

소셜 네트워크 서비스에서 사건 수사를 위한 모바일 디지털 포렌식 절차에 관한 연구

Mobile Digital Forensic Procedure for Crime Investigation in Social Network Service

장유종*, 곽진**0

Yu Jong Jang*, Jin Kwak**0

요약

소셜 네트워크 서비스는 사용자간의 통신수단 및 자신을 표현하는 하나의 수단으로 사용되면서 다양한 정보를 보유하고 있다. 이러한 정보들은 수사에 도움이 되는 유용한 증거로 사용 될 수 있다. 본 논문에서는 소셜 네트워크 서비스상에 있는 다양한 정보를 사건 수사에서 효율적으로 사용하기 위하여 소셜 네트워크 서비스를 이용하는 사용자의 스마트폰에 대한 모바일 디지털 포렌식 절차에 관한 연구를 진행하였다. 모바일 디지털 포렌식 절차 연구를 위하여 스마트폰에 저장되어 있는 소셜 네트워크 서비스 어플리케이션에 대한 DataBase 파일을 분석하여 사건 수사에 유용하게 사용할 수 있는 파일을 분류 하고 저장되어 있는 정보를 비교 분석하였다. 이를 통하여 본 논문에서는 소셜 네트워크 서비스 환경에서 사건 수사를 위한 적합한 모바일 디지털 포렌식 절차를 제안한다.

Abstract

Social network services(SNS) has been used as a means of communication for user or express themselves user. Therefore, SNS has a variety of information. This information is useful to help the investigation can be used as evidence. In this paper, A study of mobile digital forensic procedure for crime investigation in social network service. Analysis of database file taken from the smartphone at social network service application for mobile digital forensic procedure. Therefore, we propose a procedure for the efficient investigation of social network service mobile digital forensic

Key words : Mobile Digital Forensic, Social Network Service.

I. 서론

최근 소셜 네트워크 서비스(SNS : Social Network

Service)는 스마트폰 보급률의 증대와 함께 이용률이 증가하여 서비스 사용자간의 의사소통 및 사용자 자신을 표현하는 하나의 수단으로 자리 잡아가고 있다.

* 순천향대학교 정보보호학과 정보보호응용및보증연구실(ISAA Lab. Department of Information security Engineering Soonchunhyang University)

** 순천향대학교 정보보호학과(Department of Information security Engineering, Soonchunhyang University)

· 제1저자 (First Author) : 장유종(YuJong Jang)

0 교신저자 (Corresponding Author) : 곽진(Jin Kwak, Tel : +82-70-7516-6293, email : jkwak@sch.ac.kr)

· 접수일자 : 2013년 5월 31일 · 심사(수정)일자 : 2013년 5월 31일 (수정일자 : 2013년 6월 24일) · 게재일자 : 2013년 6월 30일
<http://dx.doi.org/10.12673/jkoni.2013.17.3.325>

소셜 네트워크 서비스는 사용자간의 대화내용, 사용자 위치 정보, 인적 네트워크, 사용자 심리상태와 같은 다양한 정보를 보유하고 있다. 이러한 정보들은 디지털 포렌식을 통하여 사건 수사에 도움이 되는 유용한 증거로 사용될 수 있다.

하지만, 소셜 네트워크 서비스는 디바이스에 데이터가 저장되어서 서비스를 제공하는 컴퓨팅 서비스와는 다르게 SNS 서버와 데이터를 실시간 동기화하여 서비스를 제공하고 있다. 그렇기 때문에 컴퓨터 디바이스는 소셜 네트워크 서비스 이용 로그 기록과 같은 증거로서 효력이 미약한 정보만을 저장하고 있다. 하지만, 모바일 디바이스는 소셜 네트워크 서비스를 효율적으로 제공하기 위하여 친구 목록, 대화내용, 사용자 인적 관계와 같은 다양한 정보를 저장하고 있다. 그러므로 이를 통해 문제가 발생할 경우 정보의 조작 및 훼손 없이 증거물로 사용하기 위하여 모바일 디지털 포렌식 방법이 필요하다.

본 논문에서는 디지털 증거가 훼손 및 조작 되는 경우를 방지하기 위한 소셜 네트워크 서비스 환경에 적합한 모바일 디지털 포렌식 모델을 제안한다.

