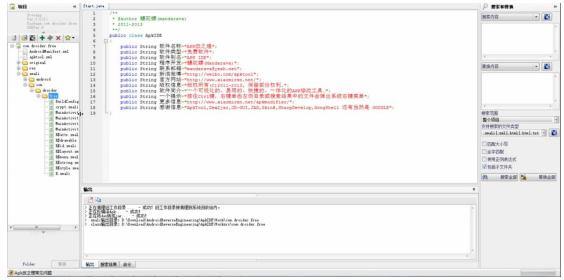
1. 试用版软件破解

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

```
invoke-virtual (p0, v2), Lcom/droider/free/MainActivity;->findViewById(I)Landroid/view/View;
                                 check-cast v2, Landroid/widget/Button;
                                 iput-object v2, p0, Lcom/droider/free/MainActivity;->btn_advanced:Landroid/widget/Button;
                                  invoke-virtual (p0, v2), Lcom/droider/free/MainActivity;->findViewById(I)Landroid/view/View;
                                   check-cast v2, Landroid/widget/Button;
                                   iput-object v2, p0, Lcom/droider/free/MainActivity;->btn_pro:Landroid/widget/Button;
                                    .line 51 iget-object v2, p0, Lcom/droider/free/MainActivity;->btn_advanced:Landroid/widget/Button;
                                   invoke-virtual~(v2,~v3),~Landroid/widget/Button; ->setVisibility(I)\,V
                                   .line 57
:cond_1
:goto_1
iget-object v2, p0, Loms/droider/free/MainActivity:->btn_free:Landroid/widget/Button;
                                   new-instance v3, Lcom/droider/free/MainActivity$1;
                                   invoke-direct (v3, p0), Loom/droider/free/MainActivity$1;-><init>(Loom/droider/free/MainActivity;)V
                                    invoke-virtual~\{v2,~v3\},~Landroid/widget/Button; -> setOnClickListener\\ (Landroid/view/View$OnClickListener;) \\ View$ConClickListener, and the contract of t
                                    .line 66
iget-object v2, p0, Loom/droider/free/MainActivity;->btn_advanced:Landroid/widget/Button;
                                   new-instance_v3. Lcom/droider/free/MainActivitu$2:
 Start java MainActivity smali public sml
   .line 31
.end local v1 # "t
:cond_2
const v2, %x7f030001
                           invoke-direct (p0, v2), Lcom/droider/free/MainActivity:->getAppKey(I)Ljava/lang/String:
                          move-result-object v2
                          invoke-direct (p0, v2), Lcom/droider/free/MainActivity;->decryptAppKey(Ljava/lang/String;)I
                          move-result v0
                          .line 32
if-nez v0, :cond_0
                           .line 33
const v0, 0x7f040001
                          goto :goto_0
                            line 52
restart local v1
                          const v2, 0x7f040003
                            if-ne v0, v2, :cond_1
                           .line 55
iget-object v2, p0, Lcom/droider/free/MainActivity;->btn_advanced:Landroid/widget/Button;
                           invoke-virtual (v2, v3), Landroid/widget/Button;->setVisibility(I)V
                            :line 54
iget-object v2, p0, Loom/droider/free/MainActivity:->_cin_pro}:Landroid/widget/Button;
                           invoke-virtual (v2, v3), Landroid/widget/Button;->setVisibility(I)V
              .method public onCreateOptionsMenu(Landroid/view/Menu;)2
```

