

米家Android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/>
此次教程以小米9为例进行教学，操作系统为Windwos 10
抓包前确保手机和电脑处于同一局域网下

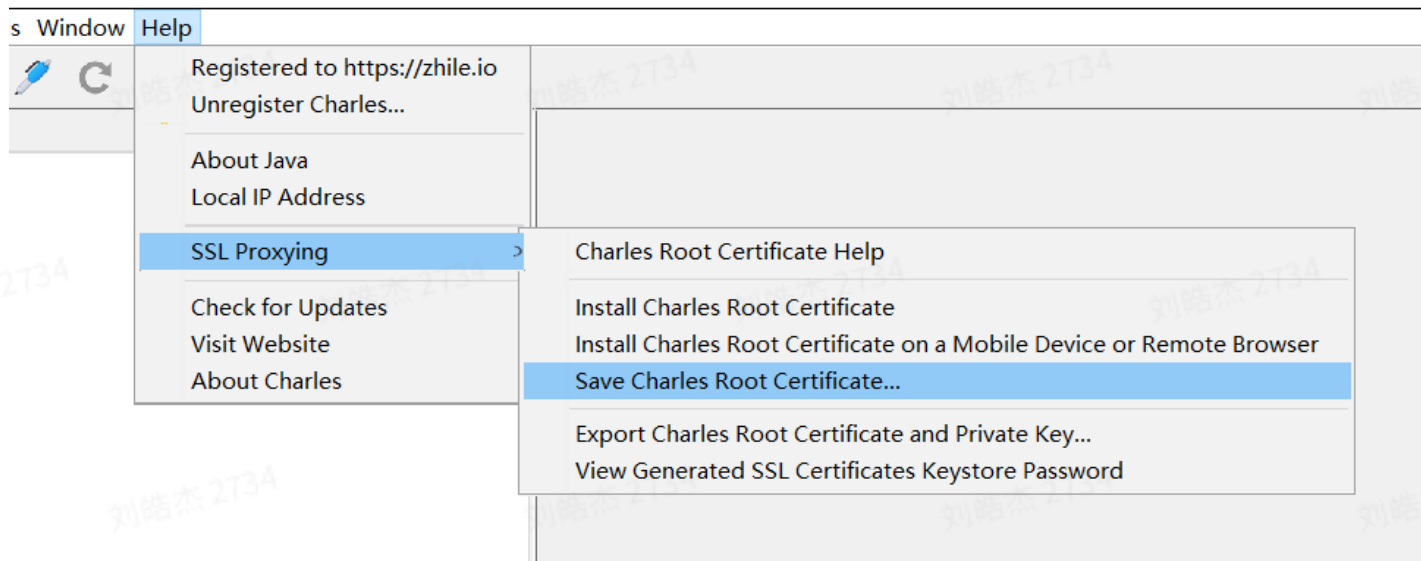
1、下载证书

打开Charles，下载证书有两种方式

一、电脑传输证书

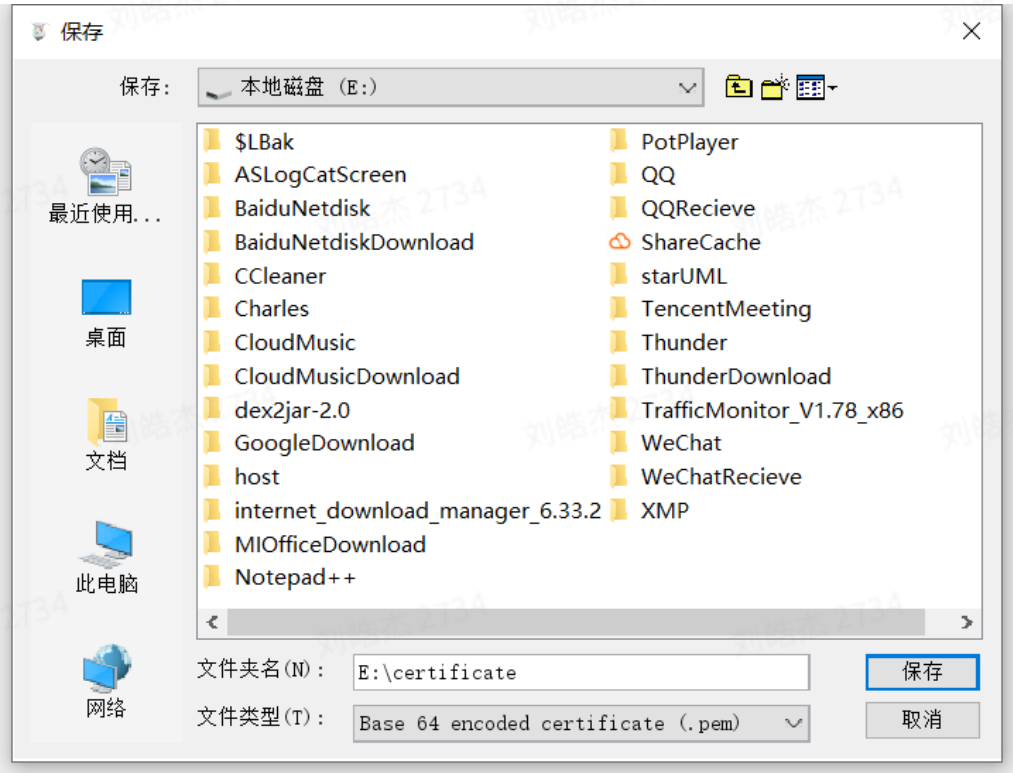
Android上优先建议使用这种方法下载证书，因为使用浏览器下载证书时有时会出现输入chls.pro/ssl后迟迟不会出现下载提示框或者证书下载失败的情况，这是手机操作系统或浏览器或Charles决定的，这时可以直接在电脑上把证书传输给手机

