Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.2, Apr. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.2.197

USIM 이용 모바일 메신저 데이터에 대한 압수·수색 허용성 고찰

김 민 동,[1†] 이 현 진,[1] 이 성 진,[1] 이 연 주,[1] 김 기 범[2‡]
[1,2]성균관대학교 (대학원생, 교수)

A Study on the Permissibility of Search and Seizure of Mobile Messenger Data Using a USIM

Min-Dong Kim,[1†] Hyeon-Jin Lee,[1] Sung Jin Lee,[1] Yeon-Ju Lee,[1] Gi-Bum Kim[2‡]
[1,2]Sungkyunkwan University (Graduate student, Professor)

요 약

최근 스마트폰이 파괴되거나 비밀번호를 해제하지 못해 모바일 메신저의 데이터를 압수하지 못하는 경우가 있다. 수사기관은 암호 해독, 백업 데이터 확보 등 다각적 방법을 강구하지만, 많은 한계에 부딪히고 있다. 따라서 본 연구에서는 피의자 스마트폰에 있는 유심을 압수하고, 수사관 스마트폰에 삽입하여 메신저 데이터를 추출하는 실험을 하였다. 텔레그램과 카카오톡에서 각 대화방에 메시지를 전송하고, 일부를 삭제한 직후와 3일이 경과한 이후의 확보 가능 여부를 살펴보았다. 실험 결과, 텔레그램에서는 경과일에 관계없이 삭제하지 않은 활성 메시지만 확보할 수 있었고, 카카오톡에서는 삭제 직후의 경우 '선택한 메시지를 모두에게서 삭제' 방법으로 삭제된 메시지를 제외한 모든 메시지를 확보할 수 있었으나 3일이 경과된 이후에는 모두 확보할 수 없었다. 이와 같은 방법을 이용한 압수·수색은 형사소송법상 영장절차를 준수할 수 있고, 송·수신이 완료된 데이터를 대상으로 하기 때문에 적법한 압수·수색으로 봐야 할 것이다. 대법원 판례에 의하면 관할권 위반이라 보기도 어렵다. 다만, 압수·수색 방법에 대한 법원심사가 필요하고, 영장범위를 벗어난 데이터는 제외해야 하며 집행 이후 메시지를 수신하는 행위는 통제해야 할 것이다.

ABSTRACT

There have been the cases in which mobile messenger data cannot be seized at the crime scene due to the damage to the smartphone or the unlocking fail of the password. Investigation authorities are trying to devise many solutions such as decryption, and securing of backup data. However, it is running up against technical limitations. So, in this study, we conducted the experiment to seize the USIM from the suspect's smartphone and insert it into the investigator's smartphone to extract the messages. The result of the experiment confirms that, while Telegram messages can be secured messages that were not deleted even if 3 days have elasped after sending it, KakaoTalk messages cannot be acquired after 3 days. But, KakaoTalk message can be secured except for selectly deleted messages for all chat room participants immediately after sending and deleting the messages. The search and seizure using a USIM is the legal considering the warrant execution procedure, not a violation of jurisdiction, and the sending and receiving data. But to minimize the abuse, the court needs to review the way of search and seizure, the data beyond the scope of the warrant should be excluded , and the receipt of messages needed to be strictly controled after the execution of warrant.

Keywords: USIM, Search and Seizure, Mobile Messenger, Mobile Forensics, Digital Evidence

Received(11. 11. 2020), Modified(1st: 01. 21. 2021, 2nd: 03 .03. 2021), Accepted(03. 03. 2021)

† 주저자, korkic123@g.skku.edu
‡ 교신저자, freekgb02@gmail.com(Corresponding author)

I. 서 론

모바일 메신저(이하 "메신저"라고 함)는 1:1부터 N:N까지 다양한 형태로 텍스트, 사진, 음성, 영상, 파일 등을 전송하고 공유할 수 있는 서비스로, 전 세계적으로 사용되고 있다. 국내 스마트폰 이용자의 주 이용 콘텐츠는 2019년 기준 '메신저'가 94.7%로 가장 높은 비율을 차지하고 있다[1]. 카카오톡의 경우 이용시간 기준 메신저 시장 점유율을 96%를 차지하고 있고, 2019년 4분기 국내 월간 활성 이용자는 4,485만 9,000여 명으로 하루 평균 110억 건의 메시지가 오간다고 한다[2]. 그러다 보니 수사기관에서 각종 범죄수사를 할 때 메신저 데이터가 중요한 증거가 되고 있다. 실제 텔레그램 'N번방' 사건, 연예인 마약 관련 '버닝썬' 사건에서도 메신저 데이터가 범인 검거에 결정적인 역할을 하였다[3].

하지만 최근에 범죄자들이 스마트폰을 파괴하거나 비밀번호를 설정하여 메신저 데이터를 확보하지 못한 사례가 발생하고 있다. 또한, 종단간 암호화 기능이 구현되어 있어 메신저 회사를 대상으로 압수·수색을 하더라도 데이터를 확보하지 못하기도 한다. 경찰에서 공직선거법위반, 뇌물수사, 자살사건 등에서 스마트폰을 압수하였으나, 비밀번호를 복호화하지 못한 사례가 다수 발생하였다[4]. 미국 연방수사국(FBI)도 2016년 캘리포니아주 샌버나디노에서 발생한 총기테러 사건에서 용의자 '사이드 리즈완 파룩(Sayeed Rizwan Farouk)'의 아이폰 5C 비밀번호를 복호화하지 못해 초기 수사에 애로를 겪었다[5]. 이에 수사기관에서 물리적 복구, 암호 해독, 백업 데이터 확보 등 다각적인 방법을 시도하고 있지만, 기술적으로 성공 가능성이 높지 않고 백업 데이터가 없는 경우도 많아 증거확보에 많은 한계를 보이고 있다.

이와 같은 문제를 해소하기 위해 본 논문에서는 범용 가입자 식별 모듈(Universal Subscriber Identify Module, 이하 '유심'이라 함)을 이용하는 압수·수색 방법을 제시하고자 한다. 즉, 피의자 스마트폰에 있는 유심을 확보하여 수사관 스마트폰에 삽입한 다음 메신저를 설치하고 본인 인증절차를 거쳐 국내·외에 있는 클라우드 서버로부터 데이터를 다운로드하여 압수하는 방식이다. 나아가 이러한 압수·수색 방법이 원격·역외 압수·수색과 차이가 있는지, 형사소송법상 허용되는 압수·수색 방법인지, 나아가 전기통신감청에 해당될 여지가 있는지 등에 대한 형사법적 검토를 통해 수사현장에서 활용될 수 있는지 판단하고자 한다.

