Android应用的破解与保护

为什么要破解其他应用

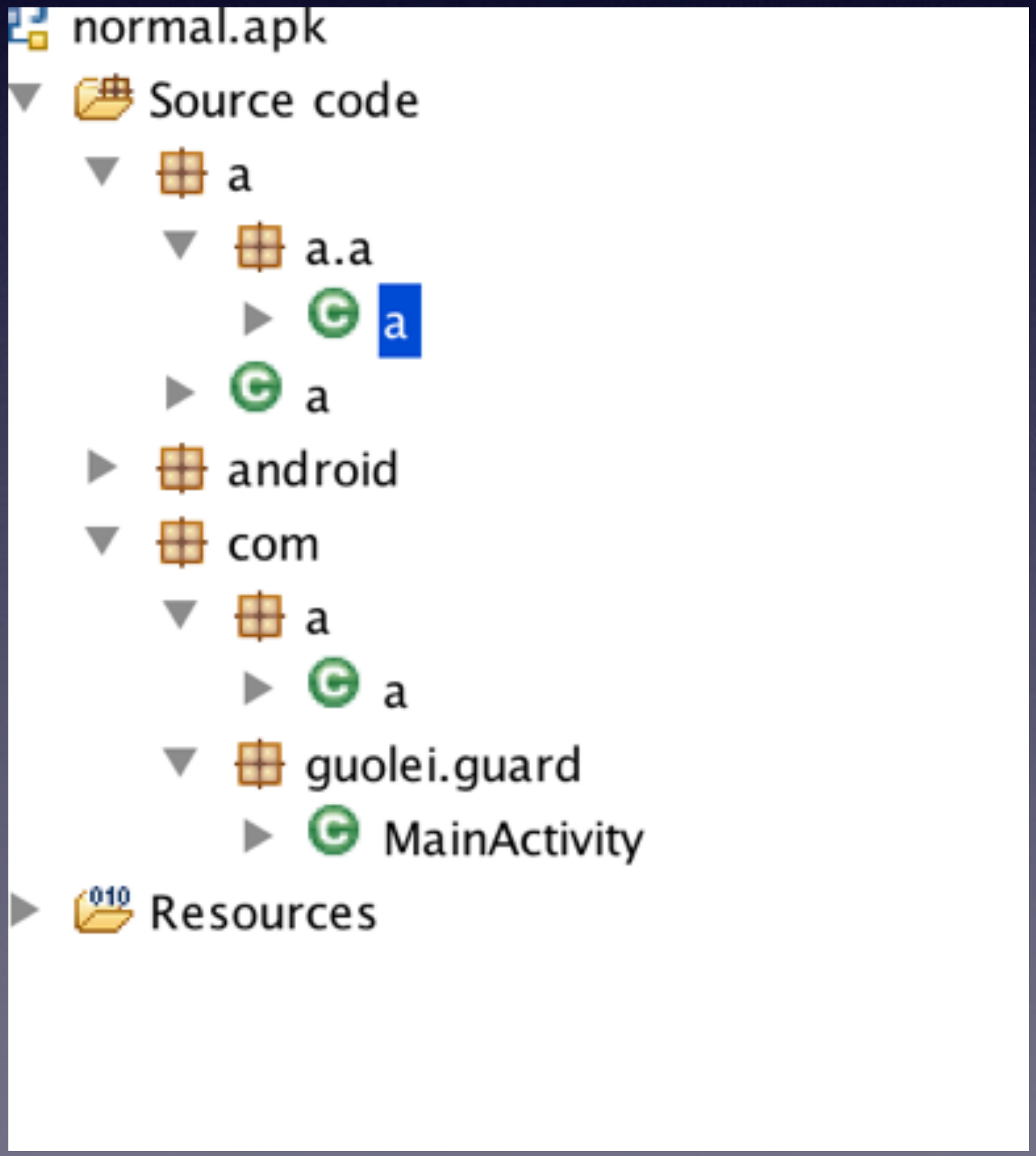
- 学习他们的代码
- 了解竞品功能的实现方式
- 破解应用对用户的限制

初级防护-混淆

- 代码混淆(Obfuscated code)亦称花指令，是将计算机程序的代码，转换成一种功能上等价，但是难于阅读和理解的形式的行为
- 代码压缩
- https://www.guardsquare.com/en/proguard
- 普通混淆
- 自定义混淆字典
- 资源混淆

普通混淆

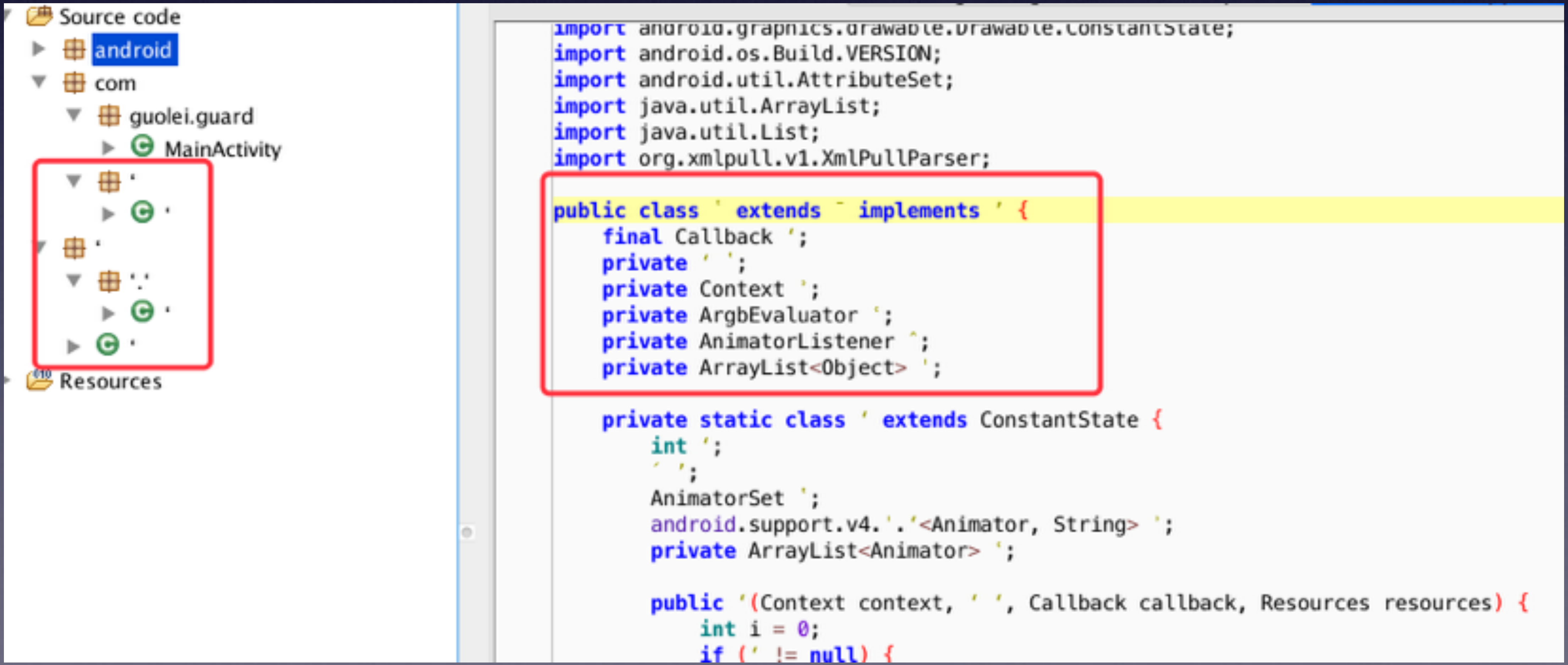
- 只单纯的配置混淆规则对代码进行混淆



```
normal.apk
▼ Source code
    ▼ a
        ▼ a.a
            ▶ a
        ▶ a
    ▶ android
    ▼ com
        ▼ a
            ▶ a
        ▼ guolei.guard
            ▶ MainActivity
▶ Resources
```

