MINYANDA YONGUI JOSE LOIC

22P071

CIN4

Résumé du cours : Théories et Pratiques de l'Investigation Numérique

Introduction

Ce résumé présente une synthèse structurée du manuel Théories et Pratiques de l'Investigation Numérique de Thierry Emmanuel Minka Mi Nguidjoi. Il met en évidence les fondements philosophiques et éthiques de la discipline, son évolution historique, ses modèles théoriques et normes internationales, ainsi que ses méthodes pratiques, outils et enjeux face à l'informatique post-quantique. Enfin, il illustre ces concepts par un cas pratique appliqué au Cameroun.

1. Fondements philosophiques et éthiques

L'investigation numérique n'est pas seulement un ensemble d'outils techniques : c'est une discipline qui engage la responsabilité de l'investigateur face à la société. L'ouvrage insiste sur la notion de philosophe-praticien, capable d'utiliser ses compétences dans le respect de principes éthiques.

Le Trilemme **CRO (Confidentialité, Fiabilité, Opposabilité)** structure la réflexion autour de la preuve numérique :

- **Confidentialité** : protéger les données sensibles, respecter la vie privée.
- **Fiabilité** : assurer la reproductibilité et l'intégrité des résultats.
- **Opposabilité** : garantir que les preuves résistent devant un tribunal.

Une charte déontologique formalise cet engagement, à travers dix commandements tels que : ne pas causer de dommages aux systèmes, documenter ses méthodes, protéger la chaîne de custody et témoigner avec honnêteté. Quatre piliers éthiques complètent cette charte : intégrité, proportionnalité, responsabilité et service.

Ainsi, la technique doit toujours être guidée par la sagesse et le sens du devoir, car l'investigation numérique impacte directement des vies humaines et des droits fondamentaux.

2. Historique et évolution de la discipline

La discipline a émergé dans les années 1970 avec les premiers litiges liés à l'informatique. Son évolution peut être découpée en grandes phases :

- **1970-1990** : Les prémices. Apparition des premiers cas judiciaires liés aux ordinateurs, comme l'affaire du groupe « 414s ».
- **1990-2000** : Professionnalisation. Création d'unités spécialisées, enquêtes emblématiques comme l'Operation Sundevil ou l'arrestation de Kevin Mitnick.
- **2000-2010** : Standardisation. Développement de cadres internationaux (ISO, NIST), avec des affaires marquantes comme Enron.
- **2010-2020** : Big data et Cloud. Émergence des cyberattaques massives (Silk Road, Panama Papers, WannaCry) qui nécessitent de nouvelles méthodes.
- **2020 à nos jours** : IA et post-quantique. Les attaques deviennent plus sophistiquées, comme SolarWinds, et posent la question de l'avenir de la cryptographie.

Ces étapes montrent que l'investigation numérique évolue constamment en fonction des menaces, des technologies et des besoins juridiques.

3. Cadre théorique et normes

3.1 Modèles théoriques

Plusieurs modèles structurent l'investigation numérique :

- **DFRWS (2001)** : définit les étapes de collecte, préservation, analyse et présentation.
- **Casey (2004)** : met l'accent sur le contexte judiciaire et l'admissibilité des preuves.
- **ISO/IEC 27037 (2012)** : norme internationale encadrant l'identification, la collecte et la préservation des preuves numériques.

3.2 Normes et standards internationaux

- **NIST SP 800-86 (USA)** : guide technique détaillé pour la gestion des enquêtes numériques.
- **RFC 3227** : introduit la notion d'« ordre de volatilité » pour prioriser la collecte.
- **ACPO Good Practice Guide (Royaume-Uni)** : énonce quatre principes garantissant l'intégrité des preuves.
- **Normes émergentes (Cloud Forensics, IoT Forensics)** : adaptées aux nouvelles infrastructures.

Ces cadres favorisent la coopération entre pays et assurent que les preuves recueillies soient reconnues au niveau international.

