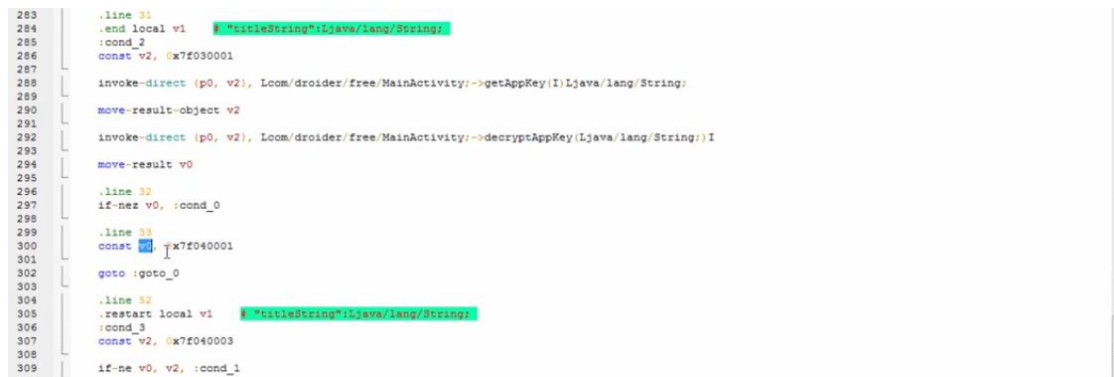
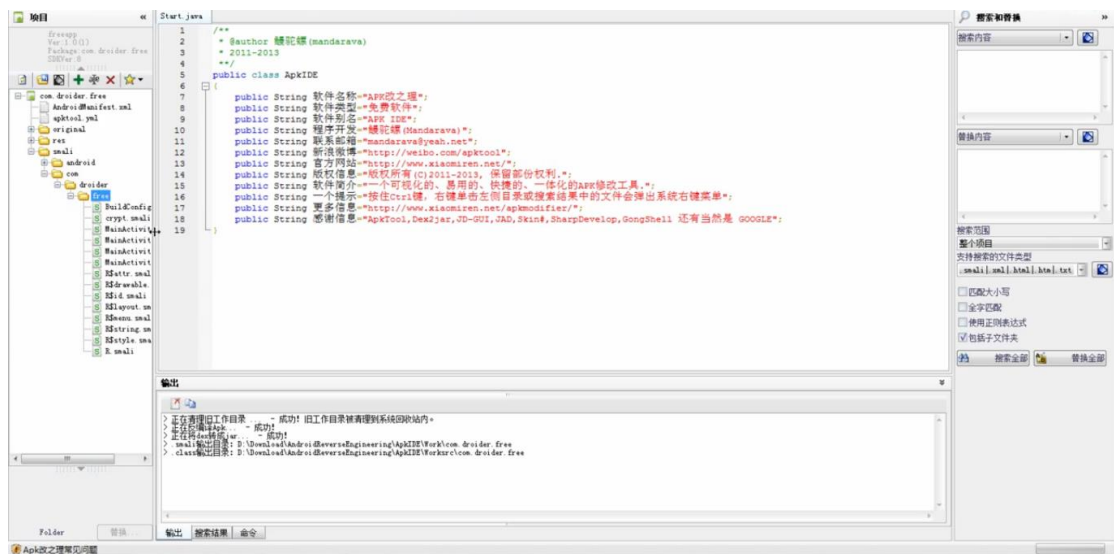
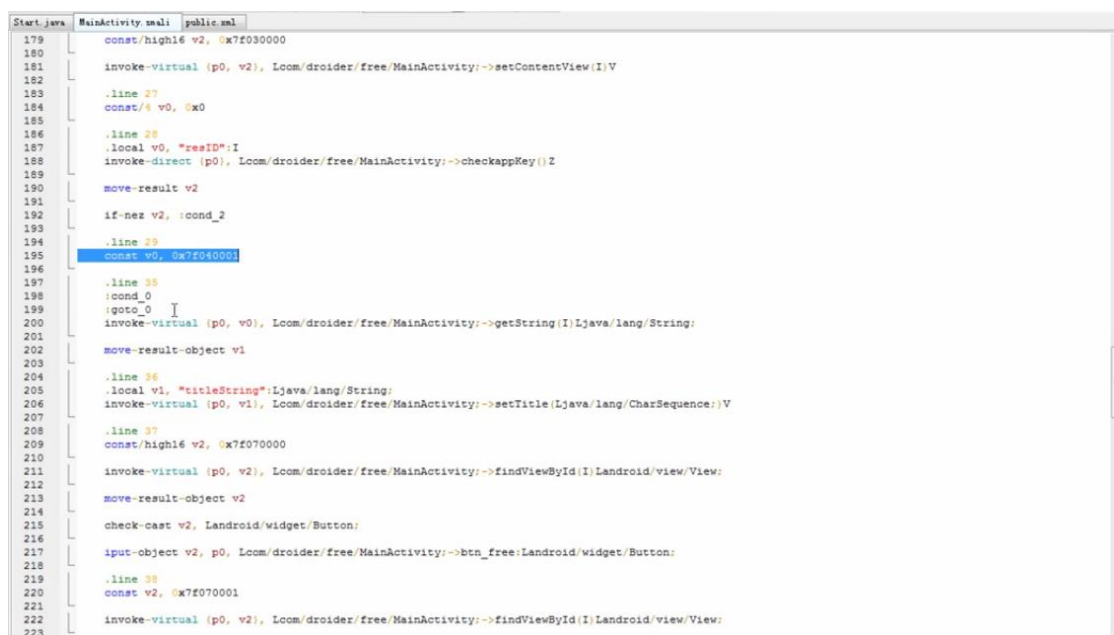


