ÉCOLE NATIONALE SUPERIEURE POLYTECHNIQUE
DE YAOUNDÉ

DEPARTEMENT DE GENIE INFORMATIQUE

INTRODUCTION AUX TECHNIQUES
D'INVESTIGATION NUMERIQUE

---

# RESUME DES EXPOSES

---


MAKEU TENKU STELY BELVA
CIN-4

*Superviseur :* M. THIERRY
MINKA

2025-2026

# Table des matières

# I POINTS SUR LES ALGORITHMES DE RECONNAISSANCE FACIALE

La reconnaissance faciale est une technologie d'intelligence artificielle (IA) qui identifie les individus en analysant leurs traits biométriques uniques (distance des yeux, forme du nez). L'exposé commence par détailler les fondements techniques de cette technologie, notamment l'architecture des systèmes biométriques et les méthodes algorithmiques employées pour détecter et comparer les visages (méthodes classiques et points d'intérêt).

Bien que cette technologie soit un outil puissant pour l'investigation numérique, permettant de traiter de grands volumes d'images dans les enquêtes judiciaires et la cybersécurité, son utilisation soulève de sérieux enjeux éthiques, sociétaux et juridiques. Les avantages en termes de sécurité et d'efficacité sont contrebalancés par des risques de faux positifs, d'atteintes à la vie privée, de discrimination et de vulnérabilités aux tentatives de dissimulation.

Par conséquent, l'efficacité réelle de la reconnaissance faciale est conditionnée par un encadrement strict. L'exposé met en lumière la nécessité absolue de mettre en œuvre des recommandations claires : une supervision technique continue, un cadre juridique actualisé et l'application stricte des principes de proportionnalité et de transparence. En définitive, pour le Cameroun, cette technologie ne peut devenir un atout majeur que si elle est gérée par une gouvernance adaptée qui concilie l'innovation sécuritaire avec le respect fondamental des droits humains.

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

L'exposé explore l'évolution cruciale de la cryptographie, passant d'un simple outil de confidentialité des communications à un instrument de preuve légale dans l'ère numérique. La protection par chiffrement asymétrique, si elle empêche l'interception, s'avère insuffisante pour garantir l'authenticité et la non-répudiation d'un échange, créant ainsi un Trilemme fondamental ( CRO ) entre Confidentitalité, Fiabilité et Opposabilité, qui compromet la recevabilité des preuves devant les tribunaux. Ce défi est adressé par une approche intégrée qui repose sur une Fondation Cryptographique (AIIP) résiliente aux attaques quantiques et sur des primitives spécifiques : la CEE assure la confidentialité sémantique, l'AOW garantit la fiabilité temporelle des données, et la SH offre l'explicabilité institutionnelle nécessaire à l'admissibilité juridique.

Ces primitives sont orchestrées au sein de l'Architecture Q2CSI (Fer-Or-Argile) et appliquées concrètement par le protocole ZK-NR (Zero-Knowledge Non-Repudiation), encadré par CLO. Ces innovations permettent de générer des attestations vérifiables grâce aux preuves à divulgation nulle de connaissance (ZKP), prouvant la validité d'une information sans révéler les données sensibles associées. En certifiant cryptographiquement la chaîne de possession, l'investigation numérique moderne ne se contente plus de collecter, mais produit des preuves inaltérables et incontestables, faisant de la cryptographie le garant de la vérité numérique indispensable à la justice et à la cybersécurité.

# III Deepfake Vocal

Le deepfake vocal est une prouesse technologique issue de l'intelligence artificielle (IA) et du Deep Learning, capable de cloner ou d'imiter la voix humaine avec un réalisme quasi indiscernable à partir de quelques échantillons audio. Initialement développée pour des usages bénéfiques comme l'accessibilité, le doublage ou les assistants vocaux, cette innovation est devenue une menace insidieuse. La voix étant le vecteur de l'identité et de la crédibilité, sa falsification fragilise la confiance dans les communications numériques. L'exposé met en lumière des cas concrets d'utilisation malveillante, notamment l'usurpation d'identité, la fraude financière (par imitation de dirigeants, comme l'illustre l'exemple de MINIMAX audio) et la manipulation de l'opinion publique par la diffusion de faux discours. Le deepfake vocal ouvre ainsi la voie à des menaces hybrides complexes, remettant en question l'authenticité des preuves audio dans des domaines critiques comme la justice et les enquêtes criminelles.

