

静态逆向工具

5.1 Apktool 工具

5.1.1 Apktool 基础与用法



Apktool 是最常用的反编译 Apk 文件的工具,它可以将 Apk 包中的 Dex 文件和资源文 一件解码,并在修改后重新构建并打包。在 GitHub 上下载它的源码和发布的版本,网址为 https://github.com/iBotPeaches/Apktool,直接下载 Jar 包。

如图 5.1 所示为 Apktool 的下载页面。

iBotPea	ches / Apktoo	l		⊙ Watch +	614	☆ Star	11.3k	Y Fork	
<> Code	() Issues (48)	I'l Pull request	1) 💿 Actions 🗇 Security 🗠 Insights						
	Releases	Tags							
		Latest release v2.5.0 -o- c83c733 Verified Compare •	Apktool v2.5.0						
			+ Assets (3)						
			P apktool_2.5.0 jar			18	4 MB		
			Source code (zip)						

图 5.1 Apktool 的下载页面

下载完毕后在命令行工具中使用 Java 命令执行,查看它的功能与用法。

\$ java - jar apktool.jar 如图 5.2所示为 Apktool 所使用的参数。 从图 5.2 中可以看到以下参数: usage: apktool - advance, -- advanced prints advance information.

- version, -- version prints the version then exits usage: apktool if install - framework [options] < framework.apk >

nodel@nodel:~/test_exam	ple/tools\$ java -jar apktool.jar
Apktool v2.4.1-dirty -	a tool for reengineering Android apk files
with small v2.3 and bak	smali v2.3
Copyright 2014 Ryszard	Wi獗niewski <brut.alll@gmail.com></brut.alll@gmail.com>
Updated by Connor Tumbl	eson <connor.tumbleson@gmail.com></connor.tumbleson@gmail.com>
usage: apktool	
-advance,advanced	prints advance information.
-version,version	prints the version then exits
usage: apktool if insta	<pre>11-framework [options] <framework.apk></framework.apk></pre>
-p,frame-path <dir></dir>	Stores framework files into <dir>.</dir>
-t,tag <tag></tag>	Tag frameworks using <tag>.</tag>
usage: apktool d[ecode]	[options] <file_apk></file_apk>
-f,force	Force delete destination directory.
-o,output <dir></dir>	The name of folder that gets written. Default is apk.out
-p,frame-path <dir></dir>	Uses framework files located in <dir>.</dir>
-r,no-res	Do not decode resources.
-s,no-src	Do not decode sources.
-t,frame-tag <tag></tag>	Uses framework files tagged by <tag>.</tag>
usage: apktool b[uild]	[options] <app_path></app_path>
-f,force-all	Skip changes detection and build all files.
-o,output <dir></dir>	The name of apk that gets written. Default is dist/name.apk
-p,frame-path <dir></dir>	Uses framework files located in <dir>.</dir>
For additional info. se	e: http://ibotpeaches.github.io/Apktool/
For smali/baksmali info	. see: https://github.com/JesusFreke/smali

图 5.2 Apktool 所使用的参数

```
- p, -- frame - path < dir > Stores framework files into < dir >.
- t, -- tag < tag >
                         Tag frameworks using < tag >.
usage: apktool d[ecode] [options] < file_apk >
-f, -- force
                        Force delete destination directory.
- o, -- output < dir >
                         The name of folder that gets written. Default is apk.out
- p, -- frame - path < dir > Uses framework files located in < dir >.
- r, -- no - res
                        Do not decode resources.
- s, -- no - src
                         Do not decode sources.
-t, -- frame - tag < tag > Uses framework files tagged by < tag >.
usage: apktool b[uild] [options] < app_path >
-f, -- force - all
                         Skip changes detection and build all files.
- o, -- output < dir >
                         The name of apk that gets written. Default is dist/name.apk
- p, -- frame - path < dir > Uses framework files located in < dir >.
```

Apktool 主要有两种用法: 一个是 d 参数,代表解码 Apk 包; 另一个是 b 参数,代表构 建 Apk 包,其中 d 参数下有两个选项需要注意。

- -r,--no-res:这个参数指定了在反编译 Apk 的过程中不去处理包内的资源文件,也就是不解码 resource.arsc 文件和 AndroidManifest.xml 文件。Apktool 在处理某些应用的时候可能会因为资源文件解码错误而导致反编译失败。如果只是对源码进行修改可以绕过资源的反编译,只对 Dex 文件进行反编译处理,在二次打包时Apktool 会将资源文件原封不动地复制回包内。
- -s,--no-src: 这个参数指定了在反编译过程中不去处理包内的源码文件,这样包内的 Dex 文件就不会被反编译成 Smali, 而 AndroidManifest. xml 与 resource. arsc 会 被解码。

这两个参数在实际使用 Apktool 的过程中十分有用。还要注意另一个参数,这个参数 在读 Apktool 源码的时候会看到: --force-manifest,虽然这个参数不在 usage 列表中,但是 可以使用的,这个参数的作用是无论是否处理资源文件都强制将 AndroidManifest. xml 文 件进行解码。

5.1.2 Apktool 源码分析

一般逆向工作中所使用的 Apktool 工具是已经编译好的发布版,但是由于各家的 Apk 包情况不同,部分应用针对 Apktool 工具做了防护,发布版会出现反编译失败的情况。这时 可以根据自己的需要动手修改源码,对 Apktool 工具进行自定义。首先从 GitHub 将项目 下载或者 clone 下来。

如图 5.3 所示为 Apktool 源码目录。

node1@node	1:	~/test	examp	le/tool	ls/A	okto	ool\$ 1:	5 -1
total 92								
drwxrwxr-x	4	node1	node1	4096	Dec	11	17:19	brut.apktool
drwxrwxr-x		node1	node1	4096	Dec	11	17:19	
drwxrwxr-x		node1	node1	4096	Dec	11	17:19	
drwxrwxr-x		node1	node1	4096	Dec	11	17:19	brut.j.util
-rw-rw-r		node1	node1	4418	Dec	11	17:19	build.gradle
-rw-rw-r		node1	node1	513	Dec	11	17:19	CONTRIBUTORS.md
drwxrwxr-x		node1	node1	4096	Dec	11	17:19	gradle
-rwxr-xr-x	1	node1	node1	5960	Dec	11	17:19	gradlew
-rw-rw-r		node1	node1	2942	Dec	11	17:19	gradlew.bat
-rw-rw-r	1	node1	node1	12605	Dec	11	17:19	INTERNAL.md
-rw-rw-r	1	node1	node1	11627	Dec	11	17:19	LICENSE
-rw-rw-r	1	node1	node1	2587	Dec	11	17:19	README.md
-rw-rw-r		node1	node1	2597	Dec	11	17:19	ROADMAP.md
drwxrwxr-x		node1	node1	4096	Dec	11	17:19	
-rw-rw-r		node1	node1	240	Dec	11	17:19	SECURITY.md
-rw-rw-r	1	node1	node1	140	Dec	11	17:19	settings.gradle

图 5.3 Apktool 源码目录

分析 Apktool 源码的出发点在 brut. Apktool 目录。其中的 Apktool-cli 目录下有一个 Main. java 文件,这就是 Apktool 的程序入口。

如图 5.4 所示为 Apktool 的 main()函数。



图 5.4 Apktool 的 main()函数

Main. java 文件负责处理运行程序时输入的参数,并根据参数选择对应的功能。 如图 5.5 所示为 Apktool 处理参数的代码逻辑。

使用 Apktool 时添加参数"-d --decode",程序会调用 cmdDecode 方法进行反编译 Apk 相关操作。在 cmdDecode 方法中会看见一个对象 ApkDecoder,这是 Apktool 负责具体反编译 工作的对象,它的定义在 Apktool/brut. apktool/apktool-lib/src/main/java/brut/ androlib/目录下的 ApkDecoder.java 文件中。接下来继续深入讨论 ApkDecoder 对象。

如图 5.6 所示为 Apktool 项目的 Androidlib 目录。

下面从 ApkDecoder 类的 decode 方法入手分析 Apktool 的反编译功能。

校验 Apk 文件初始化反编译目录:



图 5.5 Apktool 处理参数的代码逻辑





```
if (!mForceDelete && outDir.exists()) {
    throw new OutDirExistsException();
}
if (!mApkFile.isFile() || !mApkFile.canRead()) {
    throw new InFileNotFoundException();
}
try {
    OS.rmdir(outDir);
} catch (BrutException ex) {
    throw new AndrolibException(ex);
}
outDir.mkdirs();
```

上述代码负责判断输入的 Apk 文件是否有错以及初始化反编译目录。如图 5.7 所示 为处理资源文件的代码逻辑。

这段代码先判断 Apk 包中是否有资源文件,也就是 resources. arsc 文件。如果存在,则根据是否使用了参数"-r,--no-res"指定了不解码资源文件,默认是 DECODE_RESOURCES_FULL,也就是解码所有资源文件,如果有 Manifest 文件,则调用 mAndrolib. decodeManifestWithResources()方法解码 AndroidManifest. xml 文件,然后调用 mAndrolib.



