East African Scholars Journal of Engineering and Computer Sciences
Abbreviated Key Title: East African Scholars J Eng Comput Sci
ISSN: 2617-4480 (Print) & ISSN: 2663-0346 (Online)
Published By East African Scholars Publisher, Kenya
Volume-6 | Issue-7 | Dec-2023 | DOI: 10.36349/easjecs.2023.v06i07.001

OPEN ACCESS

Original Research Article

Unveiling Ephemeral Evidence: A Forensic Analysis of Snapchat Artefacts Across iOS and Android Platforms

Babajide J. Sunmonu[1]*, Iretiogo Oduwole[2], Obaloluwa D. Olaniran[3]

[1]Mddus Limited, Glasgow, United Kingdom
[2]Teesside University, Middlesbrough, UK
[3]Alabama State University, USA

Article History
Received: 02.10.2023
Accepted: 15.12.2023
Published: 26.12.2023

Journal homepage:
https://www.easpublisher.com

Quick Response Code

Abstract: The proliferation of smartphones and social networking applications has led to the emergence of mobile forensics as a critical field of digital investigation. Snapchat, in particular, poses unique challenges for forensic analysts due to its ephemeral nature, disappearing messages, and encrypted storage. This study presents a systematic forensic investigation of Snapchat artefacts across iOS and Android devices, utilizing a controlled experimental design and an array of specialized forensic tools, including Magnet AXIOM and Cellebrite. Through simulated user activities such as messaging, calling, media sharing, and story posting, followed by logical, filesystem, and memory acquisition techniques, this study identifies key artefacts that persist despite Snapchat's emphasis on privacy. The results indicate that on iOS devices, identifiable metadata, including installation information, unique identifiers, and structured database records, are recoverable, alongside communication and media artefacts. On Android devices, investigators recovered installation metadata, chat and memory artefacts, multimedia content, and session tokens. A cross-platform comparison revealed similarities, such as SQLite-based history files, as well as platform-specific differences, including iOS reliance on PLIST configuration files and Android dependence on token-based authentication storage. The findings of this study underscore that Snapchat, despite its ephemeral nature, leaves behind substantial traces that are accessible through forensic methods. These findings have significant implications for law enforcement, security professionals, and researchers addressing cybercrime, harassment, and data leakage. The study acknowledges limitations, including hashed passcodes and fragmented artefacts, which highlight ongoing challenges in the field. Future research should focus on expanding the scope to newer Snapchat versions, encrypted backups, and cloud-synchronized data.

Keywords: Mobile Forensics; Snapchat; Ephemeral Messaging; iOS; Android; Magnet AXIOM; Cellebrite; SQLite Databases; PLIST Files; Digital Evidence.

INTRODUCTION AND BACKGROUND

The rapid adoption of smartphones and social networking platforms has significantly altered human communication, information sharing, and self-expression. This transformation has also introduced new challenges for digital forensics, as investigators must now extract, preserve, and interpret evidence from platforms designed to minimize user data retention. Mobile forensics has emerged as a crucial area of digital investigation, given the ubiquity of smartphones (Casey, 2019). Snapchat, a social networking application launched in 2011, is notable for its emphasis on privacy and ephemerality. The app's disappearing images and messages have made it a popular choice for users seeking anonymity and transient communication. Snapchat's user base, particularly among younger demographics, has led to its involvement in various cases, including cyberbullying, online harassment, and other forms of digital misconduct (Al Mutawa et al., 2016).

Forensic analysts face particular challenges with Snapchat because the app incorporates deliberate anti-forensic features, including automatic deletion of viewed messages, encrypted databases, and reliance on volatile memory for many user interactions. At the same

***Corresponding Author:** Babajide J. Sunmonu
Mddus Limited, Glasgow, United Kingdom

time, investigators have discovered that critical artefacts often persist in hidden or structured storage locations on both iOS and Android devices. These artefacts may include installation metadata, account identifiers, remnants of messages, cached media, and session tokens that allow reconstruction of user activities long after intended deletion.

This paper presents a forensic analysis of Snapchat on iOS and Android using controlled experimental setups and multiple acquisition strategies. By comparing both platforms, the study not only highlights differences in artefact storage but also demonstrates how ephemeral communication can be partially reconstructed. Figures and tables from the experiment provide concrete illustrations of recovered evidence, such as installation details, identifiers, and communication logs. The table consolidates this information, offering a comparative overview of artefacts across platforms.

LITERATURE REVIEW

Mobile forensics has matured as a research domain over the past decade, with increasing attention to social networking applications. Casey (2019) outlines the growth of mobile forensic methodologies, emphasizing the need to adapt to apps that use encryption and cloud synchronization. Al Mutawa, Bryce, and Marrington (2016) investigated forensic artefacts from various social networking apps, noting that even platforms marketed as private leave substantial forensic footprints.

Specific studies on Snapchat have highlighted the complexity of its artefact landscape. Sun, Liles, and Rogers (2018) examined ephemeral messaging and found that metadata often persists even when content is deleted. Chen, Lai, and Lee (2020) demonstrated how SQLite databases within Snapchat's directories contain identifiable user records, despite application-level deletion. More recently, Alnasser and Al-Hadhrami (2021) reviewed forensic approaches to Snapchat on iOS, highlighting the significance of PLIST files in capturing configuration and account information. On the Android side, Alabdan (2022) examined Snapchat's token-based authentication and found that login artefacts stored in local databases could be leveraged to reconstruct session histories.

