RÉPUBLIQUE DU CAMEROUN
******
UNIVERSITÉ DE YAOUNDÉ I
******
ÉCOLE NATIONALE SUPÉRIEURE POLYTECHNIQUE
******
DÉPARTEMENT DU GÉNIE INFORMATIQUE

REPUBLIC OF CAMEROON
******
UNIVERSITY OF YAOUNDE I
******
NATIONAL ADVANCED SCHOOL OF ENGINEERING
******
DEPARTMENT OF COMPUTER ENGINEERING

Réponses aux questons du Chapitre II

Réalisé par : NANTIA ZAGUE AXEL FRISKYL

Matricule : 22P105

Spécialité : Cybersécurité et Investigation Numérique (CIN)

UE : Introduction aux techniques de l'Investigations Numériques

Sous la supervision de : Mr. MINKA MI NGUIDJOI Thierry Emmanuel

Année académique : 2025/2026

Exerçons-nous : Archéologie des Régimes de Vérité Numérique

Partie 1 : Analyse Historique et Épistémologique

1. Analyse Comparative des Régimes de Vérité

Question 1 : Après le choix de deux périodes, calculons leurs vecteurs de dominance $\overrightarrow{R} = (\alpha_T,\ \alpha_J,\ \alpha_S,\ \alpha_P)$

- Périodes choisies : 2000-2010 Vs 2015-2025
- Calcul des vecteurs de dominance

Pour les vecteurs de dominance $\overrightarrow{R} = (\alpha_T,\ \alpha_J,\ \alpha_S,\ \alpha_P)$ des périodes 2000-2010 et 2015-2025, basée sur les évolutions technologiques, juridiques, sociales et professionnelles :

- **Période 2000-2010**
  - Dominance technologique (T) forte, environ 0.6, avec la montée des infrastructures critiques numériques, normalisation (ISO, NIST).
  - Dominance juridique (J) modérée, 0.2, développement des cadres réglementaires et juridiques pour la preuve numérique.
  - Dominance sociale (S) faible, 0.05, consciences sociales encore émergentes.
  - Dominance professionnelle (P) modérée, 0.15, professionnalisation progressive des méthodes d'investigation.

$$\overrightarrow{R} = (0.6,\ 0.2,\ 0.05,\ 0.15)$$

- **Période 2015-2025**
  - Dominance technologique (T) modérée, environ 0.3, avec l'omniprésence de l'IA et des technologies quantiques.
  - Dominance juridique (J) faible, environ 0.1, régulations souvent en retard par rapport à la technologie.
  - Dominance sociale (S) forte, environ 0.3, sensibilisation sociétale accrue aux problématiques de sécurité, vie privée, et influence numérique.
  - Dominance professionnelle (P) élevée, 0.3, complexification des pratiques d'investigation adaptées aux environnements IA et quantique.

$$\overrightarrow{R} = (0.3,\ 0.1,\ 0.3,\ 0.3)$$

Ces valeurs s'appuient sur l'évolution des régimes de vérité numérique, l'adoption des standards, la professionnalisation des pratiques, et l'émergence des enjeux sociétaux majeurs liés à la transformation numérique.

Question 2 : Identifions les discontinuités épistémologiques selon Foucault

Dysfonctionnements 2000-2010

- Surcharge informationnelle due à l'explosion des échanges numériques, rendant la gestion des preuves complexe.

— Fracture numérique persistante malgré une meilleure accessibilité, avec des disparités dans l'appropriation des outils.
— Complexité dans la standardisation des méthodes d'investigation, avec des disparités dans la qualité des preuves.
— Cadres juridiques insuffisants face à la rapidité des innovations technologiques.

Dysfonctionnements 2015-2025

— Déficit réglementaire face aux évolutions rapides de l'IA et des technologies quantiques.
— Tensions sociales liées à la vie privée et à la surveillance accrue.
— Complexification des pratiques professionnelles, rendant la formation et la certification plus difficiles.
— Opacité algorithmique des systèmes IA, limitant la transparence et la vérification humaine.

Question 3 : Proposons une explication sociotechnique de ces ruptures

Voici une explication sociotechnique des ruptures entre les périodes 2000-2010 et 2015-2025 dans le régime de vérité numérique :

Dimension Technique

— La période 2000-2010 est marquée par la standardisation progressive des technologies numériques, la montée des infrastructures critiques et la démocratisation de l'accès à Internet. Cependant, la complexité technique reste élevée avec des vulnérabilités importantes (virus, spam) et une explosion des flux de données.
— De 2015 à 2025, la révolution numérique s'accélère avec l'introduction massive de l'intelligence artificielle, des technologies quantiques, et la généralisation de l'analyse algorithmique. Ces avancées posent de nouveaux défis, notamment en termes de transparence des systèmes et de capacités d'investigation humaines.

Dimension Sociale

— Pendant 2000-2010, la fracture numérique est encore présente et la société découvre progressivement les enjeux liés à la surveillance et à la protection de la vie privée, engendrant des réactions mitigées.
— De 2015 à 2025, les tensions sociales s'accentuent autour des problématiques de données personnelles, de contrôle social, et d'opacité algorithmique. L'individu est à la fois acteur et objet des flux numériques, dans un contexte où les normes sociales peinent à stabiliser les rapports entre liberté et sécurité.

Question 4 : La transition était-elle progressive ou révolutionnaire ?

La transition entre les périodes 2000-2010 et 2015-2025 dans le régime de vérité numérique peut être vue comme à la fois progressive et révolutionnaire, selon l'analyse foucaldienne et contemporaine :

Arguments pour une transition progressive

— Les évolutions techniques, sociales et juridiques s'appuient sur des fondations existantes (normes, infrastructures, cadres institutionnels) qui se maintiennent et s'adaptent progressivement.

— La professionnalisation des pratiques et la normalisation des méthodes s'inscrivent dans une continuité de montée en compétences et d'affinement des protocoles.
— L'adoption progressive de nouveaux outils (big data, IA) se fait avec phases d'expérimentation, régulations partielles et ajustements méthodologiques.

