RÉPUBLIQUE DU CAMEROUN
****
Paix - Travail - Patrie
****
UNIVERSITÉ DE YAOUNDÉ I
****
ECOLE NATIONALE SUPERIEURE POLYTECHNIQUE DE YAOUNDE
****
DÉPARTEMENT DE GENIE INFORMATIQUE
****

REPUBLIC OF CAMEROON
****
Peace - Work - Fatherland
****
UNIVERSITY OF YAOUNDE I
****
NATIONAL ADVANCED SCHOOL OF ENGINEERING OF YAOUNDE
****
DEPARTMENT OF COMPUTER ENGINEERING
****

RAPPORT D'INVESTIGATION
SUR WANSI GILLES GILDAS

Option :

Cybersécurité et Investigation Numérique

Rédigé par :

KALDADAK ADAMA, *24P824*

Sous l'encadrement de :
M. Minka THierry

Année académique 2025 / 2026

TABLE DES MATIÈRES

INTRODUCTION

Le présent travail s'inscrit dans une démarche à la fois pédagogique et pratique, visant à mettre en application les principes fondamentaux de l'investigation numérique. Il consiste à mener une enquête en ligne centrée sur l'identité d'une personne, en exploitant uniquement les informations accessibles publiquement sur Internet et les réseaux sociaux. L'objectif est de démontrer comment les traces numériques laissées volontairement ou involontairement peuvent être analysées pour reconstituer un profil cohérent et significatif. Cette démarche repose sur une approche rigoureuse, méthodique et éthique, respectant les règles de la protection des données personnelles et les limites légales de la recherche en sources ouvertes (OSINT). Elle mobilise différentes techniques d'analyse numérique, telles que la recherche avancée, la vérification des métadonnées, l'étude des profils sociaux, ainsi que le recoupement d'informations issues de plusieurs plateformes. Au-delà de la simple collecte de données, ce travail met en évidence la dimension critique de l'investigation numérique : il s'agit non seulement de trouver des informations, mais aussi d'en évaluer la fiabilité, la pertinence et le contexte de publication. Cette analyse permet de comprendre comment une identité numérique se construit, se renforce ou se fragilise au fil des activités en ligne. Ainsi, cette étude illustre concrètement l'importance de la vigilance numérique et de la cyberresponsabilité dans un monde où chaque action sur Internet laisse une empreinte durable. Elle montre comment les données éparses publiées sur le web peuvent être collectées, croisées et interprétées pour dresser un portrait numérique complet, révélant à la fois les opportunités offertes par la visibilité en ligne et les risques potentiels liés à la surexposition, à la désinformation ou à l'usurpation d'identité dans notre société hyperconnectée.

I Contexte : Investigation numérique

À l'ère du numérique, l'identité d'une personne ne se limite plus à ses informations administratives ou à son apparence physique : elle s'étend désormais à son **empreinte numérique**, c'est-à-dire **l'ensemble des traces qu'elle laisse sur Internet, Réseaux sociaux, plateformes professionnelles, blogs, commentaires, photos, ou encore métadonnées**. C'est dans cette même logique que **Heidegger** s'aligne :**l'être humain ne se définit plus seulement par sa présence physique mais également par son existence numérique**.

Chaque interaction contribue à façonner une identité en ligne souvent plus révélatrice que l'identité réelle elle-même. Cette évolution, amplifiée par la rapidité des échanges et la viralité de l'information, rend aujourd'hui indispensable la maîtrise des techniques d'investigation numérique pour comprendre, vérifier et authentifier les profils en ligne.

Dans le cadre de ce travail d'investigation numérique, l'objet est d'établir le profil d'identité en ligne d'une personne en recoupant les informations publiques et semi-privées disponibles sur Internet et les réseaux sociaux. L'objectif est de rassembler, analyser et documenter les éléments pertinents (comptes sociaux, adresses e-mail, numéros, publications, photos, traces géolocalisées, mentions publiques) afin d'aider à vérifier une identité, reconstruire des activités en ligne ou évaluer des risques (usurpation, comportements problématiques).

