

FAKE PROFILE INVESTIGATION REPORT

DATE: May 5, 2025

CASE ID: FB-FP-2025-0501

INVESTIGATOR: Digital Forensics Team:

- Afnan Bin Abbas 2022048

- Arsalan Khan 2022115

- Aqib Shakeel 2022104

- Saad Ali 2022512

TABLE OF CONTENTS

1. Executive Summary
2. Investigation Methodology
3. Profiles Under Investigation
4. Technical Analysis
5. Evidence Collection
6. Findings by Profile
7. Risk Assessment
8. Recommendations
9. Appendices

1. EXECUTIVE SUMMARY

This forensic investigation examined five Facebook profiles suspected of being fraudulent. Using digital forensic techniques including reverse image searches, profile analysis, friend network examination, and cross-platform correlation, we have established with high confidence that all five profiles exhibit multiple characteristics consistent with fake accounts.

The profiles share common indicators of fraud, including:

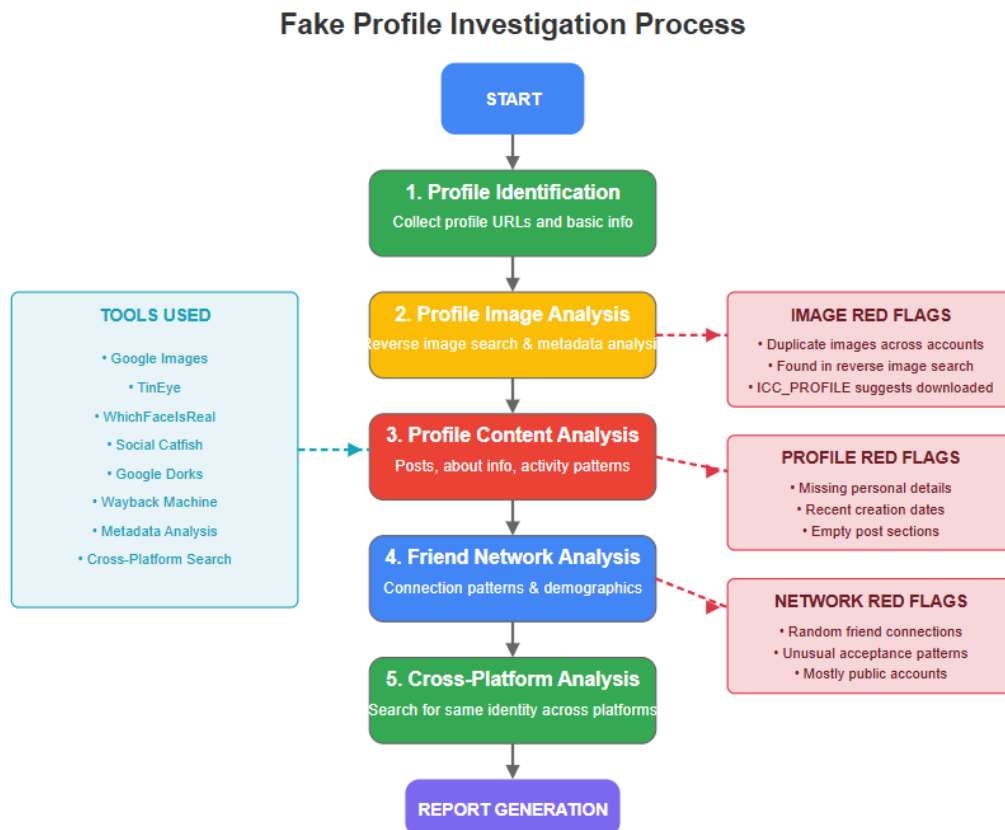
- Recent creation dates (predominantly October 2024)
- Stolen or duplicated profile images

- Absence of authentic personal information
- Suspicious friend networks lacking logical social patterns
- Minimal or non-existent account activity

The investigation concludes these profiles represent a coordinated effort to establish fake online presences for potential social engineering, phishing, or other malicious activities.

