Résumé de Cours

Théories et Pratiques de l'Investigation Numérique

MVONGO MEDJO Ordi Farel

Public : Étudiants en Cybersécurité et Investigation Numérique

16 Septembre 2025

Nombre de pages : 5

I - Fondements Philosophiques et Cadre Éthique

1. Une Discipline à la Croisée des Chemins

L'investigation numérique est présentée non comme une simple technique, mais comme une discipline philosophique à part entière. Elle interroge les fondements de la vérité, de la confiance et de la justice à l'ère du numérique. L'être humain possède désormais un **double numérique**, une extension de son identité physique qui échappe partiellement à son contrôle.

2. Le Paradoxe de l'Authenticité Invisible

Le manuel introduit un concept fondateur : il existe une tension fondamentale et mathématiquement formalisable entre :

— **L'Authenticité** (prouver qu'une preuve est vraie et intègre)
— **La Confidentialité** (ne pas révéler le contenu de la preuve)

Plus on cherche à prouver l'une, plus on tend à compromettre l'autre. Ce paradoxe est au cœur des défis de la preuve numérique moderne.

3. Le Contrat Déontologique : Le Serment de l'Investigateur

Avant toute chose, l'étudiant doit souscrire à un engagement moral solennel. Ce serment, inspiré du serment d'Hippocrate, repose sur quatre piliers :

— **Intégrité** : Véracité des conclusions et transparence des méthodes.
— **Proportionnalité** : Adéquation des moyens aux fins investigatrices.
— **Responsabilité** : Acceptation des conséquences de ses actions.
— **Service** : Mise des compétences au service de la justice et de la vérité.

La violation de ces engagements a des conséquences à la fois professionnelles (perte de crédibilité, sanctions juridiques) et morales.

4. Le Trilemme CRO : Le Cadre Théorique Fondamental

L'auteur propose une contribution majeure : le **Trilemme CRO**. Il formalise l'impossibilité d'optimiser simultanément trois axes cruciaux pour toute preuve numérique :

— **C**onfidentialité : Protection des données sensibles.
— **R**eliabilité (Fiabilité) : Intégrité et authenticité de la preuve.
— **O**pposabilité : Valeur probante et admissible en justice.

Toute construction cryptographique ou méthodologique devra faire des compromis entre ces trois pôles. Ce cadre sert de boussole pour évaluer les techniques et concevoir les systèmes de demain.

II - Évolution Historique et Cadre Technique

1. Brève Histoire de la Discipline

L'investigation numérique a évolué en plusieurs ères :

— **Les Prémices (1970-1990)** : Premiers cas (The Creeper, les "414s") et prise de conscience.
— **Professionnalisation (1990-2000)** : Opérations larges (Sundevil), arrestations médiatiques (Kevin Mitnick) et création des premiers standards.
— **Standardisation (2000-2010)** : Affaires fondatrices (Enron, Gary McKinnon) qui ont poussé à la création de méthodologies et normes (ISO, NIST).
— **Big Data & Cloud (2010-2020)** : Gestion de volumes massifs de données (Panama Papers, Silk Road) et développement d'outils d'analyse avancée.
— **Ère Post-Quantique & IA (2020-Aujourd'hui)** : Préparation à la menace quantique et intégration de l'Intelligence Artificielle dans l'analyse.

2. Les Modèles Méthodologiques

Plusieurs modèles structurent l'investigation :

— **DFRWS (2001)** : Identification, Préservation, Collection, Examination, Analysis, Presentation.
— **Casey (2004)** : Modèle intégré incluant préparation et révision.
— **ISO/IEC 27037 :2012** : Norme internationale pour l'identification, la collecte et la préservation des preuves.
— **NIST SP 800-86** : Guide pour l'intégration des techniques forensiques dans la réponse aux incidents.

3. L'Arsenal de l'Investigateur Moderne

L'analyse couvre une large gamme de techniques :

— **Acquisition & Imagerie** : Création de copies forensiques avec validation par hash (SHA-256).
— **Analyse de Mémoire (Volatility)** : Investigation de la mémoire vive pour détecter processus malveillants, connexions, etc.
— **Anti-Anti-Forensique** : Techniques pour contourner le chiffrement, détecter la stéganographie ou l'obfuscation.
— **Intelligence Artificielle** : Utilisation du Machine Learning pour classifier des logiciels malveillants et du Deep Learning pour l'analyse comportementale.

III - La Révolution Post-Quantique et le Protocole ZK-NR

1. La Menace Quantique

L'avènement de l'ordinateur quantique rend obsolètes les algorithmes cryptographiques actuels :

— **Algorithme de Shor** : Casse le RSA et l'ECC (cryptographie asymétrique).
— **Algorithme de Grover** : Réduit de moitié la sécurité des clés symétriques (ex : AES-128 n'offre plus que 64 bits de sécurité).

La stratégie **"Harvest Now, Decrypt Later"** (Collecter maintenant, déchiffrer plus tard) est une menace crédible : des adversaires stockent dès aujourd'hui des communications chiffrées pour les déchiffrer quand l'ordinateur quantique sera disponible.

2. La Cryptographie Post-Quantique (PQC)

Le NIST a sélectionné de nouveaux algorithmes résistants aux attaques quantiques :

— **CRYSTALS-Kyber** : Pour l'échange de clés (Key Encapsulation Mechanism).
— **CRYSTALS-Dilithium & FALCON** : Pour les signatures numériques.

