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, 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.

										- 0
+ + 🛄 Case (Note0418) + 🍕 Yiew + 🗇 Tools	• 附 Er	Script + 🔠 Adul Evidence +								
Home & Evidence  K										
0 1 Viewing (Entry) + III Split Mode + ()	Conditio	n 🛪 🐨 Filter 🐐 🗇 Tags 🕈 🍙 Review Package 🔹 🖛 flaw	Switch Selected + 2	Bookmark + 📵 Gom	Find Related	+ (5 Entrin + 13	Acquire + 🟦 Pro	cess @ Devic	e + 🔊 Open With	<b>8</b> 1
o audio	HIT Ta	Ne 🕂 Timeline 📱 Gallery								
b OC . backup		La Alla Contration (1982)								
O	1	1 + 11 + [] seatter 0/17003	The second second	14 A	TRANSFE		- forestere	- 10-		Balance
O dalvik-cache	100	Hame	8388	Ext	Spe	Category	Analyza	Type	Protected	complicitly
• 00 1 data	31	] browser24b	db		4,956,160	Database				
DU a conscionente analar	32	) http://utit.do	db		20,490	Defabere				
COL Internet and the second se	31	] snapshotudo	db		20,490	Dafabase				
COL COR and political and political	04	ACEBrowser.db	40		20,490 1	Database				
a non andtoid.browtet	35	) unapshots.db-journal	db	journal	0,720	Nane				
DOT NOP appearte	0.6	ACEBrowser.db-journal	db	journal	12,824	Sane				
app_databases	31	) titta suth dis journal	db	journal	12,824	None				
pi app_geolocation		] browser2.db-shm	db	shn	40,960 1	Nane				
Di App_kons	100	brawser2.db.wai	db	anial later	524,288	Database				
Di app,webwiew	3 10	) mm sai	10		4,095 (	liane				
pi k cache	711	) shitb sol-tournal	10	lournal	51.7	Nane				
Di databases	-1.41		1.1.1	e						
A CONTRACT OF A										
Fields Report Text Ed Her W De	cede 🕑	Doc 📑 Tamacrigt 📲 Picture 🗔 Console >2+File Edit	ents 🏐 Permission	i 🔄 Hash Sets 🕑 Att	billutes					() lack
Tields Report Test Billers Bolt Options "A Codepage + A Test Style + H School Biller + Style + H	code (1)	Doc Transcript Picture Console son File bat	onto 🟐 Permission os o4 all co co c	i JHach Sets J At	trillutes ao ao ait ao ao a	a de ab ao ao 1	Lite format 3		1 1.5 4 <b>4</b>	Jud
Pidds         Report         Test         Ef Hee         M De           Opbion         A Codapage         A Test 30/4 = 43         A De         A De         De           Opbion         A L 42 do 74 66 30 66 67 70 20         DO 00 00 10 00 10 00 00 00 00 00 00 00 00	code (1) Find (-) 41 74 2 00 22 0	Doc         Transcript         Protuce         Console         Not File Date           Image: Compressed View           Image: Compressed View         Image: Compressed View         Image: Compressed View         Image: Compressed View         Image: Compressed View           Image: Compressed View         Image: Compressed View         Image: Compressed View         Image: Compressed View         Image: Compressed View           Image: Compressed View         Image: Compressed	ont:	i <b>∐ Hack Sets                                   </b>	00 00 08 00 00 0 00 00 01 20 00 2	0 04 00 00 00 D 22 25 0D 0C	glate format 3		n - 115 (	Lack
Print         Iteration         Test         If Here         Image           Options         ************************************	code () Find () 41 74 2 00 22 0 83 00 8	Doc         Tenscoipt         Picture         Console         set F4+ 54           0         Compressed View         0<	ent:      Permission     A    AA     00     00     0     00     00     00     0     00     00     00     0     00     00     00     0     00     00     00     0	■ Hach Sets 2 At 0 00 00 00 00 00 00 00 00 0 00 00 00 00 00 00 00 00 0 00 07 50 06 AB 07 0 00 07 50 06 AB 07	00 00 08 00 00 0 00 00 01 10 00 2 66 06 42 04 00 0	0 04 00 00 00 0 D 22 25 0D 00 0 00 00 00 00 0	glate format 3	4	(* 8 m.a. * i •e:	Lock   -44 r 8
Interest perfit         Interest perfit           Fields         Integet         Thet         If Meyes         If Meyes           Options         * A Codapage         - A Test Style         + M           Stations         * A Codapage         - A Test Style         + M           Stations         * A Codapage         - A Test Style         + M           Stations         * A Codapage         - A Test Style         + M           Stations         * A Codapage         - A Test Style         + M           Stations         * A Codapage         - A Test Style         + M           Stations         * A Codapage         - A Test Style         + M           Stations         * A Test Style         - A Test Style         + M           Stations         * A Test Style         * A Test Style         + M           Stations         * A Test Style         * A Test Style         + M           Stations         * A Test Style         * A Test Style         * A Test Style           Stations         * A Test Style         * A Test Style         * A Test Style           Stations         * A Test Style         * A Test Style         * A Test Style           Stations         * A Test Style         * A Test Style <t< td=""><td>Code 4</td><td></td><td>Image: State State         Image: State State State         Image: State State State         Image: State State         Image: State State         Image: State         I</td><td>Image         Image         <th< td=""><td>00 00 08 00 00 0 00 00 01 20 00 2 66 00 42 04 90 0 00 00 00 00 00 0</td><td>8 04 00 00 00 D 22 28 00 00 0 00 00 00 00 0 00 00 00 00 0 00 0</td><td>glate format 3 </td><td></td><td>(* 6 m.a. == (</td><td>lock 1 - 44 1 2 1</td></th<></td></t<>	Code 4		Image: State State         Image: State State State         Image: State State State         Image: State State         Image: State State         Image: State         I	Image         Image <th< td=""><td>00 00 08 00 00 0 00 00 01 20 00 2 66 00 42 04 90 0 00 00 00 00 00 0</td><td>8 04 00 00 00 D 22 28 00 00 0 00 00 00 00 0 00 00 00 00 0 00 0</td><td>glate format 3 </td><td></td><td>(* 6 m.a. == (</td><td>lock 1 - 44 1 2 1</td></th<>	00 00 08 00 00 0 00 00 01 20 00 2 66 00 42 04 90 0 00 00 00 00 00 0	8 04 00 00 00 D 22 28 00 00 0 00 00 00 00 0 00 00 00 00 0 00 0	glate format 3 		(* 6 m.a. == (	lock 1 - 44 1 2 1
