SeoulTech

모바일 포렌식

박 종 혁 교수

UCS Lab

Tel: 970-6702

Email: jhpark1@soultech.ac.kr

목 차

모바일포렌식 개요

모바일 포렌식 개요

- 모바일 포렌식
  - 휴대폰, 스마트폰등 소형화된 기기에 저장된 데이터 추출
  - 다양한 플랫폼, 파일구조등 존재

Smart Phone

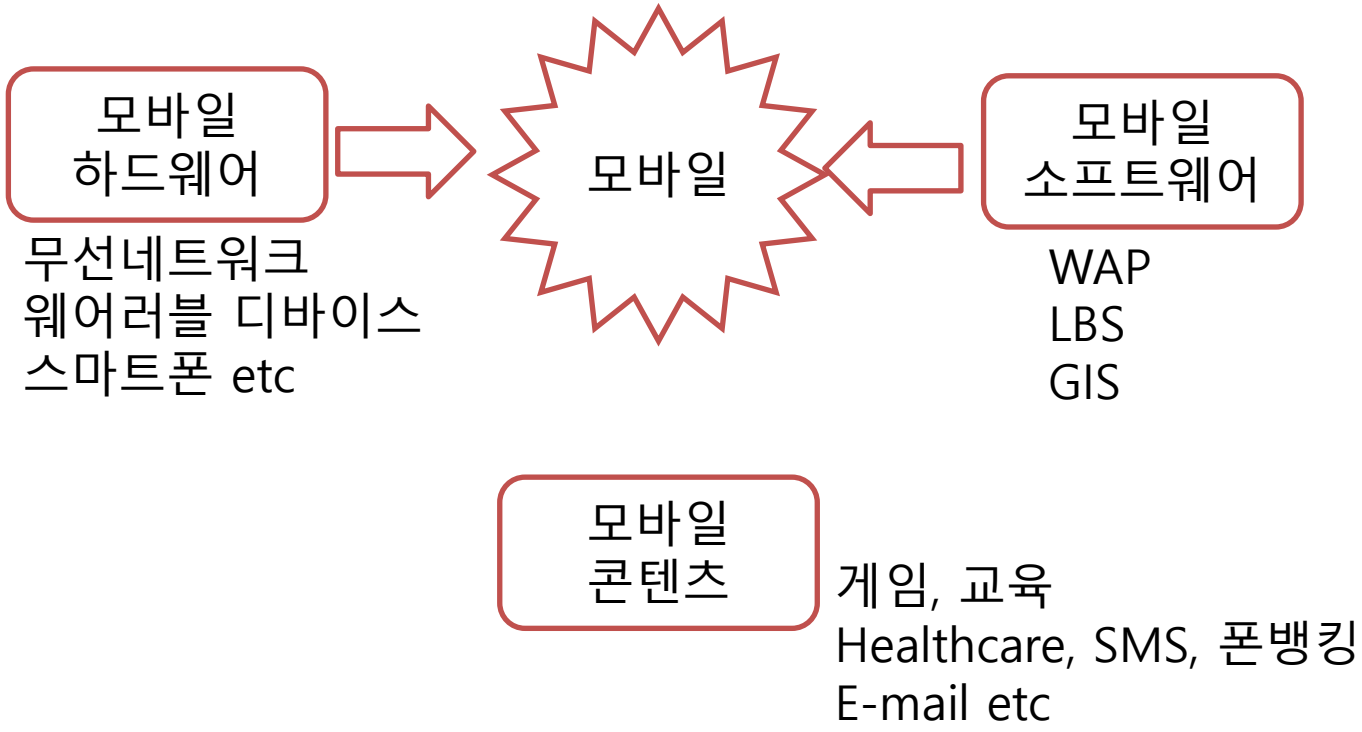
Wearable Device

USB Driver

Mobile game, Smartcard,
E-book etc..

모바일 포렌식 개요

- 모바일의 구성
  - 하드웨어, 소프트웨어, 컨텐츠로 구성
  - 디지털증거는 다양한 정보들을 수집하여 분석



모바일 포렌식 개요

- 모바일 포렌식의 문제점
  - 국내외적으로 상이한 포멧 : 국내 CDMA, 국외 GSM 방식
  - 통신환경의 급속한 변화 : 통합융합, USIM카드 도입
  - 파일의 비표준화 : 동일 모델이라도 파일 규격 상이
  - 통신케이블의 비표준화

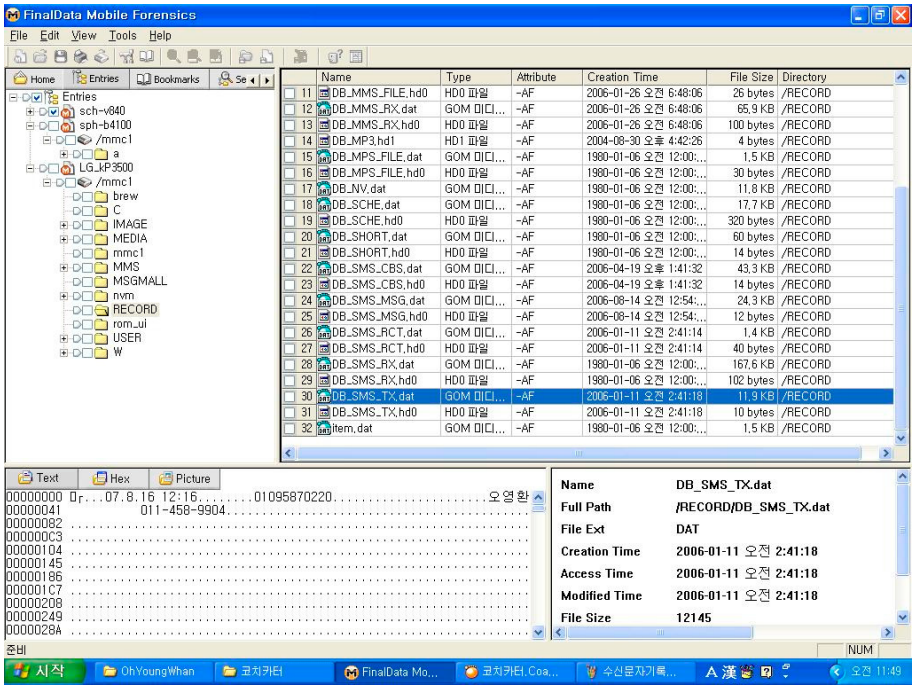
모바일 포렌식의 절차에 따른 분류

모바일 포렌식의 절차에 따른 분류

- SYN통신을 이용한 데이터 추출
  - 충전 단자의 통신 포트를 이용한 접근.
- JTAG (Joint Test Action Group) 를 이용한 데이터 추출
  - 하드웨어 칩 디버깅을 위한 프로그래밍과 삭제된 데이터 복원 기법 이용
- 플래쉬메모리 직접 데이터 추출
  - 휴대폰의 고장 혹은 파손시 지원

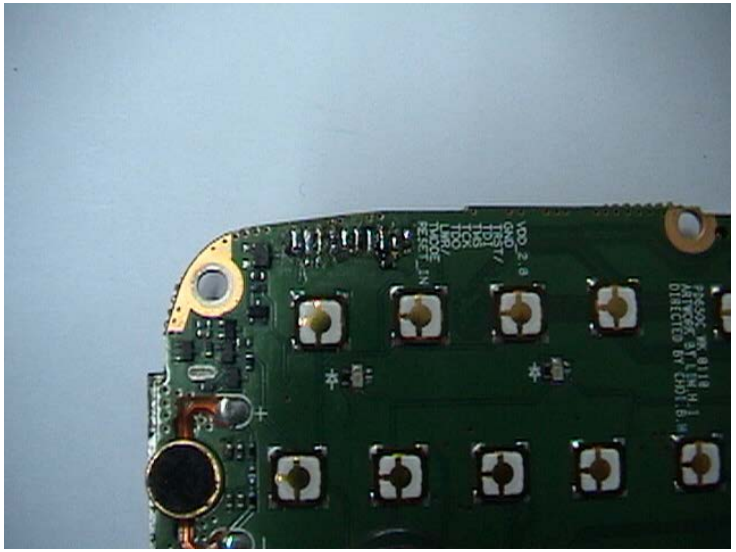
모바일 포렌식의 절차에 따른 분류

- SYN통신을 이용한 데이터 추출
  - 데이터 통신을 위하여 각 회사별로 지원하는 프로토콜 이용
  - 비할당된 영역으로부터 삭제되지 않은 데이터 및 삭제 표시가 되었으나 삭제되지 않은 데이터 추출
  - 정상적인 동작으로 라이브 데이터 유입 가능성 존재



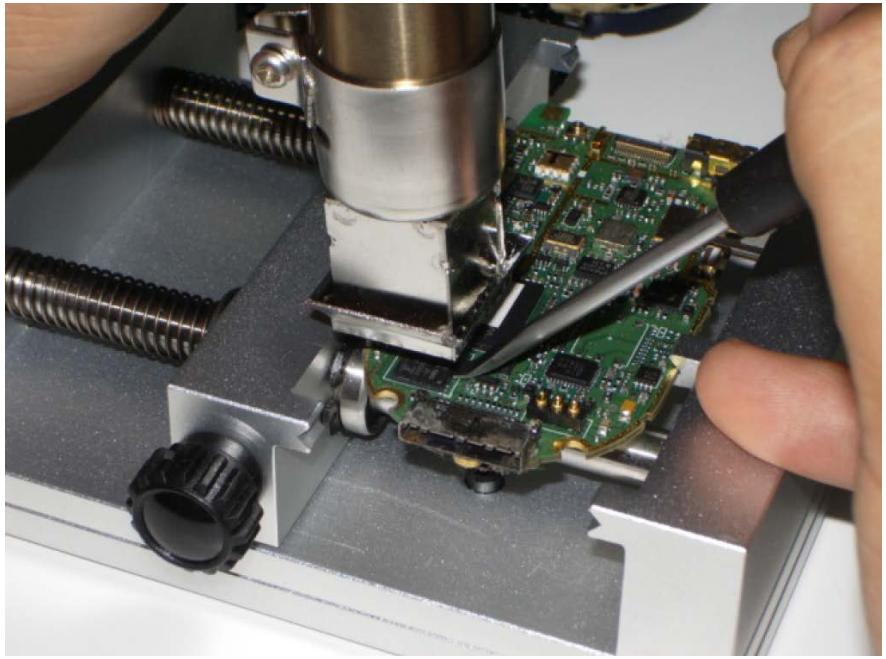
모바일 포렌식의 절차에 따른 분류

- JTAG (Joint Test Action Group) 를 이용한 데이터 추출
  - 모바일 기기의 케이블 핀 번호가 서로 다르므로 기기별로 최적화하여 분석해야 함
  - 케이블 포트를 삭제하거나 디버깅 데이터를 변환하기도 함
  - 삭제되거나 일부 덮여진 데이터 추출 가능



모바일 포렌식의 절차에 따른 분류

- 플래쉬메모리 직접 데이터 추출
  - 휴대폰의 고장, 심각한 훼손시 데이터 추출
  - 메모리를 분리하여 정보를 추출
  - 모바일의 무결성에 치명적인 손실 발생