混淆字典

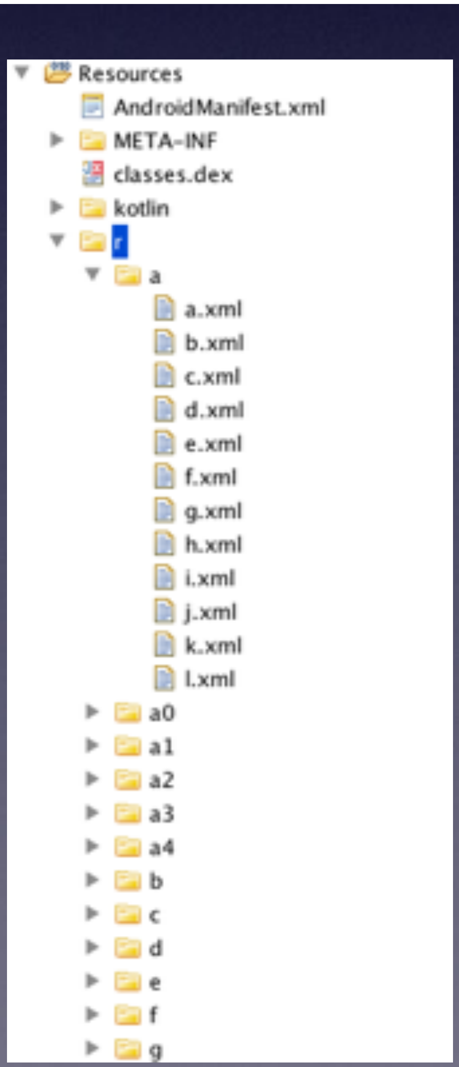
- 通过自己编写混淆字典，来配置比abc这样更具有干扰性的符号



```java
import android.graphics.drawable.Drawable.ConstantState;
import android.os.Build.VERSION;
import android.util.AttributeSet;
import java.util.ArrayList;
import java.util.List;
import org.xmlpull.v1.XmlPullParser;

public class ' extends ˉ implements ' {
    final Callback ';
    private ' ';
    private Context ';
    private ArgbEvaluator ';
    private AnimatorListener ˆ;
    private ArrayList<Object> ';

    private static class ' extends ConstantState {
        int ';
        ' ';
        AnimatorSet ';
        android.support.v4.'.'<Animator, String> ';
        private ArrayList<Animator> ';

        public '(Context context, ' ', Callback callback, Resources resources) {
            int i = 0;
            if (' != null) {
```

资源混淆

- 目的：1. 防止资源文件被盗用 2. 压缩apk体积
- https://github.com/shwenzhang/AndResGuard



```
▼ Resources
    AndroidManifest.xml
  ▶ META-INF
    classes.dex
  ▶ kotlin
  ▼ r
    ▼ a
        a.xml
        b.xml
        c.xml
        d.xml
        e.xml
        f.xml
        g.xml
        h.xml
        i.xml
        j.xml
        k.xml
        l.xml
    ▶ a0
    ▶ a1
    ▶ a2
    ▶ a3
    ▶ a4
    ▶ b
    ▶ c
    ▶ d
    ▶ e
    ▶ f
    ▶ g
```

- 混淆只能加大阅读难度，并且反编译的难度极其低。如果愿意花时间阅读，还是能理解的。
- 思考:如何加大反编译难度?

高级保护

- 经过上面的一些保护措施，还是可以很容易拿到我们源代码经过编译的产物，也可以利用一些手段进行还原。

- 加固，对dex文件进行加密

加固技术的发展

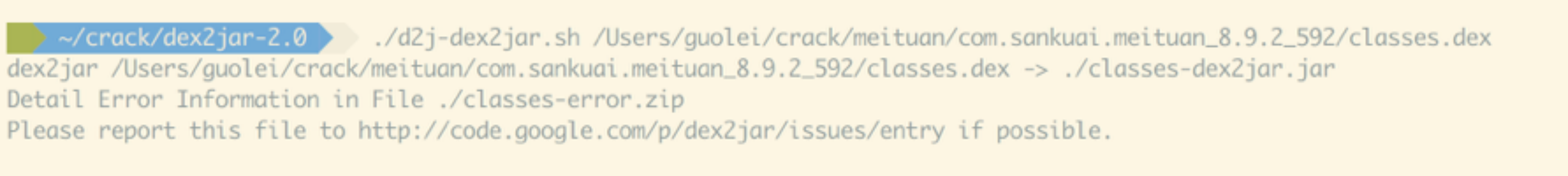
- Dex加密
- Dex抽取
- Dex动态解密与so混淆
- VMP虚拟机保护技术

Dex加密

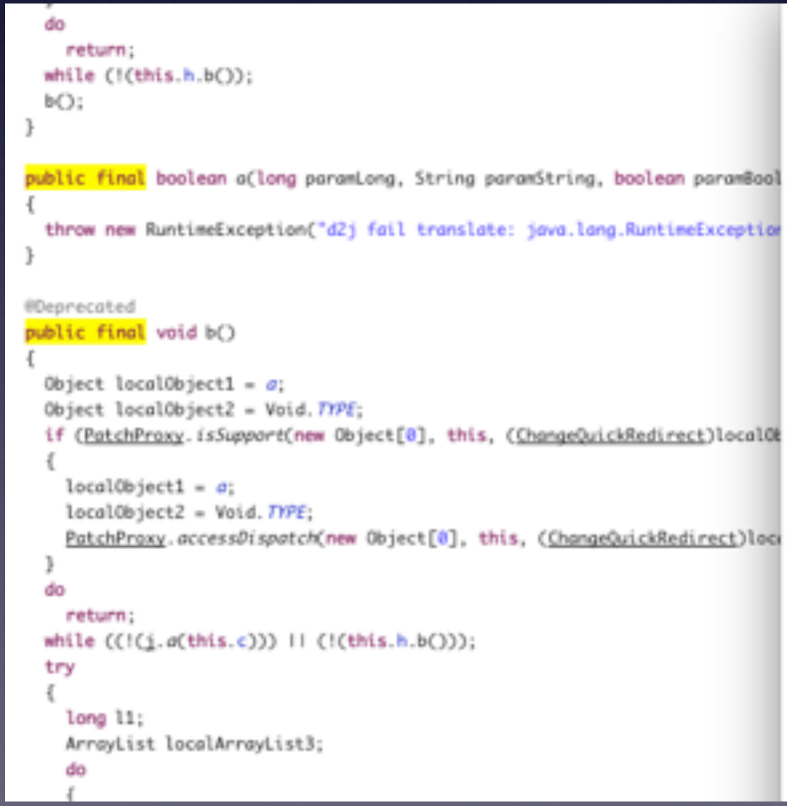
- Dex字符串加密，对dex文件中出现的字符串进行加密，保护出现的各种key,可以看下 https://github.com/MegatronKing/StringFog

