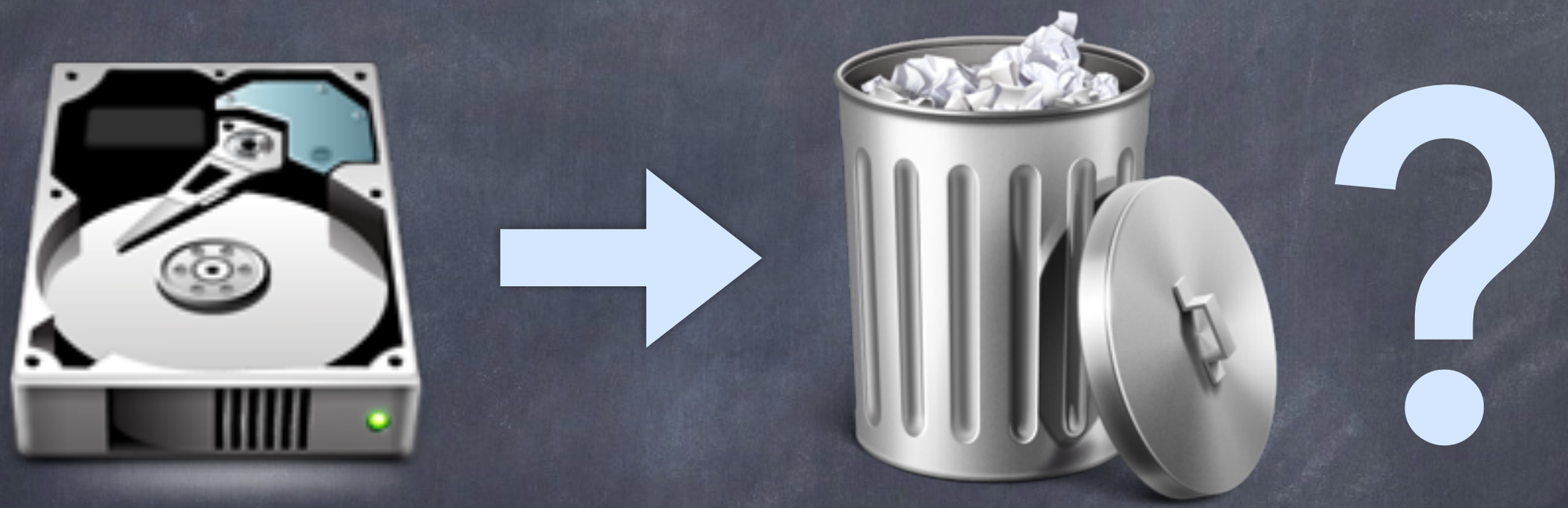
Comment effacer vraiment un disque dur, et comment retrouver des informations?



Jérôme Skoda
M2 Computer Science
University of Paris 7

Joaquim Lefranc
M2 Computer Science
University of Paris 7

contact@jeromeskoda.fr - lefrancjoaquim@gmail.com

Plan de la présentation

1. *Comment fonctionne un disque dur*
2. *Rémanence des données*
3. *Les systèmes d'exploitation*
4. *Comment récupérer nos données effacées*
5. *Comment effacer les données définitivement*

contact@jeromeskoda.fr - lefrancjoaquim@gmail.com

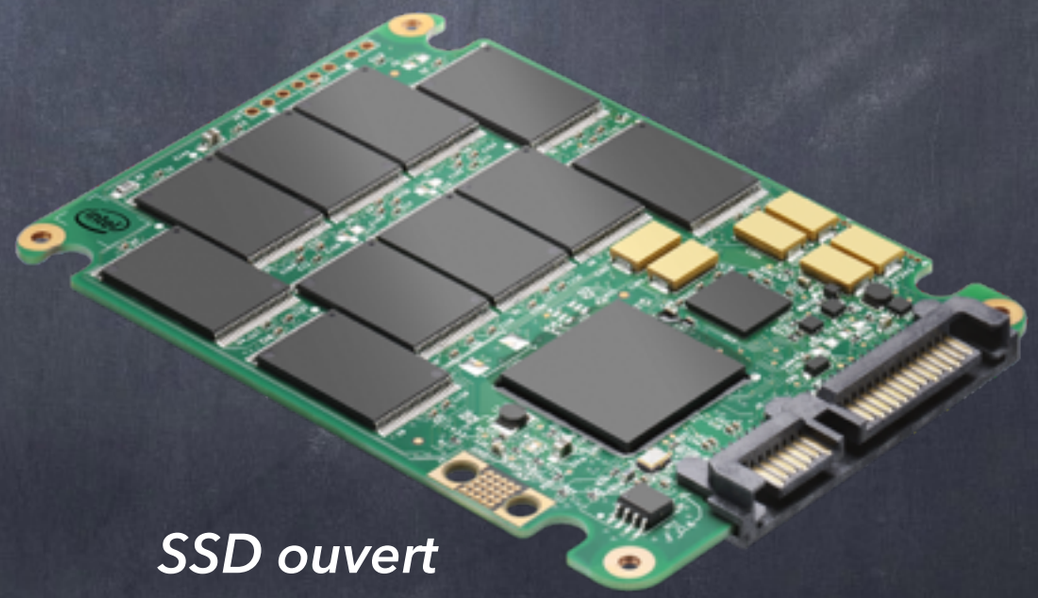
Comment fonctionne un disque dur ?

