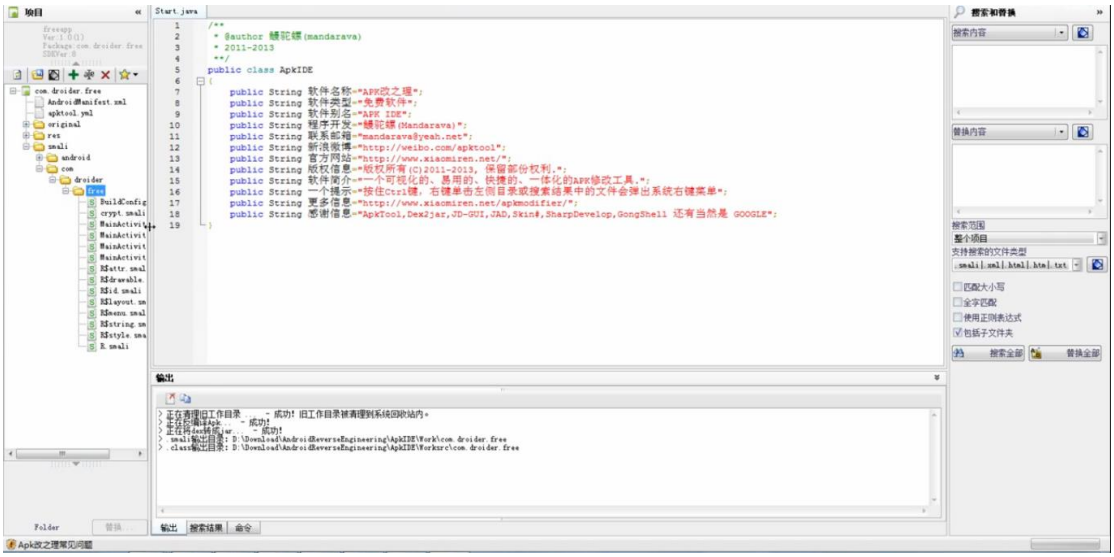
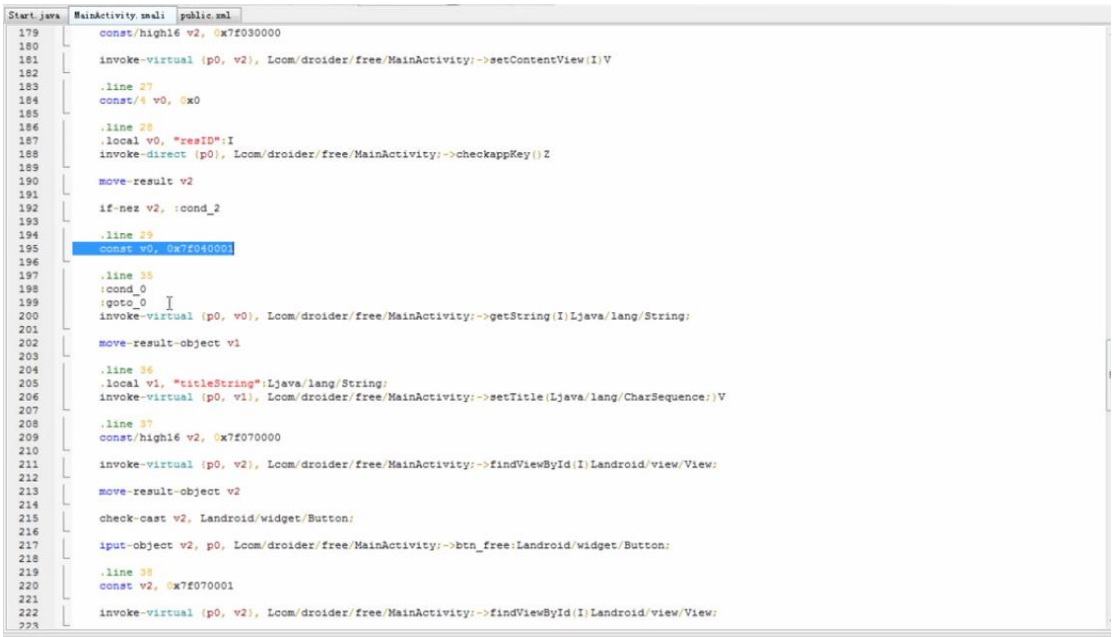
1. 试用版软件破解

