JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

FORENSICS ACTIVITY LOGGER TO EXTRACT USER ACTIVITY FROM MOBILE DEVICES USING ML

[1]Saba Muttagi, [2] S.A. Quadri

[1]PG Student, [2]Professor
[1]Department of Computer Networks & Engineering,
[1]Secab Institute of Engineering & Technology, Vijayapura, India
mailto:sabamuttagi@gmail.com

ABSTRACT: ***In today's world the favored instrument mobile device is been in use in persons way of life, thanks to new applications and their uses. There in conditions the mobile devices store personal info of the person and also the knowledge, turning into the trailing device with daily tasks regarding the person. Explanation from the data there are more tools obtainable for various tasks, there are specific applications for that specific task, that is isolated info for that specific task. Therefore, this endeavor provides a tool that gives agents access to a complete description and timetable of the actions that were still being carried out on the trick. This description combines the information offered by many foundations based on a single informational standard. In a similar manner, by sample suggestions, the circumstance bestowed the way of the response, demonstrating the applicability of the tool in practice and outlining the manner in which agents should use it.***

Index Terms – Forensics activity, User activity, Chat logs, Mobile data, Machine learning

I. INTRODUCTION

Nowadays, mobile devices are useful in daily applications for the purpose of entertainment, education, socialization, transaction, and research. Thus, the mobile devices store the users research information. As a result, they serve as a crucial evidence source for forensics investigation.

Additionally, the forensics study utilizes a collection of methods that enable the collection and retrieval of information from a variety of different platforms without altering those systems' initial characteristics. In addition, this could retrieve data recovery, internet activity, instant messaging, login information, and other types of so-called "digital evidence" data.

According to Iorio et al., the forensics analysis should take into account the following three factors: I operate systematically, which means that every forensics method results should be documented; ii) avoid contaminating the evidence to prevent misunderstandings; and iii) maintain the custody chain by using a procedure. Additionally, when conducting a forensics investigation, it is important to take legal considerations into account. If done incorrectly, these considerations might lead to the misuse of applications, fraud, theft, the distribution of proprietary information, etc. According to Taylor et al., in order to prevent the unwarranted disclosure of personal information, it is required to adhere to all legal guidelines relevant to the jurisdiction where the dispute is formed.

Encase, DFF, FTK, Helix, Oxygen, MOBIL Edit, and UFED are a few examples of applications that are used for rhetorical analysis and allow for the examination of various aspects of mobile devices (e.g., internal memory, applications, messages). Now, the alleged suites combine all of the earlier points into a single study to create a powerful and practical tool. Additionally, it's important to take into account that using free tools for forensic analysis throughout an inquiry has its advantages (e. g., no-cost, straightforward to look at in court, permits verification). However, industrial instruments are utilized as well because they offer a good selection of possibilities for examination. Six industrial and open supply applications are contrasted in Yadav et al. These tools carry out operations like convalescence, activity keyword searches, convalescence cookies, rhetorical picture creation, and digital device partition location. Additionally, Shortall, Azhar, Tajuddin, and Manaf give out a variety of cutting-edge rhetorical tools, such as Cellebrite UFED, MOBIL edit rhetorical, rhetorical Toolkit, XRY, atomic number 8 rhetorical Package, in scenario rhetorical, and Paraben's gadget seizing. Every of them includes completely unique capacities, efficacy, and data collection options, but they also offer comparable services, analytical methods, and knowledge dissemination strategies. For contrast, UFED searches for physical information on the Winchester disk to retrieve erased data, while the Chemical Element Detection Kit offers a variety of options for doing a thorough detective investigation. According to the study of the research mentioned and as far as everyone is aware, there are currently no options that provide a complete log of the consumers' activity when using a smartphone, thus the researcher utilizes more than one instrument to get all the data. In order to obtain information about the behavior of mobile device users, this paper introduces a tool that has been implemented in Python and gathers data from a variety of programmes that are installed on the device, which runs on the robot OS. Then, using the smartphone as a weapon, this data is used to keep a check on the users' actions.

