iOS5 신규 애플리케이션의 스키마 분석을 통한 포렌식 정보 획득 연구

이규원*, 양승제*, 장태주*, 윤영태*, 손기욱*
*한국전자통신연구원 부설연구소
e-mail:gwlee79@gmail.com

A Study on Forensic Information Aquisition with Schema Analysis for Newly Added Applications in iOS5

Gyu-Won Lee*, Seung-Jei Yang*, Taejoo Chang*, Young-Tae Yun*, Ki-Wook Sohn*
*The Attached Institute of ETRI

요 약

iOS5 소프트웨어가 업데이트되면서 기존과 비교하여 많은 새로운 기능들이 추가되었다. 이 기능들 중에는 사용자로 하여금 메시지와 계정 정보 등 포렌식 관점에서 중요한 정보들이 저장될 수 있는 애플리케이션들이 존재한다. 포렌식 수사에서 애플리케이션에 저장된 정보들은 사건 해결을 위한 중요한 단서가 되기도 한다. 따라서 본 논문에서는 iOS5에 새롭게 추가된 기능들 중에서 포렌식 정보들이 저장될 수 있는 애플리케이션들을 선별하고 스키마 분석 및 질의를 통하여 그 정보들을 획득 할 수 있음을 증명한다.

1. 서론

iOS5는 기존 iOS4와 비교하여 많은 기능적인 차이를 가지고 있다. 다른 iOS5 사용자와 무제한으로 문자 메시지, 사진, 비디오를 주고받을 수 있는 iMessage가 새롭게 추가되었고, 클라우드 서버를 이용하여 맥, 아이패드, 아이폰, 아이팟 터치 등 애플의 제품들끼리 데이터를 연동할 수 있게 하는 iCloud 기능이 추가되었으며, 날짜와 장소에 대한 일정을 입력하고 미리 알림 기능을 설정하면, 원하는 날짜와 장소에서 알림을 표시하는 미리 알림 기능이 추가되었다. 그리고 잡지와 신문 등 구독하고 있는 모든 앱을 한 곳에서 읽을 수 있는 뉴스 가판대가 추가되었고, 설정에서 한 번 로그인하면 사파리, 사진, 카메라, YouTube, 지도에서 곧바로 트윗을 올릴 수 있는 트위터가 iOS5에 기본으로 내장되었다. 또한 사용자에게 들어오는 문자, 이메일, 친구요청 등 정보를 빠르게 확인할 수 있는 알림 센터 기능 외에도 많은 다양한 기능들이 업데이트 되었다. 업데이트 항목들 중에는 단순히 기존의 버그 수정 및 사용자의 편의 기능을 향상시킨 것들이 많이 포함되어 있지만 포렌식 정보를 담을 수 있는 애플리케이션 또한 존재한다.

포렌식 수사에서는 이들 애플리케이션에 저장된 정보가 사건 해결의 결정적 증거로 활용되기도 한다.

따라서 본 논문에서는 iOS5에 새롭게 추가된 여러 기능들 중에서 포렌식 정보들을 저장할 수 있는 애플리케이션들에 대해서 분석한다.

2장에서 데이터 획득 방법을 알아보고, 3장에서 주요 애플리케이션들을 분석한다. 그리고 4장에서 결론을 맺는다.

2. 데이터 획득 방법

신규 애플리케이션들을 분석하기 위해서는 먼저 데이터를 획득해야만 한다. 데이터를 획득하는 방법으로는 활성 데이터를 획득하는 방법과 물리 이미지 전체를 덤프하는 방법이 존재한다.

2.1 활성 데이터 획득

활성 데이터를 획득하는 방법에는 iTunes 백업을 이용하는 방법과 Mobile Device Library의 AFC(Apple File Connection)[1]를 이용하는 방법이 있다. iTunes 백업은 AppleMobileBackup 프로그램을 이용하여 데이터들을 로컬 PC에 백업하는 방법으로 백업 데이터에 대한 메타 정보 및 데이터는 iOS3.x와 iOS4.x[2, 3] 그리고 iOS5.x 등 버전에 따라 차이가 있다. AFC를 이용하는 방법은 USB 케이블을 통해 로컬 PC에 파일을 추출할 수 있지만 접근에 대한 제한이 있으므로 탈옥(jailbreak)을 해야 한다. 탈옥을 할 경우 iTunes 백업과 달리 사용자 영역의 데이터뿐만 아니라 시스템 영역의 데이터까지 모두 획득할 수 있다. 그러나 비할당 영역의 데이터는 획득할 수 없다. 이 영역의 데이터를 획득하기 위해서는 물리 이미지 덤프가 필요하다.

