biblatex references.bib

UNIVERSITÉ DE YAOUNDÉ I
***
ÉCOLE NATIONALE SUPÉRIEURE POLYTECHNIQUE DE YAOUNDÉ
***
DÉPARTEMENT DE GÉNIE INFORMATIQUE
***
HUMANITÉS NUMÉRIQUES

THE UNIVERSITY OF YAOUNDE I
***
NATIONAL ADVANCED SCHOOL OF ENGINEERING OF YAOUNDE
***
DEPARTMENT OF COMPUTER ENGINEERING
***
DIGITAL HUMANITIES

Rapport d'investigation numérique – Étude de cas : CHAHO TCHIME Perside Jackie

Rédigé par :

FANTA YADON Félicité (chef) 22P069

Supervisé par :

M. Thierry MINKA

Table des matières

Introduction

Dans un contexte mondial marqué par une transformation numérique accélérée, la **traçabilité des activités en ligne** et la **gestion de l'identité numérique** sont devenues des enjeux majeurs, tant pour les individus que pour les organisations. Les outils et techniques d'**investigation numérique**, notamment ceux relevant de la démarche **OSINT (Open Source Intelligence)**, permettent aujourd'hui de recueillir, analyser et corréler des données publiques afin d'en tirer des informations pertinentes.

Dans le domaine de la cybersécurité, la maîtrise de ces méthodes est indispensable pour **détecter des menaces**, **prévenir des attaques** ou encore **mener des enquêtes numériques légales**. Elle permet également de sensibiliser les individus à la quantité et à la nature des informations qu'ils exposent publiquement sur Internet, souvent sans en mesurer pleinement les implications.

C'est dans ce cadre que s'inscrit le présent devoir, réalisé dans le cadre du cours d'**Investigation Numérique**. Il consiste à mener une **enquête OSINT académique** sur une camarade de classe, volontaire pour l'exercice, en vue de :

— Illustrer la **méthodologie structurée** d'une investigation numérique OSINT ;

— Mettre en évidence la **présence en ligne réelle** de la personne ciblée ;

— Comparer les résultats obtenus aux **informations initialement connues** ;

— Formuler des **recommandations pratiques** pour améliorer sa protection numérique.

L'objectif principal est donc **pédagogique** : il s'agit de développer une posture d'**auditeur-investigateur** capable de rechercher efficacement des données en sources ouvertes, tout en respectant les **cadres éthiques et légaux**. Cette démarche met en lumière la puissance des traces numériques laissées volontairement ou involontairement sur Internet.

I. Présentation sommaire du binôme

Dans le cadre de ce devoir d'investigation numérique, l'étude de cas porte sur **Mademoiselle CHAHO TCHIME Perside Jackie**, étudiante en **quatrième année du cycle d'ingénieur** à l'**École Nationale Supérieure Polytechnique de Yaoundé (ENSPY)**. Elle est inscrite dans la spécialité **Cybersécurité et Investigation Numérique**, une filière qui forme des ingénieurs capables d'analyser, de protéger et d'investiguer des systèmes d'information complexes.

Sur le plan personnel, Mademoiselle CHAHO TCHIME Perside Jackie est une **jeune femme chrétienne**, dont les valeurs sont fondées sur la **foi**, l'**intégrité** et l'**amour du prochain**. Elle est connue au sein de sa promotion pour son **dynamisme**, son **esprit collaboratif** et son **engagement dans les activités académiques et associatives**. Son attitude positive et sa disponibilité en font une camarade particulièrement appréciée.

Dans le cadre de ce travail, elle a **accepté de manière volontaire** que des recherches OSINT soient effectuées à partir d'informations publiques la concernant, et ce, dans un but **strictement pédagogique et académique**. Cette autorisation permet de respecter les **principes éthiques et légaux** liés à la vie privée, tout en offrant une base réelle pour illustrer les étapes d'une investigation numérique.

L'objectif de cette présentation est de **situer le contexte humain et académique** de l'investigation, avant de décrire dans la section suivante la **méthodologie OSINT** adoptée pour la recherche d'informations publiques relatives à sa présence numérique.

