RÉPUBLIQUE DU CAMEROUN
*****
Paix - Travail - Patrie
*****

UNIVERSITÉ DE YAOUNDÉ I
*****

ÉCOLE NATIONALE SUPÉRIEURE POLYTECHNIQUE DE YAOUNDÉ
*****

DÉPARTEMENT DE GÉNIE
*****

REPUBLIC OF CAMEROON
*****
Peace - Work - Fatherland
*****

UNIVERSITY OF YAOUNDE I
*****

NATIONAL ADVANCED SCHOOL OF ENGINEERING OF YAOUNDE
*****

COMPUTER ENGINEERING
*****

Techniques et pratiques de l'investigation numérique

Sous le thème : Résumé Techniques et pratiques de l'investigation numérique

EMBOLO MVOGO SHAWN DOUGLAS

Matricule : 22P072

Filière : CIN4

Sous la supervision de : **Mr Minka**

Année Scolaire : **2025 – 2026**

Contents

1 INTRODUCTION

Le présent document constitue une synthèse des principaux travaux réalisés dans le cadre du cours de *Techniques et pratiques de l'investigation numérique*. Il propose une version condensée et structurée des différents thèmes abordés tout au long du semestre, mettant en lumière la diversité et la richesse des approches étudiées dans ce domaine en constante évolution.

Au fil de ce travail, plusieurs thématiques majeures ont été explorées, alliant réflexion théorique, expérimentation technique et analyse critique. Parmi celles-ci figurent :

- la conception d'une vidéo deepfake mettant en scène un chef de groupe dispensant un cours ;
- la présentation détaillée du protocole ZK-NR et de ses applications potentielles en cybersécurité ;
- l'étude approfondie des algorithmes de reconnaissance faciale et de leurs implications éthiques ;
- la création d'un deepfake vocal illustrant les risques liés à la manipulation sonore ;
- l'analyse comparative des trois meilleurs logiciels de rédaction de mémoire ;
- la simulation d'une fausse conversation WhatsApp pour comprendre les techniques d'investigation numérique liées aux messageries instantanées ;
- l'examen du rôle et de l'utilité de l'investigation numérique dans la police judiciaire ;
- la présentation des dix cas les plus marquants de cyberattaques en Afrique au cours des dix dernières années ;
- et enfin, la conception d'un faux profil TikTok, illustrant les méthodes de détection et de prévention de l'usurpation d'identité numérique.

L'ensemble de ces travaux vise à renforcer la compréhension des enjeux actuels de la cybersécurité, tout en développant les compétences pratiques nécessaires à l'analyse, à la prévention et à la résolution des incidents numériques.

2 A l'aide d'une IA pour réaliser une vidéo deepfake

2.1 Définition du deepfake

Un **deepfake** est un enregistrement vidéo ou audio réalisé ou modifié grâce à l'intelligence artificielle. Ce terme fait référence non seulement au contenu ainsi créé, mais aussi aux technologies utilisées. Le mot *deepfake* est une abréviation de *Deep Learning* et *Fake*, qui peut être traduit par « fausse profondeur ». Il désigne des contenus faux rendus profondément crédibles par l'intelligence artificielle.

2.2 Comment réaliser sa vidéo deepfake avec l'IA

Pour créer une vidéo deepfake ou générée par intelligence artificielle, il est essentiel de combiner des outils capables de produire à la fois le contenu textuel et visuel. Dans notre projet, nous avons utilisé **GPT-5** pour générer le script et les instructions détaillées du premier chapitre du cours, puis **HeyGen AI** pour transformer ce script en une vidéo réaliste, animant un avatar et synchronisant voix et mouvements.

2.3 Présentation des outils : HeyGen AI et GPT-5

2.3.1 HeyGen AI

Créé en 2022, HeyGen est spécialisé dans la génération de vidéos à partir de simples instructions textuelles, sans nécessiter de compétences techniques avancées. Ses principales utilisations sont :

- Création de contenu et journalisme : diffusion de nouvelles ou histoires avec un impact visuel fort.
- Communication d'entreprise : réalisation de vidéos de présentation de produits ou services.
- Enseignement et formation : transformation des cours en expériences interactives et engageantes.

