REPUBLIQUE 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 Yaoundé I
******
NATIONAL ADVANCED SCHOOL OF ENGINEERING
******
Computer Engineering Department
******

SEC 4031 INTRODUCTION AUX TECHNIQUES D'INVESTTGATION NUMERIQUE

DEVOIR : Philosophie et Fondements de l'Investigation Numérique

Filière : HUMANITÉS NUMÉRIQUES

Niveau : IV

Rédigé par :

NGUEMO VOUFO AURELLE SANDRA 22P067 CIN4

Sous la supervision de :

Mr. MINKA

ANNEE ACADEMIQUE :2025-2026

Partie1 : Fondements Philosophiques et Épistémologiques

1. Analyse Critique du Paradoxe de la Transparence

* Le philosophe coréen Byung-Chul Han, dans la Société de la transparence, met en évidence un paradoxe central de notre ère numérique : l'exigence croissante de transparence, perçue comme une valeur démocratique et un gage de confiance, engendre en réalité une perte de liberté et une érosion de la vie privée. Dans la sociétés, la transparence est présentée comme un idéal moral et politique. Elle garantit la surveillance des gouvernants, favorise la circulation de l'information et renforce la responsabilité. Pourtant, selon Han, cette transparence absolue se transforme en tyrannie : l'individu est exposé en permanence, scruté, mesuré, noté.Un exemple concret illustre ce paradoxe : les programmes de surveillance gouvernementale, Présentés comme outils de protection contre le terrorisme, ils légitiment une collecte massive de données personnelles. La transparence de l'État vis-à-vis de ses citoyens est alors inversée : ce sont les citoyens qui deviennent totalement transparents pour l'État. La promesse démocratique est ainsi trahie.

* Ce paradoxe se retrouve dans l'investigation numérique. L'enquêteur doit arbitrer entre deux exigences contradictoires : établir la vérité (qui suppose transparence des données, accès aux traces numériques) et respecter la vie privée des individus. Trop de transparence détruit la confiance, trop de secret empêche la justice.

* Une piste peut être trouvée dans l'éthique kantienne. Kant propose comme principe fondamental l'impératif catégorique : « Agis uniquement d'après la maxime grâce à laquelle tu peux vouloir en même temps qu'elle devienne une loi universelle ». Transposé au numérique, cela signifie : collecter et traiter les données uniquement selon des règles que tout citoyen pourrait accepter comme universelles. Par exemple, accéder aux données privées uniquement lorsqu'il existe une menace avérée et proportionnée.

2.Transformation Ontologique du Numérique

* Martin Heidegger analyse la technique comme un mode de dévoilement de l'être (Gestell). L'homme moderne ne se définit plus seulement par sa présence physique mais par son rapport technique au monde. À l'ère numérique, cette analyse prend une dimension nouvelle : l'individu existe désormais à travers un double numérique, constitué de ses données et traces.

* Ce phénomène peut être décrit comme un « être-par-la-trace ». Un profil sur un réseau social comme Facebook est une projection de l'identité. Il ne s'agit pas d'une simple représentation mais d'une véritable existence, la personne interagit, communique, crée des effets sociaux à travers cette présence numérique. L'ontologie elle-même est modifiée : l'homme devient hybride(identité physique + identité numérique)

* la preuve légale doit intégrer ces traces numériques comme manifestations d'existence, mais en gardant une approche critique (volatilité, falsification possible).Ainsi, la justice doit élargir son ontologie : reconnaître que l'être humain existe aussi dans ses traces numériques, tout en mettant en place des garanties techniques et juridiques pour assurer

leur authenticité. Le numérique transforme non seulement la preuve, mais la définition même de l'existence légale.

Partie2 : Mathématiques de l'Investigation

3 : Calcul d'entropie de Shannon appliquée

L'entropie de Shannon permet de mesurer l'incertitude contenue dans un fichier. Elle se calcule par :

$$H(X) \;=\; -\sum_{x} p(x)\,\log_2 p(x)$$

où $p(x)$ est la probabilité d'apparition d'un symbole x.

* Interprétation pratique

Document texte (français naturel) : entropie approximative $H \approx 1.5$ bits par caractère. Les lettres fréquentes (par ex. « e », « a ») réduisent l'incertitude. **Image JPEG** : entropie approximative $H \approx 7.2$ bits par octet. La compression supprime des redondances et augmente l'imprévisibilité statistique des octets. **Fichier chiffré AES** : entropie approximative $H \approx 7.9$ bits par octet, proche de l'entropie maximale (uniformité).

* Seuil de détection du chiffrement Sur la base de ces valeurs, un seuil simple de détection automatique peut être posé :

$$\text{Seuil}_{\text{chiffrement}} = 7.5 \text{ bits/octet.}$$

Tout fichier ayant $H > 7.5$ peut être considéré comme *probablement chiffré*, ce qui déclenche une inspection plus approfondie par des experts.

4 : Théorie des graphes en investigation criminelle

Soit un graphe orienté ou non orienté $G = (V, E)$ représentant un réseau de communications :

— V : ensemble de personnes (abonnés),

— E : arêtes représentant les communications (appels, SMS, messages).

* Métriques usuelles

Degré $\deg(v)$: nombre de connexions directes. Identifie les individus les plus actifs.

Centralité d'intermédiarité (betweenness) : mesure le nombre de plus courts chemins passant par un nœud ; révèle les *passeurs* ou brokers.

Centralité de proximité (closeness) : inverse de la distance moyenne aux autres nœuds ; identifie les nœuds « centraux » en termes d'accessibilité.

