
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

| | | |
|-------------|------------------------------------------------------------------------|-----------|
| I | Méthodologie utilisée : OSINT Framework | 4 |
| I.1 | Présentation de l'approche OSINT | 4 |
| I.2 | Présentation du OSINT Framework | 5 |
| I.3 | Déroulement de la méthodologie d'investigation | 5 |
| I.4 | Justification de la méthodologie | 6 |
| II | Résultats obtenus | 7 |
| II.1 | Identification personnelle | 7 |
| II.2 | Présence en ligne et réseaux sociaux | 7 |
| III | Analyse du profil LinkedIn | 7 |
| III.1 | Informations de base | 7 |
| III.2 | Formation et compétences | 8 |
| III.3 | Visibilité et réseau | 8 |
| III.4 | Indicateurs OSINT exploitables | 8 |
| III.5 | Évaluation des risques numériques | 8 |
| IV | Analyse du profil Facebook | 10 |
| V | Analyse du profil Facebook | 10 |
| V.1 | Informations de base | 10 |
| V.2 | Présence et activité | 11 |
| V.3 | Réseau et interactions | 11 |
| V.4 | Indicateurs OSINT exploitables | 11 |
| V.5 | Évaluation des risques numériques | 11 |
| VI | Analyse du profil TikTok | 11 |
| VI.1 | Informations de base | 12 |
| VI.2 | Contenu et activité | 12 |
| VI.3 | Réseau et visibilité | 13 |
| VI.4 | Indicateurs OSINT exploitables | 13 |
| VI.5 | Évaluation des risques numériques | 13 |
| VII | Collecte d'informations avec Sherlock | 15 |
| VII.1 | Analyse d'un document académique partagé en ligne | 16 |
| VII.2 | Synthèse des données collectées | 17 |
| VIII | Conclusion, analyse comparative et recommandations | 18 |
| VIII.1 | Comparaison entre connaissances initiales et résultats OSINT | 18 |
| VIII.2 | Recommandations | 18 |
| VIII.3 | Conclusion générale | 18 |

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**, **Facebook**, via les profil :

III Analyse du profil LinkedIn

L'analyse du profil LinkedIn de la cible a été effectuée dans le cadre de la méthodologie OSINT en s'appuyant uniquement sur les informations accessibles publiquement. L'objectif est de produire une synthèse de son empreinte numérique professionnelle et d'évaluer les implications potentielles pour sa visibilité et sa gestion de l'identité numérique.

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

III.1 Informations de base

Le profil LinkedIn présente le nom complet « Jackie Perside Chaho » et indique le statut étudiant en cybersécurité à l'École Nationale Supérieure Polytechnique de Yaoundé, ce qui permet de confirmer l'appartenance à un cursus académique spécifique. :contentReference[oaicite :3]index=3 La différence entre l'intitulé académique et les expériences professionnelles est un facteur à noter : étant encore en formation, l'activité professionnelle semble limitée ou orientée vers des stages.

III.2 Formation et compétences

Le profil mentionne la filière cybersécurité, ce qui oriente l'évaluation vers des compétences techniques et un positionnement professionnel clair. Le fait d'indiquer cette spécialisation augmente la cohérence du profil : il devient alors plus facilement identifiable par des recruteurs ou des pairs dans le domaine de la sécurité informatique.

III.3 Visibilité et réseau

Le nombre de connexions, les recommandations ou les interactions visibles (publications, likes, commentaires) ne sont pas toujours totalement publiques. Cependant, la présence d'un profil LinkedIn actif dans un domaine technologique constitue un avantage de visibilité professionnelle. Le réseau connecté (université, camarades, formateurs) peut être exploité pour repérer des collaborations, des événements ou des publications partagées.

III.4 Indicateurs OSINT exploitables

Plusieurs éléments se dégagent comme pertinents pour une investigation numérique :

- Le nom exact et la spécialisation académique constituent des ****points d'entrée**** pour rechercher des publications, des participations à des conférences ou des projets.
- Le lien entre la formation et d'éventuels comptes ou projets GitHub/bitbucket peut être vérifié en recoupant le nom et la filière.
- Le profil LinkedIn, du fait de sa nature professionnelle, peut fournir des données contextuelles (ville, secteur, stage) utiles à une cartographie plus large.