Face à l'ampleur de ces enjeux éthiques, juridiques et sécuritaires, l'investigation numérique doit impérativement s'adapter. L'objectif n'est plus seulement de comprendre comment ces contenus sont produits, mais de développer des méthodes de riposte et de traçabilité. Il est crucial de mettre au point des outils de détection fiables pour identifier les sons générés par l'IA et de renforcer les cadres légaux pour criminaliser l'usage frauduleux de cette technologie. L'exposé conclut qu'il y a une responsabilité collective qui incombe aux chercheurs, ingénieurs et instances de régulation pour encadrer le deepfake vocal. En promouvant une éthique de l'intelligence artificielle et une vigilance accrue, il est possible d'orienter cette technologie puissante vers des usages bénéfiques, tout en préservant l'intégrité des preuves numériques et la confiance sociale.

# IV LES 10 CAS AFRICAINS LES PLUS IMPORTANTS D'HACKING DURANT LES 10 DERNIERES ANNÉES

L'Afrique est au cœur d'une révolution numérique qui, tout en stimulant la croissance des économies et des fintechs, a engendré une hausse vertigineuse des cyberattaques. Selon INTERPOL (2024), le continent est aujourd'hui confronté à plus de 3 000 attaques hebdomadaires par organisation, soit une augmentation de $300\%$ en dix ans. Ces attaques ciblent des secteurs vitaux, allant des administrations publiques aux infrastructures stratégiques (énergie, finance), entraînant des pertes économiques massives, des atteintes à la réputation et la paralysie de services essentiels. Face à cette menace systémique, l'investigation numérique s'impose comme un pilier crucial pour collecter, analyser et présenter les preuves d'attaques dans un cadre à la fois légal et scientifique.

Ce travail analyse en profondeur dix cas africains emblématiques de hacking survenus entre 2015 et 2025. Ces incidents ont été sélectionnés selon quatre critères rigoureux (taille, type d'organisation visée, volume de données affectées, conséquences financières et réputationnelles) pour mettre en lumière les faiblesses structurelles du cyberespace africain.

Les cas étudiés illustrent la diversité et la gravité des menaces :

Cyber-Espionnage et Attaques Financières Majeures : Le Piratage de la Banque Centrale du Nigeria (2015-2016), impliquant le système SWIFT et des dizaines de millions de dollars, et la Fraude au Mobile Money de MTN Nigeria (2018) (8 M USD détournés) démontrent les vulnérabilités du secteur financier. L'attaque sur Ethiopian Airlines (2023) (5 M USD d'impact) souligne, quant à elle, les risques d'espionnage industriel.

Attaques sur Infrastructures Critiques et Services Publics : L'attaque par Ransomware sur Transnet (Afrique du Sud, 2021), la Breach de la CNSS (Maroc, 2025), l'attaque sur Eneo (Cameroun, 2024), et la cyberattaque sur les systèmes de santé Tunisiens (2021) (2,5 M USD de pertes de service) mettent en évidence la vulnérabilité des services vitaux et des infrastructures clés face aux rançongiciels et aux attaques DDoS.

Menaces Sophistiquées et Ciblage Politique : Le scandale Pegasus au Maroc (2020-2021) et l'attaque par GhostLocker 2.0 (Égypte, 2024) montrent la montée des outils d'espionnage d'État et des rançongiciels à double extorsion. Enfin, le Piratage des banques ivoiriennes illustre les attaques coordonnées et ciblées sur des institutions financières régionales.

En analysant ces cas, l'exposé conclut sur l'urgence d'une refonte complète de la cybersécurité nationale pour garantir la continuité des services et la confiance dans la révolution numérique africaine.

