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 OF ENGINEERING OF YAOUNDÉ
****

DEPARTMENT OF COMPUTER ENGINEERING
****

RESUME DES DIFFERENTS EXPOSES

NOM ET PRÉNOM
AYONNEME TIOBOU Varese

MATRICULE
22P045

SPÉCIALITÉ
HN-4 CIN

EXAMINATEUR : Mr MINKA Thierry

Année Académique : 2025/2026

Contents

1. LES TROIS MEILLEURS LOGICIELS DE RÉDACTION DE MÉMOIRE

Ce document compare trois outils essentiels pour la rédaction académique : Overleaf, Microsoft Word et Zotero. L'objectif est d'identifier les logiciels les plus adaptés à la réalisation d'un mémoire universitaire, en tenant compte de leurs forces, limites et synergies possibles.

1.1. Overleaf : Excellence académique par LaTeX

- Éditeur LaTeX en ligne collaboratif, fondé en 2012
- Idéal pour les disciplines scientifiques (maths, physique, informatique)
- Atouts : qualité typographique exceptionnelle, gestion avancée des références croisées, modèles académiques
- Limites : courbe d'apprentissage élevée, édition hors ligne limitée

1.2. Microsoft Word : Le référentiel en traitement de texte

- Outil universel, interface familière
- Atouts : gestion des styles, génération automatique des tables, suivi des modifications
- Limites : gestion bibliographique basique, risques d'instabilité sur les longs documents

1.3. Zotero : Le spécialiste de la bibliographie

- Gestionnaire de références open-source et gratuit
- Fonctionnalités clés : capture automatique des métadonnées, intégration avec Word/Overleaf, synchronisation cloud
- Support de milliers de styles de citation (APA, MLA, Chicago, etc.)

1.4. Combinaisons performante

- **Word + Zotero** : Solution accessible pour débutants et sciences humaines
- **Overleaf + Zotero** : Excellence académique pour sciences exactes et recherche
- **Overleaf + Zotero Groups** : Collaboration avancée pour travaux d'équipe et thèses

Aucun outil seul ne couvre tous les besoins d'un mémoire. La combinaison **Overleaf + Zotero** est recommandée pour son équilibre entre qualité professionnelle et rigueur scientifique. Word reste pertinent pour son accessibilité, tandis que Zotero est indispensable pour la gestion bibliographique. L'essentiel reste de trouver l'équilibre entre maîtrise des outils et qualité du contenu intellectuel.

2. les 10 cas Africain les plus iportants d'Hacking durant les 10 dernieres annees

une montée exponentielle des attaques informatiques est observée en Afrique — plus de 3 000 par semaine et par organisation selon INTERPOL (2024). Ces attaques visent aussi bien les entreprises que les institutions publiques, entraînant des pertes économiques, des atteintes à la réputation et la fuite de données sensibles. L'investigation numérique y est présentée comme un pilier essentiel pour collecter et analyser les preuves dans un cadre légal et scientifique.
Le contexte général révèle une cybersécurité encore fragile, marquée par la faible maturité institutionnelle, le manque d'experts, des infrastructures obsolètes et une dépendance aux prestataires étrangers. Cependant, certains pays (Maroc, Cameroun, Nigéria, Afrique du Sud) amorcent une transformation vers une cybersouveraineté régionale.
La méthodologie d'investigation repose sur cinq étapes : identification, collecte, préservation, analyse et rapport des incidents. Les cas étudiés ont été sélectionnés selon quatre critères : taille de l'attaque, type d'organisation, volume de données compromises et impact financier/réputationnel. Les dix cas emblématiques présentés sont :

1. Transnet (Afrique du Sud, 2021) – Attaque par ransomware BlackMatter paralysant les ports, pertes estimées à 60 M USD.

2. CNSS (Maroc, 2025) – Fuite massive de données personnelles de 2 M de salariés et 500 000 entreprises.

3. Eneo (Cameroun, 2024) – Perturbation des systèmes de facturation et services clients ; pertes de plusieurs centaines de millions de FCFA.

4. GhostLocker 2.0 (Égypte, 2024) – Attaque coordonnée sur 30 organisations industrielles, pertes estimées à 20 M USD.

5. Scandale Pegasus (Maroc, 2020–2021) – Cas d'espionnage numérique impliquant des logiciels de surveillance. 6. Banques ivoiriennes – Piratage via phishing et chevaux de Troie, pertes de 6 M €.