III.5 Évaluation des risques numériques

Même si les informations professionnelles paraissent anodines, elles persistent dans le temps et peuvent être utilisées pour un profilage ou une ingénierie sociale. Par exemple, l'association de son nom, de son université et de sa spécialisation crée une ****empreinte numérique consolidée****. Il est donc recommandé de :

- Vérifier les réglages de visibilité (qui peut voir les connexions, les activités) afin de limiter la sur-exposition.
- Nettoyer ou archiver les anciennes publications ou projets qui ne reflètent plus sa position actuelle.
- Séparer, si souhaité, des comptes strictement professionnels des comptes sociaux personnels afin de limiter les croisements non souhaités.

22:32 📶 LTE 78+

← Jackie Perside Chaho




Jackie Perside Chaho · 1st

Étudiante en cybersécurité | Intérêt marqué pour la GRC et le pentesting | En quête de stages et d'opportunités de montée en compétences


Ecole Nationale Supérieure Polytechnique de Yaoundé
Yaoundé, Centre, Cameroon

500+ connections

 Merveille Noupoue Silatchou, Gildas roussel Kuekam lamene, and 186 other mutual connections

[Message](#)

Highlights


 **1 mutual group**
You and Jackie Perside are both in CYBER SECURITY FORUM INITIATIVE - CSFI


About

Actuellement étudiante en cybersécurité à l'École Nationale Supérieure Polytechnique de Yaoundé, je développe des compétences solides en sécurité des systèmes d'information, avec un intérêt marqué pour :... see more

Activity

1,253 followers

Jackie Perside Chaho commented on a post · 2w
 Samuel Rostand KWEM PEK

Jackie Perside Chaho commented on a post · 3w


Jackie Perside Chaho commented on a post · 2mo
Post pertinent, merci BALEBA

Figure 1 – Profil professionnel

IV Analyse du profil Facebook



Figure 2 – Profil réseaux sociaux

V Analyse du profil Facebook

L'analyse du profil Facebook de la cible a été réalisée dans le respect de la méthodologie OSINT, en se limitant strictement aux informations rendues publiques par l'intéressée. L'objectif était d'identifier les éléments d'identité numérique visibles, ainsi que les indices exploitables dans le cadre d'une investigation numérique.

V.1 Informations de base

Le profil Facebook présente plusieurs éléments d'identification classiques, tels que la photo de profil, la photo de couverture, ainsi que le nom complet utilisé. Ces informations permettent de confirmer l'identité de la cible et d'assurer la correspondance avec d'autres traces numériques collectées sur d'autres plateformes.

V.2 Présence et activité

L'activité publique observée inclut la publication de contenus textuels, d'images, de partages, ainsi que des interactions visibles (likes, commentaires). Cette activité fournit des indications sur la fréquence d'utilisation du compte, les heures de connexion dominantes, ainsi que les thématiques privilégiées dans les publications.

V.3 Réseau et interactions

La liste publique des amis et/ou les interactions visibles permettent de dresser une première cartographie du réseau social de la cible. Ce réseau peut révéler des cercles relationnels (famille, camarades de classe, collègues, membres d'associations, etc.) ainsi que des communautés d'intérêt. L'observation des commentaires et mentions permet aussi d'identifier les interlocuteurs récurrents.

V.4 Indicateurs OSINT exploitables

Plusieurs indices typiquement exploitables dans le cadre d'une investigation ont été relevés :

- Utilisation d'un nom réel ou facilement corrélable à d'autres comptes ;
- Publications ou photos contenant des données contextuelles (géolocalisation, environnement reconnaissable) ;
- Informations biographiques ou professionnelles visibles dans la section « À propos » ;
- Participation à des groupes ou événements publics.

