RÉPUBLIQUE DU CAMEROUN
****
Paix - Travail - Patrie
****
UNIVERSITÉ DE YAOUNDÉ I
****
ECOLE NATIONALE SUPERIEURE POLYTECHNIQUE DE YAOUNDE
****
DÉPARTEMENT DE GENIE INFORMATIQUE
****

REPUBLIC OF CAMEROON
****
Peace - Work - Fatherland
****
UNIVERSITY OF YAOUNDE I
****
NATIONAL ADVANCED SCHOOL OF ENGINEERING OF YAOUNDE
****
DEPARTMENT OF COMPUTER ENGINEERING
****

EXERCICES

Philosophie et Fondements de l'Investigation Numérique

Option :

Cybersécurité et Investigation Numérique

Rédigé par :
BAALAWE LIONEL JOSSELIN, *24P822*

Sous l'encadrement de :
Expert Thierry MINKA

Année académique 2025 / 2026

Points sur les algorithmes de reconnaissance faciale

École Nationale Supérieure Polytechnique de Yaoundé
Département de Génie Informatique

Encadreur : M. MINKA MI NGUIDJOI Thierry Emmanuel
Année académique : 2025–2026

Résumé général

La reconnaissance faciale (RF) est une technologie d'intelligence artificielle utilisée pour identifier ou vérifier l'identité d'une personne à partir de son visage. Elle s'appuie sur l'analyse de traits biométriques uniques et trouve des applications dans la sécurité, la téléphonie et l'investigation numérique. Cependant, son usage soulève d'importantes questions éthiques et juridiques liées à la vie privée et à la proportionnalité.

0.1 Présentation de la reconnaissance faciale

Un système biométrique se compose de trois étapes : l'enrôlement, l'identification et la vérification. Son architecture comprend quatre modules : la capture, l'extraction de caractéristiques, la correspondance et la décision. La précision et la fiabilité de ces modules conditionnent la performance globale du système.

0.2 Méthodes de reconnaissance

Les principales approches sont :

— **Méthodes classiques :** PCA, LDA, SVM, GMM, réseaux de neurones et modèles 3D.
— **Méthodes locales :** basées sur les traits géométriques (HMM, EBGM, appariement de gabarits).
— **Méthodes hybrides :** combinaison de modèles globaux et locaux pour une meilleure robustesse.

Des détecteurs et descripteurs tels que SIFT, HOG, SURF ou KAZE permettent d'améliorer la précision et l'invariance des systèmes.

0.3 Avantages et inconvénients

La reconnaissance faciale présente des atouts majeurs : rapidité, automatisation et capacité à traiter de grandes quantités de données. Cependant, elle est limitée par la sensibilité aux conditions d'éclairage, les biais algorithmiques, le manque d'interopérabilité et les risques de piratage ou d'usurpation (deepfakes). Les impacts éthiques (vie privée, discrimination) et juridiques (responsabilité, légitimité) nécessitent une vigilance constante.

0.4 Recommandations

0.4.1 Techniques

Documenter les pipelines, effectuer des tests locaux et utiliser des modèles hybrides pour plus de robustesse.

0.4.2 Sécurité

Effectuer des pentests réguliers, chiffrer les modèles biométriques et intégrer des contrôles de vivacité multi-capteurs.

0.4.3 Éthique et société

Conduire des études d'impact (DPIA), auditer les biais et informer le public sur les usages de la RF.

0.4.4 Juridique

Respecter la loi camerounaise sur la protection des données (n°2024/017), garantir une base légale claire et encadrer les usages sensibles par mandat judiciaire.

0.4.5 Organisation

Prévoir un budget adapté, définir des procédures opérationnelles standard (SOP) et tester les déploiements dans des contextes limités.

0.4.6 Proportionnalité

S'assurer que tout usage est nécessaire, documenté et validé par un opérateur humain ; suspendre le système en cas d'abus.

0.5 Conclusion

La reconnaissance faciale est un outil puissant d'investigation numérique et de cybersécurité, mais son efficacité repose sur un cadre rigoureux. Seule une utilisation proportionnée, transparente et conforme au droit permettra d'en faire un véritable atout pour la justice et la sécurité au Cameroun.

