ÉCOLE NATIONALE SUPERIEURE
POLYTECHNIQUE DE YAOUNDÉ

DEPARTEMENT DE GENIE INFORMATIQUE

INTRODUCTION AUX TECHNIQUES
D'INVESTIGATION NUMERIQUE

RESUME DU LIVRE D'INVESTIGATION NUMERIQUE

MAKEU TENKU STELY BELVA
CIN-4

Superviseur : M. THIERRY MINKA

2025-2026

INTRODUCTION

Le cours d'***investigation numérique*** réalisé par M. Thierry MINKA pour les étudiants de cybersécurité et d'investigation numérique présente les aspects du métier d'investigateur numérique à l'ère post-quantique et de l'intelligence artificielle (IA).
Ce résumé a pour objectif de synthétiser les principaux points abordés dans le cours, en présentant les différents chapitres et les idées clés développées par l'auteur. Il permettra au lecteur de comprendre rapidement les notions essentielles et les applications pratiques de l'investigation numérique moderne.

1 PRÉSENTATION DE L'ÉTHIQUE ET DU CADRE DÉONTOLOGIQUE

L'investigation numérique repose sur plusieurs principes éthiques et déontologiques qui permettent de faire de ce métier un noble métier. Parmi ceux-ci, nous avons les piliers éthiques tels que : « Proportionalité : adéquation des moyens aux fins, minimisation de l'intrusion, respect de la vie privée. », « Responsabilité : acceptation des conséquences de ses actions, devoir de vigilance, obligation de formation. ».
En ce qui concerne le cadre éthique, nous avons **les dix commandements de l'investigator** qui sont, entre autres :

1. Tu ne causeras pas de dommage aux systèmes que tu investigues.
2. Tu respecteras la vie privée et la dignité des personnes.
3. Tu maintiendras la chaîne de custody sans faille.
4. Tu documenteras intégralement tes processus et décisions.
5. Tu reconnaîtras les limites de tes compétences et connaissances.
6. Tu résisteras aux pressions contraires à l'éthique.
7. Tu protégeras les données sensibles dont tu as la garde.
8. Tu témoigneras avec honnêteté et objectivité.
9. Tu contribueras au développement de la discipline.
10. Tu honoreras la confiance que la société place en toi.

À ces principes et commandements s'ajoutent les sanctions et conséquences, tant sur le plan professionnel, comme la perte de crédibilité ou l'exclusion des communautés d'investigateurs, que sur le plan moral, avec la trahison de la confiance sociale et l'atteinte à l'intégrité de la discipline.

2 FONDEMENTS ET ÉVOLUTION DE L'INVESTIGATION NUMÉRIQUE

L'investigation numérique tire ses fondements de diverses sources. Nous avons des principes comme celui de Locard et les différents modèles théoriques d'investigation (DFRWS, Casey), ainsi que des normes comme l'**ISO/IEC 27037**, norme internationale pour la collecte des preuves.
En ce qui concerne l'histoire de l'investigation numérique, dès les années 1970, nous avons l'apparition des premiers crimes informatiques avec l'affaire **« The Creeper »**, puis d'autres enquêtes ont permis de poser les bases de l'investigation numérique. Dans les années 1990,l'*International Organization on Computer Evidence* fut créée, permettant de standardiser les méthodologies.
Du début des années 2000 jusqu'en 2020, diverses enquêtes ont permis l'évolution du domaine avec de nouveaux outils et techniques. De 2020 à nos jours, nous avons l'ère du post-quantique et de l'IA, encore en pleine évolution, et le défi majeur ici est « **comment va se comporter l'investigation numérique dans un contexte avec des techniques d'obfuscation avancées** ».

Période	Événements clés
1970-1990	Premiers crimes informatiques (Creeper, affaire des "414s")
1990-2000	Professionnalisation (Opération Sundevil, cas Kevin Mitnick)
2000-2010	Standardisation (Affaire Enron, création d'EnCase, RFC 3227)
2010-2020	Ère du Big Data (Silk Road, Panama Papers, WannaCry)
2020-...	Post-quantique et IA (attaque SolarWinds, défis d'obfuscation)

Table 1 – Évolution historique de l'investigation numérique

3 IMPACT DE LA RÉVOLUTION QUANTIQUE ET INTRODUCTION DU TRILEMME CRO ET DU PROTOCOLE ZK-NR

La révolution quantique représente un changement de paradigme, car elle a permis l'évolution de divers domaines comme la cryptographie, ce qui constitue un pas de géant dans le domaine de l'investigation numérique. Les protocoles *ZK-NR* pour **Zero-Knowledge Non-Répudiation** offrent une résolution du paradoxe de l'authenticité invisible. Il s'agit d'un protocole modulaire combinant quatre couches indépendantes (Merkle, STARK, BLS, Dilithium) pour préserver la vie privée avec des garanties post-quantiques.

Axe	**Signification**
Confidentialité	Protection des données sensibles et vie privée
Fiabilité	Véracité et intégrité des preuves numériques
Opposabilité	Capacité d'une preuve à être recevable juridiquement

TABLE 2 – Composantes du trilemme CRO

4 ASPECTS JURIDIQUES ET PRATIQUES OPÉRATIONNELLES DE L'INVESTIGATION NUMÉRIQUE

L'investigation numérique est régit par plusieurs juridictions tant sur le plan mondial que sur le plan Camerounais. En ce qui concerne la législation mondiale et régionale , nous avons dans le droit Américain : « Federal Rules of Evidences (FRE) »qui concerne principalement l'authentification, nous avons aussi « Stored Communications Act (SCA) »concernant la protection des communications stockées. Concernant le droit Européen, nous avons « Règlement eIDAS Régulation (EU) No 910/2014 qui concerne les signature électroniques , le « RGPD et Investigation Reglement (UE) 2016/679 ».
En Afrique, nous avons la convention de Malabo en 2014 portant sur la cybersécurité et la protection des données personnelles avec les États membres de l'UA.
Concernant le droit Camerounais , nous avons divers lois qui régissent l'investigation numérique et la cybersécurité :

1. Loi N°2010/012 du 21 décembre 2010 Relative à la cybersécurité et la cybercriminalité

2. Loi N°2010/013 du 21 décembre 2010 Régissant les communications électroniques

3. Loi N°2024/017 du 23 décembre 2024 Régissant la protection des données à caractère personnel au Cameroun

5 PRATIQUES OPÉRATIONNELLES ET CAS PRATIQUE CAMEROUNAIS

L'ouvrage met aussi en avant la dimension pratique du métier d'investigator numérique. Il ne suffit pas de connaître la théorie : il faut savoir manipuler des outils, gérer un laboratoire et rédiger des rapports conformes aux normes (ISO 27037, NIST, RFC 3227). Les SOP (Standard Operating Procedures) et la chaîne de custody sont donc essentielles.

Outils principaux : EnCase, Sleuth Kit, Volatility pour la mémoire, Wireshark pour le réseau, mais aussi des frameworks modernes intégrant l'IA.

Exemple camerounais : le cas « CyberFinance Cameroun 2025 »présenté dans le livre. Une infrastructure bancaire a été compromise par un ransomware. L'investigation a nécessité la mise en place d'une timeline forensique, l'utilisation du protocole ZK-NR pour garantir la valeur juridique des preuves, et l'application de la loi N°2024/017 sur la protection des données personnelles. Ce cas illustre l'importance de lier théorie, outils et droit dans la pratique réelle.