APP 抓包心得

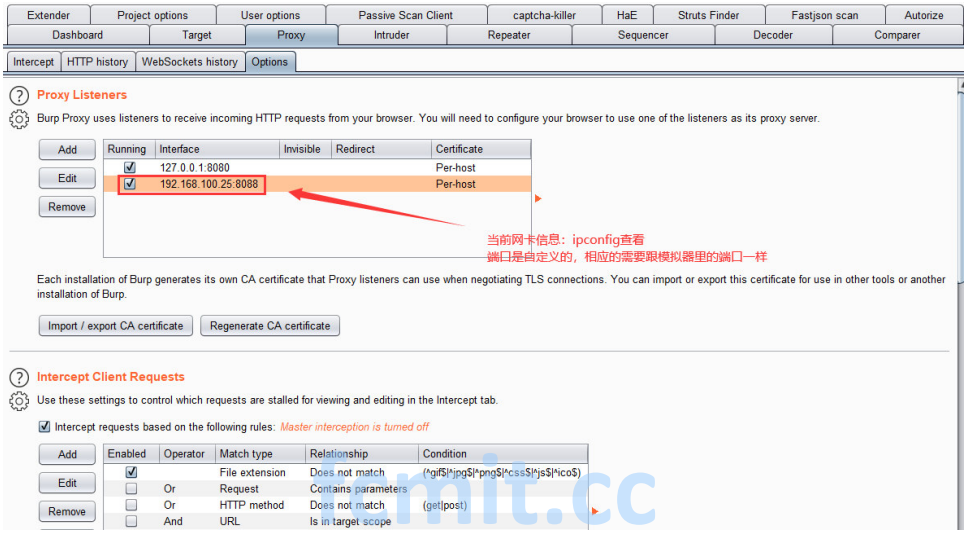
方法一：使用模拟器，个人推荐夜神模拟器或者是网易的 MuMu 模拟器

场景：需要抓取 HTTPS 的数据包

1、使用模拟器：夜神模拟器

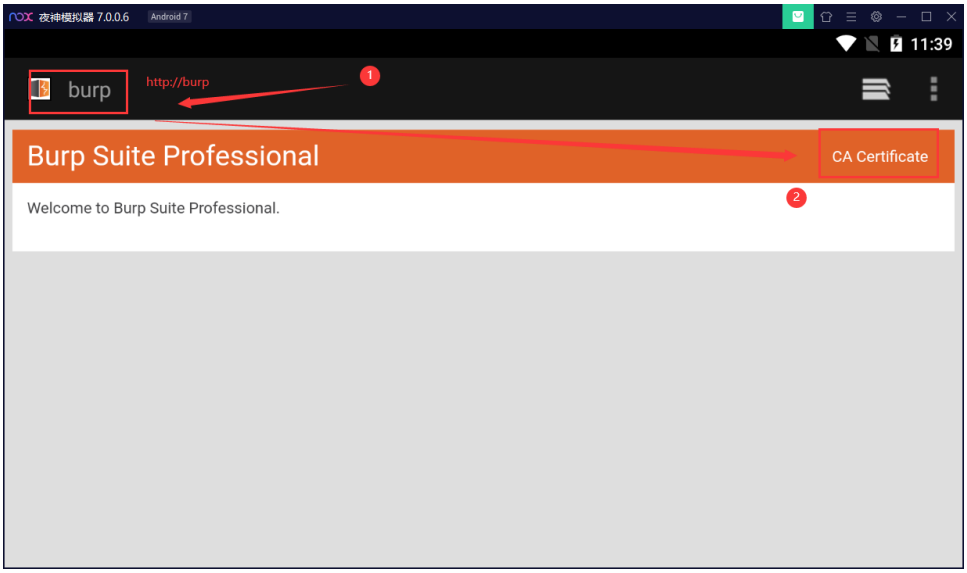
第二步是最关键的一步，不管是 Android 系统还是 IOS 系统，抓 APP 数据包都比不可少

