广汽丰田 IA5 AVNT 车机破解超详细过程

此方法非本人完成，感谢另外的车友

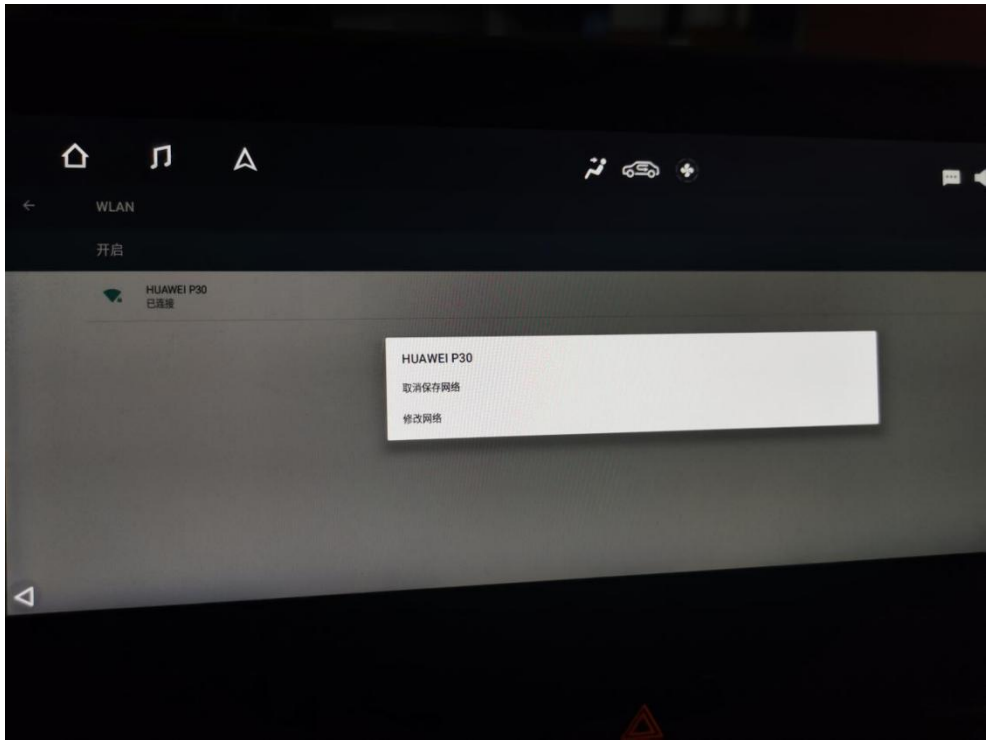
准备工作

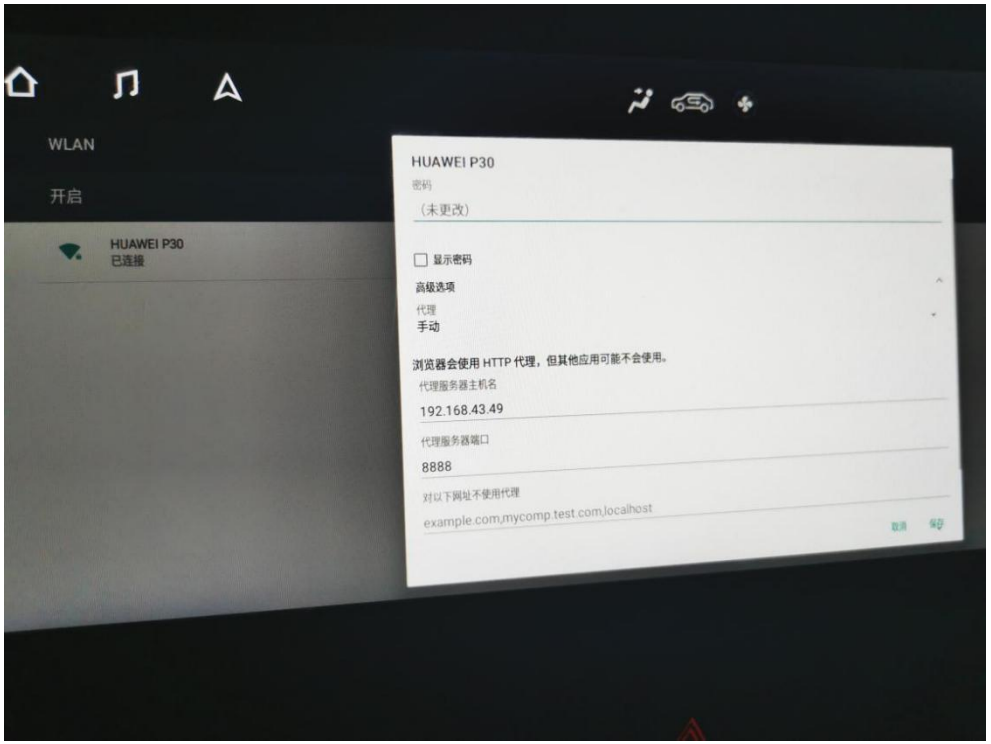
笔记本电脑一台，手机一台，charles 软件，本人使用mac 运行charles，理论上其他能跑 charles 的环境都可以，本人 charles 为 mac 最新 4.5.6 版本，其他版本可能有细微调整，并不影响最终效果。车机在应用商店下载出游 app。

