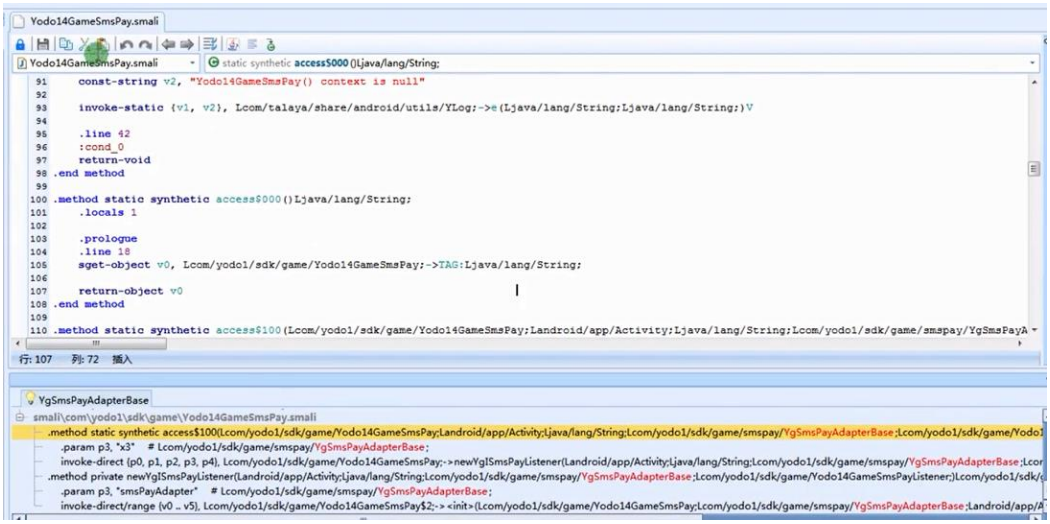
1. 破解滑雪大冒险内付

(1)根据输出 Log 信息定位购买操作的函数

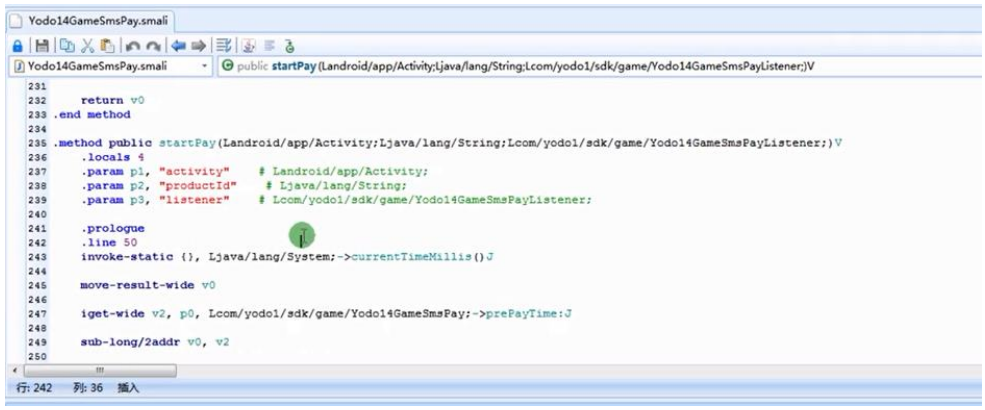

(2)定位到 SmsPay 所在的 Smali 文件

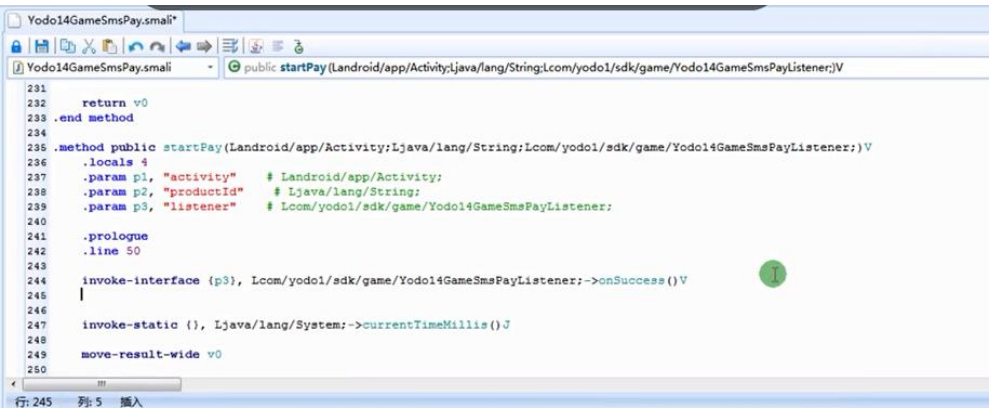