장비를 이용한 메모리 추출

스마트폰 포렌식

스마트폰 포렌식

스마트폰의 포렌식 데이터 (1/2)

❖ 스마트폰 사용 자들의 스마트폰을 이용해서 전화통화나 문자 메시지뿐 만 아니라 할 일, 일정관리, 메모, 이메일, 인터넷, 사 진, 비디오, 음악 등 상당히 많은 활동을 하며, 그 기록 들은 스마트폰에 저장함

❖ 포렌식 관점에서 스마트폰 의 기본 애플리케이션에 저장된 데이터를 정리하면 다음과 같음

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

스마트폰 포렌식

● 스마트폰의 포렌식 데이터 (2/2)

❖ 기본 애플리케이션 외에도 사용자가 직접 설치한 애플리케이션에서는 다음과 같은 개인 정보가 저장

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

스마트폰 포렌식

● 스마트폰의 포렌식의 절차

❖ 스마트폰 포렌식의 절차는 컴퓨터 포렌식의 절차와 유사하나 휴대폰의 통신 기능을 고려하여 진행

① 현장 보존
- 범죄 현장에서 스마트폰이 발견되면 사진을 찍어 현장을 보존해야 함
- 스마트 폰이 켜져 있을 경우에는 화면 사진을 캡처해 두어야 함

② 증거의 확보
- 스마트 폰을 확보했다면 네트워크 차단이 우선적으로 이뤄져야 함 (비행모드)
- 스마트 폰이 켜져있을 경우 전원을 공급하여 활성데이터를 보존해야함

③ 데이터 수집 및 분석
- 법적 효력을 갖기 위해선 다음과 같은 고려사항을 지켜야 함
  - 수사의 범위와 권한의 적정성
  - 스마트폰의 데이터 무결성
  - 스마트 폰의 증거 인멸 검증을 위한 연계 보관성
- 기종에 따라 데이터 추출 및 분석 방법이 상이하므로 올바른 방법을 선택해야 함

④ 보고서 작성
- 사건정보, 증거의 획득과정, 분석 결과 등을 작성함

스마트폰 포렌식

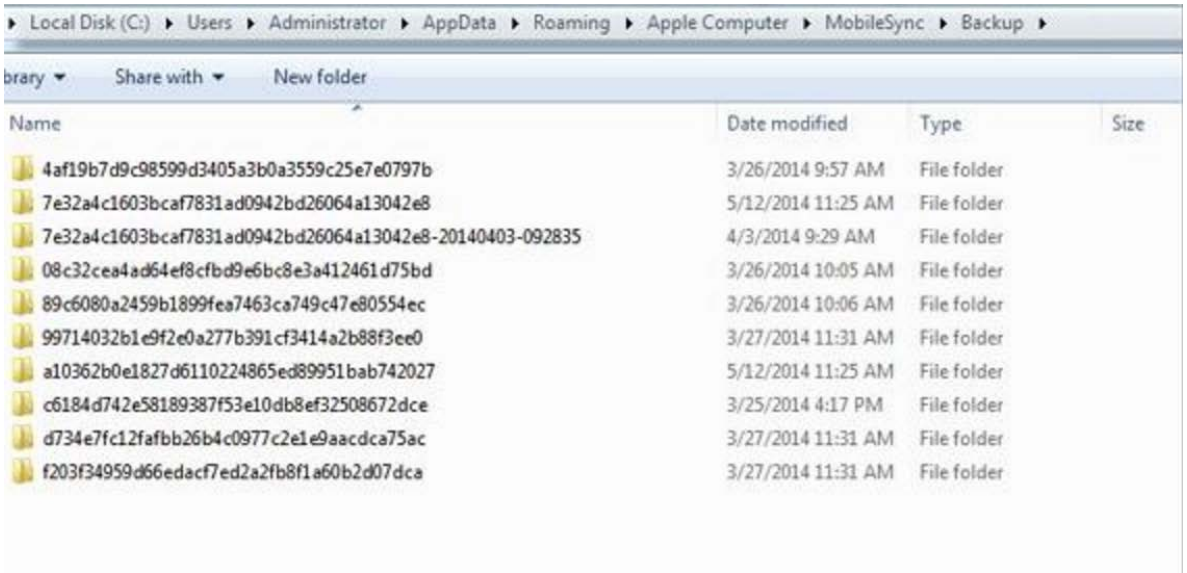
- 논리적 메모리 추출 방법
  - USB인터페이스를 이용하여 스마트폰에 저장된 파일과 디렉토리를 추출하는 방법
  - 안드로이드
  - 루팅을 통한 슈퍼유저권한을 얻어야 모든 정보를 추출 가능함
  - 안드로이드 메모리 구성
    - Cache
      - 설치파일 등의 임시파일을 저장하는 파티션
    - System
      - 기본 어플리케이션의 설치 위치
    - Data, sdcard
      - 사용자가 스마트폰을 사용하면서 생기는 모든 데이터
      - 연락처, 통화목록, 문자메시지, 사진, 등

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
외장메모리	Sdcard	FAT32	외장 SD 카드

안드로이드 메모리 구성

스마트폰 포렌식

- 논리적 메모리 추출 방법
  - **iOS**
  - iOS 디바이스에서는 슈퍼유저 권한을 얻지 않아도 대부분의 데이터를 추출 가능
  - IOS 데이터 추출은 iTunes 백업 메커니즘을 이용함
  - 현재 iOS 9 버전에서는 데이터 파일들의 SHA1 해시값을 폴더 이름하며 데이터를 추출함



스마트폰 포렌식

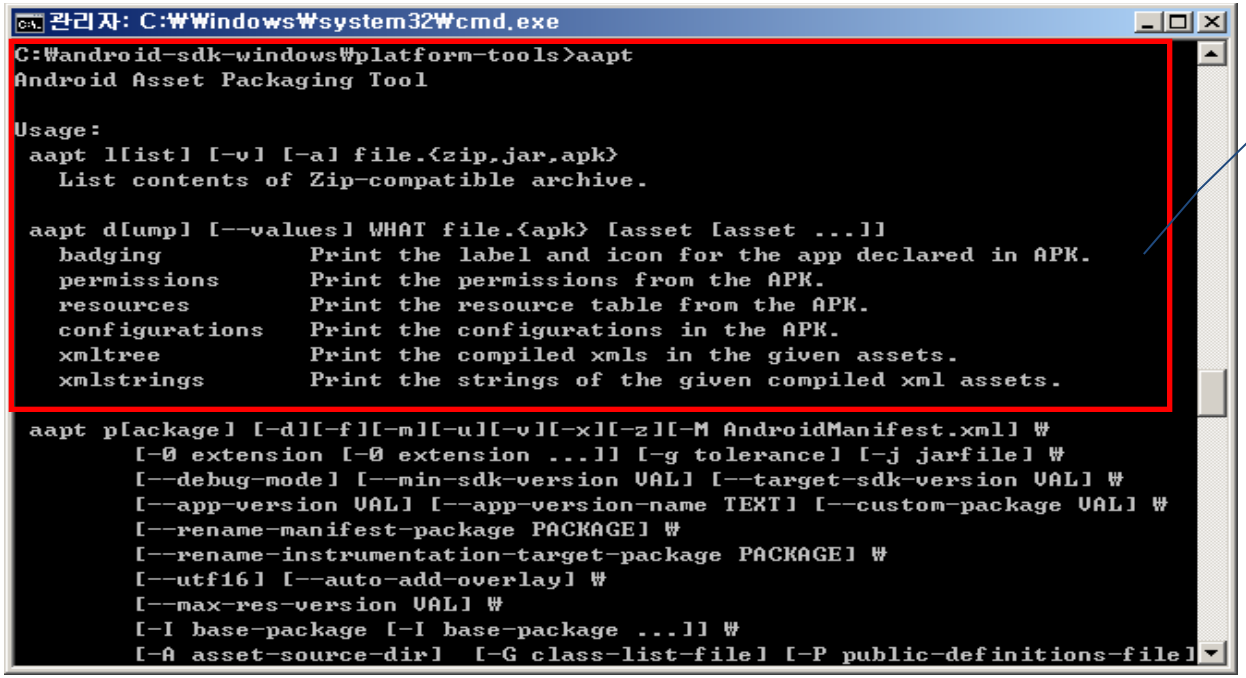
- 물리적 메모리 추출 방법
  - 플래시 메모리 **전체를 비트 단위**로 복사하는 메모리 추출 방법임
  - 물리적 추출 방법의 종류는 다음과 같음
    - 운영체제에 기반한 방법
      - 스마트폰을 부팅한 후 운영체제의 명령어를 사용하여 비트 단위의 추출을 수행하는 방법이다.
    - JTAG 포트를 이용한 방법
      - PCB(Printed Circuit Board)의 JTAG 포트에 직접 연결하거나 표준 24핀 인터페이스로 연결할 수도있다
    - 메모리 칩을 분리하는 방법
      - 메모리 칩을 스마트폰으로부터 분리하여 직접 데이터를 추출하는 방법
    - Boot loader를 이용한 방법
      - 운영체제를 커널에 올려주는 부트 로더를 통해서 모든 데이터를 추출함

스마트폰 데이터 수집

스마트폰 데이터 수집

- 안드로이드 설치 권한 체크
  - aapt 명령어로 APK의 manifest에 대한 정보를 알아보는 방법

    . package name, versionCode, versionName, permission 정보,sdkVersion 정보, 사용된 리소스에 대한 정보, supports-screens 등 정보를 알수 있음



aapt 실행화면

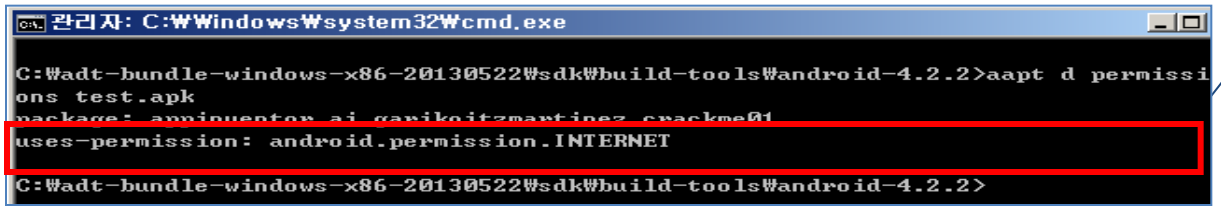
❖[adt-bundle-windows-x86-설치위치]\sdk\build-tools\android-버전\ 안에 aapt.exe 파일 존재