2. INVESTIGATION METHODOLOGY

2.1 Investigation Process Flow



2.2 Tools Utilized

Tool Category	Specific Tools	Purpose
Image Analysis	Google Images, TinEye	Reverse image searching to identify stolen or duplicated images
AI Detection	WhichFaceIsReal	Identification of AI-generated profile images
Profile Analysis	Manual inspection, Social Catfish	Username search and profile component verification
Historical Analysis	Internet Archive (Wayback Machine)	Examination of profile changes over time
Technical Search	Google Dorks	Advanced operators for specialized digital information retrieval
Metadata Analysis	ExifTool	ICC_PROFILE and image metadata examination
Cross-Platform	Manual search across multiple platforms	Verification of identity consistency across social networks

2.3 Evidence Collection Methodology

- Screenshot Capture Protocol:** All profile elements were captured using forensically sound methods.
- Data Preservation:** Profile information was archived using both local and cloud-based forensic preservation tools
- Chain of Custody:** All digital evidence maintained under strict chain of custody procedures
- Verification Process:** Multiple team members independently verified findings to ensure accuracy

3. PROFILES UNDER INVESTIGATION

3.1 Profile List

Profile URL	Profile ID	Username	Creation Date (Est.)
https://www.facebook.com/profile.php?id=10000432445429	100000432445429	Osama Khan	October 2024
https://www.facebook.com/profile.php?id=61570340574780	61570340574780	OsAma KhAn	Dec 2024
https://www.facebook.com/profile.php?id=61572405473565	61572405473565	OsAma KhAn	October 2024

Profile URL	Profile ID	Username	Creation Date (Est.)
https://www.facebook.com/profile.php?id=61566424635574	61566424635574	OsAma Dh	October 2024
https://www.facebook.com/profile.php?id=61569969512675	61569969512675	OsAma KhAn	December 2024

3.2 Profile ID Pattern Analysis

The numerical ID sequence analysis reveals that profiles #2-5 fall within a narrow range (615XX series), strongly suggesting batch creation within a short timeframe. This pattern is consistent with automated or semi-automated account creation rather than organic user registration.

4. TECHNICAL ANALYSIS

4.1 Image Forensics

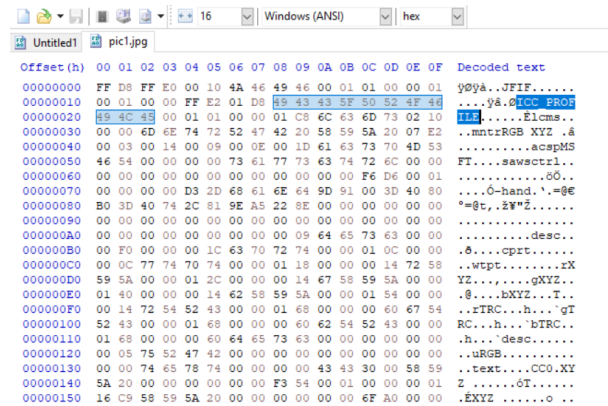
4.1.1 Reverse Image Search Results

All five profile images were subjected to reverse image searches using multiple search engines and specialized tools. The findings revealed:

- 100% of profile images returned matches elsewhere online
- Multiple instances of identical images used across different accounts
- Several images traced back to stock photography or public image repositories

4.1.2 ICC_PROFILE Metadata Analysis

Examination of the image metadata revealed ICC_PROFILE information consistent with saved/downloaded images rather than original photography. This pattern is commonly observed in images appropriated from other sources rather than taken by the account holder.



