An Observational Study on the Forensic Recoverability of Deleted Data from Popular Social Media Applications

Kovvuri Dharmitha Sri[1*] Karamsetty Sireesha[2] Neelima Bachalla[3]

[1]M.Sc. Forensic Science, Bundelkhand University, Uttar Pradesh, Jhansi, U.P.-284128, India

[2, 3]Scientific Assistant, Cyber Forensic Section, AP Forensic Science Laboratory, Mangalagiri, A.P.-522503, India

Mail ID's: dharmithakovvuri@gmail.com[1*], ragaprahas@gmail.com[2], 777neelu777@gmail.com[3]

Abstract:

Social media has come to be as an essential source of digital evidence in modern investigations but is also a major platform for Cyber crimes such as online harassment, identity misuse, financial fraud, and misinformation. In many cases, perpetrators attempt to conceal their activities by deleting posts, images, or shared links, thereby complicating the process of evidence recovery. This study examines the quantity of deleted traces that can be retrieved from social media applications by using Magnet AXIOM. The extracted dump was examined to identify residual artifacts, including activity logs, metadata, database fragments, thumbnails and cached media. The results confirm the relevance of artifact analysis and supporting cybercrime investigations.

Keywords: Deleted Data, Magnet AXIOM, Artifacts.

1. Introduction:

Digital communication has become an essential part of our everyday routine, social media platforms growing rapidly and mostly as a result of Smart phones being readily accessible.[1] Social media platforms have an increasing influence on people's interactions, viewpoints, and use of digital data in cultural, social, and psychological contexts.[2] Instant messaging and the creation of digital networks that extend through geographic borders are made possible by apps like Facebook, Twitter/X, Instagram, Threads, Snapchat and Share Chat.[3] Constantly fast internet, friendly interfaces and accessibility of mobile devices have made it possible for social media to influence on public perceptions and collective decisions on an unprecedented extent.[4] Despite all of these advantages, the social media applications increasing influence continues to present Cyber security and digital Forensic experts in issues that are challenging.[5] These social media networks are now important conduits for many cybercrimes, such as financial fraud, phishing, identity theft, harassment, impersonation, cyber bullying and extortion.[6] To conceal their activities and flee Forensic detection, criminals regularly take advantage of anonymity, disappearing messages, and instant content deletions. In an attempt to conceal malicious social activities, users constantly delete posts, stories, conversations and media.[7] Although abandoned artifacts might still be present on the device, this makes it more difficult for investigators to access the original content.[1] The purposeful creation of forged data, fabricated news and manipulated digital content, which has a tendency to promote enmity in society, degrade others or execute toward activities driven by revenge, is a further major problem.[8]

[9]Such content repeatedly reaches thousands of users before verification can take place, spreading extensively across social networks and having both digital and tangible consequences.[8] When content created by users can be easy to produce, modify or distribute, misinformation, targeted bullying and fabricated identity attacks explode on social media. In order to differentiate among authentic input from users information and content that has been altered or fabricated, the Forensic analysis of mobile device artifacts becomes important.[10] Mobile devices always preserve several types of abandoned

D. R. Reddy et al. (eds.), *Proceedings of the First International Conference on Advances in Forensics and Cyber Technologies (ICFACT 2025)*, Advances in Computer Science Research 127,
https://doi.org/10.2991/978-94-6239-610-4_33

evidentiary artifacts, such as cached image thumbnails, metadata, authentication logs, timestamps, URL previews and fragments of local chat databases, despite offenders attempts to remove the evidence.[11] Investigators can reconstruct timelines, authenticate user activity and obtain information about patterns of conduct that are relevant to cyber crime inquiries using with such artifacts.[12] The amount of recoverable deleted content varies across platforms since every social networking program employs a distinct storage architecture, ranging from local caching to data stored in the cloud.[13] Investigators may examine device patterns even after user deletion with the help of modern Forensic tools such as Magnet AXIOM, which allow advanced extractions of mobile devices.[14] Retrieved data, which include thumbnails or fragments of metadata, tend to provide important information to conduct reconstruction, investigative timelines and claim validation in cybercrime cases.[15] The Forensic recoverability of deleted social media data is the primary objective of this study and it further analyses at what number of residual artifacts from commonly adopted applications, that can assist in highly precise digital investigations.