Fields         Parson         The test graph           Options         * A Codapase         * A Test Style         * and           Sectors         * A Codapase         * A Test Style         * b 30000           Sectors         * A Codapase         * A Test Style         * b 30000           Sectors         * A Codapase         * A Test Style         * b 30000           Sectors         * A Codapase         * A Test Style         * b 30000           Sectors         * A Stole         * b 10000         * b 10000           Sectors         * B 10000         * B 10000         * b 10000           Sectors         * B 10000         * B 10000         * B 10000           Sectors         * B 100000         * B 100000         * B 100000           Sectors         * B 100000         * B 100000         * B 100000           Sectors         * B 1000000         * B 1000000         * B 1000000           Sectors         * B 100000000000000000000000000000000000	Code () Find () 41 74 3 00 22 0 53 00 8 00 00 0 00 00 0	Dox         Transcript         Proture         Console         Set Fielder           Image: Set	Image: The second sec	Hach Sets         An           0         00 <t< td=""><td>00 00 08 00 04 0 00 00 01 20 00 2 66 00 42 04 00 0 00 00 00 00 00 0 00 00 00 00 00 0 00 00</td><td>8 04 00 00 00 D II 2 25 0D 00 0 05 00 00 00 0 05 00 00 00 0 05 00 00 00 0 00 00 00 00 0 00 00 00 00</td><td>glite format s</td><td>4</td><td>(* 8 п.ч. – (.е.</td><td>- 1 - 44  1</td></t<>	00 00 08 00 04 0 00 00 01 20 00 2 66 00 42 04 00 0 00 00 00 00 00 0 00 00 00 00 00 0 00 00	8 04 00 00 00 D II 2 25 0D 00 0 05 00 00 00 0 05 00 00 00 0 05 00 00 00 0 00 00 00 00 0 00 00 00 00	glite format s	4	(* 8 п.ч. – (.е.	- 1 - 44 1
Test         Iteration         Test         Iteration           Codesyst         A test bit         Iteration         Iteration         Iteration           Codesyst         A test bit         Iteration         Iteration         Iteration         Iteration           Distor         A test bit         Iteration         Iteration         Iteration         Iteration         Iteration           Distor         A test bit         Iteration	code () Find () 41 74 1 00 22 0 53 00 0 53 00 0 00 00 0 00 00 0	Doc         Transcript         Pricure         Console         >>>         >>>           0	Image         Image <th< td=""><td>Image         Image         <th< td=""><td>Distributes         Distributes           00         Dist         Distributes           00         Distributes         Distributes</td><td>0         04         05         00         0           0         2         24         00         00           0         0         00         00         0           0         0         00         00         0           0         00         00         00         0           0         00         00         00         0           0         00         00         00         00           0         00         00         00         00</td><td>glite format 5</td><td></td><td>(* δπα* (</td><td>  Lock  44   3  </td></th<></td></th<>	Image         Image <th< td=""><td>Distributes         Distributes           00         Dist         Distributes           00         Distributes         Distributes</td><td>0         04         05         00         0           0         2         24         00         00           0         0         00         00         0           0         0         00         00         0           0         00         00         00         0           0         00         00         00         0           0         00         00         00         00           0         00         00         00         00</td><td>glite format 5</td><td></td><td>(* δπα* (</td><td>  Lock  44   3  </td></th<>	Distributes         Distributes           00         Dist         Distributes           00         Distributes         Distributes	0         04         05         00         0           0         2         24         00         00           0         0         00         00         0           0         0         00         00         0           0         00         00         00         0           0         00         00         00         0           0         00         00         00         00           0         00         00         00         00	glite format 5		(* δπα* (	Lock  44   3