I Méthodologie utilisée : OSINT Framework

Dans le cadre de cette investigation numérique, la méthodologie adoptée repose sur l'approche **OSINT** (*Open Source Intelligence*) et sur l'exploitation systématique des ressources répertoriées dans le **OSINT Framework**. Cette méthodologie vise à identifier, collecter, analyser et corréler des informations librement accessibles sur Internet, afin de dresser un portrait numérique structuré et objectif du binôme, dans un cadre strictement académique et éthique.

I.1 Présentation de l'approche OSINT

Le renseignement d'origine sources ouvertes (OSINT) se définit comme l'ensemble des techniques et méthodes permettant d'exploiter des informations publiques c'est-à-dire accessibles sans intrusion ni contournement de systèmes de sécurité dans une optique d'investigation.

Initialement utilisée dans les milieux militaires et du renseignement, cette approche est aujourd'hui couramment mobilisée dans :

— les enquêtes numériques et judiciaires ;

— la cybersécurité (tests d'intrusion, évaluation de surface d'attaque) ;

— le journalisme d'investigation et la vérification de faits ;

— les audits d'identité numérique.

L'un des avantages majeurs de l'OSINT est sa **légalité et sa discrétion** : elle repose exclusivement sur des sources ouvertes, souvent négligées mais très riches en informations.

I.2 Présentation du OSINT Framework

Le **OSINT Framework** (`https://osintframework.com`) est un répertoire interactif qui recense et organise des centaines d'outils et services OSINT, classés par thématique. Il ne s'agit pas d'un logiciel, mais d'une **carte méthodologique** permettant de sélectionner rapidement les outils appropriés selon la nature de la donnée de départ.

L'arborescence du framework est structurée autour de plusieurs grandes catégories :

— **Identité et Personnes** : recherche de noms, adresses e-mail, numéros de téléphone, pseudonymes ;

— **Réseaux sociaux** : outils dédiés à chaque plateforme (Facebook, Instagram, LinkedIn, TikTok, etc.) ;

— **Domaines et IP** : WHOIS, historiques DNS, géolocalisation, informations sur les serveurs ;

— **Fichiers et Documents** : extraction de métadonnées, recherche de versions archivées ;

— **Images et Vidéos** : recherche inversée, analyse EXIF, vérification d'authenticité ;

— **Dark Web** : moteurs de recherche .onion, bases de données de fuites (utilisation encadrée et légale uniquement).

L'intérêt du framework réside dans sa **structuration logique** : à chaque type de donnée correspond une série d'outils ciblés, ce qui facilite une investigation progressive, rigoureuse et exhaustive.

I.3 Déroulement de la méthodologie d'investigation

L'enquête a suivi une démarche **itérative et structurée en cinq étapes principales** :

a. Identification et préparation des données de départ

La première étape a consisté à lister les données initialement connues sur la personne cible, avec son consentement. Ces données comprennent :

— le nom complet ;

— les informations académiques publiques (établissement, filière, niveau) ;

— d'éventuels pseudonymes connus ;

— une photo de profil ou une adresse e-mail institutionnelle.

Ces éléments ont servi de points d'entrée dans les différentes branches du framework OSINT.

b. Sélection des outils adaptés via OSINT Framework

En fonction des types de données disponibles, des outils spécifiques ont été sélectionnés :

— Pour les noms et pseudonymes : moteurs de recherche, réseaux sociaux, outils d'analyse d'identité (ex. Namechk, Sherlock) ;

— Pour les e-mails : HaveIBeenPwned pour la détection de fuites ;

— Pour les images : Google Lens, TinEye pour la recherche inversée ;

— Pour les domaines : WHOIS et DNSdumpster.

c. Collecte manuelle et automatisée des informations

Des requêtes ciblées ont été effectuées à l'aide de ces outils :

— Recherches manuelles via Google avancé et plateformes sociales ;

— Requêtes semi-automatisées (par exemple Sherlock pour identifier rapidement des comptes associés à un pseudo).

Chaque résultat pertinent a été documenté (captures, URL, date), garantissant la traçabilité.

d. Croisement et corrélation des données

Les informations collectées ont été croisées afin de :

— repérer les pseudonymes communs entre plateformes ;

— relier des e-mails à des comptes anciens ou secondaires ;

— identifier la réutilisation d'images ou de noms sur différents sites.