图 5.7 处理资源文件的代码逻辑

decodeResourcesFull()方法解码资源文件。如果指定了不解码资源文件,则调用 mAndrolib. decodeResourcesRaw()方法,接着判断是否设置了强制解码 AndroidManifest. xml 文件; 如果设置了强制解码,则调用 mAndrolib. decodeManifestWithResources()方法解码文件。

接下来进入 mAndrolib 对象的类 Androlib, 看看 Apktool 是怎么具体处理资源文件的。 如图 5.8 所示为 Androlib 类的部分逻辑截图。



图 5.8 Androlib 类的部分逻辑截图

首先来看 decodeResourcesRaw()方法。 decodeResourcesRaw()方法:

```
public void decodeResourcesRaw(ExtFile apkFile, File outDir)
      throws AndrolibException {
    try {
```

decodeResourcesFull()方法调用 mAndRes 对象的 decode()方法,对资源文件进行解码:

```
public void decode(ResTable resTable, ExtFile ApkFile, File outDir)
          throws AndrolibException {
   Duo < ResFileDecoder, AXmlResourceParser > duo = getResFileDecoder();
   ResFileDecoder fileDecoder = duo.m1;
   ResAttrDecoder attrDecoder = duo.m2.getAttrDecoder();
   attrDecoder.setCurrentPackage(resTable.listMainPackages().iterator().next());
   Directory inApk, in = null, out;
   try {
      out = new FileDirectory(outDir);
      inApk = ApkFile.getDirectory();
      out = out.createDir("res");
      if (inApk.containsDir("res")) {
         in = inApk.getDir("res");
      }
      if (in == null && inApk.containsDir("r")) {
         in = inApk.getDir("r");
      }
      if (in == null && inApk.containsDir("R")) {
         in = inApk.getDir("R");
      }
   } catch (DirectoryException ex) {
      throw new AndrolibException(ex);
   }
   ExtMXSerializer xmlSerializer = getResXmlSerializer();
   for (ResPackage pkg : resTable.listMainPackages()) {
```

```
attrDecoder.setCurrentPackage(pkg);
      LOGGER. info("Decoding file - resources...");
      for (ResResource res : pkg.listFiles()) {
          fileDecoder.decode(res, in, out);
      }
      LOGGER. info("Decoding values * / * XMLs...");
      for (ResValuesFile valuesFile : pkg.listValuesFiles()) {
          generateValuesFile(valuesFile, out, xmlSerializer);
      }
      generatePublicXml(pkg, out, xmlSerializer);
   }
   AndrolibException decodeError = duo.m2.getFirstError();
   if (decodeError != null) {
      throw decodeError;
   }
}
```

接着来分析负责处理 AndroidManifest. xml 文件的方法 mAndRes. decodeManifest-WithResources():

public void decodeManifestWithResources(ExtFile apkFile, File outDir, ResTable resTable)
 throws AndrolibException {
 mAndRes.decodeManifestWithResources(resTable, apkFile, outDir);
 }
}

decodeManifestWithResources()同样调用了 mAndRes 对象中的同名方法,来解析 AndroidManifest.xml:

```
public void decodeManifestWithResources(ResTable resTable, ExtFile apkFile, File outDir)
         throws AndrolibException {
   Duo < ResFileDecoder, AXmlResourceParser > duo = getResFileDecoder();
   ResFileDecoder fileDecoder = duo.m1;
   ResAttrDecoder attrDecoder = duo.m2.getAttrDecoder();
   attrDecoder.setCurrentPackage(resTable.listMainPackages().iterator().next());
   Directory inApk, in = null, out;
   try {
      inApk = apkFile.getDirectory();
      out = new FileDirectory(outDir);
      LOGGER. info("Decoding AndroidManifest.xml with resources...");
      fileDecoder.decodeManifest(inApk, "AndroidManifest.xml", out, "AndroidManifest.xml");
      if (!resTable.getAnalysisMode()) {
          adjustPackageManifest (resTable, outDir.getAbsolutePath() + File.separator +
"AndroidManifest.xml");
         ResXmlPatcher.removeManifestVersions(new File(
                outDir.getAbsolutePath() + File.separator + "AndroidManifest.xml"));
```

```
mPackageId = String.valueOf(resTable.getPackageId());
}
catch (DirectoryException ex) {
   throw new AndrolibException(ex);
}
```

如果 Apk 中不存在 resources. arsc 文件,则不参照属性的引用对 AndroidManifest 文件解码:

资源文件处理完毕后再处理源码文件。一个 Apk 中可能有多个 Dex 文件,所以 decode() 方法先处理第一个 Dex 文件 classes. dex,然后再根据是否存在其他的 Dex 文件进行下 一步。

如图 5.9 所示为 Apktool 判断是否存在其他 Dex 文件的代码。



```
图 5.9 判断是否存在其他 Dex 文件
```

针对每个 Dex 文件检查传入的参数,如果参数指定了不处理 Dex 文件,则调用 decodeSourcesRaw()方法,直接将 Dex 文件复制到目标目录下。

如果是默认情况,也就是需要解码 Dex 文件,则会调用 decodeSourcesSmali()方法:

```
public void decodeSourcesSmali(File apkFile, File outDir, String filename, boolean bakdeb, int
api)
          throws AndrolibException {
   try {
      File smaliDir;
      if (filename.equalsIgnoreCase("classes.dex")) {
          smaliDir = new File(outDir, SMALI DIRNAME);
      } else {
          smaliDir = new File(outDir, SMALI DIRNAME + " " + filename.substring(0, filename.
indexOf(".")));
      }
      OS.rmdir(smaliDir);
      smaliDir.mkdirs();
      LOGGER.info("Baksmaling " + filename + "...");
      SmaliDecoder.decode(apkFile, smaliDir, filename, bakdeb, api);
   } catch (BrutException ex) {
      throw new AndrolibException(ex);
   }
}
```

decodeSourcesSmali()方法调用 Baksmali 组件将 Dex 文件反编译成 Smali 文件。

5.2 JEB 工具

JEB 是一款强大的跨平台的 Android 静态分析工具,提供了类似于 IDA Pro 的方法交 叉引用与重命名功能,同时提供脚本化功能,用于自动化分析和对抗代码混淆。

5.2.1 JEB 安装

从 JEB 官网 https://www.pnfsoftware.com/jeb/下载软件包并解压。如图 5.10 所示 为 JEB 程序目录。

JEB 的运行需要依赖 JDK8 或以上的 JDK 环境。提前下载安装 JDK 并设置系统变量 JAVA_HOME。JEB 提供了可在 Windows、Linux、macOS 上运行的 UI 客户端,在相应的

bin	2021/1/28 14:54	文件夹	
coreplugins	2019/3/19 15:39	文件夹	
doc	2019/3/19 15:39	文件夹	
scripts	2019/3/19 15:39	文件夹	
siglibs	2019/3/19 15:39	文件夹	
typelibs	2019/3/19 15:39	文件夹	
jeb_linux.sh	2019/1/19 1:01	SH 文件	2 KB
jeb_macos.sh	2019/1/19 1:01	SH 文件	2 KB
jeb_wincon.bat	2019/1/19 1:01	Windows 批处理	2 KB
nfo_viewer.exe	2019/3/19 14:44	应用程序	209 KB
🛛 roentgen.nfo	2019/3/19 16:00	系统信息文件	5 KB
音爱破解论坛	2016/2/22 11:54	Internet 快捷方式	1 KB

图 5.10 JEB 程序目录

系统执行对应文件: Windows 执行 jeb_wincon. bat; Linux 执行 jeb_linux. sh; macOS 执行 jeb_macos. sh。

如图 5.11 所示为 JEB 运行起来的效果。

dia Ca		- 0
※アジロ 日建せる 4000000000000000000000000000000000000		
Bi Ferminal		
	20 18 (2 Tenine)	

图 5.11 JEB 运行起来的效果

5.2.2 JEB 静态分析

接下来通过使用 JEB 分析一个应用来熟悉它的用法。本书将从 JEB 官网 https://www.pnfsoftware.com/jeb/manual/下载官方实例应用 Raasta. Apk 作为此章节的测试应用。

如图 5.12 所示为下载 Raasta. Apk 的页面。

从文件菜单中打开 Raasta. Apk 文件, JEB 会使用这个 Apk 文件创建一个新的项目,并 通过以下几个 Android 分析组件去处理它:

- Apk 组件负责拆解应用文件,解码它的 AndroidManifest 文件和资源文件。
- Dex 组件负责解析应用包中的 Dex 字节码文件。
- Xml 组件负责处理 Android 应用资源目录下的 XML 资源文件。

IEB Decompiler Setting Started		Auto-rename AL. ~*N Other action groups such as Native	code actions and Debugging actions are detailed in	Table of contents Decompiling
Ising JEB Workspace	~	separate sections of this manual.		Graphing Renaming
Common Actions		A Warning	单击此处下载测试程序	Commenting
Common Views Decompiling Debugging		The examples in this section are based on the in mind that features and behaviors of Action	e analysis of a sample Android applusing the Android DEX parser. Keep ns depend on the module implementing and performing them.	Navigating Cross-references Type Hierarchies
Android Analysis Android Debugging Native Code Analysis		Decompiling		Restructuring Type Hierarchies Object Overrides
WebAssembly Analysis Ethereum Analysis Miscellaneous		The next section covers decompiling	code in depth.	Rebasing Constants Auto-Rename All
xtending JEB	>	Graphing		
Configuration AQ Fips	>	Users can alternate between the defa control flow graph of the currently exa	ult interactive full disassembly view and the interactive amined method/routine.	
		Press the Space key to go back and for navigation.	orth. In some circumstances, users may prefer graph	

• 签名组件负责分析应用的签名。

打开项目后,左侧的项目浏览树会展示 Apk 包内的各类文件和目录,左侧下方的 Bytecode 结构树会显示 Dex 字节码反编译出来的源码项目结构。主要的 Dex 窗口是在项 目分析完毕后自动打开的,展示 Dex 文件反编译出来的 Smali 语句。

如图 5.13 所示为 JEB 的主界面截图。

1 IGNER	tytecole;@tassambly
	folkik Disawambiy (de classes, 301 methods, 351 fields) # Ratage com_pforthwree.reasts # Application: andresis.app.Application # (d activities, 0 envice, 0 provider, 0 encolver) # Naim Activity; com_pforthwre.reasts.Reasts (Reasts) # Disamperous Permissions: LOATION, STORAGE .class public AppHelp .wwper Activity
1218日: 私入"Enter" 余時以	.registers 1
Bytecode/BR 11	0000000 invokedirect Activity->Cinit>()V, p0 0000000 invokedirect Activity->Cinit>()V, p0
 Continues Continue	ethod public outcreate(fourlin)' registers 0 00000000 invoke-super Activity-conCreate(fourlin)', p0, p1 00000000 cont/A 4, 1 00000000 cont/Aiphid 4, 0.77930000 00000011 cont/Aiphid 4, 0.77930000 00000011 cont/Aiphid 4, 0.77930000 00000012 cont/Aiphid 4, 0.77930000 00000014 cont/Aiphid 4, 0.77930000 00000014 cont/Aiphid 4, 0.7793000 00000014 cont/Aiphid 4, 0.7793000 00000014 cont/Aiphid 4, 0.74740 00000014 cont/Aiphid 4, 0.74740 00000014 cont/Aiphid 4, 0.74740 00000014 cont/Aiphid 4, 0.74740 00000014 cont/Aiphid 4, 0.74740 00000015 cont-string 4, 0.74740 00000014 cont/Aiphid 4, 0.74740 00000014 cont/Aiphid 4, 0.74740 00000015 cont-string 4, 0.74740 00000014 cont/Aiphid 4, 0.74740 00000015 cont-string 4, 0.74740 00000014 cont/Aiphid 4, 0.74740 00000014 cont-string 4, 0.74740
	RE + 十元世紀代 Disassently Graph 年日巻
[2]集團: 編入"Enter" 用碘认	

