RÉPUBLIQUE DU CAMEROUN
Paix – Travail – Patrie
*****
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR
*****
UNIVERSITÉ DE YAOUNDÉ I
*****
ÉCOLE NATIONALE SUPÉRIEURE POLYTECHNIQUE
*****
DÉPARTEMENT DE GÉNIE INFORMATIQUE
*****

REPUBLIC OF CAMEROON
Peace – Work – Fatherland
*****
MINISTRY OF HIGHER EDUCATION
*****
UNIVERSITY OF YAOUNDE I
*****
NATIONAL ADVANCED SCHOOL OF ENGINEERING
*****
COMPUTER ENGINEERING DEPARTMENT
*****

INTRODUCTION AUX TECHNIQUES D'INVESTIGATION NUMÉRIQUE

RESUME DE COURS

Rédigé par
NZOUCK TOUMPE ERIC - OLIVIER
Matricule : ***22P060***

Sous la supervision de
Thierry MINKA, Eng

Année académique 2025/2026

L'investigation numérique ne saurait être réduite à un catalogue de techniques ou à une panoplie d'outils. Elle se définit d'abord comme une **philosophie appliquée du numérique**, c'est-à-dire une réflexion globale sur la manière dont la vérité peut être établie dans un monde où la donnée joue un double rôle : instrument de transparence et vecteur d'opacité.

À travers cette approche, la discipline dépasse largement la dimension strictement opérationnelle pour embrasser une interrogation épistémologique et ontologique. Elle pose une question essentielle :

Comment dire la vérité à partir des traces numériques, alors même que celles-ci peuvent être manipulées, altérées ou dissimulées ?

Les dimensions de la réflexion Cette réflexion se décline en plusieurs dimensions complémentaires :

- **Épistémologique :** l'être humain ne se réduit plus à sa matérialité physique. Il projette une partie de son identité dans le cyberespace, par le biais de ses interactions, communications et empreintes digitales.
- **Ontologique :** le « double numérique » constitue une véritable extension de l'être. Ces représentations, bien que virtuelles, possèdent une valeur existentielle équivalente à sa présence matérielle.
- **Phénoménologique :** les données numériques apparaissent comme des manifestations d'existence, comparables à des objets matériels ou à des témoignages humains.
- **Métaphysique :** le numérique ouvre de nouveaux modes d'existence, de relation et de temporalité. Les traces prolongent la mémoire, défient l'oubli et recomposent la condition humaine.

De cette philosophie découle un paradoxe central : **plus une donnée est rendue transparente et vérifiable, plus elle menace l'intimité individuelle**. L'investigateur doit naviguer entre deux impératifs : l'exigence de vérité et la protection des droits fondamentaux. L'investigation numérique s'appuie sur des piliers théoriques solides empruntés aux sciences fondamentales :

- **Théorie de l'information (Claude Shannon)** : quantification de l'incertitude, détection des anomalies via l'entropie, mesure de la redondance et de l'imprévisibilité.
- **Théorie des graphes** : cartographie des relations sociales, techniques et financières. Elle met en évidence les nœuds et flux cachés, essentiels pour démanteler des réseaux criminels.
- **Théorie du chaos** : dans des systèmes complexes, une variation minime peut engendrer des effets considérables. Cela impose une extrême rigueur méthodologique.

La révolution quantique a introduit une rupture épistémologique majeure. Les concepts de superposition, d'intrication ou de non-localité bouleversent les critères classiques d'authenticité.

D'où l'émergence du paradoxe de l'**authenticité invisible** : vérifier une preuve, c'est risquer d'altérer sa confidentialité.

Les **Zero-Knowledge Proofs** (preuves à divulgation nulle de connaissance) offrent une réponse élégante : démontrer la validité d'une information sans révéler l'information elle-même.

Ainsi, l'investigation numérique apparaît comme une **épistémologie appliquée doublée d'une archéologie digitale**, où l'investigateur devient un médiateur entre traces dispersées et reconstruction de la vérité.

L'éthique constitue la colonne vertébrale de la discipline. L'investigateur est non seulement un technicien, mais aussi un **gardien de la confiance sociale**. Les principes ACPO sont :

1. Ne jamais modifier les données originales.
2. Si une intervention est nécessaire, elle doit être réalisée par un expert qualifié.
3. Documenter intégralement chaque action, afin d'assurer la traçabilité.
4. Garantir, par la supervision, que le processus respecte ces principes.

À l'échelle mondiale, plusieurs standards encadrent la pratique :

- **ISO/IEC 27037** : protocole rigoureux de saisie (identification, documentation photographique, isolation, write-blocker, hachage SHA-256, scellement et transport).
- **RFC 3227** : ordre de volatilité, priorité aux données éphémères (registres, mémoire vive) avant les persistantes.
- **NIST SP 800-86** : étapes de la réponse aux incidents et intégration dans la gestion de crise.

Ce cadre normatif vise à garantir la **confidentialité, la fiabilité et l'opposabilité juridique** des preuves. Ces trois axes sont synthétisés dans le **Trilemme CRO**, véritable boussole théorique de la discipline.

L'investigation numérique s'appuie sur des méthodologies internationales éprouvées :

- **SANS FOR508** : approche en six phases (préparation, identification, confinement, éradication, récupération, leçons tirées).
- **Processus CERT/CC** : gestion structurée des incidents et coordination.
- **ENISA Forensic Framework** : méthodologie européenne axée sur la coopération transfrontalière.
- **Modèle de Casey** : approche pédagogique en phases successives.
- **Analyse formelle** : outils comme Tamarin Prover pour valider la robustesse des protocoles.
- **Supports numériques** : FTK, EnCase, Cellebrite, Magnet AXIOM.
- **Analyse réseau** : Wireshark, Zeek.
- **Mémoire vive** : Volatility 3.
- **Logs et SIEM** : Splunk, ELK.

- **IA et machine learning** : détection comportementale et attribution technique.

La discipline impose aussi une standardisation : SOP, checklists, modèles de rapports, scripts d'automatisation. Trois défis majeurs se présentent aujourd'hui :

1. **Équilibre investigation / droits fondamentaux** : le RGPD impose des contraintes fortes (minimisation, droit à l'oubli).
2. **Menace quantique** : Shor compromettra RSA/ECC, Grover réduira la robustesse des clés symétriques. Transition vers la cryptographie post-quantique (CRYSTALS-Kyber, Dilithium).
3. **Internationalisation** : les attaques transfrontalières exigent une coopération accrue (Convention de Budapest, Convention de Malabo).

Ces défis soulignent l'importance d'une éthique robuste : l'investigateur doit être garant de la vérité et protecteur des libertés.

L'investigation numérique et la cybersécurité sont indissociables :

- **L'une** incarne la réflexion philosophique et éthique.
- **L'autre** apporte les outils et standards opérationnels.

De nouveaux horizons émergent :

- Forensique d'IA (attaques générées par deep learning).
- Forensique prédictive (anticipation des comportements).
- Forensique quantique (adaptée aux environnements futurs).

Somme toute, l'investigation numérique est un **pilier du pacte social numérique**, garantissant justice, vérité et confiance, conditions indispensables à la vie collective.