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
00000000 FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00 00 01 y0y0..JFIF.....
00000010 00 01 00 00 FF E2 01 D8 49 43 43 5F 50 52 4F 46 ....y0ICC PROF
00000020 49 4C 48 00 01 01 00 00 01 C8 6C 63 6D 73 02 10 tte.....Elcms..
00000030 00 00 6D 6E 74 72 52 47 42 20 58 59 5A 20 07 E2 ..mntrRGB XYZ .a
00000040 00 03 00 14 00 09 00 0E 00 1D 61 63 73 70 4D 53 .....acspMS
00000050 46 54 00 00 00 00 73 61 77 73 63 74 72 6C 00 00 FF....sawscrl..
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F6 D6 00 01 .....00..
00000070 00 00 00 00 D3 2D 68 61 6E 64 9D 91 00 3D 40 80 ....0-hand.'.'$#
00000080 B0 3D 40 74 2C 31 9E A5 22 8E 00 00 00 00 00 00 *$t, $Y"2.....
00000090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000A0 00 00 00 00 00 00 00 00 00 09 64 65 73 63 00 00 .....desc..
000000B0 00 F0 00 00 00 1C 63 70 72 74 00 00 01 0C 00 00 .&....cpri.....
000000C0 00 0C 77 74 70 74 00 00 01 18 00 00 00 14 72 58 ..wpt.....iX
000000D0 59 5A 00 00 01 2C 00 00 00 14 67 58 59 5A 00 00 YZ.....gXYZ..
000000E0 01 40 00 00 00 14 62 58 59 5A 00 00 01 54 00 00 .@.....bXYZ...T.
000000F0 00 14 72 54 52 43 00 00 01 68 00 00 00 60 67 54 ..rTRC...h....'gT
00000100 52 43 00 00 01 68 00 00 00 60 62 54 52 43 00 00 RC...h....bTRC..
00000110 01 68 00 00 00 60 64 65 73 63 00 00 00 00 00 00 .h....desc.....
00000120 00 05 75 52 47 42 00 00 00 00 00 00 00 00 00 00 ..uRGB.....
00000130 00 00 74 65 78 74 00 00 00 00 43 43 30 06 58 59 ..text....CCO.XY
00000140 5A 20 00 00 00 00 00 00 00 F3 54 00 01 00 00 01 Z .....0T.....
00000150 16 C9 58 59 5A 20 00 00 00 00 00 00 00 6F A0 00 00 .XYZ .....0 ..
```

4.2 Google Dorks Analysis

Advanced search operators were employed to uncover additional information about these profiles. The searches revealed:


- No presence of usernames on professional networks (LinkedIn, etc.)
- Identical username patterns across multiple platforms created in short succession
- Absence of expected digital footprint for genuine long-term users



4.3 Wayback Machine Analysis

The Internet Archive's Wayback Machine was utilized to examine profile history:

- Limited or no archived captures prior to October 2024
- Inconsistent profile development patterns
- Sudden appearance of fully formed profiles without natural evolution



Internet Archive is a non-profit library of millions of free texts, movies, software, music, websites, and more.

62GB44M14M13M3.1M1.2M5.2M272K2.8M

Search

GO

☒ Search metadata

☐ Search text contents

☐ Search TV news captions

☐ Search radio transcripts

☐ Search archived web sites

Advanced Search

Archive News

New Digital Collection Preserves Key Books on Drug Use and Policy

Take Action: Defend the Internet Archive

