pour éviter qu'il ne hurle à la mort. Placez l'archive sur une clé USB pour la sauvegarder, car si votre antivirus se «réveille», il pourra effacer **darkcomet.exe**, même s'il est à l'intérieur du RAR. Lancez le logiciel et faites laccept. Cliquez sur **DarkComet-RAT** puis dans **Server Module** choisissez **Full editor**.



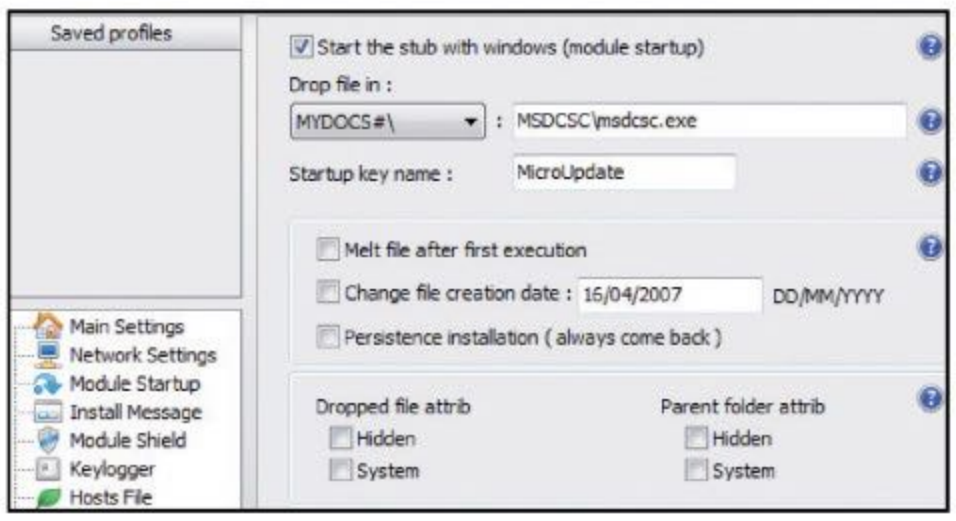
05 › CRÉATION DU «STUB»

Ici, il s'agit de créer un «stub», un programme au format EXE qui, lancé sur la machine cible, vous donnera les pleins pouvoirs sur celle-ci. Dans **Main Settings**, vous pouvez choisir un mot de passe (qu'il faudra entrer à nouveau dans **Clients settings** ultérieurement. Cliquez quelques fois sur **Random** en face de **Process Mutex** et faites **Active FWB** pour outrepasser le firewall de la machine cible. Dans **Network Settings**, mettez le DNS que vous avez créé (le nom de domaine de No-IP) et laissez le port **1604**. Faites ensuite **Add** pour ajouter votre DNS à la liste.



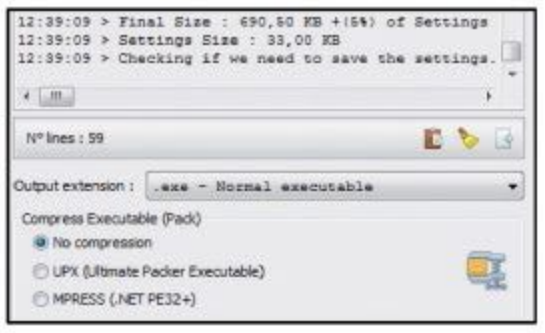
06 › RÉGLAGES ET FONCTIONNALITÉS

Dans **Module startup**, cochez **Start the stub with Windows**. Dans **Install message**, choisissez une icône et un message qui annoncera à l'utilisateur de la machine cible que le stub est bien installé (bien sûr, un méchant hacker mettra ici un message rassurant...). Les autres paramètres sont optionnels, mais rien ne vous empêche de bidouiller un peu. Vous trouverez notamment un **Keylogger**, un **File binder** permettant d'ajouter des fichiers à l'EXE et une option pour changer l'icône du stub, modifier le fichier host de la cible, rendre le stub persistant, faire disparaître l'EXE quand il sera installé, etc.



07 › LES TECHNIQUES DE FILOUS

Module Shield permet de faciliter une éventuelle infection, mais comme il s'agit ici de prendre le contrôle de la machine d'un ami, nous n'utiliserons pas ces fonctions. De même, dans **Stub Finalization**, vous pourrez camoufler le EXE ou le compresser pour qu'il ait l'air d'un programme autorisé. Lorsque vous avez fini vos réglages, faites **Build the stub** et donnez-lui un nom. On vous demandera si vous désirez garder en mémoire ce profil. Faites **Yes** pour ne pas avoir à tout recommencer au cas où votre premier essai n'est pas concluant.



08 › L'ACCÈS À LA MACHINE

Il est temps de placer le fichier stub sur la machine de la «victime». Comme vous n'avez pas utilisé de méthode de brigands, il faudra aussi désactiver l'antivirus. Lancez l'EXE. Sur votre PC, allez dans **DarkComet-RAT** et faites **Listen to new port** puis **Listen**. Normalement, vous verrez le PC cible dans ID. Bravo vous avez un accès à cette machine !

09 › UN CONTRÔLE TOTAL

Double-cliquez dessus pour profiter des nombreuses options : tchat, récupération de mot de passe, spyware, explorateur de fichiers, extinction ou mise en veille du PC, etc. Il est même possible de jouer un air de piano à votre ami ! En faisant un clic droit dans **Quick Window Open**, vous aurez même accès au **Bureau** de Windows ou à la webcam ! Voilà, nous vous laissons découvrir toutes les fonctionnalités de ce logiciel très puissant...

DeEgger → Le tout terrain

Les logiciels que nous vous proposons permettent souvent de cacher message ou documents dans une photo. Et si vous dissimuliez des éléments dans d'autres types de fichiers ? Avec DeEgger, vous envoyez des messages ou des documents sensibles cachés dans des fichiers MP3, WMA , JPEG, PNG, TIFF, AVI, MOV, MP4, 3GP et SWF ! N'oubliez pas de ne pas toucher à votre fichier final. Une compression ou une conversion serait fatale à votre fichier caché !

Difficulté :

Lien : **http://goo.gl/mS1Tz**

Crypstagram → La stégano en ligne !

Le service Crypstagram propose à peu près la même chose que les logiciels de stégano sauf qu'ici, vous n'aurez rien à installer ! Il suffit d'uploader une image, de mettre son message secret et éventuellement un mot de passe pour sécuriser la dissimulation. Il est aussi possible d'utiliser l'empreinte numérique d'un fichier que vous posséder en lieu et place d'un sésame qui pourra toujours être découvert. Et pour le déchiffrage ? Vous devrez aussi passer par le service. Il est amusant de noter que Crypstagram propose des filtres un peu rétro à la mode et un «mur» où vous pourrez placer votre création si vous le désirez.

Difficulté :

Lien : **http://cryptstagram.com**

Stegano → Le plus complet

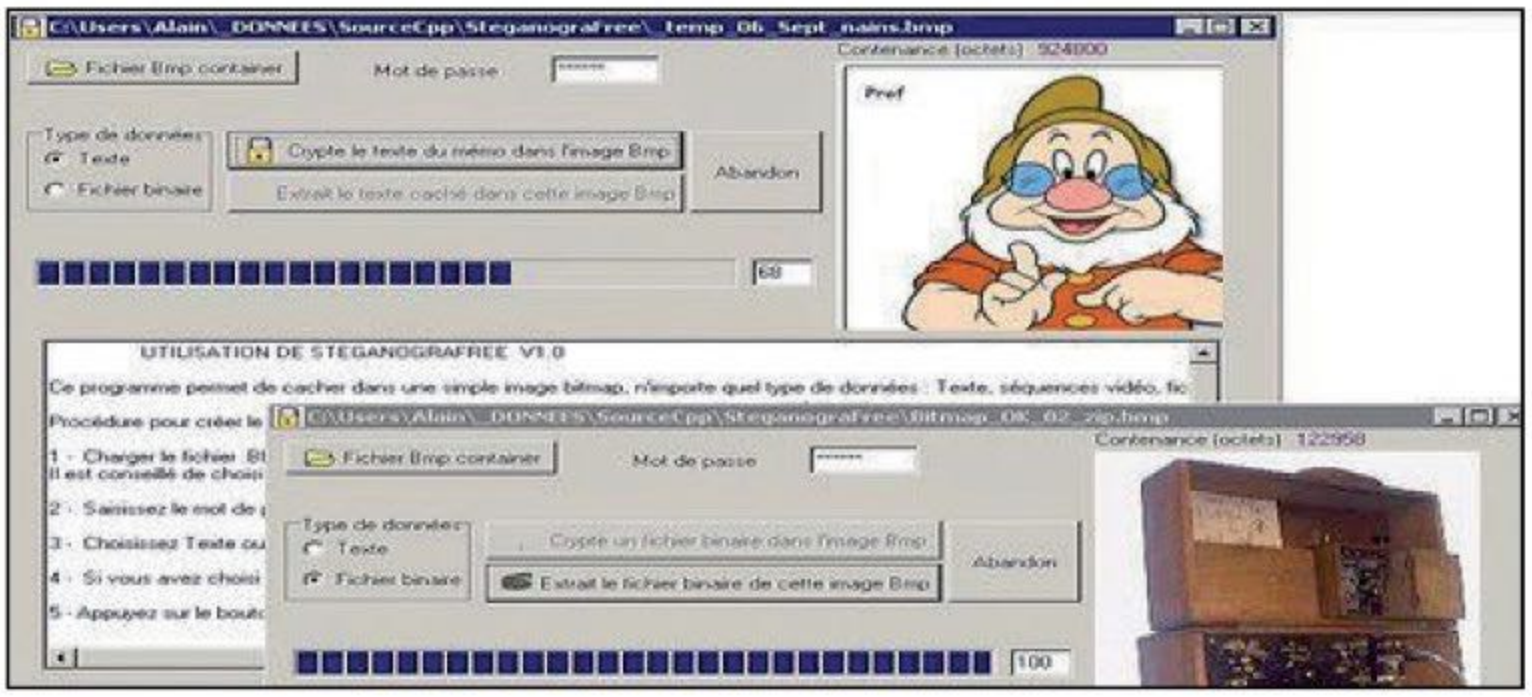
VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

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 Segano, tout en français, permet de réaliser facilement ce tour de force...

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

SteganograFree → Très efficace

Ce programme de stéganographie permet de cacher dans une simple image bitmap n'importe quel type de données : texte, séquences vidéo, fichiers sons, PDF, XLS, Word, images, ZIP, etc. Dans un BMP de 16 Mo, vous pourrez cacher jusqu'à 8 Mo de données ! L'image résultante aura exactement le même nombre d'octets que l'image originale et il sera absolument impossible de savoir s'il s'agit d'une image renfermant des données cachées.



Difficulté : ☠☠☠

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

LEXIQUE

STÉGANOGRAPHIE : Il s'agit d'un procédé qui consiste à dissimuler un message dans un autre document pour berner un éventuel petit curieux. Le document d'apparence anodine cache alors des informations sensibles qu'il est possible de faire parvenir sans éveiller les soupçons de la police ou d'un gouvernement totalitaire. Il aussi est possible d'ajouter une couche de chiffrement pour que le message reste secret même s'il est découvert.

OpenPuff → Le choix du chiffrement

Ce logiciel ne nécessitant aucune installation propose de dissimuler un document dans des fichiers JPG, WAV, MP3, MP4, MPG, FLV, SWF ou PDF. L'outil est basé sur la bibliothèque libObfuscate et permet de choisir la couche de chiffrement que vous désirez : AES 256, Serpent, Twofish, RC6, etc. Notons qu'il est possible de nettoyer les traces des fichiers dissimulés sur le disque dur avec un effacement en plusieurs passes.

Difficulté : ☠☠☠ Lien : **http://goo.gl/ihehHM**

Dissimulez des documents avec Stegano

INFOS [STEGANO]
Où le trouver ? [**http://tinyurl.com/3vggnxt**] Difficulté : ☠☠☠

TUTO

01› L'IMAGE D'ORIGINE

Une fois installé, démarrez le logiciel puis, dans l'onglet **Image d'origine**, cliquez sur les trois petits points pour ouvrir l'image de votre choix. Dans notre exemple, cette image de petite fille pèse 2529552 octets. Le logiciel vous informe alors qu'il est possible d'y dissimuler un fichier ou un texte de 1789694 octets ! Nous avons délibérément réduit la taille de l'image pour plus de visibilité, mais plus la photo est volumineuse et plus pour pourrez y cacher des infos.

02› UN MOT DE PASSE ?

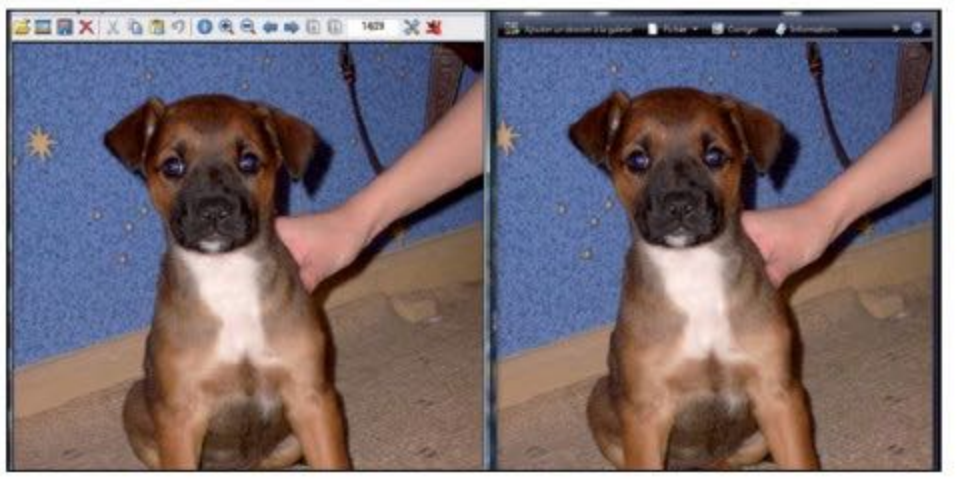
Dirigez-vous ensuite vers le deuxième onglet (**Fichier à crypter**). Ici, vous avez le choix entre taper directement un texte ou choisir un fichier de votre disque dur. Il est tout à fait envisageable de placer une autre image à l'intérieur de la première... Pour plus de sécurité, le logiciel vous permet, en plus, d'ajouter un mot de passe. En effet, si un intercepteur connaît cette méthode de dissimulation (ici, le message est caché dans les octets qui codent les couleurs), il faudra en plus qu'il connaisse le mot de passe.

03› L'IMAGE FINALE

Cliquez enfin sur **Fabriquer l'image** pour faire apparaître votre image modifiée. Sélectionnez, ensuite **Enregistrer l'image ci-dessous avec ce nom** pour sauver votre fichier sur le disque dur. Celle-ci se nomme **Message**, il faudra donc changer le nom, car une image de petite fille qui porte ce nom est plutôt suspecte. Notez que votre image finale est au format Bitmap (BMP), car ce type de fichier n'est pas compressé.

04› LA RESTITUTION DU MESSAGE

En effet, une compression en JPEG occasionnerait la perte pure et simple de votre message. Ne modifiez donc pas votre image si vous voulez que l'astuce fonctionne ! Vous pouvez vous amuser à comparer l'image de départ et l'image modifiée, mais les différences sont invisibles... Armé du même logiciel, le destinataire devra ouvrir l'image dans le troisième onglet, entrer le mot de passe et cliquer sur **Décrypter l'image**. Il retrouvera alors notre message caché dans notre second essai avec un gentil toutou.



RouterPasswords → Mots de passe de routeurs

RouterPasswords.com est un site qui répertorie les mots de passe par défauts de centaines de routeurs différents. Il suffit de sélectionner la marque et le modèle pour accéder au couple identifiant/mot de passe ainsi qu'au protocole d'échange de donnée. Si vous êtes un administrateur ou que vous dépannez souvent vos amis étourdis, vous aurez donc accès aux réglages à condition que les utilisateurs n'aient pas changé les identifiants. Si vous ne trouvez pas le modèle exact du routeur que vous recherchez, essayez un mot de passe à partir d'un modèle alternatif du même fabricant !

Difficulté : Lien : **www.routerpasswords.com**

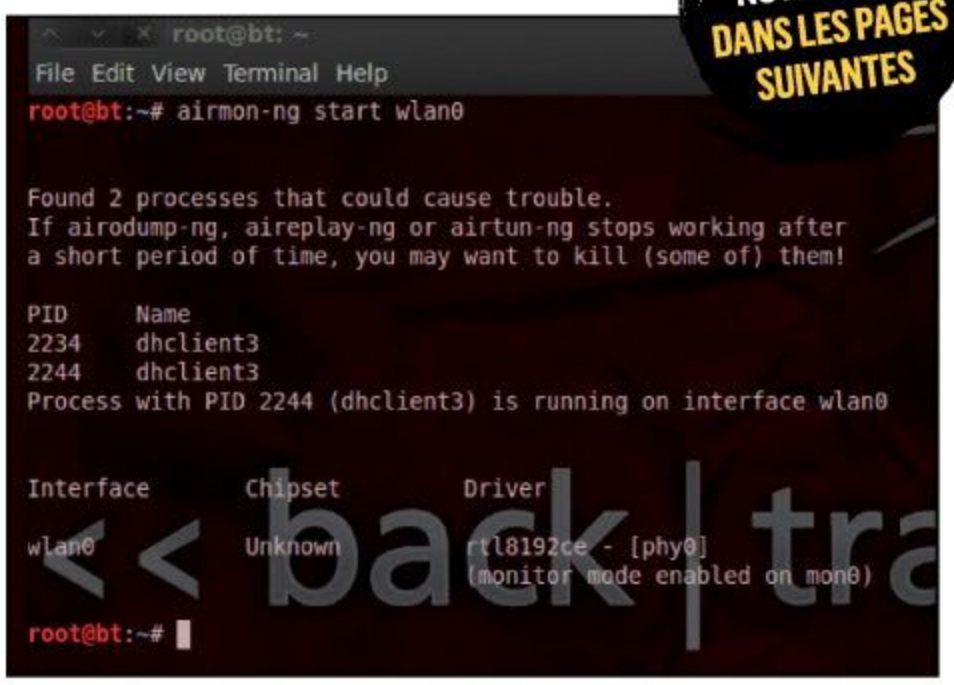
Aircrack-ng → Un classique intégré à Kali Linux

Aircrack-ng est un ensemble d'outils pour l'audit des réseaux sans fil intégré à la distribution Kali Linux. Sous réserve d'avoir un adaptateur WiFi compatible avec le DPI, le logiciel va analyser les paquets de données transitant entre le point d'accès et un appareil qui tente se s'y connecter. Qu'il s'agisse d'une clé WEP ou WPA, Aircrack-ng va récupérer la clé en utilisant la méthode brute force.

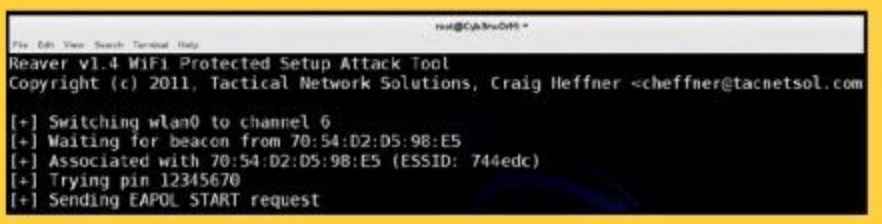
Difficulté :

Lien : **www.aircrack-ng.org**

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES



Reaver-wps → Utilisation de la méthode WPS



Si vous avez une box récente, vous êtes sans doute équipé d'un dispositif WPS. Il s'agit d'un petit bouton qui permet d'autoriser temporairement l'accès à un appareil sur votre réseau. Le but est de se connecter sans mot de passe et avec un risque très restreint puisque l'accès est refermé au bout de quelques secondes afin d'éviter les intrus. Cependant, certains appareils disposant de cette sécurité WPS connaissent une faille permettant un mode «open bar». Notez que Reaver fonctionne de concert avec Aircrack. Si l'utilisation de ce logicielvous intéresse, voici un petit tuto en attendant notre article complet dans un prochain numéro: http://goo.gl/VsC0w8.

Difficulté :

Lien : **https://goo.gl/QLWXN4**

LEXIQUE

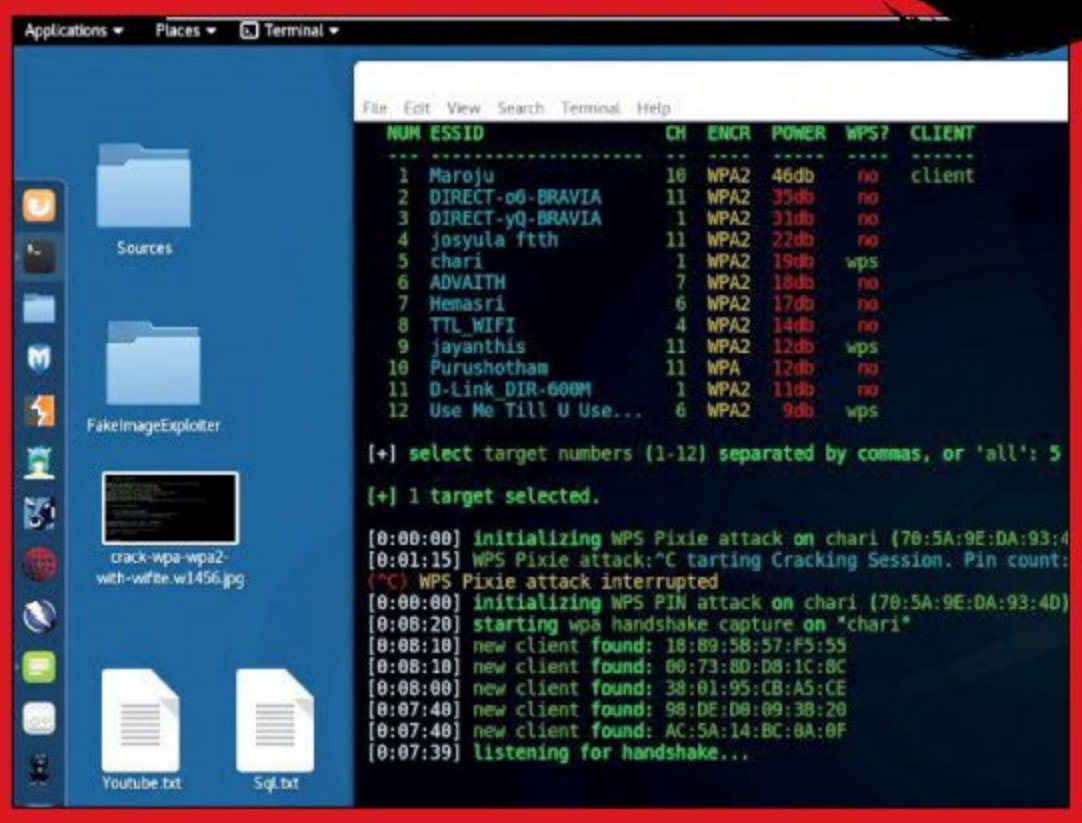
CLÉ WIFI : C'est le mot de passe à votre réseau sans fil domestique. Cette clé peut être au format WEP ou WPA. Le premier protocole est dépassé et doit être absolument proscrit tandis que le deuxième (toute version) est plus solide et ne peut être attaqué que par des attaques complexes.

ROUTEUR : C'est la machine qui relie votre réseau domestique à Internet. Cela peut être votre box ou un appareil du même type non fourni par votre FAI.

WiFite → Automatiser le pentest WiFi

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

Intégré à la distribution Kali Linux, 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 !



