한국항행학회 논문지 제 15 권 제 5 호 2011년 10월

아이패드 조사를 위한 디지털 포렌식 기법

A Study on Digital Forensic Techniques for iPad

이근기*, 이창훈**, 이상진*

Keun-Gi Lee*, Chang-Hoon Lee** and Sang-Jin Lee*

요 약

최근 아이패드가 발표되어 신규 휴대기기에 대한 관심이 높아지고 있다. 이렇듯 태블릿 PC 시장이 확대됨에 따라 태블릿 PC에 대한 조사 빈도도 급증할 것으로 예상한다. 하지만 외산 포렌식 도구를 활용한 아이패드 조사는 국내에 특화된 애플리케이션의 분석을 수행할 수 없으며 단순한 뷰어 기능만을 제공하여 체계화된 분석이 어렵다. 따라서 본 논문에서는 아이패드의 기본적인 애플리케이션과 국내에 특화된 애플리케이션을 분석하여 데이터를 획득하고 이를 이용한 효과적인 디지털 포렌식 기법에 대해 제시한다.

Abstract

Recently iPad has been released, so users interest in new portable device is increasing. As markets grow, experts are forecasting a increase of investigation about tablet PC. However iPad forensics is very difficult using existing smart phone forensic softwares. especially, those softwares can't analyze korean mobile application. This paper describes collecting/analyzing technique for iPad.

Key words : Digital Forensic, iPad., Tablet PC

Ⅰ. 서 론

디지털 산업 사회에 진입함에 따라 사용자가 편하게 휴대하여 사용할 수 있는 태블릿 PC가 급속히 보급되고 있다. 특히 애플사에서 개발한 iOS 기반의 아이패드와 삼성에서 개발한 구글 안드로이드 운영체제 기반의 갤럭시탭이 국내 시장을 크게 양분하고 있다. 2011년 1월 기준, 갤럭시탭은 국내에서 약 40만대를 판매하였으며, 아이패드는 약 10만대를 판매하였다.

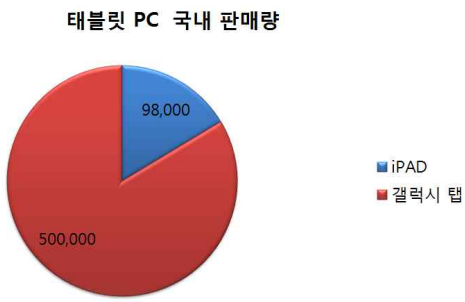

그림 1. 태블릿 PC 국내 판매량
Fig. 1. Market share about Tablet PC in S. Korea

* 고려대학교 정보보호연구원(Center for Information Security & Technologies, Korea University)
** 한신대학교 컴퓨터공학부(School of Computer Engineering, Hanshin University)
· 제1저자 (First Author) : 이근기 · 교신저자 (Corresponding Author) : 이창훈
· 투고일자 : 2011년 10월 7일
· 심사(수정)일자 : 2011년 10월 7일 (수정일자 : 2011년 10월 26일)
· 게재일자 : 2011년 10월 30일

이러한 태블릿 PC는 iOS나 안드로이드를 기반의 스마트 폰에서 활용하던 애플리케이션도 그대로 활용할 수 있을 뿐만 아니라 보다 넓은 화면에서 다양한 문서 작업을 수행할 수 있고 더 쾌적한 환경에서 멀티미디어를 활용할 수 있는 등, 기존의 스마트 폰보다 활용 범위가 넓다. 따라서 태블릿 PC를 조사할 경우, 더 많은 사용자 데이터를 확보할 수 있다.

하지만 이러한 태블릿 PC들은 기존의 2.1㎓대역의 주파수를 활용하는 3세대 네트워크를 활용할 수 있도록 3G 모뎀 장치를 탑재하여 출시하기 때문에 이를 이용한 기술 유출 및 다양한 디지털 범죄에 악용될 수 있다. 특히 기존의 유선망에서 정보보호를 위해 활용되는 소프트웨어나 하드웨어들이 태블릿 PC들이 사용하는 Wi-Fi 네트워크나 3세대 네트워크로 통하는 경로를 인식할 수 없기 때문에 이러한 태블릿 PC에 대한 조사 시 신속하게 증거를 확보할 수 있는 조사 기술에 대한 연구가 필요하다.

