# Analysis of Digital Forensics Method on the Smartphone

Sang Young Lee [#1]

[#] Department of Health Administration Namseoul University, South Korea
[1] sylee@nsu.ac.kr

***Abstract*— The increased use of social networking applications on smartphones makes these devices a goldmine for forensic investigators. Potential evidence can be held on these devices and recovered with the right tools and examination methods. This paper created a smartphone user analysis framework which can extract meaningful digital evidence for digital forensics by analyzing the user's usage of smartphone applications. Furthermore, with this method, we studied a system which can guide a digital forensic analyst to important information. In the future, structured data would be included aside from SQLite, and the system will be used to collect and analyze unstructured data online such as SNS data. In particular, it is expected to be a more efficient system in terms of digital forensic analysis if there are additional algorithms for big data analysis.**

**Keyword -** Digital, Evidence, Smartphone, SNS

## I. INTRODUCTION

The last several years have witnessed the rapid evolution of a new form of online communication known as social networking. By joining websites that offer these services, users can interact and socialize, share information and ideas, post comments and updates, participate in activities and events, upload files and photos, and engage in real-time instant messaging and conversations[1].

With the launch of various smartphones, the number of mobile users including smartphone users is dramatically increasing. This trend enables users to do web surfing, office, multimedia, call, MMS, social networking, etc. using smart devices equipped with Android or iOS instead of a computer with Windows program. As a result, the data stored on smart devices is considered as the most significant evidence in terms of digital forensics, and researches on smart devices are actively being pursued[2, 3].

However, the process wherein a digital forensic analyst manually analyzes each data and extracts useful information requires considerable time and effort. In addition, it is more difficult to look for meaningful information among a lot of information stored in smartphones in such a passive manner[4, 5]. Thus, we need to study how an analyst efficiently extracts meaningful information as digital evidence in a digital forensic point of view by analyzing the user's smartphone application usage.

In this paper, we have implemented a smartphone user analysis framework for digital forensic analysis of Android smartphone usage and studied digital forensic evidence extraction through it.

## II. ANDROID SMARTPHONE DIGITAL FORENSICS

This is a smartphone optimized for Google service by constructing OHA (Open Handset Alliance) as an open-type mobile phone platform based on the Linux operating system developed by Google [7, 8]. When a mobile device such as a mobile communication equipment is used in a crime, mobile forensics is applied as evidence of the crime [9, 10].

In digital forensics, collection of evidence is considered as an important part and securing the integrity of the evidence collected is important when it comes to dealing with the court such as in the selection of digital evidence. But one has to do a rooting operation for smartphones to collect digital evidence and do imaging work. Figure 1 shows the flow chart for the digital forensic analysis of the Android smartphone system[11].

