ETRI

2013
Electronics and
Telecommunications
Trends

사이버 보안 기술 특집

스마트폰 포렌식 기술 동향

A Trend of Smartphone Forensic Technology

최우용 (W.Y. Choi) 암호기술연구실 선임연구원
은성경 (S.K. Un) 암호기술연구실 실장

* 본 연구는 지식경제부 및 한국산업기술평가관리원의 산업원천기술개발사업의 일환으로 수행하였음(10035157, 실시간 분석을 위한 디지털 포렌식 기술 개발).

최근 들어 스마트폰의 사용이 급격하게 증가하고 있으며, 또한 스마트폰에는 통화기록과 문자 메시지뿐만 아니라 이메일, 아이디, 패스워드, GPS(Global Positioning System) 데이터, 신용카드 등 수많은 개인정보가 저장된다. 이에 따라 디지털 포렌식 수사에서도 스마트폰 포렌식의 비중이 크게 증가하고 있다. 현재 전 세계적으로 많은 종류의 스마트폰 운영체제가 상용화되고 있으나 안드로이드 OS와 iOS가 86%를 차지하고 있으며, 국내에서는 99% 이상을 차지하고 있다. 본고에서는 스마트폰 포렌식의 절차를 비롯해서 안드로이드 OS 및 iOS 디바이스로부터 데이터를 수집 및 분석하는 방법에 대해서 살펴본다.

Ⅰ. 서론

스마트폰이란 휴대전화에 인터넷 통신과 정보검색 등의 기능을 추가한 지능형 단말기로서 사용자가 원하는 애플리케이션을 설치할 수 있는 것이 특징이다. 최초의 스마트폰은 1992년 IBM사가 개발한 'Simon'으로 볼 수 있다. 이후 1996년에 노키아 9000 커뮤니케이터가 출시되고, 2001년에는 최초의 블랙베리가 출시되었다. 이 때까지만 해도 스마트폰이 대중에게 큰 관심을 얻지는 못하고 있다가 2007년 애플사에서 첫 아이폰이 출시되고, 2008년 아이폰 3G가 출시되면서 스마트폰이 급속도로 확산되게 되었다. 또한 구글에서 안드로이드 운영체제를 개발하면서 삼성, LG, SKY, HTC, 구글, 모토로라, 소니에릭슨 등 많은 제조사들이 안드로이드 운영체제를 기반으로 스마트폰을 생산하기 시작하였다. 이후 세계 스마트폰 시장은 아이폰과 안드로이드 폰이 주도하게 된다.

스마트폰에는 많은 양의 개인정보가 저장되어 있기 때문에 범죄현장에서 스마트폰을 획득한 경우 지문을 채취한 경우보다 더 많은 정보를 얻을 수 있다. 국내 스마트폰 가입자는 2009년 80만 명에서 2010년 7백만 명, 2011년 2천만 명, 그리고 2012년에는 3천만 명으로 급증하였다. 또한 2012년 12월 기준으로 전체 이동통신 대비 스마트폰 가입자는 61%에 달한다[1]. 이에 따라 디지털 포렌식 수사에서도 스마트폰 포렌식의 비중이 급격하게 증가하고 있다.

본고에서는 스마트폰 포렌식의 기술 현황에 대해서 살펴본다. 본고의 구성은 다음과 같다. Ⅱ장에서 스마트폰에 저장된 포렌식 데이터에는 어떤 것이 있는지 살펴보고, Ⅲ장에서는 스마트폰 포렌식의 절차에 대해서 기술한다. Ⅳ장과 Ⅴ장에서는 스마트폰으로부터 데이터를 추출하는 방법으로 논리적 방법과 물리적 방법에 대해서 각각 기술한다. 그리고 Ⅵ장에서는 수집된 데이터를 분석하는 방법을 기술하고, 마지막으로 Ⅶ장에서 결론을 맺는다.

Ⅱ. 스마트폰의 포렌식 데이터

2012년 전 세계 스마트폰 사용자가 10억 명을 돌파했으며, 국내 사용자도 3천만 명을 넘었다. 스마트폰 사용자들의 스마트폰을 이용해서 전화통화나 문자 메시지뿐만 아니라 할 일, 일정관리, 메모, 이메일, 인터넷, 사진, 비디오, 음악 등 상당히 많은 활동을 하며, 그 기록들은 스마트폰에 저장된다. 포렌식 관점에서 스마트폰의 기본 애플리케이션에 저장된 데이터를 정리하면 다음과 같다.