본 논문은 제2장에서 메신저 데이터의 확보에 관한 선행연구를 분석하고, 제3장에서 유심을 이용한 스마트폰의 통신 절차와 모바일 메신저의 데이터 저장 방식에 대해 살펴본다. 제4장에서는 유심을 이용하여 텔레그램과 카카오톡에서 메시지 데이터를 확보하는 실험을 하고, 그 결과를 분석하고자 한다. 마지막으로 제5장에서는 유심을 이용한 메신저 데이터 획득 방법에 대한 형사법적 쟁점을 검토하고자 한다.

II. 관련 연구

2.1 이론적 연구

최근 들어 메신저에서 데이터 확보 방법에 관한 연구들이 다양하게 소개되고 있다. 안드로이드 환경에서 카카오톡 메신저 앱의 사용흔적을 분석하고 메신저 데이터에 대한 데이터베이스의 암·복호화 방법, 연락처·채팅 데이터의 테이블 구조에 관한 연구가 소개되었다[6]. 카카오톡, 왓츠앱, 페이스북 메신저, 텔레그램, 라인에 대한 데이터 파일 아키텍처를 분석하고, 사용자가 삭제한 메신저 데이터의 복원에 관한 연구도 진행되었다[7]. 유심을 이용한 메신저 데이터의 압수·수색 방법을 가장 먼저 제시하고, 메신저 데이터가 로컬과 로컬/클라우드에 보관되는 경우와 메신저별 인증방식과 다인증 지원 여부를 조사하여 클라우드 메신저의 데이터 수집절차를 제시한 연구도 있다[8].

나아가 안드로이드 운영체제의 Oauth를 이용하여 사용자의 계정에 로그인한 후, 직접 데이터를 수집하는 방법도 제안되었고[9], 구글 계정의 크리덴셜(Credential)을 확보한 다음 다른 스마트폰에 주입하여 메신저나 클라우드 앱에 접근하여 데이터를 다운로드하는 방법도 소개되었다[10].

앞선 연구들은 유심을 이용한 압수·수색 방법을 선제적으로 제시하였다는데 커다란 기여를 하였지만, 메신저 데이터가 어떻게 존재하는지 개별적 실험이 다소 부족하였고 형사법적 쟁점에 대한 검토가 이루어지지 않아 수사현장에서 활용할 수 있는지에 대한 해답을 제시하지 못한 한계를 보이고 있다.

2.2 실증적 연구

수원지방검찰청은 2019년 도박사이트 운영진의 텔레그램 수사에 유심을 이용하였고, 이후에 대검찰

청으로부터 우수 과학수사 사례로 선정되었다[11]. 서울경찰청도 다크웹에서 마약을 거래한 피의자가 스마트폰 비밀번호를 진술하지 않자 유심을 이용하여 텔레그램에서 데이터를 확보해 피의자를 추가로 검거하였다[8]. 수사사례에 대한 영장기재 내용이나 법원의 판결내용이 확인되지 않아 법적 허용성에 관한 판단이 어렵기는 하지만, 검찰과 경찰에서 실제 사용하고 있고 대검찰청에서는 우수 수사사례로 선정한 것을 볼 때, 최소한 수사기관에서는 적법하다고 판단하는 것으로 보인다.

이와 유사한 사례로, 수사기관이 해외 이메일에 대하여 적법하게 알아낸 피의자의 계정과 비밀번호를 이용하여 역외 압수·수색을 집행한 경우가 있다. 대법원은 2017도9747 판결에서 "압수・수색할 전자정보가 압수・수색영장에 기재된 수색장소에 있는 컴퓨터 등 정보처리장치 내에 있지 아니하고 그 정보처리장치와 정보통신망으로 연결되어 제3자가 관리하는 원격지의 서버 등 저장매체에 저장되어 있는 경우에도, 수사기관이 피의자의 이메일 계정에 대한 접근권한에 갈음하여 발부받은 영장에 따라 영장 기재 수색장소에 있는 컴퓨터 등 정보처리장치를 이용하여 적법하게 취득한 피의자의 이메일 계정 아이디와 비밀번호를 입력하는 등 피의자가 접근하는 통상적인 방법에 따라 그 원격지의 저장매체에 접속하고 그곳에 저장되어 있는 피의자의 이메일 관련 전자정보를 수색장소의 정보처리장치로 내려받거나 그 화면에 현출시키는 것 역시 피의자의 소유에 속하거나 소지하는 전자정보를 대상으로 이루어지는 것"으로 허용된다고 판시하였다.

III. 모바일 메신저의 통신과 데이터 저장 방식

3.1 이동통신사, 스마트폰, 메신저 서버의 통신

스마트폰에서 전화를 걸거나 문자메시지를 전송하기 위해서는 유심이 필요하다. 유심은 '심 카드(SIM Card)'로도 불리며, 통신 네트워크에서 모바일 기기를 식별하는 모듈로 사용된다. 유심의 저장공간에는 이동통신사와 데이터 통신을 하는 데 필요한 가입자 정보, 전화번호, 요금 정보 등이 저장되어 있다[12][13]. 스마트폰에 유심을 삽입하면 저장된 인증정보를 이용하여 이동통신사로부터 전화번호를 할당받는 '유심 다운로드' 과정을 수행하고, 이후 통화, 문자메시지, 데이터 등에 대한 통신이 가능해진다. 간혹, 유심 다운로드를 수동으로 진행하거나 스마트폰의 전원을 다시 켜야 전화번호가 할당되는 경우도 있다. 스마트폰에 유심을 삽입하여 데이터 통신이 가능해지면 앱 스토어를 통해 메신저 애플리케이션을 내부 메모리에 설치할 수 있으며, 메신저를 사용하기 위해서는 간단한 인증절차를 거쳐야 한다. 텔레그램은 휴대전화 번호를 입력한 후 문자메시지로 인증 코드를 받아 입력하고, 카카오톡은 계정(이메일 또는 전화번호)과 비밀번호를 이용하여 로그인한 후 문자메시지로 인증 코드를 받아 입력하는 절차를 거친다.

3.2 메신저 데이터 저장 방식

메신저 데이터는 스마트폰 내부 메모리에 저장하는 경우와, 내부 메모리와 클라우드 서버에 모두 저장하는 방식으로 나뉜다. 즉, Table 2.와 같이 로컬 방식과 로컬/클라우드 방식으로 구분할 수 있다[8]. 로컬 방식은 스마트폰에 데이터가 저장되기 때문에 기기 변경 시 백업 기능을 활용하여 새 기기로 기존 데이터를 이전해야 한다. 하지만 로컬/클라우드 방식은 스마트폰이 메신저 클라우드 서버와 동기화되어 있어, 메신저 접속만으로 서버로부터 기존 데이터를 다운로드할 수 있다.