Arguments pour une transition révolutionnaire

— Le saut technologique apporté par l'IA, le quantique et la vérité computationnelle bouleverse radicalement les capacités d'investigation, introduisant une rupture majeure avec les anciens paradigmes.
— L'incapacité des cadres juridiques et des normes à suivre la rapidité des innovations crée une véritable crise d'opposabilité et de validité dans la construction de la preuve.
— Les tensions sociales autour de la surveillance, la confidentialité et le contrôle global témoignent d'une remise en question radicale des rapports entre individu, société et pouvoir.
— Du point de vue foucaldien, ces ruptures structurent une discontinuité épistémologique, marquant le passage d'un régime de vérité à un autre.

Enfin la transition est un processus complexe mêlant continuités dans les pratiques professionnelles et institutionnelles, et ruptures nettes dans les technologies, les normes et les rapports sociaux. Ce double mouvement reflète la nature non linéaire des transformations numériques, où la progression graduelle et la révolution coexistent et s'alimentent mutuellement.

2. Étude de Cas Archéologique Foucaldienne

Question 1 : Analyse d'une affaire historique spécifique « Enron » comme formation discursive au sens de Foucault

Contexte de l'affaire Enron

Enron, entreprise américaine du secteur de l'énergie, a fait faillite en 2001 suite à un scandale financier majeur impliquant des fraudes comptables massives, cachées par des procédés sophistiqués. L'affaire s'est traduite par une analyse très poussée de documents électroniques (e-mails, rapports, transactions), ouvrant la voie à une nouvelle façon d'appréhender la preuve numérique.

Formation discursive au sens de Foucault

Selon Foucault, une formation discursive est un système organisé d'énoncés qui structure ce qui peut être dit, comment, et qui peut parler, définissant ainsi l'objet de savoir. Elle régule les conditions d'énonciation et d'opposabilité de la vérité au sein d'un régime de vérité.

Analyse foucaldienne de l'affaire Enron

— Objet de savoir : la fraude comptable, construite et révélée par l'analyse des preuves numériques.
— Règles du discours : l'enquête s'appuie sur des méthodes d'analyse algorithmique et automatisée (TAR), légitimant l'usage des données massives comme preuves recevables.

— Sujets du discours : experts en forensic numérique, enquêteurs, juges, qui deviennent détenteurs du savoir légitime sur la fraude.
— Institutions et pouvoirs : tribunaux, réglementations (comme la loi Sarbanes-Oxley) jouent un rôle central dans la production et la validation de la vérité.
— Effet de vérité : le discours autour d'Enron crée un nouveau régime de vérité fondé sur la preuve algorithmique et institutionnelle, redéfinissant la notion même de preuve et d'autorité dans le monde numérique.

L'affaire Enron illustre une formation discursive où technique, institution et discours se mêlent pour produire un nouveau mode de vérité numérique. Cette formation exprime une transformation majeure des pratiques discursives, caractérisée par l'émergence des algorithmes et des preuves électroniques comme sources centrales de savoir et de légitimité dans le champ judiciaire et économique.

Question 2 : Identification de ce qui était « dicible » et « pensable » à cette époque

À l'époque de l'affaire Enron (2001), voici ce qui était dicible et pensable au sein de la formation discursive dominante :

Ce qui était dicible

— La fraude comptable et la manipulation financière étaient devenues des sujets d'enquête majeurs, à travers l'analyse des documents électroniques, e-mails et transactions.
— L'usage des preuves numériques (big data, analyses informatiques) était légitimé comme moyen crucial pour établir la preuve devant la justice.
— Des normes et pratiques telles que la chaîne de custody et l'audit électronique étaient reconnues comme fondamentales.
— La responsabilité pénale des dirigeants, cadres et auditeurs était affirmée ; les délits d'initiés, la destruction de preuves, la manipulation des marchés étaient explicitement dénoncés.
— La transparence et la régulation financière étaient revendiquées comme essentielles pour restaurer la confiance.

Ce qui était pensable

— Les cadres de gouvernance d'entreprise traditionnels, basés sur la confiance et la réputation, pouvaient être remis en question.
— La complexité des montages financiers et la sophistication des techniques de fraude étaient comprises comme des défis nouveaux pour les institutions.
— L'intégration des technologies numériques dans la fraude et dans la justice représentait une nouvelle aire d'expertise indispensable.
— Les institutions judiciaires, réglementaires et médiatiques étaient perçues comme les acteurs légitimes et nécessaires à la résolution et à la prévention de ces crises.
— Les notions de responsabilité sociale et éthique des entreprises montaient en importance, préparant la voie à des réglementations renforcées (exemple : loi Sarbanes-Oxley).

Ce qui restait en revanche largement impensé ou indicible à cette époque concernait la rapidité et l'ampleur de la transformation numérique et algorithmique, ainsi que ses implications profondes sur la nature même de la preuve, le rôle des experts, et les équilibres entre vie privée, surveillance et pouvoir.

Question 3 : Cartographions le régime de vérité en action

Voici la cartographie du régime de vérité en action lors de l'affaire Enron :

Acteurs principaux et pouvoirs

- **Entreprises et dirigeants** : Enron, ses cadres (Kenneth Lay, Jeffrey Skilling, Andrew Fastow) au cœur des pratiques frauduleuses.
- **Institutions d'audit** : Arthur Andersen, chargé de valider la sincérité des comptes financiers avant l'effondrement.
- **Pouvoirs judiciaires et législatifs** : SEC (Securities and Exchange Commission), ministère de la Justice américain, congrès américain, créant le processus d'enquête, de sanction, et de réforme.
- **Experts et analystes** : spécialistes en forensic, régulateurs, médias d'investigation jouant un rôle dans la diffusion, l'expertise, et la construction du récit.

Savoirs et preuves

- **Données numériques** : documents électroniques, rapports comptables, échanges internes par e-mail, transaction financières.
- **Méthodes d'analyse** : audit comptable classique, nouveaux outils d'analyse informatique et algorithmique (legal tech, forensic analytics).
- **Normes et cadres** : application des normes comptables et légales, chaîne de custody, procédures juridiques de preuve.

