Watch Your WeChat Wallet: Digital Forensics Approach on WeChat Payments on Android

Jiaxuan Zhou and Umit Karabiyik(✉)

Purdue University, West Lafayette, IN 47907, USA
{zhou757,umit}@purdue.edu

Abstract. WeChat is one of the most popular instant messaging applications in the world. In 2021, WeChat had 1.24 billion active users. Its users call it 'super app' due to its various functions, and they particularly enjoy the payment feature for both personal and business purposes. Criminals abused the platforms to facilitate illegal activities such as bank fraud. Previous research on WeChat focused mostly on the messaging function of the WeChat app, but it has rarely been considered as a wallet or payment app. The payment feature on WeChat can provide crucial evidence, especially for scam cases. Therefore, this research intends to fill the gap by performing a forensic analysis of the WeChat payment function on Android devices. This research has five stages: device preparation, data population, data extraction, analysis, and reporting. In this research, five activities were examined: registering a credit card in the account, sending and receiving money with contact, performing money transactions with the corporate account, making payment through the *Service portal*, and requesting the complete payment history from the official Weixin Pay account. The result shows that money transactions between contacts and money transactions through *Service portal* can be fully recovered. Partial information can be retrieved when users register for credit cards or purchase official account services. However, no data on payment history could be recovered from the official Weixin Pay account. Magnet Axiom Process and Examine tools were used for image extraction and artifact analysis.

Keywords: Digital Forensics · Mobile Forensics · Android Forensics · WeChat Forensics

1 Introduction

WeChat is one of the most popular applications in the world. As of 2021, there are 1.24 billion users of WeChat [4]. Wechat started as an instant messaging mobile app but later developed as a multi-purpose app. Many people call it the "super app" because it is an application for everything. Besides the basic messaging functions, it also supports online payment, mini-games, news aggregation,

S. Goel et al. (Eds.): ICDF2C 2022, LNICST 508, pp. 97–110, 2023.
https://doi.org/10.1007/978-3-031-36574-4_6

and much more. People register their credit cards in this app and make money transactions daily for both personal and business use. Especially in China, from tuition payments to restaurant checks, WeChat Pay is in every nook and corner of the country. In 2021, there were 251 billion US dollar transactions in WeChat [7]. Criminals had their eyes on this application due to the convenient money transaction feature. The traditional phone scam requires criminals to lead the victim through a full process of bank transactions. However, with WeChat, they only need to lure the victim to do a few clicks on the phone. To link criminals with the case, authorities need digital evidence such as money transaction records.

Most of the research done on WeChat so far views it mostly as an instant messaging application. Previous studies include pertinent artifacts on the device [9,13], network analysis [5], and volatile memory analysis [17]. However, few studies have been done on WeChat as a wallet application. The research carried out by Yan et al. [14] analyzed the network traffic of the fund transaction function. Transaction-related artifacts could be extremely valuable to law enforcement when investigating a WeChat-related case. When a transaction is complete, WeChat leaves a transaction record message in the chat. This chat history can give law enforcement insight into why the transaction happened, who was involved in the transaction, and when the transaction occurred.

This research fills the gap by focusing on forensic analysis of WeChat as a wallet on an Android device, identifying pertinent artifacts, and discussing privacy and security concerns. This research is broken down into four phases. The first phase is the device preparation step. The Android mobile device that was used is a Google Pixel 5a. The smartphone was rooted using TWRP and Magisk. The second phase is the data population phase. This phase was abide by the Mobile Device Data Population Setup Guide published by the National Institute of Standards and Technology (NIST [1]). The third phase is data acquisition, a physical acquisition was performed. In the fourth phase, we analyzed the image using Magnet Axiom Examine and Magnet Axiom Examine was used for artifact analysis. The last phase was to report the findings. All forensic analysis tools were chosen because they are widely adopted in the digital forensic community.

2 Literature Review

To understand the current research that has been done on WeChat, this section included research related to WeChat analysis methodologies, WeChat analysis in Android, WeChat analysis in payment features, and WeChat database decryption methodologies. It is also worth noting that WeChat continuously updates the app. These updates sometimes add new features or patch bugs, which can cause changes in the security mechanism or data storage structure. Therefore, papers earlier than 2015 are not included.

