



Fouillons les poubelles !

Garbage collector
Antoine Cervoise

HackSecuReims / 2023-03-24

Qui suis-je ?



- **Antoine Cervoise - @acervoise**
- ***Penetration tester @Synacktiv***
 - Offensive security
 - 130 ninjas : pentest, reverse engineering, développement, réponse à incidents
 - Basé à Paris, Rennes, Lyon, Toulouse et on recrute !

Plan



- **Introduction**
 - Un peu d'histoire
 - Légalité
- **Pourquoi ?**
- **Où faire les poubelles ?**
- **Un peu plus que les poubelles**
- **Prestation : faire les poubelles**



Introduction

Un peu d'histoire



- **Juillet 2000 : Oracle [...] a reconnu cette semaine avoir engagé des détectives pour fouiller les poubelles d'organisations proches de la firme de Bill Gates.**
 - <https://www.letemps.ch/economie/oracle-convaincu-despionnage-microsoft-voit-senvoler-pdg>
- **En 2008, une plongée dans les poubelles des ménages d'Île-de-France montrait que 80 % recelaient au moins un document personnel**
 - <https://www.ouest-france.fr/le-broyeur-arme-anti-espionnage-de-nos-poubelles-547279>
- **Rafale 7.02 (février 2008) - Millionnaire en fouillant les poubelles - Triskel**
 - <http://rafale.org/zineonline/archives/Rafale7.tar>

Un peu d'histoire



- **Septembre 2010 : Problème de voisinage**
 - <http://virtualabs.fr/Probleme-de-voisinage>
- **Décembre 2017 : Il cherche sa clé Bitcoin à 88 millions de dollars dans une décharge publique**
 - <https://www.presse-citron.net/cherche-cle-bitcoin-a-88-millions-de-dollars-decharg-e-publique/>
- **Décembre 2017 : Par millions, nos smartphones échappent encore au recyclage**
 - <https://l'imprevu.fr/affaire-a-suivre/par-millions-nos-smartphones-echappent-encore-au-recyclage/>
- **2022 : Morgan Stanley Smith Barney to Pay \$35 Million for Extensive Failures to Safeguard Personal Information of Millions of Customers**
 - <https://www.sec.gov/news/press-release/2022-168>

Un peu d'histoire



Internet of trash – SSTIC (Rump) – juin 2017 – Jean-Michel

https://static.sstic.org/rumps2017/SSTIC_2017-06-08_P11_RUMPS_04.mp4



CommitStrip.com

<https://twitter.com/CommitStrip/status/1092471850817466368>



Légalité



Res derelictae

Légalité



(II)légalité



■ Détecteurs de métaux

■ Pêche à l'aimant

- Nécessite une autorisation
 - <https://www.culture.gouv.fr/Regions/DRAC-Grand-Est/services/patrimoines-architecture/patrimoines/Archeologie/L-usage-des-detecteurs-de-metaux-soumis-a-autorisation-prefectorale>
 - <https://www.vendee.gouv.fr/peche-a-l-aimant-r986.html>
- Les découvertes de valeurs doivent être déclarées
 - https://www.detecterenfrance.com/trouve-de-lor-avec-votre-detecteur-de-metaux-voici-comment-en-etre-sur/#Regles_et_obligations legales_en_France_pour_les_trouvailles_en_or

Pourquoi faire les poubelles



■ Perso

- Victime de vol
- Apprendre
 - à réparer / bidouiller
 - forensic software
 - forensic hardware

■ Récupérer des objets “utiles”



Pourquoi faire les poubelles ?



■ Professionnel

- Enquête de police, détective privé
- Espionnage (industrielle, étatique)
- Journaliste
- Audit de sécurité

Exemple de bidouilles



Source : Hackable n°26 septembre-octobre 2018



Source : Hackable n°15 novembre-décembre 2016



Source : Hackable n°21 novembre-décembre 2017



Source : Hackable n°28 janvier-mars 2019



Source : Hackable n°5 mars-avril 2015

Exemple de bidouilles



Exemple de récup'



Fascinating
@fasc1nate

...

Turkish garbage collectors open a library with all of the books citizens discard in their trash



4:46 PM · Oct 6, 2022 · SocialOomph

Exemple de récup'



- I Searched 100 Dumpsters, Here's What I Found – MrBeast
 - <https://www.youtube.com/watch?v=anFxs5jXrE>



Matériel et précautions

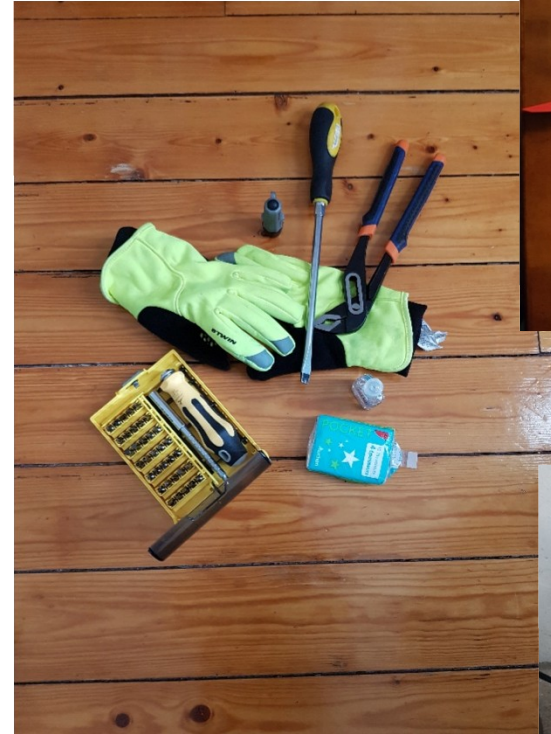


■ Kit

- Gants
- Tournevis
- Pince
- Lampe torche
- Gel hydro alcoolique

■ Précautions : noter où l'équipement a été découvert

- Faire une photo



Que trouve-t-on ?



