# 渗透测试 APP流量通用抓包方法

朋与厌 洛米唯熊 2019-11-23


毕老师之前开会的时候提起过微信、支付宝、抖音类的App会检测手机的是否挂代理，就是说不能直接在手机代理的地方做手脚，不然就会被检测到 :)


## 0x01 Proxifier代理介绍

### 1.1 **首先介绍下Proxifier：**

**Proxifier**是一款功能非常强大的代理客户端，支持Windows XP/Vista/Win7/Win10 和 MacOS，支持http/https、socks4/5、TCP、UDP等协议，可以指定端口，指定IP，指定域名、指定程序、指定用户名密码授权等运行模式，兼容性非常好，有点类似SOCKSCAP。

有许多网络应用程序不支持通过代理服务器工作，不能用于局域网或防火墙后面。这些会损害公司的隐私和导致很多限制。Proxifier解决了这些问题和所有限制，让您有机会不受任何限制使用你喜爱的软件。此外，它让你获得了额外的网络安全控制，创建代理隧道，并添加使用更多网络功能的权力。

### 1.2 **Proxifier代理流程**

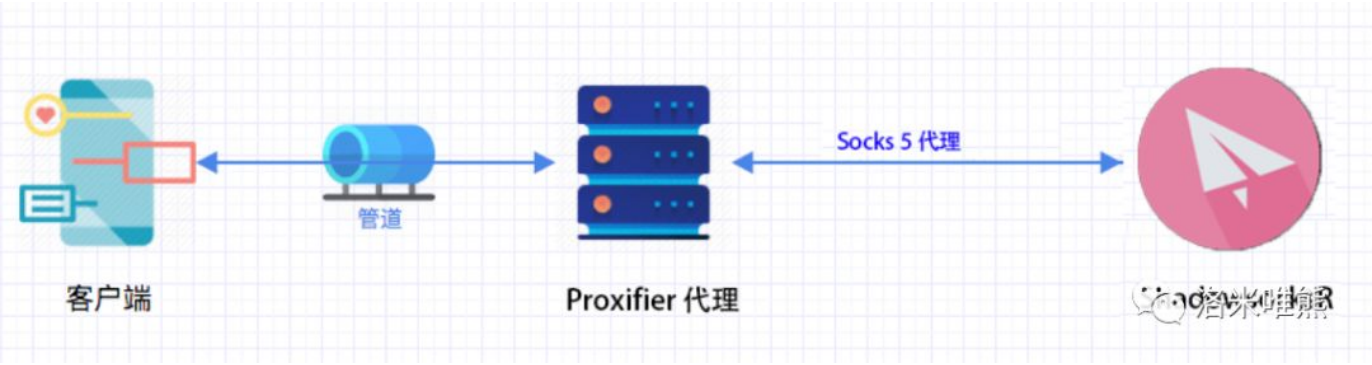
端口转发 | 流量转发

代理流程主要分为两步：

1、添加代理服务器（Socks5）

2、设置代理规则（ 设置需要设置代理 **应用程序**）

这时候应用程序 **所有流量** 经过代理服务器




这样，只要选择需要代理的应用程序，比如chrome.exe，即可实现代理流量转发

**0x02 设立猜想**

梳理了流程之后，一个很骚的思路就从脑子里蹦了出来：

代理到Socks5 流量就全部走 **小飞机** ，也就是说小飞机就是**流量的出口**。

这样就跟浏览器挂代理抓包原理是一样的。

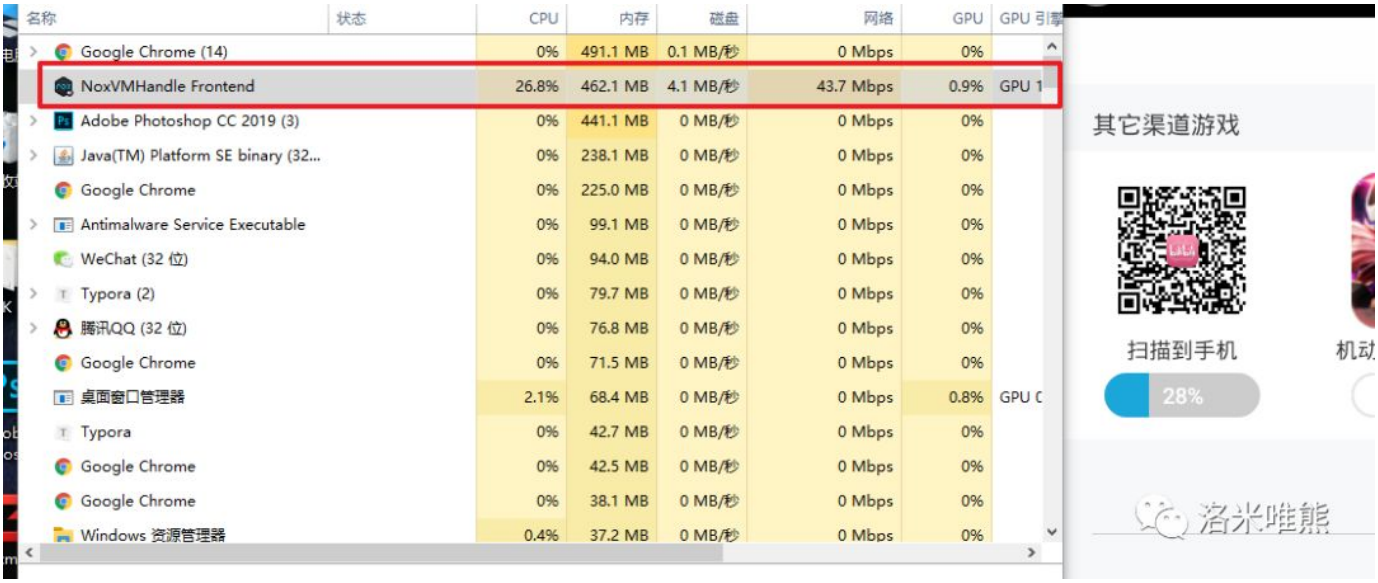
****猜想建立****

1、用代理转发工具将流量出口代理到Burp 8080端口

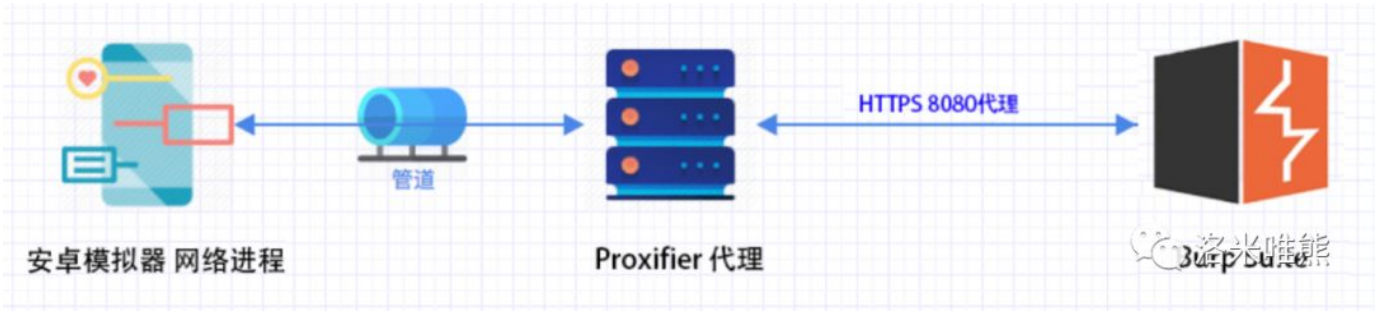
2、注入流量（**模拟器有很多进程，其中有个进程是网络的进程**）

安卓模拟器大多是使用virtualbox的虚拟网卡进行的网络通信，那么，如果直接将模拟器的网络进程的所有流量代理到burpsite即可抓取流量包，同时又绕过了关于客户端的相关校验。

打开模拟器分析网络进程，会发现模拟器使用的网络进程有：
`**virtualbox headless fronrend**`和`**NoxVMHandle Frontend**`。