Fonctionnalités clés de HeyGen

- Création d'avatars ultra-réalistes à partir de photos.
- Voix synthétiques avancées et clonage vocal précis.
- Traduction et localisation multilingue avec synchronisation labiale.
- Intégration dans des chaînes de production vidéo automatisées.

Processus de création d'une vidéo

Sélection d'un template, choix de l'avatar, rédaction du script, soumission de la vidéo pour génération rapide.

2.3.2 GPT-5

Lancé en août 2025 par OpenAI, GPT-5 est un modèle d'IA avancé capable de :

- Générer du texte, du code, des images et des applications complètes.
- Traiter de longs documents et maintenir la cohérence des échanges.
- Offrir des réponses rapides ou plus approfondies selon le besoin.

GPT-5 combine un modèle rapide à haut débit, un modèle de raisonnement et un routeur temps réel qui choisit le modèle adapté selon la complexité de la tâche. Il inclut différentes versions pour développeurs, allant de la version mini à la version nano, permettant d'optimiser vitesse et précision.

2.4 Réalisation de la vidéo

Pour le devoir, GPT-5 a été utilisé pour générer le script du premier chapitre du cours, tandis que HeyGen a permis de créer la vidéo finale, en animant l'avatar et en synchronisant voix et mouvements, grâce aux fonctionnalités avancées et à la personnalisation de l'outil.

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

Présentation synthétique des articles

3.1 Exploration de ZK-NR : Vision globale et applications

Le protocole **ZK-NR** (Zero-Knowledge Non-Repudiation) est une architecture cryptographique modulaire en couches, axée sur la non-répudiation tout en préservant la confidentialité pour la co-production de services numériques publics. Il combine des primitives post-quantiques (STARKs, signatures BLS à seuil, Dilithium) pour créer des preuves sécurisées, vérifiables et auditables, sans jamais révéler de contenu sensible. Modélisé dans *Tamarin*, il s'adresse spécifiquement aux environnements réglementés (finance, e-gouvernement), offrant des attestations juridiquement admissibles.

3.2 Le Trilemme CRO : Équilibre entre Confidentialité, Fiabilité et Opposabilité

Le **Trilemme CRO** formalise une incompatibilité fondamentale pour tout système de preuve post-quantique : il est impossible de satisfaire simultanément la Confidentialité (Priv), la Fiabilité (Rel) et l'Opposabilité Juridique (HOpp). Une borne d'impossibilité est établie par la formule :

$$\mathrm{HOpp} \leq f(\mathrm{Priv}, \mathrm{Rel}) + \eta_q(C) + \mathrm{negl}(\lambda)$$

Cette analyse théorique, validée empiriquement ($\Gamma_{\mathrm{CRO}} > 0,8$), sert de fondation aux architectures cherchant à minimiser cette violation.

3.3 Q2CSI : Infrastructure de Sécurité Quantique Composable et Contextuelle

Q2CSI (Quantum-to-Classical Security Infrastructure) est un cadre en couches conçu pour résoudre le Trilemme CRO en décomposant la sécurité en trois strates isolées mais composables :

- Fer : Fiabilité
- Or : Confidentialité
- Argile : Opposabilité

Ce cadre abstrait étend le modèle de Composabilité Universelle (UC) en intégrant des contraintes entropiques, réduisant significativement la violation du trilemme ($\Gamma_{\text{CRO}} < 0,4$). Basé sur des primitives minimales (IND-CCA2, EUF-CMA), Q2CSI propose la première architecture formelle pour des protocoles post-quantiques juridiquement vérifiables.

3.4 Design ZK-NR : Cadre théorique et modélisation

La formalisation du protocole ZK-NR s'attache à son design théorique et à sa modélisation. S'appuyant sur les contraintes du trilemme CRO, cette contribution détaille comment des primitives spécifiques (engagements Merkle, STARKs, etc.) sont agencées pour atteindre l'équilibre requis entre responsabilité et confidentialité. Cette phase inclut une preuve de concept et une modélisation dans l'outil *Tamarin*, fournissant des artefacts pratiques.