스마트폰 데이터 수집

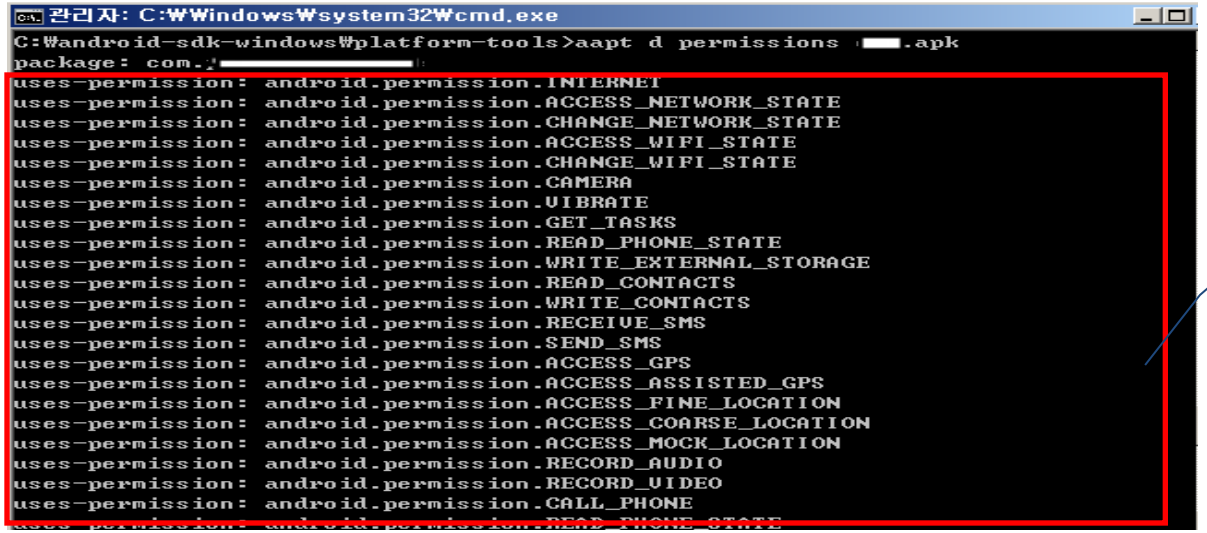
- 안드로이드 설치 권한 체크
  - aapt 명령어로 APK의 manifest에 대한 정보를 알아보기 방법

. C:\adb pull /data/app/xxx.apk

. C:\aapt d permissions dsn.apk



정상적인 앱의 권한 요구 화면



악성 앱의 권한 요구 화면

스마트폰 데이터 수집

- 안드로이드 설치 권한 체크
  - 주로 사용하는 접근 권한 (현재 110개의 퍼미션이 정의되어있음)

접근권한	내용
ACCESS_FINE_LOCATION	현재 위치정보에 접근 허용 (GPS-위치정보)
ACCESS_NETWORK_STAT	네트워크에 대한 정보 접근 허용 (네트워크 연결 정보)
ACCESS_WIFI_STATE	Wi-Fi 네트워크에 대한 정보 접근 허용 (Wi-Fi 네트워크 연결 정보)
CALL_PHONE	Dialer 사용자 인터페이스를 통하지 않고 전화통화 허용 (무단 전화걸기)
CALL_PRIVILEGED	Dialer 사용자 인터페이스를 통하지 않고 긴급전화번호를 비롯한 모든 전화번호 사용 허용 (무단 전화걸기
GET_ACCOUNTS	Accounts Service 내의 계정목록에 접근 허용(단말기에 설정되어 있는 계정)
PROCESS_OUTGOING_CALL	발신전화를 종료하거나 모니터, 수정 허용 (발신전화 모니터)
READ_CONTACTS	사용자 전화번호부 읽기 허용 (주소록)
READ_CALENDAR	사용자 캘린더 데이터 읽기 허용 (일정)
READ_HISTORY_BOOKMAR	사용자의 브라우저 히스토리와 즐겨찾기 읽기 허용(브라우저 히스토리와 즐겨찾기)
READ_OWNER_DATA	owner 데이터 읽기 허용 (파일 열람)
READ_PHONE_STATE	폰 상태 읽기 허용 (IMEI, IMSI, 폰번호, 통화중 상태)

- 안드로이드 설치 권한 체크

접근권한	내용
READ_SMS	SMS 읽기 허용 (SMS)
RECEIVE_MMS	받는 MMS 모니터링 하거나 기록 또는 가공 허용 (MMS 모니터)
RECEIVE_SMS	받는 SMS 모니터링 하거나 기록 또는 가공 허용 (SMS 모니터)
RECORD_AUDIO	오디오 기록 가능
SEND_SMS	SMS 메시지 발송 가능 (문자 발송)
USE_CREDENTIALS	AccountManager로부터 인증토큰 요청 허용 (인증토큰)
WRITE_OWNER_DATA	owner 데이터 쓰기 허용 (파일 쓰기)

스마트폰 데이터 수집

- **ADB**를 이용한 데이터 수집
  - ADB를 통한 데이터 수집을 위해서는 기기가 루팅 되어 있어야 가능함
  - 퍼미션 변경해야만 PC로 다운로드 가능함 : chmod 755 xxxx.db

```
# ls -al
ls -al
total 80
drwxrwx--x    1 10024    10024            0 Jan  7 06:39 ←[1;34m.←[0m
drwxr-x--x    1 10024    10024            0 Jan 13 03:58 ←[1;34m..←[0m
-rw-rw----    1 10024    10024        46080 Jan  7 06:39 ←[0;0mKakaoTalk
-rw-rw----    1 10024    10024        14336 Jan  7 06:39 ←[0;0mwebview.d
-rw-rw----    1 10024    10024         6144 Jan  7 06:39 ←[0;0mwebviewCa
0m
# pwd
pwd
/data/data/com.kakao.talk/databases
```

  - db 파일을 PC에 다운로드
    - adb pull /data/data/[app]/databases/xxxx.db

```
C:₩adt-bundle-windows-x86-20130522₩sdk₩platform-tools>adb pull /data/data/com.ka
kao.talk/databases/KakaoTalk.db
1551 KB/s (46080 bytes in 0.029s)
```

스마트폰 데이터 수집

- 데이터 경로
  - 안드로이드 공식 표준 경로는 다음과 같으며 기기에 따라 경로 정보가 조금씩 다를 수 있음

데이터	경로
연락처	/data/data/com.android.providers.contacts/databases/contacts2.유
통화기록	/data/data/com.android.providers.contacts/databases/contacts2.db
SMS/MMS	/data/data/com.android.providers.telephony/databases/mmssms.db
일정	/data/data/com.android.providers.calendar/databases/calendar.db
메일목록	/data/data/com.android.providers.email/databases/EmailProvider.db
메일내용	/data/data/com.android.providers.email/databases/EmailProviderBody.db
웹히스토리	/data/data/com.android.providers.browser/databases/browser.db
알람	/data/data/com.android.google.android.deskclock/databases/alarm.db
다운로드	/data/data/com.android.providers.downloads/databases/downloads.db
• • • • •	

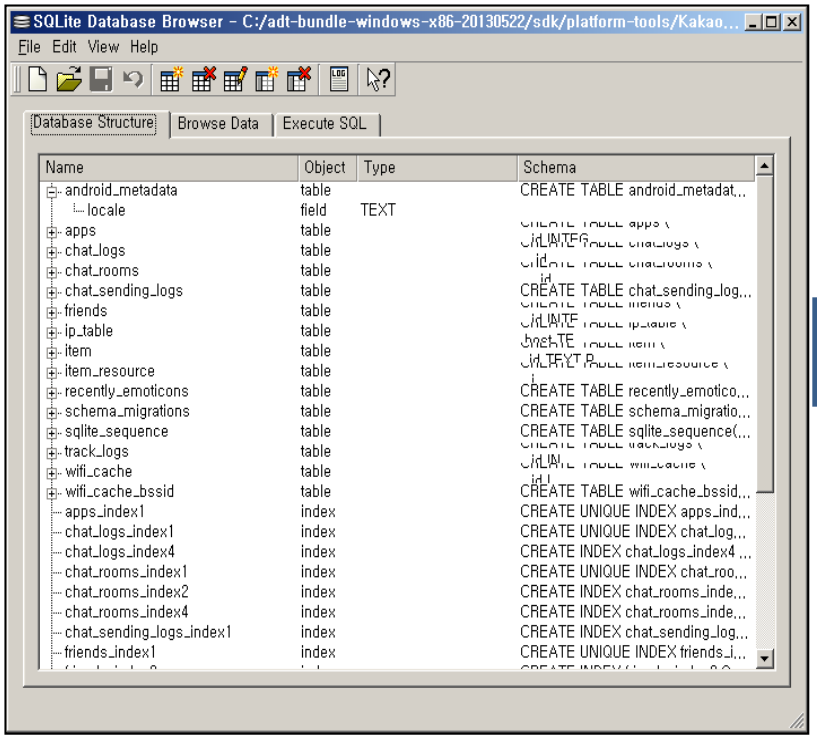
스마트폰 데이터 수집

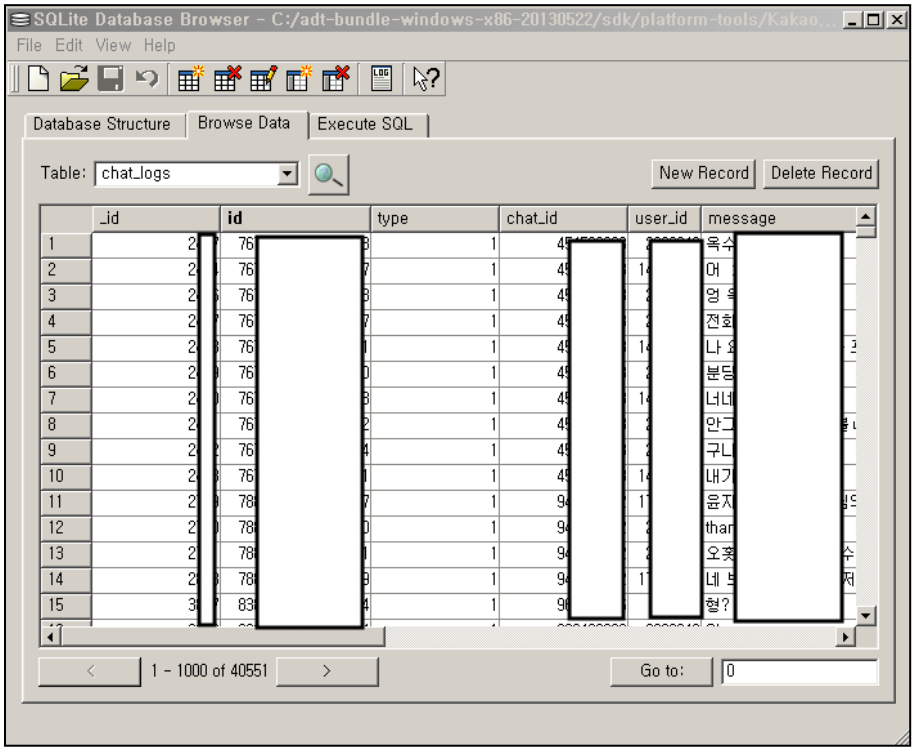
- **SD카드 데이터 수집**
  - 안드로이드의 OS의 경우 내장/외장 SD카드를 사용하여 추가적인 데이터를 저장함
  - USB를 이용한 접근이 가능 일반적이나 프로그램을 통한 자동화 된 수집이 불가함
  - ADB를 통한 “pull” 명령을 사용하면 SD 카드로부터 데이터를 저장할 수 있음.

