RÉPUBLIQUE DU CAMEROUN
*****
Paix – Travail – Patrie
*****
UNIVERSITÉ DE YAOUNDÉ I
*****
École Nationale Supérieure
Polytechnique de Yaoundé
*****
DEPARTEMENT DE GENIE INFORMATIQUE
*****

REPUBLIC OF CAMEROON
*****
Peace – Work – Fatherland
*****
UNIVERSITY OF YAOUNDÉ I
*****
National Advanced School
Engineering of Yaounde
*****
COMPUTERS ENGINEERING DEPARTMENT
*****

TRAVAIL A FAIRE N°1

Résumé du cours

Théories et Pratiques de l'Investigation Numérique

Rédigé par :

Noms & prénoms	Filière	Matricule
DSAMAGO JAFFO Tresor	**HN - CIN 4**	**22P036**

Sous la direction de :
Mr MINKA MI NGUIDJOI Thierry Emmanuel
Laboratoire LIMSI

Année académique : **2025 - 2026**

Introduction

Ce manuel représente une synthèse de deux décennies de pratique et de recherche en cybersécurité et investigation numérique. Il s'adresse aux ingénieurs et chercheurs souhaitant se spécialiser dans l'investigation numérique post-quantique, avec une attention particulière portée aux défis juridiques et techniques de l'opposabilité des preuves numériques. L'originalité de cet ouvrage réside dans l'introduction du **Trilemme CRO** (Confidentialité, Fiabilité, Opposabilité), une contribution théorique majeure qui redéfinit les limites fondamentales de la preuve numérique dans un contexte post-quantique. Ce résumé se propose de restituer l'essentiel des concepts clés, méthodologies et perspectives abordés dans ce document complet.

1 Fondements, Historique et Évolution

1.1 Philosophie et Fondements

L'investigation numérique est présentée comme une discipline philosophique à part entière, interrogeant les fondements de la vérité, de la confiance et de la justice à l'ère numérique. Elle dépasse largement le cadre technique pour embrasser des dimensions épistémologiques, éthiques et ontologiques. Le manuel introduit des concepts tels que l'**ontologie numérique**, la **phénoménologie des données** et la **métaphysique digitale**, soulignant que l'être humain se définit désormais aussi par son existence numérique.

Un apport conceptuel majeur est le **Paradoxe de l'Authenticité Invisible**, théorisé dans l'article fondateur *Exploring ZK-NR* (ePrint 2025/1138). Ce paradoxe capture la tension fondamentale entre la nécessité de prouver l'authenticité et l'intégrité des preuves numériques et l'exigence de confidentialité et de protection de la vie privée. Mathématiquement, ce paradoxe s'exprime comme une relation d'incertitude : $\Delta A \cdot \Delta C \geq h_{num}$, où ΔA représente l'incertitude sur l'authenticité, ΔC l'incertitude sur la confidentialité et h_{num} la constante numérique fondamentale.

Les fondements mathématiques et théoriques de l'investigation numérique puisent dans la théorie de l'information de Shannon (entropie), la théorie des graphes (analyse relationnelle) et la théorie du chaos (sensibilité aux conditions initiales). La révolution quantique est abordée non pas comme une simple évolution technique mais comme un changement paradigmatique complet, introduisant des concepts philosophiques radicaux comme la non-localité, l'intrication et la superposition.

1.2 Histoire et Grandes Affaires

Le manuel retrace l'histoire de l'investigation numérique depuis ses prémices (1970-1990) avec des affaires fondatrices comme celle du "414s" (1983), en passant par l'ère de la professionnalisation (1990-2000) avec l'Opération Sundevil (1990) et le cas Kevin Mitnick (1995), jusqu'à l'ère post-quantique et IA (2020-Présent) avec l'attaque SolarWinds (2020). Des affaires marquantes comme BTK Killer (2005), Stuxnet (2010) et WannaCry (2017) ont façonné la discipline, chacune apportant son lot d'innovations techniques et de leçons apprises.

2 Cadre Théorique, Normatif et Méthodologique

2.1 Cadre Théorique et Conceptuel

Le manuel présente les modèles théoriques fondamentaux de l'investigation numérique, dont le **Principe de Locard Numérique** décliné en traces primaires (logs système, artefacts de registre) et secondaires (métadonnées, corrélations réseau). Les modèles d'investigation comme le **DFRWS Framework** (2001), le modèle de Casey (2004) et les normes ISO/IEC 27037 :2012 sont détaillés.

L'état de l'art et l'évolution scientifique sont présentés sous forme de chronologie des avancées, de 1979 (première saisie de données informatiques) à 2020 (Quantum-Safe Forensics). Les paradigmes actuels incluent le **Digital Forensics as a Service (DfaaS)**, les **Proactive Forensics** et l'**IoT Forensics**.

