

Forensic Analysis of WhatsApp, WeChat, and Twitter on iOS Devices

Siwei Zhang

*Department of Computer Systems & Sciences, DSV
Stockholm University
Stockholm, Sweden
zhangsiwei729084343@gmail.com*

Yanxiang Du

*Department of Computer Systems & Sciences, DSV
Stockholm University
Stockholm, Sweden
yadu9601@win.su.se*

Yongjie Hao

*Department of Computer Systems & Sciences, DSV
Stockholm University
Stockholm, Sweden
yongjiehao18@outlook.com*

Abstract—This study explores the digital forensic analysis of three major social networking applications—WhatsApp, WeChat, LinkedIn, and Twitter—on iOS devices. By leveraging mature forensic methods, data extraction techniques, and network traffic analysis, we aim to unravel the complex digital traces left behind during user interactions. The research focuses on key components of the iOS backup file structure, including device information, installed application lists, backup metadata, and actual backup data files, to comprehensively understand the complexities of data preservation and analysis. Through a comprehensive exploration of WhatsApp chat records and related user information in the manifest.db file, the study reveals the significance of these digital artifacts in criminal investigations. Additionally, the research examines the challenges encountered in retrieving data from other applications (such as WeChat, Twitter, Facebook, and LinkedIn) within the backup file, such as data encryption and file path changes.

Keywords — *Digital Forensics, iOS Devices, Social Networking Applications, WhatsApp, Data Extraction, Backup File Structure*

I. INTRODUCTION

A. Background

Social media appears in all aspects of human life. It offers convenient lifestyles and communication, but user activity isn't fully protected, risking personal info disclosure. Social media applications enable users to control their data, connect with others, and view connection lists within the system. Personal information recorded on social platforms, such as name, date of birth, photos, emails, and phone numbers, is critical information for obtaining evidence and investigating crimes. [1] On the other hand, the widespread use of social media may also affect the security of information stored by users on social media. For instance, retrieved information may

be used by criminals for online fraud. They may create fake profiles on social media platforms to deceive users and conceal their identities, aiming to attack users on the app. [2]

In addition to WhatsApp and Twitter, there's WeChat, with 1.2 billion monthly active users globally. [3] WeChat can be used by criminals as a tool for crime; for example, criminals can use it to conduct online fraud and even sell illegal guns and ammunition. [4] The historical records of social media applications obtained from criminals' smartphones mostly serve as evidence of their crimes, playing a crucial role in the evidence collection and prosecution stages of cases. Therefore, this study will focus solely on the forensic analysis of WhatsApp, WeChat, and Twitter.

As we know, smartphones are commonly used to access social media applications. And 52% of global network traffic is carried out through mobile device. [5] Most users use Android or iOS smartphones to access social media apps, which have been widely used for years. Tens of thousands access personal social media apps via mobile devices. Similarly, criminals can easily use smartphones for more mobile-related crimes. Smartphones are now primarily used as a tool to obtain personal information. [1] The global usage rate of iOS devices is leading, expected to reach 28.46% by March 2024, surpassing Android usage. [6] So this study will mainly analyze mainstream social media apps on iOS devices globally. Additionally, law enforcement and forensic departments must grasp current technologies due to the lack of systematic regulations for investigating crimes on mobile social media apps. [1]

B. Related Work

Acquiring data from smartphones involves three main methods: manual acquisition, logical acquisition, and physical acquisition.

The manual acquisition method involves physically accessing the mobile device and manually extracting information from its native applications. [7] Logical acquisition involves retrieving data from a mobile phone using the device manufacturer's application programming interface for synchronization with a computer. [8] Logical data extraction utilizes the device's original API to access files and directories in its file system. This method is straightforward for examiners to implement and enables easy data extraction. However, it does not recover deleted data immediately, as such data is typically marked as deleted in SQLite databases on mobile devices and may be overwritten later. Physical acquisition refers to the process of extracting the complete contents of one or more flash memory chips from a cellular phone. This data is obtained in the form of a raw hexadecimal dump, which can be further parsed to retrieve file system information and human-readable data. [9] During physical acquisition, a bit-by-bit copy of the device's internal memory is obtained, typically containing both current and deleted data. [1]

