IJARST
International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

A Forensics Activity Logger to Extract User Activity from Mobile Devices

Dr.C.Ramesh Kumar [1] and Mr.P.Vinay Kumar [2]

[1] Assoc.Professor, Department of Information Technology, MREC (A), Hyderabad-500100

[2] Assistant Professor, Department of Information Technology, MREC (A), Hyderabad-500100

Abstract-Nowadays, mobile devices have become one of the most popular instruments used by a person on its regular life, mainly due to the importance of their applications. In that context, mobile devices store user’s personal information and even more data, becoming a personal tracker for daily activities that provides important information about the user. Derived from this gathering of information, many tools are available to use on mobile devices, with the restrain that each tool only provides isolated information about a specific application or activity. Therefore, the present work proposes a tool that allows investigators to obtain a complete report and timeline of the activities that were performed on the device. This report incorporates the information provided by many sources into a unique set of data. Also, by means of an example, it is presented the operation of the solution, which shows the feasibility in the use of this tool and shows the way in which investigators have to apply the tool.

Keywords: Forensic, Mobile Devices

1. Introduction

Nowadays, mobile devices are used for a wide spread of tasks (e.g., entertainment, education, communication, socialization, research, commercial transactions). As a result of said use, the devices store information related to the user´s behavior. Therefore, they constitute an important source of evidence for forensics analysis

Also, the forensics analysis uses a set of techniques that allow the collection and extraction of information from different devices without altering their original state [2]. For example, it can recover deleted files, browsing history, instant messaging information, login data, among others, all these types of information are known as digital evidence. 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 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. Thus, this paper presents a tool, which has been implemented in Python [10], that generates a unique report with all the information about the mobile device user's behavior, by means of the collection of information from different applications that are installed on the it, which runs on Android OS. This information is then used to obtain a track of the users' activities while using the mobile device.

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, 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]. Moreover, Alyahya and Kausar [13] analyze Snapchat application on an Android platform by using two forensics analysis tools, Autopsy and AXIOM Examine. On the same context, Walnycky et al., [14] analyze 20 Android applications (e.g., WhatsApp, Viber, Instagram, Facebook Messenger, Tango), in which the digital evidence that could be used for forensics analysis, is examined, and also they evaluate the security involved in sending/receiving data and application privacy

2. Literature Survey

a. The next generation for the forensic extraction of electronic evidence from mobile telephones

Electronic evidence extracted from a mobile telephone provide a wealth of information about the user. Before a court allows the trier of fact to consider the electronic evidence, the court must ensure that the subject matter, testimony of which is to be given, is scientific. Therefore, regard must, at the investigation stage, be given to fulfill the requirements of science and law, including international standards. Such compliance also moves the extraction of electronic evidence from mobile telephones into the next generation, a more rigorous position as a forensic science, by being able to give in court well- reasoned and concrete claims about the accuracy and validity of conclusions.

b. A critical review of 7 years of Mobile Device Forensics

Mobile Device Forensics (MF) is an interdisciplinary field consisting of techniques applied to a wide range of computing devices, including smartphones and satellite navigation systems. Over the last few years, a significant amount of research has been conducted, concerning various mobile device platforms, data acquisition schemes, and information extraction methods. This work provides a comprehensive overview of the field, by presenting a detailed assessment of the actions and methodologies taken throughout the last seven years. A multilevel chronological categorization of the most significant studies is given in order to provide a quick but complete way of observing the trends within the field. This categorization chart also serves as an analytic progress report, with regards to the evolution of MF. Moreover, since standardization efforts in this area are still in their infancy, this synopsis of research helps set the foundations for a common framework proposal. Furthermore, because technology related to mobile devices is evolving rapidly, disciplines in the MF ecosystem experience frequent changes. The rigorous and critical review of the state-of-the-art in this paper will serve as a resource to support efficient and effective reference and adaptation.

c. Digital evidence from mobile telephone applications

In this paper we examine the legal aspects of the forensic investigation of mobile telephone applications. Mobile telephone applications might be involved with a variety of types of computer misuse including fraud, theft, money laundering, dissemination of copyrighted materials or indecent images, or instances where mobile telephone applications have been involved in the transmission of malware for malicious or criminal purposes. In this paper we examine the process of the forensic investigation of mobile telephone applications, and the issues relating to obtaining digital evidence from mobile telephone applications

d. "Open Source Digital Forensics Tools : The Legal Argument

This paper addresses digital forensic analysis tools and their use in a legal setting. To enter scientific evidence into a United States court, a tool must be reliable and relevant. The reliability of evidence is tested by applying "Daubert" guidelines. To date, there have been few legal challenges to digital evidence, but as the field matures this will likely change. This paper examines the Daubert guidelines and shows that open source tools may more clearly and comprehensively meet the guidelines than closed source tools.

e. "Analysis of Digital Forensic Tools and Investigation Process

Popularity of internet is not only change our life view, but change the view of crime in our society or all over the world. Increasing the number of computer crime day by day is the reason for forensic investigation. Digital forensic is used to bring justice against that person who is responsible for computer crimes or digital crimes. In this paper, we explain both type of forensic tool commercial as well as open source and comparisons between them. We also classify digital forensic and digital crimes according to their working investigation. In this paper, we proposed a model for investigation process to any type of digital crime. This model is simple and gives efficient result to any type of digital crimes and better way to improve the time for investigation.

