本人的系统为 ubuntu12.04

1、所需要的工具

1）apktool，功能：反编译出 apk 所需要的资源文件和布局设置文件等，

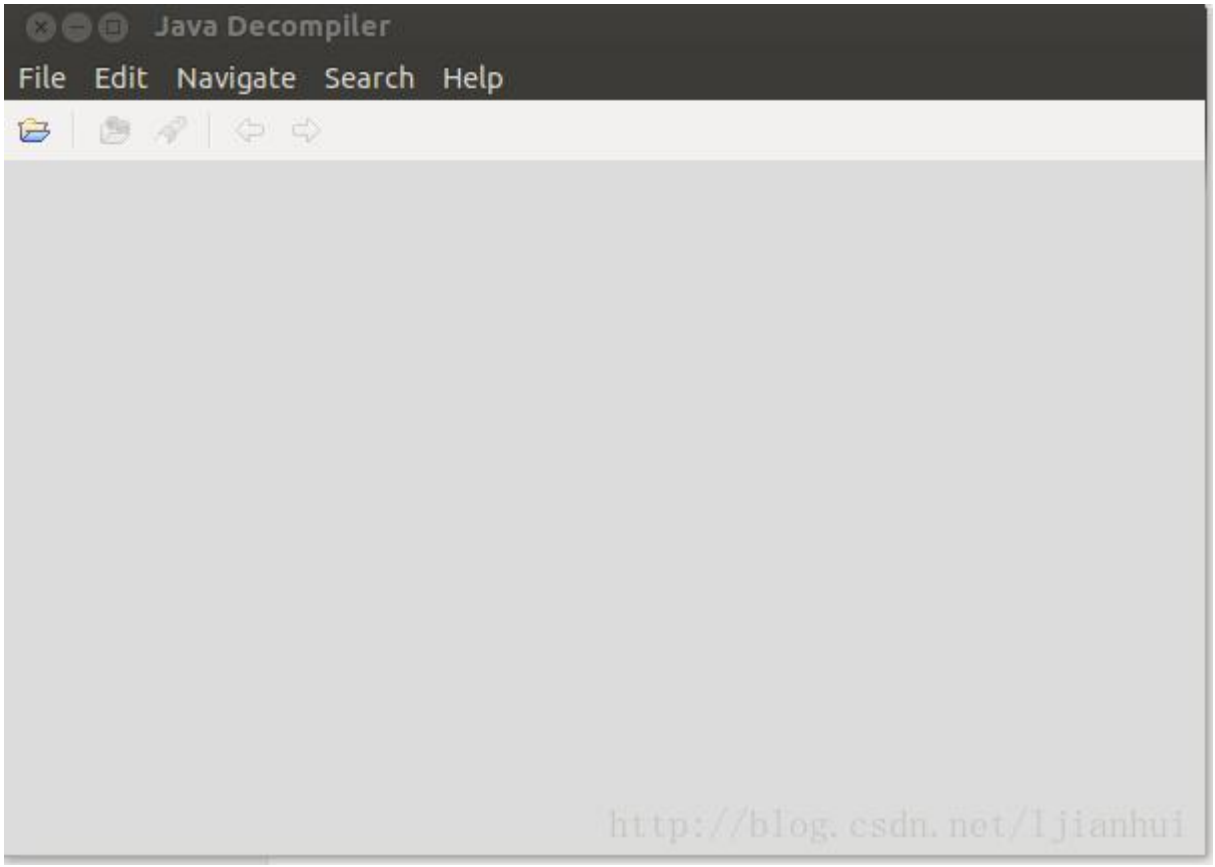
下载地址：https://code.google.com/p/android-apktool/downloads/list

需要下载 apktool1.5.2.tar.bz2 和 apktool-install-Linux-r05-ibot.tar.bz2 这两个文件，并把解压后的文件放在同一个文件夹中。

2）dex2jar，功能：反编译出 jar 文件，即 apk 的源程序文件的字节码，

下载地址：http://code.google.com/p/dex2jar/downloads/list

3）jdgui，功能：查看 dex2jar 反编译出的 jar 文件，使用该工具可以看到字节码对应的 Java 源代码，这个我在官网上没有找到，然后自己在网上下载的，但试验过能用。点击打开后，如下图所示：



