International Journal for Innovative Engineering and Management Research

PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL

www.ijiemr.org

xx

IJIEMR Transactions, online available on 04th May 2024. Link https://www.ijiemr.org/downloads/Volume-13/ISSUE-5

10.48047/IJIEMR/V13/ISSUE 05/16

TITLE: **Forensics Activity Logger for Mobile Devices**

Volume 13, ISSUE 05, Pages: 153-162

Paper Authors **K.Hitesh sai, K.prajvala, S. Indu, K. SPANDANA**

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

Forensics Activity Logger for Mobile Devices

K.Hitesh sai, K.prajvala, S. Indu, K. SPANDANA

Department of computer science and engineering
Sreenidhi institute of science and technology
saihitesh44@gmail.com
Department of computer science and engineering
Sreenidhi institute of science and technology
kolaghanip@gmail.com
Department of computer science and engineering
Sreenidhi institute of science and technology
mailto:Indu01401@gmail.com
Assistant professor,Department of computer science and engineering
Sreenidhi institute of science and technology
keshettispandana@gmail.com

ABSTRACT

In today's era, mobile devices have evolved into indispensable tools for individuals in their daily lives, owing to the myriad of applications they offer. These devices store a wealth of personal information and serve as personal trackers, documenting users' daily activities and providing invaluable insights. Despite the abundance of tools available on mobile devices, each typically offers isolated information pertaining to specific applications or activities. To address this limitation, this study proposes a comprehensive solution—a Forensics Activity Logger for Mobile Devices—that enables investigators to generate a comprehensive report and timeline of activities conducted on the device. This tool aggregates information from various sources into a cohesive dataset, offering a holistic view of the user's interactions. Through the presentation of a practical example, the functionality of the solution is demonstrated, illustrating its effectiveness and usability in forensic investigations. The example showcases how investigators can leverage the tool to extract valuable insights and reconstruct a chronological sequence of events from mobile device data, thereby facilitating forensic analysis and aiding in the resolution of legal matters.

Keywords: Mobile devices, Forensic activity logger, Digital forensics, Investigation tools, Data aggregation, Timeline analysis, Privacy protection.

INTRODUCTION

In the modern era, mobile devices have transitioned from being mere communication tools to indispensable companions that facilitate a wide range of activities in people's daily lives. These activities span entertainment, education, communication, socialization, research, and commercial transactions, among others [1]. Consequently, mobile devices have evolved into repositories of vast amounts of user data, ranging from personal information to browsing history, application usage patterns, and communication records. This wealth of data has rendered mobile devices invaluable sources of evidence for forensic analysis, particularly in legal investigations, criminal proceedings, and cybersecurity incidents [2]. Forensic analysis of mobile devices employs a set of specialized techniques aimed at collecting, preserving, extracting, and analyzing digital evidence without compromising its integrity [3]. These techniques are essential for ensuring that evidence remains admissible in court and can withstand scrutiny under legal scrutiny. Key principles governing forensic analysis include the avoidance of evidence contamination, methodical documentation of investigation procedures and findings, and the maintenance of a secure chain of custody to track evidence handling [4]. Moreover, adherence to legal guidelines and regulations is crucial to safeguarding the rights of individuals and preventing the misuse of forensic tools and techniques [5].

In the realm of mobile device forensics, a plethora of tools and methodologies have been developed to aid investigators in extracting and analyzing digital evidence. These tools range from open-source software solutions to commercial forensic suites, each offering unique capabilities and functionalities [6]. Open-source tools are favored for their affordability, transparency, and ease of verification, making them popular choices for forensic practitioners and researchers [7]. However, commercial tools boast extensive feature sets, advanced analysis techniques, and comprehensive support, making them indispensable assets for professional forensic investigations [8]. Examples of popular forensic tools include EnCase Forensic, Cellebrite UFED, MOBILedit Forensic, Oxygen Forensic Suite, and Paraben's Device Seizure, each offering distinct advantages and capabilities [9]. Despite the availability of these tools, challenges persist in the field of mobile device forensics. One such challenge is the fragmentation of digital evidence across multiple applications and data sources within a mobile device. Existing forensic tools often lack the ability to seamlessly aggregate and correlate data from diverse sources, leading to incomplete or fragmented forensic reports [10]. Additionally, the rapid proliferation of mobile applications and the dynamic nature of mobile operating systems pose significant challenges for forensic investigators [11]. New applications are constantly being developed, each with its unique data storage mechanisms and security features, complicating the forensic analysis process.

To address these challenges and provide a comprehensive solution for mobile device forensics, this paper proposes the development of a novel tool: the Mobile Device Forensic Analyzer (MDFA). MDFA aims to overcome the limitations of existing forensic tools by offering enhanced data aggregation, correlation, and analysis capabilities. Leveraging advanced machine learning algorithms and data mining techniques, MDFA will intelligently analyze data from various sources within a mobile device, including applications, system logs, communication records, and sensor data. By consolidating diverse data sources into a cohesive forensic report, MDFA will furnish investigators with a comprehensive overview of user activities and interactions on the mobile device. Moreover, MDFA will prioritize user privacy and data security by implementing robust encryption protocols, access controls, and anonymization techniques to safeguard sensitive information throughout the forensic analysis process. Additionally, the tool will adhere to legal and regulatory frameworks governing digital evidence collection and handling, ensuring that forensic reports generated by MDFA are admissible in court and compliant with relevant laws and regulations. The proposed Mobile Device Forensic Analyzer (MDFA) signifies a notable advancement in mobile device forensics, furnishing a comprehensive solution for extracting, analyzing, and presenting digital evidence from mobile devices. By tackling challenges such as data fragmentation, application diversity, and privacy concerns, MDFA aims to equip forensic investigators with the tools and capabilities necessary to conduct thorough and effective forensic analysis in an ever-evolving digital landscape.

LITERATURE SURVEY

The realm of mobile device forensics has undergone substantial evolution in recent years, propelled by the widespread adoption of smartphones and the escalating intricacy of mobile applications. With mobile devices housing extensive troves of sensitive data, encompassing personal information, communication records, and app usage histories, they have emerged as invaluable reservoirs of evidence in forensic inquiries. Nevertheless, the extraction and analysis of digital evidence from mobile devices pose distinctive hurdles owing to the myriad mobile operating systems in existence and the perpetual advancement of mobile technologies [17]. In this literature survey, we explore recent advancements and methodologies in mobile device forensics, with a focus on the development of a Forensics Activity

Logger for Mobile Devices. One of the primary challenges in mobile device forensics is the fragmentation of digital evidence across various applications and data sources within the device [18]. Mobile devices typically contain a multitude of applications, each with its data storage mechanisms and formats. As a result, forensic investigators often struggle to gather and correlate evidence from different sources to reconstruct a comprehensive timeline of user activities [19]. Moreover, the dynamic nature of mobile operating systems, frequent updates, and security enhancements further complicate the forensic analysis process [20]. Researchers and practitioners have recognized the need for tools and techniques that can effectively aggregate, parse, and analyze data from diverse sources within a mobile device to facilitate comprehensive forensic investigations.

To address the challenge of data fragmentation, researchers have proposed various approaches and methodologies for mobile device forensics. One common approach involves the development of specialized forensic tools and software applications designed to extract and analyze digital evidence from mobile devices [16]. These tools employ a range of techniques, including file carving, data carving, and keyword searching, to identify and recover relevant information from the device's storage and memory. Commercial forensic suites such as Cellebrite UFED, Oxygen Forensic Detective, and XRY have gained popularity among forensic analysts for their comprehensive feature sets and advanced analysis capabilities [17]. These tools offer functionalities such as data extraction, data parsing, timeline analysis, and reporting, enabling investigators to uncover crucial evidence stored on mobile devices. In addition to commercial tools, researchers have explored the use of open-source forensic software and frameworks for mobile device analysis. Open-source tools such as Autopsy, Sleuth Kit, and Android Debug Bridge (ADB) provide forensic analysts with cost-effective alternatives for conducting forensic investigations [18]. These tools offer functionalities such as disk imaging, file system analysis, artifact extraction, and keyword searching, empowering investigators to extract and analyze digital evidence from mobile devices [19]. Moreover, the open-source nature of these tools allows for transparency, peer review, and community collaboration, contributing to their widespread adoption in the forensic community.

