REPUBLIQUE DU CAMEROUN
PAIX-TRAVAIL-PATRIE

REPUBLIC OF CAMEROUN
PEACE-WORK-FATHERLAND

UNIVERSITE DE YAOUNDE I ECOLE NATIONALE SUPERIEURE POLYTECHNIQUE DE YAOUNDE
DEPARTEMENT

UNIVERSITY OF YAOUNDE I
NATIONAL ADVANCED SCHOOL OF ENGINEERING OF YAOUNDE
DEPARTMENT

INTRODUCTION AUX TECHNIQUES D'INVESTIGATION NUMERIQUES : RESUME

Sous la supervision de : M. MINKA Thierry E.

Présenté par : NDJEBAYI PATRICK NATANAEL 24P827 CIN3

Sept 2025

Le manuel présente une vision globale de l'investigation numérique adaptée à l'ère post-quantique, en insistant sur les défis liés à la préservation de la confidentialité, à la garantie de la fiabilité et à l'assurance de l'opposabilité juridique des preuves digitales. Ce cadre analytique, appelé Trilemme CRO, représente une innovation théorique qui guide l'analyse des pratiques et des outils dans ce domaine. L'ouvrage commence par souligner l'importance d'un engagement déontologique pour les praticiens, qui doivent utiliser leurs compétences de manière responsable, en respectant les lois, en protégeant les données et en maintenant une traçabilité stricte de leurs actions, pour éviter tout abus qui pourrait porter atteinte à la société.

Dans sa partie philosophique, le livre explore comment la société numérique transforme l'existence humaine, créant un double digital qui pose des questions sur la transparence et la vie privée. Il discute de l'épistémologie de la preuve numérique, marquant la transition d'une preuve matérielle stable à une preuve volatile et mutable, influencée par des théories comme l'entropie de l'information, les graphes pour modéliser les relations, et le chaos pour comprendre la sensibilité des systèmes. La révolution quantique est présentée comme un changement de paradigme, introduisant des concepts comme la superposition et l'intrication, qui remettent en question les notions traditionnelles de vérité.

Un paradoxe central est celui de l'authenticité invisible, où prouver l'intégrité d'une preuve sans révéler son contenu pose des défis philosophiques et pratiques. Les protocoles à connaissance zéro non-répudiables sont proposés comme solution pour équilibrer ces aspects. L'éthique est au cœur, avec l'investigateur vu comme un philosophe-praticien naviguant entre transparence et confidentialité, efficacité et proportionnalité. L'ontologie de la trace numérique est analysée comme une manifestation d'existence, nécessitant une herméneutique pour interpréter les données en tenant compte des biais.

L'histoire de l'investigation numérique est retracée depuis les années 1970 avec les premiers crimes informatiques, jusqu'à l'ère post-quantique. Des cas emblématiques comme les 414s, l'opération Sundevil, Kevin Mitnick, Enron, Gary McKinnon, Silk Road, Panama Papers et SolarWinds illustrent l'évolution des techniques et des défis, de la professionnalisation à la standardisation, en passant par le big data et l'IA.

Les fondements théoriques incluent le principe de Locard adapté au numérique, avec des traces primaires comme les logs et secondaires comme les métadonnées. Des modèles comme DFRWS, Casey et ISO 27037 sont détaillés pour structurer les processus d'investigation. La théorie de l'information est appliquée pour détecter des anomalies via l'entropie, et les graphes pour analyser les réseaux sociaux et les flux de données.

L'état de l'art couvre les avancées depuis 1979, avec l'introduction de concepts comme la forensique en mémoire, le cloud, l'apprentissage automatique et la blockchain, menant à des paradigmes actuels comme la forensique comme service, proactive et pour IoT.

Les normes internationales sont examinées, de ISO 27037 pour la collecte à NIST SP 800-86 pour l'intégration dans la réponse aux incidents, en passant par RFC 3227 pour l'archivage et ACPO pour les bonnes pratiques. Des standards émergents pour le cloud et l'IoT sont aussi discutés.

Les applications pratiques sont illustrées par des cas d'usage locaux au Cameroun, comme les fuites de données en entreprise, le cyberharcèlement judiciaire et les attaques APT en sécurité nationale, ainsi que des cas mondiaux en Amérique, Asie, Moyen-Orient, Afrique, Océanie et Amérique latine, montrant la diversité des approches

et l'importance de la coopération.

