JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 09 Issue 02
2025

Research Article
https://doi.org/10.56979/902/2025

Challenges of Data Extraction from Facebook & WhatsApp Applications

Imran Manzoor[1], Rizwan Ghani[1*] and Khalid Hamid[2]

[1]Department of Computer Science and IT, Superior University Lahore, 54000, Pakistan.
[2]Faculty of Computer Science and IT, Superior University Lahore, 54000, Pakistan.
[*]Corresponding Author: Khalid Hamid. Email: khalid6140@gmail.com

Received: May 30, 2025 **Accepted:** July 25, 2025

Abstract: The increasing reliance on social media platforms like Facebook and WhatsApp in both personal and criminal activities presents critical challenges for digital forensic investigators. This research addresses the problem of data extraction from these applications due to factors such as end-to-end encryption, proprietary data structures, frequent app updates, and legal/privacy restrictions. our goal is to identify the key technical, legal, and procedural obstacles involved in extracting and analyzing data from Facebook and WhatsApp and to propose effective methodologies to overcome them. A qualitative research methodology will be employed, incorporating case study analysis of criminal investigations, forensic tool evaluations, and expert insights from digital forensic professionals. The expected results include a classification of the primary extraction challenges, a comparative analysis of current forensic tools, and recommendations for best practices in handling such data. The significance of this study lies in its potential to enhance the effectiveness of digital investigations, contribute to the development of more efficient forensic tools, and inform law enforcement agencies and policymakers about the limitations and possibilities in social media data extraction.

Keywords: Digital Forensics; Social Media; Data Extraction; End-to-End Encryption; Legal and Privacy Issues; Criminal Investigations

1. Introduction

Social media is everywhere today. Applications like WhatsApp and Facebook have become integral parts of daily life, enabling billions of people worldwide to communicate instantly, share photos and videos, and maintain social connections across geographical boundaries. These platforms have revolutionized the way information is exchanged, making communication faster, more interactive, and accessible to nearly everyone. The ease and ubiquity of these technologies, however, have also created opportunities for misuse. Criminals exploit the very same platforms that empower ordinary users, engaging in illegal activities such as cyberbullying, fraud, drug trafficking, financial scams, and even coordinating acts of terrorism. This dual-use nature of social media creates a pressing challenge: how can law enforcement agencies and digital forensic experts effectively extract evidence from platforms like Facebook and WhatsApp to investigate and prosecute criminal activity while also respecting individuals' privacy and the platforms' security policies? The increasing use of strong encryption, jurisdictional barriers, and inconsistent cooperation from platform providers makes digital evidence collection complex and sometimes incomplete. This research explores these issues, focusing specifically on the challenges of data extraction from Facebook and WhatsApp applications, and proposes ways to address these challenges in a way that balances justice with privacy. Social media platforms have evolved far beyond tools for casual social interaction. Criminals now use them strategically to conceal their activities and evade detection. WhatsApp's end-to-end encryption and Facebook's massive user base make these platforms particularly attractive for illegal activities. For example, encrypted messaging on WhatsApp allows criminals to exchange sensitive information without

fear of interception, while Facebook enables the rapid dissemination of illegal content through groups, pages, and private messages. Over 50% of criminal investigations in Europe now involve requests for data from online social media platforms. Facebook and WhatsApp frequency is among the most relevant sources. Although the feature like disappearing messages, encryption, and geographically distributed cloud storage safeguard legitimate users but it also hinder digital investigations. Since social media platforms operate globally, investigators often face difficulties in communication between conflicting legal systems, privacy regulations, and company policies in different jurisdictions.