- 연락처: 이름, 전화번호, 주소, 이메일 주소 등
- 통화목록: 통화 상대, 날짜, 시간 등
- 문자 메시지: 보낸(받은) 사람, 시간, 내용 등
- 캘린더: 날짜, 장소, 초대한 사람 등
- 이메일: 보낸(받은) 사람, 시간, 내용, 첨부파일 등
- 웹 히스토리: 방문 URL, 검색어, 아이디, 패스워드 등
- GPS(Global Positioning System): 위치정보
- 문서 파일
- 사진, 비디오, 오디오
- IMEI(International Mobile Equipment Identity): 국제모바일기기 식별코드, 휴대전화마다 부여되는 고유번호
- IMSI(International Mobile Station Identity): 국제이동국 식별번호, USIM마다 부여되는 고유번호
- MAC(Media Access Control) 주소

기본 애플리케이션 외에도 사용자가 직접 설치한 애플리케이션에도 개인 정보가 저장되며, 각 애플리케이션에 저장되는 데이터는 〈표 1〉과 같다.

이러한 데이터는 내장 메모리, 외장 SD 카드 및 SIM 카드에 저장된다. 스마트폰의 데이터는 텍스트 또는 데이터베이스 형태로 저장되며, 경우에 따라서 암호화되거나 패스워드로 보호되기도 한다. 스마트폰 포렌식은

〈표 1〉 사용자 설치 애플리케이션 데이터

애플리케이션	데이터
Skype, Viber, Google voice	친구목록, 통화목록
Kakao talk, iMessage, Twitter DM, Facebook message	친구목록, 문자 메시지
SNS(Twitter, Facebook, me2day, Naver band 등)	친구목록, 단문 메시지, 쪽지 등
클라우드 서비스(iCloud, Dropbox, SugarSync, uCloud, Google drive, N드라이브 등)	문서 파일, 사진, 비디오, 오디오, 백업 등
키 관리 애플리케이션 (DataVault, 1Password, OneLock 등)	여권번호, 아이디, 패스워드, 신용카드, 보안카드 등
금융 애플리케이션(KB스타뱅킹, 우리은행 원터치 개인, 신한S뱅크 등)	아이디, 패스워드, 인증서, 보안카드 등
내비게이션(Olleh navi, Tmap, 김기사 등)	GPS 데이터

이러한 데이터를 추출 및 분석하여 증거로 활용하고자 하는 일련의 과정을 말한다.

Ⅲ. 스마트폰 포렌식의 절차

스마트폰 포렌식의 절차는 컴퓨터 포렌식의 절차와 유사하나 휴대폰의 통신 기능을 고려하여 진행해야 한다. 미국의 NIST에서 2006년에 발간한 "Guidelines on Cell Phone Forensics"[2]을 바탕으로 스마트폰 포렌식의 절차를 정리하면 다음과 같다.

① 현장 보존: 범죄 현장에서 스마트폰이 발견되면 사진을 찍어 현장을 보존하여야 한다. 또한 스마트폰이 켜져 있을 경우에는 화면 사진도 캡처해 두어야 한다.

② 증거의 확보: 조사해야 할 스마트폰이 확보가 되면, 우선 다른 사람이 네트워크를 통해 스마트폰의 상태를 변경하는 것을 막기 위해 네트워크를 차단해야 한다. 이때 패러데이 상자를 이용하거나 스마트폰의 에어플레인 모드를 사용할 수 있다. 스마트폰이 켜진 상태라면 전원을 공급하여 활성데이터를 보존하여야 한다.

③ 데이터 수집 및 분석: 스마트폰으로부터 데이터를 수집할 때는 수집된 데이터가 법적 효력을 가지게 하기 위해서 다음과 같은 사항을 고려하여야 한다.

- 증거인멸의 우려가 있는가?
- 스마트폰의 데이터를 수정하는가?
- 스마트폰이 네트워크에 연결되어 있는가?
- 수사의 범위는 어디까지인가?
- 수사의 권한이 있는가?

위와 같은 고려사항이 모두 충족되었으면 데이터 수집을 실행하게 된다. 스마트폰으로부터 데이터를 추출 및 분석하는 방법은 스마트폰의 운영체제와 메모리 특성에 따라 상이하므로 알맞은 방법을 선택하여야 한다.

④ 보고서 작성: 사건정보, 증거의 획득 과정, 분석 결과 등을 보고서로 작성한다.

