REPUBLIQUE 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 Yaoundé I
*****
NATIONAL ADVANCED SCHOOL OF ENGINEERING
*****
Computer Engineering Department
*****

SEC 4031 INTRODUCTION AUX TECHNIQUES D'INVESTTGATION NUMERIQUE

RESUME DU COURS

Filière : HUMANITÉS NUMÉRIQUES

Niveau : IV

Rédigé par :

NGUEMO VOUFO AURELLE SANDRA 22P067 CIN4

Sous la supervision de :

Mr. MINKA

ANNEE ACADEMIQUE :2025-2026

INTRODUCTION GENERALE DU COURS

L'investigation numérique constitue aujourd'hui une discipline scientifique et opérationnelle incontournable dans la lutte contre la cybercriminalité et la gestion des preuves numériques. À la croisée de la cybersécurité, du droit, de la cryptographie et des sciences de l'information, elle répond à des enjeux cruciaux : garantir l'intégrité, l'authenticité et l'opposabilité juridique des traces numériques dans un monde marqué par la dématérialisation et l'essor des technologies comme l'informatique quantique.Le cours est structuré en 10 grandes parties, qui couvrent à la fois les fondements théoriques, les normes et standards, les meilleures pratiques mondiales, ainsi que l'application concrète à travers une étude de cas intégrée. Chaque partie est subdivisée en chapitres, permettant d'approfondir progressivement les connaissances.

I. Fondements, Historique et Évolution

Regroupant quatre chapitres, ici est établit les bases épistémologiques de l'investigation numérique, on retrouve le principe de Locard (« toute action laisse une trace ») adapté au numérique, ainsi que les théories de Claude Shannon (théorie de l'information) et Kurt Gödel (incomplétude, limites formelles). Sur le plan historique, des affaires comme Clifford Stoll (espionnage, 1986), Silk Road ou SolarWinds montrent comment les cyberattaques ont façonné la discipline. Le paradoxe de l'« authenticité invisible » (preuve numérique valide mais intangible) est aussi présenté.Cette partie introduit l'investigation numérique comme une discipline à la croisée de la philosophie, des sciences exactes et de la cybersécurité. Elle revient sur la transformation de la société à l'ère numérique et les nouveaux enjeux liés à la preuve dématérialisée. Les fondements mathématiques (théorie de l'information, graphes, chaos) et l'arrivée du paradigme quantique redéfinissent la fiabilité des traces. L'auteur expose également le paradoxe de l'authenticité invisible, qui questionne la capacité à démontrer la vérité numérique. Enfin, un panorama historique retrace l'évolution de la discipline, des premiers hackers aux affaires comme Enron, Silk Road ou SolarWinds, montrant comment les cyberattaques ont façonné les pratiques forensiques.

II. Cadre Théorique et Conceptuel

Regroupant trois chapitres, ici sont posées les méthodes structurantes de la discipline. L'auteur mobilise le modèle DFRWS (Carrier, 2001), le modèle de Casey, et la norme ISO/IEC 27037. La théorie des graphes (Erdős et Rényi) est utilisée pour modéliser les réseaux d'interactions, tandis que Shannon éclaire la valeur informationnelle d'une trace. Le principe de Locard est décliné en version numérique : chaque interaction informatique génère une empreinte exploitable. L'ensemble construit une assise scientifique pour légitimer l'investigation numérique.Cette section présente les bases conceptuelles nécessaires pour analyser une enquête numérique. Le principe de Locard appliqué au numérique rappelle que toute interaction laisse une trace, directe ou secondaire. Les grands modèles théoriques (DFRWS, Casey, ISO/IEC 27037) structurent les méthodologies d'investigation et assurent une cohérence scientifique et opérationnelle. Les apports de la théorie de l'information permettent de mesurer la pertinence des données, tandis que la théorie des graphes aide à modéliser les relations entre acteurs ou systèmes. L'ensemble établit une

épistémologie solide pour l'investigation numérique.

III. Normes et Standards Internationaux

Regroupant quatre chapitres, cette partie presente les cadres normatifs qui garantissent la légitimité et la comparabilité des preuves numériques. Les standards ISO/IEC (27037, 27041, 27042, 27043) définissent les étapes de collecte, de conservation et d'analyse des traces numériques. Le NIST SP 800-86 et le RFC 3227 introduisent l'ordre de volatilité (préserver d'abord les données fragiles en RAM). Le guide ACPO(UK, 2007), pilier britannique, insiste sur la rigueur procédurale. Enfin, les standards émergents (Cloud Forensics, IoT Forensics) montrent l'adaptation nécessaire face aux environnements technologiques modernes.Et aussi l'ENISA en Europe et le CERT comme structures pivot. Ces standards garantissent que la preuve numérique reste juridiquement opposable.

IV. Meilleures Pratiques Mondiales

Regroupant trois chapitres, cette partie compare les méthodologies d'investigation à l'échelle internationale. Les États-Unis privilégient la puissance technologique et la normalisation (FBI, NIST), tandis que le Royaume-Uni met en avant la rigueur procédurale (ACPO). L'Europe, avec l'ENISA, insiste sur une approche collaborative, et l'Asie mise sur l'innovation technologique (Singapour, Corée du Sud). Des cas concrets – fraude mobile en Afrique, cyberterrorisme au Moyen-Orient, narcotrafic numérique en Amérique latine – illustrent l'application de ces approches. Ces cas permettent de conclure que l'excellence repose sur la contextualisation, l'adaptabilité et la coopération internationale.