다양한 분야에서 사용 가능한 아이패드를 대상으로 디지털 포렌식 조사를 수행하는 경우, 더 많은 사용자 데이터 확보가 가능하다. 하지만 외산 포렌식 도구를 활용한 태블릿 PC 조사 시 국내에 특화된 지도나 SNS와 같은 애플리케이션에 대한 분석을 수행할 수 없으므로 태블릿 PC의 효과적인 데이터의 수집과 분석 방법에 대한 정립이 필요하다.

본 논문에서는 기존에 출시된 상용 태블릿 PC 도구의 지원 범위를 살펴보고, 국내 태블릿 PC 시장에서 높은 점유율을 차지하고 있는 아이패드와 갤럭시 탭의 데이터 분석 방안에 대해 살펴본다. 이를 통해 태블릿 PC에 저장되어 있는 데이터를 분석하여 효과적으로 사용자의 정보를 획득하는 디지털 증거 획득 기술에 대해 논한다.

Ⅱ. 아이패드 포렌식 연구현황

초창기의 태블릿 PC는 높은 가격과 휴대성이 불편하며, 제공하는 기능이 제한적인 문제로 인하여 시장 점유율에서 노트북이나 넷북에 밀렸다. 하지만, 최근에 출시되는 아이패드는 성능이 뛰어나고, 네트워크 지원이 강력하며 다양한 애플리케이션을 쉽게 사용할 수 있기 때문에 PC 시장에서의 새로운 카테고리로 자리 잡고 있다. 기존의 PC에서 가능한 작업의 대부분이 태블릿 PC에서 가능하고 휴대성이 더욱 뛰어나기 때문에, 기존의 PC를 이용하여 범죄를 저지르는 행위가 태블릿 PC로 더욱 쉽고 지능적으로 변모할 가능성이 있다.

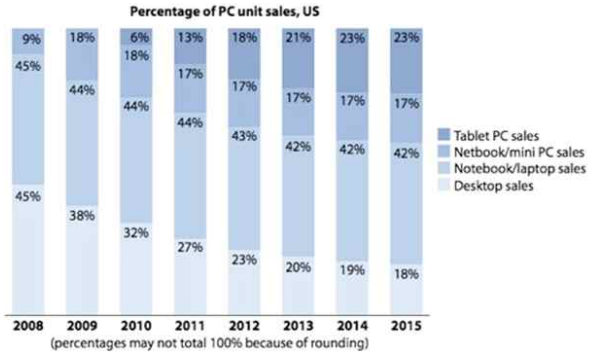

그림 2. 미국에서 판매되는 개인용 컴퓨터 점유율
Fig. 2. Market share about personal computer in US

국외의 경우에는 국내보다 아이폰이 먼저 사용되어 왔고 그에 대한 연구가 활발하게 진행되어 다양한 포렌식 도구가 출시되었다. 아이패드는 아이폰과 동일한 애플의 모바일 운영체제인 iOS를 사용하기 때문에 거의 유사한 방법으로 분석할 수 있다. 그렇기 때문에 아이폰을 지원하는 포렌식 도구는 아이패드를 대부분 지원하고 있다. 다음은 아이패드에 대한 조사를 지원하는 포렌식 도구 목록이다.

- Cellebrite UFED
- Micro Systemation XRY
- Oxygen Forensic Suite
- Kantana Forensics Lantern
- SubSosaSoft MacLockPick
- BlackBag Mobilyze
- Paraben Device Seizure
- Mobile Sync Browser
- Guidance Software EnCase Neutrino
- iPhone Analyzer

Cellbrite사의 UFED(Universal Forensic Extraction Data)는 SIM카드 및 외부 인터페이스 장치에 대한 다양한 수집능력을 가지고 있으며 유니코드 데이터 처리가 가능하다. 메모리 덤프로 파일시스템의 논리적

인 추출이 가능하며 레포트 기능이 뛰어나다. 아이패드인 경우 탈옥(Jailbreak)하지 않고 수집 및 분석이 가능하다.

Oxygen Forensic사의 Oxygen Forensic Suite는 주소록, 일정, 문자메시지, 이벤트, 파일 브라우징과 Wi-Fi 연결, Skype와 웹 캐시의 분석이 가능하다. 경찰, 군 기관과 같이 다양한 정부 기관에서 사용하고 있다.

