**一、wireshark常见命令使用：**

**过滤IP：**

IP源地址：ip.src ==192.168.1.1

IP目的地址：ip.dst== 192.168.1.1

**过滤内容：**

http contains "taobao"

http.request.method=="POST"

http.host=="wifi.shouji.360.cn"

http.request.uri contains "index"

**过滤mac地址：**

源MAC地址：eth.src==A0:00:00:04:C5:84

目的MAC地址：eth.dst==A0:00:00:04:C5:84

MAC地址（包括源和目的）：eth.addr==A0:00:00:04:C5:84

**过滤包长度：**

整个UDP数据包：udp.length==20

TCP数据包中的IP数据包：tcp.len>=20

整个IP数据包：ip.len==20

整个数据包：frame.len==20

**过滤端口：**

TCP端口：tcp.port==80

TCP目的端口：tcp.dstport == 80

TCP源端口：tcp.srcport == 80

UDP端口：udp.port eq 15000

**过滤http：**

http.request.method== "GET"

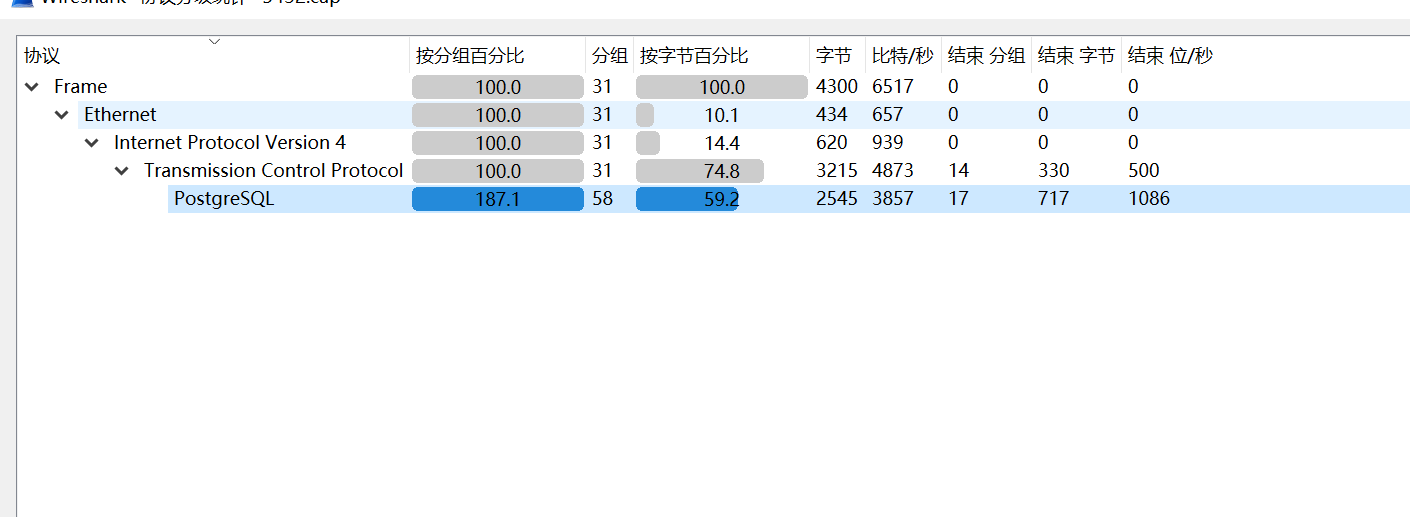
http.request.method== "POST"

http.request.uri =="/img/logo-edu.gif"