Deux type de disque dur :

HDD : électromagnétisme

SSD : mémoire électronique statique

HDD ouvert



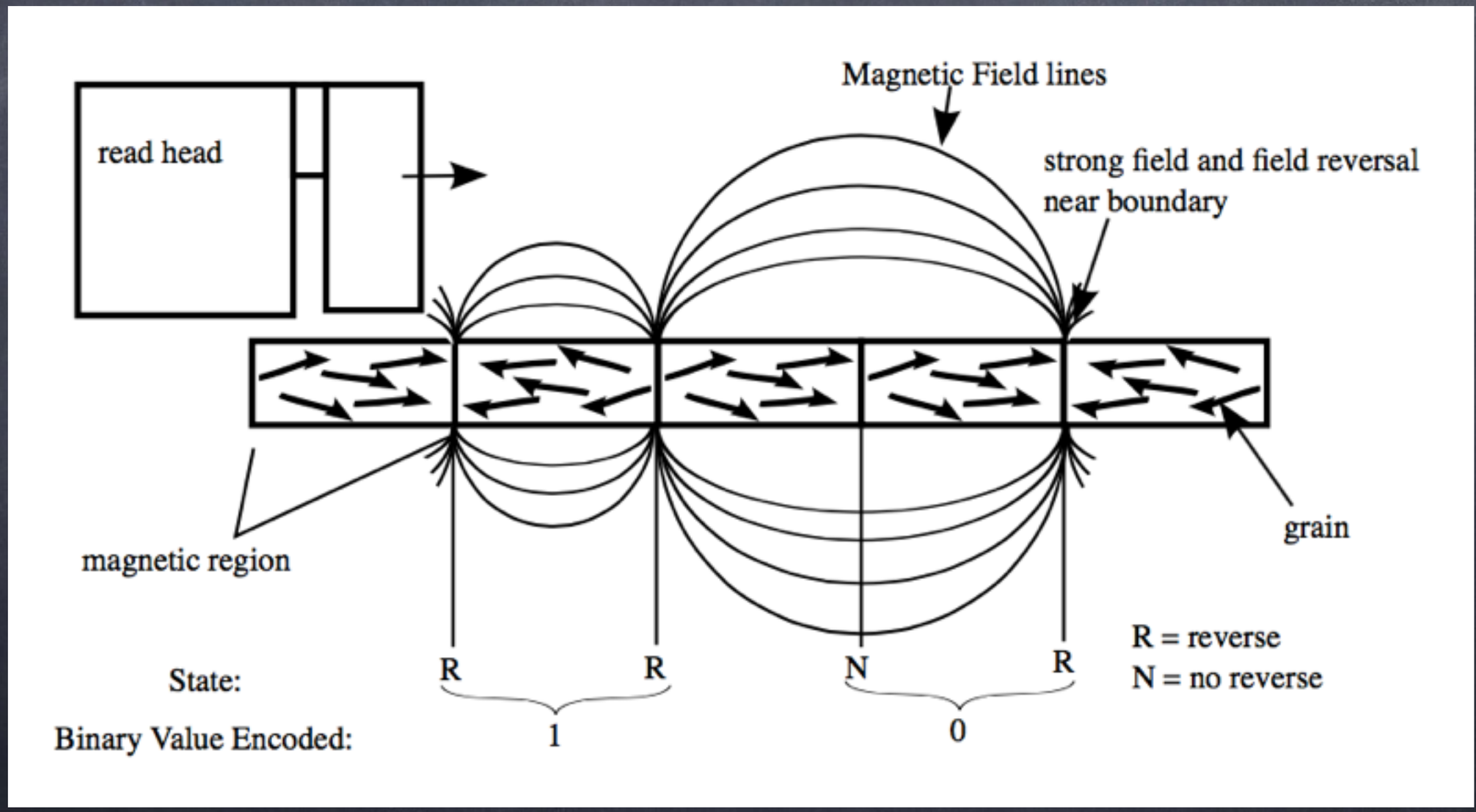
SSD ouvert

contact@jeromeskoda.fr - lefrancjoaquim@gmail.com

Comment fonctionne un disque dur ?

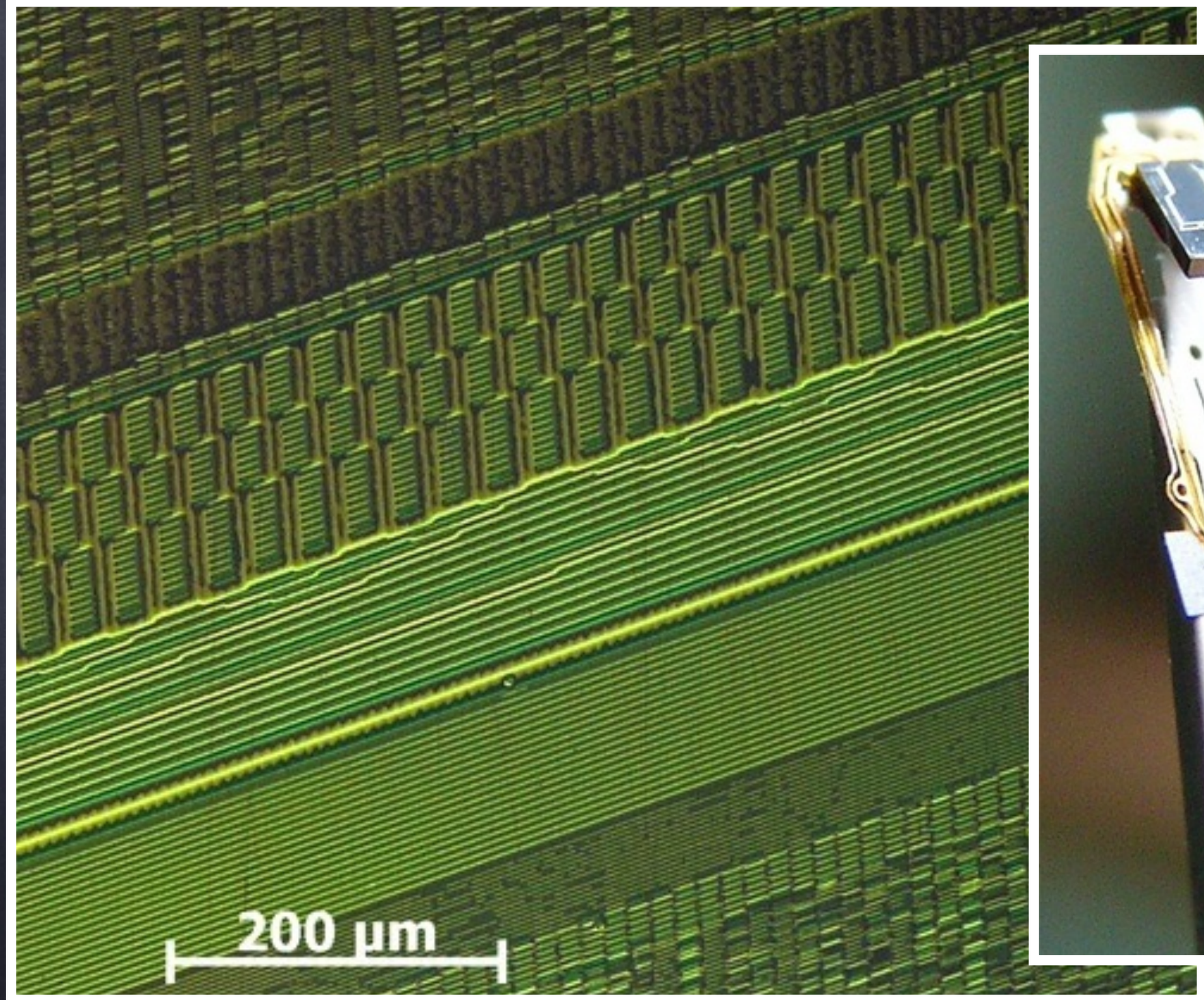
Représentation des données - HDD :

