

米家iOS抓包教程

背景

SDK中的接口大部分都涉及到网络请求，开发者在使用SDK时难免会遇到一些问题。为了加强开发者的问题自排查能力，以及在提工单时能给我们提供更直接有效的信息，需要教会开发者如何抓包米家APP的网络请求。

教程

工具：Charles：<https://www.charlesproxy.com/>

此次教程以iPhone 7为例进行教学，iOS版本为13.3，本地操作系统为Mac

抓包前确保手机和电脑处于同一局域网下

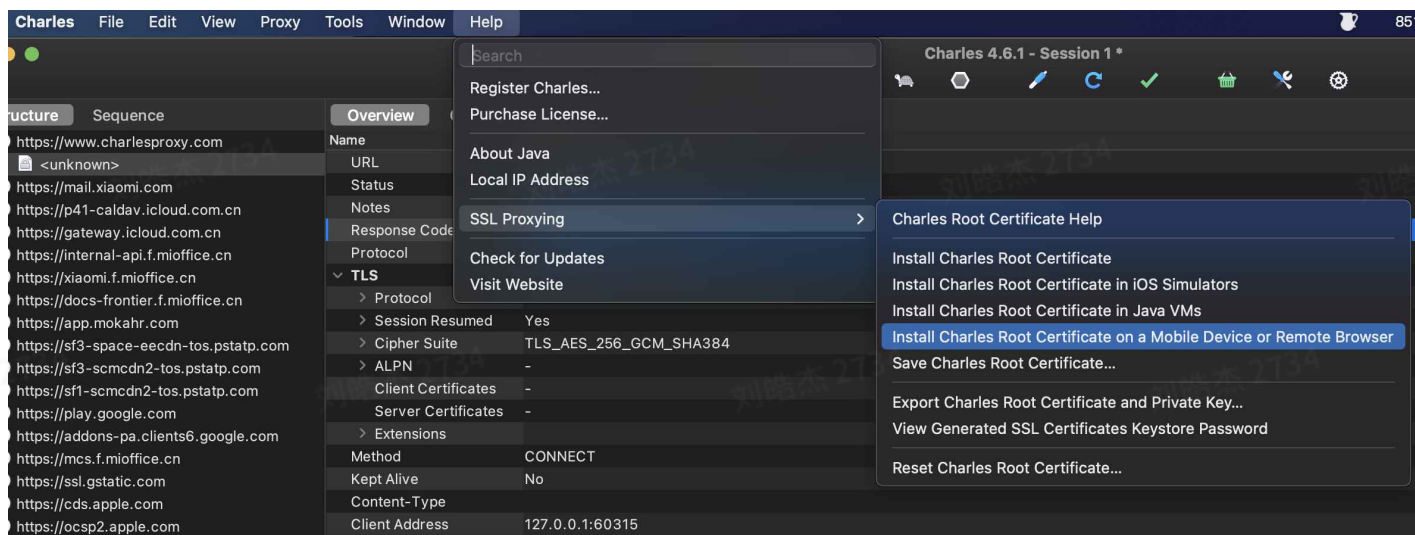
1、下载证书

打开Charles，下载证书有两种方式

一、浏览器下载证书

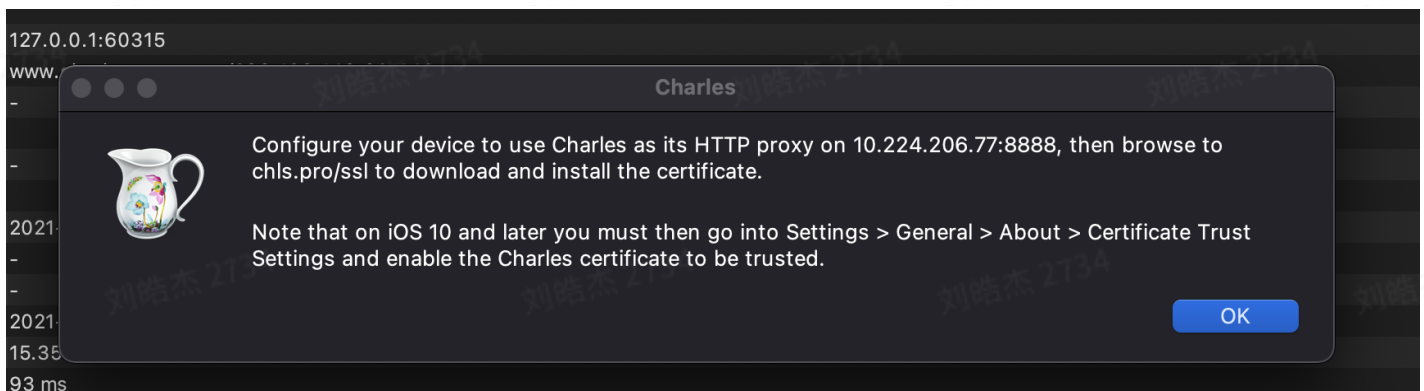
此方式在Mac系统下成功率较高，Windows系统下可能出现无法下载的情况，此时建议使用方案二

1、首先打开Charles，Help->SSL Proxying->Install Charles Root Certificate on a Mobile Device or Remote Browser



