UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escola Tècnica Superior d'Enginyeria **Informàtica**

3. Ingeniería inversa de aplicaciones móviles Android

Ciberseguridad en Dispositivos móviles
DISCA – ETS de Ingeniería informática (UPV)

Indice

- ¿Qué es Android? Conceptos básicos
- Anatomía de una app Android sencilla
- Herramientas para el desarrollo y emulación de apps Android
- Reversing de apks
- **Smali y parcheado de apks**

Código Smali

- Lo trabajaremos en prácticas

```java
@Override
public void onClick(View v) {

    startActivity(new Intent(getApplicationContext(), LoginActivity.class));

}
```

```
# virtual methods
.method public onClick(Landroid/view/View;)V
    .locals 3

    .line 26
    iget-object p1, p0, Les/upv/cdm/jcruizg/holamundo/MainActivity$1;->this$0:Les/upv/cdm/jcruizg/holamundo/MainActivity;

    new-instance v0, Landroid/content/Intent;

    invoke-virtual {p1}, Les/upv/cdm/jcruizg/holamundo/MainActivity;->getApplicationContext()Landroid/content/Context;
    move-result-object v1
    const-class v2, Les/upv/cdm/jcruizg/holamundo/LoginActivity;
    invoke-direct {v0, v1, v2}, Landroid/content/Intent;-><init>(Landroid/content/Context;Ljava/lang/Class;)V
    invoke-virtual {p1, v0}, Les/upv/cdm/jcruizg/holamundo/MainActivity;->startActivity(Landroid/content/Intent;)V

    return-void
.end method
```

https://github.com/JesusFreke/smali

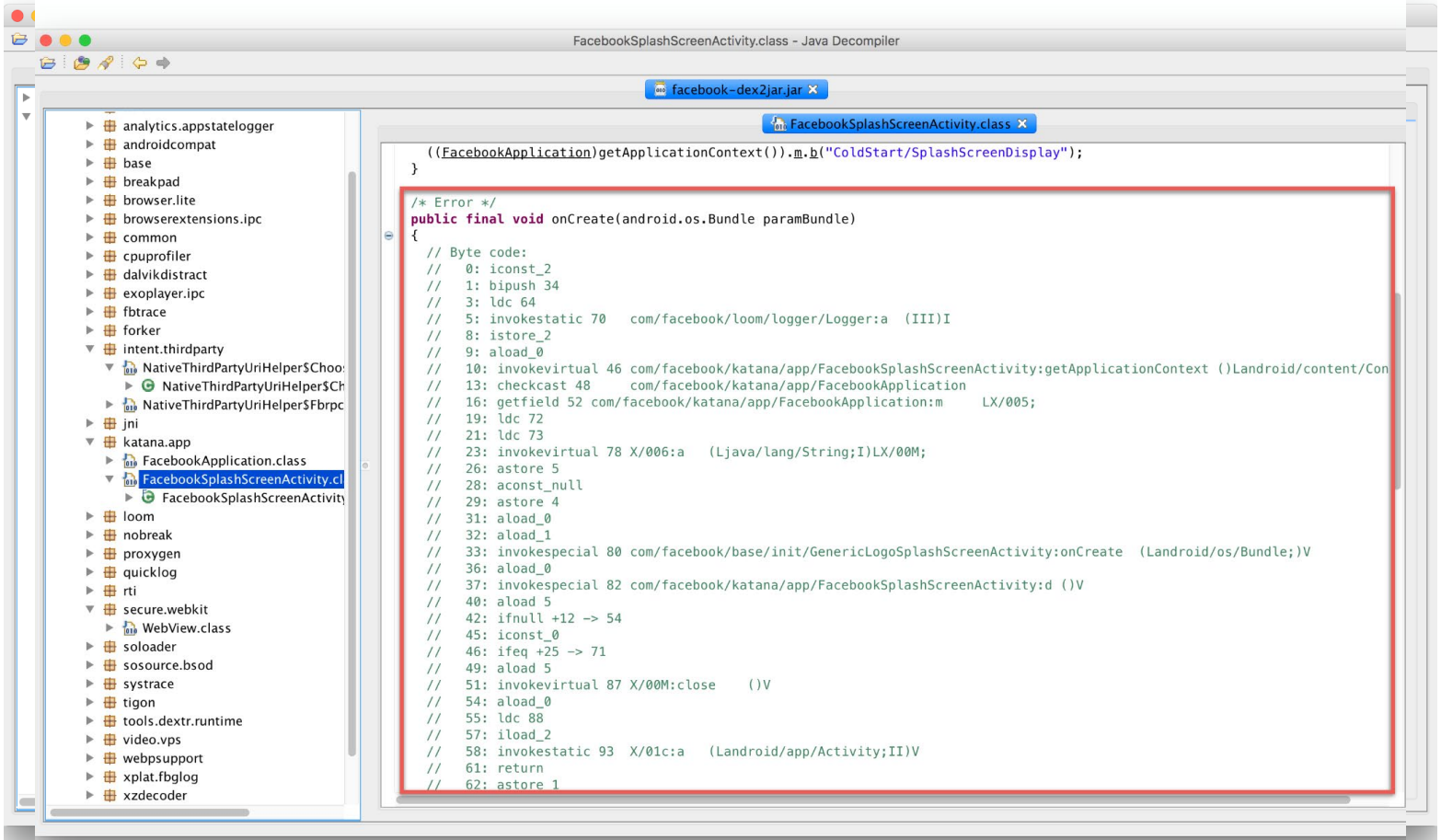
¿Qué es Smali?