Nowadays, mobile devices have become one of the most popular instruments used by a person on its regular life, mainly due to the importance of their applications. In that context, mobile devices store user's personal information and even more data, becoming a personal tracker for daily activities that provides important information about the user. Derived from this gathering of information, many tools are available to use on mobile devices, with the restrain that each tool only provides isolated information about a specific application or activity

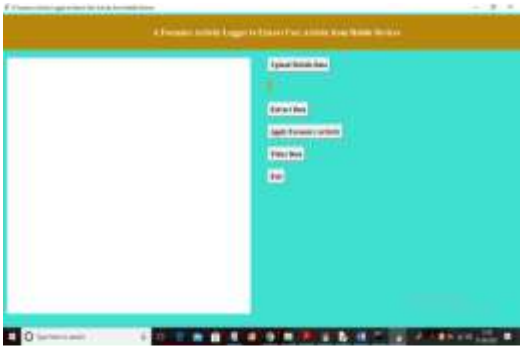
3. Proposed System

Therefore, the present work proposes a tool that allows investigators to obtain a complete report and timeline of the activities that were performed on the device. This report incorporates the information provided by many sources into a unique set of data. Also, by means of an example, it is presented the operation of the solution, which shows the feasibility in the use of this tool and shows the way in which investigators have to apply the tool.

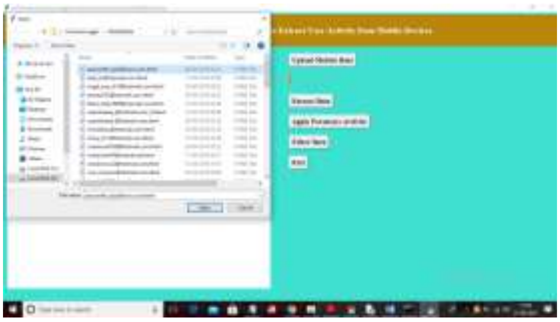
1) Upload Mobile Data: using this module we will upload chat log HTML messages files to application
2) Extract Data: using this we will extract HTML data from uploaded file and then display content of that file
3) Apply Forensics Activity: using this module we will extract file size, file creation and modification date and number of lines in that file

4) Filter Data: In this module we apply HTML parsers to remove HTML tags from chat logs and then display clean chat messages between users.

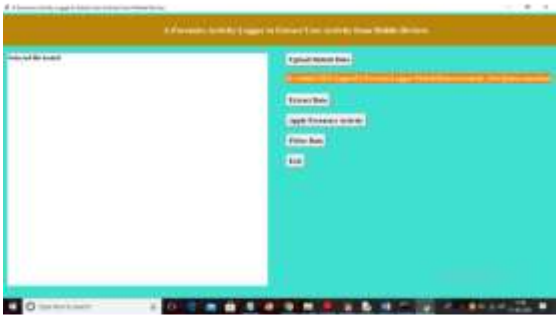
4. Results Analysis



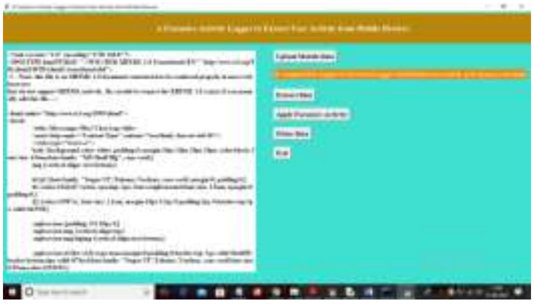
In above screen click on 'Upload Mobile Data' button to upload chat log file



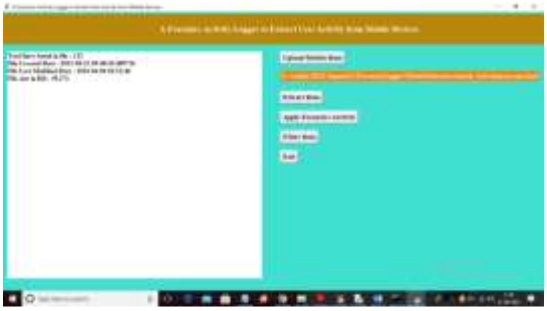
In above screen I am selecting and uploading first chat log file and then click on 'Open' button to get below screen



