

# 스마트기기 포렌식



*JK Kim*

*@pr0neer*

*forensic-proof.com*

*proneer@gmail.com*

1. 스마트기기 포렌식 소개
2. 스마트기기 데이터 획득
3. 스마트기기 파일시스템 분석
4. 스마트기기 앱 분석
5. 스마트기기 앱 아티팩트 분석
6. 스마트기기 포렌식 도구

# 스마트기기 포렌식 소개

# 스마트기기 포렌식 소개

## ■ 스마트기기란?

- 무선(cordless)으로 통신이 가능하며,
- 모바일 형태로 쉽게 이동이 가능하며,
- 연결(WiFi, 3G, 4G 등)이 항상 가능해야 하고,
- 음성/영상 통신, 인터넷 브라우징, 지리적 정보 활용 등을 할 수 있는 기기



# 스마트기기 포렌식 소개



# 스마트기기 포렌식 소개

## ■ 스마트기기 종류

- 노트북
- 스마트폰
- 태블릿 PC
- PDA, PMP, MP3
- 전자북 리더기
- 블랙박스 (?)
- 네비게이션 (?)



# 스마트기기 포렌식 소개

- 스마트폰과 태블릿 PC



iOS



Android

# 스마트기기 포렌식 소개

## ▪ 스마트폰

### • 주요 디지털 증거

#### ✓ 통신 기록

- 전화번호부, 통화 목록, 문자메시지(SMS, MMS)

#### ✓ 사용자 및 시스템 기록

- 사용자 계정 정보
- 기기 모델, 버전, 네트워크, 설치된 앱 정보

#### ✓ 응용프로그램 기록

- 카카오톡, 네이버 라인, 마이피플, 드롭박스, 구글드라이브, N드라이브, 에버노트 등
- 페이스북, 트위터, 구글+, 미투데이, 카카오톡스토리, 링크드인, 라인밴드 등
- 네이버온, 네이버맵, 다음맵, 구글맵 등
- 웹 브라우저 접속, 즐겨찾기, 검색 기록
- 이메일 송.수신 내역, 내용, 시간
- 위치 정보를 활용하는 앱의 모든 위치 정보 (Geolocation)



# 스마트기기 포렌식 소개

## ▪ 피쳐폰 vs. 스마트폰

### • 피쳐폰과 스마트폰의 차이

구분	피쳐폰	스마트폰
운영체제	Symbian, Qualcomm 등	iOS, Android, Windows Mobile, Blackberry OS
인터페이스	다양	USB
획득 방법	논리적, 물리적	논리적, 물리적, 백업
주요 데이터	연락처, 통화목록, 문자, 사진, 일정 등	연락처, 통화목록, 문자, 사진, 일정, 이메일, 웹 브라우저 흔적, SNS, 위치 정보, 애플리케이션 데이터, ID/PW 등
데이터 형식	다양	SQLite
타사 앱 사용	-	앱 전용 마켓

# 스마트기기 포렌식 소개

## ▪ iOS

### • 애플(Apple)의 스마트기기에서 사용하는 운영체제

- ✓ 아이폰
- ✓ 아이팟 터치
- ✓ 아이패드

### • 종류 및 출시 일시

출시일	버전	설명
2007. 06. 29.	iOS 1.0	-
2008. 07. 11.	iOS 2.0	아이폰 3G 출시
2009. 06. 17.	iOS 3.0	아이폰 3GS 출시
2010. 04. 03.	iOS 3.2	아이패드 출시
2010. 06. 01.	iOS 4.0	아이폰 4 출시
2011. 10. 12.	iOS 5.0	아이폰 4S, 아이패드 2 출시
2012. 09. 20.	iOS 6.0	아이폰 5 출시
2013. 09. 20.	iOS 7.0	아이폰 5C, 5S 출시

# 스마트기기 포렌식 소개

- iOS

- 아이폰 구조

- ✓ 도시바(Toshiba) 플래시 메모리 사용



# 스마트기기 포렌식 소개

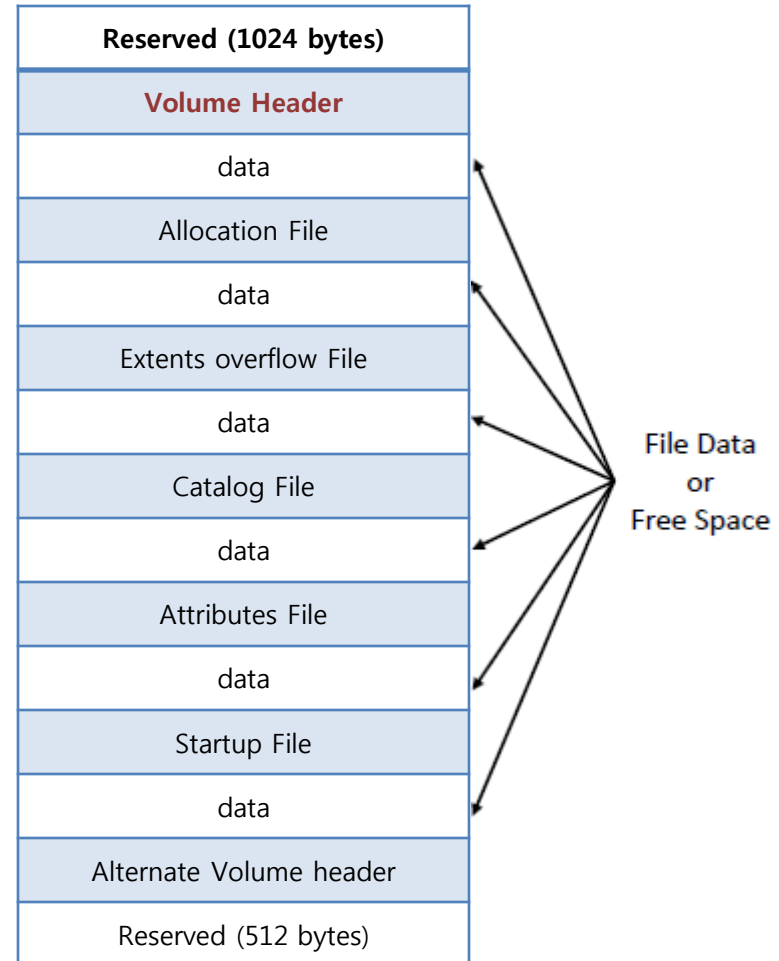
## ▪ iOS

### • 아이폰 파일시스템

#### ✓ HFS+

- 볼륨 헤더
- 카탈로그 파일
- 확장 오버플로 파일
- 속성 파일
- 할당 파일(비트맵)
- 스타트업 파일
- 저널 파일

#### ✓ 모든 데이터를 B-Tree 구조로 저장



# 스마트기기 포렌식 소개

## ■ 안드로이드

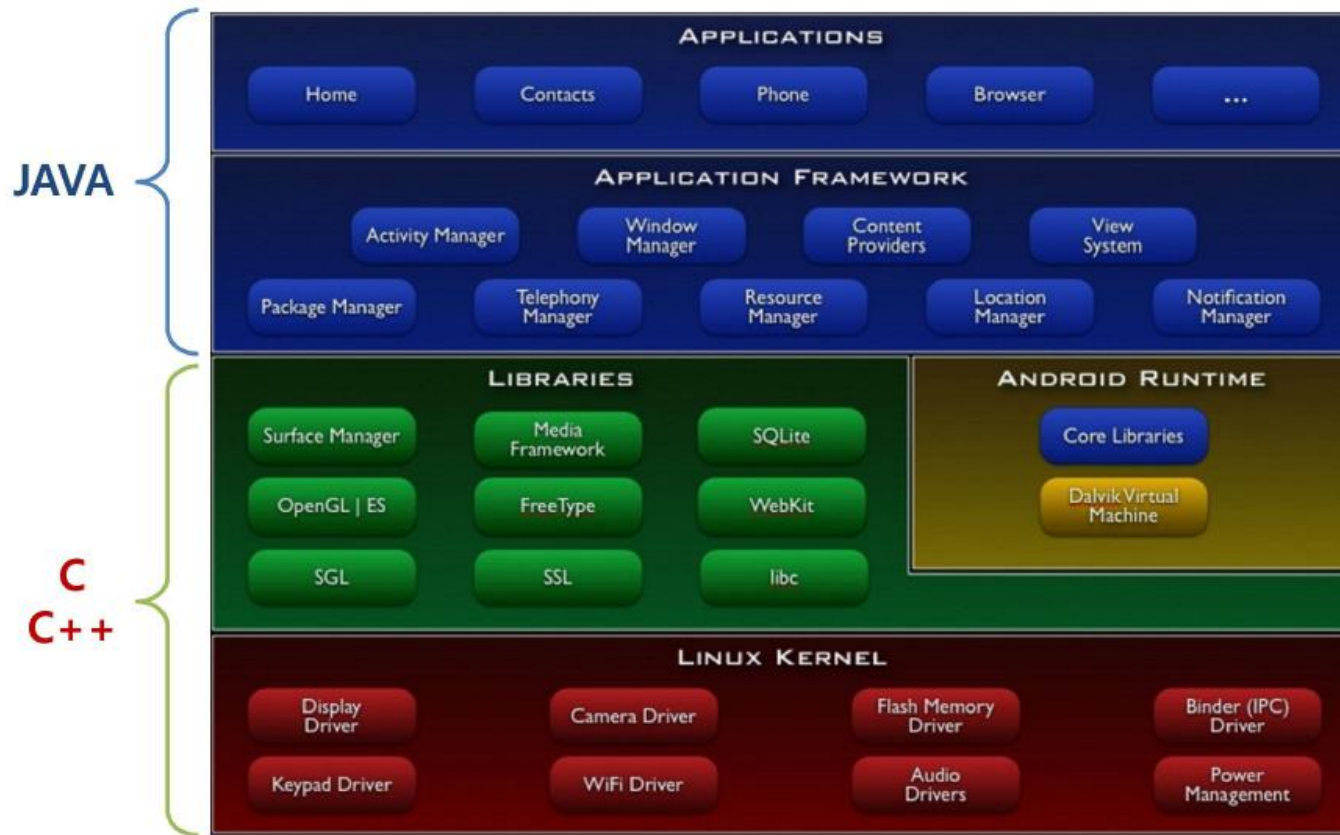
- 구글에서 개발한 공개용 임베디드 운영체제
- 개방형 플랫폼으로 다양한 기기에서 구동 가능
  - ✓ 스마트폰, 태블릿, 네비게이션, 스마트 TV, 셋톱박스, 구글 안경 등



# 스마트기기 포렌식 소개

## ■ 안드로이드

- 리눅스 커널 + 라이브러리 (C, C++ 기반으로 작성)
- 애플리케이션 (Java 기반으로 작성)
- 달빅(Dalvik) 가상 머신 위에서 동작



# 스마트기기 포렌식 소개

## ■ 안드로이드

### • 종류 및 출시 일시

출시일	버전	주요 내용
2008. 09. 23.	Android 1.0 (Apple Pie)	최초 안드로이드 버전
2009. 02. 09.	Android 1.1 (Banana Bread)	T-Mobile G1을 위해 업데이트
2009. 04. 30.	Android 1.5 (Cupcake)	새로운 기능과 UI 업데이트
2009. 09. 15.	Android 1.6 (Donut)	내장 기능과 해상도 향상
2009. 10. 26.	Android 2.0 (Éclair)	하드웨어 및 브라우저 기능 향상
2010. 05. 20.	Android 2.2 (Froyo)	성능 향상 및 어도비 플래시 지원
2010. 12. 06.	Android 2.3 (Ginger Bread)	UI 향상, NFC 지원, 버그 수정
2011. 02. 22.	Android 3.0/3.1/3.2 (Honeycomb)	태블릿 UI 지원, G토크 영상 통화 지원, 마이크로 SD 사용
2011. 05. 10.	Android 4.0 (Icecream Sandwich)	보이스 메일 지원, 캘린더/지메일 등 성능 향상
2012. 06. 28.	Android 4.1/4.2/4.3 (Jelly Bean)	UI 변경, 크롬 기본 브라우저, 플래시 미지원
2013. 10. 31.	Android 4.4 (Kitkat)	달빅 캐시 → 스왑, 클라우드 프린팅, SELinux 보안 강화

# 스마트기기 포렌식 소개

## ▪ 안드로이드

### • 플래시 메모리 설계 기법

#### ✓ oneNAND

- 삼성에서 개발한 초기 모바일 내장 스토리지
- SLC 낸드 플래시 + NOR 인터페이스 + SRAM 버퍼

#### ✓ moviNAND

- MLC 낸드 플래시 + MMC 컨트롤러

#### ✓ eMMC

- JEDEC에서 규정한 휴대용 카드 표준
- eMMC 버전 4.4부터 moviNAND를 지칭
- 파티셔닝 기능 지원
- 갤럭시 S2 이후 삼성 스마트폰은 모두 eMMC 사용



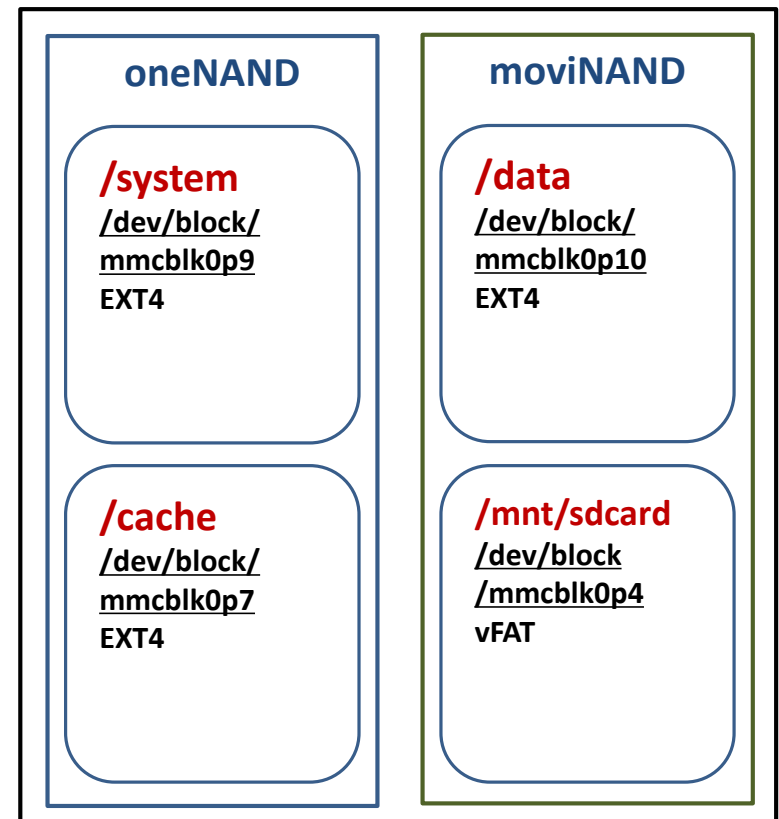
# 스마트기기 포렌식 소개

## ■ 안드로이드

### • 삼성 스마트폰

#### ✓ eMMC 플래시 메모리 사용

- 각 볼륨은 모두 다른 블록 장치에 마운트
- 사용자 데이터는 data, sdcard 파티션에 존재



# 스마트기기 포렌식 소개

## ▪ 안드로이드

### • 파일시스템

#### ✓ YAFFS2(Yet Another Flash File System 2), RFS(Robust File System)

- 스마트폰 초기 사용

#### ✓ ext (Extended File System) 2/3/4

- 블록 장치 전용 파일시스템
- 안드로이드 생강빵(v2.3)부터 ext4 사용
- 파일 단편화 최소화
- 저널링 기능 지원
- 2012년 10월 기준, 안드로이드 장치의 83.2%가 생강빵 상위 모델
- 갤럭시 S2 출시를 기점으로 대부분의 안드로이드 폰은 ext4 파일시스템 사용

