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
****

RAPPORT
Note de Lecture

Option :

Cybersécurité et Investigation Numérique

Rédigé par :
NDJEBAYI PATRICK N., *24P827*

Sous l'encadrement de :
M. Thierry MINKA

Année académique 2025 / 2026

TABLE DES MATIÈRES

0.1 Section 1 : Introduction à l'Investigation Numérique dans la Police Judiciaire

L'investigation numérique, ou *digital forensic*, est une discipline consistant à collecter, analyser, conserver et présenter des preuves numériques issues de supports électroniques (ordinateurs, téléphones, réseaux, etc.) afin de soutenir des enquêtes judiciaires, administratives ou privées. Dans un monde de plus en plus numérisé et confronté à la cybercriminalité, cette discipline revêt une importance croissante, particulièrement dans le domaine policier.

La question centrale abordée est la suivante : en quoi l'investigation numérique constitue-t-elle un outil indispensable pour la police judiciaire dans la lutte contre la criminalité moderne ? Pour y répondre, l'analyse s'articulera autour de trois axes principaux :

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

— Ses principaux domaines d'application ;

— Les outils, défis et limites de cette pratique.

Cette introduction pose les bases d'une réflexion approfondie sur le rôle stratégique de l'investigation numérique dans les enquêtes contemporaines.

0.2 Section 2 : Protocole ZK-NR et son Positionnement dans l'Investigation Numérique Moderne

Cette section présente le protocole ZK-NR (Zero-Knowledge Non-Repudiation), une architecture cryptographique modulaire visant à assurer une non-répudiation préservant la confidentialité pour les services numériques publics.

0.2.1 Concepts Fondamentaux

La **non-répudiation numérique** garantit qu'un expéditeur ou un destinataire ne peut nier avoir participé à une transaction. Ses principaux outils incluent :

— Les **signatures numériques** pour l'authentification et l'intégrité

— Les **certificats électroniques** pour l'identification des parties

— L'**horodatage numérique** pour la preuve temporelle

— Les **fonctions de hachage** pour l'intégrité des données

0.2.2 Cadre Théorique et Innovations

Le protocole ZK-NR s'appuie sur plusieurs avancées théoriques :

— Le **Trilemme CRO** qui établit l'impossibilité de satisfaire simultanément Confidentialité, Fiabilité et Opposabilité Juridique

— Le cadre **Q2CSI** qui propose une architecture modulaire pour minimiser cette incompatibilité

— Les primitives cryptographiques **CEE, AOW et SH** assurant respectivement confidentialité, fiabilité et opposabilité juridique

0.2.3 Apports pour l'Investigation Numérique

ZK-NR répond aux besoins spécifiques des enquêteurs :

— **Garantie d'intégrité** des preuves collectées

— **Non-répudiation** des actes numériques

— **Préservation de la confidentialité** des données sensibles

— **Traçabilité** via une chaîne de possession cryptographique

0.2.4 Positionnement dans l'Investigation Moderne

ZK-NR représente une avancée significative par rapport aux méthodes traditionnelles :

— Il combine **sécurité post-quantique** et **recevabilité juridique**

— Il permet de produire des **preuves vérifiables sans révéler d'informations sensibles**

— Il s'inscrit dans une **convergence entre exigences techniques et légales**

En conclusion, le protocole ZK-NR ouvre la voie à une nouvelle génération de pratiques forensiques où la preuve numérique devient à la fois techniquement robuste et légalement incontestable.

0.3 Section 3 : Les 10 cas africains les plus importants de hacking

Cette section présente une analyse des dix cyberattaques les plus significatives survenues en Afrique entre 2015 et 2025, mettant en lumière les défis de la cybersécurité sur le continent.

0.3.1 Contexte de la cybersécurité en Afrique

L'Afrique connaît une révolution numérique rapide mais fait face à d'importantes vulnérabilités :

— Faible maturité institutionnelle en matière de cybersécurité

— Pénurie d'expertise locale (moins d'1 expert/100 000 habitants)

— Infrastructures obsolètes et dépendance technologique extérieure

— Augmentation de 300% des cyberattaques en 10 ans (INTERPOL 2024)

0.3.2 Méthodologie d'investigation

L'analyse s'appuie sur une approche structurée en 5 étapes :

1. Identification de l'incident
2. Collecte des preuves
3. Préservation de l'intégrité
4. Analyse technique (Autopsy, FTK, Wireshark)
5. Rédaction du rapport