Different researchers are exploring logical acquisition and physical acquisition for data acquisition from older iOS devices. Morrissey and Campbell [30] performed logical acquisition on iPhone 2G and 3GS devices using iTunes backup. They were able to recover various types of data such as call logs, address book entries, cookies, geolocation data, web browsing history, SMS/MMS messages, multimedia files, and application data. [10] Zdziarski performed physical acquisition and utilized a recovery toolkit called iLibrary+ version 1.6 to boot an iPhone 3G and acquire a physical image using the dd command. This method allows for a bitwise copy of the memory image to be obtained. [11]

The complexity of forensic analysis on iOS devices, particularly attributed to the continually evolving security measures and discrepancies among iOS versions, can potentially impede the effectiveness of data extraction methods. Engman, M. highlighted that databases associated with applications, like the Facebook app, might not be found in their usual locations or could have undergone structural changes due to the complexities introduced with iOS version 6. Additionally, Engman, M. pointed out the limitations faced by certain forensic tools, especially concerning their compatibility with iOS 6. [12] The aforementioned issues underscore the considerations that need to be taken into account during iOS forensic analysis.

C. Research questions and contributions

The primary aim of the research is to investigate the forensic artifacts present on iOS internal storage resulting from typical interactions with social networking applications such as WhatsApp, WeChat, and Twitter. By examining the network traffic artifacts generated during the usage of these social networking applications on iOS platforms, this research aims to provide a comprehensive understanding of the digital traces left behind by users. [1]

D. Investigation Framework

Mckemmish outlines forensic investigation in four stages: identification, preservation, analysis, and presentation of digital evidence [13], a structure akin to the four-stage NIST guidelines for mobile device forensics. [14] This research adopts this framework to steer the mobile device investigation and conduct digital forensics analysis of artifacts from typical social networking applications. The following provides details for each step.

1) *Identification and extraction of data:* In the realm of digital forensics, the accurate identification and extraction of data are paramount for ensuring the integrity and reliability of evidence. In our study, evidence was meticulously collected from various sources associated with a mobile device to ensure a comprehensive forensic analysis. Specifically, data was extracted from the internal storage and internal memory of the device, alongside monitoring the network traffic to capture any data transmitted over the network.

For this research, an iPhone 7 Plus running iOS version 15.7.6 was utilized. The choice of this device and operating system version was deliberate, given their widespread usage and the unique forensic challenges they present. To facilitate a thorough analysis, a backup of the device's internal storage was acquired using established forensic techniques. This backup serves as a critical point of reference, allowing for a detailed examination of the device's contents without altering the original data.

2) *Preservation:* To identify any modifications to files extracted from an iOS device, it's essential to calculate MD5 and SHA1 hash values for each obtained file. It is known that analyzing the hash values and timestamp metadata of files uploaded and subsequently downloaded via social networking applications on iOS platforms revealed that the download process leads to modifications in both file content and timestamps. [1]

3) *Analysis:* Collected data from internal memory and internal storage of the devices was examined to determine possible data remnants of using the Facebook, Twitter, LinkedIn, and WhatsApp applications on iOS (refer to Section 2), and to answer the question of this research.

4) *Presentation:* A summary of the findings and their forensic values will be represented in this research.

D. Outline

Section 2 of this study lists the equipment used in the experiments and describes the procedures for the experimental setup. Section 3 describes the analysis of mentions of social applications on iOS devices. Finally, we summarise the results of this paper. [1]

II. EXPERIMENTAL SETUP

A. Experimental Environment And Examination Software

Evidence needs to be meticulously collected from the internal storage of the mobile device to ensure a comprehensive digital forensic investigation. In our specific context, an iPhone 7 Plus running iOS version 15.7.6 was used as the test device. A crucial part of the evidence-collection process involves acquiring a bit-for-bit image of the device's internal memory. This method ensures that an exact replica of the data is obtained, preserving the integrity and completeness of the evidence.

On an iOS device, such as the iPhone 7 Plus, a backup of the internal storage can be acquired using the Finder application on a laptop running macOS. This step involves creating a full backup of the device's data, which can then be used for detailed forensic analysis. This backup process is critical as it captures all the necessary data, including application files, system logs, and user-generated content, without altering the original data on the device.

All analyses of the files and images extracted from the internal memory are conducted on a desktop PC equipped with a macOS operating system. This setup ensures compatibility and reliability in handling the iOS data, leveraging macOS's robust capabilities for forensic analysis.

To prepare the device for data collection, the iPhone needs to be wiped and restored to its default factory settings. This process ensures that any residual data from previous uses is removed, providing a clean slate for the forensic examination. Following the restoration, specific applications are downloaded from the Apple App Store. These applications are then used to simulate typical social networking behaviors such as logging in, messaging, modifying personal information, uploading posts, and commenting. These activities are essential for generating relevant data that will be examined in the forensic analysis.

