RÉPUBLIQUE DU CAMEROUN
Paix-Travail-Patrie

UNIVERSITÉ DE YAOUNDÉ I

ÉCOLE NATIONALE SUPÉRIEURE POLYTECHNIQUE DE YAOUNDÉ

DÉPARTEMENT DE GÉNIE INFORMATIQUE

REPUBLIC OF CAMEROON
Peace-Work-Fatherland

UNIVERSITY OF YAOUNDÉ I

NATIONAL ADVANCED SCHOOL OF ENGINEERING OF YAOUNDÉ

DEPARTMENT OF COMPUTER ENGINEERING

INTRODUCTION AU TECHNIQUE D'INVESTIGATION NUMERIQUE

RÉSUME DU CHAPITRE D'INTRODUCTION : THEORIES ET PRATIQUES DE L'INVESTIGATION NUMERIQUE

DEVOIR

NOMS ET PRÉNOMS	MATRICULES	SPÉCIALITÉS
AYONNEME TIOBOU Varese	22P045	HN-4 CIN

EXAMINATRICE : Mr MINKA Thierry

Année Académique : 2025/2026

Introduction

Le manuel « Théories et Pratiques de l'Investigation Numérique » constitue un ouvrage académique de référence pour les étudiants, chercheurs et professionnels de la cybersécurité. Il présente de manière approfondie les bases théoriques, les évolutions historiques, les méthodes pratiques, les cadres juridiques et les défis éthiques liés à l'investigation numérique dans un monde en pleine mutation. L'originalité de l'ouvrage réside dans l'introduction du **trilemme CRO** (Confidentialité, Fiabilité, Opposabilité juridique), un modèle conceptuel innovant qui redéfinit la preuve numérique dans un contexte post-quantique. Ce résumé propose une synthèse structurée et détaillée en huit volets principaux.

1. Fondements et Historique de l'Investigation Numérique

L'investigation numérique est née dans les années 1970, au moment où l'informatiq commençait à pénétrer les entreprises et les institutions. La première saisie de données informatiques (1979) a ouvert la voie à une discipline encore embryonnaire. Les années 1980-1990 marquent l'apparition des premiers cas emblématiques, tels que l'affaire des « 414s » ou celle de Kevin Mitnick, mettant en évidence la nécessité de méthodes d'enquête spécialisées.

La décennie 2000 voit la professionnalisation et la standardisation des pratiques, notamment avec l'affaire Enron (2001) qui impose la conservation massive de preuves numériques. Le développement d'outils comme EnCase ou Sleuth Kit participe à la structuration de la discipline. Enfin, les années 2010-2020 sont marquées par l'ère du Big Data, du Cloud et des cyberattaques globales (Stuxnet, WannaCry, Panama Papers). Aujourd'hui, l'investigation numérique entre dans une ère post-quantique, où l'IA et l'informatique quantique bouleversent les paradigmes existants.

2. Cadre Théorique et Conceptuel

Le manuel explore en profondeur l'épistémologie de la preuve numérique. La trace numérique est envisagée comme un phénomène existentiel, produit inévitable de toute interaction avec un système informatique.

L'approche mobilise la théorie de l'information (entropie, redondance), la théorie des graphes (analyse de réseaux, relations entre entités) et la théorie du chaos (sensibilité aux conditions initiales).

Un point central est l'introduction du **trilemme CRO** qui met en évidence l'impossibilité de concilier simultanément, et de manière optimale, la confidentialité, la fiabilité et l'opposabilité juridique des preuves numériques. Cette tension structurelle oblige les investigateurs à rechercher des compromis pragmatiques selon le contexte de chaque affaire.

3. Normes et Standards Internationaux

L'investigation numérique est encadrée par un ensemble de normes internationales visant à garantir la validité juridique et scientifique des preuves collectées.

- L'**ISO/IEC 27037** définit les principes de base de l'identification, de la collecte et de la conservation des données.
- L'**ISO/IEC 27041** et **27042** détaillent respectivement les méthodes validées et les cadres d'analyse.
- L'**ISO/IEC 27043** propose un modèle global de processus d'investigation.
- Aux États-Unis, le **NIST SP 800-86** fournit un cadre pratique reconnu.
- Le **RFC 3227** établit un ordre de volatilité des données, essentiel pour la priorisation lors de la collecte.
- En Europe, l'**ACPO Guide** fixe des principes fondamentaux de proportionnalité et d'intégrité.

Le manuel met également en lumière l'adaptation locale de ces normes dans le contexte africain, notamment au Cameroun, avec la Convention de Malabo (2014) et les lois nationales sur la cybersécurité (2010/012, 2010/013 et 2024/017).

