Résumé du cours d'Investigation Numérique

Matière : Théories et Pratiques de l'Investigation Numérique

Enseignant :M. MINKA Thierry

Année académique : 2025–2026

Par l'étudiante : ZE MVONDO Océanne M.

Filière : 4e année CIN

Thématiques des chapitres

Fondements et historique (chapitres 1 à 3)

La première partie du cours pose les bases conceptuelles. On y réfléchit à la trace numérique comme nouvelle forme de preuve, avec toutes ses limites : elle peut être copiée, effacée ou manipulée. Cette fragilité amène à poser très tôt la question de l'éthique de l'investigateur. L'histoire de la discipline montre ensuite comment elle s'est construite au fil des grandes affaires, des premiers hackers des années 80 à SolarWinds en 2020.

Cadre théorique et conceptuel (chapitres 4 et 5)

La deuxième thématique développe les modèles théoriques qui structurent une enquête numérique. Le principe de Locard, adapté au numérique, affirme que toute action laisse une trace. Des modèles comme DFRWS ou ISO 27037 viennent préciser les étapes. Les mathématiques apportent aussi leur contribution (entropie, graphes) pour analyser les données.

Normes et standards internationaux (chapitres 6 et 7)

Ces chapitres mettent en avant l'importance des normes ISO/IEC et des guides NIST. Elles garantissent la recevabilité des preuves, notamment via la chaîne de custody et l'ordre de volatilité des données. Leur application à des cas concrets montre que l'investigation est à la fois locale et mondiale.

Méthodologies et outils (chapitres 8 et 9)

On découvre différentes méthodologies (SANS, CERT, ENISA) et l'arsenal de l'investigateur : imagerie disque, analyse mémoire, détection d'obfuscation. Mais face à l'anti-forensique, il faut recourir à des techniques "anti-anti-forensiques" et à l'intelligence artificielle.

L'ère post-quantique et le trilemme CRO (chapitres 10 à 13)

Ces chapitres analysent l'impact du quantique, capable de casser RSA et ECC. L'auteur introduit le trilemme CRO (Confidentialité, Fiabilité, Opposabilité juridique), qui montre qu'on ne peut pas maximiser les trois simultanément. Les primitives post-quantiques (Kyber, Dilithium) et le protocole ZK-NR ouvrent de nouvelles pistes.

Cryptanalyse et protocoles (chapitres 14 à 16)

La cryptanalyse est présentée comme un processus scientifique. Des outils comme Tamarin permettent de tester formellement la sécurité des protocoles. Les cas de ZK-NR et des signatures BLS montrent une méthodologie complète d'audit.

Cadre juridique (chapitres 17 et 18)

Les aspects juridiques sont essentiels. Le droit américain (FRE, CFAA), le droit européen (RGPD, Convention de Budapest) et le droit africain (Convention de Malabo) encadrent chacun l'usage des preuves numériques. Au Cameroun, des lois récentes organisent l'investigation, même si la pratique reste en développement.

Pratique opérationnelle et forensique système (chapitres 19 et 20)

Enfin, les deux derniers chapitres abordent la pratique : installation d'un laboratoire, procédures opérationnelles et analyse de systèmes (NTFS, EXT4, APFS). L'analyse mémoire et la timeline analysis sont des outils clés pour reconstruire les scénarios d'attaque.

Résumé des chapitres

L'investigation numérique est une discipline jeune mais en constante mutation, au carrefour de la technique, de la philosophie et du droit. Le cours commence par poser ses bases : chaque interaction dans le monde numérique laisse une trace, mais cette trace est fragile et doit être analysée avec méthode. Dès le départ, on comprend que l'investigateur numérique ne peut pas se limiter à manipuler des outils. Il doit aussi réfléchir à la signification des preuves qu'il collecte, à leur validité et surtout à leur impact sur les libertés individuelles. On nous rappelle que la technologie est un pouvoir, et qu'il faut un cadre éthique pour l'utiliser à bon escient.

L'histoire de la discipline illustre bien cette évolution. Dans les années 80, avec les premiers hackers, l'informatique devient un espace de confrontation entre innovation et illégalité. Les affaires Kevin Mitnick ou l'opération Sundevil marquent une prise de conscience : l'investigation doit se professionnaliser. Dans les années 2000, les scandales comme Enron poussent à la standardisation des méthodes. Les années 2010 apportent de nouveaux défis avec le cloud et le big data, symbolisés par Silk Road ou les Panama Papers. Enfin, l'ère actuelle, marquée par l'intelligence artificielle et la menace quantique, montre que chaque avancée technologique oblige les investigateurs à réinventer leurs pratiques. Cette perspective historique est essentielle : elle rappelle que la cybersécurité est un domaine en perpétuel mouvement, où rien n'est jamais acquis.

Sur le plan théorique, le cours insiste sur le principe de Locard appliqué au numérique : toute action laisse une trace. Mais pour exploiter ces traces, il faut s'appuyer sur des modèles structurés comme DFRWS ou ISO 27037, qui encadrent la collecte, l'analyse et la présentation des preuves. Les mathématiques apportent aussi des outils précieux : l'entropie pour mesurer l'incertitude, la théorie des graphes pour cartographier les interactions, ou encore la théorie du chaos pour comprendre la complexité des systèmes. L'évolution scientifique montre que l'investigation a toujours su intégrer les innovations : de la memory forensics à la blockchain forensics, chaque jalon renforce la discipline et la prépare à affronter de nouveaux types de menaces.