图 5.13 JEB 的主界面截图

接下来介绍 JEB 在进行静态分析时的常用功能。

1. 反编译功能

在主界面的 Dex 字节码窗口,滚动到需要反编译的部分区域,按 Tab 键就可以将 Smali 源码反编译成 Java 源码。这时会打开另一个窗口,里面是选择区域所属的 Java 类的 Java 源码。

如图 5.14 所示为 JEB 反编译应用的效果。



图 5.14 JEB 反编译应用的效果

在 Java 源码界面再按 Tab 键就会回到对应的 Smali 语句。

2. 重命名

静态分析时,可能会遇到代码被混淆的情况,多个方法名和变量被转化成类似于 a()、 ab()之类毫无意义的形式。为了应对这种情况,一个比较重要的需求是可以对代码中的各 项,比如类型、方法、例程、类变量、数据项或者包名进行重命名。JEB 提供了这一功能。

定位并单击需要重命名的项目。

• 按 N 键或者选择 Action 栏中的 Rename 选项。

• 输入新的名称。

如图 5.15 所示为 JEB 对反编译代码的项目进行重命名操作。

在"重命名"窗口中按 Ctrl+空格键可以查看之前的重命名历史记录。

3. 添加注释

在代码中的任意位置,按"/"键打开添加注释界面,输入注释内容。注释会附加在所选 择的语句的后面。

如图 5.16 所示为 JEB 为代码添加注释。

4. 导航

在做静态分析时经常需要去找某个调用方法或结构体的定义。在 JEB 中,单击选中项 目并按回车键或者在项目上双击,就会跳转到显示该项定义的窗口。可以使用快捷键"Alt+ 左箭头"或"Alt+右箭头"进行向前或者向后导航。



图 5.15 JEB 对反编译代码的项目进行重命名操作

<pre>import org.apache.http.protocol.BasicHttpContext;</pre>	
import org.apache.http.protocol.HttpContext;	
import org.json.jsonuoject;	
import org.json.jsuniokener;	
<pre>public class Reasta extends MapActivity implements LocationListener {</pre>	
private static final int DLGID_CONFIRM_EXIT = 4;	
private static final int DLGID_CUSTOMPERIOD = 8;	
private static final int DLGID_INFO = 0;	
private static final int DLGID_INFO_START_REC = 3;	
private static final int DLGID_NEWTRACE = 6;	
private static final int DLGID_SELECTMODE = 7;	
private static final int DLGID_SPLASH = 2;	
private static final int DLGID_NELCOME = 5;	
private static final int REQCODE_ENABLE_GPS = 1;	
private static final int STATE FOLLOWING = 2:	
private static final int : M EM	x
private static time: int i	
private static tinal int communication of the static transformer and the static time of t	
private static tinal int i add new comment	
private static tinal int i	
public static tinal books	
private butten bin sector	
netwate Button new hte nel 3400 Prix	
private Interview http://www.automatical.	
private InageView http://www.seconder	
private ProgressDialog dia Locatina:	
private ViewGroup frameview:	
private GosManager gosmon:	
private Menu hOptionsMenu:	
private SimpleLocation LastLoc:	
<pre>private String LastTraceFileName;</pre>	
private String m aboutbox extramsg;	
private Context m context;	
<pre>private String m_splash_message;</pre>	
private String m_splash_title;	
private MapViewEx mapview;	
private MenuItem_mockgps;	
private int nextstate;	
private PathView pathview;	
private int state;	
private GeoTrace trace;	



如图 5.17 所示为选择 set_lastSplashSequence()函数调用。

```
Prefs.set_lastSplashSequence(((Context)this), v4);
this.m_splash_title = v2.optString("cap");
this.m_splash_message = v2.optString("msg");
if(this.m_splash_title.length() <= 0) {
    return true;
    }
图 5.17 选择 set_lastSplashSequence()函数调用</pre>
```

如图 5.18 所示为 JEB 跳转到 set_lastSplashSequence()函数的定义。

```
public static void set_lastSplashSequence(Context arg4, int arg5) {
    SharedPreferences$Editor v0 = arg4.getSharedPreferences("global", 0).edit();
    v0.putInt("splashSeq", arg5);
    v0.commit();
}
```

图 5.18 JEB 跳转到 set_lastSplashSequence()函数的定义

5. 交叉引用

除了查看某个引用项的定义,有时逆向人员还需要查看某个引用项在整个项目中的引 用情况。在 JEB 中选择某项,按X 键打开交叉引用窗口,双击窗口中的项目跳转到引用点。 如图 5.19 所示为查看函数的交叉引用。

white double of the			
ublic double dct;			
ublic double ing:			
ublic long timestampMs;			
ublic SimpleLocation(double arg1, double arg3,	double arg5, long arg7) {		
<pre>super(); this.ing = arg1;</pre>	影 女双词		×
this.dt = args; this.dt = arg5;	[过读器] 输入"Enter" 未确认		
<pre>this.timestampMs = arg7;</pre>	Index 地址	板盤 注释	•
	0 Lcom/pnfsoftware/raasta/MapViewEx:->set_current_location(Lcom/pnfsoftware/raasta/SimpleLocation(V+0h		
ublic SimpleLocation(SimpleLocation arg3) {	1 Lcom/pnfsoftware/raasta/MockLocationGenerator;->generate_next_locationQLcom/pnfsoftware/raasta/SimpleLocation;+80h		
super();	2 Lcom/pnfsoftware/raasta/PathViewc->set_current_location(Lcom/pnfsoftware/raasta/SimpleLocation()V+0h		
this.lng = arg3.lng;	3 Lcom/pnfsoftware/raasta/Prefs:->get_lastLocation(Landroid/content/Context;)Lcom/pnfsoftware/raasta/SimpleLocation;+44h		
this.lot = arg3.lot;	4 Lcom/pnfsoftware/raasta/Raasta;->onLocationChanged(Landroid/location/Location()V+20h		
this.alt = arg3.alt;	5 Lcom/pnfsoftware/raasta/Prefs:>set_lastLocation[Landroid/content/ContextLcom/pnfsoftware/raasta/SimpleLocation;V+3Ah		
<pre>this.timestampMs = arg3.timestampMs;</pre>	6 Lcom/pnfsoftware/raasta/SimpleLocationc-> <init>(DDDJ)V+Eh</init>		
	7 Lcom/pnfsoftware/raasta/SimpleLocation-> <init>(Lcom/pnfsoftware/raasta/SimpleLocation;)V+16h</init>		
	8 Lcom/pnfsoftware/raasta/SimpleLocation:-> <init>(Lcom/pnfsoftware/raasta/SimpleLocation/)V+1Ah</init>		
	9 Lcom/pnfsoftware/raasta/PathOverlay:->draw(Landroid/graphics/Canvas;Lcom/google/android/maps/MapView;ZJV+18Eh		81
	10 Lcom/prfsoftware/raasta/PathView:->onDraw(Landroid/graphics/Canvas:/V+7C4h		
	Lcom/pr/software/zasta/Pa0Wew;->onDraw[Landroid/graphics/Canvas;V+81Eh Lcom/pn/software/zasta/Prefs->set lastLocation(Landroid/content/Content/Londroid/ware/zasta/SimpleLocation/V+2Ah		
	13 Lcom/pnfsoftware/raasta/SimpleLocation-> <init>(DDD/IV+Ah</init>		
	14 Loom/onfootbuare/caasta/SimpleLocation-> cinits/iLcom/onfootbuare/caasta/SimpleLocation/IV+Eh		
	15 Lcom/pnfsoftware/raasta/SimpleLocation-> sinit>(Lcom/pnfsoftware/raasta/SimpleLocation/IV+12h		
	16 Lcom/pnfsoftware/raasta/PathOverlay:->draw(Landroid/graphics/Canvas:Lcom/google/android/maps/MapViewZ)V+1A4h		
	17 Lcom/onfsoftware/raasta/PathView: + onDraw(Landroid/graphics/Canvas:W+79Ah		
	18 Lcom/pnfsoftware/raasta/PathViewc->onDraw(Landroid/graphics/Canvac/V+80Ah		
	Commentational Commentations of Commenta		

图 5.19 查看函数的交叉引用

6. 重构

JEB 提供了强大的重构能力,允许使用者在项目中创建新的包并把某个包内的类移动 到新的或者是已存在的其他包中。

作为示范,此处将使用这个功能创建一个新包 com. newPack,然后将 com. pnfsoftware. raasta 包内的 AppHelp 类移动到新包 com. newPack 中。首先按 K 键新建一个包 com. newPack。 如图 5.20 所示为在 JEB 中新建一个包。

✓ 曲 com	■ 新建包	×
✓ ⊕ pnfsoftware → ⊕ raasta	输入一个简单的或完全合乎规范的,以点分割的包名称 名: ^{□[} com.newPack]	
	(Alt Control+space to provise your input history) 通定 取消	

图 5.20 在 JEB 中新建一个包

然后按L键将AppHelp类移动到 com. newPack 包中。 如图 5.21 所示为在 JEB 中移动类。

✓	■ 移动到包 ×
 	输入一个简单的或完全合乎规范的,以点分割的包名称 名: ¹⁰ com.newPack
 G AppHelp G CoordinatesE6 	(Hit Control+Space to browse your input history)
 G GeoTrace G GpsManager 	确 定 取消
>	

图 5.21 在 JEB 中移动类

7. 修改常量

这个功能允许选择整数常量以哪种进制形式显示。选择常量后,按B键循环选择插件 提供的进制。通常插件提供八进制、十进制、十六进制方式,其他的插件可能会额外提供二 进制方式,或者是非常规的显示方式,比如基于字符。

