http://dx.doi.org/10.3745/KIPSTC.2011.18C.4.217

# iPhone의 SNS 데이터 수집 및 디지털 포렌식 분석 기법

정 진 형[†] · 변 근 덕[††] · 이 상 진[†††]


## 요 약

최근 다양한 스마트폰이 개발·보급되면서 SNS(Social Network Service)를 사용하는 사용자 또한 급격히 증가하였다. SNS는 기존 모바일 기기에서 수집할 수 있었던 문자 및 통화내역과 같은 단순한 사용자 데이터 외에도 주고 받은 사진 및 동영상, 음성쪽지나 위치 공유, 대화 내역 등 다양한 정보가 저장되어 디지털 포렌식 관점에서 유용한 데이터 획득이 가능하다. 본 논문에서는 최근 많이 사용하고 있는 아이폰을 대상으로 스마트폰에서 이용할 수 있는 SNS 클라이언트와 각 클라이언트 별로 수집할 수 있는 데이터의 종류를 살펴본다. 또, 각 데이터간의 연관관계를 통해 수집된 데이터의 효율적인 분석 방법을 제시한다.


**키워드 : 디지털 포렌식, 아이폰, 소셜네트워킹**

# Sensitive Privacy Data Acquisition in the iPhone for Digital Forensic Analysis

Jinhyung Jung[†] · Keunduck Byun[††] · Sangjin Lee[†††]


## ABSTRACT

As a diverse range of smartphones has been recently developed and diffused, the users of SNS (Social Network Service) also have been sharply increased. The SNS saves a variety of information such as exchanged pictures and videos, voice mails or location sharing, chat history, etc. as well as simple user data, so that the acquisition of data that are useful in the aspect of digital forensic is achievable. This thesis reviews the types of SNS that are available for the iPhone, a recent example of highly used smartphones, and types of data by each client. Also, efficient data analysis method for digital forensic investigations is suggested by analyzing the relationships within the collected data by each client.


**Keywords : Digital Forensics, iPhone, SNS**

## 1. 서 론

휴대용 모바일 기기는 사용자의 생활방식에 따라 고정되어 있는 PC보다 사용자와 더욱 밀접한 데이터를 저장한다. 통화기록이나 문자메시지 등은 누구와 전화통화를 하였고 어떤 메시지를 주고 받았는지 알 수 있으며, 일정과 주소록을 통해 저장되어 있는 지인들의 연락처와 사용자의 앞으로의 일정을 파악하는 것이 가능하다.

PC에서만 주로 사용하던 소셜 네트워크 서비스인 트위터나 페이스북 등을 스마트폰을 통해 사용이 가능해지면서 이런 SNS를 이용하는 사용자 또한 매우 증가하게 되었다. 특히, SNS는 사용자간에 공유한 사진 및 동영상, 위치정보, 그룹 채팅 및 대화내역 등을 저장함으로써 기존 모바일기기에서 수집할 수 있는 정보보다 더 다양한 사용자 데이터를 수집하는 것이 가능하다.

본 논문에서는 아이폰을 대상으로 하여 아이폰에서 이용할 수 있는 SNS 클라이언트의 종류를 살펴보고, 각 클라이언트에서 수집할 수 있는 데이터는 어떤 것들이 있는지, 수집한 정보를 토대로 디지털 포렌식 조사시 SNS 데이터의 활용 방안을 제시한다.

### 1.1 SNS 이용 실태 및 클라이언트 종류

SNS(Social Network Service)는 기존의 웹브라우저를 통한 서비스 외에도 전용 클라이언트 프로그램을 이용하여 서비스를 이용할 수 있다. 2010년 5월에 실시된 한국인터넷진흥원의 "인터넷 이용실태 조사"에 따르면 인터넷 이용자의

※ 본 연구는 한국연구재단을 통해 교육과학기술부의 바이오연구개발사업으로부터 지원받아 수행되었습니다(20100020634).
† 준 회 원 : 고려대학교 정보경영공학전문대학원 석사과정
†† 준 회 원 : 고려대학교 정보경영공학전문대학원 박사과정
††† 종신회원 : 고려대학교 정보경영공학전문대학원 교수
논문접수 : 2011년 3월 14일
수 정 일 : 1차 2011년 5월 14일
심사완료 : 2011년 5월 14일

〈표 1〉 국내·외 SNS 방문자수, 페이지뷰 1년간 추이 비교(출처:메트릭스, www.metrix.co.kr)

| 도메인 | 2009년 9월 | | 2010년 9월 | | 성장률 | | 서비스 시작 |
|---|---|---|---|---|---|---|---|
| | 방문자수 | 페이지뷰 | 방문자수 | 페이지뷰 | 방문자수 | 페이지뷰 | |
| cyworld.com | 22,079 | 11,792,018 | 24,653 | 9,211,123 | 11.7% | -21.9% | 1999년 9월 |
| me2day.net | 2,046 | 49,606 | 3,964 | 30,767 | 93.7% | -38.0% | 2007년 2월 |
| yozm.daum.net | - | - | 2,119 | 7,594 | N/A | N.A | 2010년 2월 |
| twitter.com | 1,379 | 9,302 | 8,654 | 175,576 | 527.7% | 1,787.5% | 2006년 7월 |
| facebook | 984 | 15,878 | 7,380 | 259,243 | 649.9% | 1,583.8% | 2004년 2월 |

65.7%가 SNS를 사용하는 것으로 조사되었으며[1], 2011년 현재 그 사용자 수는 계속 증가하고 있다. <표 1>은 인터넷 전문 조사기관인 메트릭스에서 2010년 10월에 조사한 SNS 종류별 방문자 수에 대한 변동추이이다[2]. 대표적인 국내·외의 5개 SNS 클라이언트를 대상으로 실시된 조사결과로 트위터, 페이스북의 높은 성장률을 확인할 수 있다.

본 논문에서는 <표 1>의 5개 클라이언트 외에 국내의 많은 사용자수를 확보하고 있는 네이트온의 스마트폰 버전과 카카오톡, 그리고 최근 다양한 서비스를 바탕으로 요즘(yozm)외에 새로이 서비스를 시작하고 있는 Daum의 마이피플 등 총 8가지 SNS 클라이언트를 분석대상으로 한다.

