ISSN : 1976-5304
https://kdfs.jams.or.kr

인증정보 획득을 이용한 클라우드 메신저의 사용자 데이터 획득 기법에 관한 연구

이 민 형*, 이 상 진**
서울지방경찰청 (경사)*, 고려대학교 정보보호대학원 (교수)**

A Study on the User Data Acquisition Method of Cloud-Based Messenger Using Acquisition of Authentication Information

Min-Hyung Lee*, Sang-Jin Lee**
Seoul Metropolitan Police Agency (Assistant Inspector)*
Graduate School of Information Security, Korea University (Professor)**

요 약

메신저 애플리케이션이 기존의 문자메시지를 대체하면서, 메신저의 사용자 데이터가 증거로 채택되는 경우가 많아지고 있다. 하지만 기기 내부의 메신저 저장소를 획득하여 분석하는 기존의 포렌식 방법을 사용하려면, 일부 기기의 경우 잠금을 해제해야만 한다. 그러나 수사관이 메신저의 사용자 인증정보를 획득할 수 있다면, 기기가 잠겨 있어도 클라우드 메신저의 사용자 데이터 획득이 가능할 수 있다. 수사관은 소유자의 스마트폰에서 추출한 SIM(subscriber identification module) 카드와 소유자의 인적 사항을 통해 메신저의 인증정보를 획득할 수 있다. 본 논문에서는 구글 플레이스토어를 통해 배포되고 있는바일 메신저들을 사용자 데이터 보관 방식에 따라 로컬 메신저와 클라우드 메신저로 구분하고, 인증정보를 획득하여 클라우드 메신저의 사용자 데이터를 획득하는 절차와 분석 방법을 제안하고자 한다.

주제어 : 모바일 포렌식, 클라우드 메신저, 인증우회

ABSTRACT

As messenger applications replace existing text messages, user data of messengers are often taken as evidence. However, to use the traditional forensic method of acquiring and analyzing the messenger store inside the device, some devices need to be unlocked. However, if the investigator can obtain the user authentication information of the messenger, it may be possible to obtain the user data of the cloud messenger even if the device is locked. The investigator can obtain the authentication information of the messenger through the SIM(subscriber identification module) card extracted from the smartphone of the victim and the personal information of the victim. In this paper, I would like to propose a procedure and analysis method to divide mobile messengers distributed through Google Play Store into local and cloud messengers according to the method of storing user data, and acquire authentication information to obtain user data from cloud messengers.

Key Words : Mobile Forensic, Cloud messenger, Authentication bypass

Ⅰ. 서 론

스마트폰 메신저 애플리케이션이 기존의 문자메시지를 대체하여 폭넓게 이용되면서, 메신저 데이터가 증거로 채택되는 경우가 많아지고 있다. 이로 인해 메신저 대화 내용이나 첨부파일 등을 추출하는 기법이 많이 연구되고 있다.

기존의 메신저 분석 기법은 스마트폰 내부에 존재하는 데이터베이스를 획득한 뒤 이를 가독성 있는 데이터로 변환하는 방식이 널리 사용되고 있다[1-3]. 기존의 분석 방법들은 대부분 메신저 데이터베이스 획득을 전제로 한다.

스마트폰 내부의 메신저 데이터베이스를 획득하기 위해 Android 기기는 루팅 하거나 디버깅 모드로 라이브 데이터를 획득하는 방법을 사용할 수 있고[4], iOS 운영체제 기반의 아이폰은 itunes backup을 이용하여 자료를 수집할 수 있다[5-6]. 이런 방법을 사용하면 데이터를 획득하여 선별하기 때문에 탐색과정에서 기기 내부의 데이터가 손상될 위험이 적고, 삭제된 데이터의 복원[7]과 데이터 수집 재현이 가능하다는 장점이 있다. 하지만 기기 자체가 잠겨있으면 저장소 획득이 어

▪ Received 31 October 2019, Revised 18 November 2019, Accepted 17 December 2019
▪ 제1저자(First Author) : Min-Hyung Lee (Email : mhspecial@empal.com)
▪ 교신저자(Corresponding Author) : Sang-Jin Lee (Email : sangjin@korea.ac.kr)

렵고, 분석 결과를 바로 확인 할 수 없다는 단점이 있다. 또한 기기에 데이터를 저장하지 않고 클라우드 서버에만 데이터를 저장하는 일부 애플리케이션의 경우 기존의 포렌식 방법을 적용할 수 없다.

기존의 포렌식 방법 대신 스마트폰 화면에서 대화 내용을 확인한다면 삭제된 데이터의 복원은 불가능하지만, 신속한 내용 확인이 가능하다. 하지만 스마트폰을 직접 조작하여 확인하기 위해서는 기기가 정상 작동해야 하고, 잠금 또한 해제되어 있어야 한다. 즉, 소유자수자가 협조하지 않거나, 기기가 유실물이거나, 조작이 불가능할 정도로 고장 난 상황에서는 적용할 수 없다.

2016년 FBI에서 테러 용의자가 사용한 아이폰 5C의 잠금을 해제하지 못해 애플과 충돌했던 사건은 전 세계적으로 화제가 되었다[8]. 결국 막대한 비용을 지불하고 셀러브라이트사의 도움으로 잠금을 해제하긴 했지만, 작동 불능한 스마트폰은 수사에 큰 걸림돌이 된다는 것을 보여주는 사례이다.

