International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

A FORENSICS ACTIVITY LOGGER TO EXTRACT USER ACTIVITY FROM MOBILE DEVICES

K.Venkatesh[1], K.Anusha[2], T.yashaswini,[3], M.Uma Rani [4]

[1] Assistant Professor, Department of IT ,Malla Reddy Engineering College For Women(Autonomous Institution), Maisammaguda, Dhulapally,Secunderabad,Telangana-500100

[234]UG Scholar, Department of CS,Malla Reddy Engineering College for Women, (Autonomous Institution), Maisammaguda,Dhulapally,Secunderabad,Telangana-500100
Email id: venkatesh.kummara@gmail.com

ABSTRACT

Mobile devices have come to be an essential tool of today's life, as their purposes include communication, being effective at work, or in other words, for productivity or entertainment. While serving day-to-day needs and performing functions, they can collect and store large amounts of personal data about users, which makes them vital evidence resources in investigations. However, tools primarily focus on isolated data concerning various applications or activities but have no idea of their comprehensive user behavior. This prevents investigators from having a holistic view of the interactions a user has with his device. To fill this gap, this paper introduces a new forensic tool that will generate an integrated report and timeline of all activities conducted on mobile devices. This tool, which aggregates data from a wide variety of sources, can help investigators trace events and interactions with much more ease. This solution integrates datasets, such as application usage, system logs, and user activities, into a single coherent framework.In order to illustrate the functionality of the tool and the potential application in real-world scenarios, a practical example has been included. The results here point out the tool's feasibility, usability, and value in streamlining the workflow of investigations. This tool, through its consolidated approach, allows investigators to unwind patterns and insights otherwise hidden within fragmented datasets, thereby improving the efficiency of digital forensic investigations.

Keywords :Digital forensics, mobile devices, activity tracking, data integration, Android, investigation tools.

I. INTRODUCTION

Mobile devices have become indispensable in modern life, performing a wide range of functions such as communication, entertainment, education, research, socialization, and commercial transactions. Their pervasive use results in the storage of substantial amounts of data related to user behavior, making these devices critical sources of digital evidence in forensic investigations. Digital forensics is the process of collecting and extracting data from a device without modifying the original state. It may be able to retrieve deleted files, browsing history, messaging details, login passwords, and many other kinds of data together termed as digital evidence. Forensic analysis requires strictly adherence to three key principles; avoid contamination of evidence by avoiding misinterpretation; systematic documentation of all processes in order to ensure that the chain of custody is maintained using standardized protocols. Furthermore, legal considerations, which are jurisdiction-dependent, must be followed to maintain confidentiality of personal information while preventing legal violations.

Forensic tools and applications available to support analyzing mobile devices include EnCase, DFF, FTK, Helix, Oxygen, MOBIL Edit, and UFED, among others.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

The use of these forensic tools enables an investigator to explore many different elements, for instance, memory, applications, and messages, and the following functions can be undertaken: data recovery, keyword searches, and the creation of a forensic image. While commercial tools offer vast abilities and strong features, they are often not used, as open-source tools are viewed as more cost-effective and transparent and easier to have verified in court. Considering the variety of tools existing, no solution provides a comprehensive log of user actions on a mobile device. In several cases, investigators have had to use multiple tools just to gather all the necessary information, which complicates the forensic process.

To bridge this gap, this paper introduces a tool developed in Python that consolidates information from multiple applications on Android devices into a single, unified report. This tool allows investigators to trace user activities and behaviors effectively, providing a holistic view of digital interactions. The paper is categorized into the following sections: Section 2 discusses the related work, Section 3 explains the development process of the proposed solution, Section 4 details the operation of the activity logger, Section 5 elaborates on the implementation of the forensic tools, Section 6 applies the proof of concept to analyze digital data, and Section 7 concludes the paper with insights and directions for future work.

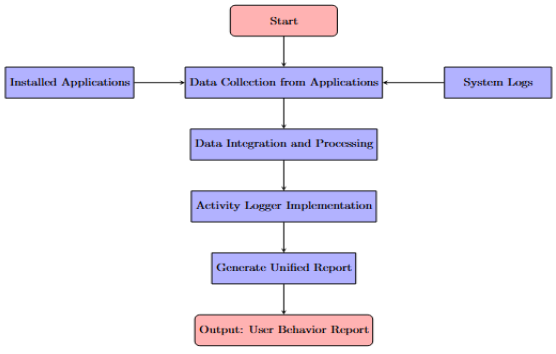

Fig 1: System Architecture

II. RELATED WORK

1.Tse, H. K. S., Chow, K. P., & Kwan, M. Y. K. (2014)
Title: The next generation for the forensic extraction of electronic evidence from mobile telephones

This is on theadvancements regarding mobil eforensic techniques to extract evidence digital from mobilephones. A new method has emerged over the sophistication of mobile systems with mobile application functions. The authors propose that this next-generation approach could adapt to modern technologies as far as data encryption goes, device locking mechanisms and then diversity in mobile platforms are being looked forward in a new way.