NORD *= 1 ;* ***SUD*** *= 0*



contact@jeromeskoda.fr - lefrancjoaquim@gmail.com

Comment fonctionne un disque dur ?



contact@jeromeskoda.fr - lefrancjoaquim@gmail.com

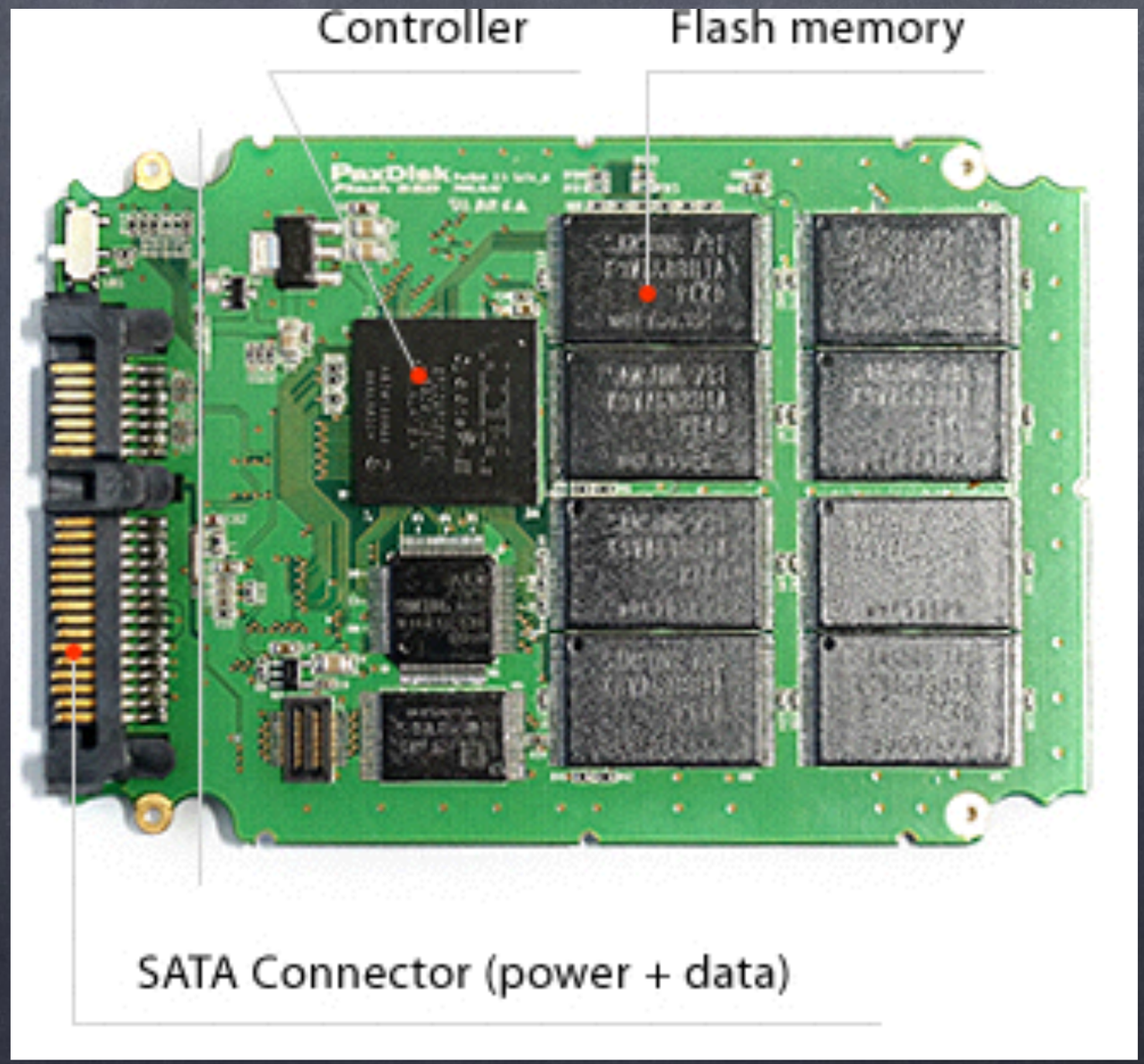
Comment fonctionne un disque dur ?