이와 같은 상황이라도 수사관이 메신저의 인증정보를 확보하면 별도의 기기로 접속하여 내용을 확인할 수 있는 경우가 있다. 메신저의 사용자 식별 정보는 일반적으로 휴대전화 번호와 이메일 형식으로 되어있고, 메신저 종류에 따라 비밀번호를 요구하는 경우도 있다. 본 연구는 잠겨있는 스마트폰에서 소유자의 협조 없이 클라우드 메신저의 인증정보를 확보하는 방법과 확보한 인증정보를 이용할 수 있는 범위에 대해 알아본다.

Ⅱ.모바일 메신저 종류 및 사용자 인증방법

2.1. 모바일 메신저의 종류와 데이터 저장소

현재 구글의 플레이스토어나 애플의 앱스토어에는 수많은 종류의 메신저 애플리케이션이 존재한다. 이 중 왓츠앱, 카카오톡처럼 오랜 기간 동안 대중에게 사랑받은 애플리케이션이 있는 반면, 출시 후 얼마 되지 않아 사라진 애플리케이션도 많이 있다. 또한 메신저가 아니지만 메신저로 취급되는 애플리케이션도 다수 존재한다. 예를 들어 인스타그램의 경우 소셜미디어 애플리케이션으로 분류되지만 'Direct Message'라는 메시징 기능을 제공하므로 메신저로 볼 수 있다. [표 1]은 2019년 10월 기준 구글 플레이스토어에서 1000만 다운로드 이상 달성한 애플리케이션 중 메신저 기능을 제공하는 애플리케이션의 목록이다.

표 1. 메신저 기능을 포함한 애플리케이션

애플리케이션 이름	분류	다운로드	애플리케이션 이름	분류	다운로드
WhatsApp	메신저	10억 이상	Telegram	메신저	1억 이상
Facebook Messenger	메신저	10억 이상	TikTok	영상공유	1억 이상
HangOut	메신저	10억 이상	Wechat	메신저	1억 이상
Instagram	소셜미디어	10억 이상	Zalo	메신저	1억 이상
Skype	전화/메신저	10억 이상	Discord	게이밍 메신저	5000만 이상
SnapChat	메신저	10억 이상	Zello	무전기	5000만 이상
imo	메신저	5억 이상	Between	폐쇄형 메신저	1000만 이상
Line	메신저	5억 이상	ICQ	메신저	1000만 이상
Viber	전화/메신저	5억 이상	Nateon	메신저	1000만 이상
Azar	영상공유/만남	1억 이상	QQ	소셜미디어	1000만 이상
KakaoTalk	메신저	1억 이상	Signal	메신저	1000만 이상
KikMessenger	메신저	1억 이상	Soma	메신저	1000만 이상
Tango	영상공유	1억 이상	slack	비즈니스	1000만 이상

메신저 애플리케이션은 사용자 데이터 보관 방식에 따라 로컬 방식과 클라우드 방식으로 나눌 수 있다. 로컬 방식은 사용자의 데이터가 사용 중인 기기 내부 저장소에만 존재한다. 왓츠앱이 대표적인 로컬 방식 메신저이다. 로컬 방식은 상대적으로 서버가 부담해야 하는 데이터 용량이 작다는 장점이 있지만, 사용자 데이터가 자동으로 서버에 동기화되지 않는다는 단점이 있다. 로컬 방식 메신저는 대화 내용이 기기별로 종속적이기 때문에, 데이터 손실 없이 로그인 기기를 변경하려면 별도의 데이터 백업 기능을 통해 대화 내용을 이전해야 한다.

반면, 클라우드 방식은 데이터가 기기 내부 저장소와 클라우드 서버에 모두 저장되는 방식이다. 이 방식에서는 기기가 메신저 서버와 연결되면 동기화가 일어난다. 페이스북 메신저가 대표적인 클라우드 방식의 애플리케이션인데, 이와 같은 유형의 애플리케이션들은 클라우드 서버에 모든 사용자 데이터가 동기화된다. 클라우드 방식에서는 로컬의 데이터가 클라우드에 모두 저장되지만, 애플리케이션마다 데이터를 관리하는 방식이 다르기 때문에 클라우드의 데이터가 로컬에 모두 저장된다고 단정 지을 수 없다. 인터넷에 연결된 환경이라면, 어떤 단말기를 사용하든지 간에 대화 내용을 동일하게 볼 수 있으며, 텔레그램과 같은 일부 애플리케이션은 멀티 로그인 기능도 제공한다 [1].

1) 텔레그램의 특징 (https://en.wikipedia.org/wiki/Telegram_(software))

〔표 2〕는 애플리케이션 별 사용자 데이터를 보관하는 위치를 나타낸다.

표 2. 애플리케이션 버전 별 데이터 저장소 및 인증 수단

애플리케이션 이름	버전	저장소	애플리케이션 이름	버전	저장소
WhatsApp	2.19.100.	로컬	Telegram	5.12.	로컬/클라우드
Facebook Messenger	236.0.	로컬/클라우드	TikTok	8.3.0.	로컬/클라우드
HangOut	26.0.1	로컬/클라우드	Wechat	7.0.8.	로컬
Instagram	114.0.	로컬/클라우드	Zalo	19.08.03	로컬/클라우드
Skype	8.52.	로컬/클라우드	Discord	3.1.5	로컬/클라우드
SnapChat	10.67.5.73	로컬/클라우드	Zello	4.74.	로컬
imo	2019.10.1.	로컬/클라우드	Between	5.4.1	로컬/클라우드
Line	9.16.6	로컬	ICQ	8.1.1	로컬/클라우드
Viber	11.6.	로컬	Nateon	3.12.1	로컬/클라우드
Azar	1.38.4	로컬/클라우드	QQ	8.1.5	로컬
KakaoTalk[2]	8.5.7	로컬/클라우드	Signal	2.24.3	로컬
KikMessenger	15.15.0	로컬	Soma	2.0.19	로컬
Tango	6.12.238092	로컬/클라우드	slack	19.10.10.	로컬/클라우드