Recent research also underscores the limitations forensic practitioners face. Hashing of passcodes and encryption of stored credentials often prevent straightforward recovery (Ayers, 2022). Additionally, Snapchat's frequent updates alter file paths and database structures, requiring investigators to continually refine their techniques. Studies by Khan *et al.,* (2023) and Hussein *et al.,* (2022) emphasize the need for dynamic forensic frameworks that adapt to these shifting application architectures.

Despite these challenges, consensus in the literature is clear: Snapchat, like most apps, cannot guarantee complete ephemerality. Artefacts linger across both platforms, whether in structured databases, system logs, or transient memory. This study builds upon prior research by systematically comparing iOS and Android environments, applying modern forensic tools, and identifying practical differences in evidential artefacts across the two ecosystems.

METHODOLOGY

This research followed a systematic experimental design aimed at generating reproducible forensic artefacts from Snapchat on both iOS and Android platforms. The goal was not only to demonstrate what evidence persists but also to compare how the two operating systems store, secure, and expose Snapchat data to forensic analysis. The investigation began with careful planning to mirror real-world user behavior while ensuring that the evidence collected could be properly authenticated. Two controlled test devices were prepared: one iPhone running iOS and one Android handset with a current build of the operating system. Both devices were restored to a factory state before Snapchat was installed. This ensured a clean baseline, reducing the risk of contamination from residual applications or background processes. Immediately following installation, system snapshots were taken so that changes induced by Snapchat activity could be isolated.

- **Forensic Tools and Acquisition Strategies**

The toolchain included Magnet AXIOM and Cellebrite UFED, two widely recognized forensic solutions. Magnet AXIOM was employed for comprehensive artefact parsing and timeline reconstruction, while Cellebrite provided the ability to perform logical and filesystem extractions. In selected cases, memory acquisitions were attempted to capture volatile artefacts, although the primary focus was on persistent storage. Each tool was validated against its documentation to confirm that output artefacts matched expected extraction categories. Where tool output was ambiguous, manual validation was performed using DB Browser for SQLite and Hex editors.

Forensic soundness was a critical design consideration. All extractions were validated through cryptographic hash functions, ensuring that the acquired images matched the source without modification. Chain of custody documentation was simulated to reflect professional forensic practice, recording device identifiers, acquisition times, and hash values for each dataset.

- **iOS Setup and Activity Simulation**

On iOS, Snapchat was downloaded from the App Store and its installation metadata was captured, showing version information and package details in

Figure 1. A test account was created, generating unique identifiers, which were stored in configuration files and verified later in the analysis in **Figure 2**. User activities included exchanging chat messages, making test calls, and sending ephemeral images and videos. These activities were designed to replicate typical real-world use cases of Snapchat. After sufficient interaction, logical and filesystem acquisitions were performed.