3.5 Problème AIIP : Authenticité et intégrité des preuves

Le **Problème d'Inversion Itérée Affine** (AIIP) est l'hypothèse cryptographique fondamentale du cadre CASH. Reposant sur la difficulté de résoudre des équations quadratiques multivariées (MQ) et des logarithmes discrets sur des courbes hyperelliptiques de genre élevé (HCDLP), l'AIIP garantit l'authenticité et l'intégrité des preuves dans les systèmes post-quantiques. Il sert de base pour les trois primitives CASH : CEE, AOW et SH.

3.5.1 CEE : Cryptographic Evidence Explainability (Confidentialité)

L'**Expansion Entropique Chaotique (CEE)** est une fonction post-quantique basée sur l'itération de cartes polynomiales. Sa sécurité repose sur l'AIIP et elle assure la confidentialité (Privacy) par une expansion entropique minimisant la prévisibilité et la distance statistique à l'uniforme. Malgré sa lenteur relative, elle garantit la résilience quantique des données.

3.5.2 AOW : Affine One-Wayness (Fiabilité)

L'**Affine One-Wayness (AOW)** est le primitif CASH dédié à la fiabilité (Reliability) via la vérification temporelle post-quantique. Basé sur l'AIIP, il permet une liaison temporelle robuste intégrée aux preuves STARKs, garantissant l'intégrité et la non-contestabilité du temps de production.

3.5.3 SH : Semantic Holder (Opposabilité)

Le **Semantic Holder (SH)** est le composant CASH dédié à l'opposabilité juridique (Opposability). Basé sur l'AIIP, il garantit des interprétations juridiques vérifiables et l'extraction algébrique des traces polynomiales, assurant un score d'opposabilité élevé ($\Omega \geq 0,60$).

Synthèse comparative

L'ensemble des travaux présentés forme un écosystème de recherche cohérent, centré sur la construction d'une sécurité cryptographique post-quantique respectant les exigences institutionnelles de confiance et de droit.

Rôle du ZK-NR dans l'Investigation Numérique

Besoins des enquêteurs

Dans le cadre des enquêtes numériques, les magistrats et les forces de l'ordre se heurtent à plusieurs contraintes majeures :

- **Garantir l'intégrité des preuves collectées** : une preuve numérique est par nature volatile et altérable. Les enquêteurs doivent donc s'assurer que le contenu d'un disque dur, d'un message électronique ou d'un log réseau n'a subi aucune modification entre sa collecte et sa présentation au tribunal.
- **Prouver la non-répudiation des actes** : il ne suffit pas de montrer qu'une donnée existe ; il faut aussi démontrer de façon irréfutable que l'acte est bien attribuable à une personne donnée (ex. : un e-mail signé électroniquement par l'auteur présumé).
- **Préserver la confidentialité des données sensibles** : certaines enquêtes impliquent des données personnelles ou stratégiques. Il est indispensable de protéger ces informations tout en permettant une vérification cryptographique de leur validité.
- **Assurer la traçabilité et la chaîne de possession (chain of custody)** : chaque mouvement d'une preuve (collecte, transfert, stockage, analyse) doit être enregistré de manière fiable et opposable.

4 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 analyse des caractéristiques uniques (distance entre les yeux, forme du nez, contours de la mâchoire ou des lèvres) et est utilisée dans divers domaines : sécurité, téléphonie mobile, réseaux sociaux, etc. Cependant, elle soulève des enjeux éthiques et juridiques liés à la protection des données personnelles et à la vie privée.

4.1 Mode de fonctionnement d'un système biométrique

Un système biométrique fonctionne en trois phases principales :

- **Enrôlement** : capture et prétraitement des caractéristiques faciales de l'utilisateur, stockées en base avec éventuellement des informations biographiques.
- **Identification** : recherche 1-N pour déterminer l'identité d'un individu inconnu parmi les profils enregistrés.
- **Vérification (authentification)** : recherche 1-1 comparant les caractéristiques extraites à celles du profil déclaré, validée si le score de similitude dépasse un seuil.