Table 1. Information Stored in USIM

Subscriber Info	Service Info	Security Info
USIM Serial Number(ICCID)	Mobile number (ADN/FDN/ SDN)	Ciphering Key (Kc)
International Mobile Subscriber ID(IMSI)	Message (SMS, EMS)	Ciphering Key Sequence Number
Mobile Station International Subscriber Directory Number (MSISDN)	Speed Dial (EFICI/EFOCI /EFADN)	Authentication Key (Ki)
Temporary Mobile Subscriber ID(TMSI)	Location (LAI/RAI)	-
Mobile Subscription Identification Number(MSIN)	-	-
Mobile Network Code	-	-

Table 2. Data Storage Methods by Application[8]

Application Name	Version	Data Storage	
		Local	Local/Cloud Server
Line	9.16.6	○	
Wechat	7.0.8	○	
WhatsApp	2.19.100	○	
Discord	3.1.5		○
FB Messenger	236.0		○
HangOut	26.0.1		○
Instagram	114.0		○
KakaoTalk	8.5.7		○
Skype	8.52		○
Telegram	5.12		○
TikTok	8.3.0		○

IV. 메신저 데이터 확보 실험 및 결과분석

4.1 실험 설계

유심을 이용한 메시지 확보 실험은 안드로이드 OS와 iOS 운영체제가 설치된 스마트폰을 각 2대씩, 총 4대를 사용하였다.

안드로이드 기기인 Galaxy Note10 5G와 iOS 기기인 iPhone 12 Pro(A2407)에서 메신저를 이용하여 메시지를 전송한 후 유심을 제거한 다음 이를 각각 안드로이드 기기인 V50 ThinQ(LM-V500N)과 iOS 기기인 iPhone Xs(A2097)에 삽입하였다. 즉, 전자는 피의자가 사용한 스마트폰(이하 "피의자 스마트폰"으로 칭함)으로, 후자는 수사관이 준비한 스마트폰(이하 "수사관 스마트폰"으로 칭함)으로 상정한 것이다. 모든 스마트폰에는 텔레그램 7.3.1 버전과 카카오톡 9.1.7 버전을 설치하였다.

이후 피의자 스마트폰에 텔레그램과 카카오톡 메신저의 1:1 대화방, 단체 대화방, 비밀 대화방을 생성하였다. 비밀 대화방의 경우 텔레그램은 1:1 대화만 지원하고, 카카오톡은 1:1 및 단체 비밀 대화방을 지원한다.

텔레그램에서는 텍스트, 이모티콘, 링크, 사진, 영상, 파일, 위치, 연락처, 음성 녹음, 영상 녹화 등 10가지 메시지를, 카카오톡에서는 텍스트, 이모티콘, 링크, 태그, 사진, 영상, 통화, 일정, 위치, 음성 메시지, 연락처, 파일 등 12가지 메시지를 하나의 묶음으로 하고, 각 대화방의 삭제 기능 수를 고려하여 3개에서 5개의 메시지 묶음을 전송하였다. 비밀 대화방의 경우, 텔레그램은 일반 대화방과 동일하게 모든 종류의 메시지 전송이 가능하지만, 카카오톡은 텍스트, 이모티콘, 링크, 사진, 영상 등 5가지의 메시지만 전송 가능하였다.

Table 3. Configuration of Devices Used in the Experiment

Device Model	OS	OS Ver.	Telegram Ver.	KakaoTalk Ver.	Use
Galaxy Note10 5G (SM-N971N)	Android	10	7.3.1	9.1.7	For suspects
V50 ThinQ (LM-V500N)	Android	10	7.3.1	9.1.7	For investigators
iPhone 12 Pro (A2407)	iOS	14.3	7.3.1	9.1.7	For suspects
iPhone Xs (A2097)	iOS	14.2	7.3.1	9.1.7	For investigators

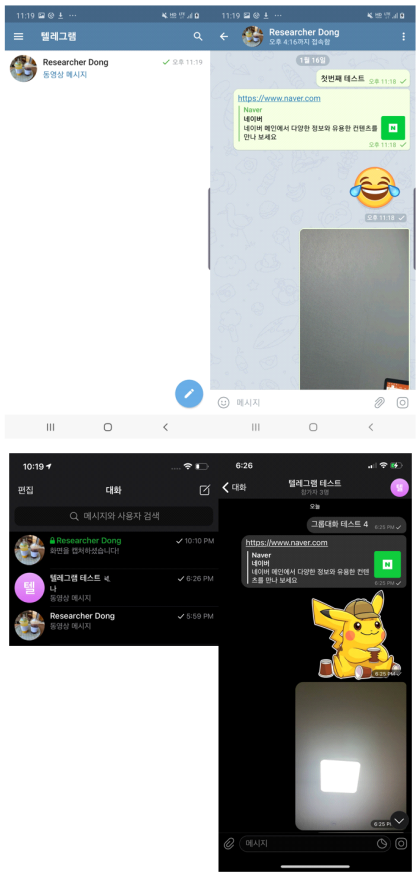


Fig. 1. Example of Telegram Data Generation in Suspect's Android(above) & iOS(below) Device

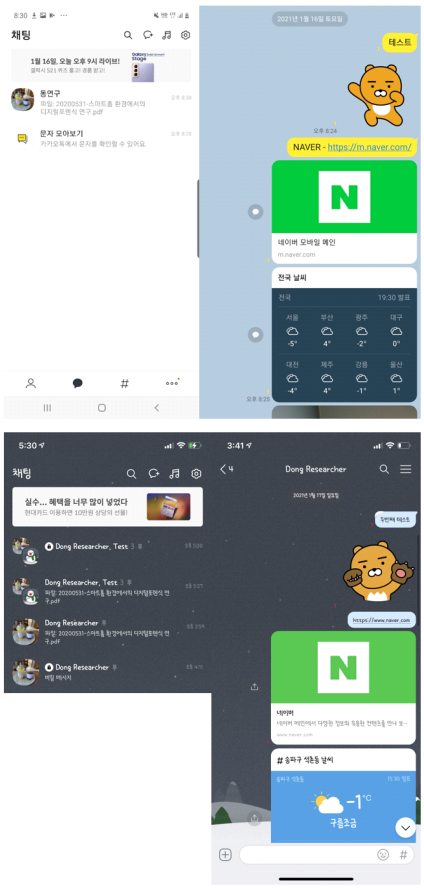


Fig. 2. Example of KakaoTalk Data Generation in Suspect's Android(above) & iOS(below) Device

이후, 대화방마다 하나의 묶음을 제외한 나머지 묶음에 대해 '모든 메시지를 모두에게서 삭제', '선택한 메시지를 모두에게서 삭제', '모든 메시지를 나에게만 삭제', '선택한 메시지를 나에게만 삭제' 등의 방법으로 메시지를 삭제하고, '메시지 전송 및 삭제 직후'와 '메시지 전송 및 삭제 이후 3일 경과' 시점에 유심을 다른 스마트폰에 탑재하여 확인 가능한 메시지 종류와 삭제한 메시지의 확보 가능 여부에 대한 실험을 진행하였다. 카카오톡의 개발사인 카카오는 최근 3일간의 메시지만 카카오톡의 클라우드 서버에 보관하고 있다고 설명하고 있어[14], 이를 확인하기 위하여 3일이 경과한 시점에 대한 실험도 진행하였다.

