



# IX JORNADAS STIC CCN-CERT

DETECCIÓN E INTERCAMBIO, FACTORES CLAVE

Madrid, 10 y 11 de diciembre 2015

# Construyendo un laboratorio de análisis de aplicaciones Android



[www.ccn-cert.cni.es](http://www.ccn-cert.cni.es)





CCN-cert  
centro criptológico nacional

- María Isabel Rojo
- Software Security Assurance Team - Indra
- mirojo@indra.es

## Índice

- 1. ¿Por qué Android?**
- 2. Problemática**
- 3. ¿Qué?**
- 4. Tipos de herramientas**
  - 1. Estáticas**
  - 2. Dinámicas**
  - 3. Reversing**
  - 4. Otros**
- 5. Distribuciones**

# ¿Por qué Android?

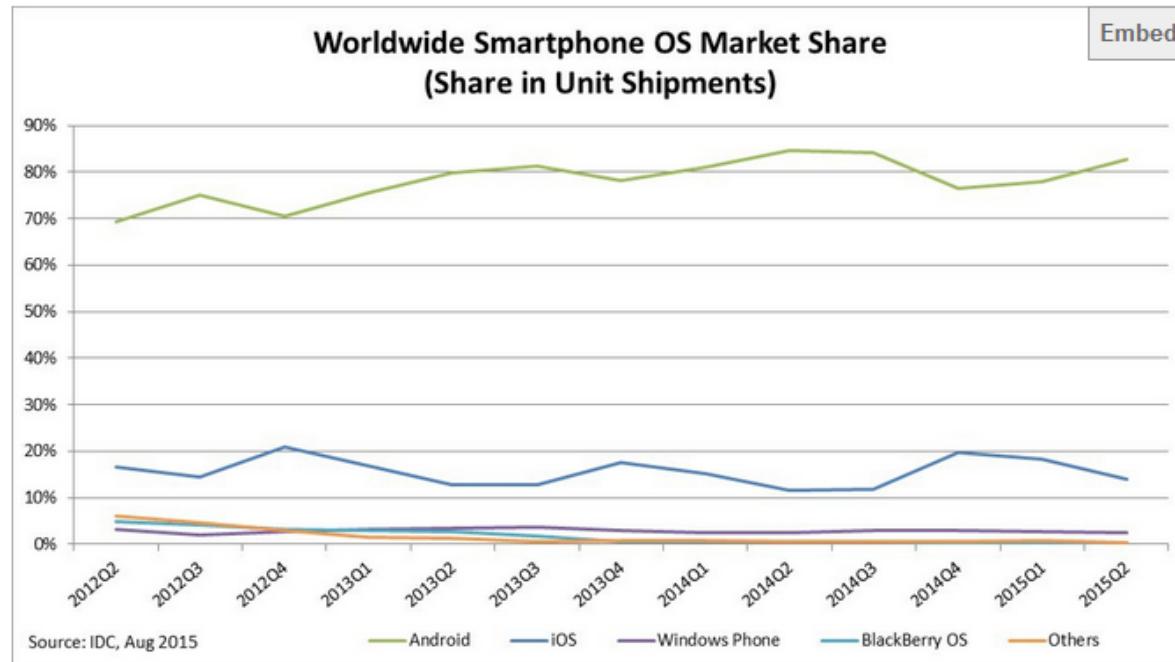
Por qué un laboratorio para Android

Period	Android	iOS	Windows Phone	BlackBerry OS	Others
2015Q2	82.8%	13.9%	2.6%	0.3%	0.4%
2014Q2	84.8%	11.6%	2.5%	0.5%	0.7%
2013Q2	79.8%	12.9%	3.4%	2.8%	1.2%
2012Q2	69.3%	16.6%	3.1%	4.9%	6.1%

Source: IDC, Aug 2015

# ¿Por qué Android?

Por qué un laboratorio para Android



## Problemática

### Primeros problemas

- Decenas de herramientas
- Desactualizadas / Abandonadas
- Rápida evolución de Android
- Nuevo malware, misma finalidad



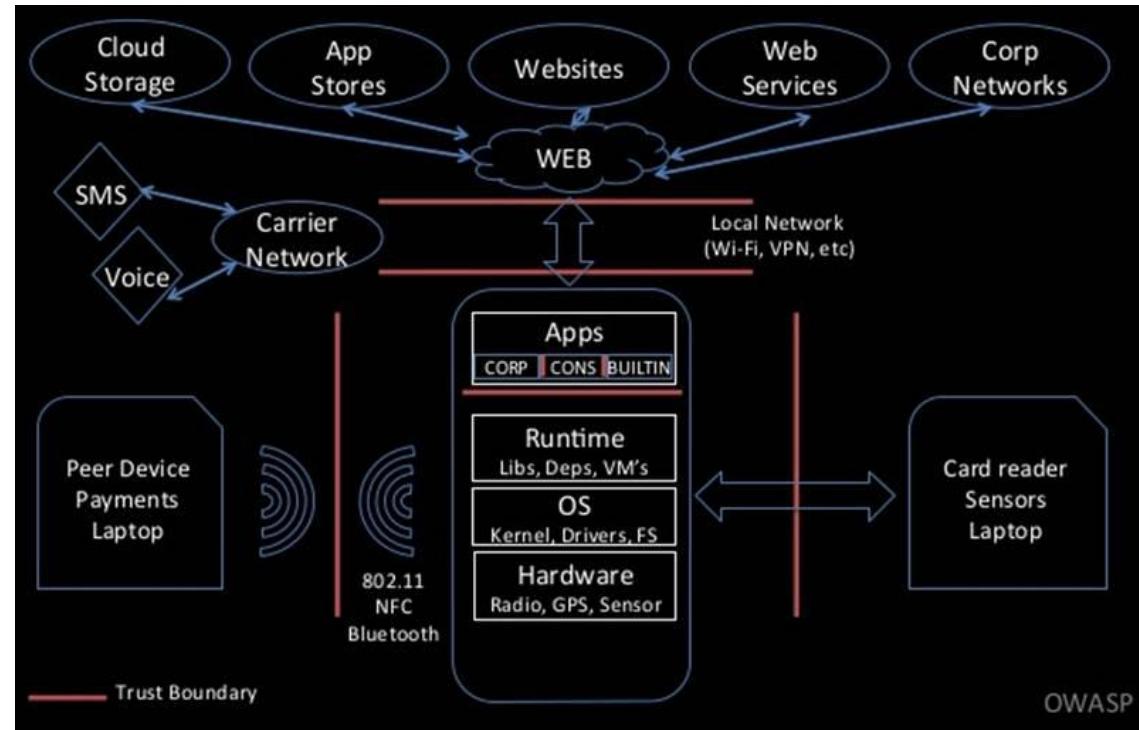
# ¿Qué?