## 2. 아이폰 SNS 데이터 수집 방법

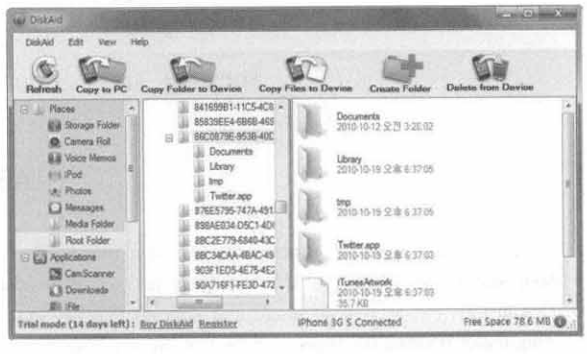
아이폰에 설치된 SNS 데이터를 수집하기 위한 방법은 크게 두 가지로 살펴볼 수 있다. 첫째로는 Jailbreak가 적용된 아이폰을 대상으로 하였을 때와 둘째로 백업데이터를 이용해 수집하는 방법이 있다. Jailbreak란 아이폰의 보안 기능을 해제하는 기법으로 Jailbreak가 적용되어 있다면 내부 데이터에 대한 직접적인 접근이 가능해진다. Jailbreak가 적용되어있지 않다면, 아이폰과 PC간 동기화 프로그램인 아이튠즈를 이용하여 내부 데이터를 PC에 백업할 수 있다. 이 백업데이터를 분석하면 SNS 데이터를 수집하는 것이 가능하다[3].


(그림 1) 아이폰 데이터 수집 개요

### 2.1 Jailbreak 적용된 아이폰의 SNS 데이터 수집

증거로 입수한 아이폰이 Jailbreak가 적용되어 있다면 iFunbox[4], DiskAid[5] 등의 프로그램을 이용하여 아이폰의 파일시스템에 직접 접근하여 내부 데이터를 수집할 수 있다.

(그림 2)는 Jailbreak가 적용된 아이폰을DiskAid를 이용하여 내부 파일시스템에 접근한 뒤 트위터 클라이언트의 데이터를 살펴보는 화면이다.




(그림 2) DiskAid를 이용한 파일시스템 탐색

### 2.2 백업데이터를 이용한 SNS 데이터 수집

일반 아이폰을 대상으로는 애플에서 제공하는 PC 동기화 프로그램인 아이튠즈를 이용해 내부 데이터를 PC에 백업하여 SNS 데이터를 추출할 수 있다. 백업데이터는 아이폰의 펌웨어인 iOS의 버전에 따라 저장방식이 다르다. 실제 저장되는 데이터는 동일하지만 이를 추출하기 위해 참조하는 메타데이터 파일에 차이가 있다.

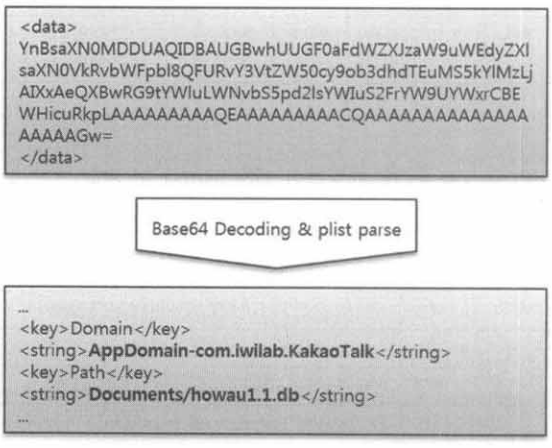
iOS 3.x 버전에서는 실제 데이터 파일에 .mddata 확장자가 추가되며 동일한 파일명의 .mdinfo 확장자를 지닌 메타데이터 파일이 한 쌍이 되어 각 하나의 백업파일에 대한 정보를 저장한다.

하지만 4.x 버전부터는 manifest.mbdx, manifest.mbdb 두 개의 파일로 모든 백업파일에 대한 정보를 저장한다.

#### 2.2.1 백업데이터의 생성

iOS의 각 버전에 따라 백업데이터를 가리키는 방법이 바뀌었을 뿐 실제 데이터의 파일명은 변동되지 않고 동일하다. 아이폰의 각 응용프로그램이나 내부 데이터들은 크게 8가지 도메인으로 구분할 수 있다.

"AppDomain", "HomeDomain", "KeychainDomain", "Managed PreferencesDomain", "MediaDomain", "RootDomain", "System PreferencesDomain", "WirelessDomain" 으로 분류될 수 있는데, 이 도메인명과 각 데이터의 경로명을 포함하여 SHA1 해쉬값이 백업데이터의 파일명을 결정한다[6].




(그림 3) iOS v3.x의 백업 메타데이터 파일 분석

iOS 3.x 버전에서는 .mdinfo 파일에 백업데이터의 메타정보를 저장하며, 애플의 파일 저장 포맷인 plist 구조를 갖고 있다. Property-List의 준말로 XML형식과 유사하게 각각의 키가 있고 그와 매치되는 값이 존재하거나 혹은 값만 존재하는 형태로 구성된다[7]. plist 파일포맷의 <data> 객체는 원본데이터가 Base64로 인코딩되어 저장되는데, mdinfo 파일의 <data> 값을 디코딩 하면 다시 별개의 plist 파일이 나타나게 되고 이 파일에 백업데이터의 실제 경로와 도메인 정보를 저장하고 있다.

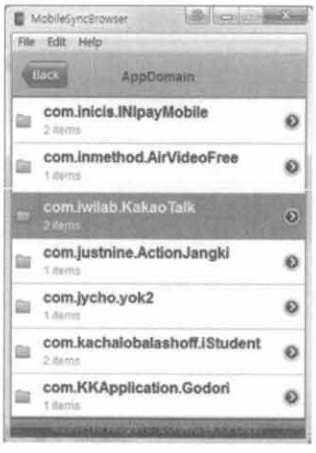
디코딩 후의 도메인과 경로 정보를 하이픈으로 조합하여 SHA1 해쉬값을 얻게 되면 다음의 결과가 나타난다.

AppDomain-com.iwilab.KakaoTalk-Documents/Talk.sqlite → (SHA1 Hash) d5bd128369e2a96f96e3314450a8955363f66035

iOS 4.x 버전에서는 각 백업데이터별로 메타 정보를 저장하던 .mdinfo 라는 구조가 사라지고 전체 백업데이터의 메타 정보를 manifest.mbdb 파일과 manifest.mbdx 두 개의 파일을 통해 관리하도록 변경되었다. 백업데이터의 원본 정보를 관리하는 방식만 변경되고 iOS 3.x 버전과 같이 데이터의 파일명의 변환 방법은 동일하기 때문에 버전에 따라 백업데이터의 파일명이 변경되지 않는다. 이는 아이폰 3GS와 아이폰 4에서도 동일하다.

백업데이터는 (그림 2)와 같이 Jailbreak가 적용된 아이폰의 내부 구조와 달리, 각 응용프로그램별로 트리 구조를 형성하고 있지 않고, 하나의 폴더에 모든 백업대상 파일이 저장된다. 그렇기 때문에 각 iOS 버전별 백업데이터의 메타파일을 분석하여 각 SNS 클라이언트의 데이터를 판별해야 한다.

MobileSyncBrowser는 아이튠즈를 통해 백업된 데이터를 분석하여 각각의 폴더로 구분하여 나타내어 준다[8].




(그림 4) MobileSyncBrowser

<표 2>는 운영체제별 아이폰 백업데이터의 경로이다.