Cette investigation, réalisée dans un cadre pédagogique, permet de mettre en pratique les notions étudiées en cours d'investigation numérique : recherche OSINT (Open Source Intelligence), collecte de preuves numériques, analyse de métadonnées et respect des principes de confidentialité et de proportionnalité. Elle contribue à illustrer concrètement c**omment les traces laissées en ligne peuvent révéler une identité**, mais aussi **comment une mauvaise gestion de celles-ci peut exposer une personne** à des menaces telles que l'usurpation, la diffamation ou la cybercriminalité.

II Profil cible

Fiche d'identité générale

Nom complet :	WANSI GILLES GILDAS
Surnoms / pseudonymes :	GILDAS ASPHAT RICH ; GILDAS ASPHAT WANSI
Sexe :	MASCULIN
Date de naissance :	20-01-2003
Lieu de naissance :	MBOUDA
Nationalité / origine :	CAMEROUNAISE
Langues parlées :	FRANCAIS
Adresse / lieu de résidence (approx.) :	CRADAT
Situation familiale :	CELIBATAIRE
Niveau d'éducation / études suivies :	Niveau 4 Ingénieur
Profession / occupation actuelle :	Entrepreneur
Religion / croyances (facultatif) :	Chrétien
Apparence physique :	Taille moyenne, corpulence moyenne
Particularités / signes distinctifs :	
Documents d'identité connus :	CNI, carte d'étudiant
Autres informations générales :	RAS

Dernière mise à jour : 18 octobre 2025

WANSI Gilles Gildas, également connu sous les pseudonymes Gildas Asphat Rich et Gildas Asphat Wansi, est un homme camerounais né le 20 janvier 2003 à Mbouda. De nationalité camerounaise et de confession chrétienne, il réside actuellement au CRADAT. Célibataire et de langue française, il poursuit un cursus de niveau 4 en cycle d'ingénieur à l'ENSP et exerce parallèlement comme entrepreneur. De taille et de corpulence moyennes, il ne présente pas de signes distinctifs particuliers. Il détient une carte nationale d'identité et une carte d'étudiant. Aucun élément particulier n'a été signalé dans les autres informations générales.

III Outils d'investigation

Outils OSINT pour les personnes

Cible	Outils	Description
Adresses e-mail	HaveIBeenPwned, Holehe (CLI), Emailrep.io	Vérifie si un e-mail a fuité ou s'il est associé à des comptes
Numéros de téléphone	TrueCaller, Sync.me, NumVerify API	Identifie le propriétaire d'un numéro
Pseudonymes / usernames	Sherlock, Maigret, Namechk, Knowem	Recherche un pseudo sur des centaines de sites
Localisation / géolocalisation	GeoSocial Footprint, Creepy	Analyse la position issue des réseaux sociaux
Images / photos	Google Images, Yandex Images, TinEye, ExifTool	Recherche inversée d'images, métadonnées EXIF

Outils OSINT pour les réseaux sociaux

Réseau	Outils OSINT dédiés	Utilisation
Facebook	Facebook Graph Search (via URL), IntelTechniques	Recherche d'amis, photos, pages, lieux
Twitter / X	Twint (CLI), TweetDeck	Extraction de tweets sans API
LinkedIn	Linkedin2Username, Phantombuster	Collecte de profils publics
Instagram	Instaloader, Inflact	Téléchargement et analyse de posts publics
TikTok / YouTube	TikTok Scraper, Social Blade	Statistiques, contenus, tendances

IV Méthodologie

La méthodologie adoptée pour cette investigation numérique repose sur une approche rigoureuse, progressive et respectueuse des cadres juridique et éthique. Elle vise à collecter, analyser et interpréter des informations accessibles publiquement en ligne afin d'établir le **profil d'identité numérique** du sujet étudié, *WANSI Gilles Gildas*. Cette démarche suit cinq étapes principales : **la préparation de l'enquête, la collecte des données, l'analyse, le recoupement des informations et la documentation des résultats.**

IV.1 Préparation de l'enquête

Cette première phase a consisté à définir le **périmètre de l'investigation** et les **objectifs de recherche**. Elle visait à déterminer :

— Les informations à rechercher (identité, activités, relations, empreinte numérique, localisation) ;

— Les plateformes prioritaires (réseaux sociaux, moteurs de recherche, bases de données publiques) ;
— Les limites légales et éthiques à respecter (seulement les données accessibles au public).

Un **profil de base** a été établi à partir des données connues (nom complet, pseudonymes, âge, profession, lieu de résidence, etc.) afin de guider les recherches OSINT.