## ¿Qué atacar en un pentesting?

- Superficie de ataque o funcionalidad
- Interacción con otros componentes
  - Interacción con los componentes IPC
  - Permisos
  - Funcionalidades expuestas
- Comunicaciones
  - Secure channel
- Datos
- Interacción con el navegador – Get, Post
- Vulnerabilidades
  - Java o vulnerabilidades del lenguaje
  - Dependencias externas vulnerables/desactualizadas

# ¿Qué?

## ¿Qué atacar en un pentesting?



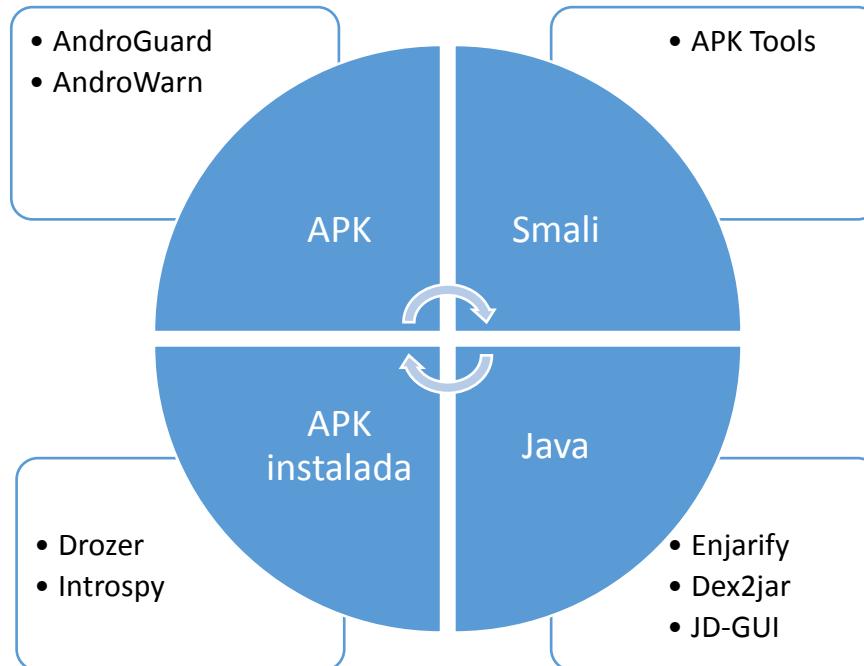
## ¿Qué?

## Posibles problemas de seguridad

Security Issue	Description
Authentication	Issues related to user identification
Access Control	Issues related to user rights after authentication
Auditing and Logging	Issues related to logs and auditing
Cryptography	Issues related to encryption and securing communications
Credential Handling	Issues related to the handling of user passwords and other credentials
Data Handling	Issues related to the handling of data vis-à-vis its sensitivity
Data Leakage	Issues related to accidental or unintended leakage of information
Error Checking	Issues related to reporting errors without providing too much data
Input Validation	Issues related to validating untrusted user input
Session Management	Issues related to best practices for user session management
Resource Handling	Issues related to the handling of resources, including memory
Patching	Issues related to timely patching/upgrade of software

## Tipos de herramientas

### Vista previa



## Tipos de herramientas

Tipologías de herramientas necesarias

- Análisis Estático
- Análisis Dinámico
- Reversing

# Herramientas Análisis Estático

## AndroGuard

```
root@AndroidKali:~/Herramientas/androguard# ./androlyze.py -s
Androlyze version 2.0
In [1]: a,d,dx = AnalyzeAPK("HolaMundo.apk",odecompiler="dad")newer.py
└── Imágenes
In [2]: a.get_permissions()
Out[2]:
['android.permission.SEND_SMS',
 'android.permission.READ_SMS',
 'android.permission.RECEIVE_SMS',
 'android.permission.READ_PHONE_STATE',
 'android.permission.READ_CONTACTS']
```

```
In [30]: a.get_permissions()
Out[30]:
['android.permission.INTERNET',
 'android.permission.ACCESS_WIFI_STATE',
 'android.permission.CHANGE_WIFI_STATE',
 'android.permission.ACCESS_NETWORK_STATE',
 'android.permission.ACCESS_COARSE_LOCATION',
 'android.permission.ACCESS_FINE_LOCATION',
 'android.permission.READ_PHONE_STATE',
 'android.permission.SEND_SMS',
 'android.permission.RECEIVE_SMS',
 'android.permission.RECORD_AUDIO',
 'android.permission.CALL_PHONE',
 'android.permission.READ_CONTACTS',
 'android.permission.WRITE_CONTACTS',
 'android.permission.RECORD_AUDIO',
 'android.permission.WRITE_SETTINGS',
 'android.permission.CAMERA',
 'android.permission.READ_SMS',
 'android.permission.WRITE_EXTERNAL_STORAGE']
```

