



# Investigation Numérique : L'apport des logiciels libres

@ : Solal.jacob@arxsys.fr

Tel : 01 46 36 25 22

[www.arxsys.fr](http://www.arxsys.fr)

[www.digital-forensic.org](http://www.digital-forensic.org)

# Sommaire

Introduction : l'investigation numérique

Évolution des logiciels

Open-source Vs propriétaires

Notre solution

Conclusion

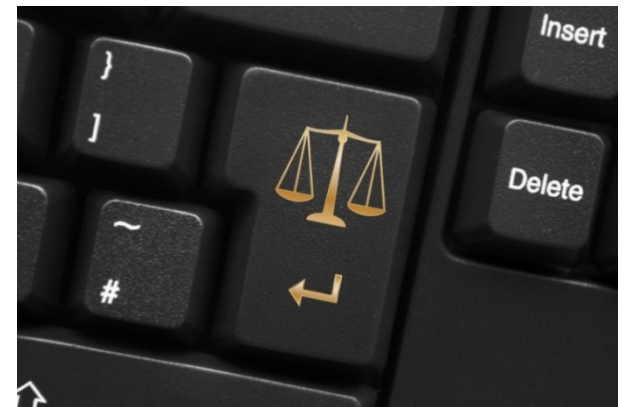
# L'investigation numérique

- **Autopsie** des systèmes numériques
- Traite les Informations Stockées électroniquement (ESI)
- Répondre aux questions
  - Qui, Quoi, Comment?



# L'investigation numérique

- Documenter une action en justice
- Respecter des procédures strictes
  - Authenticité
  - Fiabilité
  - Intégrité





# Pour qui ?

- Équipes sécurité des entreprises
- Enquêteurs & experts judiciaires
- Consultants en sécurité
- Étudiants

# Processus

## Acquisition

Supports : Disques Durs, Mémoires Flash, RAM, ...

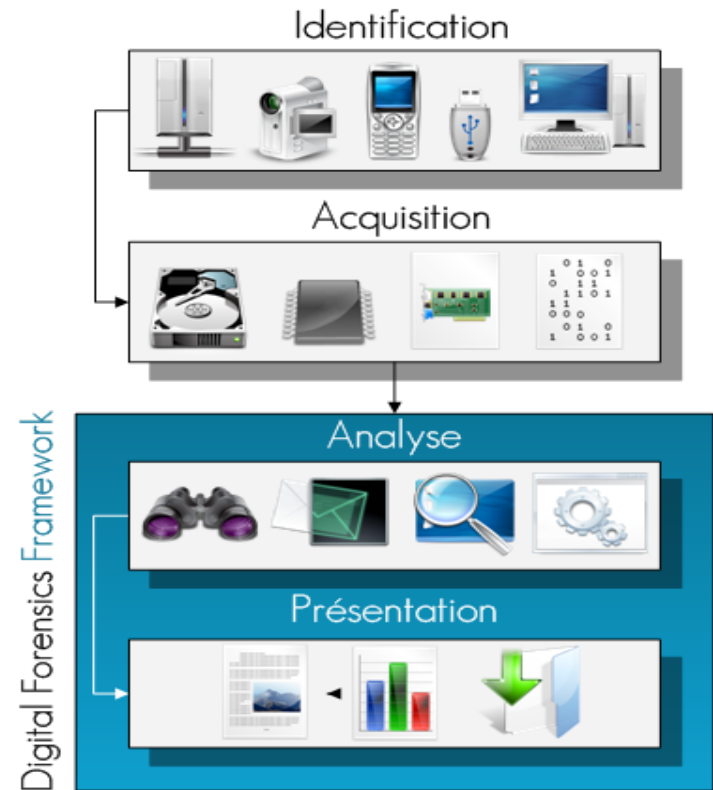
- Copies (Analyses mortes)
- Périphériques (Analyses “live”)

## Analyse

- Système de fichiers, Mémoire, Machine virtuelle, Métadonnées, Base de registres, logs, ...

