UNIVERSITÉ DE YAOUNDÉ I
***
ÉCOLE NATIONALE SUPÉRIEURE
POLYTECHNIQUE DE YAOUNDÉ
***
DÉPARTEMENT DE GÉNIE
INFORMATIQUE
***
HUMANITÉS NUMÉRIQUES

THE UNIVERSITY OF YAOUNDE I
***
NATIONAL ADVANCED SCHOOL
OF ENGINEERING OF YAOUNDE
***
DEPARTMENT OF COMPUTER
ENGINEERING
***
DIGITAL HUMANITIES

Résumé du cours d'Investigations Numériques

Rédigé par :

FANTA YADON Félicité 22P069

Supervisé par :

M. Thierry MINKA

Bien Au-Delà de la Technique, l'investigation numérique n'est plus une simple discipline technique accessoire. Elle s'est muée en *philosophie pratique de la vérité à l'ère digitale.* Ce document fondateur ne se contente pas de dresser un inventaire d'outils ou de procédures ; il érige l'investigation en **savoir fondamental**, nécessaire pour naviguer les complexités d'un monde où notre existence est désormais **hybride, à la fois physique et numérique**.

Dans un univers saturé de données, où chaque clic laisse une empreinte, **l'investigation numérique devient l'art de rétablir la cohérence dans le chaos informationnel**. Elle exige une posture intellectuelle nouvelle, qui dépasse la simple technicité : celle d'un **gardien de l'intégrité numérique**, capable de distinguer l'authentique du fabriqué, le fait de l'opinion, le signal du bruit.

Le **postulat central** de cette œuvre est audacieux : face à une **crise sans précédent de la vérité numérique** marquée par les *deepfakes*, la *désinformation massive* et les *manipulations algorithmiques* à grande échelle **l'investigateur moderne doit assumer un triple rôle** :

- **Archéologue du digital**, pour exhumer les traces enfouies dans la masse de données et reconstituer le passé numérique avec rigueur ;
- **Épistémologue pratique**, pour évaluer de manière critique la fiabilité des sources, des algorithmes et des preuves numériques ;
- **Éthicien appliqué**, pour naviguer les dilemmes moraux engendrés par la collecte, l'analyse et l'exposition publique d'informations sensibles.

Ce livre n'est donc pas seulement un manuel : **c'est un manifeste**, une **boussole intellectuelle** destinée à guider celles et ceux qui choisissent de porter cette responsabilité immense.

Sa **thèse est révolutionnaire** : la **convergence simultanée de trois révolutions technologiques** ?le *Big Data*, l'*Intelligence Artificielle* et l'*informatique quantique* impose une **refonte radicale de nos méthodologies d'investigation**. Ces technologies bouleversent notre rapport au temps (accélération des flux), à la preuve (multiplication et falsifiabilité des traces), et à la certitude (incertitude probabiliste des modèles).

La réponse proposée est le **Framework CRO** (Confidentialité – Reliability – Opposabilité) et son **implémentation pratique, le protocole ZK-NR**, conçus pour résoudre un **trilemme longtemps considéré comme insoluble** : comment garantir **à la fois** la confidentialité des données, la fiabilité des résultats et l'opposabilité juridique des preuves numériques.

Là où les approches classiques échouent à concilier ces trois impératifs, le CRO introduit une **nouvelle grammaire de l'investigation**, fondée sur la traçabilité cryptographique, l'auditabilité continue et la vérifiabilité indépendante des analyses.

Cette œuvre ne propose pas simplement une méthode, mais **une vision** : faire de l'investigation numérique non plus un geste technique isolé, mais un **acte de vérité**, à la fois **scientifique, éthique et humaniste**, capable de soutenir la confiance dans un monde où tout peut être simulé, falsifié… ou effacé.

Le concept le plus **brillant et novateur** de cet ouvrage est la formalisation du **Trilemme CRO** (*Confidentiality – Reliability – Opposability*). Il démontre, à l'aide d'une **modélisation mathématique rigoureuse**, qu'il est **impossible de maximiser simultanément ces trois impératifs** pour toute preuve numérique : *tout système de preuve doit faire un compromis, qu'il soit explicite ou implicite.*

Les trois piliers du Trilemme sont définis ainsi :

- **Confidentialité (C)** : Capacité à *protéger la vie privée, les métadonnées sensibles et le contenu stratégique*, en restreignant l'accès aux seules parties autorisées.
- **Fiabilité (R)** : Capacité à *garantir l'intégrité, l'authenticité et la non-répudiation* des preuves numériques, en assurant leur traçabilité et leur résistance à la falsification.
- **Opposabilité (O)** : Capacité à *assurer la valeur probante, la recevabilité et l'admissibilité juridique* des preuves devant une autorité tierce (tribunal, auditeur, régulateur, etc.).

