



Laboratoire d'Arithmétique,  
de Calcul Formel et d'Optimisation

UMR CNRS 6090



Laboratoire Méthodes et  
Structures Informatique

EA2632



SSTIC'2005

# La guerre du développement numérique Menaces sur la confidentialité des photos numériques

P. Dusart

dusart@unilim.fr

**D. Sauveron**

**damien.sauveron@unilim.fr**

01/06/2005

# *Plan de l'exposé*

- ⇒ Comparaison Argentique/Numérique
- ⇒ Les bornes de développement numérique
- ⇒ Problèmes de confidentialité
- ⇒ Crackage du CD Fujifilm
- ⇒ Conclusion

# Argentique versus Numérique

Prise de vue

Support intermédiaire

Support final

Argentique



Rachat

P  
H  
O  
T  
O  
G  
R  
A  
P  
H  
E



Numérique



Réutilisation

B  
O  
R  
N  
E  
S



Avantages :  
Visualisation instantanée  
+ suppression à coût nul

# *Bornes de dvpt numérique*

Sauvegarde



Tirage



Laboratoires  
de développement

# Quelques problèmes de confidentialité

	Argentique		Bornes numériques	
	PhotoLab	Laboratoire	Via CD crypté	Via l'Internet
Copie lors du développement	<b>Facile</b> <i>(Photo Obsession)</i>	<b>Difficile</b> <i>(débit important)</i>	<b>Très facile</b> <i>(DD de la borne)</i>	
Copie lors du transfert		<b>Difficile</b> <i>(débit important)</i>	<b>Très facile</b> <i>(CD cassé)</i>	<b>Très facile</b> <i>(pas de chiffrement)</i>

# Crackage du CD

## ⇒ Analyse du CD

- Insertion du CD Fujifilm dans un graveur :
  - 2 sessions dont 1 seule session fermée
  - 2<sup>ème</sup> session illisible dans un lecteur CD
  - 1<sup>ère</sup> session trop petite pour contenir les photos
- **Première protection !**

CD Fujifilm

ISO 1

ISO 2 ouverte

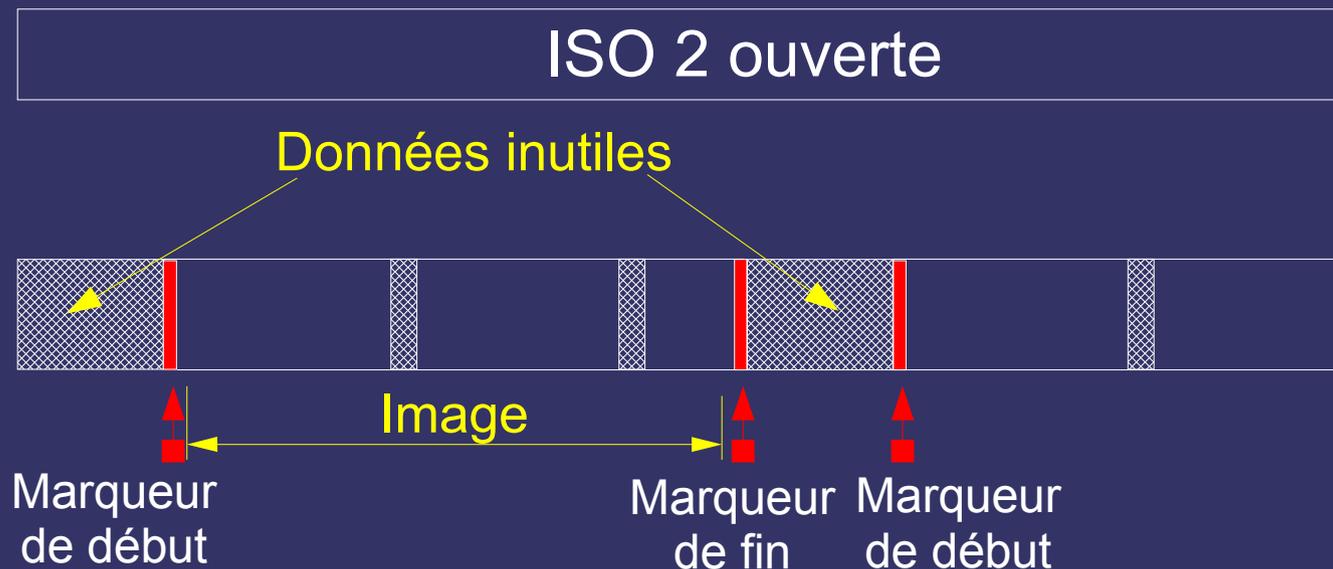
## ⇒ La récupération de la session cachée

