Malware and Vulnerability Analysis Lecture3-2

Malware Analysis #3-2

Agenda

- 안드로이드 악성코드 분석

악성코드 분석

안드로이드 악성코드 정적분석

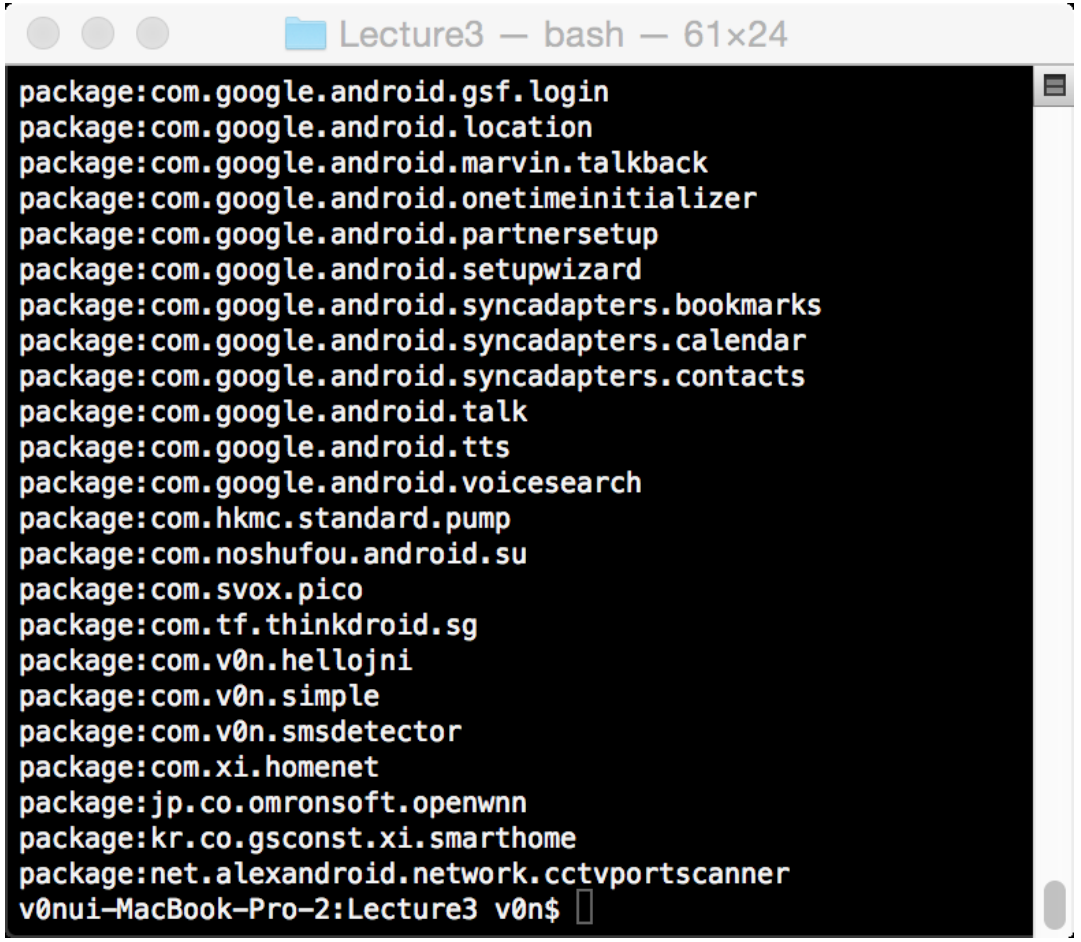
안드로이드 APK 분석

- APK 추출 #1
  - adb 명령
    - 안드로이드에 설치된 패키지 리스트 추출
    - adb shell pm list packages

```
v0nui-MacBook-Pro-2:Lecture3 v0n$ adb shell pm
usage: pm list packages [-f] [-d] [-e] [-s] [-3] [-i] [-u] [FILTER] → You will get full package list on your device
       pm list permission-groups
       pm list permissions [-g] [-f] [-d] [-u] [GROUP]
       pm list instrumentation [-f] [TARGET-PACKAGE]
       pm list features
       pm list libraries
       pm path PACKAGE → You will get a path of package
       pm install [-l] [-r] [-t] [-i INSTALLER_PACKAGE_NAME] [-s] [-f]
                   [--algo <algorithm name> --key <key-in-hex> --iv <IV-in-hex>] PATH
       pm uninstall [-k] PACKAGE
```

안드로이드 APK 분석

- APK 추출 #1
  - adb 명령
    - 안드로이드에 설치된 패키지 리스트 추출
    - adb shell pm list packages
    - adb shell pm list packages -f



안드로이드 APK 분석

- APK 추출 #1
  - adb 명령
    - adb shell pm list packages -f

```
package:/system/app/GoogleLoginService.apk=com.google.android.gsf.login
package:/system/app/NetworkLocation.apk=com.google.android.location
package:/system/app/Talkback.apk=com.google.android.marvin.talkback
package:/system/app/OneTimeInitializer.apk=com.google.android.onetimeinitializer
package:/system/app/GooglePartnerSetup.apk=com.google.android.partnersetup
package:/system/app/SetupWizard.apk=com.google.android.setupwizard
package:/system/app/ChromeBookmarksSyncAdapter.apk=com.google.android.syncadapters.bookmarks
package:/system/app/GoogleCalendarSyncAdapter.apk=com.google.android.syncadapters.calendar
package:/system/app/GoogleContactsSyncAdapter.apk=com.google.android.syncadapters.contacts
package:/system/app/Talk.apk=com.google.android.talk
package:/system/app/GoogleTTS.apk=com.google.android.tts
package:/system/app/VoiceSearchStub.apk=com.google.android.voicesearch
package:/data/app/com.hkmc.standard.pump-1.apk=com.hkmc.standard.pump
package:/system/app/Superuser.apk=com.noshufou.android.su
package:/system/app/PicoTts.apk=com.svox.pico
package:/system/app/Thinkfree.apk=com.tf.thinkdroid.sg
```