Les méthodologies incluent celles du SANS pour la réponse aux incidents, CERT/CC pour le processus Carnegie Mellon, ENISA pour le cadre européen et DFRC-K pour l'adaptation asiatique, toutes emphatisant la préparation, l'identification, le containment et les leçons apprises.

Les outils avancés couvrent l'acquisition avec validation d'intégrité, l'analyse de mémoire avec Volatility, le contournement légal de chiffrement, la détection d'obfuscation et l'utilisation de l'IA pour classer les malwares et analyser les comportements.

L'impact du quantique est analysé, avec les algorithmes de Shor et Grover menaçant la cryptographie actuelle, menant au "harvest now, decrypt later". La cryptographie post-quantique avec standards NIST comme Kyber et Dilithium est présentée comme solution, avec des opportunités en forensique quantique pour l'analyse de nombres aléatoires et la tomographie d'états.

Le Trilemme CRO est formalisé mathématiquement comme une incompatibilité entre ses trois axes, avec analyse des primitives symétriques comme AES et ChaCha, asymétriques comme RSA et ECC, post-quantiques comme Kyber et Dilithium, et avancées comme les preuves à connaissance zéro. L'architecture Q2CSI est proposée pour une sécurité composable en couches.

Le protocole ZK-NR est détaillé pour assurer une non-répudiation sans révélation, avec architecture, preuve de sécurité et applications en chain of custody post-quantique.

Les fondements de la conception sécurisée et de la cryptanalyse sont explorés, avec le Trilemme CRO comme boussole, taxonomie des failles, approches black/white box et post-quantique.

La méthodologie d'analyse formelle des protocoles inclut la modélisation des menaces avec Dolev-Yao, outils comme Tamarin et un audit en 5 étapes.

Un cas pratique analyse ZK-NR et BLS, avec recommandations pour l'investigateur.

La législation mondiale couvre le droit américain avec FRE, SCA, CFAA, européen avec eIDAS, RGPD, Convention de Budapest, et africain avec Malabo.

Le droit camerounais est détaillé avec lois de 2010 et 2024, procédures d'investigation et jurisprudence.

Les pratiques opérationnelles incluent la gestion de laboratoire, SOP, formation, forensique système avancée pour différents OS, mémoire, timeline, virtualisation, post-quantique.

La forensique réseau couvre PCAP, SIEM, threat hunting, attribution, protocoles émergents.

L'anti-forensique traite destruction, dissimulation, obfuscation, cryptanalyse, avec contre-mesures et IA.

Le benchmarking mondial compare FBI/NIST, Scotland Yard, BKA, Singapore/Corée, DGSI/ANSSI, Japon, vers un framework d'excellence universelle.

Un cas intégré sur CyberFinance Cameroun 2025 illustre les phases de détection à remédiation, avec application ZK-NR et CRO.

En conclusion, l'ouvrage appelle à une investigation sans frontières, intégrant diversité et innovation pour une excellence globale.

Le manuel met l'accent sur la nécessité d'anticiper les défis quantiques dans l'investigation numérique, en développant des compétences en cryptographie résistante et en adoptant des protocoles comme ZK-NR pour maintenir l'intégrité des preuves. Il souligne que la transition vers le post-quantique requiert non seulement des outils techniques mais aussi une réflexion éthique profonde sur la balance entre sécurité et

droits individuels. Les cas d'usage démontrent comment les contextes culturels et juridiques influencent les approches, appelant à une harmonisation internationale tout en respectant les spécificités locales.

Les analyses des primitives révèlent que les standards actuels comme RSA sont vulnérables, tandis que les nouveaux comme Dilithium offrent une résistance supérieure, bien que avec des compromis en maturité. L'architecture en couches permet de composer la sécurité pour optimiser le Trilemme CRO selon le contexte.

Les pratiques forensiques avancées, de la mémoire à la réseau, intègrent l'IA pour une efficacité accrue, tandis que l'anti-forensique nécessite des contre-mesures adaptatives pour contrer l'obfuscation.

Globalement, le livre positionne l'investigateur comme un gardien de la vérité numérique, équipé pour naviguer les complexités post-quantiques avec sagesse et intégrité.

