Vol. 15 No. 3 (2024):205-217
DOI: https://doi.org/10.61841/turcomat.v15i3.14794

# A FORENSICS ACTIVITY LOGGER TO EXTRACT USER ACTIVITY FROM MOBILE DEVICES

*[1]Dr. T.Ram Kumar,[2]Puli Mohana,[3]Police Nandhini Reddy,[4]Naredla Varshini*
*[1]Professor,[234]Students*
*Department Of CSE*
*Malla Reddy Engineering College for Women*

**ABSTRACT:**

Mobile devices have become one of the most often used tools in everyday life, mostly because of the importance of its apps. In this case, mobile devices become personal trackers for daily activities that provide important information about the user by recording extra data in addition to the user's personal information. As a consequence of this information gathering, several tools are now accessible for use on mobile devices, however each tool is only able to provide discrete details about a certain application or activity. Consequently, the present research proposes a technology that allows investigators to get a detailed report and time line of all operations performed on the device. This report combines data from several sources to generate a unique collection of facts. Furthermore, an example is provided to illustrate how the solution works, highlighting the practicality of the instrument as well as the way in which investigators need to use it.

## I. INTRODUCTION

These days, a variety of functions (such as entertainment, education, communication, socializing, research, and business transactions) are carried out via mobile devices. The gadgets record data on the user's behavior as a result of that usage. As a result, they are a valuable source of data for forensic investigation.

Additionally, forensics analysis employs a range of methods that enable information to be gathered and extracted from various devices without changing their initial state [2]. It can retrieve deleted files, internet history, instant message data, login information, and more—all of which are considered forms of digital evidence. Three factors should be taken into account during the forensics analysis, according to Iorio et al. [3]: i) avoid contaminating the evidence to prevent misunderstandings; ii) act methodically, meaning that all forensics process results must be thoroughly documented; and iii) control the chain of custody by using a protocol. When conducting a forensics investigation, it's also important to keep in mind the legal considerations that, if ignored, might result in application abuse, fraud, theft, distribution of protected content, and other issues. Therefore, in order to prevent the unnecessary disclosure of personal information, Taylor et al. [4] state that it is essential to adhere to all legal rules relevant to the jurisdiction in which the dispute arises.

Vol. 15 No. 3 (2024):205-217
DOI: https://doi.org/10.61841/turcomat.v15i3.14794

A range of software, including as Encase, DFF, FTK, Helix, Oxygen, MOBILEdit, and UFED, are also available for forensic analysis and enable the examination of several mobile device components, including internal memory, apps, and messages. These days, the so-called suites combine every earlier point into a single study to provide a strong and practical tool. It is essential to consider the benefits of using open source technologies for forensic analysis in the course of an investigation, such as their affordability, ease of examination in court, and ability to be verified [6]. However, the fact that commercial programs provide an extensive range of analytic choices is another reason for their adoption [6]. A comparison of six open-source and commercial programs is provided in Yadav et al.'s [7] work. These tools carry out tasks including retrieving, finding partitions on digital devices, recovering cookies, doing keyword searches, and producing forensic photos. Additionally, a number of well-known forensic tools are presented by Shortall and Azhar [8] and Tajuddin and Manaf [9], including Paraben's device seizure, Cellebrite UFED, MOBILedit Forensic, Forensic Toolkit, XRY, Oxygen Forensic Suite, EnCASE Forensic, and MOBILedit Forensic. They all provide comparable services, analytical methods, and ways to convey the data that has been obtained, but they also vary in terms of their efficacy, capacities, and information-gathering alternatives. For instance, the Oxygen Forensic Suite offers a range of choices to do a detailed forensics study, while UFED searches the hard drive for physical data in order to recover lost data. Based on the examination of the mentioned research, it seems that there are no available solutions that provide an exhaustive record of users' behaviors while using a mobile device. Consequently, the researcher must use several tools to get all the data. As a result, this work offers a tool that has been written in Python [10] and that, via the gathering of data from various installed programs on the Android OS mobile device, creates a unique report including all the information about the user's activity. The users' actions while using the mobile device are then monitored using this information.