Ⅳ. 논리적 추출 방법

논리적 추출 방법은 USB(Universal Serial Bus) 인터페이스를 이용하여 스마트폰의 플래시 메모리 파일 시스템으로부터 스마트폰에 저장된 파일과 디렉토리를 추출하는 방법이다. 논리적 추출 방법은 속도는 빠르지만 삭제된 데이터의 복구가 어려우며 슬랙 공간의 데이터는 추출할 수 없다는 단점이 있다. 또한 패스워드가 걸려있는 스마트폰의 경우에는 패스워드를 모르면 추출이 불가능하다.

논리적 추출을 지원하는 포렌식 도구에는 Micro Systemation사의 XRY Logical, Cellebrite사의 UFED Touch Logical, AccessData사의 MPE+, Paraben Corporation사의 Device Seizure, Logicube사의 CellXtract, BitPim사의 BitPim 등이 있다.

1. 안드로이드 OS 데이터 추출

데이터 저장을 위해서 안드로이드의 메모리는 〈표 2〉와 같이 4개의 파티션으로 구성되어 있다. Cache 파티션은 설치파일 등의 임시파일을 저장하는 곳이고, system 파티션에는 기본 애플리케이션이 설치된다. 그 외에 사용자가 스마트폰을 사용하면서 생성되는 모든 데이터는 data와 sdcard에 저장된다. 사용자의 연락처, 통화목록, 문자 메시지, 웹 접속 기록, 사진, 음악, 애플리케이션 데이터 등 모든 데이터는 기본적으로 data에 저장되며, sdcard에 저장하도록 설정을 바꿀 수도 있다. 안드로이드는 오픈 소스이므로 제조사별로 파티션의 구성이 상이할 수 있으나 〈표 2〉의 4개의 파티션은 동일하게 구성되어 있다.

안드로이드 디바이스로부터 데이터를 추출하기 위해서는 디바이스의 슈퍼유저 권한을 획득하여야 하는데, 이를 루팅이라고 한다. 루팅에는 여러 가지 방법이 있지만 Odin3 소프트웨어가 가장 많이 사용된다. Odin3와 함께 루팅된 커널 파일이 있으면 루팅이 가능하다. 이때 주의할 점은 스마트폰의 기종과 커널의 빌드 버전에 맞는 커널 파일을 사용하여야 한다.

데이터 추출을 위해서는 ADB(Android Debug Bridge) 명령어를 이용하면 된다. 많이 쓰이는 ADB 명령어를 정리하면 〈표 3〉과 같다.

예를 들어, /system/app 디렉토리의 Phone.apk 파일을 C:₩로 복사하려면 '〉adb pull /system/app/Phone.apk C:₩Phone.apk'라고 입력하면 된다.

〈표 2〉 안드로이드 파티션 구성

종류	파티션	파일 시스템	용도
내장 메모리	cache	YAFFS2 or Ext4	임시파일 저장
	system	YAFFS2 or Ext4	기본 애플리케이션 설치
	data	YAFFS2 or Ext4	사용자 데이터
외장 메모리	sdcard	FAT32	외장 SD 카드

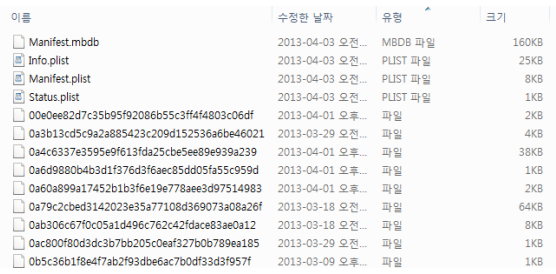
〈표 3〉 ADB 명령어

명령어	설명
adb devices	디바이스 목록 출력
adb shell 〈shell_command〉	쉘 명령어 실행
adb install 〈path-to-apk〉	애플리케이션 설치
adb pull 〈remote〉 〈local〉	디바이스에서 PC로 파일 복사
adb push 〈local〉 〈remote〉	PC에서 디바이스로 파일 복사

2. iOS 데이터 추출

안드로이드 디바이스로부터 데이터를 추출하기 위해서는 루팅을 통해 슈퍼유저 권한을 얻어야 했던 것과는 달리 iOS 디바이스에서는 슈퍼유저 권한을 얻지 않아도 대부분의 데이터를 추출할 수 있으나, 이메일, GPS 등과 같이 암호화된 데이터는 추출할 수 없다. 안드로이드의 루팅과 유사하게 iOS에도 루트 권한을 획득하는 방법이 있는데, 이를 탈옥(jailbreak)이라고 부른다. 탈옥된 iOS 디바이스에서는 이메일, GPS 등의 암호화된 데이터도 추출할 수 있다. 탈옥툴의 개발은 전문 해커들에 의해서 이루어지는데 iOS의 새 버전이 나올 때마다 그 취약점을 분석해서 탈옥툴을 공개하여 왔다. 아이폰 데브팀, 지오핫, 크로닉 데브팀 등의 탈옥팀이 활동하였으나 iOS 6.0부터는 evad3rs가 유일하게 활동하고 있다.