Un autre aspect fondamental est la normalisation. Les normes ISO et NIST assurent que les preuves collectées soient reconnues en justice, notamment grâce à la rigueur de la chaîne de custody. L'ordre de volatilité des données rappelle que certaines informations disparaissent plus vite que d'autres, ce qui impose des priorités dans la collecte. Ces normes ne sont pas que théoriques : elles trouvent leur application dans des contextes très concrets, que ce soit au Cameroun pour traiter une fuite de données ou à l'international dans des affaires de cyberterrorisme ou d'espionnage industriel. Cette mosaïque d'exemples montre bien que l'investigation numérique est à la fois locale et globale : elle dépend de lois

nationales mais doit aussi dialoguer avec des menaces transfrontalières.

Côté méthodologies et outils, on voit que les approches varient selon les organismes (SANS, CERT, ENISA), mais partagent une structure commune : identification, collecte, analyse, restitution. L'investigateur moderne doit maîtriser des outils d'acquisition disque, des frameworks d'analyse mémoire comme Volatility, mais aussi des techniques avancées pour contourner l'anti-forensique. Car les attaquants ne se contentent plus de lancer des attaques : ils cherchent activement à effacer ou camoufler leurs traces, via le chiffrement, la stéganographie ou l'obfuscation. Face à cela, l'intelligence artificielle est devenue un allié : apprentissage automatique pour classer les malwares, deep learning pour analyser des comportements suspects, etc. Mais l'IA apporte aussi des risques, puisqu'elle peut être utilisée par les cybercriminels pour perfectionner leurs attaques. Cette dualité est un fil rouge du cours.

Un des apports les plus originaux est la réflexion sur l'ère post-quantique. Les ordinateurs quantiques menacent les fondements de la cryptographie actuelle : RSA ou ECC pourraient être brisés par des algorithmes comme Shor ou Grover. Cela ouvre la voie à une stratégie inquiétante : "harvest now, decrypt later", où un attaquant stocke des données chiffrées aujourd'hui pour les déchiffrer demain. Pour y répondre, l'auteur introduit le trilemme CRO : Confidentialité, Fiabilité, Opposabilité juridique. L'idée est simple mais puissante : il est impossible de maximiser ces trois critères en même temps. Les primitives post-quantiques comme Kyber ou Dilithium, ou les protocoles de preuve à divulgation nulle de connaissance comme ZK-NR, offrent des pistes, mais montrent aussi que l'équilibre entre technique et droit est toujours précaire.

La cryptanalyse occupe également une place importante. Elle ne consiste pas seulement à "casser du code", mais à tester systématiquement la solidité des protocoles. Des outils comme le prover Tamarin permettent de vérifier formellement la sécurité de protocoles complexes. Le cas du protocole ZK-NR ou des signatures BLS montre comment une analyse rigoureuse peut révéler des surfaces d'attaque invisibles à première vue. L'investigateur doit donc être à la fois technicien et analyste, capable de comprendre les limites d'un système tout en anticipant ses vulnérabilités.

L'aspect juridique est incontournable. Le droit américain, européen et africain encadre de manière différente l'usage des preuves numériques. Aux États-Unis, les règles de preuve (FRE) et les lois comme le CFAA définissent clairement les responsabilités. En Europe, le RGPD et la Convention de Budapest mettent l'accent sur la protection des données et la coopération internationale. En Afrique, la Convention de Malabo cherche à créer un socle commun, même si sa mise en œuvre reste inégale. Au Cameroun, plusieurs lois récentes encadrent la cybercriminalité, mais le pays fait encore face à des défis de formation et de ressources. Cette diversité montre que la technique seule ne suffit pas : sans cadre juridique robuste, l'investigation perd sa légitimité.

Enfin, les chapitres pratiques rappellent que l'investigation ne se fait pas uniquement sur le papier. Monter un laboratoire forensique, définir des procédures opérationnelles, gérer la chaîne de custody physique, tout cela demande rigueur et organisation. L'investigateur doit aussi rester en veille permanente : nouvelles versions de systèmes de fichiers (NTFS, EXT4, APFS), artefacts spécifiques à Windows, Linux ou macOS, mémoire vive avec Volatility 3, ou encore traces laissées par les environnements virtualisés. La timeline

analysis permet de reconstruire le déroulement des attaques avec précision, tandis que les frameworks d'évaluation assurent la qualité du travail rendu. Ces aspects montrent que la discipline est autant une science appliquée qu'un domaine théorique.

En résumé, les chapitres dressent un panorama complet de l'investigation numérique. On y voit une discipline en construction permanente, tiraillée entre la rigueur scientifique, l'évolution rapide de la technologie et les contraintes juridiques. L'étudiante que je suis en retient surtout une leçon : être investigateur numérique, ce n'est pas seulement maîtriser des outils, mais savoir penser la preuve dans toute sa complexité — technique, éthique et légale. À l'ère du post-quantique et de l'intelligence artificielle, cette posture critique et responsable sera plus que jamais indispensable.