IV.2 Collecte des données (Phase OSINT)

Cette étape a mobilisé des **outils d'investigation numérique** permettant d'explorer les différentes facettes de l'identité en ligne du sujet. Les outils ont été sélectionnés selon le type de données recherchées :

— **Adresses e-mail** : HaveIBeenPwned pour vérifier d'éventuelles fuites ou affiliations à des comptes ;
— **Numéros de téléphone** : TrueCaller pour identifier d'éventuelles correspondances avec des comptes sociaux ;
— **Pseudonymes et usernames** : Sherlock et Maigret pour rechercher les pseudonymes *Gildas Asphat Rich* et *Gildas Asphat Wansi* sur diverses plateformes ;
— **Images et photos** : Google Images pour effectuer des recherches inversées ;
— **Réseaux sociaux** :
  — **Facebook** : Graph Search et **IntelTechniques** pour la recherche d'amis, de pages et de publications associées ;
  — **Instagram** : Instaloader pour l'analyse des posts et des stories publics ;
  — **TikTok et YouTube** : Social Blade et TikTok Scraper pour l'étude des contenus, vues et interactions ;
  — **LinkedIn** : Linkedin2Username pour collecter les profils professionnels publics.

Chaque information trouvée a été sauvegardée sous forme de **captures d'écran horodatées** et **exportations de pages web**, accompagnées de l'URL d'origine et du **hash SHA-256** pour garantir l'intégrité des preuves.

IV.3 Analyse et interprétation des données

Les données collectées ont ensuite été **classées, triées et corrélées** afin de dégager des éléments pertinents. Cette phase a permis de :

— Identifier les comptes vérifiés comme appartenant réellement au sujet ;
— Distinguer les profils potentiellement falsifiés ou inactifs ;
— Déterminer la fréquence et la nature des activités en ligne (publications, commentaires, abonnements) ;
— Évaluer le niveau d'exposition publique de la personne (données personnelles visibles, photos, géolocalisation).

L'analyse a également porté sur les **métadonnées** (dates, lieux, appareils utilisés) afin de mieux comprendre le contexte de publication et d'assurer la cohérence chronologique des traces numériques.

IV.4 Recoupement et validation

Cette étape a consisté à **vérifier la fiabilité** des informations obtenues. Les données issues de plusieurs sources ont été **comparées et croisées** pour confirmer leur authenticité. Par exemple, une photo trouvée sur Facebook a été vérifiée via recherche inversée d'images sur Google et Yandex

pour s'assurer qu'elle n'avait pas été réutilisée ailleurs. Seules les informations cohérentes, datées et vérifiables ont été retenues pour le rapport final.

IV.5 Documentation et présentation des résultats

Enfin, l'ensemble des résultats a été compilé dans un **rapport structuré**, comprenant :
— Une fiche d'identité numérique synthétique du sujet ;
— Les captures et liens de vérification ;
— Les observations analytiques sur le comportement numérique ;
— Les risques identifiés (usurpation, surexposition, fuites de données).

Chaque élément de preuve est accompagné de sa source et de son horodatage, garantissant la traçabilité et la reproductibilité de l'enquête. Cette documentation permet d'assurer la **transparence** du processus et la **recevabilité** des résultats dans un cadre académique ou judiciaire.

V Résultats

Les recherches effectuées ont permis d'obtenir plusieurs informations pertinentes sur la présence numérique du sujet, **WANSI Gilles Gildas**. Ces résultats sont issus exclusivement de sources ouvertes, accessibles publiquement, et ont été vérifiés par recoupement.

Présence en ligne et cohérence du profil

Les pseudonymes *Gildas Asphat Rich* et *Gildas Asphat Wansi* apparaissent de manière récurrente sur différentes plateformes sociales, notamment Facebook, Instagram et LinkedIn. Les informations partagées (nom, localisation, photo de profil, domaine d'étude) sont cohérentes entre elles, ce qui renforce l'authenticité du profil. Les publications recensées concernent principalement des sujets liés à la technologie, à la vie estudiantine et à l'entrepreneuriat, ce qui correspond à la profession déclarée du sujet.