4.2 메시지 데이터 확보 절차

텔레그램 메시지 확보 절차는 다음과 같다.

① 텔레그램을 사용 중인 피의자 스마트폰에서 유심을 분리하여 수사관 스마트폰에 장착한다.
② 수사관 스마트폰에서 유심 다운로드 절차가 정상적으로 수행되는지 확인한다.
③ 수사관 스마트폰에 구글 플레이 스토어 또는 앱 스토어에서 텔레그램 앱을 다운로드하여 설치한다.
④ 텔레그램 실행 후 인증화면이 나타나면 유심에 등록된 휴대전화 번호를 입력하고, 텔레그램으로부터 5자리 숫자로 구성된 인증 코드를 문자 메시지로 전달받는다.
⑤ 인증 코드를 입력한 뒤 클라우드 서버로부터 메시지를 다운로드하여 확보한다.

카카오톡은 텔레그램의 방법과 대부분 동일하나 ③번 다음에 계정 및 비밀번호를 이용한 로그인 과정이 추가적으로 필요하고, ④번에서는 인증 코드가 6자리 숫자로 구성되어 있다는 점에서 차이를 보인다.

4.3 실험 결과 분석

4.3.1 텔레그램

4.3.1.1 메시지 전송과 삭제 직후 확보 여부

피의자 스마트폰에서 텔레그램의 각 대화방에 입력한 텍스트, 이모티콘, 링크, 사진, 영상, 파일, 위치, 연락처, 음성 녹음, 영상 녹화 메시지 중 삭제하지 않은 메시지는 수사관 스마트폰에서 모두 확인할 수 있었다. 하지만 삭제한 메시지와 비밀 대화방의 메시지는 확인할 수 없었다.

세부적으로 살펴보면 피의자 스마트폰에서 메시지를 전송한 직후 1:1 대화방에 전송한 활성 메시지는 수사관 스마트폰에서 모두 확인할 수 있었으나, '모든 메시지를 상대방과 나에게서 삭제', '모든 메시지를 나에게만 삭제', '선택한 메시지를 상대방과 나에게서 삭제', '선택한 메시지를 나에게만 삭제' 등 4가지 방법으로 삭제한 메시지는 모두 확인할 수 없었다. 단체 대화방에서도 삭제하지 않은 활성 메시지는 확인 가능하였으며, '모든 메시지를 모두에게서 삭제', '선택한 메시지를 모두에게서 삭제', '선택한 메시지를 나에게만 삭제' 등의 방법으로 삭제한 메시지는 확인이 불가하였다. 1:1 및 단체 비밀 대화방에서는 모든 활성 및 삭제 메시지를 확인할 수 없었다.

Table 4. Result of Telegram Experiment One: Messages Acquired from Android OS and iOS Device (Within a Day)

Chat Type	Message state & Deletion Type		Message Type									
			Text	Emoji	Link	Image	Video	File	Location	Contact	Record Audio	Record Video
1:1 Chat Room	Remaining Messages		O	O	O	O	O	O	O	O	O	O
	Delete Messages	All Messages (For the Other Person & Me)	X	X	X	X	X	X	X	X	X	X
		All Messages (For Me)	X	X	X	X	X	X	X	X	X	X
		Selected Messages (For the Other Person & Me)	X	X	X	X	X	X	X	X	X	X
		Selected Messages (For Me)	X	X	X	X	X	X	X	X	X	X
Group Chat Room	Remaining Messages		O	O	O	O	O	O	O	O	O	O
	Delete Messages	All Messages (For Everyone)	X	X	X	X	X	X	X	X	X	X
		Selected Messages (For Everyone)	X	X	X	X	X	X	X	X	X	X
		Selected Messages (For Me)	X	X	X	X	X	X	X	X	X	X
Secret Chat Room (1:1)	Remaining Messages		X	X	X	X	X	X	X	X	X	X
	Delete Messages	All Messages (For Everyone)	X	X	X	X	X	X	X	X	X	X
		Selected Messages (For Everyone)	X	X	X	X	X	X	X	X	X	X

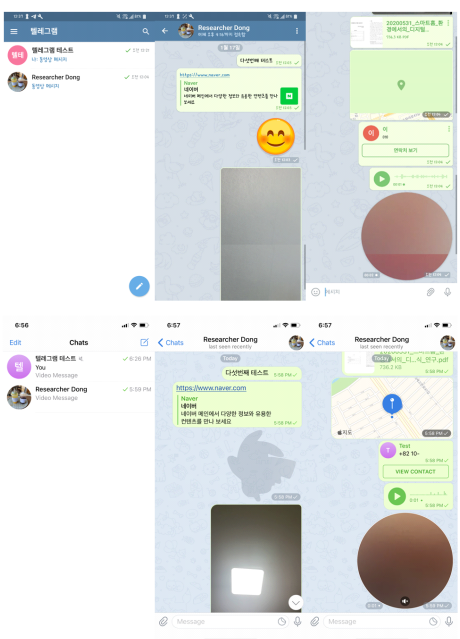


Fig. 3. Example of Telegram Data Acquisition using a USIM in Investigator's Android(above) & iOS(below) Device

실험 결과는 Table 4에 정리하였으며, 1:1 대화방에는 존재하나 단체 대화방과 비밀 대화방에 없는 삭제 기능은 표기하지 않았다.

4.3.1.2 메시지 전송과 삭제 3일 경과 후 확보 여부

피의자 스마트폰에서 메시지를 전송하고 삭제한 직후 수사관 스마트폰에서 확인할 수 있었던 1:1 대화방과 단체 대화방의 활성 메시지는 전송 및 삭제 이후 3일이 경과한 시점에서도 확인이 가능하였다.

텔레그램 메시지의 확보는 스마트폰의 운영체제 종류와 메시지 전송 및 삭제 이후 경과한 시일에 관계없이 동일한 결과를 보였다.

