RÉPUBLIQUE DU CAMEROUN
******
Paix – Travail – Patrie
******
UNIVERSITÉ DE YAOUNDÉ I
******
École Nationale Supérieure Polytechnique de Yaoundé
******
Département de Génie Informatique
******

REPUBLIC OF CAMEROON
******
Peace – Work – Fatherland
******
UNIVERSITY OF YAOUNDÉ I
******
National Advanced School Engineering of Yaounde
******
Computers Engineering Department
******

INTRODUCTION AUX TECHNIQUES D'INVESTIGATION NUMERIQUE

THEME : RESOLUTION DES EXERCICES DU CHAP 2

PAR :

NOMS & PRENOMS	FILIERE	MATRICULE
WANSI GILLES GILDAS	**HN-CIN-L4**	**22P037**

Sous la supervision de Ing THIERRY MINKA

Année Académique 2025/2026

Table des matières

1 Introduction

Ce corrigé s'appuie sur le Chapitre 2 (« Histoire de l'Investigation Numérique ») et le Guide de correction (Guide1). Les objets principaux sont les vecteurs de dominance des régimes de vérité numérique, l'analyse foucaldienne d'une affaire historique (Enron), la formalisation d'un modèle d'évolution variant dans le temps et l'analyse du trilemme Confidentialité–Fiabilité–Opposabilité (CRO).

2 Partie 1 — Analyse historique et épistémologique

2.1 1.1 Choix des périodes et vecteurs de dominance

Nous comparons deux périodes :

— **1990–2000** : professionnalisation et institutionnalisation.

— **2010–2020** : ère computationnelle (big data, cloud).

On représente chaque régime par un vecteur convexe

$$\mathbf{R} = (\alpha_T,\ \alpha_J,\ \alpha_S,\ \alpha_P)$$

avec $\alpha_i \geq 0$ et $\sum_i \alpha_i = 1$, où

α_T dominance technologique,

α_J dominance juridique / normative,

α_S dominance sociale / culturelle,

α_P dominance des pratiques professionnelles.

TABLE 1 – Vecteurs de dominance choisis

Période	α_T	α_J	α_S	α_P
1990–2000	0.20	0.40	0.20	0.20
2010–2020	0.50	0.10	0.20	0.20

Vecteurs choisis (justification en texte) :

Justification synthétique

— **1990–2000** : émergence d'institutions, de la chaîne de custody et de règles procédurales (poids élevé de α_J).

— **2010–2020** : montée en puissance des techniques d'analyse algorithmique et du cloud (poids élevé de α_T).

2.2 1.2 Discontinuités épistémologiques (Foucault)

Selon la méthode foucaldienne, une *épistémè* est reconfigurée lorsque les conditions d'énonciation et d'opposabilité changent. On identifie plusieurs ruptures :

— Passage d'une épistémè fondée sur l'expertise technique individuelle à une épistémè juridique/institutionnelle (normes, procédures).

— Transition vers une épistémè computationnelle : l'algorithme devient producteur d'énoncés probants ("vérité algorithmique").

— Ces ruptures changent ce qui est *dicible* (ce qui peut être présenté comme preuve) et *pensable* (ce qui est concevable comme preuve).

2.3 1.3 Explication sociotechnique des ruptures

Les ruptures résultent d'interactions non-linéaires entre :

1. l'évolution technologique (capacité de stockage, calcul, cryptographie),
2. la pression institutionnelle (lois, normes, cas juridiques),
3. les transformations sociales (massification des usages numériques),
4. la professionnalisation (standardisation, guides).

Nature de la transition La transition est *mixte* : lente accumulation des capacités techniques avec des événements ponctuels (scandales, grandes opérations) produisant des bascules rapides — phénomène proche du *punctuated equilibrium*.

2.4 2 — Étude de cas foucaldienne : *Enron* (2001)

2.4.1 2.1 Contexte et raisons du choix

L'affaire Enron illustre l'émergence de l'analyse algorithmique (e-discovery) et la transformation de la preuve documentaire en preuve algorithmique admise par la procédure.

2.4.2 2.2 Analyse comme formation discursive

— **Conditions de possibilité** : masses documentaires électroniques, outils d'indexation et d'analyse automatique.