Micro Systemation사의 XRY는 간단하고 빠른 수집 절차가 장점이다. 하지만 에러가 많이 발생하여 완전한 데이터 수집이 어렵다. SMS, 연락처, 이미지 등은 모두 수집이 가능하며 아이패드인 경우 탈옥하지 않고 수집 및 분석이 가능하다.

Kantana Forensics사의 Lantern은 다른 도구와는 달리 직관적인 인터페이스를 사용하여 사용법이 매우 간단하기 때문에 초보자도 쉽게 사용할 수 있다. 추가적인 기능으로 SQLite 데이터베이스 파일에서 삭제된 데이터를 복구해 준다.

SubRosaSoft의 MacLock Pick은 아이패드에 데이터 케이블을 직접 연결하여 데이터를 수집하는 방식을 사용하지 않고, 백업 디렉토리에 있는 데이터를 이용하여 분석한다. 이러한 방식을 사용하기 때문에 백업을 하지 않았으면 데이터 분석이 힘들게 된다. 백업 데이터를 이용하기 때문에 탈옥이 필요하지 않다.

Black Bag Technology의 Mobilize는 아이폰과 아이패드 전용으로 만들어진 도구이다. Mac OS X에서 구동되며, 문자메시지, 사진, 전화, 음성메모와 같은 데이터를 추출한다. 동시에 여러 대의 기기를 분석 가능하며 분석이 용이하도록 보고서 기능을 제공한다.

Paraben사의 Device Seizure는 삭제 데이터 복구가 가능하며 각 데이터에 따른 파싱 결과를 제공해준다. MD5, SHA1 해쉬값을 사용하여 데이터 변조를 확인할 수 있으며, HTML 형식으로 보고서를 생성한다. 아이패드인 경우 탈옥된 상태와 탈옥되지 않은 상태에서 모두 수집이 가능하다.

MobileSyncBrowser는 아이폰의 백업 유틸리티로, 문자메시지, 메모, 통화내역 등을 아이튠즈의 백업기능을 이용하여 접근한다. Mac과 Windows의 운영체제를 모두 지원하는 최초의 크로스 플랫폼 돌아가는 최초의 도구이다. 아이폰과 유사한 인터페이스를 제공한다.

Guidance Software사의 EnCase Neutrino는 포렌식과 관련한 법집행기관과 전문 분석가들이 사용하기 위하여 만들어 졌다. 수집된 데이터는 기존의 Encase 프로그램과 연동하여 사용이 가능하다. 아이폰, 블랙베리, 안드로이드, 윈도우모바일, 모토로라, 노키아, 삼성 등의 대부분의 스마트폰을 지원한다. 디바이스 기기의 설정 상태, 연락처, 통화목록, 이메일, 이미지, 문자메시지, 일정 등을 수집한다.

iPhoneAnalyzer는 오픈소스 프로젝트로써 크로스 플랫폼을 지원한다. 탈옥한 아이패드에서 대부분의 데이터에 접근이 가능하다. 단일 파일에 대해서 텍스트, 이진파일, plist 브라우징, sqlite 브라우징이 가능하여 효율적으로 사용이 가능하다.

국내 환경에서의 태블릿 PC의 조사를 위한 방안에 설명하기에 앞서 현존하는 도구에 대해 조사하였다. (표 1)은 외국에서 제작된 태블릿 PC 관련 조사 도구에서 아이패드의 지원 여부를 정리한 것이다. 각 도구들은 모두 모바일 포렌식 도구이며 분석 대상 태블릿 PC의 종류에 따라 사용 가능한 도구가 다른 것을 알 수 있다.

표 1. 포렌식 도구 별 아이패드 조사 지원 현황
Table 1. Forensic tool which is supporting iPad

도구 이름	아이패드 지원 여부	
	논리	물리
Oxygen Forensic Suite	○	×
Encase Neutrino	○	×
Cellbrite UFED	○	○
MicroSystemation XRY	○	○
Paraben Device Seizure	○	×

Ⅲ. 아이패드 내의 데이터 획득 방안

본 절에서는 조사 대상인 아이패드로부터 데이터를 수집하기 위한 방법에 대해 제시한다.