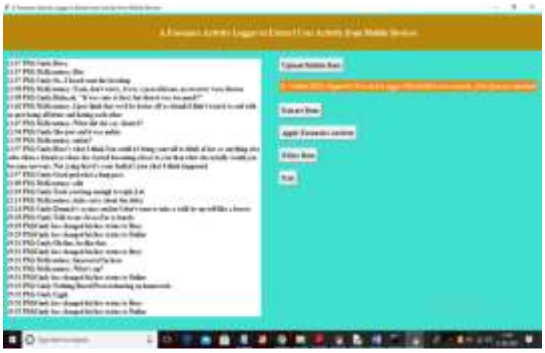
In above screen chat log file is uploaded and now click on 'Extract Data' button to extract content from file



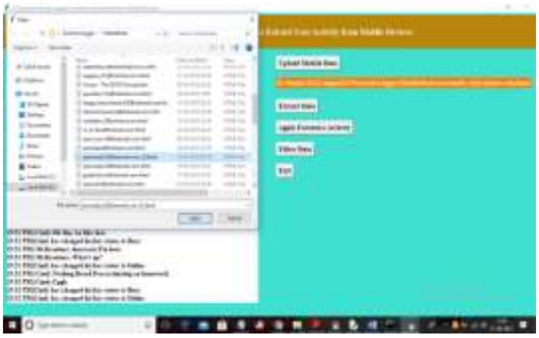
In above screen we can see entire file content is in HTML format and user cannot understand anything from that so click on 'Apply Forensics Activity' to extract details from file

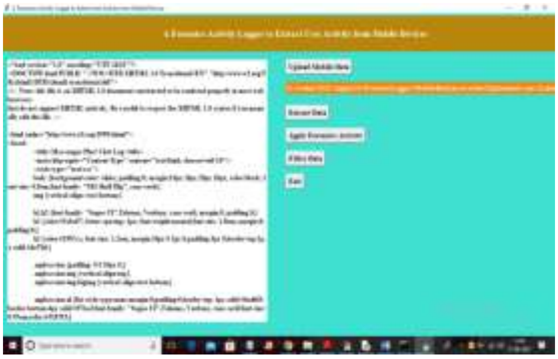


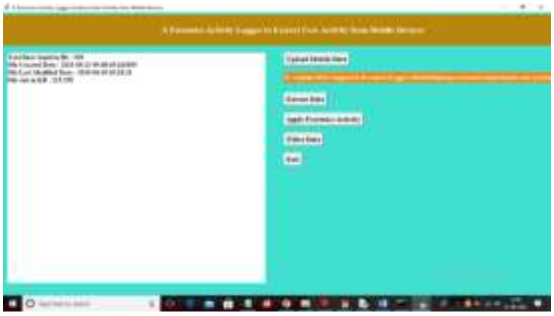
In above screen in first line we can see file contains total 113 lines and we can see file created and modified date and file size is 39.272 KB and now we extracted all details and now click on 'Filter Data' button to removed out all HTML tags to clean chat message like below screen



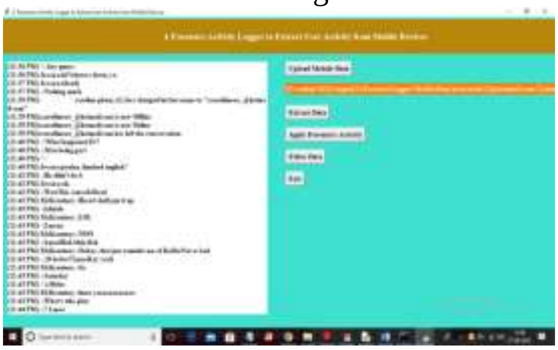
In above screen from HTML content we extracted chat messages and user can read above messages clearly. So by applying forensic activity logger we have clean chat messages from HTML tags. Similarly you can upload other file and extract messages. Now see other files







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



5. Conclusion

Based on several tests performed with different brands of Android mobile devices; it can be concluded that the activity registration tool is stable and complies with the requested examinations

The tool automates and reduces the time of evidence analysis. Selecting the right tools for the acquisition of evidence that serves as input to the application represents a crucial piece of research; however, none of them possess the ability to acquire all the information of a mobile device. Therefore, it is necessary to use several of them to improve the desired result. Finally, the advantage of using Python programming language, is that it allows to verify the source code and thus, validate that it does not alter the digital evidence

The main advantage found while using this tool is that it reduces the time used on an investigation and saves resources. This because each installed software returns large volumes of information that must be analyzed step by step by the researcher in charge. Thus, this tool avoids the manual use of more than one software to get all the information that is required for the case The evidence has to be carefully manipulated, because if the information is altered in any way, this will not be valid for the investigation

Future Work

Finally, the presented study, gives a first view on the handling of digital evidence in mobile devices with Android OS, this later can be developed for other operating systems such as iOS and Windows Phone. For further work, it is necessary to increase the interoperability to gather the information from third party solutions and propose connectors and generic ways to extract evidence. Also, it is important to measure and perform future improvements in certain non-functional characteristics of this tool (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.

[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].