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

```
    Start_javs MaisActivity.mali
    34 iput-object v0, p0, Lcom/droider/network/MainActivity:->handler:Landroid/os/Handler
16日
                                                                                                                                                                                                                                                                                        34
35
36
37
38
38
39
40
41
42
43
44
45
46
47
48
49
55
51
52
53
54
65
77
88
60
61
62
62
      hetwork
Ver'l 0(1)
Package com dreider network
SBEVer 8
    3 4 × × 4-
               con. droider. network
Android Stanifest. mal
aptical. mal
res
android
con
droider
network
Buildoc
                                                                                                                                                                                                                                                                                                                                      .method private CheckNetworkState() 2
                                                                                                                                                                                                                                                                                                                                                                                   .prologue
.line 101
const/4 v0, 0x0
                                                                                                 order

| butwerk |
| buildonfig mali |
| Crypt mali |
| Minattivity |
| Somfilia mali |
| Minattivity |
| Minattiv
                                                                                                                                                                                                                                                                                                                                                                                 invoke-virtual (p0, v2), Lcom/droider/network/MainActivity:->getSystemService(Ljava/lang/String:)Ljava/lang/Object
                                                                                                                                                                                                                                                                                                                                                                               move-result-object v1
                                                                                                                                                                                                                                                                                                                                                                               check-cast v1, Landroid/net/ConnectivityManager;
                                                                                                                                                                                                                                                                                                                                                                                   .line 104 .local v1, "manager":Landroid/net/ConnectivityManager; I .local v1, "manager":Landroid/net/ConnectivityManager; OtherworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/net/NetworkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Landroid/networkInfo()Lan
                                                                                                                                                                                                                                                                                                                                                                                   move-result-object v2
                                                                                                                                                                                                                                                                                                                                                                                   if-eqz v2, :cond 0
                                                                                                                                                                                                                                                                                        编出
```

定位到点击函数中,分析其中的操作

```
ec Start.java | MainActivity. smali | MainActivity$2. smali | MainActivity$1. smali |
                                                                             37
38
40
41
42
43
44
45
46
47
48
49
50
51
52
53
55
56
67
66
66
66
 natwork
Ver:1.0(1)
Package com droider natwork
SDEVer:0
                                                                                      ② (□ 🐼 + ※ × ☆・
con droider network
Android unifest mal
spheol yel
original
                                                                                                   .line 35 iget-object v0, p0, Lcom/droider/network/MainActivity%3;->this$0:Lcom/droider/network/MainActivity
                ord

froider

broider

Studiosofig mali

Grypt mali

Stryptills mali

Studiosofig mali
                                                                                                   # invokes: Lccm/droider/network/MainActivity;->CheckNetworkState() Z
invoke-static (v0), Lccm/droider/network/MainActivity;->access$0(Lccm/droider/network/MainActivity;) Z
                                                                                                  move-result v0
                                                                                                  if-nez v0, :cond_d
                                                                                                  .line 36
iget-object v0, p0, Lcom/droider/network/MainActivity$2;->this$0:Lcom/droider/network/MainActivity;
                                                                                                   # getter for: Lcom/droider/network/MainActivity;->txt info:Landroid/widget/TextView;
invoke-static [v0], Lcom/droider/network/MainActivity;->access$\[\(\)(Lcom/droider/network/MainActivity;\)\Landroid/widge
                                                                                                  const/high16 vl. -0x10000
                                                                                                 invoke-virtual (v0, v1), Landroid/widget/TextView;->setTextColor(I)V
                                                                          编出
                                                                           70
```

找到网络连接成功后进行的操作

```
ec Start java MainActivity smali MainActivity$2 smali MainActivity$1 smali
                                                                                                                                                                                                                                                                                                      const/high16 v1, -0x10000
                                                                                                                                                                                                                                     invoke-virtual~(v0,~v1),~Landroid/widget/TextView; ->setTextColor(I) V
.line 57 iget-object v0, p0, Lcom/droider/network/MainActivity$2;->this$0:Lcom/droider/network/MainActivity;
     con. droider. network
Android Smifest. mal
spattod. yel
res
mali
sudroid
con
droider
network
                                                                                                                                                                                                                                                                                                 # getter for: Loom/droider/network/MainActivity;->txt_info:Landroid/widget/TextView;
invoke-static (v0), Loom/droider/network/MainActivity;->access%!(Loom/droider/network/MainActivity;)Landroid/widget/network/MainActivity;)
                                                                                                                                                                                                                                                                                               const-string v1, "\u8be5\u529f\u80fd\u53ee\u80fd\u5728\u7f51\u7edo\u72b6\u6001\u4e0b\u4f7f\u7528\uff01
                                                                      reider

menterik

ferstenik

fryst mali

fryst mali

fryst mali

fryst mali

fryst mali

fryst mali

mandetiviyd: mali

mandeti
                                                                                                                                                                                                                                                                                                 invoke-virtual (v0, v1), Landroid/widget/TextView;->setText(Ljava/lang/CharSequence;)V
                                                                                                                                                                                                                                                                                                 .line 41
:goto_0
return-void
                                                                                                                                                                                                                                                                                                    .line 39 | loomd 0 | loom/droider/network/MainActivity$2;->this$0:Loom/droider/network/MainActivity; | loom/droider/network/MainActivity; | loom/droider/networ
                                                                                                                                                                                                                                                                                                    # invokes: Lcom/droider/network/MainActivity;->getData()V
invoke-static (v0), Lcom/droider/network/MainActivity;)VainActivity;)VainActivity;)V
                                                                                                                                                                                                                                                                          goto :goto_0
.end method
                                                                                                                                                                                                                         编出
                                                                                                                                                                                                                                 正在書灣日工作目录 — 成功! 日工作目录被清禮受紙使回收站內。
正在記憶本种水 — 成功! 
正在明本选择 — 成功: — 成功!
- mail版工目表: D. Uponalod/kadroidkoversellagiasering/kakIEEUwrk.com. droider. network
class版工目表: D. Uponalod/kadroidkoversellagiasering/kakIEEUwrkzrc/com. droider. network
```