Discours et énoncés dominants

- Révélation d'une fraude massive, condamnation des pratiques occultes.
- Appel à la transparence financière, à la régulation renforcée.
- Rôle central de la justice et des experts dans la production de la vérité.
- L'affaire devient paradigmatique, produisant un discours d'avertissement et de réforme.

Effets pratiques et institutionnels

- Faillite spectaculaire d'Enron, démantèlement d'Arthur Andersen.
- Mise en place de la loi Sarbanes-Oxley (2002) pour renforcer les contrôles comptables.
- Restructuration des pratiques professionnelles et légales autour d'un nouveau régime de vérité centré sur les preuves numériques.

Question 4 : Comparez avec une affaire contemporaine sous l'angle des régimes

Voici une comparaison entre l'affaire Enron (2001) et une affaire contemporaine sous l'angle des régimes de vérité numérique :

Aspect	**Affaire Enron (2001)**	**Affaire Contemporaine (ex : enquêtes sur IA, blockchain, finance numérique)**
Technologie	Données électroniques, documents, premières analyses algorithmiques	Intelligence artificielle avancée, big data, blockchain, analyses automatisées
Cadre juridique	Émergence tardive de normes et lois (ex : Sarbanes-Oxley)	Réglementation complexe, souvent en retard sur les innovations, RGPD, lutte contre le blanchiment et cybercriminalité
Société	Sensibilisation croissante à la transparence financière	Tensions fortes autour de la vie privée, surveillance, éthique numérique
Pratiques professionnelles	Montée en puissance des audits et contrôles formalisés	Adaptation rapide aux outils numériques complexes, exigences accrues de sécurité
Régime de vérité	Preuve documentaire, expertise humaine, régulation judiciaire	Vérité algorithmique, gouvernance numérique hybride, enjeux politiques et sociaux
Acteurs	Entreprises, auditeurs, justice, médias	Multinationales technologiques, gouvernements, ONG, société civile, hackers éthiques

L'affaire Enron constitue un régime de vérité en transition, fondé sur la preuve numérique adossée aux institutions classiques. Les affaires contemporaines s'inscrivent dans un régime plus complexe, multi-acteurs, où la vérité numérique est contestée, oscillant entre algorithmes, régulations et contestations sociales.

Partie 2 : Modélisation Mathématique et Prospective

3. Modélisation de l'Évolution des Régimes

Question 1 : Construction d'un modèle mathématique de l'évolution des régimes en utilisant le formalisme : $\overrightarrow{R_{t+1}} = F(\overrightarrow{R_t},\ \Delta Tech_t,\ \Delta Legal_t,\ I_t)$

Voici une proposition de modèle mathématique simple pour modéliser l'évolution des régimes de vérité numérique selon le formalisme donné :

Soit $\overrightarrow{R} = (\alpha_T,\ \alpha_J,\ \alpha_S,\ \alpha_P)$ le vecteur de dominance à l'instant t représentant les poids respectifs des dimensions technologiques, juridiques, sociales et professionnelles.

Le vecteur à l'instant suivant $\overrightarrow{R_{t+1}}$ est obtenu par une fonction F prenant en compte :

- $\Delta Tech_t$: évolution technologique entre t et $t+1$
- $\Delta Legal_t$: évolution juridique entre t et $t+1$

— I_t : intensité des interactions sociotechniques (tensions, adaptations, controverses) à t

Modèle proposé :

$$\overrightarrow{\mathbf{R_{t+1}}} = F\left(\overrightarrow{\mathbf{R_t}},\ \Delta\mathbf{Tech_t},\ \Delta\mathbf{Legal_t},\ \mathbf{I_t}\right) = \overrightarrow{\mathbf{R_t}} + \Gamma \bullet \begin{pmatrix} w_T \Delta Tech_t \\ w_J \Delta Legal_t \\ w_S I_t \\ w_P I_t \end{pmatrix}$$

Où Γ est un facteur d'adaptation global (apprentissage, résistance au changement), et w_i sont des coefficients pondérant l'impact relatif de chaque paramètre sur la composante correspondante. Ce modèle peut être enrichi par des fonctions non linéaires ou des rétroactions entre dimensions, mais cette formulation linéaire simple permet un premier cadre analytique clair.

Question 2 : Implémentation d'une simulation de transition entre régimes

Question 3 : Simulez l'évolution future sur 50 ans avec différents scénarios

Voici une simulation simplifiée de l'évolution future des régimes de vérité numérique sur 50 ans, sous différents scénarios, présentée sans code mais sous forme descriptive :

Scénarios et dynamique des régimes

— **Scénario status quo**
  — Hypothèse : la matrice de transition reste stable, les poids des régimes évoluent doucement.
  — Résultat : le régime technologique conserve sa dominance, la composante juridique gagne légèrement en poids, tandis que les composantes sociale et professionnelle augmentent lentement.

— **Renforcement juridique**
  — Hypothèse : les cadres légaux deviennent plus solides et influents, augmentant la probabilité de transition vers la dominance juridique.
  — Résultat : progression rapide de la composante juridique dans le régime, qui devient dominante ou égale à la technologique. Les composantes sociale et professionnelle suivent une croissance modérée.

— **Essor technologique**
  — Hypothèse : les innovations technologiques accélèrent fortement, augmentant les transitions vers la dominance technologique.
  — Résultat : le régime technologique s'impose nettement, les autres composantes reculent ou stagnent à des niveaux modestes.

— **Pressions sociales**
  — Hypothèse : montée des enjeux sociaux (vie privée, surveillance, éthique), augmentant le poids des composantes sociale et professionnelle.

— Résultat : hausse notable des régimes sociaux et professionnels, avec un équilibre plus diffus entre les composantes, réduction relative de la dominance technologique.