스마트폰 데이터 수집

- **DB 중요 정보 수집**
  - SQL Lite Browser를 이용하여 다운 받은 .db파일 열람

    - http://sourceforge.net/projects/sqlitebrowser 에서 프로그램 다운 필요



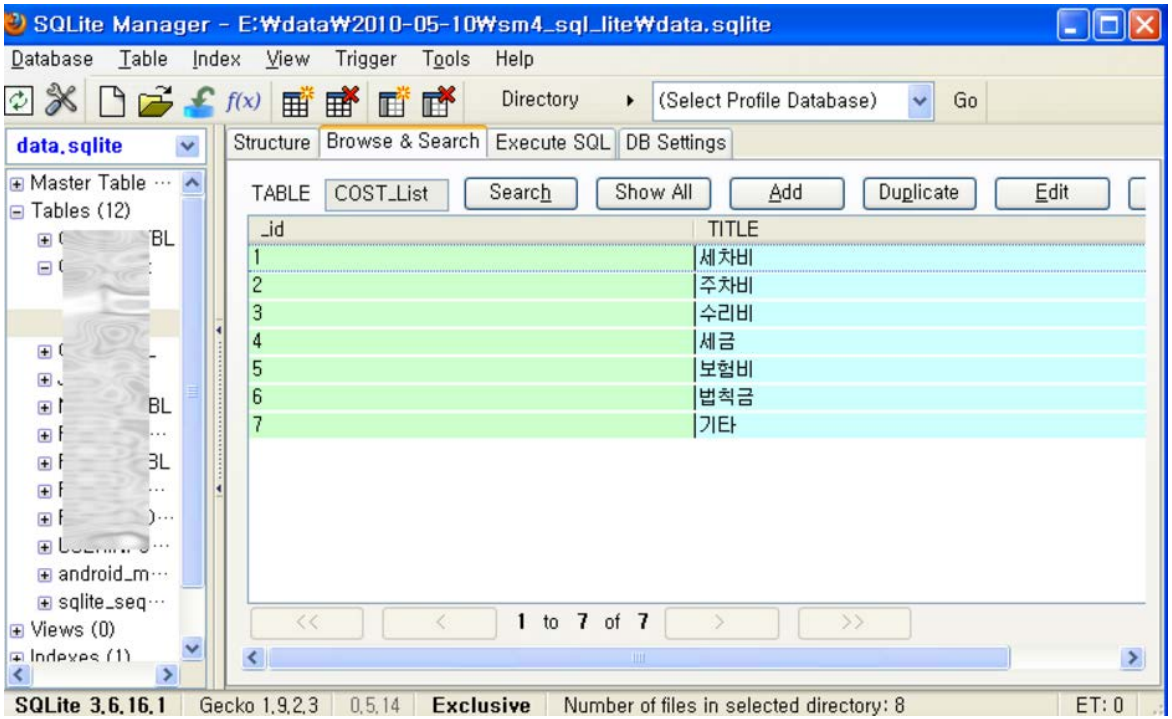


  - 다운받은 .db파일 점검

스마트폰 데이터 분석

스마트폰 데이터 분석

- 기본 응용 프로그램 분석
  - 안드로이드에 기본적으로 설치되어 있는 응용프로그램들은 모두 SQLite 데이터 파일 안에 저장됨
  - "SQLite Expert"와 같은 뷰어 프로그램을 통해 수집한 각 응용 프로그램의 SQLite 데이터베이스 파일을 분석할 수 있음



스마트폰 데이터 분석

- 멀티미디어 데이터 분석
  - 멀티미디어 데이터(사진, 동영상, 오디오)를 기본적으로 SD 카드에 저장함
  - 주기적으로 SD카드를 전체 스캔하여 각 멀티미디어 파일의 저장위치를 “external-숫자.db” 파일 안에 저장함.

DB경로	/data/data/com.android.providers.media/databases/external-숫자.db	
테이블명	Images, video, audio_meta	
필드 정보	_data	파일 경로
	_displayname	파일명
	_size	크기
	Mime_type	데이터 타입
	Data_taken	멀티미디어 생성시간
	Data_modified	멀티미디어 수정시간
	Latitude	위도
	Longtitude	경도
	title	제목

스마트폰 데이터 분석

- 위치 정보 분석
  - GPS 정보 분석
    - GPS 캐시 정보는 GPS에서 마지막으로 수신된 위치 정보를 CachedPosition 테이블에 저장함
    - 저장된 정보는 위도, 경도, 시간정보 이므로 사용자가 해당 시간에 특정 위치에 있었다는 증거로 활용될 수 있음
  - Wifi 정보
    - 사용자가 특정 Wifi에 접속하게 되면 접속한 Wifi AP의 SSID 정보와 MAC 주소가 기기 안에 저장됨
    - SSID는 "wpa_supplicant.conf"파일에 저장됨
    - 일반적으로 SSID를 설정할 때 Wifi AP의 위치한 장소 이름을 사용하는 경우가 많음
    - "Cache.wifi" 파일에는 접속했던 Wifi MAC 주소가 저장되어있음

cache.wifi

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	00	01	00	C8	00	11	37	38	3A	32	38	3A	30	39	3A	30	È 78:28:09:0
16	64	3A	34	33	3A	66	38	00	00	00	38	00	00	00	5C	40	d:43:f8 8 \@
32	42	CB	9F	79	AD	6B	08	40	5F	C1	B1	0A	64	07	11	00	BË▮y-k @_Á± d

"cache.wifi" 파일안에 저장된 MAC 주소 정보

- 삭제 데이터 복구
  - SQLite 데이터베이스의 삭제된 레코드 복구
    - 안드로이드의 대부분 데이터는 SQLite 데이터베이스 형태로 저장됨
    - 사용자가 데이터를 삭제했을 경우 SQLite 데이터베이스는 해당 레코드가 위치한 부분을 비할당 영역으로 변경함
    - 다른 레코드가 덮어 쓰거나 SQLite 데이터베이스가 비할당 영역을 정리하기 전에는 파일 내에 그대로 남아있음
    - 따라서 비할당 영역에 남아 있는 레코드들을 복구하면 삭제된 데이터를 복구할 수 있음.
    - 다음은 주요 정보별 삭제 데이터 복구 여부를 보여준다.

데이터	삭제 데이터 복구 여부	상세 정보
연락처	O	데이터 테이블 레코드 복구
통화기록	X	삭제와 동시에 비할당 영역 정리
SMS	O	SMS 테이블 레코드 복구
MMS	O	각 테이블의 레코드 복구
일정	O	Events 테이블 레코드 복구
메일	X	삭제와 동시에 비할당 영역 정리

스마트폰 데이터 분석

- 삭제 데이터 복구
  - SD카드의 삭제된 파일 복구
    - 안드로이드 OS는 USB 설정을 통해 SD카드와 PC의 연결을 지원함
    - 안드로이드 SD 카드는 FAT 32 파일 시스템을 사용함
    - 기존의 하드디스크와 같이 파일시스템 메타 데이터 복구와 카빙을 통한 복구 방식을 모두 그대로 적용할 수 있음

안드로이드 개요

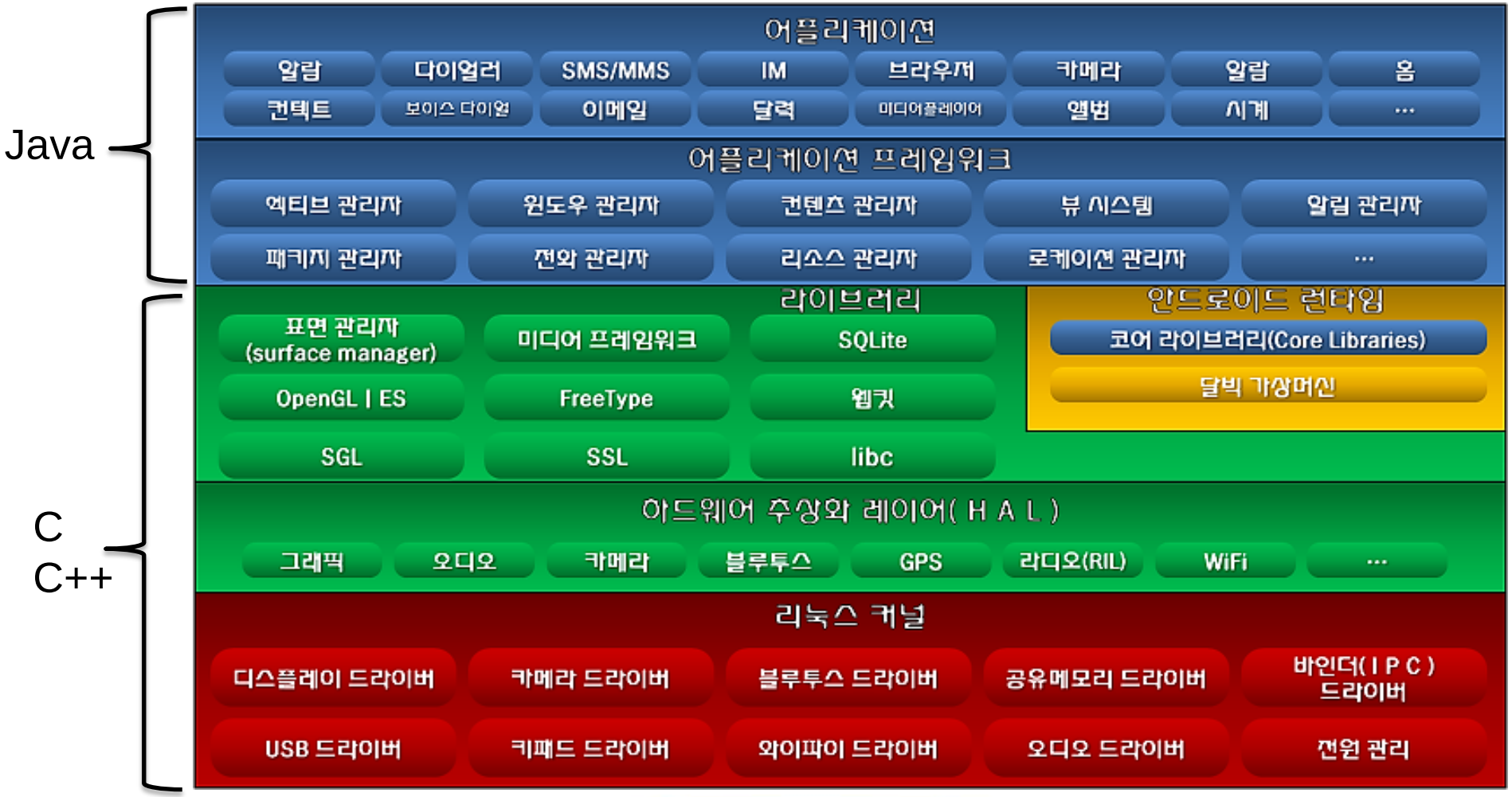
안드로이드 개요

- 안드로이드란 ?
  - 핸드폰을 포함한 모든 모바일 기기에 탑재될 수 있는 모바일 플랫폼
  - 구글이 중심이된 OHA(Open Handset Aliance)에서 개발한 완전히 개방된 모바일 플랫폼

- 주요특징
  - 다양한 기술을 수용하고 빠르게 혁신할 수 있는 개방적인 모바일 플랫폼을 구축
  - 리눅스 커널 기반 - 자바 프로그래밍 언어 - 많은 확장 라이브러리

안드로이드 개요

- 안드로이드 아키텍쳐



안드로이드 개요

● 안드로이드 아키텍쳐

- 안드로이드 어플리케이션(앱)이란?
  - **안드로이드 package(*.apk)형태**
  - 스마트폰 등 device로 다운로드하는 단위
  - **Java code + data/resource files 로 구성**
  - aapt tool(Android Asset Packaging Tool)을 사용하여 제작(eclips 내부)
  - **사용자와 안드로이드 사이에서 작동 되는 소프트웨어**
  - 안드로이드는 Core Application(기본)을 포함하고 있다.
    - SMS, Email, Calendar, Map, WebBrowser, contacts 등
  - 기본 Application 이 아닌 별도 Application도 이에 포함
    - 카카오톡, 틱톡, Facebook, 네이트온 등
  - • 모든 어플리케이션은 Java 언어로 작성되어 진다.