# Herramientas Análisis Estático

## AndroWarn

- Basado en AndroGuard

```
root@AndroidKali:~/Herramientas/Androwarn# python androwarn.py -i HolaMundo.apk -r html
-v 3
[+] Analysis successfully completed and HTML file report available './Report/com.example.mirojo.holamundo.html'
```

Androwarn Report

The screenshot shows the Androwarn Report interface. On the left, there is a sidebar with the following navigation links:

- APPLICATION INFORMATION
  - Application Name
  - Application Version
  - Package Name
  - Description
- ANALYSIS RESULTS
  - Device Settings
  - Harvesting
  - Connection Interfaces
  - Exfiltration
  - Pim Data Leakage
- APK FILE
  - File Name

In the main content area, there is a section titled "File List" which lists several XML files:

- AndroidManifest.xml
- res/anim/abc\_fade\_in.xml
- res/anim/abc\_fade\_out.xml
- res/anim/abc\_grow\_fade\_in\_from\_bottom.xml
- res/anim/abc\_popup\_enter.xml
- res/anim/abc\_popup\_exit.xml
- res/anim/abc\_shrink\_fade\_out\_from\_bottom.xml
- res/anim/abc\_slide\_in\_bottom.xml
- res/anim/abc\_slide\_in\_top.xml

The screenshot shows the Androwarn Report interface. On the left, there is a sidebar with the following navigation links:

- File List
- Certificate Information
- ANDROIDMANIFEST.XML
- Main Activity
- Activities
- Permissions
- APIs USED
- Classes List
- Internal Classes List
- External Classes List
- Internal Packages List
- External Packages List
- Intents Sent

In the main content area, there is a list of API classes:

- android.app.Fragment
- android.app.Notification
- android.app.NotificationManager
- android.app.PendingIntent
- android.app.RemoteInput
- android.app.SearchManager
- android.app.SearchableInfo
- android.app.Service
- android.app.SharedElementCallback
- android.content.BroadcastReceiver
- android.content.ClipData
- android.content.ClipDescription
- android.content.ComponentName
- android.content.ContentProvider

## Tipos de herramientas

Tipologías de herramientas necesarias

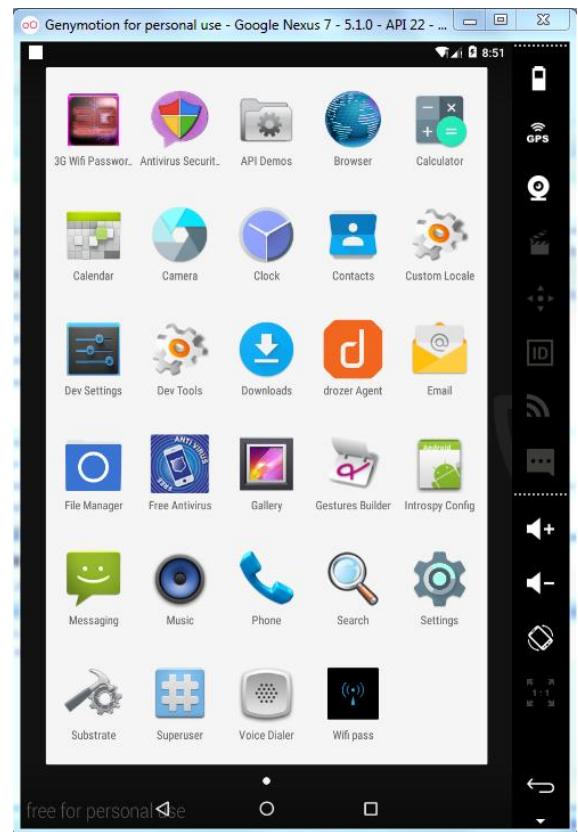
- Análisis Estático
- Análisis Dinámico
- Reversing

# Herramientas Análisis Dinámico

# Drozer

```
dz> run app.package.list
com.example.android.livewallpapers <Example Wallpapers>
com.android.providers.telephony <Mobile Network Configuration>
com.android.providers.calendar <Calendar Storage>
com.android.providers.media <Media Storage>
com.android.wallpapercropper <com.android.wallpapercropper>
ss.passion.blockgram <Free Antivirus>
com.android.voicedialer <Voice Dialer>
com.android.documentsui <Documents>
com.android.galaxy4 <Black Hole>
```

```
dz> list
app.activity.forintent      Find activities that can handle the given intent
app.activity.info           Gets information about exported activities.
app.activity.start          Start an Activity
app.broadcast.info          Get information about broadcast receivers
app.broadcast.send          Send broadcast using an intent
```



# Herramientas Análisis Dinámico

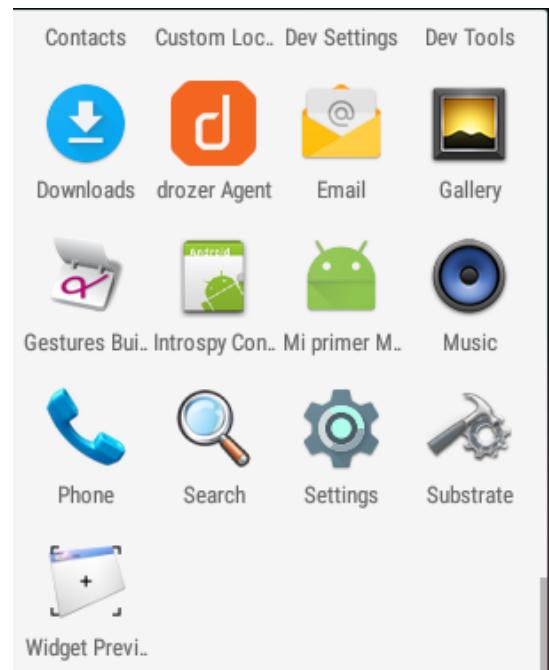
## Introspy

```
D:\Android\sdk\platform-tools>adb install "Introspy-Android Config.apk"
887 KB/s (20915 bytes in 0.023s)
    pkg: /data/local/tmp/Introspy-Android Config.apk
Success

D:\Android\sdk\platform-tools>adb install "Introspy-Android Core.apk"
984 KB/s (241983 bytes in 0.240s)
    pkg: /data/local/tmp/Introspy-Android Core.apk
Success

D:\Android\sdk\platform-tools>adb install com.saurik.substrate.apk
995 KB/s (1573498 bytes in 1.544s)
    pkg: /data/local/tmp/com.saurik.substrate.apk
Success

D:\Android\sdk\platform-tools>adb logcat -s "Introspy"
----- beginning of main
----- beginning of system
----- beginning of crash
```



# Herramientas Análisis Dinámico

## Introspy

The screenshot shows the Introspy tool interface with two tabs of traced calls:

- 61: NSURLConnection initWithRequest:delegate:**
  - Arguments:**

```
{ "request": { "URL": { "parameterString": "nil", "absoluteString": "http://conf.3g.qq.com/newConf/n", "host": "conf.3g.qq.com", "path": "/newConf/n", "query": "nil", "scheme": "Http", "port": "nil" }, "HTTPMethod": "POST", "HTTPBody": "AgMAAEElYczhNKVFMjhGNzY3RUQ3UNDrgMAwA=AAAAAAAAAAAAAAAAMAAAAAM=", "cachePolicy": 1 }, "delegate": [ "connection:didFailWithError:" ] }
```
  - Return Value:**

"Introspy - Not supported"
- 91: NSURLConnection initWithRequest:delegate:startImmediately:**
  - Arguments:**

```
{ "request": { "URL": { "parameterString": "nil", "absoluteString": "http://monitor.uu.qq.com/analytics/upload", "host": "monitor.uu.qq.com", "path": "/analytics/upload", "query": "nil" }, "HTTPMethod": "POST", "HTTPBody": "AgMAAEElYczhNKVFMjhGNzY3RUQ3UNDrgMAwA=AAAAAAAAAAAAAAAAMAAAAAM=", "cachePolicy": 1 }, "delegate": [ "connection:didFailWithError:" ] }
```

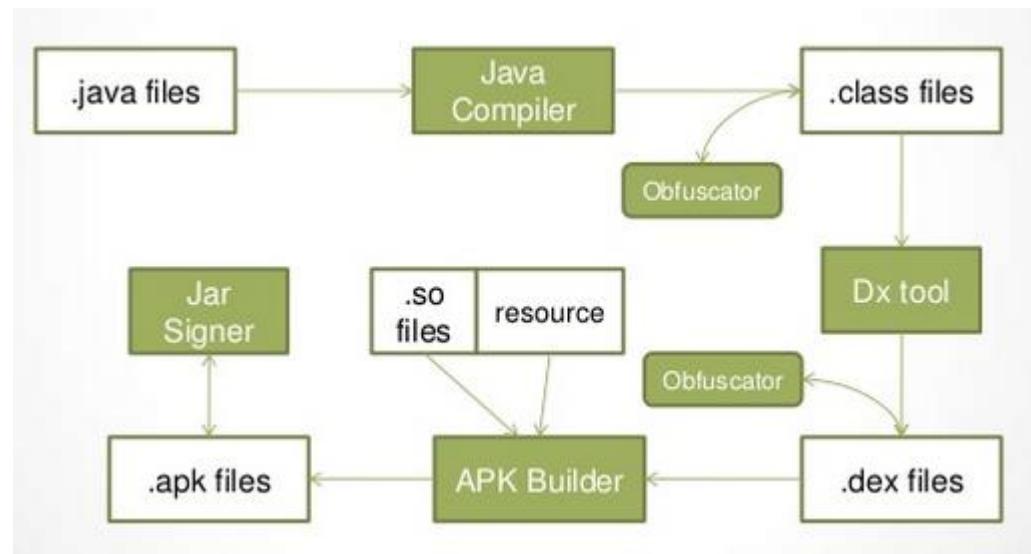
## Tipos de herramientas

Tipologías de herramientas necesarias

- Análisis Estático
- Análisis Dinámico
- Reversing

# Herramientas Reversing

## Ciclo de reversing para archivos java



# Herramientas Reversing

## Enjarify o dex2jar

```
D:\Android\dex2jar>d2j-dex2jar fbi.apk  
dex2jar fbi.apk -> ./fbi-dex2jar.jar
```

```
D:\Android\enjarify\enjarify-master>enjarify.bat fbi.apk  
1000 classes processed  
Output written to fbi-enjarify.jar  
1115 classes translated successfully, 0 classes had errors
```

 fbi-dex2jar	18/11/2015 11:12	Executable Jar File	1.100 KB
 fbi-enjarify	18/11/2015 11:08	Executable Jar File	1.766 KB

### Why not dex2jar?

Dex2jar is an older tool that also tries to translate Dalvik to Java bytecode. It works reasonable well most of the time, but a lot of obscure features or edge cases will cause it to fail or even silently produce incorrect results. By contrast, Enjarify is designed to work in as many cases as possible, even for code where Dex2jar would fail. Among other things, Enjarify correctly handles unicode class names, constants used as multiple types, implicit casts, exception handlers jumping into normal control flow, classes that reference too many constants, very long methods, exception handlers after a catchall handler, and static initial values of the wrong type.