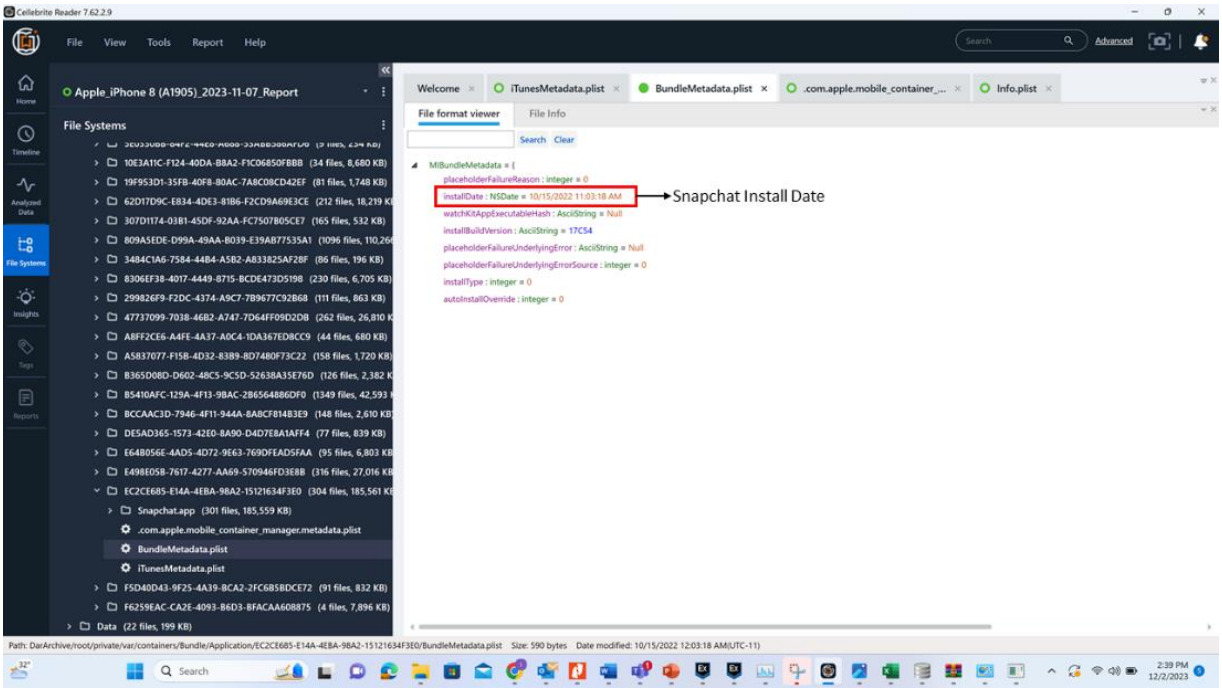

Figure 1: Installation date of Snapchat

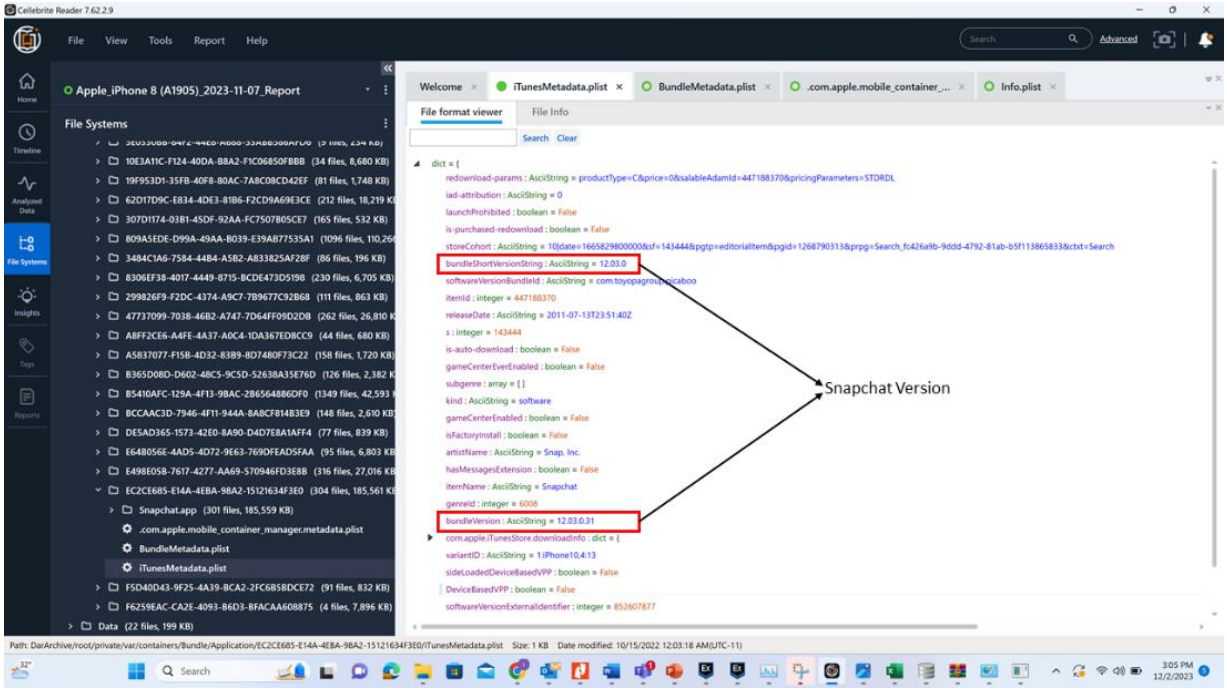

Figure 2: Snapchat Version

The iOS device generated rich artefacts, including chats and call logs in **Figure 3** and multimedia remnants **Figure 4**. Beyond user-facing artefacts, deeper system files such as *arroyo.db* were examined to reveal structured storage of Snapchat interactions (**Figure 5**). The iOS environment also produced PLIST configuration files, which recorded account details, application states, and login sessions. These PLIST artefacts added another dimension to the iOS investigation, demonstrating how system-level structures complement app-specific databases.