2.1 WeChat Payment Feature Analysis

WeChat did not specify in their retention policy about payment information, such as payment transaction and card information. Log data and chat data were

addressed. Log data has relatively long retention period, the data can stays maximum of three months [2]. Chat data stays in the internal server for maximum three hours before deletion. Under all conditions, the message is permanently deleted from internal server within 72 h after the message sent [2].

Red packet and fund transfer are basic models for the WeChat payment feature. Users can make transactions with other contacts in a conversation. Until the time of this study, there is only one paper published about the payment function. Yan et al. [14] performed a network analysis of the traffic pattern generated by red pocket and fund transfer. The result shows the traffic of red pocket and fund transfer can be differentiated from plain text and pictures. However, the research did do any analysis of the artifacts that could be on the devices.

2.2 WeChat Analysis on Android

There was a study by Sihombing, Fajar, and Utama [10] that did a systematic review of digital forensic research on instant messaging apps. The study restated that extracting data from the backup feature does not work on smartphones with Android versions later than 6.0. The authors suggested taking advantage of analytical tools such as Apktool or dex2jar.

Azfar, Choo, and Liu [3] proposed a two-dimensional taxonomy of the forensic artifacts of communication apps. The taxonomy is summarized after analyzing thirty popular Android communication apps. The generated files and data are stored in `/data/data/com.tencent.mm`. Some user picture remnants are stored in the `/sdcard/tencent/MicroMsg` folder. The main database of WeChat is `MicroMsg.db`, this database contains 73 tables inside. The taxonomy is composed of four groups: users and contact information, timestamps, exchanged messages, and others. The users and contact information group contains all user identifiable information and the contacts information. The timestamps are a group that identifies the specific time of communication. The messages exchanged identify artifacts exchanged during chat sessions, including text, multimedia, or group communication. The other category collects all artifacts that cannot fit into the three other groups mentioned above. Examples include databases, voice call duration, and group chat member lists.

Wu et al. [13] examined two basic features of WeChat: messenger and post. The study emphasized that root privilege is necessary. The directory `com.tencent.mm` contains critical data related to messages and posts. Without root privilege, the directory cannot be accessed. The study tested the Android emulator to check whether it can retrieve forensic artifacts or not. The study used two emulator tools and both showed identical results to those for smartphones. There was another important question that was discussed in the paper. Some researchers mentioned that, for Android versions older than 6.0, the 'backup' command provided by Android Debug Bridge (ADB) no longer works. An alternative proposed was to downgrade WeChat to version 6.0. However, the researchers argued that downgrading can cause inconsistency. In their paper, nine files were modified and three files were removed. Although core database

files such as `EnMicroMsg.db` were successfully extracted, researchers advised processing this method with caution.

The research done by Silla [11] used logical acquisition tools to locate and recover artifacts related to instant messaging applications, specifically WeChat data in the internal memory of an Android smartphone. The study focused on partial activities on WeChat. Partial activities include text messages, audio, videos, images, GPS locations, and downloaded documents. The authors also discussed the effectiveness of two logical extraction techniques, ADB and MPE+. The two tools cannot completely extract artifacts. The database files could not be extracted. As a sequence, the shared conversation, the contact list, and user information were not discovered. Therefore, the author claimed that file system extraction is necessary.

Menahil et al. [6] analyzed five social networking apps on Android, WeChat included the five. The scope of populated data was the account profile, friends, status, exchanged messages, video calls, and posts. Many artifacts were found in `Tencent` directory. In the path `com.tencent/media/0/MicroMsg`, the images, videos, and audios transferred during chat sessions were stored there. Account information was stored in the shared preference folder, such as the username and phone number. The capability of three forensic tools (Axiom, XRY, and Autopsy) was also evaluated. The research followed the NIST standards for smartphone analysis tools, and the result showed that Axiom is ranked first.

Wu et al. [12] proposed a new approach to analyze remote WeChat data on Android. WeChat relies heavily on local storage. However, there are many third parties that create mini services on WeChat. When users access the third-party service, the data is stored on the remote server of the third party. Wu et al. [12] proposed using the ADB shell command to obtain the WeChat data on the computer and then load the data onto the virtual machine of Android. After WeChat runs successfully on the virtual machine, researchers can start to operate the application and request data from remote servers.