# Herramientas Reversing

## JD-GUI

The screenshot shows the JD-GUI Java decompiler interface. The title bar reads "BackStackRecord\$2.class - Java Decomplier". The menu bar includes File, Edit, Navigation, Search, Help. The toolbar has icons for Open, Save, and Run. The left sidebar shows the package structure of the application, with "app" selected. The main window displays the Java code for the class BackStackRecord\$2. The code implements the ViewTreeObserver.OnPreDrawListener interface. It contains logic for removing the OnPreDrawListener from the scene root's ViewTreeObserver and setting local objects based on shared element transitions.

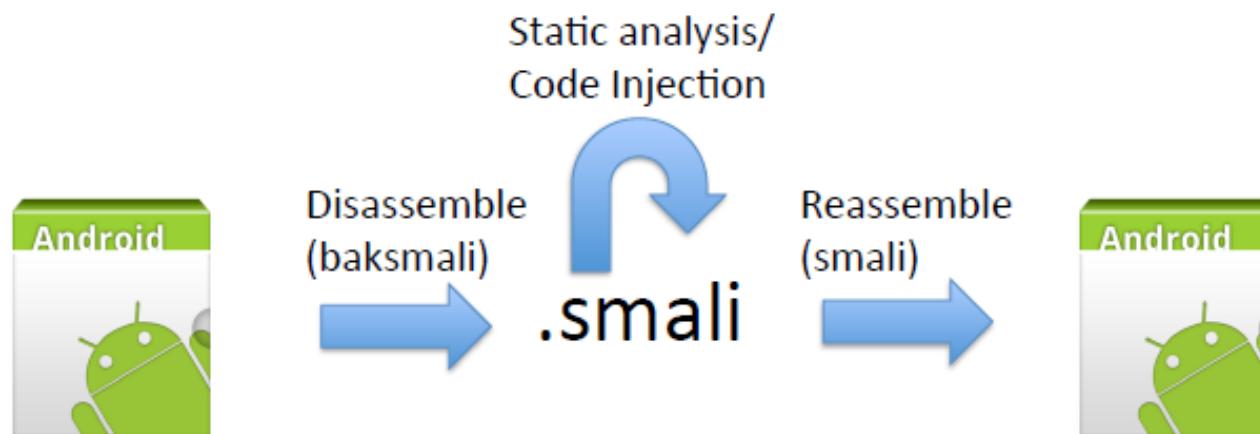
```
package android.support.v4.app;

import android.support.v4.util.ArrayMap;
import android.view.View;
import android.view.ViewTreeObserver;
import android.view.ViewTreeObserver.OnPreDrawListener;
import java.util.ArrayList;
import java.util.Collections;

class BackStackRecord$2
    implements ViewTreeObserver.OnPreDrawListener
{
    BackStackRecord$2(BackStackRecord paramBackStackRecord, View paramView, Object paramObject, ArrayList paramArrayList, BackStackRecord.TransitionState para
    public boolean onPreDraw()
    {
        this.val$sceneRoot.getViewTreeObserver().removeOnPreDrawListener(this);
        Object localObject1 = this.val$sharedElementTransition;
        Object localObject2;
        Fragment localFragment1;
        ArrayMap localArrayMap;
        if (localObject1 != null)
        {
            localObject1 = this.val$sharedElementTransition;
            localObject2 = localObject1;
            localFragment1 = localObject1;
            localArrayMap = localObject1;
        }
    }
}
```

# Herramientas Reversing

Ciclo de reversing para archivos smali



# Herramientas Reversing

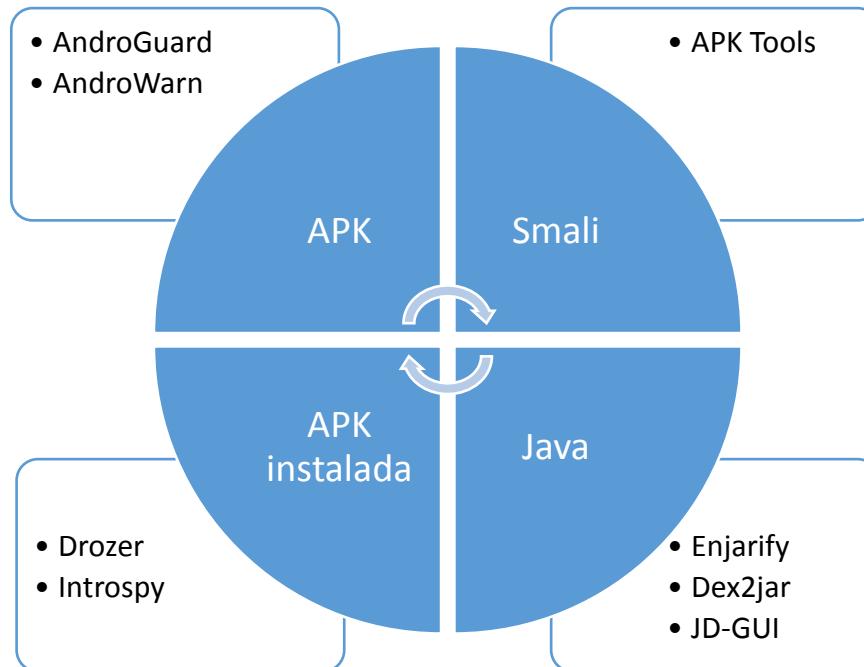
## APKTool

```
D:\Android\APKTool202>apktool_202.jar d fbi.apk
```

