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

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 29th Dec 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue12

10.48047/IJIEMR/V12/ISSUE 12/33

TITLE: An Intriguing Tale of Crime Scene Investigation and Cellular Phone Analysis: An Application Forensic Activity

Volume 12, ISSUE 12, Pages:270-277

Paper Authors **N. Sateesh1, A. Rohini2, A. Sravika2, A. Harini2**

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

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

An Intriguing Tale of Crime Scene Investigation and Cellular Phone Analysis: An Application Forensic Activity

N. Sateesh[1], A. Rohini[2], A. Sravika[2], A. Harini[2]

[1]Professor, [2]UG Student, [1,2]Department of Information Technology
[1,2]Malla Reddy Engineering College for Women (UGC – Autonomous), Maisammaguda, Hyderabad, Telangana

ABSTRACT

In the past, digital forensic investigators relied on manual methods to extract user activity data, which were often time-consuming and error prone. This involved manually copying data from the device's storage, making it challenging to handle large volumes of data and potentially risking the loss or corruption of essential evidence. Moreover, the lack of standardized procedures made it difficult to ensure the accuracy and reliability of the extracted information. To overcome these limitations, there is a clear demand for a specialized digital forensic tool designed to extract user activity data efficiently and effectively from mobile devices. Such a tool should be versatile enough to handle various mobile operating systems and should offer standardized and automated procedures to ensure consistent and reliable results. Additionally, the tool must have a user-friendly interface to cater to both experienced and novice investigators, allowing them to use it effectively. Hence, this project proposes the development of a tool that enables investigators to obtain a comprehensive report and timeline of the activities performed on a mobile device. By combining information from various sources into a unified dataset, this tool streamlines the investigative process. It demonstrates the tool's functionality through an example, showcasing its feasibility and how investigators can apply it effectively. By leveraging this tool, investigators can significantly improve their efficiency in extracting and analyzing crucial user activity data from mobile devices, thereby supporting their efforts in solving digital crimes.

Keywords: Digital forensics, Data filtering, BeautifulSoup, Information extraction.

1. INTRODUCTION

Mobile phones have become an integral part of our lives, and they often contain critical evidence in criminal cases. Think of text messages, call logs, GPS data, and much more. But the problem is that extracting this data from mobile devices can be really tough. It's like trying to unlock a puzzle, and the methods used in the past aren't always up to the task, especially as mobile technology keeps evolving. Over the years, investigators have had to adapt to the changing world of technology. We've come a long way from the early days of personal computers to the smartphones we use today. Along this journey, digital forensics has played an increasingly vital role in solving crimes. Think of cases where text messages or GPS data on a suspect's phone helped crack the case; that's the power of digital evidence.

The "Digital Forensic Tool" is significant because it can make the process of collecting and analyzing data from mobile devices faster and more reliable. This can be a game-changer for law enforcement agencies. It means investigations can move more swiftly, evidence can be gathered more effectively, and it can ultimately lead to more successful prosecutions, which helps keep our communities safe. So, why do we need this tool? Well, it's because mobile devices are getting more complex. They come in all shapes and sizes, with various operating systems and security measures. This complexity can slow down investigations and even result in vital data being lost. This project is here to fill that need for a

powerful and up-to-date tool that can handle these challenges head-on. Imagine a specialized computer program designed to help detectives and investigators solve crimes more effectively. Therefore, this project, known as "A Digital Forensic Tool for Extracting User Activity from Mobile Devices in Crime Scene Investigation Applications," is aimed at making the job of law enforcement agencies easier. It does this by helping them retrieve crucial information from mobile devices, which can be incredibly valuable in solving crimes.

2. LITERATURE SURVEY

According to Iorio et al., [3], there are three aspects that should be considered during the forensics analysis: i) avoid contamination of the evidence to prevent misinterpretations; ii) act methodically, that is, all the results of the forensics process must be well documented; and iii) control the chain of custody through the use of a protocol. Also, there are legal aspects to take into consideration when performing a forensics investigation, that do not comply always, these leads to the misuse of applications, fraud, theft, dissemination of copyrighted materials, etc. Thus, according to Taylor et al., [4] it is necessary to follow all the legal guidelines corresponding to the jurisdiction where the conflict is generated, to avoid undue exposure of personal information. Also, there are a variety of applications (e.g., Encase, DFF, FTK, Helix, Oxygen, MOBILEdit, UFED), which are used for forensic analysis and allow the inspection of various elements of mobile devices (e.g., internal memory, applications, messages). Now, the so-called suites take all the previous points and join them in a single analysis creating a powerful and useful tool [5]. Also, it is important to take into account that there are advantages of using open-source tools for forensics analysis during an investigation (e. g., no-cost, easy to examine in court, allows verification) [6]. But commercial tools are also used because they provide a great variety of alternatives for analysis [6].