Références

1. CNIL, *Reconnaissance faciale : enjeux, usages et cadre juridique.*
2. UNESCO, *Éthique de l'intelligence artificielle.*
3. ANSSI, *Sécurité des systèmes biométriques.*
4. Hobeika R., *Comprendre la reconnaissance faciale*, IMT, 2020.
5. Commission de l'UE, *Cadre RGPD et reconnaissance faciale.*

6. OCDE, *Intelligence artificielle et reconnaissance faciale : défis éthiques.*
7. ONU, *Technologies biométriques et droits humains.*

Simulation d'une série de messages sur WhatsApp entre un homme et sa maîtresse

Théories et Pratiques de l'Investigation Numérique

École Nationale Supérieure Polytechnique de Yaoundé
Département de Génie Informatique

Encadreur : M. MINKA MI NGUIDJOI Thierry Emmanuel
Année académique : 2025–2026

Résumé général

Cette étude illustre la facilité avec laquelle il est possible de falsifier des conversations WhatsApp grâce à des outils accessibles. L'objectif n'est pas de reproduire un cas réel, mais de comprendre les enjeux techniques, juridiques et éthiques liés à la manipulation de preuves numériques.

0.6 Mise en situation

Le scénario imagine un enseignant, Paul KENGNE, entretenant une relation extra-conjugale avec une étudiante. Les éléments fournis comprennent sept captures d'écran et deux photos transmises via WhatsApp. Les messages simulés comportent des propos affectifs et intimes.

0.7 Méthodologie de falsification

Deux outils ont été employés :

— **Chatsmock :** application web permettant de créer de fausses conversations WhatsApp avec personnalisation des profils, horaires et statuts.

— **Adobe Photoshop :** utilisé pour retoucher, insérer des images et corriger l'interface pour un rendu indétectable.

L'association des deux outils démontre qu'il est facile de produire des preuves numériques fausses, visuellement crédibles mais non authentiques.

0.8 Limites et comparaison

0.8.1 Limites de Chatsmock

Les limites concernent le réalisme graphique, la personnalisation restreinte et la dépendance au format image. Une expertise forensique peut parfois déceler les incohérences de métadonnées.

0.8.2 Comparaison avec d'autres outils

Des alternatives telles que *FakeChat*, *WhatsFake* ou Photoshop présentent des niveaux variables de réalisme et de complexité. Certains outils d'analyse forensique peuvent être détournés à des fins de manipulation directe des bases de données de messagerie.

0.8.3 Conclusion partielle

Chatsmock se distingue par sa simplicité, mais couplé à Photoshop, il rend la falsification très difficile à détecter sans examen approfondi.

0.9 Impact sur l'investigation numérique et recommandations

0.9.1 Impact

L'accessibilité de ces outils remet en cause la fiabilité des captures d'écran et complexifie la tâche des enquêteurs. Elle expose les institutions à des risques de manipulation et de multiplication de fausses preuves.

0.9.2 Recommandations

— Vérifier les métadonnées et signatures numériques des fichiers.

— Former juges, avocats et enquêteurs à la détection de falsifications.

— Utiliser des outils spécialisés d'analyse d'images et de données brutes.

— Renforcer le cadre légal sur la recevabilité des preuves numériques.

0.10 Conclusion

L'expérience a démontré la facilité de falsifier des preuves numériques à l'aide d'outils accessibles. Pour préserver la crédibilité de l'investigation numérique, il est impératif de renforcer les méthodes d'authentification, la formation des experts et la vigilance institutionnelle. La fiabilité des preuves dépend désormais de la rigueur et de la transparence dans le traitement des données.