Difficulté : ☠☠☠ Lien : **https://github.com/derv82/wifite**

Testez la solidité de votre réseau avec Kali Linux et Aircrack-ng

INFOS [AIRCRACK-NG]
Où le trouver ? [**www.aircrack-ng.org**] Difficulté : ☠☠☠

TUTO

NB : les crochets [et] ne doivent pas être tapés

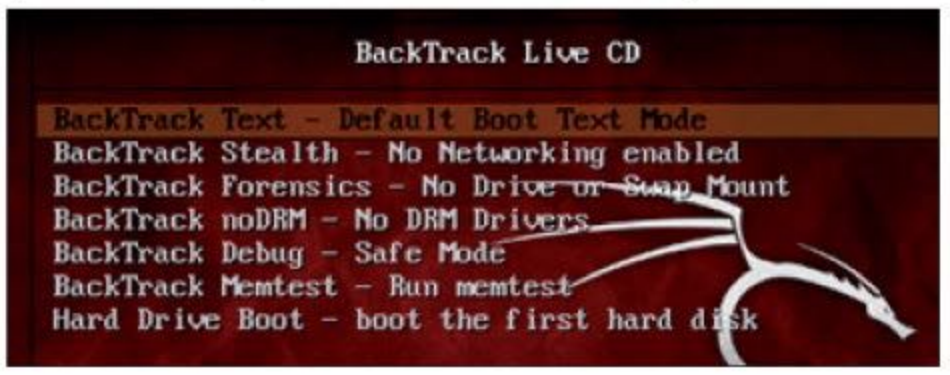
01› PRÉREQUIS

Pour cette démonstration, il vous faudra disposer de Kali Linux et d'une clé Wi-Fi qui soit compatible avec la méthode d'injection de paquets. Pour le savoir, nous vous invitons à regarder sur cette liste (**http://goo.gl/m4Fv8**) ou à tester votre matériel dans Kali. Faites **# aireplay-ng -9 mon0**. Si **Injection is working** apparaît, c'est que votre périphérique Wi-Fi est compatible. Dans le cas contraire, il faudra peut-être mettre à jour le pilote (Google est votre ami !).

```
root@kali:~# aireplay-ng -9 mon0
13:41:33  Trying broadcast probe requests...
13:41:33  Injection is working!
13:41:35  Found 1 AP

13:41:35  Trying directed probe requests...
13:41:35  10:BF:48:          channel: 1 - 'rout
13:41:36  Ping (min/avg/max): 3.735ms/27.008ms/7
13:41:36  30/30: 100%

root@kali:~#
```

02› LES PREMIERS PAS

Que vous utilisiez un LiveCD ou une version normale de Kali Linux, tapez **startx** puis **Entrée** pour obtenir l'interface graphique. Dans **Applications Menu>Settings>Keyboard**, vous pourrez configurer le clavier à la française. Ouvrez le **Terminal Emulator** (dans Applications **Menu**) et faite **sairmon-ng start wlan0** et faites **Entrée** pour voir la liste des périphériques permettant de vous connecter en Wi-Fi. Normalement, vous ne devriez en avoir qu'un seul : **Mon0** (pour monitor 0).



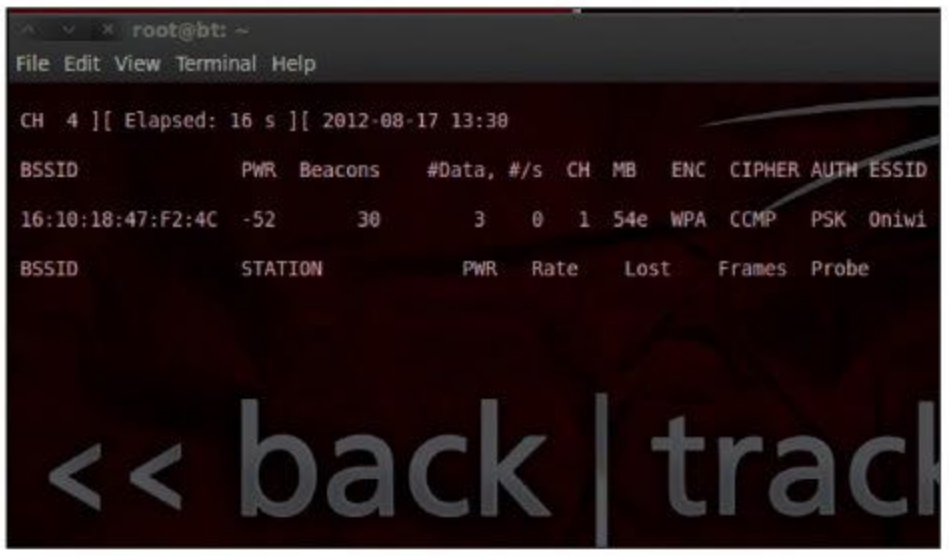
03› LISTE DES RÉSEAUX

Nous allons maintenant ouvrir une autre fenêtre pour obtenir la liste des réseaux disponibles. Tapez **airodump-ng mon0** et cherchez le nom de votre box dans la liste. Notez alors le BSSID (qui est en fait l'adresse MAC du point d'accès), car vous en aurez besoin par la suite. Notez aussi l'adresse qui figure sous **Station**. Il s'agit de l'adresse permettant de joindre un ordinateur connecté au point d'accès. Sans cette dernière, vous ne pourrez pas hacker votre clé WPA puisqu'il faut absolument qu'un ordinateur ou un appareil utilisant le Wi-Fi soit connecté sur le point d'accès que vous voulez tester.

```
CH  1 ][ Elapsed: 36 s ][ 2012-08-17 13:17

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AU

A6:15:EA:B9:3F:25  -53      102        0    0   1  54e  WPA2 CCMP   PS
A6:15:EA:B9:3F:24  -53       86        0    0   1  54e  WPA  CCMP   PS
16:10:18:47:F2:4F  -53       52        0    0   1  54e  WPA  CCMP   MG
A6:15:EA:B9:3F:27  -53      106        0    0   1  54e  WPA  CCMP   MG
00:25:15:BC:72:9C  -53       91        0    0  11  54e  WPA  CCMP   PS
92:25:15:BC:72:9D  -53       89        0    0  11  54e  OPN
F4:CA:E5:B7:F8:AE  -52      106        0    0  10  54e  WPA2 CCMP   MG
F4:CA:E5:B7:F8:AD  -53      121        0    0  10  54e  OPN
F4:CA:E5:B7:F8:AC  -52      111        0    0  10  54e  WPA  CCMP   PS
92:25:15:BC:72:9F  -52       90        0    0  11  54e  WPA2 CCMP   MG
16:10:18:47:F2:4C  -53       66        0    0   1  54e  WPA  CCMP   PS
16:10:18:47:F2:4E  -53       54        0    0   1  54e  OPN
16:10:18:47:F2:4D  -53       56        0    0   1  54e  WPA2 CCMP   PS
A6:15:EA:B9:3F:26  -53      100        0    0   1  54e  OPN

BSSID              STATION            PWR   Rate    Lost    Frames  Pr

(not associated)   00:22:3F:FF:9B:B2  -53    0 - 1      0        22  ma
```

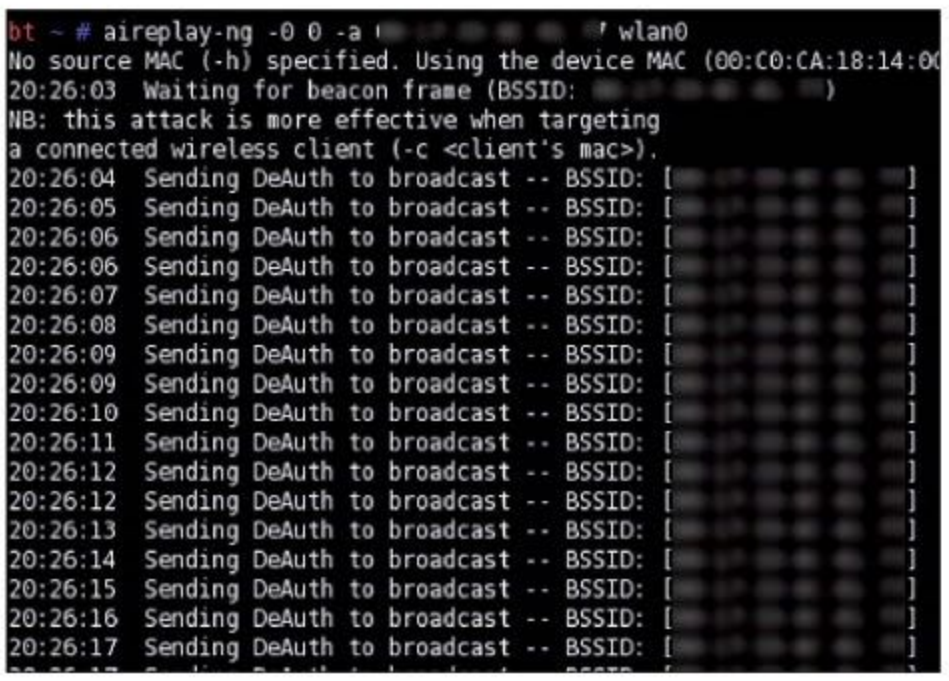
04› COMMANDE AIRODUMP

Si rien n'apparaît, ici, vous devez faire en sorte de générer un peu de trafic sur votre réseau. Connectez votre téléphone ou lancez une vidéo YouTube. Pour obtenir plus de détails et préparer la capture du handshake (le moment où deux appareils se «serrent la main»), faites **airodump-ng --write [nom de fichier] --bssid [le bssid] mon0**



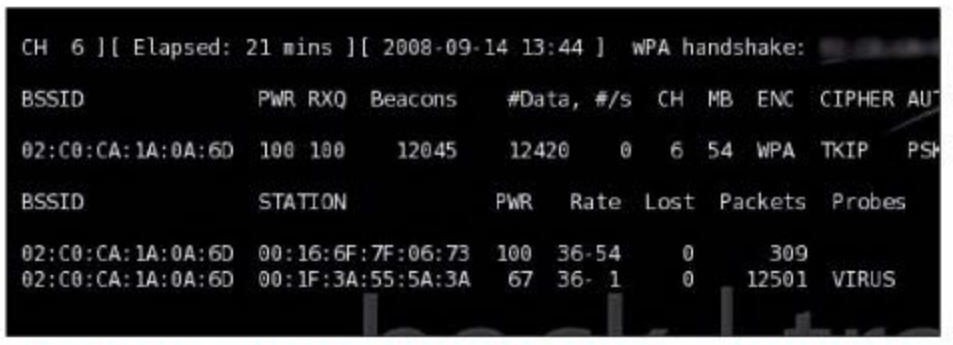
05› DÉCONNEXION DE LA STATION

Continuons par tenter de déconnecter la station du point d'accès en ouvrant deuxterminaux en parallèle :
aireplay-ng -0 0 -a [le bssid] -c [l'adresse station] mon0 et dans le second, tapez la commande **aireplay-ng -0 0 -a [le bssid] mon0**. La commande **-0** permet de faire déconnecter la station et le deuxième **0** sert à rendre infini cette fonction (la commande enverra des requêtes de désauthentification jusqu'à une déconnexion). Au bout de quelques secondes, vous pourrez arrêter l'attaque avec **Ctrl+C** dans les deux fenêtres.



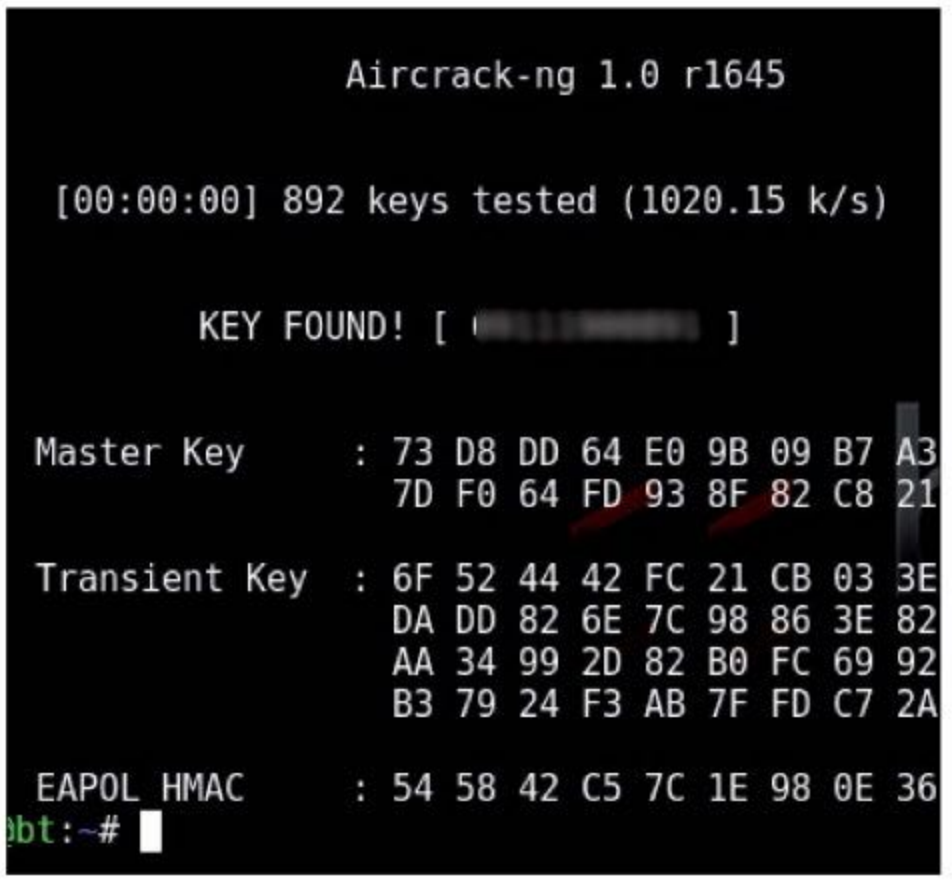
06› CAPTURE DU HANDSHAKE

Si tout s'est bien passé, vous devriez voir **WPA handshake** en haut de la fenêtre où vous avez lancé la commande **airodump**. Le handshake est maintenant dans notre fichier de capture (fonction **--write**). Sachez qu'en fonction de la force du signal, du routeur et d'autres paramètres, la capture du hanshake peut être un peu longue ou ne pas fonctionner dès la première fois.



07› BRUTE FORCE !

Il ne vous reste qu'à lancer l'attaque brute force pour trouver le bon mot de passe parmi ceux de votre dictionnaire. Tapez **aircrack-ng -w /pentest/passwords/wordlists/darkc0de.lst/ home/root/output-01.cap** puis **Entrée**. Il ne vous reste qu'à attendre. La clé testée est affichée après **Current passphrase**. Trouver le bon mot de passe peut durer un certain temps. Si votre réseau n'est pas suffisamment sécurisé, vous retrouverez donc votre mot de passe à côté de **Key found !** Il est temps de changer de sésame par quelque chose de plus solide...



WiFite : pénétrez les réseaux sans fil

INFOS [WIFITE]
Où le trouver ? [**https://github.com/derv82/wifite**] 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.

```
   2  SFR_D8C0              11  WPA   67db   wps   client
   3  NEUF_8754             11  WPA   36db   wps
   4  SFR WiFi Mobile       11  WPA2  35db    no

[+] select target numbers (1-4) separated by commas, or 'all': 2,3

[+] 2 targets selected.

[0:00:00] initializing WPS Pixie attack on SFR_D8C0 (30:7E:CB:B6:D8:C4)
[0:00:01] WPS Pixie attack:  Starting Cracking Session. Pin count: 0, Max pi..
[0:00:02] WPS Pixie attack:  Sending identity response
[0:00:03] WPS Pixie attack:  Received M1 message
[0:00:04] WPS Pixie attack:  attempting to crack and fetch psk...
[0:00:05] WPS Pixie attack failed - WPS pin not found
[0:00:00] initializing WPS PIN attack on SFR_D8C0 (30:7E:CB:B6:D8:C4)
[0:00:08] WPS attack, 0/1 success/ttl,
```

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.

```
[0:21:33] WPS Pixie attack:  WPS transaction failed (code: 0x02), re-trying ...
[0:21:34] WPS Pixie attack:  Sending identity response
[0:21:39] WPS Pixie attack:  WPS transaction failed (code: 0x02), re-trying ...
[0:21:40] WPS Pixie attack:  Sending identity response
[0:21:45] WPS Pixie attack:  WARNING: 10 failed connections in a row
[0:21:46] WPS Pixie attack:  Sending EAPOL START request
[0:21:47] WPS Pixie attack:  Sending identity response
[0:21:51] WPS Pixie attack:  WARNING: Receive timeout occurred
[0:21:52] WPS Pixie attack:  0.00% complete. Elapsed time: 0d0h21m51s.
[0:21:53] WPS Pixie attack:  Sending identity response
[0:21:58] WPS Pixie attack:  WPS transaction failed (code: 0x02), re-trying ...
[0:21:59] WPS Pixie attack:  Sending identity response
[0:22:04] WPS Pixie attack:  WPS transaction failed (code: 0x02), re-trying ...
[0:22:05] WPS Pixie attack:  Sending identity response
```

03› CAPTURER LE HANDSHAKE WPA

```
[+] 1 target selected.

[0:08:20] starting wpa handshake capture on "SFR_D8C0"
[0:08:05] listening for handshake...
[0:00:15] handshake captured! saved as "hs/SFRD8C0_30-7E-CB-B6-D8-C4.cap"

[+] 1 attack completed:

[+] 0/1 WPA attacks succeeded
       SFR_D8C0 (30:7E:CB:B6:D8:C4) handshake captured
       saved as hs/SFRD8C0_30-7E-CB-B6-D8-C4.cap

[+] starting WPA cracker on 1 handshake
[0:00:00] cracking SFR_D8C0 with aircrack-ng
[0:00:16] 6,496 keys tested (451.69 keys/sec)
```

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 Aicrack d'essayer de cracker le mot de passe contenu dans le handskake, 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**...

```
[+] 1 attack completed:

[+] 0/1 WPA attacks succeeded
       SFR_D8C0 (30:7E:CB:B6:D8:C4) handshake captured
       saved as hs/SFRD8C0_30-7E-CB-B6-D8-C4.cap

[+] starting WPA cracker on 1 handshake
[0:00:00] cracking SFR_D8C0 with aircrack-ng
[0:03:34] 95,312 keys tested (459.03 keys/sec)
[!]crack attempt failed: passphrase not in dictionary
```

NOS GUIDES WINDOWS 100% PRATIQUES

POUR UN PC

+ Puissant
+ Beau
+ Pratique
+ Sûr

Mini Prix : 3,50 €

Chez votre marchand de journaux

OS ALTERNATIFS

LEXIQUE

DUAL BOOT :
Il s'agit d'une méthode permettant d'avoir deux systèmes d'exploitation sur le même PC : Un Windows et un Linux par exemple. L'utilisateur doit faire son choix à l'allumage.

LIVE CD :
C'est une méthode pour essayer un système d'exploitation sans avoir à l'installer. La plupart des distributions Linux permettent ce genre d'action.

10 OS ALTERNATIFS POUR REMPLACER OU ÉPAULER WINDOWS

Plus léger, plus sécurisé, plus spécialisé... Les systèmes d'exploitation alternatifs ont tous de bonnes raisons d'avoir vos faveurs. Tour d'horizon de ce qu'il se fait de mieux dans le domaine.

T'es sous quoi toi ? Si l'on vous pose cette question en parlant d'informatique, c'est très rarement pour entendre "Windows" ou "Mac OS" en guise de réponse. Et pour cause : les systèmes d'exploitation alternatifs sont légions sur la toile. Majoritairement basés sur un noyau Linux, ils se déclinent sous toutes les formes, chacun y allant de sa touche personnelle. Mais pourquoi changer d'OS ? Plusieurs raisons à cela : redonner un coup de jeune à un vieux PC (les OS alternatifs sont souvent légers et peu gourmands), profiter d'une sécurité accrue (voir Qubes OS page suivante), regrouper certaines applications spécifiques (Kali Linux pour le pentesting par exemple), ou simplement pour essayer autre chose. Point commun à presque tout ce beau monde : ils sont libres, gratuits et open source. Bien sûr, il faudra faire l'impasse sur la suite Microsoft Office ou d'autre logiciels propriétaires, mais pas d'inquiétude : les alternatives embarquent souvent leurs pendants libres (LibreOffice, The Gimp...). Plus qu'à faire votre choix dans notre sélection !

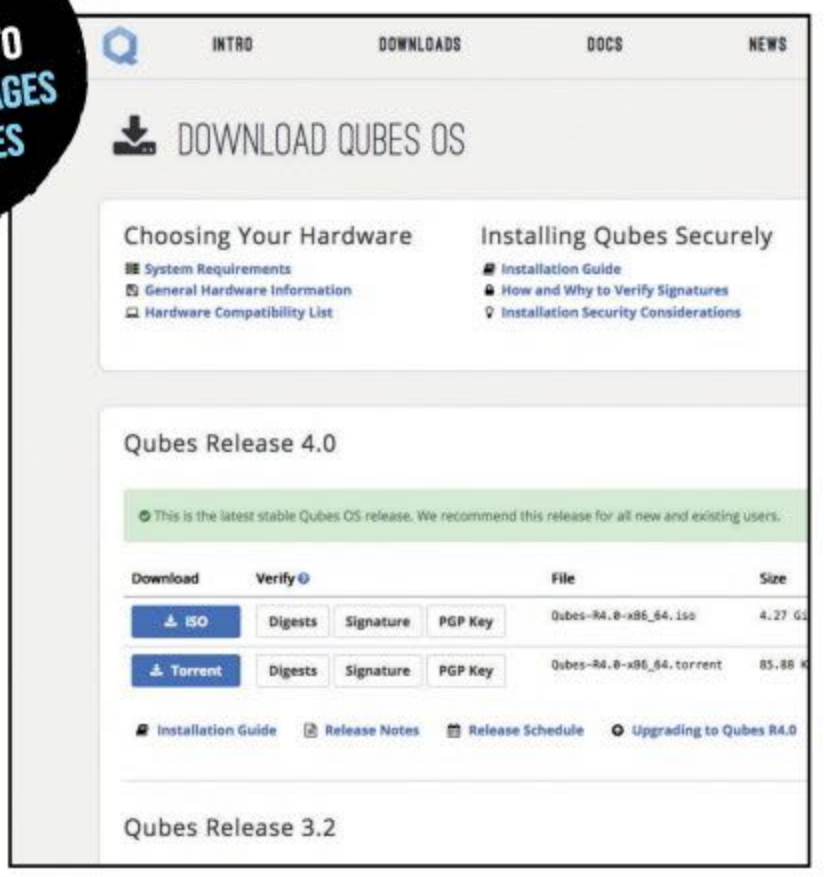
Pendant longtemps Linux a eu la réputation d'être réservé aux experts. Même si c'était le cas dans les années 90 et 2000, ce n'est plus du tout vrai ! Un OS comme Ubuntu s'installe comme un charme, reconnaît la plupart des périphériques et peut prendre place en parallèle de Windows. Cerise sur le gâteau, il est gratuit !

Qubes → Système « cloisonné »

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

Qubes OS fonctionne sur un principe de machines virtuelles (VM), ou environnements, cloisonnées. Vous pouvez par exemple avoir une VM «Travail» et une VM «Personnel», contenant chacune un navigateur Web, un traitement de texte, etc. Ce que vous faites sur l'une n'a aucune influence sur l'autre, puisque les échanges entre VM sont impossibles, sauf autorisation manuelle de votre part. Ainsi, un virus qui attaque la VM «Travail» ne pourra pas se propager aux autres VM. C'est comme si toutes vos actions s'effectuaient sur des machines différentes.