안드로이드 개요

● 안드로이드 아키텍쳐

❖ 어플리케이션 프레임워크

• Application Framework는 Core Application에서 **사용된 기능이나 개발자들이 주로 사용하는 기능**들을 제공하여 재사용성(reuse)을 높여 **개발의 편리함을 제공**한다.(JAVA)

- 뷰 관리자 : List, Grid, TextBox, Button 등 사용자와 상호작용과 풍부한 기능 및 확장성 제공
- 컨텐츠 관리자 : 앱들 간의 데이터 접근 및 자체 데이터 공유 주소록 등 다른 application이 가지고 있는 DATA에 접근
- 리소스 관리자 : 문자열, 그래픽, 레이아웃 등 자원들에 대한 접근을 제공
- 액티브 관리자 : 앱의 Life Cycle을 관리

안드로이드 개요

- 안드로이드 아키텍쳐

❖ **Libraries**

- 안드로이드 시스템에서 다양하게 사용되는 C/C++ 라이브러리
- 시스템 C 라이브러리 : 임베디드 리눅스 기반용으로 조정된 표준 C 시스템 라이브러리
- 미디어 라이브러리 : MPEG4, H.264, MP3, AAC, JPG, PNG 등 다양한 오디오/비디오 포맷과 정적 이미지
- 파일에 대한 재생과 레코딩을 지원
- OpenGL : 3D 기반 그래픽 엔진, 하드웨어 3D 가속(하드웨어적으로 지원할 경우)
- SQLite : 강력 하고 가벼운 관계형 데이터베이스 엔진
- FreeType : 비트맵, 백터 폰트 렌더링을 지원하는 라이브러리
- LIbWebCore(WebKit): 웹브라우져 엔진

- 안드로이드 아키텍쳐

❖ **Android Runtime**

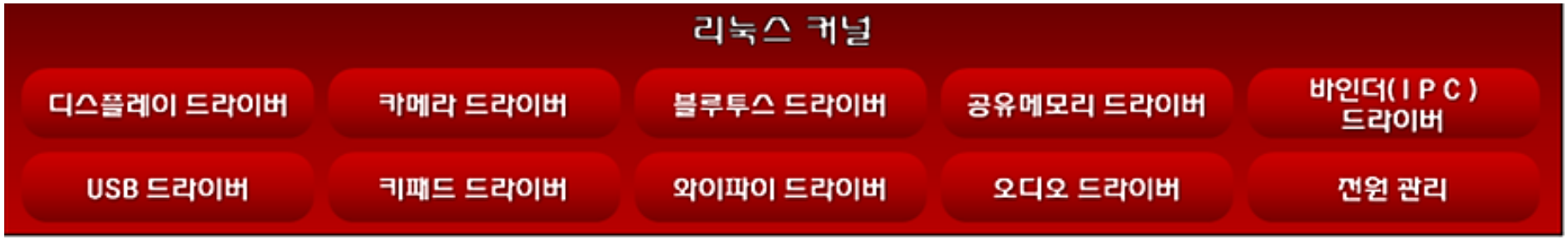
- **안드로이드에서 사용되는 달빅 가상머신과 코어 라이브러리로 구성**
- 달빅 가상머신은 안드로이드에서 자체적으로 만들었으며 무료로 배포
- 에플리케이션의 호환성과 실행 일관성을 제공하며, 최적화된 파일 포맷(.dex)과 달빅 바이트 코드를 실행
- 달빅가상 머신은 임베디드 환경을 위해 디자인 되어 디바이스별로 다양한 가상 머신 프로세스들을 지원하며, 실행시 메모리를 매우 **효율적으로 사용함**
- 코어 라이브러리들은 강력하지만 단순하고 익숙한 개발 플랫폼을 제공하는 Java언어를 위한 코어API들을 포함(데이터 구조, 유틸리티, 파일접근, 네트워크 접근, 그래픽 등)
- 안드로이드 **5.0 롤리팝(Lolipop)**부터는 ART를 새로운 런타임으로 완전히 대체

안드로이드 개요

- 안드로이드 아키텍쳐

❖ Linux Kernel

• Linux Kernel 2.6 기반
• 보안, 메모리 관리, 네트워크, 드라이버 등을 구현 및 관리
- 안드로이드에 맞게 수정된 리눅스 커널
- X-windows, glibc, 표준 리눅스 유틸리티 전체를 포함하고 있지 않음
- 하드웨어를 구동하기 위한 디바이스 드라이버, 메모리, 프로세스, 네트워크 관리 등 기본 역할 수행
- 안드로이드 시스템이 동작할 수 있도록 필요한 기능들이 추가된 형태로 구성



안드로이드 개요

- 안드로이드 아키텍쳐
  - ❖ 최근 들어 스마트폰의 사용이 급격하게 증가하고 있으며, 또한 스마트폰에는 통 화기록과 문자 메시지뿐만 아니라 이메일, 아이디, 패스워드, **GPS(Global Positioning System)** 데이터, 신용카드 등 수많은 개인정보가 저장
  - ❖ 이에 따라 디지털 포렌식 수사에서도 스마트폰 포렌식의 비중이 크게 증가
  - ❖ 스마트폰에는 많은 양의 개인정보가 저장되어 있기 때문에 범죄현장에서 스마트폰을 획득한 경우 지문을 채취한 경우보다 더 많은 정보를 얻을 수 있음

안드로이드 정적 분석

안드로이드 정적분석

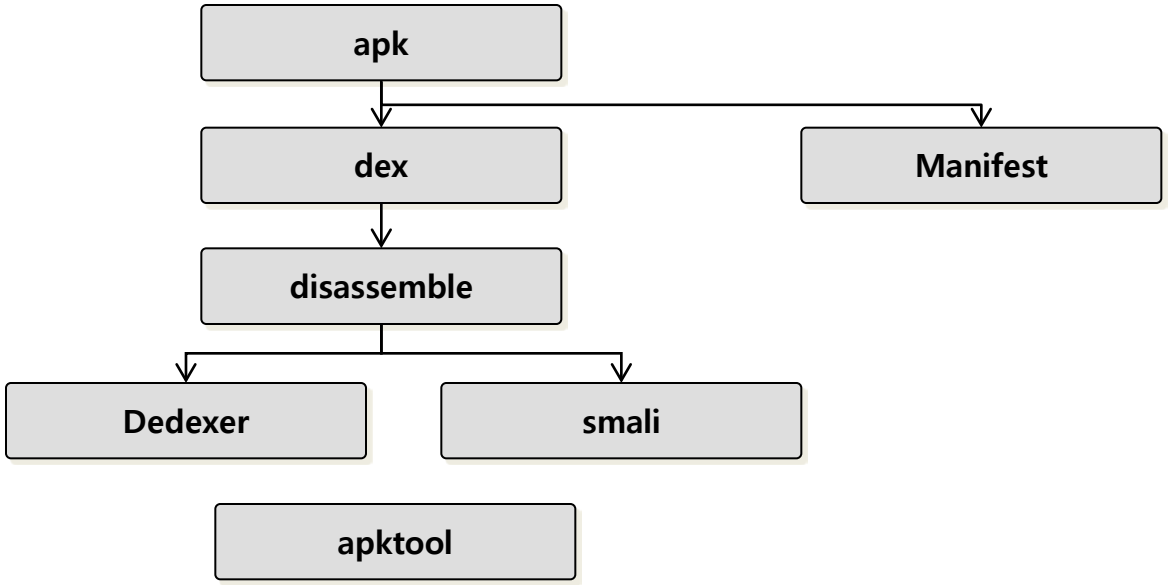
- **정적 분석이란?**

프로그램을 실행하지 않은 채 소스 코드 분석만으로 해당 모바일 앱에 대한 악성행위를 검증하는 것, 단말기로부터 사용자에 의해 설치된 모바일 앱의 APK 파일을 추출하고 이를 검증하는 방법

- **정적 분석 방법**

안드로이드 정적분석

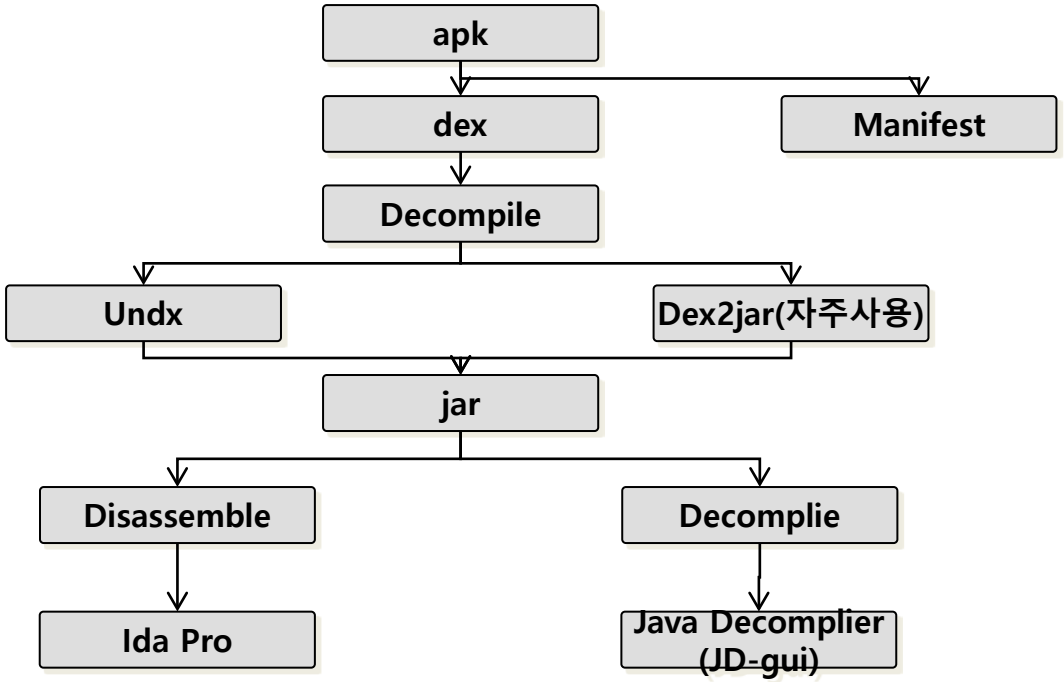
- 정적 분석 방법 (바이트 코드 추출)
  - 바이트 코드란 C언어의 기계어인 어셈블리어라 부르는 것과 같이 **안드로이드 자바의 기계어**를 의미함