2. Materials and Methods:

The aim is to examine the recoverability of deleted data from Instagram, Facebook, WhatsApp, X, Snapchat, and Share Chat using a controlled environment. Full file system extraction was performed by using Magnet AXIOM, which also extracted cached media and residual artifacts. Airplane mode prevented cloud sync, ensures reliable comparison of internally stored data across 6 social media applications.

2.1. Materials and Software used:

2.1.1. **Device Used:** Android smart phone of 64GB internal storage.

2.1.2. **Software and Tools:** Magnet AXIOM is the primary tool for SQ Lite database analysis, extraction, artifacts and cache recovery.

3. **Social media applications analysed:** (Instagram, Facebook, WhatsApp, X/Twitter, Snapchat, and Share Chat).

To ensure the precise experimentation and reliable recovery of social media artifacts, this study confined to a scientifically valid procedure that included stages and mentioned in Fig. 1.

Fig. 1. Methodology for Forensic Recovery and Analysis of Deleted Social Media Data

The procedure begins with a controlled simulation of user activity, sending messages, uploading images, browsing and sharing media. Then deleting the stored activities among the actions that were intended executed by newly formed test accounts on each of the six social media platforms. This controlled environment ensures that not any sensitive data was accessible and that every application maintained consistent patterns of activity. During each

of these procedures, the device has been placed under a 30-day waiting period to allow for automated application cleanup and natural cache expiry. Then, the device was keptin airplane mode while the waiting period to ensure total isolation, from all network connectivity to avoid cloud syncing or remote changes from altering stored artifacts. Then the acquisition was conducted by using Magnet AXIOM, to identify the residual artifacts, including cached thumbnails, metadata fragments, URL previews, deleted messages and database entries. The extracted dump was further processed to both data analysis and manual examination, in order to find concealed and incomplete artifacts. The procedure concluded with full file system extraction, to verify that any potential source of data was excluded and to allow validation of retrieved data.

4. Results:

The results revealed that each of the 6 social media applications under analysis, observed different amounts of deleted data in the form of residual artifacts. Even though cloud service networks like Instagram, Facebook and Twitter/X were incapable of complete recovery of deleted data, the device still contained residual artifacts, such as cached images, thumbnail previews, database entries, metadata fragments and login logs. Snapchat provided less recoverability because of its data involatile nature, but WhatsApp preserved valuable traces of deleted chats and media through database artifacts. Applications containing an excessive amount of media, like Share Chat created massive cache files that were still accessible long after the perpetrator deleted them from their device.

The following tables i.e., Table 1, Table 2, Table 3, Table 4, Table 5 & Table 6 provides the overview of the recoverable artifacts for each of the 6 social media applications, detailing the existence of deleted data traces found using Magnet AXIOM.

Artifact Category	Recovered Items
Account Information	Username, profile picture (cached), linked email/phone, bio
Login Data	Login timestamps, IP logs, app version
Messages	DM lists, message timestamps, limited deleted fragments
Media	Cached reel thumbnails, viewed story previews, temporary images
Activity Logs	Search history, recently viewed profiles, reel watch history
Deleted Data	Very small fragments (post ID, URL, timestamp)

Table 1. Instagram Artifacts

Artifact Category	Recovered Items
Chat Database	Sent & received messages, timestamps, group metadata
Deleted Data	Deleted messages traces in msgstore.db and WAL files
Media Files	Images, videos, audio notes, document previews
App Data	Encryption keys (Android), backup details
Activity	Status history, contact list

Table 2. WhatsApp Artifacts

Artifact Category	Recovered Items
Account Details	Profile info, profile edits, friend list logs
Login Data	IP logs, device list
Messages	Cached message attachments, timestamps
Activity Logs	Likes, comments, shares, search logs
Deleted Data	Small SQLite fragments

Table 3. Facebook Artifacts

Artifact Category	Recovered Items
Account Information	Username, language settings, profile metadata
Messages	DM lists, message timestamps
Media	Short video cache, images, meme files
Activity Logs	Post history, likes, trending topics viewed
Deleted Content	Limited thumbnail remnants

