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

**-= By surflaweb =-**

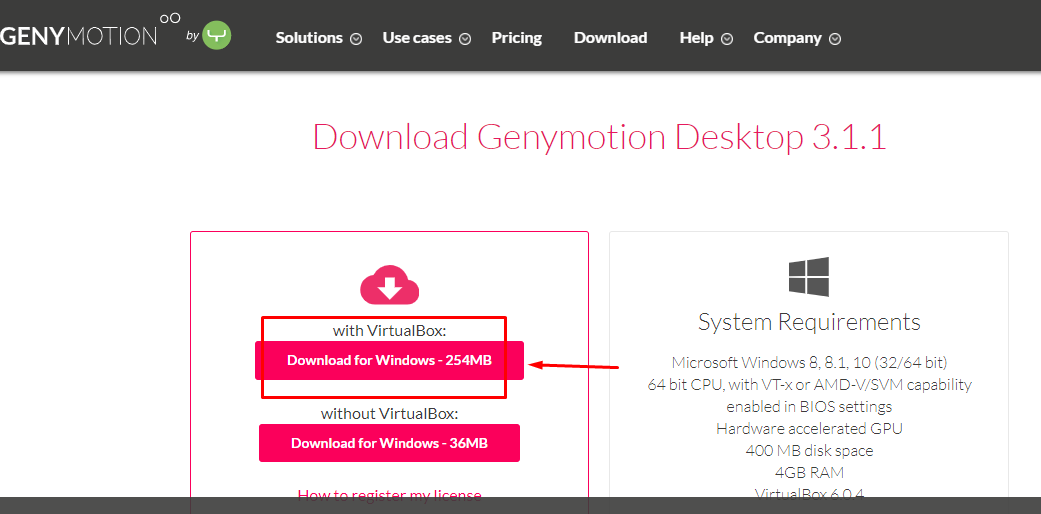
**bypass the certificate verifications for one specific app, then you can intercept all your traffic!**

**Instalar herramientas:**

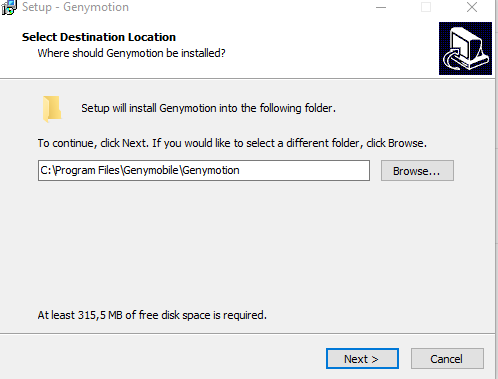
Lo primero es instalar un emulador Android el cual tiene acceso root por defecto.

1. **Descargar genymotion con virtualbox incluido:**

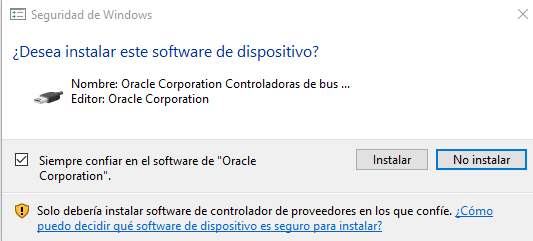
[**https://www.genymotion.com/download/**](https://www.genymotion.com/download/)