Help->SSL Proxying->Save Charles Root Certificate...



1.1.1 保存证书到本地

选择存储路径



1.1.2 选择路径

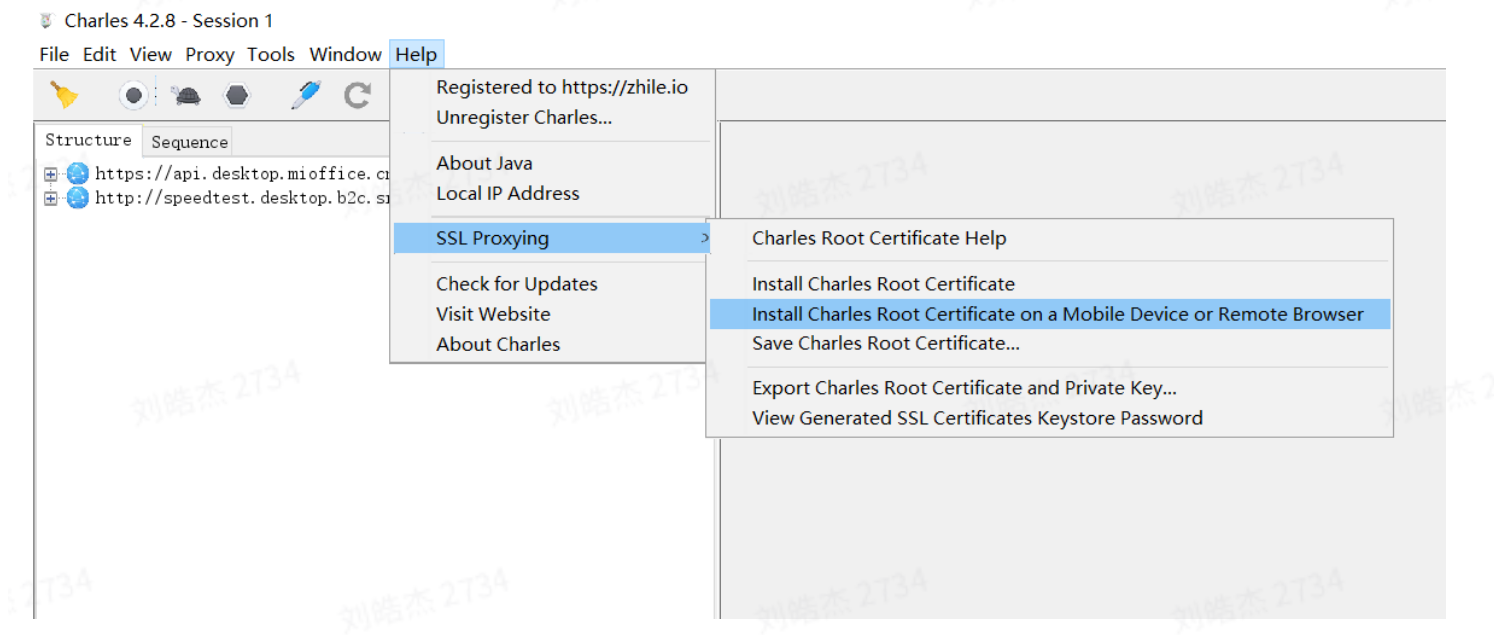
文件夹	2020/7/9 14:37	文件夹	
文件夹	2021/2/3 9:35	文件夹	
certificate.pem	2021/5/11 19:01	PEM 文件	2 KB
IDM 6.33.2.zip	2021/1/29 14:49	ZIP 压缩文件	13,200 KB
jd-gui.exe	2019/6/16 12:32	应用程序	1,487 KB
SmartHome_Dev_63906_6.5.600_de...	2021/4/29 13:17	APK 文件	108,516 KB

