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
****

RESUME DES EXPOSES

Option :

Cybersécurité et Investigation Numérique

Rédigé par :
KALDADAK ADAMA, *24P824*

Sous l'encadrement de :
M. Thierry MINKA

Année académique 2025 / 2026

0.1 L'UTILITÉ DE L'INVESTIGATION NUMÉRIQUE DANS LA POLICE JUDICIAIRE

Le rapport met en évidence que l'investigation numérique est devenue un outil incontournable pour la police judiciaire dans la lutte contre la criminalité moderne au Cameroun. Elle permet d'accéder à des preuves invisibles, d'identifier et de tracer les auteurs d'infractions, de reconstituer les événements et d'apporter des preuves recevables en justice. Cependant, son efficacité reste limitée par le manque de formation des enquêteurs, l'insuffisance des équipements techniques et les lacunes juridiques. Pour y remédier, la solution proposée repose sur trois axes majeurs : le renforcement des capacités humaines à travers la formation continue, la modernisation des moyens techniques par l'acquisition d'outils et de laboratoires spécialisés, et l'adaptation du cadre légal afin de concilier efficacité judiciaire et respect des droits fondamentaux. Cette approche intégrée vise à faire de l'investigation numérique un véritable pilier de la sécurité et de la souveraineté numérique du Cameroun.

0.2 PRÉSENTATION DÉTAILLÉE DU PROTOCOLE ZK-NR : RL ET POSITIONNEMENT DANS L'INVESTIGATION NUMÉRIQUE MODERNE

Cet exposé présente une étude approfondie sur le protocole ZK-NR (Zero-Knowledge Non-Repudiation) et son rôle dans l'investigation numérique moderne. Il met en évidence la nécessité d'aller au-delà du simple chiffrement pour garantir la non-répudiation, c'est-à-dire la capacité d'attribuer de manière certaine une action numérique à son auteur tout en assurant la confidentialité, l'intégrité et la valeur juridique des preuves. Le travail montre que le protocole ZK-NR, associé au cadre CLO (Cryptographic Legal Opposability), constitue une solution innovante aux limites actuelles des enquêtes numériques. Grâce à l'usage des preuves à divulgation nulle de connaissance et de primitives post-quantiques (comme STARKs, Dilithium, SPHINCS+), ZK-NR permet de certifier les preuves sans révéler les données sensibles, de sceller cryptographiquement la chaîne de possession et d'assurer une opposabilité juridique vérifiable devant les tribunaux. Cette approche offre ainsi une traçabilité inaltérable et une résistance aux futures menaces quantiques. L'exposé conclut que l'intégration de tels mécanismes cryptographiques dans l'investigation numérique représente une avancée majeure : elle renforce la crédibilité des preuves, sécurise les procédures judiciaires et rapproche la cryptographie de la sphère légale. ZK-NR et CLO ouvrent ainsi la voie à une nouvelle génération d'enquêtes numériques fondées sur la preuve vérifiable, confidentielle et juridiquement opposable.

0.3 Les dix cas Africain les plus important d'haking durant les 10 dernière sannées

Ce rapport dresse un panorama des **dix cas de cyberattaques les plus marquants survenues en Afrique entre 2015 et 2025**, en mettant en évidence les **failles systémiques** et la nécessité d'un renforcement de la **cybersécurité** et de l'**investigation numérique** sur le continent. Il montre que la numérisation rapide de l'Afrique, bien qu'elle favorise le développement économique, a accru la vulnérabilité des infrastructures critiques (banques, énergie, santé, transport, télécoms). Les attaques — telles que le *ransomware sur Transnet* (Afrique du Sud), la *fuite*

massive de données de la CNSS (Maroc), ou l'*intrusion sur Eneo* (Cameroun) — ont causé des pertes financières majeures et révélé des carences en formation, en outils de défense et en législation.

Face à ces menaces, **la solution proposée** par le rapport repose sur une approche continentale intégrée :

— **Former massivement les experts africains** en cybersécurité et investigation numérique ;
— **Créer des centres régionaux CERT/CSIRT** capables de coopérer en temps réel ;
— **Harmoniser les lois** à travers la Convention de Malabo pour renforcer le cadre juridique ;
— **Développer un cloud souverain africain** afin d'assurer l'hébergement et la protection locale des données ;
— **Renforcer la gouvernance numérique** dans les institutions publiques et les entreprises privées.

En conclusion, l'Afrique ne pourra bâtir un avenir numérique stable qu'en faisant de la **cybersécurité** et de l'**investigation numérique** des priorités stratégiques, garantissant ainsi sa **souveraineté technologique** et la **sécurité durable de son espace numérique**.