# 스마트기기 포렌식 소개

## ▪ 안드로이드

### • 파티션

#### ✓ 내부 메모리

- **/boot** – 운영체제 커널과 램디스크가 설치되는 공간
- **/system** – 운영체제 필수 소프트웨어 설치 공간 (쓰기 방지로 설정)
- **/recovery** – 백업이나 업그레이드 등의 기능을 사용할 수 있는 복구 영역
- **/data** – 실제 사용자 데이터가 저장되는 공간
- **/cache** – 임시 파일이 설치되는 공간
- **/misc** – CID(Carrier/Region ID), USB 구성, 특정 하드웨어 구성 등의 설정 정보 저장 공간

#### ✓ 외부 메모리

- **/sdcard** – 외부 SD 카드 영역
- **/sd-ext** – 외부 SD 카드의 확장 영역으로 표준 파티션은 아님

# 스마트기기 데이터 획득

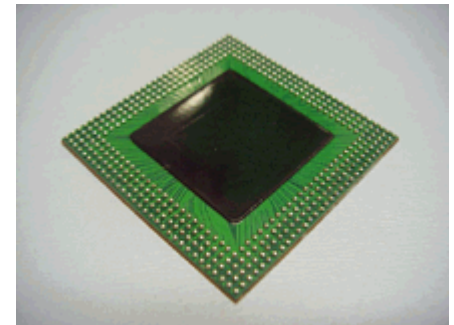
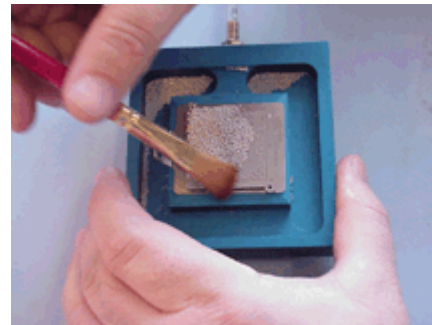
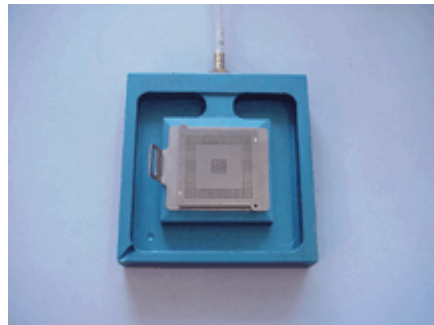
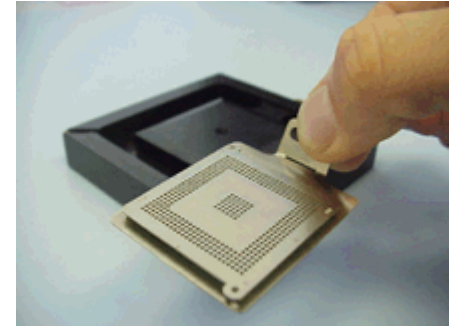
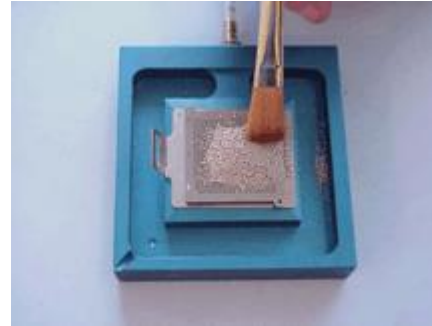
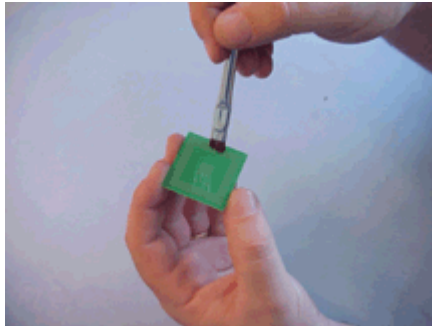
# 스마트기기 데이터 획득

- 데이터 획득 방법
  1. 물리적 획득
  2. 논리적 획득
  3. (u)SIM, SD 카드 획득

# 스마트기기 데이터 획득

## 1. 물리적 획득 (1/2)

- 플래시 메모리 칩 분리(chip-off) → 리볼링(Rebolling) → 칩 리더기를 통해 이미징

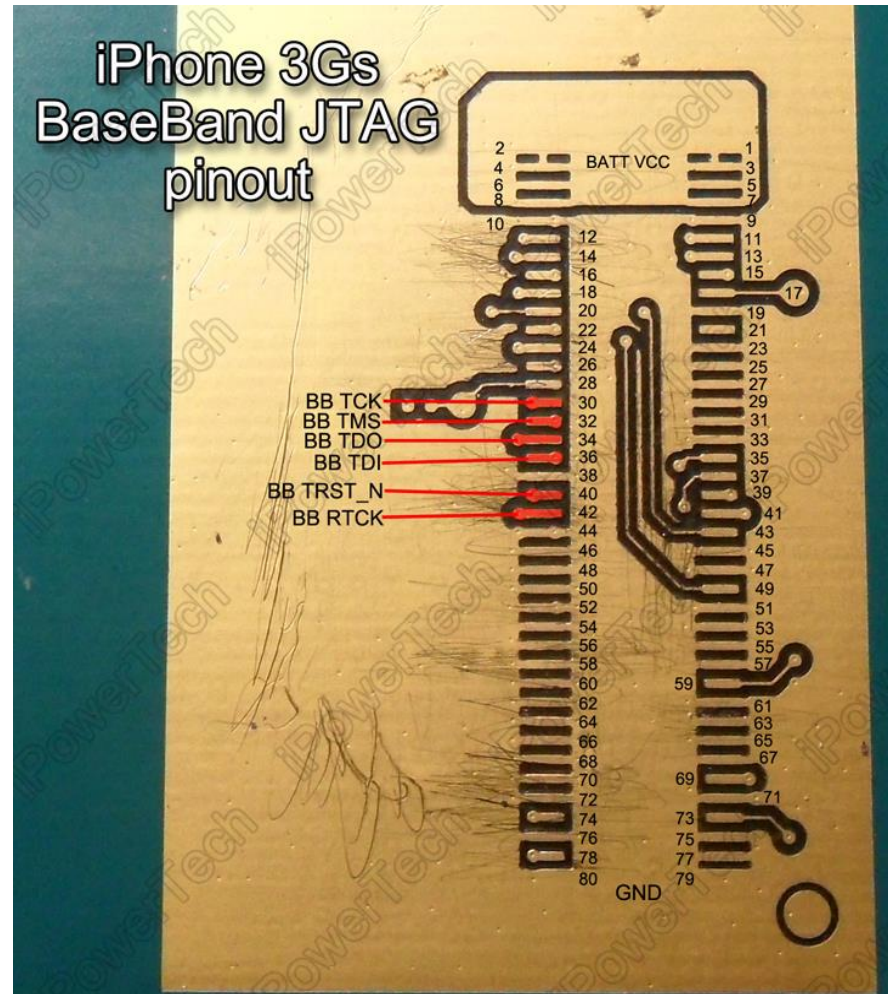
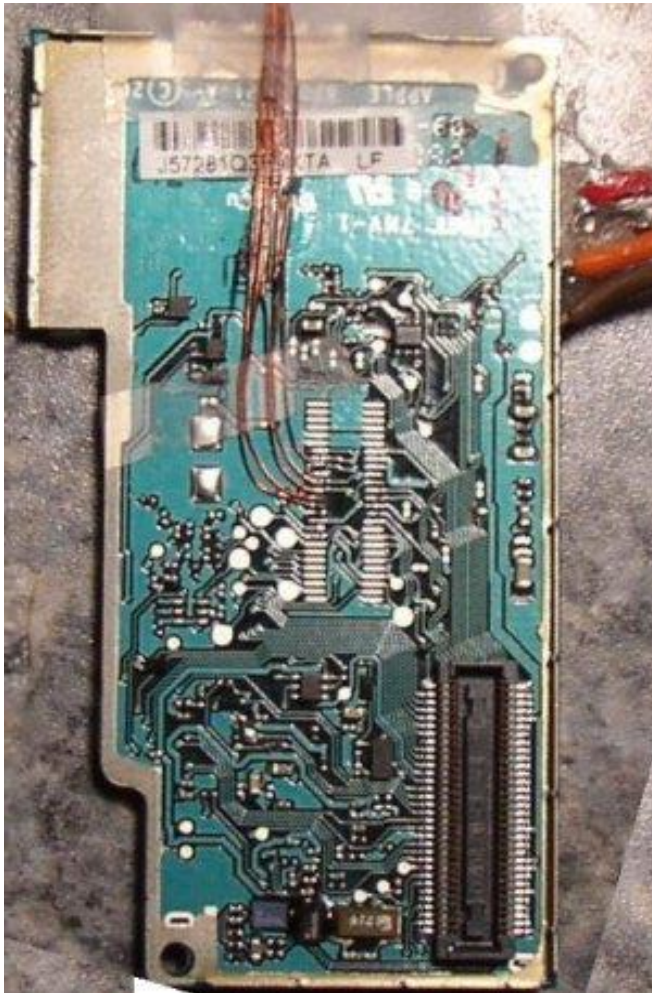




# 스마트기기 데이터 획득

## 1. 물리적 획득 (2/2)

- JTAG 단자를 이용한 이미징 → 최근에는 JTAG 단자를 제거



## 2. 논리적 획득 – iOS #1

- **취약점** – A4 칩(iPhone 4) 까지만 가능
  - ✓ 커널 익스플로잇을 이용 ➔ 사용자가 임의로 만든 부트로더로 램디스크(Ramdisk) 구성
  - ✓ 램디스크에 포함된 도구로 논리 이미징(낸드 전체 풀 덤프), 데이터 선별 추출 가능
  - ✓ Elcomsoft iOS Forensics Toolkit도 A4 까지만 동작 ➔ 이후 버전은 탈옥된 폰만 가능





## 2. 논리적 획득 – iOS #2

- 탈옥(Jailbreak)

- ✓ 탈옥된 폰에 **Custom App**을 설치하여 이미징 가능 → 원본 훼손
- ✓ 탈옥 프로그램 : blackra1n, Spirit, Redsn0w, PwnageTool, Sn0wbreeze, jailbreakme.com

- ✓ 주요 데이터 저장 경로

구분	설명	경로
Contacts	연락처	Library/AddressBook/AddressBook.sqlitedb, AddressBookImages.sqlitedb
Calendar	일정	Library/Calendar.sqlitedb
Safari	사파리 웹 흔적	Library/Safari/History.plist, Bookmark.plist, SuspendState
Notes	메모	Library/Notes/notes.db
SMS	문자 내역	Library/SMS/sms.db
Call History	통화 목록	Library/CallHistory/call_history.db
Voice Mail	음성 메일	Library/Voicemail/*.amr
Picture	사진	Media/DCIM/100APPLE/IMG_xxxx.JPG
Email	이메일	Library/Mail/(account name)/INBOX.mbox/Messages

## 2. 논리적 획득 – iOS #3

- 백업 모드

- ✓ 백업 프로토콜을 사용해 데이터 추출

1. iTunes 이용
2. AppleMobileBackup 이용

- ✓ 백업된 로컬 데이터 획득

- 암호화가 되어 있는 경우, Elcomsoft Phone Password Breaker로 복호화

- ✓ 백업 저장 경로

- 윈도우 2K/XP : %UserProfile%\Application Data\Apple Computer\MobileSync\Backup\
- 윈도우 Vista+ : %UserProfile%\AppData\Roaming\Apple Computer\MobileSync\Backup\
- MAC OS X : /Library/Application Support/MobileSync/Backup/

## 2. 논리적 획득 – iOS #3

- iFunBox – <http://blog.i-funbox.com/>



## 2. 논리적 획득 – Android #1

- Custom APK(Content Provider)를 이용한 획득

- ✓ 안드로이드의 데이터 공유 인터페이스인 Content Provider를 이용하는 방법
- ✓ URI를 공개한 애플리케이션의 샌드박스 접근 가능
  - Content://com.android.alarmclock/alarm
  - CallLog.Calls.CONTENT\_URI
- ✓ 디버깅 모드를 활성화한 후(기본 비활성화), **Custom APK**를 설치하여 원하는 데이터 추출
- ✓ 수집 대상 : 앱 목록, 통화 목록, 연락처, 인터넷 북마크/검색어, 일정, 문자 내역
- ✓ 한계점
  - 수집 앱 설치 ➔ 무결성 훼손
  - 레코드 쿼리 내용만 수집 가능 ➔ DB 파일이나 이미징 불가로 삭제된 데이터 복구 불가

## ➔ 실습

- 실습 준비

- ✓ USB 통합 드라이버 설치

- <http://www.samsung.com/sec/support/pcApplication/USB>

- ✓ 안드로이드 SDK 설치 ➔ platform-tools/adb ➔ 환경 변수 등록

- <http://developer.android.com/sdk/index.html>

## ➔ 실습

- Custom APK 앱을 설치하여 데이터 획득하기!!

### 1) AFLogical.apk 다운로드

- <https://viaforensics.com/resources/tools/>

### 2) USB 디버깅 활성화

- [설정 ➔ 일반 ➔ 개발자 옵션 ➔ USB 디버깅]

### 3) 알 수 없는 출처 활성화

- [설정 ➔ 일반 ➔ 보안 ➔ 디바이스 관리 ➔ 알 수 없는 출처]

### 4) 앱 설치 및 실행

- # adb install AFLogical.apk
- Capture

### 5) 결과 확인

- SD 카드의 "forensics" 폴더 확인

## 2. 논리적 획득 – Android #2

- 루팅(Rooting)을 이용한 획득

- ✓ 안드로이드 관리자 권한을 획득하는 행위
- ✓ 부트 관련 영역에 루팅된 이미지를 올린 후 부팅하여 루트 권한 획득
- ✓ ADB 프로토콜을 이용해 데이터 획득

## 2. 논리적 획득 – Android #2

- 루팅(Rooting)

- ✓ 주요 데이터 저장 경로

구분	경로
연락처	/data/data/com.android.providers.contacts/databases/contacts2.db
통화 목록	/data/data/com.android.providers.contacts/databases/contacts2.db
문자 내역	/data/data/com.android.providers.telephony/databases/mmssms.db
일정	/data/data/com.android.providers.calendar/databases/calendar.db
메일	/data/data/com.google.android.email/databases/EmailProvider.db /data/data/com.google.android.email/databases/EmailProviderBody.db
웹 브라우저	/data/data/com.android.browser/databases/browser.db /data/data/com.android.browser/databases/webview.db /data/data/com.android.browser/databases/webviewCache.db
다운로드 목록	/data/data/com.android.providers.downloads/databases/downloads.db
시스템 설정	/data/data/com.android.providers.settings/databases/settings.db
사진 및 동영상	/sdcard/dcim/camera/



## ➔ 실습

- 실습 준비

- ✓ 오딘(Odin3) 다운로드

- <http://atsgadgets.com/download-odin-latest-version-v3-09/>

- ✓ Busybox 다운로드

- <http://www.busybox.net/>

- ✓ 모델 별 루팅 이미지 준비

- <http://www.clockworkmod.com/>
    - <http://www.xda-developers.com/>
    - <http://pspmaster.tistory.com/>
    - <http://www.matcl.com/>

## ➔ 실습

- 안드로이드 스마트폰 루팅하기!!