Fields         Text (s) off.           Fields         Text (s) off.           Option         *)         Codages - A           Text (s) of a state	Find () 41 74 2 00 22 0 53 00 8 00 00 0 00 00 0 00 00 0 00 00 0 00 00 0 00 00 0 00 00 0		Image: Control (Control (Contro)(Control (Control (Control (Contro) (Contro) (Contro) (Contro) (C	Image         Image <th< td=""><td>Difficultes         00         00         00         00         00         0</td><td>04         00         00         00           12         24         00         00           00         00         00         00         00           0         00         00         00         00         00           0         00         00         00         00         00         00           0         00</td><td>glite format s</td><td></td><td>(</td><td>- 1 - 44 r 3 - 1</td></th<>	Difficultes         00         00         00         00         00         0	04         00         00         00           12         24         00         00           00         00         00         00         00           0         00         00         00         00         00           0         00         00         00         00         00         00           0         00	glite format s		(	- 1 - 44 r 3 - 1
Interest port         Test Solution         Test Sol	Code #		Image: Control (Control (Contro)(Control (Control (Control (Contro) (Contro) (Contro) (Contro) (C		Dilutes         00 <t< td=""><td>0         0         0         0         0         0           22         25         0</td><td>glite format s</td><td>4 (2)(</td><td>(* δπα *</td><td>- Leck  48  1</td></t<>	0         0         0         0         0         0           22         25         0	glite format s	4 (2)(	(* δπα *	- Leck 48 1
Test         Iteration         Test         Mark         Mark <t< td=""><td>code () Find () 41 74 3 00 22 0 03 00 0 00 00 0</td><td></td><td>Image: Sector (1)         Image: Sector (1)</td><td></td><td>Diffuides         00</td><td>0         44         00         00         00           0         22         24         00         00           0         0         00         00         00           0         05         00         00         00           0         05         00         00         00           0         05         00         00         00           0         00         00         00         00           0         00         00         00         00           0         00         00         00         00           0         00         00         00         00           0         00         00         00         00           0         00         00         00         00           0         00         00         00         00           0         00         00         00         00           0         00         00         00         00           0         00         00         00         00           0         00         00         00         00           00         <t< td=""><td>jiite domat S</td><td>4 (2)(*) (1</td><td>ζ</td><td><b>1</b> teck (3 - 1</td></t<></td></t<>	code () Find () 41 74 3 00 22 0 03 00 0 00 00 0		Image: Sector (1)		Diffuides         00	0         44         00         00         00           0         22         24         00         00           0         0         00         00         00           0         05         00         00         00           0         05         00         00         00           0         05         00         00         00           0         00         00         00         00           0         00         00         00         00           0         00         00         00         00           0         00         00         00         00           0         00         00         00         00           0         00         00         00         00           0         00         00         00         00           0         00         00         00         00           0         00         00         00         00           0         00         00         00         00           0         00         00         00         00           00 <t< td=""><td>jiite domat S</td><td>4 (2)(*) (1</td><td>ζ</td><td><b>1</b> teck (3 - 1</td></t<>	jiite domat S	4 (2)(*) (1	ζ	<b>1</b> teck (3 - 1
April 1         Heaved port           Column 7         Columns 7           Column	Code 4 Find 4 00 22 0 00 00 0 00 00 0 00 00 0 00 00 0 00 00	Dot         Tensorie         Fright         Concole         Nor Fields           0         Conported View         0 <td>Implicity         Implicity         Permission           01         04         8A         00</td> <td></td> <td></td> <td>0         04         00         00         00           10         12         24         00         00           0         05         00</td> <td>ginte dormat 3</td> <td></td> <td>ζ</td> <td>_ Lock : 3 - 14</td>	Implicity         Implicity         Permission           01         04         8A         00			0         04         00         00         00           10         12         24         00         00           0         05         00	ginte dormat 3		ζ	_ Lock : 3 - 14
Test         Test <th< td=""><td>Code 4 Find 4 41 74 3 00 22 0 00 00 00 0 00 00 00 0 00 00 00 00 00 00000000</td><td></td><td>Implicity         Implicity         Implicity           01         04         84.         00</td><td>Image         Hands         Sets         Image           0</td><td></td><td>04         05         05         05           0         04         05         05         05           0         05         05         05         05         05           0         05</td><td>glite format 5</td><td>4</td><td>(</td><td>_ Lock </td></th<>	Code 4 Find 4 41 74 3 00 22 0 00 00 00 0 00 00 00 0 00 00 00 00 00 00000000		Implicity         Implicity         Implicity           01         04         84.         00	Image         Hands         Sets         Image           0		04         05         05         05           0         04         05         05         05           0         05         05         05         05         05           0         05	glite format 5	4	(	_ Lock 
