



ÉCOLE NATIONALE SUPÉRIEURE POLYTECHNIQUE DE YAOUNDÉ

DÉPARTEMENT DE GÉNIE INFORMATIQUE

INTRODUCTION AUX TECHNIQUES D'INVESTIGATION NUMÉRIQUE

Rapport d'Investigation Numérique (OSINT)



MAKEU TENKU STELY BELVA
CIN-4

Superviseur : M. THIERRY
MINKA

Table des matières

| | |
|---|----------|
| Introduction | 2 |
| 1 Ce qu'on savait déjà sur la cible | 3 |
| 1.1 Informations déclaratives | 3 |
| 1.2 Hypothèses initiales | 3 |
| 2 Méthodologie utilisée pour le traquer en ligne | 4 |
| 2.1 Approche générale | 4 |
| 2.2 Outils et ressources mobilisés | 4 |
| 2.3 Procédure de collecte et d'analyse | 5 |
| 3 Résultats obtenus | 6 |
| 3.1 Inventaire des éléments trouvés | 6 |
| 3.2 Exemples d'extractions pertinentes | 6 |
| 4 Comparaison entre hypothèses et résultats | 7 |
| 4.1 Identité / Alias | 7 |
| 4.2 Localisation | 7 |
| 4.3 Synthèse générale | 8 |
| 5 Conclusion et recommandations | 9 |

Introduction

Ce rapport présente le travail d'investigation numérique réalisé dans le cadre du cours d'Introduction aux Techniques d'Investigation Numérique. L'objectif est d'appliquer une méthodologie OSINT (Open Source Intelligence) pour collecter, analyser et confronter des informations disponibles publiquement afin de vérifier certaines hypothèses sur un sujet défini.

Chapitre 1

Ce qu'on savait déjà sur la cible

1.1 Informations déclaratives

Avant le lancement de l'investigation numérique, certaines informations de base étaient déjà connues concernant la cible, identifiée sous le nom **Olivia S.**. Ces informations provenaient de sources académiques et de recoupements publics.

- **Nom** : Olivia S.
- **Parcours académique** : Titulaire du *GCE Advanced Level* obtenu en 2022, à **SBCBC**.
- **Admission** : Intégration à l'**École Nationale Supérieure Polytechnique de Yaoundé (ENSPY)** la même année, dans la filière identifiée par le code **AHN**.
- **Statut actuel** : Étudiante à l'ENSPY pour l'année académique **2024/2025**.

1.2 Hypothèses initiales

1. Olivia S. maintient une activité numérique liée à son environnement académique (groupes ENSPY, réseaux étudiants).
2. Des traces d'activité sur les réseaux sociaux permettent de confirmer son identité et son parcours.
3. L'ingénierie sociale peut aider à évaluer la nature et la cohérence de sa présence numérique.

Chapitre 2

Méthodologie utilisée pour le traquer en ligne

2.1 Approche générale

L'investigation s'inscrit dans une démarche d'**intelligence open source (OSINT)** fondée sur la recherche, la vérification et la corrélation d'informations accessibles publiquement. Elle repose sur une approche systématique visant à reconstruire la présence numérique de la cible à partir de traces éparses et non intrusives.

- **Type d'investigation** : OSINT / Analyse de métadonnées / Corrélation multi-plateforme.
- **Méthodologie** :
 1. *Collecte passive* des données ouvertes (sans interaction directe).
 2. *Enrichissement contextuel* à l'aide d'outils d'indexation et d'analyse.
 3. *Corrélation croisée* entre différentes plateformes pour valider les identités.
 4. *Archivage et documentation* des résultats (captures, empreintes).
 5. *Analyse structurée* visant à produire des conclusions vérifiables.

2.2 Outils et ressources mobilisés

Pour assurer la rigueur et la traçabilité de la recherche, plusieurs catégories d'outils ont été employées :

- **Navigateurs et extensions** : *Mozilla Firefox*, *Google Chrome*, complétés par des modules de capture et d'analyse d'en-têtes HTTP.
- **Moteurs de recherche** : *Google*, *DuckDuckGo*, avec utilisation de requêtes avancées (*Google Dorks*) pour un ciblage précis.
- **Plateformes OSINT spécialisées** : *Maltego*, *SpiderFoot*, *Hunter.io*, *Wayback Machine* pour la cartographie des liens numériques et l'historisation des pages.