## Présentation

- Extraction des données
- Génération de rapports



# Les logiciels propriétaires

1982

- Norton Utilities (undelete)

1995

- X-Ways WinHex

1997

- Guidance Software rachète ASR Expert Witness
- Encase

2001

- Access Data Forensic Tool Kit



# Les logiciels libres

1999

- TCT ( Dan Farmer & Wietse Venema)

2001

- TCT devient SleuthKit (Brian Carrier)

2005

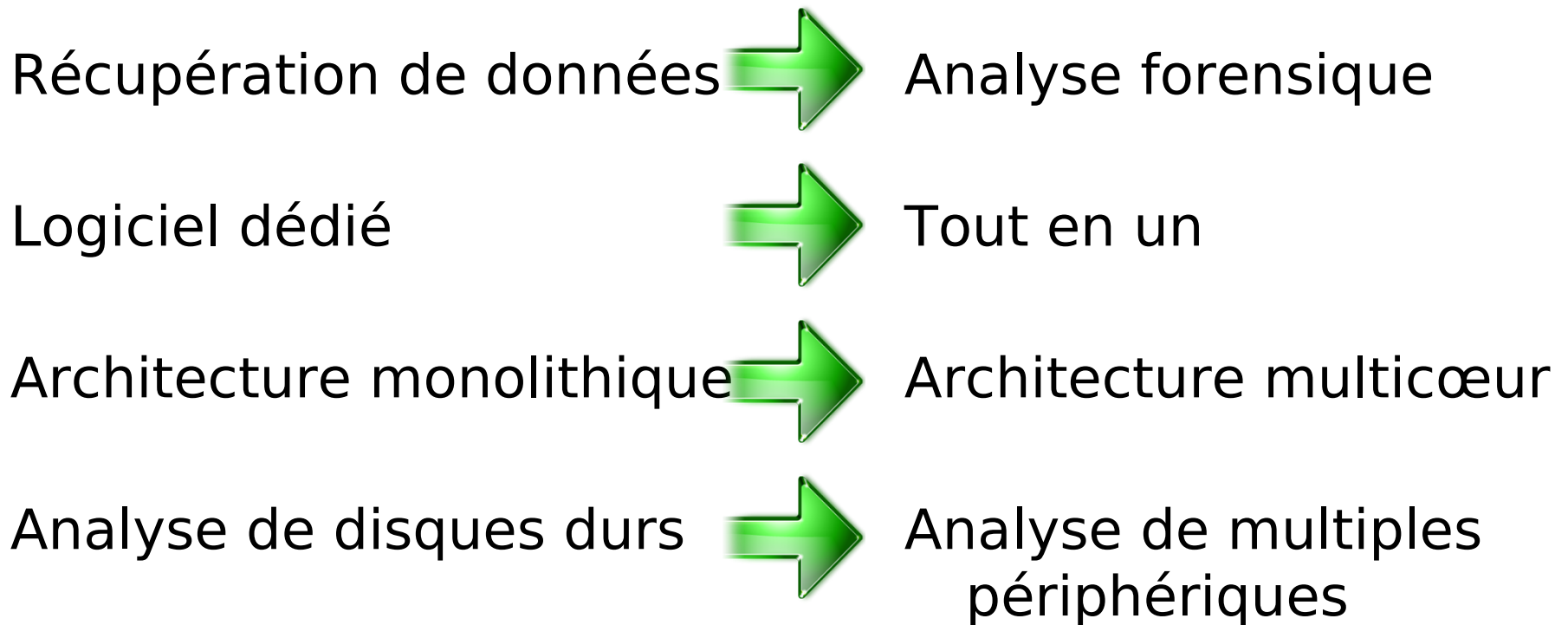
- PyFlag (Michael Cohen)

2007

- Digital Forensics Framework (ArxSys)



# L'évolution des logiciels



# Open Source Vs Propriétaire

Idée reçue : Le code ouvert permet de contourner plus facilement les logiciels

# Open Source Vs Propriétaire

Idée reçue : Le code ouvert permet de contourner plus facilement les logiciels 

## Conférence Black Hat 2007

Breaking Forensics Software: Weaknesses in Critical Evidence Collection' (ISSEC Partners)

Utilisation d'injections de données aléatoires pour trouver des failles

*'The software and methods for testing the quality of forensic software should be public.'*

# Open Source Vs Propriétaire

Idée reçue : Les logiciels propriétaires sont entièrement développés en interne

# Open Source Vs Propriétaire

Idée reçue : Les logiciels propriétaires sont entièrement développés en interne



Les logiciels propriétaire contiennent du code ouvert sous licences : LGPL ? BSD ? GPL ?