### 1) 다운로드 모드 진입

- (전원 + 홈 + 볼륨 다운) ➔ 볼륨 업
- # adb reboot download

### 2) 오딘(Odin3) 실행 (recovery.img 교체)

- Files [Download] ➔ AP 버튼 클릭 ➔ 루트 이미지 선택 ➔ Start!!

### 3) 리커버리 모드 진입

- (전원 + 홈 + 볼륨 업)

### 4) 데이터 파티션 확인

- # adb shell
- # mount | df -h | cat /proc/partitions

## ➔ 실습

- 안드로이드 스마트폰 루팅하기!!

### 5) Busybox 업로드

- # adb push busybox /tmp
- # adb shell chmod 755 /tmp/busybox

### 6) NC(Netcat)를 이용해 이미징하기

- [PC] # adb forward tcp:9999 tcp:9999
- [PHONE] # /tmp/busybox nc -l -p 9999 -e dd if=/dev/block/[data\_block]
- [PC] # nc 127.0.0.1 9999 > android.dd

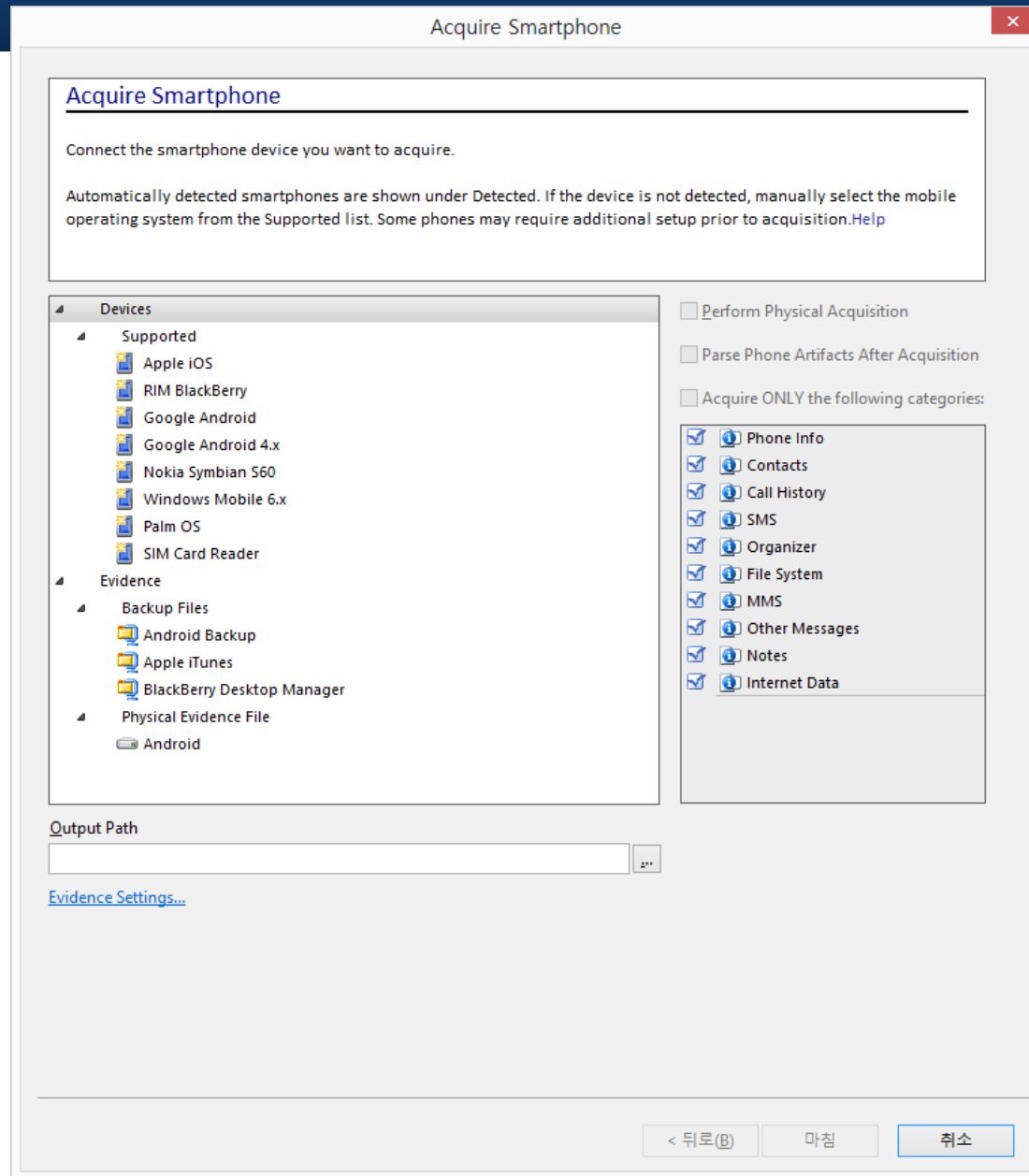
## 2. 논리적 획득 – Android #3

- ADB Backup

- ✓ 안드로이드 4.x 부터 지원

- ✓ 루트 권한 없이

- 제한된 데이터 획득 가능



## ➔ 실습

- ADB BACKUP 기능을 이용해 백업하기!!

✓ # **adb backup** [-f <file>] [-apk | -noapk] [-shared | -noshared] [-all] [-system | -nosystem]  
[<packages...>]

- **-f <file>** : 장치 데이터를 저장할 파일로 설정하지 않으면 현재 디렉터리에 "**backup.ab**"로 저장
- **-apk | -noapk** : apk 백업을 활성화/비활성화 할 수 있는 옵션으로 기본은 "**noapk**"
- **-shared | -noshared** : 공유 스토리지/SD 카드 내용의 백업을 활성화/비활성화 할 수 있는 옵션 기본은 "**noshared**"
- **-all** : 설치된 모든 앱을 백업
- **-system | -nosystem** : "-all" 옵션에 시스템 앱을 포함할 것인지에 대한 옵션, 기본은 포함
- **<packages..>** : 백업할 앱 목록

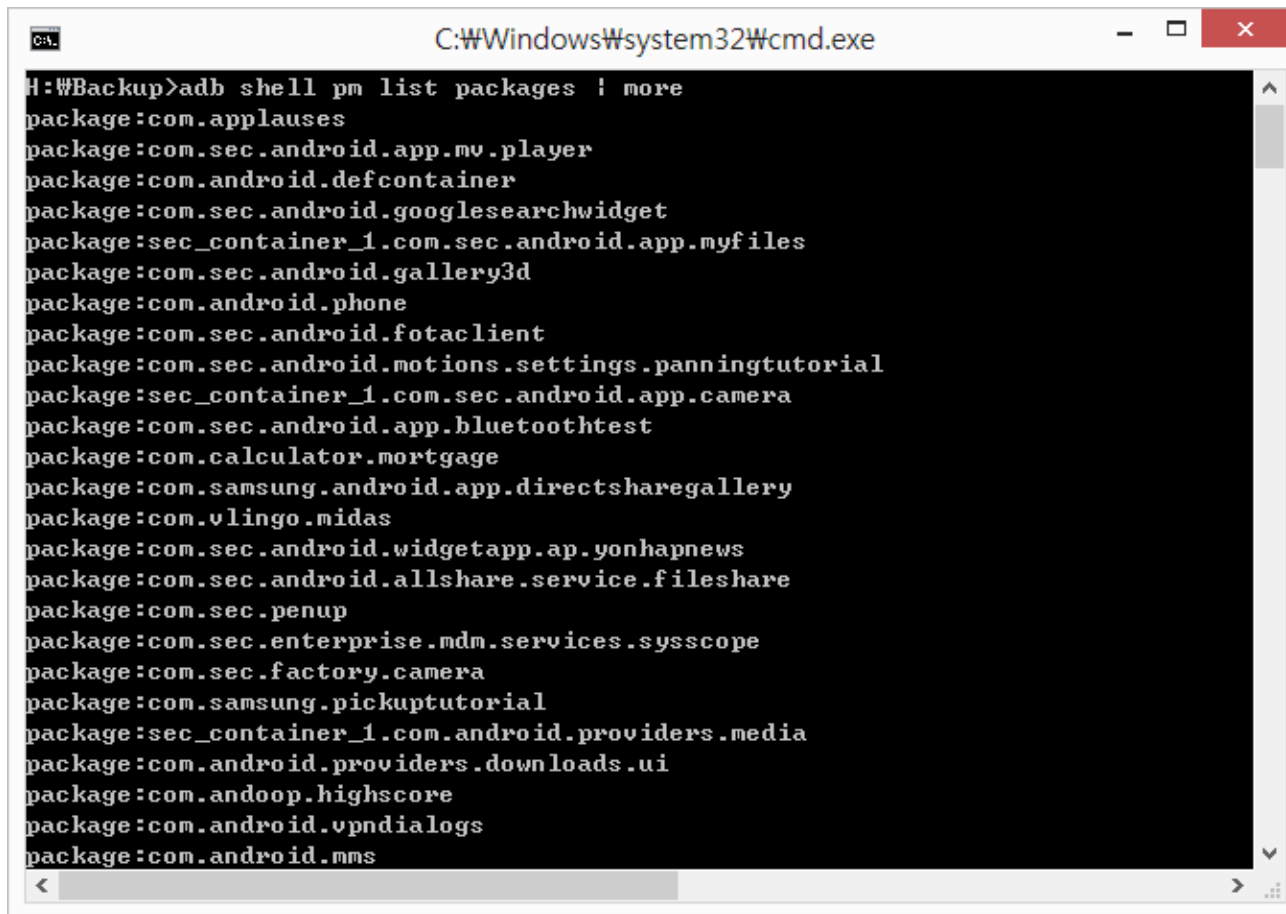
✓ # **adb restore <file>** : <file> 백업 아카이브로부터 내용을 복원

# 스마트기기 데이터 획득

## ➔ 실습

- 패키지 목록 확인하기!!

✓ # **adb shell pm list packages > list.txt**



```
C:\Windows\system32\cmd.exe

H:\#Backup>adb shell pm list packages | more
package:com.applauses
package:com.sec.android.app.mv.player
package:com.android.defcontainer
package:com.sec.android.googlesearchwidget
package:sec_container_1.com.sec.android.app.myfiles
package:com.sec.android.gallery3d
package:com.android.phone
package:com.sec.android.fotaclient
package:com.sec.android.motions.settings.panningtutorial
package:sec_container_1.com.sec.android.app.camera
package:com.sec.android.app.bluetoothtest
package:com.calculator.mortgage
package:com.samsung.android.app.directsharegallery
package:com.vlingo.midas
package:com.sec.android.widgetapp.ap.yonhapnews
package:com.sec.android.allshare.service.fileshare
package:com.sec.penup
package:com.sec.enterprise.mdm.services.sysscope
package:com.sec.factory.camera
package:com.samsung.pickuptutorial
package:sec_container_1.com.android.providers.media
package:com.android.providers.downloads.ui
package:com.andoap.highscore
package:com.android.vpndialogs
package:com.android.mms
```

# 스마트기기 데이터 획득

## → 실습

- 카카오톡 앱 백업하기!!

✓ # adb backup -f kakaotalk.ab com.kakao.talk

```
C:\Windows\system32\cmd.exe

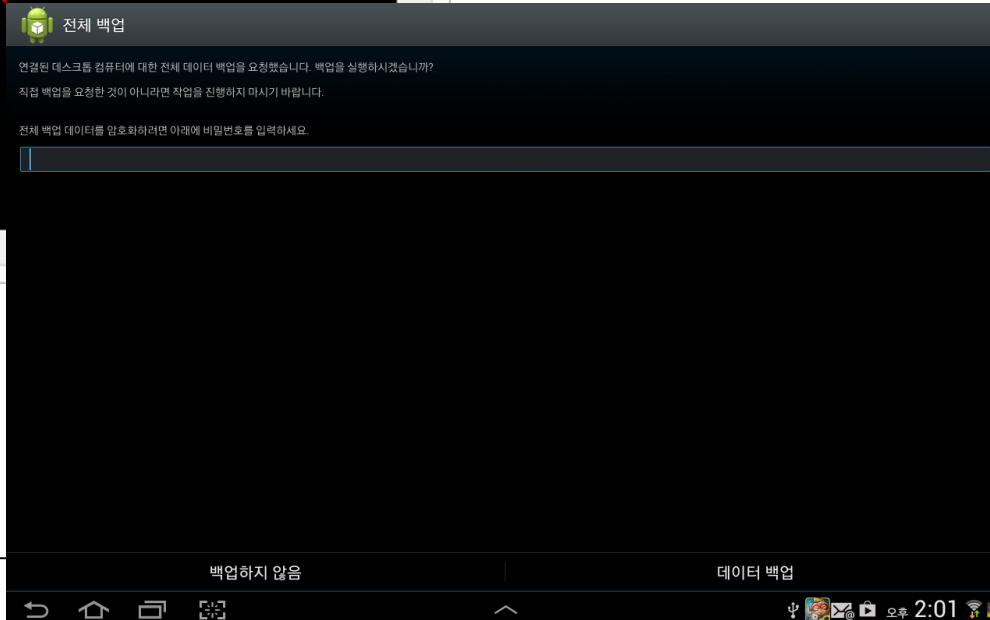
H:\Backup>adb backup -f kakaotalk.ab com.kakao.talk
Now unlock your device and confirm the backup operation.

H:\Backup>dir
H 드라이브의 볼륨: L4CTUR4
볼륨 일련 번호: AC74-45A3

H:\Backup 디렉터리

2013-11-21 오후 10:53 <DIR> .
2013-11-21 오후 10:53 <DIR> ..
2013-11-21 오후 10:57          1,092 kakaotalk.ab
                   1개 파일          1,092 바이트
                   2개 디렉터리 2,779,643,904 바이트 남음

H:\Backup>
```