(3)定位到 startPay 函数的位置


可以看出是对 listener 接口所回调方法的判断来确定是否支付成功，所以一直返回该接口的 success 方法就可以了

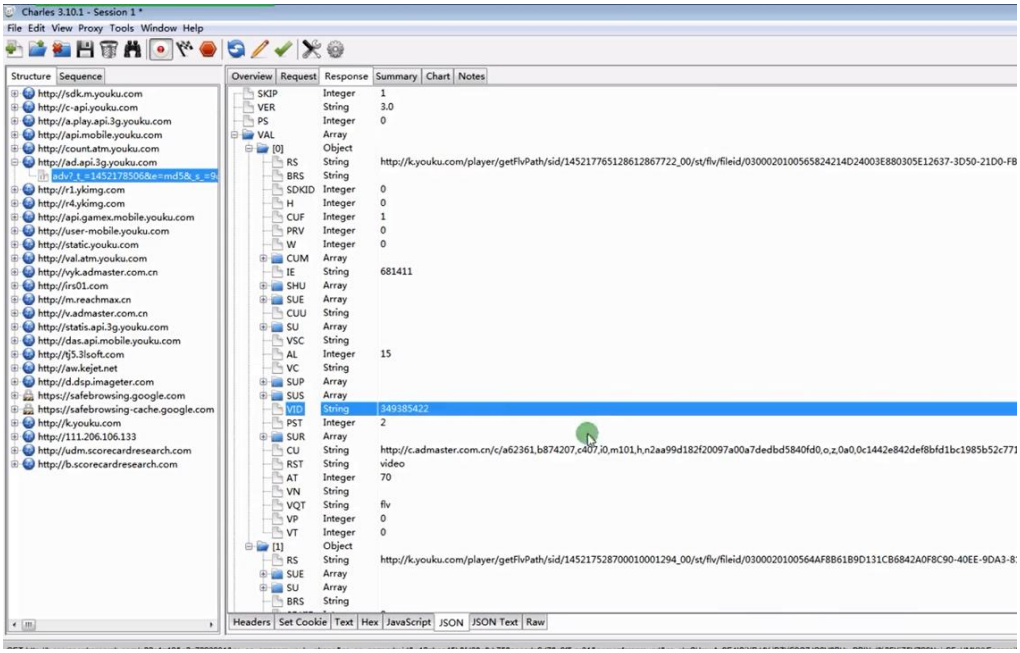
(4)进行代码修改，使得该接口一直调用 success 方法



