ÉCOLE NATIONALE SUPÉRIEURE
POLYTECHNIQUE DE YAOUNDÉ

Résumé Global des Neuf Thèmes d'Investigation Numérique

Présenté par : José Loïc Minyanda Yongui
Matricule : 22P071
Encadré par : M. MINKA MI NGUIDJOI Thierry Emmanuel
Année académique : 2025

Introduction Générale

L’évolution rapide des technologies numériques a profondément transformé la manière dont les enquêtes judiciaires et les investigations criminelles sont menées. L’investigation numérique, encore appelée *forensic informatique*, s’impose aujourd’hui comme un pilier essentiel de la sécurité numérique, du droit et de la justice.
Elle consiste à collecter, analyser et présenter des preuves électroniques dans un cadre légal rigoureux. Cette discipline joue un rôle croissant dans la lutte contre la criminalité moderne, en offrant aux enquêteurs des outils techniques permettant de retracer les activités criminelles à travers les supports numériques.

Le présent document propose une synthèse structurée des neuf thèmes étudiés dans le cadre du module *Introduction aux techniques d’investigation numérique*. Chaque thème illustre une dimension spécifique de ce domaine : de l’importance de la preuve électronique à la législation, en passant par la cryptographie, les attaques informatiques, la reconnaissance faciale, ou encore le rôle de l’intelligence artificielle dans la recherche d’indices numériques.
L’objectif est de présenter une vision globale, cohérente et intégrée de l’investigation numérique dans un contexte africain et mondial.

1. L’utilité de l’investigation numérique dans la police judiciaire

L’investigation numérique occupe une place centrale dans les enquêtes policières contemporaines. Elle permet d’obtenir et d’exploiter des preuves issues d’appareils électroniques : ordinateurs, téléphones, serveurs, réseaux, caméras, etc. Ces éléments, souvent invisibles à l’œil nu, peuvent révéler des informations cruciales telles que les communications, les localisations, les fichiers supprimés ou les activités sur les réseaux sociaux.

Dans la police judiciaire, ces preuves numériques aident à reconstituer la chronologie d’un crime, à identifier les suspects et à confirmer ou réfuter des témoignages. Au Cameroun, l’investigation numérique est utilisée pour lutter contre la cybercriminalité, les crimes financiers, le terrorisme, ou encore la diffusion de contenus illicites.
Cependant, plusieurs défis persistent : le manque de formation spécialisée, la rareté des équipements adaptés et les contraintes juridiques liées à la protection de la vie privée. Le développement d’un cadre légal solide et de compétences locales demeure donc une priorité.

2. Le protocole ZK-NR et la non-répudiation numérique

Dans le domaine du droit numérique, la notion de **non-répudiation** est fondamentale : elle garantit qu'un auteur ne puisse nier avoir émis une information ou signé un document électronique. Pour assurer cette fiabilité, plusieurs outils sont utilisés : la signature numérique, l'horodatage, la fonction de hachage et le certificat électronique.

Le protocole **ZK-NR (Zero-Knowledge Non-Repudiation)** repose sur des preuves à divulgation nulle de connaissance (*zero-knowledge proofs*) permettant de vérifier l'authenticité d'une action sans révéler le secret qui y est lié. Ce protocole constitue une avancée majeure pour la sécurité des transactions numériques, car il renforce la confidentialité tout en garantissant l'intégrité et l'irrévocabilité des preuves.
Son adoption dans les systèmes de communication judiciaire, bancaire ou contractuelle représente une étape importante vers une gouvernance numérique fiable et opposable juridiquement.

3. Les dix cas africains majeurs d'hacking (2015–2025)

Au cours de la dernière décennie, l'Afrique a été le théâtre de multiples attaques informatiques d'envergure. Parmi les plus marquantes figurent :

- L'attaque par ransomware contre **Transnet** en Afrique du Sud (2021), paralysant le transport maritime ;

- Le piratage de la **CNSS** au Maroc (2025) ;
- L'attaque contre **ENEO** au Cameroun (2024) ;
- Le scandale **Pegasus** (Maroc) lié à la surveillance illégale ;
- Les cyberattaques contre des institutions bancaires en Côte d'Ivoire et au Nigeria.

Ces incidents révèlent la fragilité des infrastructures numériques africaines et la dépendance envers les technologies étrangères.
Les pertes financières, la fuite de données sensibles et la désorganisation des services publics soulignent l'urgence de renforcer la cybersécurité continentale.
Les solutions incluent la création de **centres nationaux de réponse aux incidents (CERT)**, la **formation d'experts locaux**, et l'**harmonisation des lois** sur la cybercriminalité.
La coopération interafricaine reste une clé pour bâtir une résilience numérique durable.

4. Les logiciels de rédaction de mémoire

Bien qu'apparemment éloigné de la criminalistique numérique, ce thème met en lumière l'importance des outils de production scientifique dans la formation des ingénieurs et chercheurs. Trois logiciels essentiels sont présentés :

- **Microsoft Word**, pour sa facilité d'utilisation et sa compatibilité universelle ;
- **Overleaf (LaTeX)**, qui garantit une mise en page scientifique rigoureuse et professionnelle, très prisée dans les milieux techniques ;
- **Zotero**, un gestionnaire de références bibliographiques libre et collaboratif.

