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

EXERCICES DU CHAPITRE 2

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

Sous la supervision de
Thierry MINKA, Eng

Année académique 2025/2026

Partie 3 : Investigation Historique Appliquée

6. Reconstruction Archéologique d'Investigation

Cas étudié : *Affaire Kevin Mitnick (1995)*

Cette affaire illustre la transition entre un régime de vérité **technique** et un régime **juridico-professionnel**. Le pouvoir de véridiction se déplace du technicien individuel vers l'expert institutionnalisé, marquant ainsi la naissance d'une véritable épistémè de la traçabilité numérique.

$$\vec{R}_{1995} = (\alpha_T = 0.35,\ \alpha_J = 0.40,\ \alpha_S = 0.15,\ \alpha_P = 0.10)$$

Les caractéristiques principales :

- **La nature du régime :** juridico-technique, centré sur la chaîne de custody.
- **L'Epistémè dominante :** la vérité découle de la traçabilité et de la préservation des preuves.
- **Les acteurs clés :** enquêteurs fédéraux, experts indépendants, autorités judiciaires.

Les méthodes et outils de l'époque :

- L'analyse *manuelle* des journaux système (logs UNIX, adresses IP, timestamps).
- L'utilisation d'outils rudimentaires : `WHOIS`, `traceroute`, `netstat`.
- La corrélation temporelle humaine entre événements et connexions.
- La conservation de preuves sur supports physiques (disquettes, impressions papier).
- La légitimité de la preuve fondée sur la *réputation de l'expert.*

La reconstruction contemporaine :

- l'emploi de plateformes **SIEM** et d'intelligences artificielles de corrélation automatisée.

- La vérification d'intégrité par **empreintes cryptographiques** (hash, blockchain).
- l'analyse de graphes comportementaux pour la corrélation d'identités.
- l'archivage des preuves dans des **registres immuables et distribués**.
- l'attribution algorithmique fiable et reproductible.

Dimension	**1995**	**2025**
Collecte	Extraction manuelle	Collecte automatisée
Analyse	Corrélation humaine	Corrélation algorithmique
Autorité de preuve	Expertise individuelle	Légitimité computationnelle
Régime de vérité	Juridico-technique	Computationnel-algorithmique

> La vérité ne se dit plus, elle se calcule. La transition de la preuve technique à la preuve algorithmique illustre le passage du *sujet expert* au *système calculateur* comme producteur de vérité.

7. Projet de Recherche Archéologique

Problématique identifiée : L'archéologie de l'investigation numérique présente un *trou historique* notable : la période 1980–1990, où le hacking artisanal s'est progressivement institutionnalisé en expertise technique reconnue.

Hypothèse de recherche :

> La formalisation du cadre légal de la preuve numérique n'a pas émergé des avancées technologiques, mais des scandales médiatiques qui ont rendu la vérité technique socialement dicible.

Méthodologie archéologique :

- l'analyse des **conditions discursives de possibilité** de la preuve numérique.

- l'étude des **textes fondateurs** : RFC 1087 (*Ethics and the Internet*), Computer Fraud and Abuse Act (1986), récits médiatiques de l'affaire des 414s.
- Cartographie du **réseau d'acteurs** : hackers, journalistes, législateurs, ingénieurs.
- L'application du cadre foucaldien : repérage des formations discursives et des pratiques de légitimation de la vérité.

Résultats attendus :

- La mise en évidence d'un **proto-régime de vérité hybride**, entre artisanat technique et institutionnalisation juridique.
- L'analyse du rôle performatif du **discours médiatique** dans la création du droit numérique.
- La proposition d'un modèle dynamique reliant **visibilité sociale** et **formalisation juridique**.

  La société n'a pas légitimé la preuve technique parce qu'elle la comprenait, mais parce qu'elle la craignait. Cette peur médiatisée a constitué la matrice de la juridicisation du numérique.

