IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 11, November 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.524

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311024|

Android Log Extraction for Digital Forensic: A Review on Android Log Extraction Tool

Sharad Jadhav, Krishna Kondhare, Shivam Mulik, Jyotiraditya Panchal, Mahesh Kale

Assistant Professor, Department of Computer Engineering, DYPCOEI, Varale, Pune, Maharashtra, India

U.G. Student, Department of Computer Engineering, DYPCOEI, Varale, Pune, Maharashtra, India

U.G. Student, Department of Computer Engineering, DYPCOEI, Varale, Pune, Maharashtra, India

U.G. Student, Department of Computer Engineering, DYPCOEI, Varale, Pune, Maharashtra, India

U.G. Student, Department of Computer Engineering, DYPCOEI, Varale, Pune, Maharashtra, India

ABSTRACT: At the moment, a forensic specialist does understand that they are standing in a 'data ocean'—so m much rich and complicated information, the Marine laptop is particularly managing the information gathering noble. Among the reasons for the delays in performing these investigations are the traditional techniques used to analyze the Android logs; these tools are very meticulous and mostly time-consuming. This research presents an Android log extraction tool that provides an alternative method of extracting log files through ADB and Logcat, as opposed to manual extraction, and this tool reduces the following scientific work. The solution improves processes when log data is automatically extracted and presented, despite the integrity of the data being of utmost importance. It also mitigates concerns on legal and ethical matters. The tool has been demonstrated through various case scenarios of field investigations. This paper is targeting the traditional forensic techniques and the changes that must be implemented to achieve timely and cost-effective forensic techniques.

KEYWORDS: Android forensics, ADB, Logcat, Mobile forensics, Log extraction, Data integrity, Digital forensics.

I. INTRODUCTION

The examination of digital evidence, and particularly smartphones, is becoming more and more significant in the prosecution of crimes thanks to the use of advanced technologies [1]. These devices record a great deal of information on system and user activity, running applications, and the ensuing errors, which can be used as evidence in court. Nevertheless, it requires significant resources to carry out log retrieval and analysis since it is time-consuming and requires specialists [2]. Investigators have to assess the Android operating system and implement measures to collect data, which may include manual approaches that are also hefty and interfere with the process. Not only is the issue of resolving this tension central to all forensic work, but it is also resolving the issue of providing protection for the extracted data from tampering and other illegal use. The goal of this project is to improve the efficiency and effectiveness of the process for obtaining log files from Android devices using Android Debug Bridge and Logcat, which are tools available to developers but are not widely applied in forensic procedures. ADB facilitates easy interactions between a personal computer and the Android device, and Logcat allows for accessing system logs on the device in real time. Further in this paper, we are going to describe the application that is able to perform these processes without any interaction from the operator, with no skills required for this task, and in a more structured way. This development does not only cut on the time needed to undertake the tasks but also lowers chances of making mistakes in the process of extracting and analyzing [3]. The present forensic investigators' methods for Android log extraction are prone to a lot of errors, and this tool can help change this for the better.

II. LITERATURE SURVEY

Owing to its popularity and data generation ability, the Android gadget has played a significant role in current-day digital forensics. For these investigations, the studies considered a number of different forensic approaches designed to capture and process logs from such devices. Azfar et al. (2015) described the state of the art in the review paper on the 2012/13 phones voip Turkey mobile and explained the garnered artifacts for the forensics from mobile phones [5]. undertake the tasks but also lowers chances of making mistakes in the process of extracting and analyzing [3]. Vidas

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311024|

and Christin (2018) provided such a collection methodology that focused the attention of the forensic examiner towards the gathered evidence concerning Android devices [4]. Their efforts have prepared a ground toward the development of ADB and Logcat, which assist the process of log structuring. Kessler and Liles (2021) advocates of E for droid phone forensics were recent public release results of OMs published research paper that split [3]. The paper integrated data collection strategies into other frameworks that have also been adapted to facilitate communications while collecting data. Further, Mahajan and Dahiya (2014) also studied the forensic exploration of the instant messenger (IM) applications on the Android platform (review paper final). Their work again revealed how logs are helpful in finding out essential information for the purpose of digital investigation. To review these techniques in particular, add a software product that uses ADB and Logcat in order to simplify the synthetic process of log collecting from the Android devices. The objective of the tool is to automate such a task in order to improve the quality of forensic analysis by increasing the effectiveness without compromising the quality of logs obtained.