如图 5.22 所示为以十进制显示选中的整数常量。



图 5.22 以十进制显示选中的整数常量

如图 5.23 所示为以八进制显示选中的整数常量。

```
if(arg6 > 0) {
    int v0 = Prefs.get_traceGpsPeriod(((Context)this), this.lastTraceFileName);
    if(v0 <= 0) {
        v0 = Prefs.get_GpsPeriod(((Context)this));
    }
    this.gpsman.request_updates(((long)(v0 * 01750)), 0f);
}</pre>
```

图 5.23 以八进制显示选中的整数常量

如图 5.24 所示为以十六进制显示选中的整数常量。

```
if(arg6 > 0) {
    int v0 = Prefs.get_traceGpsPeriod(((Context)this), this.lastTraceFileName);
    if(v0 <= 0) {
        v0 = Prefs.get_GpsPeriod(((Context)this));
    }
    this.gpsman.request_updates(((long)(v0 * 0x\betaE8)), 0f);
}</pre>
```

图 5.24 以十六进制显示选中的整数常量



视频 9

5.3 Jadx-gui 工具

Jadx 是一个将 Dex 字节码文件反编译成 Java 的开源工具,作者同时提供了 UI 客户端 方便进行动态调试。Github 地址为 https://github.com/skylot/jadx。下载 Jar 包到本地 后运行 Java 命令启动:

java – jarjadx – gui.jar

如图 5.25 所示为 Jadx-gui 的启动界面。



图 5.25 Jadx-gui 的启动界面

Jadx-gui 的主要特性是:

- 处理 Apk、Dex、Aar 和 Zip 文件,将其中的 Dalvik 字节码反编译成 Java 类。
- 反编译 Android Manifest. xml 和解码其他的资源文件和 resources. arsc 文件。
- 添加了反混淆功能。
- 使用高亮语法显示反编译出来的代码。

如图 5.26 所示为 Jadx-gui 反编译代码的截图。

U OLGID CONFIRM FRIT 1	│ @ com.pnfsoftware.rassta.Xaasta Ж	
V DIGTO CUSTOMPERTOD 1	import java.io.TOExceptine;	
- V DIGIO INFO int	import java.in.Inputitraninaler;	
W DIGTO INFO START REC	import java.text.Dateformat;	
W DEGTO NEWTRACE SOT	Import jere avtil offer diant discussion in the second sec	
NUMERO SELECTIONE LAS	import organization bits of last astherestication;	
N PRETO SPLITCH LAR	insert org. southe http://alignt.forfaulthtofilent:	
N DOCTO WELCOME And	leport org.apache.http.protocol.fmsiOntpContext;	
H REACONS SHARES FOR A	import org.json.JSONObject;	
- 6 VEGCODE ENVILLE BAR	import org.joon.350HTokener;	
U STATE_POLLOWING INC		
- W STATE_IDLE int	118 public class Reasts extends PapActivity implements locationListener (
"" STATE_LOCATING int	private static final int D.63D_COMPTMP_TAIT = 4;	
-W STATE_MARKING int	private static final int court (as the state of the state	
-W STATE_NO_TRACE int	while the statis final int putty into the state at a	
-W STATE_RECORDING int	private static final int DuGD MR/RACE = 6:	
-W bDebugMode boolean	private static final int DLGED_SELECTHODE = 71	
bMockLocations boole	private static final int CLG2D_SPLASM + 21	
. btn.newtrace Button	private static final int DiSID_MELCOME + 51	
. hts record Button	private static final int ROCCOU_DIMAGIE_GPS = 1;	
. hts selectmode Image	private static final int STATE FOLLOWING = 2;	
, hts suitchulamode ?	private static final int StATE 10(1 = 0)	
dia location Poneres	private static final int Sixte Location = 4; actuate static final int Sixte Location = 5;	
a dig_tocating Progres	private static final int Sint (would - 3) entropy a static final int Sint Sint Sint (1997)	
a maneview without only	private static final int STATE BECORDING = 1	
a granan opsnanager	public static final boolean bOchugHode - false;	
- = hUptionshenu Henu	private boulsess brocklocations - false;	
= lastLoc SimpleLocati	private Button bts_newtrace = mull;	
= lastTraceFileName St	private Button bts_record = mull;	
- = m_aboutbox_extramsg	private Inagrview bts_selecteode = muli	
- = m_context Context	private inspector and private really	
- = m_splash_message Str	private representation and the second state of the	
- = =_splash_title Strin	private Galvanaper science + multi	
 mapview MagViewEx 	private tenu Noptionstenu - mulli	
- menuitem mockgos Men	private Simpleicostion lasticc + null;	
· nextstate int	private String lastTracefileHame = mull;	
- nathview Pathview	private String m_aboutbox_extransg + "";	
. state int	private Context = context = multi	
. trace GeoTrace	private scring a plant title = ***	
- view PathViewInterfa	private fasting any is a sulli	
- results manufaul) Man	private Newsites sensites suckeys - mall;	
- souble soufiet1 hool	private int newtytate - STATE NO TRACE;	
a interation isstand	private Pathview pathview - mill;	
<pre>stocecionDisplayed(</pre>	private int state - STATE_NO_TRACE;	
<pre>shouteursplayed() b</pre>	private Geofrace trace + mall;	
<pre># load_trace() void</pre>	private PathViewInterface view + null;	
a onActivityResult(int	2 THE REP. Bill contains much solution for attain social print of the state	
a onBackPressed() vold	7. Some manual constructions assess region on processing processing spectral states and programming the source of the state of the s	
e onCreate(Bundle) voi	/* 340Y MANY full(-seriable tops inference failed */	
 o onCreateOialog(int) 	/* 342K wath: Type inference failed for: rSv0, types: [com.onfseftware.rassta.Regviewte, android.view.View] %/	
a onCreateOptionsPenul	1 Statistics of the Astronomy Astronomy Astronomy and Astronomy and a statistics of the Astronomy Astronomy and the Astronomy As Astronomy Astronomy Astr	

图 5.26 Jadx-gui 反编译代码的截图

• 跳转到项目的定义。

在类、方法和类变量项目上按 Ctrl+鼠标左键跳转到该项目的定义。如图 5.27 所示为选择 set lastTraceFileName()函数。

```
public void onClick(DialogInterface dlg, int id) {
    String name = e.getText().toString();
    String filename = GeoTrace.generate_timebased_filename();
    GeoTrace t = new GeoTrace(Raasta.this.m_context, filename, true);
    t.set_name(name);
    t.save();
    Prefs.set_lastTraceFileName(Raasta.this.m_context, filename);
    Prefs.set_traceGpsPeriod(Raasta.this.m_context, filename, Prefs.get_GpsPeriod(Raasta.this.m_context));
    Raasta.this.btn_newtrace.setVisibility(Raasta.DLGID_CUSTOMPERIOD);
    Raasta.this.enable_gps(0);
    Raasta.this.load_trace();
}
```

图 5.27 选择 set_lastTraceFileName()函数

如图 5.28 所示为跳转到 set_lastTraceFileName()函数的定义。

```
public static void set_lastTraceFileName(Context context, String s) {
    SharedPreferences.Editor ed = context.getSharedPreferences("global", 0).edit();
    ed.putString("lastTraceFileName", s);
    ed.commit();
}
```

图 5.28 跳转到 set_lastTraceFileName()函数的定义

在 AndroidManifest. xml 中可以直接跳转到类的定义,如图 5.29 所示为在 AndroidManifest. xml 中找到 TraceList 类。

