VOL 2 (2018) NO 3 - 2

e-ISSN : 2549-9904
ISSN : 2549-9610

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

A Visualization Approach to Analyse Android Smartphone Data

Nurul Adhlina Hani Roslee [#], Nurul Hidayah bt Ab Rahman [#]

[#]*Information Security Interest Group, Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, Malaysia*

E-mail: adhlinahani@gmail.com, hidayahar@uthm.edu.my

***Abstract*—This study aims to design and develop an interactive system that can visualize evidence collected from Android smartphone data. This project is developing to support forensic investigator in investigating the security incidents particularly involving Android smartphone forensic data. The used of smartphone in crime was widely recognized. Several types of personnel information are stored in their smartphones. When the investigator analyses the image data of the smartphone, the investigator can know the behaviour of the smartphone's owner and his social relationship with other people. The analysis of smartphone forensic data is cover in mobile device forensic. Mobile device forensics is a branch of digital forensics relating to recovery of digital evidence from a mobile device under forensically sound condition. The digital investigation model used in this project is the model proposed by United States National Institute of Justice (NIJ) which consists four phases, which are collection phase, examination phase, analysis phase and presentation phase. This project related with analysis phase and presentation phase only. This paper introduces Visroid, a new tool that provides a suite of visualization for Android smartphone data.**

***Keywords*— Android, Digital forensic, Visualization, Interactive.**

I. INTRODUCTION

Smartphone is a cellular telephone with an advanced mobile operating system, which combine features of a personal computer operating system and typically having a touchscreen interface. The combination functionality and the storage space equipped in smartphone make smartphone become part of peoples' daily lives and often carried wherever a person goes, which can be used to determine a person's whereabouts at a particular time [1]. In cases that involve crimes predominately carried out using smartphone, especially Android, such as sexual predators, information from the smartphone alone can prove the suspect's guilt or innocence. Usually the predators will make the initial contact with the victims by contacting the victims using social media and keep exchange conversation and this will leave cyber trail that can be a big help during the investigation. Smartphone data can also plays an important role in solving crime unrelated to technologies, such as in the case of Ronald William, who was convicted of murdering his wife. The investigator found a voice mail in his wife's phone that record what happen actually at the crime scene. The voice mail captured Ronald William stating that he was going to kill his wife and the voice of his daughter pleading Ronald to stop [2]. Nowadays, there are many cyber forensic tools, in either software or hardware on the web to help the investigator in analysing digital evidence [3]. The purpose of the cyber forensic tools is to convert specific files into human readable language and format for analysis by the investigator. Usually the data involve will be large and the data viewed will be in large amount of textual-based. Digital forensic tools that have been enhanced with the interface visualization techniques can improve cognitive capacity investigators to discover criminal evidence more efficiently [4].

II. RELATED WORKS

This section discusses about the related study for digital forensic phases and visualization technique of evidence collected to support the forensic investigators.

A. Android Smartphone

Google's search chief Amit Singhal confirmed that now more Google searches happen on mobile than on desktop computers. According to a Google study quoted by Smart Insights, 48% of users start any research they make on a mobile device by using a search engine [5]. All the values showed that, nowadays, most people do any kind of transaction by using their smartphone device. The five primary functions of smartphones are calling and texting, gaming and entertainment, social media and internet browsing, time checks and camera shooting. Among all the smartphones operating system, the most popular is Android. Android dominated the smartphone market with a share of

87.6% by International Data Corporation in 2016. Google released the first Android OS by the name of 'Astro'. Google then adopted the trend of naming Android versions after any dessert or a sweet in alphabetical order.

B. Mobile Device Forensic

The United States National Institute of Justice (NIJ) document lists the four basic steps of digital forensic process. However, for this tool only involve analysis phase and reporting phase. The digital crime scene investigation includes four phases:

1) Collection phase: Collection phase: In this phase, process involve are evidence search, evidence recognition and evidence collection. All potential digital evidence will be identified and collected using procedures that preserve the integrity of the evidence. There are three-step process in evidence acquisition; developing a plan to acquire the evidence, acquiring the evidence, and verifying the integrity of the acquired evidence.

2) Examination phase: The next phase is to examine the evidence by assessing and extract the valuable data that related to the cases while preserving the integrity of the evidence. In this phase, the authority's personnel need to identify which data files that contain information of interest and exclude files or evidence that are of no interest to the examination.

3) Analysis phase: The results of the examination phase should be analyzed, using well-documented methods and techniques. The analyst should study and analyze the data or evidence and draw conclusion from it.

