Forensic Analysis of Blue Talk (Random Chat)

Francis Manna1, Animesh Kumar Agrawal

National Forensic Sciences University, Gandhinagar, Gujarat, India

Corresponding author: Francis Manna1, Email: mannafrancis8@gmail.com

Android forensics has evolved over the years; with new opportunities comes a variety of new challenges. Being open-source, the Android platform allows developers to contribute to the fast-growing Android market. However, users of Android smartphones may be unaware of the security and privacy consequences of installing applications on their mobile devices. Android applications (apps) use a permission strategy where permissions govern access to certain APIs. Unfortunately, no internal verification method is available to prevent applications from seeking too many or fewer permissions, leading to privacy issues. When applications request too many permissions, users are exposed to avoidable threats. Blue Talk (Random Chat), a social networking smartphone application, is one such popular app available on the Android play store that saves a lot of user data, which can be extracted and used as potential forensic evidence. This study describes how forensic investigators can use Blue Talk (Random Chat) on the Android platform to obtain useful information. The extraction and analysis of artifacts and the application's permission and vulnerabilities on an Android device are the key focus areas in the research.

Keywords: Artifacts, Analysis, Permission, Android Forensics

2023. In Saroj Hiranwal & Garima Mathur (eds.), *Artificial Intelligence and Communication Technologies*, 83–89. Computing & Intelligent Systems, SCRS, India. https://doi.org/10.52458/978-81-955020-5-9-8

1. Introduction

Mobile applications are widely used for communication, and social media apps play a great role in modern-day human interactions. These apps allow users to not only share information but also post photographs and videos, chat with other users and take part in real-time events and activities. The latest data has shown that, as of July 2021, about 4.48 billion people are using social media around the world [1]. While the primary goal of social media was to connect people, its anonymous nature has made it a target for criminal activities. Because of the vast number of illegal activities that may be carried out through such platforms, digital forensics is becoming increasingly important in this field. Furthermore, many app developers engage in poor security and data protection practices due to a lack of awareness or expertise. The majority of the users are also unaware of how such applications operate and how their data is handled. As a result, evaluating the security and privacy issues is also getting more complicated.

Blue Talk (Random Chat) is one of the most popular apps in the social networking category on Google Play. It is an Android-based messaging application that allows users to exchange multimedia messages [2]. The large amount of personal data that can be exchanged makes it necessary to evaluate Blue Talk (Random Chat) through the forensic lens [3]. This study looks into the permissions the application has and scans the app for vulnerabilities. The app is further examined to check if any related artifacts of evidentiary importance, could be located and retrieved from the device's internal memory.

Android Permission Model

Permission refers to the privileges granted to the application that wants to access the users' data; they assist in safeguarding user privacy by restricting access to sensitive information. These permission types range from Install-time, Normal, Signature, Runtime, and Special [4]. They determine the extent of restricted data the applications can access and extend of restricted action they can execute. Users who are misinformed and offer too many permissions risk jeopardizing their privacy.

2. Literature Review

Previous research has analyzed a range of android applications including social networking apps, where it was found that many apps failed to implement security mechanisms to secure users' sensitive data, and that forensic analysis can expose essential and relevant information [5]. Efforts were also made to automate the forensic process of analyzing mobile applications to uncover what, where and how sensitive information can be located and retrieved from android devices [6]. Unfortunately, the tool proved ineffective for lesser-known or obscure applications that which Astore ores forensically valuable data. Over the years, social media has emerged as a new area of research in digital forensics. Most social media interactions happen on smartphones and a large number of application artifacts can be stored on these smart devices [7]. Forensic analysis of popular social media apps such as Instagram [8], Facebook, Twitter, Myspace [9], LinkedIn, and Google+ [10] on different mobile devices showed that a substantial amount of the users' activities could be retrieved from iPhones and Android devices. However, no indications of such activities were recovered from Blackberry devices [9]. It was also found that data from Facebook could still be retrieved even after uninstalling the application from the mobile device [11]. Similarly, a wide range of user data including the contact number, messages, and other databases was also extracted from WhatsApp on Android smartphones [12]. Such data retrieved from mobile devices are not limited to rooted phones; instead, a significant amount of information can still be extracted from unrooted devices [13].

While the majority of the studies in this area focused on the forensic identification and recovery of data from the most popular social media apps; this study throws light on a lesser-known but quickly growing social application with equal potential for storing forensically important data. Moreover, it also examines the privacy and security aspects of the application from the standpoint of the users as well as app developers.

