Ecole Nationale Supérieure Polytechnique
Département de Génie Informatique
Cybersécurité et Investigation Numérique (CIN) Niveau 4

EPREUVE D'INTRODUCTION AUX TECHNIQUES D'INVESTIGATION NUMERIQUE

GUIDE DE CORRECTION

Enseignant : Thierry MINKA.
Durée : 3h

Le sujet est constitué de 2 grandes parties. A : des questions ouvertes couvrant l'essentiel du programme de cours et B : une discussion scientifique au choix sur les grands enjeux de l'investigation numérique.

A. Questions ouvertes (80 points)

NB : Chaque question vaut 10 points, gardez ça à l'esprit lorsque vous penserez avoir fourni une réponse complète.

1. Define the term *chain of custody* in the context of digital evidence. Why is it critical in computer forensics*? Référence au cours : Chapitre 2.*

1. Définition claire et précise (3 points) :
- 1 point : Mention de la documentation des étapes de collecte, transfert, stockage et présentation des preuves numériques.
- 1 point : Insistance sur l'objectif de garantir l'intégrité et l'authenticité des preuves.
- 1 point : Inclusion de la notion de standardisation pour assurer la recevabilité légale.
- *Exemple de formulation :* La chaîne de traçabilité consiste en une documentation exhaustive et normalisée qui détaille chaque étape de manipulation des preuves numériques, garantissant leur intégrité et leur authenticité pour leur admissibilité devant un tribunal.

2. Importance de la chaîne de traçabilité (4 points) :
- 1 point : Explication sur le maintien de l'intégrité des preuves (assurance qu'elles n'ont pas été altérées ou modifiées).
- 1 point : Traçabilité des personnes ayant manipulé la preuve (chaque acteur doit être identifié).
- 1 point : Recevabilité légale : la chaîne de traçabilité garantit que les preuves numériques peuvent être utilisées en justice.
- 1 point : Transparence : chaque étape doit pouvoir être vérifiée par un tiers (exemple : empreintes hachées).
- *Exemple de formulation:* La chaîne de traçabilité est essentielle pour garantir que les preuves numériques sont recevables devant un tribunal. Elle assure leur intégrité, identifie les acteurs ayant manipulé les preuves, et offre une transparence totale pour les processus suivis.

3. Prise en compte de la volatilité des données (2 points) :
- 1 point : Mention de la nécessité de capturer en premier les données volatiles (RAM, connexions réseau) avant qu'elles ne disparaissent.
- 1 point : Documentation des outils et méthodes utilisés pour garantir l'intégrité des données volatiles.

- *Exemple de formulation:* Les données volatiles, comme celles en RAM ou les connexions réseau, disparaissent dès que le système est éteint. Leur collecte doit être prioritaire et documentée avec des outils comme Volatility, afin d'assurer leur traçabilité.

4. **Exemple pratique (1 point) :**
   - 1 point : Fournir un exemple concret illustrant la mise en œuvre d'une chaîne de traçabilité.
   - *Exemple de formulation:* Lorsqu'un disque dur est saisi, sa chaîne de traçabilité inclut la date et l'heure de la saisie, l'identité de l'agent collecteur, le numéro de série du disque, la méthode d'imagerie (ex. : FTK Imager), et les empreintes hachées générées avant et après la copie.

2. What are the key challenges of network forensics in identifying and tracking cybercriminals? Suggest two solutions for overcoming these challenges. *Référence au cours : Chapitre 3 et 4.*

1. **Définir les enquêtes réseau (2 points) :**
   - 1 point : Définir ce qu'est une enquête réseau en relation avec les investigations numériques.
   - *Exemple de formulation:* Une enquête réseau consiste à analyser les flux de données circulant sur un réseau informatique afin de détecter, identifier et retracer des activités suspectes ou malveillantes.
   - 1 point : Mentionner leur importance dans le contexte des cyberattaques (exemple : analyse de logs pour identifier les connexions suspectes).
2. **Défis principaux (4 points) :**
   - 1 point : Volume massif de données : Les réseaux modernes génèrent d'énormes volumes de données en temps réel, ce qui complique l'identification des éléments pertinents.
   - 1 point : Chiffrement des communications : Les technologies comme TLS, VPN ou Tor rendent les données inaccessibles sans décryptage, ce qui limite les capacités d'analyse.
   - 1 point : Attribution difficile des activités : Il est complexe de relier une activité malveillante à un utilisateur spécifique (ex. : usurpation d'adresse IP).
   - 1 point : Limites juridiques et organisationnelles : Collaboration restreinte entre juridictions internationales, ou absence de ressources suffisantes pour effectuer l'analyse.

3. **Solutions adaptées (4 points) :**
   - 1 point : Automatisation de l'analyse des données réseau :Utiliser des systèmes de détection d'intrusion (IDS) comme Snort ou Suricata, capables de surveiller les flux en temps réel et d'identifier les anomalies.
   - 1 point : Analyse des journaux réseau : Exploiter les logs des routeurs et des firewalls pour reconstruire la chronologie des événements et identifier les adresses IP suspectes.
   - 1 point : Décryptage des flux chiffrés : Mettre en place des proxys SSL/TLS pour intercepter les communications et analyser les flux chiffrés localement.
   - 1 point : Coopération et ressources :Renforcer la collaboration avec des entités juridiques internationales et des équipes CERT (Computer Emergency Response Team).