1.1.3 证书

将证书手动传输到手机即可。

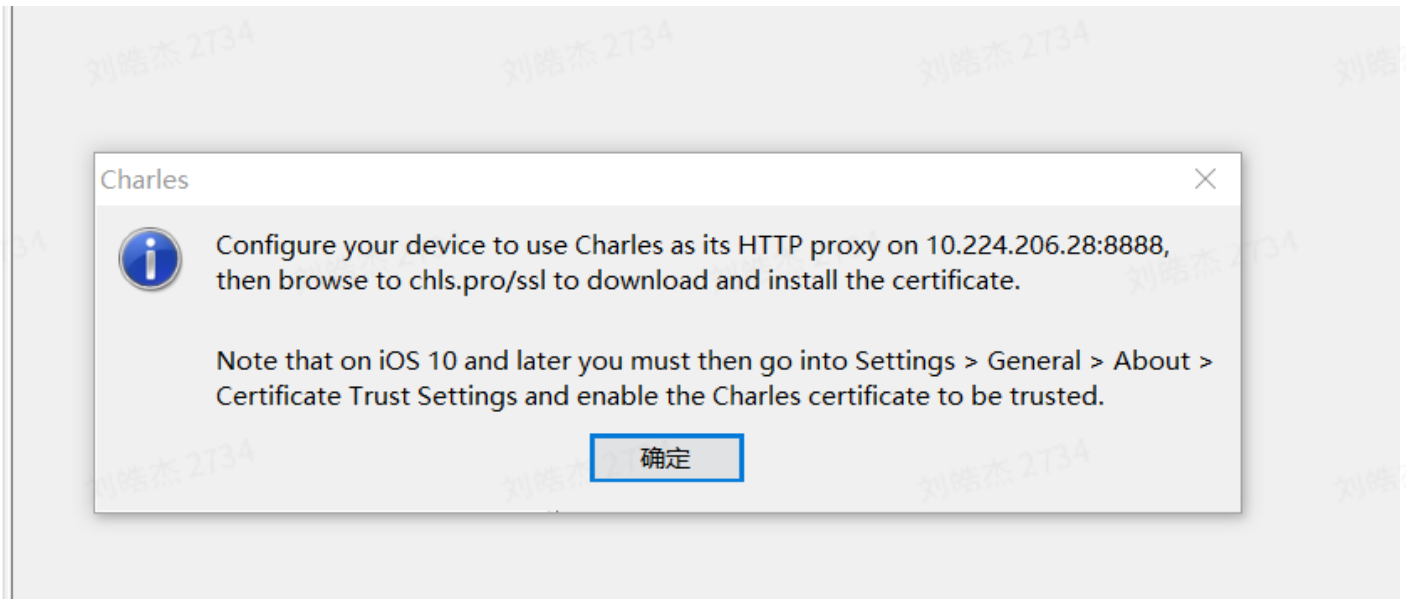
二、手机浏览器下载证书

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



1.2.1 下载证书

会弹出如下窗口



1.2.2 IP和端口

2、设置手机Wifi代理，主机名填上图中的ip部分10.224.206.28，端口也是，此处填8888。

17:23

蓝牙 信号 42%

×

MIOffice-5G 网络详情

✓

安全性

WPA/WPA2/
WPA3-Enterprise

IP 地址

10.224.205.112

子网掩码

255.255.255.0

路由器

10.224.205.254

代理

手动

主机名

10.224.206.28

端口

8888

不使用网址

example.com,mycomp.t...