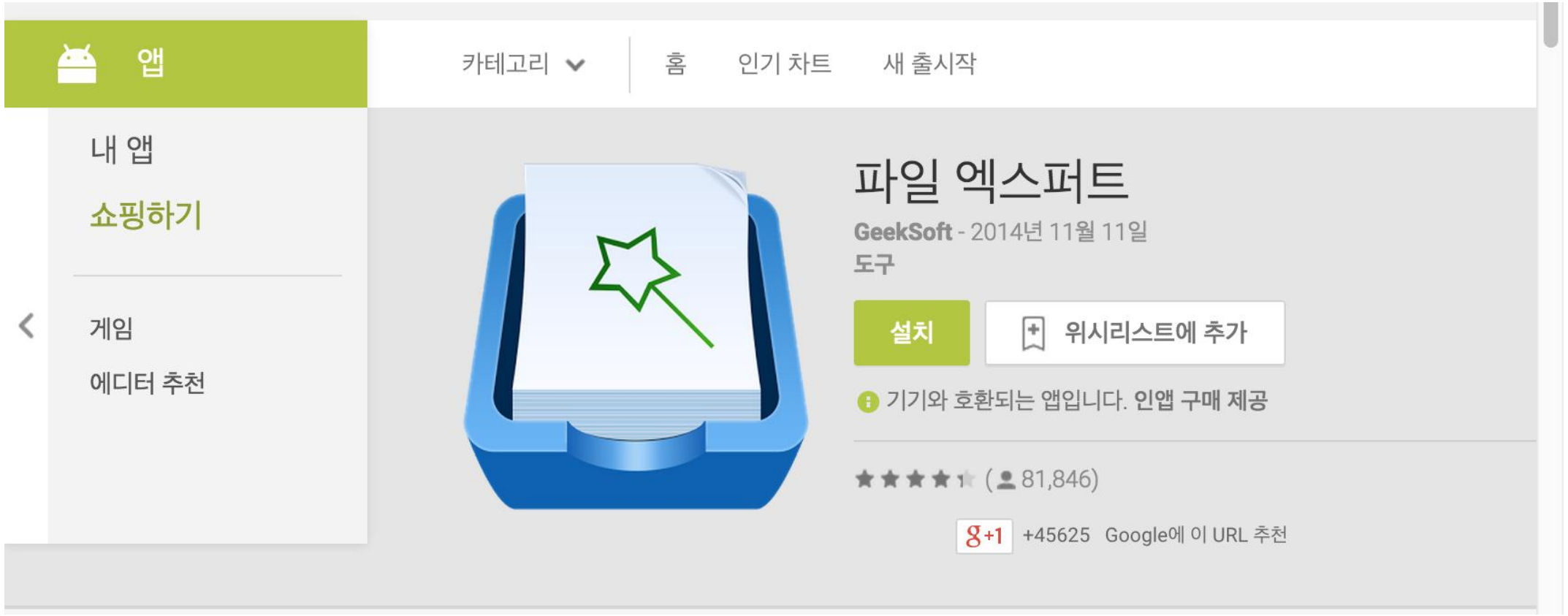
안드로이드 APK 분석

- APK 추출 #1
  - adb 명령
    - adb pull

```
package:/system/app/PicoTts.apk=com.svox.pico
package:/system/app/Thinkfree.apk=com.tf.thinkdroid.sg
package:/data/app/com.v0n.hellojni-2.apk=com.v0n.hellojni
package:/data/app/com.v0n.simple-1.apk=com.v0n.simple
package:/data/app/com.v0n.smsdetector-1.apk=com.v0n.smsdetector
package:/data/app/com.xi.homenet-1.apk=com.xi.homenet
package:/system/app/OpenWnn.apk=jp.co.omronsoft.openwnn
package:/data/app/kr.co.gsconst.xi.smarthome-1.apk=kr.co.gsconst.xi.smarthome
package:/data/app/net.alexandroid.network.cctvportscanner-1.apk=net.alexandroid.network.cctvportscanner
v0nui-MacBook-Pro-2:Lecture3 v0n$ adb pull /data/app/kr.co.gsconst.xi.smarthome-1.apk .
8040 KB/s (4861133 bytes in 0.590s)
v0nui-MacBook-Pro-2:Lecture3 v0n$ ls -al kr.co.gsconst.xi.smarthome-1.apk
-rw-r--r--  1 v0n  staff  4861133  3 29 18:25 kr.co.gsconst.xi.smarthome-1.apk
v0nui-MacBook-Pro-2:Lecture3 v0n$ file kr.co.gsconst.xi.smarthome-1.apk
kr.co.gsconst.xi.smarthome-1.apk: Zip archive data, at least v2.0 to extract
v0nui-MacBook-Pro-2:Lecture3 v0n$
```

