IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 27, Issue 3, Ser. 5 (May. – June. 2025), PP 01-05
www.iosrjournals.org

Forensic Recovery of Chat Artifacts from the Heesay App: A Manual Analysis Approach

M B Pathak, Emmanuel Ben T, Dr S S Murthy, Eswara Sai Prasad Chunduru, M Krishna, Sourav Mondal
Central Forensic Science Laboratory, DFSS, MHA, GOI, India.

Abstract:
The growing popularity of specialized dating and social networking sites, especially those serving the LGBTQ community, has presented significant difficulties for digital forensic investigators in recent years. The Heesay app is one such platform that was used in a criminal case and may have included important communication evidence. An organized forensic investigation using an Android handset running the Heesay app is presented in this case study. A thorough manual inspection revealed that the app's primary SQLite database file (blued2015.db) was present despite the lack of tool support. Several tables, such as ChattingModel, SessionModel, and UserAccountsModel, were contained in the file and were susceptible to scripting and structured queries. The results highlight the vital significance of hybrid forensic techniques that incorporate programmatic parsing, timezone-aware timestamp translation, and conventional database analysis. This case study provides useful, repeatable advice for digital forensic specialists working with unsupported or specialized mobile applications by outlining the file locations, database schema, and sequential analytical queries. The study emphasizes how useful tool-agnostic investigation techniques are for locating and verifying digital evidence in contemporary mobile settings.

Key Word*: SQLite database; Heesay; scripting; UFED; Mobile forensic.*

Date of Submission: 14-06-2025 Date of Acceptance: 28-06-2025

I. Introduction

Many of the mobile phones in use now require specific information and expertise from rhetorical experts. Having an associate's degree in computer forensics is frequently insufficient to fully understand the nuances and challenges of mobile forensics. These days, smartphones are the most popular mobile communications devices, but they are also among the most difficult to retrieve evidence from. The tactics that use evidence from mobile phones are referred to as mobile rhetorical. It is the science of recovering digital evidence from a mobile device using recognized techniques while maintaining forensically sound settings. Analysis of each SIM card and phone memory is part of it. Similar to other digital media, mobile phones have the capacity to save evidence. [7]

Dating applications (apps) are a great example of how people can find and communicate with people who may have similar interests or lifestyles, especially in a society where online engagement is the norm. Social and dating apps are now common topics of interest in both criminal and civil investigations in the field of mobile forensics. These applications are important sources of digital evidence since they frequently include location information and private messages. However, support for mainstream applications is usually given priority by commercial forensic tools, leaving specialized or regional apps—like the social and dating app Heesay-unsupported. [5]

The development of information and communication technology that is increasingly modern and sophisticated has a significant impact on human life. This technology has become an important part of everyday life, affecting the way humans communicate, work, learn, and socialize, as seen in the Telegram Mobile service application. Heesay Mobile application is a dating messaging application for LGBTQ+. Its main purpose is to facilitate user communication easily and securely through text, audio, video, images, and stickers.

Problem Statement

The forensic examination of an Android device that was received in a lab environment served as the impetus for this case study. Investigators were unable to decode or extract useful content from the Heesay application, even with the use of industry-standard tools. We used a manual investigative method, concentrating on the app's underlying SQLite database to retrieve chat messages and associated metadata, after realizing the limitations of automated tool support. This situation highlights a broader gap in mobile forensics: the need for

adaptable, manual methodologies when automated tools fall short. The lack of published research or forensic decoding methods for Heesay further compounded the challenge, necessitating a custom investigation protocol.

II. Related Works

Mobile forensics is a crucial area within digital forensics that focuses on retrieving and analysing digital evidence from mobile devices. As mobile devices become more complex and varied, they present unique challenges and opportunities for forensic investigators. This survey explores different aspects of mobile forensics, including the analysis of dating apps, health and fitness applications, third-party applications, and the tools and methods used in mobile forensic investigations.

Analysis of Dating Applications

In 2020, Knox and colleagues conducted a forensic analysis of the Happn dating app, examining both Android and iOS versions. Their study highlighted how forensic analysis of the app's activity could potentially uncover personal information. The research involved creating profiles, capturing network traffic, and acquiring device images to identify artifacts that might reveal sensitive user data. The findings showed that significant personal information could be retrieved from both network traffic and device storage, emphasizing the importance of thorough forensic examination in dating app investigations. [5]

Barros and colleagues, in their 2022 study, performed a forensic analysis of the Bumble dating app for Android devices. They identified various forensic artifacts that could be extracted from the app, including user identification and message exchanges. The research also involved creating a script to parse and visualize the main forensic artifacts, providing a valuable tool for digital forensic practitioners. The study emphasized understanding the data structure stored on the device and the potential forensic value of the recovered information. [4]

