## 安装Frida

pip install frida # 安装Frida

Pip install frida-tools # 安装frida管理工具

在线安装比较慢

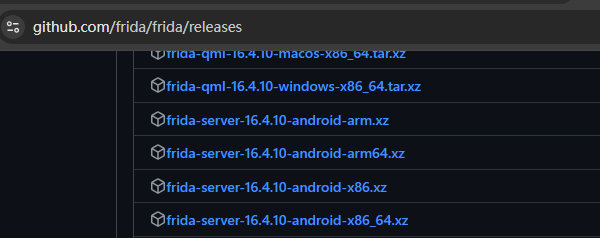
可以去<https://pypi.org/project/frida-tools/#files> 下载在安装

## 安装Frida-Server

确定Android cpu版本:



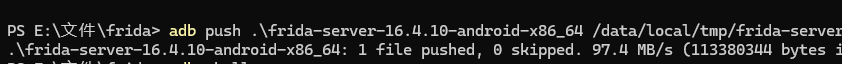
下载对应的Frida-Server



下载的:frida-server-16.4.10-android-x86\_64.xz

解压后推动到虚拟机

adb push .\frida-server-16.4.10-android-x86\_64 /data/local/tmp/frida-server



然后进入虚拟机运行Frida-server:

adb shell

Su # 获取超级权限

cd /data/local/tmp

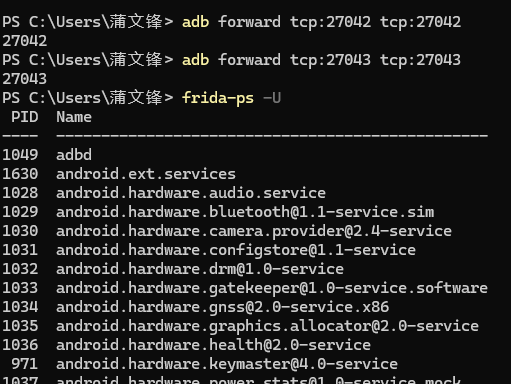
Chmod 777 frida-server

./frida-server # 运行



不要关闭此shell,另开shell

## 运行端口转发监听



adb forward tcp:27042 tcp:27042

adb forward tcp:27043 tcp:27043

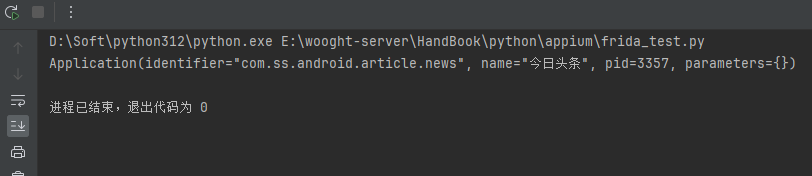
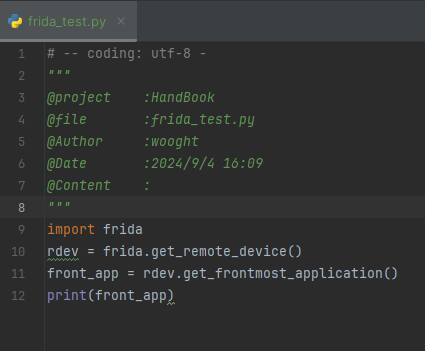
Frida-ps -U # 运行是否输出进程列表

27042端口用于frida-server通信的默认端口号，不转发的话客户端是连接不上服务端

使用默认的端口很容易被检查到,启动Frida-server的时候设置IP和端口

./frida-server -l 127.0.0.1:9999

## Python 运行测试



运行过程中,如果报:frida.TransportError: the connection is closed

则需要kill frida-serve 再重新运行Frida-server

## 淘宝Spdy协议修改

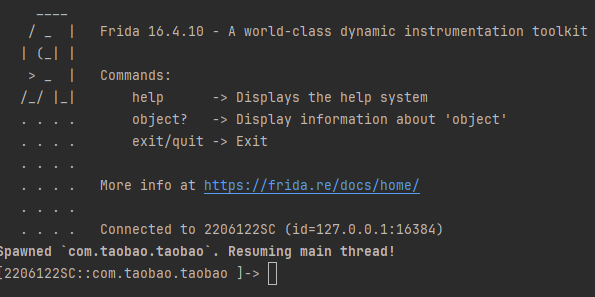
test.js:

Java.perform(function () {  
 var SwitchConfig = Java.use('mtopsdk.mtop.global.SwitchConfig');  
 SwitchConfig.isGlobalSpdySwitchOpen.overload().implementation = function () {  
 return false;  
 }  
});

Frida 执行hook(钩子)操作



运行如下则钩子植入成功:



Charles 抓包成功:

