RÉPUBLIQUE DU CAMEROUN
****
Paix - Travail - Patrie
****

UNIVERSITÉ DE YAOUNDÉ I
****

ÉCOLE NATIONALE SUPÉRIEURE POLYTECHNIQUE DE YAOUNDÉ
****

DÉPARTEMENT DE GÉNIE
****

REPUBLIC OF CAMEROON
****
Peace - Work - Fatherland
****

UNIVERSITY OF YAOUNDE I
****

NATIONAL ADVANCED SCHOOL OF ENGINEERING OF YAOUNDE
****

COMPUTER ENGINEERING
****

Techniques et pratiques de l'investigation numérique

Sous le thème : Resumé Techniques et pratiques de l'investigation numérique

EMBOLO MVOGO SHAWN DOUGLAS

22P072

Filiére : CIN4

Sous la supervision de : **Mr Minka**

Année Scolaire : **2025 – 2026**

Résumé de l'Investigation Numérique Éthique

L'investigation numérique éthique constitue un pilier central de la cybersécurité et de la lutte contre la criminalité informatique. Elle dépasse le simple cadre technique pour questionner les fondements de la vérité, de la confiance et de la justice à l'ère numérique. Elle exige un équilibre subtil entre compétences techniques pointues, sagesse, humilité et rigueur morale.

Le **Contrat Déontologique de l'Investigateur Numérique** représente un engagement moral entre l'apprenant et la communauté des professionnels, soulignant que la maîtrise des outils et des techniques numériques confère un pouvoir considérable et que l'investigation numérique n'est jamais neutre. Chaque technique maîtrisée ou outil utilisé confère une influence sur les systèmes numériques et sur les vies qui y sont connectées.

1 Engagements et Serment de l'Investigateur

Le serment de l'investigateur numérique implique des engagements fondamentaux :

- Utiliser ses compétences exclusivement à des fins légitimes, autorisées et éthiques.
- Respecter strictement les cadres juridiques nationaux et internationaux.
- Préserver l'intégrité des systèmes et des données analysées.
- Protéger la confidentialité des informations.
- Assurer une traçabilité complète et irréprochable de toutes les actions.

1.1 Limitations éthiques

L'investigateur s'engage à ne jamais utiliser ses compétences pour :

- Porter atteinte à la vie privée sans mandat légitime.
- Compromettre l'intégrité des systèmes sans autorisation.
- Altérer ou détruire des preuves numériques.
- Faciliter des activités illicites ou malveillantes.

1.2 Les quatre piliers fondamentaux

- **Intégrité** : véracité des conclusions, transparence des méthodes et reconnaissance des limites.
- **Proportionalité** : adéquation des moyens aux fins, minimisation de l'intrusion et respect de la vie privée.
- **Responsabilité** : acceptation des conséquences de ses actions, devoir de vigilance et engagement dans la formation continue.

- **Service** : mise des compétences au service de la justice, de la vérité et de la protection des droits.

1.3 Les dix commandements de l'investigateur

1. Ne pas causer de dommages aux systèmes investigués.
2. Respecter la vie privée et la dignité des personnes.
3. Maintenir une chaîne de custody irréprochable.
4. Documenter intégralement les processus et décisions.
5. Reconnaître ses limites.
6. Résister aux pressions contraires à l'éthique.
7. Protéger les données sensibles en sa garde.
8. Témoigner avec honnêteté et objectivité.
9. Contribuer au développement de la discipline.
10. Honorer la confiance que la société place en soi.

2 Philosophie et Fondements

L'investigation numérique explore ses dimensions philosophiques, épistémologiques, éthiques et ontologiques. Elle interroge la nature de l'existence numérique et les relations entre l'être physique et son double numérique. La société numérique est confrontée au paradoxe entre transparence et droit à l'intimité, et l'investigateur opère à cette intersection délicate.

2.1 Épistémologie de la Preuve Numérique

La preuve numérique se distingue de la preuve traditionnelle par son immatérialité, sa volatilité, sa mutabilité et son authenticité dépendante de la chaîne de confiance. Elle ajoute une dimension temporelle complexe, où chaque événement laisse une empreinte digitale unique.

3 Histoire et Évolution

3.1 Prémices (1970-1990)

- 1971 : The Creeper, premier ver informatique.
- 1979 : Première saisie de données par le FBI.
- 1983 : Affaire des 414s $\rightarrow$ création du Computer Fraud and Abuse Act (1986).
- 1984 : Dan Farmer formalise le concept de Computer Forensics.

3.2 Professionnalisation (1990-2000)

Structuration de la discipline et adoption d'outils spécialisés pour faire face à l'augmentation des cybermenaces.

3.3 Standardisation (2000-2010)

Publication de la RFC 3227 et développement de frameworks comme Sleuth Kit pour uniformiser les pratiques.

3.4 Big Data et Cloud (2010-2020)

Adaptation aux volumes massifs de données et au cloud computing, illustrée par les affaires Panama Papers (2016) et WannaCry (2017).

