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 Engineering of Yaounde
*****
Computers Engineering Department
*****

INTRODUCTION AUX TECHNIQUES D'INVESTIGATION NUMERIQUE

TRAVAIL A FAIRE : RESUMER « THEORIES ET PRATIQUES DE L'INVESTIGATION NUMERIQUE »

NOMS & PRENOMS	FILIERE	MATRICULE
WANSI GILLES GILDAS	**HN-CIN-M1**	**22P037**

Sous la supervision de Ing THIERRY MINKA

Année Académique 2024/2025

Introduction générale

Le manuel « Théories et Pratiques de l'Investigation Numérique » de MINKA MI NGUIDJOI Thierry Emmanuel est une œuvre dense qui ambitionne de structurer, théoriser et opérationnaliser la pratique de l'investigation numérique à l'ère du post-quantique. Son objectif est double : offrir une assise académique solide aux étudiants et chercheurs, et proposer aux praticiens des outils méthodologiques, techniques et juridiques directement exploitables. L'auteur, fort de plus de vingt années d'expérience, met en avant l'originalité de son approche : le Trilemme CRO (Confidentialité, Fiabilité, Opposabilité), cadre conceptuel innovant permettant de dépasser les débats traditionnels sur la valeur de la preuve numérique. Dès l'introduction, l'éthique est placée au centre de la démarche. Le « Contrat Déontologique de l'Investigator Numérique », inspiré du serment d'Hippocrate, engage chaque futur professionnel à agir avec intégrité, responsabilité et sens du service public, tout en respectant la proportionnalité dans ses interventions.

Partie I – Fondements philosophiques, historiques et théoriques

L'investigation numérique est d'abord analysée comme une discipline philosophique. Elle questionne la nature de la vérité dans un monde où l'humain est doté d'un « double numérique ». La preuve n'est plus seulement matérielle, mais devient immatérielle et volatile, reposant sur des chaînes techniques d'authentification. L'épistémologie de la preuve numérique s'appuie sur des concepts scientifiques : la théorie de l'information pour mesurer l'incertitude, la théorie des graphes pour modéliser les relations entre acteurs et événements, et la théorie du chaos pour illustrer la fragilité des systèmes numériques aux conditions initiales. Le manuel pré-

sente également le paradoxe de l'authenticité invisible : plus une preuve est vérifiable, plus elle révèle d'informations compromettant sa confidentialité. La solution envisagée repose sur les protocoles Zero-Knowledge, et plus particulièrement le ZK-NR.

Sur le plan historique, l'auteur retrace l'évolution de l'investigation numérique en trois grandes phases : les débuts (1970-1990), marqués par des enquêtes rudimentaires ; l'essor des cyberattaques globalisées (2000-2020), avec des affaires emblématiques comme Stuxnet ou WannaCry ; et l'ère post-quantique actuelle, où la cryptographie classique est remise en cause. Ces jalons historiques montrent comment la discipline s'est professionnalisée et structurée autour de normes internationales.

Partie II – Cadres théoriques et normatifs

L'adaptation du principe de Locard au monde numérique est l'un des apports majeurs de l'ouvrage. Chaque action numérique laisse une trace exploitable : logs, artefacts, métadonnées, corrélations croisées. L'auteur insiste sur la nécessité de distinguer les traces primaires, directement produites par un système, et les traces secondaires, issues d'analyses ou de transformations.

Les modèles d'investigation sont présentés de façon comparée : le modèle DFRWS (basé sur la collecte et l'analyse structurée), le modèle de Casey (axé sur la reconstruction des événements), et les normes ISO/IEC 27037 à 27043 qui encadrent identification, collecte, préservation et présentation des preuves numériques.

Le manuel passe ensuite en revue les grandes normes internationales : ISO/IEC 27037, NIST SP 800-86, RFC 3227 (qui insiste sur l'ordre de volatilité), et le guide ACPO, référence britannique qui repose sur quatre principes directeurs de préservation de la preuve. Une analyse comparative mondiale illustre comment le Trilemme CRO permet de situer chaque approche nationale dans un cadre

critique.