3. Describe three types of evidence collected during a forensic investigation and their importance. *Référence au cours : Chapitre 2 et 3.*

1. **Définition générale des preuves numériques (2 points) :**
   - 1 point : Les preuves numériques sont des données collectées sur des appareils électroniques (ordinateurs, téléphones, disques durs, réseaux) pour être utilisées comme éléments de preuve dans une enquête.
   - 1 point : Ces preuves doivent être collectées de manière rigoureuse pour garantir leur intégrité, authenticité et recevabilité légale.

- *Exemple de formulation*: Les preuves numériques englobent des données variées issues de systèmes informatiques et de réseaux. Elles doivent être collectées selon des normes strictes pour éviter toute altération.

2. **Types de preuves collectées (6 points) :**

   Chaque type de preuve doit être expliqué en lien avec sa méthodologie de collecte, son importance et un exemple concret tiré du cours.
   - Données volatiles (2 points) :
     - Définition : Informations temporaires présentes uniquement tant que l'appareil est allumé, comme les processus actifs, les connexions réseau, et la RAM.
     - Importance : Les données volatiles fournissent un instantané des activités en cours, crucial pour identifier des logiciels malveillants, des clés de chiffrement, ou des connexions suspectes.
     - Exemple : Capture de la RAM avec Volatility pour identifier un ransomware actif.
   - Journaux d'activité (logs) (2 points) :
     - Définition : Les logs enregistrent les événements systèmes (ex. : connexions, accès aux fichiers, erreurs). Ils sont générés par les serveurs, applications, routeurs, et firewalls.
     - Importance :
       - Permettent de reconstruire la chronologie des événements.
       - Identifient les activités suspectes ou les violations de sécurité.
     - Exemple : Analyse des logs de connexion d'un serveur avec Splunk pour détecter des tentatives d'accès non autorisées.
   - Preuves physiques (2 points) :
     - Définition : Les preuves physiques incluent les objets matériels utilisés dans la cybercriminalité, tels que disques durs, clés USB, téléphones portables.
     - Importance :
       - Elles contiennent souvent des données numériques cruciales (ex. : fichiers incriminants, emails).
       - Relient les preuves numériques à des individus spécifiques (ex. : empreintes digitales ou données utilisateur).
     - Exemple :Analyse d'un disque dur saisi avec FTK Imager pour extraire une image forensique et vérifier son contenu.

3. **Lien avec la chaîne de traçabilité (2 points) :**
   - 1 point : Insister sur la documentation complète de chaque type de preuve pour garantir leur intégrité.
   - *Exemple de formulation*: Lors de la collecte de RAM, il est nécessaire d'inclure un horodatage précis et l'outil utilisé (ex. : Volatility).
   - 1 point : Mentionner la création d'empreintes hachées pour les preuves physiques (disques durs, clés USB) et leur traçabilité.

4. During live evidence acquisition, what are the key volatile data components that must be captured first? Provide an example for each. *Référence au cours : Chapitre 2.*

1. **Définition des données volatiles (2 points) :**
   - 1 point : Les données volatiles sont des informations présentes en mémoire ou en transit sur un système et qui disparaissent dès qu'il est éteint ou redémarré.
   - 1 point : Ces données doivent être collectées en priorité lors d'une acquisition en temps réel pour garantir leur préservation.
   - *Exemple de formulation* : Les données volatiles incluent les informations contenues dans la mémoire vive (RAM), les processus actifs et les connexions réseau. Elles sont temporaires et nécessitent une collecte rapide pour éviter leur perte.

2. **Ordre de collecte des données volatiles (6 points) :**

Chaque étape doit inclure une explication, son importance, et un exemple tiré du cours.

- RAM (2 points) :
  - Explication : La RAM contient des informations critiques sur les processus en cours, les clés de chiffrement et les données temporaires utilisées par le système.
  - Importance : Ces données disparaissent dès que le système est éteint. Elles permettent d'identifier des logiciels malveillants ou des sessions actives.
  - *Exemple de formulation* :La capture de la RAM à l'aide d'un outil comme Volatility peut révéler des clés de chiffrement ou des indicateurs de compromission (IOC) présents en mémoire.
- Processus actifs (2 points) :
  - Explication : Les processus actifs montrent les programmes en cours d'exécution sur le système, y compris les logiciels légitimes et malveillants.
  - Importance : Fournissent des indications sur les actions en cours, telles que des transferts de fichiers ou des connexions suspectes.
  - *Exemple de formulation* :La commande ps aux sous Linux permet de lister tous les processus actifs, comme un malware tentant de communiquer avec un serveur distant.
- Connexions réseau actives (2 points) :
  - Explication : Les connexions réseau actives montrent les communications en cours entre le système et des serveurs distants.
  - Importance : Permettent d'identifier des adresses IP suspectes ou des serveurs de commande et de contrôle (C2).
  - *Exemple de formulation* :La commande netstat -an peut afficher les connexions TCP/UDP actives et les adresses IP des serveurs distants auxquels le système est connecté.