The Android and iOS operating systems are the main subject of recent research on mobile device forensics investigation [11], which are also limited to the examination of certain apps. When WhatsApp is installed on Android-powered devices, it creates artifacts. Anglano et al. [12] examine these artifacts and describe how they might be linked to extract various kinds of data. FTK Imager, SqliteMan, and SQLite v.3 databases are the tools they utilize [12]. The same authors' investigation on another study examines data taken from Telegram; as a result, it shows how to display a contact list, a timeline, messages sent and received, and the contents of files sent and received using the SQLite database, UFED, and Oxygen Forensic SQLite Viewer [11]. Furthermore, Alyahya and Kausar [13] use Autopsy and AXIOM Examine, two forensics analysis tools, to examine the Snapchat program on an Android platform. In a similar vein, Walnycky et al. [14] examine 20 Android apps (such as WhatsApp, Viber, Instagram, Facebook Messenger, and Tango) and look at digital evidence that might be used for forensics analysis. They also assess the security of data transmission and reception as well as application privacy.

## II. LITERATURE SURVEY

Vol. 15 No. 3 (2024):205-217
DOI: https://doi.org/10.61841/turcomat.v15i3.14794

1. The next level of technology for forensically extracting data from mobile phones

Data collected from a mobile phone might reveal a lot of personal information about the owner. The subject matter, on which testimony is to be given, must be determined to be scientific before a court permits the trier of fact to accept electronic evidence. Hence, compliance with scientific and legal criteria, as well as international standards, must be considered throughout the investigational phase. By being able to make well-reasoned and tangible statements regarding the legitimacy and correctness of results in court, such compliance also elevates the extraction of electronic evidence from mobile phones to a more rigorous position as a forensic science.

2. A Summing Up of Seven Years of Research on Mobile Device Forensics

An multidisciplinary discipline, Mobile Device Forensics (MF) applies methods to various electronic devices, such as cellphones and GPS systems. There has been a plethora of study on data gathering systems, information extraction methodologies, and mobile device platforms in recent years. By offering a thorough evaluation of the approaches and measures used during the last seven years, this book gives a thorough overview of the area. To provide a comprehensive but concise method of tracking developments in the subject, we've included a multi-level chronological classification of the key research. Regarding the development of MF, this classification chart also functions as an analytical progress report. Additionally, this study summary helps lay the groundwork for a common framework proposal, which is important since standardization efforts in this domain are still in their early stages. Additionally, fields within the MF ecosystem undergo regular transformations because to the quick evolution of mobile device-related technologies. In order to facilitate successful reference and adaptation, this study provides a thorough and critical evaluation of the current state of the art.

3. Digital proof derived from programs for mobile phones

This study takes a look at the law as it pertains to forensic investigations with mobile phone apps. There are several forms of computer misuse that mobile phone applications can be involved in. These include fraud, theft, money laundering, sharing copyrighted materials or explicit images, or even carrying out malicious malware transmissions. Here we take a look at how forensic investigations into mobile phone apps work, as well as some of the challenges that come with extracting digital evidence from these apps.

4. "The Legal Argument for Open Source Digital Forensics Tools"

Vol. 15 No. 3 (2024):205-217
DOI: https://doi.org/10.61841/turcomat.v15i3.14794

This article discusses the use of digital forensic analysis methods in a legal context. A trustworthy and applicable instrument is required to present scientific evidence in a U.S. court. Using the "Daubert" criteria, we can determine how trustworthy the evidence is. As the sector develops further, we can expect to see more legal challenges to digital evidence. Based on the analysis presented in this research, open source technologies have a better chance of clearly and completely meeting the Daubert requirements than closed source solutions.

5. "The Investigation Process and Digital Forensic Tools Analysis"

The proliferation of the internet has altered not just our perspective on life but also our perception of crime, both locally and globally. The need for forensic inquiry is driven by the steadily rising incidence of computer crime. The purpose of digital forensics is to identify and apprehend those accountable for cybercrimes. We compare and contrast two types of forensic tools—commercial and free source—in this article. Additionally, we categorize digital forensics and digital crimes based on the methods used to investigate them. We presented a methodology for investigating all forms of cybercrime in this research. There is a better method to improve investigation time and get efficient results for every form of digital crime using this basic concept.

6. "Analyzing WhatsApp Data on Well-Known Mobile Platforms for Legal Purposes

The encryption methods used by widely used messaging apps like WhatsApp, Skype, and Viber almost eliminate the possibility of detecting evidence of unlawful activity by criminal organizations. Using cutting-edge forensic tools like EnCase, UFED, and Oxygen Forensic Suite, this article discusses the difficulties of analyzing WhatsApp data on three of the most common mobile platforms: iOS, Android, and Windows Phone. Windows Phone8.1, Android 5.0.1 (Lollipop), and iOS 8.3 were the utilized operating systems. According to the results, forensic examiners may need to conduct a live forensic acquisition if they are unable to access data using the normal forensic suite, since Windows 8.1 has strong security mechanisms integrated into the system. To help forensics investigators retrieve evidence of WhatsApp data from inaccessible Windows 8.1 mobile operating systems, this document lays forth realistic ways.