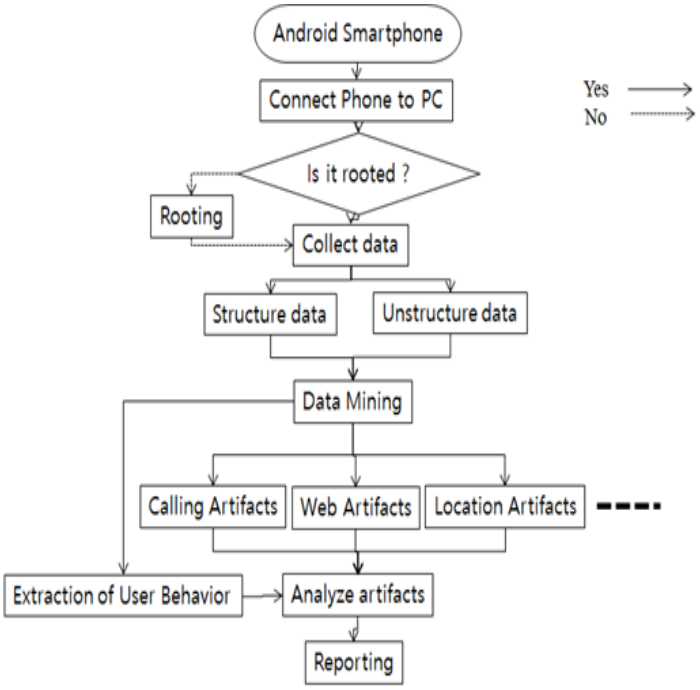


Fig.1 : Analysis procedure of android smartphone digital forensics

The Android smartphone system usually stores various data such as application usage, work data, and user's personal data. Data stored in an Android smartphone can be classified as data in SQLite database, key-value in Shared-Preferences as the XML data, and Local File data such as the myriad of log files and cookies [6]. These data are stored in the databases, files, and preferences folders of /Data/Data/ [Installed Package Name] folder

First, the Android smartphone uses SQLite small database engine to store data and it is generally stored under "/data/data/[Installed Package Name]/databases" with .db as the filename extension or nothing. Figure 2 shows SQLite data files in /data/data/ [Package Name]/databases folder of Android Smartphones.

XML data files in Preferences are constructed with a combination of Key and Values and stored under the "/data/data/ [Installed Package Name]/shared_pref" folder. Figure 2 illustrates the XML data files in /data/data/ [Package Name]/shared_pref of Android smartphones.

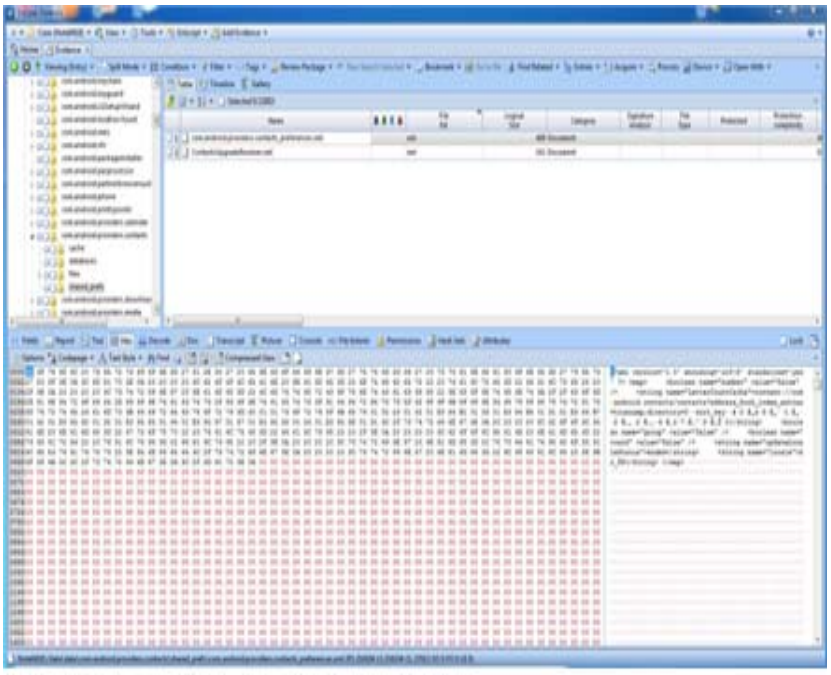

Fig. 2 : Android smartphone /data/data/ [Package Name]/ XML Data File of shared_pref folder

## III. SUB ANALYSIS SYSTEM

The SUB (Smartphone User Behavior) analysis system collects data stored under /data/data /[Package Name]/ folder based on the data type such as Unstructured data existing in the files and preference folders of /data/data folder, clipboard contents of the user storage file, files related to the network setting, and log files related to the Android system, or structure data of SQLite DB file-type stored in the database folder

These collected data will be used to formulate a system which can calculate various weight values such as values on deleted files, on repeated calls, on the reaction after the connection to important targets etc., and these will be delivered efficiently to the digital forensic analyst based on the level of importance. Figure 3 shows the SUB analysis system architecture.