Recent research on mobile forensics analysis has primarily focused on the iOS and Golem operating systems, which are only intended for the investigation of particular programmes. When WhatsApp is installed on devices running Golem, Anglano et al. examine the objects produced by the software and argue that these objects can be used to extract various types of information. They employ FTK Imager, SQLite Man, and SQLite v.3 databases as their instruments. In a separate study from the same publishers, they look at data gleaned from Telegram. Then as outcome, this offers the gratitude for displaying the customer database, the timeline of events, the posts that are modified, as well as the materials of the documents that are transmitted or accepted, of these including the recruitment of the instruments: SQLite info, UFED, and gas verbal SQLite Observer. Additionally, using the forensics investigation tools Autopsy and AXIOM Examine, AL Yahya Associate in Nursingd Kausar examined the Snapchat application on the Golem platform. In a similar perspective, Walnycky et al. examine twenty mobile apps (such as WhatsApp, Viber, Instagram, Facebook courier, Tango), wherein they evaluate the security associated with transmitting and receiving information as well as the security of the program.

II. SYSTEM DESIGN

2.1 UML schematics

UML stands for Unified Modeling Language. UML is a consistent universal modelling language that is also used in the field of object-oriented code engineering. The regulation was created and is under the control of the section administrative organization.
The primary goal is to establish UML as the de facto modelling language for object-oriented portable software programs. The two fundamental components of UML today are a conceptual model and a notation. UML could potentially be stacked or paired with another philosophy or methodology in the interval.

GOALS:

The following are the primary goals for the UML's design:

1. Provide customers with a fully prepared graphic model - based language for communication so they may create and trade significant designs.
2. Provide mechanisms for customization and flexibility to strengthen the basic concepts.
3. Work independently using specific programming technologies and methodologies, etc.

2.2 Use case model

Inside its Unified Modeling Language (UML), a use case model can be any of the operational layouts that are specified by and result from a use-case study. Its goal is to provide a graphical overview of the functionality a system offers in terms of actors, their objectives (expressed like use cases), and such links among those use cases. A use case diagram's primary role is to show the system functions an actor performs. The roles of the players in the network are frequently defined.

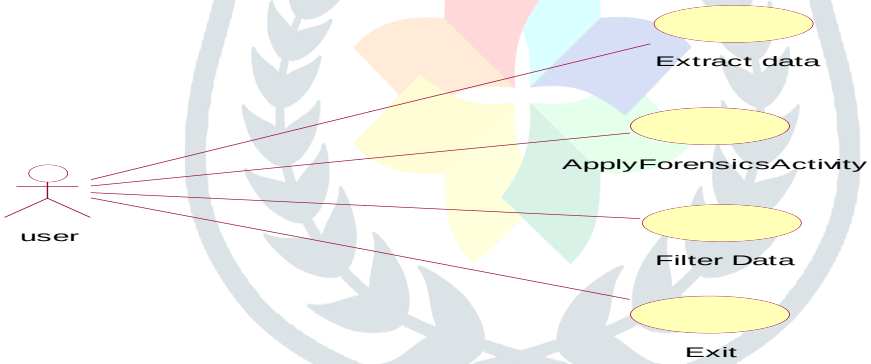


Fig 1: Use-case model

2.3 A class diagrams

In software design, a class diagram using the UML (Unified modeling language) is a type of static structural diagram that displays the classes, characteristics, functions (or procedures), and connections between the categories to represent the architecture of a system. It clarifies that the object collects information.

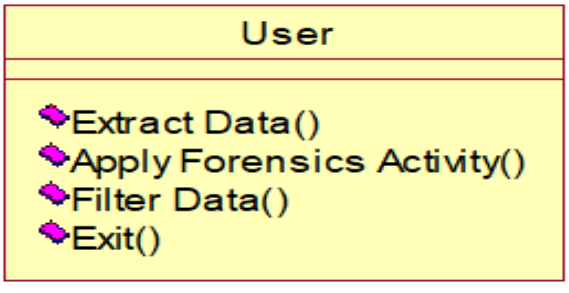


Fig 2: Class diagram

2.4 The sequence of actions

An interaction diagram that demonstrates how processes interact among themselves and according to what order is known as a sequence diagram in the Unified Modeling Language (UML). It is a Data Flow Chart construct. Event charts, event objects, and chronological attribute diagrams are common names for sequence diagrams.