0.3.3 Cas emblématiques analysés

— **Transnet (Afrique du Sud, 2021)** : Ransomware paralysant les ports, 60M$ de pertes
— **CNSS (Maroc, 2025)** : Fuite de données de 2 millions de salariés
— **Eneo (Cameroun, 2024)** : Attaque sur le fournisseur d'électricité national
— **GhostLocker 2.0 (Égypte, 2024)** : Ransomware ciblant 30 organisations
— **Pegasus (Maroc, 2020-2021)** : Logiciel espion contre des personnalités
— **Banques ivoiriennes** : Phishing et RAT, 6M€ de pertes
— **Santé tunisien (2021)** : DDoS et ransomware affectant les hôpitaux
— **Ethiopian Airlines (2023)** : Compromission du système de réservation
— **MTN Nigeria (2018)** : Fraude au mobile money (8M$)
— **Banque centrale du Nigeria (2015-2016)** : Intrusion SWIFT longue durée

0.3.4 Recommandations

Pour renforcer la cybersécurité africaine :

— Former massivement les experts en forensic numérique
— Créer des CERT/CSIRT régionaux
— Harmoniser les lois via la Convention de Malabo
— Développer un cloud souverain africain
— Renforcer la gouvernance numérique des entreprises publiques

0.3.5 Conclusion

L'avenir numérique de l'Afrique dépend de sa capacité à sécuriser ses infrastructures et à former ses talents. La cybersécurité doit devenir une responsabilité partagée pour assurer un développement numérique durable.

0.4 Section 4 : Les trois meilleurs logiciels de rédaction de mémoire

Cette section présente une analyse comparative des trois principaux logiciels utilisés pour la rédaction académique : Overleaf, Microsoft Word et Zotero.

0.4.1 Overleaf : L'excellence académique par LaTeX

— **Type** : Éditeur LaTeX en ligne collaboratif
— **Atouts** : Qualité typographique exceptionnelle, gestion avancée des références croisées, collaboration en temps réel, modèles académiques prêts à l'emploi
— **Limites** : Courbe d'apprentissage significative, édition hors ligne limitée
— **Public cible** : Domaines scientifiques et techniques (mathématiques, physique, informatique)

0.4.2 Microsoft Word : Le référencement en traitement de texte

— **Type** : Traitement de texte universel

— **Atouts** : Interface familière, gestion avancée des styles, génération automatique des tables, suivi des modifications

— **Limites** : Gestion bibliographique native limitée, risques d'instabilité sur les longs documents

— **Public cible** : Étudiants débutants, sciences humaines et sociales

0.4.3 Zotero : Le spécialiste de la bibliographie

— **Type** : Gestionnaire de références open-source

— **Atouts** : Capture automatique des métadonnées, intégration avec Word et Overleaf, gestion de milliers de styles de citation, synchronisation cloud

— **Limites** : Nécessite un apprentissage modéré

— **Public cible** : Tous les profils académiques nécessitant une gestion rigoureuse des références

0.4.4 Combinaisons gagnantes recommandées

— **Profil débutant** : Word + Zotero (accessibilité et gestion bibliographique)

— **Profil scientifique** : Overleaf + Zotero (qualité professionnelle et rigueur scientifique)

— **Profil collaboratif** : Overleaf + Zotero Groups (travail d'équipe optimisé)

0.4.5 Conclusion

Le choix optimal dépend du profil de l'étudiant et des exigences du mémoire. Aucun outil seul ne couvre tous les besoins, mais les combinaisons stratégiques permettent d'atteindre l'excellence académique. La maîtrise des outils doit servir la substance intellectuelle du travail et non la remplacer.

0.5 Section 5 : Algorithmes de reconnaissance faciale

Cette section présente une analyse approfondie des algorithmes de reconnaissance faciale, de leur fonctionnement technique aux enjeux éthiques et juridiques dans le contexte de l'investigation numérique.