2.2 물리 이미지 덤프

물리 이미지를 덤프하기 위해서는 iOS에 대한 탈옥이 선행되어야 한다. iOS5는 공개된 지 불과 1주일여 만에 아이폰 데브팀(iPhone Dev-Team)에 의해서 반탈옥(tethered jailbreak) 되었다. 반탈옥이란 재부팅 시 다시 순정모드로 돌아가는 현상을 의미한다. 반탈옥을 하기 위해서는 Redsn0w[4] 도구를 이용하면 되고 사용 방법 또한 간단하다. 일단 탈옥이 완료되면 MPE+[5], iXAM[6] 등 상용 소프트웨어를 이용하여 물리 이미지 덤프가 가능하고, iFunBox[7]와 같은 공개 소프트웨어를 통해서도 파일 추출이 가능하다. 덤프된 이미지는 파일 시스템 분석을 통하여 파일을 추출할 수 있고, 파일 분석을 통하여 필요한 정보를 획득할 수 있다. 그리고 이미지의 비할당 영역에서는 카빙(Carving) 기술을 이용하여 삭제된 데이터의 복구가 가능하다.

3. 애플리케이션 분석

본 장에서는 2장의 활성 데이터 획득을 통해 얻어진 iMessage 파일과 iCloud 계정 정보 파일, 미리 알림 데이터가 저장된 파일에 대해서 분석하고, 데이터들이 실제로 어떻게 존재하는지 확인한다.

3.1 iMessage

iMessage는 셀룰라 네트워크 및 Wi-Fi가 지원되는 환경이라면 iOS5를 사용하는 사용자간에 무료로 문자 메시지, 사진, 비디오를 주고받을 수 있다. 그리고 전송 확인 및 읽음 확인 기능을 통해 메시지를 추적할 수 있게 되었다. 이 메시지들은 <표 1>과 같이 sqlite 데이터베이스에 저장이 된다. 메시지들이 저장되는 파일과 위치는 다음과 같다.

<표 1> 파일 이름 및 저장 위치

파일 이름	저장 위치
sms.db	/var/mobile/Library

iMessage는 message 테이블과 madrid_attachment 테이블 그리고 madrid_chat 테이블과 연계되어 있다. iMessage 정보는 message 테이블에 저장이 되고, iMessage 첨부파일은 madrid_attachment 테이블에 저장된다. 그리고 madrid_chat 테이블에는 iMessage 송수신자의 채팅 정보가 저장된다. iMessage, 첨부파일, 채팅의 주요 컬럼 정보는 각각 <표 2>, <표 3>, <표 4>와 같다.

madrid_attachment 테이블의 attachment_guid 컬럼은 message 테이블의 madrid_attachmentInfo 컬럼과 연계되어 있고, madrid_chat 테이블의 account_id는 message 테이블의 madrid_account_guid와 연계되어 있다. 따라서 위 연관 관계를 이용하면 해당 메시지에 대한 첨부파일과 채팅 정보를 얻을 수 있다.

<표 2> message 테이블 정보

컬럼명	타입	설명
date	integer	생성 날짜
text	text	메시지
subject	text	제목
madrid_handle	text	송신자
madrid_account	text	계정
madrid_flags	integer	송수신 여부
madrid_attachmentInfo	blob	첨부파일
is_madrid	integer	여부
madrid_date_read	integer	읽은 날짜
madrid_date_delivered	integer	전송된 날짜
madrid_account_guid	text	계정 guid

<표 3> madrid_attachment 테이블 정보

컬럼명	타입	설명
attachment_guid	text	첨부파일 guid
created_date	integer	생성 날짜
filename	text	첨부파일 이름
mime_type	text	MIME 타입

<표 4> madrid_chat 테이블 정보

컬럼명	타입	설명
account_id	text	iMessage 계정 id
chat_identifier	text	대화상대 번호
guid	text	대화상대 guid 번호
account_login	text	iMessage 계정 로그인 번호

(그림 1)은 iMessage에 대한 질의 결과 화면으로 질의 문장은 다음과 같다.

Query = "select date, text, subject, madrid_handle, madrid_account, madrid_flags, madrid_attachmentInfo, is_madrid, madrid_date_read, madrid_date_delivered, madrid_account_guid from message where is_madrid = 1";

date	text	subject	madrid_h...	madrid_acc...	madrid_flags
341932160	공짜 iMessage		+8210925...	p:+8210542...	12289
341932223	유후!		+8210925...	p:+8210542...	36869
341932228	ㅎㅎ		+8210925...	p:+8210542...	36869
341932160	占쎈쐺?		+8210925...	p:+8210542...	12289
342079360	ㅋㅋ		+8210925...	p:+8210542...	12289
342079744	전송 테스트		+8210925...	p:+8210542...	12289
342079919	나도 전송	제목도 보냄	+8210925...	p:+8210542...	36869
342080256	아이 메시지		+8210925...	p:+8210542...	12289
342080782	송신1		+8210925...	p:+8210542...	36869
342080788	송신2		+8210925...	p:+8210542...	36869
342331904	泥⑥??똣...	첨부	+8210925...	p:+8210542...	12289
342930426	hello~		+8210925...	p:+8210542...	36869
342930432	헬로~		+8210925...	p:+8210542...	12289