- Cuando se crea una aplicación Android su apk contiene un fichero .dex, que contiene su bytecode Dalvik en formato binario
- Smali es el lenguaje de ensamblador que puede ejecutar una máquina virtual Dalvik
- Como ya hemos visto la aplicación apktool permite desensamblar un apk para obtener, entre otras cosas, su código smali

Fuentes de información

- Métodos, clases, tipos primitivos y campos de clases en Smali
  - https://github.com/JesusFreke/smali/wiki/TypesMethodsAndFields
- Operaciones que pueden usarse si se programa en Smali
  - http://pallergabor.uw.hu/androidblog/dalvik_opcodes.html
- A quick guide to Android app reversing
  - http://pages.cpsc.ucalgary.ca/~joel.reardon/mobile/smali-cheat.pdf
- Muy buena introducción con explicaciones y ejemplos paso a paso
  - https://github.com/hqt/reverse-engineering/blob/master/slide/android%20reverse%20slide.pdf

Java vs Smali



https://github.com/hqt/reverse-engineering

Tipos de datos

V	Void
Z	Boolean
B	byte
S	short
C	char
I	int
J	long (64 bits)
F	float
D	double (64 bits)

Lpackage1/package2/`className;`

```
package com.hqt.model;
class Person {
}
```

Lcom/hqt/model/ `Person;`

https://github.com/hqt/reverse-engineering

Llamadas a método

action {param1, param2}, LpackageName/ClassName;->
methodName(paramType1; paramType2)ReturnType

Log.e("hqthao", "Hello World")

```
const-string v1, "hqthao"
const-string v2, "Hello World"
invoke-static {v1, v2}, Landroid/util/Log;->e(Ljava/lang/String;Ljava/lang/String;)I
```

https://github.com/hqt/reverse-engineering

Herramientas disponibles

- APK Studio lo auna todo, pero requiere:
  - apktool (desemsanblar: dex→smali)
  - jadx (decompilar: dex → java)
  - keytool (generación de keystores)
  - Firma del apk
    - uber-apk-signer
    - apksigner (android build-tools)
- Android Studio también permite analizar y depurar un apk

grep es nuestro mejor amigo

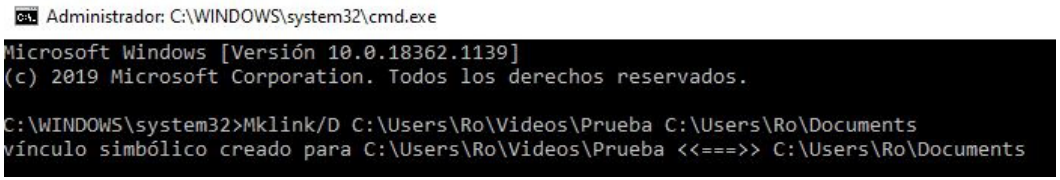
- ¿Y por qué?
  - Porque va a ser un complemento ideal en la búsqueda de strings dentro del código smali que tengamos que examinar

cadena de texto a buscar

```
grep -inr facebook.com --include=*.smali

-i ignores character case
-n display line numbers
-r recursive, search sub folders
--include=*.smali only search files matching
--color=always add coloring
```

- Si trabajáis en Windows
  - Opción 1: podéis hacer uso de findstr, pero no es tan potente
  - Opción 2: instalad Cygwin y trabajar sobre el directorio donde se encuentre el apk desde el terminal de Cygwin
    - Muy útil: podéis generar un enlace simbólico que una vuestro /home/user con cualquier directorio de vuestra máquina



Búsquedas con grep (1/4)

- Trackers
  (monitorizan la ejecución de apps)

facebook *google.com* *firebase*

urbanairship *crahlytics* *bugfender*

*track** *analytic** *ads* *…*

Búsquedas con grep (2/4)

- APIs intrusivas que ponen en juego la privacidad que ofrece una app

QueryIntentActivities *getRunningAppProcesses*

ActivityManager *PackageManager*

WifiManager *SensorManager*

BluetoothManager *Address*

LocationManager *TelephonyManager*

AdvertisingIdClient

Búsquedas con grep (3/4)

- Red (E/S)

http *https*

connect *socket* *uri* *address*

opost *.com/.net* *loadUrl*

Búsquedas con grep (4/4)

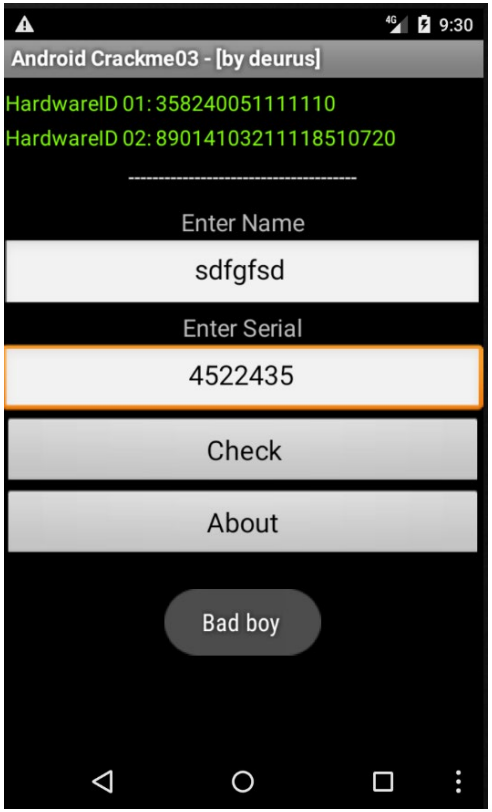
- Llamadas sospechosas / peligrosas

loadLibrary *native*

install *addJavaScriptInterface*

Caso de estudio 1

- Crackme03.apk
  - Disponible en https://deurus.info/archivos/mycrackmes y en PoliformaT (CDM)
  - Por cuestiones de permisos la app no funciona con versiones de la SDK de Android modernas. Utilizad un emulador que corra Android 22 o inferior

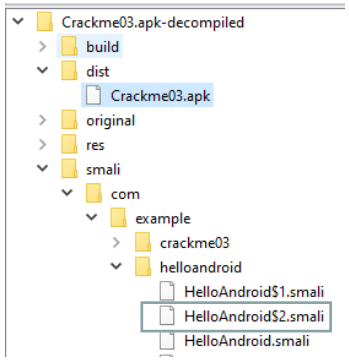


```
jucar@nuc-jcrg ~/CDM/case-studies/1.CrackMe03
$ grep -inr "Bad boy" --include=*.smali
Crackme03.apk-decompiled/smali/com/example/helloandroid/HelloAndroid$2.smali:457:    const-string v23, "Bad boy "
```