Difficulté : ☠☠☠ Lien : **qubes-os.org**

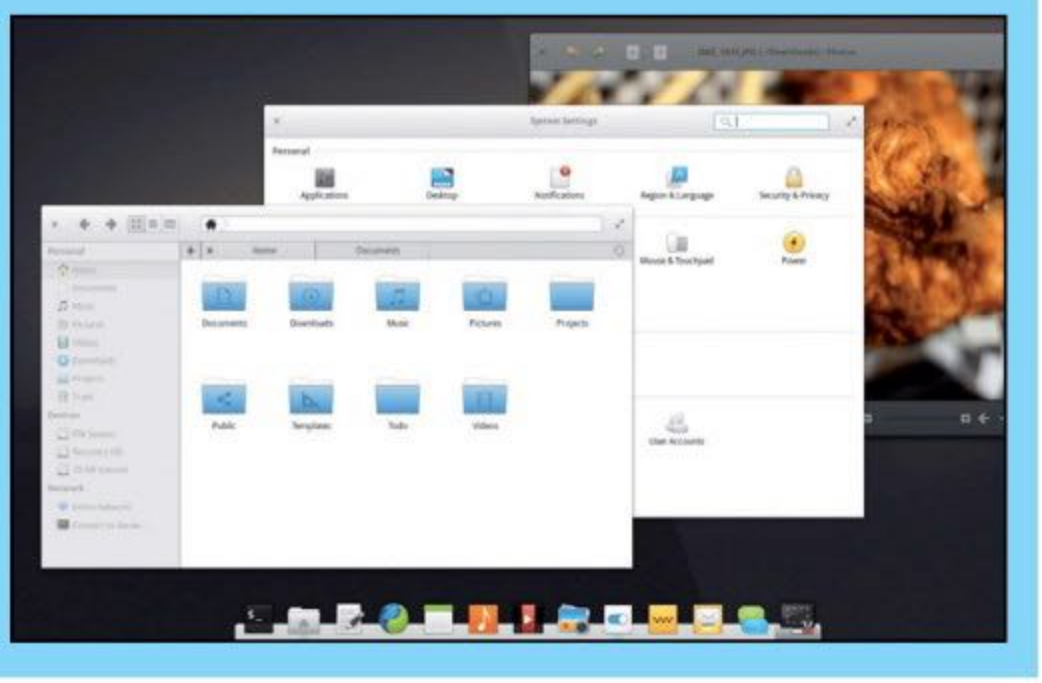


Elementary OS

→ Système « cloisonné »

Basé sur Ubuntu, Elementary OS reprend des codes graphiques propres à Apple et ses Mac, notamment la fameuse barre d'icônes en bas de l'écran. Il se veut épuré et léger, tout en profitant des applications de la logithèque d'Ubuntu. Tout le nécessaire est installé par défaut : navigateur Internet, suite bureautique, agenda, lecteur multimédia, client mail, gestionnaire d'images... Elementary OS est une bonne introduction aux OS alternatifs.

Difficulté : ☠☠☠ Lien : **elementaryos-fr.org**



Linux Mint

→ Windows-like

Probablement l'une des distributions Linux les plus connues, Linux Mint cherche à se rapprocher d'un environnement Windows familier, pour ne pas trop dérouter celles et ceux qui ont franchi le pas de l'OS alternatif. Comme la plupart de ses collègues, l'OS est accompagné de logiciels libres et open source pour être utilisable sitôt arrivé sur le bureau. Avec Elementary OS, c'est un système de choix pour tester une alternative «grand public» à Windows et MacOS.

Difficulté : ☠☠☠

Lien : **linuxmint.com**

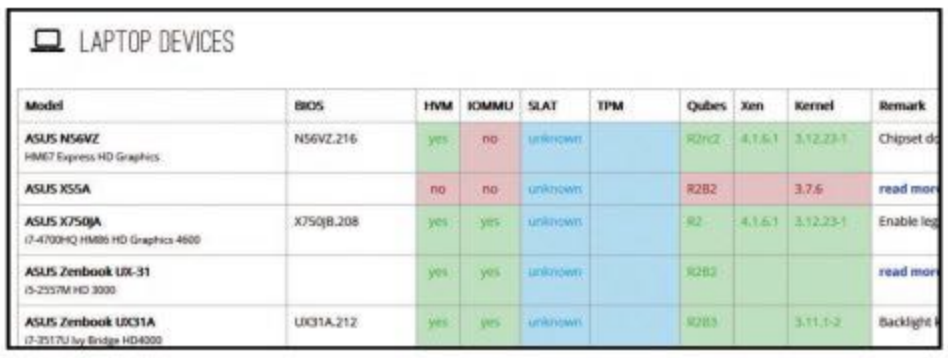
Premiers pas avec Qubes OS

INFOS [QUBES]
Où le trouver ? [**qubes-os.org**] Difficulté : ☠☠☠

TUTO

01› LA CONFIGURATION REQUISE

Qubes OS n'est pas le système d'exploitation alternatif le plus léger ou le moins gourmand. Pour en profiter, oubliez les vieilles machines : processeur 64 bits, 4 Go (au moins) de mémoire RAM et 32 Go d'espace de stockage libre sont nécessaires. La liste des matériels compatibles est disponible sur **qubes-os.org/hcl**.

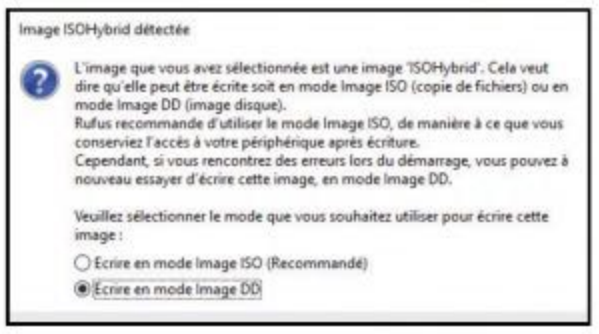


02› LES FICHIERS NÉCESSAIRES

Téléchargez l'image de Qubes OS au format ISO (4 Go) et vérifiez son intégrité avec sa signature PGP. Pour l'installation depuis une clé USB, 32 Go sont nécessaires. Téléchargez aussi le logiciel **Rufus**. Pour l'image DVD, allez sur **ftp.qubes-os.org/iso** et gravez l'image sur la galette. Attention, dans la liste vous trouverez aussi des versions Live CD. Choisissez-en une faisant moins de 4,2 Go ou vous serez obligé de passer par un DVD double densité. Lancez Rufus et choisissez l'option **Image DD** dans **Créer un disque de démarrage**.

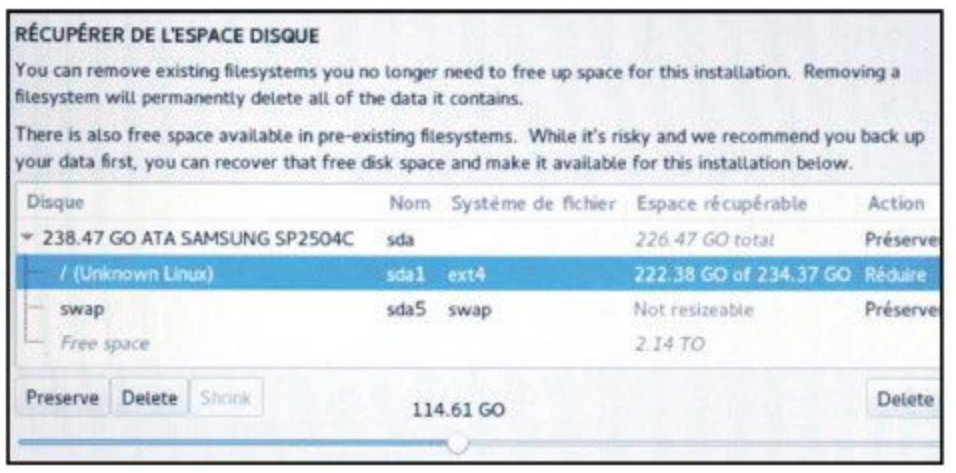
03› AVEC WINDOWS OU LINUX

Retrouvez l'ISO dans l'arborescence en choisissant **Tous les fichiers** dans la fenêtre **Ouvrir**. Rufus demande si vous souhaitez faire une Image DD. Faites **OK** puis **Démarrer**. Les fichiers nécessaires iront dans la clé USB. QubesOS n'est pas compatible avec les BIOS UEFI. Sous Linux, il faudra faire **dd if=Qubes-R3-x86_64.iso of=/dev/sdX** (en prenant soin de changer le nom de l'ISO si celui-ci a changé, de même que la partition, **sda1** par exemple).



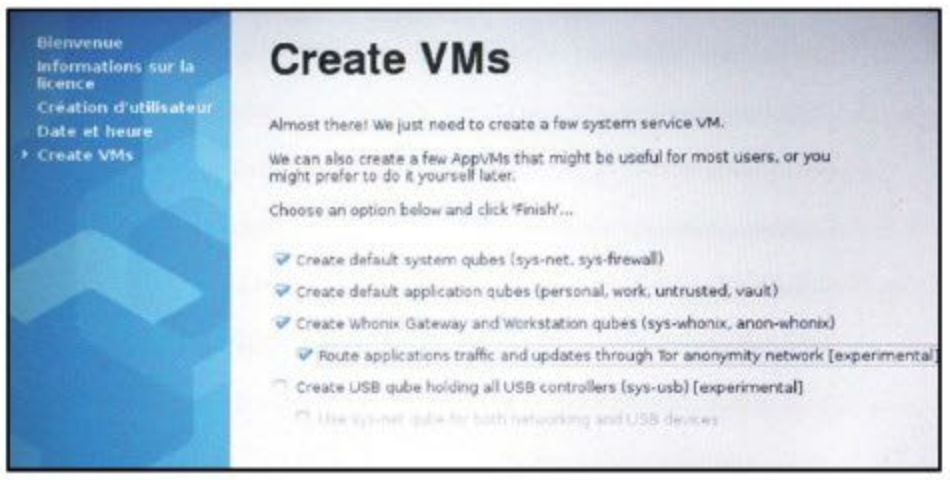
04› LE MULTIBOOT

Bootez sur la clé USB ou le lecteur optique depuis le BIOS. Vous pouvez opter pour le multiboot au démarrage, mais sachez que cela est peu sécurisé. En effet, un malware pourra accéder à **/boot**, ce qui pourrait contaminer Qubes OS depuis le Windows ou le Linux déjà présent. Il est donc préférable d'installer uniquement Qubes OS sur un PC si vous souhaitez l'utiliser de manière régulière. Pour un simple test, voici comment activer le multiboot : **qubes-os.org/doc/multiboot**.



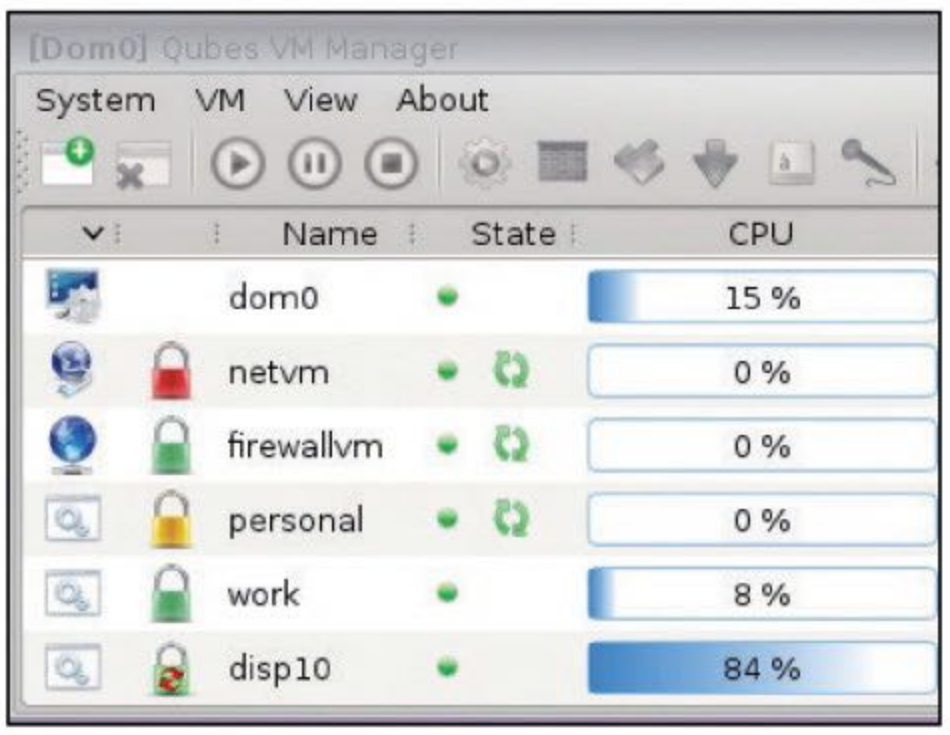
05› OPTIONS D'INSTALLATION

À l'installation, choisissez la langue et le mot de passe pour le chiffrement du disque. Vous avez aussi accès à un module permettant de créer une partition dans **Installation destination**. Vous pouvez en effet choisir de **Récupérer de l'espace** sur un disque (32 Go seront nécessaires). Après avoir entré à nouveau votre mot de passe, sélectionnez les options de départ. Cochez les 4 premières cases pour activer le support de Tor dans le même temps.



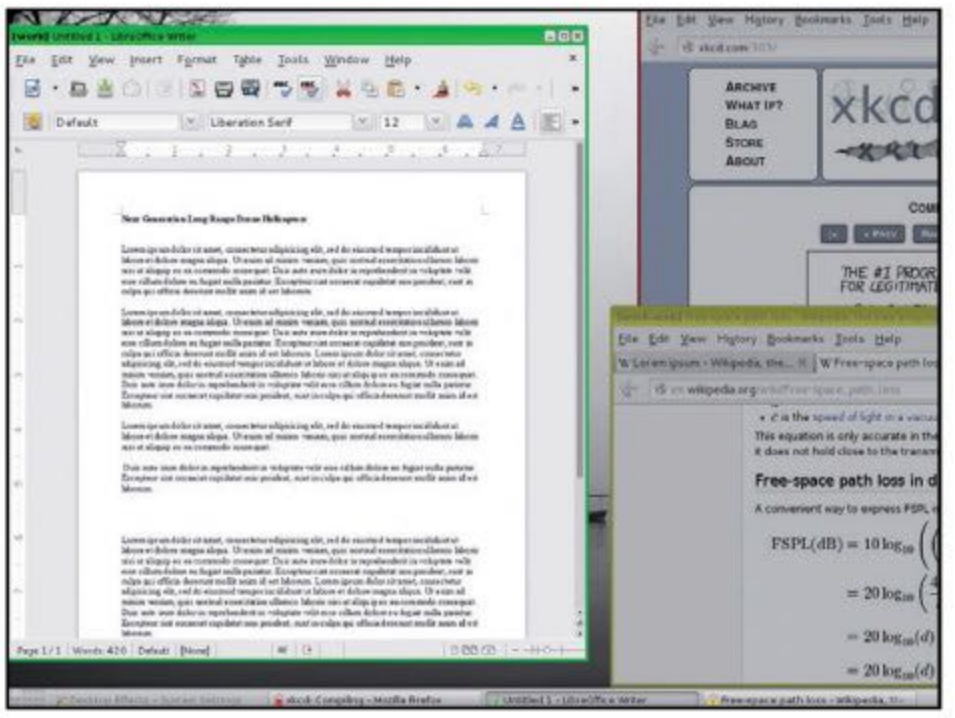
06› VOTRE BUREAU

Une fois les fichiers copiés, authentifiez-vous et découvrez le bureau. La seule fenêtre affichée concerne les qubes présents au démarrage : **dom0** (le domaine initial, père de tous les autres) ainsi que **sys-net** (gestion du réseau) et **sys-firewall** (le pare-feu). Le bureau est très sobre, juste quelques options dans **Desktop** en haut à droite et une barre des tâches en bas. Si le Wi-Fi n'est pas pris en compte, branchez le PC avec un câble Ethernet.



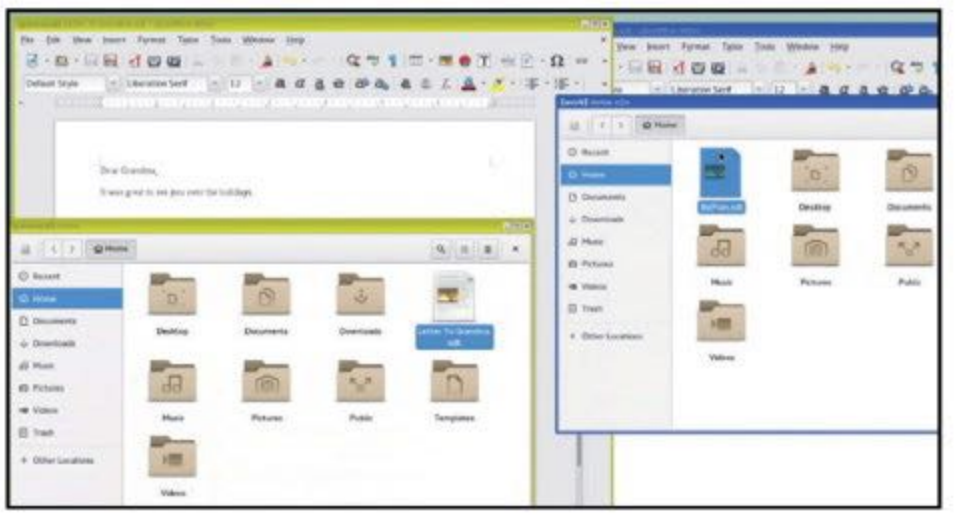
07› VOTRE PREMIER «QUBE»

Depuis le bouton en forme de logo Qubes en bas à gauche, accédez aux différents «domaines» : **vault, personal, work** et **untrusted**, correspondant à quatre niveaux de sécurité. Commençons par ouvrir un navigateur depuis un de ces domaines ou depuis le menu **Disposable VM**, qui va ouvrir un navigateur «jetable». Dans le menu **anon-whonix**, vous avez la possibilité de faire fonctionner votre navigateur avec Tor.



08› POUR LES FICHIERS AUSSI...

Dans chaque domaine, il est possible d'ajouter des raccourcis (**Add more shortcuts**...). Pour les fichiers, c'est la même chose : vous pouvez très bien sauvegarder un document dans un domaine sans que les autres ne le «voient» dans leur propre arborescence. Idéal pour de pas mélanger vos activités personnelles avec vos activités professionnelles. Ce sont de nouvelles habitudes à prendre, mais au final vous serez gagnant.

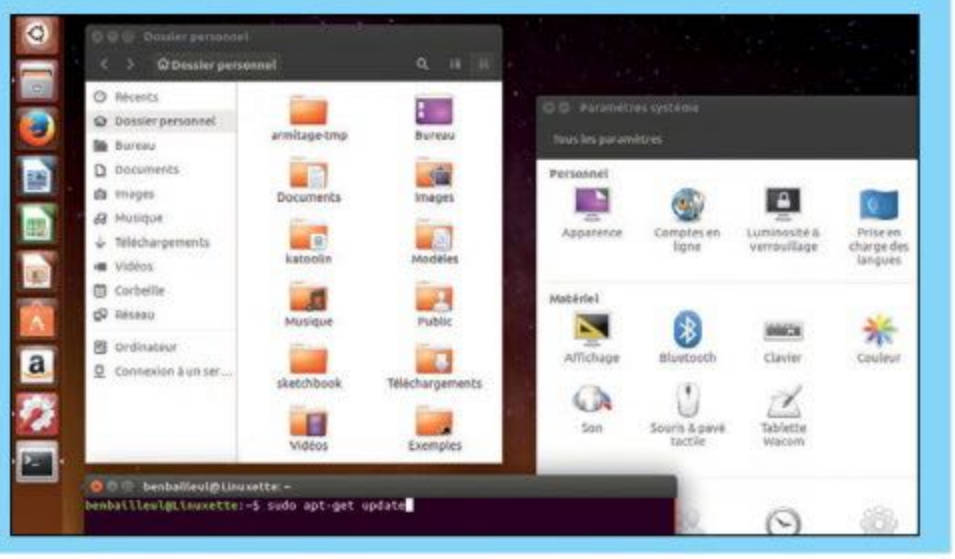


OS ALTERNATIFS

Ubuntu
→ Une référence

Célèbre distribution GNU/Linux basé sur Debian, Unbuntu est l'un des premiers OS alternatif auquel on pense lorsque l'on aborde le sujet. Décliné à toutes les sauces, ce système d'exploitation existe forcément dans une version qui répondra à vos envies, généralistes ou spécialisées : paramétrage poussé du bureau, environnement ressemblant à Windows, centre multimédia, création multimédia, etc. Comme souvent avec les OS libres, vous avez la possibilité d'ouvrir une session live, c'est à dire d'essayer Ubuntu sans devoir l'installer.

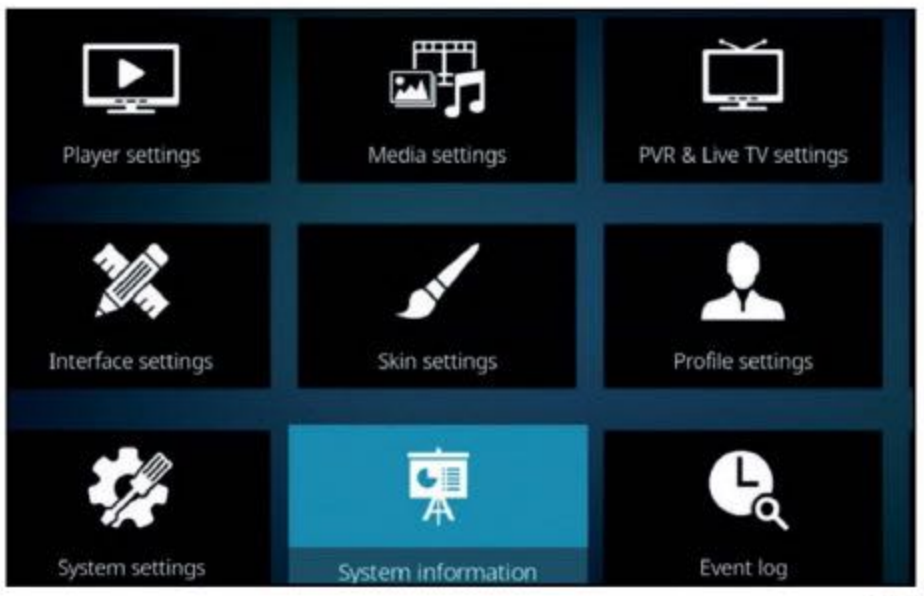
Difficulté : ☠☠☠ Lien : **ubuntu-fr.org**



OpenELEC → Mediacenter

Système d'exploitation très spécialisé s'il en est puisqu'OpenELEC est un mediacenter, du même genre que Kodi. Autrement dit, un gestionnaire de photos, films, séries TV et autres musiques présentes sur la machine, le but étant de naviguer à travers vos collections dans une interface graphique pratique et agréable à parcourir. L'avantage d'OpenELEC, c'est qu'il peut s'installer sur à peu près n'importe quoi, ce qui le rend parfait pour recycler un vieux PC inutilisé, voire un Raspberry Pi pour un mediacenter compact.

Difficulté : ☠☠☠
Lien : **openelec.tv**



Mageia → Léger

L'intérêt premier de Mageia, c'est de pouvoir tourner sur à peu près n'importe quelle machine, même si elle est équipée des premiers processeurs Pentium ! Côté mémoire vive, 512 Mo sont suffisants (2 Go pour être tranquille). L'installation minimale prend 5 Go sur l'espace de stockage, 20 Go pour la complète. Communautaire, Mageia se renouvelle environ tous les ans avec une nouvelle version. Notez qu'un assistant vous fera le tour du propriétaire sitôt arrivé sur le nouveau bureau. Pratique.

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

Difficulté : ☠☠☠ Lien : **mageia.org**

Installation de Mageia

INFOS [MAGEIA]
Où le trouver ? [**mageia.org**] Difficulté :

TUTO

01› LA BONNE VERSION

Allez dans la section des téléchargements du site et téléchargez la version de Mageia qui vous convient. Si votre processeur est compatible 64 bits, optez pour cette version, mais dans le doute, prenez la version 32 bits. L'image ISO de 3,5Go devra être gravée (en tant qu'image de disque) sur un DVD depuis votre logiciel de gravure. Vous n'avez pas de lecteur de disque ? Pas de problème ! Il est possible d'installer depuis une clé USB. Suivez ce tutoriel : **http://goo.gl/xrBESj**. Vous pouvez aussi essayer avec le logiciel XBoot.