〈표 2〉 운영체제별 아이폰 백업데이터 경로

| 운영체제 | 경 로 |
|---|---|
| Win XP | %USERPROFILE%\Application Data\Apple Computer\Mobile Sync\Backup |
| Win Vista&7 | %USERPROFILE%\AppData\Roaming\Apple Computer\Mobile Sync\Backup |
| Mac OS | /Library/Application Support/Mobile Sync/Backup |

## 3. SNS 데이터의 수집 및 분석

본 장에서는 각 클라이언트별로 디지털 포렌식 관점의 유용한 데이터는 어떤 것들이 존재하는지 조사하였다. 또한, 데이터 수집 방법에 따라 해당 데이터에 접근할 수 있는 데이터 경로와 각 파일명을 정리하였다. 데이터 경로는 각 응용프로그램의 루트로부터의 경로이고, 백업파일명은 iOS 4.x 버전의 백업데이터를 기준으로 나타내었으며 3.x 버전의 경우는 동일한 파일명의 .mddata 확장자를 가진 파일이 데이터 파일이다. 각 클라이언트별로 수집할 수 있는 데이터를 <표 3>과 같이 요약할 수 있다. SNS 클라이언트의 주요 데이터를 크게 "사용자 정보", "친구 목록", "메시지", "사진/미디어" 4가지로 분류하고 각 클라이언트별 고유한 데이터를 포함하여 수집할 수 있는 데이터와 수집할 수 없는 데이터를 O, X로 표시하였고, 해당 분류에 대한 전체 데이터를 수집하지 못하는 경우 △로 표시하였으며, 상세한 내역은 각 절에서 설명한다.

### 3.1 SNS 클라이언트별 데이터 수집

#### 3.1.1 싸이월드

싸이월드는 국내의 미니홈피 서비스를 아이폰에서 이용할 수 있는 응용프로그램으로 자신과의 일촌 목록을 관리할 수 있고 업로드한 사진 및 방명록 등을 열람할 수 있다.

〈표 3〉 SNS 클라이언트별 수집 데이터 종류

| 구분 | 싸이월드 / v.1.3.3 | | | | 미투데이 / v.1.8 | | | | Daum요즘 / v.1.2.4 | | | | 트위터 / v.3.2.2 | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 데이터 | 사용자 정보 | 친구 목록 | 메시지 | 사진/ 미디어 | 사용자 정보 | 친구 목록 | 메시지 | 사진/ 미디어 | 사용자 정보 | 친구 목록 | 메시지 | 사진/ 미디어 | 사용자 정보 | 친구 목록 | 멘션/ DM | 전체 메시지 | 사진/ 미디어 |
| 유무 | O | O | X | O | O | △ | X | O | O | O | O | O | O | △ | O | O | O |
| 구분 | 페이스북 / v.3.3.3 | | | | 네이트온UC / v.1.0.17 | | | | 카카오톡 / v.2.3 | | | | 마이피플 / v.2.0 | | | | |
| 데이터 | 사용자 정보 | 친구 목록 | 메시지 | 사진/ 미디어 | 사용자 정보 | 친구 목록 | 메시지 | 사진/ 미디어 | 사용자 정보 | 친구 목록 | 메시지 | 사진/ 미디어 | 사용자 정보 | 친구 목록 | 메시지 | 사진/ 미디어 | 음성 쪽지 |
| 유무 | O | O | △ | O | O | O | X | X | O | O | O | O | O | O | O | O | O |

〈표 4〉 미니홈피의 수집 데이터 및 경로

| 구 분 | | 경로(응용프로그램 루트) / 백업파일명 |
|---|---|---|
| 사용자 정보 | JB | Library/preferences/com.nate.minihompy.plist |
| | 백업 | cc1993f656f199b44f3b015c80fcf3d7d24817a2 |
| 친구목록 | | Documents/MiniHompy/[TID] |
| 사진/미디어 | | Documents/MiniHompy/[TID]/* |

미니홈피의 데이터는 Documents/MiniHompy 하위에 싸이월드의 개인 고유 번호인 tid 값으로 폴더가 생성되고 내부에는 방문한 사용자 미니홈피의 열람한 이미지 파일이 저장된다.

3.1.2 미투데이

미투데이는 NHN에서 운영하는 SNS로 메시지 내역은 저장되지 않고, 검색한 사용자의 정보와 사진 등이 저장된다.

〈표 5〉 미투데이의 수집 데이터 및 경로

| 구 분 | | 경로(응용프로그램 루트) / 백업파일명 |
|---|---|---|
| 사용자 정보 | JB | Library/Preferences/com.nhncorp.me2DAY.plist |
| | 백업 | f1012cea6e78e3f3ae241faa16d1c5eec895df40 |
| 검색ID목록 | | Library/Caches/me2DAY/faceImage/* |
| 사진/미디어 | | tmp/me2DAY/profileImage/me2day.net/images/user/[ID]/*.cache |

친구목록이 저장되지 않기 때문에 검색한 사용자의 정보만 파악이 가능하며, 프로필 이미지와 함께 캐쉬폴더에 저장된다.

3.1.3 Daum요즘

요즘(yozm)은 Daum에서 운영하는 SNS의 한 종류로 최근에는 마이피플이란 서비스도 지원하고 있다. 요즘(yozm)은 친구 목록과 메시지를 데이터베이스 파일로 저장한다. 하지만 친구 목록의 경우 모든 사용자의 목록이 저장되어 있는 것이 아니라 최근 메시지를 등록한 경우 확인할 수 있으며 해당 사용자의 프로필 이미지 URL이 DB에 함께 저장된다.

ImageCache의 사진 파일은 방문했던 사용자의 프로필 사진과 최근 받은 소식의 이미지 등이 저장된다.

〈표 6〉 Daum요즘의 수집 데이터 및 경로

| 구 분 | | 경로(응용프로그램 루트) / 백업파일명 |
|---|---|---|
| 사용자 정보 | JB | Library/Preferences/net.daum.yozm.plis |
| | 백업 | e82b91a282f74efafef591e53ce100f6e25b2dda |
| 친구목록 | JB | Documents/Yomamte.sql |
| | 백업 | 406cefcc95c117b83780a57ca58e0682d9bfe4c7 |
| 메시지 | JB | Documents/Yomamte.sql [message] |
| | 백업 | 406cefcc95c117b83780a57ca58e0682d9bfe4c7 |
| 사진/미디어 | | Library/Caches/ImageCache/* |

3.1.4 트위터

트위터는 페이스북과 더불어 전 세계적으로 대표적인 SNS 중 하나이다. 지인 또는 다른 사용자와 팔로우(follow)라는 개념을 도입하여 메시지를 주고 받을 수 있으며, 이런 메시지는 plist 구조로 저장하고 있다.

