

.:: Bypass **SSL** Pinning en Android Apps::.

-= By surflaweb =-

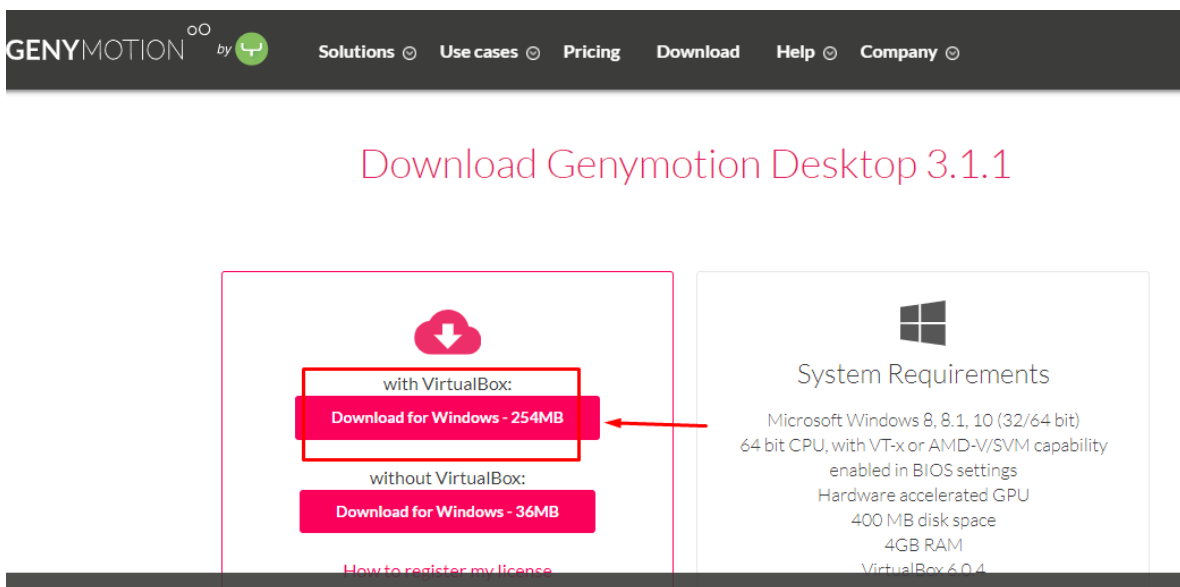
bypass the certificate verifications for one specific app, then you can intercept all your traffic!

Instalar herramientas:

Lo primero es instalar un emulador Android el cual tiene acceso root por defecto.

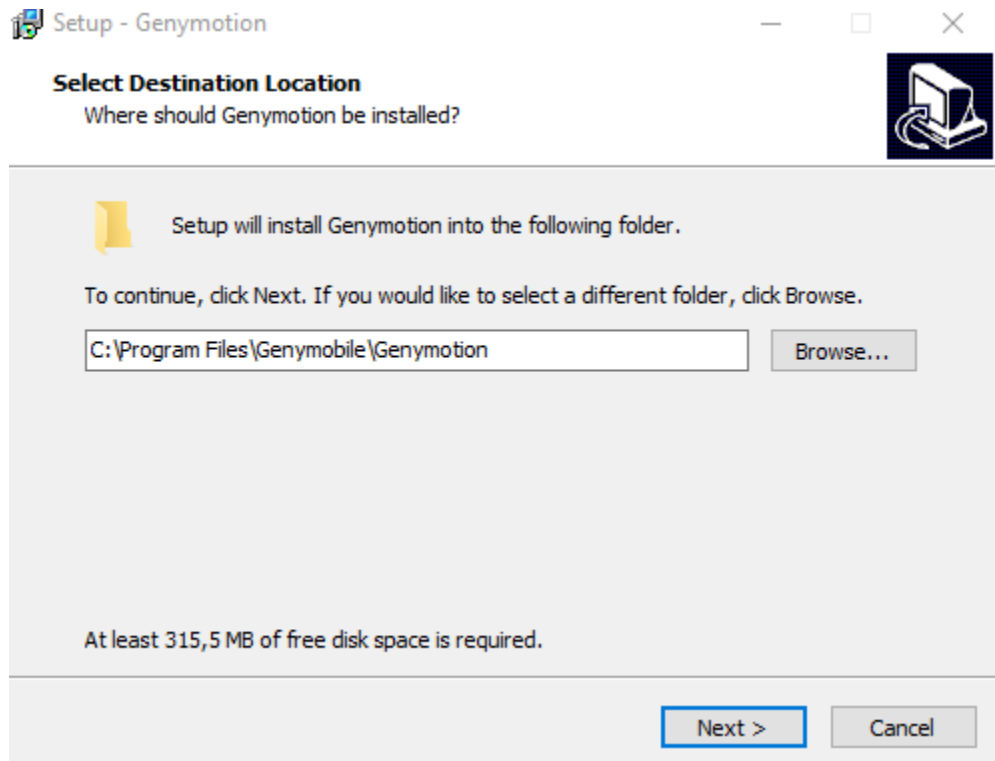
1. Descargar genymotion con virtualbox incluido:

<https://www.genymotion.com/download/>



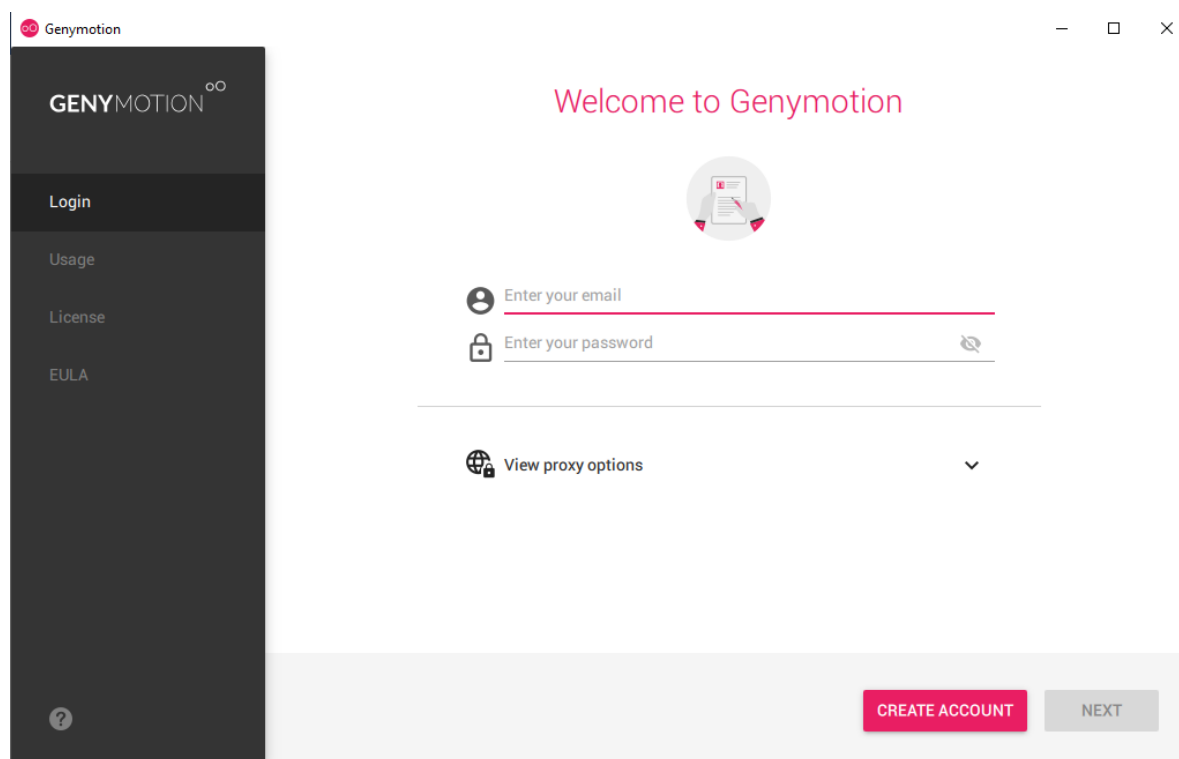
The screenshot shows the Genymotion website's download page. At the top is a dark navigation bar with the Genymotion logo and links for Solutions, Use cases, Pricing, Download, Help, and Company. Below this, the text 'Download Genymotion Desktop 3.1.1' is displayed in pink. The main content area is divided into two columns. The left column, titled 'Download', contains two download options: 'with VirtualBox: Download for Windows - 254MB' and 'without VirtualBox: Download for Windows - 36MB'. The 'with VirtualBox' option is highlighted with a red box and a red arrow points to it from the right. The right column, titled 'System Requirements', lists the necessary hardware and software: Microsoft Windows 8, 8.1, 10 (32/64 bit), 64 bit CPU, with VT-x or AMD-V/SVM capability enabled in BIOS settings, Hardware accelerated GPU, 400 MB disk space, 4GB RAM, and VirtualBox 6.0.4. A link 'How to register my license' is visible at the bottom of the left column.

2. Instalar genymotion.

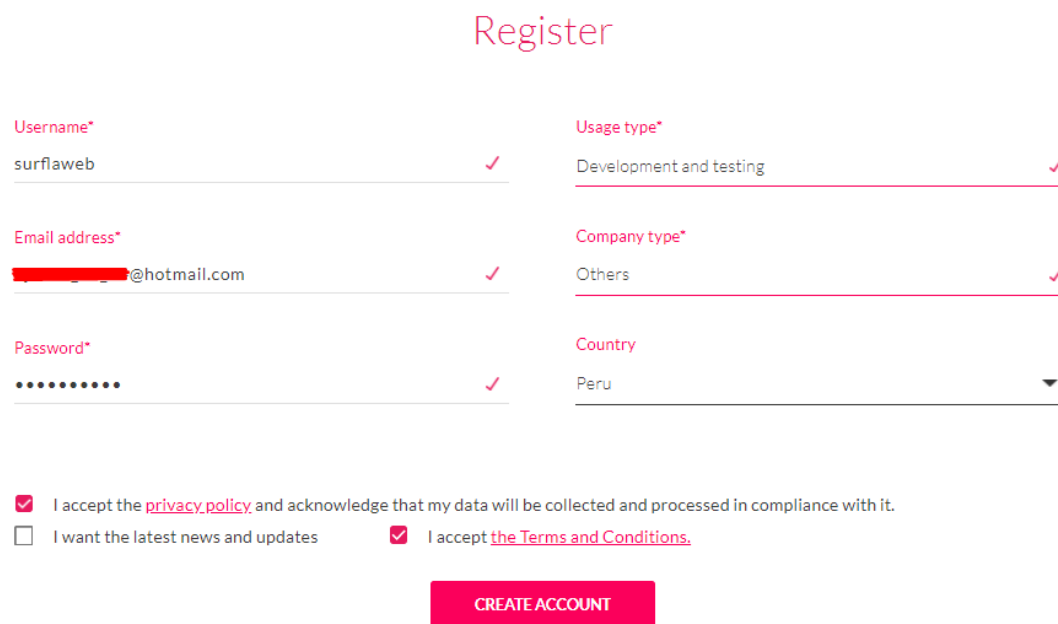




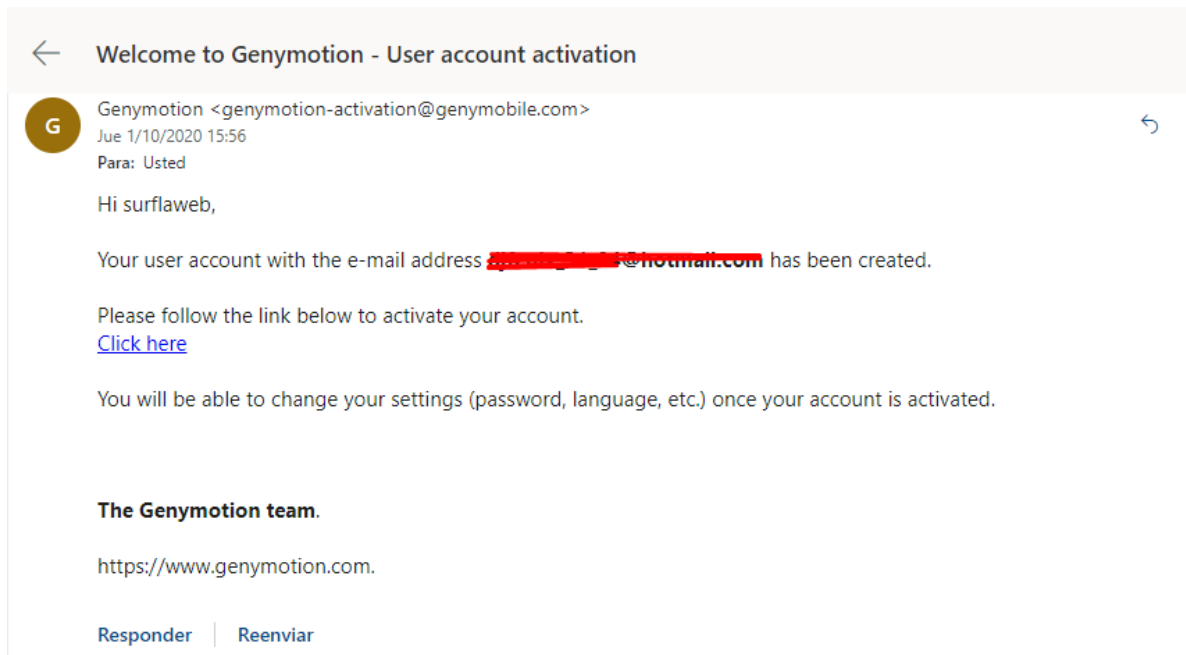
3. Abrimos genymotion y nos pide que creamos una cuenta:



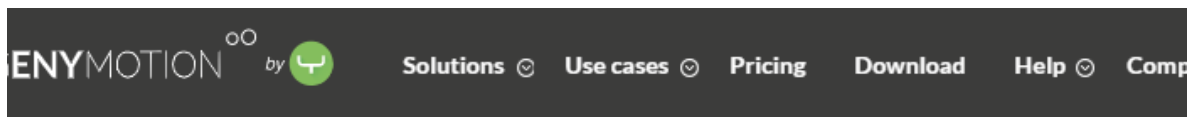
Nos registramos:



Luego debemos activar la cuenta nos enviaron un código al correo.



Hacemos click en el enlace para activar la cuenta.



Account activation

Lo siguiente es iniciar sesión en el programa genymotion y crear un emulador.

Genymotion requires a license



Use of Genymotion requires a license

Genymotion is a professional tool for which all kinds of profit-making businesses need a valid license. A very light version of Genymotion is available without a license, but strictly restricted to a personal use.