La tension fondamentale du Trilemme est que toute tentative d'optimiser l'un de ces axes entraîne une fragilisation des deux autres. Par exemple :

- Un système **très confidentiel** (chiffrement fort, cloisonnement extrême) produit des preuves difficilement **opposables**, car non vérifiables par des tiers.
- Un système **hautement fiable** et traçable génère une quantité importante de **métadonnées sensibles**, ce qui affaiblit la **confidentialité**.
- Un système **fortement opposable** doit exposer des preuves dans un format lisible et vérifiable, ce qui peut compromettre à la fois leur **confidentialité** et leur **intégrité**.

De ce dilemme émerge le **Paradoxe de l'Authenticité Invisible** :

> « *Plus une preuve est authentique et vérifiable, plus elle tend à révéler d'informations compromettant la confidentialité. Inversement, plus une preuve préserve la confidentialité, plus son authenticité devient difficile à établir.* »

Ce paradoxe illustre une **contradiction structurelle au cœur de l'investigation numérique moderne** : le besoin simultané de **prouver sans exposer**, de **convaincre sans divulguer**, et de **valider sans révéler**.

La solution pratique proposée à ce paradoxe est l'émergence des **protocoles ZK-NR** (*Zero-Knowledge Non-Repudiation*), directement inspirés des **preuves à divulgation nulle de connaissance (ZKP)**.

Ces protocoles permettent à un investigateur de :

- **Prouver l'authenticité d'une information** (son existence, sa date, son intégrité, sa provenance),
- **Sans jamais révéler le contenu de cette information** à un tiers vérificateur.

En d'autres termes, ils **transforment la preuve d'un objet à examiner en un processus à vérifier** : ce n'est plus la donnée qui est soumise à examen, mais un **engagement cryptographique** et un **protocole de vérification publique** qui attestent de sa validité sans l'exposer.

Cette approche constitue une **avancée conceptuelle majeure** : elle permet de **réconcilier partiellement les trois axes du Trilemme CRO** et d'**élever le niveau de confiance dans l'investigation numérique**, même dans des environnements hostiles ou juridiquement sensibles.

En somme, le ZK-NR incarne un **changement de paradigme** : passer d'une logique de *preuve exposée* à une logique de *preuve démontrée*, où l'investigateur n'est plus un simple collecteur de données, mais un **architecte de la confiance numérique**.

L'ouvrage se distingue par son **approche résolument globale et contextuelle**. Plutôt que de proposer un modèle unique, il met en lumière une **mosaïque de pratiques forensiques** adaptées aux réalités **juridiques, culturelles et technologiques** propres à chaque région du monde.
Cette démarche repose sur une série de **cas d'usage emblématiques** qui illustrent la diversité des contextes d'application et les défis spécifiques que doit relever l'investigation numérique contemporaine :

Cette **« mosaïque forensique »** démontre que :

- L'**excellence forensique n'a pas de modèle unique**,
- La **coopération internationale** et l'**adaptabilité contextuelle** sont les véritables clés de la réussite.

Dans cette perspective, le **framework CRO** agit comme un **langage universel d'évaluation et d'harmonisation**, permettant de **relier des pratiques hétérogènes autour de principes communs**, tout en respectant la diversité des environnements où se déploie l'investigation numérique.

La **menace quantique n'est pas de la science-fiction**. Les algorithmes de rendront obsolètes la majorité des cryptosystèmes classiques

Pire encore, la stratégie dite *« Harvest Now, Decrypt Later »* signifie que **des adversaires stockent déjà des données chiffrées aujourd'hui dans l'espoir de les déchiffrer demain** à l'aide d'ordinateurs quantiques matures.

Face à ce danger, l'ouvrage **sonne l'alarme** et propose un **plan de migration concret vers la cryptographie post-quantique (PQC)**.

Il introduit également une **architecture de sécurité novatrice**, appelée **Q2CSI (Quantum Composable Contextual Security Infrastructure)**, qui **sépare dialectiquement les préoccupations en trois couches indépendantes** :

- **Couche IRON** : Fiabilité et intégrité temporelle des preuves.
- **Couche GOLD** : Confidentialité et préservation sémantique des données.
- **Couche CLAY** : Opposabilité et ancrage institutionnel des résultats.

