REPUBLIQUE DU CAMEROUN
Paix – Travail – Patrie

UNIVERSITE DE YAOUNDE I

ECOLE NATIONALE SUPERIEURE POLYTECHNIQUE DE YAOUNDE

DEPARTEMENT DE GENIE INFORMATIQUE

REPUBLIC OF CAMEROON
Peace – Work – Fatherland

UNIVERSITY OF YAOUNDE I

NATIONAL ADVANCED SCHOOL OF ENGINEERING OF YAOUNDE

DEPARTMENT OF COMPUTER SCIENCE

Résumé du cours portant sur les théories et pratiques de l'investigation numérique dans cette nouvelle ère

Participant

Matricule : 22P035

Spécialité : Cybersécurité et Investigation Numérique

Noms : MBETSI DJOFANG AIME LINDSEY

Niveau : 4

Superviseur

M. MINKA MI NGUIDJOI Thierry Emmanuel

Année Scolaire : 2025–2026

Résumé du Cours "Théories et Pratiques de l'Investigation Numérique"

L'investigation numérique est devenue aujourd'hui une discipline incontournable dans un monde où chaque geste laisse une empreinte technologique. Ce qui, autrefois, pouvait sembler invisible ou impossible à retracer se transforme désormais en un immense réservoir de données que l'on peut exploiter pour comprendre, enquêter et juger. Il ne s'agit plus seulement de récupérer un fichier effacé sur un ordinateur, mais de reconstituer des événements complexes en combinant informatique, droit et éthique. Pour se représenter cela simplement, on peut imaginer qu'un téléphone portable est comme un grand livre ouvert : chaque application utilisée, chaque message envoyé, chaque photo prise laisse une marque. Ces marques ne disparaissent pas totalement et l'enquêteur numérique est celui qui sait les lire et les interpréter pour raconter une histoire complète. Cette activité prend encore plus d'importance dans un contexte où les technologies évoluent sans cesse, parfois plus vite que les lois censées les encadrer.

Un exemple simple peut rendre cette idée plus tangible. Imaginons qu'une personne soit victime d'une usurpation d'identité sur un réseau social. À première vue, il pourrait sembler presque impossible de retrouver l'auteur de cette fraude, puisque celui-ci utilise un faux profil et cache ses traces. Pourtant, l'investigation numérique permet d'exploiter des indices invisibles pour l'utilisateur lambda : l'adresse IP enregistrée lors de la connexion, les métadonnées d'une photo mise en ligne ou encore l'heure précise des interactions. En recoupant ces éléments, l'enquêteur est capable de reconstituer le parcours suivi par l'escroc et de remonter jusqu'à lui. C'est un peu comme si un détective suivait des empreintes de pas invisibles à l'œil nu, mais qui apparaissent clairement sous une lumière spéciale.

Les bases de cette discipline reposent sur un principe ancien formulé par Edmond Locard : toute action laisse une trace. Ce principe, né pour la police scientifique traditionnelle, est encore plus vrai dans le domaine numérique. Là où une empreinte physique peut s'effacer avec le temps, les machines gardent en mémoire des milliers de traces invisibles à l'œil nu. Quand une photo est supprimée d'un téléphone, elle n'est pas réellement détruite, mais simplement marquée comme espace libre. Tant qu'aucune nouvelle donnée ne vient l'écraser, elle reste récupérable, parfois pendant des années. Cela illustre bien la force de l'investigation numérique : faire apparaître ce qui semblait disparu. Les traces numériques se présentent sous deux formes. Les traces primaires regroupent des éléments comme les journaux systèmes, les fichiers temporaires ou les registres. Elles sont souvent techniques et détaillées. Les traces secondaires concernent plutôt les habitudes, les métadonnées ou les flux Internet, qui révèlent comment une personne utilise ses appareils et interagit en ligne. Dans les deux cas, ces indices constituent des pièces essentielles pour reconstruire une histoire fiable.

L'histoire de l'investigation numérique est riche en exemples marquants. L'affaire du BTK Killer aux États-Unis, en 2005, en est une illustration célèbre. Dennis Rader, qui croyait être prudent, avait transmis à la police une disquette contenant un simple document Word. Ce document renfermait en réalité des métadonnées, des informations invisibles à première vue mais révélatrices. En l'analysant, les enquêteurs ont découvert son prénom et le nom de son église, ce qui a permis son arrestation. En 2010, l'affaire Stuxnet a montré une nouvelle facette : l'utilisation d'un virus informatique pour attaquer spécifiquement une infrastructure industrielle. C'était la naissance des cyberarmes modernes, capables d'endommager des installations sans le moindre missile. Plus récemment, en 2017, le rançongiciel WannaCry a contaminé des centaines de milliers d'ordinateurs dans plus de 150 pays, bloquant hôpitaux, entreprises et administrations. Ces exemples montrent que l'investigation numérique n'est pas théorique : elle sauve des vies, protège des États et permet de juger des criminels.

