ArxSys

About this presentation :

- Learning : What is Digital Forensics ?
- Political : Digital Forensics and Open Sources licensing
- Tool time : Digital Forensics Framework

Presented by Solal Jacob core dev. of DFF and CEO @ArxSys

What's Digital Forensics ?

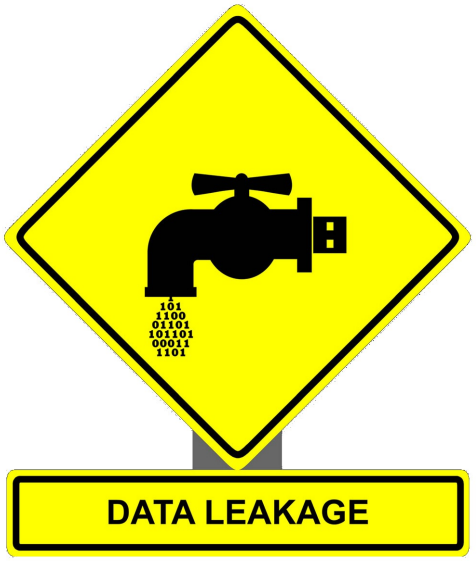
ArxSys

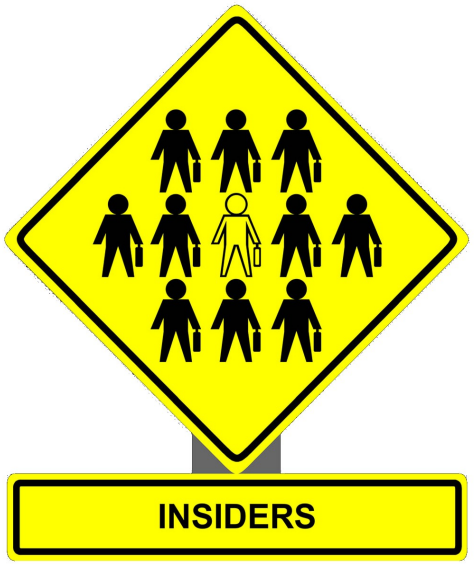
Forensics : from latin *forensis : forum.* Belonging to, used or adapted to trial or public debate.

Usage of Science or technologies during an investigation in order to establish evidences that can be receivable in a court.

When use it

ArxSys





Who use it ?