1. 试用版软件破解

使用 ApkIde 打开要破解的 app 进行反编译



分别显示各个按钮的相关 smali 代码



```
Start.java MainActivity.smali public.smali
221
222     invoke-virtual {p0, v2}, Lcom/droider/free/MainActivity;->findViewById(I)Landroid/view/View;
223
224     move-result-object v2
225
226     check-cast v2, Landroid/widget/Button;
227
228     iput-object v2, p0, Lcom/droider/free/MainActivity;.>btn_advanced:Landroid/widget/Button;
229
230     .line 39
231     const v2, 0x7f070002
232
233     invoke-virtual {p0, v2}, Lcom/droider/free/MainActivity;->findViewById(I)Landroid/view/View;
234
235     move-result-object v2
236
237     check-cast v2, Landroid/widget/Button;
238
239     iput-object v2, p0, Lcom/droider/free/MainActivity;.>btn_pro:Landroid/widget/Button;
240
241     .line 40
242     const v2, 0x7f040002
243
244     if-ne v0, v2, :cond_3
245
246     .line 51
247     iget-object v2, p0, Lcom/droider/free/MainActivity;.>btn_advanced:Landroid/widget/Button;
248
249     invoke-virtual {v2, v3}, Landroid/widget/Button;.>setVisibility(I)V
250
251     .line 57
252     :cond_1
253     :goto_1
254     iget-object v2, p0, Lcom/droider/free/MainActivity;.>btn_free:Landroid/widget/Button;
255
256     new-instance v3, Lcom/droider/free/MainActivity$1;
257
258     invoke-direct {v3, p0}, Lcom/droider/free/MainActivity$1;.><init>(Lcom/droider/free/MainActivity;)V
259
260     invoke-virtual {v2, v3}, Landroid/widget/Button;.>setOnClickListener(Landroid/view/View$OnClickListener;)V
261
262     .line 66
263     iget-object v2, p0, Lcom/droider/free/MainActivity;.>btn_advanced:Landroid/widget/Button;
264
265     new-instance v3, Lcom/droider/free/MainActivity$2;
266
267     return-void
268
269     .line 31
270     .end local v1
271     :cond_2
272     const v2, 0x7f030001
273
274     invoke-direct {p0, v2}, Lcom/droider/free/MainActivity;.>getAppKey(I)Ljava/lang/String;
275
276     move-result-object v2
277
278     invoke-direct {p0, v2}, Lcom/droider/free/MainActivity;.>decryptAppKey(Ljava/lang/String;)I
279
280     move-result v0
281
282     .line 32
283     if-nez v0, :cond_0
284
285     .line 33
286     const v0, 0x7f040001
287
288     goto :goto_0
289
290     .line 52
291     .restart local v1
292     :cond_3
293     const v2, 0x7f040003
294
295     if-ne v0, v2, :cond_1
296
297     .line 53
298     iget-object v2, p0, Lcom/droider/free/MainActivity;.>btn_advanced:Landroid/widget/Button;
299
300     invoke-virtual {v2, v3}, Landroid/widget/Button;.>setVisibility(I)V
301
302     .line 54
303     iget-object v2, p0, Lcom/droider/free/MainActivity;.>btn_pro:Landroid/widget/Button;
304
305     invoke-virtual {v2, v3}, Landroid/widget/Button;.>setVisibility(I)V
306
307     goto :goto_1
308
309     .end method
310
311     .method public onCreateOptionsMenu(Landroid/view/Menu;)Z
312     .local v1
313     .line 2
314     .end local v1
315     .end method
```