Park et al. in [8] performed an analysis of WeChat on Windows and Android platforms. The populated artifacts include the five categories: user information, chatting room, chatting, posting, and app usage. The result shows that the Android device can retrieve more artifacts than the Windows device. The authors analyzed the location card and real location sharing functions on both devices. The capabilities of the two devices are different. Only the mobile device can send location cards and join real-time location sharing. The Windows device can only receive location cards. For both devices, all populated location data was recovered. In the Android device, the location data was located in the `EnMicroMsg.db`, and the `MSG0.db` file stores the location data in Windows.

2.3 WeChat Database Decryption

Zhang et al. in [16] conducted a forensic analysis of the WeChat application. The paper identified the location of databases and the recovery of voice and deleted messages. It also analyzed what encryption the WeChat database uses, as well as analyzing how to decrypt the database.

3 Methodology

The objective of this study is to identify payment-related artifacts from the WeChat application on Android phone. The methodology consists of five stages: device preparation, data creation, image acquisition, image analysis, and reporting. The test and examination process is consistent with the guidelines of the National Institute of Standards and Technology (NIST). The workflow is shown in the diagram 1.

Fig. 1. Workflow for WeChat analysis on Android

3.1 Test Environment and Requirements

To make sure the experiment could be conducted, a set of hardware and software was prepared in advance. The list is shown below:

- Google Pixel 5a with Android 11
- USB cable
- Workstation with Windows 10, Intel i7, 64 bit
- WeChat application with version 8.0.18
- TWRP barbet application
- Minimal ADB and Fastboot with version 1.4.3
- Magisk application with version 21.0
- Magisk Manager application with version 8.0.2
- Root checker application with version 6.5.0
- DB Browser for SQLCipher tool with version 4.4.0
- DB browser for SQLite tool with version 3.12.1
- Magnet Axiom Process tool with version 4.9.1
- Magnet Axiom Examine tool with version 4.9.1

3.2 Device Preparation

The Pixel 5a was rooted in this stage to maximize artifacts that can be retrieved in the analysis stage. The smartphone was set to developer mode and connected to a Windows workstation. On the workstation, the Minimal ADB and Fastboot tool was initiated, and the command `fastboot flashing unlock` was entered to unlock the bootloader of the smartphone. The TWRP software installed the

custom firmware on the smartphone by entering the command `fastboot boot twrp.img`, and the device entered the custom recovery mode. Then, the Magisk app was installed on the smartphone. It is worth noting that the Magisk app is not available in the Google Play store, the setting must allow third-party download. In recovery mode, the Magisk file was installed and the smartphone was restarted. Later, the root checker app verified that the Android device was successfully rooted.

3.3 Data Creation

In this first stage, our goal was to create a real-life scenario and to perform a list of real user activities. We reset the phone to manufacture mode and downloaded the WeChat app from the Google Play Store. Then we created a new WeChat account on the phone and then started to populate the data. Real users usually make personal transactions when they discuss an event with other contacts, such as visiting a restaurant or going shopping, the transaction renders as a chat message in a chat room. We mimic real users, populated text messages of an event, and the transaction. Next, we paid to a corporate account. WeChat has many third-party corporate accounts providing paid services such as psychological evaluation. Once the transaction is complete, the user received a receipt from the WeChat Pay account (WeChat payment management account). Besides virtual services, the WeChat platform is a universal payment platform for offline activities. In the Services module, WeChat provides offline activity assistance that covers all aspects of life, such as booking movie tickets, paying utility bills, scheduling taxis, and more. We also made a payment for an offline activity in the *Services* module as well. The WeChat Pay account records all user transactions on the WeChat platform. We requested bill histories from this account. In summary, we focused on the following five activities:

1. Register a credit card to the account
2. Send and receive money with friend
3. Send money to corporate account
4. Use the Services function and purchase movie ticket
5. Request full payment history from the Weixin Pay account

3.4 Data Acquisition

We want to acquire the maximum amount of information from the device so that we can understand how much information is left on the phone locally using the WeChat app. We performed a full image acquisition of the phone in Magnet Axiom Process, having root access guarantees Magnet Axiom Process that the full image acquisition was successful.

