

République Algérienne ~~Démocratique~~ et Populaire

**Centre de Recherche sur l'Information
Scientifique et Technique**

- CERIST -

*Mémoire pour l'obtention du Diplôme de post graduation
spécialisée en sécurité informatique*

Thème

Computer Forensic

(Investigation légale des ordinateurs)

P méthodes et II

Propose et dirige par :

Mr M. Halim KHELALFA

Elaboré Par :

M^r Noureddine MILOUDI.
M^r Ahcen OUBAD

Devant le jury :

Mme LOUNI Sakina	Presidente
Mme BENMEZIANE Souad	Examinatrice
Mr TANDJAOUI Djamel	Examineur
Mr KARA Directeur des etudes DGSN	(invite)
M. KHELALFA Halim	Promoteur

Juin 2002

Remerciements

Nous tenons à exprimer notre vive gratitude a notre promoteur Mr KHELALFA pour l'intérêt porté a ce travail et surtout pour sa lecture pointilleuse de ce document, sans oublier de remercier tout le staff du CERIST (enseignements et responsables) en particulier la sympathique Melle Houria ZAIDI chef de service formation et relations extérieurs qui avec son sourire a toujours été presente et disponible.

Ahcene et Nouredine

Dedicates

A kinane ...

NourEddine

A Karima ma femme
Et
Meriem ma fille

Ahcene

PARTIE 1 : Investigation légale

CHAPITRE I :	Definitions
INTRODUCTION	1
I.1-Crime, fraude : Définitions	2
I.1.1- Fraude : 1 ^{ère} définition	2
I.1.2- Fraude : 2 ^{ème} définition	2
I.2- L'expérience Américaine	2
I.2.1- Crime informatique	2
I.2.2- Quelques chiffres	3
I.3- L'expérience Française	4
I.3.1- Infractions de droit commun	5
I.3.2- Infractions spécifiques à la contrefaçon	5
I.3.3-Infractions qui portent atteinte à la vie privée	5
I.3.3.1- Intrusion	5
I.3.3.2- Les atteintes à l'intégrité du système	5
I.3.3.3- L'entrave au système	6
I.3.3.4- Fausser le fonctionnement du système	6
I.3.3.5- Les atteintes aux données	6
I.3.3.6- Associations de malfaiteurs	6

CHAPITRE II :	Preuves
II.1- Introduction	7
II.2- Définition De La Preuve	7
II.3- Types De Preuves	8
II.4- Règles De Preuve	9
II.4.1- La meilleure preuve(best evidence)	9
II.4.2- Preuve rejetée	10
II.4.3- Règle de oui-dire(herasay rule)	10
II.5- Témoignage D'experts	11
II.5.1- Qu'est ce qu'un expert ?	11
II.5.2- En quoi un expert est-il différent ?	11
II.5.3- catégories d'experts	11
II.6- Chaîne De La Preuve Irréfutable	11
II.7- Recevabilité De La Preuve	12
II.7.1- Cas pratique	13
II.8- Cycle De Vie De La Preuve	13
II.8.1- Recueil et identification	14
II.8.2- Sécurisation	14
II.8.3- Présentation devant un tribunal	15
II.8.4- Restitution	15

CHAPITRE III :**Conduire une Procédure d'Investigation**

III.1- Poursuite Judiciaire	16
III.1.1-Poursuite suivant le droit Criminel	16
III.1.2-Poursuite suivant le droit Civil	16
III.1.3-Poursuite suivant le droit contractuel	16
III.2- Entamer Des Poursuites Judiciaires Ou Pas ?	17
III.3- L'équipe Et Le Plan	19
III.4- Détection	19
III.5- Investigation Préliminaire	20
III.6-Faut-il divulguer ?	20
III.7- Qui Doit Conduire L'investigation ?	21
III.8- Méthodologie à suivre pour mener une investigation	21
III.8.1- Identifier le type de système	21
III.8.2- Constituer l'équipe de recherche et de saisie	22
III.8.2.1- Obtenir un mandat de perquisition	22
III.8.3- Le système est-il encore en risque ?	22
III.9- Exécution Du Plan	22
III.10- Autres Eléments A Prendre En Compte	23
III.11- Surveillance	24
III.12- Autre Source D'information	25
III.13- Etablir Des Rapports D'investigation	25

