École Nationale Supérieure Polytechnique de Yaoundé

RESUME DU LIVRE
Théories et Pratiques de l'Investigation Numérique

Nom et Prenoms de l'etudiant : MELONE Andre Vladmir

Matricule : 22p059

Unité d'Enseignement : Introduction aux Techniques d'Investigation Numérique

Classe : Niveau 4

Filière : Cybersécurité et Investigation Numérique

Enseignant :
Monsieur MINKA MI NGUIDJOI Thierry Emmanuel

1 Introduction

Introduction

L'investigation numérique, encore appelée forensique numérique, désigne l'ensemble des méthodes scientifiques, techniques et juridiques permettant d'identifier, de collecter, de conserver, d'analyser et de présenter des preuves issues de supports ou environnements informatiques. Dans le contexte du Cameroun où la criminalité s'est largement déplacée vers le cyberespace avec par exemple des scammers, des harcelements en ligne par exemples, la question centrale demeure : comment garantir la fiabilité et la recevabilité des preuves numériques face à des menaces de plus en plus sophistiquées et à des environnements technologiques complexes ? Pour y répondre, ce document s'articule autour de plusieurs axes complémentaires : une présentation des fondements de l'investigation numérique et des normes internationales qui l'encadrent, une analyse des méthodologies pratiques utilisées par les experts, une mise en perspective du cadre juridique applicable, et enfin une ouverture sur des exemples concrets illustrant l'importance de cette discipline dans la lutte contre la cybercriminalité. .

2 Fondements Philosophiques et Historiques

2.1 Philosophie de l'Investigation Numérique

L'investigation numérique dépasse la technique et touche à la philosophie, interrogeant la vérité, la confiance et la justice à l'ère numérique. Elle repose sur des fondements mathématiques comme la théorie de l'information (entropie de Shannon), la théorie des graphes et la théorie du chaos.

2.2 Histoire de la Discipline

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

2.3 Grandes Affaires

— **BTK Killer (2005) :** Importance des métadonnées.
— **Stuxnet (2010) :** Première cyberarme.
— **WannaCry (2017) :** Pandémie numérique.

3 Cadre Théorique et Normes

3.1 Principes Théoriques

— **Principe de Locard numérique :** Toute action laisse une trace.
— **Modèles d'investigation :** DFRWS, Casey, ISO/IEC 27037.

3.2 Normes Internationales

— **ISO/IEC 27037 :** Guidelines pour l'identification, collecte et préservation des preuves.
— **NIST SP 800-86 :** Guide pour l'intégration des techniques forensiques.
— **RFC 3227 :** Ordre de volatilité (Farmer & Venema).
— **ACPO Good Practice Guide :** Quatre principes fondamentaux.

4 Méthodologies et Outils

4.1 Méthodologies d'Investigation

— **SANS FOR508 :** Six phases (Préparation, Identification, Containment, Eradication, Recovery, Lessons Learned).
— **CERT/CC :** Processus de réponse aux incidents.
— **ENISA :** Cadre forensique européen.
— **DFRC-K :** Modèle coréen adapté aux spécificités locales.

4.2 Outils et Techniques

— **Acquisition :** Outils d'imagerie (dd, FTK, EnCase).
— **Analyse mémoire :** Volatility Framework.
— **Anti-anti-forensique :** Techniques de contournement de chiffrement, détection de stéganographie.
— **IA en investigation :** Machine Learning pour classification de malware, Deep Learning pour analyse comportementale.

5 L'Ère Post-Quantique

5.1 Impact du Quantique

— **Algorithme de Shor :** Casse RSA et ECC.
— **Algorithme de Grover :** Réduction de la sécurité des clés symétriques.
— **Harvest Now, Decrypt Later :** Stratégie de stockage pour décryptage futur.

5.2 Cryptographie Post-Quantique (PQC)

— **Standards NIST :** CRYSTALS-Kyber (KEM), CRYSTALS-Dilithium (signatures).
— **Migration hybride :** Combinaison de crypto classique et PQC.