3.5 Forensic Analysis

In the analysis stage, we processed the image in Axiom Examine and analyzed the artifacts using both the auto-carved artifacts and the manually carved artifacts

of the file system. In addition, we took a close look at the database that stores messages. An enormous amount of chat messages are stored inside that database file, which is a gold mine for forensic investigators. However, the database was encrypted, we needed to crack the database file. Zhang and Yin [15] declare that manual decryption of the WeChat database file is possible, as long as we obtain the WeChat database file, the uin value, and the IMEI serial number. The MD5 value of the IMEI serial number and the uin value are the decryption key. However, this method does not apply to all phones.

4 Results

This section presents the findings of the study and explains the findings in detail. A summary of the findings is organized in Table 2. Due to the nature that it is a communication app originally developed by a Chinese company, some carved files contain Chinese characters. Before diving into the details, an analysis of the file structure was performed. The full path and the primary artifacts are listed in Table 1.

Table 1. List of Behaviors and Recovered Artifacts

Artifact Path	Artifact Description
`\data\data\com.tencent.mm\MicroMsg\ab84a9f6209480113c856a38b719582e\EnMicroMsg.db`	The database stores message information
`\data\data\com.tencent.mm\MicroMsg\mmslot\webcached\`	Stores articles posted by followed official account
`data\data\com.tencent.mm\MicroMsg\ab84a9f6209480113c856a38b719582e\TextStatus.db`	A database stores status information
`\data\data\com.tencent.mm\MicroMsg\ab84a9f6209480113c856a38b719582e\SnsMicroMsg.db`	Stores moment post information
`\data\data\com.tencent.mm\files\mmkv\`	Stores memory synced data
`\data\data\com.tencent.mm\MicroMsg\ab84a9f6209480113c856a38b719582e\avatar\`	Stores contact avatars
`\data\data\com.tencent.mm\cache\ab84a9f6209480113c856a38b719582e\finder\avatar\`	Stores creator avatars of viewed videos
`\data\data\com.tencent.mm\cache\ab84a9f6209480113c856a38b719582e\finder\image\`	Stores image clips of viewed videos

4.1 Registered Credit Card

Two credit cards were registered in the WeChat account. When the cards were registered, additional personally identifiable information was required, such as legal name, gender, passport number, etc. Among these data, only part of the credit card information was found: bank type and card tail (last four

Table 2. List of Behaviors and Recovered Artifacts

Behavior	Artifacts Recovered
Registered Credit Card	Partial
Money transfer between friends	Yes
Red packet sent between friends	Yes
Official account service receipt	Yes
Official account service details	No
Third party service receipt	Yes
Third party service details	Yes

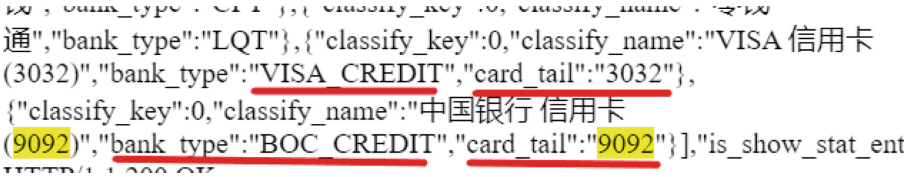

Fig. 2. Information of credit cards

digits of the card number). The carved information is shown in Fig. 2. This data is located in the path `\data\data\com.tencent.mm\cache\Default\HTTPCache\0c45d524731a6b5f_0`. No personally identifiable information was found.

4.2 Money Transaction with Friends

The money transaction between friends can take two forms: red pocket and money transfer. The two forms of monetary transactions were captured in the `EnMicroMsg.db` database file, under the path `\data\data\com.tencent.mm\MicroMsg\9d8d3de00f8797d8e2f4d 83d76640a5d`".

For money transfer, the sent time, the received time, the amount, the sender and the receiver username were retrieved as shown in Fig. 3. The money transfer remained in uncollected status for two hours and WeChat automatically generated a reminder message in the chat room to remind the uncollected transaction. This screenshot of the autogenerated reminder message is shown in Fig. 4.

The red packet is shown in Fig. 5, the sent time, received time, and memo were able to be retrieved in the `EnMicroMsg.db` database file as well. However, the text does not include the transaction amount.