Table 4. ShareChat Artifacts

Artifact Category	Recovered Items
Account Data	Username, Bitmoji details, linked phone/email
Device Logs	Login timestamps, IP logs
Chats	Saved messages, unopened messages, stickers/GIF metadata
Media	Memories, cached images, thumbnails, story previews
Activity Logs	Search history, friend requests, streak metadata
Deleted Data	Very limited fragments (opened snaps gone)
Location	Snap Map logs (if enabled)

Table 5. Snapchat Artifacts

Artifact Category	Recovered Items
Account Information	Username, handle, cached profile picture
Activity Logs	Liked tweets, retweet logs, search history
Messages (DMs)	Sent/received messages stored on device
Deleted Data	Limited fragments from SQLite caches
Media	Tweet image/video thumbnails, cached media
Browser/WebView Data	Login tokens, cookies, tweet URLs

Table 6. Twitter Artifacts

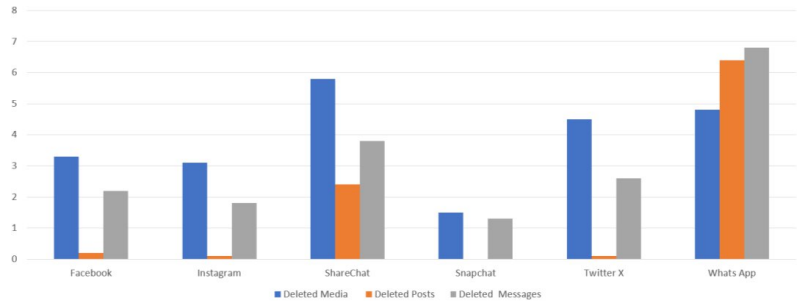

Fig. 2. Recoverability of deleted Social Media Data Depending on Storage

The graph shows how the basic storage system of 6 social media applications impacts on the recoverability of deleted data. Instagram, Facebook, and Twitter(X) are mostly relied on cloud storage. These applications show limited recoverability of deleted posts and messages, leaving only a small number of residual artifacts on the device, including cached thumbnails and other data fragments. On the other hand, applications like WhatsApp and Share Chat which have more emphasis on internal storage on devices exhibit higher recovery potential. Even after the intentional deletion, these platforms store message remains, cache files, and application databases in the device storage. The graph indicates, how social media data storage procedures have impact on the quantity of deleted content that can still recovered and by proving the vitality of specific applications analysis in mobile Forensic investigations.

5. Discussion:

When the results of this study are compared to previous studies on social media Forensics, Riadi and Rafiq (2022) examined the NIST method for examining only two applications, WhatsApp and Instagram. Their study was to examine the effectiveness of Forensic techniques in extracting evidence from these applications, while their work is valuable, it does not compare various platforms or indicate which applications retain more deleted data.[15] But the present study, analyses 6 popular social media applications, including Instagram, Facebook, WhatsApp, Share Chat, Snapchat, and Twitter (X). By examination through all 6 combined, this study offers a more comprehensive and clear explanation of how multiple social media platforms preserve deleted data.

Similarly, Menahil *et al*.'s in their study (2021) examined a number of applications, including Instagram, WeChat, LINE, and Wickr, to see whether any data continues to persist throughout when a user deletes information. Their study has revealed that Forensic instruments can still be used to recover significant evidence. Even so, the existence or absence of data remained was the main objective of their study. They did not provide an entire overall analysis of the different types of evidence that could have been recovered [16] but in present study compared which applications provided stronger or weaker artifacts.

Compared to the prior two studies, The present study analysed the performance of each application during full file system extraction and confirming that artifacts can be recovered as well as Identified Clear differences in cached media, metadata fragments, deleted message and database remains. These outcomes allow investigators in examination of deleted artifacts in social media related crime investigations by assisting them to identify which applications has more likely to provide more credible evidence.