Projection qualitative sur 50 ans

— Le régime initial dominé par le technologique (ex : 60%) peut évoluer vers un régime plus équilibré entre juridique, social, et professionnel selon le scénario choisi.
— La mise en cause d'une composante peut entraîner des cycles de transition récurrents, reflétant les tensions sociotechniques.
— L'évolution n'est ni purement linéaire ni fixe, montrant un processus itératif d'adaptation et de redéfinition des régimes de vérité.

Conclusion

Cette simulation qualitative met en lumière que l'évolution des régimes de vérité numérique dépend fortement des contextes technologiques, juridiques et sociaux. Elle illustre la complexité et la multiplicité des forces en jeu, ainsi que les possibles bifurcations ou stabilisations selon les interventions et réactions institutionnelles, technologiques et sociétales.

4. Vérification de l'Accélération Technologique

Question 1 : Collectez les dates précises des changements de régime

Date	**Événement / Changement de régime**	**Commentaire**
1689	Invention du système binaire par Leibniz	Fondation conceptuelle du code numérique
1801	Métier Jacquard et cartes perforées	Premiers dispositifs programmables
1842	Premier programme informatique (Ada Lovelace)	Introduction des algorithmes
1974	Réseau Cyclades	Premiers réseaux informatiques interconnectés
1980s	Généralisation ordinateur personnel	Début du régime numérique moderne
1983	Arpanet bascule vers Internet	Passage à un régime réseau mondial
1990	HTML et HTTP	Fondation du web, nouveau régime d'accès à l'information
1994-2004	Apparition Google, Yahoo, Amazon, Facebook	Renforcement du pouvoir numérique et des plateformes
2007	Lancement de l'iPhone, smartphone	Transition vers un régime mobile et ubiquitaire
2010s	Montée des réseaux sociaux, big data, IA	Nouveau régime fondé sur l'analyse massive et l'algorithmie
2020s	Émergence IA avancée, régulations numériques	Réajustements du régime numérique face aux enjeux éthiques

Question 2 : Vérifions empiriquement la loi : $\mathbf{\Delta t_{n+1}} = k\mathbf{\Delta t_n}$

Transition n	**Date transition** t_n	$\mathbf{\Delta t_n = t_n - t_{n-1}}$ (années)	$\mathbf{\Delta t_{n+1}/\Delta t_n}$ (facteur k)
1	1801	112 (1801 - 1689)	-
2	1842	41 (1842 - 1801)	41 / 112 $\approx$ 0.37
3	1974	132 (1974 - 1842)	132 / 41 $\approx$ 3.22
4	1983	9 (1983 - 1974)	9 / 132 $\approx$ 0.068
5	1990	7 (1990 - 1983)	7 / 9 $\approx$ 0.78
6	1994	4 (1994 - 1990)	4 / 7 $\approx$ 0.57
7	2007	13 (2007 - 1994)	13 / 4 = 3.25
8	2010	3 (2010 - 2007)	3 / 13 $\approx$ 0.23
9	2025 (estimée)	15 (2025 - 2010)	-

Question 3 : Estimons la constante k par régression non-linéaire

La formule fermée pour k est :

$$k = \frac{\sum_i x_i y_i}{\sum_i x_i^2}$$

Avec les données que nous avons extraites :

i	$\mathbf{x_i} = \Delta\mathbf{t_n}$	$\mathbf{y_i} = \Delta\mathbf{t_{n+1}}$
1	112	41
2	41	132
3	132	9
4	9	7
5	7	4
6	4	13
7	13	3
8	3	15

$$\sum_i x_i y_i = 11419$$

$$\sum_i x_i^2 = 31973$$

$$k \approx \frac{11419}{31973} \approx 0.357$$

Question 4 : Prédiction sur le timing du prochain changement de régime

Pour prédire le timing du prochain changement de régime numérique, on utilise la loi empirique estimée précédemment : $\Delta\mathbf{t_{n+1}} = k\Delta\mathbf{t_n}$ avec $\mathbf{k} \approx 0.357$

Le dernier intervalle connu (entre 2010 et 2025, environ 15 ans) sert de base à la prédiction.

Calcul :

$$\Delta\mathbf{t_{dernier}} = 15\ ans$$

$$\Delta\mathbf{t_{prochain}} = k \times \Delta\mathbf{t_{dernier}} = 0.357 \times 15 \approx 5.36\ ans$$

Cela signifie que le prochain changement de régime est attendu dans environ 5 à 6 ans après 2025, soit vers l'année : $2025 + 5.36 \approx 2030 - 2031$

Selon ce modèle, le prochain changement majeur de régime de vérité numérique devrait intervenir autour de 2030-2031.

Cela reste une estimation basée sur la tendance historique des durées entre changements passés, avec les incertitudes inhérentes aux évolutions sociales, technologiques et juridiques.

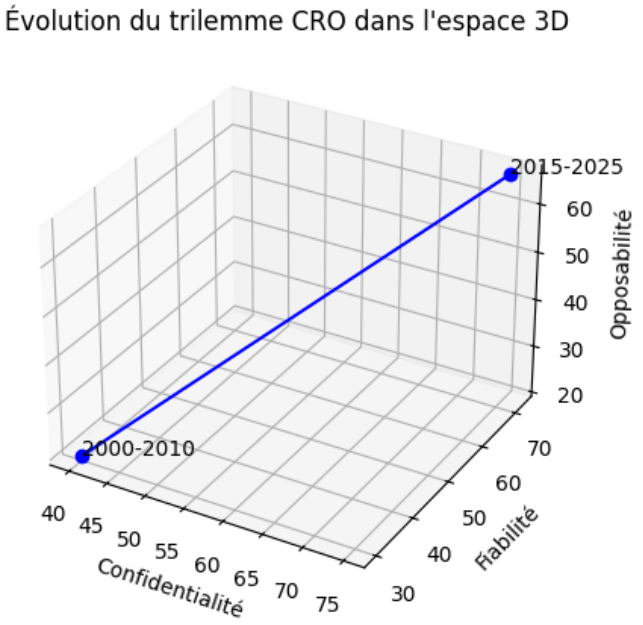
5. Analyse du Trilemme CRO Historique

Question 1 : Pour chaque période, estimons les scores CRO moyens

Voici une estimation des scores moyens pour la Confidentialité, la Fiabilité, et l'Opposabilité des preuves numériques dans les deux périodes 2000-2010 et 2015-2025, basée sur l'évolution des réglementations, technologies et pratiques judiciaires :