로컬 메신저는 사용자 데이터 백업을 지원하지 않기 때문에 사용자가 백업을 위해 별도의 도구를 사용해야 한다. 안드로이드 사용자는 Google Drive Backup을 사용할 수 있고, iOS 사용자는 iCloud를 사용하여 데이터 백업을 할 수 있다[3]. 백업 도구를 사용하지 않은 상태에서 기기를 변경했다면, 과거 기기의 사용자 데이터는 새로운 기기에 동기화되지 않는다. 결국 수사관은 과거 사용했던 기기의 사용자 데이터를 확보하기 위해 과거의 기기를 추가로 확보해야 한다.

클라우드 메신저는 모든 사용자 데이터가 클라우드 서버에 존재한다. 하지만 사용자가 기기를 변경해서 설치한 직후에는 최근의 데이터만 동기화되어 저장된다. 이와 같은 방식으로 동기화되는 이유는 모바일 데이터 사용에 따른 요금 문제로 추정된다. 만약 사용자가 애플리케이션을 설치하고 최초 구동한 시점에 과거의 모든 데이터를 기기에 동기화한다면, 데이터 통신이 과도하게 발생되기 때문이다. 그래서 애플리케이션을 설치한 직후엔 기기의 저장소에 최근의 데이터만 저장되는데, 이 시점에 기존의 포렌식 방법으로 증거를 수집한다면 과거의 대화 내용과 첨부파일은 수집되지 않는다.

해당 내용을 검증하기 위해 LG-F600S 스마트폰에 Telegram(5.12)을 설치하고, 데이터가 많은 사용자의 계정으로 로그인한 직후, 한컴GMD의 MD-NEXT(1.87)와 KDF Mobile 3.0으로 분석한 결과 〔그림 1〕과 같은 결과를 확인할 수 있었다. 이때 연락처는 모두 기기와 동기화 되어있었지만, 대화내용은 각 대화방 별 가장 최근의 내용 1개와 인증 메시지만 동기화되어있었다. 이어서 스마트폰을 직접 조작하여 각각의 대화방에 들어가 과거의 데이터를 스크롤 하고 동일한 방법으로 데이터를 분석하자, 〔그림 2〕와 같이 추가로 스크롤 한 데이터가 동기화된 것을 확인할 수 있었다.

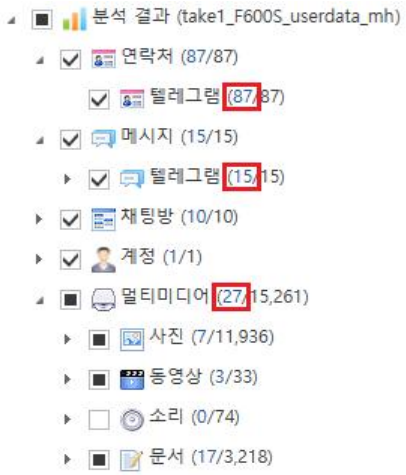

그림 1. Telegram 설치 직후 분석결과(예시)

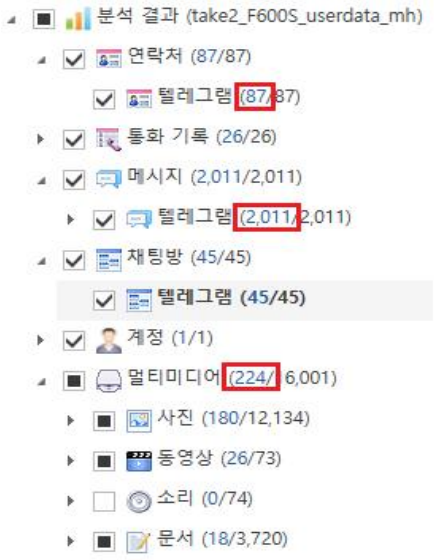

그림 2. 대화 내용 스크롤 후 분석결과(예시)

2) 카카오톡은 최근 3일치 데이터를 클라우드 서버에 저장함 (https://cs.kakao.com/helps?service=8&category=24&locale=ko&device=9& articleId=1073192185)

3) WhatsApp의 iPhone 데이터 백업 예시 (https://faq.whatsapp.com/en/iphone/26000285)

이와 같은 문제를 해결하려면, 클라우드 메신저를 분석할 때 기기를 직접 조작하여 증거로 수집할 데이터가 존재하는 대화방에 들어가서 해당 데이터까지 스크롤 한 뒤 증거를 수집해야 한다. 만일 이 사실을 모르고 분석할 경우 수사관은 과거 데이터의 존재 여부를 인지하지 못할 가능성이 있다. 다시 말해, 클라우드 메신저를 분석할 때, 기존의 포렌식 방법에만 의지해서는 안 된다.

2.2. 모바일 메신저의 사용자 인증방식

사용자가 메신저 서비스에 가입하거나, 기기를 변경하거나, 초기화하거나, 앱을 재설치하면 메신저는 다양한 방식으로 사용자를 인증한다. 인증방식은 크게 전화번호기반 인증코드입력방식, ID/PW방식, 소셜 네트워크 서비스 로그인 인증방식으로 나뉜다.