使用 ApkIde 打开要破解的 app 进行反编译

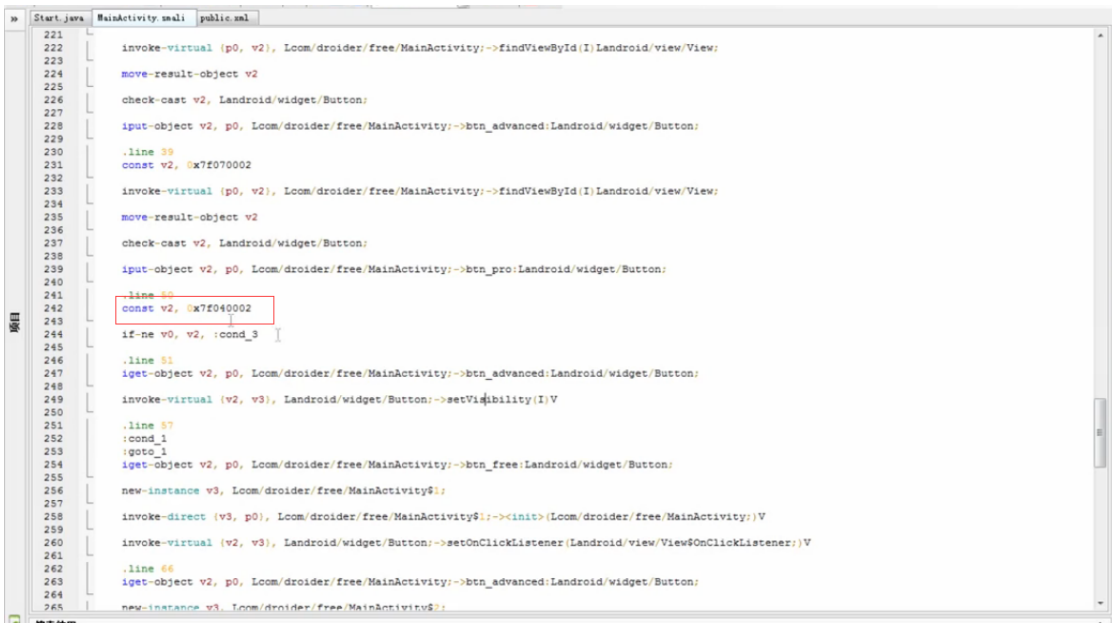


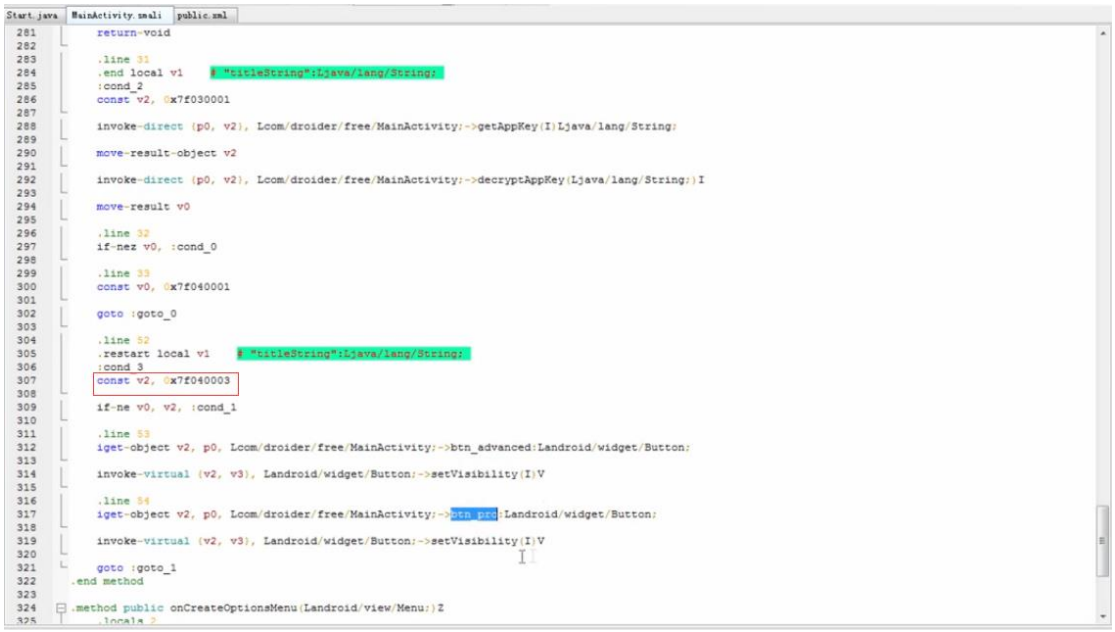
```
283     .line 31
284     .end local v1    # "titleString":Ljava/lang/String;
285     :cond_2
286     const v2, 0x7f030001
287
288     invoke-direct {p0, v2}, Lcom/droider/free/MainActivity;->getAppKey(I)Ljava/lang/String;
289
290     move-result-object v2
291
292     invoke-direct {p0, v2}, Lcom/droider/free/MainActivity;->decryptAppKey(Ljava/lang/String;)I
293
294     move-result v0
295
296     .line 32
297     if-nez v0, :cond_0
298
299     .line 33
300     const v0, 0x7f040001
301
302     goto :goto_0
303
304     .line 52
305     .restart local v1    # "titleString":Ljava/lang/String;
306     :cond_3
307     const v2, 0x7f040003
308
309     if-ne v0, v2, :cond_1
```