〈표 7〉 트위터의 수집 데이터 및 경로

| 구 분 | | 경로(응용프로그램 루트) / 백업파일명 |
|---|---|---|
| 사용자 정보 | JB | Documents/com.atebits.tweetie.application-state/app.state |
| | 백업 | eb8899d553cf563080453f9a366600de1dcf6286 |
| 멘션/DM | | Documents/com.atebits.tweetie.streams/[32bytes characters] |
| 전체메시지 | | Documents/com.atebits.tweetie.streams/[32bytes characters] |
| 사진/미디어 | | Library/Caches/com.atebits.tweetie.profile-images/* |

트위터의 메시지 특성상 쪽지 기능과 동일한 DM(Direct Message)와 친구 간에 주고 받는 공개 대화인 Mention 데이터는 전체 메시지와 별도로 저장되어 있다. 그리고 프로필 이미지의 경우는 Following과 Follower의 구분 없이 모두 저장된다.

3.1.5 페이스북

페이스북은 트위터와 함께 한글서비스를 지원하면서 국내 사용자 또한 급격히 증가하고 있는 SNS이다. 페이스북은 대화내역과 친구 목록을 파일로 저장하고 있다.

〈표 8〉 페이스북의 수집 데이터 및 경로

| 구 분 | | 경로(응용프로그램 루트) / 백업파일명 |
|---|---|---|
| 사용자 정보 | JB | Library/Preferences/com.facebook.Facebook.plist |
| | 백업 | 384eb9e62ba50d7f3a21d9224123db62879ef423 |
| 친구목록 | JB | Documents/friends.db |
| | 백업 | 6639cb6a02f32e0203851f25465ffb89ca8ae3fa |
| 사진/미디어 | | Library/Caches/Three20/* |

Three20 폴더에는 사진 데이터 외에 XML 파일 형식으로 대화내역이 함께 저장되어 있다.

3.1.6 네이트온UC

네이트온UC는 국내의 대표적인 메신져 서비스인 네이트온의 스마트폰용 클라이언트 프로그램으로 싸이월드와의 연동이 가능하며, 스마트폰을 이용해서 등록되어 있는 친구들과 대화 및 쪽지를 주고 받을 수 있다. 하지만 PC용 네이트온과 동일하게 스마트폰을 이용해 전송된 메시지 또한 네이트온 서버에 저장하고 있어 직접적인 확인이 불가능하다.

〈표 9〉 네이트온UC의 수집 데이터 및 경로

| 구 분 | | 경로(응용프로그램 루트) / 백업파일명 |
|---|---|---|
| 사용자 정보 | JB | Library/Preferences/com.nate.nateon.plist |
| | 백업 | 575308d6756147c7cbc5994ef765ce8aa746bc6b |
| 친구목록 | JB | Documents/UC.db |
| | 백업 | 2945a0d8601dbfcd4fc184384c0453c0e050cc4c |

네이트온UC의 경우는 쪽지나 대화내역은 저장되지 않지만 사용자 정보와 친구 목록이 상세하게 저장된다. 사용자 정보의 경우 자동 로그인 설정된 계정과 동기화 시간이 저장되며, 친구 목록은 싸이월드 정보, 전화번호, E-mail 등이 모두 기록된다.

3.1.7 카카오톡

카카오톡은 국내에서 개발되어 스마트폰 전용으로 서비스중인 SNS로써 많은 사용자 수를 확보하고 있다. 카카오톡은 하나의 데이터베이스 파일 내에 친구목록과 주고 받은 메시지, 그룹채팅의 정보를 모두 저장하고 있다.

〈표 10〉 카카오톡의 수집 데이터 및 경로

| 구 분 | | 경로(응용프로그램 루트) / 백업파일명 |
|---|---|---|
| 사용자 정보 | JB | Library/Preferences/com.iwlab.KakaoTalk.plist |
| | 백업 | 4903197cb3ac6b15b086afe9e437472614ef29e1 |
| 친구목록 | JB | Documents/Talk.sqlite |
| | 백업 | d5bd128369e2a96f96e3314450a8955363f66035 |
| 메시지 | JB | Documents/Talk.sqlite |
| | 백업 | d5bd128369e2a96f96e3314450a8955363f66035 |
| 사진/미디어 | | Library/Caches/Three20/[32bytes characters] |

사진 데이터는 페이스북과 동일하게 Three20 폴더에 이미지 파일이 저장된다.

3.1.8 마이피플

마이피플은 Daum에서 새로이 시작하는 SNS로 음성메시지를 주고 받을 수 있으며, Daum Map을 이용한 위치 공유 서비스를 지원하여 공유하고자 하는 위치정보를 주고 받을 수 있다. 이 외에도 마이피플은 다양한 정보를 저장하고 있는데 특히 아이폰의 주소록을 별도의 plist 파일로 저장하고 있는 것을 확인할 수 있다.

〈표 11〉 마이피플의 수집 데이터 및 경로

| 구 분 | | 경로(응용프로그램 루트) / 백업파일명 |
|---|---|---|
| 사용자 정보 | JB | Library/Preferences/net.daum.air21.plist |
| | 백업 | 45f054b67052e4637ee0908bbd969566e4bbb989 |
| 친구목록 | JB | Documents/myPeopleList.archive |
| | 백업 | ba08e750aa66a337c820dff7f33e391ab8471cc9 |
| 메시지 | JB | Documents/Air21-0.1.2.sqlite |
| | 백업 | ff97a3423571c6785a9fe2dc945f59ee16fb552b |
| 전체 주소록 | JB | Documents/allContactsList.archive |
| | 백업 | 305584c73efa66f168bf6105bf3c372a87f1f23c |
| 사진 | | Documents/*.png |
| 음성 쪽지 | | Documents/*.m4a |

또한, 아이폰의 주소록에서 마이피플을 사용하는 사용자들의 목록과 즐겨찾기에 등록되어 있는 사용자 목록을 별도로 관리하고 있다.

3.2 SNS 수집 데이터 분류

앞 절에서는 각 클라이언트별로 수집할 수 있는 데이터의 종류와 파일의 저장 위치를 살펴보았다. 본 절에서는 실제 디지털 포렌식 분석을 위해 의미 있는 데이터와 사건 수사에 도움이 될 정보는 어떤 것들이 있는지 살펴본다.

3.2.1 사용자 정보

사용자 정보는 각 클라이언트를 이용하기 위해 로그인하기 위한 계정 정보와 닉네임, E-mail, 전화 번호 등의 데이터를 일컫는다. 각 클라이언트별로 저장하고 있는 사용자 정보의 형태는 각기 다르지만, 이러한 계정 정보 등을 수집하게 되면, 이를 통해 다른 웹 서비스나 이 외의 SNS 클라이언트에서 사용하는 계정 정보를 유추할 수 있다.

(그림 5)는 네이트온UC에서 저장하고 있는 사용자 정보로써, 로그인 ID와 패스워드, E-mail 계정 등이 평문으로 저장되어 실제 값을 확인할 수 있다.

