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

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

MIT disques dur d'occas / 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.
    Source

référence :

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

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 (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

Récupération de données

- Logiciels :
  - GPL like : TestDisk, PhotoRec, TCT, sleuthkit...
  - Commerciaux : GetDataback...
  - Même après repartitionnement, reformatage : si les blocks où les fichiers sont stockés n'ont pas été ré-écrits
- Sociétés spécialisées dans la récupération de données

Autres supports d'information

- Mémoires FLASH : téléphones mobiles, appareils photos numériques, organiseurs personnels, récepteur GPS, équipement de réseau, clés USB, memory sticks, cartes PCMCIA...



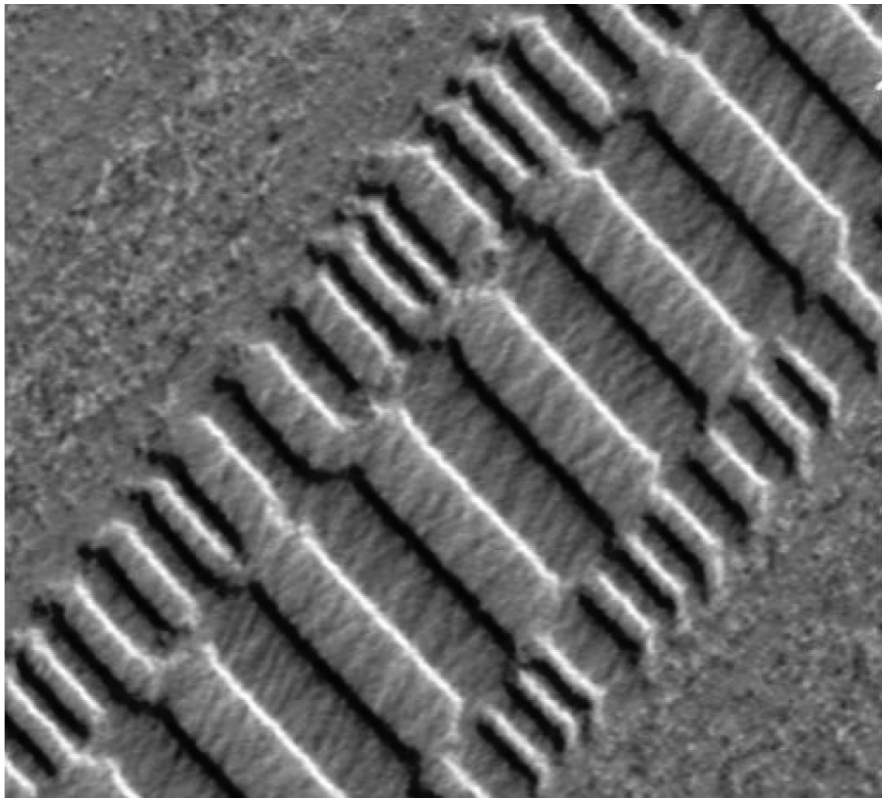
- Stockage optique : CDROM, DVD

- Bandes magnétiques : DLT, LTO, DAT...
- Support papier...

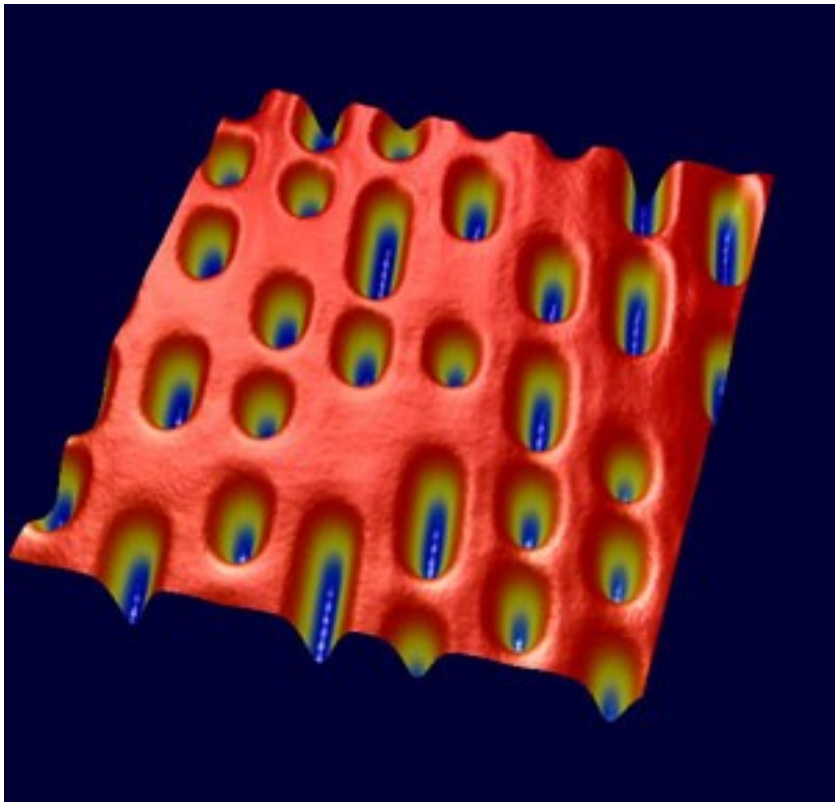
Effacement incomplet

- Mettre un fichier à la poubelle : ce n'est pas un 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) : 1 seul bloc modifié sur tout le disque
- Reformatage («format c:», «mkfs /dev/hda1») :
  - Généralement : lecture de tous les blocs pour savoir s'ils sont valides
  - Écriture de quelques blocs seulement

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

Techniques d'effacement de données (efficaces)

- Effacement sécurisé par démagnétisation (dégausseur) : destruction du support magnétique
- Effacement par ré-écriture :
  - Exemple du standard DoD 5220-22.M du Département de la Défense Américaine : plusieurs passes : la première avec un caractère fixe, la seconde avec son complément et la troisième avec des données aléatoires.
- Guttman method : ré-écriture 35 fois avec des motifs différents
  http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html
- Commandes unix simples :

  dd if=/dev/zero of=/dev/hda bs=8192 conv=noerror
  dd if=/dev/urandom of=/dev/hda bs=8192 conv=noerror

  et vérifier que 'dd' a bien écrit sur tout le disque
- Logiciels : dban (Darik's Boot and Nuke)...

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

Biblio

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

  Référence :

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

- NIST : Guidelines for Media Sanitization : SP 800-88 September 2006

  Référence :
  http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf