ECOLE NATIONALE SUPERIEURE POLYTECHNIQUE DE YAOUNDE
DEPARTEMENT DES ARTS ET HUMANITES NUMERIQUES

RESUME DU COURS D'INTRODUCTION À L'INVESTIGATION NUMÉRIQUE

Présenté par :
GHOUMO DONFACK
Olivia Shelsie
Classe : CIN 04
Matricule : 22p023
Professeur : M. Thierry MINKA

Année universitaire 2025-2026

1. Introduction et Philosophie de l'Investigation Numérique

1.1 Contexte et Enjeux

— L'investigation numérique est une discipline **philosophique, technique et juridique**.

— Elle interroge la nature de la **vérité**, de la **confiance** et de la **justice** à l'ère numérique.

— **Problématique** : Comment concilier **confidentialité**, **fiabilité** et **opposabilité juridique** des preuves numériques dans un contexte **post-quantique** ?

1.2 Le Paradoxe de l'Authenticité Invisible

— Plus une preuve est authentique et vérifiable, plus elle risque de compromettre la confidentialité (et inversement).

$$\Delta A \cdot \Delta C \geq h_{num}$$

  — ΔA : Incertitude sur l'authenticité.
  — ΔC : Incertitude sur la confidentialité.
  — h_{num} : Constante numérique fondamentale.

1.3 Le Trilemme CRO

— **C**onfidentialité : Protection des données sensibles.

— **R**eliabilité (Fiabilité) : Intégrité et authenticité des preuves.

— **O**pposabilité juridique : Valeur probante en justice.

— Il est théoriquement impossible de maximiser ces trois points.

1.4 Éthique et Responsabilité

— **Serment de l'Investigateur Numérique** :
  — Utiliser les connaissances exclusivement à des fins légitimes.
  — Respecter les cadres juridiques nationaux et internationaux.
  — Protéger la confidentialité et l'**intégrité des systèmes**.
  — Documenter intégralement les méthodologies.

— **Quatre piliers déontologiques** :
  1. **Intégrité** (véracité, transparence).
  2. **Proportionalité** (adéquation des moyens).
  3. **Responsabilité** (devoir de vigilance).
  4. **Service** (mettre les compétences au service de la justice).

2. Cadre Théorique et Conceptuel

2.1 Fondements Théoriques

— **Théorie de l'Information (Shannon)** :
  — **Entropie** pour détecter des anomalies.
  — **Distance de Hamming** pour analyser la similarité entre fichiers.

— **Théorie des Graphes** :
  — Modélisation des **réseaux sociaux** et des **flux de données**.
  — Détection de **communautés cachées** et de **chemins de fuite**.
— **Théorie du Chaos** :
  — Sensibilité aux **conditions initiales**.

2.2 Modèles d'Investigation

Table 1 – Comparaison des Modèles d'Investigation

Modèle	Phases Clés	Application Typique
DFRWS (2001)	Identification → Préservation → Collecte → Examen → Analyse → Présentation	Standard académique et opérationnel.
Casey (2004)	Préparation → Déploiement → Scène physique → Scène numérique → Révision	Enquêtes criminelles complexes.
ISO/IEC 27037	Identification → Collecte → Préservation → Documentation	Norme internationale pour la collecte.
NIST SP 800-86	Collection → Examen → Analyse → Rapport	Intégration à la réponse aux incidents.

2.3 Normes et Standards Internationaux

— **ISO/IEC 27037** : Lignes directrices pour l'identification, la collecte et la préservation des preuves numériques.
— **NIST SP 800-86** : Intégration des techniques forensiques à la réponse aux incidents.
— **RFC 3227** : Ordre de volatilité (Farmer & Venema) pour la collecte des preuves.
— **ACPO (Royaume-Uni)** : 4 principes clés (pas de modification des données, compétence requise, audit trail, responsabilité).

3. L'Ère Post-Quantique et ses Défis

3.1 Menaces Quantiques

Table 2 – Impact des Algorithmes Quantiques sur la Cryptographie Classique

Algorithme Quantique	**Impact sur la Cryptographie Classique**	**Conséquences pour l'Investigation**
Shor	Cassage de RSA et ECC en temps polynomial.	Preuves historiques compromises.
Grover	Réduction de moitié de la sécurité des clés symétriques.	Attaques "Harvest Now, Decrypt Later".

3.2 Cryptographie Post-Quantique (PQC)

— **Algorithmes sélectionnés par le NIST (2022)** :
  — **Signatures** : CRYSTALS-Dilithium (basé sur les réseaux), SPHINCS+ (hash-based).
  — **Chiffrement** : CRYSTALS-Kyber (KEM basé sur LWE).
— **Migration progressive** :
  — **Court terme** : Hybridation (RSA + Kyber).
  — **Long terme** : Remplacement complet par PQC.

3.3 Quantum Forensics

— Analyse de nombres aléatoires quantiques (QRNG vs PRNG).
— Tomographie d'état quantique pour valider l'intégrité des preuves.
— Protocoles ZK-NR pour une non-répudiation post-quantique.