2、安装 burp 证书，burp 设置好代理



- 来到模拟器—>设置—>WALN—修改网络—>手动，如下图：主机名和端口与 burp 一致

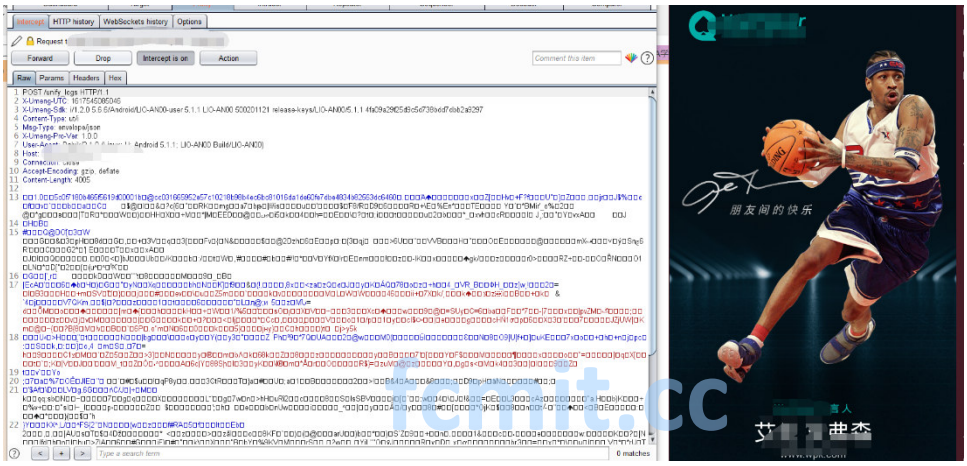
- 设置完成之后，需要导入 burp 证书，访问 http://burp，下载证书。



- 下载完成后把证书改名：crt 格式（**ps：模拟器或手机支持的格式**）
- 导入到模拟器中
- 设置->安全->SD 卡安装证书，找到对应的证书

- 安装下一步，任意命名即可。

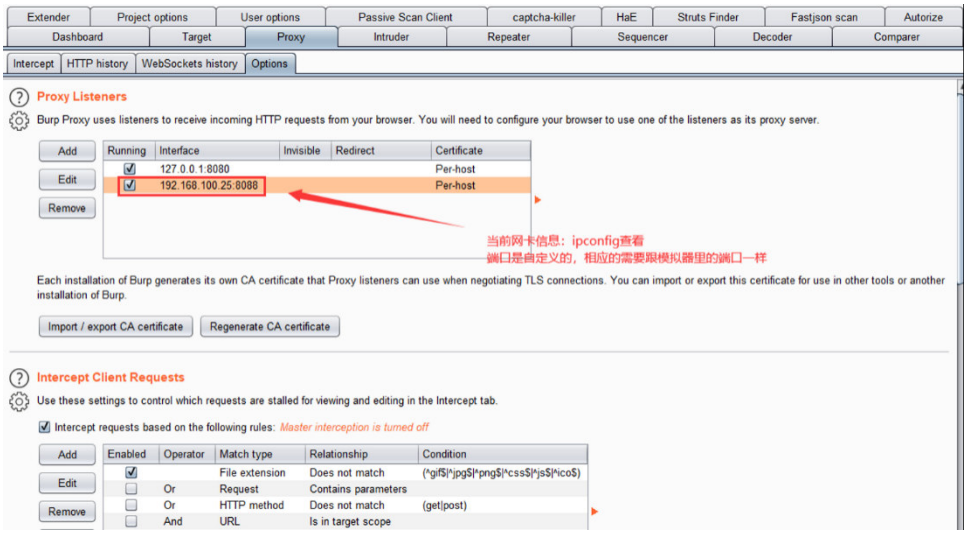
3、burp 抓包成功，如下图



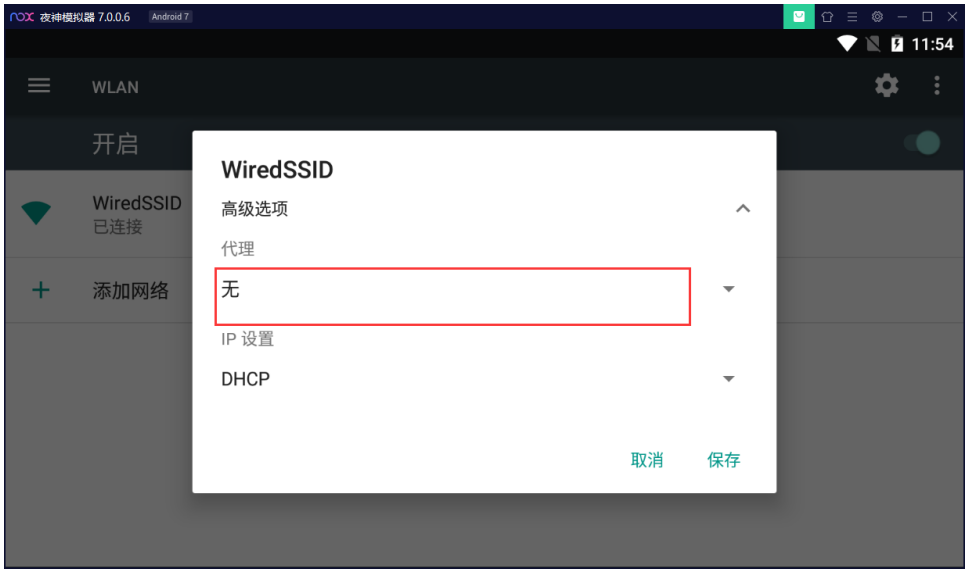
方法二（在安装有证书的前提下没有安装证书的回头看方法一）：Proxifier+burp

