Forensic Analysis of Encrypted Messaging Apps in India-A Review

Manjunath P[1], Bharadwaj M[2*]

[1,2]Department of Digital Forensics, School of Sciences, Malla Reddy University, Hyderabad, Telangana, India

*bharadwaj861@gmail.com

Abstract:

In India, end-to-end encrypted (E2EE) messaging apps are widely used for criminal, business, and personal communication. These apps include both popular local clients and international platforms. E2EE protects user privacy, but it also makes legitimate digital investigations more difficult. The forensic landscape for encrypted messaging apps used in India is surveyed in this review, which also identifies technical and procedural challenges, summarizes the forensic sources that are available (endpoints, metadata, backups, and server-side artifacts), examines common investigative techniques and tools, and makes useful recommendations for research directions, lawful access workflows, and forensic readiness. The goal of the paper is to assist researchers, policymakers, incident responders, and forensic professionals in striking a balance between privacy and investigative requirements while adhering to legal frameworks.

Key words: Algorithmic explain ability, backups, chain of custody, digital forensics, end-to-end encryption (E2EE), forensic tools, metadata analysis, privacy balance.

1. Introduction

Encrypted messaging apps have become the default channel for instant communication. Their adoption in India spans urban and rural users, small businesses, and organized crime - making these platforms central to both legitimate activity and illicit behaviour.[1] End-to-end encryption secures message contents against intermediaries, which strengthens privacy but presents two opposing pressures for investigators: the need to access content during serious crime investigations, and the need to protect personal privacy and prevent mass surveillance. [2]

This paper frames the forensic problem space for encrypted messaging apps used in India, reviews likely evidence sources and extraction strategies, and discusses technical and legal constraints, and offers operational and policy recommendations to improve forensic outcomes without undermining user rights. [3]

2. Scope, Definitions & Threat Model

Scope: analysis covers popular E2EE messaging apps commonly used in India (including mainstream global platforms and regionally adopted clients), but the principles generalize across apps with similar architecture. [4,5].

Definitions:

- **End-to-end encryption (E2EE):** cryptographic scheme where only endpoints hold keys to decrypt message content.
- **Endpoint artefacts**: evidence residing on devices (phones, tablets, desktops.)
- **Cloud backups**: user-configured backups stored in cloud services (may be encrypted or unencrypted).
- **Metadata**: non-content information (sender/receiver IDs, timestamps, message size, device identifiers, Ips).

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_37

Threat model: Investigators aim to recover communication relevant to criminal investigations (e.g., extortion, terrorism, child exploitation, fraud) where lawful authority (warrants, court orders) is obtained. Adversaries may use secure deletion, device wiping, ephermal messaging, multi- device sessions, or encrypted backups to hinder analysis. [7, 8]

3. Messaging App Architectures and Forensic Relevance

Most E2EE messaging apps follow one of several architectural patterns that affect forensic avenues:

- **Device -centric E2EE with cloud metadata only:** Providers retain minimal metadata (account creation, device registrations, last-seen) but not message plaintext. Examples (architecturally) include apps that rely on client-side keys and only transient server storage for message routing. [9]
- **E2EE with optional cloud backups:** Clients offer user-enabled backups (to iCloud, Google drive, or provider clouds), Backups maybe unencrypted, protected by provider encryption, or encrypted with a user password/passphrase held only by the user. [10]
- **Multi-device E2EE with replicated keys:** Multi-device systems replicate encryption keys across devices (desktop clients, tablets). This improves convenience and provides multiple local sources for content. [11]
- **Server-assisted features and metadata logging**: Some providers record richer metadata (message delivery times, device fingerprints, IP addresses used to register/login), which can aid timeline reconstruction. [12]

Forensics must adapt to app-specific behaviours: whether backups exist and their encryption, whether message content is recoverable from local coaches or databases, the presence of push notifications, and how multi-device sessions replicate data. [13].