4. Méthodes, outils et anti-forensique

4.1 Méthodologies d'investigation

- **SANS FOR508** : méthodologie centrée sur la réponse aux incidents et la gestion de crise.
- **CERT/CC** : processus d'investigation en lien avec la cybersécurité opérationnelle.
- **ENISA Framework** : méthodologie européenne adaptée aux contextes réglementaires stricts.
- 4.2 Outils de l'investigateur moderne
- **Acquisition & imagerie :** duplication bit à bit des disques (FTK Imager, EnCase).
- **Analyse mémoire** : outils comme Volatility pour détecter des malwares en RAM.
- **Timeline analysis** : reconstitution des événements dans le temps (Plaso, Autopsy).
- **SIEM et logs** : systèmes centralisés pour analyser d'énormes volumes de données.
- **Intelligence artificielle** : machine learning pour classifier les malwares, deep learning pour analyser des comportements suspects.

4.3 L'anti-forensique et ses contremesures

Les criminels numériques utilisent des techniques d'anti-forensique :

- Effacement sécurisé des données.
- Obfuscation et chiffrement des fichiers.
- Stéganographie avancée.

Face à cela, l'investigateur déploie des techniques de contre-détection (déobfuscation, analyse comportementale, cryptanalyse forensique) et construit des frameworks de résilience capables d'anticiper et neutraliser ces stratégies.

5. Enjeux post-quantiques et cryptographie

L'arrivée des ordinateurs quantiques bouleverse l'investigation numérique. Les algorithmes de Shor et Grover rendent obsolètes RSA et ECC. Pour contrer ces menaces, le manuel met en avant la cryptographie post-quantique (Kyber pour l'échange de clés, Dilithium pour les signatures).

Le recours aux Zero-Knowledge Proofs permet de vérifier une information sans la divulguer, renforçant la protection de la vie privée et l'opposabilité des preuves.

Le Trilemme CRO prend ici toute son importance comme outil d'évaluation des compromis entre sécurité, confidentialité et valeur juridique. La chaîne de custody doit être renforcée avec des protocoles post-quantiques pour résister aux attaques futures.

6. Cadre juridique et cas pratique Cameroun 2025

6.1 Cadre juridique

- **États-Unis** : Federal Rules of Evidence, CFAA.
- **Europe** : RGPD, eIDAS, Convention de Budapest.
- **Afrique** : Convention de Malabo (2014).
- **Cameroun** : Lois de 2010 sur la cybersécurité et loi de 2024 renforçant l'investigation numérique.

Ces textes encadrent la collecte, la conservation et l'utilisation des preuves numériques devant les tribunaux.

6.2 Cas pratique : CyberFinance Cameroun 2025

Ce cas illustre les étapes d'une enquête réelle :

1. **Détection** : identification d'une attaque par ransomware affectant une infrastructure bancaire.
2. **Réponse initiale** : confinement des systèmes et préservation des preuves.
3. **Analyse technique** : étude du ransomware et des vecteurs d'infection.
4. **Collecte de preuves** : application de la norme ISO 27037 et du protocole ZK-NR.
5. **Timeline & attribution** : reconstruction des événements et identification probable des auteurs.
6. **Remédiation** : renforcement des défenses et mise en place de contre-mesures post-quantiques.
7. **Procédure judiciaire** : constitution d'un dossier recevable devant les tribunaux camerounais.

Ce cas montre l'importance de la transversalité : compétence technique, maîtrise juridique et gestion organisationnelle.

Conclusion

L’investigation numérique est devenue une discipline incontournable dans un monde dominé par le numérique. Elle se situe au croisement de la technique, de l’éthique et du droit.

À l’ère de l’intelligence artificielle et du post-quantique, l’investigateur doit :

- Maîtriser des compétences pluridisciplinaires.
- Respecter des principes éthiques stricts.
- Intégrer les nouvelles normes et cryptographies post-quantiques.
- Travailler en synergie avec les acteurs juridiques et institutionnels.

L’avenir de la discipline repose sur sa capacité à anticiper les mutations technologiques, à renforcer la confiance sociale et à garantir l’opposabilité des preuves numériques dans un monde globalisé.