- 对抗反编译，利用一些反编译工具现有的bug，在源代码中加入一些花指令使得反编译失效

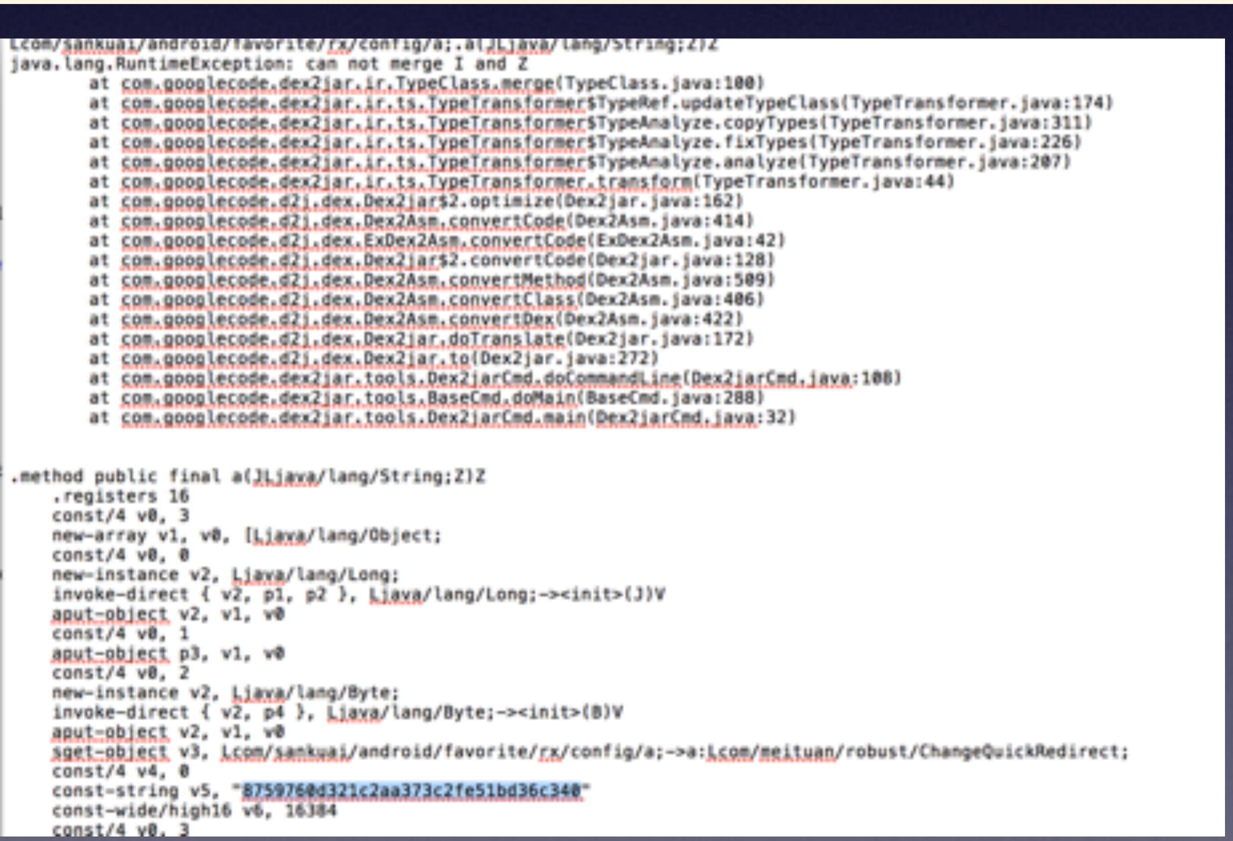
- 样本：美团
- 反编译工具：dex2jar



```
~/crack/dex2jar-2.0  ./d2j-dex2jar.sh /Users/guolei/crack/meituan/com.sankuai.meituan_8.9.2_592/classes.dex
dex2jar /Users/guolei/crack/meituan/com.sankuai.meituan_8.9.2_592/classes.dex -> ./classes-dex2jar.jar
Detail Error Information in File ./classes-error.zip
Please report this file to http://code.google.com/p/dex2jar/issues/entry if possible.
```

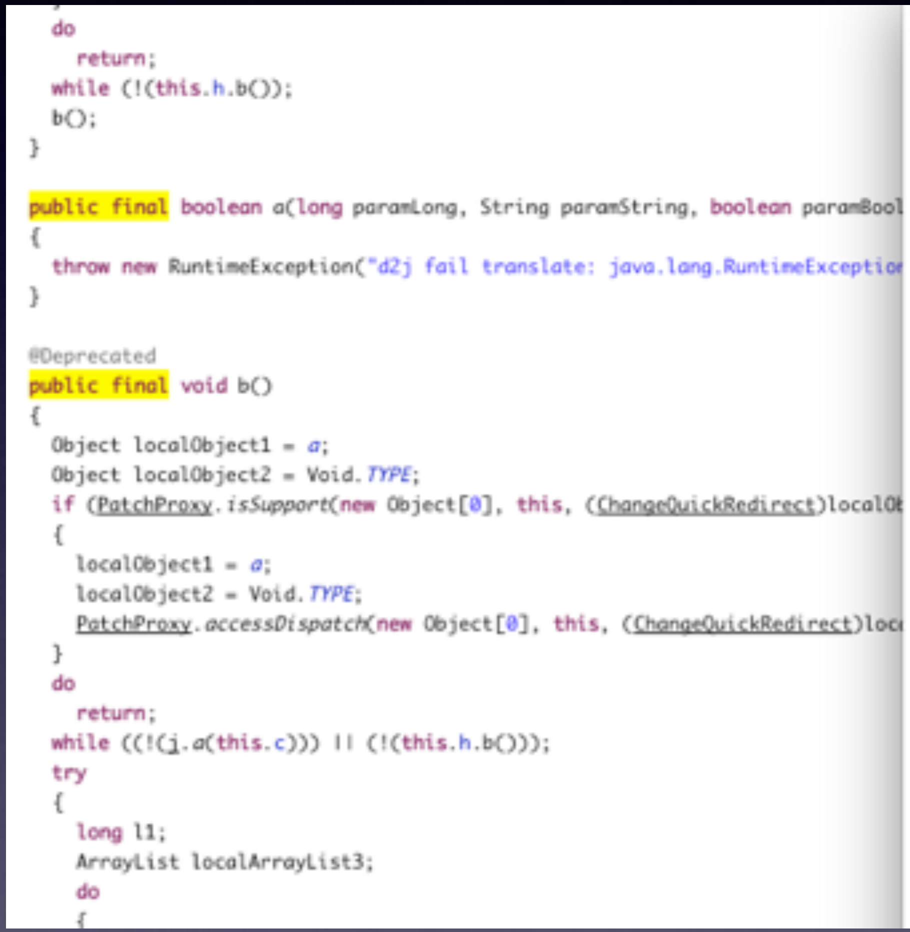


```
  do
    return;
  while (!(this.h.b()));
  b();
}

public final boolean a(long paramLong, String paramString, boolean paramBool
{
  throw new RuntimeException("d2j fail translate: java.lang.RuntimeExceptio
}

@Deprecated
public final void b()
{
  Object localObject1 = a;
  Object localObject2 = Void.TYPE;
  if (PatchProxy.isSupport(new Object[0], this, (ChangeQuickRedirect)localOb
  {
    localObject1 = a;
    localObject2 = Void.TYPE;
    PatchProxy.accessDispatch(new Object[0], this, (ChangeQuickRedirect)loc
  }
  do
    return;
  while ((!(j.a(this.c))) || (!(this.h.b())));
  try
  {
    long l1;
    ArrayList localArrayList3;
    do
    {
```