3. **Lien avec la traçabilité (2 points) :**
   - 1 point : Chaque étape de collecte doit être **documentée**, incluant les outils utilisés, l'heure de capture, et les empreintes hachées des données capturées (ex. : RAM).
   - 1 point : Une documentation complète garantit la recevabilité des données collectées devant un tribunal.
   - *Exemple de formulation* : Lors de la capture de la RAM, l'utilisation de Volatility doit être documentée, avec un horodatage précis et une empreinte hachée SHA256 générée pour vérifier l'intégrité des données.

5. A company suspects an employee of sending sensitive data via email. Outline the steps for conducting an email investigation, including key tools used. *Référence au cours : Chapitre 4.*
   1. **Définition et objectif d'une enquête sur les emails (2 points) :**
      - 1 point : Définir ce qu'est une enquête sur les emails en informatique légale.
      - *Exemple de formulation* : Une enquête sur les emails consiste à analyser les échanges électroniques d'un utilisateur afin de détecter d'éventuelles violations, telles que des fuites de données ou des communications suspectes.
      - 1 point : Mentionner l'objectif principal dans ce contexte : identifier les emails suspects contenant des informations sensibles et collecter des preuves pour confirmer ou infirmer les soupçons.

- **Étapes de l'enquête (6 points) :**
  Chaque étape doit inclure une description, son importance et un outil spécifique recommandé dans le cours.
  - Identification des comptes email suspectés (2 points) :

- Explication : Identifier les adresses email potentiellement impliquées, notamment celles utilisées pour envoyer ou recevoir des données sensibles.
- Importance : Cibler les comptes précis permet de réduire le périmètre de l'enquête et d'éviter d'analyser des données inutiles.
- *Exemple de formulation* :Identifier les comptes de messagerie en fonction des échanges suspectés, par exemple prenom.nom@entreprise.com.

- Extraction des emails suspects (2 points) :
  - Explication : Récupérer les emails en question à partir du serveur ou des archives locales (Outlook PST, sauvegardes, etc.).
  - Importance : Assure que toutes les preuves sont collectées et conservées sans modification.
  - Outils recommandés : FTK Imager pour extraire les fichiers email en préservant leur intégrité.
  - *Exemple de formulation* : Utiliser FTK Imager pour extraire les archives PST d'un compte Outlook ou les messages stockés localement sur le poste de travail.
- Analyse des métadonnées et du contenu des emails (2 points) :
  - Explication : Examiner les métadonnées (expéditeur, destinataire, date d'envoi, adresses IP) et analyser les pièces jointes pour identifier des fuites de données.
  - Importance : Les métadonnées permettent de retracer l'origine et le chemin de l'email, tandis que le contenu confirme la nature des informations divulguées.
  - Outils recommandés : MailXaminer ou Magnet AXIOM pour analyser les métadonnées et le contenu.
  - *Exemple de formulation* : Analyser les adresses IP pour identifier l'origine des messages et vérifier les pièces jointes suspectes avec MailXaminer.

2. **Documentation et traçabilité (2 points) :**
   - 1 point : Chaque étape doit être documentée dans un journal, incluant les outils utilisés et les empreintes hachées des emails récupérés.
   - 1 point : Mentionner la création d'un rapport détaillé pour présenter les résultats de l'enquête.
   - *Exemple de formulation* : Documenter l'extraction des emails avec des empreintes hachées SHA256 pour garantir leur intégrité, et inclure les résultats dans un rapport final destiné au responsable de l'enquête.

6. Expliquez l'importance du journal des activités (*log*) dans une enquête numérique. Comment ces journaux peuvent-ils être manipulés par des attaquants, et comment s'en prémunir ? *Référence au cours : Chapitre 2 et 3.*

1. **Définition des journaux d'activité (2 points) :**
   - 1 point : Définir les logs comme des fichiers ou enregistrements automatiques générés par les systèmes informatiques, enregistrant les événements tels que les connexions, les erreurs, ou les accès aux fichiers.
   - 1 point : Souligner leur rôle dans la traçabilité des activités sur un système ou un réseau.
   - *Exemple de formulation* : Les journaux d'activité (logs) sont des enregistrements détaillés des événements sur un système ou réseau, incluant les connexions, les modifications de fichiers ou les erreurs. Ils constituent une ressource essentielle pour reconstituer la chronologie des actions effectuées.
2. **Importance des journaux dans une enquête numérique (4 points) :**
   - 1 point : Reconstruction de la chronologie des événements : Permet de retracer les actions suspectes (ex. : tentatives de connexion, accès non autorisés).
   - 1 point : Identification des anomalies : Détecte les comportements inhabituels ou malveillants (ex. : exfiltration de données, modification non autorisée).