[Buy a license](#) (if you don't already have one)

☐ I have a license

☒ Personal Use

BACK

NEXT

Creamos un emulador con la versión 8 de Android

Type	Device	Android API	Size	Density	Source	
	Samsung Galaxy S6	7.1 - API 25	1440 x 2560	640 - XXXHDPI	Genymotion	
	Samsung Galaxy S7	7.1 - API 25	1440 x 2560	560	Genymotion	
	Custom Phone	8.0 - API 26	768 x 1280	320 - XHDPI	Genymotion	
	Custom Tablet	8.0 - API 26	1536 x 2048	320 - XHDPI	Genymotion	
	Google Nexus 5X	8.0 - API 26	1080 x 1920	420	Genymotion	
	Google Nexus 6	8.0 - API 26	1440 x 2560	560	Genymotion	
	Google Nexus 6P	8.0 - API 26	1440 x 2560	560	Genymotion	

CANCEL
NEXT

Le ponemos un nombre al emulador y lo instalamos.

Virtual device installation

Name

Display

☒ Predefined
 768 x 1280
 320 - XHDPI

☐ Custom

☐ Start in full-screen mode

System

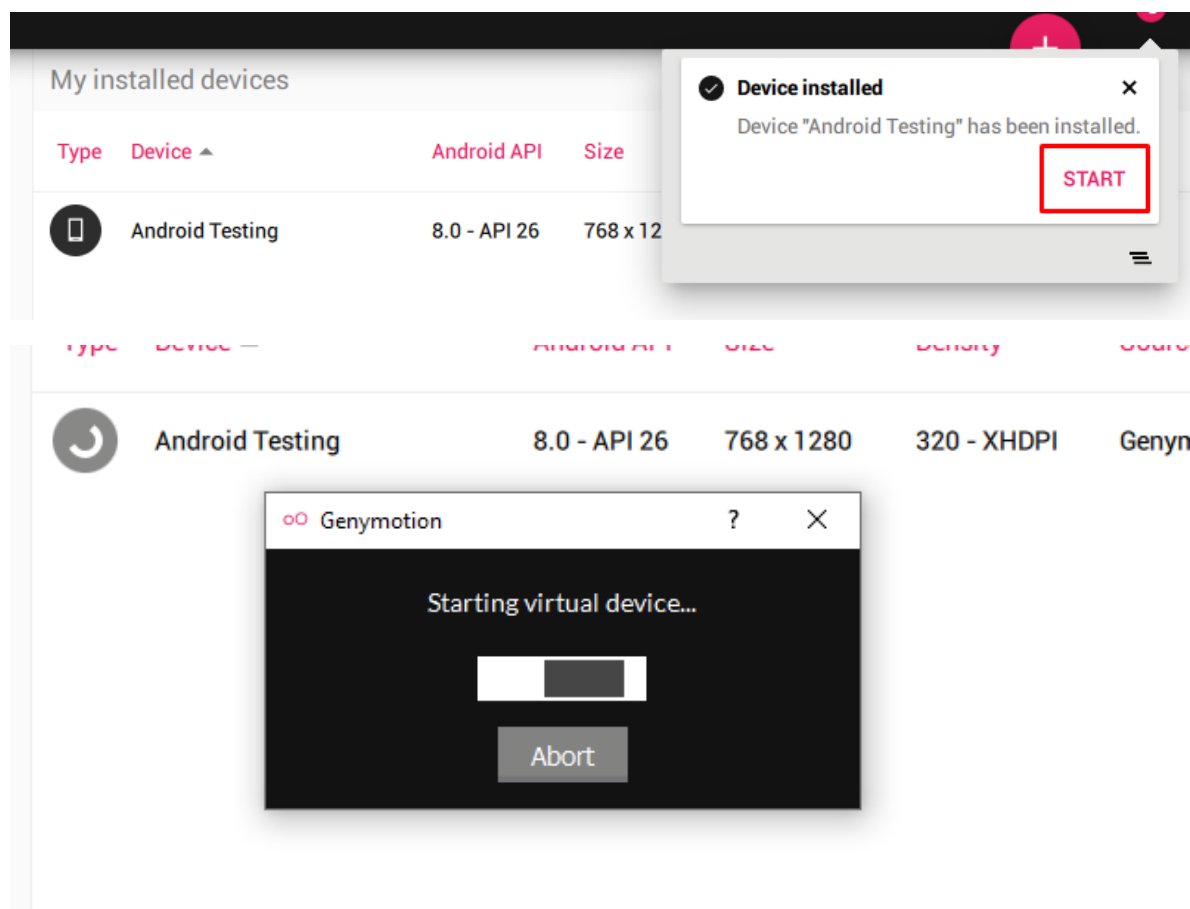
Android version
 8.0

Processor(s)
 4

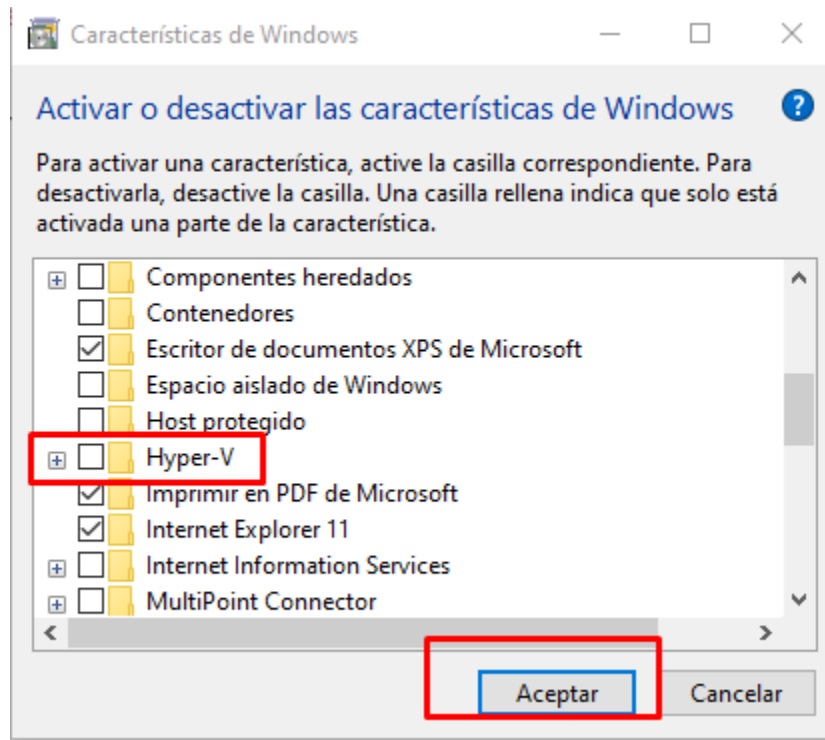
Memory size
 2048

BACK
INSTALL

Una vez creado el emulador lo iniciamos:

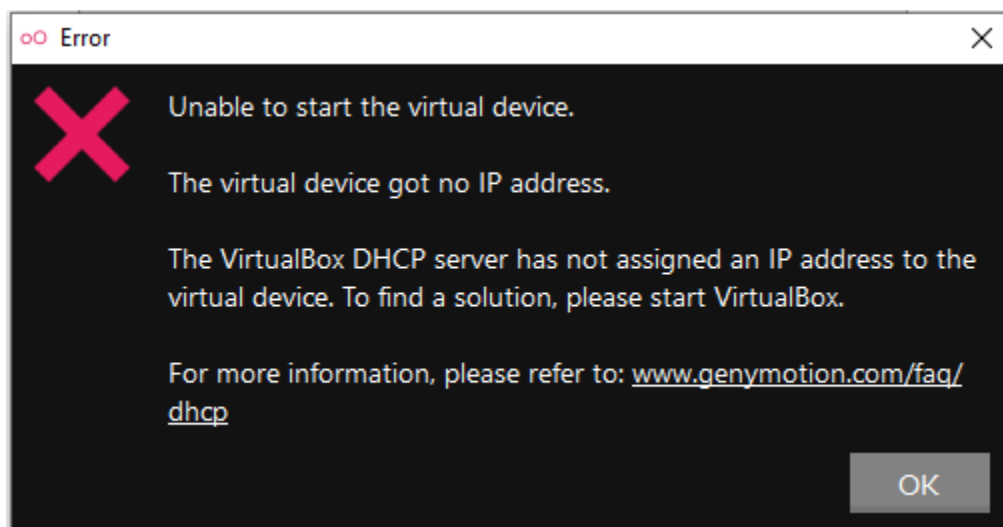


En caso de iniciarse el emulador desactivar Hyper-v de Windows si lo teníamos activado.

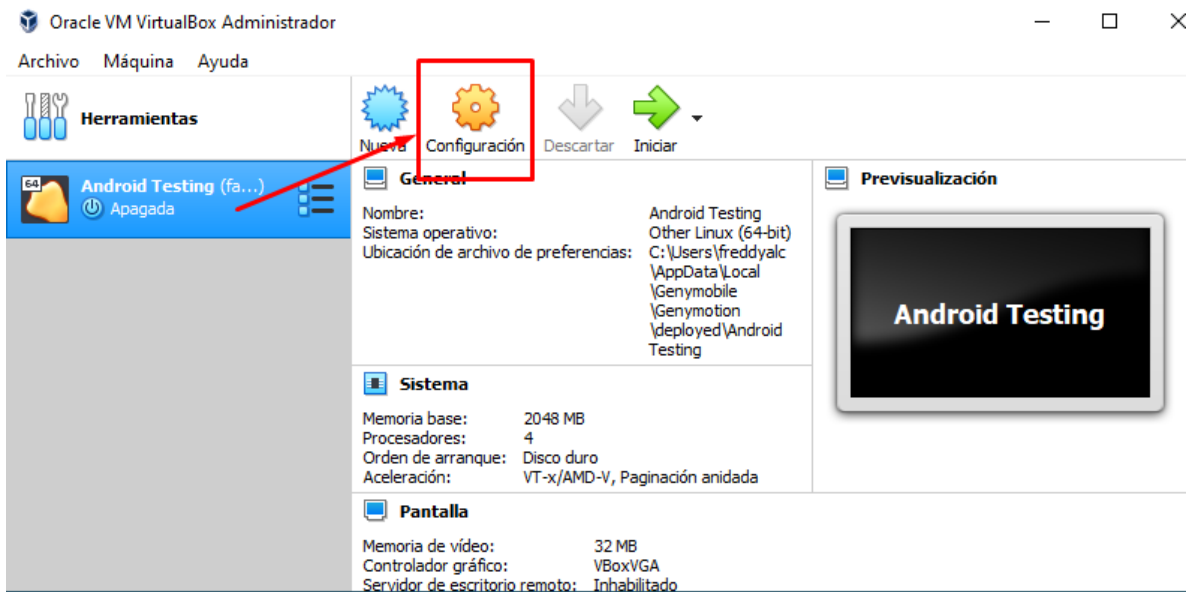


Luego de desactivar Hyper-v se reiniciar el PC.

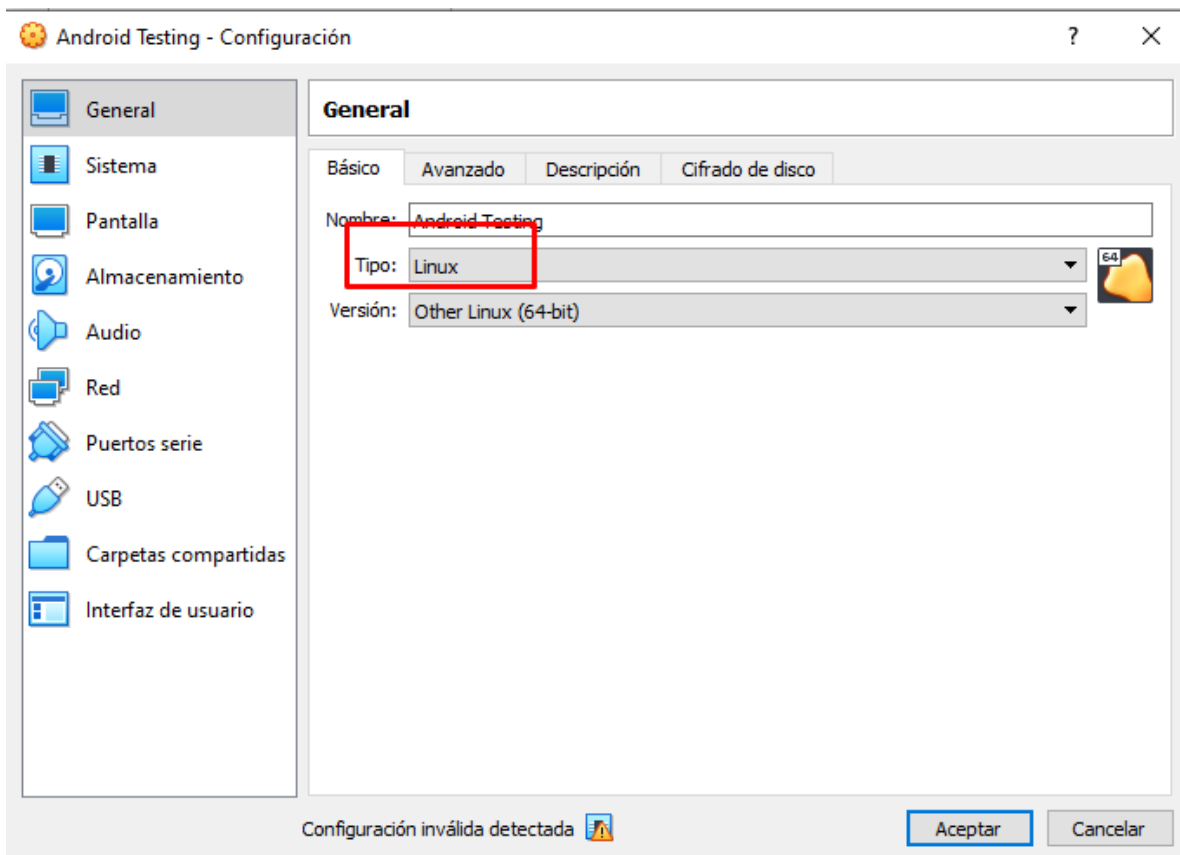
Sin embargo, luego de iniciar el dispositivo sale el error de que no se pudo obtener IP para el dispositivo. Veremos como solucionarlo.