4. Méthodologies et Meilleures Pratiques

L'ouvrage compare diverses méthodologies issues de grandes institutions :

- La méthodologie du **SANS Institute (FOR508)**
- Celle du **CERT/CC** pour la réponse aux incidents
- Le cadre européen proposé par l'**ENISA**

- Des approches asiatiques (Corée, Japon)

Ces méthodes sont appliquées à l'investigation de systèmes, de réseaux et de données dans des environnements complexes. Le manuel insiste sur l'importance de la documentation, de la traçabilité (*chain of custody*) et du respect de l'éthique professionnelle.

Il détaille également l'utilisation d'outils forensiques tels que :

- **Volatility** pour l'analyse mémoire
- **DFIR Tools** pour la reconstruction temporelle
- Les **SIEM** pour la corrélation de logs

L'intégration de l'intelligence artificielle permet désormais la classification automatisée de malwares et l'analyse comportementale avancée via des modèles de *machine learning* et *deep learning*.

5. L'Ère Post-Quantique et la Cryptographie

Le développement de l'informatique quantique représente une menace sérieuse pour les algorithmes de cryptographie classique.

- L'algorithme de **Shor** compromet les systèmes RSA et ECC.
- L'algorithme de **Grover** accélère la recherche dans les systèmes symétriques.

Le manuel présente les solutions de cryptographie post-quantique, notamment :

- **CRYSTALS-Kyber** (échange de clés)
- **CRYSTALS-Dilithium** (signatures)

Il introduit également le protocole **ZK-NR** (Zero Knowledge – Non-Repudiation) qui permet d'assurer une preuve vérifiable sans divulguer d'informations sensibles. Ces avancées s'inscrivent dans le cadre de l'architecture **Q2CSI** et du trilemme **CRO**, qui deviennent des outils conceptuels et pratiques incontournables pour l'investigateur de demain.

6. Cadre Juridique et Enjeux Éthiques

Le droit joue un rôle central dans l'investigation numérique.

- Aux **États-Unis**, les **Federal Rules of Evidence (FRE)** encadrent la recevabilité des preuves, tandis que le **CFAA** réprime la fraude informatique.
- En **Europe**, le **RGPD** impose des contraintes strictes sur la collecte et l'utilisation de données.
- En **Afrique**, la **Convention de Malabo** constitue le texte de référence.
- Au **Cameroun**, les lois nationales (2010/012, 2010/013, 2024/017) encadrent la cybercriminalité et la protection des données personnelles.

Cependant, des défis persistent en matière de formation des experts agréés et de sensibilisation des magistrats. L'auteur insiste sur le **contrat déontologique** de l'investigateur numérique, fondé sur les principes d'intégrité, de proportionnalité, de responsabilité et de service.

7. Pratique Opérationnelle et Laboratoires Forensiques

Le manuel fournit un guide concret pour la mise en place d'un laboratoire forensique.

- **Environnements techniques** : SIFT, Remnux, VMware, Hyper-V.
- **Procédures opérationnelles standard** : checklists, modèles de rapports, scripts d'automatisation.
- **Mécanismes** : Certification, accréditation, formation continue, veille technologique.
- **Pratiques avancées** : Threat intelligence, exercices de red teaming.

Des sections spécifiques traitent de la forensique système (NTFS, EXT4, APFS), de la forensique mémoire (Volatility 3), et de la forensique réseau (analyse PCAP, SIEM, détection d'intrusions).

8. Étude de Cas : CyberFinance Cameroun 2025

L'ouvrage se conclut par un cas pratique intégrateur illustrant une attaque de type *ransomware* visant une institution financière camerounaise. Les phases

de l'enquête sont détaillées :

- Détection et réponse initiale
- Collecte de preuves selon ISO 27037
- Analyse technique post-quantique
- Attribution de l'attaque
- Remédiation et renforcement
- Aspects juridiques et préparation du dossier pour le tribunal

L'étude met en évidence les défis du contexte africain (ressources limitées, cadre légal en évolution) et les opportunités offertes par l'adoption des meilleures pratiques mondiales et des outils post-quantiques. Ce cas sert de synthèse et de mise en pratique des concepts étudiés.

Conclusion Générale

Le manuel offre une vision globale et intégrée de l'investigation numérique, où se croisent philosophie, science, technique et droit. Il propose une réflexion sur la **responsabilité éthique** de l'investigateur numérique et sur la nécessité d'adapter les pratiques à l'ère post-quantique. Il constitue un outil indispensable pour former des experts capables de relever les défis technologiques, juridiques et humains de la cybersécurité moderne. Ce résumé met en évidence la richesse de l'ouvrage et son rôle de guide académique et pratique dans un domaine en constante évolution.