8. Analyse Prospective des Régimes Futurs (2030–2050)

Scénario envisagé : *Régime neuro-digital*

Ce régime émergerait de la convergence entre **IA cognitive**, **biométrie neuronale** et **interfaces cerveau-machine**. La trace numérique deviendrait *interne au sujet*, incorporée à son activité cérébrale.

Les conditions de possibilité :

- La captation et interprétation directe des signaux neuronaux comme éléments de preuve.
- la validation des souvenirs numériques par empreintes cérébrales certifiées.

- le déplacement du sujet de savoir : du corps technique à l'esprit numérisé.

Méthodologie d'investigation adaptée :

- **Neuro-forensique** : analyse des patterns cérébraux liés aux actes numériques.
- **La blockchain cognitive** : enregistrement sécurisé des flux neuronaux.
- **Audit éthique par IA** : supervision non intrusive garantissant la confidentialité mentale.

Défis éthiques et épistémologiques :

- **Opposabilité :** comment vérifier une preuve sans violer la vie mentale ?
- **Authenticité :** comment distinguer un souvenir réel d'une reconstruction neuronale ?
- **Confiance :** la machine peut-elle devenir sujet de vérité ?

  Le régime neuro-digital représenterait une discontinuité radicale. Il verrait l'abandon du *sujet parlant* au profit du *sujet calculant et observé*. La vérité ne serait plus énoncée, mais extraite du signal cérébral, inaugurant une ère post-humaine de l'investigation.

Partie 2 : Modélisation Mathématique et Prospective

3. Modélisation de l'évolution des régimes (question par question)

Modèle général On représente chaque régime par un vecteur de dominance :

$$\vec{R}_t = (\alpha_T, \alpha_J, \alpha_S, \alpha_P), \qquad \sum \alpha_i = 1.$$

La transition est modélisée par une fonction paramétrique :

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

où $\Delta Tech_t$ et $\Delta Legal_t$ sont des variables numériques représentant l'amplitude du changement technique et juridique entre t et $t+1$, I_t est un indicateur d'incidents critiques, et θ l'ensemble des paramètres du modèle.

Approche discrétisée (chaîne de Markov conditionnée) Pour passer de la représentation vectorielle à une distribution de probabilités de *changement d'état*, on discrétise l'espace des régimes en états finis :

$$\mathcal{S} = \{T, J, S, C\}$$

(Technique, Juridique, Standardisé, Computationnel). On modélise la probabilité conditionnelle

$$P(R_{t+1} = j \mid R_t = i, X_t) \quad (j \in \mathcal{S})$$

où $X_t = (\Delta Tech_t, \Delta Legal_t, I_t)$. Une paramétrisation usuelle est la *multinomial logit* (softmax) :

$$score_j = \beta_{j0} + \beta_{j1}\,\Delta Tech_t + \beta_{j2}\,\Delta Legal_t + \beta_{j3}\,I_t,$$

$$P(R_{t+1} = j \mid R_t = i, X_t) = \frac{\exp(score_j)}{\Sigma_{k\in\mathcal{S}} \exp(score_k)}.$$

Calcul numérique d'exemple On illustre la formule avec un jeu de paramètres β et des valeurs de X_t.

Paramètres choisis (exemple pédagogique) :

$$\begin{aligned}
Pour j = T: &\ \beta_{T0} = 1.0,\ \beta_{T1} = 2.0,\ \beta_{T2} = -1.0,\ \beta_{T3} = -0.5,\\
Pour j = J: &\ \beta_{J0} = 0.5,\ \beta_{J1} = 0.5,\ \beta_{J2} = 1.5,\ \beta_{J3} = 0.8,\\
Pour j = S: &\ \beta_{S0} = 0.2,\ \beta_{S1} = 0.3,\ \beta_{S2} = 0.7,\ \beta_{S3} = 0.1,\\
Pour j = C: &\ \beta_{C0} = -0.5,\ \beta_{C1} = 1.0,\ \beta_{C2} = 0.2,\ \beta_{C3} = 0.9.
\end{aligned}$$

