Standard Model for Mobile Forensic Image Development

Sojung Oh[1], Eunjin Kim[1], Eunji Lee[1], Yeongseong Kim[2], and Gibum Kim[1*]
[1] Department of Forensic Sciences, Sungkyunkwan University
Seoul 03063, South Korea
[e-mail: mira0809@naver.com, eunjin810@g.skku.edu, jamemanionda@g.skku.edu, freekgb02@gmail.com]
[2] Telecommunication Technology Association(TTA)
Gyeonggi-do 13591,South Korea
[e-mail: akdl44@tta.or.kr]
[*]Corresponding author: Gibum Kim

Received August 15, 2022; revised October 14, 2022; revised November 15, 2022; accepted November 22, 2022; published February 28, 2023

Abstract

As mobile forensics has emerged as an essential technique, the demand for technology development, education and training is increasing, wherein images are used. Academic societies in South Korea and national institutions in the US and the UK are leading the Mobile Forensic Image development. However, compared with disks, images developed in a mobile environment are few cases and have less active research, causing a waste of time, money, and manpower. Mobile Forensic Images are also difficult to trust owing to insufficient verification processes. Additionally, in South Korea, there are legal issues involving the Telecommunications Business Act and the Act on the Protection and Use of Location Information. Therefore, in this study, we requested a review of a standard model for the development of Mobile Forensic Image from experts and designed an 11-step development model. The steps of the model are as follows: a. setting of design directions, b. scenario design, c. selection of analysis techniques, d. review of legal issues, e. creation of virtual information, f. configuring system settings, g. performing imaging as per scenarios, h. Developing a checklist, i. internal verification, j. external verification, and k. confirmation of validity. Finally, we identified the differences between the mobile and disk environments and discussed the institutional efforts of South Korea. This study will also provide a guideline for the development of professional quality verification and proficiency tests as well as technology and talent-nurturing tools. We propose a method that can be used as a guide to secure pan-national trust in forensic examiners and tools. We expect this study to strengthen the mobile forensics capabilities of forensic examiners and researchers. This research will be used for the verification and evaluation of individuals and institutions, contributing to national security, eventually.

Keywords: Mobile Forensics, Digital Forensic Image, Image Development Model, Digital Forensics, Digital Evidence

This study was supported by the Institute for Information & Communication Technology Planning & Evaluation (IITP) (No.2022-0-00007, ICT Standardization Study in South Korea) funded by the government (Ministry of Science and ICT) in 2022. And a preliminary version of this paper was presented at APIC-IST 2022, and was selected as an outstanding paper.

http://doi.org/10.3837/tiis.2023.02.019 **ISSN : 1976-7277**

1. Introduction

The importance of mobile forensics has been emphasized in academics and industries with the rapid increase in the usage of mobile devices. Owing to their small sizes and large storages, mobile devices are actively used for crime. So, there have been essential evidence for almost all cases. Accordingly, the demand for mobile forensic training has increased sharply, resulting in an increase in the number of mobile forensic courses, and such training has become a requirement for professional qualifications. In particular, various attempts have been made in South Korea, such as establishing standards for Mobile Forensic Image (hereinafter, MFI) development processes. In **Table 1**, the number of mobile forensics cases carried out by the Korean National Police Agency (KNPA) increased by a factor of 32.5 in 10 years from 1,611 cases in 2010 to 52,479 cases in 2020 [1]. Mobile devices account for approximately 80% of digital forensic analysis cases, indicating that mobile forensic is the mainstream [2].

Table 1. Status of Mobile Forensics in South Korea (National Police Agency, Number of device)

Div	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Digital Forensic	5,493	6,247	7,388	10,429	11,200	14,899	24,295	32,281	36,060	45,103	56,440	63,935
Mobile Device	658	1,611	3,352	5,870	7,332	10,656	19,526	26,408	30,238	36,986	46,551	52,479
Ratio	12.0%	25.8%	45.4%	56.3%	65.5%	71.5%	80.4%	81.8%	83.9%	82.0%	82.5%	82.1%

However, most of the digital Forensic Images used in training are images generated in the disk environment, and these images are mainly developed on disks. It is therefore difficult to say whether this situation enhances the capacity for mobile forensics. South Korea relies on foreign countries for ISO/IEC 17043 and ISO/IEC 17025 accreditation and this framework is used in the national system without any guidelines or standards. Consequently, the capacity for mobile forensics is at a standstill, and it is difficult to guarantee the reliability of MFI used by the country. Examples of limitations in mobile forensic technology can be found in South Korea and the US. In South Korea, there was the ‘Baksa Bang’ case [3], which became a grave social issue owing to the sexual exploitation, making and distribution of illegally filmed through Telegram (2020), and the rape and murder case at a famous university, where a smartphone video of the crime became critical evidence (2022) [4]. Additionally, digital evidence analysts in the US failed to unlock the iPhones of the suspects during the San Bernardino terrorist attack (2015) [5] and the Sutherland Springs church shooting (2017) [6, 7]. In 2019, actual personal information was disclosed in the MFI released for a forensic competition in South Korea, and the competition was canceled. These cases revealed the limitation of South Korea's MFI development capabilities [8]. There is a limit to developing images due to the lack of advanced research and mobile devices are application-oriented. Therefore, this paper proposes a standard model for image development and verification processes suitable for mobile devices.

First, in Chapter 2, we explain the need for a standard development process based on previous studies and a survey conducted by our research team. In Chapter 3, we discuss the design of the development process based on the results of the expert survey. Finally, in Chapter 4, we review each stage of the development process and discuss the implications of the study and applications of the proposed method.

2. Theoretical View of Mobile Forensic Image

2.1 Definition of Mobile Forensic Image

Generally, "Image" refers to a photograph or graphic [9]. In digital forensics, however, it means a copy created as a result of imaging a partition or disk. The definition of "image" is not unified academically, and the word is defined in various ways by the Supreme Court of South Korea, the Telecommunications Technology Association (TTA), and relevant government authorities. The Supreme Court defines it as 'a file created by duplicating the bit string method in the same way as data storage media' [10]. The Telecommunications Technology Association Standard (TTAS) of TTA defines a disk image as "*bit-unit data of a digital data source*" and an image file as "*data output as a result of imaging as a digital evidence copy*" [11]. Kirschenbaum (2008) defined an image as expressing all bits of information in the original media as they are so that all recorded information is stored in the original storage structure [12]. Accordingly, an image is a copy of all data recorded on a device in a special file format, which can ensure the integrity of digital evidence. Kim et al. (2015) defined the image created by digital forensic tools as a '*dataset*' [13]. Park et al. (2016) defined data that provide information on development as '*data set for reference*' for collection, and results for verifying data collected from digital devices [14]. This definition can't cover images that reflect user actions.