- 1 point : Validation des hypothèses : Fournit des preuves solides pour confirmer ou réfuter des soupçons.
- 1 point : Corrélation avec d'autres preuves : Les logs peuvent être croisés avec d'autres données (RAM, fichiers) pour affiner l'analyse.
- *Exemple de formulation* :Les journaux permettent de retracer une tentative de connexion échouée suivie d'un accès non autorisé, ce qui valide une hypothèse d'attaque par force brute.

3. **Risques de manipulation des journaux (2 points) :**
   - 1 point : Suppression des entrées critiques : Les attaquants peuvent effacer leurs traces en supprimant les logs liés à leurs actions.
   - 1 point : Altération des données : Modification des horodatages ou des événements pour masquer leur origine réelle.
   - *Exemple de formulation* : Un attaquant peut supprimer les logs de connexion pour dissimuler son intrusion ou modifier les horodatages pour détourner l'attention des enquêteurs.

4. **Moyens de prévention contre la manipulation (2 points) :**
   - 1 point : Stockage sécurisé et immuable : Configurer les journaux pour être stockés sur des systèmes immuables (ex. : disques WORM).
   - 1 point : Surveillance proactive des anomalies : Utiliser des solutions SIEM (ex. : Splunk, ELK) pour détecter et signaler les manipulations.
   - *Exemple de formulation* :En configurant les journaux pour être envoyés vers un serveur central immuable et surveillés par un SIEM, il est possible de détecter toute tentative de manipulation.

7. Dans une enquête sur un crime numérique, décrivez comment utiliser un logiciel d'imagerie bit-à-bit pour préserver l'état d'un disque dur suspect. *Référence au cours : Chapitre 2.*

1. **Définition de l'imagerie bit-à-bit (2 points) :**
   - 1 point : Expliquer que l'imagerie bit-à-bit consiste à créer une copie exacte d'un support de stockage, incluant les fichiers visibles et les zones inaccessibles à l'utilisateur, comme l'espace libre ou les secteurs supprimés.
   - 1 point : Mentionner son objectif : garantir que les données originales restent intactes tout en fournissant une copie exploitable pour l'analyse.
   - *Exemple de formulation* : L'imagerie bit-à-bit est une technique de duplication complète d'un disque dur, capturant chaque bit d'information, y compris les zones supprimées ou inactives. Elle préserve les données originales pour garantir leur intégrité et leur admissibilité en justice.

- **Étapes de préservation de l'état d'un disque dur suspect (6 points) :**
  Chaque étape doit inclure une description, son importance, et un outil recommandé basé sur le cours.
  - Utiliser un bloqueur d'écriture (2 points) :
    - Explication : Empêcher toute modification accidentelle ou intentionnelle des données sur le disque original.
    - Importance : Garantit que le disque reste dans son état initial, ce qui est crucial pour sa recevabilité légale.
    - Outils recommandés : Bloqueurs matériels (ex. : Tableau WriteBlocker) ou logiciels (ex. : DD sous Linux).
    - *Exemple de formulation* :Connecter le disque dur à un bloqueur d'écriture matériel comme Tableau pour éviter toute modification des données.
  - Créer une image bit-à-bit (2 points) :

- Explication : Effectuer une copie complète du disque dur à l'aide d'un logiciel forensique.
- Importance : L'image sert de base pour l'analyse sans altérer l'original.
- Outils recommandés : FTK Imager ou EnCase pour la capture de l'image.
- *Exemple de formulation* : Utiliser FTK Imager pour créer une copie bit-à-bit du disque suspect, en incluant les zones supprimées et les secteurs cachés.

o Générer une empreinte hachée (2 points) :
- Explication : Calculer une empreinte hachée (ex. : SHA256) pour vérifier que l'image est une copie exacte de l'original.
- Importance : Permet de garantir l'intégrité des données et d'identifier toute modification ultérieure.
- Outils recommandés : Utilisation d'outils comme HashCalc ou des fonctionnalités intégrées dans FTK Imager.
- *Exemple de formulation* : Après la création de l'image, générer une empreinte hachée SHA256 pour s'assurer qu'elle correspond exactement au disque original.

2. Documentation et traçabilité (2 points) :

o 1 point : Maintenir un journal de collecte détaillant les étapes effectuées, les outils utilisés, les empreintes hachées générées, et l'identité des responsables de la collecte.

o 1 point : Noter les informations essentielles du disque (numéro de série, fabricant, taille) et les conditions de stockage de l'original.

o *Exemple de formulation* : Documenter chaque étape dans un journal, incluant les détails du disque (numéro de série, modèle), l'outil utilisé pour l'imagerie (ex. : FTK Imager), et l'empreinte hachée générée.

8. Un fichier supprimé a été récupéré sur un système suspect. Expliquez comment vous valideriez son authenticité en utilisant des outils standards de forensique. *Référence au cours : Chapitre 2 et 3.*

1. Définition de l'authenticité des fichiers en forensique (2 points) :

o 1 point : Expliquer que l'authenticité d'un fichier consiste à s'assurer que son contenu n'a pas été altéré depuis sa récupération.

o 1 point : Mentionner que la validation de l'authenticité inclut la vérification de l'intégrité, des métadonnées et de l'origine du fichier.

o *Exemple de formulation* : L'authenticité d'un fichier en forensique consiste à garantir que son contenu est intact et qu'il correspond exactement à l'état dans lequel il a été récupéré, sans altération ni manipulation.