- **Données personnelles**
- **Mots de passe**
- **Informations sensibles**
 - Pro
 - Perso
- ...



Où faire les poubelles ?



Où faire les poubelles ?



- **Présentation des différentes possibilités**
 - au travers d'exemples
 - illustrée de mesures préventives

Où faire les poubelles ?



- Dans les poubelles ...



Où faire les poubelles ?



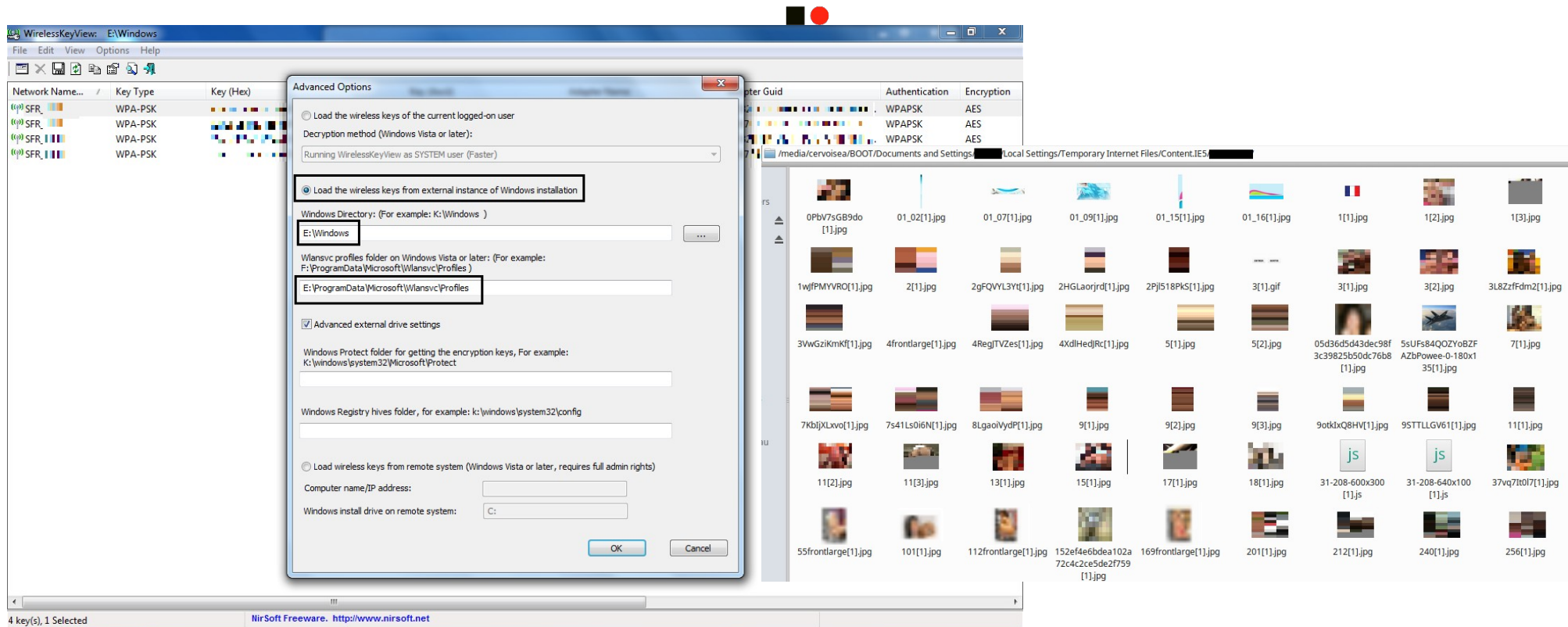
■ Dans les poubelles ...



Poubelles “classiques”



Poubelles classiques



Où faire les poubelles ?



- Dans les poubelles ...



Poubelles “papiers”



VOTRE E-BILLET



PARIS NORD / DOUAI

55.00 EUR
EC

Nom : CERVOISE
Prénom : ANTOINE
Voyageur : ADULTE

DOSSIER VOYAGE

Référence client :

N° e-billet :



Vous voyagez avec un tarif TGV Pro ou Fréquence : retrouvez vos avantages Pro Flexi, Pro Express et Pro Mobile sur [sncf.com](https://www.sncf.com)

N°

Départ / Arrivée	Date / Heure	TGV	TGV PRO-ECH/REMB INCLUS. CONDITIONS APRES DEPART
PARIS NORD	28/09 à 07h52	TRAIN N°7105 VOITURE 17 - PLACE 36 2e CLASSE / PLACE ASSISE FENETRE DUO	E-Billet valable uniquement sur ce train
DOUAI	28/09 à 08h58		

Présence à quai obligatoire 2 mn avant départ.

Poubelles “papiers”

Numéro de référence interne	
N° colis	
Poids du colis	0.1 Kg
Expédié le	23/07/2018
Livré le	26/07/2018

Statuts		Preuve de livraison	
Date	Heure	Statuts	Lieu
26/07/2018	11:23	Le colis est livré au destinataire	Agence DPD de Vemars (95)
26/07/2018	08:54	Predict vous informe : le destinataire est prévenu de la mise en tournée de livraison de son colis	
26/07/2018	08:14	Votre colis est en cours de livraison	Agence DPD de Vemars (95)
26/07/2018	06:59	Votre colis est en cours d'acheminement	Agence DPD de Vemars (95)
24/07/2018	09:49	Un rendez-vous a été pris pour la livraison du colis	Agence DPD de Vemars (95)
24/07/2018	07:27	Votre colis est en cours d'acheminement	Agence DPD de Vemars (95)
23/07/2018	23:06	Instruction destinataire Le destinataire a fait le choix de se faire livrer à son adresse	
23/07/2018	19:46	Predict vous informe : propositions de dates et créneaux de livraison envoyées au destinataire	
23/07/2018	17:40	Votre colis est pris en charge par DPD	Agence DPD de Saint-Etienne (42)
23/07/2018	17:40	Votre colis est pris en charge par DPD	Agence DPD de Saint-Etienne (42)
23/07/2018	15:37	Le colis est en préparation chez l'expéditeur	Agence DPD de Saint-Etienne (42)