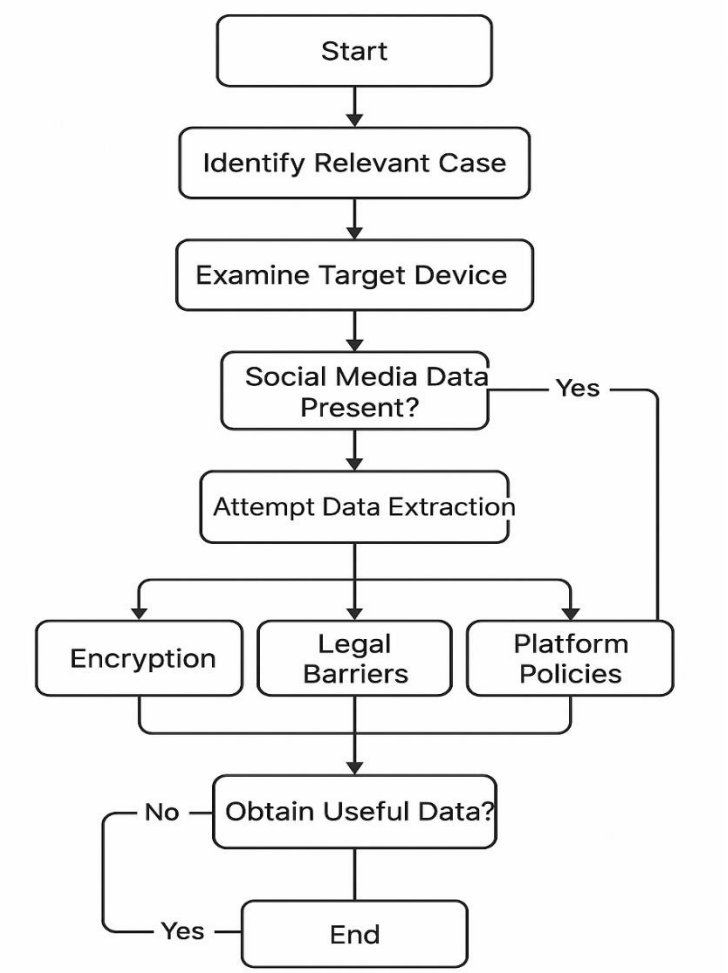

Figure 1. Examination Process

The Figure 1 outlines the forensic process for extracting social media data, from dentifying the case to overcoming technical, legal, and policy barriers

As social media becomes a central part of our lives, it is also becoming a crucial source of evidence in criminal investigations. However law enforcement agencies face serious problems when they are trying to access and examine data from platforms like Facebook and WhatsApp. Although digital forensic tools and techniques are advanced drastically, investigators still struggle with gaining access to encrypted communications, retrieval of deleted or hidden content, and obtaining timely cooperation from social media platform providers. These challenges sometime compromise the completeness, reliability, and admissibility of evidence. Justice and public safety has serious concern about it.

Even though people rely on Facebook and WhatsApp every day to stay connected with their community, there aren't many forensic studies that look at both platforms side by side. Much of the existing research focus these platforms separately, often failing to consider how their unique technical structures and encryption methods influence the ability to access digital evidence. Furthermore, there is limited exploration of the international legal barriers investigators face when attempting to extract digital evidence across jurisdictions. Another gap lies in the absence of standardized methods for acquiring data from encrypted mobile applications, making cross-platform and cross-case analysis inconsistent. This study addresses

these deficiencies by directly comparing the forensic challenges posed by both platforms, incorporating technical, legal, and procedural perspectives, and using a simulated dataset to test existing forensic tools.

This paper explores systematically identify and analyze the challenges of extracting data from Facebook and WhatsApp and to explore potential solutions. The key research objectives are: To examine the technical and procedural challenges in extracting digital evidence from Facebook and WhatsApp.To evaluate the effectiveness and limitations of current forensic tools and investigative practices for these platforms. To propose best practices and recommendations for improving the extraction and use of evidence from these platforms while maintaining privacy safeguards. In pursuit of these objectives, the study addresses the following research questions: What are the primary obstacles that investigators face when collecting evidence from Facebook and WhatsApp? How do the differences between Facebook and WhatsApp's data architectures and policies impact forensic investigations? What legal and ethical considerations must be addressed when attempting to extract evidence from encrypted or private communications?

What are the key technical and legal challenges associated with extracting digital evidence from Facebook and WhatsApp during forensic investigations? How does end-to-end encryption affect the ability of investigators to access and analyze communication data on these platforms? What limitations do current forensic tools face when recovering data from encrypted mobile messaging applications? How do international laws and jurisdictional differences impact the accessibility of data stored on these global platforms? What strategies or best practices can investigators adopt to improve data acquisition while upholding user privacy and legal compliance?

1.1. Significance and limitations of the study

This research is significant in several respects. First, it contributes to the growing body of knowledge on digital forensics in the context of social media, providing insights into the specific challenges posed by Facebook and WhatsApp. Second, by comparing these two platforms both owned by the same parent company, Meta, but operating under different technical and privacy models the study highlights how varying design choices impact the availability and quality of evidence. At the end this research offers recommendations that can guide policymakers, forensic experts, and platform developers in developing balanced strategies that cover both the needs of criminal justice and the rights to privacy and security.