Abrimos virtualbox y vamos a configuración del dispositivo creado:



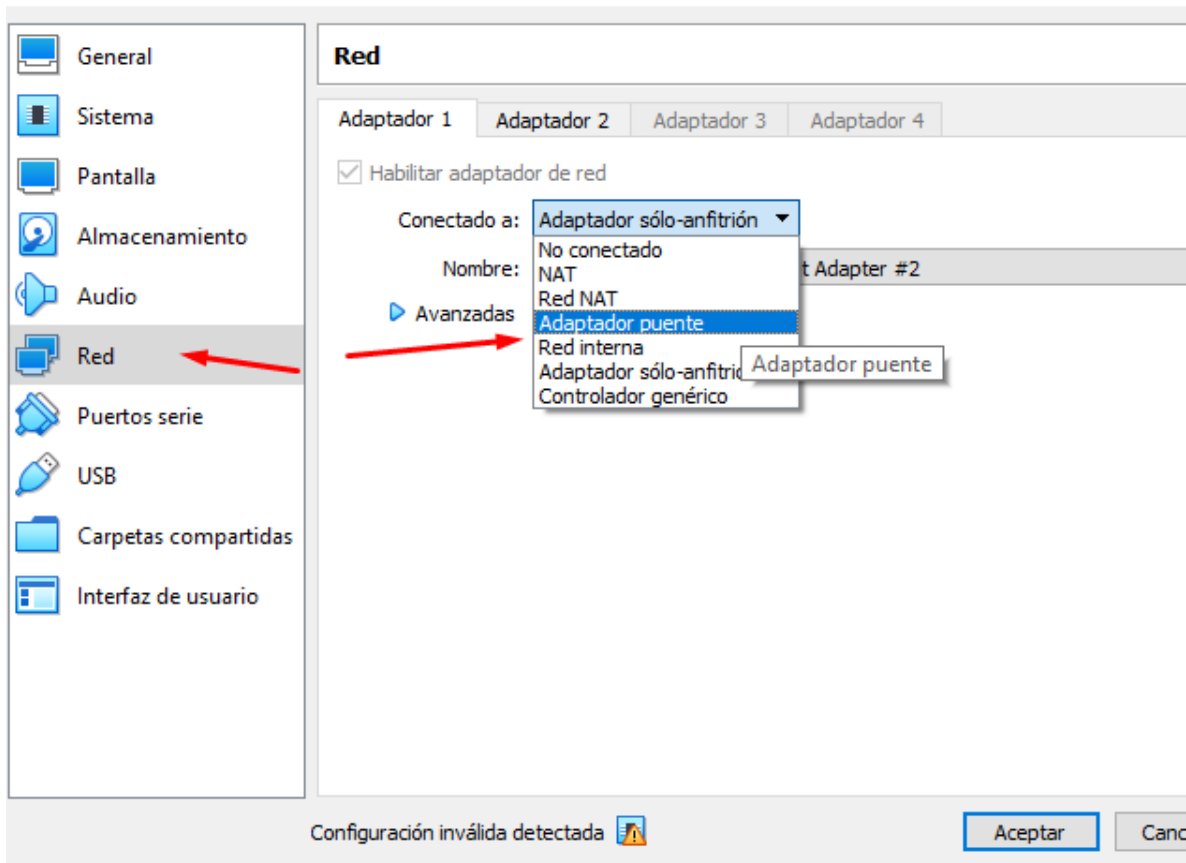
Vamos a cambiar el tipo de sistema operativo a Windows.



Nombre:	Android Testing
Tipo:	Microsoft Windows
Versión:	Windows 10 (64-bit)



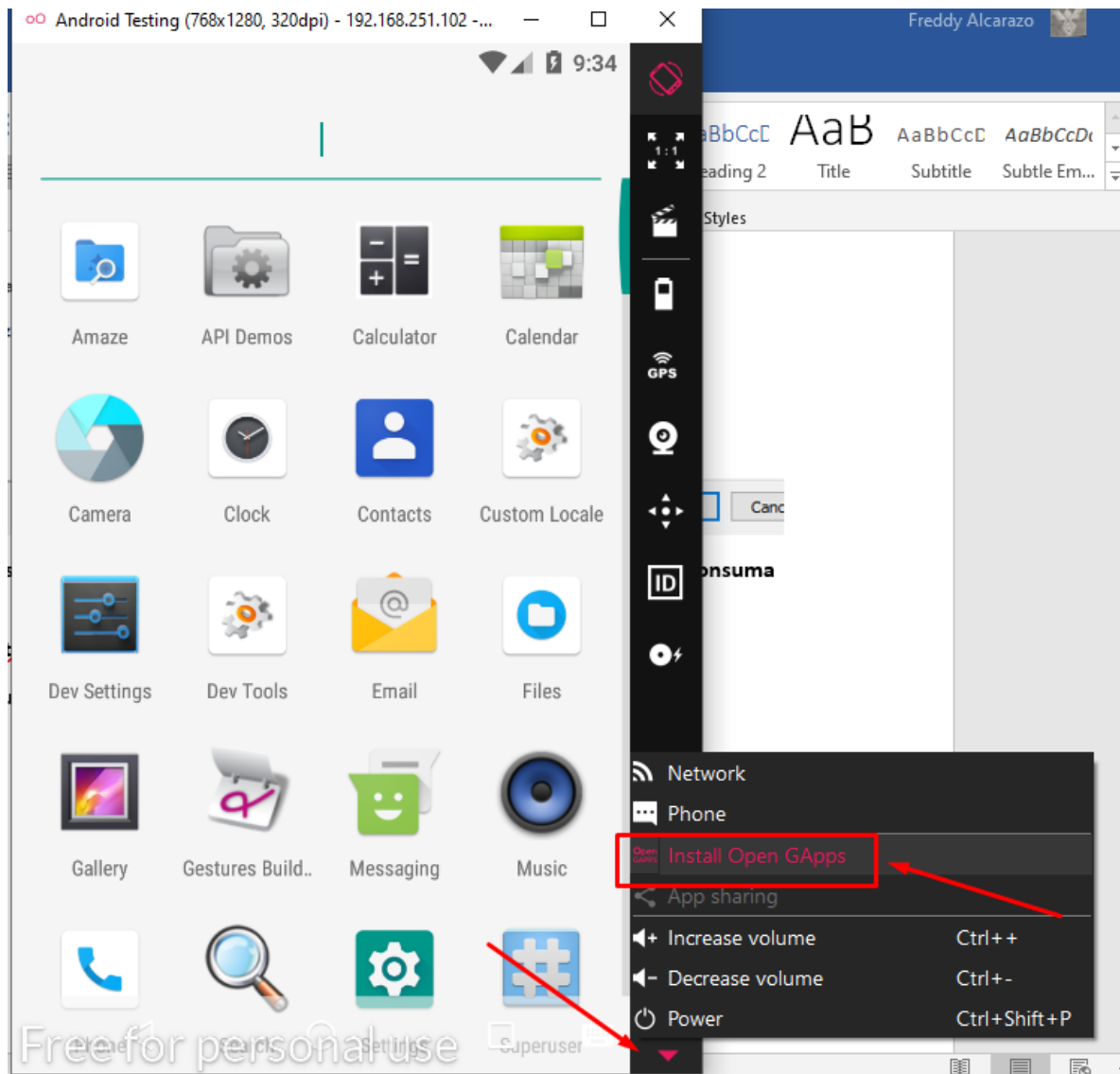
Luego nos vamos a la opción de “RED” y configuramos la red como “adaptador de puente”:



Aceptamos y volvemos a iniciar el emulador “cerramos virtualbox para que no consuma memoria”

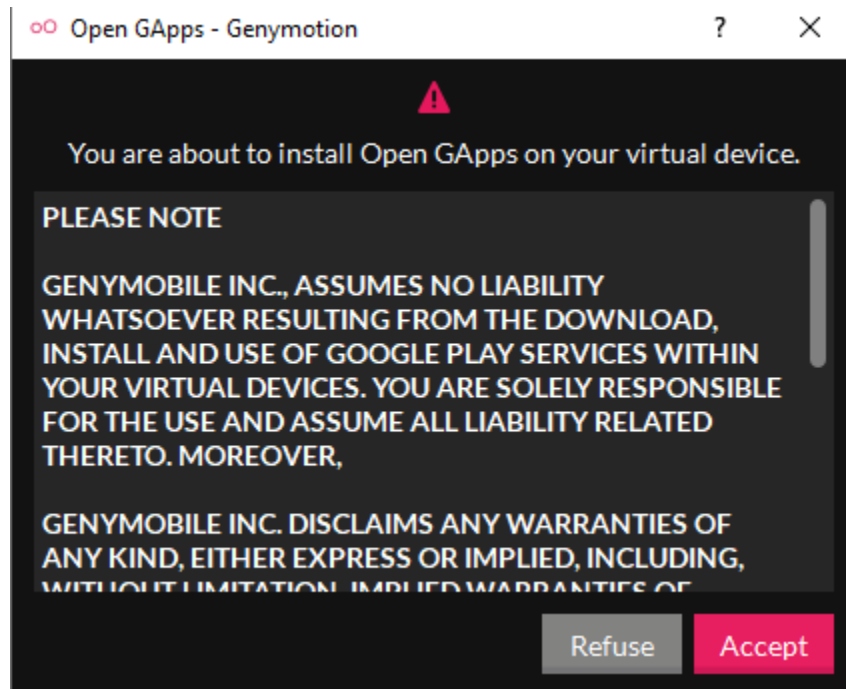
4. Instalar Google play store en genymotion.

Con el emulador abierto nos vamos a esta opción:



Seleccionamos "Install Open GApps":

Y aceptamos los términos.



Lo siguiente será instalar “Xposed-Frame-work” en este le instalaremos un módulo para hacer bypass a SSL Pinning.



Hacemos click en el enlace que nos lleva a un foro ahí luego aremos click en el siguiente enlace para descargar la versión SDK26 de xposed que funciona para Android 8.

Downloads:

XposedInstaller_*.apk from this thread: Must be installed to manage installed modules, the framework won't work without it.

xposed*.zip from <https://dl-xda.xposed.info/framework/> Must be flashed with a custom recovery (e.g. TWRP) to install the framework. SDK21 is Android 5.0 (Lollipop), SDK22 is Android 5.1 (also Lollipop) and SDK23 is Android 6.0 (Marshmallow). For Nougat, SDK24 is Android 7.0 and SDK25 is Android 7.1. For Oreo, SDK26 is Android 8.0 and SDK27 is Android 8.1. I only support the latest Xposed version per Android release!

<https://forum.xda-developers.com/showthread.php?t=3034811>

Index of /framework/

../	
sdk21/	10-Sep-2015 12:40
sdk22/	10-Sep-2015 12:40
sdk23/	08-Nov-2015 21:03
sdk24/	06-Oct-2017 10:24
sdk25/	06-Oct-2017 11:06
sdk26/	08-Jan-2018 20:04
sdk27/	08-Jan-2018 18:02
uninstaller/	18-Jan-2018 17:40

<https://dl-xda.xposed.info/framework/>

Index of /framework/sdk26/

../		
arm/	28-Jan-2018 19:54	-
arm64/	29-Jan-2018 17:44	-
x86/	29-Jan-2018 17:44	-

Index of /framework/sdk26/x86/

../		
xposed-v90-sdk26-x86-beta1.zip	08-Jan-2018 20:13	4760846
xposed-v90-sdk26-x86-beta1.zip.asc	08-Jan-2018 20:13	833
xposed-v90-sdk26-x86-beta2.zip	17-Jan-2018 21:40	4761534
xposed-v90-sdk26-x86-beta2.zip.asc	17-Jan-2018 21:40	833
xposed-v90-sdk26-x86-beta3.zip	28-Jan-2018 19:54	4770182
xposed-v90-sdk26-x86-beta3.zip.asc	28-Jan-2018 19:54	833

Este equipo > Escritorio > GenyMotion y Xposed >

Nombre	Fecha de modificación	Tipo	Tamaño
bypass SSL Pinning	1/10/2020 16:41	Microsoft Word D...	1,005 KB
xposed-v90-sdk26-x86-beta3	1/10/2020 16:41	Archivo WinRAR Z...	4,659 KB
genymotion-3.1.1-vbox	1/10/2020 15:45	Aplicación	248,051 KB

Volvemos al foro y descargamos el apk:

<https://forum.xda-developers.com/showthread.php?t=3034811>

master key, the files are signed with subkey 852109AA.

Known issues:

- Before Nougat: **Bootloops on Samsung stock ROMs**. That's due to Samsung's changes to ART. The ROM.
- Sony seems to have shipped some ROMs with corrupted services.odex (the embedded .dex is invalid exception expected: java.lang.ArrayIndexOutOfBoundsException" error, which I unfortunately cannot reproduce).
- Dell ships (at least) their Venue 8 7840 with a non-standard version of ART that is somewhere between Lollipop and Nougat. See <https://github.com/rovo89/Xposed/issues/77>

For discussions, please use the discussion threads (Lollipop and Nougat) matching one in this subforum.

Attached Files

XposedInstaller_3.1.5.apk [Click for QR Code] (2.96 MB, 3602986 views)

Descargar el apk de xposed.