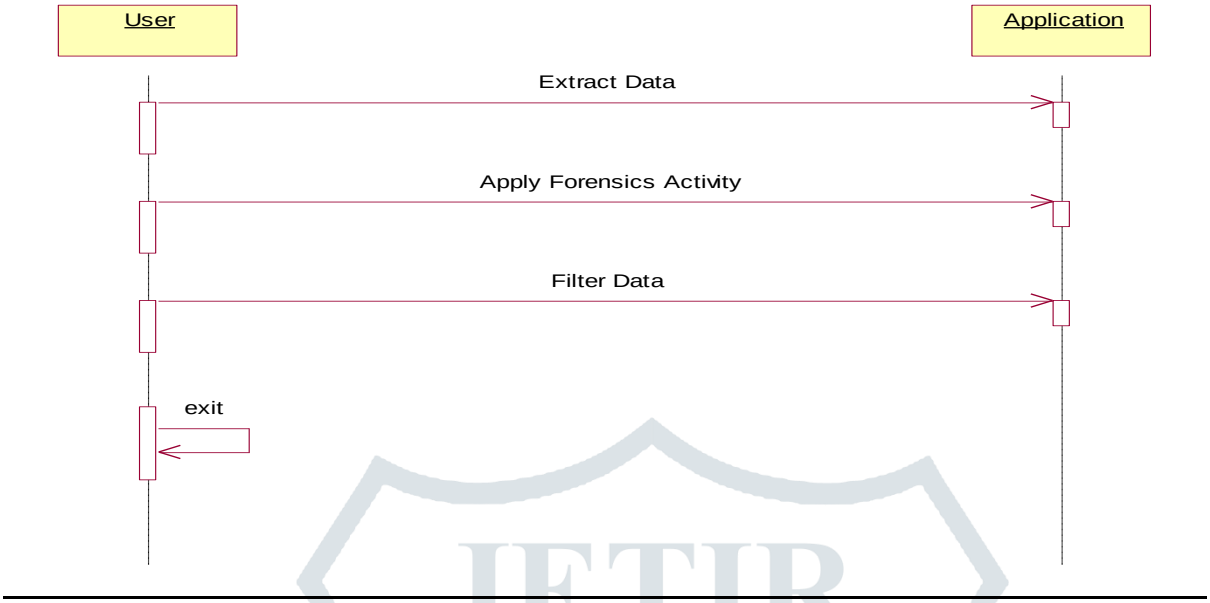


Fig 3: Sequence diagram

2.5 Implementation

Modules:

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.

III. RESEARCH METHODOLOGY

3.1 Existing system

Nowadays, mobile devices became one in all the foremost well-liked instruments utilized by an individual on its regular life, primarily because of the importance of their applications. therein context, mobile devices store user's personal data and even additional knowledge, changing into a private hunter for daily activities that gives vital data regarding the user. Derived from this gathering of knowledge, several tools area unit offered to use on mobile devices, with the restrain that every tool solely provides isolated data a few specific application or activity.

3.2 Proposed system

The current work therefore suggests a device that allows researchers access to a comprehensive documentation and timeline of the operations that were carried out on the devices. This paper combines the relevant data to create a brand-new knowledge body. Additionally, the functionality of such solution is demonstrated by way of an example, demonstrating both the viability of using this instrument and the manner in which researchers must put it to use.

Calculates the number of documents in accordance with the type after being discovered.

- Establishes how many sheets, columns, and rows there are in an Excel spreadsheet as well as how many lines there are in text files.

This process is done to show how long each file is.

- Retrieves the column containing the date / time of an individual's action.
- Contrasts the evidence's date with the date the forensics researcher entered.
- The cleaned data is kept.
- Combines all of the information into one file.
- Creates a regular pattern by sorting the information in lowest to highest.
- Removes redundant info.
- Gives each action a code.
- Stores the document

3.3 System study

Feasibility study:

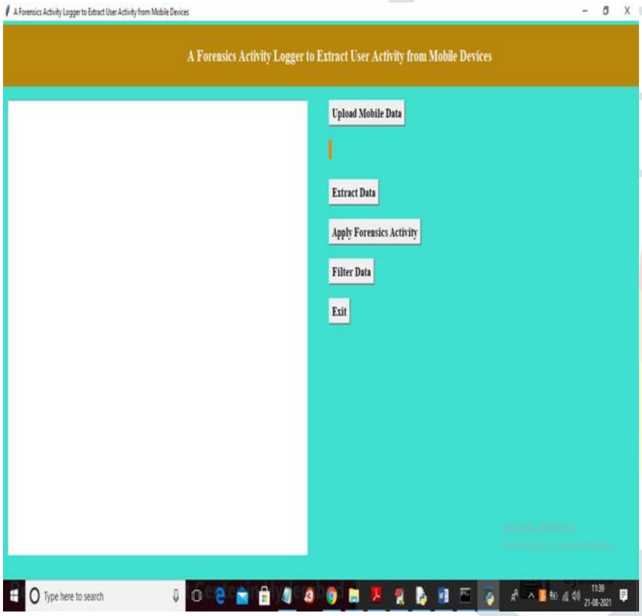
The project's viability is examined in this stage, and a business plan is presented along with a very basic plan for the endeavor and a number of cost estimates. The feasibility assessment of the proposed system should be used all across the network analysis phase. something might be done to ensure that the intended system won't burden the business. Determining the top needs for such system is necessary for achievability study.