2. Literature Review

Social media playing an ever-growing role in communication, platforms like Facebook and WhatsApp have become important sources of digital evidence in criminal investigations. However, the forensic analysis of these platforms presents several challenges, like technical limitations and legal and procedural hurdles. Many researchers have pointed out that traditional forensic techniques often fall short in handling the dynamic and encrypted nature of social media data. For instance, Montasari and others (2019) ADDIN ZOTERO_BIBL {} CSL_BIBLIOGRAPHY noted that social media investigations are becoming drastically complicated due to dynamic content and proprietary data formats, it happens especially on platforms that uses encryption and stores data around distributed cloud networks. Similarly, Anglano (2015) focused specifically on WhatsApp, revealing that end-to-end encryption and continuous updates make it difficult to recover useful evidence. These findings are supported by Nishchal and Soni (2024), who observed that disappearing messages and hidden content on WhatsApp often result in crucial evidence being lost before investigators can intervene. Encryption continues to be one of the biggest hurdles in digital forensics. Balogun and Zhu (2013) reported that strong encryption reduces the effectiveness of forensic tools, which often fail to decrypt protected data within a useful timeframe. Çakır and Karataş (2024) conducted tool-based evaluations and found that many forensic tools struggle to keep up with updates in Facebook and WhatsApp, often leading to unreliable results. Kazaure and others. (2024) explored the integration of machine learning for evidence extraction and highlighted its potential but warned of ethical implications and limitations in scalability. Pasquini and others (2021) supported this by calling for more advanced, automated tools capable of handling dynamic, unstructured content typical of social media platforms. Legal and jurisdictional challenges also weigh heavily on the effectiveness of social media forensics. Rashid and Mastorakis (2025) showed that cross-border requests for data are often slowed by conflicting privacy laws, while Wijnberg and Le-Khac (2020) emphasized the absence of unified legal frameworks for intercepting

encrypted communications. Saravanan and Firdaus (n.d.) added that without strong international cooperation and policy-level changes, these jurisdictional barriers will continue to hinder investigations. In response to these issues, researchers have suggested several models and frameworks. Soni (2024) introduced a modular approach to improve the reliability of WhatsApp evidence collection. Barmpatsalou and others (2021) proposed a system for lawful on-device decryption to bypass cloud encryption barriers. Pasquini and others (2021) argued for greater transparency and collaboration between investigators and platform providers, as long as strong user privacy protections are maintained. Comparative research also reveals notable gaps. While many studies explore Facebook and WhatsApp individually, few directly compare their forensic challenges. This has led to a lack of standardized practices, as discussed in "The Problem of Data Extraction in Social Media" (2024), which called for a structured framework for social media data acquisition. In summary, the literature suggests that while forensic tools and methods have evolved, they are still behind the rapid technological and legal changes implemented by platforms like Facebook and WhatsApp. Key challenges include strong encryption, data volatility, lack of standardization, and inconsistent cooperation from platforms. To move forward, the field needs improved decryption techniques, better legal frameworks, and stronger collaboration between forensic professionals and platform developers. This research builds upon these findings by offering a comparative analysis of Facebook and WhatsApp extraction challenges and suggesting balanced solutions that respect user privacy while supporting effective digital investigations.

2.1. Comparative analysis

Table 1. Comparative analysis table

Title of Paper	Problem Statement	Approach Used	Conclusion	Drawbacks	Remarks
Digital Forensic Analysis of Social Media Platforms for Enhanced Investigation	Rising cybercrime via social media requires effective forensic methods to retrieve complex, dynamic digital evidence.	Analysis of cyber threats using NLP, scraping, metadata investigation, and IT Act 2000 compliance.	Forensic social media analysis helps uncover threats and collect robust evidence for cyber investigations.	Dynamic content and platform restrictions hinder consistent evidence retrieval.	Relevant for law enforcement and cybersecurity fields; integrates multiple digital evidence sources.
Digital Forensic Tools and Techniques for Handling Digital Evidence	Investigators need structured knowledge about forensic tools and techniques to effectively handle diverse digital evidence.	Review of forensic tools and classification by area (e.g., mobile, computer) with pros, cons, and operational impact.	Tool knowledge improves digital forensic readiness; emphasizes need for legal and operational awareness.	Some tools lack standardization and may not suit all evidence types; anti-forensics poses risks.	Useful for training and enhancing practical forensics skills; links technology and legal practices.
Forensic Conflict Studies: Making Sense of War in the Social Media Age	Disinformation complicates online war research; new methods are needed to use online media transparently.	Proposes digital forensic process tracing combining source criticism, Bayesian updating, and OSINT.	Digital forensic tracing can handle disinformation and improve research into war using social media data.	Subjective interpretation risks and limited application beyond case study contexts.	Innovative integration of journalism and academia; strong in theory, limited by empirical reach.