Deepfake Vocal

Option : Cybersécurité et Investigation Numérique

École Nationale Supérieure Polytechnique de Yaoundé
Département de Génie Informatique

Encadreur : M. Thierry MINKA
Année académique : 2025–2026

Résumé général

Le deepfake vocal est une innovation issue de l'intelligence artificielle permettant d'imiter la voix humaine de manière réaliste. Bien qu'utilisé à des fins légitimes, il représente une menace croissante pour la sécurité numérique et la fiabilité des preuves. Ce rapport présente les aspects techniques, éthiques et juridiques du phénomène, avec une étude de cas sur la technologie MINIMAX Audio.

0.11 Généralités sur le deepfake audio

Les deepfakes audio exploitent le deep learning pour cloner des voix à partir d'enregistrements réels.

0.11.1 Évolution

De 1939 à nos jours, la synthèse vocale a évolué du *Voder* aux modèles neuronaux comme *WaveNet* et *Tacotron*. Depuis 2016, le clonage vocal est devenu accessible et parfois malveillant (fraudes, usurpations, désinformation).

0.11.2 Contexte d'utilisation

Les usages sont légitimes (accessibilité, doublage, assistants virtuels) ou malveillants (fraudes financières, manipulation politique, falsification de preuves). Ces derniers menacent directement la fiabilité des enquêtes numériques.

0.12 Enjeux pour l'investigation numérique

Les deepfakes vocaux compromettent :

— **La confidentialité** des communications ;

— **La fiabilité** des preuves audio ;

— **L'opposabilité** judiciaire des enregistrements.

Les enquêteurs doivent maîtriser les techniques de détection acoustique et garantir la transparence méthodologique.

0.13 Cas pratique : MINIMAX Audio

0.13.1 Présentation

MINIMAX Audio est un outil de clonage vocal basé sur l'IA, capable d'imiter la voix humaine avec une fidélité remarquable.

0.13.2 Utilisation

L'outil comprend plusieurs modules : *Voice Clone* (création du clone vocal), *Text to Speech* (génération de discours), et *Voice Isolator* (nettoyage audio). Les rendus produits sont presque indétectables à l'oreille humaine.

0.13.3 Risques et aspects éthiques

Les dangers incluent l'usurpation d'identité, la fraude financière et la manipulation médiatique. En 2019, une entreprise britannique a perdu 220 000€ après une escroquerie utilisant une voix clonée de PDG.

0.14 Contre-mesures et prévention

- **Détection technologique :** intégration d'outils d'analyse vocale et de marquage numérique.
- **Sensibilisation :** formation du public et des professionnels à la reconnaissance des deepfakes.
- **Cadre légal :** adoption de lois spécifiques et de sanctions pour usage frauduleux.
- **Authentification renforcée :** recours à la reconnaissance vocale dynamique et à la multi-authentification.
- **Éthique de l'IA :** transparence, consentement et gouvernance responsable.

0.15 Conclusion

Le deepfake vocal illustre la dualité entre innovation et menace. S'il favorise l'accessibilité et la créativité, il remet aussi en cause la confiance numérique. Son encadrement requiert une combinaison de solutions techniques, légales et éthiques. Seule une approche responsable permettra d'en exploiter le potentiel tout en protégeant la société contre ses dérives.

Conception et analyse d'un faux profil TikTok

Choix d'une niche dans le cadre d'une investigation numérique

Option : Cybersécurité et Investigation Numérique

École Nationale Supérieure Polytechnique de Yaoundé
Département de Génie Informatique

Encadreur : M. Thierry MINKA, Eng.
Année académique : 2025–2026

Résumé général

Ce travail d'investigation numérique a consisté à concevoir et analyser un faux profil TikTok dans un cadre pédagogique. L'objectif principal était de comprendre les mécanismes d'influence numérique, les dynamiques d'engagement et les enjeux éthiques liés à la simulation d'identité. Le profil *Innotrends25*, centré sur la thématique de la cybersécurité, a permis d'observer les réactions des utilisateurs tout en sensibilisant aux bonnes pratiques de sécurité en ligne.

0.16 Démarche méthodologique adaptée

0.16.1 Création du faux profil

Le profil a été créé à l'aide d'un service de messagerie temporaire (*Temp Mail*) pour préserver l'anonymat et éviter toute liaison avec les données personnelles réelles. Ce faux compte a servi de base à la diffusion de contenus éducatifs dans le cadre de notre observation.

