ISSN 2409-2665
Journal of Logistics, Informatics and Service Science
Vol. 9 (2022) No.1, pp.68-84
DOI:10.33168/LISS.2022.0106

Mobile Digital Forensics Framework to Increase Security Level of for Smartphone User

Sang Young Lee

Namseoul University, South Korea

sylee@nsu.ac.kr

Abstract. Blockchain-based digital forensics technology is an efficient way to prevent forgery/modulation of evidence including collecting and analyzing evidential data using the technology in compliance with smartphone forensics procedures after a smartphone is seized. Moreover, the use of large-capacity storage devices and various digital devices have become a realistic solution for its development of IT in situations where the existing digital forensics analysis methods are regarded as limitations. This paper analyzed user's status on smartphone application and implemented a smartphone user analysis framework that may extract significant digital evidence in a digital forensic way based on a blockchain perspective. In this paper researched a system that may provide important information to digital forensic analysts through these frameworks. It is expected that the proposed system will be expanded by much more structured data and online unstructured data such as SNS reports.

Keywords: Blockchain, digital forensics, mobile

1. Introduction

As high-level computing technology and digital storage devices are advancing rapidly, digital crimes using large amounts of information in the form of digital data are increasing accordingly. Digital evidence has a very significant meaning in solving cybercrimes (Zhang, X. O., et al., 2020) (Srivastava, P., et al., 2015).

Digital forensics technology that investigates digital evidence in most of all forensic fields for instance, analysis on cybercrime, violent crimes, fraud, defamation, accounting fraud, tax evasion, and leakage of trade secrets, was attracted as a cutting-edge technology. This brings legal effect through the process of collecting evidence, recovery of evidence (evidential data acquisition) and analyzing evidence. To effectively analyze digital data for digital forensics, ICT-based analysis for instance, storage media, file system, data processing, and networking is required.

An nvestigation technique that may provide preventive measures is required which uses Malicious Code in order to respond to intelligent cybercriminals by identifying the cause of the accident and proceeding with prompt recovery. The advent of convenient smartphones enabled the number of users to increase rapidly. Due to the rapid spread of smartphones, users are receiving services for instance, phone call, MMS, and social network functions for web surfing, office work, multimedia, while others on personal computers with Windows or smart devices based on Android or iOS (Mac Dermott, et al., 2018) (Li, S., et al., 2019).

Moreover, it is difficult to find significant information among a lot of information stored in the smart phone passively. Therefore, smartphone applications can analyze users' usage patterns and efficiently extract digital evidence in important crimes through digital forensics. Since most of the data is stored in mobile devices that is related to daily life, the need of mobile forensics in digital forensic investigations is being highlighted significantly.

Although the advent of smartphones, various operating systems and products for mobile devices, Android and iOS are used the most worldwide. Mobile forensics is conducted through a digital forensic for smartphones, tablet PCs, wearable devices, and others, and many research have been conducted since the late 2000s when smartphones have rapidly increased worldwide.

The smartphone market in the initial times was dominated by Apple’s iOS and BlackBerry, however as Google’s Android have emerged that is based on open source, Android and iOS have been leading after Samsung, LG, Motorola, and HTC have developed smartphone based on Android. Google and Apple have further advanced their operating systems and released not only smartphones but also various mobile devices, as a result, various mobile devices for instance smartphones and tablet PCs have made modern life convenient and become data storage media in which data most closely related to modern people’s life.

Accordingly, data stored in smart devices is recognized as very important evidential data, and research on smart devices is also being actively conducted from a digital forensic point of view. However, if a digital forensic analyst wants to manually analyze the meaning of each data and extract useful information, it requires considerable time and effort.

With the development of IT and the rapid diffusion of smart phones, the use of large-capacity storage devices and various digital devices have resulted to analysis target as they caused large-capacity and diversification, which show the limitations of the existing digital forensic analysis methods. When users use various functions such as web surfing, phone calls, MMS, and social network functions with smart devices, they are required to further develop technologies. Accordingly, research on digital forensics technologies that may solve this problem is being actively conducted, as data stored in smart devices has been recognized as very important evidence. However, It is difficult to find significant information among a lot of information, and it is more difficult to apply when the user's digital evidence is distributed in several places (Zhang, X., et al., 2019) (Philomin, S., et al., 2020).

Therefore, this study implemented a smartphone user analysis framework that may extract digital forensically significant digital evidence by analyzing users' status on smartphone application that is encrypted on the basis of blockchain. This study also conducted specific research which digital forensic technology may be effectively used by analyzing the implemented system.