4 Fondements Théoriques

4.1 Principe de Locard Numérique

Le principe original d'Édmond Locard stipule que "toute action laisse une trace". En investigation numérique, ce principe se décline en deux catégories de traces :

- **Traces Primaires** :
  - *Logs système* : Enregistrements horodatés des événements.
  - *Artefacts de registre* : Modifications dans les bases de registre.
  - *Fichiers temporaires* : Incluant le cache, le swap et les fichiers d'hibernation.
- **Traces Secondaires** :
  - *Métadonnées* : Telles que les données EXIF, les timestamps et les propriétés de fichiers.
  - *Corrélations réseau* : Incluant les flux NetFlow et les captures PCAP.
  - *Empreintes comportementales* : Des schémas d'utilisation révélant des patterns d'activité.

4.2 Modèles d'Investigation

Plusieurs modèles structurés guident l'approche des investigations numériques pour assurer une méthodologie rigoureuse :

- **Le Modèle DFRWS (Digital Forensic Research Workshop Framework) (2001)** :
  1. *Identification* : Reconnaître les incidents.
  2. *Préservation* : Isoler et protéger les preuves.
  3. *Collection* : Acquérir les preuves de manière méthodique.

4. *Examination* : Réaliser une analyse détaillée.
5. *Analysis* : Corréler les informations et reconstituer les événements.
6. *Presentation* : Préparer le rapport et le témoignage.

- **Le Modèle de Casey (Enhanced Integrated Digital Investigation Process) (2004)** :

1. Phase 1 : *Readiness* (Préparation)
2. Phase 2 : *Deployment* (Déploiement)
3. Phase 3 : *Physical Crime Scene* (Scène de crime physique)
4. Phase 4 : *Digital Crime Scene* (Scène de crime numérique)
5. Phase 5 : *Review* (Révision)

- **Le Modèle ISO/IEC 27037:2012** : Ce standard international fournit des lignes directrices pour :
  - L'Identification des preuves numériques.
  - La Collection/Acquisition des preuves.
  - La Préservation des preuves.
  - La Documentation des processus.

4.3 6.1 Normes et Standards Internationaux

- **ISO/IEC 27037:2012** : "Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'identification, la collecte, l'acquisition et la conservation des preuves numériques".
- **ISO/IEC 27041:2015** : "Lignes directrices pour assurer la pertinence et l'adéquation des méthodes d'enquête sur les incidents".
- **ISO/IEC 27042:2015** : "Lignes directrices pour l'analyse et l'interprétation des preuves numériques".
- **ISO/IEC 27043:2015** : "Principes et processus d'enquête sur les incidents".
- **NIST SP 800-86** : "Guide pour l'intégration des techniques forensiques dans la réponse aux incidents".
- **RFC 3227 (BCP 55)** : "Lignes directrices pour la collecte et l'archivage des preuves".

L'investigation numérique s'adapte différemment selon les contextes géopolitiques, juridiques et culturels, présentant cette diversité comme une richesse méthodologique et un défi d'harmonisation. Les cas mondiaux sont souvent évalués selon le framework du **Trilemme CRO (Confidentialité, Fiabilité, Opposabilité juridique)**.

5 Cadre Normatif et Réglementaire

- ISO/IEC 27037, ISO/IEC 27041-27043
- NIST SP 800-86
- RFC 3227
- ACPO Good Practice Guide
- Adaptation aux environnements Cloud et IoT : ISO/IEC 27050, CSA Guidelines, IEEE P2933, ETSI TR 103 939

6 Applications et Cas d'Usage

6.1 Local – Cameroun

Le Cameroun sert d'exemple pour illustrer l'application de l'investigation numérique dans un contexte local.

6.1.1 7.1.1 Environnement d'Entreprise : Fuite de Données Sensibles

- **Contexte et Incident** : Une entreprise pharmaceutique de 10 000 employés subit une fuite de formules brevetées.
- **Méthodologie appliquée (ISO 27043)** :
  - *Détection* : Alerte d'un système de prévention des pertes de données (DLP).
  - *Préservation* : Création de snapshots de machines virtuelles suspectes, isolation réseau et préservation des logs via un SIEM.
  - *Collecte* : Acquisition d'images disque des postes de travail (avec dd, dcfldd), exportation des logs centralisés et capture du trafic réseau (tcpdump).
  - *Analyse* : Utilisation d'outils comme Plaso/log2timeline pour l'analyse chronologique, RegRipper pour l'analyse du registre et examen des fichiers PST pour les e-mails.
  - *Résultats* : Identification d'une menace interne (insider threat), reconstruction du chemin d'exfiltration et création d'un paquet de preuves.

6.2 International

Exemples : cyber-espionnage industriel, ransomwares, manipulation électorale, cyberterrorisme, fraude mobile, criminalité environnementale digitale, narcotrafic numérique. Chaque contexte nécessite une adaptation méthodologique selon le Trilemme CRO (Confidentialité, Fiabilité, Opposabilité juridique).

L'investigation numérique est une discipline dynamique, intégrant intelligence artificielle, big data et cryptographie post-quantique. Elle repose sur l'éthique, la rigueur scientifique

et la responsabilité sociale. L'excellence d'un investigateur se mesure à son engagement moral et sa capacité à protéger la vérité, la justice et la mémoire collective dans un monde numérique complexe et globalisé.