CHAPITRE IV :**Investigation légale des ordinateurs**

IV.1- Introduction	26
IV.2- Définition De L'investigation Légale D'un Ordinateur	26
IV.3- Accès Aux Données D'un Ordinateur	26
IV.4- Types De Données Résidents Sur Un Ordinateur	26
IV.5- Autres Informations Pouvant Etre Découvertes Dans Un Ordinateur	27
IV.6- Processus D'investigation	28
IV.6.1- Précautions à prendre avant l'analyse	28
IV.6.2- L'analyse	29
IV.6.3- Analyser le système	30
IV.6.4- reconstruire le système du suspect	32
IV.6.5- Restaurer et analyser	32
IV.6.6- Notes et rappels	32
IV.7- Cas Pratiques Selon IACIS®	33
IV.7.1- Examen complet du disque dur	33
IV.7.2- Les imitations de l'examen complet	34

PARTIE II : Investigation technique

CHAPITRE I :

Principes

I.1- Acteurs	35
I.2- Considérations Informatiques	35
I.2.1- La micro-informatique	36
I.2.2- Clone ou originale ?	36
I.3- Considérations De Préservations De La Preuve	36
I.3.1- Fragilité de la preuve informatique	36
I.3.2- La copie 'Bitstream' comme principe d'investigation	37
I.4- Considérations légales de présentation de la preuve devant un tribunal	37
I.5- Considérations cyber espace et coopération internationale	38
I.6- L'Internet Est Partout Et Instantané	38
I.7- Vie Privée	38

CHAPITRE II :

Enquêtes Digitale

II.1- Le Temps	40
II.2- Systèmes Echappant A La Compréhension Des Responsables	40
II.3- Le Système Informatique Vie Et Evolue	40
II.4- Les Attaques Internes	41
II.5- Détective Digital	41
II.6- les fichiers logs	41
II.7- Complexité des systèmes	42
II.7.1- Exemple de déroulement d'une commande	42
II.8- Niveau D'abstraction Et Visibilité	43
II.9- Plus Difficile D'effacer	45
II.10- Qu'est ce qui s'exécute sur notre machine ?	45
II.11- Fréquence d'utilisation	46
II.12- L'effet 'ZERO'	46
II.13- Système de contrôle d'accès	47
II.14- Slack Files Ou Espaces Résiduels	47
II.15- Mots De Passe	48
II.16- Cryptographie	48
II.17- Stéganographie	49

III.1- Introduction	51
III.2- Fonctionnement de Mactimes	51
III.3- Suivre L'activite Ou Systeme	52
III.4- Action a posteriori	53
III.5- Precautions a prendre dans l'utilisation de Mactimes	54
III.6- MACTIME : un outil pour mieux connaître le système	54
III.7- Comment Mactime Devient Un Outil De Securite	55
III.8- Inconvenients de Mactimes	55
III.9- Conclusion	56

Récupération de Données**CHAPITRE IV :**

	57
IV.1- Introduction	58
IV.2- Aperçus sur le système de fichier Unix	59
IV.3- Outils de récupération	59
IV.3.1- Unrm	60
IV.3.2- Outils d'analyse Lazarus	60
IV.3.2.1- Principe s de lazarus	61
IV.4- Unerase sous Windows	62
IV.5- Commandes Unix	62
IV.6- Conclusion	

Processus**CHAPITRE V :**

	63
V.1- Processus : Commande De Base	63
V.2- Analyse avancée	64
V.3- Analyse du programme	65
V.3.1- Code et donnée	67
V.4- Analyse statique d'un programme	68
V.5- Reverse engineering	68
V.6- Simulation et machine virtuelle	69
V.7- Analyse dynamique d'un programme	69
V.7.1- Debug	69
V.7.2- Appel système	70
V.8- Conclusion : quelques questions	

Réseau**CHAPITRE VI :**

	71
VI.1- un réseau sécurisé	71
VI.2- Niveaux d'investigation	71
VI.3- L'instrumentation de système de base	72
VI.4- L'instrumentation avancée du système	72
VI.5- L'instrumentation extrêmes du système	72
VI.6- LAN est un élément de transport et non pas de stockage	73
VI.7- Préparer un réseau	73
VI.7.1- Outil : Cisco NetFlows	73
VI.7.2- Sniffer sur un réseau	74
VI.8- Etape finale : modifier infrastructure	73
VI.9- Conclusion : réseaux et machine hote	

Conclusion générale

	75
synthèse	75
Partie 1	75
Les lois	75
Systèmes d'information	75
Les utilisateurs en tant qu'acteurs	75
Science sociale	76
Partie 2	76
Systèmes informatiques	76
Systèmes d'exploitation et application	76
Programmation système et langages de programmation	76

Securite informatique	77
Securite informatique et Computer Forensic	77
Distinction entre securite informatique et computer Forensic	77
En conclusion	79
Compromis	79
