RÉPUBLIQUE DU CAMEROUN
*****
Paix – Travail – Patrie
*****
UNIVERSITÉ DE YAOUNDÉ I
*****
ÉCOLE NATIONALE SUPÉRIEURE POLYTECHNIQUE DE YAOUNDÉ
*****
DEPARTEMENT DE GENIE INFORMATIQUE
*****

REPUBLIC OF CAMEROON
*****
Peace – Work – Fatherland
*****
UNIVERSITY OF YAOUNDÉ I
*****
NATIONAL ADVANCED SCHOOL ENGINEERING OF YAOUNDE
*****
COMPUTERS ENGINEERING DEPARTMENT
*****

TRAVAIL À FAIRE N°3

Résumé de notes des exposés

Théories et Pratiques de l'Investigation Numérique

Rédigé par :

Noms & Prénoms	Filière	Matricule
DSAMAGO JAFFO Trésor	HN – CIN 4	22P036

Sous la direction de :
M. **MINKA MI NGUIDJOI Thierry Emmanuel**

Année académique : 2025–2026

1 Réalisation d'une vidéo deepfake avec GPT-5 et HeyGen

Pour cet exposé, une vidéo deepfake a été générée dans laquelle le chef de groupe, **AYOMENE Tiobou Varesse**, dispense le premier chapitre sur les deepfakes. Le script a été produit avec GPT-5, détaillant les concepts fondamentaux, les inconvénients et l'avenir des deepfakes. La vidéo elle-même a été synthétisée via HeyGen, utilisant la technologie d'avatar parlant et de clonage vocal pour créer un rendu réaliste. Ce travail démontre le potentiel créatif de l'IA générative tout en alertant sur les risques de manipulation et la nécessité d'une utilisation éthique et encadrée.

2 Falsification de conversations WhatsApp avec Chatsmock et Photoshop

Cet exposé détaille la méthodologie de falsification d'une conversation WhatsApp à l'aide de Chatsmock et d'Adobe Photoshop, en simulant une relation extra-conjugale entre un enseignant, **Mr Paul KEGNE** et une étudiante. Il présente les limites de Chatsmock (manque de réalisme sur certains détails, fonctionnalités restreintes) et les compare à d'autres outils comme FakeChat ou Photoshop. L'analyse souligne l'impact de ces outils sur l'investigation numérique, fragilisant la fiabilité des captures d'écran, et recommande des vérifications techniques (métadonnées, données brutes) et un renforcement du cadre légal pour contrer les falsifications.

3 Utilité de l'investigation numérique dans la police judiciaire

L'investigation numérique s'est imposée comme un outil indispensable au sein de la police judiciaire camerounaise, répondant à la migration de la criminalité vers le numérique. Elle permet d'accéder à des preuves invisibles dans le monde physique, de lutter contre la cybercriminalité, d'identifier et tracer les auteurs grâce aux adresses IP et données de communication, et de reconstituer la chronologie des événements. Bien qu'elle offre des preuves recevables en justice lorsqu'elle respecte les procédures de collecte et de conservation, elle se heurte à des défis substantiels comme l'explosion du volume de données, la complexité technique croissante, les contraintes juridiques locales, et des limites matérielles et humaines, notamment la pénurie d'experts certifiés et le coût élevé des équipements.

4 Protocole ZK-NR et non-répudiation

Le protocole ZK-NR (Zero-Knowledge Non-Repudiation) représente une avancée majeure dans le domaine de la cryptographie appliquée à l'investigation numérique. Cette architecture modulaire en couches combine des primitives post-quantiques comme les STARKs et les signatures BLS à seuil pour créer des preuves sécurisées et vérifiables sans jamais révéler de contenu sensible. Le protocole s'attaque au trilemme CRO qui formalise l'incompatibilité fondamentale entre Confidentialité, Fiabilité et Opposabilité Juridique. En offrant des attestations juridiquement admissibles tout en préservant la confidentialité des données, ZK-NR comble le fossé entre la sécurité cryptographique et les exigences institutionnelles, répondant ainsi aux besoins des enquêteurs en matière d'intégrité des preuves, de non-répudiation des actes et de traçabilité complète de la chaîne de possession.