2. Étapes pour valider l'authenticité d'un fichier récupéré (6 points) :

Chaque étape inclut une description, son importance, et un outil ou méthode spécifique mentionné dans le cours.

o Comparaison des empreintes hachées (2 points) :
- Explication : Calculer l'empreinte hachée (ex. : SHA256) du fichier récupéré et la comparer avec celle générée lors de sa collecte initiale.
- Importance : Garantit que le fichier n'a pas été modifié après sa récupération.
- Outils recommandés : HashCalc, FTK Imager ou la commande sha256sum.
- *Exemple de formulation* : Utiliser FTK Imager pour générer une empreinte SHA256 et la comparer avec celle documentée lors de la récupération du fichier.

o Analyse des métadonnées (2 points) :
- Explication : Vérifier les métadonnées du fichier, comme la date de création, modification ou accès, et les attribuer à des événements spécifiques.
- Importance : Identifie les manipulations ou les incohérences dans le fichier.
- Outils recommandés : ExifTool ou Autopsy pour extraire et analyser les métadonnées.
- *Exemple de formulation* : Examiner les métadonnées du fichier avec ExifTool pour vérifier si la date de modification correspond à l'activité suspectée.

o Recherche de contenu altéré (2 points) :

- Explication : Comparer le contenu du fichier avec d'autres versions ou éléments de contexte pour détecter des modifications.
- Importance : Permet de repérer des falsifications ou des ajouts non autorisés.
- Outils recommandés : Autopsy ou EnCase pour analyser le contenu en détail.
- *Exemple de formulation* :Utiliser Autopsy pour vérifier si le contenu du fichier récupéré est cohérent avec les données attendues ou supposées.

3. **Documentation et traçabilité (2 points) :**
   - 1 point : Documenter toutes les étapes, y compris les outils utilisés, les empreintes hachées calculées, et les résultats des analyses.
   - 1 point : Inclure les observations dans un rapport d'analyse détaillé destiné à l'enquêteur ou au tribunal.
   - *Exemple de formulation* : Maintenir un journal détaillant les outils utilisés pour la vérification (ex. : FTK Imager, ExifTool) et inclure un rapport décrivant l'intégrité du fichier, les incohérences éventuelles et les conclusions.

B. Discussion (20 points)

Choisir et traiter, en 600 mots maximum, un des 3 sujets suivants sous forme de discussion scientifique, telle que vue en classe.

Sujet 1 : Impact de l'intelligence artificielle et des deepfakes sur l'investigation numérique : défis et solutions :

1. **Introduction :**

L'intelligence artificielle (IA) et les deepfakes redéfinissent les contours de l'investigation numérique, apportant à la fois des opportunités et des défis sans précédent. D'une part, l'IA améliore la détection des cyberattaques et l'automatisation des enquêtes ; d'autre part, les deepfakes compliquent la validation des preuves numériques en introduisant des falsifications complexes. Ce texte examine leur impact, les défis qu'ils posent et les solutions pour renforcer les enquêtes numériques.

2. **L'intelligence artificielle dans l'investigation numérique (6 points)**

L'IA joue un rôle essentiel dans l'investigation numérique en améliorant la rapidité, l'efficacité et la précision des analyses. Les algorithmes d'apprentissage automatique et d'intelligence artificielle sont utilisés pour :

- **Automatiser l'analyse de grandes quantités de données (2 points) :** Les outils basés sur l'IA, comme Magnet AXIOM et EnCase, permettent de trier des téraoctets de données rapidement. Ils identifient les fichiers suspects et reconstruisent des chronologies complètes.
- **Détecter les anomalies (2 points) :** Grâce à des modèles prédictifs, l'IA détecte des comportements inhabituels dans les logs ou les flux réseau, facilitant la détection des intrusions et des activités malveillantes.
- **Reconstituer les événements (2 points) :** Les outils d'IA corrèlent des preuves multiples, comme les logs système et les métadonnées de fichiers, pour créer une vue cohérente des activités suspectes.

REMARQUES:

- Chaque sous-section doit démontrer que l'IA réduit significativement le temps nécessaire pour traiter de grandes quantités de données, tout en identifiant des schémas d'attaque qui seraient difficiles à repérer manuellement.

3. **Les deepfakes : une menace pour l'intégrité des preuves numériques (6 points)**

Les deepfakes, créés grâce à des techniques d'intelligence artificielle, consistent à manipuler des fichiers multimédias pour leur donner une apparence réaliste mais falsifiée. Ces contenus posent plusieurs défis majeurs :

- **Manipulation de preuves (2 points) :** Dans un contexte judiciaire, un deepfake audio ou vidéo peut être présenté comme une preuve authentique, ce qui complique la tâche des enquêteurs pour valider son authenticité.
- **Désinformation et propagation virale (2 points) :** Les deepfakes sont largement utilisés pour diffuser des fausses informations à grande échelle, ce qui peut compromettre des enquêtes ou des campagnes de communication.
- **Accessibilité accrue (2 points) :** Les outils pour créer des deepfakes sont désormais disponibles publiquement, ce qui permet même à des amateurs de produire des manipulations crédibles.