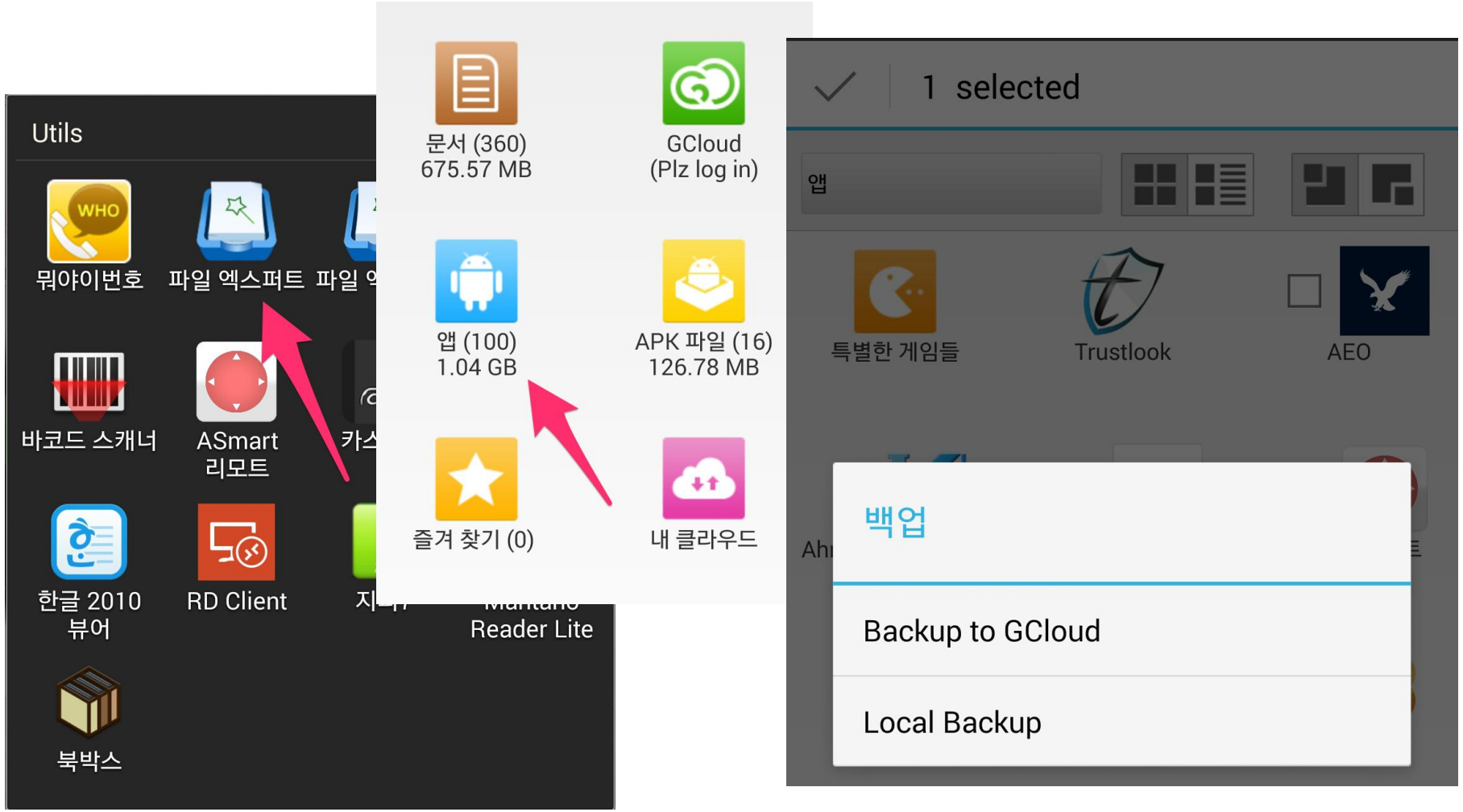
안드로이드 APK 분석

- APK 추출 #2
  - File 관리 앱



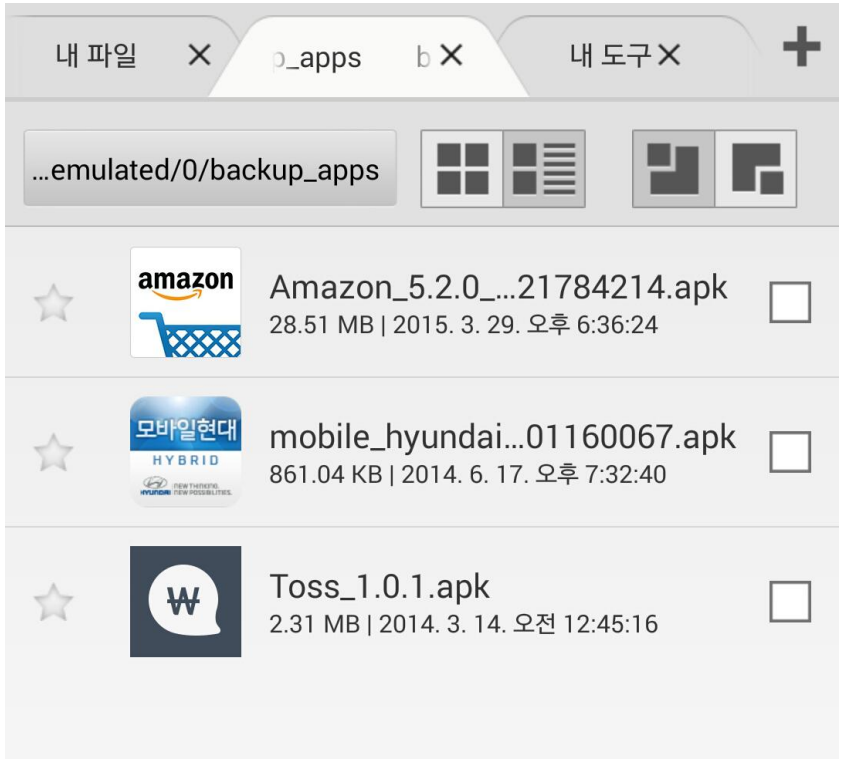
안드로이드 APK 분석

- APK 추출 #2
  - File 관리 앱



안드로이드 APK 분석

- APK 추출 #2
  - File 관리 앱
    - /sdcard/backup_apps/[FILENAME].apk



안드로이드 APK 분석

- APK 정적 분석
  - Unzip APK
    - APK는 ZIP으로 압축한 파일이므로 내용 확인을 위해 Unzip
  - AndroidManifest.xml
    - Encoding되어 있으므로 Decoding이 필요
  - classes.dex
    - DEX→JAR(JD-GUI)
  - libxxxxxx.so
    - IDAPro

안드로이드 APK 분석

- APK 정적 분석 : AndroidManifest.xml

AndroidManifest.xml

```
0300 0800 a80a 0000 0100 1c00 3805 0000
2400 0000 0000 0000 0000 0000 ac00 0000
0000 0000 0000 0000 1a00 0000 3400 0000
5200 0000 7600 0000 8200 0000 9c00 0000
a800 0000 b600 0000 c400 0000 dc00 0000
f000 0000 0401 0000 1601 0000 6e01 0000
7201 0000 8401 0000 9801 0000 c201 0000
cc01 0000 e001 0000 0202 0000 4202 0000
8202 0000 bc02 0000 d602 0000 ea02 0000
0803 0000 2603 0000 3603 0000 6e03 0000
8203 0000 c603 0000 da03 0000 f603 0000
3a04 0000 0b00 7600 6500 7200 7300 6900
6f00 6e00 4300 6f00 6400 6500 0000 0b00
7600 6500 7200 7300 6900 6f00 6e00 4e00
6100 6d00 6500 0000 0d00 6d00 6900 6e00
5300 6400 6b00 5600 6500 7200 7300 6900
6f00 6e00 0000 1000 7400 6100 7200 6700
6500 7400 5300 6400 6b00 5600 6500 7200
7300 6900 6f00 6e00 0000 0400 6e00 6100
6d00 6500 0000 0b00 6100 6c00 6c00 6f00
7700 4200 6100 6300 6b00 7500 7000 0000
0400 6900 6300 6f00 6e00 0000 0500 6c00
```

```
root@ubuntu:~/tools/axmlprinter2# ls -al
total 32
drwxr-xr-x  2 root root  4096 2013-03-06 23:53 .
drwxr-xr-x 13 root root  4096 2014-01-26 04:31 ..
-rw-r--r--  1 root root 24552 2008-10-09 20:17 AXMLPrinter2.jar
root@ubuntu:~/tools/axmlprinter2# java -jar AXMLPrinter2.jar
Usage: AXMLPrinter <binary xml file>
root@ubuntu:~/tools/axmlprinter2#
```

안드로이드 APK 분석

- APK 정적 분석 : AndroidManifest.xml

```
root@ubuntu:~/android_analysis/smarthome/gs_xi_done/kr.co.gsconst.xi.smarthome_j
ar# ls -al
total 1660
drwxr-xr-x  4 root root    4096 2014-12-15 05:56 .
drwxr-xr-x  5 root root    4096 2014-12-15 06:23 ..
-rw-r--r--  1 root root   10956 2014-12-15 05:56 AndroidManifest.xml
-rw-r--r--  1 root root 1051708 2014-12-15 05:56 classes.dex
-rw-r--r--  1 root root  573033 2014-12-15 05:56 classes_dex2jar.jar
drwxr-xr-x  2 root root    4096 2014-12-15 05:56 META-INF
drwxr-xr-x 10 root root    4096 2014-12-15 05:56 res
-rw-r--r--  1 root root   42784 2014-12-15 05:56 resources.arsc
root@ubuntu:~/android_analysis/smarthome/gs_xi_done/kr.co.gsconst.xi
ar# xxd AndroidManifest.xml | more
0000000: 0300 0800 cc2a 0000 0100 1c00 8c13 0000  .....*..........
0000010: 4d00 0000 0000 0000 0000 0000 5001 0000  M...........P...
0000020: 0000 0000 0000 0000 1a00 0000 3400 0000  ............4...
0000030: 5200 0000 7600 0000 8200 0000 a400 0000  R...v...........
0000040: b200 0000 be00 0000 cc00 0000 e400 0000  ................
0000050: 0a01 0000 3001 0000 4201 0000 9a01 0000  ....0...B.......
0000060: 9e01 0000 b001 0000 c401 0000 fc01 0000  ................
0000070: 0a02 0000 1e02 0000 4002 0000 7a02 0000  ........@...z...
0000080: cc02 0000 1603 0000 4e03 0000 b403 0000  ........N.......
0000090: 0c04 0000 4e04 0000 8a04 0000 c604 0000  ....N...........
00000a0: e004 0000 f404 0000 4e05 0000 a005 0000  ........N.......
00000b0: be05 0000 ce05 0000 1e06 0000 7806 0000  ............x...
00000c0: 8c06 0000 9e06 0000 c406 0000 d806 0000  ................
00000d0: 2607 0000 5e07 0000 a207 0000 fe07 0000  &...^...........
00000e0: 5808 0000 ba08 0000 1009 0000 6409 0000  X...........d...
```

```
root@ubuntu:~/android_analysis/smarthome/gs_xi_done/kr.co.gsconst.xi.smarthome_j
ar# java -jar ~/tools/axmlprinter2/AXMLPrinter2.jar AndroidManifest.xml > Androi
dManifest_decoded.xml
root@ubuntu:~/android_analysis/smarthome/gs_xi_done/kr.co.gsconst.xi.smarthome_j
ar# ls -al
total 1668
drwxr-xr-x  4 root root    4096 2015-04-13 07:55 .
drwxr-xr-x  5 root root    4096 2014-12-15 06:23 ..
-rw-r--r--  1 root root    7478 2015-04-13 07:55 AndroidManifest_decoded.xml
-rw-r--r--  1 root root   10956 2014-12-15 05:56 AndroidManifest.xml
-rw-r--r--  1 root root 1051708 2014-12-15 05:56 classes.dex
-rw-r--r--  1 root root  573033 2014-12-15 05:56 classes_dex2jar.jar
drwxr-xr-x  2 root root    4096 2014-12-15 05:56 META-INF
drwxr-xr-x 10 root root    4096 2014-12-15 05:56 res
-rw-r--r--  1 root root   42784 2014-12-15 05:56 resources.arsc
root@ubuntu:~/android_analysis/smarthome/gs_xi_done/kr.co.gsconst.xi.smarthome_j
ar#
```

안드로이드 APK 분석

- APK 정적 분석 : AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest
    xmlns:android="http://schemas.android.com/apk/res/android"
    android:versionCode="8"
    android:versionName="1.0.7"
    package="kr.co.gsconst.xi.smarthome"
    >
    <uses-sdk
        android:minSdkVersion="8"
        android:targetSdkVersion="15"
        >
    </uses-sdk>
```