- Extraction avec *Easy CD Creator* au format ISO

# Crackage du CD

## ⇒ Analyse du fichier ISO

- Constat :
  - Images + données inutiles
- **Deuxième protection !**



## ⇒ L'extraction des fichiers images corrompus

- Utilisation des marqueurs JPEG pour extraire les images

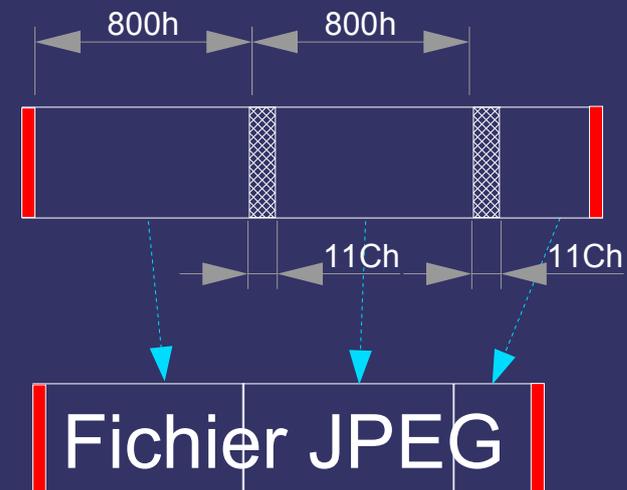
# Crackage du CD

## ➔ Analyse des fichiers JPEG

- Constat :

- tailles des images obtenues  $>$  tailles des images originales
- Chaque image contient des données rajoutées de longueur fixe (11Ch octets) et se répétant de façon périodique tous les 800h octets (soit aux positions 800h, 1000h, 1800h, ...)

- **Troisième protection !**



## ➔ La reconstruction des images

- Après suppression, les images obtenues sont identiques aux images initiales.

# Résumé de l'attaque

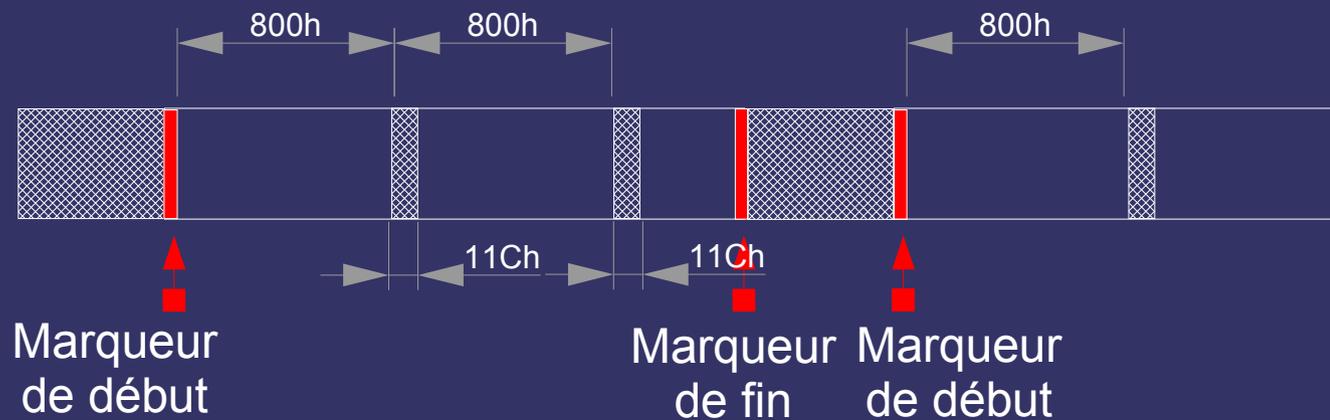
CD Fujifilm

Étape 1

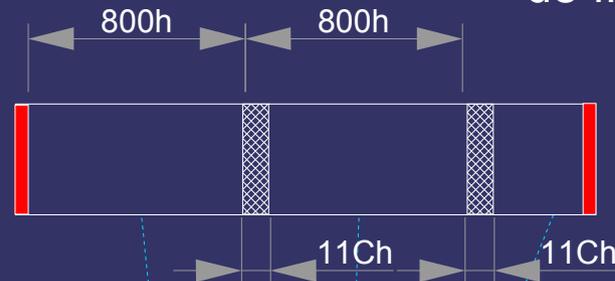
ISO 1

ISO 2 ouverte

Étape 2



Étape 3



Étape 4



# *Conclusions*

- ➔ Le numérique multiplie les menaces
- ➔ Les solutions déployées pour assurer la confidentialité sont faibles
- ➔ Il est nécessaire d'utiliser de vrais mécanismes cryptographiques
- ➔ Une bonne information du consommateur est essentielle
- ➔ Utilisation des nouveaux services numériques à mettre en balance avec les risques

# *Copyright et accord*

- ➔ Les illustrations utilisées dans cette présentation sont la propriété exclusive de leurs auteurs et toute utilisation commerciale ne peut se faire sans leur accord.
- ➔ La société Fujifilm a été informée de nos travaux et nous a autorisé à les publier.