RÉPUBLIQUE DU CAMEROUN
****
Paix - Travail - Patrie
****
UNIVERSITÉ DE YAOUNDÉ I
****
ECOLE NATIONALE SUPERIEURE POLYTECHNIQUE DE YAOUNDE
****
DÉPARTEMENT DE GENIE INFORMATIQUE
****

REPUBLIC OF CAMEROON
****
Peace - Work - Fatherland
****
UNIVERSITY OF YAOUNDE I
****
NATIONAL ADVANCED SCHOOL OF ENGINEERING OF YAOUNDE
****
DEPARTMENT OF COMPUTER ENGINEERING
****

RESUME DU LIVRE

Théories et Pratiques de l'Investigation Numérique

Option :

Cybersécurité et Investigation Numérique

Rédigé par :
KALDADAK ADAMA, *24P824*

Sous l'encadrement de :
Expert Thierry MINKA

Année académique 2025 / 2026

L'originalité de cet ouvrage réside dans l'introduction du Trilemme **CRO (Confidentialité, Fiabilité, Opposabilité juridique**), une contribution théorique majeure qui redéfinit les limites fondamentales de la preuve numérique dans un contexte post-quantique.

Fondements, Historique et Évolution

Cette partie établit les bases théoriques de l'investigation numérique, en adaptant le principe de Locard au monde digital : *toute interaction laisse une trace, primaire ou secondaire*. Différents modèles et normes, tels que **DFRWS (2001)**, **Casey (2004)** et **ISO/IEC 27037 :2012**, fournissent une méthodologie structurée pour collecter et analyser les preuves numériques. **La théorie de l'information** (entropie, distance de Hamming) et **la théorie des graphes** sont mobilisées pour détecter anomalies et analyser réseaux et flux de données.

Un état de l'art retrace les grandes avancées, depuis la première saisie informatique (1979) jusqu'aux memory forensics, cloud forensics et forensique post-quantique, en passant par les outils spécialisés comme EnCase ou The Sleuth Kit. Aujourd'hui, l'investigation numérique tend à devenir proactive et externalisée ("DFaaS"), intégrant l'IoT Forensics et les évolutions technologiques, confirmant qu'il s'agit d'une discipline vivante et en constante transformation.

Cadre Théorique et Conceptuel

Cette partie établit les bases théoriques de l'investigation numérique, en adaptant le principe de Locard au monde digital : toute interaction laisse une trace, primaire ou secondaire. Différents modèles et normes, tels que DFRWS (2001), Casey (2004) et ISO/IEC 27037 :2012, fournissent une méthodologie structurée pour collecter et analyser les preuves numériques. La théorie de l'information (entropie, distance de Hamming) et la théorie des graphes sont mobilisées pour détecter anomalies et analyser réseaux et flux de données.

Un état de l'art retrace les grandes avancées, depuis la première saisie informatique (1979) jusqu'aux memory forensics, cloud forensics et forensique post-quantique, en passant par les outils spécialisés comme EnCase ou The Sleuth Kit. Aujourd'hui, l'investigation numérique tend à devenir proactive et externalisée (DFaaS), intégrant l'IoT Forensics et les évolutions technologiques, confirmant qu'il s'agit d'une discipline vivante et en constante transformation.

Normes et Standards Internationaux

Cette partie met en avant le cadre normatif qui structure la pratique de l'investigation numérique à l'échelle mondiale. Plusieurs standards internationaux sont présentés, en commençant par la série **ISO/IEC 27037, 27041, 27042 et 27043**, qui définissent respectivement les principes de collecte de preuves, la validation des méthodes, l'analyse et les modèles de processus. À cela s'ajoutent des références comme le **NIST SP 800-86**, le **RFC 3227** avec son ordre de volatilité, ou encore le Guide ACPO utilisé au Royaume-Uni. Ces normes assurent une homogénéité des pratiques et garantissent la fiabilité et l'opposabilité des preuves devant les juridictions.

La partie insiste aussi sur les standards émergents, adaptés aux nouveaux environnements technologiques. La **Cloud Forensics** et l'**IoT Forensics** en sont deux exemples, car les preuves numériques se trouvent de plus en plus dans des environnements distribués, virtualisés ou embarqués dans des objets connectés. L'intégration de ces contextes dans les normes vise à répondre à la complexité croissante des infrastructures numériques modernes.