CERT

Law Enforcement

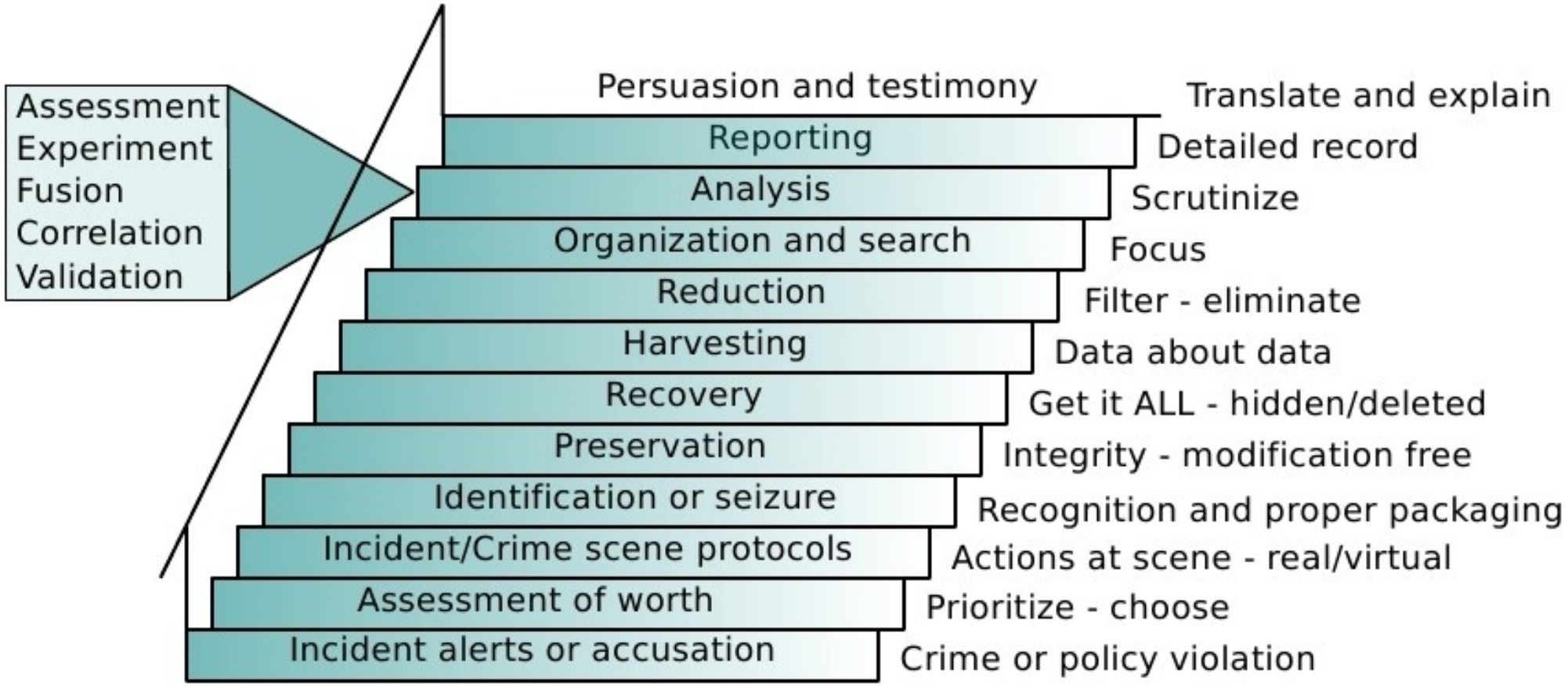
Expert

Student

The goal

ArxSys

Processes

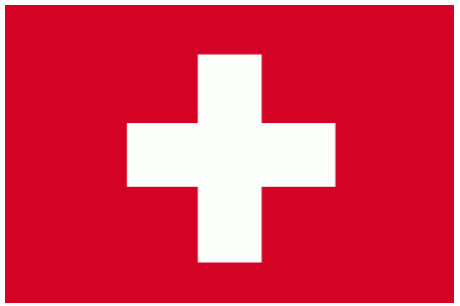


Mostly:

Identification → Acquisition → Analysis → Reporting

Reliability of evidence

Traceability



Neutrality

Software evolution

ArxSys

- **1982**
  - Norton Utilities (undelete)
- **1995**
  - X-Ways WinHex
- **1997**
  - Guidance Software rachète ASR Expert Witness
  - Encase
- **2001**
  - Access Data Forensic Tool Kit