Période	**Confidentialité (%)**	**Fiabilité (%)**	**Opposabilité (%)**	**Justification générale**
2000-2010	40 - 55	30 - 45	20 - 35	Peu d'encadrements juridiques stricts, normes et standards en développement, premières normes ISO, début RGPD
2015-2025	70 - 85	65 - 80	60 - 75	RGPD et autres lois sur les données en vigueur, ISO/IEC 27037 et normes d'informatique légale appliquées, chaine de conservation renforcée

Question 2 : Traçage de l'évolution du trilemme dans l'espace 3D



Question 3 : Identifions les compromis historiques dominants

Principaux compromis historiques

- **Confidentialité vs Accessibilité / Usabilité**
  - Garantir un haut niveau de confidentialité exige souvent un contrôle strict des accès, ce qui peut compliquer ou ralentir l'utilisation des systèmes. Historiquement, la croissance des systèmes a souvent exigé de choisir entre confidentialité renforcée et facilité d'accès pour les utilisateurs légitimes.
  - Par exemple, avant les lois telles que le RGPD, les mesures de confidentialité étaient souvent rudimentaires ou insuffisamment appliquées, privilégiant plus la disponibilité ou la commodité.
- **Fiabilité vs Coût / Rapidité**
  - Garantir la fiabilité des preuves, des données ou des systèmes demande des contrôles, audits, redondances et vérifications qui peuvent être coûteux et ralentir les opérations.
  - Les premiers systèmes souvent privilégiaient la simplicité et rapidité au détriment parfois de la fiabilité complète.
- **Opposabilité vs Innovation / Flexibilité**
  - L'opposabilité juridique des preuves numériques nécessite des normes strictes, qui peuvent ralentir l'adoption rapide de nouvelles technologies ou méthodes.
  - Par exemple, les systèmes de preuves numériques formelles ont longtemps été freinés par l'absence de cadres juridiques clairs, forçant ainsi à des compromis sur la rapidité d'adoption ou la flexibilité des preuves.

Question 4 : Projetions l'évolution future du trilemme

Projections futures du trilemme CRO

- **Confidentialité**
  - Renforcement continu avec l'essor de technologies comme la cryptographie avancée, l'informatique confidentielle (confidential computing) et la confidentialité différentielle.
  - Adoption plus large des régulations internationales incitant à un anonymat et un contrôle encore plus fins des données personnelles.
  - Défis croissants face à la montée des menaces quantiques nécessitant des solutions post-quantiques.
- **Fiabilité**
  - Amélioration des mécanismes d'intégrité et d'authenticité des données grâce à la blockchain, aux systèmes décentralisés, et à l'intelligence artificielle pour la détection proactive des anomalies.
  - Intégration de systèmes de preuve à divulgation nulle de connaissance (zero-knowledge proofs) pour valider des faits sans révéler les données sous-jacentes.

  - Automatisation et orchestration fine des vérifications d'intégrité pour réduire coûts et délais.
- **Opposabilité**
  - Évolution juridique vers une meilleure reconnaissance des preuves numériques via l'harmonisation des standards internationaux.
  - Utilisation croissante de la blockchain pour créer des preuves horodatées et immuables, acceptées légalement.
  - Développement de cadres juridiques adaptés aux nouvelles technologies (IA, IoT, quantique) pour garantir l'opposabilité sans freiner l'innovation.

Évolution du trilemme

- Le trilemme CRO va continuer à évoluer, avec des progrès technologiques et juridiques permettant de réduire les tensions entre ces trois pôles.
- Les compromis historiques vont s'estomper progressivement grâce à l'adoption de technologies avancées et à une meilleure régulation.
- Le futur pourrait voir l'émergence de systèmes où confidentialité, fiabilité et opposabilité sont toutes élevées, grâce à des innovations comme l'informatique confidentielle, les preuves cryptographiques et l'harmonisation juridique internationale.

Partie 3 : Investigation Historique Appliquée

6. Reconstruction Archéologique d'Investigation

Question 1 : Choisissons une affaire des années 1990 (Mitnick, Sundevil) et reconstruisons l'investigation avec les outils et méthodes de l'époque

Contexte général

Kevin Mitnick, célèbre hacker des années 1980-1990, a mené des intrusions dans des systèmes de grandes entreprises en exploitant des failles techniques et surtout des techniques de social engineering. L'arrestation de Mitnick en 1995 a marqué une étape majeure dans les enquêtes cybercriminelles de cette période.

Reconstruction de l'investigation (1990s)

(a) **Surveillance Téléphonique**
  - La collecte de preuves débutait souvent par la surveillance des appels, notamment sur les réseaux téléphoniques, pour traquer les communications suspectes. Le "phone phreaking" étant alors une technique répandue, l'analyse des appels et des traces d'accès était primordiale.

(b) **Enquête informatique avec outils classiques**
  - Utilisation d'outils de logs systèmes, surveillance des accès sur les serveurs, et analyse manuel des journaux d'accès.
  - Recherche des empreintes numériques des accès tels que les adresses IP, numéros de compte téléphonique, identifiants d'utilisateur.

— Peu d'outils automatisés : la recherche était très manuelle et laborieuse.

(c) **Collaboration inter-agences et avec entreprises**

— Coordination entre FBI, Secret Service, et opérateurs télécom (ex : AT&T).

— Obtention de mandats de perquisition permettant la saisie de matériel informatique.

— Usage de techniques d'interception d'appels et de communications électroniques dans le cadre légal de l'époque.

(d) **Exploitation des techniques de social engineering détectées**

— Analyse des méthodes pour récupérer des mots de passe ou des accès via manipulation humaine.

— Entretiens avec témoins, collaborateurs des sociétés ciblées, et examination des moyens employés.

