抓包总结

WSExplorer 可以根据进程。但是不能补货逍遥模拟器的

Attilax Fiddler 只能代理模式。。。需要在app设置代理麻烦

在我们做接口测试的时候，经常需要验证发送的消息是否正确，或者在出现问题的时候，查看手机客户端发送给server端的包内容是否正确，就需要用到抓包工具。而工程师和程序常用的抓包工具有哪些呢？今天我们就来简单聊一聊最常用的2种。

Fiddler是在windows上运行的程序，专门用来捕获HTTP，HTTPS的。

wireshark能获取HTTP，也能获取HTTPS，但是不能解密HTTPS，所以wireshark看不懂HTTPS中的内容。

总结，如果是处理HTTP,HTTPS 还是用Fiddler, 其他协议比如TCP,UDP 就用wireshark。

二、Wireshark

Wireshark是另外一种抓包工具，这种工具比fiddler更强大，消息量更多。大家可能会问：有了fiddler，为什么还要用wireshark呢？这里说下，在测试中，发现用fiddler抓包，有些包是没有抓到的，比如在验证反作弊信息的时候，反作弊pingback信息的消息用fiddler就没抓到，用wireshark就抓到了。还有另外一种情况，就是在验证cna的时候，如果先用fiddler抓包，如果没有种下cna的时候，以后就永远没有cna了，情况很诡异。解决办法就是把包卸载了重新安装，第一次用wireshark抓包。

Wireshark优势：

1、强大的协议解析能力，一到七层全解码，一览无遗，对于协议细节的研究特别有帮助。

2、对于https加密流量，只要将浏览器的session key 自动导入wireshark，Wireshark可以自动解密https流量。

Wireshark不足之处：

尽管可以自定义过滤列表，但为了抓取一个特定TCP Flow /Session 流量需要写一个长长的过滤列表，这对于初学者很不友好。

测试员常用抓包工具：fiddler和wireshark对比