Poubelles “papiers”



Numéro de référence interne

N° colis

Poids du colis

Expédié le

Livré le

0.1 Kg

23/07/2018

26/07/2018

Statuts

Preuve de livraison



Voici le bordereau de livraison :

12	CERVOISE ANTOINE - , [REDACTED]	CERVOISE
.....		
SHOPIX/OSE, F-42160 ANDREZIEUX BOUTHEON (DPD 042)		
.....		
PRE Cl: ecom568985	042-313255252 7	0.10
.....		
Divers	1 Colis en bon état	0.10
042 313255252: Liv.: 26/07/18 10:45-11:45 1		

SIGNATURE

Nom, tampons, signature (26.07.2018)

Signature électronique en temps réel du destinataire :

Se protéger



■ Se protéger

■ Broyeur à papier

- La norme DIN 32757 en 5 classes : DIN 1 à DIN 5
- Deux niveaux supplémentaires existent :
 - DIN 6 : Transforme une feuille A4 en plus de 15 000 particules
 - DIN 7 : Transforme une feuille A4 en plus de 60 000 particules

■ Utilisation d'un marqueur



Où faire les poubelles ?



- **Les encombrants / monstres**
 - La collecte se fait tôt le matin
→ passer la veille



Les encombrants / monstres



- **Changement d'organisation**
 - Notamment à Paris
 - Passage "n'importe quand"
 - Nécessite de prendre un RDV
 - Par exemple à Paris sur : <https://teleservices.paris.fr/ramen/>



Les encombrants / monstres



■ Exemple de découverte



Les encombrants / monstres



■ Données personnelles

- Contrat de travail (de sa fille)
- Dossier d'inscription en école de commerce (de sa fille)
- Avis d'imposition
- Attestation de mutuelle
- Dossier hébergement (inconnu) : Fiche de paie, pièce d'identité, justificatif de domicile, relevé d'imposition
- Dossier hébergement (de sa fille) : même documents que précédemment pour elle, sa fille et son ex-mari (et la CNI de son fils...)
- Photos: famille, vacances, voyages pro
- Nom/Prénom étudiants + login/mdp
- Log FTP

Les encombrants / monstres



■ Mots de passe

```
root@kali:/media/root/OS/Windows/System32/config# samdump2 system sam
*disabled* Administrateur:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
*disabled* Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
V[REDACTED]:1000:aad3b435b51404eeaad3b435b51404ee:0[REDACTED]:9:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:a[REDACTED]:d:::
```

```
root@kali:/media/root/OS/Windows/System32/config# john --format=NT /root/hash.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Rules/masks using ISO-8859-1
Loaded 1 password hash (NT [MD4 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:04:30 3/3 0g/s 33195Kp/s 33195Kc/s 33195KC/s atm20271..atm202aa
Session aborted
```


Les encombrants / monstres



■ Mots de passe

```
root@kali:~/firefox_decrypt# python firefox_decrypt.py ../go58ucmn.default/
```

```
2018-03-14 09:35:56,898 - WARNING - profile.ini not found in  
../go58ucmn.default/
```

```
2018-03-14 09:35:56,898 - WARNING - Continuing and assuming  
'../go58ucmn.default/' is a profile location
```

```
Master Password for profile ../go58ucmn.default/:
```

```
2018-03-14 09:35:58,259 - WARNING - Attempting decryption with no Master  
Password
```

Les encombrants / monstres



■ Mots de passe

`http://twitter.com`

`http://www.oscaro.com`

`http://videos.domyos.fr`

`https://www.airbnb.fr`

`https://paye.employeur.tld`

`https://www.mon-
compte.bouyguestelecom.fr`

`https://www.okcupid.com`

`https://www.groupon.fr`

`https://www.easyjet.com`

`http://www.voyages-sncf.com`

`https://extranet.employeur.tld`

`http://www.bravofly.fr`

`https://www.amazon.fr`

`https://www.laredoute.fr`

`http://webmail.employeur.tld`

`https://accounts.google.com`

`https://www.eurowings.com`

`http://ilovia.com`

`https://www.maif.fr`

Les encombrants / monstres



■ Mots de passe

```
root@kali:/media/root/OS/Windows/System32/config# samdump2 system sam
*disabled* Administrateur:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
*disabled* Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
V[REDACTED]:1000:aad3b435b51404eeaad3b435b51404ee:0:[REDACTED]:9:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:a[REDACTED]:d:::
```

```
root@kali:~# john --format=NT /root/hash.txt --wordlist=pass.txt --rules
Using default input encoding: UTF-8
Rules/masks using ISO-8859-1
Loaded 1 password hash (NT [MD4 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
[REDACTED] (?)
1g 0:00:00:00 DONE (2018-03-14 09:37) 100.0g/s 1200p/s 1200c/s 1200C/s [REDACTED]
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~#
```

Les encombrants / monstres



■ Exemple de la valeur (au rachat) :

- <https://www.hackread.com/wp-content/uploads/2018/03/your-entire-identity-is-for-sale-on-dark-web-2.png>

■ Scénario de fraude :

- Souscriptions de prêts à la consommation
- Livraison Amazon / La redoute

Bonjour Monsieur [REDACTED],

Bonne nouvelle ! Votre commande N°FRA [REDACTED] est disponible dans votre magasin.
Votre colis vous attendra pendant 14 jours après réception de cet email.