  - dex : 안드로이드 런타임에서 동작하는 바이너리 실행 파일
  - Manifest : 앱에 대한 정보 및 실행권한 등의 정보를 가지는 xml
  - Disassemble : Apktool을 이용하여 안드로이드 어플을 해제하고 Smali코드를 분석

안드로이드 정적분석

- 정적 분석 방법 (자바 소스 추출)



- Decompile – dex2jar 와 decompiler(jad, jd-gui)를 사용하여 자바코드 분석
- Undx는 apk파일안의 dex파일을 .class로 만드는 것
- Decompiler는 .class를 .java형태로 변환

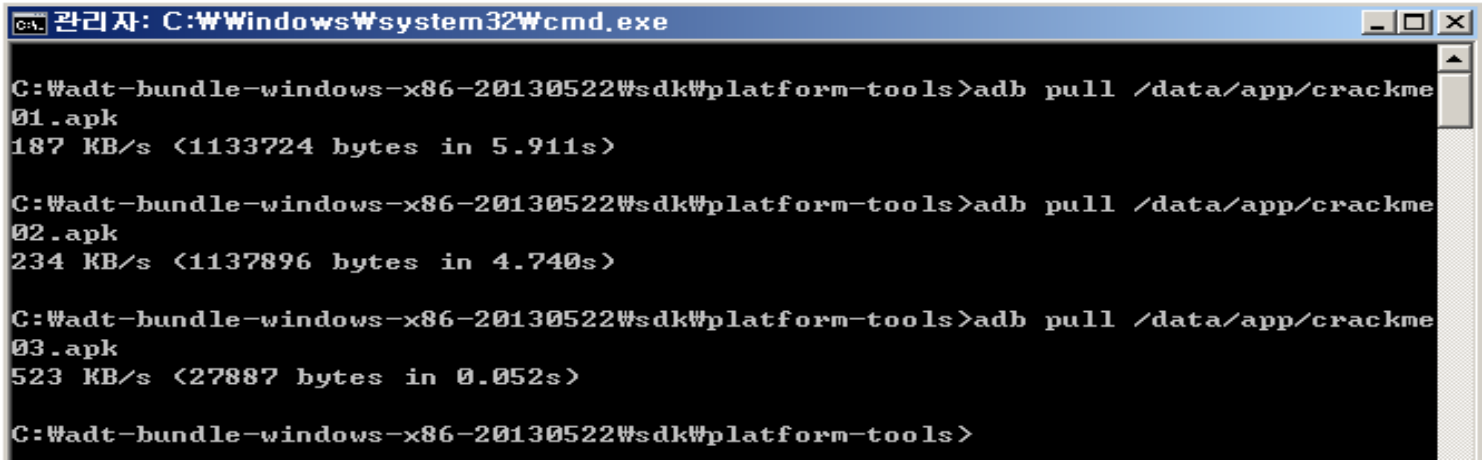
- 정적 분석 방법

  - **apk 파일 추출 (일반 APP)**

    - ADB을 이용하여 apk파일을 로컬 PC로 복사
    - adb(Android Debug Bridge)란?
      개발자 툴이며, 안드로이드 기기에 명령을 내릴 수 있는 프로그램

cd C:\Android SDK 설치 장소\sdk\platform-tools

C:\Android SDK 설치 장소\sdk\platform-tools\adb pull /data/app/test.apk



※ 일반 APP은 안드로이드 폰의 /data/app/ 디렉터리 안에 존재
※ apk 보호를 위해 관리자권한이 없는 핸드폰에서는 볼 수 없음 (루팅)

안드로이드 정적분석

- 정적 분석 방법
  - 정적 분석툴(baksmali)

❖ **baksmali, smali**

- http://code.google.com/p/smali/
- dex포맷을 위한 어셈블러/디어셈블러
- 아이슬란드 말로 baksmali(디어셈블러), smali(어셈블러)에 상응하는 의미

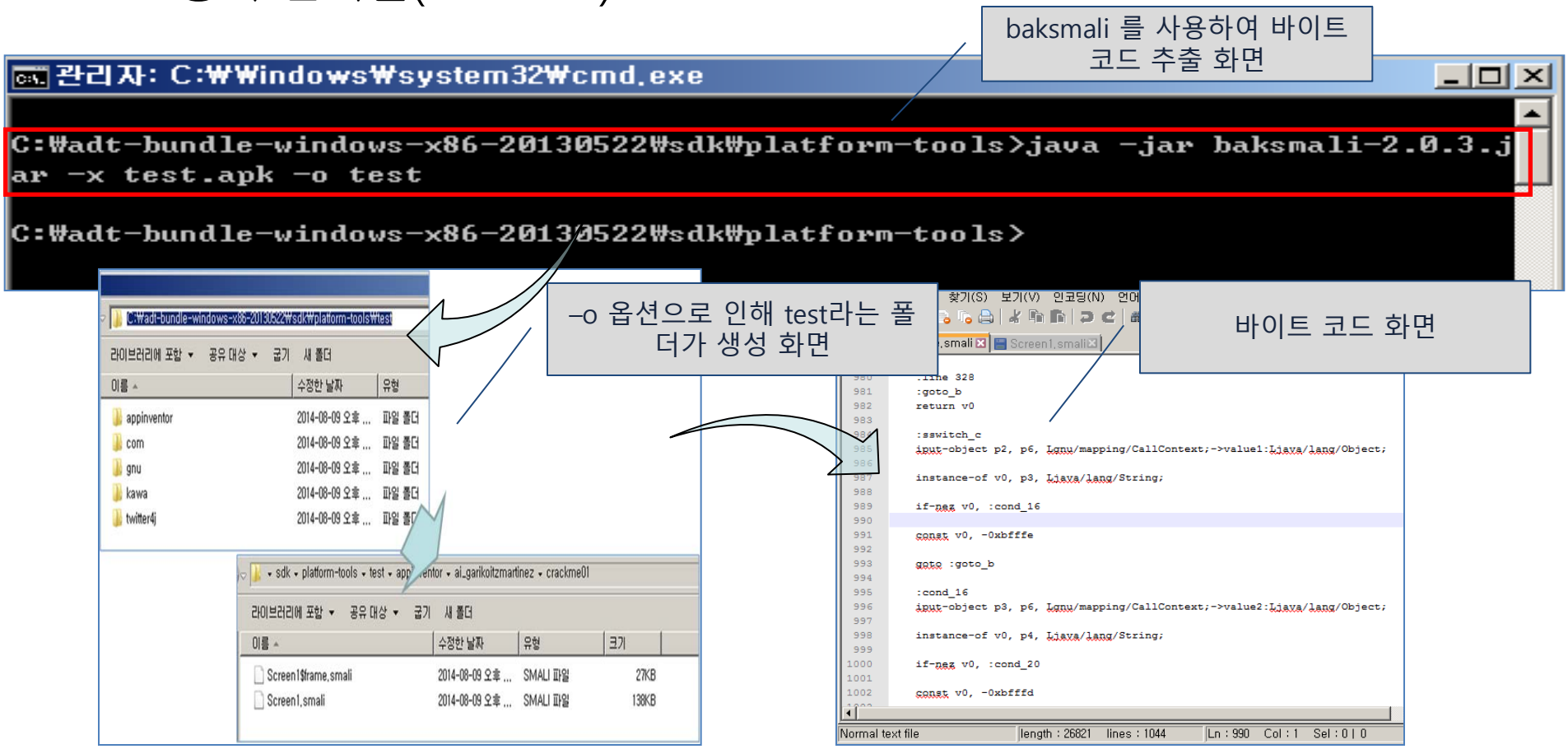
사용법

java -jar [baksmali 파일] -x [압축을 풀 dex 파일 or apk 파일] -o [압축 풀릴 폴더 이름]

C:\Android SDK 설치 장소\sdk\platform-tools\java - jar baksmali.jar – x classess.dex(dex 파일경로) 또는
C:\Android SDK 설치 장소\sdk\platform-tools\java - jar baksmali.jar – x crackme01.apk(apk 파일경로)

안드로이드 정적분석

- 정적 분석 방법
  - 정적 분석툴(baksmali)



안드로이드 정적분석

● 정적 분석 방법

▪ 정적 분석툴(dex2jar)

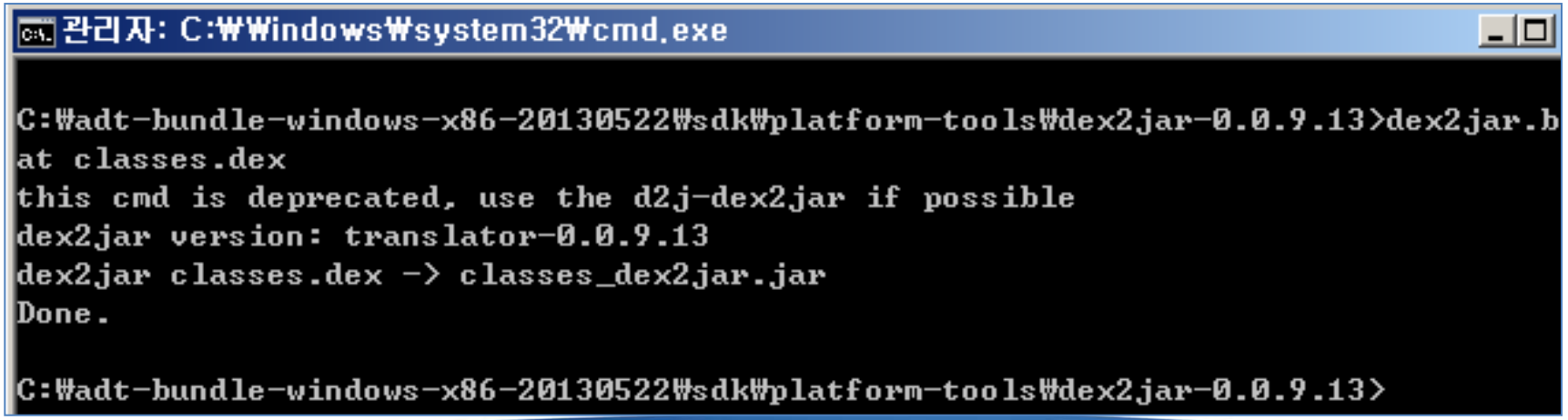
❖ dex2jar

• http://code.google.com/p/dex2jar/

•.dex 형식을 .class 형식으로 변환시키는 도구

사용법

```
dex2jar classes.dex 또는
dex2jar test.apk
```

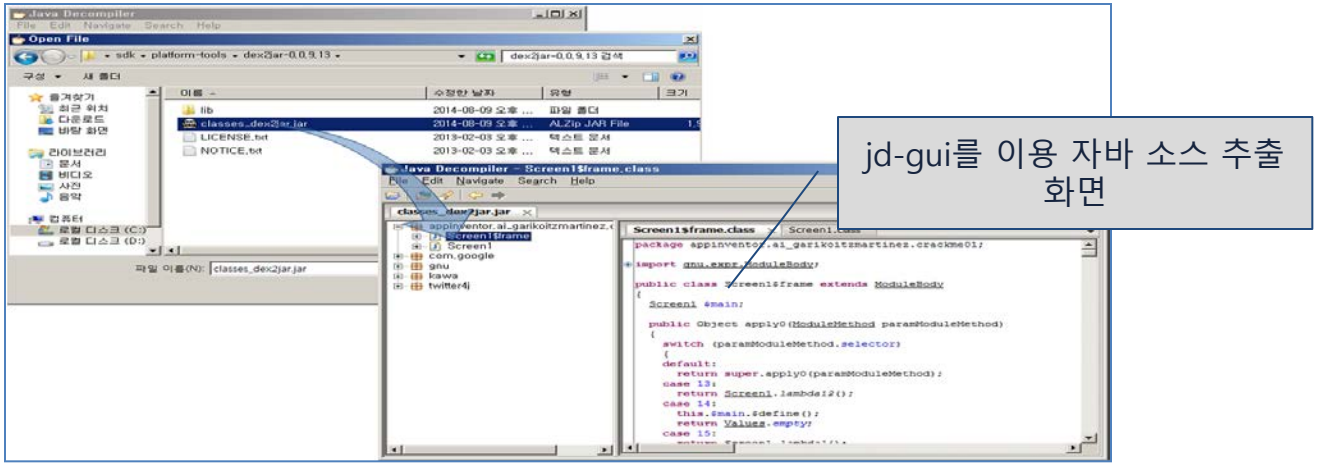


정적 분석툴(jd-gui)

