heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

Tél. : 024 557 63 30
Fax : 024 557 64 04

info@heig-vd.ch
http://www.heig-vd.ch

Travail de diplôme 2005

Département Electricité et Informatique

HEIG-VD
Route de Cheseaux 1
CH - 1401 Yverdon-les-Bains

Les sciences forensiques ("forensics") dans Windows

Contexte

Aujourd'hui, les développements dans la technologie de l'information posent de nouveaux défis pour le maintien de l'ordre. De plus en plus, la technologie de l'information devient un instrument de l'activité criminelle. C'est pourquoi la profession de policier doit être constamment adaptée à ce monde numérique en constante évolution.

Lorsque l'analyse d'un ordinateur doit être effectuée, des spécialistes en informatique forensique disposent d'outils particuliers et d'un mode opératoire défini pour extraire des preuves depuis les traces numériques saisies.

Les sciences forensiques se définissent comme l'ensemble des principes scientifiques et des méthodes techniques appliqués à l'investigation criminelle, pour prouver l'existence d'un crime et aider la justice à déterminer l'identité de l'auteur et son mode opératoire.

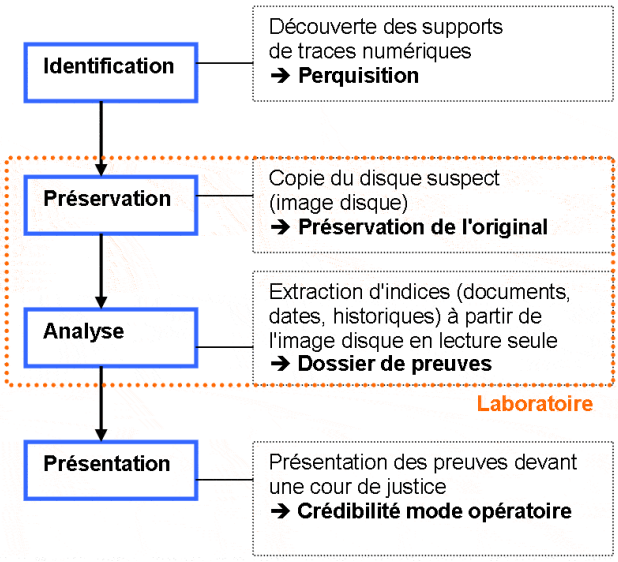
Motivation

Les sciences forensiques appliquées à Windows permettent la recherche de la preuve informatique.

Ce travail de diplôme se préoccupe principalement de l'analyse d'un ordinateur éteint (dite analyse à froid) grâce à des outils gratuits, sous licence GPL.

L'objectif est la création d'un laboratoire qui sensibilise les étudiants à l'analyse forensique. Elle permet de présenter des preuves à partir de traces de navigation Internet, d'échanges de courriers électroniques, de fichiers dissimulés et même effacés.

Mode opératoire



Auteur: **Alexandre DELEZ**
Prof. responsable: **Christian BUCHS**
Sujet proposé par: **Christian BUCHS**

Hes·so
Haute Ecole Spécialisée de Suisse occidentale