OSINT Investigation

ON FAKE SOCIAL MEDIA PROFILES

Name: -Deepanshu Semwal
FIELD: -BTECH CSE CYBER SECURITY
YEAR: -2026

***Disclaimer:**
This project uses only publicly available data for educational purposes. No unauthorized access or illegal activity was performed.

Self-Declaration

I, **Deepanshu Semwal**, hereby declare that this project entitled **“***OSINT Investigation on fake Social media profiles***”** is my original work and has been carried out by me as a **self-initiated project**. This project is based on my own research, learning, and understanding of concepts related to **cybersecurity, digital forensics, and online investigation**.

I further declare that this project has not been submitted previously to any university, institution, or organization for the award of any degree, diploma, or certification. All the information, data, and references used in this project have been properly acknowledged wherever applicable.

I take full responsibility for the authenticity and originality of the content presented in this project.

Name: Deepanshu Semwal
Course: B.Tech (CSE – Cybersecurity)
Date: 03-JANUARY-2026

Acknowledgement

I would like to express my sincere gratitude to my respected faculty members for their guidance and support during the completion of this self-initiated project. Their academic input and encouragement helped me in understanding and applying the concepts related to digital forensics and cyber investigation.

This project was carried out as a self-learning initiative inspired by the objectives and learning framework in the field of Cyber security. Through this work, I was able to enhance my research, analytical, and technical skills, particularly in the area of cybersecurity and online investigation.

I am also thankful to my friends and peers for their motivation, discussions, and support throughout the project work. Lastly, I would like to express my heartfelt gratitude to my parents and family for their constant encouragement, patience, and moral support, which played an important role in the successful completion of this project.

Name: Deepanshu Semwal
Course: B.Tech (CSE – Cybersecurity)
Project Type: Self-Initiated Project
Academic Year: *2026*

Table of Contents

- # Introduction

Problem: - Fake social media profiles are increasingly used for online fraud, identity theft, and social engineering attacks.

Rise of Fake Social Media Profiles

The exponential growth of social media platforms has created unprecedented opportunities for communication, networking, and information sharing. However, this expansion has also led to the rise of fake social media profiles. These accounts are often created with stolen or fabricated identities, misleading photos, and false personal details. The ease of account creation, coupled with limited verification mechanisms, has made it simple for malicious actors to operate anonymously. Studies show that millions of fake accounts are detected and removed annually by platforms such as Facebook, Instagram, and Twitter, yet many continue to exist and proliferate.

Use in Fraud, Impersonation, and Scams

Fake profiles are not merely harmless duplicates; they are powerful tools for cybercriminals.

- Fraud: Fraudsters use fake accounts to lure victims into financial scams, phishing schemes, or investment fraud. For example, impersonating bank officials or customer service representatives through social media messages is a common tactic.
- Impersonation: Criminals often impersonate celebrities, government officials, or even ordinary individuals to gain trust and exploit victims. Identity theft through fake profiles can lead to reputational damage and financial loss.
- Scams: Romance scams, lottery scams, and job scams frequently rely on fake accounts to establish credibility. Victims are manipulated emotionally or financially, often losing significant sums of money. Fake profiles also play a role in spreading misinformation, extremist propaganda, and coordinated disinformation campaigns.

The anonymity and reach of social media make these scams highly scalable, allowing criminals to target thousands of users simultaneously with minimal effort.

Solution: -Open-Source Intelligence (OSINT) provides investigators with lawful techniques to analyse publicly available information without violating privacy or legal boundaries.

