Journal of Computing & Biomedical Informatics Volume 11 Issue 01
ISSN: 2710 - 1606 2026

Research Article
https://doi.org/10.56979/1101/2026/1406

Forensic Correlation of WhatsApp View-Once Video Artifacts with Device-Resident Source Media Using SQLite Metadata Analysis

Abdullah Afzal Raja[1]

[1]Punjab Forensic Science Authority, Lahore, 53700, Pakistan.
*Corresponding Author: Abdullah Afzal Raja. Email: abdullah.afzal@pfsa.gop.pk

Received: March 08, 2026 **Accepted:** May 30, 2026

Abstract: Privacy-oriented messaging features such as WhatsApp view-once media introduce significant challenges for mobile forensic investigations by limiting user-side visibility and complicating direct artifact attribution. This study presents a forensic correlation framework for linking a transmitted WhatsApp view-once video artifact with a candidate device-resident source video recovered from a Unisoc-based ZTE Z2350 smartphone following physical extraction. Direct examination of the recovered msgstore.db database enabled identification of the target message record and associated media metadata, including file attributes, logical storage paths, and a surviving thumbnail BLOB. Because platform-induced transcoding altered file size and resolution, direct hash equivalence was not feasible. Instead, correlation was established through structured comparison of duration, format consistency, temporal and chat-context relevance, and visual similarity between the recovered thumbnail and visible video frames. The results demonstrate that reliable attribution of WhatsApp view-once multimedia remains achievable with high forensic confidence despite expected media transformation during transmission. These findings highlight the evidentiary importance of relational SQLite analysis and metadata-driven attribution strategies in investigations involving privacy-preserving messaging features.

Keywords: WhatsApp forensics; view-once media; mobile device forensics; SQLite database analysis; multimedia correlation; metadata attribution; Android forensics; ephemeral messaging

1. Introduction

WhatsApp artifacts continue to hold significant evidentiary value in mobile forensic investigations because the application routinely mediates the exchange of images, videos, voice notes, and other user-generated content. Earlier forensic studies established that Android-resident WhatsApp artifacts stored in SQLite databases and associated media repositories can be correlated to reconstruct message chronology, delivery state, and user interaction patterns [1], [2]. These foundational works demonstrated that meaningful evidentiary reconstruction often depends on interpreting relationships between message records and associated media metadata rather than relying on isolated artifacts.

Recent platform developments have shifted forensic attention toward privacy-preserving communication features, particularly disappearing messages and ephemeral multimedia. Prior work has shown that despite application-level deletion semantics, endpoint artifacts frequently remain recoverable through local databases, notification records, cache remnants, or residual storage structures [3]–[6]. This evidentiary persistence is especially relevant in modern investigations where transient communication mechanisms are increasingly used to reduce traceability.

A parallel challenge arises from platform-level media transformation. Messaging applications routinely apply compression, transcoding, and metadata stripping during media transmission, resulting in substantial changes to file size, embedded metadata, and cryptographic hashes [7], [8]. As a

consequence, direct hash-based comparison between a transmitted media artifact and a candidate source file stored elsewhere on the device may no longer be reliable, even when both originate from the same recording event. This limitation is significant in practical investigations, particularly when examiners attempt to associate transmitted ephemeral media with locally stored device content.

The present study addresses this gap through a real-device case investigation involving a WhatsApp view-once video artifact recovered from msgstore.db and a candidate source video recovered from device storage following physical extraction of a Unisoc-based ZTE Z2350 handset. Rather than relying on direct file-hash equality, correlation was established through SQLite-derived media metadata, including duration consistency, MIME-type alignment, file-size transformation patterns, and thumbnail-assisted visual validation. Additional device-resident contextual artifacts were considered during temporal consistency assessment. The findings demonstrate that reliable linkage of WhatsApp view-once multimedia can be achieved with strong forensic confidence even when application-level transcoding prevents direct binary equivalence [9].

