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 :
BAALAWE LIONEL JOSSELIN, *24P822*

Sous l'encadrement de :
Expert Thierry MINKA

Année académique 2025 / 2026

Résumé du manuel : Théories et pratiques de l'investigation numérique post-quantique

Ce manuel, rédigé par Thierry MINKA, offre une synthèse originale et ambitieuse de l'investigation numérique. Il ne se limite pas à décrire des techniques, mais croise la philosophie, la science, le droit et la pratique, tout en intégrant la problématique émergente de l'ère post-quantique. L'apport central de l'ouvrage est le **Trilemme CRO** (Confidentialité, Fiabilité, Opposabilité juridique), un modèle conceptuel qui formalise les tensions auxquelles la preuve numérique est soumise. L'auteur démontre que l'investigation numérique est une discipline vivante, constamment appelée à évoluer face aux mutations technologiques, aux enjeux juridiques et aux défis éthiques du XXI^{e} siècle.

Fondements et historique

L'investigation numérique, telle que nous la connaissons aujourd'hui, est le fruit d'une évolution progressive qui s'étend sur plus de quatre décennies. Elle repose sur un principe fondateur issu de la criminalistique classique : le **principe de Locard**, adapté au numérique, selon lequel « toute action laisse une trace ». Ainsi, chaque interaction avec un système informatique — connexion, copie de fichier, navigation web ou communication réseau — laisse des artefacts exploitables par un enquêteur.

Dans les années 1980, les premiers cas de **cybercriminalité** apparaissent avec des intrusions dans des systèmes universitaires ou gouvernementaux. Ces affaires étaient souvent traitées de manière empirique, sans méthodologie ni outils standardisés. Elles ont toutefois suscité une prise de conscience sur la nécessité de développer des techniques d'analyse spécifiques.

Les années 2000 marquent un tournant, avec la multiplication des attaques et la montée en puissance de la criminalité organisée dans le cyberespace. Des incidents emblématiques illustrent cette évolution :

— **Stuxnet** (2010) : premier cyberarme connue, conçue pour saboter des centrifugeuses nucléaires iraniennes. Cet événement a montré que des malwares pouvaient causer des dégâts physiques, inaugurant l'ère de la cyberguerre.

— **WannaCry** (2017) : ransomware de portée mondiale exploitant une faille de Windows. En quelques heures, il a paralysé hôpitaux, administrations et entreprises, soulignant la vulnérabilité des infrastructures critiques.

— **Panama Papers** (2016) : fuite massive de documents confidentiels d'un cabinet d'avocats, révélant des pratiques d'évasion fiscale à grande échelle. Cet épisode a montré que l'investigation numérique pouvait avoir des implications politiques et économiques planétaires.

Ces affaires démontrent que l'investigation numérique est passée d'une simple *expertise technique ponctuelle* à une **discipline stratégique**, indispensable pour la sécurité nationale, la stabilité économique et la transparence sociale.

Enfin, au-delà de son aspect technique, l'investigation numérique s'accompagne d'une réflexion philosophique et éthique. L'usage d'outils intrusifs pour collecter et analyser des preuves pose la question de l'équilibre entre efficacité des enquêtes et respect des libertés individuelles. La discipline se développe donc à la croisée de la **philosophie**, de l'**histoire** et des **sciences de l'information**, et son évolution traduit les tensions permanentes entre sécurité, vie privée et souveraineté numérique.

Transition : Ces fondements historiques et philosophiques ont conduit à la nécessité de construire un **cadre théorique et normatif** solide, capable de donner une légitimité scientifique et juridique aux enquêtes numériques.

Cadre théorique et conceptuel

Après les fondements historiques et philosophiques, il est nécessaire de donner à l'investigation numérique un **cadre théorique et scientifique solide**. Celui-ci permet de dépasser les approches empiriques pour inscrire la discipline dans une logique rigoureuse, comparable aux sciences exactes et juridiques.

Le premier principe mobilisé est celui de **Locard**, adapté au numérique : « toute action laisse une trace ». Ce postulat fonde la recherche de *traces numériques*, c'est-à-dire d'artefacts laissés volontairement ou involontairement par un utilisateur ou un système. Ces traces se classent en deux grandes catégories :

— **Traces primaires** : elles proviennent directement des activités de l'utilisateur ou du système, comme les fichiers créés, les journaux (logs) ou les captures réseau.

— **Traces secondaires** : elles résultent d'indices indirects, comme les métadonnées, les horodatages ou encore les résidus de mémoire. Ces éléments sont souvent cruciaux pour reconstruire une chronologie des événements.

Afin d'exploiter ces traces de manière fiable, plusieurs **modèles méthodologiques** ont été proposés :

— Le modèle **DFRWS** (2001), considéré comme un des premiers cadres structurés pour l'investigation numérique.