Rendez-vous à l'accueil muni d'une pièce d'identité et de votre numéro de commande
N°FRA [REDACTED]

Si vous le souhaitez, une tierce personne peut récupérer votre colis. Il lui faudra pour cela se munir d'une photocopie de votre pièce d'identité ainsi que de votre numéro de commande.

Votre facture est disponible dans [Mon compte](#).

Les encombrants / monstres



■ Se protéger

- Chiffrement du disque
 - Bitlocker
 - <https://www.veracrypt.fr/en/Home.html>
 - LUKS (Linux)
- Effacement du disque (logiciel)
 - Dban <https://dban.org/> / SRM
 - Explication
<https://www.comptoirsecu.fr/video/seclair-leffacement-s%C3%A9curis%C3%A9/>
- Effacement de disque (matériel) : Marteau / Perceuse
 - => Séance de sensibilisation via la réalisation d'une *fury room* où l'on « détruit » de la donnée

Où faire les poubelles ?



- Les poubelles spécialisées : Déchets d'équipements électriques et électroniques (DEEE)



Le contenu de ces poubelles n'est pas *Res derelictae*

Où faire les poubelles ?

- Dans les zones où le dépôt de déchet est explicitement interdit



DEEE



■ Exemple de découvertes



Le contenu de ces poubelles n'est pas *Res derelictae*

DEEE



■ Carte SD

- Comptabilité ancienne d'un restaurant (2005 à 2009)
- Un contrat de travail
- Photorec : un second contrat de travail

■ Disque défectueux (bruit étrange)

- Pas de données sensibles dessus
- Occasion de tester <https://lifehacker.com/5515337/save-a-failed-hard-drive-in-your-freezer-redux>

Save a Failed Hard Drive in Your Freezer, Redux



Adam Pash

4/12/10 2:35pm • Filed to: MACGYVER TIP

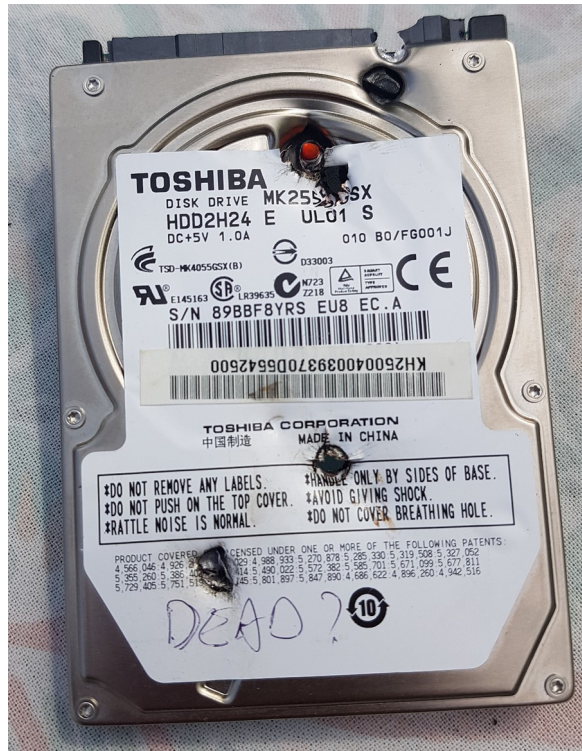
432.7K 177 4



DEEE



■ Se protéger





Plus que les poubelles



Par terre



■ Carte Micro SD

- Provenant d'un BlackBerry
- Présence de nombreuses photos (très) personnelles

Par terre



■ Clé USB

- Appartenant à une étudiante
- Mémoire de master en cours d'écriture sur la clé
 - L'étudiante n'avait pas de backup



Mathias GIREL
@MathiasGIREL

Follow

Je suis comme d'autres un peu traumatisé par l'appel de cette doctorante qui a perdu dans le train son ordinateur avec le seul exemplaire de sa thèse. Pour elle, j'espère qu'on va retrouver son ordinateur et la rappeler, mais pour mes étudiants, les doctorants et les autres:

1:11 PM - 4 Apr 2019

Source : <https://twitter.com/MathiasGIREL/status/1113896781392371712>

franceinfo:



"On ne peut qu'attendre et espérer" : un père lance un appel pour retrouver un ordinateur qui contient la thèse de sa fille

Par franceinfo – France Télévisions

Mis à jour le 05/04/2019 | 15:34 – publié le 05/04/2019 | 15:34

Source : https://mobile.francetvinfo.fr/economie/transports/on-ne-peut-qu-attendre-et-esperer-un-pere-lance-un-appel-pour-retrouver-un-ordinateur-qui-contient-la-these-de-sa-fille_3266949.amp

Par terre



Dans la rue, elle trouve par terre un ticket gagnant de l'Euromillion et empoche 12 millions d'euros

Après huit années de procédures, la justice a récemment conclu que Bercy n'était pas en droit de taxer une femme qui va récupérer 12 millions d'euros sur un ticket retrouvé dans la rue en 2011.

La rédaction • Publié le 28/07/2019 à 16:30, mis à jour le 28/07/2019 à 16:30

<https://www.nicematin.com/insolite/dans-la-rue-elle-trouve-par-terre-un-ticket-gagnant-de-leuromillion-et-empoche-12-millions-deuros-401165>

Les brokers



Explorer par catégories

Q Rechercher sur eBay

Toutes les catég...