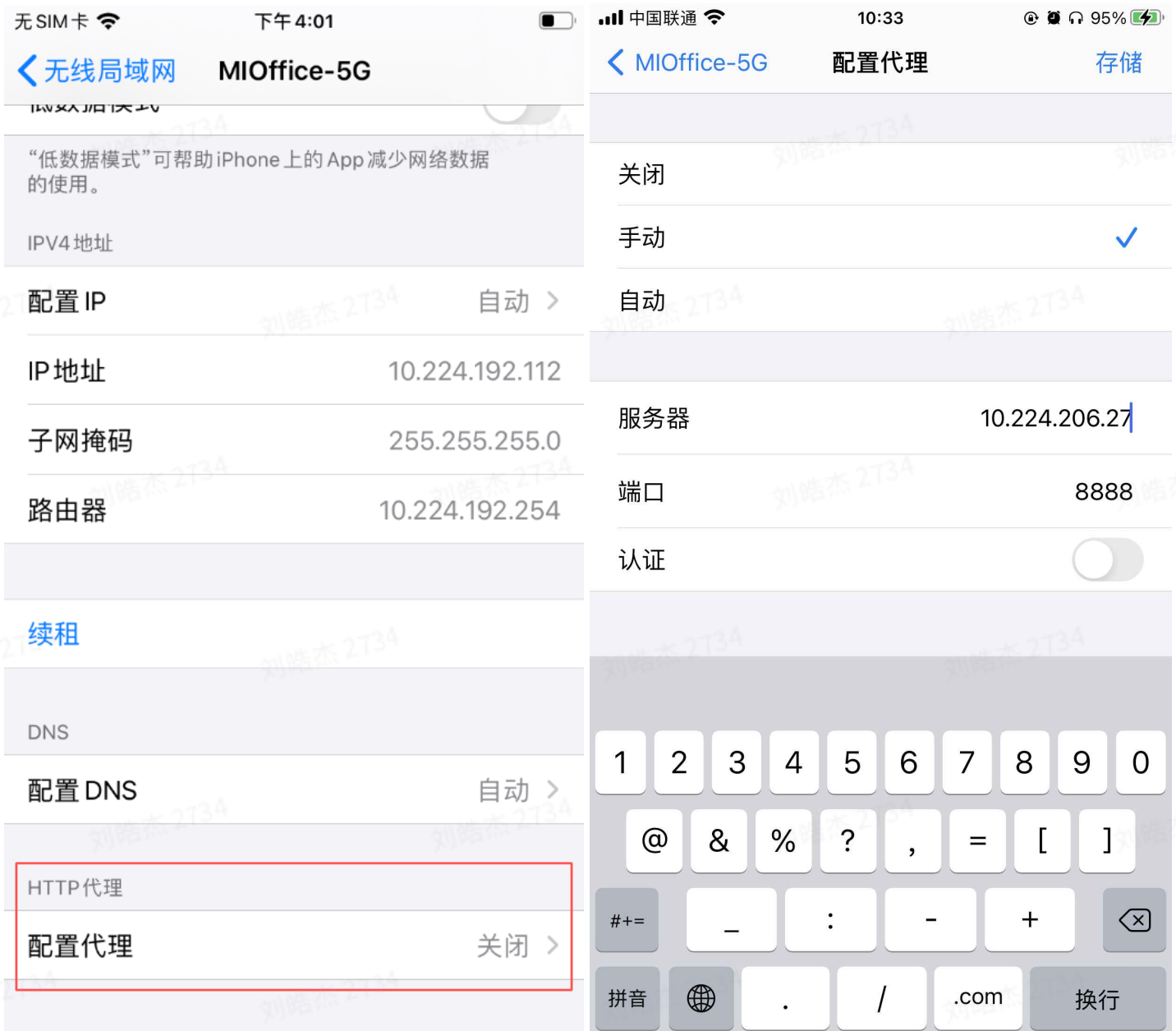
1.1.1手机安装证书

会弹出如下窗口



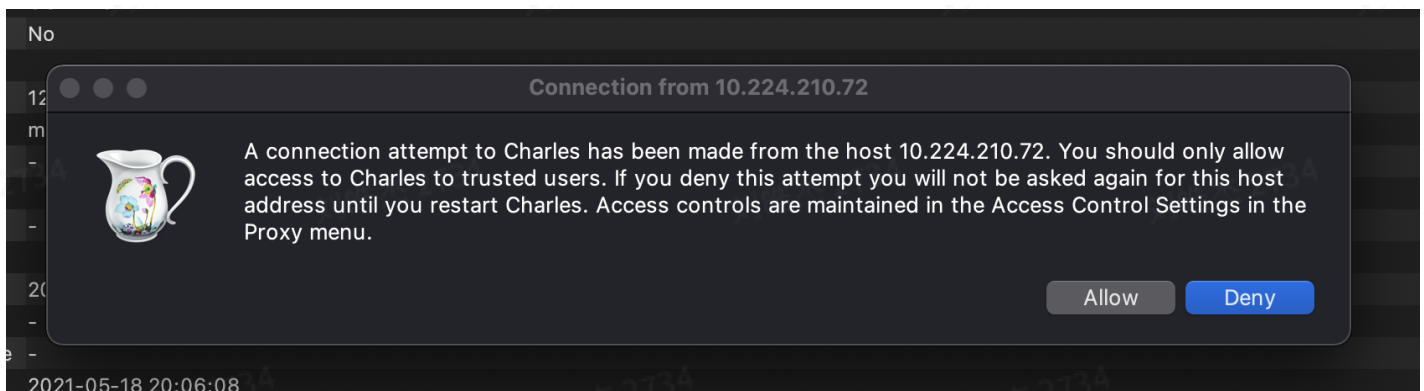
1.1.2 IP和端口

2、设置手机HTTP代理，主机名填上图中的ip部分10.224.