4) Reporting phase: This phase includes a detailed outline of the examination process and a complete listing of the data collected. Notes, including all documentation, must be preserved for discovery and subsequent testimony. The acquired and extracted evidence will be present in the court of law.

C. Visualization and Interactive

A smartphone is a useful evidence to find related criminals because smartphones store their contacts information but simply using smartphone data is difficult to grasp the relationship between the user and connected people. If an investigator can use the recorded data on the smartphone and look at the contact data as a number, they therefore, can grasp the relationship between the user and the contact, which will be a more efficient way of finding people of interest. For example, a high number means they are close to one another.

Visualization is important for understanding information; such as analytical data (for example; computing, medical and crime scene evidence) and for understanding analysis process such as network capability assessment, data file reconstruction and planning scenarios [6]. In digital forensic, there are challenges that arise in analysis phase, where the investigator needs to analyze a large amount of data, which will be viewed in textual-based interface [7], [11],[12].

Visualization explores the accuracies, inconsistencies and discrepancies of the collected data and information. Visualization also can spot the patterns and it will be useful in forensic investigations as it can increase efficiency, reduce errors and tedium and help non-technical people to understand investigator's conclusions [7]. Visualization is the process of representing information synoptically for the purpose of recognizing, communicating and interpreting pattern and structure. The representation may be displayed in symbolically, graphically and are most often differentiated from others form of expression such as textual, verbal or formulaic [8]. Main purpose of visualization is to allow user to get insight into data because by using visualization one can easily identify the anomaly in the data [9]. Interactive system meant that a system that allows dialogues between the system and the user.

D. Comparison with existing tools

Three systems are studied in terms of functionality, advantages and disadvantages of the system. Through this study, the additional requirements are identified in developing new systems. The chosen system is related to the field of study.

1) Twitter Forensic

Twitter forensic toolkit is a forensic tool where you can investigate on a criminal or a prime suspect's Twitter account hence you can get all the information. It focuses on four activities; identify suspect or illegal content by using powerful search engine.

Next is data mining that instantly parse thousands of tweets, retweets and quotes for specific terms or users and drill down from hundreds of results to highlight specific material of interest. The third function of twitter forensic toolkit is it will automatically download profile content, tweets, and uploaded media files and preserve content in secure evidential form and will generate the account timeline. The last function is the capability to produce clear expert reports and evidence packages. Twitter forensic toolkit works by extract information from prime suspect's Twitter account, which is then visualized.

2) Webscavator

Webscavator is a forensic tool that provides a suite of visualizations for web history data. Webscavator focuses on visualize the web history data in info graphic instead of table and textual data. Some visualizations give broad overviews of what the web history looks like - such as peak times of use and top domain names visited, whilst others give an in-depth look at the data itself such as a breakdown of all the local files accessed and search terms used in search engines. Webscavator also provide feature of an interactive timeline, which allows the investigator to zoom and pan around the web history data, highlighting and removing data using the customizable filters available.

3) Immersion

Immersion is a tool that collects only the metadata (From, To, Cc and Timestamp) of email. Immersion focuses on providing users with a number of different perspectives by leveraging on the fact that the web, and emails, are now an important part of our past.

Immersion provides an artistic representation that exists only in the presence of the visitor. Immersion also helps

explore privacy by showing users data that they have already shared with others.

TABLE 1
COMPARISON BETWEEN THE PROPOSED SYSTEM AND EXISTING SYSTEM

Details	Twitter forensic toolkit	Websca-vator	Immer-sion	Proposed system (Visroid)
Visualization of data	Yes	Yes	Yes	Yes
Interactive system	Yes	Yes	No	Yes
Type of visualization:				
-Timeline	Yes	Yes	Yes	Yes
-Heat map	No	Yes	No	No
-Bar chart	Yes	Yes	Yes	Yes
-Word cloud	No	Yes	No	Yes
-Pie chart	No	Yes	No	Yes
Generate report	No	Yes	No	Yes

Table 1 presents the comparison between the three related systems for producing useful comparative decision to develop the proposed system.

III. METHODOLOGY

The methodology used in this project is Object-Oriented Software Development Model. This model will be assist in the development of the system so that it is done gradually.

All the activities in developing this project is divided into particular phases. The activities and output of each phase are summarized as in Table 2. In the object-oriented analysis and design phases, the user of the proposed system is identified and the modules of the proposed system are design according to the requirement analysis. The proposed system is built in implementation phase based on the output from design phase and tested to ensure the proposed system can be run smoothly and the objective is achieved.

