École Nationale Supérieure Polytechnique de Yaoundé

RESUME DES EXPOSES
Théories et Pratiques de l'Investigation Numérique

Nom et Prenoms de l'etudiant : **MELONE** Andre Vladmir

Matricule : **22p059**

Unité d'Enseignement : **Introduction aux Techniques d'Investigation Numérique**

Classe : **Niveau 4**

Filière : **Cybersécurité et Investigation Numérique**

Enseignant :
Monsieur MINKA MI NGUIDJOI Thierry Emmanuel

Table des matières

1 Theme 1 : Realisation d'unee video deepfake

Un deepfake est un enregistrement vidéo ou audio réalisé ou modié grâce à l'intelligence articielle. 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" . En fait, il fait référence à des contenus faux qui sont rendus profondément crédibles par l'intelligence artificielle. En 2014, Ian Goodfellow invente le GAN (Generative Adversarial Network), une technologie révolutionnaire où deux algorithmes s'entraînent mutuellement : l'un crée des images ou vidéos réalistes, tandis que l'autre tente de détecter les faux. Ce concept a donné naissance aux deepfakes, capables de générer des contenus audiovisuels presque indiscernables du réel. Bien qu'utiles pour le cinéma, la communication ou la formation, les deepfakes présentent aussi de graves inconvénients, notamment la propagation de fausses informations, l'usurpation d'identité et les atteintes à la vie privée. Dans le cadre de notre projet, nous avons utilisé GPT-5 et HeyGen AI. GPT-5, grâce à ses capacités de génération de texte et de raisonnement, a servi à rédiger le script du premier chapitre du cours. Ce script a ensuite été exploité dans HeyGen AI, une IA spécialisée dans la création de vidéos, pour produire une présentation claire, interactive et professionnelle destinée aux étudiants. Cette approche illustre comment l'intelligence artificielle peut transformer l'enseignement en rendant l'apprentissage plus immersif et dynamique, tout en ouvrant de nouvelles perspectives pédagogiques et créatives.

2 Theme 2 : Simulation de faux messages whatsapp pouvant pousser a un divorce

Dans cet exercice d'investigation numérique, une fausse conversation WhatsApp entre un enseignant et une étudiante a été simulée à l'aide de Chatsmock et d'Adobe Photoshop. Chatsmock a servi à créer les échanges fictifs avec noms, messages et horaires personnalisés, tandis que Photoshop a permis de retoucher les captures pour un rendu parfaitement réaliste. Cette combinaison démontre la facilité de falsification des preuves numériques et souligne la fragilité des captures d'écran comme éléments de preuve fiables. Chatsmock est un outil simple permettant de simuler des conversations WhatsApp, utile dans des contextes ludiques ou éducatifs. Cependant, il présente plusieurs limites : un manque de réalisme graphique, des fonctionnalités restreintes et une dépendance au format image. De plus, une analyse forensique approfondie peut révéler des incohérences dans les métadonnées, compromettant la crédibilité des faux générés. Comparativement, FakeChat offre davantage d'options visuelles mais reste peu fiable pour un usage expert, tandis que WhatsFake privilégie l'aspect divertissement au détriment du réalisme. Photoshop et d'autres éditeurs avancés permettent une falsification plus poussée, mais exigent des compétences techniques. Ces outils, bien qu'efficaces, posent un sérieux défi à l'investigation numérique, car ils facilitent la manipulation de preuves. D'où la nécessité d'une vérification technique systématique, d'une formation accrue des acteurs judiciaires et d'un encadrement légal renforcé pour garantir l'intégrité des preuves numériques.