0.16.2 Justification du choix de la niche

La cybersécurité est une thématique essentielle face à la croissance des menaces numériques. Le choix de cette niche s'explique par sa pertinence technique et éducative : elle permet de sensibiliser tout en respectant les limites éthiques de l'investigation numérique. Cette approche valorise la prévention et la pédagogie plutôt que la tromperie.

0.16.3 Stratégie de contenu utilisée

Notre stratégie reposait sur un ton à la fois éducatif et engageant, utilisant des visuels attractifs et des messages accessibles. Les principales thématiques abordées étaient :

— La sécurité des mots de passe ;

— La gestion des données personnelles ;

— Les arnaques en ligne et le phishing.

Les contenus ont été conçus avec des outils comme **ChatGPT** (génération de textes), **Canva** (création graphique) et **TikTok Analytics** (suivi des interactions). L'ensemble des publications respectait les règles de la plateforme et visait à observer les comportements sans causer de préjudice.

0.16.4 Outils et moyens de suivi

Le suivi des performances du profil a reposé sur :

— L'analyse des statistiques internes de TikTok (likes, vues, abonnés, taux d'engagement) ;

— Des captures d'écran réalisées à différentes étapes du projet ;

— L'utilisation d'un tableau de bord pour noter observations et hypothèses.

Le profil *Innotrends25* a suscité un réel intérêt, atteignant plus de 100 mentions « j'aime » sur six publications liées à la cybersécurité.

0.17 Analyse et observation

0.17.1 Pertinence de la stratégie déployée

La stratégie de contenu s'est révélée efficace. L'association entre humour, éducation et visuels dynamiques a favorisé la portée du message et l'engagement des utilisateurs. Les sujets pratiques comme les mots de passe ou le Wi-Fi public ont facilité l'identification du public cible.

0.17.2 Comportement des utilisateurs face au profil

Les réactions observées témoignent de l'influence des réseaux sociaux sur la perception et la confiance des utilisateurs. Bien que mené dans un cadre pédagogique, ce projet souligne la nécessité de maintenir un cadre éthique rigoureux pour éviter toute confusion entre expérimentation et manipulation.

0.17.3 Recommandations

Plusieurs pistes d'amélioration sont proposées :

— Renforcer la formation en cybersécurité dès le secondaire ;

— Promouvoir l'usage responsable des outils numériques ;

— Encadrer légalement les projets éducatifs basés sur la simulation d'identité ;

— Encourager la collaboration entre les domaines technique, juridique et communicationnel.

0.18 Conclusion

Ce projet d'investigation numérique a permis d'explorer de manière concrète les enjeux de l'identité numérique et de la sensibilisation sur les réseaux sociaux. L'expérience montre que les plateformes comme TikTok peuvent devenir des vecteurs efficaces d'éducation à la cybersécurité, à condition d'être utilisées dans un cadre responsable et éthique. Elle met en évidence l'importance d'une approche critique et maîtrisée des outils numériques dans toute démarche d'investigation.

Introduction aux techniques de l'investigation numérique

Les trois meilleurs logiciels de rédaction de mémoire

École Nationale Supérieure Polytechnique de Yaoundé
Département de Génie Informatique

Encadreur : Mr. MINKA MI NGUIDJOI Thierry Emmanuel

Année académique : 2025–2026

Résumé général

Ce rapport présente une étude comparative des principaux logiciels de rédaction de mémoire : **Overleaf**, **Microsoft Word** et **Zotero**. L'objectif est d'analyser leurs avantages, limites et complémentarités afin d'aider les étudiants en investigation numérique à choisir les outils les mieux adaptés à leurs besoins. La combinaison idéale de ces solutions permet d'allier rigueur académique, productivité et collaboration.

0.19 Introduction

La rédaction d'un mémoire représente un défi académique exigeant, mêlant structuration, gestion bibliographique et mise en page professionnelle. Le choix du logiciel joue un rôle déterminant dans la réussite du projet. Ce travail compare trois solutions largement utilisées dans le monde académique : Overleaf, Microsoft Word et Zotero, en évaluant leurs performances selon des critères d'efficacité, de collaboration et de rigueur scientifique.