Architecture d'un système biométrique

Un système biométrique se compose de quatre modules :

1. **Capture/Acquisition** : collecte des données via caméra ou scanner.
2. **Extraction de caractéristiques** : transformation des données en représentation mathématique (vecteur de caractéristiques).
3. **Correspondance** : comparaison du vecteur extrait avec les modèles stockés.
4. **Décision** : confirmation ou rejet de l'identité selon le score obtenu.

4.2 Méthodes de reconnaissance faciale

Les algorithmes de reconnaissance faciale se répartissent en trois catégories : classiques, points d'intérêt et apprentissage automatique/profond.

Méthodes classiques

- **Méthodes globales** : utilisent l'ensemble du visage. Rapides mais sensibles aux variations de lumière, pose ou expression. Exemples : PCA (Eigenfaces), LDA, SVM, réseaux de neurones, GMM, modèles 3D.
- **Méthodes locales (traits géométriques)** : se concentrent sur des régions spécifiques (yeux, nez, bouche), réduisant le bruit mais sensibles aux changements de vue. Exemples : HMM, EBGM, Eigen Object, template matching.
- **Méthodes hybrides** : combinent approches globales et locales pour unir leurs avantages, par exemple deep learning global + descripteurs locaux (SIFT, HOG) pour plus de robustesse.

5 Deepfake Audio

Un **deepfake audio** est un enregistrement sonore falsifié généré par intelligence artificielle (IA), capable d'imiter la voix d'une personne et de produire des paroles qu'elle n'a jamais prononcées. Il repose sur l'apprentissage profond et soulève des enjeux pour l'investigation numérique.

5.1 Évolution des deepfakes audio

- **1930-1990** : naissance des reproductions vocales (Voder, vocoders, synthèse par concaténation).
- **2000-2015** : modèles statistiques (HMM) plus naturels mais encore artificiels.
- **2016** : révolution du deep learning (WaveNet, DeepMind) et démonstrations publiques (Adobe VoCo, Lyrebird).
- **2017-2020** : démocratisation avec modèles Tacotron, Deep Voice et outils open-source (SV2TTS, Real-Time-Voice-Cloning).
- **2019-aujourd'hui** : usage malveillant croissant (fraudes, usurpations d'identité, désinformation).

Contexte d'utilisation

Applications légitimes :

- Accessibilité et inclusion (personnes ayant perdu la parole).
- Doublage audiovisuel et production multilingue.
- Assistants virtuels et interfaces vocales.
- Préservation des voix (mémoire ou patrimoine).

Applications malveillantes :

- Escroqueries et fraudes financières par imitation vocale.
- Usurpation d'identité et chantage.
- Manipulation de l'opinion publique.
- Falsification de preuves numériques.

5.2 Enjeux pour l'investigation numérique

Les deepfakes audio compromettent le triptyque CRO :

- **Confidentialité** : fuite de données sensibles.
- **Fiabilité** : remise en cause de l'authenticité des preuves.
- **Opposabilité** : difficulté à présenter les preuves devant un tribunal.

Ils rendent la vérification plus complexe et nécessitent transparence et compréhension technique (réseaux neuronaux, vocodeurs, spectrogrammes) pour anticiper les falsifications.

Cas pratique : MINIMAX Audio

- **Présentation** : outil de clonage vocal par IA, reproduisant timbre, intonation et rythme d'un locuteur réel.
- **Applications positives** : éducation, doublage multilingue, assistants vocaux personnalisés.
- **Applications détournées** : usurpation d'identité, escroqueries téléphoniques, diffusion de fausses informations.
- **Risque éthique et sécuritaire** : atteinte à la réputation, fraude, chantage. Exemples : fraude par PDG (2019), tromperie de systèmes de reconnaissance vocale (Stanford, 2020), clonage à partir de 5 secondes d'enregistrement (MIT, 2022).