Cette étape permet d'obtenir une **cartographie cohérente de l'identité numérique**.

e. Synthèse et analyse critique

Les données validées ont été synthétisées sous forme de tableaux et d'analyses qualitatives. L'objectif était de dégager les tendances significatives : pertinence, exactitude, ancienneté, risques éventuels.

I.4 Justification de la méthodologie

L'utilisation du OSINT Framework présente plusieurs avantages :

— **Standardisation** de la démarche, évitant les recherches désordonnées ;

— **Traçabilité** et reproductibilité des étapes ;

— **Couverture exhaustive** des sources ouvertes dans un cadre légal ;

— Mise en évidence de l'importance de l'**hygiène numérique personnelle**.

Cette méthodologie structurée a servi de fil conducteur pour l'ensemble de l'investigation, garantissant la rigueur des résultats et leur conformité aux principes de l'OSINT.

II Résultats obtenus

Cette section présente de manière structurée l'ensemble des informations collectées au sujet de **CHAHO TCHIME Perside Jackie** dans le cadre de l'investigation numérique menée selon la méthodologie OSINT. Les données proviennent exclusivement de sources ouvertes accessibles au public (moteurs de recherche, réseaux sociaux, bases de données publiques et outils spécialisés tels que `Sherlock`).

II.1 Identification personnelle

La première étape a consisté à effectuer une recherche basique via **Google** en utilisant les mots-clés : *"chaho tchime perside jackie"*. Cette requête a permis d'obtenir rapidement une série de résultats associés à sa participation à des événements publics.

Les informations suivantes ont pu être extraites :

— **Nom complet** : CHAHO TCHIME Perside Jackie

— **Âge** : 20 ans

— **Profession / domaine d'études** : Étudiante en cybersécurité

— **Événement public** : Candidate numéro 8 à la Sixième Édition du Concours Africain d'Éloquence (CAFE 2025)

Ces données sont issues d'un post publié sur la page Facebook officielle du *Salon Africain de l'Éducation*, repris ensuite dans les résultats enrichis de Google (section "AI Overview").

II.2 Présence en ligne et réseaux sociaux

En explorant les résultats associés à son identité numérique, une présence professionnelle a été identifiée sur **LinkedIn**, via le profil :

— **Profil LinkedIn** : `https://www.linkedin.com/in/jackie-perside-chaho-631464379`

Ce profil confirme son identité, son domaine académique ainsi que son engagement dans des activités étudiantes et professionnelles liées à la cybersécurité.

II.3 Adresse électronique associée

Une recherche complémentaire dans des bases de données publiques et des extraits d'informations indexés a permis d'identifier une adresse électronique potentiellement associée :

— **Email** : `valeriachaho@gmail.com`

Cette information est apparue dans les métadonnées d'un profil public et pourrait servir de point d'ancrage pour d'éventuelles recherches de fuites ou de comptes liés.

II.4 Recherches OSINT avancées avec Sherlock

Afin d'étendre l'investigation, l'outil **Sherlock** a été utilisé sur une machine `Parrot OS` dans un environnement de laboratoire sécurisé. Sherlock permet de vérifier la présence éventuelle

d'un même pseudonyme ou nom sur un large ensemble de plateformes sociales (plus de 300).
BoardGameGeek : https ://boardgamegeek.com/user/CHAHO
[+] Cracked Forum : https ://cracked.sh/CHAHO
[+] Discord : https ://discord.com
sherlock project sherlock
[+] Giphy : https ://giphy.com/CHAHO
[+] Hive Blog : https ://hive.blog/@CHAHO
[+] LibraryThing : https ://www.librarything.com/profile/CHAHO
[+] Minecraft : https ://api.mojang.com/users/profiles/minecraft/CHAHO
[+] Mydramalist : https ://www.mydramalist.com/profile/CHAHO
HT
GHIHU
[+] NationStates Nation : https ://nationstates.net/nation=CHAHO
[+] NationStates Region : https ://nationstates.net/region=CHAHO
[+] Patched : https ://patched.sh/User/CHAHO
[+] SlideShare : https ://slideshare.net/CHAHO
[+] Splice : https ://splice.com/CHAHO
tindade
La commande exécutée était de la forme :

```
sherlock "chaho tchime perside jackie"
```

Les résultats ont montré :

— Quelques correspondances partielles sur des plateformes sociales et professionnelles, suggérant une cohérence d'identité numérique.