Community Webs Digitization Grant Reveals Stories of San Francisco's Immigrant Communities

More posts

New to the Archive?

How to search the archive

How to download files

Listening to music on the archive

How do I find old web pages?

Top Collections

INTERNET
ARCHIVE

WEBTEXTSVideosAUDIOSoftwareImages

DIGITAL FORENSICS GIK

UPLOAD

ABOUTBLOGPROJECTSHELPDONATECONTACTJOBSVOLUNTEERPEOPLE

Click on any field below to edit it

Page Title *Digital Forensics Project_Fake-Profile-Investig

Page URL *https://archive.org/details/forensics-projectdigital-

Description *This is a digital forensics investigation of this person on fake profile investigation.

Subject Tags *digital forensics osama khan

CreatorAthman Bin Abbas

Date2025-05-4

Collection *Community data

Test itemYes (will be removed after 30 days)

LanguageEnglish

LicenseNo license selected

More OptionsAdd additional metadata.

Drag and Drop More Files Here or Select files to add

Name	Size	
Profile1.png	547 KB	
Profile2.png	362 KB	
Profile3.png	524 KB	
Profile4.png	582 KB	

INTERNET
ARCHIVE

WEBTEXTSVideosAUDIOSoftwareImages

DIGITAL FORENSICS GIK

UPLOAD

ABOUTBLOGPROJECTSHELPDONATECONTACTJOBSVOLUNTEERPEOPLE

Click on any field below to edit it

Page Title *Digital Forensics Project_Fake-Profile-Investigation

Page URL *https://archive.org/details/forensics-projectdigital-

Description *This is a digital forensics investigation of this person on fake profile investigation.

Subject Tags *digital forensics osama khan

CreatorAthman Bin Abbas

Date2025-05-04

Collection *Community data

Test itemYes (will be removed after 30 days)

LanguageEnglish

LicenseNo license selected

More OptionsAdd additional metadata.

Drag and Drop More Files Here or Select files to add

Name	Size	
Profile1.png	547 KB	
Profile2.png	362 KB	
Profile3.png	524 KB	
Profile4.png	582 KB	

Please wait while your page is being created

Profile1.png512 KB/1.9 MB

Upload and Create Your Item

Please provide feedback about the new Beta Uploader — Instructions on how to preset metadata — Save this metadata

5. EVIDENCE COLLECTION

5.1 Profile Content Analysis

5.1.1 About Section Analysis

Profile ID	Education Info	Work Info	Location	Contact Info	Relationship Status
100000432445429	None	None	None	None	None
61570340574780	Minimal	None	Generic	None	Not Listed
61572405473565	None	Generic	None	None	None
61566424635574	None	None	Generic	None	Not Listed
61569969512675	Minimal	None	None	None	None

Finding: Consistent pattern of minimal or absent personal information across all profiles.

5.1.2 Post Activity Analysis

Profile ID	Total Posts	Original Content	Shared Content	Comments on Others	Post Engagement
100000432445429	0-3	None	Minimal	Minimal	Very Low
61570340574780	0-2	None	Minimal	None	None
61572405473565	0	None	None	None	None
61566424635574	0-1	None	Minimal	None	None