分别显示各个按钮的相关 smali 代码

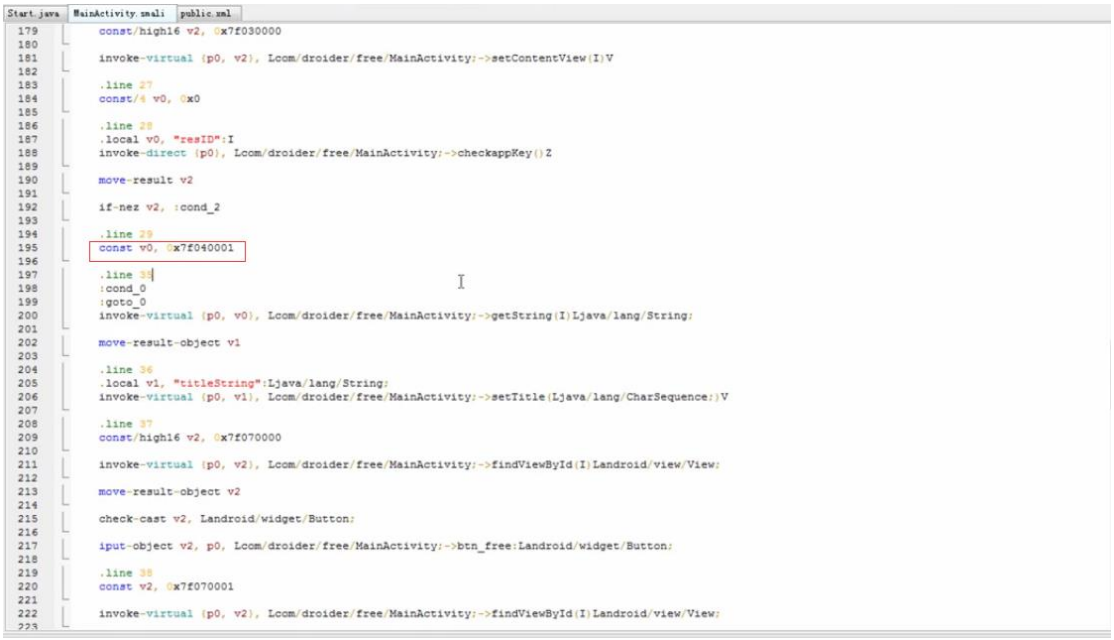


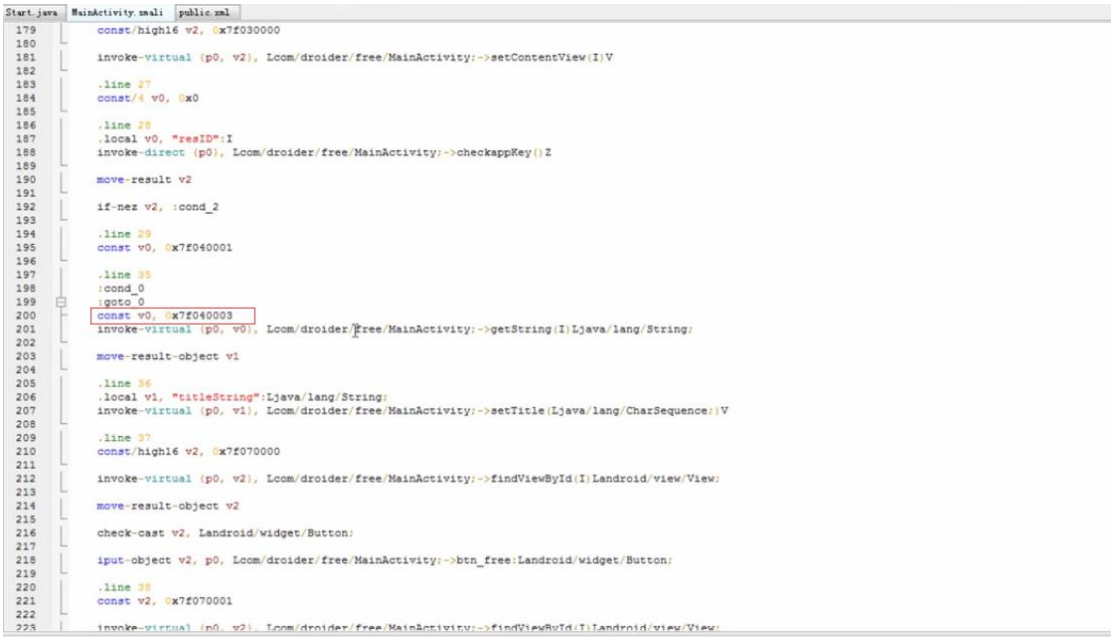
```
179     const/high16 v2, 0x7f030000
180
181     invoke-virtual {p0, v2}, Lcom/droider/free/MainActivity;->setContentView(I)V
182
183     .line 27
184     const/4 v0, 0x0
185
186     .line 28
187     .local v0, "resID":I
188     invoke-direct {p0}, Lcom/droider/free/MainActivity;->checkappKey()Z
189
190     move-result v2
191
192     if-nez v2, :cond_2
193
194     .line 29
195     const v0, 0x7f040001
196
197     .line 35
198     :cond_0
199     :goto_0
200     invoke-virtual {p0, v0}, Lcom/droider/free/MainActivity;->getString(I)Ljava/lang/String;
201
202     move-result-object v1
203
204     .line 36
205     .local v1, "titleString":Ljava/lang/String;
206     invoke-virtual {p0, v1}, Lcom/droider/free/MainActivity;->setTitle(Ljava/lang/CharSequence;)V
207
208     .line 37
209     const/high16 v2, 0x7f070000
210
211     invoke-virtual {p0, v2}, Lcom/droider/free/MainActivity;->findViewById(I)Landroid/view/View;
212
213     move-result-object v2
214
215     check-cast v2, Landroid/widget/Button;
216
217     iput-object v2, p0, Lcom/droider/free/MainActivity;->btn_free:Landroid/widget/Button;
218
219     .line 38
220     const v2, 0x7f070001
221
222     invoke-virtual {p0, v2}, Lcom/droider/free/MainActivity;->findViewById(I)Landroid/view/View;
```