Meanwhile, Oh et al. (2021) defined an image as "*a file produced in a special format that cannot be modified to enable simulation after intentionally recording traces of planned use based on a virtual scenario on a digital device*" [15]. Therefore, we defined the *MFI* as "*a special type of file produced by recording traces of use on a mobile device in a pre-planned scenario-based virtual environment and copying it in a bit string format*".

2.2 Trends in Mobile Forensic Image

MFI is being developed steadily for competitive contests held by academic societies, companies, and investigative agencies. In South Korea, scenarios and topics are developed every year by the Korean Digital Forensics Society (KDFS) [16], Korean Information Protection Society (KIISC) [17], and Korean Institute of Forensic Science [18]. Honeynet held the "Digital Forensics challenge on hacking and security incidents", which was discontinued in 2015 [19]. The Digital Forensics Research Workshop (DFRWS) was produced with the theme of Linux, data carving, and malware and has included the latest devices and technologies, such as the Internet of Things, since 2017 [20]. The United Nations Office on Drugs and Crime (UNODC) held and developed the "*Africa Digital Forensics Challenge*" for Africa, in which MFI was used [21]. Since 2018, Magnet has held "*Magnet CTF*", with various topics such as networks and memory [22]. In academia, Choi et al. (2010) proposed a composition plan for images of computer forensic tool verification suitable for Korea [23], and Kim et al. (2015) developed a dataset and verified it by using forensics tools to analyze both time-related data criteria and user actions criteria [13].

In the US and Europe, investigative agencies have led the development and distribution of images. The National Institute of Standards and Technology (NIST) of the US produced datasets from separate projects: Computer Forensics Tool Testing (CFTT) [24] and Computer Forensics Reference Data Sets (CFReDS) [25]. CFTT provided guidelines for verifying Windows forensic tools, and CFReDS aims to provide images for tool verification. The European Union Agency for Cybersecurity (ENISA) published an educational dataset called "Training for Cybersecurity Specialists", but updates stopped in 2019 [26]. Digital Corpora also provided content necessary for image development, such as media and documents, but

updates are not active [27]. In addition, the ISO/IEC, ITU, and Korea Laboratory Accreditation Scheme (KOLAS) produced images for the purpose of accrediting testing institutes and proficiency testing institutes. However, these projects are often suspended in part, and even though the types of mobile devices are being developed, their use is limited due to the low frequency of updates. Above all, most of them are limited to disks; thus, they do not meet the needs of the latest technologies used in training, and technique development for mobile forensics.

Michel et al. (2022) developed '*AutoPoD-Mobile*', an open-source framework for automating MFI generation [28]. Europe Digital Corpora developed and distributed images for Android devices (Android 10) [27]. Magnet Forensics distributes images through the CFReDS project every year [29], and DFRWS developed images for mobile environments in 2011 and 2014 and released them through challenges [20]. In particular, Cellebrite distributed images twice through the CFReDS project for Android and iPhone environments in 2021 [25]. Currently, in the field of mobile forensics, it is difficult to meet the needs of consumers because images are developed and used only once and there is no guideline for the development process. Because of the nature of mobile devices, the storage method and types of artifacts differ from those of the disk; thus, it is difficult to apply the digital forensic method or process as it is [30].

2.3 Development and Comparison of Disk Forensic Image

The Digital Forensic Image development process consists of 10 steps: a. needs analysis, b. scenario design, c. criminal act identification, d. analysis technique selection, e. legal review, f. establishment of system environment, g. information development for crime, h. criminal act execution, i. performing imaging, j. verification **Table 2**. It is meaningful in that this study is the first to model the image development process that applies to all types of digital media. However, it is difficult to apply the steps of analysis technique selection, system environment establishment, and criminal act execution to a mobile environment.

Table 2. Digital Forensics Image Development Model (Oh et al., 2021)

No	Development	Content	No	Development	Content
1	Needs analysis	- Client interview - Basic survey	6	Establishment of System environment	- Device initialization - Setting partition and OS - Installation of application software
2	Scenario design	- Selection of topic - Character selection and role assignment - Technology environment and plot setting	7	Information development for crime	- Development of personal identification information - Development of content information
3	Criminal act specific	- Identification of criminal acts	8	Criminal act execution	- Applying basic information - Conducting criminal/non-criminal acts
4	Analysis technique selection	- Defining method of crime - Selection of analysis technique	9	performing imaging	- Selection of image format - performing imaging and hash calculation
5	Legal review	- Selection of legal experts - Reviewing legality of personal identification information - Reviewing legal issue of content information	10	Verification	- Self-inspection - External verification and correction

Because a mobile device can perform actions through an application, it is necessary to identify its functions in advance. In addition, because mobile devices are difficult to manipulate artificially, it is virtually impossible to modify the acts(or artifacts). Finally, there

is a limit to finding a sample that can be analyzed, due to the lack of image cases developed on mobile devices. Digital media require specialized processes and guidelines, as different data are stored and deleted in different ways.

3. Development Method of Mobile Forensic Image

3.1 Design of Development Process

We analyzed the design of the draft of development processes based on research by Oh et al. (2021) and Park et al. (2016) and documents distributed by national institutions such as NIST to prepare a draft image development process suitable for mobile devices. Then, we conducted semi-structured written interviews to validate the reliability of the initial model and supplemented it through a correction-and-deletion process. In the interview, five digital analysts with professional experience in producing MFI or more than eight years of working experience in digital forensics were selected. The survey covered five topics: development status, considerations for the development, development process (proposal), verification, and evaluation. It consisted of 12 questions related to topics such as application classification, removal methods of illegal issues, the appropriateness of development processes, and the appropriateness of evaluation indicators **Table 3**. As a result, the final proposal was shortened from 13 steps of three stages to 11 steps of three stages.