2. Mobile digital forensics

Previous studies related to the field of mobile is focused on data acquisition and restoration. In particular, restoration technology and general forensic analysis of smart devices have been researched in terms of criminal investigation. A lot of research has been conducted based on software-centered data that may acquire hardware-oriented data and restore corrupted data. Moreover, there are various foreign and domestic standard documents that are related to mobile forensic procedures (Oriwoh, E., et al., 2013) (Kebande, V. R., et al., 2016) (Ngobeni, S., et al., 2010).

The mobile forensic procedure is basically expanded to the procedure established in computer forensics, and as new mobile devices are continuously released, responds to this matter are continuously proposed and established. A representative foreign standard document related to mobile forensics procedures is the "Guidelines on Mobile Device Forensics" SP 800-101 Revision 1 of NIST, United States. This document was first published in 2006 and last revised in May 2014 to be suitable for the features of new mobile devices (Cebe, M., et al., 2018) (Ikuesan, A. R., et al., 2017).

In this document, the mobile forensic execution procedure is divided into four stages: Preservation, Acquisition, Examination and Analysis, and Reporting.

1. The stage of preservation is about how to respond when a mobile device is found in the field, for instance, respond to blocking radio waves and networks.
2. The Acquisition stage is about how to identify and secure the device through model name of the mobile device, and others, and how to collect inside data with the mobile forensic tool.
3. The stage of examination and analysis stage is about listing the types of data to be analyzed that are collected in mobile device data and analyzing data using a mobile forensic analysis tool.
4. The stage of reporting is about drawing up of a written report on the overall performance of mobile forensics.

ISO/IEC 27043, "Information technology – Security techniques – Incident investigation principles and process" also covers procedures related to mobile forensics. Based on this procedure, Emilio Raymond Mumba confirmed the effectiveness of the procedure through real case studies. The name of the procedure is "Harmonized Digital Forensic Investigation Process", which is divided into five stages: Readiness processes, Initialization processes, Acquisitive processes, Investigative processes, and Concurrent processes (Sang, Y. L., 2021) (Manal, I. M., 2021).

- The stage of readiness processes is about corresponding to advance preparation in general digital forensics.

It includes constructing scenarios for accidents that may occur and implementing effective digital forensics at minimal cost and time through procedures for responding to them, and preparing tool and system, etc.

- The stage of initialization processes is the initial response to an incident, investigation planning, and preparation.

- The stage of acquisitive processes is about identifying and securing devices that are collected on site, and performing data collection, transportation, and storage.

- The stage of investigative processes is about researching and analyzing the collected digital data and finalizing the investigation.

- Investigative processes are conducted in all four stages at the same time, which are the stages to maintain evidential capacity of digital evidence by having investigation authority, documenting, conducting investigation procedure management, and maintaining chain of custody.

In addition to this, there are procedures proposed by Cynthia A. Murphy and Archit Goel. The stages of the procedure proposed by the standard documents and studies vary according to the degree of subdivision, however the core contents are

similar. In general, mobile forensics secure necessary information through portable devices such as mobile phones, PDAs, laptops, digital diary, digital cameras, and USB memory cards for analysis.

Mobile forensic techniques may be classified into three types according to the method of extracting stored data (Abdelkarim, B. C., et al., 2021) (Naga M. R. et al., 2019).

Smartphone forensics collect data saved on various services, such as contact information, photos, videos, phone records, Internet, SNS, and financial transactions, and submits documenting information to the court that may be used as evidence. Smartphone forensics is based on the mobile forensic procedure, and some procedures must be performed for evidential data based on some smartphone procedures.

Basic smartphone forensics procedures may be classified into advance preparation, evidence collection, evidence analysis, and preparation of result report. Advance preparation step for smartphone forensics is about various matters for collecting and analyzing smartphone data smoothly. It may be classified as advance preparation for data necessary for initial evidence collection and analysis, evidence collection in advance, evidence analysis on the collected evidence, and writing a result report according to the analysis procedure. Preparations for forensic investigations may include various results depending on the composition of forensic experts, administrative procedures for investigation, environment of subject of target and the scope of the cases, proportion of events, training experience of a forensic member, and planning for investigation (Sang Y. L., 2020).

- Composition of forensic experts

A smartphone forensic expert must know the file system of the smartphone operating system, the directory structure and form of important data, and others. The forensic team should be composed of experts who can to use smartphone forensic tools and have expertise in the field of mobile forensics.

- Administrative procedures for investigation

Prior to smartphone forensics, administrative documents and procedures necessary for investigation should be made to proceed in compliance with laws and regulations

- Selection of subject of analysis and scope

The subject of analysis and scope should be selected to collect evidential data of smartphone rapidly and correctly on a crime scene.

- Planning of evidential data collection

Planning of evidential data collection should be performed considering that the method of collecting evidence differs depending on the type of smartphone. In other words, when planning evidential data, each investigator should take each different

role for planning evidential data according to their skills and abilities. What should be considered is whether the smartphone's operating system and built-in memory are included or not, and check whether smartphone supports evidence collection such as system time information, user account information, process information, network information, and document information for collecting evidential data. Therefore, it is important to check the components included in the smartphone forensic tool to avoid errors when collecting evidential data.