4.3.2 카카오톡

4.3.2.1 메시지 전송과 삭제 직후 확보 여부

피의자 스마트폰에서 카카오톡의 각 대화방에 입력한 텍스트, 이모티콘, 링크, 태그, 사진, 영상, 통화, 일정, 위치, 음성 메시지, 연락처, 파일 메시지 중 '선택한 메시지를 모두에게서 삭제' 방법으로 삭제

Table 5. Result of KakaoTalk Experiment One: Messages Acquired from Android OS and iOS Device (Within a Day)

Chat Type	Message State & Deletion Type		Message Type											
			Text	Emoji	Link	Tag	Image	Video	Call	Calendar	Location	Voice Note	Contact	File
1:1 Chat Room	Remaining Messages		O	O	O	O	O	O	O	O	O	O	O	O
	Delete Messages	All Messages (For Me)	O	O	O	O	O	O	O	O	O	O	O	O
		Selected Messages (For the Other Person & Me)	△	△	△	△	△	△	△	△	△	△	△	△
		Selected Messages (For Me)	O	O	O	O	O	O	O	O	O	O	O	O
Group Chat Room	Remaining Messages		O	O	O	O	O	O	O	O	O	O	O	O
	Delete Messages	All Messages (For Me)	O	O	O	O	O	O	O	O	O	O	O	O
		Selected Messages (For Everyone)	△	△	△	△	△	△	△	△	△	△	△	△
		Selected Messages (For Me)	O	O	O	O	O	O	O	O	O	O	O	O
Secret Chat Room (1:1 & Group)	Remaining Messages		X	X	X	-	X	X	-	-	-	-	-	-
	Delete Messages	All Messages (For Everyone)	X	X	X	-	X	X	-	-	-	-	-	-
		Selected Messages (For Everyone)	X	X	X	-	X	X	-	-	-	-	-	-

※ △ : Impossible to check content, but can check deletion
- : Unsupported message type

한 메시지와 비밀 대화방의 메시지를 제외한 모든 메시지는 수사관 스마트폰에서 확인할 수 있었다.

세부적으로 살펴보면 1:1 대화방에서 '모든 메시지를 나에게만 삭제', '선택한 메시지를 나에게만 삭제' 등의 방법으로 삭제한 메시지와 활성 메시지는 전송 및 삭제한 직후 수사관 스마트폰에서 모두 확인할 수 있었으나, '선택한 메시지를 상대방과 나에게서 삭제' 방법으로 삭제한 메시지는 삭제 여부만 확인이 가능하고 메시지 내용의 확인은 불가하였다. 단체 대화방에서도 '모든 메시지를 나에게만 삭제', '선택한 메시지를 나에게만 삭제' 등의 방법으로 삭제한 메시지 및 활성 메시지는 모두 확인할 수 있었으나, '선택한 메시지를 모두에게서 삭제' 방법으로 삭제한 메시지는 삭제 여부만 확인이 가능하고 그 내용의 확인은 불가하였다. 비밀 대화방에서는 모든 활성 및 삭제 메시지를 확인할 수 없었다.

실험 결과는 Table 5에 정리하였으며, 1:1 대화

Fig. 4. Example of Message Deletion

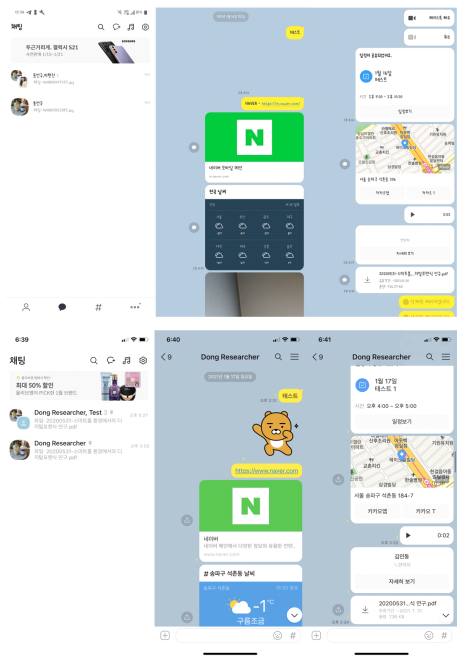


Fig. 5. Example of KakaoTalk Data Acquisition using a USIM in Investigator's Android OS(above) & iOS(below) Device

방과 단체 대화방에는 존재하나 비밀 대화방에 없는 삭제 기능은 표기하지 않았다.

4.3.2.2 메시지 전송과 삭제 3일 경과 후 확보 여부

피의자 스마트폰에서 메시지를 전송 및 삭제한 직후 수사관 스마트폰에서 확인할 수 있었던 1:1 대화방과 단체 대화방의 메시지는 전송 및 삭제 이후 3일이 경과한 시점에서 모두 확인이 불가하였다.

카카오톡 메시지의 확보는 텔레그램과 같이 운영체제 종류와 관계없이 동일한 결과를 보였다.

4.4 소결

텔레그램은 피의자 스마트폰에서 메시지 전송 및 삭제 직후, 수사관 스마트폰에서는 1:1 대화방 및 단체 대화방의 활성 메시지만 확보할 수 있었으며, 모든 삭제 메시지 및 비밀 대화방 내 메시지는 확인할 수 없었다. 메시지 전송 이후 3일이 경과한 시점에도 1:1 대화방 및 단체 대화방의 활성 메시지는 확인이 가능하였다.

카카오톡은 피의자 스마트폰에서 메시지 전송 및 삭제 직후, 수사관 스마트폰에서 1:1 대화방 및 단체 대화방의 '선택한 메시지를 모두에게서 삭제' 방법으로 삭제한 메시지와 비밀 대화방 내 메시지를 제외한 모든 메시지를 확보할 수 있었다. 다만, '선택한 메시지를 모두에게서 삭제' 방법으로 선택 삭제한 메시지의 경우 메시지 내용의 확인은 불가하였으나, 해당 메시지의 삭제 여부는 확인할 수 있었다. 하지만 전송 및 삭제 이후 3일이 경과한 경우에는 활성 메시지를 포함한 모든 메시지를 확인할 수 없었다.

두 메신저는 공통적으로 운영체제의 영향을 받지 않고 동일한 실험 결과를 보였으며, 비밀 대화방의 메시지는 클라우드 서버에 저장되지 않기 때문[15][16]에 시간 경과와 관계없이 확보가 불가하였다.

다만, 텔레그램의 경우 메시지 삭제 직후 삭제한 메시지를 확인할 수 없었으나 카카오톡은 삭제 직후에도 '선택한 메시지를 모두에게서 삭제' 방법으로 삭제한 메시지를 제외한 모든 메시지를 확인할 수 있었다. '선택한 메시지를 모두에게서 삭제' 방법으로 삭제한 경우 메시지의 내용은 확인이 불가하였으나, 해당 메시지의 삭제 여부는 확인할 수는 있었다. 또한, 텔레그램에서는 전송 이후 3일이 경과한 메시지의 확보가 가능하였지만, 카카오톡은 3일 경과 이후 모든 메시지의 확보가 불가하였다는 점에서 차이가 있었다.

V. 유심 이용 메신저 데이터 압수·수색 허용성

5.1 유심 이용 압수·수색의 특징

유심 이용 압수·수색은 원격 압수·수색과 역외 압수·수색과 비슷한 점이 많다. 원격 압수·수색은 최초 압수·수색 장소의 수색 대상 컴퓨터를 이용하여 네트워크로 연결된 다른 컴퓨터에 저장되어 있는 범죄혐의와 관련된 디지털증거를 수색하여 압수하는 방법을 말한다[17]. 역외 압수·수색은 원격 압수·수색이 타국까지 확장하는 집행하는 방법을 의미한다[18][19][20].