— **Acteurs** : experts forensiques, avocats, juges, journalistes.

— **Discours dominant** : l'algorithme et l'indexation documentaire produisent des énoncés admissibles comme preuve si la méthode est reproduite.

— **Régime d'énonciation** : transformation du statut de la preuve (du document isolé à l'ensemble corrélé et analysé).

2.4.3 2.3 Dicible / pensable à l'époque

— *Dicible* : corrélations entre documents, correspondances électroniques, motifs de fraude identifiés par des outils d'analyse.

— *Non-pensable ou problématique* : perte d'information liée aux métadonnées détruites, limites d'opposabilité des résultats d'algorithmes non-transparent.

2.4.4 2.4 Comparaison (Enron vs Silk Road)

Enron (2001) : preuve textuelle et documentaire, e-discovery, méthodes d'analyse textuelle.

Silk Road (2013) : multi-couches (blockchain, Tor, métadonnées), corrélation blockchain + réseau, forte dépendance computationnelle.

La différence clé : Silk Road exige une investigation transverse (cryptographie + réseau + application), tandis qu'Enron reposait principalement sur l'analyse documentaire.

3 Partie 2 — Modélisation mathématique et prospective

3.1 Modèle mathématique proposé

Reprenons la formalisation proposée dans le chapitre :

$$\mathbf{R}_{t+1} = F\Big(\mathbf{R}_t,\ \Delta Tech_t,\ \Delta Legal_t,\ I_t\Big)$$

Pour construire un modèle simple, on choisit une dynamique additive suivie d'une normalisation convexe :

$$\mathbf{R}_{t+1} = \text{Normalize}\Big(\mathbf{R}_t + \beta\Delta Tech_t + \gamma\Delta Legal_t + \varepsilon_t\Big),$$

avec :

- Normalize$(\mathbf{v}) = \dfrac{\max(\mathbf{v}, 0)}{\sum_i \max(v_i, 0)}$ pour obtenir un vecteur convexe,
- $\Delta Tech_t$ vecteur qui pousse l'état vers la dominance technologique (ex. $(1, 0, 0, 0)$ normalisé),
- $\Delta Legal_t$ vecteur qui pousse vers la dominance juridique (ex. $(0, 1, 0, 0)$),
- ε_t choc stochastique (incident : scandale, attaque), modélisé par une variable aléatoire à faible probabilité annuelle.

Commentaires sur le modèle Ce modèle demeure pédagogique ; il est extensible en :

- modélisation non-linéaire (effets seuils) : F non-linéaire,
- modèle markovien caché (HMM) pour capter états latents,
- couplage entre composantes (retro-action), ou formulation différentielle stochastique.

3.2 Simulation numérique (50 ans)

Une simulation simple a été exécutée (paramètres pédagogiques) en prenant pour point de départ $\mathbf{R}_{2020} = \mathbf{R}_{2010-2020}$.

Paramètres illustratifs

- dérive technologique $\beta = 0.025$ (annuelle, faible),
- dérive légale $\gamma = 0.007$,
- probabilité d'incident annuel $p = 0.08$,
- simulation : 50 pas (2020 à 2070).

3.3 4 — Vérification de la loi d'accélération

La loi proposée dans le chapitre est :

$$\Delta t_{n+1} = k \cdot \Delta t_n, \quad 0 < k < 1.$$

Données élémentaires (Chap.2) Périodes et durées :

$$\begin{aligned} 1970\text{–}1990: &\quad \Delta t_1 = 20 \\ 1990\text{–}2000: &\quad \Delta t_2 = 10 \\ 2000\text{–}2010: &\quad \Delta t_3 = 10 \\ 2010\text{–}2020: &\quad \Delta t_4 = 10 \end{aligned}$$

Calcul des ratios

$$\left\{ \frac{\Delta t_2}{\Delta t_1}, \ \frac{\Delta t_3}{\Delta t_2}, \ \frac{\Delta t_4}{\Delta t_3} \right\} = \{0.5, \ 1.0, \ 1.0\}.$$

Estimation simple par moyenne :

$$\hat{k} = \frac{0.5 + 1 + 1}{3} \approx 0.8333.$$

Prédiction grossière :

$$\Delta t_5 \approx \hat{k} \cdot \Delta t_4 = 0.8333 \times 10 \approx 8.33 \text{ ans},$$

donc changement estimé vers $2020 + 8.33 \approx 2028.3$.