5.3 Contre-mesures et prévention

- Détection technologique : outils d'analyse des signaux vocaux.
- Sensibilisation et éducation : formation à la reconnaissance des risques.
- Cadre légal et réglementaire : lois spécifiques et marquage numérique.
- Techniques de sécurisation : authentification vocale dynamique et multi-facteur.
- Éthique et gouvernance de l'IA : consentement et transparence dans l'usage.

MINIMAX Audio illustre le potentiel éducatif et les risques du deepfake vocal. Seule une combinaison de détection, régulation, sécurisation et éthique permettra d'en tirer les bénéfices tout en limitant les abus.

6 Outils pour la Rédaction de Mémoire

La rédaction d'un mémoire représente un défi majeur pour l'étudiant. La réussite dépend du choix des outils logiciels, qui doivent offrir :

- Un environnement adapté aux longs documents (LaTeX ou traitement de texte classique)
- Une gestion rigoureuse des références bibliographiques
- Une mise en forme conforme aux standards académiques

Nous présentons ici trois outils : Overleaf, Microsoft Word et Zotero.

Overleaf : L'Excellence Académique par LaTeX

1.1 Historique

Fondé en 2012 par John Hammersley et John Lees-Miller, Overleaf simplifie la rédaction collaborative en LaTeX. Racheté par Springer Nature en 2023, il est devenu un standard mondial pour les publications scientifiques.

6.1 Atouts majeurs

- Qualité typographique exceptionnelle
- Gestion avancée des références croisées
- Collaboration en temps réel
- Modèles académiques prêts à l'emploi

1.4 Limites et alternatives

- Courbe d'apprentissage élevée pour les novices
- Édition hors ligne limitée en version gratuite
- Alternatives : LyX, TeXmaker, TeXstudio, Authorea

Microsoft Word : Le Référencement en Traitement de Texte

L'outil universel

Word est l'outil de traitement de texte le plus répandu, familier et compatible avec la majorité des utilisateurs et institutions.

6.2 Points forts académiques

- Gestion avancée des styles et structuration
- Génération automatique des tables (matières, figures, tableaux)
- Suivi des modifications et commentaires
- Compatibilité et accessibilité

Zotero : Le Spécialiste de la Bibliographie

Présentation

Zotero est un gestionnaire de références open-source, centralisant et organisant toutes les sources d'un mémoire.

6.3 Fonctionnalités essentielles

- Capture automatique des références depuis le web
- Intégration avec Word, LibreOffice et Overleaf (BibTeX)
- Gestion avancée des styles de citation (APA, MLA, Chicago, etc.)
- Synchronisation et stockage cloud des PDF

Intégrations techniques

- Export BibTeX depuis Zotero vers Overleaf
- Plugins Zotero pour Word
- Styles de citation cohérents sur tous les outils

6.4 Tableau Comparatif des Fonctionnalités

Fonctionnalité	**Overleaf**	**Microsoft Word**	**Zotero**
Type d'outil	Éditeur LaTeX en ligne	Traitement de texte	Gestionnaire de références
Prix	Gratuit limité / Payant	Payant (Office 365) / Gratuit version web	Entièrement gratuit
Courbe d'apprentissage	Élevée	Faible	Modérée
Collaboration	Excellent	Bon	Via Zotero Groups
Gestion bibliographique	Via BibTeX	Basique	Exceptionnelle
Qualité typographique	Professionnelle	Variable	N/A
Styles de citation	Personnalisables	Limités	10 000+ styles
Gestion des équations	Excellente	Correcte	N/A
Structure document	Via LaTeX code	Styles Word	Collections
Export PDF	Natif	Correct	Oui
Stockage cloud	Intégré	OneDrive / 300 MB gratuit	Synchronisation manuelle
Modèles académiques	Nombreux	Quelques-uns	N/A

7 Simulation de Conversations WhatsApp et Investigation Numérique

Dans le contexte actuel, les applications de messagerie instantanée comme WhatsApp sont à la fois des sources d'information et des vecteurs de manipulation. L'investigation numérique vise à analyser et comprendre ces environnements, notamment les traces laissées par les utilisateurs et les possibilités de falsification.