Health and Fitness Applications

Al-Ghamdi and colleagues, in their 2024 study, investigated the forensic analysis of health and fitness applications on Android devices. They aimed to identify potential forensic artifacts within these applications and assess their implications for user privacy and security. The research involved analysing various popular health and fitness apps to understand how securely they store user data and how this data can be utilized in forensic investigations. The findings highlighted the importance of choosing secure applications that protect user privacy, a crucial consideration for both users and developers. [1]

Third-Party Applications

Althebaity and colleagues, in their 2020 study, analysed the forensic implications of third-party mobile applications, focusing on the Instagram app. Their study aimed to determine the location and types of recoverable data after the uninstallation of social networking apps from a smartphone. The research involved creating a scenario-based methodology to conduct a comprehensive forensic investigation, providing significant insights into the recoverable data and its potential forensic value. The findings emphasized the importance of understanding the data left behind by third-party applications and its relevance to forensic investigations. [2]

Tools and Methodologies

Mobile Device Forensic Tools

In 2014, Ayers and colleagues provided an in-depth look into mobile devices and the technologies involved in their forensic examination. The study discussed the classification of mobile forensic tools and the capabilities of these tools in preserving, acquiring, examining, and reporting digital evidence. The research highlighted the importance of understanding the hardware and software characteristics of mobile devices and the various tools and techniques used in their forensic analysis. [3]

Challenges and Opportunities

Umale and colleagues, in their 2023 review, discussed the challenges and opportunities in mobile phone forensics, emphasizing the need for specialized knowledge and tools to extract evidentiary data from mobile devices. The study discussed the various obstacles faced by forensic investigators, including the diversity of mobile devices, data protection mechanisms, and the limitations of forensic tools. The research underscored the importance of continuous training and the development of comprehensive forensic toolkits to address the evolving landscape of mobile forensics. [7]

Ryu and colleagues, in their 2018 study, focused on the forensic analysis of third-party applications for mobile forensic investigations. Their research aimed to identify the location and types of recoverable data from third-party applications, particularly focusing on social networking apps. The study involved scenario-based methods to conduct forensic analysis and emphasized the importance of understanding the data left by these applications and its relevance to forensic investigations. [6]

The literature surveyed in this paper highlights the critical role of mobile forensics in digital investigations. The studies reviewed demonstrate the complexity and diversity of mobile devices and the challenges they present to forensic investigators. The analysis of dating apps, health and fitness applications, and third-party applications underscores the importance of thorough and methodical forensic examination to uncover valuable digital evidence. The development and validation of forensic tools and methodologies are essential to ensure the integrity and admissibility of the evidence recovered from mobile devices. Continuous research and collaboration among forensic practitioners are crucial to address the evolving challenges in mobile forensics and to enhance the effectiveness of digital investigations.

III. Methodology

Device and Data Acquisition

The suspect device was an Android smartphone, Redmi 8, acquired using logical and file system extraction methods. Extraction was performed using the forensic tool Cellebrite UFED. The Heesay application was identified during the app enumeration phase using the UFED Physical Analyser, but no decoded artifacts were available within the tool interfaces

The Figure 1 and Figure 2 shows the interface of the UFED Physical Analyser showing the decoded information available for chat and messaging application and Figure 3 shows the database/db. file of the Heesay app