6. Systèmes de santé tunisiens (2021) – Attaque DDoS et ransomware paralysant des hôpitaux, pertes de 2,5 M USD.

7. Ethiopian Airlines (2023) – Fuite des données personnelles de passagers, pertes de 5 M USD.

8. MTN Nigeria (2018) – Fraude au Mobile Money entraînant un détournement de 8 M USD.

9. Banque centrale du Nigeria (2015–2016) – Intrusion sur le réseau SWIFT, pertes de plusieurs dizaines de millions de dollars.

Les recommandations prônent la formation massive d'experts africains, la création de centres régionaux (CERT/CSIRT), l'harmonisation des lois, le développement d'un cloud souverain, des audits réguliers et la mise en place de fonds de cyber-résilience.
En somme, l'Afrique se trouve à un tournant décisif : la cybersécurité doit devenir une responsabilité partagée entre États, entreprises et citoyens. Le renforcement des capacités d'investigation numérique et la souveraineté technologique sont présentés comme des conditions indispensables pour un développement numérique durable et sécurisé.

3. Deepfake Vocal

le phénomène du **deepfake vocal**, une application de l'intelligence artificielle (IA) permettant d'imiter ou de recréer une voix humaine avec un réalisme saisissant. S'appuyant sur des modèles d'apprentissage profond, cette technologie soulève des enjeux considérables en matière de sécurité, d'éthique et de fiabilité des preuves numériques.

Le deepfake audio consiste à produire des sons artificiels imitant la voix d'un individu à partir d'échantillons réels. Son évolution s'étend des premiers vocodeurs (1930–1990) à la révolution du deep learning en 2016 avec **WaveNet** (DeepMind) et des outils comme **Adobe VoCo** et **Lyrebird**. Depuis 2019, la démocratisation de modèles open-source tels que *Real-Time-Voice-Cloning* a facilité son usage, parfois à des fins frauduleuses.

Deux grandes catégories d'usage se distinguent :

- **Applications légitimes** : accessibilité vocale pour les personnes muettes, doublage multilingue, assistants virtuels réalistes, ou préservation de voix historiques.
- **Applications malveillantes** : escroqueries financières, usurpations d'identité, désinformation politique, et falsification de preuves judiciaires.

Le deepfake vocal remet ainsi en question la crédibilité des enregistrements utilisés comme éléments de preuve dans les enquêtes numériques.

L'apparition de voix clonées fragilise le **trilemme CRO** :

- **Confidentialité** : risque de divulgation ou d'utilisation non consentie d'enregistrements vocaux.
- **Fiabilité** : les preuves audio deviennent falsifiables et perdent leur valeur probatoire.
- **Opposabilité juridique** : la difficulté à démontrer l'authenticité d'un enregistrement réduit sa recevabilité devant un tribunal.

La transparence des méthodes de détection et la compréhension du fonctionnement des modèles IA deviennent indispensables pour les experts en cyberenquête.

Le rapport illustre la création d'un deepfake vocal à l'aide de la plateforme **MINIMAX Audio**, un outil d'IA basé sur le deep learning. Après l'étape de *Voice Cloning*, l'utilisateur peut générer un discours artificiel via la fonction *Text to Speech*. Le rendu obtenu est quasi indiscernable de la voix réelle. Ce cas pratique met en évidence :

- le potentiel pédagogique et d'accessibilité de ces technologies ;

- mais aussi les risques d'usurpation d'identité, de fraude et de désinformation.

Des cas réels d'arnaques (Forbes 2019, MIT Tech Review 2022) montrent l'ampleur de la menace mondiale.

Les mesures de riposte reposent sur quatre axes :

1. **Détection technologique** : analyse des signatures acoustiques et anomalies dans les spectrogrammes.
2. **Sensibilisation et formation** : éducation des utilisateurs et renforcement de la vigilance en entreprise.
3. **Cadre légal et marquage numérique** : lois encadrant la création de contenus synthétiques et obligation de *watermarking*.
4. **Sécurisation et éthique de l'IA** : adoption de protocoles d'authentification vocale robustes et respect du consentement.

Le deepfake vocal symbolise une avancée technologique majeure mais aussi un défi pour la cybersécurité. S'il offre des opportunités dans l'éducation et le divertissement, il menace la fiabilité des preuves numériques et la confiance sociale. Seule une approche combinant **technologie de détection**, **réglementation**, et **éthique de l'IA** permettra d'en exploiter les bénéfices sans compromettre la sécurité.