Représentation des données - SSD :

- Contrôleur

- Mémoire

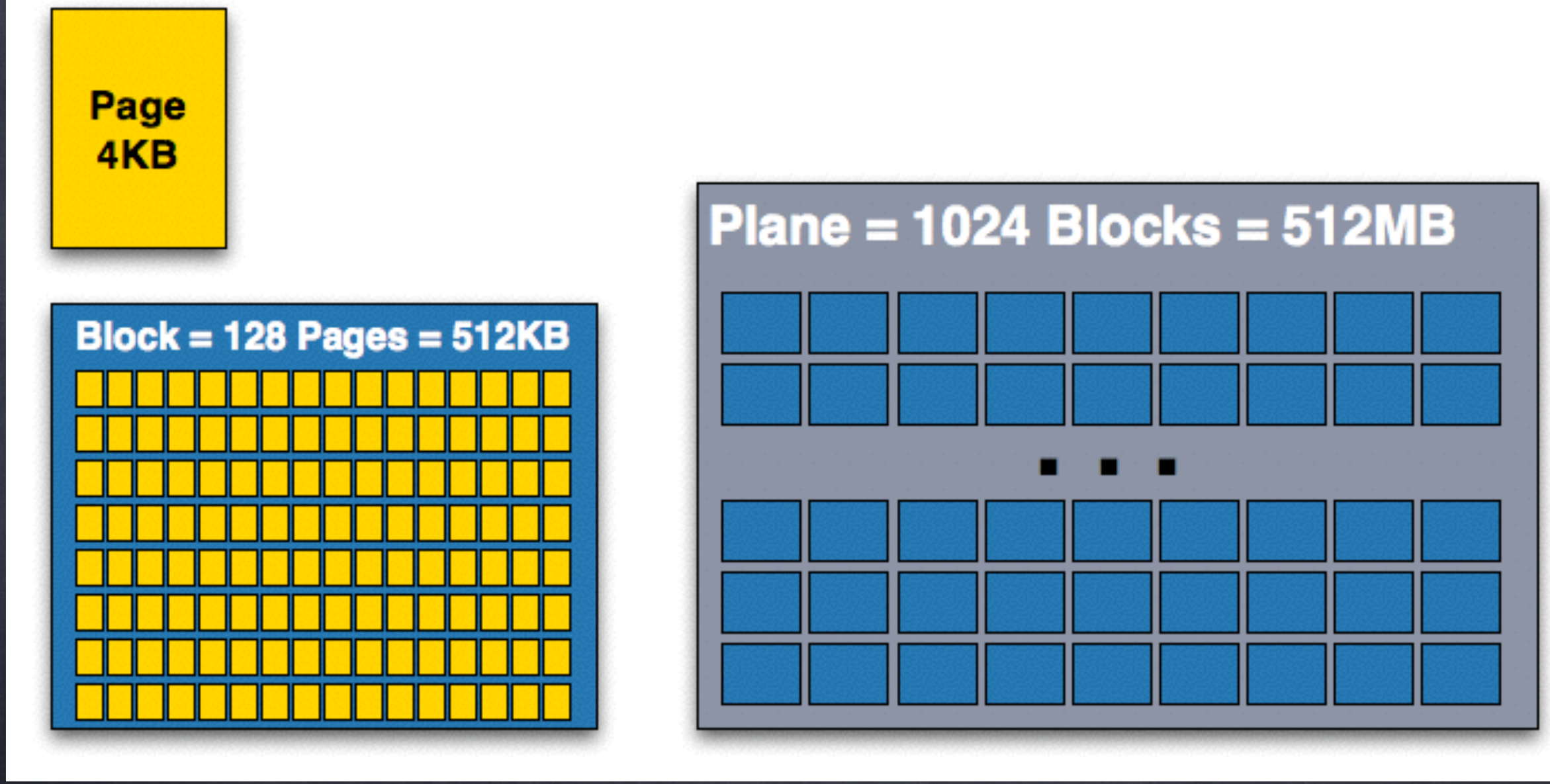
- Interface hôte



Composition d'un SSD

contact@jeromeskoda.fr - lefrancjoaquim@gmail.com

Comment fonctionne un disque dur ?



Répartition en Page / Block / Plane

contact@jeromeskoda.fr - lefrancjoaquim@gmail.com

Rémanence des données

- *Pas de fonctionnalité d'effacement*
- *Réécriture sur les anciennes données*

Imparfait car imprécisions de la tête de lecture

Il reste des traces exploitables des anciennes données

Rémanence des données

Orientation imparfaite des bits :

NORD : 0.7 - 1.0
SUD : 0.0 - 0.3
ERREUR : 0.4 - 0.6

D = 1 0 1 0
E = 0 0 0 0

D = 0.8 0.2 0.8 0.2
E = 0.3 0.0 0.3 0.1

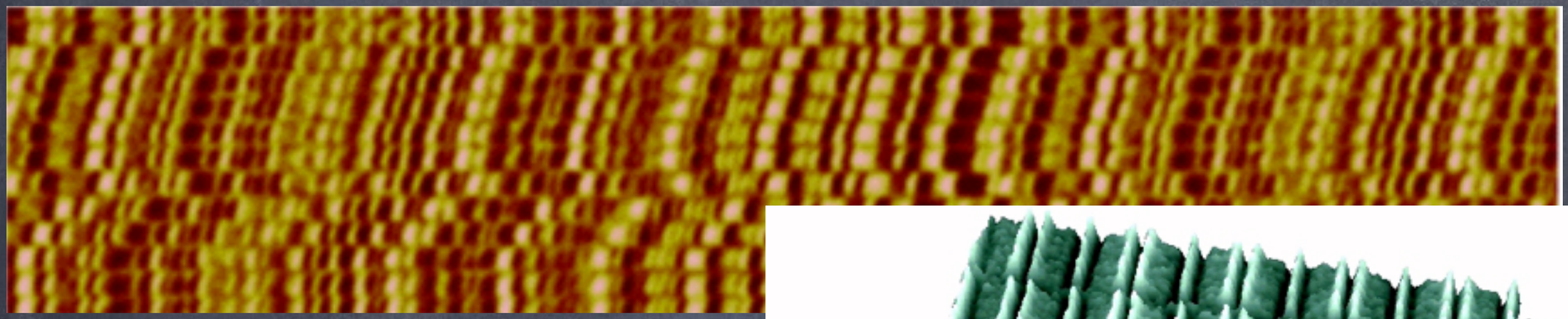
On peut voir ici que l'écriture à 0 des bits 1 et 3 ont eu pour conséquence de "renforcer" les bits 2 et 4.