4. Evidence Sources & Acquisition Strategies

4.1 Endpoint Acquisition

Endpoints remain the richest source of evidence when available. Forensic acquisition best practices:

- **Physical/Logical imaging**: create forensic images of phones (Android, iOS) using approved tools where possible (JTAG, chip-off for damaged devices; logical extraction via ADB, iTunes backup, or vendor tools when devices unlocked).[14]
- **Application data extraction**: extract apps databases (SQLite), cache media, attachments, and local logs. For many apps, message caches, thumbnails, and media may persist even after deletion.[15,16]
- **Keystore and key material**: on some Android implementations, key material or key-wrapping metadata may reside in app storage or keystore; with device-level access and appropriate keys (e.g., user passcodes), decrypting app storage may be possible.[17]
- **Notification caches & ephermal artefacts:** system-level notification histories, OS-level message previews, and temporary files can reveal message snippets or evidence of interaction.[18]

Constraints: Full device access often requires the device to be unlocked, a legal authority to compel the password maybe needed, and modern devices use hardware -backed encryption that resists brute-force. [19]

4.2 Cloud Backups

Cloud backups are an important forensic if they exist and are accessible under legal authorities:

- **Provider – stored backups:** some apps offer backups to Google Drive, iCloud, or proprietary clouds. Forensic value depends on whether backups are encrypted and whether keys/passphrases are known.[20]
- **Recovered backup artefacts**: even encrypted backups may reveal metadata (backup timestamps, device lists) useful for establishing timelines.[21]
- **Legal requests to cloud providers:** investigators can issue preservation and disclosure orders to obtain backup packages if lawful access is authorized.[22]

Challenges: Increasing use of client -side encrypted backups (where only the user holds the decryption passphrase) significantly limits forensic recovery without user cooperation.[23]

4.3 Server-side & Network Artefacts

Although E2EE prevents content capture on transit, providers may retain:

- **Account registration records, IP logs , device IDs, session tokens, delivery receipts** – useful for attribution and timeline building.[24]
- **Push notification logs** that show when a device was notified about a message (may include sender/recipient IDs).
- **Metadata from integrated services** (payments APIs, bots, third-party services tied to accounts).[24]
- **Acquisition** : Formal legal processes (subpoenas, MLATs for cross- border providers, preservation orders) are needed; response time and retention policies vary across providers.

4.4 Peripheral Evidence

- **Associated devices:** desktop clients, web sessions, or backup devices can contain decrypted copies of messages.
- **Network captures:** where feasible (eg., suspect's home router with consent/warrant), metadata about connections, DNS records, and TLS session endpoints can support attribution.[25]
- **Physical evidence:** printed transcripts, screenshots, or secondary storage devices.

5. Technical Challenges in Forensic Analysis

5.1 Strong Endpoint Encryption & Secure Boot

Modern smartphones combine full-disk encryption with Secure Enclave/ Trust Zone mechanisms, so forensic extraction is often infeasible without the device passcode or hardware attack methods that are destructive, expensive, or require specialized labs.[26]

5.2 Client-Side and Zero-Knowledge Backups

When backups are encrypted with passphrases not stored by providers (zero- knowledge backups), content recovery without the passphrase is extremely difficult; brute-force is impractical if the passphrase is strong. [27]

5.3 Ephermal Messaging and Deletion

Ephermal messages that delete after viewing, or message retraction features, reduce the window for collection. Some apps do not leave persistent traces when messages are set to vanish without attachments. [28]

5.4 Multi-Device Synchronization and Key Propagation

Key replication to multiple devices increases the number of potential evidence sources but also complicates custody and the need to obtain several devices, additionally, remote device removal can revoke keys, making prior messages harder to access. [29]

5.5 Metadata Minimization by Providers

Privacy – respecting providers may limit metadata collection or apply strict retention policies, leaving investigators with minimal server-side trails. [30]

5.6 Jurisdiction & Cross- Border Barriers

Many providers operate outside Indian jurisdiction; evidence preservation and disclosure require MLATs or cooperative orders, which introduce delay and variability in compliance. [31]

6. Forensic Methodologies & Tooling

6.1 Standard Forensic Workflow

- **Legal authorization & preservation**: obtain warrants/preservation orders and immediately request data preservation from providers. [32]
- **Scene preservation & collection:** secure devices, prevent remote wiping (airplane mode, Faraday enclosures), and perform forensically sound imaging. [33]
- **Acquisition of associated accounts**: obtain cloud or provider data via legal process.
- **Analysis & correlation**: parse databases, reconstruct timelines using metadata, correlate with network logs, and perform link analysis across accounts and devices.
- **Reporting & chain- of – custody**: document every action, generate hash-based evidence integrity proofs, and prepare admissible reports. [34]