아이튠즈는 애플에서 제공하는 멀티미디어 재생 프로그램으로 주로 애플 제품군의 백업 및 콘텐츠를 관리하는데 사용한다. 따라서 아이패드 내의 데이터는 (그림 3)과 같이 아이튠즈의 백업 기능을 사용하거나 아이튠즈에 내장되어 있는 AppleMobileBackup.exe 유틸리티를 사용하여 해당 디바이스 내에 존재하는 애플리케이션 데이터를 획득할 수 있다[5]. 이와 같은 방법으로 획득한 데이터는 사용자가 사용했었던 애

플리케이션의 설정 정보이거나 혹은 태블릿 PC를 사용하면서 남는 사용자의 정보 등이다. 추출된 데이터의 파일 형태는 SQLite 데이터베이스 파일 또는 Plist 파일 또는 기타 독립적인 파일 형태로 구성되어 있다. 태블릿 PC에 저장된 다양한 애플리케이션 데이터를 수집하고 분석하여 사용자 정보 획득이 가능하다. 이와 같이 아이튠즈의 백업 기능을 이용한 아이패드의 데이터 획득 방법은 쉽고 간단하지만, 이메일과 같이 특정 애플리케이션의 데이터는 백업되지 않고, 삭제된 데이터에 접근할 수 없기 때문에 완벽한 사용자 데이터 획득에 한계를 가지고 있다.

아이패드에 대한 포렌식 조사 시 사용자가 남긴 정보를 최대한 많이 확보하기 위하여 관리자 권한 획득 기술을 이용할 수 있다. 통상 Jailbreak로 알려진 관리자 권한 획득을 통해 최고 관리자 권한을 획득하면 아이패드에 대한 이미징이 가능하다. 또한 Jailbreak를 수행하고 나면 아이튠즈에서 백업되지 않는 특정 데이터의 수집이 가능하다. 단순 애플리케이션의 데이터 수집뿐만 아니라, 아이패드의 파일시스템에 접근하여 삭제된 데이터의 존재 유무를 파악할 수 있다.

그림 3. 아이튠즈의 데이터 백업
Fig. 3. Data backup of iTunes

메모리 덤프는 (그림 3)에서와 같이 아이패드의 마운트 정보와 크기 정보를 확인한 후 DD 명령어를 수행함으로써 이미지를 생성할 수 있다. 한 가지 유의할 점은 iOS 4.0부터 이미지 자체를 암호화 하고 있기 때문에, 물리 데이터를 추출하고 나면 이에 대한 적절한 해독 절차를 수행한 후에, iOS에 저장된 데이터 분석을 수행해야 한다.

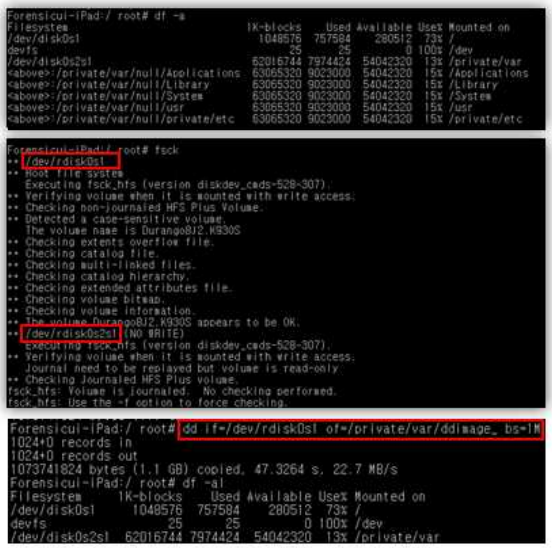

그림 4. iPad 이미지 생성
Fig. 4. Imaging of iPad

Ⅳ. 디지털 포렌식 관점의 아이패드 데이터 분석 방안

아이패드는 전화번호부, 통화기록, SMS/MMS와 같은 기본 기능과 일정, 메일, 사진 및 동영상 등 사용자가 자주 사용하는 기능을 지원하는 애플리케이션들을 기본적으로 제공한다. 이러한 기본 애플리케이션은 접근하기가 쉽기 때문에 사용자의 정보를 많이 담고 있을 가능성이 높다. 따라서 아이패드의 포렌식 조사를 위해 기본 애플리케이션의 데이터를 수집하고 분석을 우선적으로 수행하여 효율적인 분석 작업을 한다.

