2.app渗透 微信小程序抓包

1.burpsuite Proxifier 微信pc端 小程序抓包

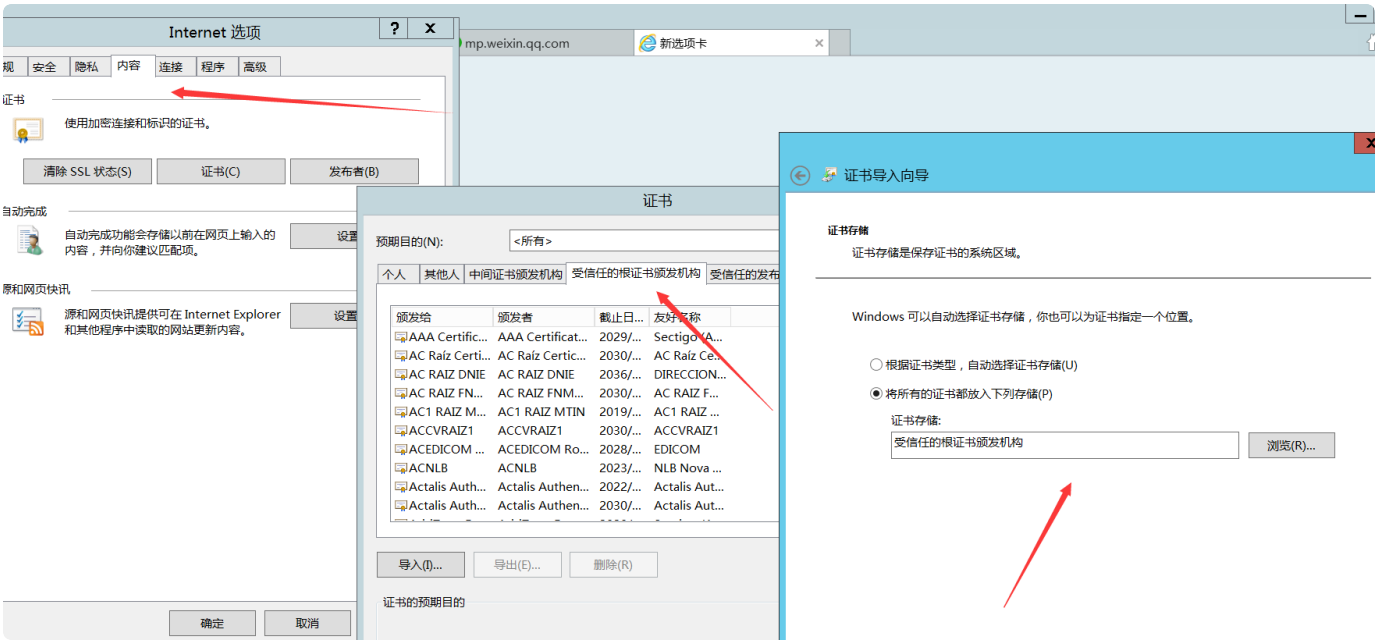
测试的时候微信最新的版本 3.9.2.23

burpsuite 主要是拦截包和改包

Proxifier 隧道代理工具

burpsuite安装好后访问 http://localhost:8080/ 下载证书到本地

打开ie浏览器 internet 选项 –> 证书–> 受信任的根证书–>确定