REMARQUES :

- L'étudiant doit démontrer sa compréhension des impacts des deepfakes en donnant des exemples concrets de leur utilisation frauduleuse et de leurs conséquences dans les enquêtes numériques.

4. Solutions pour relever les défis de l'IA et des deepfakes (6 points)

Pour lutter contre les impacts négatifs des deepfakes tout en exploitant les avantages de l'IA, plusieurs approches doivent être envisagées :

a. Détection des deepfakes (2 points) :

- Utilisation d'outils spécialisés comme Deepware Scanner, qui détectent des incohérences visuelles ou auditives dans les contenus suspects.
- Développement de solutions d'IA capables de repérer les artefacts typiques des deepfakes, comme des anomalies dans les mouvements faciaux ou les transitions audio.

b. Blockchain pour l'authenticité des preuves (1 point) :

- La blockchain peut être utilisée pour horodater et sceller les fichiers multimédias, garantissant ainsi qu'ils n'ont pas été altérés après leur création.

c. Formation et expertise (1 point) :

- Former les enquêteurs numériques aux techniques de détection des manipulations basées sur l'IA et renforcer leurs compétences en validation des preuves numériques.

d. Cadre juridique renforcé (2 points) :

- Adopter des lois spécifiques contre les deepfakes, incluant des sanctions claires pour leur création et leur diffusion dans des contextes frauduleux.
- Établir des standards pour l'admissibilité des preuves numériques, en tenant compte des menaces posées par les deepfakes.

REMARQUES :

- Le candidat doit proposer des solutions réalistes et applicables, en tenant compte des aspects techniques (outils et formations) et juridiques (cadres légaux adaptés).

5. Opportunités et menaces : trouver un équilibre (2 points)

Malgré les défis posés par les deepfakes, l'IA reste un outil indispensable pour l'investigation numérique. Elle améliore l'efficacité des enquêtes et permet de traiter des volumes massifs de données que les humains seuls ne pourraient pas analyser. Cependant, ces opportunités nécessitent une vigilance accrue pour anticiper et contrer les risques liés à la manipulation des preuves numériques.

REMARQUES :

- Cette partie synthétique doit montrer que l'équilibre entre opportunités et menaces est central pour l'avenir des enquêtes numériques.

6. Conclusion (2 points)

L'intelligence artificielle et les deepfakes transforment radicalement le domaine des investigations numériques. Si l'IA offre des possibilités exceptionnelles pour améliorer la détection, l'analyse et la reconstitution des faits, les deepfakes menacent la fiabilité des preuves numériques en introduisant des falsifications sophistiquées. Une réponse globale, intégrant technologie, expertise humaine et cadre juridique adapté, est essentielle pour garantir l'intégrité et l'équité des enquêtes.

REMARQUES :

- La conclusion doit être concise et synthétiser les points clés en insistant sur la nécessité d'une approche multidimensionnelle.

Sujet 2 : Technologies quantiques : opportunités et menaces pour le chiffrement et l'investigation numérique :

1. Introduction :

Les technologies quantiques représentent une révolution dans le domaine de la cybersécurité et des enquêtes numériques. Elles apportent des opportunités inédites pour renforcer la cryptographie et la puissance des outils d'investigation, tout en posant des menaces sans précédent pour les systèmes actuels de chiffrement. Cette discussion explore leurs impacts, les défis associés et les solutions adaptées pour anticiper et s'adapter à ces transformations.

2. Opportunités offertes par les technologies quantiques (6 points)

Les technologies quantiques, basées sur les principes de superposition et d'intrication, offrent des avancées majeures dans plusieurs domaines, notamment :

- **Chiffrement quantique inviolable (2 points)** :
  - La cryptographie quantique, en particulier le protocole de distribution de clés quantiques (QKD, Quantum Key Distribution), permet de garantir la sécurité des communications. Toute tentative d'interception modifie l'état des photons et peut être immédiatement détectée.
  - *Exemple de formulation* : Le protocole BB84 garantit une communication inviolable en détectant toute tentative d'écoute, assurant ainsi la confidentialité des données.
- **Amélioration des capacités d'analyse en investigation numérique (2 points)** :
  - Les ordinateurs quantiques permettent d'accélérer des analyses complexes, comme la recherche de motifs dans des données massives ou le cassage de codes malveillants.
  - Ils facilitent également la reconstruction rapide des événements numériques en corrélant des preuves multiples.
  - *Exemple de formulation* : Un ordinateur quantique pourrait analyser des logs réseau massifs en quelques secondes, une tâche qui prendrait des jours avec les outils classiques.
- **Simulation avancée pour la cybersécurité (2 points)** :
  - Les technologies quantiques permettent de simuler des cyberattaques complexes pour tester les défenses des systèmes en temps réel.
  - *Exemple de formulation* : Les simulations quantiques offrent la possibilité de prévoir les schémas d'attaques inconnues, renforçant ainsi les capacités de défense proactive.