— La norme **ISO/IEC 27037** (2012), qui définit les bonnes pratiques pour l'identification, la collecte et la préservation des preuves numériques.

La dimension théorique repose également sur les **outils mathématiques**, qui offrent un langage commun pour analyser la complexité des données :

— L'**entropie**, qui mesure le degré de désordre ou d'incertitude dans une information, utile pour détecter un chiffrement ou une dissimulation.

— Les **graphes**, qui permettent de représenter les relations entre machines, utilisateurs ou événements, et de visualiser les structures cachées dans un réseau.

— La **théorie du chaos**, qui met en évidence la sensibilité des systèmes numériques aux conditions initiales et aide à comprendre l'imprévisibilité apparente de certaines attaques.

En réunissant ces éléments — principes, modèles et outils scientifiques —, le cadre conceptuel fournit à l'investigation numérique une légitimité comparable à celle des sciences criminelles classiques.

Transition : Fort de ce socle théorique, il devient indispensable d'inscrire la pratique dans un **cadre normatif international**, afin d'assurer la fiabilité et l'opposabilité juridique des preuves recueillies.

Meilleures pratiques et outils modernes

Les meilleures pratiques mondiales découlent de décennies d'expérience. Le **SANS Institute** propose des cadres méthodologiques de réponse aux incidents. Le **CERT** diffuse des bonnes pratiques en matière de détection et de gestion de crises. L'**ENISA** émet des recommandations

adaptées à l'Europe. Singapour et la Corée du Sud montrent, quant à eux, comment intégrer la forensique dans des politiques publiques ambitieuses.

Les outils ont suivi cette évolution. L'imagerie disque permet de capturer intégralement un support. La **mémoire forensics** (Volatility, Rekall) révèle les malwares résidents et les processus furtifs. Les solutions de capture réseau (Wireshark, tcpdump) et les SIEM facilitent la corrélation des logs. L'intelligence artificielle ouvre de nouvelles perspectives : elle permet la classification automatisée de malwares, la détection d'anomalies comportementales et l'analyse massive de données issues du cloud.

La discipline doit aussi contrer l'**anti-forensique**, c'est-à-dire les techniques utilisées pour effacer ou camoufler les traces : chiffrement, stéganographie, obfuscation, effacement sécurisé. L'anti-anti-forensique vise à détecter et neutraliser ces méthodes.

L'Ère du Post-Quantique

L'avènement de l'informatique quantique constitue une véritable rupture dans l'histoire des technologies de l'information. Alors que la cryptographie moderne — fondée sur RSA, ECC ou encore AES — a longtemps constitué le socle de la sécurité numérique, l'arrivée de nouveaux algorithmes quantiques remet en cause cet équilibre.

Deux avancées majeures illustrent cette menace :

— **L'algorithme de Shor** (1994) : capable de factoriser rapidement de grands entiers et de résoudre le logarithme discret. Cela compromet directement RSA et les courbes elliptiques (ECC), qui sont aujourd'hui largement utilisés pour l'authentification et la signature électronique.

— **L'algorithme de Grover** : réduit la complexité de recherche dans une base non structurée de $O(N)$ à $O(\sqrt{N})$. Concrètement, il divise par deux la sécurité effective des algorithmes symétriques comme AES, obligeant à doubler la taille des clés pour conserver un niveau de protection équivalent.

Les conséquences pour l'investigation numérique sont profondes :

— Les **données chiffrées**, utilisées comme preuves, risquent d'être déchiffrées rétroactivement lorsque les calculateurs quantiques deviendront accessibles.

— La **chaîne de custody**, qui repose sur des signatures numériques pour garantir l'intégrité et l'authenticité des preuves, pourrait être fragilisée si ces signatures deviennent falsifiables.

— Les **protocoles de communication sécurisés** (TLS, VPN, certificats numériques) pourraient perdre toute validité juridique, compromettant la confidentialité et la fiabilité des preuves recueillies.

Face à ces défis, la communauté scientifique et les organismes de normalisation explorent plusieurs pistes :

— Le développement de la **cryptographie post-quantique**, avec des algorithmes résistants comme *Kyber* (échange de clés) et *Dilithium* (signatures), récemment standardisés par le NIST.

— L'émergence du **Quantum Forensics**, une discipline nouvelle qui vise à analyser les traces numériques dans des environnements hybrides, où coexistent technologies classiques et quantiques.

— L'adoption de **protocoles hybrides**, combinant primitives classiques et post-quantiques, pour assurer une transition progressive et garantir la résilience des enquêtes.

Enfin, le **Trilemme CRO** (Confidentialité, Fiabilité, Opposabilité) prend une dimension nouvelle à l'ère quantique : comment protéger la confidentialité des preuves face à des attaquants surpuissants ? Comment maintenir la fiabilité des outils alors que les primitives changent ? Comment assurer l'opposabilité juridique de preuves fondées sur des schémas encore émergents ?

