CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

Effacement d'un disque dur avant mise au rebut

Denis PUGNÈRE – IN2P3/IPNL

d.pugnere@ipnl.in2p3.fr

A3IMP - La Grande Motte - 24-26/09/2007

Notes de révision

- 09/2007 : version initiale
- 05/2011 :
  - ajout vérifications après écriture, options oflag=direct à dd
  - Ajout page « autres standards d'effacement de données »
  - Notes sur l'efficacité des méthodes

Rappel des faits

- Pourquoi on se préoccupe de l'effacement de données
  - Vol, perte d'ordinateurs (portables ou non)
  - Interventions de tiers sur le matériel : garanties, contrats de maintenance, pannes, échanges standards...
  - Mise au rebut

Quelques exemples

- Étude BBC :
  - Enquête sur les vieux ordinateurs expédiés en Afrique par le Royaume-Uni.
  - « Les données bancaires de milliers de Britanniques étaient en vente en Afrique pour seulement 30 euros chacune, révèlent les enquêteurs. »

    http://news.bbc.co.uk/2/hi/business/4790293.stm
    http://news.bbc.co.uk/2/hi/programmes/real_story/4791167.stm

Autres études

- University of Glamorgan : 317 disques dur d'occasion achetés en Angleterre, en Australie, Allemagne et aux États Unis :
  - 35 à 40% provenaient d'entreprises
  - 5% contenaient des données sensibles
- Autre étude de British-Telecom sur 200 disques :
  - ¼ étaient correctement effacés
  - Beaucoup avaient simplement des fichiers effacés depuis Windows, d'autres étaient reformatés
  - Les outils d'effacement par ré-écriture ne fonctionnent pas forcément comme prévu

Étude MIT disques dur d'occasion / ebay :

- Achat de 158 disques durs sur Ebay :
  - plus de 80% étaient en état de fonctionnement.
  - Des informations ont été récupérées dans + de 43% des disques durs.
  - Dans plus de 70% d'entre eux l'information était privée ou confidentielle (données du personnel d'une entreprise, données médicale, numéros de cartes de crédits, courrier électronique, images pornographiques...).
  - Seuls 7.59% des disques durs, étaient passés par un processus d'effacement sécurisé des données.
  - Dans leur majorité, ces dispositifs avaient été re-formatés.

  Référence :

http://www.simson.net/clips/academic/2003.IEEE.DiskDriveForensics.pdf

Autres supports d'information concernés

- Mémoires FLASH : Clés USB, memory sticks, cartes PCMCIA, organiseurs personnels, équipement de réseau (routeurs, commutateurs), téléphones mobiles, appareils photos numériques, récepteur GPS...

- Stockage optique : CDROM, DVD

- Bandes magnétiques · DLT, LTO, DAT...

- Support papier

Panne disque != perte de données

- De 1% (minimum), moyenne de 2% à 4%, jusqu'à 13% de panne de disque annuel :