III. METHODOLOGY

The core technologies used in Android Log Extraction Tool include:

A. Android Debug Bridge (ADB):

• Function: ADB is a command-line interface used for data exchange and information management between a desktop computer and any mobile device powered by Android, among other uses.
• How It Works: Android Debug Bridge requires USB debugging to be enabled in the device settings. After being connected, ADB commands are sent to various functions and retrieve and manipulate various logs, as well as copy files to and from the device [4].
• Purpose in Tool: As described, ADB will serve the purpose of obtaining an Android device from a remote access point to be able to initiate the processes of retrieving device log data.

B. Logcat:

• Function: Logcat is the tool in the Android SDK for recording the system log and any application's errors and disease in real time [6]. It gathers system information to retrieve error warnings and other constituents during the execution phase that adds value to forensic information.
• How It Works: Logcat retrieves log entries from the circular buffer available on the device. Kernel messages, system logs, and application logs reveal the chronological log entries at constant intervals.
• Purpose in Tool: Logcat is intended to be a sweep of panic to gather the forensic logs required to perform a device impersonation. It shall be done in combination with ADB for the purpose of fetching logs in an automatic manner.

C. PC Interface (Frontend Application):

• Function: An intuitive graphical interface that makes it possible for the user of the tool under investigation to operate the tool without acquiring technical ADB or Logcat commands knowledge as well as skills.
• How It Works: The user interface is a basic graphical user interface (GUI) optionally implemented in Python (using Tkinter or PyQT) or Java (using Swing or JavaFX) [7]. The frontend will execute the procedures required to establish a connection with the device, retrieve the logs, and prepare the reports.
• Purpose in Tool: Makes it easier to work with a forensic utility, allowing users to quickly retrieve logs and demonstrate findings.

D. File Handler:

• Function: An instrument that organizes the retrieved logs into available formats (bay forms) and deals with their proper custody awaiting future exploration [8].
• How It Works: Within the file handler module, log files are handled as being transferred and secured in some permanent form that cannot be altered blamelessly with options of encryption and hashing of contents for verification.
• Purpose in Tool: To ensure that the information is untouched and hence ensures that log data is reported and stored in a safe manner.

E. Report Generator:

• Function: Upon completion of log extraction, the report generator automatically compiles the pertinent data into legible and comprehensive reports for investigators.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311024|

• How It Works: Raw logs are generated by the generator but re-formatted into easier and more appealing formats (pdfs or web pages) ready for scratches by the users, although all the logs are properly arranged. It may include specific triggers, like alarm settings during the preparation of logs, such as errors or abnormalities in the logs.
• Purpose in Tool: Substantiates the circumference of the logs process offered for examination by the data extraction and gives results that are timely approximated on conclusions and are available for further usage as an element of a forensic examination.