02› BOOTER DEPUIS LE DISQUE

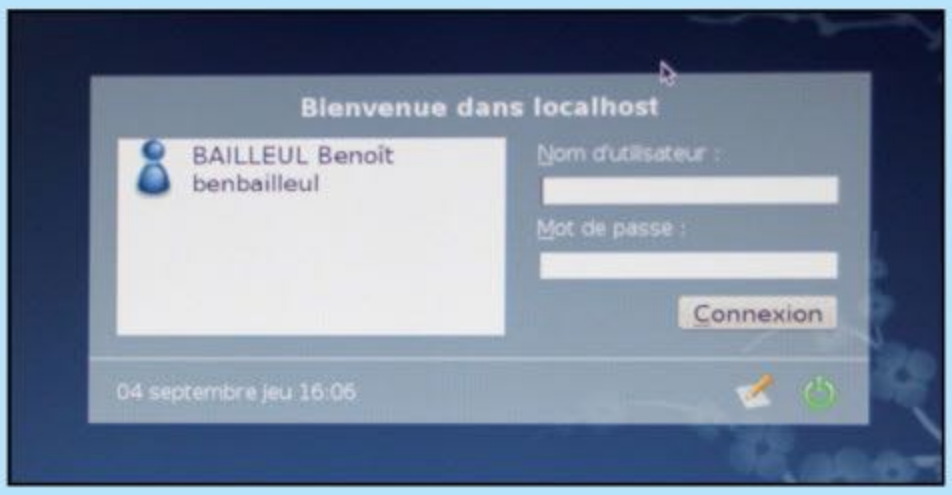
Une fois que votre DVD est prêt, il faudra juste penser à booter sur votre lecteur de disque. Faites **Suppr, F1, F2** ou **F12** (en fonction de votre modèle de carte mère) juste après avoir allumé le PC et entrez dans le BIOS (**Setup**). Trouvez l'option **Boot Sequence** (qui peut aussi être sélectionnable avant même l'entrée dans les menus) et modifiez l'ordre en mettant en premier le lecteur de CD/DVD. Redémarrez le PC pour arriver à l'assistant d'installation de Mageia.

03› L'INSTALLATION

Faites **Install Mageia4**, choisissez le français comme langue de base et sélectionnez l'option **Enlever Microsoft Windows** si votre disque dur contient encore une partition de ce type. Bien sûr, ce n'est pas obligé, vous pouvez très bien créer une autre partition. Sélectionnez ensuite votre type de bureau (KDE est plus «Windows» dans son organisation donc nous avons choisi celui-là) et laissez le système s'installer !

04› LES PREMIERS RÉGLAGES

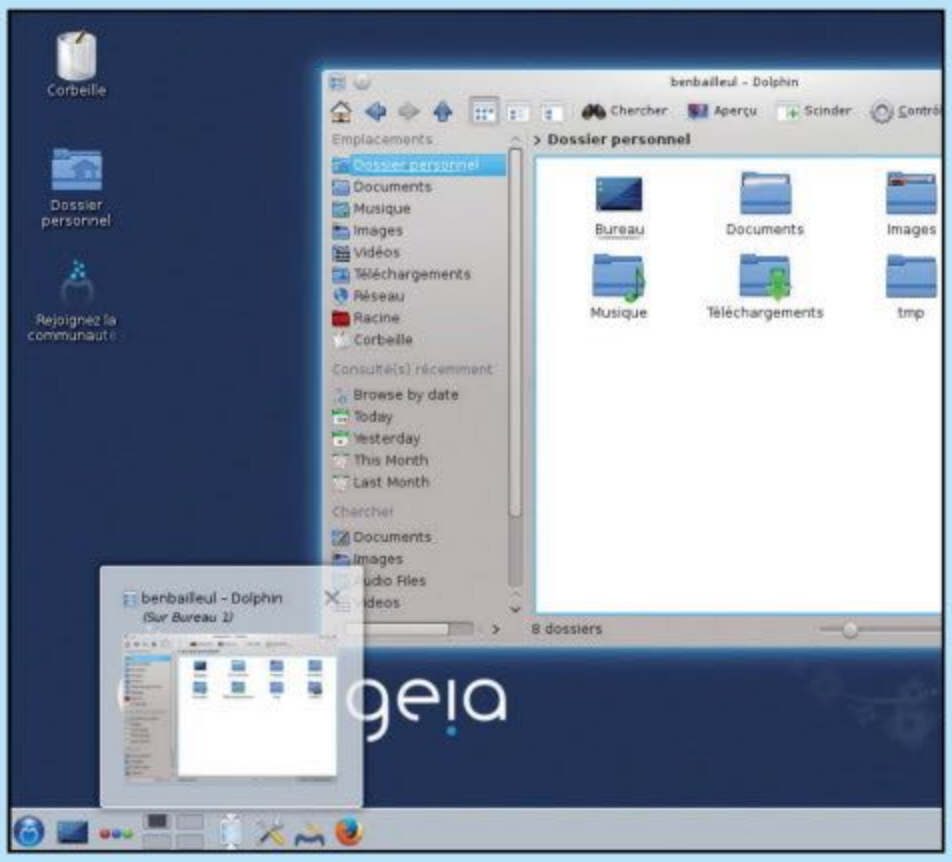
Une petite heure après, il faudra remplir vos informations personnelles (rappelez-vous bien de vos mots de passe **root** et utilisateur). À la fin, Mageia vous dressera un résumé des périphériques qui ont été pris en compte et vous proposera une mise à jour. Validez, retirez le DVD du lecteur



lorsqu'il s'éjectera automatiquement et redémarrer le PC. Entrez votre mot de passe utilisateur et... vous voici sous Linux ! Bravo.

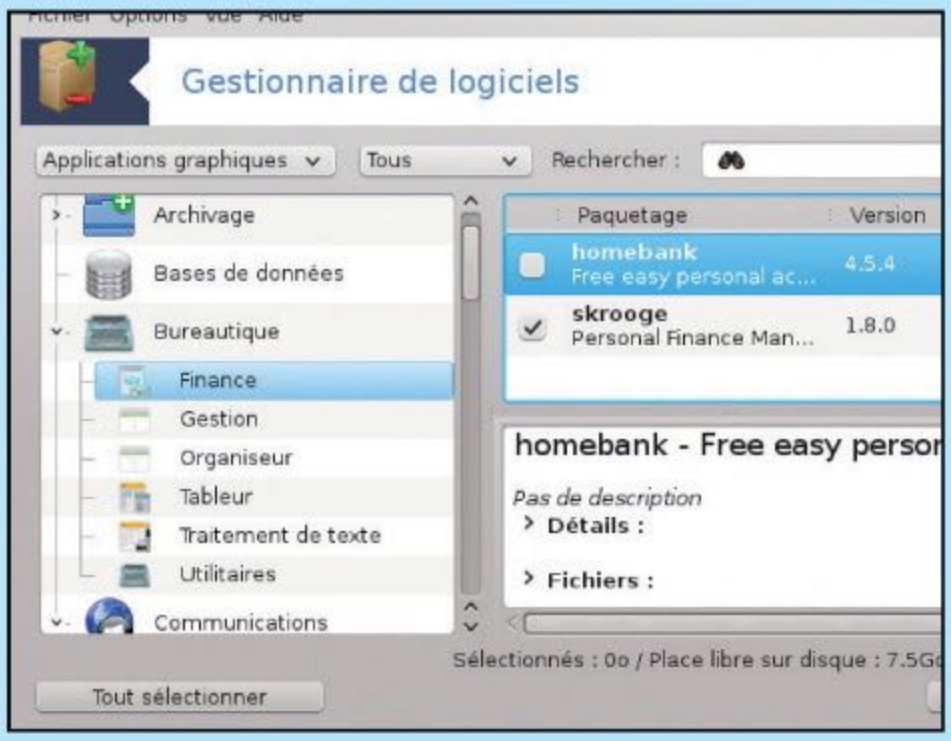
05 › L'ASSISTANT ET LES PREMIERS PAS

Dès le début, un assistant vous présentera le projet Mageia et le système, mais vous pouvez tout de suite commencer l'aventure. En bas à droite, vous verrez l'icône de **Dolphin** le gestionnaire de fichiers. C'est ici que vous retrouverez vos documents, le contenu de votre disque dur, clé USB, etc. À l'extrême gauche, le bouton **Démarrer** vous dirigera vers les programmes préinstallés. Ils sont classés par type. Retrouvez LibreOffice, Firefox, GIMP et plein d'autres inconnus. Essayez-les !



06 › AJOUTER DES PROGRAMMES

Si vous voulez tout de même installer d'autres logiciels, allez dans le gestionnaire de logiciel, toujours en bas à gauche. Entrez votre mot de passe root et faites votre marché. Si le logiciel que vous convoitez n'est pas dans la liste, il faudra aller le chercher sur le site de l'éditeur. Pour avoir accès à une sorte de **Panneau de Configuration**, c'est encore en bas à gauche que ça se passe dans **Configurer votre PC**.

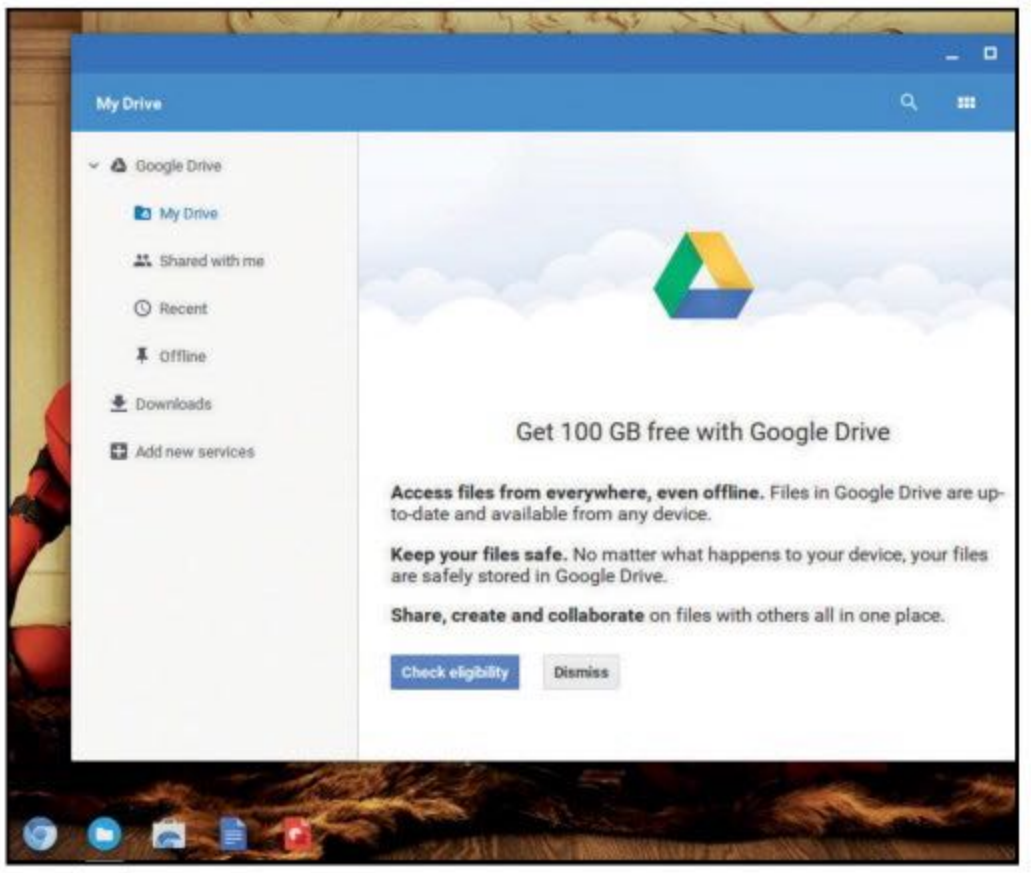


CloudReady OS → ChromeOS libre

Vous connaissez les ChromeBooks ? Ces ordinateurs portables tournant sous ChromeOS, le système d'exploitation made in Google où tout se passe dans le Cloud ? CloudReady OS en est une version libre, basé sur Chromium OS. Finie la limitation aux seules machines crées pour l'occasion, CloudReady OS tourne sur PC et Mac. Là aussi, l'intégralité des fonctions est accessible du moment que l'ordinateur est connecté au Web. On apprécie aussi les mises à jour automatiques régulières et automatiques.

Difficulté : ☠☠☠

Lien : **neverware.com**



Kali Linux → Pentesting

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

Anciennement nommée BackTrack, Kali Linux est une distribution spécialisée dans l'audit réseau, le pentesting et plus généralement le hacking. Parmi les outils inclus, vous trouverez des logiciels pour cracker des mots de passe, des logiciels de rétro-engineering, des modules pour pénétrer des réseaux sans fil, mais aussi le langage Arduino ou CHIRP (radio amateur). Une vraie mine d'or pour les hackers débutants ou confirmé(e)s. La plupart des logiciels dont nous vous parlions dans la partie sur le crack de mot de passe sont présents dans Kali...

Difficulté : ☠☠☠ Lien : **kali.org**

Les outils de Kali Linux

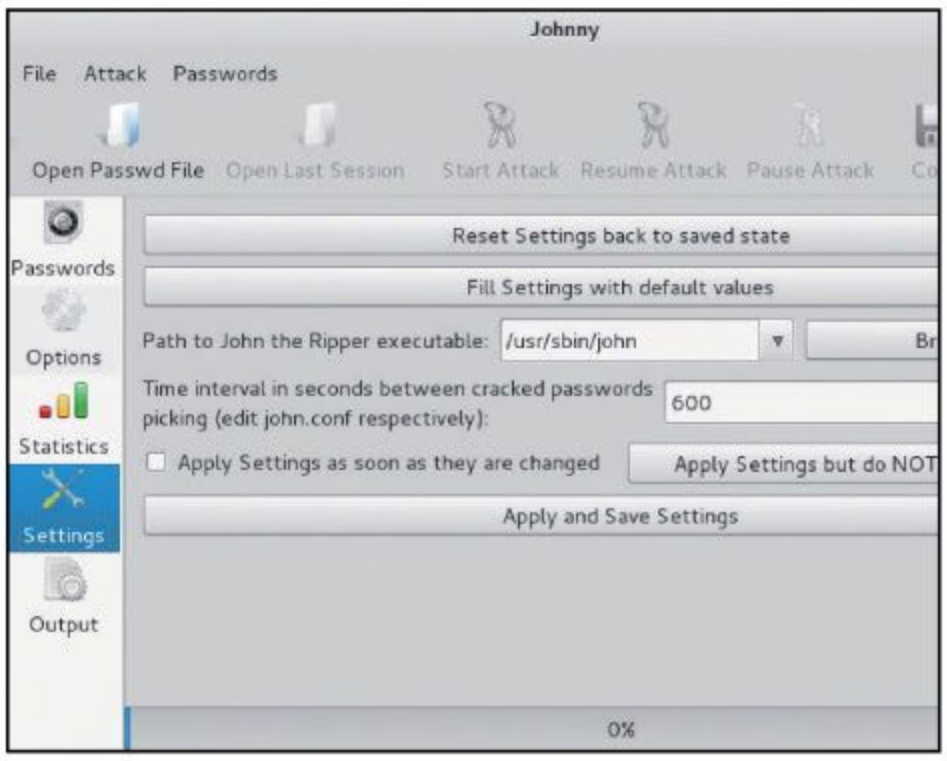
Nous avons déjà parlé de certains outils de Kali Linux dans les pages précédentes, mais voici une rapide présentation d'autres logiciels indispensables de cette distribution.

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

TUTO

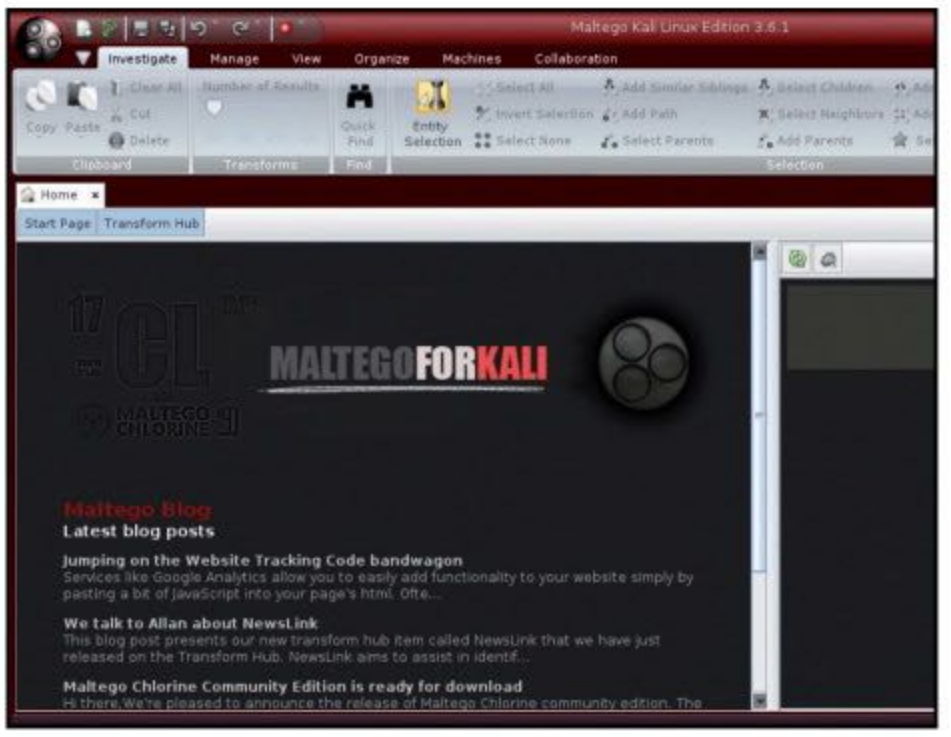
01› JOHNNY

John the Ripper est un logiciel de cassage de mot de passe : un «crack» du crack (voir précédemment). Il dispose de plusieurs cordes à son arc : permutation de caractères, brute force, attaque par dictionnaire, etc.
Le logiciel est en ligne de commande, mais pour ceux qui sont allergiques, Johnny est l'interface graphique qui se greffe dessus.



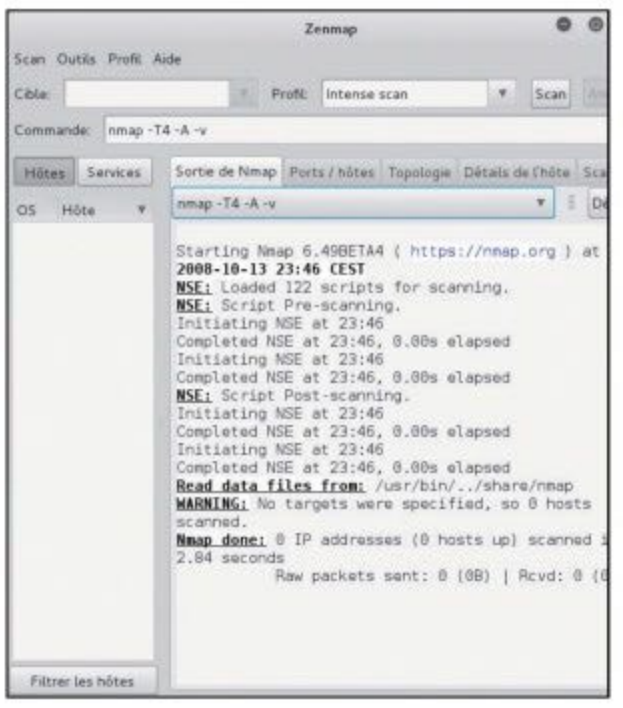
02› MALTEGO

Conçu pour recouper des informations numériques venues des 4 coins du Web, Maltego est une plate-forme open source de renseignements. Le programme va piocher des informations à la demande dans ses serveurs et va les afficher sous forme de diagramme. Tout est passé en revue : Facebook, LinkedIn, Twitter, adresse e-mail, numéro de téléphone, données de géolocalisation, etc. Diablement efficace pour trouver des informations personnelles sur des individus, des sites ou des sociétés, Maltego pourra vous aider pour une embauche par exemple ou pour du social engineering.



03› MAP ET ZENMAP

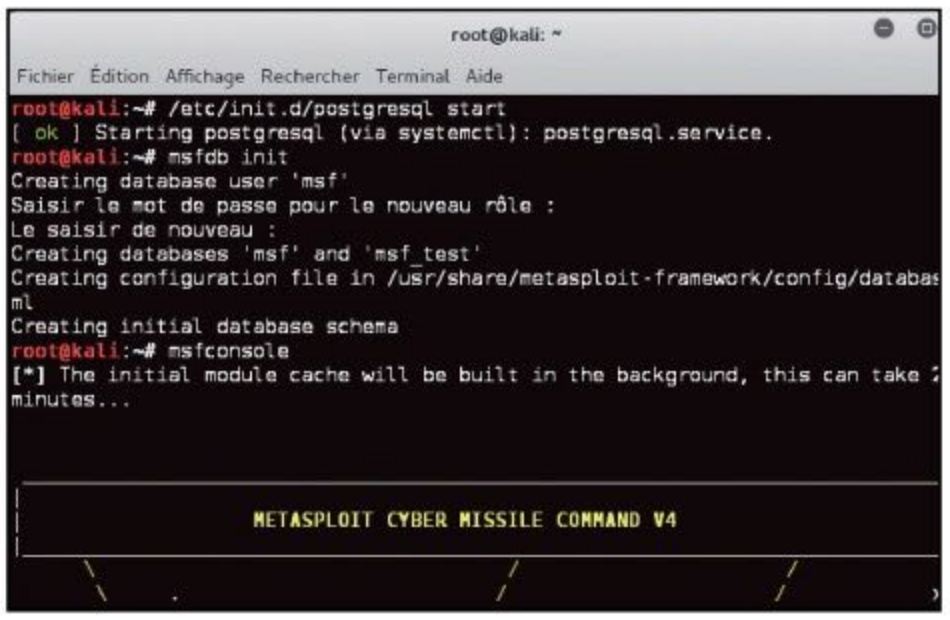
ZenMap est l'interface graphique de Nmap, un logiciel permettant de mapper un réseau : scan des ports, noms des services utilisés par ces derniers, détection des versions des logiciels et systèmes, tests



de vulnérabilité, exploitation des faiblesses, etc. Même les systèmes derrière des pare-feu ou des filtres à IP ne sont pas à l'abri. Un logiciel à ne pas mettre entre toutes les mains.

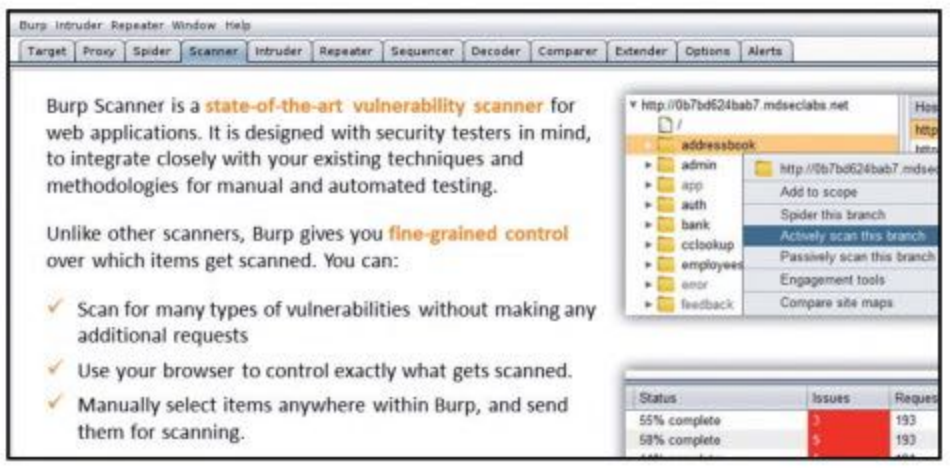
04 › METASPLOIT ET ARMITAGE

Armitage est l'interface graphique pour Metasploit. Ce dernier est une plate-forme fournissant des renseignements sur les vulnérabilités des systèmes informatiques : les fameux «exploits». Ce type d'informations peuvent être utilisées par les administrateurs pour tester la vulnérabilité de leurs systèmes afin de les rendre «étanches». Au programme : sniffing, backdooring, keylogging et des centaines d'autres fonctions impossibles à lister ici.