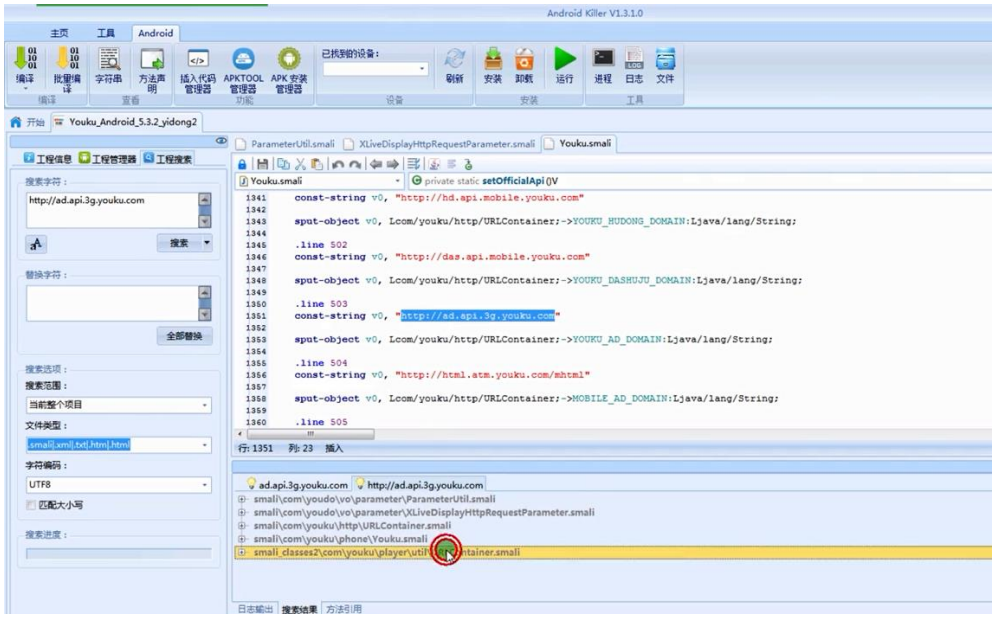

2. 去除优酷 app 广告

(1)抓包获取网络连接信息，工具：Charles。设置网络代理，Proxy 为当前主机的 ip 地址，端口为 8888。




抓取到的 ad 地址开头的数据包为广告的网络数据信息，阻止 app 访问该地址来达到去除广告的效果。

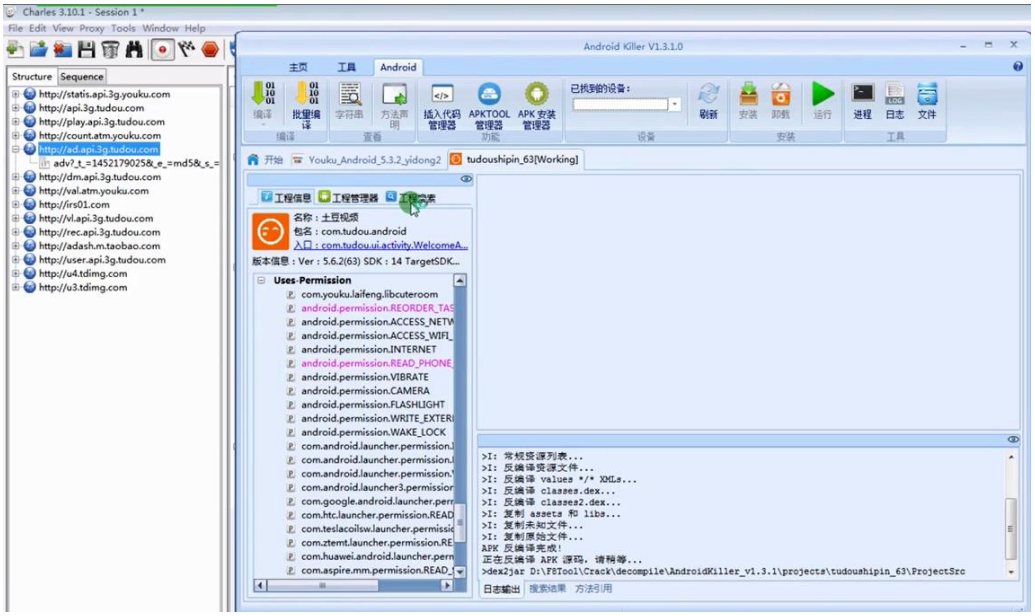
(2)找到该地址字段在 app 中的位置

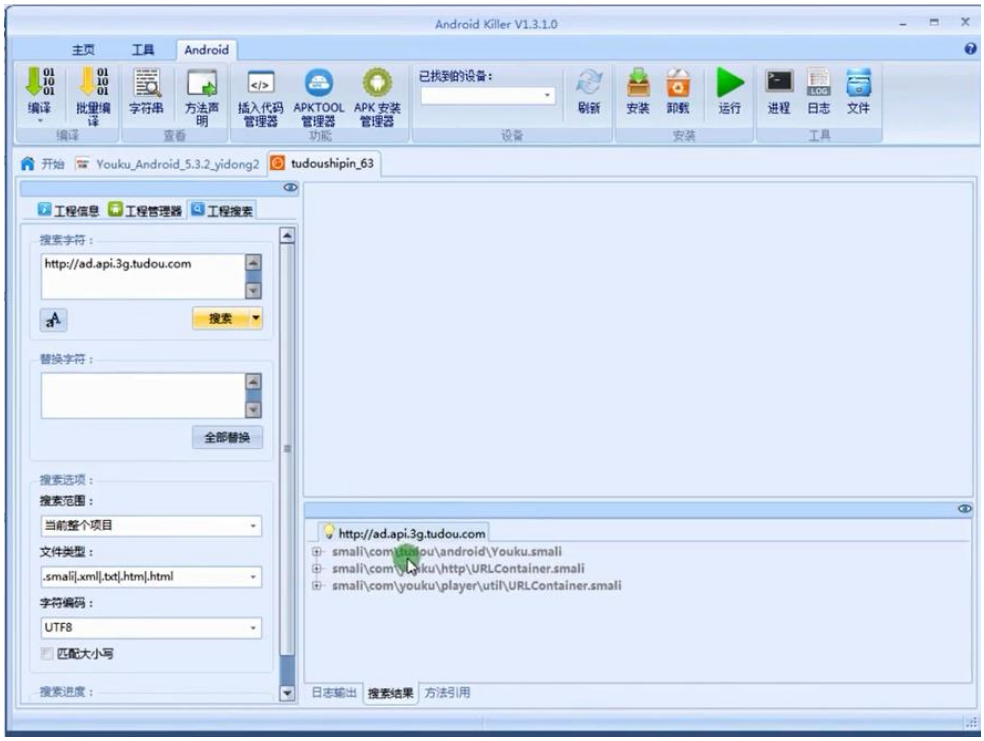



将该地址字段全都替换为空值，来达到去除广告的效果

3. 去除土豆 app 广告

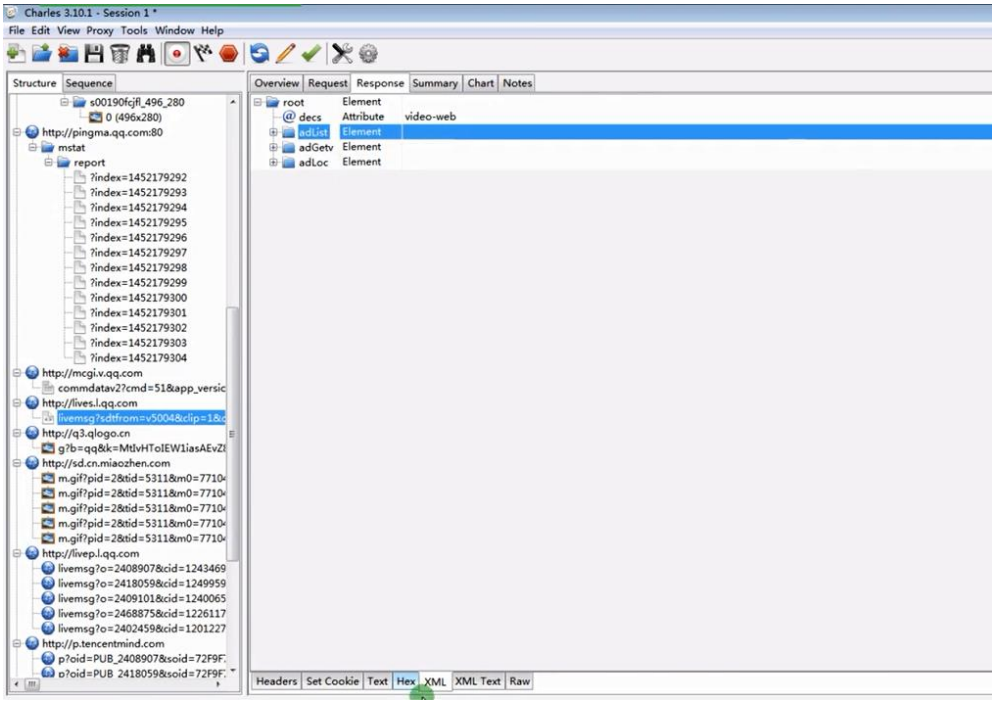