전화번호기반 인증코드입력방식은 사용자가 입력한 휴대전화번호로 일회용 인증코드가 포함된 문자메시지를 전송한 뒤, 사용자에게 인증코드를 물어보고 입력받은 코드가 전송된 코드와 일치하는지 확인함으로써 상대방을 등록된 사용자로 인증하는 방식이다[9]. 전화번호기반 인증코드입력방식은 휴대폰의 도난이나 분실 시 취득자에게 해당 기기에 대한 물리 접근이 가능해진다는 것과 인증 문자메시지를 우회시켜 공격자에게 발송시키는 것이 가능하다는 단점이 있다. 그럼에도 불구하고, 사용자가 ID와 비밀번호를 따로 기억할 필요가 없고, 서비스 제공자의 비용부담이 매우 저렴하면서, 전 세계 대부분의 이용자에게 적용할 수 있기 때문에 사용자의 주 인증수단 사용이 불가능한 상황(패스워드 분실 등)에 흔히 사용된다[그림 3].

ID/PW방식은 사용자의 ID와 비밀번호 쌍이 서버에 저장되어 있고, 사용자가 자신의 ID와 비밀번호를 입력하면 서버의 정보와 사용자의 입력정보를 비교한 뒤 일치할 경우 인증하는 방식이다. 메신저에서 사용되는 ID는 일반적으로 휴대전화번호 또는 이메일주소 유형이다. ID가 휴대전화번호라면, 최초 가입 시 전화번호기반 인증코드입력방식을 통해 해당 휴대전화번호를 검증한다. 만일 ID가 이메일주소라면 최초 가입 시 입력한 이메일에 확인 링크를 보내거나, 인증코드를 보내서 이메일 주소를 검증한다. 비밀번호가 유출되면 제3자에 의한 접근이 가능하다는 단점이 있지만, 휴대전화가 없고 인터넷만 연결되어있는 상황에서도 사용될 수 있다는 장점이 있다[그림 4].

소셜 네트워크서비스 로그인 방식은 페이스북, 트위터, 카카오톡과 같은 소셜 네트워크 서비스의 계정에 의존해서 새로운 계정을 만들거나 계정에 접속하는 방식으로, 사용자에게는 번거로운 회원가입 절차 없이 기존 소셜 서비스 가입정보를 통해 편하게 로그인할 수 있고, 서비스 제공자는 ID와 비밀번호를 따로 관리할 필요가 없고, 동시에 이용자들의 서비스 진입 장벽을 낮출 수 있어 최근 흔히 사용되는 방식이다[그림 5] [4].

그림 3. 전화번호기반 인증코드방식(signal)

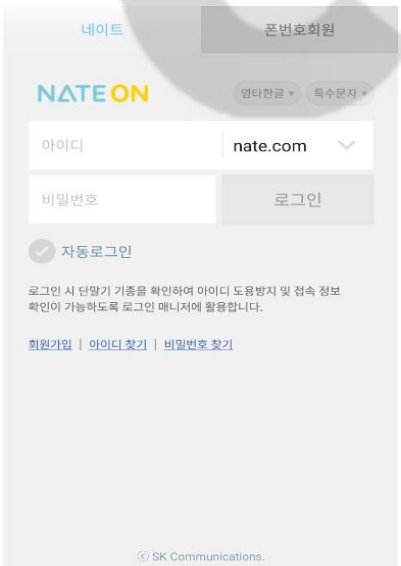

그림 4. ID/PW방식(NateOn)

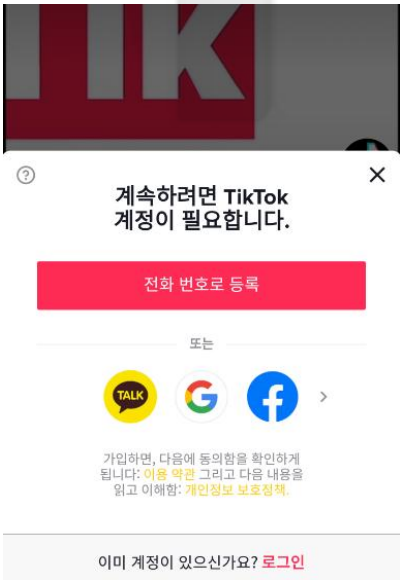

그림 5. 전화번호기반 인증코드방식과 소셜 네트워크서비스 로그인방식 혼합(Tiktok)

언급된 인증방식 중 [그림 5]처럼 2가지 이상의 인증방식을 제공하고 사용자에게 그 중 하나를 선택하여 로그인할 수 있게 하는 메신저가 있는가 하면, 2가지 이상의 인증에 모두 성공해야 로그인을 허용하는 다중인증(Multi-factor login)을 지원하는 메신저도 있다. 각각의 메신저별 인증방식과 다중인증 지원 여부는 [표 3]과 같다.