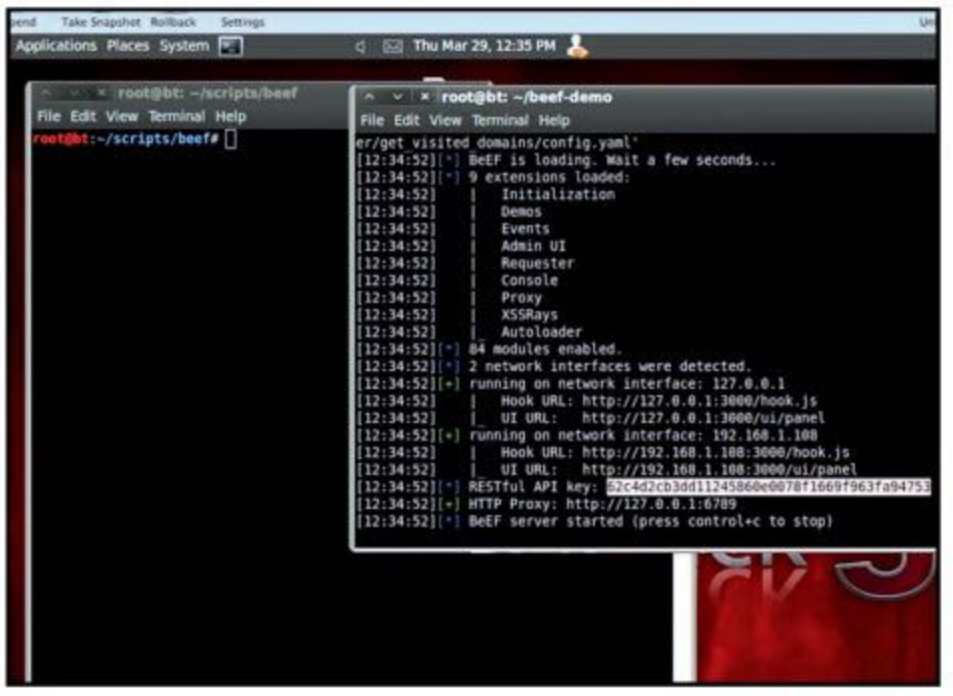
05 › BURP SUITE ET WIRESHARK

Ces deux-là n'ont rien à voir ensemble, mais nous nous devions d'en parler. Burp Suite est une solution de pentesting pour les applications Web : attaque Man-in-the-middle depuis un proxy, Web crawler, etc. Wireshark analyse les protocoles et inspecte les paquets de données qui transitent (avec capture à la volée et analyse hors ligne).



06 › BEEF

BeEF est spécialisé dans les failles cross-site scripting (XSS). Il s'agit, ici, de polluer un site avec des bouts de code malicieux pour que le navigateur de l'utilisateur interprète ce code et contamine le système. Comme tous les outils présentés ici, il s'agit de tester vos propres réseaux et sites pour repérer des failles de sécurité, pas de jouer aux pirates. Heureusement qu'on vous fait confiance !



OS ALTERNATIFS

Kodachi → Discrétion absolue

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

Basé sur la distribution Debian, Kodachi tire son nom d'un type de sabre japonais. C'est un système misant sur l'anonymat, la sécurité et la mobilité. Disponible uniquement en mode Live CD (sur DVD ou clé USB), cet OS comprend quantité d'outils pour masquer son identité et son emplacement : Tor, chiffrement, VPN, etc. Attention, Kodachi ne s'adresse pas forcément aux experts d'autant qu'on vous explique le fonctionnement un peu plus loin...

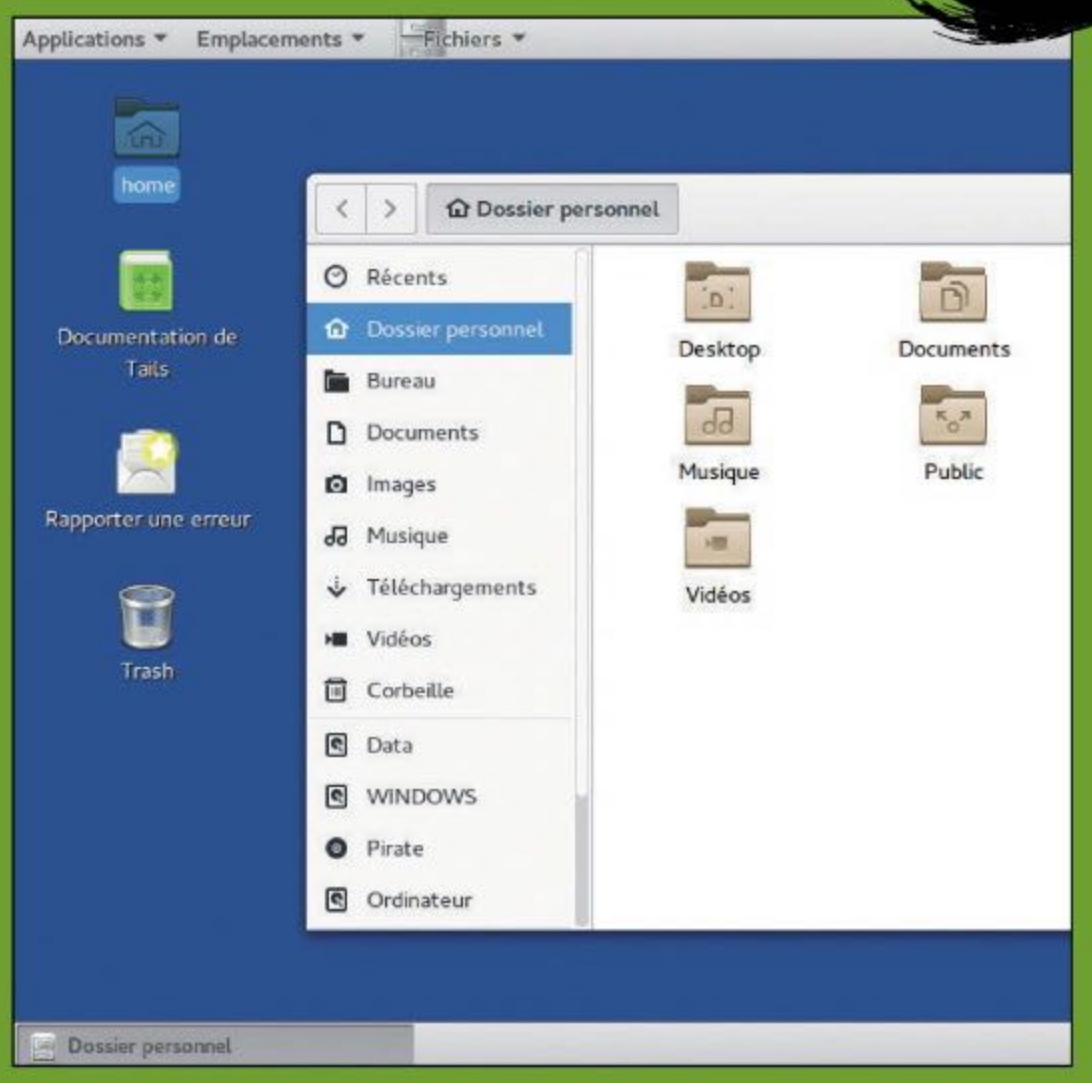
Difficulté : ☠☠☠

Lien : **www.digi77.com/linux-kodachi**

Tails → La bête noire du renseignement

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

Tails (The Amnesic Incognito Live System) est la réponse ultime aux Internautes exigeant un anonymat sans faille. Basé à la fois sur la distribution Linux Debian (comme Kali Linux) et sur Tor au niveau des communications, cet OS pensé comme un Live CD est un système autonome. En plus d'une connexion obligatoire par Tor, Tails contient tout ce qu'il faut pour chiffrer vos e-mails, effacer vos traces, etc. La mise en place est un peu plus compliquée que pour les autres Live CD : il vous faudra posséder deux clés USB de 4 Go et créer un espace de stockage chiffré, mais rien d'insurmontable non plus. Quand vous débranchez la clé, toutes vos traces s'effacent...



Difficulté : ☠☠☠ Lien : **tails.boum.org**

Présentation de Kodachi

INFOS **[KODACHI]**
Où le trouver ? [**www.digi77.com/linux-kodachi**] Difficulté : ☠☠☠

TUTO

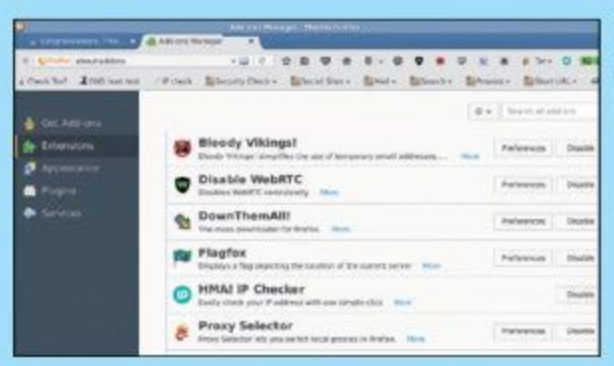
01› LE BOOT

Comme pour tous les systèmes de type Live CD qui se chargent dans la RAM, il faudra juste graver l'ISO sur un DVD (ou placer le fichier sur une clé USB avec Rufus par exemple) et faire booter le PC sur le bon périphérique. On peut aussi envisager l'utilisation d'une machine virtuelle avec VMware. Dans le menu de boot, choisissez le mode **Live** et attendez que le bureau s'affiche.

02› PREMIERS CONTACTS

Allez dans la barre d'outils en haut pour ajouter le français comme langue par défaut (clic droit dans **US** puis **Preferences** et onglet **Input Method**). Ajoutez aussi votre réseau local dans l'assistant de connexion juste à côté. Dès qu'il sera authentifié, Kodachi va commencer à activer le VPN, le chiffrement de DNS et la connexion à Tor.

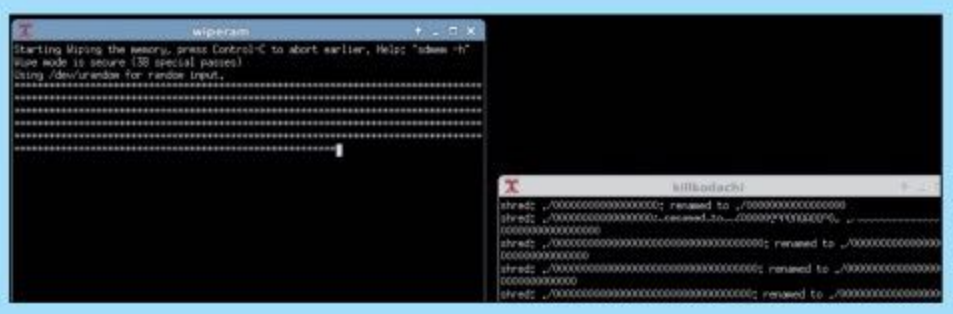
03› LA CONNEXION AVEC TOR



Normalement, vous n'avez rien à faire pour être anonyme avec Kodachi, mais nous allons nous en assurer. La distribution embarque le Tor Browser et un autre navigateur (Kodachi Browser) qui utilise aussi Tor pour se connecter. Cliquez sur le premier pour mettre à jour Tor et, une fois terminé, faites un tour dans le second. Vous devriez voir votre IP d'emprunt avec un message de confirmation. L'avantage du navigateur de Kodachi c'est le nombre de plugins préinstallés pour brouiller les pistes : adresse e-mail temporaire, agent de connexion permettant de masquer votre configuration, antipub, anti-tracker, proxy, etc.

04› EFFACER VOS TRACES

Avec Tails (voir page suivante), il suffit de retirer la clé USB du PC pour effacer la RAM et le contenu du bureau. Dans Kodachi, il faut aller dans la partie **Panic Room** où vous pourrez faire **Wipe the RAM** ou **Wipe RAM then Shutdown**. Le processus est plus long que dans Tails. Si vous utilisez Kodachi depuis longtemps et que vous voulez absolument tout effacer sans laisser de trace, faites **Destroy Kodachi**. Vous perdrez absolument toutes les données !



Mise en place et fonctionnalités de Tails

INFOS [TAILS]
Où le trouver ? [**tails.boum.org**] Difficulté : ☠☠☠

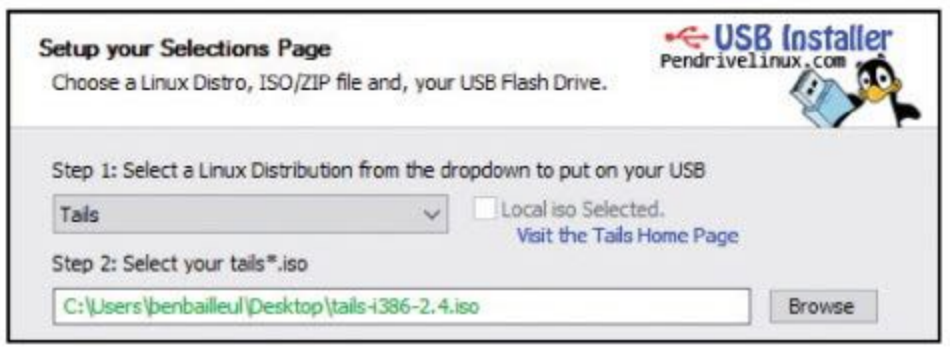
TUTO

01› L'IMAGE DE TAILS

Sur la page principale, cliquez sur **Installer Tails** puis **En route** et enfin choisissez votre système. Nous avons choisi de l'installer sous Windows, mais le principe est le même pour Linux ou Mac OS. Si vous ne connaissez personne disposant de Tails, faites **Installer depuis Windows**. Notez que vous pouvez aussi graver Tails sur un DVD. Si vous disposez de Firefox, vous aurez à disposition une extension pour télécharger et vérifier l'intégrité de l'ISO. Dans le cas contraire, utilisez BitTorrent et OpenPGP comme expliqué.

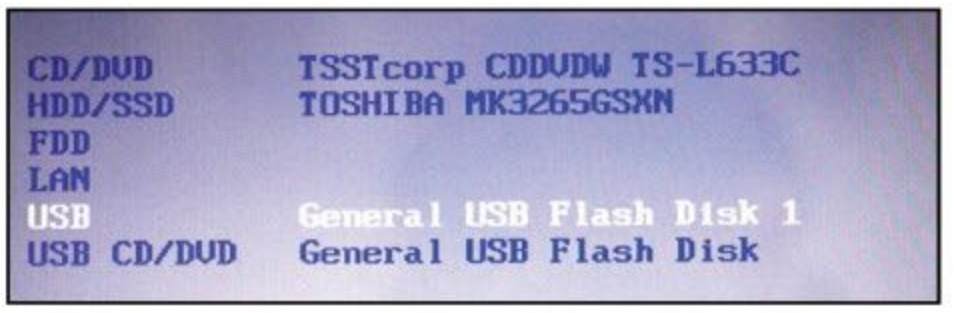
02› TAILS SUR LA PREMIÈRE CLÉ

Après avoir récupéré l'image de Tails, suivez le lien pour télécharger Universal USB Installer. Trouvez **Tails** dans la liste (tapez **T** sur le clavier après avoir ouvert le menu déroulant), trouvez votre fichier ISO puis la lettre de la clé USB qui va vous servir pour le Tails intermédiaire. N'oubliez pas de cocher la case pour le formatage de la clé.



03› BOOTER

Une fois la clé prête, «bootez» dessus : faites **Suppr**, **F8** ou **F12** (en fonction de votre modèle de carte mère) juste après avoir allumé le PC et entrez dans le BIOS (Setup). Trouvez l'option **Boot Sequence** (parfois sélectionnable avant même l'entrée dans les menus) et modifiez l'ordre en mettant en premier votre clé. Si vous avez des difficultés (comme avec ces maudits BIOS UEFI !), jetez un coup d'œil sur Google avec le nom de votre matériel.



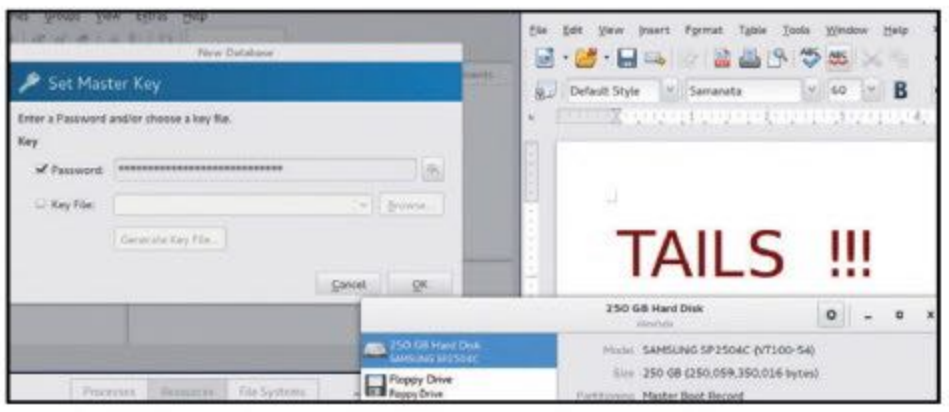
04› CLONER SUR LA DEUXIÈME CLÉ

Sur l'écran de boot de Tails, choisissez **Live** et attendez de voir l'écran d'accueil. Choisissez votre langue en bas et cliquez sur **Démarrer**. Le bureau de Tails va s'afficher, mais attention, ce n'est que le système intermédiaire : vous n'êtes pas encore en sécurité. Allez dans

Applications>Tails>Programme d'installation de Tails. Branchez votre seconde clé USB (sans retirer la première) et choisissez **Install by cloning**. Trouvez votre clé dans la liste et faites **Install Tails**.

05› LE BOOT FINAL

À la fin du processus, sortez du programme, éteignez l'ordinateur, retirez la clé USB n°1 et laissez la deuxième. Rallumez le PC en bootant encore sur la seconde clé. Comme pour le Tails intermédiaire, choisissez votre langue et faites **Démarrer**. Bravo vous êtes sous Tails ! Paramétrez Internet en haut à droite et, au bout de quelques secondes, vous devriez voir un message en bas vous avertissant que Tor est prêt.

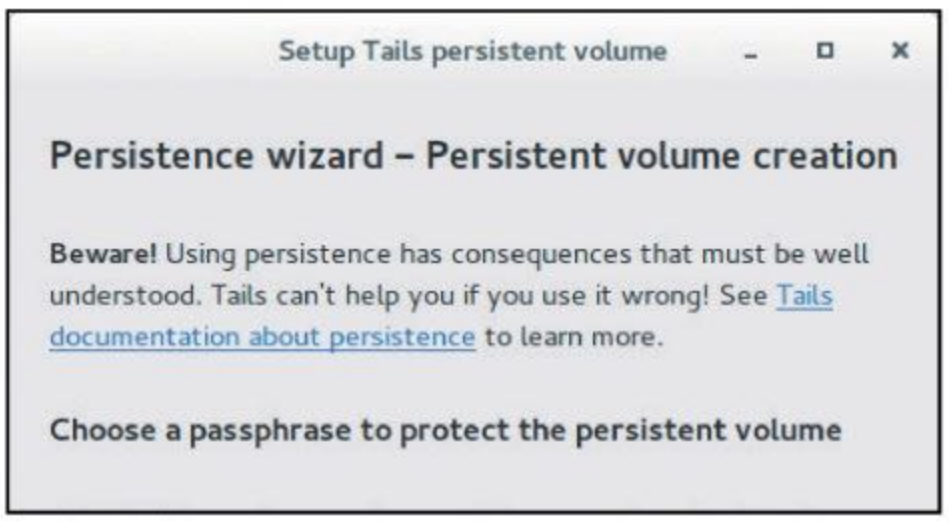


06› NAVIGUEZ PAR TOR

Dans **Application > Internet > Tor Browser**, lancez le navigateur. Sur la première page, cliquez à droite dans **Vérification de Tor** pour être sûr d'être protégé par le routage en oignon. À vous la navigation anonyme ! En cherchant un peu sur des sites spécialisés, vous pouvez aussi trouver les fameux «hidden services», des sites cachés accessibles uniquement par Tor. Attention, on y trouve autant de bons sites pour la liberté d'expression que des choses horribles.

07› LE VOLUME PERSISTANT

Il est temps de créer notre volume chiffré persistant. Cette étape n'est pas obligatoire, mais va se révéler utile si vous souhaitez garder sous le coude des documents confidentiels. Allez dans **Applications>Tails>Configurer le volume persistant** et trouvez un mot de passe suffisamment alambiqué. Faites **Create** et sélectionnez ce que vous voulez y stocker. Nous vous conseillons de choisir **Données personnelles** pour commencer, mais on peut y mettre des clés de chiffrement, vos e-mails, etc.



08› DERNIER REDÉMARRAGE

Avant d'utiliser ce volume, il faudra redémarrer Tails en utilisant votre seconde clé USB (vous n'aurez plus jamais besoin de la première). Faites activer la persistance lors de l'écran d'accueil et tapez votre mot de passe. Tous les documents sensibles qui seront stockés dans votre volume **Persistent** seront automatiquement chiffrés. Vous pouvez néanmoins chiffrer des fichiers avec le clic droit si vous préférez vous passer de ce volume spécial. **Persistent** sera disponible dans votre gestionnaire de fichiers comme un disque dur.

CHIFFREMENT

85
NOTES CHIFFRÉES

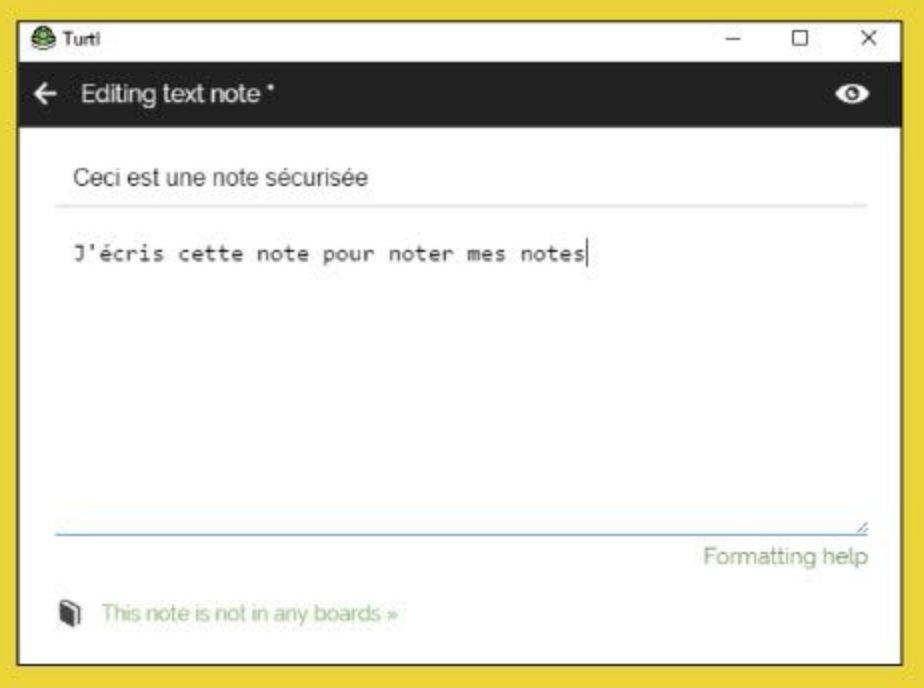
87
DONNÉES CHIFFRÉES

88
MESSAGERIES

Turtl

→ Prise de notes sécurisée

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES



De nombreux services et applications permettent de prendre des notes, stockées dans le Cloud. La particularité de Turtl, c'est que vos données sont chiffrées, donc illisibles tant pour d'éventuels pirates que pour les propriétaires du service lui-même. Ce qui n'empêche pas le partage, sécurisé évidemment. Téléchargez et installez le logiciel client sur votre PC, et l'appli pour en profiter aussi sur votre téléphone Android.