网络抓包获取广告字符串，并定位广告字符串位置



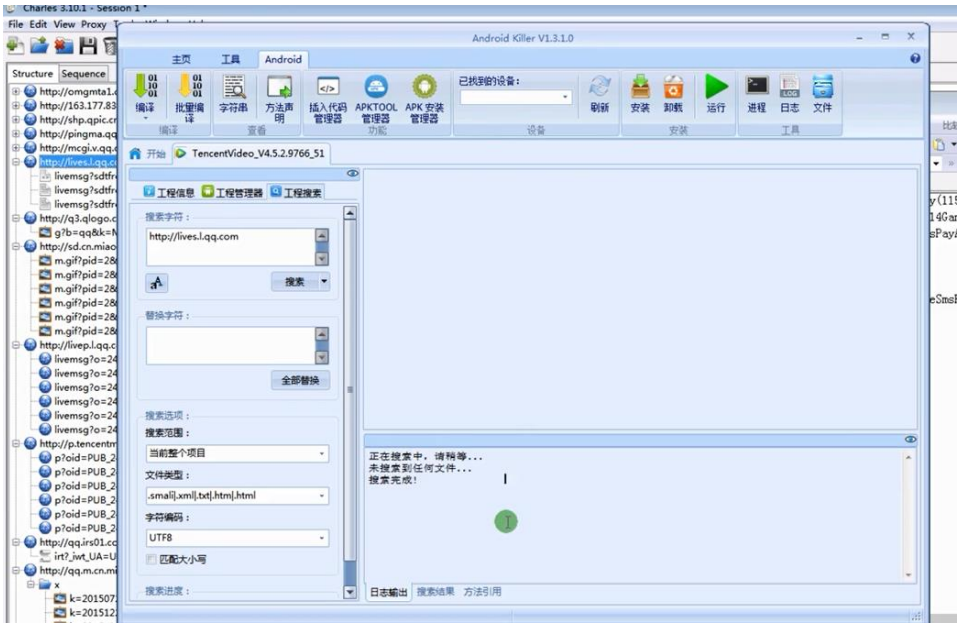



4. 去除腾讯视频 app 广告

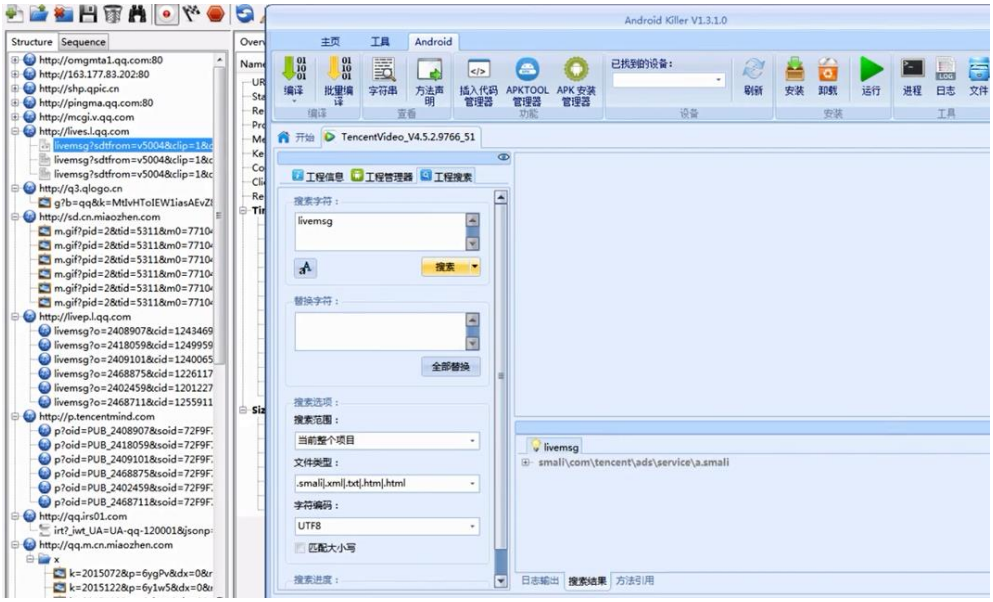
网络抓包定位广告字符串



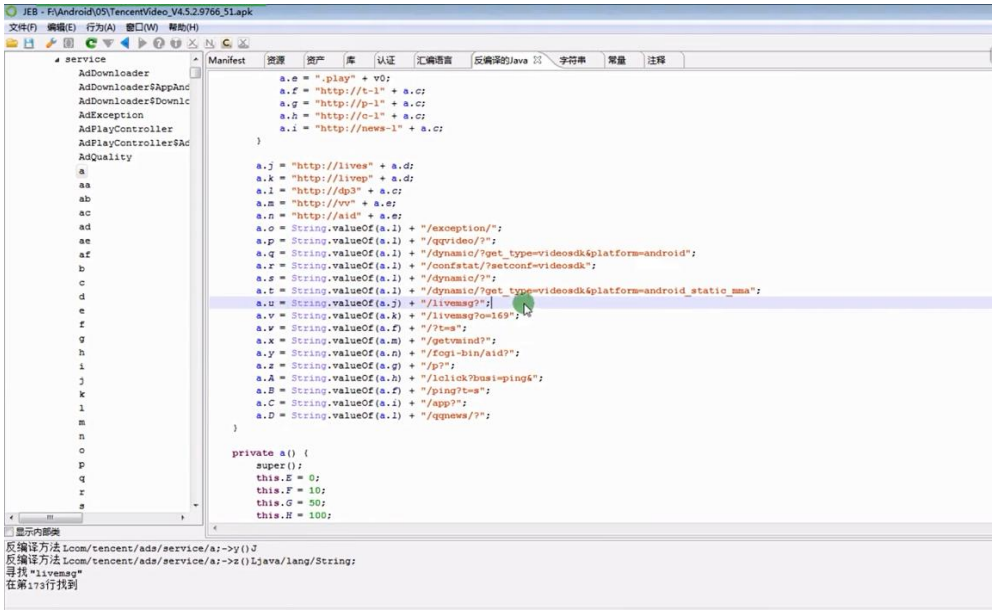

搜索广告地址字符串