Transition : Ces enjeux montrent la nécessité d'examiner de manière approfondie les **primitives cryptographiques** adaptées au monde post-quantique, afin de garantir la continuité et la légitimité des investigations numériques.

Cryptanalyse et protocoles

La cryptanalyse, loin d'être un simple exercice académique, est au cœur de la discipline. Elle permet d'anticiper les vulnérabilités et de valider la robustesse des protocoles. L'auteur propose une méthodologie en cinq étapes : compréhension, modélisation, analyse manuelle, automatisation et test d'implémentation.

Deux exemples majeurs l'illustrent : le protocole **ZK-NR**, qui combine preuves à divulgation nulle de connaissance et non-répudiation, et les **signatures BLS**, utilisées dans la blockchain forensics. Ces cas démontrent que la cryptanalyse est indispensable pour mesurer la conformité des protocoles au Trilemme CRO et garantir leur utilisabilité dans des enquêtes judiciaires.

Cadre juridique

La technique ne suffit pas : une preuve n'a de valeur que si elle est juridiquement reconnue. Les cadres juridiques internationaux ont progressivement intégré l'investigation numérique. Aux États-Unis, les **Federal Rules of Evidence** fixent les règles de recevabilité. En Europe, le **RGPD** et la **Convention de Budapest** encadrent la collecte et le traitement des données. En Afrique, la **Convention de Malabo** a jeté les bases d'une régulation régionale.

Le Cameroun a adopté un cadre national avec les lois 2010/012 et 2010/013, récentes complétées par la loi 2024/017. Ces textes traitent de cybersécurité, de cybercriminalité et de protection des données personnelles.

Le défi est double : adapter les législations à l'évolution rapide des technologies, et former des magistrats capables de comprendre la valeur et les limites de la preuve numérique.

Pratique du Forensique

Après les bases théoriques et juridiques, l'investigation numérique prend forme dans la **pratique du forensique**. Celle-ci regroupe les méthodes et outils qui permettent d'identifier, de collecter et d'analyser les preuves numériques dans un cadre rigoureux.

Organisation et laboratoire

Un laboratoire forensique comprend des postes sécurisés, des équipements d'acquisition (write blockers, stations d'imagerie) et des logiciels spécialisés comme *EnCase*, *Sleuth Kit* ou *Volatility*. Chaque étape — saisie, acquisition, analyse et rapport — est guidée par des procédures normalisées garantissant l'intégrité des preuves.

Forensique système et réseau

L'analyse des systèmes (Windows, Linux, macOS) permet d'exploiter fichiers supprimés, journaux et mémoire vive. Côté réseau, les captures de trafic (*PCAP*), les journaux de sécurité et les plateformes SIEM servent à retracer des attaques et attribuer des comportements suspects.

Anti-forensique et contre-mesures

Les attaquants utilisent des techniques d'effacement, de chiffrement ou de dissimulation. Le rôle du praticien est de les détecter et de les contourner grâce à des outils et méthodes adaptés.

Approches internationales

Les pratiques varient selon les pays : le FBI mise sur la technicité, Scotland Yard sur la procédure, l'Allemagne et Singapour sur l'innovation, et la France sur le cadre légal. Toutes poursuivent un même but : produire des preuves **fiables et recevables en justice**.

Transition : Pour illustrer concrètement ces méthodes, le manuel propose un **cas pratique camerounais** qui synthétise théorie et pratique.

Cas pratique : CyberFinance Cameroun 2025

Le manuel se conclut par une étude de cas appliquée. Une banque camerounaise est victime d'un ransomware sophistiqué. L'enquête suit toutes les étapes théoriques et normatives : détection et confinement de l'incident, collecte de preuves selon ISO 27037, application du protocole ZK-NR pour la non-répudiation, analyse post-quantique pour anticiper les faiblesses cryptographiques, et poursuite judiciaire fondée sur le cadre légal camerounais.

Ce cas montre la complémentarité entre la théorie, les normes, les pratiques et le droit. Il illustre aussi la nécessité d'adapter les méthodologies aux réalités locales, tout en tenant compte des évolutions technologiques mondiales.

Conclusion

L'investigation numérique se révèle comme une discipline hybride, située à l'intersection de la philosophie, de la science, du droit et de la pratique opérationnelle. Le **Trilemme CRO** constitue un apport théorique majeur pour comprendre les compromis de l'ère post-quantique. L'avenir dépendra de la capacité des investigateurs à intégrer de nouvelles cryptographies, à renforcer la chaîne de confiance et à maintenir un équilibre entre protection des données, efficacité des enquêtes et respect du droit.