Difficulté : ☠☠☠ Lien : **https://turtlapp.com**

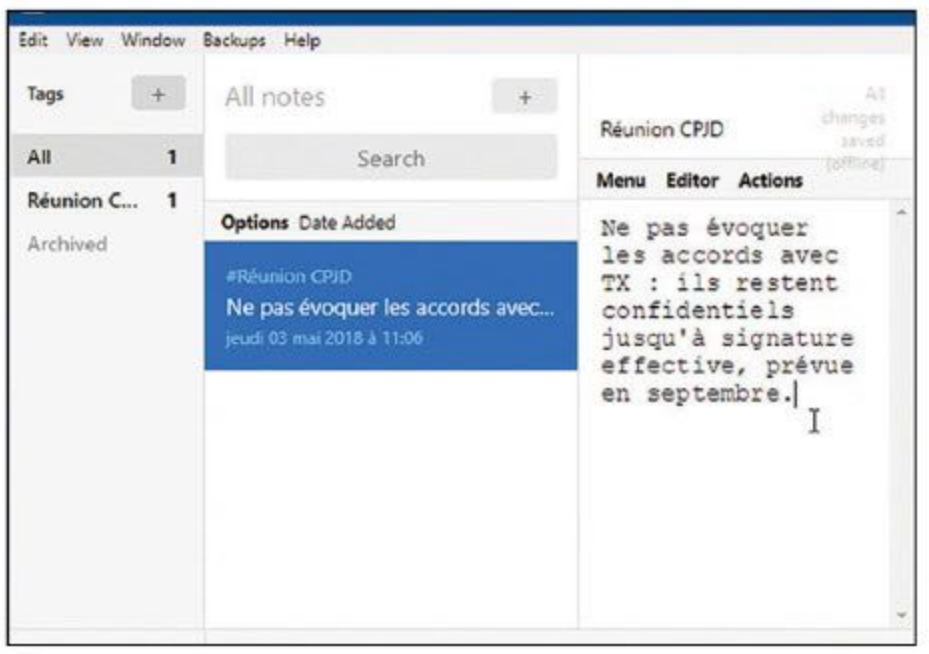
Standard Notes

→ Notes chiffrées

Une alternative à Turtl, à essayer si le concept de notes sécurisées vous séduit. Standard Notes est plus simple, même si moins complet dans sa version gratuite. Autre avantage, l'application cliente est disponible sur toutes les plates-formes, y compris iOS. Il est même possible d'exploiter le service directement via un navigateur Web, sans rien installer, depuis un ordinateur qu'on vous prête.

Difficulté : ☠☠☠

Lien : **https://standardnotes.org**

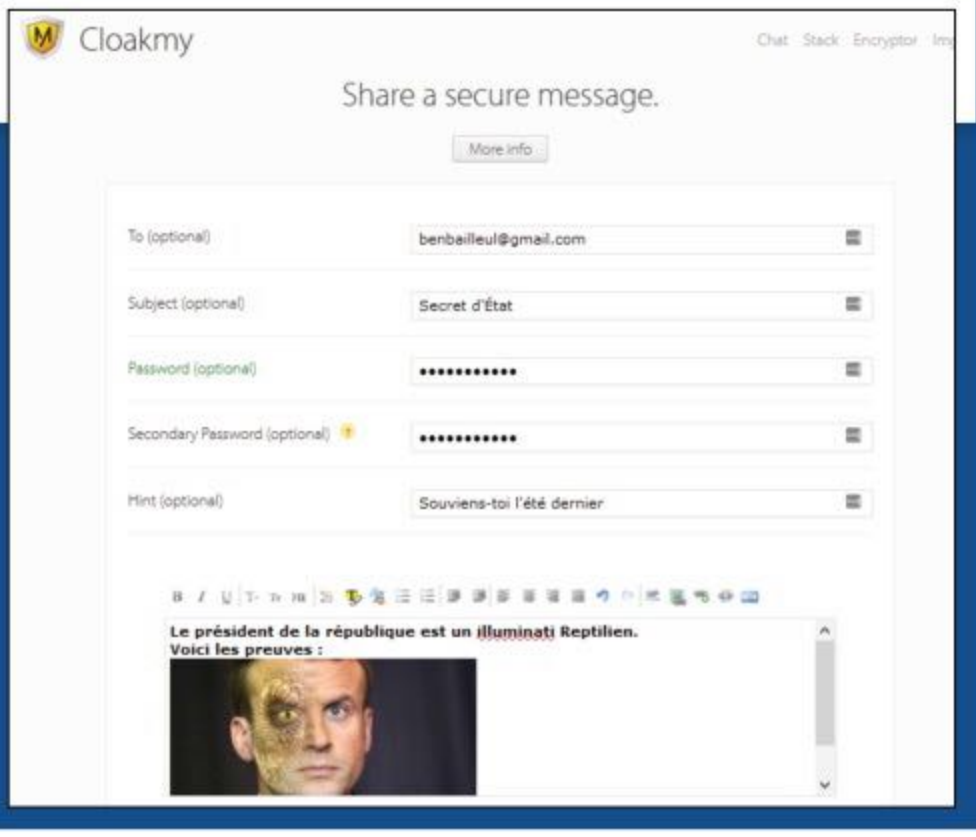


CloakMy → Partage de notes

CloakMy est une autre solution de partage de notes chiffrées accessible sans avoir à installer de logiciel. Renseignez le champs dédiés à votre correspondant, votre mot de passe (il est possible de mettre un indice pour votre ami) et c'est tout ! Vous pouvez même écrire un article complet avec images, lien, etc. À vous de paramétrer sa durée de vie.

Difficulté : ☠☠☠

Lien : **https://cloakmy.org**



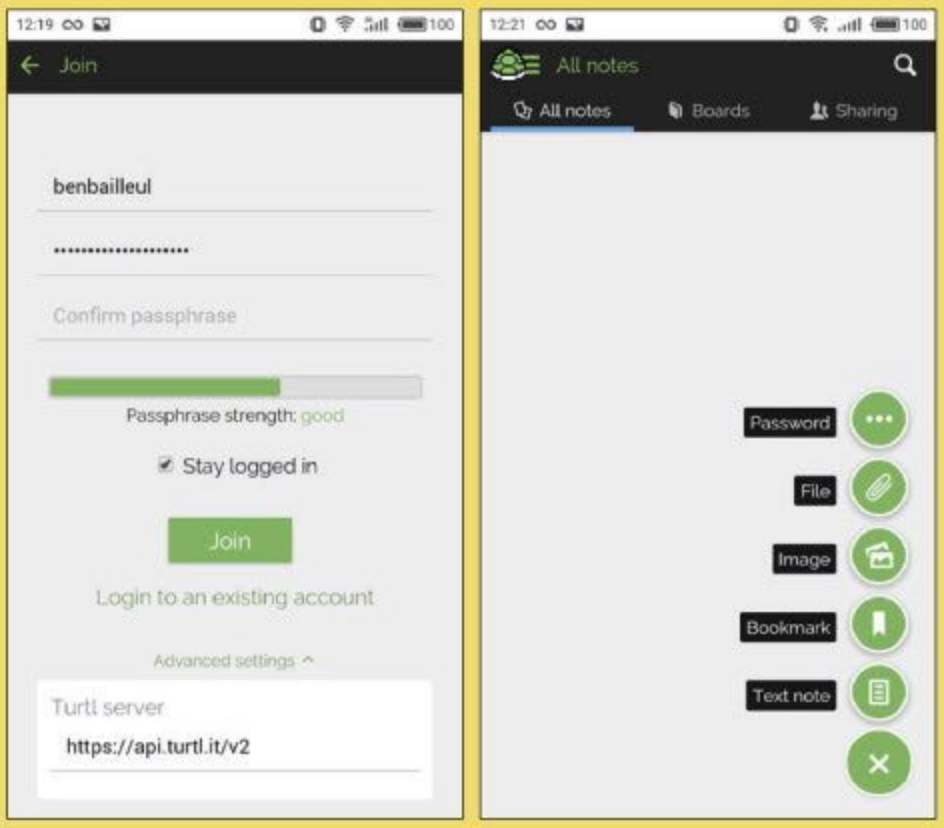
Comment fonctionne Turtl ?

INFOS [TURTL]
Où le trouver ? [**https://turtlapp.com**] Difficulté :

TUTO

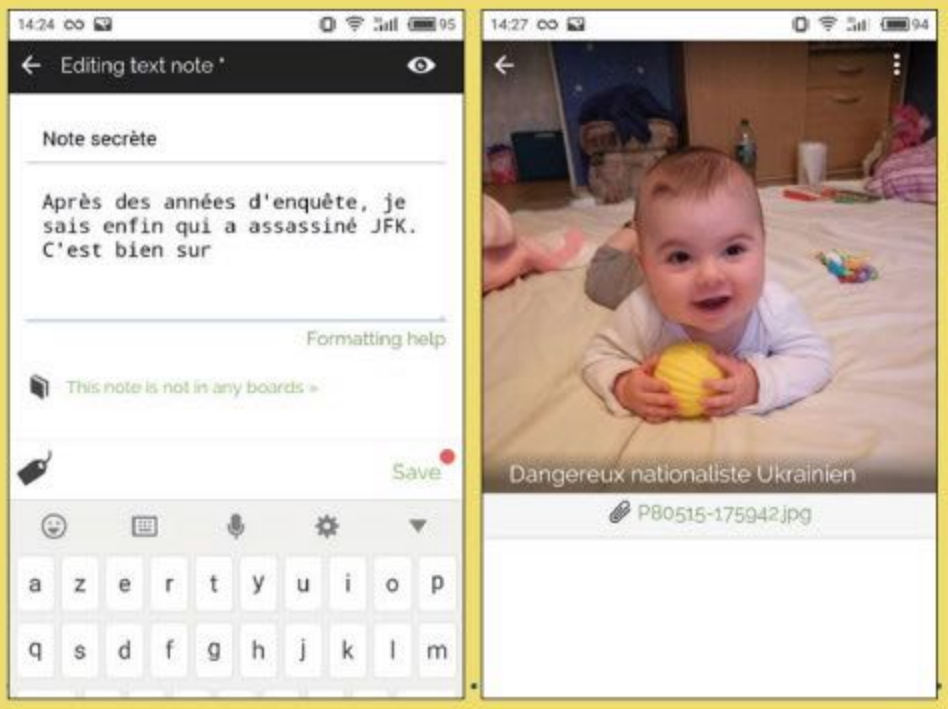
01› OPEN SOURCE ET MULTI PLATES-FORMES

Disponible pour Windows, OSX et Linux, nous avons décidé d'utiliser la version Android de Turtl pour changer un peu. Bien sûr, les fonctions sont les mêmes sur toutes ces plates-formes. Il faudra commencer par ouvrir un compte. Cette étape est indispensable si vous désirez synchroniser vos notes avec d'autres appareils. Attention, il faudra bien se rappeler de ses identifiants, car ce logiciel open source propose du chiffrement de bout en bout.



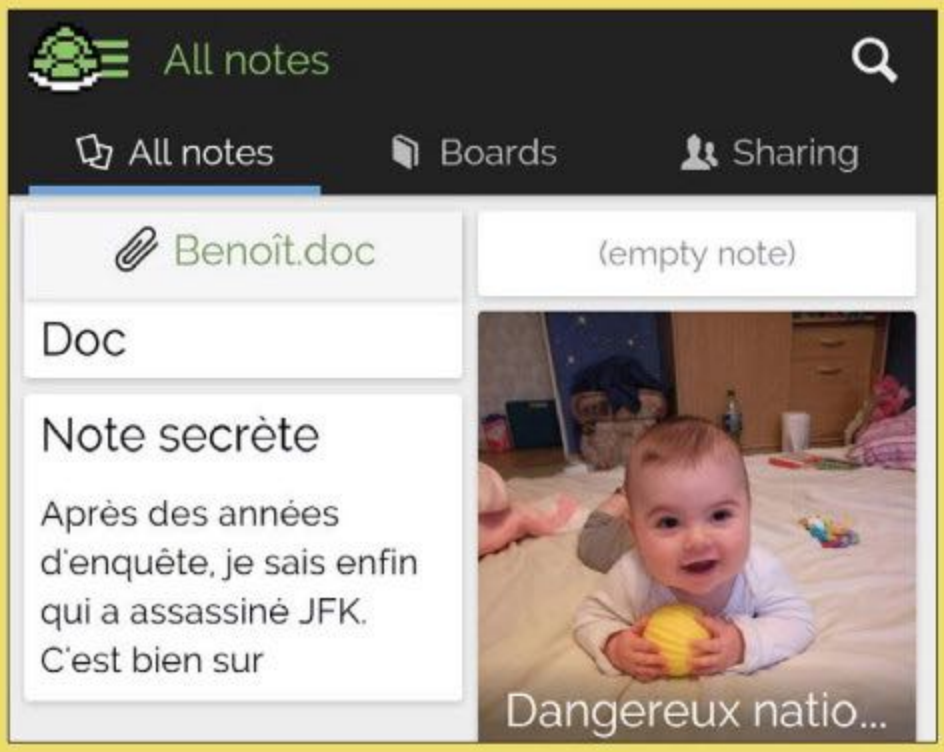
02› LES DIFFÉRENTS TYPES DE FICHIERS

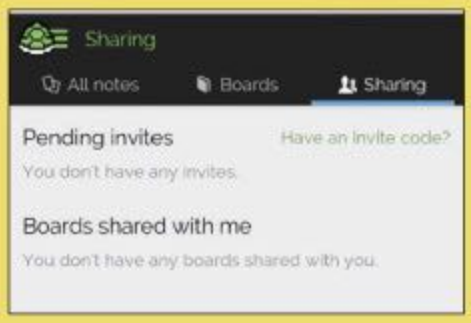
Le menu en anglais est très simple. Vous pouvez stocker des notes écrites, des photos, des mots de passe des favoris ou n'importe quel fichier de votre smartphone ou disque dur. Pour le texte, vous pouvez mettre en page de manière succincte (titre, puces, etc.) et pour les photos, vous pouvez les choisir depuis votre appareil ou depuis une page Internet.



03› PARTAGEZ VOS NOTES

Vos notes seront affichées dans l'onglet **All notes** et vous pourrez les partager avec des amis dans dans **Sharing**. D'ici vous pourrez envoyer des codes «ami» et vous faire inviter dans les **Board** de vos correspondants. Notez que même si vos mots de passe ne sont stockés nulle part en ligne, vous pouvez paramétrer votre propre serveur pour avoir un contrôle total sur le contenu.



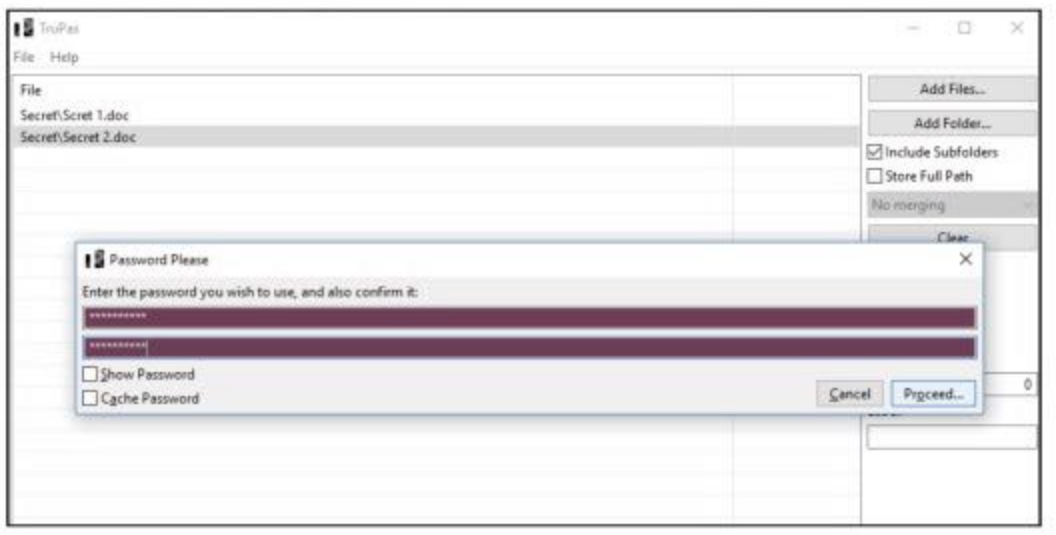


Trupax → Chiffrez vos fichiers privés

TruPax vous permet de chiffrer vos fichiers et dossiers sensibles. Sous une interface un peu minimaliste, il s'avère simple à utiliser, puisqu'il suffit de faire glisser les fichiers ou dossiers à protéger dans la fenêtre du logiciel, avec la souris. Il suffit ensuite d'indiquer l'emplacement du conteneur chiffré et de taper un mot de passe. Bien entendu, il faut repasser par le logiciel pour déchiffrer les données.

Difficulté : ☠☠☠

Lien : **www.coderslagoon.com**

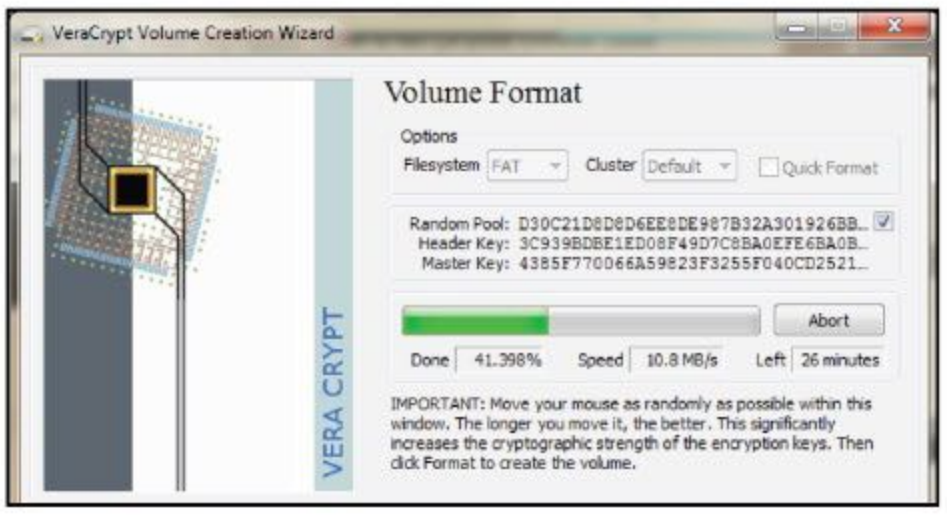


VeraCrypt → La référence pour chiffrer vos données

Outil de référence, conseillé par la CNIL, VeraCrypt est un logiciel de chiffrement très puissant. Vous réservez un espace « conteneur » sur votre disque dur, qui apparaîtra ensuite comme une partition indépendante. Tout ce que vous y copiez est chiffré. La mise en place de VeraCrypt n'est pas un modèle de simplicité, mais son utilisation s'avère ensuite assez pratique, et le niveau de sécurité atteint justifie largement l'effort. Un must.

Difficulté : ☠☠☠

Lien : **www.veracrypt.fr**



Secrecy → Chiffrer vos documents sur mobile

Si vous avez une vieille version d'Android ne prenant pas en charge le chiffrement natif des fichiers, vous pouvez utiliser Secrecy. L'appli propose une solution simple et open source. Il suffit de se confectionner un espace chiffré en AES 256 où vous pourrez placer vos documents sensibles. Personne ne pourra accéder à vos photos, vidéos, PDF et autres fichiers. Vous choisissez l'emplacement de ce coffre fort (mémoire interne ou carte SD) et la sélection des fichiers se fait via le menu partage qui est commun à toutes les applications. Si vous désinstallez Secrecy ou que vous exportez vos conteneurs chiffrés vers un PC par exemple vous pourrez les déchiffrer avec un logiciel compatible AES 256 comme 7Zip.

Difficulté : ☠☠☠

Lien : **http://goo.gl/0NOsSE**

CHIFFREMENT

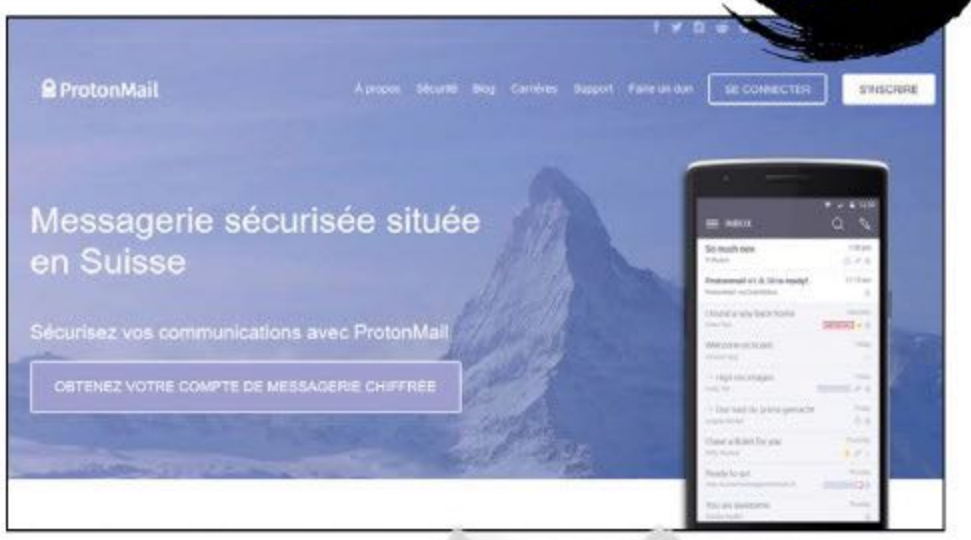
ProtonMail → Webmail chiffré

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

Lancé par trois anciens scientifiques du CERN, la prestigieuse organisation européenne de recherche nucléaire basée à Genève, ProtonMail est né d'un constat simple : nos trois compères estimaient que leurs échanges de mails n'étaient pas assez sécurisés. Basé en Suisse, ProtonMail propose un chiffrement de bout en bout comme c'est la mode en ce moment. Attention, personne ne pourra vous redonner l'accès à vos e-mails si vous perdez le mot de passe. Mais vous le savez bien si vous nous lisez, le problème avec les solutions chiffrées c'est qu'il faut que tous les correspondants utilisent le même système. Comme Tutanota, ProtonMail utilise donc une astuce pour chiffrer les messages que vous envoyez à une personne n'ayant aucune connaissance et aucune intention de s'inscrire à ce service : un simple mot de passe à entrer pour accéder à la conversation.

Difficulté : ☠☠☠

Lien : **https://protonmail.com/fr**



LEXIQUE

***CHIFFREMENT DE BOUT EN BOUT :**

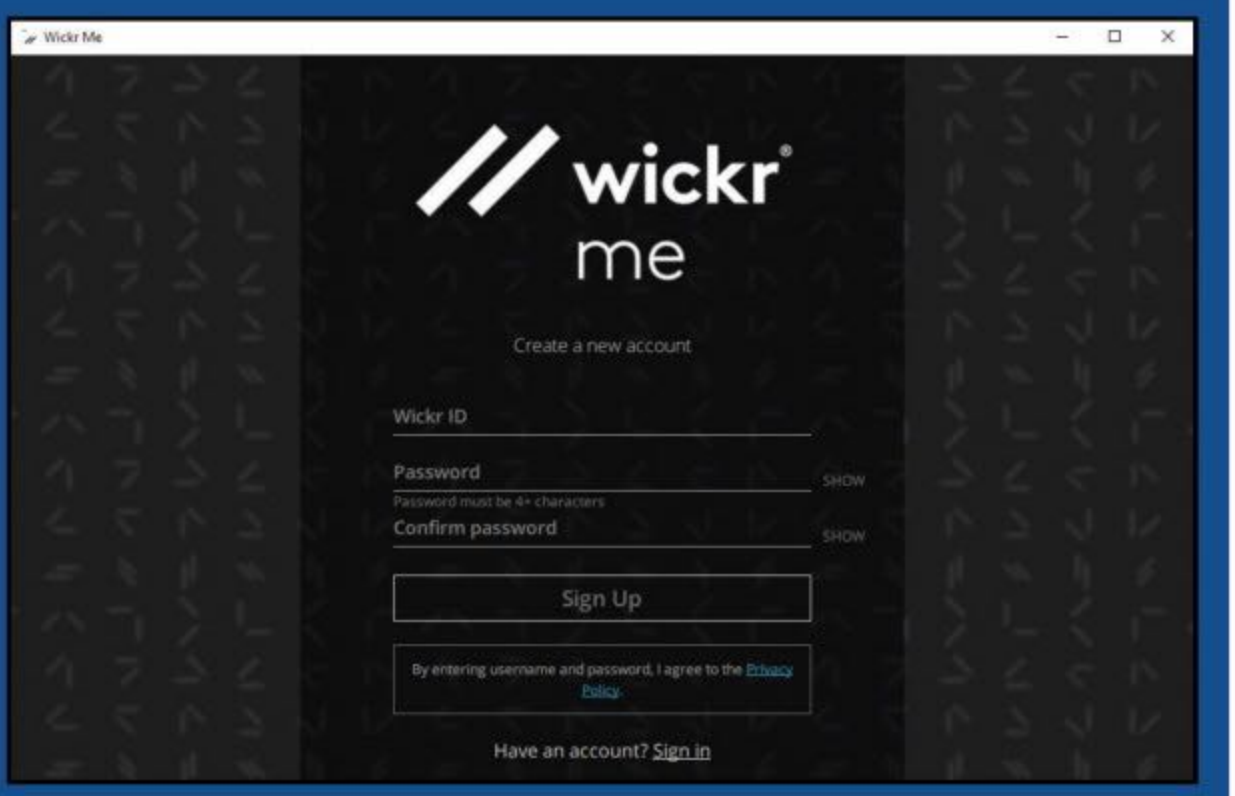
Ou «end-to-end» dans la langue de Donald Trump (l'anglais pas le mongol, suivez un peu !). Il s'agit d'un système de communication où seules les personnes impliquées peuvent lire les messages échangés. Il évite le problème d'écoute électronique, car les clés ne sont pas échangées sur le réseau.

