RÉPUBLIQUE DU CAMEROUN
*****
Paix – Travail – Patrie
*****
UNIVERSITÉ DE YAOUNDÉ I
*****
École Nationale Supérieure Polytechnique de Yaoundé
*****
Département de Génie Informatique
*****

REPUBLIC OF CAMEROON
*****
Peace – Work – Fatherland
*****
UNIVERSITY OF YAOUNDÉ I
*****
National Advanced School Engineering of Yaounde
*****
Computers Engineering Department
*****

INTRODUCTION AUX TECHNIQUES D'INVESTIGATION NUMERIQUE

THEME : L'UTILITÉ DE L'INVESTIGATION NUMÉRIQUE DANS LA POLICE JUDICIAIRE

PAR :

NOMS & PRENOMS	FILIERE	MATRICULE
TAPA KEMEGNE LOIC BRAYAN	**HN-CIN-L4**	**22P108**
HEYA SALOMON FLORIAN	**HN-CIN-L4**	**22P046**
WANSI GILLES GILDAS	**HN-CIN-L4**	**22P037**

Sous la supervision de Ing THIERRY MINKA

Année Académique 2024/2025

Table des matières

1 Introduction

L'investigation numérique (ou *digital forensic*) est une discipline qui consiste à **collecter, analyser, conserver et présenter des preuves numériques** issues d'ordinateurs, de téléphones, de réseaux ou de tout autre support électronique, dans le but d'appuyer une enquête (judiciaire, administrative ou privée). De nos jours, elle se voit octroyée progressivement une plus grande importance dans un monde marqué par la digitalisation et la cybercriminalité et plus dans le domaine policier.

De ce fait, en quoi l'investigation numérique constitue-t-elle un outil indispensable pour la police judiciaire dans la lutte contre la criminalité moderne ? Dans la suite de notre analyse nous verrons tout d'abord les apports essentiels de l'investigation numérique à la police judiciaire, ensuite ses principaux domaines d'application et enfin les outils, défis et limites de l'investigation numérique.

2 Les apports essentiels de l'investigation numérique à la police judiciaire

2.1 Accès à des preuves invisibles dans le monde physique

— L'investigation numérique permet de retrouver des traces **difficiles à effacer** : historiques de navigation, conversations supprimées, métadonnées, fichiers effacés mais récupérables.

— Elle ouvre ainsi une "scène de crime virtuelle" complémentaire à la scène physique.

2.2 Lutte contre la cybercriminalité

— Les enquêtes sur le **piratage informatique, les fraudes en ligne, les ransomwares, le phishing** reposent directement sur ces techniques.

— Sans investigation numérique, ces infractions resteraient **impossibles à résoudre** car elles laissent très peu de traces matérielles.

2.3 Identification et traçage des auteurs

— Analyse des adresses IP, des journaux système, des connexions réseaux permettent de **remonter jusqu'au suspect**.

— Récupération de données de géolocalisation ou de communication (SMS, WhatsApp, email) fournit des **éléments d'identification et d'alibi**.

2.4 Reconstitution des événements

— L'investigation permet de **reconstituer une chronologie numérique** :

  — Quand un fichier a été créé, modifié, transféré ?

  — À quelle heure un utilisateur s'est connecté ?

  — Quelles données ont été effacées ou copiées ?

— Ces éléments aident les enquêteurs à **reconstruire le scénario d'un crime**.

2.5 Apport de preuves recevables en justice

— Les procédures de collecte et de conservation (intégrité, traçabilité) assurent que les preuves numériques sont **valides et utilisables devant un tribunal**.

— Cela permet à la justice de prendre des décisions **basées sur des preuves techniques solides**.

2.6 Soutien aux enquêtes traditionnelles

— L'investigation numérique **complète les méthodes classiques** :

  — Vidéosurveillance + analyse des communications téléphoniques.

  — Fouilles physiques + recherche d'indices numériques.

— Elle donne une vision **globale** des faits.