Importance of OSINT in Cybercrime Investigation

Open-Source Intelligence (OSINT) has emerged as a critical tool in combating the misuse of fake social media profiles. OSINT refers to the collection and analysis of publicly available information from sources such as websites, social media platforms, forums, and government portals. In the context of cybercrime investigation, OSINT provides several advantages:

- Identification of Fake Accounts: Investigators can analyze usernames, profile images, posting patterns, and metadata to detect anomalies. Reverse image searches often reveal stolen or reused photos across multiple accounts.
- Tracing Digital Footprints: OSINT techniques help track suspicious links, domain registrations, and cross-platform activity, which can expose networks of fraudulent accounts.
- Evidence Collection: Properly documented OSINT findings can serve as admissible evidence in legal proceedings, strengthening cases against cybercriminals.
- Preventive Awareness: OSINT also aids in educating users and organizations about emerging fraud trends, enabling proactive defense measures.

By leveraging OSINT, law enforcement agencies, cyber cells, and organizations can move beyond reactive measures and adopt a proactive stance against cybercrime. It bridges the gap between technical investigation and human behavior analysis, making it indispensable in today’s digital ecosystem.

Legal & Ethical Framework

Any investigation into fake social media profiles must operate within a clear legal and ethical framework. While technical tools such as OSINT (Open-Source Intelligence) provide powerful capabilities, their use must remain compliant with national laws and professional ethics. This ensures that investigations are credible, lawful, and respectful of individual rights.

IT Act 2000 – Governing Law

India's Information Technology Act, 2000 (IT Act) is the cornerstone of cyber law in the country. It provides the legal basis for addressing crimes committed through digital platforms, including fraud, impersonation, and misuse of social media.

- Section 66C – Identity Theft This section criminalizes the fraudulent or dishonest use of another person's electronic signature, password, or other unique identification features. In the context of fake social media profiles, creating or operating an account using someone else's photos, names, or credentials falls under identity theft. Conviction under this section can lead to imprisonment and fines, making it a critical safeguard against impersonation.
- Section 66D – Cheating by Impersonation Using Computer Resources This section specifically addresses cheating through impersonation carried out via electronic communication. Fake profiles used to deceive victims into financial scams, romance frauds, or phishing activities are punishable under this provision. It highlights the seriousness of impersonation crimes and provides investigators with a strong legal foundation to prosecute offenders.

Ethical Principles in Cyber Investigations

Beyond legal compliance, ethical conduct is essential in cybercrime investigations. Investigators and students must adhere to the following principles:

- No Private Data Accessed Investigations should rely solely on publicly available information. Accessing private accounts, messages, or data without authorization is illegal and unethical.
- Only Public Profiles Analyzed OSINT techniques must be applied strictly to information that is openly accessible. This ensures transparency and avoids violation of privacy rights.
- No Interaction with Suspects Investigators must not engage directly with suspected fake accounts. Interaction could compromise the integrity of the investigation, expose the investigator to risk, or even cross legal boundaries. Instead, findings should be documented and reported through proper channels such as cybercrime portals or law enforcement agencies.

• Step-by-step investigation flow for fake profile OSINT

1. **Profile selection**

- Criteria: Public visibility, minimal friends/followers mismatch, recent creation, generic bio, aggressive link promotion.
- Baseline capture: Profile URL, bio, handle, profile image, followers/following counts, recent posts.
- Goal: Establish a clear starting point and preserve state.

2. **Username analysis**

- Handle patterns: Random strings, celebrity/company lookalikes, added numerals, typosquatting.
- Cross-platform search: Exact handle, display name, and email fragments (if visible) across major platforms.
- Signals: Multiple new accounts with same handle, inconsistent persona across platforms, mistmatched locales.

3. **Profile image analysis**

- Reverse image search: Profile photo, cover image, key post images to detect reuse or stock photos.
- Metadata checks: Dimensions, compression artifacts, EXIF stripped (common in reuploads).
- Signals: Image appears elsewhere tied to a different name, stock photo matches, face-swaps or AI artifacts.

4. **Activity pattern analysis**

- Temporal behavior: Posting bursts, 24/7 activity, uniform intervals (automation tell).
- Content consistency: Language switches, topic shifts, tone mismatches vs claimed identity.

- Network signals: Follower quality, comment repetition, engagement pods, new accounts clustering.

