

N°42 NOUVELLE FORMULE + DE PAGES + DE HACKS + DE TUTOS



Août / Oct. 2019

PIRATE INFORMATIQUE

DERNIÈRE CHANCE

TOP 6 DES
LiveCD

POUR RÉPARER,
SAUVEGARDER
ET DÉSINFECTER

LE GUIDE PRATIQUE

DU PIRATE

LIBRA

TOUT SAVOIR SUR
L'ANTI-BITCOIN
DE FACEBOOK



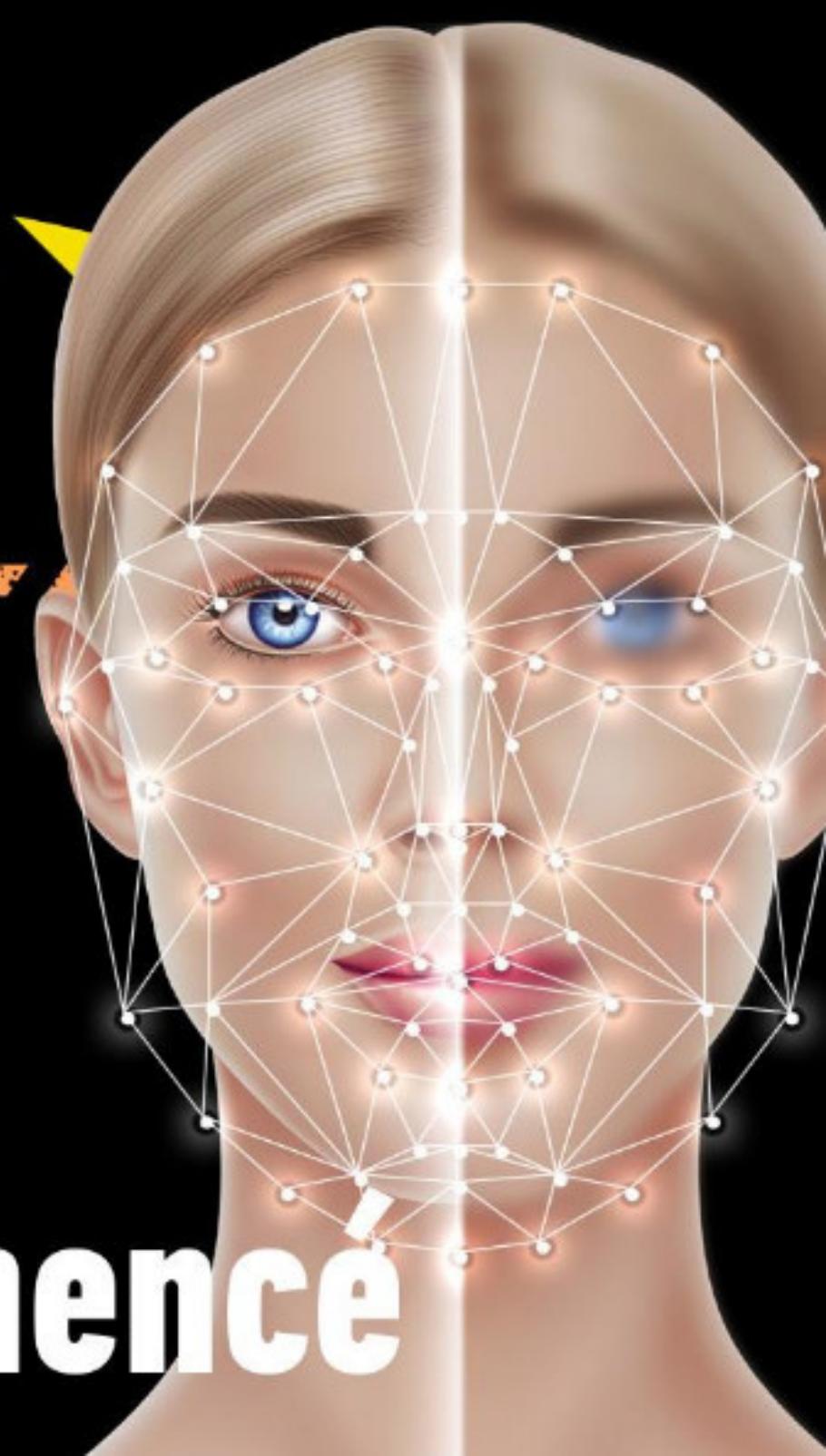
INTERVIEW
L'INDÉPENDANCE
DE QWANT
EST-ELLE À
VENDRE ?

WI-FI
HACKÉ
TESTEZ
VOTRE
RÉSEAU

BLACK DOSSIER

>> Sexe, IA,
Mensonges & Vidéos

DeepFakes :
L'invasion a commencé





SOMMARE

BLACK DOSSIER
16–25
DeepFakes : L'invasion a commencé

HACKING

26–28

WINDOWS FILE TOOLS :

surveillez l'activité de Windows

29–32

Les LIVE CD au SECOURS

de votre PC...

34–36

L'ATTaque DDOS,

c'est quoi ?



37–39

ÉCRAN CASSÉ :

que faire avec votre appareil ANDROID ?

40–43

WIFITE : intrusion dans un RÉSEAU SANS FIL

44

MICROFICHES



ANONYMAT

46–47

QWANT, un moteur de recherche respectueux de votre VIE PRIVÉE ?



SOUTENEZ-NOUS !

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

48-49

OPERA : le navigateur avec **VPN** gratuit

50

MICROFICHES



PROTECTION

52-53

DOUBLE AUTHENTIFICATION : une protection inviolable ?



54-55

BITKILLER : êtes-vous sûr d'avoir **TOUT EFFACÉ** ?



56-57

MICROFICHES

MULTIMÉDIA

58-59

FAKE ! Nos astuces pour **DÉTECTER** les fausses images

60-61

MICROFICHES

62-63 > NOTRE SÉLECTION DE MATÉRIELS

ÉDITO

BONJOUR AUX HABITUÉS COMME AUX NOUVEAUX VENUS !

Ce numéro 42 (nombre cher à Douglas Adams) se veut plus éclectique que jamais. Nous nous intéresserons aux attaques DDoS, mais aussi à la cryptomonnaie Libra qui sera bientôt lancée par Facebook. Kevin nous expliquera les mécanismes de la double authentification et les moyens de repérer les fakes. Nous avons aussi eu la chance d'avoir pu poser nos questions à Tristan Nitot de Qwant concernant les données qui seraient envoyées à Microsoft et le moins qu'on puisse dire, c'est que nous n'en sommes pas sortis

déçus. Dans ce magazine vous trouverez aussi des sujets plus pratiques avec la prise en main de WiFi sous Linux pour tester votre réseau sans fil ou sur les solutions en votre possession si vous avez cassé l'écran de votre smartphone. Enfin, nous vous avons préparé un dossier sur le phénomène Deepfake : inquiétant et fascinant à la fois.

N'hésitez pas à nous faire part de vos commentaires et de vos souhaits pour les prochaines éditions sur benbailleul@idpresse.com

Benoît BAILLEUL.



PIRATE

N°42 INFORMATIQUE

Août / Oct. 2019

Une publication du groupe ID Presse.

Impasse de l'Espéron - Villa Miramar

13960 Sausset Les Pins

E-mail : redaction@idpresse.com

Directeur de la publication :

David Côme

Le Loup : Benoît Bailleul

Nif-Nif, Naf-Naf & Nouf-Nouf :

Aude Boireau, Kevin Dachez & Team Blackbird

Dingo & Clarabelle : Sergueï Afanasiuk & Stéphanie Compan

Correctrice : Marie-Line Bailleul

Imprimé en France par / Printed in France by :

Léonce Deprez

ZI Le Moulin 62620 Ruitz

Distribution : MLP

Dépôt légal : à parution

Commission paritaire : en cours

ISSN : 1969 - 8631

«Pirate Informatique» est édité par SARL ID Presse, RCS Aix-En-Provence 491 497 665

Parution : 4 numéros par an.

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



CELLEBRITE PEUT DÉVERROUILLER N'IMPORTE QUEL SMARTPHONE ?

L'entreprise Cellebrite, spécialisée dans la cybersécurité, a créé un outil qui fait beaucoup parler de lui. Le Universal Forensic Extraction Device (UFED) permet de déverrouiller n'importe quel iPhone et de très nombreux modèles de smartphones sous Android. On parle des appareils sous iOS 7 à iOS 12.3, des Samsung Galaxy (de S6 à S9) mais aussi des Xiaomi et des Huawei. L'appareil est bien sûr exclusivement réservé aux autorités et aux forces de police du monde entier et même si on en sait peu sur les mécanismes de collecte, la société parle d'effectuer des extractions du système de fichiers complet malgré un verrouillage. Cellebrite est une société sérieuse et on les imagine mal raconter n'importe quoi. On a hâte qu'un de ces petits appareils se retrouve dans la nature...



25

LE CHIFFRE
MILLIONS !



drins se remplissent les poches avec les revenus publicitaires. Pour l'instant les 25 millions de smartphones contaminés se situent majoritairement au Pakistan, en Inde, aux USA et en Russie. La solution pour se protéger ? N'installez jamais une appli de source inconnue...

Selon les experts en cybersécurité de Checkpoint, le malware Agent Smith (en référence au méchant de Matrix) utilise la vieille faille Janus pour s'infiltrer dans les vieux smartphones qui ne sont plus mis à jour. En effet, Janus a été patchée sur les versions 7 (Nougat) et supérieures, mais les versions 4, 5 et 6 d'Android sont potentiellement vulnérables (à moins que les constructeurs n'aient pensé à votre modèle). Agent Smith se propage via des Store alternatifs ou des APK faudruleux. Une fois infecté, votre smartphone va remplacer les applications installées par des applis publicitaires. Les pubs sont tellement nombreuses que les appareils deviennent presque inutilisables. Bien sûr, les malan-

En Bref...

LE PIRATE BULGARE TRAVAILLAIT DANS LA SÉCU

- Le fisc bulgare a dernièrement connu une attaque sans précédent causant la fuite de 3% des données présentes sur les serveurs. C'est un pirate de 20 ans qui serait à l'origine de cette cyberattaque. Ce dernier travaille en fait dans une société de cybersécurité...

DES MACROS CONTRE DES CRYPTOS

- Les temps sont durs pour les pirates de 20 ans puisqu'au Pays bas, c'est la police néerlandaise spécialisée dans les cybercrimes qui a arrêté un fournisseur de macros malveillantes appelées Rubella et Dryad sévissant sur Word ou Excel. Le hacker échangeait ces malwares contre des cryptomonnaies.

ANUBIS CE GROS CHACAL !

- Le malware Android Anubis est de retour ! Ce dernier simule une page de connexion de votre application bancaire tellement bien que vous n'y verrez que du feu. D'après les spécialistes de TrendMicro, Anubis peut s'attaquer à plus de 188 applications bancaires, de diverses nationalités.



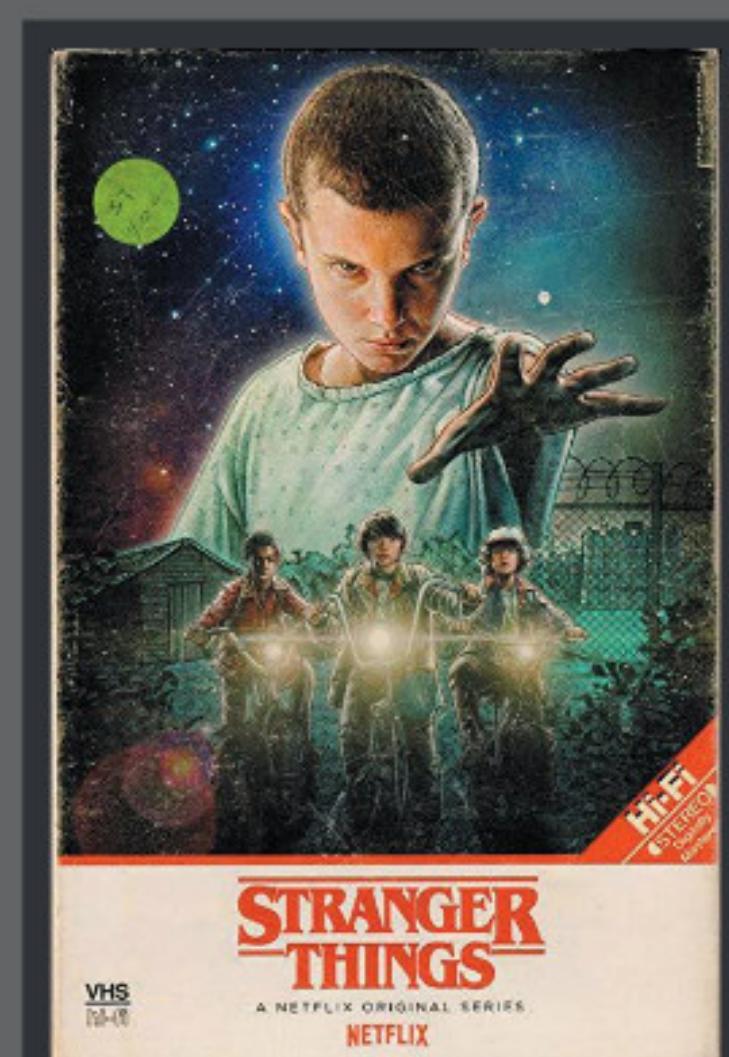
The screenshot shows the YouTube channel page for 'Null Byte'. The channel has 252,359 subscribers. The main video thumbnail is titled 'Hunt down Social Media Accounts with Sherlock' and has 134k views. Other visible thumbnails include 'Launch fireworks remotely with ESP8266 + Arduino', 'Top 10 web browser extensions for Hackers & OSINT...', 'Defend your Mac from Malware & evil maid attacks', and 'Crack Password-Protected Microsoft Office files...'. The sidebar shows various recommended channels like TechnoidFR, Android MT, BLACKBIRD TE..., Monkey Comp..., OUATCH, and Wild in the jard... The top of the page displays a large amount of exploit development code.

YOUTUBE FAIT LA CHASSE AUX HACKERS ?

La plate-forme YouTube a dernièrement changé ses conditions d'utilisation concernant certaines vidéos sensibles. Depuis le 5 avril 2019, il est donc interdit de montrer des vidéos expliquant comment «contourner la sécurité d'un système informatique». C'est ainsi que la chaîne Null Byte spécialisée dans le pentesting s'est vue «striker» une vidéo. Le problème c'est que cette chaîne est réputée pour son contenu pédagogique et rien ne peut les associer à des gens dangereux. Il s'agit bien sûr d'une énième victime des robots de YouTube. Il existe cependant un recours puisque, toujours dans cette même charte, il est précisé que YouTube peut autoriser «la diffusion d'une vidéo contenant des activités prohibées si l'objectif premier est éducatif, documentaire, scientifique ou artistique». Mais à cette heure la vidéo est toujours manquante...

DOWN ↗ NETFLIX SE FAIT PIRATER... DIRECTEMENT À LA SOURCE !

Il est très facile de pirater des vidéos sur Netflix en enregistrant le flux via des moyens détournés (capture et encodage avec une perte de qualité). Dans ce cas la team responsable de la release doit ajouter la mention WEBrip dans le titre. Or une version avec la mention WEB de la dernière saison de Stranger Things en 4K s'est retrouvée sur la Toile. C'est assez étonnant puisque cette mention désigne normalement un fichier brut, sans «rip». Cela signifie qu'il s'agit de fichiers sources directement issus des serveurs de Netflix. On peut donc en déduire que des pirates ont réussi à mettre à casser le mécanisme de chiffrement des contenus 4K de la plate-forme américaine. Le groupe DEFLATE n'en est pas à son coup d'essai puisque plus tôt dans l'année, il avait fait parler de lui avec la fuite en ligne des films de la collection James Bond en 4K d'iTunes.





TOP 10 SITES DE TÉLÉCHARGEMENT ILLÉGAUX



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

1.	Annuaire-Téléchargement	Site de DDL généraliste francophone	=
2.	YggTorrent	Tracker torrent francophone généraliste	+1
3.	Zone-Téléchargement	Site de streaming & DDL francophone	-1
4.	Torrent9	Planet-Streaming	=
5.	Extreme-Down	Site de DDL généraliste francophone	=
6.	LibertyVF	Site de DDL & Streaming francophone	+2
7.	VoirSeries	Site de streaming généraliste francophone	-1
8.	DPStream	Site de streaming généraliste francophone	E
9.	Time2Watch	Site de streaming généraliste francophone	E
10.	Planet-Streaming	Site de streaming généraliste francophone	E

Sources : NetxWarez.com

NOS GUIDES WINDOWS 100% PRATIQUES

POUR UN PC

- + Puissant
- + Beau
- + Pratique
- + Sûr



Chez votre marchand
de journaux



libra

LA CRYPTOMONNAIE DE FACEBOOK



C'est au mois de juin que Facebook a dévoilé Libra, une cryptomonnaie qui devrait être lancée courant 2020. L'omniprésence et la puissance de Facebook poussent à s'interroger sur les conséquences de ce lancement, et ce que cela impliquera pour les utilisateurs.

QU'EST CE QU'UNE CRYPTOMONNAIE ?

Les cryptomonnaies portent beaucoup de noms, pas forcément plus explicites pour le commun des mortels. Cryptoactif, cryptodevise, ou encore monnaie cryptographique, le dénominateur commun reste malgré tout le «crypto» ! Il s'agit en fait de monnaies, utilisables sur un réseau informatique. On parle souvent de «monnaies alternatives», dans la mesure où elles ne sont validées par aucun État. La première, et la plus connue, est le Bitcoin, lancé en 2009.



Ces monnaies utilisent un système de validation, permettant d'éviter les contrefaçons. Elles sont conçues de manière à ce que la création de nouvelles unités de monnaie soit progressive. Cela, associé à un plafond marquant la quantité maximale de monnaie en circulation, permet d'éviter l'hyperinflation.

Contrairement aux monnaies d'état, les cryptomonnaies n'ont pas de contrevaluer physique. Si une monnaie d'état voit sa valeur garantie par son équivalent en or, une cryptomonnaie n'a pas cette assurance. Une exception cependant : le Securiumcoin dont le capital est garanti par un stock... de diamants ! Et bientôt une autre exception, avec Libra, puisque la stabilité de cette monnaie est l'argument phare de Facebook.

Toutes les transactions effectuées avec une cryptomonnaie sont consultables dans le livre des comptes (appelé blockchain) : tout est en principe

transparent, et sécurisé. Malgré cela, certaines cryptomonnaies garantissent l'anonymat de l'utilisateur, comme le Darkcoin ou le Zerocoin.

QUEL INTÉRÊT POUR FACEBOOK ?

Facebook, c'est toute une communauté déjà existante. Avec près de 2,3 milliards de membres actifs, c'est un point de départ idéal pour lancer une cryptomonnaie ! Facebook s'immisce progressivement du côté du commerce en ligne, avec la Marketplace qui brasse déjà énormément de transactions, et donc d'argent. Mais l'intérêt d'une cryptomonnaie, c'est de réussir à la faire adopter par de plus en plus de monde, non seulement des utilisateurs de Facebook, mais aussi des internautes en dehors de ce réseau social.



Si Libra voit le jour, il s'agira d'une monnaie transnationale portée par un groupement d'entreprises privées. Inédit dans l'Histoire...



L'un des objectifs est de permettre aux habitants de pays émergents n'ayant pas la possibilité d'avoir un compte en banque d'avoir néanmoins accès à une monnaie stable et sécurisée. Mais avec des partenaires fondateurs comme Paypal, Uber ou Mastercard, on peut aisément imaginer que Libra vise également l'ensemble de la population connectée. Une monnaie pour les gouverner tous... Si le lancement est réussi (il est prévu pour 2020), et il le sera probablement grâce aux 28 entreprises partenaires, c'est un marché colossal qui s'ouvrira pour Facebook. Malgré la concurrence, la stabilité de Libra garantie par les investisseurs et le nombre d'utilisateurs potentiels (ceux de Facebook, mais aussi WhatsApp et Instagram) peuvent faire la différence, et placer Facebook en leader sur le marché de la cryptomonnaie.

LES AVANTAGES POUR LES UTILISATEURS

Du côté des utilisateurs, tout va être simplifié. Libra pourra être utilisé pour faire des achats en ligne, évidemment, mais aussi pour des paiements «physiques». Le partenariat avec MasterCard et Visa permettra d'utiliser cette monnaie au quotidien, pour s'acheter un café, un ticket de bus, ou à peu près n'importe quoi. Les paiements via Paypal, les abonnements Free ou Spotify : bientôt tout pourra passer par Libra.

Vous voulez envoyer de l'argent à un proche au bout du monde ? Ce sera possible, directement sur WhatsApp. Facebook permet pour l'instant des frais de transactions «bon marché et transparents», attendons néanmoins le lancement de Libra et de Calibra, l'application dédiée, avant de convertir l'ensemble de notre fortune en Libra !

Pour la plupart des gens, la cryptomonnaie reste une chose obscure, et il risque d'y avoir une vraie méfiance au début. C'est le vaste écosystème créé par les partenaires qui pourra inciter le grand public à se lancer et à utiliser Libra. Des utilisations très spécifiques peuvent être trouvées, notamment grâce au paiement de sommes inférieures au centime. Cela pourrait permettre de payer la lecture d'articles en ligne, ou de rémunérer des artistes qui pour l'instant utilisent des systèmes comme Utip ou Kofi. Le paiement en Libra pourrait faciliter les choses, et transformer l'économie des cryptomonnaies.

Au niveau des pays émergents, puisque c'est l'un des arguments phares de Facebook, il a effectivement été constaté que si les gens n'avaient souvent que peu accès à des banques, et à l'ouverture d'un compte, ils ont en

revanche pour la plupart généralement un smartphone dans la poche. Libra et ses partenaires leur permettraient donc d'accéder à de nombreux services, ce qui pourrait changer leur quotidien. D'autres pays sont en grande difficulté à cause de l'hyperinflation (notamment le Venezuela, dont le taux d'inflation est passé à 1.370.000 % en 2018) : leurs habitants pourraient trouver une porte de sortie grâce à Libra.

LES DIFFÉRENCES ENTRE LIBRA ET LES AUTRES CRYPTOMONNAIES

Depuis le lancement du Bitcoin en 2009, le marché des cryptomonnaies prend son envol. Beaucoup ont été lancées très vite, et ont disparu tout aussi rapidement, d'autres ont réussi à se trouver une place assez stable. Malgré tout, ces monnaies qui conservent une aura un peu sulfureuse, sont très en vogue sur le Dark Web, mais peu connues et utilisées par le grand public. Toutes ces cryptomonnaies ont le même défaut cependant : elles ne sont liées à aucune valeur pouvant les stabiliser. La conséquence ? Des fluctuations extrêmes, et des monnaies dont la valeur triple en un jour, ou s'effondre en quelques heures. Le bitcoin a déjà dépassé les 19 000\$, avant de retomber rapidement, et de rester aux alentours de 9 000\$. Difficile de faire confiance à une cryptomonnaie dans ces circonstances, non ?

C'est sur ce point que Facebook entend faire la différence, avec l'aide de ses partenaires. Libra sera gérée par une fondation à but non lucratif, composée des entreprises partenaires. Pour éviter les fluctuations, et proposer une monnaie ayant un cours stable, la fondation adossera en titres gouvernementaux ou en devises l'équivalent de chaque achat de Libra.

Outre cette stabilité pratiquement garantie, c'est le nombre de partenaires qui fera sûrement la différence. Alors que jusqu'à présent les cryptomonnaies pouvaient surtout être utilisées en ligne (qui va payer son journal en Bitcoin ?), le fait d'avoir pour partenaires des mastodontes du paiement (Visa, Mastercard...) devrait permettre de démocratiser rapidement le paiement physique en Libra. Si en Europe les commerçants peuvent accepter tout paiement dans une monnaie autre que l'Euro, ils pourraient néanmoins voir un avantage certain à cette monnaie dématérialisée. À une condition peut-être ! Que ce nouveau système de paiement n'engendre pas de frais supplémentaires pour eux. Si Facebook et ses partenaires réussissent à mettre cela en place, ça pourrait bien être le jackpot...



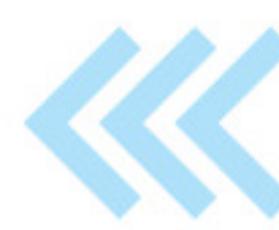


LES DANGERS DE LIBRA

Les promesses sont belles, les objectifs paraissent louables, et «fondation à but non lucratif», ça sonne bien. Malgré tout, certains tirent déjà la sonnette d'alarme, imaginant les dérives possibles d'une telle monnaie, entre les mains d'une puissance telle que Facebook. L'utilité d'un réseau social, tout comme celle d'une monnaie, augmente en même temps que le nombre d'utilisateurs. Si l'on peut se passer d'un réseau social même si tout son entourage est inscrit dessus (et le peut-on réellement ?), il n'en sera pas forcément de même pour une monnaie. Si l'usage se démocratise, et que Libra prend de l'ampleur, ce qui sera probablement le cas, puisqu'on peut faire confiance à Facebook pour en rendre l'usage facile et ludique, il deviendra difficile de s'en passer.

Derrière l'objectif louable d'aider les personnes sans compte en banque à accéder à une monnaie internationale, on retrouve malgré tout une fondation composée d'entreprises privées. Entreprises qui, soyons honnêtes, ont plutôt tendance à favoriser leur profit que la résolution de problèmes mondiaux. Est-il vraiment judicieux de leur confier une énorme part de l'économie ? Chaque transaction se verra ponctionnée d'une fraction de son montant, générant du profit allant directement dans les poches des entreprises privées. C'est le cas pour tous les paiements électroniques, bien sûr, mais c'est toujours bon de garder cela en tête.

Autre point sur lequel il serait bon de s'interroger : les libertés individuelles et la vie privée. On le sait, on vit avec : nos moindre faits et gestes sur internet peuvent être traqués, nos paiements



Pour éviter l'instabilité et les fluctuations, Libra sera gérée par une fondation à but non lucratif qui adossera en titres gouvernementaux ou en devises l'équivalent de chaque achat de Libra.

par carte bancaire également, et ne parlons pas de l'utilisation de nos smartphones... Avec Libra, et Calibra, l'application associée, c'est l'ensemble de notre vie, finances comprises, qui pourra être observé. Quelles garanties avons-nous concernant la protection de nos données? Quelles garanties avons-nous que l'usage de cette monnaie ne sera pas contrôlé, que notre portefeuille ne se trouvera pas bloqué un jour, en raison d'une action effectuée sur Facebook ou d'une photo postée sur Instagram ? Libra sera basée sur une blockchain fermée, dont le fonctionnement ne dépendra que des membres de la fondation. Tout cela sera basé sur un nouveau langage de programmation, développé par Facebook, ce qui est bien éloigné d'une démarche d'open source, et peut alimenter les soupçons concernant un potentiel contrôle de la monnaie, voire une censure. La monnaie sera limitée aux entreprises partenaires : cela risque de créer un écosystème économique dont l'utilisateur sera captif. Libra rendra facile les achats dans les entreprises partenaires, donc l'utilisateur ne verra pas l'intérêt d'aller à la concurrence, et restera dans cet écosystème. Quelqu'un de pessimiste dirait que ce que nous gagnerons en simplicité et rapidité, nous le perdrons en liberté et libre arbitre.





CHEZ SFR, LE FEMTOCELL VA À LA POUBELLE !

Le service Femtocell de SFR met la clé sous la porte. Que va-t-il advenir de tous les campagnards qui misent sur cette fonctionnalité pour avoir des communications téléphoniques «normales»? Le VoWiFi semble prometteur, mais tout le monde n'est pas logé à la même enseigne...

On l'oublie parfois, mais il existe encore des endroits en France où l'on capte très mal, voire pas du tout, avec un téléphone portable. Pour les personnes qui souhaitent être jointes sur leur smartphone chez eux, il existe les boîtiers Femtocell, loués par votre opérateur Internet. Ces derniers permettent de créer un point d'accès 3G/4G à la maison pour pouvoir appeler depuis son portable si votre domicile est dans une zone pas ou peu couverte. Les trois opérateurs historiques proposent ce genre d'option, mais dernièrement les abonnés SFR ont reçu un e-mail indiquant que la compagnie allait mettre un terme au service Femtocell dans les «prochaines semaines», car il est devenu «obsolète». Déjà merci pour la date très précise, ça fait toujours plaisir.

LE VOWIFI, UNE SOLUTION DE REMplacement ?

Votre fidèle serviteur, abonné chez SFR depuis 2008 et habitant dans un village de 502 habitants, a fait un bond de 2 mètres en apprenant la nouvelle, mais comme il est écrit que la technologie est obsolète, ils ont forcément une solution de remplacement chez SFR, hein? Après avoir appelé le service client au 1023, le soufflé est retombé. Pourtant le gentil monsieur au téléphone (ils sont souvent gentils chez SFR) lui explique que «*Oui, il y a une solution : les appels WiFi!*». Appelé aussi VoWiFi (pour Voice over WiFi), il s'agit en fait d'utiliser le WiFi à la place

de la 4G pour faire passer le signal vocal. Parfait! Sauf que non. Le gentil monsieur ne trouve pas le modèle de mon smartphone dans sa liste. Forcément c'est un vieux modèle! Eh bien non. C'est un OnePlus 6 sous Android 9. Idem pour le Xiaomi Mi A2 Lite de Madame. Ça lui semble bizarre à Tarik (le gentil monsieur) et il cherche de plus belle, mais non. La réponse est sans appel : il faudra «attendre que le fabricant fasse une mise à jour, car vos appareils ne sont pas compatibles». Sur la liste de Tarik, il n'y avait que des appareils sous Android 8 «Oreo» (avec les explications à donner aux clients pour activer le VoWiFi), mais rien avec Android 9 «Pie». Même si chez Bouygues ou Orange, rien ne dit que les boîtiers Femtocell vont tirer leur révérence, sachez que la liste des compatibilités est encore plus mince avec seulement les appareils d'Apple, les smartphones haut de gamme Samsung et quelques Sony... De plus, il apparaît que certains appareils ne sont compatibles que s'ils ont été achetés chez un opérateur particulier, avec un «carrier» bien spécifique. Pour être clair, votre Samsung Galaxy S10 peut être compatible...si vous l'avez acheté chez SFR. Parfois ce n'est pas nécessaire, mais rien n'est mentionné sur la liste de compatibilité et inutile de demander, les téléconseillers ne sont absolument pas au courant et tombent parfois des nues quand on leur parle de VoWiFi...





Hey les gars, vous savez, cette technologie gratuite et fonctionnelle qui vous sauvait la mise... Et bien, on l'arrête. Voilà. Merci d'avoir choisi SFR sinon hein...

Interview d'un responsable de la communication chez SFR

Nous avons donc contacté le service communication de SFR pour avoir plus de détails et jauger les alternatives proposées par le fournisseur. Après avoir compris que nous ne travaillions pas pour Le Journal de Mickey, la personne qui nous a répondu a désiré voir son nom rayé des tablettes. Le responsable communication a préféré ne pas communiquer donc... Applaudissons son courage !

JE SUIS ABONNÉ SFR ET DÉBUT JANVIER J'AI REÇU UN E-MAIL POUR ME DIRE QUE LE SERVICE FEMTO ÉTAIT «OBSOLÈTE» ET QU'IL ALLAIT S'ARRÊTER "DANS LES PROCHAINES SEMAINES" ? Y A-T-IL UNE DATE PLUS PRÉCISE ? CERTAINS DE NOS LECTEURS NOUS ONT DIT QUE LE SERVICE ÉTAIT ARRÊTÉ DEPUIS LONGTEMPS CHEZ EUX. IL Y A UN ARRÊT PROGRESSIF ?

La coupure se fera de façon progressive sur le premier semestre 2019. Les clients seront avertis à minima un mois à l'avance par téléphone ou par SMS avant leur coupure.

J'HABITE À LA CAMPAGNE ALORS JE SOUHAITAIS SAVOIR SI SFR AVAIT UNE SOLUTION DE REMplacement. J'AI COMPOSÉ LE 1023 ET LE MONSIEUR AU BOUT DU FIL M'A PARLÉ DES APPELS WIFI (OU VOWIFI). IL A DEMANDÉ MON MODÈLE DE TÉLÉPHONE, MAIS POUR LE ONEPLUS 6 (LE MIEN) OU LE XIAOMI MI A2 LITE (CELUI DE MA FEMME), IL N'AVAIT PAS DE TUTO. NOUS AVONS CHERCHÉ L'OPTION ENSEMBLE, MAIS EN VAIN. NOTEZ QUE LES DEUX APPAREILS SONT SOUS LA DERNIÈRE VERSION D'ANDROID ET SONT PLUTÔT RÉCENTS. Y A-T-IL UNE LISTE DE SMARTPHONES COMPATIBLES MISE À JOUR ?

La liste est dans «**Comment en bénéficier**» à cette adresse : <https://frama.link/4z2WoLHz>. Il y a des tutos par marque. Pour votre information 94 terminaux sont actuellement compatibles avec les appels WiFi chez SFR ! [Au 19 avril 2019, NDLR]

EN REGARDANT SUR INTERNET J'AI VU QUE LES SMARTPHONES ACHEtÉS CHEZ SFR (ET DONC AVEC

UNE ROM SFR) ONT PLUS DE CHANCE D'ÊTRE COMPATIBLES AVEC CE VOWIFI. EST-CE VRAI ?

Oui pour les systèmes Android, pour iOS d'Apple, ils le deviennent, quelle que soit l'origine.

QUELLE SOLUTION DE REPLI SFR PROPOSE-T-IL AUX CLIENTS QUI N'ONT PAS D'APPAREILS COMPATIBLES ET QUI AIMERAIENT QUAND MÊME TÉLÉPONER DEPUIS LEUR DOMICILE ?

En cas de mobile non compatible, SFR proposera aux clients un renouvellement de mobile avantageux.

OUI MAIS ALORS LES CLIENTS SFR QUI N'ONT PAS DE SMARTPHONES ESTAMPILLÉS SFR SE RETROUVENT DONC POUR L'INSTANT SANS SOLUTION ? Comme je vous le disais, les appareils sous iOS deviennent compatibles avec la VoWiFi de SFR quelle que soit l'origine tandis que pour Android cela dépend du modèle.

Nous vous confirmons donc que SFR va supprimer un service qui fonctionne avec 100% des téléphones pour une solution pour le moins «incertaine». Entre les smartphones Xiaomi et OnePlus qui sont clairement mis à l'écart et ceux qui sont compatibles, mais qui nécessitent la surcouche SFR, nous sommes loin d'une solution de remplacement pérenne.
Espérons que les fabricants vont proposer des mises à jour rendant compatibles leurs appareils avec les appels WiFi. Pour l'instant, ils ne sont pas pressés.



Les réseaux sociaux au service des assureurs ?

C'est un problème que nous connaissons tous : nous diffusons trop d'informations personnelles sur les réseaux sociaux. Déplacements, habitudes alimentaires, rencontres, voyages... C'est pratiquement notre vie entière qui peut être reconstituée, grâce aux messages et aux photos postés sur Facebook, Twitter, Instagram, Snapchat et les autres. Mais que risquons-nous vraiment ? Les assureurs et les banquiers peuvent-ils nous espionner par ce biais, et utiliser ces informations ?

AUX ÉTATS-UNIS, UNE LOI QUI FAIT FROID DANS LE DOS

C'est dans l'État de New York qu'une loi est sur le point de passer, autorisant les assureurs à utiliser les réseaux sociaux pour calculer les droits et cotisations de leurs clients. L'objectif ? Récupérer un maximum d'informations sur chaque client, pour évaluer les risques, et fixer leurs tarifs en conséquence. Vous postezi sur Instagram un selfie vous montrant à la terrasse d'un fast-food, cigarette à la main ? Vous donnez ainsi deux raisons à votre assureur

d'augmenter vos cotisations, puisque vous affichez deux comportements mauvais pour votre santé. Cette loi est proposée pour imposer un cadre légal aux entreprises qui agissent déjà de cette manière, mais elle risque de pénaliser les utilisateurs au lieu de les protéger. D'autant que certains assureurs pourraient aller plus loin ! Dans le cadre de cette loi, ils pourraient être autorisés à analyser le contenu de votre téléphone, pour établir votre profil en analysant votre comportement. Vous commandez des repas sains et bio, vous utilisez une appli de fitness, et êtes souvent géolocalisé à la salle de sport ? Bravo, vous êtes un bon assuré, vos cotisations ne seront pas impactées. Adieu vie privée, bonjour Big Brother. Cette loi en cours de validation aux États-Unis pourrait bien donner des idées aux assureurs et banquiers français. Des risques mieux évalués signifient pour eux moins de danger financier, et donc plus de profit. En France, aucune loi n'encadre pour l'instant ces pratiques, et aucune société n'a pour l'instant été pointée du doigt pour usage abusif de données personnelles. Mais cela ne signifie pas pour autant que nos données ne sont pas collectées et utilisées... discrètement.

LES OBJETS CONNECTÉS : DES PETITS ESPIONS À VOS CÔTÉS

Votre tension. Votre poids. Votre taux de cholestérol. Ce sont des informations que vous ne divulguez pas, qui sont confidentielles, et vous souhaitez qu'elles le restent ! Mais le sont-elles vraiment ? Si vous portez une montre connectée, si vous utilisez une appli pour faire du sport, si votre balance est connectée à votre Wifi, toutes les données qu'elles contiennent peuvent potentiellement échapper à votre contrôle.



Impossible ? Malheureusement, non... En parcourant Facebook, il est fréquent de voir des messages de type «J'ai parcouru 5KM en 40 minutes, avec l'application FitnessImpact !». Ces messages sont automatiques : ils sont envoyés par l'application, directement sur votre profil Facebook, sans que vous ne l'ayez choisi. Enfin soyons honnêtes : vous l'avez choisi. Si, si, en validant les autorisations demandées à l'installation de l'application ! Tout ce qu'on valide sans vraiment le lire, parce que sans validation, impossible d'installer l'application. Alors vos informations se retrouvent non seulement sur votre smartphone, mais aussi potentiellement sur les réseaux sociaux, généralement partagées en mode public. Et hop, tout le monde a accès à votre rythme cardiaque, aux calories brûlées, à votre vitesse de courses... Autant d'informations qui peuvent en dire long sur votre état de santé. Tous ces éléments pourraient permettre à votre assurance, ou à votre banquier dans le cas d'un prêt, d'ajuster de manière extrêmement précise le montant de vos cotisations. Tant que vous êtes en bonne santé, vous payez un prix abordable, mais si subitement vous faites de l'hypertension, si vous abandonnez le sport, ou passez en surpoids vous pourriez voir votre contrat modifié. Si cela n'a pas l'air d'être une pratique fréquente en France, il n'en reste pas moins que nos données, parfois particulièrement sensibles, peuvent rapidement et facilement tomber entre de mauvaises mains, et impacter notre vie parfois à notre insu.

DES EMPLOYEURS PEU SCRUPULEUX

Les assureurs et les banquiers ne sont pas les seuls à pouvoir exploiter les réseaux sociaux pour garder un œil sur vous. Certains employeurs traquent leurs salariés en ligne, pour vérifier que personne ne profite d'un arrêt maladie pour aller faire du surf,

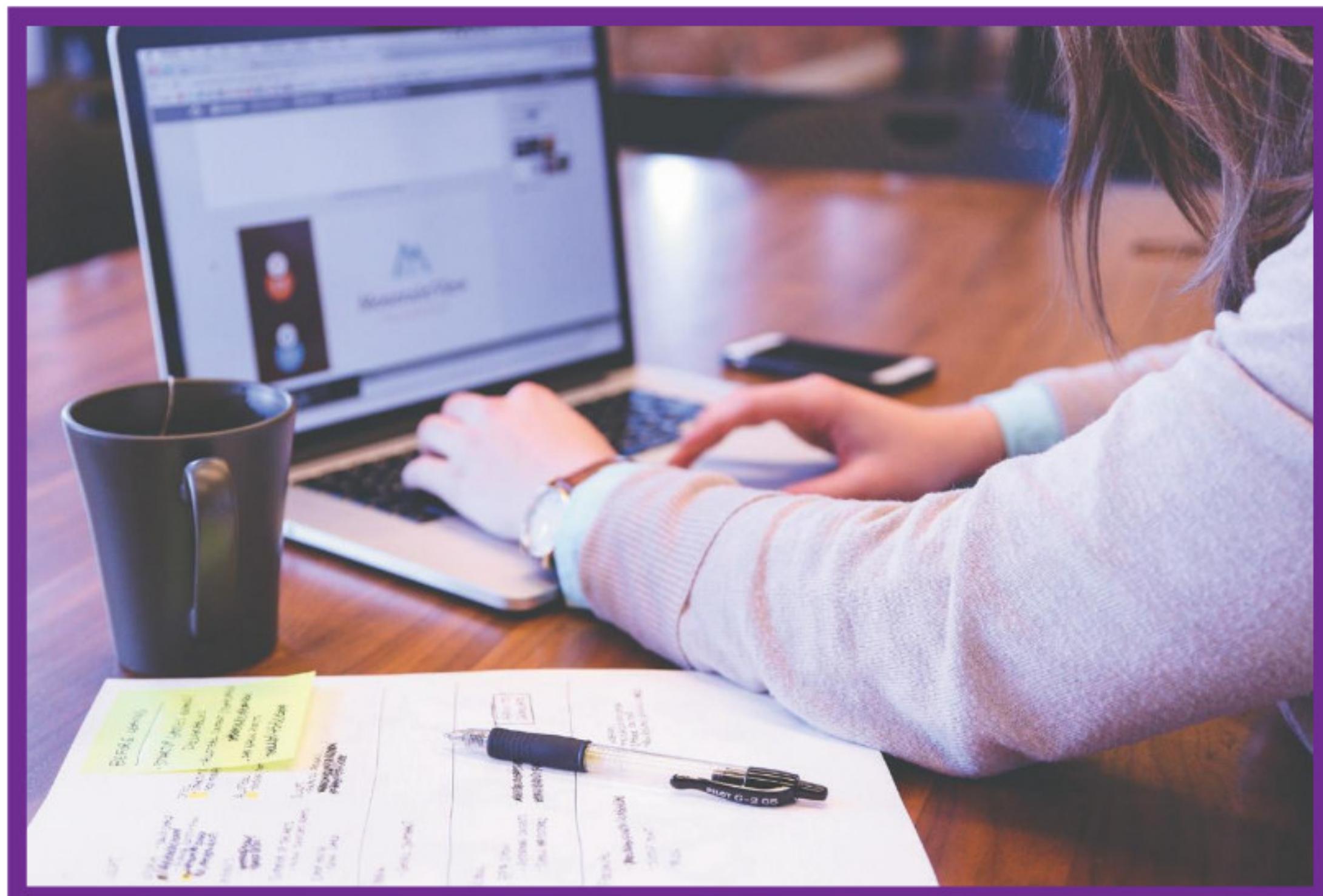


ou pour s'assurer que vous ne dénigrez pas votre entreprise en public. Si vous n'enfreignez pas la loi (pas d'injure publique, de diffamation, d'incitation à la haine, de discrimination), un employeur n'a pas le droit, légalement, de vous licencier pour des propos tenus sur internet. Malgré tout, il pourra trouver un autre prétexte pour le faire, il faut donc rester particulièrement vigilant à ce que vous publiez. Si votre profil est privé, votre employeur ne pourra vous reprocher vos propos, qui relèvent de la correspondance privée (ce qui peut être invalidé néanmoins si vous avez un très grand nombre de contacts sur ce réseau social : s'adresser à 3000 personnes s'apparente plus à une prise de parole publique qu'à une correspondance privée). De la même manière, des informations liées à votre vie quotidienne (sorties pendant un arrêt maladie entre autre) ne peuvent théoriquement pas être utilisées contre vous. Attention toutefois : si un employeur constate via une publication sur un réseau social que vous ne semblez pas respecter les termes de votre arrêt maladie, il peut, sans avoir à se justifier,

demander à la sécurité sociale d'effectuer un contrôle.

Alors faut-il bannir les réseaux sociaux de notre quotidien ? Ce serait difficilement possible en l'état actuel des choses. Mais la prochaine révolution informatique pourrait bien être liée à la protection des données personnelles.

Nous prenons tous peu à peu conscience que nos données sont éparpillées aux quatre vents, et que des entreprises les utilisent sans complexe. À nous de devenir plus vigilants, et plus exigeants sur les garanties offertes par les différentes applications pour protéger notre vie privée !



« Imiter n'importe qui pour lui faire dire et faire n'importe quoi ». Non, ce n'est pas la nouvelle punchline de Rémy Gaillard, mais le sous-titrage implicite de toute vidéo « deepfake ». Sortez les popcorns et préparez-vous aux turbulences.

DEEPFAKES : L'INVASION A COMMENCÉ

Début 2019, Paul Scharre, du Centre pour une Nouvelle Sécurité Américaine, s'alarmait : « Au cours des deux prochaines années, nous verrons des vidéos truquées jouer un rôle dans les campagnes politiques aux États-Unis ou en Europe (...) pour essayer d'influencer ou de salir les candidats, et ce sera un défi pour les démocraties. »

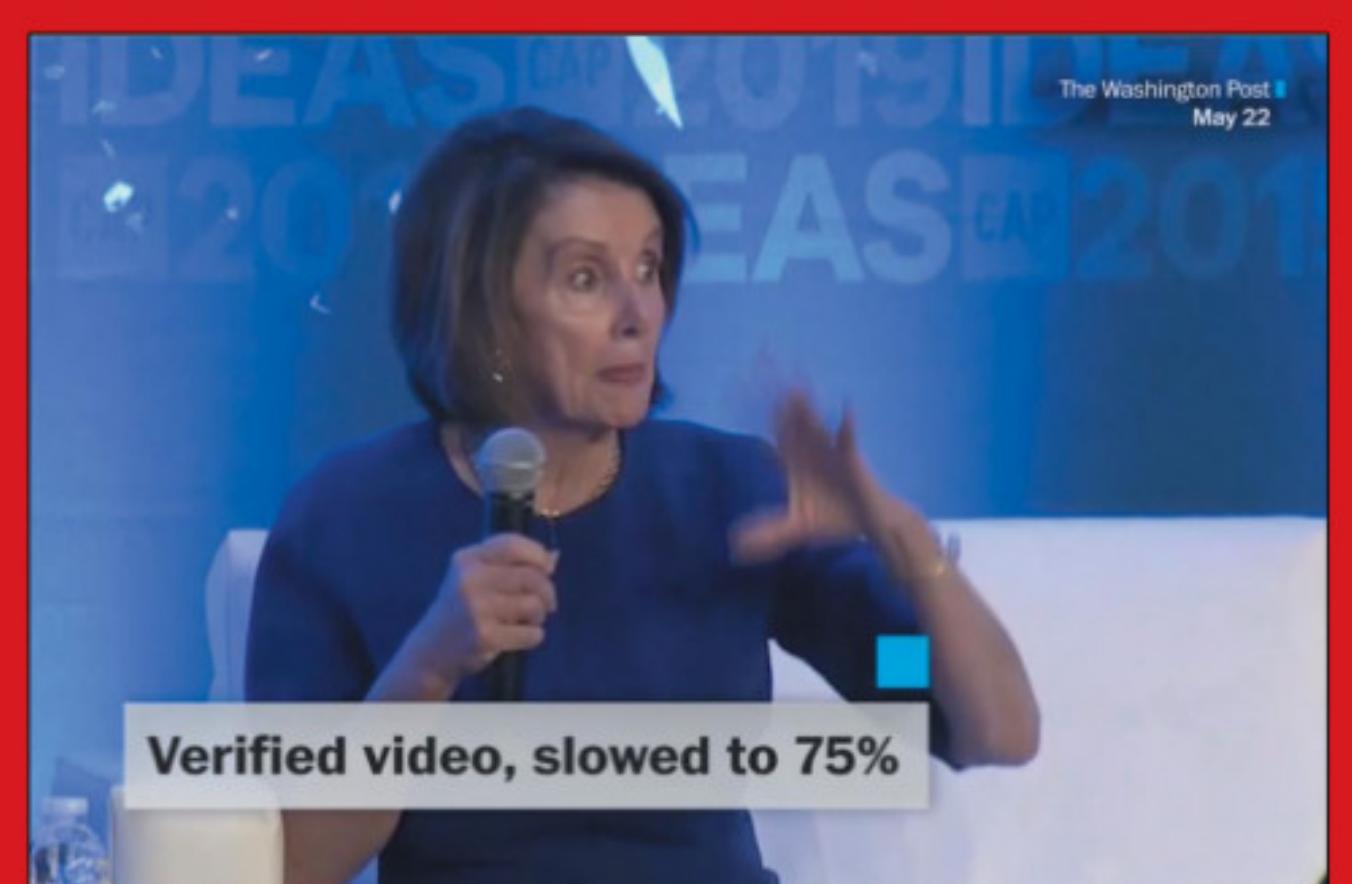
DEEP LEARNING ET FAKE NEWS

Pourquoi « Deepfake » et quelles différences avec les effets spéciaux utilisés par l'industrie du cinéma ? Fake pour « Faux », comme une Fake News. Deep comme « Deep learning », une expression consacrée qui résume le travail de certaines intelligences artificielles (IA) apprenant de leurs erreurs



CHEAPFAKE : LA DEEPFAKE DU PAUVRE

Pas besoin de vidéos ultra travaillées à coup d'intelligence artificielle pour tromper son monde. À côté des Deepfakes, il y a les « cheapfake », des vidéos bidouillées en amateur mais qui démontrent qu'il ne faut pas forcément des dizaines d'ingénieurs en effets spéciaux pour obtenir un impact délétère. Ici, une vidéo trafiquée de mai 2019 fait apparaître Nancy Pelosi (farouche opposante à Trump) comme une femme ivre et à l'élocution douteuse. En fait, le débit est simplement ralenti et quelques astuces de montage utilisées. En 48h, les Républicains ont relayé l'info sans se poser de questions et des millions d'Américains ont été trompés par les moeurs scandaleux de cette alcoolique de Pelosi ! Certains en sont toujours persuadés...





EN 2018, LE GRAND PUBLIC DÉCOUVRAIT BARACK OBAMA TRAITANT SON SUCCESEUR, DONALD TRUMP, « D'IDIOT TOTAL ET ABSOLU » DANS UNE VIDÉO DE QUELQUES MINUTES... AVANT QUE LA SUPERCHERIE NE SOIT LEVÉE À LA FIN, LORSQU' APPARAÎT LE COMÉDIEN JORDAN PEELE, DONT LES MOUVEMENTS FACIAUX ÉTAIENT CALQUÉS SUR LE VISAGE DE BARACK OBAMA.

en utilisant des schémas de confrontation/sélection ultra-rapides grâce à des algorithmes utilisant notre architecture d'apprentissage neuronale. Plus les puissances de calcul sont importantes, plus ces « cerveaux » sont en mesure de traiter rapidement des quantités faramineuses de données.

Hier, il fallait des équipes entières, du travail collaboratif, beaucoup de temps et d'argent pour réaliser des trucages qualitatifs. Aujourd'hui, grâce aux IA et programmes en open source, une journée peut suffire à un mec seul au fond de son garage pour bidouiller une deepfake de qualité moyenne mais qui aura son petit effet. Avec 10 mecs seulement et une petite semaine de boulot, on arrive à des résultats absolument bluffants.

LA SYNTHÈSE VOCALE SUIT LA CADENCE

Et ces vidéos truquées vont se perfectionner avec le temps. D'autant que la recherche progresse également sur l'analyse et la synthèse de la voix. Des outils gratuits comme Lyrebird ambitionnent déjà de reproduire à l'identique votre voix après l'avoir écoutée seulement une minute !

