RÉSUMÉ DU COURS D'INVESTIGATION NUMÉRIQU

PAR : **HEYA SALOMON FLORIAN CIN-4 22P046**

SOUS LA SUPERVISION DE : **M. MINKA**

ANNÉE : 2025 - 2026

Fondements, Historique et Évolution de l'Investigation Numérique

L'investigation numérique (ou *digital forensics*), souvent appelée informatique légale en français, est la science qui consiste à recueillir, analyser et présenter des preuves numériques dans un cadre légal. Elle s'est construite sur des fondements solides et a connu une évolution rapide et passionnante, directement liée à l'explosion du numérique.

Les Fondements de l'Investigation Numérique

L'investigation numérique repose sur quatre piliers fondamentaux qui garantissent la validité et l'admissibilité des preuves en justice.

1. **L'Intégrité (La Preuve est Non-Altérée) :**
    - **Principe :** Toute preuve numérique doit être collectée et analysée sans être modifiée. C'est le principe le plus critique.
    - **Application :** On utilise des *write-blockers* (bloqueurs d'écriture) pour connecter un disque dur en lecture seule et on calcule des sommes de contrôle (hashs) comme MD5 ou SHA-256. Le hash initial doit correspondre au hash après analyse pour prouver l'intégrité.
2. **La Méthodologie et la Traçabilité (Processus Auditable) :**
    - **Principe :** Toutes les actions de l'enquêteur doivent être documentées, répétables et justifiables.
    - **Application :** Tenue d'un journal de bord (log) détaillant chaque étape, les outils utilisés, les paramètres et les résultats. Un autre expert doit pouvoir refaire les mêmes manipulations et obtenir les mêmes résultats.

Historique et Évolution

L'histoire de l'investigation numérique est récente mais extrêmement dense. On peut la découper en plusieurs phases.

Les Prémisses (Années 1980) : La Prise de Conscience

- **Contexte :** L'émergence des PC (IBM, Apple) dans les entreprises et les foyers coïncide avec les premières affaires de fraude informatique.
- **Événements marquants :**
    - Le **FBI** crée une des premières unités dédiées à l'analyse des médias numériques (Magnetic Media Program, 1984).
    - Les forces de l'ordre réalisent qu'elles doivent développer des compétences spécifiques pour traquer les preuves sur ces nouveaux supports.
- **Méthodes :** Très artisanales. On apprenait "sur le tas". Peu d'outils spécialisés existaient.

Défis Futurs et Perspectives

L'évolution ne ralentit pas. Les enquêteurs font face à de nouveaux défis de taille :

- **L'Informatique Quantique :** Capable de casser les algorithmes de chiffrement actuels, elle menace à la fois la sécurité des données mais aussi les méthodes d'investigation.
- **L'Intelligence Artificielle Générative :** Comment investiguer des crimes utilisant des *deepfakes* pour du chantage ou de la désinformation ? Comment prouver l'authenticité d'un contenu ?
- **La Confidentialité Renforcée :** La société exige une meilleure protection de la vie privée (RGPD), ce qui entre en tension avec les besoins d'enquête.
- **La Pénurie de Compétences :** Le besoin d'experts qualifiés dépasse largement le nombre de formations disponibles.

Cadre Théorique et Conceptuel de l'Investigation Numérique

Le cadre théorique et conceptuel est l'ensemble des principes fondamentaux, des modèles et des concepts qui fondent la méthodologie de l'investigation numérique. Il assure que la preuve numérique est collectée, analysée et présentée de manière **scientifiquement valide, reproductible et légalement admissible**.

Ce cadre peut être divisé en plusieurs piliers conceptuels.

1. Les Principes Fondamentaux (Les Lois Immobiles)

Ces principes, souvent attribués aux pionniers du domaine, sont les règles d'or qui gouvernent toute action.

- **Le Principe de Locard (Adapté au Numérique) :** "Tout contact laisse une trace". En numérique, toute interaction avec un système (navigation, connexion, création de fichier) laisse une **trace numérique** (artefact) quelque part : logs, fichiers temporaires, registre, mémoire vive.
- **Le Principe de l'Intégrité des Preuves :** La preuve numérique doit être manipulée de manière à ce qu'elle ne soit **ni altérée, ni modifiée**. C'est le principe le plus critique. On utilise pour cela des algorithmes de hachage (MD5, SHA-256) qui génèrent une empreinte unique du support. Toute modification changerait cette empreinte.
- **Le Principe de la Chaîne de Custodie (Chaîne de Continuité) :** Documenter de manière précise et ininterrompue **toute personne qui a eu la preuve en main**, quand, pourquoi et quelles actions ont été entreprises. Cela garantit la traçabilité et permet de contester toute allégation d'altération.

Normes et Standards Internationaux en Investigation Numérique

1. Pourquoi des Standards Internationaux ?

- **Interopérabilité :** Les crimes numériques transcendent les frontières. Les forces de l'ordre de différents pays doivent pouvoir collaborer et se comprendre.
- **Admissibilité légale :** Une preuve collectée selon une norme reconnue internationalement a beaucoup plus de poids devant un tribunal et résiste mieux aux contestations de la défense.
- **Assurance Qualité :** Ils fournissent un cadre pour garantir la compétence des praticiens et la qualité des laboratoires d'analyse.
- **Efficacité :** Ils permettent d'éviter la réinvention de la roue et de standardiser les bonnes pratiques.