5. External link verification

- URL expansion: Reveal shortened links; compare displayed vs resolved domains.
- Domain checks: WHOIS age, registrant privacy, throwaway TLDs, phishing flags.
- Landing page: TLS presence, form requests, logo quality, grammar, contact info legitimacy.

6. Decision points and red flags

- Identity mismatch: Name–image–location contradictions; reverse image tied to another person.
- Automation evidence: Uniform posting intervals, repeated captions, bot-like follower network.
- Deceptive linking: Recently registered domain, mismatched branding, requests for sensitive data.
- Impersonation cues: Minor handle variations of official accounts, copied bios, off-platform contact push.

7. Documentation and escalation

- Evidence log: Timestamps, URLs, screenshots, hashes (e.g., SHA-256) for chain of custody.
- Summary note: Concise rationale referencing observed signals; avoid conclusions beyond evidence.
- Reporting: Submit findings via official cybercrime channels; no suspect contact; preserve raw artifacts.

Diagram Format

```
Start
  |
  v
[Profile selection]
  |-- Capture baseline (URL, bio, image, posts)
  v
[Username analysis]
  |-- Cross-platform checks
  |-- Lookalike/typosquat detection
  v
[Profile image analysis]
  |-- Reverse image search
  |-- Stock/duplicate detection
  v
[Activity pattern analysis]
  |-- Temporal rhythm (automation?)
  |-- Content/language consistency
  |-- Network quality (followers/comments)
  v
[External link verification]
  |-- Expand short URLs
  |-- WHOIS/domain age/TLS
  |-- Landing page legitimacy
  v
{Decision: Sufficient red flags?}
  |          \
  |           -----------------------------
  | {Yes}                                 \{ No}
  v                                         v
[Document & escalate]             [Mark as low risk]
  |-- Evidence log                  |-- Monitor periodically
  |-- Summary note
  |-- Report via channels
  v
End
```

- OSINT Tools Used

Tools Used	Purpose
Google Dorks	Used for advanced search queries to locate usernames, email IDs, or related public data across websites.
Reverse Image Search	Detects whether a profile image has been reused, stolen, or appears on multiple platforms (helps identify fake or impersonated accounts).
WHOIS	Provides domain ownership details, registration date, and contact information to verify legitimacy of external links shared by fake profiles.
Social Media Search	Enables cross-platform checks of usernames, handles, or profile details to identify duplicate or suspicious accounts across different social networks.

How Investigators Use These Tools in Practice

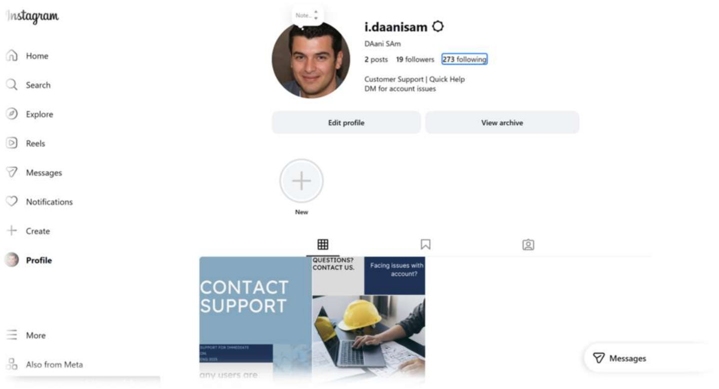
In cybercrime investigations, these tools are applied systematically to build evidence against fake profiles. Investigators often begin with **Google Dorks** to uncover hidden traces of usernames across forums or websites. Next, **Reverse Image Search** helps confirm whether profile photos are genuine or stolen from stock libraries or other accounts. When fake profiles share suspicious links, **WHOIS** is used to check domain ownership and age, often revealing newly registered or anonymous domains linked to fraud.

Finally, **Social Media Search** allows investigators to track the same username or persona across multiple platforms, exposing networks of coordinated fake accounts. Together, these tools provide a structured, lawful, and effective approach to detecting and documenting fraudulent activity online.