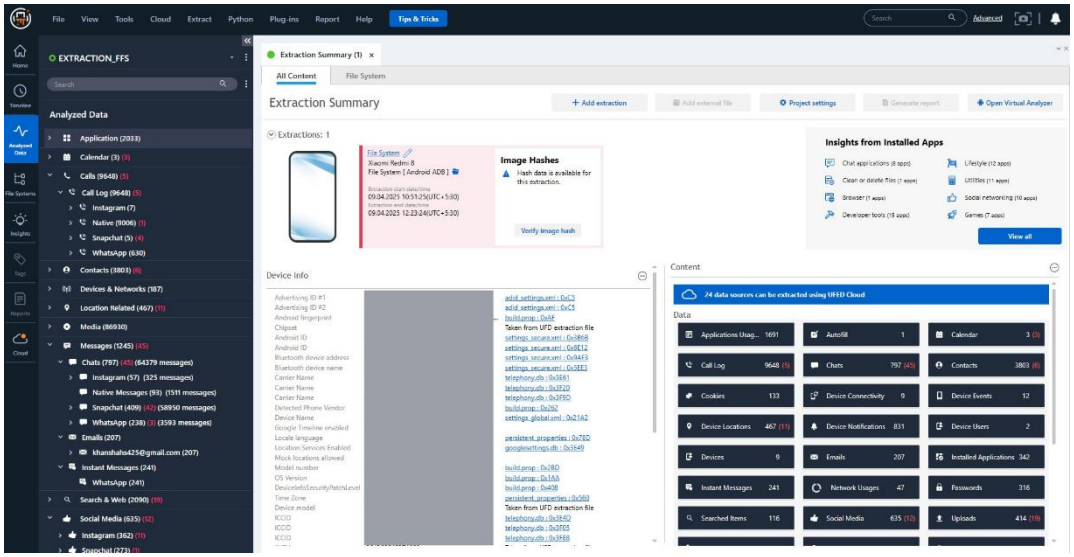

Figure 1

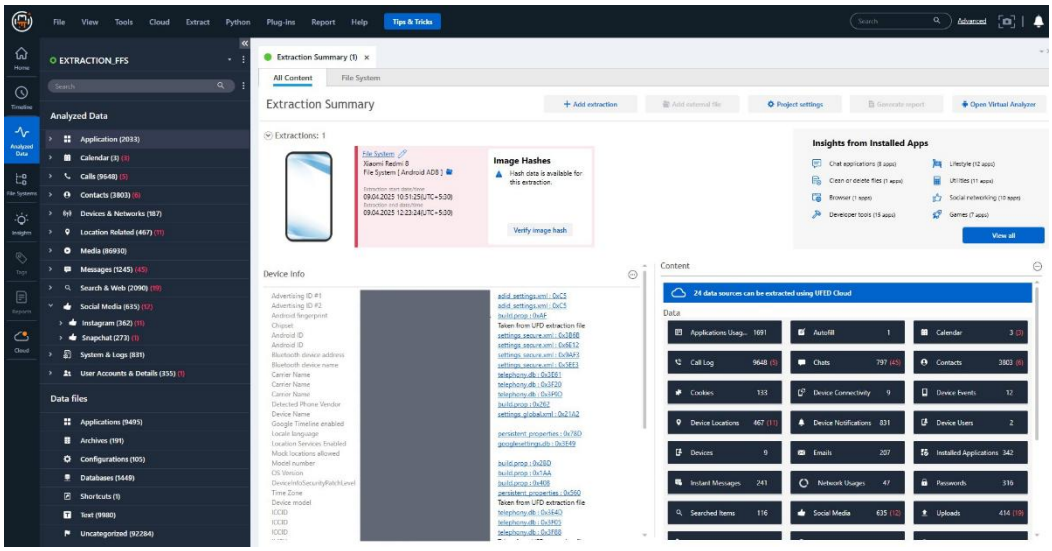

Figure 3

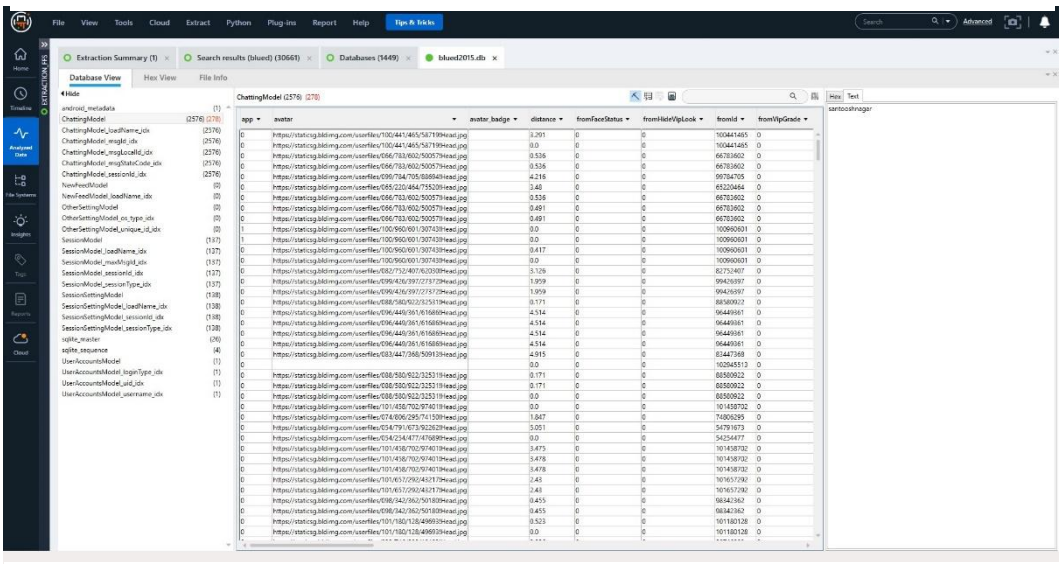

Figure 2

Identification of App Artifacts

Using file system access, we located the Heesay app's data directory within:
/data/data/com.blued.international/databases/
The database of interest was named blued2015.db. It was copied and opened using DB Browser for SQLite for manual inspection.