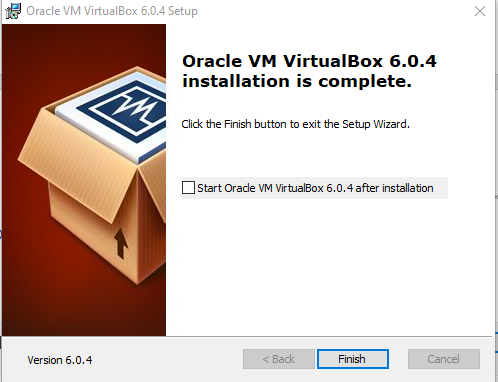


1. **Instalar genymotion.**

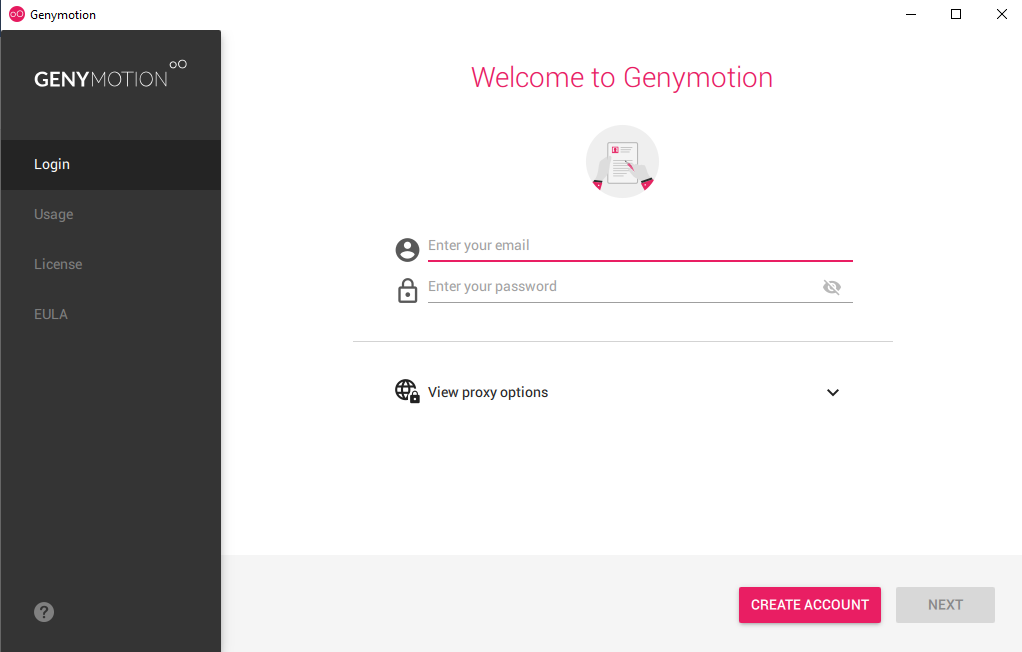




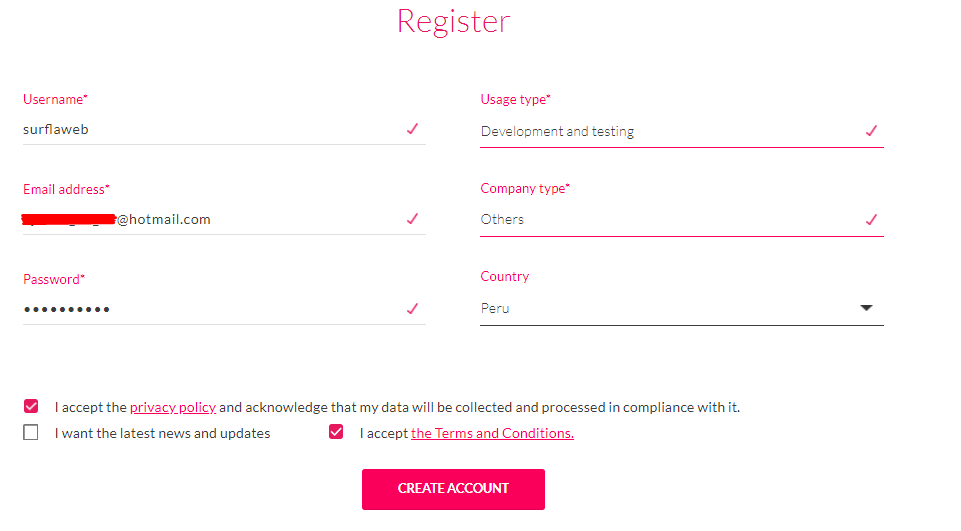




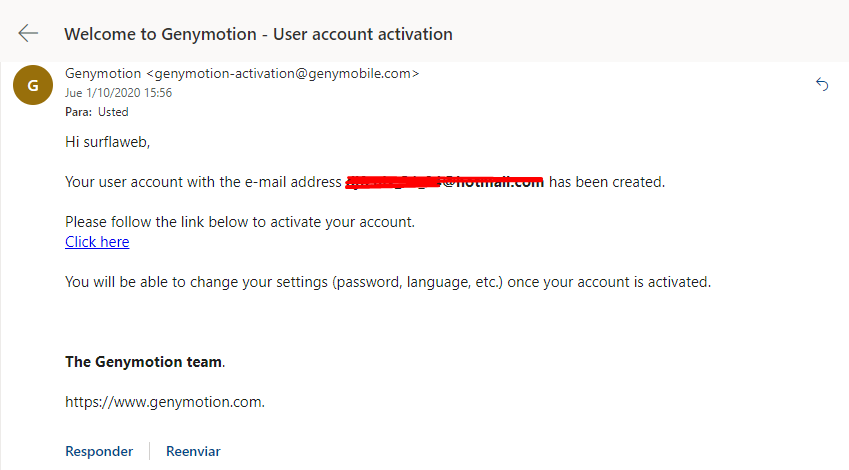
1. **Abrimos genymotion y nos pide que creemos una cuenta:**



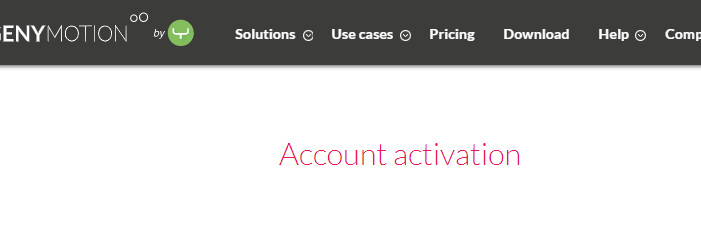
**Nos registramos:**



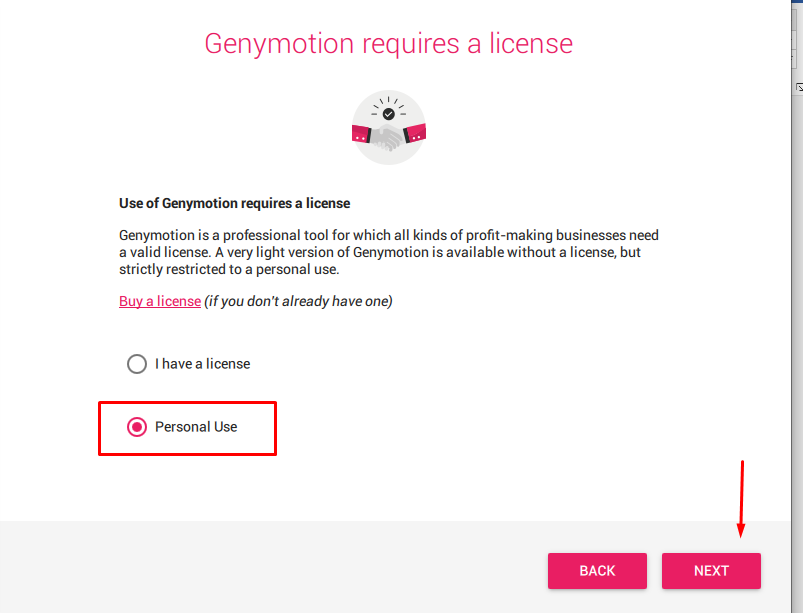
**Luego debemos activar la cuenta nos enviaran un código al correo.**



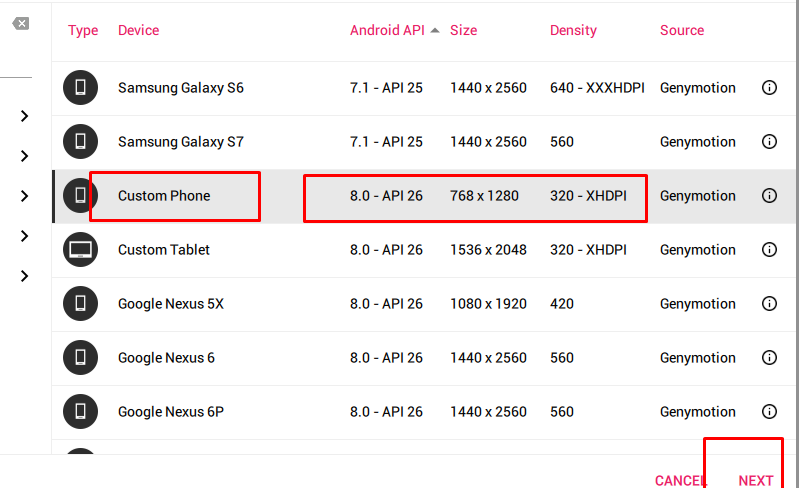
**Hacemos click en el enlace para activar la cuenta.**



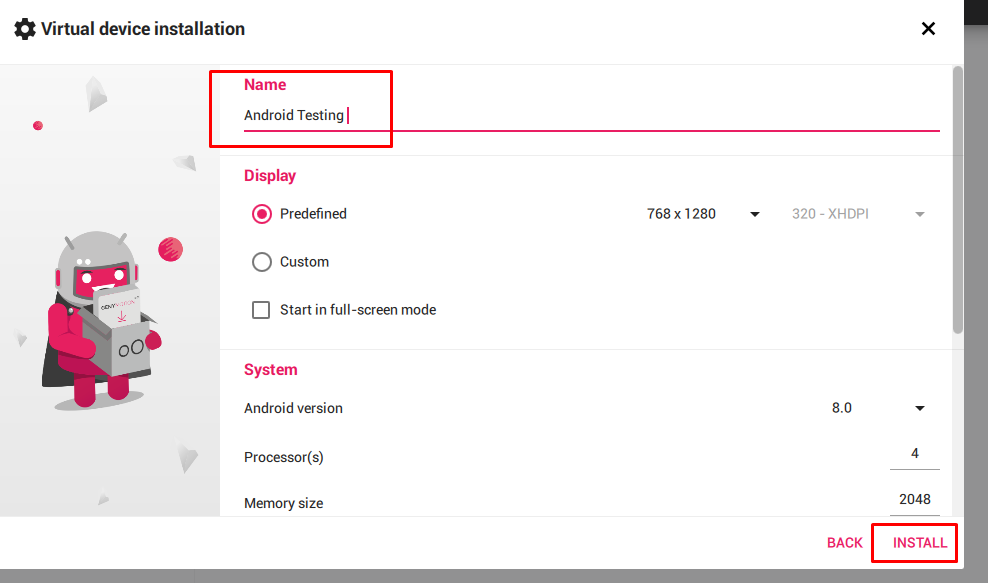
**Lo siguiente es iniciar sesión en el programa genymotion y crear un emulador.**



