RÉPUBLIQUE DU CAMEROUN
Paix – Travail – Patrie
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR
UNIVERSITÉ DE YAOUNDÉ I
ÉCOLE NATIONALE SUPÉRIEURE POLYTECHNIQUE
DÉPARTEMENT DE GÉNIE INFORMATIQUE

REPUBLIC OF CAMEROON
Peace – Work – Fatherland
MINISTRY OF HIGHER EDUCATION
THE UNIVERSITY OF YAOUNDÉ I
NATIONAL ADVANCED SCHOOL OF ENGINEERING
COMPUTER ENGINEERING DEPARTMENT

RÉSUMÉ – LIVRE 1

Théorie et pratique de l'investigation numérique

Chaho Tchime Perside Jackie

Classe : CIN 4 — Matricule : 22p094

Département de Génie Informatique — ENSPY

Introduction

L'investigation numérique a évolué d'une simple pratique technique vers une discipline philosophique et scientifique complète, confrontée à ses défis les plus importants : l'avènement de l'informatique quantique, la massification des données et la nécessité absolue d'une éthique rigoureuse. Ce document synthétise les fondements, l'histoire, la méthodologie et les perspectives futures de ce domaine, tel que présenté dans un manuel de référence, en se focalisant sur une vision globale, de la philosophie à la pratique opérationnelle.

1 L'Engagement Déontologique

« La technique la plus sophistiquée ne vaut rien sans l'intégrité de celle ou celui qui la manie. »
— Minka Mi Nguidjoi Thierry Emmanuel

La maîtrise technique doit être guidée par une éthique rigoureuse, ses principes directeurs (les 4 piliers) sont :

- **Intégrité:** Honnêteté intellectuelle et rectitude morale.
- **Proportionalité:** Adapter les moyens techniques à la gravité de l'infraction.
- **Responsabilité:** Assumer l'entière responsabilité de ses actes et conclusions.
- **Service:** Servir la justice et la vérité, et non des intérêts privés

1.1 Les Dix commandements de l'investigation numérique

1. Tu ne causeras pas de dommage aux systèmes que tu investigues
2. Tu respecteras la vie privée et dignité des personnes
3. Tu maintiendras la chaine de custody sans faille
4. Tu documenteras intégralement tes processus et décisions
5. Tu reconnaîtras les limites de tes compétences et connaissances
6. Tu résisteras aux pressions contraires à l'éthique
7. Tu protégeras les données sensibles dont tu as la garde
8. Tu témoigneras avec honnêteté et objectivité
9. Tu contribueras au développement de la discipline
10. Tu honoreras la confiance que la société place en toi

La **chaîne de custody** est la traçabilité complète et ininterrompue de chaque manipulation d'une preuve numérique, depuis sa découverte jusqu'à sa présentation devant un tribunal.

2 La Nature de la Preuve Numérique

La preuve numérique est fondamentalement différente de la preuve traditionnelle :

- **Immatérielle, mutable et fragile:** Elle est constituée de données (0 et 1) qui peuvent être facilement altérées.
- **Authentique par confiance:** Son authenticité ne repose plus sur son apparence mais sur une **chaîne de confiance** (processus de collecte, hash, horodatage, intégrité de l'expert).

2.1 Le Paradoxe de l'Authenticité Invisible

Ce paradoxe est central :

- Prouver l'authenticité d'une preuve nécessite souvent de la divulguer, ce qui compromet la confidentialité de son contenu.
- Protéger sa confidentialité (en la chiffrant) rend la preuve de son authenticité difficile.
- La résolution de ce paradoxe appelle à l'utilisation de technologies avancées comme les **protocoles Zero-Knowledge**.

3 Le Trilemme Éthique Fondamental

L'investigateur doit constamment naviguer entre trois tensions contradictoires :

1. **Transparence vs Vie privée:** Comment rendre le processus vérifiable sans violer la vie privée des personnes ?
2. **Efficacité vs Proportionnalité:** Faut-il tout collecter pour être efficace ou seulement ce qui est nécessaire et proportionné ?
3. **Innovation vs Responsabilité:** Privilégier les outils nouveaux (IA) ou les méthodes éprouvées et compréhensibles pour un tribunal ?

