网络空间安全市赛Misc一道简单的流量分析题

原创

疯狂的1998 于 2021-11-28 12:47:33 发布 4259 收藏 2

分类专栏： CTF 文章标签： 安全

本文链接：https://blog.csdn.net/MarkRao/article/details/121589667

这道题给了一个流量包，内部分了7个小题

题目介绍：

1、使用Wireshark查看并分析服务器桌面下的attack.pcapng数据包文件，通过分析数据包attack.pcapng找出黑客的IP地址，并将黑客的IP地址作为FLAG（形式：[IP地址]）提交

2、继续查看数据包文件attack.pacapng，分析出黑客扫描了哪些端口，并将全部的端口作为FLAG（形式：[端口名1,端口名2,端口名3…,端口名n]）从低到高提交；

3、继续查看数据包文件attack.pacapng分析出黑客最终获得的用户名是什么，并将用户名作为FLAG（形式：[用户名]）提交；

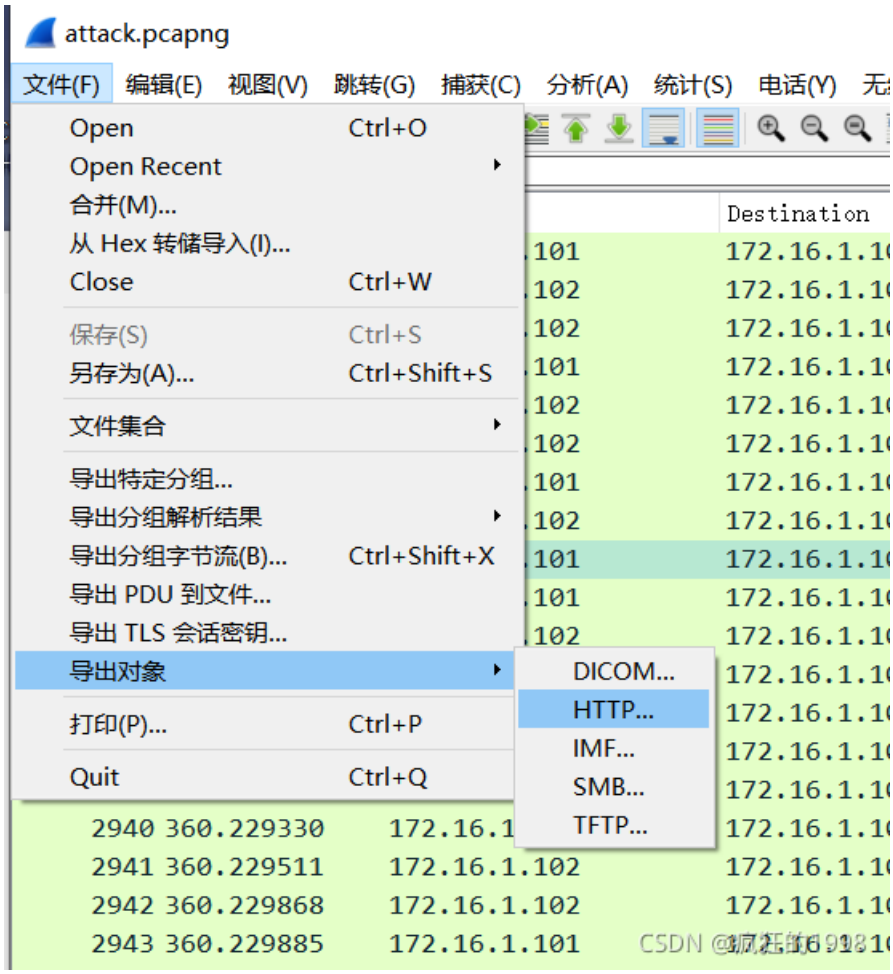
4、继续查看数据包文件attack.pacapng分析出黑客最终获得的密码是什么，并将密码作为FLAG（形式：[密码]）提交；