Table 3. Five selected experts

Div	Expert A	Expert B	Expert C	Expert D	Expert E
Organization	Investigative agency	Investigative agency	Investigative agency	Law firm	Investigative agency
Duty	Examiner	Examiner	Examiner	Specialist	Examiner
Work experience	9 years	8 years	12 years	12 years	21 years
experience	O	O	O	O	O

3.2 Establishment of Development Process

We presented the following to the experts in the planning stage: a. establishment of design principles, b. scenario design, c. selection of analysis techniques, d. review of virtual information, e. review of legal issues, f. creation of virtual information, g. device configuration, h. artifact generation, i. performing imaging, j. Developing a checklist. Finally, in the validation stage, k. self-verification, l. third-party verification, and m. completeness evaluation and acceptance judgement were presented. However, experts suggested that legal review is necessary prior to image development. Thus, we enacted in a macroscopic sense the “design principle”, and established it as a process to review the design direction. In particular, the experts emphasized the importance of factory initialization before image development because mobile devices often record personal information. Therefore, an image must be created after adding the system setup process for the image and performing the scenario. Finally, we supplemented 11 elements: a. setting of design directions, b. scenario design, c. selection of analysis techniques, d. review of legal issues, e. creation of virtual information, f. configuring system settings, g. performing imaging as per scenarios, h. developing a checklist, i. internal verification, j. external verification, and k. confirmation of validity. We attempted to divide the whole process into several sub-stages including the planning, development, and

verification stages for more systematic development.

The planning stage consists of setting the design directions, designing scenarios, selecting analysis techniques, and reviewing legal issues. The first step, ‘setting of design directions’ involves defining the development purpose in detail by organizing the requirements of the person who requests the development of the MFI and determining whether to accept it. Next, ‘scenario design’ involves selecting the subject of the crime to be used in development and designing specific criminal acts. The ‘selection of analysis techniques’ is a step to review whether the scenario and criminal behavior were planned by reflecting the client's requirements. And the most suitable technique is selected for analyzing artifacts generated according to the criminal behavior. In ‘review of legal issues’, relevant laws are examined to consider the legal constraints related to personal information, location information, and SIM information that can only be obtained from mobile devices. We presented this as a stage to prepare performance guidelines by listing the virtual information and actions necessary to perform the scenario and to deal with legal issues in advance.

The development stage consists of creation of virtual information, configuring system settings, and performing imaging as per scenarios. The ‘creation of virtual information’ step involves producing virtual information that has been legally reviewed before performing the scenario. In other words, the virtual information necessary for performing scenarios is generated, the environment of the mobile device is set, and an artifact is generated as per the planned function. The ‘configuring system settings’ involves performing factory initialization on the device and setting virtual information in the system. In ‘performing imaging as per scenarios’, the scenario's action is performed on the mobile device to record digital evidence and perform imaging to create a copy.

The verification stage comprises checklist writing, internal verification, external verification, and confirmation of validity. ‘Developing a checklist’ involves preparing a comprehensive review list based on the client's requirements, design principles, and analysis techniques. Therefore, we presented that evaluating the completeness of the product is essential for quality control and maintenance. Next, ‘internal verification’ involves checking and correcting errors by analyzing the completed MFI and checking whether all planned items are reflected and detected correctly. The ‘external verification’ is a stage of secondary verification performed by requesting verification and evaluation from a third party. ‘Confirmation of validity’ is vital in determining whether to pass and distribute MFI. We presented the verification stage in detail so that it can be efficiently designed for quality control in the future. Furthermore, specific criteria for determining whether to distribute images were suggested by presenting the evaluation stage.

4. Modeling of Mobile Forensic Image Development

4.1 Planning Stage

4.1.1 Setting of Design Directions

‘Setting of design directions’ is the process of establishing the necessary principles to follow in the development of MFI. We suggested to the expert that the client should present the purpose of use, because a MFI is developed with a special purpose. The file type and difficulty of the analysis technique of MFI are determined by the purpose of utilization; therefore, the request should be organized through an interview with clients before developing an image. In particular, it is necessary to determine the development period and the theme of the scenario. In this regard, experts said that it is important to identify problems in advance because sensitive

information may be included owing to personal authentication, and it is difficult to modify behavior in a mobile environment. They suggest that more detailed design plan is needed than under disk environment and that it is necessary to interview the clients and check their list of analysis tools. We revised the design direction setting not only to define the purpose and establish the design direction between the client and developer but also to discuss the status of mobile forensic analysis tool possession, analyst job, development period, and distribution methods in detail. Additional modifications should be made if the clients have any other special requests.

4.1.2 Scenario Design

'Scenario design' is the process of sharing specific stories about the selected topics. When designing a scenario, the number and the role of characters should be determined, and the behavior of each character should be selected so that the topic can be clearly recognized. Experts have suggested consists a scenario with topics frequently encountered addressed in the area. They referred that it is appropriate to select a topic with a high frequency of occurrence and to provide various images so that the investigative agency could experience various situations. They also suggested that a process to check whether there is a limit to implementing the planned behavior and whether the development purpose can be achieved or not, is needed. Experts have divided the development purpose into training, qualification verification, tool testing, competition, and technology development. When the technical difficulty for each development purpose was scored out of 10 points (with 10 corresponding to the highest difficulty), competition and technique development had the highest score (9.2 points), followed by tool tests (9 points), qualification (8 points), and training (7.2 points). The technical difficulty of competitions and technology development are high because new analysis techniques must be developed. The tool test is used to test performance, and although the topic is unimportant, it is suggested that topics that can be analyzed in certain situations such as SQLite, malicious code, and remote-access logs from messenger apps, are good **Table 4**.

Table 4. Subjects selected by experts for each development purpose

Purpose of development	Characteristics	Selected topics (technologies)
Tool validation	Topics with artifacts that can be analyzed in special situations	Restoring conversation details of messenger apps, analyzing malicious code, analyzing remote-access apps, etc.
Qualification verification	Topic that is used as a medium for materials that can be easily produced or distributed via mobile	Leakage of industrial secrets, development and distribution of illegal photographs, internet gambling, etc.
Training	Topic of conversation through messenger application	Internet goods fraud, distribution of pornography, voice phishing, etc.
Competition	Topics that identify application information analysis technology not supported in commercial tools	Malware analysis, tracking of virtual assets, leakage of industrial secrets, etc.
Development of techniques	Topics for responding to the latest fashions	Development of hash generation technology for videos such as deepfake, development of internet gambling investigation technology, development of decoding technology, etc.