L'approche la plus connue pour réaliser une deepfake est la substitution d'un visage à un autre et son animation la plus parfaite possible. Il faut prendre une personne qui ressemble un peu à la cible si possible et la filmer sous différents angles et éclairages en lui demandant de faire de expressions faciales variées. Le programme se servira de cette base pour animer artificiellement le « vrai visage » de la cible en suivant l'animation de référence du complice.

Mais la plus ambitieuse est bien sûr la synthèse intégrale de visages, de discours et d'actions. Pour animer un visage, il faut avoir accès à plusieurs milliers de clichés d'une personne, sous des angles différents. Souvent, la collecte image par image d'une vidéo peut suffire.

Si la perspective de voir des dizaines de fausses vidéos polluer chaque semaine le débat public est angoissant, certains rappellent que les mêmes inquiétudes sont apparues avec la démocratisation de Photoshop et de programmes open source similaires au début des années 2000. Les citoyens s'adapteront, apprendront à développer davantage leur critique de l'image et ne se feront pas si facilement berner prédisez certains. Mouais...

Le problème, et nous l'avons vu avec les fake news qui pourrissent les réseaux sociaux, c'est qu'elles hystérisent le débat en permanence, provoquent des émotions puissantes, deviennent virales avant d'être démenties, etc. En bref, il faut 10 secondes

pour que notre cerveau soit durablement imprégné d'une émotion déclenchant un avis ou une prise de position tranchée. Et combien de temps faut-il pour les déconstruire avec le seul recours à notre froide raison, une fois que l'on sait que la source de cette émotion était falsifiée ?

INTELLIGENCE ARTIFICIELLE VS BÊTISE ORDINAIRE

Le verbe est un puissant déclencheur d'émotions. On monte d'un cran avec une image choc. La vidéo balaie nos défenses naturelles encore plus facilement. De nombreux humains se fichent d'ailleurs d'être contredits par les faits : « Ok, cette vidéo est fausse mais ce que j'ai ressenti correspond à mes convictions, cela "pourrait être vrai" d'ailleurs, je n'ai pas envie de remettre en question mon mode de pensée même si vous m'amenez 20 démonstrations à analyser. Je m'en tiens aux 3 arguments et 2 fausses vidéos qui confortent mon idée. Et pis c'est tout ! »

La vidéo balaie nos défenses naturelles encore plus facilement

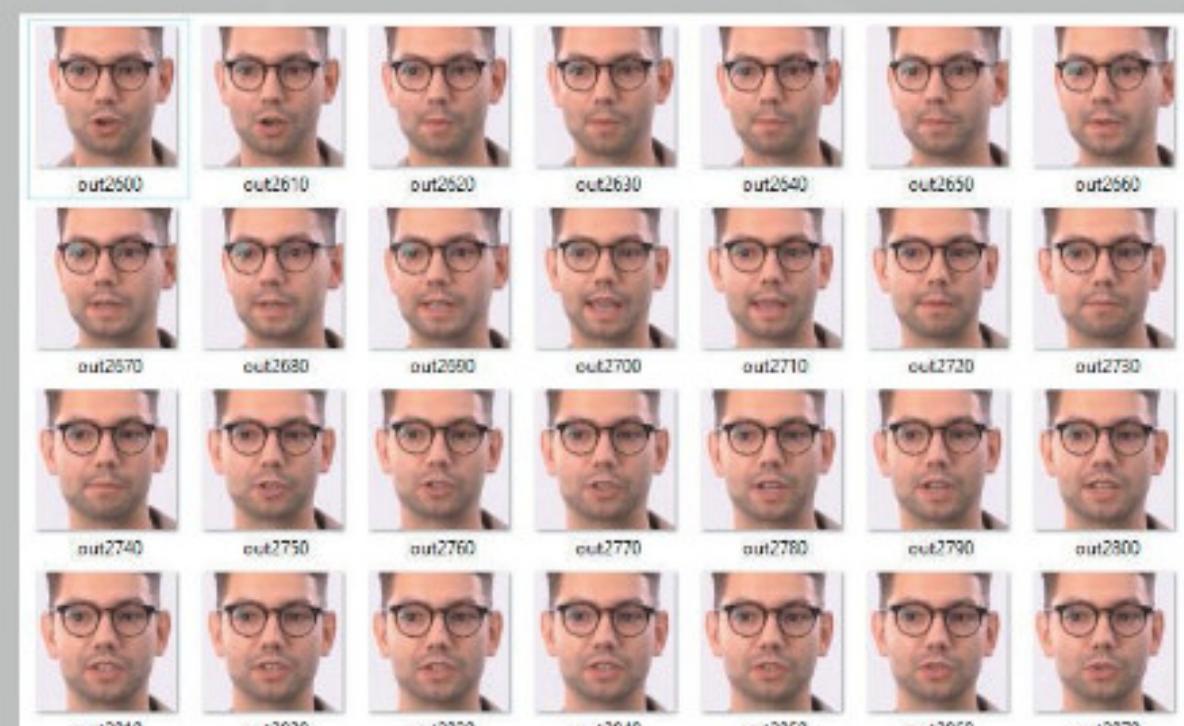
Rappelez-vous de Sean Spicer, le premier porte-parole de la Maison-Blanche sous l'ère Donald Trump. Il avait déclaré en janvier 2017, après l'investiture de ce dernier : « Jamais plus grande foule n'avait assisté à une investiture, point final ». Quelques photos présentées avec des angles avantageux ont suffi à appuyer son discours. Bien sûr, cela était faux. Des dizaines d'autres photos et statistiques ont pu prouver le contraire. Kellyanne Conway, l'ex-directrice de campagne de Donald Trump n'a pu s'empêcher de défendre son président et Sean Spicer : « Ce n'est pas un mensonge, Sean Spicer a présenté « des faits alternatifs », a-t-elle affirmé avec assurance. Donc préparez-vous à de nombreux échanges qui vous expliqueront qu'une fausse vidéo n'est pas vraiment une fausse vidéo mais un « fait alternatif ». Et ça, ce sera dans le meilleur des cas, celui où l'on aura prouver à temps la falsification d'un contenu. Car ces satanés IA progressent à une vitesse démentielle. Bienvenus dans l'ère du doute et de la confusion permanente.

» TOP 5 DES PROGRAMMES STARS DE LA NÉBULEUSE DEEPFAKE

Chacun propose une approche différente, tous sont aujourd'hui incontournables sur la scène du DeepFake.

> FAKEAPP, L'OUTIL ACCESSIBLE À TOUS

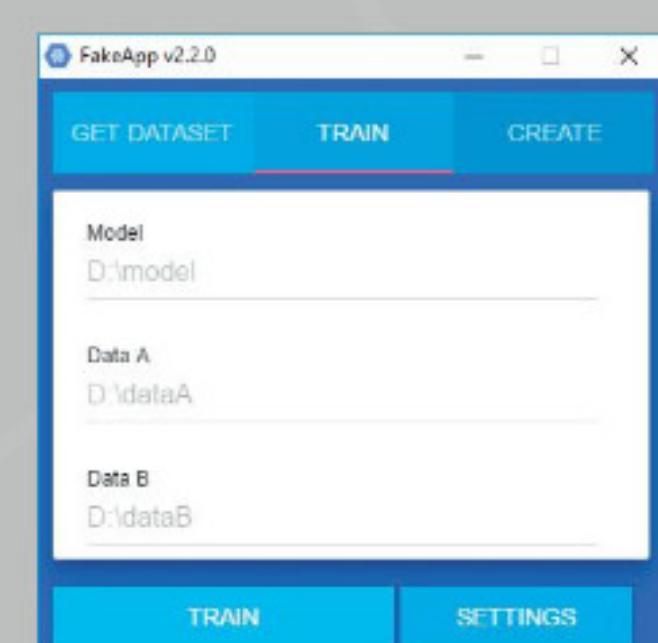
C'est le logiciel grand public le plus utilisé, gratuit et assez simple à prendre en main. Son but est d'effectuer un « face swap » sur une vidéo, mouvements du visage et des lèvres inclus bien sûr pour un rendu le plus réaliste possible. De bonnes connaissances en informatique (mais sans plus) et surtout un ordinateur puissant suffisent.



COMMENT ÇA MARCHE?

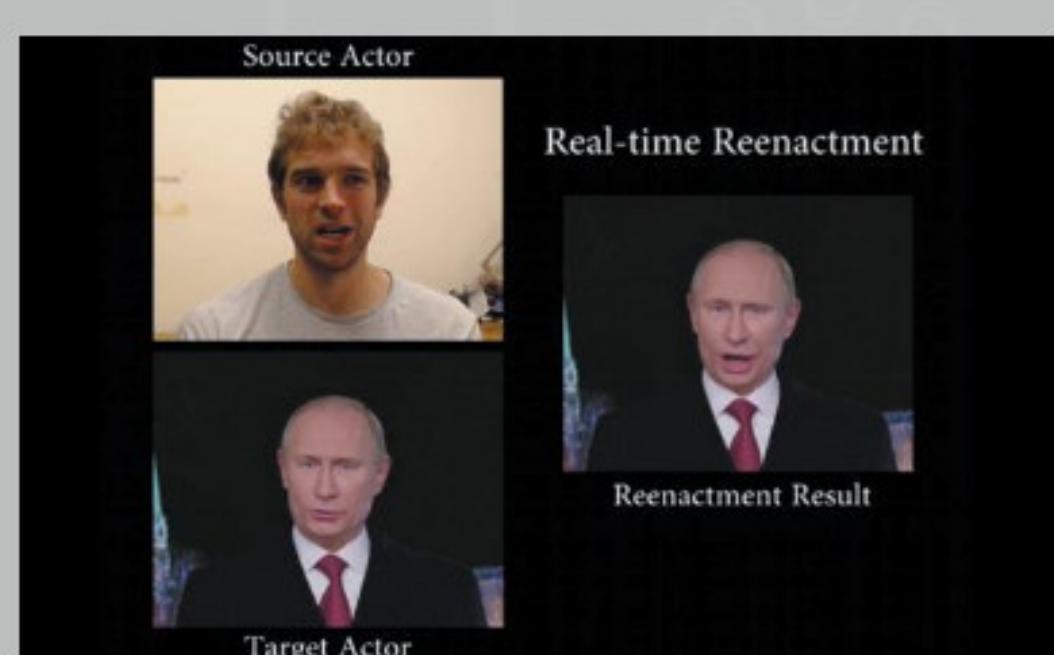
Pour entraîner FakeApp, l'utilisateur doit le nourrir avec des centaines (des milliers, c'est mieux) d'images d'un personnage A (la cible) et d'un personnage B (celui dont le visage sera appliqué). Il est possible d'importer des bases de données ou aussi des vidéos qui seront utilisées par FakeApp pour extraire ces images frame par frame.

Le programme va ensuite mettre en compétition ces bases A et B grâce à l'apprentissage en réseau neuronal, jusqu'à ce qu'un résultat probant soit obtenu (le logiciel indique qu'un taux d'erreur de 0,02 % est acceptable). Il suffit d'appuyer ensuite sur « Create » pour lancer la production de la vidéo truquée.



> FACE2FACE : LA LÉGENDE DU TRUCAGE EN TEMPS RÉEL

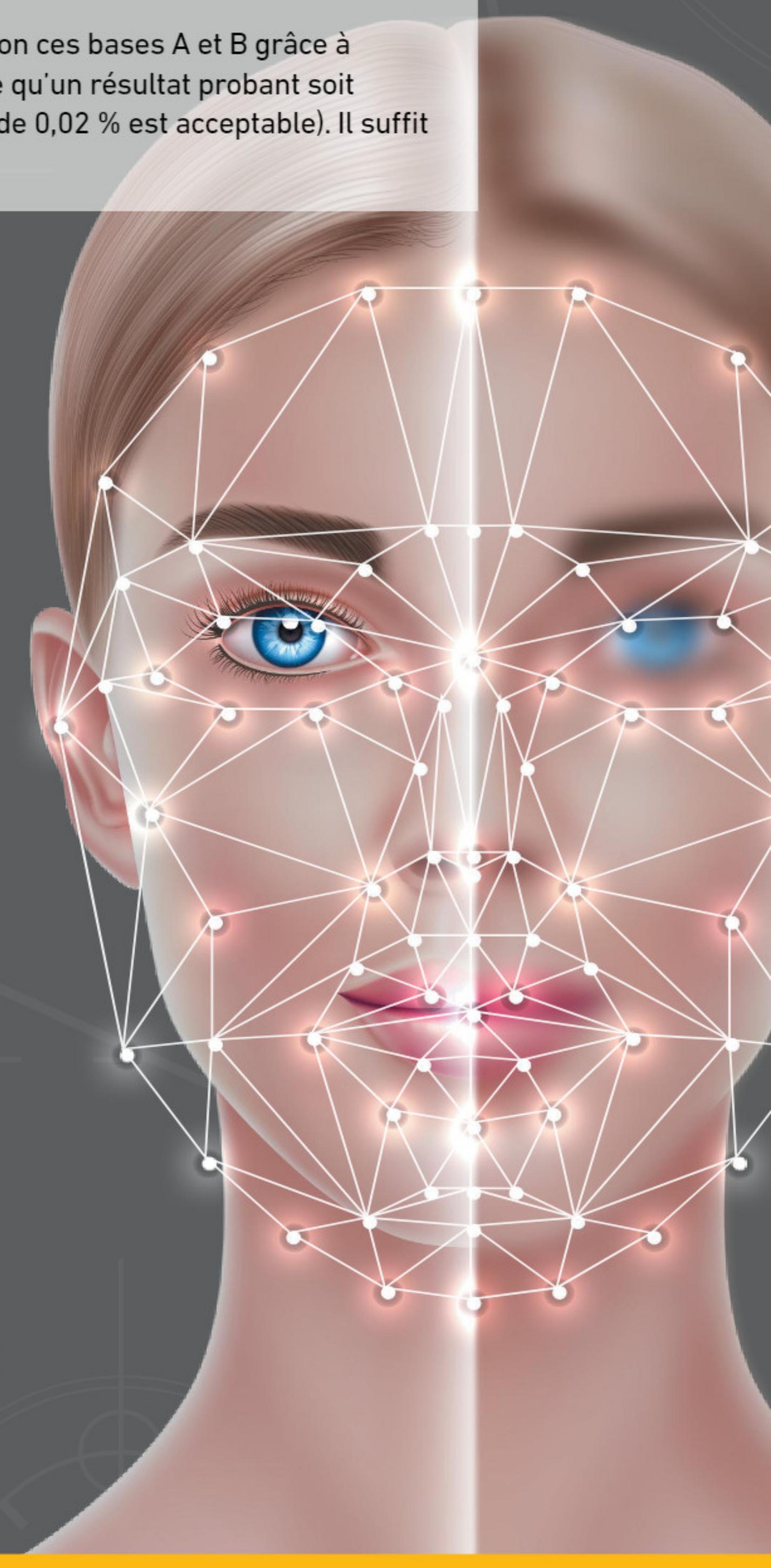
C'est l'application pionnière et celle qui fait encore fantasmer les experts. Imaginez, dès 2016, une équipe de chercheurs allemands faisait la démonstration d'un trucage encore inégalé. Pendant qu'ils filmaient un comédien, les mouvements du visage de ce dernier se calquaient en temps réel et avec un réalisme bluffant sur le visage d'un autre personnage sur une vidéo B... et en utilisant une simple webcam !



COMMENT ÇA MARCHE ?

Personne ne le sait vraiment. Au point même que des doutes subsistent quant à la réalité de la prouesse accomplie à l'époque. L'équipe de chercheurs allemands, menée par Matthias Niessner, n'a pas publié le code source de son programme et ne communique plus sur le sujet. Temps réel, pas de collecte de données,

réalisme du rendu, facilité d'utilisation : si Vincent Nozick, créateur de Mesonet - un détecteur de Deepfakes - trouve cet exploit « génial », il le qualifie aussi de « méga flippant ». Dans un interview accordé en juin dernier à Technikart, le chercheur explique qui plus est que sa « méthode de détection ne fonctionne pas avec Face2Face, donc elle est déjà dépassée. Là où je m'interroge, c'est que les Allemands n'ont pas mis leur logiciel en accès libre comme d'autres l'ont fait. Soit ils se sont rendu compte de sa dangerosité, soit ils l'ont vendu. Cela peut représenter plus de 100 fois la dotation annuelle de leur laboratoire, c'est inestimable. »



000000005658655656
0000000000025658795 589476
45540000000000 00000025136

> TENSORFLOW, BRIQUE ESSENTIELLE

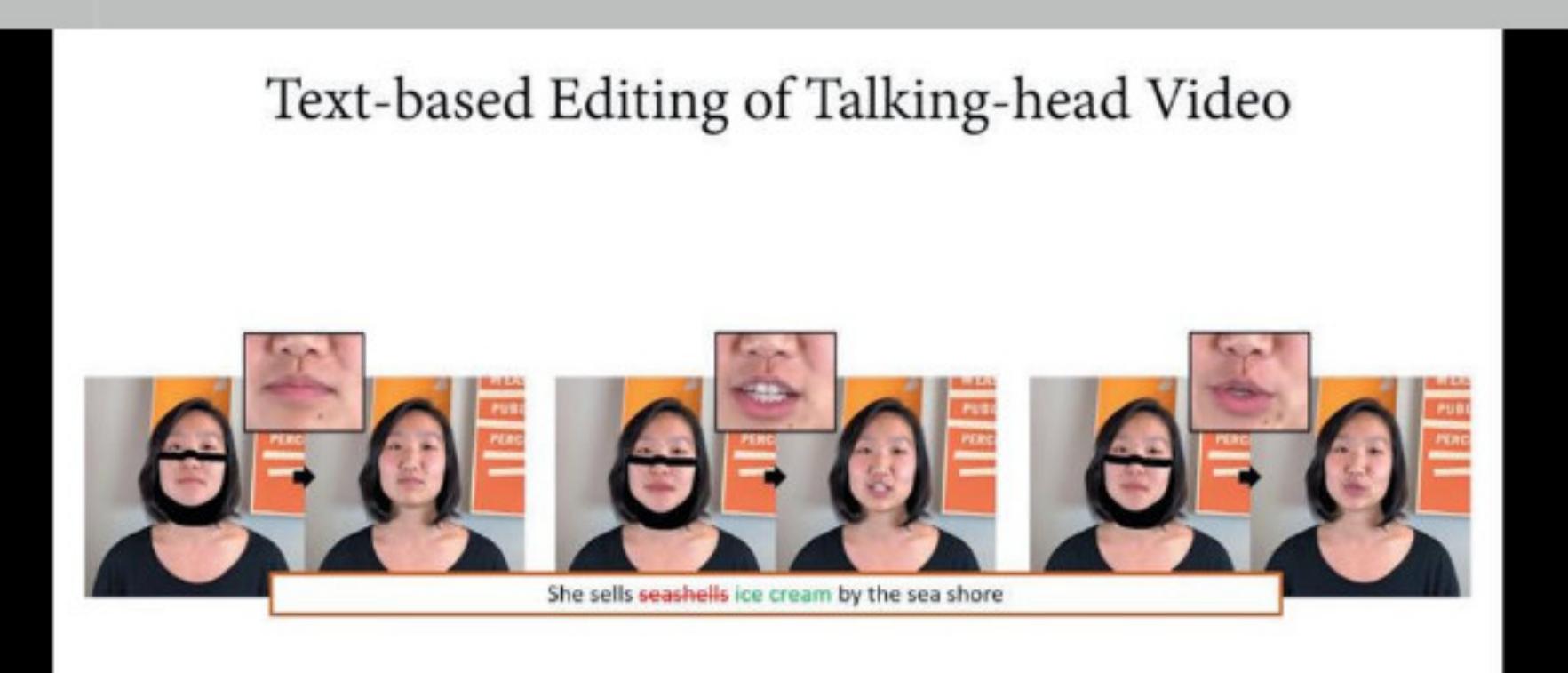
TensorFlow n'est pas un outil clé en main permettant de réaliser des Deepfakes. C'est ce qu'on appelle un «framework», dédié à l'apprentissage profond. Créé dans les labos de Google Brain - le département IA de Google -, il est opensource depuis 2015 et sert depuis au développement de nombreux outils nécessitant une bonne dose de « deep learning », notamment en reconnaissance faciale. Les développeurs peuvent utiliser ses puissants algorithmes comme moteur d'apprentissage pour leurs programmes, et ce avec une facilité déconcertante. Un codeur avec des connaissances moyennes peut créer son propre logiciel grâce à cet outil ultra puissant mis à disposition de tous. C'est notamment TensorFlow qui est utilisé derrière FakeApp que nous vous présentons ci-contre. D'autres frameworks concurrents existent aujourd'hui sur le marché, comme PyTorch, Cognitive Tools, MXnet ou encore Caffe.



TensorFlow

> LA SOLUTION D'ADOBÉ, BIENTÔT SUR VOS ÉCRANS

Vous tapez votre texte, l'IA se charge de modifier la vidéo pour que le personnage prononce votre discours avec une synchronisation du visage et des lèvres la plus réaliste possible bien sûr. On fait difficilement plus simple comme solution aujourd'hui. Cette nouvelle technologie nous était présentée en juin dernier par des scientifiques de l'Université de Stanford, de l'Institut Max Planck pour l'informatique, de l'Université de Princeton et en partenariat avec Adobe Research. Leur travail n'est pas encore accessible au grand public mais Adobe dévoile déjà des briques de ce programme, sans doute pour obtenir un retour d'expérience des utilisateurs avant sa commercialisation.



Text-based Editing of Talking-head Video

COMMENT ÇA MARCHE?

Pour l'instant, le logiciel a besoin d'un enregistrement initial de 40 mn (image + voix) de la personne cible. Il isole chaque phonème et expression faciale associée. Ensuite, il crée un modèle 3D de la moitié inférieure du visage. Une fois ces trois bases de données établies, l'utilisateur peut éditer son texte et laisser le moteur tourner pour obtenir sa vidéo finale. Lors des tests présentés en juin dernier, 60 % du panel test n'avait pas détecté de manipulation. Cela peut sembler faible... mais ce taux n'était que de 80 % pour la vraie vidéo avec ce même panel !

> SAMSUNG AI : VIDÉO À PARTIR D'UNE SEULE PHOTO

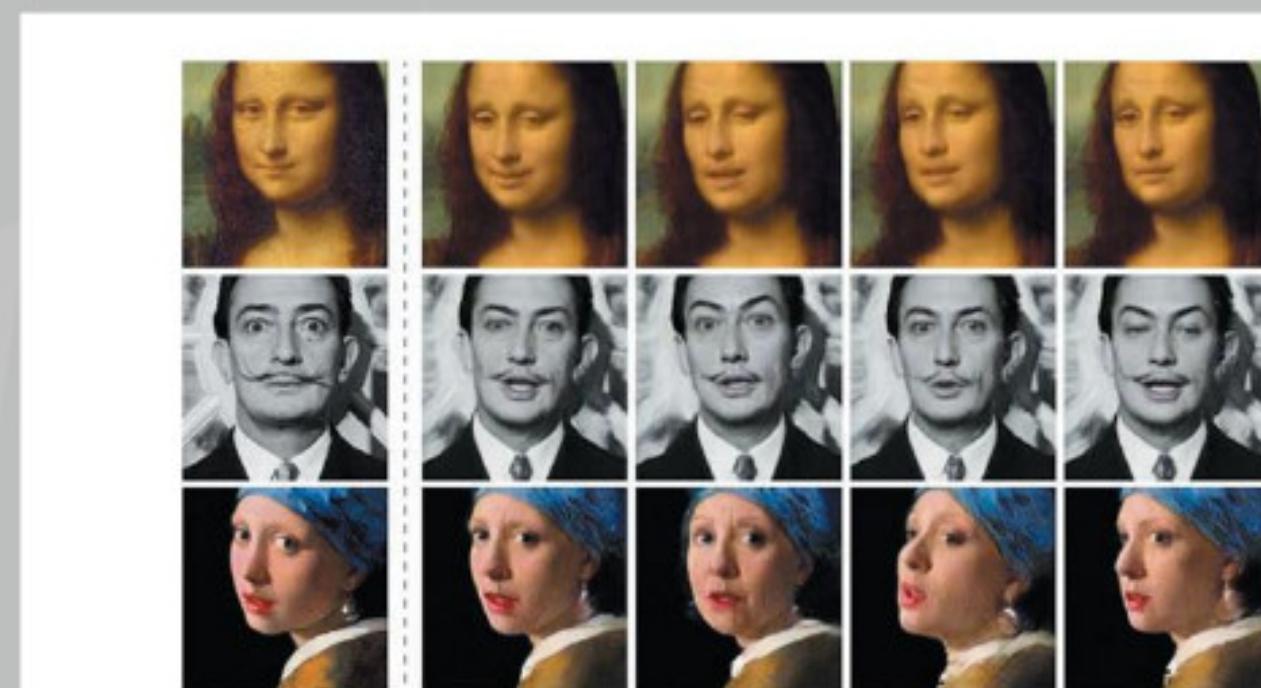
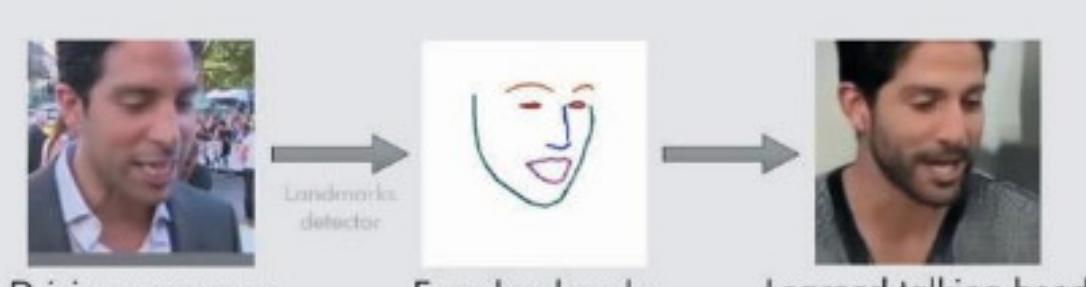
Le laboratoire russe de recherche en IA de Samsung, basé à Skolkovo, a impressionné ses interlocuteurs en faisant la démonstration d'animations vidéo plutôt réussies à partir d'une seule image fixe (même si plusieurs images avec des angles différents augmentent nettement la qualité du rendu final).

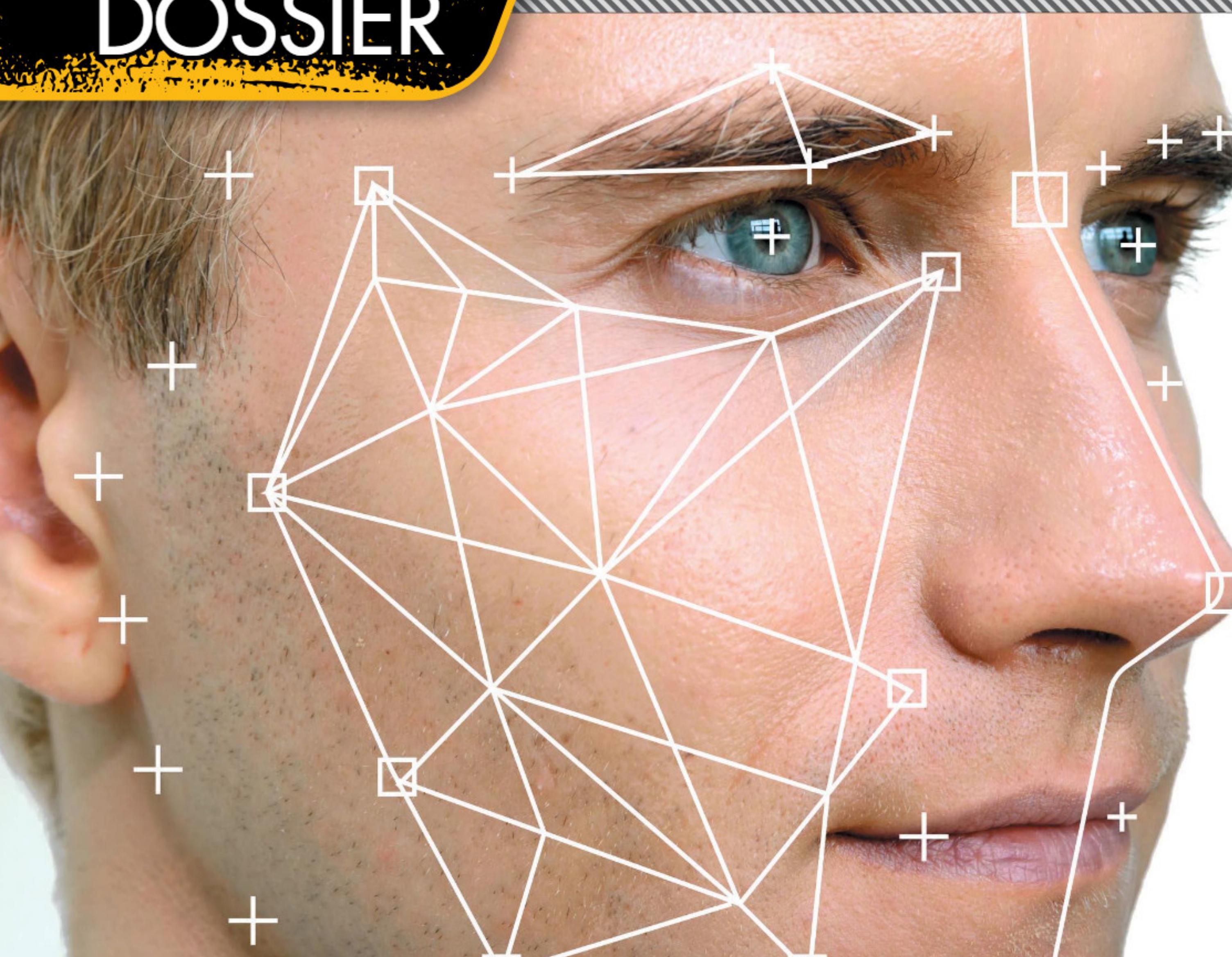
COMMENT ÇA MARCHE?

Habituellement, les deepfakes nécessitent une quantité de données importante pour truquer une vidéo, ici c'est un peu la logique « Face2Face » qui est utilisée par l'équipe, le temps réel en moins. L'outil de Samsung détecte les points et caractéristiques clés d'un visage (photo, dessin ou peinture) et extrapole les éléments invisibles. Mais comme nous vous le suggérons plus haut, Samsung doit aussi utiliser une vidéo de référence, prise avec un comédien ou autre, qui va reproduire les gestes, mimiques ou actions que l'on souhaite appliquer au personnage de l'image fixe.

Learning talking heads from few examples

Training frames:





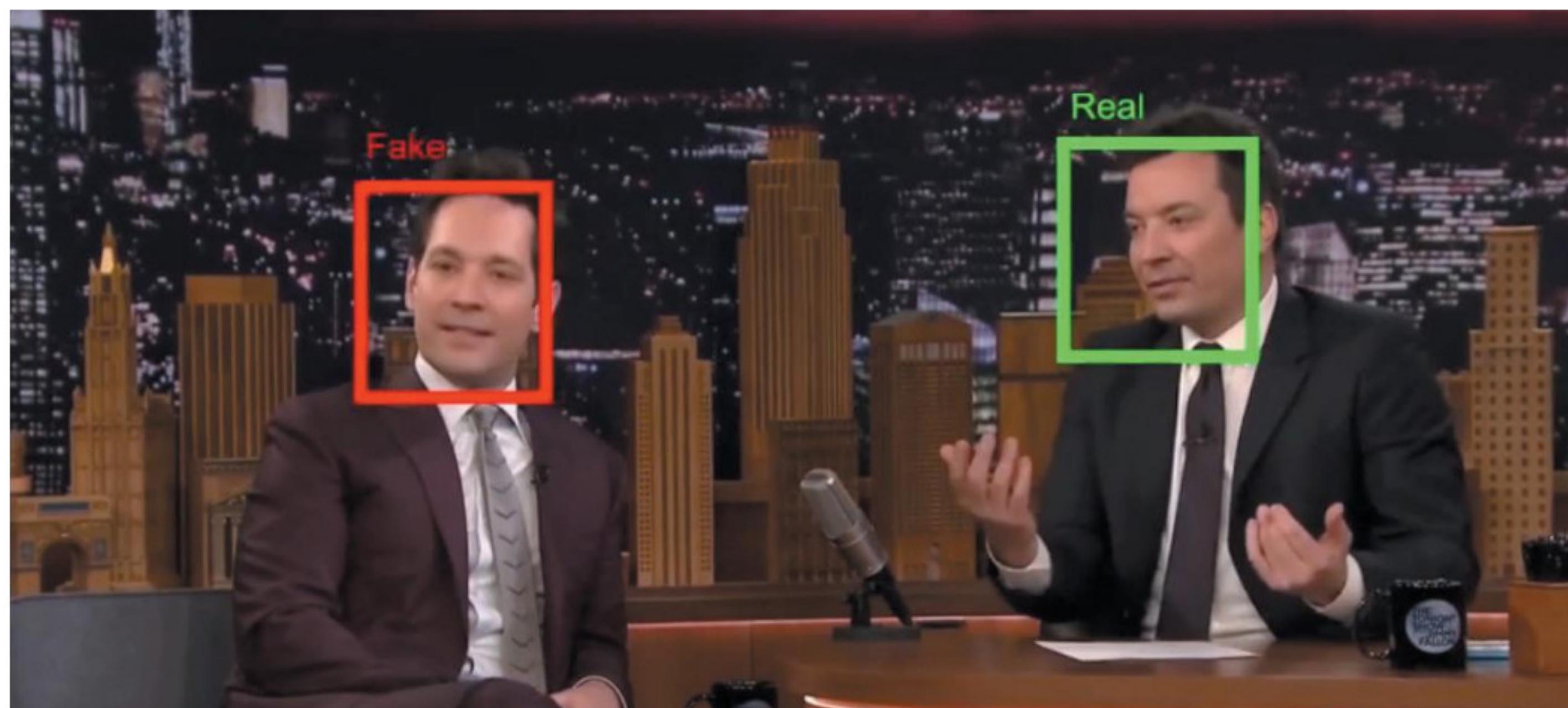
ÉTAT DES LIEUX

EST-IL POSSIBLE DE DÉTECTOR UNE VIDÉO TRUQUÉE ?

Bip Bip « la fake news » et Coyote « le garde chiourme » sont repartis pour de nouvelles aventures, sur fond de course à la détection de vidéos truquées. Nous savons tous très bien qui gagne à la fin.

En juin 2018, le professeur Siwei Lyu, de l'université d'Albany aux États-Unis, présentait le nouvel outil de détection de deepfakes mis au point par son équipe. La plupart des fausses vidéos de « célébrités » (politiques ou autres) présentait un même défaut : l'absence ou une anomalie du clignement des yeux. À cela rien d'étonnant puisque les algorithmes IA puissent aujourd'hui dans les clichés diffusés dans le domaine public (banques d'images, Google, etc.) et que le nombre de photos avec des personnalités aux yeux fermés y est ultra-minoritaire. Le talon d'Achille des outils deepfakes était donc trouvé !

Le logiciel mis au point par le chercheur permettait de se concentrer sur cet aspect des vidéos afin d'y déceler toute anomalie probante (avec un taux de réussite de 92,7 % en 2018). Las, peu de temps après cette publication, le Pr Siwei Lyu s'apercevait que de nouveaux outils « réparant » ces anomalies avaient été développés. « La prochaine génération sera certainement plus réaliste et plus difficile à repérer », concédait-il. « Nous devons donc nous y préparer.»



MESONET ANALYSE LES ZONES STRATÉGIQUES DU VISAGE, CELLES OÙ LES ERREURS SONT LE PLUS SUSCEPTIBLE D'APPARAÎTRE AUJOURD'HUI. ICI, UNE VIDÉO ANALYSÉE AVEC DEUX JIMMY FALLON, L'UN RÉEL À DROITE ET SON AVATAR À GAUCHE.



PLATE-FORME AUTOMATISÉE

L'Agence américaine pour les projets de recherche avancée de défense, la Darpa, poursuit le financement du professeur et d'autres équipes de chercheurs via son programme Medifor (pour Media Forensic). L'objectif : créer une plate-forme et des outils automatisés pour une analyse en temps réel de tout contenu sensible. Mais avec la crainte d'avoir toujours un wagon de retard, reconnaissant eux-mêmes « la disponibilité à grande échelle d'applications d'édition d'images et de vidéos sophistiquées, ainsi que d'algorithmes de manipulation automatisés » alors que les « outils de criminalistique utilisés aujourd'hui manquent de robustesse et d'évolutivité et ne traitent que de certains aspects de l'authentification de média ».

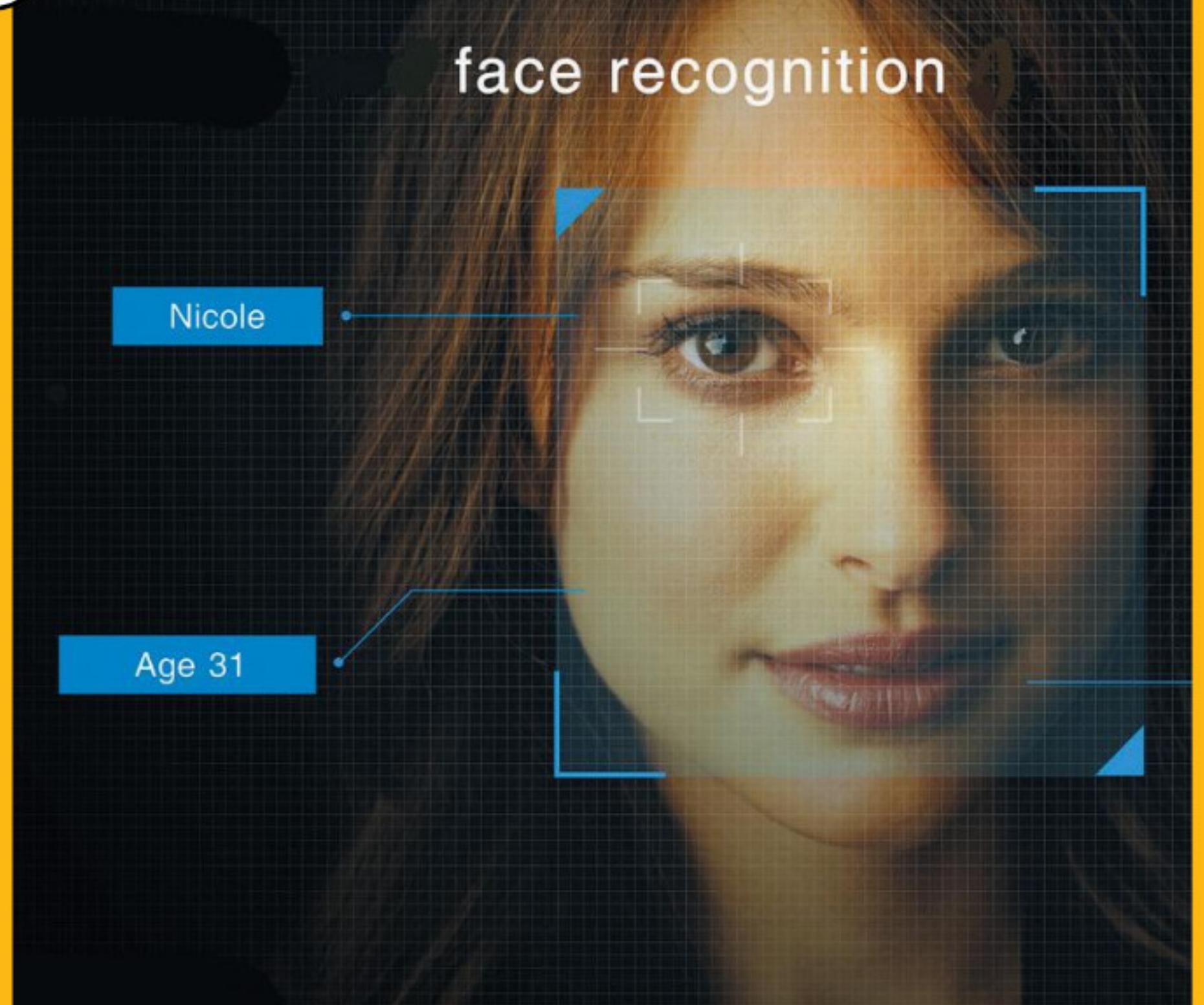
La recherche d'anomalies visuelles et de rendu (même difficile ou impossible à détecter à l'œil nu), cela fonctionne tout de même assez bien aujourd'hui : recherches de flous ou de cinématiques visuelles caractéristiques, colorimétrie et warping, analyses pixel par pixel, etc.

LES ANOMALIES VISUELLES BIENTÔT INDÉTECTABLES?

Cocréateur de Mesonet, un outil de détection de deepfake, Vincent Nozick (chercheur au laboratoire d'informatique Gaspard Monge) explique que "les zones les plus stratégiques avec notre approche sont le nez, les yeux et la bouche de la personne filmée. C'est là que se situe la majorité des irrégularités détectées par notre outil". Avec un taux de réussite supérieur à 90 %, Mesonet doit cependant être entraîné « continuellement pour que ce taux ne baisse pas car les techniques évoluent en permanence », précise le chercheur. Plus les intelligences artificielles et les moteurs d'édition graphique évolueront, plus les fausses vidéos sauront se rendre quasi indétectables au fur et à mesure qu'une nouvelle technique de détection sera connue.

CHAÎNE DE CONFIANCE

Une autre approche consiste à lister l'ensemble des pré-requis et des étapes de production d'une « vraie » image donnée (fixe ou animée) et des enregistrements sonores qui lui sont éventuellement associés. Types de matériels de prise de vue et de numérisation originale, formats d'encodage, logiciels de traitement utilisés, lumière, etc. : tout ceci laisse des traces numériques qui doivent être identifiables, cohérentes et/ou immuables en tout point d'une timeline. Si des incohérences apparaissent à certains moments, c'est que du « faux » s'est glissé dans un enregistrement. Mais la multiplicité des acteurs (fabricants, éditeurs, etc.), le fait qu'ils soient bien sûr réticents à partager leurs « recettes maison » et que eux-même utilisent maintenant des solutions IA intégrées et évolutives à leurs solutions de capture numériques (regardez les dernières prouesses des smartphones!) risquent de rendre ce recueil de données parcellaire, très imparfait sinon impossible.



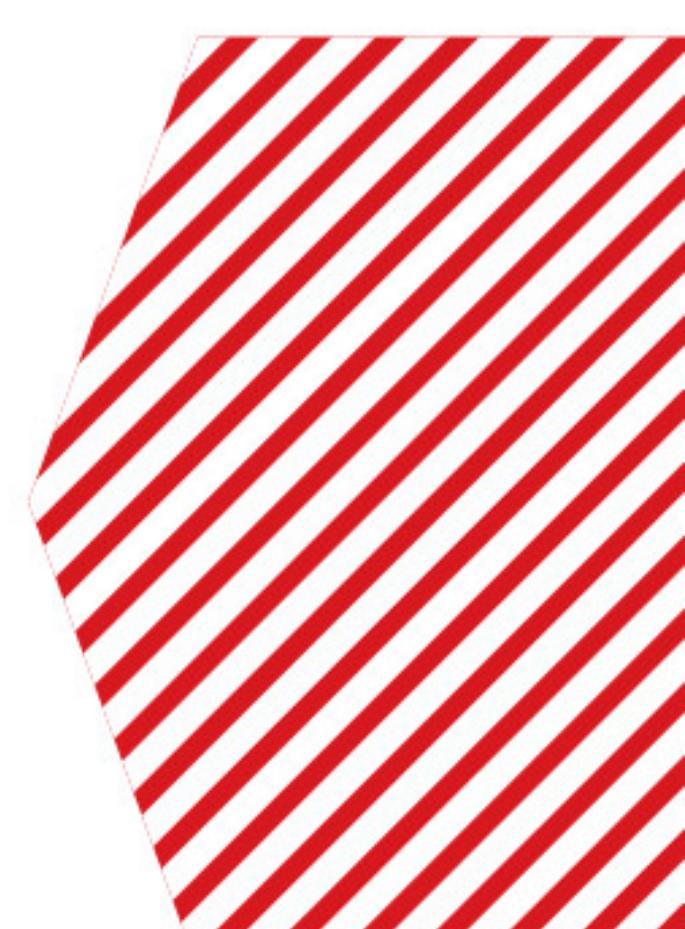
SÉCURITÉ ET RECONNAISSANCE FACIALE

Tous les services utilisant la reconnaissance faciale comme sésame d'identification ont du souci à se faire. On le savait déjà avec les images fixes (une simple photo suffit à déverrouiller de nombreux smartphones). Mais la nouvelle tendance est à l'analyse de séquences animées. Depuis 2017, Alibaba développe un système de paiement appelé « Smile to pay » avec Paypal. Vous l'aurez compris, il faut sourire pour s'identifier.

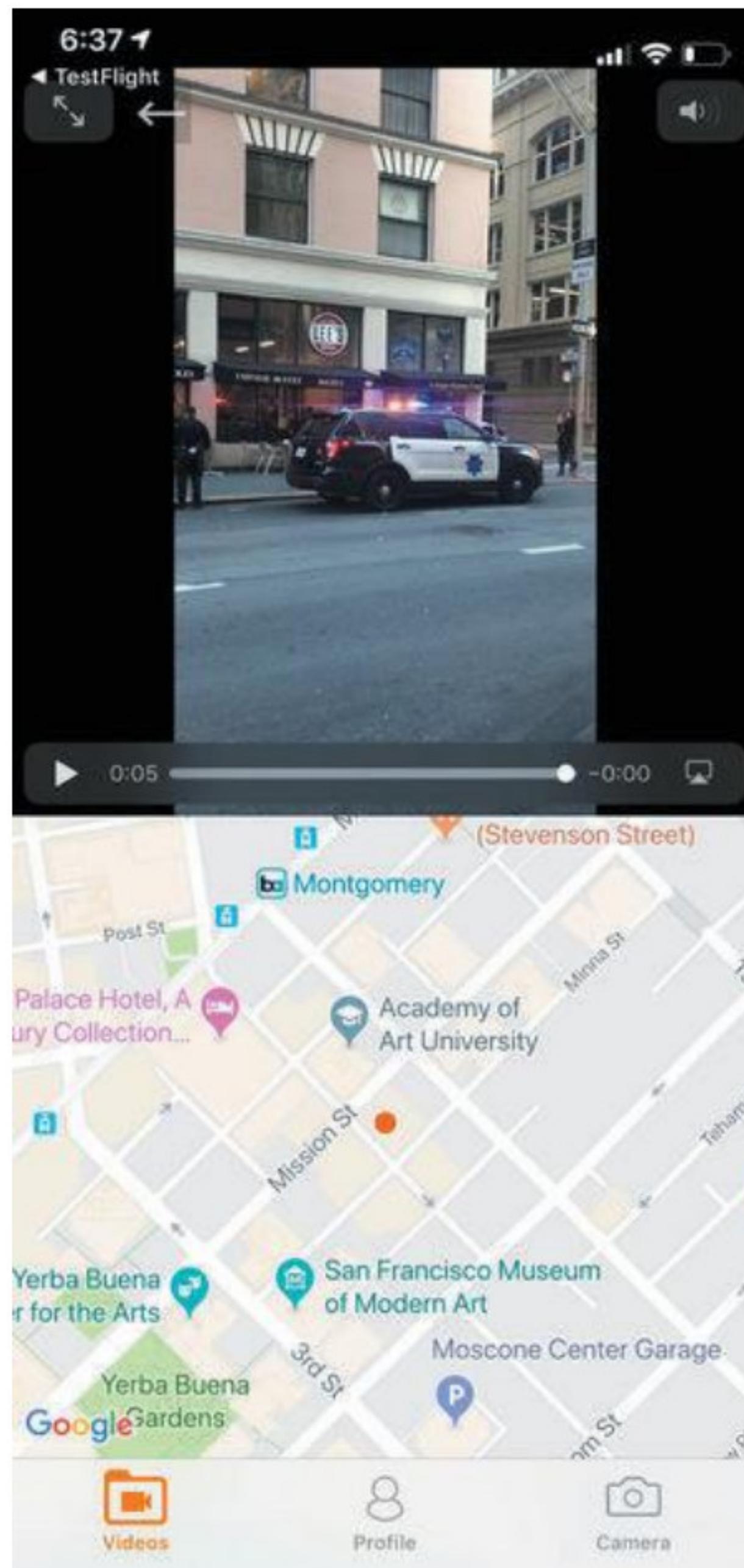
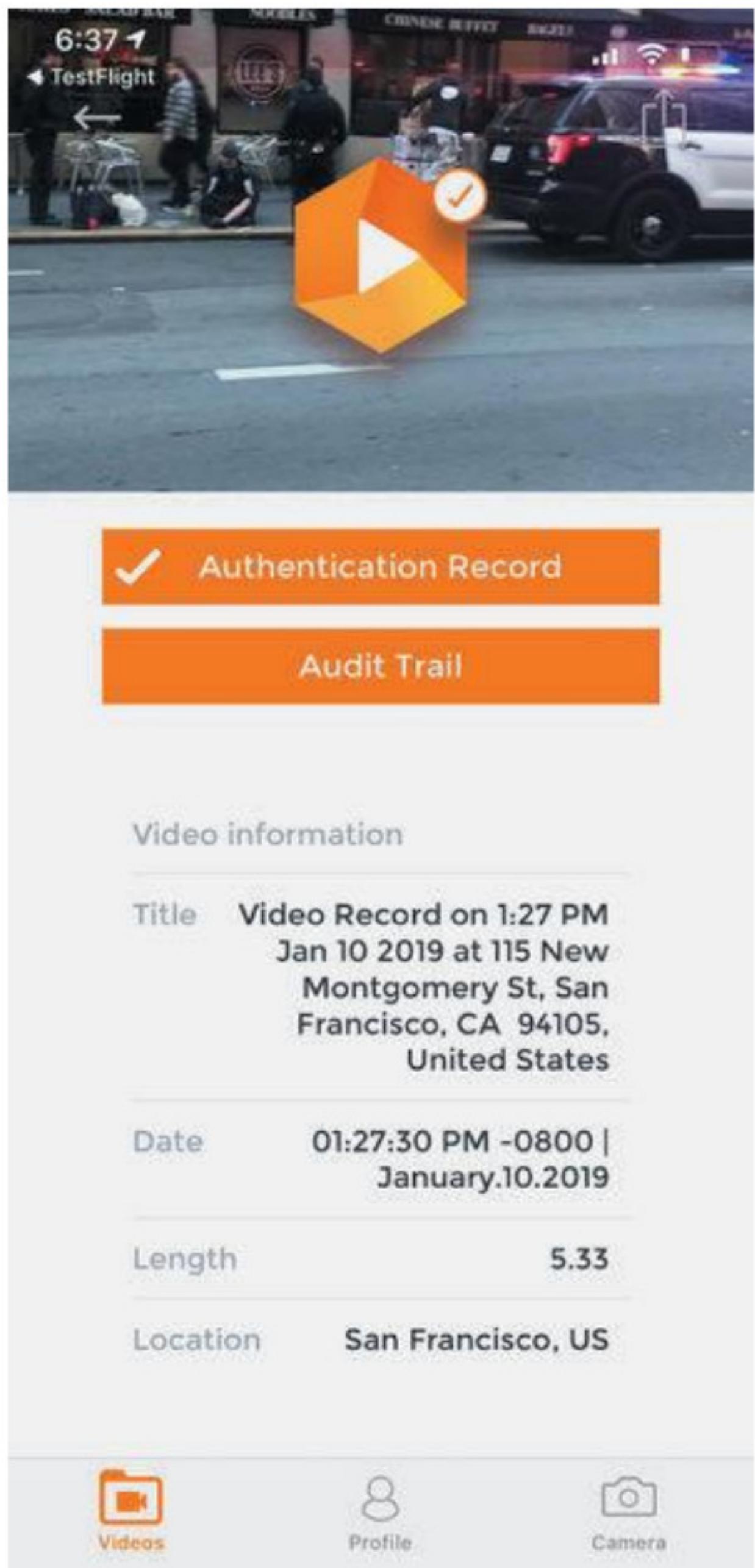
Une photo, un écran, une pincée d'IA... et hop, je crée en 2 mn une vidéo de mon voisin déclenchant son plus beau sourire. Alibaba a dû implémenter une deuxième couche d'identification pour sécuriser ce service... via un bon vieux code SMS sur le téléphone de l'utilisateur (l'idée était quand même de le supprimer). On avance.