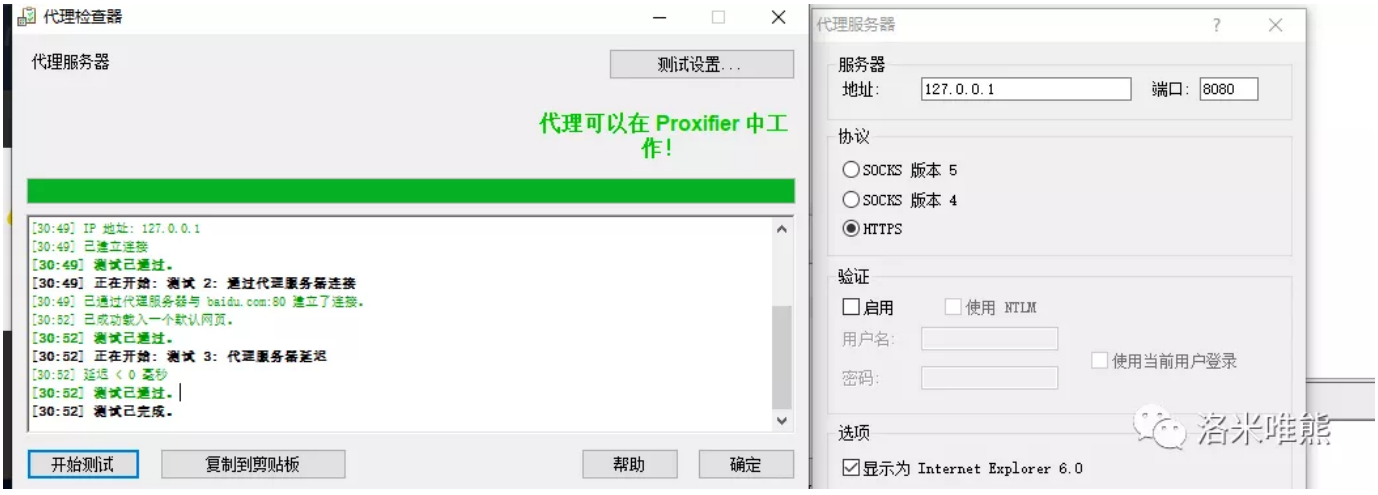

**总体流程图如下：**




*****验证猜想*****

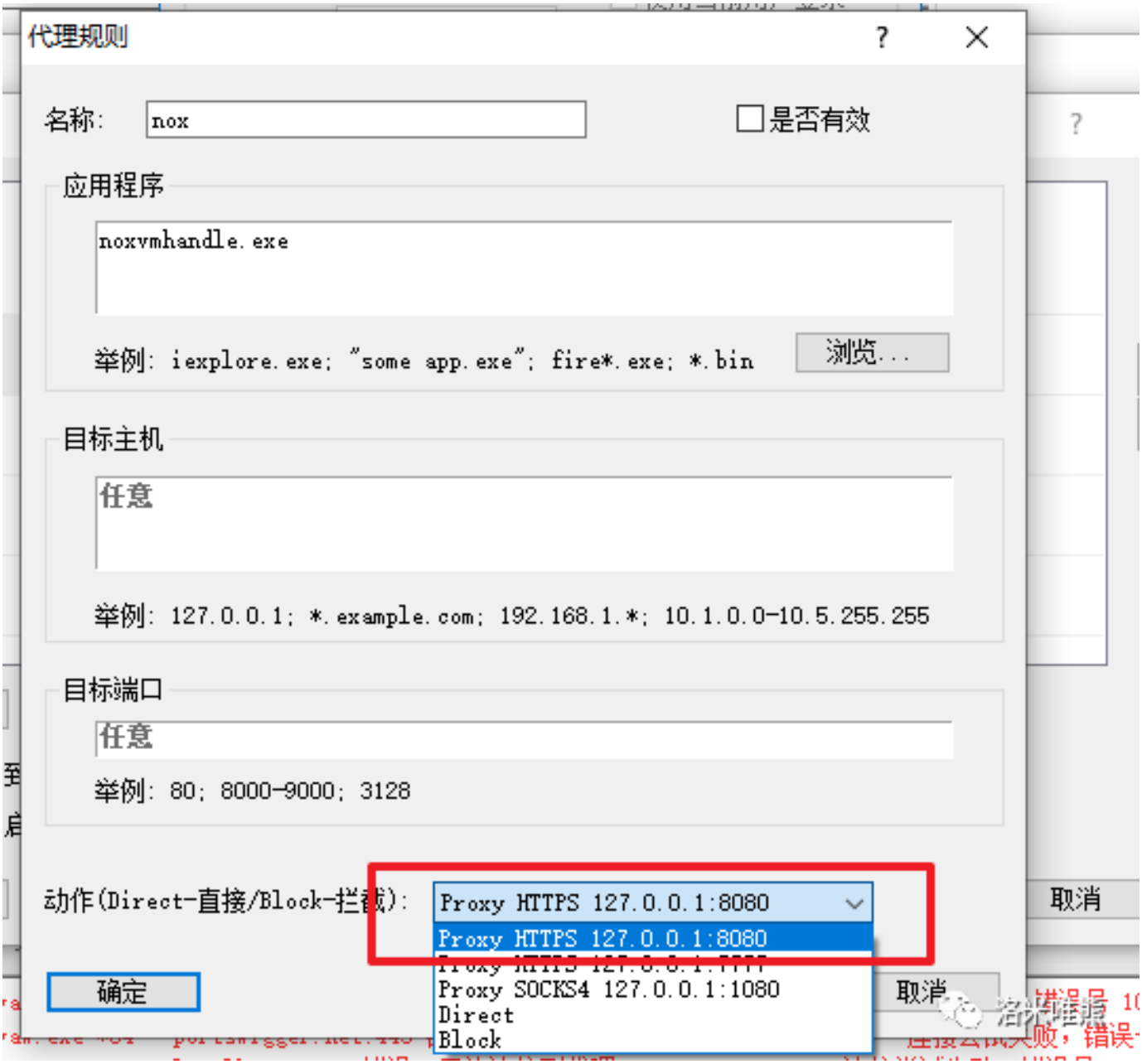