Mise en situation

Le scénario simulé concerne un enseignant (Paul KENGNE) ayant une relation extra-conjugale avec une étudiante. Éléments fournis pour l'analyse :

- Sept captures d'écran WhatsApp
- Deux photos envoyées via WhatsApp

7.1 Contenu des échanges

- Messages à caractère affectif et sexuel explicite
- Invitations à se rencontrer en dehors du cadre scolaire
- Expressions telles que *"Bonsoir mon cœur"*, *"Je t'aime mon sucre"*
- Promesse de l'époux de quitter sa femme

7.2 Méthodologie de falsification

Deux outils ont été utilisés : Chatsmock et Adobe Photoshop.

7.2.1 Chatsmock

- Création de fausses conversations WhatsApp
- Définition des participants (nom, photo, numéro)
- Génération de messages personnalisés avec date, heure et statut de lecture
- Export de captures d'écran réalistes

7.2.2 Adobe Photoshop

- Correction graphique (alignement, bulles, couleurs)
- Insertion ou modification d'images
- Retouche pour correspondre à l'interface réelle d'un smartphone

Conclusion méthodologique

La combinaison Chatsmock + Photoshop permet de créer des preuves numériques visuellement crédibles, montrant les limites des captures d'écran comme preuves irréfutables.

7.3 Limites et comparaison des outils

7.4 Limites de Chatsmock

- Réalisme limité sur certains détails graphiques
- Fonctionnalités restreintes (notes vocales, appels, réactions)
- Export uniquement au format image
- Détectable par une analyse forensique attentive

7.5 Comparaison avec d'autres outils

- **FakeChat** : plus d'options visuelles mais moins crédible pour un expert
- **WhatsFake** : orienté blagues, interface moins personnalisable
- **Photoshop et éditeurs graphiques avancés** : liberté totale, réalisme quasi indétectable
- **Outils forensiques détournés** : manipulation directe des bases de données

3.3 Conclusion partielle

Chatsmock est simple et accessible, mais ses limites peuvent être compensées par Photoshop ou d'autres outils plus sophistiqués.

7.6 Impact sur l'investigation numérique et recommandations

- Diminution de la fiabilité des captures d'écran
- Besoin accru de compétences techniques pour les experts
- Risque de manipulation judiciaire ou disciplinaire
- Multiplication des faux dossiers

Recommandations

- Vérification technique des preuves (métadonnées, signature numérique)
- Sensibilisation et formation des acteurs judiciaires
- Utilisation d'outils spécialisés de détection de manipulations
- Préférence pour les données brutes extraites des bases de données
- Renforcement du cadre légal sur l'acceptabilité des preuves numériques

8 L'Investigation Numérique au Service de la Police Judiciaire

L'investigation numérique, ou digital forensic, consiste à collecter, analyser, conserver et présenter des preuves numériques issues d'ordinateurs, téléphones, réseaux ou autres supports électroniques, dans le cadre d'enquêtes judiciaires, administratives ou privées. Son importance croissante découle de la digitalisation et de la cybercriminalité.

Apports essentiels à la police judiciaire

8.1 Accès à des preuves invisibles

- Récupération de traces difficiles à effacer : historiques, conversations supprimées, métadonnées, fichiers récupérables.
- Création d'une "scène de crime virtuelle" complémentaire à la scène physique.

8.2 Lutte contre la cybercriminalité

- Résolution de piratage, fraudes en ligne, ransomwares, phishing.
- Sans investigation numérique, ces infractions seraient presque impossibles à résoudre.

8.3 Identification et traçage des auteurs

- Analyse d'IP, journaux systèmes, connexions réseau.
- Récupération de géolocalisation et communications (SMS, WhatsApp, emails).

8.4 Reconstitution des événements

- Chronologie des fichiers créés, modifiés ou transférés.
- Connexions utilisateurs et données effacées.

8.5 Preuves recevables en justice

- Respect de l'intégrité et traçabilité des données.
- Permet à la justice de prendre des décisions sur des preuves fiables.

8.6 Soutien aux enquêtes traditionnelles

- Complète vidéosurveillance, fouilles physiques, recherches d'indices.