4 Évolution Historique

L'histoire de la discipline se découpe en cinq ères :

- **1970-1990 :** Les prémices (premiers vers, affaire du "414s").
- **1990-2000 :** Professionnalisation (opération Sundevil, arrestation de Kevin Mitnick).
- **2000-2010 :** Standardisation (affaire Enron, Gary McKinnon).
- **2010-2020 :** Big Data et Cloud (Silk Road, Panama Papers).
- **2020-Présent :** Ère post-quantique et IA (attaque SolarWinds).

Des affaires emblématiques comme BTK Killer (métadonnées), Stuxnet (cyberarme) et WannaCry (analyse en temps réel) ont façonné les pratiques.

5 Fondements Théoriques

Le **principe de Locard numérique** ("toute action laisse une trace") est central. Les modèles d'investigation se sont standardisés (DFRWS, ISO/IEC 27037) et s'appuient sur des théories mathématiques comme celle de l'information (Shannon) pour détecter des anomalies ou la théorie des graphes pour modéliser les réseaux.

6 Le Cadre Normatif Global

Un ensemble de standards internationaux guide la pratique :

- **ISO/IEC 27037, 27041, 27042, 27043** pour la gestion des preuves.
- **NIST SP 800-86** pour l'intégration de la forensique dans la réponse aux incidents.
- **RFC 3227** pour l'ordre de volatilité lors de la collecte.
- **ACPO Good Practice Guide** et ses quatre principes fondamentaux.

7 Méthodologies Systématiques

Face à la complexité des incidents, des cadres méthodologiques standardisés sont essentiels pour garantir l'exhaustivité et la défensabilité juridique. Les modèles présentés sont :

- **SANS FOR508 (Incident Response) :** Un cycle en six phases (Préparation, Identification, Confinement, Éradication, Récupération, Leçons Apprises) qui insiste sur la préparation en amont.
- **CERT/CC :** Un flux opérationnel continu (Détecter, Trier, Répondre, Post-Incident).
- **ENISA (Européen) :** Un modèle en trois macro-étapes (Pré-investigation, Investigation, Post-investigation).
- **Modèles Asiatiques (ex: DFRC-K) :** Ils illustrent l'**adaptation contextuelle** nécessaire, intégrant des spécificités locales (prédominance des smartphones, systèmes d'identification, contextes légaux).

8 L'Arsenal Technique

L'expert dispose d'une palette d'outils pour chaque étape de l'investigation :

- **Acquisition et Imagerie :** Création d'une copie bit-for-bit à l'aide d'outils comme FTK Imager ou `dd`, avec l'usage obligatoire de *write-blockers* et de hashs cryptographiques (SHA-256) pour prouver l'intégrité.
- **Analyse de Mémoire Vive (Memory Forensics) :** Utilisation d'outils comme **Volatility Framework** pour analyser la RAM et y trouver des processus, connexions ou malwares furtifs.
- **Stéganalyse :** Techniques (analyses statistiques, Machine Learning) pour détecter des données cachées dans des fichiers.

- **Classification de Malware par IA :** Utilisation de modèles de Machine Learning (Random Forest, réseaux de neurones) pour classer automatiquement les malwares par famille face au volume exponentiel.
- **Techniques Anti-Anti-Forensique (AAF) :** Contre-mesures pour contourner les techniques adverses, comme les attaques *Cold Boot* ou *DMA* pour extraire des clés de chiffrement de la RAM.

9 La Menace Quantique et la Réponse Post-Quantique

L'avènement de l'ordinateur quantique constitue une menace existentielle pour la cryptographie actuelle.

9.1 Nature de la Menace

- L'**algorithme de Shor** rendra obsolètes les algorithmes asymétriques (RSA, ECC).
- L'**algorithme de Grover** réduira la sécurité des algorithmes symétriques (AES).
- La stratégie **"Harvest Now, Decrypt Later"** incite des acteurs à stocker dès aujourd'hui des données chiffrées pour les déchiffrer plus tard avec un ordinateur quantique.

9.2 La Migration vers le PQC

Transition vers des algorithmes **post-quantiques** résistants, standardisés par le NIST (ex: **CRYSTALS-Dilithium** pour les signatures, **CRYSTALS-Kyber** pour le chiffrement), souvent déployés via des **architectures hybrides**.

9.3 Implications pour la Preuve

Cette migration impacte directement la **chaîne de custody** (les signatures scellant les preuves doivent être migrées) et pourrait permettre une analyse rétrospective de preuves chiffrées, tout en ouvrant un nouveau champ : la **Quantum Forensics**.