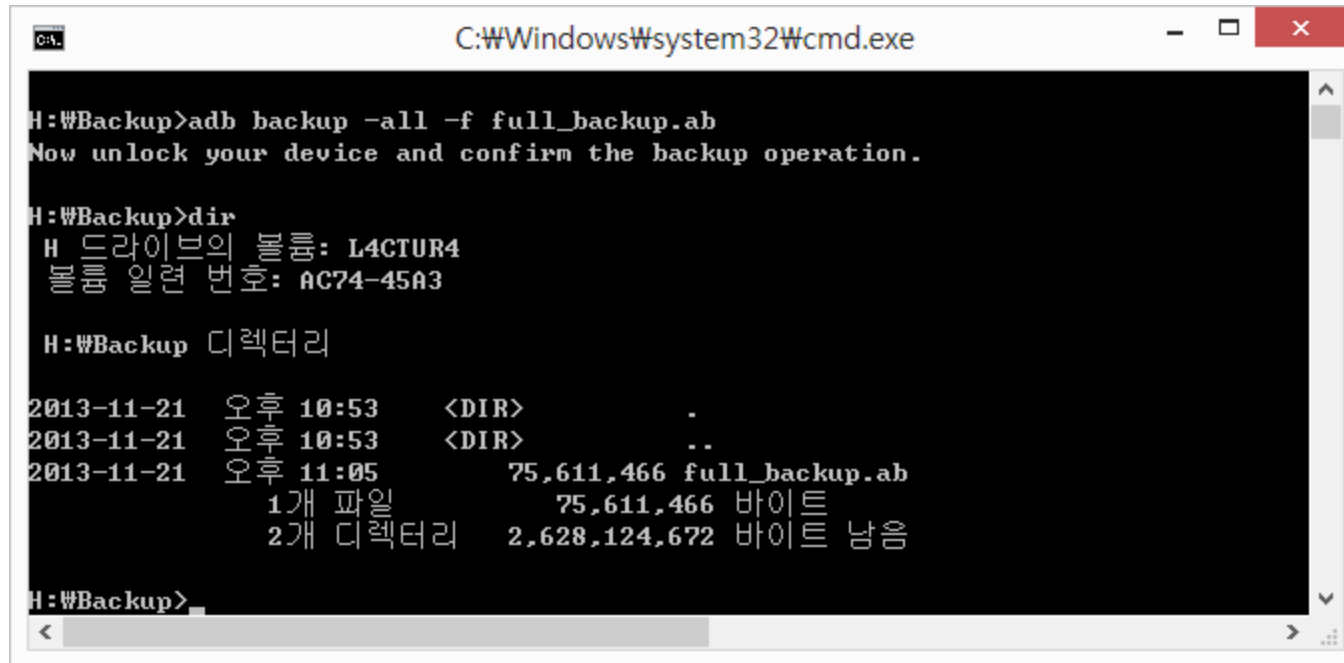


# 스마트기기 데이터 획득

## ➔ 실습

- 전체 앱 백업하기

✓ # **adb backup -all -f full\_backup.ab -shared**



```
C:\Windows\system32\cmd.exe

H:\Backup>adb backup -all -f full_backup.ab
Now unlock your device and confirm the backup operation.

H:\Backup>dir
H 드라이브의 볼륨: L4CTUR4
볼륨 일련 번호: AC74-45A3

H:\Backup 디렉터리

2013-11-21 오후 10:53 <DIR> .
2013-11-21 오후 10:53 <DIR> ..
2013-11-21 오후 11:05      75,611,466 full_backup.ab
                   1개 파일      75,611,466 바이트
                   2개 디렉터리  2,628,124,672 바이트 남음

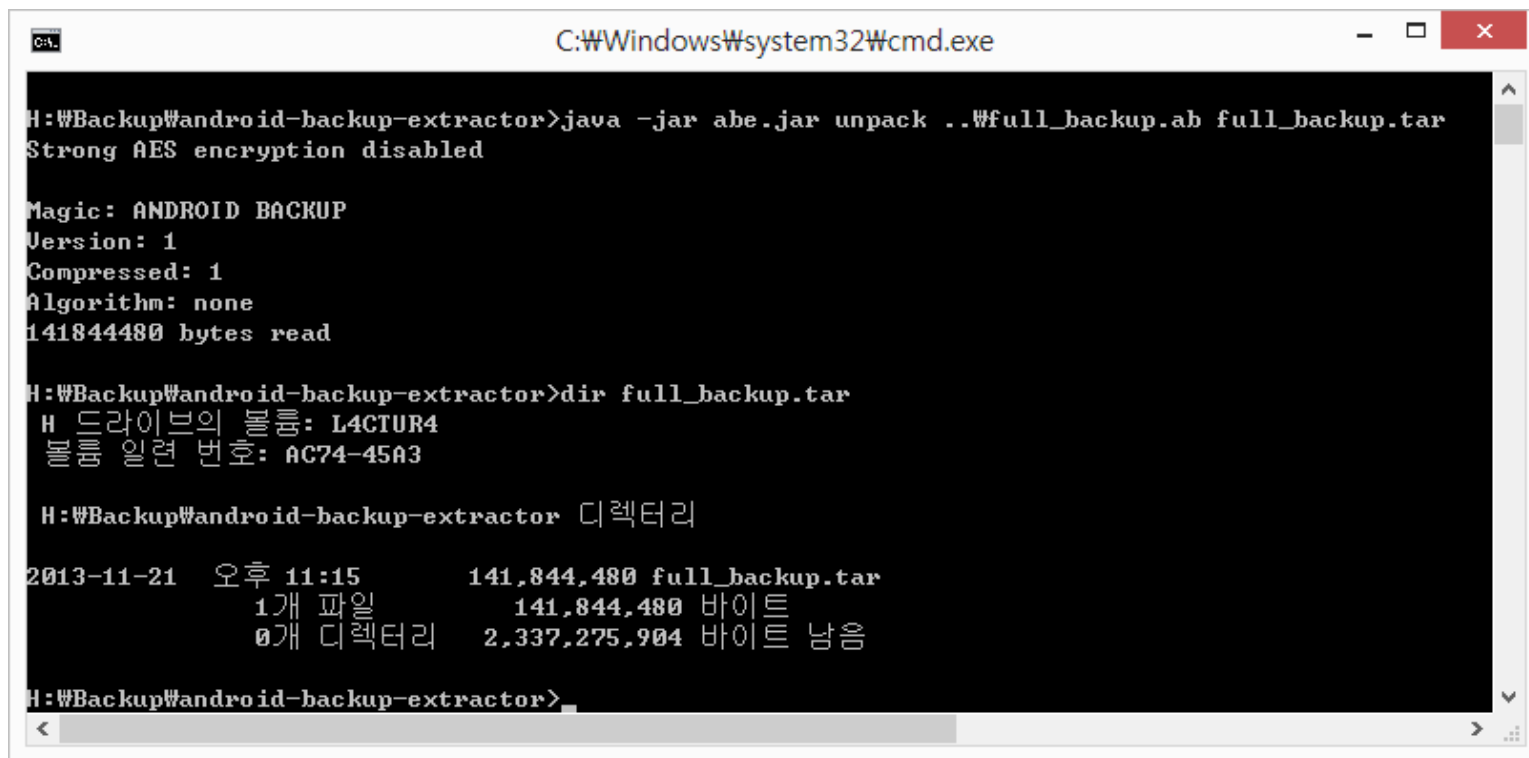
H:\Backup>
```



# 스마트기기 데이터 획득

## → 실습

- 백업 파일 언팩하기!!
  - ✓ JRE, <http://www.oracle.com/technetwork/java/javase/downloads/index.html>
  - ✓ Android Backup Extractor, <http://sourceforge.net/projects/adbextractor/>
  - ✓ # `java -jar abe.jar unpack [backup file] [unpacked file] [password]`



```
C:\Windows\system32\cmd.exe

H:\Backup\android-backup-extractor>java -jar abe.jar unpack ..\full_backup.ab full_backup.tar
Strong AES encryption disabled

Magic: ANDROID BACKUP
Version: 1
Compressed: 1
Algorithm: none
141844480 bytes read

H:\Backup\android-backup-extractor>dir full_backup.tar
H 드라이브의 볼륨: L4CTUR4
볼륨 일련 번호: AC74-45A3

H:\Backup\android-backup-extractor 디렉터리

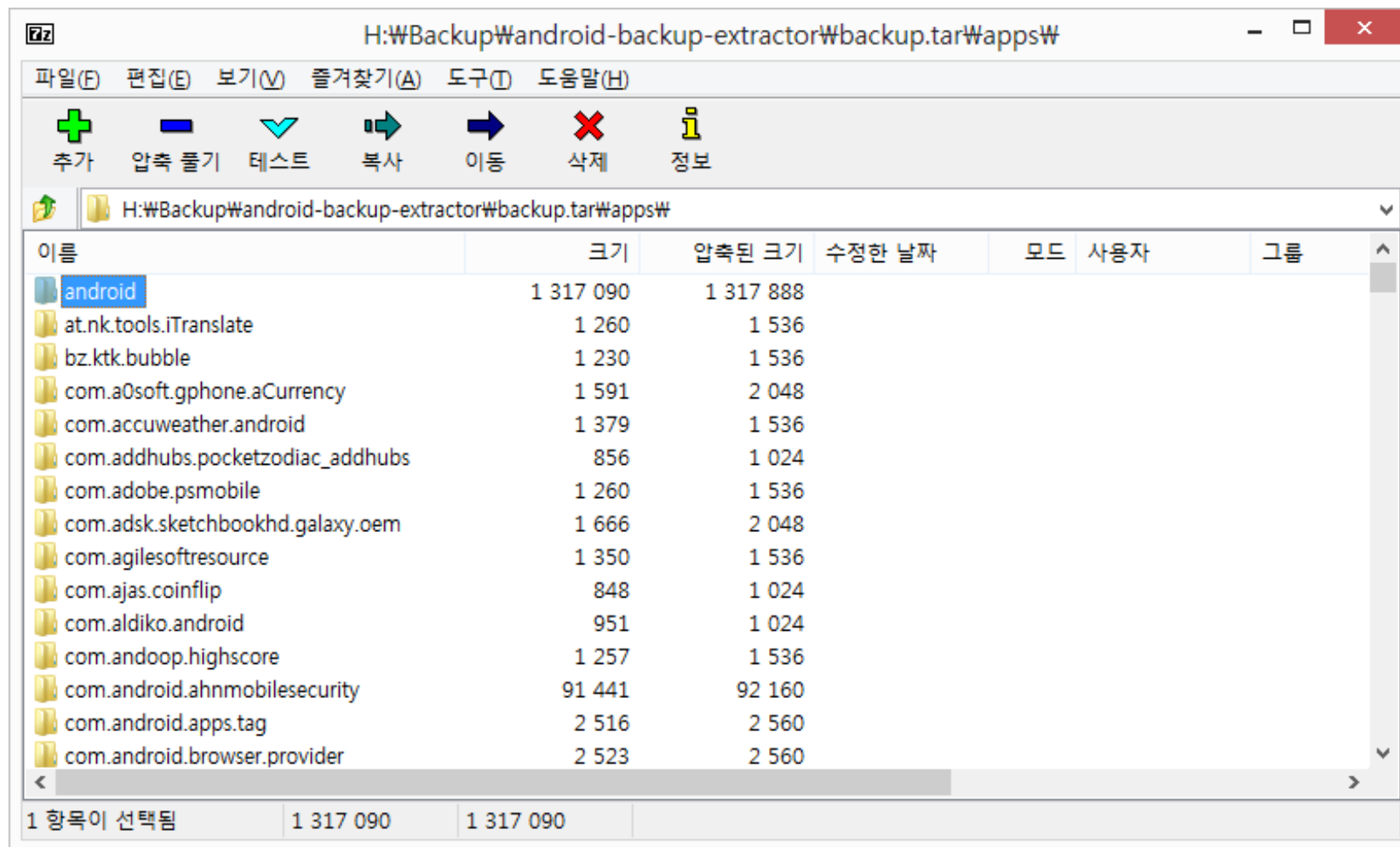
2013-11-21 오후 11:15      141,844,480 full_backup.tar
                1개 파일      141,844,480 바이트
                0개 디렉터리  2,337,275,904 바이트 남음

H:\Backup\android-backup-extractor>
```

# 스마트기기 데이터 획득

## ➔ 실습

- 언팩 백업파일에서 앱 데이터 확인하기!!



## ➔ 실습

- 엔케이스 v7을 이용해 안드로이드 ADB 백업하기!!

## 2. 논리적 획득 – Android #4

- 부트/복구 파티션 플래싱(Flashing)

1. 사용자 정의 복구 이미지(CRMI, Custom Recovery Mode Image) 생성

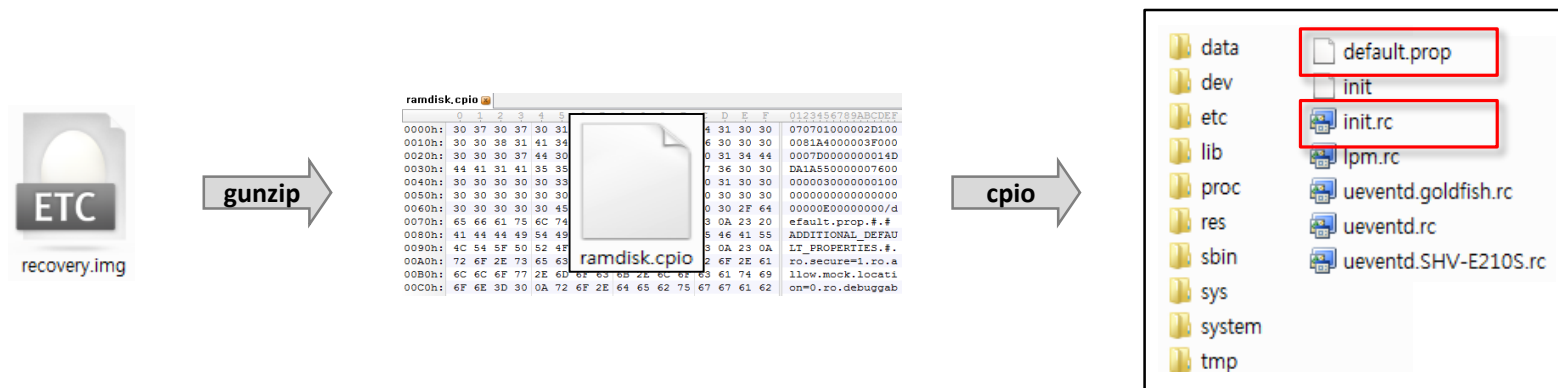
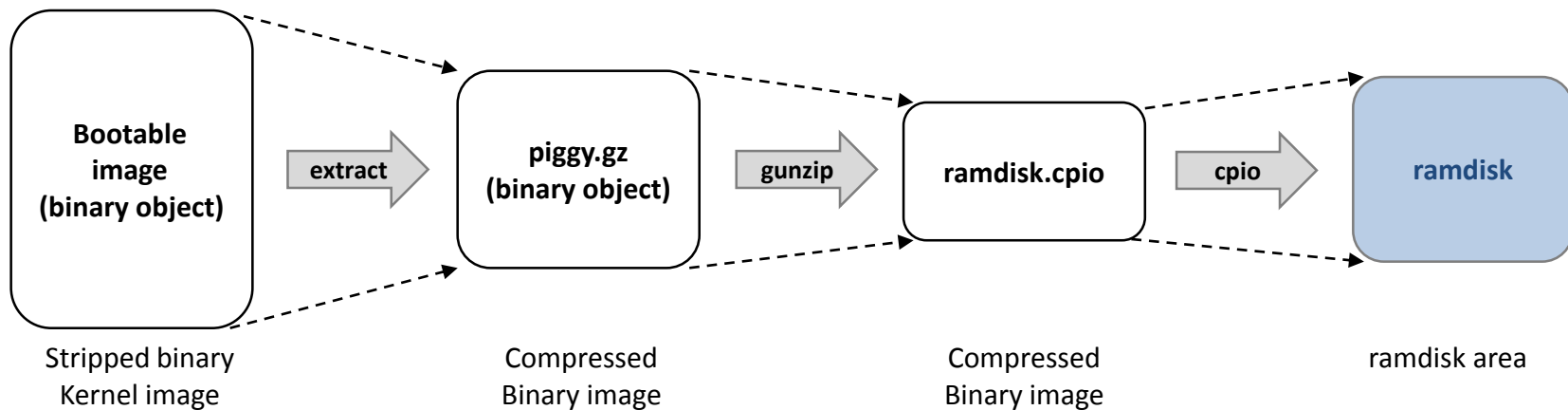
- ✓ 대상 모델명 확인 후, 인터넷에서 복구 이미지(커널+램디스크+기타) 다운로드
- ✓ 복구 이미지를 압축해제 한 후, root 권한을 위해 램디스크 파일 수정 (init.rc, adbd 등)
- ✓ 커널이 데이터 파티션을 접근하는 모델의 경우 재컴파일을 통해 접근 차단
- ✓ 수정 완료 후 다시 재압축하여 CRMI 생성 완료