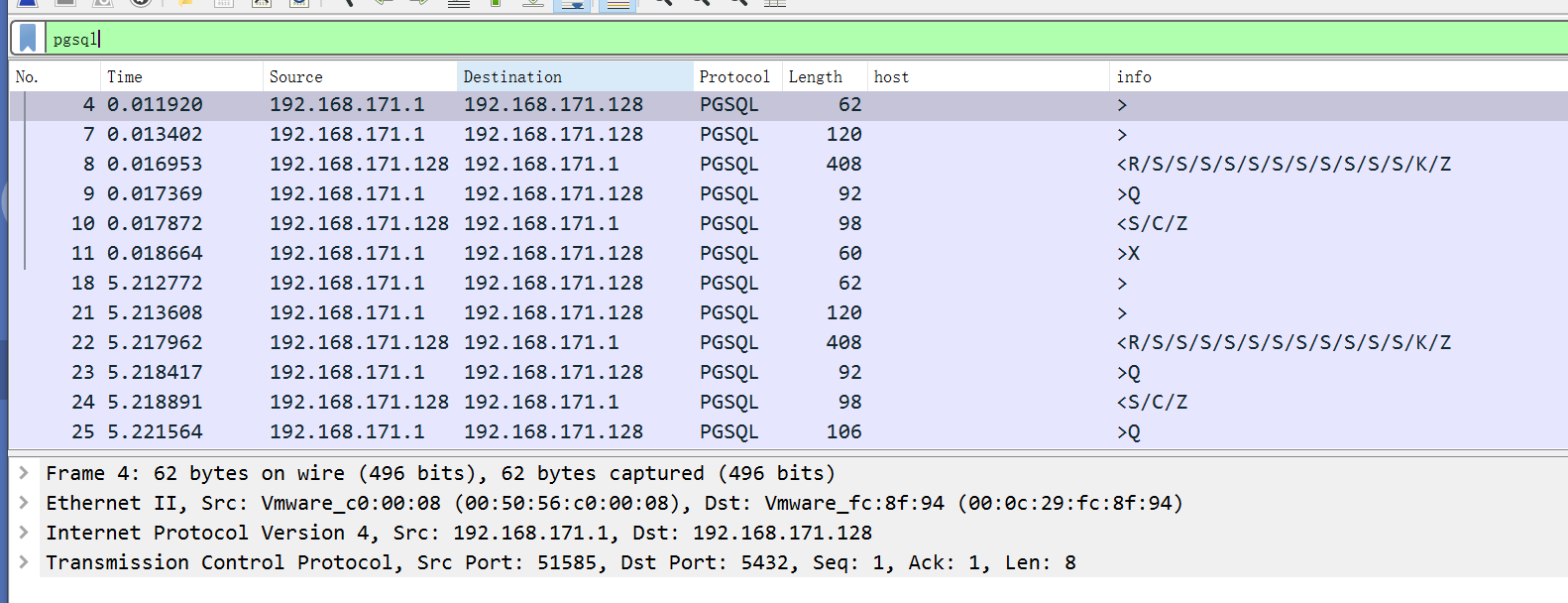
http contains "PNG"