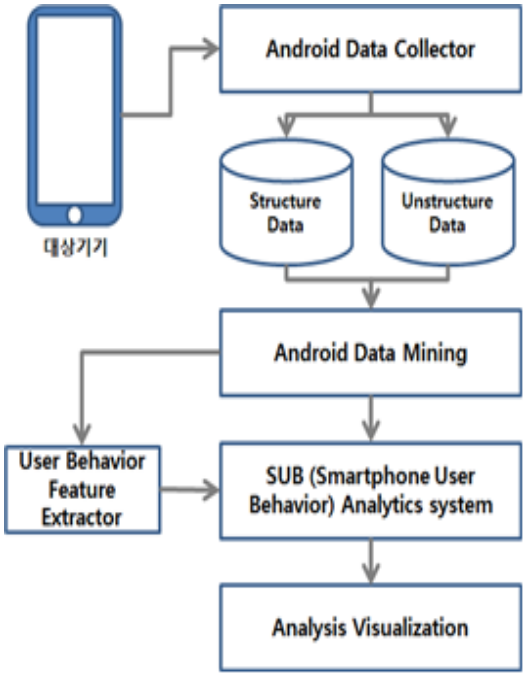


Fig.3.: SUB Analysis System Architecture

## IV. EXPERIMENT AND DISCUSSION

In this paper, we directly access necessary data by rooting and applying the Encase program to collect data from an Android smartphone. Figure 4 shows the image data extraction of LGGX2 Android smartphone using EnCase.

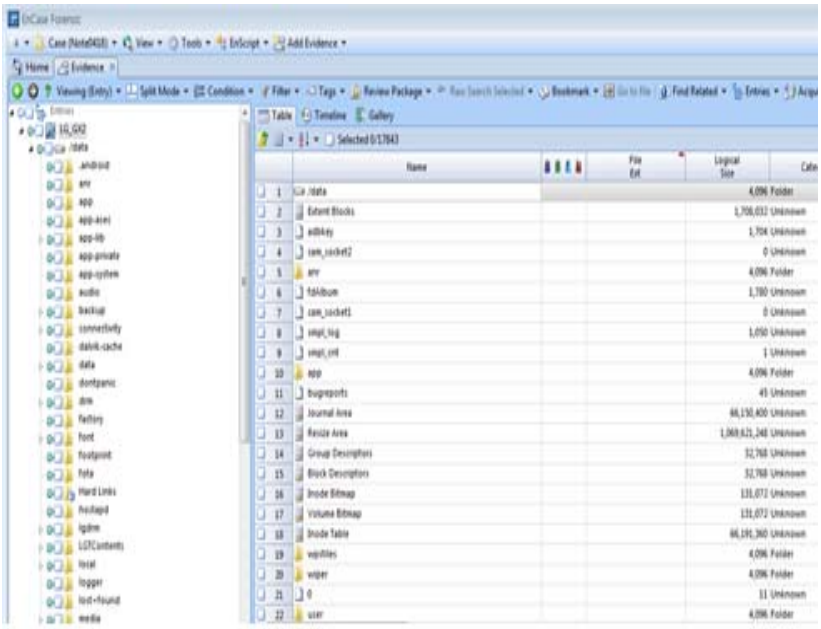

Fig. 4. Physical collection of LGGX2 Android Smartphone Data using EnCase

The storage path of the user's behavior data from the collected smartphone images for digital forensics analysis is as follows. Call related behavior of smartphone users is stored in "com.android.providers.contacts/databases/contacts2.db SQLite databases" and SMS/MMS related behavior is stored in "com.android.providers.telephony/databases/mmssms.db SQLite databases". Also, the contents of Internet WIFI connection related behavior is stored in /data/misc/wifi/WifiConnectionSuccessList and /data/misc/wifi/WifiConnectionFailList. Moreover, the data on Pictures and Videos related behavior using smartphones are stored in /sdcard/dcim/camera/.

There was a total of 919 user data collected from the LGGX2 Android smartphone in the experiment. Among these, only 822 meaningful data are separated and used for the analysis.

