République du Cameroun

Paix-Travail-Patrie

Université de Yaoundé I

Faculté des sciences

Republic of Cameroon

Peace-Work-Fatherland

University of Yaoundé I

Faculty of Science

RAPPORT

TP 323 : INVESTIGATION NUMERIQUE

Groupe :

Les Participants :

- **WOUATCHI BEUMO ANNE GENIALE 18T2506**
- **TSOUALLA TATIDOUNG GRACE**
- **VLANIA AURELIE GRACE**

Supervisé par : Dr Ebele

SOMMAIRE

INTRODUCTION

Les enquêtes judiciaires sont aujourd'hui de plus en plus confrontées à des éléments de preuves qui se manifestent sous formes de documents informatiques ou retrouvés dans la mémoire d'un dispositif électronique. La démocratisation de l'accès à l'informatique, la globalisation et l'essor des réseaux sociaux par le biais de l'internet ont été des facteurs de développement du cybercrime qui représente une nouvelle forme de criminalité et des délinquances qui se distingue des formes traditionnelles en ce qu'elle se situe dans un espace virtuel. De là, une discipline criminalistique est née : celle qui traite la preuve numérique. A cet effet surgit la nécessité de mettre sur pied des logiciels adéquats qui permettront de faciliter l'activité de la recherche des traces d'infraction et d'exaction de ces cybercrimes sur les systèmes d'information. Dans l'optique d'appréhender notre projet, nous nous attèlerons à vous présenter les différents éléments appliqués aux modules du cas d'espèce de notre application et vous faire part des orientations choisies pour la réussite de celui-ci

I.PRESENTATION DPROJET

<<image accueil>>

1) Le but du projet

Le projet qui nous a été assigné à savoir, le montage d'une application d'investigation numérique de notre choix, vise la détection des traces, à fournir les preuves d'activités malveillantes, suspectes et proscrits étant donné un système informatique et cela, tant que possible. En se rapportant plus spécifiquement et plus singulièrement au cas d'espèce de notre application, son but est de procéder à une analyse poussée et pointue de l'état des équipements informatiques tels que les ordinateurs portables ou encore une clé USB en passant par un disque dur externe afin de collecter de précieuses informations sur la moindre activité perpétré par un tiers sur le système. Notre application, se décompose donc en un ensemble d'activités ou de fonctionnalités pour la recherche de contenu suspect dans un équipement ou système informatique.

2) Le choix d'orientation de l’application

La spécialisation de notre application est édictée par l'étude des contenus ou informations renseignant de l'activité ou des activités d'une personne lambda sur l'état d'un système ou d'un équipement informatique. En effet, garder la main mise sur le fonctionnement d'un système, et avoir en temps réel un rendu du contenu et de l'impact d'une action sur un système informatique donné permet à tout moment et à coup sûr de révéler les traces de manipulations suspectes et donc par ricochet de fournir les preuves d'infractions, d'intrusion ou encore d’exactions. C'est dans cette dynamique que s'inscrit notre application dont l'approche consiste en une veille constante et en temps réel sur les manipulations entreprises au sein d'un système.

3) Le choix du langage : PYTHON

Le langage de programmation python, a été choisi sur le tas et parmi la multitude pour ses atouts pléthoriques tout comme ses possibilités, notamment dans le domaine de l'investigation numérique. On peut relever entre autres :

Sa syntaxe facile, claire et précise qui a été un facteur propulsant pour le respect des délais impartis aux projet.

La facilité de conception d'algorithmes de fouille de données qui constitue l'essence même de notre application en s'inscrivant au cœur de sa dynamique.

Et enfin, on ne saurait pas souligner la simplicité de la prise en charge d'une interface graphique cohérente, conforme et fidèle à un modèle à l'aide de la libraire pyQt5. Celle-ci étant impulsé par une utilisation particulière, originale et remarquable du puissant concept de la programmation orienté objet.

4) Revue rapide des modules de l'application

Notre application peut être découpée en quatre grands modules ayant chacun un but spécifique tout en maintenant une corrélation forte et cohésion logique entre eux.