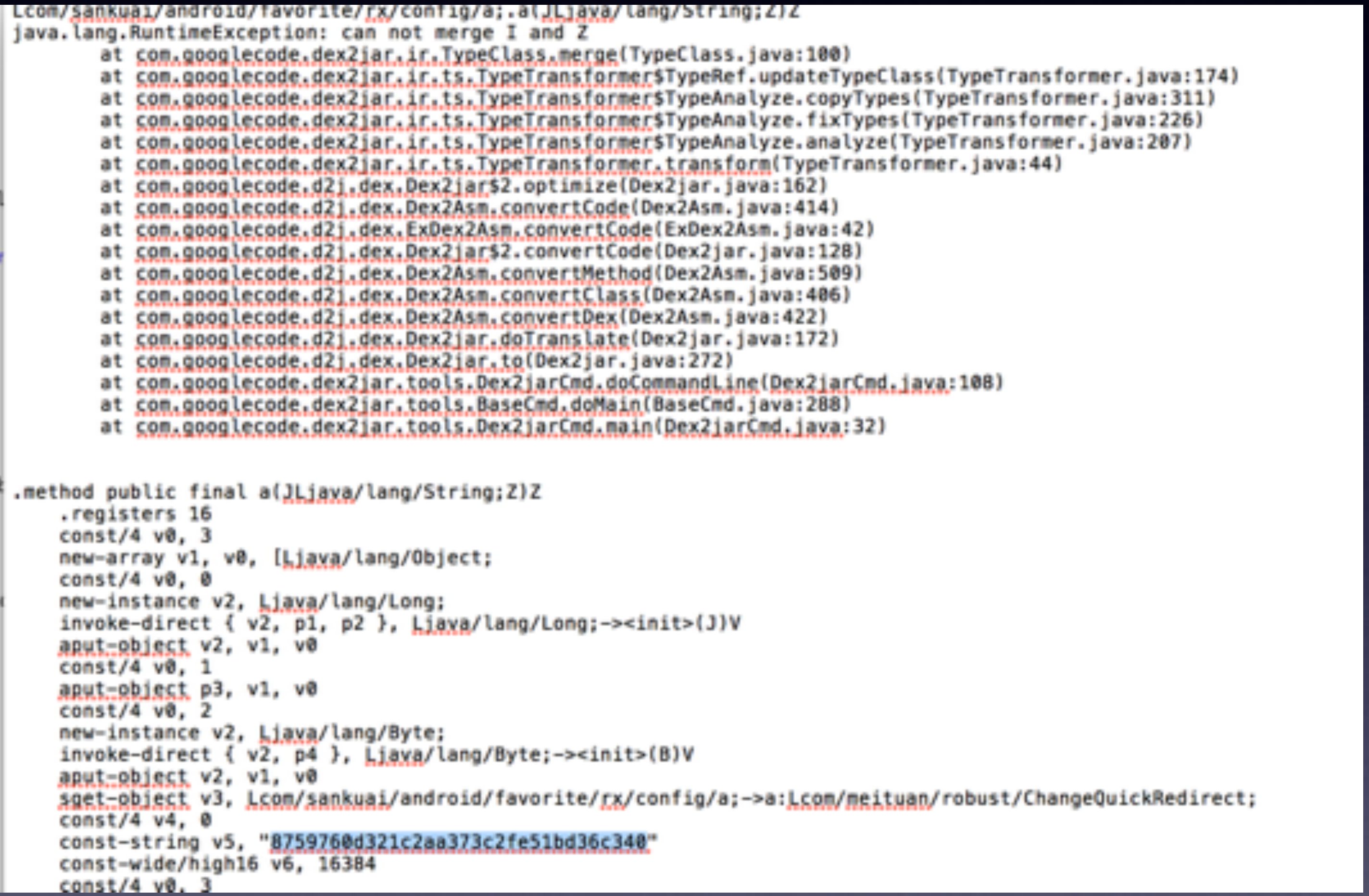


```
Lcom/sankuai/android/favorite/rx/config/a;.a(JLjava/lang/String;Z)Z
java.lang.RuntimeException: can not merge I and Z
        at com.googlecode.dex2jar.ir.TypeClass.merge(TypeClass.java:100)
        at com.googlecode.dex2jar.ir.ts.TypeTransformer$TypeRef.updateTypeClass(TypeTransformer.java:174)
        at com.googlecode.dex2jar.ir.ts.TypeTransformer$TypeAnalyze.copyTypes(TypeTransformer.java:311)
        at com.googlecode.dex2jar.ir.ts.TypeTransformer$TypeAnalyze.fixTypes(TypeTransformer.java:226)
        at com.googlecode.dex2jar.ir.ts.TypeTransformer$TypeAnalyze.analyze(TypeTransformer.java:207)
        at com.googlecode.dex2jar.ir.ts.TypeTransformer.transform(TypeTransformer.java:44)
        at com.googlecode.d2j.dex.Dex2jar$2.optimize(Dex2jar.java:162)
        at com.googlecode.d2j.dex.Dex2Asm.convertCode(Dex2Asm.java:414)
        at com.googlecode.d2j.dex.ExDex2Asm.convertCode(ExDex2Asm.java:42)
        at com.googlecode.d2j.dex.Dex2jar$2.convertCode(Dex2jar.java:128)
        at com.googlecode.d2j.dex.Dex2Asm.convertMethod(Dex2Asm.java:509)
        at com.googlecode.d2j.dex.Dex2Asm.convertClass(Dex2Asm.java:406)
        at com.googlecode.d2j.dex.Dex2Asm.convertDex(Dex2Asm.java:422)
        at com.googlecode.d2j.dex.Dex2jar.doTranslate(Dex2jar.java:172)
        at com.googlecode.d2j.dex.Dex2jar.to(Dex2jar.java:272)
        at com.googlecode.dex2jar.tools.Dex2jarCmd.doCommandLine(Dex2jarCmd.java:108)
        at com.googlecode.dex2jar.tools.BaseCmd.doMain(BaseCmd.java:288)
        at com.googlecode.dex2jar.tools.Dex2jarCmd.main(Dex2jarCmd.java:32)


.method public final a(JLjava/lang/String;Z)Z
    .registers 16
    const/4 v0, 3
    new-array v1, v0, [Ljava/lang/Object;
    const/4 v0, 0
    new-instance v2, Ljava/lang/Long;
    invoke-direct { v2, p1, p2 }, Ljava/lang/Long;-><init>(J)V
    aput-object v2, v1, v0
    const/4 v0, 1
    aput-object p3, v1, v0
    const/4 v0, 2
    new-instance v2, Ljava/lang/Byte;
    invoke-direct { v2, p4 }, Ljava/lang/Byte;-><init>(B)V
    aput-object v2, v1, v0
    sget-object v3, Lcom/sankuai/android/favorite/rx/config/a;->a:Lcom/meituan/robust/ChangeQuickRedirect;
    const/4 v4, 0
    const-string v5, "8759760d321c2aa373c2fe51bd36c340"
    const-wide/high16 v6, 16384
    const/4 v0, 3
```