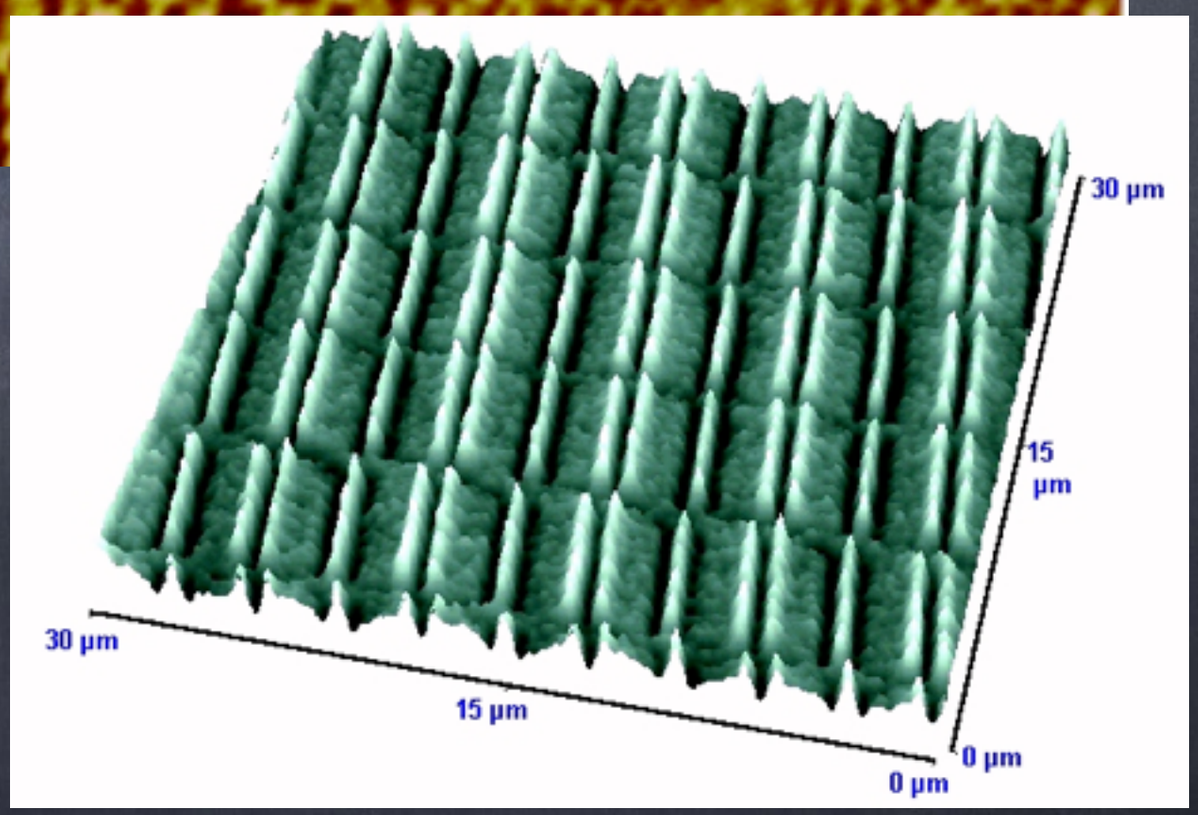
contact@jeromeskoda.fr - lefrancjoaquim@gmail.com

Rémanence des données

Outils d'analyse :

- La microscopie à force magnétique (MFM)