- **Réseaux sociaux** : *Facebook*, *X (Twitter)*, *LinkedIn*, *Instagram*, explorés à partir d'indices de pseudonymes et de connexions académiques.
- **Analyse de métadonnées** : utilisation de *exiftool*, *strings* et *yt-dlp* pour extraire les données cachées des fichiers multimédias et publications en ligne.
- **Archivage et intégrité** : documentation par *captures d'écran*, exportations *PDF* et génération de *hachages SHA-256* garantissant la traçabilité des preuves.

2.3 Procédure de collecte et d'analyse

La démarche suivie s'est déroulée en quatre grandes phases :

1. **Recherche initiale** : identification des mots-clés pertinents (nom, pseudonymes, adresses mail, affiliations académiques) et repérage des premiers profils associés.
2. **Vérification et enrichissement** : confrontation des données issues de plusieurs plateformes afin de confirmer l'identité de la cible et d'enrichir son empreinte numérique.
3. **Analyse approfondie** : extraction de métadonnées, identification de la chronologie des publications et évaluation de la cohérence entre les différentes traces.
4. **Archivage et documentation** : conservation des résultats sous format horodaté, production de journaux de recherche et consignation des sources pour garantir la reproductibilité.

L'ensemble de la procédure a été mené de manière éthique et conforme aux principes de confidentialité, sans recours à des techniques intrusives ni à des interactions directes avec la cible.

Chapitre 3

Résultats obtenus

3.1 Inventaire des éléments trouvés

L'investigation menée autour de la cible **Olivia S.** a révélé une présence numérique relativement faible. Les recherches sur les moteurs classiques et les plateformes sociales n'ont permis de retrouver que des traces indirectes, suggérant un profil discret, peu exposé publiquement et probablement prudent dans sa gestion de l'identité numérique.

| N° | Type | Source (URL) | Date | Emplacement | Confiance |
|----|-------------------|--------------------------|------|-------------|-----------|
| 1 | Profil académique | (LinkedIn / ENSPY) | 2024 | Yaoundé | Élevée |
| 2 | Mention d'examen | (GCE Board 2022) | 2022 | Cameroun | Élevée |
| 3 | Référence ENSPY | (Liste d'admission 2022) | 2022 | ENSPY | Élevée |

3.2 Exemples d'extractions pertinentes

Malgré la rareté des traces personnelles directes, certaines informations contextuelles ont pu être confirmées :

- **Profil académique** : le nom apparaît sur des listes officielles liées au *GCE A 2022 (SBCBC)* et à l'*ENSPY 2022 (AHN)*, confirmant une trajectoire académique cohérente.
- **Affiliation actuelle** : la mention *ENSPY (2024/2025)* a été repérée dans des documents institutionnels, suggérant une poursuite d'études en cours.
- **Empreinte numérique** : absence de comptes sociaux associés aux pseudonymes habituels, ce qui traduit une stratégie de faible exposit

Chapitre 4

Comparaison entre hypothèses et résultats

4.1 Identité / Alias

Ce qu'on savait : La cible, identifiée sous le nom **Olivia S.**, aurait obtenu le *GCE Advanced Level* en 2022 (SBCBC) et intégré l'*École Nationale Supérieure Polytechnique de Yaoundé (ENSPY)* la même année, dans la filière AHN. Aucune information initiale ne faisait état d'un pseudonyme ou d'une activité notable sur les réseaux sociaux.

Ce que les preuves montrent : Les recherches OSINT confirment la présence du nom dans les bases académiques du *GCE Board* et sur les listes officielles d'admission de l'ENSPY. En revanche, aucune trace exploitable d'un alias ou d'un pseudonyme actif n'a été détectée sur les principales plateformes sociales (Facebook, Instagram, X, LinkedIn).

Conclusion : *Hypothèse confirmée partiellement.* L'identité réelle est validée par les sources institutionnelles, mais l'absence d'alias connus ou de comptes actifs empêche toute corrélation vers une présence numérique personnelle.