V.5 Évaluation des risques numériques

L'ensemble de ces éléments, bien que publics, peut être utilisé à des fins de corrélation ou de profilage. Une exposition non maîtrisée de données personnelles (photos, opinions, géolocalisation, etc.) accroît la surface d'attaque potentielle dans le cadre d'une ingénierie sociale ou d'usurpation d'identité.

En conséquence, il est recommandé à la cible de :

- Revoir les paramètres de confidentialité de ses publications ;
- Limiter la quantité d'informations biographiques affichées publiquement ;
- Nettoyer régulièrement les anciennes publications pouvant contenir des données sensibles ;
- Éviter la géolocalisation en temps réel dans les publications publiques.

VI Analyse du profil TikTok

L'analyse du profil TikTok de la cible a été effectuée dans le cadre de la méthodologie OSINT, en s'appuyant uniquement sur les informations accessibles publiquement. L'objectif est de produire une synthèse de son empreinte numérique dans l'environnement des courtes vidéos et d'évaluer les implications en matière de visibilité et d'identité numérique.

VI.1 Informations de base

Le lien observé est : <https://vm.tiktok.com/ZMHv2FYVANULR-V0ruG/>. Le profil semble utiliser le pseudonyme « [Insérer pseudonyme exact] » ou bien est directement associé à son nom complet « CHAHO TCHIME Perside Jackie ». L'avatar, la biographie (s'il est public) et les premières vidéos visibles indiquent que le compte est actif et suppose une certaine volonté de partage de contenu à destination large.

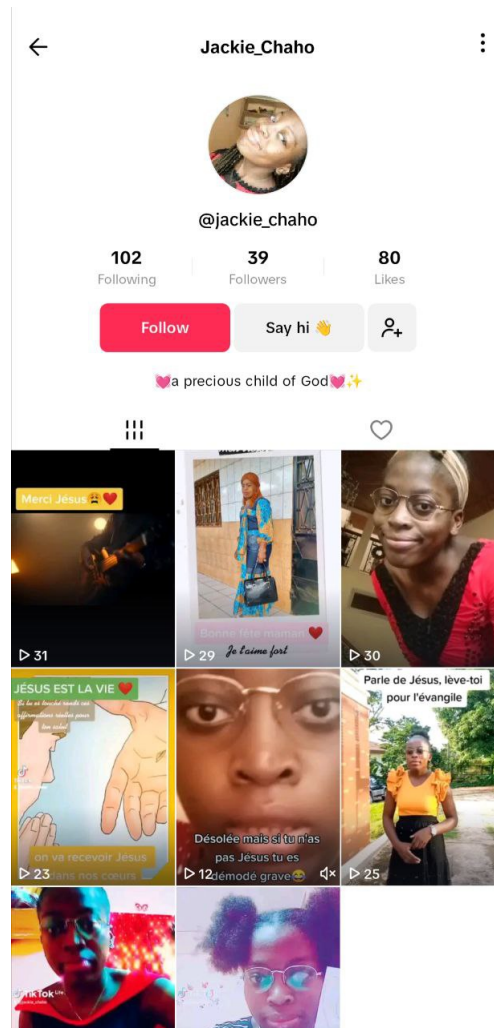


Figure 3 – Tiktok

VI.2 Contenu et activité

Les premières observations montrent que le compte publie des vidéos [décrire : thème(s), fréquence, type de contenu — ex. danse, humoristique, éducatif, personnel]. La visibilité publique des vidéos, des likes et des commentaires permet de déterminer une certaine **activité d'audience**. Le style des vidéos, la nature des interactions (commentaires publics, partages) et la cohérence des thèmes utilisés constituent des indicateurs d'engagement potentiel.

VI.3 Réseau et visibilité

Même si TikTok limite l'accès à certains paramètres (followers, vues, statistiques détaillées) à moins de passer en compte Pro/Créateur, on peut tout de même observer :

- Le nombre approximatif de vues ou de likes visibles sur les vidéos.
- Les commentaires publics — qui permettent d'identifier d'éventuels interlocuteurs, cercles relationnels ou communautés d'intérêt.
- Le style visuel et les hashtags utilisés — ce qui peut indiquer les audiences ciblées.