« La prochaine génération sera certainement plus réaliste et plus difficile à repérer »

- Pr Siwei Lyu



LE BLACK DOSSIER



DANS SON APPLI APPLE, AMBER AUTHENTICATE ENCOURAGE MÊME LES VIDEO-BLOGGERS ET JOURNALISTES INDÉPENDANTS À UTILISER SES SERVICES POUR COUVRIR DES ÉVÉNEMENTS « CONTROVERSÉS » OU POUR TOUT BESOIN DE PREUVE FILMÉE, AFIN QUE PERSONNE NE PUISSE LES ACCUSER ENSUITE D'AVOIR FALSIFIÉ UNE PARTIE DU CONTENU.

Faudra-t-il être certifié « Deepfake free » pour avoir le droit de produire et diffuser ses propres images?

DONNER LES CLÉS AUX PRODUCTEURS ET DIFFUSEURS

Les autorités se tournent alors vers les principaux diffuseurs de contenus : médias et plates-formes de diffusion d'images et de vidéos. Puisque ce sont eux qui disposent des bases de données les plus importantes en terme d'images et de sons « véritables », imposons-leur d'automatiser l'inscription sur chaque fichier d'une signature électronique invisible (une sorte

de watermark). Chaque contenu original produit et/ou diffusé via leur entremise conservera cette trace indélébile ainsi qu'un certain nombre de datas associées. Cette signature ne pourrait être retirée, contrefaite et serait forcément altérée par l'intervention d'une IA puisque cette dernière utilise jusqu'à présent des sources multiples et variées pour produire un faux contenu original.

Cette approche est par exemple proposée par l'application Amber Authenticate. Cette solution fournit clé-en-main une technologie «fingerprint» qui marquera de façon invisible les contenus de ses clients. Dans sa version de base, Amber Authenticate affiche un cadre vert si la séquence est bien originale... et un cadre rouge apparaît si une partie semble avoir été modifiée.

Les techniques de chiffrement pouvant être appliquées à ces solutions semblent assez robustes pour résister à l'évolution des IA (il faudrait passer à des algorithmes quantiques pour les plus puissantes d'entre-elles). Mais le frein est davantage politique : comment imposer ce type de technologie au niveau d'une nation entière ou, pire, au niveau international ? Pas impossible si l'initiative vient, individuellement, des principaux acteurs concernés (chaînes de télé, agences photo, moteurs de recherche ou plates-formes vidéos, etc.) pour crédibiliser et protéger leurs contenus originaux et ceux de leurs utilisateurs.



Mais très compliqué à faire accepter si cela vient d' « en haut ». Et, dans les deux cas de figure, jamais tous les acteurs producteurs et diffuseurs au niveau mondial ne s'y plieront de façon transparente et potentiellement contrôlée. Hors, demain, les IA auront de moins en moins besoin de bases de données larges. Une seule capture vidéo et son de quelques secondes ou minutes ne suffira-t-elle pas à produire des quantités parfaitement fausses et originales de contenus intraçables ? Imagine-t-on le dirigeant de tel pays interdire toute prise d'images non autorisée lors de ses déplacements publics ou en visite dans telle ou telle contrée plus ou moins « inamicale » ?



L'HORIZON DU COMPORTEMENT

Vous pouvez aller plus loin et rajouter une analyse « comportementaliste » à votre détecteur de fausses vidéos.

Après avoir visionné des heures de séquences de l'ancien président Barack Obama, Shruti Agarwal (Université de Berkeley – USA) a remarqué des « tics » physiques notables. Comme le fait qu'à « chaque fois qu'il dit « Bonjour tout le monde », il remue la tête vers la gauche ou la droite, puis il se serre les lèvres ». Avec son directeur de thèse, Hany Farid, ils ont rassemblé des séquences vidéos de cinq personnalités politiques américaines majeures - Hillary Clinton, Barack Obama, Bernie Sanders, Donald Trump et Elizabeth Warren - et les ont analysées à l'aide de la boîte à outils open source d'analyse du comportement du visage OpenFace2. Leur objectif : être en mesure de disposer d'un outil efficace pour les élections présidentielles américaines de 2020.

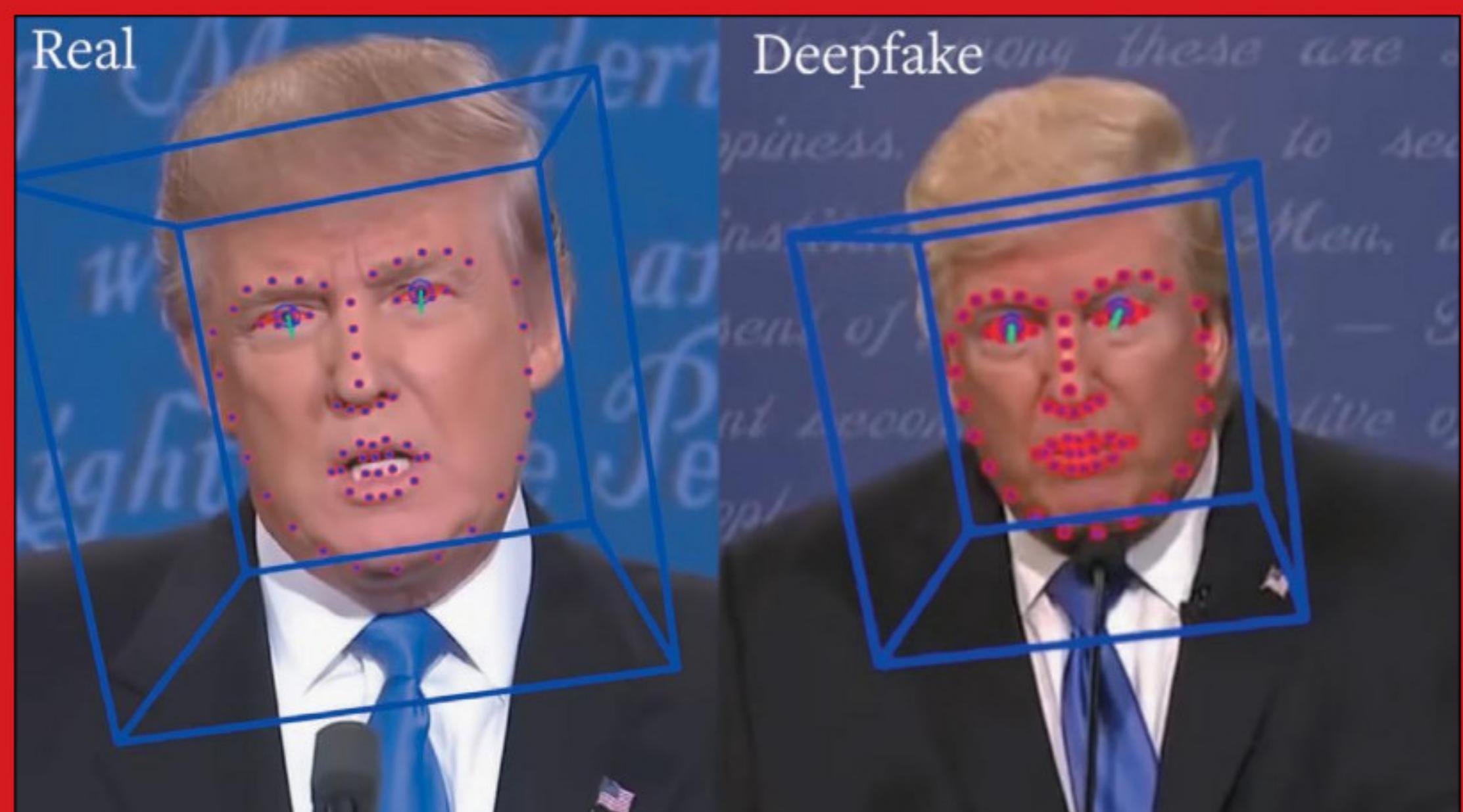
ET LA SPHERE PRIVÉE ?

Ils ont ensuite utilisé les résultats pour créer ce que l'équipe appelle des modèles « biométriques souples », qui établissent une corrélation entre les expressions faciales et les mouvements de la tête pour chaque chef politique. Avec cette approche, ils ont obtenu un taux de détection de fausses vidéos supérieur à 92 %. La technique fonctionne bien lorsqu'elle est appliquée à des personnalités politiques qui prononcent des discours officiels, car elles ont tendance à s'en tenir à des comportements bien répétés dans ces contextes. Mais cela pourrait ne pas fonctionner aussi bien dans d'autres contextes: par exemple, Obama pourrait ne pas avoir les mêmes tics lorsqu'il échange avec ses proches à l'occasion d'un dîner informel où serait servi du homard géant et, surtout, après avoir ingurgité quelques verres d'un grand cru français.

Les créateurs de vidéos deepfake pourront bien sûr se familiariser avec ces modèles de discours et apprendre à incorporer dans leurs vidéos les éléments de langage non verbal caractéristiques. Mais, vous l'aurez compris, plus les techniques des experts anti-deepfakes se perfectionneront, plus les technologies de falsification efficaces seront réservées à des groupes aux moyens conséquents.

LE GRAND MATCH DES AI

Quelques soient les techniques et approches « anti-deepfakes » utilisées, seules ou associées, c'est la confrontation entre intelligences artificielles qui sera passionnante à suivre. Car si des IA « deep learning » sont mises à contribution pour créer des vidéos truquées, d'autres sont bien sûr appelées à la rescouasse pour les repérer. Des chercheurs de l'USC Information Sciences Institute (Californie du Sud) utilisent ainsi un outil qui s'est entraîné sur plus de 1000 vidéos manipulées, analysant à la fois les micro-expressions visuelles et les artefacts dans les fichiers. Selon une étude publiée par la Computer Vision Foundation, le taux de repérage efficace serait aujourd'hui de 96 %. Et comme on nous promet une invasion de vidéos deepfake dans les années à venir, ce type d'approche « deeplearning » ne manquera pas de nouveaux contenus à analyser...



 LE LOGICIEL DE SUIVI
OPENFACE ANALYSE
UNE VRAIE VIDÉO DU
PRÉSIDENT TRUMP À
GAUCHE ET UNE IMITATION À
DROITE. LES CHERCHEURS
DE L'UNIVERSITÉ DE
BERKELEY ÉTUDIENT ICI LES
TICS DE LANGAGE PROPRES
AU PRÉSIDENT EN FONCTION
DU CONTEXTE, COMME LE
MOUVEMENT DES SOURCILS,
DU MENTON OU DES
ÉPAULES.

© UC Berkeley -
Stephen McNally.

LES GUIGNOLS DE L'INFOX

La culture Mème est sortie des faubourgs de l'Internet pour s'inviter dans tous les forums Web de la vie publique. Les outils Deepfake sont et seront utilisés pour nous faire rire aux dépends d'autrui (surtout si autrui est riche, puissant et célèbre, c'est quand même plus drôle...).

Il y a 80 ans, l'on caricaturait en dessins. Il y a 40 ans, l'on s'extasiait devant des imitateurs plus vrais que nature. Il y a 25 ans, nous avions les Guignols de l'Info qui offraient une vie de latex à leurs victimes. Depuis 15 ans, on double, on photoshope, on mixe... Canteloup fait encore marrer la ménagère de moins de 50 ans avec ses (vraies) vidéos faussement triturées et doublées.

Mais l'Internet et ses montages génialement foireux sont le véritable espace de défoncement de la jeune génération. Parions qu'il ne faudra pas attendre longtemps pour voir débarquer des hordes de nouveaux plaisantins assumés, repoussant les limites du réel pour jouer avec notre crédulité (consentante) grâce à des IA aussi ingénieuses que déstabilisantes.

PARODIES ASSUMÉES

D'autant que, comme nous vous l'avons présenté ici, les logiciels et services disponibles sont déjà accessibles au plus grand nombre. Quel prochain humoriste « star du Web » sera le grand spécialiste du deepfake ? Réponse avant 2020, nous tenons les paris. Comme le Gorafi, il ne sera pas question ici de « faire croire que », le côté parodique sera revendiqué. Il y aura bien quelques

crédules idiots comme Christine Boutin ou Marine Le Pen pour tomber dans le panneau et, découvrant la lune, débouler dans les rédactions en s'écriant « Non mais vous avez vu, c'est un scandale !? Macron et Mélenchon participent à des parties fines à Ibiza, jetant du homard pas frais sur la statue du Général de Gaulle, entourés de chippendales islamo-gays ! »

SOMMES-NOUS PRÊTS?

Au-delà de la blague facile, il faut quand même se demander si notre psyché saura s'adapter à cette évolution. On prête aux humoristes un pouvoir d'influence énorme, notamment en politique. Nous savons tous qu'il s'agit de « faux », de traits caricaturaux et souvent grossiers mais notre cerveau enregistre une émotion qui entre en compétition avec notre réflexion (et c'est tant mieux). Le but du jeu est de déstabiliser nos certitudes et de combattre les « bullshits » des politiques par des exagérations et contrepoints assumés (et drôles, eux). Sans oublier que l'humour fonctionne d'autant mieux qu'une partie du discours peut avoir l'apparence du vraisemblable ou révéler une faiblesse réelle chez la « victime ».

Quel prochain humoriste « star du Web » sera le grand spécialiste du deepfake ?



 UNE FAUSSE VIDÉO DE MARC ZUCKERBERG DOPÉE À L'AI PLAÇAIT LES PAROLES SUIVANTES DANS LA BOUCHE DU FONDATEUR DE FACEBOOK EN JUIN DERNIER : "IMAGINEZ ÇA UNE SECONDE: UN HOMME AVEC LE CONTRÔLE TOTAL DES DONNÉES VOLÉES DE MILLIARDS DE PERSONNES, LEURS SECRETS, LEURS VIES, LEURS AVENIRS. JE DOIS TOUT CELA À SPECTRE. SPECTRE M'A MONTRÉ QUE QUICONQUE CONTRÔLE LES DONNÉES CONTRÔLE L'AVENIR". C'EST AMUSANT, NOUS SOURIONS AUSSI. MAIS PAS QUE..."

SOURCE : BILL POSTERS

Mais quand nos propres sens seront trompés, où tout aura l'apparence de la réalité, notre cerveau donnera-t-il plus de poids aux émotions ressenties, aura-t-il plus de mal à s'en distancer ? Voir une marionnette, un dessin ou une image détournée d'un leader politique en fâcheuse posture est une chose. Le visionner sur petit écran préférer ou faire des horreurs aura un autre impact quand nous le reverrons ensuite « en vrai » essayant de défendre telle ou telle idée. Les Guignols de l'Info ont été accusés par l'opposition d'avoir rendu Jacques Chirac sympathique (« Mangez des Pommes ! ») en 2002 et d'avoir joué un rôle non négligeable dans sa réélection. Sortez le pop-corn, les débats s'annoncent passionnants ces prochaines années...



QUAND LE PERSONNAGE FICTIONNEL JOHN SNOW S'EXCUSE
DU SCÉNARIO DE LA SAISON 8 DE GAME OF THRONES, LE
DEEFAKE NE TROMPE PERSONNE ET AMUSE LES FANS...

SOURCE : [YOUTUBE.COM/C/EATINGTHINGS](https://www.youtube.com/c/EATINGTHINGS)



DeepNude

FAKE TON BOOTY



« Le monde n'est pas prêt ». C'est en tout cas ce qu'ont déclaré les éditeurs estoniens de l'application DeepNude. Crée en mars 2019, cette dernière a affolé la Toile fin juin avant d'être retirée au bout de quelques jours. DeepNude permettait (sous Linux et Windows) de recomposer la nudité supposée d'une femme à partir d'une simple photo, en piochant dans une base de plus de 10000 clichés de nus. Bien sûr, les dérives sont arrivées en escadron : publications et partages de fausses photos, revenge porn et autres joyeusetés ont pourri la vie de centaines de femmes.

Après la divulgation du code source, de nombreuses autres clones du logiciel se sont mis à circuler depuis. Et personne n'est dupe, ce type de « service » continuera à être développé et perfectionné.

LOI BALBUTIANTE

Hasard du calendrier, l'État de Virginie aux États-Unis ajoutait le 1^{er} juillet la notion de deepfake dans la loi

interdisant depuis 2014 le “revenge porn” (publier une vidéo porno sans le consentement de la personne). Une première, car si les législateurs se sont penchés sur les infox utilisant intelligence artificielle et deepfakes, rien encore (ou presque) sur les falsifications de contenus « olé-olé ».

UNE IA À L'ESPRIT MAL TOURNÉ

Tout débute pourtant dès novembre 2017. Sur le forum de discussion Reddit, l'utilisateur « Deepfakes » diffuse les premières vidéos de pornos où le visage d'une actrice a été remplacé par celui de célébrités. Le résultat n'est pas encore convaincant mais d'autres internautes prennent le relais. Daisy Ridley (*Star Wars*), Emma Watson (*Harry Potter, La Belle et la Bête...*) ou Gal Gadot (*Wonder Woman*) se retrouvent ainsi bien malgré elles dans des positions plus que compromettantes. Derrière ces premiers essais, l'on retrouve le code de TensorFlow, un outil d'apprentissage profond dédié aux images et aux vidéos... développé par le très puritain Google.



HACKING



POUR QUI ?

Pour les bidouilleurs

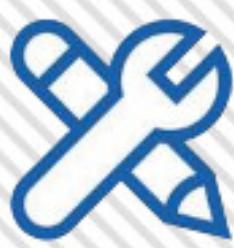
POUR QUOI FAIRE ?

Pour avoir un rapport détaillé des activités de votre Windows

SURVEILLEZ L'ACTIVITÉ DE VOTRE SYSTÈME WINDOWS

Une fois lancé, Windows File Tools va enregistrer les modifications apportées aux fichiers et dossiers de Windows. Cela permet de mesurer l'impact d'une installation, de mieux cerner les malwares ou tout simplement de surveiller l'activité des utilisateurs de l'ordinateur cible.





INFOS [Windows File Tools]

Où le trouver ? [www.phrozen.io/freeware/windows-file-tools]

Difficulté : 🧟🧟🧟

➤ Surveillance Windows

Créé par la société française Phrozen, Windows File Tools est un logiciel dans la continuité de ce qu'était Windows File Monitor. Le principe est le même qu'auparavant, il s'agit de surveiller les activités des fichiers en temps réel en générant une arborescence d'événements. Une fois lancé, le programme va enregistrer les événements suivants : création, modification, mise à jour et suppression de fichier ou de dossier. Le but d'un logiciel de ce type est à la fois de surveiller l'activité d'un PC lorsque vous n'êtes pas présent (PC de travail, à l'école, etc.), mais aussi de regarder de près ce qu'un malware pourrait déclencher comme modification sur votre ordinateur. Pour éviter de se retrouver avec des tonnes d'informations dans les journaux, on peut bien sûr filtrer les événements, les chemins spécifiques à surveiller (éventuellement de manière récursive), des extensions de fichiers spécifiques (mode liste blanche). Windows File Tools est compatible avec toutes les versions de Windows de XP à Windows 10.

 **UN CODE COULEUR DANS LA LISTE D'ÉVÉNEMENTS PERMET D'EN SAVOIR PLUS SUR TELLE OU TELLE ACTIVITÉ...**

UN LOGICIEL PHROZEN SAS



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

Lien : www.phrozen.io

The screenshot shows a software interface for Phrozen SAS. At the top, there's a navigation bar with icons for Stop, Options, and a menu. Below it, a tree view labeled "Tree" shows a folder structure on drive D: containing "ID Presse", "ANDROID-MT", and a "DONE" folder which itself contains a "TEST_Sony Xperia 10+" folder with a "clichés" subfolder holding three files: "DSC_0033.JPG", "DSC_0018.JPG", and "DSC_0017.JPG".

Below the tree view is an "Events List" table:

Date Time	Item 1	Item 2	Event
09/07/2019 22:29:00	C:\Users\benba...		File Updated
09/07/2019 22:29:30	C:\Users\benba...		File Deleted
09/07/2019 22:58:06	D:\ID Presse\AN...		File Deleted
09/07/2019 22:58:06	D:\ID Presse\AN...		New File
09/07/2019 22:58:06	D:\ID Presse\AN...		File Updated
09/07/2019 22:58:06	D:\ID Presse\AN...		File Updated
09/07/2019 22:58:06	D:\ID Presse\AN...		File Updated

The screenshot shows the Windows File Tools application interface. At the top, there are "Stop" and "Options" buttons. On the right, there's a menu icon. The main area has two sections: "Tree" and "Events List".

The "Tree" section shows a file system structure on drive D: with folders "ID Presse", "ANDROID-MT", and a "DONE" folder containing "TEST_Sony Xperia 10+", "clichés", and three image files: "DSC_0033.JPG", "DSC_0018.JPG", and "DSC_0017.JPG".

The "Events List" section displays a table of file system events:

Date Time	Item 1	Item 2	Event
09/07/2019 22:29:00	C:\Users\benba...		File Updated
09/07/2019 22:29:30	C:\Users\benba...		File Deleted
09/07/2019 22:58:06	D:\ID Presse\AN...		File Deleted
09/07/2019 22:58:06	D:\ID Presse\AN...		New File
09/07/2019 22:58:06	D:\ID Presse\AN...		File Updated
09/07/2019 22:58:06	D:\ID Presse\AN...		File Updated
09/07/2019 22:58:06	D:\ID Presse\AN...		File Updated



HACKING

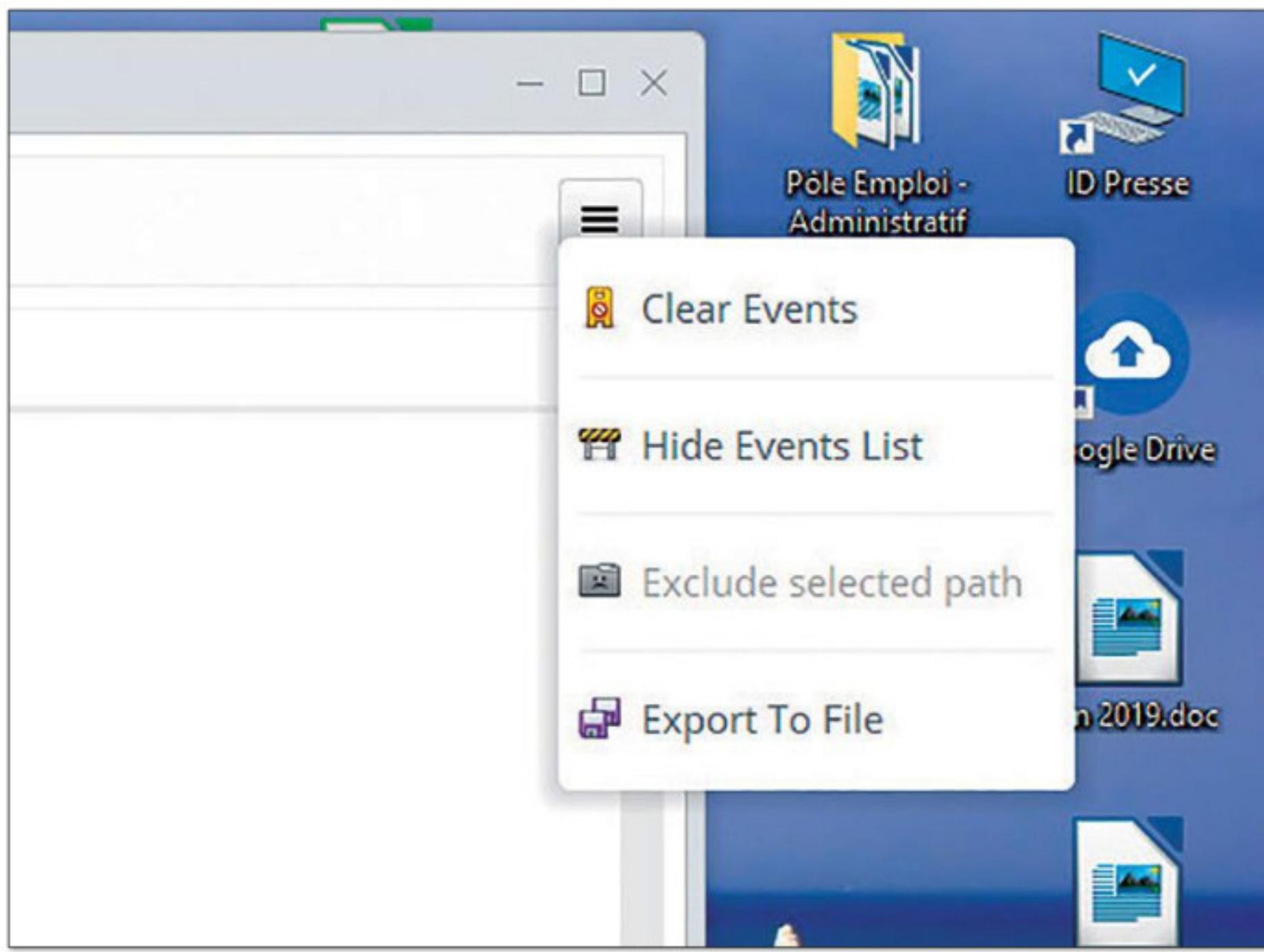
Surveillance Windows

COMMENT FONCTIONNE WINDOWS FILE TOOLS ?

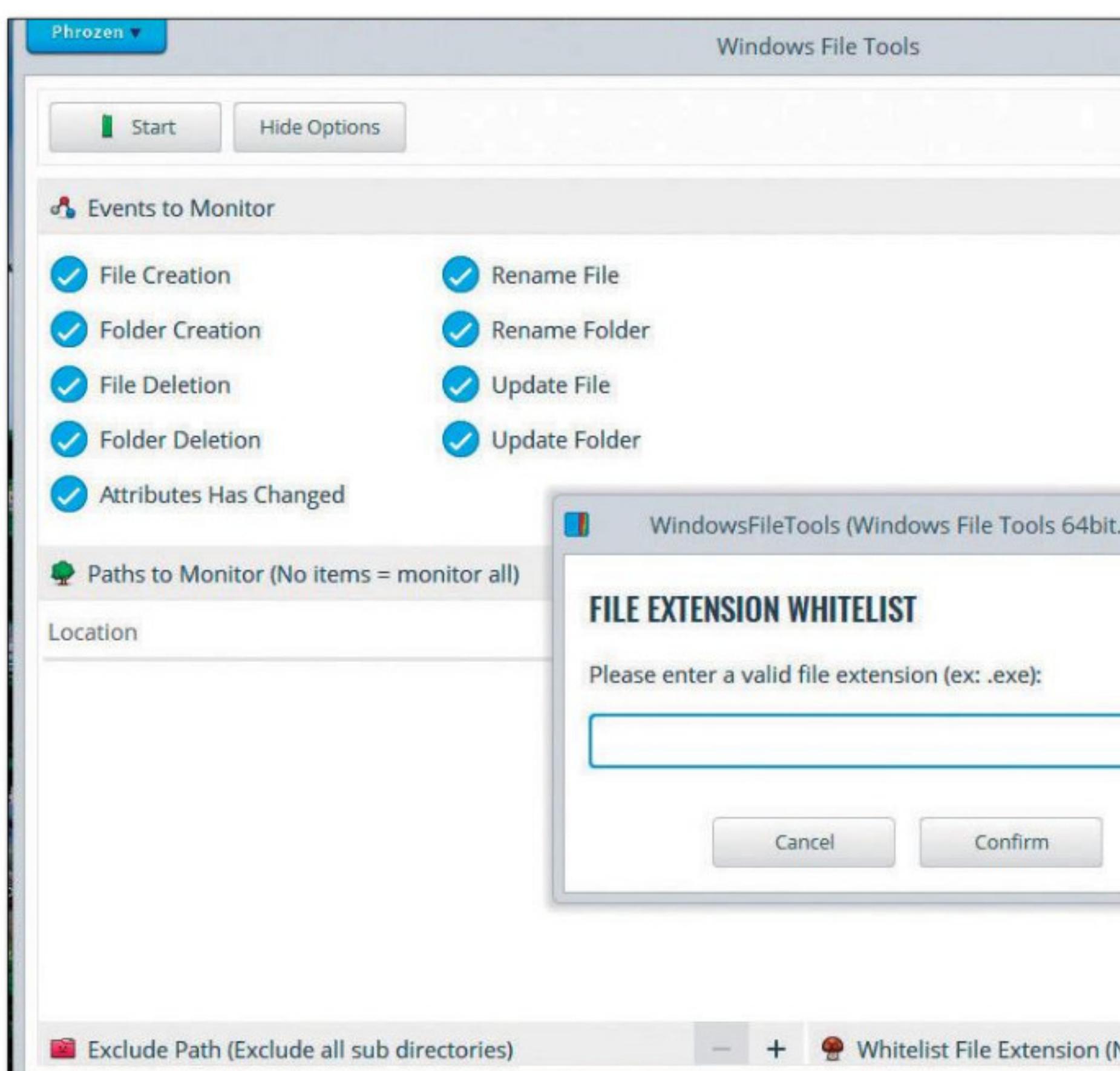


01 > PREMIER PAS...

Le logiciel ne nécessite pas d'installation, mais il requiert des droits administrateur. Dans l'archive, vous trouverez une version pour les OS 32 bits et une autre pour les systèmes 64 bits. Après le démarrage, cliquez dans le menu Phrozen pour passer au français si vous le désirez.



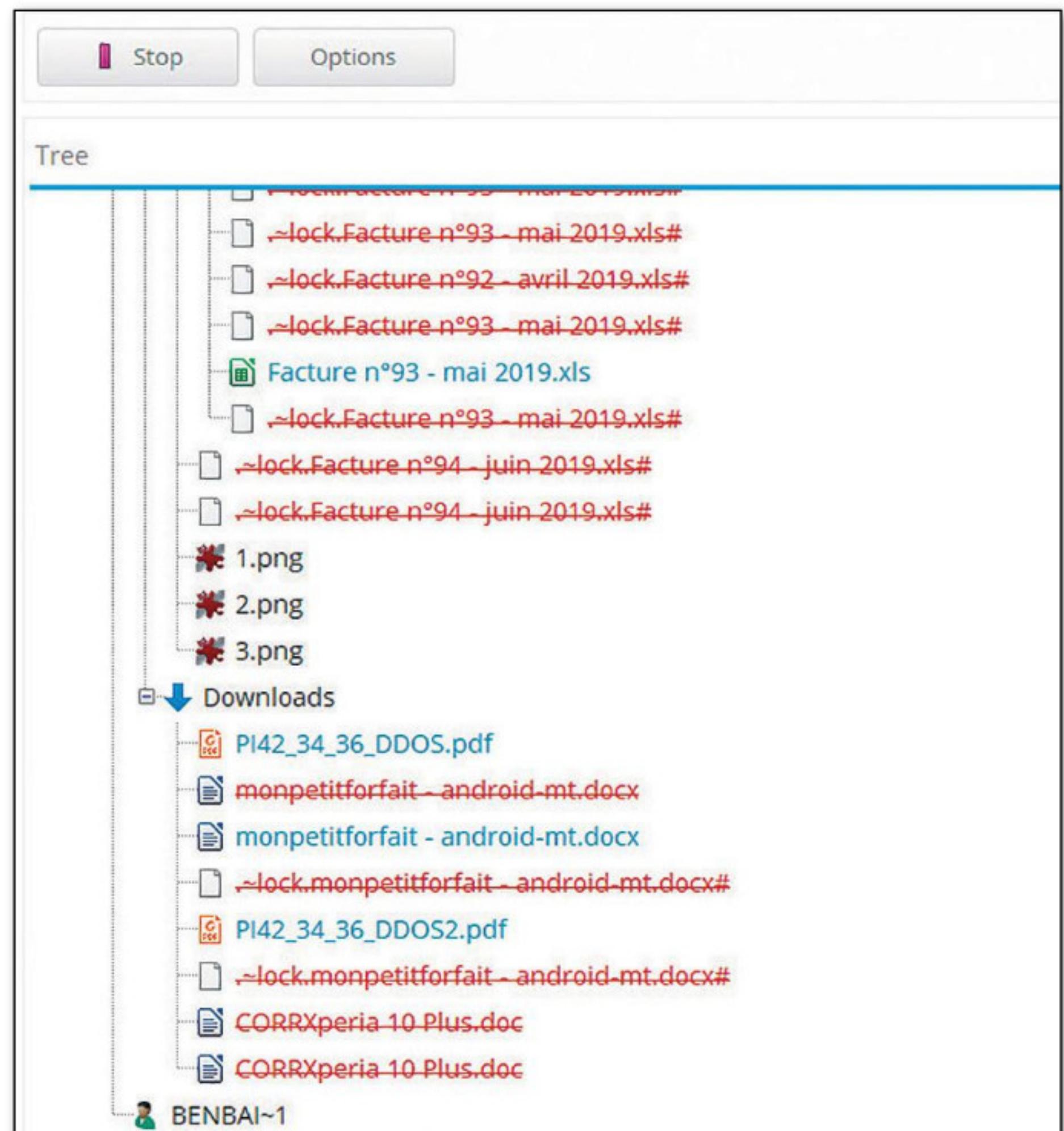
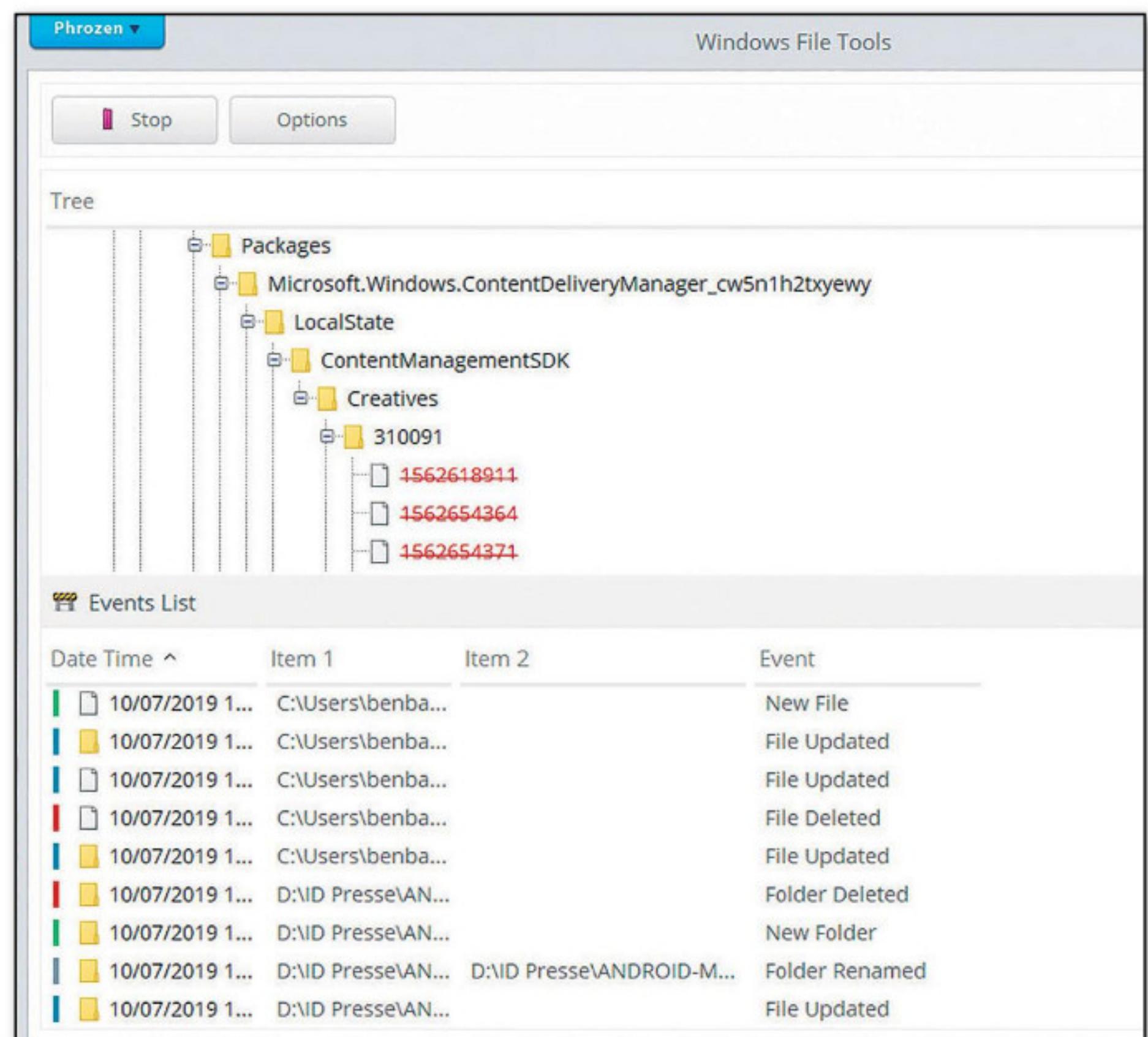
02 > LES OPTIONS ET LES FILTRES



Pour démarrer le suivi et l'enregistrement de l'activité dans le journal, vous pouvez faire Start, mais avant, allons faire un tour dans les options. Ici vous pourrez choisir quel type d'activité moniter, mais aussi définir un chemin dans votre système (Path to Monitor) ou à l'opposé en exclure un. On peut aussi surveiller une seule extension de fichier si nécessaire.

03 > LE JOURNAL

Une fois lancée, la fenêtre du bas va afficher les modifications. Parfois, le système réagit tout seul à certaines tâches automatiques. Pour y voir plus clair, le logiciel ajoute des codes couleurs en face de chaque événement : vert pour la création d'un fichier ou d'un dossier, rouge pour un effacement, gris si un élément est renommé et bleu pour une modification ou un changement d'attribut : lecture seule, archive, fichier caché, fichier système, etc. À vous de jouer avec ces options pour trouver ce qui cloche dans votre Windows ou pour vous rassurer...



POUR QUI ?

Pour les utilisateurs qui ont l'habitude d'assurer la maintenance pour tata Lydie

POUR QUOI FAIRE ?

Pour réparer, sauvegarder, désinfecter, auditer, etc.

LIVE CD : AU SECOURS DE VOTRE PC...

Il y a des signes qui ne trompent pas : ralentissements, publicités non sollicitées, faux messages d'alerte, crash à répétition ou tout ça à la fois ? Qu'il s'agisse d'une infection, d'un problème de registre ou d'un bug du système, votre valeureux PC a besoin d'être réparé. Que vous ayez la main sur Windows ou non, voici nos solutions «Live CD»... Ha oui la plupart sont compatibles avec Linux.


INFOS

[Hiren's Boot CD]

Où le trouver ?
[www.hirensbootcd.org]


[F-Secure Rescue Disk]

Où le trouver ?
[<https://goo.gl/6D36ol>]


[FalconFour's Ultimate Boot CD]

Où le trouver ?
[<http://beta.falconfour.com/category/bootcd>]


[AVG Rescue CD]

Où le trouver ?
[www.avg.com/fr-fr/rescue-cd-business-edition]


[MediCat]

Où le trouver ?
[<https://goo.gl/3imeh8>]


[Ultimate Boot CD]

Où le trouver ?
[www.ultimatebootcd.com]

Difficulté :



HACKING



DECRYPTAGE

CHANGEZ LE BOOT



Options avancées



Voir plus d'options de récupération

De base, votre PC va «booter» sur le disque dur pour charger Windows. Pour afficher les menus de votre Live CD, il faudra changer ce réglage dans le BIOS. Il faudra faire Suppr, F1, F2 ou F8 (en fonction de votre modèle de carte mère) juste après avoir allumé le PC et entrer 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 ou votre port USB si c'est cette solution que vous avez choisie. Attention, certains fabricants de cartes mères intègrent depuis quelques années un BIOS sécurisé et un peu pénible appelé UEFI. Voici un article très intéressant si vous avez ce type de BIOS : <http://goo.gl/KSDTS5>

Les Live CD fonctionnent tous de la même manière. Il faut télécharger une image de disque au format ISO puis la graver sur un CD ou un DVD en fonction de leur taille. Pour certains d'entre eux, il est même possible de les placer sur une clé USB (pratique si votre lecteur est absent ou cassé). Avec le logiciel Xboot, vous pouvez même vous faire une compilation de différents Live CD sur une seule et même clé USB. Veillez juste à ce que votre BIOS accepte le boot depuis un port USB.

DES DVD BOURRÉS DE SOLUTIONS

En fonction du Live CD que vous aurez choisi, les outils à l'intérieur permettront une désinfection, des diagnostics (RAM, disque dur), une réparation (registre, secteur de disque), une sauvegarde, etc. Lorsque vous aurez terminé, il faudra relancer Windows en croisant les doigts pour qu'il veuille bien se lancer. Si ce n'est pas le cas, les dégâts seront moindres si vous devez formater et réinstaller un système puisque vous aurez sauvegardé vos mots de passe et vos fichiers... Si vous avez un numéro de licence Windows (un autocollant avec une suite de caractères sur votre unité centrale), mais pas le DVD d'installation (versions dites «OEM»), rien ne vous empêche de télécharger un Windows sur Internet. Le téléchargement est légal si vous ne changez pas de PC : profitez-en !

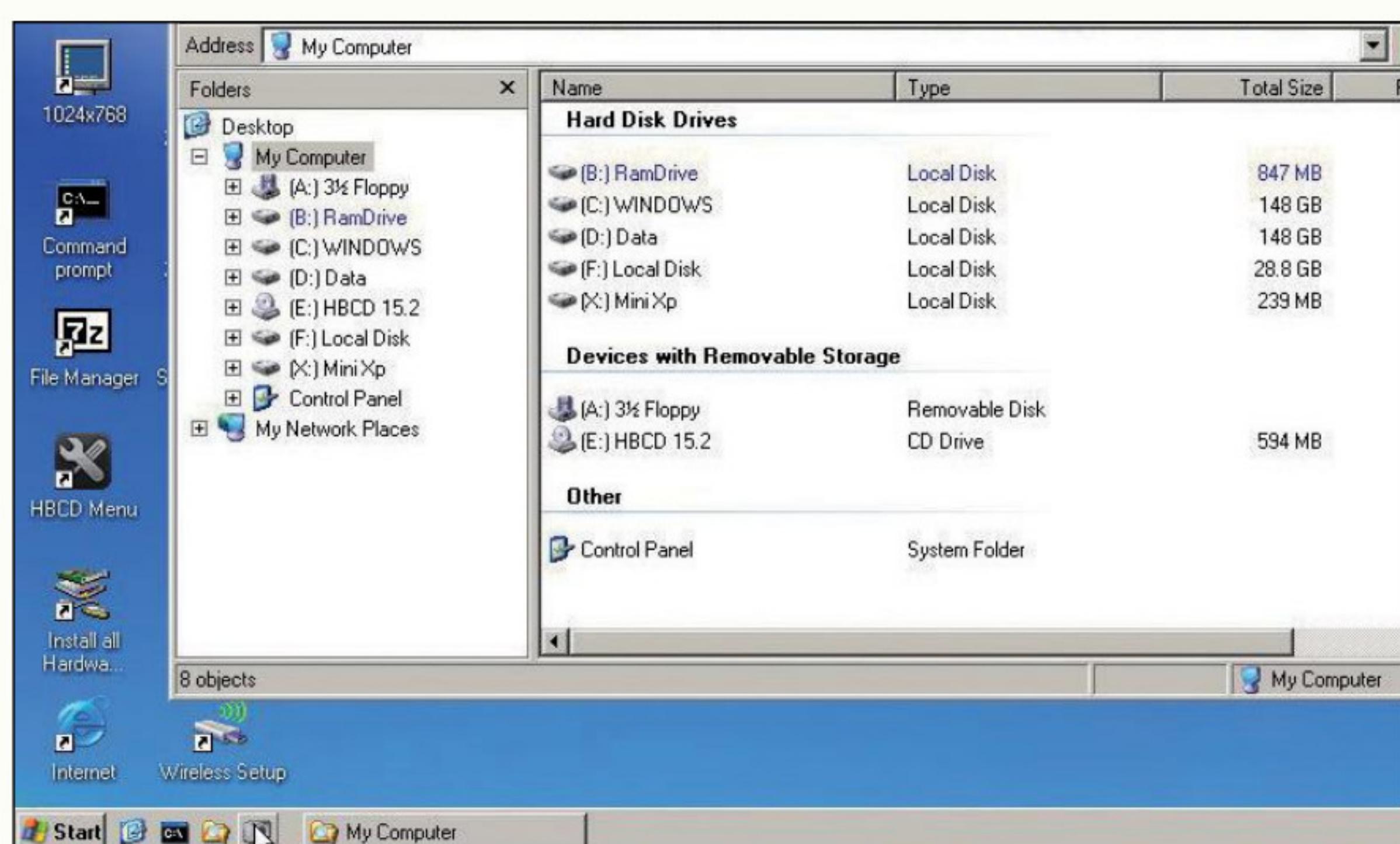
6 LIVE CD INDISPENSABLES POUR LA BIDOUILLE

PRATIQUE



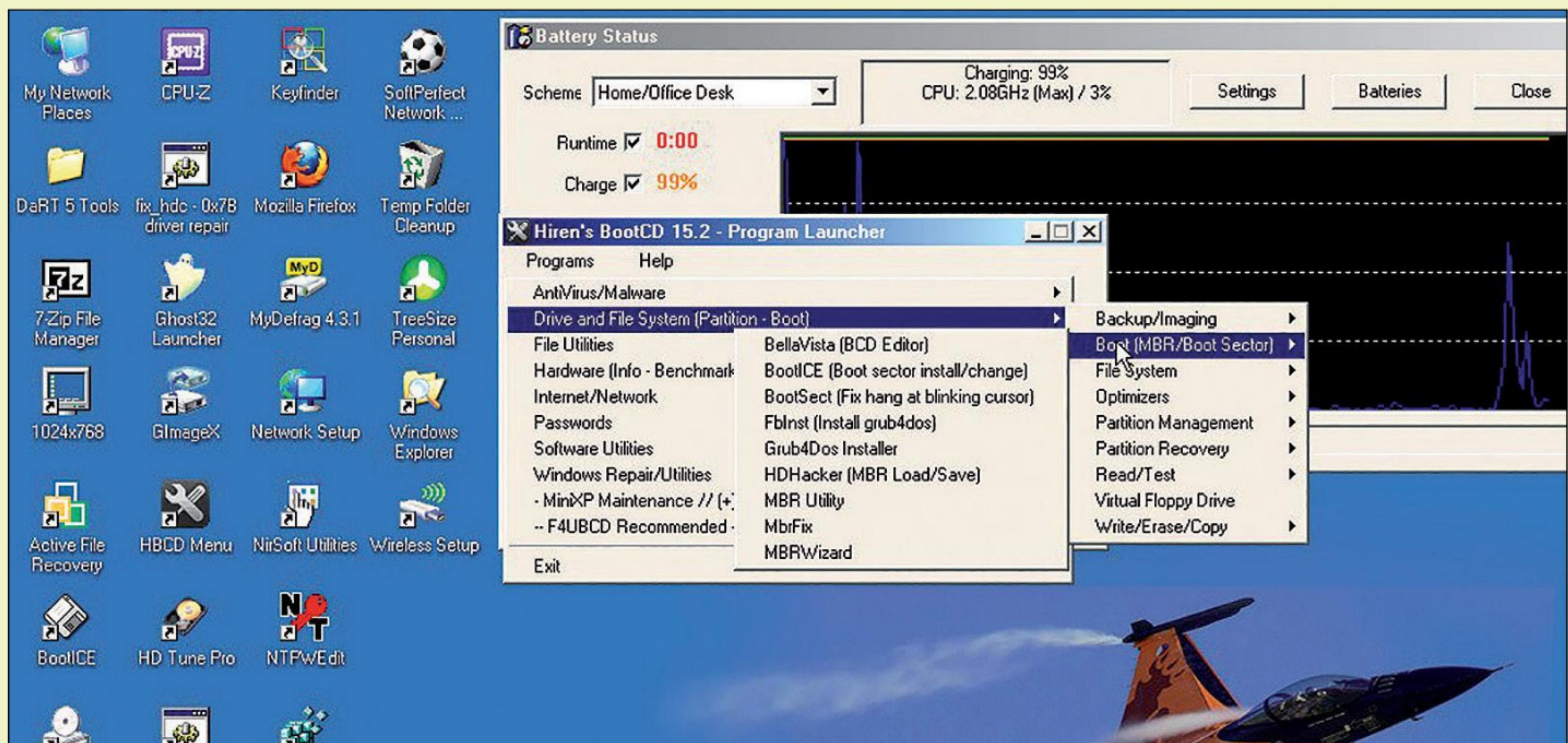
HIREN'S BOOT CD

Hiren's Boot CD fait office de couteau suisse. Il contient énormément de programmes permettant de restaurer un système ou de faire des tests : RAM, processeur, gestionnaire de fichiers, programme DOS, récupération de vos mots de passe, etc. Mais la partie la plus sympa reste son mode MiniXP qui va imiter le fonctionnement d'un système Windows à minima. Vous aurez donc une interface graphique pour lancer tous les programmes contenus dans le CD. Ce mode est aussi idéal pour faire vos sauvegardes de fichiers. Branchez une clé USB ou un disque dur et transférez vos documents ! Attention, il n'est plus mis à jour...