After simulating these behaviors, bit-to-bit logical images of the device are taken. These images are exact copies of the device's data, ensuring that all information is captured accurately for forensic examination. The necessary software for mobile device examination is then installed on the workstation where the analysis will be carried out. This workstation is equipped with both open-source and commercial software tools, providing a comprehensive suite of applications for analyzing the data.

The mobile review was conducted using a combination of open-source and commercial software to ensure a thorough and multifaceted analysis. The selection of tools is critical to cover various aspects of the forensic investigation, from data extraction to analysis and reporting. All hardware and software used for analyzing the artifacts present on the iOS device

are listed in Table 1, providing a detailed overview of the tools and resources utilized in this study. This rigorous process of data identification and extraction, coupled with the use of advanced software tools, ensures that the forensic investigation is thorough and reliable, capable of uncovering and preserving critical digital evidence from social network applications.

TABLE I
DEVICES USED IN THE STUDY

Devices/Tools	Introduction	Specification/Versions
Mac OS	Workstation	MacOS 13.5
iPhone 7 Plus	The device to be examined	iOS version 15.7.6
LinkedIn Application	Application to be examined	iOS version
WhatsApp Application	Application to be examined	iOS version 24.8.78
WeChat Application	Application to be examined	iOS version 8.0.48
Twitter Application	Application to be examined	iOS version 10.36.2
DB Browser for SQLite	Software for examining SQLite files	Windows Version 3.12.2
Plist Editor Pro	Software for examining plist files	Windows Version 2.5.0

B. Performed User Behaviors

In this study, we installed four widely-used social networking applications—WeChat, Twitter, Facebook, and LinkedIn—on the mobile device to conduct a comprehensive forensic analysis. Each of these applications was chosen due to their significant user bases and the diverse range of interactions they facilitate. This selection ensures that our study covers various social networking behaviors and the corresponding forensic data they generate.

To effectively analyze user interactions, we developed specific user behavior models for each application. These models represent the typical actions that users perform on these platforms. In the realm of digital forensics, the data resulting from these user behaviors is considered potential evidence. Consequently, replicating and documenting these behaviors on the mobile device is crucial for capturing comprehensive forensic data.

For each application, we executed a series of application-specific behaviors. These actions were carefully chosen to encompass a wide range of typical user activities, ensuring that the collected data reflects common usage patterns. The objective was to generate a diverse set of data artifacts that could provide insights into user activities and serve as valuable evidence in forensic investigations.

The characteristics of each application and the specific behaviors performed during the study are as Table 2. Table 2 lists commonly accepted user behaviors and actions, providing a clear framework for understanding the forensic evidence associated with each application.

Application	Performed User Behaviors
WeChat	Logging in, sending text and voice messages, making voice and video calls, sharing moments (similar to status updates), using WeChat Pay for transactions, and interacting with official accounts and mini-programs.
Twitter	Tweeting, retweeting, liking tweets, replying to tweets, sending direct messages, following and unfollowing accounts, and engaging with trending topics and hashtags.
Facebook	Logging in, posting status updates, liking and commenting on posts, sending and receiving private messages, joining and participating in groups, and uploading photos and videos.
LinkedIn	Logging in, updating professional profiles, making and accepting connection requests, sending and receiving messages, posting updates and articles, and engaging with professional groups and job listings.
Whatsapp	Sending text messages, sharing links, participating in group chats, blocking contacts deleting contacts, managing the friends list"

TABLE II
USER BEHAVIORS PERFORMED IN APPLICATION

Each of these actions generates specific data artifacts within the application's storage on the device. By performing these behaviors, the study aims to capture a wide array of forensic evidence, including metadata, log files, cached information, and user-generated content. These artifacts are critical for understanding how the applications are used and can provide detailed insights into user behavior, which is essential for forensic analysis.

The data generated from these user behaviors were collected and analyzed using various forensic tools and methodologies. This comprehensive approach ensures that the forensic evidence is accurately captured and preserved, allowing for a detailed examination of user interactions with these applications.

Table 3 serves as a reference point for the types of user behaviors analyzed and the corresponding forensic data produced. It highlights the importance of understanding application-specific behaviors to effectively gather and interpret digital evidence. This structured approach ensures that the forensic analysis is thorough, replicable, and capable of uncovering detailed insights into user interactions with these social networking applications.