- Planning of analyzing evidential data

Planning for analysis of evidential data should be established. To avoid modulation with the original image during the analysis, the analysis should be conducted using a copy and the priority of the file format should be selected that may contain evidential data in relation to an incident. In addition, if data is found to be forged or modified, anti-forensics should be conducted through data recovery that suits for the file system.

A typical procedure of Android smartphone digital forensic analysis is as follows. Google had developed an open mobile phone platform based on the Linux operating system. It is a smartphone platform optimized for Google services including the concept of Open Handset Alliance (OHA).

Furthermore, mobile forensics should be applied as evidential data of the crime when a mobile device is involved in a crime for instance, as s mobile communication device. Evidential collection is important for digital forensics, and securing the integrity of important evidence collected is significant for the courts in terms of selecting digital evidential data. However, Android smartphones collect digital evidence after rooting in order to do imaging. The flowchart for digital forensics analysis of Android smartphone systems is shown in Figure 1.

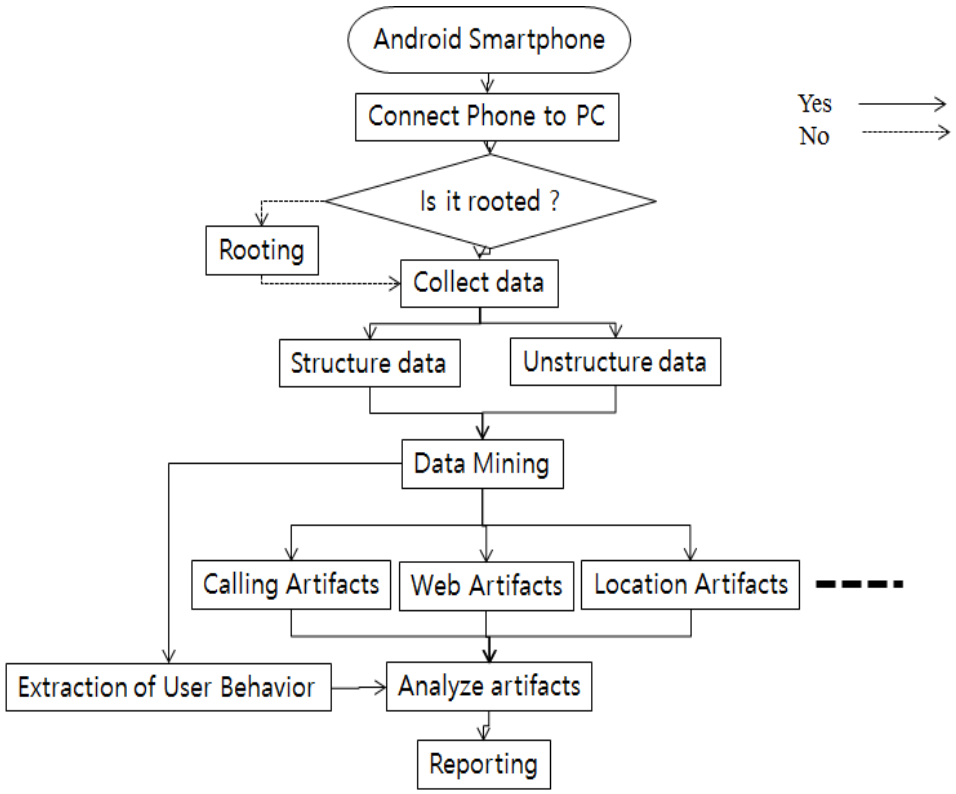

Fig. 1: Android smartphone digital forensic analysis procedure

Android smartphone systems save a lot of data, for instance, personal user data and application use and work data. The data stored in the Android smartphone includes Data stored in the SQLite database, which is a database, Key-value data stored in Shared-Preferences, which is XML data, and Local file such as various logs or cookies. Most of these data are stored in the folder of databases, files, and preferences with the name of /Data/Data/ [installation package name].

First SQLite compact database engine is often used to store data on an Android smartphone and saved in the folder with the name of " /data/data/ [Installed Package Name]/databases" and as a form of .db or a form without an extension.