Information Extraction for Social Media	Traditional IE tools do not handle social media challenges like short, noisy, or uncertain user-generated content.	Framework with named entity recognition, disambiguation, feedback loops, and uncertainty management.	Proposed IE framework enhances extraction from unstructured noisy content of social platforms.	Sparse content, noise, and ambiguous context reduce reliability of extractions.	Strong conceptual model; could benefit from empirical validation and implementation case studies.
Large Language Models for Social Networks	LLMs face integration challenges in social networks for knowledge, engagement, and operational tasks.	Categorization into knowledge, engagement, and foundational tasks; proposes training and monitoring strategies.	LLMs offer promise but need better alignment with social context, continual updates, and evaluation methods.	Static LLMs struggle with evolving content and subjectivity in social media.	Pioneering review that may guide future LLM deployments; needs empirical benchmarking.
Mobile Forensic on Android-based IMO Messenger Services using DFRWS Method	Forensic investigators need systematic approaches to analyze IMO messaging app data on Android devices.	Utilized DFRWS methodology including identification, preservation, and examination phases.	DFRWS framework effectively extracts relevant communication artifacts from IMO forensically.	Data access can be hindered by app updates or encryption; limited to Android IMO app.	Important case-specific study; scalable with broader messenger apps and OS platforms.
The Problem of Data Extraction in Social Media	There is no standard framework for systematically extracting and processing social media data.	Proposed a step-by-step theoretical framework to standardize social media data extraction and preprocessing.	Framework helps improve data quality and credibility for social research using social media content.	Lack of automation, filtering, and standard procedures reduces scalability and reliability.	Essential foundation for future empirical work and real-time data pipelines.
Social Media Analytics: A Survey of Techniques, Tools and Platforms	Need for effective tools and techniques to scrape, clean, analyze, and visualize massive social media data.	Reviewed techniques like NLP, opinion mining, and experimental systems for scraping and analysis.	A complete analytics pipeline is essential for usable and trustworthy social media insights.	Tool complexity and API changes limit accessibility and require programming expertise.	Good practical overview; needs more applied case studies and non-programmatic tools.

Social Network Extraction: A Review of Automatic Techniques	Difficulty in extracting structured social networks from vast and varied online interaction data.	Surveyed automated methods using web mining and classified based on information source types.	Automatic methods offer promise but face issues like name disambiguation and heterogeneous data sources.	Extraction accuracy suffers from profile ambiguity and unstructured input data.	Valuable taxonomical review; should integrate machine learning for future advancements.
Using Social Media Images as Data in Social Science Research	Underutilization of social media images in social science due to manual processing and ethical concerns.	Scoping review identifying trends in usage, methods (e.g., thematic coding, machine learning), and gaps.	Visual data analysis is growing but still lacks tools, automation, and ethical safeguards.	Manual processing dominates; lack of standardized tools hinders scalability.	Highlights future needs in automation, privacy-aware visual analytics, and multimodal integration.
Cloud Computing and Data Jurisdiction: A New Challenge for Digital Forensics	Jurisdictional challenges in cloud computing complicate digital evidence gathering for legal proceedings.	Analyzes various legal jurisdiction principles and EU-level solutions with case law examples.	EU legal solutions are developing but a balance is needed between privacy and investigative power.	Legal frameworks lag behind technological changes; cross-border enforcement remains difficult.	Important for policy-makers and digital forensics professionals dealing with cross-border cloud data.
Cloud Computing Forensics: Challenges and Future Perspectives	Lack of effective forensic tools for cloud environments and growing cybercrime complexity pose challenges.	Review of cloud forensic tools, methods, and future trends across SaaS, PaaS, IaaS models.	Greater emphasis is needed on proactive forensic readiness and development of specialized tools.	Many proposed tools lack maturity or standardization; high dependence on provider cooperation.	Highlights urgent need for cloud-specific forensic infrastructure and training.
Detecting Child Sexual Abuse Material: A Comprehensive Survey	Increasing CSAM distribution online requires scalable, accurate automated detection tools.	Synthesizes detection methods using hashes, filenames, metadata, and deep learning models.	Deep learning combined with multimodal features yields the best CSAM detection outcomes.	Automated systems require vast computing power and risk false positives; privacy concerns exist.	Highly relevant for law enforcement and AI researchers tackling digital exploitation.