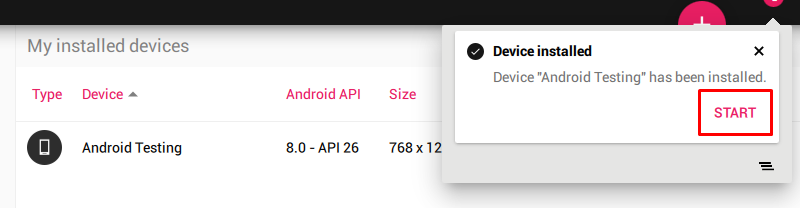
**Creamos un emulador con la versión 8 de Android**

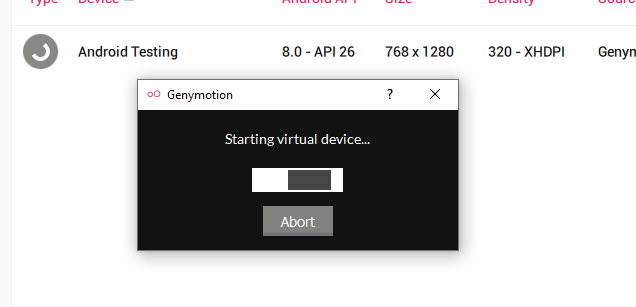


**Le ponemos un nombre al emulador y lo instalamos.**

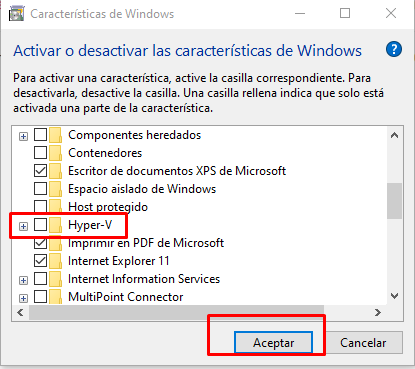


**Una vez creado el emulador lo iniciamos:**



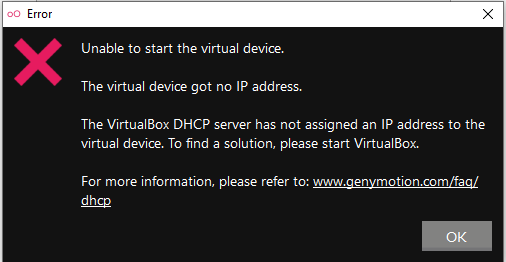


**En caso de iniciarse el emulador desactivar Hyper-v de Windows si lo teníamos activado.**

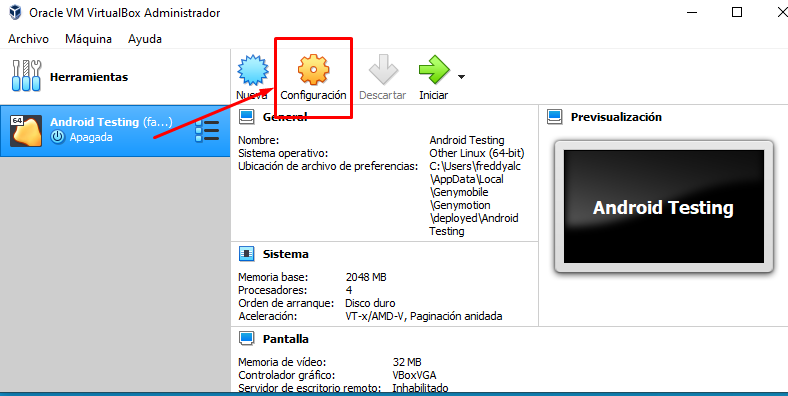


**Luego de desactivar Hyper-v se reiniciar el PC.**

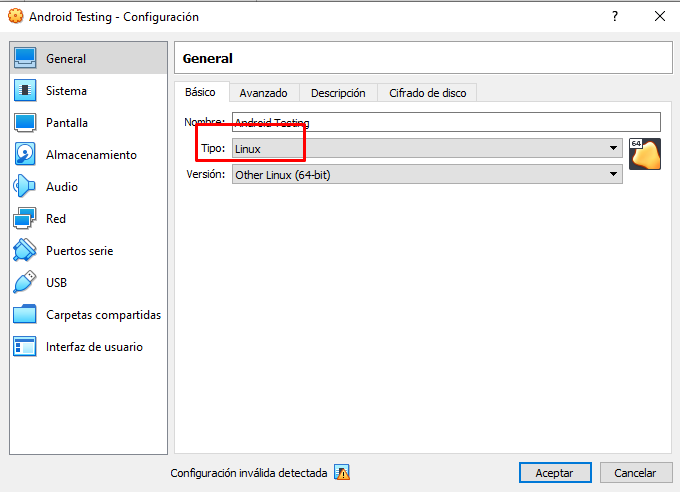
Sin embargo, luego de iniciar el dispositivo sale el error de que no se pudo obtener IP para el dispositivo. Veremos como solucionarlo.

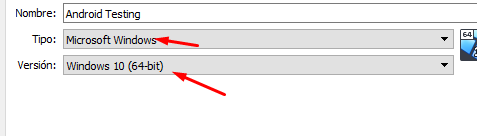


**Abrimos virtualbox y vamos a configuración del dispositivo creado:**

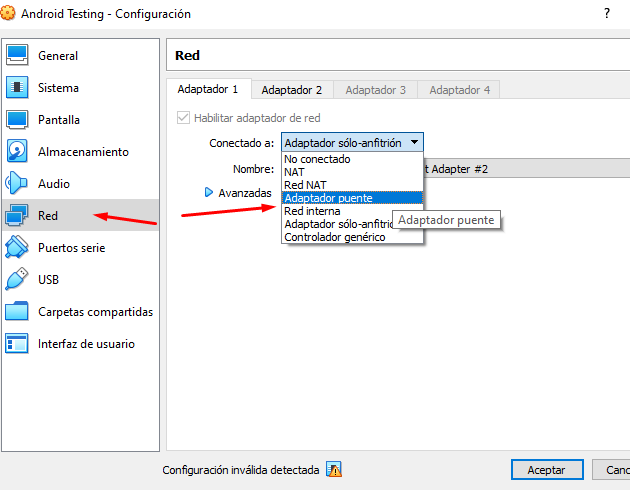


**Vamos a cambiar el tipo de sistema operativo a Windows.**





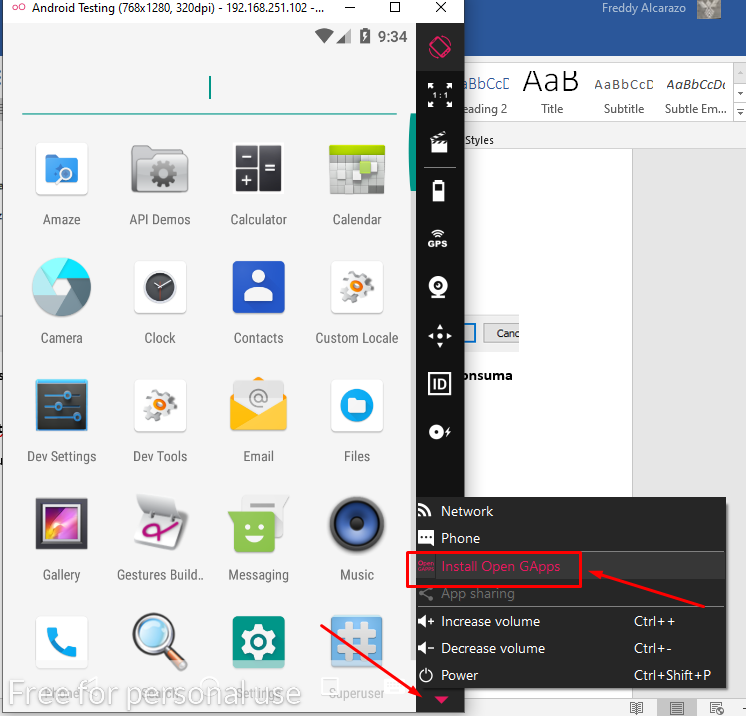
**Luego nos vamos a la opción de “RED” y configuramos la red como “adaptador de puente”:**



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

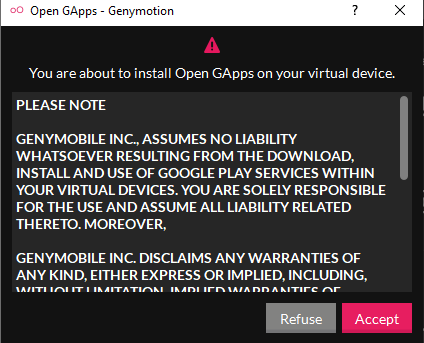
1. **Instalar Google play store en genymotion.**

Con el emulador abierto nos vamos a esta opción:

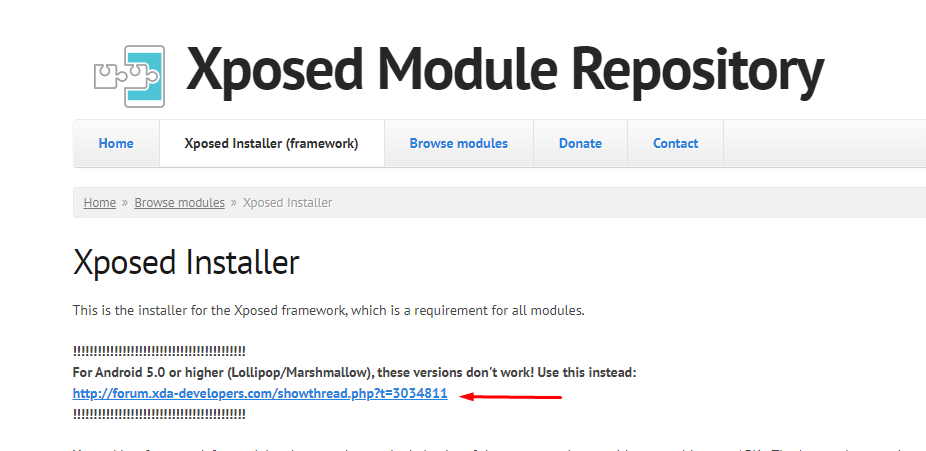


Seleccionamos “Install Open GApps”:

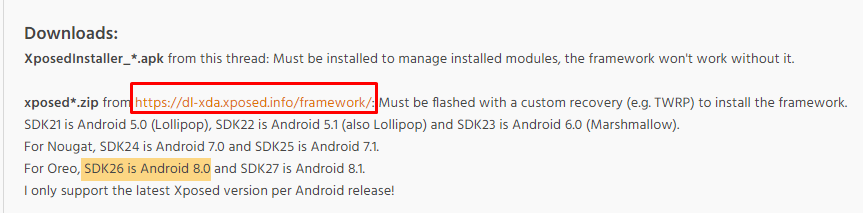
Y aceptamos los términos.



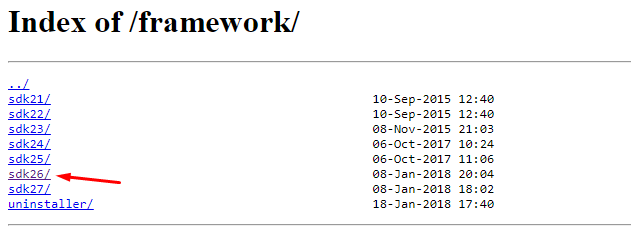
**Lo siguiente será instalar “Xposed-Frame-work” en este le instalaremos un módulo para hacer bypass a SSL Pinning.**



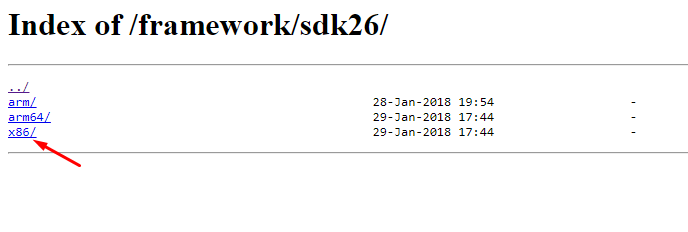
**Hacemos click en el enlacen que nos lleva a un foro ahí luego aremos click en el siguiente enlace para descargar la versión SDK26 de xposed que funciona para Android 8.**

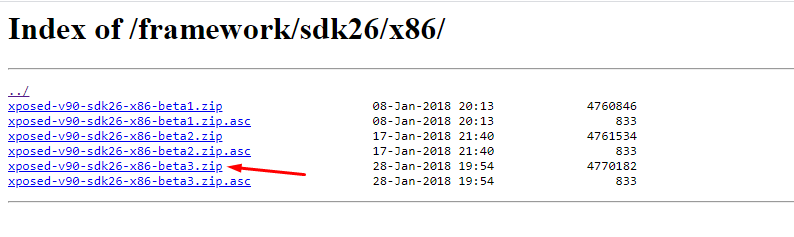


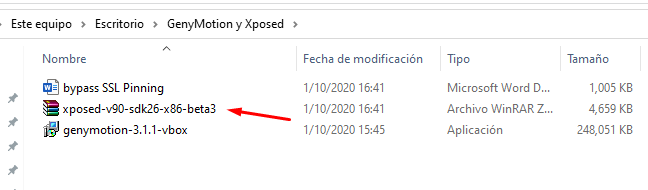
[**https://forum.xda-developers.com/showthread.php?t=3034811**](https://forum.xda-developers.com/showthread.php?t=3034811)



[**https://dl-xda.xposed.info/framework/**](https://dl-xda.xposed.info/framework/)

