REPUBLIQUED UCA MEROUN
***** *****
PAIX-TRAVAIL-PATRIE
***** *****
MINISTRED E
L'ENSEIGNEMENTS UPERIEUR
***** *****
UNIVERSITED EY AOUNDE1
***** *****
ECOLEN ATIONALE
SUPERIEURE
POLYTECHNIQUE
***** *****
DEPARTEMENTD EG ENIE
INFORMATIQUE

REPUBLIC OFCA MEROON
***** *****
PEACE–WORK-FATHERLAND
***** *****
MINISTRYO F
HIGHER EDUCATION
***** *****
UNIVERSITYO FY AOUNDEI
***** *****
NATIONAL
ADVANCEDS CHOOLO F
ENGINEERING
***** *****
COMPUTER ENGINEERING
DEPARTMENT

INVESTIGATION NUMERIQUE

PROJET SOUS LE THEME

RESUME DU COURS D'INVESTIGATION NUMERIQUE

MATRICULE	NOMS & PRÉNOMS	FILIERE
22P056	NNA FRANCIS EMMANUEL ROMEO	CIN-4

Sous la supervision de :

MINKA THIERRY

INTRODUCTIONG ENERALE

Ce manuel présente les fondements de l'investigation numérique, en soulignant une forte emphase sur l'**éthique** et la **responsabilité** de l'investigateur, incarnées par les "Dix Commandements" et les "Quatre Piliers de la Pratique Éthique". Il parcourt l'**histoire de la discipline** à travers des affaires marquantes et expose les **cadres théoriques et méthodologiques** reconnus internationalement, comme le Principe de Locard Numérique et les modèles DFRWS ou SANS. Une section significative est dédiée à l'**impact de la révolution quantique**, introduisant le **Trilemme CRO (Confidentialité, Fiabilité, Opposabilité)** et le **Protocole ZK-NR (Zero-Knowledge Non-Repudiation)** comme solutionsi nnovantespour garantirl 'intégritédes preuves dans ce nouveau paradigme. Enfin, l'ouvrage aborde les **aspects juridiques mondiaux et camerounais**, ainsi que des **pratiques opérationnelles avancées** pour la gestion d'un laboratoire forensique etl a lutte contre l'anti-forensique.

[U-RESUME]

[U-FORZ] **L'investigation numérique éthique** est une discipline philosophique qui dépasse la technique : l'investigateur est à la fois **archéologue digital, épistémologue et éthicien**. Elle repose sur des engagements fondamentaux (légalité, intégrité, confidentialité, traçabilité), quatre piliers (intégrité, proportionnalité, responsabilité, service), et dix commandements (respect de la vie privée, préservation des preuves, honnêteté, etc.).

À l'ère **post-quantique**, de nouveaux impératifs apparaissent : produire des preuves résistantes aux attaques quantiques, anticiper l'avenir, préserver l'oubli, et résoudre le **Trilemme CRO** (confidentialité, fiabilité, opposabilité). Les protocoles **ZK-NR** offrent un équilibre pratique.

En somme, l'investigation numérique est une **praxis de liberté** qui protège la justice et la confiance sociale, guidée par la devise : « La technique s'apprend, maisl 'éthique se cultive. »

- **La cryptographie post-quantique (PQC)** vise à protéger les systèmes contre les futurs ordinateurs quantiques capables de briser RSA, ECC et autres algorithmes classiques (via Shor et Grover). Le NIST a standardisé en 2022 de nouveaux algorithmes comme **CRYSTALS-Dilithium, FALCON, SPHINCS+**(signatures)et **CRYSTALS-Kyber**(KEM).

Pourl '**investigation numérique**, cela impose :

- d'adopterdes s ignatureset hor odatagespos t-quantiques,
- d'utiliserdes ar chitectureshybr ides(classiques+ PQ C),
- d'assurer la confidentialité, la fiabilité et l'opposabilité (Trilemme CRO),
- de recourir à des protocoles comme ZK-NR et à des outils comme OpenQuantumSafe.

En bref, la PQC est une **révolution** qui redéfinit la cybersécurité, la validité des preuves et la chaîne de possession, nécessitant une adaptation technique, éthique etj uridique.