📁 assets	18/11/2015 11:20	Carpeta de archivos
📁 original	18/11/2015 11:20	Carpeta de archivos
📁 res	18/11/2015 11:20	Carpeta de archivos
📁 smali	18/11/2015 11:20	Carpeta de archivos
📄 AndroidManifest	18/11/2015 11:20	Archivo XML 3 KB
📄 apktool.yml	18/11/2015 11:20	Archivo YML 1 KB

## Tipos de herramientas

### Resumen



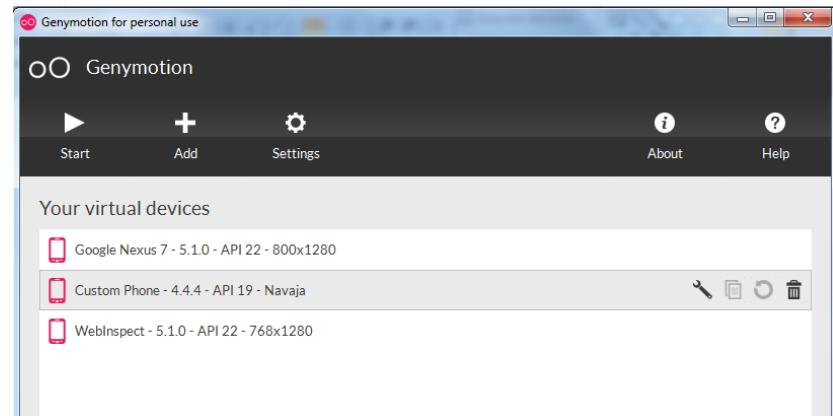
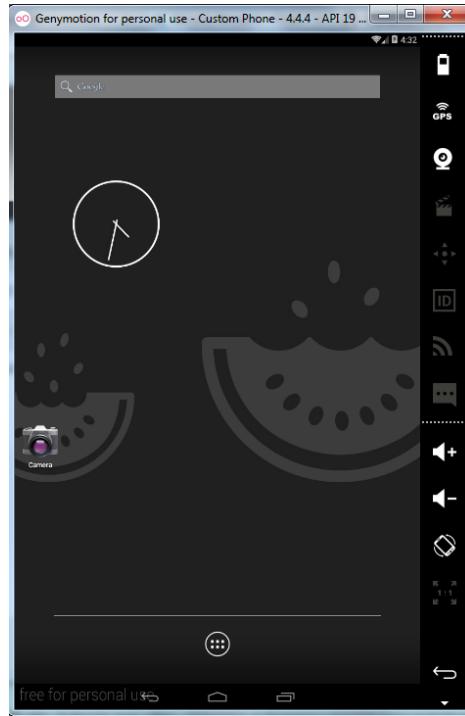
## Otras Herramientas

Otras herramientas de interés

- Genymotion
- Burp Proxy
- WireShark
- Android Studio
  - Lint
- Agnitio

## Otras Herramientas

### Otras herramientas de interés. Genymotion



## Otras Herramientas

### Otras herramientas de interés. Burp Proxy

Burp Suite Free Edition v1.6

Target Proxy Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

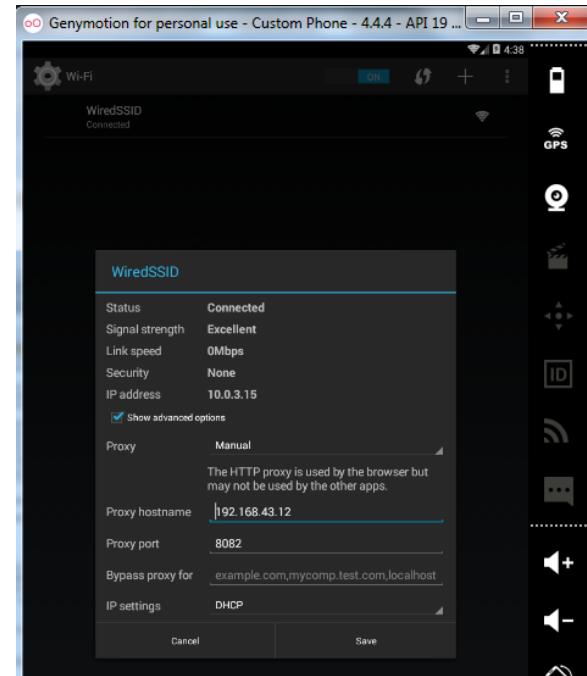
#	Host	Method	URL	Params	Edited	Status	Length	MIME type
5	https://mobile.twitter.com	GET	/i/config?client=android		<input checked="" type="checkbox"/>	200	4247	JSON
6	https://api.twitter.com	GET	/1/account/settings.json?lang=en&country=GB		<input checked="" type="checkbox"/>	200	1159	JSON
7	https://api.twitter.com	GET	/1/users/show.json?user_id=2723359616&include_media_features...		<input checked="" type="checkbox"/>	200	3830	JSON
8	https://api.twitter.com	POST	/scr...		<input checked="" type="checkbox"/>	200	863	
9	https://api.twitter.com	GET	/1/timeline/home.json?user_id=2728355961&pc=true&learned=true...		<input checked="" type="checkbox"/>	200	902	JSON
10	https://api.twitter.com	POST	/1/account/push_destinations.json?user_id=12e0166acd008612&enable...		<input checked="" type="checkbox"/>	200	870	JSON
11	https://api.twitter.com	GET	/1/account/timeline.json?woeid=1&tmezone=Africa%2fJohannesbur...		<input checked="" type="checkbox"/>	200	6432	JSON
12	https://api.twitter.com	POST	/1/help/settings.json		<input checked="" type="checkbox"/>	200	80	
13	https://api.twitter.com	GET	/1/help/settings.json		<input checked="" type="checkbox"/>	200	24650	JSON
14	https://api.twitter.com	GET	/1/help/experiments.json		<input checked="" type="checkbox"/>	200	29978	JSON
15	https://api.twitter.com	GET	/1/direct/messages.json?since_id=494185366711455744&count=1		<input checked="" type="checkbox"/>	200	788	JSON
16	https://api.twitter.com	GET	/1/direct/messages/send.json?count=200&include_entities=true&l...		<input checked="" type="checkbox"/>	200	788	JSON
17	https://api.twitter.com	GET	/1/activities/friends.json?model_version=7&send_error_codes=true...		<input checked="" type="checkbox"/>	200	788	JSON
18	https://api.twitter.com	GET	/1/account/about.json?max_results=10&card_error_codes=tr...		<input checked="" type="checkbox"/>	200	788	JSON