L'approche philosophique approfondie permet de comprendre comment les traces numériques ne sont pas de simples données mais des extensions de l'existence humaine, requérant une interprétation nuancée pour éviter les erreurs judiciaires. La discussion sur le paradoxe de l'authenticité met en lumière les tensions entre preuve et privacy, résolues par des innovations comme ZK-NR qui permettent de vérifier sans révéler.

Dans l'historique, l'évolution montre une maturation de la discipline, des premiers hacks amateurs aux attaques étatiques sophistiquées, soulignant l'importance de l'apprentissage continu face à des menaces en constante mutation. Les grandes affaires servent d'exemples concrets, illustrant comment des preuves numériques ont résolu des crimes complexes, de serial killers à des cyberarmes comme Stuxnet.

Le cadre théorique fournit les bases pour une investigation rigoureuse, en appliquant des principes scientifiques pour extraire la vérité des données. L'état de l'art encourage l'adoption de technologies émergentes pour rester en avance sur les criminels.

Les normes assurent l'interopérabilité et la validité legale des preuves, essentielles pour des enquêtes transfrontalières. Les cas d'usage variés enrichissent la compréhension pratique, montrant des adaptations locales à des problèmes globaux.

Les méthodologies structurées guident l'investigateur à travers les étapes critiques, minimisant les risques d'erreurs. Les outils, de l'acquisition à l'analyse IA, sont présentés comme indispensables pour traiter les volumes massifs de données.

Le focus post-quantique prépare à un avenir où la cryptographie actuelle sera obsolète, promouvant la migration vers des systèmes résilients. Le Trilemme CRO offre un outil analytique pour évaluer les compromis inévitables en sécurité.

Le protocole ZK-NR est un pilier pour des preuves opposables sans compromettre la confidentialité, avec des applications directes en justice. La cryptanalyse enseigne à penser comme l'adversaire pour renforcer les défenses.

Les aspects juridiques ancrent la technique dans la réalité légale, avec un accent sur le Cameroun pour contextualiser localement. Les pratiques opérationnelles transforment la théorie en action, de la gestion de labo à l'analyse système détaillée.

La forensique réseau révèle les chemins cachés des attaques, tandis que l'anti-forensique arme contre les tentatives de dissimulation. Le benchmarking inspire en montrant les meilleures pratiques mondiales, adaptables partout.

Le cas CyberFinance intègre tous les éléments, démontrant une réponse complète à une crise, de la détection à la prévention future. Au final, le manuel inspire une pratique éthique et innovante pour protéger la société numérique.

Les engagements déontologiques rappellent que le pouvoir technique implique une

grande responsabilité, avec des piliers comme l'intégrité et la proportionalité guidant chaque action. Les dix commandements servent de boussole morale pour l'investigateur.

La philosophie post-quantique envisage une éthique adaptée aux nouvelles réalités, où l'investigation devient un acte de liberté préservant les droits fondamentaux. L'histoire souligne les leçons tirées des échecs passés pour mieux affronter les menaces futures.

Les fondements théoriques, ancrés dans la science, assurent la robustesse des conclusions forensiques. L'évolution scientifique montre un champ en pleine expansion, intégrant l'IA et le quantique pour des analyses plus précises.

Les normes globales favorisent une uniformité qui facilite la coopération internationale. Les applications régionales mettent en évidence des défis uniques, comme en Afrique avec des ressources limitées mais une innovation croissante.

Les méthodologies variées permettent une flexibilité selon le contexte, tandis que les outils avancés démocratisent l'accès à des techniques sophistiquées. Le quantique représente à la fois une menace et une opportunité pour réinventer la forensique.

Le Trilemme CRO force à des choix éclairés, équilibrant les trois aspects pour des solutions optimales. ZK-NR illustre comment la technologie peut résoudre des paradoxes anciens.

La cryptanalyse formelle prévient les vulnérabilités, avec des cas pratiques renforçant la compréhension. Le cadre juridique assure que les preuves tiennent en cour, adapté aux contextes locaux.

Les opérations quotidiennes, de labo à terrain, exigent une préparation minutieuse. La forensique système et réseau révèle les secrets cachés dans les machines et connexions.

Contre l'anti-forensique, des stratégies proactives maintiennent l'avantage. Le benchmarking mondial encourage l'excellence par l'émulation des leaders.