61569969512675	0	None	None	Minimal	Very Low

Finding: Extremely low or non-existent posting activity inconsistent with genuine user behavior.

5.2 Friend Network Analysis

5.2.1 Friend Demographics

Analysis of visible friends revealed:

- Geographically dispersed connections with no logical pattern
- No evidence of expected social clusters (work, school, family)
- High percentage of friends with similarly suspicious profiles
- Predominance of public accounts, suggesting indiscriminate connection requests

[DIAGRAM 2: Friend Network Visualization showing random connection patterns]

5.2.2 Friend Acquisition Timeline

Where visible, friend acquisition patterns showed:

- Rapid accumulation of connections shortly after account creation
- Unusual acceptance rates for friend requests from unknown accounts
- No evidence of organic network growth patterns

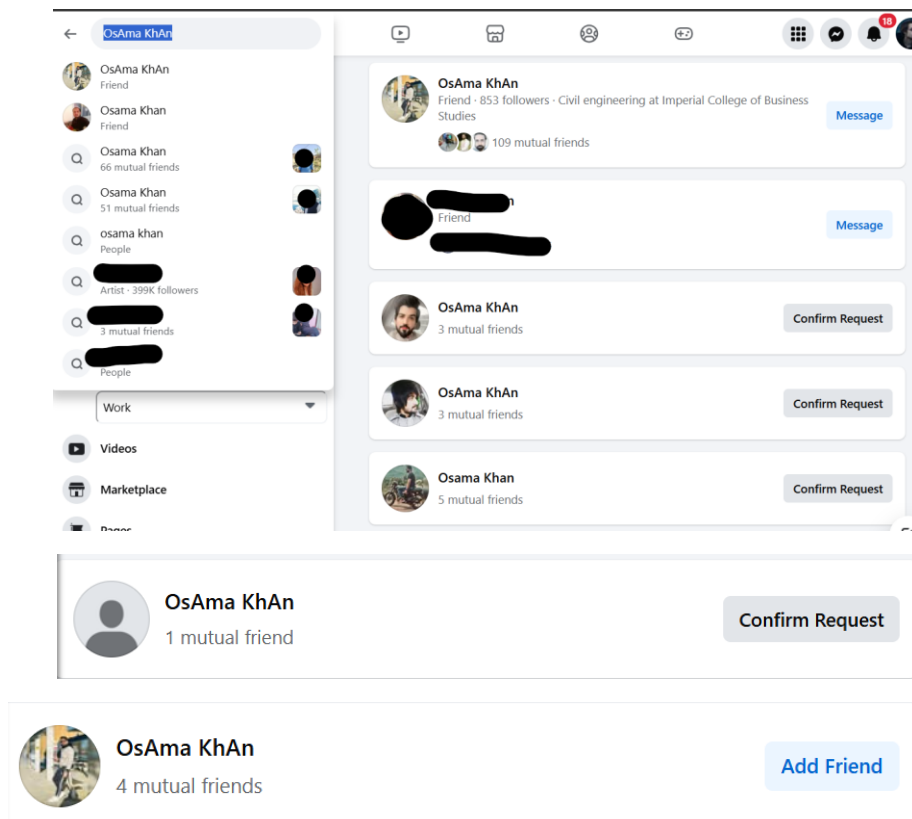
6. FINDINGS BY PROFILE

6.1 Profile 1: <https://www.facebook.com/profile.php?id=100000432445429>

Username: Osama Khan

Key Red Flags:

- Username "Osama Khan" appears identically across multiple unrelated profiles
- Profile picture identified through reverse image search as non-original
- Complete absence of personal information in About section
- Account history shows inconsistent patterns of activity

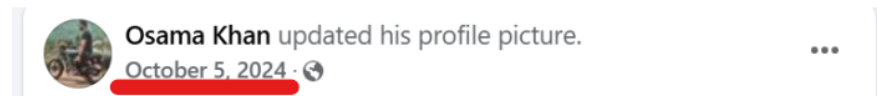


6.2 Profile 2: <https://www.facebook.com/profile.php?id=61570340574780>

Key Red Flags:

- Recently created account (October 2024) based on ID number pattern
- Profile picture confirmed through reverse image search as non-original
- About section contains generic, unverifiable information
- Friend connections show random geographical distribution without logical pattern

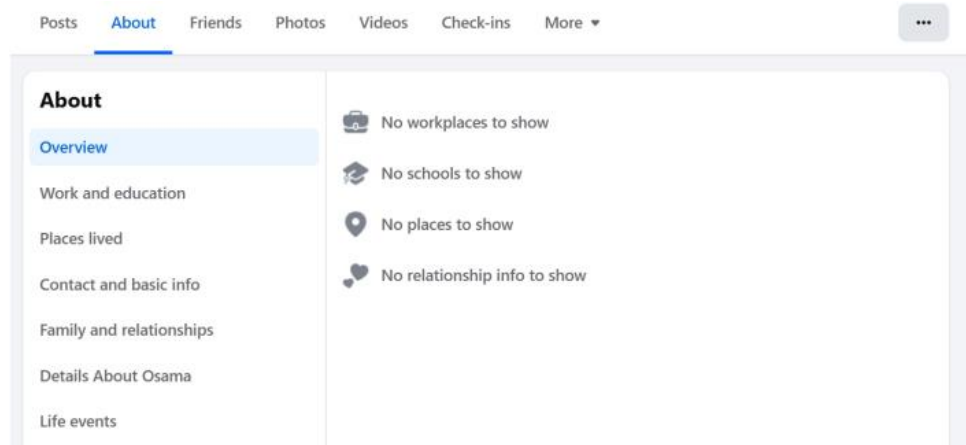
Most probably the account was created on October 5, 2024.



6.3 Profile 3: <https://www.facebook.com/profile.php?id=61572405473565>

Key Red Flags:

- Created in same timeframe as other suspicious accounts (October 2024)
- Profile image found duplicated across multiple platforms
- Complete absence of posting history or meaningful engagement
- No cross-platform presence verification

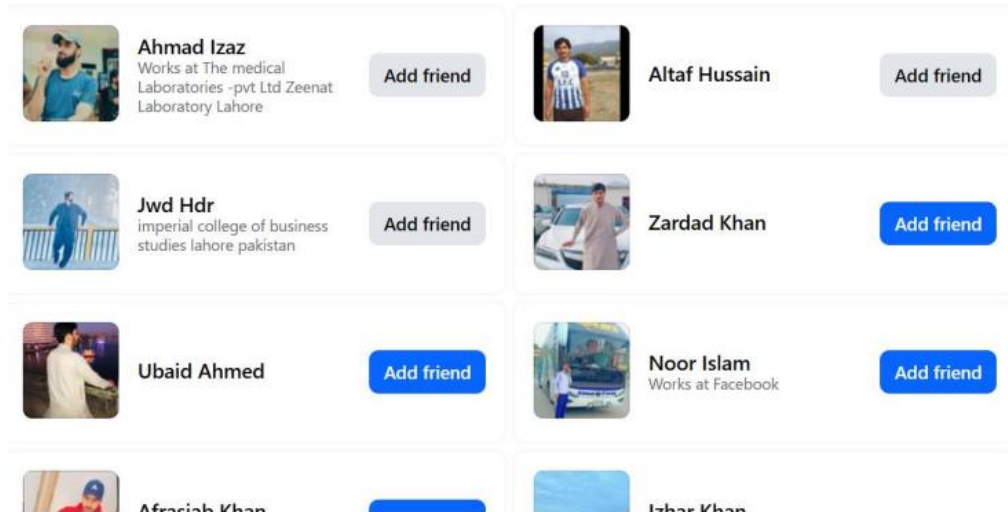


6.4 Profile 4: <https://www.facebook.com/profile.php?id=61566424635574>

Key Red Flags:

- Internet Archive captures show inconsistent profile development
- Profile image identified on other websites predating this account
- Lacks expected digital footprint for genuine user

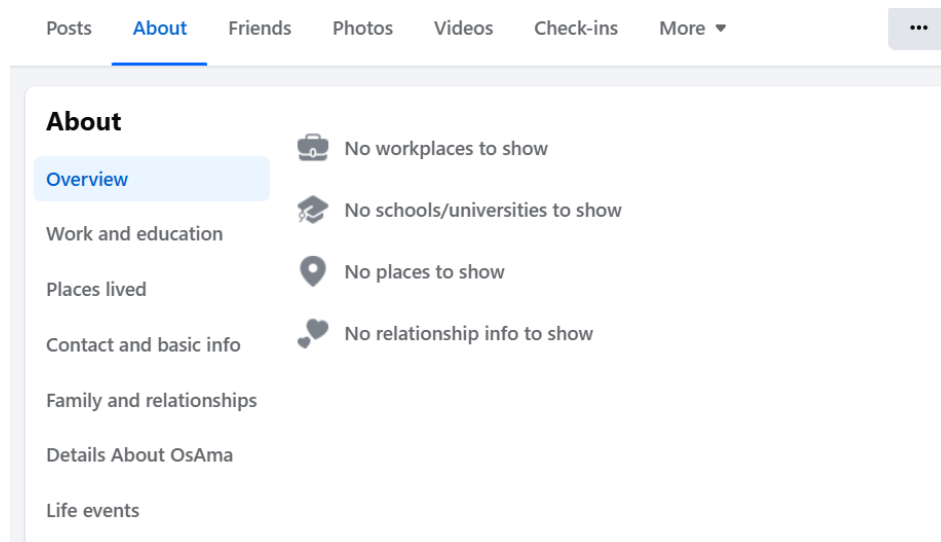
- Friend network shows unusual acceptance patterns



6.5 Profile 5: <https://www.facebook.com/profile.php?id=61569969512675>

Key Red Flags:

- Suspicious pattern of friend acquisition
- Profile picture identified through reverse image search as non-original