3 Principaux domaines d'application de l'investigation numérique

L'investigation numérique, ou forensic numérique, est devenue un outil stratégique dans les missions régaliennes des forces de l'ordre. Elle permet d'identifier, de collecter, d'analyser et de préserver des preuves numériques issues de téléphones, ordinateurs, serveurs, réseaux ou systèmes électroniques, afin de résoudre des affaires criminelles complexes et de soutenir la justice. Au Cameroun, son importance ne cesse de croître, notamment dans la lutte contre la cybercriminalité, la grande criminalité transfrontalière, la criminalité financière, et les crimes violents.

3.1 Lutte contre la cybercriminalité

La cybercriminalité regroupe toutes les infractions commises à l'aide de moyens numériques, telles que le piratage informatique, la fraude en ligne, l'usurpation d'identité ou la diffusion de contenus illicites.

Exemples camerounais :

— En 2022, un réseau de fraude en ligne basé à Douala a été démantelé après que les enquêteurs aient analysé les transactions numériques et localisé les auteurs grâce à la récupération des adresses IP et des journaux de connexion (logs).

— La Gendarmerie nationale, par son unité spécialisée, a utilisé des techniques d'investigation numérique pour identifier des fraudeurs impliqués dans des opérations de phishing ciblant des entreprises camerounaises.

Techniques employées :

— Analyse des journaux de connexion et logs de serveurs.

— Récupération de données effacées sur disques durs et smartphones.

— Traçage des flux financiers numériques pour identifier les auteurs.

3.2 Lutte contre la grande criminalité transfrontalière et le terrorisme

Les réseaux criminels transfrontaliers, tels que le trafic de drogues, la traite d'êtres humains, et le terrorisme, exploitent souvent les outils numériques pour coordonner leurs activités. L'investigation numérique permet de suivre ces réseaux et d'anticiper leurs actions.

Exemples camerounais :

— Interpol Cameroun, à travers son pôle spécialisé, a permis d'identifier et d'arrêter plusieurs réseaux de trafic de stupéfiants entre le Nigeria et le Cameroun grâce à l'analyse des données informatiques et téléphoniques saisies lors d'opérations conjointes.

— Dans la lutte contre Boko Haram, l'extraction et l'analyse de messages sur téléphones et ordinateurs saisis dans l'Extrême-Nord ont permis de cartographier les réseaux logistiques et d'anticiper des attaques.

Techniques employées :

— Analyse de métadonnées de communications (SMS, emails, applications de messagerie).

— Géolocalisation et suivi des appareils numériques.

— Profilage et cartographie des réseaux criminels via l'exploitation de données volumineuses.

3.3 Lutte contre la criminalité financière et économique

La criminalité économique implique souvent des flux financiers complexes et des fraudes numériques. L'investigation numérique est essentielle pour détecter la corruption, le blanchiment d'argent et les détournements de fonds publics ou privés.

Exemples camerounais :

— En 2021, un réseau de détournement de fonds publics a été démantelé après l'analyse des fichiers numériques provenant d'ordinateurs administratifs et de comptes bancaires électroniques.

— Des audits numériques ont permis d'identifier des fraudes fiscales et des transactions suspectes dans plusieurs entreprises opérant au Cameroun.

Techniques employées :

— Traçage et analyse des transactions électroniques.

— Corrélation entre données numériques et documents physiques.

— Data mining et analyse de bases de données comptables et bancaires.

3.4 Lutte contre la criminalité organisée et les crimes violents

Les enquêtes sur les homicides, kidnappings et vols à main armée bénéficient grandement de l'investigation numérique. Elle permet de reconstituer des événements et de relier des suspects entre eux.

Exemples camerounais :

— Affaire de kidnapping à Yaoundé : l'analyse des téléphones des victimes et suspects a permis de reconstituer les déplacements et d'identifier les complices.

— Vols à main armée dans le Littoral : l'exploitation des vidéos de vidéosurveillance et des données des téléphones portables a permis d'élucider plusieurs affaires complexes.