Ahora vamos a flashear el emulador con los archivos del .zip del framework lo arrastramos al emulador de genymotion:

GenyMotion y Xposed

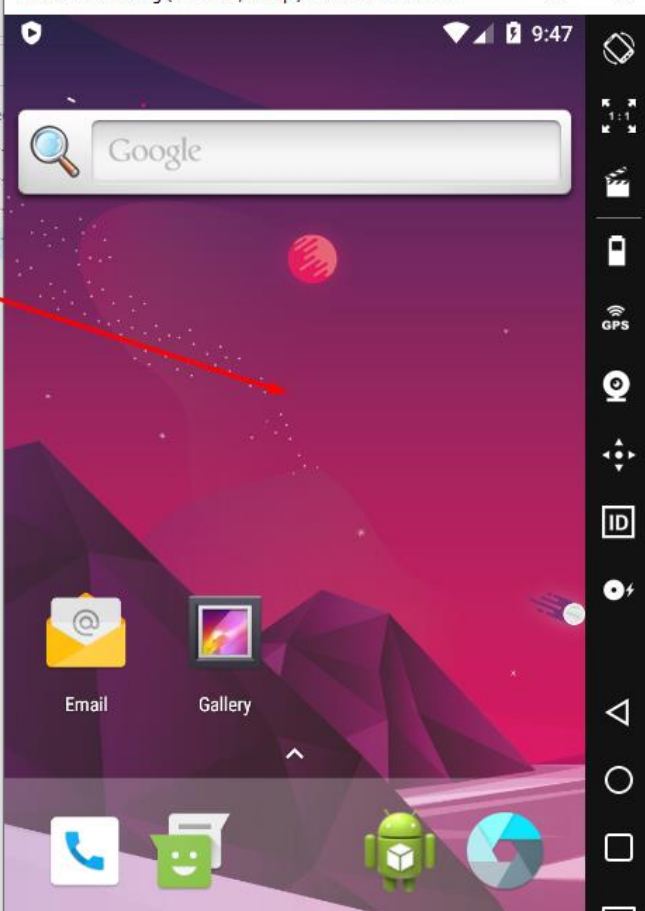
Compartir Vista

> Este equipo > Escritorio > GenyMotion y Xposed

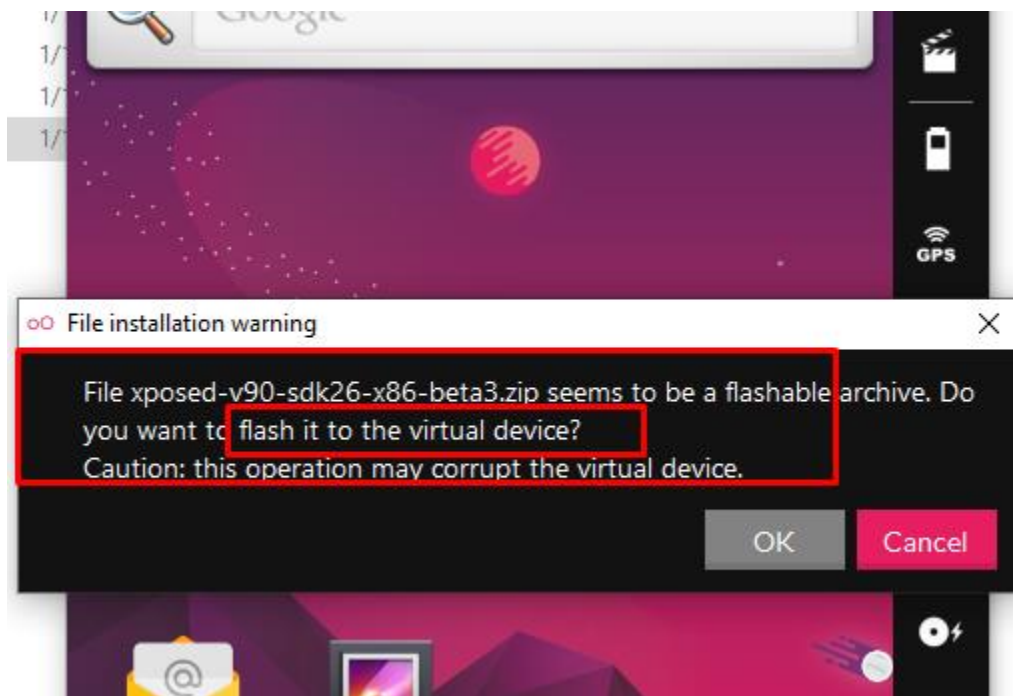
Nombre

bypass SSL Pinning
genymotion-3.1.1-vbox
XposedInstaller_3.1.5.apk
xposed-v90-sdk26-x86-beta3

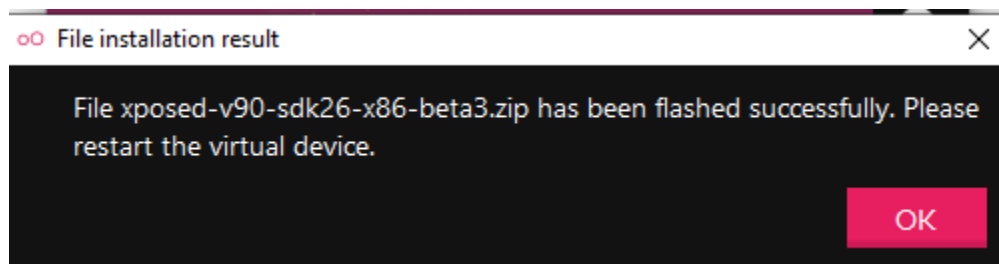
Android Testing (768x1280, 320dpi) - 192.168.251.102 - ...



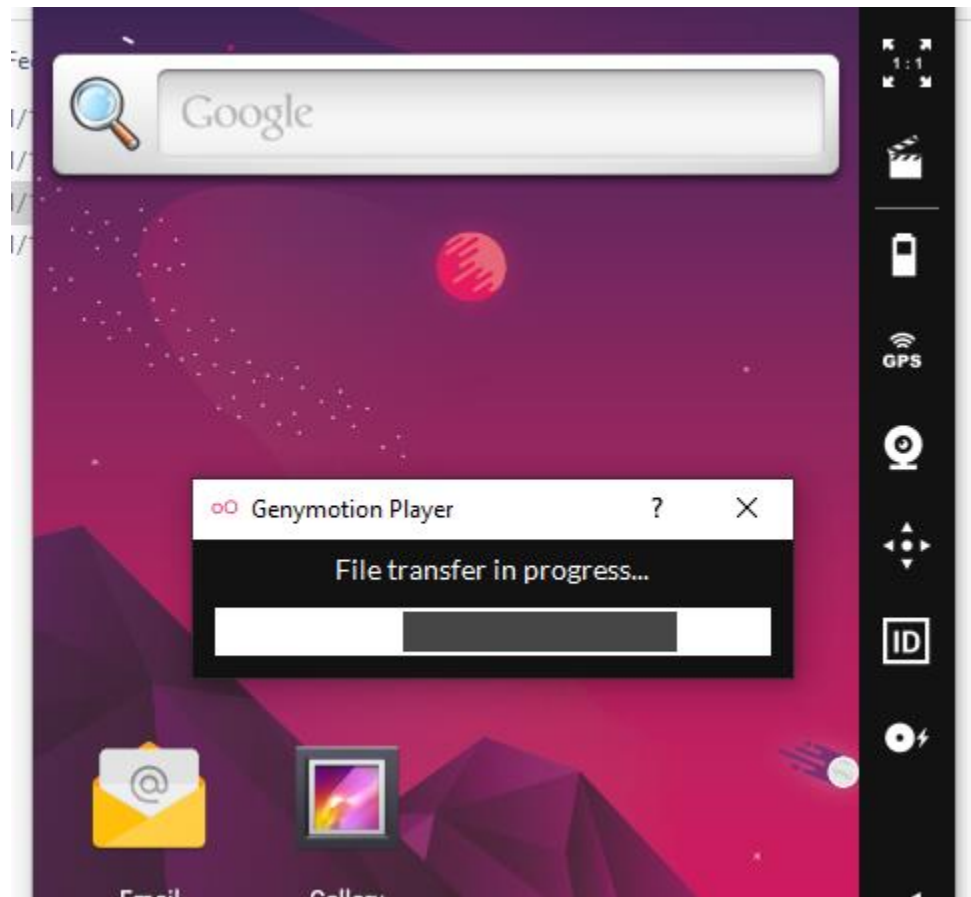
Presionamos el “ok”



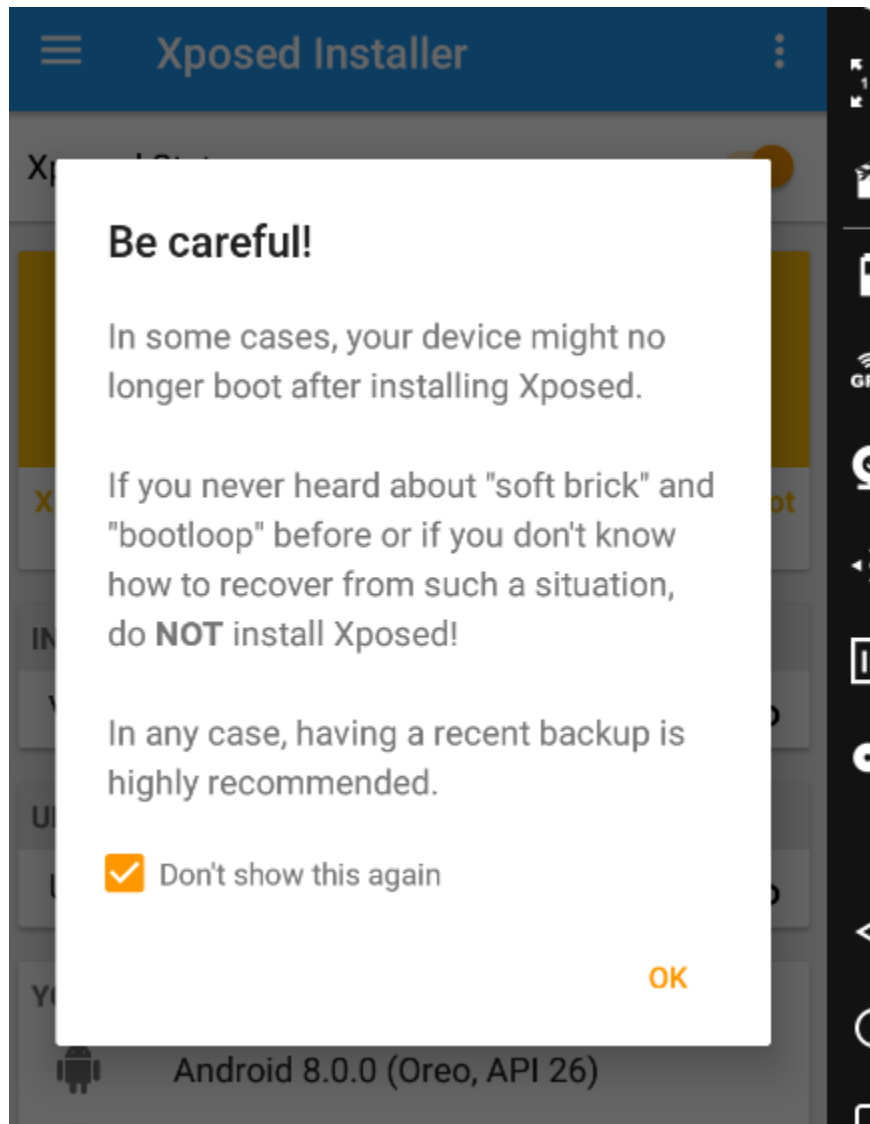
Resultado exitoso:



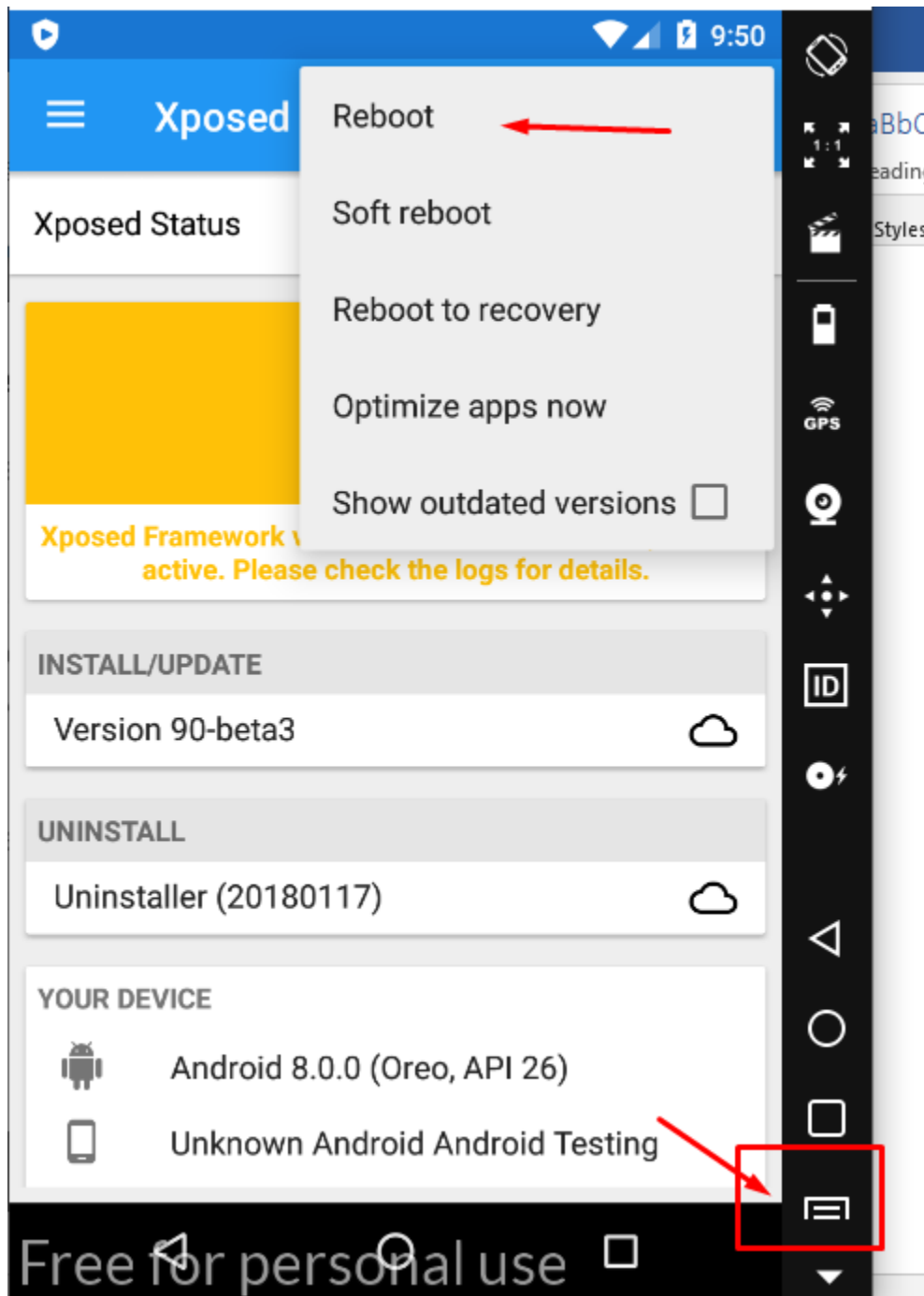
Ahora arrastramos el apk del framework:



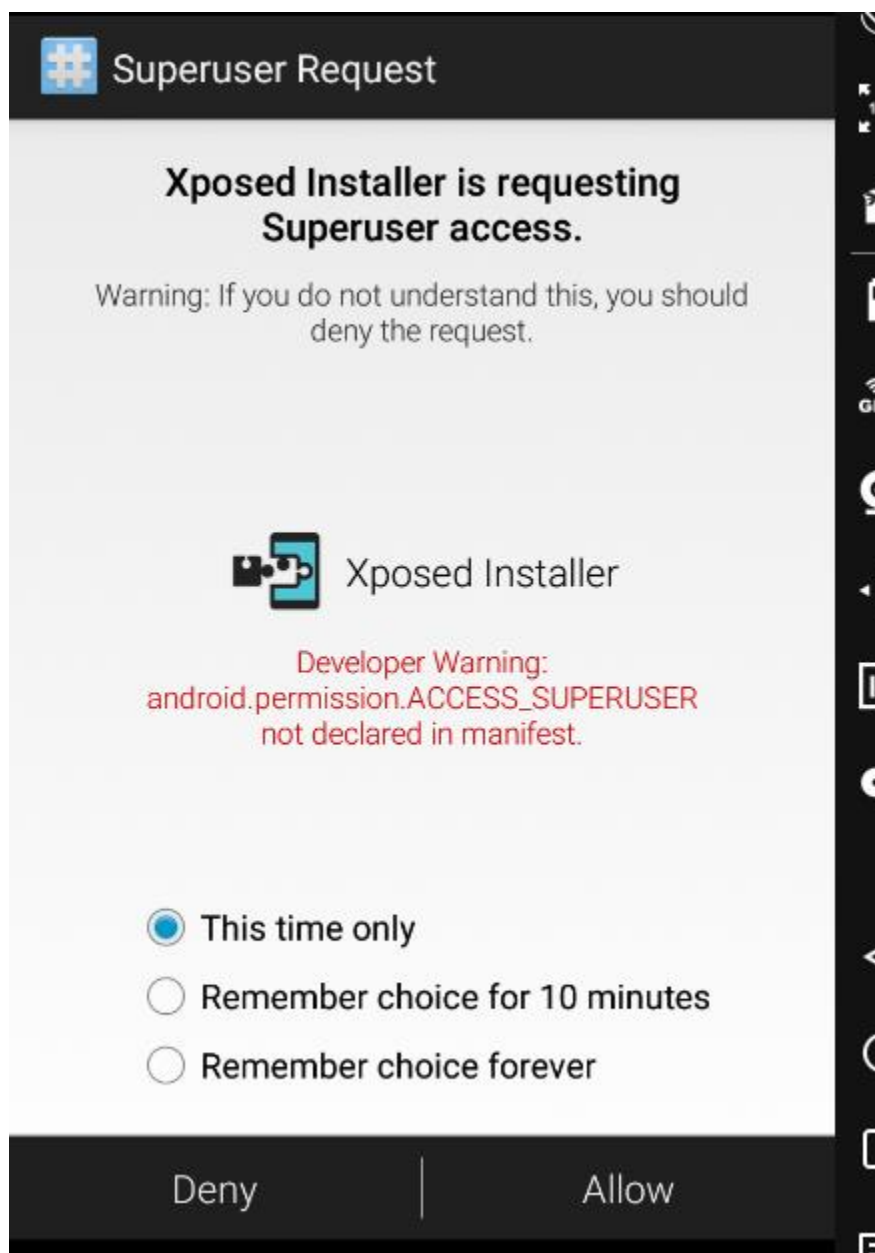
Y se instala:



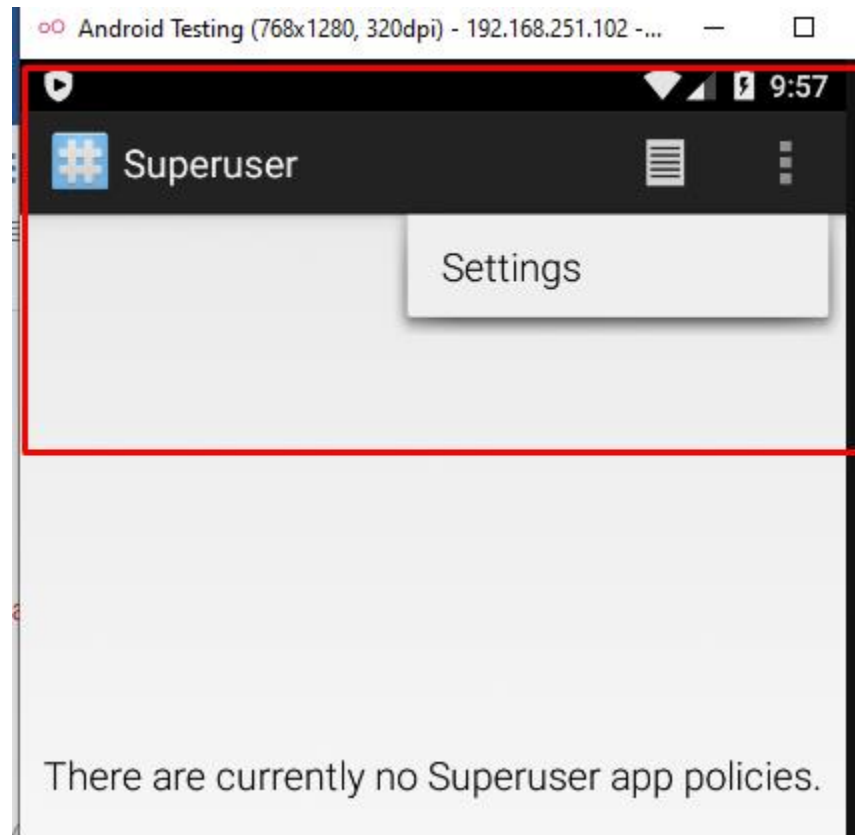
Reiniciamos:



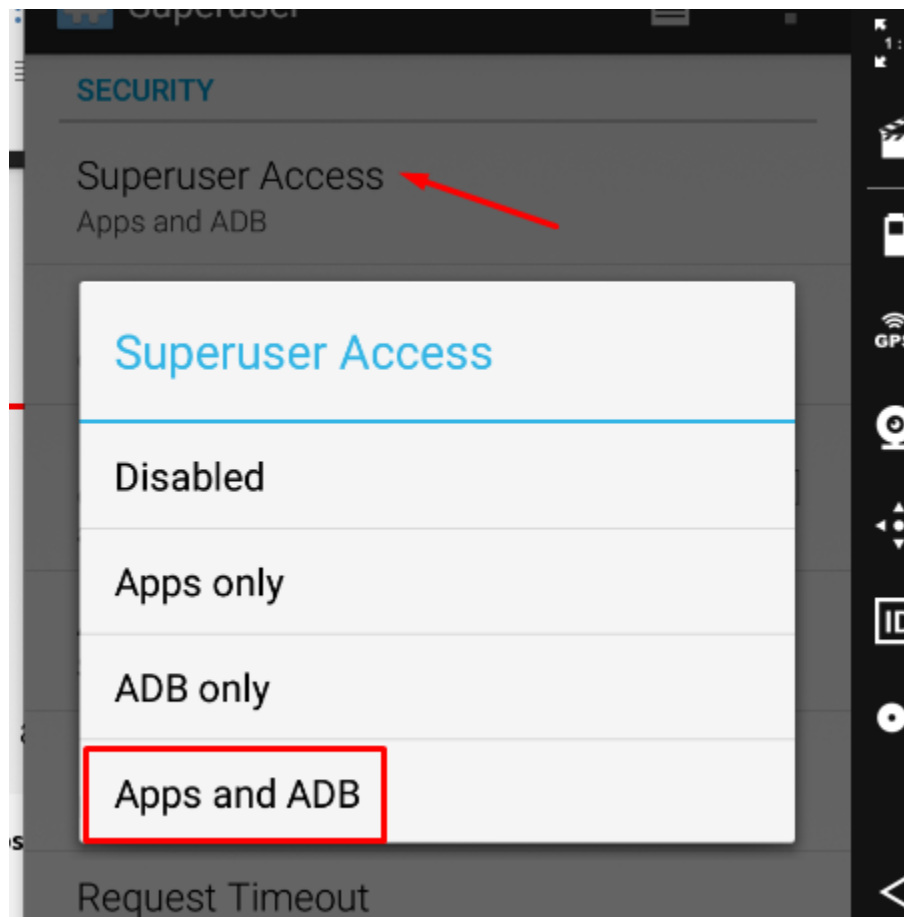
Nos pide permiso ROO le damos en “Allow”



Si se traba cerramos el emulador y luego lo iniciamos otra vez y esta vez abrimos el “Super User:”



Nos vamos a “Settings”:



SECURITY

Superuser Access

Apps and ADB

Multiuser Policy

Only the device owner can request Superuser

Declared Permission

Only allow requests from apps that declare
android.permission.ACCESS_SUPERUSER

☐

Automatic Response

Show confirmation dialog for new requests

PIN Protection

Require entry of a PIN to approve Superuser requests

Request Timeout

Superuser requests will time out and be denied

Automatic Response

Prompt

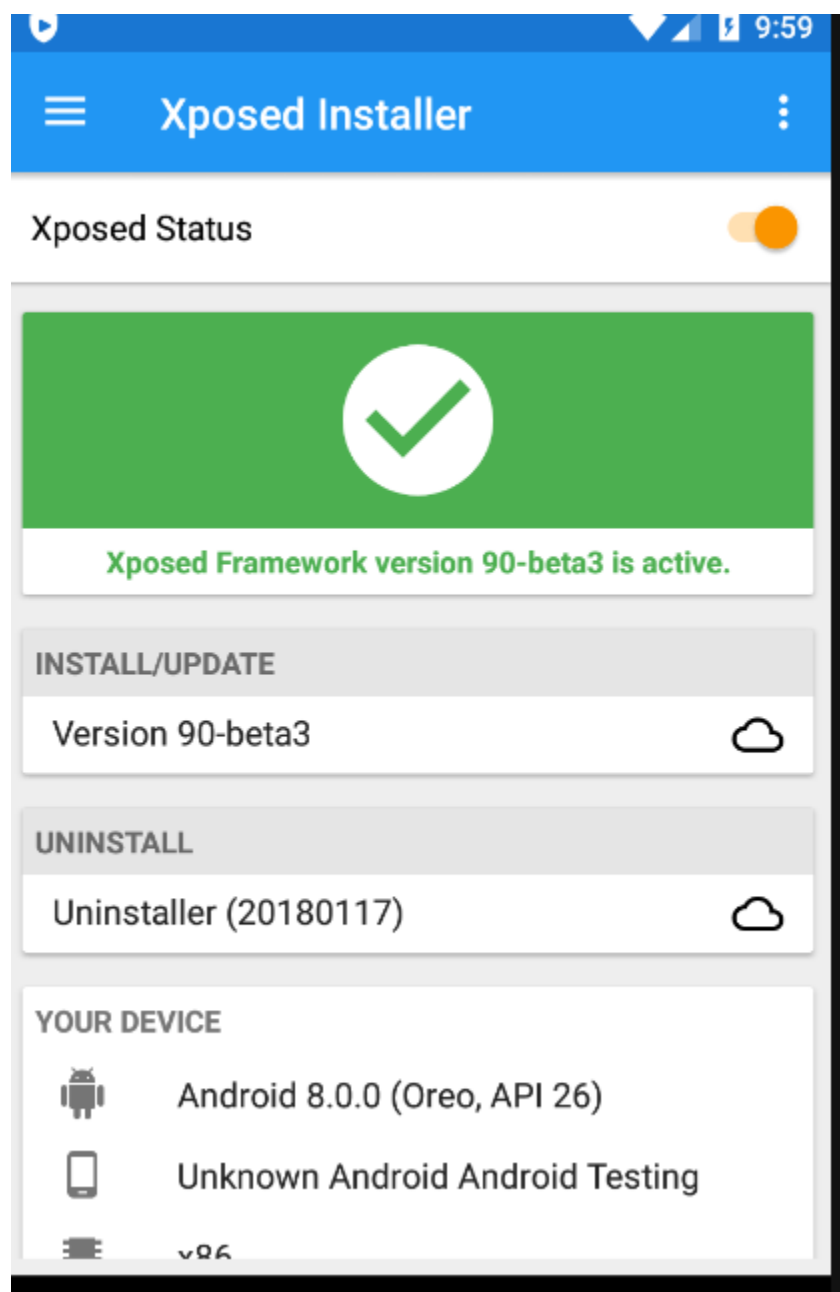
Deny

Allow

Require entry of a PIN to approve Superuser requests

Request Timeout

Ahora al abrir xposed en realidad no lo abrí ya estaba abierto si no estaba lo abrimos y ya aparece en verde que quiere decir que esta activado, si les pide reiniciar le dan en reiniciar. A mi se me trabó en el paso anterior por eso cerré el emulador.



Ahora descargaremos el Apk de SSLUnpinning:

⇒ <https://repo.xposed.info/module/mobi.acpm.sslunpinning>

SSLUnpinning - Certificate Pinning Bypass

If you need to intercept the traffic from an app which uses certificate pinning, with a tool like Burp Proxy, the SSLUnpinning will help you with this hard work!

The SSLUnpinning through Xposed Framework, makes several hooks in SSL classes to bypass the certificate verifications for one specific app, then you can intercept all your traffic.

API

- org.apache.http.conn.ssl.*

OKHTTP

- okhttp3.*

Attention: I'm working in a new suite of tools that include SSLUnpinning feature and many, many others! Look here -> <https://github.com/ac-pm>

Author(s): [acarlosmartins](#)

Support/Discussion URL: <http://forum.xda-developers.com/xposed/modules/mod-sslunpinning-certificate-pinning-t3221452>

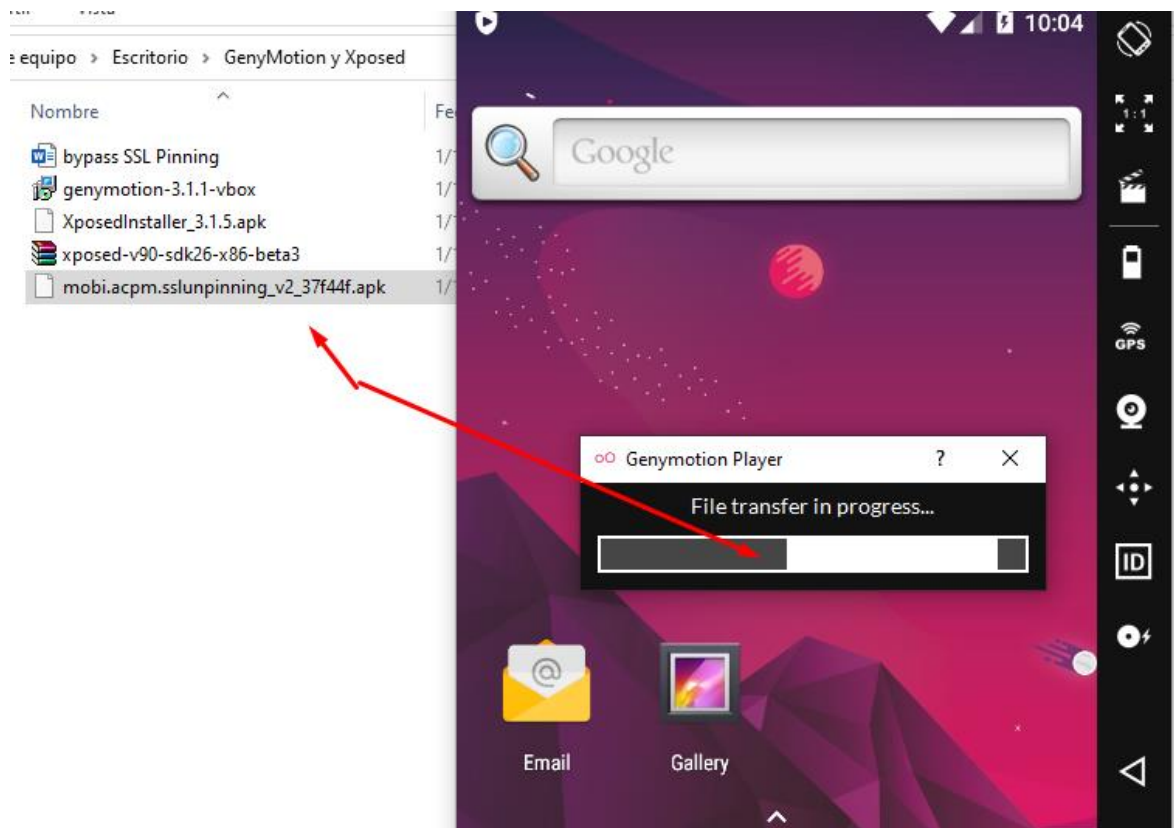
Source code URL: https://github.com/ac-pm/SSLUnpinning_Xposed

Package: mobi.acpm.sslunpinning

Version name:	2.0
Release type:	Stable (low risk of bugs)
Download:	mobi.acpm.sslunpinning_v2_37f44f.apk (1.02 MB)
Number of downloads:	35,331 in total ~ 48 in the last 24 hours
MD5 checksum:	37f44f9279c719dff575363f09bf2d58
Uploaded on:	Monday, September 12, 2016 - 05:48
Changes:	Added XPrefs instead of read/write file, okhttp3 pinning hooked and list all apps after user apps.