4.3 Money Transaction with Corporate Account

A corporate account was followed that specializes in entertainment personality tests. The account offers paid services. To access a test, a description article was first viewed. At the bottom of the page, the "one-click

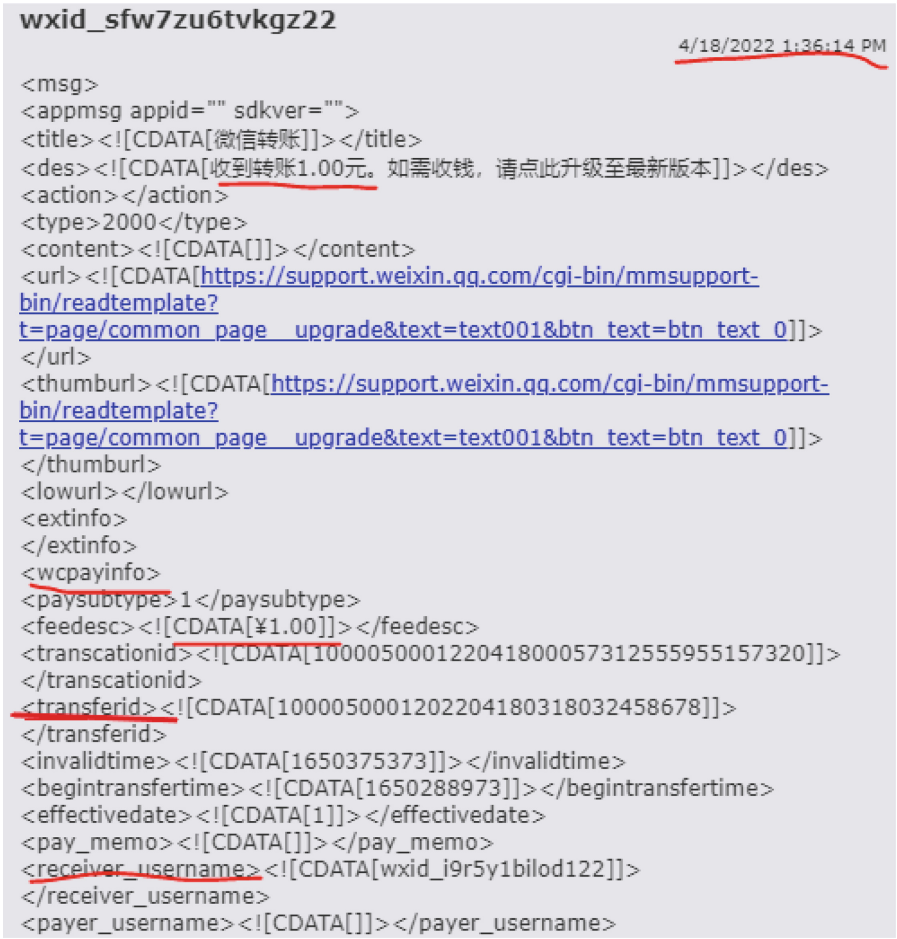

Fig. 3. Message of monetary transfer

purchase" button was clicked to complete the purchase. On the path `\data\data\com.tencent.mm\MicroMsg\mmslot\webcached\900\0\1833744_content_matched___biz:MzU3MTkxNTExMg==-mid:2247491051-idx:4-`, the article was found. The recovered metadata are the corporate account nickname, the title of the article, and the description of the article as shown in Fig. 6. The article was written in Chinese, and the metadata stayed in Chinese characters. It did not provide an English translation, but all viewed articles are cached in the same folder.

The corresponding payment receipt was also found on the path `\data\data\com.tencent.mm\MicroMsg\9d8d3de00f8797d8e2f4d83d76640a5d\EnMicroMsg.db`. The WeChat pay account automatically generates a message to the user with timestamp and amount (see Fig. 7).

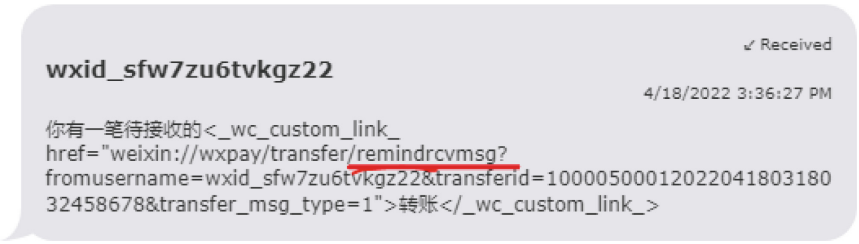

Fig. 4. Reminder message of transfer waiting

Fig. 5. Messages exchanges of red packet (Color figure online)

4.4 Money Transaction with Services Function

The service used was a movie ticket vendor and a movie ticket was ordered. The Service Notification account, an official WeChat account in charge of third-party service messages, was sending information to the user. The conversation was located in the `EnMicroMsg.db` database file as shown in Fig. 8. The notification message contains the timestamp, movie name, movie time, seat information, and movie theater. However, all information was delivered in Chinese and no corresponding English translations were found. It is also worth noting that the timestamp is a few seconds later than the exact time at which the payment transaction took place.