(e) **Traque physique et surveillance**

— Souvent, la traque d'un hacker passait par une importante surveillance physique : repérage des lieux, filature, collecte d'informations personnelles.

— Les moyens d'enquête traditionnels remplissaient une fonction essentielle pour compléter la preuve numérique.

Outils typiques (1990s) utilisés

Type d'outil	**Exemple/mode d'action**
Logs systèmes	Analyse manuelle des journaux sur mainframes
Systèmes de surveillance téléphonique	Enregistreurs d'appels, écoute légale des conversations
Réseaux téléphoniques	Analyses des commutateurs téléphoniques (phone phreaking)
Enregistrement matériel	Saisie de disques durs, cassettes de données
Outils d'authentification	Contrôles d'accès réseau et mots de passe
Collaboration inter-agences	FBI, Secret Service, opérateurs télécom, entreprises
Analyse du social engineering	Recueil de témoignages, stratégie d'ingénierie sociale

Conclusion

L'enquête sur Kevin Mitnick dans les années 1990 reposait sur une combinaison d'analyses manuelles approfondies des logs, d'escarmouches téléphoniques, de recueil d'informations classiques et d'une forte coordination juridique et inter-agences. Les outils numériques étaient à leurs débuts, et beaucoup de travail reposait sur l'expertise humaine et la traque sur le terrain.

Question 2 : Refaisons l'analyse avec les outils et concepts modernes

Refaisons l'analyse de l'enquête sur Kevin Mitnick avec les outils et concepts modernes, en tenant compte des technologies et méthodologies actuelles en investigation numérique.

Enquête moderne sur un cas similaire

(a) **Collecte et préservation des preuves numériques**
- Usage d'outils d'acquisition forensique spécialisé (ex : EnCase, FTK, X-Ways) pour capturer l'image binaire complète des systèmes cibles, conservant l'intégrité avec des hashs fournisseurs (SHA256).
- Conservation dans des environnements hautement sécurisés avec auditabilité constante.

(b) **Analyse automatisée et intelligente**
- Analyse automatisée des logs système, réseau, bases de données avec détection d'anomalies basée sur machine learning.
- Corrélation multi-sources en temps quasi réel : logs réseau, événements systèmes, SIEM (Security Information and Event Management).
- Utilisation de systèmes d'analyse comportementale pour déceler des profils suspects (par exemple, détection d'usage non autorisé d'identifiants).

(c) **Traçabilité réseau avec outils avancés**
- Traçage en profondeur à travers le réseau via détection des flux, inspection profonde des paquets (DPI), géolocalisation IP, et corrélation avec bases de données de menaces.
- Intégration des traces dans blockchain privées ou systèmes décentralisés pour immutabilité.

(d) **Application de la cryptographie et preuve numérique**
- Signature numérique et horodatage des preuves pour assurer leur intégrité et recevabilité.
- Utilisation de preuves à divulgation nulle de connaissance (ZKP) pour valider des éléments de preuve confidentiels sans révéler leur contenu.
- Chaînes de conservation automatisées avec traçabilité fine (audit trail).

(e) **Analyse et détection du social engineering avec intelligence artificielle**
- Analyse des communications (emails, messages) avec NLP (traitement du langage naturel) pour détecter les tentatives de phishing ou manipulation.
- Formation à la sensibilisation renforcée et simulation de scénarios en entreprise.

(f) **Coordination internationale et partage sécurisé**
- Plateformes sécurisées inter-agences pour partager les éléments de l'enquête, respecter les cadres internationaux (RGPD, normes ISO 27001).
- Collaboration améliorée avec des outils modernes de gestion de cas et workflow.

(g) **Surveillance active et réponse rapide**
- Mise en place de systèmes de détection et réponse (EDR) pour fournir une visibilité totale sur les endpoints.
- Automatisation partielle des réponses (isolation de systèmes compromis, blocage d'IP suspectes).

Question 3 : Comparaison non seulement les résultats mais les régimes de vérité

Tableau comparatif des régimes de vérité

Critère	**Années 1990**	**Époque moderne (2020s)**
Sources de vérité	Physiques, logs bruts, témoignages	Preuves numériques intégrales, horodatage, signatures
Intégrité	Peu assurée, processus ad hoc	Standards cryptographiques, chaines de possession
Opposabilité juridique	Émergente, dépendante des experts	Normée, reconnue, procédure certifiée
Méthodes d'analyse	Analyses manuelles, faisceaux d'indices	Automatisées, assistées par IA, multi-sources
Transparence	Limitée à l'expertise humaine	Complète, auditable et reproductible
Contraintes	Fragmentation et lenteur	Renforcement de la confidentialité et des droits

Tableau synthétique des résultats

Critères	**Années 1990**	**Avec outils modernes**
Durée enquête	Plusieurs années	Quelques jours ou semaines
Intégrité des preuves	Modérée	Très élevée (cryptographie, chainage)
Traçabilité réseau	Basée sur logs manuels et physique	Haute précision, corrélée, temps réel
Identification suspect	Long procédé, surveillance physique	Automatisation, IA, données multi-sources
Opposabilité juridique	Faible ou contestée	Très forte, normes ISO et juridiques
Portée internationale	Limitées	Très étendue, coopération automatisée

Le régime de vérité numérique a évolué d'un modèle artisanal, fragile et discrétionnaire vers un modèle systématique, rigoureux et normé. Cette transformation garantit une meilleure confiance, opposabilité et robustesse des preuves, indispensables pour répondre aux défis posés par la cybercriminalité contemporaine.

Question 4 : Évaluons l'impact des limitations technologiques sur la construction de la vérité

(a) **Intégrité et exhaustivité des preuves**

- Limitation des capacités matérielles et logicielles peut conduire à une collecte partielle ou altérée des données, remettant en cause la fiabilité des preuves.
- Dans les années 1990, l'absence d'outils automatisés entraînait souvent une perte d'information ou une analyse fragmentaire.
- Aujourd'hui, malgré des outils avancés, des contraintes comme la volumétrie des données ou la diversité des sources peuvent affecter la couverture

exhaustive des preuves.