3 Theme 3 : Les trois meilleurs logiciels pour rediger des memoires :

La rédaction d'un mémoire constitue un défi académique majeur, exigeant rigueur, méthode et outils adaptés. Face à la complexité de la gestion des sources et des normes, le choix du logiciel de rédaction devient déterminant. Trois solutions majeures se distinguent : Overleaf, Microsoft Word et Zotero. Overleaf, fondé en 2012, offre un environnement LaTeX collaboratif en ligne alliant accessibilité, rigueur typographique et travail d'équipe. Idéal pour les disciplines scientifiques, il garantit une mise en forme professionnelle et une gestion avancée des références, malgré une courbe d'apprentissage initiale. Word, de son côté, reste l'outil universel de rédaction grâce à sa familiarité, son intégration bureautique et sa compatibilité étendue. Il se montre efficace pour structurer un mémoire via les styles et les tables automatiques, mais ses fonctions bibliographiques demeurent limitées sans l'appui d'un outil externe. C'est là qu'intervient Zotero, gestionnaire open-source de références bibliographiques. Gratuit et puissant, il centralise, synchronise et intègre les sources dans Word ou Overleaf, tout en supportant des milliers de styles de citation. L'efficacité optimale réside dans la combinaison de ces outils : Word + Zotero pour la simplicité, Overleaf + Zotero pour l'excellence scientifique, ou encore Overleaf + Zotero Groups pour la collaboration. Ces synergies assurent une rédaction fluide, une bibliographie rigoureuse et une qualité académique élevée. Le choix dépend donc du profil de l'utilisateur : débutant, scientifique ou collaboratif. Ensemble, ces solutions constituent un écosystème complet au service de la réussite académique.

4 Theme 4 : Les 10 plus grands cas de hacking en Afrique

La cybersécurité africaine connaît une phase décisive marquée par une forte numérisation de tous les secteurs : santé, énergie, finance, éducation, administration mais aussi par une fragilité structurelle. Le continent souffre encore d'un faible cadre législatif, d'un manque criant de compétences locales, d'infrastructures obsolètes et d'une dépendance vis-à-vis des prestataires étrangers. Ces faiblesses favorisent la prolifération des attaques : ransomwares, fraudes au mobile money, espionnage politique, DDoS et désinformation. outefois, plusieurs pays (Maroc, Cameroun, Nigéria, Afrique du Sud) amorcent une transition vers une cybersouveraineté grâce à la création de CERT, de lois et de formations spécialisées. L'investigation numérique repose sur cinq étapes clés : identification, collecte et préservation des preuves, analyse technique et rédaction de rapport. L'évaluation des incidents s'appuie sur quatre critères : taille de l'attaque, type d'organisation, volume de données et impact économique. Dix cas emblématiques illustrent la diversité des menaces : ransomware sur Transnet (Afrique du Sud, 2021), fuite massive à la CNSS (Maroc, 2025), attaque sur Eneo (Cameroun, 2024), ransomware GhostLocker 2.0 (Égypte, 2024), scandale Pegasus (Maroc), piratages bancaires ivoiriens, cyberattaque du système de santé tunisien, compromission d'Ethiopian Airlines, fraude au Mobile Money (MTN Nigeria, 2018) et piratage de la Banque centrale du Nigeria. Ces incidents ont entraîné des pertes cumulées de plusieurs centaines de millions de dollars et révèlent une vulnérabilité systémique.

Dans ce contexte, le renforcement des capacités nationales et la coopération régionale apparaissent essentiels pour bâtir une cybersécurité africaine souveraine et durable.