Heards Sorti         Test	Code 4 Find 4 41 74 3 00 22 0 53 00 0 00 00 00 0 00 00 00 0 00 00 00 00 00 0 00 00 00 00 00 00000000		Image: Control         Image:	Hann Sets 3 4 4 0 00 00 00 00 00 00 00 00 0 00 00 00 00 00 00 0 00 00 00 00 00 0 00 00 00 00 00 0 0 00 0 0 00 00 0 0 00 0 0 00 00 0 0 00		0         44         00         00         00           0         24         00 <td>(iite formet 5</td> <td></td> <td>(</td> <td>_ Lock</td>	(iite formet 5		(	_ Lock
Tests         Test Set         Test Set Set         Set Set Set Set Set Set Set Set Set Set	Coole     C		Image: Control of the second	Image: Set:         Material Set:         Material Set:         Material Set:         Material Set:           0	Diffuse         Diffuse <thdiffuse< th=""> <thdiffuse< th=""> <thd< td=""><td>4         44         0.0</td><td>jiite donmat 5</td><td></td><td>(* 8ma** (**</td><td>_ Lock</td></thd<></thdiffuse<></thdiffuse<>	4         44         0.0	jiite donmat 5		(* 8ma** (**	_ Lock
Test:         Iteration         Test:         Test: <td>Code     Code     Code</td> <td></td> <td>Image: Second Second</td> <td>I Heath State:         J Im           0         00</td> <td>billiones         00         00         00         00         01         00         01</td> <td></td> <td>gitte formet s</td> <td></td> <td>( 8 m 1 (</td> <td>Lock ( ) - 44 ( ) - 14</td>	Code		Image: Second	I Heath State:         J Im           0         00	billiones         00         00         00         00         01         00         01		gitte formet s		( 8 m 1 (	Lock ( ) - 44 ( ) - 14
Tests         Test soft         Test soft <thtest soft<="" th=""> <thtest soft<="" th=""> <thtest< td=""><td>4         1         2           Find         2         3         0           83         02         3         0           90         10         0         0           00         0         0         0           00         0         0         0           00         0         0         0           00         0         0         0           00         0         0         0           00         0         0         0           00         0         0         0           00         0         0         0           00         0         0         0           00         0         0         0           00         0         0         0           00         0         0         0           00         0         0         0           00         0         0         0           00         0         0         0</td><td>Dot         Insurant         Fiture         Console         Ne Fite bit           0         <t< td=""><td></td><td>I black 5etc         J all           0         00         01</td><td></td><td></td><td>(j.i.e. formet ) </td><td></td><td>(*. 8na * . (*e</td><td>- Lock</td></t<></td></thtest<></thtest></thtest>	4         1         2           Find         2         3         0           83         02         3         0           90         10         0         0           00         0         0         0           00         0         0         0           00         0         0         0           00         0         0         0           00         0         0         0           00         0         0         0           00         0         0         0           00         0         0         0           00         0         0         0           00         0         0         0           00         0         0         0           00         0         0         0           00         0         0         0           00         0         0         0           00         0         0         0	Dot         Insurant         Fiture         Console         Ne Fite bit           0 <t< td=""><td></td><td>I black 5etc         J all           0         00         01</td><td></td><td></td><td>(j.i.e. formet ) </td><td></td><td>(*. 8na * . (*e</td><td>- Lock</td></t<>		I black 5etc         J all           0         00         01			(j.i.e. formet ) 		(*. 8na * . (*e	- Lock
Tests         Iterato         Test Set         Set Set	41         41         42         42         42         43         42         42         43         42         42         43         42         43         42         43         42         43         42         43         43         43         43         43         43         43         43         44<			Hack Sets         All           0         01         <			jitte formet s		(	- Lock
	Code					$\begin{array}{cccccccccccccccccccccccccccccccccccc$	Lite formt 5	4	(* 8mg	- Lock 
	Code						Lite Sount 5 · · · · · · · · · · · · · · · · · · ·		(*	teck
	Find 42 4 4 2 2 4 4 5 4 4 5 4 4 5 4 4 5 4 4 5 4 4 5 4 4 5 4 4 5 4 5						Eite form: 1 	.goleou mas	(*	i -45 r S i
	Find 42 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4						Litte format 5 <b>S V</b> 0 to <b>S V</b> 0 to sequention Elizer 1.4. to all sets		( Š II u (-e Š II u (-e Š II u (-e Š II u (-e Š II u (-e S II u (-e S II u (-e S II u (-e S II u (-e	Lack