본 논문의 구성은 2장에서는 관련연구로서 디지털 포렌식과 소셜 네트워크 서비스를 통한 수사 사례를 분석하고 소셜 네트워크 서비스에 적합한 디지털 포렌식 연구의 필요성에 대하여 분석한다. 3장에서는 소셜 네트워크 서비스에 적합한 모바일 디지털 포렌식 모델을 제안하고, 이를 통한 기대효과를 분석한다. 4장에서는 본 논문의 결과와 향후 연구 방향에 대한 설명으로 끝을 맺는다.

II. 관련연구

2-1 디지털 포렌식

컴퓨팅 기술의 발전으로 디지털 사회로 변화함에 따라 사건 수사에는 필수적으로 디지털 기기가 증거자료로 수집된다. 하지만 디지털 기기의 자료는 수정 및 삭제가 용이 하기 때문에 수집된 디지털 기기 그대로 증거 자료로 사용하기는 어려움이 따른다. 그렇기 때문에 디지털 기기에서 자료를 분석하여 사건 수

사에 대한 올바른 증거자료로 사용하기 위한 일련의 방식인 디지털 포렌식 과정이 사용된다.

2-2 소셜 네트워크 서비스를 통한 수사 사례

최근 페이스북과 트위터와 같은 소셜 네트워크 서비스에 저장되어 있거나 공유되는 디지털 정보(글, 사진 및 동영상)를 사건 수사에서 디지털 증거로 사용하여 범죄 사실을 밝히는 사례가 늘고 있다[1].

소셜 네트워크 서비스는 사용자 개인의 일정, 친구와의 대화, 현재 위치와 같은 개인적인 데이터를 생성하고 공유한다. 이러한 정보를 분석하여 사건 용의자의 생활 패턴, 범행동기 등을 알아낼 수 있다. 또한, 사용자의 과거 일정을 도출해내거나 앞으로의 일정을 예측할 수 있다.

□ 동영상 정보 활용 사례

2012년 7월, 피의자가 성폭행을 당한 사건에서 피의자는 의식이 없어 성폭행 사실을 기억하지 못했지만, 경찰은 페이스북에 올린 사진과 동영상을 통하여 가해자를 추적하여 가해자 일당을 체포하였다[1].

□ 정황증거 활용 사례

2011년 5월, 모 대학교수 부인 살해 사건에서 강 모 교수는 자신과 내연녀가 주고받은 ‘카카오톡’ 대화내용을 회사에 찾아가 서버에서 삭제하였다. 하지만 경찰 측에서 데이터를 복원하여 남편과 내연녀가 주고받은 대화 내용을 복구하여 살인을 계획한 정황증거로 제시하였다[2].

□ 용의자 파악 및 범행동기 파악 사례

2013년 4월, 보스턴 마라톤 테러사건에서 용의자를 파악하기 위하여 경찰측에서 현장에 있던 사람들의 SNS 정보(사진, 동영상 등)를 수집하였다. 이를 통하여 당시 용의자의 인상착의를 유추하였다. 또한 유추해낸 용의자의 SNS 정보를 통하여 용의자의 정치사상, 범행동기 등을 유추하였다[3].

2-3 소셜 네트워크 디지털 포렌식 필요성

소셜 네트워크 서비스는 사용자의 다양한 정보를 보유하고 있다. 사용자가 공유하고 있는 정보들은 업무상 정보 또는 회사 기밀정보 보다 사용자의 일정, 친구와의 대화, 현재 위치와 같은 개인적인 데이터를 주로 생성하고 공유한다. 이러한 정보를 통하여 사건 용의자의 생활 패턴을 분석할 수 있다. 또한 용의자의 일정이나, 앞으로의 행동을 예측할 수 있다.

소셜 네트워크 서비스는 디바이스에 데이터가 저장되어 서비스를 제공하는 컴퓨팅 서비스와는 다르게 SNS 서버와 데이터를 실시간 동기화하여 서비스를 제공하고 있다[4].