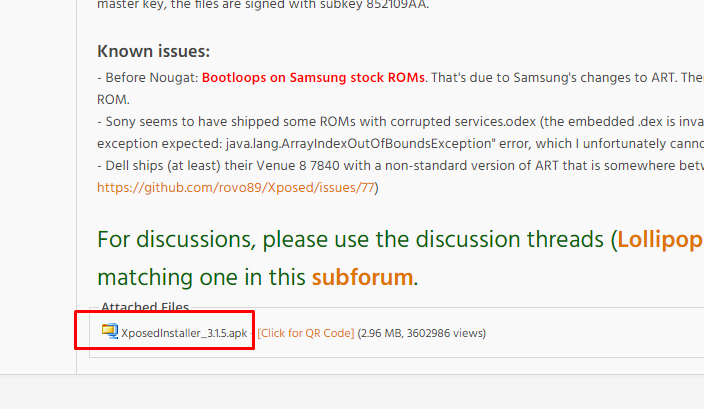






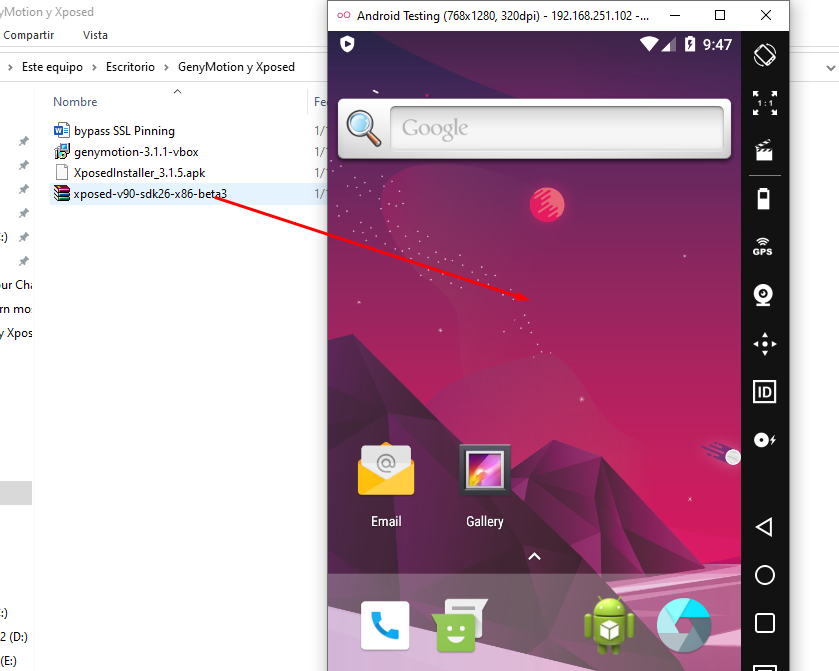
**Volvemos al foro y descargamos el apk:**

[**https://forum.xda-developers.com/showthread.php?t=3034811**](https://forum.xda-developers.com/showthread.php?t=3034811)

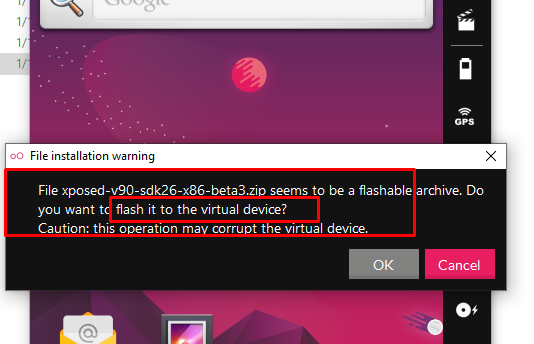


**Descargar el apk de xposed.**

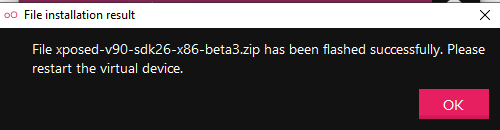
**Ahora vamos a flashear el emulador con los archivo del .zip del framework lo arrastramos al emulador de genymotion:**



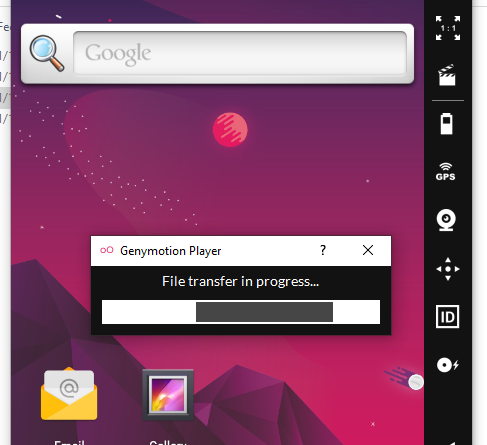
**Presionamos el “ok”**



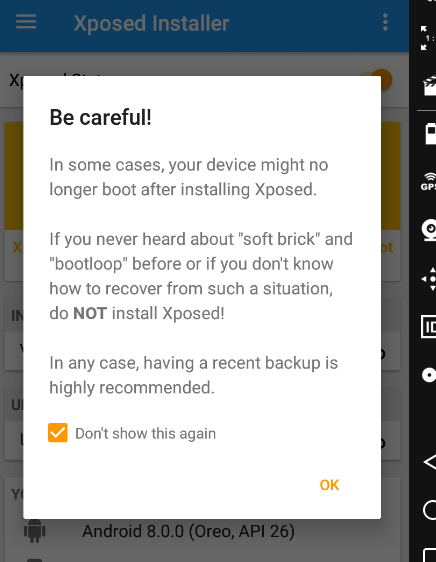
**Resultado exitoso:**



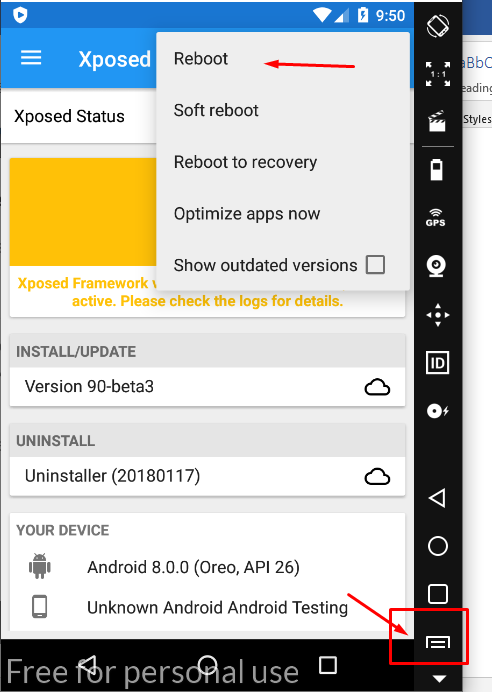
**Ahora arrastramos el apk del framework:**



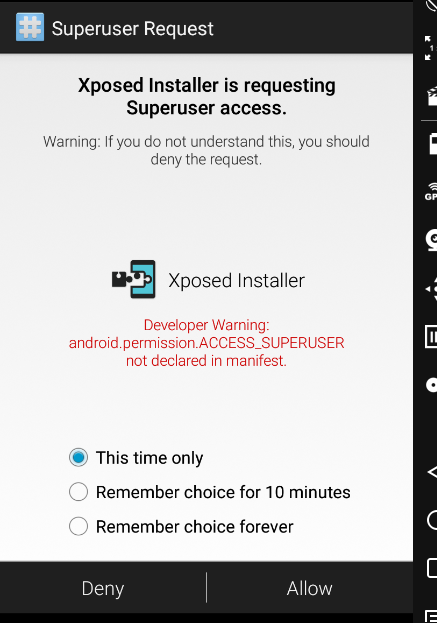
**Y se instala:**



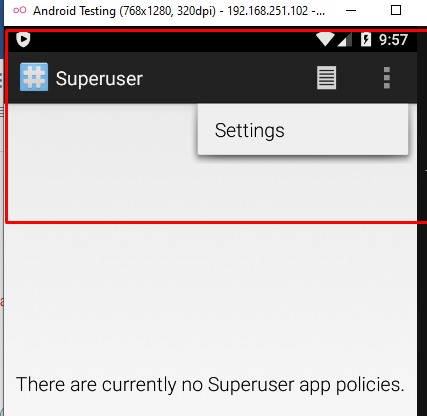
**Reiniciamos:**



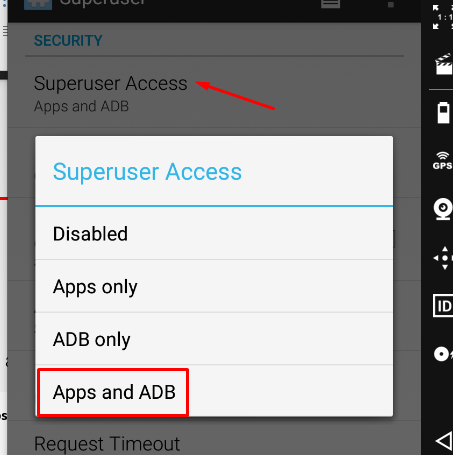
**Nos pide permiso ROO le damos en “Allow”**

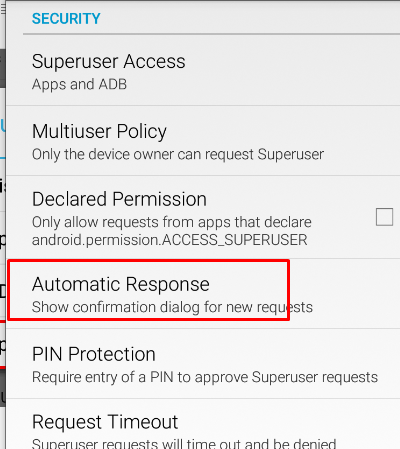


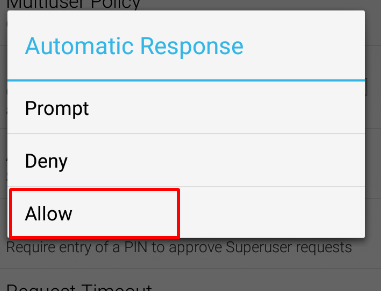
**Si se traba cerramos el emulador y luego lo iniciamos otra vez y esta vez abrimos el “Super User:”**



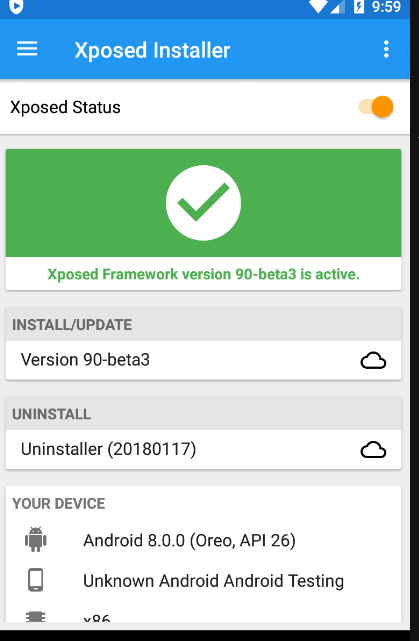
**Nos vamos a “Settings”:**





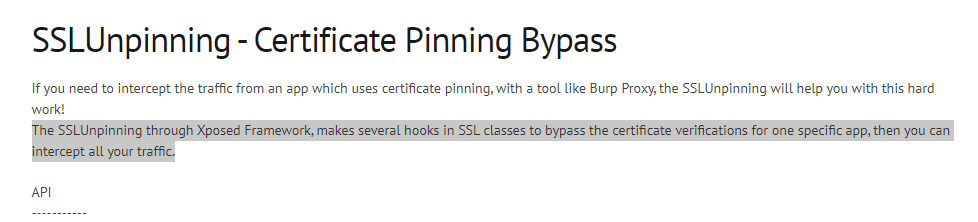


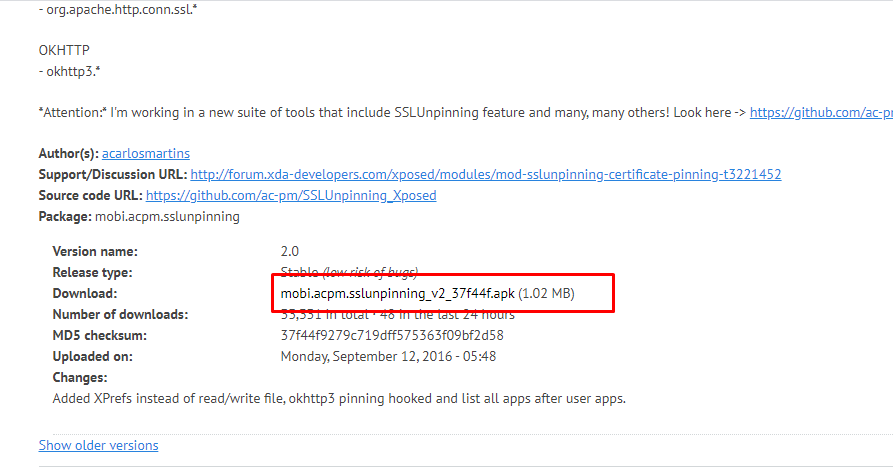
**Ahora al abrir xposed en realidad no lo abri ya estaba abierto si no estaba lo abrimos y ya aparece en verde que quiere decir que esta activado, si les pide reiniciar le dan en reiniciar. A mi se me trabo en el paso anterior por eso cerre el emulador.**



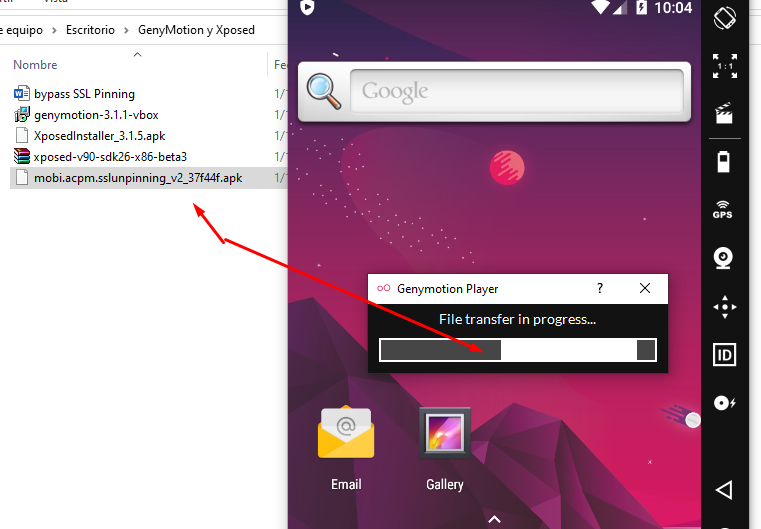
**Ahora descargaremos el Apk de SSLUnpinning:**

* [**https://repo.xposed.info/module/mobi.acpm.sslunpinning**](https://repo.xposed.info/module/mobi.acpm.sslunpinning)



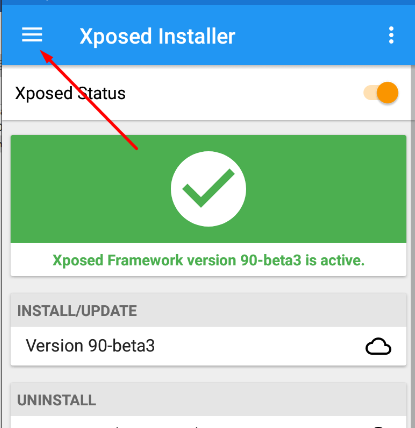


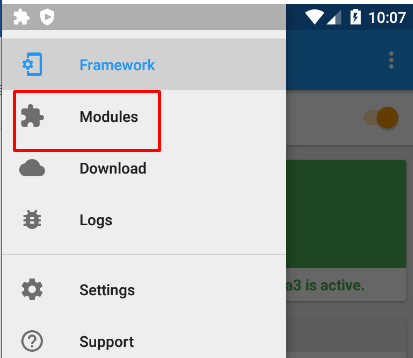
**Ahora instalaremos el APK descargada en el emulador, solamente la arrastramos:**



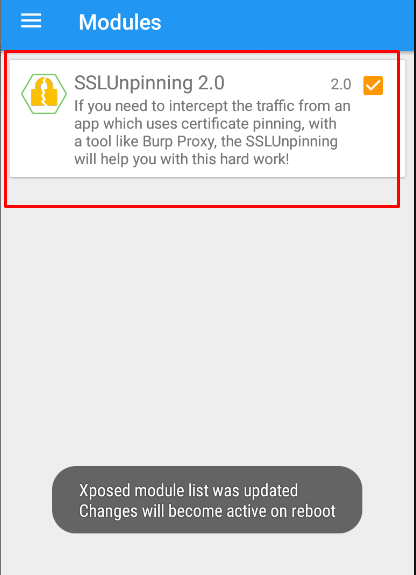
**Y ya esta, ahora nos pide que App seleccionar para hacer bypass de ssl pinning pero falta activar el modulo instalado en xposed.**

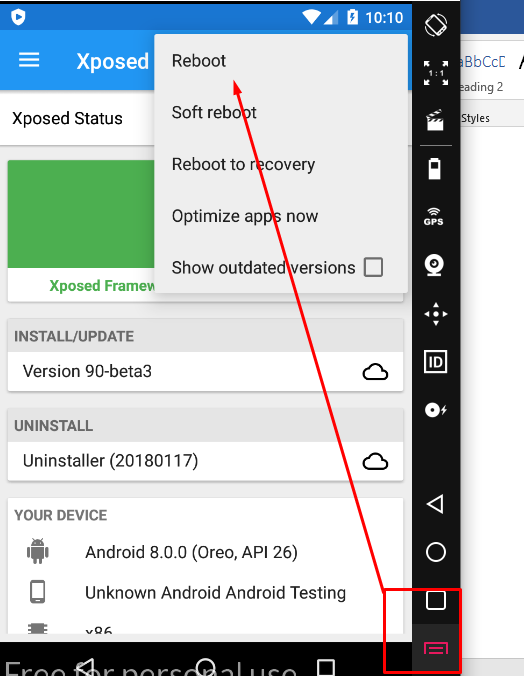
**Para activar el modulo nos vamos al xposed app:**

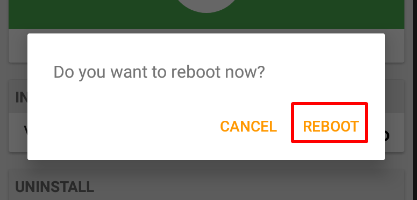




**Seleccionamos el modulo y luego nos pide reiniciar:**



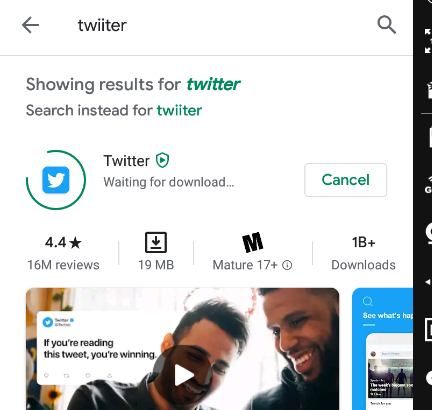




**Si se traba cierran el emulador eso equivale a reiniciar:**

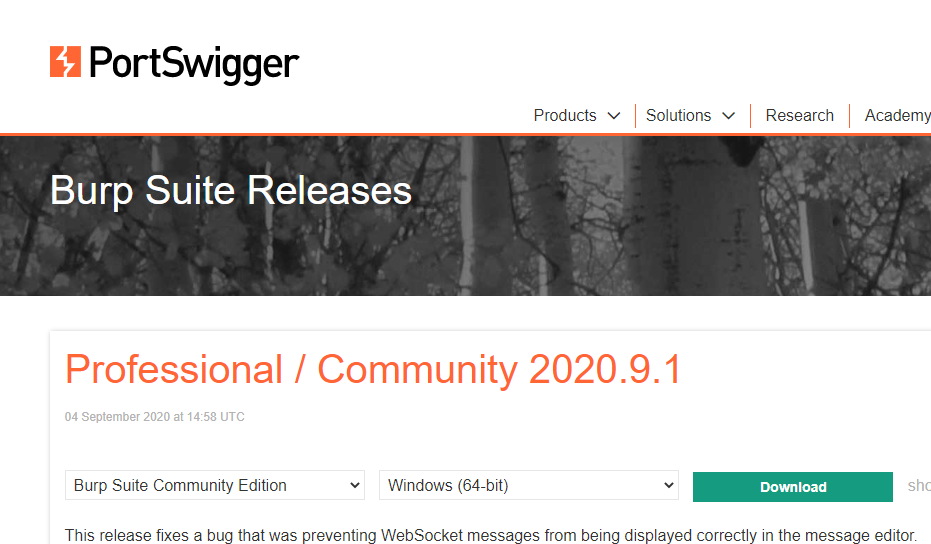
**Abierto el emulador otra vez vamos a instalar una App objetivo a hacerle Bypass SSL Pinning. Para probar voy a instalar twitter. Luego configuraremos el proxy del programa Burp Suite en Android:**

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



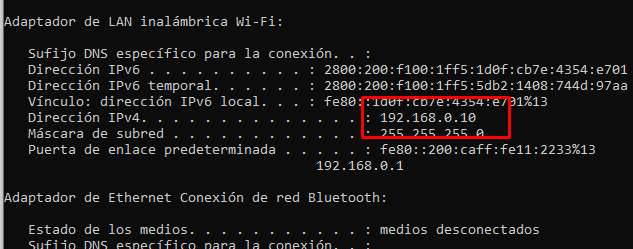
**Luego de que se instale configuramos el proxy.**

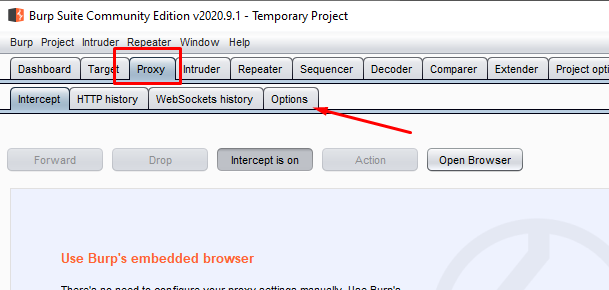
1. **Abrimos Burp Suite**

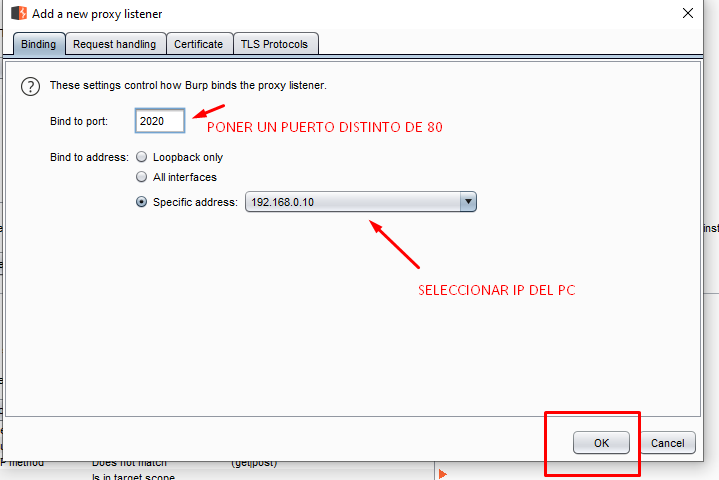
* **Descarga:**
* 

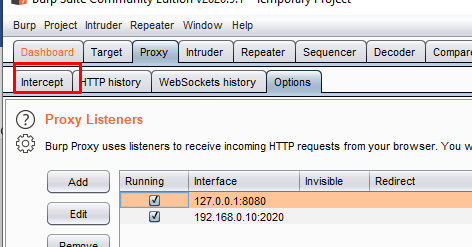
[**https://portswigger.net/burp/releases/professional-community-2020-9-1?requestededition=community**](https://portswigger.net/burp/releases/professional-community-2020-9-1?requestededition=community)

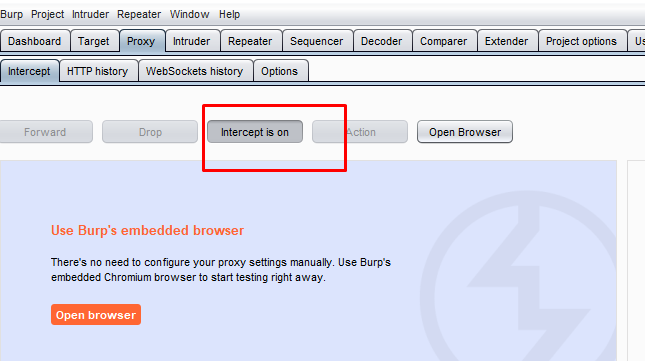
**Averiguamos que IP tenemos:**





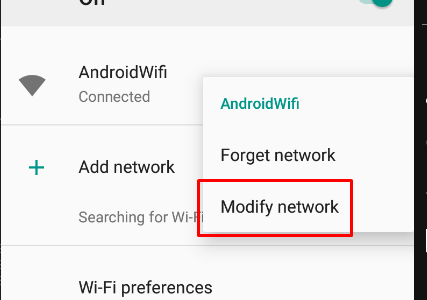


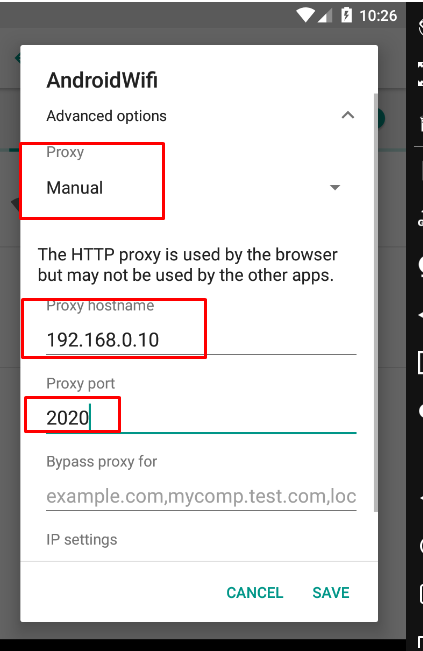




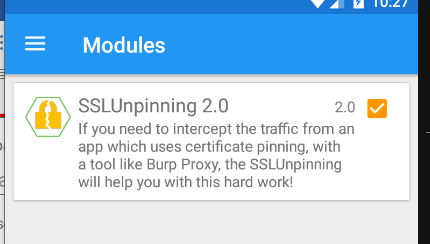
**Podemos poner en ON o en OFF el “Intercep”.**

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

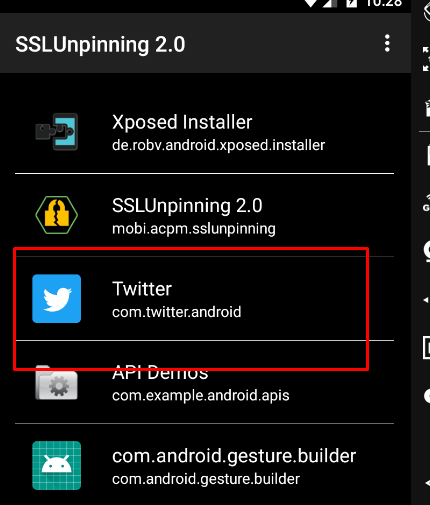


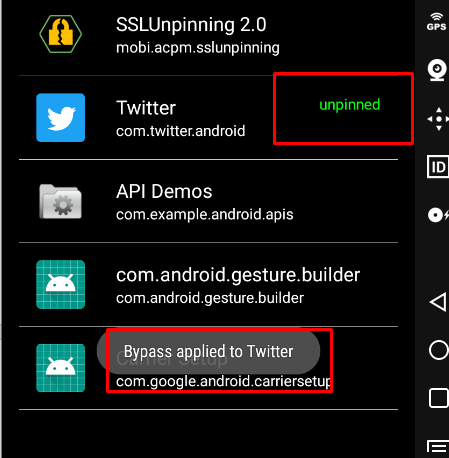


**Ahora vamos a xposed app y seleccionamos el modulo instalado SSLUnpinning este nos abrirá una interfaz para seleccionar el App objetivo a hacer bypass SSL Pinning:**

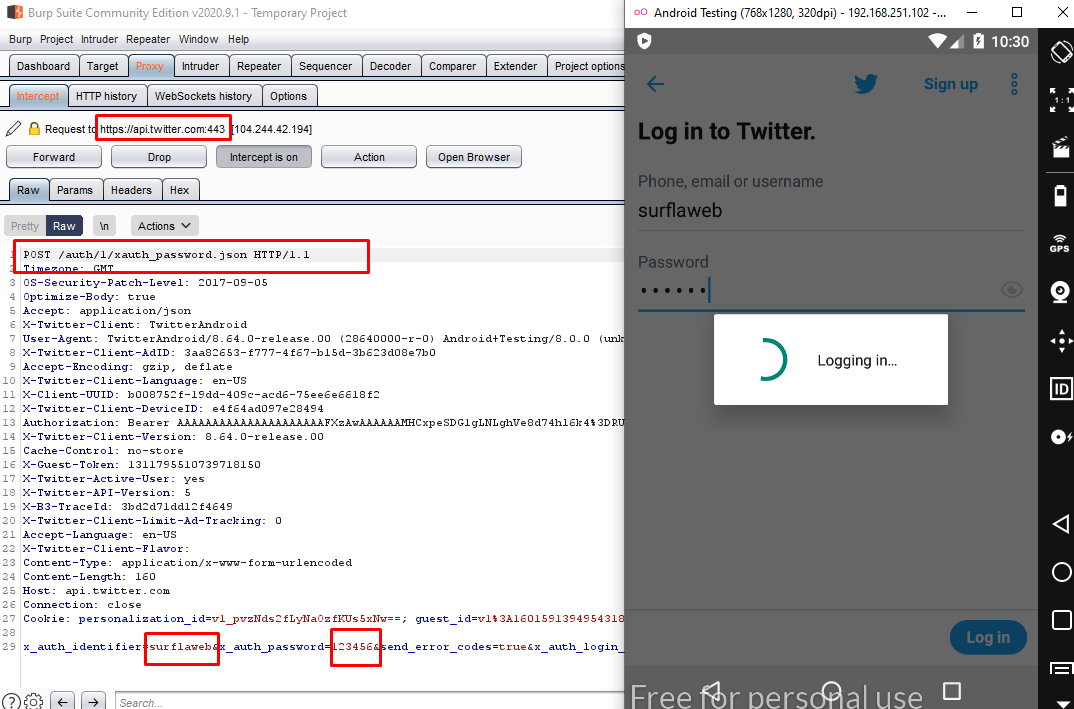


**En este caso elijo “twitter”**





**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=gMJ28SPWsV0**](https://www.youtube.com/watch?v=gMJ28SPWsV0) **(Analizar el trafico de un app android (Detecta endpoints, webservices, urls etc.)**

**En dicho tutorial solo se analiza el trafico usando el certificado de Burp Suite pero con ese certificado no se puede hacer bypass a SSL asi 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**](https://github.com/alcarazolabs/bypassSSLPinnigAndroid)

**Saludos.**