iOS 디바이스의 데이터 추출은 iTunes 백업 메커니즘을 이용한다. iOS의 버전이 업그레이드되면서 iTunes 백업 메커니즘도 변경되었다. iOS 1.x에서는 .mdbackup이라는 확장자를, iOS 2 & 3에서는 .mddata와 .mdinfo



(그림 1) 아이폰 백업파일의 구조

라는 확장자를 사용하였으나, iOS 4 이후부터는 확장자를 사용하지 않고, SHA1 해시값을 파일이름으로 사용하고 있다. iOS 6.x의 백업파일 구조는 (그림 1)과 같다.

여기서 해시값으로 표시된 파일이 실제 애플리케이션 데이터 파일이며, 이 파일과 실제 파일과의 매핑 정보가 Manifest.mbdb 파일에 들어 있다. 그리고 3개의 plist 파일에는 디바이스, 백업, 설정, 버전 정보 등이 포함되어 있다.

Ⅴ. 물리적 추출 방법

논리적 추출 방법은 속도가 빠른 반면, 파일 시스템이 관리하는 파일에 대해서만 수집이 가능하다. 따라서 삭제 파일이나 슬랙 공간의 데이터는 추출할 수 없다. 이러한 단점을 극복하기 위해서 물리적 추출 방법이 사용된다. 물리적 추출 방법은 플래시 메모리 전체를 비트 단위로 복사하는 방법이다. 이 방법은 스마트폰의 파일 시스템 데이터는 물론 펌웨어와 슬랙 공간의 데이터도 추출할 수 있는 장점이 있는 반면, 시간과 비용이 많이 든다는 단점도 있다.

물리적 추출을 지원하는 포렌식 도구에는 Micro Systemation사의 XRY Physical, Cellebrite사의 UFED Touch Ultimate, AccessData사의 MPE+, (주)지엠디시스템의 MD-Smart 등이 있다.

물리적 추출 방법의 종류는 다음과 같다.

① 운영체제에 기반한 방법: 스마트폰을 부팅한 후 운영체제의 명령어를 사용하여 비트 단위의 추출을 수행하는 방법이다. 이 방법을 사용하기 위해서는 슈퍼유저 권한이 있어야 한다. 즉, 안드로이드 폰은 루팅된 상태, 아이폰은 탈옥된 상태여야 한다. 슈퍼유저 권한을 얻게 되면 dd 명령어를 사용하여 물리 이미지를 추출할 수 있다. Micro Systemation사의 XRY Physical과 AccessData사의 MPE+가 이 방법을 사용한다.

② JTAG(Joint Test Action Group) 포트를 이용한 방법: PCB(Printed Circuit Board)의 JTAG 포트에 직접 연결하거나 표준 24핀 인터페이스로 연결할 수도 있다. 하지만 최근 스마트폰은 출시될 때 JTAG 포트를 끊는 경우가 많아서 JTAG 포트를 찾기가 매우 어렵다. 국내업체인 (주)지엠디시스템의 MD-Smart가 이 방법을 사용한다.

③ 메모리 칩을 분리하는 방법: 메모리 칩을 스마트폰으로부터 분리하여 직접 데이터를 추출하는 방법이다.

④ Flasher box를 이용한 방법: Flasher box 장비를 이용하여 물리적 추출을 수행한다. 펌웨어나 소프트웨어 업데이트를 통하여 메모리를 추출하므로 포렌식 관점에서는 문제가 될 수 있다. 그러나 SIM 카드가 손상되거나 PIN으로 잠겨 있는 경우, 그리고 배터리가 없는 경우에도 데이터를 추출할 수 있는 장점이 있다.

⑤ Boot loader를 이용한 방법: Boot loader란 시스템을 부팅할 때 운영체제의 커널을 메모리에 올려 실행시키는 프로그램을 말한다. 이 방법은 운영체제에 의존하지 않으며, 동일한 종류의 디바이스에서는 범용으로 사용할 수 있다. 또한 스마트폰의 메모리를 변경하지 않고, 비할당 영역의 데이터도 수집이 가능하다는 장점이 있다. Cellebrite사의 UFED Touch Ultimate가 이 방법을 사용한다.