실시간 동기화 서비스는 디바이스에 데이터가 저장되는 서비스와는 데이터 관리 형태가 다르다. 디바이스에 데이터가 저장되는 서비스는 증거물로 디바이스를 확보한 상태에서는 디바이스에 저장된 데이터에 대한 무결성이 보장되기 때문에 디지털 증거물로서 사용할 수 있다. 하지만 실시간 동기화 서비스는 용의자의 디지털 디바이스를 확보하여도 다른 디바이스를 통하여 동일 계정으로 소셜 네트워크 서비스에 접근하여 데이터 변경 및 삭제가 가능하다. 또한 소셜 네트워크 서비스의 특성상 다른 사용자가 용의자의 데이터에 접근이 가능하다. 이러한 접근은 디지털 데이터의 무결성을 훼손 시킬 수 있다. 무결성이 훼손된 디지털 데이터는 증거로서의 가치를 상실한다. 또한 용의자의 디지털 데이터가 다른 사용자에게 유출되어 수사에 증거로 사용되는 디지털 증거물이 악용되는 경우가 발생할 수 있다.

위와 같은 문제점들 때문에 소셜 네트워크 서비스의 데이터를 사건 수사에 올바르게 사용하기 위한 소셜 네트워크 서비스에 적합한 디지털 포렌식 모델이 필요하다.

Ⅲ. 소셜 네트워크 서비스

모바일 디바이스 데이터 수집 절차

소셜 네트워크 서비스를 사용하는 모바일 디바이스에 대한 디지털 포렌식을 효율적으로 적용시키기 위해서는 서비스 제공환경인 실시간 동기화 환경과

개방성을 고려해야 한다.

본 논문에서는 제안하는 소셜 네트워크 서비스에 대한 모바일 디지털 포렌식 절차는 실시간 동기화 서비스에 대한 디지털 포렌식 절차에서 소셜 네트워크 서비스 환경의 특성을 고려하여 제안되었다[4].

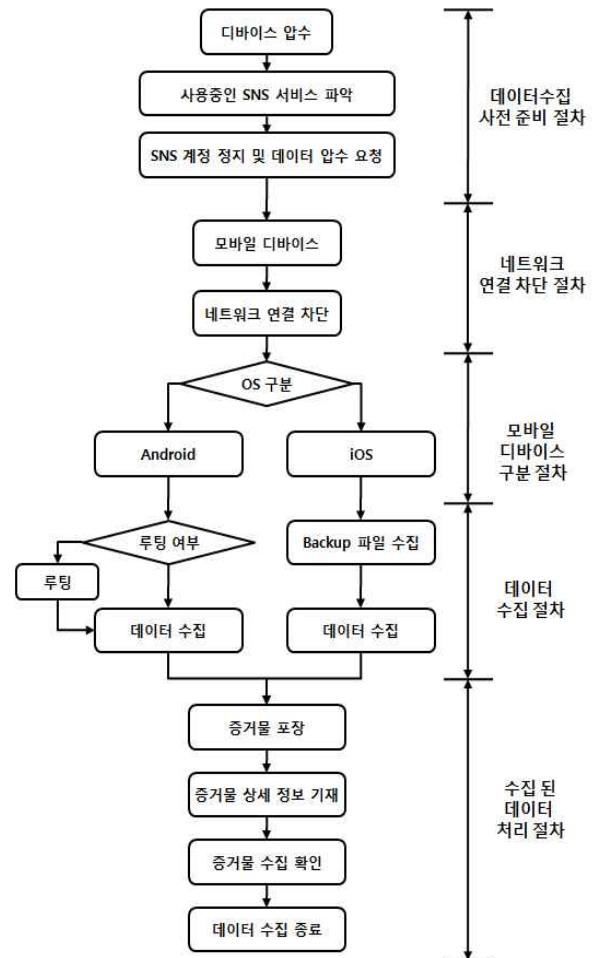


그림 1. 모바일 디지털 포렌식 순서도
Fig. 1. Mobile Digital Forensic Procedure

3-1 데이터 수집 사전 준비단계

용의자의 모바일 디바이스 확보 과정은 기존의 디지털 포렌식 과정과 동일하다. 디바이스를 확보하고 난 후 디지털 포렌식 조사관은 용의자가 사용하는 SNS 서비스를 파악하고 해당 SNS 서비스의 용의자 계정에 대한 정지 요청 및 데이터 로그 확보 요청을 한다. 용의자 계정 정지를 통하여 용의자가 다른 디바이스를 통해 소셜 네트워크 서비스의 접근하는 것

을 차단한다. 또한 이를 통하여 다른 사용자의 접근을 차단한다. 이를 통하여 소셜 네트워크 서비스상에 있는 디지털 데이터에 대한 무결성을 유지한다.