将 v0 置为专业版的密钥

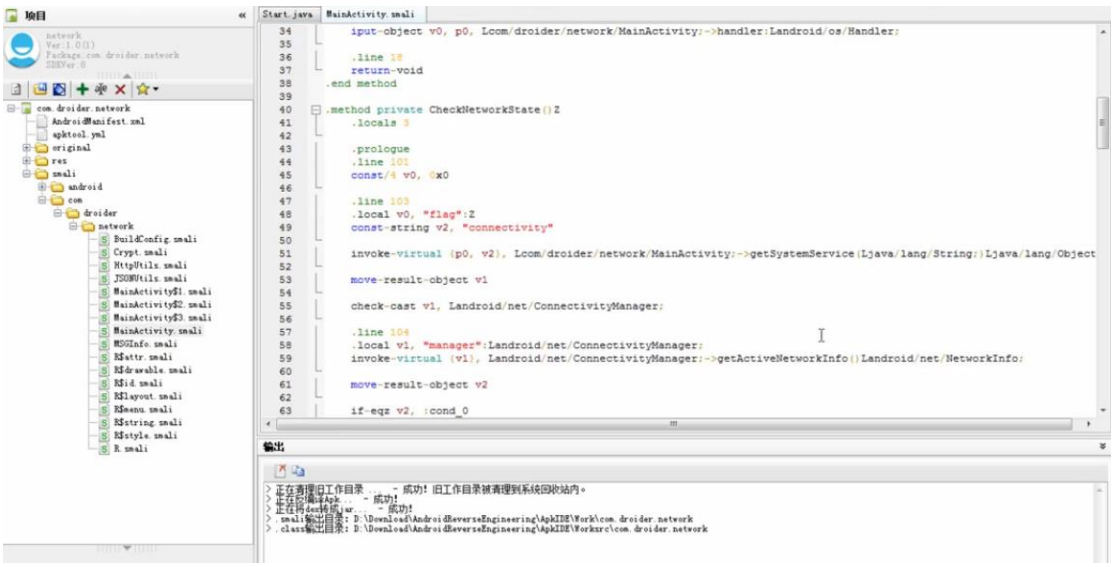




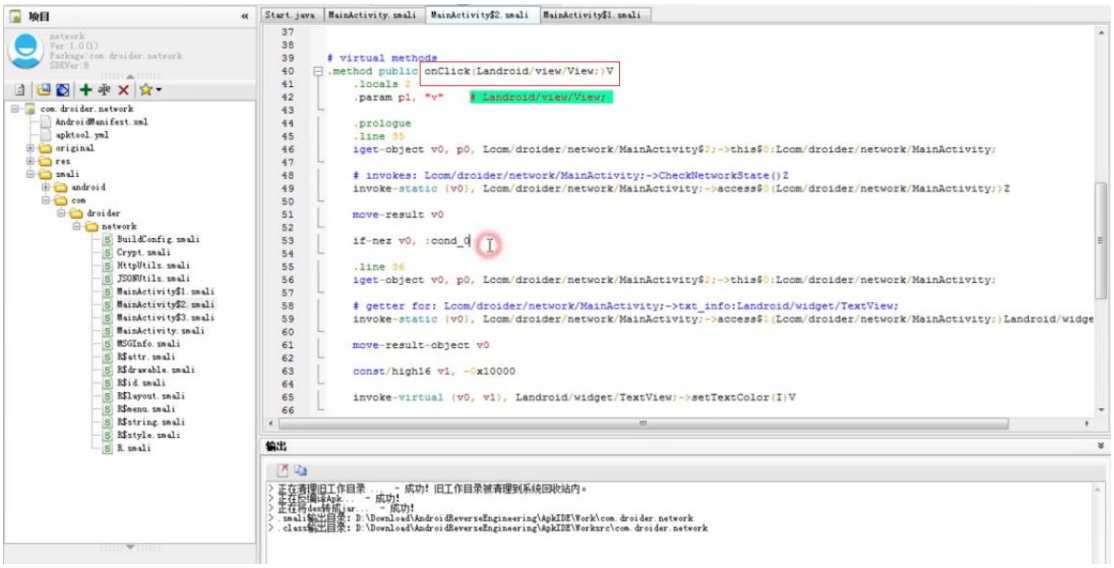
保存后重新编译，破解成功

2. **网络验证**