图 5.29 在 Android Manifest. xml 中找到 TraceList 类

如图 5.30 所示为从 AndroidManifest 中跳转到 TraceList 类。

<pre>import android.app.Activity; import android.app.BistActivity; import android.app.IistActivity; import android.app.IistActivity; import android.app.IistActivity; import android.app.ListActivity; import android.content.Context; import android.content.Intent; import android.content; private static final int DIGD_REMUME = 4:00; private static final int D_GODS_EPENTE = 0:00; private static final int D_GODS_EPE</pre>		package com.pnfsoftware.raasta;
<pre>import android.app.LiterSyj, import android.app.LiterSyj, import android.app.LiterSyj, import android.app.LiterStatUity; import android.app.LiterStatUity; import android.content.DialogInterface; import android.content.Intent; import android.content.Intent; import android.content.Intent; import android.content.Uni; import android.content.Uni; import android.content.Uni; import android.content.Uni; import android.content.Uni; import android.vidget.StatUity; import android.vidget.StatUity; import android.vidget.StatUity; import android.vidget.StatUity; import android.vidget.LiterSty; import android.vidget.LiterSty; import android.vidget.LiterSty; import android.vidget.LiterSty; import android.vidget.LiterSty; import android.vidget.LiterSty; import java.lot.File; import java.util.Vector; private static final int DLGID_CHCNES = 1; private static final int DLGID_CHCNES = 2; private static final int DLGID_CHCNES = 6; private static final int DLGID_CHCNES = 6; private static final int DLGID_CHCNES = 6; private static final int DLGID_CHCNES = 0; private static final int DLGID_CHCNES = 0; private static final int DLGID_CHCNES_PENAME = 8192; private static final int DLGIDSE_CHETE = 8192; private static final int DLGID_CHCNES_PENAME = 4090; private Statid g.d_d_chces = null; private DLGID g.d_d_chces = null; priva</pre>		import android and Activity.
<pre>import android.app.Dialog; import android.app.Colladog; import android.app.Colladog; import android.content.Context; import android.content.ColladogInterface; import android.content.Intent; import android.content; private static final int DIGD_REMUME = 409; private static final int D_REMUME = A09; private static final int D_REMU</pre>		import android.app.Activity;
<pre>import minicipation in the importance is a set of the import and import and the import and</pre>		import android an Dialor.
<pre>import and/oid.app.PrictureIN(); import and/oid.app.PrictureIN(); import and/oid.content.Context; import and/oid.content.Intent; import and/oid.os.Bundle; import and/oid.os.Bundle; import and/oid.os.Bundle; import and/oid.widget.ArrayAdapter; import and/oid.widget.Button; import and/oid.widget.Button; import and/oid.widget.LinearLayout; import java.io.File; import java.util.Vector; 72 public class TraceList extends ListActivity implements View.OnClickListener, DialogInterface.OnClickListener { private static final int DLGID_CHOSE = 1; private static final int DLGID_CHOSE = 2; private static final int DLGID_CHOSE = 3; private static final int DLGID_CHOSE = 5; private static final int DLGID_EREATE = 0; private static final int DLGID_EREATE = 0; private static final int DLGID_EREATE = 3; private static final int DLGIOS_EXPORT = 3; private static final int DLGIOS_EXPORT = 3; private static final int DLGIOS_EXPORT = 3; private static final int D_CHOSE_EXPORT = 8; private static final int D_CHOSE_EXPORT = 8; private static final int D_CHOSE_EXPORT = 8; private static final int D_CHOSE_EXPORT, ID_CHOSE_EXPORT, ID_CHOSE_EXPORT, ID_CHOSE_ELETE}; private static final int D_CHOSE_EXPORT, ID_CHOSE_EXPORT, ID_CHOSE_ELETE}; private static final int D_CHOSE_EXPORT, ID_CHOSE_EXPORT, ID_CHOSE_ELETE}; private Claig g_dlg_chose = null; private Dialog g_dlg_chose = null;</pre>		import android applicates,
<pre>import and/oil.content.Context; import and/oil.content.Context; import and/oil.content.Intent; import and/oil.content.Intent; import and/oil.content.Intent; import and/oil.content.Intent; import and/oil.content.Intent; import and/oil.content.Intent; import and/oil.content.Unent; import and/oil.content.Unent; import and/oil.content.Unent; import and/oil.content.Unent; import and/oil.content.Unent; import and/oil.content.Unent; import and/oil.content.Unent; import and/oil.content.Unent; import and/oil.content.Unent; import java.util.Vector; public class TraceList extends ListActivity implements View.OnClickListener, DialogInterface.OnClickListener { private static final int DLGID_CHOOSE = 1; private static final int DLGID_CHOOSE = 2; private static final int DLGID_CHOOSE = 2; private static final int DLGID_CHOOSE_2; private static final int DLGOSE_DELETE = 8; private static final int D_CHOOSE_DELETE = 8; private static final in</pre>		import android an Program (blan)
<pre>import amount content.content, import android.content.linet; import android.content.linet; import android.os.Bundle; import android.view.View; import android.view.View; import android.widget.Button; import android.widget.linearLayout; import android.widget.linearLayout; import android.widget.linearLayout; import android.widget.linearLayout; import android.widget.linearLayout; import android.widget.listView; import android.widget.listView; import android.widget.listView; import android.widget.listView; import java.io.Fil; import java.io.Fil; import java.io.Fil; import java.io.Fil; import static final int DIGID_CHOSE = 1; private static final int DIGID_CHOSE = 1; private static final int DIGID_CHOSE = 3; private static final int DIGID_CREATE = 0; private Static g_d_d_cREATE = 0; privat</pre>		import android content Contact,
<pre>import minorodictionent.Interface; import android.content.Interface; import android.oret.Uni; import android.vidget.ArrayAdapter; import android.widget.ArrayAdapter; import android.widget.EditTer; import android.widget.ListView; import android.widget.ListView; import android.widget.ListView; import android.widget.ListView; import java.to.File; import java.to.File; import java.to.File; import java.to.File; import static final int DIGTD_CHOOSE = 1; private static final int DIGTD_CHOOSE = 3; private static final int DIGTD_CHOOSE = 3; private static final int DIGTD_CHOOSE = 6; private static final int DIGTD_RENAME = 2; private static final int ID_CHOOSE_EXPORT = 8194; private static final int ID_CHOOSE_EXPORT = 8194; private static final int ID_CHOOSE_EXPORT = 8194; private static final int ID_CHOOSE_COPEN = 8192; private static final int ID_CHOOSE_COPEN = 8192; private static final int ID_CHOOSE_COPEN = 8192; private static final int ID_CHOOSE_COPEN, ID_CHOOSE_RENAME, ID_CHOOSE_EXPORT, ID_CHOOSE_DELETE); private static final int ID_CHOOSE_COPEN, ID_CHOOSE_RENAME, ID_CHOOSE_EXPORT, ID_CHOOSE_DELETE); private static final int ID_CHOOSE_RENAME = 4097; private static final int ID_CHOOSE_RENAME = 4097; priv</pre>		import android content Dialographering.
<pre>import shorod.net.Uni; import android.net.Uni; import android.co.Bundle; import android.view.Wiew; import android.widget.ArrayAdapter; import android.widget.EditText; import android.widget.LinearLayout; import android.widget.LinearLayout; import android.widget.LinearLayout; import android.widget.LinearLayout; import android.widget.Toast; import android.widget.Toast; import android.widget.Toast; import java.toil.Vector; public class TraceList extends ListActivity implements View.OnClickListener, DialogInterface.OnClickListener { private static final int DLGD_CREATE = 0; private static final int DLGD_CREATE = 0; private static final int DLGD_REMANE = 2; private static final int ID_CHOSS_DELTE = 8195; private static final int ID_CHOSS_DELTE = 8195; private static final int ID_CHOSS_DELTE = 8193; private static final int ID_CHOSS_DELTE = 8193; private static final int ID_CHOSS_DEMANE = 4096; private static final int ID_CHOSS_DEMANE = 4096; private static final int ID_CHOSS_DEMANE = 4097; private static final int ID_CHOS</pre>		import android.content.bladginerrace;
<pre>import shift of the second secon</pre>		import android concertification
<pre>Import and/old.os.Envirs. Import and/old.os.Envirs. Import and/old.os.Envirs. Import and/old.view.View; Import and/old.widget.ArrayAdapter; Import and/old.widget.EditText; Import and/old.widget.LinearLayout; Import and/old.widget.InearLayout; Import and/old.widget.InearLayout; Import and/old.widget.Toast; Import java.io.File; Import java.io.File; Import java.io.File; Import java.io.File; Import java.io.File; Import static final int DLGID_CROSE = 1; private static final int DLGID_CREATE = 0; private static final int DLGID_EETE = 0; private static final int DLGID_EETE = 5; private static final int DLGID_EETE = 5; private static final int DLGID_EETE = 5; private static final int DLGID_EETE = 8195; private static final int DLCHOOSE_EETE = 8195; private static final int D_CHOOSE_EETE = 8193; private static final int D_CHOOSE_EETEMAME = 4097; private static final int D_CHOOSE_EETEALWE = 4096; private static final int D_CREATE_TRACENAME = 4096; private static final int D_REATE_TRACENAME = 4096; priva</pre>		import android or Bundlas
<pre>import and/oid.view.View; import and/oid.view.View; import and/oid.vidget.Button; import and/oid.vidget.EditText; import and/oid.vidget.Listview; import and/oid.vidget.Tosst; import com.phfsoftware.rassta.GeoTrace; import java.util.Vector; 22 public class TraceList extends ListActivity implements View.OnClickListener, DialogInterface.OnClickListener { private static final int DLGID_CHOOSE = 1; private static final int DLGID_CHOOSE = 5; private static final int DLGID_CHOOSE = 6; private static final int DLGID_REQLOSE = 6; private static final int DLGID_REQLOSE = 6; private static final int D_CHOOSE_ENDERT = 8192; private static final int D_CHOOSE_ENDERT = 8192; private static final int D_CHOOSE_ENDERT = 8192; private static final int D_CHOOSE_RENAME = 48193; private static final int D_CHOOSE_RENAME = 4899; private static final int D_CHOOSE_POENT.ND_CHOOSE_RENAME, ID_CHOOSE_EXPORT, ID_CHOOSE_DELETE); private static final int D_RENAME_TAACENAME = 4899; private static string[] m_action_names; private static string[] m_action_names; private foldag m_dlg_choose = null; private Dialog m_dlg_choose = null; private String m_patcheod_filename = ""; private String m_selected_filename = ""; private String m_se</pre>		import android of Savinace,