Un deuxième volet présente des applications et cas d'usage concrets à différentes échelles. Au Cameroun, par exemple, l'investigation numérique s'applique aussi bien à la gestion d'incidents en entreprise (fuite de données sensibles) qu'au domaine judiciaire (cyberharcèlement) ou à la sécurité nationale (analyse post-attaque APT). Sur le plan mondial, des cas emblématiques sont détaillés : espionnage industriel aux États-Unis, manipulation électorale assistée par IA en Inde, cyberterrorisme multi-plateforme au Moyen-Orient, fraude bancaire mobile en Afrique de l'Ouest, criminalité environnementale en Australie, ou encore narcotrafic numérique en Amérique latine.

Enfin, la partie propose une synthèse comparative internationale. Chaque région développe ses propres forces, mais toutes convergent vers une même logique : bâtir une expertise robuste, standardisée et adaptée à leur contexte géopolitique et technologique. Les leçons apprises mettent en avant des best practices universelles : respect des normes, coopération transfrontalière, anticipation proactive et usage raisonné de l'intelligence artificielle. L'objectif ultime est de tendre vers une investigation numérique sans frontières, capable de répondre aux cybermenaces globalisées.

Meilleures Pratiques Mondiales

Cette partie expose les méthodologies d'investigation numérique adoptées par les grandes institutions mondiales. On retrouve la méthodologie du SANS Institute (FOR508), axée sur la traçabilité et la reconstruction d'incidents ; celle du CERT/CC, centrée sur la réponse aux incidents et la gestion des crises ; ainsi que le cadre de l'ENISA en Europe et le modèle du DFRC-K en Corée du Sud. Ces approches, bien que différentes dans leur organisation, partagent un objectif commun : structurer l'investigation autour d'étapes claires (acquisition, analyse, corrélation, présentation) pour garantir la robustesse et la validité des preuves.

Un deuxième volet présente l'arsenal technique de l'investigateur moderne. Celui-ci va des outils d'acquisition et d'imagerie (création de copies fidèles de disques ou mémoires) aux solutions d'analyse mémoire avancée (**ex. Volatility**), en passant par la reconstitution de lignes temporelles. L'investigateur doit aussi composer avec des adversaires qui utilisent l'anti-forensique : chiffrement, obfuscation, effacement de données. D'où le développement de techniques dites d'anti-anti-forensique, qui visent à contourner ou détecter ces manœuvres.

Enfin, un accent particulier est mis sur l'usage de l'intelligence artificielle en investigation numérique. Le machine learning est déjà exploité pour la classification automatique de malwares, tandis que le deep learning permet l'analyse comportementale afin de détecter des schémas suspects. Ces outils offrent un gain d'efficacité et de rapidité, mais exigent aussi une vigilance accrue pour éviter les biais ou les erreurs d'interprétation.

En résumé, cette partie montre que les meilleures pratiques mondiales reposent sur trois piliers : **des méthodologies éprouvées**, **un arsenal technique** en constante évolution et une **intégration progressive de l'intelligence artificielle**. L'investigateur numérique doit donc conjuguer rigueur scientifique, maîtrise technologique et capacité d'adaptation pour rester efficace face aux cybermenaces modernes.

L'Ère du Post-Quantique

Cette partie met en lumière l'impact de l'informatique quantique sur l'investigation numérique. Les algorithmes de **Shor** et de **Grover** menacent directement les systèmes cryptographiques classiques : le premier fragilise RSA et ECC en rendant leur factorisation efficace, tandis que le second accélère considérablement la recherche dans de grandes bases de données. Ces avancées créent un

risque majeur dit **Harvest Now, Decrypt Later**, où des données chiffrées aujourd'hui pourraient être décryptées demain une fois les machines quantiques matures.

Les implications pour l'investigation sont considérables : la chaîne de custody (traçabilité des preuves) elle-même pourrait être compromise si les mécanismes de signature ou de chiffrement utilisés deviennent vulnérables. Pour contrer cette menace, la cryptographie post-quantique (PQC), avec des standards en cours de normalisation par le NIST, devient indispensable. L'intégration de ces primitives dans les pratiques forensiques garantit la pérennité et l'opposabilité des preuves numériques.

Au-delà de la menace, le quantique ouvre aussi des opportunités inédites. Des techniques comme la quantum random number analysis ou la tomographie d'état quantique pourraient servir à renforcer la fiabilité des preuves et créer de nouvelles méthodes d'authentification. Ce champ émergent, appelé Quantum Forensics, pourrait révolutionner la manière dont les investigateurs recueillent, analysent et valident les traces numériques.