TABLE I: Statistical Analysis s

| Classification | | Week | Hour | Send/ Receive | Duration |
|---|---|---|---|---|---|
| N | Valid | 822 | 822 | 822 | 500 |
| N | Missing | 0 | 0 | 0 | 322 |
| Average | | | 13.83 | | 42.19 |
| Median | | | 14.00 | | .00 |
| Mode | | | 13 | | 0 |
| Standard Deviation | | | 5.042 | | 143.990 |
| Dispersion | | | 25.423 | | 20733.103 |
| Range | | | 23 | | 1824 |
| Minimum Value | | | 0 | | 0 |
| Maximum Value | | | 23 | | 1824 |
| Total | | | 11368 | | 21097 |

Targets for key digital evidence can be identified by analyzing the amount of calls and the number of calls of Android smartphone users. In addition, new targets can be added by analyzing the daily and hourly calls on the previous major target.

## V. CONCLUSION

With the development of IT technology, the use of mass storage devices and various digital devices has resulted in diversification and high capacity devices, and thus, conventional digital forensic analysis method shows limitations. Moreover, with the proliferation of smartphones, users can do web surfing, office, multimedia, call, MMS, social network, etc. by using smart devices equipped with Android or iOS. As a result, the data stored on smart devices is considered as the most significant evidence in digital forensics and researches on smart devices are also actively being pursued. This case becomes more important if one has to analyze various data which are spread everywhere. Among the tremendous amount of data, it is difficult for one to find meaningful information.

In this paper, we created a smartphone user analysis framework which can extract meaningful digital evidence for digital forensics by analyzing the user’s usage of smartphone applications. Furthermore, with this method, we studied a system which can guide a digital forensic analyst to important information. In the future, structured data would be included aside from SQLite, and the system will be used to collect and analyze unstructured data online such as SNS data. In particular, it is expected to be a more efficient system in terms of digital forensic analysis if there are additional algorithms for big data analysis

## ACKNOWLEDGMENT

Funding for this paper was provided by Namseoul university

## REFERENCES

[1] Al Mutawa N, Al Awadhi I, Baggili I, Marrington A,. Forensic artifacts of Facebook’s instant messaging service. In: Proceedings of the 2011 International Conference for Internet Technology and Secured Transactions (ICITST); pp. 771–6, 2011.
[2] Abu Dhabi, UAE. Al Zarouni M., Mobile handset forensic evidence: a challenge for law enforcement. In: Proceedings of the 4th Australian Digital Forensics Conference; 2006. Perth, Australia, 2006.
[3] Sam Brothers, How Cell Phone Forensics Tools Work, AAFS 2012, Washington, DC, 2012.
[4] Bader M, Baggili I., iPhone 3GS forensics: logical analysis using apple itunes backup utility. Small Scale Digital Device Forensics Journal,Vol. 4(1), 2010.
[5] Burnette MW. Forensic examination of a RIM (BlackBerry) wireless device. 2012.

[6] de Paula AMG. Security aspects and future trends of social networks. In: Proceedings of the Fourth International Conference of Forensic Computer Science; pp. 66–77, 2009.
[7] Kubasiak R, Morrissey S, Varsalone J., Macintosh OS X, iPod, and iPhone forensic analysis DVD toolkit. Burlington, MA: Syngress; 2009.
[8] Lessard J, Kessler GC., Android forensics: simplifying cell phone examinations. Small Scale Digital Device Forensics Journal, Vol. 4(1). 2010.
[9] Vidas T, Zhang C, Maloof M., Toward a general collection methodology for Android devices. In: Proceedings of the Eleventh Annual DFRWS Conference, Vol. 8, 2011.
[10] Liu, H., Darabi, H., Banerjee, P., Liu, J., Survey of Wireless Indoor Positioning Techniques and Systems, IEEE Transactions on Systems, Man, and Cybernetics – Part C: Applications and Reviews, Vol. 37, No. 6, 2007.
[11] Digital Forensics Research Workshop, A Road Map for Digital Forensics Research, 2001.

## AUTHOR PROFILE

Sang-Young Lee Professor, Dept. of Health Administration, Namseoul University, South Korea.