아이패드로부터 추출한 사용자 데이터의 파일명은 실제 파일이 존재하는 전체 경로에 대한 해쉬값으로 저장되며, 전화번호부나, 일정, 메모 등 사용자의 정보가 담긴 파일은 특정 경로에 존재하기 때문에 서로 다른 독립적인 해쉬값을 갖는다. 따라서 추출된 수많은 데이터 파일 중 해쉬값으로 저장된 파일명을 통해 선별적 분석이 가능하다. 추출된 데이터의 파일 형태는 SQLite 데이터베이스 파일 또는 독립된 파일 형태로 구성되어 있다. (표 2)는 아이패드에 존재하는 사용자 데이터 중 분석해야 할 기본 데이터와 경로 및 해쉬값 정보이다. SQLite 데이터베이스 파일을 분석 시 단순히 하나의 테이블로 정보를 표현하여 쉽

게 데이터 획득이 가능한 데이터베이스 파일도 있으나, 여러 테이블간의 정보를 조합해야 데이터 획득이 가능한 복잡한 데이터베이스 파일도 존재한다.

표 2. 아이패드 기본 애플리케이션 추출 정보
Table 2. Default application information in iPad

데이터	경로
	해쉬값
주소록	/private/var/mobile/Library/AddressBook/AddressBook.sqlitedb
	31bb7ba8914766d4ba40d6dfb6113c8b614be442
일정	/private/var/mobile/Library/Calendar/Calendar.sqlitedb
	2041457D5FE04D39D0AB481178355DF6781E6858
메모	/private/var/mobile/Library/Notes/notes.sqlite
	ca3bc056d4da0bbf88b5fb3be254f3b7147e639c
E-메일	/private/var/mobile/Library/Mail
	아이튠즈를 이용하여 데이터 백업하지 않음.
사진, 동영상	/private/var/mobile/Media/DCIM/100APPLE/
	정해진 값 없음. 시그니처 검사로 판단.

4-1 메모

아이패드의 메모 애플리케이션은 사용자가 원하는 어떠한 정보를 빠르게 저장할 수 있도록 도와준다. 또한 정보의 추가 삭제가 쉽고 편한 특징을 가지며, 자주 사용되는 기본 애플리케이션중 하나이다. 메모 애플리케이션의 추출 데이터는 SQLite 형식으로 저장되어 있으며, 추출된 데이터를 통해 사용자가 기록했었던 메모 내용과 기록된 시간을 파악할 수 있다.

메모 분석을 위해 메모 내용을 담고 있는 ZNOTEBODY 테이블과 메모의 제목 및 요약 정보가 담긴 ZNOTE 테이블을 사용한다. ZNOTE 테이블에는 각 메모의 시간정보가 담겨 있으며 두 테이블의 정보를 조인하기 위해 ZNOTEBODY의 Z_PK 필드를 Primary Key로 사용하여 분석한다.

4-2 주소록

주소록에는 해당 태블릿 PC에 저장된 전화번호나 주소를 파악할 수 있으며 해당 데이터는 SQLite 형식으로 저장되어 있다. 주소록 분석을 위해 해당 데이터베이스 파일에 존재하는 여러 테이블 중 ABMultiValueLabel, ABMultiValueEntryKey, ABGroup, ABMultiValues, ABMultiValueEntry, ABPerson, ABGroupMember 테이블을 사용한다. ABMultiValueLabel 테이블은 태블릿 PC의 주소록에 저장되어 있는 전화번호의 종류를 파악할 때 사용되는 테이블이며, ABMultiValueEntryKey 테이블은 저장된 주소를 표현할 때 사용된다. (표 3)에서 정리된 것과 같이 ABMultiValues 테이블의 Property, Identifier, Label 필드 정보를 통해 전화번호의 종류를 파악할 수 있다.