搭建 charles 运行环境

使用手机开一个热点，mac 和车机都连接手机热点，运行 charles，在车机的系统设置中长按车辆信息，打开 Android 系统设置，找到 wifi 设置，长按 wifi 名字，选择修改网络，打开高级设置选项，设置代理为 mac 的 ip 地址，端口号填 8888 (charles 的默认代理端口)

图示：





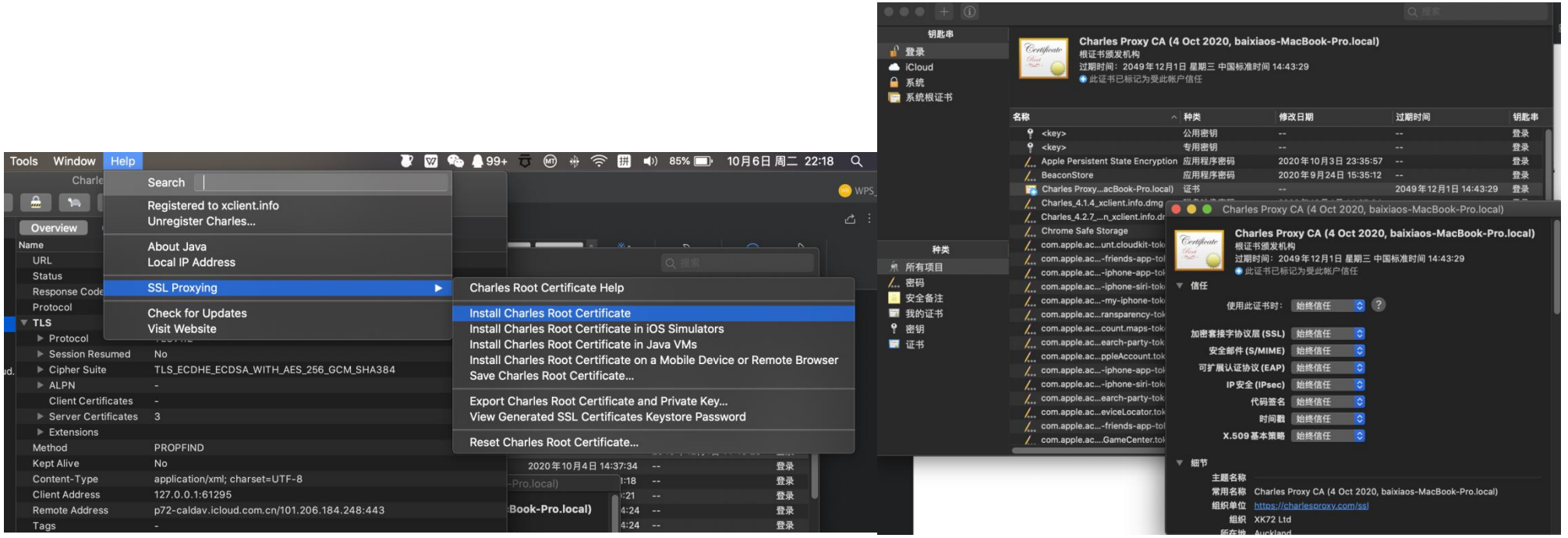
安装电脑和车机的 ssl 证书

如果不安装会出现 unknow 情况，无法正常抓包。

安装电脑 ssl 证书

进入 Charles – 》Help – 》SSL Proxying – 》Install Charles Root Certificate ， 会打开证书，安装进去，然后在钥匙串里面设置信任。