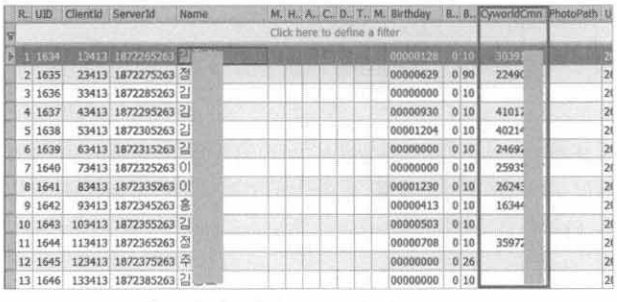
ID와 패스워드가 노출되기 때문에 네이트온UC에 접속하는 것은 물론, 저장되어 있는 E-mail 계정과 유사한 다른 클라이언트에서 위 인증정보를 통해 로그인을 시도해 볼 수 있다.


(그림 5) 네이트온UC의 사용자 정보

3.2.2 친구 목록 및 메시지

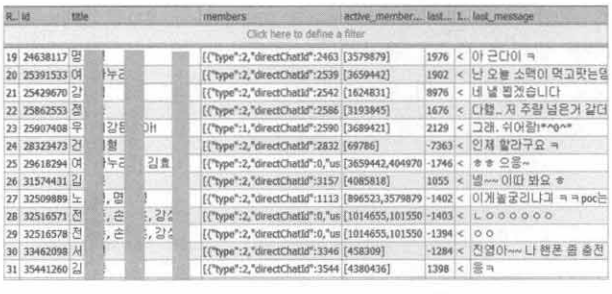
친구 목록과 메시지 내역은 기존 모바일 기기에서 사용하는 연락처나 SMS 메시지와 유사한 부분으로, 가장 최근에 어떤 SNS 클라이언트를 통해 누구와 대화를 나누었는지 알 수 있다. 특히 일부 클라이언트에서는 친구 목록 저장시 프로필 이미지를 같이 저장하기 때문에 지인의 모습까지 확인할 수 있다.

네이트온UC는 친구 목록에 싸이월드의 tid값을 저장하고 있어 연동된 미니홈피의 주소를 알 수 있다.




(그림 6) 네이트온UC의 친구 목록

CyworldCmn 필드의 값을 미니홈피 URL의 tid값에 입력하면 지인의 미니홈피를 확인할 수 있다. 카카오톡은 대화내역을 chat_id를 통해 관리하며 다중 대화의 경우 대화에 참여한 사용자들의 목록이 모두 저장되어 지인간의 관계를 파악할 수 있다.




(그림 7) 카카오톡의 대화 내역

트위터를 제외한 모든 SNS 클라이언트는 이런 대량의 데이터를 저장하기 위해 SQLite DB 포맷을 사용한다.

3.2.3 멀티미디어 데이터

아이폰을 이용해 촬영한 사진에는 GPS 정보가 기본적으로 포함되기 때문에 내장되어 있는 사진 보기를 통해 사진을 촬영한 위치를 파악할 수 있다. 하지만 GPS정보가 포함되어 있는 이미지라도 SNS 클라이언트를 통해 공유할 경우 GPS 정보뿐만 아니라 기본적인 EXIF 데이터까지도 제외된 상태로 저장되거나 혹은 PNG와 같은 별개의 이미지 포맷으로 변환이 된다. 그렇기 때문에 이미지의 GPS 정보를 활용한 사진 촬영 위치까지는 파악하기 어렵지만, 아이폰이 저장하는 이미지와는 별개로 각 클라이언트별 이미지 데이터를 저장 관리하기 때문에 아이폰의 사진이 삭제되었더라도 SNS를 통해 공유했던 이미지에는 영향이 없다.

사진 이외에도 촬영한 동영상을 SNS 클라이언트를 통해 지인들과 공유할 수 있으며, 이 또한 아이폰의 동영상과 별개로 저장이 된다. 아이폰의 동영상은 Apple Quicktime용 멀티미디어 포맷인 MOV 파일 포맷을 통해 저장되고 이와 동일한 포맷으로 저장되는 클라이언트도 존재하지만, m4v와 같은 MPEG 비디오 포맷으로 저장하는 경우도 있다.

마지막으로 음성 데이터가 있는데, Daum의 마이피플에서는 음성 쪽지 기능을 통해 녹음한 음성을 상대방에게 전송할 수 있다. 최대 30초간 녹음할 수 있으며, 데이터는 MPEG 오디오 포맷인 m4a 파일포맷으로 저장된다.

3.2.4 기타 데이터

앞서 언급한 데이터 분류 외에도 최근의 SNS는 다양한 데이터를 공유할 수 있는데, Daum의 마이피플에서는 위치정보를 공유할 수 있는 장소 공유 기능을 제공한다. 이 장소 공유 기능은 아이폰의 GPS 정보를 이용해 Daum Map에 해당 위치를 표시해 주는 것으로 URL을 통해 E-mail이나 다른 사용자에게도 전송할 수 있다.


(그림 8) 마이피플의 장소공유

장소 공유는 특정 포맷으로 저장되는 것이 아니라 (그림 8)과 같이 GPS 좌표가 포함된 URL 정보를 대화내역 데이터베이스에 저장하고 있다.

## 4. SNS 데이터에 대한 디지털 포렌식 분석

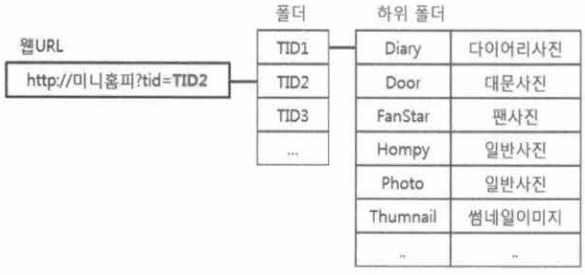
3.2절에서는 수집된 데이터에 대한 큰 분류를 살펴보았다. 본 장에서는 각 클라이언트별로 저장되는 데이터 내의 연관

관계를 분석하여 디지털 포렌식 조사시 효과적인 데이터 분석 방법을 제시한다.

### 4.1 SNS 클라이언트별 데이터 연관관계 분석

#### 4.1.1 싸이월드

싸이월드는 사진 데이터외의 다른 정보는 저장되지 않는다. 각 사진 폴더별로 구분되어 저장되며, 방문한 사용자의 폴더가 모두 공개되어 있어도 열람하지 않으면 정보는 저장되지 않는다. 구조를 살펴보면 (그림 9)와 같다.