5.3 Quantum Forensics

Nouvelles opportunités : analyse de randomité quantique, tomographie d'état quantique pour preuves.

6 Le Trilemme CRO

6.1 Formalisation

Le **Trilemme CRO** établit une incompatibilité formelle entre :
— **Confidentialité (C) :** Protection des données.
— **Fiabilité (R) :** Intégrité et authenticité.
— **Opposabilité (O) :** Valeur probante légale.
Aucune primitive n'optimise simultanément les trois axes.

6.2 Analyse des Primitives

6.3 Architecture Q2CSI

Infrastructure à couches :
— **Iron Layer :** Fiabilité (intégrité temporelle).
— **Gold Layer :** Confidentialité (preuves zero-knowledge).
— **Clay Layer :** Opposabilité (ancrage institutionnel).

Primitive	C	R	O	Résistance Q
AES-256	0.95	0.90	0.30	Non
RSA-2048	0.85	0.90	0.95	Non
ECDSA	0.88	0.92	0.90	Non
Kyber-768	0.92	0.85	0.40	Oui
Dilithium-3	0.20	0.94	0.75	Oui

TABLE 1 – Scores CRO des primitives cryptographiques

7 Primitives Cryptographiques et Opposabilité

7.1 Protocole ZK-NR

Zero-Knowledge Non-Repudiation Protocol :

- Combine Merkle Commitments, STARK Proofs, Threshold BLS, Dilithium.
- Permet une non-répudiation préservant la vie privée.
- Sécurité UC (Universal Composability) prouvée.

7.2 Applications

- **Chaîne de possession post-quantique :** Transfert sécurisé de preuves.
- **Preuves vérifiables sans divulgation :** Préservation de la confidentialité.

8 Cadre Juridique

8.1 Droit International

- **États-Unis :** FRE Rule 901, SCA, CFAA.
- **Europe :** Règlement eIDAS, RGPD, Convention de Budapest.
- **Afrique :** Convention de Malabo, cadres régionaux (CEDEAO, SADC).

8.2 Droit Camerounais

- **Loi 2010/012 :** Cybersécurité et cybercriminalité.
- **Loi 2010/013 :** Communications électroniques.
- **Loi 2024/017 :** Protection des données personnelles.
- **Procédure :** Enquête préliminaire, expertise judiciaire, experts agréés.

9 Pratique du Forensique

9.1 Gestion de Laboratoire

- **Installation :** Matériel, logiciels (SIFT, REMnux), outils open source et commerciaux.
- **Procédures :** Checklists, modèles de rapports, scripts d'automatisation.
- **Accréditation :** Normes internationales, certification.

9.2 Forensique Système

- **Analyse de fichiers :** NTFS, EXT4, APFS (spécificités forensiques).
- **Artefacts :** Windows (Prefetch, Registre), Linux (logs, bash history), macOS (Spotlight, logs unifiés).
- **Mémoire :** Volatility 3, détection de menaces quantiques.
- **Timeline analysis :** Reconstruction temporelle multi-sources.

9.3 Forensique Réseau

- **Capture PCAP :** Architecture haute performance, validation d'intégrité.
- **Analyse de trafic :** DPI avec IA, détection de canaux cachés.
- **Protocoles chiffrés :** Analyse TLS, détection PQC.

9.4 Anti-Forensique

- **Techniques :** Effacement sécurisé, stéganographie, obfuscation.
- **Contremesures :** Détection, IA défensive, frameworks de résilience.

10 Conclusion

L'investigation numérique évolue vers une discipline globale, intégrant des aspects techniques, juridiques et éthiques. Le **Trilemme CRO** et les protocoles comme **ZK-NR** offrent un cadre pour naviguer les compromis entre confidentialité, fiabilité et opposabilité. La préparation à l'ère post-quantique est essentielle pour maintenir la confiance dans les preuves numériques.