```
<uses-permission
    android:name="android.permission.INTERNET"
    >
</uses-permission>
<uses-permission
    android:name="android.permission.ACCESS_NETWORK_STATE"
    >
</uses-permission>
<uses-permission
    android:name="android.permission.READ_PHONE_STATE"
    >
</uses-permission>
<uses-permission
    android:name="android.permission.VIBRATE"
    >
</uses-permission>
<permission
    android:name="kr.co.gsconst.xi.smarthome.permission.C2D_MESSAGE"
    android:protectionLevel="0x00000002"
    >
</permission>
<uses-permission
    android:name="kr.co.gsconst.xi.smarthome.permission.C2D_MESSAGE"
    >
```

안드로이드 APK 분석

- APK 정적 분석 classes.dex
  - 안드로이드 앱을 개발할 때,
    - java → class/jar → dex
  - clases.dex를 분석할 때(from dex to jar),
    - dex → jar → java

dex2jar

Tools to work with android .dex and java .class files

1. dex-reader/writer: Read/write the Dalvik Executable (.dex) file. It has a light weight API similar with ASM.
2. d2j-dex2jar: Convert .dex file to .class files (zipped as jar)
3. smali/baksmali: disassemble dex to smali files and assemble dex from smali files. different implementation to smali/baksmali, same syntax, but we support escape in type desc "Lcom/dex2jar\t\u1234;"
4. other tools: d2j-decrypt-string

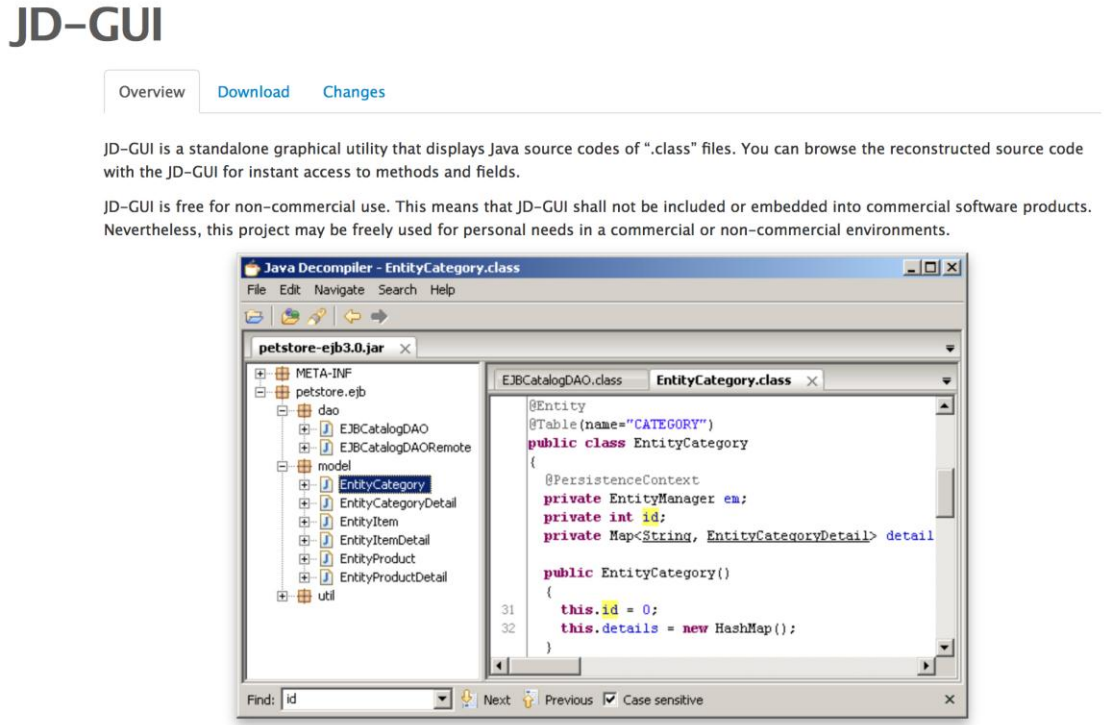
안드로이드 APK 분석

- APK 정적 분석 classes.dex