4) 소셜 네트워크서비스 로그인 방식 (https://en.wikipedia.org/wiki/Social_login)

표 3. 애플리케이션 별 인증방식과 다중인증 지원 여부

애플리케이션 이름	인증방식			다중인증 지원여부	비고
	전화번호	ID/PW	SNS		
WhatsApp	✔				
Facebook Messenger	✔	✔		✔	
HangOut			✔		Google 로그인
Instagram	✔	✔	✔	✔	Facebook 로그인
Skype	✔	✔			
SnapChat		✔			
imo	✔				
Line	✔		✔	✔	Facebook 로그인
Viber	✔				
Azar			✔		
KakaoTalk	✔	✔		✔	
KikMessenger		✔			
Tango	✔		✔		Facebook/Google 로그인
Telegram	✔	✔		✔	
TikTok	✔		✔		Facebook/Kakaotalk/Google 로그인
Wechat	✔		✔		Facebook 로그인
Zalo	✔				
Discord		✔			
Zello		✔			
Between		✔	✔		Facebook 로그인
ICQ	✔				
Nateon	✔	✔			
QQ	✔				
Signal	✔				
Soma	✔				
slack		✔			

2.3. 보조인증 (비밀번호 찾기)

사용자가 비밀번호 등 인증정보를 망각하면 서비스를 이용할 수 없다. 일부 메신저는 이러한 경우에 망각한 인증정보와 로그인상태를 복구할 수 있도록 보조인증기능을 제공하기도 한다.

보조인증 방법은 전화번호기반 인증코드입력방식, 이메일기반 인증방식, 소셜 네트워크서비스로그인 방식, OTP[5]방식 등이 있다.

기본 로그인 수단으로 전화번호기반 인증코드입력방식만을 사용하는 메신저는, 인증 시점마다 일회용 비밀번호가 생성되므로 사용자가 기억해야 하는 비밀번호가 없기 때문에 별도로 보조인증을 제공하지 않는다. 또한 소셜 네트워크서비스 로그인 방식을 사용하는 메신저는 사용자가 비밀번호를 망각했다 하더라도 인증 과정을 이미 소셜 네트워크서비스에 위탁하였기 때문에 메신저가 별도의 보조인증을 제공하지 않는다. 하지만 ID/PW 방식을 사용하는 메신저는 사용자가 비밀번호를 기억하지 못할 경우 비밀번호 이외의 정보를 이용하여 사용자를 재 인증해야 한다. 메신저 애플리케이션 별 보조인증 방법은 〔표 4〕와 같다.

5) One-time password

표 4. 애플리케이션 별 보조인증 방법(비밀번호 분실 시)

애플리케이션 이름	보조인증방식				비고
	전화번호	e-mail	SNS	OTP	
WhatsApp	✔				
Facebook Messenger	✔	✔		✔	Google Authenticator, DUO OTP 지원
HangOut			✔		Google 계정
Instagram	✔	✔		✔	Google Authenticator, DUO OTP 지원
Skype	✔	✔		✔	Microsoft Authenticator OTP 지원
SnapChat		✔		✔	Google Authenticator OTP 지원
imo	✔				
Line		✔			
Viber					
Azar			✔		
KakaoTalk	✔	✔			
KikMessenger					
Tango	✔		✔		
Telegram	✔	✔			
TikTok	✔		✔		
Wechat	✔	✔			
Zalo	✔				
Discord		✔			
Zello					
Between		✔	✔		
ICQ	✔				
Nateon	✔	✔			Nate 계정 연동 필요
QQ	✔				
Signal	✔				
Soma	✔				
slack		✔			

Ⅲ. 클라우드 메신저의 인증우회

3.1. 보조인증을 이용한 인증우회

클라우드 메신저 애플리케이션의 경우 클라우드 저장소를 사용하기 때문에 내용 확인을 위해 반드시 사용자의 기기를 확인해야 할 필요가 없다. 즉, 기기가 잠겨있더라도 수사관이 사용자 인증 권한을 획득하게 된다면 다른 스마트 기기나 PC버전 프로그램을 이용해서 사용자 데이터에 접근할 수 있다.

전화번호기반 인증코드입력방식만을 사용하는 메신저는 발송된 문자메시지를 확인할 수 있다면 우회할 수 있다. 수사관은 잠겨있는 스마트폰에서 SIM 카드를 추출하여 여분의 스마트폰에 삽입한 뒤, 해당 SIM 카드로 기기의 전화번호를 설정하고, 애플리케이션을 설치하여 인증코드메시지를 수신하는 방식으로 인증을 우회할 수 있다.

이메일 인증방식과 소셜 네트워크서비스 로그인 방식은 모두 특정 사이트에 계정과 비밀번호를 넣고 로그인을 하는 절차를 거쳐 인증된다. 일반적인 포털 사이트와 소셜 네트워크 서비스에서는 비밀번호를 망각하였을 때 일정한 본인 인증 절차를 거치면 비밀번호를 획득할 수 있기 때문에, 수사관은 대상자의 인적 사항과 SIM 카드를 가지고 비밀번호를 획득할 수 있다. 하지만 비밀번호 복구에 대한 절차와 필요조건은 사이트 또는 서비스마다 다를 수 있다. 〔그림 6〕은 네이버의 비밀번호 찾기 화면이다. 네이버의 경우 2단계 인증을 설정하지 않았다면 전화번호와 개인정보만으로 비밀번호를 변경할 수 있다.