(그림 1) iMessage 질의 결과 화면

3.2 iCloud

iCloud는 클라우드 서버에 사용자마다 기본으로 5GB의 저장 공간을 할당해주고 백업을 할 수 있도록 지원한다. 저장 공간이 더 필요할 경우 '추가 저장 공간 구입'을 하면 된다. iCloud에는 메일, 연락처, 캘린더, 미리 알림, 책갈피, 메모, 사진스트림, 도큐먼트 및 데이터를 저장할 수 있다. 클라우드 서버에 접속을 하기 위해서는 iCloud 계정 정보가 필요하다. 이 정보들은 plist 파일로 저장이 되며 <표 5>와 같이 저장되어 있다.

<표 5> 파일 이름 및 저장 위치

파일 이름	저장 위치
com.apple.coreservices.appleidauthenticationinfo.plist	/var/mobile/Library/Preferences

iCloud 계정 정보는 Accounts 키에 저장되어 있고, 인증서 정보를 가지고 있는 AuthCertificates 키와 연계되어 있다. iCloud 계정 정보와 인증서의 주요 컬럼 정보는 각각 <표 6>, <표 7>과 같다.

<표 6> Accounts 정보

키	타입	설명
AppleID	string	애플 아이디
CreationDate	date	계정 생성 날짜
HashedPasswordRef	data	해시 패스워드 참조
LastSuccessfulConnect	date	마지막 연결 성공 날짜
ModificationDate	date	수정 날짜
ValidationDate	date	유효 날짜
EncDsId	string	디지털 서명 암호화 아이디

<표 7> AuthCertificates 정보

키	타입	설명
AuthCertificates's Key	dict	디지털 서명 암호화 아이디
CertStatus	string	인증서 발행 여부
CertificatePrivateKeyReference	data	인증서 개인키 참조
CertificateReference	data	인증서 참조
CreationDate	date	인증서 생성 날짜
Expires	date	인증서 만료 날짜
IntermediateCertificateReference	data	중간 인증서 참조
ModificationDate	date	수정 날짜
NextRenewalAttempt	date	다음 갱신 시도 날짜
SericalNumber	string	시리얼 번호
EncDsId	string	디지털 서명 암호화 아이디

Accounts 정보의 인증서 정보는 디지털 서명을 암호화하여 EncDsId 키에 저장하고 있고, 그 키는 AuthCertificates 정보의 키, EncDsId 키와 상호 일치한다. PlistEditor[8]로 분석한 결과 iCloud에 대한 사용자의 계정 정보 및 인증서 정보는 각각 (그림 2), (그림 3)과 같이 저장되어 있다.

```
<key>Accounts</key>
<dict>
  <key>forener2527@me.com</key>
  <dict>
    <key>AppleID</key>
    <string>forener2527@me.com</string>
    <key>CreationDate</key>
    <date>2011-11-08T03:25:22Z</date>
    <key>Dirty</key>
    <false/>
    <key>HashedPasswordRef</key>
    <data>
    Z2VucAAAAAAAAAAd
    </data>
    <key>LastSuccessfulConnect</key>
    <date>2011-11-14T00:05:04Z</date>
    <key>ModificationDate</key>
    <date>2011-11-14T00:05:07Z</date>
    <key>ValidationDate</key>
    <date>2011-11-14T00:05:04Z</date>
    <key>encDsId</key>
    <string>38504b674e2f524c334c586e46474f594b33773432673d3d</string>
  </dict>
</dict>
```


(그림 2) 계정 정보

```
<key>AuthCertificates</key>
<dict>
  <key>38504b674e2f524c334c586e46474f594b33773432673d3d</key>
  <dict>
    <key>CertStatus</key>
    <string>CERT_ISSUED</string>
    <key>CertificatePrivateKeyReference</key>
    <data>
    a2V5cwAAAAAAAAAT
    </data>
    <key>CertificateReference</key>
    <data>
    Y2VydAAAAAAAAAAK
    </data>
    <key>CreationDate</key>
    <date>2011-11-14T00:05:07Z</date>
    <key>Dirty</key>
    <true/>
    <key>Expires</key>
    <date>2012-11-06T18:15:48Z</date>
    <key>IntermediateCertificateReference</key>
    <data>
    Y2VydAAAAAAAAAAL
    </data>
    <key>ModificationDate</key>
    <date>2011-11-14T00:05:07Z</date>
    <key>NextRenewalAttempt</key>
    <date>2012-08-09T01:43:07Z</date>
    <key>SerialNumber</key>
    <string>10cd797a0fdc6a95</string>
    <key>encDsId</key>
    <string>38504b674e2f524c334c586e46474f594b33773432673d3d</string>
  </dict>
</dict>
```