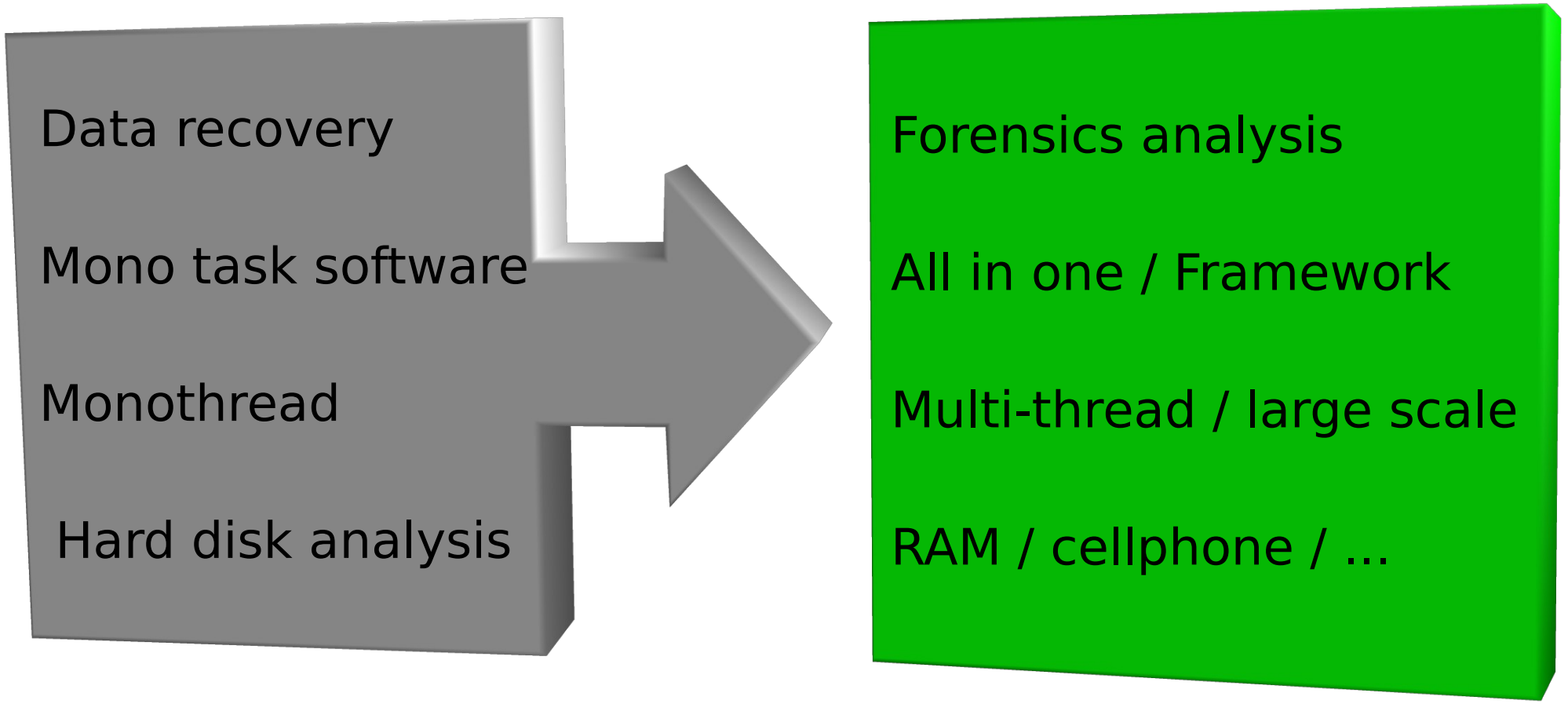
Software evolution

ArxSys

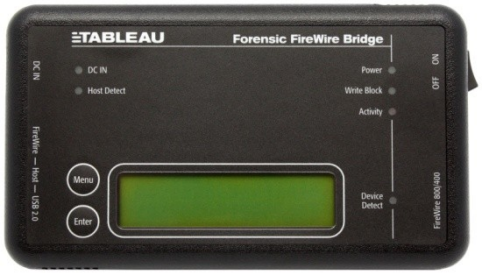
- 1999 · TCT (Dan Farmer & Wietse Venema)
- 2001 · TCT devient SleuthKit (Brian Carrier)
- 2005 · PyFlag (Michael Cohen)
- 2007 · Digital Forensics Framework (ArxSys)

Software evolution : Sum up

ArxSys



Hardware (Acquisition)



Open Source Digital Forensics

ArxSys

Open source digital forensics

ArxSys

Misconception : Criminal have access to source code so they can protect themselves more easily.

Open source digital forensics

ArxSys

Misconception : Criminal have access to source code so they can protect themselves more easily.

Black Hat 2007 :

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

Usage of fuzzing to exploit software bugs.

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

Open source digital forensics

ArxSys

Misconception : Criminal have access to source code so they can protect themselves more easily.

All of the closed source tools use some open-source code (LGPL, BSD, GPL ?), to handle outlook format, OCR, ...

Open source digital forensics

ArxSys

Problem : Closed source software are admissible in court (in USA) not open-source one.

Open source digital forensics

ArxSys

Problem : Closed source software are admissible in court (in USA) not open-source ones

Frye VS the United States

The court had to decide the admissibility of a polygraph test as evidence.

“Testimony given by an expert must have a scientific basis that is established and accepted”

Open source digital forensics

ArxSys

Problem : Closed source software are admissible in court (in USA) not open-source one

Daubert v. Merrell Dow Pharmaceuticals in 1993

- 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?