By systematically documenting and analyzing these behaviors, the study contributes to the broader field of digital forensics. It offers methodologies and findings that can aid forensic practitioners in examining social network applications, ensuring that the evidence collected is reliable and actionable.

C. Data Acquisition Process

1) *Backup Creation:* After simulating user behaviors, a complete backup of the iPhone's internal storage was created using the Finder application on a macOS laptop. The following

steps were involved in the backup creation process:

1. *Connecting the Device:* The iPhone was connected to the macOS laptop via a USB cable.
2. *Creating an Encrypted Backup:* In Finder, the device was selected, and the option to create an encrypted backup was chosen. Encryption is crucial as it ensures that sensitive data, such as passwords, secure tokens, and other confidential information, is included in the backup.

The resulting backup file serves as a snapshot of the device's state at the time of backup, capturing all relevant data generated by the simulated user behaviors.

2) *Examination and Analysis of Backup File Structure:* The backup file created from the iPhone contains several key components essential for forensic analysis. To examine and analyze these components, the backup file was input into DB Browser for SQLite and Plist Editor Pro. These tools facilitate the exploration and extraction of data stored within the backup. The main components of the backup file structure include:

1. *Device Information:* Stored in the Info.plist file, this includes details such as the device name, product type, serial number, and IMEI. This information provides a comprehensive overview of the device's identity and characteristics.
2. *Installed Applications List:* The backup records the applications installed on the device, with each application's related information stored as key-value pairs.
3. *Backup Metadata:* Contained within the Manifest.db file, an SQLite database, which includes metadata for all files in the backup. This encompasses file paths, sizes, and hash values. Additionally, the Manifest.plist and Status.plist files provide a detailed description of the backup's content and structure, as well as the backup status, such as completion status and backup date.
4. *Backup Data Files:* The actual data files from the backup are stored in multiple folders named with hash values. These folders contain the data corresponding to various applications and system components.

3) *Data Extraction and Analysis:* 1. To extract and analyze the data, the following steps were undertaken: Exploration with DB Browser for SQLite: This tool was used to browse and query the SQLite databases within the backup, such as Manifest.db. The databases contain critical information about the files stored in the backup, including their locations and metadata.

2. Analysis with Plist Editor Pro: This tool was employed to examine plist files, which store structured data in a hierarchical format. These files include Info.plist, Manifest.plist, and Status.plist, among others.

3. Identification of Relevant Data: By meticulously examining the backup file structure, specific files and databases relevant

5. **Comprehensive Analysis:** The extracted data was analyzed to uncover insights into user behaviors, interactions, and application usage. This involved parsing chat records, examining metadata, and analyzing multimedia content.

'ZWACLBLACKLISTITEM' is used to store information about blacklisted contacts, such as those who are blocked by the user.

D. Group Related

The 'ZWAGROUPINFO', 'ZWAGROUPMEMBER' and 'ZWAGROUPMEMBERSCHANGE' tables are instrumental in providing comprehensive information about users in groups within the chat application. 'ZWAGROUPINFO' is a table in the WhatsApp database that stores information about groups. It primarily includes key details such as the group's name, creation date, creator, subject, and picture. Each group has a unique identifier for distinguishing between different groups. The 'ZWAGROUPMEMBER' table encompasses several key fields that provide detailed insights into group membership dynamics within the chat application. 'ZMEMBERJID' field represents the unique identifier (JID) of the group member. The JID typically includes information such as the user's unique ID or username, which allows the system to track and manage group membership accurately.

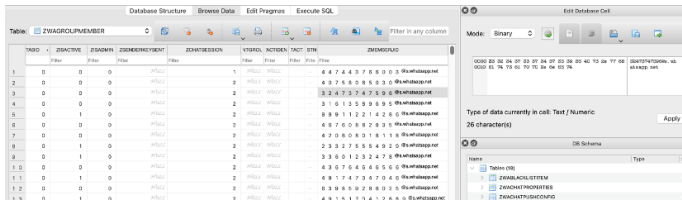


Fig. 3. ZWAGROUPMEMBER

The 'ZWAGROUPMEMBERSCHANGE' table records changes in group membership. It tracks various alterations such as members being added or removed, along with timestamps for these modifications.