F. System Architecture:

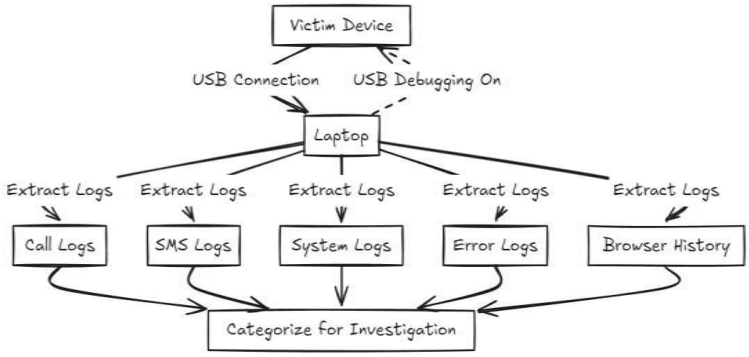
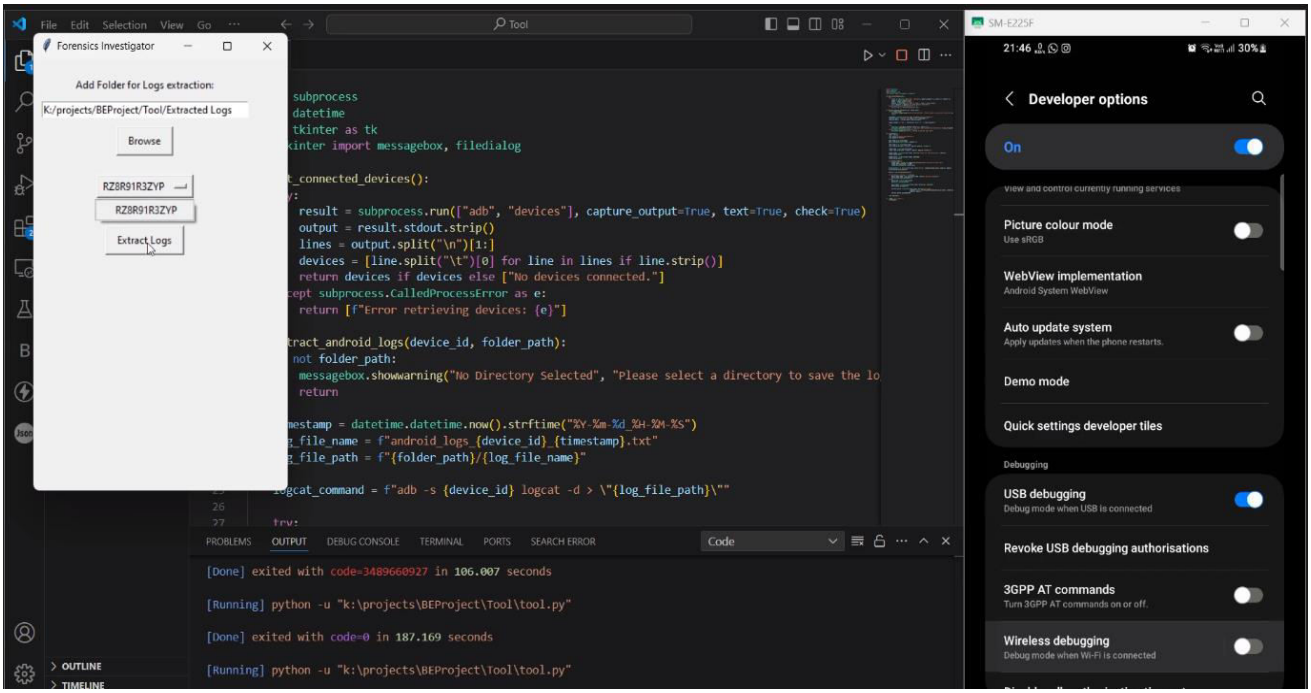


Fig.1. System Architecture

IV. EXPERIMENTAL RESULTS



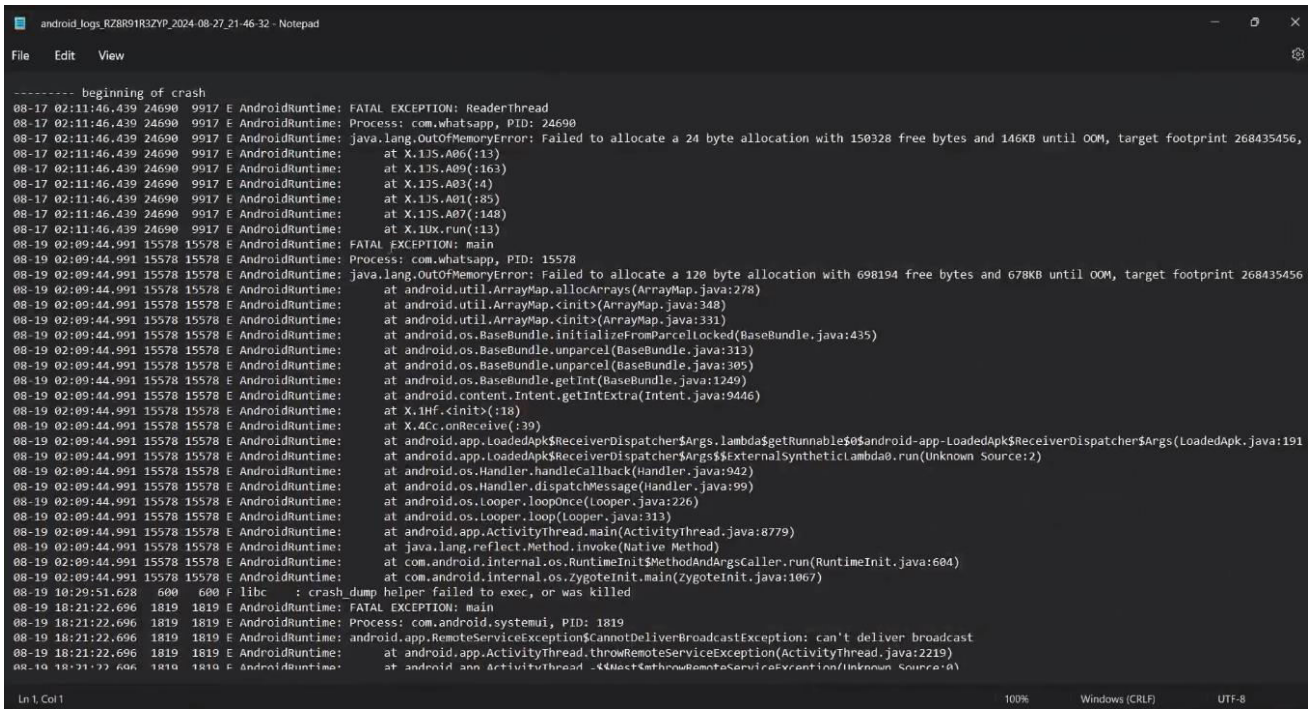
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311024|