```
root@ubuntu:~/android_analysis/smarthome/gs_xi_done/kr.co.gsconst.xi.smarthome_jar# ll
total 1108
drwxr-xr-x  4 root root    4096 2015-04-13 08:00 ./
drwxr-xr-x  5 root root    4096 2014-12-15 06:23 ../
-rw-r--r--  1 root root    7478 2015-04-13 07:55 AndroidManifest_decoded.xml
-rw-r--r--  1 root root   10956 2014-12-15 05:56 AndroidManifest.xml
-rw-r--r--  1 root root 1051708 2014-12-15 05:56 classes.dex
drwxr-xr-x  2 root root    4096 2014-12-15 05:56 META-INF/
drwxr-xr-x 10 root root    4096 2014-12-15 05:56 res/
-rw-r--r--  1 root root   42784 2014-12-15 05:56 resources.arsc
root@ubuntu:~/android_analysis/smarthome/gs_xi_done/kr.co.gsconst.xi.smarthome_jar# ~/tools
/dex2jar/dex2jar.sh
dex2jar version: translator-0.0.9.8
dex2jar file1.dex0Rapk file2.dex0Rapk ...
root@ubuntu:~/android_analysis/smarthome/gs_xi_done/kr.co.gsconst.xi.smarthome_jar# ~/tools
/dex2jar/dex2jar.sh classes.dex
dex2jar version: translator-0.0.9.8
dex2jar classes.dex -> classes_dex2jar.jar
Done.
root@ubuntu:~/android_analysis/smarthome/gs_xi_done/kr.co.gsconst.xi.smarthome_jar# ls -al
classes*
-rw-r--r-- 1 root root 1051708 2014-12-15 05:56 classes.dex
-rw-r--r-- 1 root root  567552 2015-04-13 08:00 classes_dex2jar.jar
root@ubuntu:~/android_analysis/smarthome/gs_xi_done/kr.co.gsconst.xi.smarthome_jar#
```

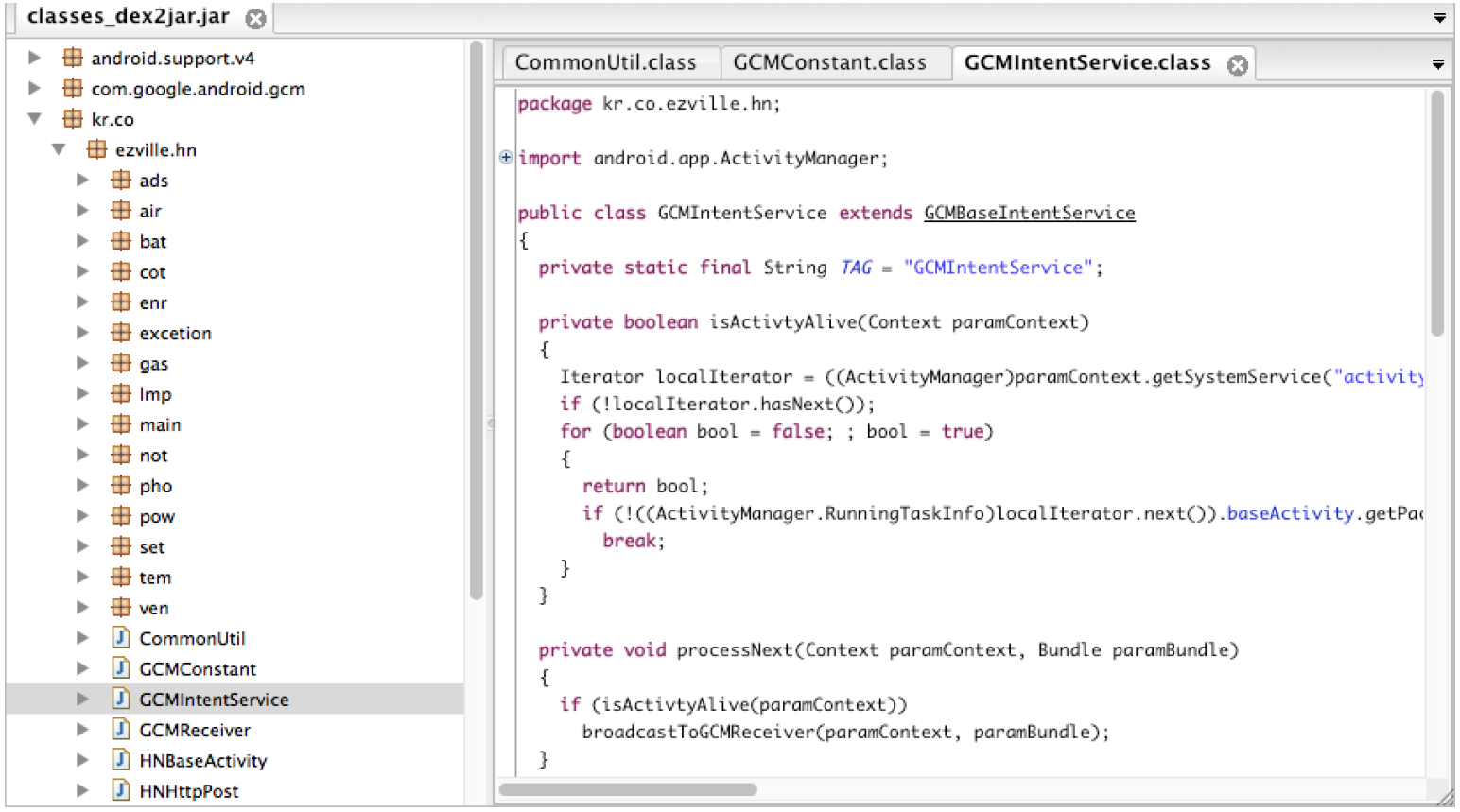
안드로이드 APK 분석

- APK 정적 분석 classes.dex
  - JAR는 Class 파일 Archive
    - Class파일의 Decompile을 통해 Java 코드를 구할 수 있음
  - Java Decompile
    - jd-gui : http://jd.benow.ca
    - jad : http://varaneckas.com/jad/



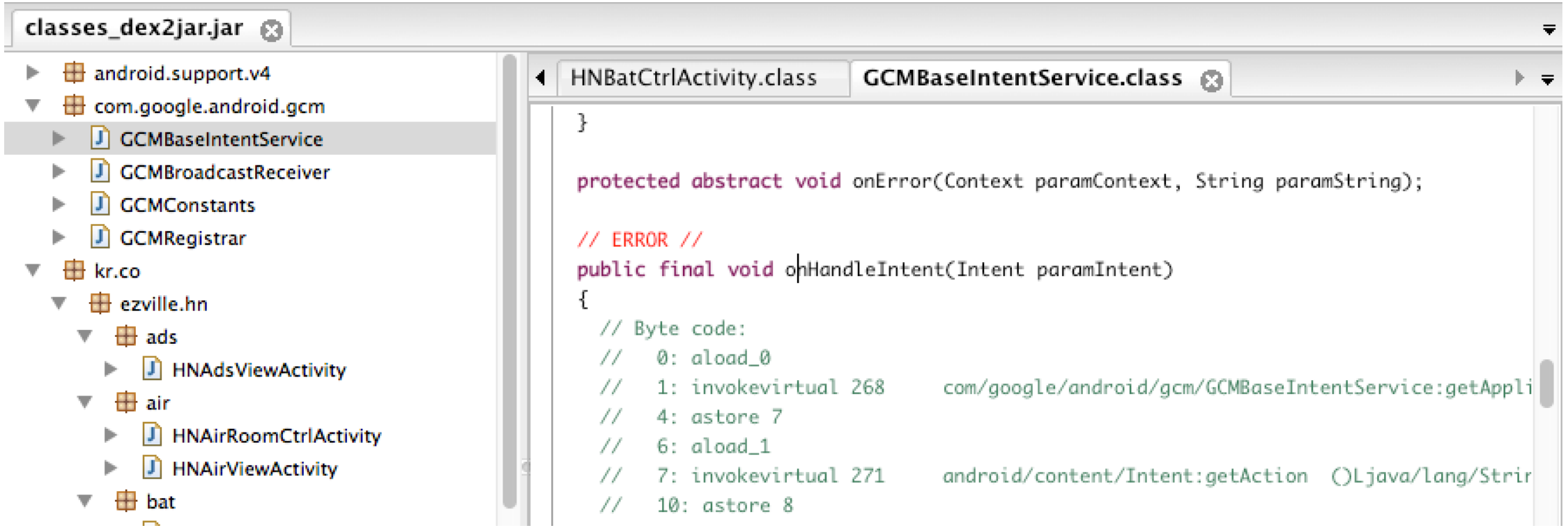
안드로이드 APK 분석

- APK 정적 분석 classes.dex
  - jd-gui를 사용한 Decomplie



안드로이드 APK 분석

- APK 정적 분석 classes.dex
  - jd-gui의 문제점 : // ERROR //(Decompile 오류로 인해 Java코드 볼 수 없음)



안드로이드 APK 분석

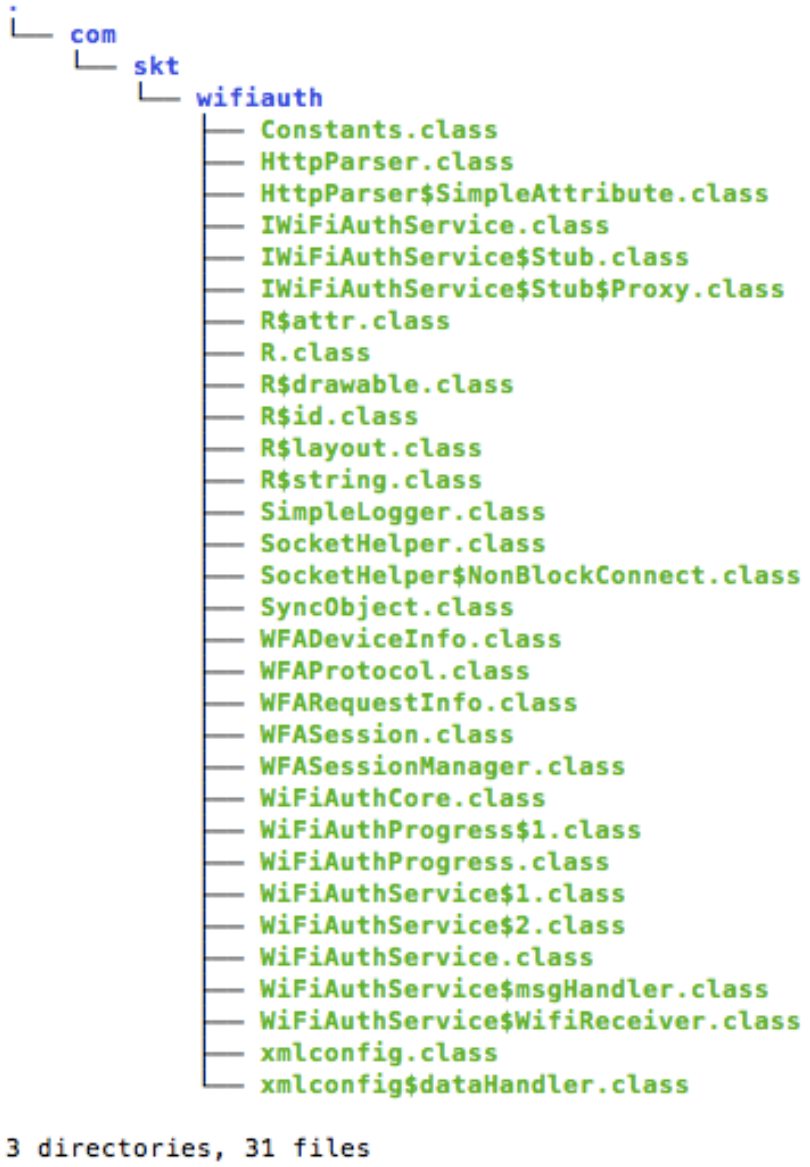
- APK 정적 분석 classes.dex
  - Decompile 오류로 코드를 읽을 수 없는 경우 대처 방안
    - jad
    - smali(apktool) : http://ibotpeaches.github.io/Apktool/
      - dex → smali code

A tool for reverse engineering Android apk files

