ENGINEERING IN ADVANCED RESEARCH SCIENCE AND TECHNOLOGY

ISSN 2350-0174
Vol.03, Issue.03
October-2023
Pages: 921-929

A NOVEL FORENSICS ACTIVITY LOGGER TO EXTRACT USERS ACTIVITY USING CELLULAR UNITS

[*]Dr. M.VANITHA
D.Neharika[1], D.Prathima[2], D. Hari Priya[3], G. Naga Namratha[4]
[*]Professor, [1]UG Scholar, [*,1,2,3,4] Department of Computer Science and Engineering
[1,2,3,4] Malla Reddy Engineering College for Women (A), Maisammaguda, Medchal, Telangana.

Abstract

Nowadays, cellular units have emerge as one of the most famous units used through a character in its normal life, basically due to the significance of their applications. In that context, cellular units save user's non-public facts and even extra data, turning into a private tracker for day by day things to do that gives vital statistics about the user. Derived from this gathering of information, many equipment are reachable to use on cell devices, with the restrain that every device solely affords remoted statistics about a unique software or activity. Therefore, the current work proposes a device that permits investigators to reap a entire record and timeline of the things to do that have been carried out on the device. This record contains the data supplied by way of many sources into a special set of data. Also, by means of capability of an example, it is introduced the operation of the solution, which indicates the feasibility in the use of this device and indicates the way in which investigators should follow the tool.

Keywords: significance, cellular units, investigators, timeline

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 Crime Scene Examination analysis. Also, the Crime Scene Examination 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 Crime Scene Examination analysis: i) avoid contamination of the evidence to prevent misinterpretations; ii) act methodically, that is, all the results of the Crime Scene Examination 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 Crime Scene Examination 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 Crime Scene Investigation 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 Crime Scene Examination 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 Crime Scene Investigation images and locating partitions of the digital devices. Also, Shortall and Azhar [8] and Tajuddin and Manaf [9] present several popular Crime Scene Investigation tools, such as Cellebrite UFED, MOBILedit Crime Scene Investigation, Crime Scene Investigation Toolkit, XRY, Oxygen Crime Scene Investigation Suite, EnCASE Crime Scene Investigation, 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 Crime Scene Investigation Suite has a variety of options to perform a deep Crime Scene Examination 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 Crime Scene Examination 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 Crime Scene Investigation SQLite Viewer [11]. Moreover, Alyahya and Kausar [13] analyze Snapchat application on an Android platform by using two Crime Scene Examination 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 Crime Scene Examination analysis, is examined, and also they evaluate the security involved in sending/receiving data and application privacy

2. Literature Survey

The next generation for the Crime Scene Investigation 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 Crime Scene Investigation science, by being able to give in court well- reasoned and concrete claims about the accuracy and validity of conclusions.

A critical review of 7 years of Mobile Device Crime Scene Examination

Mobile Device Crime Scene Examination (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.

Digital evidence from mobile telephone applications

In this paper we examine the legal aspects of the Crime Scene Investigation 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 Crime Scene Investigation investigation of mobile telephone applications, and the issues relating to obtaining digital evidence from mobile telephone applications

"Open Source Digital Crime Scene Examination Tools : The Legal Argument

This paper addresses digital Crime Scene Investigation 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.

"Analysis of Digital Crime Scene Investigation 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 Crime Scene Investigation investigation. Digital Crime Scene Investigation 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 Crime Scene Investigation tool commercial as well as open source and comparisons between them. We also classify digital Crime Scene Investigation 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.

"Crime Scene Investigation Acquisitions of WhatsApp Data on Popular Mobile Platform

Encryption techniques used by popular messaging services such as Skype, Viber and WhatsApp make traces of illegal activities by criminal groups almost undetectable. This paper reports challenges involved to examine data of the WhatsApp application on popular mobile

platforms (iOS, Android and Windows Phone) using latest Crime Scene Investigation software such as EnCase, UFED and Oxygen Crime Scene Investigation Suite. The operating systems used were Windows phone 8.1, Android 5.0.1 (Lollipop) and iOS 8.3. Results show that due to strong security features built into the Windows 8.1 system Crime Scene Investigation examiners may not be able to access data with standard Crime Scene Investigation suite and they must decide whether to perform a live Crime Scene Investigation acquisition. This paper provides Crime Scene Examination examiners with practical techniques for recovering evidences of WhatsApp data from Windows 8.1 mobile operating systems that would otherwise be inaccessible.

Crime Scene Investigation investigation and analysis on digital evidence discovery through physical acquisition on smartphone

Cybercriminals are changing their strategies as users are less concerns on the smartphone and social networks security risks such as spams, that will threaten them as they are more dependent on the smartphone [1]. Thus, there's a need to perform the smartphone Crime Scene Examination analysis to retrieve and analysed the potentially great amounts and extremely valuable information on these devices. This paper investigates a wealth of personal and sensitive data by types of digital information as evidence and conducted Crime Scene Investigation analysis on a popular smartphone Samsung Galaxy Note III. The standard approach applied to extract information from smartphone through physical acquisition and analysis using Cellebrite UFED. The results are presented to demonstrate the smartphone as a goldmine for investigators and as sources of digital evidence. Furthermore this research also presents the Crime Scene Investigation tool and techniques for acquiring and examining digital evidence on this device. The evidence discovered include files, contacts, events of smartphone and social network data storage and location. The smartphone examined produced abundant user information and in total 98,127 artefacts were recovered. Performing the extraction and analysis of digital evidence over smartphone activities show the possibility of identifying potential suspects that could assist the Crime Scene Investigation investigators in crime investigations.

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.