## 2.1 设置Proxifier代理服务器

代理服务器设置为burp监听端口。




## 2.2 设置代理规则

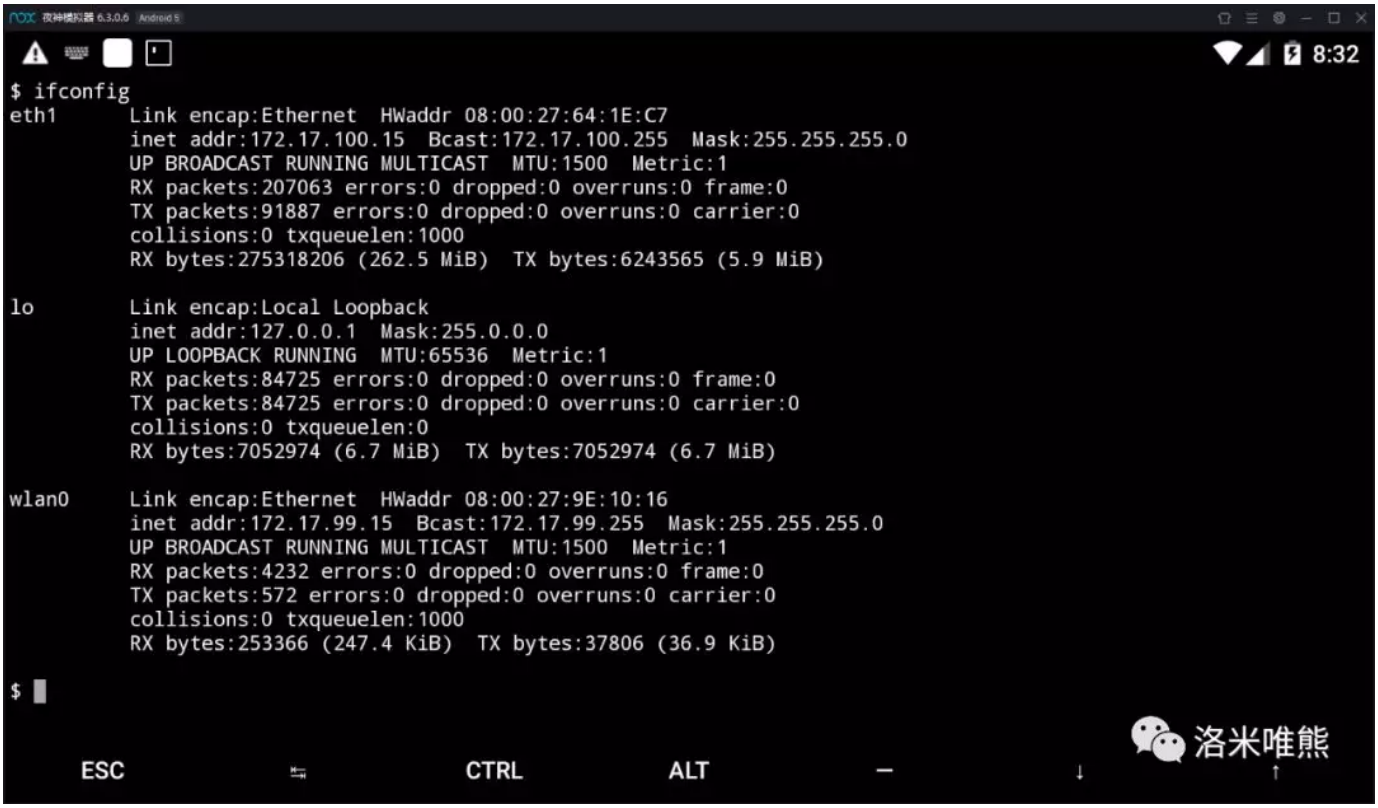
将`NoxVMHandle Frontend`进程对应的应用程序文件加入代理规则。