0.4 LES TROIS MEILLEURS LOGICIELS DE RÉDACTION DE MÉMOIRE

Ce document présente une analyse comparative des trois meilleurs logiciels pour la rédaction de mémoires universitaires : Overleaf, Microsoft Word et Zotero. Overleaf, fondé en 2012 et désormais propriété de Springer Nature, se distingue par sa qualité typographique professionnelle, sa collaboration en ligne et son intégration LaTeX, bien qu'il exige une certaine maîtrise technique. Word reste l'outil le plus accessible et universel, apprécié pour sa compatibilité et ses fonctions de mise en forme, mais limité en gestion bibliographique. Zotero, gestionnaire open-source, complète ces deux outils en offrant une gestion rigoureuse, automatique et gratuite des références bibliographiques. L'étude recommande l'association Overleaf + Zotero pour un équilibre optimal entre rigueur scientifique et efficacité, tout en rappelant que la maîtrise des outils doit toujours servir la qualité intellectuelle du travail.

0.5 Points sur les algorithmes de reconnaissance faciale

La reconnaissance faciale est une technologie d'intelligence artificielle utilisée pour identifier ou vérifier une personne à partir de ses traits du visage. Elle constitue un outil précieux pour l'investigation numérique et les enquêtes judiciaires, car elle permet de traiter rapidement de grandes quantités d'images et de vidéos. Toutefois, malgré sa rapidité et sa précision, elle présente des limites liées à la fiabilité des algorithmes, à la protection des données biométriques et aux risques d'atteinte à la vie privée. Pour un usage sûr et efficace, il est recommandé de mettre en place un cadre juridique clair, de renforcer la sécurité des systèmes (anti-usurpation, chiffrement, tests réguliers) et de garantir une supervision humaine et éthique. Bien encadrée, la reconnaissance faciale peut devenir un atout majeur pour la cybersécurité et la justice au Cameroun.

0.6 DeepFake vocal

Les deepfakes audios, produits par l'intelligence artificielle, ont des usages à la fois légitimes et malveillants. Ils peuvent servir à aider les personnes privées de parole, au doublage audiovisuel ou

à la conservation de voix, mais aussi être utilisés pour des fraudes, de l'usurpation d'identité ou la falsification de preuves. Ces manipulations menacent la confidentialité, la fiabilité et l'opposabilité des enregistrements dans les enquêtes numériques. Le cas de MINIMAX Audio illustre ce double visage : outil innovant pour l'éducation et le divertissement, il présente aussi des risques sécuritaires et éthiques. Pour y faire face, il est nécessaire de développer des outils de détection, de renforcer la réglementation et la sensibilisation, et de promouvoir une éthique de l'IA. Enfin, la mise en place d'une boîte à outils pour les investigateurs numériques est essentielle afin d'améliorer la détection, l'analyse et la fiabilité des preuves audio.

0.7 Simulation d'une serie de messages sur WhatsApp entre un homme et sa maitresse

Ce devoir met en évidence, à travers une simulation d'échanges WhatsApp falsifiés, la facilité avec laquelle il est possible de créer de fausses preuves numériques à l'aide d'outils tels que Chatsmock et Adobe Photoshop. Dans le scénario étudié, une conversation simulant une relation entre un enseignant et une étudiante a été fabriquée pour illustrer les risques liés à la manipulation de données numériques. L'expérience montre que, bien que ces outils soient simples et efficaces, ils compromettent la fiabilité des captures d'écran utilisées comme preuves judiciaires. Leur usage rend la distinction entre données authentiques et falsifiées difficile, augmentant ainsi le risque de fraude et de manipulation. Le rapport recommande donc de renforcer les méthodes de vérification technique (analyse des métadonnées, signatures numériques), de former les acteurs judiciaires à détecter les falsifications, et de privilégier les données brutes issues directement des appareils ou serveurs. En conclusion, cette étude souligne la nécessité d'un encadrement rigoureux et d'une vigilance accrue dans l'investigation numérique afin de garantir la fiabilité et l'intégrité des preuves dans un contexte où la falsification devient de plus en plus accessible.

0.8 CONCEPTION ET ANALYSE D'UN FAUX PROFIL TIKTOK : CHOIX D'UNE NICHE DANS LE CADRE D'UNE INVESTIGATION NUMÉRIQUE

Ce rapport présente une investigation numérique menée dans un cadre pédagogique à travers la création d'un faux profil TikTok consacré à la cybersécurité. L'objectif était d'analyser les réactions des utilisateurs, de comprendre les mécanismes de viralité et de sensibiliser à la sécurité numérique tout en respectant les principes éthiques. À l'aide d'outils tels que ChatGPT, Canva, Temp Mail et les statistiques internes de TikTok, l'équipe a conçu un contenu éducatif et attractif, abordant des thèmes comme la protection des mots de passe, les arnaques en ligne et la gestion des données personnelles. Les résultats ont montré un bon engagement du public et un intérêt réel pour la thématique. Toutefois, le projet souligne aussi les risques éthiques liés à l'usage de faux profils, même à des fins éducatives, et la nécessité d'un cadre clair pour éviter toute dérive. En conclusion, cette expérience démontre que les réseaux sociaux peuvent être des outils puissants de sensibilisation à la cybersécurité, à condition que leur utilisation reste responsable, encadrée et conforme aux valeurs éthiques et légales.