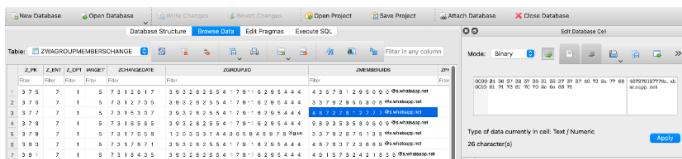


Fig. 4. ZWAGROUPMEMBER

E. Message

In the WhatsApp database, several tables collectively form the complete chat content. The 'ZWACHATSESSION' table stores basic information about each chat session, including the participant's Jabber ID (ZCONTACTJID), tags (ZETAG), the last message text (ZLASTMESSAGETEXT), and the chat partner's name (ZPARTNERNAME), providing an overview of each chat session. The 'ZWAMESSAGE' table records the actual message content, including the message text, timestamps, and sender and receiver Jabber IDs, forming the core of the chat records. The 'ZWAMESSAGEADDAITEM' table contains additional information related to messages, such as media file paths, message statuses (read, unread, etc.), and message types (text, image, video, etc.), adding detail and context to the messages. Lastly, the 'ZWAMESSAGEINFO'

table provides essential metadata for each message, including its unique identifier, entity type, versioning information, a reference to the message content, and receipt details. Together, these tables work in unison to provide a comprehensive and detailed chat record system within WhatsApp, ensuring that every aspect of the chat sessions and messages is thoroughly documented and organized.

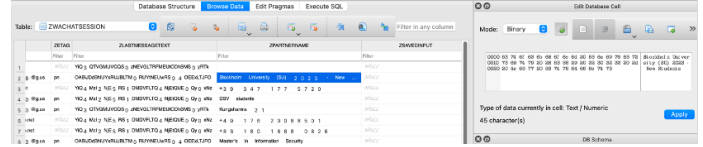


Fig. 5. ZWACHATSESSION

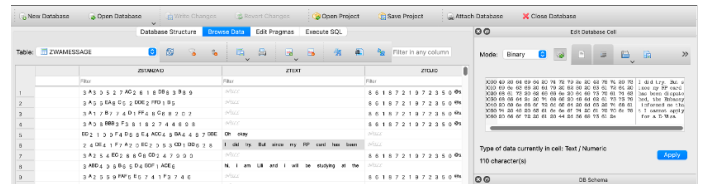


Fig. 6. ZWAMESSAGE

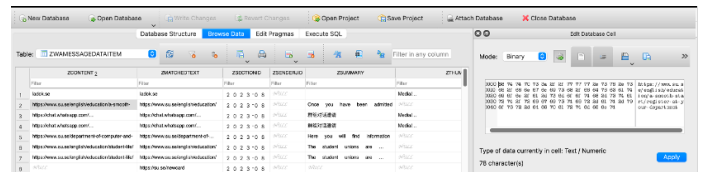


Fig. 7. ZWAMESSAGEADDAITEM

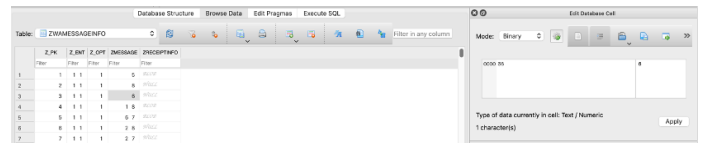


Fig. 8. ZWAMESSAGEINFO

The WhatsApp database contains tables for user information, including profile pictures, push names, and blacklist data. It also has tables for group details, membership, and changes, as well as tables for storing chat session details, messages, additional message information, and message metadata. Additionally, there are tables for multimedia content, push notifications, configuration, and other related data. WhatsApp database is invaluable for investigations, providing user identification through profile pictures and push names, insights into group dynamics, and the ability to reconstruct message histories with detailed metadata. It also offers multimedia evidence and configuration settings that reveal user behavior and potential attempts to hide communication.

F. Other Application

When searching for data related to other application like WeChat, Twitter, Facebook, and LinkedIn in the manifest.db

file within a backup, it is often found that many corresponding fileIDs are missing from the backup folder. The potential reasons could be:

1. Data Encryption: Some applications may encrypt or protect their data, making it impossible to directly recognize or access these files through conventional methods. Encryption is used to safeguard user privacy and security, and access to such data requires specific decryption methods or keys. [15]

2. File Path Changes: Applications may change the file paths or methods for storing data, resulting in discrepancies between the paths stored in the backup and the actual storage paths. As a result, the path information in the backup files may not directly correspond to the actual file locations. [16]

These factors highlight the complexities involved in data backup and retrieval, especially when dealing with applications that employ advanced security measures or undergo frequent updates and modifications. As forensic investigators or data analysts, understanding these potential challenges is crucial for accurately interpreting backup data and extracting relevant information for investigative purposes.