解决办法



```
  do
    return;
  while (!(this.h.b()));
  b();
}

public final boolean a(long paramLong, String paramString, boolean paramBool
{
  throw new RuntimeException("d2j fail translate: java.lang.RuntimeExceptio
}

@Deprecated
public final void b()
{
  Object localObject1 = a;
  Object localObject2 = Void.TYPE;
  if (PatchProxy.isSupport(new Object[0], this, (ChangeQuickRedirect)localOb
  {
    localObject1 = a;
    localObject2 = Void.TYPE;
    PatchProxy.accessDispatch(new Object[0], this, (ChangeQuickRedirect)loc
  }
  do
    return;
  while ((!(j.a(this.c))) || (!(this.h.b())));
  try
  {
    long l1;
    ArrayList localArrayList3;
    do
    {
```



```
Lcom/sankuai/android/favorite/rx/config/a;.a(JLjava/lang/String;Z)Z
java.lang.RuntimeException: can not merge I and Z
        at com.googlecode.dex2jar.ir.TypeClass.merge(TypeClass.java:100)
        at com.googlecode.dex2jar.ir.ts.TypeTransformer$TypeRef.updateTypeClass(TypeTransformer.java:174)
        at com.googlecode.dex2jar.ir.ts.TypeTransformer$TypeAnalyze.copyTypes(TypeTransformer.java:311)
        at com.googlecode.dex2jar.ir.ts.TypeTransformer$TypeAnalyze.fixTypes(TypeTransformer.java:226)
        at com.googlecode.dex2jar.ir.ts.TypeTransformer$TypeAnalyze.analyze(TypeTransformer.java:207)
        at com.googlecode.dex2jar.ir.ts.TypeTransformer.transform(TypeTransformer.java:44)
        at com.googlecode.d2j.dex.Dex2jar$2.optimize(Dex2jar.java:162)
        at com.googlecode.d2j.dex.Dex2Asm.convertCode(Dex2Asm.java:414)
        at com.googlecode.d2j.dex.ExDex2Asm.convertCode(ExDex2Asm.java:42)
        at com.googlecode.d2j.dex.Dex2jar$2.convertCode(Dex2jar.java:128)
        at com.googlecode.d2j.dex.Dex2Asm.convertMethod(Dex2Asm.java:509)
        at com.googlecode.d2j.dex.Dex2Asm.convertClass(Dex2Asm.java:406)
        at com.googlecode.d2j.dex.Dex2Asm.convertDex(Dex2Asm.java:422)
        at com.googlecode.d2j.dex.Dex2jar.doTranslate(Dex2jar.java:172)
        at com.googlecode.d2j.dex.Dex2jar.to(Dex2jar.java:272)
        at com.googlecode.dex2jar.tools.Dex2jarCmd.doCommandLine(Dex2jarCmd.java:108)
        at com.googlecode.dex2jar.tools.BaseCmd.doMain(BaseCmd.java:288)
        at com.googlecode.dex2jar.tools.Dex2jarCmd.main(Dex2jarCmd.java:32)


.method public final a(JLjava/lang/String;Z)Z
    .registers 16
    const/4 v0, 3
    new-array v1, v0, [Ljava/lang/Object;
    const/4 v0, 0
    new-instance v2, Ljava/lang/Long;
    invoke-direct { v2, p1, p2 }, Ljava/lang/Long;-><init>(J)V
    aput-object v2, v1, v0
    const/4 v0, 1
    aput-object p3, v1, v0
    const/4 v0, 2
    new-instance v2, Ljava/lang/Byte;
    invoke-direct { v2, p4 }, Ljava/lang/Byte;-><init>(B)V
    aput-object v2, v1, v0
    sget-object v3, Lcom/sankuai/android/favorite/rx/config/a;->a:Lcom/meituan/robust/ChangeQuickRedirect;
    const/4 v4, 0
    const-string v5, "8759760d321c2aa373c2fe51bd36c340"
    const-wide/high16 v6, 16384
    const/4 v0, 3
```