Request Response

Raw Params Headers Hex

```
GET /i/config?client=android HTTP/1.1
X-Twitter-Polling: True
X-Twitter-API-Version: 5
Accept-Language: es-GB
Authorization: OAuth realm="http://api.twitter.com/", oauth_version='1.0',
oauth_token="27283559619m9j0icXepgQGm9Rc49T9cSM75pMvn9lUr0A", oauth_nonce="17579119873115068021382C0406291",
oauth_timestamp="1406748104", oauth_signature="zFyBHe1c455%2FTnnXoOC4WhsuXt9%3D",
oauth_consumer_key="3iVtSoCBZuxU4vzUxfbv", oauth_signature_method="HMAC-SHA1"
X-Twitter-Client: TwitterAndroid
Accept-Encoding: gzip
User-Agent: TwitterAndroid/5.19.0 (3030722-r623) Galaxy Nexus/4.3 (samsung;Galaxy Nexus;google/yakju;0;1)
X-Twitter-Client-DeviceID: 12e0166acd666512
X-Twitter-Client-Version: 5.19.0
X-Client-UUID: 526a9eae-48ad-46fd-9a98-bcffee50b222
Host: mobile.twitter.com
Connection: Keep-Alive
```

Type a search term 0 matches



## Otras Herramientas

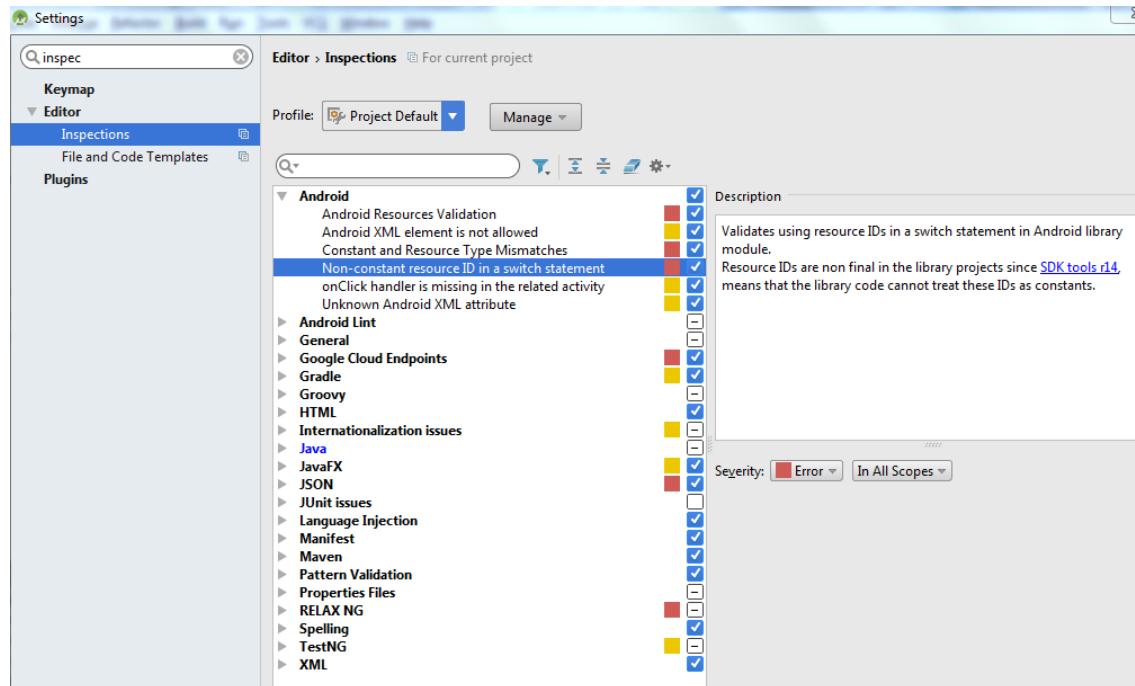
Otras herramientas de interés. Wireshark

The screenshot displays a Wireshark capture of network traffic on 'VirtualBox Host-Only Network #2'. The packet list shows many TCP connections between 192.168.80.1 and 192.168.80.101. The details and bytes panes provide a detailed view of the captured frames.