2.Barmpatsalou, K., Damopoulos, D., Kambourakis, G., & Katos, V. (2013)
Title: A critical review of 7 years of Mobile Device Forensics

This critical review deals with in-depth analysis on the progress of mobile device forensics made over seven years ago. Its technological progression, challenges, and tools were discussed within a forensic investigation. The discussion also addressed trends related to mobile usage, forensic tools, encryption of data, privacy concerns, the complexity involved in the extraction process of modern mobile devices, as well as legal and ethical aspects of mobile forensics.

3. Di Iorio, A., Sansevero, R., & Castellote, M. (2013) Title: La recuperación de la información y la informática forense: Una propuesta de proceso unificado

This paper will present a unified process for information recovery and digital forensics, especially on mobile devices. The authors will discuss challenges in trying to come up with a standardized approach in handling digital

evidence from one platform and jurisdiction to another. In addition, methodologies for the improvement of the accuracy and efficiency of digital forensic investigations, particularly in the context of mobile devices, will be presented; such contexts include data being scattered or encrypted.

4.Taylor, M., Hughes, G., Haggerty, J., Gresty, D., & Almond, P. (2012)

Title: Digital evidence from mobile telephone applications

I will explain in words in the next response: The study examines the role of mobile phone applications as a source of digital evidence in forensic investigation. In particular, the application on a smartphone tends to hold vast personal and sensitive information. The authors address the difficulties involved in the collection, preservation, and analysis of data from mobile applications. The paper thus puts great emphasis on the necessity for specialized forensic tools and techniques in the extraction of evidence from non-traditional sources

III IMPLEMENTATION

The implementation of mobile forensics, as described in the literature, is a comprehensive procedure for data extraction, analysis, and preservation. Mobile devices usually are analyzed using two principal methods of data acquisition: physical and logical. Logical acquisition involves extraction through the device's file system or operating system interfaces, such as ADB for Android or iTunes for iOS. Acquiring the physical requires retrieving the raw data directly from the memory of the device, such as the files deleted.• Extraction tools for such acquisitions are Andriller and Oxygen Forensics, among others. Once data○ have been acquired, they require ensuring the integrity through hashing techniques, ensuring authenticity, as detailed in other research works by Tse et al. (2014) and Barmpatsalou et al. (2013).

Forensic analysis of messaging applications, such as WhatsApp and Telegram, is important in mobile forensics, as provided by Anglano (2014) and Shortall & Azhar (2016). All data stored in an SQLite database (msgstore.db) for WhatsApp contains messages, timestamps, as well as media files. With the use of SQL queries, messages and attachments can be retrieved by analysts. In the same way, Telegram stores data both locally in Android devices and in the cloud. Analysis of these databases can allow the recovery of messages and chat histories. Using open-source tools like Andriller and commercial tools like Oxygen Forensics will also be significant in streamlining data extraction. These tools are helpful to extract information from various mobile platforms, such as apps, contact data, call logs, and media files.

Reporting is an important step in the forensic analysis process where details related to methods, tools, and findings should be documented. A forensic report that has details from a timeline of events along with the recovered data and compliance with the chain of custody procedures ensures the integrity of the evidence for use in litigation. A further consideration is that at all times ethical and legal considerations must be strictly applied throughout the process to maintain privacy and ensure regulatory compliance with guidelines such as the ISO/IEC and national standards. This structured approach ensures that data acquired and analyzed remain reliable and would hold up in court.

IV ALGORITHM

1.Data Collection:

Gather data from multiple sources on the mobile device, such as:

Application Usage: Logs of apps opened, duration of usage, timestamps.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

- System Logs: Detailed logs from the operating system, device settings, notifications, and events.
- User Activities: Actions such as taps, swipes, app installations, and configuration changes.

- Ensure that data collection is comprehensive, capturing various user behaviors and device interactions.

2.Data Aggregation:

- Integrate the collected data from various sources into a unified data structure.
- Normalize the data to ensure consistency across different formats (timestamps, actions, device states).
- Combine disparate data points into a cohesive report, ensuring no data is omitted from the analysis.

3.Event Correlation:

- Identify and correlate related events from different datasets (e.g., identifying a system log entry related to an application launch).
- Group activities into user sessions or event timelines, based on timeframes or sequences of interactions.

4.Pattern Recognition:

- Analyze the aggregated data to identify patterns of user behavior, such as frequently used apps or unusual system activity.
- Highlight events that could be of investigative importance, such as application crashes, new installations, or suspicious app usage.

5. Timeline Generation:

- Construct a chronological timeline of events, visualizing the sequence of activities conducted on the device.
- Ensure the timeline reflects key interactions such as app usage, system log events, and other user activities.

6. Report Generation:

- Produce a comprehensive report that summarizes the integrated findings from the timeline and aggregated data.
- The report should provide insights into user behavior, including key activities, app usage patterns, and potential suspicious events.
- Present the report in an easy-to-understand format for investigators.

7.Evaluation and Refinement:

- Test the tool in real-world scenarios to assess its effectiveness in streamlining investigations.
- Refine the tool based on feedback and any limitations identified during testing.