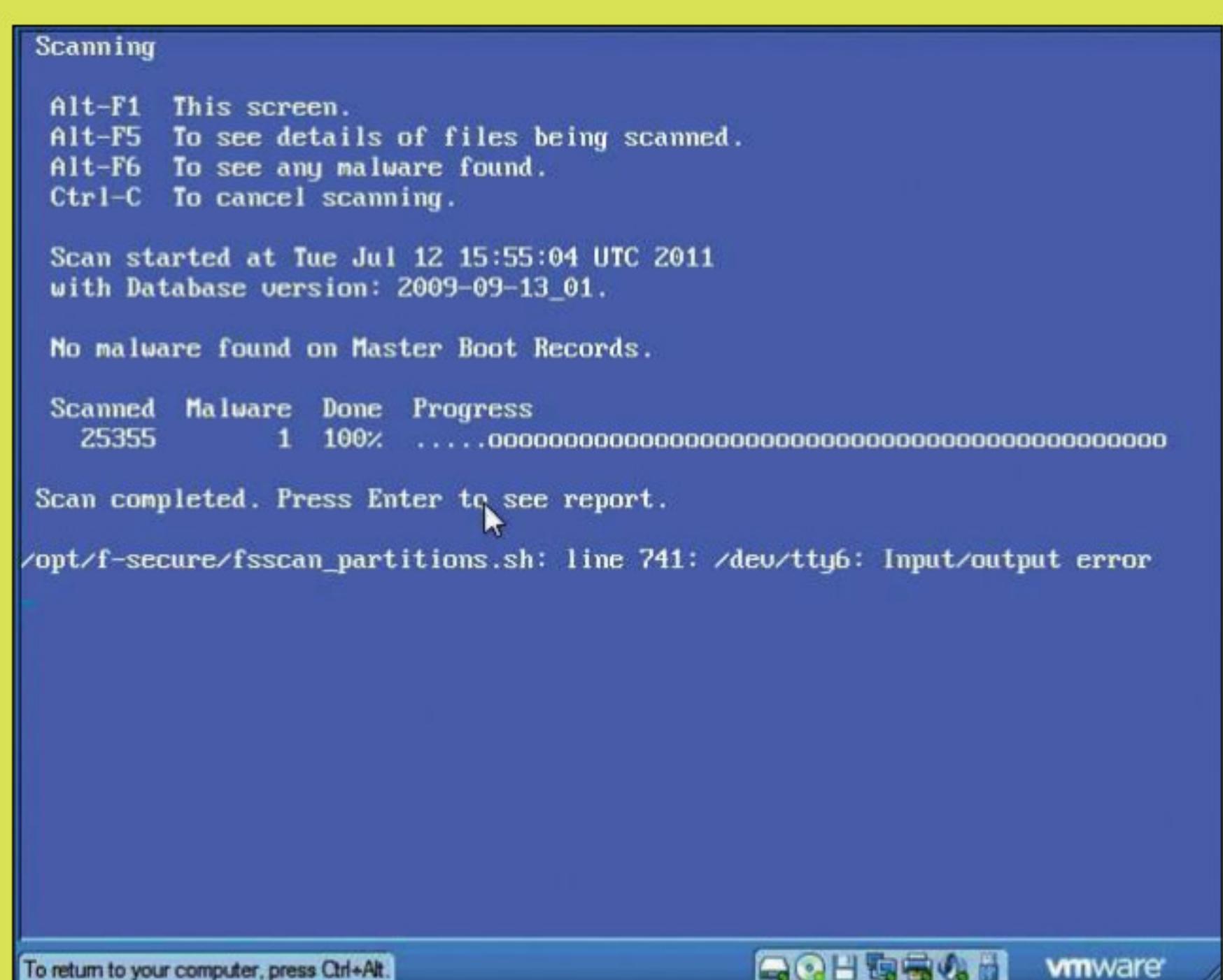
» FALCONFOUR'S ULTIMATE BOOT CD

Le Live CD de FalconFour's est une amélioration de Hiren Boot avec des options de boot plus complètes, mais toujours avec son mode MiniXP. On y trouve des outils pour réparer des partitions, récupérer des données perdues ou des mots de passe, des logiciels d'audit réseau et quelques antivirus. Comme ses camarades, FalconFour's Ultimate Boot CD est disponible en version DVD ou en forme d'ISO à placer sur une clé USB.



» F-SECURE RESCUE DISK

F-Secure Rescue Disk est un autre Live CD qui propose un antivirus très pratique. Pour mettre à jour la base de données virale, nous vous conseillons de brancher le PC en Ethernet à votre box, car le WiFi fonctionne rarement. Lancez ensuite l'analyse. Lorsque les virus seront découverts, n'oubliez pas de choisir systématiquement l'option la moins radicale : il vaut mieux tenter de guérir un fichier contaminé ou de le mettre en quarantaine que de l'effacer...



Scan	Configure and run on-demand scan.
Scan Result	View and process last scan result.
Update	Configure and run update.
Vault	Inspect Windows virus vault.
Mount	Re-mount Windows volumes.
Network	Configure network.
USB	Create bootable USB Flash Drive.
Utilities	Miscellaneous utilities.
Eject	Eject rescue cd.
Reboot	Reboot system.
Shutdown	Shutdown system.
About	Rescue CD and AVG version info.

» AVG RESCUE CD

Et voici l'ultime antivirus ! Au lancement du DVD, choisissez **AVG Rescue CD** et attendez que le contenu se charge dans la RAM. Vous devriez avoir le menu principal avec l'accès à la mise à jour de la base de données virale (**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**. Il faudra alors sélectionner les éléments à scanner. Si vous ne connaissez pas l'origine du problème, optez pour une recherche en profondeur en sélectionnant toutes les options possibles dans **Scan Options**.



HACKING

Live CD

MEDICAT

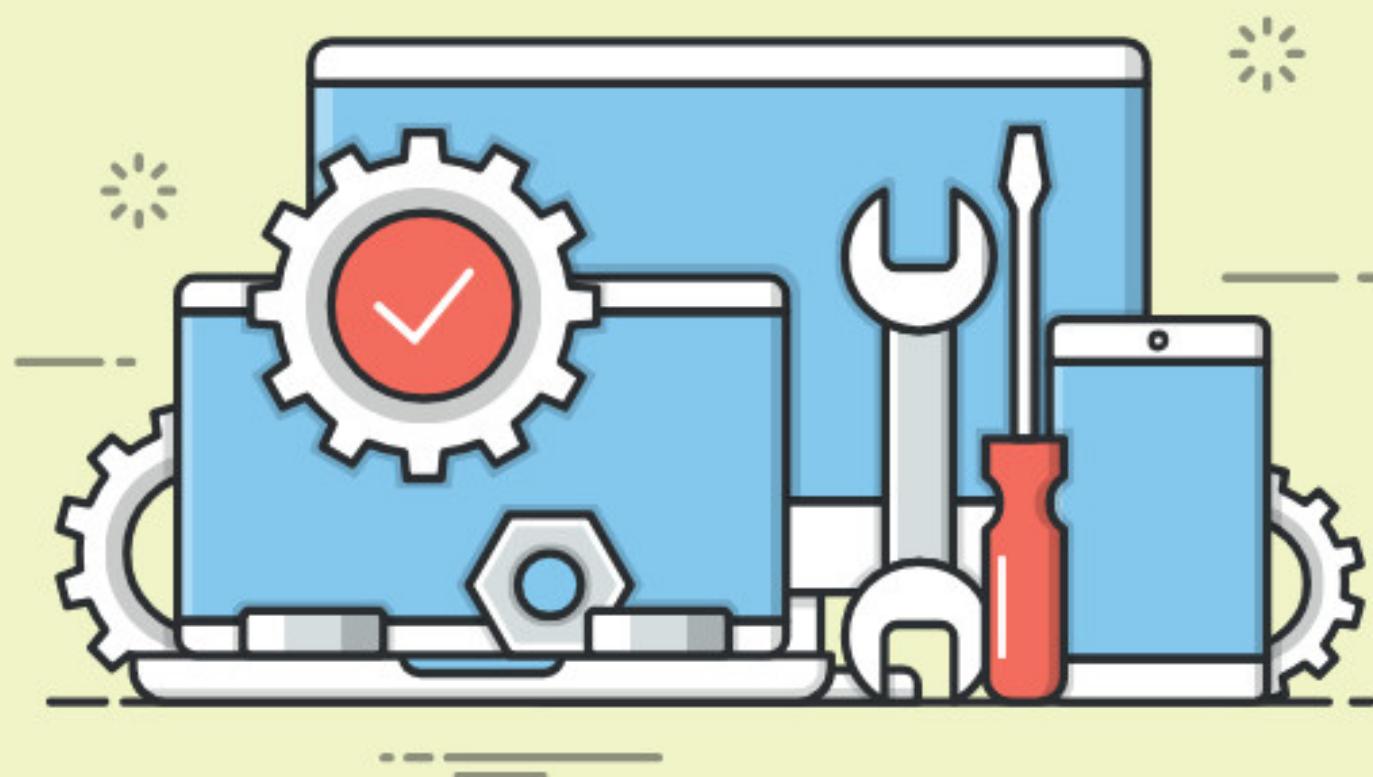
Cette compilation permet de faire la chasse aux virus, de restaurer un Windows bancal, de sauvegarder des données en cas de problème physique ou de mettre un peu d'ordre dans vos partitions. MediCat comprend aussi des outils de diagnostic en tout genre, plusieurs logiciels pour récupérer vos mots de passe. Idéal pour les altruistes qui n'hésitent pas à se déplacer



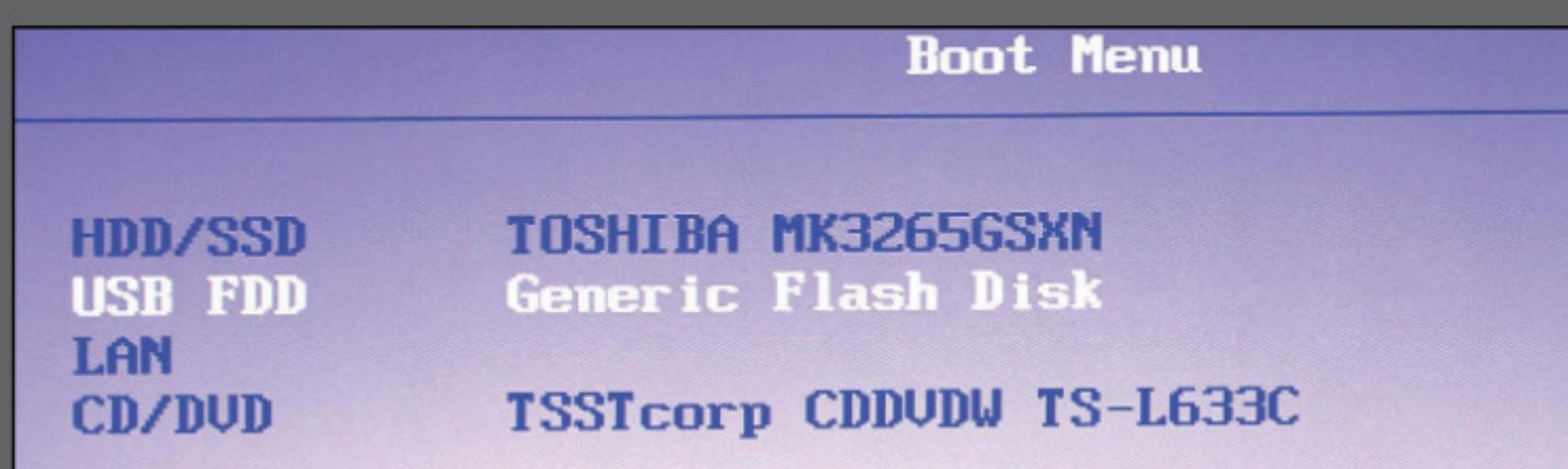
pour réparer l'ordi d'un ami, MediCat est indispensable. La version la plus «lourde» peut aisément prendre place sur une vieille clé USB de 8 Go, raison de plus pour la garder tout le temps avec soi. Là où Hiren's Boot CD donnait l'accès à un Windows XP «light», MediCat propose un Mini Windows 10 et Lubuntu.

ULTIMATE BOOT CD

Ultimate Boot CD est une autre compilation d'outils de dépannage informatique pour Linux ou Windows. Il contient des outils pour le diagnostic, le clonage ainsi que le nettoyage du disque dur. L'utilisateur aura entre autres à sa disposition ViVARD, permettant d'effectuer des tâches de maintenance sur le périphérique de stockage en vue d'optimiser ses performances. On compte aussi des utilitaires de modification mot de passe comme Offline NT Password & Registry Editor qui permet de supprimer le mot de passe d'une session Windows. Enfin, le CD comprend des outils de désinfection : Avast, AVG, ou encore McAfee.

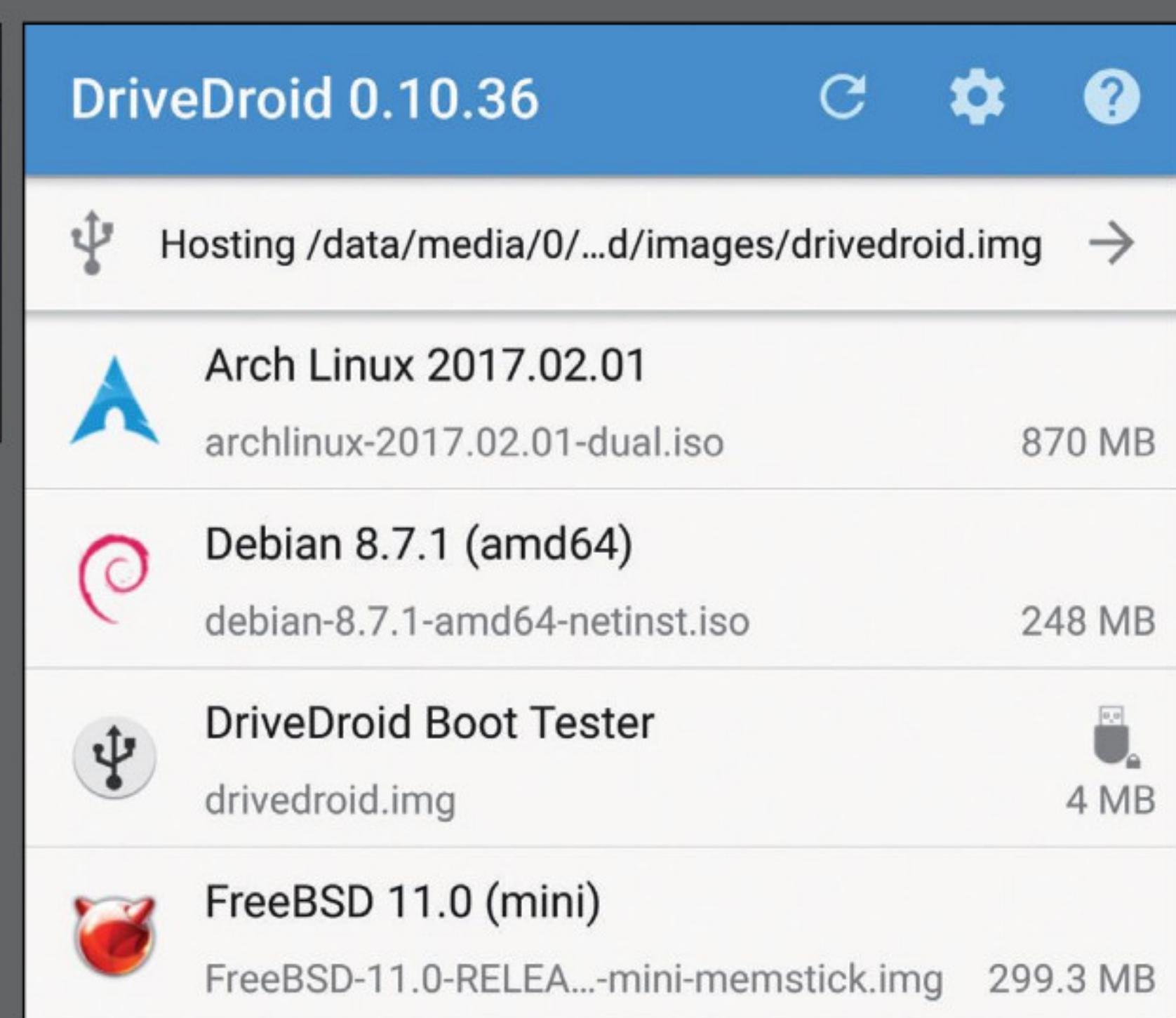


BOOTER SON PC GRÂCE À UN MOBILE AVEC DRIVEDROID



Si vous avez l'utilité de démarrer votre PC ou celui des autres depuis un LiveCD pour réparer, hacker ou changer d'OS, vous allez aimer DriveDroid. Cette appli permet de booter votre PC à partir d'une image (Windows, Linux, etc.) stockée sur votre mobile. Cela peut se révéler pratique dans le cas où vous ne disposez pas de clé USB ou si vous voulez avoir un Kali, un Ubuntu ou un MediCat sous la main, quelle que soit la circonstance. Sélectionnez l'ISO à monter, branchez le câble USB entre votre smartphone et votre PC et c'est parti !

Lien : <https://goo.gl/7FUYIU>



LES DOSSIERS DU **Pirate**

DES DOSSIERS
THÉMATIQUES
COMPLETS

PETIT FORMAT

MINI PRIX

CONCENTRÉ
D'ASTUCES



SERVICES
GRATUITS
100 % ANONYMES

À DÉCOUVRIR
EN KIOSQUES



Actuellement #Guide pratique



HACKING

00110011
10100100110
00110010

DECRYPTAGE

POUR QUI ?
Pour les curieux !

POUR QUOI FAIRE ?
Pour mieux comprendre le mécanisme de DoS/DDoS

QU'EST-CE QUE L'ATTaque DOS ?

L'attaque DDoS (pour Distributed Denial of Service ou «déni de service» en français) vise à saturer de requêtes un site pour qu'il ne soit plus en mesure de répondre. Voyons comment cela fonctionne et comment s'en protéger...

Merci à la Blackbird Team pour cet article !

Une attaque par déni de service (denial of service attack, d'où l'abréviation DoS) est une attaque ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes de l'utiliser. Il peut s'agir de :

- L'inondation d'un réseau afin d'empêcher son fonctionnement ;
- La perturbation des connexions entre deux machines, empêchant l'accès à un service particulier ;
- L'obstruction d'accès à un service ou à une personne en particulier.

- L'attaque par déni de service peut ainsi bloquer un serveur de fichiers, rendre impossible l'accès à un serveur Web, empêcher la distribution de courriel dans une entreprise ou rendre indisponible un site internet.

C'EST QUOI LE D EN PLUS DANS DDOS ?

Et concernant le DDoS ? Prenez l'acronyme précédent et rajoutez «Distributed» c'est à dire «distribué». Qu'est-ce que cela change ? Eh bien au lieu d'utiliser une seule machine (peu efficace), plusieurs machines vont s'investir dans l'opération. Avec, ou sans le consentement de

leurs propriétaires. Il existe en effet deux types de DDoS :

- Les attaques orchestrées par des hacktivistes qui utilisent la fonction Hivemind de LOIC (un logiciel permettant de faire des attaque DDoS de manière très simple) : vous mettez votre machine à contribution, ou alors vous participez de votre côté comme un grand.
- Les attaques DDoS qui utilisent des Botnets. Ce sont des réseaux de machines contrôlées par un hacker (ou plus souvent par une équipe) qui lancent des attaques DDoS sans que le propriétaire de ladite machine soit au courant... Ces hackers vont alors «emprunter» plusieurs machines pour être plus efficaces. Le plus grand Botnet de l'histoire a atteint 500 000 machines...

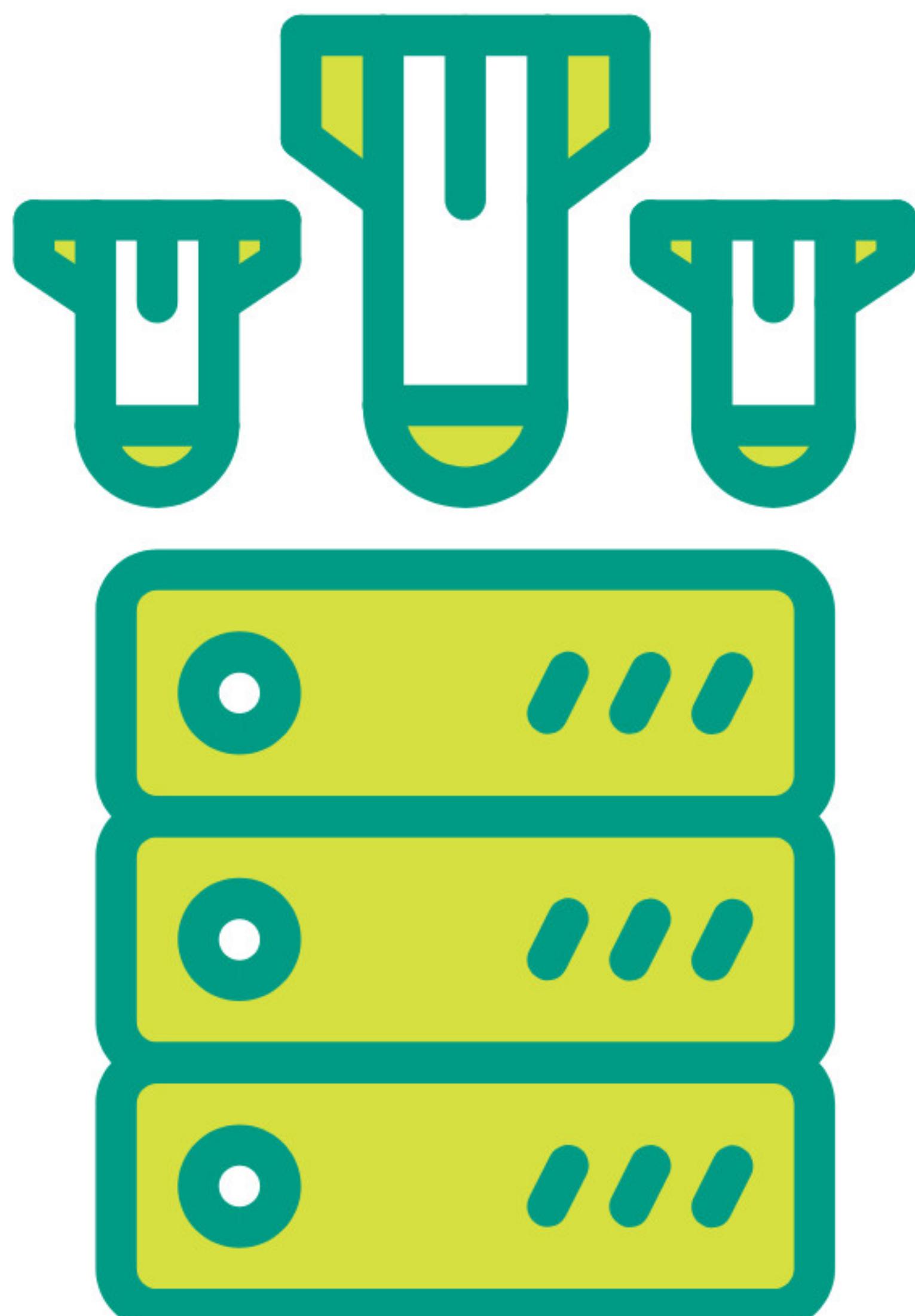
COMMENT SE PROTÉGER

Nous avons bien identifié le problème des attaques DDoS, mais existe-t-il des moyens de se protéger ? Outre les recommandations habituelles en matière de sécurité informatique, voici quelques bonnes pratiques utiles contre les attaques DDoS :

- Utiliser des pare-feux et des répartiteurs de charge pour contribuer à absorber certaines attaques DDoS
- Utiliser des équipements de filtrage spécifiques aux attaques DDoS (filtrage par liste blanche ou liste noire)
- Utiliser un filtrage effectué par un opérateur de transit
- Utiliser les protections offertes par les hébergeurs.
- Utiliser un CDN, pour limiter sa vulnérabilité vis à vis des autres localisations géographiques.
- Utiliser les services de protection dédiés offerts par les fournisseurs cloud.

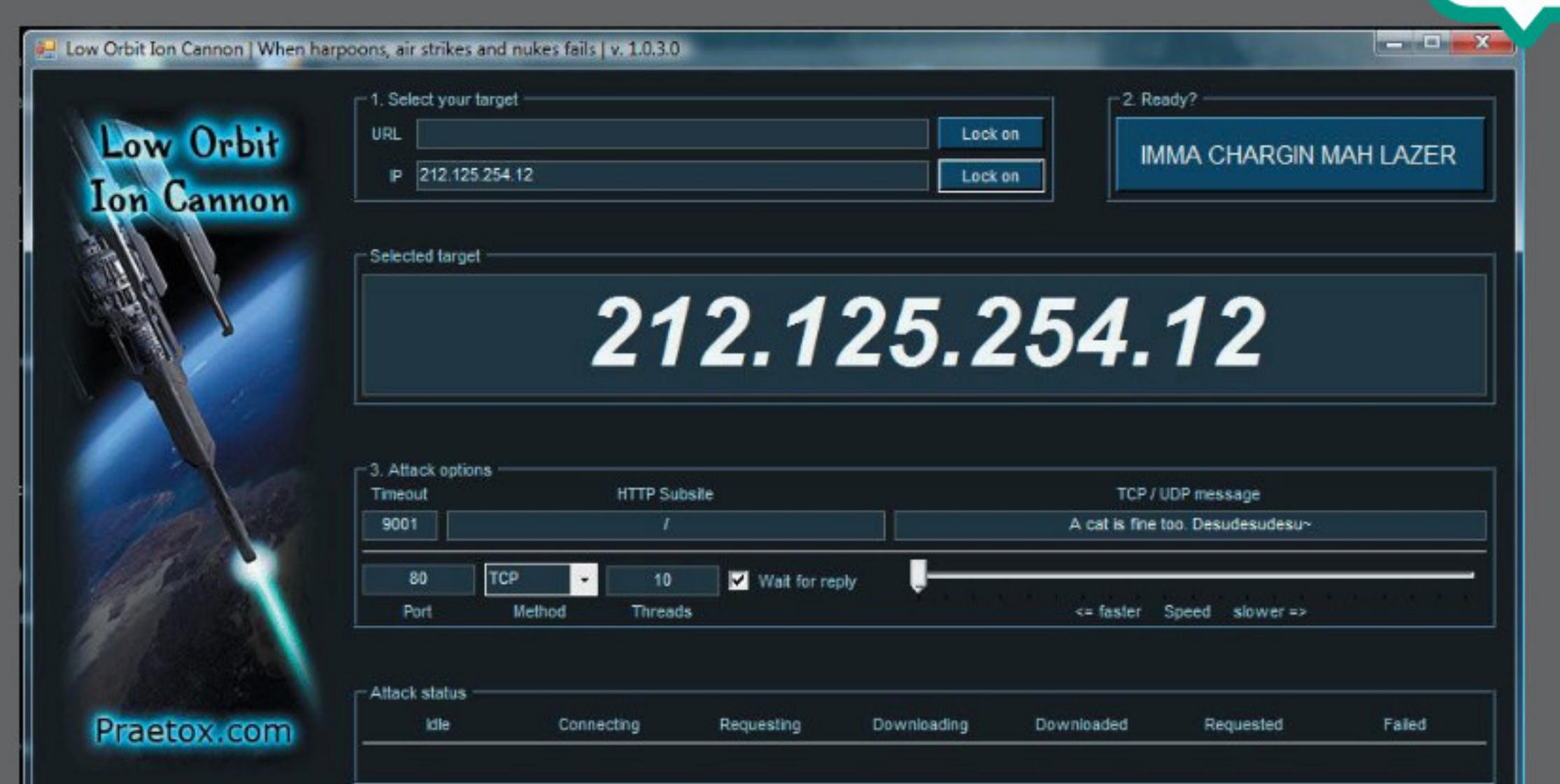
QUELQUES OUTILS INDISPENSABLES...

<https://github.com/adsfdasdf/tros>
 contenant (Akbar, Sadattack, etc.)
<https://github.com/zanyarjamal/xerxes>
<https://github.com/0x01h/pyddoz>



LE LOGICIEL LOIC

L'opération Payback a eu lieu fin 2010 et début 2011. Il s'agissait pour des hacktivistes proches des Anonymous de rendre la monnaie de leur pièce aux majors et à ceux qui les protègent : MPAA (Motion Picture Association of America) et RIAA (Recording Industry Association of America) en tête. L'originalité de Payback résidait dans son système d'attaque. Au lieu de s'en prendre à un serveur avec une seule machine ou une grosse quantité de PC «zombies», le groupe de hackers a préféré se bâtir une petite communauté de «soldats». Et pour que chacun puisse prendre part à l'attaque Anonymous met à disposition un programme répondant au doux nom de LOIC (comme le «Low Orbit Ion Cannon» de L'Empire contre-attaque). Pour utiliser ce logiciel, pas la peine d'être un pro de la sécurité informatique ou un pirate aguerri, il suffit de rentrer une adresse IP et de cliquer sur un bouton à l'heure du «rendez-vous».





HACKING

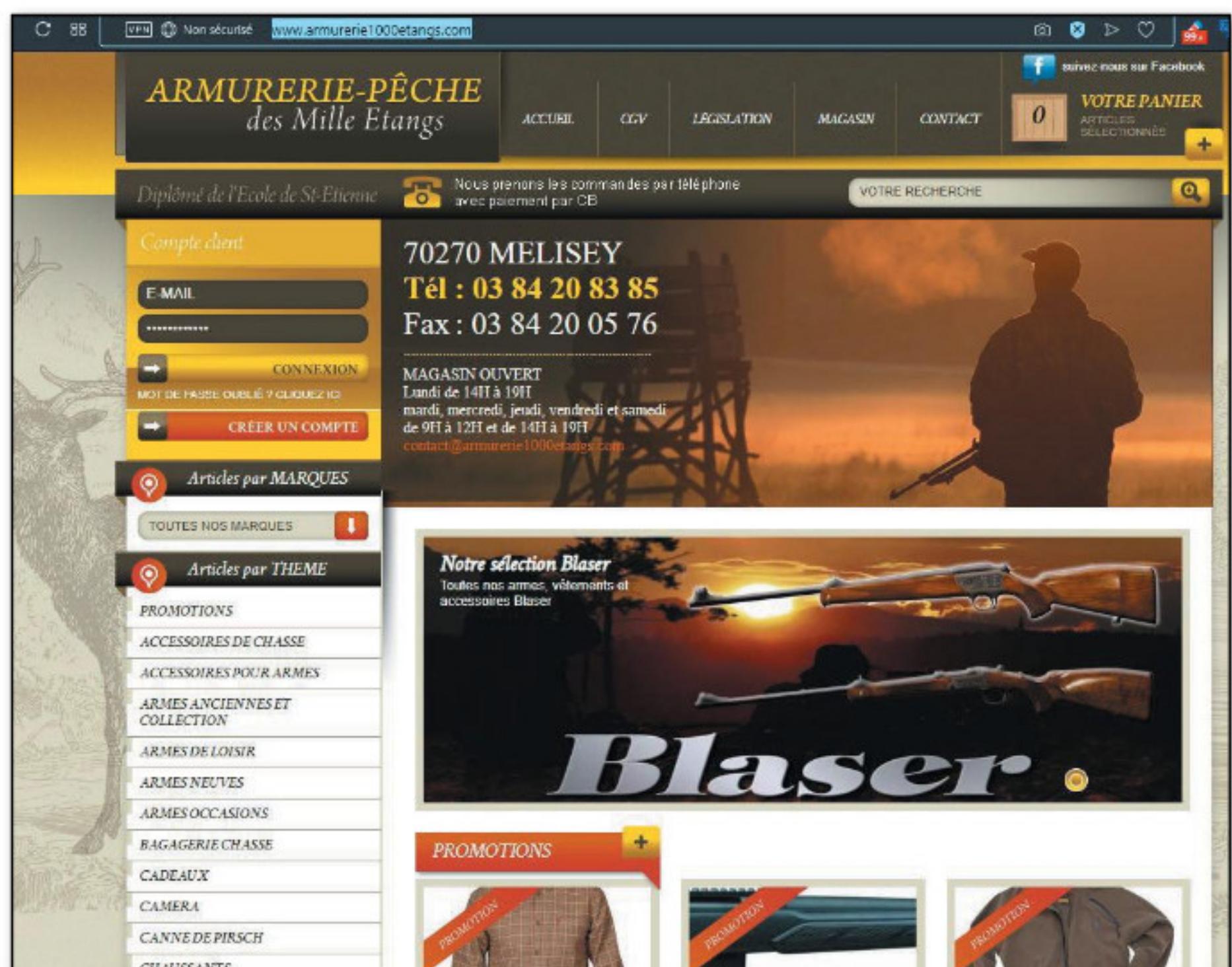
Attaque

PRATIQUE
▼

DÉMONSTRATION D'UNE ATTAQUE DOS

01 > LE CHOIX DU SITE

Selectionnez un site qui est sous la forme de « http », c'est à dire sans chiffrement SSL. Dans notre démo nous avons sélectionné un site test. Attention, cette démonstration n'a pas pour but d'attaquer un site, il ne s'agit que d'un exemple. Nous vous invitons à tester cette démonstration sur votre propre site.

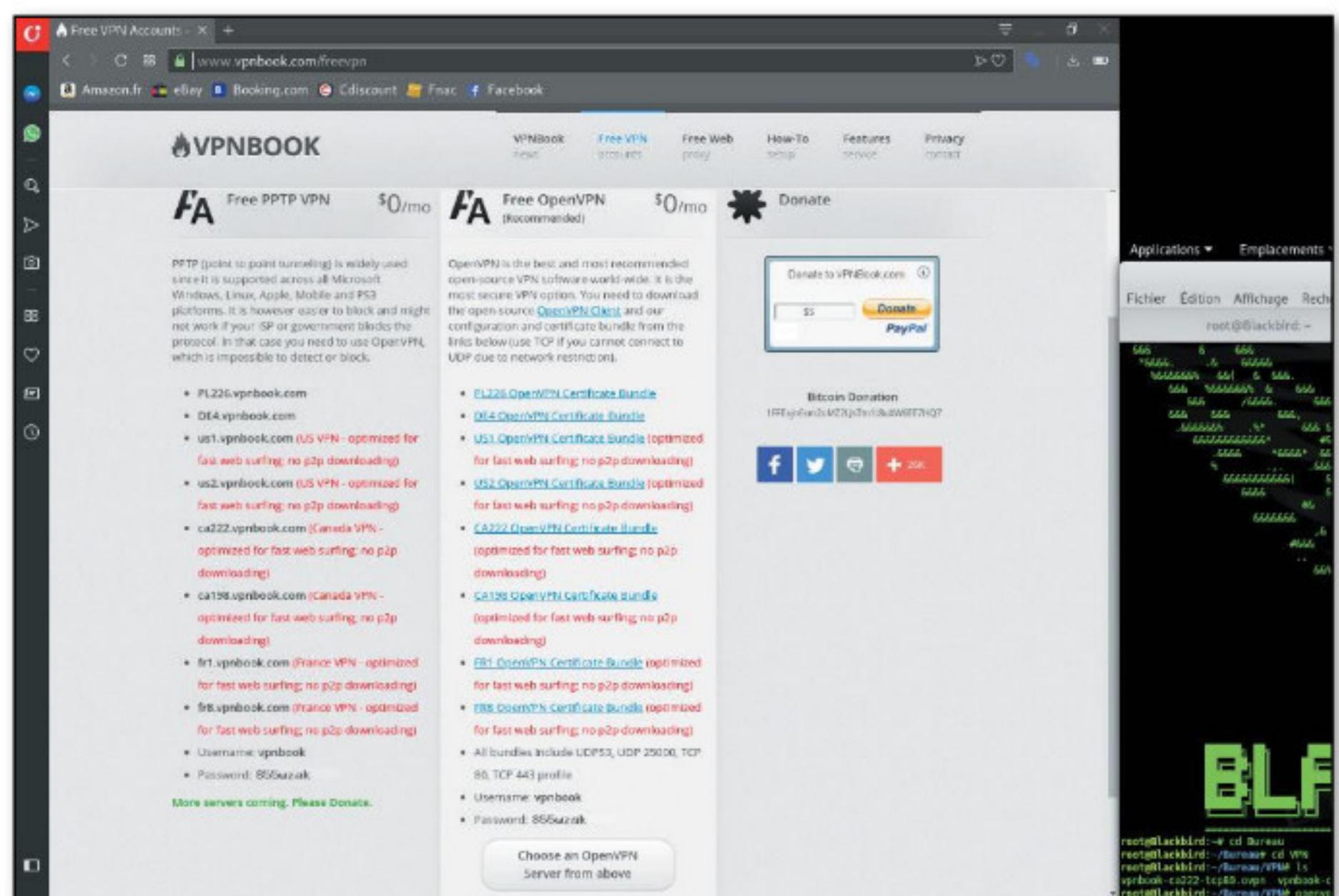


02 > LANCEMENT DU SCRIPT

Masquer notre adresse IP, nous rendra moins visibles sur le net. Ouvrez un terminal et dirigez-vous vers l'emplacement de votre script pour le DoS/DDoS. Dans notre cas nous avons déjà un dossier contenant notre outil. Dans notre script il suffit d'ajouter l'URL du site pour débuter l'attaque.

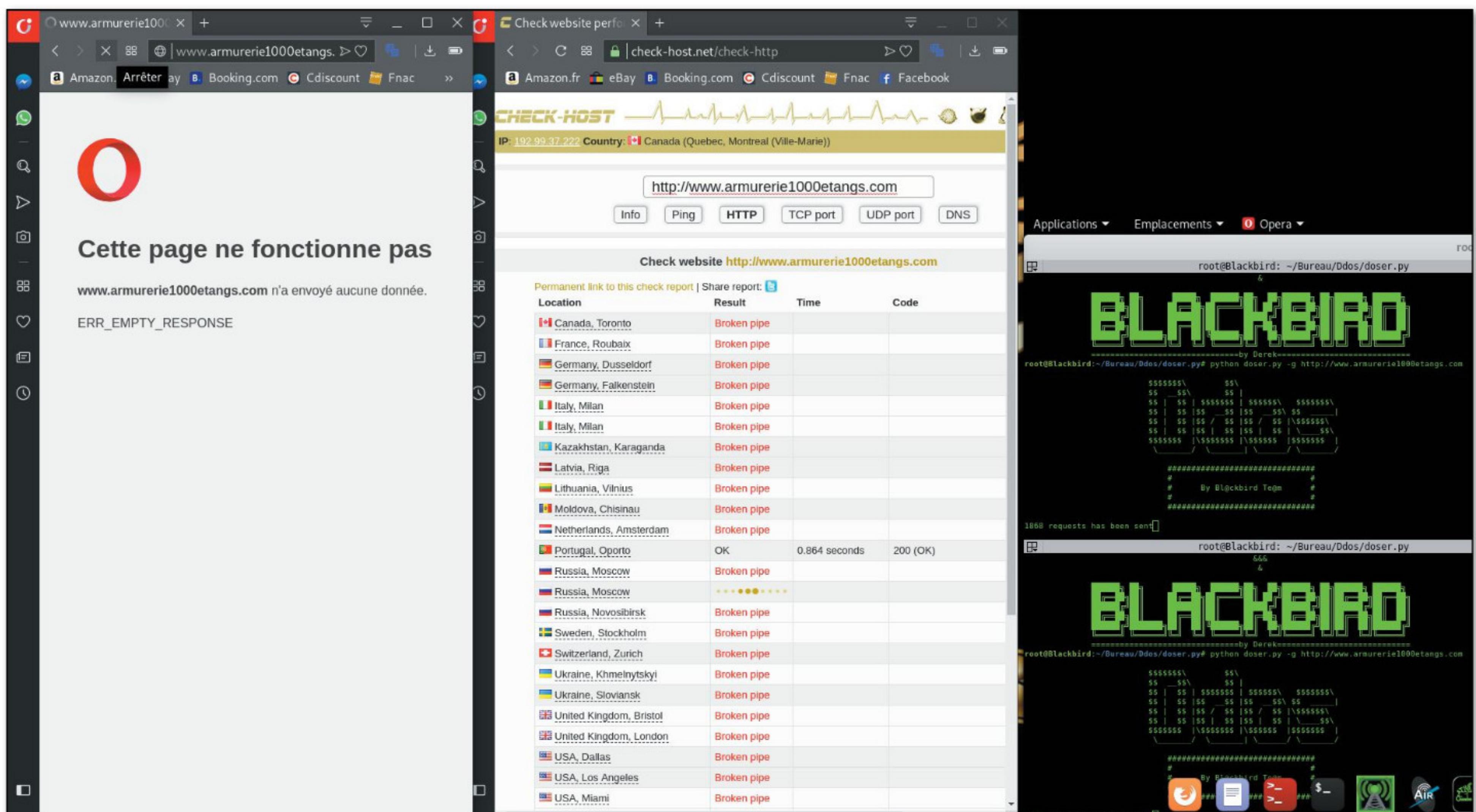
Dans le terminal je tape la commande suivante :

Python doser.py -g http://(nom du site)



03 > SUCCÈS DE L'ATTAQUE

Pour plus d'efficacité, nous allons utiliser plusieurs fenêtres et ouvrir sur le navigateur le check-host. Vérifions maintenant si le site répond toujours. La connexion est impossible avec le site.





ÉCRAN CASSÉ : QUE FAIRE AVEC VOTRE APPAREIL ANDROID ?

Vous avez laissé tomber votre smartphone et votre fidèle compagnon à l'écran complètement cassé ? Certes ça fait mal de devoir se séparer d'un appareil à plusieurs centaines d'euros, mais le pire ce serait la perte des données qu'il contient. Voyons comment récupérer vos photos, vidéos et autres documents...

Au moment de récupérer vos données, il y a 2 cas de figure : l'écran est encore réactif et partiellement fonctionnel ou l'écran ne fonctionne plus ou est trop «noir» pour voir quoi que ce soit. Il faut savoir que lorsqu'un écran est cassé son état de santé peut vite empirer : il ne faut pas tarder à intervenir. Il faut pouvoir en premier lieu le déverrouiller. Si vous avez un capteur d'empreintes au dos, pas de problème, mais si vous utilisez un schéma de déverrouillage ou un code PIN et que l'écran ne répond plus, il va falloir gruger en se servant de l'option OTG du mobile. OTG signifie «On The Go» il s'agit d'une technologie appelée aussi «USB host» qui permet d'utiliser le port USB de votre smartphone comme celui d'un PC. Votre port USB est à la fois une «sortie», mais aussi une «entrée» permettant pas mal de choses intéressantes comme connecter un disque dur, une clé USB, une manette ou une imprimante. Ici nous allons nous en servir pour brancher une souris USB sur votre smartphone. Pour cela, il faudra un adaptateur micro USB ou USB-C (selon votre modèle de smartphone) vers USB type A femelle. Ce type de gadget coûte moins de 8€ et cela pourra vous servir pour d'autres choses à l'avenir...

POUR QUI ?

Pour les maladroits et ceux qui connaissent des maladroits

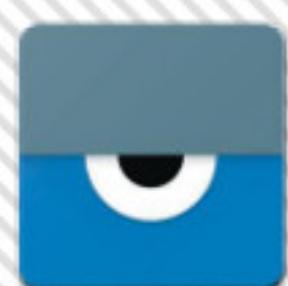
POUR QUOI FAIRE ?

Récupérer le maximum de données d'un smartphone





HACKING



INFOS [Vysor]

Où le trouver ? [https://frama.link/Dza_PNPL]

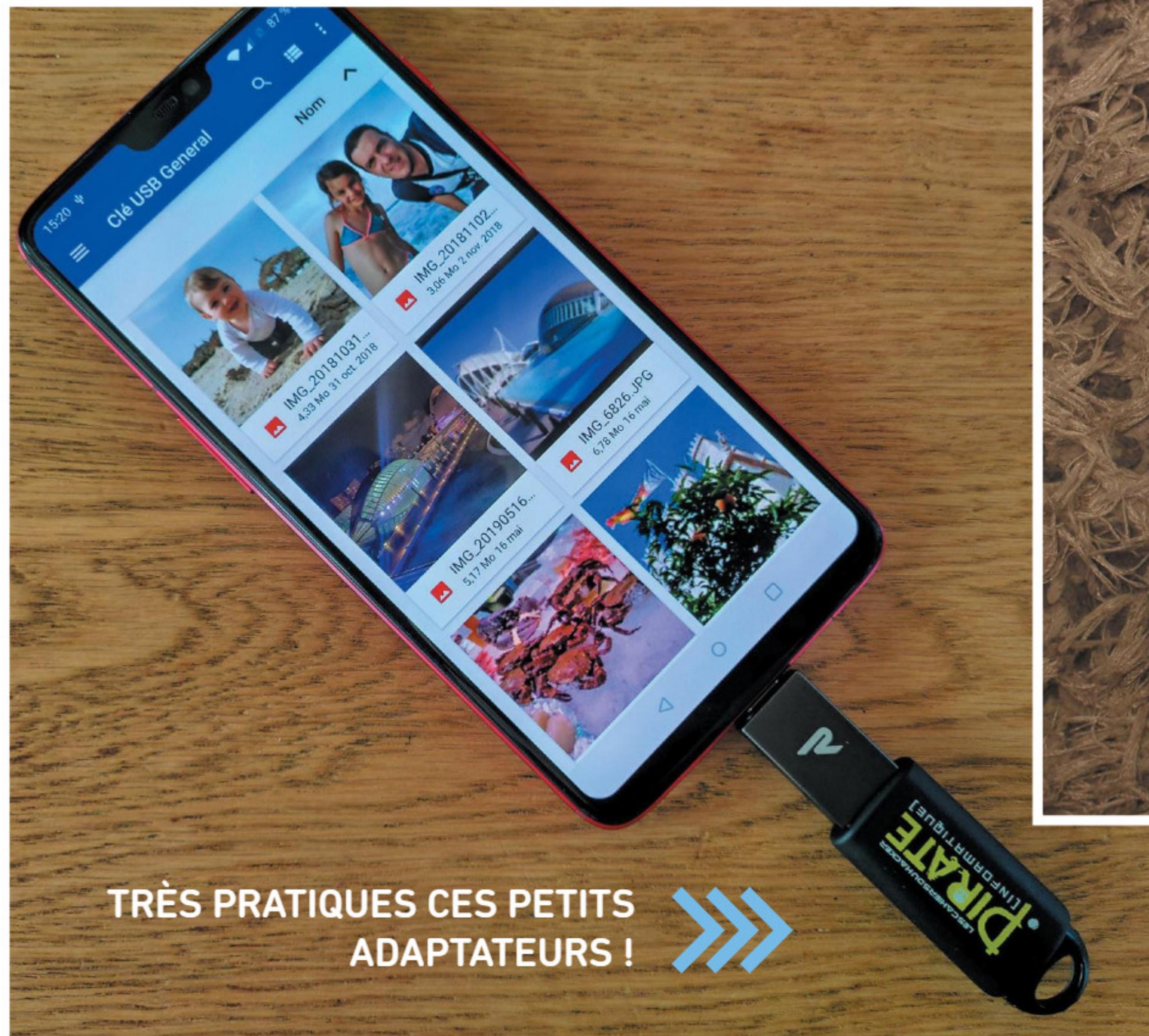
Difficulté : 🧟🧟🧟

COMMENT RÉCUPÉRER LES DONNÉES SUR UN PC ?

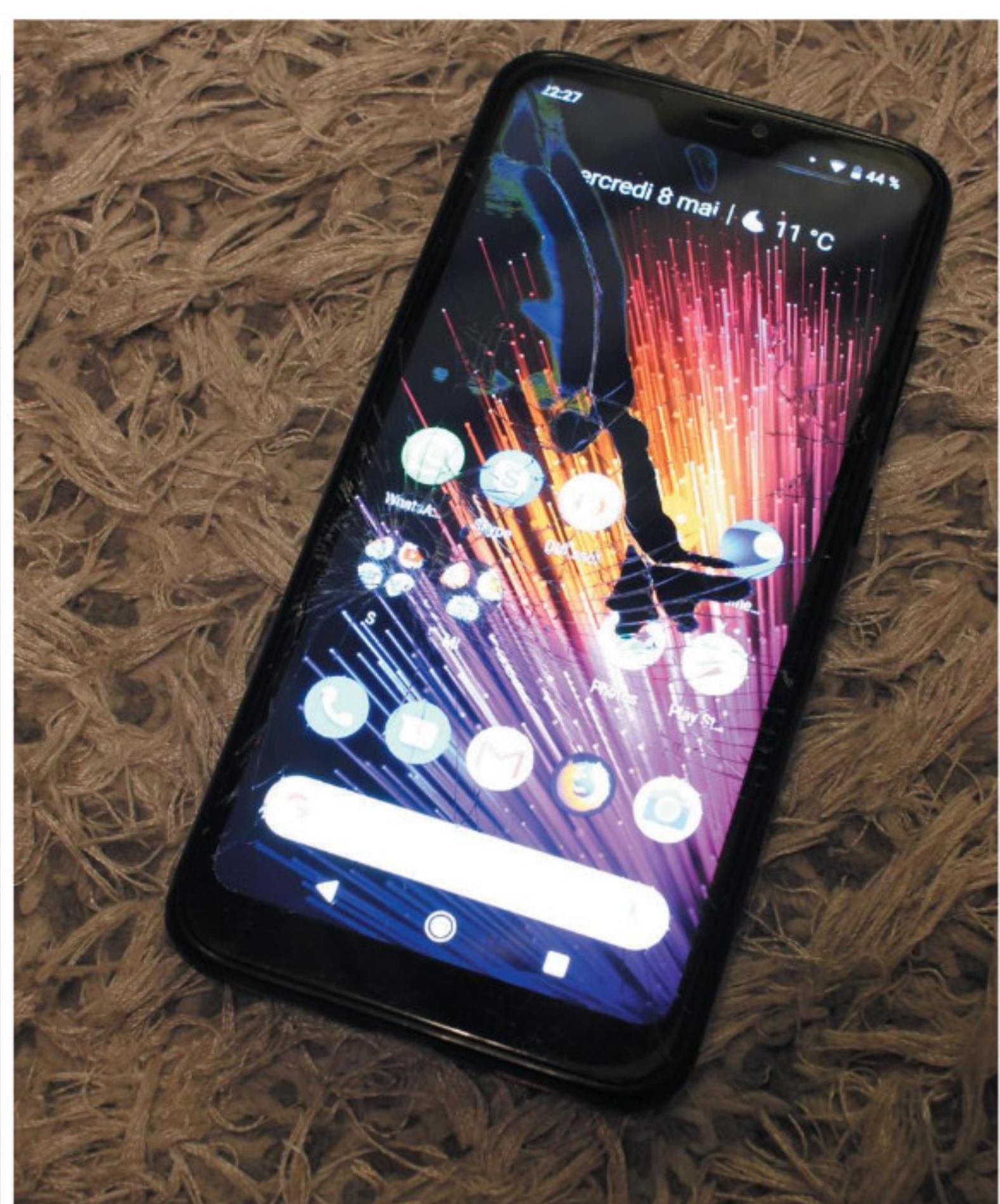


01 > L'ÉCRAN RÉPOND COMPLÈTEMENT OU PARTIELLEMENT

Une fois déverrouillé, vous allez pouvoir brancher le smartphone à votre ordinateur. Il faudra ensuite activer l'option de **Transfert de fichiers**. C'est un peu délicat, car c'est encore sur le smartphone qu'il faudra agir et c'est peut-être encore dans un endroit de l'écran qui ne répond plus ou n'est plus visible. Aidez-vous de l'astuce avec la souris si vous n'y arrivez pas depuis l'écran. Attention, il vous faudra un hub USB pour brancher la souris + le câble de connexion au PC. Une fois que l'appareil est déverrouillé et que l'option de transfert de fichier est activée, vous pouvez transférer vos fichiers sur votre ordinateur. Les photos sont dans le dossier DCIM, mais vous pouvez aussi tout transférer et faire le tri après...