Valeurs des variables :

$$\Delta Tech_t = 0.4, \qquad \Delta Legal_t = 0.2, \qquad I_t = 1.$$

Étape 1 — calcul des scores linéaires

$s_T = \beta_{T0}+\beta_{T1}\cdot 0.4+\beta_{T2}\cdot 0.2+\beta_{T3}\cdot 1 = 1.0+2.0\times 0.4+(-1.0)\times 0.2+(-0.5)\times 1 = 1$

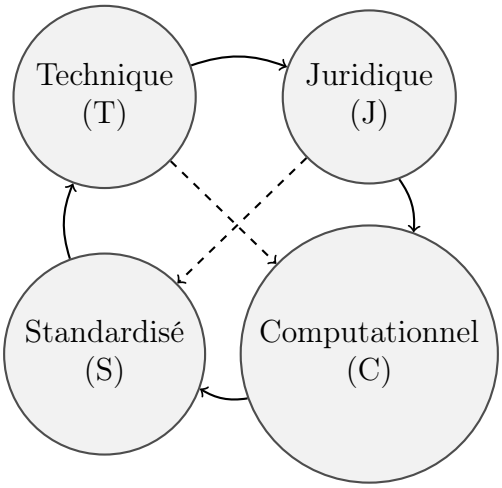

Figure 1: Espace d'états discretisé (exemple) : quatre régimes et transitions possibles.

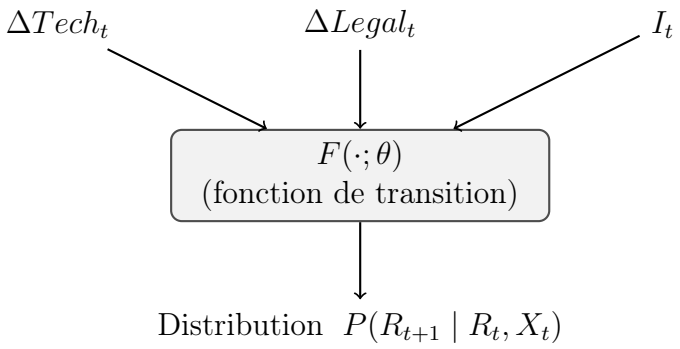

Figure 2: Schéma fonctionnel : entrée (features) vers la fonction de transition F puis distribution de sortie.

Figure 3: Histogramme des probabilités de transition calculées dans l'exemple numérique (softmax).

Étape 2 — exponentiation (softmax numerator)

Nous calculons $\exp(s_j)$ pour chaque score (valeurs arrondies à 10 décimales) :

$\exp(s_T) = e^{1.10} \approx 3.0041660239$, $\exp(s_J) = e^{1.80} \approx 6.0496474644$, $\exp(s_S) = e^{0}$

Étape 3 — normalisation

Somme des exponentielles :

$$Z = \sum_{j \in \{T,J,S,C\}} \exp(s_j) \approx 3.0041660239+6.0496474644+1.7506725003+2.316366$$

Étape 4 — probabilités finales

$$P_T = \frac{3.0041660239}{13.1208529654} \approx 0.2289611835 \ (\approx 22.896\%), P_J = \frac{6.0496474644}{13.1208529654} \approx 0.4$$

Ces nombres illustrent comment, pour les valeurs choisies, l'état *Juridique* (J) a la probabilité la plus élevée de devenir le régime suivant.

Remarques méthodologiques

- Les coefficients β sont estimables par maximum de vraisemblance sur une série historique de transitions observées (log-likelihood multinomial).
- Dans la pratique, on conditionne souvent la probabilité sur l'état courant R_t (effet d'auto-corrélation) et on ajoute des variables d'interaction (par ex. $I_t \times \Delta Tech_t$).
- Validation : cross-validation temporelle, calibration probabiliste (reliability diagrams) et tests de robustesse aux incidents extrêmes.

4. Vérification de l'accélération technologique

Loi proposée On teste la loi empirique :

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

Pratiquement, on dispose d'une suite de dates $t_0 < t_1 < \ldots < t_N$ où des ruptures de régime sont datées ; on forme $\Delta t_n = t_n - t_{n-1}$ pour $n = 1, \ldots, N$.