7. The use of smartphones for forensic examination and investigation of digital evidence

As people become increasingly reliant on their smartphones, cybercriminals are adapting their tactics to take advantage of consumers' lack of awareness about security threats associated with social networks, such as spam [1]. Forensics examination of smartphones is therefore necessary in order to recover and evaluate the vast quantities of potentially priceless data stored on these devices. Using many forms of digital evidence, this article examines a plethora of private and sensitive data, and it employs forensic analysis on the widely used Samsung Galaxy Note III smartphone. The conventional method for

Vol. 15 No. 3 (2024):205-217
DOI: https://doi.org/10.61841/turcomat.v15i3.14794

retrieving data from smartphones by means of physical capture and analysis using Cellebrite UFED. We provide these findings to prove that cellphones are a treasure trove of digital evidence that may help solve crimes. In addition, the methods and tools for forensic analysis of digital evidence stored on this device are detailed in this study. Data stored on social networks, as well as files, contacts, and events from smartphones, have been found as proof. The studied smartphone generated a large amount of user data, with a total of 98,127 artifacts being retrieved. Forensic detectives may be able to narrow down their search for a suspect by extracting and analyzing digital data pertaining to smartphone usage.

## III. SYSTEM ANALYSIS

### 3.1 EXISTING SYSTEM:

Due in large part to the significance of its applications, mobile devices have emerged as one of the most widely utilized tools in daily life. In such a scenario, mobile devices record additional data in addition to the personal information of the user, turning them become a personal tracker for everyday activities that yields crucial information about the user. Many tools are available for usage on mobile devices as a result of this information collecting, albeit each tool is limited to providing isolated information about a particular application or behavior.

### PROPOSED SYSTEM:

Consequently, the present research proposes a technology that allows investigators to get a detailed report and time line of all operations performed on the device. This report combines data from several sources to generate a unique collection of facts. Furthermore, an example is provided to illustrate how the solution works, showing the practicality of the tool as well as how investigators need to use it.

Finds and counts the quantity of files based on the kind.

- Ascertains how many lines there are in text files and how many sheets, columns, and rows there are in a Microsoft Excel file. The purpose of this action is to show how long each file is.
- Retrieves the column containing the user's activity's date and time.
- Examines the date that the evidence was received and the date that the forensics investigator entered.
- Keeps the data filtered.
- Combines all of the data into one file.
- Places the data in chronological order by organizing it in decreasing order.

Vol. 15 No. 3 (2024):205-217
DOI: https://doi.org/10.61841/turcomat.v15i3.14794

- Eliminates redundant data.
- Gives every action a code.
- Preserves the document

## IV. IMPLEMENTATION:

**MODULES:**

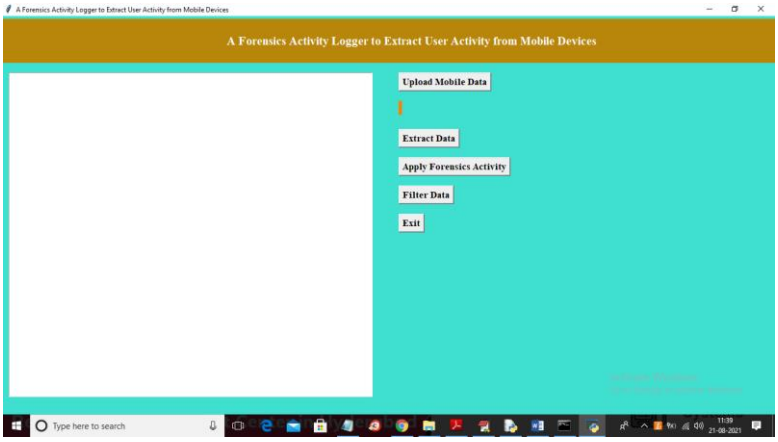
1) Upload Mobile Data: We will upload chat log HTML message files to the application using this module.

2) Extract Data: this will allow us to show the content of the uploaded file after extracting the HTML data from it.