Another message was received from the WeChat Pay account, shown in Fig. 9. This message is a digital payment receipt with the timestamp, the amount paid, and the last 4 digits of the credit card used.

Fig. 6. Metadata of corporate article

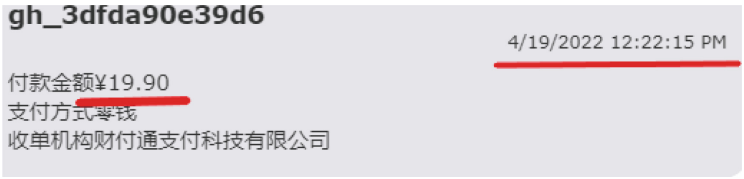

Fig. 7. Receipt message of the corporate service

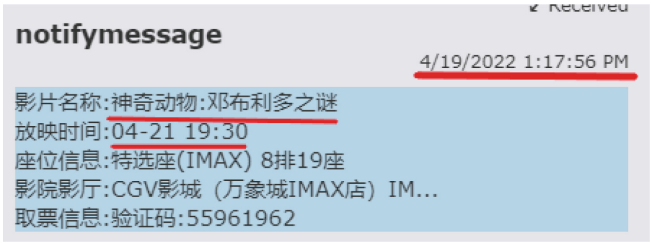

Fig. 8. Notification of third party service

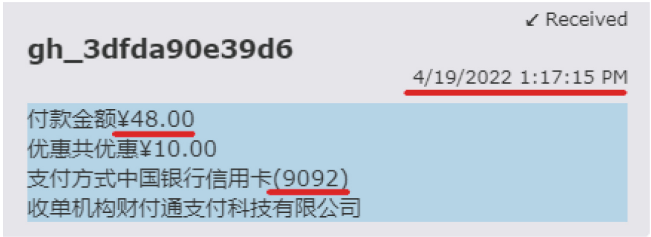

Fig. 9. WeChat Payment account notification

Fig. 10. WeChat Payment account notification

4.5 Full Transaction History

The full transaction history was requested in the WeChat Pay account. The history displays all money transactions with personal and business accounts. It was attempted to retrieve the full transaction history of the WeChat Pay account. However, we were unable to find them. Only receipt messages were retrieved. Although it may seem similar, the full transaction history and receipt messages are different. Full transaction history composed of all monetary transactions that happened in this account. WeChat Pay account has receipt messages for all business-purpose payments in the `EnMicroMsg.db` database file as shown in Fig. 10.

5 Conclusion and Future Work

WeChat app is one of the most popular instant messaging apps in the world, and the company aims to build the app as a multi-purpose platform. The payment feature was launched and loved by the Chinese community due to its easy and real-time operation. Unfortunately, the two features also became the reason scammers pay attention to the app. Furthermore, WeChat does not provide a detailed explanation of its features and updates. It is extremely difficult for beginners to understand the scope of the app and the available functions. Moreover, because it is a product of a Chinese company, much of the information is written in only Chinese. These reasons set a high bar for investigators when a case involves WeChat. This study fills the gap by performing an analysis of the WeChat payment feature on Android. The structure of the data and the identified artifacts can help investigators better locate forensic artifacts from the Android device. The results show that `EnMicroMsg.db` is a critical file that contains a large number of payment transaction records and payment receipts. For personal payment transactions, the red packet and the money transfer can be differentiated. The red packet option contains the keyword "red packet". The money transfer option has its transfer id and the transfer amount. Both options can retrieve the sent time, received time, sender username, and receiver username. For corporate service, the viewed articles were able to be retrieved with the payment receipt. For the third-party service, two pieces of evidence were able to be found, service details and the receipt. The service details, including time, event and location, were able to be found. The receipt contains the amount paid, the timestamp and the last four digits of the card. Although the full payment history could not be found, the list of business purpose payments history was found with the amount and timestamp.