3-2 데이터 수집 사전 준비단계

모바일 디바이스는 어플리케이션을 통하여 소셜 네트워크 서비스를 이용한다. 이러한 어플리케이션은 데이터 베이스에 사용자의 인적 관계 또는 사용자 간 대화 내용, 서비스 이용 형태와 같은 수사에 유용한 다양한 정보를 포함하고 있다. 이러한 정보가

실시간 동기화를 통하여 변경되지 않도록 모바일 디바이스를 확보하면 네트워크 연결을 차단한다.

그림 3은 컴퓨터 디바이스를 사용하여 친구 관계를 끊은 경우 모바일 디바이스의 네트워크 연결 상태, 네트워크 연결 차단 상태, 로그아웃 상태와 같은 3가지 상태에서 페이스북 어플리케이션에 저장된 내부 데이터의 차이점을 보여주고 있다. 모바일 디바이스에 네트워크가 지속적으로 연결된 상태에서는 다른 디바이스를 통하여 데이터를 수정한 경우(친구 목록 삭제) 실시간 동기화를 통하여 내부 데이터(친구 목록)에서 6번 친구의 데이터가 삭제된 것을 보여주고 있다. 하지만, 네트워크 연결이 차단된 모바일 디

바이스는 실시간 동기화를 할 수 없기 때문에 내부 데이터(친구 목록)가 수정되지 않고 있다.

디지털 포렌식 관점에서 증거물을 확보한 경우 데이터가 변조되면 증거물로서의 가치를 상실하기 때문에 용의자 또는 다른 사용자가 증거로서 사용될 수 있는 소셜 네트워크 서비스 내부데이터를 회손 및 수정하는 경우를 방지할 수 있도록 네트워크 연결을 차단 하여야한다. 또한, 네트워크가 연결되어 있는 모바일 디바이스는 자동 로그아웃 기능이나 원격 로그아웃 기능을 사용할 수 있기 때문에 내부 데이터가 삭제되는 로그아웃을 막기 위하여 네트워크 연결은 차단되어야 한다.

모바일 디바이스의 데이터는 OS마다 다른 형태로 저장된다. 그렇기 때문에 데이터를 올바르게 수집하기 위해서는 모바일 디바이스의 OS를 구별하여 데이터 수집을 진행하여야 한다. 현재 국내에서 사용하고 있는 모바일 디바이스의 대표적인 두 가지 OS는 안드로이드와 iOS이다[5].

- 안드로이드 : Rooting을 통한 데이터 수집
- iOS : Backup 파일을 통한 데이터 수집

inter	contact_id	data
1	1	Y29udGFjdC...{"contactId":"Y2A3","profileFbid":"1007","graphApiWriteld":"contact_108207","name":{"firstName":"가령","lastName":"김","displayName":"김가령"},
2	2	Y29udGFjdC...{"contactId":"Y2I1","profileFbid":"1000","graphApiWriteld":"contact_100985","name":{"firstName":"창균","lastName":"노","displayName":"노창균"},
3	3	Y29udGFjdC...{"contactId":"Y2IjU4","profileFbid":"1038","graphApiWriteld":"contact_167258","name":{"firstName":"민호","lastName":"이","displayName":"이민호"},
4	4	Y29udGFjdC...{"contactId":"Y2Igz","profileFbid":"1083","graphApiWriteld":"contact_101483","name":{"firstName":"Insu","lastName":"Mun","displayName":"Insu M"},
5	5	Y29udGFjdC...{"contactId":"Y2TA5","profileFbid":"1009","graphApiWriteld":"contact_118509","name":{"firstName":"유경","lastName":"위","displayName":"위유경"},
6	7	Y29udGFjdC...{"contactId":"Y2Mdc4","profileFbid":"1078","graphApiWriteld":"contact_350078","name":{"firstName":"슬기","lastName":"최","displayName":"최슬기"},