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

L'exposé présente une investigation numérique menée sur TikTok dans un cadre strictement pédagogique, visant à décrypter les enjeux de l'identité numérique, de la viralité et de la manipulation de l'information. L'approche a consisté à créer un faux profil fictif centré sur le thème de la cybersécurité. L'objectif principal était d'analyser les types d'interactions et les réactions générées par ce contenu ciblé, tout en explorant les limites entre l'authenticité et la fiction sur cette plateforme incontournable, particulièrement influente auprès des jeunes. Ce travail a été réalisé en respectant des principes éthiques rigoureux, excluant toute usurpation réelle ou atteinte à autrui, pour garantir la responsabilité numérique de la démarche.

Cette expérience concrète a démontré la puissance des réseaux sociaux comme vecteurs de sensibilisation à la cybersécurité. En exploitant des outils et des stratégies de contenu propres à TikTok, le projet a réussi à toucher un public réel et à prouver que les messages de prévention peuvent circuler efficacement et de manière interactive. L'exercice a également souligné l'impératif d'une approche éthique, encadrée et réfléchie dans l'utilisation de ces plateformes. En somme, cette investigation souligne que la maîtrise des outils digitaux, associée à une conscience critique de leurs impacts potentiels, est aujourd'hui fondamentale pour tout acteur du numérique, permettant une éducation à la cybersécurité plus impactante et proche des réalités du terrain.

# VI L'UTILITÉ DE L'INVESTIGATION NUMÉRIQUE DANS LA POLICE JUDICIAIRE

L'investigation numérique (digital forensic) s'est imposée comme un outil indispensable pour la police judiciaire, notamment dans le contexte camerounais, face à une criminalité qui a massivement migré vers le numérique. Elle va au-delà de la simple collecte de données pour permettre d'accéder à des preuves invisibles, d'identifier les auteurs de crimes et de reconstituer des événements avec une précision inédite. Ses apports sont essentiels, couvrant un large éventail d'applications allant de la lutte contre la cybercriminalité (fraudes, hacking) à la résolution des crimes violents et au démantèlement des réseaux transnationaux, illustrant son utilité opérationnelle dans de multiples affaires. Ainsi, la discipline est passée d'une compétence spécialisée à un pilier fondamental de toute enquête criminelle moderne, essentiel à la sécurité nationale et à l'efficacité de la justice.

Cependant, l'efficacité maximale de cet atout majeur se heurte à des défis et limites substantielles. L'explosion du volume de données, la complexité technique croissante (IA, métavers, deepfakes) et les contraintes juridiques constituent des obstacles permanents. De plus, le Cameroun fait face à des limites matérielles et humaines notables, incluant la pénurie d'experts formés et le coût élevé des équipements spécialisés. Pour consolider ses acquis et anticiper les défis de l'ère post-quantique, il est impératif d'investir massivement dans la formation continue, de renforcer les moyens logistiques des unités spécialisées et d'adapter en permanence le cadre juridique. L'investigation numérique n'est donc pas une option, mais un élément stratégique dont la maîtrise déterminera le succès du pays dans la lutte contre la criminalité de demain.

# VII LES TROIS MEILLEURS LOGICIELS DE RÉDACTION DE MÉMOIRE

La rédaction d'un mémoire est un défi académique majeur, confrontant l'étudiant à la gestion fastidieuse des sources, au respect des normes formelles et à la structuration d'un contenu complexe. Le choix d'outils logiciels efficaces est donc crucial. Un logiciel idéal doit offrir un environnement de rédaction adapté aux longs documents (que ce soit LATEX ou un traitement de texte), garantir une gestion rigoureuse des références, et faciliter la mise en forme académique. Pour répondre à la question des outils les plus performants, l'analyse s'est concentrée sur trois solutions spécialisées et complémentaires : Overleaf pour son environnement LATEX professionnel, Microsoft Word comme traitement de texte universel, et Zotero en tant que gestionnaire de références bibliographiques indispensable.