❖ jd-gui

- http://java.decompiler.free.fr/?q=jdgui
- class 파일을 .java 파일로 디컴파일 하는 툴
- jd-gui는 GUI 기반의 툴임(dex2jar 프로그램 실행이 선행되어야 함)

Jad -o –sjava class파일명.class : class파일 하나만 컴파일 할 경우
Jad –o –r –sjava –dsrc 패키지명/xxx/xxx/*.class : package를 디컴파일 할 경우

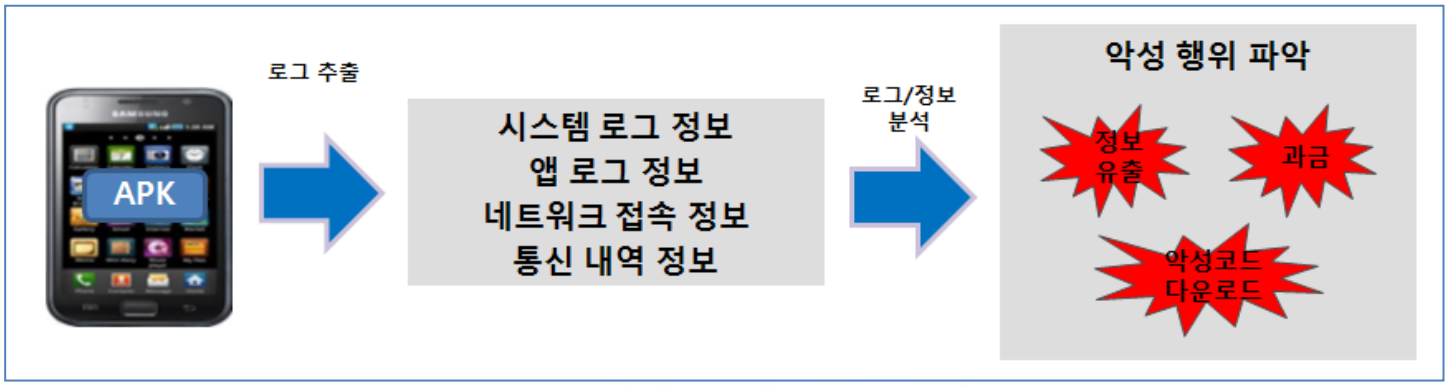


안드로이드 동적분석

안드로이드 동적분석

- 동적 분석이란?
  - 정적 분석 방법과는 달리, 실제로 프로그램을 실행시켜 테스트한 결과를 토대로 권한 우회, 정보유출, 악성행위 수행 여부 등을 검증하는 것
- 동적 분석 방법

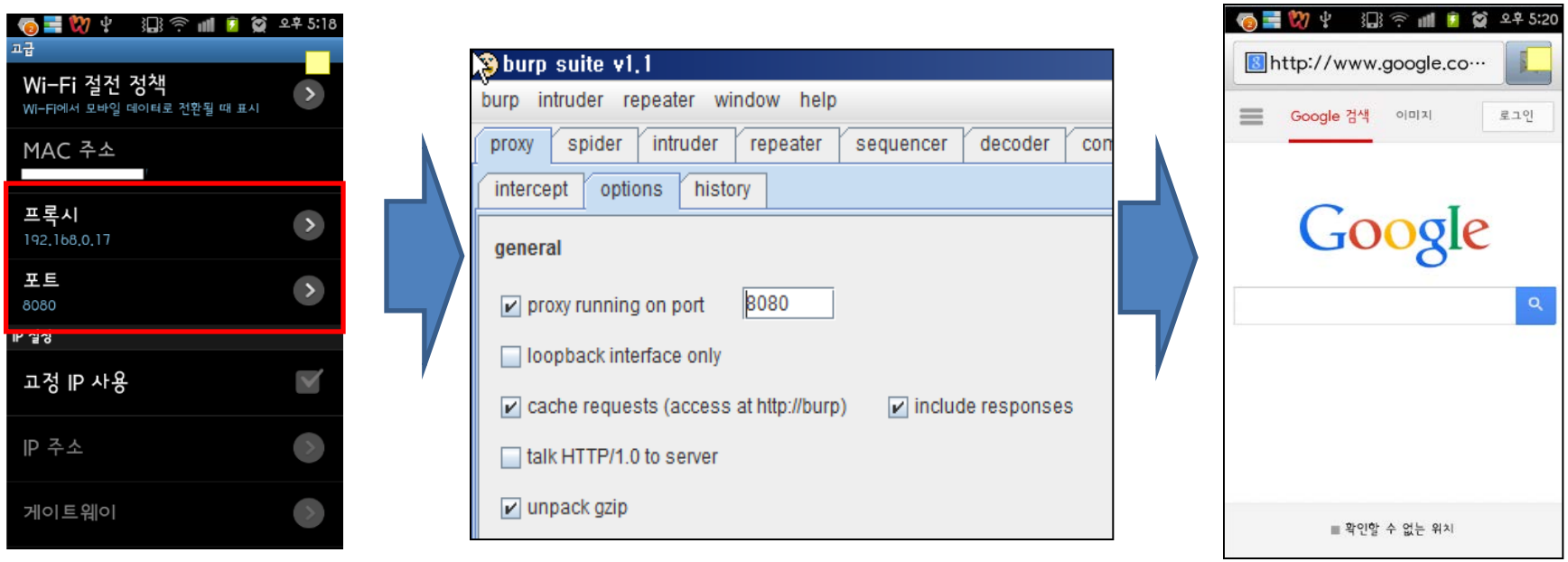
  특정 모바일 앱을 단말기에 설치하고 실제로 구동하여 단말기 동작에 대한 로그를 추출하고 이를 통해 권한 우회, 정보유출, 악성행위 여부를 분석하는 방법
  - 동적 분석을 통해 모바일 앱이 사용자 정보에 접근하고 조작하는지를 실시간으로 감시
  - 감시하고 있는 데이터가 네트워크 혹은 다른 방법으로 전송될 경우, 관련된 모바일 앱이나 도착지 정보를 로그화
  - 사용자 의사와 무관하게 다른 악성코드를 다운로드받거나 과금서비스를 사용하는지 감시



안드로이드 동적분석

● 스마트폰 환경에서의 프록시 설정 – 기본 브라우저 설정 이용

안드로이드 앱이 실행하였을 때 외부로 통신하기 위해 나가는 패킷을 분석하는 방법



웹 해킹 시 사용하는 웹 프록시 툴을 이용

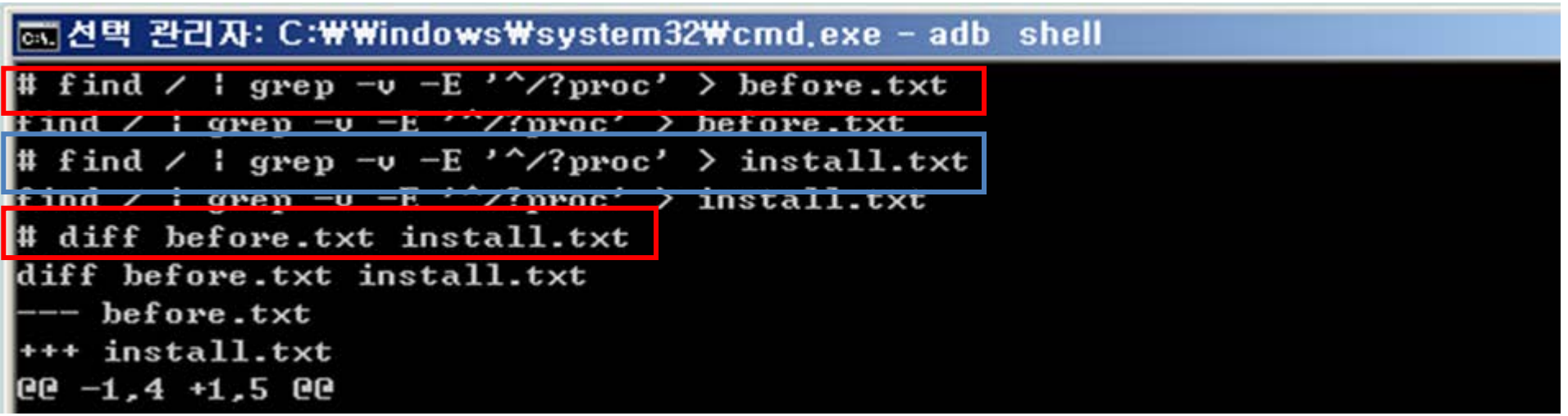
스마트폰에서 전송하는 패킷을 특정 아이피와 포트로 전송하는 것을 중간에 웹 프록시 툴이 가로채어 분석

❖ 환경 설정 -> 무선 및 네트워크 -> Wi-Fi설정 -> 고급설정 -> 프록시, 포트 설정

안드로이드 동적분석

- 앱 설치 전과 후 비교(새로 생성된 파일에 중요한 내용 포함 여부 확인)

1) Find 명령을 통하여 파일 리스트를 파일로 생성한다
분석할 앱을 설치하기 전 아래 명령을 수행하여 파일 리스트를 생성한다.
- #find / | grep –v –E '^/?proc' > before.txt (설치 전**)**
분석할 앱을 설치 한 후 아래 명령을 수행하여 파일 리스트를 생성한다.
- #find / | grep –v –E '^/?proc' > install.txt (설치 후**)**
2) Diff 명령으로 파일 비교 **(+** 는 추가된 파일**, -** 는 삭제된 파일을 나타낸다**)**
- #diff before.txt install.txt



안드로이드 동적분석

- 앱 설치 전, 삭제 후 비교(삭제된 파일에 대해 중요 내용 포함 여부 확인)

1) Find 명령을 통하여 파일 리스트를 파일로 생성한다

분석할 앱을 설치하기 전 아래 명령을 수행하여 파일 리스트를 생성한다.