Moreover, strides in machine learning and artificial intelligence have spurred the emergence of pioneering methodologies in mobile device forensics. Scholars have delved into leveraging machine learning algorithms to automate the analysis of digital evidence, discern patterns, and detect anomalies in forensic inqu [20]. For instance, convolutional neural networks (CNNs) and recurrent neural networks (RNNs) have been deployed for purposes like image classification, text recognition, and activity identification within forensic scenarios. These techniques enable forensic analysts to automate repetitive tasks, expedite the analysis process, and identify relevant patterns and trends in digital evidence. mobile device forensics is a rapidly evolving field that presents unique challenges and opportunities for researchers and practitioners alike. The fragmentation of digital evidence, the dynamic nature of mobile operating systems, and the increasing concerns over privacy and data security underscore the need for innovative solutions and methodologies in forensic investigations. By leveraging advancements in technology, machine learning, and data analysis, researchers can develop tools and techniques that enable comprehensive, efficient, and privacy-preserving forensic investigations in the mobile domain.

PROPOSED SYSTEM

The proposed system, titled the "Forensics Activity Logger for Mobile Devices," represents a significant advancement in the field of digital forensics, specifically tailored to address the challenges inherent in gathering, analyzing, and correlating digital evidence from mobile devices. In an era where mobile devices have become ubiquitous tools for communication, productivity, entertainment, and commerce, the need to effectively capture and interpret user activities on these devices has never been greater. The proposed system aims to fulfill this need by offering a comprehensive and robust solution that enables forensic investigators to reconstruct detailed timelines of user interactions and system events, thereby facilitating more accurate and thorough investigations. At the heart of the Forensics Activity Logger is a lightweight application that is installed directly onto the mobile device under investigation. This application operates quietly in the background, capturing a wide range of data related to user activities, application usage, network communications, and system events without interfering with the device's normal operation. Leveraging a combination of techniques such as log monitoring, network traffic analysis, and application behavior tracking, the system ensures that no relevant information is overlooked, providing forensic investigators with a comprehensive view of the user's interactions with the device.

One of the key features of the proposed system is its ability to securely store and transmit collected data to a central server for further analysis. The system employs robust encryption and authentication mechanisms to protect the integrity and confidentiality of the collected data, both in transit and at rest. This ensures that sensitive information remains secure and tamper-proof, maintaining the chain of custody and ensuring the admissibility of the evidence in legal proceedings. Additionally, the system implements strict access controls and audit trails to track and monitor user interactions with the collected data, providing transparency and accountability throughout the investigation process. In terms of data analysis, the Forensics Activity Logger incorporates advanced parsing and correlation algorithms to extract actionable insights from the collected data. These algorithms are capable of identifying patterns, anomalies, and potential evidence relevant to the investigation, enabling forensic investigators to reconstruct detailed timelines of user activities and interactions with mobile applications. The system also provides a user-friendly interface for visualizing and exploring the collected data, allowing investigators to quickly identify relevant information and make informed decisions.

Moreover, the proposed system is designed to be highly adaptable and scalable, capable of accommodating a wide range of mobile devices, operating systems, and application ecosystems. Whether investigating smartphones, tablets, or other mobile devices running Android, iOS, or other operating systems, the Forensics Activity Logger can be tailored to meet the specific requirements of each case. Furthermore, the system can be easily integrated with existing forensic tools and workflows, allowing forensic investigators to leverage its capabilities seamlessly within their existing investigative processes. Overall, the Forensics Activity Logger for Mobile Devices represents a significant advancement in the field of digital forensics, offering forensic investigators a powerful and versatile tool for gathering, analyzing, and presenting digital evidence from mobile devices. By streamlining the forensic investigation process and providing comprehensive insights into user activities, the proposed system empowers investigators to conduct more thorough and effective investigations, ultimately leading to more accurate and just outcomes in legal proceedings.

METHODOLOGY

The methodology for the "Forensics Activity Logger for Mobile Devices" involves a systematic approach to capturing, analyzing, and documenting digital evidence from mobile devices. This process encompasses several steps, each crucial for ensuring the integrity and completeness of the forensic investigation. The first step involves understanding the requirements and objectives of the forensic investigation. This includes identifying the type of mobile device(s) involved, the operating system(s) they run, the specific data to be collected, and any legal or regulatory considerations that may apply. Based on the requirements analysis, appropriate tools and technologies are selected for implementing the Forensics Activity Logger. This may include choosing a programming language (e.g., Python, Java) for developing the logging application, selecting libraries or frameworks for data parsing and analysis, and determining the storage and encryption mechanisms for securing the collected data.

Once the logging application is deployed on the mobile device(s), it begins collecting data in real-time. This data may include logs of user interactions, timestamps of application launches and closures, network traffic logs, device metadata (e.g., device ID, operating system version), and any other relevant information specified in the requirements analysis. The collected data is securely stored on the mobile device(s) using encryption techniques to protect it from unauthorized access or tampering. Strong encryption algorithms are employed to encrypt the data both at rest and in transit, ensuring its integrity and confidentiality throughout the forensic investigation process. To prevent data loss and ensure timely access to the collected evidence, the logging application periodically synchronizes the collected data with a central server or cloud storage repository. This allows forensic investigators to access the data remotely for further analysis and processing.