L’usage combiné de ces outils permet d’améliorer la qualité rédactionnelle, la rigueur scientifique et la traçabilité des sources.
Dans le contexte académique, ces logiciels préparent également les étudiants aux exigences de documentation et d’intégrité scientifique, essentielles dans toute démarche d’investigation numérique.

5. Les algorithmes de reconnaissance faciale

La reconnaissance faciale est une application concrète de l’intelligence artificielle dans la sécurité. Elle repose sur des algorithmes capables d’analyser les traits du visage pour identifier ou authentifier une personne. Les méthodes utilisées vont des approches statistiques classiques (PCA, LDA, SVM) aux réseaux neuronaux profonds (Deep Learning).

Ces technologies sont déployées dans les aéroports, les systèmes de vidéosurveillance, ou encore les applications de téléphonie mobile.
Cependant, leur efficacité soulève des préoccupations éthiques : intrusion dans la vie privée, biais raciaux, erreurs d’identification, ou surveillance abusive.
Les autorités doivent encadrer l’usage de ces outils pour concilier sécurité et respect des libertés fondamentales. En Afrique, un cadre réglementaire solide reste à construire pour éviter les dérives et garantir la confiance du public.

6. Intelligence artificielle et investigation numérique

L’intelligence artificielle transforme profondément le domaine de l’investigation numérique. Grâce à l’apprentissage automatique, l’IA permet d’analyser des masses de données, de détecter des schémas suspects et d’anticiper les comportements criminels.
Des logiciels d’IA peuvent, par exemple, reconnaître des fichiers altérés, classer des preuves ou générer des rapports automatisés.

Cependant, cette automatisation pose un dilemme : si elle accroît l’efficacité, elle réduit parfois la transparence des processus décisionnels.
La responsabilité juridique en cas d’erreur algorithmique reste une question ouverte.
Pour cette raison, l’usage de l’IA dans les enquêtes doit rester sous supervision humaine, avec des systèmes explicables, contrôlables et éthiques.

7. La téléphonie mobile dans les enquêtes

Les téléphones portables constituent aujourd’hui une source majeure de preuves numériques.
Chaque appareil renferme un écosystème complet : communications, données GPS, messageries, réseaux sociaux, fichiers multimédias, etc.
L’analyse forensique des téléphones permet de retracer les déplacements, les relations et les intentions d’un suspect.

Des logiciels spécialisés permettent d’extraire les données, même supprimées, et de les présenter comme éléments de

preuve.
Cependant, cette extraction doit respecter la législation sur la vie privée et les règles de procédure pénale.
L'usage abusif de ces techniques sans autorisation judiciaire peut invalider une enquête.
Ainsi, la rigueur juridique et la compétence technique doivent aller de pair pour que la preuve numérique soit recevable et crédible.

8. Le Dark Web et l'investigation numérique

Le Dark Web est la zone cachée d'Internet, accessible uniquement via des navigateurs comme Tor.
S'il permet à certains de préserver leur anonymat pour des raisons légitimes, il est aussi le lieu de nombreuses activités illégales : trafic de drogues, armes, données personnelles, exploitation sexuelle, blanchiment d'argent.

Les enquêteurs numériques s'y infiltrent pour identifier des réseaux criminels.
Ils utilisent des techniques d'analyse d'adresses Bitcoin, de surveillance de forums et de recoupement de données.
Ces opérations nécessitent des outils de pointe et une coordination internationale, car les auteurs agissent souvent au-delà des frontières.
L'un des défis majeurs est d'agir efficacement tout en respectant les cadres légaux nationaux et internationaux.

9. L’importance de la législation et de la formation

La réussite des investigations numériques dépend avant tout d’un cadre légal solide et d’une formation continue des acteurs concernés.
Au Cameroun et en Afrique, les textes de référence tels que la **loi de 2010 sur la cybersécurité** et la **Convention de Malabo** définissent les règles relatives à la collecte et à l’exploitation des preuves numériques.
Cependant, l’application de ces textes demeure limitée par le manque d’expertise et d’équipements.

La formation des magistrats, policiers, ingénieurs et experts en cybersécurité est donc cruciale.
Des programmes universitaires spécialisés doivent être développés pour renforcer les capacités locales et garantir des enquêtes efficaces, conformes aux normes internationales.

Conclusion Générale

L’investigation numérique constitue aujourd’hui un **outil stratégique incontournable** pour les systèmes judiciaires modernes.
Elle repose sur une alliance entre la technologie, le droit et l’éthique.
Les neuf thèmes étudiés démontrent la richesse de ce domaine : il ne s’agit pas seulement d’une discipline technique, mais d’un champ interdisciplinaire au service de la justice et de la sécurité.

Dans le contexte africain, l’enjeu majeur reste la **souveraineté numérique** : former des experts, créer des laboratoires forensiques, moderniser les lois et encourager la coopération internationale.
L’intelligence artificielle, la cryptographie avancée et les nouvelles technologies offriront de nouvelles opportunités, à condition d’être encadrées par des principes humains et éthiques.

Ainsi, l’investigation numérique, bien maîtrisée, représente non seulement une **arme contre la criminalité moderne**, mais aussi un **symbole de progrès scientifique et de responsabilité sociale** pour les générations futures.