3) Use Forensics Activity: We will extract the file's size, creation and modification dates, and line count using this module.

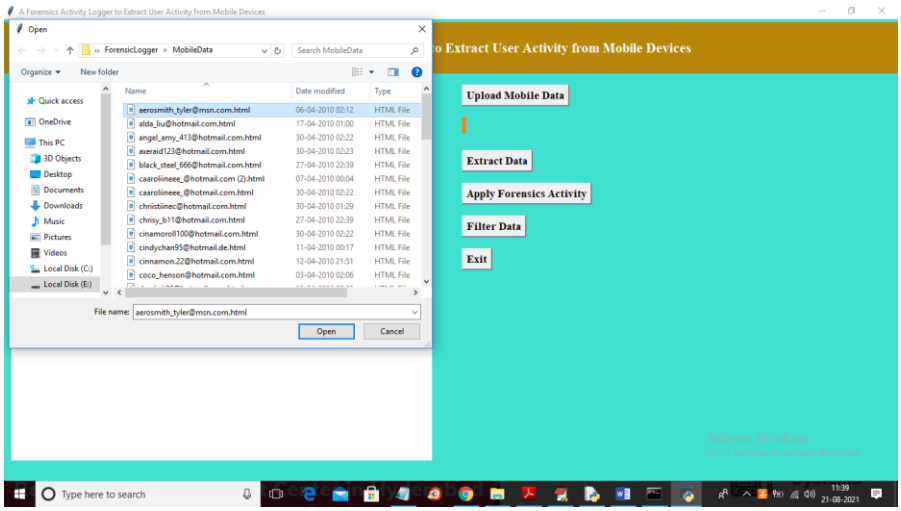
4) Filter Data: This module uses HTML parsers to extract HTML elements from chat logs so that user communications are presented in a clean format.

## V. SCREEN SHOTS

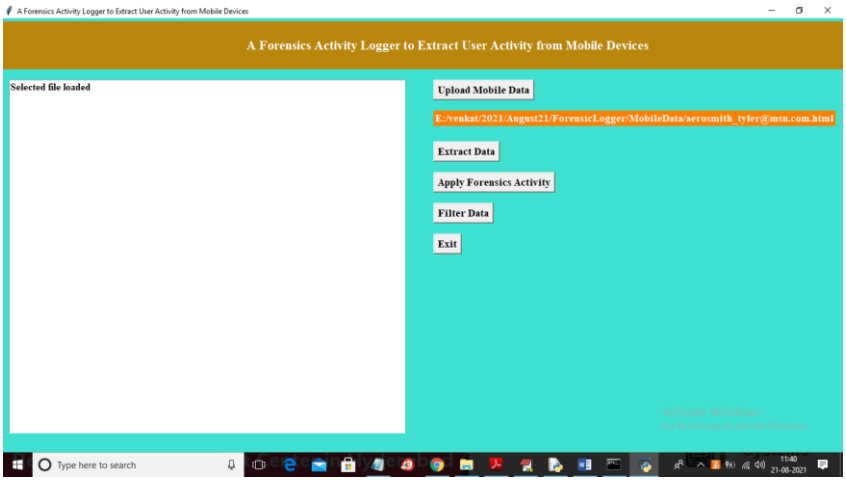



To upload a conversation log file, choose the "Upload Mobile Data" option in the page above.

Vol. 15 No. 3 (2024):205-217
DOI: https://doi.org/10.61841/turcomat.v15i3.14794

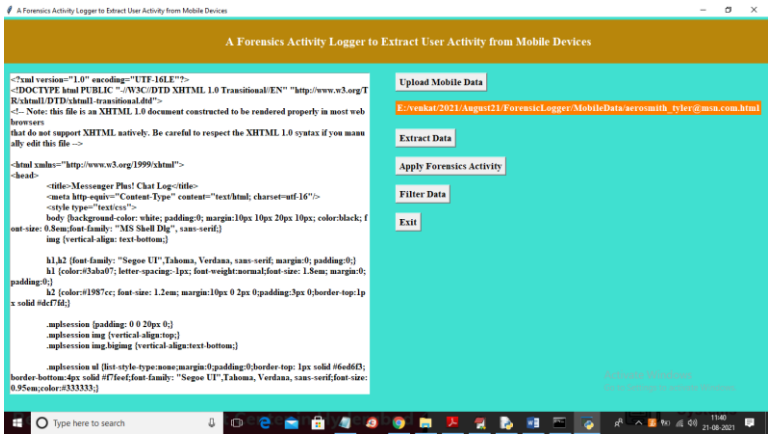



I'm choosing and uploading the conversation log file in the above panel, and then I'm clicking the "Open" button to see the screen below.