206.77，端口也是，此处填8888



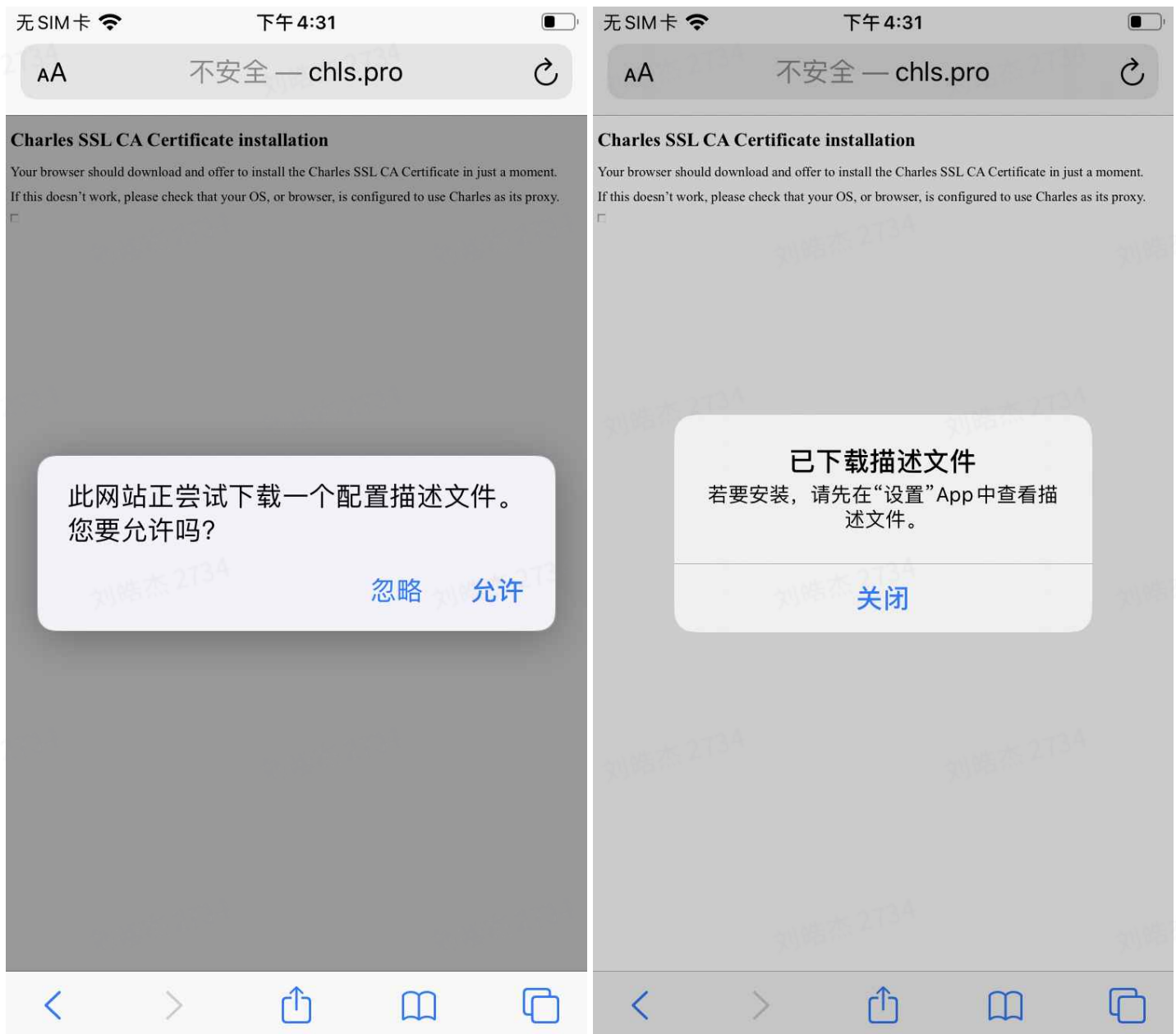
1.1.3 设置代理

3、设置好后随便进行一次网络请求，Charles会弹出提示框，点击Allow



1.1.4 允许代理