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.

E Incare formic										<u> </u>	60	a x
a + 👔 Case (NoteDESE) + 🖏 View + 🌖 Tools + 🕂 Erd	cript = 2	Add Evidence *										ų -
Home Stidence ×												
O O ? Vening Brind * D Salt Made * D2 Condition		ter * - Tant * 👶 Enview Package * 🌞 East Levent Selects	et v sa find	mark + Jel Gabatte I d		Related + St.	Entries =	Al Acaster +	A Process Sil De	nice + 22.0	an With Y	
to C I E ma untre longert	The second second	Contractory Product	0.04000		1944	come e 🖷		and an of the		1000		
- DI I con uplui pri agent	1000	e D mene it carey										
> O(1 + Unit ustul anotony	17 11	* 21 *										*
o Colline concustor una hand they		Name		776	<b>n</b> -	Logical		Category	Signature	10	Protected	P =
in office research and a control of		1000		(M		924		outlid	Analysii	1/04		30
- DO - exclustive supersu	1.1	getteffett				41	BI Folder					
- Of a dectacyoundful service	1 2	mage				4,0	195 Folde					
b DC kr. co. hancom hancomi ever androidmarket	0.3	anage				4,0	96 folder					
A CVT I A ICO ADDIVISION MODIAL ADDIVISIO	14	a mage				4.0	196 Polder					
1. To 1 is and within w	0.5	ending				4.0	96 Folder					
a collected	114	anders				40	the Falder					
100 000		Record					-					
NO + DODARS		A CONTRACTOR OF A CONTRACTOR OFTA CONTRACTOR O					29 - 010 C					
I IN THE REAL	11 8	Afreca				4.0	596 7 GIG#					
POLI A Mar	9	a mezzo				4.0	196 Polder					
-Di marcipica	10	idat ist				4,0	196 Folde	ŧ				
		a com2us_smore.www_20150708_ver21_500x800_27.jpg		(c) g		143,4	64 Picture					
- DI - atransia	12	afreeca spacemarble 150408 500x800.jpg		80		96.5	55 Picture	*				
1-DOTE automotion	0.18	3 # 150721 500x600 Tal.ing		log .		101.0	43 Picture					
OUT NADY	11.14	states and the lease and the				10.0						
DOT to oblace gigritu	1 14	aussos ibscenauss rankos okorno (bš		P9		19,0	er eldun					
1-DCT R out whose a doctor taxe	1 15	a naneda		nomedia		4,0	99 FUIDE					
> OC I menun	15	a m_balloon_114.png		pog		55,5	55 Picture					
C doctbaus	17	🚔 m_ballson_33.prig		png		44,9	III Picture	e				
FOC an	1 18	🚄 m,bailoon,44.png		png		42,4	ILL Picture					
OC I fattory	19	a balloon 333 pmp		png		50.4	27 Picture					
> OC test	0.11	a balaco Si eso		002		51.0	AA Richard					
-CC featured		a balan Mara										
OC tota	21	a statistication bod		bug		42,4	33 PICOAN					-
4 H 4	4.1	and the second sec	_									- A
1) Fields - Report - Text - 12 Have - Decode - 1	Doc (F)	Transcript P. Parture	tinine off	tash fata 10 Attributes								ert 🔁
Li une Cluber Clue Olue II serve Cl		training in cause of cause so the states in the	The second se	ann ann A suiteann								··· 🖵
Codepage * A Text Style * 94 Find	3 4 .	Compressed View						1140				1.