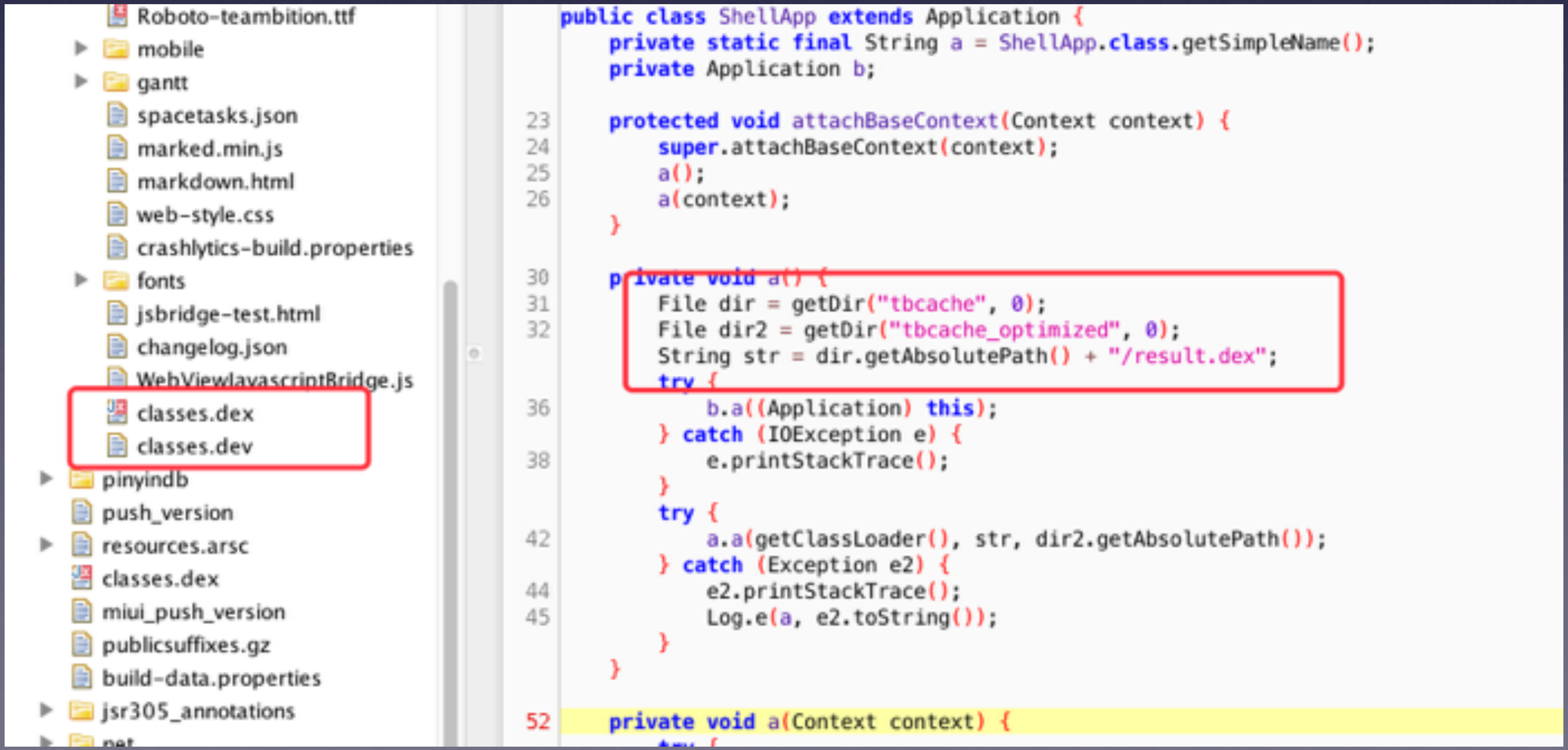
或者花时间研究smail

* https://github.com/Ivonhoe/dexguard

Dex抽取

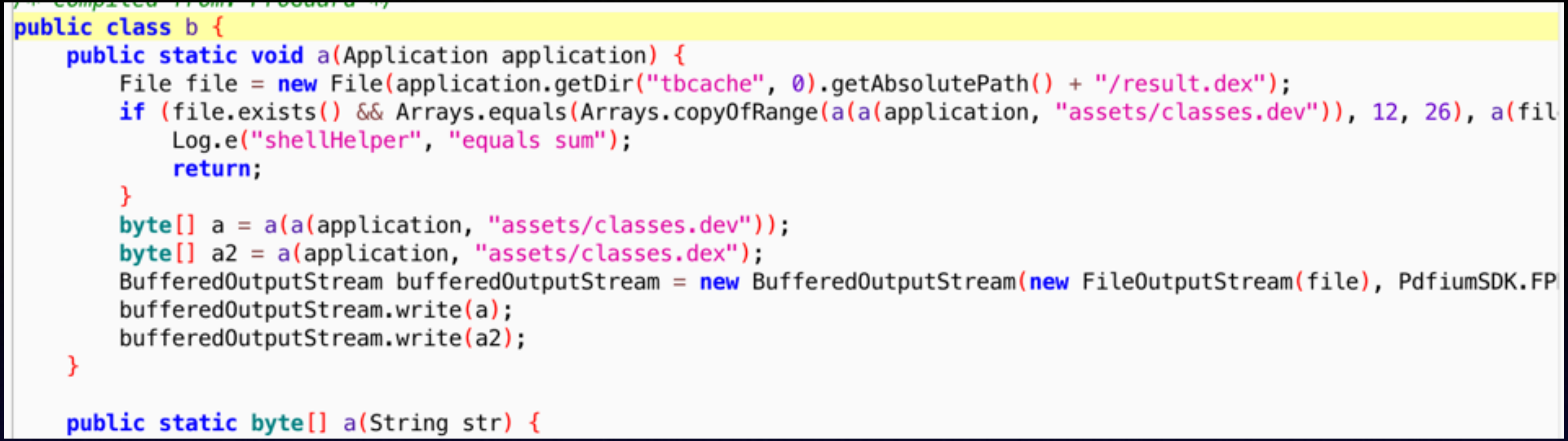
- 将核心逻辑抽取成单独的Dex文件并进行伪装，利用DexClassLoader进行动态加载

- 样本：teambition

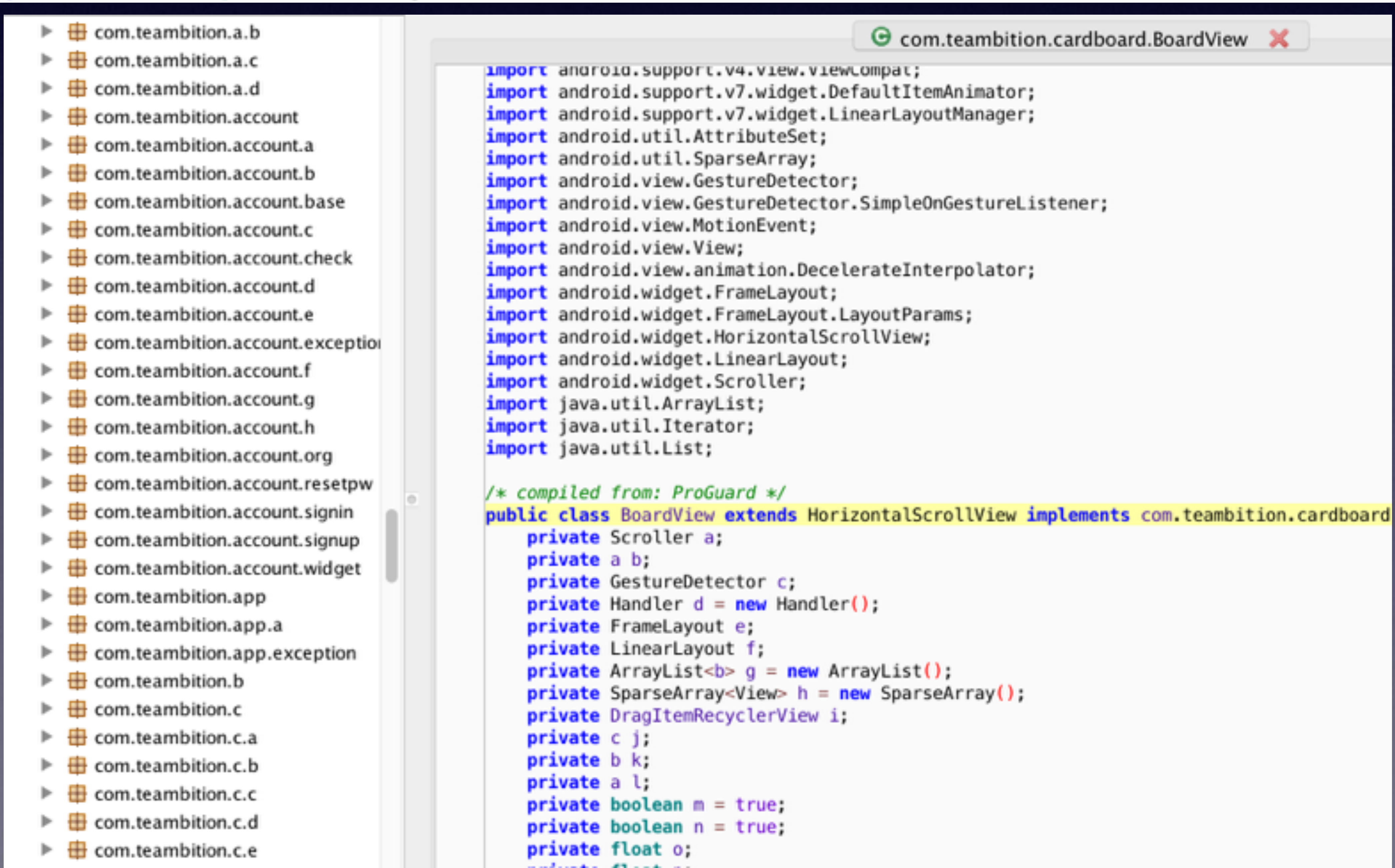


```
    Roboto-teambition.ttf
  ▶ mobile
  ▶ gantt
    spacetasks.json
    marked.min.js
    markdown.html
    web-style.css
    crashlytics-build.properties
  ▶ fonts
    jsbridge-test.html
    changelog.json
    WebViewJavascriptBridge.js
    classes.dex
    classes.dev
▶ pinyindb
  push_version
▶ resources.arsc
  classes.dex
  miui_push_version
  publicsuffixes.gz
  build-data.properties
▶ jsr305_annotations
▶ net
```

```java
public class ShellApp extends Application {
    private static final String a = ShellApp.class.getSimpleName();
    private Application b;

    protected void attachBaseContext(Context context) {
        super.attachBaseContext(context);
        a();
        a(context);
    }

    private void a() {
        File dir = getDir("tbcache", 0);
        File dir2 = getDir("tbcache_optimized", 0);
        String str = dir.getAbsolutePath() + "/result.dex";
        try {
            b.a((Application) this);
        } catch (IOException e) {
            e.printStackTrace();
        }
        try {
            a.a(getClassLoader(), str, dir2.getAbsolutePath());
        } catch (Exception e2) {
            e2.printStackTrace();
            Log.e(a, e2.toString());
        }
    }

    private void a(Context context) {
        try {
```



```java
/* compiled from: ProGuard */
public class b {
    public static void a(Application application) {
        File file = new File(application.getDir("tbcache", 0).getAbsolutePath() + "/result.dex");
        if (file.exists() && Arrays.equals(Arrays.copyOfRange(a(a(application, "assets/classes.dev")), 12, 26), a(fil
            Log.e("shellHelper", "equals sum");
            return;
        }
        byte[] a = a(a(application, "assets/classes.dev"));
        byte[] a2 = a(application, "assets/classes.dex");
        BufferedOutputStream bufferedOutputStream = new BufferedOutputStream(new FileOutputStream(file), PdfiumSDK.FP
        bufferedOutputStream.write(a);
        bufferedOutputStream.write(a2);
    }

    public static byte[] a(String str) {
```