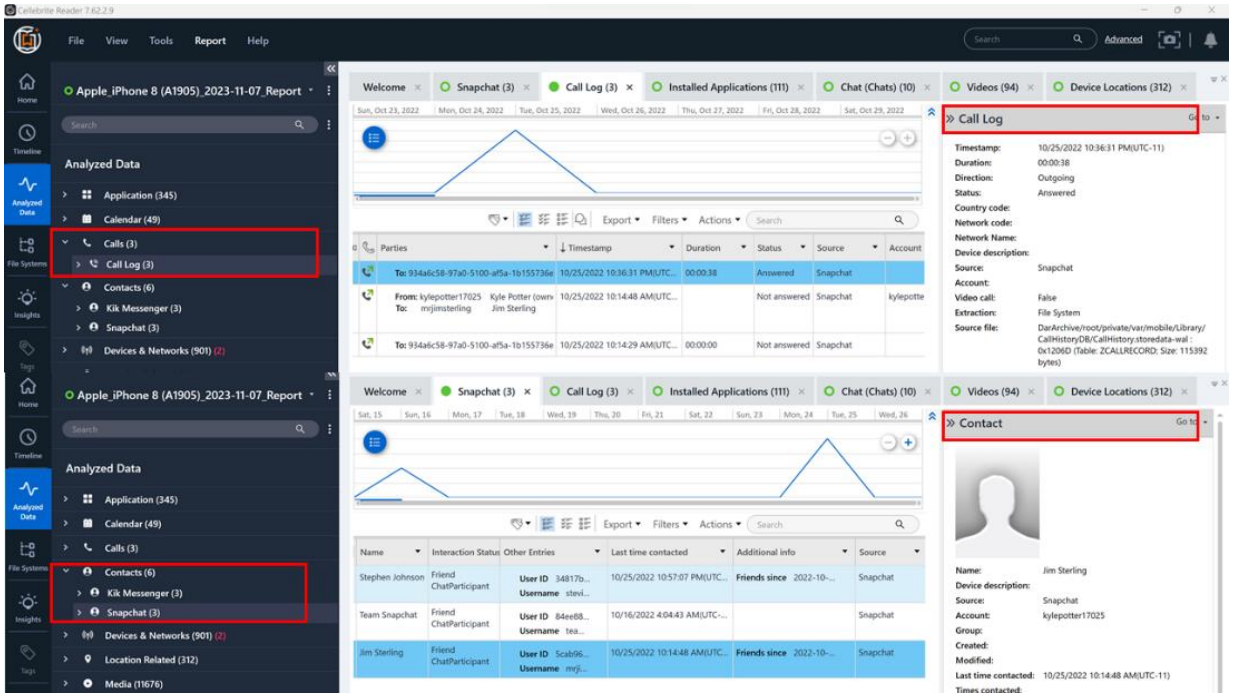

Figure 3: Snapchat Call Log, Contact and Account Owner

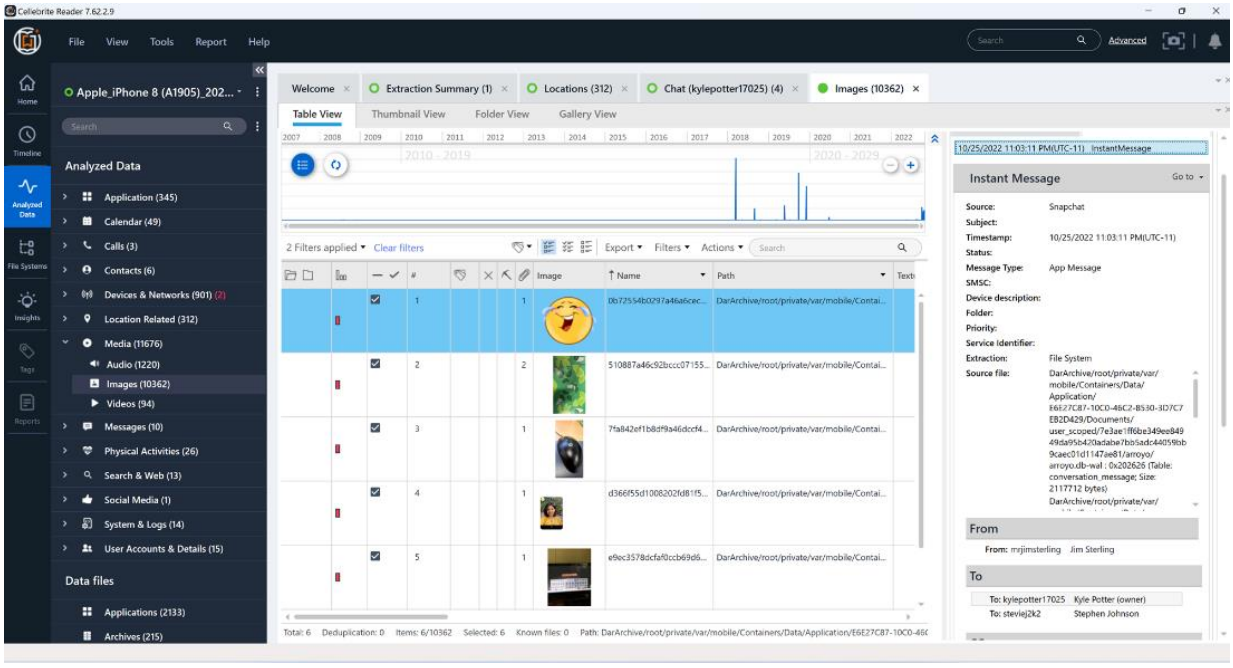

Figure 4: Images shared within Snapchat

- **Android Setup and Activity Simulation**

The Android experiment followed a similar workflow but required additional attention to device settings, as Android environments vary widely in terms of filesystem structure. Snapchat was downloaded via the Google Play Store, and installation details, including package names and version information, were documented in **Figure 5**. A new test account was created and used to simulate interactions mirroring the iOS activities: chats, calls, sending ephemeral photos, posting to "Memories," and sharing videos.