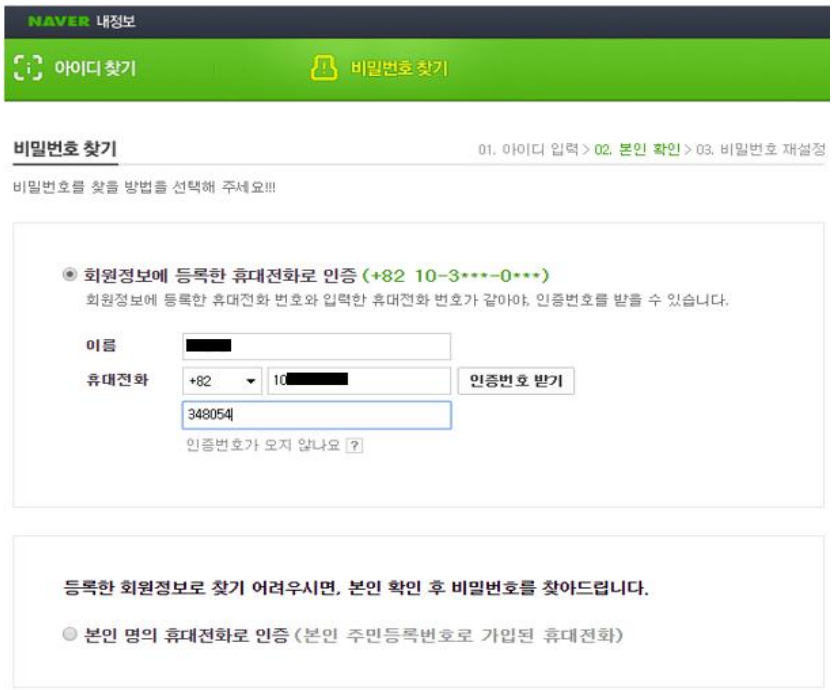

그림 6. 네이버의 비밀번호 찾기

OTP를 보조인증수단으로 사용하고 있다면 반드시 OTP를 확보해야 한다. 메신저에서 사용되는 OTP는 대부분 모바일 애플리케이션이므로, 여분의 스마트폰이나 태블릿과 같은 모바일 기기가 존재하는지 확인해야 한다.

〔그림 7〕은 2단계 인증을 제공하는 Telegram의 인증 우회 프로세스이다.

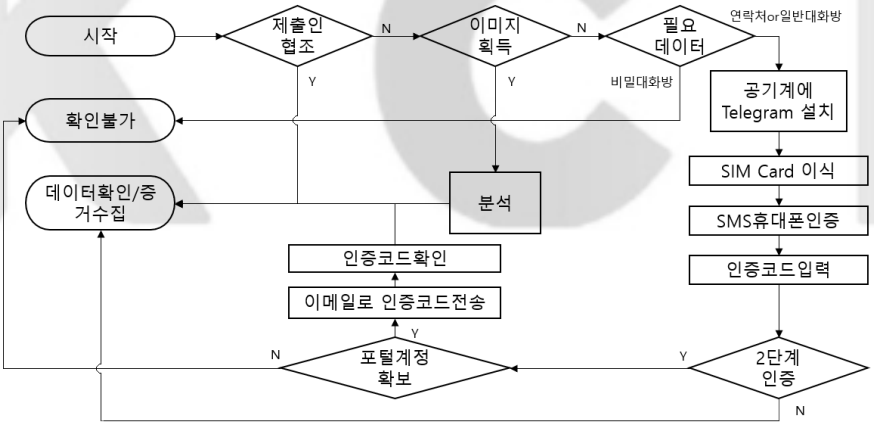

그림 7. Telegram 메신저의 인증 우회 프로세스

3.2. 인증 우회 시 고려사항

인증정보를 확보하여 메신저에 직접 접근하는 방법은 기존의 포렌식 방법으로 분석이 불가한 경우에 유용하게 사용될 수 있다. 하지만 다음과 같은 상황에 주의해야 한다.

첫 번째, 인증정보가 확보되면 신속히 보존조치를 취해야 한다. 클라우드 메신저의 사용자 데이터는 메신저의 관리 정책이나 공범 등 제3자에 의해 삭제될 수 있기 때문이다. 백업되지 않은 클라우드 데이터가 삭제되면 대화 상대방의 계정에 접근하지 않는 한 열람이 불가하므로 데이터가 훼손되지 전에 신속히 보존조치를 취해야 한다.

두 번째, 삭제된 데이터 복원이 불가능하다. 기존의 포렌식 방법을 이용하면 대화 내용이 저장되어있는 데이터베이스에 직접 접근할 수 있기 때문에 삭제된 데이터를 복원할 수 있다. 하지만, 여분의 기기에 데이터를 설치한 경우 데이터베이스 파일을 동기화하는 것이 아니라 대화 내용과 첨부파일 등 삭제되지 않은 사용자 데이터만 동기화하기 때문에 삭제된 데이터의 복원이 불가능하다.

세 번째. 클라우드에 저장되지 않는 일부 데이터는 확인할 수 없다. 텔레그램과 네이트온과 같은 일부 애플리케이션은 '비밀대화방' 기능을 제공한다. 비밀대화방을 이용해서 메시지를 주고 받을 경우, 메시지는 기존의 기기에만 암호화되어 저장되고, 클라우드에 저장되지 않는다.

네 번째. 대상 스마트폰에서 추출한 SIM 카드와 수사관이 사용하는 스마트폰이 호환되지 않는다면 사용이 불가할 수도 있다. 스마트폰에 삽입되는 SIM카드는 세 가지 크기가 있다[6]. 또한 일부 스마트폰의 경우 SIM에 종속적인 약정이나 통신사 제약, 국가 제약에 따라 호환이 되지 않는다. 수사관은 인증 우회작업을 위해 다양한 SIM 크기에 대응할 수 있는 SIM adaptor를 준비하고, 가급적 작업에 사용되는 스마트폰은 SIM카드의 영향을 받지 않는 자급제 폰(Unlock phone)을 이용하여 작업하는 것이 좋다.