- **Le Trilemme CRO (Confidentialité, Fiabilité, Opposabilité)** montre qu'il est impossible d'optimiser simultanément ces trois propriétés d'une preuve numérique, surtout à l'ère post-quantique. Chaque primitive cryptographique doit donc être évaluée selon ces axes (ex. RSA fort en opposabilité mais vulnérable à Shor, Kyber résistant au quantique mais faible en opposabilité).

Pour y répondre, on recommande des **architectures hybrides** (classiques + post-quantiques) et des protocoles avancés comme **ZK-NR**, intégrés dans des cadres tels que **Q2CSI**, afin d'équilibrer sécurité future, validité juridique etpr otection desdonnées .

En somme, le Trilemme CRO est une **boussole théorique et pratique** guidant la conception et l'éthique de l'investigation numérique face aux défisquant iques.

- **Les preuves numériques inviolables** doivent garantir intégrité, authenticité et résistance aux altérations, notamment face aux menacespos t-quantiques. Leurpr otection repose sur:
- **Intégrité & Authenticité** :as suréespar l a chaînede conf iance et la chaîne de custody documentée.
- **Éthique de l'investigateur** : préserver l'intégrité des données et anticiperl esm enacesquant iques.
- **Cryptographie post-quantique (PQC)** : signatures comme **CRYSTALS-Dilithium**pour s écuriserl espr euvesà l ong terme.
- **Protocoles ZK-NR** : vérification sans divulgation, garantissant confidentialité, fiabilité etnon- répudiation.
- **Architecture Q2CSI** : couches de sécurité, notamment l'**Iron Layer**dédi ée à l'intégrité temporelle.
- **Lutte anti-forensique** : détection et contremesures contre la destruction, dissimulation ou falsification de données.

L'inviolabilité est donc une combinaison de **méthodes techniques, éthiqueset j uridiques**, adaptée à l'ère post-quantique.

- **L'investigation numérique mondiale** est structurée par des **cadres normatifs** (DFRWS, Casey, ISO/IEC 27037-27043, NIST SP 800-86, RFC 3227, ACPO) qui fournissent une base commune.

Chaque région développe sess pécificités:

- **États-Unis** : excellence technique (NIST, FBI, EEA), forte innovation.
- **Royaume-Uni** : rigueur procédurale (ACPO), blockchain & quantums ealing.

- **Allemagne** : validation scientifique stricte, métrologie et reproductibilité.
- **Singapour & Corée du Sud** : IoT urbain, IA, blockchain, métavers, communication quantique.
- **France**: s ouveraineté numérique, ANSSI, droiteur opéen.
- **Japon**: K aizen appliqué, miniaturisation, edge forensics.
- **Afrique de l'Ouest (CEDEAO)** : approche mobile-first, lutte contre la fraude transfrontalière, contraintesd' infrastructure.

Le **Trilemme CRO (Confidentialité, Fiabilité, Opposabilité)**, proposé par Minka et al., sert de **langage universel** pour évaluer les compromis des approches forensiques et orienter la transition post-quantique.

En **ère post-quantique**, less olutionscom binent:

- **Cryptographie PQC** (Dilithium, Kyber) pour protéger les preuves.
- **Protocoles ZK-NR** pour garantir non-répudiation et confidentialité.
- **Architecture Q2CSI** (Iron, Gold, Clay Layers) pour composer la sécurité.
- **IA & XAI** pour détection d'anomalies, lutte anti-forensique et justification judiciaire.

L'ensemble forme une **mosaïque forensique mondiale**, où le Trilemme CRO agit comme boussole pour concilier innovations technologiques, exigencesj uridiqueset cont extesl ocaux.

CONCLUSION

L'excellence en investigation numérique mondiale émerge de la capacité à transcender les approches monolithiques, à intégrer les spécificités culturelles et légales, à innover dans l'adaptation méthodologique, à collaborer efficacement au-delà des frontières et à anticiper les évolutions géopolitiques et technologiques. Le Trilemme CRO et les protocoles ZK-NR sont des fondations solides pour cette transition complexe vers une investigation numérique post-quantique et éthique, assurant que la vérité et la justice peuvent être établies même face aux défisl espl usavancés