## 安装

<https://pypi.org/project/frida/#files> 支持环境如列表所示。

不支持Python3.7 环境

Pip install wheel

pip install frida

pip install frida-tools

注意观察frida版本。

查看模拟器架构

adb.exe shell getprop ro.product.cpu.abi

根据cpu架构及版本去下载相应 <https://github.com/frida/frida/releases>

frida-server-15.1.3-android-x86.xz

解压得到 frida-server-15.1.3-android-x86，移动到模拟器目录下

将文件推送到手机目录，放到/data/local/tmp/下，此目录目录权限比较方便

adb push frida-server-15.1.3-android-x86 /data/local/tmp/

进入模拟器

adb shell

切换到root权限

Su

赋予server权限

Cd /data/local/tmp

chmod 777 frida-server-15.1.3-android-x86

## 启动服务

先关闭防火墙

setenforce 0

启动服务

./frida-server-15.1.3-android-x86

如下报错，不影响

{"type":"error","description":"TypeError: r.art::mirror::Object::Clone is not a function","stack":"TypeError: r.art::mirror::Object::Clone is not a function\n at Kt (frida/node\_modules/frida-java-bridge/lib/android.js:1184:1)\n at Gt.replace (frida/node\_modules/frida-java-bridge/lib/android.js:1029:1)\n at Function.set [as implementation] (frida/node\_modules/frida-java-bridge/lib/class-factory.js:1010:1)\n at Function.set [as implementation] (frida/node\_modules/frida-java-bridge/lib/class-factory.js:925:1)\n at installLaunchTimeoutRemovalInstrumentation (/internal-agent.js:424:24)\n at init (/internal-agent.js:51:3)\n at c.perform (frida/node\_modules/frida-java-bridge/lib/vm.js:11:1)\n at g.\_performPendingVmOps (frida/node\_modules/frida-java-bridge/index.js:238:1)\n at frida/node\_modules/frida-java-bridge/index.js:213:1\n at c.perform (frida/node\_modules/frida-java-bridge/lib/vm.js:11:1)","fileName":"frida/node\_modules/frida-java-bridge/lib/android.js","lineNumber":1184,"columnNumber":1}

开启端口转发

adb forward tcp:27042 tcp:27042

查看模拟器进程

frida-ps -U

## 开始调试

先进入目标包看能否连接

frida -U com.baidu.ipc

Exit 推出

## 开始抓包

参考文章

<https://bbs.pediy.com/thread-222427.htm>

脚本地址

<https://github.com/scopion/frida-ssl-pinning>

注意文章中 cf = CertificateFactory.getInstance("X.509");

少了var声明，脚本中已修复。

导入证书

adb push cert.crt /data/local/tmp/cert.crt

开始抓包

frida -U -f com.baidu.ai -l .\frida-android-repinning\_sa1.js --no-pause