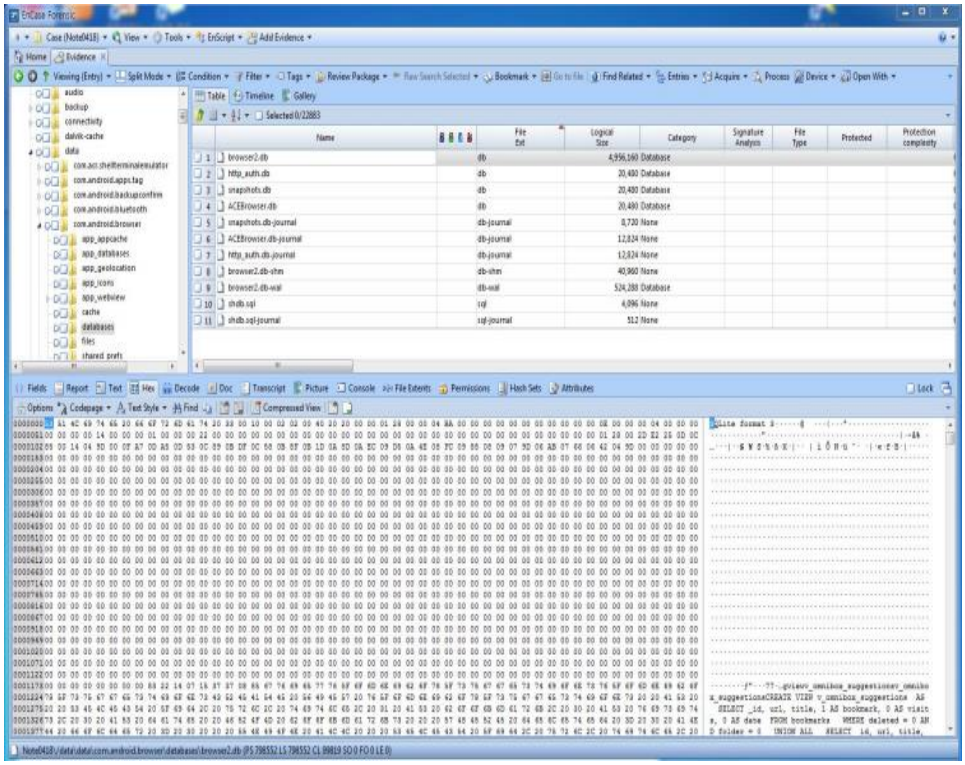

Fig. 2 : SQLite data file in the android databases folder

Figure 2 shows SQLite data file saved in the folder of an Android smartphone.

Preferences, which is XML data file, have a structure that stores data as a combination of Key and Value, and often saved in the folder named "Android databases Folder"

Figure 3 shows the XML data file in the Android smartphone /data/data/ [package name]/shared_pref folder. Local file is a method that stores a string or an image in an arbitrary format, and all data storage methods are included except for preference that is, database format of SQLite and XML format. In general, it is saved in the folder of Cache and Files named "/data/data/ [package name]/."

3. Blockchain-based analysis system

In general, blockchain technology is one of the types that is distributed database, which is a ledger technology that records changes on addition, modification, or deletion related to specific information in block units and sharing and managing them. A general ledger means a list of ordinary transactions, but if interpreted as shared information, blockchain technology can be applied to all data.

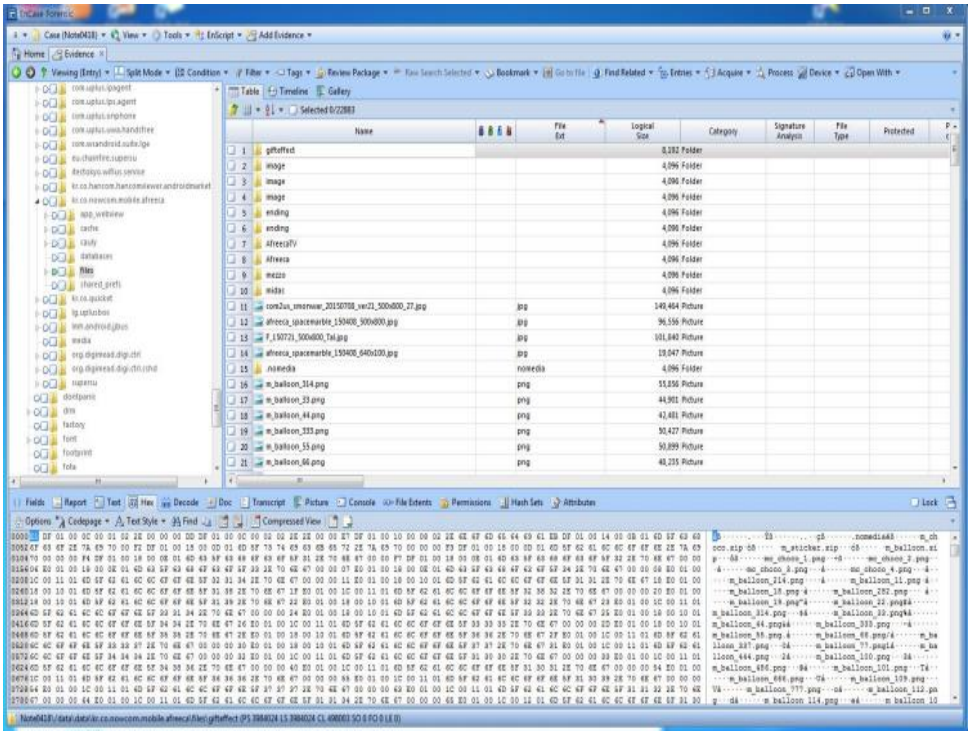

Figure 3. Local File in Cache and Files Folder of Android Smartphone /data/data/ [package name]/