# 스마트기기 데이터 획득

## 2. 논리적 획득 – Android #4

- 부트/복구 파티션 플래싱(Flashing)

### 1. 사용자 정의 복구 이미지(CRMI, Custom Recovery Mode Image) 생성



## 2. 논리적 획득 – Android #4

- 부트/복구 파티션 플래싱(Flashing)

- 사용자 정의 복구 이미지(CRMI, Custom Recovery Mode Image) 생성

- ✓ 보통 부트 파티션과 복구 파티션 영역의 크기는 동일
- ✓ 일부 제품은 복구 파티션 영역이 크므로 수정하여 부트 파티션에 맞춰줌

장치	부트 파티션	복구 파티션
Droid (A855)	3584	4608
Galaxy S2 (SHW-M250S)	8192	8192
Galaxy Nexus (SHW-M420K)	8192	12224
Galaxy Note (SHV-E160S)	10240	10240
Galaxy S3 (SHV-E210S)	8192	8192
Galaxy Note 2 (SHV-E250S)	8192	8192
Vega LTE (IM-A800S)	10240	10240

## 2. 논리적 획득 – Android #4

- 부트/복구 파티션 플래싱(Flashing)

### 2. 장치 부팅

- ✓ 장치를 플래시 모드(flash mode)로 부팅

### ✓ 안드로이드 부팅 모드

- 일반 모드
- 플래시 모드
- 복구 모드

## 2. 논리적 획득 – Android #4

- 부트/복구 파티션 플래싱(Flashing)

### 3. 사용자 정의 복구 이미지(CRMI) 플래싱

- ✓ 수정된 복구 이미지를 어디에 플래싱 할 것인가?

- 부트 파티션?
- 복구 파티션?

- ✓ 복구 파티션에 플래싱 할 경우,

- 장치 부팅 시 복구 모드로 진입 필요
- 만약, 실패하면??

- ✓ 부트 파티션 플래싱

- 안전하게 복구 모드로 자동 진입



## 2. 논리적 획득 – Android #4

- 부트/복구 파티션 플래싱(Flashing)

### 4. 사용자 데이터 획득

✓ CRMI 플래싱 후 장치 재부팅 → 복구 모드(root 권한)로 자동 진입

✓ 파일 복사

- ADB 명령을 통해 파일 복사

✓ 이미징

- 램디스크의 rootfs 파티션을 읽기/쓰기 모드로 마운트
- rootfs 파티션에 Busybox 복사
- Busybox에 포함된 다양한 도구를 이용해 이미징

## 2. 논리적 획득 – Android #4

- 부트/복구 파티션 플래싱(Flashing)

### 5. 상태 복원

- ✓ 데이터 획득 후 다시 원래 부트 파티션으로 복원
- ✓ /system/build.prop 파일을 통해 펌웨어 정보 확인
- ✓ [모델명 + 펌웨어]에 맞는 원본 부트 파티션 이미지를 다운받음
- ✓ ADB Push 명령을 이용해 부트 파티션 복원

장치	복구 파티션
Droid (A855)	/dev/block/mtdblock5
Galaxy S2 (SHW-M250S)	/dev/block/mmcblk0p5
Galaxy Nexus (SHW-M420K)	/dev/block/mmcblk0p7
Galaxy Note (SHV-E160S)	/dev/block/mmcblk0p8
Galaxy S3 (SHV-E210S)	/dev/block/mmcblk0p5
Galaxy Note 2 (SHV-E250S)	/dev/block/mmcblk0p8
Vega LTE (IM-A800S)	/dev/block/mmcblk0p8

## ➔ 실습

- 부트/복구 파티션을 플래싱하여 데이터 획득하기!!

## 2. 논리적 획득 – Android #5

- 펌웨어 프로토콜??
  - ✓ 펌웨어 수준의 저수준 프로토콜 이용

## 2. 논리적 획득 – iOS vs. Android

- **iOS**

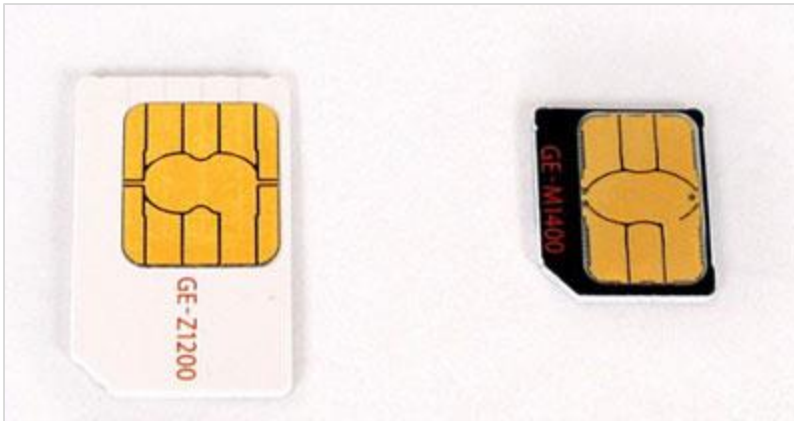
- ✓ A4 칩 이후 버전에서는 이미징 불가능
- ✓ 백업 모드를 통해 대부분 원하는 데이터 획득 가능
- ✓ (A4 칩 이후) 비밀번호가 걸려있는 경우???

- **Android**

- ✓ 다양한 기기에 대응하기가 어려움
- ✓ 디버깅 모드를 활성화하여 APK를 이용한 데이터 획득은 기본 내장 App만 가능
- ✓ 루팅 후 ADB 프로토콜로 데이터 획득 가능
- ✓ 부트/복구 파티션을 플래싱하여 데이터 획득 가능
- ✓ 비밀번호가 걸려있는 경우???

## 3. (u)SIM, SD 카드 획득

- 별도의 보호 메커니즘이 없어 물리적인 접근만 되면 획득 가능



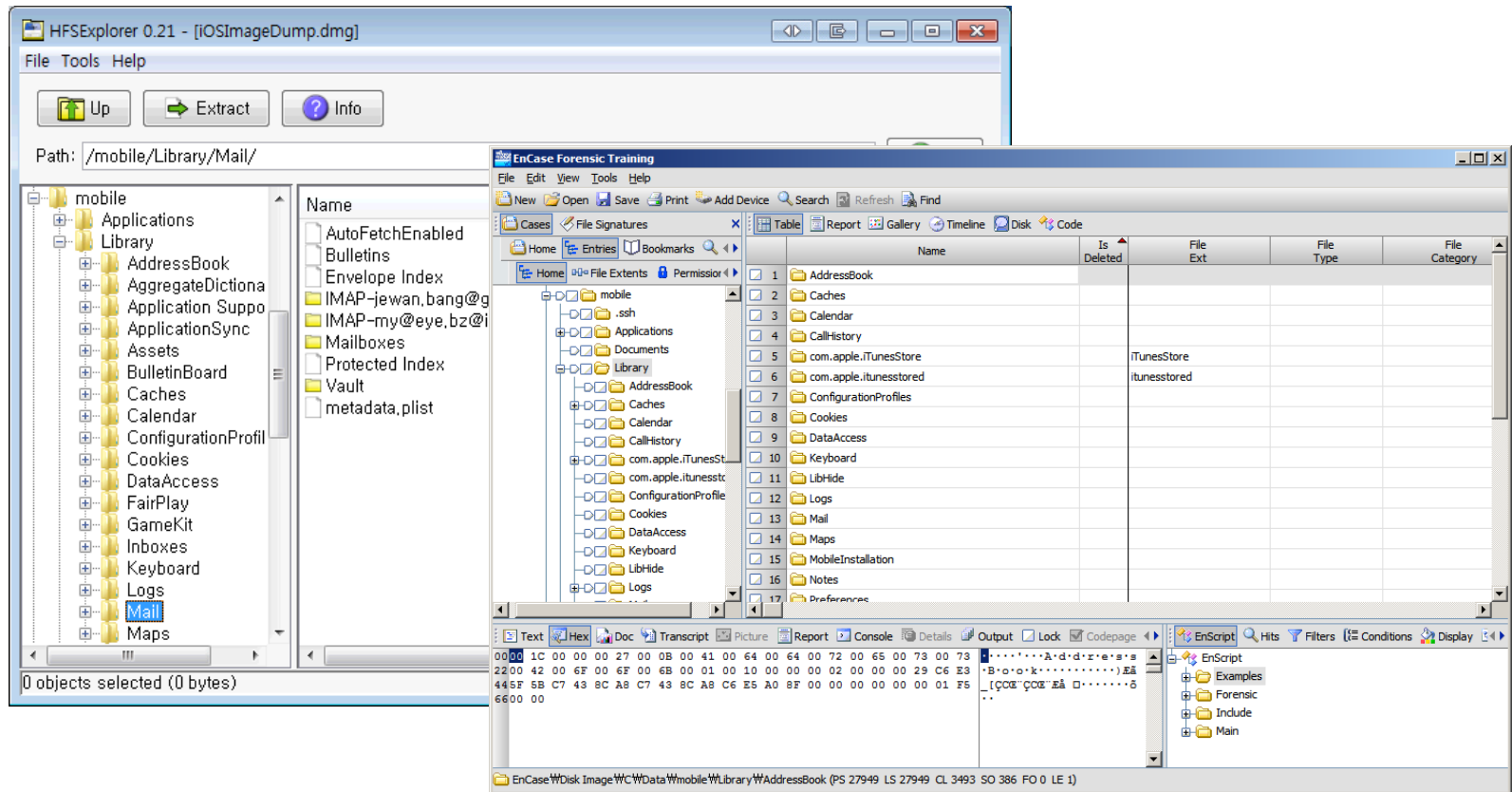
# 스마트기기 파일시스템 분석

# 스마트기기 파일시스템 분석

## ■ 이미지 파일 분석 – iOS

### • iOS 이미지 (A4칩 이전)

- ✓ 통합 포렌식 도구에 로드하여 파일시스템(HFS+) 분석
- ✓ EnCase, X-Ways Forensics, X-Ways WinHex, HFSExplorer 등



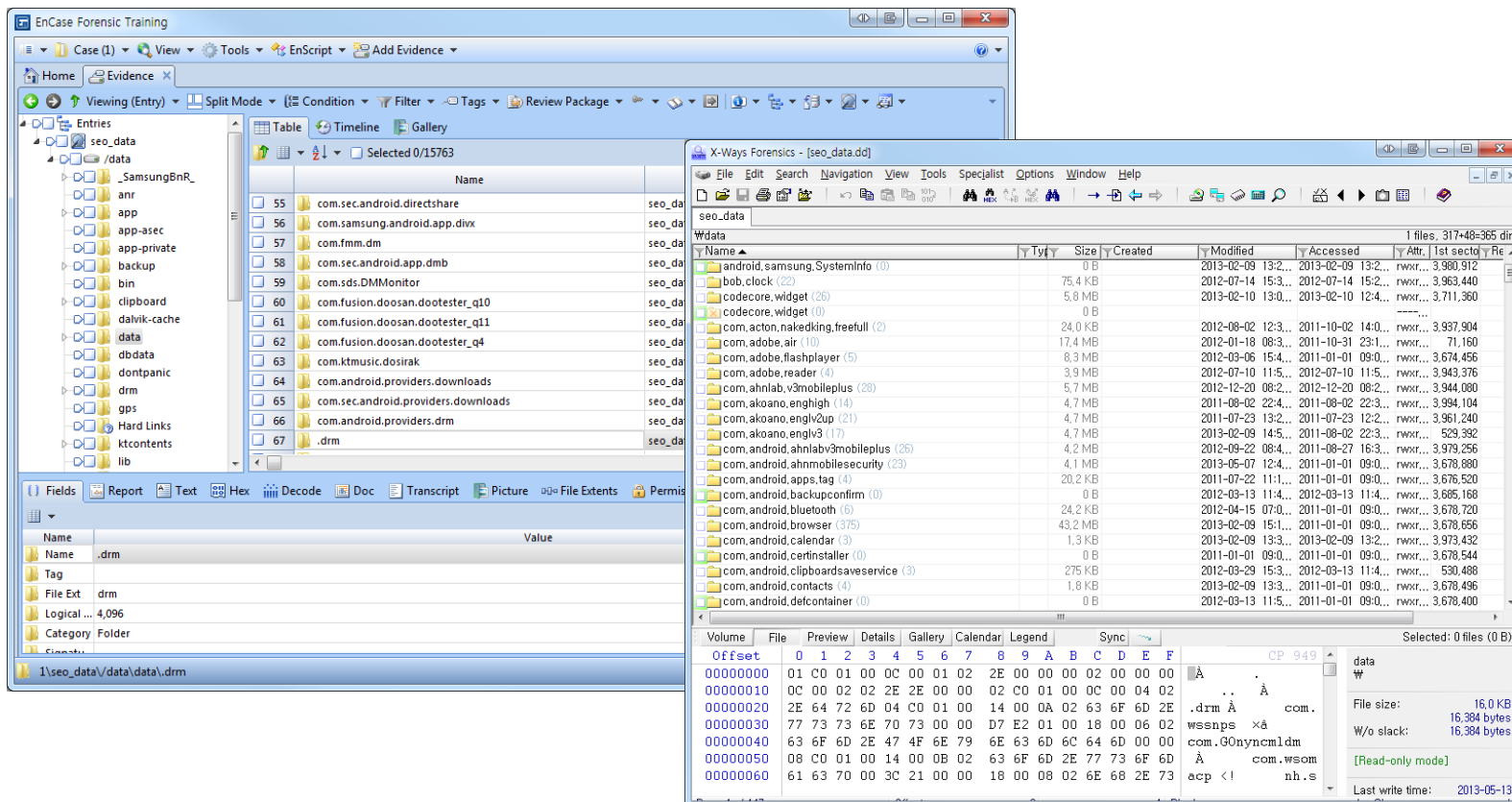


# 스마트기기 파일시스템 분석

## ■ 이미지 파일 분석 – Android

### • 안드로이드 이미지

- ✓ 통합 포렌식 도구에 로드하여 파일시스템(ext4) 분석
- ✓ EnCase, X-Ways Forensics, X-Ways WinHex 등



# 스마트기기 파일시스템 분석

- 이미지 파일 분석 – Android

- 안드로이드 이미지

- ✓ 할당 영역

- 앱 SQLite 파일, XML 파일 추출 후 분석

- ✓ 비할당 영역

- 사진, 동영상, 삭제된 앱 등 데이터 복구 후 분석

# 스마트기기 파일시스템 분석

## ➔ 실습

- 안드로이드 이미지 파일시스템 분석하기!!