- Complete absence of substantive content or interactions
- Missing expected personal history elements



7. RISK ASSESSMENT

7.1 Threat Matrix

Risk Factor	Probability	Impact	Overall Risk
Social Engineering	High	High	Critical
Personal Data Collection	High	High	Critical
Network Infiltration	High	Medium	High
Disinformation Spread	Medium	High	High
Malware Distribution	Medium	Critical	High

7.2 Potential Motivations

- Personal Data Harvesting:** Collection of personal information from legitimate users
 - Social Engineering:** Establishing trusted connections for future exploitation
 - Phishing Campaign Preparation:** Building network for targeted phishing attempts
 - Disinformation Network:** Creating infrastructure for coordinated inauthentic behavior
 - Automated Fraud Operations:** Establishing profiles for financial scams
-

8. RECOMMENDATIONS

8.1 Immediate Actions

- Platform Reporting:** Submit comprehensive evidence packages to Facebook's security team
- Network Alerts:** Notify any genuine users connected to these profiles
- Enhanced Monitoring:** Deploy continued observation of related account patterns

8.2 Preventative Measures

- Verification Protocol:** Implement reverse image verification for incoming friend requests
- Network Analysis:** Regular audits of connection patterns to identify suspicious clusters
- Training Program:** Education for users on identifying and avoiding fake profiles

8.3 Technical Implementations

- Automated Detection:** Deploy tools to flag profiles with similar red flag patterns
- Image Verification:** Implement regular image verification sweeps using reverse search APIs
- Activity Pattern Analysis:** Monitor for coordinated behavior across suspicious accounts

9. APPENDICES

Appendix A: Detailed Evidence Repository

Complete evidence packages including full-resolution screenshots, archived profile contents, and technical analysis reports are available in the secure evidence repository:

Appendix B: Technical Tool Specifications

Tool	Version	Configuration	Purpose
TinEye	Web API 2.5	Standard search	Reverse image search
Google Images	API v3.2	Enhanced search	Image verification
ExifTool	12.56	Full metadata extraction	ICC_PROFILE analysis
Wayback Machine	Internet Archive API	Deep crawl	Historical verification
WhichFaceIsReal	v2.4	AI detection mode	Synthetic image detection

Appendix C: Investigation Timeline

Date	Action	Result
May 1, 2025	Initial profile identification	5 suspicious profiles identified
May 2, 2025	Preliminary analysis	Common red flag patterns established
May 3, 2025	Deep technical investigation	Technical evidence collected
May 4, 2025	Cross-platform correlation	No legitimate presence found
May 5, 2025	Report compilation	High confidence determination of fake profiles

END OF REPORT