

# META MERIANAE

Analyse Criminelle Informatique

Modélisation, automatisation et restitution



SSTIC 2004

02 Juin 2004

Thomas «DomTom» DUVAL [thomas.duval@supelec.fr](mailto:thomas.duval@supelec.fr)

Bernard JOUGA [bernard.jouga@supelec.fr](mailto:bernard.jouga@supelec.fr)

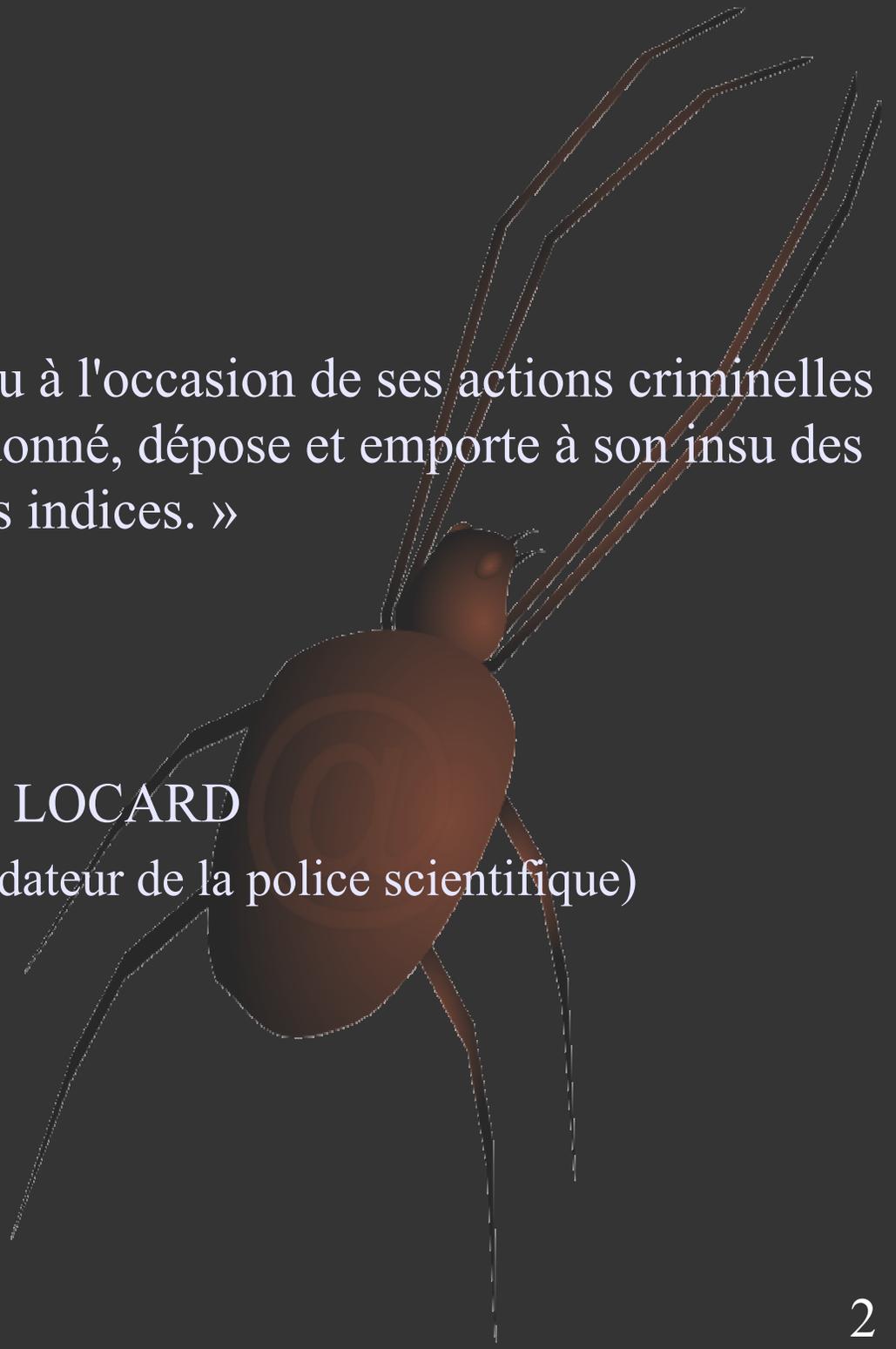
Laurent ROGER [roger@celar.fr](mailto:roger@celar.fr)