VI.4 Indicateurs OSINT exploitables

Plusieurs éléments se dégagent comme exploitables dans le cadre d'une investigation numérique :

- L'association du pseudonyme ou nom complet à un réseau vidéo court, ce qui renforce l'empreinte numérique de la cible.
- Le type de contenu (personnel vs public) : contenu trop public peut accroître l'exposition.
- La répétition thématique ou visuelle : des habillages visuels identiques à ceux d'autres plateformes permettent de croiser avec d'autres comptes (ex. Instagram, YouTube).
- Le style et la fréquence : un compte actif avec de nombreux partages publics multiplie les traces exploitables.

VI.5 Évaluation des risques numériques

Même si le compte semble rester dans une logique personnelle et non professionnelle, quelques aspects méritent attention :

- Une forte visibilité publique (nombre élevé de vues/likes) ou des contenus personnels (géolocalisation, entourage, lieu) peuvent augmenter la surface d'attaque (ex. ingénierie sociale).
- L'absence de cloisonnement entre vie privée et publique – si le même pseudonyme est utilisé sur d'autres plateformes – renforce la corrélation inter-plateformes.
- Le manque de confidentialité ou la non-utilisation de paramètres de visibilité stricts (public au lieu de privé) peut rendre l'identification ou le recoupement d'informations plus facile.

En conséquence, il est recommandé à la cible de :

- Vérifier les paramètres de confidentialité de son compte TikTok — limiter l'accès aux vidéos à ses followers ou restreindre les commentaires/publications visibles.
- Éviter de publier des données de localisation, ou des vidéos dans des lieux identifiables de façon publique.
- Différencier clairement ses pseudonymes / comptes (loisir vs vie académique/professionnelle) afin de limiter la consolidation de son identité numérique.
- Surveiller régulièrement les vidéos publiées et les commentaires pour détecter d'éventuels reposts ou usages non autorisés.

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`



Jackie Perside's profile

<https://www.linkedin.com/in/jackie-perside-chaho-631464379>



Email

valeriachaho@gmail.com

Figure 4 – email

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.

VII Collecte d'informations avec Sherlock

Afin d'étendre l'investigation et de vérifier la cohérence de l'identité numérique de la cible sur plusieurs plateformes sociales, l'outil **Sherlock** a été utilisé dans un environnement de laboratoire sécurisé, sur une machine Parrot OS. **Sherlock** est un outil OSINT open source permettant de rechercher automatiquement la présence d'un pseudonyme ou d'un nom sur plus de **300 plateformes sociales, professionnelles et communautaires**. Il compare le nom fourni à une base d'URL prédéfinies et identifie les comptes potentiellement associés.

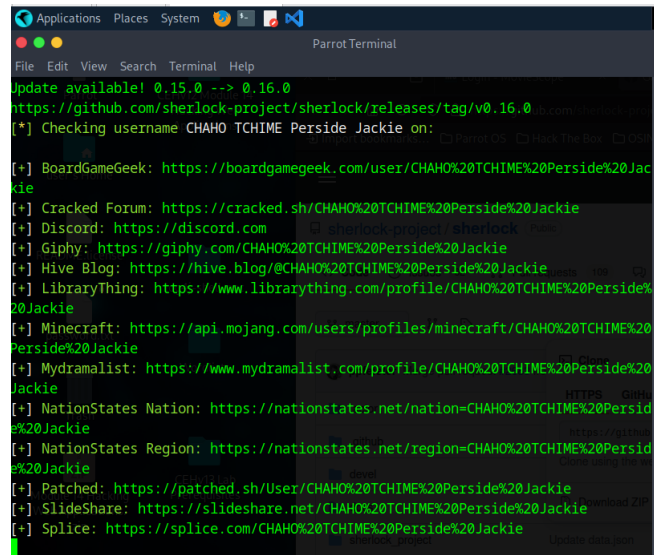


Figure 5 – Exécution de Sherlock dans l'environnement Parrot OS

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

Cette recherche visait à identifier toute occurrence publique du nom complet de la cible sur différentes plateformes. L'objectif était de :