TABLE 2
SUMMARIZATION OF THE DEVELOPMENT OF PROPOSED SYSTEM

Phase	Activities	Output
Object-oriented analysis	-Study the background and features related to mobile forensic. -Perform background studies on existing analysis forensic tools.	-List in details the input, process and output specification.
Object-oriented design	-Design the interface, classes and the proposed tool's modules.	-Unified Modeling Language (UML) diagrams. -The user interface design, algorithm modules and tool.
Object-oriented implementation	-Built and develop user interface and classes.	-Data is presented using visualization technique.
Object-oriented testing	-Perform functional testing.	-Test report. -Complete system

IV. IMPLEMENTATION AND TESTING

In this section will be discusses in detail about the development and implementation of Interactive Forensic Analysis Tool for Android Smartphone Data (Visroid).

A. Implementation

The main function of Visroid is the visualization of Android smartphone data, which can help the investigator when they analyze the evidence. Figure 1 shows an example of module to visualize the selected worksheet using word cloud technique. User need to press ctrl c to copy the column or section that need to visualize and paste it in the textbox in the word cloud page.

Fig 1 Visualization page

B. Testing

Table 3 is a result of testing, which running to find any error in the system and to find any weakness in the system. Testing is the best way to ensure that the system fulfill the user requirement.

TABLE 3
RESULT OF SYSTEM TESTING

No	Testing	Expected outcome	Result
1	Button function	Functioning as expected	Successful
2	Connected and browse Excel file	Connecting as expected	Successful
3	Enter and save all details in text file	Save as expected	Successful
4	Excel data visualization	Visualize using word cloud technique	Successful

V. CONCLUSION

In conclusion, increasing usage of smartphones posed residual evidence of interest in the phone. All the data in smartphones are evidence and can help in the investigation. Thus, this project aims to support the forensic investigator when analyze then evidence collected. The proposed system needs to enhance and improve its functionality for future

work so the system can give more advantage to the user and can fight with other assessment system on the market.

ACKNOWLEDGMENT

The authors express appreciation to the FSKTM and Universiti Tun Hussein Onn Malaysia (UTHM). This research is supported by Gates IT Solution Sdn. Bhd. under its publication scheme. Thank you to anonymous reviewer for valuable comments.

REFERENCES

[1] J. E. R. McMillan, W. B. Glisson, and M. Bromby, "Investigating the increase in mobile phone evidence in criminal activities," *In Proc. of the Annual Hawaii International Conference on System Sciences*, 2013, pp. 4900– 4909.

[2] E. McMillan Casey and B. Turnbull, B, *Digital Evidence on Mobile Devices*. Digital Evidence and Computer Crime, 3.49 mb, pp. 1–44, 2011.

[3] McMillan Lowman, S., & Ferguson, I. (2010). Web History Visualization for Forensic Investigations, 668 kb(September), pp. 1–15.

[4] McMillan Altiero, R. A. (2015). Digital Forensics Tool Interface Visualization (Doctoral dissertation, Nova Southeastern University).

[5] (2015) Mobile Searches Surpass Desktop Searches At Google For The First Time. [Online]. Available: https://techcrunch.com/2015/10/08/mobile-searches-surpass-desktop-searches-at-google-for-the-first-time/

[6] D. Schofield, and K. Fowle, "Technology Corner Visualising Forensic Data: Evidence (Part 1). ," *Journal of Digital Forensics, Security and Law*, vol. 8(1), pp. 73–90, 2013. [Online]. Available: http://www.jdfsl.org/subscriptions/abstracts/JDFSL-V8N1-tech corner-Schofield.pdf

[7] Lowman, S., & Ferguson, I. (2010). Web History

[8] Visualization for Forensic Investigations, 668 kb(September), pp. 1–15.

[9] Tassone, C., Martini, B., Choo, K.K.R., (2017). Forensic Visualization: Survey and Future Research Directions. Contemporary Digital Forensic Investigations of Cloud and Mobile Applications. pp. 163–184.

[10] M. S.Chavhan, and M. S. Nirkhi, "Visualization Techniques for Digital forensics: A Survey," *International Journal of Advanced Computer Research*, vol. 2(4), pp. 74-78, 2012.

[11] S. Alqahtany, and N. Clarke, "A Forensically-Enabled IaaS Cloud Computing Architecture," *In Proc. of the 12th Australian Digital Forensics Conference*, 2014, p. 75–83.

[12] B. Inglot, and L. Liu, "Enhanced timeline analysis for digital forensic investigations," *Information Security Journal: A Global Perspective*, vol. *23*(1–2), pp. 32–44, 2014. [Online]. Available: https://doi.org/10.1080/19393555.2014.897401