<pre>import and/oid.widget.ArrayAdapter; import and/oid.widget.ArrayAdapter; import and/oid.widget.EditText; import and/oid.widget.ListView; import and/oid.widget.ListView; import and/oid.widget.Insarta; import java.io.File; import java.io.File; import java.iot.File; import java.iot.File; import java.iot.File; import static final int DLGID_CHOOSE = 1; private static final int DLGID_CHOOSE = 0; private static final int DLGID_CHETE = 0; private static final int DLGID_CHETE = 0; private static final int DLGID_ENDATE = 0; private static final int D_CHOOSE_ENDATE = 8195; private static final int D_CHOOSE_ENDATE = 8192; private static final int D_CHOOSE_ENDATE = 8193; private static final int D_CHOOSE_OELETE); private static final int D_CHOOSE_OELETE = 8193; private static final int D_CHOOSE_OELETE = 8194; private static final int D_CHOOSE_OELETE = 8195; private static final int D_CHOOSE_OELETE = 8195; private static final int D_CHOOSE_OELETE = 8195; private static final</pre>		import and 100.05.civil offerity
<pre>import android.widget.Button; import android.widget.Button; import android.widget.Elitext; import android.widget.LinearLayout; import android.widget.LinearLayout; import android.widget.LinearLayout; import java.io.File; import java.io.File; import java.util.Vector;</pre>		import android view view,
<pre>import and/oid.widget.EditText; import and/oid.widget.ListVext; import and/oid.widget.ListVext; import and/oid.widget.ListVext; import and/oid.widget.ListVext; import and/oid.widget.ListVext; import java.lo.File; import java.lo.File; import java.utl.Vector; 22 public class TraceList extends ListActivity implements View.OnClickListener, DialogInterface.OnClickListener { private static final int DLGID_CHOOSE = 1; private static final int DLGID_CHOOSE = 2; private static final int DLGID_REMAWE = 2; private static final int DLGID_REMAWE = 2; private static final int DLGID_REMAWE = 8195; private static final int ID_CHOOSE_DELETE = 8195; private static final int ID_CHOOSE_DELETE = 8192; private static final int ID_CHOOSE_REMAWE = 8193; private static final int ID_CHOOSE_REMAWE = 4096; private static final int ID_CHOOSE_REMAWE = 4096; private static final int ID_CHOOSE_REMAWE = 4096; private static final int ID_CHOOSE_REMAWE = 4097; private static final int ID_CHOOSE_REMAWE = 4096; private static final int ID_CHOOSE_REMAWE = 4097; private static final int ID_CHOOSE_REMAWE = 4096; private static final int ID_CHOOSE_REMAWE = 4096; private static final int ID_CHOOSE_REMAWE = 4096; private static string[] m_action_names; private former m_context; private former m_contex</pre>		import android videat Button
<pre>import and/oik.niget.tinerlayout; import and/oik.widget.linerlayout; import and/oik.widget.linerlayout; import java.io.File; import java.util.Vector;</pre>		import android.Huget.button;
<pre>import android.widget.ListVev; import android.widget.ListVev; import android.widget.ListVev; import java.to:Pile; import java.to:Pile; import java.util.Vector;</pre>		import and old.winget.cuitext;
<pre>import android.wiget.Tost; import android.wiget.Tost; import java.io.File; import java.io.File; import java.io.File; import java.util.Vector;</pre>		import android videat istviau
<pre>import annothinger.indext</pre>		import android videst Tast.
<pre>import Computering Control of the control of t</pre>		import and outwright, road;
<pre>import jowa.util.Vector; import jowa.util.Vector; z public class TraceList extends ListActivity implements View.OnClickListener, DialogInterface.OnClickListener { private static final int DLGID_CREATE = 0; private static final int DLGID_ENETE = 5; private static final int DLGID_REVORT = 3; private static final int DLGID_REVORT = 2; private static final int DLGID_REVORT = 8195; private static final int D_CHOOSE_ENETE = 8195; private static final int D_CHOOSE_ENETE = 8193; private static final int D_CHOOSE_OPEN = 4096; private static final int D_CHOOSE_TERACHAVE = 4097; private static final int D_RENAWE_TRACENAVE = 4097; private static string[] m_action_names; private static string[] m_action_names; private static string[] m_action_names; private Context m_context; private Dialog m_dlg_choose = null; private Dialog m_dlg_choose = null; private Dialog m_dlg_ceporting = null; private String m_selected_filename = ""; private String m_selected_filename = "";</pre>		import completion en adstateorrace;
<pre>public class TraceList extends ListActivity implements View.OnClickListener, DialogInterface.OnClickListener { private static final int DLGID_CHOOSE = 1; private static final int DLGID_DELETE = 0; private static final int DLGID_DELETE = 5; private static final int DLGID_REQUOSE = 6; private static final int DLGID_REQUOSE = 6; private static final int D_CHOOSE_DELETE = 8195; private static final int D_CHOOSE_DELETE = 8192; private static final int D_CHOOSE_REMAWE = 8193; private static final int D_CHOOSE_REMAWE = 4897; private static final int D_CHOOSE_REMAWE = 4096; private static final int D_CHOOSE_REMAWE = 4096; private static final int D_CHOOSE_REMAWE = 4097; private static final int D_CHOOSE_OPEN = 10_CHOOSE_REMAWE, ID_CHOOSE_EXPORT, ID_CHOOSE_DELETE); private static string[] m_action_names; private static string[] m_action_names; private Dialog m_dlg_choose = null; private Dialog m_dlg_choose = null; private Dialog m_dlg_cexport = null; private Dialog m_dlg_cexp</pre>		import java uti Vactor
<pre>72 public class TraceList extends ListActivity implements View.OnClickListener, DialogInterface.OnClickListener { private static final int DLGID_CREATE = 0; private static final int DLGID_EXEATE = 0; private static final int DLGID_EXEATE = 3; private static final int DLGID_EXEATE = 3; private static final int DLGID_REQLOSE = 6; private static final int DLGID_REQLOSE = 6; private static final int DLGID_REQLOSE = 6; private static final int D_CHOOSE_DELETE = 8195; private static final int D_CHOOSE_DELETE = 8195; private static final int D_CHOOSE_RENAME = 8192; private static final int D_CHOOSE_RENAME = 4096; private static final int D_RENAME TRACENAME = 4096; private static final int D_RENAME TRACENAME = 4096; private static string[] m_action_names; private static string[] m_action_names; private folds_choose = null; private Dialog m_dlg_choose = null; private Dialog m_dlg_choose = null; private Dialog m_dlg_choose = null; private Dialog m_dlg_cnemame = null; private String m_path_exportedTrace = null; private</pre>		Import Java.uti.vector;
<pre>private static final int DLGTD_CHOOSE = 1; private static final int DLGTD_CREATE = 0; private static final int DLGTD_ERLETE = 5; private static final int DLGTD_RENAME = 2; private static final int DLGTD_RENAME = 2; private static final int ID_CHOOSE_ENPORT = 8194; private static final int ID_CHOOSE_ENPORT = 8194; private static final int ID_CHOOSE_ENPORT = 8194; private static final int ID_CHOOSE_ENPORT = 8193; private static final int ID_CHOOSE_ENPORT = 8193; private static final int ID_CHOOSE_ENPORT = 8193; private static final int ID_CREATE_TRACENAME = 4096; private static final int ID_CREATE_TRACENAME = 4096; private static final int ID_CREATE_TRACENAME = 4097; private static string[] m_action_names; private static string[] m_action_names; private static string[] m_action_names; private final m_alg_choose = null; private Dialog m_alg_choose = null; private Dialog m_alg_choose = null; private Dialog m_alg_create = null; private String m_aselected_filename = ""; private String m_selected_filename = "";</pre>	72	public class TraceList extends ListActivity implements View.OnClickListener, DialogInterface.OnClickListener {
<pre>private static final int DLGTD_CREATE = 0; private static final int DLGTD_DELTE = 5; private static final int DLGTD_EXPORT = 3; private static final int DLGTD_REVLOSE = 6; private static final int D_CHOOSE_DELETE = 8195; private static final int ID_CHOOSE_DELETE = 8192; private static final int ID_CHOOSE_REVLAYE = 8193; private static final int ID_CHOOSE_REVLAYE = 4096; private static final int ID_CHOSE_REVLAYE = 4096; private static final int ID_CREATE_TRACENAVE = 4096; private static final int ID_CREATE_TRACENAVE = 4096; private static final int ID_RENAVE_TRACENAVE = 4096; private static final int ID_RENAVE_TRACENAVE = 4096; private static string[] m_action_names; private static string[] m_action_names; private context m_context; private Context m_context; private Dialog m_dlg_choose = null; private Dialog m_dlg_choose = null; private Dialog m_dlg_choose = null; private Dialog m_dlg_cexport = null; private String m_patheted_filename = ""; private String m_selected_filename = "";</pre>		private static final int DLGID_CHOOSE = 1;
<pre>private static final int DLGTD_DELETE = 5; private static final int DLGTD_EXPORT = 3; private static final int DLGTD_RENAWE = 2; private static final int DLGTD_REQLOSE = 6; private static final int DLGTD_REQLOSE = 6; private static final int ID_CHOOSE_DELETE = 8194; private static final int ID_CHOOSE_TEXPORT = 8193; private static final int ID_CREATE_TRACENAME = 4096; private static final int ID_CREATE_TRACENAME = 4096; private static final int ID_RENAME_TRACENAME = 4097; private static final int ID_RENAME_TRACENAME = 4097; private static final int ID_CREATE_TRACENAME = 4097; private static String[] m_action_names; private static String[] m_action_names; private Activity; private Otalog m_alg_choose = null; private Dialog m_alg_choose = null; private Dialog m_alg_choose = null; private Dialog m_alg_exporting = null; private Dialog m_alg_exporting = null; private Dialog m_alg_encodes = null; private String m_selected_filename = ""; private String m_selected_name = "";</pre>		private static final int DLGID_CREATE = 0;
<pre>private static final int DLGTD_EXPORT = 3; private static final int DLGTD_REQCLOSE = 6; private static final int DLGTD_REQCLOSE = 6; private static final int D_CHOOSE_EDELTE = 8195; private static final int D_CHOOSE_EDELTE = 8192; private static final int D_CHOOSE_GPEN = 8192; private static final int D_CHOOSE_GPENME = 4096; private static final int D_CREATE_TRACENAWE = 4096; private static final int D_CREATE_TRACENAWE = 4096; private static final int D_RENAWE_TRACENAWE = 4096; private static string[] = dtoin_names; private static string[] = action_names; private context = context; private Context = context; private Dialog m_dlg_choose = null; private Dialog m_dlg_choose = null; private Dialog m_dlg_cexport = null; private Dialog m_dlg_</pre>		private static final int DLGID_DELETE = 5;
<pre>private static final int DLGTD_REMANE = 2; private static final int DLGTD_REQUOSE = 6; private static final int ID_CHOOSE_DELETE = 8195; private static final int ID_CHOOSE_DELETE = 8194; private static final int ID_CHOOSE_RENAME = 8193; private static final int ID_CHOOSE_RENAME = 4996; private static final int ID_CREATE_TRACENAME = 4096; private static final int ID_RENAME = RACENAME = 4096; private static string[] m_action_names; private static string[] m_action_names; private static string[] m_action_names; private context m_context; private Dialog m_dlg_choose = null; private Dialog m_dlg_choose = null; private Dialog m_dlg_choose = null; private Dialog m_dlg_cename = null; private String m_selected_filename = ""; private String m_selected_filename = ""; private String m_selected_filename = "";</pre>		private static final int DLGID_EXPORT = 3;