4. Deepfake Video

Ce projet explore l'utilisation de l'intelligence artificielle générative pour créer des contenus vidéo pédagogiques. L'objectif était de réaliser une vidéo sur le thème des deepfakes en combinant GPT-5 pour la rédaction du script et HeyGen AI pour la génération vidéo.

Les Deepfakes

- **Définition** : Contenu vidéo ou audio créé/modifié par IA (contraction de "Deep Learning" et "Fake")
- **Origine** : Technique des GAN (Generative Adversarial Networks) inventée par Ian Goodfellow en 2014
- **Fonctionnement** : Deux algorithmes s'entraînent mutuellement - l'un crée des contrefaçons, l'autre les détecte

Enjeux et Avenir

- **Risques** : Propagation rapide sur les réseaux sociaux, atteinte à la vie privée et au droit à l'image
- **Contrôles** : Projet de "désidentification" par Facebook, cadre législatif par la CNIL
- **Éthique** : Nécessité d'équilibrer innovation et protection des individus

Outils Utilisés HeyGen AI

- Plateforme de génération vidéo par IA (créée en 2022)
- Transforme du texte en séquences audiovisuelles réalistes
- Applications : création de contenu, communication d'entreprise, enseignement
- Fonctionnalités clés :
  - Avatars parlants ultra-réalistes
  - Clonage vocal et bibliothèque de 300+ voix
  - Traduction multilingue avec synchronisation labiale
  - Templates et intégrations avancées

GPT-5

- Modèle d'IA générative d'OpenAI (sorti en août 2025)
- Capacités unifiées : raisonnement avancé + réponses rapides
- Utilisation : génération du script pédagogique sur les deepfakes
- Avantages : fiabilité améliorée, moins d'hallucinations, contexte étendu

Méthodologie de Création

1. **Script** : Génération du contenu pédagogique avec GPT-5 basé sur le cours
2. **Préparation** : Création de prompts précis pour HeyGen
3. **Production** :
   - Sélection d'un template vidéo
   - Choix d'un avatar parlant
   - Personnalisation de la voix et du ton
   - Ajout des ressources complémentaires
4. **Génération** : Production de la vidéo finale en quelques minutes

Cette expérience démontre le potentiel des outils d'IA générative pour la création de contenus pédagogiques réalistes. La combinaison GPT-5/HeyGen offre des possibilités innovantes mais soulève également des questions importantes concernant les limites techniques, les risques d'abus et les enjeux éthiques liés à l'utilisation des deepfakes et des technologies similaires.

5. CONCEPTION ET ANALYSE D'UN FAUX PROFIL TIKTOK

L'objectif est d'étudier les dynamiques de l'identité numérique et de la sensibilisation à la cybersécurité à travers la création contrôlée d'un faux profil sur TikTok. ce travail met en avant le rôle croissant des réseaux sociaux dans la formation des opinions et la propagation d'informations. Le projet s'inscrit dans une démarche éthique et pédagogique visant à comprendre les risques de manipulation et à promouvoir la responsabilité numérique.
La démarche méthodologique comprend quatre étapes principales :

- Création du faux profil à l'aide d'une adresse temporaire pour préserver l'anonymat.
- Choix de la niche centrée sur la cybersécurité, domaine à la fois éducatif et d'actualité.
- Stratégie de contenu axée sur la sensibilisation aux bonnes pratiques numériques (sécurité des mots de passe, arnaques en ligne, Wi-Fi public) à travers des vidéos courtes et visuels attractifs.
- Outils et suivi utilisant TikTok Analytics, captures d'écran, ChatGPT, Canva et un tableau de bord pour l'observation des interactions.

L'analyse montre que la stratégie déployée — à la fois ludique, informative et cohérente — a généré un fort engagement des utilisateurs, tout en respectant les principes éthiques. Le profil « Innotrends25 » a reçu plus de 100 mentions « j'aime » et suscité une participation réelle. Cependant, le rapport souligne les limites éthiques inhérentes à la création de faux profils, même à but pédagogique.
Les recommandations insistent sur l'importance de l'éducation à la cybersécurité dès le secondaire, d'un encadrement légal pour ce type d'exercices, et de la collaboration entre disciplines (informatique, droit, communication). En conclusion, cette expérience démontre que la sensibilisation à la cybersécurité peut être à la fois interactive et impactante grâce aux réseaux sociaux, à condition qu'elle reste strictement encadrée par une approche éthique et responsable.