- Repérer d'éventuels comptes actifs ou abandonnés portant le même nom ;
- Détecter des profils usurpés ou des pseudonymes divergents ;
- Cartographier la cohérence de l'identité numérique sur l'ensemble des réseaux. L'exécution de Sherlock a produit plusieurs correspondances potentielles sur différentes plateformes communautaires et de partage de contenu. Parmi les plateformes où des occurrences partielles ou complètes ont été détectées, on retrouve notamment :

- **BoardGameGeek** : <https://boardgamegeek.com/user/CHAH0%20TCHIME%20Perside%20Jackie>
- **Cracked Forum** : <https://cracked.sh/CHAH0%20TCHIME%20Perside%20Jackie>
- **Giphy** : <https://giphy.com/CHAH0%20TCHIME%20Perside%20Jackie>
- **Hive Blog** : <https://hive.blog/@CHAH0%20TCHIME%20Perside%20Jackie>
- **LibraryThing** : <https://www.librarything.com/profile/CHAH0%20TCHIME%20Perside%20Jackie>
- **Minecraft API** : <https://api.mojang.com/users/profiles/minecraft/CHAH0%20TCHIME%20Perside%20Jackie>

- **Mydramalist** : <https://www.mydramalist.com/profile/CHAH0%20TCHIME%20Perside%20Jackie>

VII.1 Analyse d'un document académique partagé en ligne

Au cours de l'investigation, un document au format PDF, hébergé sur une plateforme publique de partage en ligne, a été retrouvé. Il s'agit d'une **fiche d'inscription académique officielle** émanant de l'**École Nationale Supérieure Polytechnique de l'Université de Yaoundé I**, relative à l'année académique 2024–2025.

Le document présente plusieurs informations personnelles sensibles de l'individu investigué, notamment :

- **Nom et prénoms complets** : CHAHO TCHIME Perside Jackie
- **Matricule** : 22P094
- **Date et lieu de naissance** : 11 octobre 2005 à Mbouda
- **Classe** : ING-3 CIN
- **Liste détaillée des unités d'enseignement** suivies durant l'année académique (codes, intitulés et crédits)
- **Date de signature** du document : 31 décembre 2024

La présence publique de ce document sur une plateforme accessible sans authentification soulève plusieurs points importants :

1. **Exposition d'informations personnelles et académiques** : matricule, date de naissance et parcours académique peuvent être exploités à des fins de *phishing ciblé*, d'ingénierie sociale ou d'usurpation d'identité.
2. **Indice d'authenticité et de fiabilité de l'identité** : ce type de document officiel renforce la vérification de l'identité numérique de la personne investiguée, en la liant à une institution universitaire identifiable.
3. **Traçabilité temporelle** : la date de signature permet de situer la chronologie de la présence en ligne de l'individu (fin 2024), ce qui peut être utile dans une analyse OSINT longitudinale.

Sur le plan méthodologique, ce type de découverte illustre la pertinence d'explorer non seulement les réseaux sociaux classiques, mais aussi les **plateformes de partage de documents publics** telles que Scribd, Academia.edu, SlideShare ou Google Docs. Il s'agit souvent de sources riches en données, parfois involontairement exposées.

Un autre document au format PDF, publié sur un site institutionnel, a été mis en évidence au cours de l'investigation. Il s'agit du communiqué d'admission en première année dans les filières « Arts Numériques Humanités Numériques » de l'École Nationale Supérieure Polytechnique de Yaoundé (ENSPY) pour l'année académique 2022/2023. :contentReference[oaicite:1]index=1

Le document recense plusieurs éléments d'intérêt pour l'analyse OSINT :

- Il contient une liste nominative de candidats admis et en liste d'attente, ce qui inclut le nom exact « CHAHO TCHIME Perside Jackie ».

- Il confirme le cycle, la filière et l'année d'admission (filières « Arts Numériques » et « Humanités Numériques », première année) ce qui permet de situer la personne dans son parcours académique.
- Il s'agit d'un document officiel, ce qui en renforce la fiabilité (publication par le ministère ou l'institution).