4、打开Safari浏览器，输入地址: chls.pro/ssl，在弹窗中点击允许，下载证书

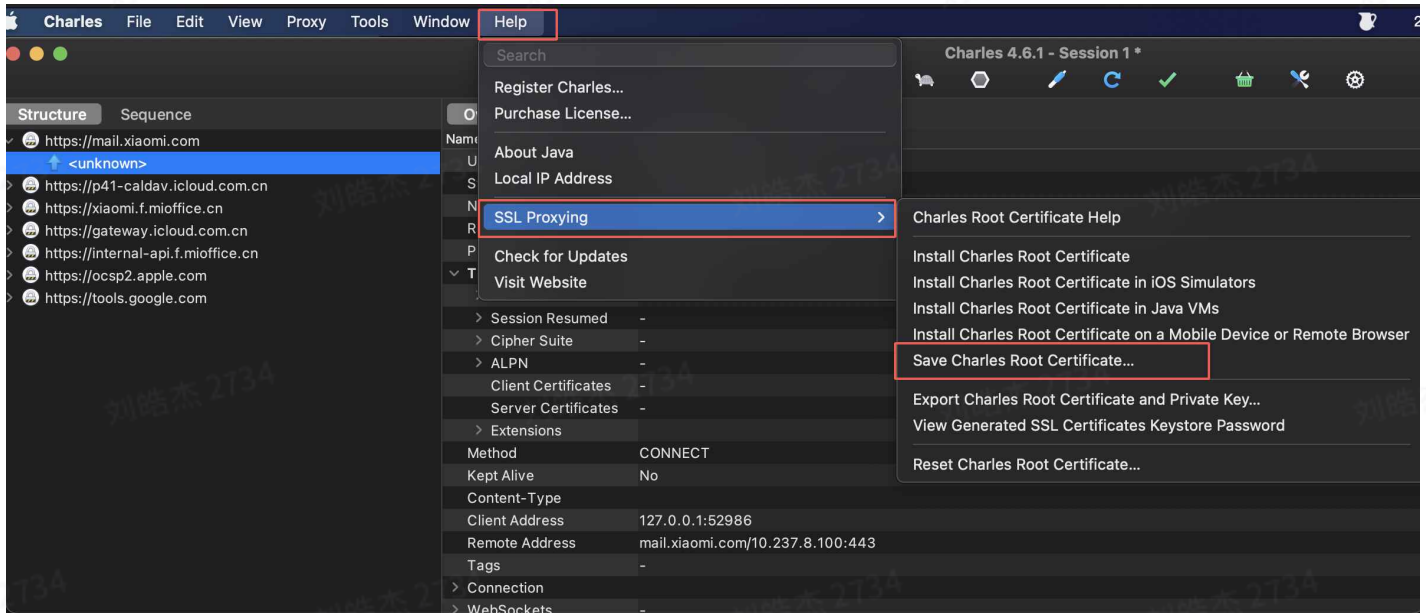


1.1.5 下载证书

二、电脑传输证书

使用Mac的 **隔空投送** 传递证书给iPhone

1、下载证书到Mac本地， 打开Charles， Help->SSL Proxying->Save Charles Root Certificate...



1.2.1 保存证书

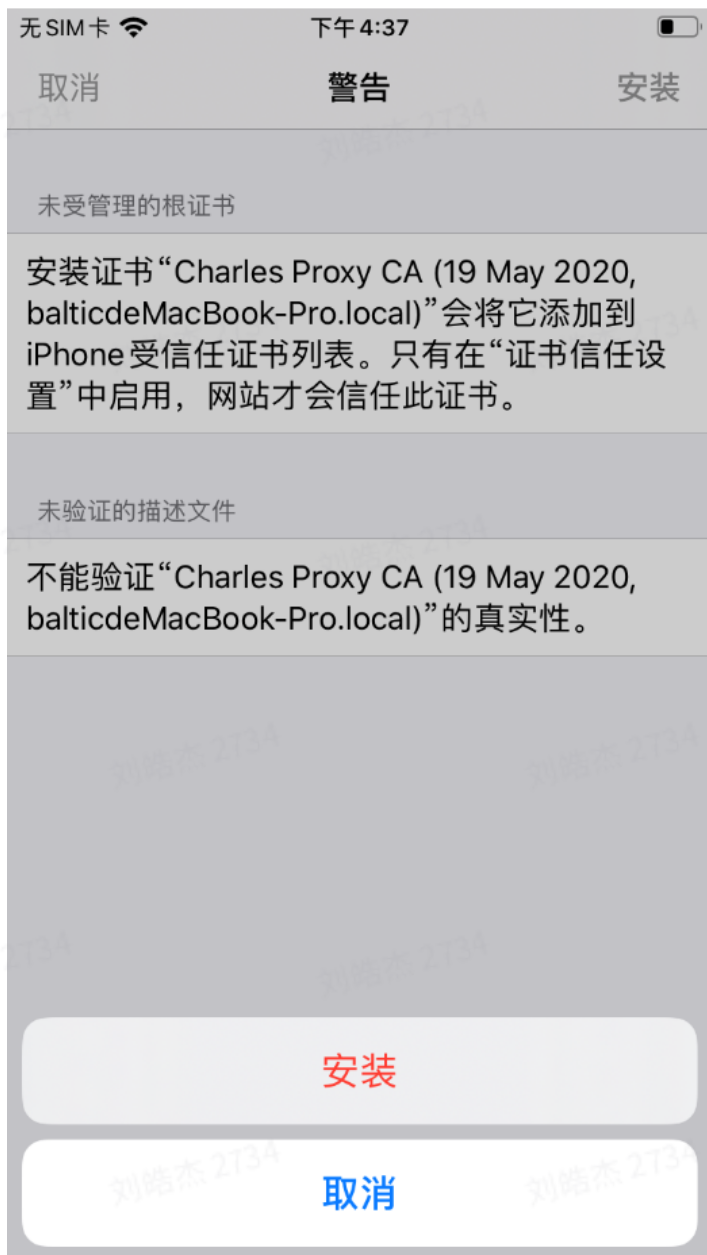
2、打开Mac和iPhone的**隔空投送**，将下载到Mac本地的证书传递给iPhone

2、信任证书

如1.1.2弹窗所示，在iOS在系统版本高于10的机型上，需要在 **设置->通用->关于本机->证书信任设置** 中信任证书

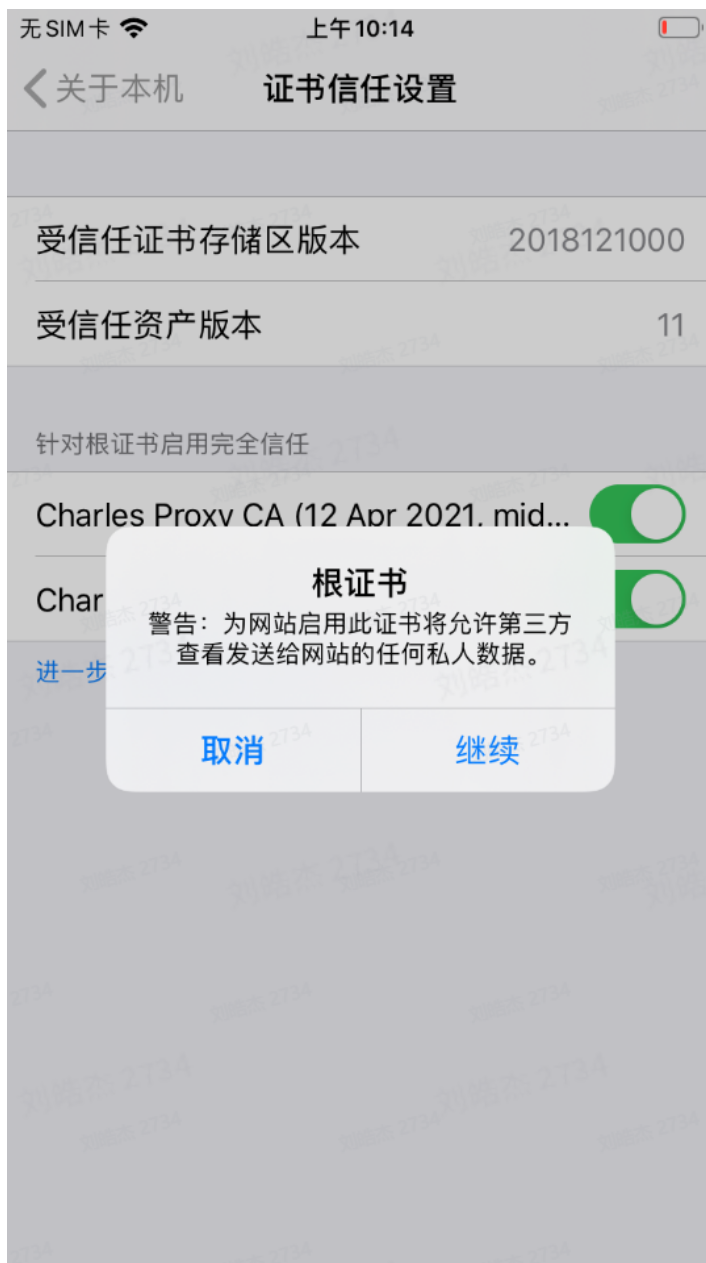