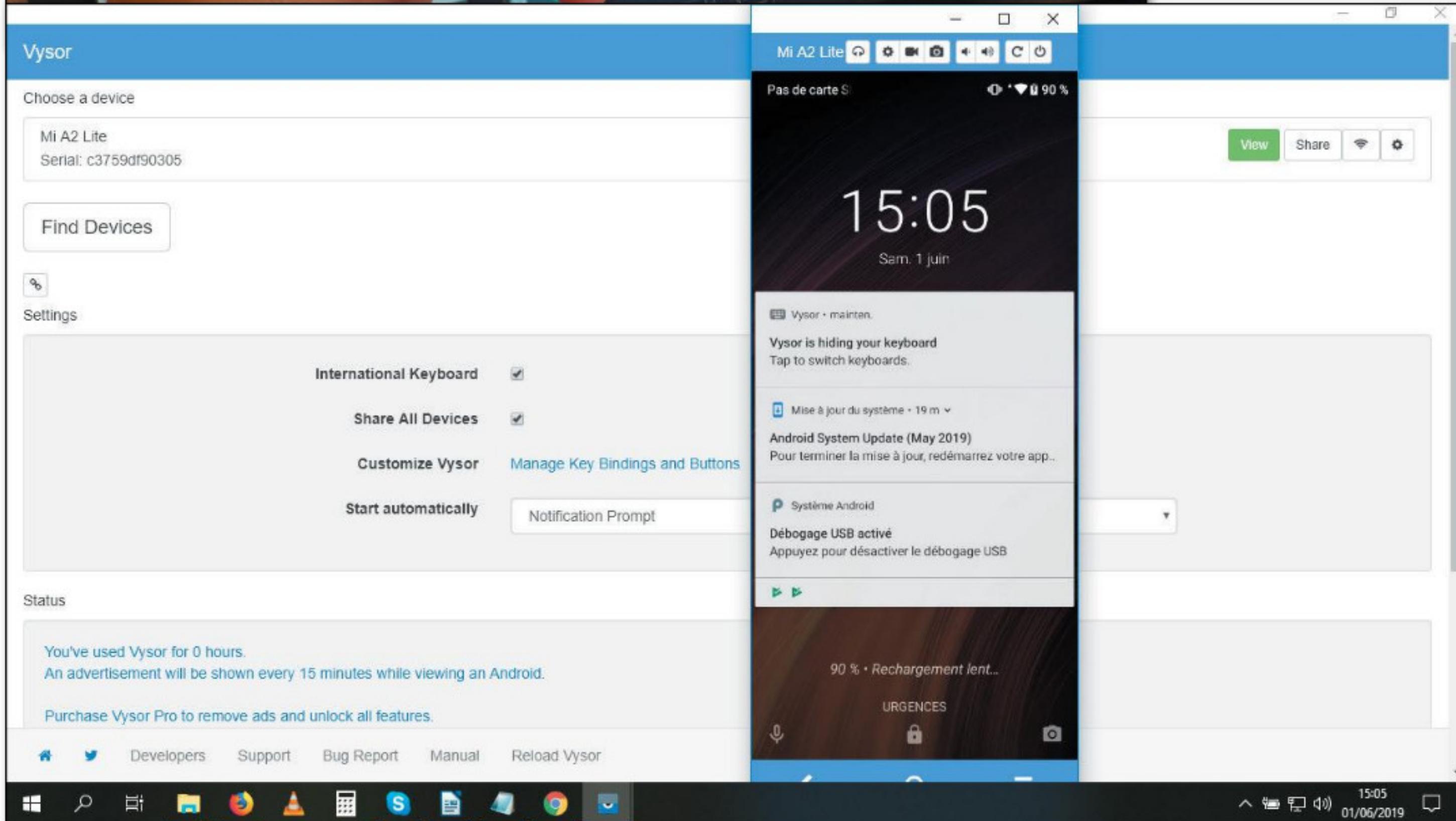


TRÈS PRATIQUES CES PETITS ADAPTATEURS !



CE XIAOMI MI A2 LITE N'A PAS RÉSISTÉ À UNE MAUVAISE CHUTE



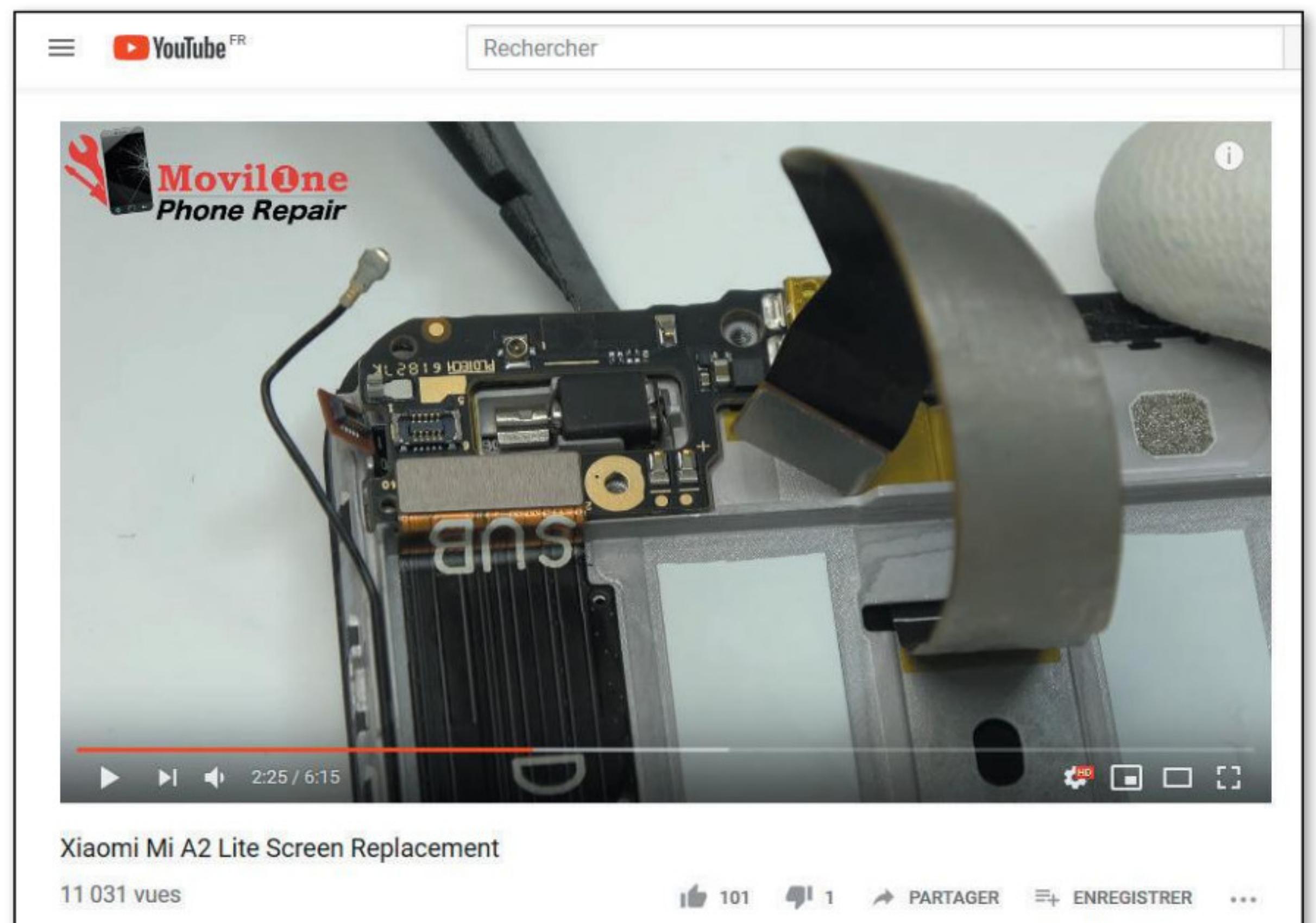


02 > L'ÉCRAN EST COMPLÈTEMENT MORT !

Si votre écran est complètement noir, c'est un peu plus compliqué. En réalité, c'est presque impossible si vous n'avez pas activé le mode débogage USB avant la chute malencontreuse. Pour activer ce mode, il faut d'abord afficher les **Options développeurs** qui sont... cachées. Allez dans **Paramètres**, puis dans **À propos du téléphone** (ou **Système**>**À propos du téléphone**), trouvez le **Numéro de build** (ou **de version**) et tapez dessus 7 fois. Vous verrez un message indiquant que les **Options pour développeurs** sont disponibles. Vous les trouverez dans **Système**. Parcourez-les pour activer le mode **Débogage USB**. Si ce mode est activé, c'est gagné ! Il suffit de télécharger l'extension Chrome Vysor, de connecter votre appareil au PC et de faire **Lancer l'appli** puis **Find Device**. Sélectionnez votre appareil et en quelques secondes vous aurez une représentation graphique de votre appareil sur l'écran de votre PC : vous allez pouvoir entrer le schéma de déverrouillage ou votre code PIN, puis activer le mode de partage de fichier pour enfin récupérer vos fichiers !

03 > ET LA RÉPARATION ?

Si Vysor n'a rien pu faire pour vous, l'ultime solution consiste à réparer ou faire réparer votre smartphone. C'est devenu de plus en plus compliqué, car les fabricants ne pensent pas vraiment à ce cas de figure en imaginant leurs appareils : il faut souvent démonter tout l'appareil pour remplacer la dalle. Demandez un devis auprès du constructeur et faites aussi jouer la concurrence ! Si vous voulez le faire vous-même, il faudra vous équiper de quelques outils et d'une bonne vidéo de tuto. La chaîne YouTube MovilOne Phone Repair en propose plein ! Un écran est cher, mais moins cher que votre appareil. À vous de peser le pour et le contre. L'avantage c'est que vous n'aurez pas à racheter un smartphone neuf et vous récupérerez toutes vos données. N'oubliez pas d'expliquer ce détail à votre réparateur !





HACKING



POUR QUI ?

Pour les personnes qui veulent tester leur réseau

POUR QUOI FAIRE ?

Tenter de s'introduire dans un réseau WiFi

WIFITE : INTRUSION DANS UN RÉSEAU SANS FIL

LEXIQUE

*KALI LINUX :

Anciennement 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, etc.

*PENTESTING :

Mot valise réunissant «penetration» et «testing». Il s'agit de tester les forces et faiblesses d'un ordinateur, d'un réseau, d'un site ou d'une base de données avec des logiciels spécialisés. Bien sûr, ces derniers peuvent être utilisés à des fins moins nobles.



WiFite (à ne pas confondre avec Wii Fit, le célèbre périphérique qui te fait croire que tu fais du sport) est un logiciel inclus dans Kali Linux et le moins qu'on puisse dire c'est qu'il ne fait pas de détails. Alors qu'il est assez complexe d'utiliser Aircrack,

Dans cet article, nous allons voir comment utiliser WiFite, un script particulièrement malin qui va tester les résistances de votre propre réseau Wi-Fi. Ce logiciel n'existe malheureusement pas sous Windows, il va donc falloir utiliser Linux. La distribution Kali semble donc toute indiquée...

en particulier avec le WPA, WiFite automatise les tests de pénétration. Sous réserve d'avoir une carte Wi-Fi compatible avec l'injection de paquet (voir notre encadré), WiFite va tester les réseaux des environs et tenter de s'y introduire qu'ils soient protégés en WEP ou WPA.

LOGICIEL TOUT TERRAIN ET TERRIBLEMENT FLIPPANT

Plus fort, il va même tenter de forcer l'entrée des box ou routeurs protégés par WPS. Le plus beau, c'est que tout se fait presque automatiquement. Les puristes diront que c'est un logiciel de script kiddies, mais il s'agit ici de vérifier la sécurité de son réseau. Si ce dernier est perméable à WiFie c'est que n'importe qui peut y avoir accès. Il sera donc temps de blinder la sécurité...

```
root@kali: ~
Fichier Édition Affichage Rechercher Terminal Aide
WPA:
--wpa Only target WPA networks (works with --wps --wep).
--wpat WPAT Time to wait for WPA attack to complete (seconds).
--wpadt WPADT Time to wait between sending deauth packets (seconds)
--strip Strip handshake using tshark or pyrit.
--crack Crack WPA handshakes using [dic] wordlist file.
--dict DIC Specify dictionary to use when cracking WPA.
--aircrack Verify handshake using aircrack.
--pyrit Verify handshake using pyrit.
--tshark Verify handshake using tshark.
--cowpatty Verify handshake using cowpatty.

WEP:
--wep Only target WEP networks.
--pps PPS Set the number of packets per second to inject.
--wept WEPT Sec to wait for each attack, 0 implies endless.
--chopchop Use chopchop attack.
--arpreplay Use arpreplay attack.
--fragment Use fragmentation attack.
--caffelatte Use caffe-latte attack.
--p0841 Use P0842 attack.
--hirte Use hirte attack.
--nofakeauth Stop attack if fake authentication fails.
--wepca WEPCA Start cracking when number of IVs surpass [n].
```

```
root@kali: ~
Fichier Édition Affichage Rechercher Terminal Aide
WPA:
--wpa Only target WPA networks (works with --wps --wep).
--wpat WPAT Time to wait for WPA attack to complete (seconds).
--wpadt WPADT Time to wait between sending deauth packets (seconds)
--strip Strip handshake using tshark or pyrit.
--crack Crack WPA handshakes using [dic] wordlist file.
--dict DIC Specify dictionary to use when cracking WPA.
--aircrack Verify handshake using aircrack.
--pyrit Verify handshake using pyrit.
--tshark Verify handshake using tshark.
--cowpatty Verify handshake using cowpatty.

WEP:
--wep Only target WEP networks.
--pps PPS Set the number of packets per second to inject.
--wept WEPT Sec to wait for each attack, 0 implies endless.
--chopchop Use chopchop attack.
--arpreplay Use arpreplay attack.
--fragment Use fragmentation attack.
--caffelatte Use caffe-latte attack.
--p0841 Use P0842 attack.
--hirte Use hirte attack.
--nofakeauth Stop attack if fake authentication fails.
--wepca WEPCA Start cracking when number of IVs surpass [n].
```

VOTRE CARTE WI-FI EST-ELLE COMPATIBLE AVEC L'INJECTION DE PAQUETS ?

Attention pour que notre démonstration fonctionne, il faudra absolument que votre carte ou clé Wi-Fi soit compatible avec la méthode d'injection de paquets. Dans Kali, ouvrez un Terminal et faites **service network-manager stop** puis **aireplay-ng -9 wlan0**. 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. Si vous avez un autre message, rien ne vous empêche d'essayer WiFie quand même...

LE SYSTÈME WPS ET SES FAILLES



Le système WPS équipé par certains routeurs ou box permet de facilement se connecter à un réseau sans fil sans avoir à taper une longue clé d'authentification : pression sur un bouton physique ou code PIN. Et c'est là que la vulnérabilité existe. Certains constructeurs utilisent le même PIN pour tous leurs produits. WiFie va tout simplement tenter d'exploiter ces failles. Jetez un œil aux microfiches de cette rubrique pour découvrir l'appli WPS Connect sur Android qui propose ce genre de pentest en mode «mobile».

LEXIQUE



EN UTILISANT LES «ARGUMENTS» DE WIFI, VOUS POURREZ GAGNER DU TEMPS ET AFFINER VOS TESTS...

*WEP ET WPA :

Deux mécanismes de sécurisation des réseaux sans fil. Le WEP est maintenant démodé, car trop vulnérable tandis que le WPA, et le WPA2 ajoutent une couche de chiffrement (TKIP ou CCMP). Il est tout de même possible de pénétrer un réseau de ce type dans des conditions particulières.

*SCRIPT KIDDIES :

C'est un «pirate» qui utilise des logiciels «clé en main» sans vraiment en connaître le fonctionnement pour se faire mousser ou réaliser des méfaits. Ne soyez pas ce gars !

*DICTIONNAIRE :

Il s'agit d'une liste de mots dont le logiciel va se servir en espérant trouver le bon mot de passe dedans.



*BRUTE FORCE :

Méthode de récupération de mot de passe qui consiste à essayer toutes les combinaisons de caractères pour tomber sur la bonne entrée.



HACKING



INFOS [Kali Linux]

Où le trouver ? [www.kali.org]

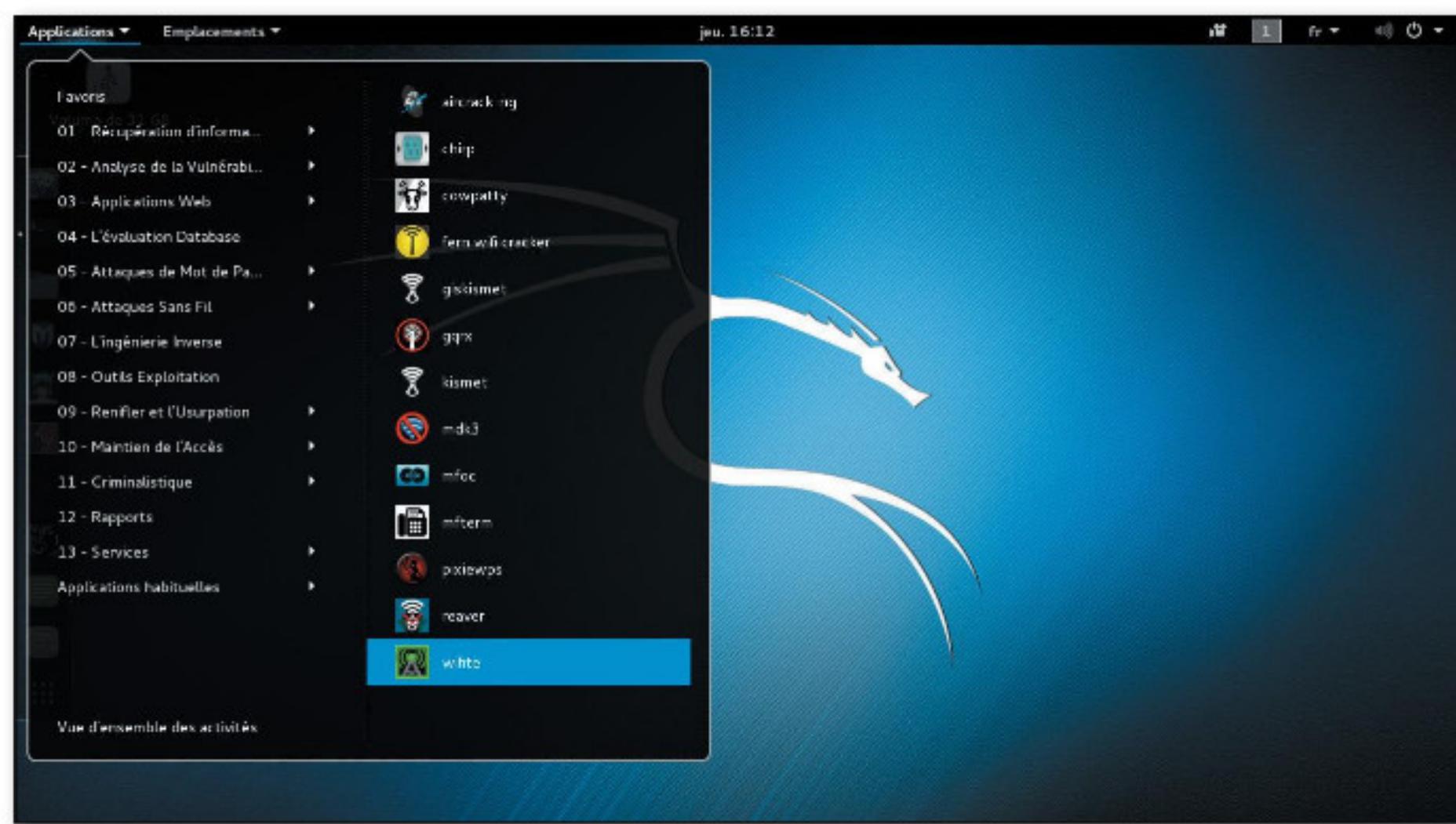
Difficulté :



TEST D'INTRUSION AVEC WIFITE

01 > L'EMPLACEMENT DU LOGICIEL

Pas besoin d'installer WiFie sur Kali 2, vous le trouverez dans **Applications>Attaques Sans Fil**. Cliquez dessus pour lancer un terminal avec la liste des arguments (les choses à taper dans vos lignes de commandes pour mieux cibler ou ajouter des options). Si vous n'êtes pas à l'aise avec les lignes de commande, le mieux est de garder cette liste



d'arguments devant vous comme un pense-bête et d'ouvrir un second terminal pour le pentest.

```
root@kali: ~
Fichier Édition Affichage Rechercher Terminal Aide
WiFite v2 (r87)
automated wireless auditor
designed for Linux

usage: wifite [-h] [--check CHECK] [--cracked] [--all]
               [-i INTERFACE] [--mac] [--mon-iface MONITOR_INTERFACE]
               [-c CHANNEL] [-e ESSID] [-b BSSID] [--showb] [--nodeauth]
               [--power POWER] [--tx TX] [--quiet] [--update] [--wpa]
               [--wpat WPAT] [--wpadt WPADT] [--strip] [--crack] [--dict DI]
               [--aircrack] [--pyrit] [--tshark] [--cowpatty] [--wep]
               [--pps PPS] [--wept WEPT] [--chopchop] [--arpreplay]
               [--fragment] [--caffelatte] [--p0841] [--hirte] [--nofakeauth]
               [--wepca WEPCA] [--wepsave WEPSAVE] [--wps] [--pixie]
               [--wpst WPST] [--wpsratio WPSRATIO] [--wpsretry WPSRETRY]

optional arguments:
  -h, --help            show this help message and exit
```

PAS ASSEZ RAPIDE ?

Vous trouvez que les attaques sont trop longues et vous voudriez accélérer les choses ? Rapprochez-vous du point d'accès que vous voulez tester ! Notez aussi que plus il y a de trafic entre le point d'accès et les utilisateurs du réseau et plus le processus sera rapide. Pour capturer le handshake, il faudra absolument qu'il y ait une activité sur le réseau ciblé. Attention, en ciblant plusieurs réseaux autour de vous, vous risquer de multiplier les temps d'attente.



02 > LES BASES

Commençons par stopper le service **network-manager** pour éviter les conflits en tapant **service network-manager stop**. Faites ensuite **wifite** puis **Entrée** et le logiciel ira scanner les réseaux alentour. Tapez **Ctrl+C**

```
root@kali: ~
Fichier Édition Affichage Rechercher Terminal Aide
NUM ESSID           CH ENCR POWER WPS? CLIENT
-----
1 SFR WiFi Mobile 11 WPA2 75db no
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 MI message
[0:00:04] WPS Pixie attack: attempting to crack and fetch psk...
[0:00:05] WPS Pixie attack failed - WPS pin not found
[0:00:06] initializing WPS PIN attack on SFR_D8C0 (30:7E:CB:B6:D8:C4)
[0:00:08] WPS attack, 0/1 success/ttl,
```

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. Ce faisant, WiFie va faire appel aux logiciels Aircrack et Reaver pour tenter de pénétrer votre réseau par tous les moyens. Or cela va prendre énormément de temps. Il est heureusement possible d'affiner le test.

03 > LE WEP DÉPASSÉ

Laissons de côté les protections WEP puisque celles-ci sont devenues rares. Si votre réseau est protégé par ce biais, faites juste **wifite -wep** et vous verrez que le mot de passe s'affichera en quelques minutes. Le WPS est plutôt long, mais les chances sont bonnes de réussir

```
root@kali: ~
Fichier Édition Affichage Rechercher Terminal Aide
[0:09:03] WPS Pixie attack: WARNING: Detected AP rate limiting, waiting 60 ...
[0:10:03] WPS Pixie attack: WARNING: Detected AP rate limiting, waiting 60 ...
[0:11:03] WPS Pixie attack: WARNING: Detected AP rate limiting, waiting 60 ...
[0:12:05] WPS Pixie attack: WARNING: Detected AP rate limiting, waiting 60 ...
[0:13:05] WPS Pixie attack: WARNING: Detected AP rate limiting, waiting 60 ...
[0:14:05] WPS Pixie attack: WARNING: Detected AP rate limiting, waiting 60 ...
[0:15:05] WPS Pixie attack: WARNING: Detected AP rate limiting, waiting 60 ...
[0:16:05] WPS Pixie attack: WARNING: Detected AP rate limiting, waiting 60 ...
[0:17:05] WPS Pixie attack: WARNING: Detected AP rate limiting, waiting 60 ...
[0:18:05] WPS Pixie attack: WARNING: Detected AP rate limiting, waiting 60 ...
[0:19:05] WPS Pixie attack: WARNING: Detected AP rate limiting, waiting 60 ...
[0:20:05] WPS Pixie attack: WARNING: Detected AP rate limiting, waiting 60 ...
[0:21:05] WPS Pixie attack: WARNING: Detected AP rate limiting, waiting 60 ...
[0:22:05] WPS Pixie attack: Sending identity response
[0:22:07] WPS Pixie attack: attempting to crack and fetch psk...
[0:22:08] WPS Pixie attack failed - WPS pin not found
[0:00:06] initializing WPS PIN attack on SFR_D8C0 (30:7E:CB:B6:D8:C4)
[0:11:00] WPS attack, 0/5 success/ttl,
[!] unable to complete successful try in 660 seconds
[+] skipping SFR_D8C0
[0:08:20] starting wpas handshake capture on "SFR_D8C0"
[0:08:08] new client found: 7C:4F:B5:73:6C:CA
[0:07:57] new client found: 00:E0:4C:9D:D8:49
[0:01:50] sending 5 deauth to *broadcast*...
```

votre intrusion. WiFie va tenter de découvrir le code PIN permettant un accès rapide au hotspot. Certains routeurs bannissent les adresses Mac des appareils qui tentent de

se connecter et échouent. Il faut alors anonymiser l'adresse Mac avec l'argument **-mac**.

04 > LES LIMITATIONS DU WPS

Autre point important : les points d'accès disposent de mesures de protection permettant d'empêcher le brute force en autorisant la saisie que d'un PIN toutes les 60 secondes. Pour cela, pas de solution miracle : il faudra emprunter une adresse Mac «amie». Cette technique étant plus complexe (Google est votre ami) nous iront au plus simple en tapant **wifite -wps -mac**. Comme plus haut, faites **Ctrl+C** pour choisir les SSID à attaquer.

```
root@kali: ~
Fichier Édition Affichage Rechercher Terminal Aide
[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
[0:22:10] WPS Pixie attack: WPS transaction failed (code: 0x02), re-trying
[0:22:12] WPS Pixie attack: Sending identity response
[0:22:17] WPS Pixie attack: WPS transaction failed (code: 0x02), re-trying
[0:22:18] WPS Pixie attack: Sending identity response
[0:22:23] WPS Pixie attack: 0.00% complete. Elapsed time: 0d0h22m23s.
[0:22:25] WPS Pixie attack: Sending EAPOL START request
[0:22:30] WPS Pixie attack: Sending identity response
[0:22:35] WPS Pixie attack: WPS transaction failed (code: 0x02), re-trying
[0:22:36] WPS Pixie attack: Trying pin 12345678.
```

05 > CAPTURE DU HANDSHAKE WPA

L'intrusion d'un réseau protégé par WPA ou WPA2 est plus compliquée puisqu'il faudra capturer le «handshake», le moment où un appareil et un point d'accès Wi-Fi vont tenter de s'authentifier mutuellement. Le mot de passe chiffré est contenu dans ce handshake. Une fois capturé, il prendra place dans **root/hs** (regardez **Dossier Personnel**). Il faudra le travailler au corps, soit par brute force, soit par une attaque dictionnaire. Heureusement, Kali Linux dispose de tous les outils nécessaires comme John The Ripper.

```
root@kali: ~
Fichier Édition Affichage Rechercher Terminal Aide
NUM ESSID CH ENCR POWER WPS? CLIENT
--- -----
1 SFR_D8C0 11 WPA 74db n/a client
2 SFR WiFi Mobile 11 WPA2 73db n/a
3 NEUF_8754 11 WPA 39db n/a
4 SFR WiFi Mobile 11 WPA2 38db n/a

[+] select target numbers (1-4) separated by commas, or 'all': 1
[+] 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
[0:03:34] 95,312 keys tested (459.03 keys/sec)
[!] crack attempt failed: passphrase not in dictionary

[+] quitting
```

06 > ATTAQUE DU HANDCHECK

Nous pouvons aller au plus simple en demandant à Aircrack de tenter de cracker le mot de passe contenu dans le handcheck en tapant simplement **wifite -wpa -aircrack**. Dans notre cas, l'attaque a échoué. Même si le handcheck 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 handcheck avec un meilleur dictionnaire ou avec un logiciel de brute force...

```
root@kali: ~
Fichier Édition Affichage Rechercher Terminal Aide
4 SFR WiFi Mobile 11 WPA2 38db n/a

[+] select target numbers (1-4) separated by commas, or 'a'
[+] 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
[0:03:34] 95,312 keys tested (459.03 keys/sec)
[!] crack attempt failed: passphrase not in dictionary

[+] quitting
```

POUR VOUS PROTÉGER...

Si vous avez réussi à pénétrer votre propre réseau, c'est que d'autres y arriveront. Si vous utiliser encore le WEP (sérieusement ?), il faudra commencer par changer pour du WPA/WPA2. Si l'attaque WPS a réussi, vous pouvez soit mettre à jour le firmware ou carrément bannir cette fonctionnalité sur votre routeur ou box. Connectez-vous à <http://192.168.1.1> ou <http://192.168.0.1> pour accéder aux réglages. Dans tous les cas, changez de mots de passe régulièrement et optez pour un sésame qui pourra difficilement se retrouver dans un dictionnaire d'attaque et suffisamment long pour rendre le brute force difficile comme **F4k»^5DgTs_4à\$7dD1çui825** par exemple.





HACKING

Micro-fiches

Apprenez à programmer ! > AVEC GRASSHOPPER

Grasshopper est une application gratuite et sans publicité permettant d'apprendre à programmer en JavaScript. Même si ce langage connaît des détracteurs, il s'agit d'un bon point de départ pour la programmation. Non seulement les mécaniques pourront être utilisées avec un autre langage, mais le JavaScript est utilisé dans pas mal de domaines : la création de pages Web interactive, pour les serveurs ou dans les plates-formes comme Node.js. L'utilisateur se verra

Today Is the Day

In this puzzle, you'll declare a new variable. For example, `var month = 'August'` creates a variable named month and assigns the value 'August' to it.

INSTRUCTIONS

Declare a new variable to remember what day it is.

- Create a variable called `day`.
- Assign it the string '`'Friday'`'.
- Print the variable using `print(day)`.

HINT (tap to reveal)

EXAMPLE SOLUTION

```
> August
> Friday
```

YOUR SOLUTION

```
> August
```

exposer en premier lieu la base de la programmation avec une courte intro puis commenceront les exercices pratiques. Après une courte leçon, on vous invite à afficher des couleurs, à définir une variable, etc. Les instructions sont à entrer grâce à des blocs et on utilise aussi parfois le clavier virtuel. Au fur et à mesure de la progression, vous aurez aussi des QCM auxquels il faudra répondre avant de continuer. Toute l'interface est très "graphique" et on peut obtenir de l'aide à tout moment ou réinitialiser son programme. Le concept est génial et serait idéal pour des enfants, mais le problème c'est que Grasshopper est uniquement en anglais...

Lien : <https://frama.link/4Ayu21qY>



Les permissions Linux faciles > AVEC CHMOD CALCULATOR

Lorsqu'on commence sous Linux, le concept de permissions/droits n'est pas facile à appréhender. Sur ce site (en anglais), vous devrez juste cocher des cases correspondantes aux permissions que vous voulez accorder au propriétaire, au groupe et aux autres : lecture, écriture et exécution. On trouve aussi d'autres options complémentaires : silent, verbose, recursive, sticky, etc. Votre ligne de commande est prête à être copiée-collée dans un terminal immédiatement !

Lien : <https://chmodcommand.com>

Chmod 764

Chmod calculator allows you to quickly generate permissions in numerical and symbolic formats. All extra options are included (recursive, sticky, etc). You'll be ready to copy/paste your chmod command into your terminal in seconds.

Owner Rights (u)	Group Rights (g)	Others Rights (o)
Read (4) <input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Write (2) <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Execute (1) <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Extra chmod command options

Verbose Recursive Setuid
 Changes Preserve-Fileset Setgid
 Silent Reference File Sticky Bit

Use the octal CHMOD Command:
chmod -R 764 folder_name

OR use the symbolic CHMOD Command:
chmod -R a+rwx,g-x,o-wx folder_name

Automatisation de tâches sur mobile > AVEC IFTTT

IFTTT (prononcez «ift») est l'acronyme de «If This Then That» que nous pourrions traduire par «Si Ceci Alors Cela». Il s'agit en fait d'une application permettant de programmer simplement des actions en fonction d'événements. On pouvait auparavant faire ses propres "recettes", mais le service a évolué : elles sont maintenant "préconçues" et sélectionnables depuis l'interface. Le nom aussi a changé, on les appelle maintenant les "applets". Par exemple, grâce à IFTTT, vous pouvez demander à recevoir un e-mail ou un SMS pour savoir s'il va pleuvoir ou demander à Instagram de poster vos nouveaux clichés sur Twitter. On peut aussi imaginer placer automatiquement un document de OneDrive sur Google Drive ou de remercier par Gmail les nouveaux followers de votre compte Twitter. On peut aussi demander au smartphone de mettre la sonnerie plus forte après un appel manqué, ajouter à Spotify une chanson que vous avez likée dans YouTube, etc. Les possibilités sont presque infinies puisque IFTTT est compatible avec une centaine de services : <https://ifttt.com/services>. Cela fonctionne aussi avec les assistants vocaux (Alexa, Google Assistant), les produits de domotique (Philips Hue, WeMo), l'électroménager (Samsung, Whirlpool, LG), mais on trouve aussi des clouds, des messageries instantanées, des voitures connectées, des listes de contacts, des services musicaux, des appareils de contrôle de l'environnement, des services de notification ou de localisation d'animal de compagnie, etc. Tous ces sites/appareils/services peuvent donc fonctionner ensemble pour vous faciliter la vie. La liste est très longue : les partenaires sont plus de 300 et les applets sont innombrables.

Lien : <https://frama.link/kuvQtH6o>

Applets for voice assistants

PHILIPS hue

Blink your Hue lights when your Amazon Alexa timer hits 0

46k works with

Send messages from Google Assistant to Messenger

7k works with

Create a note by telling it to Google Assistant

IFTTT

Applets for voice assistants

Recommended for you

Set ringer to high after missing a call.

120k works with

Add songs from videos you like to a Spotify playlist

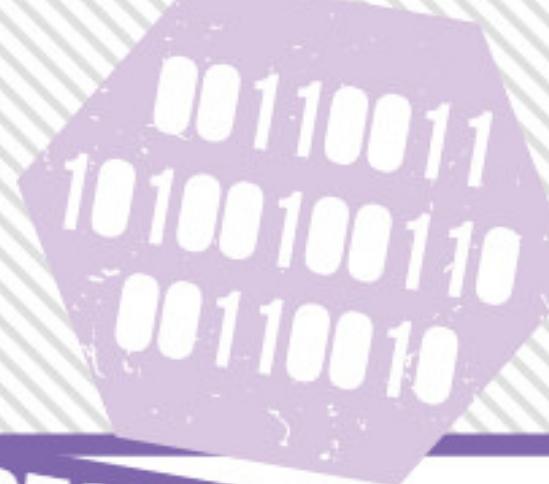
NOUVEAU !

The image shows the cover of the magazine "L'officiel PC Raspberry Pi" Volume 11. The cover features a large central illustration of a Raspberry Pi board with two green leaves on top, resembling a raspberry. The title "RASPBERRY PI" is written in large white letters across the middle. Below it, the subtitle "Idées & Projets Clés en Main" is visible. The price "7,90 € LE GUIDE COMPLET" is shown in the top right corner. The left side of the cover has a red vertical bar with "RASPBERRY PI" and "POUR DÉBUTANTS & CONFIRMÉS". The right side has a blue vertical bar with "VOLUME 11". The center of the cover is filled with various project ideas and tutorials, such as "MAO SONIC PI V3 : PROGRAMMEZ VOTRE MUSIQUE", "Jeux vidéo TRANSFORMEZ RASPBERRY PI EN AMIGA!", "LoRAWAN PASSEZ À LA COMMUNICATION RADIO", "Micro:bit LA PETITE CARTE QUI MONTE", and "ETC!". A large banner across the middle reads "RASPBERRY PI LE GUIDE DE L'UTILISATEUR". To the right of this banner is a badge that says "TOUT FAIRE DE A à Z BEST-OF TUTOS & CODE". At the bottom right, there's a smaller image of a robot-like character made from a Raspberry Pi and other components. The overall design is colorful and informative.

Par l'équipe
de *Pirate
Informatique!*

GUIDE
COMPLET

CHEZ VOTRE MARCHAND DE JOURNAUX



Qwant

UN MOTEUR DE RECHERCHE RESPECTUEUX DE LA VIE PRIVÉE ?



Depuis quelques semaines, Qwant fait parler de lui. Le moteur de recherche français respectueux de la vie privée serait copain comme cochon avec Microsoft. Il enverrait même des informations sur les utilisateurs à l'américain... Un comble, non ? Démêlons le vrai du faux.

LEXIQUE

***USER AGENT STRING :** Il s'agit d'une chaîne de caractères envoyée dans les communications HTTP pour identifier le système et le navigateur d'un utilisateur. Cela permet d'optimiser l'affichage du contenu Web (qui peut prendre différentes formes selon que vous vous connectez depuis Firefox, Windows ou sous Chrome avec un appareil Android). Or, ce User Agent peut être utilisé pour réaliser "l'empreinte" d'un individu.

***HACHAGE/ SALAGE :** Une fonction de hachage (hash function) va transformer une donnée en clair vers une suite alphanumérique qui sera très difficile à inverser. Le salage va ajouter une fonction aléatoire au hachage pour rendre impossible toute récupération de l'information initiale.

Interview de Tristan Nitot, vice-président de Qwant

ENTRONS DANS LE VIF DU SUJET, QU'EST-CE QUI EST SOUS-TRAITÉ PAR MICROSOFT DANS LES RECHERCHES DE QWANT EXACTEMENT ?

Dans cette histoire beaucoup crient au loup, mais la vérité c'est que Microsoft est un partenaire historique de Qwant. Depuis des années nous utilisons la régie publicitaire de Microsoft et nous ne nous en cachons pas puisque sur les encarts, c'est explicitement mentionné : «publicité fournie par Microsoft». Après nous avons notre propre régie et nous espérons la voir prospérer à l'avenir. Mais pour comprendre nos liens avec Microsoft, il faut savoir qu'un moteur de recherche c'est 4 sous-systèmes. On a d'abord le «crawler». C'est un robot qui parcourt le Web et copie des pages en local. On a ensuite la création de l'index qui est similaire à ce qu'on peut trouver à la fin d'un livre (tel mot se rapporte à telle page). Cet index va scanner des dizaines de milliards de pages et des centaines de milliards de liens. Pour ce faire, il faut une grosse capacité de calcul et donc, une grosse infrastructure. Vient ensuite le ranking qui va établir une pertinence entre les pages. Si vous tapez «soupe à la tomate», vous ne voulez pas savoir comment cultiver la tomate ou les pays producteurs de tomates, vous voulez sans doute une recette de soupe à la tomate. Cette étape est encore très coûteuse en puissance de calcul.

Dans ces 3 premiers éléments (crawler, index et ranking), tout est public. Par contre le 4^{ème} est plus sensible puisqu'il s'agit de la partie «front end» où Qwant dispose en clair de l'IP de la personne qui tape «soupe à la tomate». Cette information n'est pas de la data publique, mais comme Qwant est respectueux de la vie privée, cette adresse IP est utilisée pour délivrer les résultats, mais elle est ensuite hashée et salée avant d'être stockée pour éviter toute récupération.

En ce moment, toutes ces étapes sont gérées par Qwant, mais dans quelques semaines, sans doute à la rentrée, nous allons louer à Microsoft des serveurs situés en UE pour augmenter notre puissance de calcul, indexer plus de pages et augmenter la pertinence du ranking. L'étape 4 s'effectuera toujours sur nos serveurs.



Tristan Nitot a rejoint Qwant l'année dernière, mais avant cela, il a passé 17 ans à la fondation Mozilla. Il est aussi écrivain et membre du comité de prospective de la CNIL.

Sur Tweeter ou dans la presse spécialisée, on entend beaucoup parler de Qwant en ce moment. On soupçonne le moteur de recherche français de copinage avec Microsoft et même de lui envoyer des informations. Rappelons pour ceux qui ne connaissent pas, que Qwant se limite au minimum en ce qui concerne les incursions dans votre vie privée. Pourtant, on parle aussi de user agent string et d'IP partiellement envoyée à la régie pub du géant américain. Pour y voir plus clair, nous avons demandé à un responsable de Qwant de bien vouloir répondre à nos questions et c'est Tristan Nitot qui s'y est collé. On aurait pu tomber plus mal...

Le but d'une location de serveur c'est d'éviter de devoir les acheter et de potentiellement être condamné à ne les faire tourner que quelques heures par jour. Lorsque vous êtes un étudiant sans argent, vous allez en premier lieu louer un appartement plutôt que d'acheter, non ?

SELON LE VIRUS INFORMATIQUE (DANS SON N°40), QUAND ON CLIQUE SUR UNE PUBLICITÉ, QWANT FOURNIT À MICROSOFT l'IPv4/24 [UNE IP AMPUTÉE DES 3 DERNIERS CHIFFRES] PLUS L'USER AGENT DE L'UTILISATEUR. IL S'AGIT APPAREMMENT D'UNE MESURE PERMETTANT D'ÉVITER LES FRAUDES AUX CLICS. SELON EUX, IL EST POSSIBLE EN RECOUPANT CES DEUX INFORMATIONS DE LOCALISER UNE PERSONNE, MÊME S'IL S'AGIT DE CAS RARES [NOTONS AU PASSAGE QUE MICROSOFT N'A CONTRACTUELLEMENT PAS LE DROIT DE LE FAIRE, NDLR]. DANS SON ARTICLE, LE JOURNALISTE PREND L'EXEMPLE HYPOTHÉTIQUE D'UN UTILISATEUR DE QWANT DANS UN PETIT VILLAGE QUI UTILISERAIT UN ATARI ST POUR SE CONNECTER...

Ils ont raison. Si toutes les planètes sont alignées, dans un cas extrême, c'est potentiellement possible. Comme il s'agit d'une IP4/24, il y a une chance sur 256 de trouver son emplacement. Tout ça à condition que tout ce petit monde dispose d'une IP fixe et que le user agent string soit suffisamment exotique. Nous sommes en train de corriger cela. Nous souhaitons faire en sorte de remplacer le user agent string des utilisateurs par une chaîne de caractères générique : Chrome/Windows par exemple, même si l'utilisateur utilise iOS. C'est prévu, car nous souhaitons être parfaits.

LE BUT ULTIME DE QWANT EST-IL DE DEVENIR INDÉPENDANT À L'AVENIR ?

Bien sûr nous avons pour vocation de devenir complètement indépendants.

The image contains two side-by-side screenshots. The left screenshot shows a mobile map application interface for 'Gare de Kiev' (Kievsky railway station) in Moscow. It includes a sidebar with station details, a 'FAVORS' button, a 'PARTAGER' (share) icon, and an 'ITINERAIRE' (route) icon. The right screenshot shows the 'Masq ALPHA' app interface, which promises 'Stockage sécurisé et gratuit de vos préférences et informations personnelles directement sur votre appareil'. It features a central icon of a smartphone with a lock and a key, surrounded by icons for a gear, a heart, and a magnifying glass. Below the main text are two sections: 'Respect de la vie privée' and 'Stockage des données sur vos appareils'.

QWANT INVESTIT ÉNORMÉMENT DANS DE NOUVELLES FONCTIONNALITÉS. QWANT MAPS, EN COLLABORATION AVEC OPEN STREET MAP, ET MASQ SONT LES DERNIERS REJETONS DU MOTEUR DE RECHERCHE FRANÇAIS.

POUR METTRE LES CHOSES EN PERSPECTIVE, POUVEZ-VOUS NOUS DIRE D'OÙ QWANT TIRE SON ARGENT ?

Qwant est en pleine croissance, les chiffres sont phénoménaux et nous avons besoin de grossir constamment. Il s'agit même d'un miracle de faire de tels résultats avec le peu d'argent que nous avons à disposition. Car outre les salaires, nous investissons énormément. Qwant propose des publicités contextuelles. À ne pas confondre avec les publicités ciblées de Google. Avec votre mobile Android, votre compte Gmail, Google Maps, Chrome, Calendar, YouTube, Waze et toutes ces applications, Google a une vision bien claire de qui vous êtes, ce que vous voulez, ce que vous allez faire, etc. Chez nous, si vous tapez «soupe à la tomate» [C'est une fixation, NDLR], on vous proposera par exemple une publicité pour un mixeur ou des boîtes de gazpacho, mais rien n'est enregistré et on ne sait rien du background de la personne. Nous avons aussi Qwant Shopping qui va vous proposer un produit en fonction de votre recherche. Si vous tapez «télévision 4K», on pourra vous en recommander quelques unes et Qwant prendra une commission en cas d'achat. Nous pouvons aussi compter sur des investisseurs privés. En ce moment Qwant pourrait être profitable, mais nous préférions miser sur la recherche et le développement pour proposer de nouvelles fonctionnalités. Par exemple nous travaillons en ce moment sur Qwant Maps en collaboration avec Open Street Map et sur Masq qui permet de chiffrer des données en local (favoris, itinéraires, etc.) avec synchronisation, sans passer par un serveur.

ÇA NE DOIT PAS ÊTRE FACILE DE CONVAINCRE DES INVESTISSEURS AVEC LE GÉANT GOOGLE FACE À VOUS ET CETTE POLITIQUE D'INVESTISSEMENT INTENSIVE...

Pas forcément, car l'argent n'est pas la première motivation pour tous. La Caisse des Dépôts et Consignations [qui a investi 15 millions d'euros en 2017] a par exemple pour but de redonner un peu de souveraineté à la recherche en ligne. Pareil pour Axel Springer qui a d'autres motivations [Ce groupe de presse allemand n'est pas vraiment fan de Google qu'il accuse de voler le contenu de ses articles, NDLR].



ANONYMAT



POUR QUI ?

Accessible à tout le monde

POUR QUOI FAIRE ?

Un VPN sert à établir une connexion sécurisée où les données entre votre appareil et Internet sont chiffrées, pour empêcher toute interception frauduleuse.

OPERA : LE NAVIGATEUR AVEC VPN GRATUIT

En 2016, Opera ajoutait à son navigateur un VPN illimité et gratuit. Un service malheureusement trop lent pour être utilisable, et condamné à être bloqué par certains sites. Aujourd'hui, Opera 60 est là : nouvelle interface, portefeuille de cryptomonnaie et un VPN tout neuf.

Souvenez-vous, en 2016 Opera ajoutait à son navigateur un VPN gratuit et illimité. Une excellente nouvelle pour ses utilisateurs. Seulement ce service n'était pas encore très au point et souffrait de nombreuses latences. Conséquence directe, le blocage du VPN par certains sites comme Netflix. Avril 2019, l'éditeur norvégien annonce une nouvelle mise à jour majeure pour son navigateur. Son nom : Reborn 3. Avec cette version, les développeurs veulent mettre l'accent sur la sécurité et la confidentialité de ses utilisateurs. Au programme, un portefeuille de cryptomonnaie intégré, un navigateur Web 3 ou BlockChain, et un VPN tout beau tout neuf. Il faut néanmoins nuancer. On ne peut pas vraiment parler de VPN, mais plutôt d'un serveur proxy sans chiffrement des paquets IP, efficace pour contourner les blocages régionaux par exemple, ou cacher son adresse IP d'origine.

UN VPN GRATUIT MAIS LIMITÉ

Forcément, le VPN gratuit d'Opera n'offre pas autant de possibilités qu'une version payante. Vous n'aurez par exemple le choix qu'entre 3 zones de connexion : Europe, Amérique et Asie. Vous pouvez également choisir de vous connecter sur le meilleur emplacement à proximité. Après quelques tests, la version 2019 se montre plus rapide que



l'ancien opus, notamment sur les zones Europe et Amérique. La connexion asiatique souffre encore de nombreuses latences, et il est très compliqué, voire impossible, de regarder un film dans son intégralité. Autre point, il faut rappeler qu'un serveur proxy ne garantit pas un anonymat total. Tout ce que vous faites sur Opera est transmis aux serveurs d'Opera. Et quand on sait que la société a été rachetée par un consortium chinois, il est de bon ton de se montrer prudent sur le devenir de nos données personnelles.



INFOS [Opera]

Où le trouver ? [www.opera.com/fr]

Difficulté :



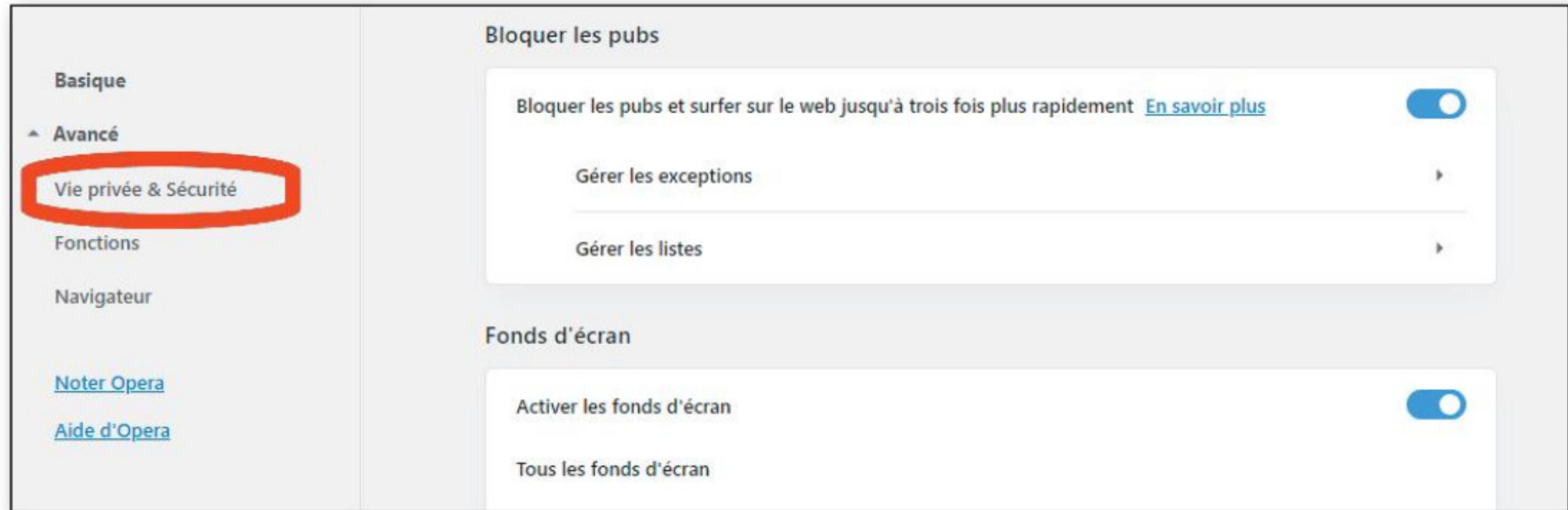
COMMENT ACTIVER LE VPN D'OPERA ?

PRATIQUE



01 > LE MENU

Téléchargez la dernière version d'Opera ou mettez la vôtre à jour. Une fois sur la page d'accueil d'Opera, rendez-vous dans les paramètres et cliquez sur la rubrique **Avancé**, puis **Vie privée et sécurité**.