0.20 Overleaf : L'excellence académique par LaTeX

0.20.1 Historique

Créé en 2012 par John Hammersley et John Lees-Miller, Overleaf avait pour objectif de simplifier la rédaction scientifique en LaTeX. Son rachat par Springer Nature en 2023 a renforcé son statut de plateforme académique mondiale.

0.20.2 Présentation et philosophie

Overleaf est un éditeur LaTeX en ligne fondé sur trois principes :

— **Accessibilité :** permettre l'usage de LaTeX sans installation complexe ;

— **Collaboration :** offrir un espace de travail partagé en temps réel ;

— **Qualité :** assurer une mise en page typographique professionnelle.

0.20.3 Atouts majeurs

— Qualité typographique exceptionnelle ;
— Gestion automatique des références croisées (figures, équations, sections) ;
— Collaboration instantanée et historique des modifications ;
— Modèles académiques conformes aux normes universitaires.

0.20.4 Limites et alternatives

— Courbe d'apprentissage relativement élevée ;
— Fonctionnement hors ligne restreint ;
— Moins intuitif pour les corrections rapides.

Alternatives : LyX, TeXmaker, TeXstudio ou Authorea pour une approche locale.

0.21 Microsoft Word : Le référencement en traitement de texte

0.21.1 L'outil universel

Word reste le logiciel de traitement de texte le plus utilisé dans le monde académique. Son interface familière, sa compatibilité universelle et son intégration à la suite Microsoft Office en font une solution accessible à tous les niveaux.

0.21.2 Points forts académiques

— Gestion hiérarchique des styles (Titres, Sous-titres) pour structurer les documents longs ;
— Génération automatique des tables des matières et des figures ;
— Suivi des modifications et commentaires intégrés ;
— Compatibilité élevée entre étudiants et encadrants.

0.21.3 Défis et concurrents

— Gestion bibliographique native limitée ;
— Risque de corruption sur les longs documents ;
— Structuration parfois incohérente sans utilisation rigoureuse des styles.

Alternatives : LibreOffice Writer et Google Docs pour une solution gratuite ou collaborative.

0.22 Zotero : Le spécialiste de la bibliographie

0.22.1 Présentation générale

Zotero est un gestionnaire de références bibliographiques open-source, créé par le Center for History and New Media de l'Université George Mason. Il permet de collecter, organiser et insérer automatiquement les citations et bibliographies.

0.22.2 Fonctionnalités académiques essentielles

— Capture automatique des métadonnées depuis les bases de données académiques ;
— Intégration directe avec Word, LibreOffice et Overleaf via BibTeX ;
— Gestion de milliers de styles de citations (APA, MLA, Chicago, etc.) ;
— Synchronisation cloud et partage collaboratif via Zotero Groups.

0.22.3 Écosystème et alternatives

Extensions clés : ZotFile (gestion PDF) et Better BibTeX (export LaTeX). **Alternatives :** Mendeley, EndNote et Citavi.

0.23 Combinaisons gagnantes et workflows optimisés

0.23.1 Les synergies logicielles

— **Word + Zotero :** combinaison la plus accessible pour débutants ;
— **Overleaf + Zotero :** solution optimale pour la recherche scientifique ;
— **Overleaf + Zotero Groups :** environnement collaboratif idéal pour les travaux d'équipe.

0.23.2 Recommandations selon le profil

— **Débutants :** Word + Zotero pour la simplicité d'usage ;
— **Scientifiques :** Overleaf + Zotero pour la rigueur et la qualité typographique ;
— **Collaboratifs :** Overleaf + Zotero Groups pour la synchronisation et le travail d'équipe.