WinHex - [note3.dd]

File Edit Search Navigation View Tools Specialist Options Window Help

note3

15+0+5=20 files, 44 dir.

Name	Ext.	Path	Size	Created	Modified	Accessed	Inode modification	Attr.	1st sector
.container_1		₩	8.0 KB	1970-01-01 09:17:25.4	2013-09-14 19:41:01.5	1970-01-01 09:17:25.4	1970-01-08 01:35:33.6	rwxr...	12,648,...
.container_2		₩	4.0 KB	1970-01-01 09:17:25.4	1970-01-01 09:17:25.4	1970-01-01 09:17:25.4	1970-01-08 01:35:33.6	rwxr...	16,842,...
.container_3		₩	4.0 KB	1970-01-01 09:17:25.4	1970-01-01 09:17:25.4	1970-01-01 09:17:25.4	1970-01-08 01:35:33.6	rwxr...	25,231,...
anr		₩	4.0 KB	1970-01-01 09:17:25.4	1970-01-01 09:17:25.4	1970-01-01 09:17:25.4	1970-01-08 01:35:33.6	rwxr...	16,842,...
app		₩	8.0 KB	1970-01-01 09:17:25.4	2013-11-21 01:45:10.9	1970-01-01 09:17:25.4	1970-01-08 01:35:33.6	rwxr...	42,008,...
app-asec		₩	4.0 KB	1970-01-01 09:17:25.4	1970-01-01 09:17:25.4	1970-01-01 09:17:25.4	1970-01-08 01:35:33.6	rwxr...	29,425,...
app-lib		₩	8.0 KB	1970-01-01 09:17:25.4	2013-11-21 01:45:10.9	1970-01-01 09:17:25.4	1970-01-08 01:35:33.6	rwxr...	37,814,...
app-private		₩	4.0 KB	1970-01-01 09:17:25.4	1970-01-01 09:17:25.4	1970-01-01 09:17:25.4	1970-01-08 01:35:33.6	rwxr...	25,231,...
audio		₩	4.0 KB	1970-01-01 09:17:25.4	1970-01-01 09:17:25.4	1970-01-01 09:17:25.4	1970-01-08 01:35:33.6	rwxr...	65,720
backup		₩	4.0 KB	1970-01-01 09:17:25.4	2013-01-01 09:01:42.4	1970-01-01 09:17:25.4	1970-01-08 01:35:33.6	rwxr...	29,425,...
bcmnfc		₩	4.0 KB	1970-01-01 09:17:25.8	2013-01-01 09:01:48.8	1970-01-01 09:17:25.8	1970-01-08 01:35:33.6	rwxr...	33,620,...
clipboard		₩	4.0 KB	2013-01-01 09:01:41.3	2013-01-01 09:01:41.3	2013-01-01 09:01:41.3	2013-01-01 09:01:41.3	rwxr...	16,842,...
connectivity		₩	4.0 KB	1970-01-01 09:17:25.4	2013-01-01 09:00:03.1	1970-01-01 09:17:25.4	1970-01-08 01:35:33.6	rwxr...	16,842,...
container		₩	4.0 KB	1970-01-01 09:17:25.4	2013-01-01 09:01:45.5	1970-01-01 09:17:25.4	2013-11-21 02:08:02.8	rwxr...	65,712
dalvik-cache		₩	16.0 KB	1970-01-01 09:17:25.4	2013-11-21 01:45:10.9	1970-01-01 09:17:25.4	1970-01-08 01:35:33.6	rwxr...	4,259,9...
data		₩	16.0 KB	1970-01-01 09:17:25.4	2013-11-21 01:45:10.2	1970-01-01 09:17:25.4	1970-01-08 01:35:33.6	rwxr...	21,037,...
data1		₩	4.0 KB	2013-01-01 09:01:45.5	2013-09-14 13:42:38.4	2013-01-01 09:01:45.5	2013-11-21 02:08:02.8	rwxr...	46,203,...
dontpanic		₩	4.0 KB	1970-01-01 09:17:25.4	1970-01-01 09:17:25.4	1970-01-01 09:17:25.4	1970-01-08 01:35:33.6	rwxr...	33,620,...
drm		₩	4.0 KB	1970-01-01 09:17:25.4	2013-01-01 09:01:46.9	1970-01-01 09:17:25.4	1970-01-08 01:35:33.6	rwxr...	33,620,...
fota		₩	4.0 KB	1970-01-01 09:17:25.4	1970-01-01 09:17:25.4	1970-01-01 09:17:25.4	1970-01-08 01:35:33.6	rwxr...	33,620,...
hostapd		₩	4.0 KB	1970-01-01 09:17:25.4	1970-01-01 09:17:25.4	1970-01-01 09:17:25.4	1970-01-08 01:35:33.6	rwxr...	37,814,...
KEqvTaYkUjR1Mn+t-SwFvbgYo_		₩	4.0 KB	2013-09-14 19:39:57.4	2013-09-14 19:39:57.5	2013-09-14 19:39:57.4	2013-09-14 19:39:57.5	rwxr...	4,260,0...
local		₩	4.0 KB	1970-01-01 09:17:25.4	1970-01-01 09:17:25.4	1970-01-01 09:17:25.4	1970-01-08 01:35:33.6	rwxr...	12,648,...
log		₩	4.0 KB	1970-01-01 09:17:15.4	2013-11-21 02:08:35.6	1970-01-01 09:17:15.4	2013-11-21 02:08:35.6	rwxr...	4,259,9...
lost+found		₩	4.0 KB				1970-01-08 01:35:33.6	rwxr...	65,704
media		₩	4.0 KB	1970-01-01 09:17:25.9	2013-01-01 09:01:44.0	1970-01-01 09:17:25.9	2013-11-21 02:08:06.6	rwxr...	37,814,...
mediadrms		₩	4.0 KB	1970-01-01 09:17:25.4	1970-01-01 09:17:25.4	1970-01-01 09:17:25.4	1970-01-08 01:35:33.6	rwxr...	37,814,...
misc		₩	4.0 KB	1970-01-01 09:17:25.4	1970-01-01 09:17:25.4	1970-01-01 09:17:25.4	1970-01-08 01:35:33.6	rwxr...	8,454,2...
monitor		₩	4.0 KB	2013-01-01 09:01:41.3	2013-01-01 09:01:41.3	2013-01-01 09:01:41.3	2013-11-21 02:07:59.9	rwxr...	25,231,...

# 스마트기기 앱 분석

## ■ 앱 분석의 필요성

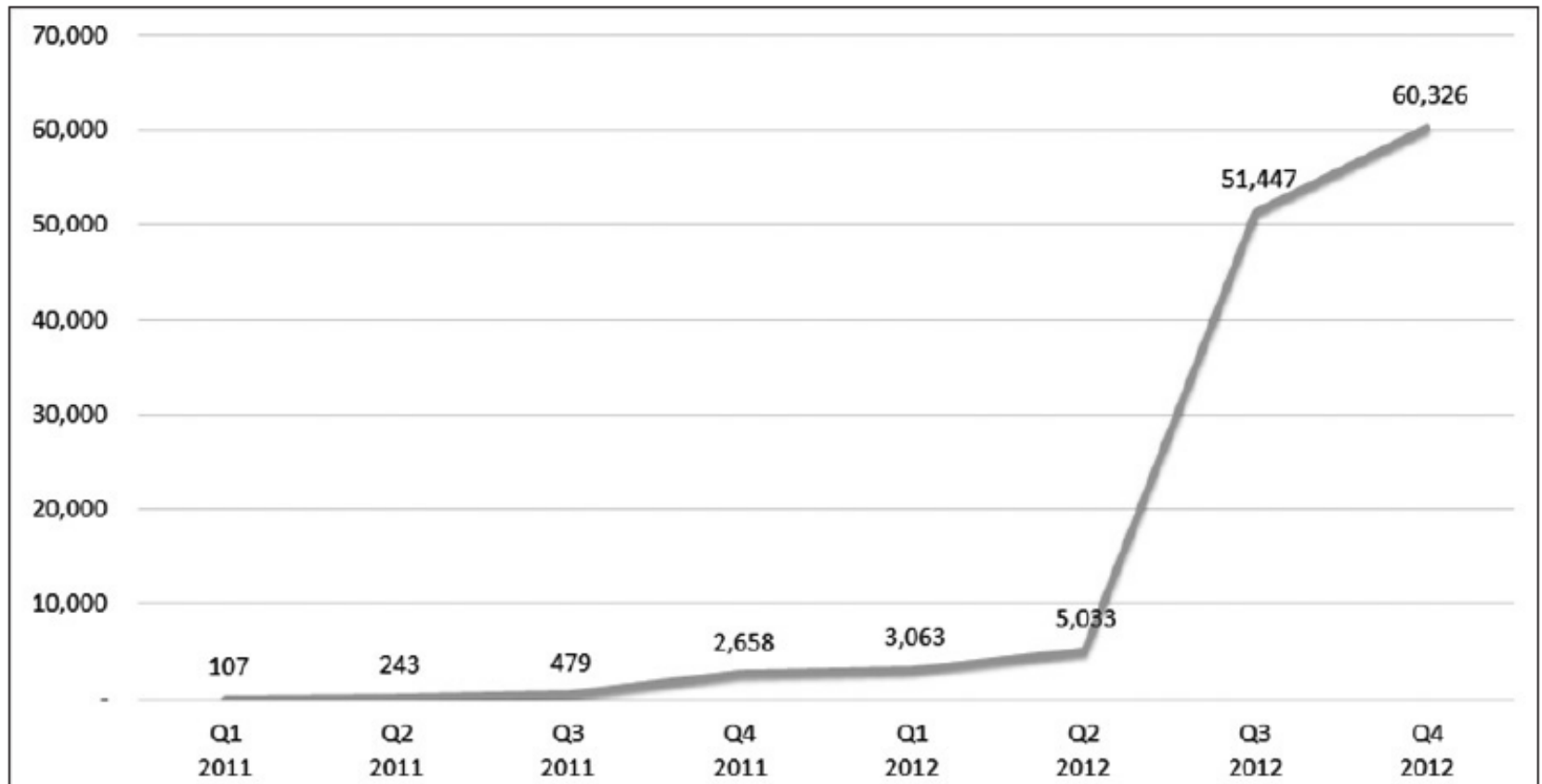
### • 안드로이드 보안위협

- ✓ 개인정보 유출 (SMS, 주소록, 통화내역, 위치정보 등)
- ✓ 공인인증서 탈취
- ✓ 과금 유도
- ✓ 원격 제어
- ✓ 소액 결제
- ✓ 스팸 메일, 문자 발송
- ✓ 추가 악성코드 배포

# 스마트기기 앱 분석

## ■ 보안 위협

- 분기별 APK 형태의 보안위협 발견 수



[http://www.f-secure.com/en/web/labs\\_global/whitepapers/reports](http://www.f-secure.com/en/web/labs_global/whitepapers/reports)

## ▪ 안드로이드 플랫폼 환경

### • APK (Android Package)

✓ 앱 설치를 위해 배포되는 패키지

✓ APK 파일 구성 요소

- **AndroidManifest.xml** : 앱 설명, 실행 권한 등의 정보를 가진 XML 파일
- **classes.dex** : 달빅 가상머신에서 동작하는 바이너리 실행 파일
- **/res** : 컴파일되지 않은 리소스 파일로 아아콘, 이미지, 음악 등 포함
- **META-INF** : 배포 시 인증서로 서명한 내용, APK 파일 내부의 파일/폴더의 SHA-1 해시값
- **resources.arsc** : 컴파일된 리소스 파일

### • DEX (Dalvik Executable)

✓ 달빅 가상머신에서 동작하도록 클래스 파일을 바이트 코드로 변환한 파일

✓ 자바 파일 컴파일 ➔ 클래스 파일 ➔ DEX

## ■ 정적 분석 방법

- 프로그램 실행 없이 파일 자체로만 분석하는 방법
- 설치된 앱의 APK 파일을 추출한 후 이를 검증

### 1) 앱의 권한 분석

- ✓ AndroidManifest.xml 파일을 분석하여 요구하는 권한 분석
- ✓ 각 권한의 의미 파악
  - <http://developer.android.com/reference/android/Manifest.permission.html>

### 2) 악성코드 은닉 여부

- ✓ 이미지, XML 파일로 가장한 악성코드 점검

### 3) 소스코드 분석

- ✓ 디컴파일된 소스를 분석하여 악성 행위 파악



## ➔ 실습

- 안드로이드 앱 정적 분석하기!!

- 1) AFLogical 앱 설치 후 실행하기

- <https://viaforensics.com/resources/tools/android-forensics-tool/>

- 2) ADB(Android Debug Bridge) 설치된 AFLogical 앱 추출하기

- # adb shell
- # pm list packages -f
- # adb pull /data/app/xxx.xxxxx.apk

- 3) APK 파일 디컴파일하기

- APKTOOL을 이용해 디컴파일, <https://code.google.com/p/android-apktool/>
  - # apktool d[ecode] [OPTS] xxxxx.apk
- ➔ AndroidManifest.xml, smali 코드 분석

## ➔ 실습

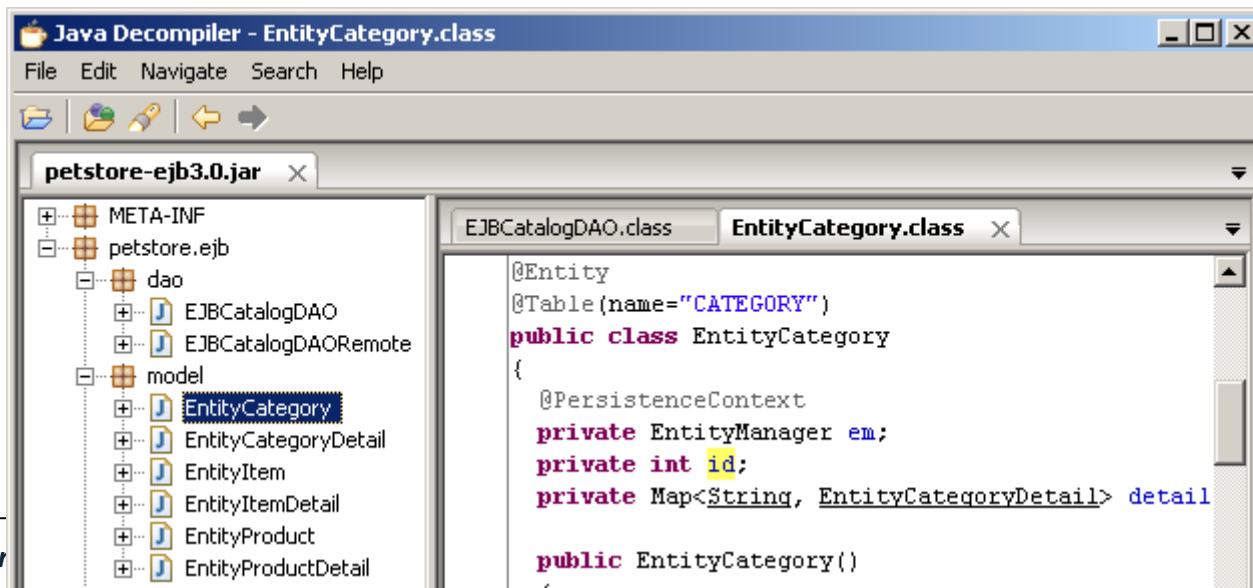
- 안드로이드 앱 정적 분석하기!!