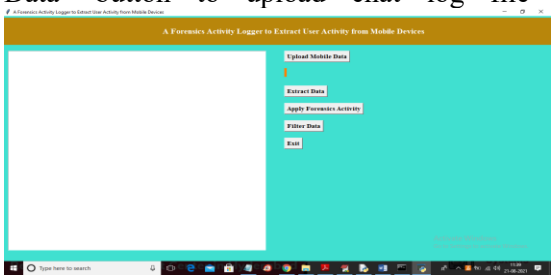
Detects and counts the number of files according to the type.

- Determines the number of sheets, columns and rows in a Microsoft Excel file and the number of lines in text files. This activity is performed to indicate the length of each file.
- Gets the column that contains the date and time of the users' activity.
- Compares the date entered by the Crime Scene Examination

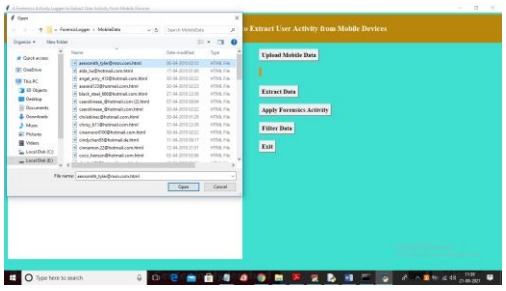
investigator with the date of the evidence.
- Saves the filtered data.
- Merges the data in a single file.
- Organizes the data in a descending order, so it is chronologically order.
- Deletes repeated data.
- Assigns a code to each activity.
- Saves the report.

4. RESULTS

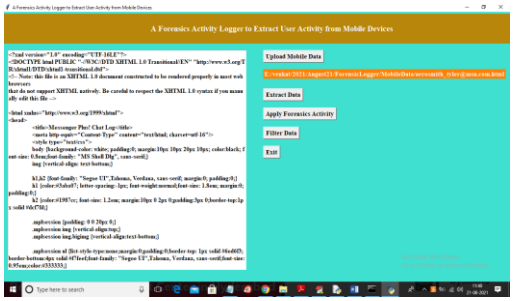
In above screen click on 'Upload Mobile Data' button to upload chat log file



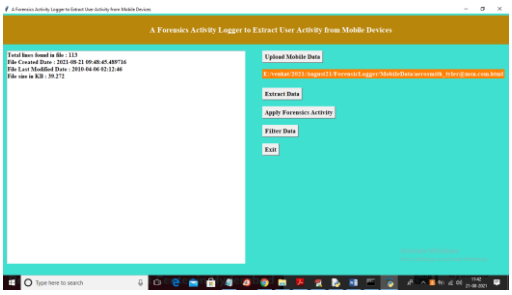
In above screen I am selecting and uploading first chat log file and then click on 'Open' button to get below screen



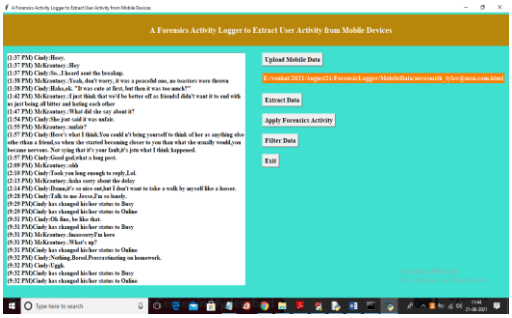
In above screen I am selecting and uploading first chat log file and then click on 'Open' button to get below screen



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



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

5. Conclusion

Based on quite a few checks carried out with extraordinary manufacturers of Android cell devices; it can be concluded that the endeavor registration device is steady and complies with the requested

examinations The device automates and reduces the time of proof analysis. Selecting the proper equipment for the acquisition of proof that serves as enter to the utility represents a vital piece of research; however, none of them possess the potential to gather all the facts of a cell device. Therefore, it is critical to use various of them to enhance the favored result. Finally, the benefit of the use of Python programming language, is that it approves to affirm the supply code and thus, validate that it does no longer alter the digital evidence.

The foremost gain located whilst the usage of this device is that it reduces the time used on an investigation and saves resources. This is due to the fact every established software program returns massive volumes of statistics that have to be analyzed step by using step by way of the researcher in charge. Thus, this device avoids the guide use of extra than one software program to get all the records that is required for the case. The proof ought to be cautiously manipulated, due to the fact if the records is altered in any way, this will no longer be legitimate 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 Crime Scene Investigation extraction of electronic evidence from mobile telephones,” Int. Work. Syst.
Approaches Digit. Crime Scene Examination Eng., SADFE, 2014.

[2] K. Barmpatsalou, D. Damopoulos, G. Kambourakis, and V. Katos, “A critical review of 7 years of Mobile Device Crime Scene Examination,” 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 Crime Scene Examination 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 Crime Scene Investigation Tools and Investigation Process," High Perform. Archit. Grid …, pp. 435–441, 2011.

[8] A. Shortall and M. A. H. Bin Azhar, "Crime Scene Investigation 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, "Crime Scene Investigation 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, "Crime Scene Investigation analysis of Telegram Messenger on Android smartphones," Digit. Investig., vol. 23, pp. 31–49, 2017.

[12] C. Anglano, "Crime Scene Investigation 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 Crime Scene Investigation 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 Crime Scene Investigation analysis of Android social-messaging applications," Digit. Investig., vol. 14, no. S1, pp. S77–S84, 2015.

[15] I. P. Agus, "Prototyping SMS Crime Scene Investigation Tool Application Based On Digital Crime Scene Investigation 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 Crime Scene Investigation 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 Crime Scene Examination - Mobile Crime Scene Examination solutions: software and hardware." [Online]. Available: https://www.oxygen-Crime Scene Investigation.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].

[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].

AUTHOR

Dr.M.Vanitha Professor, Department of CSE,MallaReddy Engineering College for Women, Hyderabad, vanitha. official @gmail.com