*Exemples : e-mails, OCR, ...*

Certaines fonctionnalités sont développées par d'autres sociétés

*Exemples : indexation, analyse d'images, ...*

# Open Source Vs Propriétaire

Idée reçue : La R&D et les brevets donnent un avantage aux logiciels propriétaires

# Open Source Vs Propriétaire

Idée reçue : La R&D et brevets donnent un avantage aux logiciels propriétaires



- Les éditeurs de logiciels propriétaires protègent leurs licences par des 'dongles'
- Pas de brevets logiciels en Europe
- La recherche est faite par des indépendants (Ex: DFRWS)
- Les éditeurs propriétaires s'inspirent de la recherche indépendantes ( Analyse mémoire, téléphone )
- Pas de réelles innovations fournies par les éditeurs propriétaires

# Open Source Vs Propriétaire

Les logiciels propriétaires sont utilisables devant une cour de justice (aux États-Unis)

- Pourtant le cas 'Daubert v. Merrell Dow Pharmaceuticals in 1993' désigne ces 4 points :
  - Has the scientific theory or technique been empirically tested; or, is it falsifiable
  - Has the theory or technique been subjected to peer review and publication?
  - What is the known or potential error rate?
  - Is the theory or technique generally accepted within the relevant scientific community?

# Les besoins professionnels

Support technique

Plateformes supportées (Windows)

Formation & certifications

Pérennité



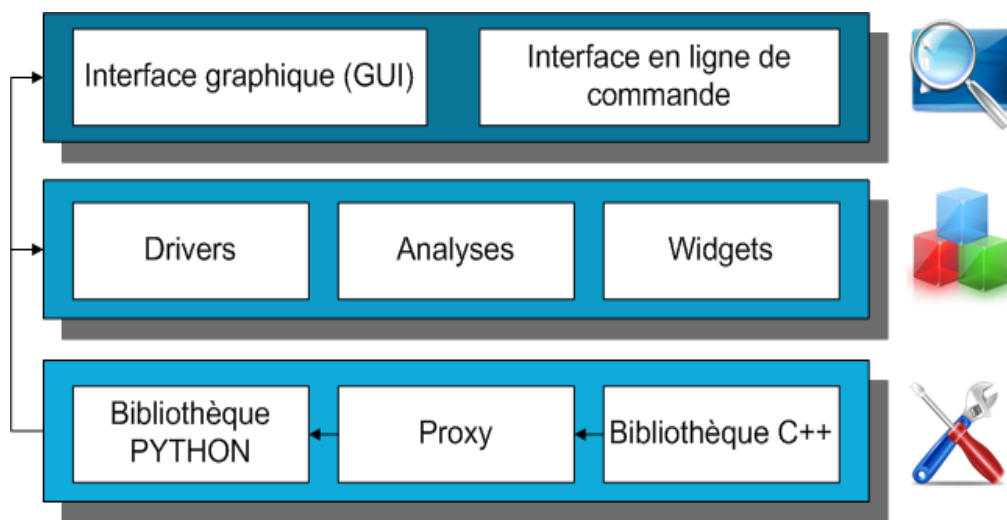
# Tour d'horizon technologique

- Framework orienté objet
- Développé en Python et C++
- Interconnexion des langages via swig
- Interface Utilisateur Graphique en PyQt
- Chaîne de compilation avec Cmake