이렇게 볼 때 유심 이용 압수·수색은 집행 방법 측면에서 원격 압수·수색과 유사하지만, 텔레그램 등 타국 클라우드에 접속한다는 측면에서는 역외 압수·수색의 성격 또한 가지고 있다. 즉, 압수·수색 장소에 임장하여 원격지에 있는 국내 클라우드에 접속하여 압수하고, 피처분자에게 영장제시, 참여권 보장, 압수목록(수색증명서) 교부 등의 절차를 수행한다는 측면에서 원격 압수·수색과 유사하다. 단, 원격 압수·수색은 압수·수색 장소에 있는 컴퓨터·서버를 이용하여 집행하지만, 유심 이용 압수·수색은 수사관이 별도로 준비한 스마트폰을 이용하여 집행한다는 측면에서 차이가 있다. 수사관이 인증 코드를 입력한 후에 해외 클라우드 서버를 대상으로 집행하고, 압수·수색 종료 이후에 추가적인 집행이 가능하다는 문제점을 안고 있다는 측면에서 역외 압수·수색과 유사하다.

5.2 압수·수색 방법으로써 허용 여부

5.2.1 법적 쟁점

유심 이용 압수·수색이 형사소송법에서 예정하고 있는 압수·수색으로 허용할 수 있는지에 대한 논란이 있다. 수사 실무에서는 인터넷과 네트워크가 발전하면서 원격 압수·수색과 역외 압수·수색이 허용되고 있고 대법원에서도 이를 인정하고 있지만, 명문의 규정이 없다는 측면에서 부정하는 견해도 있을 수 있다. 따라서 형사소송법에서 규정하고 있는 영장집행에 대한 사전통지, 영장제시, 참여권 보장, 압수목록(수색증명서) 교부 등의 절차를 준수하는지, 수사관

스마트폰에 메신저 접속을 위해 인증 코드를 수신하는 행위가 영장의 집행범위에 포함되는지에 대한 검토가 필요하다. 나아가 해외 클라우드 서버에 있는 메시지를 압수하는 행위가 관할권을 침해하는지도 검토해야 한다.

5.2.2 압수・수색 절차 준수 여부

유심 이용 압수·수색은 수사관이 압수·수색 현장에 임장하여 피처분자에게 영장을 제시하고(형사소송법 제219조, 제118조), 유심을 압수한 다음 현장에서 클라우드 서버에 접속하여 메시지를 다운로드한다. 피처분자에 대해 영장집행 일시·장소를 사전에 통지할 수 있고(제122조), 피처분자의 참여권 보장도 가능하다(제121조 내지 제123조). 현장이나 수사기관의 사무실에서 집행을 종료하면 압수목록(제129조)이나 수색증명서(제128조)도 교부할 수 있어 형사소송법상 압수·수색 절차를 준수할 수 있다. 유심 자체가 압수대상이기 때문에 수사현장에서 집행이 어려우면 수사기관 사무실에서 집행할 수도 있다. 다만, 수사관 스마트폰에 인증 코드를 입력할 경우 영장에 기재된 사람, 기간, 내용과 관계없는 메시지가 모두 다운로드되는 문제가 있다. 이 중에서 압수·수색영장에 기재된 내용을 벗어나는 메시지를 압수·수색하는 경우에는 적법한 압수·수색 절차로 인정할 수 없을 것이다.

5.2.3 메신저 인증 코드 수신의 적법성

수사관이 클라우드 서버로부터 5~6개의 숫자로 구성된 인증 코드를 수신하는 행위가 영장의 집행대상에 포함되는지 쟁점이 될 수 있다. 인증 코드 수신은 수사관 스마트폰과 클라우드 서버 간 기계적 통신행위로 피의자와 그 상대방의 대화내용으로 볼 수 없어 전기통신감청이 아닌 형사소송법상 압수·수색에 필요한 처분으로 해석해야 한다(제120조 제1항). 실제 계정과 비밀번호를 확보하여 로그인하는 행위[21]나 인터넷 계정의 비밀번호 해제, 데이터·파일의 복호화하는 행위도 필요한 처분의 대상으로 해석하고 있다[22].

5.2.4 관할권 침해 여부

해외에 있는 클라우드 서버에 접속하여 메시지를 압수하는 경우 관할권 침해에 대한 논란이 발생할 수 있다. 전통적인 관할권 개념에서는 관할권 침해에 대한 논란이 충분히 수긍이 된다. 하지만 인터넷 환경에서는 관할권의 개념을 다른 각도에서 해석할 필요가 있다. 수사기관이 물리적으로 타국의 관할권을 침해하지 않은 것은 분명하다. 수사관이 압수·수색영장을 집행한 대상은 텔레그램 서버가 아니라 정보주체인 피의자가 소유·소지하는 메시지로 관할권을 침해했다고 보기 어렵다[23]. 대법원도 2017도9747 판결에서 해외 클라우드 서버에 소재하는 이메일 내용에 대해서 정보주체인 피의자가 소유·소지하는 디지털증거로 판단하여 관할권 침해가 아니라고 보았다. 나아가 피의자가 다른 장치로 접속하여 메시지를 삭제할 수 있는 상황에서 장시간 소요되는 형사사법공조 절차에만 의존하여 수사를 할 수 없는 현실적인 이유도 인정해야 할 것이다. 만약 관할권 침해라고 한다면 수사기관이 타국에 있는 상대방과 국제전화를 하여 진술을 청취·녹음하는 행위, 인터넷을 이용하여 타국의 데이터를 열람하는 행위까지 관할권을 침해했다는 결과를 가져오게 된다[24].

5.3 전기통신 감청 해당 여부

5.3.1 법적 쟁점

유심 이용 압수·수색이 전기통신감청 대상이 될 수 있는지에 대해 검토가 필요하다. 통신비밀보호법에서 감청은 “전기통신에 대하여 당사자의 동의없이 전자장치・기계장치 등을 사용하여 통신의 음향・문언・부호・영상을 청취・공독하여 그 내용을 지득 또는 채록하거나 전기통신의 송・수신을 방해하는 것”으로 정의하고 있다(제2조 제7호). 이러한 관점에서 수사기관이 클라우드 서버에 있는 메시지를 다운로드하여 압수·수색하는 행위와 압수·수색이 종결된 이후에도 계속하여 메시지를 수신하는 행위가 압수·수색 또는 전기통신감청 대상인지를 살펴볼 필요가 있다.

5.3.2 클라우드 서버 내 메시지 실시간 수신행위

수사관이 인증 코드를 입력하자마자 다운로드한 메시지는 이미 클라우드 서버에 송·수신이 완료된 메시지로 압수·수색 대상으로 봐야 한다. 이때 메시지는 피의자와 그 상대방 간의 통신내용이 아니라 클라우드 서버에 저장된 통신내용이기 때문에 압수·수색

대상으로 봐야 한다. 대법원도 2012도4644 판결에서 감청에 대해 "대상이 되는 전기통신의 송·수신과 동시에 이루어지는 경우만을 의미하고, 이미 수신이 완료된 전기통신의 내용을 지득하는 등의 행위는 포함되지 않는다"고 판시하였다.