将 v0 置为专业版的密钥

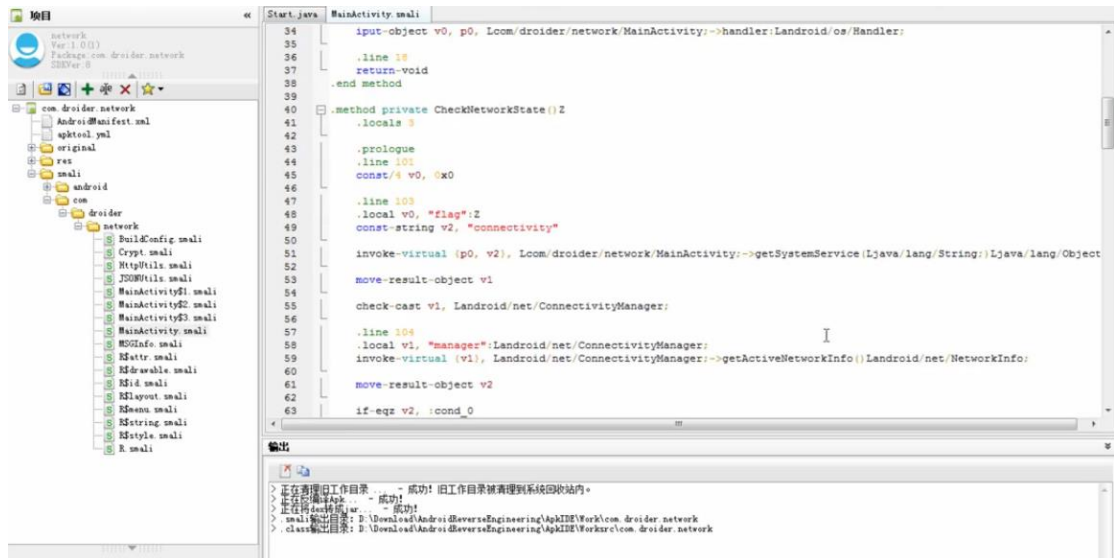
Start.java	MainActivity.smali	public.xml
179	const/high16 v2, 0x7f030000	
180		
181	invoke-virtual {p0, v2}, Loom/droider/free/MainActivity;~>setContentView(I)V	
182		
183	.line 27	
184	const/4 v0, 0x0	
185		
186	.line 28	
187	.local v0, "resID":I	
188	invoke-direct {p0}, Loom/droider/free/MainActivity;~>checkAppKey()Z	
189		
190	move-result v2	
191		
192	if-nez v2, :cond_2	
193		
194	.line 29	
195	const v0, 0x7f040001	
196		
197	.line 30	
198	:cond_0	
199	:goto_0	
200	invoke-virtual {p0, v0}, Loom/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}, Loom/droider/free/MainActivity;~>setTitle(Ljava/lang/CharSequence;)V	
207		
208	.line 37	
209	const/high16 v2, 0x7f070000	
210		
211	invoke-virtual {p0, v2}, Loom/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, Loom/droider/free/MainActivity;~>btn_free:Landroid/widget/Button;	
218		
219	.line 38	
220	const v2, 0x7f070001	
221		
222	invoke-virtual {p0, v2}, Loom/droider/free/MainActivity;~>findViewById(I)Landroid/view/View;	
223		