```
$ apktool d test.apk
I: Using Apktool 2.0.0 on test.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: 1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
$ apktool b test
I: Using Apktool 2.0.0 on test
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
I: Building apk file...
I: Copying unknown files/dir...
$
```

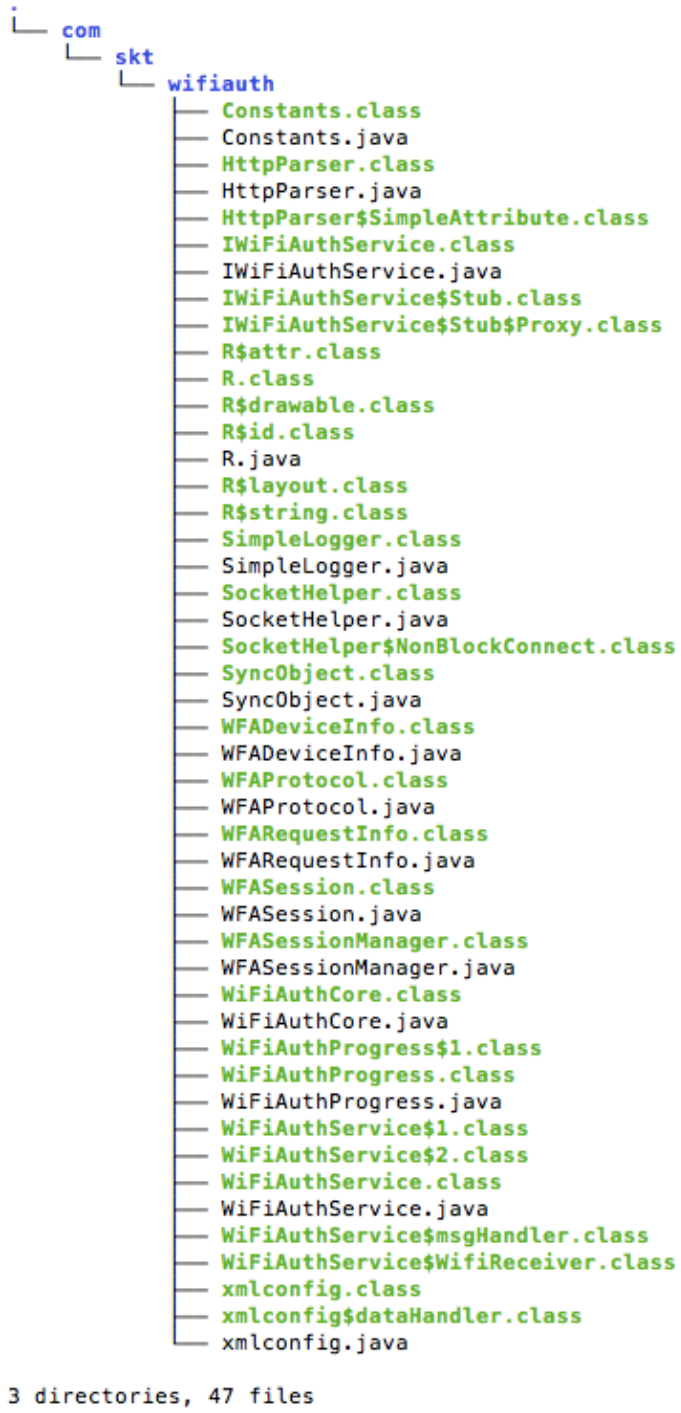
안드로이드 APK 분석

- APK 정적 분석 classes.dex
  - jad 사용법
    - class → java(jad)
      - jad -o -r -sjava **/*.class
      - jad -o -sjava [name].class



안드로이드 APK 분석

- APK 정적 분석 classes.dex
  - jad 사용법
    - class → java(jad)
      - jad -o -r -sjava **/*.class
      - jad -o -sjava [name].class



안드로이드 APK 분석

- APK 정적 분석 classes.dex
  - jad 사용법
    - class → java(jad)

```
    public void printBin(int j, String s, byte abyte0[])
    {
        if(mLogLevel <= j) goto _L2; else goto _L1
_L1:
        return;
_L2:
        byte abyte1[] = new byte[16];
        abyte1[0] = 48;
        abyte1[1] = 49;
        abyte1[2] = 50;
        abyte1[3] = 51;
        abyte1[4] = 52;
        abyte1[5] = 53;
        abyte1[6] = 54;
        abyte1[7] = 55;
        abyte1[8] = 56;
        abyte1[9] = 57;
        abyte1[10] = 65;
        abyte1[11] = 66;
        abyte1[12] = 67;
        abyte1[13] = 68;
        abyte1[14] = 69;
        abyte1[15] = 70;
                                    } else
                                    {
                                        int l1 = k1 + 1;
                                        abyte2[k1] = 32;
                                        k = l1;
                                    }
                                    l++;
                                } while(true);
                                if(true) goto _L1; else goto _L3
                            _L3:
```

안드로이드 APK 분석

- APK 정적 분석 classes.dex
  - apktool 사용법
    - apktool d[ecode] [OPTS] <file.apk> [<dir>]
    - apktool b[uild] [OPTS] [<app_path>] [<out_file>]

```
root@ubuntu:~/android_analysis/ysu_seminar# ll HelloActivity.apk
-rwxr-xr-x 1 root root 180132 2013-12-01 21:19 HelloActivity.apk*
root@ubuntu:~/android_analysis/ysu_seminar# apktool d HelloActivity.apk HelloActivity_smali
I: Baksmaling...
I: Loading resource table...
I: Loaded.
I: Loading resource table from file: /root/apktool/framework/1.apk
I: Loaded.
I: Decoding file-resources...
I: Decoding values*/* XMLs...
I: Done.
I: Copying assets and libs...
```

안드로이드 APK 분석

- APK 정적 분석 classes.dex
  - apktool 사용법
    - apktool d를 사용하여 Decompile할 때, Resource Error가 발생할 경우
    - apktool을 update하거나 –r 옵션 사용