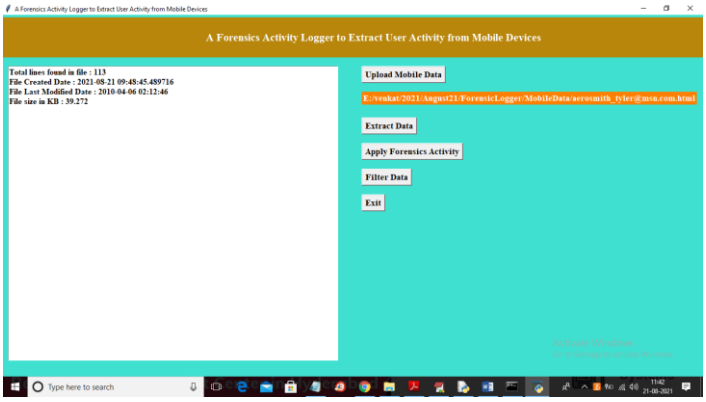



The conversation log file is uploaded in the top page; to extract the information, click the "Extract Data" button.

Vol. 15 No. 3 (2024):205-217
DOI: https://doi.org/10.61841/turcomat.v15i3.14794

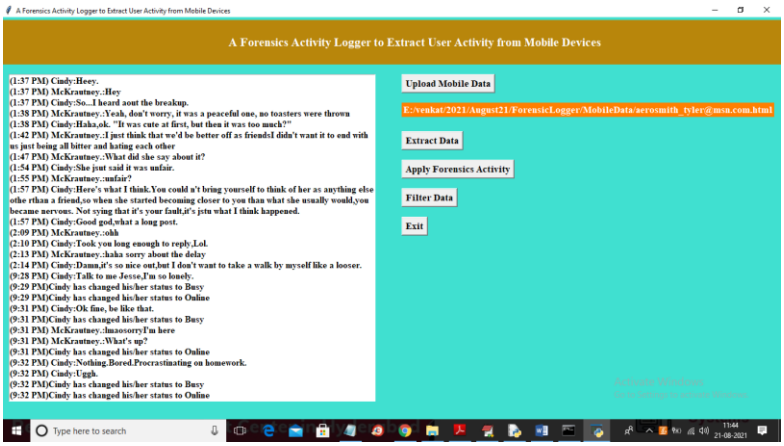



The full file content is shown in HTML format on the screen above, making it impossible for the user to interpret. To extract information from the file, click "Apply Forensics Activity."

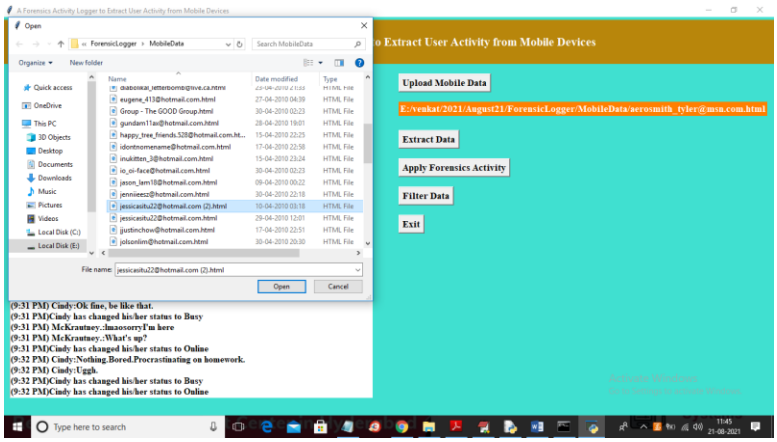



The first line of the above page shows that there are 113 lines in total, that the file was generated and edited on, and that its size is 39.272 KB. After extracting all of the information, we select the "Filter Data" button to remove all HTML elements from the chat message, as seen in the screen below.