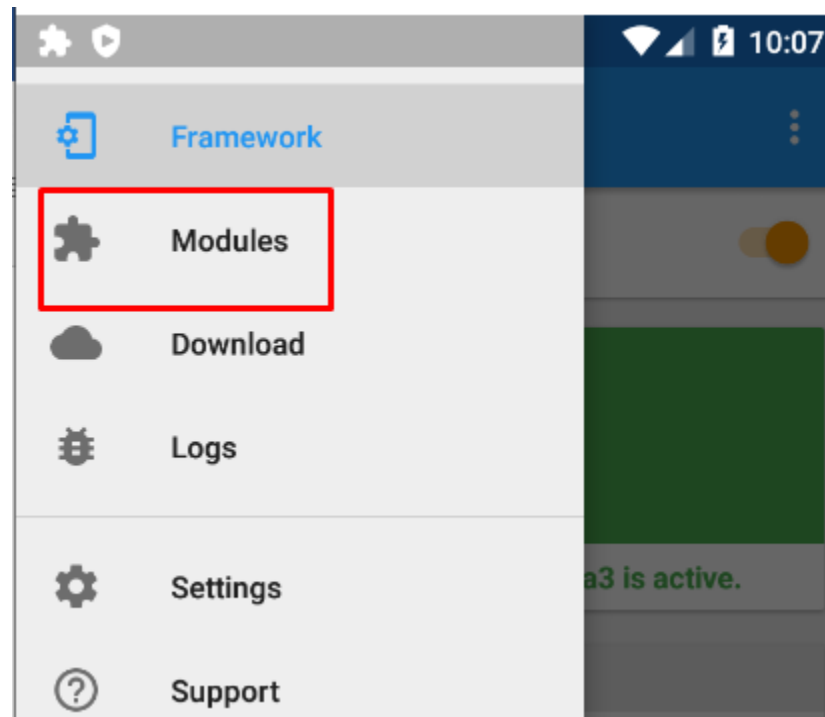
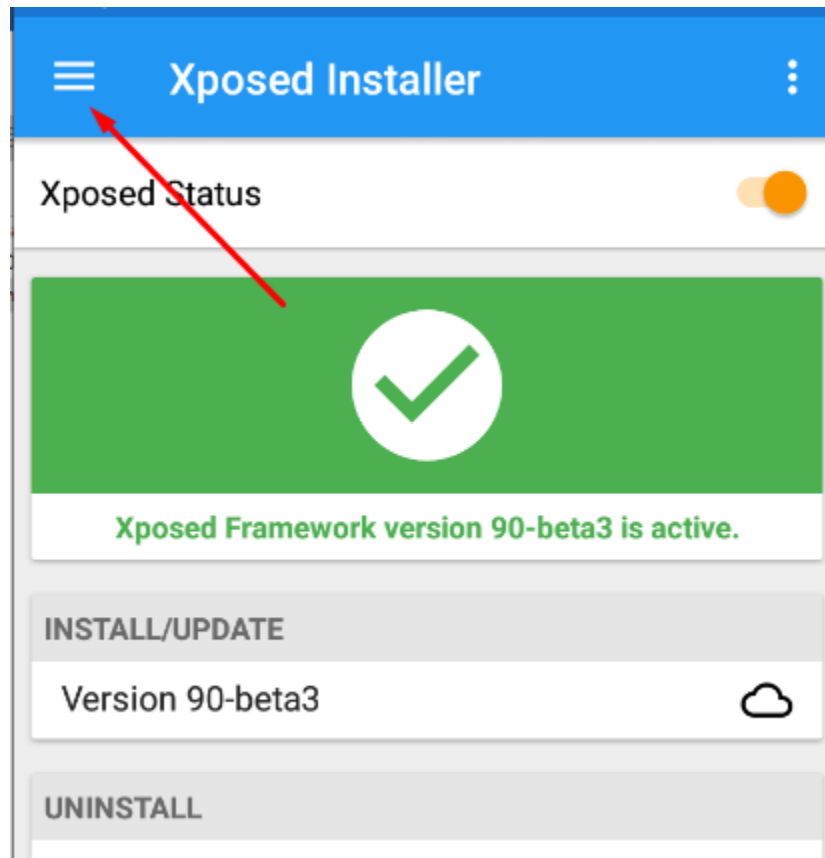
[Show older versions](#)

Ahora instalaremos el APK descargada en el emulador, solamente la arrastramos:

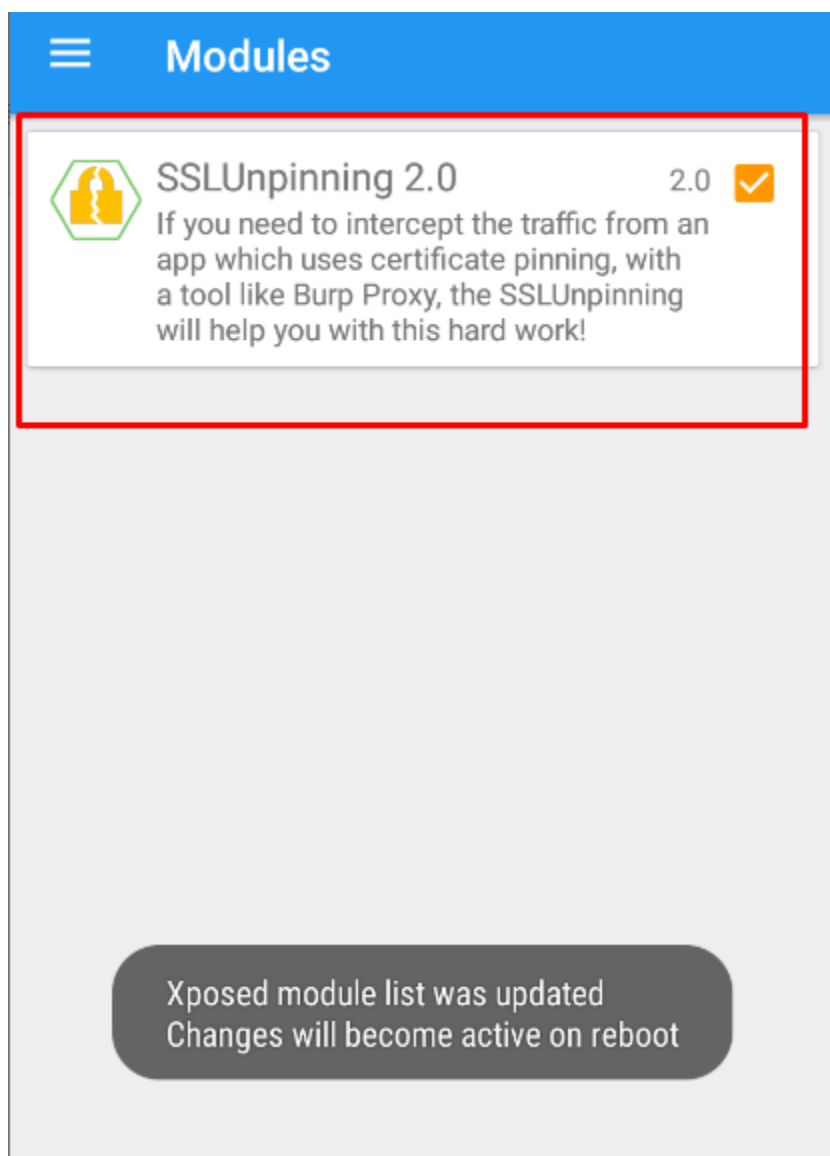


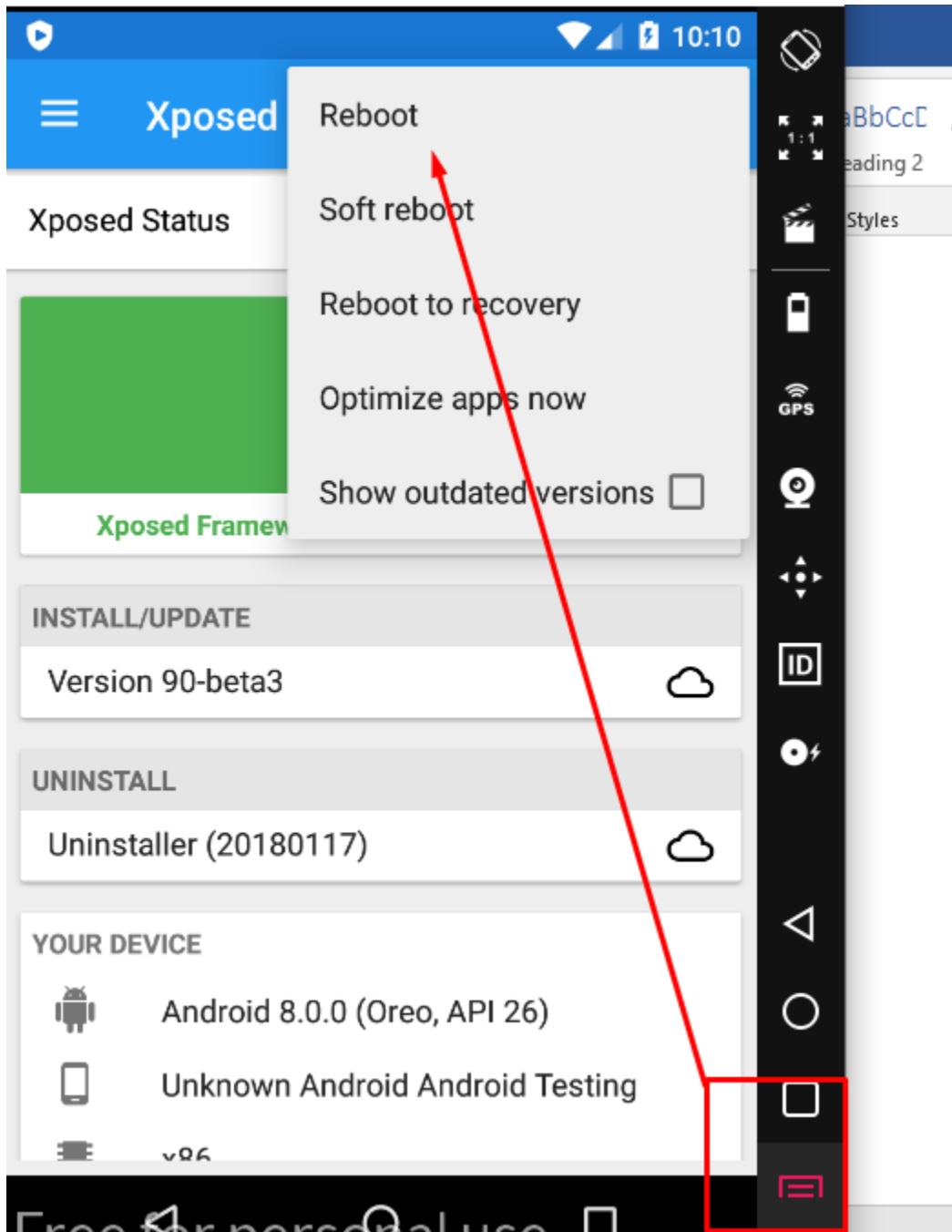
Y ya esta, ahora nos pide que App seleccionar para hacer bypass de ssl pinning pero falta activar el modulo instalado en xposed.