Un concept théorique central dans le domaine est celui du trilemme CRO, imaginé par l'auteur du livre M. MINKA. Il met en évidence l'impossibilité d'obtenir simultanément au maximum trois qualités : la confidentialité, la fiabilité et l'opposabilité. La confidentialité protège les données sensibles contre tout accès non autorisé. La fiabilité garantit que les preuves sont intactes et authentiques. L'opposabilité assure que les preuves peuvent être utilisées devant un tribunal et reconnues comme valides. Mais comme pour une voiture que l'on voudrait à la fois rapide, économique et peu chère, il faut accepter des compromis. Un exemple simple est celui d'une enquête sur une fraude bancaire. *Un petit programme peut calculer des indices montrant que la confidentialité des données des clients est gravement compromise, que la fiabilité technique est encore correcte mais que l'opposabilité juridique est faible, car les preuves sont endommagées.* Cet exemple démontre comment une enquête doit prioriser certaines dimensions sans pouvoir toutes les atteindre à la perfection.

Pour encadrer ce domaine, des méthodes reconnues internationalement ont été mises en place. Le modèle DFRWS, élaboré en 2001, décrit six étapes incontournables. Tout commence par l'identification du problème. Vient ensuite la préservation, qui consiste à isoler et protéger les preuves. La collecte permet de rassembler ces éléments de manière ordonnée, suivie par l'examen détaillé et l'analyse, qui recoupent les informations et reconstituent les faits. Enfin, la présentation sert à rédiger un rapport clair et à témoigner si nécessaire devant la justice. Pour illustrer cela, *un script simple en Bash montre comment copier un disque dur suspect, en calculant une empreinte numérique avant et après la copie afin de garantir que l'image obtenue est identique à l'original.* Cette rigueur assure que le travail de l'enquêteur sera reconnu devant un tribunal.

Les normes internationales renforcent ces pratiques. L'ISO/IEC 27037, par exemple, fixe quatre principes : pertinence, fiabilité, exhaustivité et traçabilité. Ne collecter que ce qui est utile, garantir des résultats reproductibles, veiller à ne rien oublier d'important et documenter soigneusement chaque étape. Ces exigences sont comparables à celles d'un laboratoire scientifique : toute expérience doit pouvoir être reproduite à l'identique par un autre chercheur pour être validée.

L'évolution technologique oblige aussi à adapter sans cesse les techniques d'enquête. Chaque système d'exploitation gère les fichiers de manière différente. Windows, avec son système NTFS, conserve énormément de métadonnées comme la Master File Table, véritable registre de tous les fichiers. Linux, avec EXT4, permet de retrouver des informations grâce à la journalisation avancée. Même lorsqu'un fichier est supprimé, il reste souvent possible de le récupérer. *Un petit programme en Python montre comment lire les entrées de cette table et générer une preuve cryptographique de leur intégrité.* Ces méthodes permettent d'aller fouiller dans la mémoire cachée des machines.

Le réseau constitue un autre champ d'investigation essentiel. Sur Internet, chaque communication laisse des traces, que ce soit des adresses IP, des protocoles ou des paquets de données. Les enquêteurs peuvent capturer et analyser ce trafic pour comprendre les échanges.
Une fonction de détection permet d'identifier si des données ont été cachées dans des communications apparemment normales, en étudiant par exemple les intervalles entre les paquets. Ce type d'analyse rend visible des canaux secrets que des cybercriminels utilisent pour dissimuler leurs activités.

L'intelligence artificielle modifie aussi profondément la discipline. Là où un humain passerait des jours à analyser des milliers de fichiers, une machine peut apprendre à reconnaître en quelques secondes des modèles caractéristiques de virus. *Un algorithme peut par exemple extraire des caractéristiques d'un fichier exécutable, comme le nombre de sections, la taille du code, le degré de désordre interne, et classer le fichier comme suspect ou non.* De la même manière, des systèmes intelligents analysent les comportements et signalent des anomalies, comme un employé qui se connecte à des heures inhabituelles ou accède à des fichiers sensibles de façon répétée.

Les défis de l'ère post-quantique s'ajoutent à ce tableau. Les ordinateurs quantiques promettent une puissance de calcul telle qu'ils pourront briser les systèmes de chiffrement actuels. L'algorithme de Shor peut casser RSA, tandis que celui de Grover réduit la sécurité des clés classiques. Certains pirates adoptent déjà une stratégie dite "collecter maintenant, déchiffrer plus tard", en stockant des données chiffrées dans l'attente des futures capacités. Pour y répondre, de nouvelles solutions cryptographiques émergent. Le NIST a sélectionné des algorithmes résistants aux attaques quantiques comme CRYSTALS-Kyber pour l'échange de clés, Dilithium pour les signatures numériques ou SPHINCS+. *Un exemple de chiffrement hybride montre comment combiner une méthode classique comme RSA avec une méthode post-quantique comme Kyber, afin de garantir la sécurité à la fois aujourd'hui et demain.* Ces transitions doivent être planifiées progressivement pour ne pas désorganiser les infrastructures.