0.5.1 Fonctionnement et architecture des systèmes biométriques

— **Enrôlement** : Capture et stockage des caractéristiques faciales dans une base de données

— **Identification** : Recherche 1-N pour retrouver une identité parmi tous les profils enregistrés

— **Vérification** : Comparaison 1-1 pour confirmer une identité déclarée

— **Architecture modulaire** : Acquisition → Extraction → Correspondance → Décision

0.5.2 Méthodes de reconnaissance

— **Méthodes globales** : Utilisent l'ensemble du visage (PCA/Eigenfaces, LDA, SVM)

— **Méthodes locales** : Se concentrent sur des régions spécifiques (yeux, nez, bouche)

— **Méthodes hybrides** : Combinent approches globales et locales

— **Détecteurs de points d'intérêt** : SIFT, HOG, SURF pour l'extraction de caractéristiques

0.5.3 Avantages et limites techniques

— **Atouts** : Rapidité, automatisation, capacité à traiter de grands volumes de données

— **Limites** : Performance dégradée en conditions réelles (lumière, angles), architecture "boîte noire", problèmes d'interopérabilité

0.5.4 Enjeux sécuritaires et éthiques

— **Vulnérabilités** : Attaques adversariales, deepfakes, protection des données biométriques

— **Impact éthique** : Atteinte à la vie privée, biais algorithmiques, discrimination

— **Enjeux juridiques** : Conformité légale, responsabilité, supervision et traçabilité

0.5.5 Recommandations pour le contexte camerounais

— **Technique** : Documentation des pipelines, tests locaux, approches hybrides

— **Sécurité** : Tests d'intrusion, anti-spoofing multi-sensoriel, chiffrement des templates

— **Éthique** : Études d'impact, audits de biais, communication transparente

— **Juridique** : Base légale claire, alignement sur la loi sur les données personnelles

— **Opérationnel** : Validation humaine obligatoire, procédures documentées, déploiement progressif

0.5.6 Conclusion

La reconnaissance faciale représente un outil puissant pour l'investigation numérique mais nécessite un encadrement strict pour concilier efficacité opérationnelle, sécurité technique et respect des droits fondamentaux. Son déploiement au Cameroun doit s'accompagner d'un cadre juridique robuste et de procédures de contrôle rigoureuses.

0.6 Section 6 : Deepfake Vocal - Enjeux et Investigation

Cette section analyse les deepfakes vocaux, leur évolution technologique et leurs implications pour l'investigation numérique.

0.6.1 Évolution des deepfakes audios

— **1930-1990** : Premières reproductions vocales électroniques (Voder, vocoders)

— **2000-2015** : Modèles statistiques HMM pour une synthèse plus naturelle

— **2016** : Révolution avec WaveNet (DeepMind) et le deep learning

— **2016-2017** : Premiers démonstrations publiques (Adobe VoCo, Lyrebird)
— **2017-2020** : Démocratisation avec outils open-source (SV2TTS)
— **2019-aujourd'hui** : Usage malveillant (fraudes, usurpation d'identité)

0.6.2 Contextes d'utilisation

— **Applications légitimes** : Accessibilité pour personnes handicapées, doublage audiovisuel, assistants vocaux, préservation de voix
— **Applications malveillantes** : Escroqueries financières, usurpation d'identité, manipulation politique, falsification de preuves

0.6.3 Enjeux pour l'investigation numérique

— **Atteinte au triptyque CRO** :
  — Confidentialité compromise par la diffusion non autorisée
  — Fiabilité remise en question des preuves audio
  — Opposabilité juridique fragilisée
— **Complexification de la vérification** : Nécessité de techniques avancées de détection
— **Besoin de compréhension technique** : Maîtrise des réseaux neuronaux et vocodeurs essentielle

0.6.4 Cas pratique : MINIMAX Audio

— Plateforme de synthèse vocale par IA permettant le clonage vocal
— Processus : Voice Clone → Text To Speech → Génération de deepfakes
— Résultat : Rendu réaliste indétectable à l'oreille humaine
— Applications détournées : Escroqueries, usurpation, désinformation

0.6.5 Contre-mesures et prévention

— **Détection technologique** : Outils d'analyse des anomalies vocales
— **Sensibilisation** : Formation des utilisateurs aux risques
— **Cadre légal** : Lois spécifiques et watermarking obligatoire
— **Sécurisation** : Authentification multi-facteur et reconnaissance dynamique
— **Éthique** : Charte de transparence et respect du consentement

0.6.6 Conclusion

Les deepfakes vocaux représentent une double facette : opportunité d'innovation et menace sécuritaire. Leur encadrement nécessite une approche multidimensionnelle combinant solutions techniques, cadre juridique et éthique pour préserver l'intégrité des preuves numériques.

0.7 Section 7 : Simulation de Falsification de Conversations WhatsApp

Cette section présente une étude pratique sur la falsification de conversations WhatsApp et ses implications pour l'investigation numérique.

