RÉPUBLIQUE DU CAMEROUN
Paix – Travail – Patrie
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR
UNIVERSITÉ DE YAOUNDÉ I
ÉCOLE NATIONALE SUPÉRIEURE POLYTECHNIQUE
DÉPARTEMENT DE GÉNIE INFORMATIQUE

REPUBLIC OF CAMEROON
Peace – Work – Fatherland
MINISTRY OF HIGHER EDUCATION
THE UNIVERSITY OF YAOUNDÉ I
NATIONAL ADVANCED SCHOOL OF ENGINEERING
COMPUTER ENGINEERING DEPARTMENT

NOTES EXPOSÉ

Théorie et pratique de l'investigation numérique

Chaho Tchime Perside Jackie

Classe : CIN 4 — Matricule : 22p094

Département de Génie Informatique — ENSPY

1 L'utilité de l'investigation numérique pour la police judiciaire

L'investigation numérique est devenue un outil indispensable pour la police judiciaire, notamment au Cameroun, face à la montée de la criminalité moderne liée au numérique. Elle permet d'accéder à des preuves invisibles, d'identifier les auteurs et de reconstituer les événements avec une grande précision, renforçant ainsi l'efficacité des enquêtes.

Cependant, ces avantages s'accompagnent de défis importants : volume de données considérable, complexité technologique, et limites juridiques, financières et humaines — notamment la pénurie d'experts qualifiés. Pour en tirer pleinement profit, le pays doit investir dans la formation, renforcer les moyens logistiques et adapter sa législation. L'avenir de cette discipline dépendra de sa capacité à anticiper les enjeux émergents, tels que l'intelligence artificielle ou la manipulation numérique, qui transforment continuellement la lutte contre la criminalité.

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

Le protocole **ZK-NR (Zero-Knowledge Non-Repudiation)** est une innovation cryptographique post-quantique qui renforce la non-répudiation, la confidentialité, la fiabilité et l'opposabilité juridique dans l'investigation numérique. Il démontre comment les signatures numériques, certificats électroniques, horodatages et fonctions de hachage garantissent l'intégrité et l'authenticité des preuves.

Fondé sur le trilemme **CRO** (Confidentialité, Fiabilité, Opposabilité), le cadre **Q2CSI** et le problème **AIIP**, le protocole s'appuie sur les primitives **CASH** (CEE pour la confidentialité, AOW pour la fiabilité et SH pour l'opposabilité). Il offre un système sécurisé et vérifiable, résistant aux attaques quantiques et garantissant la traçabilité et la valeur légale des preuves numériques.

Des cas concrets tels que la cyberfraude bancaire, les escroqueries par e-mail, l'affaire SIMBOX et EncroChat illustrent son utilité. Ainsi, ZK-NR et le cadre **CLO (Cryptographic Legal Opposability)** marquent une étape majeure où la cryptographie devient un instrument de vérité juridique et scientifique.

3 Conception et analyse d'un faux profil TikTok

Ce travail vise à comprendre les enjeux de l'identité numérique, de la viralité des contenus et des risques de manipulation sur les réseaux sociaux, notamment TikTok.

Les étudiants ont créé un faux profil intitulé **Innotrends25**, centré sur la cybersécurité, afin d'observer les réactions des utilisateurs et de sensibiliser à la sécurité en ligne. La niche a été choisie pour son intérêt technique et éducatif. L'objectif était d'informer sur les bonnes pratiques (sécurité des mots de passe, protection des données, arnaques en ligne), tout en maintenant un cadre éthique.

Le profil a obtenu plus de 100 mentions « J'aime » en six publications. L'analyse montre que la stratégie fut pertinente, suscitant un réel intérêt, mais soulève des questions éthiques : même à but éducatif, un faux profil peut induire des malentendus.

4 Deepfake Vocal

Cet exposé analyse le phénomène du **deepfake vocal**, ses mécanismes techniques et ses implications éthiques, juridiques et sécuritaires. Il explique le fonctionnement des deepfakes audio et illustre leurs usages et dérives à travers le cas **MINIMAX Audio**.

Les risques majeurs concernent la fiabilité et l'opposabilité des preuves audio. Des contre-mesures sont proposées : détection technologique, cadre légal adapté, gouvernance éthique, authentification multi-factorielle et bonnes pratiques de gestion des preuves.

L'exposé conclut sur la nécessité d'une **régulation robuste** et de **protocoles de vérification avancés** pour préserver la confiance dans les enquêtes numériques.