IP 设置

DHCP

隐私

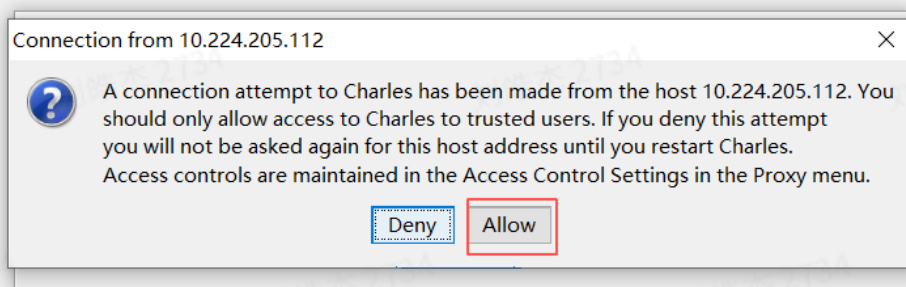
使用设备 MAC

修改密码

删除网络

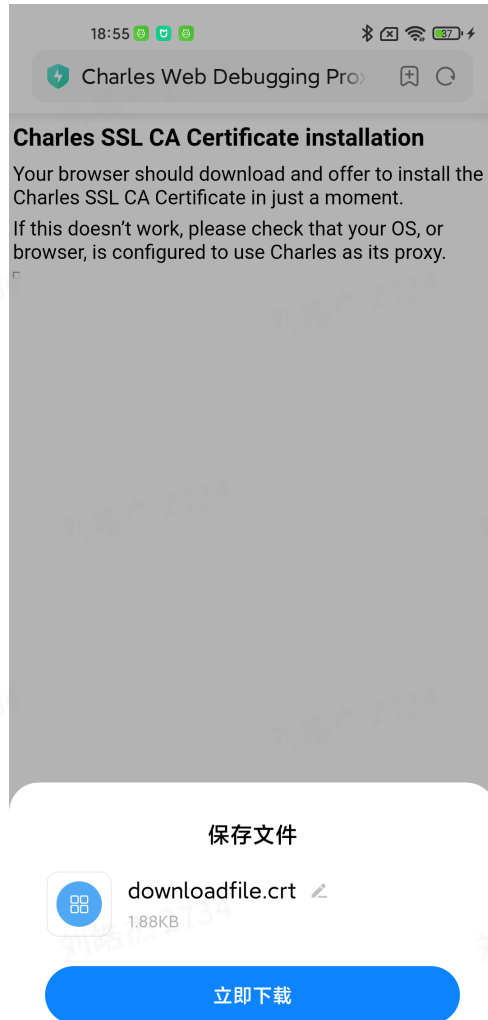
1.2.3 设置wifi代理

设置好随便进行一次网络请求，后Charles会弹出提示框，点击Allow。