Tool time

ArxSys

DFF

digital forensics framework

In

No

You can

It

Tool time

ArxSys

DFF

digital forensics framework

In

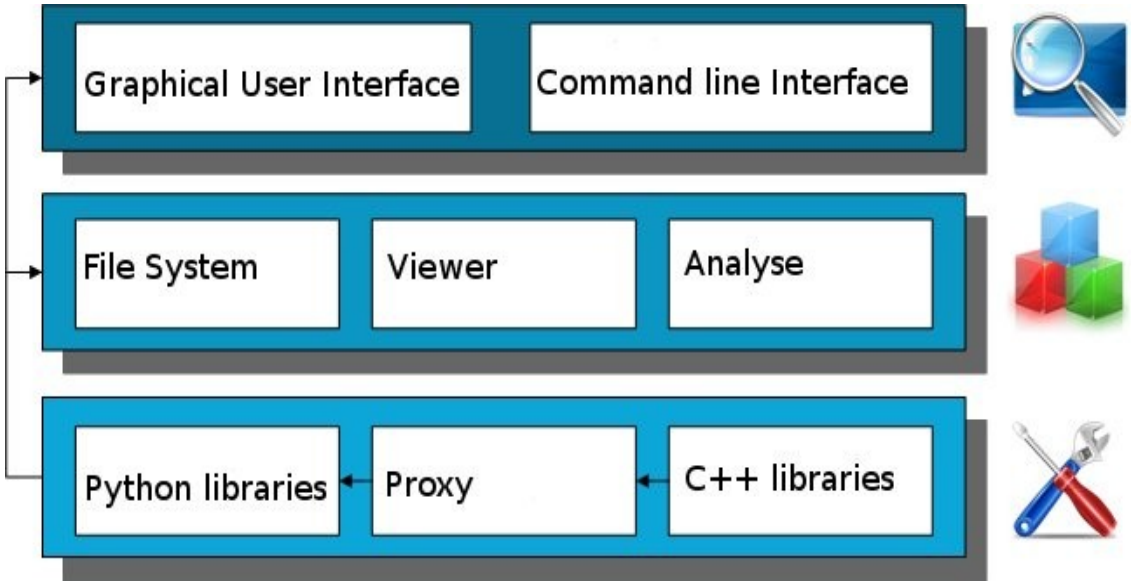
No

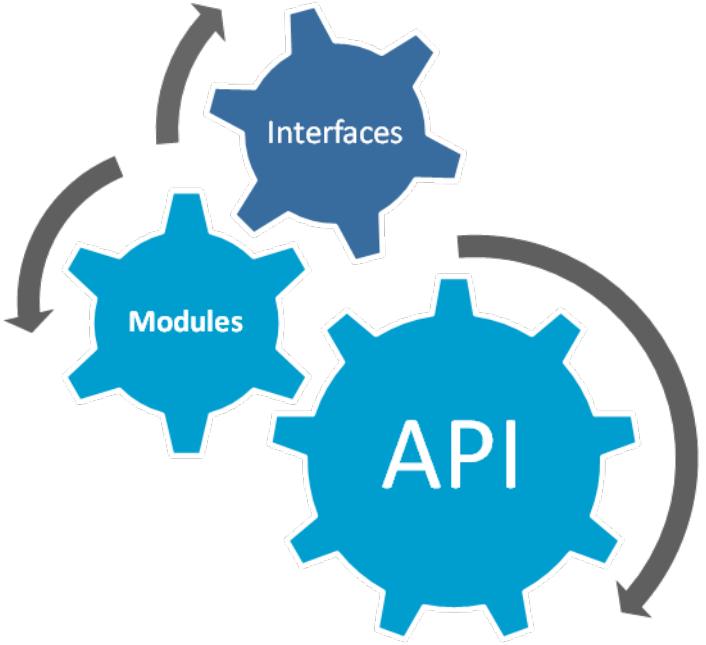
You can

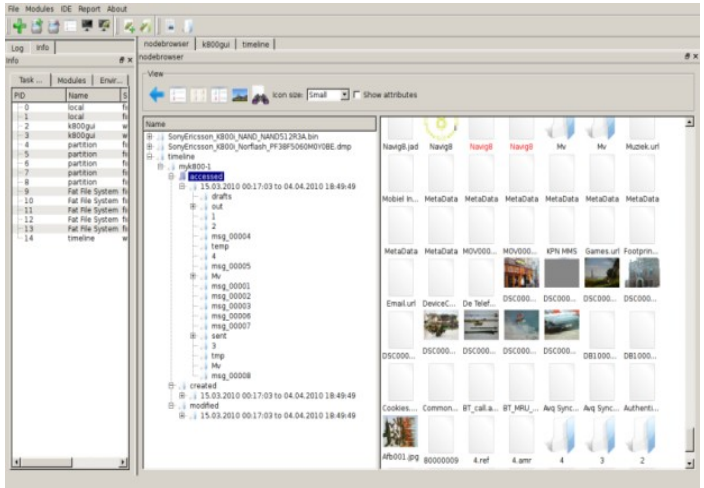
It

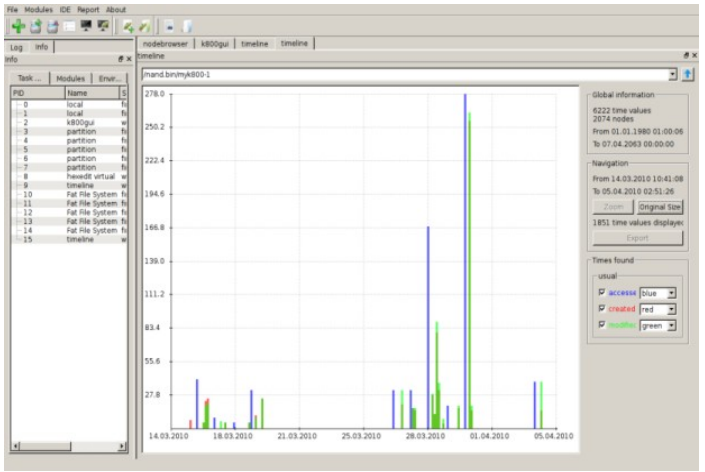
Digital Forensics Framework

ArxSys





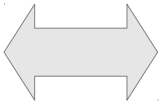


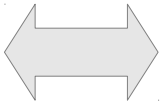


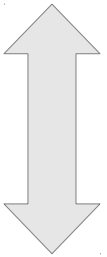
```
dff / >
information     : fileinfo      statistics
search          : carver        find
builtins        : load          cd              show_cwd        show_db         ls
help            : man
viewer          : hexedit       player          viewerimage     bindiff         cat
parser          : volatility
shared memory   : touch         shm
crypto          : unxor
mobile          : smsdecode
file system     : local         partition       fatfs
hash            : hash          hdatabase
process         : extract       post_process    eval            batch
Integrity       : integrity
archive         : unzip
dff / >
```