Techniques employées :

— Reconstitution chronologique des événements à partir des appareils numériques.

— Analyse vidéo et extraction d'informations depuis les images de surveillance.

— Analyse des communications téléphoniques pour identifier les réseaux de complicité.

3.5 Protection de l'enfance et lutte contre la pédopornographie

L'investigation numérique permet d'identifier et de neutraliser les réseaux diffusant des contenus pédopornographiques, protégeant ainsi les victimes.

Exemples camerounais :

— En 2022, le Commissariat central de Yaoundé a démantelé un réseau de diffusion de contenus pédopornographiques sur les réseaux sociaux grâce à l'analyse de données numériques et à la collaboration avec Interpol et Europol.

Techniques employées :

— Analyse d'images et vidéos pour identifier les victimes.

— Traçage des adresses IP et des comptes en ligne des auteurs.

— Collaboration internationale pour le recoupement des informations et l'identification des suspects.

3.6 Investigation numérique dans les enquêtes judiciaires classiques

Même pour des enquêtes ne relevant pas directement de la cybercriminalité, l'exploitation des données numériques renforce la capacité des forces de l'ordre à établir des preuves solides.

Exemples camerounais :

— Affaires de fraude électorale locale : l'analyse des bases de données électorales et des tableurs numériques a permis de détecter des irrégularités dans plusieurs bureaux de vote.

— Conflits fonciers : l'exploitation des messages électroniques et documents numériques a permis de révéler des falsifications et transactions illégales.

Techniques employées :

— Analyse et authentification de documents numériques.

— Extraction de preuves depuis ordinateurs, smartphones et serveurs.

— Préservation des preuves numériques pour leur utilisation en justice.

3.7 Synergie avec les organisations internationales et autres forces

L'investigation numérique au Cameroun ne se limite pas aux forces locales. Les collaborations internationales sont cruciales pour traquer les réseaux criminels transnationaux.

Exemples camerounais :

— Le pôle Interpol de Yaoundé coordonne des opérations avec des services étrangers pour identifier des fraudeurs et cybercriminels opérant depuis le Cameroun vers l'Europe et l'Afrique.

— Les échanges de données sécurisés permettent d'enquêter sur des réseaux de trafic de drogues, blanchiment d'argent et cyberfraude à l'échelle internationale.

Techniques employées :

— Partage sécurisé et légal de preuves numériques.

— Utilisation de logiciels spécialisés d'analyse de données massives.

— Coopération inter-agences pour la traque et l'arrestation de suspects internationaux.

4 Les outils, défis et limites de l'investigation numérique

4.1 Les principaux outils et techniques

4.1.1 Logiciels de récupération et d'analyse de données

— **Récupération des données supprimées** : Utilisation d'outils comme Autopsy (gratuit), FTK Imager ou Cellebrite pour restaurer fichiers, messages et historiques même après suppression

— **Analyse forensic avancée** : Examens approfondis des métadonnées, signatures numériques et artefacts système

— **Spécialisation mobile** : Oxygen Forensic Detective et Mobiledit pour l'extraction données smartphones

4.1.2 Techniques d'investigation réseau et surveillance

— **Analyse de trafic** : Wireshark pour intercepter et analyser communications réseau

— **Investigation sur dark web** : Outils comme AIL pour surveiller marchés illicites et forums criminels

— **Surveillance légale** : Plateformes de Lawful Interception pour interception communications sous mandat

4.1.3 Lutte contre le chiffrement et protection des données

— **Cryptanalyse** : Techniques pour contourner chiffrements légers et mots de passe faibles

— **Accès sécurisé** : Write-blockers pour garantir intégrité preuves durant acquisition

— **Attaques dictionnaire/brute force** : Hashcat pour craquage mots de passe sur ordonnance judiciaire

4.2 Les défis rencontrés au Cameroun

4.2.1 Explosion et complexité des données

— **Volume exponentiel** : Un smartphone peut contenir 128GB+ de données à analyser