1.2.4 允许代理

3、打开手机浏览器，输入地址: chls.pro/ssl，下载证书。



1.2.5 下载证书

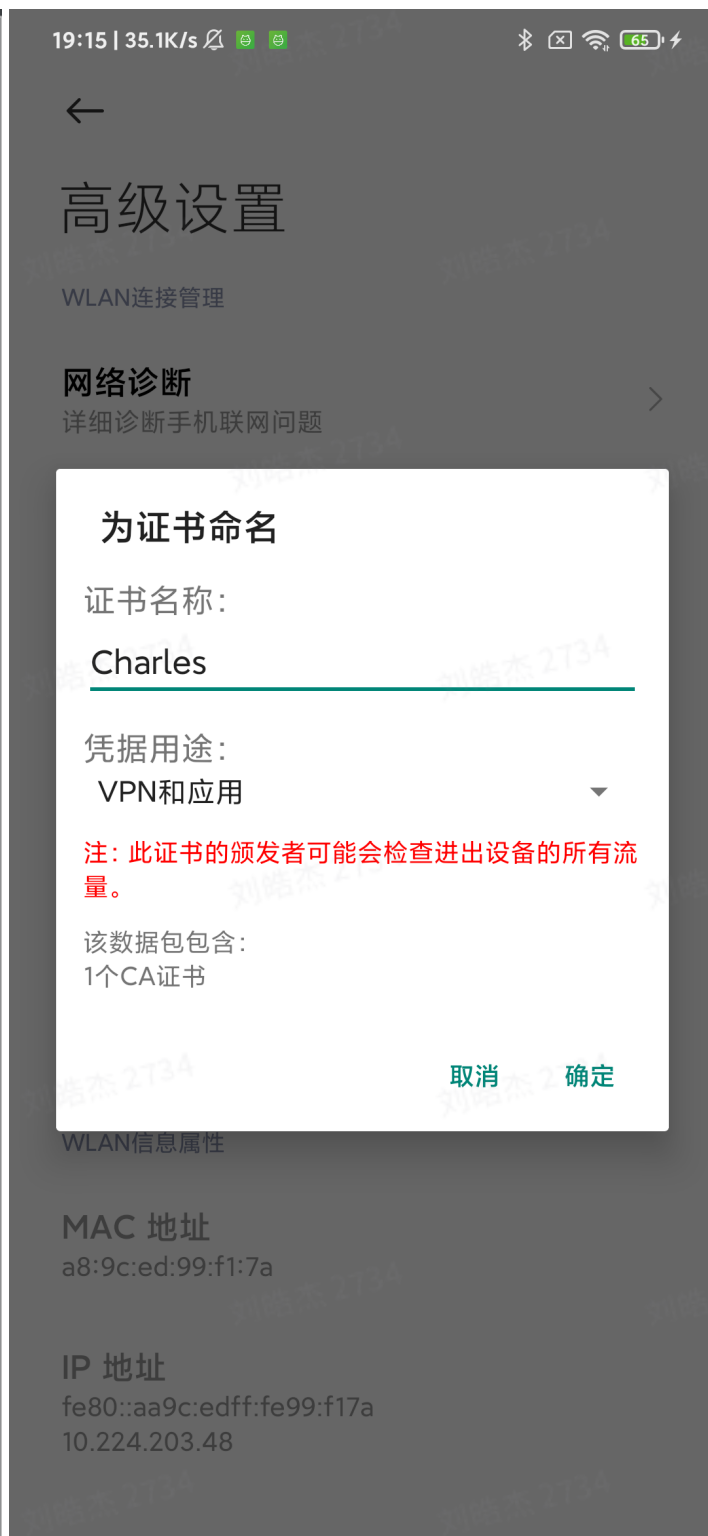
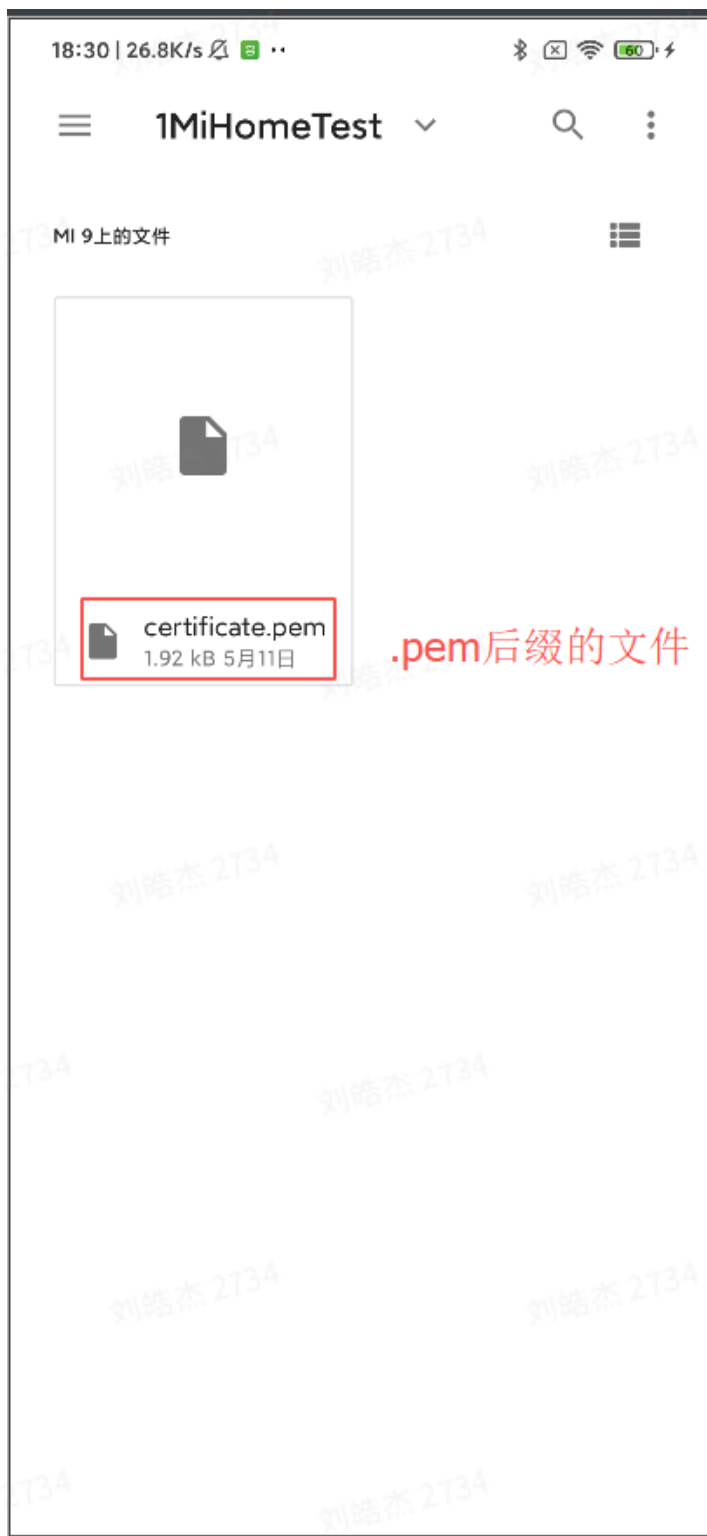
2、安装证书