6. Points sur les algorithmes de reconnaissance faciale

la reconnaissance faciale (RF) est defini comme une méthode d'identification biométrique reposant sur l'analyse des traits du visage. Elle fonctionne selon trois étapes : l'enrôlement, l'identification et la vérification, et s'appuie sur une architecture comportant quatre modules : acquisition, extraction de caractéristiques, correspondance et décision.
Les méthodes de reconnaissance se divisent en approches classiques (PCA, LDA, SVM, réseaux de neurones), locales (HMM, EBGM) et hybrides (combinaisons de modèles globaux et locaux), complétées par des détecteurs/descripteurs de points d'intérêt (SIFT, SURF, HOG).
les avantages et limites : rapidité et automatisation, mais aussi problèmes de fiabilité, de biais, de sécurité et de respect de la vie privée. Les vulnérabilités majeures concernent les

attaques adversariales, la protection des données biométriques et les risques d'usurpation (deepfakes). Sur le plan éthique, les enjeux liés à la vie privée, aux discriminations algorithmiques et aux effets sociétaux sont cruciaux. Le document souligne également les contraintes juridiques (base légale, responsabilité, traçabilité) et organisationnelles (coûts, infrastructure, acceptabilité).
des recommandations pour un usage responsable de la reconnaissance faciale : documentation technique, tests locaux, chiffrement des données, contrôles anti-usurpation, audits de biais, conformité à la législation camerounaise sur les données personnelles, formation des opérateurs et supervision humaine systématique. En conclusion, la reconnaissance faciale est présentée comme un outil puissant mais à double tranchant : utile pour la cybersécurité et les enquêtes judiciaires, mais nécessitant un encadrement rigoureux, une gouvernance transparente et une proportionnalité stricte pour préserver les droits fondamentaux.

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

ce travail présente le protocole **ZK-NR (Zero-Knowledge Non-Repudiation)** et son rôle dans la modernisation de l'investigation numérique à l'ère post-quantique. Il s'articule autour de la non-répudiation numérique, un principe garantissant qu'un émetteur ne puisse nier avoir envoyé un message, et qu'un récepteur ne puisse contester l'avoir reçu.

La non-répudiation constitue un pilier de la sécurité informatique et juridique. Elle repose sur divers outils cryptographiques : signatures numériques, certificats électroniques, horodatage et fonctions de hachage. Ces mécanismes assurent l'authenticité, l'intégrité et la traçabilité des données échangées, renforçant ainsi la confiance dans les transactions électroniques.

Les travaux récents introduisent des architectures cryptographiques post-quantiques intégrant la **confidentialité**, la **fiabilité** et l'**opposabilité juridique**. Le **trilemme CRO** démontre l'impossibilité de satisfaire pleinement ces trois critères simultanément. Le protocole **ZK-NR** tente d'équilibrer ces dimensions en combinant des primitives comme les **STARKs**, **Dilithium** et les signatures à seuil, offrant des preuves vérifiables sans divulguer les données sensibles. Des cadres tels que **Q2CSI** et **CASH** complètent cette approche en décomposant la sécurité en couches modulaires (Confidentialité, Fiabilité, Opposabilité).

Les enquêteurs font face à quatre défis : garantir l'intégrité des preuves, prouver la non-répudiation, préserver la confidentialité et maintenir une chaîne de possession traçable. Le **ZK-NR** et le **CLO (Cryptographic Legal Opposability)** apportent des solutions via :

- des attestations invisibles mais vérifiables (Zero-Knowledge Proofs) ;
- une traçabilité certifiée cryptographiquement ;
- une résistance aux attaques quantiques ;
- une recevabilité juridique accrue.

Des études de cas au Cameroun et en Europe (fraudes bancaires, cyberescroqueries BEC, fraude SIMBOX, affaire EncroChat) illustrent l'application de la cryptographie à la preuve

numérique. Les techniques de hachage et de signature électronique ont permis de garantir l'intégrité et l'authenticité des éléments présentés en justice.

L'investigation numérique moderne dépasse la simple collecte de données : elle intègre des mécanismes cryptographiques avancés conciliant rigueur scientifique et opposabilité légale. Les protocoles **ZK-NR** et cadres comme **CLO** marquent une évolution majeure vers une *preuve numérique incontestable*, résiliente aux menaces quantiques et juridiquement exploitable.