1690 IF 01 00 0C 00 01 02 2E 00 00 00 DE DE 01	00 00 1	0 02 02 2E 2E 01 00 E7 DF 01 00 10 00 00 02 2E 41	E 47 6D 66 1	4 69 61 EB DF OL OS	14.4	DO OR OI ED B	7 63 60	Bristy	- 24	çå	nedia43 n	ch r
1052 6F 63 6F 2E 7A 65 70 10 FZ DF 01 00 15 00 00	01 CD -	7 73 74 63 63 65 65 72 25 74 65 70 60 00 00 23 05	01 00 18 0	0 00 01 00 57 62 61	10.1	10 AF AF AE 2	2 7A 63	cco.gip ca	m_sticks	z.zip cò	m_balloon	-81
BISGOG RO OI OD 10 OD OR OI 6D 63 SF 63 68 6F 63	47 57 1	19 3E 70 6E 67 00 00 07 E0 01 80 18 00 0E 01 6D 60	1 SF 63 68 1	7 62 67 67 34 35 70	a 1	67 00 00 de B	0 01 00	4	choco à.png		shose 4.png	
320810 00 11 01 4D 5F 43 41 40 40 4F 48 5F 53	01 04 1	E 70 6E 67 00 00 00 11 E0 01 00 10 00 10 01 60 53	F 62 61 60 0	C 67 67 68 57 51 51	22.1	10 KE 67 10 E	0 01 00	m m ball	son_214.png	4	alloon_li.pag	£
NEWEIS OF 10 OF SE SF SE ST SC SF SF SF SF SF SF	35 25	0 6E 67 1F E0 01 00 10 00 11 01 6D 8F 62 61 60 60	tr tr tr tr	8 32 38 32 25 70 65	47.5	1 05 00 00 00	0 01 00	m_ball	ocu_19 bud a	" "_ballo	on_282.pnp	422 - L
They ch sh at th	62 65	0 88 87 22 80 01 08 18 00 10 01 80 87 82 81 80 80		7 10 00 07 70 67 61	00.0	CO 01 00 10 0	0 10 01	m halloon	lis ror is	halle	an 10 years	
1416 CD 57 62 61 6C 6C 6F 6F 6E 57 54 54 2E 70 6E	47 26 1	10 01 00 10 00 11 01 6D 5F 62 61 60 60 6F 6F 6E 53	F 03 33 35 1	E 70 6E 67 00 00 00	10 1	to di do 18 D	0 10 01	n balloon	44.pngiá	m_balloon_3	10.png	
2448.60 87 82 81 80 80 87 87 88 88 38 38 28 70 81	47 28 1	to 01 D0 18 D0 10 01 4D 8F 42 41 4C 4C 4F 4F 4E 55	7 36 36 2K	0 68 67 27 80 01 00	10 0	NR 11 01 60 8	F 62 61	m_balloon_	35.prg é	n_ballom_6	8.prg/4n	be.
BE28 SC 4C 4F 4F 4E 5F 18 18 17 12 TO 4E 4T 00 01	00 30 1	10 01 00 18 00 10 01 4D SP 63 61 4C 4C 4F 6F 6E 68	8 37 37 28 1	D 62 67 21 20 01 00	10.0	00 11 01 4D E	7 62 61	11ann_227.	prg bi	n halloon 7	7.pagiá m	ha
1002 00 00 00 00 00 00 00 04 04 00 00 00 00	48 47 1		. av av av i	# 10 4# 97 00 00 00	67.0	10 01 00 10 0	0 01 01	m halloun	and rear that	n parioon 1	an 101 mm	11
DETRIC OF 11 O1 4D SF 62 41 4C 8C 6F 4F 6E SF 35	36.36	E TO ME 47 00 00 00 88 ED 01 00 10 00 11 01 60 80	F 82 41 40 1	C 6F 6F 6E 6F 31 33	39 2	28 70 48 47 D	0 00 00	······································	000 668.prg	74 n. b	alleon 109.prg	2.0-0
072064 20 01 00 10 00 11 01 4D 57 42 41 40 40 47	67 62 1	8 19 19 17 17 12 73 4E 67 00 00 00 63 E0 01 00 1C 00	1 11 01 éD i	7 62 61 60 60 67 67	62.5	F 31 31 32 1	E 70 4E	W	halloon 717.po	q	w halloon 112	.pa
2785 67 00 00 00 64 20 01 00 10 00 11 01 6D 5F 62	61 60	IC 67 67 62 57 61 51 54 22 75 62 67 55 50 65 55	01 00 10 1	0 15 01 60 57 62 61	40.4	10 CT ST SE 5	5 31 30	gir då i i i	m balloon 11	4.pog ek	m balloon	10 *
NoteD4181/data/data/ikr.co.mowcom.mobile.afreecal.files/gift	affect (PS	1959024 LS 3959024 CL 496063 SO 6 PC 9 LE 0)										