Implications pour l'investigation numérique La découverte de ce document présente plusieurs implications notables :

1. **Confirmation de l'identité académique** : L'apparition du nom complet dans un document officiel renforce la correspondance entre l'identité déclarée et la personne investiguée.
2. **Exposition publique** : Le document étant librement accessible, il offre des informations précises (nom, filière, cycle) qui peuvent être exploitées pour des recoupements d'identité, ce qui augmente la surface d'exposition numérique.
3. **Traçabilité éducative** : Le document permet de dater l'admission (2022/2023) et le cycle, ce qui peut servir de repère temporel dans la cartographie de l'empreinte numérique.

Recommandations spécifiques En guise de recommandations liées à cette découverte :

- Vérifier la visibilité de ce type de document : bien que partie d'un processus légal et institutionnel, l'individu pourrait envisager de limiter l'accès ou de contrôler la diffusion excessive (par exemple via moteurs de recherche) si souhaité.
- Surveiller les usages du nom dans ce contexte : étant donné que l'admission est publique, l'utilisation du nom complet dans d'autres contextes (forums, réseaux, pseudonymes) peut amplifier l'empreinte numérique.
- Consolider l'identité numérique : veiller à ce que les comptes académiques, personnels et professionnels soient bien différenciés, afin de limiter les croisements involontaires entre données privées et données académiques.

VII.2 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 |
| Réseaux sociaux | Profils LinkedIn, FaceBook, Instagram Tiktok confirmés |
| Email associé | valeriachaho@gmail.com |
| Présence sur d'autres plateformes | Quelques correspondances Sherlock, identité cohérente |

Table 1 – Synthèse des résultats OSINT collectés

VIII 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.

VIII.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.

VIII.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.

VIII.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.

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.

Références

- [1] Justin Nordine. *OSINT Framework*. Disponible sur : <https://osintframework.com> [Consulté le 18 octobre 2025].
- [2] Sherlock Project. *Sherlock : Hunt down social media accounts by username across social networks*. GitHub, 2025. Disponible sur : <https://github.com/sherlock-project/sherlock> [Consulté le 18 octobre 2025].
- [3] Meta Platforms Inc. *Facebook*. Disponible sur : <https://www.facebook.com> [Consulté le 18 octobre 2025].
- [4] LinkedIn Corporation. *LinkedIn*. Disponible sur : <https://www.linkedin.com> [Consulté le 18 octobre 2025].
- [5] INTERPOL. *African Cyberthreat Assessment Report*. INTERPOL, 2024. Disponible sur : <https://www.interpol.int> [Consulté le 18 octobre 2025].
- [6] Bazzell, Michael. *Open Source Intelligence Techniques : Resources for Searching and Analyzing Online Information*. 10^e édition, 2024.
- [7] EC-Council. *Certified Ethical Hacker (CEH) v13 Official Courseware*. EC-Council, 2023.
- [8] Phil Harvey. *ExifTool by Phil Harvey*. Disponible sur : <https://exiftool.org> [Consulté le 18 octobre 2025].
- [9] ICANN. *WHOIS Lookup Service*. Disponible sur : <https://lookup.icann.org> [Consulté le 18 octobre 2025].
- [10] Google Inc. *Google Images – Recherche inversée*. Disponible sur : <https://images.google.com> [Consulté le 18 octobre 2025].
- [11] École Nationale Supérieure Polytechnique de Yaoundé. *Fiche d'inscription académique de CHAHO TCHIME Perside Jackie*. Disponible sur : <https://share.google/7QF61Rtes8EWE1LL0> [Consulté le 18 octobre 2025].
- [12] École Nationale Supérieure Polytechnique de Yaoundé. *Résultats d'admission en 1^{ère} année - Arts Numériques et Humanités Numériques*. Disponible sur : https://polytechnique.cm/wp-content/uploads/2022/08/Resultat-ENSPY-2022_1ere-annee-Arts-Num-et-Humanites-Num.pdf [Consulté le 18 octobre 2025].