4.2 Localisation

Ce qu'on savait : Olivia S. serait résidente à Yaoundé, probablement à proximité du campus de l'ENSPY, sans certitude sur le lieu exact.

Résultat obtenu : Les informations disponibles (mentions institutionnelles, périodes académiques, connexions réseau ENSPY) suggèrent bien une localisation dans la ville de **Yaoundé**. Aucune métadonnée géographique (EXIF, IP, géotag) n'a été retrouvée dans les rares documents associés à la cible.

Niveau de confiance : **Élevé** pour la localisation générale (Yaoundé), **faible** pour toute précision plus fine (quartier, résidence).

4.3 Synthèse générale

- **Hypothèses confirmées :**
 - Obtention du GCE Advanced Level (SBCBC) en 2022.
 - Admission à l'ENSPY (AHN) en 2022.
 - Statut académique actif à l'ENSPY en 2024/2025.
- **Hypothèses infirmées :**
 - Existence d'un alias identifiable ou d'une forte présence sur les réseaux sociaux.
 - Traces multimédias comportant des métadonnées exploitables.
- **Points restant à vérifier :**
 - Usage éventuel de pseudonymes non corrélés à l'identité réelle.
 - Traces indirectes (commentaires, interactions tierces, bases de données secondaires).
 - Éventuelles présences sur des plateformes professionnelles à accès restreint.

En conclusion, les hypothèses de départ se trouvent globalement confirmées dans leur dimension académique, mais les données collectées soulignent la faible empreinte numérique de la cible. Cette discrétion volontaire ou maîtrisée constitue un élément marquant de son profil, révélant une gestion prudente de son identité en ligne.

Chapitre 5

Conclusion et recommandations

Conclusion

Ce travail d’investigation numérique a permis de mettre en évidence l’importance d’une démarche méthodique, éthique et documentée dans la recherche d’informations en sources ouvertes (OSINT). À travers une approche structurée — allant de la collecte passive à l’analyse corrélée — il a été possible d’établir une image cohérente, bien que limitée, de la présence numérique de la cible **Olivia S.**

Les résultats obtenus confirment l’identité et le parcours académique annoncés (GCE 2022, ENSPY 2022–2025), tout en révélant une empreinte numérique volontairement réduite. Cette discrétion témoigne d’une conscience des enjeux liés à la vie privée et de la maîtrise des traces laissées en ligne. Ainsi, ce cas illustre non seulement les limites techniques des investigations en l’absence de données publiques, mais aussi la nécessité d’une interprétation prudente des résultats — l’absence d’information pouvant elle-même constituer une information significative.

Recommandations

Afin d’améliorer la qualité, la fiabilité et l’éthique des investigations futures, plusieurs axes de progression peuvent être envisagés :

- **Renforcer la vérification croisée des sources** Multiplier les points de comparaison entre bases de données publiques, archives web et plateformes sociales pour améliorer la fiabilité des corrélations.
- **Automatiser l’archivage des preuves** Mettre en place des scripts ou outils d’automatisation (par exemple avec SpiderFoot ou theHarvester) permettant la sauvegarde systématique et horodatée des résultats.

- **Adopter une veille OSINT continue** Mettre à jour régulièrement les données collectées pour observer l'évolution éventuelle du profil numérique de la cible ou l'apparition de nouvelles traces en ligne.
- **Sensibiliser aux bonnes pratiques éthiques et légales** Veiller à respecter les cadres juridiques encadrant la collecte et l'utilisation des données publiques, tout en favorisant une culture de la confidentialité et de la responsabilité numérique.
- **Documenter rigoureusement les démarches** Conserver les journaux de recherche, empreintes cryptographiques et sources originales pour garantir la traçabilité et la reproductibilité des analyses.

En somme, cette investigation illustre la valeur ajoutée d'une approche OSINT disciplinée tout en soulignant ses limites face à des individus maîtrisant leur exposition numérique. La prudence, la transparence méthodologique et le respect de l'éthique demeurent les piliers essentiels d'une enquête numérique crédible et responsable.