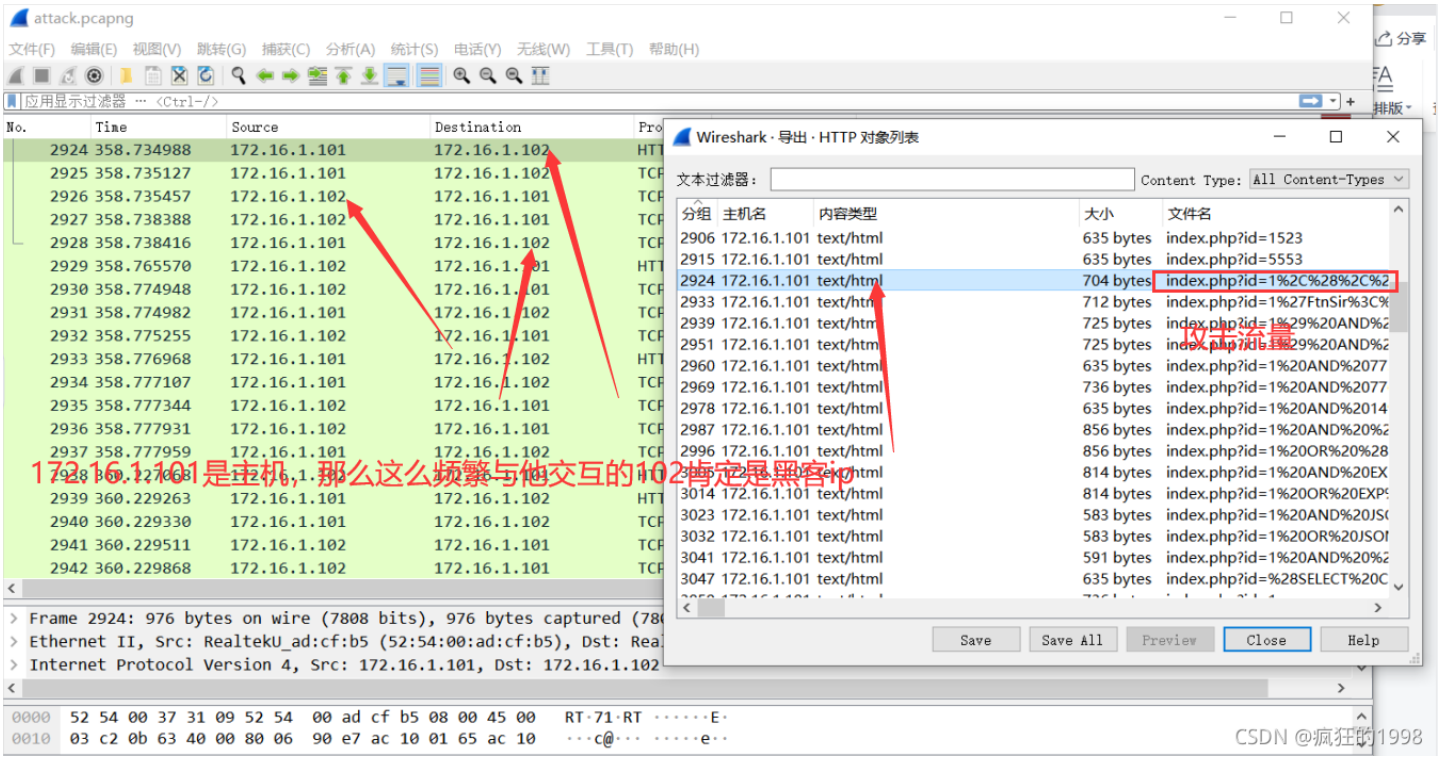
5、继续查看数据包文件attack.pacapng分析出黑客连接一句话木马的密码是什么，并将一句话密码作为FLAG（形式：[一句话密码]）提交；