Future extensions of this study can test other WeChat platforms, such as Windows, MacOS, and the iPhone. Another direction can be the cloud analysis, which may provide additional information such as third-party services and mini programs. Some data are only stored on the third-party server. In addition, other features such as floating articles, channels, and shaking are worth looking at. These features could reflect the location, interest, and social interactions of the user. This information can offer valuable forensic artifacts to investigators.

References

1. Mobile devices (2017). https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/cftt-technical/mobile
2. WeChat privacy policy (2022). https://www.wechat.com/en/privacy_policy.html
3. Azfar, A., Choo, K.K.R., Liu, L.: An Android communication app forensic taxonomy. J. Forensic Sci. **61** (2016). https://doi.org/10.1111/1556-4029.13164
4. Iqbal, M.: WeChat revenue and usage statistics. Business of Apps (2022). https://www.businessofapps.com/data/wechat-statistics/

5. Kao, D.Y., Wang, T.C., Tsai, F.C.: Forensic artifacts of network traffic on WeChat calls. In: 2020 22nd International Conference on Advanced Communication Technology (ICACT), pp. 262–267 (2020). https://doi.org/10.23919/ICACT48636.2020.9061437
6. Menahil, A., Iqbal, W., Iftikhar, M., Shahid, W., ul Hassan, K., Rubab, S.: Forensic analysis of social networking applications on an Android smartphone. Wirel. Commun. Mob. Comput. **2021**, 1–36 (2021). https://doi.org/10.1155/2021/5567592
7. Nancy: The WeChat scams sweeping Asia. HackerNews (2019). https://myhackernews.com/blog/the-wechat-scams-sweeping-asia/
8. Park, E., Kim, S., Kim, J.: Analysis of WeChat Messenger on Windows and Android platforms. In: Digital Forensics Research, vol. 14, pp. 205–220 (2020)
9. Rathi, K., Karabiyik, U., Aderibigbe, T., Chi, H.: Forensic analysis of encrypted instant messaging applications on Android. In: 2018 6th International Symposium on Digital Forensic and Security (ISDFS), pp. 1–6 (2018). https://doi.org/10.1109/ISDFS.2018.8355344
10. Sihombing, H.C., Fajar, A.N., Utama, D.N.: Instant messaging as information goldmines to digital forensic: a systematic review. In: 2018 International Conference on Information Management and Technology (ICIMTech), pp. 235–240 (2018). https://doi.org/10.1109/ICIMTech.2018.8528089
11. Silla, C.: WeChat forensic artifacts: Android phone extraction and analysis (2015)
12. Wu, S., Sun, W., Liu, X., Zhang, Y.: Forensics on Twitter and WeChat using a customised Android emulator. In: 2018 IEEE 4th International Conference on Computer and Communications (ICCC), pp. 602–608 (2018). https://doi.org/10.1109/CompComm.2018.8781056
13. Wu, S., Zhang, Y., Wang, X., Xiong, X., Du, L.: Forensic analysis of WeChat on Android smartphones. Digit. Invest. **21** (2017). https://doi.org/10.1016/j.diin.2016.11.002
14. Yan, F., et al.: Identifying WeChat red packets and fund transfers via analyzing encrypted network traffic. In: 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), pp. 1426–1432 (2018). https://doi.org/10.1109/TrustCom/BigDataSE.2018.00198
15. Zhang, C., Yin, J.: Research on security mechanism and forensics of SQLite database. In: Sun, X., Zhang, X., Xia, Z., Bertino, E. (eds.) ICAIS 2021. CCIS, vol. 1423, pp. 614–629. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-78618-2_51
16. Zhang, L., Yu, F., Ji, Q.: The forensic analysis of WeChat message. In: 2016 Sixth International Conference on Instrumentation Measurement, Computer, Communication and Control (IMCCC), pp. 500–503 (2016). https://doi.org/10.1109/IMCCC.2016.24
17. Zhou, F., Yang, Y., Ding, Z., Sun, G.: Dump and analysis of Android volatile memory on WeChat. In: 2015 IEEE International Conference on Communications (ICC), pp. 7151–7156 (2015). https://doi.org/10.1109/ICC.2015.7249467