3. Menaces posées par les technologies quantiques (6 points)

Malgré leurs promesses, les technologies quantiques posent des menaces considérables pour les systèmes actuels de chiffrement et les méthodologies d'investigation numérique :

- **Obsolescence des systèmes de chiffrement classiques (2 points)** :
  - Les ordinateurs quantiques, grâce à des algorithmes comme Shor, peuvent casser rapidement les schémas cryptographiques asymétriques (ex. : RSA, ECC) en factorisant les grandes clés de chiffrement.
  - *Exemple de formulation* :Un ordinateur quantique pourrait casser une clé RSA 2048 en quelques heures, alors qu'il faudrait des milliards d'années avec des ordinateurs classiques.
- **Augmentation des risques de cyberattaques (2 points)** :
  - Les cybercriminels pourraient exploiter les technologies quantiques pour contourner les systèmes de sécurité actuels.
  - Les techniques d'attaque quantique pourraient aussi compromettre les données sensibles stockées aujourd'hui, rendant obsolètes les protections mises en place.
  - *Exemple de formulation* :Les attaques par ordinateur quantique pourraient cibler des bases de données critiques, comme celles des gouvernements ou des banques.
- **Complexité accrue pour les investigations (2 points)** :

- Les preuves numériques issues d'environnements quantiques pourraient nécessiter des outils totalement nouveaux pour être collectées et analysées.
- *Exemple de formulation* :L'analyse des schémas de cryptographie post-quantique nécessitera une refonte des méthodologies actuelles en investigation numérique.

4. Solutions pour anticiper les impacts des technologies quantiques (6 points)

Pour relever les défis des technologies quantiques, plusieurs solutions peuvent être mises en œuvre :

a. Adoption de la cryptographie post-quantique (2 points) :

- Développer et déployer des algorithmes résistants aux attaques quantiques, comme ceux proposés par le NIST (National Institute of Standards and Technology).
- *Exemple de formulation* :Les algorithmes post-quantiques, comme le schéma de cryptographie à réseau (lattice-based cryptography), offrent une résistance prouvée aux attaques quantiques.

b. Investissements dans la recherche quantique (1 point) :

- Soutenir la recherche pour développer des outils d'investigation compatibles avec les environnements quantiques.
- *Exemple de formulation* : Des investissements dans la recherche permettront de concevoir des solutions d'investigation capables de gérer les systèmes de chiffrement post-quantiques.

c. Formation et sensibilisation des enquêteurs numériques (1 point) :

- Former les professionnels de l'investigation numérique aux impacts des technologies quantiques et aux nouveaux outils émergents.
- *Exemple de formulation* : Les enquêteurs doivent être formés pour comprendre les principes de la cryptographie quantique et les défis qu'elle impose.

d. Collaboration internationale (2 points) :

- Encourager la coopération entre pays et organisations pour établir des standards mondiaux de sécurité face aux menaces quantiques.
- *Exemple de formulation* : La création de cadres juridiques internationaux facilitera l'adoption harmonisée de la cryptographie post-quantique.

5. Opportunités et menaces : trouver un équilibre (2 points)

Les technologies quantiques offrent des possibilités extraordinaires pour renforcer la cybersécurité et améliorer les outils d'investigation. Cependant, elles posent des menaces graves à la sécurité des systèmes actuels. La transition vers des schémas résistants aux attaques quantiques est essentielle pour minimiser ces risques.

REMARQUES :

- Cette partie doit insister sur la nécessité de s'adapter rapidement à ces changements technologiques pour maximiser les avantages tout en limitant les menaces.

6. Conclusion (2 points)

Les technologies quantiques marquent un tournant majeur pour la cybersécurité et l'investigation numérique. Si elles promettent des avancées significatives dans l'analyse et la protection des données, elles rendent également obsolètes les systèmes cryptographiques actuels. Anticiper ces impacts grâce à des solutions technologiques, des formations spécialisées et une collaboration internationale est essentiel pour garantir la résilience face à ces changements révolutionnaires.

Sujet 3 : Investigation numérique en Afrique et au Cameroun : défis liés aux infrastructures et au cadre juridique.

1. Introduction :

L'investigation numérique est un domaine en pleine expansion en Afrique, notamment au Cameroun, où la lutte contre la cybercriminalité est devenue un enjeu majeur. Cependant, cette pratique se heurte à des défis liés aux infrastructures technologiques, au cadre juridique et au développement des compétences. Ce texte explore ces défis et propose des solutions adaptées pour renforcer les capacités d'investigation numérique dans ce contexte spécifique.