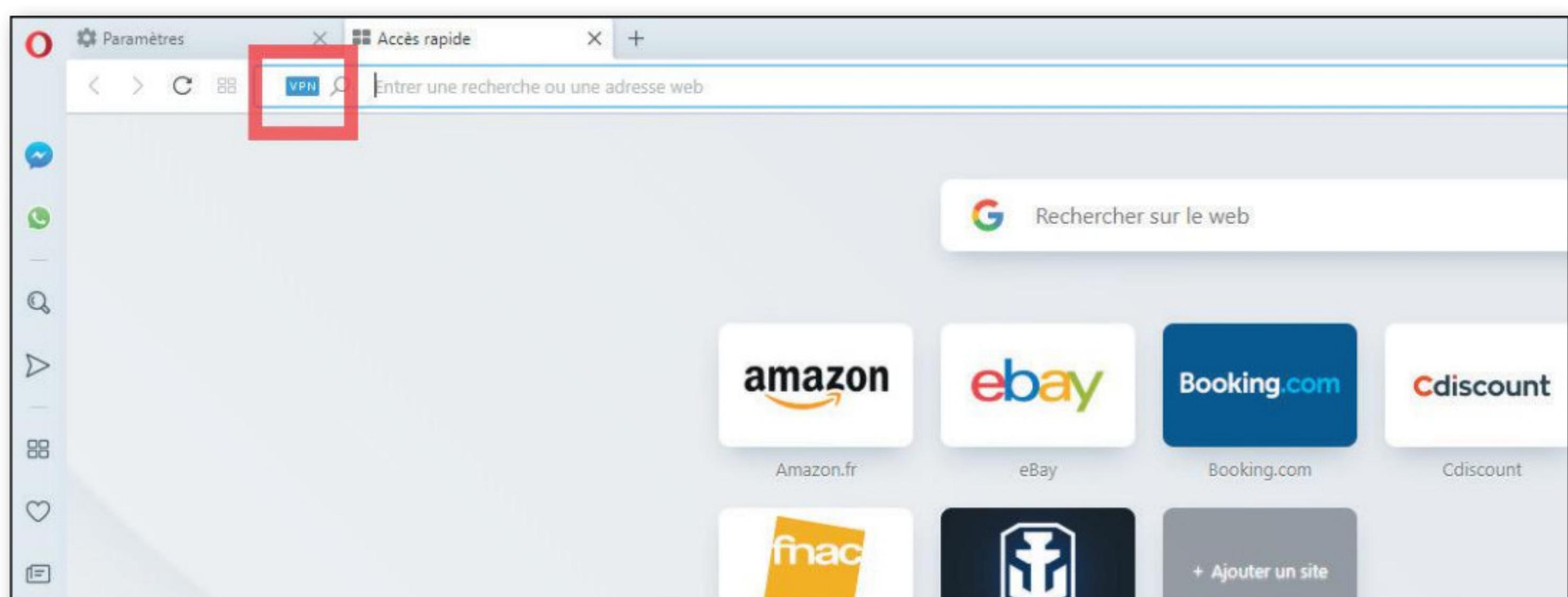
02 > ACTIVEZ LE VPN

Faites défiler jusqu'à tomber sur l'onglet VPN et activez-le. Notez que la vitesse de votre trafic peut être légèrement altérée.



03 > LE VOLUME DE DONNÉES UTILISÉ

Ceci fait, vous pouvez apercevoir dans la barre de recherche un bouton VPN. Cliquez dessus pour choisir votre emplacement de connexion, savoir le nombre de données transférées ce mois-ci ou encore votre adresse IP.

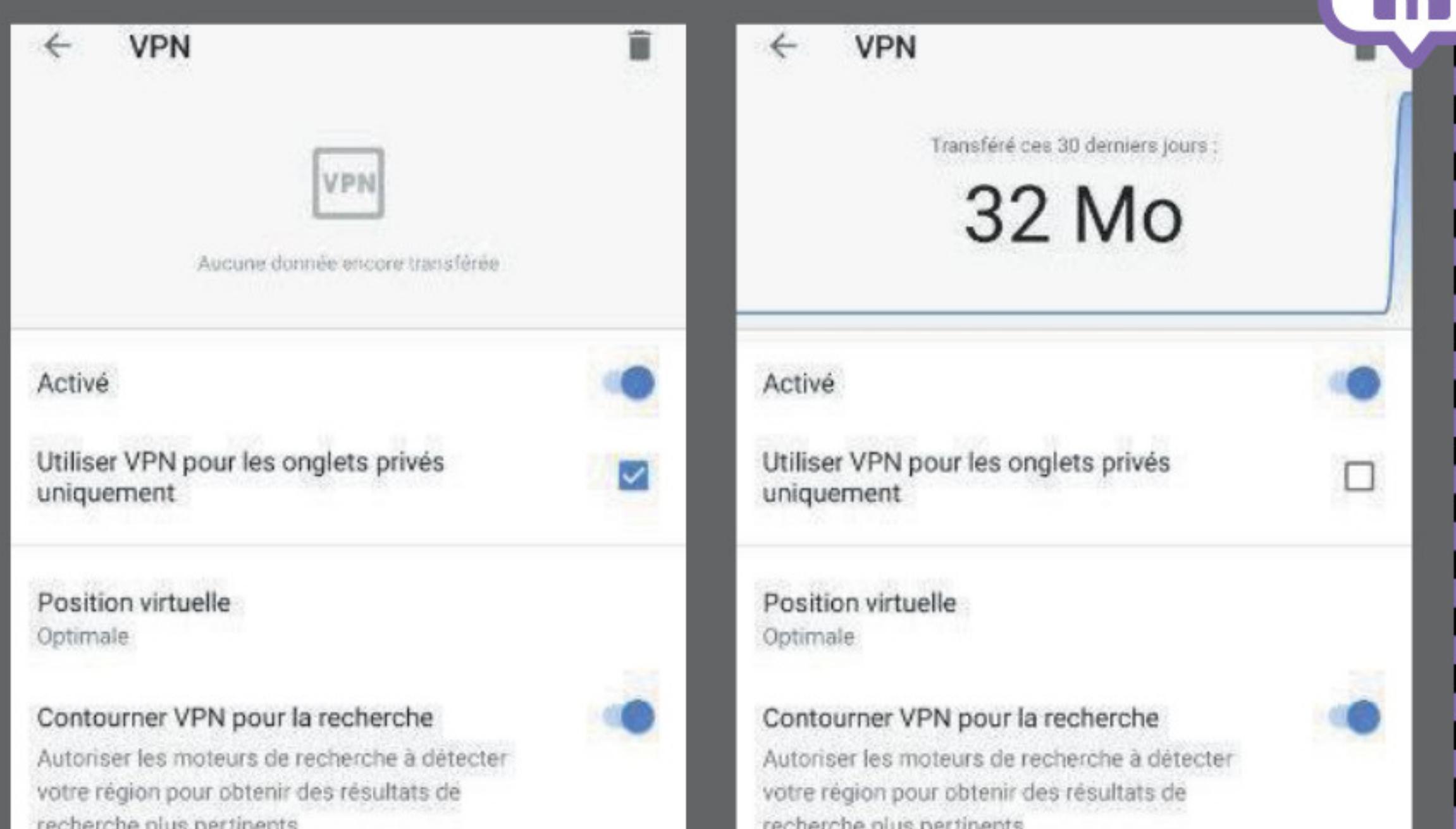


OPERA SUR MOBILE ?



Utilisateurs d'Opera sur mobile, vous serez ravis d'apprendre que le VPN est également disponible sur vos smartphones. Il suffit de vous rendre dans les paramètres du navigateur et d'activer le VPN. Il peut se cantonner aux onglets de navigation privée, et il est possible comme sur PC de choisir un emplacement de connexion (Europe, Amérique et Asie). Nous vous conseillons de rester sur le réglage **Optimal** pour éviter toute perte de connexion. Vous pourrez également profiter d'un bloqueur de pub, un portefeuille de cryptomonnaie et d'un mode d'économies de données.

Lien : <https://frama.link/mVP210MF>





Une messagerie auto destructible > AVEC CONFIDE

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

Lien : <https://getconfide.com>

The screenshot shows the Confide application interface across three devices: a desktop computer, a tablet, and two smartphones. The desktop screen displays a list of contacts with their last message status. The tablet screen shows a message composition screen with a red brick wall background. The smartphone screens show a list of messages and a destruction timer. A large orange button at the bottom right of the mobile interface says "DOWNLOAD FOR FREE".

Vous déconnecter de plusieurs services automatiquement > AVEC SUPER LOGOUT

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

Lien : <http://superlogout.com>

SUPER LOGOUT

- AOL: **OK**
- Amazon: **OK**
- Blogger: **OK**
- Delicious: **OK**
- DeviantART: **OK**
- DreamHost: **OK**
- Dropbox: **OK**
- eBay: **OK**
- Gandi: **OK**
- GitHub: **OK**
- GMail: **OK**
- Google: **OK**
- Hulu: **OK**
- Instapaper: **OK**
- Linode: **OK**
- LiveJournal: **OK**
- MySpace: **OK**
- NetFlix: **OK**
- New York Times: **OK**

Testez votre messagerie > AVEC EMAIL PRIVACY TESTER

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

Lien : www.emailprivacytester.com

The screenshot shows the Email Privacy Tester interface with the email address "Testing peyrot.yann.mt@gmail.com" entered. Below the address is a "Send Another Email" button. The main area is a grid of buttons representing different tracking tags and technologies:

- Row 1: tag, Atom feed, Audio tag, Background attribute, BGSound tag, CSS Attachment
- Row 2: background-image, CSS behavior, CSS content, CSS font-face, CSS import, CSS link tag
- Row 3: ion Notification, DNS Prefetch - Anchor, DNS Prefetch - Link, Iframe img, Iframe meta refresh
- Row 4: g, Image Submit Button, Image tag, Img srcset attr, Link Prefetch, Manifest, Meta refresh
- Row 5: ag - data, Object tag - Flash, OpenSearch, Return Receipt, RSS feed, Script inside script
- Row 6: g (javascript), SVG attachment with CSS, SVG inline with remote image, Video MP4, Video Ogg
- Row 7: deo poster, Video tag, Video Webm, view-source URI

L'INFORMATIQUE FACILE POUR TOUS !

**CHEZ
VOTRE
MARCHAND
DE JOURNAUX**



LA DOUBLE AUTHENTIFICATION : UNE PROTECTION QUASI INVOLABLE

Le mot de passe est une protection totalement dépassée depuis bien longtemps. Aujourd’hui les pirates ont des dizaines et des dizaines de moyens possibles pour s’emparer facilement de vos identifiants. Alors, en attendant que les industriels trouvent une meilleure solution, prenez les devants et bétonnez vos comptes avec la double authentification.



Recommandée par les géants du Web, la double authentification est à l’heure actuelle le meilleur moyen de sécuriser l’accès à vos comptes. Vous vous en doutez bien, un mot de passe se « crack » souvent les mains dans les poches. Les hackers ont l’embarras du choix pour subtiliser vos identifiants : envoi de faux mails avec des formulaires falsifiés, tentative d’interception sur des réseaux Wi-Fi publics peu sécurisés, phishing, cheval de Troie, malwares en tout genre planqués dans des applications Android et iOS. Bref, c’est la fête. Et pour continuer dans la métaphore, la double authentification, ce sont les policiers qui viennent mettre un terme à la petite sauterie vers 3h du matin. Aussi appelée 2FA (pour Double Factor Authentication), la double authentification est un procédé qui permet de

vérifier que vous êtes bien le propriétaire d’un compte, lorsque vous procédez à plusieurs actions clés : connexion au compte, et surtout changement de mot de passe. En plus de vous demander vos identifiants et mots de passe, le site sur lequel vous vous connectez va exiger de vous un *Authenticator*. Ou en d’autres termes, un moyen supplémentaire de confirmer votre identité, via votre numéro de téléphone (par SMS), un appareil ou sur une adresse mail secondaire. De fait, si un pirate parvient à récupérer votre mot de passe, il ne lui servira à rien, car il n’aura pas toutes les clés en mains pour entrer.

ADOPTEZ LA POUR LES SITES LES PLUS SENSIBLES

Pour ses détracteurs, la double authentification est trop complexe, et ralentit énormément le processus de connexion. Soit, c’est un fait et il est difficile de leur donner tort. Mais ce que vous perdez en confort, vous le gagnez au centuple en sécurité. Bien évidemment, vous n’êtes pas obligé de l’appliquer à tire-larigot sur tous les sites sur lesquels vous avez un compte. En revanche, il

The screenshot shows the homepage of the Have I Been Pwned website. At the top, there's a navigation bar with links like Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. Below the navigation is a large button with the text "'--have i been pwned?'" in white. Underneath it, a smaller text says "Check if you have an account that has been compromised in a data breach". There's a search bar with the placeholder "email address" and a "pwned?" button next to it. At the bottom of the page, there are some stats: "8,043,815,683 pwned accounts", "99,037 pastes", and "119,804,587 paste accounts". There are also links for "Generate secure, unique passwords for every account" and "Learn more at 1Password.com".



LE SITE HAVEIBEENPWNED.
COM RÉFÉRENCE 5 MILLIARDS
D’IDENTIFIANTS VOLÉS SUR PLUS
DE 250 SITES.

y a des sites à protéger en priorité : messagerie, réseaux sociaux, les comptes cloud et les services bancaires en ligne.

Pour les hackers, accéder à une boîte mail, c'est un peu comme ouvrir la caverne d'Ali Baba. Il peut y dénicher des tonnes et des tonnes d'informations sur vous (identifiants divers et variés, mails de réinitialisation de mot de passe, etc.) Les réseaux sociaux sont les reflets de votre personnalité, imaginez les dégâts potentiels d'une usurpation d'identité. Bon nombre d'entre vous sont également des aficionados du travail collaboratif, et il n'est jamais agréable de voir ses recherches spoliées ou totalement effacées par un hacker sans merci. Et puis pour les services bancaires, pas besoin de vous faire un dessin.

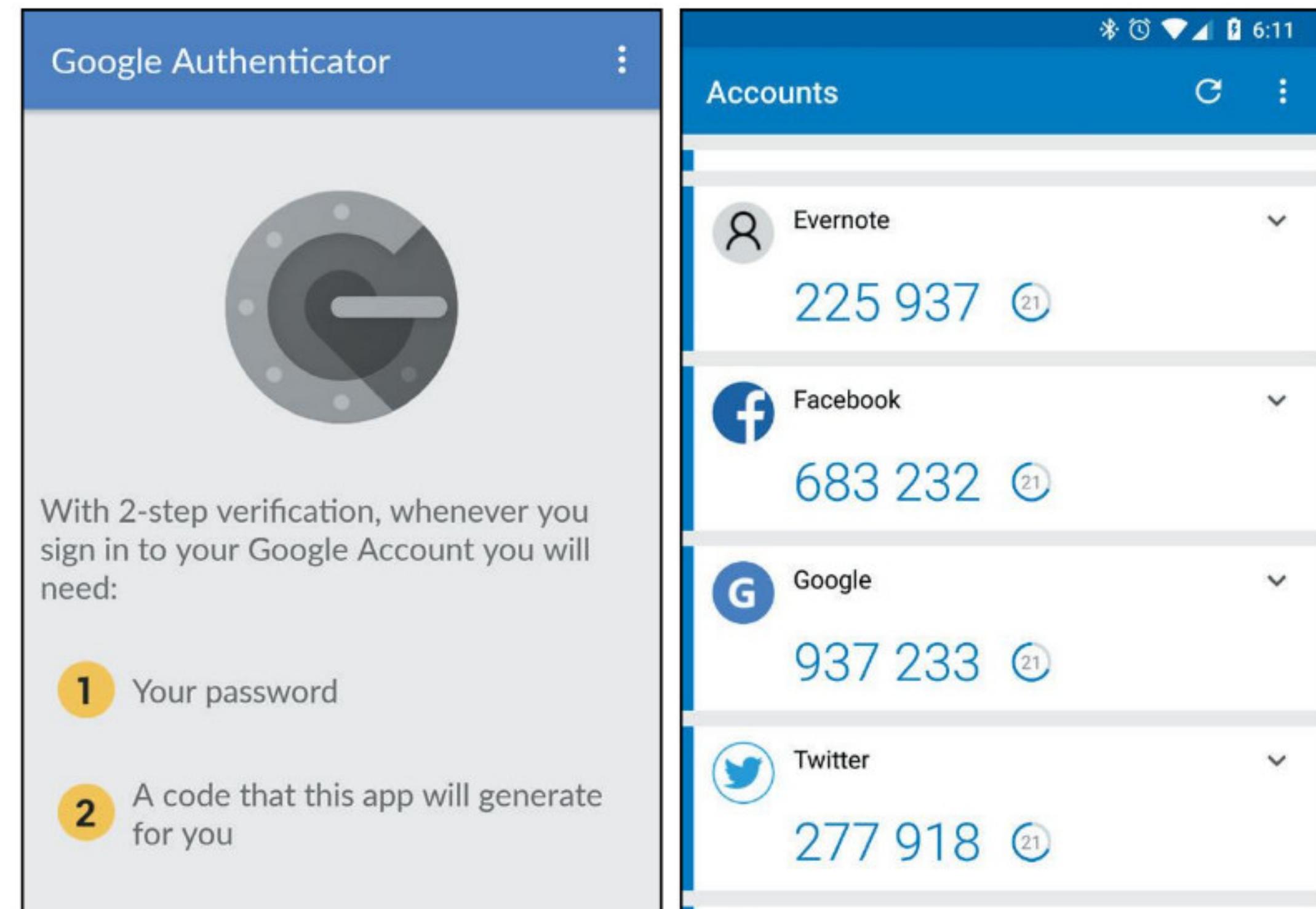
COMMENT LA METTRE EN PLACE ?

La quasi-totalité des services de messagerie proposent des compatibilités avec la double authentification. Si ce n'est pas votre cas, fuyez pauvre fou et tournez vous vers les alternatives ultra-sécurisées, comme ProtonMail ou Tutanota par exemple. En général, les méthodes varient : envoi d'un code unique à 4 ou 6 chiffres par SMS ou par mail, appel téléphonique, ou encore envoi de notification en cas de connexion depuis un appareil inconnu.

Du côté de chez Google et Microsoft, il faudra télécharger leurs applications dédiées : Google Authenticator et Microsoft...Suspens... Authenticator. Ces deux applis ont pour avantage, une fois configurées, de générer des codes uniques sans avoir besoin de réseau téléphonique. À la moindre connexion depuis un appareil non-identifié, et juste après avoir renseigné votre mot de passe, le site internet sur lequel vous vous connectez vous demandera de rentrer un code à 6 chiffres, code directement généré par l'application. Vous voilà double authentifié !

LIMITEZ LES RISQUES AU MAXIMUM

Malheureusement, tout n'est pas tout rose dans le monde de la double authentification. Quoique très efficace, elle n'est pas infaillible. Les SMS avec code unique envoyés par les



différents services pour vous authentifier peuvent être interceptés par des hackers chevronnés, notamment grâce au clonage de carte SIM. Alors comment faire pour être totalement hermétique ? La clé de sécurité. Dans ce domaine, l'entreprise Yubico est le leader incontesté. Le principe est très simple : en plus des méthodes traditionnelles utilisées pour la double authentification, il est possible de connecter une clé USB à votre PC ou à votre téléphone portable (via le NFC). Ce standard est reconnu par Facebook, Dropbox, Google, Twitter et une pléthora d'autres sites. L'avantage de ce produit, c'est que hormis s'introduire chez vous et la voler "à l'ancienne", un pirate ne pourra jamais l'intercepter, la hacker, la détourner, vous avez compris.

LES 5 CONSEILS DE GOOGLE POUR ÊTRE EN SÉCURITÉ SUR INTERNET

Google est ce qu'il est, mais la firme de Mountain View prodigue de temps en temps des bons conseils pour se prémunir des dangers sur la toile.

1. Avoir un téléphone et/ou une adresse mail de secours pour la double authentification.
2. Utiliser un mot de passe unique pour chaque compte. Selon une enquête réalisée par Google, 65% des sondés se servent du même mot de passe pour plusieurs comptes... D'accord, c'est une organisation à mettre en place, mais il est impératif de le faire. Imaginez, c'est comme si vous aviez la même clé pour le garage, la voiture, et le coffre-fort. Si quelqu'un la trouve, vous pouvez tout perdre.
3. Gardez vos applications et votre PC à jour.
4. Optez systématiquement pour la double authentification.
5. Inscrivez-vous au système de protection avancée de Google (ça, c'est vous qui voyez).





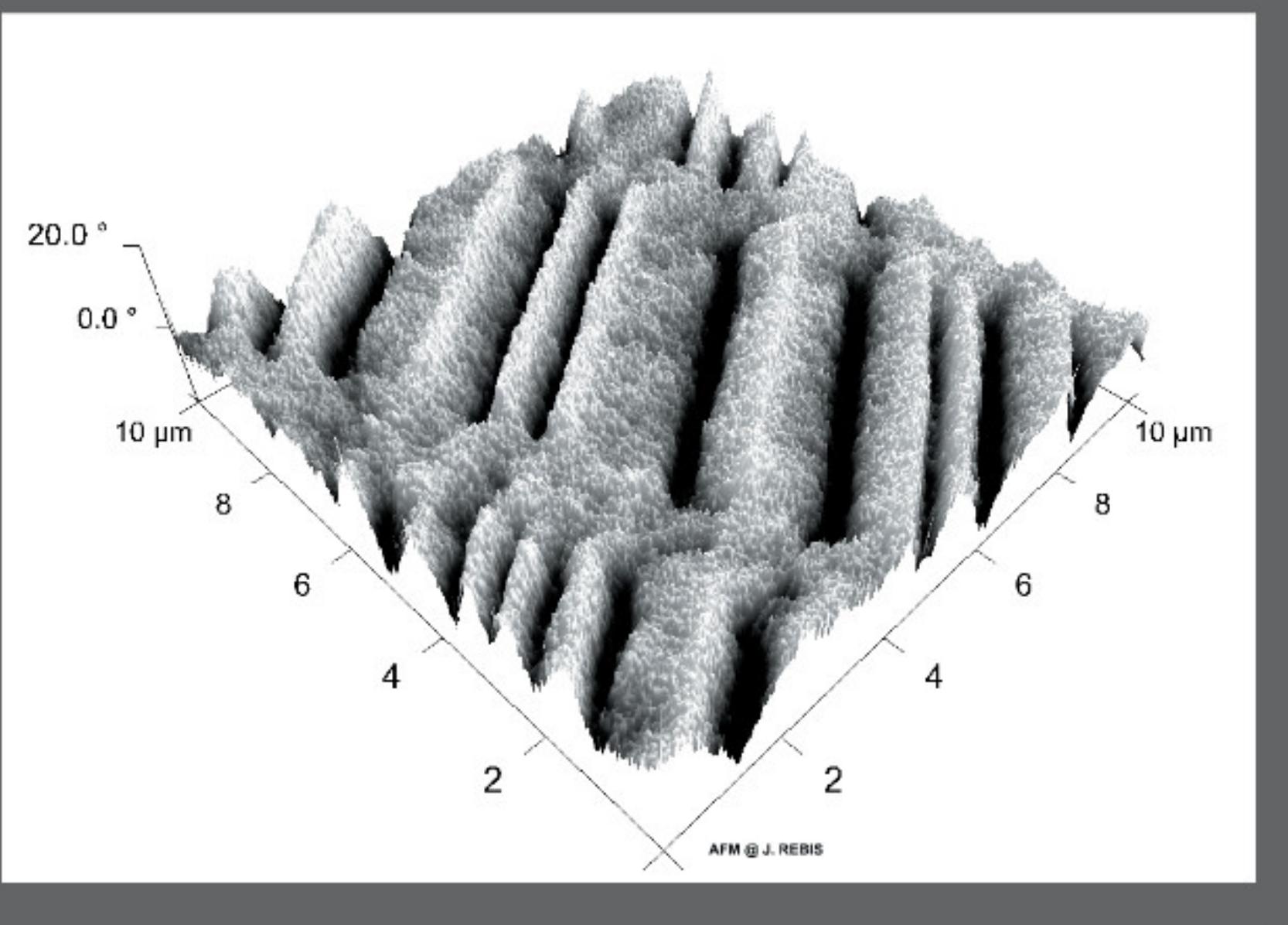
ÊTES-VOUS SÛR D'AVOIR BIEN EFFACÉ VOS FICHIERS ?

Comme vous le savez certainement, ce n'est pas parce que vous avez vidé votre corbeille que les fichiers qui s'y trouvaient sont effacés. Certes, vous n'y avez plus accès depuis Windows, mais ils sont encore sur le disque dur jusqu'à ce que d'autres fichiers viennent prendre la place qu'ils occupaient. Pour être vraiment sûr d'un effacement total, il faudra passer par un logiciel.

LE TOUR DU DISQUE EN 60 SEMAINES

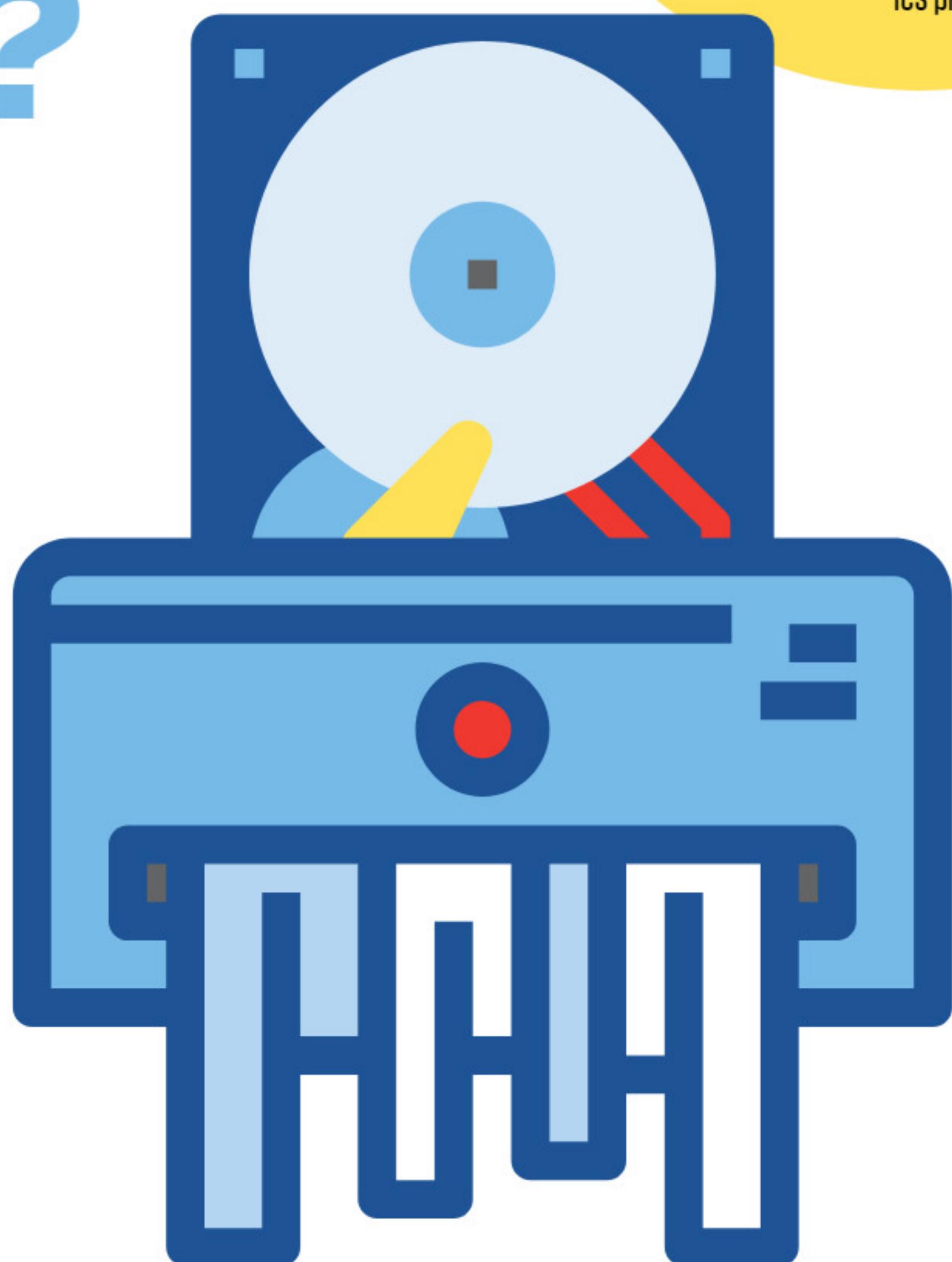


En utilisant un MFM (Magnetic Force Microscope), il est possible de reconstituer la surface des plateaux d'un disque dur. Par contre, il faudra la bagatelle de 60 semaines pour balayer la surface totale. Cette technique, utilisée par la NSA notamment, ne semble donc utilisable que sur de très petits volumes de données.



PETER GUTMAN,
UN SACRÉ PARANO

En 1996, Peter Gutmann a publié une étude sur la difficulté d'effacer de façon sécurisée un disque dur. Considéré comme une référence, cette étude préconise d'écraser les données et de réécrire dessus 35 fois ! Même les auteurs de BitKiller ne semblent pas convaincus de l'utilité de faire 35 passes, mais la question «*quelqu'un est-il vraiment capable de le faire ?*» n'est pas forcément pertinente : certains risques sont inacceptables, quelles que soient les probabilités.



Si vous avez beaucoup de fichiers à effacer de manière sécurisée (vente d'un PC familial avec des photos, etc.), le mieux est d'utiliser un logiciel qui va non seulement effacer les données, mais réécrire plusieurs fois là où elles étaient stockées. En effet, un formatage, même de bas niveau, ne permet d'effacer que les emplacements des fichiers et pas les fichiers eux-mêmes. BitKiller va réécrire sur votre fichier, réinitialiser la taille à 0 octet, le renommer de manière aléatoire jusqu'à 10 fois et l'effacer encore une fois. Avant cela, le logiciel propose plusieurs types d'effacement : placer des 0 en lieu et place de chaque bit, écrire des données aléatoires ou chiffrées jusqu'à 35 fois (méthode «Peter Gutman»). Aucun risque de voir resurgir votre liste de gens à entarter, ces photos un peu dérangeantes ou ces vidéos encore plus dérangeantes... Une fois que vous en aurez fini avec votre disque dur, personne ne pourra savoir ce qu'il contenait.



INFOS [BitKiller]

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

Difficulté : 💀💀💀

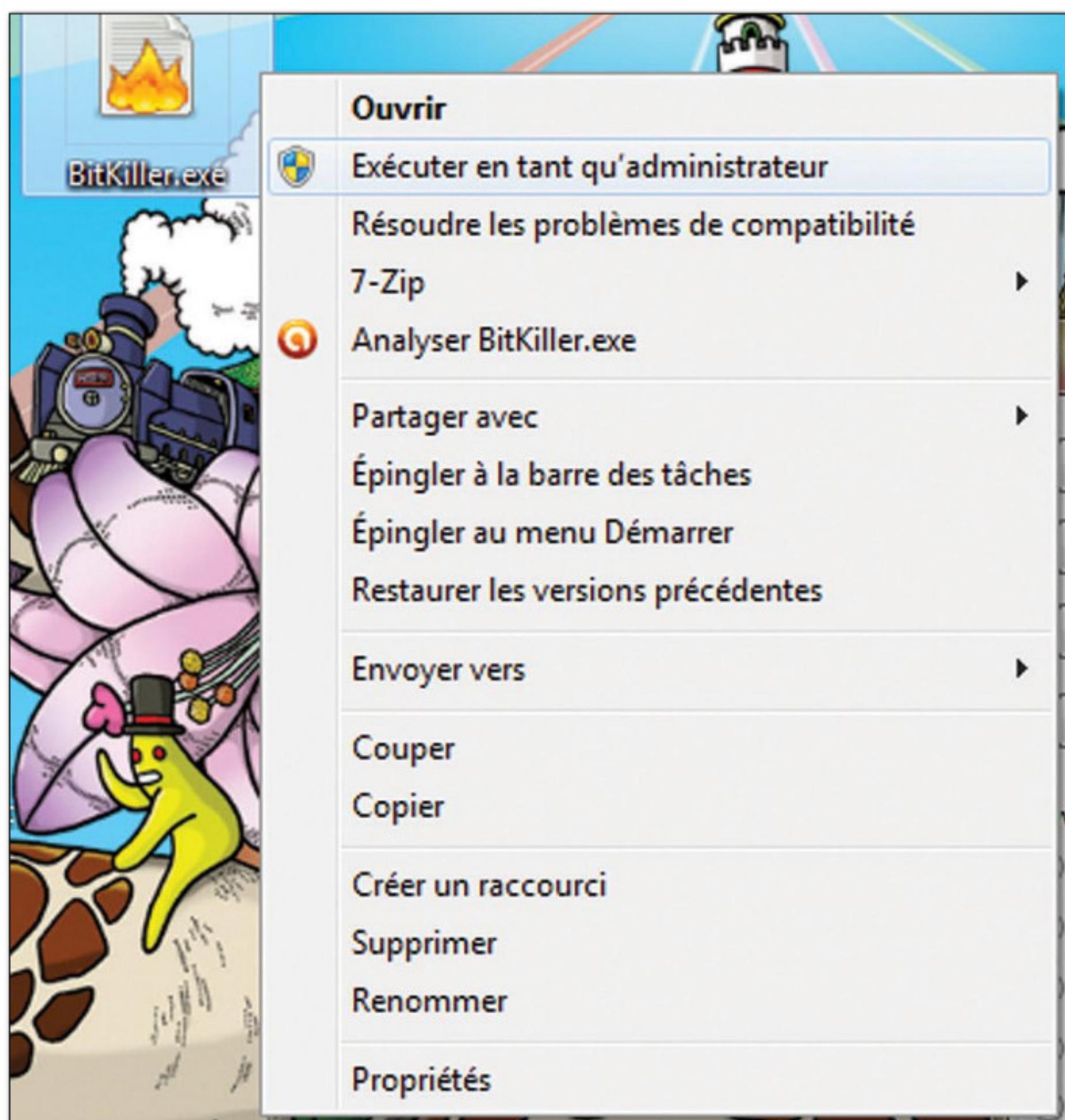
Rémanence des fichiers

BITKILLER : IL EFFACE, EFFACE ET EFFACE ENCORE UNE FOIS.



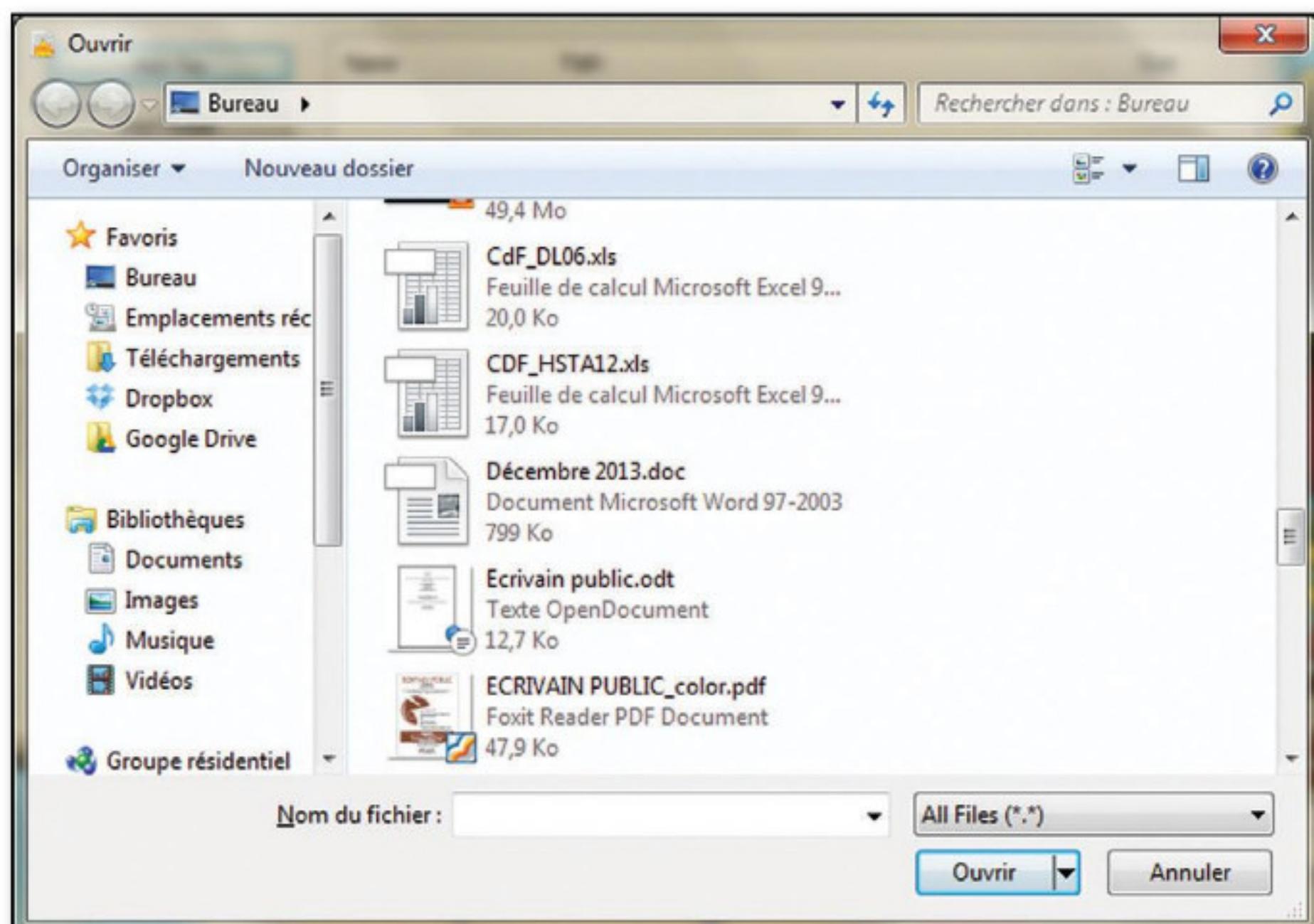
01 > MODE ADMINISTRATEUR

Bonne nouvelle, BitKiller ne nécessite aucune installation ! Vous êtes donc libre de l'emmener sur une clé USB puisqu'une fois dé-zippé il ne pèse que 40 ko. Si vous lancez le logiciel au travail où sur un poste qui n'est pas le vôtre, nous vous conseillons de le lancer en mode admin (clic droit dans le EXE puis **Exécuter en tant qu'administrateur**).



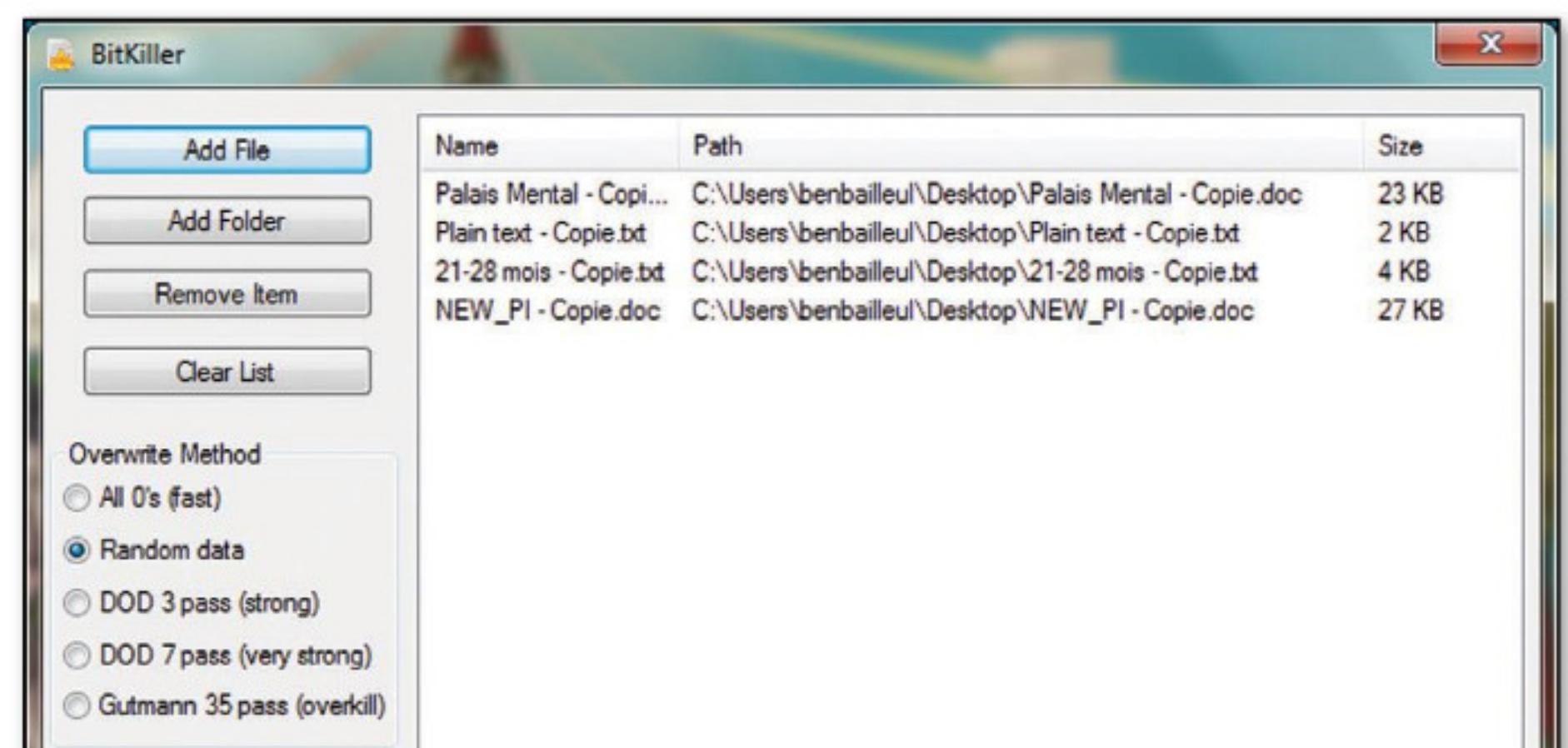
02 > L'INTERFACE

Difcile de faire plus simple au niveau de l'interface. Sur la droite, vous trouverez les boutons permettant d'ajouter un fichier, un dossier, de retirer une entrée ou de tout remettre à zéro. Ensuite, vous aurez les différentes méthodes d'effacement (voir étape 3) et les éléments à traiter sur la droite la fenêtre.



03 > LES MÉTHODES

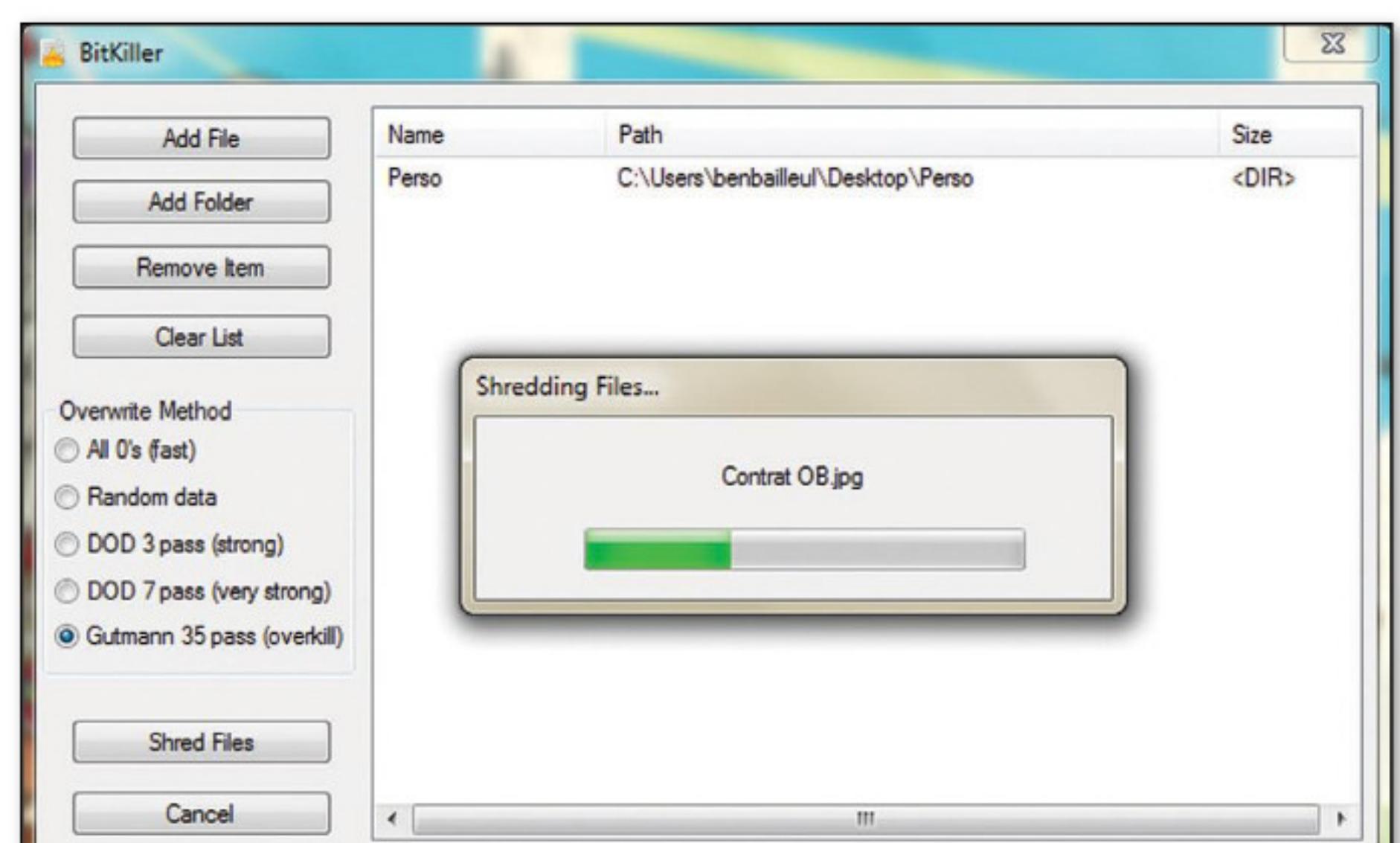
Les méthodes sont classées par ordre de solidité. La première met tous les octets d'un fichier à 0, la deuxième va placer des octets de manière aléatoire. **DOD** est la méthode préconisée par le gouvernement américain (Department Of Defense). Vous la trouverez ici en 3 ou 7 passes. Il s'agit en fait de remplacer les adresses



(l'emplacement des fichiers) par un caractère fixe, puis un caractère aléatoire et de recommencer 3 ou 7 fois. Enfin, vous pouvez aussi choisir la méthode **Gutman** (voir encadré).

04 > BYE BYE !

Après avoir pointé vers les fichiers/dossiers que vous voulez effacer, il suffit de faire **Shred Files**. Pour des fichiers personnels, nous vous conseillons la méthode DOD 3 ou 7 passes. Attention, car les fichiers seront directement effacés sans passer par la case «corbeille» !



FICHIER DLL MANQUANT ?

Si vous recevez un message d'erreur vous avertissant que votre PC ne contient pas tel ou tel fichier DLL, il faudra simplement que vous alliez télécharger le Package Microsoft Visual C++. Après un redémarrage, tout devrait rentrer dans l'ordre.

Lien : <http://goo.gl/FbZK6>



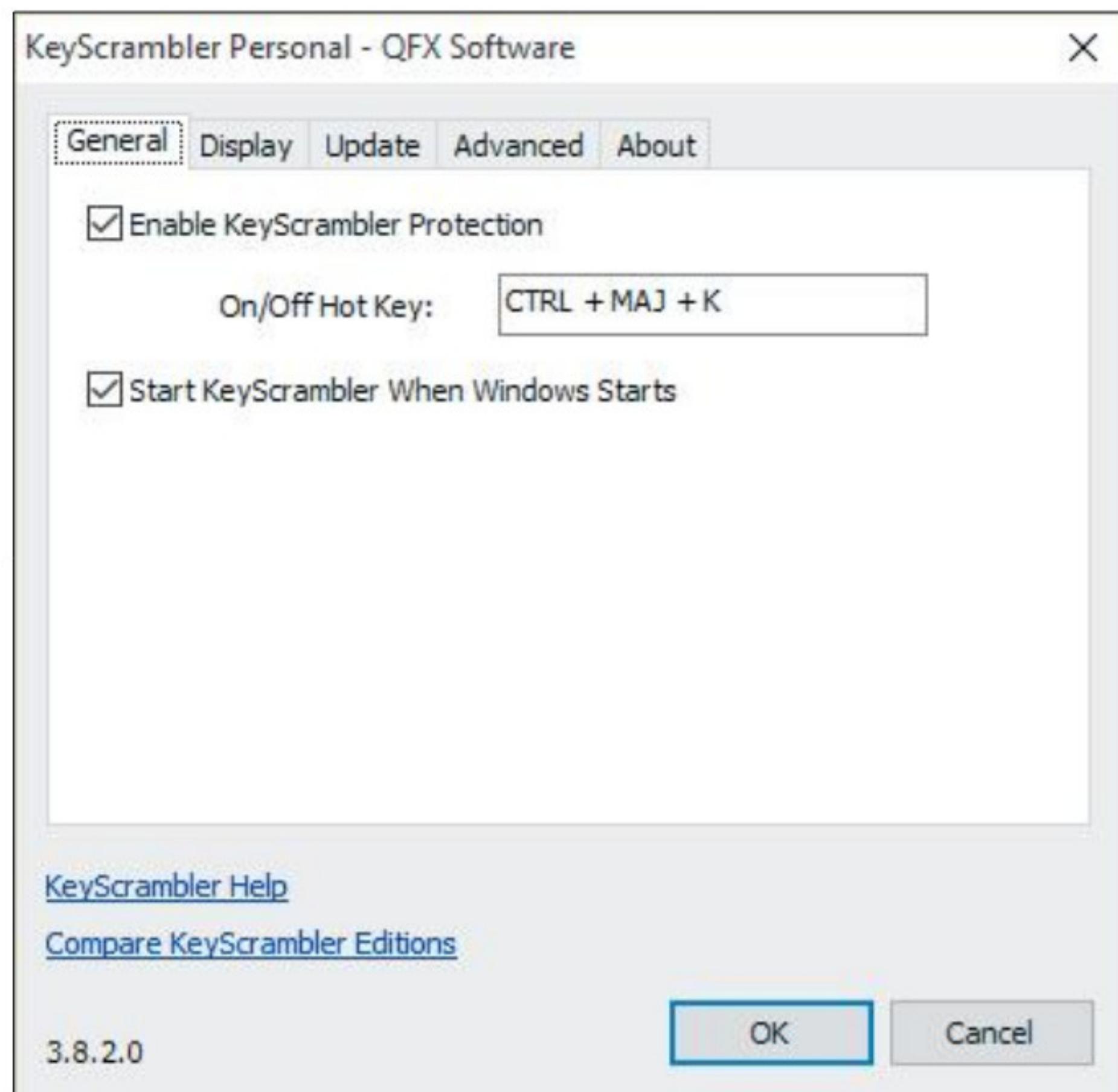


PROTECTION

Cryptez vos frappes au clavier

> AVEC KEYSCRAMBLER

Nous vous avons parlé plusieurs fois des keyloggers, ces logiciels malveillants qui, une fois installés sur vos PC, vont récupérer tout ce que vous saisissez au clavier : mots de passe, informations bancaires, etc. Même si un antivirus est



la meilleure arme contre ces malwares, il arrive que certains passent au travers du filet. Pour lutter contre cette menace, nous vous conseillons KeyScrambler un logiciel qui va crypter toutes les frappes directement au niveau du pilote de votre clavier pour ne le décrypter que dans votre navigateur Web (IE, Firefox ou Flock). Si un pirate essaye de lire vos frappes, il se retrouvera avec du texte inexploitable...