Código actividad HelloAndroid

```
14 public class HelloAndroid extends Activity {
15     private View.OnClickListener pulsarBoton = new View.OnClickListener() {
16         /* class com.example.helloandroid.HelloAndroid.AnonymousClass2 */
17
18         public void onClick(View v) {
19             String name3 = ((EditText) HelloAndroid.this.findViewById(R.id.txt_name)).getText().toString();
20             int name3lenght = name3.length();
21             String name4 = "";
22             String serial_entered = ((EditText) HelloAndroid.this.findViewById(R.id.txt_serial)).getText().toString();
23             if (name3lenght < 4) {
24                 try {
25                     Toast.makeText(HelloAndroid.this.getApplicationContext(), "Min 4 chars", 1).show();
26                 } catch (Exception e) {
27                     Toast.makeText(HelloAndroid.this.getApplicationContext(), "Another Error Ocurred :(", 1).show();
28                 }
29             } else {
30                 for (int i = 0; i < name3.length(); i++) {
31                     name4 = String.valueOf(name4) + ((int) name3.charAt(i));
32                 }
33                 String name42 = String.valueOf(Integer.parseInt(name4.substring(0, 5)) ^ 438294);
34                 TelephonyManager mTelephonyMgr = (TelephonyManager) HelloAndroid.this.getSystemService("phone");
35                 String imei2 = mTelephonyMgr.getDeviceId();
36                 String simsn = mTelephonyMgr.getSimSerialNumber();
37                 String temp02 = imei2.substring(0, 6);
38                 if ((String.valueOf(name42) + "-" + String.valueOf((long) (Integer.parseInt(temp02) ^ Integer.parseInt(simsn.substring(0, 6)))) + "-" + temp02).equals(serial_entered)) {
39                     Toast.makeText(HelloAndroid.this.getApplicationContext(), "God boy", 1).show();
40                 } else {
41                     Toast.makeText(HelloAndroid.this.getApplicationContext(), "Bad boy ", 1).show();
42                 }
43             }
44         }
45     };
```

Comprobaciones




```
70      .line 77
71      .local v10, "name3":Ljava/lang/String;
72      invoke-virtual {v10}, Ljava/lang/String;->length()I
73
74      move-result v11
75
76      .line 78
77      .local v11, "name3lenght":I
78      const-string v12, ""
79
80      .line 79
81      .local v12, "name4":Ljava/lang/String;
82      move-object/from16 v0, p0
83
84      iget-object v0, v0, Lcom/example/helloandroid/HelloAndroid$2;->this$0:Lcom/example/helloandroid/HelloAndroid;
85
86      move-object/from16 v22, v0
87
88      const v23, 0x7f050006
89
90      invoke-virtual/range {v22 .. v23}, Lcom/example/helloandroid/HelloAndroid;->findViewById(I)Landroid/view/View;
91
92      move-result-object v21
93
94      check-cast v21, Landroid/widget/EditText;
95
96      .line 80
97      .local v21, "txtserial":Landroid/widget/EditText;
98      invoke-virtual/range {v21 .. v21}, Landroid/widget/EditText;->getText()Landroid/text/Editable;
99
100     move-result-object v22
101
102     invoke-interface/range {v22 .. v22}, Landroid/text/Editable;->toString()Ljava/lang/String;
103
104     move-result-object v15
105
106     .line 84
107     .local v15, "serial_entered":Ljava/lang/String;
108     const/16 v22, 0x4
109
110     move v0, v11
111
112     move/from16 v1, v22
113
114     if-ge v0, v1, :cond_0
```

Código smali

- Buscamos ":cond_0" en el código smali y vemos que el flujo de ejecución no varía hasta
  - Salto a ":cond_1" en la línea 162 (notificación de introducción de menos de 4 caracteres)
  - Salto a ":cond_2" que si no se da nos lleva a obtener el mensaje "God boy"

```
320     if-eqz v22, :cond_2
321
322     .line 111
323     move-object/from16 v0, p0
324
325     iget-object v0, v0, Lcom/example/helloandroid/HelloAndroid$2;->this$0:Lcom/example/helloandroid/HelloAndroid;
326
327     move-object/from16 v22, v0
328
329     invoke-virtual/range {v22 .. v22}, Lcom/example/helloandroid/HelloAndroid;->getApplicationContext()Landroid/content/Context;
330
331     move-result-object v22
332
333     .line 112
334     const-string v23, "God boy"
335
336     const/16 v24, 0x1
337
338     .line 111
339     invoke-static/range {v22 .. v24}, Landroid/widget/Toast;->makeText(Landroid/content/Context;Ljava/lang/CharSequence;I)Landroid/widget/Toast;
340
341     move-result-object v13
342
343     .line 113
344     .restart local v13    # "notificacionToast":Landroid/widget/Toast;
345     invoke-virtual {v13}, Landroid/widget/Toast;->show()V
```

Solución 1

- Si comentamos este último salto

  #if-eqz v22, :cond_2

  sea cual sea el resultado de la comprobación de los valores introducidos entraremos obtendremos “God boy” como respuesta
- Pero necesitaremos introducir 4 caracteres al menos en el campo de nombre
  - Para intentar solucionarlo podemos realizar este cambio:

```
move v0, v11
move/from16 v1, v22
if-ge v0, v1, :cond_0
.line 86
:try_start_0
```

```
move v0, v11
move/from16 v1, v22
goto :cond_0
.line 86
:try_start_0
```

  - … pero no funcionará

Solución 2

- Para evitar tener que introducir “nada” en el campo de nombre realizamos los siguientes cambios

```
const/16 v22, 0x4
move v0, v11
move/from16 v1, v22
#if-ge v0, v1, :cond_0
goto :cond_3
.line 86
:try_start_0
```