Principaux domaines d'application

8.7 Cybercriminalité

- Exemples : réseaux de fraude en ligne à Douala, phishing ciblant entreprises.
- Techniques : analyse logs, récupération données effacées, traçage flux financiers.

8.8 Grande criminalité transfrontalière et terrorisme

- Exemples : trafic de stupéfiants Nigeria-Cameroun, cartographie de Boko Haram.
- Techniques : analyse métadonnées, géolocalisation, profilage réseaux criminels.

8.9 Criminalité financière et économique

- Exemples : détournements fonds publics, fraudes fiscales.
- Techniques : traçage transactions électroniques, data mining, corrélation données.

8.10 Criminalité organisée et crimes violents

- Exemples : kidnapping à Yaoundé, vols à main armée dans le Littoral.
- Techniques : reconstitution chronologique, analyse vidéo, communications téléphoniques.

8.11 Protection de l'enfance et lutte contre la pédopornographie

- Exemples : démantèlement de réseaux pédopornographiques.
- Techniques : analyse images/vidéos, traçage IP, coopération internationale.

8.12 Enquêtes judiciaires classiques

- Exemples : fraudes électorales, conflits fonciers.
- Techniques : authentification documents numériques, extraction preuves depuis ordinateurs et smartphones.

9 Investigation Numérique et Cyberattaques en Afrique (2015-2025)

Contexte général

Depuis une décennie, l'Afrique connaît une révolution numérique rapide, avec :

- L'essor des technologies de l'information.
- La digitalisation des services publics.
- L'émergence des fintechs et des services numériques.

3. Dix cas africains emblématiques (2015-2025)

9.1 Cas 1 – Ransomware Transnet (Afrique du Sud, 2021)

- Type : Entreprise publique logistique et transport.
- Taille : Nationale, ports de Durban, Cape Town, Ngqura.
- Volume : 7 To de données logistiques et ERP chiffrées.
- Impact financier : 60 millions USD de pertes, 3 semaines d'arrêt.

9.2 Cas 2 – Breach CNSS (Maroc, 2025)

- Type : Organisme étatique de sécurité sociale.
- Taille : 2 millions de salariés, 500 000 entreprises.
- Volume : Données personnelles, salaires, historiques médicaux.
- Impact financier : perte de confiance, coûts de remédiation élevés.

9.3 Cas 3 – Attaque Eneo (Cameroun, 2024)

- Type : Fournisseur national d'électricité.
- Taille : Perturbation des systèmes de facturation et prépayés.
- Volume : Données clients et journaux de transaction compromis.
- Impact financier : plusieurs centaines de millions de FCFA.

9.4 Cas 4 – GhostLocker 2.0 (Egypte, 2024)

- Type : Entreprises industrielles et gouvernementales.
- Taille : 30 organisations ciblées.
- Volume : Documents stratégiques, données industrielles, accès VPN volés.
- Impact financier : 20 millions USD rançon + pertes indirectes.

9.5 Cas 5 – Scandale Pegasus (Maroc, 2020-2021)

- Type : Entreprises industrielles et gouvernementales.
- Taille : 30 organisations.
- Volume : Données industrielles et documents stratégiques volés.
- Impact financier : 20 millions USD + pertes indirectes.

9.6 Cas 6 – Piratage banques ivoiriennes

- Type : Banques privées (UBA, BNI, NSIA Bank).
- Taille : Attaques simultanées sur plusieurs systèmes.
- Volume : Données clients, identifiants bancaires, transactions SWIFT.
- Impact financier : 6 millions EUR de pertes.

9.7 Cas 7 – Systèmes de santé tunisien (2021)

- Type : Ministère de la Santé et hôpitaux.
- Taille : Attaque DDoS + ransomware.
- Volume : Dossiers médicaux et serveurs hospitaliers.
- Impact financier : 2,5 millions USD, retards dans traitements.

9.8 Cas 8 – Ethiopian Airlines (2023)

- Type : Compagnie aérienne nationale.
- Taille : Compromission mondiale du système de réservation.
- Volume : Données personnelles de milliers de passagers.
- Impact financier : 5 millions USD + atteinte réputation.

