

手机抓包实验

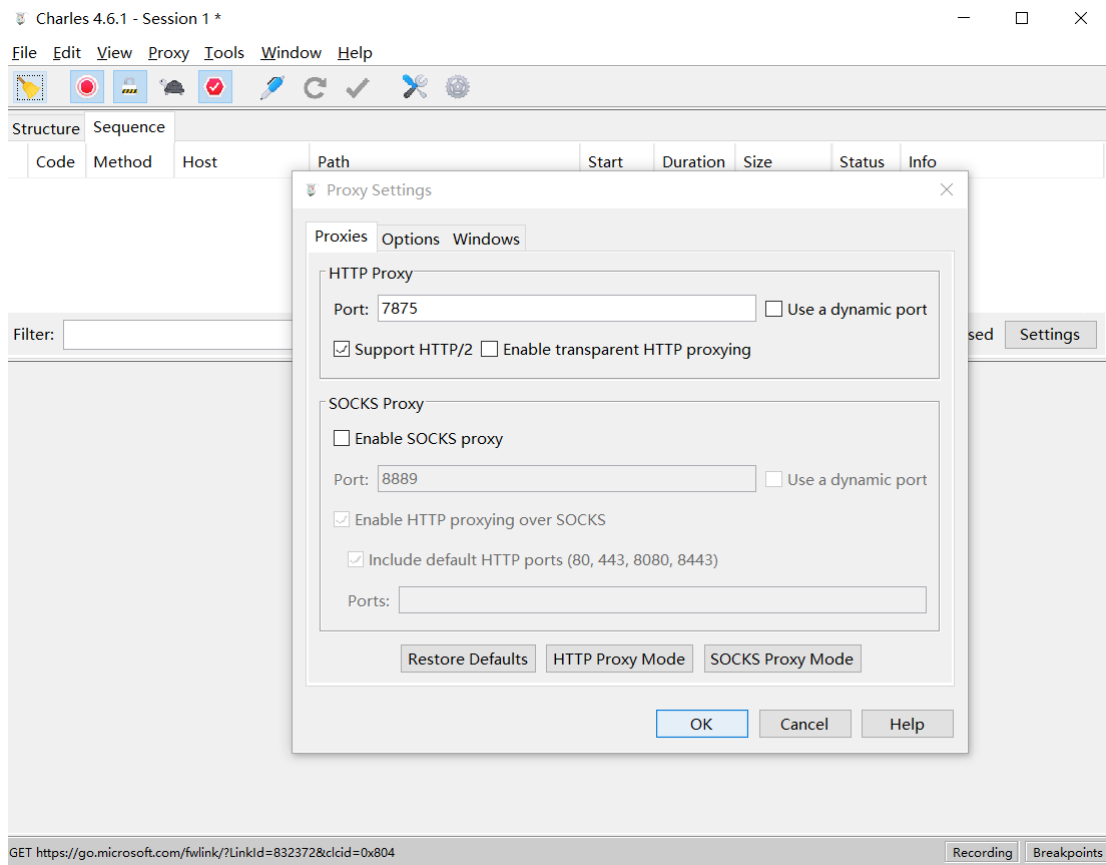
- xiabee

0x00 实验目的

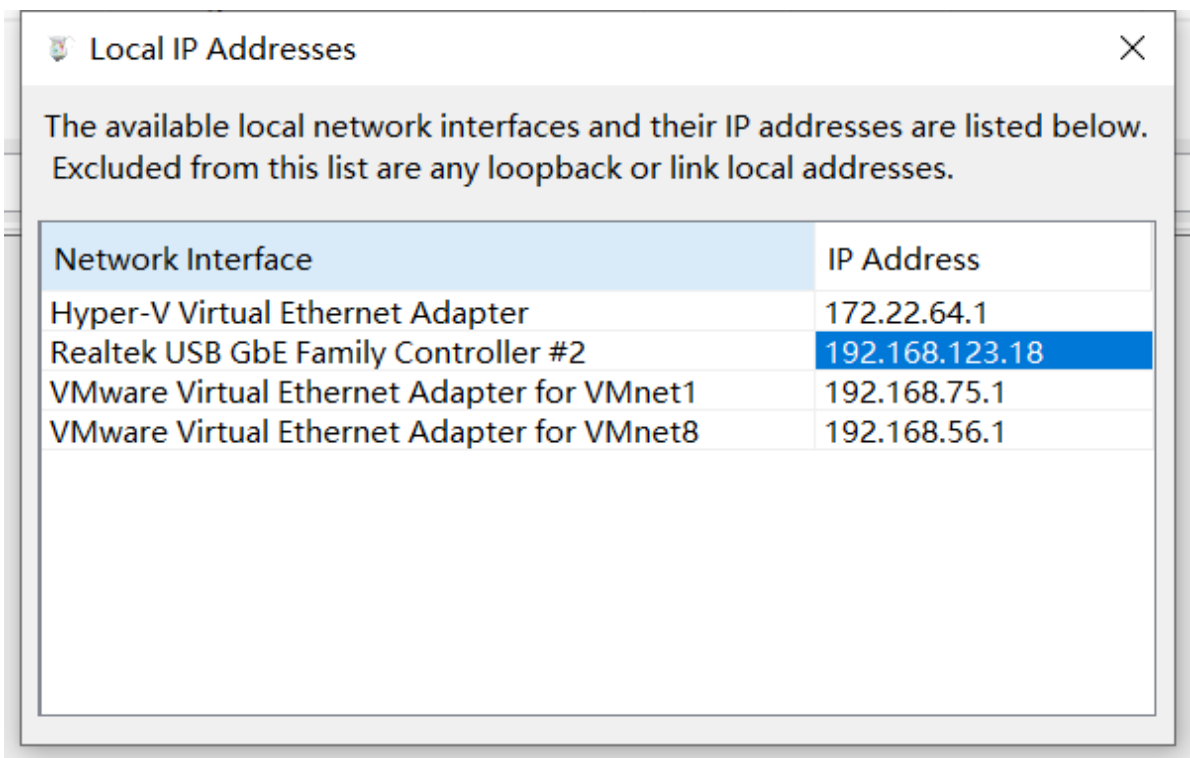
- 学习 Charles 的使用
- 了解手机 APP 的流量结构

0x01 实验过程

- 设置 Charles 代理，并将 SSL 证书装入手机：



- 查看本机 IP：



- 手机连接局域网，设置手机代理：