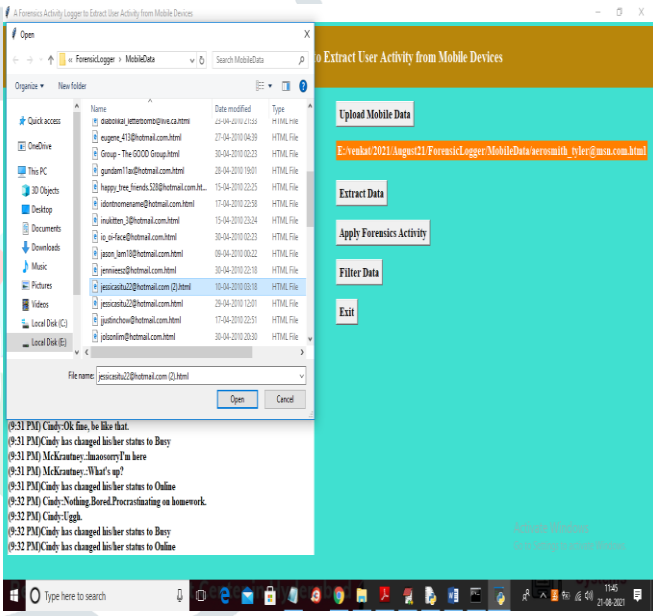
The feasibility analysis takes into account three main factors: i.e.

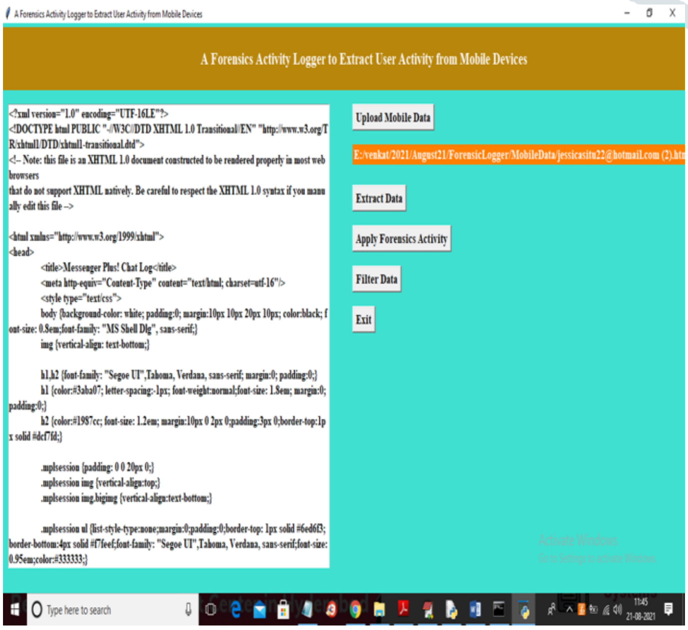
- Business viability
- Technical feasibility
- Social acceptability