Modélisation d'imagerie MFM sur un disque dur

contact@jeromeskoda.fr - lefrancjoaquim@gmail.com

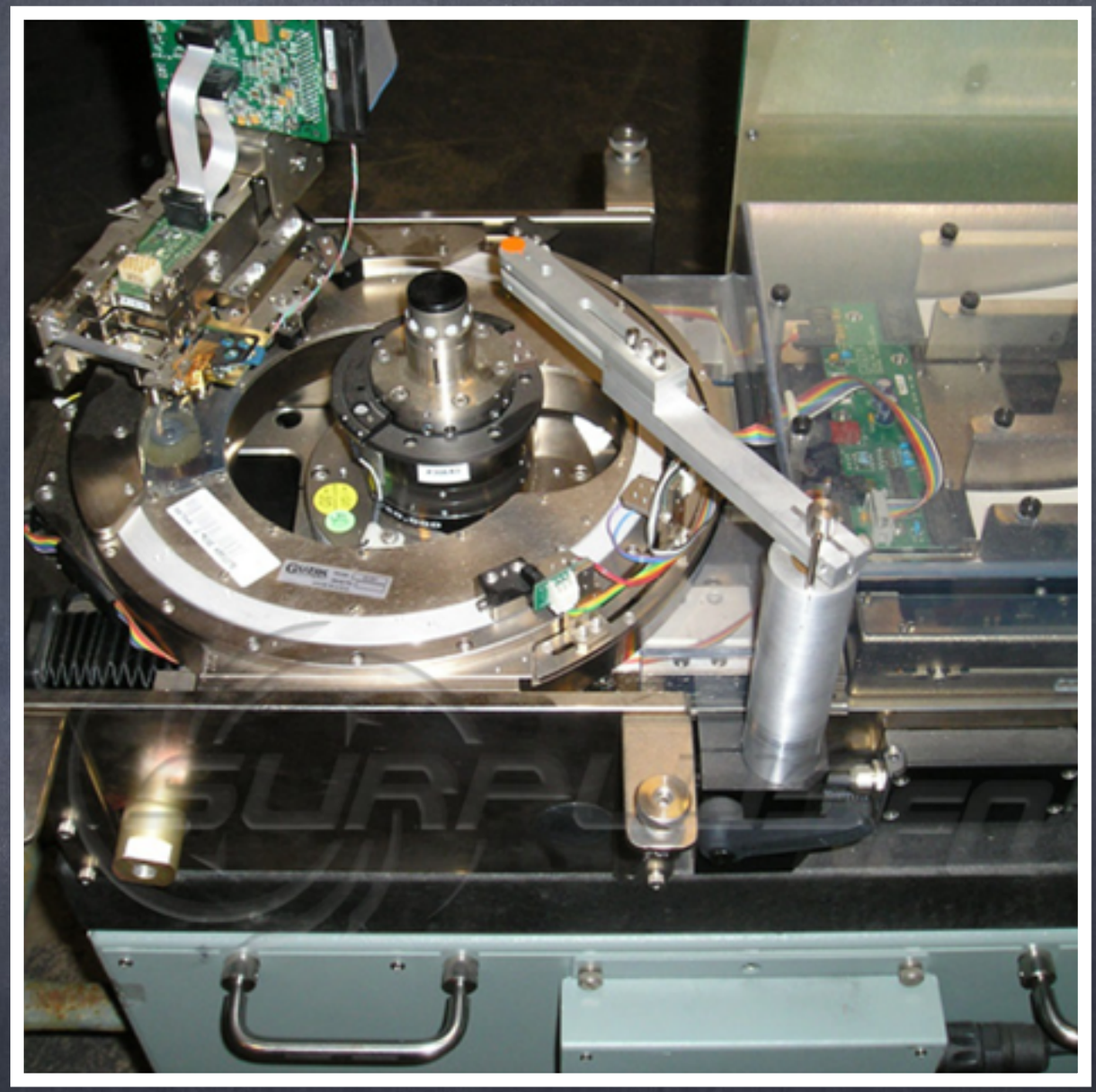
Rémanence des données

Outils d'analyse :

- Analyse sur un Spin-stand

Classique : 1 -> 0.95

SpinStand : 1 -> 1.05

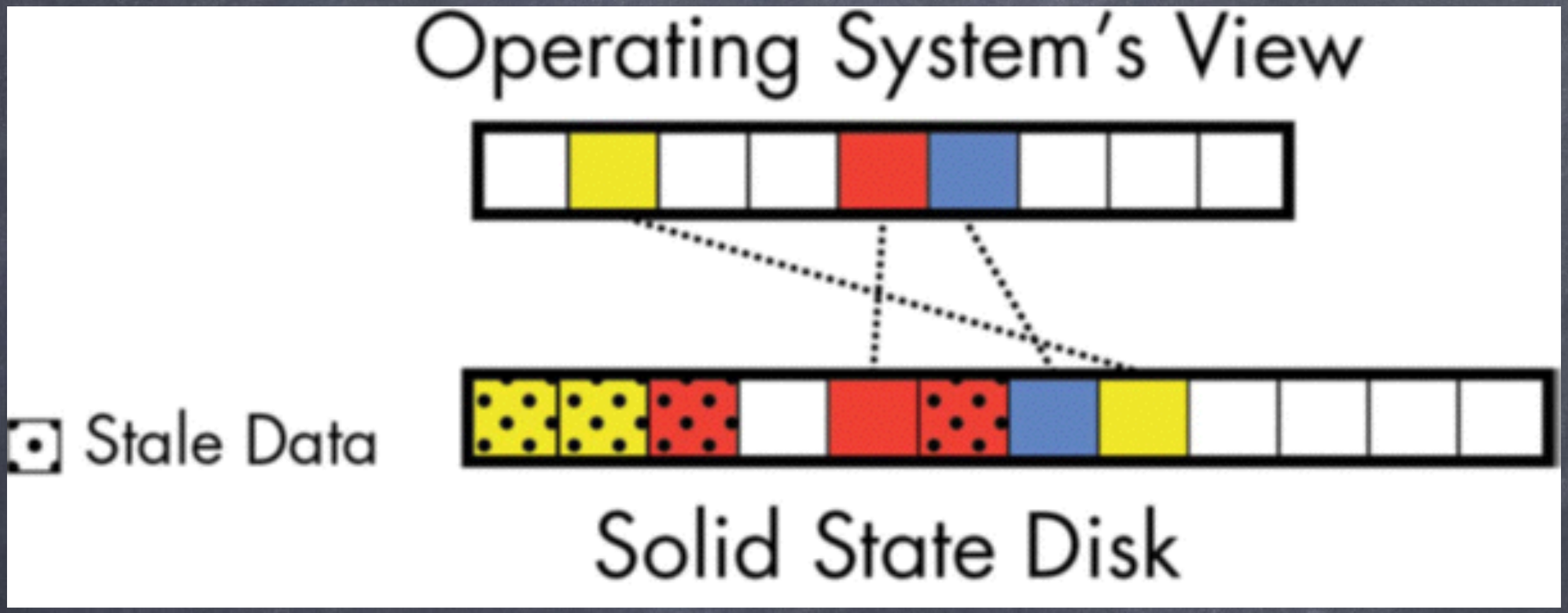


Head test spin stand

contact@jeromeskoda.fr - lefrancjoaquim@gmail.com

Rémanence des données

SSD :



Répartition des anciennes données conservé sur SSD

Impossible de s'assurer qu'un fichier est définitivement supprimé sur un SSD sans procéder à un effacement complet

contact@jeromeskoda.fr - lefrancjoaquim@gmail.com

Le système d'exploitation

Supprime t-il vraiment les fichiers ?