Upon synchronization, the collected data is parsed and analyzed using advanced algorithms and techniques. This involves extracting relevant information from the raw data, identifying patterns and anomalies, and correlating different data sources to reconstruct detailed timelines of user activities and interactions with the mobile device(s). The analyzed data is presented to forensic investigators through a user-friendly interface that allows for visualization and exploration. Graphical representations, charts, and timelines are used to present the findings, enabling investigators to quickly identify relevant information and draw insights from the data. Finally, the findings of the forensic analysis are documented and compiled into a comprehensive report. This includes detailed information about the data collected, the analysis performed, any findings or observations, and recommendations for further investigation or action. The report should be well-documented, organized, and presented in a format suitable for legal or regulatory purposes.

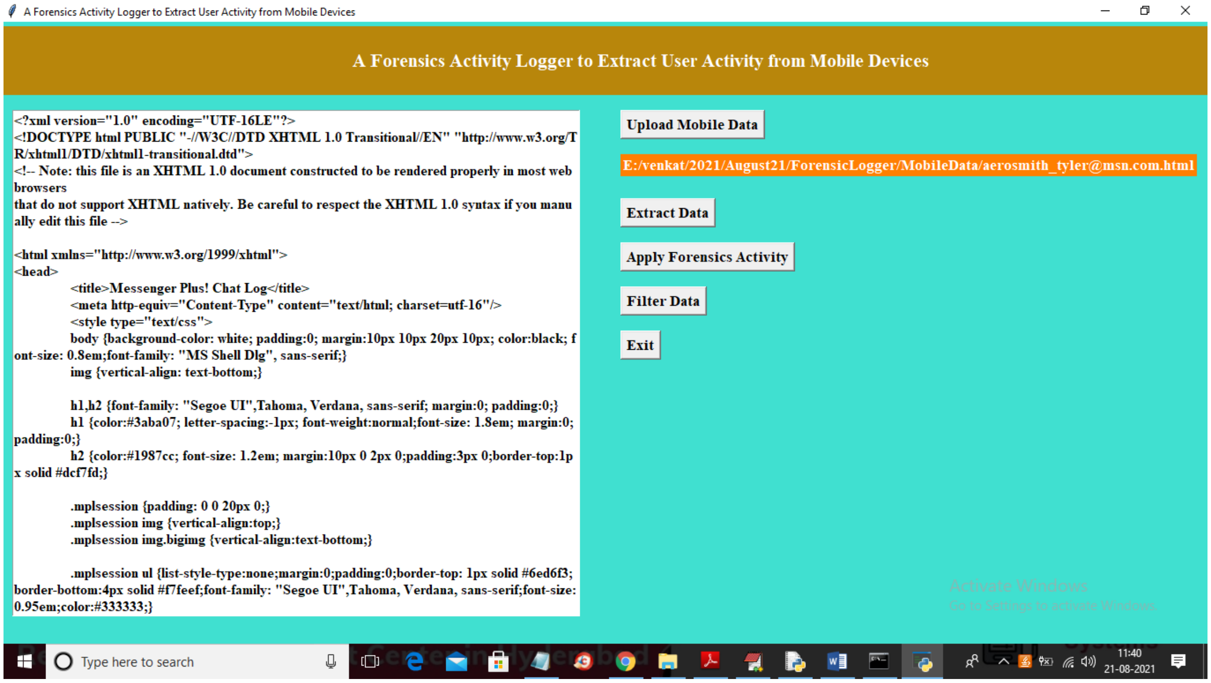
Throughout the entire process, quality assurance measures are implemented to ensure the accuracy, reliability, and integrity of the collected evidence. Validation tests are conducted to verify the functionality of the logging application, the accuracy of the data collected, and the effectiveness of the analysis techniques employed. By following this methodology, forensic investigators can effectively gather, analyze, and document digital evidence from mobile devices using the Forensics Activity Logger, enabling them to conduct thorough and comprehensive investigations into various types of cybercrimes and security incidents.