18:52 0.5KB/s 0.5KB/s 5G Netw...

✕ 连不上网，我很抱歉_5G Netw... ✓

Subnet mask 255.255.255.0

Gateway 192.168.123.1

Proxy Manual >

Hostname 192.168.123.18

Port 7875

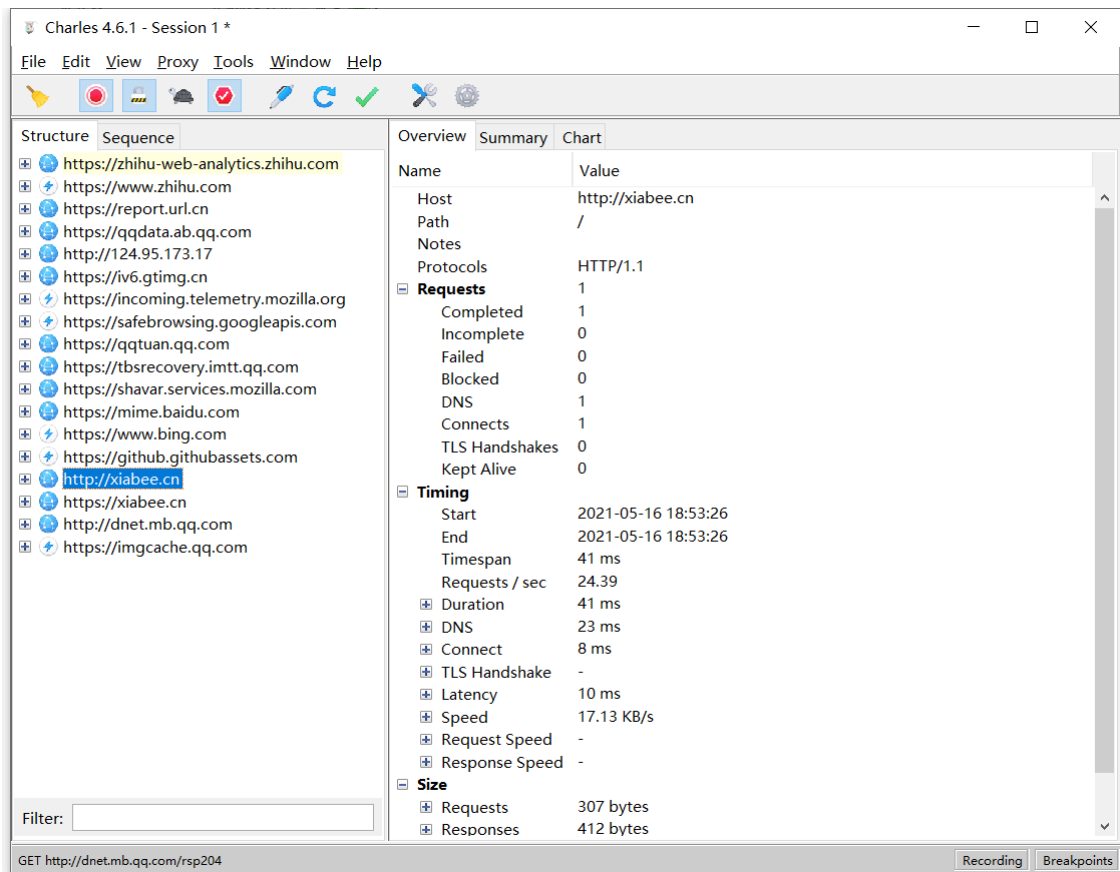
Bypass for example.com,mycomp.test....