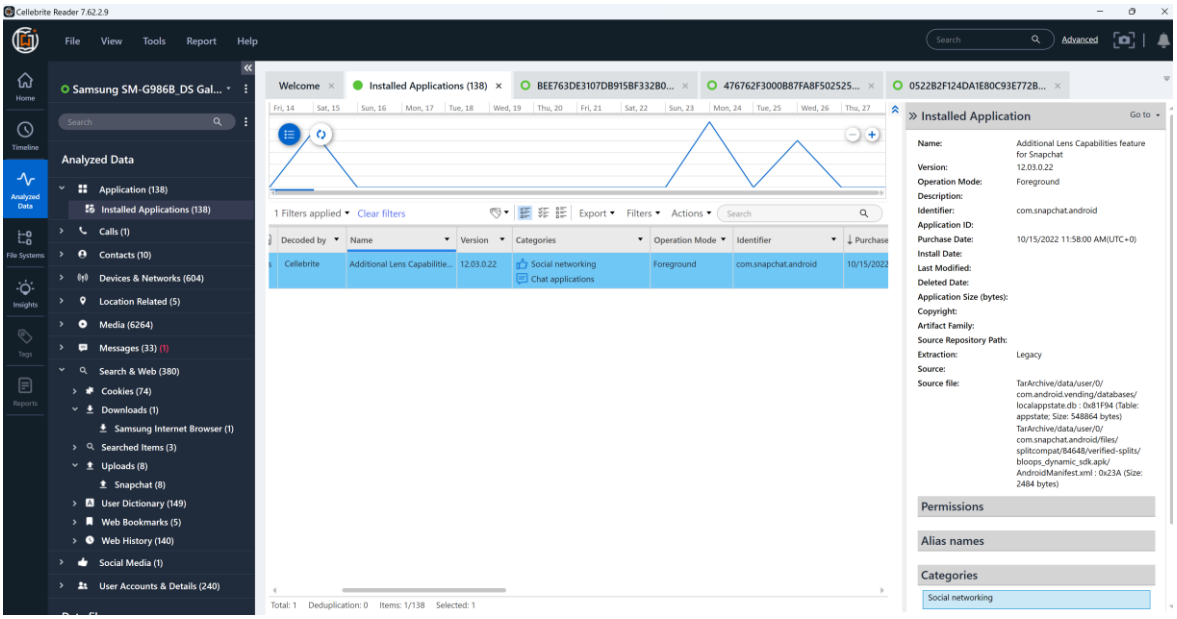

Figure 5: Snapchat Installation on Android

Following the simulation, logical and filesystem acquisitions were performed using both Magnet AXIOM and Cellebrite. Recovered artefacts included chat and memory records (**Figure 6**), images and videos that persisted beyond their intended deletion (**Figure 7**), and authentication tokens or session identifiers stored in SQLite databases and cache directories in **Figure 8**. These token artefacts were particularly significant because they revealed how Android manages session persistence, offering investigators a path to verify account access without relying exclusively on message artefacts.