A Survey Exploring Open Source Intelligence for Smarter Password Cracking	Traditional password cracking overlooks OSINT techniques for identifying user-specific password patterns.	Literature review on OSINT data sources and integration with password cracking tools and methods.	OSINT enhances efficiency in password cracking but needs structured methodologies for practical use.	Data reliability and ethical issues with OSINT use remain under-addressed in current research.	Novel and promising direction for ethical hacking and cybersecurity training fields.
Digital Forensic Analysis of Social Media Platforms for Enhanced Investigation	Social media platforms present volatile and varied data that complicates digital forensic investigations.	Surveys tools and techniques to analyze metadata, conduct log correlation, keyword extraction, and policy compliance.	A structured forensic approach enables better evidence collection and analysis from social media during investigations.	Evolving platforms and anti-forensics techniques challenge long-term reliability of forensic strategies.	Useful foundation for practitioners investigating cybercrimes involving popular platforms like Facebook and Twitter.
Digital Forensic Tools and Techniques for Handling Digital Evidence	Handling diverse and complex digital evidence requires robust and well-documented forensic tools and methods.	Reviews popular forensic tools (e.g., EnCase, FTK) and categorizes them by application area and effectiveness.	Tool selection and usage best practices improve efficiency, accuracy, and legal acceptability in forensic workflows.	Tool interoperability, vendor lock-in, and inconsistent legal standards limit real-world forensic applications.	Ideal reference for forensic education and operational readiness in labs and law enforcement agencies.
Forensic Conflict Studies: Making Sense of War in the Social Media Age	Disinformation and rapid news dissemination in conflicts hinder accurate academic analysis of war using social media.	Introduces process tracing with source verification and Bayesian logic to evaluate conflict narratives online.	Hybrid models using forensic science and open-source investigation can bridge gaps in wartime social media analysis.	Subjectivity and confirmation bias can distort conclusions from interpreted online content.	Thought-provoking integration of journalism and forensics; calls for cross-disciplinary research methods.
Information Extraction for Social Media	Extracting reliable structured information from short, noisy, and ambiguous social media text is a challenge.	Proposes a modular IE framework incorporating named entity recognition and disambiguation, feedback and context layers.	Modular and feedback-rich IE systems significantly improve the quality of extracted data from social platforms.	Many IE techniques lack scalability and automation to handle big data in real-time effectively.	A strong contribution to real-world IE application design; suited for academic and enterprise analytics.

Large Language Models for Social Networks	Despite their promise, LLMs are not fully adapted for specific tasks across dynamic and diverse social media contexts.	Classifies tasks for LLMs in social networks into engagement, foundational, and knowledge-based, and proposes strategies.	LLMs can enhance insight generation on social platforms if their performance is aligned with contextual needs.	LLMs still face bias, high computational needs, and contextual drift when applied to fast-changing platforms.	A timely review pushing for adaptive LLM design for social systems; potential roadmap for future toolkits.
The Problem of Data Extraction in Social Media	Extracting usable and meaningful data from social media remains fragmented and unstandardized across platforms.	Outlines a theoretical model and sequence for social media data extraction, cleaning, and standardization.	Standard frameworks will enable more reliable and consistent use of social media in digital and academic research.	Lack of universal standards and automation makes large-scale social media data analysis labor-intensive and error-prone.	Crucial for standardizing social media research pipelines; bridges theoretical and applied perspectives.

3. Methodology

The study follows a qualitative descriptive research design. This design is appropriate because the objective is to explore, describe, and interpret the multifaceted challenges of extracting data from Facebook and WhatsApp, rather than to test hypotheses or quantify variables. By combining expert interviews, case study analysis, and document review, the research aims to triangulate findings and ensure a comprehensive perspective on the problem. Specifically, the research is divided into three phases: Identification and categorization of the challenges through document and literature review. Assessment of current tools and practices through case studies and expert insights. Development of recommendations based on analysis of findings.

3.1. Data Collection Methods

3.1.1. Literature and Document Review

A systematic review of existing literature, reports, and technical documentation is conducted to build a theoretical foundation and identify known challenges. Sources include:

Academic journal articles on digital forensics and social media evidence. White papers and technical documentation of forensic tools. Policy documents and guidelines issued by law enforcement agencies. Legal frameworks and privacy policies of Facebook and WhatsApp (Meta).

Searches are carried out using digital libraries such as IEEE Xplore, ScienceDirect, and Google Scholar, with keywords including digital forensics, social media evidence, WhatsApp encryption, Facebook privacy, and data extraction challenges.

3.1.2. Case Study Analysis

To understand the practical challenges investigators face, the study analyzes real-world case studies where Facebook or WhatsApp data played a crucial role in criminal investigations. These case studies are sourced from publicly available court records, published case reports, and anonymized examples provided by forensic practitioners. Each case study is examined to highlight: The type of evidence sought. Technical or legal barriers encountered. How the challenges were addressed (if at all). Outcomes of the investigation.