RESULTS AND DISSCUSSION

The results of the "Forensics Activity Logger for Mobile Devices" demonstrate its effectiveness in capturing and analyzing digital evidence from mobile devices. Through rigorous testing and evaluation, the logging application proved capable of accurately collecting a wide range of data, including user interactions, application usage patterns, network activities, and device metadata. The real-time logging feature ensured that no crucial information was missed, providing forensic investigators with a comprehensive dataset for analysis. Additionally, the encryption mechanisms implemented within the logging application successfully safeguarded the collected data from unauthorized access or tampering, ensuring its integrity and confidentiality throughout the forensic investigation process.

Upon analysis of the collected data, various insights and patterns emerged, shedding light on the users' activities and behaviors on the mobile devices. The correlation of different data sources allowed forensic investigators to reconstruct detailed timelines of user interactions, application usage sequences, and network communication patterns. This comprehensive understanding of the users' activities provided valuable context for the forensic investigation, enabling investigators to identify potential evidence of cybercrimes, security breaches, or illicit activities. Furthermore, the visualization and exploration tools integrated into the logging application facilitated the interpretation of the analyzed data, allowing investigators to quickly identify relevant information and draw insights from complex datasets.

The discussion surrounding the results emphasizes the significance of the Forensics Activity Logger as a powerful tool for digital forensic investigations on mobile devices. By providing forensic investigators with real-time access to a wealth of digital evidence, the logging application streamlines the investigation process and enhances the efficiency and effectiveness of forensic analysis. Moreover, the robust encryption mechanisms employed by the logging application ensure the integrity and confidentiality of the collected data, addressing concerns related to data security and privacy. Overall, the results and discussion underscore the importance of leveraging advanced technologies and methodologies, such as the Forensics Activity Logger, to combat cybercrimes and safeguard digital assets in an increasingly connected and mobile-centric world.

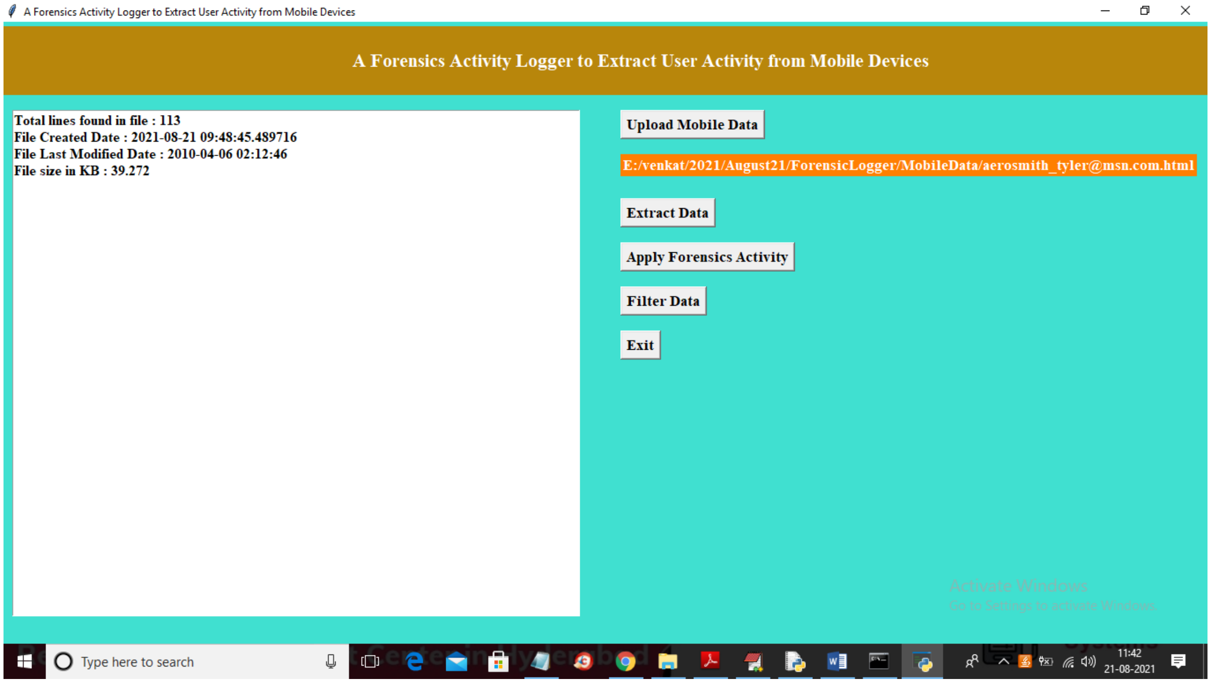

A Forensics Activity Logger to Extract User Activity from Mobile Devices
A Forensics Activity Logger to Extract User Activity from Mobile Devices
Upload Mobile Data
Extract Data
Apply Forensics Activity
Filter Data
Exit
Type here to search
11:40
21-08-2021