2. Materials and Methods

This study follows a structured digital forensic methodology involving acquisition, preservation, and analysis of artifacts extracted from a mobile device. All procedures were conducted in a controlled forensic environment to ensure evidentiary integrity and reproducibility.

2.1. Device and Acquisition

The examined device was a ZTE Z2350 smartphone based on a Unisoc chipset. A physical extraction of the handset was performed using Oxygen Forensic Detective, which provided direct access to the device's userdata partition and enabled recovery of the live WhatsApp application database in plain SQLite format (msgstore.db), rather than an encrypted backup container. This allowed immediate database examination without requiring a separate decryption workflow. The extraction also recovered device-resident multimedia artifacts relevant to the investigation. All subsequent examinations were conducted on verified forensic working copies to preserve the integrity of the original evidence.

2.2. Tools

Post-acquisition examination was conducted on verified forensic working copies. The extracted msgstore.db database was analyzed using DB Browser for SQLite, an open-source SQLite viewer selected for structured query execution and direct table inspection. The tool was used exclusively in a read-only analytical workflow on the working copy to preserve evidentiary integrity.

2.3. SQLite Database Analysis

The recovered msgstore.db database was examined through direct SQL querying of the message, message_media, and message_thumbnail tables. The message of forensic interest was first identified through the contextual information provided by the investigating officer and corroborative review of the relevant WhatsApp chat conversation. Once the target outgoing view-once video message was established within the chat context, focused SQL queries were applied to extract associated metadata fields, including message identifiers, timestamps, transmission status, media duration, MIME type, logical file path references, thumbnail identifiers, and media file names.

A representative query structure used to retrieve the metadata associated with the identified message is shown below:

```
SELECT m.key_id, mm.file_name, mm.mime_type, mm.media_duration, mt.thumbnail
FROM message m
JOIN message_media mm ON m._id = mm.message_row_id
LEFT JOIN message_thumbnail mt ON m.key_id = mt.key_id
WHERE m.key_id = ?;
```

2.4. Correlation Methodology

A metadata-driven correlation approach was employed to evaluate linkage between the transmitted WhatsApp view-once video artifact and the candidate device-resident video. Because application-level

transcoding and compression alter binary structure and invalidate direct hash equivalence [6], [7], correlation was established using the following attributes:

- Media duration
- MIME type and container consistency
- transformed file-size relationship
- temporal consistency between creation and transmission
- thumbnail-assisted visual similarity

These attributes were jointly assessed to establish reliable linkage between the transmitted artifact and the candidate source media with strong forensic confidence.

3. Results

3.1 Identification of View-Once Media Artifact

Analysis of the WhatsApp database revealed a message record corresponding to a view-once video. The message was identified based on its message type and associated metadata. Key attributes extracted from the database are summarized in Table 1.

Table 1. Metadata of View-Once Message.

Parameter	Value
Message ID	A54AF1239E86DA2B499C0BBD6F750D96
Direction	Outgoing
Message Type	43 (View-once video)
Timestamp	18-Nov-2025 21:39:55
Delivery Status	Delivered
Duration	12 seconds
MIME Type	video/mp4
File Size	~1.83 MB

3.2 Media Metadata Associated with the View-Once Record

Further examination of the message_media and message_thumbnail tables revealed the media metadata associated with the identified view-once message. The recovered record confirms the presence of a transmitted MP4 video artifact together with a surviving thumbnail BLOB entry. Key metadata extracted from the joined tables are summarized in Table 2.

Table 2. Media metadata associated with the identified view-once message.

Parameter	Value
Message ID	A54AF1239E86DA2B499C0BBD6F750D96
Media File Name	789661be-659f-4923-8933-b69e54c001ff.mp4
Logical File Path	/data/user/0/com.whatsapp.w4b/files/ViewOnce/VID-20251118-WA0057.mp4
MIME Type	video/mp4
File Size	1,925,754 bytes (~1.83 MB)
Duration	12 seconds
Resolution	478 × 850
Thumbnail Artifact	BLOB present

The recovered metadata confirms that the transmitted artifact was stored as a video/mp4 object within WhatsApp's dedicated ViewOnce directory structure. The presence of a surviving thumbnail BLOB within the SQLite database further demonstrates residual visual artifact persistence despite the view-once transmission semantics.