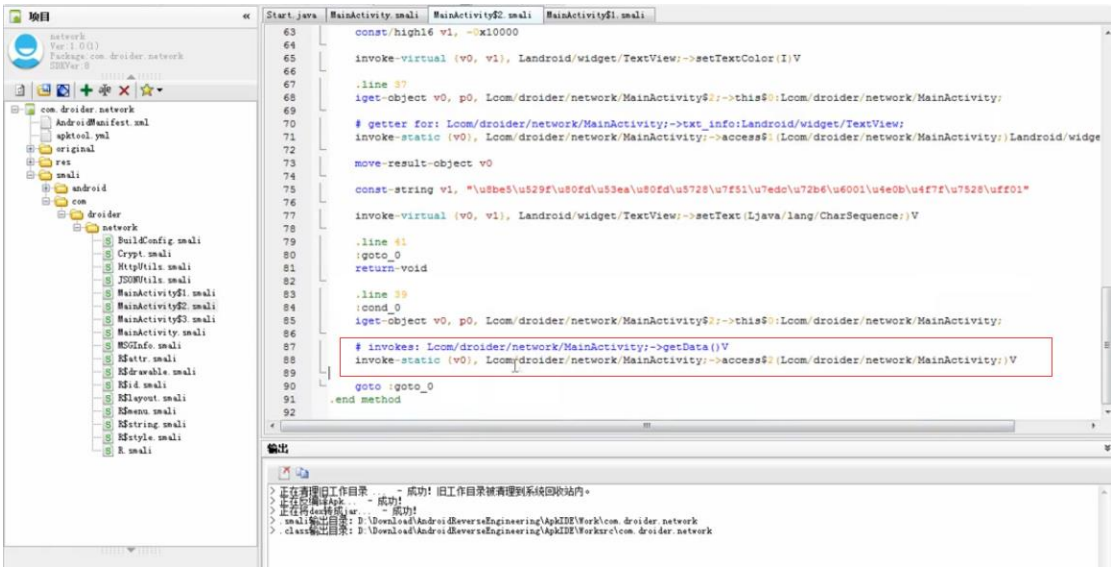
使用 apkIde 对目标 app 进行反编译操作



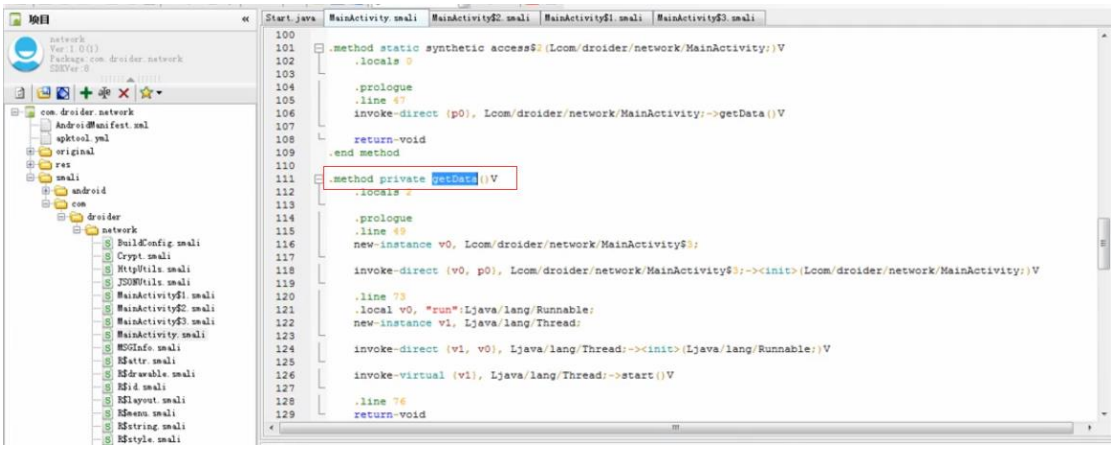
定位到点击函数中，分析其中的操作



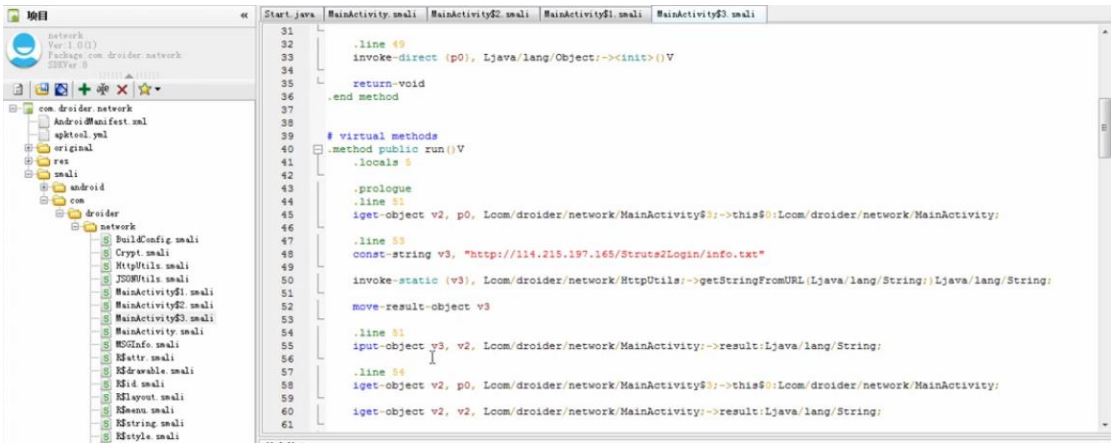