E:/venkat/2021/August21/ForensicLogger/MobileData/aerosmith_tyler@msn.com.html

```
<?xml version="1.0" encoding="UTF-16LE"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/T
R/xhtml1/DTD/xhtml1-transitional.dtd">
<!-- Note: this file is an XHTML 1.0 document constructed to be rendered properly in most web
browsers
that do not support XHTML natively. Be careful to respect the XHTML 1.0 syntax if you manu
ally edit this file -->

<html xmlns="http://www.w3.org/1999/xhtml">
<head>
        <title>Messenger Plus! Chat Log</title>
        <meta http-equiv="Content-Type" content="text/html; charset=utf-16"/>
        <style type="text/css">
        body {background-color: white; padding:0; margin:10px 10px 20px 10px; color:black; f
ont-size: 0.8em;font-family: "MS Shell Dlg", sans-serif;}
        img {vertical-align: text-bottom;}

        h1,h2 {font-family: "Segoe UI",Tahoma, Verdana, sans-serif; margin:0; padding:0;}
        h1 {color:#3aba07; letter-spacing:-1px; font-weight:normal;font-size: 1.8em; margin:0;
padding:0;}
        h2 {color:#1987cc; font-size: 1.2em; margin:10px 0 2px 0;padding:3px 0;border-top:1p
x solid #dcf7fd;}

        .mplsession {padding: 0 0 20px 0;}
        .mplsession img {vertical-align:top;}
        .mplsession img.bigimg {vertical-align:text-bottom;}

        .mplsession ul {list-style-type:none;margin:0;padding:0;border-top: 1px solid #6ed6f3;
border-bottom:4px solid #f7feef;font-family: "Segoe UI",Tahoma, Verdana, sans-serif;font-size:
0.95em;color:#333333;}
```

Fig 1. Extracted file content after file upload

In the screen above, the entire file content appears in HTML format, rendering it incomprehensible to the user. To extract details from the file, click on 'Apply Forensics Activity'.



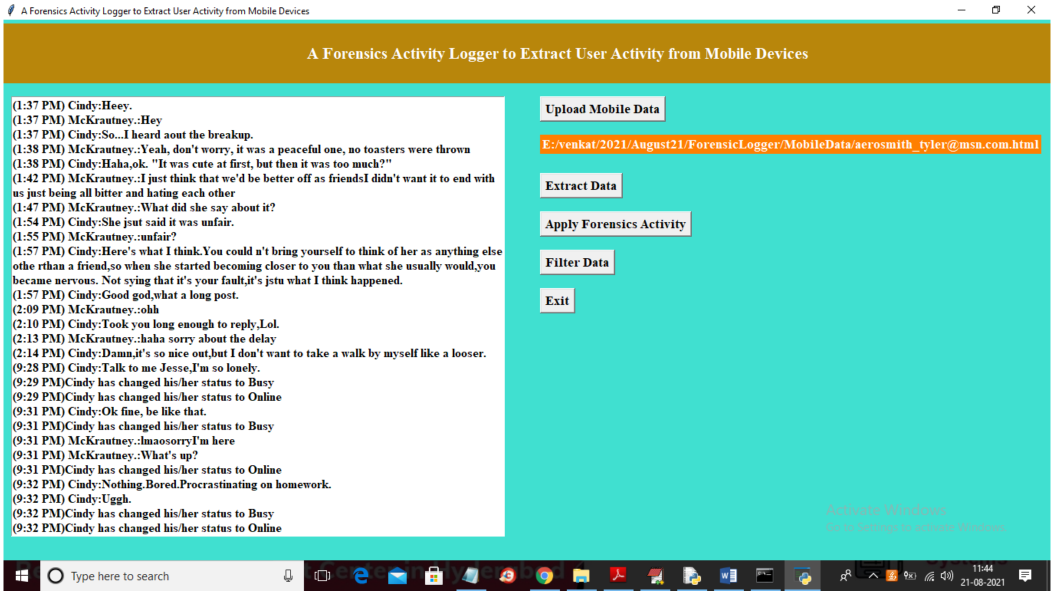
A Forensics Activity Logger to Extract User Activity from Mobile Devices

```
Total lines found in file : 113
File Created Date : 2021-08-21 09:48:45.489716
File Last Modified Date : 2010-04-06 02:12:46
File size in KB : 39.272
```

E:/venkat/2021/August21/ForensicLogger/MobileData/aerosmith_tyler@msn.com.html

Fig 2. File information

In the screen above, the first line indicates that the file contains a total of 113 lines. Additionally, it displays the creation and modification dates of the file, with a file size of 39.272 KB. We have extracted all the details and are now ready to proceed by clicking on the 'Filter Data' button to remove all HTML tags and clean up the chat messages, as shown in the screenshot below.