5.3.3 압수·수색 집행 후 메시지 실시간 수신행위

수사관이 유심을 이용하여 압수·수색을 종료한 이후에도 계속해서 실시간 수신되는 메시지는 전기통신 감청 대상으로 봐야 한다. 피의자와 그 상대방 간의 실시간 대화내용으로 명백한 전기통신감청 대상이다. 따라서 수사관이 압수·수색 영장을 집행한 이후에 계속하여 메시지를 실시간으로 수집하는 행위는 위법한 수사절차가 된다.

5.4 적법성 확보 및 통제방안

유심 이용 압수·수색은 수사기관이 일반적으로 사용하였던 방법이 아니기 때문에 논란이 발생할 수 있다. 따라서 이러한 논란을 최소화하기 위하여, 압수·수색영장에 압수물건, 수색할 장소, 압수·수색 방법을 보다 구체적으로 기재하여 법원의 심사를 받는 것이 필요하다. 또한, 수사관이 메시지를 다운로드할 때에는 영장범위에서 벗어나는 기간, 사람, 내용에 대해서는 압수·수색 대상에서 제외하여야 한다. 나아가 수사관이 메시지를 다운로드한 후 유심을 이용한 추가적인 메시지 다운로드를 통제하는 절차도 마련해야 할 것이다.

VI. 결 론

본 논문은 유심을 이용하여 피의자의 텔레그램·카카오톡 메신저의 데이터를 확보하는 기술에 대한 실험과 집행 방법의 허용성에 대해서 살펴보았다.

실험 결과, 텔레그램은 피의자 스마트폰에서 메시지를 전송하고 일부를 삭제한 직후 수사관 스마트폰에서 1:1 대화방 및 단체 대화방에서 활성 메시지를 확보할 수 있었으나, 모든 삭제 메시지와 비밀 대화방의 메시지는 확보할 수 없었다. 하지만 메시지 전송 이후 3일이 경과한 시점에서도 1:1 대화방 및 단체 대화방에서는 활성 메시지를 여전히 확보할 수 있었다. 카카오톡은 피의자 스마트폰에서 메시지 전송 및 삭제 직후, 수사관 스마트폰에서 1:1 대화방과 단체 대화방의 '선택한 메시지를 모두에게서 삭제' 방법으로 삭제한 메시지 및 비밀 대화방 내 메시지를 제외한 모든 메시지를 확보할 수 있었다. '선택한 메시지를 모두에게서 삭제' 방법으로 삭제한 메시지의 경우 메시지 내용은 확인할 수 없지만, 삭제 시 대체되는 삭제 알림 문구를 통해 해당 메시지의 삭제 여부를 확인할 수 있었다. 하지만 메시지 전송 및 삭제 이후 3일이 경과한 경우에는 모든 메시지를 확인할 수 없었다. 두 메신저는 모두 운영체제와 관계없이 각각 동일한 결과를 나타냈고, 비밀 대화방의 메시지는 로컬 방식으로만 저장하기 때문에, 메시지 전송 및 삭제 이후 경과 일시와 관계없이 수사관 스마트폰에서 확보할 수 없었다. 나아가 텔레그램은 메시지 삭제 직후 삭제한 메시지를 확인할 수 없었으나 카카오톡은 삭제 직후에도 '선택한 메시지를 모두에게서 삭제' 방법으로 삭제한 메시지를 제외한 모든 메시지를 확인할 수 있다는 차이가 있었다. 또한, 텔레그램은 전송 이후 3일이 경과한 메시지를 확보할 수 있었지만, 카카오톡은 3일 경과 이후에는 모든 메시지를 확보할 수 없었다. 해당 실험은 피의자의 스마트폰을 통하지 않고 유심만을 이용하여 메시지를 확보할 수 있음을 보여주었으며, 로컬/클라우드 방식으로 메신저 데이터를 저장하는 다른 메신저에서도 동일한 방법과 절차를 통해 활성 및 삭제 메시지를 확보할 수 있을 것으로 예상한다.

이와 같은 유심 이용 압수·수색은 원격 압수·수색과 유사하여 영장집행 사전통보, 영장제시, 참여권 보장, 압수목록(수색증명서) 교부 등의 절차를 모두 준수할 수 있다. 클라우드 서버로부터 인증 코드를 수신하는 행위는 형사소송법상 압수·수색에 필요한 처분의 대상으로 해석할 수 있다(제120조 제1항). 관할권 침해가 논란이 될 수 있지만, 수사기관이 물리적으로 관할권을 침해하지 않고, 영장집행이 텔레그램 서버가 아닌 정보주체인 피의자가 소유·소지하는 메시지라고 볼 수 있어 관할권을 침해했다고 보기 어렵다. 대법원 역시 역외 압수·수색을 허용한 바 있다. 나아가 인증 코드 입력 후에 다운로드한 메시지는 이미 송·수신이 완료된 데이터로 압수·수색 대상에 해당하는 것이 분명하다. 다만, 이후에도 계속하여 수신하는 데이터는 전기통신감청 대상으로 봐야 하기 때문에 영장의 집행범위를 벗어난다.

이렇게 볼 때 유심 이용 압수·수색은 적법한 강제처분으로 볼 수 있다. 다만, 적법성 논란을 최소화하기 위해 영장에 압수물건, 수색할 장소, 압수·수색

방법을 기재하여 법원의 심사를 받고, 메시지를 다운로드할 때 영장범위를 벗어난 기간, 사람, 내용에 관한 데이터는 제외하여야 한다. 나아가 집행완료 이후 유심을 이용하여 메시지를 다운로드하는 행위는 엄격하게 통제해야 할 것이다.

References

[1] Ministry of Science and ICT, "Results Of Survey On Overdependence Of Smartphones In 2019", https://www.msit.go.kr/SYNAP/skin/doc.html?fn=47bc67acceecf733a23a9d2354357691&rs=/SYNAP/sn3hcv/result/ (accessed: Nov. 7, 2020)

[2] Kwangju Ilbo, "From National Messenger to Comprehensive Platform", http://www.kwangju.co.kr/article.php?aid=1583247600690617166 (accessed: Feb. 11, 2021)

[3] IT Newspaper, "Focus on digital forensics, 'a 21st century Sherlock Holmes'", https://www.koit.co.kr/news/articleView.html?idxno=79279 (accessed: Feb. 12, 2021)

[4] Yeong-Woong Kim, Gi-Bum Kim, Ji-Hun Son, Yu-Ri Son and Sung-Hyun Park, "Control Measures for Smartphone Forensics Using Fingerprint Information," Journal of Korean Public Police and Security Studies, 16(1), pp. 73-92, May 2019.