### 2.3 安装证书

这里不再详细讲。

虚拟机都是用的虚拟网卡 不能直接访问到宿主机

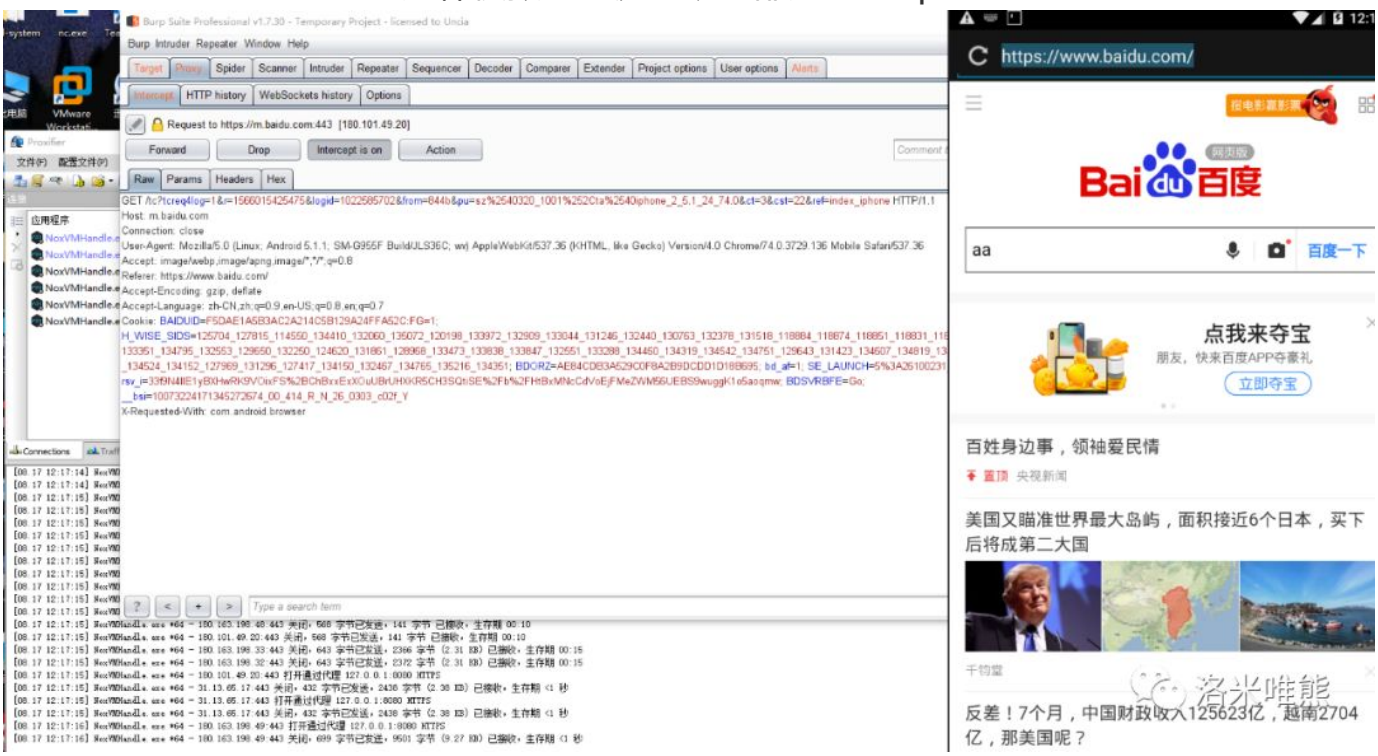



将Burp的CA证书文件复制到模拟器安装就可以了

## 2.4 抓取流量包