Ⅵ. 분석 방법

수집된 스마트폰 데이터를 분석하기 위해서는 원하는 데이터가 어느 위치에 어떤 형식으로 저장되어 있는지를 알아야 한다. 데이터 저장 위치 및 파일이름은 스마트폰의 운영체제 및 애플리케이션 버전에 따라 다르므

〈표 4〉 안드로이드 애플리케이션의 데이터 저장 형식

저장 방식	파일 형식	저장 위치
SQLite	.db	/data/data/〈package〉/databases
Prefer-ence	.xml	/data/data/〈package〉/shared_prefs
Local File		/data/data/〈package〉/Cache, /data/data/〈package〉/files

로 버전을 확인하는 작업이 필요하다. 본 장에서는 안드로이드 OS와 iOS의 분석 방법에 대해서 살펴본다.

1. 안드로이드 OS 분석

안드로이드 애플리케이션이 데이터를 저장하는 방식은 SQLite, preferences, local file 형식으로 저장되며, /data/data/〈package〉 디렉토리에 저장된다. 데이터 저장 형식은 〈표 4〉와 같다.

안드로이드 운영체제에서 대부분의 데이터는 SQLite 데이터베이스로 저장된다. Preference는 xml 포맷으로, 주로 환경설정 값이 저장되며, SQLite와 preference를 제외한 모든 파일은 임의의 형태로 local file에 저장된다. 안드로이드 OS 4.0.4를 기준으로 주요 데이터의 위치와 파일이름을 정리하면 〈표 5〉와 같다.

〈표 6〉 Manifest.mbdb 파일 구조[3]

Offset	데이터	설명
4byte	mbdb0x05	Signature
String	AppDomain-net.daum.maps	Domain name
String	Library/Preferences/net.daum.maps.plist	File Path
4byte	0x000001F5	User ID
4byte	0x000001F5	Group ID
4byte	0x500E6FBA	Last modified time
4byte	0x500E6FBA	Last access time
4byte	0x500E6FBA	Created time
8byte	0x000000000001D25	파일의 길이

2. iOS 분석

Ⅳ장의 (그림 1)에서와 같이 수집된 파일에는 Manifest.mbdb, Info.plist, Manifest.plist, Status.plist, 그리고 애플리케이션 데이터 파일들이 있다. 이 중에서 데이터 파일들은 해시값을 파일이름으로 사용하고 있어서 이로부터 직접 데이터의 위치를 파악하기는 쉽지 않다. 그러나 Manifest.mbdb를 해석하면 수집된 파일에 대한 정보를 알 수 있다. Manifest.mbdb에는 모든 데이터 파

〈표 5〉 안드로이드 OS 4.0.4의 주요 파일

항목	파일 경로
연락처	/data/data/com.android.providers.contacts/databases/contacts2.db
통화목록	/data/data/com.android.providers.telephony/databases/telephony.db
문자 메시지	/data/data/com.android.providers.telephony/databases/mmssms.db
웹 히스토리	/data/data/com.android.browser/databases/browser.db
인터넷 패스워드	/data/data/com.android.browser/databases/webview.db
캘린더	/data/data/com.android.providers.calendar/databases/calendar.db
이메일	/data/data/com.android.email/databases/EmailProvider.db, /data/data/com.android.email/databases/EmailProviderBody.db
알람	/data/data/com.sec.android.app.clockpackage/databases/alarm.db
페이스북	/data/data/com.htc.socialnetwork.facebook/databases/facebook.db
카카오톡	/data/data/com.kakao.talk/databases/KakaoTalk.db, /data/data/com.kakao.talk/shared_prefs/KakaoTalk.perferences.xml
메모	/data/data/com.sec.android.app.memo/databases/Memo.db