Remarques statistiques Cette estimation est indicative. Pour une vérification rigoureuse il faudrait :

— collecter des dates précises d'événements (telles que définitions de normes, opérations majeures, scandales),

— appliquer une régression non-linéaire sur une série temporelle plus longue,

— tester la significativité statistique (p-valeurs, intervalles de confiance).

3.4 5 — Analyse du trilemme CRO historique

On considère le triplet (C, R, O) dans $[0, 1]^3$ (Confidentialité, Fiabilité, Opposabilité).

Table 2 – Estimation indicative des scores CRO par période

Période	Confidentialité (C)	Fiabilité (R)	Opposabilité (O)
1970–1990	0.25	0.70	0.60
1990–2000	0.35	0.80	0.65
2000–2010	0.55	0.75	0.70
2010–2020	0.70	0.60	0.50
2020–...	0.85	0.55	0.45

Interprétation

— La confidentialité augmente avec les avancées cryptographiques et les pratiques de protection des données.

— La fiabilité a connu une hausse à la professionnalisation, mais peut décliner si les systèmes deviennent opaques (black-box IA).

— L'opposabilité est contrainte lorsque la vérification demandée entre en conflit avec la confidentialité : difficulté à prouver publiquement des résultats issus d'algorithmes non-expliqués.

4 Conclusion et recommandations

— La méthode proposée (vecteur de dominance + modèle additif normalisé) fournit un cadre reproductible pour simuler l'évolution des régimes de vérité.

— Les ruptures historiques sont en grande partie expliquées par l'interaction technologie / loi / société / pratiques ; toutefois, les événements ponctuels restent déterminants.

— Pour une étude approfondie : collecter événements datés, réaliser des estimations statistiques robustes (régression non-linéaire, tests d'hypothèse), et développer un modèle stochastique plus riche.

PARTIE 3

5 Exercice 6 : Reconstruction archéologique d'une investigation

5.1 6.1 Choix de l'affaire : Kevin Mitnick (1995)

L'affaire Kevin Mitnick constitue un cas emblématique de la décennie 1990 : premier « super-hacker » médiatisé, il fut traqué et arrêté grâce à une collaboration entre autorités américaines et experts indépendants (notamment Tsutomu Shimomura).

5.2 6.2 Investigation avec les outils et méthodes de l'époque

Contexte technologique (1990–1995).

— Réseaux : dial-up, protocole TCP/IP rudimentaire, traçage limité aux logs ARPANET/ISP.

— Outils forensiques : scripts Unix, `tcpdump`, `whois`, analyse manuelle des fichiers log.

— Méthodologie : approche artisanale, expertise individuelle, absence de normalisation (pas de NIST SP 800–86 ni d'ISO 27037).

Chaîne de custody : Pratiquement inexistante ; les preuves reposaient sur la crédibilité technique des experts. La validité épistémique était garantie par l'autorité de l'expert (*régime de vérité technique*).

5.3 6.3 Analyse moderne de la même affaire

Outils contemporains.

— Analyse automatisée de métadonnées ;

— Corrélation temporelle multi-sources ;

— Honeypots, détection comportementale, machine learning pour attribution ;

— Archivage forensique normalisé (ISO 27037, RFC 3227).

Évolution du régime de vérité.

Élément	1995 : régime technique	2020 : régime computationnel
Preuve légitime	Logs systèmes	Corrélations algorithmiques
Autorité	Expert individuel	Processus algorithmique + institution
Chaîne de custody	Informelle	Normalisée et opposable

5.4 6.4 Impact des limitations technologiques

— **Fiabilité :** absence d'horodatage précis et d'intégrité cryptographique → fragilité juridique.

— **Confidentialité :** protection faible, exposition accrue des traces.

— **Opposabilité :** dépendance au témoignage d'experts ; absence de standard international.