Wickr → Messagerie multi plates-formes

Wickr est un logiciel multi-supports (Windows, Linux, iOS, Android, Mac) permettant de chiffrer vos messages, des photos ou autres fichiers. Vous choisissez qui peut lire ce que vous envoyez et le déchiffrage se fait localement par l'intermédiaire des serveurs de Wickr. Une fois la transmission terminée, tout est effacé.

Difficulté : ☠☠☠

Lien : **https://wickr.com**



Mailvelope → Une extension pour les chiffrer tous !

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**

Telegram → Du mobile au PC

Utilisé par 200 millions de personnes dans le monde, Telegram intègre un chiffrement de bout en bout sur mobile. Le problème, que relèveront les anti-Telegram, est que cette fonctionnalité n'est pas activée par défaut. Il faut en effet aller dans le menu, puis faire **New Secret Chat** pour initier une conversation privée. Avec cette précaution, vous ne laisserez aucune trace de vos messages sur les serveurs de Telegram et il sera impossible d'avoir une trace sur l'application PC/Mac. Sans cela, les messages envoyés sont tout de même chiffrés, mais ils reposent sur les serveurs de Telegram. L'autre problème qui hérisse les poils des adversaires de Telegram c'est la notion d'open source. Le client est en effet ouvert, comme Signal, et on peut donc vérifier qu'aucune backdoor n'ira compromettre vos messages. Par contre au niveau de la partie serveur, le logiciel est propriétaire. Impossible donc d'être sûr que les messages ne sont pas lus. Pour le créateur de Telegram la solution est simple : utilisez le tchat secret si vous ne faites pas confiance à Telegram ! L'appli dispose d'une version pour PC et même d'un client sur navigateur : https://web.telegram.org. Dernier détail : on peut maintenant téléphoner avec Telegram !

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

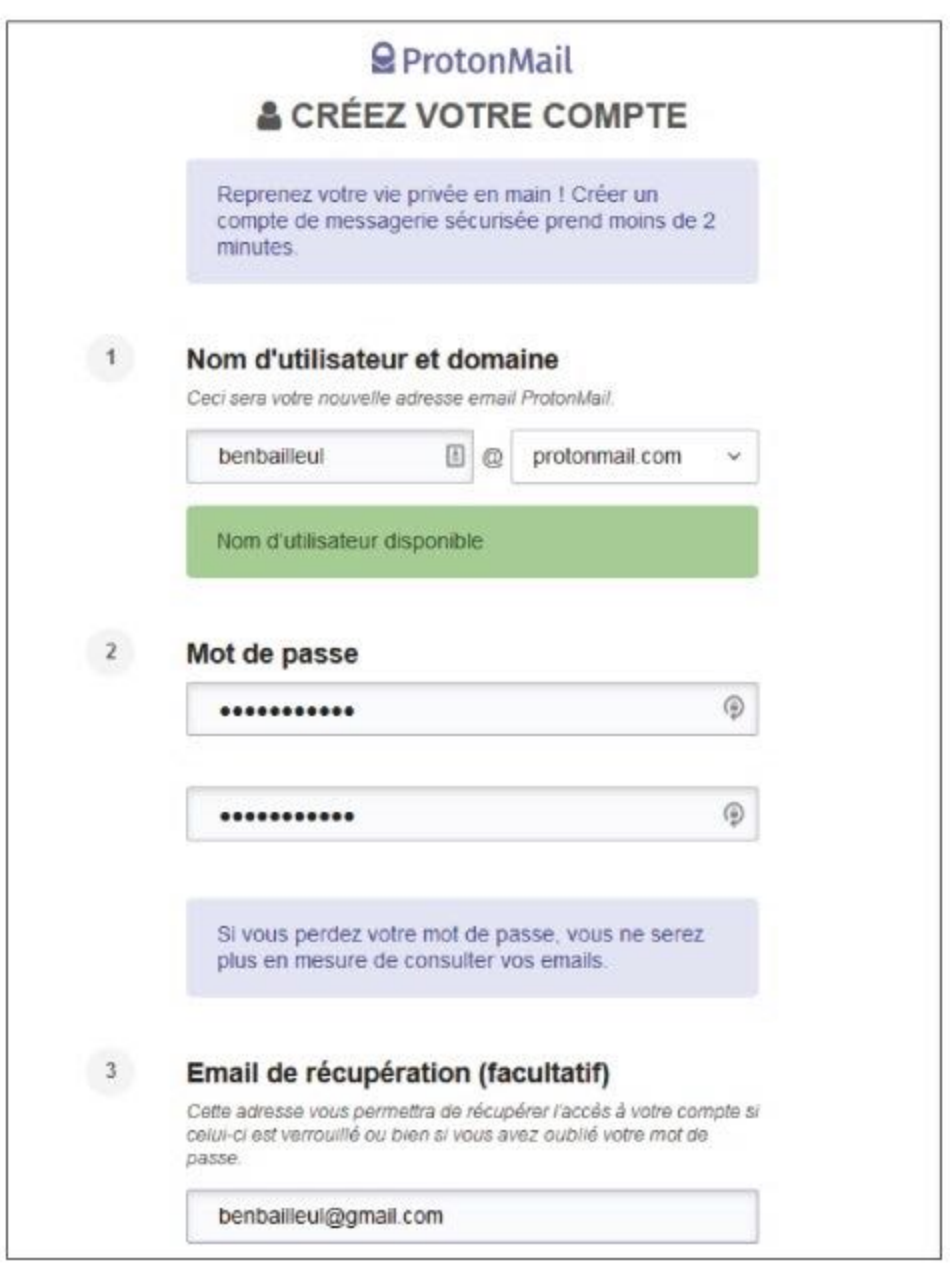
ProtonMail en mode «invité»

INFOS [PROTON MAIL]
Où le trouver ? [**https://protonmail.com/fr**] Difficulté :

TUTO

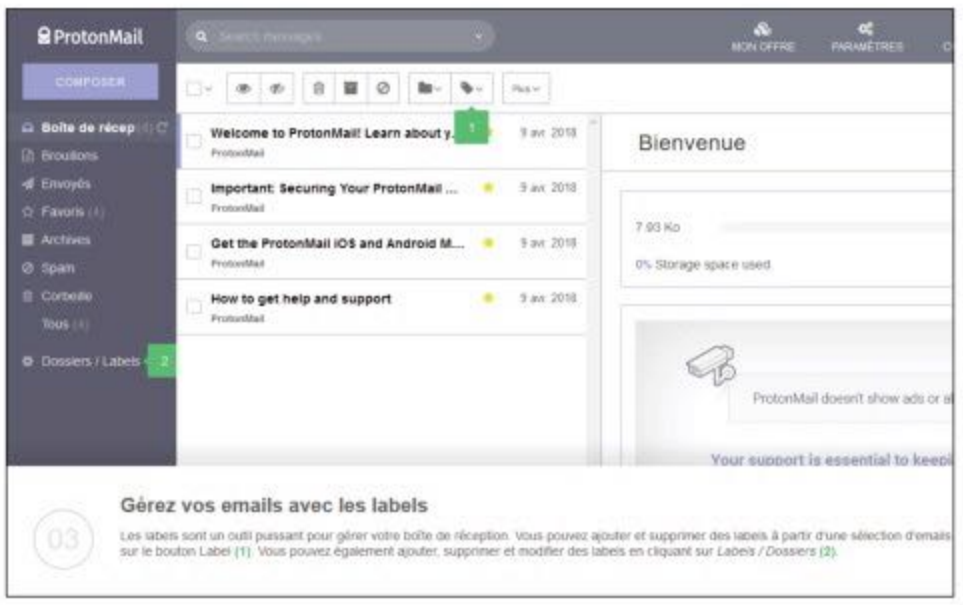
01› L'INSCRIPTION

Sur le site, allez dans **S'inscrire**, optez pour le compte gratuit et choisissez vos identifiants. Il est possible de paramétrer un compte de récupération. Inutile de préciser que ce dernier devra être bien sécurisé avec un mot de passe solide. Libre à vous de télécharger l'appli pour téléphone portable à la fin du processus.



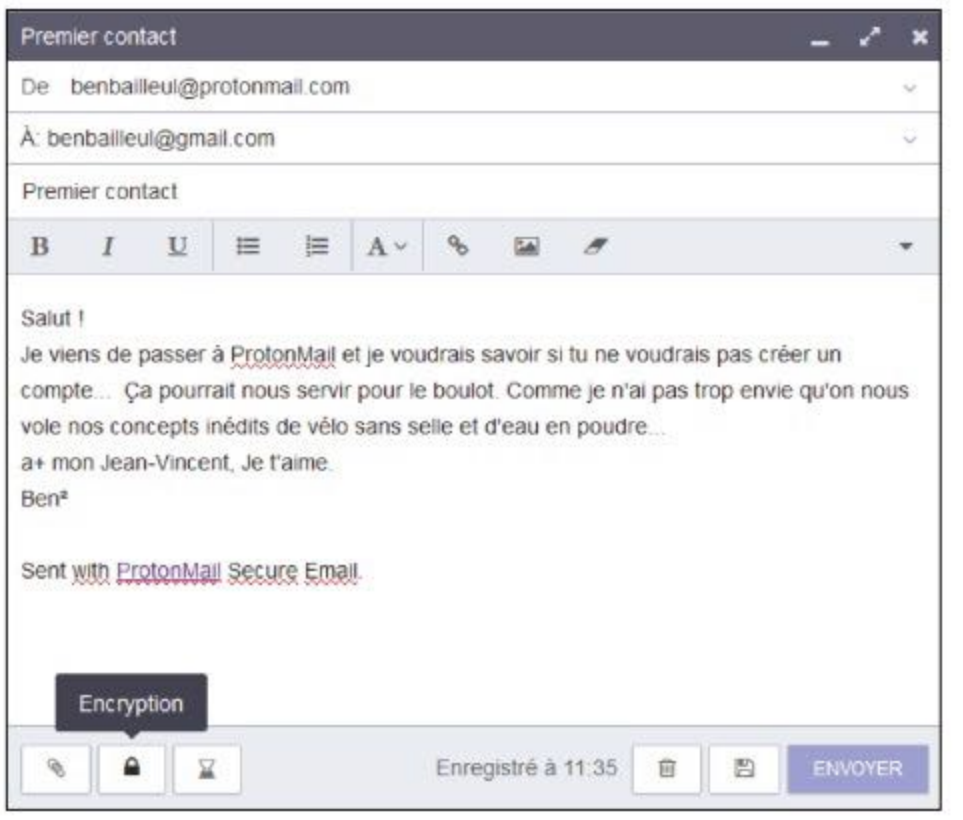
02› L'INTERFACE

Votre boîte aux lettres devrait comporter 4 e-mails pour vous expliquer le fonctionnement, mais ils sont en anglais. À l'inverse, le tuto dans le bandeau en bas est en français, comme toute l'interface d'ailleurs. Faites **Composer** pour écrire votre premier e-mail.



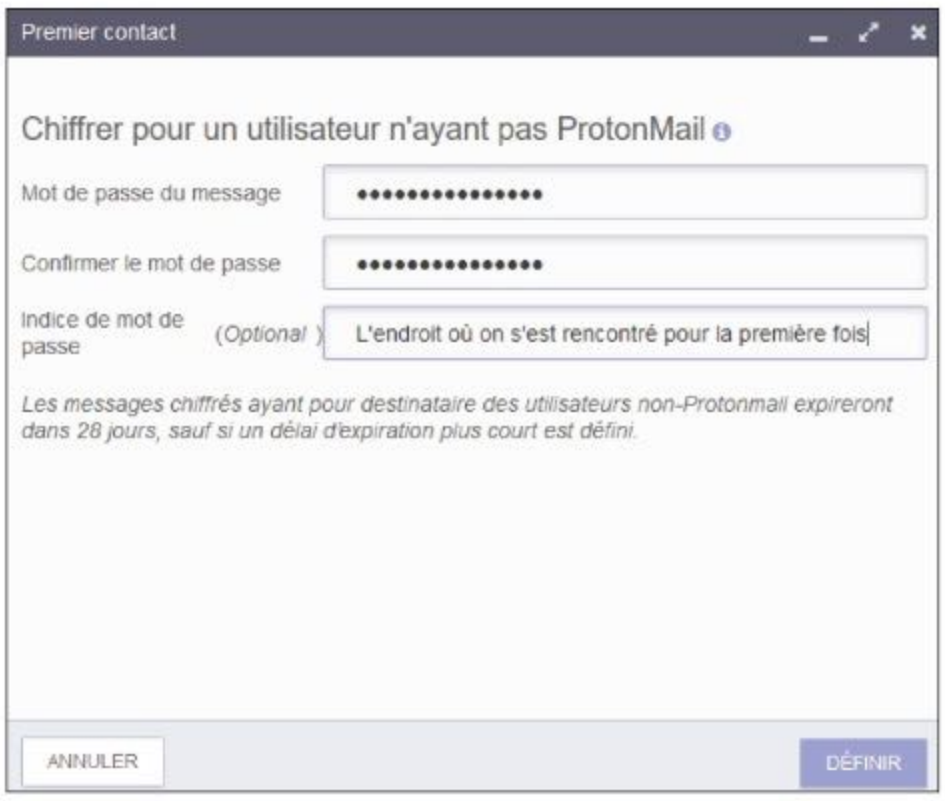
03› LES 3 BOUTONS

En bas à gauche, vous pourrez trouver des boutons pour ajouter une pièce jointe (qui sera aussi chiffrée) ou mettre un délai d'expiration (en semaines, jours ou heures). Notez que si vous décidez de chiffrer un e-mail pour un utilisateur n'ayant pas ProtonMail, le délai de rétention sera de 28 jours par défaut sauf si vous décidez de mettre un délai plus court.



04› LE MODE «INVITÉ»

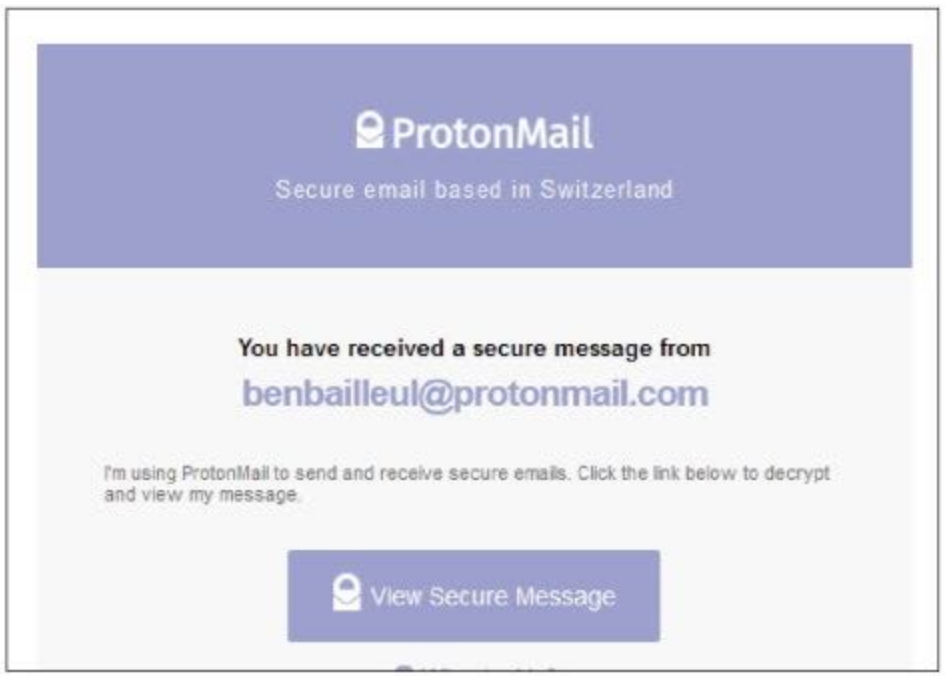
Pour un ami qui a un compte ProtonMail, rien ne vous sera demandé, mais si ce dernier ne l'a pas, vous pouvez soit l'envoyer sans chiffrement soit utiliser l'option **Encryption** avec le cadenas. Définissez un mot de passe et éventuellement



un indice pour votre ami «*L'endroit où on s'est rencontré pour la première fois*» ou «*Le nom de ton roman préféré*». Évitez «*La couleur de ta voiture*» ou «*Le nom de ton chien*», trop facile à deviner ou trouver sur le Net (merci Facebook). Vous pouvez aussi ne donner aucun indice et communiquer ce sésame avec une méthode secondaire : de vive voix, depuis Signal ou Telegram.

05› LA RÉCEPTION

Sur sa boîte non sécurisée, votre ami recevra un e-mail (malheureusement en anglais)



pour lui expliquer que vous essayez de le joindre sur un canal sécurisé. Il lui suffira de cliquer sur le lien **View Secure Message** et de rentrer le mot de passe qu'il aura deviné grâce à l'indice. Il peut y répondre et échanger librement ou s'inscrire et lui aussi opter pour ProtonMail.

06› SUR MOBILE

Sur smartphone c'est la même chose. L'appli est très bien conçue, mais si votre correspondant n'a pas ProtonMail, il sera dirigé vers son navigateur pour répondre… comme sur PC. En ayant testé les deux solutions (ProtonMail et Tutanota), nous ne saurons en conseiller une plus que l'autre. Pour être franc, c'est le nombre d'amis qui ont opté pour l'un ou l'autre service qui fera pencher la balance.

MULTIMÉDIA

SUPER© → Le très pointu

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

Difficulté : ☠☠☠

Lien : **www.erightsoft.com**

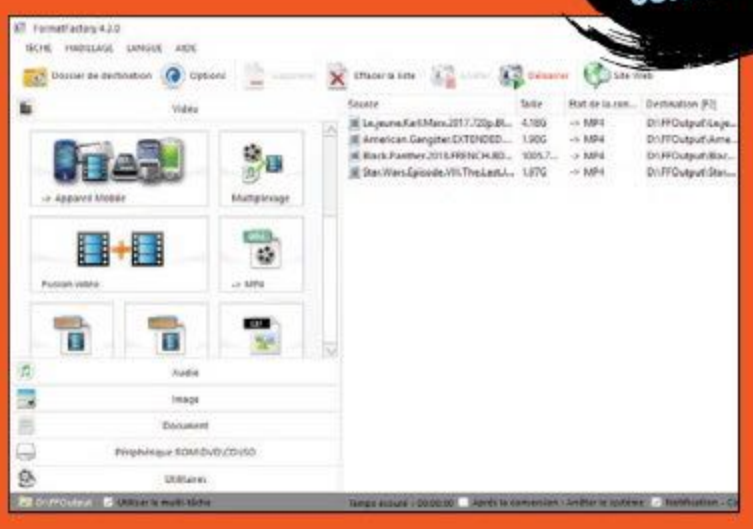
M4ng v5 → De l'encodage à la carte

Medi4 next gen (abrégé en m4ng) est un logiciel permettant de faire énormément de manipulations avec vos précieuses vidéos. Vous avez un DVD ou un Blu-ray plein d'épisodes de votre série préférée et vous voudriez les lire sur votre iPad, PC, Surface ou smartphone Android ? Cette vidéo téléchargée ne fonctionne pas sur votre machine de prédilection ? Changer l'encodage du son uniquement ou fusionner deux vidéos en une seule ? Pour toutes ces tâches, m4ng s'en sortira sans problème. Il est aussi possible de couper, coller, isoler le son, recréer les chapitres d'un DVD ou d'un Blu-ray, si vous avez un graveur de ce type. Un module permet même d'éditer leurs fichiers SRT ou SUB.

Difficulté : ☠☠☠ Lien : **www.m4ng.fr**

Format Factory → Pour les débutants et les autres

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES



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

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

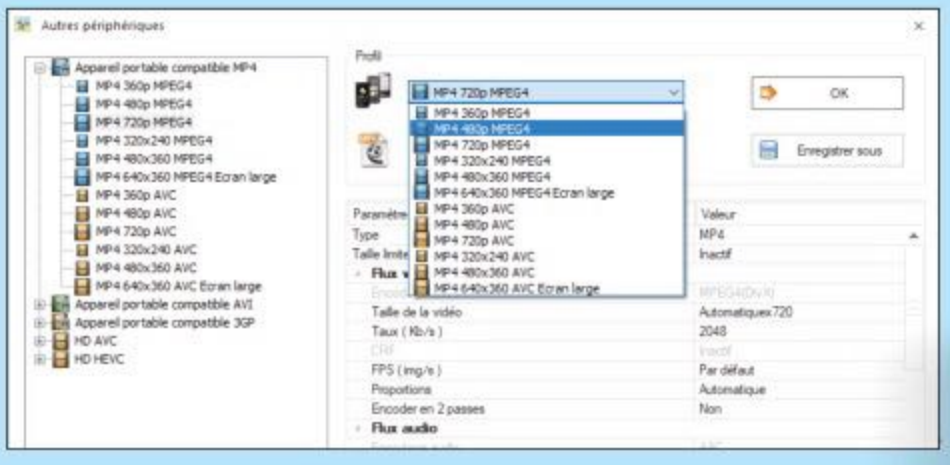
L'encodage avec Format Factory

INFOS [FORMAT FACTORY]
Où le trouver ? [**https://format-factory.fr.softonic.com**] Difficulté : ☠☠☠

TUTO

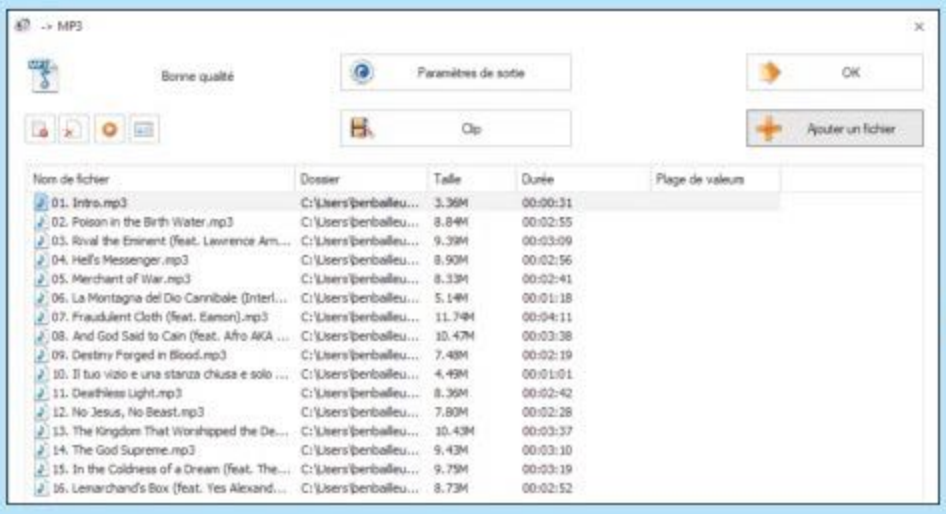
01› UN EXEMPLE...

