RÉPUBLIQUE DU CAMEROUN
*****
Paix – Travail – Patrie
*****
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR
*****
UNIVERSITÉ DE YAOUNDÉ I
*****
ÉCOLE NATIONALE SUPÉRIEURE POLYTECHNIQUE
*****
DÉPARTEMENT DE GÉNIE INFORMATIQUE

REPUBLIC OF CAMEROON
*****
Peace – Work – Fatherland
*****
MINISTRY OF HIGHER EDUCATION
*****
UNIVERSITY OF YAOUNDE I
*****
NATIONAL ADVANCED SCHOOL OF ENGINEERING
*****
COMPUTER ENGINEERING DEPARTMENT

INTRODUCTION AUX TECHNIQUES D'INVESTIGATION NUMÉRIQUE

RESUME DE COURS 0

N°	MLE	NOMS ET PRÉNOMS	NOTE
1	22P064	MENGUE BISSA MARGUERITE	

Sous la supervision de : M.MINKA Thierry

ANNÉE ACADÉMIQUE 2025 – 2026

L'investigation numérique n'est pas seulement un ensemble de techniques ; elle repose sur une véritable **philosophie du numérique**. Elle s'inscrit dans une interrogation épistémologique profonde : **comment établir la vérité dans un monde où la donnée est à la fois source de transparence et d'opacité ?**

Cette réflexion se décline en plusieurs dimensions complémentaires, chacune apportant un éclairage particulier :

- **Dimension épistémologique :** l'être humain n'existe plus seulement dans sa réalité physique, mais également dans son prolongement numérique. À travers ses traces digitales, chaque individu projette une part de son identité dans le cyberespace. Ces empreintes deviennent autant de témoins de son existence.
- **Dimension ontologique :** le "double numérique" est considéré comme une véritable extension de l'être, aussi réelle et signifiante que sa présence matérielle. L'existence humaine ne se limite donc plus au monde tangible : elle s'étend au virtuel.
- **Approche phénoménologique :** les données numériques sont envisagées comme des manifestations d'existence, au même titre que des témoignages oraux ou des traces matérielles. Chaque fichier, chaque log ou métadonnée constitue une preuve de passage.
- **Dimension métaphysique :** cette réflexion ouvre la voie à de nouveaux modes d'existence et de relation rendus possibles par le digital. Le numérique n'est plus seulement un outil, il devient un espace d'être.

Cette philosophie du numérique révèle un **paradoxe central** : la tension entre **transparence** et **intimité**. Le numérique tend à rendre les données accessibles et vérifiables, mais cette exigence entre en conflit avec le droit fondamental à la vie privée. Ainsi, l'**investigateur numérique** doit naviguer dans une zone grise où se confrontent vérité universelle et préservation de l'intimité.

Sur le plan théorique, plusieurs disciplines scientifiques enrichissent l'investigation numérique. Elles apportent chacune des outils de compréhension spécifiques :

- **La théorie de l'information de Shannon :** elle permet de mesurer l'incertitude informationnelle et de détecter des anomalies à travers le calcul de l'entropie.
- **La théorie des graphes :** elle fournit des outils puissants pour modéliser les relations sociales et techniques, en mettant en évidence des structures cachées et des réseaux d'influence.
- **La théorie du chaos :** elle montre que dans des systèmes complexes, de petites altérations peuvent produire des conséquences majeures. Elle souligne ainsi l'importance de la rigueur dans la manipulation des preuves numériques.

La révolution quantique a accentué cette complexité. En remettant en cause les certitudes du déterminisme classique, elle introduit des notions comme la superposition, la non-localité et l'intrication, qui bouleversent les critères traditionnels de preuve et d'authenticité. C'est dans ce cadre que surgit le paradoxe de l'authenticité invérifiable :**plus une preuve numérique est révélée pour attester de son authenticité, plus elle fragilise sa confidentialité**. La cryptographie moderne, notamment les preuves à divulgation nulle de connaissance (Zero-Knowledge Proofs), tente de résoudre cette tension en conciliant exigence de vérification et protection de la vie privée.

L'investigation numérique apparaît ainsi comme une discipline hybride : elle est à la fois archéologie digitale, épistémologie appliquée et éthique pratique.L'investigateur devient un médiateur entre vérité et secret, chargé de préserver l'intégrité de la mémoire collective tout en respectant les droits fondamentaux.

Sur le plan opérationnel, cette médiation s'incarne dans le respect strict de principes directeurs universels. Les principes ACPO (Association of Chief Police Officers) en sont le fondement intangible : Aucune action ne doit modifier les données originales ; Si une modification est

nécessaire, la personne doit être compétente pour le faire ; Un audit complet de toutes les actions doit être conservé ; Le responsable de l'enquête doit assurer la conformité à ces principes. Ces règles ne sont pas de simples recommandations mais la condition sine qua non de l'opposabilité juridique de la preuve numérique, garantissant que son intégrité n'a pas été altérée de sa collecte à sa présentation en justice.