2.2 Normes et Standards Internationaux

Un chapitre complet est consacré au cadre normatif global, incluant les standards ISO/IEC (27037, 27041, 27042, 27043), le **NIST SP 800-86**, le **RFC 3227** (BCP 55) avec son ordre de volatilité de Farmer & Venema, et l'**ACPO Good Practice Guide** avec ses quatre principes fondamentaux. Les standards émergents pour le Cloud Forensics et l'IoT Forensics sont également abordés.

2.3 Méthodologies et Outils

Le manuel compare les méthodologies d'investigation du **SANS Institute** (FOR508), du **CERT/CC**, de l'**ENISA** et du **Digital Forensics Research Center Korea**. L'arsenal de l'investigateur moderne est détaillé, couvrant l'acquisition et l'imagerie, l'analyse de mémoire avancée avec Volatility 3, les techniques d'anti-anti-forensique, et l'intelligence artificielle en investigation (machine learning pour la classification de malware, deep learning pour l'analyse comportementale).

Des scripts pratiques sont fournis, comme un script d'acquisition avec validation, un plugin Volatility 3 custom pour la détection de processus suspects, et des modèles de machine learning pour la classification de malware et l'analyse comportementale.

3 L'Ère Post-Quantique et le Trilemme CRO

3.1 Impact du Quantique sur l'Investigation

La révolution quantique menace les fondements cryptographiques actuels. L'**algorithme de Shor** peut factoriser de grands nombres en temps polynomial, menaçant RSA, ECC et DSA/ECDSA. L'**algorithme de Grover** offre une accélération quadratique pour la recherche, réduisant la sécurité effective des clés symétriques (AES-128 → sécurité 64-bit).

La stratégie "**Harvest Now, Decrypt Later**" pose un défi majeur : les adversaires stockent des communications chiffrées aujourd'hui en attendant de pouvoir les décrypter avec des ordinateurs quantiques futurs. Cela impacte directement la **chain of custody** et l'intégrité long-terme des preuves.

Les contre-mesures incluent la migration vers la **cryptographie post-quantique (PQC)**. Les standards NIST Round 4 sont présentés : **CRYSTALS-Kyber** (KEM), **CRYSTALS-Dilithium** (signatures), **FALCON** et **SPHINCS+**. Le manuel discute

également des nouvelles opportunités offertes par le **Quantum Forensics**, comme l'analyse de randomité quantique (QRNG vs PRNG) et la tomographie d'état quantique pour les preuves.

3.2 Le Trilemme CRO et son Formalisme

Le **Trilemme CRO** (Confidentialité, Fiabilité, Opposabilité) est une contribution théorique majeure de l'auteur. Il établit une incompatibilité formelle entre l'optimisation simultanée des trois axes : - **Confidentialité** : Protection des données sensibles - **Fiabilité** (Reliability) : Intégrité et authenticité - **Opposabilité juridique** : Valeur probante légale

Mathématiquement, le trilemme est formalisé comme : où $C(\Pi)$, $R(\Pi)$ et $O(\Pi)$ sont les indices de confidentialité, fiabilité et opposabilité, et λ le paramètre de sécurité.

3.3 Architecture Q2CSI et Protocole ZK-NR

Pour répondre au trilemme CRO, l'auteur propose l'**architecture Q2CSI** (Quantum Composable Contextual Security Infrastructure) qui sépare dialectiquement les préoccupations en trois couches : - **Iron Layer** (Fiabilité) : Intégrité temporelle et logging - **Gold Layer** (Confidentialité) : Préservation de l'entropie sémantique - **Clay Layer** (Opposabilité) : Ancrage institutionnel

Le **protocole ZK-NR** (Zero-Knowledge Non-Repudiation) est une implémentation pratique combinant **Merkle Commitments**, **STARK Proofs** (zero-knowledge post-quantique), **Threshold BLS** (signatures distribuées) et **Dilithium** (authentification post-quantique). Il permet de créer des attestations légalement opposables tout en préservant la confidentialité grâce aux preuves zero-knowledge.

4 Analyse Cryptographique et Cadre Juridique

4.1 Analyse des Primitives selon le Trilemme CRO

Le manuel applique méthodiquement le cadre CRO aux principales primitives cryptographiques, révélant les compromis inhérents. Chaque primitive est évaluée selon trois indices normalisés entre 0 et 1, avec des considérations de résistance quantique, de maturité et de complexité.