— **Diversité des formats** : Fichiers multimédias, applications, cloud data nécessitant outils spécialisés

— **Temps d'analyse** : Une analyse forensic complète peut prendre plusieurs semaines

4.2.2 Respect des droits fondamentaux

— **Vie privée vs sécurité** : Équilibre délicat entre investigation et respect Article 9 Constitution camerounaise

— **Cadre légal** : Nécessité stricte de mandats conformément à la loi cybersécurité Cameroun 2010

— **Proportionnalité** : L'investigation doit être ciblée et justifiée par nécessité enquête

4.2.3 Évolution technologique et formation

— **Obsolescence rapide** : Nouveaux OS, applications et techniques de chiffrement mensuelles

— **Besoins formation continue** : Nécessité recyclage permanent des enquêteurs

— **Coût des équipements** : Licences logicielles dépassant souvent 10 millions FCFA/an

4.3 Les limites actuelles

4.3.1 Difficultés juridiques camerounaises

— **Admissibilité preuves** : Risque de rejet si chaîne de custody non respectée

— **Preuve numérique fragile** : Vulnerable altération, contestation authenticité

— **Harmonisation légale** : Besoin standards clairs pour preuves électroniques tribunaux

4.3.2 Dépendance à l'expertise technique

— **Pénurie experts** : Moins de 50 experts certifiés au Cameroun

— **Centralisation compétences** : Expertise concentrée à Yaoundé et Douala

— **Délais allongés** : Files d'attente pour analyses urgentes

4.3.3 Contraintes matérielles et financières

— **Équipements coûteux** : Station forensic complète est d'environ 25 millions FCFA

— **Maintenance difficile** : Pannes, mises à jour, support technique limité

— **Budget insuffisant** : Priorisation nécessaire entre enquêtes

5 Conclusion

En définitive, cette analyse a démontré de manière éclatante que l'investigation numérique s'est imposée comme un outil indispensable au sein de la police judiciaire, et plus particulièrement dans le contexte camerounais. Face à une criminalité moderne qui a massivement migré vers le numérique, elle est passée du statut de compétence spécialisée à celui de pilier fondamental de toute enquête criminelle.

Notre réflexion a successivement mis en lumière ses apports essentiels – en faisant un instrument privilégié pour accéder à des preuves invisibles, identifier les auteurs et reconstituer des événements avec une précision inédite. Nous avons ensuite exploré la diversité de ses domaines d'application, de la lutte contre la cybercriminalité à la résolution des crimes violents en passant par le démantèlement des réseaux transnationaux, illustrant son utilité opérationnelle à travers de multiples affaires traitées sur le sol camerounais.

Cependant, cet exposé a aussi dressé un constat lucide : cet atout majeur se heurte à des défis et des limites substantielles. L'explosion du volume de données, la complexité technique croissante, les contraintes juridiques et les limites matérielles et humaines, notamment la pénurie d'experts et le coût des équipements, constituent des freins réels à son efficacité maximale au Cameroun.

Malgré ces obstacles, la trajectoire est tracée : il n'y a pas de retour en arrière possible. L'investigation numérique n'est plus une option, mais une nécessité pour la sécurité nationale et l'efficacité de la justice. Pour consolider ses acquis, le Cameroun doit impérativement investir dans la formation continue de ses enquêteurs, le renforcement des moyens logistiques des unités spécialisées et l'adaptation permanente de son cadre juridique.

En guise d'ouverture, l'avenir de l'investigation numérique s'annonce à la fois passionnant et périlleux. L'avènement de l'intelligence artificielle, l'utilisation croissante du métavers par les criminels, la menace des deepfakes pour la manipulation de preuves et les défis de l'ère post-quantique constituent les nouvelles frontières que la police judiciaire devra explorer. La capacité du Cameroun à anticiper ces mutations technologiques déterminera son succès dans la lutte contre la criminalité de demain. Ainsi, loin d'être un simple outil technique, l'investigation numérique s'affirme comme un élément stratégique pour la souveraineté et la sécurité numérique de la nation.