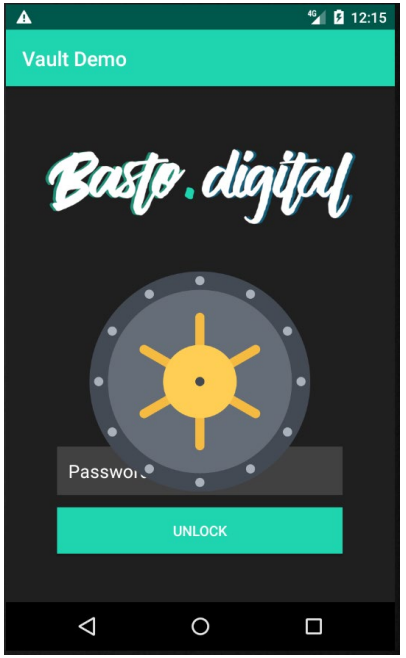
+

```
invoke-virtual {v14, v15}, Ljava/lang/String;->equals(Ljava/lang/
    Object;)Z
move-result v22
if-eqz v22, :cond_2
:cond_3
.line 111
move-object/from16 v0, p0
```

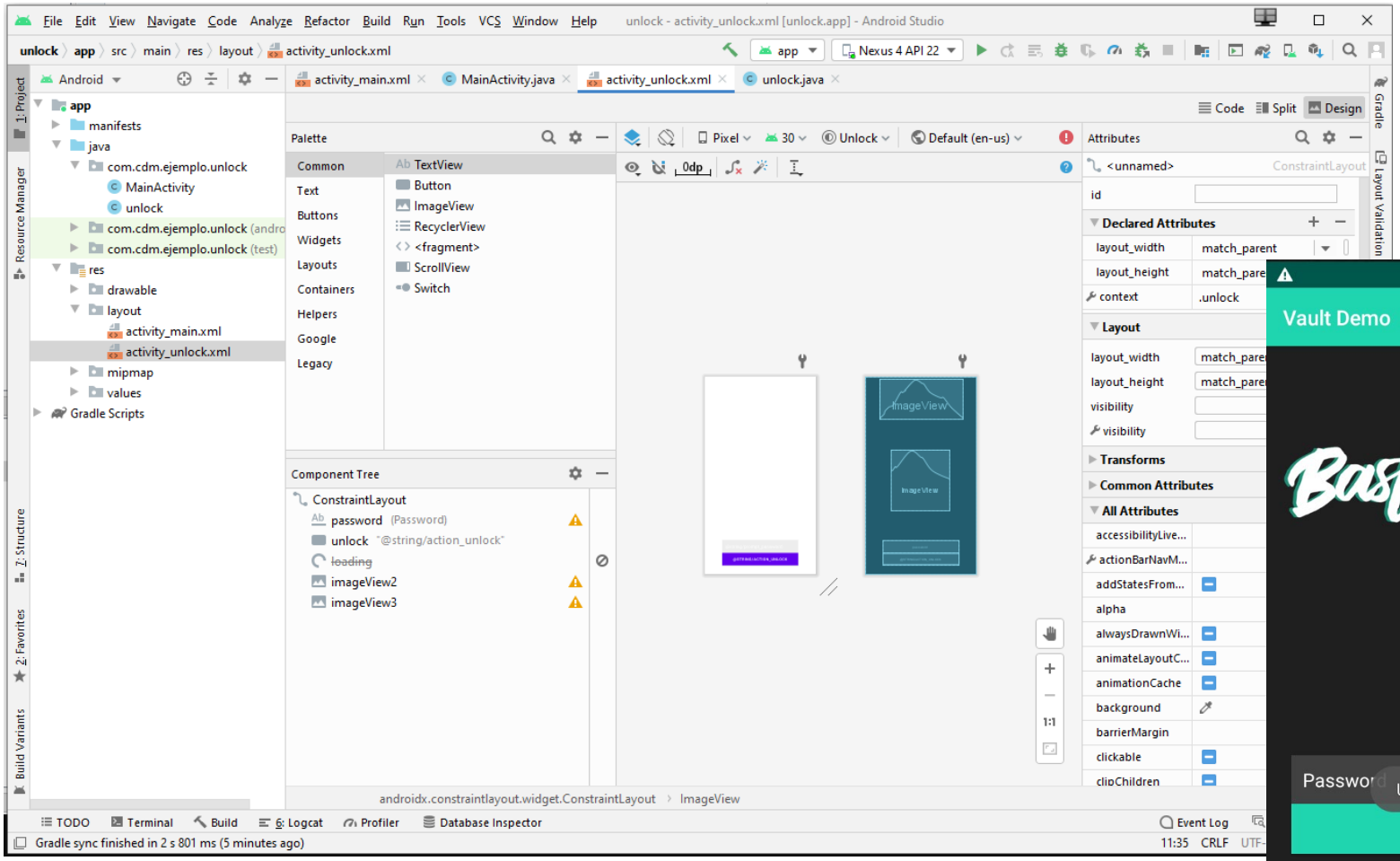
- Aplicar, reensamblar e instalar la nueva apk para ver que funciona

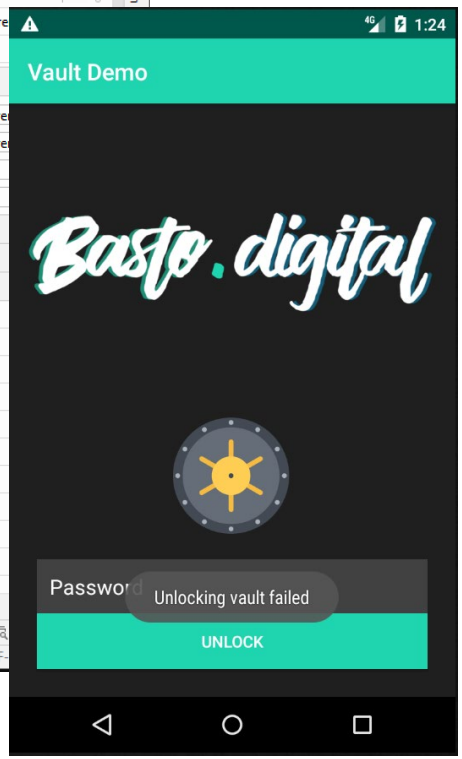
Caso de estudio 2

- vault.apk
  - Disponible en https://basto.digital/download/vault.apk
  - Este ejemplo es más sencillo, pero conlleva entender qué parte de la app hay que modificar