进入手机设置->WLAN->高级设置->安装证书，找到下载好的证书并命名安装。



2.1 WLAN设置->安装证书

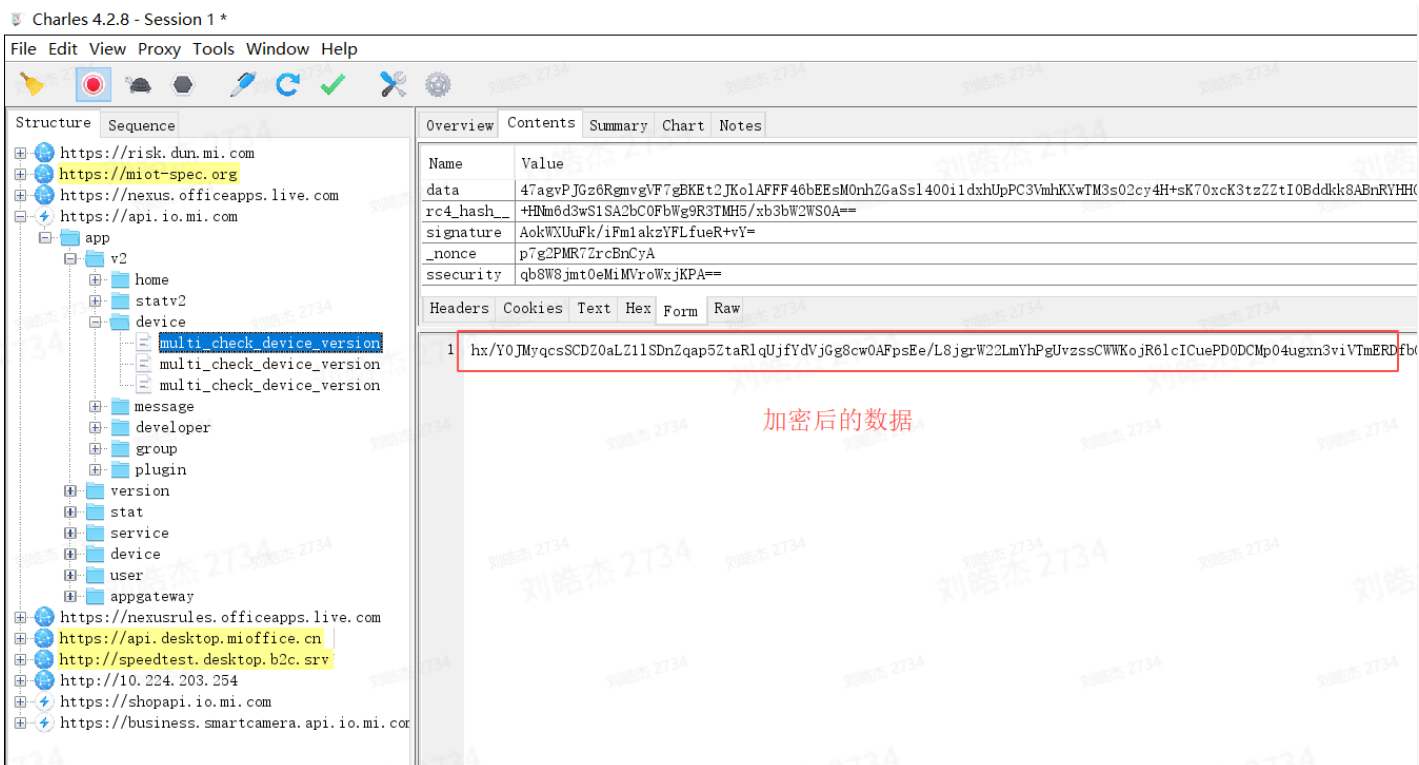
在“凭据用途”这个选项，选择"VPN和应用"即可。



2.2 安装证书

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中打开明文传输开关。



3.1 加密后的数据

Android米家APP需要使用在firm上下载的APP<http://d.7short.com/MiHomeForAndroid>(密码:keliyuan)

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“是否强制使用明文传输数据”即可。



3.2 开启抓包模式

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。

The screenshot shows the Charles Proxy interface. The Structure pane on the left displays a tree view of intercepted requests. The Overview pane on the right shows statistics for the selected request.

Structure Pane:

- https://api.desktop.mioffice.cn
- http://speedtest.desktop.b2c.srv
- https://api.io.mi.com (Selected)
- app
 - service
 - v2
 - homeroom
 - product
 - room
 - user
 - home
 - group
 - router
 - message
 - aiot
 - device
 - statv2
 - plugin
 - scene
 - device
 - stat
 - user
 - appgateway
 - miotspec
 - mipush
- https://business.smartcamera.api.io.mi.com
- https://miot-spec.org
- https://risk.dun.mi.com
- https://internal-api-space.f.mioffice.cn
- https://internal-api.f.mioffice.cn
- https://array601.prod.do.dsp.mp.microsoft.com
- https://geo.prod.do.dsp.mp.microsoft.com
- https://kv601.prod.do.dsp.mp.microsoft.com
- https://account.xiaomi.com
- https://api.account.xiaomi.com
- https://shopapi.io.mi.com
- https://trade.m.xiaomiyoupin.com

Overview Pane:

Name	Value
Host	https://api.io.mi.com
Path	/
Notes	SSL Proxying enabled for this host