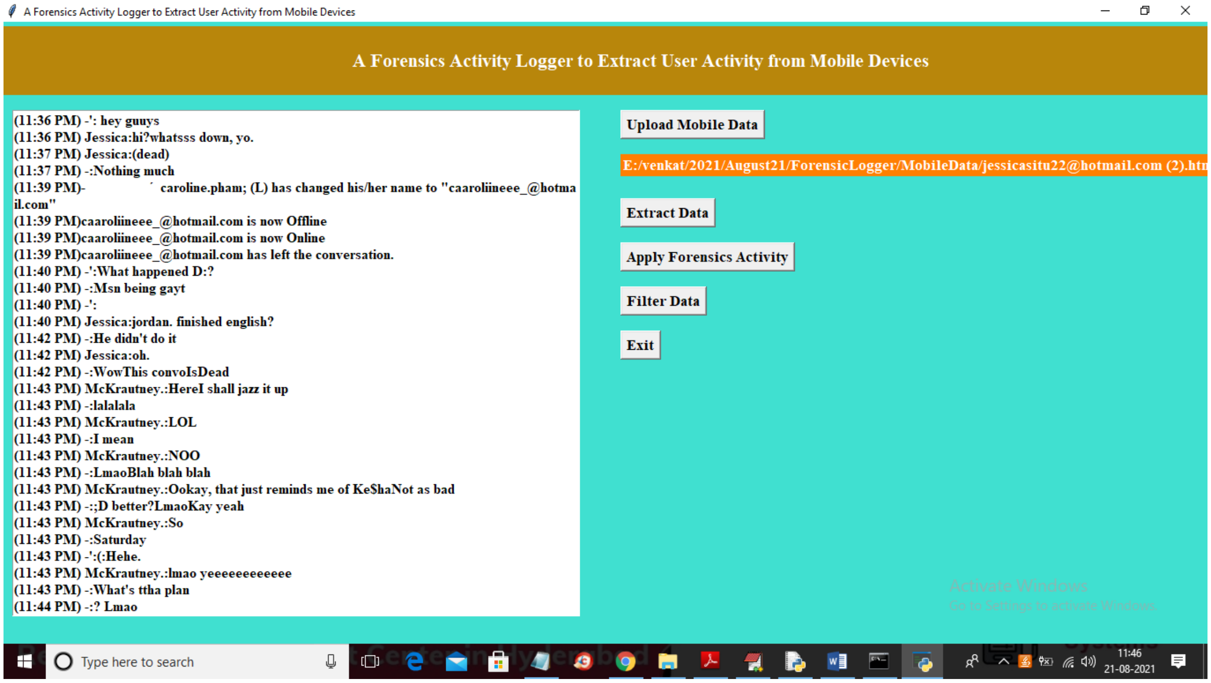
A Forensics Activity Logger to Extract User Activity from Mobile Devices

```
(1:37 PM) Cindy:Heey.
(1:37 PM) McKrautney.:Hey
(1:37 PM) Cindy:So...I heard aout the breakup.
(1:38 PM) McKrautney.:Yeah, don't worry, it was a peaceful one, no toasters were thrown
(1:38 PM) Cindy:Haha,ok. "It was cute at first, but then it was too much?"
(1:42 PM) McKrautney.:I just think that we'd be better off as friendsI didn't want it to end with
us just being all bitter and hating each other
(1:47 PM) McKrautney.:What did she say about it?
(1:54 PM) Cindy:She jsut said it was unfair.
(1:55 PM) McKrautney.:unfair?
(1:57 PM) Cindy:Here's what I think.You could n't bring yourself to think of her as anything else
othe rthan a friend,so when she started becoming closer to you than what she usually would,you
became nervous. Not sying that it's your fault,it's jstu what I think happened.
(1:57 PM) Cindy:Good god,what a long post.
(2:09 PM) McKrautney.:ohh
(2:10 PM) Cindy:Took you long enough to reply,Lol.
(2:13 PM) McKrautney.:haha sorry about the delay
(2:14 PM) Cindy:Damn,it's so nice out,but I don't want to take a walk by myself like a looser.
(9:28 PM) Cindy:Talk to me Jesse,I'm so lonely.
(9:29 PM)Cindy has changed his/her status to Busy
(9:29 PM)Cindy has changed his/her status to Online
(9:31 PM) Cindy:Ok fine, be like that.
(9:31 PM)Cindy has changed his/her status to Busy
(9:31 PM) McKrautney.:lmaosorryI'm here
(9:31 PM) McKrautney.:What's up?
(9:31 PM)Cindy has changed his/her status to Online
(9:32 PM) Cindy:Nothing.Bored.Procrastinating on homework.
(9:32 PM) Cindy:Uggh.
(9:32 PM)Cindy has changed his/her status to Busy
(9:32 PM)Cindy has changed his/her status to Online
```