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.

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

Table 1: Android smartphone analysis environment and target

EnCase Forensic						
📕 💌 🚹 Case (Note0418) 💌 🖏 View 💌 🍈 Tools 💌 🏤 En	Script 🔻 😤 A	dd Evidence 🔻				
A Home Reference						
C A Viewing (Entra) = Shit Made = (= Condition	n v 🐨 Filter	- Jan	Selected <b>* O Bookmark *</b>	Go to file 🗿 Find P	alatad w 🖧 Entrier	
Spin wode + (c= conduct		Orage to Book	i Selected + St bookinaik +		ciated • Ha citates	s . Ω∋ ×cdα
LG GX2	a lable	Timeline E Gallery				
/data	1 🖉 🖉 🗸	2↓ ▼ 🔲 Selected 0/17843				
		Name	8858	File	Logical	Cate
_ <b>⊳_</b> ] anr		💷 /data		EAL	4.096	Folder
- <b>D</b>		Extent Blocks			1,708,032	Unknown
- app-asec		adbkey			1 704	Unknown
p p lib		a cam socket2			-,	Unknown
app-private		anr			4 096	Folder
audio	E 6	fdAlbum			1.780	Unknown
backup		cam socket1			-,	Unknown
connectivity		smpl log			1.050	Unknown
- alvik-cache	9	smpl cnt			1	Unknown
⊳- <b>⊳_</b> ] ]} data	10				4.096	Folder
-p] lontpanic	11	buareports			45	Unknown
⊳ <b></b> drm	12	lournal Area			66 1 50 400	Unknown
actory	13	Resize Area			1 069 621 248	Unknown
footnint	14	Group Descriptors			32 768	Unknown
fota	15	Block Descriptors			32,768	Unknown
Hard Links	16	Inode Bitmap			131.072	Unknown
hostapd	17	Volume Bitmap			131.072	Unknown
⊳_∎_] Igdrm	18	Inode Table			66 191 360	Unknown
▶- <b>▶</b> □]] LGTContents	19	wnstiles			4 096	Folder
⊳- <b>⊳</b> _]]} local	20	wiper			4,096	Folder
- D logger	20	0			11	Unknown
lost+tound	22	user			4 096	Folder

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.