6. Conclusion:

This study clearly proves that different social media applications deleted data differently, some protect important artifacts while others entirely remove traces, on the results of Forensic recovery. Comparing artifacts across 6 social media applications is extremely important because each application uses a different storage architectural design, cached media, metadata fragments and deleted data, which results in large differences in what investigators can recover. These artifacts become important sources of evidence, because it is not always possible to fully recover deleted social media data because of encryption, only cloud storage, automatic cache cleaning, or intentional deletion. By identifying and recording cached media, metadata fragments, URL previews, thumbnails, and message traces in each of the 6 social media applications. This study explains which type of artifacts can still persist even after user remove content. The artifact comparison given in this study can assist investigators in artifact analysis, currently used in Digital Forensics and provides an effective method that law enforcement agencies and Forensic laboratories dealing with social media related Cybercrimes.

References:

1. Al Mutawa N, Baggili I, Marrington A. Forensic analysis of social networking applications on mobile devices. Digital investigation. 2012 Aug 1;9: S24-33.
2. Pasquini C, Amerini I, Boato G.Media Forensics on social media platforms: a survey. EURASIP Journal on Information Security. 2021 May 1;2021(1):4.
3. Majeed A, Zia H, Imran R, Saleem S. Forensic analysis of three social media apps in windows 10. In2015 12th International Conference on High-capacity Optical Networks and Enabling/Emerging Technologies (HONET) 2015 Dec 21 (pp. 1-5). IEEE.
4. Wagler A, Cannon KJ. Exploring ways social media data inform public issues communication: An analysis of Twitter conversation during the 2012-2013 drought in Nebraska. Journal of Applied Communications. 2015;99(2):5.
5. Heinrichs JH, Lim JS, Lim KS. Influence of social networking site and user access method on social media evaluation. Journal of Consumer Behaviour. 2011 Nov;10(6):347-55.
6. Ezeji CL. Emerging technologies and cyber-crime: strategies for mitigating cyber-crime and misinformation on social media and cyber systems. International Journal of Business Ecosystem & Strategy (2687-2293). 2024 Dec 1;6(4):271- 84.
7. Cao Q, Yang X, Yu J, Palow C. Uncovering large groups of active malicious accounts in online social networks. In Proceedings of the 2014 ACM SIGSAC conference on computer and communications security 2014 Nov 3(pp.477- 488).
8. Paulin M, Boon SD. Revenge via social media and relationship contexts: Prevalence and measurement. Journal of Social and Personal Relationships. 2021 Dec;38(12):3692-712.
9. Trninić D, Kuprešanin Vukelić A, Bokan J. Perception of "fake news" and potentially manipulative content in digital media—a generational approach. Societies. 2021 Dec 24;12(1):3.
10. Tyagi AK, Naithani K, Tiwari S. Security and Possible Threats in Today's Online Social Networking Platforms. Online Social Networks in Business Frameworks. 2024 Oct 22:159-99.
11. Ayobami U. Automated Metadata Extraction and Correlation Techniques for Digital Evidence Analysis in Cybercrime Investigations.
12. Chen B, Jia S, Xia L, Liu P. Sanitizing data is not enough! Towards sanitizing structural artifacts in flash media. In Proceedings of the 32nd Annual Conference on Computer Security Applications 2016 Dec 5 (pp. 496-507).
13. Odun-Ayo I, Ajayi O, Akanle B, Ahuja R. An overview of data storage in cloud computing. In2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS) 2017 Dec 11 (pp. 29-34). IEEE.

14. Mehta J, Bhadania Y, Shah P, Prajapati P. Comparative Study of Mobile Forensics Tools: Autopsy, Belkasoft X and Magnet Axiom. In2024 5th International Conference on Electronics and Sustainable Communication Systems (ICESC) 2024 Aug 7 (pp. 1257-1263). IEEE.
15. Riadi I, Rafiq IA. Forensic Mobile Analysis on social media Using National Institute Standard of Technology Method. International Journal of Safety & Security Engineering. 2022 Dec 1;12(6).
16. Menahil A, Iqbal W, Iftikhar M, Shahid WB, Mansoor K, Rubab S. Forensic analysis of social networking applications on an android smartphone. Wireless Communications and Mobile Computing. 2021; 2021(1):5567592.s