다섯 번째, 소유자의 협조 없이 수사관이 임의로 인증정보를 우회하는 상황이라면 반드시 관련 압수영장을 발부받아 관련자의 참여하에 진행하여야 한다. 또한, 가급적 전문가의 입회 하에 작업하며, 전체 과정을 채증하는 것이 좋다[10]. 소유자가 협조하지 않는 상황에서 개인정보를 이용하여 소유자인 것처럼 인증을 받는 행위는 소유자의 기본권을 침해하는 강제수사에 해당하기 때문이다. 만일 영장이 없는 상황에 외부 공범의 삭제가 우려되는 등 긴급한 상황이라면, 소유자 또는 변호인의 참여하에 데이터를 별도의 저장소에 백업 및 봉인 해 두고 2차 영장을 발급 받아 진행하는 것이 좋다.

클라우드 메신저의 사용자 데이터를 수집하는 절차는 [그림 8]과 같다.

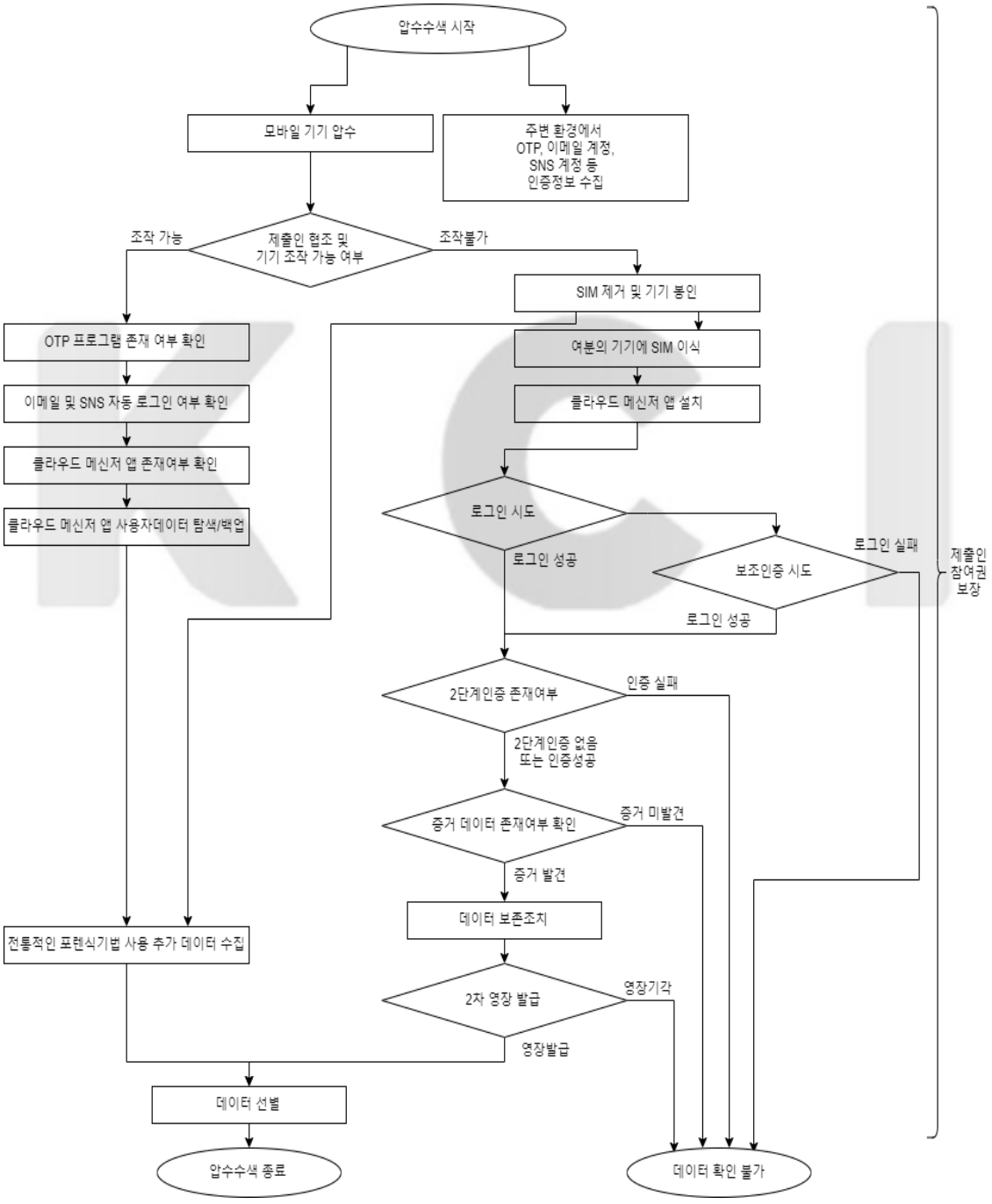

그림 8. 클라우드 메신저 사용자 데이터 수집 절차

6) 모바일폰에 삽입되는 3가지 크기의 SIM card : Mini, Micro, Nano (https://en.wikipedia.org/wiki/SIM_card)

3.3. 클라우드메신저 인증 우회 시나리오

다크웹에서 마약 구매자로 위장한 경찰관이 마약을 판매한 것으로 의심되는 피의자를 검거하였다. 피의자의 신체와 자택을 압수수색한 결과 스마트폰 1개와 노트북 1대를 발견하였다. 스마트폰은 아이폰 8인데 pin번호로 잠겨있었고, 노트북은 Bitlocker로 암호화 된 상태였다. 하지만 피의자는 암호 해제 및 진술을 거부했다.

경찰관이 마약구매자로 위장해서 피의자와 연락할 당시 텔레그램을 사용했으므로, 피의자의 텔레그램 대화 내용을 확인하면 마약 구매자를 추가로 특정하고 피의사실을 명확히 할 수 있을 것이라 기대하였다.