Rectificar el layout de la app





Análisis

```
jucar@nuc-jcrg ~/CDM/case-studies/2.Vault
$ grep -inr "Unlocking vault" --include=*.smali

jucar@nuc-jcrg ~/CDM/case-studies/2.Vault
$ grep -inr "Unlocking vault" --include=*
Binary file vault.apk matches
Binary file vault.apk-decompiled/build/apk/resources.arsc matches
Binary file vault.apk-decompiled/build/resources.zip matches
Binary file vault.apk-decompiled/dist/vault.apk matches
vault.apk-decompiled/res/values/strings.xml:63:    <string name="unlock_failed">
Unlocking vault failed</string>

jucar@nuc-jcrg ~/CDM/case-studies/2.Vault
$ grep -inr "Unlocking vault" --include=*
Binary file vault.apk matches
Binary file vault.apk-decompiled/build/apk/resources.arsc matches
Binary file vault.apk-decompiled/build/resources.zip matches
Binary file vault.apk-decompiled/dist/vault.apk matches
vault.apk-decompiled/res/values/strings.xml:63:    <string name="unlock_failed">Unlocking vault failed</string>
jucar@nuc-jcrg ~/CDM/case-studies/2.Vault
$ grep -inr "unlock_failed" --include=*
Binary file vault.apk matches
Binary file vault.apk-decompiled/build/apk/classes.dex matches
Binary file vault.apk-decompiled/build/apk/resources.arsc matches
Binary file vault.apk-decompiled/build/resources.zip matches
Binary file vault.apk-decompiled/dist/vault.apk matches
vault.apk-decompiled/res/values/public.xml:1388:    <public type="string" name="unlock_failed" id="0x7f0d003c" />
vault.apk-decompiled/res/values/strings.xml:63:    <string name="unlock_failed">Unlocking vault failed</string>
vault.apk-decompiled/smali/digital/basto/vault/R$string.smali:138:.field public static final unlock_failed:I = 0x7f0d003c
vault.apk-decompiled/sources/digital/basto/vault/R.java:1434:        public static final int unlock_failed = 2131558460;
vault.apk-decompiled/sources/digital/basto/vault/ui/view/UnlockViewModel.java:38:        this.unlockResult.setValue(new UnlockResul
t(Integer.valueOf((int) R.string.unlock_failed)));
```

Análisis (cont.)

UnlockViewModel.java

```
public void unlock(String password) {
    Result<VaultData> result = this.vaultRepository.unlock(password);
    if (result instanceof Result.Success) {
```

VaultRepository.java

```
public Result<VaultData> unlock(String password) {
    Result<VaultData> result = this.dataSource.unlock(password);
    if (result instanceof Result.Success) {
        setVault((VaultData) ((Result.Success) result).getData());
    }
    return result;
}
```

VaultDataSource.java

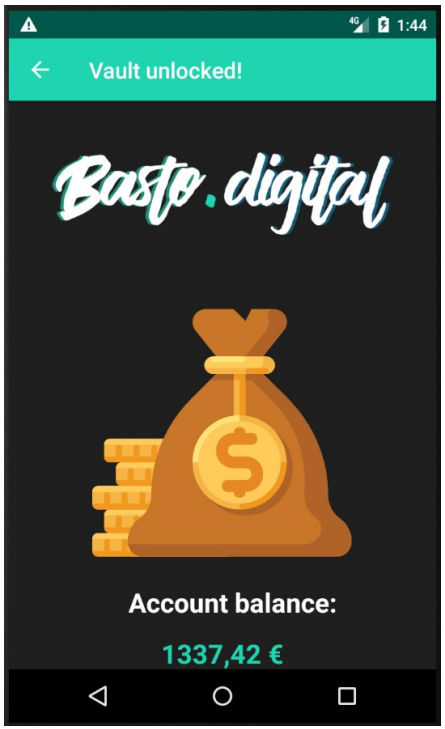
```
public class VaultDataSource {
    private String vaultCombination = "Subscribe!";

    public Result<VaultData> unlock(String password) {
        try {
            if (this.vaultCombination.equals(password)) {
                return new Result.Success(new VaultData(1337.42f));
            }
            return new Result.Error(new AccessControlException("Wrong password!"));
        } catch (Exception e) {
            return new Result.Error(new IOException("Error unlocking view!", e));
        }
    }
```