**协议分析：**

统计--协议级分析，可查看当前数据包包含的哪些协议



如此处重点关注postgresql协议，可右键选中，重点去查看该协议



**数据流跟踪**

在关注的http数据包或tcp数据包中选择流汇聚，可以将HTTP流或TCP流汇聚或还原成数据，在弹出的框中可以看到数据内容。

选中数据分组后，右击选择追踪流->TCP流|HTTP流

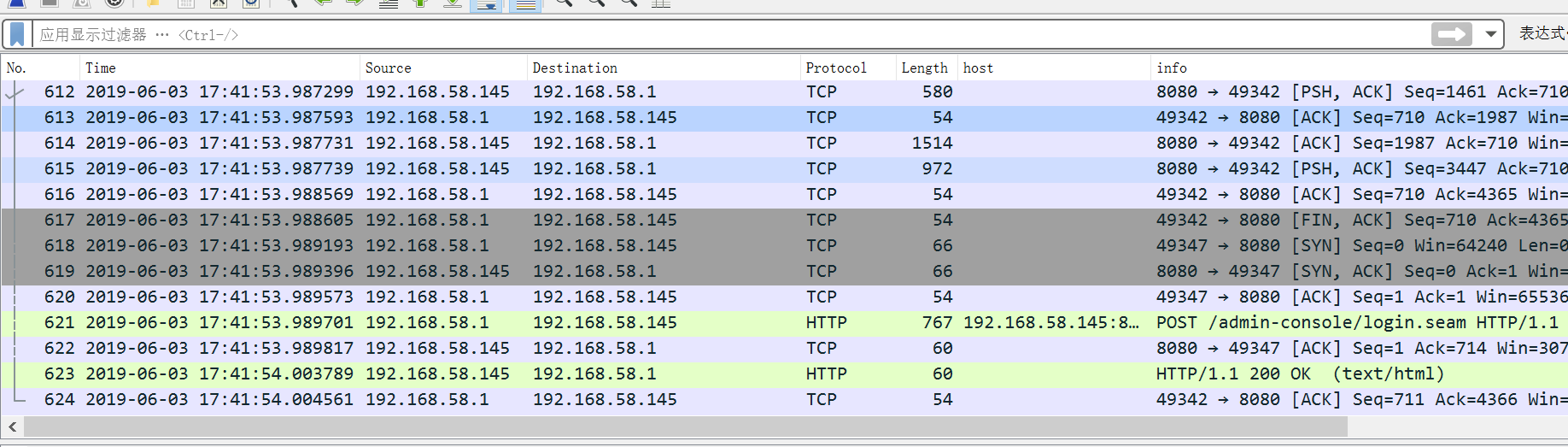