8. L'UTILITÉ DE L'INVESTIGATION NUMÉRIQUE DANS LA POLICE JUDICIAIRE

L'investigation numérique (digital forensic) consiste à collecter, analyser, conserver et présenter des preuves numériques issues de supports électroniques. Cette discipline est devenue indispensable dans un monde marqué par la digitalisation et la cybercriminalité, particulièrement dans le domaine policier.

Apports essentiels de l'investigation numérique

- **Accès à des preuves invisibles** : Historiques, conversations supprimées, métadonnées
- **Lutte contre la cybercriminalité** : Piratage, fraudes en ligne, ransomwares
- **Identification et traçage** : Analyse d'adresses IP, géolocalisation, communications
- **Reconstitution des événements** : Chronologie numérique des actions
- **Preuves recevables en justice** : Procédures garantissant l'intégrité des preuves
- **Soutien aux enquêtes traditionnelles** : Complémentarité avec les méthodes classiques

Domaines d'application au Cameroun

- **Cybercriminalité** : Démantèlement de réseaux de fraude (Douala 2022)
- **Criminalité transfrontalière** : Trafic de stupéfiants, lutte contre Boko Haram
- **Criminalité financière** : Détournement de fonds publics, fraudes fiscales
- **Crimes violents** : Kidnapping, vols à main armée (Yaoundé, Littoral)
- **Protection de l'enfance** : Réseaux pédopornographiques (2022)
- **Enquêtes judiciaires classiques** : Fraudes électorales, conflits fonciers
- **Collaboration internationale** : Interpol, coopération transfrontalière

Outils principaux

- **Récupération de données** : Autopsy, FTK Imager, Cellebrite
- **Analyse réseau** : Wireshark, surveillance dark web
- **Lutte contre chiffrement** : Cryptanalyse, attaques par force brute

Défis au Cameroun

- Volume exponentiel et complexité des données
- Respect des droits fondamentaux et vie privée
- Évolution technologique rapide et formation continue
- Coût élevé des équipements (licences $>$ 10 millions FCFA/an)

Limites actuelles

- **Difficultés juridiques** : Admissibilité des preuves, cadre légal
- **Pénurie d'experts** : Moins de 50 experts certifiés au Cameroun
- **Contraintes matérielles** : Stations forensic à 25 millions FCFA

L'investigation numérique est devenue un pilier fondamental de la police judiciaire camerounaise. Malgré les défis techniques, juridiques et financiers, son importance stratégique pour la sécurité nationale est incontestable. Le Cameroun doit investir dans la formation, les équipements et l'adaptation du cadre juridique pour faire face aux nouvelles menaces numériques (IA, métavers, deepfakes) et garantir sa souveraineté numérique.

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

Ce travail explore la falsification de conversations WhatsApp dans le cadre de l'investigation numérique. L'objectif est de démontrer la facilité avec laquelle il est possible de créer de fausses preuves numériques et d'analyser l'impact de ces pratiques sur les enquêtes.

- **Scénario** : Relation extra-conjugale simulée entre un enseignant (Paul KENGNE) et son étudiante
- **Outils utilisés** :
  - **Chatsmock** : Génération de fausses conversations WhatsApp
  - **Adobe Photoshop** : Retouches graphiques pour améliorer le réalisme
- **Contenu** : Échanges affectifs et sexuels explicites, promesses de quitter l'épouse

outils de creation de faux compte

- **Chatsmock** : Interface non parfaitement réaliste, fonctionnalités limitées (pas d'appels/réactions), export uniquement image
- **Comparaison** : FakeChat (plus d'options mais moins crédible), Photoshop (réalisme optimal mais compétences requises)
- Les falsifications restent détectables par analyse forensique (métadonnées, anomalies graphiques)

Impact sur l'Investigation Numérique

- Baisse de fiabilité des captures d'écran comme preuves
- Difficulté accrue pour les experts
- Risques de manipulation judiciaire et disciplinaire
- Multiplication des faux dossiers

Recommandations

- Vérifier les métadonnées et signatures numériques
- Sensibiliser les acteurs judiciaires aux falsifications
- Privilégier les données brutes depuis bases de données
- Utiliser des outils de détection de manipulations
- Renforcer le cadre légal sur l'acceptabilité des preuves

La simulation démontre la vulnérabilité des preuves numériques basées sur des captures d'écran. L'investigation numérique doit évoluer vers des méthodes de vérification plus rigoureuses et une sensibilisation accrue des acteurs pour garantir la fiabilité des preuves dans un contexte où la falsification devient de plus en plus accessible.