Enfin, la partie introduit le Trilemme CRO (Confidentialité, Fiabilité, Opposabilité) comme cadre théorique central. Il formalise l'impossibilité d'optimiser pleinement ces trois dimensions en même temps : un système très confidentiel peut perdre en opposabilité juridique, tandis qu'une preuve juridiquement robuste peut sacrifier une partie de la confidentialité. Ce trilemme devient la boussole de la conception de protocoles post-quantiques et rappelle que l'équilibre entre science, technique et droit est au cœur de l'investigation numérique de demain.

Primitives Cryptographiques et Opposabilité

Cette partie approfondit l'analyse des primitives cryptographiques à travers le prisme du **Trilemme CRO** (**Confidentialité, Fiabilité, Opposabilité**). Une méthodologie d'évaluation est proposée : chaque algorithme est étudié selon des indices et paramètres CRO afin de mesurer son équilibre entre sécurité technique et valeur juridique. Cette grille de lecture permet d'aller au-delà de la simple robustesse mathématique pour juger de la pertinence d'une primitive dans un contexte forensique.

Les primitives classiques (AES, RSA, ECC) et modernes (ChaCha20, signatures à seuil) sont évaluées, de même que les primitives post-quantiques comme Kyber (KEM) et Dilithium (signatures). L'analyse comparative montre que si les algorithmes traditionnels restent performants en termes de fiabilité et d'opposabilité, ils sont vulnérables face aux avancées quantiques. Les primitives post-quantiques renforcent la confidentialité mais posent parfois des défis d'implémentation et de standardisation.

Un focus particulier est mis sur les protocoles avancés tels que les preuves à divulgation nulle de connaissance (Zero-Knowledge Proofs) et les signatures distribuées (BLS, signatures à seuil). Ces technologies permettent de préserver la confidentialité tout en maintenant une opposabilité forte, mais leur complexité soulève des enjeux pratiques de vérification et d'adoption par les juridictions. L'objectif est d'arriver à des architectures hybrides, combinant plusieurs primitives pour compenser leurs faiblesses respectives.

Enfin, la partie se conclut avec l'introduction du protocole **ZK-NR**, spécialement conçu pour garantir la non-répudiation dans un environnement post-quantique. Ce protocole s'intègre à la chaîne de custody numérique en apportant une traçabilité résistante au quantique et une validation cryptographique robuste. Il illustre la direction à suivre : créer des solutions où la cryptographie et le droit avancent de concert pour préserver la valeur probatoire des preuves dans un futur incertain.

Cryptanalyse et Analyse de Protocoles

Cette partie s'intéresse à la cryptanalyse et à l'audit des protocoles de sécurité, deux dimensions essentielles pour évaluer la solidité des systèmes utilisés en investigation numérique. Elle commence par les principes de la conception sécurisée, qui reposent sur la simplicité, la transparence et l'adaptabilité. Le Trilemme CRO est ici utilisé comme une véritable boussole de conception : il aide à identifier les compromis entre confidentialité, fiabilité technique et opposabilité juridique.

Une taxonomie des failles cryptographiques est proposée, regroupant les attaques possibles (par canal auxiliaire, par collision, par brute force, etc.) et montrant que la sécurité parfaite n'existe pas. La cryptanalyse est ensuite introduite comme une discipline en deux approches : black-box (observation sans connaissance interne du système) et white-box (analyse en profondeur avec accès aux détails). Avec l'avènement du quantique, la cryptanalyse connaît un tournant majeur, car des attaques autrefois impraticables deviennent théoriquement possibles.

Pour structurer l'audit, une méthodologie en **5 étapes** est présentée : **compréhension du protocole, modélisation des menaces, analyse manuelle, analyse automatisée** (ex. avec l'outil Tamarin) et **test d'implémentation**. Cette démarche systématique garantit une évaluation rigoureuse et reproductible des protocoles cryptographiques.

Enfin, deux cas pratiques sont étudiés : **le protocole ZK-NR** et **la signature BLS**. L'analyse du ZK-NR montre son potentiel pour la non-répudiation post-quantique, mais aussi ses surfaces d'attaque qu'il faut surveiller. La signature BLS, appréciée pour sa légèreté et son efficacité dans les systèmes distribués, présente des forces mais aussi des vulnérabilités face à la cryptanalyse quantique. Ces exemples illustrent concrètement la nécessité d'une vigilance constante et d'une mise à jour continue des pratiques forensiques face aux innovations cryptographiques.