5 Les dix cas africains les plus importants de hacking (2015–2025)

Cette étude présente dix cas emblématiques de cyberattaques survenues en Afrique entre 2015 et 2025, illustrant la diversité des menaces :

- Ransomware sur **Transnet** (Afrique du Sud, 2021)
- Piratage de la **CNSS** (Maroc, 2025)
- Attaque sur **Eneo** (Cameroun, 2024)
- Attaque par **GhostLocker 2.0** (Égypte, 2024)
- Scandale **Pegasus** (Maroc, 2020–2021)
- Piratage de **banques ivoiriennes**
- Cyberattaque sur les **systèmes de santé tunisiens** (2021)
- Piratage de **Ethiopian Airlines** (2023)
- Fraude au **Mobile Money MTN Nigeria** (2018)
- Piratage de la **Banque centrale du Nigeria** (2015–2016)

6 Les trois meilleurs logiciels de rédaction de mémoire

La combinaison d'outils adaptés optimise la rédaction et la gestion des mémoires. L'association **Overleaf + Zotero** est recommandée pour concilier rigueur scientifique et efficacité.

Outils complémentaires

Aucun logiciel ne couvre tous les besoins. La synergie entre **Word + Zotero** ou **Overleaf + Zotero** permet une meilleure structuration, gestion des références et collaboration.

Avantages spécifiques

- **Overleaf :** qualité typographique et structuration scientifique.
- **Word :** accessibilité et simplicité d'usage.

- **Zotero :** gestion automatisée et rigoureuse des références.

La réussite dépend autant de la maîtrise des outils que de la qualité du contenu.

7 Simulation d'une série de messages WhatsApp falsifiés

Cet exposé met en lumière la facilité de falsification des conversations WhatsApp grâce à des outils comme **Chatsmock** et **Adobe Photoshop**. Cette manipulation remet en question la fiabilité des captures d'écran comme preuves judiciaires.

Pour y remédier, il est nécessaire de recourir à l'analyse des métadonnées, aux outils forensiques spécialisés et à la collecte directe de données. La sensibilisation des acteurs judiciaires et un cadre légal renforcé sont essentiels pour garantir l'intégrité des preuves numériques.

8 Réalisation d'un deepfake à l'aide de l'IA

Cet exposé démontre comment les **deepfakes** peuvent usurper l'identité et tromper la perception humaine. En combinant **GPT-5** (pour le script) et **HeyGen AI** (pour la génération vidéo), le groupe a créé une séquence où un faux discours semble authentique.

Un deepfake est une vidéo modifiée par intelligence artificielle à l'aide du deep learning et des réseaux **GAN**, capables d'imiter fidèlement la voix et le visage d'une personne. L'expérience illustre la puissance et les dérives potentielles de ces technologies — manipulation, désinformation et usurpation d'identité — et encourage un usage éthique et responsable dans l'investigation numérique.

9 Points sur les algorithmes de reconnaissance faciale

La reconnaissance faciale est une technologie d'intelligence artificielle permettant d'identifier ou de vérifier l'identité d'une personne à partir de ses traits du visage. Elle repose sur des algorithmes de détection, d'extraction et de comparaison des caractéristiques faciales, et joue un rôle majeur en cybersécurité et en investigation numérique.

9.1 Fonctionnement général

Un système biométrique de reconnaissance faciale suit trois étapes principales :

- **Enrôlement :** enregistrement du visage et des données de référence.
- **Identification (1-N) :** recherche d'une correspondance dans la base.
- **Vérification (1-1) :** comparaison d'un visage à un profil donné.

L'architecture d'un système de reconnaissance faciale comprend quatre modules :

1. Capture
2. Extraction
3. Correspondance
4. Décision

9.2 Méthodes de reconnaissance

Trois grandes catégories de méthodes sont utilisées :

- **Méthodes classiques :** PCA, LDA, SVM, HMM, EBGM, etc.
- **Descripteurs de points d'intérêt :** SIFT, HOG, SURF, etc.
- **Méthodes hybrides :** combinaisons de modèles profonds et de descripteurs locaux pour plus de robustesse.

9.3 Avantages et limites

Atouts

- Rapidité
- Automatisation
- Précision en conditions contrôlées

Limites

- Baisse de performance en conditions réelles
- Architectures complexes et peu transparentes
- Risques de biais et d'erreurs

Risques sécuritaires

- Piratage
- Attaques adversariales
- Usurpation via deepfakes ou masques

Enjeux éthiques et juridiques

- Atteinte à la vie privée
- Discriminations
- Légalité du traitement
- Responsabilité des acteurs

Contraintes organisationnelles

- Coûts élevés
- Besoin d'infrastructure
- Acceptabilité sociale