6、继续查看数据包文件attack.pacapng分析出黑客下载了什么文件，并将文件名及后缀作为FLAG（形式：[文件名.后缀名]）提交；

7、继续查看数据包文件attack.pacapng提取出黑客下载的文件，并将文件里面的内容为FLAG（形式：[文件内容]）提交。

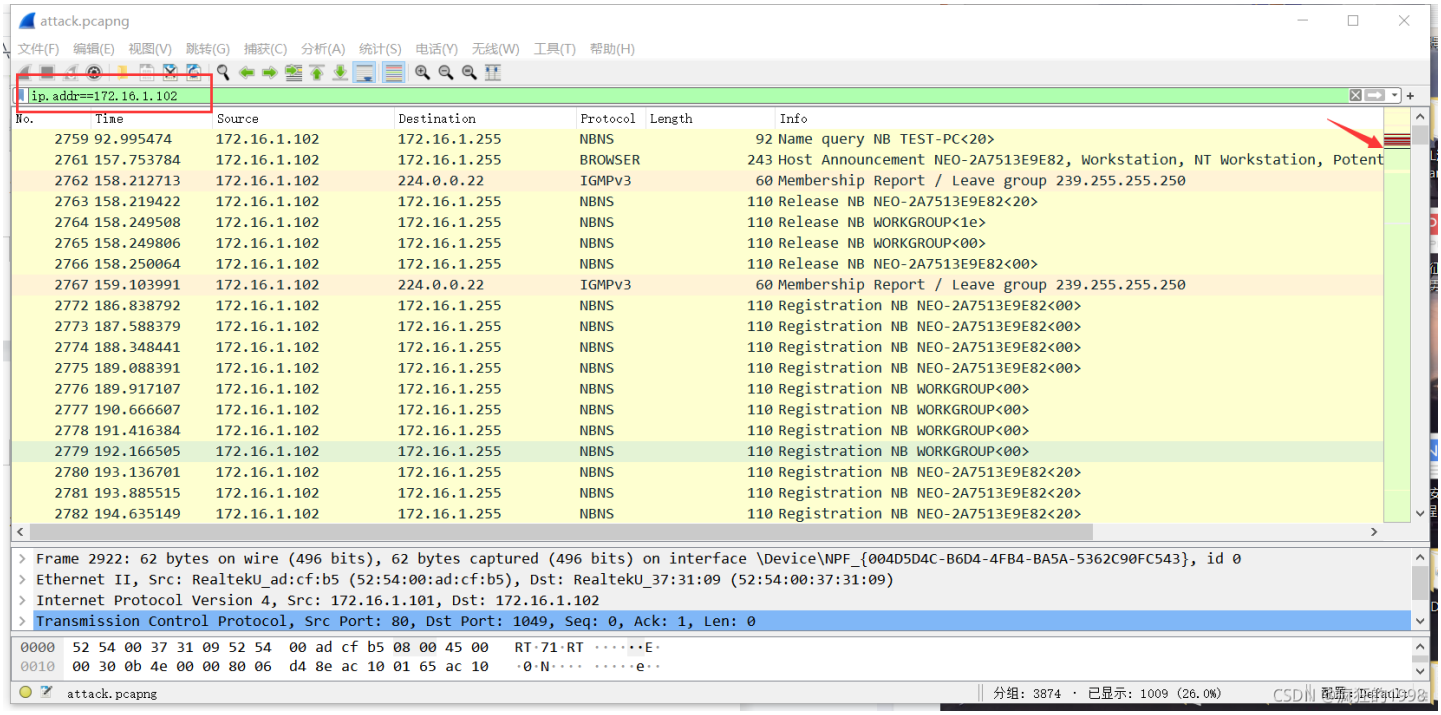
1：首先可以在导出HTTP中查看攻击流量



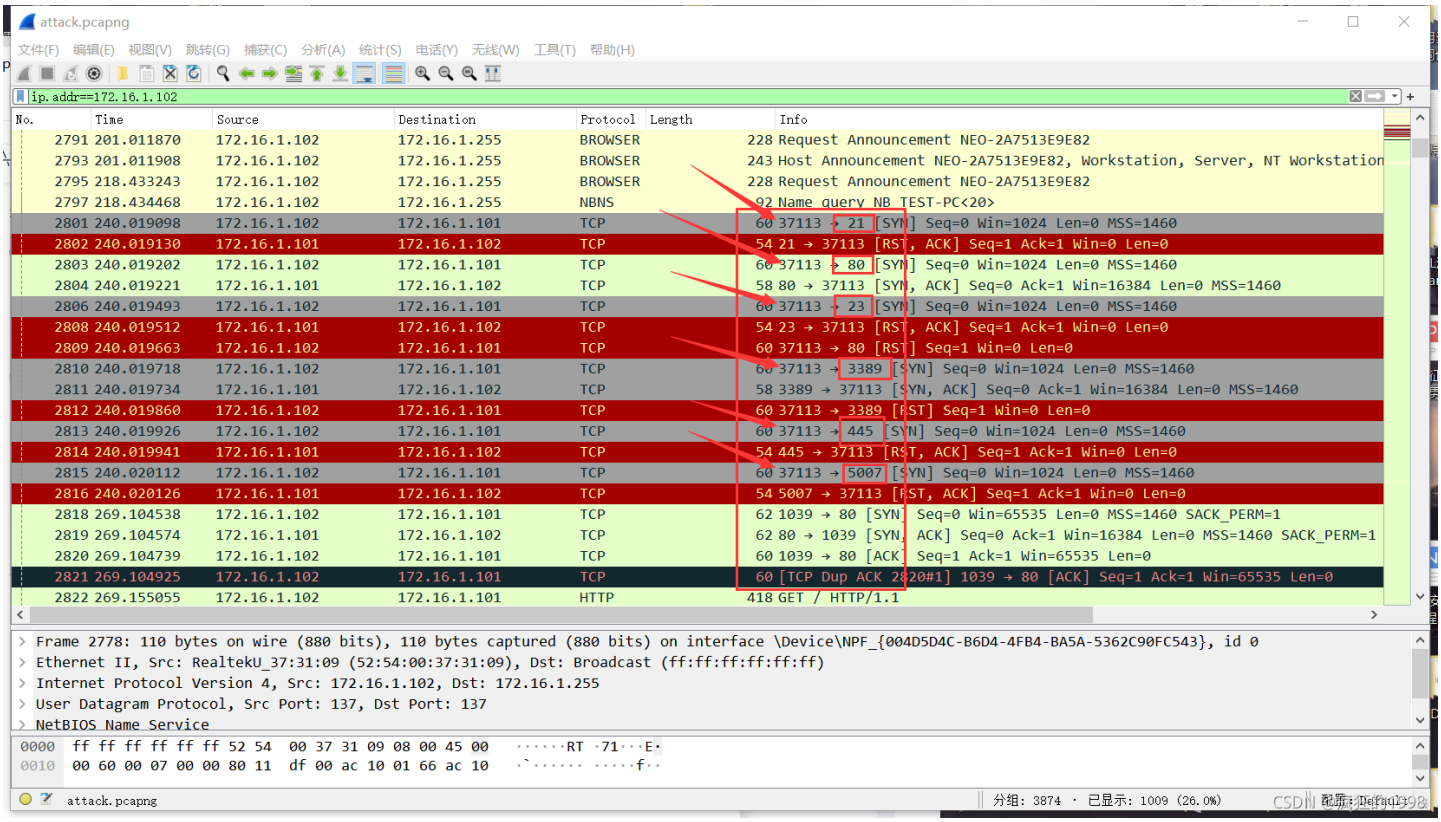


第一题的flag答案便是： [172.16.1.101]