Finally, according to expert opinions, a scenario needs to be designed as follows: a. thematic materialization; b. setting the roles and personalities of characters; c. selecting direct actions; d. selecting indirect actions. The character's role determines the 'direct actions' and influences the selection of tracking techniques. 'Indirect actions' occur on a daily basis and are not directly related to crimes. The number and implementation of indirect behaviors should be carefully determined so as not to affect direct behavioral analysis.

4.1.3 Selection of Analysis Techniques

‘Selection of analysis techniques’ is the process of analyzing techniques that can track the direct actions of scenarios listed and selected in consideration of the client's tools. Mobile devices mostly use Linux-based operating systems; thus, there are few Windows-based analysis tools. Rather than having a set technique for extracting artifacts, it focuses on analysis, such as acquisition of related databases or logs [31]. Thus, the technical difficulty depends on the function. Experts agreed with this, and we presented a list of human actions that can be performed on mobile environment based on the development of the disk based Forensic Image. Initially, 13 actions were presented, but we added ‘sharing’, ‘separation’, ‘viewing’, and ‘certification’ reflecting the experts’ opinions, suggesting a total of 17 actions **Table 5**. Some experts referred that the "certification" should be included in the payment systems such as Samsung Pay and Apple Pay and mobile banking applications such as Toss. However, considering actual personal information needs to be recorded on the device, it has been concluded that the ‘certification’ stage is not suitable for MFI development. Therefore, we excluded applications that require actual personal authentication but included applications that only use passwords. However, it is suggested that biometric authentication can be achieved by printing and utilizing fake fingerprints or faces using a 3D printer or laser printer and by providing biometric information in a scenario. Therefore, we added this to the act of “locking.” Information produced by wireless communication such as GPS, Bluetooth, and Wi-Fi, as well as hardware such as the Universal Subscriber Identity Module (USIM) and modulators, can be a clue to track the character's movements and should be included in important analysis elements. However, automatically generated artifacts can cause confusion during analysis. We took details as follows: a. clearly distinguished direct and indirect actions in the scenario and b. determined a technical method for tracking the action.

Table 5. Acquisition of information by action and related applications

No.	Act	Obtainable information	Related applications
1	Power	Power on	Setting, shutdown, power button, etc.
		Power off with user request	
		Shutdown with low battery	
2	Reboot	User request	Fast reboot, restart, reboot manager, etc.
		Recovery mode	Reboot into recovery, recovery reboot, etc.
3	Lock	Password	Setting, lock screen, lock screen, lock password, etc.
		Pattern	
		Biometric information	
		PIN number	
4	Insert	USIM	SIM card, etc.
		SD card	SD card manager for Android, files to SD card, etc.
5	Connection	Wi-Fi	Setting, Wi-Fi manager, tethering, etc.
		Hotspot	Setting, mobile hotspot, Wi-Fi hotspot, etc.
		Bluetooth	Bluetooth pairing, Bluetooth Auto Connect, Bluetooth sharing, etc.
6	Execution	Application	Shopping, reservation, streaming, gaming, etc.
		Website	Chrome, Samsung Internet, Opera, Firefox, Whale, etc.
		File	File Manager, Polaris Office, Zipper, Document Viewer, etc.
7	Communication	Call	Call, T Call, WhoWho, Google Call, etc.
		Message	Message, Google Message, iMessage, etc.
		Messenger	KakaoTalk, LINE, Discord, Telegram, WhatsApp, etc.

		Location information	T map, Apple Maps, KakaoMap, Google Maps, Naver Map, etc.
		NFC	NFC Tools, NFC Reader Writer, NFC Tasks, etc.
		E-mail	Gmail, Samsung Email, Naver Mail, Daum Mail, myMail, etc.
8	Search	Local device search	Finder, etc.
		Website search	Chrome, Samsung Internet, Google, NAVER, etc.
		In-app search	KakaoTalk, Instagram, Maps, TikTok, etc.
9	Creation	Photo	Camera, Snow, Ulike, Silent camera, SODA, Foodie, Capture, etc.
		Video	Camera, YouCut, VivaVideo, Snow, Ulike, Slient Camera, etc.
		Recording	Samsung Voice Record, Recorder, Voice Recorder, Voice Memo, etc.
		Memo	Samsung Note, ColorNote, Naver Memo, FolderNote, etc.
		Calendar	Calendar, Google Calendar, Naver Calendar, etc.
		Health	Samsung Health, Google Fitness, Huawei Health, iOS Health, etc.
10	Download	Application	Google Play, iOS App Store, etc.
		File	Chrome, Samsung Internet, NAVER, Kakaotalk, Dropbox, etc.
11	Modification	System	Setting, etc.
		File	Polaris Viewer, Google Document, Microsoft Office, etc.
12	Deletion	Application	application deletion—uninstallation, uninstallation program, etc.
		File	Junk Cleanup, File Management Expand Storage Space, etc.
		Communication details	Call, Message, History Eraser, etc.
13	Concealment	Encryption	Safe Camera—Photo Encryption, gallery vault, etc.
		File concealment	Safe Folder, Photo Lock(Smart Gallery), Hide Photo/Video etc.
		Recovery mode	Recovery Reboot, etc.
14	Share	Cloud service	iCloud, Google Drive, NDrive, One Drive, etc.
		SNS	Instagram, Facebook, YouTube, etc.
		Contents	Private Share, Shared Album, etc.
15	Separation	Dual apps	WhatsApp, Facebook, KakaoTalk, Instagram, etc.
16	Watch	OTT	Netflix, Wave, YouTube, etc.
17	Certification	Personal information	PASS, OTP, Google Authenticator, etc.

4.1.4 Review of Legal Issues

‘Review of legal issues’ is the process of designing guidelines to be used for examining scenarios and determining whether there is any possibility of legal violation in implemented actions, content used, etc. A mobile device can record large amount of data, which is called a collection of personal information. Therefore, there is considerable potential for sensitive issues to arise, depending on the type of information. For example, personal information can give rise to a legal issue if privacy infringement occurs and the content used in MFI violates the copyright. As experts have suggested that this process is the most important, we classified the information included in the image by feature. It is classified into 'virtual personal content,' which can be used to identify characters, and 'virtual content,' which is used to perform other scenarios. ‘Virtual personal content’ is information that arbitrarily sets a name, media account information, phone number, SNS account information, and e-mail address. Virtual content is information that serves as a clue for tracking behavior using files such as documents and photos used for action. It also includes additional information that can capture the character's job, daily life, and hobbies. Experts suggested that many factors can lead to legal violations in the development of images, such as personal information or illegal activities. Therefore, we revised the process to confirm that the virtual information listed by the developer can be performed within the design principle. In addition, the process of separately reviewing legal

issues in the verification stage after the completion of development is added.