Protoc...	HTTP/2.0
Requests	55
Comple...	55
Incompl...	0
Failed	0
Blocked	0
DNS	0
Connects	1
TLS Handsha...	1
Kept Al...	54
Timing	
Start	21-5-11 19:32:16
End	21-5-11 19:33:29
Timespan	1 m 13 s
Requests / ...	0.75
Duration	9.05 s
DNS	-
Connect	29 ms
TLS Handsh...	63 ms
Latency	8.90 s
Speed	11.17 KB/s
Request Sp...	644.16 KB/s
Response Sp...	3.91 MB/s
Size	
Requests	28.99 KB
Respon...	72.09 KB
Combined	101.08 KB
Compress...	62.4%

3.3 米家APP的请求地址

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。

Charles 4.2.8 - Session 1 *

File Edit View Proxy Tools Window Help

Structure Sequence

- https://api.desktop.mioffice.cn
- http://speedtest.desktop.b2c.srv|
- https://api.io.mi.com
 - app
 - v2
 - plugin
 - statv2
 - device
 - multi_check_device_version
 - devicerss1?signature=ucvolsZQ/
 - get_atom_rec?signature=0i0ETr8
 - multi_check_device_version
 - scene
 - home
 - developer
 - message
 - group
 - service
 - home
 - mipush
 - device
 - apgateway
 - version
 - user
 - stat
- https://home.mi.com
- https://data.mistat.xiaomi.com
- https://internal-api.f.mioffice.cn
- http://10.224.203.254
- https://shopapi.io.mi.com
- https://business.smartcamera.api.io.mi.com
- https://risk.dun.mi.com
- https://internal-api-space.f.mioffice.cn
- https://xiaomi.f.mioffice.cn

Overview Contents Summary Chart Notes

Name	Value
signature	MF3dk0kgYAXdBuLb70P5UAgMIRE+a6hi/0u0Tws0RJY=
_nonce	FFSskr+JVvQBnCyD
data	{"app_level": "63907", "platform": "android", "check_reqs": [{"did": "338198331", "plugin_level": "18"}]}