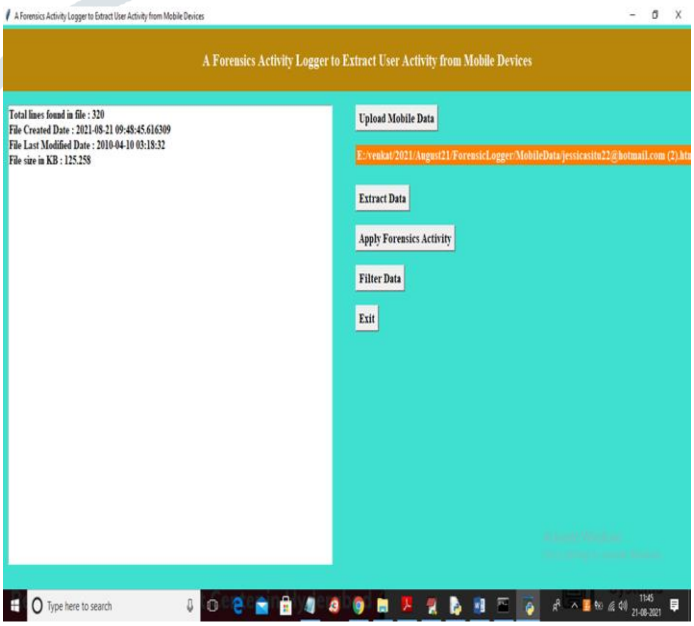
IV. RESULTS

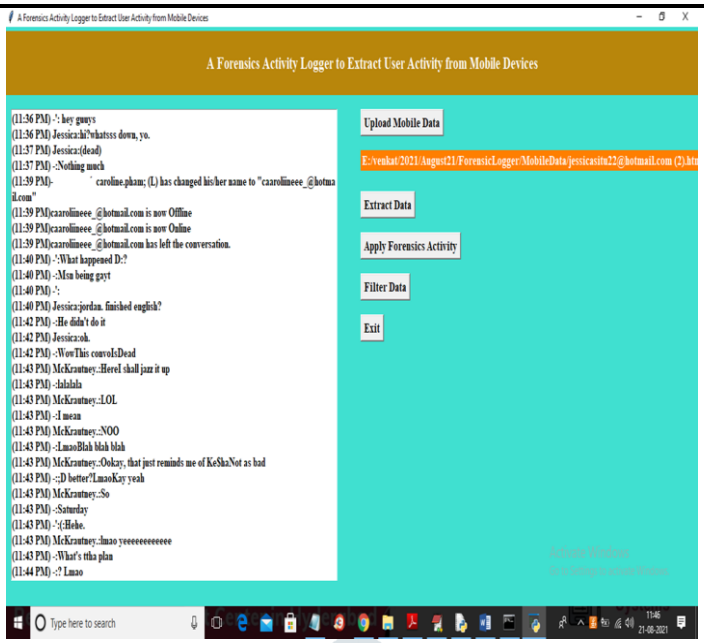
a. To upload the chat log file, click the "Upload Mobile Data" button in the previous screen.
b. I'm choosing and uploading a chat file in the screen above. After that, I click the "Open" button to bring up the screen below.
c. Above the panel chat log file is uploaded and now click on ‘Extract Data’ button to extract content from file
d. 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.
e. In above screen in first line, we can see file contains total 320 lines and we can see file created and modified date and file size is 125.258 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.
f. 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.











V. CONCLUSION

It can be deduced from a number of tests using various Android smartphone brands that the event reporting device is reliable and meets the requirements for the specified tests.

The programme speeds up and automates the analysis of the evidence. Finding the best tools for gathering data that will be used as input for the application is an important part of the research process, but none of them can get all the data from a mobile device. As a result, combining multiple of them is required to achieve the desired outcome. The ability to examine the source code consequently, confirm that because it does not change the electronic evidence is the final benefit of utilising the Python programming language.

The key benefit of utilizing this device is that it saves time and resources by cutting down on the amount of time spent on an investigation. This is due to the fact that each installed software generates substantial amounts of data that the lead researcher must carefully analyse. As a result, using this application eliminates the need to manually use many pieces of software to gather all the necessary data. The evidence must be handled with care since, if it is changed in any way, it will no longer be reliable for the investigation

VI. FUTURE WORK

The work described here provides a preliminary look at how digital evidence is handled in mobile devices running the Android OS; similar research could subsequently be done for mac OS and Windows Mobile. Increased interoperability is required for future work in order to collect data from third-party solutions and to suggest connectors and general strategies for extracting evidence. Additionally, it is crucial to assess and make future changes to certain of this tool's non-functional qualities (e.g., productivity, potential, serviceability).

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. S. Yadav, K. Ahmad, and J. Shekhar, “Analysis of Digital Forensic Tools and Investigation Process,” High Perform. Archit. Grid …, pp. 435–441, 2011.
4. 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.
5. 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.
6. Anglano, M. Canonico, and M. Guazzone, “Forensic analysis of Telegram Messenger on Android smartphones,” Digit. Investig., vol.23, pp.31–49, 2017.
7. T. Alyahya and F. Kausar, “Snapchat Analysis to Discover Digital Forensic Artifacts on Android Smartphone,” Procedia Comput. Sci., vol. 109, pp. 1035–1040, 2017.
8. P. Agus, “Prototyping SMS Forensic Tool Application Based on Digital Forensic Research Workshop 2001 (DFRWS) Investigation Model,” 2016.