In Yadav et al., [7] it is presented a comparison among six commercial and open-source applications. Those tools perform processes such as: recovering, performing keyword searches, recovering cookies, creating forensic images, and locating partitions of the digital devices. Also, Shortall and Azhar [8] and Tajuddin and Manaf [9] present several popular forensic tools, such as Cellebrite UFED, MOBILedit Forensic, Forensic Toolkit, XRY, Oxygen Forensic Suite, EnCASE Forensic, and Paraben's device seizure. Each one of them has different capabilities, effectiveness, and options to acquire information, but also, they offer similar services, analysis techniques and ways to present retrieved data. For example, UFED looks for physical data on the hard drive-in order to recover deleted data, while the Oxygen Forensic Suite has a variety of options to perform a deep forensics analysis. By the analysis of the indicated studies, and as far as we know, there are not solutions that provide a complete log of the users' actions when using a mobile device, therefore the investigator needs to use more than one tool in order to recover all the data.

Recent studies on forensics analysis for mobile devices are mostly focused on Android and iOS operating systems [11], which also are only oriented to the study of specific applications. Anglano et al, [12] study the artifacts generated by WhatsApp when it is deployed on devices running Android and explain how those artifacts are correlated to extract several types of data. The tools that they use are: FTK Imager, SqliteMan and SQLite v.3 databases [12]. On another study by the same authors, they analyze data obtained from Telegram; as a result, 286 it presents the way to show the contact list, the chronology, the messages that have been exchanged, and the contents of the files that have been sent or received, all these with the use of the tools: SQLite database, UFED and Oxygen Forensic SQLite Viewer [11].

3. EXISTING TECHNIQUE

Traditional digital forensic tools often focus on a single specific task, such as data extraction or analysis. In this project, the tool is primarily designed for data extraction and limited forensic analysis. The tool relies on manual user interactions to upload, extract, and analyze data. Users must initiate each step of the process individually. The forensic analysis provided by the tool is limited to displaying basic file attributes (creation date, modification date, file size) and counting the total number of lines in the file. It lacks advanced forensic analysis capabilities, such as timeline reconstruction, data carving, or artifact analysis. The tool lacks reporting capabilities. Traditional digital forensic systems often generate detailed reports that can be used as evidence in legal cases. But there is no provision for user authentication or access control, which can be critical in forensic investigations to maintain the integrity of the data.

Limitations

- Scalability: The tool may not scale well to handle large volumes of data or complex investigations, as it relies on manual operations.
- Lack of Data Integrity Verification: It does not perform data integrity checks to ensure that the extracted data has not been tampered with or modified.
- Limited Data Sources: The project focuses on a single data source (mobile device files) and does not consider data sources like cloud backups, network traffic, or external databases.
- Platform Dependence: The tool is platform-dependent and may not work seamlessly on different operating systems or with diverse mobile device data.

4. PROPOSED METHODOLOGY

4.1 Overview

This project develops a basic digital forensic tool with a graphical user interface (GUI) built using the Tkinter library in Python. The tool is designed for extracting and analyzing user activity data from mobile devices. It offers a basic framework for a digital forensic tool to analyze and extract user activity data from mobile devices. Here's an overview of the project's functionality and components:

Step 1 – GUI Interface: The tool has a graphical user interface with various buttons, labels, and a text box for displaying information.

Step 2 – Main Features

- Upload Mobile Data: Users can click the "Upload Mobile Data" button to select a mobile device data file (presumably in a specific format) using a file dialog. The selected file's path is displayed on the GUI.
- Extract Data: Clicking the "Extract Data" button parses the content of the selected file (assumed to be in UTF-16 encoding). The content is processed using the BeautifulSoup library, and the parsed data is stored in the testData variable. The content is also displayed in a text box.
- Forensic Activity: When the "Forensic Activity" button is clicked, the tool provides forensic information about the selected file. This information includes the total number of lines in the file, the file's creation date, the last modification date, and the file size in kilobytes.
- Filter Data: Clicking the "Filter Data" button filters the loaded data and displays lines that contain "PM)" or "AM)". This feature is likely intended to identify and extract time-related information from the data.