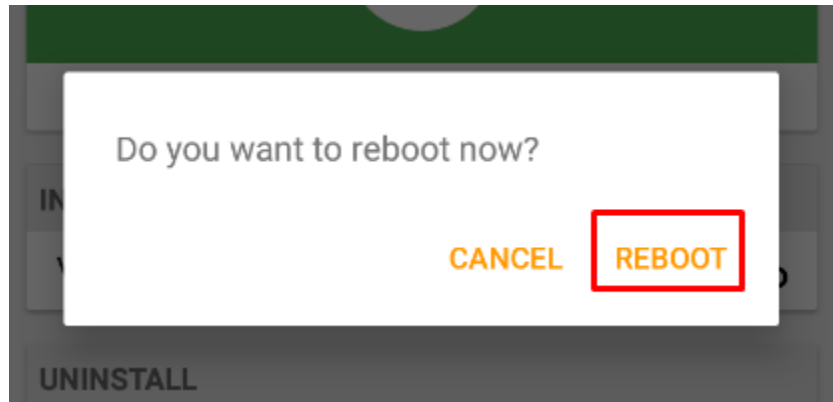
Para activar el modulo nos vamos al xposed app:



Seleccionamos el modulo y luego nos pide reiniciar:



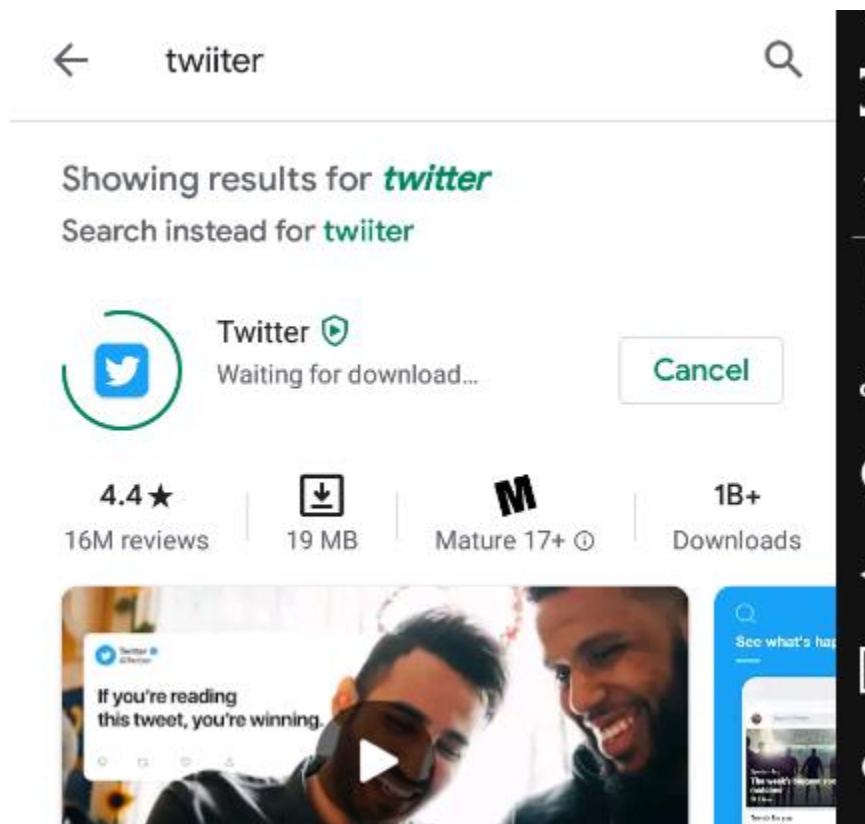




Si se traba cierran el emulador eso equivale a reiniciar:

Abierto el emulador otra vez vamos a instalar una App objetivo a hacerle Bypass SSL Pinning. Para probar voy a instalar twitter. Luego configuraremos el proxy del programa Burp Suite en Android:

(*) Para instalar apps en el emulador, Google play les pedirá una cuenta Gmail. Inicia sesión e instalan el app a probar.



Luego de que se instale configuramos el proxy.

1. Abrimos Burp Suite

⇒ Descarga:



Products ▾ | Solutions ▾ | Research | Academy

Burp Suite Releases

Professional / Community 2020.9.1

04 September 2020 at 14:58 UTC

Burp Suite Community Edition ▾

Windows (64-bit) ▾

Download

shc

⇒

This release fixes a bug that was preventing WebSocket messages from being displayed correctly in the message editor.

<https://portswigger.net/burp/releases/professional-community-2020-9-1?requestededition=community>

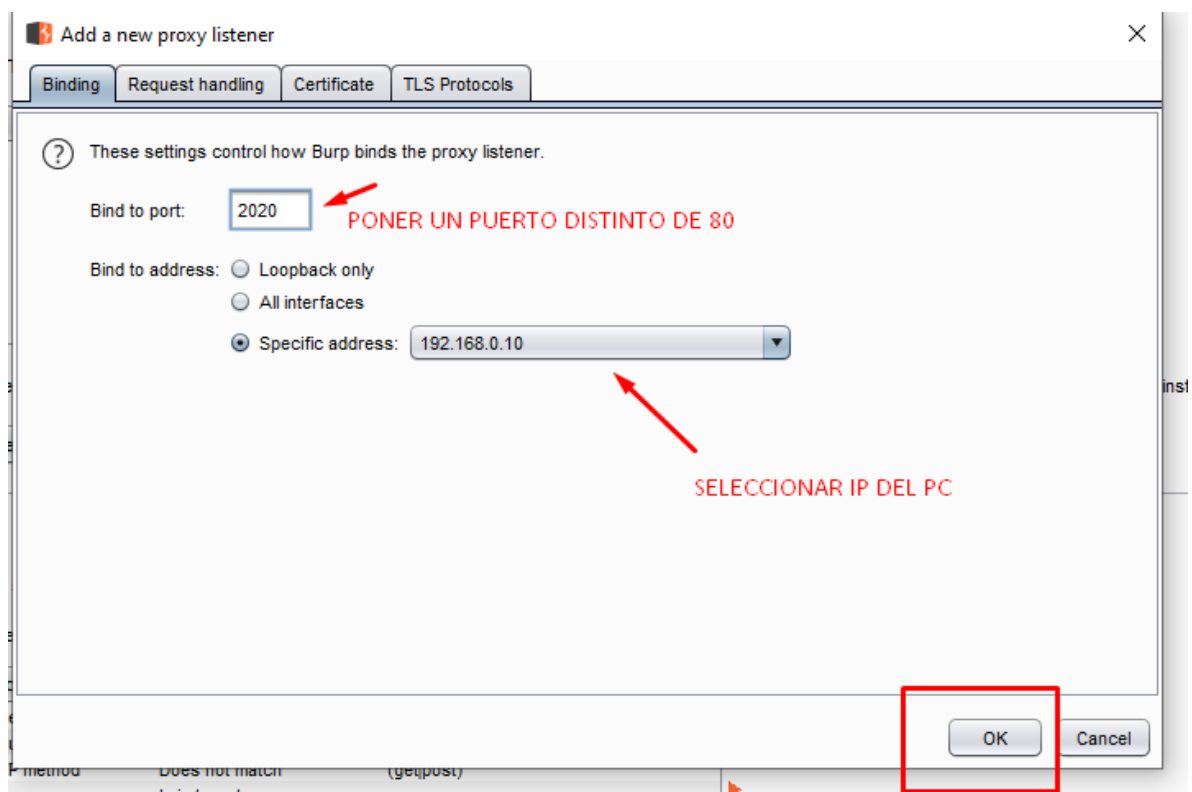
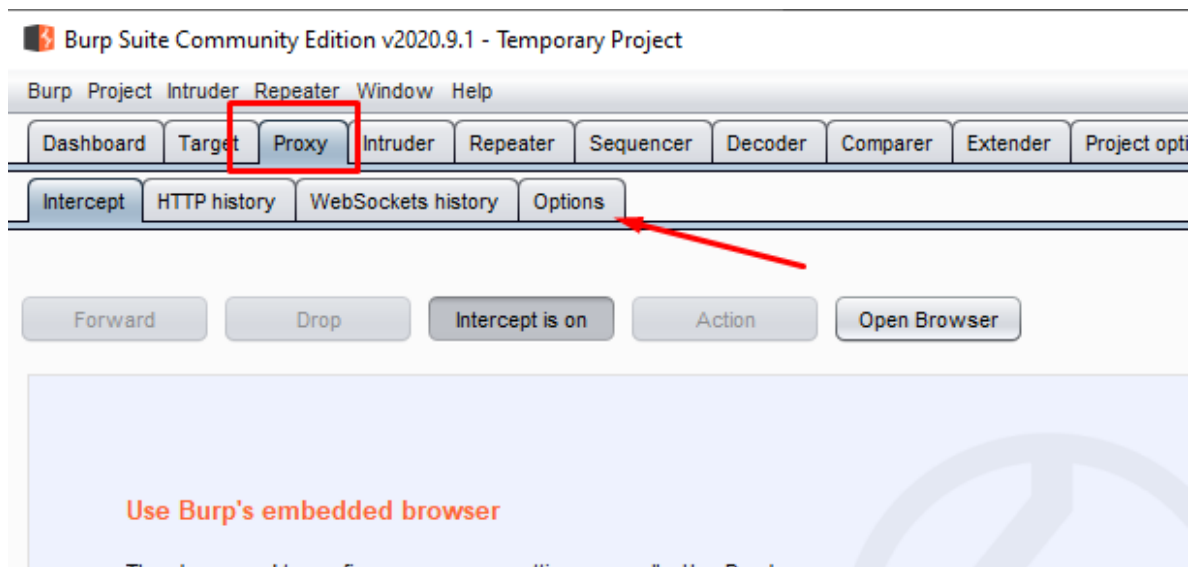
Averiguamos que IP tenemos:

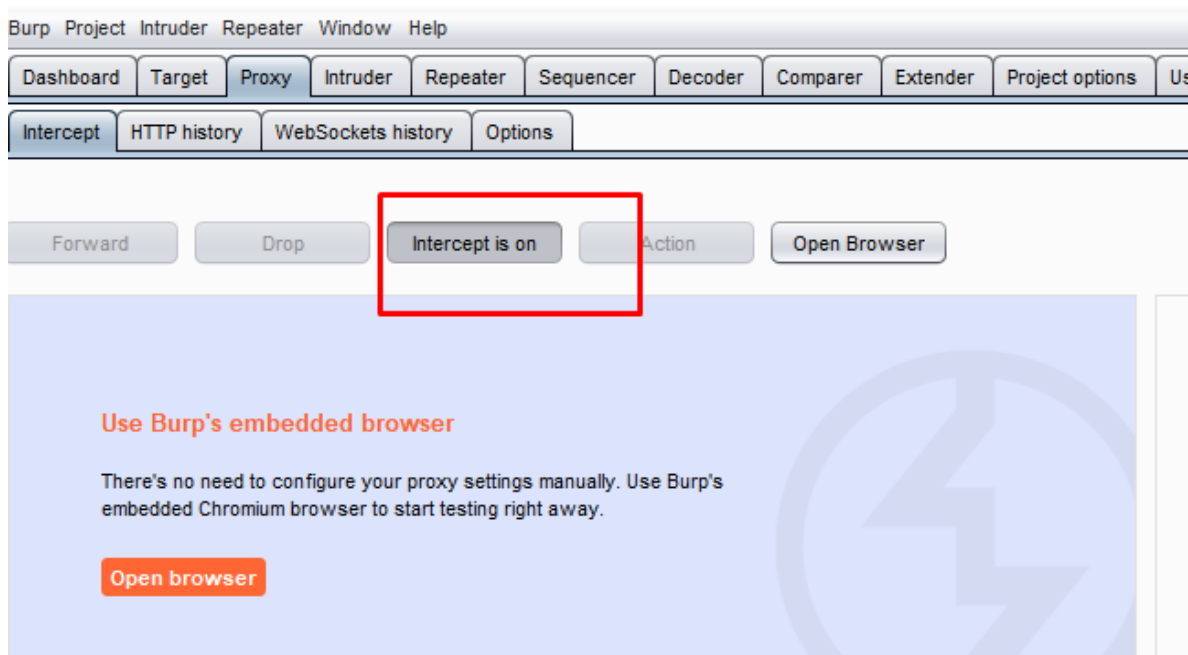
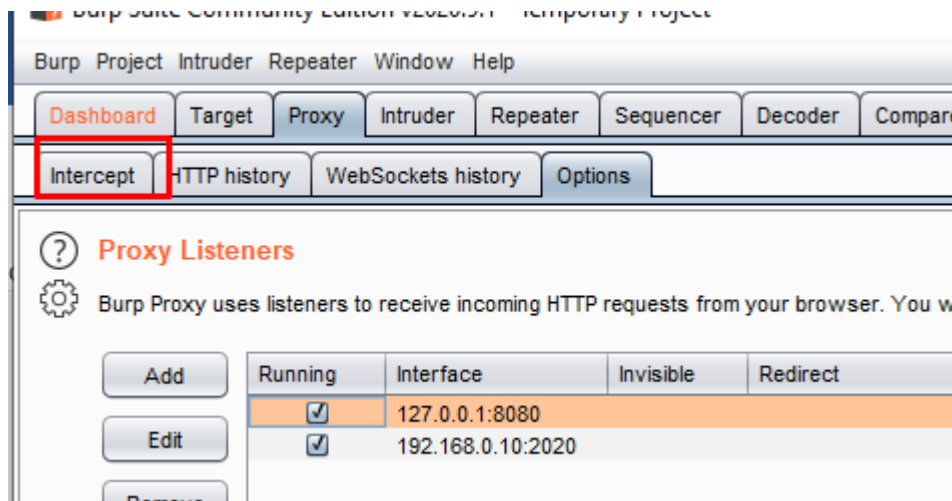
Adaptador de LAN inalámbrica Wi-Fi:

```
Sufijo DNS específico para la conexión. . . :
Dirección IPv6 . . . . . : 2800:200:f100:1ff5:1d0f:cb7e:4354:e701
Dirección IPv6 temporal. . . . . : 2800:200:f100:1ff5:5db2:1408:744d:97aa
Vínculo: dirección IPv6 local. . . : fe80::1d0f:cb7e:4354:e701%13
Dirección IPv4. . . . . : 192.168.0.10
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . : fe80::200:caff:fe11:2233%13
192.168.0.1
```

Adaptador de Ethernet Conexión de red Bluetooth:

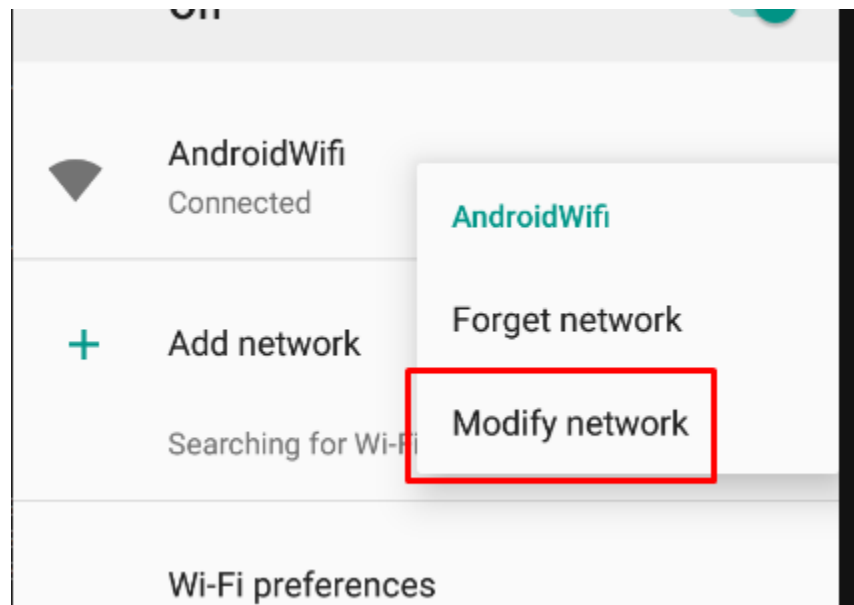
```
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . :
```