5 Les 10 cas africains majeurs de hacking

Cet exposé analyse une sélection de dix cyberattaques majeures survenues en Afrique entre 2015 et 2025, incluant des incidents tels que le ransomware contre Transnet en Afrique du Sud, la fuite de données de la CNSS au Maroc, l'attaque contre Eneo au Cameroun, et l'arnaque au mobile money au Nigeria. Chaque cas est évalué selon des critères incluant la taille de l'attaque, le type d'organisation ciblée, le volume de données affectées et l'impact financier. L'étude souligne l'importance cruciale de l'investigation numérique pour comprendre ces incidents, retracer leurs origines, et formuler des recommandations pour renforcer la cybersécurité et la résilience du continent.

6 Les trois meilleurs logiciels de rédaction de mémoire

Cette analyse comparative détaille les atouts respectifs de trois logiciels essentiels pour la rédaction académique : Overleaf, Microsoft Word et Zotero. Overleaf, éditeur LaTeX en ligne, excelle pour la qualité typographique professionnelle et la gestion des références croisées, idéal pour les documents scientifiques complexes. Microsoft Word reste la solution la plus accessible et universelle, avec une prise en main immédiate mais une gestion bibliographique native limitée. Zotero, gestionnaire de références open-source, automatise la collecte et la citation des sources. L'exposé recommande des combinaisons gagnantes selon le profil utilisateur, comme le duo Word + Zotero pour les débutants ou la triade Overleaf + Zotero pour l'excellence scientifique.

7 Algorithmes de reconnaissance faciale

La reconnaissance faciale, technologie biométrique basée sur l'IA, permet l'identification ou la vérification d'individus à partir de leurs traits du visage. L'exposé présente son architecture (acquisition, extraction de caractéristiques, correspondance, décision), ses méthodes (globales, locales, hybrides) et ses applications dans l'investigation numérique. Il examine également ses avantages opérationnels (rapidité, automatisation) et ses inconvénients majeurs, incluant les vulnérabilités aux attaques, les biais algorithmiques, les impacts sur la vie privée et les défis juridiques. Des recommandations techniques, éthiques et réglementaires sont proposées pour un usage responsable au Cameroun.

8 Deepfake vocal : cas de MINIMAX Audio

Le deepfake vocal, illustré par l'outil MINIMAX Audio, consiste à cloner une voix à partir de quelques échantillons grâce à l'IA. L'exposé retrace son évolution technique, de la synthèse basique aux réseaux neuronaux, et présente ses contextes d'utilisation, qu'ils soient légitimes (accessibilité, doublage) ou malveillants (usurpation, fraude). Il détaille un cas pratique de création de deepfake vocal avec MINIMAX Audio, démontrant la facilité de génération d'un audio réaliste. Les risques sécuritaires, éthiques et juridiques sont analysés, et des contre-mesures sont proposées, incluant la détection technologique, la sensibilisation et un cadre légal adapté.

9 Conception d'un faux profil TikTok à des fins pédagogiques

Dans le cadre d'un exercice pédagogique, un faux profil TikTok nommé "Innotrends" a été créé autour de la niche cybersécurité. Utilisant une adresse email temporaire et une stratégie de contenu éducatif (mots de passe, Wi-Fi public, hameçonnage), le profil a généré un engagement significatif (plus de 100 likes, plusieurs centaines de vues par publication). L'expérience a permis d'analyser les réactions des utilisateurs et de démontrer l'efficacité des réseaux sociaux pour la sensibilisation, tout en soulignant les questions éthiques liées à l'usage de fausses identités, même à des fins éducatives.