IP settings DHCP >

Modify network

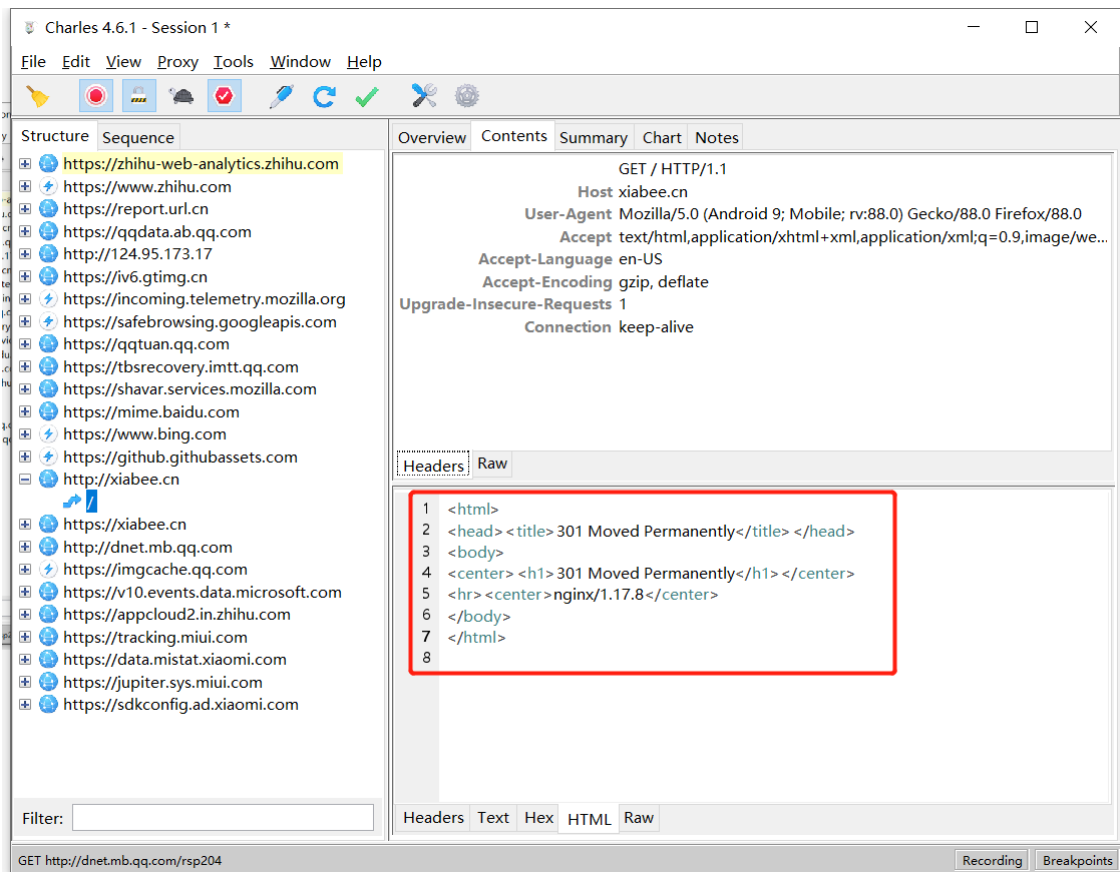
Forget network

- 手机访问网页，观察 Charles 界面：



0x02 实验结果

- 观察浏览器数据流，发现其访问 `http://xiabee.cn`，并进行了 301 跳转



0x03 实验不足

- 由于安卓 7.0 及以上系统不再信任用户证书，手动导入的 SSL 证书并没有生效，故无法解析 https 的流量
- 解决上述问题需要将用户证书安装在根目录，需要 root 权限.....或者使用苹果设备

0x04 实验心得

- https 不是绝对安全的，不要随意安装 SSL 证书