— Exit: The "Exit" button allows users to close the application.

Step 3 – Global Variables: It uses global variables (filename, testData, and content) to store and share information among the different functions within the application.

Step 4 – Display of Results: Extracted and filtered data, as well as forensic information, is displayed in a text box within the GUI. The text box supports scrolling to view large amounts of data.

Key features

— User Interaction: Users interact with the tool by clicking buttons to perform specific actions, such as uploading a file, extracting data, viewing forensic details, and filtering data.
— User Interface Design: The GUI is designed using Tkinter and provides a user-friendly way to interact with the tool, making it accessible to users without programming expertise.

4.2 Extract Data

This feature is designed to parse and extract information from the selected mobile device data file. It assumes that the data file is in UTF-16 encoding and uses BeautifulSoup, an HTML parsing library, to process the content.

Working

— When the "Extract Data" button is clicked, the tool reads the content of the selected file using the open function with the 'rb' (read binary) mode to ensure proper encoding handling.
— The content is then decoded from UTF-16 encoding into a Unicode string.
— BeautifulSoup is used to parse the HTML content. Note that in the code, the entire content is treated as HTML even if it's not necessarily HTML; this assumes the data has some structure resembling HTML.
— The parsed data is stored in the testData global variable.
— The extracted content is displayed in a text box on the GUI for the user to review.
— Use Cases: This feature is useful for quickly examining the content of a mobile device data file, potentially revealing structured information such as timestamps, user actions, or other data of interest.

4.3 Forensic Activity

This feature provides users with essential forensic details about the selected file, helping them assess the file's relevance and integrity for digital forensic analysis.

Output

— Total lines found in the file: This indicates the overall size of the file in terms of lines.
— File Created Date: The date when the file was created.
— File Last Modified Date: The date when the file was last modified.
— File size in KB: The size of the file in kilobytes.

Working

— It uses the pathlib library to gather file-related information.
— The number of lines is determined by splitting the testData (assumed to contain text data) into lines and counting them.

- File creation and modification dates are obtained using st_ctime (creation time) and st_mtime (modification time) attributes, respectively.
- File size is calculated using the st_size attribute of the pathlib.Path object.

Use Cases: This feature assists forensic analysts in quickly assessing key file attributes, such as file size and timestamps, which are essential for investigations.

4.4 Filter Data

This feature is designed to extract and display specific lines from the loaded data that contain the text "PM)" or "AM)".

Working

- When the "Filter Data" button is clicked, the tool searches through the loaded data stored in the testData variable.
- It identifies lines that contain "PM)" or "AM)" and extracts these lines into a new text string.
- The extracted lines are displayed in the text box on the GUI.

Use Cases: This feature is particularly useful for filtering and displaying time-related information from the data, such as timestamps indicating whether an event occurred in the morning or afternoon.

Overall, these three functionalities in the project cater to different aspects of digital forensic analysis. "Extract Data" helps to quickly view the content of a data file, "Forensic Activity" provides essential file attributes for assessment, and "Filter Data" extracts and displays specific information based on a predefined pattern, facilitating the identification of relevant data points within the file.

5. RESULTS AND DISCUSSION

To implement this project, we have designed following modules:

- Upload Mobile Data: This module is used to upload chat log HTML messages files to application.
- Extract Data: This module will extract HTML data from uploaded file and then display content of that file.
- Forensics Activity: This module will extract file size, file creation and modification date and number of lines in that file.
- Filter Data: This module will apply HTML parsers to remove HTML tags from chat logs and then display clean chat messages between users.

Figure 1 illustrates the result of a user action, such as clicking a button labeled "extract data." It shows the content of the uploaded HTML file displayed within the application's interface. This content includes the HTML structure of the messages. Figure 2 displays the results of a forensic analysis conducted on the extracted data. It includes details such as the total number of lines found in the data, the creation date and last modified date of the uploaded file, and the size of the file in a graphical format. From Figure 2, the first line shows that the uploaded file contains total 113 lines and the file created and modified date and file size is 39.272 KB.

