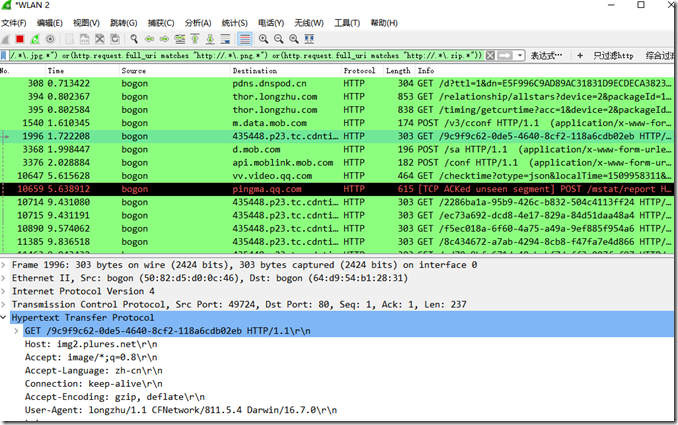
**[wireshark利用正则表达式过滤http协议中的jpg png zip等无用的数据包](https://www.cnblogs.com/caianhua/p/7794510.html)**

主要工具：小度随身wifi热点 + wireshark抓包工具。（强烈不建议使用360的产品，非常垃圾，而且干扰代理#墙IP，搞得你不能科学上网）

利用wireshark这个强大的协议分析利器。去分析某些直播平台的http协议。以及开发出一些软件，无往不利。

[](http://images2017.cnblogs.com/blog/545403/201711/545403-20171106182640934-243093851.png)

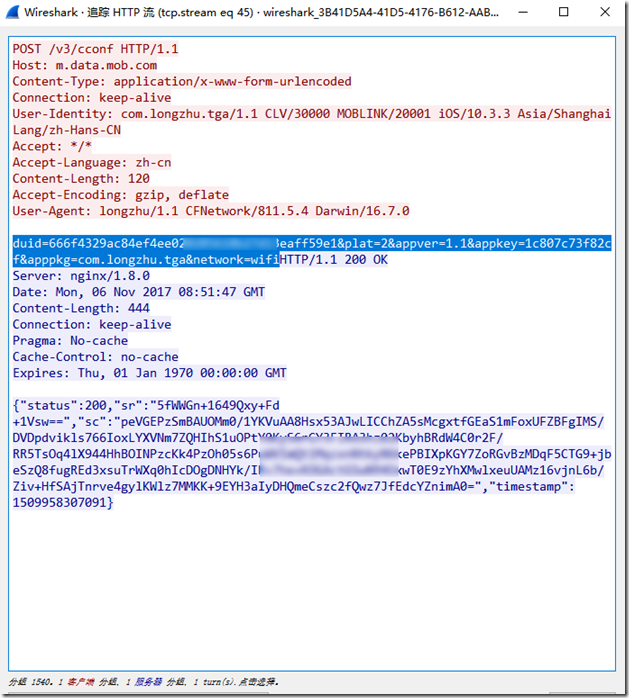
我们需要监控 某个 手机app 发包数据，这个用Fiddler是无法抓。上图是某个视频直播平台的数据包。

我们的过滤条件是：①只需要http的包；②过滤掉jpg；③过滤掉png；④过滤掉zip

根据正则通配符 ，结合逻辑 and  、 or ，小括号 ()  组合的模式，综合过滤。

http.request and !((http.request.full\_uri matches "http://.\*\.jpg.\*") or(http.request.full\_uri matches "http://.\*\.png.\*") or(http.request.full\_uri matches "http://.\*\.zip.\*"))

找到某条包之后，可以追踪http流，看到Post 客户端 和 服务器端一次完整 交互：

[](http://images2017.cnblogs.com/blog/545403/201711/545403-20171106182438653-638848769.png)

OK，wireshark过滤http中jpg,png,zip数据就写到这。