The screenshot shows the Wireshark interface. At the top, it says "The World's Most Popular Network Sniffer and Analyzer" and "Version 1.12.7 (v1.12.7-0-gfc8978 from 2012-07-10)". Below that is a blue bar with the word "Capture". The main area has a title "Interface List" with a gear icon. It displays a live list of capture interfaces: "Conexión de área local 3", "Conexión de red inalámbrica 2", "VirtualBox Host-Only Network" (which is selected and highlighted in blue), "Conexión de red inalámbrica 3", "VMware Network Adapter VMnet8", "Conexión de área local", "VirtualBox Host-Only Network #2", and "VMware Network Adapter VMnet1". A "Start" button with a green arrow icon is visible, followed by the instruction "Choose one or more interfaces to capture from, then Start".

# Otras Herramientas

## Otras herramientas de interés. Lint



## Otras Herramientas

### Otras herramientas de interés. Agnitio

Checklist Editor			
The checklist questions shown below can be modified and saved			
Number	Principle/s	Questions	Type
62	Auditing and Logging	Are logs correctly sanitised to ensure that sensitive data is not logged in clear text by the application?	Both
63	Auditing and Logging	Are all application errors logged to a central log server?	Both
64	Auditing and Logging	Does the design identify the level of auditing & logging needed and identify key parameters to be logged & audited?	Both
65	Auditing and Logging	Does the design ensure that successful and unsuccessful attempts to execute privileged actions are logged?	Both
66	Auditing and Logging	Does the design ensure that the content of audit logs meet the requirements of company/regulatory standards?	Both
78	Auditing and Logging	Does the application have non-repudiable logs for users access to paid resources?	Mobile
15	Authentication	Are application trust boundaries identified on the data flow diagrams in the design document?	Both
16	Authentication	Does the design identify the identities that are used to access resources across all trust boundaries?	Both
17	Authentication	Does the application require authentication for all resource access attempts except for publicly accessible resources?	Both
18	Authentication	Does the design identify the mechanisms used to protect user credentials whilst in transit?	Both
19	Authentication	Does the application ensure that minimal error information is returned in the event of authentication failure?	Both
20	Authentication	Does the application use authentication controls that fail in a secure manner?	Both

## Distribuciones

Distribuciones especializadas en Android

- Appie – 02/2015 <https://manifestsecurity.com/appie/>
- Santoku – 2014 <https://santoku-linux.com/>
- MobiSec – 05/2015 <http://mobisec.professionallyevil.com/>
- Vezir – 06/2015 <https://github.com/oguzhantopgul/Vezir-Project>

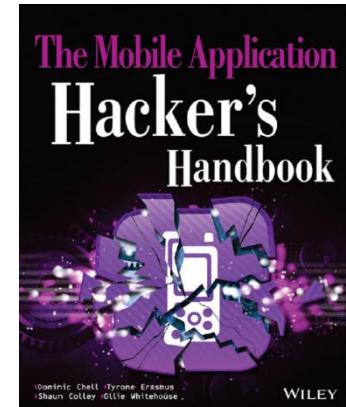
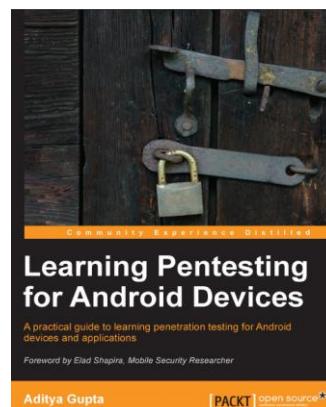
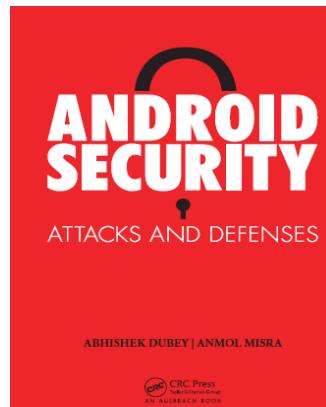
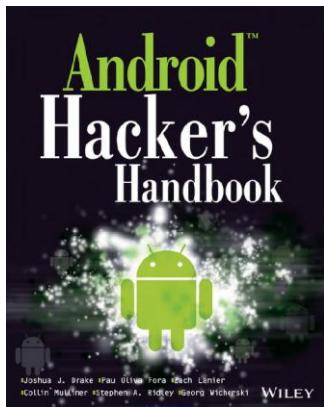
## Referencias

### Herramientas

- APKTool <http://ibotpeaches.github.io/Apktool/>
- Enjarify <https://github.com/google/enjarify>
- Dex2Jar <https://github.com/pxb1988/dex2jar>
- JD-GUI <http://jd.benow.ca/>
- AndroGuard <https://github.com/androguard/androguard>
- Androwarn <https://github.com/maaaaz/androwarn>
- Introspy <https://github.com/iSECPartners/Introspy-Android>
- Drozer <https://www.mwrinfosecurity.com/products/drozer/>

## Referencias

### Referencias



<https://koodous.com>

## ➤ E-Mails

- [info@ccn-cert.cni.es](mailto:info@ccn-cert.cni.es)
- [ccn@cni.es](mailto:ccn@cni.es)
- [sondas@ccn-cert.cni.es](mailto:sondas@ccn-cert.cni.es)
- [redsara@ccn-cert.cni.es](mailto:redsara@ccn-cert.cni.es)
- [organismo.certificacion@cni.es](mailto:organismo.certificacion@cni.es)

## ➤ Websites

- [www.ccn.cni.es](http://www.ccn.cni.es)
- [www.ccn-cert.cni.es](http://www.ccn-cert.cni.es)
- [www.oc.ccn.cni.es](http://www.oc.ccn.cni.es)



Síguenos en LinkedIn