查找：

ctrl+f

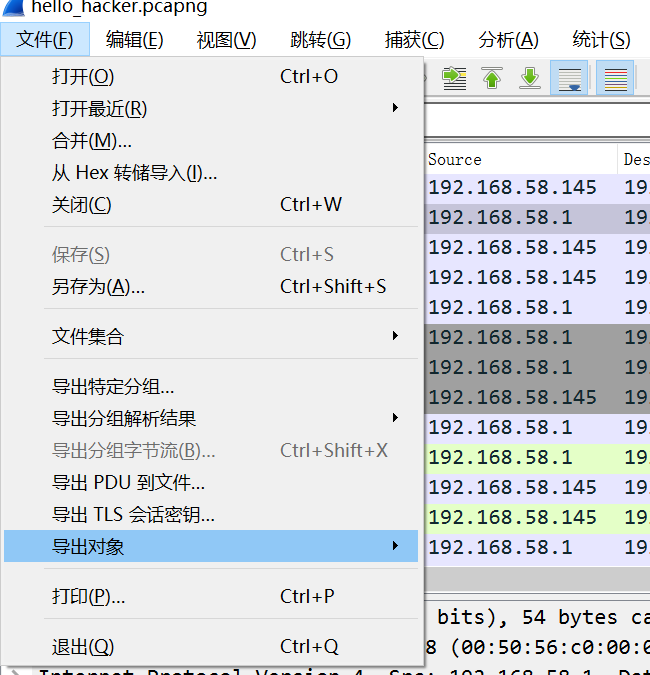
**二、ctf流量分析**

在了解了wireshark基本用户法后，在找个ctf中的流量分析题目进行分析。

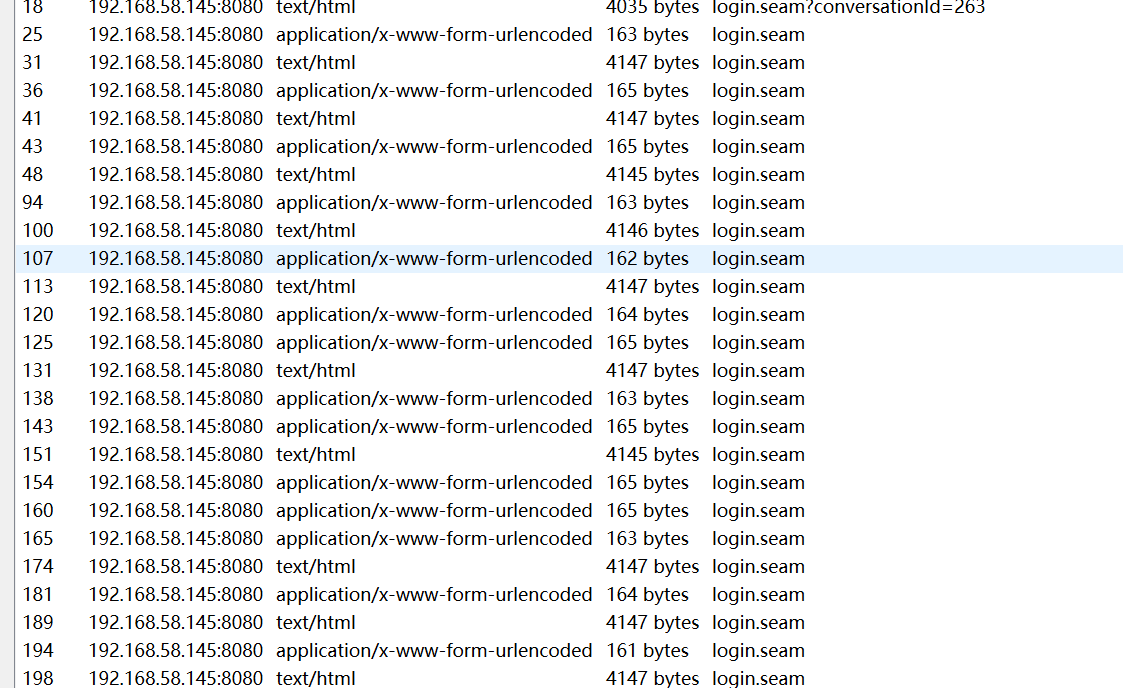
打开数据包如下，这么多数据看的好晕



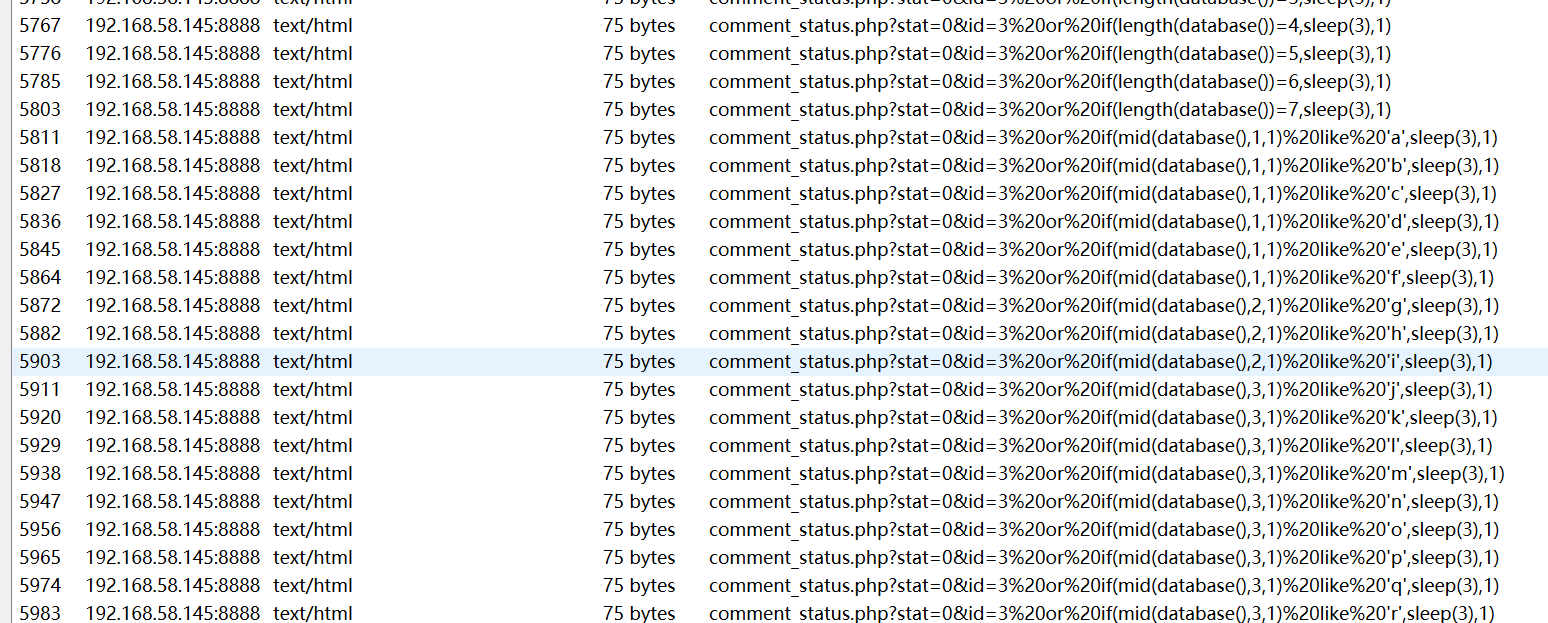