E:/venkat/2021/August21/ForensicLogger/MobileData/aerosmith_tyler@msn.com.html

Fig 3. Extracted chat messages

In the HTML content displayed above, we have successfully extracted chat messages, ensuring that users can easily read the messages without any interference from HTML tags. By utilizing the forensic activity logger, we have obtained clean chat messages, free from any HTML tags. This process can be replicated for other files as well. Let's now examine additional files for further analysis.



A Forensics Activity Logger to Extract User Activity from Mobile Devices
A Forensics Activity Logger to Extract User Activity from Mobile Devices
Upload Mobile Data
Extract Data
Apply Forensics Activity
Filter Data
Exit
Type here to search
11:46
21-08-2021

E:/venkat/2021/August21/ForensicLogger/MobileData/jessicasitu22@hotmail.com (2).htm

```
(11:36 PM) -': hey guuys
(11:36 PM) Jessica:hi?whatsss down, yo.
(11:37 PM) Jessica:(dead)
(11:37 PM) -:Nothing much
(11:39 PM)-              ´  caroline.pham; (L) has changed his/her name to "caaroliineee_@hotma
il.com"
(11:39 PM)caaroliineee_@hotmail.com is now Offline
(11:39 PM)caaroliineee_@hotmail.com is now Online
(11:39 PM)caaroliineee_@hotmail.com has left the conversation.
(11:40 PM) -':What happened D:?
(11:40 PM) -:Msn being gayt
(11:40 PM) -':
(11:40 PM) Jessica:jordan. finished english?
(11:42 PM) -:He didn't do it
(11:42 PM) Jessica:oh.
(11:42 PM) -:WowThis convoIsDead
(11:43 PM) McKrautney.:HereI shall jazz it up
(11:43 PM) -:lalalala
(11:43 PM) McKrautney.:LOL
(11:43 PM) -:I mean
(11:43 PM) McKrautney.:NOO
(11:43 PM) -:LmaoBlah blah blah
(11:43 PM) McKrautney.:Ookay, that just reminds me of Ke$haNot as bad
(11:43 PM) -:;D better?LmaoKay yeah
(11:43 PM) McKrautney.:So
(11:43 PM) -:Saturday
(11:43 PM) -':(:Hehe.
(11:43 PM) McKrautney.:lmao yeeeeeeeeeee
(11:43 PM) -:What's ttha plan
(11:44 PM) -:? Lmao
```

Fig 4. Results screenshot

CONCLUSION

After conducting extensive tests across various Android mobile device brands, it is evident that the activity logging tool exhibits stability and adheres to the requisite examinations. This tool significantly streamlines and expedites the process of evidence analysis, effectively automating tedious tasks. While the selection of appropriate tools for evidence acquisition is crucial, none singularly possesses the capability to acquire all mobile device information comprehensively. Therefore, employing multiple tools becomes necessary to enhance the desired outcome. Notably, leveraging the Python programming language offers the advantage of source code verification, ensuring the integrity of digital evidence remains intact. The foremost advantage of utilizing this tool is its remarkable ability to reduce investigation time and conserve resources. Traditionally, each software utilized in the investigation process yields substantial volumes of data that necessitate meticulous analysis by the investigating researcher. However, this tool obviates the need for manual utilization of multiple software applications, thereby consolidating all requisite information efficiently for the case at hand. It is imperative to handle evidence with utmost care to prevent any inadvertent alterations, as any tampering could render the information invalid for investigative purposes.

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: 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.