(그림 9) 싸이월드의 데이터 저장 구조

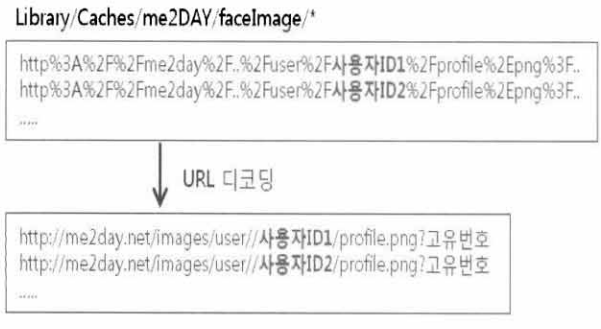
<표 4>에서 언급한 Documents/MiniHompy의 경로에는 8자리 숫자로 생성된 폴더들의 목록이 있으며, 이 숫자가 의미하는 값은 싸이월드에 가입한 사용자의 고유번호인 tid 값이다. tid 값은 다음의 URL을 이용하여 해당 사용자의 미니홈피에 접속할 수 있다.

http://minihp.cyworld.com/pims/main/pims_main.asp?tid=TID2

각 tid 폴더별로 하위에는 메인사진, 다이어리, 사진첩 등에 업로드 되어있는 이미지 중 열람했던 이미지만 저장된다.

#### 4.1.2 미투데이

미투데이는 검색한 사용자에 대해서는 정보를 파악할 수 있지만 친구관계의 판단은 할 수 없다. <표 5>의 "검색ID목록" 항목에 faceImage라는 폴더가 존재하는데 이 경로에 저장되는 파일은 모두 PNG 파일로써, 파일명의 의미는 웹에서 확인할 수 있는 URL 인코딩 값을 나타낸다. 각 PNG파일은 검색한 사용자의 프로필 이미지로써 해당 사용자의 판별은 (그림 10)과 같이 할 수 있다.

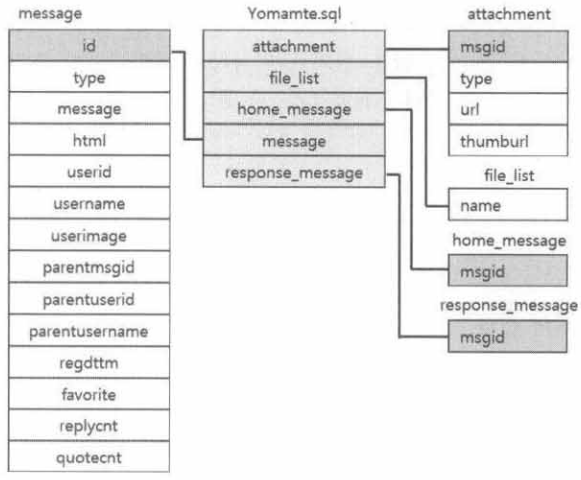



(그림 10) 미투데이의 사용자 검색 목록 판별

#### 4.1.3 Daum요즘

Daum요즘에는 Yomamte.sql 파일이 존재하여 첨부 이미지나 등록된 친구들과의 메시지 내역을 관리한다. Yomamte.sql 파일의 구조는 (그림 11)과 같다.

Yomamte.sql 데이터베이스는 attachment, file_list 등 5개의 테이블로 이루어져 있으며, file_list 테이블을 제외한 각각의 테이블에는 공통적인 msgid 값을 갖는다. 이 msgid값을 통해 각 테이블 간의 연관관계를 찾을 수 있다. message 테이블의 id값 "17957326"인 메시지는 attachment 테이블의 동일한 msgid 레코드에서 url 컬럼의 값을 통해 (그림 12)와 같이 첨부된 이미지를 확인할 수 있다.




(그림 11) Daum요즘의 데이터베이스 구조

(그림 12) msgid를 이용한 연관관계 분석

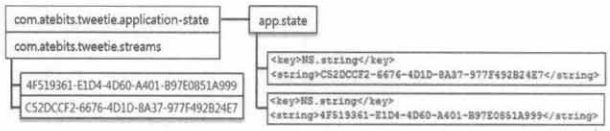
#### 4.1.4 트위터

트위터는 정보를 데이터베이스 파일로 관리하지 않기 때문에 데이터 저장형태가 체계적이지 않다. 트위터의 메시지와 대화내역은 총 3개의 plist 파일로 구분되어 저장된다. <표 7>의 사용자 정보 파일인 app.state파일은 트위터 클라이언트를 이용하고 있는 사용자 정보가 저장되어 있다. 또한, 다른 사용자와 주고 받은 최근 메시지와 Direct Message가 저장되는데, 이 형태는 plist의 일반적인 구조인 Key와 Value의 형태가 아니라 단순한 문자열로 저장된다.

app.state파일에는 모든 메시지와 대화내역이 저장되지 않는다. 전체 메시지 내역인 타임라인 데이터를 저장하는 파일과 Direct Message나 등록된 친구 간에 나눈 대화만 저

<string>http://a1.twimg.com/profile_images/12[redacted]7/ProfilePhoto_normal.png</string>
<string>Nam</string>
<string>Haengun-dong, Gwanak-gu, Seoul</string>
<string>1984/프로그래밍/백열등/Coffee/Rock/책읽기/쓸데없는삶에대한고찰</string>

(그림 13) 트위터의 사용자 정보

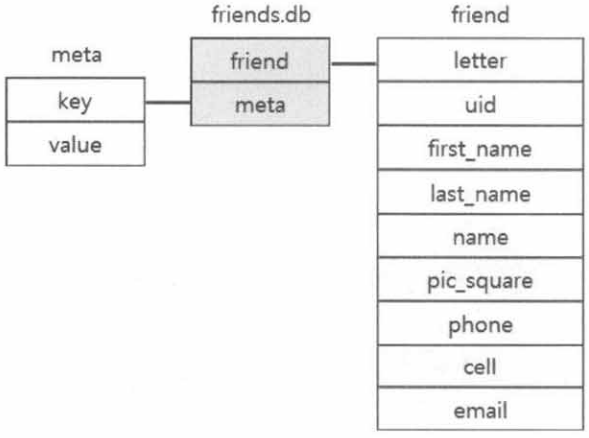



(그림 14) App.state파일과 메시지 파일과의 관계

장하는 형식이 존재하는데 해당 파일명은 app.state 파일내의 NS.String 키 값을 살펴보면 각각의 파일이름이 저장되어 있다. 저장 방식은 app.state 와 동일하게 plist 파일 형식을 사용한다.

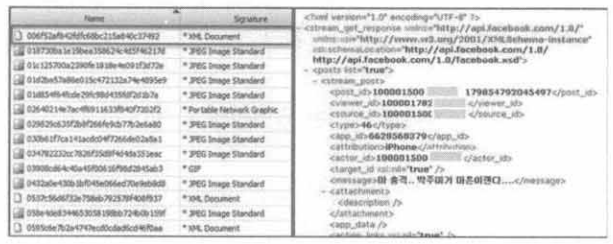
4.1.5 페이스북

페이스북은 friends.db라는 데이터베이스 파일을 이용해 친구 목록을 관리한다. "meta", "friend" 2개의 테이블로 구성되어 있다.