场景：APP 识别到模拟器开有代理，导致数据包错误或者 hi 不能正常打开访问 APP，这种情况我们可以利用以代理的方式，达到绕过的效果。

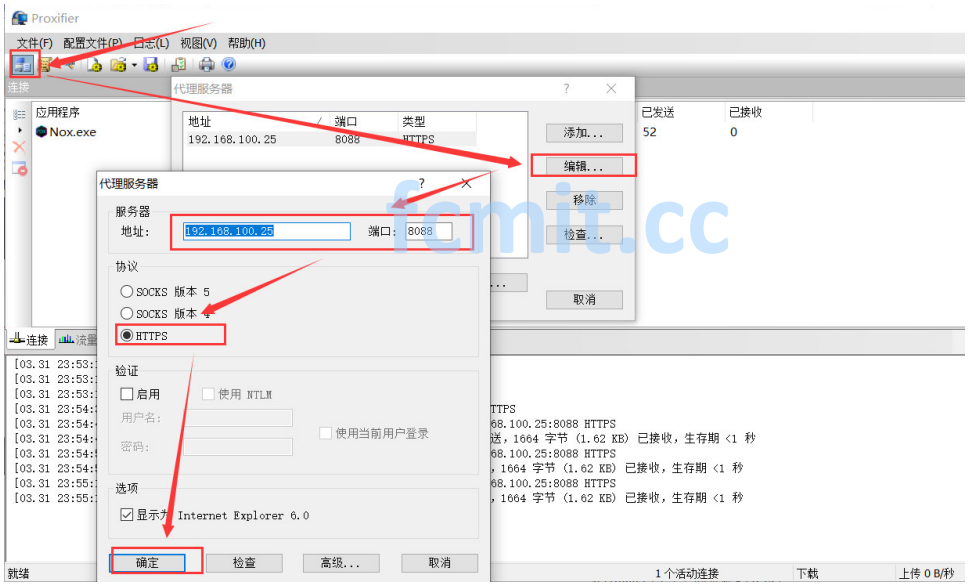
1、burp 设置好代理



2、关闭模拟器的代理，**不需要开启代理！**



3、下载 Proxifier 并打开修改完成，如下图：IP 与端口需要对应 BURP 设置的 IP 和端口

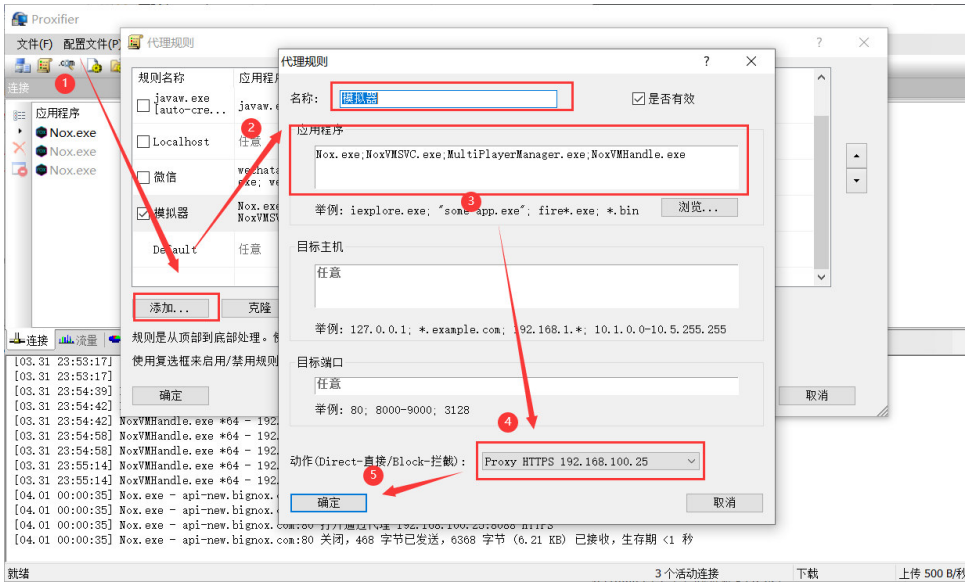


4、点击配置文件—>代理规则—>设置代理规则—>添加一条代理规则

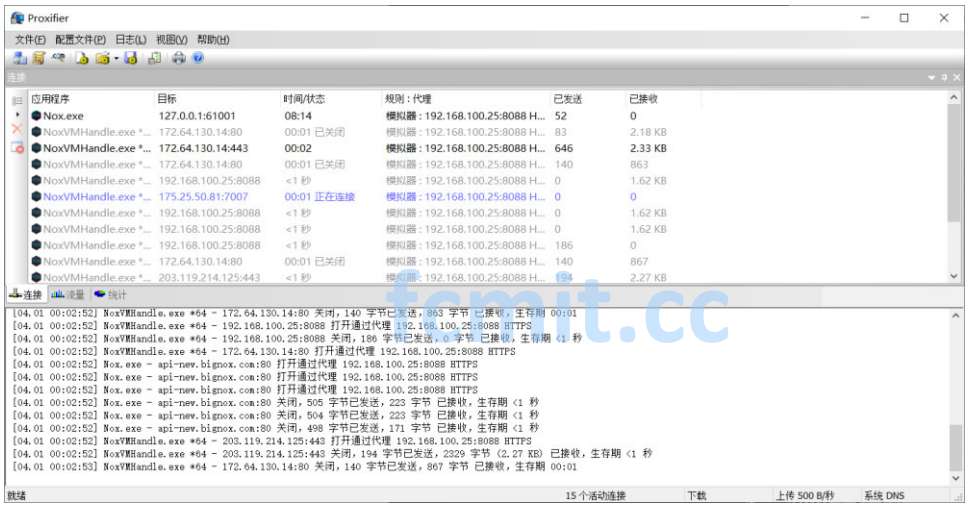
代理的名称任意填，应用程序需要抓取模拟器程序的进程，这里用的夜神。

multiplayermanager.exe; nox.exe; noxrepair.exe; noxvmsvc.exe; noxvmhandle.exe

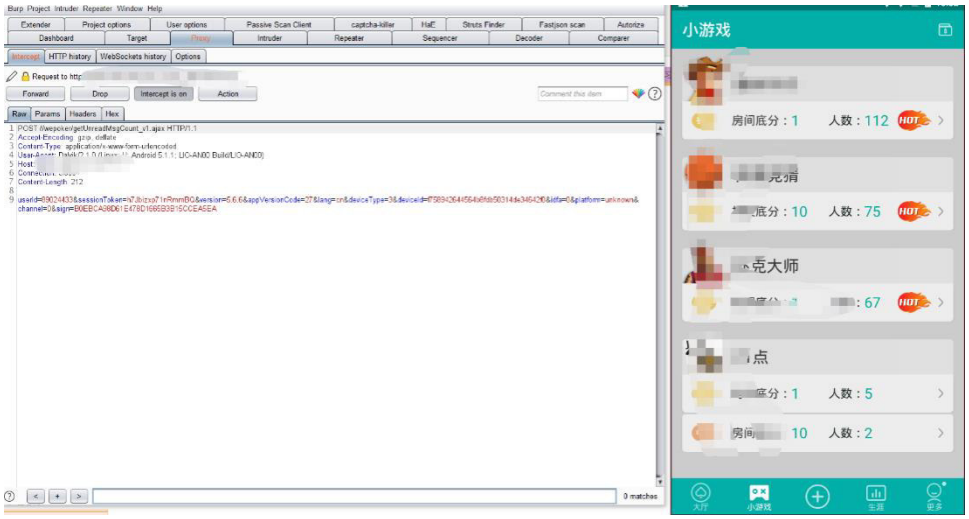
选取进程试最好是点击浏览，找到该进程的文件路径，并选取防止找不到路径导致找不到包



5、确定完成即可，运行 APP 可以看到模拟器的数据，如下图:



6、burp 抓包成功，如下图

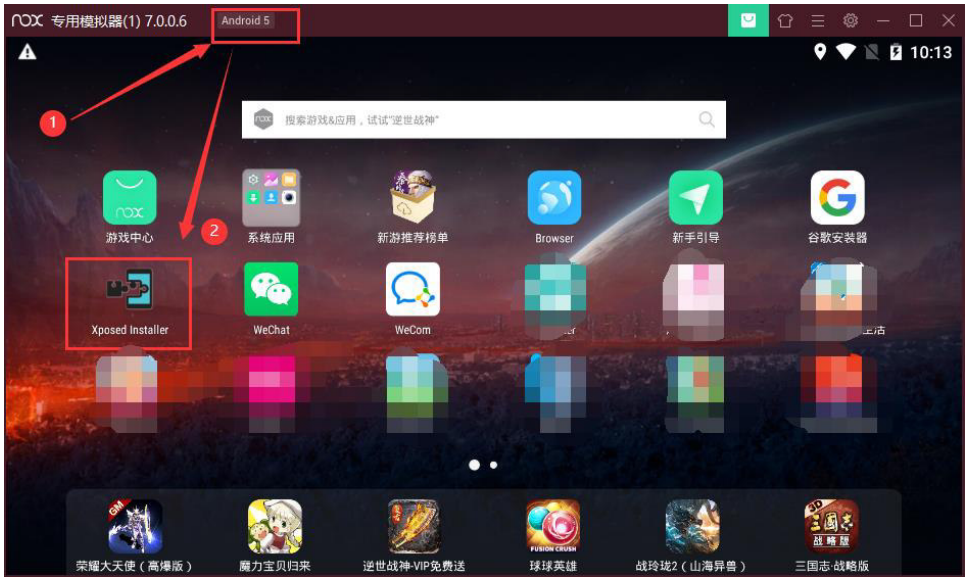


方法三：夜神+xposed+JustTrustMe 可突破双向验证

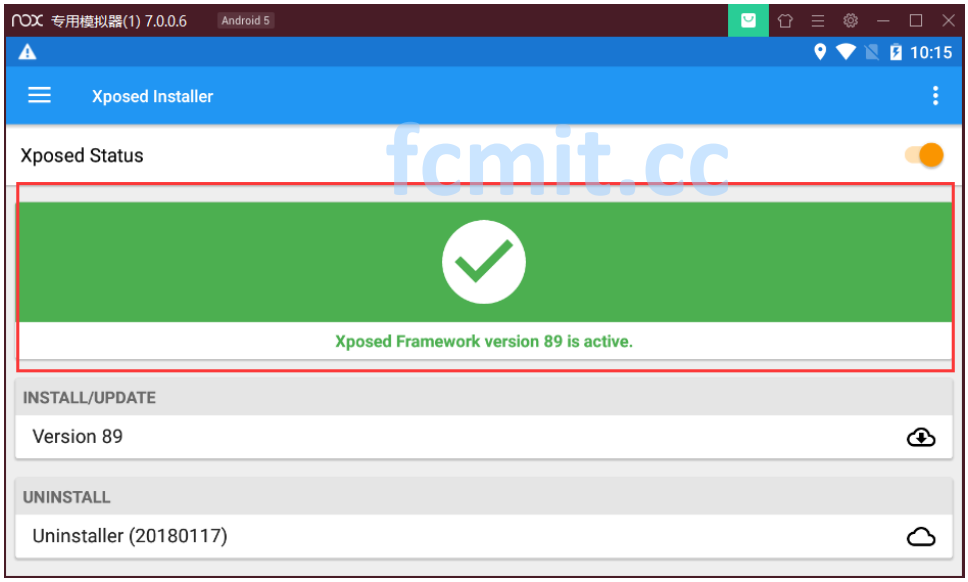
环境准备:

夜神模拟器（Android 5 版本）、JustTrustMe、xposed
安装完成如下图：

- 安装 xposed 生成一个 APP



- 安装完成之后会打个绿√（踩坑点：xposed 貌似不支持 Android 7 版本的）

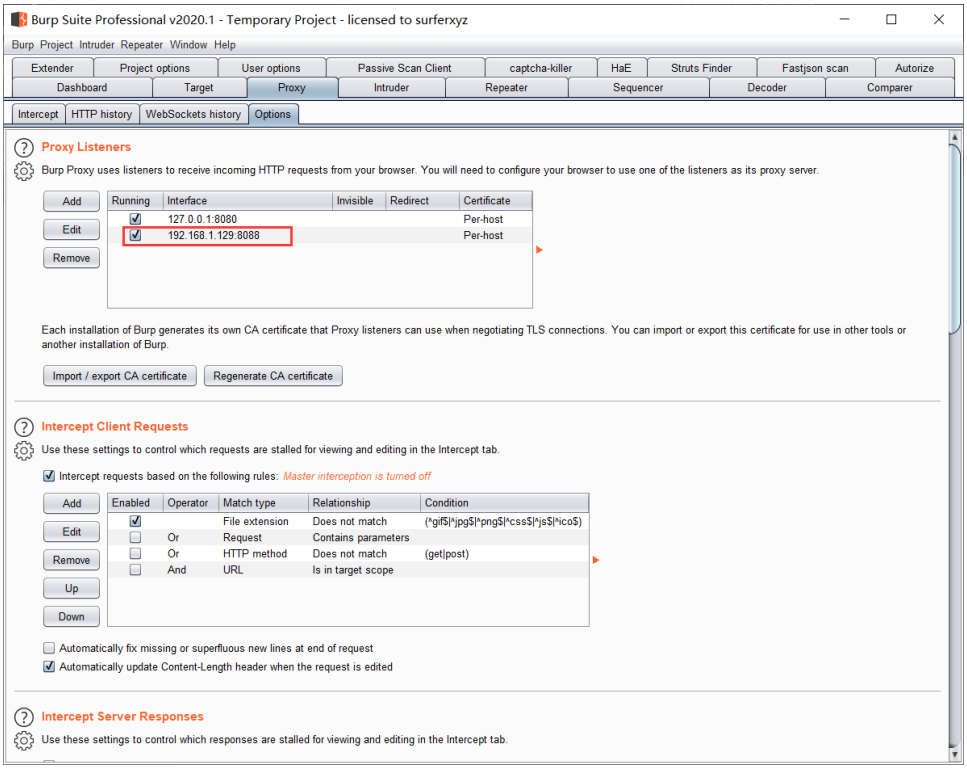


- 安装完成后，可以专门绕过一些对模拟器有防护的 APP，然后抓包方式与方法一一致。

方法四：使用真机（Android and IOS）的方式

场景：在实际的环境中，有很多的 APP 在模拟器中打开，会直接闪退，或者提示检测到使用模拟器打开。

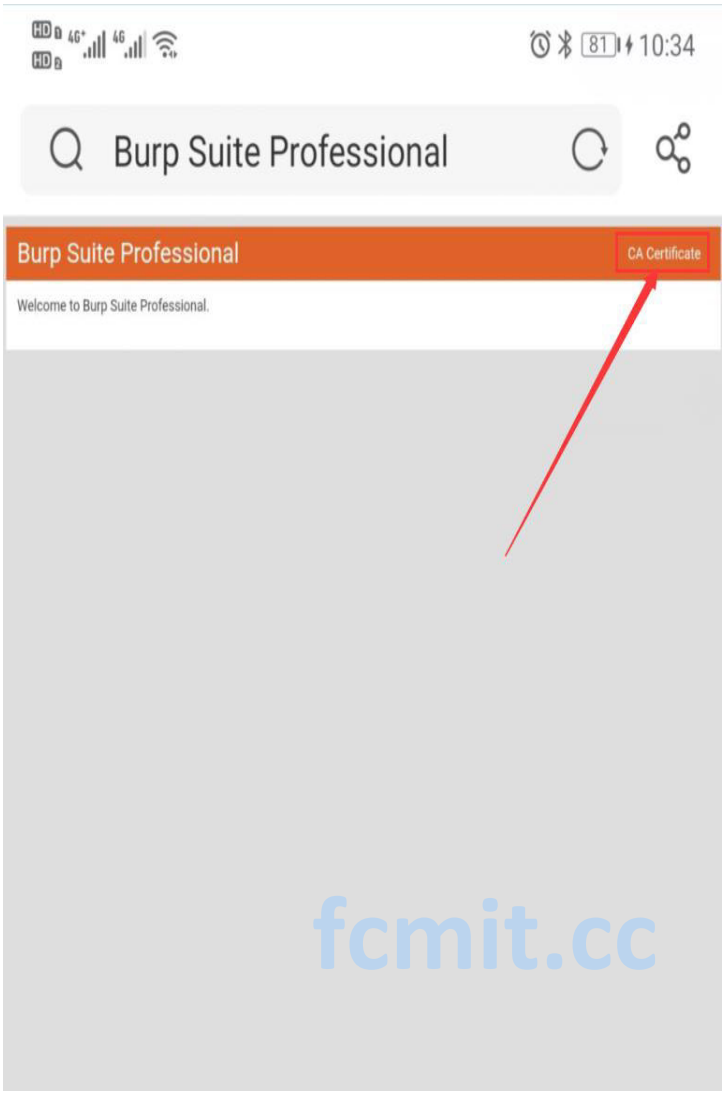
1、安装 burp 证书，burp 设置好代理（ps:设置的 IP 和端口要与真机的一致）



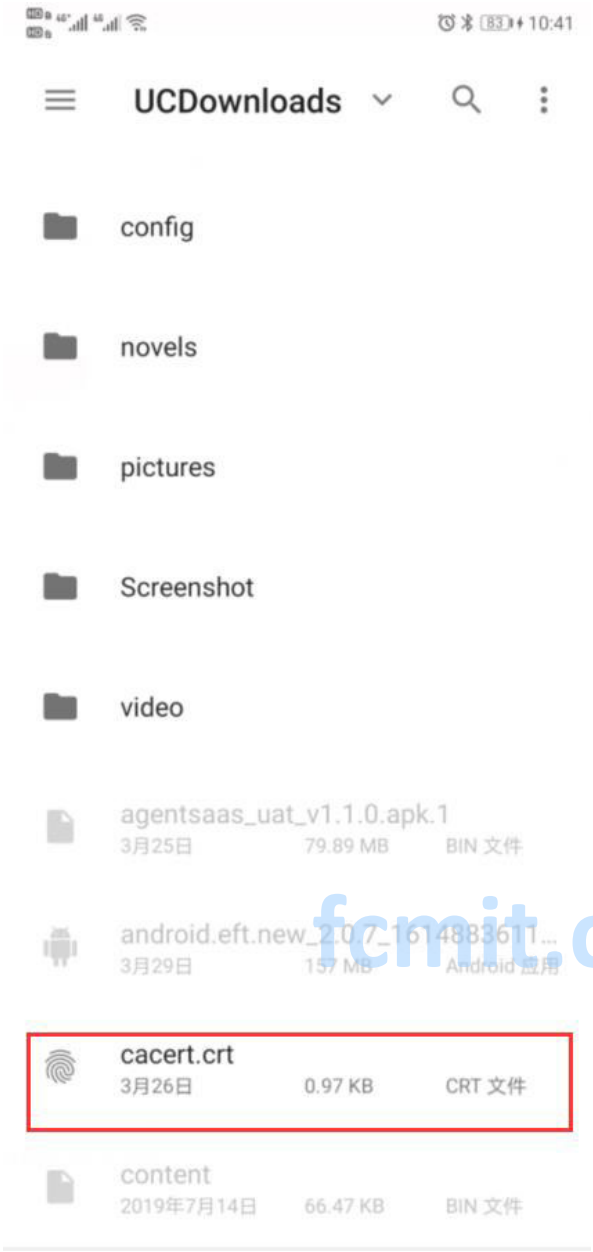
Android 环境

- 来到真机（本人的 P20 如下图）—>设置—>WALN—修改网络—>手动，如下图：主机名和端口与 burp 一致

- 设置完成之后真机也需要安装 BURP 的证书，如下图，访问 http://burp,下载好证书



- 下载完成后，回到设置—>安全—>更多安全设置—>加密和凭据—>从存储设备安装证书，找到下载的证书**（ps：证书的命名要以.crt 的格式作为后缀名），如下图：**

- 

- 点击安装，默认安装，安装完成即可。

IOS 环境

- 来到真机（本人的 IOS 如下图）—>设置—>WALN—点击网络—>配置代理—>自动修改为手动，如下图：主机名和端口与 burp 一致

- 设置完成之后真机也需要安装 BURP 的证书，如下图，访问 http://burp,点击右上角的证书，并安装，出现相关提示

- 根据提示，回到设置—>通用—>关于本机—>证书信任设置—>针对根证书启用完全信任，把 PortSwigger CA 选择即可安装完成，**如下图：**


无 SIM 卡
下午10:51
关于本机
证书信任设置
受信任证书存储区版本
2018121000
针对根证书启用完全信任
PortSwigger CA
进一步了解被信任的证书
fcmit.cc