RETRIEVAL OF DELETED MESSAGE IN WHATSAPP USING DIGITAL FORENSICS

Mahesh K S [1], Nivedita M Hanamasagar[2], Manosree Ramana S[3], Rashmi Babu Moger[4], Kavya R K[5]

[1] Assistant Professor, [2,3,4,5] UG Student,
Department of Computer Science & Engineering, Sri Jayachamarajendra College of Engineering, JSSSTU, Mysore

ABSTRACT

WhatsApp is one of the frequently used apps for Android handsets. WhatsApp can be used inappropriately, including unlawfully. The detectives need to utilize forensic techniques to carry out an investigation utilizing smartphone devices. However, WhatsApp and mobile technology are developing more quickly than the technology behind the forensic tools that are now in use. WhatsApp and mobile devices are constantly updated. In order to manage a case involving Android cellphones and WhatsApp in particular, study on the effectiveness of the current forensic tools must be done. For performing forensic analysis on WhatsApp using WhatsApp artifact, this study examined one of the forensic tools currently available. In this paper, we show how to implement the retrieval of deleted messages in instant messaging applications, that is WhatsApp.

Keywords: - *Cyber Bullying, Digital Forensics, Whatsapp Application*

1. INTRODUCTION

With the availability of numerous communication methods in this Internet era, cyberbullying has grown to be a serious worry. Cyberbullying has found a home on several electronic platforms, particularly Instant Messaging Applications (IMAs) like WhatsApp. The structure of the WhatsApp databases is as follows. The chat database, or msgstore.db, was the first database. As implied by its name, it keeps thorough records of all text and multimedia messages that were sent and received. The three tables that make up msgstore.db are messages, chat list, and sqlite sequence. The contacts database, wa.db, is the second database. Three tables, wa contacts, android metadata, and sqlite sequence, make up most of it. A subfield of forensic science called "digital forensics" is dedicated to finding, obtaining, processing, analyzing, and documenting electronically stored material. Nearly all illegal acts involve the use of electronic evidence, making digital forensics support essential for law enforcement investigations. By demonstrating a mobile application that retrieves any deleted messages, we here suggest a tes ted fix for WhatsApp's "delete for everyone" functionality.

2. PROPOSED SOLUTION METHODS

If the WhatsApp notification reads "The message had been deleted," we look for the content of the deleted message in RAM (random access memory) via Notification Listening Service feature. The last resort is to check the WhatsApp database. Compared to using merely cache or RAM to recover deleted messages, this produces more accurate results.

The application's notification listening service monitors notifications in the background and alerts the user when new messages have been received via the WhatsApp app. It then recovers the content of the deleted message and saves it to a log file if the transmitted message is one that has been deleted.

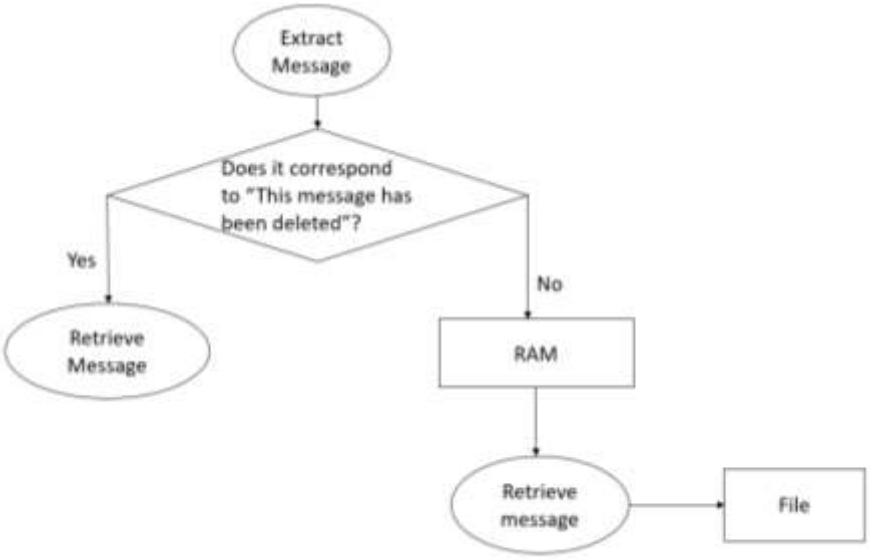

Fig 2.1: Flow Chart

3. IMPLEMENTATION

The project's System Implementation phase is covered in this section. In addition, a thorough explanation of each step is provided in this section. If the WhatsApp notification on the phone says, "The message has been deleted," we inspect the RAM using forensic analysis to see if it contains the deleted message's content. Through a background notification listener, the application monitors the notification bar. The notice is then considered if it comes from the WhatsApp instant messaging service. Additionally, after the deleted communication has been recovered it is then saved with permission.

Implemented are several crucial components like the following: For a user to interact with an application, widgets present information in a particular way. Android text view is only a view that assists in displaying text to the user and also gives us the option to edit it. The local class in the application inherits the built-in classes NotificationListenerService and StatusBarNotification to extract the required messages from the status bar. Kotlin-written software must undergo unit testing.