The blockchain-based SUB (Smartphone User Behavior) analysis system collects structured data of the SQLite DB file type existing in the databases folder according to the data type that is saved in the folder of "/data/data/ [installation package name]/" and unstructured data existing in preference folder of Android system-related log files, network setting related files, storage files of user's clipboard contents, and /data/data folder.

The data collected in this way implements a system that may give weights for deleted contents, repeated calls, next action after connecting to important subjects and others, which efficiently presents high-importance content to digital forensic analysts by applying them to time or connection subjects. Figure 4 shows the architecture of blockchain-based analytics system.

The actions of Android smartphones that may be significantly interpreted to digital forensics may be defined as follows.

- Calls-related actions: voice calls, video calls, recent calls list, etc.
- SMS/MMS-related actions: sending and receiving messages, message list
- E-mail-related actions: sending and receiving e-mails, deleting e-mails, etc.
- Internet browser-related actions: visiting websites, search word, URLs, etc.
- Map-related actions: map location search, list of favorites, etc.
- Camera-related actions: taking pictures and videos
- File-related actions: file download, file execution, etc.
- Micro SD card related actions: Inserting and removing Micro SD card
- Network access related actions: WIFI access, GPS access, etc.

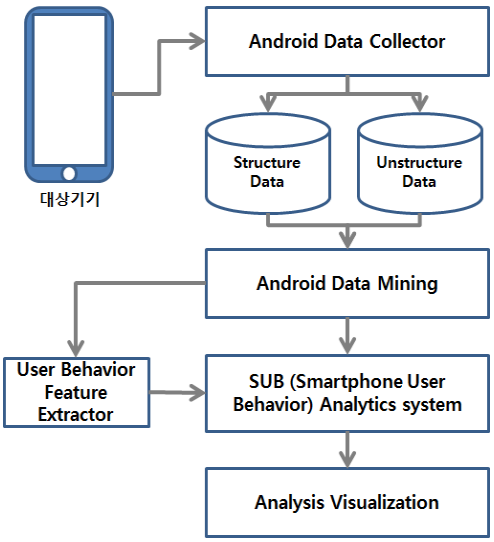

Fig. 4: Architecture of blockchain-based analytics system

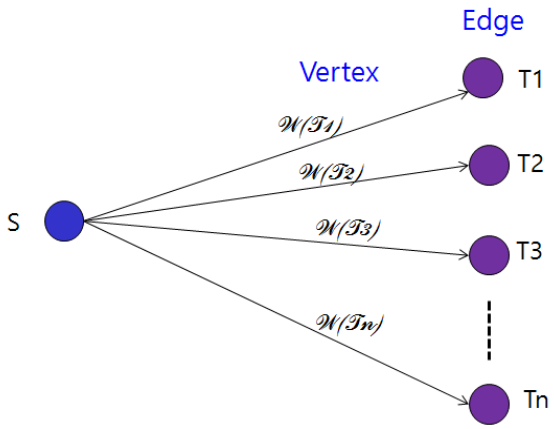

Fig. 5: Weights for action targets of SUB analysis system

4. Experiments and considerations

The analysis information about Android smartphones used in the experiment and the devices on the analysis are shown in Table 1.

Table 1: Android smartphone analysis environment and target

Kind	Name	Version
DEVICE	LGGX2	4.4.2
SOFTWARE	EnCase Forensics Tool	7
	Mobile Phone Examiner plus	5.5
	R	3.2.0
	Python	2.7.10