- Le module Récupération des fichiers comme son nom l'indique, fourni comme rendu, une repertoriation ordonnée et logique des fichiers de votre équipement ou systèmes informatiques, que ces fichiers soient existants ou bien qu'ils aient été supprimés.
- Le module Analyse des fichiers permet d'étudier les métadonnées autour d'un fichier afin de révéler de possibles incohérences dans son historique de manipulation selon l'hypothèse que l'on souhaite éclairer.
- Le module Gestion des preuves, qui représente le noyau de l'application, se charge en complément de l'étude des autres contenus relatifs à l'état d'un système en dehors des fichiers. Ces contenus, pouvant être impactés par les actions ou manipulations d'un quelconque utilisateur. L'intérêt de ce module est donc de pouvoir recensèrent temps réel ou bien encore à un moment donné, les changements subis par un système.
- Le module Réingénierie des processus, se charge de l'étude et de l'observation de la dynamique des activités ou encore des états des processus ou programmes en cours d'exécution au sein d'un système informatique.

II-PRESENTATION ET EXPLICATION DES DIFFERENTS MODULES

1) Récupération des fichiers

Ce module permet de fournir un mécanisme pour l'acquisition et la répertoriassions des fichiers stockés sur votre équipement informatique de manière ordonnée et logique en appliquant un filtre de l'extension des fichiers que vous souhaitez localiser. Il prend en charge une panoplie d'autres supports de stockage de données mis à part, le disque dur interne de notre ordinateur. Il s'agit d'un disque dur externe, d'une clé USB, de CD ou encore de DVD. Il se subdivise en deux grandes branches ou articulations :

- La récupération des fichiers existants

Elle vise la localisation des fichiers actuellement existants et accessible par un utilisateur, sur l'espace disque de votre équipement et cela de façon exhaustive en fonction du répertoire logique choisi afin qu'on puisse faire une capture (avec le bouton <<Capture>>) si à jamais l'utilisateur détecte la présence d'un fichier suspect !

- La récupération des fichiers supprimés

Elle vise la localisation de l'emplacement de fichiers qui ont été supprimés par un utilisateur quelconque et qui ne sont donc pas visible sue l'espace disque et compliqués d'accès mis à part ceux se trouvant encore dans la corbeille.

Ce module est d'un grand intérêt et d'une grande importance en ce sens que la plus grande batterie des opérations sont effectués sur le contenu des fichiers, il est donc primordial de pouvoir localiser chaque fichier au sein du système.

Le bouton « Analysé ! » permet d'Analysé un fichier contenu dans un sous dossier choisit.

La date Présent dans chaque module permet de prouver la validité des preuves en Temps réelle et cella à travers des capture d'écrans via le bouton « Capture » !

2) Analyse des fichiers

Ce module s'intéresse aux métadonnées autour d'un fichier et traite de leur examen. Les métadonnées sont des sources précieuses d'informations car elles sont au premier plan de l'activité d'un individu sur un fichier dont la résultante ou encore la conséquence en est leur affectation directe. Nous avons choisi l'examen de certaines de ces métadonnées d'un quelconque fichier. Après avoir sélectionné le fichier à l'aide du bouton <<sélectionnez un fichier>> des informations concernant ce dernier s'afficherons notamment :

- Le nom du fichier qui joue le rôle d'identificateur pouvant être modifié à tout moment par un utilisateur X après opération de son forfait afin de brouiller ou de flouter sa reconnaissance