```
root@ubuntu:~/android_analysis/moca# ~/tools/apktool/apktool d moca_03.00.43.apk moca
I: Baksmaling...
I: Loading resource table...
I: Loaded.
I: Loading resource table from file: /root/apktool/framework/1.apk
I: Loaded.
I: Decoding file-resources...
W: Cant find 9patch chunk in file: "drawable-hdpi/menu_bar2.9.png". Renaming it to *.png.
I: Decoding values*/* XMLs...
I: Done.
I: Copying assets and libs...
root@ubuntu:~/android_analysis/moca#
```

안드로이드 APK 분석

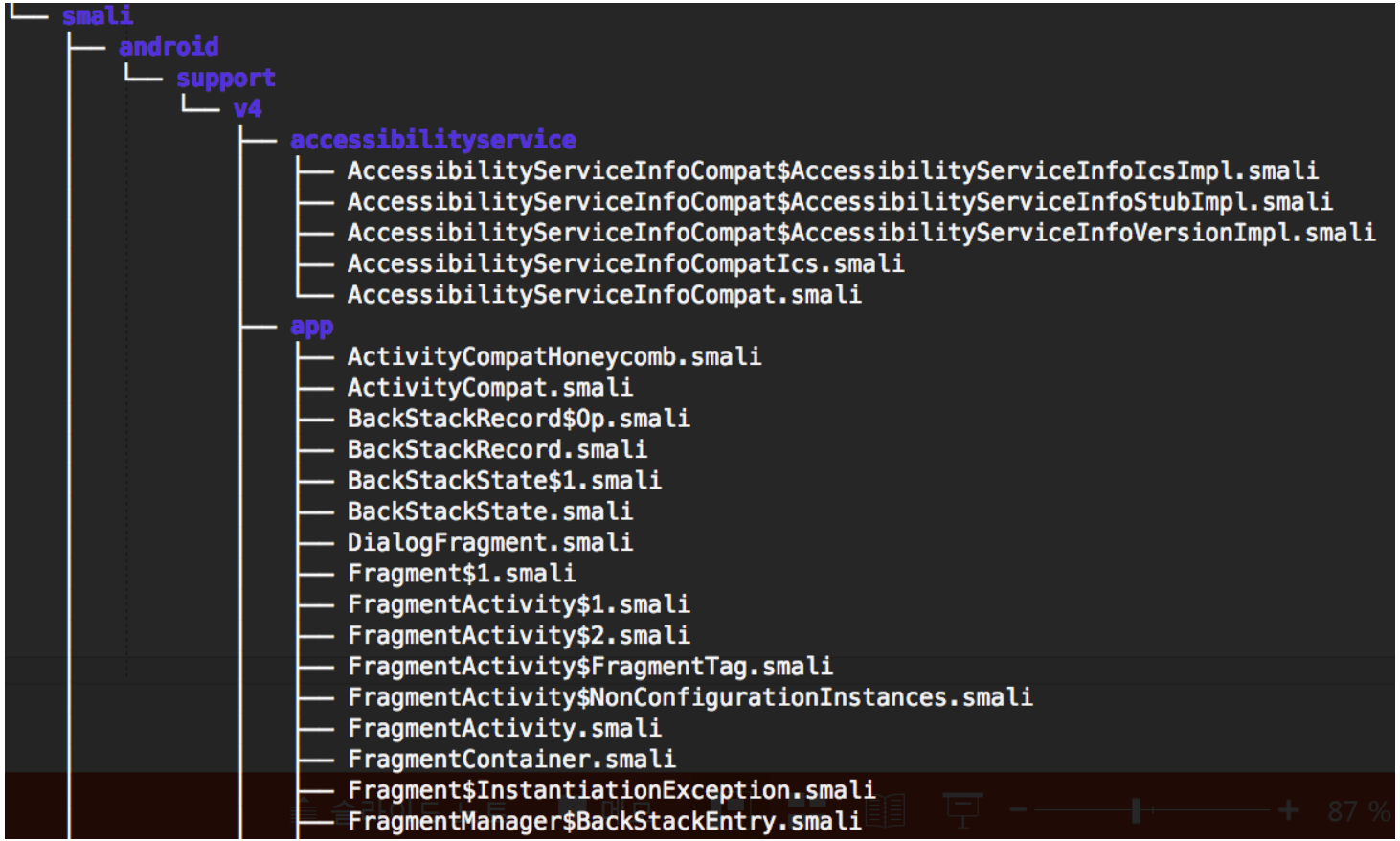
- APK 정적 분석 classes.dex
  - apktool은 Decompile한 결과 코드를 smali 디렉토리에 저장

```
root@ubuntu:~/android_analysis/ysu_seminar# ll HelloActivity.apk HelloActivity_smali
-rwxr-xr-x 1 root root 180132 2013-12-01 21:19 HelloActivity.apk*

HelloActivity_smali:
total 24
drwxr-xr-x  4 root root 4096 2015-04-13 08:22 ./
drwxr-xr-x  6 root root 4096 2015-04-13 08:22 ../
-rw-r--r--  1 root root  769 2015-04-13 08:22 AndroidManifest.xml
-rw-r--r--  1 root root   96 2015-04-13 08:22 apktool.yml
drwxr-xr-x 11 root root 4096 2015-04-13 08:22 res/
drwxr-xr-x  4 root root 4096 2015-04-13 08:22 smali/
root@ubuntu:~/android_analysis/ysu_seminar#
```

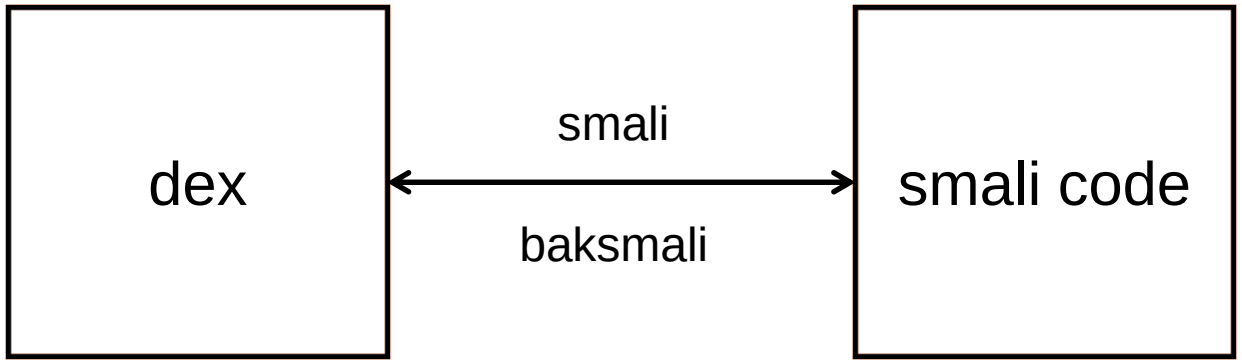
안드로이드 APK 분석

- APK 정적 분석 classes.dex
  - smali 디렉토리는 classes 구조 그대로 디렉토리 구조로 저장



안드로이드 APK 분석

- APK 정적 분석 classes.dex
  - apktool : smali/baksmli → assembler/disassembler



안드로이드 APK 분석

- APK 정적 분석 classes.dex
  - smali code 분석
    - http://pallergabor.uw.hu/androidblog/dalvik_opcodes.html

```
.method public static declared-synchronized getInstance()Lcom/skt/wifiauth/SimpleLogger;
    .locals 2

    .prologue
    .line 23
    const-class v0, Lcom/skt/wifiauth/SimpleLogger;

    monitor-enter v0

    :try_start_0
    sget-object v1, Lcom/skt/wifiauth/SimpleLogger;->mInstance:Lcom/skt/wifiauth/SimpleLogger;

    if-nez v1, :cond_0

    .line 24
    new-instance v1, Lcom/skt/wifiauth/SimpleLogger;

    invoke-direct {v1}, Lcom/skt/wifiauth/SimpleLogger;-><init>()V

    sput-object v1, Lcom/skt/wifiauth/SimpleLogger;->mInstance:Lcom/skt/wifiauth/SimpleLogger;

    .line 25
    :cond_0
    sget-object v1, Lcom/skt/wifiauth/SimpleLogger;->mInstance:Lcom/skt/wifiauth/SimpleLogger;
    :try_end_0
    .catchall {:try_start_0 .. :try_end_0} :catchall_0

    monitor-exit v0

    return-object v1
```

안드로이드 APK 분석

- APK 정적 분석 classes.dex
  - smali code 분석 #1

```
.method public constructor <init>()V
    .locals 1
    .prologue
    .line 64
    invoke-direct {p0}, Lcom/kt/android/showtouch/base/BaseActivity;-><init>()V