### 4) JAVA 코드 분석하기

- APK 파일 확장자를 ZIP으로 변경한 후 압축 해제
- DEX2JAR를 이용해 classes.dex 파일 JAR로 변환, <https://code.google.com/p/dex2jar/>
- # d2j-dex2jar [options] classes.dex

### 5) 자바 디컴파일러로 자바 코드 분석하기

- JAD, jd-gui 도구로 JAVA 코드 분석,



## ➔ 실습

- 안드로이드 앱 정적 분석하기!!

### 6) Dexter로 앱 정적 분석하기

- Dexter, <https://dexter.bluebox.com/>

## ▪ 동적 분석 방법

- 프로그램을 실제로 동작시킨 후 모니터링하여 분석하는 방법
- 네트워크 접속 정보, 통신 내역, 동작 로그, 시스템 로그 등
- **Monkey**, <http://developer.android.com/tools/help/monkey.html>
  - ✓ Android SDK에서 제공
  - ✓ 앱을 실행한 후 클릭, 터치, 제스처 등 사용자 이벤트를 무작위로 발생시킨 후 로그 수집
- **Tcpdump**, <http://www.tcpdump.org/>
  - ✓ Tcpdump를 스마트폰에 넣은 후 루트 권한으로 실행 후 로그 수집

## ▪ 온라인 서비스 이용

- **SandDroid**, <http://sanddroid.xjtu.edu.cn/>
- **AndroTotal**, <http://andrototal.org/>
- **Anubis**, <http://anubis.iseclab.org/>
- **AMAT**, [http://dunkelheit.com.br/amat/analysis/index\\_en.php](http://dunkelheit.com.br/amat/analysis/index_en.php)
- **CopperDroid**, <http://copperdroid.isg.rhul.ac.uk/copperdroid/>
- **Dexter**, <https://dexter.bluebox.com/>
- **Mobile Sandbox**, <http://mobilesandbox.org/>

## ➔ 실습

- SandDroid로 악성 앱 분석하기!!
  - ✓ 악성 앱 다운로드
    - <http://rogunix.com/docs/Android/Malware/>
    - <http://contagiominedump.blogspot.com.es/?m=1>

# 스마트기기 앱 아티팩트

## ▪ 앱 아티팩트 분석 방법

### • 데이터베이스 파일

- ✓ 기본 정보와 대부분의 App은 관련 데이터를 데이터베이스(주로 SQLite) 파일로 관리

### • 위치 정보

- ✓ 위치 기반 App의 위치 정보와 시간 정보를 이용해 사용자의 이동 경로 추적

### • 타임라인 분석

- ✓ 다양한 App 데이터를 시간 정보를 기준으로 분석

### • 연관관계 분석

- ✓ 통화/문자빈도, 통화시간, 문자 건수 등 다양한 데이터 연관관계 분석

### • 삭제된 데이터

- ✓ 비할당 영역 복구, SQLite 복구



## ▪ SQLite 분석

### • SQLite

✓ 스마트기기의 대부분은 SQLite 형식의 파일 데이터베이스 사용

#### ✓ 분석 방법

- 테이블 데이터 추출
- 필요에 따라 테이블간 키 값 조인
- 삭제된 레코드 복구

#### ✓ 분석 도구

- **Oxygen Forensic SQLite Viewer** (삭제된 레코드 복구 기능 포함)  
<http://www.oxygen-forensic.com/en/features/analyst/data-viewers/sqlite-viewer>
- **SQLite Expert**  
<http://www.sqliteexpert.com/download.html>

# 스마트기기 앱 아티팩트

## ■ SQLite 분석

### • 주요 앱 데이터베이스 경로

앱	경로
페이스북	/data/data/com.facebook.katana/databases/fb.db
트위터	/data/data/com.twitter.android/databases/twitter
카카오톡	/data/data/com.kakao.talk/databases/KakaoTalk.db
에버노트	/data/data/com.evernote/databases/Evernote.db /data/data/com.evernote/databases/webview.db
스카이프	/data/data/com.skype.raider/files/skype
구글맵	/dbdata/databases/com.google.android.apps.maps/search_history.db /data/data/com.google.android.apps.maps/databases/search_history.db /data/data/com.google.android.apps.maps/files/DATA_STARRING
다음맵	/data/data/net.daum.android.map/map/data/favorite.db /data/data/net.daum.android.map/map/data/history.db
네이버맵	/data/data/com.nhn.android.nmap/databases/mapHistory.db
드롭박스	/data/data/com.dropbox.android/databases/db.db
네이버 라인	/data/data/jp.naver.line.android/databases/naver_line
네이트온	/data/data/Uxpp.UC/databases/nateon.db /data/data/Uxpp.UC/databases/nateon_message.db

# 스마트기기 앱 아티팩트

## ■ SQLite 분석

### • 예) 카카오톡 분석

#### ✓ 아티팩트 저장 경로

- /data/data/com.kakao.talk/databases/KakaoTalk.db

#### ✓ 테이블

- chat\_logs – 채팅 메시지
- chat-rooms – 채팅 방 정보
- Friends – 친구 목록

RecNo	_id	id	type	chat_id	user_id	message	attachment	created_at
Click here to define a filter								
2	2	27094084020	1	164547305	13166188	행님!!! 기계 많이 팔았소 ㄱ	<null>	1305340177
3	3	27094322394	1	164547305	1765860	한개도 못팔았다	<null>	1305340245
4	4	27094425034	1	164547305	1765860	경산	<null>	1305340274
5	5	27094576995	1	164547305	13166188	경산은 뭐코	<null>	1305340318
6	6	27094667163	1	164547305	1765860	경상남도 함안으로 가는중 이니 말시키지마	<null>	1305340343
7	7	27094756679	1	164547305	13166188	기계 배달가나	<null>	1305340369
8	8	23677831315	1	145647677	11985893	고마 디비지라!! 갓다원나??	<null>	1304248495
9	9	18178279596	1	14866807	1072301	너도 카톡을 하네....	<null>	1302227927
10	10	17542553930	1	117196722	9244478	조수? 5월말까지 ㄱ기 가능하디네	<null>	1301976312
11	11	70188022024	1	388351672	180	라.	<null>	1314179374
12	12	70188340516	1	388351672	180	케 많	<null>	1314179409
13	13	70280761976	1	388351672	1		<null>	1314189166
14	14	70309047743	1	388351672	180		<null>	1314191819
15	15	70738340418	1	388351672	180		<null>	1314264473
16	16	71099868074	1	388351672	1		<null>	1314325440
17	17	75302132725	1	408924848	2	요?	<null>	1314964091
18	18	75302647608	1	408924848	2	카톡	<null>	1314964142
19	19	75304818899	1	408924848	1		<null>	1314964358
20	20	75305595706	1	408924848	2		<null>	1314964435
21	21	75305886122	1	408924848	1		<null>	1314964464
22	22	76992591451	1	388351672	1		<null>	1315232058
23	23	76992952883	1	388351672	1		<null>	1315232084
24	24	76993044374	1	388351672	180		<null>	1315232091
25	25	76993062134	1	388351672	1		<null>	1315232092
26	26	76993616480	1	388351672	180		<null>	1315232133
27	27	76993646305	1	388351672	1		<null>	1315232135
28	28	76993936428	1	388351672	18032629	그냥 컴퓨터 앞에서 이것저것 하고 있다	<null>	1315232156
29	29	76994191261	1	388351672	1765860	세상 이 질ㄴ	<null>	1315232174
30	30	76994396533	1	388351672	18032629	10시16분 1시간 차이다	<null>	1315232190
31	31	76994958864	1	388351672	1765860	세상이 지랄같아서	<null>	1315232231
32	32	76995196321	1	388351672	18032629	또 와....	<null>	1315232248
33	33	76995627688	1	388351672	1765860	맥주함잔한다	<null>	1315232280

# 스마트기기 앱 아티팩트

## ■ SQLite 분석

### • 예) 카카오톡 분석

#### ✓ chat\_logs 테이블

Database: KakaoTalk Table: chat\_logs File: C:\Users\dohyun\Desktop\테스트\비밀1\KakaoTalk.db

RecNo	_id	id	type	chat_id	user_id	message	attachment	created_at
1	1	5978995999	1	14866807	1072301	경녕아 앞으로 카톡을 많이 써라	<null>	1295327528
2	2	27094084020	1	164547305	13166188	행님!!! 기계 많이 팔았소 ㄱ	<null>	1305340177
3	3	27094322394	1	164547305	1765860	한개도 못팔았다	<null>	1305340245
4	4	27094425034	1	164547305	1765860	깡산	<null>	1305340274
5	5	27094576995	1	164547305	13166188	깡산은 뭐코	<null>	1305340318
6	6	27094667163	1	164547305	1765860	경상남도 함안으로 가는중 이니 말시키지마	<null>	1305340343
7	7	27094756679	1	164547305	13166188	기계 배달가나	<null>	1305340369
8	8	23677831315	1	145647677	11985893	고마 디비지라!! 갓다완나??	<null>	1304248495
9	9	18178279596	1	14866807	1072301	너도 카톡을 하네....	<null>	1302227927
10	10	17542553930	1	117196722	9244428	주소? 5월말경 출고 가능하다네	<null>	1301976312
11	11	70188022024	1	388351672	18032629	경녕아 잘 있나? 이번 겨울에는 함 놀러 오너라....	<null>	1314179374
12	12	70188340516	1	388351672	18032629	너도 카톡을 다하고 많이 발전했다. 형님한테 많이 배웠지.....	<null>	1314179409
13	13	70280761976	1	388351672	1765860	니때에 자다갓다	<null>	1314189166
14	14	70309047743	1	388351672	18032629	뭐한다고... 대낮부터 잠이나 자고....	<null>	1314191819
15	15	70738340418	1	388351672	18032629	오늘도 자고 있나?	<null>	1314264473
16	16	71099868074	1	388351672	1765860	안잔다	<null>	1314325440
17	17	75302132725	1	408924848	2201679	삼촌! 민정이에요~! 일요일 몇시까지 가야해요?	<null>	1314964091
18	18	75302647608	1	408924848	2201679	ㄱㄱ 안녕하세요 조서방입니다 민정이가 제 카톡으로 메세지 보냈네요	<null>	1314964142
19	19	75304818899	1	408924848	1765860	오후 한시반에 시작이라ندا	<null>	1314964358
20	20	75305595706	1	408924848	2201679	네 그날 봐어요 엄마는 내일 올라오신대요	<null>	1314964435

# 스마트기기 앱 아티팩트

## ■ SQLite 분석

### • 예) 카카오톡 분석

#### ✓ chat\_rooms 테이블

Database: KakaoTalk Table: chat\_rooms File: C:\Users\dohyun\Desktop\테스트\비밀\1\KakaoTalk.db

RecNo	_id	id	type	title	members	active_member_ids
1	1	14866807	DirectChat		[1072301]	[1072301]
2	2	117196722	DirectChat		[9244428]	[9244428]
3	3	145647677	DirectChat		[11985893]	[11985893]
4	4	164547305	DirectChat		[13166188]	[13166188]
5	5	388351672	DirectChat		[18032629]	[18032629]
6	6	408924848	DirectChat		[2201679]	[2201679]
7	7	446355680	MultiChat		[19042694,6112102,395693,7158117,3554909,1954010,4057119,9785560]	[7158117,1954010]
8	8	481548606	DirectChat		[10563520]	[10563520]
9	9	590710061	DirectChat		[27349894]	[27349894]
10	10	658561316	DirectChat		[1410488]	[1410488]
11	11	685729722	MultiChat		[7169995,11926937,8098405,24474528,9174372,8135523,8940150,9079939,25065911,5068374,20825627,29565561,27599058,7938203]	[8135523,7169995,9079939]

# 스마트기기 앱 아티팩트

## ■ SQLite 분석

### • 예) 카카오톡 분석

#### ✓ friends 테이블

Database: KakaoTalk Table: friends File: C:\Users\#dohyun\Desktop\테스트\디비\#1\KakaoTalk.db

Database SQL Data Design DDL

Refresh

RecNo	_id	contact_id	id	type	uuid	phone_number	raw_phone_number	name
1	2	182	250637	2				
2	3	43	1721248	2				
3	4	173	1169683	2				
4	6	80	288288	2	pahkpd			
5	7	38	297043	2	busanyc			
6	8	895	1960123	2				
7	9	107	2054278	2	siny76			
8	11	155	533928	2				
9	12	49	2437279	2	ATATURK			
10	14	48	2035360	2	prprpp			
11	16	52	1465583	2				
12	19	199	3290447	2				

## ▪ SQLite 분석

### • 삭제된 데이터 복구

✓ **SQLite Viewer** – Oxygen Forensics

- <http://www.oxygen-forensic.com/en/features/analyst/data-viewers/sqlite-viewer>

✓ **UNDARK** – pldaniels

- <http://pldaniels.com/undark/>

✓ **SQLParse.py** – Another Forensics Blog

- <http://az4n6.blogspot.kr/2013/11/python-parser-to-recover-deleted-sqlite.html>

## ▪ XML 파일 분석

### • 주요 XML 파일

#### ✓ 시스템, 앱, 사용자 설정 정보 저장

- /data/data/com.android.vending/shared\_prefs/**vending\_preferences.xml**
- /data/data/com.android.vending/shared\_prefs/**finsky.xml**
- /data/data/com.android.phone/shared\_prefs/**com.android.phone\_preferences.xml**
- /data/data/Com.sktelecom.minit/shared\_prefs/**com.sktelecom.minit\_preferences.xml**
- /data/data/com.kakao.talk/shared\_prefs/**KakaoTalk.preferences.xml**
- /data/data/com.kth.widgets.uucloud/shared\_prefs/**UCloudPref.xml**
- /data/data/Uxpp.UC/shared\_prefs/**nateon\_login.xml**
- ... ..