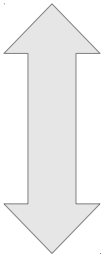
DFF : Software component

ArxSys



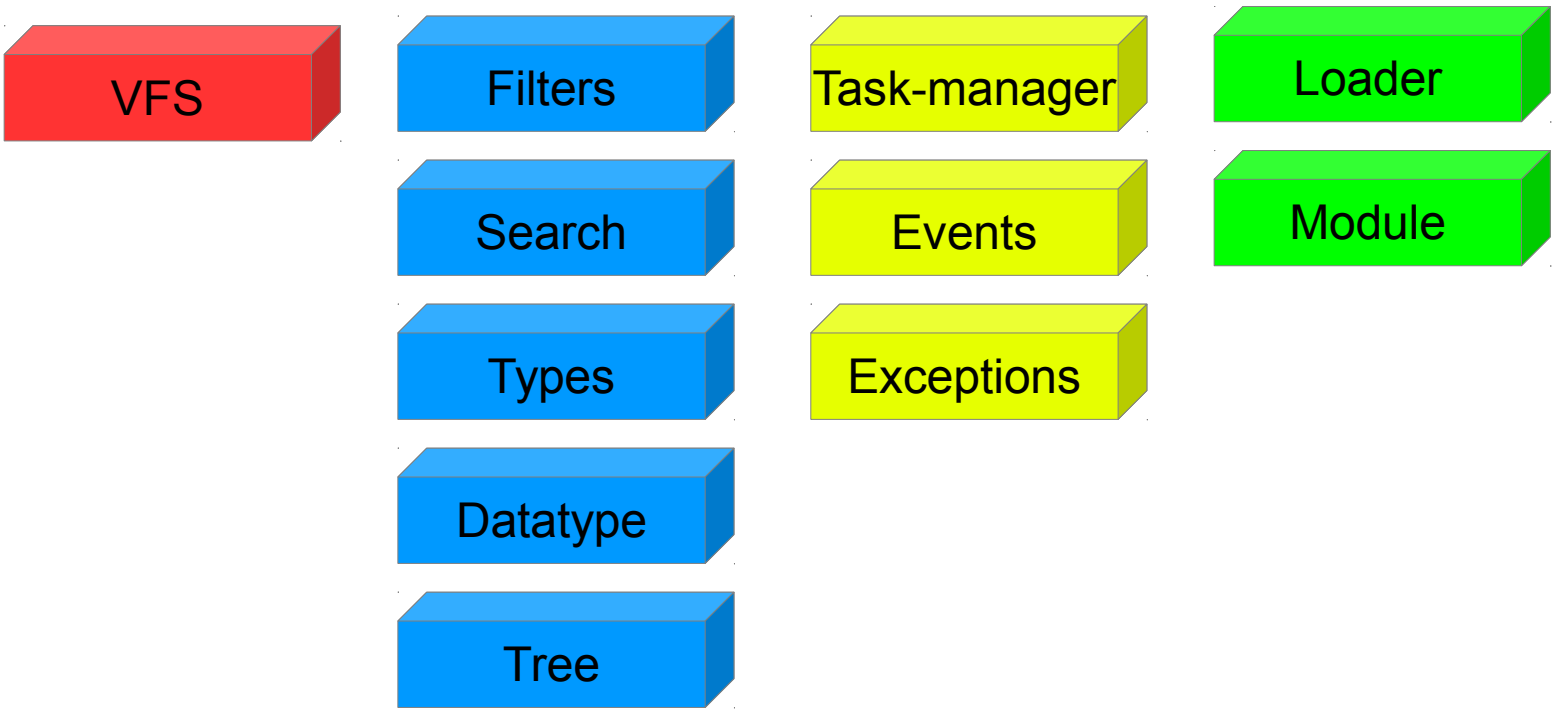






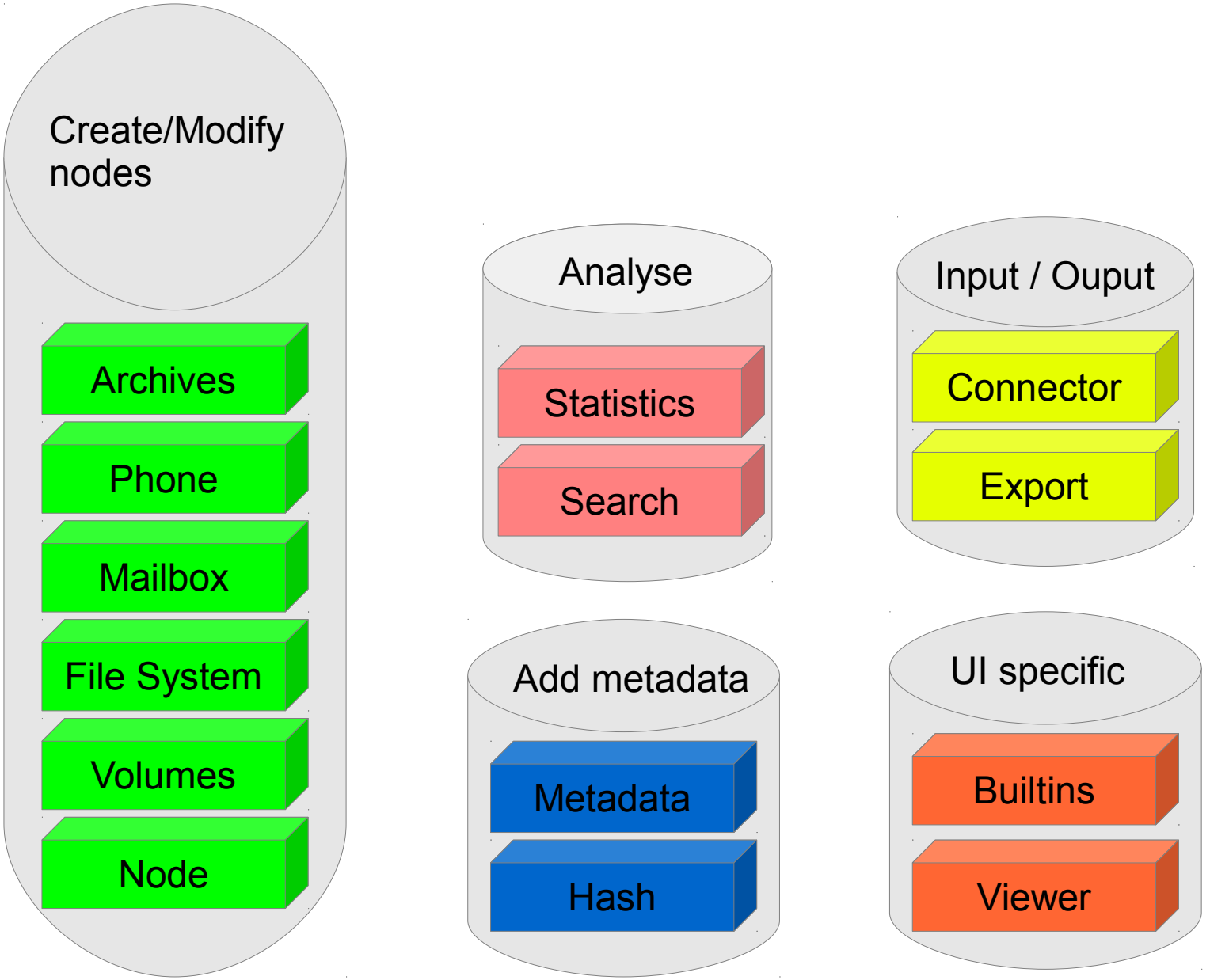
DFF : API Libraries

ArxSys



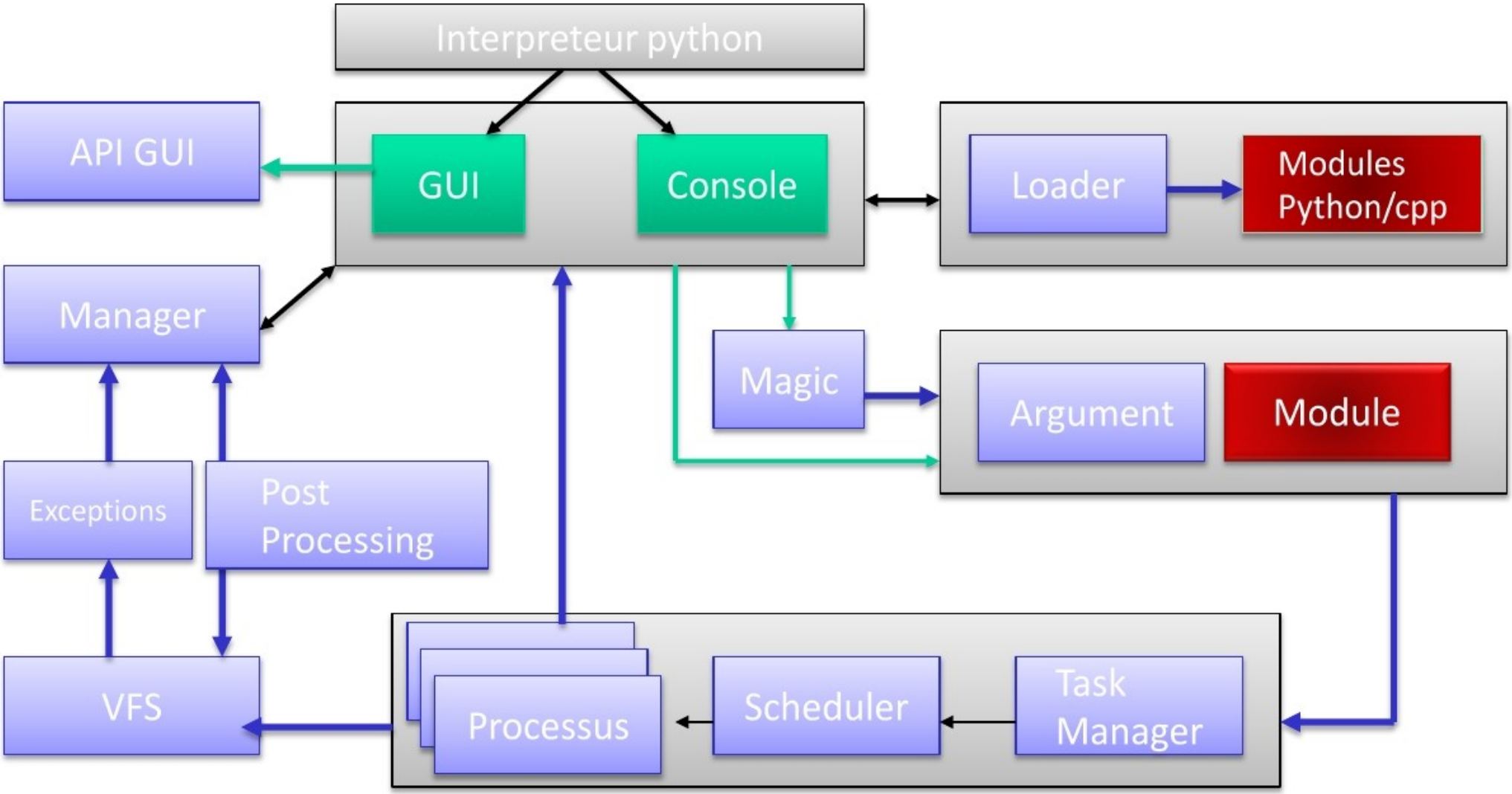
DFF : Modules Tags

ArxSys

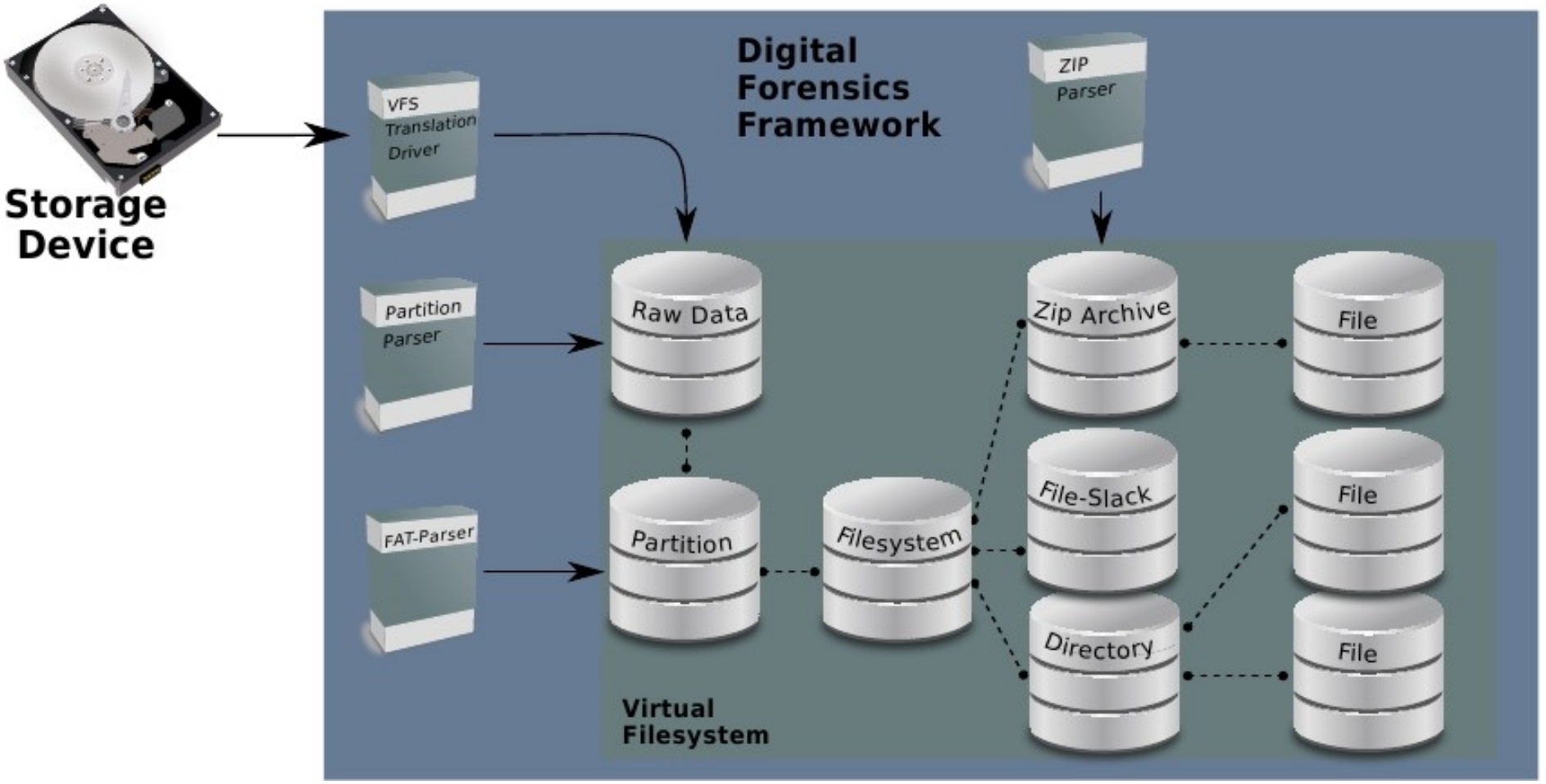


DFF : Module execution