[5] Youngjin Song, "Compelled Decryption and the Privilege Against Self-Incrimination: Recent Court Decisions in the United States and Legislation of the United Kingdom," Korean Criminological Review, 31(1), pp. 159-190, Mar. 2020.

[6] Jong-cheol Yoon and Yong-suk Park, "Forensic Analysis of KakaoTalk Messenger on Android Environment," Journal of the Korea Institute Of Information and Communication Engineering (JKIICE), 20(1), pp. 72-80, Jan. 2016.

[7] Tae-jin Hwang, Dong-ho Won and Young-sook Lee, "A study on the Comparison Analysis for Messenger Evidence Using Mobile Forensics," Journal of convergence security, 18(2), pp. 25-32, Jun. 2018.

[8] Min-hyung Lee and Sang-jin Lee, "A Study on the User Data Acquisition Method of Cloud-Based Messenger Using Acquisition of Authentication Information," Journal of Digital Forensics, 13(4), pp. 331-341, Dec. 2019.

[9] Gi-hoon Nam, Seong-hyeon Gong, Byoung-jin Seok and Chang-hoon Lee, "Study on Remote Data Acquisition Methods Using OAuth Protocol of Android Operating System," Journal of The Korea Institute of Information Security and Cryptology (JKIISC), 28(1), pp. 111-122, Feb. 2018.

[10] Jong-won Choi and Jeong-hyun Yi, "Analysis on Personal Information Leakage of Google Account App on Android," Journal of Digital Forensics, 8(2), pp. 65-81, Dec. 2014.

[11] Dong-A Ilbo, "Prosecutors to restore Telegram through USIM...Didn't 'the brilliant move' work?", https://www.donga.com/news/Politics/article/all/20200730/102234712/1 (accessed: Nov. 7, 2020)

[12] D. G. Koshy and S. N. Rao, "Evolution of SIM Cards - What's Next?," 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 1963-1967, Sep. 2018.

[13] Nuril Anwar, Imam Riadi and Ahmad Luthfi, "Forensic SIM Card Cloning Using Authentication Algorithm," Int. J. of Electronics and Information Engineering, vol. 4, no. 2, pp. 71-81, July 2016.

[14] Kakao Customer Service, "For how long

are the messages stored on the server?", https://cs.kakao.com/helps?articleId=1073188987&service=8&category=24&device=1013&locale=ko (accessed: Jan. 19, 2021)
〔15〕 Telegram FAQ, "How are secret chats different?", https://www.telegram.org/faq#1498786448 (accessed: Jan. 17, 2021)
〔16〕 Kakao Customer Service, "What is a Secret Chat?", https://cs.kakao.com/helps?service=8&category=24&locale=ko&device=1013&articleId=1073189010 (accessed: Jan. 17, 2021)
〔17〕 Dae-Yong Jeong, Gi-bum Kim and Sangjin Lee, "Issues and Legislative Approach aboutthe Long-Distance Search and Seizure via the Searching Computer Located Remotely," Korean Lawyers Association Journal (KLAJ), 65(3), pp. 40-84, Apr. 2016.
〔18〕 Seung-deuk Cheun and Gu-min Kang, "A Study of the Search and Seizure Procedure for Remote Servers through the Practical Affairs," Theories and Practices of Criminal Procedure (TPCP), 11(1), pp. 57-90, June 2019.
〔19〕 Soyeon Jeong, "Study on Extra-territorial Seizure of Digital Evidence from Legal Perspective," Journal of Digital Forensics, 11(1), pp. 61-71, June 2017.
〔20〕 Dae-Young Jeong, Gi-bum Kim, Hun-Young Kwon and Sangjin Lee, "Issues and Legislative Approach about the Extra-territorial Search and Seizure of Digital Evidence - Focucing on Remote Search and Seizure to Foreign Sever via Accessing Account -," Korean Lawyers Association Journal (KLAJ), 65(9), pp. 133-182, Feb. 2016.
〔21〕 Sookyeon Lee, "Handling and Admissibility of Digital Evidence in Criminal Procedure," Ph.D. Thesis, Korea University, Feb. 2011.
〔22〕 Seung-un Lee, Cyber Law & Case, PUBPLE, p.394, 2019.
〔23〕 Hyun-wook Jeon et al, "A Study on the Improvement of Law for the Effective Investigation of Cyber Crime," National Research Council for Economics, Humanities and Social Sciences, pp. 114-115, Dec. 2015.
〔24〕 Kwanhee Lee and Sangjin Lee, "A Study on Permissibility and Conditions of Extra-territorial Data Search," Journal of Digital Forensics, 14(2), pp. 169-177, June 2020.

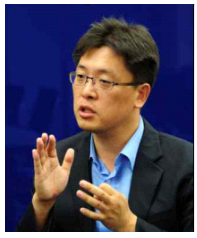
〈저자소개〉

김 민 동 (Min-Dong Kim) 정회원
2021년 2월: 성균관대학교 과학수사학과 석사수료
〈관심분야〉 디지털포렌식, 정보보호

이 현 진 (Hyeon-Jin Lee) 정회원
2018년 2월: 목포대학교 정보보호학과 졸업
2019년 3월~현재: 성균관대학교 과학수사학과 석사과정
2016년 6월~현재: 한국인터넷진흥원(KISA) 사이버침해대응본부
〈관심분야〉 정보보호, 디지털포렌식, 취약점분석 등

이 성 진 (Sung Jin Lee) 종신회원
2004년 2월: 단국대학교 컴퓨터공학과 졸업
2006년 2월: 서울대학교 전기컴퓨터공학부 석사
2015년 8월: 연세대학교 법학 석사
2018년 2월: Indiana University Kelley School of Business MBA
2021년 2월: 성균관대학교 과학수사학과 박사수료
2011년 1월~현재: 금융감독원 자본시장특별사법경찰 선임검사역
〈관심분야〉 디지털포렌식, 전자금융, IT검사, 정보보호 등

이 연 주 (Yeon-Ju Lee) 정회원
2003년 8월: 성균관대학교 법학과 졸업
2007년 2월: 성균관대학교 행정학 석사
2021년 2월: 성균관대학교 과학수사학과 박사수료
〈관심분야〉 디지털포렌식, 범죄수사, 형사정책



김 기 범 (Gi-Bum Kim) 종신회원
1997년 2월: 경찰대학 행정학과 졸업
2009년 2월: 고려대학교 정보보호대학원 석사
2017년 2월: 고려대학교 정보보호대학원 박사
2014년 2월~2020년 2월: 경찰대학 경찰학과 교수/국제사이버범죄연구센터장
2020년 3월~현재: 성균관대학교 과학수사학과(디지털포렌식) 부교수
〈관심분야〉 디지털포렌식, 사이버범죄, 범죄수사, 과학기술치안, 국제개발협력

`