# 스마트기기 앱 아티팩트

## ■ XML 파일 분석

### • 주요 XML 파일

✓ /system/packages.xml

```
packages.xml
704 </package>
705 <package name="com.gogii.textplus" codePath="/data/app/com.gogii.textplus" />
706 <sigs count="1">
707   <cert index="12" key="3082026b308201d4a00302010202044b3c01a" />
708 </sigs>
709 <perms>
710   <item name="android.permission.READ_EXTERNAL_STORAGE" />
711   <item name="android.permission.PROCESS_OUTGOING_CALLS" />
712   <item name="android.permission.WRITE_EXTERNAL_STORAGE" />
713   <item name="android.permission.WRITE_CALL_LOG" />
714   <item name="android.permission.WRITE_SMS" />
715   <item name="android.permission.ACCESS_WIFI_STATE" />
716   <item name="android.permission.RECEIVE_SMS" />
717   <item name="android.permission.CALL_PHONE" />
718   <item name="android.permission.GET_ACCOUNTS" />
719   <item name="android.permission.READ_CONTACTS" />
720   <item name="android.permission.WRITE_CONTACTS" />
721   <item name="android.permission.READ_PHONE_STATE" />
722   <item name="android.permission.READ_SMS" />
723   <item name="android.permission.RECEIVE_BOOT_COMPLETED" />
724   <item name="android.permission.MANAGE_ACCOUNTS" />
725   <item name="android.permission.BROADCAST_STICKY" />
726   <item name="android.permission.USE_SIP" />
727   <item name="android.permission.RECORD_AUDIO" />
728   <item name="android.permission.WAKE_LOCK" />
729   <item name="android.permission.ACCESS_NETWORK_STATE" />
730   <item name="android.permission.SEND_SMS" />
731   <item name="android.permission.RECEIVE_MMS" />
732   <item name="com.google.android.c2dm.permission.RECEIVE" />
733   <item name="android.permission.MODIFY_AUDIO_SETTINGS" />
734   <item name="android.permission.DISABLE_KEYGUARD" />
735   <item name="com.android.vending.BILLING" />
736   <item name="android.permission.BLUETOOTH" />
737   <item name="android.permission.WRITE_SETTINGS" />
738   <item name="android.permission.INTERNET" />
739   <item name="com.gogii.textplus.permission.C2D_MESSAGE" />
740   <item name="android.permission.VIBRATE" />
741   <item name="android.permission.READ_CALL_LOG" />
742   <item name="android.permission.CHANGE_NETWORK_STATE" />
```

- **Plist 파일 분석**

- **Plist(Property List)**

- ✓ iPhone에서 앱이나 사용자 설정 정보 저장을 위해 사용

- **앱 정보**

- ✓ 국가 정보, 마지막 업데이트 시간 등

- **사용자 설정 정보**

- ✓ 전화번호, 닉네임, 이메일, User ID, 프로필 정도 등

- **분석 방법**

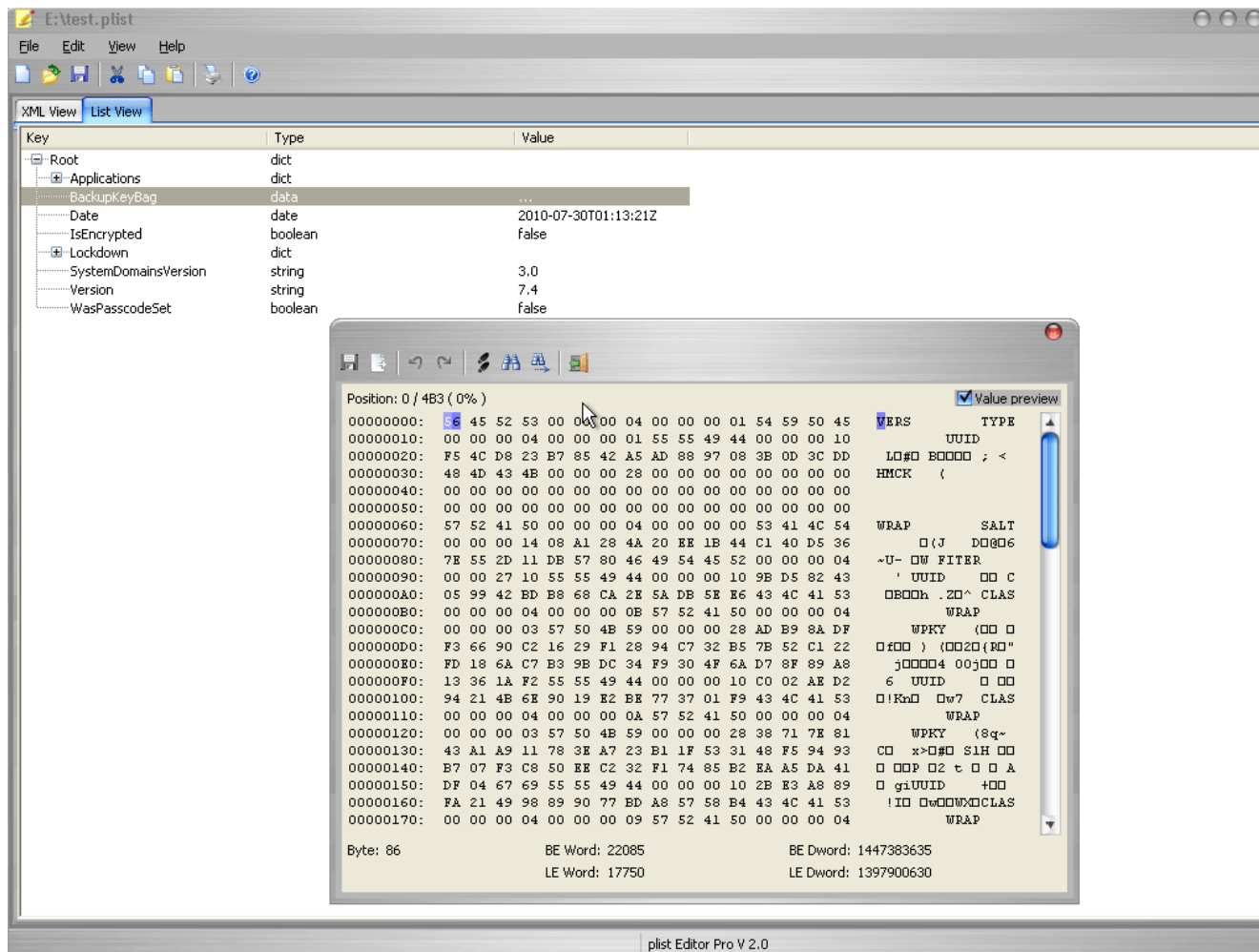
- ✓ Plist 편집기를 이용해 분석

- ✓ **Plist Editor** – <http://www.icopybot.com/plist-editor.htm>

# 스마트기기 앱 아티팩트

## ■ Plist 파일 분석

### • Plist Editor



# 스마트기기 포렌식 도구

# 스마트기기 포렌식 도구

## ▪ 주요 스마트기기 포렌식 도구

- GMD System **MD-UBOX, MD-Smart** (펌웨어 프로토콜?)
- DATA DOCTOR **SMART NEBULA** (복구 이미지 플래싱)
- EnCase **Smartphone Examiner**
- AccessData **MPE+(Mobile Phone Examiner Plus)**
- Oxygen Software **Oxygen Forensic Suite** (루팅, APK 설치)
- Cellbrite **UFED** (취약점 이용)
- Micro Systemation **XRY/XACT** (루팅, APK 설치)
- Paraben **Device Seizure**

# 스마트기기 포렌식 도구

## ■ GMD System MD-\*

### • 데이터 획득

✓ MD-BOX, MD-Extractor

- JTAG을 이용한 추출
- 아이폰 백업 데이터 추출

✓ MD-UBOX

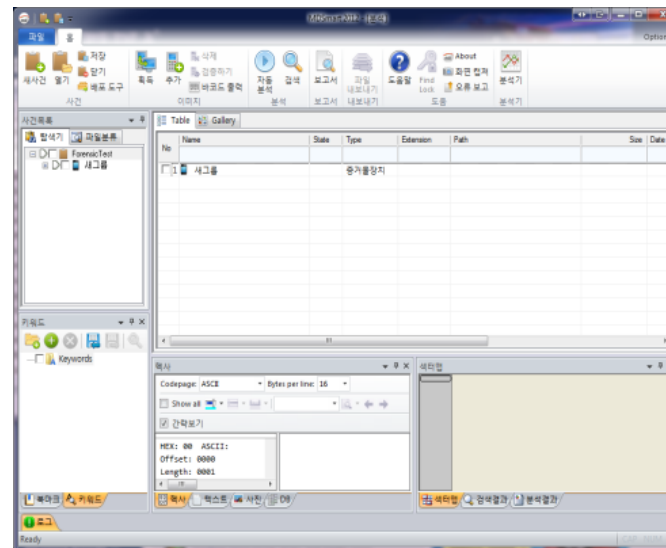
- 안드로이드 펌웨어 프로토콜 추출?



### • 데이터 분석

✓ MD-Smart

- 파일시스템 분석
- 앱 데이터 분석



# 스마트기기 포렌식 도구

## DATA DOCTOR Smart\*

### 데이터 획득

#### ✓ SMART JMR

- JTAG를 이용한 추출

#### ✓ SMART UMR

- 안드로이드 플래싱

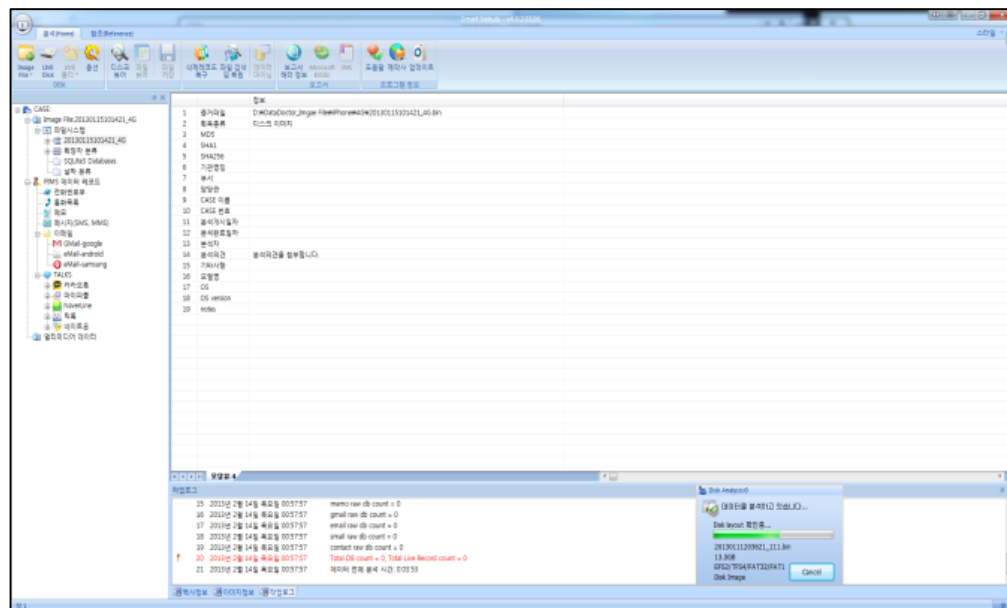
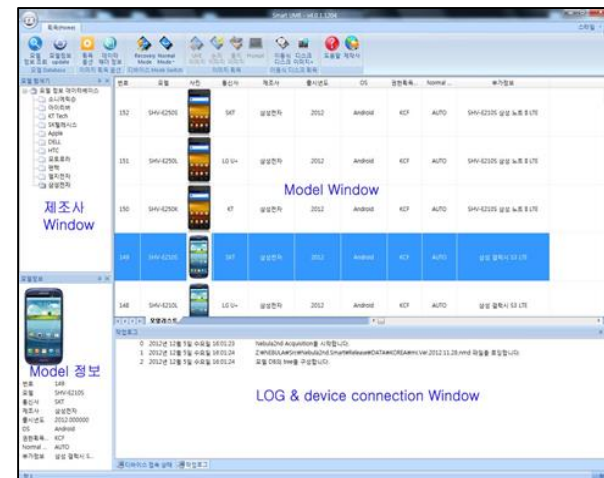
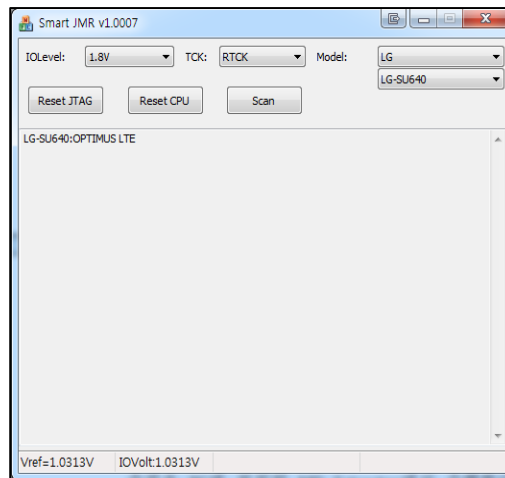
#### ✓ AcquiPhone

- 아이폰 백업 데이터 추출

### 데이터 분석

#### ✓ SMART NEBULA

- 파일시스템 분석
- 앱 데이터 분석



# 스마트기기 포렌식 도구

## ■ Cellebrite UFED

### • 데이터 수집

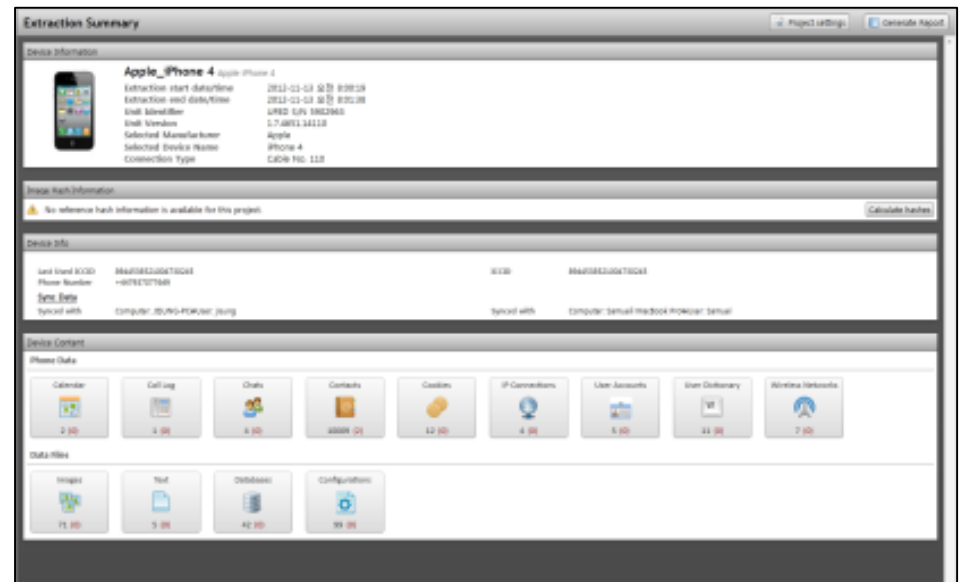
#### ✓ UFED Touch

- 안드로이드 익스플로잇 루팅
- 아이폰 백업 데이터 추출

### • 데이터 분석

#### ✓ Physical Analyzer

- 파일시스템 분석
- 앱 데이터 분석





# 스마트기기 포렌식 도구

## ■ Micro Systemation XRY

### • 데이터 획득

#### ✓ XRY Extraction Wizard

- 안드로이드 CP를 사용하여 추출
- 아이폰 백업 데이터 추출
- 다수의 국내 스마트폰 미지원



### • 데이터 분석

#### ✓ XRY

- 파일시스템 분석
- 앱 데이터 분석
- 타임라인