Results

Fig 1:Upload Mobile Data

Fig 2:Extract Data

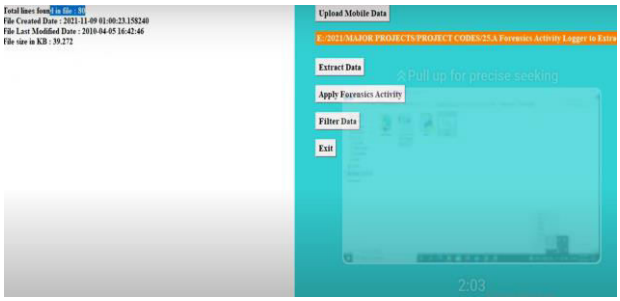

Fig 3: Apply Forensics Activity

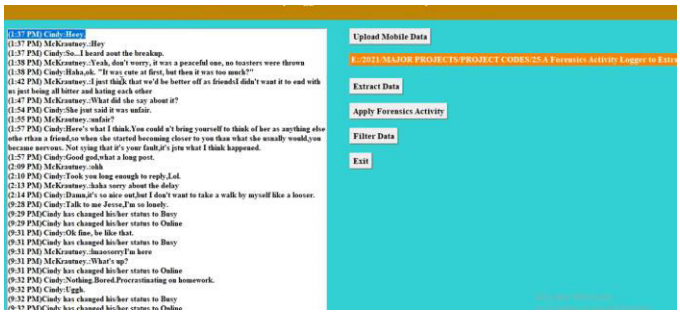

Fig 4: Filter Data

CONCLUSION

Thus, the proposed activity registration tool for Android device forensics analysis is a reliable and time-saving method to obtain and assess digital evidence. The overall process of obtaining the details for forensic analyses, which requires many hours or even days depending on its size, now takes almost no time to complete after automation by using this data collection tool in mobile device forensics.

Despite its efficiency, it must be realized that no single tool is going to retrieve all the data from a mobile device; therefore, a set of tools should be used in the analysis process. Using Python in developing this tool increases the transparency of the tool, thereby ensuring that the integrity of evidence is kept intact as investigators can view the source code and validate that digital evidence is intact.

The tool's next development should extend to covering other mobile OSes like iOS and Windows Phone. Third-party solution integration also needs to be optimized to a great extent for this kind of tool. Increasing efficiency, reducing latency, and also making the tool user-friendly will help this tool increase in applicability with diverse forensic investigations. That would make this tool a great basis for the future in mobile device forensic analysis, making the workflow smooth and enabling investigators to uncover those more effectively and quickly.

REFERENCES

[1] Gobierno del Ecuador, "Ley Orgánica de Educación Intercultural." 2012.

[2] "National Institute of Standards and Technology | NIST." [Online]. Available: https://www.nist.gov/. [Accessed: 30-Aug-2018].

[3]"SWGDE." [Online]. Available: https://www.swgde.org/. [Accessed: 30-Aug-2018].

[4] "Oxygen Forensics - Mobile forensics solutions: software and hardware." [Online]. Available: https://www.oxygen-forensic.com/en/. [Accessed: 21-Aug-2018].

[5] ISO/IEC, "Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence." 202AD.

[6] "ISO/IEC 27037:2012 - Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence." [Online]. Available: https://www.iso.org/standard/44381.html. [Accessed: 30-Aug-2018].

[7] T. Killalea and D. Brezinski, "Guidelines for Evidence Collection and Archiving."

[8] I. P. Agus, "Prototyping SMS Forensic Tool Application Based On Digital Forensic Research Workshop 2001 (DFRWS) Investigation Model," 2016.

[9]"Norma UNE 71505-1:2013." [Online]. Available: https://www.une.org/encuentra-tu-

norma/busca-tunorma/norma/?c=N0051411. [Accessed: 21-Aug-2018].

[10] "Andriller | Android Forensic Tools." [Online]. Available: https://www.andriller.com/. [Accessed: 21-Aug-2018].

[11] M. Taylor, G. Hughes, J. Haggerty, D. Gresty, and P. Almond, "Digital

evidence from mobile telephone applications," Comput. Law Secur. Rev., vol. 28, no. 3, pp. 335–339, 2012.

[12] B. B. Carrier, "Open Source Digital Forensics Tools : The Legal
Argument.," @Stake, no. October, p. 11, 2002.
[13] G. F. Limodio and P. A. Palazzi, "El uso de software abierto para el
análisis de la evidencia digital," 2016.
[14]H. K. S. Tse, K. P. Chow, and M. Y. K. Kwan, "The next generation for the forensic extraction of electronic evidence from mobile telephones,"

Int. Work. Syst. Approaches Digit. Forensics Eng., SADFE, 2014.

[15]K. Barmpatsalou, D. Damopoulos, G. Kambourakis, and V. Katos, "A critical review of 7 years of Mobile Device Forensics," Digit. Investig.,

vol. 10, no. 4, pp. 323–349, 2013.

[16] A. Di Iorio, R. Sansevero, and M. Castellote, "La recuperación de la información y la informática forense: Una propuesta de proceso

unificado," no. March, 2013.