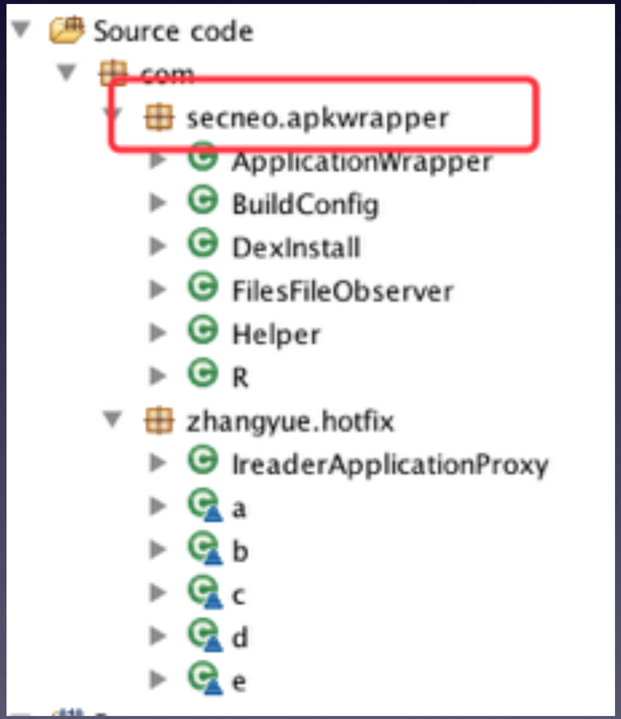


- com.teambition.a.b
- com.teambition.a.c
- com.teambition.a.d
- com.teambition.account
- com.teambition.account.a
- com.teambition.account.b
- com.teambition.account.base
- com.teambition.account.c
- com.teambition.account.check
- com.teambition.account.d
- com.teambition.account.e
- com.teambition.account.exceptio
- com.teambition.account.f
- com.teambition.account.g
- com.teambition.account.h
- com.teambition.account.org
- com.teambition.account.resetpw
- com.teambition.account.signin
- com.teambition.account.signup
- com.teambition.account.widget
- com.teambition.app
- com.teambition.app.a
- com.teambition.app.exception
- com.teambition.b
- com.teambition.c
- com.teambition.c.a
- com.teambition.c.b
- com.teambition.c.c
- com.teambition.c.d
- com.teambition.c.e

```java
import android.support.v4.view.ViewCompat;
import android.support.v7.widget.DefaultItemAnimator;
import android.support.v7.widget.LinearLayoutManager;
import android.util.AttributeSet;
import android.util.SparseArray;
import android.view.GestureDetector;
import android.view.GestureDetector.SimpleOnGestureListener;
import android.view.MotionEvent;
import android.view.View;
import android.view.animation.DecelerateInterpolator;
import android.widget.FrameLayout;
import android.widget.FrameLayout.LayoutParams;
import android.widget.HorizontalScrollView;
import android.widget.LinearLayout;
import android.widget.Scroller;
import java.util.ArrayList;
import java.util.Iterator;
import java.util.List;

/* compiled from: ProGuard */
public class BoardView extends HorizontalScrollView implements com.teambition.cardboard
    private Scroller a;
    private a b;
    private GestureDetector c;
    private Handler d = new Handler();
    private FrameLayout e;
    private LinearLayout f;
    private ArrayList<b> g = new ArrayList();
    private SparseArray<View> h = new SparseArray();
    private DragItemRecyclerView i;
    private c j;
    private b k;
    private a l;
    private boolean m = true;
    private boolean n = true;
    private float o;
```

Dex动态解密

- 运行时动态解密，分段加载，但是并不释放到文件系统中，只加载到进程中，目前一部分加固厂商应该正在使用的方案
- 样本:掌阅ireader 采用梆梆加固VIP版
- 破解方法，内存dump
- https://github.com/bunnyblue/DexExtractor



```
▼ Source code
  ▼ com
    ▼ secneo.apkwrapper
      ▶ ApplicationWrapper
      ▶ BuildConfig
      ▶ DexInstall
      ▶ FilesFileObserver
      ▶ Helper
      ▶ R
    ▼ zhangyue.hotfix
      ▶ IreaderApplicationProxy
      ▶ a
      ▶ b
      ▶ c
      ▶ d
      ▶ e
```

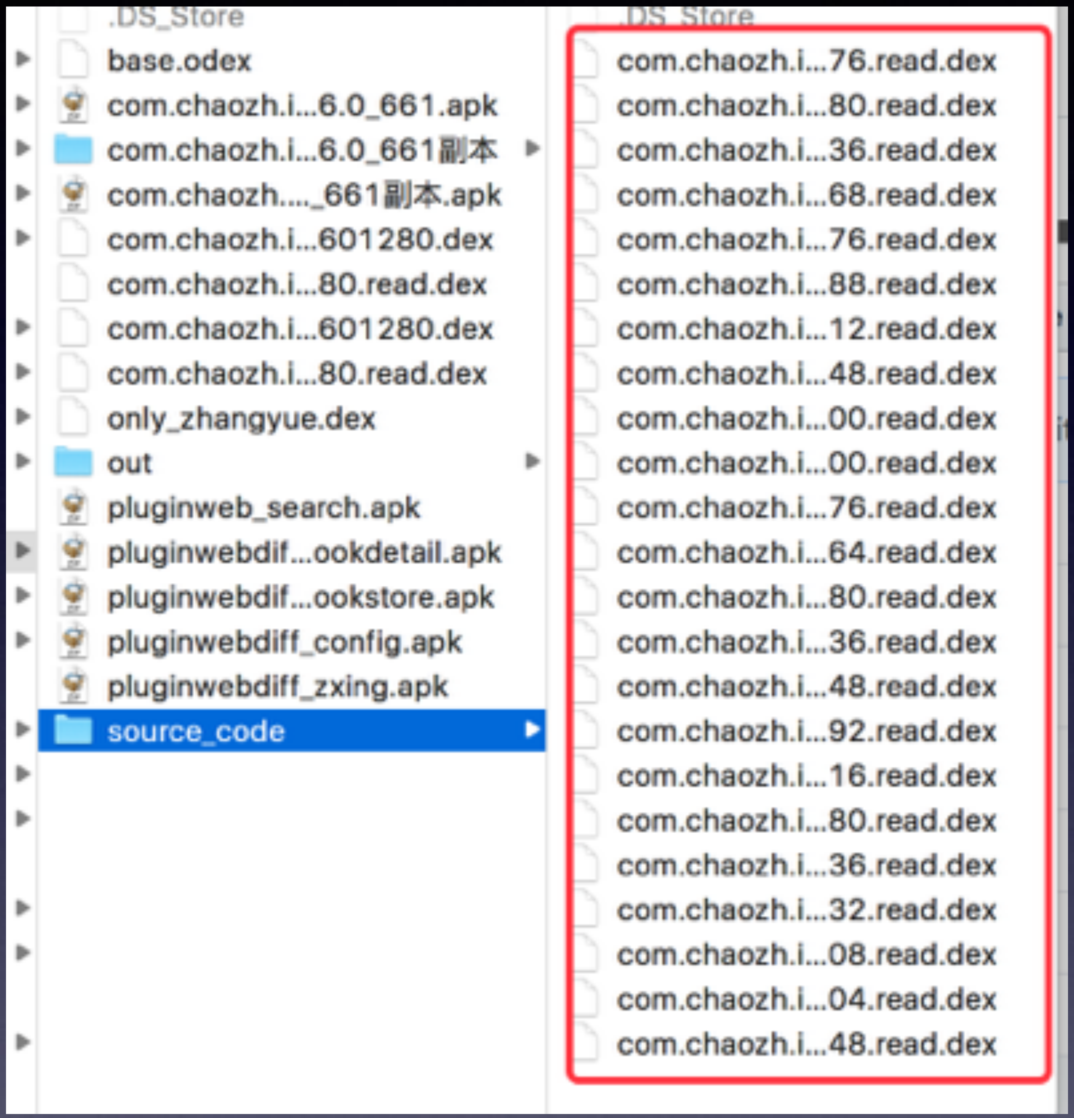
操作步骤

- 已emulator -writable-system -system xxx.img -avd Nexus_5X_API_19 -no-snapshot-load -qemu的方式启动模拟器，下载安装并运行样本，在/sdcard/下面会生成dex后缀的一些文件，比较多