Analyse des images et métadonnées

Une recherche inversée d'images via Google Images et Yandex a permis de confirmer l'origine et la cohérence de plusieurs photos associées au profil. Les métadonnées EXIF récupérées à l'aide de l'outil *ExifTool* indiquent des prises de vue au Cameroun, corroborant la localisation du sujet au CRADAT. Aucune anomalie ni signe de réutilisation d'images provenant d'autres profils n'a été détectée, ce qui réduit la probabilité d'usurpation d'identité.

Résultats OSINT techniques

Les vérifications réalisées sur *HaveIBeenPwned* et *Holehe* n'ont révélé aucune fuite de données associée aux adresses e-mail connues du sujet. Les recherches via *TrueCaller* et *NumVerify* confirment la correspondance des numéros de téléphone avec des comptes authentiques. Les analyses sur *Social Blade* et *TikTok Scraper* n'ont mis en évidence aucun contenu problématique ni activité suspecte sur les plateformes observées.

Risques identifiés

Bien que la présence numérique du sujet reste cohérente et modérée, certains risques potentiels ont été relevés :

— **Surexposition des données personnelles :** certaines informations (localisation, photos publiques, détails sur la vie privée) sont accessibles sans restriction, exposant le sujet à des risques d'ingénierie sociale ou d'usurpation.
— **Corrélation inter-profils :** la réutilisation identique des pseudonymes sur plusieurs plateformes facilite la traçabilité et la cartographie numérique du sujet.
— **Absence de gestion de confidentialité :** les paramètres de visibilité sur certains comptes ne sont pas optimisés, ce qui pourrait compromettre la confidentialité.

Synthèse des résultats

En résumé, l'investigation a permis de :
— Confirmer l'existence d'une identité numérique authentique et cohérente ;
— Identifier les principales plateformes utilisées par le sujet ;
— Évaluer le niveau d'exposition publique et les risques potentiels liés à la visibilité en ligne ;
— Démontrer l'importance de la gestion de la confidentialité et du contrôle des données personnelles.

VI Recommandations

Au terme de cette investigation, plusieurs recommandations sont formulées afin d'améliorer la sécurité et la maîtrise de l'identité numérique du sujet étudié :

[label=6.]

1. **Renforcer la confidentialité :** paramétrer les comptes sociaux pour limiter l'accès aux informations personnelles (photos, géolocalisation, liste d'amis).
2. **Varier les pseudonymes :** éviter la réutilisation des mêmes identifiants sur plusieurs plateformes afin de réduire la traçabilité.
3. **Surveiller régulièrement sa présence numérique :** effectuer des recherches périodiques sur son nom et ses pseudonymes afin de détecter d'éventuelles usurpations ou fuites.
4. **Utiliser des mots de passe robustes et uniques :** adopter un gestionnaire de mots de passe et activer la double authentification sur les comptes sensibles.
5. **Limiter la diffusion publique d'informations personnelles :** ne publier que des contenus nécessaires et maîtriser leur visibilité.
6. **Sensibiliser à la cyberhygiène :** promouvoir une culture de la vigilance numérique, notamment auprès des étudiants et jeunes professionnels.

Ces mesures s'inscrivent dans les bonnes pratiques recommandées par les experts en cybersécurité et investigation numérique, notamment par le *Centre for Internet Security (CIS)*, l'*ANSSI* et la *Cybersecurity and Infrastructure Security Agency (CISA)*.

CONCLUSION

Cette investigation numérique, centrée sur l'analyse de l'identité en ligne de Wansi Gilles Gildas, a permis de démontrer l'efficacité des outils OSINT dans la collecte et la corrélation d'informations publiques. Elle illustre comment les traces laissées sur le web peuvent être analysées de manière rigoureuse pour dresser un profil numérique fiable, tout en respectant les cadres éthique et légal. L'étude révèle que, bien qu'il soit possible de reconstruire une image assez complète d'une personne à partir de données publiques, la frontière entre vie privée et vie numérique reste fragile. Ce travail souligne donc la nécessité d'une vigilance accrue et d'une éducation numérique renforcée, afin de prévenir les risques d'usurpation, de désinformation ou d'exploitation malveillante des données personnelles. En définitive, la maîtrise de son identité numérique apparaît aujourd'hui comme une compétence essentielle dans un monde connecté, où chaque donnée partagée peut devenir un élément d'enquête, mais aussi une potentielle vulnérabilité.