V. FEASIBILITY AND CHALLENGES

The viability of this project is great because Android Debug Bridge (ADB) and Logcat are often used tools in the process of developing Android applications [10]. ADB enables the user to directly access and control Android devices, while Logcat records the system log in real-time. However, several challenges remain, including:
1) Cost-effective: The work is focused on the use of available free programs (ADB and Logcat) that do not overcome the budgetary parameters of the project [6]. The tool will be provided to law enforcement organizations free of charge, which will eliminate economic constraints on forensic departments of the organizations, especially those that are poorly funded.

2) Quick Time Frame: Log retrieval has been computerized, thereby shortening the time taken to extract such information compared to sitting out or typing it out; this enables forensic experts to concentrate on analysis rather than cumbersome information accumulation tasks.

3) Lower Hardware Requirements: The application does not require any sophisticated hardware equipment apart from a regular computer and a USB output for the Android device, making it easy to deploy for forensic units that have limited resources [11].

4) Legal and Ethical Issues: The application will be designed with regard to data protection laws in that there will be policies and limits on how the tool will be used to ensure that legal and moral principles are followed.

VI. CONCLUSION

The project's objective is to develop an effective, convenient, and trustworthy device for Android log extraction that would serve forensic specialists. The complexity of this tool eases the process of log extraction and analysis and enables forensic specialists to devote their attention to the most important tasks in a timely manner. In addition, its use is characterized by compliance with legal and ethical standards, which guarantees that the available evidence is gathered and handled to meet the legal provision. Thank you for taking the time to read this. Such continued work may focus on incorporating similar tool enhancements to support additional data extraction and analysis tasks and be compatible with more devices and Android OS versions.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311024|

REFERENCES

1. H. Mahalik and D. Crognale, "FOR585: Smartphone Forensic Analysis In-Depth," SANS Institute, 2023.
2. C. C. Cheng, C. Shi, N. Z. Gong, and Y. Guan, "LogExtractor: Extracting Digital Evidence from Android Log Messages via String and Taint Analysis," Forensic Science International: Digital Investigation, vol. 36, 2021.
3. J. L. a. G. C. Kessler, "Android Forensics: Simplifying Cell Phone Examinations," Journal of Digital Forensics, Security and Law, vol. 7, 2021.
4. C. Z. a. N. C. T. Vidas, "Toward a General Collection Methodology for Android Devices," Digital Investigation, vol. 8, Aug. 2018.
5. K.-K. R. C. a. L. L. A. Azfar, "Android Mobile VoIP Apps: A Survey and Examination of Their Forensic Artefacts," Digital Investigation, vol. 12, Mar. 2015.
6. D. Q. a. K.-K. R. Choo, "Pervasive Social Networking Forensics: Investigation of an Android-Based Instant Messaging Application," Digital Investigation, vol. 10, May 2014.
7. M. D. a. H. S. A. Mahajan, "Forensic Analysis of Instant Messenger Applications on Android Devices," Advances in Computer Science: An International Journal, vol. 2, May 2014.
8. D. Q. a. K.-K. R. Choo, "Digital Forensics for Cloud Computing: A Perspective of Internet Investigators," Digital Investigation, vol. 10, Feb. 2013.
9. A. C. L. M. a. G. G. R. I. J. Sylve, "Acquisition and Analysis of Volatile Memory from Android Devices," Digital Investigation, vol. 8, Sept. 2012.
10. E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 2011.
11. J. H. D. G. a. P. A. M. Taylor, "Forensic Investigation of Cloud Computing Systems," Network Security, vol.11, Mar. 2011.
12. B. P. a. G. M. A. Distefano, "Android Anti-forensics Through a Local Paradigm," Aug. 2010

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details