〈표 7〉 iOS 6.x의 주요 파일의 Manifest.mbdb 분석 결과

항목	도메인	파일 경로	파일 이름(해시값)
연락처	HomeDomain	Library/AddressBook/AddressBook.sqlitedb	31bb7ba8914766d4ba40d6dfb6113c8b614be442
통화목록	WirelessDomain	Library/CallHistory/call_history.db	2b2b0084a1bc3a5ac8c27afdf14afb42c61a19ca
문자 메시지	HomeDomain	Library/SMS/sms.db	3d0d7e5fb2ce288813306e4d4636395e047a3d28
웹 히스토리	HomeDomain	Library/Safari/History.plist	1d6740792a2b845f4c1e6220c43906d7f0afe8ab
캘린더	HomeDomain	Library/Calendar/Calendar.sqlitedb	2041457d5fe04d39d0ab481178355df6781e6858
트위터	AppDomain-com.atebits.Tweetie2	User/Library/Twitter/Twitter.splite	7a0c2551ecd6f950316f55d0591f8b4922910721
페이스북	AppDomain-com.facebook.Facebook	Library/Preferences/com.facebook.Facebook.plist	384eb9e62ba50d7f3a21d9224123db62879ef423, 6639cb6a02f32e0203851f25465ffb89ca8ae3fa
카카오톡	AppDomain-com.iwilab.KakaoTalk	Library/Preferences/com.iwilab.KakaoTalk.plist	4903197cb3ac6b15b086afe9e437472614ef29e1

일의 도메인, 실제 파일이름, MAC(Modification, Access, Creation) 시간 등이 기록되어 있다. Manifest.mbdb 파일 구조는 〈표 6〉과 같다.

iOS 6.x의 주요 파일에 대한 Manifest.mbdb 분석 결과를 정리하면 〈표 7〉과 같다.

Ⅶ. 결론

본고에서는 스마트폰 포렌식의 기술 동향에 대해서 기술하였다. 스마트폰에 저장된 데이터를 포렌식 관점에서 기술하였고, 스마트폰 포렌식의 절차와 데이터 수집 및 분석 방법에 대해서 설명하였다. 스마트폰 데이터 추출 방법은 논리적 방법과 물리적 방법이 있다. 논리적 방법은 빠른 수집 및 선택적 수집이 가능하고, 물리적 방법은 삭제된 데이터도 복구할 수 있다는 장점이 있다.

약어 정리

ADB Android Debug Bridge
GPS Global Positioning System
IMEI International Mobile Equipment Identity
IMSI International Mobile Station Identity

용어해설

디지털 포렌식 '컴퓨터 법의학'이라 불리는데 전자증거물을 사법기관에 제출하기 위해 휴대폰, PDA, PC, 서버 등에서 데이터를 수집 및 분석하는 디지털 수사과정을 말함.

애플리케이션 '스마트폰 애플리케이션'의 줄임말로, 스마트폰에서 사용되는 응용 프로그램임. iOS는 애플 앱스토어에서, 안드로이드는 구글플레이에서 구매할 수 있음.

MAC 주소 이더넷의 물리적인 주소로 네트워크상에서 통신이 이루어질 때 각 네트워크 장치들은 MAC 주소에 의해서 구분됨.

패러데이 상자 도체로 만들어진 속이 텅 빈 밀폐된 상자나 전도성 물질로 만들어진 그물망으로 외부의 정전기장을 차단시키는 역할을 함.

슬랙 공간(slack space area) 저장매체의 물리적인 구조와 논리적인 구조의 차이로 발생하는 낭비 공간. 즉, 물리적으로는 할당된 공간이지만 논리적으로는 사용할 수 없는 공간을 의미함. 슬랙 공간에는 램 슬랙, 드라이브 슬랙, 파일 시스템 슬랙, 볼륨 슬랙이 있음.

JTAG 포트 PCB나 IC를 테스트하기 위해 JTAG 에뮬레이터에 연결할 수 있도록 만든 장치. 최근에는 테스트가 끝나면 JTAG 포트를 없애는 경우가 많음.

PCB 인쇄 회로 기판으로 PWB(Printed Wiring Board)라고도 함. 전기절연체 표면에 집적 회로, 저항기, 스위치 등을 형성시킨 얇은 판임.

Flasher box 플래시 메모리 덤프 장비이다. 메모리 종류에 따라 다양한 제품이 출시되어 있음.

JTAG	Joint Test Action Group
MAC	Media Access Control
MAC	Modification, Access, Creation
NIST	National Institute of Standards and Technology
PCB	Printed Circuit Board
PWB	Printed Wiring Board
USB	Universal Serial Bus

참고문헌

[1] 방송통신위원회. http://www.kcc.go.kr

[2] W. Jansen and R. Ayers, "Guidelines on Cell Phone Forensics," National Institute of Standards and Technology Special Publication 800-101, 2006.

[3] 소재현,"아이폰 백업 파일의 흔적을 찾아라," AhnLab Tech Report, 2012. 11. 06. http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=20118