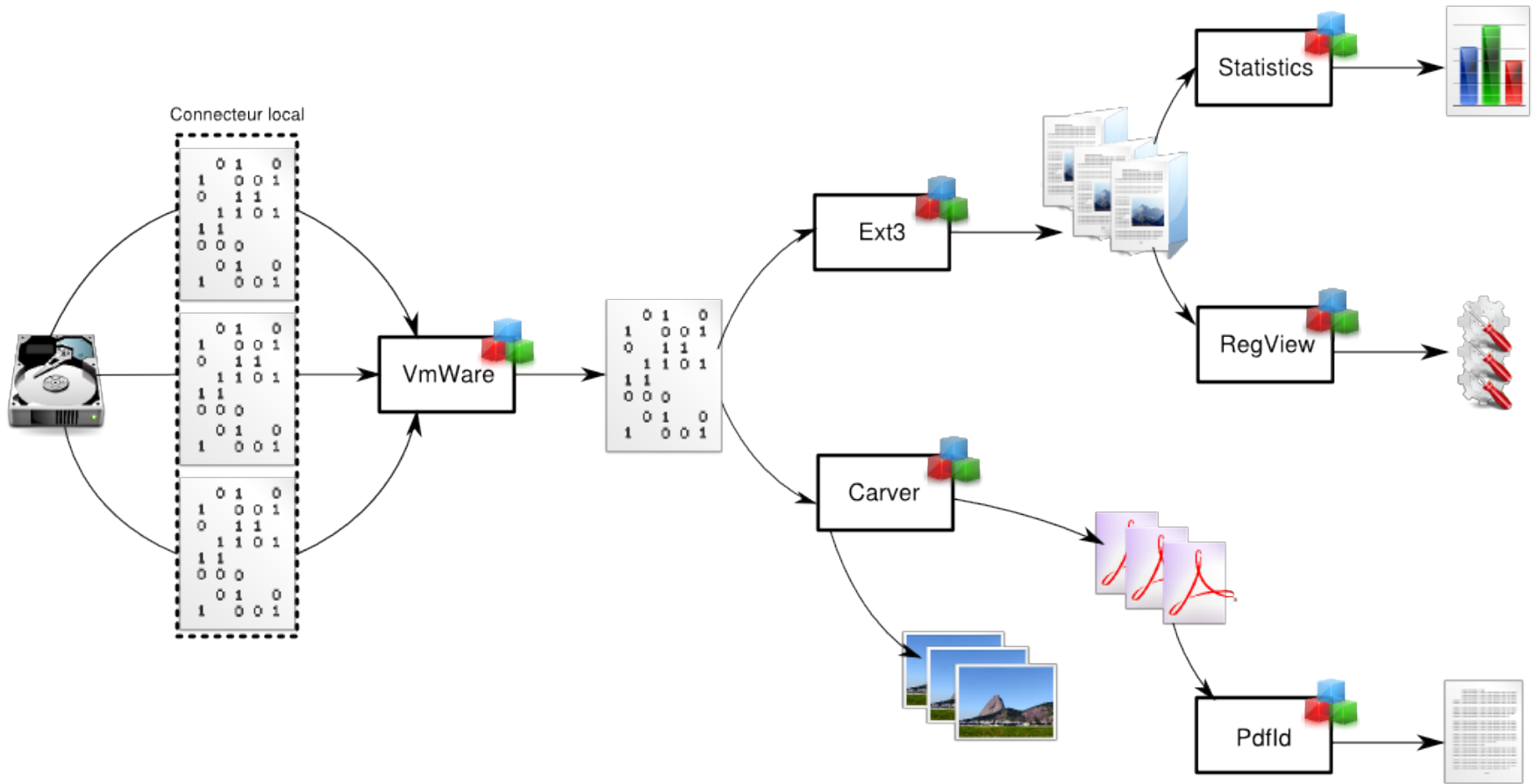


## Une architecture moderne

- Ouverte
- Modulaire
- Automatisable
- Portable
- Multiplateforme



# Une architecture moderne



# Une communauté active

- Plus de 20 000 téléchargements
- Une communauté internationale d'utilisateurs
  - Chercheurs / universitaires
  - Professionnels de la sécurité
  - Enquêteurs
- Des contributeurs actifs
  - Thèses universitaires
- Participe à l'évolution et à l'amélioration de DFF



# Démonstration

Notre philosophie : Apporter un savoir-faire et une expertise plutôt qu'un droit d'usage sur un logiciel

Support professionnel

Formation

Conseil et ingénierie

# Questions ?



@ : Solal.jacob@arxsys.fr

Tel : 01 46 36 25 22

[www.arxsys.fr](http://www.arxsys.fr)

[www.digital-forensic.org](http://www.digital-forensic.org)