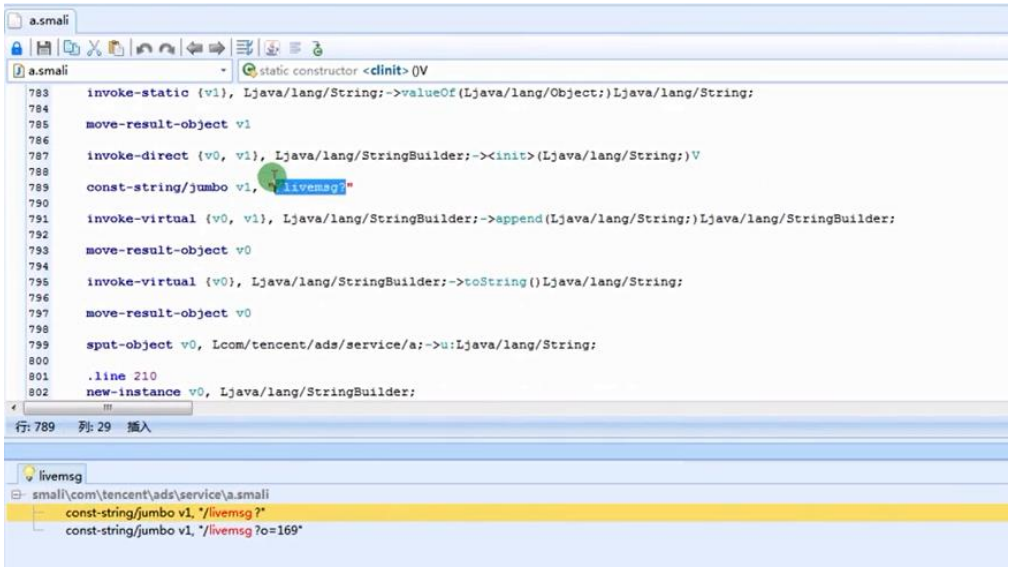

但是搜索失败，显然腾讯是做了处理的，然后分开搜索部分字段

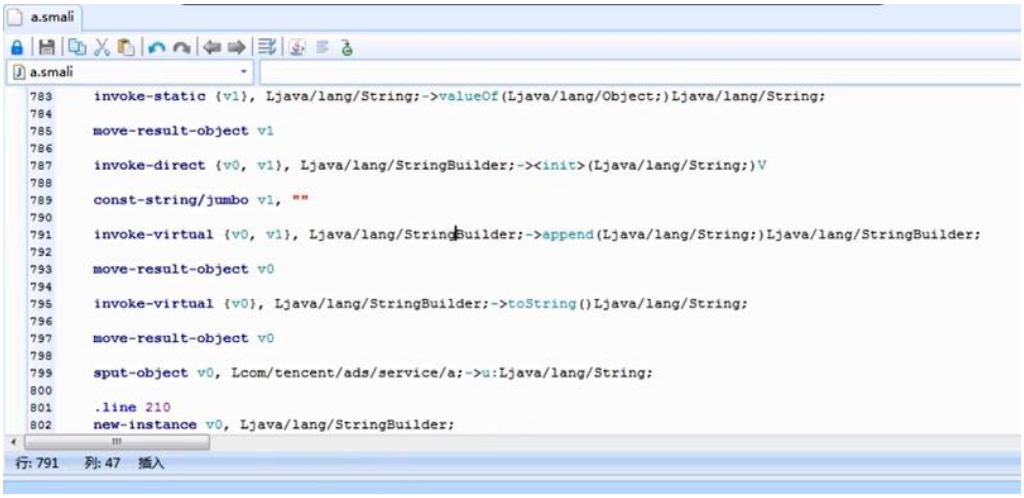



能够搜索到部分字段的内容，并在 jeb 中分析该字符串的定义和调用



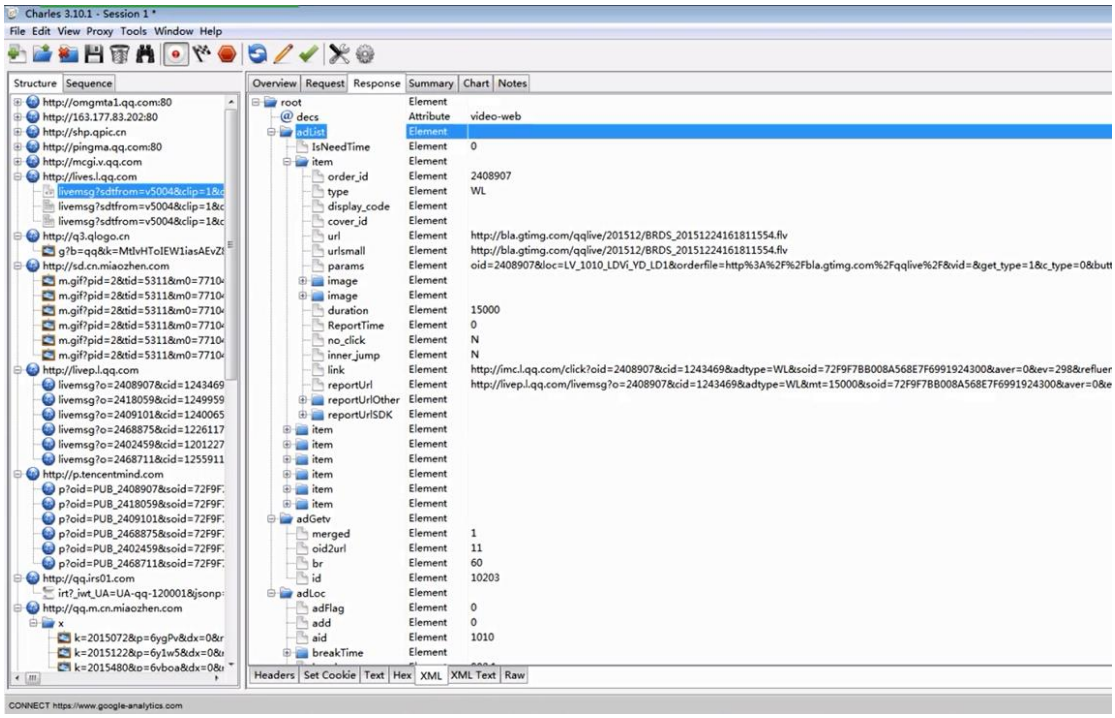