0.24 Conclusion

Le choix du logiciel influence profondément la qualité d'un mémoire. Overleaf se distingue par sa rigueur scientifique, Word par sa simplicité et Zotero par sa gestion bibliographique. La combinaison **Overleaf + Zotero** offre un équilibre idéal entre exigence académique et efficacité. Cependant, la réussite d'un mémoire repose avant tout sur la réflexion et la structure du contenu, les outils n'étant que des facilitateurs au service de la pensée.

Présentation détaillée du protocole ZK-NR : RL et positionnement dans l'investigation numérique moderne

Option : Humanités Numériques et Investigation Numérique

École Nationale Supérieure Polytechnique de Yaoundé
Département de Génie Informatique

Encadreur : M. Thierry MINKA
Année académique : 2025–2026

Résumé général

Ce document présente une étude approfondie du protocole **ZK-NR** (Zero-Knowledge Non-Repudiation) et de son rôle dans l'investigation numérique moderne. L'objectif est de montrer comment ce protocole, combiné au cadre **CLO** (Cryptographic Legal Opposability) et aux primitives post-quantiques (CEE, AOW, SH), permet de produire des preuves numériques vérifiables, sécurisées et légalement opposables. Des exemples concrets d'investigations au Cameroun et à l'international illustrent l'application pratique de ces concepts.

0.25 Concepts clés

0.25.1 Non-répudiation numérique

La non-répudiation garantit qu'un message ou un acte numérique ne peut être contesté par l'expéditeur ou le destinataire. Elle repose sur plusieurs outils :

- **Signature numérique** : assure l'authenticité et l'intégrité du message via une clé privée et une clé publique.
- **Certificat électronique** : identifie de manière fiable une personne ou une organisation et associe une clé publique.
- **Horodatage numérique** : atteste qu'un document existait à une date et heure précises.
- **Fonction de hachage** : garantit l'intégrité des données en produisant une empreinte unique.

0.26 État de l'art et travaux récents

0.26.1 Protocole ZK-NR et architectures associées

ZK-NR combine des primitives post-quantiques (STARKs, signatures BLS à seuil, Dilithium) pour générer des preuves vérifiables sans révéler de données sensibles. Il s'adresse aux environnements réglementés et intègre le **Trilemme CRO** (Confidentialité, Fiabilité, Opposabilité), ainsi que l'infrastructure **Q2CSI** pour la sécurité quantique composable.

0.26.2 Primitives CASH

— **CEE (Chaotic Entropic Expansion)** : assure la confidentialité via une expansion entropique post-quantique.

— **AOW (Affine One-Wayness)** : garantit la fiabilité temporelle des preuves.

— **SH (Semantic Holder)** : permet l'opposabilité juridique des preuves.

0.26.3 Synthèse comparative

Tous les travaux convergent vers la sécurisation et la non-répudiation des preuves, la résilience post-quantique et l'opposabilité juridique, conformément aux contraintes théoriques du Trilemme CRO.

0.27 Acteurs et communauté scientifique

0.27.1 Pôles majeurs

— **Zero-Knowledge et STARKs** : Eli Ben-Sasson, Alessandro Chiesa, Jens Groth, Matthew D. Green.

— **Cryptographie post-quantique** : Daniel J. Bernstein, NIST PQC.

— **Sécurité formelle et composabilité** : Ran Canetti (Universal Composability).

— **Investigation numérique et opposabilité juridique** : Eoghan Casey.

0.27.2 Entreprises et projets

— StarkWare et Zcash : mise en production des ZK-STARK et confidentialité des transactions.

— Groupes académiques : MIT, Berkeley, Technion, INRIA ; développement de primitives post-quantiques et outils open-source (arkworks, libsnark).

0.28 Rôle du ZK-NR dans l'investigation numérique

ZK-NR répond aux besoins des enquêteurs :

— Assurer l'intégrité et la traçabilité des preuves collectées.

— Garantir la non-répudiation des actes numériques.

— Préserver la confidentialité des données sensibles.

— Fournir des preuves juridiquement opposables.

0.29 Apports du ZK-NR et CLO

— Création d'attestations invisibles mais vérifiables via Zero-Knowledge Proofs.

— Certification cryptographique de la chaîne de possession.