Retourner aux résultats de recherche | Catégorie de mise en vente : Informatique, réseaux > Réseau d'entreprise, serveurs > Commutateurs, concentrateurs > Commutateurs réseau



Switch Cisco SG220-50 50 Ports

État : Occasion

Prix : 90,00 EUR

Achat immédiat

Ajouter au panier



Vous en avez un à vendre ? [Vendez le vôtre](#)

Accueil > Informatique > Ile-de-France > Paris > Paris 75009 9e Arrondissement > Dell Latitude 3490 intel core i5 Ram 8go ,



Voir les 7 photos

Dell Latitude 3490 intel core i5 Ram 8go , 256 go SSD

199 € Livraison : à partir de 4,99 €

11/04/2022 à 19:05



Les brokers



■ **Achat de switch sur Ebay (2012)**

- Présence des anciennes configurations (mots de passe, configuration réseau, etc.).
- Secteur bancaire

■ **Achat d'un PC sur leboncoin (2014)**

- PC Remis à neuf
- Photorec -> récupération de secrets industriels
- Possible car le disque n'était pas chiffré à la base

Les brokers



- **J'ai fouillé des disques durs sur leboncoin – 2021 – Micode**
 - Partie 1 : <https://www.youtube.com/watch?v=vt8PyQ2PGxI>
 - Partie 2 : <https://www.youtube.com/watch?v=aOBVZUL1iBA>
 - Partie 3 : https://www.youtube.com/watch?v=xf_cKTIOYLo
- **J'ai fouillé des disques durs sur leboncoin (encore) – 2022 – Micode**
 - <https://www.youtube.com/watch?v=FDnH4NVKHco>

Les brokers



Lot n° 96

RP



Mise à prix : 500 €

Prix obtenu : 1 800 €

Taxe de 11% en sus du prix de vente

Lieu de vente : 3 AV DU CHEMIN DE PRESLES
94410 ST MAURICE

Date de vente : 17 mai 2018 13:30:00

Conditions spécifiques d'achat :

- Lot réservé aux professionnels

DESCRIPTIF

Lot de 45 smartphones APPLE iPhone 6 modèle A1586, non testé.

Les objets sont susceptibles de contenir des données concernant la vie privée de leurs anciens propriétaires. L'acquéreur s'engage à ne pas divulguer ces éléments privés et à vider ou faire vider, sous sa responsabilité, les mémoires internes des objets avant toute utilisation, cession ou transmission de ceux-ci.

Source : https://encheres-domaine.gouv.fr/hermes/details_bien/lots-12478.html

Les brokerscantes



Les brokerscantes



■ Game Boy Camera



Les brokerscantes



■ Game Boy Camera



Couchsurfing / Airbnb



- Accès à des équipements informatiques en l'absence du propriétaire
 - Mot de passe du Wi-Fi + accès physique à la box
 - PC fixe / portables
 - Non chiffré -> USB Live
 - Accès libre (avec le compte du propriétaire ou un compte invité)

```
C:\Windows\system32\cmd.exe
C:\Users\ [redacted] >whoami
[redacted]
C:\Users\ [redacted] >net user [redacted] [redacted]
Non d'utilisateur
Non complet
Commentaire
Commentaires utilisateur
Code du pays
000 (Valeur par défaut du système)
Compte : actif
Le compte expire
Oui
Jamais
Mot de passe : dernier changmt.
Le mot de passe expire
13/05/2017 08:07:08
Le mot de passe modifiable
13/05/2017 08:07:08
Mot de passe exigé
Non
Oui
Stations autorisées
Tout
Script d'ouverture de session
Profil d'utilisateur
Répertoire de base
Dernier accès
03/02/2019 14:30:41
Heures d'accès autorisés
Tout
Appartient aux groupes locaux
*Administrateurs
*NoneUsers
Appartient aux groupes globaux
*None
La commande s'est terminée correctement.
```

Voitures de location



- **Synchronisation Bluetooth avec le téléphone**
 - Contenu complet du répertoire d'un ancien locataire



Martin Bos
@cantcomputer

Follow

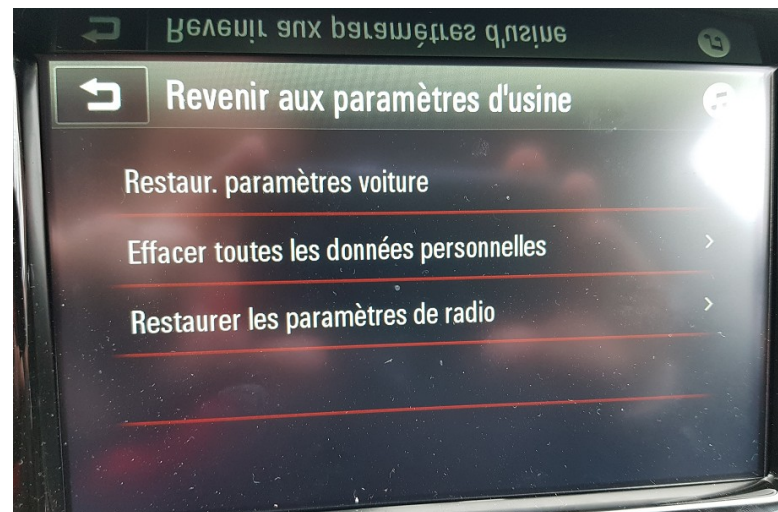
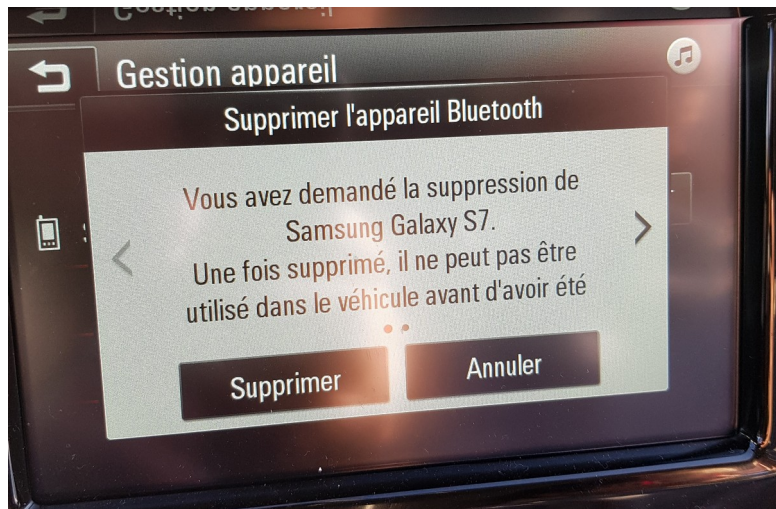


Remember to delete peoples old paired phones and contacts in rental cars. Don't be a douche. Nice deeds have a ripple effect across the universe.