4. RESULTS ANALYSIS

To analyze the result, we first run the application in the mobile device with the interface as shown below.

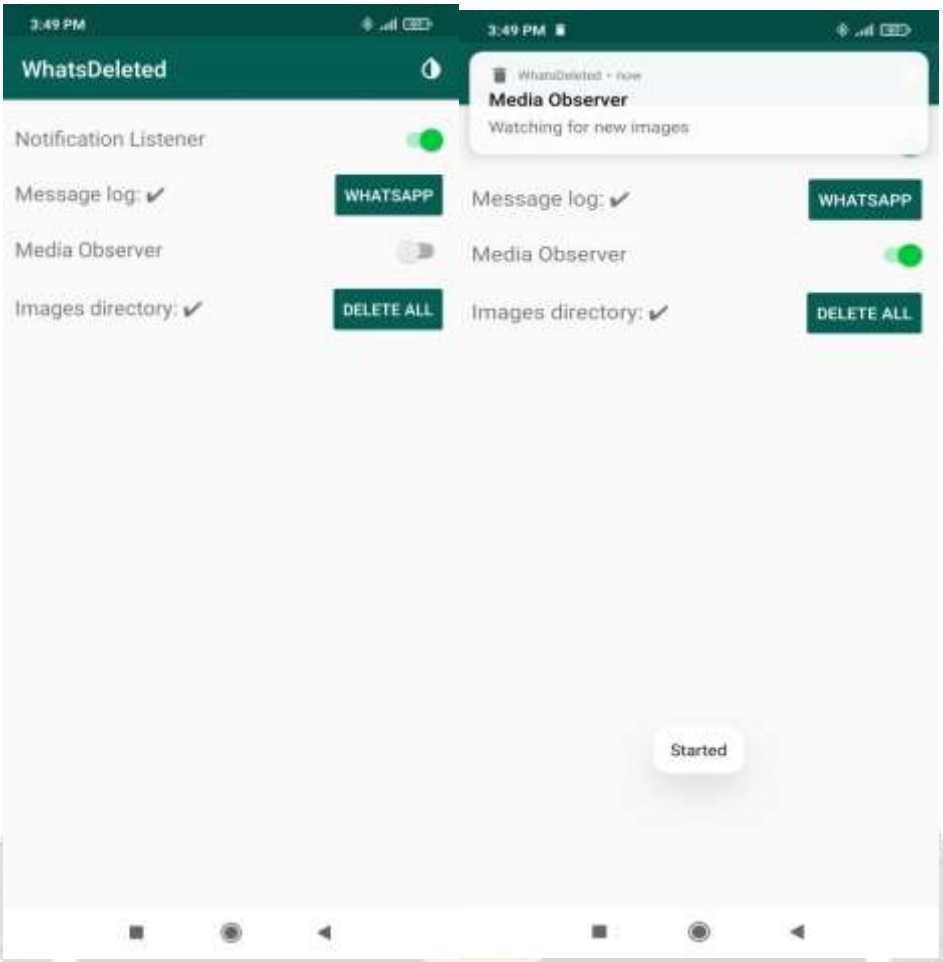

Fig 4.1: Home page of application and same with media observer enabled

For example, we tried to send message and did “deleted for everyone” as shown below,