Lien : www.qfxsoftware.com

Protégez votre système d'une infection USB

> AVEC AUTORUN ANTIVIRUS PRO

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

Lien : <https://goo.gl/iUb9zj>

Vaccinez vos clefs USB

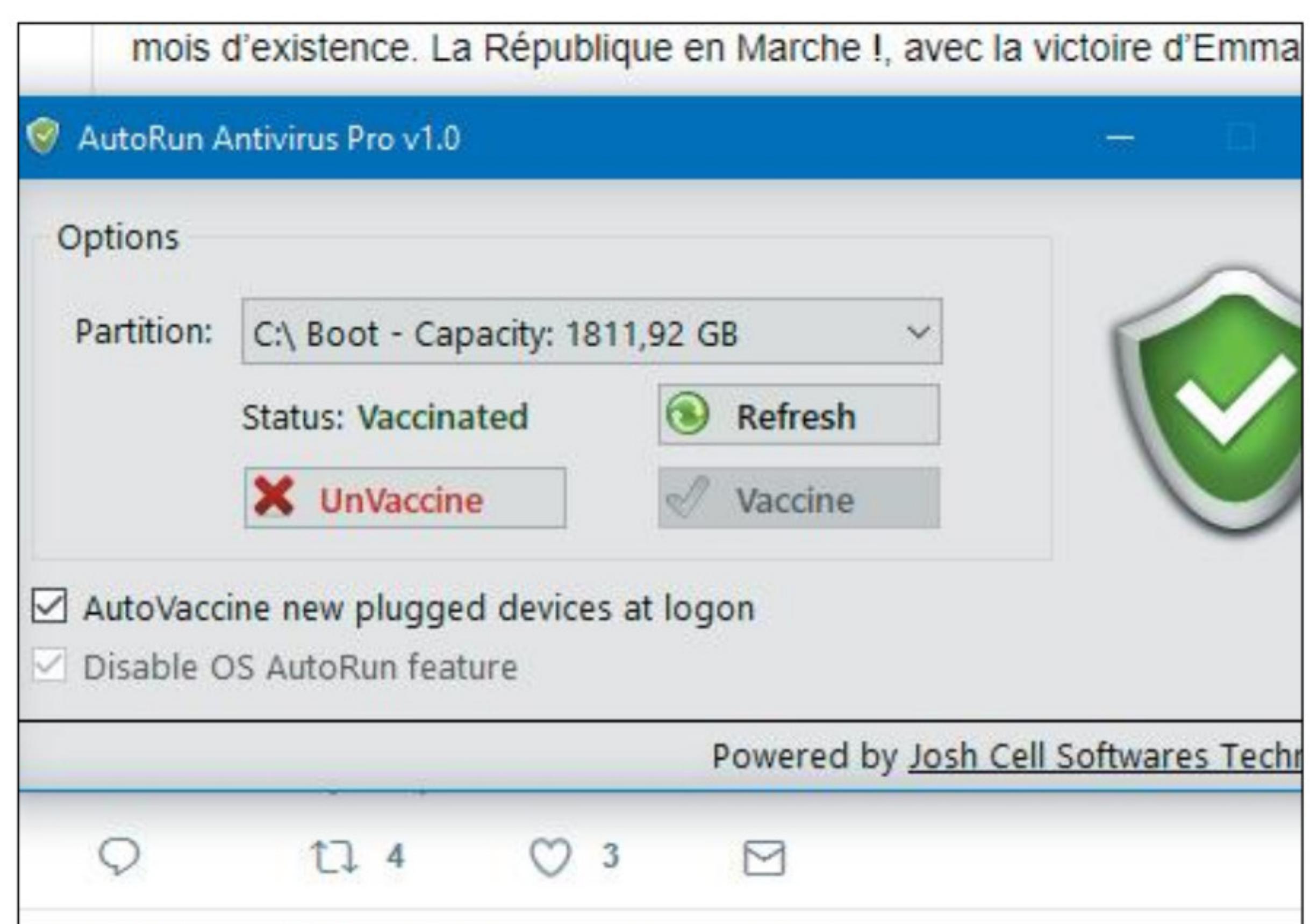
> AVEC USBFIX FREE

En complément d'AutoRun Antivirus Pro, qui se charge de protéger votre système d'une infection provoquée à cause d'une clef USB vétérane, utilisez USBFix. Le logiciel se charge de détruire les infections



repérées sur le périphérique de stockage externe, de la vacciner et tente de restaurer les fichiers qui ont été endommagés. Si d'autres fichiers sont infectés, ils iront en **Quarantaine**. Commencez par faire **Recherche** et effectuez un **Nettoyage** si des menaces sont repérées.

Lien : www.usbfix.net

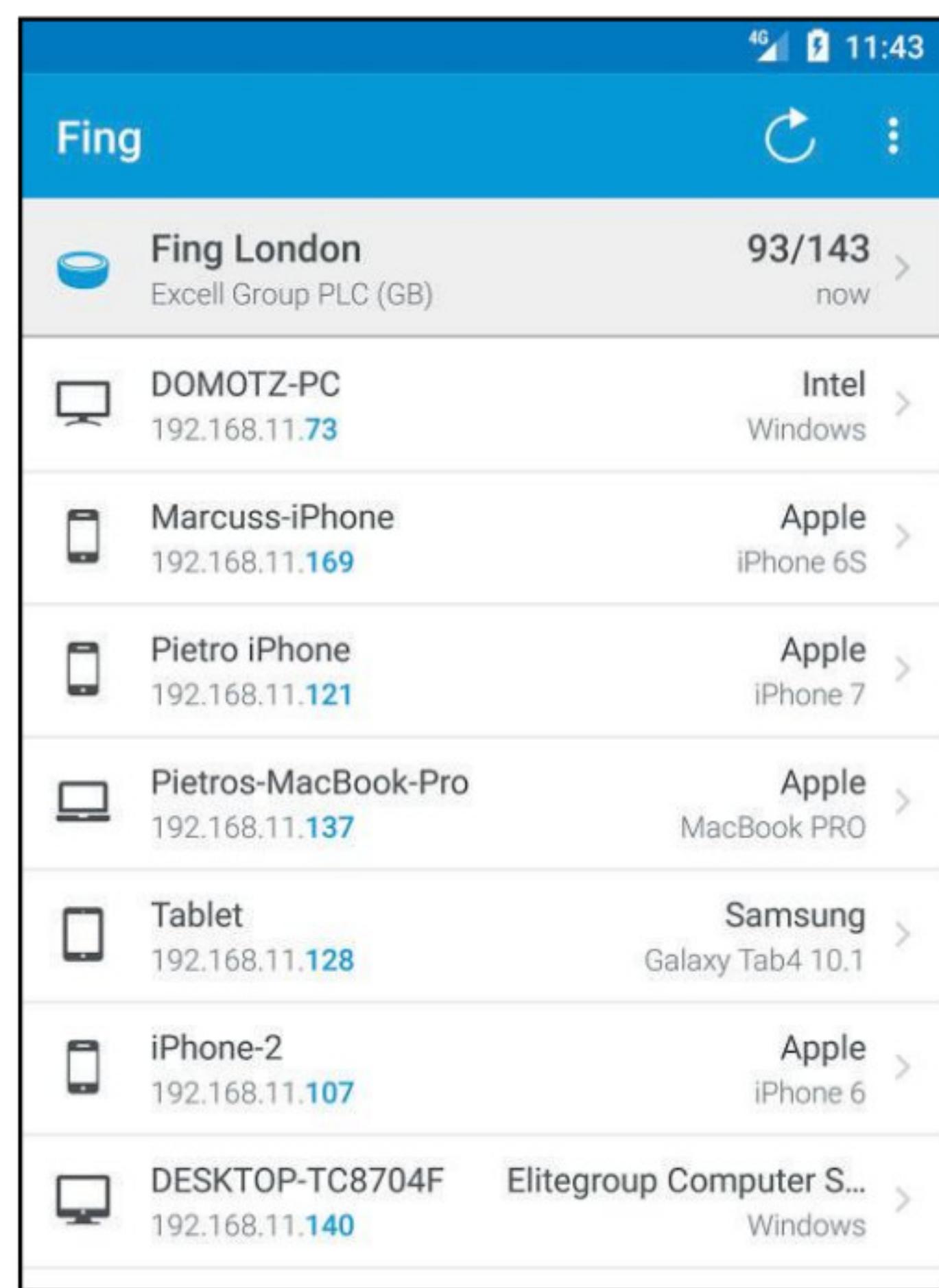


Expulsez les squatteurs de réseau Wi-Fi

> AVEC FING NETWORK TOOLS

Rien de plus rageant que de voir son réseau Wi-Fi complètement aux fraises, sans aucune raison. Impossible de regarder une vidéo en streaming, de faire une petite partie de DOOM en ligne ou de télécharger de la musique en toute légalité... Vous ne le savez peut-être pas, mais il est possible que certains voisins mal intentionnés ne se privent pas d'utiliser votre connexion. Avec l'application gratuite Fing Network Tools, disponible sur Android, vous dénichez les squatteurs et vous les expulsez par la même occasion. On ne peut pas s'emparer d'une connexion Wi-Fi impunément.

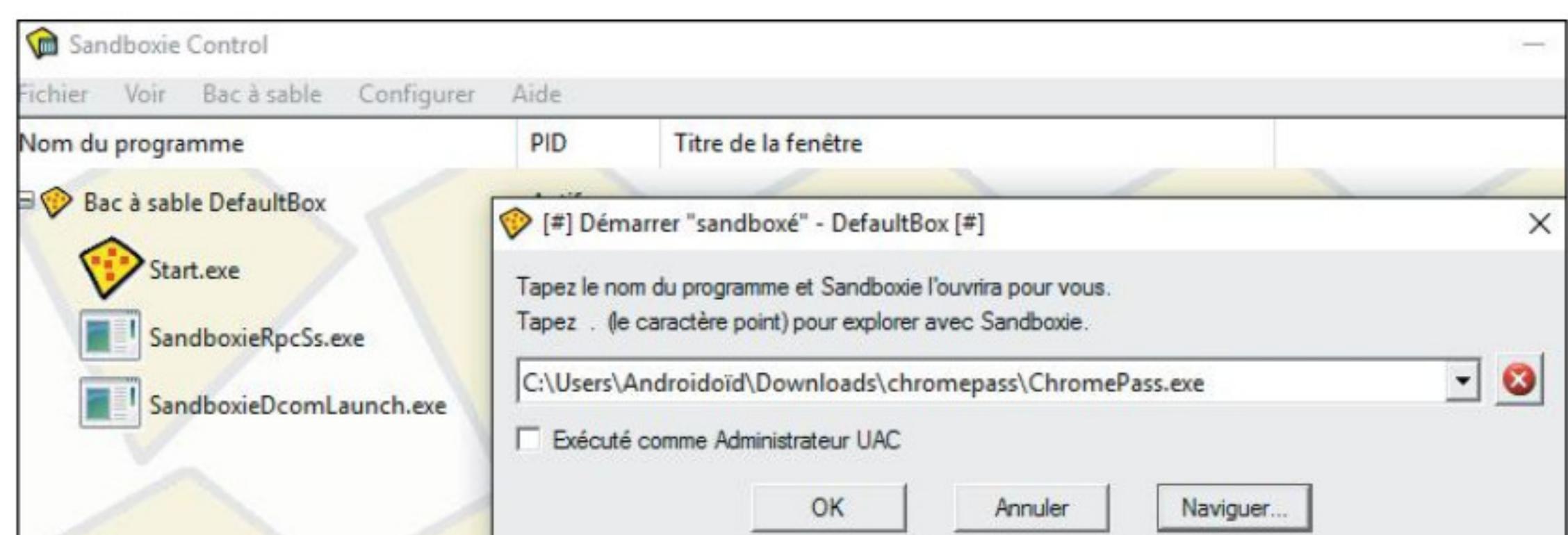
Lien : <https://goo.gl/rild3>



Testez un logiciel douteux avant de l'installer > AVEC SANDBOXIE

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

Lien : www.sandboxie.com



Scannez les ports de votre PC

> AVEC INOCULER

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

Résultat du scanner		
Ports ouverts ⓘ		
Aucun		
Ports fermés ⓘ		
port	service	commentaire
80	http	Le protocole HTTP est sûrement le plus utilisé sur le web pour les pages html majeures. Par contre, les applications assurant son traitement sont souvent bo
Ports masqués ✅		
port	service	commentaire
21	ftp	Utilisé pour le transfert de fichier entre ordinateurs. Les serveurs FTP ouvre Les hackers adorent les ports ftp anonymes.
22	ssh	Le shell SSH permet de se connecter à un serveur de façon sécurisée. SSH connexions, il encrypte toutes les échanges. SSH est donc un outil conseillé réseau.
		Le service telnet (en écoute sur le port 23) permet à deux machines distants

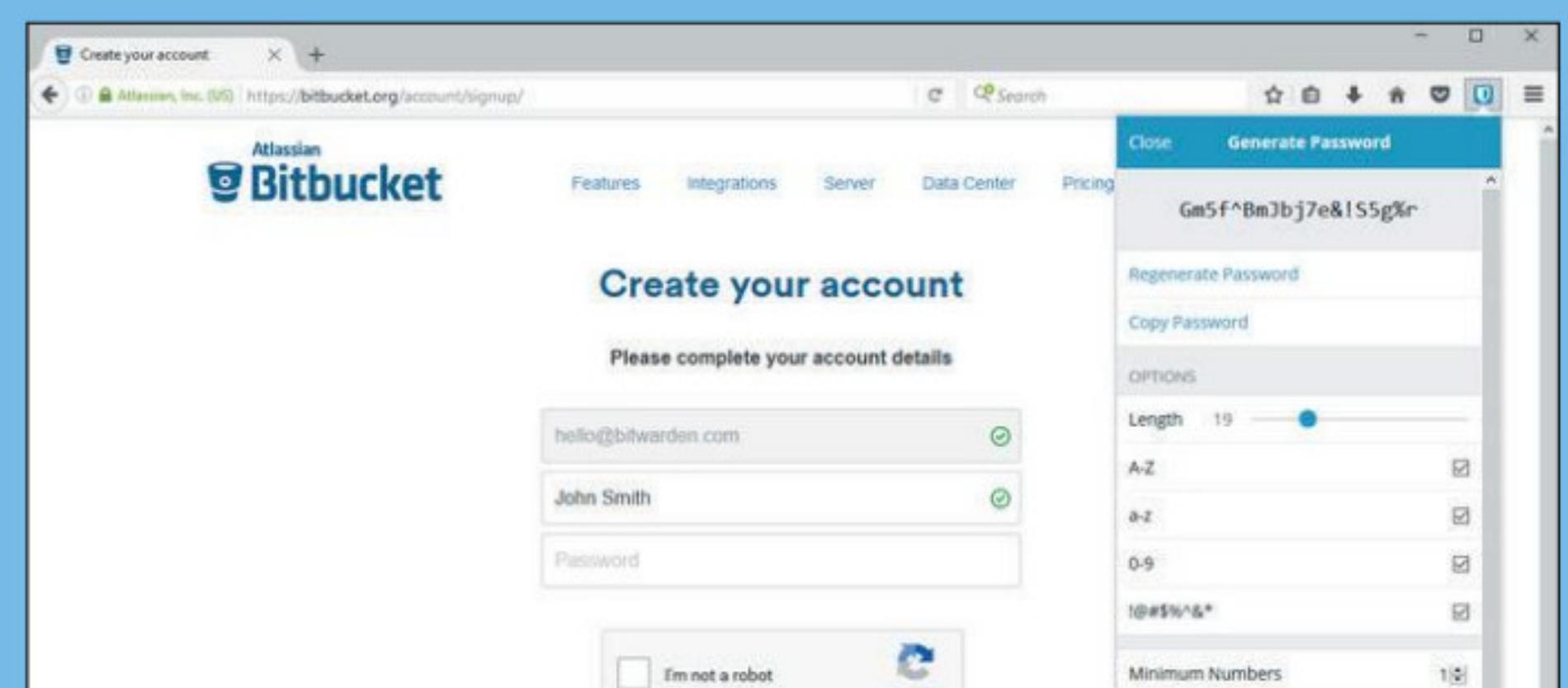
Lien : www.inoculer.com

Rapatriez tous vos mots de passe dans un gestionnaire Open Source

> AVEC BITWARDEN

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

Lien : <https://bitwarden.com>





FAKE

Nos ASTUCES POUR DÉTECTER LES FAUSSES IMAGES

Avec les réseaux sociaux, les fausses images et vidéos ont trouvé un formidable terreau. Une information en chasse une autre, la vérification devient accessoire, et les plus crédules peuvent facilement tomber dans le panneau. Voilà comment on commence à se persuader que Poutine chevauche des ours, et qu'Albert Einstein faisait du vélo pendant l'explosion de la première bombe nucléaire. Voici quelques conseils et astuces pour repérer ces fake pictures.



Tout est une question d'observation. Premièrement, lorsque vous tombez sur une photo suspecte, cherchez avant toute chose son origine. Qui l'a mise en ligne ? Qui en est l'auteur ? Le compte paraît-il sérieux ? Là encore, faites appel à votre bon sens. Si le compte à l'origine du cliché a été créé il y a 5 minutes par un profil nébuleux, sans description, posez vous la question. Ensuite, il convient d'analyser la fiabilité d'un site. Premièrement, vérifiez les adresses. Prenez par exemple les sites en .gouv ou .org, vous avez la certitude que vous surfez sur un site géré par l'État français. Les informations distillées sont censées être fiables. Si le doute persiste, faites un tour sur l'outil du journal Le Monde Décodeur. Rentrez l'URL du site suspect et découvrez s'il est fiable ou non. Pratique. Heureusement, tous les faussaires ne sont pas des ténors de Photoshop et il suffit de s'attarder trente secondes sur la photo pour se rendre compte de la supercherie. Prenons l'exemple des réseaux sociaux. Ce n'est pas parce qu'il y a marqué Twitter ou Facebook, que l'image est vraie. Certains malins s'amusent à reproduire l'interface de ces plates-formes pour donner l'illusion d'une vraie publication. Dans ce cas précis, il convient de s'attarder sur certains détails : taille et police utilisées, l'apparence et le placement du logo, couleurs similaires ou légèrement différentes, emplacements des différents modules (messages, likes, conversations, etc.) Certaines petites erreurs permettent de voir le pot aux roses. Dites-vous qu'en France,



AVANT

selon un rapport de Médiamétrie daté de 2016, 17% des jeunes s'informent uniquement sur les réseaux sociaux ! D'où l'importance cruciale de savoir distinguer le vrai du faux...

Autre conseil appréciable, si une photo vous paraît trop belle, incroyablement spectaculaire, follement insolite, ou totalement WTF, elle est probablement fausse. Regardez ce poney par exemple. Ou comment rendre une photo banale et plutôt ennuyeuse en quelque chose d'assez dramatique et poétique, n'est-ce pas ?

APRÈS LA RÉFLEXION, LA DÉTECTION ET L'ÉLIMINATION

Maintenant que vous avez mis en doute quelques éléments de la photo suspecte, vous pouvez vous assurer définitivement de sa fiabilité. Plusieurs méthodes accessibles existent. La première consiste à effectuer une recherche inversée. Pour ce faire il suffit de copier l'adresse du lien et de faire une recherche sur Google Images. Vous pouvez également enregistrer le cliché sur votre disque dur et l'importer directement sur le moteur de recherche. Ceci fait, Google va chercher des images similaires ou portant sur le même thème. Si l'image en question a été partagée plusieurs fois par plusieurs sites réputés comme sérieux, sa véracité semble tout indiquée. L'inverse est tout aussi vrai. Si l'image a été partagée par des sites conspirationnistes, parodiques, politiquement engagés, et tutti quanti sa véracité semble bien compromise.



Ensuite, les fins limiers pourront scruter les métadonnées de la photo. Les métadonnées c'est en quelque sorte la carte d'identité d'un cliché : modèle d'appareil utilisé, objectif, ouverture focale, isométrie, date et localisation, nom de l'auteur, etc. Pour accéder à ces infos (également appelées EXIF) vous pouvez soit faire un clic droit sur la photo, puis propriétés et détails, soit utiliser des outils disponibles en ligne. Exif Viewer reste une valeur sûre tout comme Jeffrey's image Metadata Viewer.

Il ne vous reste plus qu'à comparer l'image

Jeffrey's Image Metadata Viewer

Jeffrey Friedl's Image Metadata Viewer (How to use)

Some of my other stuff
- My Blog - Lightroom plugins - Pretty Photos - "Photo Tech"

URL: URL of image on the web
File: Choisir un fichier Aucun fichier choisi

Je ne suis pas un robot reCAPTCHA Confidentialité - Confidentialité

View Image Data

This tool remains available so long as I can keep it free and the bandwidth doesn't cost me too much. A gift of thanks is always appreciated, but certainly not required. Send a gift via PayPal, or perhaps an Amazon gift certificate (to: jrfiedl@yahoo.com), or perhaps send me some good karma by doing something kind for a stranger.

If you have questions about this tool, please see the FAQ.

avec les données affichées. Exemple : la luminosité est-elle trop forte par rapport à l'isométrie renseignée ? La netteté de tel ou tel sujet paraît-elle excessive avec cet appareil ? Là encore, il faudra être vigilant et s'attarder sur le moindre détail. Dans ce cas précis, il faut des connaissances en photographie (direction tutoriel sur Youtube ou bienappelez votre copain photographe, on en a toujours un). En appliquant ces quelques conseils, vous préservez un peu l'humanité de l'avalanche de conneries présentes sur la toile. Peut-être pas l'humanité, mais au moins vous et votre entourage. C'est déjà pas mal.

DÉCOUVREZ SI UNE PHOTO EST TRUQUÉE AVEC FORENSICALLY



Forensically est un site qui vous propose de savoir si une photo a été truquée ou si des éléments ont été ajoutés et modifiés. Il suffit d'uploader votre fichier et d'utiliser les différents menus comme Error Level Analysis ou Clone Detection pour voir les irrégularités. Même retravaillée par un virtuose, vous briserez l'illusion à chaque fois...

Forensically Beta Open File Help

Magnifier Magnification 4 Enhancement Histogram Equalization

Clone Detection

Error Level Analysis

Noise Analysis

Level Sweep



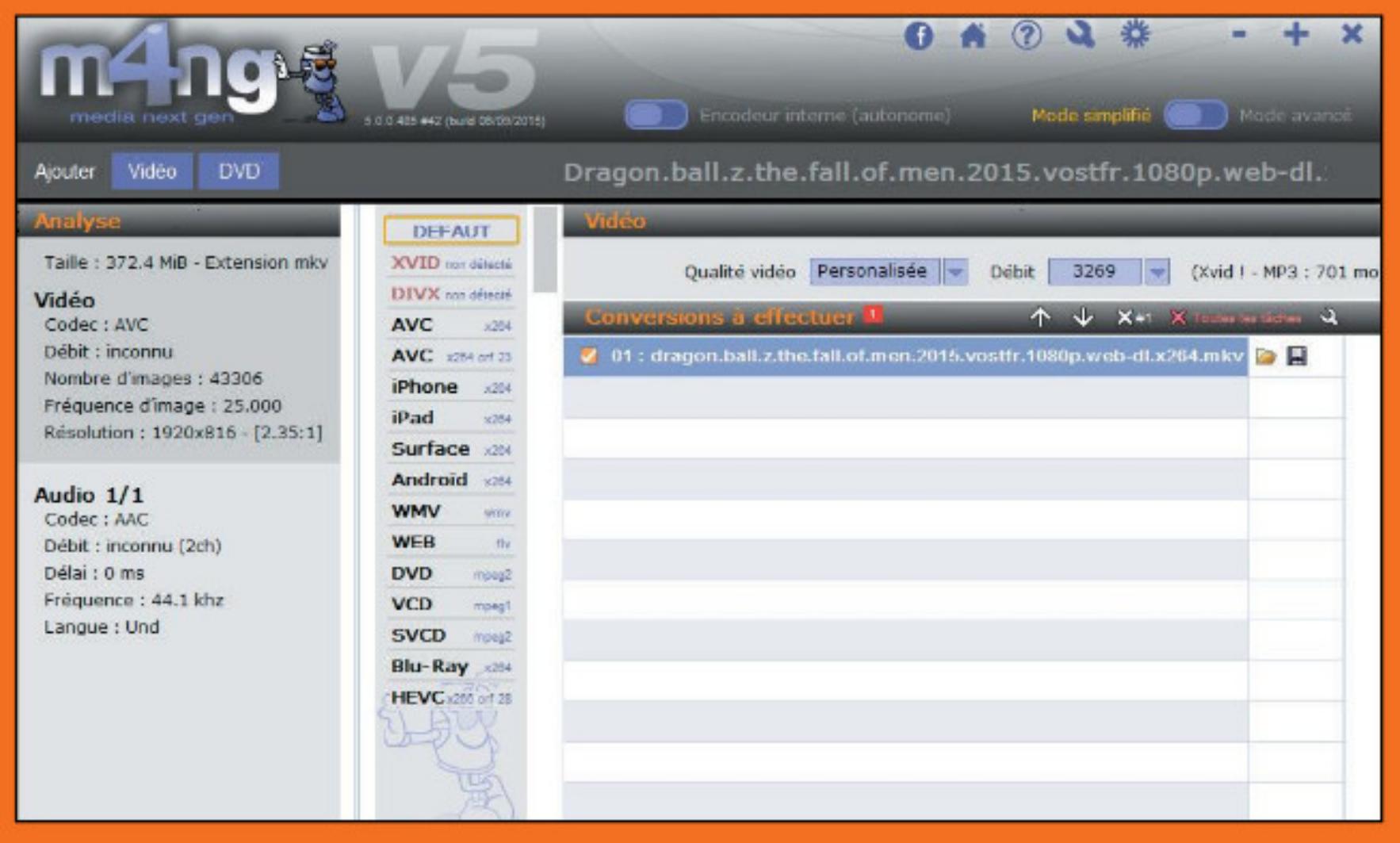
MULTIMÉDIA

De l'encodage à la carte

> AVEC M4NG V5

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'éisodes de votre série préférée et vous voudriez les lire sur votre iPad, PC, PSP ou smartphone Android ? Cette vidéo téléchargée ne fonctionne pas sur votre machine de prédilection ? Changer l'encodage du son uniquement ou fusionner deux vidéos en une seule ? Pour toutes ces tâches, m4ng s'en sortira sans problème. Il est aussi possible de couper, coller, isoler le son, 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.

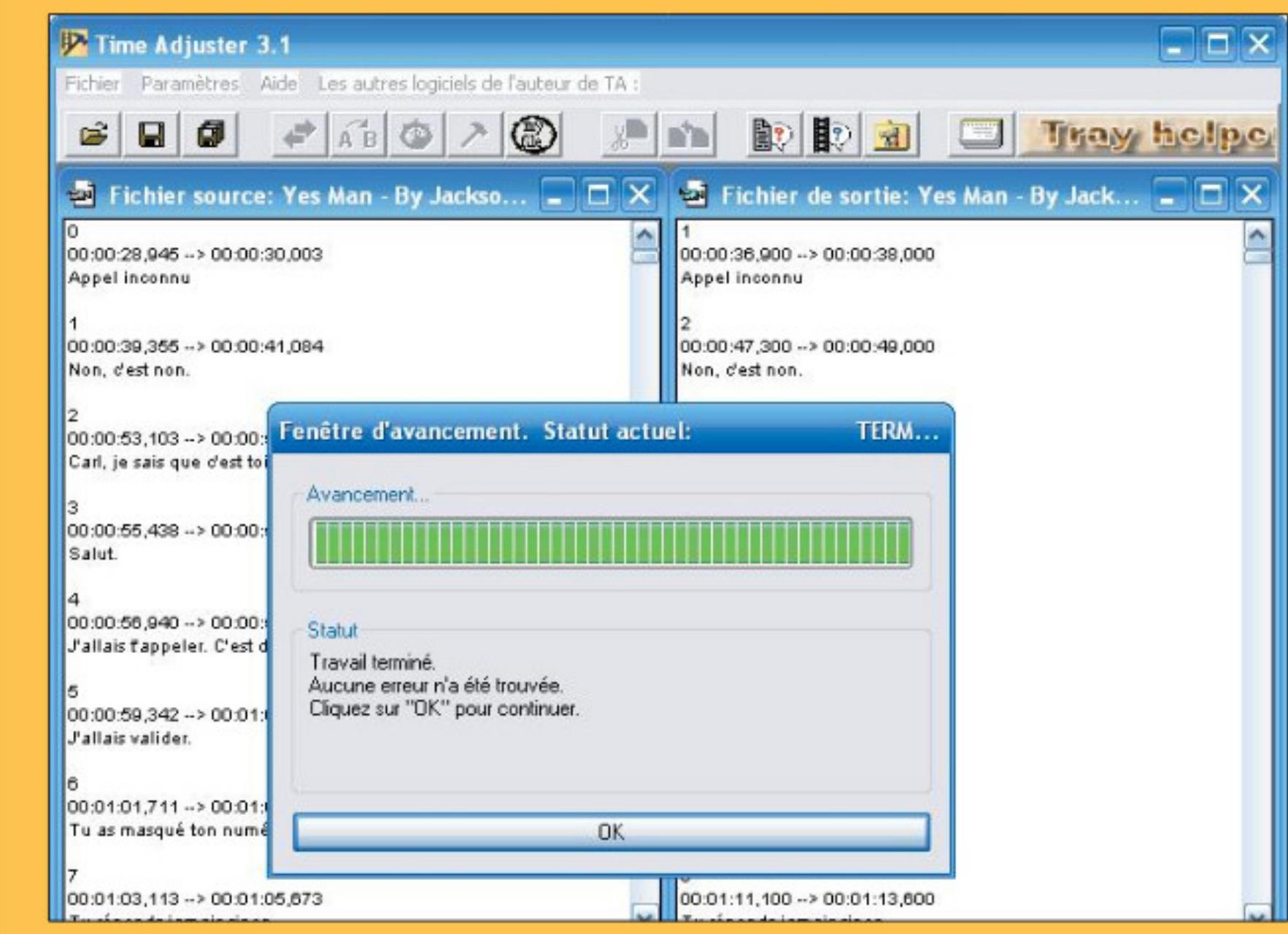
Lien : www.m4ng.fr



«Calez» vos sous-titres très simplement > AVEC TIME ADJUSTER

Il arrive souvent que les sous-titres et la vidéo soient décalés lorsque vous regardez un film ou une série. Gênant pour certains, insupportable pour les autres... Time Adjuster permet de remédier à ce problème en synchronisant les deux fichiers. Il suffit de charger le fichier SUB ou SRT puis de cliquer sur **Synchroniser**. Arrêtez la vidéo au moment où le son et le texte correspondent. Notez que le programme permet aussi de séparer, réunir, réparer ou convertir des fichiers de sous-titres.

Lien : www.ireksoftware.com/ta

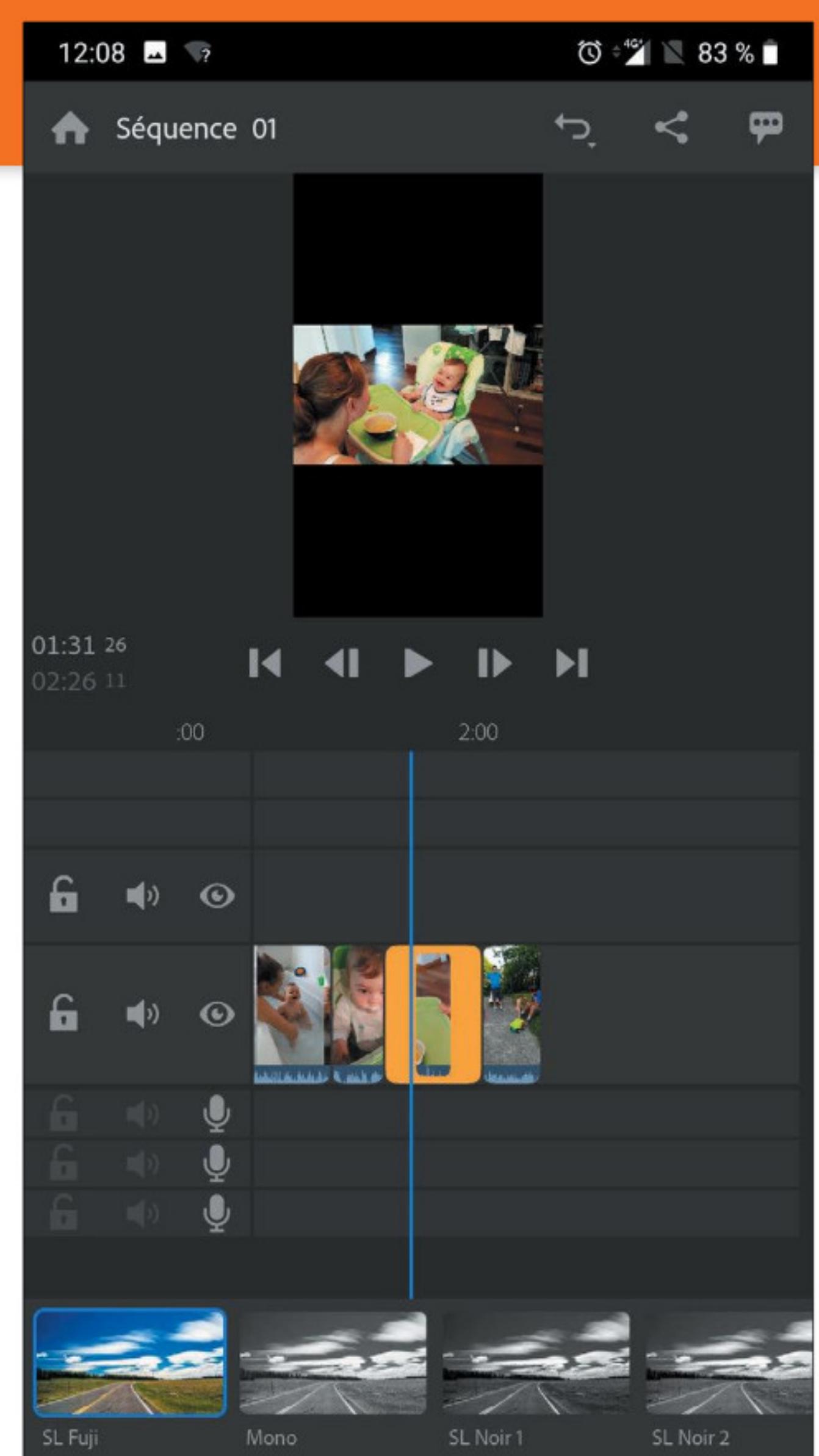


Le montage vidéo sur mobile

> AVEC ADOBE PREMIERE RUSH

Adobe Premier Rush est une application de montage vidéo sur mobile très performante. Avec cette dernière, vous allez pouvoir créer, partager et monter des vidéos le plus simplement du monde tout en profitant de la puissance des solutions Adobe dans ce domaine. Car "Rush" dispose d'une interface intuitive avec des fonctionnalités inédites jusque là sur mobile. Les monteurs amateurs ou les pros de Premiere ne seront pas dépayrés puisque l'appli reprend les codes et les fonctionnalités des logiciels PC. Il s'agit donc d'une appli qui gère le multipiste, propose des transitions, des filtres, des corrections de couleur, de cadrage et un outil de titrage. Le but de Rush est de proposer un outil presque complet aux YouTubeurs, créatifs et community managers pour tout faire depuis leur mobile dans le train ou dans l'avion sans avoir à sortir leur PC. Une fois montée la vidéo peut être très simplement partagée sur Youtube, Facebook ou Instagram. Le cloud Adobe permet aussi de stocker vos travaux en cours ou finalisés. Il ne s'agit pas d'une solution pour Monsieur Tout le Monde, mais elle est très intéressante notamment pour sa compatibilité avec l'application Adobe Premiere Pro, mais aussi avec les outils After Effects, Audition et Adobe Sensei. Commencez le travail sur votre Mobile et finissez-le sur votre ordinateur ! Un outil si puissant est forcément payant. Vous avez pourtant 3 exportations gratuites pour tester toutes les fonctionnalités, mais si vous êtes séduit, il faudra passer par un abonnement mensuel à 10,99 € avec 100 Go de stockage vidéo offerts. Notez que si vous avez déjà un abonnement à Creative Cloud (formule *Toutes les applications* ou *Premiere Pro*), Rush est compris dans le prix. Le seul hic c'est que les smartphones compatibles ne sont pas très nombreux. Eh oui, il en faut de la puissance pour faire tourner une appli de ce type !

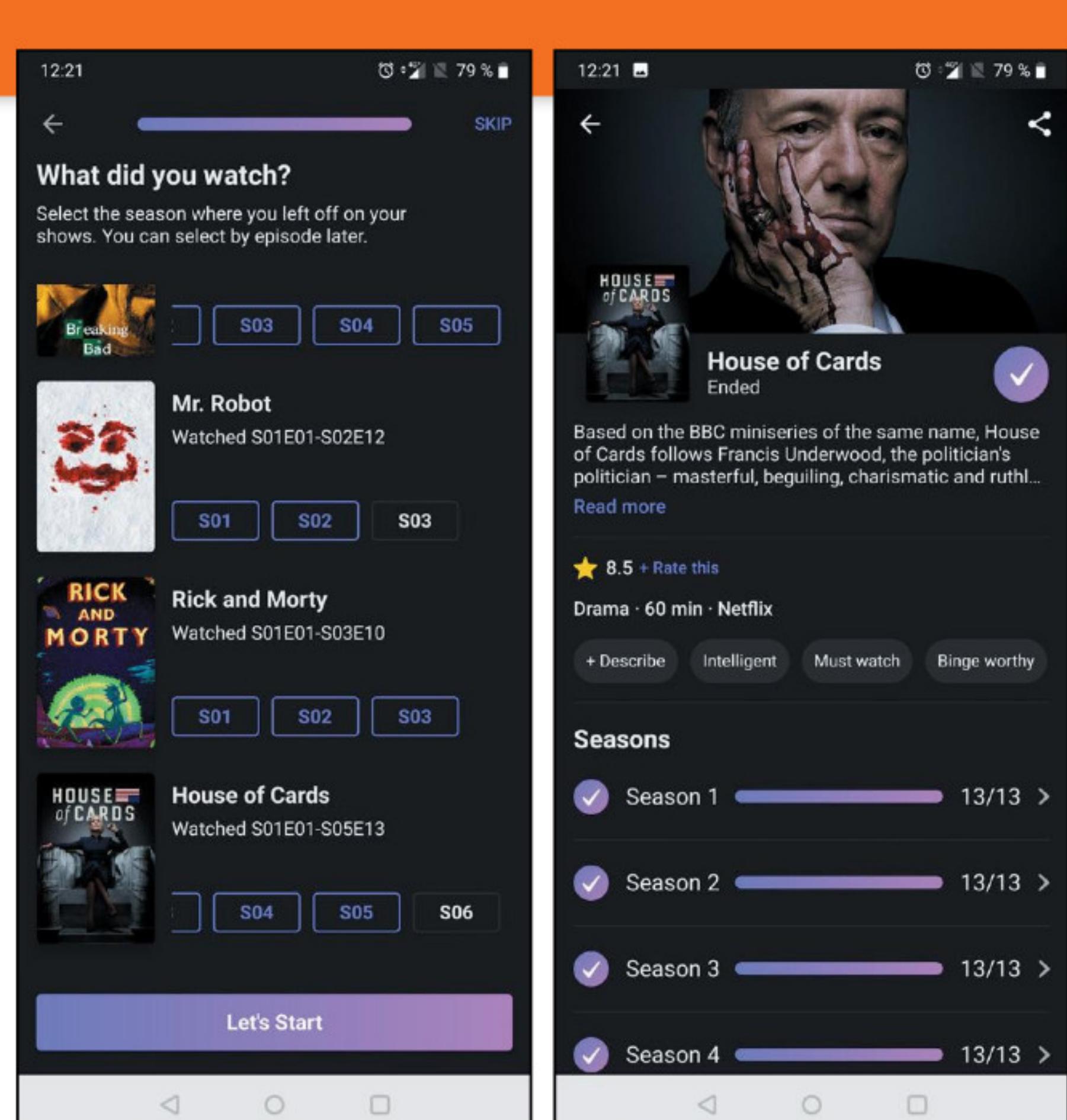
Lien : https://frama.link/fe6_2WRA



Ne ratez plus un épisode > AVEC HOBI

Hobi est une application qui permet de suivre l'avancement de vos séries. Pas facile en effet de garder le rythme entre les séries qui s'arrêtent pour reprendre l'année d'après, les pauses à mi-saison et les heures de diffusions américaineson peut vite fait oublier un épisode ! Hobi vous proposera de choisir les séries que vous regardez dans une liste de contenus populaires, mais libre à vous d'ajouter celles qui ne sont pas mises en avant. Pour chaque série, il faudra ensuite dire à l'appli où vous en êtes saison par saison et même épisode par épisode. Si vous n'êtes pas "à jour", cela peut prendre un peu de temps...sauf si vous avez un compte Trakt ! Ce service qui permet de gérer votre collection de films et séries TV garde le fil de ce que vous regardez sur Netflix ou sur des media center type Kodi et Plex. Vous pouvez programmer une soirée puisque vous savez exactement quand tel ou tel épisode sort avec l'heure exacte : que vous soyez accro à Netflix, OCS ou plutôt YggTorrent, c'est parfait ! Selon les séries que vous regardez et suivez, Hobi vous propose des programmes en adéquation avec vos goûts (**Tailored to your taste**) ou tout simplement à la mode (**Trending**).

Lien : https://frama.link/_fSUW27A



La télé sans prise de tête > AVEC TNT FLASH TV

Il existe quantité d'applications permettant de regarder la TV sur son smartphone, mais il arrive souvent que les publicités les envahissent. TNT Flash TV permet de regarder les chaînes de télévision de la TNT, ainsi que de consulter les programmes et les résumés. Il ne s'agit pas d'IPTV illégale, l'utilisateur est mis en relation avec les flux vidéos officiels des chaînes. L'ensemble de ces canaux provient directement des sources officielles, aucune copie ou modification n'est effectuée. Il y a Canal+ dans la liste; mais vous ne pouvez



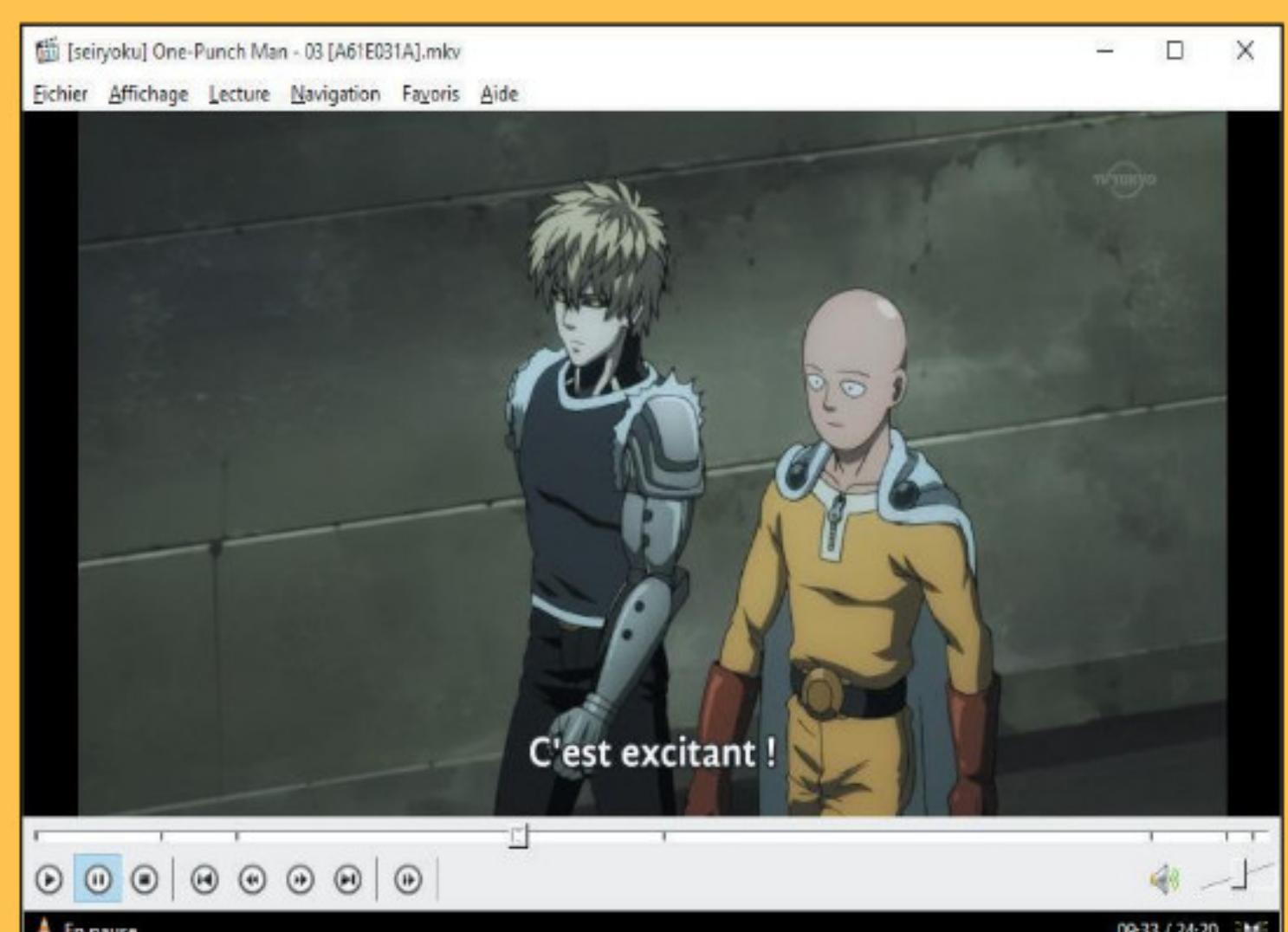
regarder que lorsque les programmes sont en clair par exemple. L'appli compte 48 chaînes de la TNT sans compter les France 3

de chaque région. Il est possible de voir les programmes par chaîne, mais aussi les diffusions en direct au moment où vous consultez l'appli. Vous pouvez aussi regarder les programmes du soir d'un simple coup d'œil. Il est possible de choisir la qualité de diffusion. Selon les chaînes on peut même avoir du 720p, mais on peut aussi descendre à beaucoup moins pour économiser la bande passante ou son forfait data (144 ou 180p).

Lien : <https://frama.link/0HmZZNjf>

Un player qui privilégie la simplicité > AVEC MEDIA PLAYER CLASSIC

Ce lecteur multimédia est une alternative crédible à Windows Media Player ou à VLC puisqu'en plus d'être léger il permet de lire la plupart des formats que vous pourrez



trouver. Très à l'aise avec la vidéo (DivX, Xvid, Blu-ray, MKV, H265, Sub, etc.) il lit aussi les formats musicaux. Ce Media Player Classic est avant tout pour les possesseurs de configurations plus anciennes, mais vous pouvez aussi l'utiliser lorsque votre processeur est sollicité.

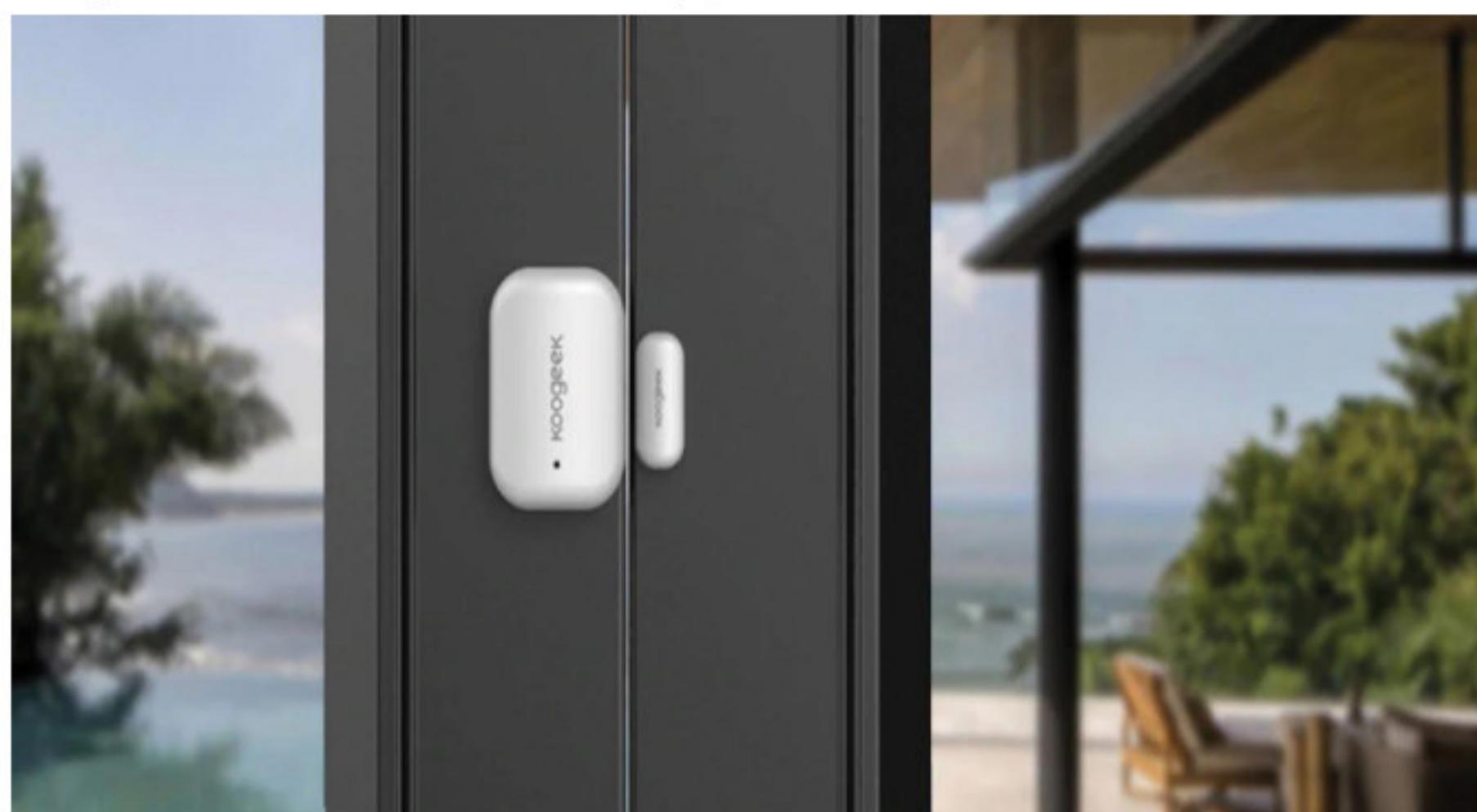
Lien : <http://goo.gl/WBBLx>



MATÉRIEL

» CAPTEUR D'OUVERTURE DE PORTE KOOGEEK, LA DOMOTIQUE FACILE

La domotique devient de plus en plus simple et de moins en moins onéreuse. Même sans être un geek de niveau 58, vous pouvez très simplement gérer vos luminaires, votre chaudière et plein d'autres choses grâce à vos appareils mobiles et à votre assistant connecté (même si vous n'en avez pas forcément besoin). Ici nous vous proposons une belle promotion sur le système de détection d'ouverture/fermeture Koogeek. Si vous avez un Apple Homekit, Alexa ou un module Google Assistant, le



module Koogeek va se connecter à lui et vous notifier en cas d'ouverture et de fermeture de votre porte ou fenêtre. Il suffit de l'installer à l'aide d'autocollants très adhésifs (des autocollants supplémentaires sont livrés au cas où vous voudriez déplacer l'appareil) et l'alimentation se fait par une simple pile au lithium à changer tous les 2 ans. Vous ne tomberez pas en panne, car l'appli vous préviendra en cas de batterie faible. C'est un produit idéal pour prévenir des accidents domestiques, des cambriolages ou du mauvais temps.