2、查端口，我们找到黑客ip后便过滤ip，输入ip.addr==172.16.1.102



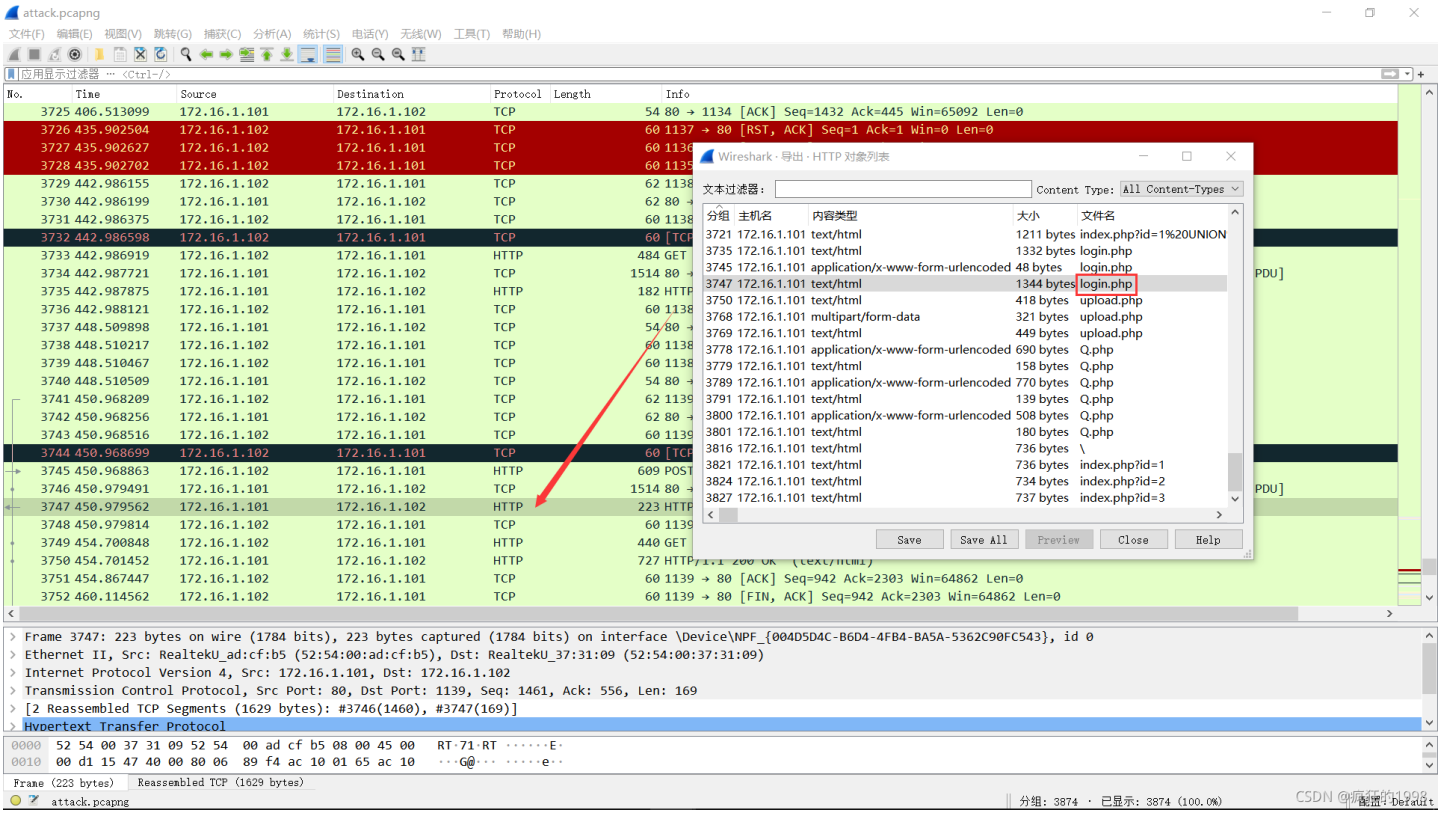
往下分析你会发现很集中的有端口扫描现象，黑客是通过37113来扫描的，你只需要看这些便可，便能得到flag，所以第二题flag为[21,23,80,445,3389,5007]