# Introduction

« Tout individu à l'occasion de ses actions criminelles en un lieu donné, dépose et emporte à son insu des traces et des indices. »



Edmond LOCARD  
(père fondateur de la police scientifique)  
1910



# Forensics

## Objectifs



**Déterminer les dégats et les attaques**

**Réparer les dégats**

**Trouver l'auteur des faits**



# Forensics

## Méthodes



Analyse des variables éphémères



Analyse de la topologie réseau



Analyse des fichiers d'audit



Analyse du système (fichiers cachés / supprimés)



Analyse de la composante humaine

# Forensics

Remarques



Sonner l'alarme



« Pull the plug ! »



pour arrêter l'attaquant

pour garder les preuves intacts

# Méthodologie

## Introduction

### Objectifs :

- ❗ Aider les enquêteurs dans leurs investigations
  - ⚠ sur les attaques
  - ⚠ sur les attaquants (profils)

### Méthodes :

- ❗ Sous la forme d'un système expert
- ❗ Utilisant les Réseaux Bayésiens pour l'inférence



# Méthodologie

# Attaques

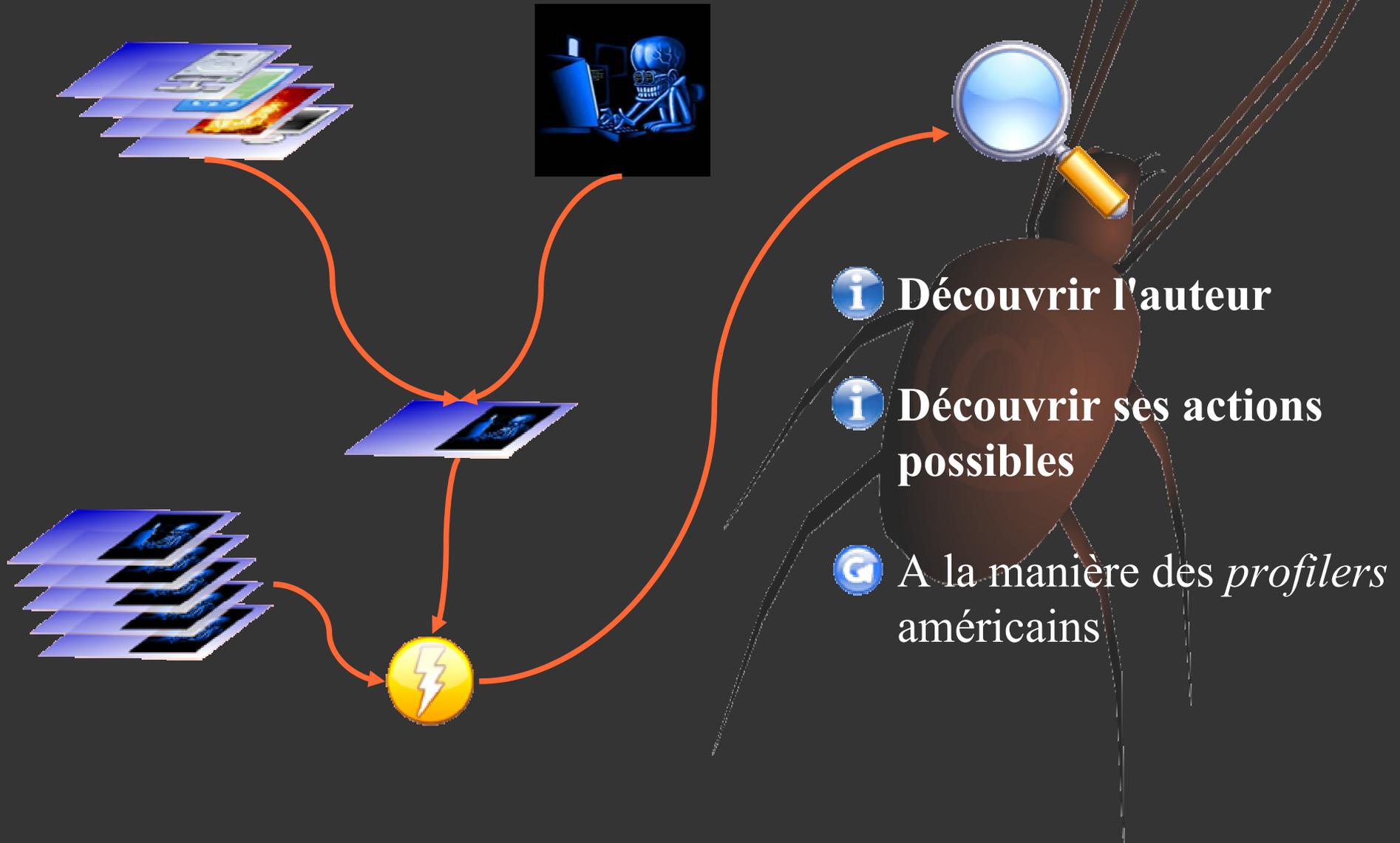


1 plan =  
1 attaque  
1 composant



# Méthodologie

## Attaquants



# Méthodologie

## Travaux en cours

The screenshot shows the XMeta software interface. The title bar reads "XMeta Inquiry num: system@127.0.0.1". The menu bar includes "New", "Edit", "Link", "Configure", "Delete", "Search", "Exit", "Save this Plan", and "Help". The main window is titled "System@127.0.0.1 Attack Source Address:" and has radio buttons for "local", "intern", "extern", and "Unknown".

**WHERE**

station  server  commut  pda  storage  net

Type of Equipment: server windows