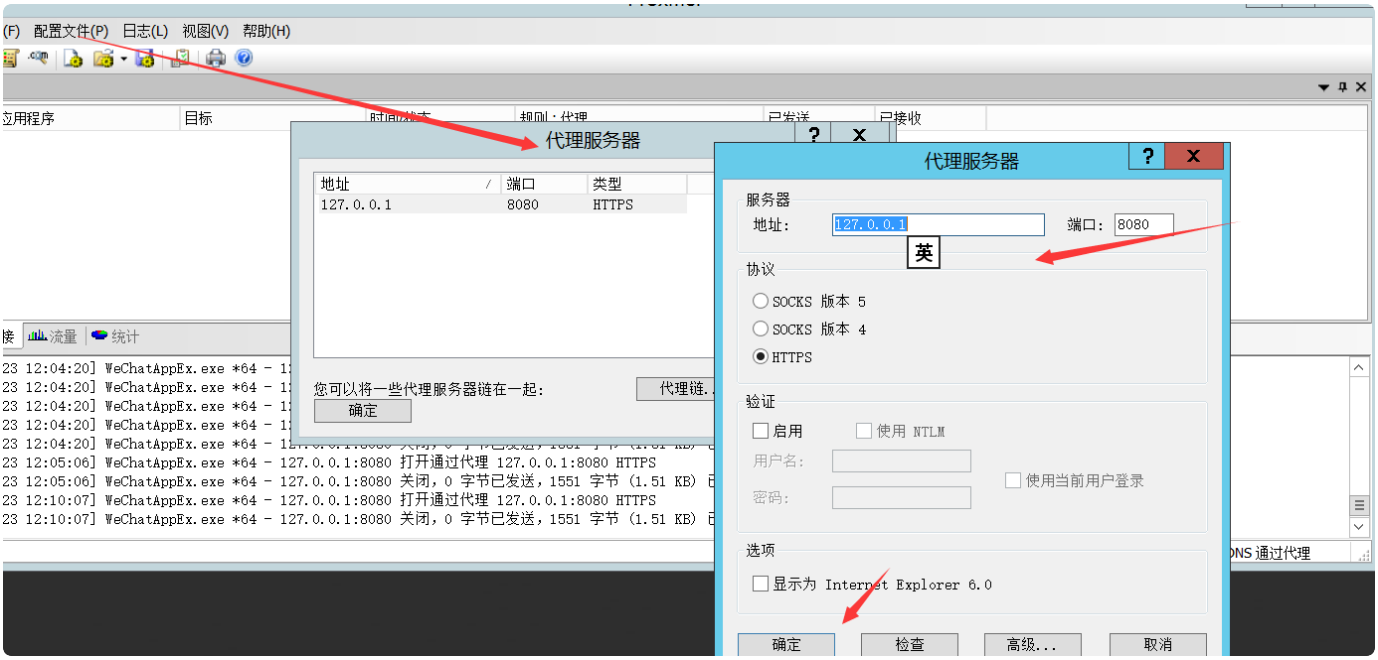


导入证书后 浏览器就可以抓取https的利浏览包

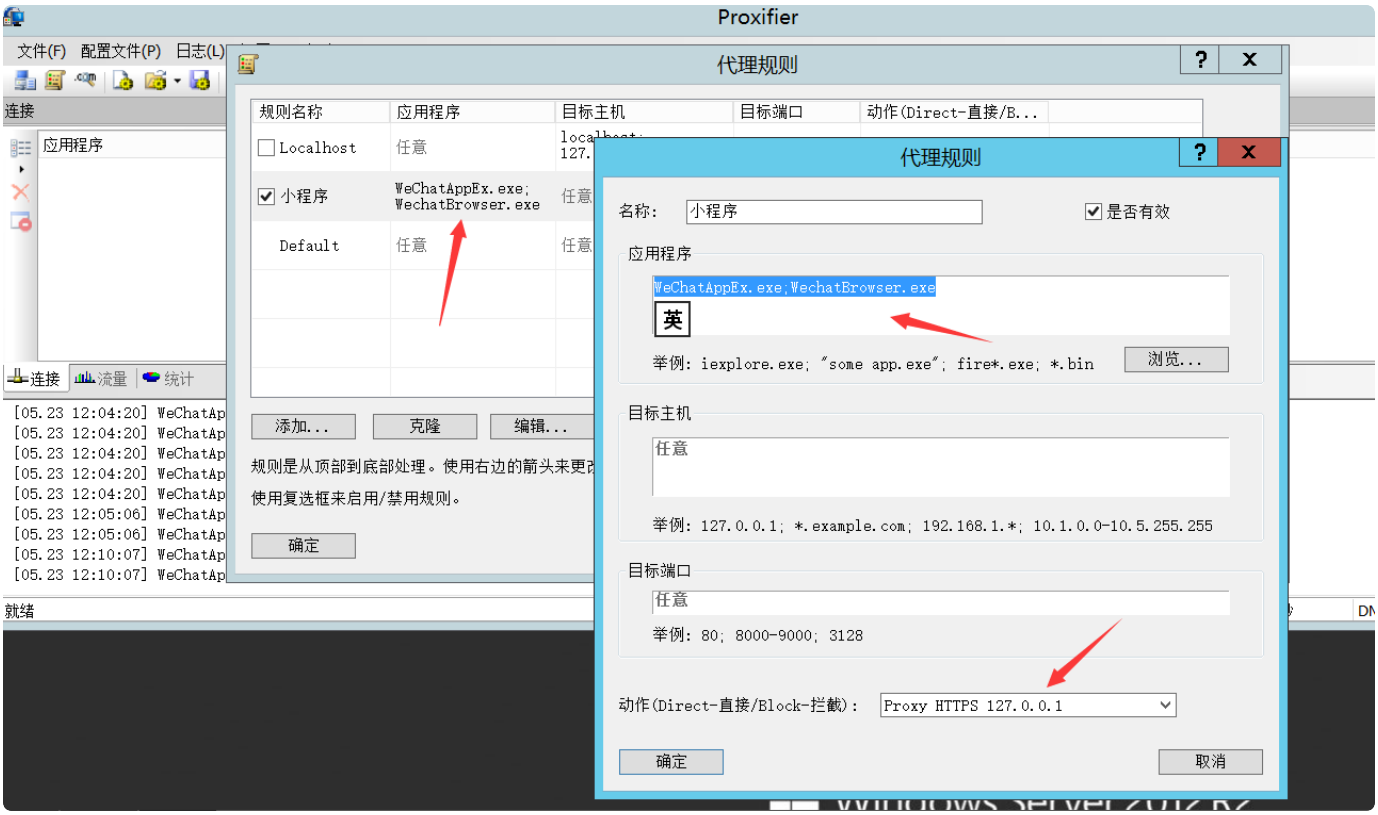
安装Proxifier 下面是激活码

```
5EZ8G-C3WL5-B56YG-SCXM9-6QZAP
G3ZC7-7YGPY-FZD3A-FMNF9-ENTJB
YTZGN-FYT53-J253L-ZQZS4-YLBN9
```

设置隧道 https隧道



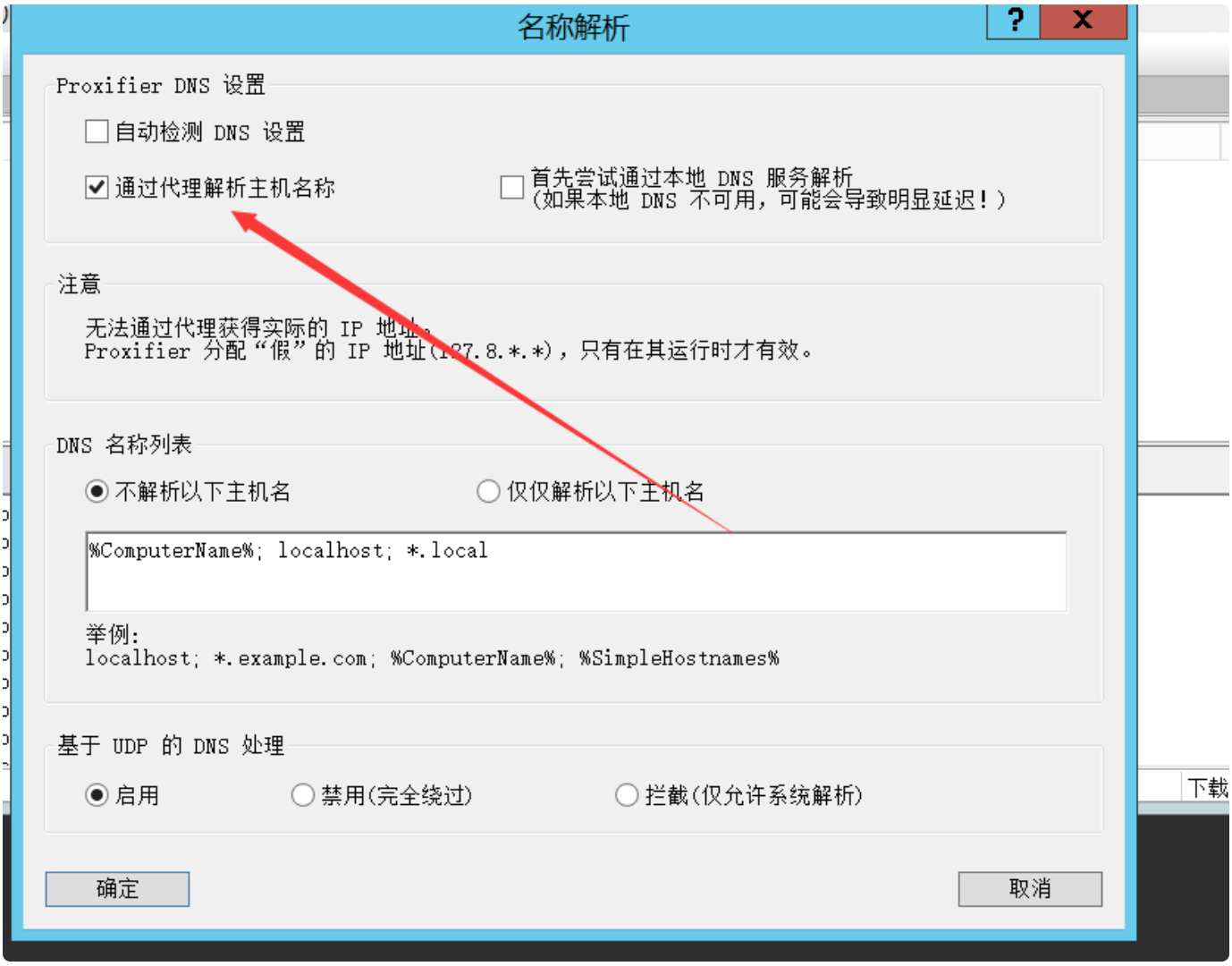
设置代理规则



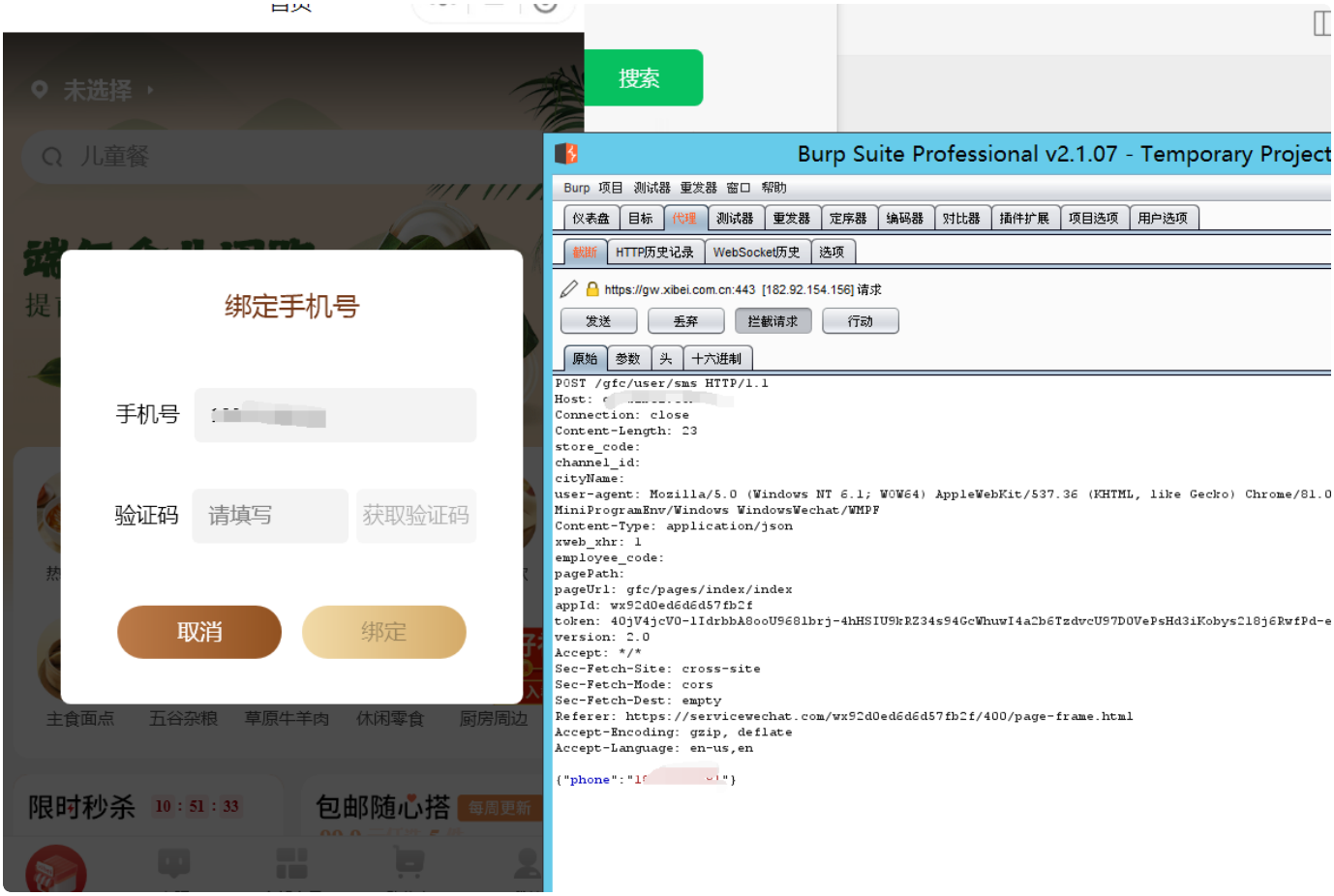
设置抓取代理的exe文件 这两个访问小程序的exe文件 需要设置访问时候代理的隧道

```
WeChatAppEx.exe;WechatBrowser.exe
```

在名称解析把通过代理解析主机名称勾上

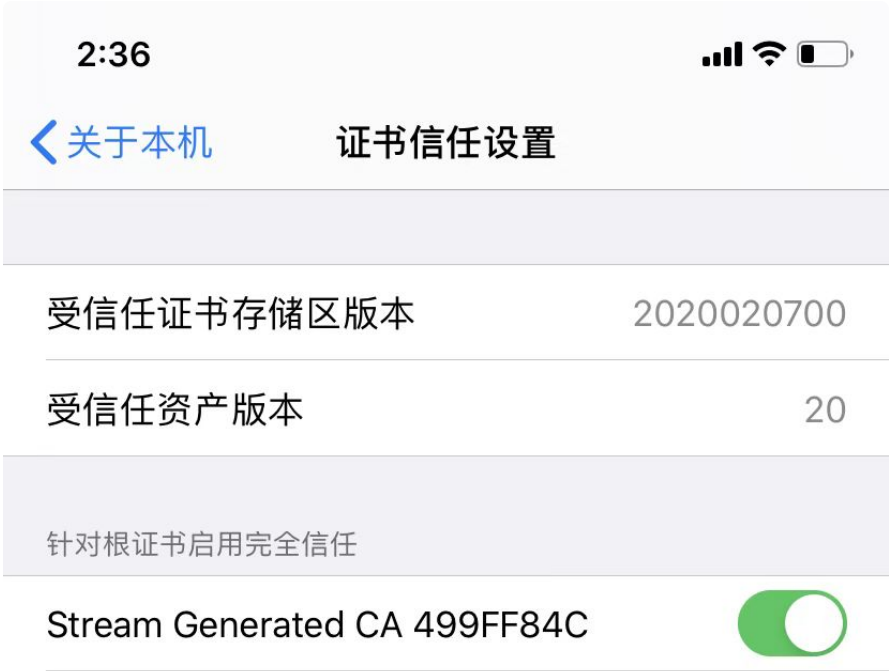


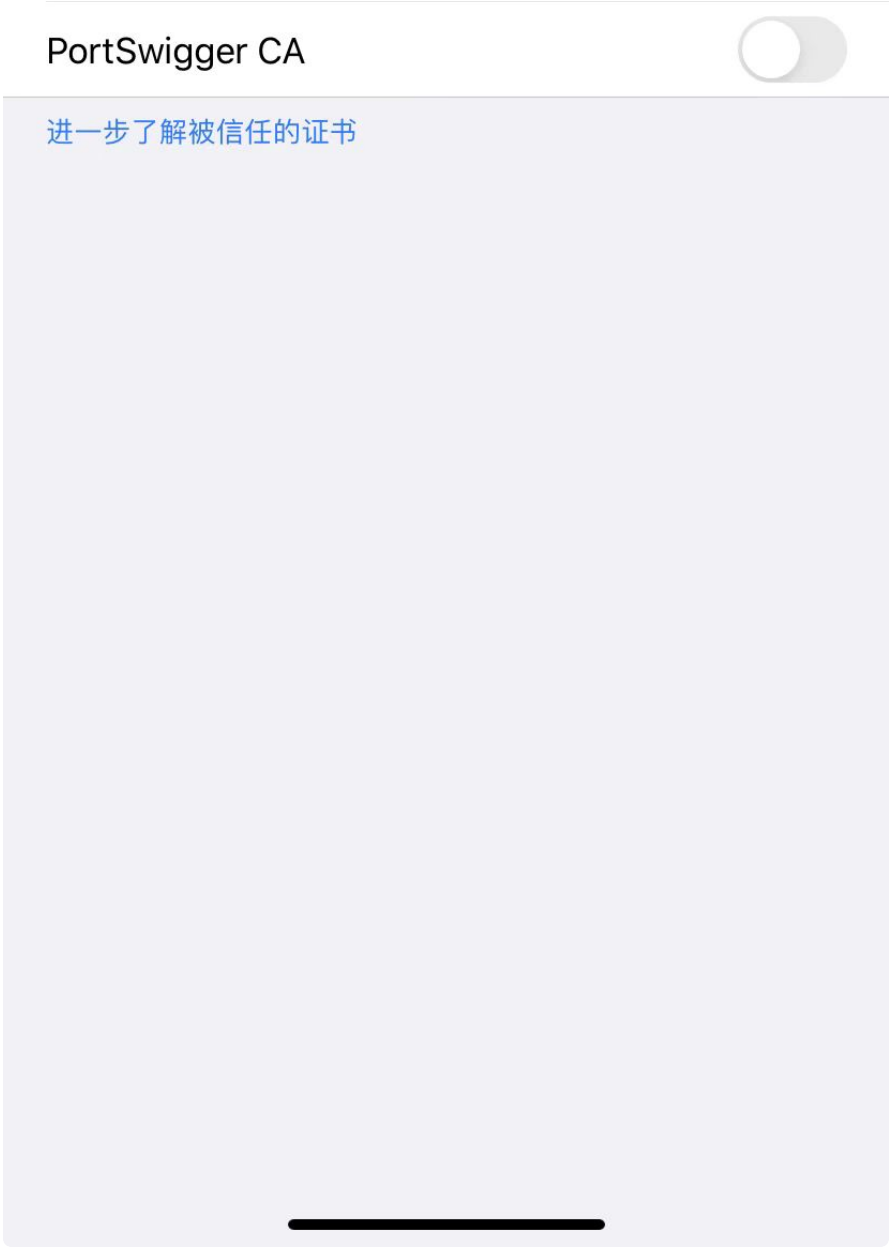
随便搜索一个小程序 访问 抓包成功



2.使用Stram iso系统抓微信小程序包

1、前往AppStore 免费下载 Stream





2、滑动到底部，在settings中点击HTTPS Sniffing(https抓包)