(그림 15) 페이스북의 데이터베이스 구조

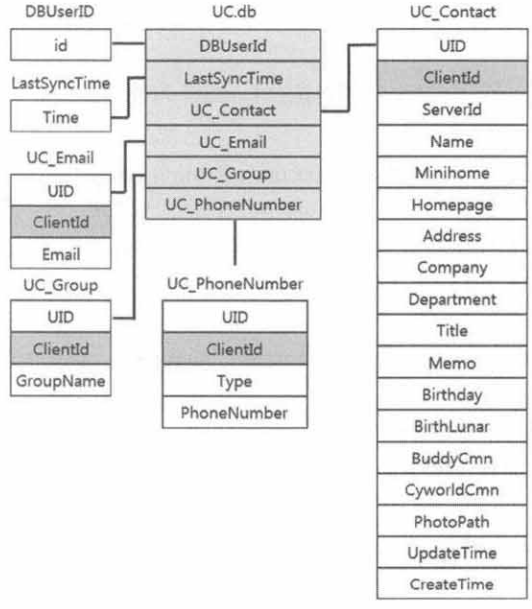
Meta 테이블에는 버전 정보만 명시되어 있고, 친구 목록은 friend 테이블에 저장되어 있다. 이름과 프로필 이미지 URL을 알 수 있지만, e-mail 주소와 전화번호는 평문이 아니기 때문에 식별하기 어렵다. 다만, Library/Cache/Three20 폴더 내에는 32byte 길이의 문자열로 파일이 생성되는데, JPG, GIF, PNG, XML 파일 등이 혼재하여 저장된다. (그림 16)은 페이스북을 이용하며 생성되는 임시 캐쉬 파일의 목록이며, XML 파일은 페이스북 클라이언트를 통해 탐색한 글, 사진, 프로필 등의 정보를 모두 저장한다. 작성된 글은 등록된 친구의 글이라면 <actor_id> 태그값과 friend 테이블의 uid를 비교하여 글 작성자와의 관계를 파악할 수 있다. 하지만 임시 파일은 백업되지 않으므로 Jailbreak가 적용 되어 있는 아이폰의 경우에만 수집이 가능하다.




(그림 16) 대화내역을 저장하고 있는 캐쉬 파일

4.1.6 네이트온UC

네이트온은 UC 버전으로 업데이트 되면서 데이터베이스 파일을 통해 친구 목록을 관리하고 있다. 총 6개의 테이블로 구성되어 있으며, 네이트온의 주소록을 같이 저장하고 E-mail과 전화번호를 별도의 테이블로 분리하여 저장한다.



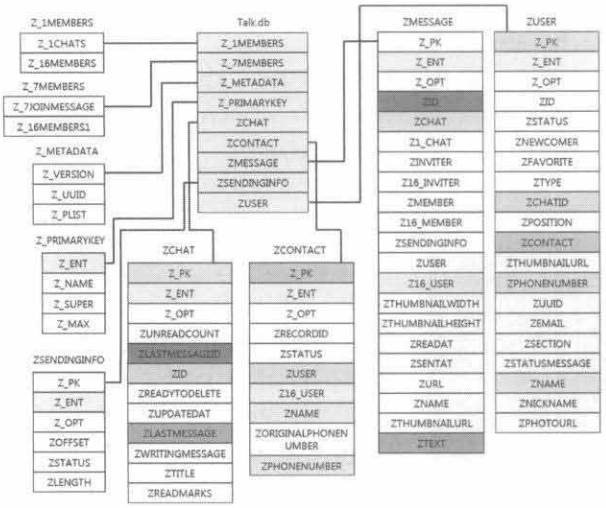

(그림 17) 네이트온UC의 데이터베이스 구조

각 테이블에 저장되어 있는 값은 ClientId 값을 통해 서로 매치되며, UID 는 변수이기 때문에 참조할 수 없다. 앞서 Cyworld에서 tid값을 이용해 해당 사용자의 미니홈피 주소를 열람할 수 있었는데 CyworldCmn 컬럼의 값이 tid 값과 동일하다.

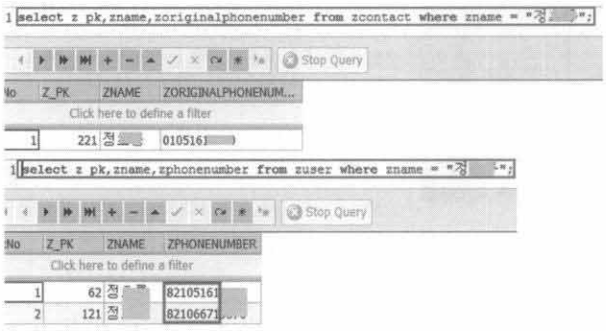
4.1.7 카카오톡

카카오톡은 데이터베이스 파일을 통해 많은 정보를 저장하고 있으며, (그림 18)과 같이 다른 테이블에 동일한 컬럼이 존재하며, 이를 통해 각 테이블간의 연관관계를 파악할 수 있다.

ZCONTACT 테이블은 실제 클라이언트 상에서는 보이지 않지만 아이폰의 주소록을 저장하고 있는 테이블이며, ZUSER 테이블은 주소록 상에서 카카오톡을 이용하고 있는 사용자들에 대한 목록이다. 카카오톡은 기존에 등록되어 있



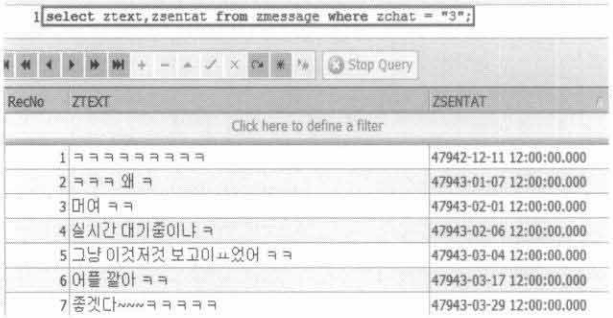

(그림 18) 카카오톡의 데이터베이스 구조




(그림 19) ZUSER 테이블의 연락처 변경 흔적

는 친구의 연락처가 변경되었을 경우 유효하지 않은 친구로 표시한다. 사용자가 이런 유효하지 않은 친구를 목록에서 삭제하더라도 (그림 19)와 같이 ZUSER 테이블에는 삭제된 기록이 존재한다.

ZCHAT 테이블과 ZMESSAGE 테이블은 대화방과 대화 메시지가 분리되어 저장된 개념이다. ZCHAT 테이블의 ZLASTMESSAGE 값은 ZMESSAGE 테이블의 여러 ZTEXT 값 중 하나와 매치되는 칼럼이다. 만약 ZMESSAGE 테이블의 메시지 중 특정 대화내역을 알고자 한다면, (그림 20)과 같은 쿼리를 사용할 수 있다.