Smali objetivo

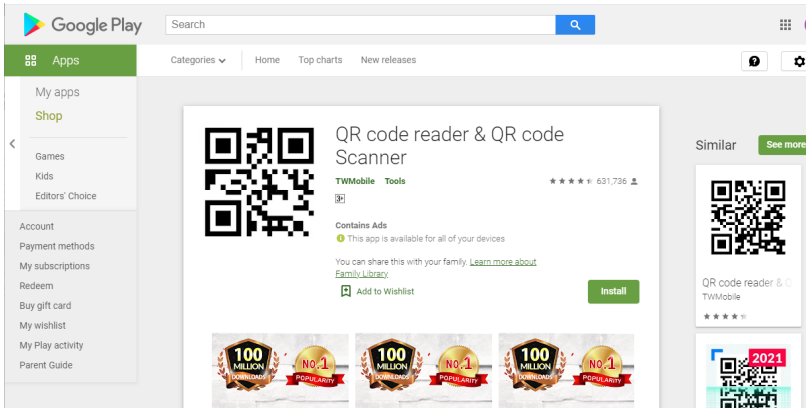
```
34 .method public unlock(Ljava/lang/String;)Ldigital/basto/vault/data/Result;
35     .locals 4
36     .param p1, "password"    # Ljava/lang/String;
37     .annotation system Ldalvik/annotation/Signature;
38         value = {
39             "(",
40             "Ljava/lang/String;",
41             ")",
42             "Ldigital/basto/vault/data/Result<",
43             "Ldigital/basto/vault/data/model/VaultData;",
44             ">;"
45         }
46     .end annotation
47
48     .line 15
49     :try_start_0
50     iget-object v0, p0, Ldigital/basto/vault/data/VaultDataSource;->vaultCombination:Ljava/lang/String;
51
52     invoke-virtual {v0, p1}, Ljava/lang/String;->equals(Ljava/lang/Object;)Z
53
54     move-result v0
55
56     if-eqz v0, :cond_0
57
58     .line 16
59     new-instance v0, Ldigital/basto/vault/data/model/VaultData;
60
61     const v1, 0x44a72d71
62
63     invoke-direct {v0, v1}, Ldigital/basto/vault/data/model/VaultData;-><init>(F)V
64
65     .line 19
66     .local v0, "unlockData":Ldigital/basto/vault/data/model/VaultData;
67     new-instance v1, Ldigital/basto/vault/data/Result$Success;
68
69     invoke-direct {v1, v0}, Ldigital/basto/vault/data/Result$Success;-><init>(Ljava/lang/Object;)V
70
71     return-object v1
72
73     .line 21
74     .end local v0    # "unlockData":Ldigital/basto/vault/data/model/VaultData;
75     :cond_0
76     new-instance v0, Ldigital/basto/vault/data/Result$Error;
77
78     new-instance v1, Ljava/security/AccessControlException;
79
80     const-string v2, "Wrong password!"
```

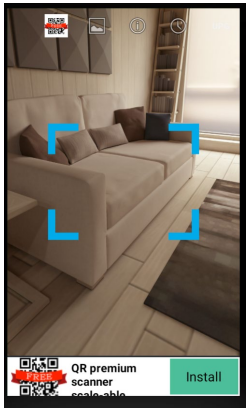
```
55
56      #if-eqz v0, :cond_0
57
```

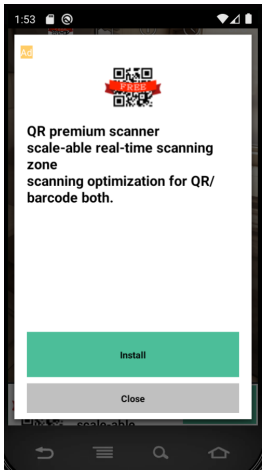


Caso de estudio 3

- QR Code Reader
  - https://apkpure.com/es/qr-code-reader-qr-code-scanner/tw.mobileapp.qrcode.banner
  - https://play.google.com/store/apps/details?id=tw.mobileapp.qrcode.banner