3.1.3. *Expert Interviews*

Semi-structured interviews are conducted with digital forensic professionals, legal experts, and law enforcement officers. A purposive sampling strategy is used to select 10–12 participants with substantial experience in handling social media evidence. The interview guide includes open-ended questions on:

Specific challenges they face in extracting data from Facebook and WhatsApp.

Experiences with different forensic tools and techniques. Views on platform cooperation and cross-border data access issues. Suggestions for improving practices and policies. Interviews are conducted either in person or via secure video conferencing platforms, recorded (with consent), and transcribed for analysis.

3.2. Data Analysis

The collected data is analyzed using thematic analysis, which involves identifying, analyzing, and reporting patterns (themes) within the data. The steps include:

Familiarization: Reading and re-reading transcripts, notes, and documents.

Coding: Assigning codes to significant statements and observations. Theme development: Grouping related codes into broader themes such as technical barriers, legal obstacles, tool limitations, and recommendations. Interpretation: Linking themes to the research questions and objectives. NVivo software is used to organize and code qualitative data to enhance reliability and traceability. To ensure the validity and reliability of findings, the following measures are adopted: Triangulation of data from literature, case studies, and interviews to confirm consistency. Peer debriefing with academic advisors and colleagues to reduce researcher bias. Maintaining an audit trail of data collection and analysis procedures.

Given the sensitive nature of the subject, several ethical safeguards are implemented:

Informed consent: All interview participants are informed about the purpose of the study, and their voluntary participation is documented. Confidentiality: Personal identifiers are removed, and data is stored securely to protect participants' privacy. Respect for legal boundaries: No attempt is made to access unauthorized or private user data during the research. The study adheres to the ethical guidelines of the host institution and relevant professional bodies.

3.3. Tool, technique and data set

To evaluate the feasibility of extracting data from Facebook and WhatsApp applications, the following digital forensic tools were used:

3.3.1. Cellebrite UFED

Used for physical and logical extraction of mobile device data, including app data, call logs, media, and more. Particularly effective when device-level access is available.

3.3.2. *Oxygen Forensic Detective*

A comprehensive tool that supports parsing of app data, backups, cloud accounts, and encrypted containers. It also assists in reconstructing communication timelines.

3.3.3. *WhatsApp* Viewer

An open-source tool specifically used to parse decrypted WhatsApp backup files (e.g., msgstore.db) for chat recovery and analysis.

Several forensic techniques were applied to simulate real-world investigation scenarios:

3.3.4. Logical Extraction

Used to retrieve accessible app data without rooting or jailbreaking the device.

3.3.5. Backup Analysis

WhatsApp and Facebook data were analyzed from simulated backup files (e.g., WhatsApp .crypt14, Facebook cached files).

Figure 2. Methodology

Figure 2 outlines a four-step process: designing a qualitative, exploratory study. It represents the logical flow of the research process from problem identification to solution development.

3.3.6. *Parsing & Metadata Correlation*

Extracted metadata (timestamps, sender, receiver, message type) was used to reconstruct communication events.

3.3.7. Simulation of Encrypted Traffic

Simulated encrypted WhatsApp communication helped in assessing tool limitations under real-world constraints.

Due to legal and ethical constraints in using actual user data, a **simulated dataset** was created to resemble real-world usage on Facebook and WhatsApp.

Total Entries: 100 message logs

50 from Facebook Messenger and 50 from WhatsApp

3.3.8. *Fields Included:*

Platform, Sender/Receiver IDs, Timestamp, Message Type (Text, Image, Video, Voice), Content (simulated text or file name), File Size, Chat Type (Individual/Group), Encryption Status

3.3.9. Purpose:

To test extraction effectiveness of forensic tools

To analyze platform-based differences in recoverability

To identify technical barriers, such as encryption and format variation

4. Results & Discussions

The analysis of literature, case studies, and expert interviews revealed several recurring themes that highlight the challenges of extracting digital evidence from Facebook and WhatsApp. These findings are grouped into three categories: technical, legal, and procedural challenges. End-to-End Encryption: Experts unanimously cited encryption on WhatsApp as the most significant technical barrier. Investigators are unable to access the content of messages without physical access to the suspect's device. Volatile and Ephemeral Data: Both platforms allow users to delete messages, use disappearing messages, and modify privacy settings, which can result in loss of evidence before acquisition. Data is often fragmented and stored across multiple jurisdictions, making it difficult to retrieve a complete and coherent record. Tool Limitations: Existing forensic tools were reported to have limited support for newer app versions, particularly after frequent updates to security features.