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

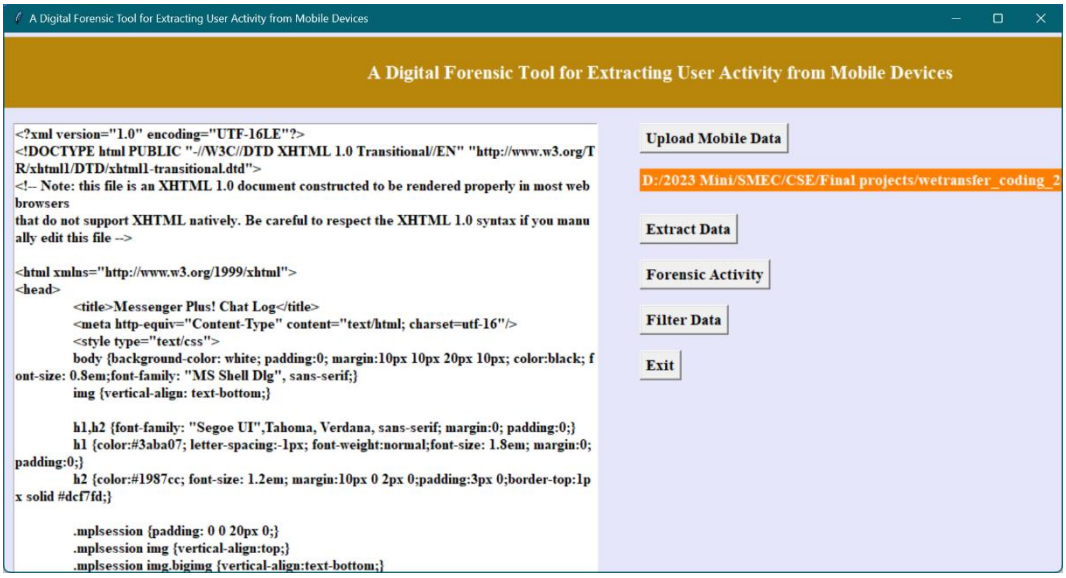

Figure 1: Displaying the uploaded file content in HTML format by clicking on extract data module.

Figure 2: Illustrating the forensic activity on extracted data module with the total lines found, file creation and last modified date and the size of the file.

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

Figure 3: Chat logs extracted data after applying the filtering to clean chat messages for user understating.

Figure 3 represents the output within the GUI application after a specific filtering process has been applied to the chat logs extracted data. Here's a detailed explanation of Figure 3:

- Chat Logs Display: This part of the figure displays the chat logs or chat messages from the extracted data, but with some cleaning or filtering applied to make the messages more understandable to the user.
- Filtered Content: The content displayed consists of chat messages that have been processed or filtered to remove irrelevant or noisy information. Filtering involves removing system messages, duplicates, or any other content that doesn't contribute to the user's understanding of the chat.
- Clean Formatting: The chat messages are presented in a clean and structured format, making it easy for the user to read and comprehend. This includes timestamps, user IDs, and the actual message text.
- User-Friendly Presentation: The primary aim of this figure is to present the chat data in a way that is user-friendly and facilitates a better understanding of the conversation. It involves arranging messages in chronological order, highlighting important elements, or using different colors or fonts for improved readability.

From Figure 3, the chat messages are extracted from the HTML content and user can read above messages clearly. So, this proposed system has a clean chat message from HTML tags by applying crime scene investigation logger. Similarly, any file can be uploaded, and the messages can be extracted as discussed in above outcome.

5. CONCLUSION AND FUTURE SCOPE

This project serves as a starting point for a digital forensic tool designed to extract and analyze user activity data from mobile devices. It offers a basic but functional GUI that allows users to upload mobile device data files, extract information from them, perform forensic analysis, and filter specific data points. The tool is a valuable foundation for digital forensic analysis but has room for further improvement and expansion. The project can be extended to handle various mobile device data formats

beyond the assumed UTF-16 encoding. Support for multiple file formats (e.g., JSON, XML, SQLite) would enhance the tool's versatility. In addition, additional forensic analysis features can also be added, such as data integrity checks, user activity timelines, and pattern recognition algorithms to identify suspicious or noteworthy activities. Further, user authentication and access control can be incorporated to ensure data security and compliance with privacy regulations.

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.

[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: 25-Aug-2023].

[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.