Cadre Juridique

Cette partie traite du droit encadrant l'investigation numérique à l'échelle mondiale, régionale et nationale. Elle commence par le droit américain, avec les Federal Rules of Evidence (FRE), qui définissent les conditions d'admissibilité des preuves, ainsi que des lois spécifiques comme le Stored Communications Act (SCA) ou le Computer Fraud and Abuse Act (CFAA). En Europe, le règlement eIDAS, le RGPD et la Convention de Budapest sont les piliers qui encadrent la valeur juridique et la protection des données. En Afrique, la Convention de Malabo (2014) fixe un cadre continental, complété par divers dispositifs régionaux.

Le cadre camerounais est ensuite détaillé : il s'appuie sur les **lois de 2010/012** et **2010/013** relatives à la **cybersécurité** et à **la cybercriminalité**, et plus récemment sur la **loi 2024/017** qui renforce les mécanismes juridiques de lutte contre la criminalité numérique. Ces textes définissent les incriminations, les procédures d'enquête et les sanctions, tout en posant les bases de l'opposabilité des preuves numériques devant les tribunaux.

Un accent est mis sur la procédure d'investigation au Cameroun, avec un cadre procédural qui encadre la saisie, la conservation et l'exploitation des preuves numériques. Le rôle des experts agréés y est crucial, puisqu'ils garantissent la validité technique et juridique des opérations. La jurisprudence camerounaise, encore en construction, révèle toutefois des défis persistants, notamment en matière de reconnaissance internationale des preuves et de coordination entre acteurs judiciaires et techniques.

En somme, cette partie souligne que l'investigation numérique n'a de valeur que si elle repose sur un socle juridique solide, garantissant à la fois la protection des droits fondamentaux et la recevabilité des preuves. Elle met aussi en évidence la nécessité d'une harmonisation internationale,

car la cybercriminalité ne connaît pas de frontières, alors que les systèmes juridiques restent encore cloisonnés.

Pratique du Forensique

Cette partie présente la mise en œuvre pratique de l'investigation numérique en laboratoire forensique, incluant l'installation complète, la configuration d'environnements spécialisés (**SIFT, Remnux, VM SANS**), l'intégration d'outils open source et commerciaux, et la mise en place de procédures standardisées (SOP, checklists, rapports, scripts). La gestion repose sur la certification, l'accréditation et une chaîne de custody rigoureuse.

L'investigation technique couvre la forensique système (analyse de fichiers NTFS, EXT4, APFS, artefacts Windows/Linux/macOS, mémoire, timelines, virtualisation), la forensique réseau (PCAP, SIEM, threat hunting, attribution technique) et l'analyse post-quantique. La partie traite aussi de l'anti-forensique, où destruction et chiffrement de données nécessitent des contremesures adaptatives assistées par IA, illustrant la dynamique offensive-défensive de la cybersécurité.

Enfin, un benchmarking mondial (FBI/NIST, Scotland Yard, BKA, Singapour, Corée du Sud, France) permet de proposer un framework d'excellence combinant rigueur, innovation et adaptation locale, avec des recommandations pour l'Afrique.

Cas Pratique Intégré (l'affaire CyberFinance Cameroun 2025)

Enfin, après une partie théorique bien fournie sur l'investigation numérique, nous passons à la phase suivante, qui est la mise en pratique de l'investigation numérique à travers un cas concret : l'affaire CyberFinance Cameroun 2025, dont voici un résumé :

En janvier 2025, CyberFinance Cameroun, fintech majeure avec 500 000 clients, a été victime d'un ransomware sophistiqué (LockBit 3.0), entraînant le chiffrement de sa base clients et l'exfiltration de 850 GB de données, avec une demande de rançon de 10 millions d'euros en Bitcoin. L'incident a été détecté grâce aux alertes IDS et des mesures immédiates ont été prises, incluant l'isolement du réseau, la capture des données volatiles et l'activation du plan de crise. L'investigation forensique a révélé une attaque par spear-phishing, PowerShell malveillant, mouvement latéral, exfiltration via HTTPS et chiffrement via GPO, attribuée au groupe LockBit "GoldManager" d'Europe de l'Est. Les preuves ont été collectées selon ISO 27037 et sécurisées avec le protocole ZK-NR, puis analysées via le trilemme CRO et Q2CSI. La remédiation a combiné actions immédiates (isolation, MFA, EDR), court terme (reconstruction systèmes, SIEM, threat hunting) et long terme (Zero Trust, migration post-quantique, SOC 24/7). Les causes identifiées mêlaient failles techniques, humaines et procédurales, conduisant à des recommandations critiques pour renforcer la résilience et la conformité juridique, illustrant l'importance d'une approche intégrée mêlant cybersécurité avancée, preuve légale opposable et préparation post-quantique.