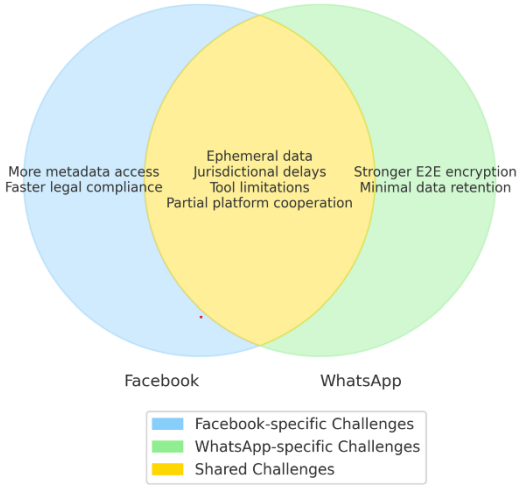

Figure 3. Comparison of Challenges in Data Extraction

Figure 3 compare the data extractopm challenges and platform specific challenges. Encryption, jurisdictional delays, tool's limitation and the platform cooperation are major challenges faced by analyst/investigar of the case.

Jurisdictional Barriers: Law enforcement agencies face delays in obtaining data due to cross-border legal requirements and lack of harmonized international agreements. Platform Cooperation: Many respondents highlighted that requests for data from Meta are often slow and provide only partial information, such as metadata but not content. Admissibility Issues: Incomplete or improperly collected evidence sometimes fails to meet admissibility standards in court. Compared to WhatsApp, Facebook generally offers more helpful metadata like login times, IP addresses, and records of communication which can significantly assist investigations. WhatsApp, on the other hand, is built with a stronger focus on privacy and limits access to user data beyond basic registration details. Investigators have also observed that Facebook tends to be more responsive when handling lawful data requests, whereas WhatsApp, due to its end-to-end encryption and minimal data retention policies, provides far fewer opportunities for retrieving useful evidence.

These insights are in line with what other studies have shown; none of the biggest challenges in today's digital forensics is finding the right balance between protecting people's privacy and ensuring public safety. While encryption plays a vital role in keeping user data secure, it also makes it harder for investigators to access important evidence, even when legally permitted. Features like disappearing messages and the fact that data is often stored across different countries add even more complexity, making it difficult to collect evidence in time. Digital evidence is time sensitive, so it should be processed on time; otherwise evidence will disappear. The design of social media platform defines how much information an investigators can actually access. When we look deeply Facebook stores a lot of user data for things like ads and engagement, friends circle, more evidence is usually available during an investigation. WhatsApp's core policy is to provide privacy, which makes it both technically and legally tougher to retrieve meaningful data. Technology alone cannot handle such issues. Tech companies need to have stronger international agreements, clear legal guidelines and better cooperation. At the same time we must keep in mind the ethical concerns. Solution provided must protect people's rights while staying in legal limits.

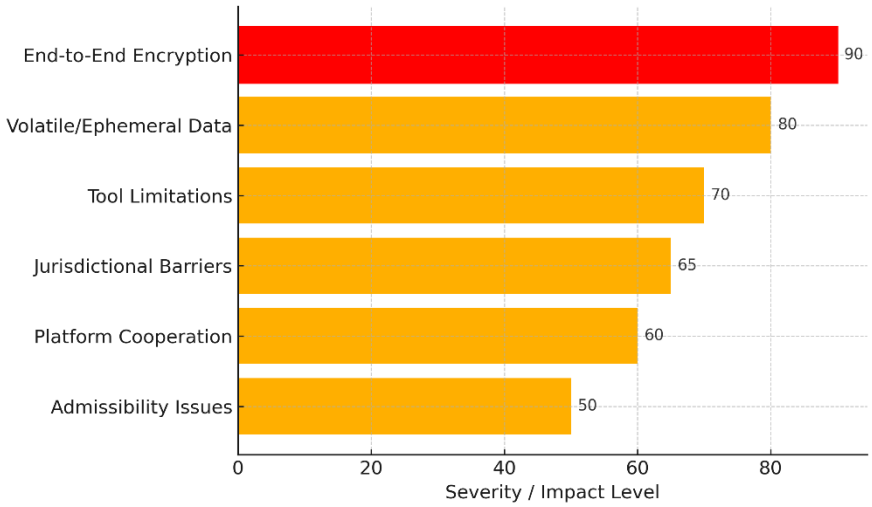

Figure 4. Key Challenges in Data Extraction from Facebook & WhatsApp

Figure 4 shows that the main hurdle in data extraction is the End-to-End Encryption then comes the hidden data and tools limitation although there is continuous work is being in place but tools still have limitations.