Série des Normes ISO/IEC 27000 (Sécurité de l'information)

Cette série est cruciale car elle lie directement la sécurité de l'information aux processus forensiques.

- **ISO/IEC 27037:2012** : Lignes directrices pour l'**identification, la collecte, l'acquisition et la préservation** des preuves numériques. C'est la norme fondamentale pour la phase amont.
- **ISO/IEC 27042:2015** : Guide l'**analyse et l'interprétation** des preuves numériques.
- **ISO/IEC 27050:2020** : Traite spécifiquement de la **découverte électronique (eDiscovery)** dans le contexte des litiges civils.

Le Computer Forensics Tool Testing Program (CFTT) du NIST

- **Objectif :** Établir des méthodologies de test **scientifiquement valides** pour vérifier que les outils forensiques (comme FTK, X-Ways, AXIOM) fonctionnent **correctement et de manière fiable**.
- **Impact :** Un enquêteur peut s'appuyer sur les résultats du CFTT pour prouver que son outil produit des résultats exacts, renforçant ainsi la crédibilité de son témoignage.

Le National Software Reference Library (NSRL) du NIST

- **Objectif :** Une collection massive de hashs (empreintes numériques) de logiciels, de fichiers systèmes et de fichiers communs.
- **Utilité :** Permet lors d'une analyse de **filtrer les fichiers connus et non pertinents** (fichiers du système d'exploitation, logiciels légitimes), accélérant ainsi considérablement l'identification des fichiers suspects ou uniques.

Meilleures Pratiques Mondiales en Investigation Numérique

Préservation de la Scène Numérique

- Isoler immédiatement les dispositifs concernés
- Documenter l'état initial par photographies et notes détaillées
- Maintenir une chaine de custody ininterrompue

Méthodologie d'Analyse

- **Approche scientifique** : hypothèses testables et reproductibilité
- **Analyse multi-outils** : validation des résultats par plusieurs outils
- **Documentation complète** : journal de bord détaillé de toutes les actions

L’Ere du Post-Quantique

L'Impact Direct sur l'Investigation Numérique

Les pratiques actuelles de l'investigation numérique sont construites autour de la capacité à parfois contourner, ou à analyser, des systèmes chiffrés. Le post-quantique change la donne.

La Fin du Rêve du Contournement du Chiffrement :

- **Aujourd'hui :** Les enquêteurs espèrent souvent trouver des clés en mémoire vive (RAM), extraire des mots de passe, ou utiliser des vulnérabilités pour déchiffrer des dispositifs.
- **Demain :** Si les données ont été chiffrées avec un algorithme vulnérable (RSA) et que l'adversaire a stocké la communication chiffrée, il pourra la déchiffrer rétroactivement. **L'enquêteur n'aura peut-être même pas besoin de la clé** ; l'algorithme quantique fera le travail. Cela semble être un avantage... mais c'est une arme à double tranchant.

La Menace pour l'Intégrité des Preuves et la Chaîne de Custodie :

- **Signatures Numériques :** Les signatures digitales qui authentifient les rapports d'enquête, les images forensiques (hachages signés) ou les certificats des outils pourraient être falsifiées si elles utilisent RSA ou ECC.

Primitives Cryptographiques et Opposabilité (Admissibilité) en Investigation Numérique

Que sont les Primitives Cryptographiques ?

Ce sont les briques de base, les algorithmes fondamentaux sur lesquels reposent la sécurité informatique et la confidentialité des données. Leur rôle est de garantir trois propriétés essentielles, souvent appelée la "triade de la sécurité de l'information" (CIA) :

C - Confidentialité : Assurer que seules les parties autorisées peuvent accéder à l 'information.

I - Intégrité : Détecter toute modification ou altération intentionnelle ou accidentelle des données.

A - Authenticité (et Non-Répudiation) : Garantir l'origine d'une donnée et empêcher l'expéditeur de nier être à l'origine d'un message (non-répudiation).

Cryptanalyse et Analyse de Protocoles en Investigation Numérique

La cryptanalyse et l'analyse de protocoles représentent des disciplines avancées en investigation numérique qui visent à comprendre, tester et potentiellement contourner les mécanismes de sécurité pour accéder à des preuves numériques

Cryptanalyse : Science consistant à analyser les systèmes cryptographiques dans le but de trouver leurs faiblesses

- **Objectifs principaux** :
    - Récupération de données chiffrées sans clé
    - Vérification de la solidité des implémentations cryptographiques
    - Identification de vulnérabilités dans les algorithmes

Cryptanalyse : Science consistant à analyser les systèmes cryptographiques dans le but de trouver leurs faiblesses

- **Objectifs principaux** :
    - Récupération de données chiffrées sans clé
    - Vérification de la solidité des implémentations cryptographiques
    - Identification de vulnérabilités dans les algorithmes