Behavior Type	Data Storage Path			
Phone Call	databases/contacts2.db			
SMS/MMS Behavior	databases/mmssms.db			
SNS Activity	databases/KakaoTalk.db			
Internet	databases/browser.db			
browser	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/			

Table 2: Android smartphone user behavior data storage path

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

000000 65 73 73 69 64 3D 4B 54 5F 57 4C 41 4E 5F 38 31 44 42 09 64 61 74 65 ·essid=KT WLAN 81DB date 00245F 69 6E 66 6F 3D 32 30 31 35 2D 30 38 2D 30 32 20 31 35 3A 34 30 3A 33 info=2015-08-02 15:40:3 004830 09 65 72 72 6F 72 5F 74 79 70 65 3D 30 09 6B 65 79 5F 74 79 70 65 3D 0 error\_type=0 key\_type= 0072 57 50 41 5F 50 53 4B 09 62 73 73 69 64 3D 30 30 3A 32 37 3A 31 63 3A 38 WPA PSK bssid=00:27:1c:8 009631 3A 31 64 3A 62 61 00 5C 73 73 69 64 3D 69 70 74 69 6D 65 09 64 61 74 | 1:1d:ba·\ssid=iptime dat 0120 65 5F 69 6E 66 6F 3D 32 30 31 35 2D 30 38 2D 30 32 20 31 35 3A 34 33 3A e info=2015-08-02 15:43: 014430 36 09 65 72 72 6F 72 5F 74 79 70 65 3D 30 09 6B 65 79 5F 74 79 70 65 06 error type=0 key type 0168 3D 4E 4F 4E 45 09 62 73 73 69 64 3D 30 30 3A 32 36 3A 36 36 3A 64 62 3A =NONE bssid=00:26:66:db: 019231 62 3A 63 38 00 60 73 73 69 64 3D 6F 6C 6C 65 68 57 69 46 69 20 09 64 1b:c8.`ssid=ollehWiFi d 021661 74 65 5F 69 6E 66 6F 3D 32 30 31 35 2D 30 38 2D 30 32 20 31 35 3A 34 | ate info=2015-08-02 15:4 024034 3A 35 33 09 65 72 72 6F 72 5F 74 79 70 65 3D 30 09 6B 65 79 5F 74 79 4:53 error type=0 key ty 026470 65 3D 4E 4F 4E 45 09 62 73 73 69 64 3D 30 30 3A 32 35 3A 61 36 3A 62 pe=NONE bssid=00:25:a6:b 028835 3A 34 33 3A 64 36 00 6A 73 73 69 64 3D 4B 54 5F 57 4C 41 4E 5F 38 31 5:43:d6 jssid=KT WLAN 81 0312 44 42 5F 35 47 48 7A 09 64 61 74 65 5F 69 6E 66 6F 3D 32 30 31 35 2D 30 DB 5GHz date info=2015-0 033638 2D 30 32 20 31 39 3A 35 35 3A 30 32 09 65 72 72 6F 72 5F 74 79 70 65 8-02 19:55:02 error type 03603D 30 09 6B 65 79 5F 74 79 70 65 3D 57 50 41 5F 50 53 4B 09 62 73 73 69 =0 key type=WPA PSK bssi 038464 3D 30 30 3A 32 37 3A 31 63 3A 38 31 3A 31 64 3A 62 39 00 65 73 73 69 d=00:27:1c:81:1d:b9 essi 0408 64 3D 4B 54 5F 57 4C 41 4E 5F 38 31 44 42 09 64 61 74 65 5F 69 6E 66 6F d=KT WLAN 81DB date info 0432 3D 32 30 31 35 2D 30 38 2D 30 32 20 32 30 3A 32 31 3A 31 37 09 65 72 72 =2015-08-02 20:21:17 err 0456 6F 72 5F 74 79 70 65 3D 30 09 6B 65 79 5F 74 79 70 65 3D 57 50 41 5F 50 or type=0 key type=WPA P 048053 4B 09 62 73 73 69 64 3D 30 30 3A 32 37 3A 31 63 3A 38 31 3A 31 64 3A SK bssid=00:27:1c:81:1d:

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.

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

Table 3: Analysis results

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
IN	Missing	1	0	0	312
Ave	rage		13.53		43.19
Med	lian		14.10		
Мо	ode		12		0
Standard	Deviation		5.142		142.990
Vari	ance		26.423		20735.103
Rai	nge		25		1824
Mini	mum		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 integrated ghtweight 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.