Imaginons que vous vouliez encoder un fichier vidéo pour votre téléphone ou tablette. Dans la partie **Vidéo**, cliquez sur **-> Appareil Mobile**. Dans la colonne de gauche, vous verrez une liste d'appareils longue comme le bras. Vous trouverez sans doute votre machine. Si ce n'est pas le cas, cliquez sur un format que votre gadget sait lire (3GP, AVI ou MP4) et peaufinez vos réglages dans la partie de droite.



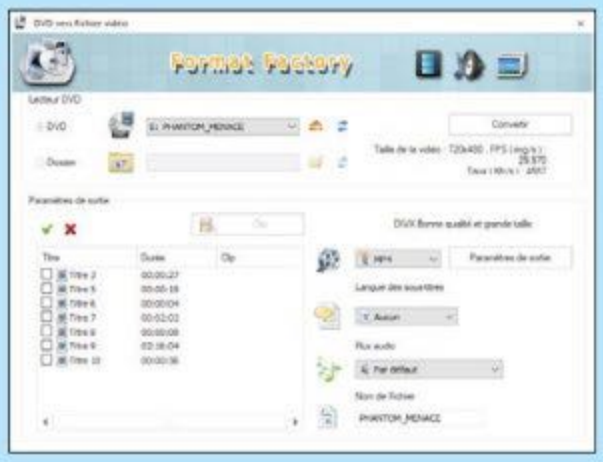
02› ... PARMI TANT D'AUTRES !

Pour les fichiers audio ou les photos, c'est à peu près la même chose. Dans l'onglet adéquat, cliquez sur **Tout type vers [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. Faites **OK** puis, une fois revenu à la fenêtre principale, cliquez sur **Démarrer**.



03› EXTRACTION AUDIO OU VIDÉO

Enfin, sachez que Format Factory permet aussi de «ripper» le contenu d'un CD, d'un DVD ou d'un Blu-ray pour en faire des fichiers exploitables par votre PC. Allez dans **ROM périphérique/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.)



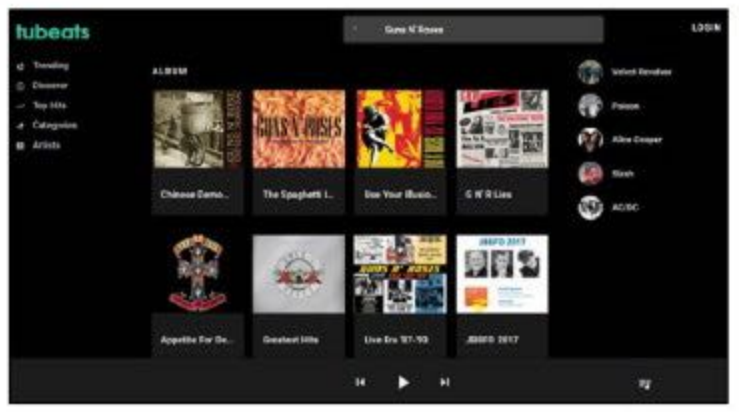
LEXIQUE

ENCODAGE : L'encodage consiste à modifier les données d'un fichier multimédia pour le faire fonctionner sur un appareil en particulier ou ne permettant pas l'installation de codec. Avec ces logiciels d'encodage, il est par exemple possible de changer un film lu sur PC (codec Xvid, conteneur AVI) pour le lire sur une PlayStation 3 (codec H264, conteneur MP4). Cela fonctionne aussi pour l'audio.

CODEC : Mot-valise pour «codeur-décodeur». Il s'agit d'un programme capable de compresser et/ou de décompresser un signal numérique : audio ou vidéo. Par exemple, il vous faudra le codec Xvid installé sur votre PC pour lire un fichier AVI encodé en Xvid.

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

Écouter de la musique gratuitement → avec Tubeats



Tubeats est un service de streaming audio totalement gratuit. Ce dernier va piocher les morceaux qu'il propose dans le répertoire de YouTube ou d'autres plates-formes de vidéos plus confidentielles. En vous inscrivant au service avec **Register**, vous vous concoctez des playlists. Pour une simple écoute, utilisez le champ **Search Music** pour trouver les artistes ou les morceaux qui vous intéressent. Vous lancez la lecture avec le bouton **Play**.

Difficulté : **http://tubeats.com**

Nuclear → Le meilleur !

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

Au lieu d'investir une dizaine d'euros dans un service de streaming audio, pourquoi ne pas profiter d'un lecteur audio gratuit donnant accès gratuitement à quantité de titres ? C'est le service que rend Nuclear en proposant également les habituelles fonctionnalités de ces derniers. Le tout sans pub. Avec Nuclear, pas d'interface Web. Ici, il s'agit d'un bon vieux logiciel que vous installez sur votre PC. Depuis ce dernier, vous vous constituez votre bibliothèque musicale en piochant des chansons ou albums complets depuis différentes sources (Youtube, Bandcamp, Soundcloud ou encore Vimeo). Nuclear propose les fonctionnalités « classiques », celles que l'on trouve sur n'importe quel service de streaming audio. Recherche par chanson ou album, création de playlists à partir de ces derniers, découverte d'artistes similaires... l'utilisation du soft ne requiert aucune inscription. Notez que vous pouvez même télécharger, au format .mp3, les morceaux ou albums que vous recherchez.

Difficulté :

Lien : **https://nuclear.gumblert.tech**

LEXIQUE

STREAMING : Procédé de diffusion permettant la lecture en direct de flux audio ou vidéo. Cela s'oppose au principe de téléchargement qui présuppose la récupération préalable des données d'un morceau ou d'une vidéo pour en permettre la lecture.

NoiseQ → Un clone gratuit de Spotify

Nous ne sommes pas peu fiers de notre découverte ! 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 elle 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.

Difficulté : Lien : **http://noiseq.com**

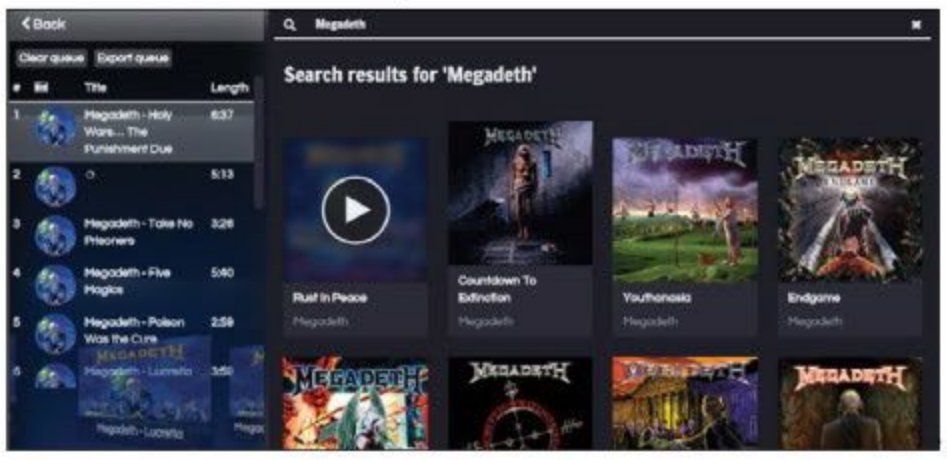
Organiser sa musique avec Nuclear

INFOS [NUCLEAR]
Où le trouver ? [**https://nuclear.gumblert.tech**] Difficulté : ☠☠☠

TUTO

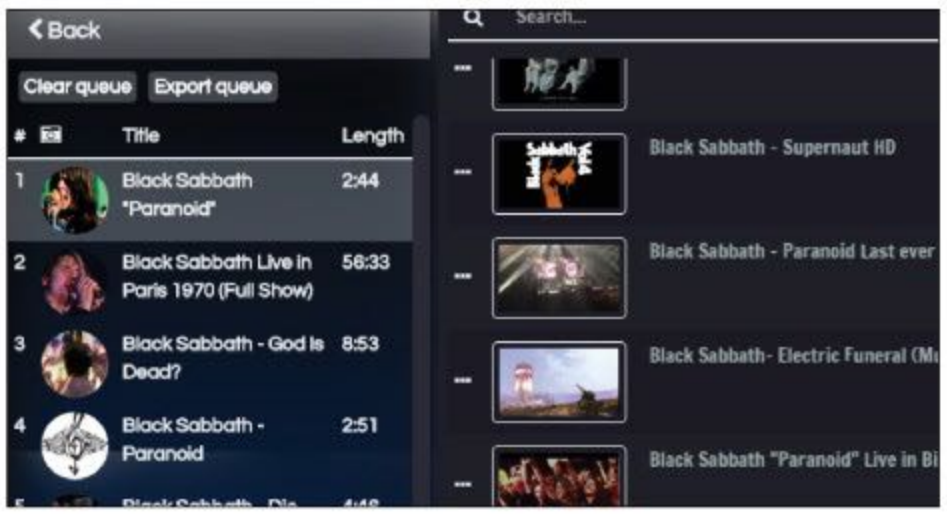
01› RECHERCHER

Ouvrez Nuclear puis cliquez sur **Find albums** puis recherchez à l'aide du nom de l'artiste ou de l'album désiré. Cliquez sur la pochette qui vous intéresse pour débuter la lecture. Les morceaux contenus dans l'album s'ajoutent dans la liste de lecture (**Queue**). Avec **Search**, vous cherchez directement les morceaux que vous ajoutez à votre liste de lecture avec le **+** (en survolant la miniature).



02› CRÉER UNE PLAYLIST

Commencez par ajouter des morceaux à votre liste de lecture (**Queue**) en vous servant des outils de recherche présentés en étape 1. Allez ensuite dans l'onglet **Queue** pour choisir **Export queue**. Un message mentionne que votre playlist a été enregistrée. Faites **Clear queue** pour en démarrer une nouvelle ou allez dans **My Playlists** puis choisissez **Play** en dessous de la playlist de votre choix pour en démarrer la lecture.

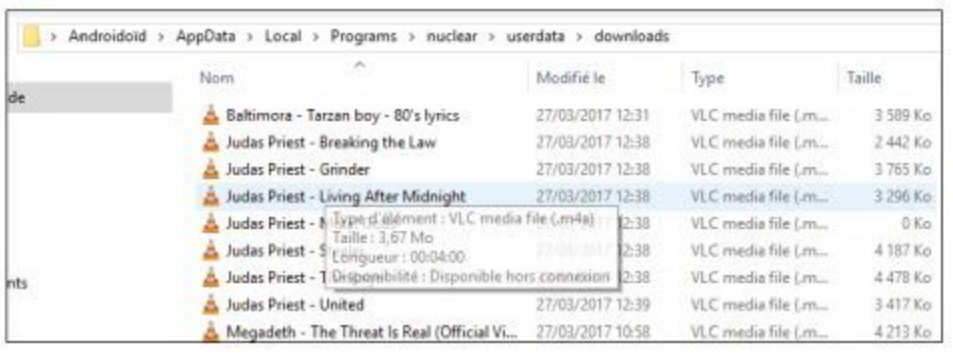


03› TÉLÉCHARGER

Depuis Nuclear, vous avez la possibilité de télécharger les morceaux de votre choix au format .mp3. Lancez votre recherche (de chanson ou d'album) via **Search** puis cliquez sur les trois petits points avant de choisir **Download**. Allez ensuite dans l'onglet **Downloads** pour lancer l'opération avec **Start downloading**. Patientez quelques instants.

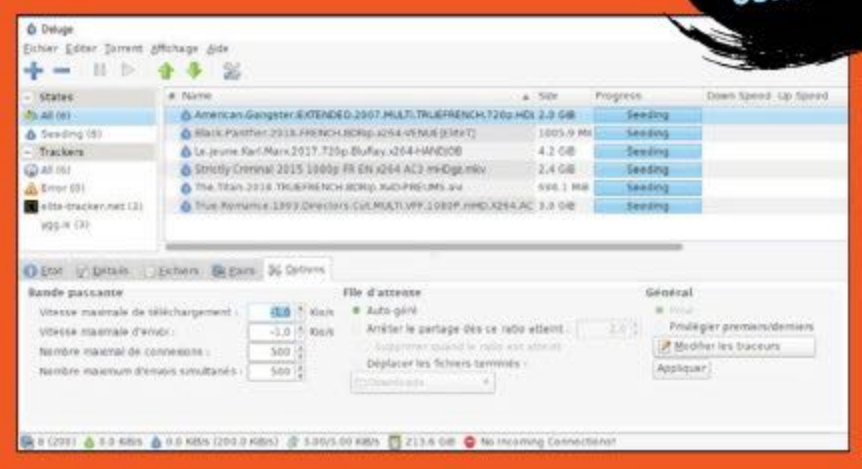
04› RETROUVER LES MORCEAUX

Partez à la pêche des morceaux que vous venez de télécharger. Pour ce faire, suivez le chemin **C:\Users\ « votre nom d'utilisateur »\AppData\Local\Programs\nuclear\userdata**. Accédez aux morceaux que vous venez de télécharger en explorant le contenu du dossier **Downloads**. Faites un double clic sur le morceau de votre choix pour en débuter la lecture depuis votre lecteur multimédia de votre choix.



Deluge → Un client Torrent léger comme l'air

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

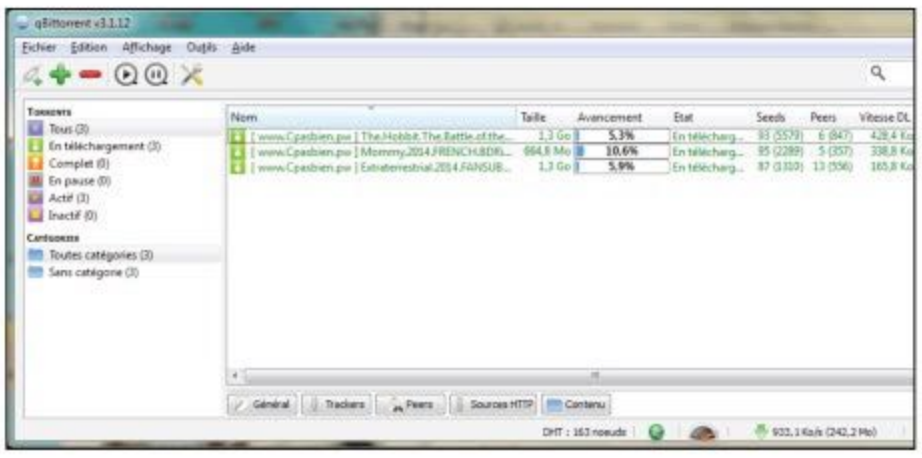


Très populaire auprès des utilisateurs de seedbox, Deluge conviendra parfaitement à ceux qui sont devenus allergiques à µTorrent ou qBitorrent. Il propose aussi un grand nombre de plugins permettant d'ajouter des fonctionnalités et d'automatiser de nombreuses opérations (renommer, récupérer des métadonnées, copier, etc.) 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.

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

qBittorrent → La relève des clients Torrent

Vous en avez marre de µTorrent : consommation de ressources excessive, logiciels additionnels étranges, etc. qBittorrent est un client que les amoureux des premières versions de µTorrent



vous adorer. Il est léger, simple et propose des options pratiques et claires. Il est compatible avec le DHT, les flux RSS et les liens magnet. Cerise sur le gâteau ce dernier est open source et complètement en français. Il est peut-être temps de changer de crèmerie...

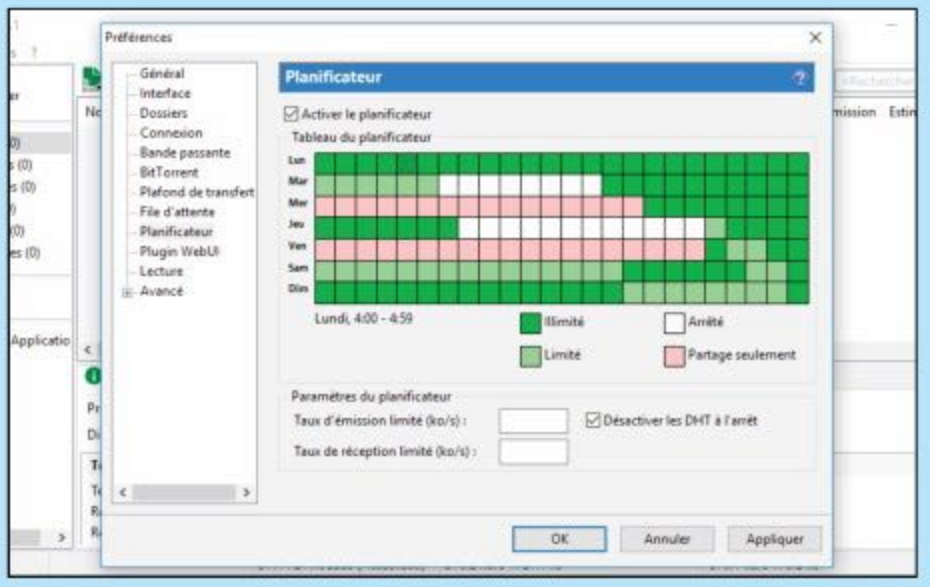
Difficulté : ☠☠☠
Lien : **www.qbittorrent.org**

µTorrent → Le vieux lion

Même après avoir été racheté par la société BitTorrent, µTorrent reste un de nos clients Torrent préférés. Attention, nous ne parlons pas des versions récentes (lourdes, avec une version Premium bidon et des spywares) mais bien de la mythique v2.2. C'est cette version que vous retrouverez en suivant notre lien. µTorrent c'est un planificateur très malin, la possibilité de gérer ses téléchargements à distance sur un autre PC ou sur mobile et des options de partage et de maîtrise du ratio indispensable.

Difficulté : ☠☠☠

Lien : **https://tinyurl.com/ztou95q**

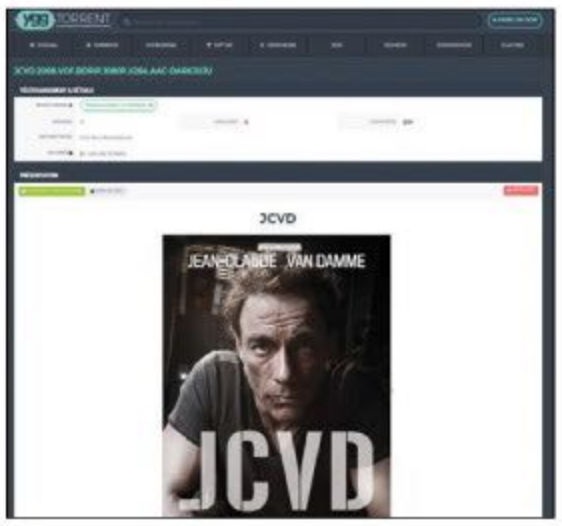


Familiarisez-vous avec Deluge

INFOS [DELUGE]
Où le trouver ? [**http://deluge-torrent.org**] Difficulté :

TUTO

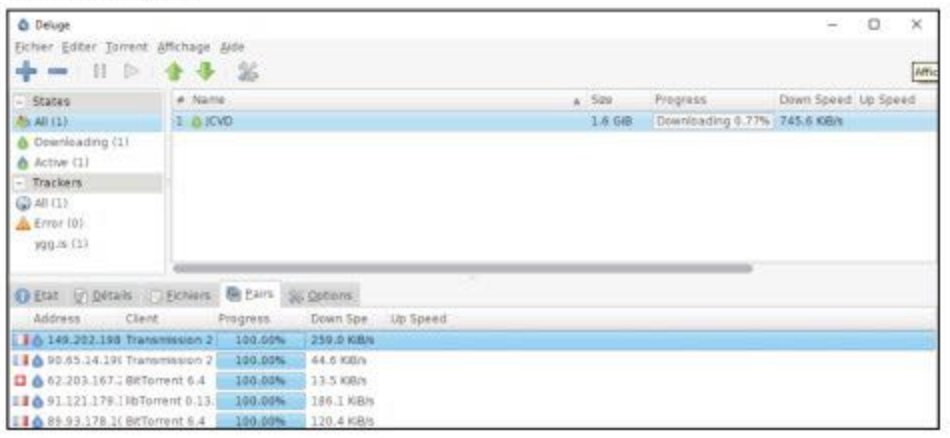
01› TROUVER UN .TORRENT ET LE PLACER



Les débutants ne seront pas perturbés puisque s'ils veulent simplement télécharger un fichier avec un lien Torrent, il n'y a rien de plus facile. Il suffit de cliquer sur + ou de copier-déplacer votre fichier .torrent dans la fenêtre principale. Parfois certains sites proposent des liens «magnet». Il suffit de cliquer dessus pour que le client prenne le relais automatiquement. Attention, il faudra que votre logiciel soit le programme par défaut (normalement on vous le demandera à l'installation.)

02› LES DONNÉES DE VOTRE .TORRENT

Si votre Torrent ne démarre pas, c'est peut-être qu'il y a un problème : vieux fichier, nécessité de s'inscrire sur le site où vous l'avez trouvé. En bas vous trouverez des onglets pour voir l'état du fichier, différents détails, les pairs avec qui vous partager le fichier et différentes options sur la bande passante et la file d'attente : pratique si vous galérez avec votre connexion.

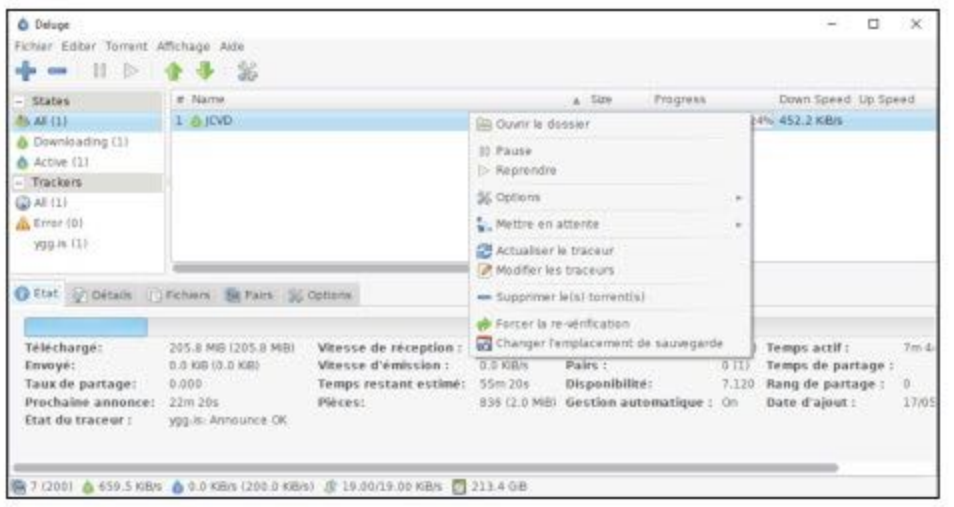


03› PLUS DE PARAMÈTRES

Pour plus d'options, il faudra aller en haut dans l'icône avec la clé et le tournevis. Ici vous trouverez des paramètres plus ou moins utiles selon votre maîtrise du protocole : gestions des ports, emplacement des fichiers téléchargés, gestion des vitesses de téléchargement, gestion des ratios, proxy, divers plugins et la possibilité d'accéder à vos téléchargements depuis une interface Web (pratique si vous n'êtes pas chez vous!)

04› DES OPTIONS AU CAS PAR CAS

En faisant en clic droit dans un Torrent, vous avez la possibilité de les gérer au cas par cas : pause, changer l'emplacement, actualiser les données du tracker en cas de problème ou changer ces données à la main en cas de changement de domaine. N'oubliez pas que si vous voulez que d'autres puissent profiter du fichier, il faudra jouer le jeu et laisser vos téléchargements fonctionner même arrivés à 100 % : c'est d'ailleurs obligatoire avec des trackers privés ou semi-publics.



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.

BEST-OF 2018

LA TROUSSE À OUTILS ULTIME DU PIRATE

LES 99 MEILLEURS LOGICIELS ESSENTIELS & GRATUITS

IDPRESSE

L 14376 - 16 - 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