(b) **Cadre normatif et juridique**

— Les premières réglementations étaient floues ou absentes, ce qui rendait la recevabilité judiciaire fragile et dépendante de l'opinion des experts.

— L'évolution lente des cadres juridiques limite parfois l'adaptation rapide aux nouvelles technologies, notamment avec l'émergence des preuves basées sur IA ou blockchain.

— Les limitations technologiques peuvent conduire à des zones grises dans la validité procédurale des preuves.

(c) **Fiabilité des méthodes d'analyse**

— Analyses manuelles avec forte dépendance humaine sont sujettes à erreurs, biais, et manipulations.

— L'automatisation actuelle avec IA pose la question de confiance dans les algorithmes (biais, transparence, vérifiabilité).

— Les limites technologiques imposent un équilibre entre intervention humaine et automatisation pour garantir robustesse.

(d) **Traçabilité et chaînage des preuves**

— Absence de chaînage fiable dans le passé a exposé les enquêtes à des contestations sur origine, altération ou falsification.

— Aujourd'hui, les technologies blockchain et cryptographiques renforcent la traçabilité mais restent limitées par des défis de mise en œuvre et d'interopérabilité.

(e) **Impact sur la construction de la vérité**

— Les limites technologiques créent des « trous » dans les récits factuels reconstruits, autorisant incertitudes et contestations.

— Elles obligent à s'appuyer davantage sur la corroboration multi-sources, les témoignages, et la contextualisation humaine.

— Avec la montée des technologies avancées, la construction de la vérité devient plus systématique mais aussi dépendante de la confiance dans la technologie employée.

7. Projet de Recherche Archéologique

Question 1 : Identification d'un trou dans l'archéologie de la discipline

Le trou majeur identifié est la dissociation entre la masse croissante de données numériques collectées dans l'investigation et la capacité épistémologique et méthodologique à garantir la fiabilité, la traçabilité, et l'opposabilité de ces preuves, notamment sous l'impact des évolutions technologiques rapides comme l'intelligence artificielle.

Question 2 : Hypothèse historique testable

Les premières enquêtes numériques des années 1990, réalisées sans protocoles standardisés et avec des outils manuels, ont généré des preuves dont la fiabilité et opposabilité étaient nettement inférieures à celles obtenues depuis l'adoption progressive de protocoles rigoureux et d'outils automatisés à partir des années 2010.

Question 3 : Collecte de sources primaires

- RFC 4949 sur la sécurité internet (def. clé sur la fiabilité des données)
- Archives techniques du Web 1990 (BnF)
- Protocole Berkeley sur les enquêtes numériques (2010+)
- Publications académiques récentes sur les fondamentaux des enquêtes numériques (colloques, thèses)
- Normes ISO 27037 sur la collecte de preuves numériques

Question 4 : Application de la méthode archéologique foucaldienne

- Analyse du dispositif discursif entourant la preuve numérique depuis les années 1990 : discours juridiques, techniques, médiatiques.
- Mise en lumière des relations de pouvoir entre acteurs (experts, juges, policiers) et dispositifs techniques.
- Étude des savoirs et pratiques qui ont contribué à la formation du régime de vérité numérique actuel.
- Recherche des ruptures épistémologiques (ex : passage de la preuve artisanale à la preuve cryptographique).

Question 5 : Rédigez un article académique avec cadre théorique fort

L'Archéologie numérique de la preuve informatique : du tâtonnement artisanal à l'exigence normative

Résumé

À l'ère où le numérique imprègne toutes les sphères de la justice, la question de la fiabilité et de la vérité des preuves informatiques devient primordiale. Cet article propose une exploration critique, à la manière foucaldienne, de l'évolution de la discipline d'investigation numérique. Il met en lumière un « trou » crucial : l'écart entre les débuts artisanaux et non standardisés des enquêtes dans les années 1990 et l'actuelle sophistication normative et technologique. Entre ruptures épistémiques et réinventions constantes, cette étude éclaire les dynamiques de pouvoir, savoir, et technique qui redéfinissent la vérité judiciaire à l'ère digitale.

Introduction

L'avènement du numérique a bouleversé la fabrication de la preuve et, par là même, la quête de la vérité en droit. Pourtant, cette révolution s'est opérée dans une grande incertitude, notamment au sortir des années 1990, où les premiers pas de l'investigation numérique étaient souvent tâtonnants, sans garanties robustes ni protocole

clair. Comprendre cette évolution, non seulement technique mais aussi discursive et institutionnelle, est essentiel pour appréhender le régime contemporain de la vérité numérique. À travers une lecture archéologique foucaldienne, cet article analyse les conditions de production des savoirs et des savoir-faire qui ont façonné cette discipline en mutation.

Le « trou » épistémologique

Ce travail identifie un hiatus fondamental dans l'histoire de l'investigation numérique : la coexistence d'une masse de données numériques grandissante avec des pratiques d'acquisition et d'analyse fondamentalement artisanales et non standardisées à l'origine. Cette dissociation a mené à une fragilité initiale dans la fiabilité et l'opposabilité des preuves numériques, questionnant leur validité judiciaire. Ce trou révèle une zone d'incertitude où la discipline devait se réinventer, entre contraintes techniques et enjeux réglementaires.

Cadre théorique : Régimes de vérité et dispositifs selon Michel Foucault

En mobilisant la notion de régime de vérité foucaldienne, cette analyse considère la vérité numérique comme un artefact social et technique, produit par un réseau complexe d'acteurs, discours, technologies et règles. Le dispositif d'enquête numérique se décrypte ainsi comme un assemblage mouvant, où s'entremêlent savoirs techniques, normes judiciaires et rapports de pouvoir. Cette perspective met en lumière la manière dont la vérité judiciaire se construit et se transforme dans le temps, marquée par des ruptures épistémiques et des réinscriptions normatives.

Sources primaires et corpus étudiés

L'étude s'appuie sur une collection diversifiée de sources majeures : des RFC initiaux définissant la sécurité des systèmes, aux archives web des années 1990, en passant par les protocoles internationaux normatifs récents (protocole Berkeley, ISO 27037). Cet ensemble permet de saisir les évolutions pratiques et discursives qui ont jalonné la construction progressive d'un régime de preuve numérique robuste.