— Résilience face aux attaques quantiques grâce aux primitives post-quantiques (Dilithium, SPHINCS+).

— Renforcement de l'opposabilité juridique des preuves numériques.

0.29.1 Cas pratiques

— **Cyberfraude bancaire – Cameroun, 2022** : identification des cybercriminels via logs et blockchain.

— **Cyberescroquerie BEC – Yaoundé, 2021** : traçage d'e-mails falsifiés et récupération partielle des fonds.

— **Affaire SIMBOX – Cameroun, 2019** : géolocalisation des équipements frauduleux et vérification cryptographique des journaux.

— **Affaire EncroChat – Europe, 2020** : exploitation des failles de chiffrement et arrestations massives.

0.30 Positionnement dans l'investigation numérique moderne

— Les méthodes classiques (hashing, signatures simples) restent utiles mais limitées face aux menaces quantiques et exigences légales internationales.

— Les nouvelles approches (ZK-NR, CLO, primitives CASH) permettent un équilibre entre sécurité technique et recevabilité juridique.

— L'investigation numérique moderne requiert une convergence crypto-légale, garantissant la validité des preuves dans des contextes nationaux et transfrontaliers.

0.31 Conclusion

La cryptographie évolue pour devenir un instrument d'opposabilité juridique. ZK-NR, CLO et les primitives post-quantiques offrent aux enquêteurs des outils pour produire des preuves numériques vérifiables, inaltérables et légalement recevables. L'investigation numérique moderne s'inscrit ainsi dans une démarche intégrée où sécurité technique et valeur juridique convergent.

Introduction aux techniques d'investigation numérique

Thème : L'utilité de l'investigation numérique dans la police judiciaire

Option : Cybersécurité et Investigation Numérique

École Nationale Supérieure Polytechnique de Yaoundé
Département de Génie Informatique

Sous la supervision de : Ing. Thierry MINKA

Année Académique : 2025/2026

Résumé général

Ce travail porte sur l'investigation numérique et son utilité au sein de la police judiciaire au Cameroun. L'objectif est de comprendre comment la collecte, l'analyse et la préservation de preuves numériques renforcent l'efficacité des enquêtes criminelles modernes. Le document explore les apports essentiels de l'investigation numérique, ses principaux domaines d'application, les outils utilisés, ainsi que les défis et limites rencontrés dans le contexte camerounais. L'étude met en évidence son rôle stratégique dans la lutte contre la cybercriminalité, la criminalité financière, les crimes violents et la protection des enfants, tout en soulignant la nécessité de former des experts et d'adapter le cadre juridique.

0.32 Introduction

L'investigation numérique (ou digital forensic) consiste à collecter, analyser, conserver et présenter des preuves numériques issues d'ordinateurs, téléphones, réseaux ou tout autre support électronique, dans le but d'appuyer une enquête (judiciaire, administrative ou privée). Avec la digitalisation et la cybercriminalité croissante, elle devient un outil indispensable pour la police judiciaire. Cette étude analyse ses apports essentiels, ses domaines d'application ainsi que ses outils, défis et limites au Cameroun.

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

0.33.1 Accès à des preuves invisibles dans le monde physique

— Retrouver des traces difficiles à effacer : historiques de navigation, conversations supprimées, métadonnées, fichiers effacés mais récupérables.

— Complémentarité avec la scène de crime physique grâce à une "scène de crime virtuelle".

0.33.2 Lutte contre la cybercriminalité

— Résolution d'infractions comme le piratage, les ransomwares et le phishing.

— Sans investigation numérique, ces infractions resteraient très difficiles à résoudre.

0.33.3 Identification et traçage des auteurs

— Analyse des adresses IP, journaux système et connexions réseau pour remonter jusqu'au suspect.

— Récupération de données de géolocalisation et communications électroniques pour identifier auteurs et alibis.

0.33.4 Reconstitution des événements

— Chronologie numérique des fichiers créés, modifiés ou transférés.

— Horaires de connexion et actions de l'utilisateur.

— Aide à reconstruire le scénario d'un crime.