<pre>private static final int DLGTO_REQCLOSE = 6; private static final int ID_CHOOSE_DELETE = 8195; private static final int ID_CHOOSE_EXPORT = 8194; private static final int ID_CHOOSE_EXPORT = 8192; private static final int ID_CHOOSE_EXPORT = 8193; private static final int ID_CREATE_TRACEMAME = 4096; private static final int ID_CREATE_TRACEMAME = 4096; private static int[] action_bri_ids = (ID_CHOOSE_OPEN, ID_CHOOSE_RENAME, ID_CHOOSE_EXPORT, ID_CHOOSE_DELETE}; private static string[] m_action_names; private static string[] m_action_names; private foldog m_dls_choose = null; private Dialog m_dls_choose = null; private Dialog m_dls_choose = null; private Dialog m_dls_choose = null; private Dialog m_dls_cename = null; private String m_selected_filename = ""; private String m_selected_name = "";</pre>		private static final int DLGID_RENAME = 2;
<pre>private static final int ID_CHOOSE_DELETE = 8195; private static final int ID_CHOOSE_DORT = 8194; private static final int ID_CHOOSE_RENAME = 8192; private static final int ID_CHOOSE_RENAME = 4996; private static final int ID_CREATE_TRACENAME = 4996; private static int] action_Inti_ds = {ID_CHOOSE_OPEN, ID_CHOOSE_RENAME, ID_CHOOSE_EXPORT, ID_CHOOSE_DELETE}; private static string[] m_action_names; private static string[] m_action_names; private context m_context; private context m_context; private Dialog m_dlg_choose = null; private Dialog m_dlg_choose = null; private Dialog m_dlg_delet = null; private Dialog m_dlg_create = null; private String m_path_exportedTrace = null; private String m_selected_filename = ""; private String m_selected_name = "";</pre>		private static final int DLGID_REQCLOSE = 6;
<pre>private static final int ID_CHOOSE_EXPORT = 8194; private static final int ID_CHOOSE_ERNAME = 8193; private static final int ID_CHOOSE_RENAME = 4096; private static final int ID_CREATE_TRACENAME = 4097; private static final int ID_RENAME_TRACENAME = 4097; private static string[] m_action_btn_ids = {ID_CHOOSE_OPEN, ID_CHOOSE_RENAME, ID_CHOOSE_EXPORT, ID_CHOOSE_DELETE}; private static string[] m_action_names; private static string[] m_action_names; private Activity; private Oialog m_dlg_choose = null; private Dialog m_dlg_create = null; private Dialog m_dlg_create = null; private Dialog m_dlg_exporting = null; private Dialog m_dlg_exporting = null; private Dialog m_dlg_exportedTrace = null; private Dialog m_dlg_exportedTrace = null; private Dialog m_dlg_exportedTrace = null; private String m_selected_name = ""; private String m_selected_name = ""; private String m_selected_name = "";</pre>		private static final int ID_CHOOSE_DELETE = 8195;
<pre>private static final int ID_CHOOSE_OPEN = 8192; private static final int ID_CHOOSE_RENAME = 8193; private static final int ID_RENAME_TRACENAME = 4097; private static int[] action_names; private static string[] m_action_names; private context m_context; private Dialog m_dlg_choose = null; private String m_selected_filename = ""; private String m_selected_filename = "";</pre>		private static final int ID_CHOOSE_EXPORT = 8194;
<pre>private static final int ID_CHOOSE_RENAME = 8193; private static final int ID_CREATE_TRACENAME = 4099; private static final int ID_RENAME_TRACENAME = 4097; private static string[] m_action_names; private static string[] m_action_names; private static string[] m_action_names; private context m_context; private Context m_context; private Dialog m_dlg_choose = null; private Dialog m_dlg_choose = null; private Dialog m_dlg_choose = null; private Dialog m_dlg_cexport = null; private Dialog m_dlg_export = null; private Dialog m_dlg_export = null; private Dialog m_dlg_export = null; private Dialog m_dlg_rename = null; private String m_selected_filename = "; private String m_selected_filename = "; privat</pre>		private static final int ID_CHOOSE_OPEN = 8192;
<pre>private static final int ID_CREATE_TRACENAME = 4096; private static final int ID_RENAME_TRACENAME = 4097; private static int[] action_btn_ids = {ID_CHOOSE_OPEN, ID_CHOOSE_RENAME, ID_CHOOSE_EXPORT, ID_CHOOSE_DELETE}; private static String[] m_action_names; private Activity; private Dialog m_dlg_choose = null; private Dialog m_dlg_create = null; private Dialog m_dlg_create = null; private Dialog m_dlg_create = null; private Dialog m_dlg_exporting = null; private Dialog m_dlg_exporting = null; private Dialog m_dlg_enemae = null; private Dialog m_dlg_exportedTrace = null; private Dialog m_dlg_exportedTrace = null; private Dialog m_dlg_exportedTrace = null; private String m_selected_filename = ""; private String m_selected_name = "";</pre>		private static final int ID_CHOOSE_RENAME = 8193;
<pre>private static final int ID_RENAME_TRACENAME = 4997; private static final int ID_RENAME_TRACENAME = 4997; private static String[] m_action_names; private static String[] m_action_names; private context m_context; private context m_context; private Dialog m_dlg_choose = null; private Dialog m_dlg_choose = null; private Dialog m_dlg_cexte = null; private Dialog m_dlg_export = null; private Dialog m_dlg_exporting = null; private Dialog m_dlg_exporting = null; private Dialog m_dlg_encame = null; private String m_path_exportedTrace = null; private String m_selected_filename = ""; private String m_selected_name = "";</pre>		private static final int ID_CREATE_TRACENAME = 4096;
<pre>private static int[] action_btn_ids = {I0_HOOSE_OPEN, I0_CHOOSE_RENAME, I0_CHOOSE_EXPORT, ID_CHOOSE_DELETE}; private static string[] m_action_names; private Activity m_activity; private Dialog m_dlg_choose = null; private Dialog m_dlg_choose = null; private Dialog m_dlg_choose = null; private Dialog m_dlg_export = null; private Dialog m_dlg_exporting = null; private Dialog m_dlg_reqclose = null; private Dialog m_dlg_reqclose = null; private Dialog m_dlg_reqclose = null; private Dialog m_dlg_reqclose = null; private String m_selected_filename = ""; private String m_selected_name = ";</pre>		private static final int ID_RENAME_TRACENAME = 4097;
<pre>private static String[] m_action_names; private Activity m_activity; private Context m_context; private Dialog m_dlg_choose = null; private Dialog m_dlg_cepte = null; private Dialog m_dlg_export = null; private Dialog m_dlg_exporting = null; private Dialog m_dlg_exporting = null; private Dialog m_dlg_encase = null; private Dialog m_dlg_encase = null; private Dialog m_dlg_encase = null; private Dialog m_dlg_encase = null; private String m_selected_name = ""; private String m_selected_name = ";</pre>		<pre>private static int[] action_btn_ids = {ID_CHOOSE_OPEN, ID_CHOOSE_RENAME, ID_CHOOSE_EXPORT, ID_CHOOSE_DELETE};</pre>
<pre>private Activity m_activity; private Context m_context; private Dialog m_dlg_choose = null; private Dialog m_dlg_cetet = null; private Dialog m_dlg_export = null; private Dialog m_dlg_exporting = null; private Dialog m_dlg_rename = null; private Dialog m_dlg_rename = null; private Dialog m_dlg_rename = null; private Dialog m_dlg_rename = null; private String m_selected_filename = ""; private String m_selected_filename = ";</pre>		<pre>private static String[] m_action_names;</pre>
<pre>private Context m_context; private Dialog m_dlg_choose = null; private Dialog m_dlg_create = null; private Dialog m_dlg_export = null; private Dialog m_dlg_exporting = null; private Dialog m_dlg_reqaices = null; private Dialog m_dlg_reqaices = null; private String m_path_exportedTrace = null; private String m_selected_filename = ""; private String m_selected_name = ";</pre>		private Activity m_activity;
<pre>private Dialog m_dlg_choose = null; private Dialog m_dlg_crate = null; private Dialog m_dlg_delte = null; private Dialog m_dlg_export = null; private Dialog m_dlg_exporting = null; private Dialog m_dlg_reqtose = null; private Dialog m_dlg_reqtose = null; private String m_path exportedTrace = null; private String m_selected_filename = ""; private String m_selected_name = ";</pre>		private Context m_context;
<pre>private Dialog m_dlg_create = null; private Dialog m_dlg_delete = null; private Dialog m_dlg_export = null; private Dialog m_dlg_exporting = null; private Dialog m_dlg_rename = null; private Dialog m_dlg_reqclose = null; private String m_path_exportedTrace = null; private String m_selected_filename = ""; private String m_selected_name = ";</pre>		private Dialog m_dlg_choose = null;
<pre>private Dialog m_dlg_export = null; private Dialog m_dlg_export = null; private Dialog m_dlg_exporting = null; private Dialog m_dlg_reqclose = null; private Dialog m_dlg_reqclose = null; private String m_path_exportedTrace = null; private String m_selected_filename = ""; private String m_selected_name = ";</pre>		<pre>private Dialog m_dlg_create = null;</pre>
<pre>private Dialog m_dlg_export = null; private Dialog m_dlg_exporting = null; private Dialog m_dlg_rename = null; private Dialog m_dlg_reqclose = null; private String m_path_exportedTrace = null; private String m_selected_filename = ""; private String m_selected_name = "";</pre>		private Dialog m_dlg_delete = null;
<pre>private Dialog m_dlg_exporting = null; private Dialog m_dlg_rename = null; private Dialog m_dlg_reqclose = null; private string m_path_exportedTrace = null; private String m_selected_filename = ""; private String m_selected_name = ";</pre>		private Dialog m_dlg_export = null;
<pre>private Dialog m_dlg_rename = null; private Dialog m_dlg_reqtose = null; private String m_path_exportedTrace = null; private String m_selected_filename = ""; private String m_selected_name = ";</pre>		private Dialog m_dlg_exporting = null;
<pre>private Dialog m_dlg_reqclose = null; private String m_path_exportedTrace = null; private String m_selected_filename = ""; private String m_selected_name = "";</pre>		private Dialog m_dlg_rename = null;
<pre>private String m_path_exportedTrace = null; private String m_selected_filename = ""; private String m_selected_name = "";</pre>		private Dialog m_dlg_reqclose = null;
<pre>private String m_selected_filename = ""; private String m_selected_name = "";</pre>		<pre>private String m_path_exportedTrace = null;</pre>
<pre>private String m_selected_name = "";</pre>		<pre>private String m_selected_filename = ";</pre>
		<pre>private String m_selected_name = "";</pre>
<pre>private Thread m_thread_exporting = null;</pre>		<pre>private Thread m_thread_exporting = null;</pre>
<pre>private Vector<string> m_trfilenames;</string></pre>		<pre>private Vector<string> m_trfilenames;</string></pre>
<pre>private Vector<string> m_trnames;</string></pre>		<pre>private Vector<string> m_trnames;</string></pre>