5 Theme 5 : Deepfake vocal :

Le deepfake audio désigne la synthèse vocale falsifiée créée par des modèles d'apprentissage profond, capables d'imiter avec précision le timbre, l'intonation et le rythme d'une personne à partir d'enregistrements réels. Né des progrès de la synthèse vocale depuis les premiers vocoders jusqu'au tournant de 2016 marqué par WaveNet et les architectures neuronales. le phénomène s'est popularisé grâce à modèles comme Tacotron, Deep Voice et des outils open-source (SV2TTS, Real-Time-Voice-Cloning). Cette démocratisation ouvre des usages positifs : accessibilité pour personnes aphoniques, doublage multilingue, assistants vocaux personnalisés ou préservation de voix. Toutefois, elle permet aussi des détournements dangereux : escroqueries financières, usurpations d'identité, manipulation politique, falsification de preuves et contournement d'authentifications vocales. Des incidents marquants (fraude du PDG en 2019, études montrant la vulnérabilité des systèmes commerciaux, clonage à partir de quelques secondes d'audio) illustrent l'ampleur du risque.Pour l'investigation numérique, les deepfakes audio posent trois défis principaux : atteinte à la confidentialité, remise en cause de la fiabilité des preuves et difficulté d'opposabilité devant les juridictions. Ils contraignent les experts à renforcer les protocoles forensiques collecte et conservation d'empreintes acoustiques, analyses spectrales et métadonnées, recours à des détecteurs basés sur l'IA tout en garantissant la transparence méthodologique exigée par les tribunaux. Les contre-mesures combinent progrès technologiques (outils de détection intégrés, watermarking, traçabilité des modèles), sécurisation des authentifications (MFA, biométrie dynamique, vérification out-of-band), sensibilisation des utilisateurs, formation des forces de l'ordre et coopération internationale en matière de réglementation et de recherche. Des initiatives académiques et industrielles développent datasets et benchmarks pour améliorer la détection, mais la course entre synthèse et détection reste active. Maîtriser techniquement et éthiquement les deepfakes audio est désormais indispensable : condition pour tirer parti de leurs bénéfices tout en protégeant l'intégrité des preuves, la vie privée et la confiance numérique essentielle.

6 Theme 6 : La place de l'investigation numerique dans la police judiciaire

L'investigation numérique constitue aujourd'hui un pilier majeur de la police judiciaire, offrant des capacités inédites pour l'accès, l'analyse et la validation des preuves numériques. Elle permet d'exploiter des traces invisibles dans le monde physique telles que les historiques de navigation, les fichiers supprimés ou les métadonnées, ouvrant ainsi une véritable « scène de crime virtuelle ». Ces techniques s'avèrent essentielles pour lutter contre la cybercriminalité (fraudes, ransomwares, piratage, phishing), où les indices matériels sont rares, mais les traces numériques multiples. L'investigation numérique facilite également l'identification et le traçage des auteurs grâce à l'analyse des adresses IP, des

journaux système, des données de géolocalisation ou de messagerie. Elle permet la reconstitution précise de la chronologie des événements, en déterminant quand et comment les fichiers ont été créés, modifiés ou transférés. Ces éléments contribuent à l'élaboration du scénario du crime. Par ailleurs, les procédures d'acquisition et de conservation des preuves garantissent leur intégrité et leur recevabilité devant les tribunaux, assurant ainsi des décisions judiciaires fondées sur des éléments fiables. L'investigation numérique complète et renforce aussi les enquêtes traditionnelles : l'analyse de communications ou de vidéosurveillance vient appuyer les fouilles physiques, offrant une vision globale et cohérente des faits. En conclusion, l'investigation numérique transforme profondément le travail de la police judiciaire. Elle fournit des moyens techniques puissants pour détecter, comprendre et prouver les infractions dans un monde de plus en plus dématérialisé, où les traces numériques sont devenues les témoins clés de la vérité judiciaire.