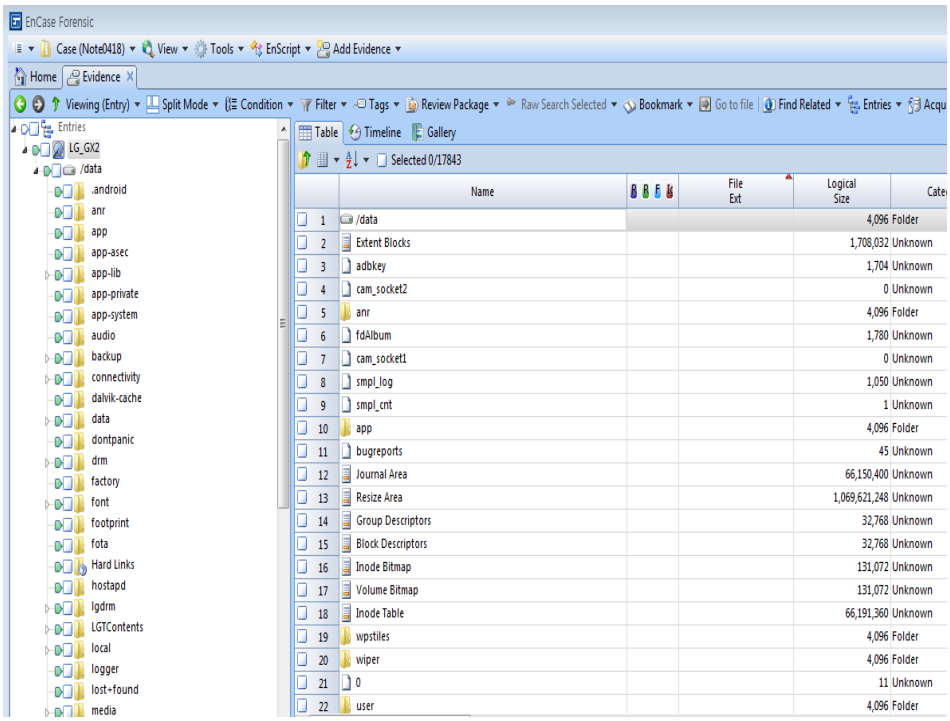

Fig. 6: Android smartphone data physical collection using EnCase

This study collected the data through direct access and rooting in order to collect Android smartphone using a digital forensic tool, EnCase.

Table 2: Android smartphone user behavior data storage path

Behavior Type	Data Storage Path
Phone Call	databases/contacts2.db
SMS/MMS Behavior	databases/mmssms.db
SNS Activity	databases/KakaoTalk.db
Internet browser	databases/browser.db
	databases/webview.db
Download	databases/downloads.db
Google Maps	databases/search_history.db
WIFI Access	/data/misc/wifi/WifiConnectionSuccessList /data/misc/wifi/WifiConnectionFailList
Photo/Video	/sdcard/dcim/camera/

Figure 5 shows a screen for extracting information from LGGX2 Android smartphone images collected by EnCase.

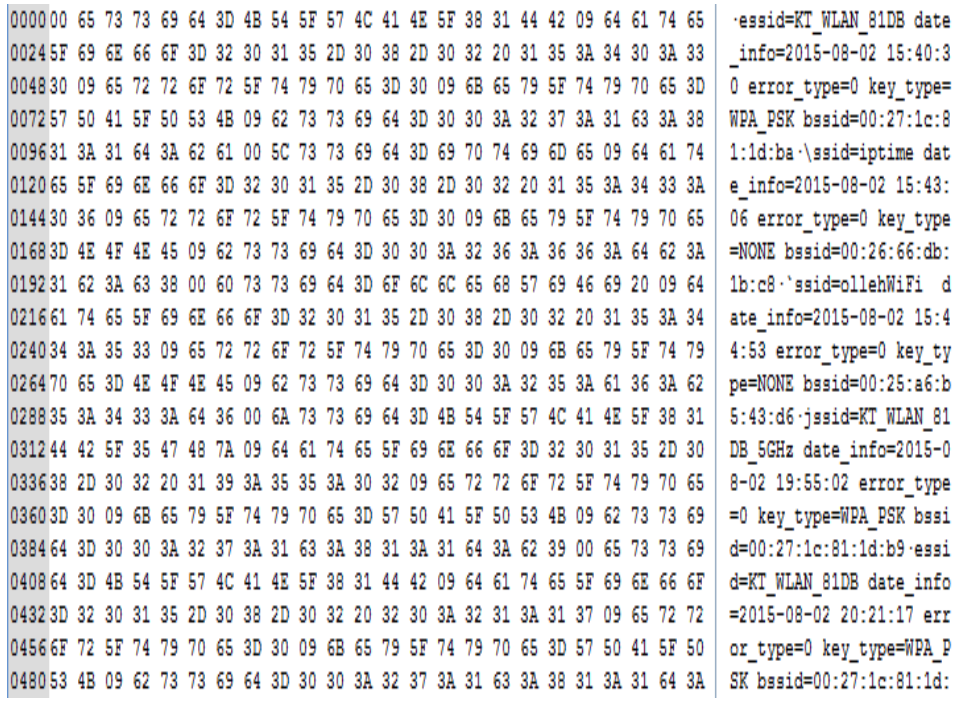

Fig. 7: Wi-Fi network connection data

The data storage path for analyzing user behavior patterns based on the collected smartphone images is as follows. Call behaviors of smartphone users are stored in the com.android.providers.contacts database. SMS/MMS actions are stored in the com.android.providers.telephony database. Also, Internet Wifi connection behavior is stored in /data/misc/wifi/WifiConnectionSuccessList and /data/misc/wifi/WifiConnectionFailList.