V. L'Ère du Post-Quantique

Regroupant trois chapitres, ici est presenté l'impact des ordinateurs quantiques sur la sécurité. Les algorithmes de Shor (1994) et Grover (1996) menacent RSA et AES. Le concept « Harvest Now, Decrypt Later » (intercepter aujourd'hui, déchiffrer demain) est un danger majeur. Le NIST (2016–2022) pilote la sélection de nouvelles primitives de cryptographie post-quantique (lattice-based, code-based, multivariate).Cette partie analyse l'impact imminent de l'informatique quantique sur la cybersécurité et l'investigation. Des algorithmes menacent les cryptosystèmes actuels, permettant de casser le chiffrement asymétrique ou d'accélérer la recherche dans de grandes bases de données. Le concept « Harvest Now, Decrypt Later » illustre le danger des données interceptées aujourd'hui pour être décryptées plus tard. Face à cela, la cryptographie post-quantique (PQC) émerge, avec les standards en cours de sélection par le NIST. L'investigation doit intégrer ces nouveaux outils pour garantir la validité et l'opposabilité des preuves à long terme.

VI. Primitives Cryptographiques et Opposabilité

Regroupant trois chapitres, cette section développe le Trilemme CRO (Confidentialité, Fiabilité, Opposabilité juridique), qui illustre l'impossibilité d'optimiser simultanément ces trois dimensions dans une preuve numérique. L'introduction du protocole ZK-NR (Zero-Knowledge Non-Repudiation) propose une solution innovante pour valider des

preuves sans compromettre la confidentialité. L'architecture Q2CSI offre une modularité permettant d'adapter la collecte et la vérification des preuves selon les besoins. Cette partie insiste sur la nécessité de penser la cryptographie non seulement comme un outil technique, mais aussi comme un garant juridique de la validité des preuves.L'objectif est de concilier exigences techniques (sécurité, efficacité) et validité devant un tribunal.

VII. Cryptanalyse et Analyse de Protocoles

Regroupant trois chapitres, cette partie aborde la vérification et les vulnérabilités. Ici est cité le modèle formel de Dolev–Yao (1983) et des outils modernes comme Tamarin ou ProVerif pour tester les protocoles. La cryptanalyse est divisée entre approche black-box et white-box. L'étude de cas avec BLS (Boneh–Lynn–Shacham, 2001) et le protocole ZK-NR illustre les forces mais aussi les limites des nouvelles primitives. L'enjeu : s'assurer que les protocoles garantissent bien l'intégrité et la valeur probante des preuves.cette partie expose ici les méthodes d'évaluation de la robustesse des protocoles et algorithmes utilisés en investigation. L'opposition entre approches black-box et white-box permettent de comprendre les vulnérabilités exploitées. L'analyse formelle (via le modèle de Dolev-Yao et des outils comme Tamarin) structure l'audit en cinq étapes, de la compréhension à l'implémentation. L'objectif est de donner à l'investigateur une grille de lecture critique et une checklist d'évaluation face à des protocoles complexes.

VIII. Cadre Juridique

Regroupant trois chapitres,La diversité légale est examinée ici : * États-Unis : ils structurent la recevabilité des preuves avec la Federal Rules of Evidence, CFAA (1986), Patriot Act (2001).

* Europe :privilégie la protection des données avec la Convention de Budapest (2001), RGPD (2018).

* Afrique : Convention de Malabo (2014), lois nationales (ex. Cameroun 2010, 2024). Les défis principaux sont la cybercriminalité transnationale, l'extraterritorialité des preuves et l'équilibre entre vie privée et sécurité. Ici le droit tente de suivre la vitesse des innovations technologiques.Cette partie met en lumière l'importance des lois et conventions qui encadrent l'investigation numérique.ici on insiste sur les défis juridiques : coordination transfrontalière, reconnaissance des preuves, équilibre entre sécurité et vie privée.

IX. Pratique du Forensique

Regroupant quatres chapitres,Un guide pratique pour créer et gérer un laboratoire forensique. L'infrastructure peut utiliser des distributions comme SIFT (SANS), Remnux, ou des outils commerciaux (EnCase, FTK). Les procédures standardisées (SOP), la chaîne de custody et la traçabilité sont essentielles. L'auteur cite aussi Carrier et Spafford (2004) sur la rigueur scientifique. La formation continue, les certifications (ex. CFCE, EnCE) et les exercices de red teaming assurent une qualité constante.Cette partie fournit un guide pratique pour l'installation et la gestion d'un laboratoire forensique. Elle décrit l'infrastructure nécessaire (SIFT, Remnux, outils open source et commerciaux), les procédures standards (checklists, rapports types, scripts d'automatisation) et les exigences de certification. La gestion efficace d'un laboratoire repose sur la maîtrise de la chaîne de custody

physique et numérique. L'auteur insiste aussi sur la formation continue, la veille technologique et les exercices de red teaming pour maintenir un haut niveau de compétence et de réactivité.

X. Cas Pratique Intégré

Ce dernier chapitre applique les concepts théoriques dans une étude de cas réelle : l'affaire CyberFinance Cameroun 2025, une attaque ransomware post-quantique. L'analyse retrace six phases : détection, investigation technique, collecte de preuves, analyse approfondie, remédiation et aspects juridiques. L'usage de la norme ISO 27037, du protocole ZK-NR et des standards post-quantiques illustre la mise en œuvre pratique des notions vues précédemment. La conclusion tire des leçons sur la résilience organisationnelle et propose un cadre post-quantique pour préparer les futures enquêtes.