# 背景

近期测试项目的时候拿到PC客户端程序即.exe文件，测试需要抓取数据包，在此介绍一下PC客户端的抓包方法。

# 工具

PC客户端程序抓包需要两个工具结合，一个是Fiddler，另一个是Proxifier，Fiddler大家比较熟悉就不详细讲了，看下另一个Proxifier；

Proxifier是一款功能非常强大的socks5客户端，可以让不支持通过代理服务器工作的网络程序能通过HTTPS或SOCKS代理或代理链。

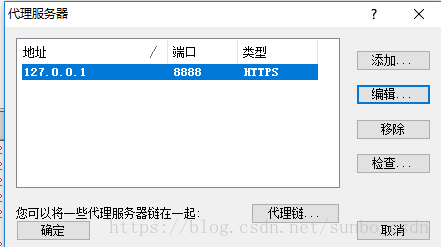
由于一般的C/S客户端不能设置代理，所以我们FIddler检测不到数据，我们可以通过Proxifer来实现把所有的请求抓发给Fiddler，这样我们就可以在Fiddler分析客户端请求。

具体安装就不讲了，直接百度可以搜到Proxifier工具。

设置很简单，下图所示，两步就OK

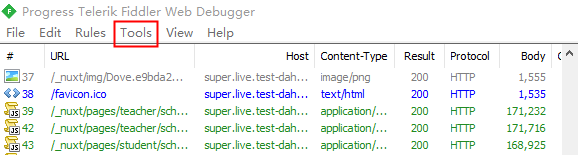


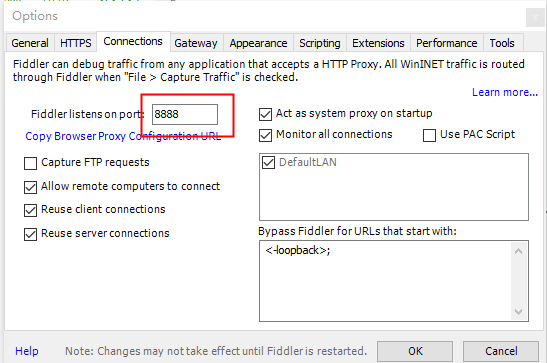
a).设置代理服务器和Fiddler代理设置匹配



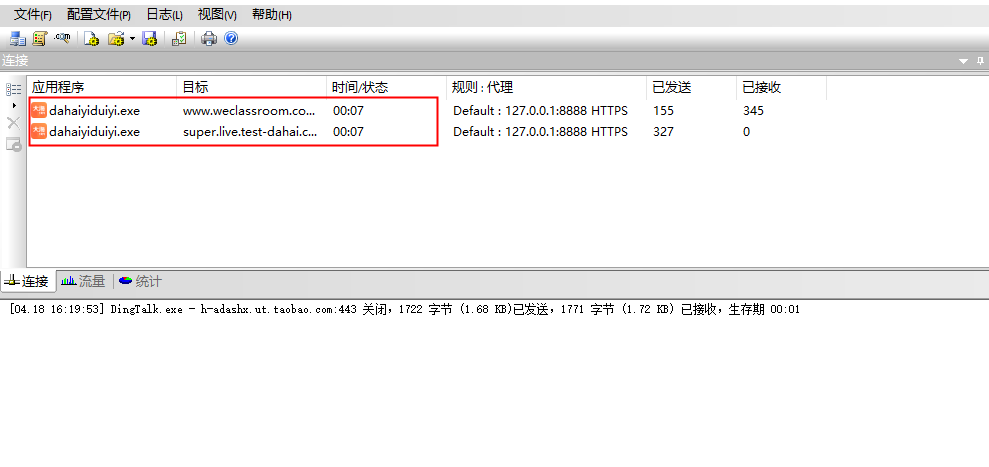
b).Fiddler代理设置为；

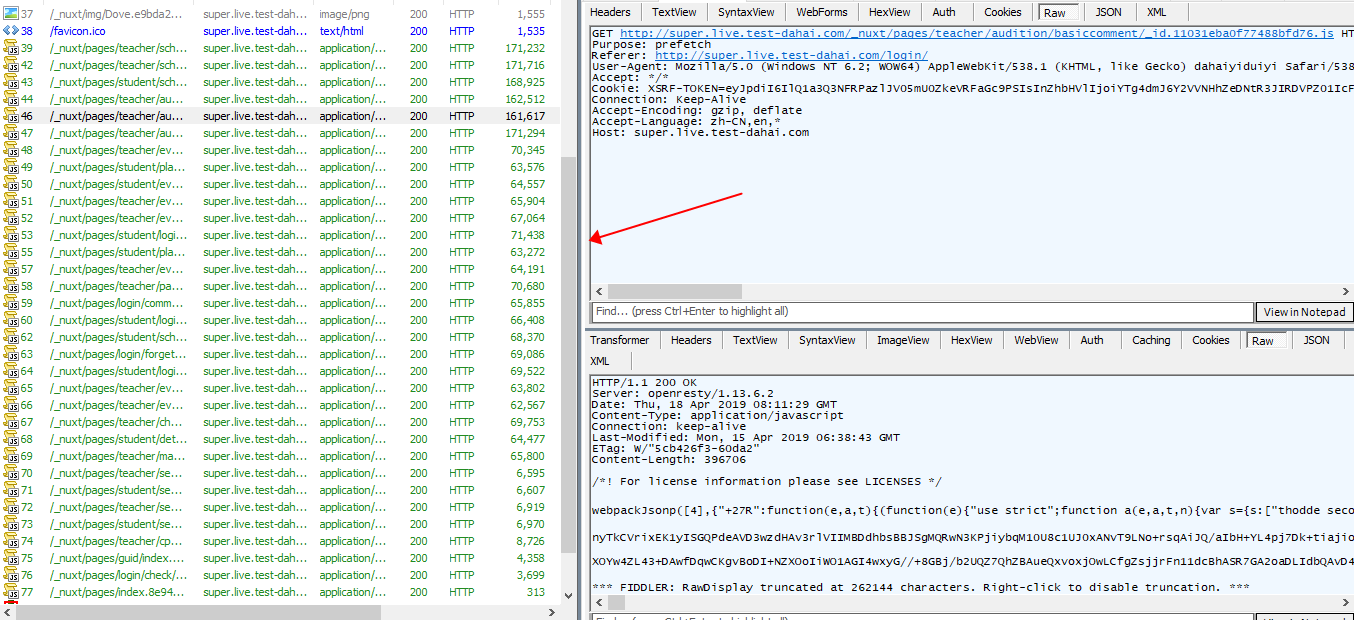
Tools—Options；



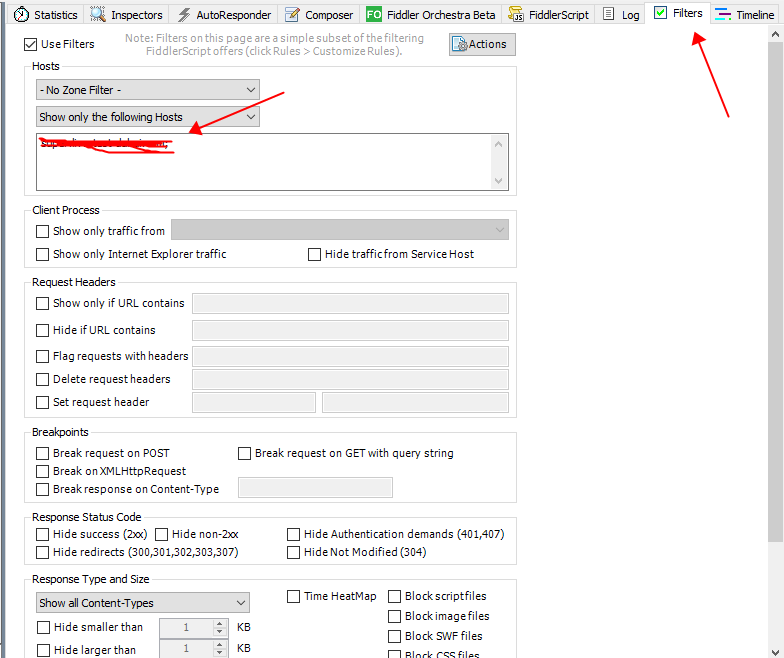


这里设置的端口和Proxifier一样就可以了，到这里就设置完毕了，我们可以打开客户端程序，在Fiddler和Proxifer看下数据；