Ces contraintes expliquent pourquoi la vérité de l'époque était une « vérité d'autorité », non encore computationnelle.

6 Exercice 7 : Projet de recherche archéologique

6.1 7.1 Identification d'un « trou » historique

Sujet proposé : *L'émergence oubliée des pratiques forensiques dans les réseaux Unix (1980–1985).* Les premiers administrateurs système ont développé des procédures implicites de collecte et d'interprétation de traces, sans formalisation.

6.2 7.2 Hypothèse historique testable

H_0 : $Lespremièrespratiquesforensiques Unixontconstituéuneproto-archéologiedelapreuvenumériq$

6.3 7.3 Sources primaires à collecter

— **RFC historiques :** RFC 706 (1976), RFC 819 (1982) ; traces d'administrations réseau.

— **Publications techniques :** *USENIX Proceedings*, *Bell Labs Notes*, articles sur la sécurité système.

— **Archives Unix :** scripts shell, `syslog`, `auditd`.

6.4 7.4 Méthode foucaldienne appliquée

1. **Archéologie des pratiques** : identifier les conditions d'apparition du discours « trace numérique » ;
2. **Analyse des énoncés** : repérer dans les RFC et manuels les formulations « preuve », « sécurité », « intégrité » ;

3. **Cartographie du régime de vérité** : experts Unix machines procédures implicites ;
4. **Mise en relation avec les discontinuités ultérieures** : comment ces pratiques se sont institutionnalisées.

6.5 7.5 Structure d'article académique (suggestion)

— Introduction : problématique et justification du « trou » historique ;
— Cadre théorique : Foucault, Latour, Kuhn ;
— Méthodologie : analyse archéologique et comparative ;
— Résultats : repérage des premières normes implicites ;
— Discussion : institutionnalisation ultérieure ;
— Conclusion : continuités et discontinuités épistémiques.

7 Exercice 8 : Analyse prospective des régimes futurs

7.1 8.1 Scénario crédible pour 2030–2050

Scénario : le régime neuro-quantique Entre 2030 et 2050, les interfaces cerveau–machine (BCI) et l'informatique quantique convergent. Les enquêtes numériques impliquent alors des traces neuronales et quantiques, fusionnant données cognitives et logiques quantiques d'exécution.

7.2 8.2 Régime de vérité correspondant

$$\text{Régime de Vérité Neuro-Quantique} : \begin{cases} \text{Preuve : état quantique–neuronal (superposé)} \\ \text{Autorité : protocole IA explicable et vérifié par ZK–quantiqu} \\ \text{Institution : cour mixte techno–juridique} \end{cases}$$

7.3 8.3 Conditions de possibilité

- Maturité technologique : calcul quantique fiable, interfaces BCI sécurisées.
- Cadres légaux : normes post-quantiques, régulations bioéthiques.
- Infrastructures : réseaux quantiques fiables, protocoles ZK–STARKs universels.

7.4 8.4 Méthodologie d'investigation adaptée

1. Collecte : enregistrement d'états quantiques/neuraux via capteurs certifiés ;
2. Préservation : chaîne de custody quantique basée sur horodatages ZK–NR ;
3. Analyse : superposition de modèles probabilistes et décodage IA transparente ;
4. Vérification : preuve zero-knowledge quantique garantissant l'opposabilité sans divulgation.

7.5 8.5 Défis éthiques et épistémologiques

- **Confiance algorithmique :** l'enquête dépend d'IA autonomes, risque de biais inévitables.
- **Consentement cognitif :** l'investigation neuro-numérique nécessite un cadre bioéthique renforcé.
- **Opposabilité :** comment un tribunal humain peut-il comprendre une preuve qu'il ne peut observer ?
- **Persistance du trilemme CRO :** la confidentialité (états neuraux) entre en tension avec la fiabilité et l'opposabilité quantique.

8 Conclusion

Les exercices 6–8 démontrent l'importance d'une approche archéologique et critique de l'investigation numérique. Reconstituer les pratiques passées éclaire les ruptures présentes ; modéliser les futurs possibles permet d'anticiper les dilemmes éthiques et les régimes de vérité émergents.