3. Research Methodology

The main goal of this research is to look at the Blue Talk (Random Chat) app from a forensic standpoint and identify the various artifacts of evidentiary value. In this study, artifacts from the Blue Talk (Random Chat) application were investigated using qualitative search methods followed by static analysis[14]. Qualitative research focuses on non-numerical data; this research method primarily uses observation, prediction, and interpretation to provide a practical understanding of a subject. The data was recovered from the phone's memory using Autopsy, a standard data recovery tool employing a qualitative method. Static analysis was done with MobSF to check how much permission the application has and Ostorlab mobile security scanner was used to check the application vulnerabilities.

The sequence followed in the research methodology is:

- Resetting the device to factory defaults.
- Installing Blue Talk (Random Chat) app and creating a user account.
- Performing common user's activities through the user account created.
- Putting the device in airplane mode and isolating it by wrapping it in a faraday bag.
- Rooting the device.
- Performing a full acquisition of the device and storing the image on a forensically sterile computer.
- Analyzing the results using Autopsy.
- Static analysis using MobSF.
- Static Analysis using Ostorlab mobile security scanner.

3.1 Experimental Setup

Having the correct laboratory setup is important for the forensic investigation process. A workstation equipped with basic forensic tools as given in Table 1, an Android smartphone with Blue Talk (random chat) installed, a laptop with Windows 10 running,and a USB data cable was prepared. After the setup, common user activities were performed with the exchange of text messages and sending multimedia files (audio, video, and image) through Blue Talk (random chat) social network. After a series of text and media file exchanges, the Android smartphone was placed in airplane mode to prevent it from receiving any more communication or updates.

Table 1. Installed software on a forensically sterile computer

Tool Name	Version	Description
Android SDK Platform-Tools	31.0.2	A tool that lets one communicate with an android device, e.g. moving content to and from the phone.
Magnet ACQUIRE	2.42.0.26725	Used to acquire digital forensic images from android, iOS, removable media, and hard devices
MobSF	v3.4 beta	An open-source tool for evaluating the security flaws in mobile apps
Autopsy	4.18.0	Free tool for hard drives and smartphones analysis with unique features to examine multiple cases.
Ostorlab online security and privacy scanner	-	It is a security and privacy scanner for mobile applications and mobile system backbends

The android device was rooted to acquire a full image for analysis. Rooting the device allows superuser permission and privileged control of the device system. Using Android SDK Platform-Tools (ADB) the process of rooting the device is brought out in Figure 1.

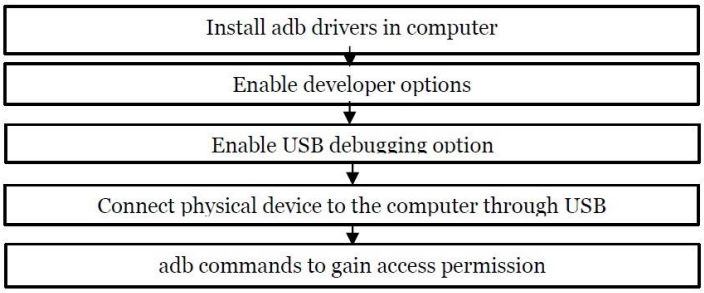

Figure 1. Process Flow

3.2 Logical Acquisition

Using Magnet ACQUIRE a full physical image was extracted of the rooted android device. This forensic tool has a unique user interface with reliable and fast extractions, giving data quickly and easily which will help in gathering maximum evidence in the fastest way possible. The image was extracted and examined with the help of an Autopsy to establish the recoverable artifacts.

3.3 Finding Hidden Files

The acquisition of the app data through the use of Autopsy enabled the identification of crucial SQLite database file "fcm_queued_messages.lb". This file provides substantive information regarding user activities on the mobile device. The path of this database file on the target device is /data/com.google.android.gms/files/fcm_queued_messages.lab. Obtaining these database files from this folder allows gathering details of user activities via the application, which is crucial in forensic investigation. The fcm_queued_messages.ldb database contains essential forensic data concerning user activities, including received messages and the location of the URL on the server which stores the Multimedia file.

3.4 Static Analysis

3.4.1 MobSF

Static analysis was done on the Blue talk apk using MobSF. MobSF examines the permissions of an Android app, assesses its criticality, and provides a description of the permissions without executing the application.