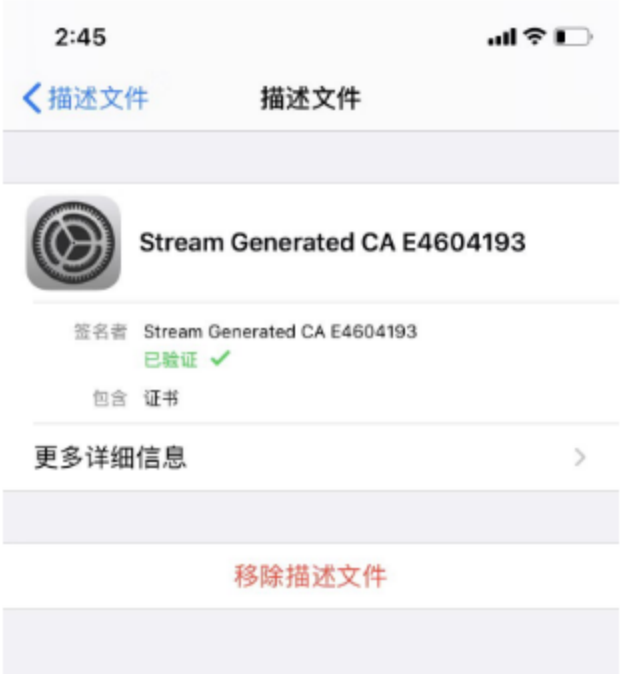
3.点击安装ca证书,在下图的页面选中INSTALL CA CERTIFICATE

4.IOS的警告信息，直接点击允许即可

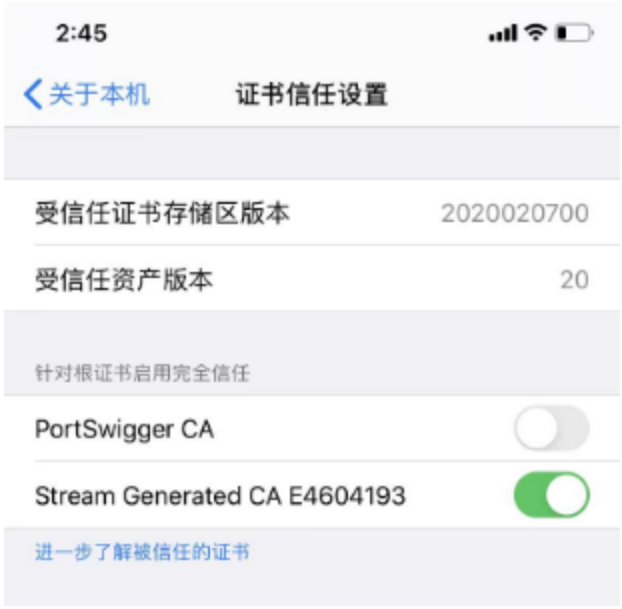
5.CA证书的安装与配置，手机设置–通用– –往下滑找到–VPN与设备管理–点击已下载的描述文件