(그림 3) 인증서 정보

3.3 미리 알림

미리 알림 기능은 날짜와 장소에 대한 일정을 입력하고 미리 알림 기능을 설정하면 원하는 날짜와 장소에서 알림을 표시하는 기능이다. 이 일정 정보는 기존의 Calendar 데이터베이스에 동일하게 저장되지만 Event 테이블이 CalendarItem 테이블로 바뀌었으며 Calendar 테이블의 rowid로 미리 알림 기능을 식별한다. 데이터들이 저장되는 파일과 위치는 <표 8>과 같다.

<표 8> 파일 이름 및 저장 위치

파일 이름	저장 위치
Calendar.sqlitedb	/var/mobile/Library/Calendar

미리 알림 정보는 CalendarItem 테이블에 저장되어 있고, Calendar 테이블, Store 테이블과 연계되어 있다. 미리 알림, 달력, 저장의 주요 컬럼 정보는 각각 <표 9>, <표 10>, <표 11>과 같다.

<표 9> CalendarItem 테이블 정보

컬럼명	타입	설명
summary	text	미리 알림 내용
description	text	미리 알림 메모
start_date	real	지정한 날짜에 미리 알리기
calendar_id	integer	달력 아이디
last_modified	real	마지막 수정 날짜
creation_date	real	미리 알림 생성 날짜

<표 10> Calendar 테이블 정보

컬럼명	타입	설명
rowid	integer	달력 Private Key
store_id	integer	저장 아이디
title	text	달력 종류

<표 11> Store 테이블 정보

컬럼명	타입	설명
rowid	integer	저장 아이디
name	text	저장 이름

Calendar 테이블의 rowid 컬럼은 CalendarItem 테이블의 calendar_id 컬럼과 연계되어 있고, Store 테이블 정보의 row_id는 Calendar 테이블의 store_id와 연계되어 있다. 따라서 위 연관 관계를 이용하면 미리 알림 메시지에 대한 정보를 얻을 수 있다.

(그림 4)는 미리 알림 정보에 대한 질의 결과 화면으로 질의 문장은 다음과 같다.

Query = "select summary, location_id, description, start_date, start_tz, end_date, calendar_id, status, last_modified from CalendarItem where calendar_id = 10";

summary	location_id	description	start_date	start_tz
피아노포르테	0			_float
점심 약속	0			Asia/Seoul
이발	0			Asia/Seoul
개발 및 테스트	0			Asia/Seoul
보고서 완료	0			Asia/Seoul
발표	0			Asia/Seoul
세미나	0			Asia/Seoul
미리 알림기능	0	미리 알리기	342,608,400...	Asia/Seoul
팀 회식	0		342,610,200...	Asia/Seoul
여자 후배 결혼식	0		342,765,000...	Asia/Seoul
남자 후배 결혼식	0	이순신 결혼	342,774,000...	Asia/Seoul

(그림 4) 미리 알림 정보

4. 결론

본 논문에서는 iOS5에 새롭게 추가된 여러 기능들 중에서 iMessage와 iCloud, 미리 알림 기능 애플리케이션에 대해서 분석하였다.

이들 애플리케이션에는 사용자의 메시지와 계정 정보 그리고 일정 정보 등 포렌식 정보들이 저장될 수 있음을 스키마 분석 및 질의를 통하여 확인하였다.

디지털 포렌식에서는 사이버 범죄와 같은 특정 사건 발생 시 그 사건에 대한 사용자의 행위에 대해서 반드시 증명이 필요하다. 이 때 iOS5 이전 버전에서 기 분석된 정보들과 본 논문에서 분석한 정보들을 잘 활용한다면 향후 발생할 수 있는 디지털 포렌식 수사에서 범죄자의 유·무죄를 판단하는데 결정적인 자료로 활용될 수 있다고 본다.

참고문헌

[1] http://theiphonewiki.com/wiki/index.php

[2] 황현욱, 김기범, 장태주, 손기욱, 김민호, "모바일 백업 프로토콜을 이용한 아이폰 활성 데이터 수집 기법", 2011 디지털포렌식기술 워크샵, pp. 9-12, 2011

[3] 정진형, 변근덕, 이상진, "iPhone 기반 SNS 사용자 데이터 분석", 한국정보보호학회 동계학술대회 논문지, Vol.20, No.2, pp.225-228, December 2010

[4] http://blog.iphone-dev.org

[5] http://accessdata.com/products/computer-forensics/mobile-phone-examiner

[6] http://www.ixamforensics.com/

[7] http://www.i-funbox.com/

[8] http://www.icopybot.com/buy.php?id=plist-editor