REPUBLIQUE DU CAMEROUN

Paix – Travail – Patrie

****

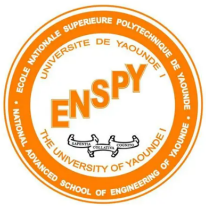
UNIVERSITE DE YAOUNDE I

****

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 ENGINEERING

Résumé du Manuel: Théories et Pratiques de l'Investigation Numérique

---

Étudiant: TAPA LOIC
Matricule: 22P108

Superviseur: M. Minka
Cours: Investigation Numérique

Année Académique: 2025/2026

Date: September 16, 2025

Introduction

L'investigation numérique combine technique, éthique et enjeux sociaux. Chaque compétence confère un pouvoir sur les systèmes numériques, imposant une responsabilité éthique. Les principes d'intégrité, proportionnalité et responsabilité guident les actions des professionnels.

Philosophie et Fondements

Redéfinition de la vérité et justice à l'ère numérique. Le pouvoir technique s'accompagne d'une responsabilité éthique. Préservation de l'intégrité des systèmes et des données.

Histoire de l'Investigation Numérique

Évolution depuis les années 1970. Opération Sundevil et nécessité de méthodologies standardisées. Affaires emblématiques comme Enron et Silk Road.

Les Grandes Affaires

Affaires BTK, Stuxnet et WannaCry. Rôle crucial des métadonnées. Importance de l'analyse des données et collaboration.

Fondements Théoriques

Principe de Locard : "toute action laisse une trace". Modèles théoriques comme DFRWS. Approche scientifique rigoureuse.

État de l'Art et Évolution

Évolution des techniques vers cloud forensics. Analyse des données massives et IA. Adaptation continue nécessaire.

Cadre Normatif Global

Normes ISO et NIST essentielles. Défis de l'application mondiale. Harmonisation internationale cruciale.

Applications et Cas d'Usage

Diversité des approches selon contextes culturels. Framework CRO (Confidentialité, Fiabilité, Opposabilité).

Méthodologies d'Investigation

Méthodologies SANS Institute. Procédures opérationnelles standardisées. Structuration de la réponse aux incidents.

Outils et Techniques Avancées

Acquisition et imagerie forensiques. Méthodes anti-anti-forensique. Mise à jour régulière des outils.

Impact du Quantique

Implications de l'algorithme de Shor. Risque de décryptage quantique. Nécessité d'algorithmes post-quantiques.

Le Trilemme CRO

Compromis entre confidentialité, fiabilité et opposabilité. Cadre crucial pour la conception de systèmes sécurisés.

Analyse des Primitives

Évaluation des primitives cryptographiques. Compromis inhérents à chaque primitive. Architectures hybrides nécessaires.

Le Protocole ZK-NR

Zero-Knowledge Non-Repudiation. Préservation de la confidentialité. Applications en investigation numérique.

Conception et Cryptanalyse

Principes de conception sécurisée. Devoir de méfiance et minimalisme. Taxonomie des failles cryptographiques.

CAnalyse Formelle de Protocoles

Modèle Dolev-Yao. Formalisation des propriétés de sécurité. Outil Tamarin pour validation.

Cas Pratique du Protocole ZK-NR

Application de l'analyse formelle. Résistance aux attaques post-quantiques. Vulnérabilités des signatures BLS.

Législation Mondiale

Cadres juridiques américains et RGPD. Tensions entre droit à l'effacement et préservation des preuves. Harmonisation africaine.

Droit Camerounais

Cadre législatif camerounais. Défis de formation. Sensibilisation et formation continue.

Pratiques Opérationnelles

Mise en place de laboratoire forensique. Procédures standardisées. Formation continue des enquêteurs.

Forensique Système Avancée

Analyse des artefacts systèmes. Défis des systèmes modernes (APFS, NTFS). Préservation de l'intégrité.

Forensique Réseau

Reconstitution des activités numériques. Analyse passive, active et prédictive.

Anti-Forensique

Techniques d'entrave aux enquêtes. Méthodes de dissimulation et destruction. Contremesures et protocoles.

Benchmarking des Pratiques

Évaluation des pratiques forensiques mondiales. Partage d'informations. Cadre d'excellence adaptatif.

Perspectives Futures

Défis technologiques et réglementaires. Innovation continue et collaboration internationale. Adaptation aux nouvelles réalités.

Conclusion Générale

Synthèse des concepts du Trilemme CRO et protocole ZK-NR. Collaboration internationale essentielle. Adoption de pratiques standardisées.

Bibliographie

Références essentielles classées par catégories : recherches, normes techniques et cadres juridiques.