图 5.30 从 Android Manifest 中跳转到 TraceList 类

• 查找项目的引用。

在项目上右击,在弹出的快捷菜单中选择 Find Usage 命令,就会弹出该项目的所有引用。 如图 5.31 所示为在 Jadx-gui 中查找引用。

return;	@ 查找	×
	童找用例: 🧳 com pufsoftware ransta Frefs.get_traceGpsPeriod 0	Context. String) int
806: Multi-variable seard RN: Multi-variable type i	节点	代码
d show_AboutBox() {	& com.pnfsoftware.raasta.Prefs.get_traceGpsPeriod(public static int get_traceGpsPeriod(Context context
te nam,	<pre>com.pnfsoftware.raasta.Raasta.onCreateDialog(int</pre>	<pre>int p = Prefs.get_traceGpsPeriod(this, this.lastTrac</pre>
name = getPackageManager	com.pnfsoftware.raasta.Raasta.onPrepareDialog(in	e.setText(new StringBuilder().append(Prefs.get_trace
n (Packagenanager, namenot name = "?";	<pre>com.pnfsoftware.raasta.Raasta.enable_gps(int) bo</pre>	<pre>int p = Prefs.get_traceGpsPeriod(this, this.lastTrac</pre>
	com.pnfsoftware.raasta.Raasta.onPrepareDialog(in	Toast.makeText(getApplicationContext(), String.forma
<pre>[] objarr = new object[bt [0] = getString(R.string.</pre>	4	
<pre>[1] = vername;</pre>	() 費示了 5 个结果中的第 1 至第 5 个	
<pre>[2] = getString(R.string. [3] = getString(R.string.</pre>		
<pre>[4] = getString(R.string.</pre>		HEI RA
r.setTitle(R.string.about): en wieleningeningenieel(enin);	
r.setHessage(Html.fromHtm	l(String.valueOf(String.format("%s v%scbr>%scbr>cbr>ca)	href='%s'>%s (c) 2012 ", objArr)) + " " + this.m_aboutbox_extram
<pre>class com.pnfsoftware.ra</pre>	ing.ok, new DialogInterface.OnClickListener() { asta.Raasta.AnonymousClass21 */	
dlg.dismiss():	nterface dig, int id) (

图 5.31 在 Jadx-gui 中查找引用

• 文本搜索。

Jadx-gui 提供全局文本搜索,在整个项目的范围内查找字符串,可以匹配类名、方法名、 变量名、代码。

如图 5.32 所示为在 Jadx-gui 中进行文本搜索。



图 5.32 在 Jadx-gui 中进行文本搜索

Jadx-gui 功能相比较于 JEB 要少一些,但是 Jadx-gui 是开源项目,轻量小巧,足够应付静态分析的任务。

5.4 010-editor 工具

010-editor 可以说是目前最强大的一款十六进制编辑器,可以编辑与查看各种十六进制文件,可以通过加载不同的文件模板解析各种文件格式。

5.4.1 010-editor 解析 so 文件

010-editor 官网有 elf 的文件模板网址为 https://www.sweetscape.com/010editor/ repository/files/ELF.bt,将其复制下来,单击 Templates 选项,选择 New Templates 打开 模板。使用 010-editor 打开 so 文件后按 F5 键即可使用对应的模板。

010-editor 模板对照 elf 文件定义的格式从十六进制中直接解析出 so 文件的各段表。 010-editor 的优点是可以更加直观地去定位某个结构的值在整个文件中的位置,可以配合

Hex editor 等十六进制文件编辑器对 so 文件直接进行修改。 如图 5.33 所示为使用 010-editor 打开 so 文件的界面。

libh_db.so ×							
0 1 2 3 4 5 0000h: 17 45 4C 46 02 01 00010h: 03 08 70 01 00	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	F Ó12340 00 .ELF. 00 00	- 56789/ 1 P- 8 - (5 - - - - - - - - - - - - - - - - - -	48CDEF		
Template Results - ELF.bt 🧟							
Name	Value	Start	Size	Color		Comment	
 struct file 		0h	11B38h	Fg:	Bg:		
struct elf_header		Oh	40h	Fg:	Bg:	The main elf header basically tells	
struct e_ident_t e_ident	FT 0101 (0)	Oh	10h	Fg:	Bg:	Magic number and other info	
enum e_type64_e e_type	EI_DYN (3)	10h	2h	Fg:	Bg:	Object file type	
enum e_machine64_e e	183	12h	2h	Fg:	Bg:	Architecture	
enum e_version64_e e_ve	EV_CURRENT (1)	14h	4h	Fg:	Bg:	Object file version	
Elf64_Addr e_entry_STAR	0x000000000043	18h	8h	Fg:	Bg:	Entry point virtual address	
Elf64_Off e_phoff_PROGR	64	20h	8h	Fg:	Bg:	Program header table file offset	
Elf64_Off e_shoff_SECTIO	6233456	28h	8h	Fg:	Bg:	Section header table file offset	
Elf32_Word e_flags	30h	4h	rg:	Bg:	Processor-specific flags		
Elfo4_Hait e_ensize_ELF_H	04 56	34N 26L	2n 2L	rg:	вg: в_	ELF Header size in bytes	
Elf64 Half e phone NLL	90	206	2n 2h	rg: Fai	bg: Rai	Program header table entry size	
Elf64 Half e sheetsize SE	6 64	246	2n 2h	rg: For	Bg: Bg:	Section header table entry count	
Elf64 Half a shour NUM	20	206	211	Fo:	Ba:	Section header table entry size	
Elifet Half a chtrady STRI	25	256	211	For	Ba:	Section header string table index	
struct program header table	55	40h	1006	For	Ba:	Program headers - describes the	
struct program table ent	(R X) Loadable Se	40h	38h	Fa:	Ba:		
struct program table ent	(RW.) Loadable S	78h	38h	Fa:	Ba:		
struct program table ent	(RW) Dynamic Se	B0h	38h	Fq:	Bq:		
struct program table ent	(R_) Note	E8h	38h	Fg:	Bg:		
struct program_table_ent	(R_) Note	120h	38h	Fg:	Bg:		

图 5.33 使用 010-editor 打开 so 文件的界面

5.4.2 010-editor 解析 Dex 文件

Dex 的文件模板可以在 010-editor 官网上找到, 网址为 https://www.sweetscape. com/010editor/repository/files/DEX.bt,按照上面的做法加载模板, 打开 Dex 文件。可以 将 Apk 包用 Zip 工具解压缩获得 Dex 文件。

如图 5.34 所示为使用 010-editor 打开 Dex 文件的界面。

classes.dex ×																						
0000h: 0010h: 0020h: 0030h: 0050h: 0050h: 0050h: 0070h: 0070h: 0080h: 0080h: 0080h: 0080h: 0080h: 0080h: 0080h: 0080h: 0080h: 0080h: 0080h: 0080h: 0080h: 0080h: 0080h: 010h: 0120h: 0130h: 0130h: 0150h: 0140h: 0150h: 0160h: 0170h:	0 54 99C 00 65 8F 6F 4C 05 5F 97 00 05 8F 6F 4C 05 5F 97 05 00 1 2 7F 40 05 67 A 3 1	1 65 00 930 008 205 72 73 73 73 74 74 75 75 76 76 76 76 77 77 77 77 77 77	2 78 F9 10 00 00 13 13 13 13 13 13 13 13 13 13 13 13 13	3 A 9A 9A 9A 000 000 000 000 000 000 000	4 30 EF 700 80 50 50 50 50 50 50 50 50 50 50 50 50 50	5 33 A8 00 92 0E CF 29 72 73 73 73 73 74 74 74 75 75 76 76 76 76 76 77	35 600 10 10 13 13 13 13 13 13 13 13 13 13 13 13 13	70000000000000000000000000000000000000	8 6F CD 78 45 45 45 45 45 45 45 45 45 45 45 45 45	9 75 84 56 43 00 3EC 72 73 73 73 74 74 74 75 75 75 76 76 76 76 77	A 03 87 34 00 00 00 17 13 13 13 13 13 13 13 13 13 13 13 13 13	8 48 62 12 00 00 00 00 00 00 00 00 00 00 00 00 00	C F0 19 00 70 DFC E8 20 DFC DFC 20 DFC 20 DFC 20 DFC 2 DFC 20 DFC 20 DFC	D 6A 000 300 300 72 73 73 73 74 75 75 75 76 76 76 76 76 77	E 25 8F 000 01 03 05 13 13 13 13 13 13 13 13 13 13 13 13 13	E 2E AE 000 000 000 000 000 000 000 000 000	016 2. 6. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0	1234565 ex.035 .051 (".P .A'. 	89A ou. 1\$‡ \$ xV4 \$ c. xV4 \$ c. xV4 \$ c.	BCDE Hðj%. b		
Templat	te Re	sult	s - (lex.l	bt <	,																
Name Value									Start			Size		e	Color		Comment					
struct header_item dex_header									Oł	h			70h		Fg	: 1	Bg:	Dex file header				
struct string_id_list dex_string_i 17287 strings									70	70h			10E1Ch		Fg	: 1	Bg:	String ID list				
struct type_id_list dex_type_ids 2149 types									10	10E8Ch			2194h		Fg	: 1	Bg:	Type ID list				
struct proto_id_list dex_proto_i 3397 prototypes										bes	13	13020h			9F3Ch		Fg	: 1	Bg:	Method prototype ID list		
struct field_id_list dex_field_ids 11407 fields										10	1CF5Ch			16478h		Fg	; (Bg:	Field ID list			
struct method_id_list dex_meth 1								16041 methods				33	333D4h			1F548h		Fg	: 1	Bg:	Method ID list	
struct class_def_item_list dex_cl.						l 1	391	class	ses		52	291Ch			ADE	0h	Fg	: 1	Bg:	Class definitions list		
struct map_list_type dex_map_l.					I 1	. 18 items				10	1D92C0h			DCh		Fg	: 1	Bg:	Map list			

图 5.34 使用 010-editor 打开 Dex 文件的界面

5.5 本章小结

本章介绍了对 Android 应用进行静态分析常用的工具以及使用方法,包括各种工具对 Native 层与 Java 层的静态逆向分析。互联网中还有许多集成了图形化操作界面的 Android 分析工具,比如 Android Killer,这些分析工具本质上是对 Baksmali、Apktool 等工 具的集成。这些工具还会在后面实战篇中陆续出现,本书也会结合具体需求介绍更多的用 于逆向分析的实战工具。