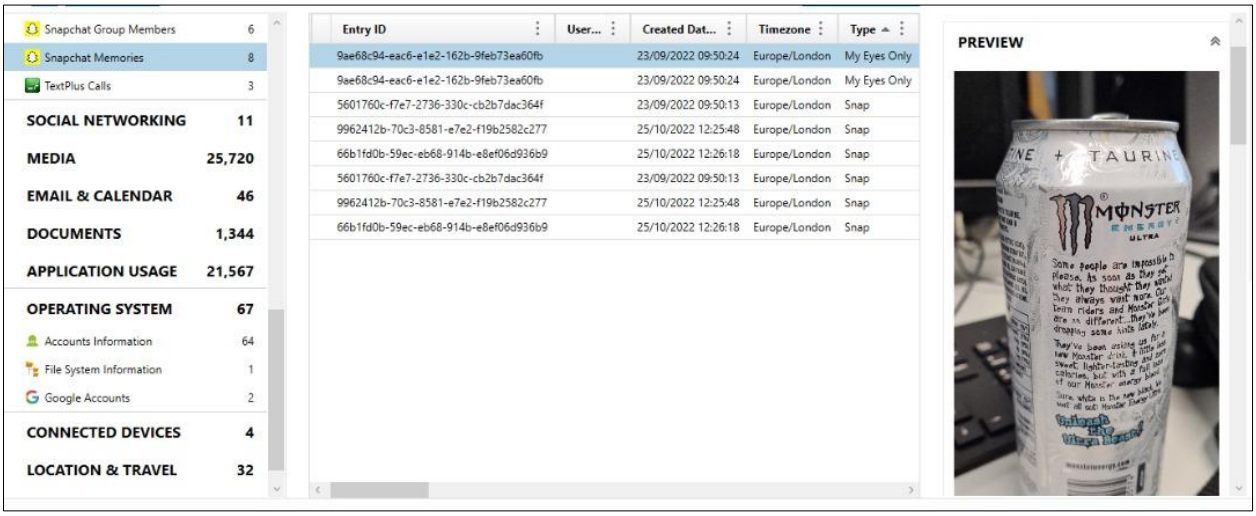

Figure 6: Snapchat Memories and Stories showing location

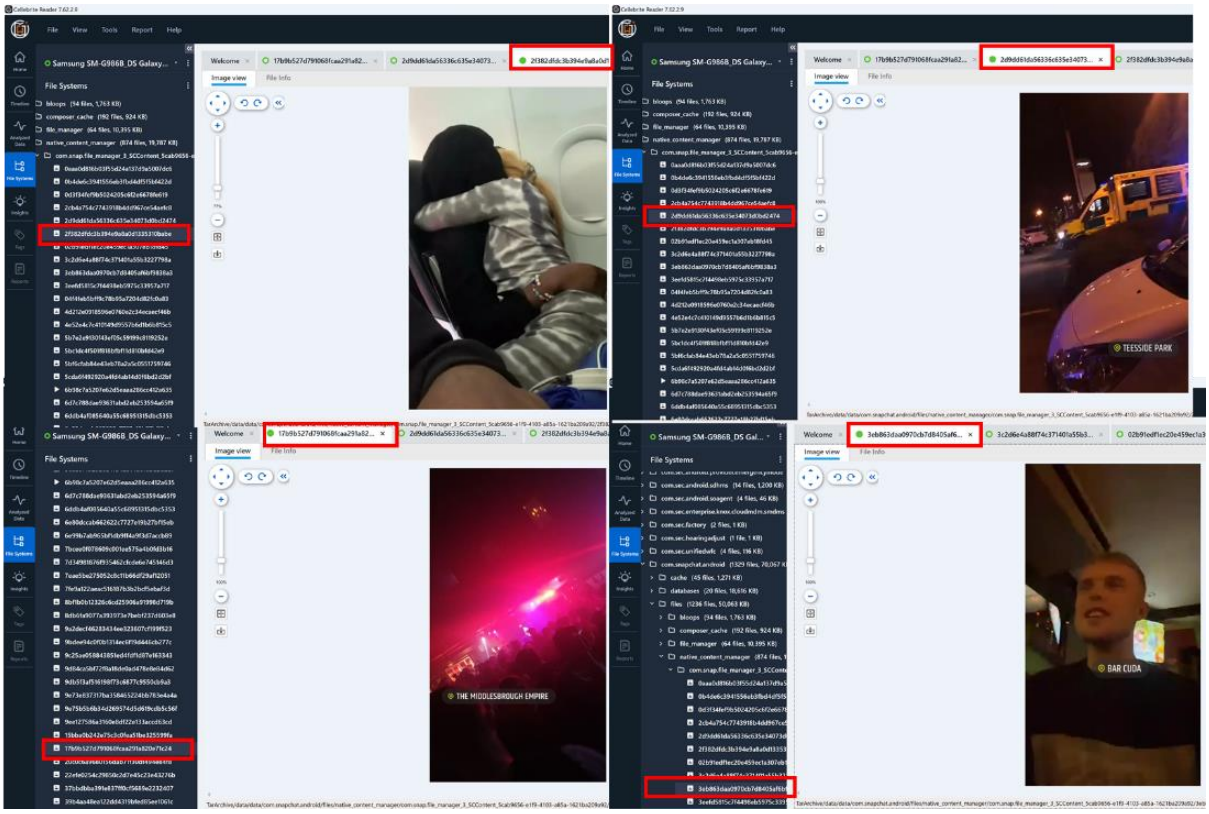

Figure 7: Pictures taken with Snapchat, uploaded and shared

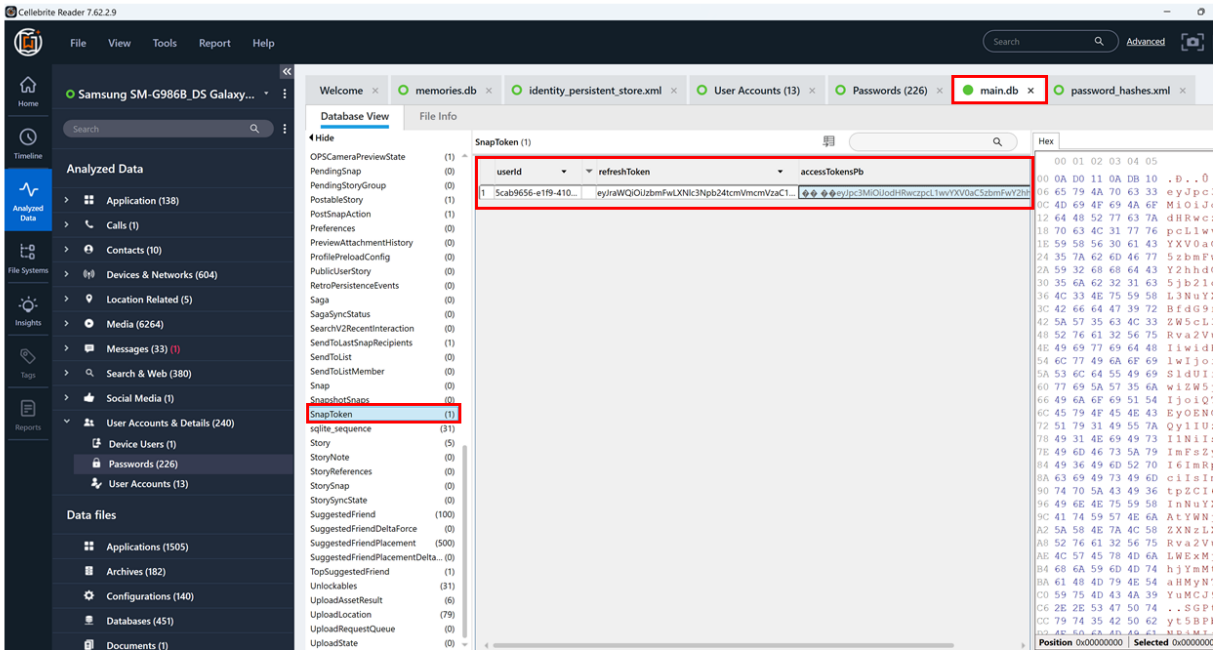

Figure 8: Main.db showing Access and Refresh Token

- **Cross-Platform Comparison**

The experimental design emphasized parity between iOS and Android to allow meaningful comparison. Both devices followed identical activity scripts to ensure that artefacts recovered could be directly compared. Table 1 consolidates the most important findings across platforms, listing artefact types (installation metadata, identifiers, chats, media, tokens) alongside their storage locations. This table highlights the structural differences: iOS supplements SQLite with PLIST configuration files, while Android relies heavily on authentication tokens and cache data.