Estimation de k en transformant logarithmiquement :

$$\ln(\Delta t_{n+1}) = \ln k + \ln(\Delta t_n).$$

Donc une régression linéaire simple (sans intercept centré si on préfère) sur les paires $(\ln \Delta t_n, \ln \Delta t_{n+1})$ donne une estimation de $\ln k$; on en déduit $k = \exp(\widehat{\ln k})$.

Procédure pratique

1. Calculer Δt_n à partir des dates historiques.
2. Prendre logarithme : $y_n = \ln(\Delta t_{n+1})$, $x_n = \ln(\Delta t_n)$.
3. Estimer par moindres carrés : $y_n = a + bx_n + \varepsilon_n$. Le coefficient b proche de 1 indique une relation multiplicative directe ; ici on s'attend à $b \approx 1$ et $a = \ln k$.
4. Tester $b = 1$ et significativité de a (p-valeur).
5. Robustesse : utiliser un estimateur robuste (Theil–Sen) si outliers (événements extrêmes).

Remarque de mise en garde La «loi» est empirique : la constance de k doit être testée par période ; un seul k global est rarement réaliste sur un siècle.

5. Analyse du Trilemme CRO (question 5)

Définition Pour un système S on considère trois scores normalisés :

$C(S) \in [0,1]\,(Confidentialit), \quad R(S) \in [0,1]\,(Fiabilit), \quad O(S) \in [0,1]\,(O$

Le trilemme affirme qu'il est impossible d'atteindre simultanément $C = R = O = 1$.

Représentation géométrique On place ces trois dimensions aux sommets d'un triangle de décisions ; les régimes historiques se projettent à l'intérieur.

Analyse quantitative Si l'on dispose de mesures C_n, R_n, O_n pour différentes époques n, on peut :

- tracer la trajectoire (C_n, R_n, O_n) dans l'espace de décision (PCA ou coordonnées barycentriques) ;
- rechercher des compromis optimaux via une optimisation multi-objectif (Pareto front).

Partie 1 : Analyse Historique et Épistémologique

1. Analyse comparative des régimes de vérité

a)Choix des deux périodes

b) Calcul des vecteurs de dominance

$$\vec{R}_t = (\alpha_T, \alpha_J, \alpha_S, \alpha_P), \qquad \sum_i \alpha_i = 1, \qquad \alpha_i = \frac{s_i}{\sum_j s_j}.$$

$$\vec{R}_{1990-2000} = (0.12, 0.47, 0.06, 0.35), \quad \vec{R}_{2010-2020} = (0.45, 0.10, 0.20, 0.25)$$

c) Discontinuités épistémologiques (Foucault)

d) Explication sociotechnique des ruptures

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

où $\Delta Tech_t$ = progrès techniques (cloud, IA), $\Delta Legal_t$ = retard juridique, I_t = incidents critiques (Silk Road, Panama Papers). L'augmentation de α_T et la diminution de α_J traduisent la technicisation du régime de vérité.

e) Nature de la transition

Transition progressive dans le temps, mais révolutionnaire dans sa nature :

$$\lim_{N\to\infty} \frac{Analysehumaine}{Analysealgorithmique} = 0.$$

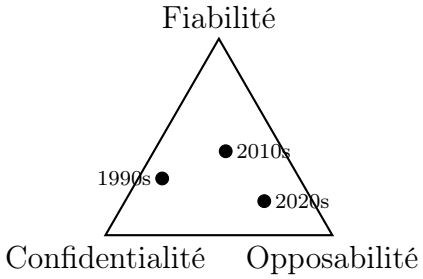

Figure 4: Triangle du Trilemme CRO — positionnement indicatif de régimes historiques.