请求参数

Headers Cookies Text Hex Form Raw

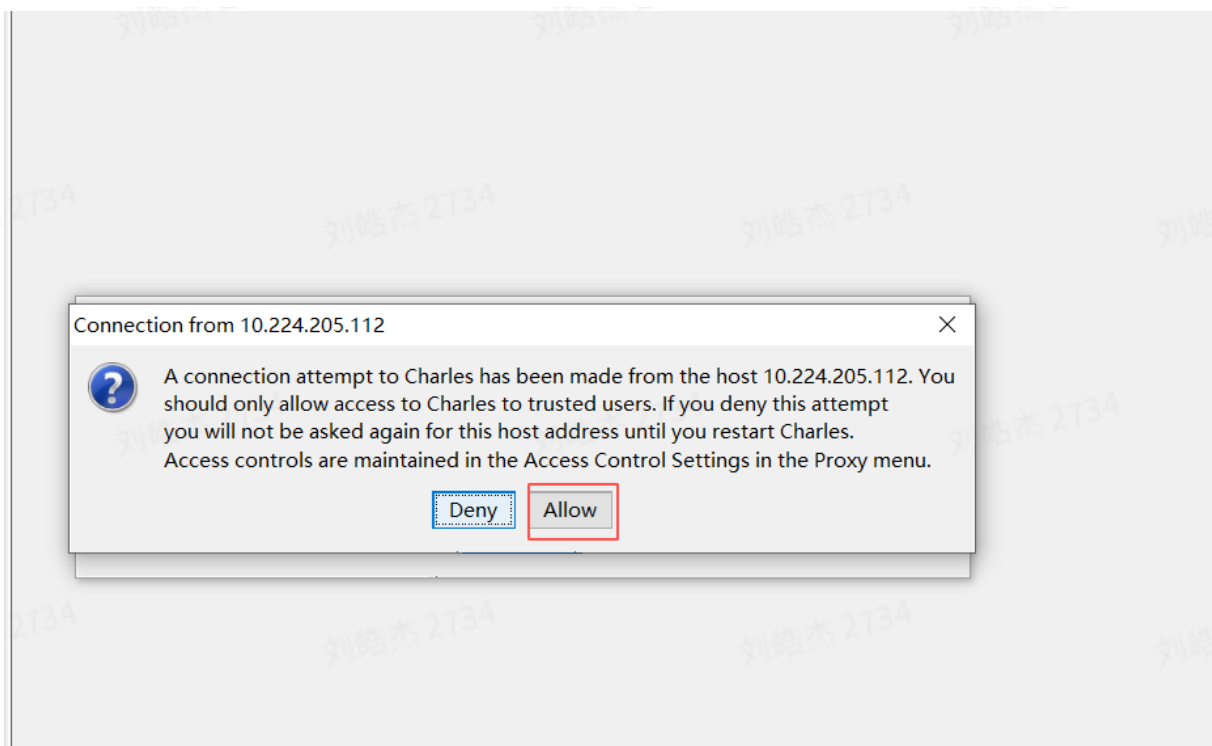
```
{
  "code": 0,
  "message": "ok",
  "result": {
    "auto_upgrade_switch": false,
    "upgrade_notify_switch": true,
    "user_set_switch": true,
    "list": [
      {
        "did": "338198331",
        "updating": false,
        "curr": "2.0.1",
        "latest": "2.0.1",
        "description": "",
        "isLatest": true,
        "ota_progress": 0,
        "ota_status": "idle",
        "ota_failed_code": 0,
        "ota_failed_reason": "",
        "timeout_time": 180,
        "ota_start_time": 0,
        "force": false,
        "rec": false,
        "upload_time": 0
      }
    ]
  }
}
```

服务器返回数据

3.4 明文数据

4、注意事项

- 1、每次抓包前请确保手机设置好了wifi代理。
- 2、当手机设置了代理后电脑端如果关闭了Charles的话手机将无法访问网络。
- 3、每次设置好代理后请看一眼Charles的弹窗，务必点击Allow，否则将无法抓包。



4、Charles一次性记录抓包数据时间过长时，会使APP的网络请求变慢，所以建议经常清理抓包记录和不必要时关闭抓包。

Charles 4.2.8 - Session 1 *