找到网络连接成功后进行的操作

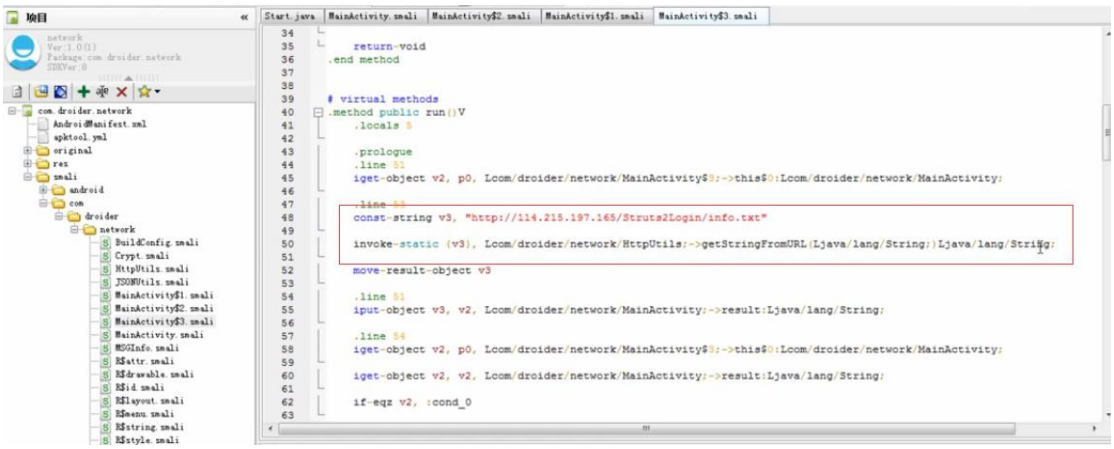


定位到 getData()函数

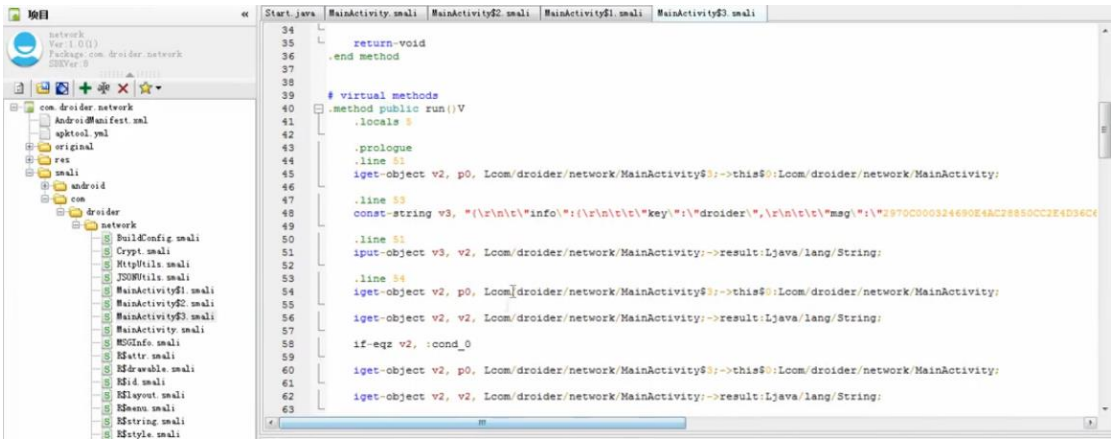


找到网络 URL 相关的函数