L'investigator moderne doit allier une maîtrise technique des outils actuels, une rigueur méthodologique et une vision à long terme pour anticiper les ruptures technologiques comme l'informatique quantique.

10 Le Trilemme CRO (Confidentialité, Fiabilité, Opposabilité)

Cette contribution théorique majeure formalise une impossibilité : **aucune primitive cryptographique ne peut optimiser simultanément la Confidentialité (C), la Fiabilité (R) et l'Opposabilité juridique (O)**. Un compromis (trade-off) is toujours nécessaire. Par exemple :

- **RSA** offre une excellente Opposabilité (O=0.9) mais une faible Confidentialité future (C=0.1).
- **zk-SNARKs** offrent une Confidentialité forte (C=0.98) mais une Opposabilité faible (O=0.4).

Cette analyse permet de concevoir des **architectures hybrides** (ex: RSA + Kyber) et d'adapter le choix des primitives au contexte.

11 Le Protocole ZK-NR (Zero-Knowledge Non-Repudiation)

Pour résoudre le paradoxe de l'authenticité invisible, le protocole **ZK-NR** est proposé. Il permet de **prouver l'authenticité et l'origine d'une preuve (non-répudiation) sans en révéler le contenu (confidentialité)**, en utilisant des preuves à divulgation nulle de connaissance (ZK). C'est une brique technologique essentielle pour l'ère post-quantique, offrant une base pour une "chaîne de custody privative".

12 Paysage Juridique International et Camerounais

La discipline évolue dans un cadre juridique complexe :

- **International :** FRE (USA), RGPD et eIDAS (Europe), Convention de Budapest.
- **Cameroun :** Loi N°2010/012 sur la cybercriminalité, Loi N°2010/013 sur les communications électroniques, et Loi N°2024/017 sur la protection des données. La procédure d'investigation est codifiée et requiert des experts agréés.

13 Gestion d'un Laboratoire Forensique

La pratique opérationnelle nécessite un laboratoire équipé, des Procédures Opérationnelles Standards (SOP), une gestion rigoureuse de la chaîne de custody et une formation continue face à l'évolution des menaces.

14 Forensique Avancée (Système et Réseau)

Les analyses techniques couvrent en profondeur les systèmes de fichiers (NTFS, EXT4, APFS), la mémoire vive (Memory Forensics avec Volatility), la reconstruction temporelle d'événements et la forensique réseau (analyse PCAP, logs, threat hunting). L'ère post-quantique impose désormais de scanner les systèmes pour détecter l'usage de cryptographie PQC.

15 Benchmarking Global et Excellence

Une analyse comparative des pratiques mondiales (FBI/NIST, Scotland Yard, BKA, ANSSI, modèles asiatiques) montre que l'excellence forensique émerge de la capacité à adapter les méthodologies aux contextes locaux tout en respectant un socle de principes universels.

16 Cas Pratique Intégré : L'Affaire Cyberfinance

Le chapitre 24 illustre de manière concrète l'application de l'ensemble des concepts à une affaire fictive de ransomware au Cameroun en 2025. Il détaille les phases :

1. **Détection et réponse initiale.**

2. **Investigation technique** (analyse du malware, timeline).
3. **Collecte de preuves** avec application des standards ISO et considérations ZK-NR.
4. **Analyse approfondie** et attribution using MITRE ATT&CK.
5. **Remédiation** et renforcement avec migration PQC.
6. **Volet juridique** camerounais et préparation du dossier pour le tribunal.

Cette étude de cas synthétise les enseignements : la nécessité d'une **réponse structurée**, l'importance de **l'innovation technique** (face au quantique et à l'IA), et l'indispensable **respect du cadre légal et éthique**.

Conclusion

L'investigation numérique s'oriente vers une discipline **globale, interculturelle et interjuridictionnelle**. Son avenir sera façonné par sa capacité à :

1. **Intégrer l'éthique** au cœur de chaque action technique.
2. **Anticiper les ruptures technologiques**, notamment quantiques, par l'innovation (protocoles ZK-NR, architectures hybrides).
3. **S'adapter aux contextes locaux** tout en fostering la **coopération internationale**.
4. **Maintenir l'équilibre** du trilemme CRO dans la conception des systèmes futurs.

Le cadre CRO et les protocoles comme ZK-NR offrent une base solide pour construire une investigation numérique capable de relever les défis de l'ère post-quantique, où l'intégrité de l'investigateur reste la pierre angulaire face à la sophistication technique.