0.33.5 Apport de preuves recevables en justice

— Maintien de l'intégrité et de la traçabilité des preuves.

— Assure que les preuves numériques sont valides devant un tribunal.

0.33.6 Soutien aux enquêtes traditionnelles

— Complément des méthodes classiques : vidéosurveillance, analyse téléphonique, fouilles physiques.

— Fournit une vision globale et précise des faits.

0.34 Principaux domaines d'application

0.34.1 Lutte contre la cybercriminalité

— Piratage informatique, fraude en ligne, usurpation d'identité.

— Exemples : démantèlement de réseaux de fraude à Douala (2022), opérations de phishing ciblant des entreprises.

— Techniques : analyse des logs, récupération de données effacées, traçage des flux financiers.

0.34.2 Lutte contre la grande criminalité transfrontalière et le terrorisme

— Suivi des réseaux criminels transfrontaliers : trafic de drogues, traite d'êtres humains, terrorisme.

— Exemples : opérations conjointes avec Interpol pour arrêter des réseaux de stupéfiants et cartographie des réseaux Boko Haram.

— Techniques : analyse de métadonnées, géolocalisation, profilage de réseaux.

0.34.3 Lutte contre la criminalité financière et économique

— Détection de fraudes, corruption, blanchiment d'argent.

— Exemples : détournements de fonds publics (2021), audits numériques dans entreprises.

— Techniques : traçage des transactions, corrélation données numériques/documents physiques, data mining.

0.34.4 Lutte contre la criminalité organisée et crimes violents

— Enquêtes sur homicides, kidnappings, vols à main armée.

— Exemples : analyse de téléphones et vidéos de surveillance pour élucider des affaires complexes.

— Techniques : reconstitution chronologique, analyse vidéo, communication téléphonique.

0.34.5 Protection de l'enfance et lutte contre la pédopornographie

— Identification et neutralisation de réseaux diffusant des contenus illicites.

— Exemples : démantèlement de réseaux sur réseaux sociaux (2022) avec Interpol et Europol.

— Techniques : analyse d'images et vidéos, traçage des comptes, coopération internationale.

0.34.6 Investigation numérique dans les enquêtes judiciaires classiques

— Renforcement de la preuve même hors cybercriminalité.

— Exemples : fraude électorale, conflits fonciers détectés via données numériques.

— Techniques : analyse et authentification de documents, extraction depuis ordinateurs/serveurs, préservation des preuves.

0.34.7 Synergie avec organisations internationales et autres forces

— Collaboration pour traquer réseaux criminels transnationaux.

— Exemples : opérations Interpol Yaoundé, échanges sécurisés de données.

— Techniques : partage sécurisé de preuves, logiciels d'analyse massive, coopération inter-agences.

0.35 Outils, défis et limites

0.35.1 Principaux outils et techniques

Logiciels de récupération et d'analyse

Autopsy, FTK Imager, Cellebrite, Oxygen Forensic Detective, Mobiledit.

Investigation réseau et surveillance

Wireshark, AIL, plateformes de Lawful Interception.

Chiffrement et protection des données

Write-blockers, Hashcat, cryptanalyse légère.

0.35.2 Défis au Cameroun

— Explosion et complexité des données.

— Respect des droits fondamentaux.

— Évolution technologique et formation.

0.35.3 Limites actuelles

— Difficultés juridiques : admissibilité des preuves, harmonisation légale.

— Dépendance à l'expertise technique : pénurie d'experts, centralisation.

— Contraintes matérielles et financières : coût des équipements, maintenance.

0.36 Conclusion

L'investigation numérique est devenue un outil stratégique indispensable pour la police judiciaire camerounaise. Elle permet d'accéder à des preuves invisibles, identifier les auteurs, reconstituer les événements et soutenir la justice. Malgré les défis techniques, juridiques et financiers, son rôle reste central. L'avenir implique de renforcer la formation des experts, moderniser les équipements et anticiper les mutations technologiques, notamment l'IA, le métavers et les deepfakes, pour garantir l'efficacité des enquêtes et la sécurité nationale.