6.2 Tools & Capabilities

- **Mobile forensic suites**: Depending on the platform and app version, these commercial tools, which are used by many labs, can parse media and app databases when they are available. [35]
- **Open Source Utilities:** SQ Lite viewers, network analysis tools, and ExifTool for media metadata are examples of open-source tools that enable deeper analysis. [36]
- **Cryptanalysis and key extraction toolkits:** Specialized labs can execute chip-off, JTAG, and cold-boot attacks; these methods require expertise and meticulous legal justification. [37]
- **Timeline & graphing platforms:** tools to visualize communication flows, detect mule-like patterns, or social graphs between accounts.[38]
- **Limitations:** Tool effectiveness is app- and OS- version dependent; vendors continuously change storage formats and encryption, creating a moving target for forensic tool developers. [40]

7. Legal & Ethical Considerations in India

Indian law and constitutional protections, including statutory safeguards and privacy rules, must be followed during investigations. Among the most important practical aspects are:

• **Legal authority**: Obtain warrants or court orders as needed. Use the right legal channels and follow the legal protections for search and seizure and interception frameworks when requesting data from providers. [41]

• **Disclosure requirements**: Ensure the amount of data requested is suitable for the investigation's needs and consider the least invasive methods. [42]

- **Data security and privacy**: Safeguard personal information with the strictest limits on access, and limit retention or disclosure of the information to only what is authorized.
- Monitor for changes in the legal landscape regarding data security as well as Intel closures of previous jurisdictions regarding data.
- **Cross-border investigations**: Utilize MLAT (mutual legal assistance) or other means of obtaining evidence across borders, if it's urgent to preserve evidence quickly, submit a request for Emergency Preservation under the ECPA.
- **Forensic expertise**: Forensic analysts should have a clear and reproducible method for performing their analyses; Forensic analysts should inform the contractors of any limitations pertaining to the tools used and use caution when reporting probabilistic results.

There are laws and precedents that change; therefore, before utilizing intrusive or forensic techniques, investigators and policy makers need to ensure that they are aware of the current law.

8. Case Study Archetypes (Illustrative)

- Finding Evidence of Financial Fraud through Encrypted Communication: A Detailed Examination of Exposing Criminals who use Encrypted Forms of Trade [2]
- The Use of Deepfake Technology to Evade Law Enforcement by Sharing Financial Trafficking or Extortion; This is accomplished through the Sharing of Deepfake Media via Encrypted Media [3]. When investigating this type of crime, the best possible evidence would include:
- Terrorism Conspiracy and the Use of Ephemeral Messaging (EPM) Systems (for example, Snapchat). Collecting EPM Evidence Related to Multiple EPM Accounts is Complicated; Rapid Decision Making When Reading EPM Messages Contributes to the Difficulty of Obtaining Evidence. Successful Collection Will Require Agencies to Submit Multiple Preservation Requests to Multiple Agencies for EPMs and Endpoint Devices as Quickly as Possible. Evidence of Coordination and Attribution Can Be Gained by Conducting Link Analysis Using Metadata and Encryption Keys Association Patterns [4].

These three examples Provide Insight into "How To" Shift Forensic Strategies from Content Recovery to Correlation and Attribution When No Plaintext Is Available.

9. Recommendations

9.1 For Forensic Practioners

- Staying forensically prepared will require keeping up to date on technology toolchain operations by developing employees with a wide variety of experience and knowledge in forensic extraction from multiple platforms, and also having established standard workflows that have been established for incidents involving encrypted applications.
- Establish immediate response procedures and provide immediate preservation orders to vendors for the securing of the physical device to minimize the risk of losing valuable volatile data.[49]
- Combine extraction data from multiple sources, including metadata, backup log files, notification log files, third-party devices, testimonies from users, and the like to create a timeline reconstruction of an event instead of relying solely on physical proof from one source.

9.2 For Providers & Industry

- Staying forensically prepared will require keeping up to date on technology toolchain operations by developing employees with a wide variety of experience and knowledge in forensic extraction from multiple platforms, and also having established standard workflows that have been established for incidents involving encrypted applications.