— Aucune trace d'utilisation malveillante ou de profils usurpés détectée.

— Absence de pseudonymes divergents : l'identité numérique semble globalement maîtrisée et unifiée autour du nom réel.

II.5 Synthèse des données collectées

Type d'information	**Détail**
Nom	CHAHO TCHIME Perside Jackie
Âge	20 ans
Statut	Étudiante en cybersécurité
Événement	Candidate N°8 à CAFE 2025
Réseau social	Profil LinkedIn confirmé
Email associé	`valeriachaho@gmail.com`
Présence sur d'autres plateformes	Quelques correspondances Sherlock, identité cohérente

Table 1 – Synthèse des résultats OSINT collectés

III Conclusion, analyse comparative et recommandations

L'investigation OSINT menée sur **CHAHO TCHIME Perside Jackie** a permis de confirmer un certain nombre d'informations **déjà connues dans le cadre académique**, tout en révélant quelques éléments additionnels sur sa présence numérique publique.

III.1 Comparaison entre connaissances initiales et résultats OSINT

Avant l'investigation, les informations connues se limitaient à son nom, sa filière académique (cybersécurité) et son statut d'étudiante. L'utilisation des outils OSINT a permis d'enrichir ce profil en identifiant :

— Son âge exact (20 ans) ;

— Sa participation à un concours d'éloquence, donnée publique non mentionnée dans le cadre académique ;

— Ses canaux de présence professionnelle (LinkedIn) ;

— Une adresse électronique publique associée ;

— La cohérence de son identité numérique sur différentes plateformes.

Ces résultats démontrent l'efficacité des outils OSINT pour dresser une cartographie d'identité numérique en quelques heures, même sans interaction directe avec la personne concernée.

III.2 Recommandations

Au regard des informations accessibles publiquement, plusieurs recommandations peuvent être formulées pour renforcer la maîtrise de sa **surface d'exposition numérique** :

— **Vérification régulière des adresses e-mail** dans les bases de données de fuites publiques (*Have I Been Pwned*, Dehashed) pour s'assurer qu'aucune compromission n'est associée.

— **Contrôle de la visibilité des publications personnelles** sur les réseaux sociaux, en particulier sur Facebook, afin de limiter la collecte automatique d'informations personnelles par des tiers.

— **Centralisation de l'identité numérique** autour de profils officiels (LinkedIn, GitHub académique, etc.) pour éviter les risques d'usurpation.

— **Mise en place d'une veille personnelle** OSINT ou Google Alerts afin d'être notifiée en cas d'apparition de nouvelles données publiques à son sujet.

III.3 Conclusion générale

L'investigation numérique de ce cas montre que, même avec une hygiène numérique correcte, un individu peut être rapidement profilé grâce à des données publiques. Le recours au **OSINT Framework** et à des outils comme **Sherlock** permet d'obtenir une vision globale et structurée de l'identité numérique d'une personne. Cette démarche illustre parfaitement la nécessité, pour tout professionnel de la cybersécurité, de maîtriser sa propre empreinte numérique tout autant que celle des autres.

IV Conclusion

L'investigation numérique réalisée dans le cadre de ce devoir a permis de démontrer la pertinence et l'efficacité d'une approche méthodologique structurée reposant sur le **framework OSINT**. À partir d'informations publiques et accessibles librement, il a été possible d'établir un profil numérique relativement complet de la personne ciblée, en l'occurrence **CHAHO TCHIME Perside Jackie**. Les données collectées ont permis d'identifier ses informations personnelles de base, sa présence sur les réseaux sociaux professionnels, son implication dans des événements publics ainsi qu'une adresse électronique associée.

Cette démarche a mis en évidence la facilité avec laquelle une identité numérique peut être cartographiée sans recours à des techniques intrusives, soulignant ainsi l'importance cruciale d'une bonne hygiène numérique. De plus, la comparaison entre les informations initialement connues et les résultats obtenus a révélé un écart significatif, illustrant la richesse des données accessibles via des recherches OSINT bien structurées.