发现腾讯视频 app 中广告字段是由多个字符串动态组合生成的，尝试清空该字符串，观察是否去除了广告



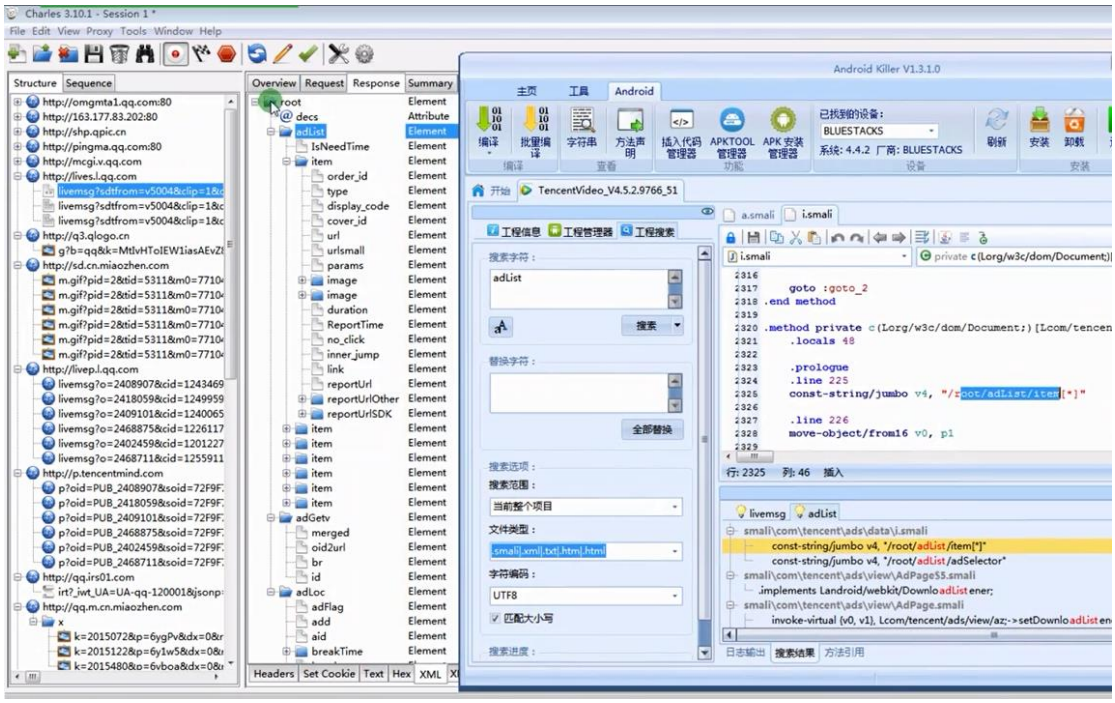




然而去除字段后没有达到去广告的效果。

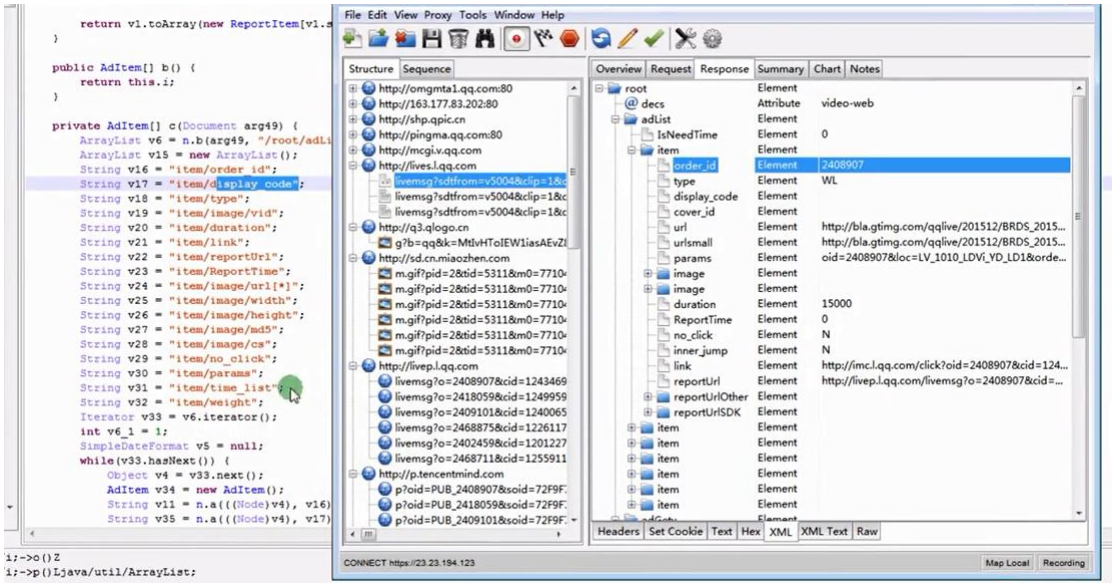
换种思路，查找解析 Response 数据的代码




找到 adList 准确的位置，符合 Response 数据中的/root/adList/item 字段




通过 jeb 找到分析返回广告数据的位置




使返回的 item 数据为空=>去掉循环 or 去掉添加的方法（把解析的结果加到结尾）

注释掉 add 方法对应的 Smali 代码，最后达到了去除广告的效果