Downloading and using photographs or files may violate copyright laws. The Copyright Act of South Korea stipulates that a person can be punished if they use copyrighted content or other people's unique creations at no reasonable price (Article 136 Paragraph 1 sub 1). When opening the USIM in South Korea, using other people's names is subject to the Telecommunications Business Act (Article 30). Activating a mobile device with the name of another person to provide or lend funds is strictly prohibited (Article 32-4 Paragraph 1 sub 1). And the possibility of finding stored personal information using the mobile device cannot be ruled out. It is also suggested to prevent to use illegal contents. During actions such as downloading content or performing scenarios, viewing, possessing, and transmitting child or youth sexual exploitation materials may be subject to punishment under the Act on the Protection of Children and Youth against Sex Offenses; relevant data should be considered if not intended (Article 11). The act of selling or promoting legally prohibited goods, such as drugs and guns, may violate the Narcotics Control Act (Article 3 Paragraph 12). If false information is displayed by transforming the number using a transformer such as a symbol or a VoIP gateway, this may be punished by the Telecommunications Business Act. When the topic is voice phishing, care should be taken not to use relevant hardware, because the Telecommunications Business Act states, "a. No person shall fabricate or use a false phone number of a caller while making phone calls for making financial profits by deceiving other persons or for harming them by verbal abuse, threats, harassment, etc. b. No person shall provide services for fabricating or using a false phone number of a caller for profit" (Article 84-2 Paragraph 1, 2). Location information may be recorded while performing the scenario with possession of a mobile device. If this information is collected and used without consent, it may violate the Act on the Protection and Use of Location Information, which stipulates, "No one shall collect, use, or provide any location information without the consent of the subject of relevant location information"(Article 15 Paragraph 1). Thus, because illegal actions can be unintentionally committed while performing the scenario, countermeasures should be prepared by reviewing them in advance. There is need for a method in which a developer first reviews the entire development process and then requests it from an expert.

4.2 Development Stage

4.2.1 Creation of Virtual Information

'Creation of virtual information' is the process of creating the virtual information necessary for performing a particular scenario. In this process, it is important to accurately reflect the planned behavior to perform actions in the scenario without any mistakes. The virtual information, which includes personal information about characters and essential content for performing actions in the scenario, reviewed earlier should be utilized. Experts have suggested that foreign or completely fictional names should be used for naming the characters. In addition, they have suggested that the resident registration number should be written only as the front digit and that the phone number should be set differently. In the case of illegal content such as pornography, there is an opinion that data from actual cases should be used through de-identification in investigative agencies, but it is appropriate to mark "pornography" or "evidence." Therefore, the researchers have specified this step as the one wherein all essential virtual information are created before performing actions in the scenario.

4.2.2 Configuring System Settings

'Configuring System Settings' is the process of factory resetting a mobile device and recording virtual information in the system so that the actions can be performed immediately. Legitimate virtual information should be created, and no data should be stored on the device. In particular, if the device is not new, repeated resetting is recommended to complete the initialization process. After this, the device should be connected to the network. At this time, personal information, such as location, can be obtained from Wi-Fi connection history; thus, a location where the available Wi-Fi can be used and the Wi-Fi password should be determined in advance. Device account information is registered when the device is connected to the network. Then, following the virtual information guidelines, an account is registered on the device, and essential information is registered on social media, messengers, and other applications. Thereafter, content such as photographs and contact with other characters required to perform the actions in the scenario is stored on the device. Experts have suggested that configuring system settings is a necessary process and should be emphasized as a separate step. Therefore, we established the configuring system settings as a separate step in this process.

4.2.3 Performing imaging as per scenarios

'Performing imaging as per scenarios' is the process of actually performing scenario actions, recording digital evidence, and creating devices' copy via imaging. There are two main types of imaging methods; physical and logical. In physical acquisition, data are copied bit-by-bit from the entire device, and in the logical acquisition, copies of logical storage are obtained in the allocated space [32]. Logical acquisition needs less storage than physical acquisition and is suitable for unrooted devices [33].

If the administrative authority of the operating system is obtained through rooting, the device may be damaged or an infinite reboot may occur. It is important to check in advance what forensic tools the client has and determine through tests how appropriate they are for imaging. Experts have stated that artifacts in the MFI can be used to prove behavior from the perspective of an analyst and are therefore not significant from the perspective of a developer; thus, we changed it to performing in the scenario. In particular, it has been suggested that criminal acts are not the only acts that criminals perform using mobile devices; it is necessary to also appropriately reflect on the daily acts of criminals. Acts can be classified as direct, indirect, or irrelevant. In this process, direct and indirect acts were performed according to a timed manner in a planned scenario. At this time, irrelevant acts were defined as actions performed in daily life, hobbies, etc., and should be appropriately reflected to identify direct and indirect behaviors; i.e., we specified it as a step of performing the planned action in the scenario and creating a copy to obtain the log.

4.3 Verification Stage

4.3.1 Developing a checklist

'Developing a checklist' is the process of preparing an overall review list of MFI, including design principles and analysis techniques. Experts have stated that the content should be reviewed by investigators with experience with actual cases related to the scenario. They have suggested that developers should be able to add items autonomously because the checkpoints may change depending on the MFI development process, scenario, and criminal acts. Therefore, we added a process in which developers must analyze on their own and describe the detailed settings for image development when the image is completed. The third-party verification step is based on a checklist prepared for the accurate verification of the completed

image. Third parties are not aware of the details, because they do not participate in image development; thus, developers must provide details so that the third parties can learn everything from the checklist **Table 6**.