0.7.1 Mise en situation

- Scénario : Relation extra-conjugale entre un enseignant (Paul KENGNE) et son étudiante
- Éléments fournis : 7 captures d'écran WhatsApp et 2 photos compromettantes
- Contenu des échanges : Messages affectifs, sexuels explicites, promesses de quitter l'épouse

0.7.2 Méthodologie de falsification

- **Chatsmock** : Application web pour générer de fausses conversations WhatsApp
  - Définition des participants (noms, photos de profil)
  - Génération de messages avec date/heure personnalisées
  - Statut de lecture modifiable
- **Adobe Photoshop** : Retouche graphique pour améliorer le réalisme
  - Correction des détails graphiques (alignement, couleurs)
  - Insertion d'images supplémentaires
  - Adaptation à l'interface d'un smartphone réel

0.7.3 Limites et comparaison d'outils

- **Limites de Chatsmock** :
  - Interface pas toujours à jour avec les dernières versions WhatsApp
  - Fonctionnalités limitées (pas de notes vocales, appels, réactions)
  - Export uniquement en format image
  - Détection possible par analyse forensique
- **Outils alternatifs** : FakeChat, WhatsFake, Photoshop, outils forensiques détournés

0.7.4 Impact sur l'investigation numérique

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

0.7.5 Recommandations

- Vérification technique des métadonnées et signatures numériques
- Sensibilisation des acteurs judiciaires aux falsifications
- Utilisation d'outils spécialisés de détection de manipulations
- Privilégier les données brutes des bases de données plutôt que captures d'écran
- Renforcement du cadre légal sur l'acceptabilité des preuves numériques

0.7.6 Conclusion

La facilité de falsification des conversations WhatsApp démontre la fragilité des preuves numériques basées sur des captures d'écran. L'investigation numérique doit adopter des méthodes de vérification rigoureuses et des techniques avancées pour garantir l'intégrité des preuves dans un environnement où la manipulation devient de plus en plus accessible.

0.8 Section 8 : Conception et Analyse d'un Faux Profil TikTok

Cette section présente une étude pratique sur la création d'un faux profil TikTok à des fins pédagogiques d'investigation numérique.

0.8.1 Démarche méthodologique

— **Création du profil** : Utilisation d'un service de messagerie temporaire (temp-mail.org) pour préserver l'anonymat

— **Identité** : Profil "InnoTrends" avec la bio : *"Découvre ce que les hackers ne veulent pas que tu saches"*

— **Approche éthique** : Cadre strictement pédagogique sans usurpation réelle

0.8.2 Choix de la niche : Cybersécurité

— Thématique d'actualité et essentielle face aux menaces numériques

— Permet une mission éducative de sensibilisation

— Respecte le cadre éthique de l'investigation

— Aborde des sujets variés : mots de passe, données personnelles, arnaques en ligne

0.8.3 Stratégie de contenu

— Approche éducative et engageante avec ton léger et humoristique

— Thématiques accessibles : sécurité des mots de passe, Wi-Fi public, phishing

— Visuels attractifs (bandes dessinées, messages interactifs)

— Respect des règles de la plateforme sans manipulation

0.8.4 Outils utilisés

— TikTok Analytics pour le suivi des performances

— ChatGPT pour la génération de contenu

— Canva pour la création des visuels

— Temp Mail pour l'anonymat

— Tableau de bord personnel pour les observations

0.8.5 Contenus publiés

- 6 publications orientées cybersécurité :
  - Bonnes pratiques des mots de passe
  - Dangers du Wi-Fi public
  - Détection des arnaques de phishing (faux lien Orange Money)
  - Protection des informations personnelles
  - Gestion de l'empreinte numérique
- Résultats : Plus de 100 likes, jusqu'à 310 vues par publication

0.8.6 Analyse et observations

- Stratégie pertinente : contenu éducatif + ton ludique + visuels accrocheurs
- Thématiques proches du quotidien facilitent l'engagement
- Bio percutante essentielle pour l'attractivité
- Limites éthiques de la création de faux profils même à but pédagogique

0.8.7 Recommandations

- Renforcer l'éducation à la cybersécurité dès le secondaire
- Encadrer l'usage des faux profils pédagogiques dans un cadre légal
- Promouvoir la collaboration interdisciplinaire
- Intégrer des exercices pratiques dans les programmes académiques

0.8.8 Conclusion

L'expérience démontre l'efficacité des réseaux sociaux pour la sensibilisation à la cybersécurité, tout en soulignant l'importance d'une approche éthique et encadrée dans ce type d'investigation numérique pédagogique.