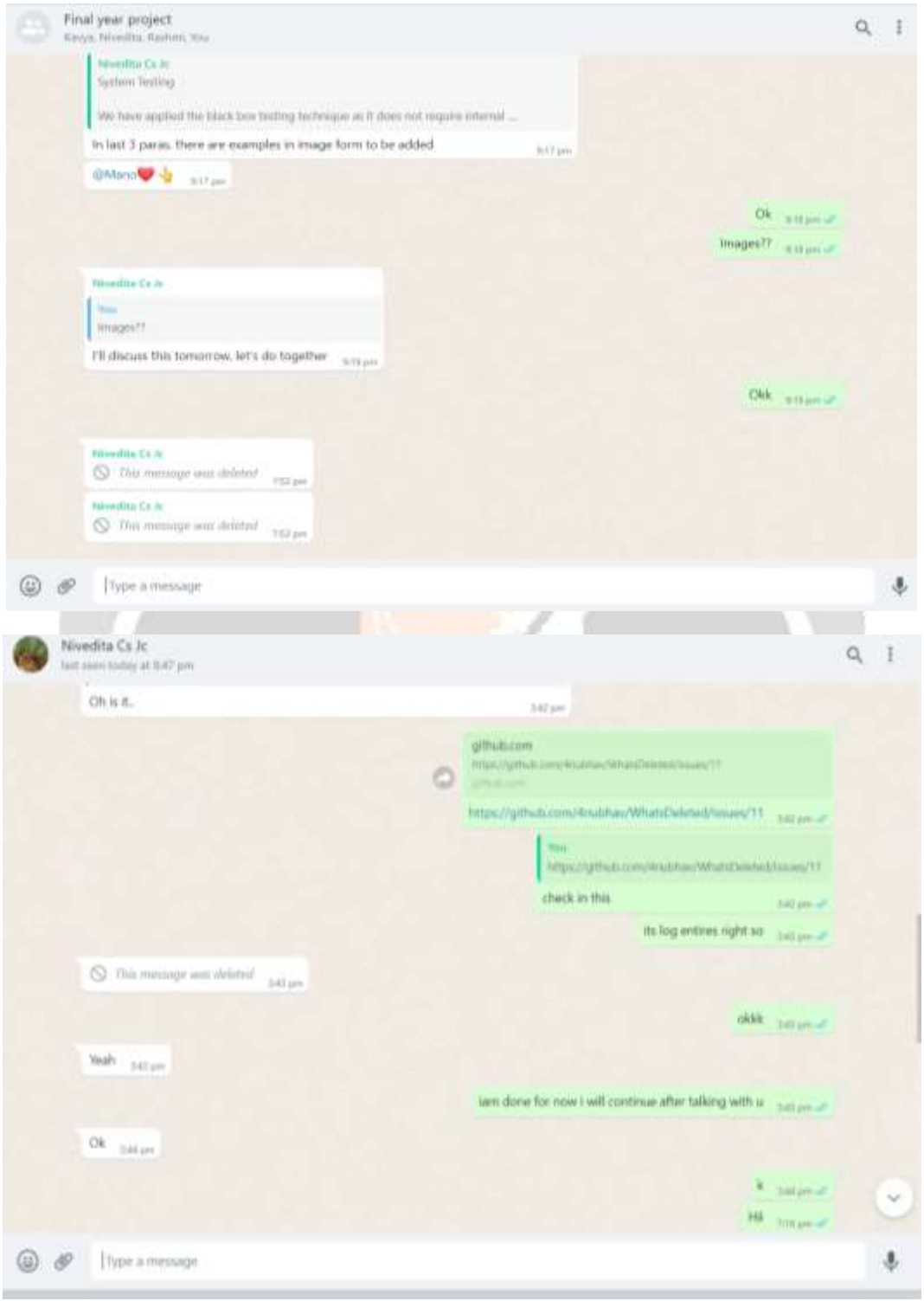

Fig 4.2: Deleted messages in WhatsApp

On execution of this developed application, the obtained results are as follows that can be viewed in the log file as shown.

Fig 4.3: Viewing sent messages in log file

The application developed for retrieval of deleted message when tested for Whats App artifacts data found, following table describes the same,

Data Found	Android
Contact	✓
Text	✓
Deleted Text	✓
Media	×
Deleted Media	×

Table 4.1: WhatsApp artifacts from application

5. CONCLUSION

Cybercrimes committed via IMAs have dramatically increased in number. This study examined IMA's forensic investigations' anti-forensic problems. Even though WhatsApp is among the most widely used applications in comparison to other online messaging services, we have identified a privacy vulnerability in WhatsApp that could provide further difficulties for the community of digital forensics. In order to lessen cyberbullying, the tool also retrieves deleted messages from WhatsApp.

6. FUTURE WORK

As for our future work, it is intended to continue researching additional potential anti-forensic tactics on Android and iOS in addition to working on creating an open-source digital forensics solution that recovers the majority of the digital evidence related to the misuse of WhatsApp. We can also restore a recent addition to WhatsApp, known as the recovery of view-only media, which was made available. Our attempt to recover lost texts from instant messaging applications using digital forensics can be extended to include recovering deleted media like photographs and movies first. Second, there is room for future work with WhatsApp's recently adopted View Only Once capability for media retrieval. Thirdly, built applications may support other applications like Signal that allow users to view deleted communications.

7. REFERENCES

[1]. Rusydi Umar, Imam Riadi and Guntur Maulana Zamroni, “A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements” International Journal of Advanced Computer Science and Applications(IJACSA), 8(12), 2017

[2]. Alissa, K., Almubairik, N.A., Alsaleem, L. et al. A comparative study of WhatsApp forensics tools. SN Appl. Sci. 1, 1320 (2019)

[3]. S. Adwan and F. Salamah, "A Manual Mobile phone forensic approach towards the analysis of WhatsApp Seven-Minute Delete Feature," 2018 21st Saudi Computer Society National Computer Conference (NCC), 2018, pp. 1-5, doi: 10.1109/NCG.2018.8593153.

[4]. A. Shortall and M. A. H. Bin Azhar, "Forensic Acquisitions of WhatsApp Data on Popular Mobile Platforms," 2015 Sixth International Conference on Emerging Security Technologies (EST), 2015, pp. 13-17, doi: 10.1109/EST.2015.16.

[5]. SalvationData, "WhatsApp Forensics: Decryption of encrypted Databases and extraction of deleted messages on non-rooted android devices", 2018

[6]. M. M. Mirza, F. E. Salamh and U. Karabiyik, "An Android Case Study on Technical Anti-Forensic Challenges of WhatsApp Application," 2020 8th International Symposium on Digital Forensics and Security (ISDFS), 2020, pp. 1-6, doi: 10.1109/ISDFS49300.2020.9116192