web  tx  apache  iis  other  no  
syst  linux  windows  other  no  
sec

util\_res N/A   
back\_door N/A   
ids N/A   
serv\_def http   
no\_serv N/A   
dos N/A   
supp N/A   
conf\_data N/A   
scan yes   
illegal\_data N/A   
seg\_fault N/A

**WHAT**

diversion (94.6%)  decrypt (91.7%)  bounce (91.9%)  repeat (88.2%)  
 net\_listen (86.0%)  intercept (90.3%)  troyen (77.9%)  intercept\_block (76.2%)  
 broadcast (68.5%)  bypass (76.4%)  parasit (74.1%)  overrun (73.0%)  
 chaff (65.8%)  yp (42.3%)  blocking (69.6%)  degrad (100.0%)  
 brut\_force (100.0%)  listen (58.3%)  embezzlement (57.4%)  usurp (100.0%)  
 exploit (100.0%)

encrypt (95.1%)  invert\_trap (92.8%)  trap (92.3%)  del (86.6%)  
 login\_inst (79.2%)  cmx\_illic (100.0%)  infection (78.2%)  attribute (78.1%)  
 inhib\_detect (93.8%)  scan\_use (68.0%)  hidden\_channel (54.1%)  msg (61.7%)

**HOW**

What you would do :

comm (85.1%)  check\_net (80.8%)  topo\_int (88.9%)  
 topo\_ext (100.0%)  physic (74.4%)  check\_syst (100.0%)  
 log\_net (65.1%)  var\_syst (100.0%)  image (73.9%)  
 retrieve (89.5%)

JAVA

API BNJ

BIF

CFXR

# Travaux futurs

- ➔ Gestion des profils
- ➔ Etude des techniques de comparaison de RB
- ➔ Exploitation des bases de vulnérabilités
- 🔍 Travail sur des données réelles (avec la DGA)





SSTIC 2004  
02 Juin 2004

# QUESTIONS ?

<http://www.rennes.supelec.fr/ren/perso/tduval/>

Thomas «DomTom» DUVAL [thomas.duval@supelec.fr](mailto:thomas.duval@supelec.fr)

Bernard JOUGA [bernard.jouga@supelec.fr](mailto:bernard.jouga@supelec.fr)

Laurent ROGER [roger@celar.fr](mailto:roger@celar.fr)