Cet ouvrage dépasse le cadre d'un simple manuel technique : **c'est un véritable traité de philosophie appliquée pour le XXI^{e} siècle numérique.**

Une Vision Prospective : Une préparation indispensable à l'avènement de l'ordinateur quantique et à ses implications disruptives sur les chaînes de confiance numériques.

Un Langage Universel : Le **framework CRO** et les **protocoles ZK-NR**, permettant d'évaluer, de concevoir et de communiquer sur la sécurité et la fiabilité des preuves digitales.

L'ère numérique dans laquelle nous sommes entrés n'est plus une simple mutation technologique ; elle constitue une transformation ontologique de notre rapport au monde, aux autres et à nous-mêmes. L'information est devenue la matière première de nos sociétés, et sa manipulation, son interprétation et sa conservation façonnent désormais le réel aussi puissamment que l'acier ou le pétrole en d'autres temps. C'est dans ce contexte qu'émerge la nécessité impérieuse d'une discipline nouvelle, plus large que la technique, plus rigoureuse que l'opinion : **l'investigation numérique comme philosophie appliquée de la vérité**.

Cet ouvrage a démontré que l'investigation numérique ne saurait être réduite à un ensemble d'outils, de procédures ou de protocoles figés. Elle constitue une **démarche intellectuelle et éthique**, qui exige

de l'investigateur qu'il soit à la fois **archéologue du digital** capable d'exhumer les traces enfouies dans l'immensité des données , **épistémologue pratique** apte à évaluer avec méthode la fiabilité de ce qu'il observe et **éthicien appliqué** conscient des dilemmes moraux que soulève toute recherche de la vérité. À travers ces trois figures, l'investigation numérique devient un art de discerner le vrai sans trahir le juste, et de produire des certitudes tout en respectant les droits fondamentaux.

Mais cette quête se heurte à un défi central : le **trilemme CRO (Confidentialité, Fiabilité, Opposabilité)**. Cet ouvrage en a proposé une formalisation inédite, démontrant qu'il est impossible de maximiser simultanément ces trois impératifs, et qu'un équilibre doit être recherché en conscience. C'est là qu'interviennent les **protocoles ZK-NR**, inspirés des preuves à divulgation nulle de connaissance, qui permettent de prouver l'authenticité d'une information sans en révéler le contenu. Cette avancée conceptuelle transforme la preuve, d'un objet passif à examiner, en un **processus dynamique à vérifier** une révolution silencieuse, mais décisive, dans l'histoire de la justice numérique.

L'ouvrage a également souligné que l'excellence forensique n'est jamais universelle : elle est toujours **contextuelle et située**, enracinée dans les cultures juridiques, les infrastructures techniques et les dynamiques sociales propres à chaque région du monde. Des enquêtes menées dans la *Silicon Valley* aux cyberattaques sur les réseaux énergétiques en *Europe*, des manipulations électorales en *Inde* aux fraudes mobiles en *Afrique de l'Ouest*, les cas étudiés ont montré que la coopération internationale et l'adaptabilité contextuelle sont les conditions mêmes de la réussite. Le **framework CRO** s'impose ici comme un langage universel, permettant d'harmoniser des pratiques hétérogènes sans les uniformiser.

Enfin, cet ouvrage a tiré la sonnette d'alarme sur une menace émergente : **la cryptographie post-quantique**. Les algorithmes de Shor et de Grover promettent de rendre obsolètes la plupart des cryptosystèmes actuels d'ici 2035, et la stratégie Harvest Now, Decrypt Later menace déjà la confidentialité des données sensibles. En réponse, une **architecture Q2CSI** a été proposée, structurant la sécurité numérique en trois couches dialectiques (IRON, GOLD, CLAY), afin d'anticiper et d'absorber le choc quantique à venir.

En définitive, ce livre n'est pas seulement un manuel technique ni même un traité de cybersécurité avancée. Il est **un manifeste pour une gouvernance éthique de la vérité numérique**. Il appelle à former une nouvelle génération de professionnels : des **gardiens de l'intégrité informationnelle**, capables de conjuguer rigueur scientifique, discernement moral et responsabilité citoyenne. Car dans un monde où la frontière entre le réel et le digital s'estompe chaque jour davantage, préserver la vérité devient un acte de justice et la justice, un acte de lucidité.