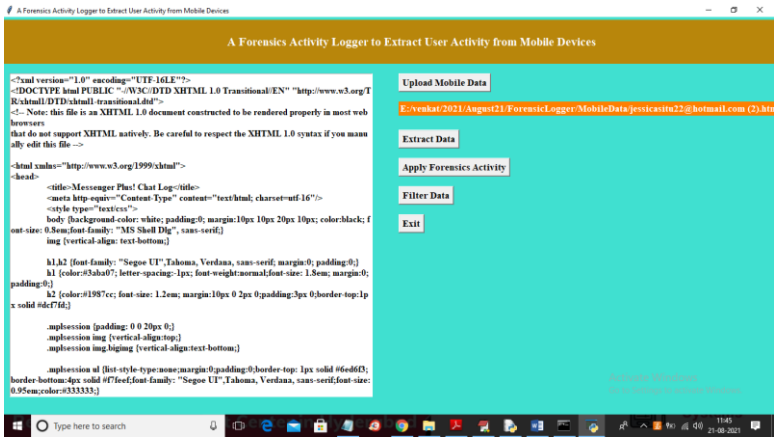
Vol. 15 No. 3 (2024):205-217
DOI: https://doi.org/10.61841/turcomat.v15i3.14794

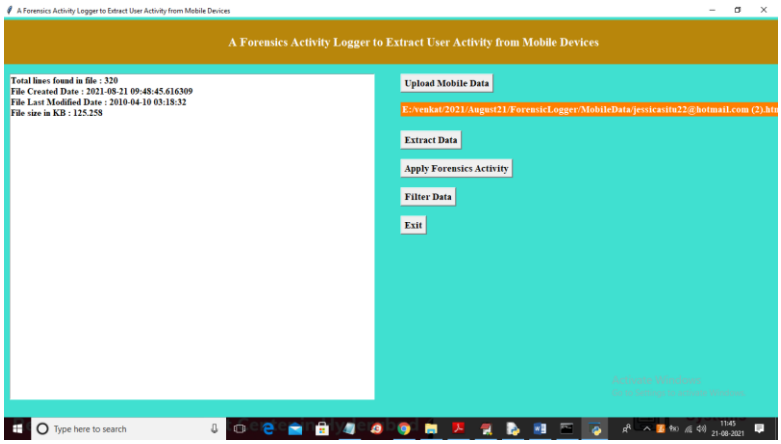



The user can plainly view the chat messages that we retrieved from the HTML content in the above page. We have thus obtained clean conversation messages from HTML elements by using forensic activity logger. You may upload additional files and extract messages in a same manner. View other files now

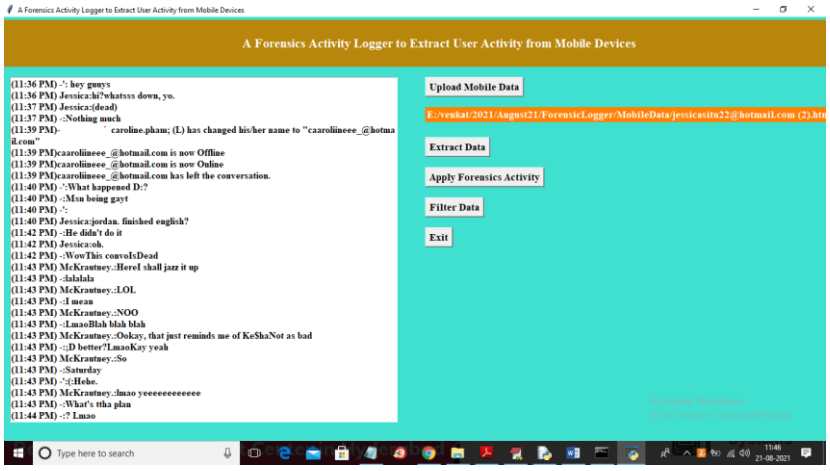


Vol. 15 No. 3 (2024):205-217
DOI: https://doi.org/10.61841/turcomat.v15i3.14794




In above screen for new file the size 125 KB with 320 chat messages lines



Vol. 15 No. 3 (2024):205-217
DOI: https://doi.org/10.61841/turcomat.v15i3.14794

## VI. CONCLUSION

After conducting many testing on various Android smartphone manufacturers, it can be said that the activity registration tool is reliable and compliant with the necessary checks.

The technology expedites and shortens the time needed to analyze the evidence. Choosing the appropriate instruments to get data for the application is an essential research task; all of them are unable to obtain all of the information from a mobile device, however. For the intended outcome to be improved, many of them must be used. Last but not least, using the Python programming language has the benefit of enabling source code verification, which ensures that the digital evidence is not altered.