Analyse comparative (scores arrondis) :

- **AES-256** : C=0.95, R=0.90, O=0.30 (Score CRO=0.95)
- **RSA-2048** : C=0.85, R=0.90, O=0.95 (Score CRO=0.95)
- **ECDSA** : C=0.88, R=0.92, O=0.90 (Score CRO=0.92)
- **Kyber-768** : C=0.92, R=0.85, O=0.40 (Score CRO=0.92)
- **Dilithium-3** : C=0.20, R=0.94, O=0.75 (Score CRO=0.94)
- **zk-SNARKs** : C=0.98, R=0.75, O=0.40 (Score CRO=0.98)
- **zk-STARKs** : C=0.85, R=0.90, O=0.60 (Score CRO=0.90)

Cette analyse démontre qu'aucune primitive n'optimise simultanément C, R et O, justifiant le besoin d'architectures hybrides combinant primitives classiques (pour l'opposabilité immédiate) et post-quantiques (pour la confidentialité future).

4.2 Cadre Juridique Mondial et Africain

Le manuel couvre le cadre juridique mondial avec le droit américain (Federal Rules of Evidence, Stored Communications Act, Computer Fraud and Abuse Act), le droit européen (règlement eIDAS, RGPD, Convention de Budapest) et le droit africain (Convention de Malabo de 2014, cadres régionaux de la CEDEAO, SADC et EAC).

Le droit camerounais est particulièrement détaillé, avec les lois N°2010/012 (cybersécurité et cybercriminalité), N°2010/013 (communications électroniques) et N°2024/017 (protection des données). La procédure d'investigation au Cameroun, le statut d'expert agréé, et la jurisprudence camerounaise (affaires CAMTEL c. X, Ministère Public c. Y) sont présentés.

5 Pratique Forensique et Études de Cas

5.1 Pratiques Opérationnelles

Le manuel fournit un guide complet pour la mise en place et la gestion d'un laboratoire forensique, incluant l'installation et configuration des environnements SIFT/Remnux/SANS VM, l'intégration d'outils open source et commerciaux, les procédures opérationnelles standards (SOP), les checklists d'intervention, les modèles de rapports, et les scripts d'automatisation.

La gestion de laboratoire couvre l'infrastructure technique, la chaîne de custody physique, la certification et accréditation, ainsi que la formation pratique continue (veille technologique, threat intelligence, red team exercises).

5.2 Forensique Système et Réseau Avancée

Des chapitres techniques détaillent la forensique système avancée (analyse NTFS/EXT4/APFS, artefacts Windows/Linux/macOS, memory forensics avec Volatility 3, timeline analysis) et la forensique réseau opérationnelle (capture et analyse PCAP, analyse de protocoles chiffrés, log analysis et SIEM, threat hunting, attribution technique d'attaques).

L'approche intègre constamment les concepts post-quantiques et le framework CRO, avec des scripts et méthodologies pour la détection de cryptographie quantique, l'analyse comportementale avec IA, et la reconstruction temporelle multi-sources avec validation CRO.

5.3 Études de Cas Internationales

Le manuel présente une analyse comparative d'études de cas internationaux illustrant la diversité des approches forensiques selon les contextes géopolitiques, juridiques et culturels :

- **États-Unis** : Cyber-espionnage industriel dans la Silicon Valley
- **Europe** : Attaque d'infrastructure critique avec coordination transnationale
- **Inde** : Manipulation d'élections par IA et deepfakes
- **Moyen-Orient** : Cyberterrorisme multi-plateforme sous contraintes géopolitiques
- **Afrique de l'Ouest** : Fraude bancaire mobile money transfrontalière
- **Australie** : Criminalité environnementale digitale avec falsification de données

— **Amérique Latine** : Narcotrafic numérique avec cryptomonnaies et communications chiffrées

Chaque cas est analysé selon le framework CRO, révélant des patterns d'excellence différents selon les régions : innovation et rigueur légale aux États-Unis, coopération transnationale en Europe, adaptation contextuelle et innovation en Afrique, etc.

Conclusion

Ce manuel représente une contribution majeure à la discipline de l'investigation numérique, proposant une vision unifiée intégrant les dimensions techniques, juridiques, éthiques et philosophiques. L'introduction du Trilemme CRO et du protocole ZK-NR offre un cadre conceptuel puissant pour aborder les défis de l'ère post-quantique, en particulier la tension fondamentale entre confidentialité, fiabilité et opposabilité juridique.

La richesse des études de cas internationales démontre que l'excellence forensique émerge de la capacité à adapter les méthodologies aux contextes locaux tout en maintenant des standards internationaux. L'approche modulaire de l'architecture Q2CSI et la combinaison judicieuse de primitives cryptographiques classiques et post-quantiques offrent une voie praticable pour la transition vers une investigation numérique résiliente aux menaces quantiques.

L'investigation numérique est ainsi présentée non pas comme une simple technique, mais comme une voie philosophique et éthique nécessitant autant de sagesse que de compétence, où chaque décision technique a des implications humaines, légales et sociétales profondes. Le manuel se positionne comme un guide essentiel pour les investigateurs devant naviguer cette complexité croissante tout en préservant les valeurs fondamentales de justice, de vérité et de protection des droits.