Le cas intégré synthétise tout, montrant l'efficacité d'une approche holistique. En somme, ce manuel équipe pour un avenir numérique sécurisé et juste.

Les ressources pédagogiques complémentaires, disponibles en ligne, renforcent l'apprentissage par des supports multimédias et collaboratifs. L'avant-propos positionne l'ouvrage comme fruit de décennies d'expérience, ciblant les spécialistes en cybersécurité.

La dédicace personnelle ajoute une touche humaine, rappelant le soutien nécessaire pour l'innovation. L'engagement moral insiste sur l'usage légitime des compétences, évitant les atteintes illégitimes.

Les piliers éthiques – intégrité, proportionalité, responsabilité, service – forment la base d'une pratique vertueuse. Les commandements guident le quotidien, de la non-destruction à l'honnêteté testimoniale.

Les engagements post-quantiques préparent à anticiper les disruptions technologiques. La philosophie fondatrice relie l'humain au digital, questionnant l'être dans un monde connecté.

L'épistémologie évolue avec les deepfakes, nécessitant de nouvelles vérifications. Les mathématiques sous-tendent l'analyse, de l'entropie à la chaos théorie.

Le quantique bouleverse les certitudes, avec superposition challengeant la causalité. Le paradoxe d'authenticité demande des preuves invisibles, résolues par ZK-NR intégré au CRO.

L'éthique post-quantique appelle à des impératifs adaptés, voyant l'investigation comme affirmation de liberté. L'histoire trace le chemin des pionniers aux experts actuels.

Les affaires clés montrent l'impact réel, de captures criminelles à détections d'armes cyber. Les théories comme Locard numérique guident la recherche de traces.

Modèles standards structurent le travail, assurant reproductibilité. La théorie informationnelle détecte anomalies, graphes révèlent connexions.

L'état de l'art chronique innovations, de forensique mémoire à quantum-safe. Normes ISO et NIST assurent qualité, ACPO principes éthiques.

Cas camerounais adaptent à contextes locaux, mondiaux montrent variété. Méthodologies SANS à DFRC-K couvrent divers scénarios.

Outils comme Volatility analysent mémoire, IA classe menaces. Quantique menace chiffrement, PQC protège futur.

Trilemme CRO analyse primitives, Q2CSI compose sécurité. ZK-NR sécurise preuves sans exposition.

Conception sécurisée évite failles, cryptanalyse teste robustesse. Analyse protocoles avec Tamarin vérifie propriétés.

Cas ZK-NR/BLS appliquent théorie. Lois US/EU/Afrique régulent, Cameroun adapte localement.

Labos forensiques exigent SOP, formation continue. Forensique système examine OS en profondeur, mémoire révèle volatil.

Réseau analyse flux, hunt menaces. Anti-forensique contre dissimulation, IA aide détection.

Benchmark inspire, cas CyberFinance pratique intégrée. Conclusion vise excellence globale.

L'ouvrage encourage une communauté collaborative pour avancer la discipline, avec ressources open source favorisant le partage. La version préliminaire invite à des retours pour amélioration, visant une édition anglaise internationale.

Les engagements spécifiques par domaine, comme post-quantique ou protection données, spécialisent l'éthique. L'auto-évaluation continue maintient les standards élevés.

La philosophie lie existentialisme à digital, herméneutique interprète données comme textes. Histoire montre progression de chaos à ordre.

Affaires emblématiques enseignent résilience. Fondements théoriques ancrent pratique en science.

Évolution scientifique anticipe tendances. Normes unifient approches globales.

Applications bridges théorie et réel. Méthodologies guident efficacité.

Outils empower investigateurs. Post-quantique redéfinit sécurité.

Trilemme CRO balance trade-offs. ZK-NR innove preuves.

Cryptanalyse fortifie systèmes. Analyse formelle prévient breaches.

Cas pratiques illustrent application. Juridique valide preuves.

Opérationnel implémente théorie. Système/réseau uncover hidden.

Anti-forensique challenge, overcome par innovation. Benchmark set bars high.

Cas intégré tie all together. Conclusion inspire future generations.

Les annexes fournissent glossaire, outils, templates pour usage pratique. Contacts réseaux facilitent collaboration.

Globalement, ce manuel est un guide complet pour maîtriser l'investigation numérique post-quantique, alliant théorie profonde et pratique actionable pour un monde plus sécurisé.