네트워크 연결 상태

inter	contact_id	data
1	1	Y29udGFjdC...{"contactId":"Y29udG","profileFbid":"1C","graphApiWriteld":"c18207","name":{"firstName":"가령","lastName":"김","displayName":"김가령"},
2	2	Y29udGFjdC...{"contactId":"Y29udG","profileFbid":"10","graphApiWriteld":"c5785","name":{"firstName":"창균","lastName":"노","displayName":"노창균"},
3	3	Y29udGFjdC...{"contactId":"Y29udG","profileFbid":"1","graphApiWriteld":"567258","name":{"firstName":"민호","lastName":"이","displayName":"이민호"},
4	4	Y29udGFjdC...{"contactId":"Y29udG","profileFbid":"1","graphApiWriteld":"681483","name":{"firstName":"Insu","lastName":"Mun","displayName":"Insu M"},
5	5	Y29udGFjdC...{"contactId":"Y29udG","profileFbid":"","graphApiWriteld":"748509","name":{"firstName":"유경","lastName":"위","displayName":"위유경"},
6	6	Y29udGFjdC...{"contactId":"Y29udG","profileFbid":"1f","graphApiWriteld":"d06614","name":{"firstName":"연상","lastName":"변","displayName":"변연상"},
7	7	Y29udGFjdC...{"contactId":"Y29udG4","profileFbid":"3","graphApiWriteld":"8850078","name":{"firstName":"슬기","lastName":"최","displayName":"최슬기"},

네트워크 연결이 차단

inter	contact_id	data
<div style="border: 1px solid black; padding: 5px; width: fit-content; margin: 0 auto;"> <p style="color: red; font-weight: bold; font-size: 1.2em;">데이터 삭제</p> </div>		

로그아웃

그림 2. 내부 데이터 상태
Fig. 2. Inside Data State

3-3 디지털 데이터 처리 단계

모바일 디바이스 대한 데이터 수집이 완료 되면 기존의 디지털 포렌식의 증거물 처리과정과 동일한 과정을 수행한다[6].

IV. 소셜 네트워크 서비스

모바일 디바이스 데이터 분석 방법

소셜 네트워크 서비스에 대한 데이터를 수집하고 난 후 수집된 데이터에 대한 올바른 분석방법이 필요하다. 이러한 분석은 용의자의 소셜 네트워크 서비스를 데이터를 수사에 도움이 되는 유용한 데이터로 추출해내는 방법이다.

컴퓨터 디바이스를 사용한 소셜 네트워크 서비스는 서버에 있는 데이터를 실시간으로 웹 브라우저에 보여주게 되어 있다. 웹 브라우저를 통해 보여주는 데이터는 컴퓨터 디바이스에 저장되지 않는다. 그렇기 때문에 컴퓨터 디바이스에 대한 디지털 포렌식을 진행 하여도 소셜 네트워크 서비스에 대한 증거를 찾아내기는 힘들다.

모바일 디바이스를 사용한 소셜 네트워크 서비스는 모바일 디바이스에 저장된 소셜 네트워크 서비스 어플리케이션을 통하여 서비스가 이루어지고 있다.

이러한 어플리케이션은 원활한 서비스 제공을 위하여 로그인시 사용자의 다양한 정보를 소셜 네트워크 서비스 서버에서 불러와 어플리케이션 DB에 저장하고 난 후 서비스를 제공 해주고 있다. 디지털 포렌식 조사관은 이러한 DB의 정보를 통하여 수사에 유용한 정보를 분석할 수 있다.

본 논문에서는 현재 국내 이용자수가 가장 많은 소셜 네트워크 서비스인 페이스북의 어플리케이션 DB를 분석 하였다.