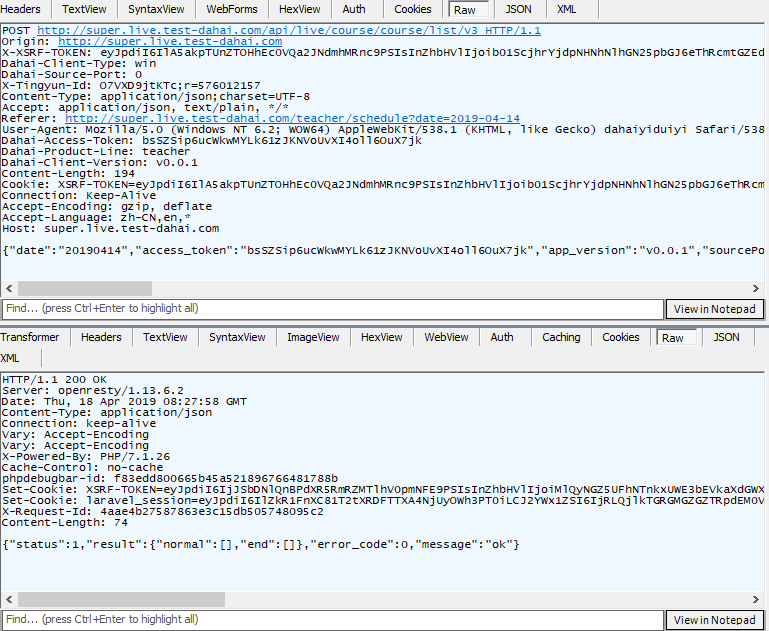




抓取的时候可以在Fiddler白名单域名设置我们只需要抓取的程序；

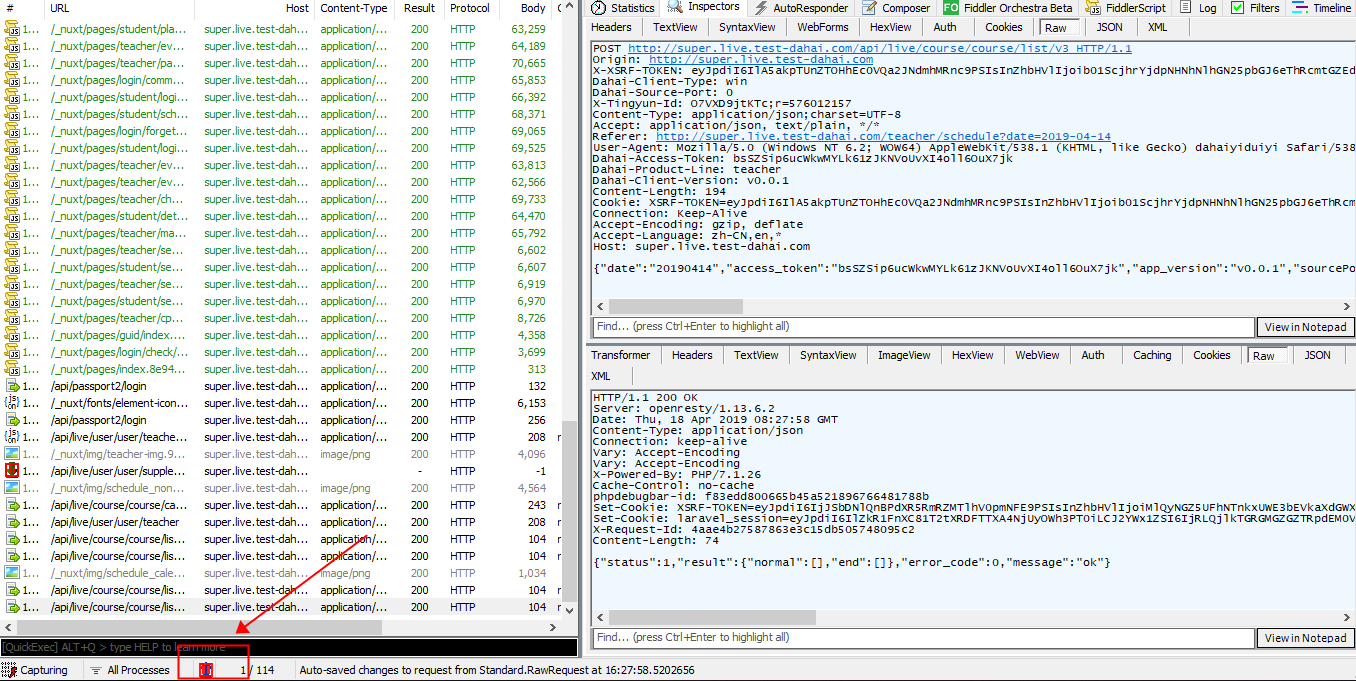


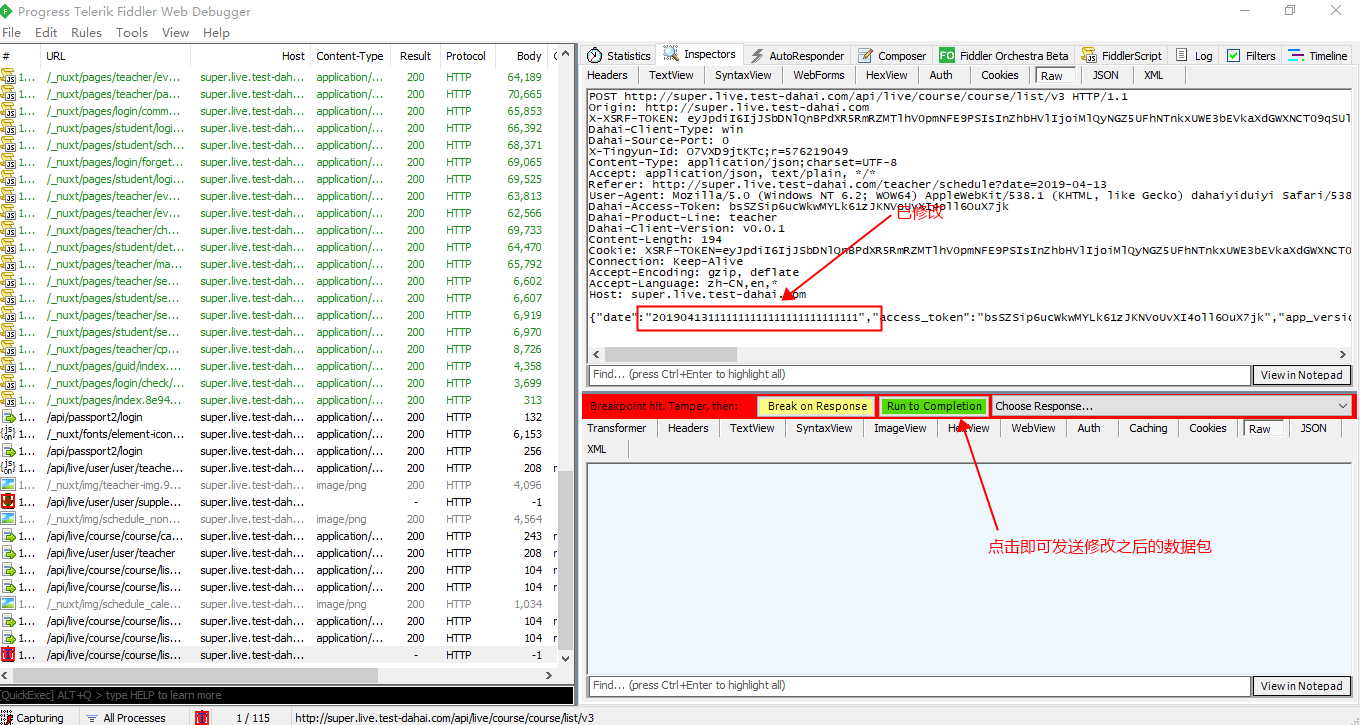
Fiddler抓取的数据包和burpsuite抓取的数据包很像，如下图；