Si la philosophie fonde l'investigation numérique, c'est la cybersécurité et la forensique qui en assurent l'efficacité opérationnelle. Leur objectif est de garantir **la fiabilité et la valeur légale des preuves, tout en s'adaptant à des environnements technologiques en constante mutation. Cette adaptation est encadrée par une armature normative robuste et multiniveaux.**

Les standards internationaux jouent un rôle central. Les normes ISO/IEC (27037, 27041, 27042, 27043) et les guides comme le NIST SP 800-86 ou le RFC 3227 fixent les principes fondamentaux de la collecte, de l'analyse et de la conservation des preuves numériques. La norme ISO 27037, par exemple, décrit un processus de saisie rigoureux : identification préliminaire du dispositif, documentation photographique, isolation (notamment via des sacs Faraday pour les mobiles), acquisition avec un write-blocker obligatoire, vérification par hachage cryptographique (SHA-256 minimum), puis scellement et transport. Le RFC 3227, quant à lui, établit l'ordre de volatilité, dictant la priorité de collecte en commençant par les données les plus éphémères (registres CPU, mémoire vive) pour terminer par les plus persistantes (disques durs).

Ces standards et principes s'illustrent dans des contextes variés : affaires de fuite de données, où l'analyse des logs SIEM et l'imagerie des postes de travail sont cruciales ; cyberharcèlement, où la saisie judiciaire et l'expertise des communications sont centrales ; espionnage industriel ou cyberattaques contre des infrastructures critiques, où le threat hunting et l'analyse des mouvements latéraux dans le réseau prennent le dessus. Chaque cas met en évidence l'importance d'une grille d'évaluation solide, comme le cadre CRO (Confidentialité, Fiabilité, Opposabilité), qui sert de référence universelle pour évaluer la

qualité et les compromis inhérents à toute investigation. La Fiabilité (Reliability) assure ici l'intégrité, l'authenticité et la disponibilité de la preuve. Une preuve très fiable (une signature cryptographique) peut avoir une faible confidentialité, et inversement. Le cadre CRO formalise ce trilemme et guide l'investigateur dans ses choix techniques. Au-delà des normes, plusieurs méthodologies structurées sont mobilisées :

- **Le modèle SANS FOR508** (Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned) et le processus CERT/CC offrent des cadres d'action clairs pour la réponse aux incidents.
- **Le modèle de Casey et les lignes directrices de l'ENISA complètent ce paysage méthodologique**. Ces approches rappellent que la discipline ne se limite pas à la collecte d'indices, mais qu'elle s'inscrit dans un cycle global de prévention, de réaction et d'amélioration continue.
- **L'analyse formelle avec des outils comme Tamarin Prover** permet, en amont, de modéliser les protocoles de sécurité et de vérifier automatiquement leurs propriétés contre un adversaire actif

La tension entre investigation et RGPD est permanente : le droit à l'effacement s'oppose à la préservation des preuves, la minimisation des données à la collecte exhaustive nécessaire à l'enquête. L'article 23 du RGPD offre des dérogations pour la prévention et la détection d'infractions, mais leur application demande une appréciation minutieuse au cas par cas : Un premier défi majeur concerne donc l'équilibre entre sécurité et liberté individuelle. Garantir l'intégrité et l'opposabilité des preuves ne doit pas se faire au détriment des droits fondamentaux. L'investigateur doit être à la fois garant de la vérité et protecteur de la vie privée, un équilibre qui repose sur une éthique professionnelle robuste et une connaissance fine du cadre juridique, qu'il soit international (Convention de Budapest), européen (eIDAS) ou local (comme la Loi camerounaise de 2010 sur la cybersécurité),un

second défi, plus technique, réside dans l'anticipation des menaces post-quantiques. L'arrivée d'ordinateurs quantiques capables de briser les systèmes cryptographiques actuels impose une révision profonde des standards de sécurité et des pratiques d'archivage des preuves. Une signature numérique, parfaitement opposable aujourd'hui, pourrait être forgée dans une décennie, anéantissant sa valeur probante à long terme. Il devient impératif de migrer vers des schémas cryptographiques hybrides ou purement post-quantiques pour les scellés numériques et les horodatages.Enfin, l'internationl'internationalisation des menaces appelle une coopération mondiale renforcée. Les cyberattaques ne connaissent pas de frontières, ce qui rend indispensable une harmonisation des normes et des procédures, ainsi qu'une collaboration opérationnelle et juridique accrue entre États, entreprises et institutions judiciaires. Des cadres comme la Convention de Budapest jettent des bases, mais leur application concrète reste un défi quotidien.

L'investigation numérique et la cybersécurité apparaissent ainsi comme les deux faces indissociables d'une même médaille :

- **La première** enracine la discipline dans une réflexion philosophique et éthique profonde sur la vérité et la mémoire numérique.
- **La seconde** lui confère une efficacité opérationnelle à travers des normes, des méthodologies structurées et des outils sophistiqués. Ensemble, elles dessinent une discipline hybride, à la fois conceptuelle et pratique, capable de répondre aux enjeux actuels et futurs.

L'avenir de cette discipline dépendra de sa capacité à concilier rigueur scientifique, agilité technologique et respect des droits fondamentaux. Elle devra intégrer de nouveaux paradigmes comme l'analyse prédictive, la forensique d'IA (pour investiguer les attaques générées par des modèles de deep learning) et peut-être un jour, la forensique quantique. Loin d'être un simple domaine technique, l'investigation numérique se révèle comme une composante essentielle de notre pacte social numérique, au service de la justice, de la vérité et de la confiance collective sans laquelle aucune société ne peut fonctionner.