6.来自IOS的警告，直接点击安装就行了

7.出现下图中的样式，即安装成功



8.再到–手机设置–通用–关于本机–往下滑找到–证书信任设置–把stream开头的那个开关打开



9.点击STREAM软件顶部的SNIFF NOW即可进行抓包。

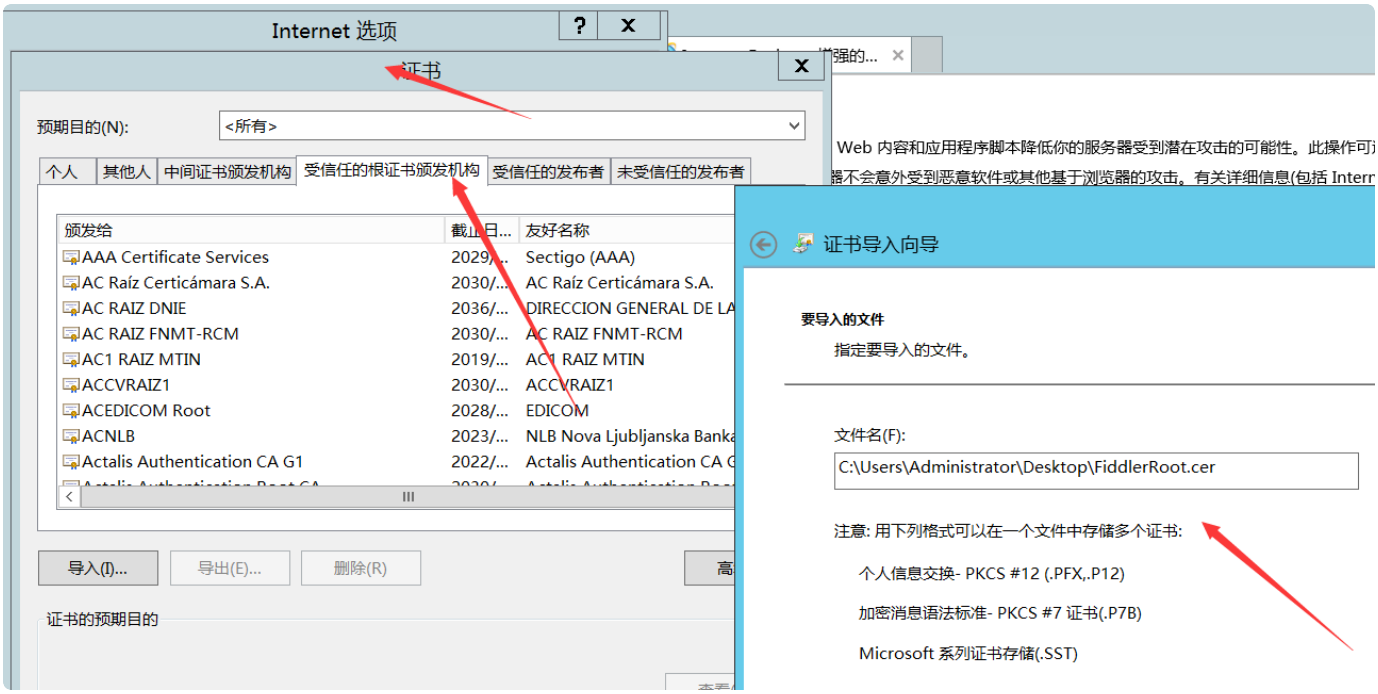
3.fiddler 导入Stram app数据包并修改提交

打开 fiddler 安装ca证书

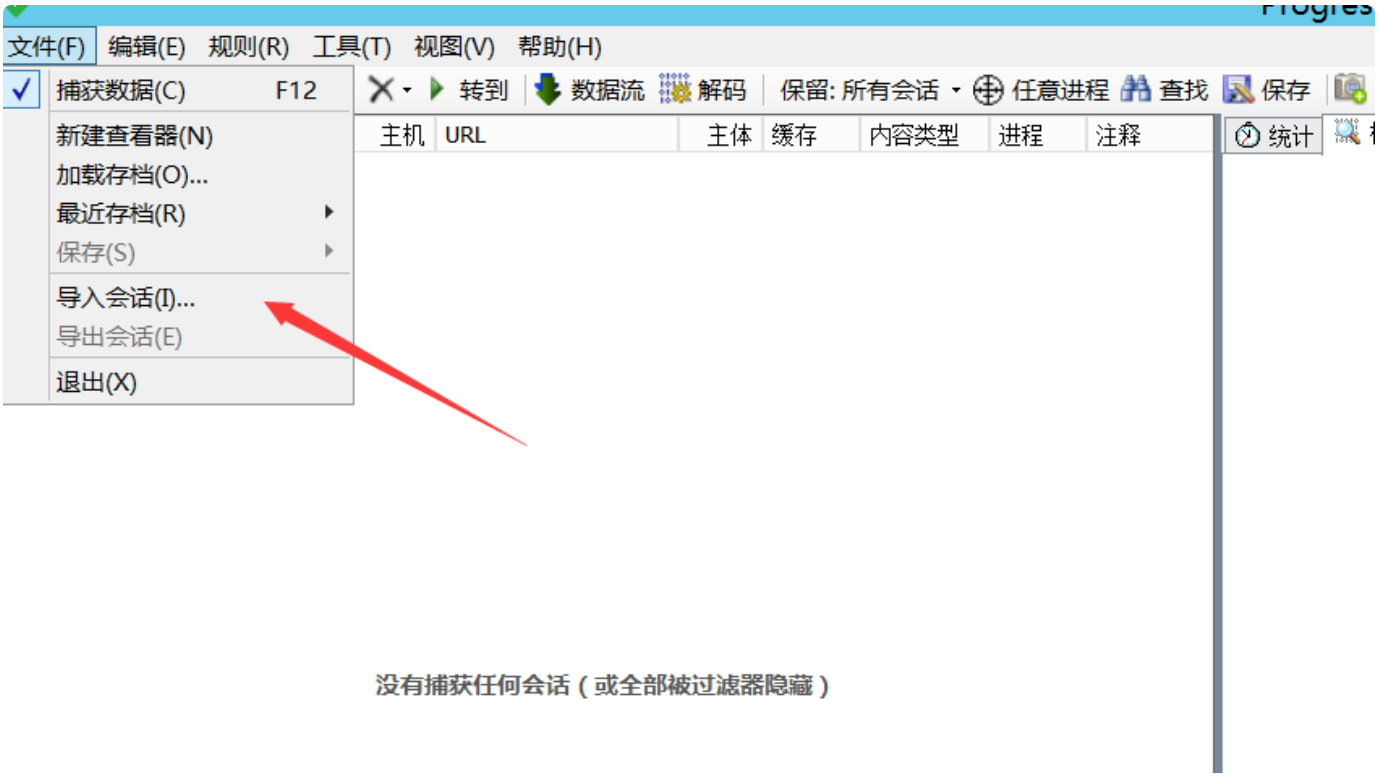
工具 选择 https 把解密https流量 勾上

操作 导出ca证书

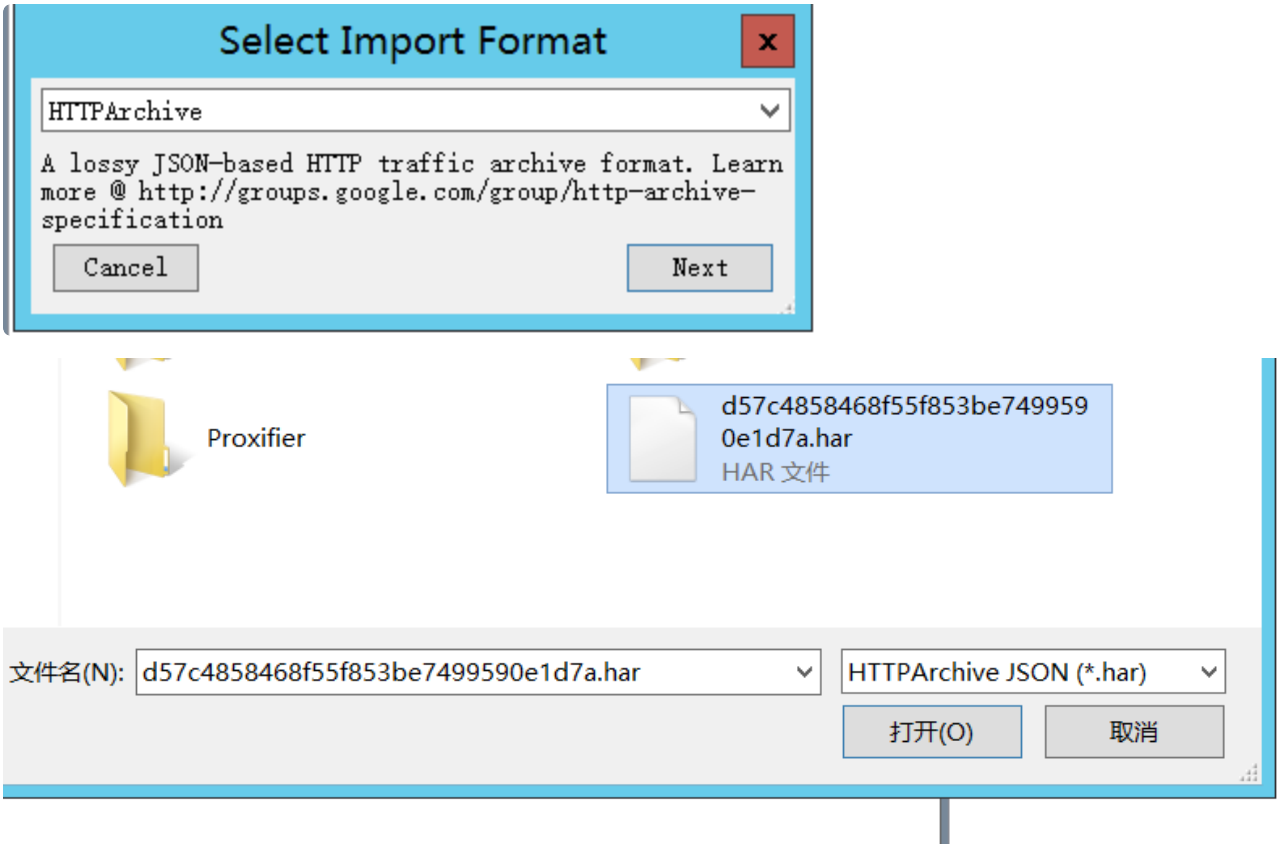