  - No siempre necesitamos modificar el código de la app

Objetivo: Eliminar la publicidad

- Localizar los ids de publicidad y eliminarlos

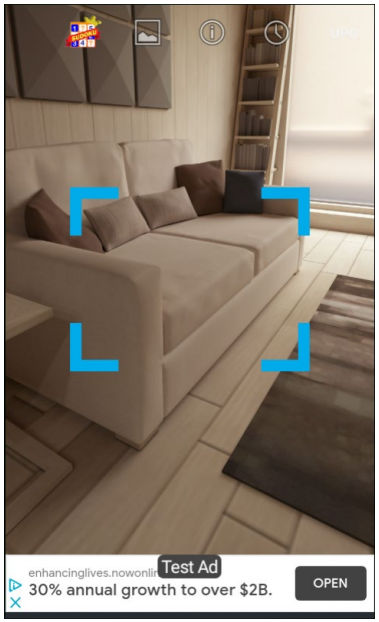
```
jucar@nuc-jcrg ~/CDM/case-studies/3.QrReader
$ grep -inr "ads" --include=*.smali | grep "tw.mobileapp.qrcode.banner"
```

```
jucar@nuc-jcrg ~/CDM/case-studies/3.QrReader
$ grep -inr "AdView" --include=*.smali | grep "tw.mobileapp.qrcode.banner"
```

```
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2021:    iput-object v1, p0, Ltw/mobileapp/qrcode/banner/x;->Z:Lcom/google/android/gms/ads/AdView;
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2025:    invoke-virtual {v1, v2}, Lcom/google/android/gms/ads/AdView;->setAdSize(Lcom/google/android/gms/ads/AdSize;)V
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2027:    iget-object v1, p0, Ltw/mobileapp/qrcode/banner/x;->Z:Lcom/google/android/gms/ads/AdView;
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2031:    invoke-virtual {v1, v2}, Lcom/google/android/gms/ads/AdView;->setAdUnitId(Ljava/lang/String;)V
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2033:    iget-object v1, p0, Ltw/mobileapp/qrcode/banner/x;->Z:Lcom/google/android/gms/ads/AdView;
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2041:    iget-object v1, p0, Ltw/mobileapp/qrcode/banner/x;->Z:Lcom/google/android/gms/ads/AdView;
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2049:    iget-object v2, p0, Ltw/mobileapp/qrcode/banner/x;->Z:Lcom/google/android/gms/ads/AdView;
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2063:    iget-object v1, p0, Ltw/mobileapp/qrcode/banner/x;->Z:Lcom/google/android/gms/ads/AdView;
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2075:    iget-object v2, p0, Ltw/mobileapp/qrcode/banner/x;->Z:Lcom/google/android/gms/ads/AdView;
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2081:    invoke-virtual {v2, v3}, Lcom/google/android/gms/ads/AdView;->setAdListener(Lcom/google/android/gms/ads/AdListener;)V
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2083:    iget-object v0, p0, Ltw/mobileapp/qrcode/banner/x;->Z:Lcom/google/android/gms/ads/AdView;
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2085:    invoke-virtual {v0, v1}, Lcom/google/android/gms/ads/AdView;->loadAd(Lcom/google/android/gms/ads/AdRequest;)V
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2098:    iget-object v0, p0, Ltw/mobileapp/qrcode/banner/x;->a0:Lcom/google/android/gms/ads/AdView;
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2108:    iget-object v0, p0, Ltw/mobileapp/qrcode/banner/x;->a0:Lcom/google/android/gms/ads/AdView;
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2116:    iget-object v1, p0, Ltw/mobileapp/qrcode/banner/x;->a0:Lcom/google/android/gms/ads/AdView;
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2130:    iget-object v0, p0, Ltw/mobileapp/qrcode/banner/x;->a0:Lcom/google/android/gms/ads/AdView;
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2137:    new-instance v0, Lcom/google/android/gms/ads/AdView;
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2141:    invoke-direct {v0, v1}, Lcom/google/android/gms/ads/AdView;-><init>(Landroid/content/Context;)V
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2143:    iput-object v0, p0, Ltw/mobileapp/qrcode/banner/x;->a0:Lcom/google/android/gms/ads/AdView;
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2147:    invoke-virtual {v0, v1}, Lcom/google/android/gms/ads/AdView;->setAdSize(Lcom/google/android/gms/ads/AdSize;)V
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2149:    iget-object v0, p0, Ltw/mobileapp/qrcode/banner/x;->a0:Lcom/google/android/gms/ads/AdView;
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2153:    invoke-virtual {v0, v1}, Lcom/google/android/gms/ads/AdView;->setAdUnitId(Ljava/lang/String;)V
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2155:    iget-object v0, p0, Ltw/mobileapp/qrcode/banner/x;->a0:Lcom/google/android/gms/ads/AdView;
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2163:    iget-object v0, p0, Ltw/mobileapp/qrcode/banner/x;->a0:Lcom/google/android/gms/ads/AdView;
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2171:    iget-object v1, p0, Ltw/mobileapp/qrcode/banner/x;->a0:Lcom/google/android/gms/ads/AdView;
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2185:    iget-object v0, p0, Ltw/mobileapp/qrcode/banner/x;->a0:Lcom/google/android/gms/ads/AdView;
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2197:    iget-object v1, p0, Ltw/mobileapp/qrcode/banner/x;->a0:Lcom/google/android/gms/ads/AdView;
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2203:    invoke-virtual {v1, v2}, Lcom/google/android/gms/ads/AdView;->setAdListener(Lcom/google/android/gms/ads/AdListener;)V
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2205:    iget-object p1, p0, Ltw/mobileapp/qrcode/banner/x;->a0:Lcom/google/android/gms/ads/AdView;
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2207:    invoke-virtual {p1, v0}, Lcom/google/android/gms/ads/AdView;->loadAd(Lcom/google/android/gms/ads/AdRequest;)V
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2613:    iget-object v0, p0, Ltw/mobileapp/qrcode/banner/x;->Z:Lcom/google/android/gms/ads/AdView;
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2619:    invoke-virtual {v0}, Lcom/google/android/gms/ads/AdView;->destroy()V
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2621:    iput-object v1, p0, Ltw/mobileapp/qrcode/banner/x;->Z:Lcom/google/android/gms/ads/AdView;
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2624:    iget-object v0, p0, Ltw/mobileapp/qrcode/banner/x;->a0:Lcom/google/android/gms/ads/AdView;
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2628:    invoke-virtual {v0}, Lcom/google/android/gms/ads/AdView;->destroy()V
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2630:    iput-object v1, p0, Ltw/mobileapp/qrcode/banner/x;->a0:Lcom/google/android/gms/ads/AdView;
```

Análisis

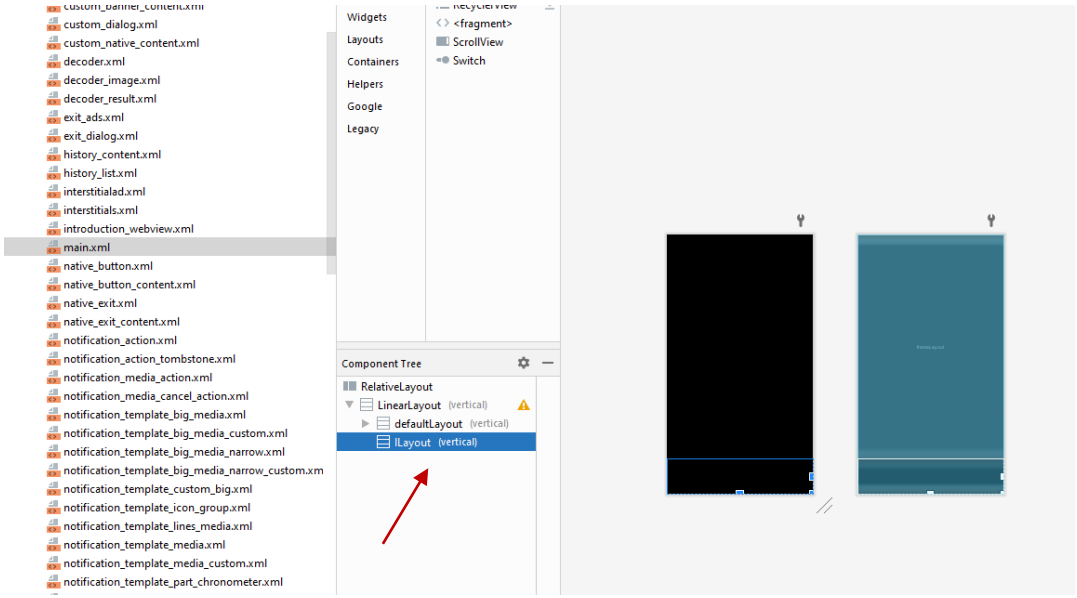
```
public void C1() {
    FrameLayout frameLayout = (FrameLayout) this.d0.findViewById(C0061R.id.adLayout);
    if (frameLayout != null) {
        AdView adView = new AdView(this.Y);
        this.Z = adView;
        adView.setAdSize(AdSize.MEDIUM_RECTANGLE);
        this.Z.setAdUnitId("ca-app-pub-9549147931362796/1676924541");
        if (this.Z.getParent() != null) {
            ((ViewGroup) this.Z.getParent()).removeView(this.Z);
        }
```