1、可通过导出对象方式--HTTP查看数据包情况



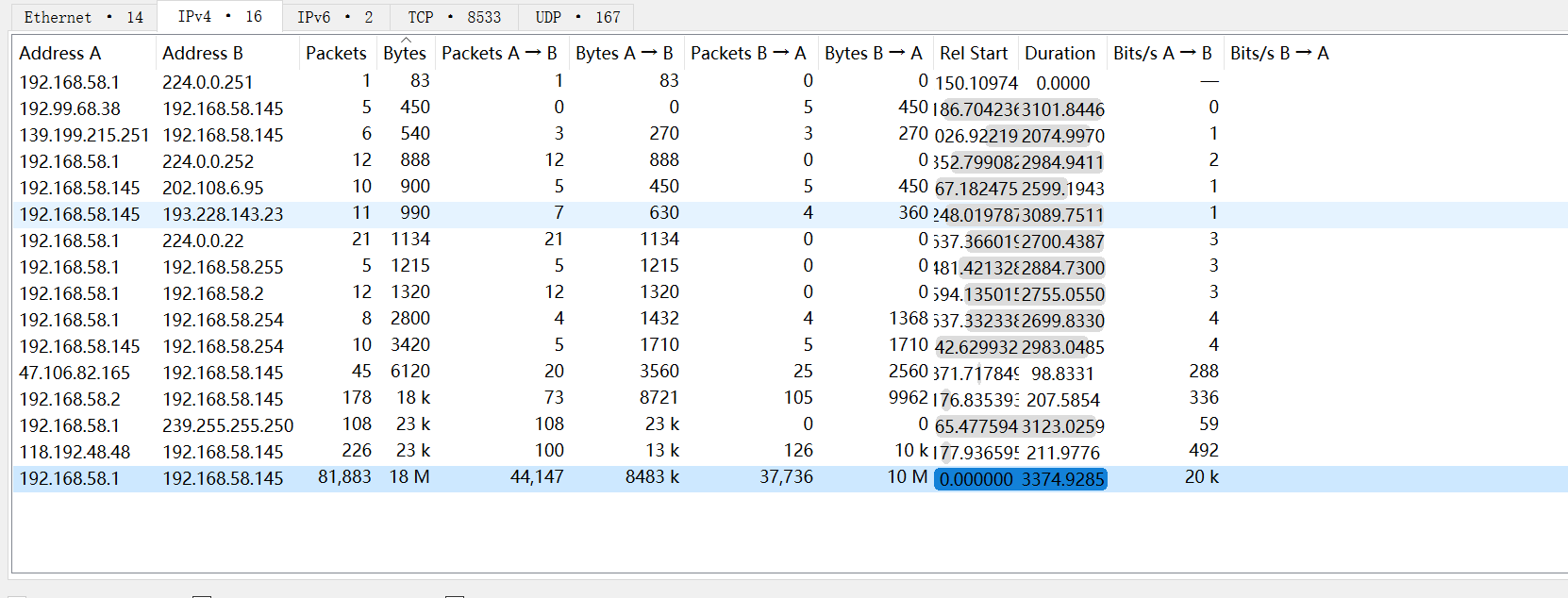
查看数据包情况如下，开始是一直在访问login.seam,查看单个数据包，发现是对登录页面的暴力破解，



2、接着继续向看，貌似发现了不一样的数据，这不是sql注入么，根据题目已经给的提示“最近新搭的服务被入侵了，你能通过这个流量包找到hacker都拿到了什么数据么？”，可以推测，攻击者通过sql注入拿到了部分数据