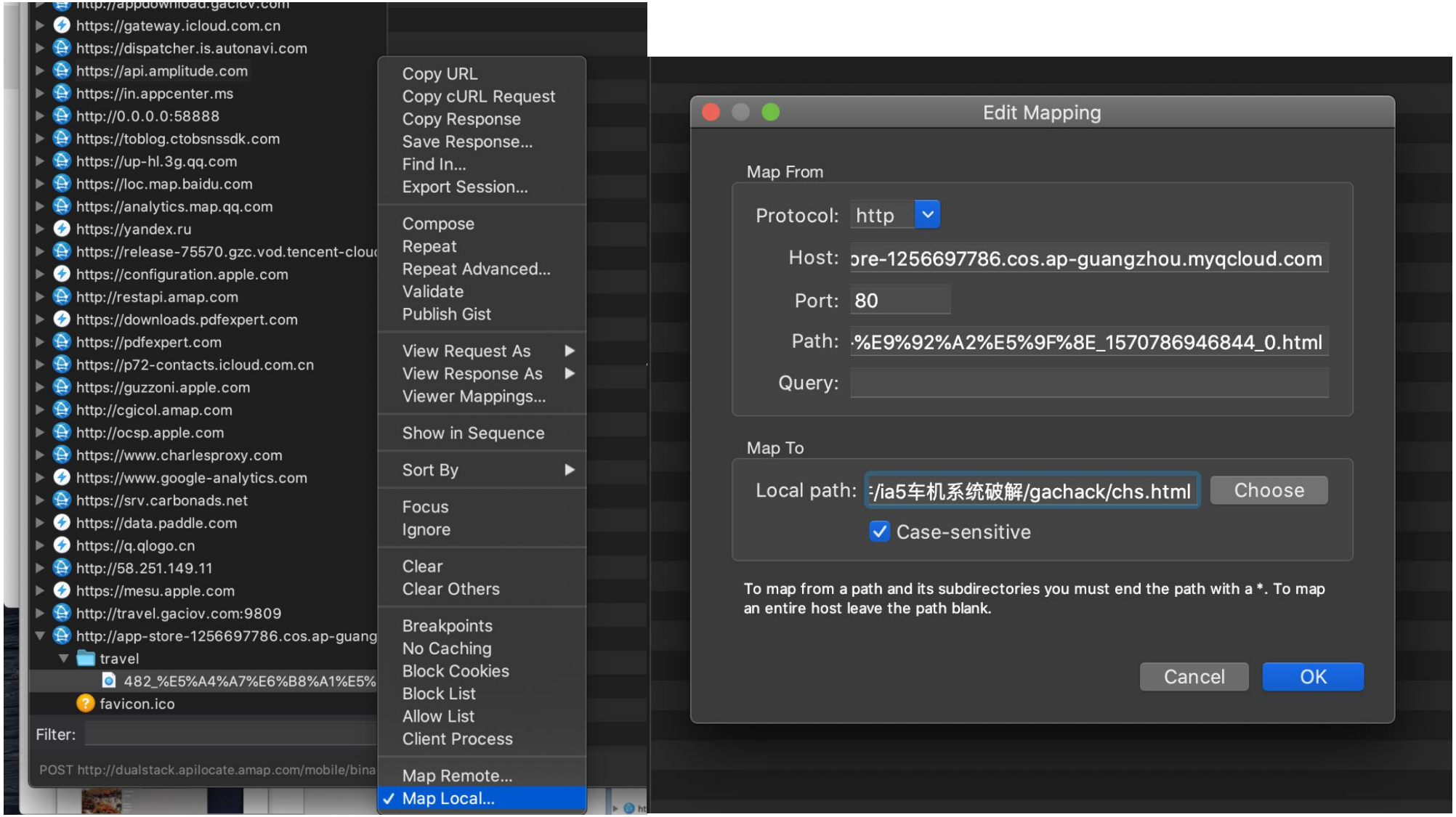
如图：



安装车机 ssl 证书

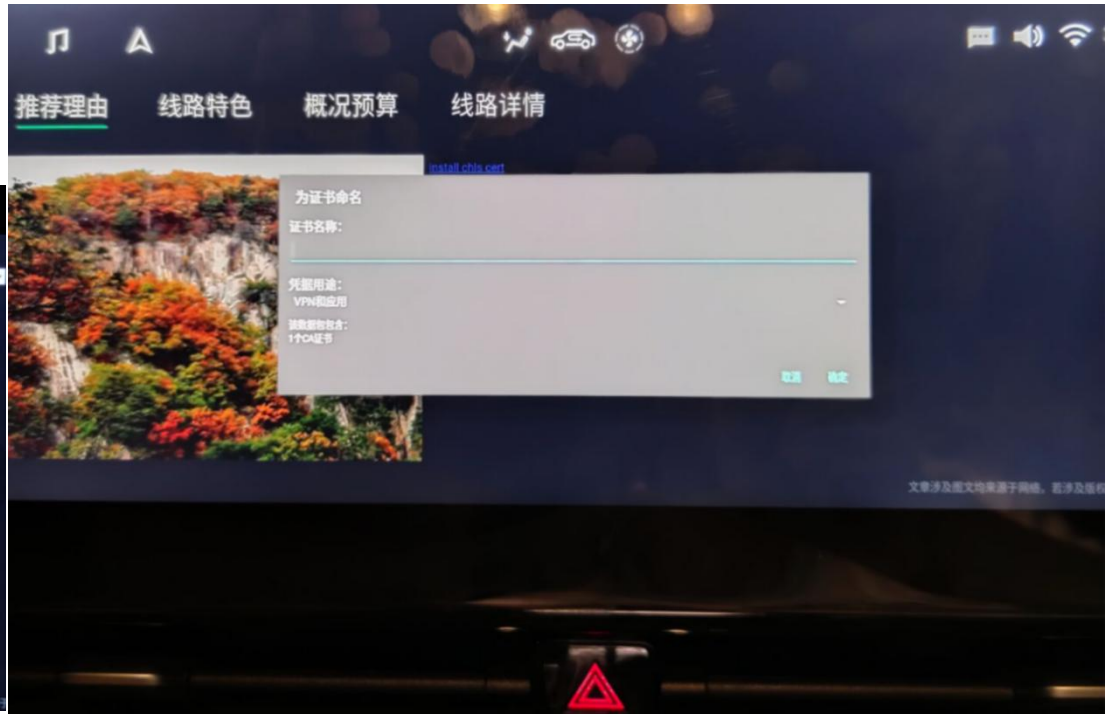
打开车机的出游 app，定位到任何一个景点页面， 打开详情，

这时发现 html 请求：http://app-store-1256697786.cos.ap-guangzhou.myqcloud.com/travel/*****.html
使用 charles map local 功能，map 该请求到附件中的 chs.html
如图：



重新进入刚才所点击的景点详情页，发现内容已被替换，点击 install charles cert 过一会弹出安装证书界面，点击安装。 此时会需要设置证书名字和设置系统密码，随意设置即可。

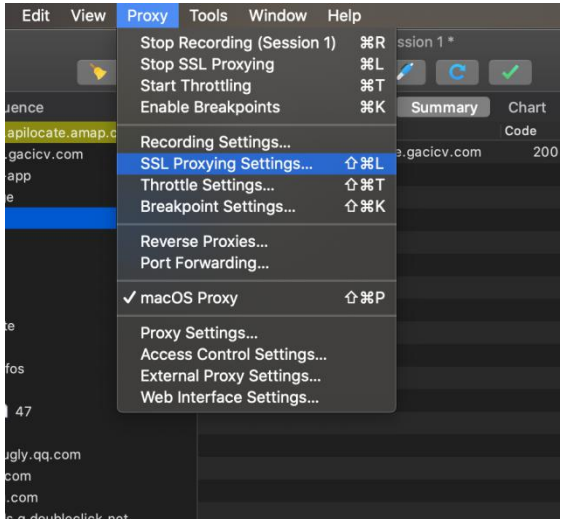
如图：

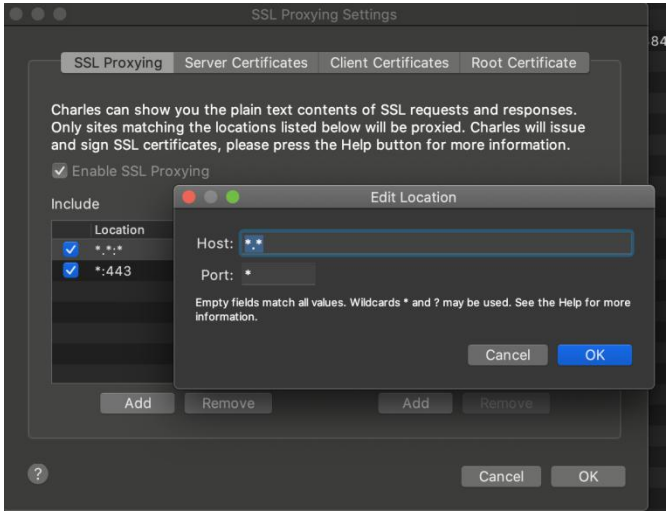


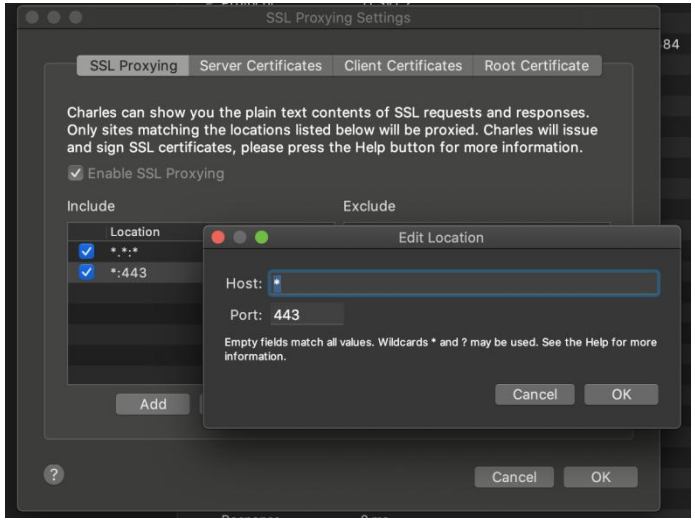
设置 Charles 的 https 白名单

不然会出现 unknow

如图：







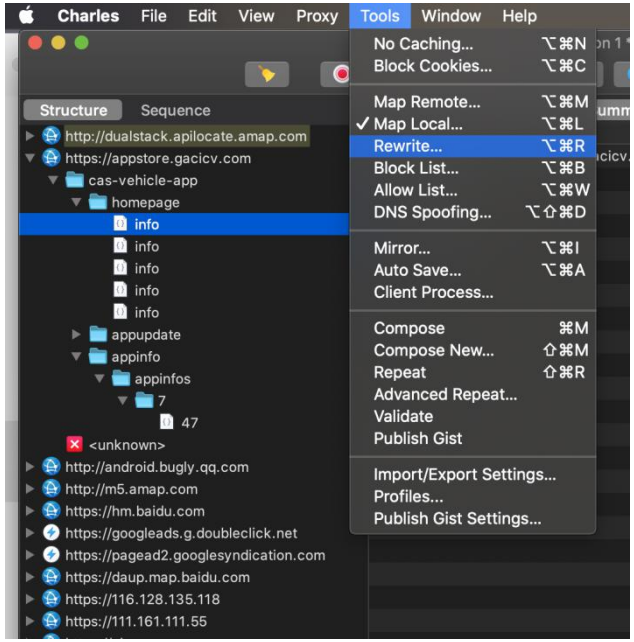
替换应用商店 apk

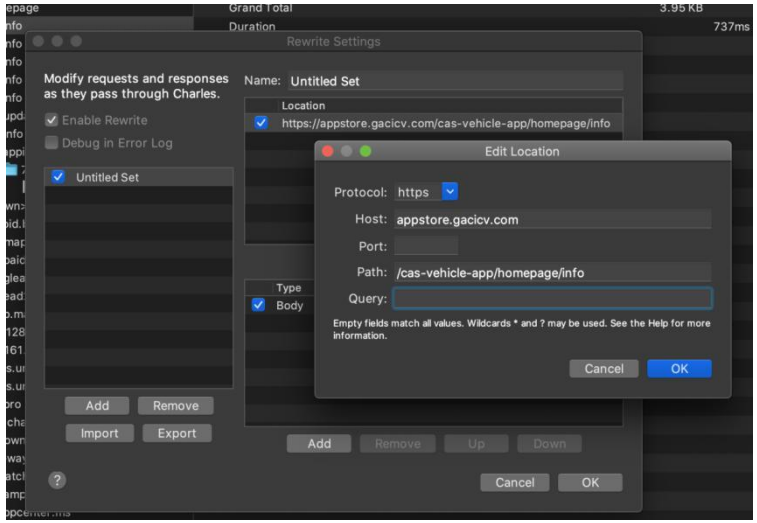
经过上面的步骤，再打开应用商店 App ， 发现应用列表请求:

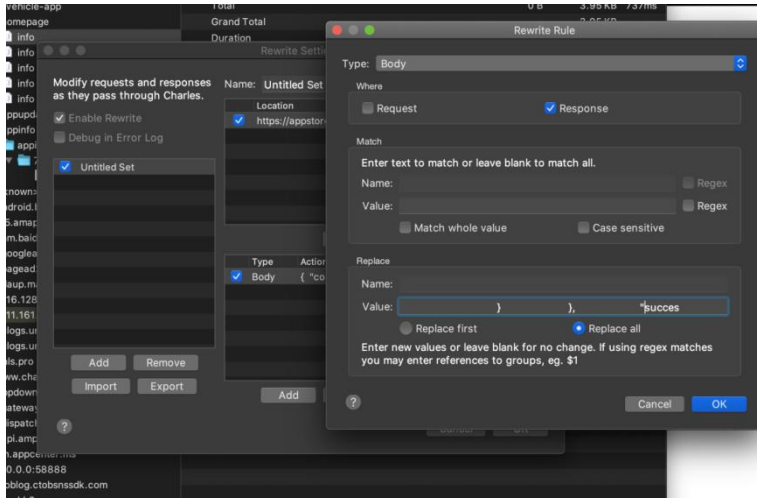
https://appstore.gacicv.com/cas-vehicle-app/homepage/info

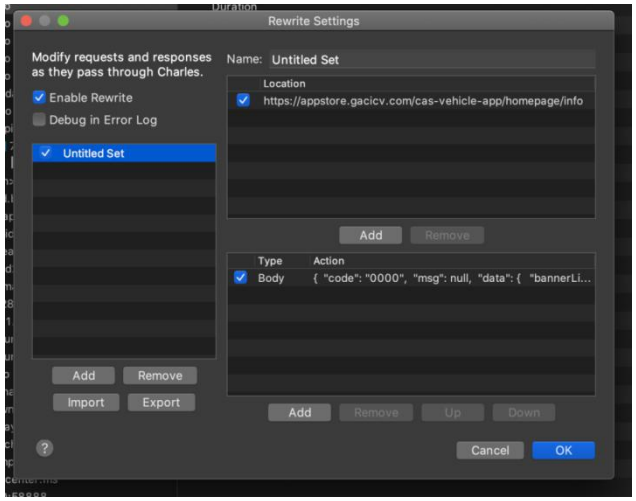
使用 Charles rewrite 功能，把请求内容 rewrite 为附件中 app_list.json 中的内容

如图:





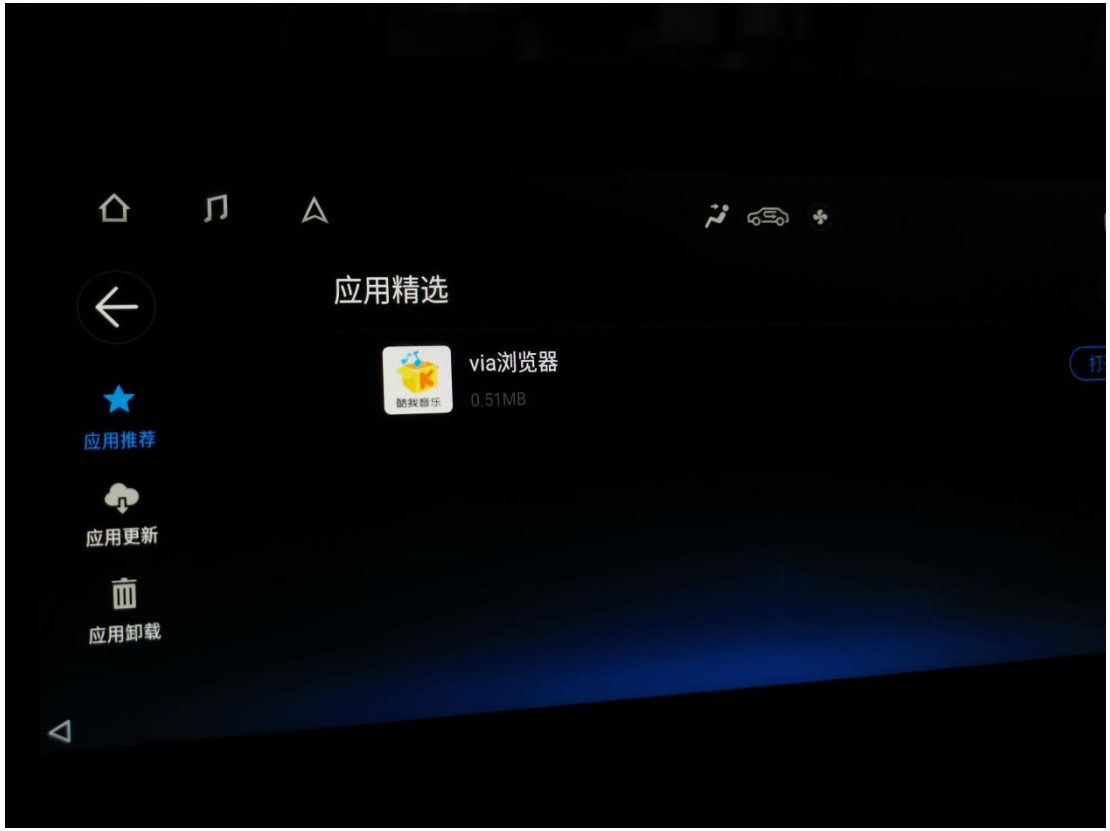




安装

下拉刷新应用商店，发现第一个 APP 已被替换为 via 浏览器，点击安装， 过一会安装完成，之后就可以用 via 浏览器下载其他 apk 安装到车机了。

至此！大功告成!
图示：



补充

车机上打开 via 浏览器，输入 https://log.gs/res/fm.apk，可以安装一个很好用的文件管理器，就可以用 U 盘安装 apk 了。