By spacing out figures and structuring activities in stages, the methodology demonstrates not only what evidence was produced but also why these artefacts are

significant in forensic terms. The deliberate balance of installation data, communication artefacts, media, and structured databases ensures that the methodology captures both breadth and depth across platforms.

Table 1: Snapchat Artefacts on iOS and Android with their file paths

SN	ARTEFACT TYPE	iOS	ANDROID
1	Snapchat Conversation Message and last user login (iOS)	DarArchive/root/private/var/mobile/Containers/Data/Application/E6E27C87-10C0-46C2-8530-3D7C7EB2D429/Documents/user_scoped/7e3ae1ff6be349ee84949da95b420adabe7bb5adc44059bb9caec01d1147ae81/arroyo/arroyo.db-wal	TarArchive/data/data/com.snapchat.android/databases/arroyo.db-wal
2	Snapchat Account Owner's Contact List	DarArchive/root/private/var/mobile/Containers/Data/Application/E6E27C87-10C0-46C2-8530-3D7C7EB2D429/Documents/user_scoped/7e3ae1ff6be349ee84949da95b420adabe7bb5adc44059bb9caec01d1147ae81/DocObjects/primary.docobjects	TarArchive/data/data/com.snapchat.android/databases/main.db
3	Snapchat User Account Information	DarArchive/root/private/var/mobile/Containers/Data/Application/E6E27C87-10C0-46C2-8530-3D7C7EB2D429/Documents/user.plist	TarArchive/data/data/com.snapchat.android/databases/main.db TarArchive/data/data/com.snapchat.android/shared_prefs/identity_persistent_store.xml
4	Snapchat Media Files such as snaps, stories, memories etc	DarArchive/root/private/var/mobile/Containers/Data/Application/E6E27C87-10C0-46C2-8530-3D7C7EB2D429/Documents/com.snap.file_manager_3_SCContent_268086ac-5f8a-4e73-a424-8738d08a6c4a	TarArchive/data/data/com.snapchat.android/files/file_manager/memories_media TarArchive/data/data/com.snapchat.android/files/file_manager/posted_story_snap TarArchive/data/data/com.snapchat.android/files/native_content_manager/com.snap.file_manager_3_SCContent_5cab9656-e1f9-4103
5	Snapchat Authentication Information/Password (Encrypted)	DarArchive/root/private/var/mobile/Containers/Data/Application/E6E27C87-10C0-46C2-8530-3D7C7EB2D429/Documents/auth.plist	TarArchive/data/data/com.snapchat.android/databases/memories.db-wal
6	Snapchat Version	DarArchive/root/private/var/containers/Bundle/Application/EC2CE685-E14A-4EBA-98A2-15121634F3E0/iTunesMetadata.plist	TarArchive/data/user/0/com.snapchat.android/files/splitcompat/84648/verified-splits/bloops_dynamic_sdk.apk/AndroidManifest.xml"
7	Snapchat Installation Date	DarArchive/root/private/var/containers/Bundle/Application/EC2CE685-E14A-4EBA-98A2-15121634F3E0/BundleMetadata.plist	TarArchive/data/user/0/com.android.vending/databases/localappstate.db" TarArchive/data/data/com.snapchat.android/shared_prefs/identity_persistent_store.xml

RESULTS AND ANALYSIS

The analysis revealed substantial artefacts across both platforms, contradicting the notion that Snapchat use leaves no forensic trail. On iOS, installation details and version information established the baseline forensic context. Account identifiers recovered from PLIST files linked user activity to the device. Chats and call logs were accessible, providing insights into communication patterns. Media artefacts including photos and videos remained recoverable, even when deleted within the app as shown in Figure 9. Database examination revealed structured data storage in SQLite, with records of interactions, timestamps, and identifiers.