L'analyse démontre que la réussite repose sur la combinaison stratégique des atouts de chaque outil. Overleaf excelle par sa qualité typographique irréprochable et son approche structurante, idéale pour les documents complexes comme les thèses et mémoires de master. Microsoft Word conserve son avantage indéniable en matière d'accessibilité et de prise en main immédiate. Quant à Zotero, il apporte la rigueur scientifique nécessaire en automatisant la gestion des références avec une précision inégalée. La recommandation principale s'oriente vers la synergie Overleaf + Zotero, qui offre le meilleur équilibre entre qualité professionnelle, rigueur scientifique et efficacité. Toutefois, l'exposé met en garde contre la négligence du fond au profit de la forme : la maîtrise technique des outils ne doit jamais éclipser la substance intellectuelle et la profondeur de la recherche.

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

L'exposé porte sur une investigation numérique pratique visant à évaluer la fiabilité des preuves issues des applications de messagerie instantanée, en particulier WhatsApp, dans un contexte d'enquête. Le travail a consisté à simuler une série de messages échangés entre deux individus en utilisant deux outils spécifiques : Chatsmock pour la génération de la fausse conversation, et Adobe Photoshop pour l'affinage et la personnalisation de l'apparence. L'objectif de cette simulation, menée sans jugement moral sur le contenu fictif, était d'illustrer les possibilités techniques de falsification offertes par ces logiciels et, par extension, de questionner la fiabilité des captures d'écran comme preuves numériques dans les affaires judiciaires ou privées.

L'expérience a démontré de manière éloquente la facilité déconcertante avec laquelle il est possible de créer des preuves numériques trompeuses. Ce constat met en évidence la fragilité des éléments de preuve basés sur la simple apparence des échanges. L'étude souligne un double impératif pour la discipline : d'une part, reconnaître les menaces que ces falsifications représentent pour la crédibilité des investigations numériques ; d'autre part, insister sur la nécessité pour les experts judiciaires d'adopter des méthodes de vérification rigoureuses et avancées. L'investigation numérique ne peut plus se contenter de l'analyse apparente des données, elle doit intégrer la sensibilisation et la vérification technique approfondie pour garantir l'intégrité et la fiabilité des preuves dans un environnement numérique où la manipulation est de plus en plus accessible.

# IX Deepfake

Ce rapport présente un projet académique réalisé dans le cadre du cours d'Introduction aux Techniques d'Investigation Numérique à l'École Nationale Supérieure Polytechnique de Yaoundé. L'objectif principal consiste à créer une vidéo pédagogique utilisant l'intelligence artificielle, dans laquelle le chef de groupe dispense le premier chapitre du cours portant sur les deepfakes. Le travail s'articule autour de trois axes principaux. Premièrement, une présentation théorique des deepfakes, définis comme des contenus audio ou vidéo créés ou modifiés par intelligence artificielle, basés sur la technologie GAN (Generative Adversarial Networks) développée par Ian Goodfellow en 2014. Cette section aborde également les inconvénients liés à ces technologies et les initiatives réglementaires en cours, notamment celles de Facebook et de la CNIL. Deuxièmement, une description détaillée des outils utilisés : GPT-5, modèle d'intelligence artificielle d'OpenAI capable de générer des textes structurés et cohérents, et HeyGen AI, plateforme spécialisée dans la génération de vidéos par IA offrant des avatars réalistes, des voix synthétiques dans plus de 175 langues, et une traduction multilingue avec synchronisation labiale. Troisièmement, la méthodologie de réalisation suivant un processus en quatre étapes : sélection d'un template vidéo, choix d'un avatar, rédaction du script avec GPT-5, et génération finale avec HeyGen. En conclusion, ce projet démontre le potentiel considérable de l'IA générative dans la création de contenus pédagogiques immersifs, tout en soulignant l'importance d'une réflexion éthique sur l'utilisation responsable de ces technologies face aux risques d'abus et aux enjeux de désinformation.