2. Défis liés aux infrastructures technologiques (6 points)

Le développement limité des infrastructures numériques en Afrique et au Cameroun représente un obstacle majeur pour les enquêtes numériques efficaces. Ces défis incluent :

- **Manque d'équipements spécialisés (2 points) :**
  - Les outils forensiques tels que FTK Imager, EnCase ou Magnet AXIOM sont rares dans les services de police et les institutions publiques en raison de leurs coûts élevés.
  - *Exemple de formulation* : L'absence d'équipements forensiques modernes limite la capacité des enquêteurs à collecter, analyser et préserver les preuves numériques de manière conforme aux standards internationaux.
- **Connexions Internet peu fiables (2 points) :**
  - Une connexion Internet instable ou de faible qualité entrave les investigations en ligne, comme l'analyse des réseaux sociaux, la surveillance des cyberattaques ou la collecte de données distantes.
  - *Exemple de formulation* : Les interruptions fréquentes d'Internet ralentissent les enquêtes nécessitant une analyse en temps réel, comme l'identification d'adresses IP suspectes.
- **Absence de centres spécialisés (2 points) :**
  - Peu de pays africains disposent de laboratoires numériques dédiés à la criminalistique informatique, ce qui oblige souvent les enquêteurs à externaliser les analyses, retardant ainsi le processus judiciaire.
  - *Exemple de formulation* : L'absence de centres d'investigation numérique spécialisés complique la gestion rapide des preuves, créant des goulets d'étranglement dans le traitement des affaires.

3. Défis liés au cadre juridique (6 points)

Le cadre juridique en Afrique et au Cameroun n'est souvent pas suffisamment développé ou harmonisé pour répondre aux besoins des enquêtes numériques. Les principaux défis sont les suivants :

- **Lacunes législatives (2 points) :**
  - Bien que certains pays africains, y compris le Cameroun, aient adopté des lois contre la cybercriminalité, celles-ci ne couvrent pas toujours les avancées technologiques récentes, comme la cryptographie ou les deepfakes.
  - *Exemple de formulation* : Au Cameroun, la loi de 2010 relative à la cybersécurité et à la cybercriminalité reste insuffisante pour traiter des menaces modernes, telles que les manipulations avancées de preuves numériques.
- **Manque de standards internationaux (2 points) :**
  - L'absence d'harmonisation avec les standards internationaux, tels que ceux de la Convention de Budapest, limite la collaboration transfrontalière dans les enquêtes impliquant des cybercriminels opérant au-delà des frontières.
  - *Exemple de formulation* : L'absence de ratification de la Convention de Budapest par certains pays africains entrave la coopération internationale en matière de cybercriminalité.
- **Formation limitée des magistrats et enquêteurs (2 points) :**
  - Les professionnels du droit et les enquêteurs manquent souvent de connaissances techniques sur l'analyse des preuves numériques, ce qui peut conduire à leur rejet en justice.
  - *Exemple de formulation* : De nombreux magistrats ne maîtrisent pas les concepts techniques nécessaires pour évaluer la validité des preuves numériques dans un procès.

4. Solutions pour surmonter ces défis (6 points)

Pour renforcer les capacités d'investigation numérique en Afrique et au Cameroun, plusieurs mesures doivent être prises :

a. Renforcement des infrastructures (2 points) :

- Investir dans des laboratoires forensiques nationaux équipés d'outils modernes (FTK Imager, Magnet AXIOM, bloqueurs d'écriture).
- Développer des infrastructures Internet stables et résilientes pour faciliter les enquêtes en ligne.
- *Exemple de formulation* : L'établissement de centres spécialisés au Cameroun permettrait de réduire la dépendance aux services internationaux d'analyse numérique.

b. Mise à jour du cadre légal (2 points) :

- Adapter les lois existantes pour couvrir les nouvelles formes de cybercriminalité (ex. : deepfakes, cryptomonnaies).
- Ratifier les accords internationaux comme la Convention de Budapest pour favoriser la coopération transfrontalière.
- *Exemple de formulation* : Une mise à jour de la loi sur la cybercriminalité au Cameroun doit inclure des dispositions sur les manipulations numériques avancées.

c. Formation et sensibilisation (2 points) :

- Former les enquêteurs, magistrats et professionnels du droit aux techniques modernes d'investigation numérique et de gestion des preuves.
- *Exemple de formulation* : Les formations certifiantes, comme celles basées sur la norme ISO 27037, aideraient les enquêteurs camerounais à acquérir des compétences reconnues internationalement.

5. Opportunités et menaces : un équilibre nécessaire (2 points)

Malgré les défis, l'Afrique et le Cameroun disposent d'un potentiel important pour développer leurs capacités d'investigation numérique. Les investissements dans les infrastructures et la formation, combinés à une coopération internationale, pourraient transformer ces défis en opportunités pour mieux lutter contre la cybercriminalité.

REMARQUES :

- Cette partie doit démontrer que, malgré les obstacles, des efforts ciblés peuvent faire progresser significativement le domaine.

6. Conclusion (2 points)

Les défis liés aux infrastructures et au cadre juridique freinent l'évolution de l'investigation numérique en Afrique et au Cameroun. Cependant, des investissements dans des laboratoires spécialisés, une réforme des lois et une formation accrue des enquêteurs et des magistrats sont essentiels pour surmonter ces obstacles. La réussite de ces initiatives repose également sur une coopération internationale accrue, garantissant un avenir où les enquêtes numériques seront plus efficaces et plus justes.

« *Like a conscientious and methodical craftsman, every day, refine your practice. Only in this way will you be and remain an Expert.* »

Thierry MINKA.