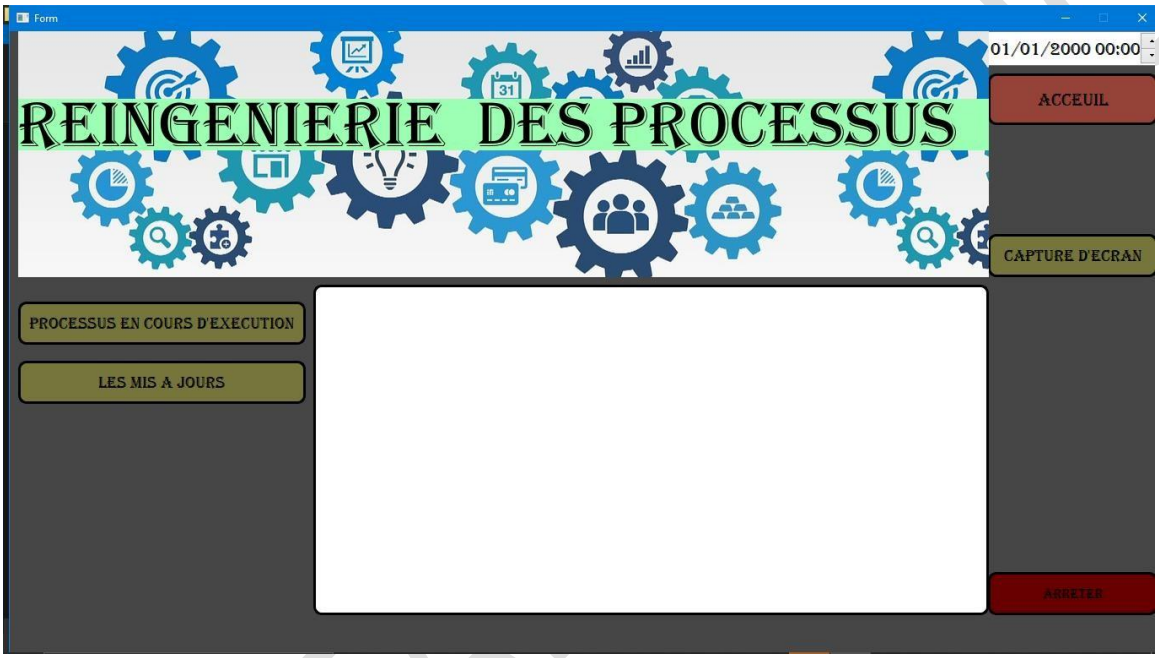
- La date de création du fichier
- La date de dernier accès qui permet de renseigner sur le fait que le fichier a été consulté outre mesure de l'historique reconnu par le propriétaire auquel appartient l'équipement ou système dans lequel il est contenu.
- La date de dernière modification qui permet de prouver qu'un fichier a par exemple été modifié plus souvent qu'il ne l'aurait dû en procédant à une relève régulière et périodique de cette date.
- Les droits d'accès sur le fichier, qui permet de connaitre qui ou quels sont les catégories d'utilisateurs qui ont le droit d'accéder à un fichier. Restreindre des droits d'accès ou en attribuer outre mesure peut dénoter d'une activité suspecte sur le fichier.
- La taille du fichier qui évidemment, dénote de toute modification procédée sur le fichier.

Le bouton <<Analysé >> Permet d'analyser un fichier jadis sélectionné dans le module « récupération des fichiers »

3) Gestion des preuves

La « Preuve numérique » représente toute information pouvant être utilisé comme preuve dans une affaire de type judiciaire. Les outils numériques tels que les signatures numériques, les documents numériques etc… constituent des éléments nécessaires à la défense en cas de mise en cause permettant ainsi la traçabilité au sein du système. C'est dans cette optique que notre application permet de fournir l'historique de navigation, des informations sur les logiciels installés dans le système, les pilotes du système, les infos sur le système de sécurité, le réseau ainsi que des périphériques du système fournissant ainsi les éléments qui se sont déroulés dans le système et les éléments du contexte indispensables à l'interprétation ultérieure de la trace. C'est dans cette même visée que l'application permet de fournir des captures d'écran des infos recensées à restituer au besoin.

4) REINGENIERIE DES PROCESSUS



La réingénierie se définit par le chargement dans la façon de faire un travail dans un processus existant dans le but d'obtenir de meilleurs résultats. La réingénierie est un élément qui s'ajoute au principe de qualité du fait que le travail, les manipulations de données sont faites sur des processus qui fournissent des détails sur l'état du système. De ce fait, l'application fournis des informations sur les processus en cours d'exécution ainsi que sur les mises à jour du système

CONCLUSION

C'est ainsi que nous parvenons à la fin de notre projet portant sur la réalisation d'une application d'investigation numérique pouvant recenser les fichiers d'un système d'information, les analysant en présentant les traces des activités du système tout en gérant les processus en cours dans le système. Nous devons avouer rétrospectivement nous sommes satisfaites du travail accompli puisque nous avons atteint des objectifs qui au préalable nous semblaient très fastidieux. En effet ce projet nous a permis d'apprendre un nouveau langage dont le Python avec lequel notre application a été réalisé, à appréhender ses fonctionnalités et à les utiliser, à manipuler des modules propres au langage qui auparavant nous étaient méconnus. Ce projet nous a également enseigner à travailler en groupe mais surtout à se dépasser. Nous ne prétendrons pas avoir résolus le problème posé qui est celui de repérer des traces d'intrusions dans un système mais nous sommes convaincus que le travail élaboré n'est qu'une étape primaire aussi bien pour une carrière professionnelle que pour des études plus approfondies.