- 导出文件，这些文件都是odex文件，需要转化为smail，利用baksmal，不过过程中会出现找不到xxx.odex的情况，我们把模拟器整个system/framework目录 pull下来，java -jar baksmali-2.2.1.jar deodex ireader/source_code/com.chaozh.iReaderFree_classes_255600.read.dex -d system/framework/

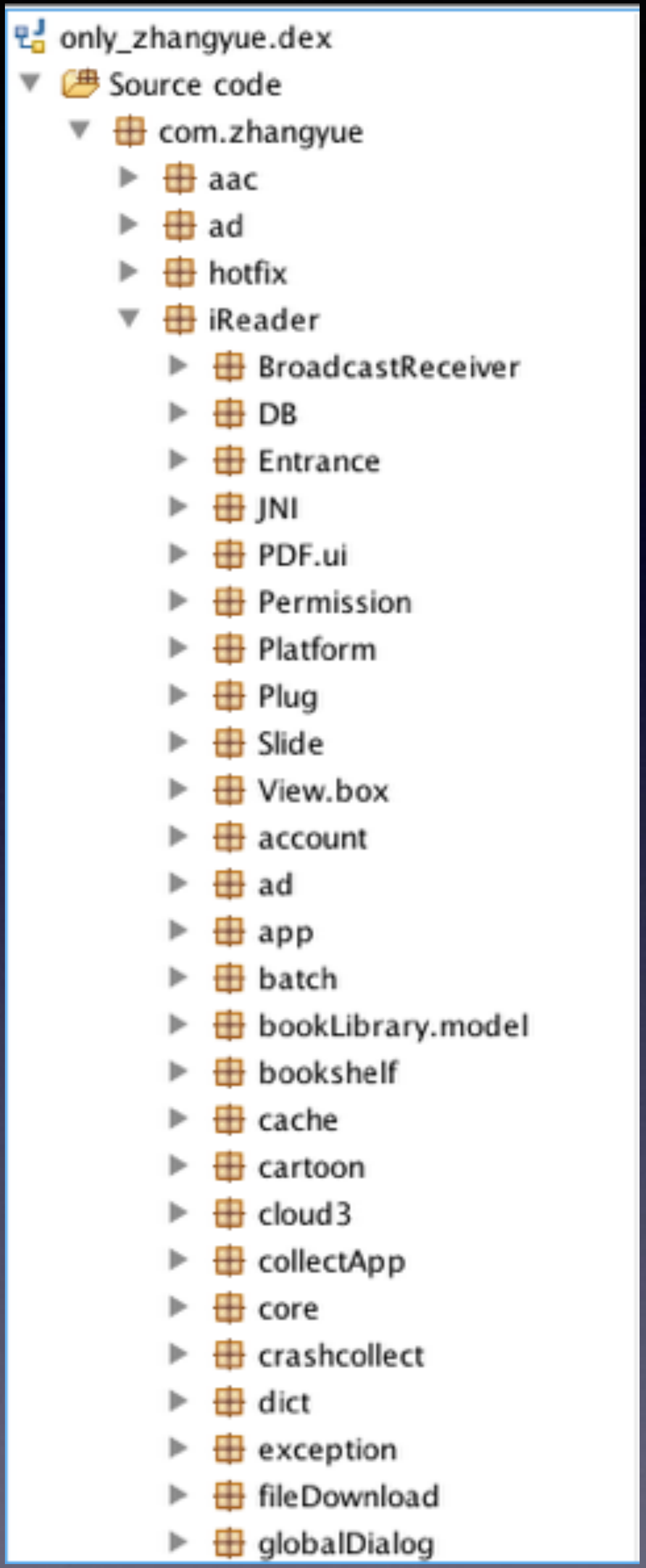
- 经过一系列操作之后，代码就变成smali了。如果觉得看起来不方便，转成jar。转化过程中可能会遇见错误，可以选择单独包转换

- 说明：模拟器要非google apis的，一般不要x86的，如果emmulator有问题，就到sdk/emulator下运行



.DS_Store
base.odex
com.chaozh.i...6.0_661.apk
com.chaozh.i...6.0_661副本
com.chaozh...._661副本.apk
com.chaozh.i...601280.dex
com.chaozh.i...80.read.dex
com.chaozh.i...601280.dex
com.chaozh.i...80.read.dex
only_zhangyue.dex
out
pluginweb_search.apk
pluginwebdif...ookdetail.apk
pluginwebdif...ookstore.apk
pluginwebdiff_config.apk
pluginwebdiff_zxing.apk
source_code

.DS_Store
com.chaozh.i...76.read.dex
com.chaozh.i...80.read.dex
com.chaozh.i...36.read.dex
com.chaozh.i...68.read.dex
com.chaozh.i...76.read.dex
com.chaozh.i...88.read.dex
com.chaozh.i...12.read.dex
com.chaozh.i...48.read.dex
com.chaozh.i...00.read.dex
com.chaozh.i...00.read.dex
com.chaozh.i...76.read.dex
com.chaozh.i...64.read.dex
com.chaozh.i...80.read.dex
com.chaozh.i...36.read.dex
com.chaozh.i...48.read.dex
com.chaozh.i...92.read.dex
com.chaozh.i...16.read.dex
com.chaozh.i...80.read.dex
com.chaozh.i...36.read.dex
com.chaozh.i...32.read.dex
com.chaozh.i...08.read.dex
com.chaozh.i...04.read.dex
com.chaozh.i...48.read.dex



```
only_zhangyue.dex
▼ Source code
  ▼ com.zhangyue
    ▶ aac
    ▶ ad
    ▶ hotfix
    ▼ iReader
      ▶ BroadcastReceiver
      ▶ DB
      ▶ Entrance
      ▶ JNI
      ▶ PDF.ui
      ▶ Permission
      ▶ Platform
      ▶ Plug
      ▶ Slide
      ▶ View.box
      ▶ account
      ▶ ad
      ▶ app
      ▶ batch
      ▶ bookLibrary.model
      ▶ bookshelf
      ▶ cache
      ▶ cartoon
      ▶ cloud3
      ▶ collectApp
      ▶ core
      ▶ crashcollect
      ▶ dict
      ▶ exception
      ▶ fileDownload
      ▶ globalDialog
```

VMP虚拟机加固

- 自定义一套虚拟机指令和对应的解释器，并将标准的指令转换成自己的指令，然后由解释器将自己的指令给对应的解释器。

参考资料

- https://juejin.im/entry/5816e3c3128fe1005592d774