Table 6. The element of Checklist on Mobile Forensic Image's development

Step	Checklist	Contents
Design Direction	Purpose of use	Is it designed to suit the purpose of basic training in digital forensics laboratories?
	Retention tools	Have you checked the status of forensic tools such as AXIOM and MD-series?
	Analyst duties	Is the difficulty level of the analysis set according to the researcher's competency?
	Development period	Was it made within 2 weeks of the development request period?
	Device/OS	Is it built in the Galaxy S10 and Android 10?
	Publishing method	Is it published as external storage?
Scenario	Subject	Is it appropriately reflected as the theme of industrial technology leakage?
	Device capacity	Is it built with a capacity of 128 GB?
	Character setting	Did you set the virtual name for the scenario configuration?
		Is the role of each character appropriate and not obstructed from the analysis?
	Direct acts	Is the scenario designed to identify the act of filming and selling confidential data, attempts to purchase drugs, and the concealment of criminal facts?
	Indirect/irrelevant acts	Is the scenario designed to identify facts that are non-criminal, such as using SNS, web search logs, watching YouTube, and creating cryptocurrency wallets?
Analysis Techniques	Analysis techniques	Are appropriate analysis techniques used, such as phone and text logs, network information, messenger conversation logs extraction, decryption, password decryption, and app data extraction?
	Applications	Does it include analysis techniques for applications such as SNS (Twitter), messengers (Telegram), Cryptocurrency App, Gmail, Camera, Chrome, Recording App, and File Sharing App?
		Are artifacts that can be analyzed in each application created?
Virtual Information	Personal information	Is individual information (e.g., name, phone number, e-mail address, and account address) not exposed as virtual information?
	Content	Is all the content to be used in the scenario, such as confidential documents, conference videos, and document photographs, listed and produced?
		Have you checked for unintended content?
Legal Issues	Telecommunications Business Act	When the USIM was opened, did it check whether it violated the Telecommunications Business Act owing to the use of personal information? Have you taken action?
	Personal Information Protection Act	When creating and utilizing new accounts, by employing names, phone numbers, e-mail, SNS, and messengers, did it check whether they violated the Personal Information Protection Act? Have you taken action?
	Copyright Act	When producing documents, videos, and photographs, did they check whether they violated the Copyright Act? Have you taken action?
	Act on the Protection and Use of Location Information	Did it check whether the Act on the Protection and Use of Location Information was violated by not using location information recorded on mobile devices without permission? Have you taken action?
Artifacts	Direct acts	Are artifacts for criminal acts, such as photographs, videos, recorded files, messengers, e-mails, clouds, networks, applications, and file concealment, generated in time?
		Is content such as photographs, videos, and recorded files loaded and checked normally?
	Indirect acts	Are artifacts for criminal-related acts, such as cryptocurrency, messengers, e-mails, web searches and visits, and SNS properly generated by referring to criminal acts?
	Irrelevant acts	Are artifacts for non-criminal acts, such as photographs, SNS, navigation, document browsing, system logs, search records, and web visits, generated in time?
Performing imaging	Imaging method	Have you acquired a physical image?
	Tools for use	Is it imaged so that it can be analyzed with forensic tools possessed by the client?
	Image format	Is the image format set to DD?

4.3.2 Internal Verification

'Internal verification' is the process of checking whether all design directions, scenarios, and behaviors are reflected based on the checklist. Developers can easily identify mistakes in the development process and find deficiencies or errors. Experts have suggested that the step in which the error occurred must be checked. If the client's requirements are not reflected, it is considered that an error is made in the design direction, and one must return to that step wherein the error occurred and reset the design direction and scenario. We specified that if an error is found in the artifact, the missing artifact should be reflected further. If an action contrary to the purpose of the design is accidentally included or an action that must be included is not performed, the process returns to the step involving the setting of preferences, i.e., "reset version of factory," which is performed again from the beginning of the scenario. If the individual information is unintentionally included and can be viewed by those published, it should also be reproduced.

4.3.3 External Verification

'External verification' is the process of requesting verification from third parties to secure completeness and reliability after internal verification. Two or more experts who have not participated in the development process need to be selected as verifier. Experts must have a high level of familiarity with mobile forensics technology and need relevant knowledge. Specific selection requirements, such as a Master's degree(or higher) or '≥3' years of working experience, must be established.

4.3.4 Confirmation of validity

'Confirmation of validity' is the process of determining pass or fail and whether to deploy MFI **Table 7**. We derived the evaluation items that can be employed to determine whether an image can be accepted using a checklist. Experts agreed on the appropriateness and importance of all the evaluation indices that we have presented. When the evaluation index is delivered to the verifier, it should include information indicating whether the verifier's career meets the qualification requirements, internal or external personnel, and consent to the use of personal information.

The evaluation items were divided into absolute evaluations that must be met and relative evaluations that must be met above a certain level. If all absolute evaluations are met and the relative evaluation result is ≥90 points, "pass" is selected; >80 and <90 points corresponds to suspension, and ≤80 points corresponds to failure. In the case where critical errors are detected, e.g., when information other than virtual information is found, "failure" is selected even if the evaluation result is ≥90 points. If one or more failures occur, they are determined to be rejected. In this case, it should be discarded without delay, and the evaluation opinion or reason for the judgement should be described and replied to.

Table 7. Evaluation Elements for Mobile Forensics Image Verification

Stage	Behavior index	Evaluation index	Points
Planning	Setting of design directions	Are all the requirements of the client reflected?	1–10
		Can it be analyzed with the client's tools or commercial tools?	P/F
		Is it produced to be deployed at the client's request?	P/F
	Scenario design	Are the scenarios suitable for the development purposes?	1–7

		Are the number of characters and roles properly reflected in the subject?	1–3
		Is the scenario appropriate for the analyst's job?	1–5
	Selection of analysis techniques	Can the analysis technique be used to analyze the behavior reflected?	1–10
		Is analysis difficulty appropriate for the analyst's level of expertise?	1–5
		Have measures been taken to prevent violation of the law?	1–7
	Review of legal issues	Have you conducted an internal or external review of legal issues?	P/F
		Have measures been taken for violations of the law?	1–7
Development	Creation of virtual information	Is all the virtual information needed for analysis derived?	1–5
		Is the virtual information necessary for the scenario derived and produced?	1–7
	Configuring system settings	Has a factory reset been performed and a network been configured?	P/F
		Are all the required applications installed?	1–3
	Performing imaging as per scenarios	Are all the artifacts for direct acts reflected (detected)?	1–7
		Are all the artifacts for indirect acts reflected (detected)?	1–7
		Did you use irrelevant acts at a level that did not interfere?	1–5
		Can the file be analyzed?	P/F
Verification	Developing a checklist	Are the design direction and scenario reflected correctly?	1–5
		Is the checklist prepared and checked and is the problem corrected?	1–7
	Internal verification	Has the error been checked through self-analysis?	P/F
		Have follow-up measures been taken, such as correction/redevelopment to fix errors?	P/F
	External verification	Has an external expert been requested to verify?	P/F
		Have follow-up measures been taken, such as correction/redevelopment due to errors?	P/F
	Confirmation of validity	Is it possible to deploy it to the client?	P/F