3.3 Candidate Source Video Metadata

A candidate source video was identified within the device storage at /Data/media/0/DCIM/Camera/ and selected for comparative analysis based on temporal relevance and matching media characteristics. Key metadata extracted from the file are summarized in Table 3.

Table 3. Key metadata of the candidate source video recovered from device storage.

Parameter	Value
File Name	VID_20251115_093102.mp4
File Path	/Data/media/0/DCIM/Camera/VID_20251115_093102.mp4
Format	MP4
File Size	19.1 MB
Duration	12 seconds
Resolution	1920 × 1080
Video Codec	H.264
Audio Codec	AAC
Creation Timestamp	2025-11-15 04:31:02 UTC

The identified candidate video exhibits strong metadata consistency with the transmitted WhatsApp artifact in terms of duration and container format, while also demonstrating expected differences in file size and resolution attributable to platform-level transcoding and downscaling during transmission. In addition, the embedded creation timestamp is temporally consistent with the reported timeline of the incident under investigation, further strengthening the evidentiary relevance of the candidate source file.

3.4 Correlation of the WhatsApp Artifact with the Candidate Source Video

A structured comparison was performed between the metadata of the transmitted WhatsApp view-once artifact (Table 2) and the candidate source video identified in device storage (Table 3). The comparison focused on the attributes defined in the correlation methodology, namely duration, format consistency, temporal alignment, file-size transformation, and resolution scaling.

Table 4. Correlation matrix between the WhatsApp view-once artifact and the candidate source video.

Attribute	WhatsApp Artifact	Candidate Video	Correlation Assessment
Container / MIME	video/mp4	MP4	Format-consistent
Duration	12 s	12s	Consistent
File Size	1.83 MB	19.1 MB	Expected reduction after transcoding
Resolution	478 × 850	1920 × 1080	Expected reduction after transcoding
Temporal Relevance	Transmission timestamp consistent with case timeline and chat context of message exchange between the accused	Creation timestamp consistent with case timeline	Strong temporal and contextual alignment
Thumbnail / Visual Similarity	Transmission timestamp consistent with case timeline and chat context of message exchange between the accused	Visual comparison of thumbnail and visible video frames	Supportive visual consistency

4. Discussion

The findings demonstrate that WhatsApp view-once media can retain substantial evidentiary value despite the application's privacy-oriented presentation semantics. Consistent with prior work on disappearing and ephemeral messaging artifacts [3], [4], residual metadata persisted within msgstore.db,

including message identifiers, transmission timestamps, MIME information, file-size attributes, logical storage paths, and a surviving thumbnail BLOB. These artifacts enabled reconstruction of the transmitted media event even though the message was designed for limited visibility.

A key contribution of this study is the demonstration that reliable attribution of a transmitted ephemeral video remains feasible even when direct binary equivalence is not available. The substantial reduction in file size and resolution observed between the WhatsApp artifact and the candidate device-resident video is consistent with known messaging-platform transcoding and metadata transformation behavior [6], [7]. Rather than treating these expected transformations as disqualifying differences, the present results show that duration consistency, format alignment, temporal relevance, bilateral chat context, and visual thumbnail comparison collectively provide a stronger and more practically defensible correlation framework.

The SQLite-centric workflow used in this study also extends prior WhatsApp forensic database analyses [8], [9] by demonstrating that view-once media correlation can be achieved through structured linkage of records across the message, message_media, and message_thumbnail tables. This reinforces the forensic importance of relational database interpretation rather than isolated artifact recovery, particularly in modern versions of WhatsApp where encrypted backup containers and privacy-preserving features increasingly complicate traditional evidence recovery.