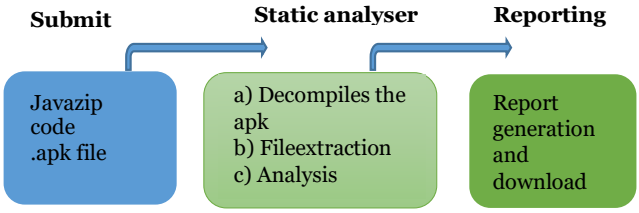

Figure 2. MobSF Static Analyzer Architecture

3.4.2 Ostorlab Security and Privacy Scanner

Multiple approaches are used to uncover vulnerabilities in Ostorlab during static analysis. The static engine looks for passwords, tokens, encryption keys, and hardcoded secrets such as API Keys that shouldn't be used in a mobile app.

4. Results

Blue Talk (Random Chat) offers only user-to-user communication. Users can exchange plain text messages, geolocation data, contacts cards, and multimedia files like images, video, and audio during communication.

4.1 Examination using Autopsy

Blue Talk application was examined using autopsy and the following directories, as shown in Table 2, were discovered.

Table 2: Blue Talk (random chat) Artifacts

Content	Directory	Data
Log files	/data/kr.jungrammer.bluetalk/files/log-files	log-files
App databases	/data/kr.jungrammer.bluetalk/databases	databases
Chat database	/data/com.google.android.gms/files/fcm_queued_messages.ldb	fcm_queued_messages.ldb
App apk	/data/app/kr.jungrammer.bluetalk-1	
App Data	/data/kr.jungrammer.bluetalk	Various files

4.2 Multimedia Message

Various activities take place in the background as soon as the user sends a multimedia file. The multimedia file is copied and uploaded to the Blue Talk (Random Chat) server, where the server functions as an easy way to return the corresponding multimedia URL location. The sender sends the multimedia URL embedded in the message to the receiver, and then the recipient sends an acknowledgment when the URL with the message is received by the recipient. A record is preserved in the sender's message database once the above procedures are finished. The dump in Figure 3 shows the file type. The URL's location on the server that stores the Multimedia file is temporarily stored in the chat database field.

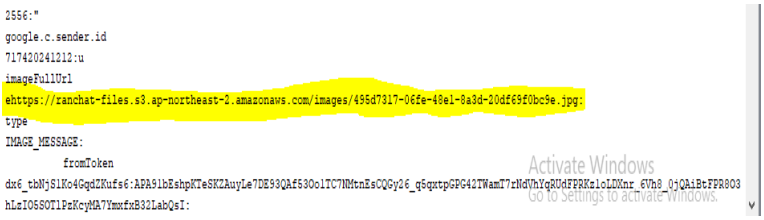

Figure 3. Multimedia URL corresponding to the file

The fcm_queued_messages.ldb database provides meaningful forensic data concerning communication between individuals. Among the details recovered are the sender chat messages as shown in Figure 4.

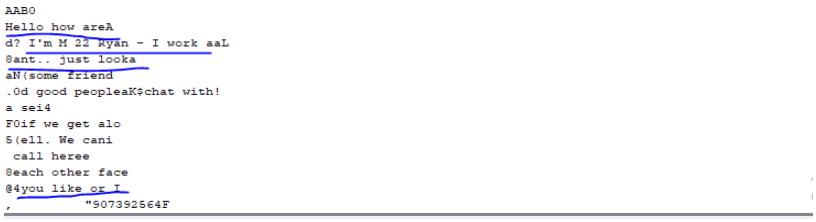

Figure 4. Received messages

From MobSF static analysis, it was discovered that Blue Talk has four dangerous permissions as shown in Table 3.

Table 3. Blue Talk dangerous permission

Permission	Status	Description
WRITE_EXTERNAL_STORAGE	Dangerous	Allow the application to write to the device's external storage
READ_EXTERNAL_STORAGE	Dangerous	Allow the application to read from the device's external storage
RECORD_AUDIO	Dangerous	Audio record path can be accessed by the application
CAMERA	Dangerous	Images taken by the camera can be seen by the application at any time

4.3 Examine App SQLite database

Using Autopsy, the following data of interest as shown in Table 4 was found in the SQLite database "fcm_queued_messages.ldb" after a physical examination.

Table 4. User Activities

Activities Performed	(Found / Not Found)
Login User's ID	Found but without Timestamp
Received chat messages	Found but without Timestamp
Outgoing Messages	Not Found
Sent Images	Found but without Timestamp
Received Images	Found but without Timestamp
Sent Videos	Found but without Timestamp
Received Videos	Found but without Timestamp
Link to send images URL	Found but without Timestamp
Link to received image URL	Found but without Timestamp

From the report of Ostorlab online security and privacy scanner static analysis, the following risks were discovered in the Blue Talk application.