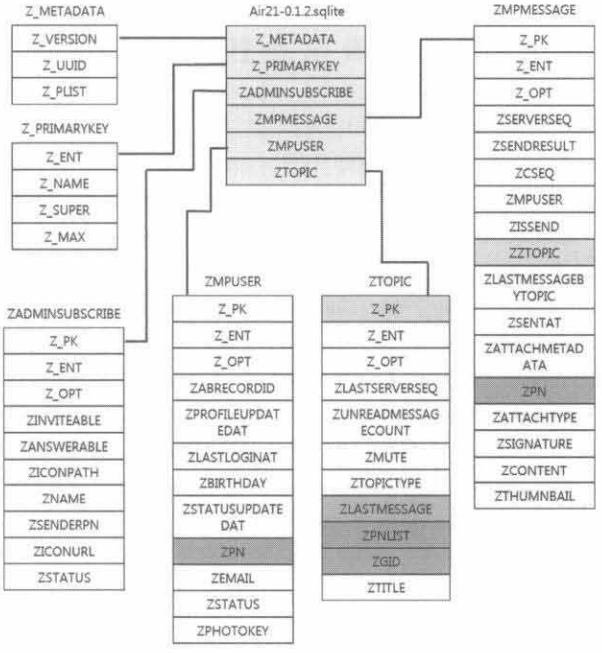

(그림 20) 효과적인 조사를 위한 쿼리 실행

Z_PRIMARYKEY 테이블에서는 각 테이블에서의 주요한 값들에 대한 통계를 가지고 있다.

### 4.1.8 마이피플

마이피플 역시 카카오톡과 유사한 테이블명 구조를 가지고 있는데 이는 iOS SDK를 이용해 데이터베이스를 모델링 할 때의 특징으로 인해 동일한 테이블명과 유사한 컬럼명을 갖는다[9].

마이피플은 지원하는 기능은 많지만 데이터베이스 구조는 단순하다. 파일을 저장하는 것 역시 데이터베이스 파일과 동일한 폴더에 모든 파일이 동시에 저장된다. 마이피플이 지원하는 주요 기능은 장소공유, 음성쪽지, 최근 업데이트 후 추가된 무료통화 기능 등이 있다. 각 기능의 사용 여부에 대해서는 ZMPMESSAGE 테이블에 모두 기록되며, 녹음된 음성파일, 다운로드 한 사진 및 동영상도 모두 Documents 폴더에 저장된다. 마이피플은 ZTOPIC 테이블을 이용해 카카오톡과 비슷한 개념인 대화방을 관리한다. 관리자에 의해 전달 받는 메시지는 ZADMINSUBSCRIBE 테이블을 별도로 두고, 대화내역은 ZMPMESSAGE, 대화상대와 친구목록은 ZMPUSER에서 휴대폰 번호인 ZPN칼럼을 이용해 조회할 수 있다.




(그림 21) 마이피플의 데이터베이스 구조

(그림 8)에서도 보았듯이, 마이피플의 위치공유 서비스는 GPS 정보와 함께 웹을 통해 바로 확인할 수 있다. 이 기능은 현재 위치를 저장하는 것이 아니라 공유하고자 하는 장소를 지도에 표시하여 좌표 값을 전송한다. 장소공유와 무료통화 기능의 저장형태는 데이터베이스 파일의 ZMPMESSAGE 테이블내에 "[장소 공유] 주소 URL"과 "XX초 무료통화" 형식으로 각 기능의 사용여부를 표시한다.

## 5. 결 론

스마트폰의 보급률 증가는 SNS의 사용자 증가와 아주 밀접한 관계가 있다. 높은 휴대성은 물론이고 기존의 SMS나 멀티미디어 데이터 공유를 위한 MMS보다 훨씬 저렴한 비용과 다양한 데이터 요금제로 인해 모바일 인터넷의 사용률과 함께 사용자간의 연락 및 대화 수단에서 SNS가 차지하는 비중은 매우 높다고 할 수 있다.

본 논문에서는 국내에서도 많은 사용자를 확보하고 있는 아이폰을 대상으로 SNS 클라이언트 종류와 데이터의 수집 및 분석 방법을 살펴보았다. 특히 수집된 파일과 데이터베이스 내에서 각 테이블과 컬럼을 분석하여 데이터간의 연관성을 보이고, 의미 있는 데이터를 산출하기 위한 조사 방법을 제시하였다.

기존의 모바일 기기에서 수집할 수 있는 SMS나 연락처, 통화 목록 이외에 SNS 정보를 수집하게 되면 사용자에 대해 더 자세한 정보와 주변 지인과의 사회적, 인적 관계 등을 효과적으로 분석할 수 있다.

SNS 사용증가와 함께 디지털 포렌식 조사시 SNS 클라이언트에 대한 분석이 더욱 중요해지고 있다. 본 논문은 이에 대한 기초 연구 자료로 활용 될 수 있을 것이다.

## 참 고 문 헌


[1] 한국인터넷진흥원, "2010년 인터넷이용실태조사 요약보고서", KISA-2010-0022, 2010년 12월.

[2] 메트릭스, "국내외 SNS 방문자수, 페이지뷰 1년간 추이 비교", 2010년 10월.

[3] i-FunBox, ifunbox.dev, (http://www.i-fun box.com)

[4] DiskAid, DigiDNA, (http://www.digidna. net/products/diskaid/download)

[5] "iPhone 및 iPod Touch : 백업에 관하여", http://support.apple.com/kb/HT1766

[6] Adam Crosby, "iPhone Forensics, sans iPhone", March, 2010.

[7] Property List Programming Guide, Apple, http://developer.apple.com/library/ios/documentation/Cocoa/Conceptual/PropertyLists

[8] MobileSyncBrowser, Vaughn S. Cordero, (http://mobilesyncbrowser.com)

[9] Core Data Tutorial for iOS, Apple, http://developer.apple.com/library/ios/documentation/DataManagement/Conceptual/iPhoneCoreData01



### 정 진 형

e-mail : blueliony@gmail.com

2008년 국립목포대학교 정보보호학과(학사)

2009년~현 재 고려대학교 정보경영공학전문대학원 석사과정

관심분야 : 디지털 포렌식, 모바일 포렌식



### 변 근 덕

e-mail : gdfriend@korea.ac.kr

2004년 아주대학교 정보및컴퓨터공학과 (학사)

2006년 고려대학교 정보경영공학전문대학원 (석사)

2006년~현 재 고려대학교 정보경영공학전문대학원 박사과정

관심분야 : 임베디드 포렌식, 역공학



### 이 상 진

e-mail : sangjin@korea.ac.kr

1987년 고려대학교 수학과(학사)

1989년 고려대학교 수학과(이학석사)

1994년 고려대학교 수학과(이학박사)

1989년~1999년 ETRI 연구원

1999년~현 재 고려대학교 정보경영공학전문대학원 교수

관심분야 : 디지털 포렌식, 모바일 포렌식, 심층 암호, 해쉬 함수