Source : <https://twitter.com/cantcomputer/status/1106908333951180800>

Voitures de location





Prestation : faire les poubelles



Prestation : faire les poubelles



■ Papier



Prestation : faire les poubelles



■ Papiers

- Documents avec des données
 - Personnelles (factures, bon de livraison...)
 - Médicales (ordonnances, questionnaire de santé...)
 - Document avec des informations indirectes (billets de trains, suivi de livraison...)
- Documents de connexion
 - Login + mots de passe

Prestation : faire les poubelles



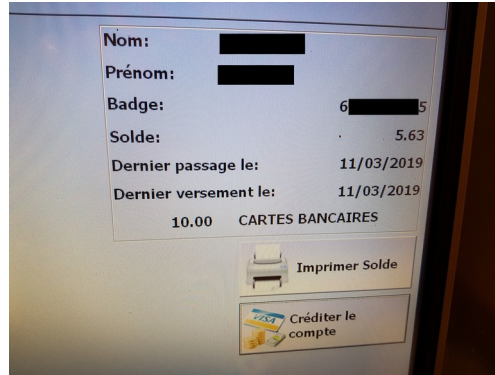
■ Les broyeurs à papier



Prestation : faire les poubelles



- **Borne de recharge de cantine**
 - Accessible avant les portiques
 - Affiche
 - Le nom du collaborateur (important pour cibler une personne avec des accès privilégiés)
 - l'ID partiel de l'utilisateur



Prestation : faire les poubelles



- **Imprime un ticket avec l'ID**
 - A chaque recharge
 - A la demande pour avoir le solde
 - Contient aussi le nom de la société



Prestation : faire les poubelles



- **Imprime un ticket avec l'ID**
 - À chaque recharge
 - À la demande pour avoir le solde
 - Contient aussi le nom de la société
- **=> Possibilité de bruteforcer l'ID**



Prestation : faire les poubelles



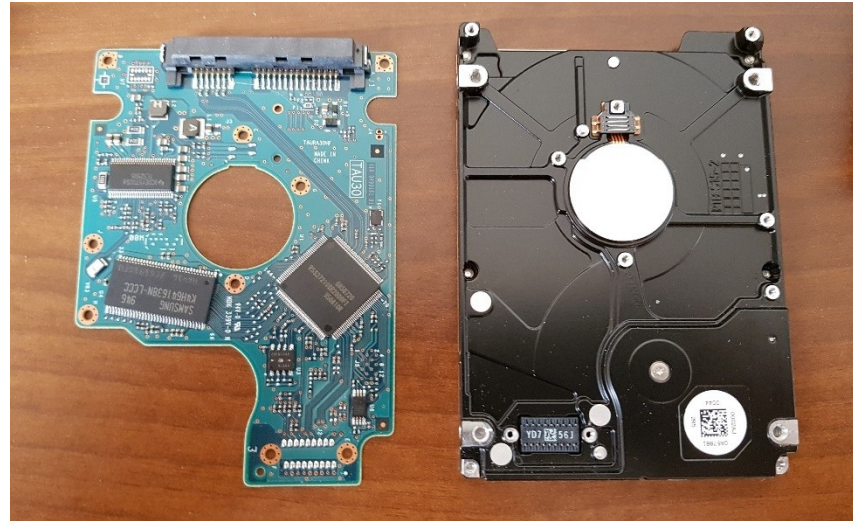
■ Proxmark

```
[usb] pm3 --> lf em 410x read
[+] EM 410x ID 38001829DF
[usb] pm3 --> lf em 410x demod
[+] EM 410x ID 38001829DF
[+] EM410x ( RF/64 )
[=] ----- Possible de-scramble patterns -----
[+] Unique TAG ID      : 1C001894FB
[=] HoneyWell IdentKey
[+]   DEZ 8            : 01583583
[+]   DEZ 10           : 0001583583
[+]   DEZ 5.5          : 00024.10719
[+]   DEZ 3.5A         : 056.10719
[+]   DEZ 3.5B         : 000.10719
[+]   DEZ 3.5C         : 024.10719
[+]   DEZ 14/IK2       : 00240519752159
[+]   DEZ 15/IK3       : 000120260695291
[+]   DEZ 20/ZK        : 01120000010809041511
[=]
[+] Other              : 10719_024_01583583
[+] Pattern Paxton     : 942434271 [0x382C67DF]
[+] Pattern 1          : 4462459 [0x44177B]
[+] Pattern Sebury     : 10719 24 1583583 [0x29DF 0x18 0x1829DF]
[=] -----
```

Prestation : faire les poubelles



- Déchets numériques : disques dur (abimé)



Prestation : faire les poubelles



- **Récupération d'un disque dur**
 - Changement de la carte : 15\$ sur Ebay
 - Récupération des données sur le disque



Pointez sur l'image pour zoomer



Carte électronique disque dur WD1600JS

État : Occasion
"Occasion"

Temps restant : 3j 17h (23 mars 2018 10:38:38 Paris)