표 3. ABMultiValues 테이블 내의 전화번호 종류
Table 3. Phone number type in ABMultiValues table

전화번호 종류	Property	Identifier	Label
휴대전화	3	0	1
집전화	3	1	4
직장전화	3	2	5
팩스번호	3	3	6
이메일	4	0	4
홈페이지	22	0	7
주소	5	0	4

그림 5. ABGroup, ABPerson, ABGroupMember 테이블 관계
Fig. 5. Table relationship among ABGroup, ABPerson, ABGroup

ABGroup 테이블은 그룹 정보를 담고 있으며, ABPerson 테이블은 주소록에 저장된 사람 이름이 담겨 있다. ABGroupMember 테이블은 ABGroup 테이블과 ABPerson 테이블의 ROWID를 사용하여 그룹 멤버 정보를 구성한다.

4-3 일 정

사용자 추출 데이터 중 일정 데이터는 SQLite 형식으로 저장되고 있으며, 해당 데이터로부터 저장된 일정 관련 정보와 일정의 발생 시점을 분석할 수 있다. 해당 데이터베이스의 테이블 중 Calender 테이블은 일정 저장 단위의 정보로 구성되어 있으며 Event 테이블의 Unique_identifier 필드를 구성하기 위해 랜덤 넘버를 생성한다. Occurrence Cache 테이블은 일정의 발생시점을 저장한 테이블로써 반복이 설정된 일정의 경우 OccurrenceCache 테이블에 발생 시점을 계산하여 저장한다. 이때 Calendar_id와 event_id 정보가 필요하며 시간 정보는 Mactime을 사용한다. day필드에는 occurrence_date에서 시간 부분을 뺀 정보를 기입하여 표현한다.

Ⅴ. 결 론

디지털 산업 사회에 진입함에 따라 휴대하기 편하며 다양한 기능을 제공하는 태블릿 PC가 급속히 보급되고 있다. 이러한 시장의 흐름에서 국외에서는 태블릿 PC에 대한 연구는 많이 진행되고 도구들이 개발되어 상용으로 팔리고 있는 추세이다. 특히, 아이패드에 대한 연구 및 개발은 활발하게 진행되고 있다. 반면에 국내에서는 아이패드에 대한 연구의 진행 상황은 국외에 비하여 부족하다. 국내에서도 사건에서 아이패드를 접했을 경우, 디지털 포렌식 관점에서의 수집 및 분석 기법을 정립하면 디지털 포렌식 조사에 도움이 될 것이라고 판단된다.

본 논문에서는 아이패드에 대한 포렌식 조사 관점에서 중요한 사용자 정보를 담고 있는 기본 애플리케이션을 수집하는 기법과 이를 분석하는 방법에 대해서 제시하였다.

감사의 글

이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(No. 2011-0005648)

참 고 문 헌

[1] 이성휘, “태블릿 PC 산업 동향과 시사점”, *정보통신산업진흥원 IT Spot Issue 2010-SO4*, May 2010.

[2] 주윤경, “2011년 IT트렌드 전망 및 정책방향”, *한국정보문화진흥원* , pp. 1-9, Jan 2011.

[3] 한은미, 진홍국, “태블릿 PC 산업 지각 변동 예고”, *HI Tech Issue Report,* Oct 2010.

[4] 강신규, 국내외 태블릿 PC 시장의 동향과 시사점, *한국전파진흥원*, 2010.

[5] 황현욱, “모바일 백업 프로토콜을 이용한 아이폰 활성 데이터 수집 기법”, *디지털포렌식기술워크샵*, 2011.

이 근 기 (李謹基)

2007년 2월 : 부경대학교 전자컴퓨터정보통신공학부(공학사)
2010년 8월 : 고려대학교 정보보호학과(공학석사)
2010년 9월~현재 : 고려대학교 정보보호학과 박사과정
관심분야 : 디지털포렌식, 기업 수사, 모바일 포렌식

이 창 훈 (李창훈)

2001년 2월 : 한양대학교 수학과(이학사)
2003년 2월 : 고려대학교 정보보호대학원 석사(공학석사)
2008년 2월 : 고려대학교 정보경영공학대학원 박사(공학박사)
2009년 3월~현재 : 한신대학교 조교수
관심분야 : 정보보호, 암호학, 디지털 포렌식

이 상 진 (李相珍)

1987년 : 고려대학교 수학과 (이학사)
1989년 : 고려대학교 수학과(이학석사)
1994년 : 고려대학교 수학과(이학박사)
1989년~1999년 : ETRI 연구원
1999년~현재: 고려대학교 정교수
관심분야 : 디지털포렌식, 모바일 포렌식, 심층암호, 해쉬함수