Photos and videos taken using a smartphone are stored in /sdcard/dcim/camera/.And Android smartphones support Wi-Fi connection for data communication. When a user connects to a specific wifi, SSID information and MAC address information of the connected Wi-Fi AP are stored.

In the experiment, 919 data related to users of LGGX2 Android smartphone were collected. Among them, 822 of valid data were used for analysis.

Table 3: Analysis results

Time	Action Type	Action	Information
2020-05-22 16:08:49	SMS/MMS	receive text message	phone book registrant
2020-05-22 16:09:00	SMS/MMS	receive text message	Kakao Talk Verification Number
2020-05-22 19:13:01	SMS/MMS	receive text message	bank information letter
2020-05-23 17:02:31	Download	file download	google file download
2020-05-25 13:43:22	SMS/MMS	receive text message	missed call
2020-05-25 14:55:55	SMS/MMS	receive text message	missed call
2020-05-25 19:55:07	SMS/MMS	receive text message	missed call
2020-05-26 06:57:10	Download	file download	google file download
2020-05-26 11:09:00	WIFI access	connection failure	wifi connection
2020-05-27 11:06:56	SMS/MMS	receive text message	University Notice
2020-05-27 20:57:00	WIFI access	connection failure	wifi connection
2020-05-27 21:46:33	SMS/MMS	receive text message	University Notice
2020-05-28 09:44:55	SMS/MMS	receive text message	University Notice
2020-05-29 09:17:25	SMS/MMS	receive text message	missed call
2020-05-29 12:06:30	SMS/MMS	receive text message	University Notice

2020-05-29 22:03:00	WIFI access	connection failure	wifi connection
2020-05-29 22:03:32	WIFI access	connection failure	wifi connection
2020-05-30 07:54:00	SMS/MMS	receive text message	phone book registrant
2020-05-30 07:54:11	SMS/MMS	send text message	phone book registrant
2020-05-30 07:54:46	SMS/MMS	receive text message	phone book registrant
2020-05-30 07:55:00	SMS/MMS	send text message	phone book registrant
2020-05-30 07:56:02	SMS/MMS	receive text message	phone book registrant
2020-05-30 08:00:37	SMS/MMS	send text message	phone book registrant
2020-05-31 20:24:31	SMS/MMS	receive text message	missed call
2020-05-31 23:59:31	SMS/MMS	receive text message	missed call
2020-06-02 12:14:22	WIFI access	connection failure	wifi connection
2020-06-02 19:00:03	SMS/MMS	receive text message	phone book registrant
2020-06-02 19:00:57	SMS/MMS	send text message	phone book registrant
2020-06-02 19:15:26	SMS/MMS	receive text message	phone book registrant
2020-06-02 19:42:26	SMS/MMS	receive text message	missed call

Table 4: Analysis statistics

Division		Week	Hour	Send/Receive	Duration
N	Available	833	833	833	550
	Missing	1	0	0	312
Average			13.53		43.19
Median			14.10		.
Mode			12		0
Standard Deviation			5.142		142.990
Variance			26.423		20735.103
Range			25		1824
Minimum			0		0

Maximum		24		1724
Sum		11344		21197

It discovers major subjects for digital evidence through an analysis on the number of calls and call volumes of Android smartphone users by each user and subject.

In addition, a new analysis target may be discovered by the analysis on the details of calls by day and hour. Figure 8 shows the data analysis for the subjects of the calls and text messages.