首先安装证书，在**设置->通用->描述文件与设备管理** 中





2.1 安装证书

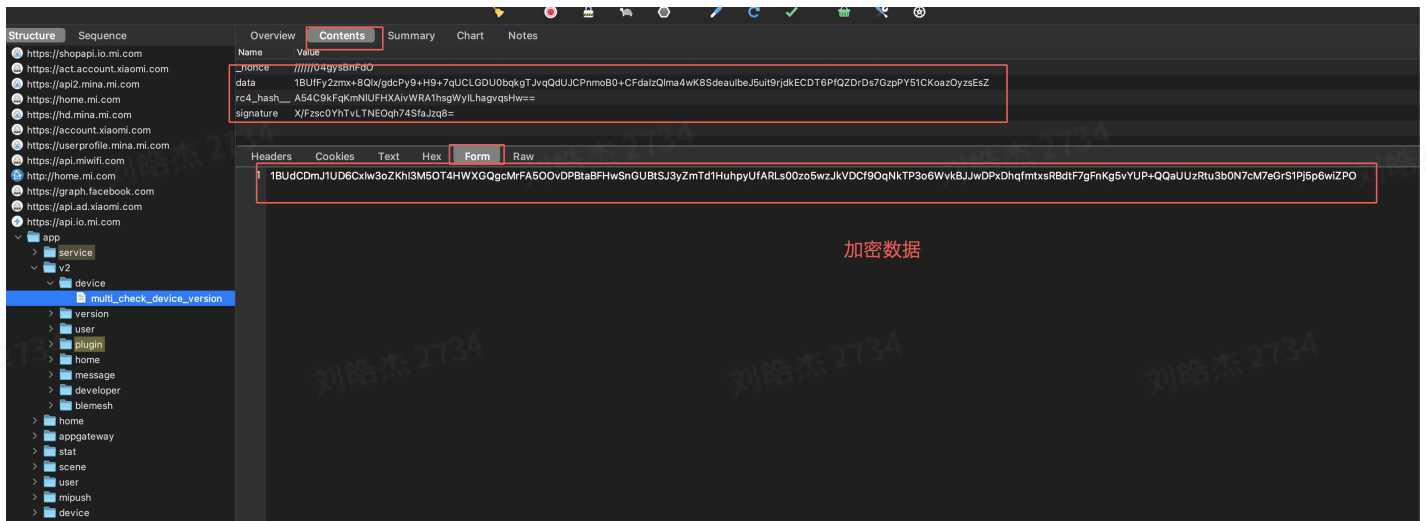
信任证书，找到设置->通用->关于本机->证书信任设置 打开证书的开关，点击继续即可