4.4. Implication

We presented a standard model with 11 steps with three stages for the MFI development process **Table 8**. Various issues that may arise from the development of images through the review of legal issues and verification are prevented to ensure completeness and reliability of the developed image and to avoid the discarding of the image, which was developed with significant difficulty. As the demand for mobile forensics has increased, the need for the proposed development, design, and verification processes has been recognized. For example, as the importance of smartphone forensics has recently increased, investigative agencies in South Korea have deployed mobile forensic tools and expanded their manpower [34].

Table 8. Mobile Forensic Image development process

No.	Stage	Step	Content
1	Planning	Setting of design directions	Organize the requirements of the person who requests the development of the MFI and define the purpose of development in detail after deciding whether to accept it
2		Scenario design	Select the subject of the crime to be used in development through design principles and design specific criminal activities

3		Selection of analysis techniques	Review the intended criminal activity by the scenario and select the appropriate analysis techniques
4		Review of legal issues	List the virtual information and actions required to perform the scenario and review them to establish guidelines for performance to avoid legal issues
5	Development	Creation of virtual information	Produce legal-reviewed virtual information before performing the scenario and factory-reset the mobile device to initialize the action
6		Configuring system settings	Perform a scenario action, record digital evidence, and perform imaging to obtain an image
7		Performing imaging as per scenarios	Perform scenario actions and record digital evidence, and perform imaging
8	Verification	Developing a checklist	Create a comprehensive review list of client requirements and scenarios, including design principles and analysis techniques established
9		Internal verification	Perform self-analysis of completed MFI to find and correct errors
10		External verification	Select and verify two or more experts who did not participate in the development process after completion of the self-evaluation
11		Confirmation of validity	Evaluate the completeness and decide whether to deploy the MFI

The proposed development process can be used for training, qualification verification, tool tests, competitions, etc. by investigative agencies and private enterprises. With regard to international standardization, the suggested model can be used by the laboratory accreditation scheme and operating institutions in the field of digital forensics. Testing laboratories can use it to evaluate the qualifications and equipment of employees in digital forensic laboratories or to produce and deploy images from proficiency testing operators such as CTS [35] and ISFCE [36] to conduct proficiency testing. It can also be used in proficiency tests to ensure the reliability of appraisal results in criminal investigations and trials. If the capabilities of tools and professionals can be verified using commonly established MFI, it can also be used in international cases. Similar to the US and the UK, South Korea must also introduce policies to develop and steadily deploy various images by establishing platforms at national institutions. To suggest a way, after deploying the standard model through the platform, images must be provided and utilized with the participation of the public. This method is also cost-effective and competitiveness can be secured through implementing simulations. Because there are only a few platforms that allow the uploading of shared projects without a guide, it is necessary to limit the verifiers that are provided to national institutions to share only images that have passed the verification and evaluation stages. However, because related research on the development process is insufficient and the analysis techniques differ among individuals, the contents of the expert survey conducted by the researchers may not include all analyst opinions. In addition, many applications on mobile devices require personal authentication; thus, there may be limitations about applications that can be used, except for related applications, which do not require actual personal information.

5. Conclusion

Mobile devices have recently become a major. The demand for standardized mobile forensics techniques has increased due to the wide distribution of mobile devices. MFI is expected to fulfill the social demand for mobile forensics, such as in training, and technology development. The term “image” has not been defined academically but is used by the Supreme Court and TTA to refer to a copy of digital evidence that can be used as evidence of guilt in criminal

investigations. In addition, images are actively used in challenges and training; however, the terms are not clearly defined. Therefore, we defined an MFI and found that such images can be used for various purposes. In addition, we established a development process for MFI, including a process to ensure that there are no legal issues or errors after the image is produced. The development process is divided into three stages (planning, development, and verification) and 11 steps: a. setting of design directions, b. scenario design, c. selection of analysis techniques, d. review of legal issues, e. creation of virtual information, f. configuring system settings, g. performing imaging as per scenarios, h. Developing a checklist, i. internal verification, j. external verification, and k. Confirmation of validity. The principles and guidelines for the verification and evaluation processes were also presented. Through this research, we attempted to resolve various technical and legal issues arising from the development of MFI and prevent controversies in advance.

Finally, a plan was proposed to establish the proposed process as a standard and to utilize it as a policy. Specifically, measures for human-resource development, training through standard distribution, and the development of forensic companies and national technologies were suggested. We hope that this research will be used as a standard guide to secure pan-national trust in analysts and forensic tools. Social safety issues can be resolved by using the proposed process for analyst qualification verification, advanced technology development, and tool validation. Furthermore, following this study, we expect discussions on standard guidelines based on empirical research to be active globally.