4,99 EUR 0 enchères

Saisir votre enchère maximum

Enchérir

- ♦ Ajouter à votre liste d'Affaires à suivre
- ★ Ajouter à la collection

Lieu : France

Livraison : **2,00 EUR** Economique | [Détails](#)

Lieu où se trouve l'objet : Amagney, France métropolitaine
Lieu de livraison : Monde entier

Délai de livraison : Estimé entre le jeu. 29 mars et le mer. 4 avr. ⌚

Paielements : **PayPal**   

Cartes de crédit traitées par PayPal

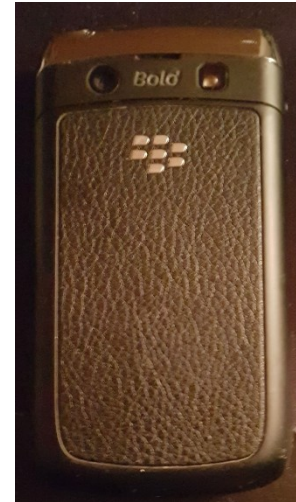
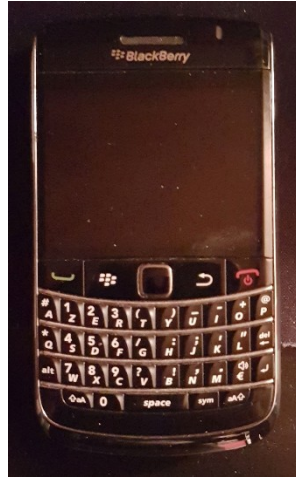
Chèque personnel

[Afficher les informations de paiement](#)

Prestation : faire les poubelles



■ Déchets numériques : téléphones



Prestation : faire les poubelles



- **Récupération de smartphones**
 - Effacé de ma manière sécurisée : 0/4
 - Nettoyage partiel (manuel) : 1/4
 - Sécurisé par un mot de passe : 1/4

Prestation : faire les poubelles



■ Récupération de smartphones

	Contacts pro	Contacts perso	Mails pro	Mots de passe	SMS pro	SMS perso
Téléphone 1	Oui	Oui	Oui		Oui	Oui
Téléphone 2	Oui	Oui				
Téléphone 3	Oui	Oui	Oui	Oui	Oui	Oui

Prestation : faire les poubelles



- **Récupération de smartphones - Cas particulier du 3ème téléphone**
 - Échanges de messages liés à une relation extra-conjugale
 - Informations disponibles :
 - Nom/prénom, numéro de téléphone du propriétaire
 - Nom/prénom, numéro de téléphone de sa conjointe/femme
 - Prénom, numéro de téléphone de sa maîtresse

Prestation : faire les poubelles



■ Récupération de smartphones – Se protéger

- Supprimer les données
- Remettre en version d'usine
- Dans le doute détruire le téléphone

■ Note :

- Si le téléphone est chiffré, remettre en version d'usine avec un nouveau chiffrement est suffisant
- Dans le doute détruire le téléphone



L'échec



- **On cherche beaucoup plus que l'on ne trouve**
- **Et quand on trouve, ça peut ne rien donner**
 - Carte SD dans un R4
 - Sac contenant plus d'une centaine de CD/DVD gravés
 - ...

Les échecs

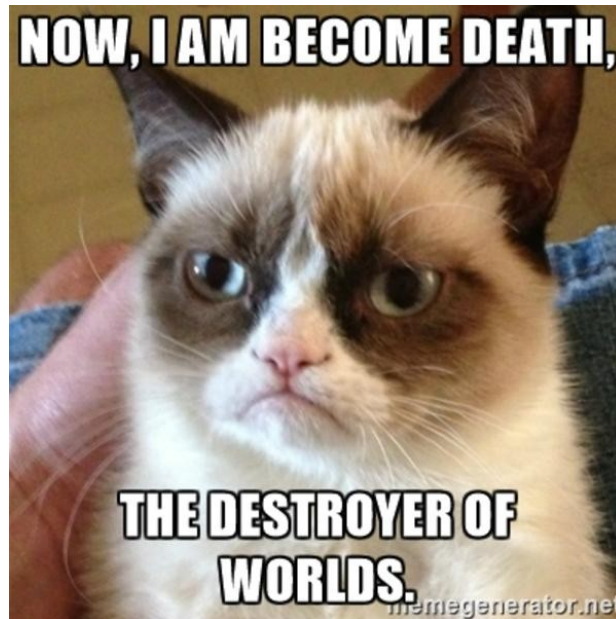


■ “Protections”





Et si on détruisait de la donnée



Destruction



■ Support numérique

- Destruction physique : broyeur, destructeur magnétique
- Destruction logique :
 - DBAN - <https://dban.org/>
 - SRM
 - (re)Chiffrer (complètement) le support

■ Support papier

- Destruction physique « complète » : broyeur, feu, eau
- Destruction physique partielle : marqueur (POSCA) ou alternative DIY (<http://graffsociety.com/Tutorials/How-to-Make-Kiwi-Mop.html>)

Destruction matérielle



Destruction matérielle



svbl
@svblxyz

Follow

Made a new 256GB drive!



12:28 PM - 23 Dec 2017



svbl @svblxyz · 23 Dec 2017

If you look for a cut resistant hard drive, Samsung was the toughest, followed by Seagate and WD. Oh and SSD are a joke to cut 🤔



♡ 60



svbl @svblxyz · 23 Dec 2017

Thanks :) The Makita portaband I used went through them quite easy. Serious upgrade from the "big-ass hammer" method I used before:



💬 1



♡ 3

Source : <https://twitter.com/svblxyz/status/944666066151723009>

Destruction “artisanale”



Zero Day Initiative
@thezdi

...