IV. CONCLUDING REMARKS

In this study, we conducted an in-depth forensic analysis of four major social networking applications—WhatsApp, WeChat, LinkedIn, and Twitter—on iOS devices. By leveraging mature forensic methods, data extraction techniques, and network traffic analysis, we aimed to unravel the complex digital traces left behind during user interactions. Our comprehensive approach involved creating a complete backup of the iPhone's internal storage, examining the backup file structure using tools such as DB Browser for SQLite and Plist Editor Pro, and analyzing the key components essential for forensic analysis.

Our findings highlight the critical importance of understanding application-specific behaviors to effectively gather and interpret digital evidence. Each application generated a unique set of data artifacts, including metadata, log files, cached information, and user-generated content. These artifacts provided detailed insights into user activities, serving as valuable evidence in forensic investigations.

The study underscores the significance of encryption in the backup process, ensuring that sensitive data such as passwords and secure tokens are included. The backup file structure, encompassing device information, installed applications list, backup metadata, and actual data files from the applications, proved to be a rich source of forensic data. The meticulous examination and analysis of these components allowed us to identify and extract relevant forensic data, contributing to the broader field of digital forensics.

Through this research, we have demonstrated the potential of digital forensic analysis in uncovering detailed insights into user interactions with social networking applications. Our methodologies and findings offer valuable guidance for forensic practitioners, enabling them to examine social network applications with greater accuracy and reliability. As social media continues to play an integral role in modern communication, the ability to effectively analyze and interpret digital evidence from these platforms will be increasingly crucial for law enforcement and forensic departments.

Despite the promising results, this study is not without its limitations. One significant limitation is the scope of applications analyzed. While we focused on four widely used social networking applications, there are many other applications that could also yield valuable forensic insights. Future studies should consider expanding the range of applications to provide a more comprehensive understanding of social network forensics.

Another limitation is the dependency on specific tools and methods for data extraction and analysis. The use of DB Browser for SQLite and Plist Editor Pro, while effective, may not cover all possible data artifacts or encryption methods used by different applications. Future research should explore alternative tools and methodologies to ensure a broader and more inclusive forensic analysis.