2.2 信任证书

3、打开抓包开关

经过上述步骤就已经可以在Charles上看到米家APP传输的数据了，不过是APP加密后的数据，要看到明文数据还得在APP中打开抓包模式。



3.1 加密后的数据

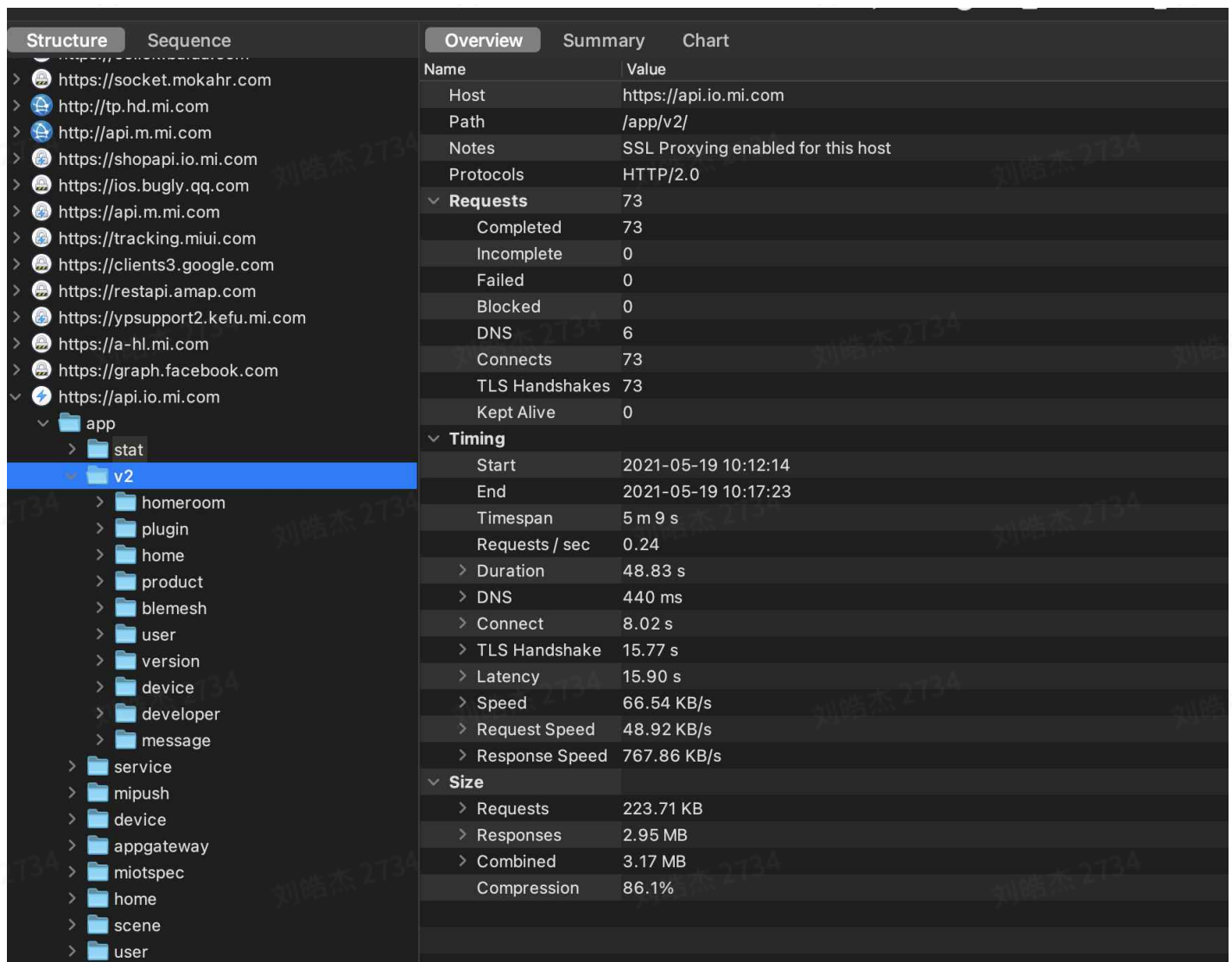
iOS米家APP抓包需要在<http://d.7short.com/mijiadevelopment> (密码:keliyuan)下载DB包，登录开发者账号，在“我的”->“开发者选项”->“开发者模式”->“其他设置”中打开“是否开启抓包模式”即可。



3.2 打开抓包模式

打开开关后在某些情况下可能还是无法看到明文数据，退出APP重进一次即可。

米家APP的所有网络请求都在<https://api.io.mi.com/app>下，其中插件请求的接口大部分都在v2下。



3.3 常见接口

Charles中选中某个接口，右边窗口选择Content->Form，就能看到这个接口的数据请求与返回。