- *La récupération de fichiers supprimés est un standard pour l'expérience utilisateur*

- *Transfère vers la corbeille et ajout de méta-données*

Récupération possible des documents effacés

Même après vidage de la corbeille les données existent encore

contact@jeromeskoda.fr - lefrancjoaquim@gmail.com

Le système d'exploitation

Les métadonnées persistante

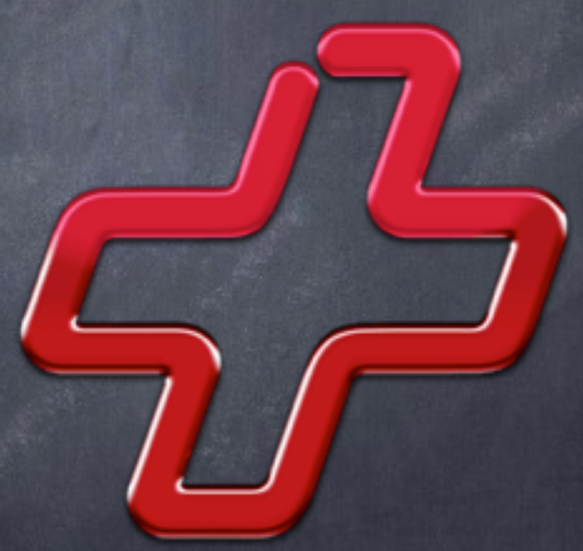
- *Traces d'indexation, fichiers temporaires, miniatures*
- *Miniatures générées dans des fichiers cachés*
- *Indices pour les enquêtes*

.DS_Store

Comment récupérer nos données effacées ?

Logiciels disponibles :

- *DataRescue (MacOS)*



Tri-edre DataRescue

contact@jeromeskoda.fr - lefrancjoaquim@gmail.com

Comment effacer les données définitivement ?

Les enjeux d'une suppression efficace sont multiple :

- *Suppression d'informations personnelles ou professionnelles*
- *Avant de jeter ou vendre un HDD*
- *Espionnage industriel*