  référence : http://www.cs.cmu.edu/~bianca/fast07.pdf

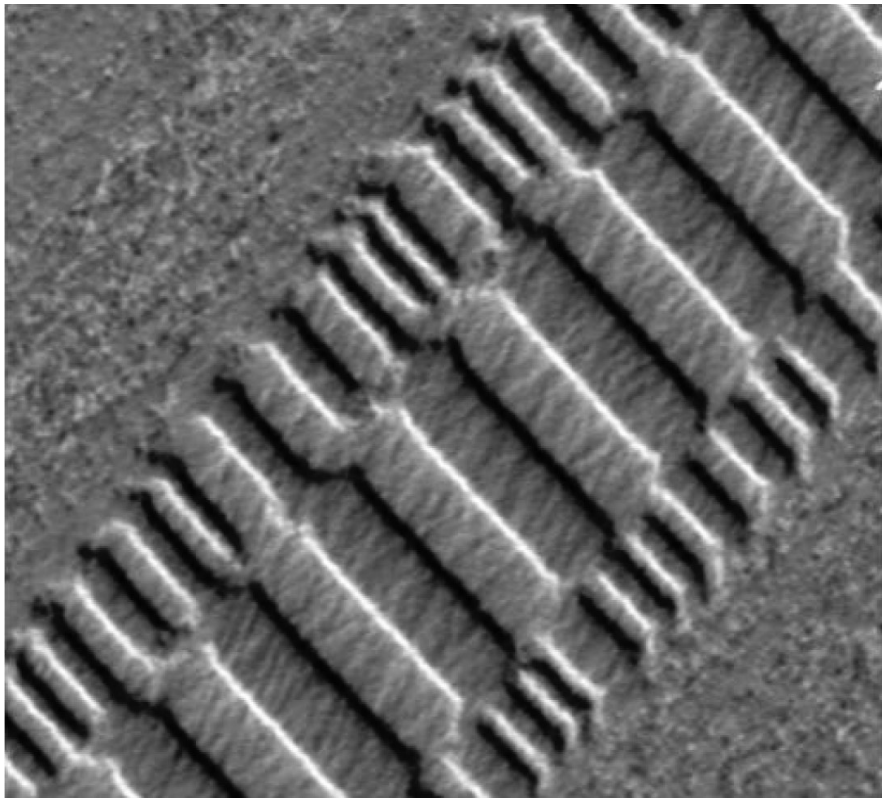
- Pannes mécaniques : têtes de lecture (choc, chute, usure...), moteur (rotation disque), servo-moteur (déplacement têtes), headcrash (les têtes heurtent les plateaux)
- Pannes électroniques : Carte contrôleur
  - Peuvent être changés en salle blanche
  - Disque inerte, composants endommagés (surtension, foudre, chaleur excessive...)

=> Panne disque ≠ perte de données

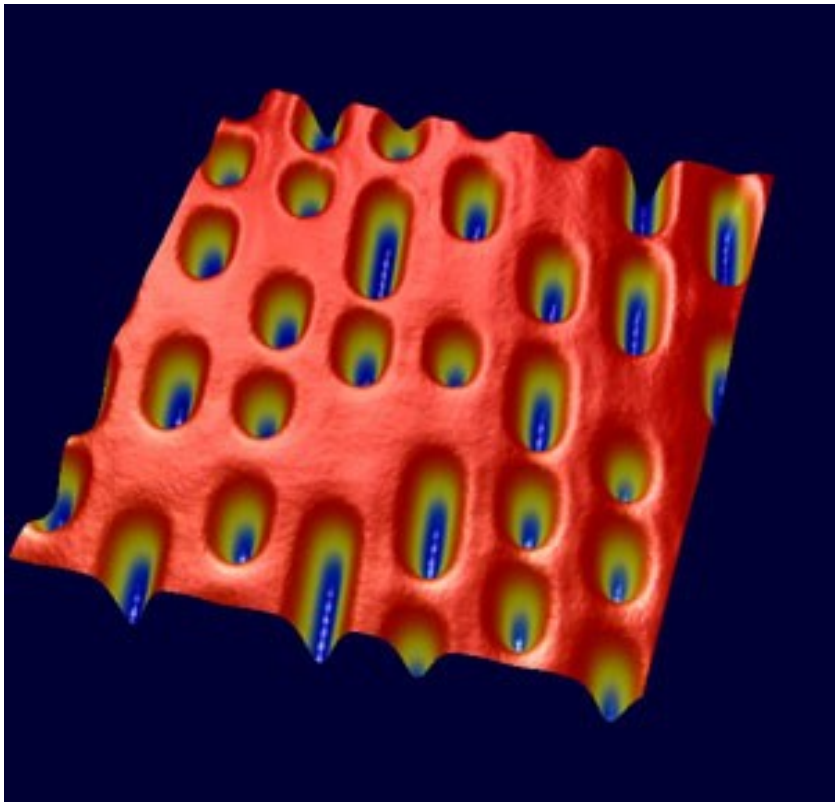
Effacement ?

- Mettre un fichier à la poubelle ≠ **effacement**, (presque) rien n'a changé :
  Effacer un fichier = modifier les méta-données qui pointent sur les blocs ou sont stockés le fichier (les blocs de données sont intacts)
- Suppression des partitions (fdisk, parted) : 1 seul bloc modifié sur tout le disque ≠ **effacement**
- Reformatage d'une partition («format c:», «mkfs /dev/hda1»...) ≠ **effacement**
  - Généralement : lecture de tous les blocs pour savoir s'ils sont valides
  - Écriture de quelques blocs seulement
  - Tous les reformatages ne ré-écrivent pas tous les blocs de la partition
  - Et la partition swap ?