ArxSys

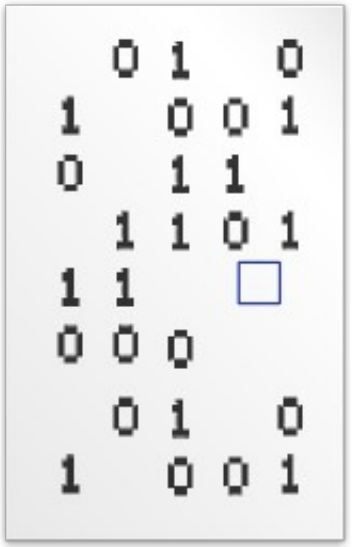


DFF API : Stacked VFS



DFF : Virtual Mapping

dump.dd



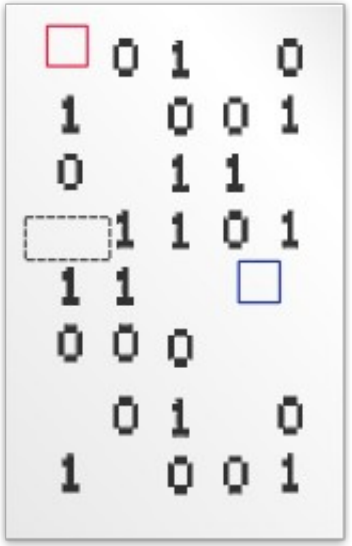
foo.bar

1) push(0, 512, dump.dd, 12348745)

DFF : Virtual Mapping

ArxSys

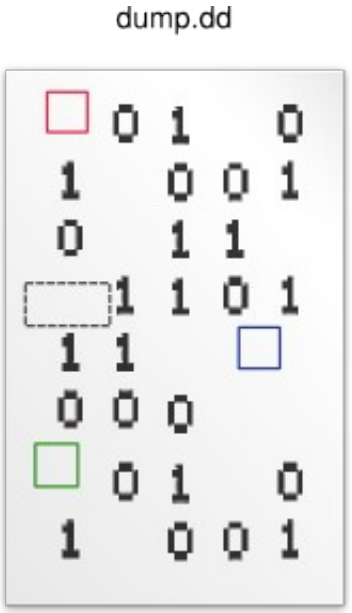
dump.dd



foo.bar

1) push(0, 512, dump.dd, 12348745)
2) push(512, 512, dump.dd, 10240)

DFF : Virtual Mapping



1) push(0, 512, dump.dd, 12348745)

2) push(512, 512, dump.dd, 10240)

N) push(1310720, 42, dump.dd, 4965478)

End

ArxSys

Don't forget tomorrow there is a two hours workshop :
“Being an investigator” : solving a digital crime with DFF
(14h00 / 2 A.M. / 0xe @ H211)

Please install DFF 1.3 before coming
(Not all modules are needed if it can run it's ok :)

Web site : http://www.digital-forensic.org
IRC : #digital-forensic / freenode

Tracker : http://tracker.digital-forensic.org
Wiki : http://wiki.digital-forensic.org
Git : http://git.digital-forensic.org

Professional Support : http://www.arxsys.fr