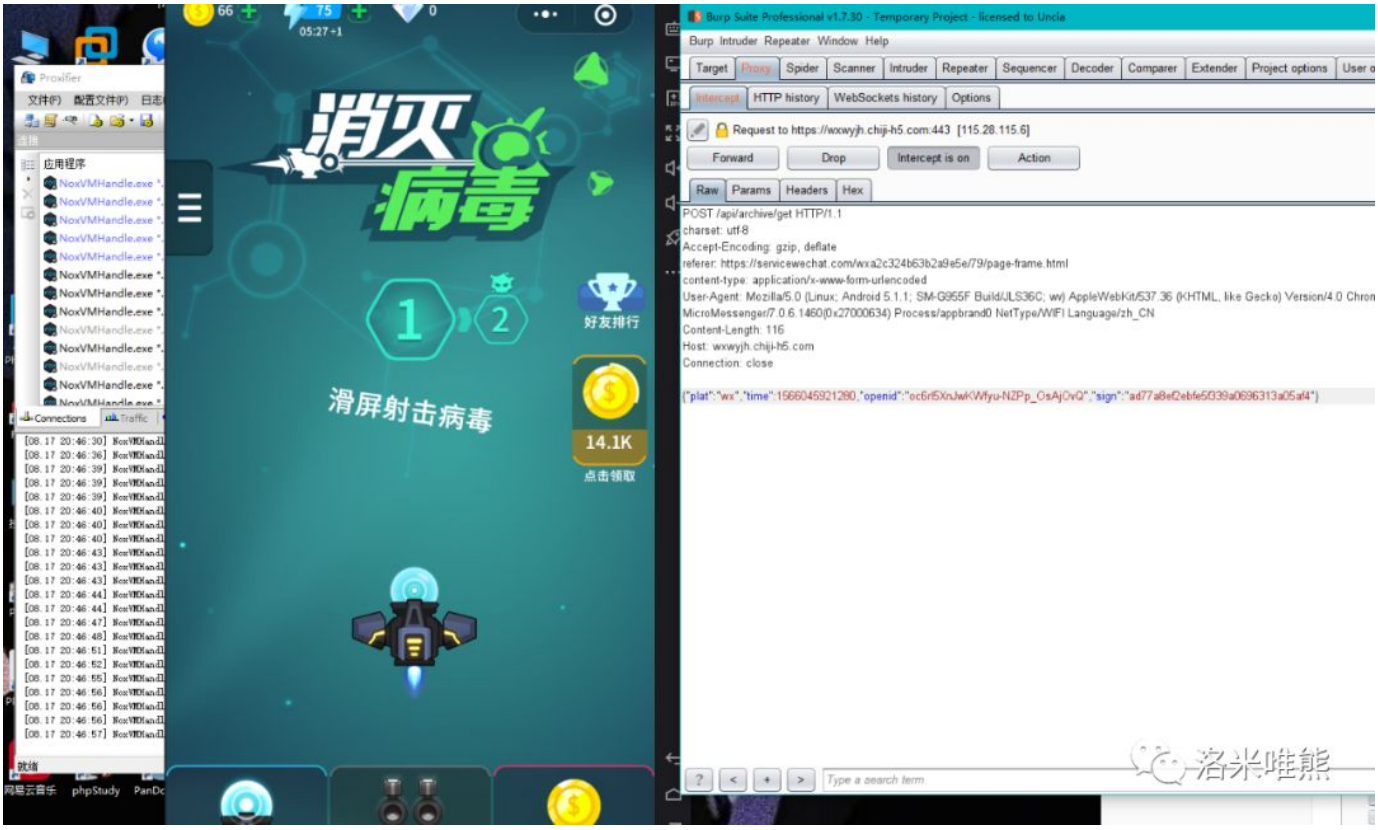
配置之后，即可在proxifier中获取到模拟器内对应app的流量

这样模拟器的流量就全部走向Burp了



## 实现

微信登录数据包


## 完毕收工


这有一个
很可爱的公众号
关注它吧
洛米唯熊