4.3.1 Attribute "hasFragileUserData" not set

When a user uninstalls an app, the android:hasFragileUserData property indicates whether or not the user should be prompted to keep the app's data; "false" is the default value. This value should be explicitly set in the application to indicate whether or not the program is handling sensitive user data.

```
<application xmlns:android="http://schemas.android.com/apk/res/android" android:hasCode="false">
  <meta-data android:name="com.android.vending.derived.apk.id" android:value="3"/>
</application>
```

4.3.2 Backup mode enabled

By default, Android backs up applications, including private files saved on the /data sector. These files are uploaded to the user's Google Drive account by the Backup Manager Service.

```
<application xmlns:android="http://schemas.android.com/apk/res/android" android:hasCode="false">
  <meta-data android:name="com.android.vending.derived.apk.id" android:value="3"/>
</application>
```

4.3.3 Insecure Network Configuration Settings

Android Network Security Configuration allows the user to specify the application's network security. A network security configuration is missing from the application.

5. Conclusion

Blue Talk (Random Chat) has grown in popularity as a social networking application where people may share personal as well as professional information. This study's findings revealed a wide range of users' personal information including User Id, incoming chat messages, multimedia files, URLs, etc., which can prove to be crucial in a forensic investigation. Moreover, from the privacy aspect, four dangerous permissions, as well as existing risks, were identified. According to this study, a person can obtain complete access to all the data in Blue Talk and other similar social networking programs. The strategy used in this study provides a general framework for all of the similar programs that operate on Android devices. The concept described in this study may further be customized to show user-specific information based on an individual's requirements.

References

[1] Global Social Media Stats, https://datareportal.com/social-media-users last accessed 2021/8/1.

[2] APPSFORWINDOWSPC, https://appsforwindowspc.com/download-blue-talk-random-chat-for-pc-windows/ last accessed 2021/8/2.

[3] STE Primo App store, https://steprimo.com/android/us/search/Blue-Talk-Random-Stranger-Chat/ last accessed 2021/8/8.

[4] Android for Developers, https://developer.android.com/guide/platform/ last accessed 2021/9/21.

[5] Kitsaki, T. I., Angelogianni, A., Ntantogian, C., & Xenakis, C. (2018, November). A forensic investigation of Android mobile applications. In Proceedings of the 22nd Pan-Hellenic Conference on Informatics (pp. 58-63).

[6] Xiaodong Lin, Ting Chen, Tong Zhu, Kun Yang, Fengguo Wei, "Automated forensic analysis of mobile applications on Android devices," Digital Investigation, Volume 26, Supplement, 2018, Pages S59-S66.

[7] Agrawal, A. K., Sharma, A., & Khatri, P. (2019, March). Digital forensic analysis of Facebook app in a virtual environment. In 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 660-664). IEEE.

[8] Carolin Alisabeth and Yoga Restu Pramadi, "Forensic Analysis of Instagram on Android Artifacts" IOP Conf. Series: Materials Science and Engineering 1007 (2020).

[9] Noora Al-Mutawa, Ibrahim Baggili, Andrew Marrington, Forensic analysis of social networking applications of mobile devices, Digital Investigation, Volume 9, Supplement, 2012, Pages S24-S33.

[10] Norouzizadeh Dezfouli, F., Dehghantanha, A., Eterovic-Soric, B., & Choo, K. K. R, "Investigating Social Networking applications on smartphones detecting Facebook, Twitter, LinkedIn and Google+ artifacts on Android and iOS platforms", Australian Journal of forensic sciences, vol.48(4), pp.469-488,2016.

[11] M. A. Thebaity, S. Mishra, and M. K. Shukla, "Forensic Analysis of Third-party Mobile Application", Helix, vol. 10, no. 04, pp. 32-38, Aug. 2020.

[12] Echo-Promise, Iyobor, Bamidele Ola, Aaron Arhin, and Richard Assuming. "A Forensic Analysis of WhatsApp on Android smartphone" IRJCS: International Research Journal of Computer Science: AM Publications, I India, 2020.

[13] Agrawal A.K., Sharma A., Khatri P., Sinha S.R.," Forensic of Unrooted Mobile Device", in International Journal of Electronic Security and Digital Forensics, 2019, vol. 12, no.1, pp.118-137.