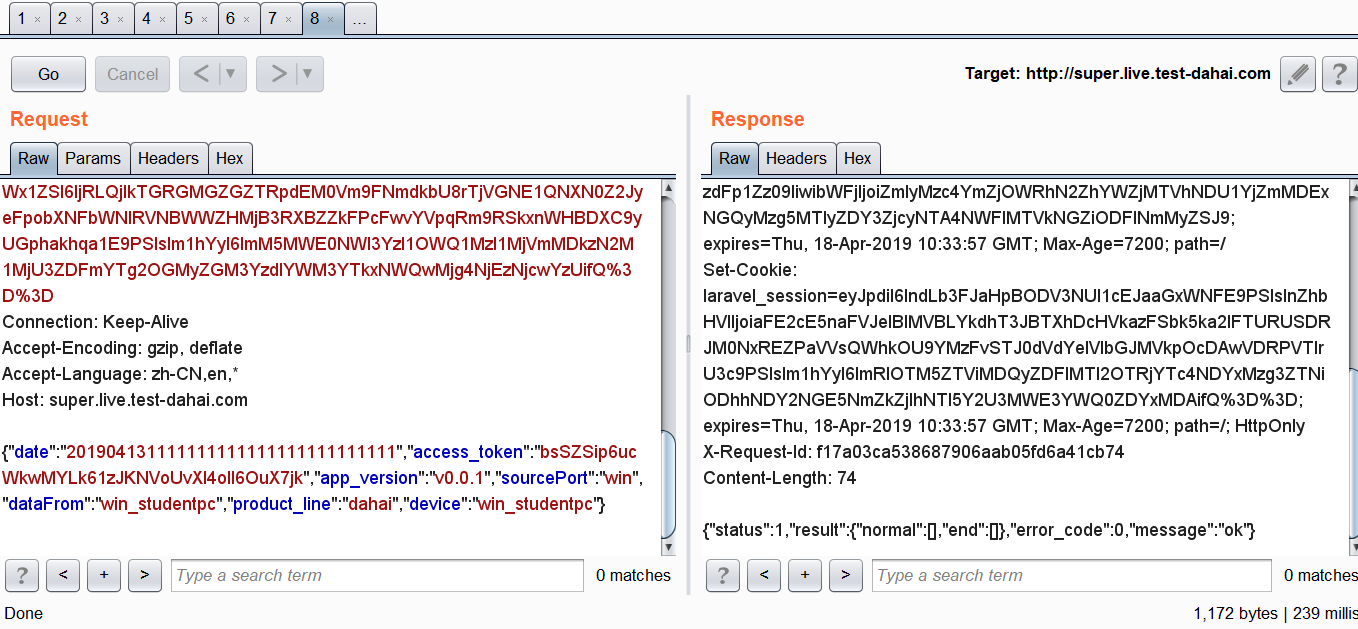
我们可以在抓取的时候灵活修改我们的数据包之后再发送，如下图；

需要点击左下角这个按钮，即可灵活修改我们的数据包之后发送；





我们也可以把这里的数据包直接复制到burpsuite里面使用Intruder,Sqlmap等模块。



至此完成PC客户端程序的抓包。

# 相关参考

https://blog.csdn.net/sunbo\_csdn/article/details/82292379