Exemples de supports



Défauts d'alignement des têtes d'écriture d'un disque dur : on remarque (au centre la dernière écriture) et en périphérie les précédentes écritures. (scan de 25 µm)



Visualisation des bits écrits sur un CD (11µm x 13 µm)

Source :http://www.veeco.com

Récupération de données

- Logiciels :
  - Open source : TestDisk, PhotoRec, TCT, sleuthkit...
  - Commerciaux : GetDataback...
  - Efficaces même après re-partitionnement ou un reformatage : du moment que les blocks ou les fichiers sont stockés n'ont pas été ré-écrits
- Sociétés spécialisées dans la récupération de données

Considérations générales (non techniques)

- **L'effacement efficace des données** de supports électroniques mis au rebut n'est qu'un aspect parmi d'autres qui **doit être Prise en compte de la politique de sécurité des systèmes d'information (PSSI)**
- L'analyse de risque permet de répondre à la question : Que faire du support d'informations (CD, disque dur, papier...) ?
- La PSSI prendra aussi en considération les circuits de circulation de l'information sur tous les types de média :
  - Réseaux informatiques,
  - Procédures administratives

Techniques d'effacement de données

- Destruction mécanique du disque : électronique + support magnétique : Écrasement, incinération, torsion...
- Effacement sécurisé par démagnétisation (dégausseur)
- Méthodes d'effacement logicielles par ré-écriture (surcharge) :

Nom méthode	Nombre de passes	Description
U.S. Navy Staff Office Publication NAVSO P-5239-26	3	1 caractère, son complément, un motif aléatoire (vérification obligatoire)
NSA/CSS Storage Device Declassification Manual (SDDM)	N/A	Degaussage ou destruction physique
British HMG Infosec Standard 5, Baseline Standard	1	Motif = 0, vérification facultative
British HMG Infosec Standard 5, Enhanced Standard	3	Motif = 0, motif = 1, un motif aléatoire, vérification obligatoire
Communications Security Establishment Canada ITSG-06	3	Motif = 0 ou 1, le complément du caractère, un motif aléatoire,
Peter Gutmann's Algorithm	1 à 35	Différents motifs, purement théorique
Bruce Schneier's Algorithm	7	Motif = 0, motif = 1 et 5 motifs aléatoires

Effacement par ré-écriture efficace ?

- Nécessité de plusieurs passes ? : pas forcément [1]
- Mais :
  - Secteurs défectueux, rattrapage...
  - Commandes constructeur spécifiques,
  - zones cachées (DCO, HPA)
  - Spécificités des supports de stockage non magnétique (clés USB, cartes à mémoire, mémoires FLASH)

[1] : "Overwriting Hard Drive Data: The Great Wiping Controversy" : Wright, Craig; Kleiman, Dave; Sundhar R.S., Shyaam (December 2008)

Logiciels spécifiques

- Logiciels :
  - dban (Darik's Boot and Nuke), wipe, shred, srm...
  - Blanco (qualifié par la l'ANSSI http://www.ssi.gouv.fr/site_rubrique52.html)
- Commandes unix simples (Attention : zones DCO et HPA non prises en comptes) :

  « dd if=/dev/zero of=/dev/sdX bs=8192 conv=noerror oflag=direct »
  suivi de :
  « dd if=/dev/urandom of=/dev/sdX bs=8192 conv=noerror oflag=direct »

  « dd if=/dev/zero of=/dev/sdX » ne suffit pas : Il s'arrête dès qu'un secteur défectueux est présent sur le disque

- Vérifier que « dd » a bien sur-écrit tout le disque :
  - Calcul d'empreintes de secteurs avant / après et comparaison
  - Utilisation d'un logiciel de récupération de données (photorec...)

Biblio

- Guide technique n° 972-1/SGDN/DCSSI : « Guide technique pour la confidentialité des informations enregistrées sur les disques durs à recycler ou exporter. »

  http://www.ssi.gouv.fr/archive/fr/documentation/Guide_effaceur_V1.12du040517.pdf

- Effacement des supports de stockage de masse

  http://www.ssi.gouv.fr/site_article172.html

  http://en.wikipedia.org/wiki/Data_erasure

  http://www.forensicswiki.org/wiki/DCO_and_HPA