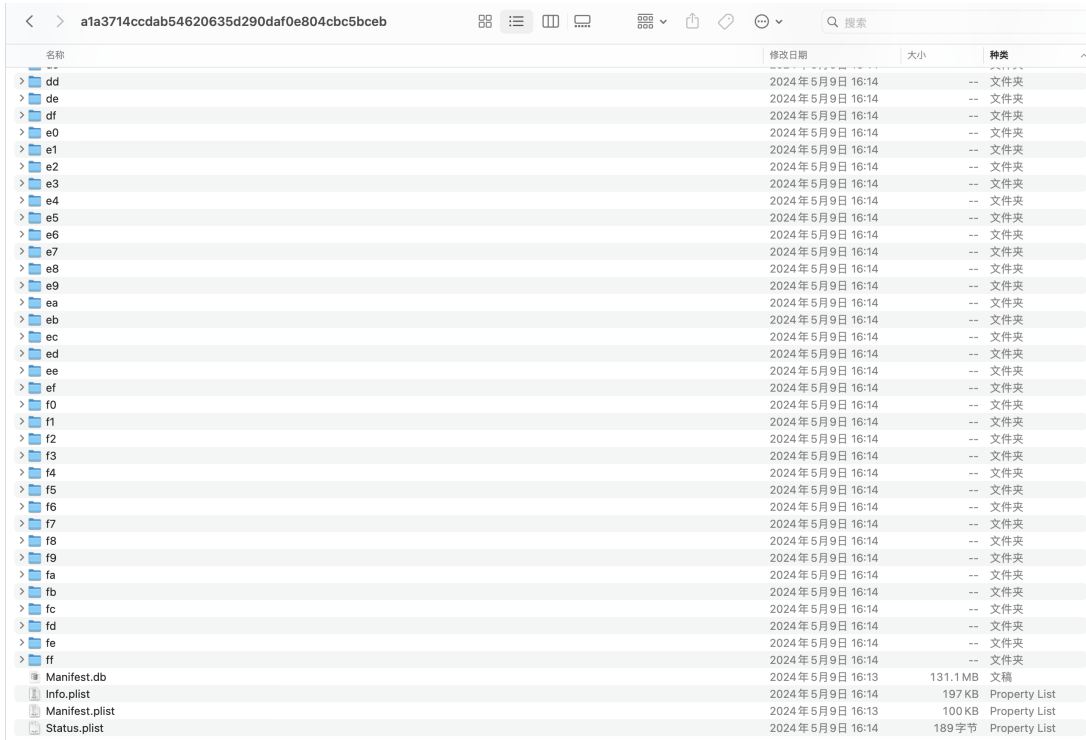
REFERENCES

- [1] F. Norouzizadeh Dezfouli, A. Dehghantanha, B. Eterovic-Soric, and K.-K. R. Choo, "Investigating social networking applications on smartphones detecting facebook, twitter, LinkedIn and google+ artefacts on android and iOS platforms," vol. 48, no. 4, pp. 469–488.
- [2] N. Al Mutawa, I. Baggili, and A. Marrington, "Forensic analysis of social networking applications on mobile devices," vol. 9, pp. S24–S33.
- [3] Exploding Topics, "Most popular messaging apps (2024)." Accessed: Apr. 17, 2024, 2024.
- [4] S. Wu, Y. Zhang, X. Wang, X. Xiong, and L. Du, "Forensic analysis of WeChat on android smartphones," vol. 21.
- [5] F. G. Eriş and E. Akbal, "Forensic analysis of popular social media applications on android smartphones," vol. 9, no. 44, pp. 386–397. Publisher: MUSA YILMAZ.
- [6] StatCounter Global Stats, "Mobile vendor market share worldwide." Accessed: Apr. 17, 2024, 2024.
- [7] P. M. Mokhonoana and M. S. Olivier, "Acquisition of a symbian smart phone's content with an on-phone forensic tool."
- [8] S. Bommisetty, R. Tamma, and H. Mahalik, *Practical Mobile Forensics*. Packt Publishing Ltd.
- [9] D. C. A. Murphy, "Developing process for mobile device forensics,"
- [10] S. Morrissey and T. Campbell, *iOS Forensic Analysis: for iPhone, iPad, and iPod touch*. Apress.
- [11] J. Zdziarski, *iPhone Forensics: Recovering Evidence, Personal Data, and Corporate Assets*. O'Reilly Media, Inc.
- [12] M. Engman, "Forensic investigations of apple's iphone," 2013.
- [13] R. McKemmish, "What is forensic computing?,"
- [14] R. Ayers, S. Brothers, and W. Jansen, *Guidelines on mobile device forensics*. No. NIST SP 800-101r1, National Institute of Standards and Technology.
- [15] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley & Sons, 2 ed., 1996.
- [16] D. Giampaolo, *Practical File System Design with the Be File System*. Morgan Kaufmann Publishers, 1999.