Start.java	MainActivity.smali	public.xml
179	const/high16 v2, 0x7f030000	
180		
181	invoke-virtual {p0, v2}, Loom/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}, Loom/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	const v0, 0x7f040003	
201	invoke-virtual {p0, v0}, Loom/droider/free/MainActivity;~>getString(I)Ljava/lang/String;	
202		
203	move-result-object v1	
204		
205	.line 36	
206	.local v1, "titleString":Ljava/lang/String;	
207	invoke-virtual {p0, v1}, Loom/droider/free/MainActivity;~>setTitle(Ljava/lang/CharSequence;)V	
208		
209	.line 37	
210	const/high16 v2, 0x7f070000	
211		
212	invoke-virtual {p0, v2}, Loom/droider/free/MainActivity;~>findViewById(I)Landroid/view/View;	
213		
214	move-result-object v2	
215		
216	check-cast v2, Landroid/widget/Button;	
217		
218	iput-object v2, p0, Loom/droider/free/MainActivity;~>btn_free:Landroid/widget/Button;	
219		
220	.line 38	
221	const v2, 0x7f070001	
222		
223	invoke-virtual {p0, v2}, Loom/droider/free/MainActivity;~>findViewById(I)Landroid/view/View;	

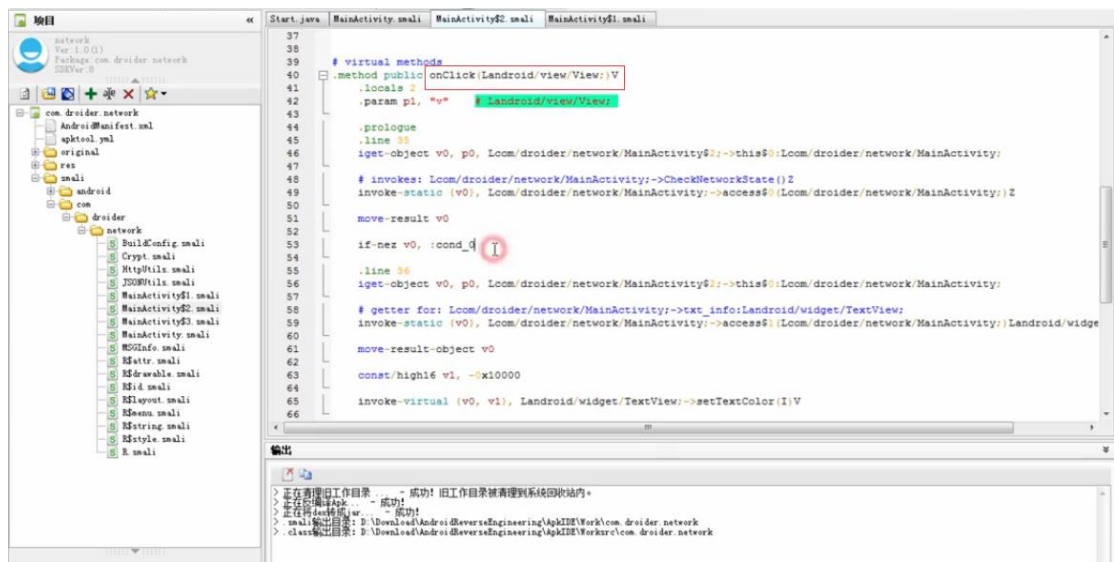
保存后重新编译，破解成功

2. 网络验证

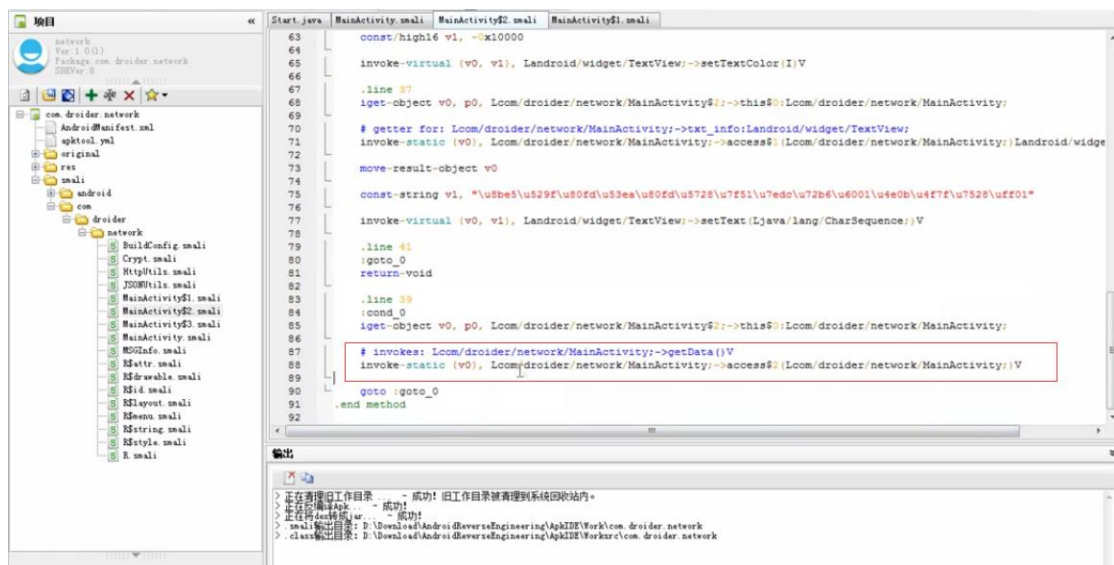
使用 apkIde 对目标 app 进行反编译操作



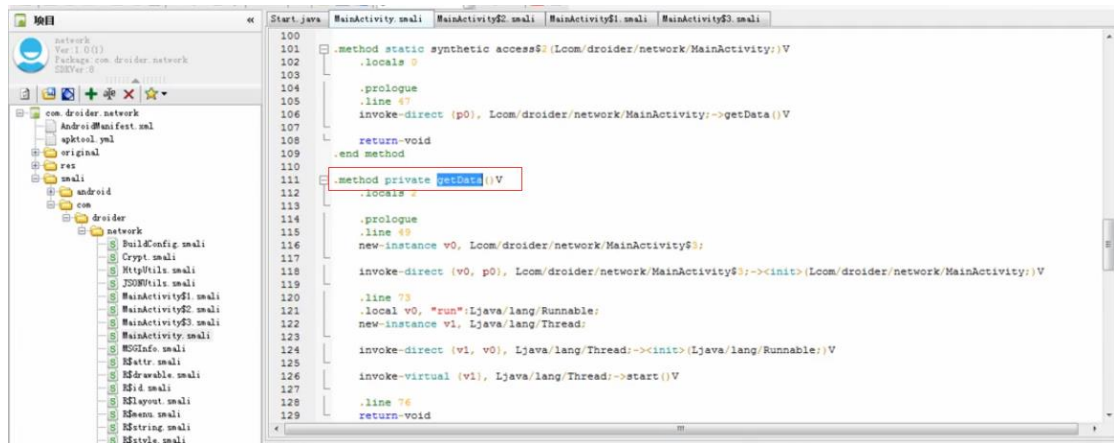
定位到点击函数中，分析其中的操作



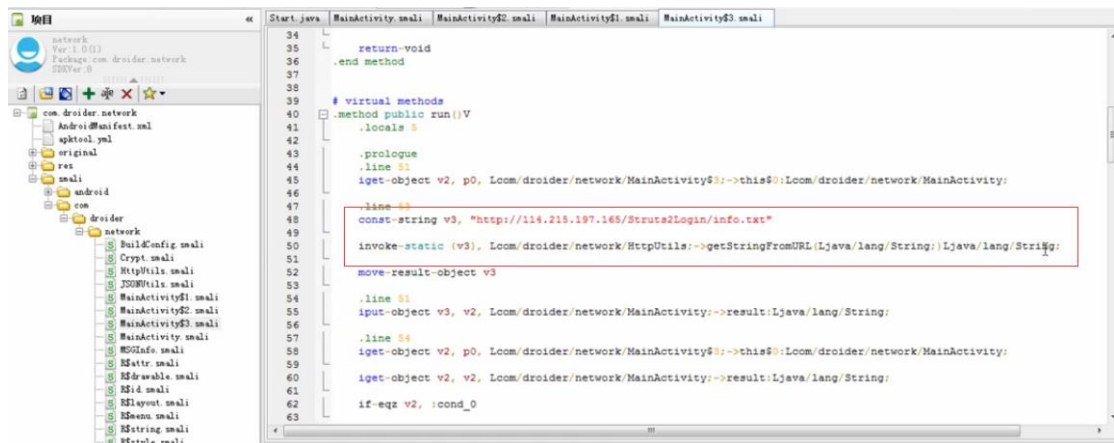
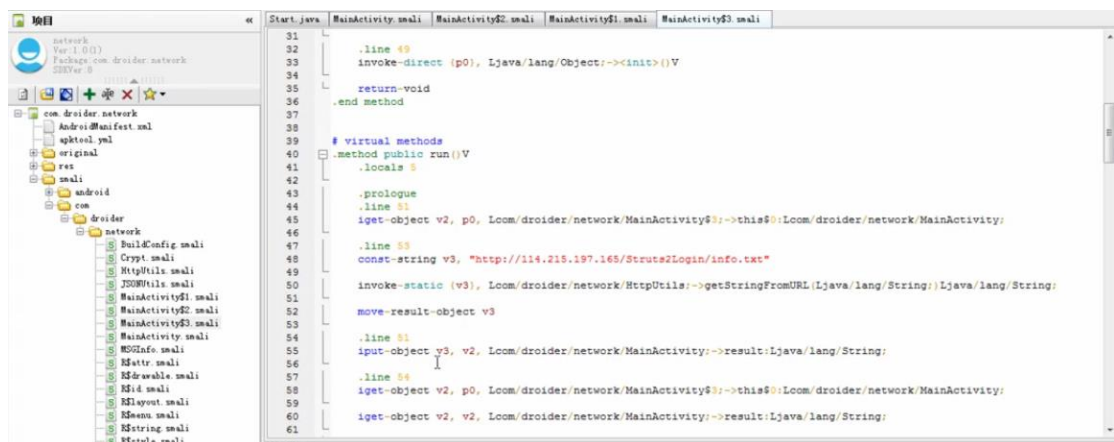
找到网络连接成功后进行的操作