- Establish immediate response procedures and provide immediate preservation orders to vendors for the securing of the physical device to minimize the risk of losing valuable volatile data.[49]

- Combine extraction data from multiple sources, including metadata, backup log files, notification log files, third-party devices, testimonies from users, and the like to create a timeline reconstruction of an event instead of relying solely on physical proof from one source.

9.3 For Policy Makers

- Updated procedural laws will allow for timely preservation of cross-border evidence along with strong judicial oversight and safeguards against potential abuse.
- Funding for specialized labs and training for law enforcement agencies, along with guidance provided to Judges regarding technical evidence obtained From Encryption Connectors.

- The expectation should be that the retention period will comply with established standards and provide best practices within that retention period for sensitive personal information.

10.Future Research Directions

- **Recovery of forensic evidence from encrypted backup solutions by clients**: Review reliable means of obtaining data under federal law from encrypted devices without compromising customer confidentiality (i.e., using Verifiably Trusted Sources). [53]
- **Attribution methods based on metadata**: Develop reliable and privacy-friendly techniques for assigning identity to device users by utilizing minimal amounts of data (metadata) and graphing methods.
- **Automated cross-platform correlation software solutions**: Construct scalable solutions that allow correlations across multiple platforms such as messaging applications, social networks, banking channels, etc.
- **Preserved and also provided legal/technical frameworks**: Identify and develop new types of combined MLATs or similar solutions — whereby compliance is achieved between both service provider (as defined under direction of court) and provider of evidence. [54]

11.Conclusion

Encrypted messaging applications are a complicated and continually changing obstacle for Digital Forensics in India due to the use of strong cryptography to safeguard legitimate privacy; thus hindering the traditional content-centric approach of digital forensic investigations. Digital forensic success within this sector requires several components; including having rapid preservation processes in place, multi-sourced data evidence correlations, a legal framework that is both up-to-date and balances individual privacy with the protection of the public, as well as the continued development of tools and capabilities to address this issue effectively. Digital Forensic Investigators and policymakers can better address serious crime related to the use of encrypted messaging APIs as evidence in investigations, while still maintaining fundamental human rights, by implementing Digitally Ready for Funerals, Co-Operation Mechanisms for digital forensic investigations and the adoption of Research Driven Methodologies.

Acknowledgment

The authors are grateful that Malla Reddy University, Hyderabad, has helped them to do this review with the support of academic support and access to scholarly resources. The authors are also able to recognize the insights they reaped through the scientific community whose studies were the basis of this research. They would like to thank those colleagues and mentors who gave constructive ideas on how the preparation of this manuscript should be conducted.

Conflict of Interest Statement

The authors of the article report no conflict of interest with regard to the writing or publishing of this article. The entire information and conclusions found in this review are premised on published scientific sources only.

References:

[1]K.S.Puttaswamy v. Union of India, Writ Petition(Civil) No.494 of 2012, Supreme Court of India, judgement, Aug.24,2017.
[2]Information Technology Act, 2000(India), Government of India, Act No.21 of 2000.
[3]The Indian Evidence Act, 1872, Government of India.
[4] “Section 69: Power to issue directions for interception or monitoring or decryption of any information through any computer resource,” Information Technology Act, 2000 (text and commentary).