References

[1] Min-gwon Gill, “Police analyzed 63,000 digital forensics cases last year, doubling in three years,” *DailySecu*, Oct. 12, 2021. Article (CrossRefLink)
[2] Korean National Police Agency, “Status of Digital Evidence Analysis(2010~2020),” 2021. Article (CrossRefLink)
[3] H. J. Choi, “Provide clues to the victims and the media! ‘God-god’ was captured like this,” *Ilyonews*, May. 14. 2020. Article (CrossRefLink)
[4] J. H. Park, “Inha University's sexual assault victim screams and appeals for help.. Even the sound of falling is saved,” *Financial News*, Aug. 18. 2022. Article (CrossRefLink)
[5] Brian Day, “San Bernardino mass shooting: 2 suspects killed in shootout with police,” *The Sun*, Dec. 2. 2015. Article (CrossRefLink)
[6] Anthony Cuthbertson, "FBI Wants Apple to Hack 'Blood-Spattered' iPhone Used by Sutherland Springs Shooter," *Newsweek*, Nov. 20. 2017.
[7] Yu-ji Lee, ““If making 10 mistakes, delete it all,” Pay attention to iPhone security in forensic challenge,” *Hankookilbo*, Dec. 5, 2019. Article (CrossRefLink)
[8] Young-il Jung, “Korea Digital Forensics Society, ‘Personal Information Leakage’ at Forensic Competition,” *etnews*, Sep. 18. 2019. Article (CrossRefLink)
[9] Sungmi Kim, “A study on the Ontological Meaning of Photographic Images,” M.S thesis, Dept. Philosophy, Changwon Univ, Changwon, Republic of Korea, 2012.
[10] Supreme Court Decision 2017Do13263 Decided Feb. 8, 2018.
[11] Data Expression Standard for Digital Forensic Investigation: Part 1. Overview and Requirements, TTAK.KO-12.0353-Part1, Dec. 11, 2019.
[12] M. G. Kirschenbaum, *Mechanisms: New Media and the Forensic Imagination*, MA, USA: Cambridge, 2007.
[13] Min-Seo Kim, Sang-jin Lee, “Development of Windows forensic tool for verifying a set of data,” *Journal of The Korea Institute of Information Security & Cryptology*, vol. 25, no. 6, pp. 1421-1433, Dec. 2015. Article (CrossRefLink)

[14] Park, Jungheum, James R. Lyle, Barbara Guttman, “Introduction of NIST's Digital Forensic Tool Verification System,” *Korea Institute of Information Security and Cryptology*, vol. 26, no. 5, pp. 54-61, Oct. 2016. Article (CrossRefLink)
[15] Sojung Oh, Taegi Lee, Gibum Kim, “A Study on Digital Forensic Image Development Model,” *Journal of Digital Forensics*, vol. 15, no. 2, pp. 273-286, Jun. 2021. Article (CrossRefLink)
[16] KDFS Forensics Challenge. Article (CrossRefLink)
[17] KIISC, Digital Forensics Challenge. Article (CrossRefLink)
[18] KOREAN INSTITUTE OF FORENSIC SCIENCE. Article (CrossRefLink)
[19] The Honeynet Project. Article (CrossRefLink)
[20] DFRWS. Article (CrossRefLink)
[21] UNODC. Article (CrossRefLink)
[22] Magnet Forensics. Article (CrossRefLink)
[23] Jaemin Choi, Jung-Hoon Oh, SangJin Lee, “A Study on Forensic Image Design for Domestic Computer Forensic Tool Testing,” *Journal of Digital Forensics*, vol. 4, no. 2, pp.65-83, 2010.
[24] Computer Forensics Tool Testing Program (CFTT). Article (CrossRefLink)
[25] Computer Forensic Reference Data Sets(CFReDS). Article (CrossRefLink)
[26] ENISA. Article (CrossRefLink)
[27] Digital Corpora. Article (CrossRefLink)
[28] Margaux Michel, Dirk Pawlaszczyk, and Ralf Zimmermann, “AutoPoD-Mobile—Semi-Automated Data Population Using Case-like Scenarios for Training and Validation in Mobile Forensics,” *Forensic Sci*., vol. 2, no. 2, pp. 302-320, Mar. 2022. Article (CrossRefLink)
[29] 2022 Takeout – Magnet CTF. Article (CrossRefLink)
[30] Weon Shin, “Analysis for Digital Evidences using the Features of Digital Pictures on Mobile Phone,” *Journal of Korea Multimedia Society*, vol. 12, no. 10, pp.1450-1456, Oct. 2009. Article (CrossRefLink)
[31] Gandeva Bayu Satrya, Soo Young Shin, “Proposed Method for Mobile Forensics Investigation Analysis of Remnant Data on Google Drive Client,” *Journal of Internet Technology*, Vol. 19, No. 6, pp. 1741-1752, Dec. 2018. Article (CrossRefLink)
[32] Lim, Yoon mi, “A study on improvement of the forensic acquisition of mobile devices: Focusing on classification and prioritization,” M.S. thesis, Dept. Information Security, Dongguk Univ., Seoul, South of Korea, 2018.
[33] Sneha C Sathe, Nilima M Dongre, “Data Acquisition Techniques in Mobile Forensics,” in *Proc. of 2018 2nd International Conference on Inventive Systems and Control (ICISC)*, pp. 280-286, 2018. Article (CrossRefLink)
[34] H. J. Lee, “Police to step up digital forensic investigations... Smartphone unlock tool deployment and dedicated personnel ↑,” *BizChosun*, Apr. 26. 2022. Article (CrossRefLink)
[35] Collaborative Testing Services. Article (CrossRefLink)
[36] The International Society of Forensic Computer Examiners. Article (CrossRefLink)

Sojung Oh received the B.S. degree in Computer Science from SangMyung University, Seoul, Republic of Korea, M.S. degree in Forensic Science from Sungkyunkwan University, Seoul, Republic of Korea. She works at digital forensic laboratory as a researcher and simultaneously, she serves as the administrative staff of the Korean Society for Digital Forensics. Her research interests include Digital Forensic, the Criminal Procedure Act, Cybercrime Investigation.

Eunjin Kim received the Bachelor degree in Computer Engineering from Soongsil University, Seoul, Republic of Korea. She is currently a M.S. degree in Forensic Science and majoring in Digital Forensics from Sungkyunkwan University, Seoul, Republic of Korea. Her research interests include Digital Forensics, Mobile Forensics, and Digital Forensic Policy.

Eunji Lee received the Bachelor degree in Computer Engineering from Dongseo University, Busan, Republic of Korea. She is currently a M.S. degree in Forensic Science and majoring in Digital Forensics from Sungkyunkwan University, Seoul, Republic of Korea. Her research interests include Digital Forensics, Mobile Forensics, and Digital Forensic Standardization.

Yeongseong Kim received his B.A. degree in Philosophy from Kyunghee University, Seoul, Republic of Korea. He is currently an senior researcher in Telecommunication Technology Association. His research interests include Digital Forensics, ICT Standardization, and ICT Policies.

Gibum Kim received the Ph. D degree in Information Security from Korea University, Seoul, Republic of Korea. He is a professor and Department Chair of Dept. Forensic Science at Sungkyunkwan University, Seoul, Republic of Korea. His research interests focus on Digital Forensics, Cybercrime Investigation, and Digital Forensic Standardization.