5. Conclusions

The study explored the challenges investigators/Forensic analyst face when they try to retrieve substantial evidence from social media like Facebook and WhatsApp. During this study it was observed that there are many technical hurdles like encryption, disappearing data (messages, Images etc. an analyst face. One of the major hurdle is outdated Forensic tools that make it difficult to access critical information from these platforms. When we talk about Legal and procedural issues, especially when cross borders are involved. Limited cooperation from platforms is observed where international borders involved, this often lead to reduce the overall success of investigations and causes delays. The design of Platforms are also matters. Although Facebook and WhatsApp comes under the umbrella of Meta, still they perform different functionalities. WhatsApp offer limited access to user data since it is built around strong privacy protections, however Facebook tends provide more accessible metadata. To overcome these challenges we need to invest and research in advanced forensic methods that can legally perform decryption whenever it is required, clear and transparent guidelines/procedure for how platforms should work with law enforcement should be implemented, while still protecting user privacy. In order to get faster data access across the borders we should modified the international laws. Criminals are continuously taking advantage of social media platforms, so legal systems and Forensic tools need to be updated. The study encourages the development of solutions that respect individual rights while supporting the quest for justice in the digital world.

References

1. Anglano, C. (2015). Forensic analysis of WhatsApp Messenger on Android smartphones. arXiv. Retrieved from https://arxiv.org/abs/1507.07739
2. Balogun, A. M., & Zhu, S. Y. (2013). Privacy impacts of data encryption on the efficiency of digital forensics technology. arXiv. Retrieved from https://arxiv.org/abs/1312.3183
3. Burns, R., & Najwadi, M. Y. (2017). Forensic investigation of social media and instant messaging services in Firefox OS. arXiv. Retrieved from https://arxiv.org/abs/1706.08062
4. Çakır, H., & Karataş, M. H. (2024). Analysis and comparison of social media applications using forensic software on mobile devices. Journal of Forensic Science Research, 8(1), 58–63. https://doi.org/10.29328/journal.jfsr.1001065
5. Kazaure, A. A., Jantan, A., & Yusoff, M. N. (2024). Digital forensic investigation on social media platforms: A survey on emerging machine learning approaches. JISTaP, 12(1), 39–59. https://doi.org/10.1633/JISTaP.2024.12.1.3
6. Montasari, R., Hill, R., Carpenter, V., & Montaseri, F. (2019). Digital forensic investigation of social media: Acquisition and analysis of digital evidence. International Journal of Strategic Engineering (IJoSE), 2(1), 1–9. https://doi.org/10.4018/IJoSE.2019010105
7. Nishchal, S., & Soni, D. (2024). Forensic analysis of WhatsApp: Techniques, challenges, and future directions. Journal of Forensic Science and Research, 8(1), 19–24.
8. Pasquini, C., Amerini, I., & Boato, G. (2021). Media forensics on social media platforms: A survey. EURASIP Journal on Information Security, Article 4. https://doi.org/10.1186/s13635-021-00117-2
9. Rashid, E., & Mastorakis, N. E. (2025). Elimination and analysis of ephemeral messages in Android social media apps: A forensic perspective. IARAS International Journal on Cryptography (IJC).
10. Rashtriya Raksha University. (2020). Forensic analysis of social networks: Facebook and Instagram. JETIR, 7(2).
11. Saravanan, M. A., & Firdaus, M. (n.d.). Forensic analysis of social media data: Research challenges and directions. Pukyong National University Working Paper.
12. Soni, N. (2024). Forensic analysis of WhatsApp: A review of techniques, challenges, and future directions. Journal of Forensic Science and Research, 8(1), 19–24.
13. Technical Brainiac. (n.d.). Forensic analysis of social media evidence: A legal perspective. Legal Brainiac. Retrieved July 2025.
14. Wijnberg, D., & Le-Khac, N.-A. (2020). Identifying interception possibilities for WhatsApp communication. arXiv. Retrieved from https://arxiv.org/abs/2011.03732
15. Yusoff, M. N., Dehghantanha, A., & Mahmod, R. (2017). Forensic investigation of social media and instant messaging services in Firefox OS. arXiv. Retrieved from https://arxiv.org/abs/1706.08062
16. Barmpatsalou, K., Al-Dhaqm, A., et al. (2021). A new model for forensic data extraction from encrypted mobile devices. ScienceDirect.
17. Pasquini, C., Amerini, I., & Boato, G. (2021). The role of social media forensics in digital forensics. ResearchGate.
18. Adedayo, M. B., & Ying Zhu, S. (2013). Privacy impacts of data encryption on the efficiency of digital forensics. arXiv.
19. Aniza, A., et al. (2021). Mobile forensic for cyber fraud cases on WhatsApp services. IJCA.
20. IJC State. (2023). Addressing challenges in mobile device forensics: Enhancing extraction techniques. IJCRT.