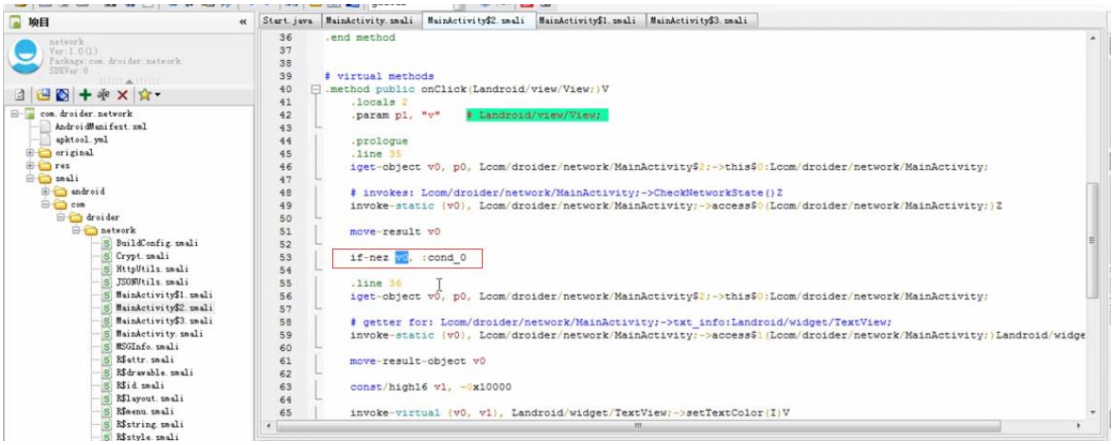


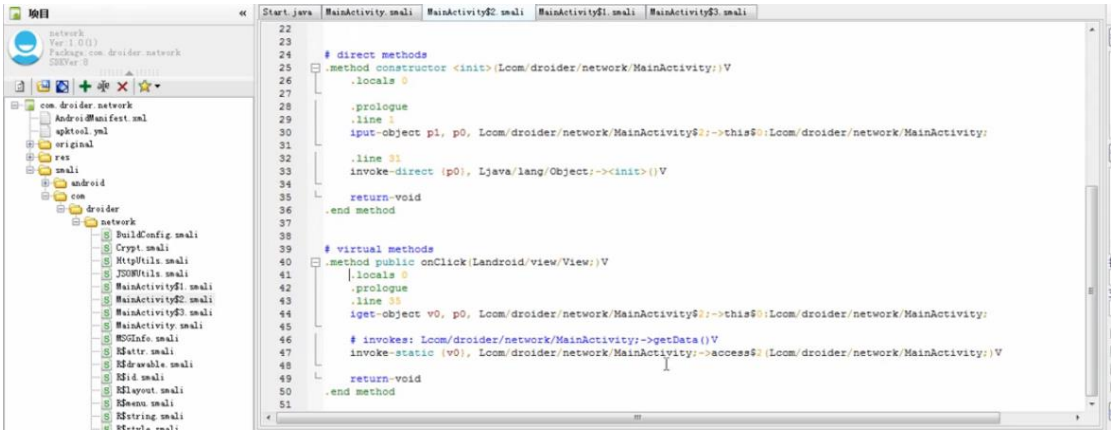


对参数 v3 进行修改，将网络链接中的内容直接写入



然后对判断网络状态的内容进行修改





重新编译后安装运行，绕过了联网验证