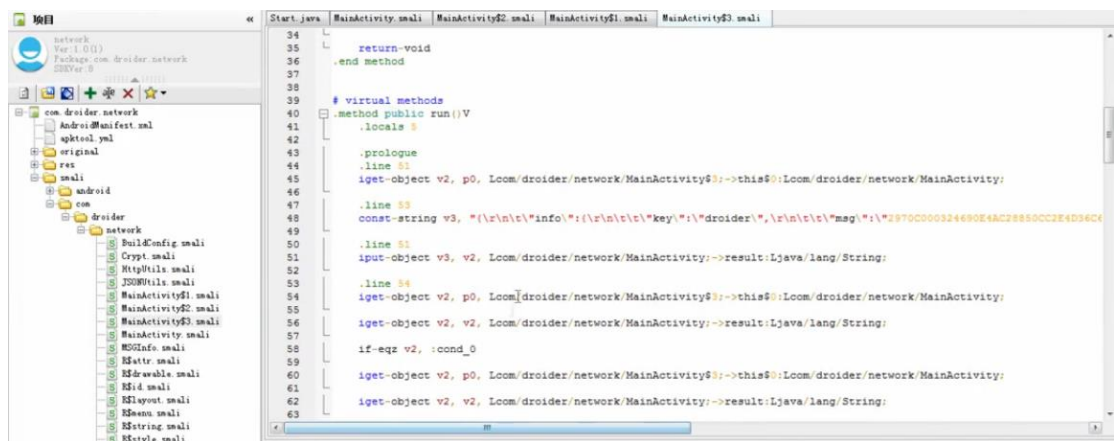
定位到 getData()函数



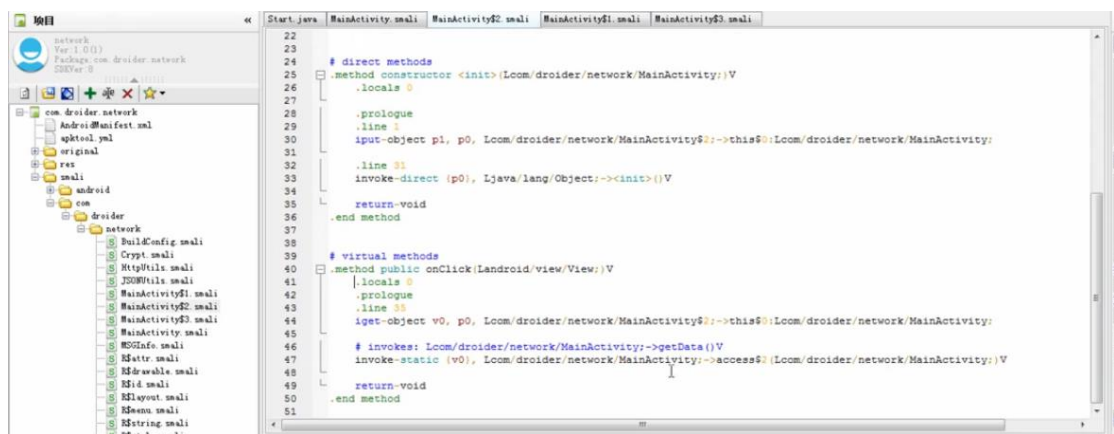
找到网络 URL 相关的函数



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