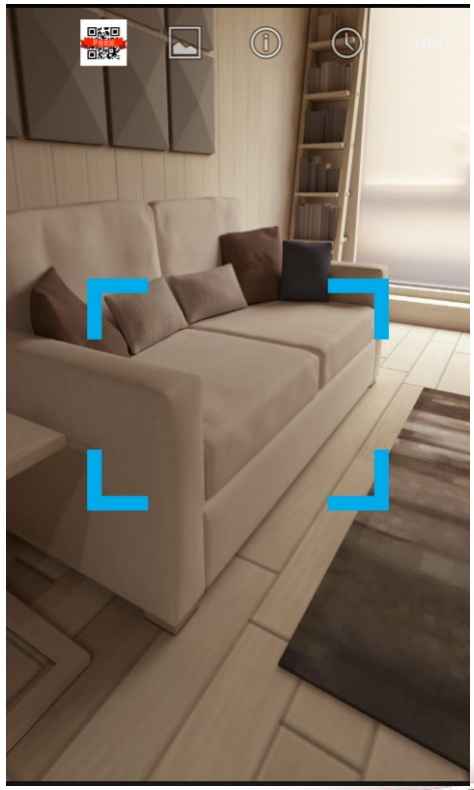



```
jucar@nuc-jcrg ~/CDM/case-studies/3.QrReader
$ grep -inr "ca-app" --include=*.smali
qr.apk-decompiled/smali/com/google/android/gms/ads/internal/util/zzj.smali:514:    const-string v1, "^ca-app-pub-[0-9]{16}~[0-9]{10}$"
qr.apk-decompiled/smali/com/google/android/gms/internal/ads/xz2.smali:136:    const-string v0, "^ca-app-pub-[0-9]{16}~[0-9]{10}$"
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/ApplicationQRCode.smali:396:    const-string v2, "ca-app-pub-9549147931362796/4066079934"
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/InterstitialsAdStart.smali:138:    const-string v1, "ca-app-pub-9549147931362796/2650539336"
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/l.smali:876:    const-string v3, "ca-app-pub-9549147931362796/1533222455"
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/l.smali:2428:    const-string v1, "ca-app-pub-9549147931362796/2653156372"
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/MainFragmentActivity.smali:1141:    const-string v2, "ca-app-pub-9549147931362796/6396362471"
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/PermissionActivity.smali:414:    const-string v1, "ca-app-pub-9549147931362796/8818394220"
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2029:    const-string v2, "ca-app-pub-9549147931362796/1676924541"
qr.apk-decompiled/smali/tw/mobileapp/qrcode/banner/x.smali:2151:    const-string v1, "ca-app-pub-9549147931362796/2653156372"
```

Idea feliz

- Si el anuncio aparece abajo se habrá reservado en el layout un espacio a tal fin. ¿Y si lo elimino de main.xml?





¿Y el menú de opciones?

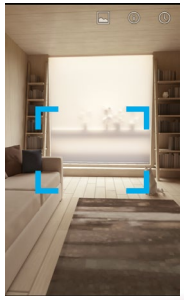
```xml
<?xml version="1.0" encoding="utf-8"?>
<RelativeLayout android:layout_width="fill_parent" android:layout_height="fill_parent"
  xmlns:android="http://schemas.android.com/apk/res/android">
    <LinearLayout android:orientation="vertical" android:layout_width="fill_parent" android:layout_height="fill_parent">
        <LinearLayout android:orientation="vertical" android:id="@id/defaultLayout" android:layout_width="fill_parent" android:layout_height="100.0dip" android:layout_weight="1.0">
            <FrameLayout android:id="@id/frameLayout" android:layout_width="fill_parent" android:layout_height="fill_parent" />
        </LinearLayout>
    </LinearLayout>
</RelativeLayout>
```

- En el código de MainFragmentActivity.java se localiza la carga de un menú

```java
public boolean onCreateOptionsMenu(Menu menu) {
    getMenuInflater().inflate(C0061R.menu.menu_main, menu);
    if (this.o == null) {
        this.o = menu;
        G(this.n);
    }
    return super.onCreateOptionsMenu(menu);
}
```

```xml
<?xml version="1.0" encoding="utf-8"?>
<menu
  xmlns:android="http://schemas.android.com/apk/res/android">
    <item android:icon="@drawable/flashlight_off" android:id="@id/menu_flashlight" android:orderInCategory="1" android:title="@string/menu_flashlight" android:showAsAction="always|withText" />
    <item android:icon="@android:drawable/ic_menu_gallery" android:id="@id/menu_image" android:orderInCategory="8" android:title="@string/menu_image" android:showAsAction="always|withText" />
    <item android:icon="@android:drawable/ic_menu_recent_history" android:id="@id/menu_history" android:orderInCategory="12" android:title="@string/menu_history" android:showAsAction="always|withText" />
    <item android:icon="@drawable/icon" android:id="@id/menu_icon" android:orderInCategory="0" android:title="" android:showAsAction="always|withText" />
    <item android:icon="@drawable/pro" android:id="@id/menu_pro" android:orderInCategory="50" android:title="@string/menu_pro" android:showAsAction="always|withText" />
    <item android:icon="@android:drawable/ic_menu_info_details" android:id="@id/menu_help" android:orderInCategory="10" android:title="@string/menu_help" android:showAsAction="always|withText" />
</menu>
```

- ¿Y si elimino las opciones de menu_icon y menu_pro?



Indice

- ¿Qué es Android? Conceptos básicos
- Anatomía de una app Android sencilla
- Herramientas para el desarrollo y emulación de apps Android
- Reversing de apks
- Smali y parcheado de apks

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escola Tècnica Superior d'Enginyeria **Informàtica**

3. Ingeniería inversa de aplicaciones móviles Android

Ciberseguridad en Dispositivos móviles
DISCA – ETS de Ingeniería informática (UPV)