그림 3은 모바일 디바이스의 data/data/com.facebook.katana/database에 위치한 페이스북의 DB 파일들을 보여주고 있다. 이러한 DB 파일들은 실시간으로 연동되는 페이스북의 데이터를 받아와서 저장하여 사용자가 서비스를 이용할 때 빠른 서비스가 가능하게 한다.

com.facebook.katana		2013-05-27	00:12
app_acra-reports		2013-05-21	20:34
app_dex		2013-05-21	20:34
app_minidumps		2013-05-21	20:34
app_outdex		2013-05-21	20:34
app_secondary-program-dex-jars		2013-05-21	20:34
app_secondary_program_dex		2013-05-21	15:55
app_secondary_program_dex_opt		2013-05-21	20:34
cache		2013-05-22	00:32
databases		2013-05-27	09:52
analytics_db2	36864	2013-05-27	09:12
bookmarks.db	26624	2013-05-22	03:46
contacts_db2	1160192	2013-05-27	07:58
fb.db	51200	2013-05-27	00:12
graphql	6144	2013-05-22	07:31
newsfeed_db	125952	2013-05-22	12:45
notifications.db	256000	2013-05-27	09:05
pages_db	5120	2013-05-22	05:35
prefs_db	38912	2013-05-27	09:52
qe_db	9216	2013-05-27	09:12
threads_db2	83968	2013-05-27	06:12
timeline_db	5120	2013-05-22	09:32
webview.db	14336	2013-05-22	00:43
webviewCache.db	192512	2013-05-22	00:14
dex-lock-dummy	1	2013-05-27	07:31
files		2013-05-22	00:32
lib		2013-05-21	12:29
shared_prefs		2013-05-27	09:52

그림 3. 페이스북 DataBase 파일
Fig. 3. Facebook DataBase File

디지털 포렌식 조사관이 분석하는 어플리케이션 DB 파일은 모바일 디바이스를 확보하고 난 후 네트워크 연결을 차단하기 때문에 확보하였을 당시의 데이터를 보존하고 있다.

그림 4에서 보여지는 DB 파일 중 수사에 유용한 정보를 포함하고 있는 파일은 analytics_db2.db, contacts_db2.db, fb.db, threads_db2 이다. 이러한 파일에서 추출할 수 있는 정보를 분석하여 다음 [표 1]에 표시 하였다.

표 1을 통해 분석 할 수 있는 정보는 사용자의 친구 관계, 사용자의 대화정보, 평소 사용자의 친밀도와 같은 정보를 분석할 수 있다. 또한 남아 있는 정보들을 통하여 실제 웹 브라우저에서 다른 사용자의 정보나 대화를 확인 할 수 있다.

V. 기대효과

본 논문에서 제안한 소셜 네트워크 서비스에 대한 모바일 디지털 포렌식은 소셜 네트워크 서비스 환경에서 효율적으로 수사가 가능하도록 한다.

표 1. DataBase 파일 정보

Table 1. DataBase File Information

파일 이름	요약	정보
analytics_db2	모바일 디바이스 사용형태	GPS 여부, 사용 통신망, 접속한 나라, 모바일 배터리 상태 등
contacts_db2	사용자 친구 정보 (그림 3)	contactId : 친구 연결 관계 ID, profileFbid : 친구 ID값, graphApiWriteId : 친구 관계, name : 친구 이름, smallPictureUrl : https://fbcdn-profile-a.akamaihd.net/hprofile-ak-snc6/c32.9.117.117/s100x100/190686_103259136424781_7050306_a.jpg : 친구 프로필 사진. communicationRank : 친밀도, displayNumber : 휴대폰 번호
fb	사용자의 정보 저장	uid : 사용자 ID, secret : 암호 해쉬값, username : 사용자 메일 주소, machine_id : 사용자 기계 ID, , access_token : 접근 토큰 값, session_key : 세션 연결 해쉬 값, profile : 사용자 이름 https://fbcdn-profile-a.akamaihd.net/hprofile-ak-ash4v273835_100002545740576_1019605470_q.jpg : 사용자 사진
threads_db2	사용자 대화 정보	사용자의 대화 내용 저장

컴퓨터 디바이스는 실제 데이터가 저장되는 것이 아닌 소셜 네트워크 서비스 서버간의 통신이 로그 기록으로만 저장되어 있어 수사에 사용하기에는 정보가 미흡하다. 하지만, 모바일 디바이스에 대한 디지털 포렌식은 본 논문에서 수집 및 분석하였듯이 친구 관계, 사용자의 마지막 행동, 서비스 접속 형태와 같은 다양한 정보를 저장 하고 있어, 수사에 효율적으로 사용할 수 있다.

소셜 네트워크 서비스에 대한 디지털 포렌식으로 얻을 수 있는 정보(증거)를 통한 효과는 다음과 같다.