APPENDIX A

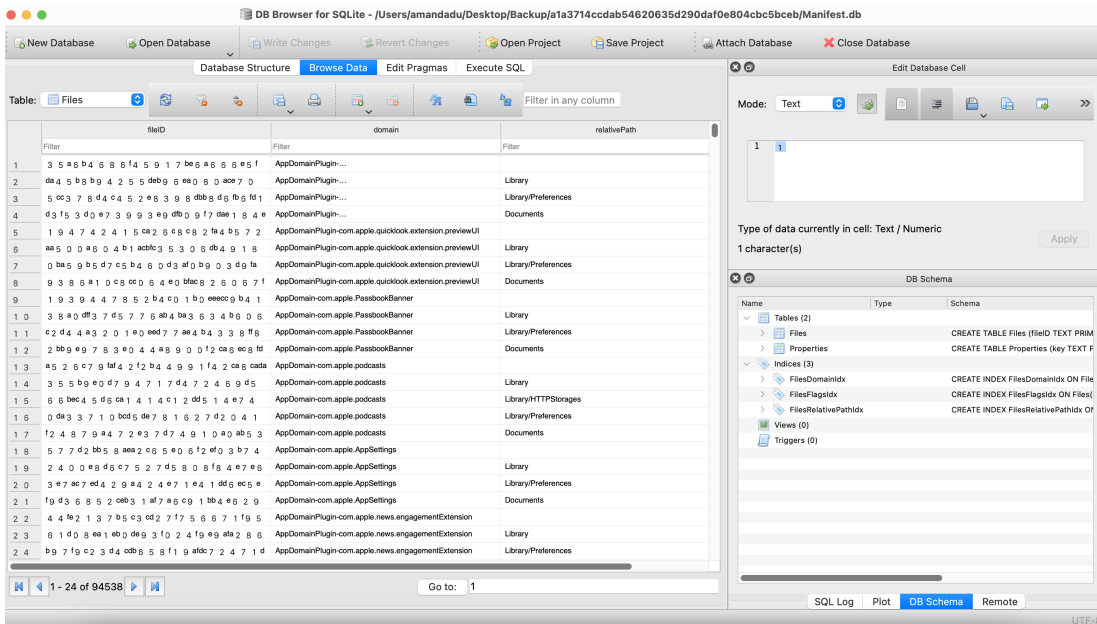
OVERVIEW OF BACKUPS AND MANIFEST.DB FOR

WHATSAPP



名称	修改日期	大小	种类
dd	2024年5月9日 16:14	--	文件夹
de	2024年5月9日 16:14	--	文件夹
df	2024年5月9日 16:14	--	文件夹
e0	2024年5月9日 16:14	--	文件夹
e1	2024年5月9日 16:14	--	文件夹
e2	2024年5月9日 16:14	--	文件夹
e3	2024年5月9日 16:14	--	文件夹
e4	2024年5月9日 16:14	--	文件夹
e5	2024年5月9日 16:14	--	文件夹
e6	2024年5月9日 16:14	--	文件夹
e7	2024年5月9日 16:14	--	文件夹
e8	2024年5月9日 16:14	--	文件夹
e9	2024年5月9日 16:14	--	文件夹
ea	2024年5月9日 16:14	--	文件夹
eb	2024年5月9日 16:14	--	文件夹
ec	2024年5月9日 16:14	--	文件夹
ed	2024年5月9日 16:14	--	文件夹
ee	2024年5月9日 16:14	--	文件夹
ef	2024年5月9日 16:14	--	文件夹
f0	2024年5月9日 16:14	--	文件夹
f1	2024年5月9日 16:14	--	文件夹
f2	2024年5月9日 16:14	--	文件夹
f3	2024年5月9日 16:14	--	文件夹
f4	2024年5月9日 16:14	--	文件夹
f5	2024年5月9日 16:14	--	文件夹
f6	2024年5月9日 16:14	--	文件夹
f7	2024年5月9日 16:14	--	文件夹
f8	2024年5月9日 16:14	--	文件夹
f9	2024年5月9日 16:14	--	文件夹
fa	2024年5月9日 16:14	--	文件夹
fb	2024年5月9日 16:14	--	文件夹
fc	2024年5月9日 16:14	--	文件夹
fd	2024年5月9日 16:14	--	文件夹
fe	2024年5月9日 16:14	--	文件夹
ff	2024年5月9日 16:14	--	文件夹
Manifest.db	2024年5月9日 16:13	131.1 MB	文稿
Info.plist	2024年5月9日 16:14	197 KB	Property List
Manifest.plist	2024年5月9日 16:13	100 KB	Property List
Status.plist	2024年5月9日 16:14	189 字节	Property List

Fig. 9. Overview of Backups



fileID	domain	relativePath
1	AppDomainPlugin...	Library
2	AppDomainPlugin...	Library/Preferences
3	AppDomainPlugin...	Documents
4	AppDomainPlugin...	Library
5	AppDomainPlugin-com.apple.quicklook.extension.previewUI	Library/Preferences
6	AppDomainPlugin-com.apple.quicklook.extension.previewUI	Documents
7	AppDomainPlugin-com.apple.quicklook.extension.previewUI	Library
8	AppDomainPlugin-com.apple.quicklook.extension.previewUI	Library/Preferences
9	AppDomain-com.apple.PassbookBanner	Documents
10	AppDomain-com.apple.PassbookBanner	Library
11	AppDomain-com.apple.PassbookBanner	Library/Preferences
12	AppDomain-com.apple.PassbookBanner	Documents
13	AppDomain-com.apple.podcasts	Library
14	AppDomain-com.apple.podcasts	Library/HTTPStorages
15	AppDomain-com.apple.podcasts	Library/Preferences
16	AppDomain-com.apple.podcasts	Documents
17	AppDomain-com.apple.podcasts	Library
18	AppDomain-com.apple.AppSettings	Library/Preferences
19	AppDomain-com.apple.AppSettings	Library
20	AppDomain-com.apple.AppSettings	Library/Preferences
21	AppDomain-com.apple.AppSettings	Documents
22	AppDomainPlugin-com.apple.news.engagementExtension	Library
23	AppDomainPlugin-com.apple.news.engagementExtension	Library/Preferences
24	AppDomainPlugin-com.apple.news.engagementExtension	Library/Preferences

Fig. 10. Overview of Backups