L'algorithme de Freeman (centralité de degré normalisée) et d'autres algorithmes (PageRank, centralité d'intermédiarité de Brandes) permettent d'identifier des cibles prioritaires. Dans un réseau criminel, le chef n'est pas nécessairement le plus connecté ; il peut être un nœud avec forte intermédiarité et faible visibilité publique.

* Application

L'analyse des communications téléphoniques peut révéler des coordinateurs discrets (faible degré apparente mais forte intermédiarité). La visualisation (avec tailles et couleurs proportionnelles aux mesures de centralité) facilite l'orientation des enquêtes.

5 : Modélisation de l'effet papillon en forensique

Considérons un système de logs comprenant $N = 1000$ événements corrélés. La modification d'un seul timestamp (par ex. déplacement aléatoire de ± 30 secondes) peut avoir un effet en cascade sur plusieurs événements corrélés. Une estimation heuristique donnée dans le chapitre est :

$$\lceil \log_2(1000) \rceil \; = \; 10,$$

ce qui signifie qu'une altération peut perturber la corrélation d'environ 10 événements connexes.

Modèle dynamique

On modélise l'évolution d'une erreur $\delta(t)$ par :

$$\delta(t) \approx \delta(0)\, e^{\lambda t},$$

où λ est l'exposant de Lyapunov effectif du système. Plus λ est grand, plus le système est sensible aux petites perturbations (comportement chaotique).

Conséquences forensiques

Une petite falsification (effacement ou modification d'un log) peut conduire à une reconstruction temporelle fortement biaisée. L'investigateur doit :

- introduire des marges d'incertitude dans la timeline,
- recouper plusieurs sources indépendantes (logs réseaux, SIEM, appliances, sauvegardes),
- utiliser des méthodes probabilistes et bayésiennes pour estimer la vraisemblance des scénarios.

Partie 3 : Révolution Quantique et Ses Implications

6. Expérience de Pensée Schrödinger Adaptée

7. Calculs sur la Sphère de Bloch

On considère un qubit avec $\theta = \pi/3$, $\varphi = \pi/4$:

* Impact en preuve quantique Un système de preuve basé sur qubit ne donnerait pas une certitude absolue mais une probabilité (par ex. 75% de $|0\rangle$). En justice, la preuve deviendrait *probabiliste* plutôt qu'absolue.

8.Analyse du Théorème de Non-Clonage

Partie 4 : Paradoxe de l'Authenticité Invisible

9 : Formalisation mathématique du paradoxe de l'authenticité invisible

Soit une preuve P caractérisée par :

— Authenticité $A(P)$,

— Confidentialité $C(P)$,
— Opposabilité $O(P)$,
tous compris entre 0 et 1.

La relation fondamentale est :

$$A(P) \cdot C(P) \leq 1 - \delta, \quad \delta > 0.$$

*Expérimentation
Pour trois systèmes de preuve :
— Système classique : $A = 0.8, C = 0.4$,
— Système blockchain : $A = 0.9, C = 0.6$,
— Système ZK-NR : $A = 0.7, C = 0.8$.
On vérifie dans chaque cas l'inégalité.

Constante quantique numérique : Une incertitude analogue à celle d'Heisenberg est postulée :

$$\Delta A \cdot \Delta C \geq \frac{\hbar_{\text{num}}}{2}.$$

10 : Implémentation simplifiée ZK-NR

On peut simuler un protocole ZK-NR en Python :
— Le prouveur P démontre la possession d'une information sans la révéler.
— Le vérificateur V obtient l'assurance mais pas le secret.
Évaluation :
— Confidentialité améliorée,
— Vérifiabilité maintenue,
— Coût computationnel supplémentaire ($\approx 15\%$ de surcharge).

Partie 5 : Intégration et Synthèse Avancee

11 : Étude de Cas « QuantumLeaks »

Recommandations techniques

1. **Chiffrement post-quantique** :
   — Signature : Dilithium ou Falcon
   — Chiffrement : Kyber
2. **Protocoles de preuve** :
   — ZK-NR pour l'authentification
   — Preuves à divulgation nulle de connaissance
3. **Archivage à long terme** :
   — Codes correcteurs Reed-Solomon
   — Réplication géo-distribuée

Respect du trilemme CRO

$$\text{CRO} : \begin{cases} \text{Confidentialité} \geq 1 - 2^{-128} \\ \text{Fiabibilité} \geq 0.999 \\ \text{Opposabilité garantie juridiquement} \end{cases}$$

Compétence	Acquis	En cours	À revoir
Compréhension des fondements philosophiques		oui	
Maîtrise des outils mathématiques			oui
Application des concepts quantiques		oui	
Résolution du paradoxe authenticité/confidentialité	oui		
Intégration interdisciplinaire			oui

TABLE 1 – Grille de progression personnelle

12 : Débat Philosophique Structuré

Thèse réaliste

- L'observation quantique modifie nécessairement le système
- La neutralité absolue est physiquement impossible (Wheeler)
- L'investigateur est un « observateur participant »

Thèse constructiviste

- La neutralité est un idéal régulateur (Kant)
- Les pratiques évoluent avec les paradigmes (Kuhn)
- La réflexivité permet d'approcher la neutralité

Synthèse L'investigateur post-quantique adopte une position « méta-réflexive » :

- Conscience des biais d'observation
- Documentation transparente des méthodes
- Validation intersubjective des résultats

13 : Projet de Recherche Personnel

Grille d'Auto-Évaluation