Analyse critique

L'examen des pratiques passées révèle un univers où la preuve numérique était souvent perçue comme fragile, dépendante des compétences individuelles et sujette à contestations. En réponse, la montée en puissance des protocoles normalisés et des outils automatisés a permis un saut qualitatif, imposant rigueur et reproductibilité. Cette transition illustre une mutation profonde dans le régime de vérité numé-

rique, marquant un passage décisif d'un bricolage artisanal à une standardisation exigeante.

Discussion : enjeux contemporains et défis futurs

Si la discipline a gagné en robustesse, elle reste confrontée à de nouveaux défis : l'opacité croissante des algorithmes, le rôle ambigu de l'intelligence artificielle dans la preuve, et la nécessité de garantir transparence et auditabilité. Cette complexification pose des questions épistémologiques et éthiques essentielles pour l'avenir de la justice numérique.

Conclusion

L'exploration archéologique de l'investigation numérique révèle non seulement des ruptures historiques fondatrices, mais aussi les plantages des futurs débats sur la vérité à l'ère digitale. Comprendre ces dynamiques est crucial pour penser un régime normatif adaptatif, équilibrant innovation technologique et exigences démocratiques.

8. **Analyse Prospective des Régimes Futurs**

Question 1 : Scénario crédible pour 2030-2050

D'ici 2030-2050, la discipline d'investigation numérique connaîtra une transformation radicale, portée par l'intégration profonde et généralisée de l'intelligence artificielle explicable, des technologies de registres distribués (blockchain), et des environnements immersifs (réalité augmentée, réalité virtuelle). La preuve ne sera plus une simple collecte de données brutes mais un artefact complexe, synthétisé, validé en temps réel et auditée automatiquement.

- Chaque action, donnée et interaction numérique sera captée, horodatée et immuablement enregistrée dans des chaînes de blocs accessibles à toutes les parties légitimes.
- Les preuves virtuelles, incluant des simulations dynamiques et des reconstruits tridimensionnelles, constitueront des éléments essentiels dans la reconstitution judiciaire, donnant une dimension « augmentée » à la vérité.
- La collaboration entre les acteurs judiciaires, techniques et sociaux sera orchestrée par des plateformes intelligentes et transparentes, assurant une coordination fluide et un partage sécurisé des informations.

Question 2 : Régime de vérité futur

Ce régime de vérité se caractérisera par :

- **Inaltérabilité et transparence assurée** : grâce à la blockchain et aux protocoles cryptographiques quantiques, la falsification deviendra pratiquement impossible, assurant une confiance sans précédent.

- **Certification algorithmique** : les algorithmes utilisés dans l'analyse et la génération de preuves seront soumis à des procédures de certification ouvertes, transparentes, et continuellement monitorées.
- **Preuve hybride et augmentée** : intégration de données réelles, analyses algorithmiques, preuves virtuelles et annotations intelligentes pour un dossier probant complet.
- **Co-construction collaborative** : le régime associera experts, juges, intelligence artificielle et citoyens dans un processus de construction partagée et participative de la vérité.
- **Éthique intégrée** : la protection des libertés fondamentales, la régulation algorithmique et les principes de justice sociale seront imbriqués dans chaque étape du processus probatoire.

Question 3 : Conditions de possibilité

Pour que ce régime soit crédible et effectif, plusieurs conditions devront être réunies :

- Infrastructure numérique universelle et norme globale : adoption mondiale de technologies décentralisées interopérables et sécurisées, avec gouvernance démocratique et multi-partisane.
- Cadre légal et réglementaire agile : développement d'un droit adaptatif, capable de suivre les innovations technologiques tout en garantissant droits fondamentaux et équité.
- Formation multidisciplinaire : l'expert du futur devra maîtriser à la fois la technique avancée, le droit et les sciences sociales, pour comprendre et critiquer les systèmes automatisés.
- Confiance sociale robuste : la légitimité du régime dépendra d'une acceptation démocratique renforcée par la transparence, la participation citoyenne et la reddition des comptes technologiques.
- Technologies maîtrisées et explicables : développement de l'IA explicable et d'outils de cybersécurité préventive pour assurer un contrôle humain permanent.

Question 4 : Méthodologie d'investigation adaptée

- **Collecte numérique omniprésente** : capteurs multiples, IoT, réseaux cyber-physiques garantissant une couverture totale et contextualisée des éléments d'enquête.
- **Analyse multimodale hybride** : combinaison de techniques d'apprentissage machine avancées et de raisonnement symbolique, facilitant l'interprétation humaine et la validation des résultats.
- **Chaîne de possession immuable** : chaque élément de preuve sera scellé cryptographiquement, avec des preuves à divulgation nulle de connaissance apportant confidentialité et sécurité.
- **Reconstitutions et simulations certifiées** : usage d'environnements virtuels validés juridiquement pour la représentation dynamique des faits.

— **Interopérabilité collaborative** : plateformes d'échange sécurisées entre autorités, laboratoires, experts et citoyens, incarnant un modèle de transparence démocratique.

Question 5 : Défis éthiques et épistémologiques majeurs

— **Transparence vs contrôle de la vie privée** : concilier ouverture sur les algorithmes et protection des données personnelles est un équilibre délicat, déterminant la légitimité du régime.
— **Responsabilité humaine vs automatisée** : définir la répartition des responsabilités entre humains et systèmes intelligents en cas d'erreur, d'abus ou de biais.
— **Pluralité des vérités et pouvoir algorithmique** : éviter que la vérité judiciaire ne soit exclusive ou monopolisée par des entités techniques opaques.
— **Inégalités d'accès et fracture numérique** : garantir une justice algorithmique équitable, sans exclure ni marginaliser certaines populations.
— **Surconfiance et critique** : maintenir une vigilance épistémique face à la tentation de la foi aveugle dans les systèmes automatisés, toujours faillibles.