Des innovations conceptuelles apparaissent aussi, comme le protocole ZK-NR. Il permet de prouver qu'une preuve est authentique sans en révéler le contenu. *Un programme illustre la création d'une attestation légale contraignante en plusieurs étapes : engagement cryptographique, preuve zero-knowledge, signature par plusieurs clés et authentification post-quantique.* Cela ouvre la voie à une justice numérique plus sécurisée, adaptée aux menaces du futur.

Cependant, face aux enquêteurs, les criminels développent des techniques d'anti-investigation. Ils utilisent l'effacement sécurisé, qui consiste à écraser plusieurs fois des données pour les rendre irrécupérables.**Un outil peut détecter ce type de tentative en reconnaissant des motifs d'écrasement caractéristiques.* D'autres emploient la stéganographie pour cacher des informations dans des images ou des vidéos, ou encore l'obfuscation pour rendre du code illisible. À cela s'ajoutent des systèmes de chiffrement de plus en plus puissants. Pour répondre à ces menaces, de nouvelles défenses voient le jour. *Un modèle de défense adaptative met en place une journalisation renforcée, des marqueurs pour l'investigation et une surveillance constante de l'intégrité des données.* L'intelligence artificielle joue aussi un rôle, en détectant automatiquement des techniques d'évasion sophistiquées.

L'aspect juridique n'est jamais loin. À l'échelle internationale, la Convention de Budapest de 2001 fut le premier traité sur la cybercriminalité.
Le règlement européen eIDAS encadre les signatures électroniques, tandis que le RGPD impose une protection stricte des données personnelles. Au Cameroun, la loi de 2010 sur la cybersécurité et la cybercriminalité fixe les règles. Les enquêtes suivent un processus formalisé, de la plainte initiale jusqu'à la présentation d'un rapport d'expertise au tribunal. Mais des défis subsistent : manque de formation des juges, délais d'expertise longs, coûts élevés et absence de normes nationales précises.

Un cas pratique éclaire ces difficultés : l'affaire CyberFinance Cameroun en 2025. Cette société de services financiers a subi une attaque par rançongiciel LockBit 3.0. Plus de 500 000 clients ont été affectés et 850 gigaoctets de données volées, avec une rançon de dix millions d'euros exigée. *Un script illustre la réponse d'urgence : isoler le réseau, couper la connexion et capturer les données volatiles comme les processus actifs ou les connexions ouvertes.* L'analyse a montré que le virus utilisait le chiffrement ChaCha20 combiné à RSA-2048 et qu'il s'était propagé via un email de phishing. La reconstruction chronologique a permis de dater chaque étape, depuis l'ouverture de la pièce jointe jusqu'au déploiement du rançongiciel. L'indice CRO a révélé une atteinte majeure à la confidentialité, confirmant où concentrer les efforts. Des mesures immédiates ont été prises : isolement des systèmes, réinitialisation des mots de passe et mise en place de la double authentification. À plus long terme, la société a planifié une migration vers la cryptographie post-quantique, en déployant progressivement TLS hybride et les protocoles ZK-NR pour l'audit.

La conclusion générale du manuel insiste sur la polyvalence que doit acquérir un enquêteur numérique. Il doit maîtriser les techniques informatiques, comprendre les réseaux et la cryptographie, connaître les procédures légales et agir avec une éthique irréprochable. La discipline évolue vite : les solutions d'aujourd'hui peuvent devenir obsolètes demain. Le trilemme CRO et les protocoles ZK-NR ouvrent des perspectives inédites. À court terme, le monde se dirige vers une adoption des solutions post-quantiques. À moyen terme, une standardisation internationale devrait voir le jour. À long terme, l'idée même d'une enquête numérique quantique native pourrait se concrétiser. Pour l'Afrique et le Cameroun, c'est une opportunité unique :

sauter directement vers les technologies les plus avancées sans devoir moderniser de vieux systèmes. Cela pourrait faire du continent un acteur majeur de l'investigation numérique de demain. L'enquêteur moderne doit ainsi conjuguer rigueur scientifique, compétences juridiques et sens moral. Comme le rappelle l'auteur du livre M. MINKA : *tel un artisan consciencieux et méthodique, chaque jour affine ta pratique, car ce n'est qu'ainsi que tu seras et demeureras expert.*