Partie III – Méthodologies et outils pratiques

Les méthodologies décrites couvrent plusieurs continents : - le SANS Institute (FOR508) avec ses six phases de réponse aux incidents ; - le CERT/CC avec un processus en quatre étapes ; - l'ENISA, qui propose un modèle européen en trois phases. Ces méthodologies convergent vers l'idée que l'investigation doit être structurée, reproductible et documentée.

Les outils pratiques incluent des scripts d'acquisition avec validation par hachage, des logiciels spécialisés dans l'imagerie mémoire et disque, des techniques anti-anti-forensiques permettant de contourner le chiffrement ou la stéganographie, et des applications d'intelligence artificielle pour classer et analyser les malwares. Des exemples de code Python basés sur des réseaux de neurones LSTM illustrent l'utilisation de l'IA en pratique.

Partie IV – L'ère post-quantique et le Trilemme CRO

L'auteur identifie la révolution quantique comme un tournant critique. Les algorithmes de Shor et Grover menacent l'ensemble des schémas cryptographiques actuels. La stratégie « Harvest Now, Decrypt Later » met en lumière un risque immédiat : les données sensibles chiffrées aujourd'hui pourraient être compromises demain.

Face à cette menace, la cryptographie post-quantique (Kyber, Dilithium, Falcon, etc.) devient incontournable. Le manuel montre comment ces algorithmes cherchent à maintenir un équilibre entre sécurité, efficacité et opposabilité juridique.

L'application du Trilemme CRO aux primitives cryptographiques illustre qu'aucune solution n'atteint la perfection : les schémas symétriques sont solides en confidentialité mais faibles en opposa-

bilité, les schémas asymétriques sont fiables mais menacés par le quantique, et les solutions post-quantiques manquent encore de recul juridique.

Le protocole ZK-NR, conçu par l'auteur, constitue une tentative de résolution : il associe engagements Merkle, preuves STARK et signatures distribuées BLS et Dilithium. Ce protocole vise à garantir une preuve confidentielle, vérifiable et juridiquement opposable à l'ère post-quantique.

Partie V – Cryptanalyse et cadre juridique

La cryptanalyse est abordée à travers une démarche structurée en cinq étapes : compréhension du protocole, modélisation théorique, analyse manuelle, analyse automatisée via l'outil Tamarin, et tests d'implémentation. Cette approche permet de détecter les vulnérabilités cachées et de renforcer la sécurité des systèmes.

Le cadre juridique est traité de manière exhaustive. L'auteur analyse les législations américaine (FRE, CFAA), européenne (RGPD, eIDAS, Convention de Budapest), africaine (Convention de Malabo) et camerounaise (lois de 2010 et 2024). Il souligne les tensions permanentes entre l'efficacité de l'investigation et la protection des droits fondamentaux, notamment la vie privée.

Partie VI – Pratiques opérationnelles et cas pratique

La dimension pratique du manuel se matérialise par des chapitres sur la gestion d'un laboratoire forensique, les procédures opérationnelles standardisées (SOP), la certification et l'accréditation. L'analyse des artefacts couvre plusieurs systèmes d'exploitation (Windows, Linux, macOS) ainsi que la mémoire vive, étudiée grâce à Volatility 3.

La forensique réseau inclut l'analyse des fichiers PCAP, la détection des protocoles cachés, le Deep Packet Inspection (DPI) et l'attribution d'attaques complexes. Des contre-mesures face à l'anti-forensique sont également proposées, renforçant la capacité de l'investigateur à préserver l'intégrité des preuves.

Un cas pratique conclut l'ouvrage : une enquête sur un ransomware déployé au Cameroun en 2025. Ce scénario mobilise l'ensemble des concepts, outils et cadres normatifs étudiés, de la collecte des preuves jusqu'à leur présentation devant une autorité judiciaire.

Conclusion générale

Le manuel se distingue par son ambition de relier éthique, technique et droit dans une approche cohérente et globale. Il propose une vision internationale adaptée aux réalités locales, et met en lumière l'importance d'une discipline rigoureuse face aux bouleversements technologiques à venir. Le Trilemme CRO et le protocole ZK-NR sont appelés à devenir des cadres de référence pour l'investigation numérique post-quantique.