导入证书



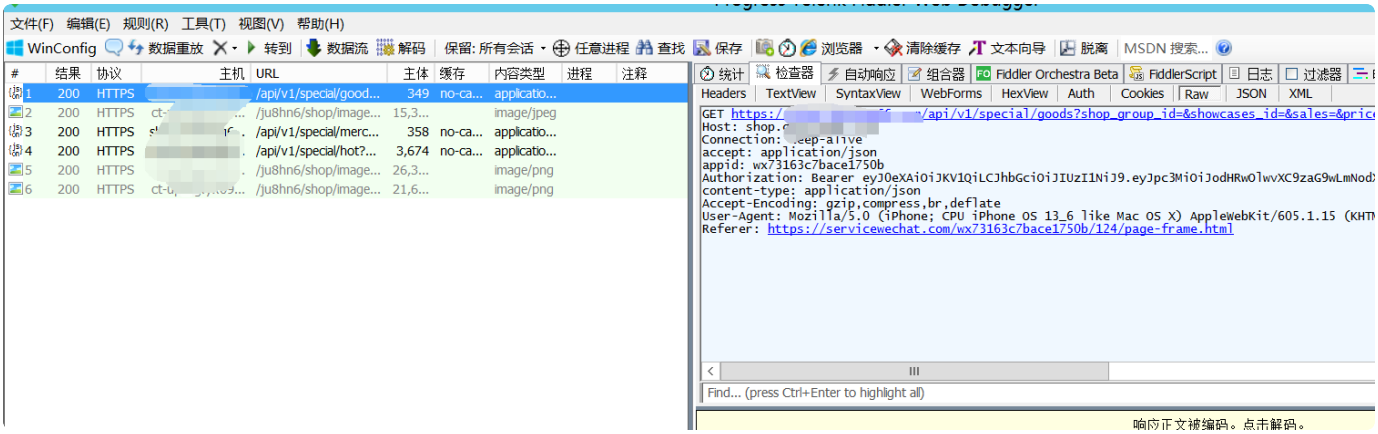
导入保存的.har文件



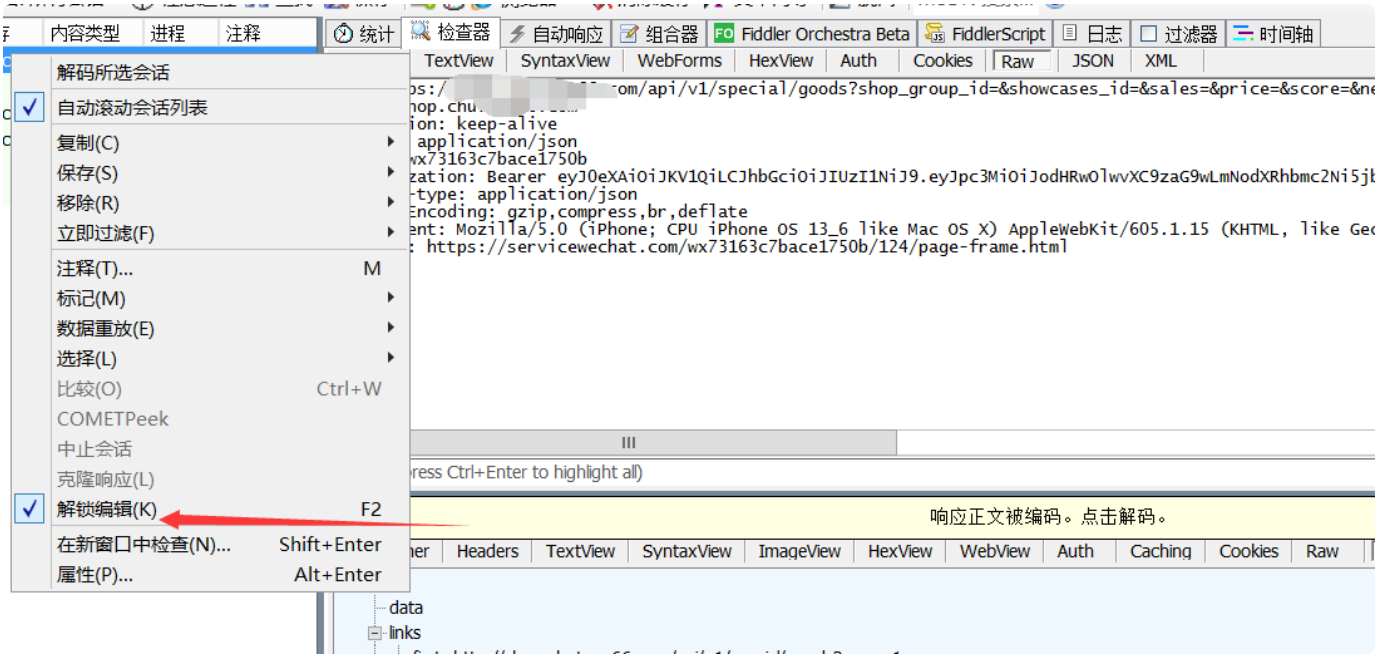
选择HTTPArchive



成功导入



接着就要可以解决编辑 修改包 重放包


内容类型
进程
注释
统计
检查器
自动响应
组合器
Fiddler Orchestra Beta
FiddlerScript
日志
过滤器
时间轴
TextView
SyntaxView
WebForms
HexView
Auth
Cookies
Raw
JSON
XML
解码所选会话
自动滚动会话列表
复制(C)
保存(S)
移除(R)
立即过滤(F)
注释(T)... M
标记(M)
数据重放(E)
选择(L)
比较(O) Ctrl+W
COMETPeek
中止会话
克隆响应(L)
解锁编辑(K) F2
在新窗口中检查(N)... Shift+Enter
属性(P)... Alt+Enter
application/json
Encoding: gzip,compress,br,deflate
https://servicewechat.com/wx73163c7bace1750b/124/page-frame.html
响应正文被编码。点击解码。
Headers
TextView
SyntaxView
ImageView
HexView
WebView
Auth
Caching
Cookies
Raw
data
links