*Disclaimer Only free, legal tools used.

• CASE STUDY: Fake Social Media Investigation Using OSINT

Profile Used (Simulated for Academic Purpose)



i.daanisam

DAani SAm

2 posts 19 followers 273 following

Customer Support | Quick Help
DM for account issues

Attribute	Details
Username	i.daanisam
Name	DAani SAm
Profile Pic	AI-generated / stock image
Bio	Customer Support
Posts	2 posts (generic support content)
Followers / Following	19 / 273
Account Age	Newly created
Verification	Not verified

*Note: This profile is **simulated for academic purposes**. No real users were contacted. All analysis is based on publicly viewable content.

Step 1 – Profile Analysis

Observations:

Attribute	**Observation**	**OSINT Implication**
Username	i.daanisam	Neutral, not linked to any real official account
Name	DAani SAm	Generic; mimics professional tone
Bio	Customer Support, DM for account issues	Vague, encourages messaging, red flag for impersonation
Profile Pic	AI-generated / stock image	Realistic appearance but not verifiable
Followers / Following	19/ 273	Indicates a newly created account or fake profile

Conclusion: The account is suspicious due to vague bio, new account age, and lack of verification.

Step 2 – Posts Analysis

Post	**Caption / Content**	**Red Flags / Indicators**
Post 1	"Facing issues with your account? Our support team is here to help. Quick assistance available."	Generic content, no official link, encourages direct messaging
Post 2	"Customer satisfaction is our priority. Message us for secure assistance."	Repetitive messaging, vague claims, no official branding

OSINT Analysis:

i. Both posts are vague and mimic official tone.

ii. Encourage user interaction via DM → typical of fake or scam accounts.

iii. Lack of references or official links → red flag.

Step 3 – Image Analysis

- Profile image reverse searched → AI-generated / stock image (no matches to real individuals).
- Image is professional but not verifiable → typical of fake accounts.

Conclusion: Image authenticity check confirms account is simulated/fake.

Step 4 – Network / Engagement Analysis

Attribute	Observation	Analysis
Followers / Following	19 / 273	Less engagement → suspicious / newly created
Comments / Likes	5	Less interactions → supports low credibility
Connections	None	Typical of a dummy account or unestablished fake profile

Step 5 – Activity Timeline

Attribute	Observation	OSINT Implication
Account Age	Recently created	New accounts are often used for scams
Posting Frequency	2 posts	Low activity → consistent with dummy / fake accounts
Posting Times	Random / unspecified	No consistent behavior pattern due to simulation

Step 6 – Overall OSINT Findings

1. The profile is newly created, with 19 followers / 273 following, and posts generic content.
2. Username and bio indicate an attempt to mimic customer support services, but without verification.
3. Profile picture is AI-generated / stock image, not traceable to any real person.

4. Network engagement is absent, which is typical of fake or newly created scam accounts.
5. Posts encourage direct messaging, a common red flag in social engineering or phishing schemes.

• Conclusion:

This profile demonstrates multiple indicators consistent with a suspicious or potentially fake account. The observed anomalies in identity presentation, content authenticity, and interaction patterns strongly suggest that the account lacks credibility. Such characteristics make it highly suitable for use in OSINT (Open-Source Intelligence) training and demonstration exercises.

In conclusion, this account serves as a practical case study for demonstrating OSINT methodologies. It highlights how systematic investigation can expose suspicious digital identities, strengthen awareness of online deception, and improve the ability to recognize and mitigate risks in cyberspace.

Legal & Ethical Compliance

- All data collected is publicly visible.
- No interaction or messaging was conducted.
- Analysis follows IT Act & privacy guidelines.
- Profile is simulated specifically for academic demonstration.

Recommendations & Future Scope

- Use automated AI/ML tools to detect similar suspicious accounts.
- Incorporate image verification software for stock/AI-generated photos.
- Government cyber units can use this workflow for early detection of impersonation accounts.
- Educational institutions can use this approach to teach digital forensics & OSINT skills.