9.9 Cas 9 – Fraude Mobile Money MTN Nigeria (2018)

- Type : Télécom et fintech.
- Taille : Réseau mobile de millions d'utilisateurs.
- Volume : Données transactionnelles et identifiants mobiles.
- Impact financier : 8 millions USD.

9.10 Cas 10 – Piratage Banque Centrale Nigeria (2015-2016)

- Type : Institution financière étatique.
- Taille : Intrusion longue durée sur serveurs SWIFT.
- Volume : Données financières et courriers internes.
- Impact financier : plusieurs dizaines de millions USD.

10 Investigation Numérique sur TikTok : Projet Innotrends

Contexte

À l'ère des réseaux sociaux, TikTok influence l'opinion, les comportements et les interactions humaines. Ce projet s'inscrit dans une démarche pédagogique visant à :

- Comprendre les enjeux de l'identité numérique.
- Analyser la viralité des contenus et les risques de manipulation.
- Sensibiliser aux bonnes pratiques de sécurité en ligne.

Pour ce faire, un faux profil a été créé autour de la cybersécurité, dans un cadre strictement fictif et éthique, afin d'observer les réactions et interactions générées.

10.1 1.1 Création du faux profil

- Utilisation d'une messagerie temporaire (Temp Mail) pour préserver l'anonymat.
- Base d'observation et d'analyse des interactions dans la niche cybersécurité.

Stratégie de contenu

- Contenu éducatif et engageant autour de thématiques :
  - Sécurité des mots de passe
  - Gestion des données personnelles
  - Arnaques en ligne
- Ton léger et humoristique pour favoriser l'engagement.
- Publications accompagnées de visuels attractifs (bandes dessinées, vidéos courtes).
- Respect des règles de la plateforme et observation des réactions sans manipulation.

10.2 Outils et moyens de suivi

- TikTok Analytics : vues, likes, partages, taux d'engagement, abonnés.
- Captures d'écran et suivi des publications.
- Générateurs de contenu : ChatGPT (messages), Canva (visuels).
- Temp Mail pour le compte, WhatsApp pour partager les accès.
- Tableau de bord personnel pour noter observations et hypothèses.

Analyse et observation

10.3 Pertinence de la stratégie

- Contenu éducatif + ton ludique + visuels accrocheurs = engagement du public.
- Thématiques proches du quotidien (Wi-Fi public, mots de passe, arnaques) favorisent identification et interactions.
- La bio percutante contribue à l'attractivité et à la crédibilité du profil.

10.4 Comportement des utilisateurs

- Même fictif, le faux profil soulève des enjeux éthiques liés à la simulation de comportements frauduleux.
- Nécessité de ne pas tromper ni mettre en danger les utilisateurs.
- Met en lumière le pouvoir de manipulation des réseaux sociaux et la responsabilité des diffuseurs de contenu.

Conclusion générale

Ce projet d'investigation numérique autour d'un faux profil TikTok a permis de mettre en lumière plusieurs enseignements clés. Tout d'abord, il illustre le pouvoir des réseaux sociaux pour capter l'attention et diffuser des informations, même dans un cadre fictif et pédagogique. La cybersécurité, en tant que thématique, s'est révélée pertinente pour sensibiliser les utilisateurs aux risques numériques et aux bonnes pratiques à adopter.

Ensuite, l'expérience souligne l'importance de l'éthique et de la responsabilité dans toute démarche d'investigation numérique. Même à des fins éducatives, la création de faux profils et la diffusion de contenus simulés nécessitent un encadrement strict afin de protéger les utilisateurs et de respecter leur vie privée.

Enfin, ce travail met en évidence le potentiel pédagogique de l'observation et de l'analyse des interactions numériques. Il permet non seulement de comprendre le comportement des utilisateurs, mais également d'identifier les vecteurs de diffusion de l'information et les vulnérabilités numériques.

Ainsi, l'investigation numérique, combinée à une approche éthique et structurée, constitue un outil précieux pour l'éducation, la prévention et la sensibilisation à la cybersécurité, tout en renforçant la réflexion critique sur les usages des plateformes sociales.