The primary benefit of employing this tool is that it saves money and cuts down on the amount of time needed for an inquiry. This is due to the fact that every installed program generates massive amounts of data that the lead researcher must carefully review. As a result, this application eliminates the need to manually utilize many pieces of software to get all the data needed for the case.

The evidence must be handled properly as it will not be acceptable for the inquiry if the data is changed in any manner.

## FUTUREWORK

In conclusion, the research that was provided provides an initial understanding of how digital evidence is handled in Android-powered mobile devices; similar work may subsequently be done for iOS and Windows Phone. To facilitate future research, it is essential to enhance interoperability in order to collect data from other solutions and provide connectors and general methods for extracting evidence. Additionally, it is critical to assess and make changes in the future to a few of this tool's non-functional attributes (e.g., efficiency, latency, usability).

## REFERENCES:

1. 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.
2. 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.
3. 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.
4. 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.

Vol. 15 No. 3 (2024):205-217
DOI: https://doi.org/10.61841/turcomat.v15i3.14794

5. B. B. Carrier, "Open Source Digital Forensics Tools : The Legal Argument.," @Stake, no. October, p. 11, 2002.
6. G. F. Limodio and P. A. Palazzi, "El uso de software abierto para el análisis de la evidencia digital," 2016.
7. S. Yadav, K. Ahmad, and J. Shekhar, "Analysis of Digital Forensic Tools and Investigation Process," High Perform. Archit. Grid …, pp. 435–441, 2011.
8. A. Shortall and M. A. H. Bin Azhar, "Forensic Acquisitions of WhatsApp Data on Popular Mobile Platforms," Proc. - 2015 6th Int. Conf. Emerg. Secur. Technol. EST 2015, pp. 13–17, 2016.
9. T. B. Tajuddin and A. A. Manaf, "Forensic investigation and analysis on digital evidence discovery through physical acquisition on smartphone," 2015 World Congr. Internet Secur. WorldCIS 2015, pp. 132–138, 2015.
10. "Welcome to Python.org." [Online]. Available: https://www.python.org/. [Accessed: 21-Aug-2018].
11. C. Anglano, M. Canonico, and M. Guazzone, "Forensic analysis of Telegram Messenger on Android smartphones," Digit. Investig., vol. 23, pp. 31–49, 2017.
12. C. Anglano, "Forensic analysis of whats app messenger on Android smartphones," Digit. Investig., vol. 11, no. 3, pp. 201–213, 2014.
13. T. Alyahya and F. Kausar, "Snapchat Analysis to Discover Digital Forensic Artifacts on Android Smartphone," Procedia Comput. Sci., vol. 109, pp. 1035–1040, 2017.
14. D. Walnycky, I. Baggili, A. Marrington, J. Moore, and F. Breitinger, "Network and device forensic analysis of Android social-messaging applications," Digit. Investig., vol. 14, no. S1, pp. S77–S84, 2015.
15. I. P. Agus, "Prototyping SMS Forensic Tool Application Based On Digital Forensic Research Workshop 2001 ( DFRWS ) Investigation Model," 2016.
16. "Norma UNE 71505-1:2013." [Online]. Available: https://www.une.org/encuentra-tu-norma/busca-tunorma/norma/?c=N0051411. [Accessed: 21-Aug-2018].
17. "Andriller | Android Forensic Tools." [Online]. Available: https://www.andriller.com/. [Accessed: 21-Aug-2018].
18. "MOBILedit." [Online]. Available: https://www.mobiledit.com/. [Accessed: 21-Aug-2018].
19. "Oxygen Forensics - Mobile forensics solutions: software and hardware." [Online]. Available: https://www.oxygen-forensic.com/en/. [Accessed: 21-Aug-2018].
20. ISO/IEC, "Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence." 202AD.
21. "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].

Vol. 15 No. 3 (2024):205-217
DOI: https://doi.org/10.61841/turcomat.v15i3.14794

22. T. Killalea and D. Brezinski, “Guidelines for Evidence Collection and Archiving.”
23. “National Institute of Standards and Technology | NIST.” [Online]. Available: https://www.nist.gov/. [Accessed: 30-Aug-2018].
24. “SWGDE.” [Online]. Available: https://www.swgde.org/. [Accessed: 30- Aug-2018].
25. Gobierno del Ecuador, “Ley Orgánica de Educación Intercultural.” 2012.
26. “Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution.” [Online]. Available: https://www.kali.org/. [Accessed: 21- Aug-2018].