2、反编译过程

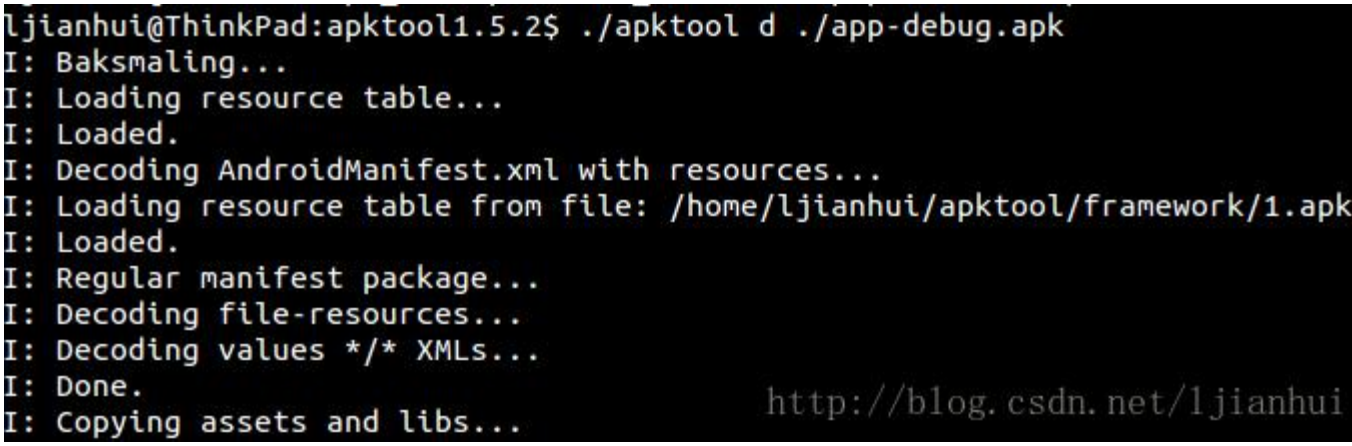
1）反编译出资源文件

使用 apktool 工具，进入 apktool 所在的目录下，使用如下的命令：

./apktool d ./xxx.apk（apk 所在的路径）

d 表示 decode，在当前目录下就会生成一个名为 xxx 的目录，里面就是反编译出来的各种资源文件，其中 res 表示资源文件，smali 表示源代码，不过是字节码，不能直接查看。

以本人的实验为例子，如下图所示：



此时会在当前目录下生成一个目录 app-debug。

2）源代码的反编译

a）因为 apk 文件其实是使用 zip 进行打包压缩生成的文件，所以先把 xxx.apk 文件改名为 xxx.zip 文件，并对其进行解压。

b)进入解压后的目录，其中有一个 classes.dex 文件，这个文件就是 java 文件编译再通过 dx 工具打包而成的，源代码就包含在这个文件中。

c）把前一步生成的文件 classes.dex 复制到 dex2jar 工具的根目录中，并使用如下命令对其进行反编译：

```
./dex2jar.sh d classes.dex
```

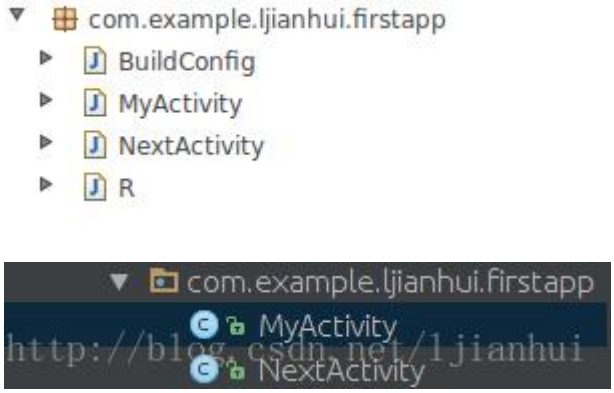
就会在当前目录下生成一个 classes_dex2jar.jar 文件

d）点击打开 jdgui 工具，这是一个图形化的工具，然后打开上上述的 classes_dex2jar.jar 文件就可以看到 apk 对应的源代码。

对于本人的实验如下：

```
ljianhui@ThinkPad:apktool1.5.2$ cd ../dex2jar-0.0.9.15/
ljianhui@ThinkPad:dex2jar-0.0.9.15$ ./dex2jar.sh d classes.dex
this cmd is deprecated, use the d2j-dex2jar if possible
dex2jar version: translator-0.0.9.15
dex2jar d -> d_dex2jar.jar
. while process file: [d]
.. ROOT cause:
java.io.FileNotFoundException: File 'd' does not exist
        at org.apache.commons.io.FileUtils.openInputStream(FileUtils.java:5
        at org.apache.commons.io.FileUtils.readFileToByteArray(FileUtils.ja
)
        at com.googlecode.dex2jar.reader.DexFileReader.readDex(DexFileReade
a:143)
        at com.googlecode.dex2jar.v3.Main.doFile(Main.java:63)
        at com.googlecode.dex2jar.v3.Main.main(Main.java:86)
dex2jar classes.dex -> classes_dex2jar.jar
Done.
```


源代码与反编译出来的代码比较如下（白色为反编译内容，黑色为原内容）：



```
protected void onCreate(Bundle paramBundle)
{
  super.onCreate(paramBundle);
  setContentView(2130903040);
  ((Button)findViewById(2131230721)).setOnClickListener(new View.OnClickListener()
  {
    public void onClick(View paramAnonymousView)
    {
      MyActivity.this.showMessage();
    }
  });
  ((Button)findViewById(2131230722)).setOnClickListener(new View.OnClickListener()
  {
    public void onClick(View paramAnonymousView)
    {
      MyActivity.this.writeToEdit();
    }
  });
  this.editText = ((EditText)findViewById(2131230723));
  ((Button)findViewById(2131230724)).setOnClickListener(new View.OnClickListener()
  {
    public void onClick(View paramAnonymousView)
    {
      MyActivity.this.gotoNextActivity();
    }
  });
  ((ListView)findViewById(2131230726));
}
```

```
protected void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    setContentView(R.layout.activity_my);

    Button btnShow = (Button)findViewById(R.id.button_show);
    btnShow.setOnClickListener(new OnClickListener() {
        @Override
        public void onClick(View view) {
            showMessage();
        }
    });

    Button btnWrite = (Button)findViewById(R.id.button_write);
    btnWrite.setOnClickListener(new OnClickListener() {
        @Override
        public void onClick(View view) {
            writeToEdit();
        }
    });
    editText = (EditText)findViewById(R.id.editText);

    Button btnNext = (Button)findViewById(R.id.button_next);
    btnNext.setOnClickListener(new OnClickListener() {
        @Override
        public void onClick(View view) {
            gotoNextActivity();
        }
    });

    ListView lst = (ListView)findViewById(R.id.listView);
}
```