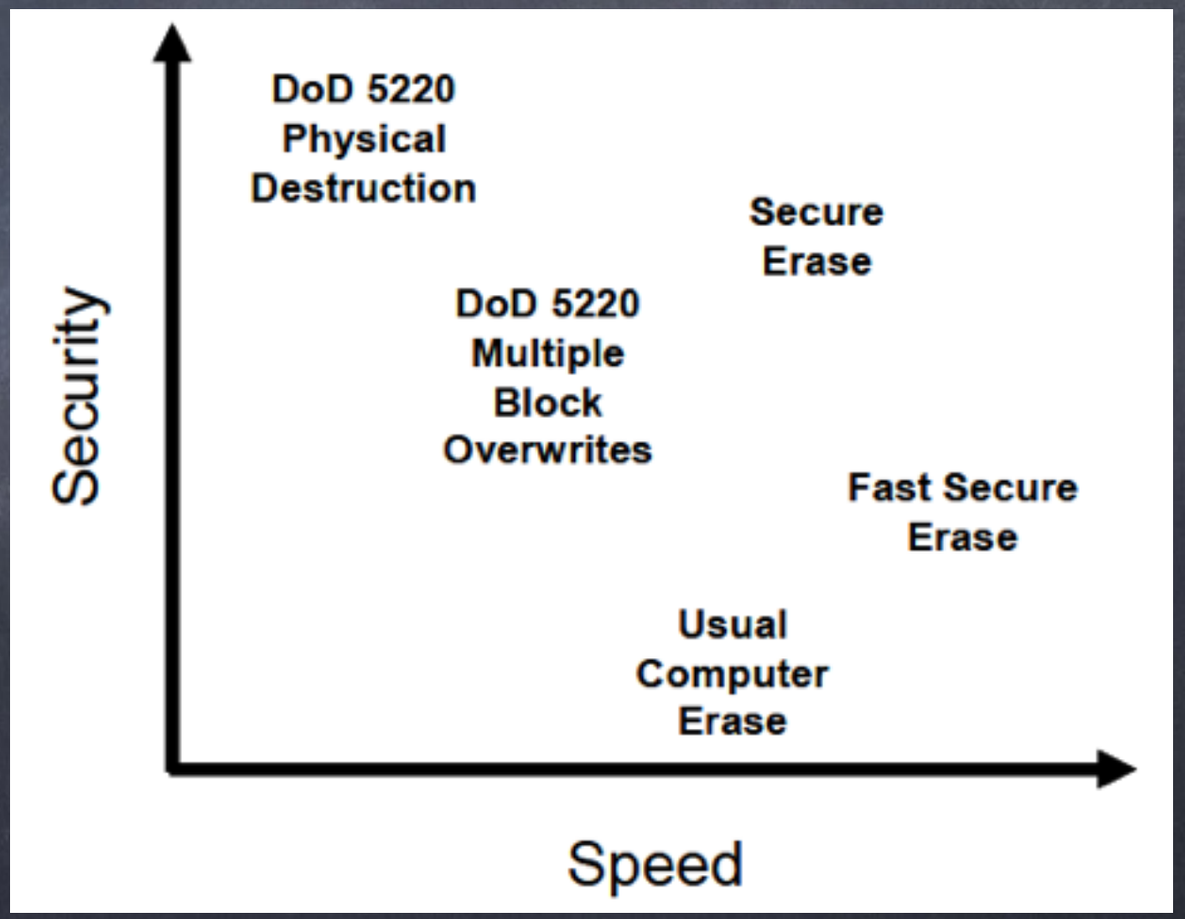


Tableau comparatif
Sécurité vs. Vitesse

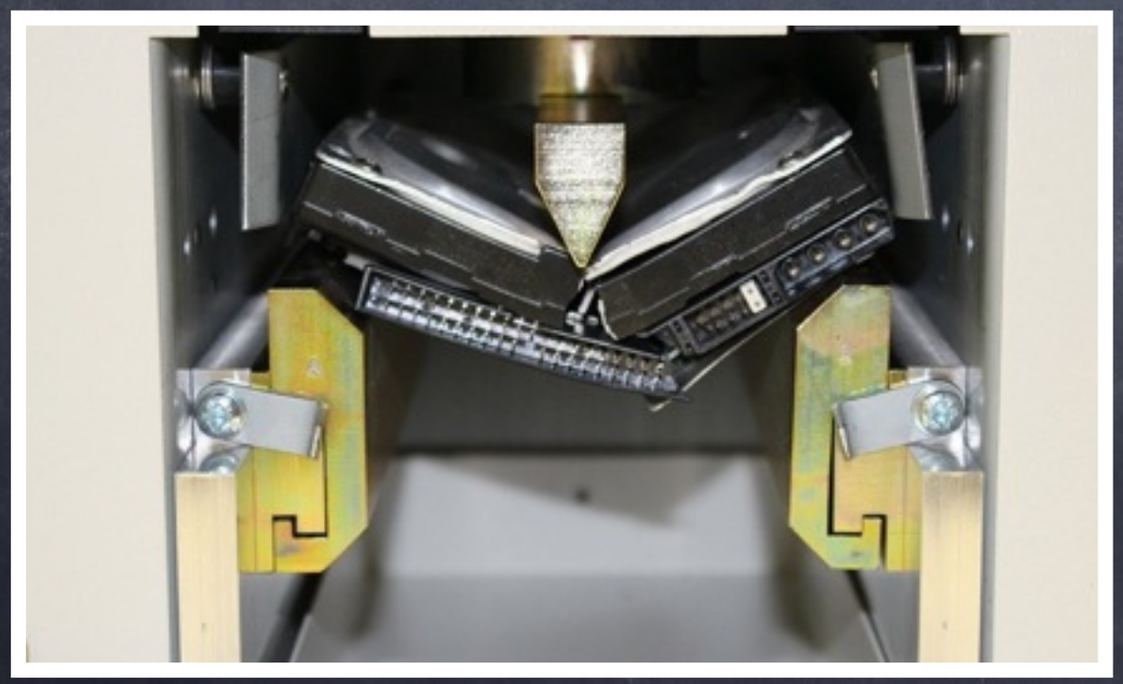
contact@jeromeskoda.fr - lefrancjoaquim@gmail.com

Comment effacer les données définitivement ?

Destruction du lecteur physique :

- *Les dégât des eaux, feu ou surtension*
- *Le micro-onde*

Le découpage, perçage ou pliage des plateaux



Pliage d'un disque dur

Perçage d'un disque dur

contact@jeromeskoda.fr - lefrancjoaquim@gmail.com

Comment effacer les données définitivement ?

Effacement par réécriture :

$ sudo dd if=/dev/zero of=/dev/sdX

Pas suffisant comme vu précédemment

$ sudo dd if=/dev/zero of=/dev/sdX
$ sudo dd if=/dev/urandom of=/dev/sdX

C'est sur ce principe que fonctionne la plupart des algorithmes d'effacement sécurisé.

Comment effacer les données définitivement ?

Quelques algorithmes :

Algorithme	Passe 1	Passe 2	Passe 3
DoD 5220.22-M	'0'	'1'	aléatoire
CSEC ITSG-06	'1' or '0'	not(passe1)	aléatoire
AR 380-19	aléatoire	spécifié	not(spécifié)
AFSSI-5020	1	0	aléatoire

Darik's Boot and Nuke (DBAN) *un logiciel libre pouvant être lancé depuis un clef USB bootable*

contact@jeromeskoda.fr - lefrancjoaquim@gmail.com

Comment effacer les données définitivement ?

Effacement total d'un SSD :

- *Identifier le SSD à effacer*

  $ hdparm -I /dev/sdX *- Affiche les informations sur un lecteur.*

  $ hdparm -I /dev/sdX | grep Model *- Affiche le modèle du lecteur*

- *Vérifier que le disque est ni bloqué ni gelé*

  $ hdparm -I /dev/sdX | grep locked *- Affiche si le disque est bloqué*

  $ hdparm -I /dev/sdX | grep frozen *- Affiche si le disque est gelé*

- *Effacement du SSD*

  $ hdparm –security-erase PASS /dev/sdX *- Efface le SSD*

contact@jeromeskoda.fr - lefrancjoaquim@gmail.com

Comment effacer les données définitivement ?

Effacement d'un fichier sur disque dur :

- *"shred" ou "srm"*
- *Plusieurs passes d'écrasement des données*

Effacement d'un fichier sur SSD :

Il n'existe pas de possibilité de supprimer définitivement un fichier d'un SDD avec certitude sans passer par un effacement complet.

Effacement sécurisé de données chiffrées :

Il est possible de supprimer les clés de déchiffrement ce qui rend toutes les données stockées inaccessibles

contact@jeromeskoda.fr - lefrancjoaquim@gmail.com

Conclusion

Pour conclure …

C’est très mal

C’est très bien

contact@jeromeskoda.fr - lefrancjoaquim@gmail.com

Sources

https://www.cs.auckland.ac.nz/%7Epgut001/pubs/secure_del.html

https://escholarship.org/uc/item/26g4p84b

https://www.nber.org/sys-admin/overwritten-data-guttman.html

https://www.researchgate.net/publication/228740643_Secure_erase_of_disk_drive_data

https://cseweb.ucsd.edu/~swanson/papers/Fast2011SecErase.pdf

cmrr.ucsd.edu/_files/data-sanitization-tutorial.pdf

https://standards.freedesktop.org/trash-spec/trashspec-latest.html

http://caselaw.findlaw.com/us-3rd-circuit/1522221.html

https://www.nodisknorisk.com/fr/exemple-de-la-recuperation-de-donnees-perdues

https://doc.ubuntu-fr.org/shred

contact@jeromeskoda.fr - lefrancjoaquim@gmail.com