Période	**Caractéristiques générales**
1990–2000 (Ère de la professionnalisation)	Naissance d'une discipline ; juridicisation forte ; émergence de standards et de la *chain of custody*.
2010–2020 (Ère du Big Data et du Cloud)	Explosion des volumes de données ; algorithmisation des procédures ; dominance des infrastructures cloud et des méthodes computationnelles.

Axe	**Indicateurs principaux**	**1990–2000 (s_i)**	**2010–2020 (s_i)**
Technologie (T)	Internet, PC, honeypots / cloud, IA, blockchain	2	9
Juridique (J)	CFAA, IOCE, chain of custody / RGPD, cadres cloud	8	2
Social (S)	Fracture numérique / culture crypto, dark web	1	4
Professionnel (P)	Standardisation, ISO, forensics / data science	6	5
Somme $\sum s_i$		**17**	**20**

Dimension	**1990–2000**	**2010–2020**	**Rupture observée**
Autorité du vrai	Expert, tribunal	Algorithme, corrélation	Passage du sujet expert à l'autorité computationnelle
Objet du savoir	Document, log	Dataset massif, blockchain	Mutation de la trace en donnée analysable
Procédure de véridiction	Chaîne de custody, norme ISO	Calcul automatisé, machine learning	De la preuve normative à la preuve statistique
Régime de pouvoir	Régulation disciplinaire	Pouvoir infrastructural	Déplacement vers le pouvoir technique

2. Étude de cas : *Silk Road* (2013)

a) Contexte factuel

Marché noir sur Tor, paiement en Bitcoin, saisie de 144 000 BTC, enquête FBI, analyse blockchain forensique pionnière.

b) Formation discursive (Foucault)

[nosep]

- Objets : anonymat, traçabilité, cryptomonnaie.
- Sujets autorisés : analystes blockchain, FBI, data scientists.
- Règles d'énonciation : validité fondée sur la signature cryptographique.
- Champ d'énonciation : espace techno-juridique global.
- Condition de vérité : traduction de la preuve algorithmique en preuve légale.

c) Ce qui est dicible et pensable

[nosep]

- Dicible : « La blockchain permet la traçabilité totale des transactions. »
- Pensable : corrélation d'identités pseudonymes.
- Inimaginable avant 2010 : recevabilité juridique d'une preuve purement algorithmique.

d) Cartographie du régime de vérité (La *Stack*)

e)Synthèse comparative

La preuve algorithmique remplace la preuve documentaire : la vérité circule du code vers le droit par des traductions successives. Le pouvoir de véridiction passe des institutions à l'infrastructure technique.

L'investigateur devient opérateur de modèles ; la *preuve computationnelle* devient paradigmatique.

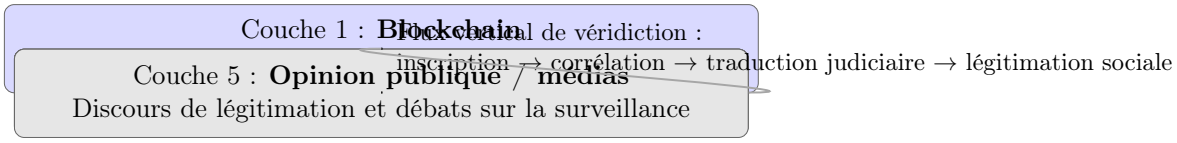

Figure 5: Cartographie multi-couches du régime de vérité dans l'affaire *Silk Road*.

Élément	**1990–2000**	**2010–2020 (Silk Road)**	**Discontinuité**
Régime de vérité	Juridico-professionnel	Computationnel	Mutation d'épistémè
Vecteur $\vec{R}$	(0.12, 0.47, 0.06, 0.35)	(0.45, 0.10, 0.20, 0.25)	$\uparrow \alpha_T$, $\downarrow \alpha_J$
Preuve paradigmatique	Chaîne de custody	Blockchain / Big Data	De la norme à la donnée
Autorité épistémique	Expert / Tribunal	Algorithme / Analyste data	Déplacement du pouvoir de validation
Type de transition	Progressive	Révolutionnaire	Changement d'échelle computationnel