Database Structure Analysis

We identified several tables, with ChattingModel being the primary repository of chat content. Key fields in this table included:

- msgContent: message text
- msgTimestamp: time of message (epoch format)
- fromId, toId: sender and recipient identifiers
- nickName: display name of sender
- sessionId: conversation identifier

***Alternate Methods*:**

1. Using SQL Query: Structured Query Language (SQL) was utilized to interact directly with the SQLite database file (blued2015.db). This method allowed for:

- Targeted data retrieval: Extracting relevant fields such as msgContent, msgTimestamp, and fromId from key tables like ChattingModel.
- Sorting and filtering: Isolating recent chats, filtering by sender/receiver, and identifying different message types.

2. Using python script: Python scripts using libraries such as sqlite3, pandas, and json were developed to automate and enhance the analysis:
   - Timestamp conversion: Chat timestamps stored in Unix format were converted to human-readable datetime values in IST (Indian Standard Time).
   - Content decoding: JSON-encoded strings in chat fields were parsed to extract embedded metadata or media information.
   - Data aggregation: Grouping and cross-referencing messages across users and sessions to reconstruct conversation threads.
   - Python provided the added advantage of flexibility and reproducibility, making it suitable for larger datasets and custom logic implementation.

IV. Discussion

The difficulties forensic investigators encounter when working with unsupported programs such as Heesay are highlighted in this case study. Commercial solutions are unable to analyze data from these apps; thus, manual analysis is required. Although this process takes time, it can provide insightful information.

Key Observations:

Manual Analysis Necessity: The Heesay app's data was not accessible through standard forensic tools, highlighting the need for manual database examination.

Structured Data Retrieval: By analyzing the ChattingModel table, investigators could retrieve structured chat data, including message content, timestamps, and user identifiers.

Non-Textual Data Indicators: The presence of JSON-formatted strings in the msgContent field indicates the storage of non-textual data, such as multimedia messages or system notifications.

These findings align with challenges noted in other forensic analyses, where unsupported apps require tailored approaches for data extraction and interpretation

V. Conclusion

The limitations of using only commercial forensic tools are illustrated by the forensic analysis of the Heesay app, particularly when working with specialized or unsupported programs. Crucial chat data was extracted by manual examination of the application's SQLite database, highlighting the significance of:

Developing Custom Queries: Crafting specific SQL queries to retrieve relevant data fields.

Understanding Database Structures: Gaining insights into the app's data storage mechanisms to effectively interpret retrieved information.

Adapting to Data Anomalies: Recognizing and addressing irregularities in data formats, such as timestamp conversions.

This case study serves as a reference for digital forensic practitioners, highlighting the need for adaptability and in-depth analysis techniques when encountering unsupported mobile applications. Future work may focus on developing automated tools or scripts to streamline the analysis of similar apps, enhancing efficiency and accuracy in digital investigations.

Reference

[1]. Al-Ghamdi, N. J., Al-Akhras, M., & Alhosban, F. (2024). Forensic analysis of health and fitness applications on Android. International Journal of Information & Digital Security, 2(1), 17-28.

[2]. AlThebaity, M., Mishra, S., & Shukla, M. K. (2020). Forensic analysis of third-party mobile application. Journal of Information Processing Systems, 16(3), 568-578.

[3]. Ayers, R., Brothers, S., & Jansen, W. (2014). Guidelines on mobile device forensics. NIST Special Publication, 800(101r1).

[4]. Barros, A., Almeida, R., Melo, T., & Frade, M. (2022). Forensic analysis of the Bumble dating app for Android. Forensic Science, 2(1), 201-221.

[5]. Knox, S., Moghadam, S., Patrick, K., Phan, A., & Choo, K. K. R. (2020). What's really 'Happning'? A forensic analysis of Android and iOS Happn dating apps. Computers & Security, 94, 101833.

[6]. Ryu, J. H., Kim, N. Y., Kwon, B. W., Suk, S. K., Park, J. H., & Park, J. H. (2018). Analysis of a third-party application for mobile forensic investigation. Journal of Information Processing Systems, 14(3), 568-578.

[7]. Umale, M. N., Deshmukh, A. B., & Tambhakhe, M. D. (2023). Mobile phone forensics challenges and tools classification: A review. International Journal of Advanced Research in Computer Science, 8(3), 1-5.