- 용의자 인적 네트워크 분석
- 용의자 범행동기 파악
- 2차 범죄 사전 예측
- 용의자 위치 파악
- 알리바이 검증 등

VI. 결 론

소셜 네트워크 서비스는 최근 스마트폰의 보급률 증가와 함께 사용자가 크게 증가하였다. 이러한 소셜 네트워크 서비스는 사용자간의 통신수단 및 자신을 표현하는 하나의 수단으로 다양한 정보를 보유하고 있다.

본 논문에서는 소셜 네트워크 서비스에서 공유되는 정보를 사건 수사에 증거로 활용하기 위하여 소셜 네트워크 서비스에 적합한 모바일 디지털 포렌식 모델을 제안하였다. 이러한 절차는 실시간 동기화 환경에서 서비스를 제공하는 소셜 네트워크 서비스에 대한 효율적인 자료 수집 및 분석이 가능하다. 이렇게 얻어진 데이터는 추가적인 수사와 방향에 큰도움이 될 것이다. 하지만 서비스의 형태는 지속적으로 발전해나가고 있으므로 이러한 서비스형태의 발달에 따른 지속적인 조사와 분석이 필요할것으로 생각한다.

감사의 글

본 연구는 미래부가 지원한 2013년 정보통신·방송(ICT) 연구개발사업의 연구결과로 수행되었음

Reference

- [1] InSun Kim (2013. April). *Crame caught the tail SNS. Etnews* [Online]. Available: <http://www.etnews.com>
- [2] SunWoong Im (2011. May). *Wife murderer professor at cooperation his Girlfriend. MBC NEWS* [Online]. Available: <http://www.imbc.com>
- [3] JeHun Choi (2013. April). *Boston Marathon Terror Suspect Arrest. SeoulNewspaper* [Online]. Available: <http://www.seoul.com>
- [4] Jeehee Lee, Hyunji Jung, Sangjin Lee, "Forensic Investigation Procedure for Real-time Synchronization Service", *Journal of Korea Institute of Information Security and Cryptology*, Vol. 22, No. 5, pp. 1363-1374, Dec. 2012.
- [5] GiHong Park, SiYoung No, "Cloud Services for the Forensic Aspects of the Investigative Methods", *Journal of Korea Industrial Information System Society*, Vol. 17, No. 1, pp. 39-46, Mar. 2012.
- [6] B. Carrier and E.H Spafford. "Getting Physical with the Digital Investigation Process". *International Journal of Digital Evidence*. Vol. 2, No. 2, Fall. 2003.

장 유 종 (Yu-Jong Jang)



2012년 2월 : 순천향대학교 정보보호학과(공학사)
 2013년 3월~현재 : 순천향대학교 정보보호학과 석사과정
 관심분야 : 디지털 포렌식, 스마트그리드, 소셜네트워크 서비스 보안, 암호 프로토콜 등

곽진 (Jin Kwak)



1994년~2006년 : 성균관대학교 학사, 석사, 박사
 2006년 4월 : 일본 큐슈대학교 시스템정보공학부 방문연구원
 2006년 8월~2006년 11월 : 일본 큐슈 시스템정보기술연구소 특별연구원
 2006~2007년 : 정보통신부 개인정보보호기획단 개인정보보호팀 통신사무관
 2007~현재 : 순천향대학교 정보보호학과 교수
 2007~2009년 : 정보통신연구진흥원 집필위원
 2009~2009년 : 순천향대학교 공과대학 교학부장
 2009~2010년 : 순천향대학교 정보보호학과 학과장
 2010~2010년 : 교육과학기술부 국가기술수준평가 전문위원
 현재 : 정보통신산업진흥원 기술평가위원, 사)국제정보능력평가원 쇼핑몰 플래너 자격 검정 출제 및 채점위원, 한국과학기술정보연구원 충남 과학기술 정보협의회 전문위원, 지식경제부 지식경제기술혁신평가단 평가위원, 순천향BIT 창업보육센터 센터장, 순천향대학교 중소 기업산학협력센터 센터장
 관심분야 : 암호프로토콜, 응용시스템보안, 개인정보보호, 정보보호제품평가, 클라우드 컴퓨팅 보안, 스마트워크 등