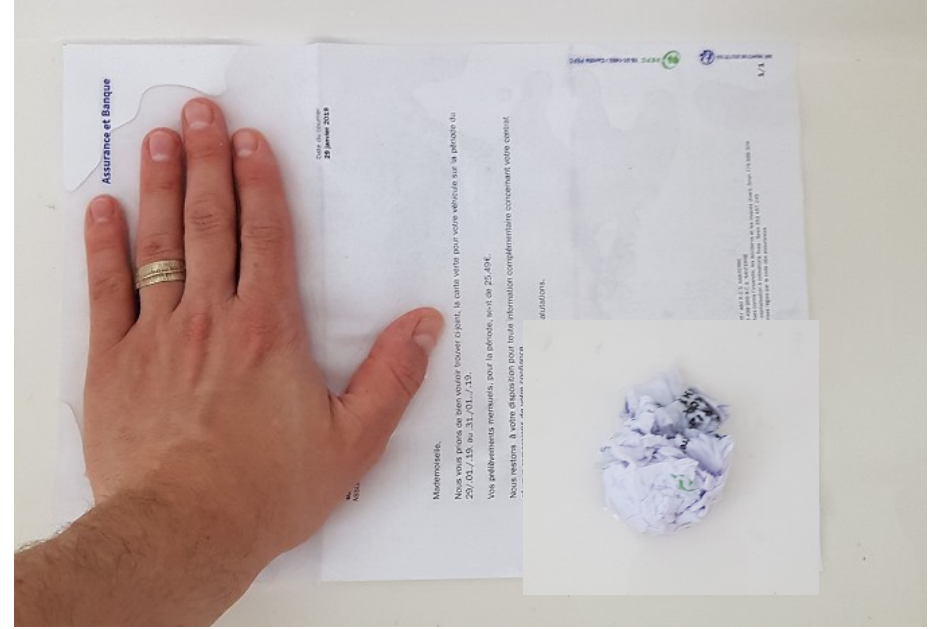
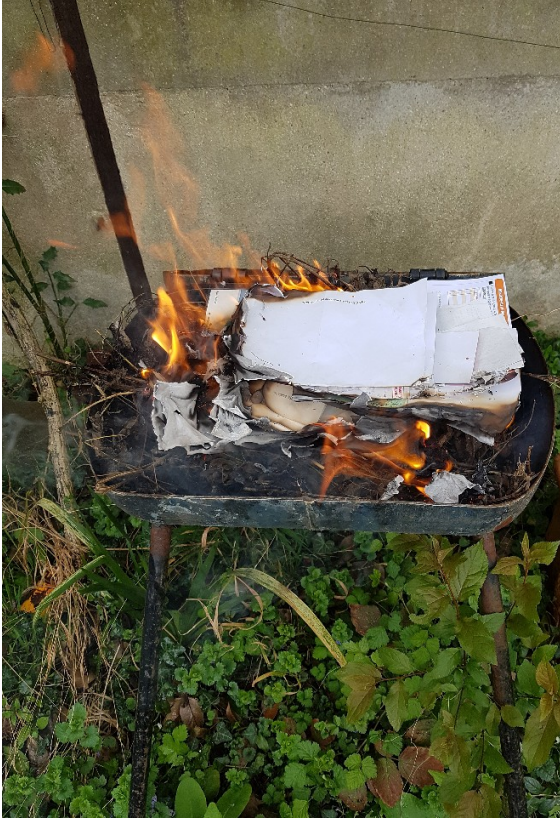
The ritual post-[#Pwn2Own](#) smashing of the USB drives has begun. [#LeaveNoTrace](#)



6:41 PM · Apr 21, 2022 · TweetCaster for iOS

Source : <https://twitter.com/thezdi/status/1517181725461336065>

Destruction “artisanale”

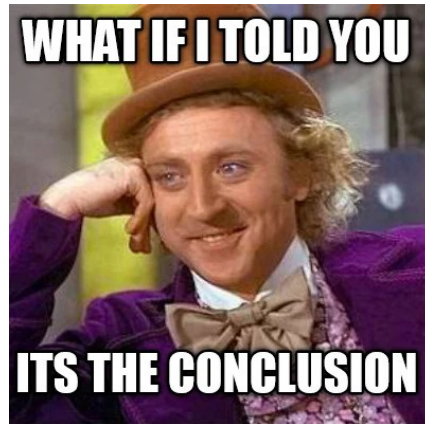


Destruction “artisanale”





Conclusion



Conclusion



- Protéger vous !
- Apprenez, recyclez, amusez-vous !
- Partager vos découvertes !

Liste des outils



■ Offensif

- Récupération de clés Wi-Fi : WirelessKeyView
http://www.nirsoft.net/utils/wireless_key.html
- Cassage de mots de passe : John the Ripper
<https://www.openwall.com/john/>
- Récupération de profil Firefox : Firefox Decrypt
https://github.com/unode/firefox_decrypt
- Récupération de fichiers effacés : PhotoRec
https://www.cgsecurity.org/wiki/PhotoRec_FR
- Attaque de badge : Proxmark

Liste des outils



■ Défensif

- Chiffrement du disque
 - VeraCrypt
<https://www.veracrypt.fr/en/Home.html>
 - LUKS (Linux)
- Effacement de disque (software)
 - <https://dban.org/>
 - SRM (man srm)

Liste des outils



■ Récupération de sauvegarde Game Boy

- GbxCart RW v1.3 Pro
 - <https://www.gbxcart.com/>
- FlashGBX
 - <https://github.com/lesserkuma/FlashGBX#installing-and-running>
- GB Camera Saver v1.12
 - https://shop.insidegadgets.com/wp-content/uploads/2018/05/GBxCart_RW_GB_Camera_Saver_v1.12.zip



<https://www.linkedin.com/company/synacktiv>

<https://twitter.com/synacktiv>

Nos publications sur : <https://synacktiv.com>