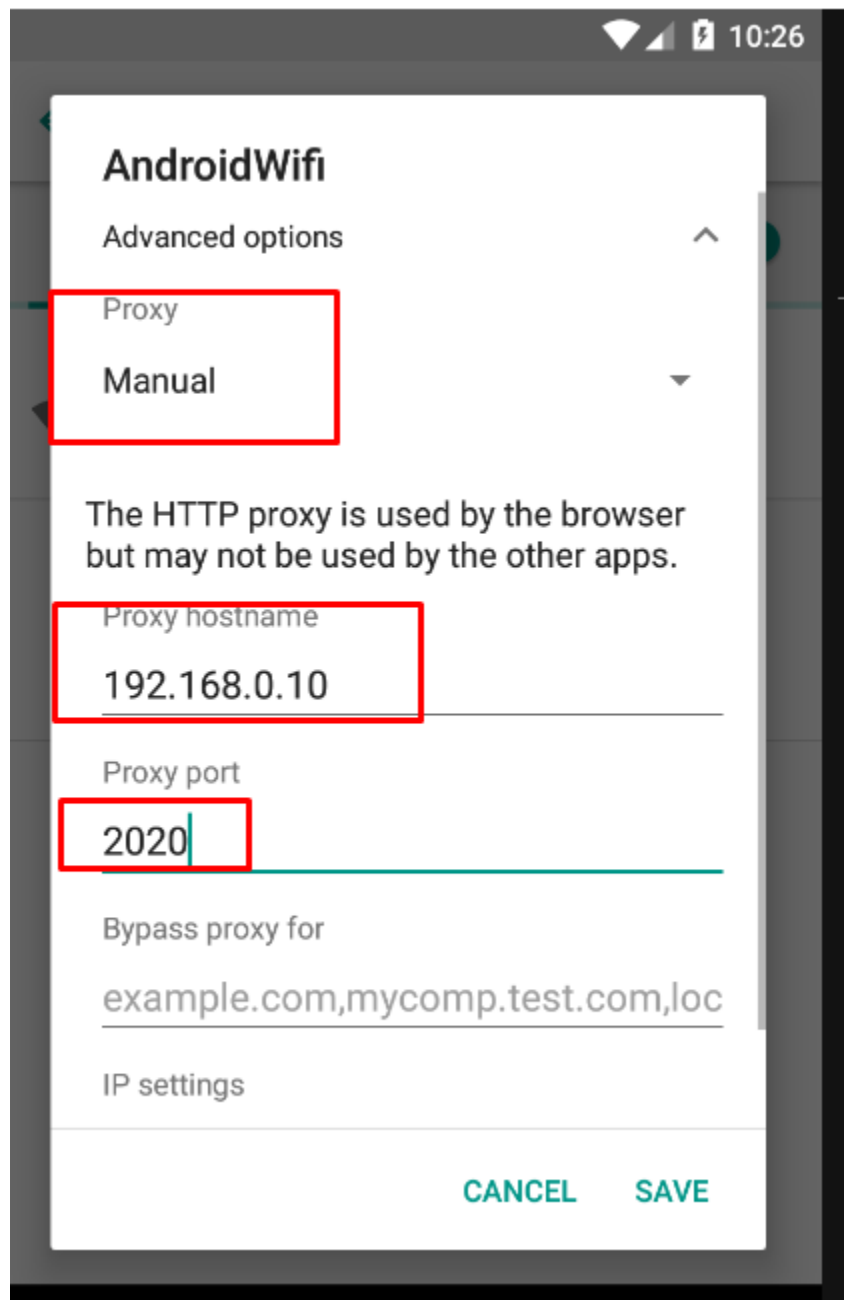




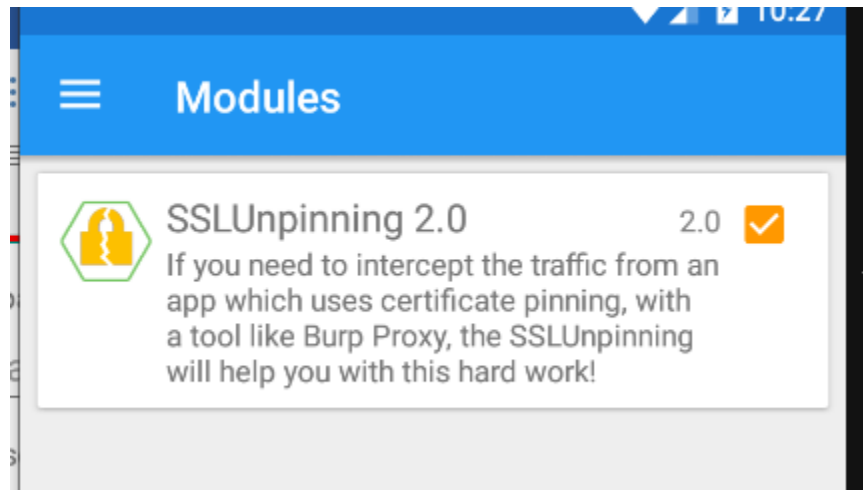
Podemos poner en ON o en OFF el “Intercep”.

Ahora vamos al emulador Android a configurar el PROXY a la red:

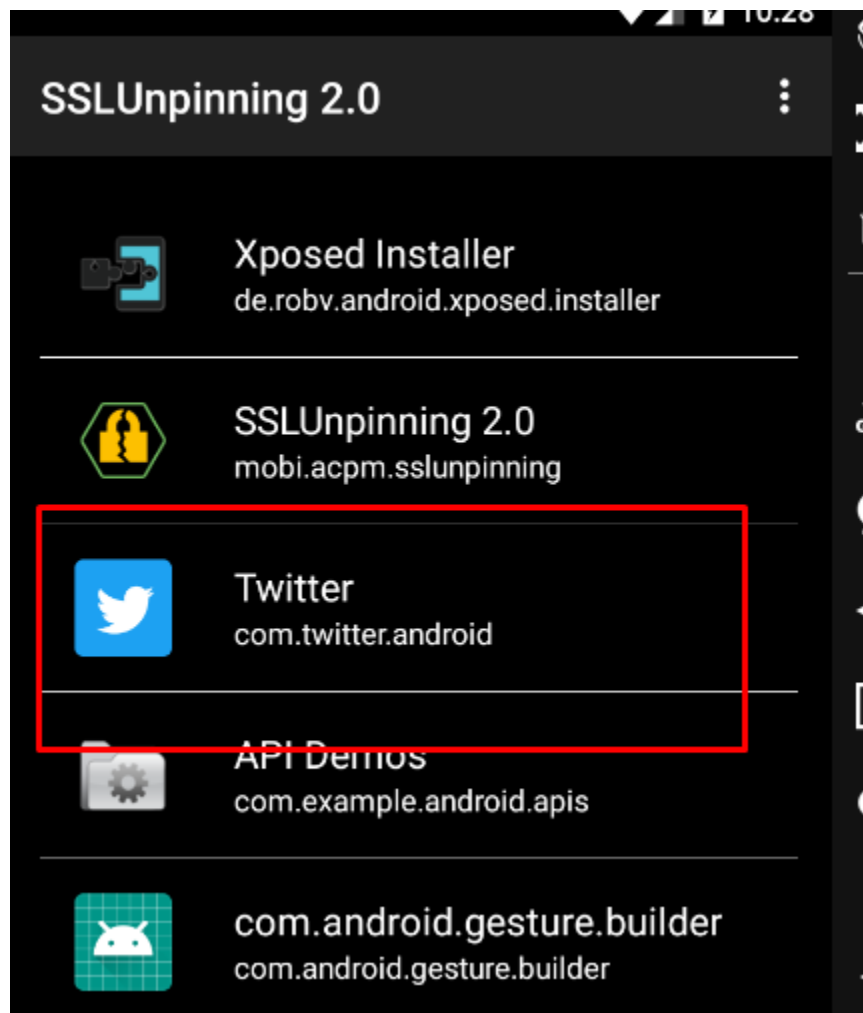


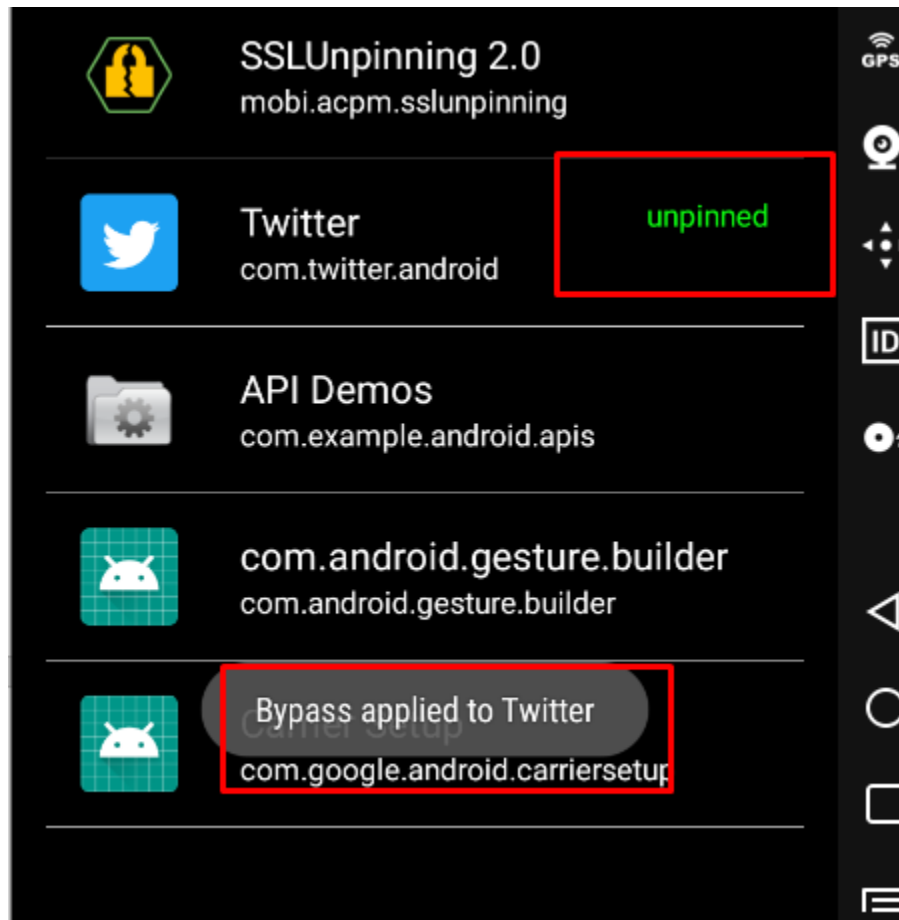


Ahora vamos a xposed app y seleccionamos el modulo instalado SSLUnpinning este nos abrirá una interfaz para seleccionar el App objetivo a hacer bypass SSL Pinning:

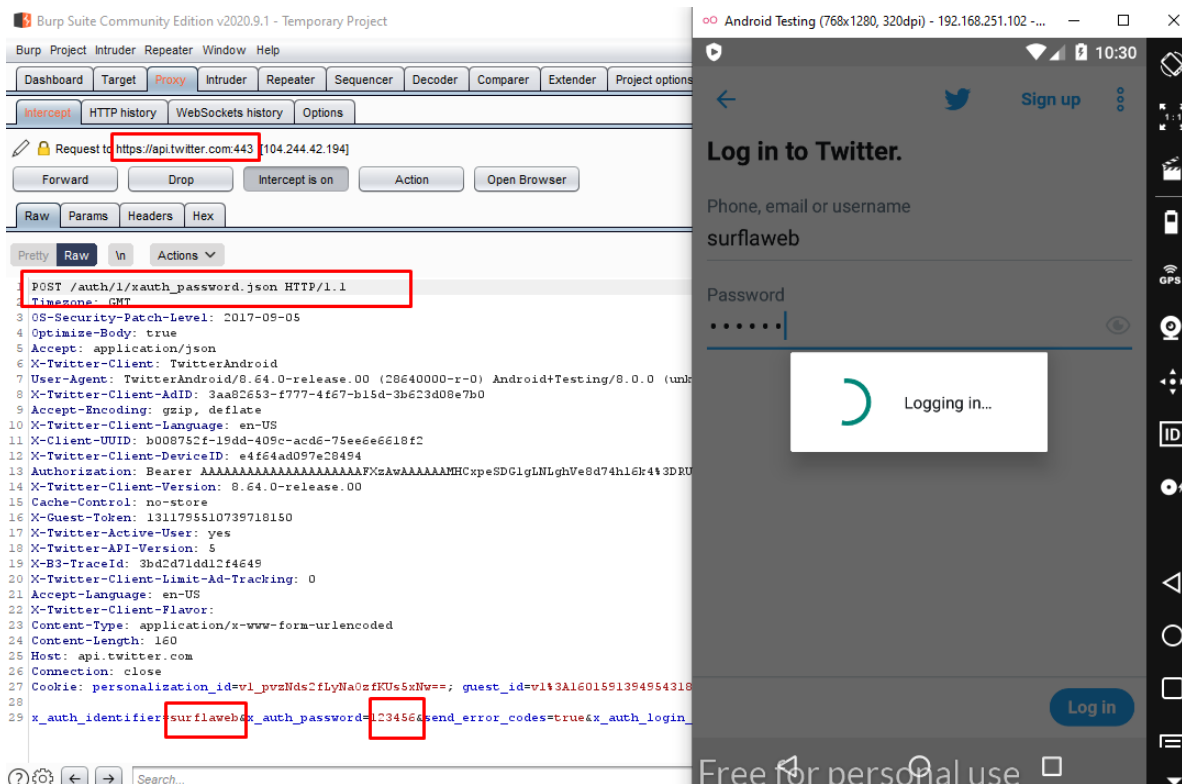


En este caso elijo "twitter"





Ahora abrimos el App y comenzaremos a interceptar desde Burp:



¡Y magia!

(*) No olvidemos presionar en Forward para que las peticiones continúen en el servidor.

Ahora es momento de testear muchas apps, buscar endpoints y testear su seguridad. De esta manera también pueden testear la seguridad de sus aplicaciones.

(*) Este manual es la complementación de este tutorial:

<https://www.youtube.com/watch?v=gMJ28SPWsVO> (Analizar el tráfico de un app android (Detecta endpoints, webservices, urls etc.)

En dicho tutorial solo se analiza el tráfico usando el certificado de Burp Suite pero con ese certificado no se puede hacer bypass a SSL así que con este material se complementa.

(*) Si a la fecha no pueden descargar los archivos vayan a este repositorio en donde podrán descargarse todo el material:

<https://github.com/alcarazolabs/bypassSSLPinnigAndroid>

Saludos.