경찰관은 디지털포렌식 센터에 스마트폰과 노트북을 분석 의뢰했지만, 암호 해제에 실패해서 분석 불가 회신을 받았다. 고민 끝에 경찰관은 피의자 신문 도중 본인의 PC에 텔레그램을 설치하고 피의자의 휴대전화번호로 로그인을 시도했다. 피의자의 휴대폰에서 추출한 SIM 카드를 업무용 스마트폰에 넣자, 업무용 스마트폰에 텔레그램의 인증코드가 전송되었다. 이런 상황을 지켜 본 피의자는 진술을 하기 시작했고, 아이폰의 잠금을 해제하였다. 결국 경찰관은 텔레그램 대화 내용을 확인하여 추가 피의자를 특정할 수 있었다.

Ⅳ. 결론

모바일 기기가 잠겨있거나, 작동 불능인 상태라도 인증정보를 우회하면 클라우드 저장소를 사용하는 메신저의 사용자 데이터를 추출할 수도 있다는 사실을 확인하였다. 인증 우회에는 일반적으로 사용자의 SIM 카드와 개인정보가 이용되며, 경우에 따라서 OTP와 같은 장치의 정보가 필요하다는 것을 확인하였다.

하지만 이런 방법을 사용해도 삭제된 데이터 복원은 불가능하고, 재현이 불가할 수도 있다. 또한, 인증 우회 행위는 피의자의 참여와 법원의 영장이 확보된 상황에서 사용해야 한다는 제약도 있다.

인증 우회 행위는 사용자가 아님에도 사용자의 개인정보와 전화번호를 이용하기 때문에 법적인 다툼이 있을 수 있다. 본 연구에서는 인증 우회의 가능성과 사용 효과에 대해 알아보았지만, 법적 다툼 가능성과 이에 따른 추가 연구가 필요하다.

또한, 클라우드 메신저를 대상으로 연구를 진행했지만, 클라우드 저장소를 사용하는 다양한 유형의 애플리케이션(파일저장소, 사진백업, 제조사 백업)에도 적용할 수 있을 것이라 예상되므로 관련 애플리케이션의 적용 가능성에 대한 추가 연구가 필요하다.

참 고 문 헌 (References)

〔1〕 Khushboo Rathi, Umit Karabiyik, Temilola Aderibigbe and Hongmei Chi, "Forensic analysis of encrypted instant messaging applications on android", International Symposium on Digital Forensic and Security (ISDFS), 2018 6th, pp. 1 - 6, 2018.

〔2〕 Yoon, Jongcheol and Park, Yongsuk, "Forensic Analysis of KakaoTalk Messenger on Android Environment", Journal of the Korea Institute of Information and Communication Engineering, vol. 20(1), pp. 72 - 80, Apr. 2016.

〔3〕 Yang, Teing Yee, Ali Dehghantanha, Kim-Kwang Raymond Choo, and Zaiton Muda, Windows instant messaging app forensics: Facebook and Skype as case studies., PloS one, vol. 11, no. 3, Mar. 2016.

〔4〕 Jung-Hoon Oh and Sang-Jin Lee, "A Study on the Analysis Methodology of Smartphone for Android Forensics", Journal of Digital Forensics, vol. 9, pp.47-75, Dec. 2012.

〔5〕 Bon-Min Goo, "Collection and Analysis of the Digital Evidence for Android and iOS Smart Phones", Journal of the Korea Institute of Information Security & Cryptology, vol. 21, pp.167-175, Feb. 2011.

〔6〕 Zdziarski, Jonathan, iOS forensic investigative methods. Technical Report, International Tele communication Union, http://www.zdziarski.com/blog/wp-content/uploads/2013/05/iOS-Forensic-Investigative-Methods, pdf, 2008.

〔7〕 Byungchan Jung, "A Study on the Possibility of Recover ing Deleted Data through Analysis of SQLite Journal in Messenger Application", Journal of Digital Forensics, vol. 12, pp.11-20, Dec. 2018.

〔8〕 K. Stephan, "Apple Versus the Feds: How a smartphone stymied the FBI.," IEEE Consumer Electronics Magazine, vol. 6, pp.103-104, Apr. 2017.

〔9〕 Mulliner, C., Borgaonkar, R., Stewin, P. and Seifert, J.P., "SMS-based one-time passwords: attacks and defense", International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Springer, Berlin, Heidelberg, pp. 150-159, July. 2013.

〔10〕 Cheun, Seung-Deuk and Kang, Gu-Min, "A Study of the Search and Seizure Procedure for Remote Servers through the Practical Affair", The Korean Association of Criminal Procedure Law, 11(1), 57-90, june. 2019.

저 자 소 개

이 민 형 (MinHyung Lee)
준회원
2010년 8월 : 건국대학교 컴퓨터소프트웨어학과 졸업
2016년 2월~현재 : 서울지방경찰청 디지털포렌식계
2018년 9월~현재 : 고려대학교 정보보호대학원 디지털포렌식학과 석사과정
관심분야 : 디지털 포렌식, 정보보호

이 상 진 (SangJin Lee)
종신회원
1989년 10월~1999년 2월 : ETRI 선임 연구원
1999년 3월~2001년 8월 : 고려대학교 자연과학대학 조교수
2001년 9월~현재 : 고려대학교 정보보호대학원 교수
2008년 3월~현재 : 고려대학교 디지털포렌식연구센터 센터장
관심분야 : 디지털 포렌식, 심층암호, 해쉬함수