

Synthèse des Exposés d'Investigation Numérique

Cours d'Investigation Numérique

Auteur : MVONGO MEDJO ORDI FAREL

Matricule : 22P039

Année Académique : 2025/2026

Introduction

Cette synthèse présente une analyse consolidée des différents exposés réalisés dans le cadre du cours d'Investigation Numérique. Elle couvre les principaux thèmes abordés, allant des outils techniques aux enjeux opérationnels, en passant par les aspects éthiques et juridiques de l'investigation numérique moderne.

1 – L'utilité de l'investigation numérique dans la police judiciaire

- **Thème principal** : Rôle stratégique de l'investigation numérique dans les forces de l'ordre
- **Contribution** : Démonstration des apports essentiels aux enquêtes judiciaires
- **Points clés** :
 - Accès aux preuves numériques invisibles dans le monde physique
 - Lutte contre la cybercriminalité et identification des auteurs
 - Reconstitution des événements et production de preuves recevables
 - Domaines d'application : criminalité financière, terrorisme, protection de l'enfance
- **Défis identifiés** : Explosion des données, respect des droits fondamentaux, limites techniques et financières

2 – Protocole ZK-NR et opposabilité légale

- **Thème principal** : Cryptographie avancée pour la non-répudiation
- **Contribution** : Présentation du protocole ZK-NR (Zero-Knowledge Non-Repudiation)
- **Concepts innovants** :

- Trilemme CRO (Confidentialité, Fiabilité, Opposabilité)
- Primitives cryptographiques : CEE, AOW, SH
- Résilience post-quantique
- **Application** : Renforcement de la valeur juridique des preuves numériques

3 - Investigation Numérique Les 10 cas de hacking en Afrique.pdf

- **Thème principal** : Analyse des cyberattaques majeures en Afrique
- **Contribution** : Étude comparative de 10 cas emblématiques (2015-2025)
- **Cas notables** :
 - Ransomware Transnet (Afrique du Sud, 2021)
 - Fuite CNSS (Maroc, 2025)
 - Attaque Eneo (Cameroun, 2024)
 - Scandale Pegasus (Maroc, 2020-2021)
- **Critères d'analyse** : Taille de l'attaque, type d'organisation, volume de données, impact financier
- **Recommandations** : Formation, CERT régionaux, harmonisation légale

4 – Les trois meilleurs logiciels de rédaction de mémoire

- **Thème principal** : Outils académiques pour l'investigation numérique
- **Contribution** : Analyse comparative des logiciels de rédaction
- **Outils étudiés** :
 - Overleaf (LaTeX) - Excellence académique
 - Microsoft Word - Accessibilité
 - Zotero - Gestion bibliographique
- **Combinaisons recommandées** :
 - Word + Zotero (débutants)
 - Overleaf + Zotero (scientifiques)
 - Overleaf + Zotero Groups (collaboration)

5 – Algorithmes de reconnaissance faciale

- **Thème principal** : Biométrie et identification faciale
- **Contribution** : Analyse technique et éthique des systèmes RF
- **Aspects techniques** :
 - Architecture des systèmes biométriques

- Méthodes de reconnaissance (globales, locales, hybrides)
- Détecteurs de points d'intérêt (SIFT, HOG, SURF)
- **Enjeux identifiés :**
 - Biais algorithmiques et discrimination
 - Protection des données biométriques é légale et vie privée
- **Recommandations :** Documentation, tests locaux, cadre réglementaire

6 – Deepfake vocal

- **Thème principal :** Falsification audio par intelligence artificielle
- **Contribution :** Étude technique et éthique des deepfakes vocaux
- **Évolution technologique :** De Voder (1939) à MINIMAX Audio (2024)
- **Applications :**
 - Légitimes : accessibilité, doublage, préservation vocale
 - Malveillantes : usurpation, escroqueries, manipulation
- **Enjeux pour l'investigation :** Fiabilité des preuves audio, détection des falsifications
- **Contre-mesures :** Détection technologique, cadre légal, sensibilisation

7 – Faux profil TikTok dans une niche cybersécurité

- **Thème principal :** Investigation des réseaux sociaux et sensibilisation
- **Contribution :** Création et analyse d'un faux profil éducatif
- **Stratégie :** Profil "InnoTrends" dédié à la cybersécurité
- **Contenu :** Mots de passe, Wi-Fi public, phishing, empreinte numérique
- **Résultats :** Engagement significatif (100+ likes, 300+ vues)
- **Enseignements :** Efficacité pédagogique, questions éthiques, responsabilité numérique

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

- **Thème principal :** Création de contenu synthétique pédagogique
- **Contribution :** Production d'un deepfake éducatif utilisant l'IA générative
- **Outils utilisés :**
 - GPT-5 : génération du script
 - HeyGen : création de l'avatar et synthèse vocale
- **Fonctionnalités exploitées :** Avatar IA, clonage vocal, traduction multilingue
- **Réflexion :** Potentiel pédagogique vs risques d'abus et enjeux éthiques

9 – Falsification de conversations WhatsApp

- **Thème principal** : Manipulation des preuves numériques
- **Contribution** : Démonstration pratique de falsification de conversations
- **Outils utilisés** : Chatsmock et Adobe Photoshop
- **Scénario** : Conversation fictive entre enseignant et étudiante
- **Conclusions** :
 - Facilité de falsification des preuves numériques
 - Limites de fiabilité des captures d'écran
 - Nécessité de méthodes de vérification avancées
- **Recommandations** : Analyse des métadonnées, formation des acteurs judiciaires

Conclusion Générale

Les exposés analysés démontrent la richesse et la diversité des thématiques en investigation numérique. Plusieurs tendances se dégagent :

- **Diversification des outils** : De la cryptographie avancée (ZK-NR) aux deepfakes en passant par les réseaux sociaux
- **Enjeux éthiques croissants** : Biais algorithmiques, falsification des preuves, protection de la vie privée
- **Nécessité d'encadrement** : Cadres légaux adaptés, formation continue, collaboration internationale
- **Innovation technologique** : IA générative, biométrie, preuves zero-knowledge

L'investigation numérique moderne nécessite une approche pluridisciplinaire intégrant compétences techniques, conscience éthique et connaissance juridique pour faire face aux défis croissants de la criminalité numérique.

Synthèse réalisée par MVONGO MEDJO ORDI FAREL
Dans le cadre du cours d'Investigation Numérique