La migration vers une **cryptographie hybride** (combinaison d'algorithmes classiques et PQC) est essentielle pour une transition en douceur.

3. Le Protocole ZK-NR : Une Solution Innovante

Pour résoudre le Paradoxe de l'Authenticité Invisible et répondre au Trilemme CRO, l'auteur propose le protocole **ZK-NR** (Zero-Knowledge Non-Repudiation). C'est une contribution majeure détaillée dans plusieurs articles (ePrint).

— **Fonction** : Il permet de prouver l'authenticité et l'intégrité d'une preuve (document, log, etc.) **sans en révéler le contenu**, garantissant ainsi la confidentialité.
— **Composants** : Il combine intelligemment plusieurs technologies :
  — **Preuves Zero-Knowledge (STARKs)** : Pour la vérification sans divulgation.
  — **Signatures à seuil (BLS)** : Pour la non-répudiation distribuée.
  — **Signatures post-quantiques (Dilithium)** : Pour la résistance future.
— **Application** : Il est parfait pour sécuriser la **chaîne de possession (Chain of Custody)** des preuves à l'ère quantique, en apportant une opposabilité juridique forte tout en préservant le secret de l'enquête.

IV - Analyse Cryptographique et Cadre Juridique

1. Analyse des Primitives selon le Trilemme CRO

Le manuel applique méthodiquement le cadre CRO pour évaluer et comparer les algorithmes cryptographiques. Ce tableau synthétique en est le résultat :

Primitive Cryptographique	Confidentialité (C)	Fiabilité (R)	Opposabilité (O)	Résistance
AES-256 (Symétrique)	0.95	0.90	0.30	No
RSA-2048 (Asymétrique)	0.85	0.90	0.95	No
ECDSA (Asymétrique)	0.88	0.92	0.90	No
CRYSTALS-Kyber (PQC - KEM)	0.92	0.85	0.40	**Ou**
CRYSTALS-Dilithium (PQC - Sig.)	0.20	0.94	0.75	**Ou**
zk-SNARKs (Preuves ZK)	0.98	0.75	0.40	No
Protocole ZK-NR (Hybride)	**0.85**	**0.90**	**0.88**	**Ou**

Conclusion : Aucune primitive n'est parfaite sur les 3 axes. Le choix doit être contextuel. Les architectures hybrides (comme ZK-NR) sont nécessaires pour approcher un optimum.

2. Cadre Juridique International et Camerounais

L'investigation s'inscrit dans un cadre légal strict :

— **Droit International** : Convention de Budapest (coopération), RGPD (protection des données, avec dérogations pour l'enquête).

— **Droit Américain** : Federal Rules of Evidence (FRE), Computer Fraud and Abuse Act (CFAA).

— **Droit Camerounais** : Régi principalement par la Loi N°2010/012 sur la cybersécurité et la cybercriminalité. Elle définit les procédures de perquisition, les infractions et les sanctions. L'expertise doit être réalisée par un **Expert Agréé** par le Ministère de la Justice.

V - Pratique Forensique et Conclusion Synthétique

1. Pratique Opérationnelle

Le manuel détaille la pratique avancée sur les différents systèmes :

— **Forensique Système (Windows/Linux/macOS)** : Analyse approfondie des artefacts (MFT, Prefetch, journals, logs unifiés) et de la mémoire (Volatility 3).
— **Forensique Réseau** : Analyse de trafic (PCAP), détection de canaux cachés, analyse des protocoles chiffrés (TLS) et threat hunting.
— **Gestion de Laboratoire** : Mise en place d'un lab, procédures opérationnelles standardisées (SOP), gestion de la chaîne de custody.

2. Étude de Cas Intégrée : L'Affaire CyberFinance Cameroun 2025

Un cas pratique complet illustre l'application de l'ensemble des concepts :

— **Scénario** : Attaque par ransomware contre une institution financière.
— **Déroulement** : Détection, réponse, investigation technique (analyse du malware, timeline), collecte de preuves avec application du protocole ZK-NR, attribution, remédiation et aspects juridiques camerounais.
— **Conclusion** : Le cas démontre l'importance d'une méthodologie structurée, de l'utilisation d'outils adaptés et de la préparation à la menace quantique.

3. Conclusion Synthétique et Perspectives

L'Investigation Numérique Moderne repose sur cinq piliers :

1. **Une Éthique Indispensable** : La puissance technique exige une déontologie forte et un sens aigu des responsabilités.
2. **Un Cadre Théorique Solide** : Le Trilemme CRO et le Paradoxe de l'Authenticité Invisible fournissent une boussole pour évaluer les technologies et prendre des décisions éclairées.
3. **Une Menace Imminente** : La transition vers le post-quantique n'est pas une option. Il faut dès aujourd'hui préparer la migration cryptographique et les méthodes d'investigation.
4. **Une Innovation Continue** : Les protocoles comme ZK-NR montrent la voie pour concilier confidentialité, fiabilité et opposabilité dans les preuves numériques futures.
5. **Une Pratique Rigoureuse** : Maîtriser les outils et les méthodologies forensiques sur tous les types de systèmes et de preuves (disque, mémoire, réseau) reste fondamental.

En résumé, ce manuel forme des "philosophes-praticiens" du numérique, capables non seulement de maîtriser les outils techniques, mais aussi de comprendre les enjeux profonds, éthiques et théoriques, de leur pratique, pour servir la justice à l'ère post-quantique.