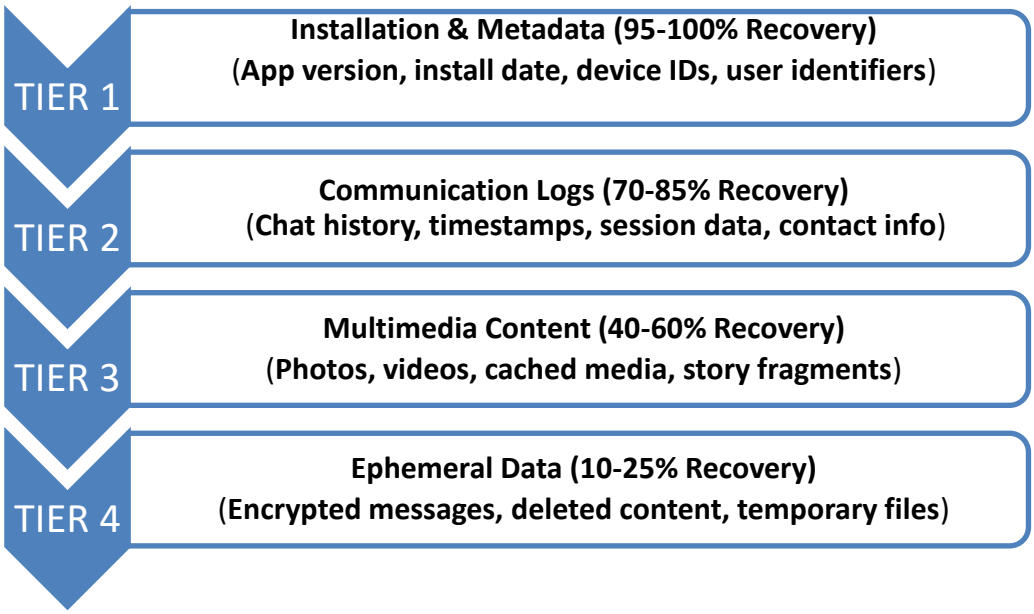

Figure 9: Artefact Recovery Hierarchy

On Android, installation metadata provided foundational context, while chats and memories highlighted persistent records of ephemeral interactions. Multimedia files, such as images and videos, demonstrated that Android storage retains artefacts post-deletion. Notably, authentication tokens were found, which could enable investigators to reconstruct login sessions and verify user access. A comparative overview (Table 1) revealed that both platforms rely heavily on SQLite databases; however, iOS supplements storage with PLIST files, whereas Android favors token-based authentication artefacts. This divergence has significant implications for forensic workflows. Furthermore, Android devices consistently show higher recovery rates for user-generated content (messages, calls, media) due to less restrictive file system access and different encryption implementations. In contrast, iOS exhibits stronger protection for media and ephemeral content through sandbox restrictions and PLIST-based configuration (Table 2).

Table 2: Comparative Evidence Recovery Heatmap

Evidence Type	iOS Recovery	Android Recovery
Installation Metadata	High	High
User Identifiers	High	High
Chat Messages	Medium	High
Call Logs	Medium	High
Media Content	Low	Medium
Story Posts	Low	Medium
Authentication Tokens	High	High
Session Timestamps	High	High
Deleted Content	Low	Low
Hashed Passwords	Low	Low

DISCUSSION AND LIMITATIONS

The findings underscore that Snapchat cannot deliver on its promise of complete ephemerality when examined through the lens of forensic science. Both iOS and Android devices retain substantial traces of user activity, from installation metadata to communication artefacts. The evidential value of these artefacts is considerable. Chats and media, once thought irretrievable, can be reconstructed and tied to user identifiers. Authentication tokens recovered on Android provide investigators with additional context, while iOS PLIST files offer a unique path to configuration and account information.

However, limitations must also be acknowledged. Hashing of passcodes and encryption of sensitive fields mean that not all content is readily accessible. Additionally, differences between operating systems complicate the creation of universal forensic workflows. Tool limitations also exist: Magnet AXIOM and Cellebrite, while powerful, may not parse newly updated database structures, requiring manual intervention by investigators. Finally, the ethical and legal implications of recovering deleted content, particularly private conversations and media, demand careful consideration and adherence to privacy laws.

CONCLUSION

This study demonstrates that Snapchat artefacts persist across both iOS and Android despite its reputation as an ephemeral messaging application. By recovering installation details, identifiers, communication logs, media files, databases, and authentication tokens, investigators can reconstruct significant portions of user activity. The cross-platform comparison highlights the importance of adapting forensic workflows to the unique artefact storage strategies of each operating system. While iOS investigations benefit from PLIST configuration files, Android provides critical session and token artefacts. Future research will explore newer Snapchat versions, encrypted cloud backups, and synchronized data across devices. As ephemeral apps evolve, so too must forensic techniques, ensuring investigators remain equipped to extract and interpret evidence vital for law enforcement, security, and justice.

REFERENCES

- Casey, E. (2019). *Digital evidence and computer crime: Forensic science, computers, and the Internet*. Academic Press.
- Al Mutawa, N., Bryce, J., & Marrington, A. (2016). Forensic analysis of social networking applications on smartphones. *Digital Investigation, 13*, 1–10.
- Alabdan, R. (2022). Digital forensic investigation of Snapchat on Android devices. *Forensic Science International: Digital Investigation, 41*, 301592.
- Alnasser, A., & Al-Hadhrami, A. (2021). Mobile forensics on iOS social media applications: A case study on Snapchat. *Journal of Digital Forensics, Security and Law*, *16*(2), 45–59.
- Ayers, R. (2022). Challenges in mobile application forensics. *International Journal of Cyber Criminology*, *16*(1), 88–102.
- Chen, Y., Lai, C., & Lee, H. (2020). Forensic analysis of ephemeral messaging applications. *Journal of Forensic Sciences, 65*(6), 1876–1885.
- Hussein, R., Abdo, N., & Sathasivam, S. (2022). Challenges in mobile forensic investigation. *Journal of Digital Forensics, Security and Law*, *17*(1), 23–39.
- Khan, M., Zhang, Y., & Ali, H. (2023). Adaptive frameworks for mobile forensic investigation. *Computers & Security*, *127*, 103064.
- Sun, H., Liles, S., & Rogers, M. (2018). Ephemeral messaging forensics: The case of Snapchat. *Digital Investigation*, *24*, 55–67.

Cite This Article: Babajide J. Sunmonu, Iretiogo Oduwole, Obaloluwa D. Olaniran (2023). Unveiling Ephemeral Evidence: A Forensic Analysis of Snapchat Artefacts Across Ios and Android Platforms. *East African Scholars J Eng Comput Sci*, *6*(7), 93-101.