定位到 getData()函数

```
« Start.java MainActivity. smali MainActivity$2. smali MainActivity$1. smali MainActivity$3. smali
con draider nature?

Andreider nature?

Andreider nature?

Andreider nature?

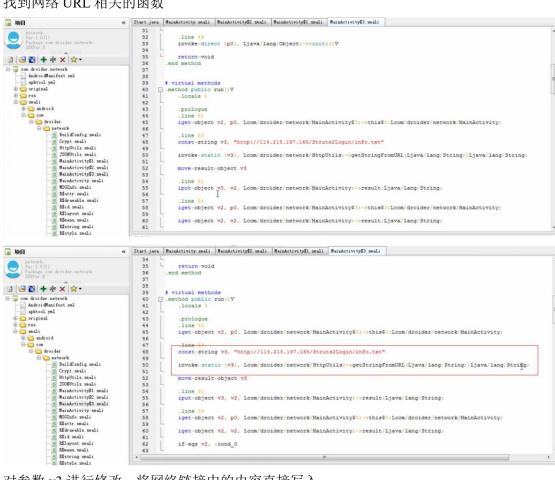
Andreider nature?

Andreider nature?

Andreider nature?

Smith of the control 
                                                                                                                                                                                                                   ☐ .method static synthetic access$2(Lcom/droider/network/MainActivity;)♥
.locals 0
                                                                                                                                                                                                                                                     .prologue .line 47 invoke-direct (p0), Lcom/droider/network/MainActivity;->getData()V
                                                                                                                                                                                             104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
                                                                                                                                                                                                                                       return-void
                                                                                                                                                                                                                   method private getData () V
                                                                                                                                                                                                                                                 .prologue
.line 49
new-instance v0, Loom/droider/network/MainActivity$5;
                                                                                                                                                                                                                                              invoke-direct (v0, p0), Lcom/droider/network/MainActivity$3;-><init>(Lcom/droider/network/MainActivity;)V
                                                                                                                                                                                                                                                 invoke-direct (v1, v0), Ljava/lang/Thread:-><init>(Ljava/lang/Runnable:)V
                                                                                                                                                                                                                                                    invoke-virtual (v1), Ljava/lang/Thread;->start()V
```

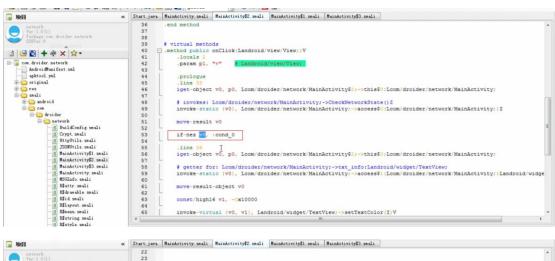
找到网络 URL 相关的函数

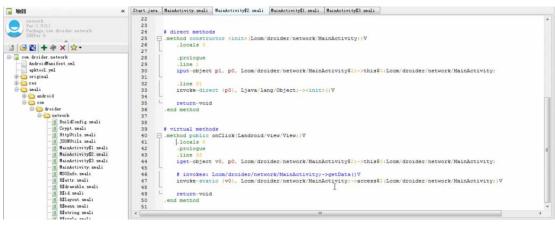


对参数 v3 进行修改,将网络链接中的内容直接写入

```
| Start java | Maindativity, small | Maindativity | Small |
```

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