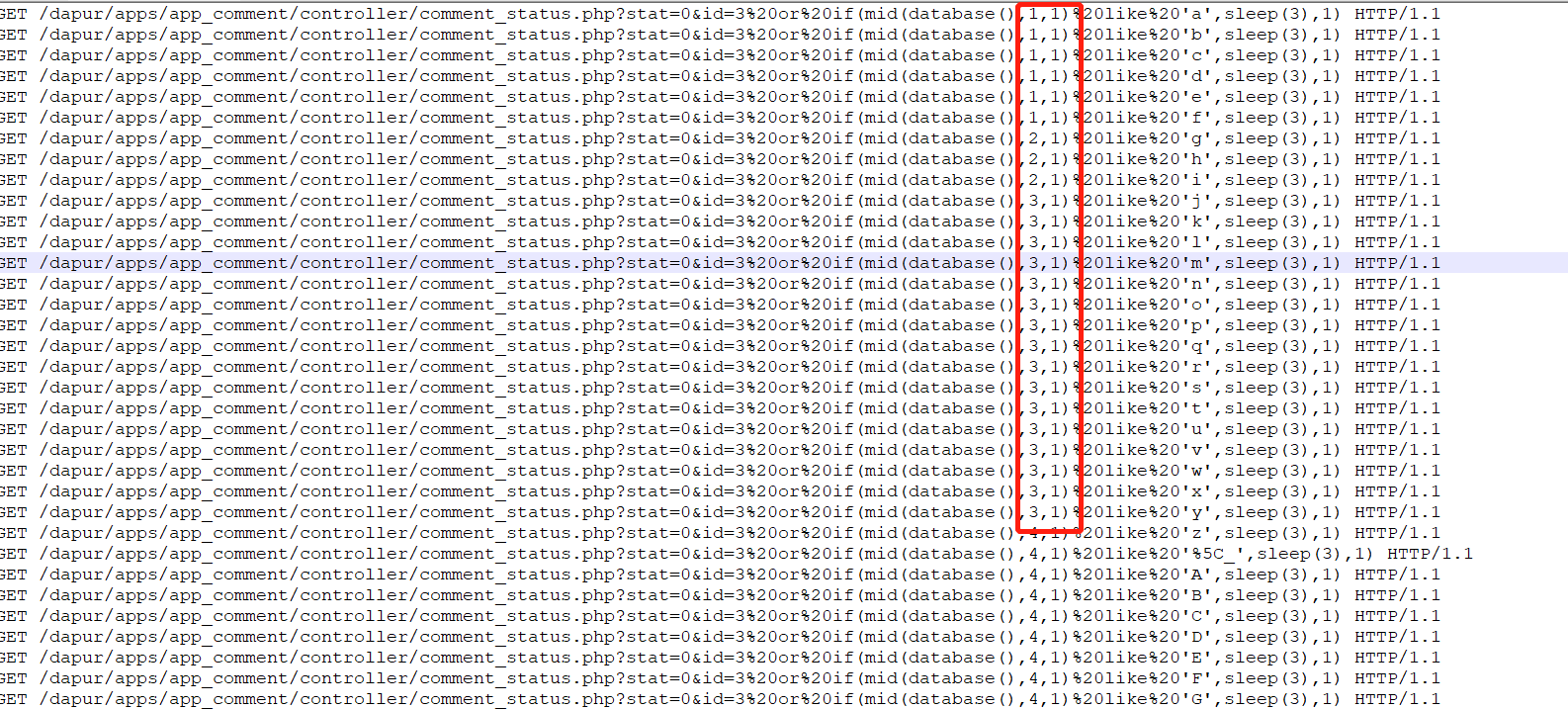


3、查看“统计”---“会话”情况

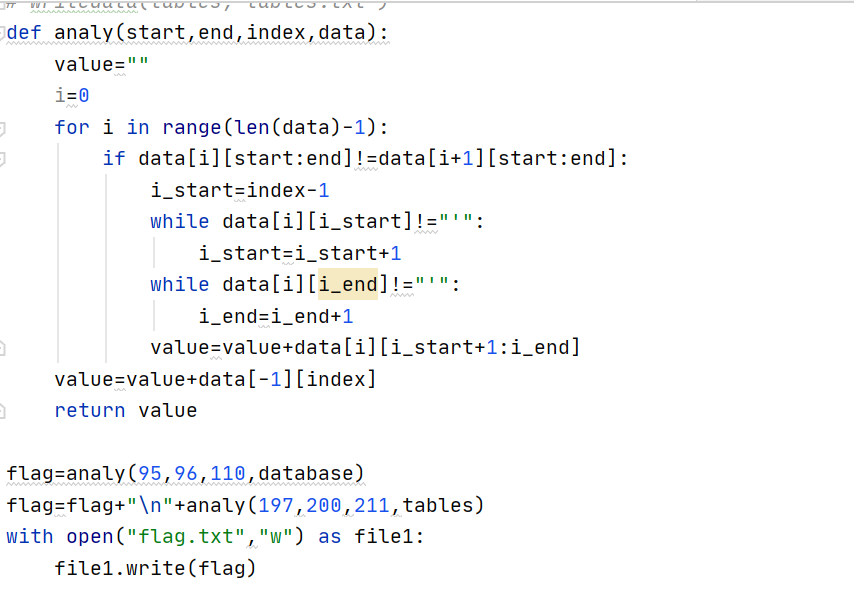


可看出192.168.58.1 到192.168.58.145之间通信比较多，在加上之前的分析，可初步确定，192.168.58.145为受害主机地址。

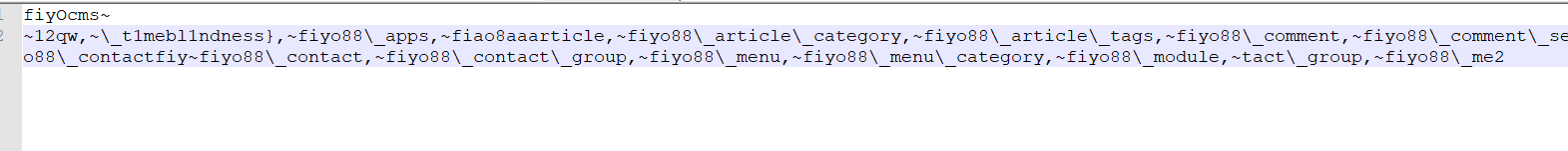
通过分析数据包，可以发现系统存在时间盲注，标红代表测试的是第几个字符，以探测第一个字符为例，先是尝试测试第一个字符是否是a，在探测到f时，发现系统又开始探测第二个字符，所以由此可以判断数据库名的第一个字符为f，由此可依次判断，如果内容比较少，可以人工进行判断得到数据库名称。



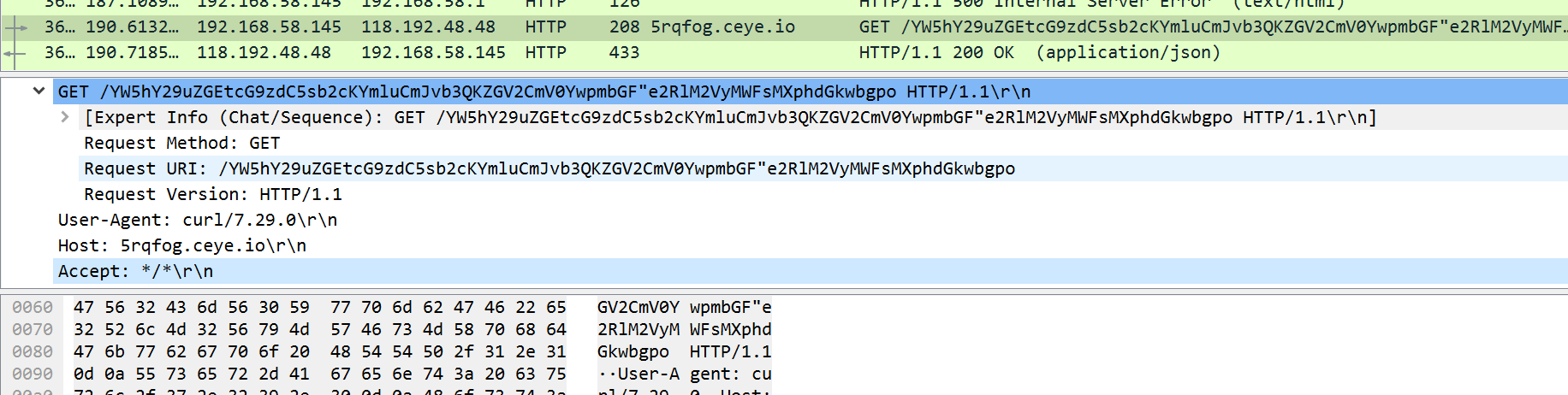
尝试采用脚本方式读出数据库的名称，当相邻两行的数据库名称的字符位置发生变化时，说明字符探测成功，即当database(),1,1变为database(),2,1时，说明最后的一个含有database(),1,1的请求探测的字符是正确的，而字符在请求中为110位，数据库名称位置的数为95位，同理可获取表的名称，最终脚本如下：



对获取的数据，在进行简单分析可获取具体的数据库名称和表名称，可看到t1mebl1ndness}，后一半的flag



继续观察字符串，可发现一串base64编码



进行base64解码如下：

anaconda-post.log

bin

boot

dev

etc

fla

{de3er1al1zati0n

h

得出flag为：flag{de3er1al1zati0nt1mebl1ndness}

由于题目给出提示是时间盲注，所以用s替代3,用i替代1，用o替代0，

最终flag为flag{deserializationtimeblindness}

小结：

借助该流量分析题目，将部分流量分析需要用到方法进行巩固，随着https普及以及http2、QUIC特性的使用，传统网络层看到的将是一串加密二进制数据，不再是http下的明文字符，基于黑特征的检测拦截能力都将失效，解决办法是将流量接入层下移，比如位于接入网关GW/LB解密卸载之后；同时对于某些场景，需要降低对黑特征、关键字的依赖，综合利用大数据、AI等手段，构建基于行为的检测机制，比如木马主控C&C行为的发现。

参考：<https://www.jianshu.com/p/685cbb34afc7>

<https://security.tencent.com/index.php/blog/msg/148>