4. Le Protocole ZK-NR : Innovation Majeure

4.1 Architecture du Protocole

— **Couches** :
  1. **Merkle Commitments** : Structure d'engagement pour l'intégrité.
  2. **STARK Proofs** : Preuves zero-knowledge post-quantiques et transparentes.
  3. **Threshold BLS** : Signatures distribuées pour la résilience.
  4. **Dilithium** : Authentication post-quantique.
— **Flux** :
  — Engagement → Preuve ZK → Signature à seuil → Authentification PQC.

4.2 Sécurité UC (Universal Composability)

— **Modèle de sécurité** :
  — Non-répudiation.
  — Zero-Knowledge (aucune information révélée).
  — Résistance quantique.
— **Preuve formelle** (via Tamarin Prover) :
  — Vérification des propriétés de confidentialité, intégrité et authenticité.

4.3 Applications Pratiques

— **Chaîne de custody post-quantique** :
  — Horodatage quantique + signatures ZK-NR pour une traçabilité inviolable.
— **Preuves judiciaires** :
  — Opposabilité garantie même dans un contexte quantique.

5. Techniques d'Anti-Anti-Forensique

— **Contournement de chiffrement** :
  — Cold Boot Attack (récupération de clés en RAM refroidie).
  — Evil Maid Attack (installation de keyloggers hardware).
— **Détection de stéganographie** :
  — Analyse statistique (entropie, chi-square).
  — Machine Learning pour identifier les patterns cachés.
— **Déobfuscation de code** :
  — Analyse dynamique (sandboxing).
  — Symbolic Execution pour comprendre les logiques obscurcies.

6. Cadre Juridique et Applications Pratiques

6.1 Législation Mondiale

TABLE 3 – Cadre Juridique par Région

Région	**Cadre Juridique Clé**
États-Unis	FRE (Federal Rules of Evidence), CFAA (Computer Fraud and Abuse Act).
Europe	eIDAS (signatures électroniques), RGPD (protection des données), Convention de Buda
Afrique	Convention de Malabo (cybercriminalité), Loi camerounaise 2010/012.
Cameroun	Loi 2010/012 (cybersécurité), Loi 2024/017 (protection des données).

6.2 Procédure d'Investigation au Cameroun

1. Plainte/Signalement.
2. Enquête préliminaire.
3. Commission rogatoire.
4. Expertise judiciaire.
5. Rapport d'expertise.
6. Audience.

6.3 Cas Pratique : Affaire CyberFinance Cameroun 2025

— **Scénario** :
  — Attaque ransomware (LockBit 3.0) sur une fintech camerounaise.
  — Exfiltration de 850 GB de données clients.
  — Demande de rançon : 10M EUR en Bitcoin.
— **Réponse** :
  — Isolation du réseau → Acquisition forensique (ISO 27037) → Analyse ZK-NR.
  — Attribution : Groupe LockBit affiliate "GoldManager" (Europe de l'Est).
  — Remédiation : Migration vers CRYSTALS-Kyber et Dilithium, déploiement du framework Q2CSI.

7. Benchmarking Mondial et Best Practices

7.1 Comparaison des Approches

Table 4 – Benchmarking des Agences Forensiques Mondiales

Agence	Forces	Faiblesses
FBI/NIST	Innovation technologique, normalisation.	Complexité juridique.
Scotland Yard	Rigueur procédurale, coopération internationale.	Lenteur administrative.
BKA (Allemagne)	Précision technique, validation métrologique.	Manque de flexibilité.
Singapour	Technologie de pointe, IA et IoT.	Coût élevé.
France (ANSSI)	Souveraineté numérique, cadre juridique solide.	Adoption lente des innovation

7.2 Framework d'Excellence Universelle

— **Hybridation des meilleures pratiques** :
  — Innovation américaine (FBI/NIST) + rigueur allemande (BKA) + adaptabilité africaine.

— **Recommandations stratégiques** :
  1. Former les investigateurs aux protocoles ZK-NR et Q2CSI.
  2. Migrer vers PQC (Kyber, Dilithium) d'ici 2030.
  3. Automatiser la chaîne de custody avec des preuves cryptographiques.
  4. Renforcer la coopération internationale (Convention de Budapest, MLAT).

8. Synthèse et Perspectives

8.1 Leçons Clés

1. Le Trilemme CRO est inévitable : Aucune solution ne maximise simultanément confidentialité, fiabilité et opposabilité.
2. Les protocoles ZK-NR et Q2CSI offrent un équilibre optimal pour l'ère post-quantique.
3. L'investigation numérique moderne doit intégrer :
   — Cryptographie post-quantique.
   — Intelligence artificielle (détection d'anomalies, attribution).
   — Cadre juridique adaptatif.

8.2 Roadmap pour l'Afrique

Table 5 – Roadmap pour l'Afrique

Horizon	Actions Clés
2025-2027	Formation aux protocoles ZK-NR, déploiement de laboratoires forensiques.
2027-2030	Migration vers PQC (Kyber, Dilithium), adoption du framework Q2CSI.
2030+	Leadership mondial en investigation post-quantique (leapfrogging).

> « L'investigation numérique n'est pas qu'une discipline technique, mais une **praxis de liberté** : elle protège la vérité dans un monde où le numérique redéfinit constamment les frontières du réel. » — **MalEtYOn**