    .line 66
    const-string v0, "MOCA_Wallet UserJoinActivity"
    iput-object v0, p0, Lcom/kt/android/showtouch/activity/main/UserJoinActivity;->TAG:Ljava/lang/String;

    .line 77
    const/4 v0, 0x0
    iput-boolean v0, p0, Lcom/kt/android/showtouch/activity/main/UserJoinActivity;->isKeyboard:Z

    .line 121
    new-instance v0, Lcom/kt/android/showtouch/activity/main/UserJoinActivity$1;
    invoke-direct {v0, p0}, Lcom/kt/android/showtouch/activity/main/UserJoinActivity$1;-><init>(Lcom/kt/android/showtouch/activity/main/UserJoinActivity;)V
    iput-object v0, p0, Lcom/kt/android/showtouch/activity/main/UserJoinActivity;->getHeightThread:Ljava/lang/Thread;

    .line 64
    return-void
.end method
```

```
# virtual methods
.method public d(Ljava/lang/String;)I
    .locals 2
    .parameter "msg"

    .prologue
    .line 59
    iget v0, p0, Lcom/skt/wifiauth/SimpleLogger;->mLogLevel:I
```

안드로이드 APK 분석

- APK 정적 분석 classes.dex
  - smali code 분석 #2

```
.line 155
    :try_start_0
    const-string v3, "/moca/NewSetKmcSms.php"

    invoke-virtual {v0, v3}, Lcom/kt/android/showtouch/manager/ApiManager;->setApiUri(Ljava/lang/String;)Lcom/kt/android/showtouch/manager/ApiManager;

    move-result-object v3

    invoke-virtual {v3}, Lcom/kt/android/showtouch/manager/ApiManager;->clearParams()Lcom/kt/android/showtouch/manager/ApiManager;

    move-result-object v3

    iget-object v4, p0, Lcom/kt/android/showtouch/activity/main/UserJoinActivity;->userRegParamList:Ljava/util/ArrayList;

    invoke-virtual {v3, v4}, Lcom/kt/android/showtouch/manager/ApiManager;->appendParamList(Ljava/util/List;)Lcom/kt/android/showtouch/manager/ApiManager;

    move-result-object v3
```

안드로이드 APK 분석

- APK 정적 분석 classes.dex
  - smali code 분석 #3

```
invoke-virtual {v3}, Lcom/kt/android/showtouch/manager/ApiManager;->read()Z
:try_end_0
.catch Ljava/lang/Exception; {:try_start_0 .. :try_end_0} :catch_0

.line 161
:goto_0
invoke-direct {p0}, Lcom/kt/android/showtouch/activity/main/UserJoinActivity;->setSmsReceiverHandler()V

.line 162
return-void

.line 156
:catch_0
move-exception v1

.line 157
.local v1, e:Ljava/lang/Exception;
const-string v3, "MOCA_Wallet UserJoinActivity"

new-instance v4, Ljava/lang/StringBuilder;

invoke-direct {v4}, Ljava/lang/StringBuilder;-><init>()V
```

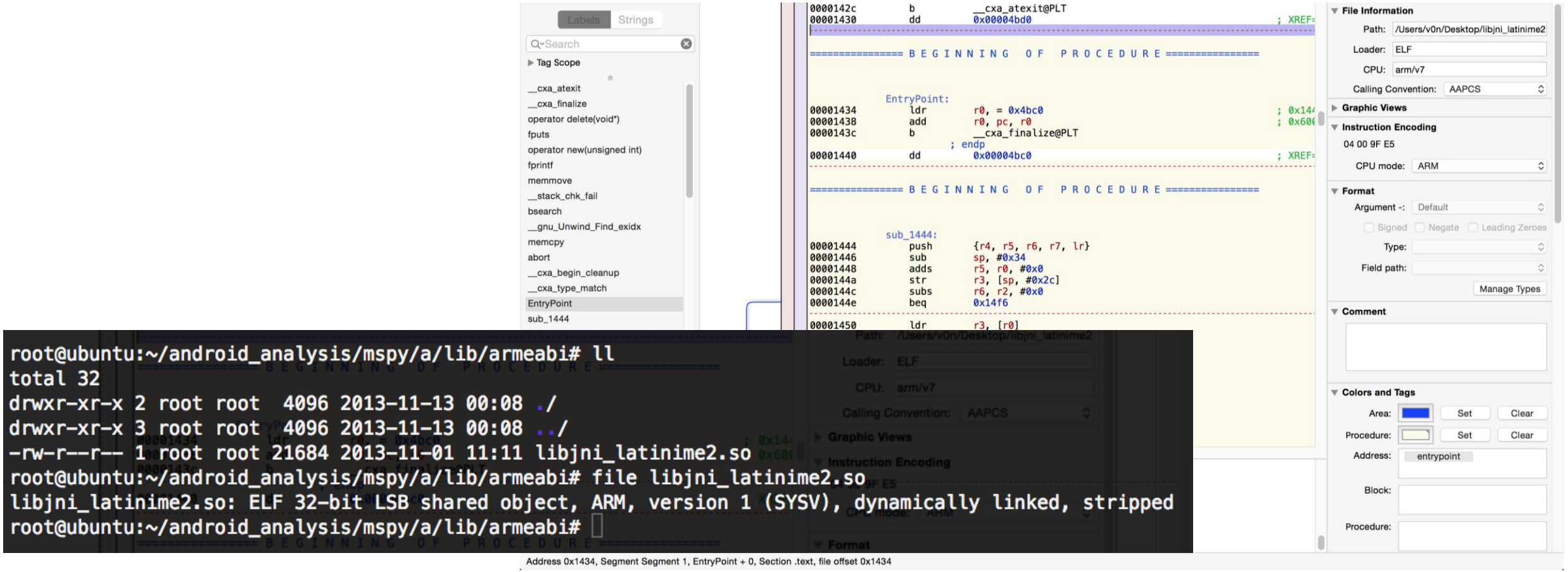
안드로이드 APK 분석

- APK 정적 분석 classes.dex
  - smali code 분석 #4

```
new-instance v6, Ljava/lang/StringBuilder;
invoke-static {p2}, Ljava/lang/String;->valueOf(Ljava/lang/Object;)Ljava/lang/String;
move-result-object v7
invoke-direct {v6, v7}, Ljava/lang/StringBuilder;-><init>(Ljava/lang/String;)V
const-string v7, "("
invoke-virtual {v6, v7}, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;
move-result-object v6
array-length v7, p3
invoke-virtual {v6, v7}, Ljava/lang/StringBuilder;->append(I)Ljava/lang/StringBuilder;
move-result-object v6
const-string v7, ")"
invoke-virtual {v6, v7}, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;
move-result-object v6
invoke-virtual {v6}, Ljava/lang/StringBuilder;->toString()Ljava/lang/String;
move-result-object v6
invoke-virtual {p0, v6}, Lcom/skt/wifiauth/SimpleLogger;->i(Ljava/lang/String;)I
```

안드로이드 APK 분석

- APK 정적 분석 : libxxxxxx.so




```
root@ubuntu:~/android_analysis/mspy/a/lib/armeabi# ll
total 32
drwxr-xr-x 2 root root  4096 2013-11-13 00:08 ./
drwxr-xr-x 3 root root  4096 2013-11-13 00:08 ../
-rw-r--r-- 1 root root 21684 2013-11-01 11:11 libjni_latinime2.so
root@ubuntu:~/android_analysis/mspy/a/lib/armeabi# file libjni_latinime2.so
libjni_latinime2.so: ELF 32-bit LSB shared object, ARM, version 1 (SYSV), dynamically linked, stripped
root@ubuntu:~/android_analysis/mspy/a/lib/armeabi#
```

안드로이드 APK 분석

- APK 정적 분석 : Decompile
  - classes.dex → jar(dex2jar)
  - classes.dex → smali(apktool)
  - class → java(jad)

Q&A