A practical limitation of the present study is that the correlation process relies on examiner-guided interpretation of contextual and visual consistency, particularly in the absence of exact hash equivalence. However, this limitation reflects real-world investigative conditions and aligns with contemporary forensic practice, where platform-induced transcoding necessitates metadata-driven attribution strategies. Future research may explore automated similarity scoring based on thumbnail extraction, visual frame comparison, and the incorporation of forensic image and facial comparison techniques to further standardize correlation confidence assessment.

5. Conclusion

This study demonstrates that reliable forensic linkage between a WhatsApp view-once video artifact and a device-resident candidate source video can be established through structured correlation of SQLite metadata, contextual message evidence, and visual consistency indicators, even when platform-induced transcoding prevents direct hash equivalence. The findings highlight the evidentiary importance of relational analysis across WhatsApp database tables and support the broader use of metadata-driven attribution strategies in investigations involving privacy-preserving messaging features.

Data Availability Statement: The data supporting the findings of this study are derived from a real forensic case and contain sensitive evidentiary material. To protect case confidentiality and privacy obligations, the underlying data are not publicly available. De-identified metadata excerpts relevant to the reported findings may be made available from the corresponding author upon reasonable request and subject to institutional and legal restrictions.

Ethical Considerations: All case-specific identifiers and personally sensitive contextual details were excluded or abstracted to preserve confidentiality and protect the integrity of the underlying investigation.

Conflicts of Interest: The author declares no conflict of interest.

References

1. C. Anglano, "Forensic analysis of WhatsApp Messenger on Android smartphones," Digital Investigation, vol. 11, no. 3, pp. 201–213, 2014, doi: 10.1016/j.diin.2014.04.003.
2. D. Walnycky, I. Baggili, A. Marrington, J. Moore, and F. Breitinger, "Network and device forensic analysis of Android social-messaging applications,"Digital Investigation vol. 14, Suppl. 1, pp. S77–S84, 2015, doi: 10.1016/j.diin.2015.05.009.
3. H. Heath, Á. MacDermott, and A. Akinbi, "Forensic analysis of ephemeral messaging applications: disappearing messages or evidential data?," Forensic Science International: Digital Investigation, vol. 46, p. 301585, 2023, doi: 10.1016/j.fsidi.2023.301585.
4. D. Sudiana, C. H. Nuruddin, M. Rizkinia, and D. Husna, "Forensic analysis of WhatsApp disappearing message on unrooted Android using mobile device forensics methodology NIST SP 800-101r1," Evergreen, vol. 11, no. 1, pp. 516–524, 2024, doi: 10.5109/7172316.
5. M. Azhar, A. R. Onik, J. Brown, C. Walker, and I. Baggili, "Forensic analysis of ephemeral messaging applications on mobile devices," International Journal on Advances in Security, vol. 13, no. 1–2, 2020.
6. N. Soni, "Forensic value of Exif data: an analytical evaluation of metadata integrity across image transfer methods," Perspectives in Legal and Forensic Sciences, vol. 2, p. 10006, 2025, doi: 10.70322/plfs.2025.10006.
7. H. Studiawan, A. M. Islami, and A. M. Shiddiqi, "Forgery classification on compressed images from social networks to assist forensic analysis," Discover Computing, vol. 28, p. 331, 2025, doi: 10.1007/s10791-025-09825-6.
8. H. Fayyad-Kazan, S. Kassem-Moussa, H. J. Hejase, and A. J. Hejase, "Forensic analysis of WhatsApp SQLite databases on the unrooted Android phones," HighTech and Innovation Journal, vol. 3, no. 2, pp. 175–195, 2022, doi: 10.28991/HIJ-2022-03-02-06.
9. W. A. Prabowo, F. Mohsen, and S. R. Selamat, "WhatsApp Mobile Applications in the Lens of Digital Forensics: Deciphering the Msgstore.db.crypt14 File," Journal of Cyber Security and Mobility, vol. 14, no. 4, pp. 823–848, 2025, doi: 10.13052/jcsm2245-1439.1443.