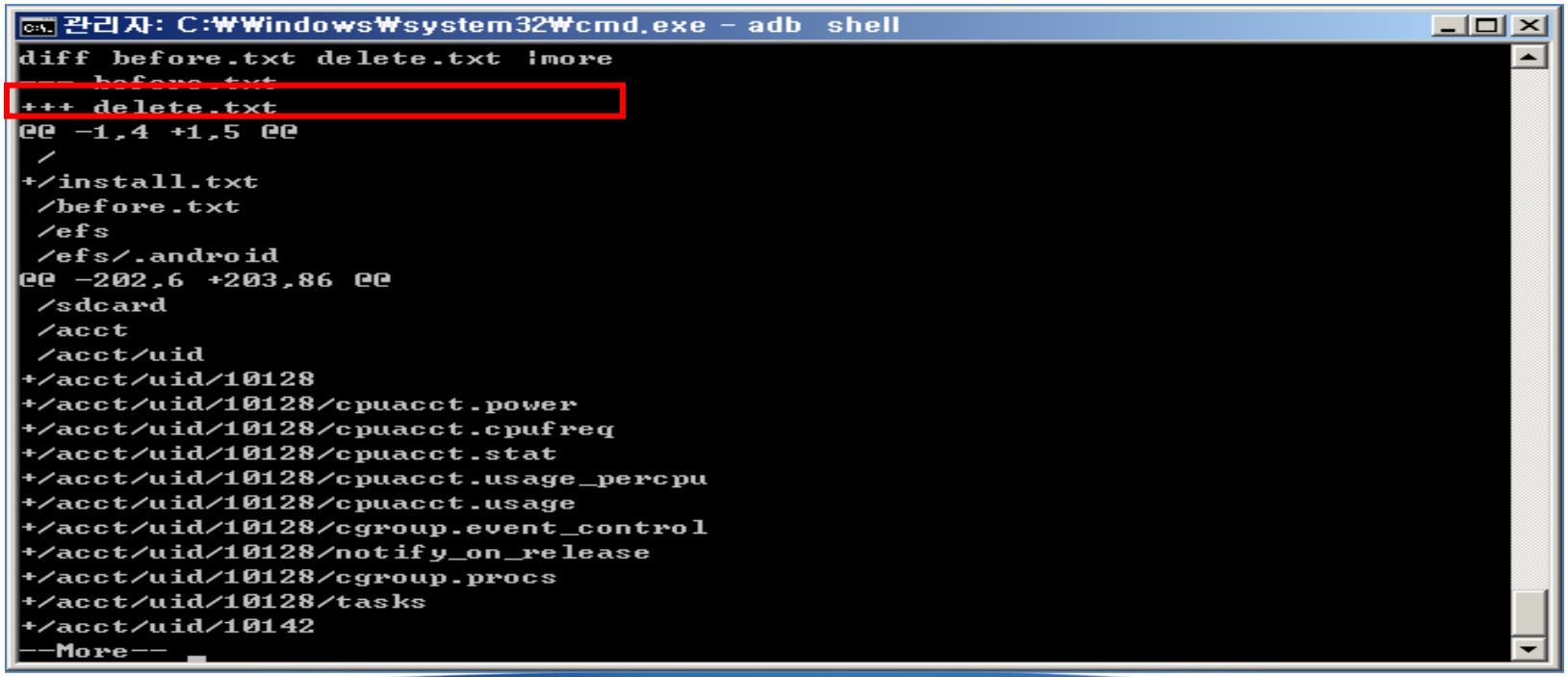
- #find / | grep –v –E '^/?proc' > before.txt (설치 전)

분석할 앱을 삭제 한 후 아래 명령을 수행하여 파일 리스트를 생성한다.

- #find / | grep –v –E '^/?proc' > delete.txt (삭제 후)

2) Diff 명령으로 파일 비교 (+ 는 추가된 파일, - 는 삭제된 파일을 나타낸다)

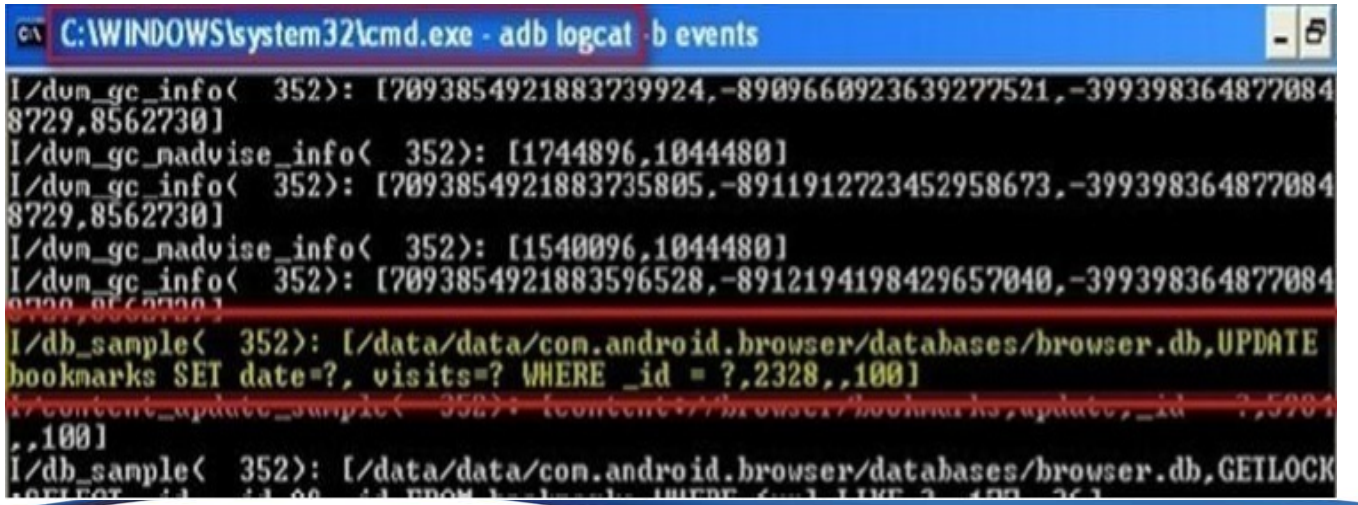
- #diff before.txt delete.txt



안드로이드 동적분석

- **logcat 사용(스마트 폰에서 발생시키는 로그를 분석)**

1) c:\>adb logcat –c : 로그삭제
2) c:\>adb logcat *:W : warning이상만 출력
   ① 우선순위 : Verbose < Debug < Info < Warning < Error < Fatal < Silent
   ② Filter는 각 우선순위의 첫 대문자로 설정
   ③ Filter 이상의 우선순위를 갖는 로그를 출력
3) c:\>adb logcat –f /dev/log/test.txt : -f 옵션은 파일로 저장
   adb logcat –h : help
   adb logcat –b events /dev/log/events 내용 출력
4) Grep 을 이용하여 특정문자열 검색 하여 출력
   c:\>adb shell
   #logcat | grep update

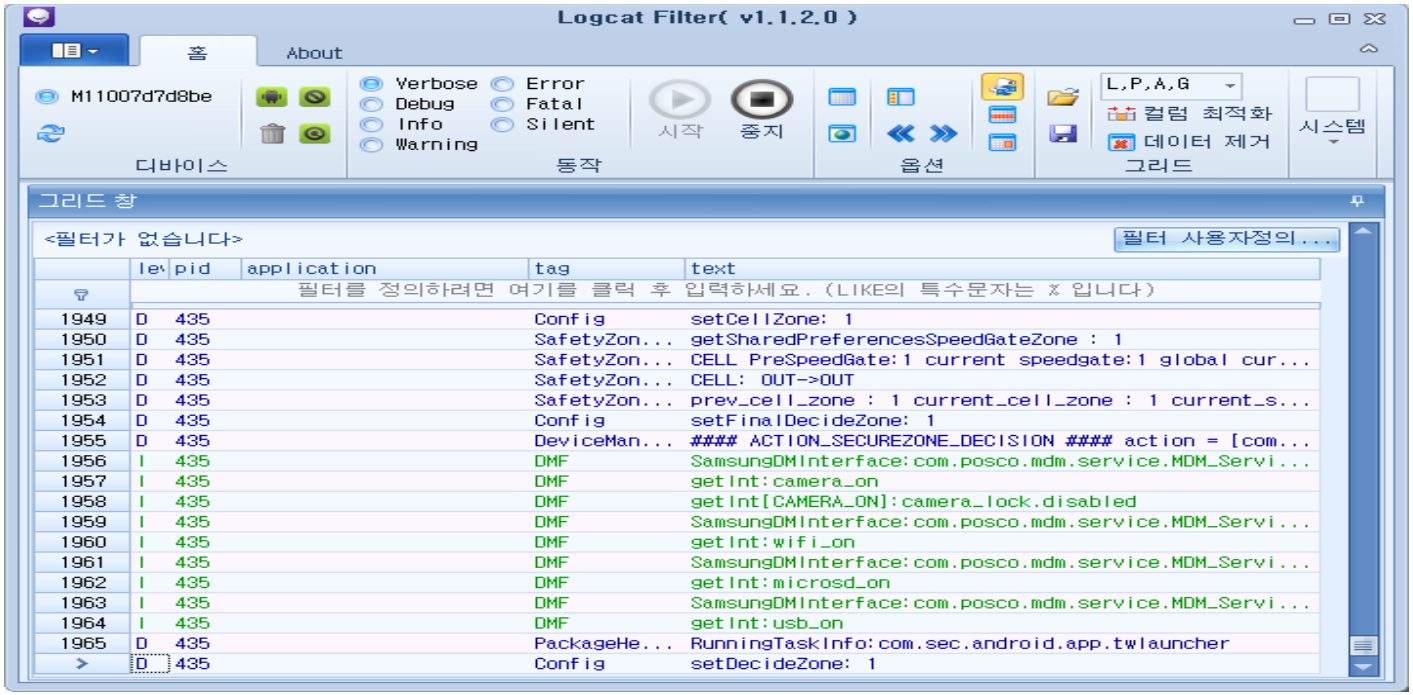


안드로이드 동적분석

- **logcat filter 활용(스마트 폰에서 발생시키는 로그를 분석)**

  아래 주소에서 다운 가능하다.

  http://cafe.naver.com/LogcatFilter



❖ 맨 좌측에는 디바이스정보가 나오며 중간은 로그의 순위를 나타낸다. 마지막으로 밑부분은 필터를 적용하여 검색 기능 활용 가능

Q & A

Reference

- 이창선, 김희현, 유진호, 컴퓨터 보안 창과 방패, 이한미디어, **2014**
- 조정원 외 **3**명, 안드로이드 모바일 악성코드와 모의 해킹 진단, 에어콘, **2014**
- 이동 전화 포렌식 가이드라인, 정보통신단체표준, **TTAS.KO-12.0059, 2007**
- 최우용, 은성경, “스마트폰 포렌식 기술 동향”, 한국전자통신연구원, 사이버 보안 기술 특집, **2013**
- 이규안, “모바일 포렌식의 현황과 전망”, **www.krnet.or.kr/board/include/download.php?no=1305&db=dprogram&fileno=2**, 대검찰청
- 오정훈, 이상진, “안드로이드 스마트폰 포렌식 분석 방법에 관한 연구”, 디지털 포렌식 연구, **2012**