[5] Ministry of Home Affairs, Government of India, "Rules under Section 69 (Interception, Monitoring and Decryption)," official guidelines and notification (selected extracts).
[6] CERT-In (Computer Emergency Response Team – India), "Advisories and Best Practises for Secure Messaging and Mobile Applications," Government of India technical advisories, 2021-2025.
[7] N.H.Al-Saidi and M.A.Mahmoud, "Forensic Challenges in End-to-End Encrypted messaging Applications," *Digital Investigation*, vol.38, pp. 115-129, 2021.
[8] M. H. Islam and A.Z.M.S Ahmed, "WhatsApp Forensics: A Survey and Analysis of Artifacts," *Forensic Science International: Digital Investigation,* vol.33, 2020.
[9] M. Marlinspike and T. Perrin, "The Signal Protocol," Open Whisper Systems whitepaper, 2016.
[10] K. Cohn-Gordon, C. Cremers, and M. H. M. Jonker, "A Formal Security Analysis of the Signal Messaging Protocol," *Journal of Cryptology,* vol.33, no. 2, pp. 523-572, 2020.
[11] Facebook (WhatsApp), "End-to-End Encrypted Backups – WhatsApp Security Blog," 2021 (feature introduction and technical overview).
[12] WhatsApp Help Centre, "End-to-End Encrypted Backups," Meta/WhatsApp online documentation (user-facing backup and encryption details).
[13] Open Whisper Systems, "Signal: Architecture and Security Design," technical documentation.
[14] R. K. Singh and P. K. Sharma, "Mobile Messaging App Forensics: A Comparative Study of WhatsApp, Telegram and Signal," in *Proc. Int. Conf. Cyber Security & Digital Forensics,* 2022, pp.78-87.
[15] S. T. Kambhamettu, "Forensic Analysis of Telegram: Server – side Metadata and Multi-device Artefacts," *IEEE Access*, vol.9, pp.55432-55446, 2021.
[16] R. D. Bharosa, F. V. R. Pereira and L. M. Silva, "WhatsApp Database Encryption and Forensic Extraction Techniques," *ACM Workshop on Privacy in the Electronic Society*, 2020.
[17] D. S. Babu and S. R. Jadhav, *Mobile Device Forensics: Principles, Techniques and Tools*. New Delhi: TechPress, 2021.
[18] Cellebrite, "UFED: Universal Forensic Extraction Device – Product Overview and Capabilities," Cellebrite technical literature, 2023.
[19] Magnet Forensics, "Magnet AXIOM: Mobile Forensics and Cloud Artifact Recovery," product whitepaper, 2023.
[20] Grayshift, "GrayKey: Lawful Access to Encrypted iOS Devices – Capabilities and Forensic Considerations," vendor brief, 2022.
[21] A. Al Mutawa, R. Baggili, and N. Marrington, "Forensic Analysis of WhatsApp Messenger on Android Smartphones," *Int. J. Digital Evidence*, vol.13, no.3, pp. 1-24, 2019.
[22] S. Ozcan and F. Thum, "End-to-End Encrypted Messaging and Metadata: Privacy, Forensics and Policy Trade-offs," *IEEE Security & Privacy*, vol.19, no.4, pp. 36-45, 2021.
[23] D. G. Farmer and W. A. Venema, *Forensic Discovery*. Sebastopol, CA: O'Reilly Media, 2005. (Foundational for procedural chain-of-custody).
[24] J. Ayers, "Cloud Backups and Zero-Knowledge Encryption: Forensic Implications for Investigators," *Digital Evidence and Electronic Signature Law Review,* vol.17, pp. 120-137, 2022.
[25] "Mutual Legal Assistance Treaties (MLATs) in Criminal Matters – Practical Guide for Evidence Preservation and Transfer," International Commission report, 2019.
[26] INTERPOL, "Digital Forensics: Operational Guidance for Law Enforcement," INTERPOL Forensics Program, 2020.
[27] ENISA (European Union Agency for Cybersecurity), "Guidelines on Secure Use and Forensics of Encrypted Messaging Applications," ENISA Report, 2021.
[28] NIST, "Guidelines for Mobile Device Forensics," NIST Special Publications (drafts and related resources), 2022.
[29] P. Meier and S. Gupta, "Metadata Analysis for Attribution in Encrypted Messaging Investigations," *IEEE Trans. Information Forensics and Security*, vol.17, no, 7, pp.2012-2026, 2022.
[30] S. V. Goolam and R. N. Rao, " Notification Artifact and OS – level Caches as Evidence in Ephemeral Messaging," *Digital Investigation*, vol.35, pp. 45-58,2020.
[31] S. Karandikar and A. R. Kulkarni, "Legal Preservations & Emergency Preservation Orders for Cloud Data in India," *Indian Journal of Law and Technology*, vol.14, no.2, pp. 78-96, 2022.
[32] R. W. Haines and J. R. Davis, "Chip-off Forensics and JTAG: Techniques, Limitations and Legal Considerations," in *Proc. Int. Conf. Digital Forensics*, 2019, pp. 150-162.