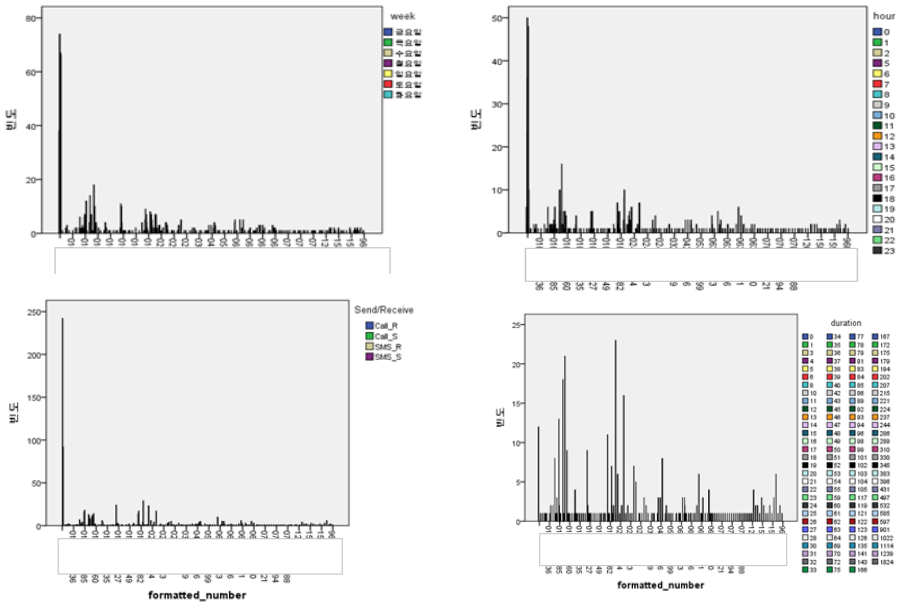

Fig. 8: Data analysis for call and text users

5. Conclusion

Blockchain-based digital forensics technology is an efficient way to prevent forgery or modulation of evidence including collecting and analyzing evidential data using the technology in compliance with smartphone forensics procedures after a smartphone is seized.

Moreover, the use of large-capacity storage devices and various digital devices have become a realistic solution for its development of IT in situations where the existing digital forensics analysis methods are regarded as limitations.

This paper analyzed user's status on smartphone application and implemented a smartphone user analysis framework that may extract significant digital evidence in a digital forensic way based on a blockchain perspective. In conclusion, this study

researched a system that may provide important information to digital forensic analysts through the proposed frameworks. It is expected that this system will be expanded by more structured data and online unstructured data such as SNS data.

Acknowlwdgements

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government (2021R1F1A1052848)

References

Xiaolu Zhang, Oren Upton, Nicole Lang Beebe, Kim-Kwang Raymond Choo, (2020). Iot botnet forensics: a comprehensive digital forensic case study on mirai botnet servers. *Forensic Science International: Digital Investigation*, 32(Supplement), 300926.

Srivastava, P. & Garg, N. (2015). Secure and optimized data storage for iot through cloud framework. *International Conference on Computing, Communication Automation, IEEE*, 720-723.

Mac Dermott, A., Baker, T., & Shi, Q. (2018). Iot forensics: challenges for the ioa era. *2018 9th IFIP International Conference on New Technologies Mobility and Security (NTMS), IEEE*, 1-5.

Li, S., Choo, K. R., Sun, Q., Buchanan, W. J., & Cao J. (2019). Iot forensics: amazon echo as a use case. *IEEE Internet of Things Journal*, 6(4), 6487-6497.

Zhang, X., Choo, K. R., Beebe, N. L. (2019). How do I share my iot forensic experience with the broader community?. An automated knowledge sharing iot forensic platform. *IEEE Internet of Things Journal*, 6(4), 6850-6861.

Philomin, S., Singh, A., Ikuesan, A. & Venter, H. (2020). Digital forensic readiness framework for smart homes. *International Conference on Cyber Warfare and Security*, Academic Conferences International Limited. 627.

Oriwoh, E. & Sant, P. (2013). The forensics edge management system: a concept and design. *2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing, IEEE*, 544-550.

Kebande, V. R. & Ray, I. (2016). A generic digital forensic investigation framework for internet of things (iot). *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), IEEE*, 356-362.

Ngobeni, S., Venter, H. & Burke, I. (2010). A forensic readiness model for wireless networks. *IFIP International Conference on Digital Forensics*, 107-117.

Cebe, M., Erdin, E., Akkaya, K., Aksu, H. & Uluagac, S. (2018). Block4forensic: An integratedghtweight blockchain framework for forensics applications of connected vehicles. *IEEE Commun. Mag.*, 56(10), 50-57.

Ikuesan, A. R. & Venter, H. S. (2017). Digital forensic readiness framework based on behavioralbiometrics for user attribution. *2017 IEEE Conference on Application, Information and Network Security (AINS), IEEE,* 54-59.

Sang, Y. L. (2021). Blockchain-based Medical Information Sharing Service Architecture. *International Journal of IT-based Public Health Management*, 8(1), 27-32..

Manal, I. M. (2021). The Efficacy of Distance Electronic Learning in Developing Achievement Motivation for Children within the Coronavirus Pandemic. *International Journal of Future Generation Communication and Networking,* 14(2), 77-92.

Abdelkarim, B. C., Mohamed, F. & Mohamed C. (2021). Comparative Performance Evaluation of Intrusion Detection System: Suricata and Snort. *International Journal of Security and Its Applications,* 15(2), 23-32.

Naga M. R. & Neeraja, S. (2019). A Survey On Map Reduce Framework For Clustering Security. *International Journal of Private Cloud Computing Environment and Management*, 6(1), 9-16.

Sang Y. L. (2020). Cloud based Blockchain Technology for Personal Health. *International Journal of Advanced Nursing Education and Research*, 5(3), 14-20.