République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université des sciences et de la technologie houari Boumediene

Faculté d'Electronique et d'Informatique

Département Informatique

Mémoire de Master

Option

Sécurité des systèmes informatiques

Thème

Analyseur de fichiers pour détecter des preuves numériques

Sujet proposé par :

M^r D.TANDJAOUI

M^me C.BENZAID

Présenté par :

M^elle AZZAZ Yasmine

M^elle ZANOUN Zehour

Soutenu le **22/06/2016**

Devant le jury composé de:

M^me BOUYAKOUB	Présidente
M^me BOUTOUHAMI	Membre

Binôme N°208/2016

Remerciements

Tout d'abord, nous tenons à remercier Dieu le tout puissant d'avoir éclairé notre chemin, de nous avoir accordé la force, le courage et toutes les bénéfices pour arriver à ce stade d'étude.

Nous adressons nos sincères remerciements et notre reconnaissance à nos Promoteurs Dr. TANDJAOUI Djamel et Dr. BENZAID Chafika d'avoir accepté de diriger ce travail et pour leurs aide et encouragements.

Nous présentons nos respects et remerciements à la présidente et à la membre du jury pour l'évaluation de ce travail.

Nous remercions Mr AYACHE pour le temps qu'il a consacré afin de nous aider et orienter durant la réalisation de ce projet. De même, on tient à remercier Mr KHALDI d'avoir répondu à nos questions pendant les recherches.

A tous les professeurs, pour leurs efforts afin de nous assurer une meilleure formation, à tous les responsables de l'USTHB et tous ceux qui ont contribué de près ou de loin à la réalisation de ce travail

Dédicace

A nos parents,

« Vous nous avez donné la force et le courage, tout ce qu'on peut vous offrir ne pourra pas exprimer l'amour et la reconnaissance qu'on vous porte. En témoignage, on tient à vous dédier ce modeste travail pour tous les sacrifices déployées pour nous élever dignement et assurer notre éducation dans les meilleures conditions »

« Que dieu vous préserve et vous procure une longue et heureuse vie »

A nos frères et sœurs,

« On vous remercie pour votre aide et assistance pendant la réalisation de ce travail, vous étiez toujours là pour nous supporter et encourager, merci »

A nos amis,

« Vous nous avez encouragé et soutenu aux moments difficiles, merci pour votre esprit collaboratif et fraternel, pour l'ambiance joyeuse que vous créez, on a passé des moments inoubliables, merci »

Sommaire

Introduction générale……1
I. Criminalité informatique et investigation numérique……3
I.1 Introduction……3
I.2 Cybercriminalité……3
I.3 Classification des cybercrimes……3
I.3.1 L'ordinateur ou le réseau est la cible……3
I.3.2 L'ordinateur ou le réseau est l'outil pour commettre le crime……6
I.4 Evolution de la cybercriminalité……7
I.5 La lutte contre la cybercriminalité……8
I.6 Investigation numérique……8
I.7 Computer Forensics……9
I.8 Information numérique……9
I.9 Preuve numérique……10
I.10 Méthodologie de l'investigation numérique……10
I.10.1 Phase d'identification……11
I.10.2 Phase d'acquisition (Collecte et préservation)……12
I.10.3 Phase d'analyse……13
I.10.4 Phase de présentation……14
I.11 Contrôle de la preuve numérique……14
I.11.1 Rapport de garde……14
I.11.2 Calcul de l'empreinte numérique……14
I.12 Les problèmes de la phase d'analyse……15
I.13 Boîte à outils……16
I.14 Conclusion……16
II Organisation du disque et systèmes de fichiers NTFS……17
II.1 Introduction……17
II.2 Organisation du disque dur……17
II.2.1 Structure physique du disque dur……17
II.2.2 Structure logique du disque dur……19
II.2.3 Organisation interne du disque dur……20
II.3 Système de fichiers NTFS (New Technology File System)……21
II.3.1 Historique……21
II.3.2 Caractéristiques……22
II.3.3 Structure interne……23
II.4 Master File Table……24
II.4.1 Les fichiers de métadonnées……25
II.4.2 Structure des entrées MFT……25
II.5 Les ADS (Alternate Data Stream)……32
II.6 Conclusion……33

III Conception de l'analyseur de fichiers……34
III.1 Introduction……...34
III.2 Motivation et objectifs……..34
III.3 Etapes de conception……34
III.3.1 Détection des partitions ……34
III.3.2 Détection des espaces non partitionnés……38
III.3.3 Analyse du VBR dans une partition NTFS……...38
III.3.4 Sélection des entrées de la table MFT……..39
III.3.5 Extraction et réorganisation des attributs……41
III.3.6 Décodage et interprétation du contenu des attributs……45
III.3.7 Récupération des fichiers……..46
III.4 Conclusion……49
IV Implémentation de l'analyseur de fichiers……50
IV.1 Introduction.....50
IV.2 Outils logiciels utilisés……..50
IV.3 Stratégie d'implémentation……50
IV.4 Implémentation des étapes de conception……...51
IV.4.1 Détection des partitions.....51
IV.4.2 Détection des espaces non partitionnés……....53
IV.4.3 Analyse du VBR dans une partition NTFS……...55
IV.4.4 Sélection des entrées de la table MFT……..56
IV.4.5 Extraction et réorganisation des attributs……57
IV.4.6 Décodage et interprétation du contenu des attributs……59
IV.4.7 Récupération des fichiers……60
IV.4.8 Les ADS……..61
IV.5 Fonctionnalités supplémentaires……...62
IV.5.1 Copie de fichiers……...62
IV.5.2 Hash cryptographique de fichiers……63
IV.6 Conclusion……64
Conclusion générale……65
Références bibliographiques
Annexes