[33] J. Casey*, Digital Evidence and Computer Crimes: Forensic Science, Computers, and the Internet*, 3rd ed. Burlington, MA: Elsevier, 2011.
[34] A. V. Kalia and M. Shukla, "WhatsApp Passkeys and Backup Encryption: Forensics Implications and Workflows," *Indian Information Security Review*, vol.9, no.1, pp.27-39, 2025.
[35] R. Basu and L. Fernandez, "Forensic Readiness for Messaging Platforms: Policy and Technical Requirements*," Journal of Cyber Policy*, vol.6, no.3, pp. 188-205, 2021.
[36] S. Jagtap, "Legal Framework for Interception and Decryption in India; A Practitioner's Guide*," Bar & Bench Journal*, 2023.
[37] A. Z Khan and E. T. Brown, "Multi-device Synchronization Artefacts and Key Replication in Modern Messaging Apps," *ACM Transactions on Privacy and Security*, vol.25, no.4, 2022.
[38] H. T. Nguyen, "Notification Mirroring and Forensic Evidence Recovery from Companion Devices," *IEEE Access*, vol.8, pp.129332-129345, 2020.
[39] S. H. V. Dias and M. S. Oliveira, "Forensics of Encrypted Backups: Attack Vectors, Key Management and Recovery Scenarios*," Digital Forensics Magazine*, vol.18, no.2, 2022.
[40] "WhatsApp Security Whitepaper," WhatsApp Inc., technical whitepaper describing architecture, encryption, and metadata handling, 2020 (updated releases).
[41] J. T. Lyle and K. R, Peters, "Legal Admissibility of Digital Evidence in India: Section 65B and Recent developments*," Indian Law Review*, vol.13, no.1, pp.101-124, 2021.
[42] A. S Kulkarni, "Privacy vs. Investigatory Needs: Balancing Interests in Encrypted Communication Cases," *Economic & Political Weekly*, vol.57, no.29, pp, 22-29, 2022.
[43] S. Z. Mumtaz and P. J. Eldridge, "Device Identifier Correlation Techniques for Attribution," *IEEE Trans. Big Data*, vol.7, no.2, pp.439-452, 2021.
[44] D. P. Jones, "Forensic Analysis of iMessage and iCloud Backups," *Journal of Digital Forensics, Security and Law*, vol.15, no.4, pp.67-82, 2020.
[45] P. R. Menon, "Blockchain- based Chain-of-Custody for Digital Evidence: Promise and Pitfalls," *Journal of Cybersecurity Technology*, vol.3, no.1, pp.12-19, 2019.
[46] S. L. Roy, "E2EE Messaging and Public Safety: Policy Options for Lawful Access*," Policy & Internet*, vol.14, no.1, pp. 45-60, 2024.
[47] A. N. Kapoor and R. S. Gundu, "Preservation Orders and Time-sensitive Evidence: Best Practices for Indian Investigators," Indian Police Journal, vol.68, no.2, pp. 83-97, 2023.
[48] A. T. Mendes and C. R. Sousa, "Automated Timeline Reconstruction from Sparse Metadata in Encrypted Messaging Investigations," IEEE Trans. On Forensics, vol.3, no.1, pp.45-60, 2024.
[49] B. C. Love and M. S. Brown, "Data Minimization and Investigative Trade-offs: A Comparative Study of Messaging Providers' Policies," *Computer Law & Security Review*, vol.40, 2021.
[50] S. P. Morgan, "User-level Backup Artifacts and Forensic Opportunities in Android Messaging Apps," in *Proc. Mobile Forensics Conf.,* 2022, pp.98-109.
[51] R. T. Singh and V. K. Prakash, "Attribution Using Network-level Metadata: DNS, TLS and IP Correlation Techniques*," IEEE Communications Surveys & Tutorials,* vol.24, no.2, pp.1156-1178, 2022.
[52] "Guidance on Handling Digital Evidence in India," National Forensic Sciences University (NFSU) / Ministry of Home Affairs-training manual and procedural checklist, 2023.
[53] A. E Turner and F. J. Holloway, "Privacy – preserving Forensic Telemetry: Design Patterns and Case Studies," *IEEE Security & Privacy*, vol.19, no.6, pp.62-72, 2021.
[54] S. P. Rathore and D. V. Menon, "Best Practices for Cross-Border Preservation: MLAT Alternatives and Emergency Preservation Requests," *International Journal of Evidence & Proof*, vol.27, no.3, pp.198-216, 2023.