7 Theme 7 : creation et administration d'un faux profil TikTok

L'investigation numérique menée sous le thème **Innotrends** s'inscrit dans une démarche éducative et éthique visant à sensibiliser les internautes aux risques de la cybersécurité à travers les réseaux sociaux. Le projet a consisté à créer un faux profil TikTok, conçu comme un outil de sensibilisation et d'observation, afin d'étudier les comportements des utilisateurs face à des contenus liés à la sécurité numérique. Ce choix s'appuie sur la volonté d'apporter une valeur ajoutée positive en informant sans nuire, tout en respectant la vie privée et les règles éthiques de l'investigation numérique. La stratégie de contenu adoptée reposait sur une approche ludique et éducative, articulée autour de thématiques accessibles comme la sécurité des mots de passe, la gestion des données personnelles ou la prévention contre les arnaques en ligne. Les publications, accompagnées de visuels attractifs et de messages humoristiques, ont su capter l'attention tout en diffusant des messages de prévention pertinents. Le ton utilisé, proche du langage des jeunes internautes, a favorisé l'engagement sans manipulation ni tromperie, rendant la démarche à la fois informative et participative. Plusieurs outils de suivi ont été mobilisés : TikTok Analytics pour mesurer les interactions (vues, likes, abonnés), Canva et ChatGPT pour la création de contenus, Temp Mail pour la gestion du compte, ainsi qu'un tableau de bord personnel pour consigner les observations. Les résultats ont montré un intérêt réel, avec plus de 100 mentions « j'aime » et une bonne réceptivité des utilisateurs aux messages de cybersécurité. L'analyse a mis en lumière la pertinence de la stratégie et l'importance d'un cadre éthique dans la simulation d'identités en ligne. Bien que le projet ait suscité un engagement positif, il a aussi révélé les risques potentiels liés à la diffusion de contenus ambigus. D'où plusieurs recommandations : renforcer l'éducation numérique dès le secondaire, encadrer l'usage pédagogique des faux profils et promouvoir une approche interdisciplinaire alliant technique, droit et communication. En conclusion, cette expérience démontre qu'une sensibilisation efficace à la cybersécurité peut être à la fois interactive, responsable et ancrée dans les réalités numériques actuelles.

8 Theme 8 : Presentation des algorithmes de reconnaissance faciale

La reconnaissance faciale (RF) est une technique biométrique d'intelligence artificielle permettant d'identifier ou de vérifier une personne à partir de ses traits faciaux. Utilisée en sécurité, téléphonie et réseaux sociaux, elle repose sur des algorithmes qui extraient des caractéristiques discriminantes (distance interoculaire, contours, etc.). Pour l'investigateur numérique, la RF est un outil stratégique pour traiter rapidement de grands volumes d'images et de vidéos extraites de scènes publiques ou d'appareils saisis, mais elle soulève d'importantes questions techniques, juridiques et éthiques. Un système biométrique fonctionne en trois phases : enrôlement (capture et stockage d'un modèle facial), identification (recherche 1-N) et vérification (comparaison 1-1). Son architecture comprend quatre modules : capture, extraction de caractéristiques, correspondance et décision. Les méthodes utilisées vont des approches classiques (PCA, LDA, SVM) aux détecteurs/descripteurs locaux (SIFT, HOG, SURF) jusqu'aux modèles de machine/deep learning (embeddings, réseaux profonds). Les approches hybrides cherchent à combiner robustesse locale et puissance globale. Les avantages opérationnels sont clairs : automatisation, vitesse et capacité d'analyser des heures de vidéo pour repérer des individus. Néanmoins, la RF présente de nombreuses limites : sensibilité aux conditions (éclairage, pose, masques), « boîte noire » des modèles profonds rendant l'explicabilité difficile, interopérabilité limitée entre solutions, vulnérabilités aux attaques adversariales et risques d'usurpation (deepfakes, replays, masques 3D). Sur le plan éthique et sociétal, la RF pose des risques de violation de la vie privée, de discrimination (biais selon l'origine, le genre, l'âge) et d'effet dissuasif sur les libertés publiques. Sur le plan juridique, l'utilisation des données biométriques nécessite une base légale (consentement ou mandat), une traçabilité stricte et des études d'impact. Les enjeux organisationnels incluent des coûts matériels (GPU, stockage), maintenance, acceptabilité sociale et formation des opérateurs. Pour un déploiement responsable et spécialement dans le contexte camerounais il est recommandé de documenter les pipelines et versions de modèles, réaliser des tests locaux (benchmarks), mettre en place des contrôles anti-spoofing multi-sensoriels, chiffrer les templates, effectuer des DPIA et audits de biais, encadrer juridiquement les usages (mandat judiciaire pour identification ciblée), piloter des déploiements restreints et exiger la validation humaine pour toute décision critique. En conclusion, la reconnaissance faciale peut être un atout puissant pour l'investigation numérique si elle est encadrée par des garanties techniques, juridiques et éthiques. Sans ces garde-fous, elle risque des dérives majeures ; avec eux, elle contribue efficacement à la sécurité tout en respectant les droits fondamentaux.