Prix : 30 € **Lien :** <https://frama.link/7HMBN0bW>

» SCANNER 3D CICLOP HE3D :

Apparue à la fin des années 70, la technologie de triangulation laser a ouvert la voie aux premiers équipements capables de numériser en 3D des objets. Longtemps réservé aux industriels, cet outil s'est peu à peu démocratisé à tel point que l'on retrouve aujourd'hui des scanners 3D abordables et faciles à prendre en main. Ce modèle He3D de Ciclop repose sur la technologie de triangulation laser et permet de numériser des objets en moins de huit minutes. Vendu en kit, ce scanner permet de retranscrire en fichier numérique un objet pour une impression 3D ultérieure (de 5x5cm à 20x20cm et maximum 3kg)

Prix : 107 €
Lien : <https://frama.link/W45q8Yqt>



» BOX TV BEELINK GT-KING : PETIT, MAIS COSTAUD

Si vous désirez investir dans un box TV / média center, pourquoi prendre un appareil à bas prix qu'il faudra changer dans quelques mois ? La Beelink GT-King est la superstar du milieu avec un processeur surpuissant, une compatibilité 4K, une télécommande qui répond à la voix et une connectique très complète. Pour moins de 100 €, c'est une aubaine ! Rappelons que ces boîtiers électroniques prennent place sous votre TV et servent à récupérer tous les fichiers de votre réseau pour en profiter sur votre Home Cinema. Que vos films, séries, photos ou MP3 soient sur votre PC, votre NAS ou un disque dur externe, vous pourrez les atteindre à travers le réseau. On peut aussi brancher directement des périphériques USB sur la box ou appairer un appareil en Bluetooth. Cette GT-King est donc une box TV sous Android 9 qui propose tout ce que le Google Play Store a à offrir : applis (Netflix, Molotov, OCS), jeux, VoD, etc. Il s'agit aussi du plus puissant des appareils de ce genre puisqu'il embarque un processeur Amlogic S922X 8 cœurs avec 4 Go de RAM LPDDR4. Cette configuration musclée permet de prendre en charge les derniers codecs, mais aussi la 4K en 60 fps. L'appareil comporte 64 Go de stockage pour les apps mais c'est surtout sa connectique qui impressionne avec 2 ports USB 3.0 (+ 1 USB 2.0), un audio SPDIF, un RJ45 1000Mbps, le WiFi ac de 5ème génération, un slot pour carte mémoire et l'HDMI 2.0. La télécommande incluse répond même à la voix !



Prix : 98 €
Lien : <https://frama.link/8PCWZqLK>

» RASPBERRY PI 4 : LE RETOUR DE LA REVANCHE

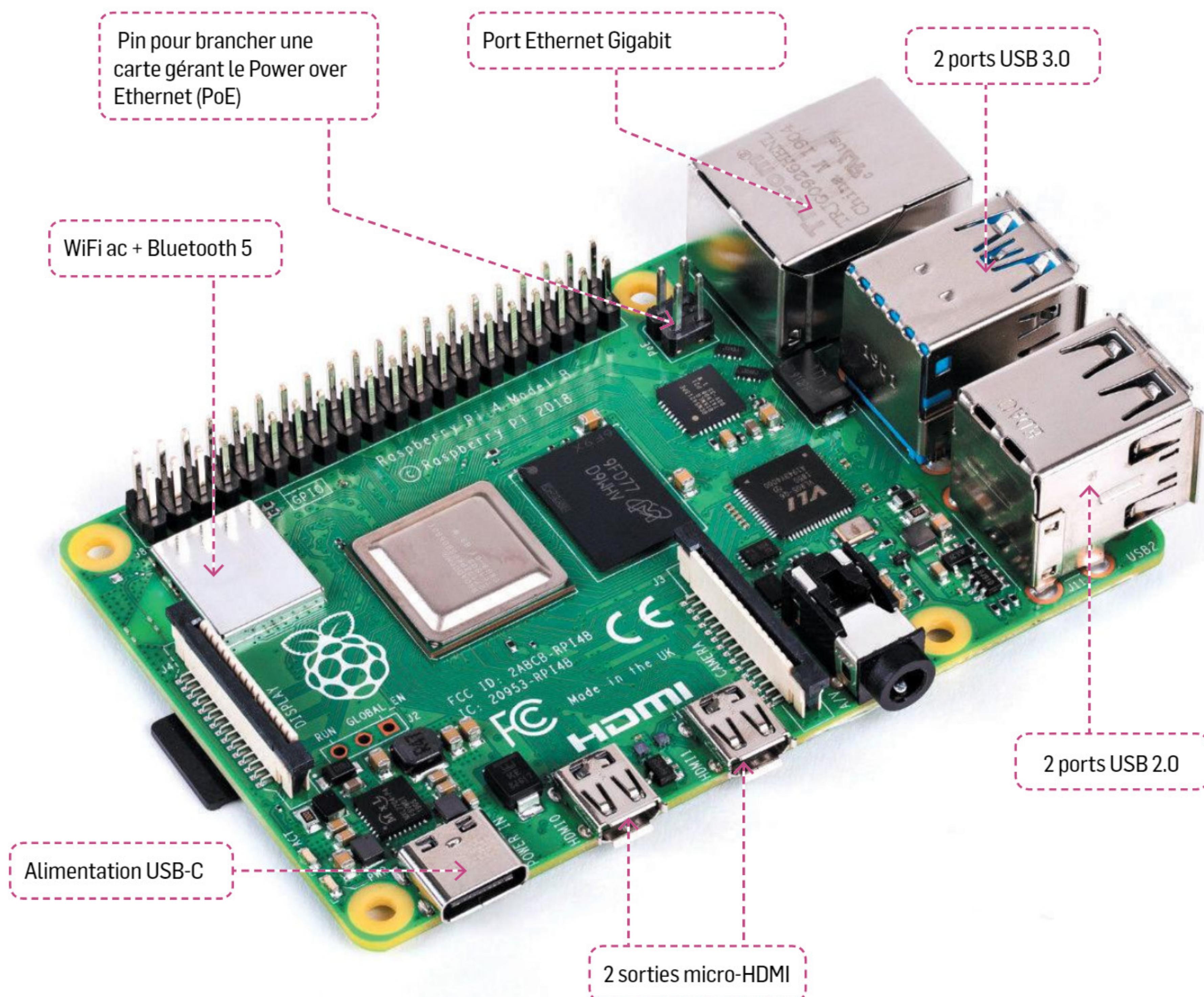
Le Raspberry Pi vient de sortir et le moins qu'on puisse dire c'est que la fondation a vu grand avec ce dernier avec des évolutions révolutionnaires. Bien sûr les dernières améliorations de 3B+ comme le PoE sont de la partie, mais le processeur Cortex A72 remplace le vieillissant A53 tout en passant d'une fréquence de 1,4 à 1,5 GHz. De même la RAM passe à 4 Go de DDR4 (même si on trouve aussi des versions 1 et 2 Go) et le circuit vidéo connaît aussi une amélioration puisqu'il permet maintenant de décoder de la vidéo 4K en 60 fps. On compte aussi deux sorties HDMI, le WiFi bi-bande 2,4/5,0 GHz, une compatibilité Bluetooth 5, un port Gigabit Ethernet et 2 ports USB 3.0 (les deux autres sont au format 2.0). On se rapproche plus des performances d'un PC d'entrée de gamme que d'une carte programmable. Mais pour une fois, tout n'est pas tout rose au pays de la Framboise puisque la communauté râle un peu.

Les makers (un peu) mécontents

Premièrement, la sortie de cette quatrième version a surpris tout le monde. Lancée en secret, nombreux sont les écrivains qui ont dû corriger leur manuscrit à la va-vite et ne parlons pas de nos camarades de Garatronic qui ont dû jeter des épreuves de leur carte NadHat 2 à cause du positionnement de certains branchements. Nous avons aussi été pris au dépourvu puisque dans notre magazine l'Officiel PC – Raspberry Pi sorti fin juin, nous n'avons pas eu le temps d'écrire un article dessus. Enfin, l'alimentation USB-C qui équipe maintenant la Framboise 4 est problématique. Elle ne respecte apparemment pas le standard de l'industrie et il faudra absolument acquérir une alimentation officielle pour être sûr de voir la carte démarrer. Ces petits soucis vont-ils obscurcir l'avenir du Raspberry Pi 4 ? Apparemment pas, car la version avec 4Go de RAM est en rupture de stock un peu partout au moment où nous écrivons ces lignes...

Prix : entre 38 € et 59 €

Lien : <https://frama.link/T3gNmej5>





CLASSEMENT



SÉLECTION

TOP 15 SÉLECTION DE LOGICIELS

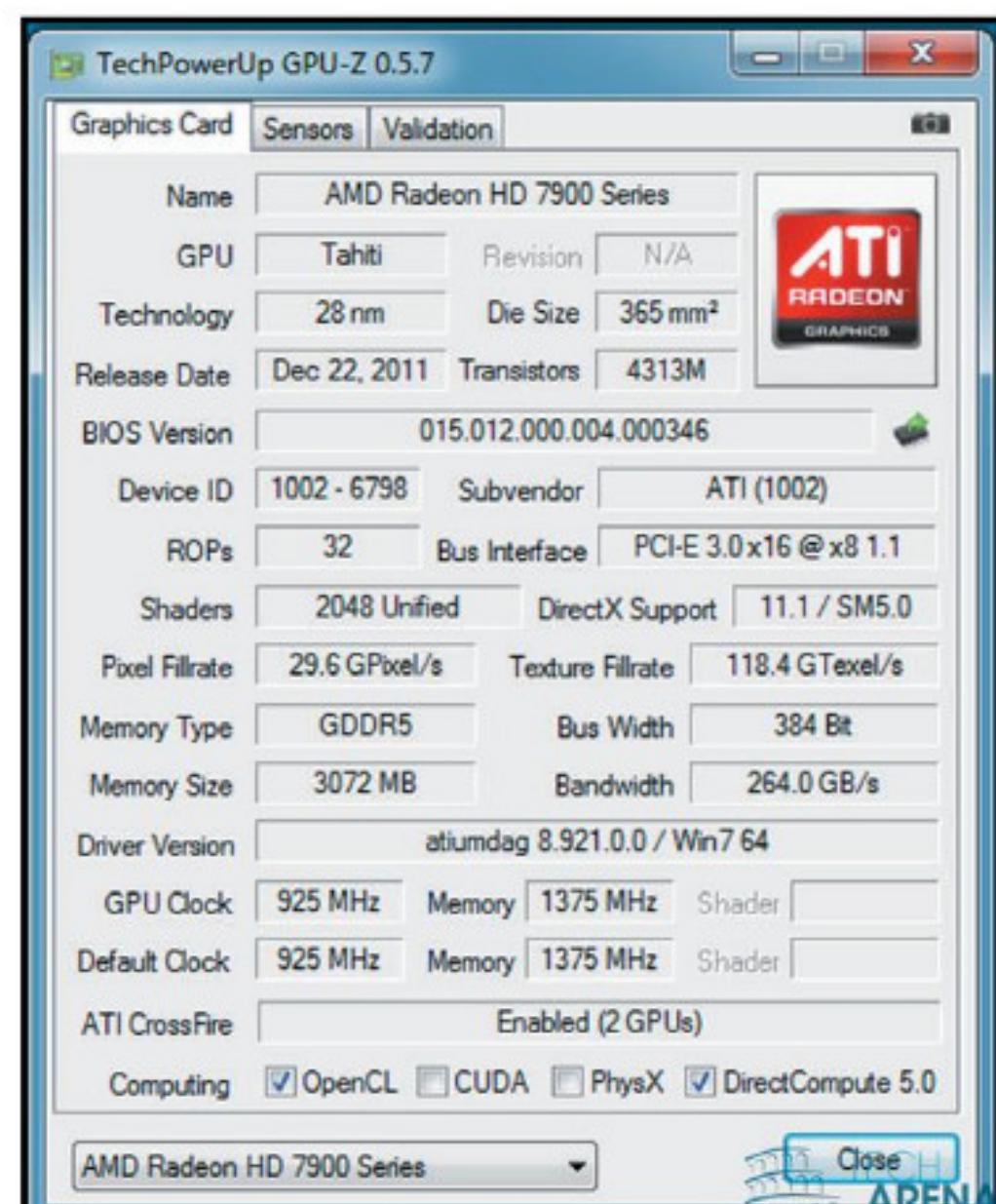
Vous vous demandez quel logiciel choisir pour tel ou tel usage ? En cherchant sur le Net, vous vous retrouvez avec des produits incomplets ou payants ? Dans chaque numéro, retrouvez ici notre Top 5 dans 3 catégories. La crème de la crème !

» TOP5 OVERCLOCKING

CPU-Z

CPU-Z permet de connaître en temps réel la fréquence du CPU et du bus, la tension d'alimentation, la fréquence, les timings et les possibilités de la mémoire (via le SPD), etc. Disponible gratuitement sous Windows, il existe même une version pour les SoC des appareils Android.

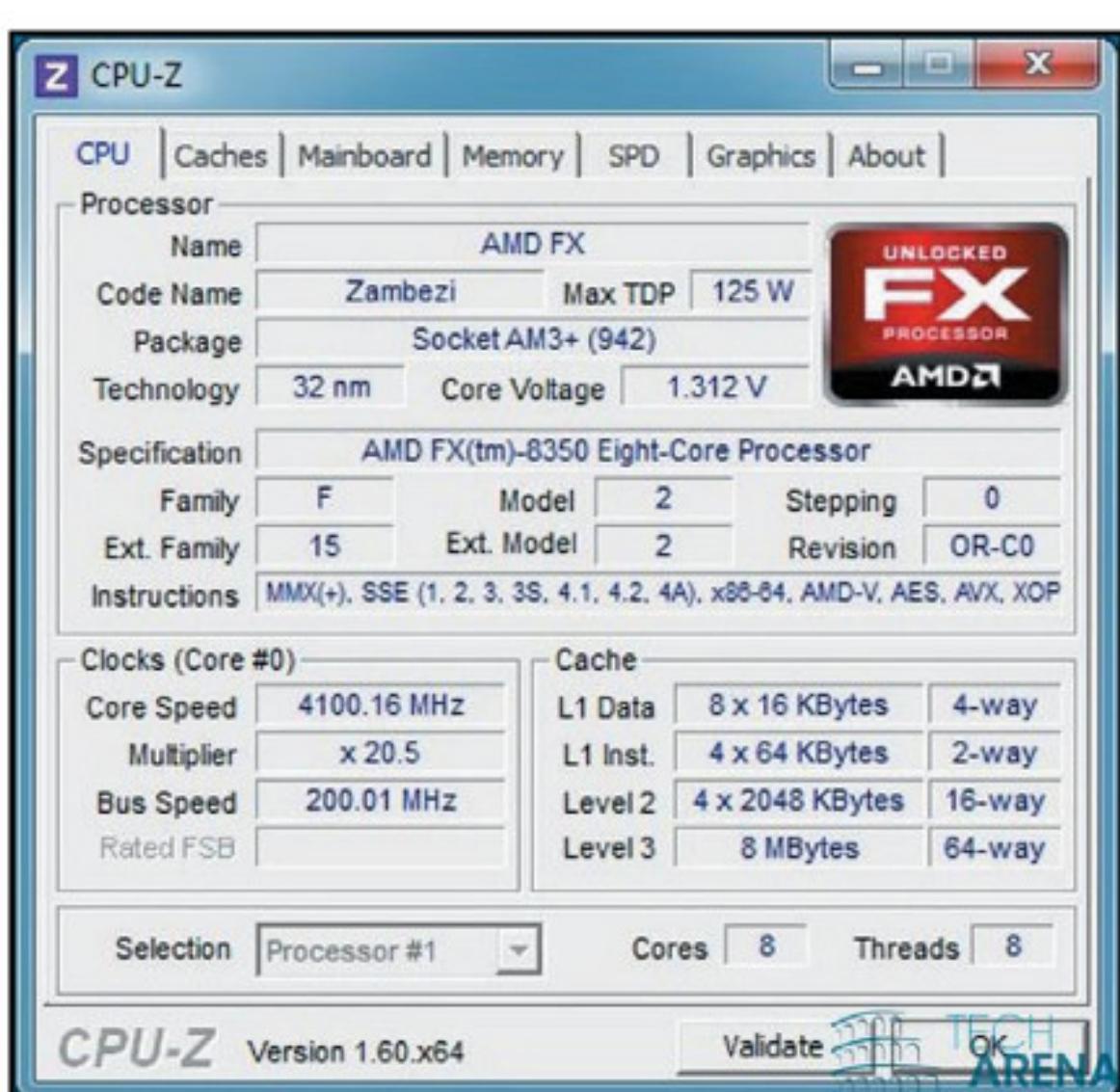
Lien : www.cpuid.com



GPU-Z

GPU-Z est dédié aux cartes graphiques et permet d'afficher des informations aussi variées que le nom exact de la carte et le type de GPU utilisé, la fréquence de la mémoire et des shaders, mais aussi le nombre de ROP, la largeur du bus mémoire, etc.

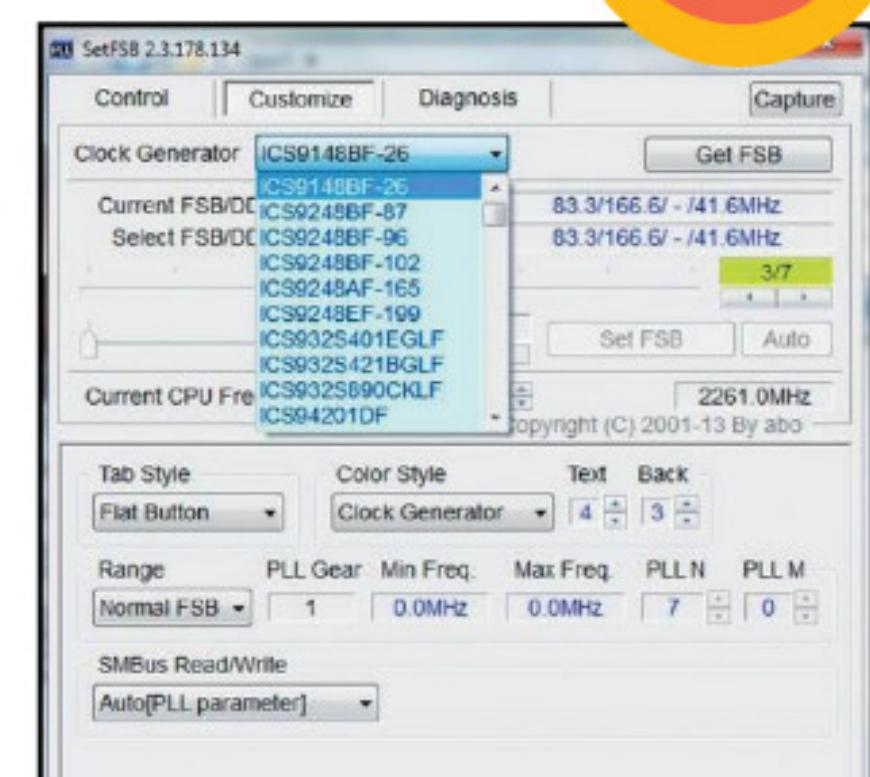
Lien : www.techpowerup.com/gpuz



SETFSB

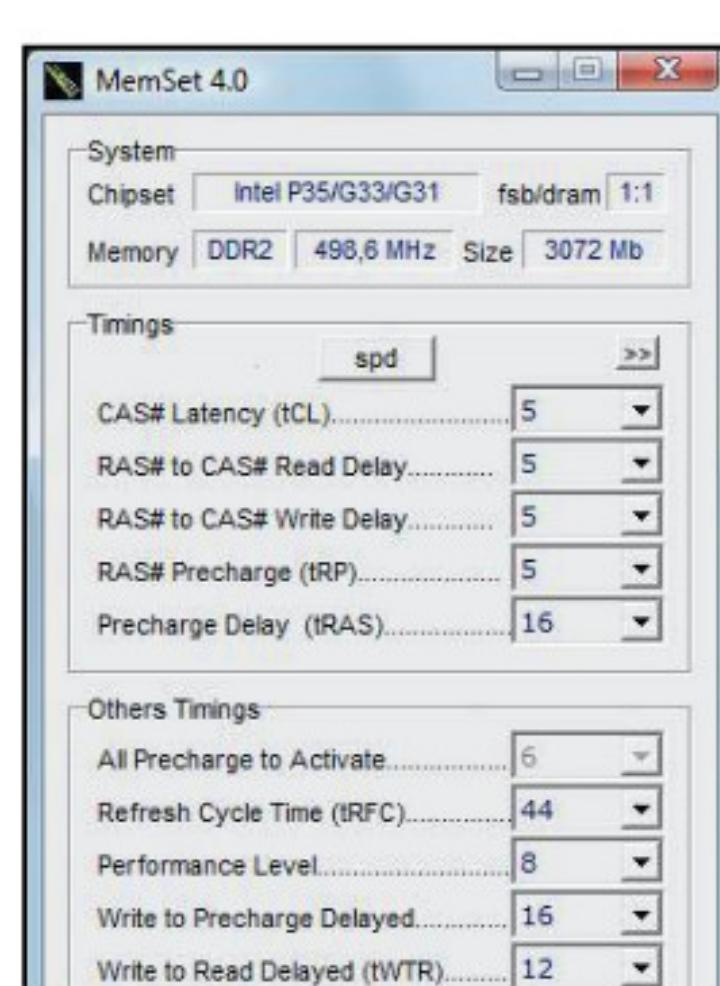
SetFSB permet de régler la fréquence du bus directement depuis Windows. Il est compatible avec énormément de cartes mères et nécessite simplement de connaître le PPL embarqué sur votre carte mère (Qwant est votre ami!).

Lien : <https://frama.link/NotL3xCe>



MEMSET

Memset permet de régler finement les timings de la mémoire sans passer par les réglages du BIOS. Intéressant, car il fonctionne avec toutes les versions de Windows et évite de devoir redémarrer à chaque fois. Attention, à utiliser prudemment !



Lien : www.tweakers.fr/memset.html



RIVATUNER

RivaTuner fonctionne aussi bien sur les cartes graphiques NVIDIA que celle d'AMD. Il permet d'overclocker sans réelle limite de fréquence et de modifier indépendamment la fréquence des shaders et celle du GPU.

Lien : www.guru3d.com/content-page/rivatuner.html

» TOP5 PROXY ET GÉOLOCALISATION

PROXYSITE

Ne laissez pas votre patron ou votre gouvernement vous empêcher d'accéder à vos sites préférés. Lorsque vous vous connectez à un site web grâce à notre proxy web, vous n'êtes pas réellement connecté au site que vous consultez. ProxySite.com va se connecter au site et vous le retransmettre. Peu importe si le site de destination est sécurisé (SSL) ou non.



Lien : www.proxysite.com/fr

STEALTHY

Stealthy est une extension pour Google Chrome et Firefox qui va

Metadata	Country	Connection Speed	Speed	Anonymity	Protocol	Port	IP Address
22a	ID	High	High	Low	https	8080	118.97.113.162
34b	TZ	Medium	Medium	Medium	https	8080	41.29.27.00
42a	IR	Low	Low	Low	http	8080	106.198.78.290
43b	AR	Medium	Medium	Low	http	8080	201.221.02.137
49a	IR	Medium	Medium	Low	https	3128	200.51.51.80.542
52b	CN	Low	Low	Low	http	8080	122.225.22.22
57a	ID	Low	Low	Low	http	3128	14.93.65.20
205	ID	Low	Low	Low	https	3128	118.07.139.06
3m7a	US	High	High	Medium	http	116.64.24.00.542	
3m8a	IN	Low	Low	Low	https	3128	183.82.07.186
3m12a	BR	Low	Low	Low	https	3128	201.64.254.228
3m34a	US	High	High	Low	http	80	50.37.170.105
3m39a	ID	Low	Low	Low	http	8081	202.137.7.349
3m36a	CN	Low	Low	Low	https	80	122.72.0.6
3m37a	CO	Low	Low	Low	https	8080	193.0.43.98

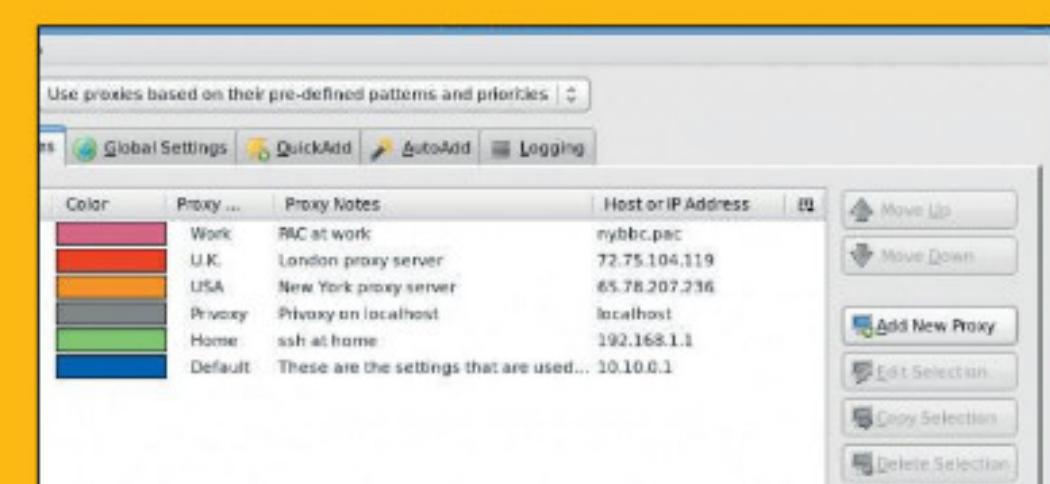
vous permettre de masquer votre IP lorsque vous êtes sur Internet. Plus précisément, vous «empruntez» une IP autre que la vôtre : celle de votre proxy.

Lien : <https://frama.link/d2u0W6WL>

FOXYPROXY

Se connecter facilement à des centaines de proxy de par le monde depuis n'importe quelle version de Firefox. Elle offre davantage de fonctionnalités que SwitchProxy, ProxyButton, QuickProxy, ProxyTex, TorButton, etc

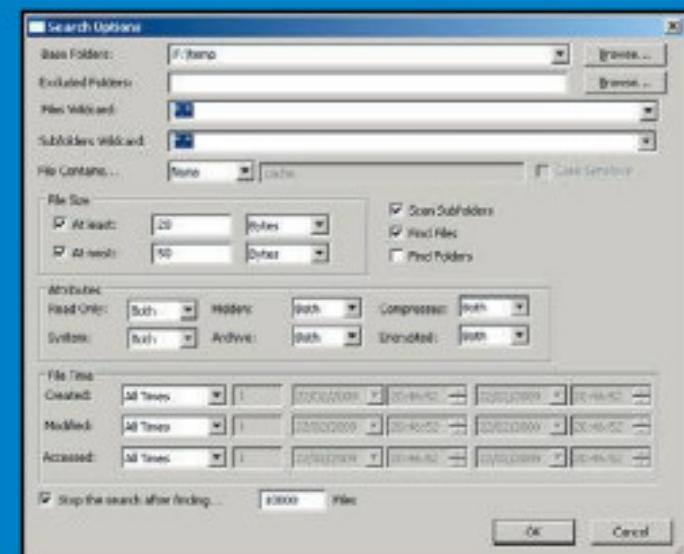
Lien : <https://frama.link/c4CVEeLK>



Les meilleurs logiciels/services

» TOP5 ORGANISER SES FICHIERS

SEARCHMYFILE

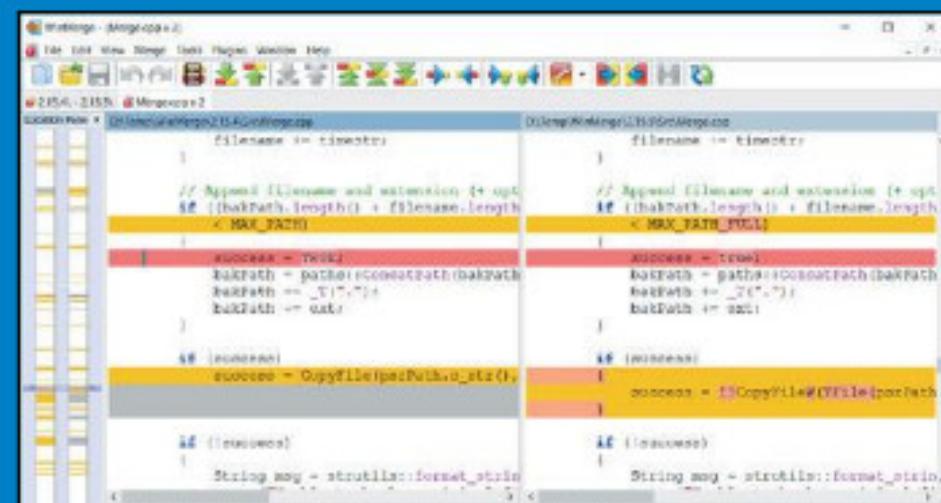


Un très bon logiciel pour retrouver vos fichiers très facilement. Beaucoup plus efficace que le module de Windows... NirSoft est un site très austère où vous trouverez plus de 180 logiciels programmés en C++. L'avantage de ce langage ? Des programmes très légers et peu gourmands en mémoire. Si

vous désirez une version 32 bits de ces logiciels, il faudra aller les chercher sur le site.

Lien : www.nirsoft.net

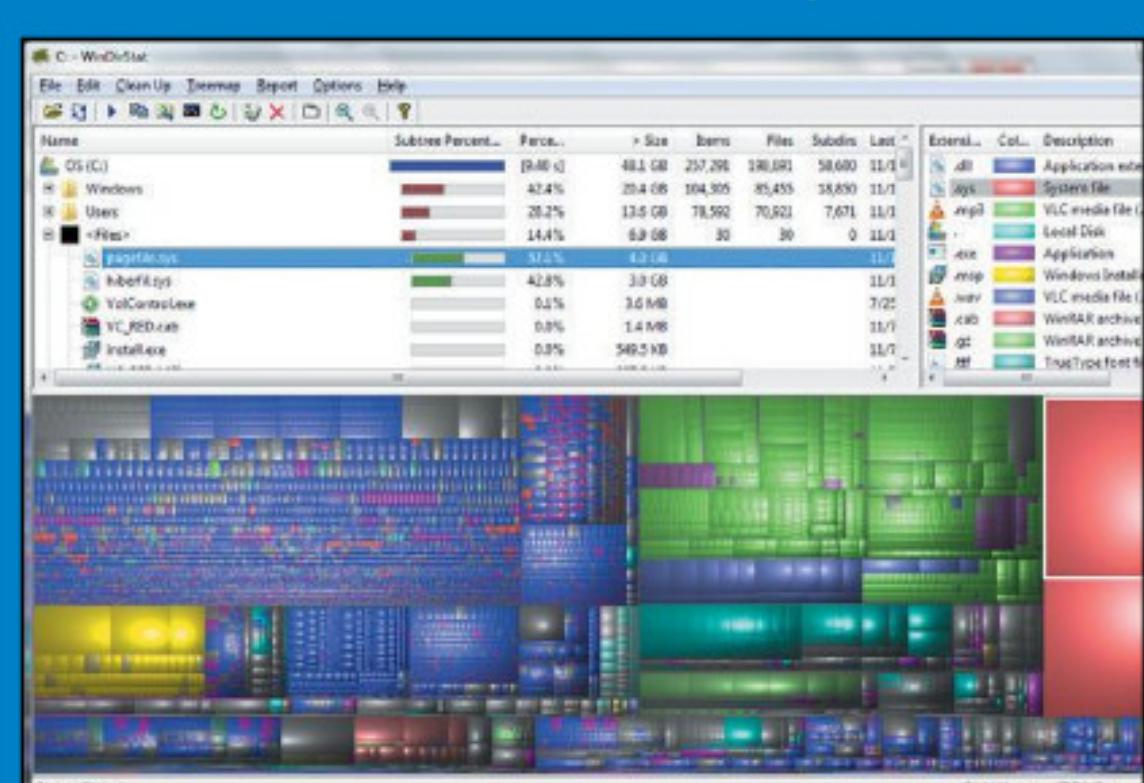
WINMERGE



WinMerge est un outil Open Source de différenciation et de fusion pour Windows. WinMerge peut comparer et les dossiers et les fichiers, en représentant les différences dans un fichier texte visuel qui est facile à comprendre ou manipuler. Pour Linux, cherchez KDirStat

Lien : <http://winmerge.org>

WINDIRSTAT



Ce logiciel permet de réaliser graphiquement un plan de l'organisation et de l'occupation de vos disques durs. Plus un fichier est gros et plus il prend de place sur l'interface. Si vous êtes un peu bordélique (comme le rédacteur

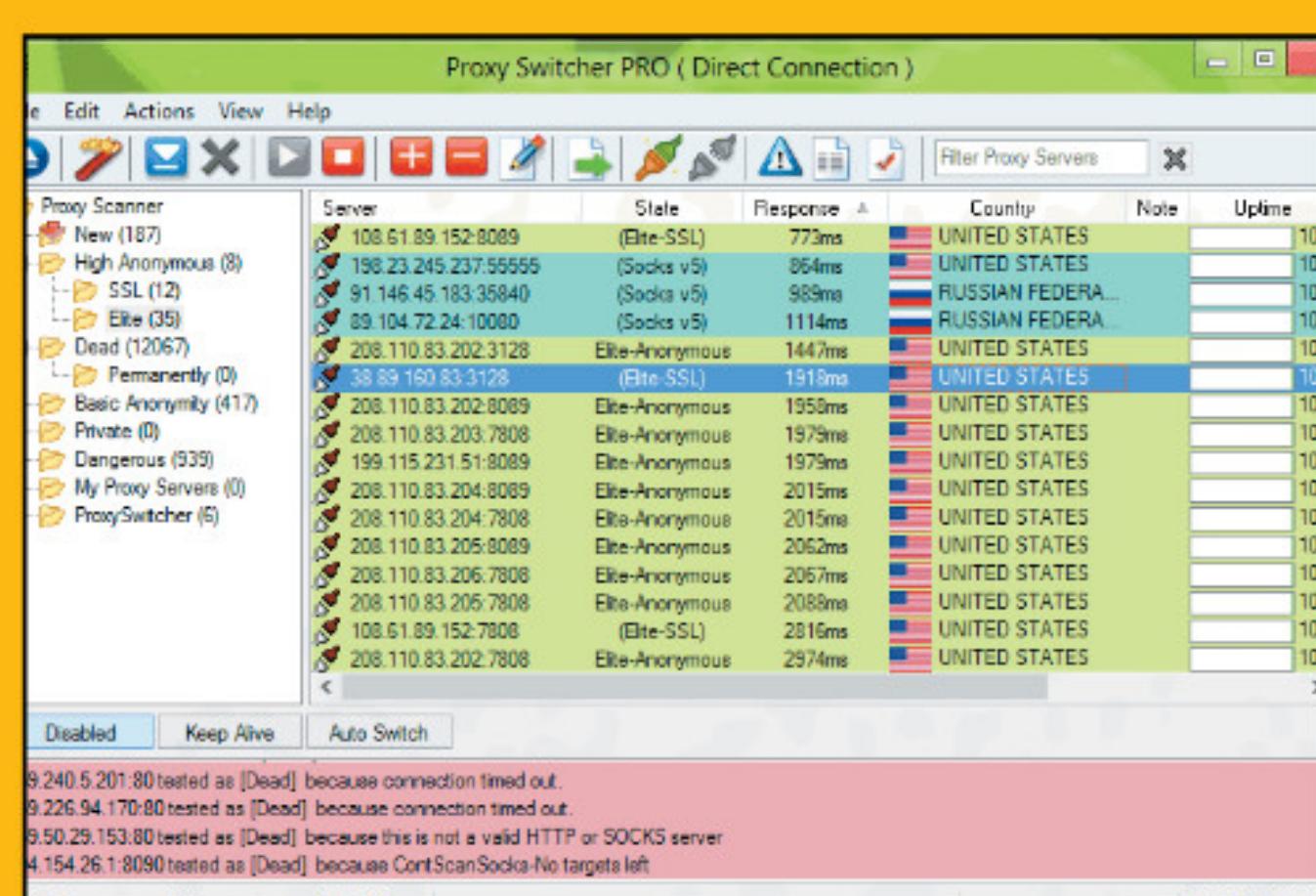
en chef), vous pourrez retrouver ces fameux fichiers de plusieurs Gigaoctets qui sont perdus ça et là ou faire le ménage dans vos fichiers temporaires... Pour Linux, cherchez KDirStat.

Lien : <https://windirstat.net>

PROXY SWITCHER

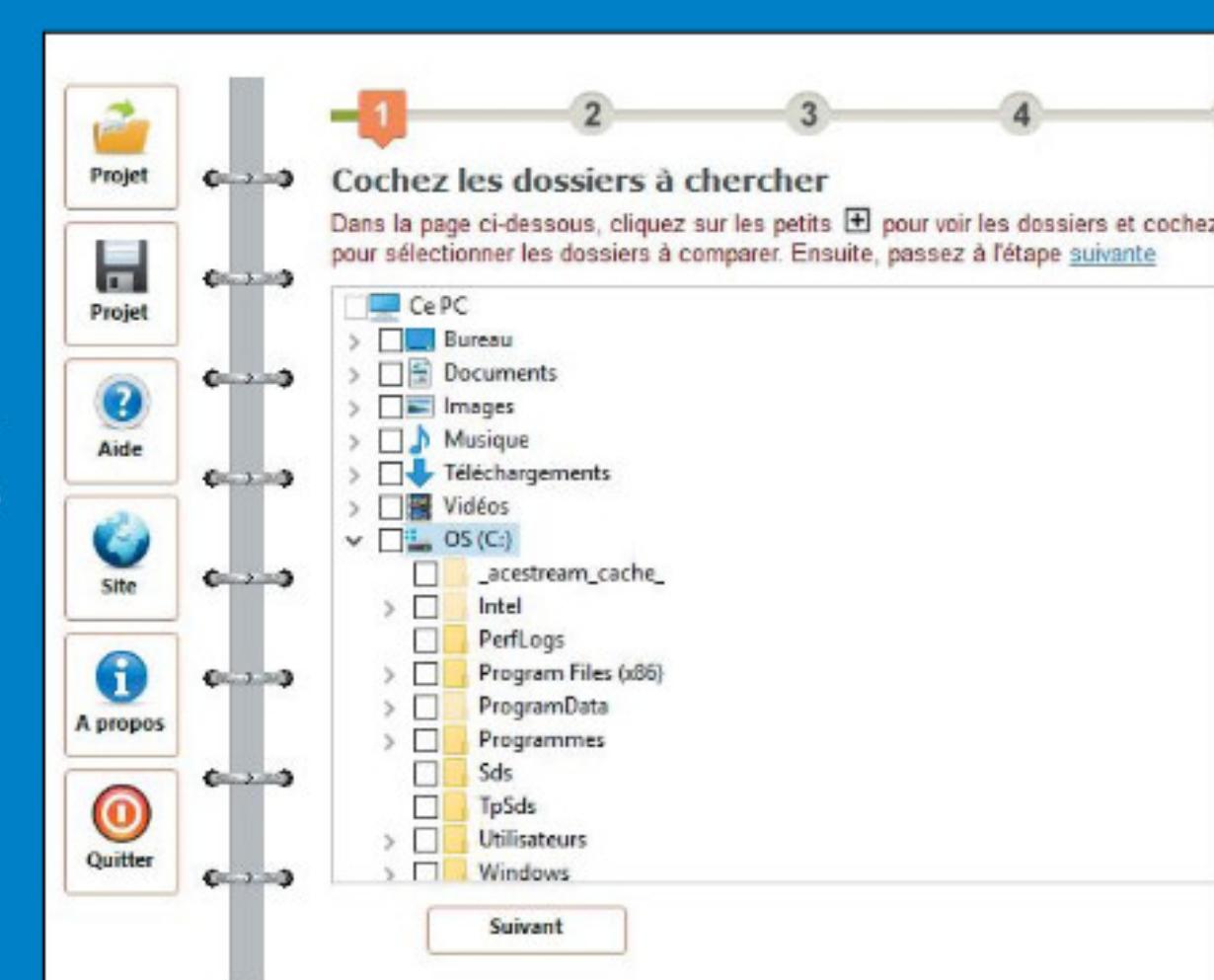


Proxy Switcher permet de rechercher des proxy disponibles directement depuis l'interface et de tester leur rapidité. Il est même possible de paramétriser un changement automatique de proxy en cas de saturation.



Lien : www.proxyswitcher.com

SUPPRIMER LES DOUBLONS



Supprimer les doublons vous guide pas à pas dans la recherche de fichiers en double sur votre disque dur. Le logiciel n'est pas gratuit, mais cette version d'essai vous permettra de profiter de toutes les fonctions en attendant de savoir si vous voulez mettre la main à la poche.

Lien : www.marseillesoft.com/telecharger

MEDIAMONKEY

MediaMonkey est un programme qui vous servira à la fois de lecteur multimédia, mais surtout à organiser votre médiathèque. Après son installation, il va se charger d'analyser votre disque dur à la recherche de tous les fichiers musicaux disponibles. Le logiciel se connecte de lui-même à une base de données en ligne pour récupérer toutes sortes d'informations concernant les albums comme leurs jaquettes, etc.

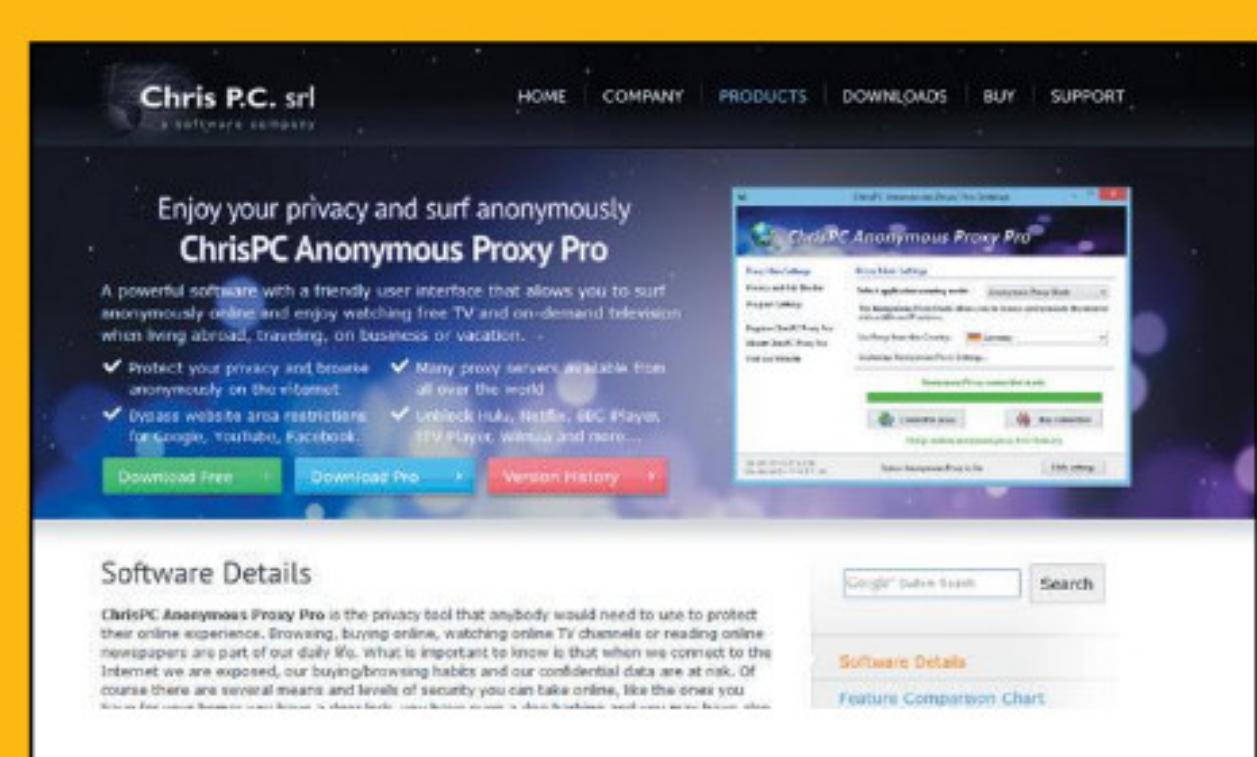
Lien : www.mediamonkey.com



CHRISPC FREE ANONYMOUS PROXY



ChrisPC propose la solution Free Anonymous Proxy. Plus simple à mettre en place que TOR, ce dernier permet de se connecter à un proxy dans le pays de votre choix pour faire croire à tout le réseau que vous surfez de ce pays.



Lien : www.chris-pc.com/proxy



CLASSEMENT



WORLD HACK WEB

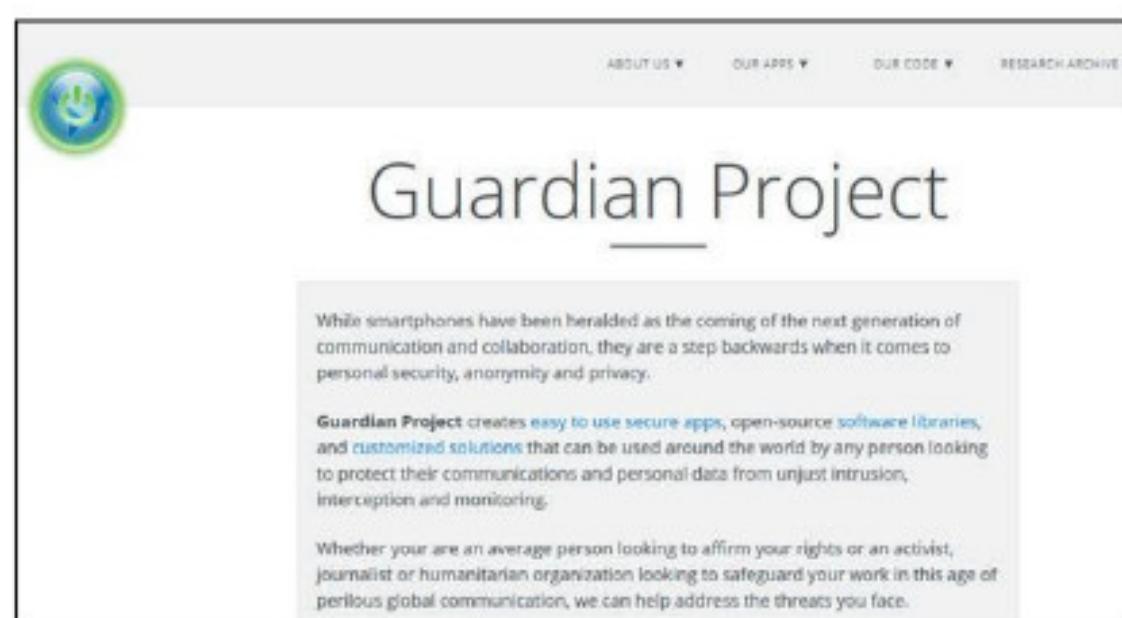
Lors de nos recherches ou au détour d'une discussion, nous faisons connaissance avec des sites ou des services intéressants. Au lieu de les garder pour nous, nous les partageons dorénavant sur cette page... N'hésitez pas à nous envoyer vos sites de prédilection à cette adresse : benbailleul@idpresse.com

GUARDIAN PROJECT

>APPLICATIONS ANDROID

Lancée par la Freedom of the Press Foundation et le Guardian Project, Haven rejoint la liste des applications permettant de protéger sa vie privée comme Obscuracam, Orbot ou ChatSecure.

Lien : <https://guardianproject.info>



ROLLAPP

>LOGICIEL DANS LE CLOUD

Ce site connaît plus de 500 types d'extension de fichier et permet de les ouvrir en un clic. Pour cela, il pioche dans une sélection d'application en ligne. Il est même possible d'éditer certains documents. La version payante à 5€/mois permet de traiter ses fichiers depuis son cloud et de travailler avec plusieurs types de fichiers différents.

Lien : www.rollapp.com

The screenshot shows the RollApp homepage. At the top, there's a navigation bar with links for Apps, Products, Pricing, About, and Support. Below the header, a large green banner features the text "Apps cloud: all-in-one service to get things done". It highlights that over 290 apps are available on nearly any device. A "Try now!" button is overlaid on a circular icon. To the right, a list of integrated services includes Google Drive, Dropbox, OneDrive, Box, and WebDAV. At the bottom, there are two sections: "Always up-to-date and secure" and "Especially great for Chromebooks".

COINBASE

>ACHAT ET VENTE DE CRYPTOS

Coinbase constitue la plate-forme la plus populaire au monde pour acheter et vendre des Bitcoins, des Ethereum et des Litecoins. Il faudra bien sûr montrer patte blanche et disposer d'un «wallet».

Lien : www.coinbase.com

The screenshot shows the OpenNIC Project website. The header includes links for Wiki, Projects, Contact, Servers, Announcements, and Members. The main content area has a large blue background with the text "OpenNIC" and "DNS LIBRES". It explains the purpose of OpenNIC to avoid censorship and lists several server addresses at the bottom. There are also "FIND OUT MORE" and "DISCOVER SITES" buttons.

ALLDEBRID >DU DDL SANS LIMITES

Ce service permet de débrider les services d'hébergement spécialisés dans le téléchargement direct. L'offre gratuite permet uniquement de télécharger pendant les «happy hours»...



Lien : alldebrid.fr

The screenshot shows the Coinbase homepage. It features a navigation bar with links for Products, Prices, Company, Sign In, and Get Started. The main content area includes sections for "Manage your portfolio", "Recurring buys", and "Vault protection". On the right, there are several charts showing price trends for different cryptocurrencies like Bitcoin, Ethereum, and Litecoin. A "Get Started" button is located in the top right corner.

LE MAILING-LIST OFFICIELLE de

Pirate Informatique et des Dossiers du Pirate

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.

**INSCRIVEZ-VOUS
GRATUITEMENT !**



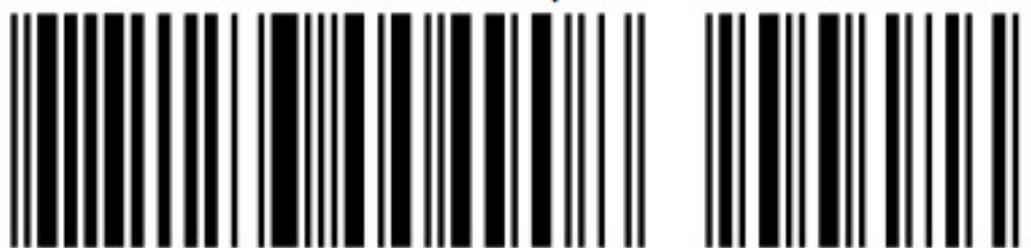
PENTESTING
MENACES **ESPIONNAGE**
SMARTPHONE **RÉSEAUX SOCIAUX**
MOTS DE PASSE
ANTI-SURVEILLANCE **WI-FI**
RANSOMWARE
RÉSEAUX ALTERNATIFS
ANONYMAT **CRACKS**
VPN **MATÉRIELS**



PIRATE
INFORMATIQUE



L 12730 - 42 - F: 4,90 € - RD



BEL/LUX : 6 € - DOM : 6,10 € - CH : 8,50 ChF - PORT.CONTR. : 6 € - CAN : 7,99 \$ cad
- POL/S : 750 CFP - NCAL/S : 950 CFP - MAR : 50 mad - TUN : 9,8 tnd