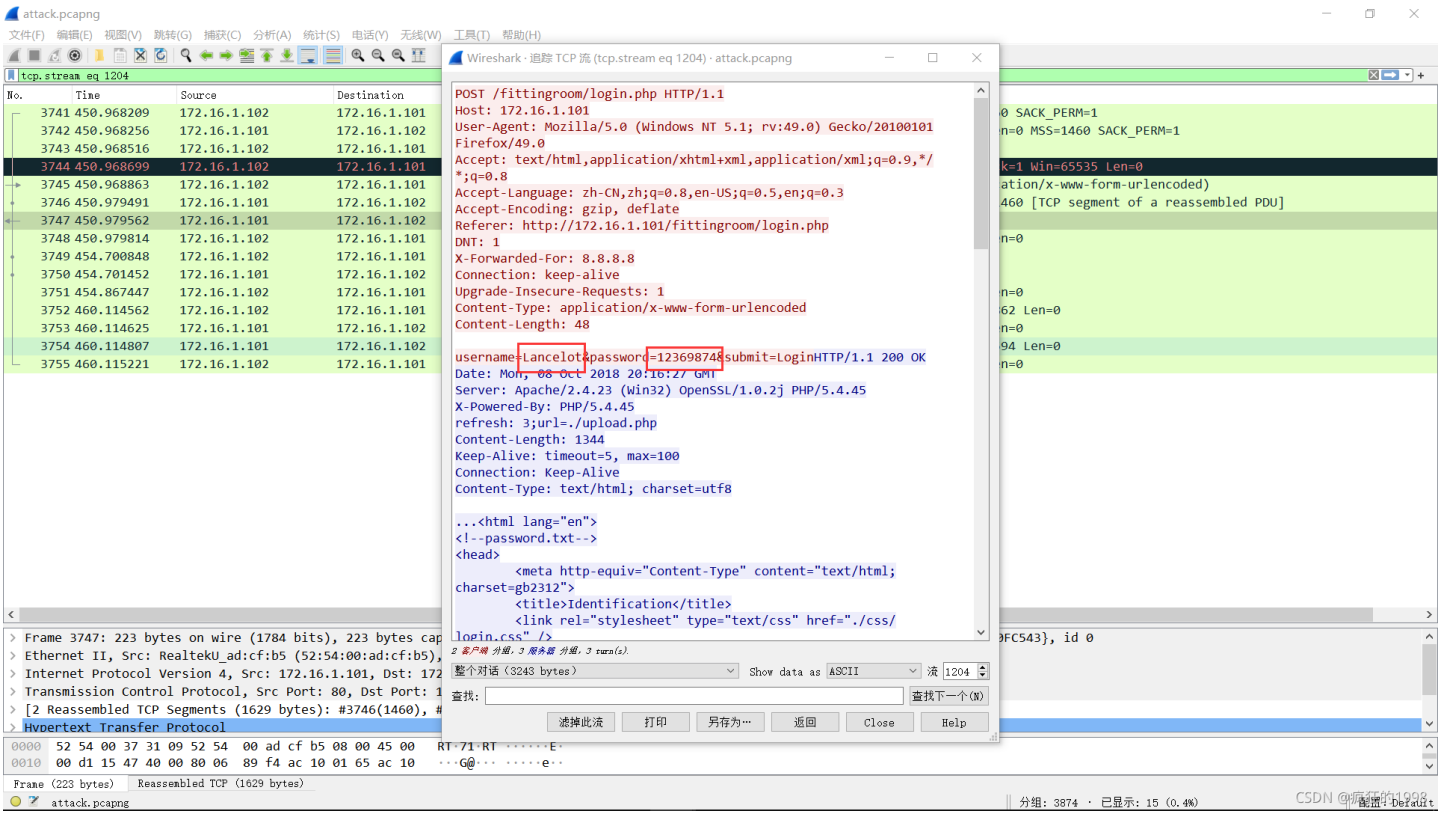


3/4两题、要分析出黑客最终获得的用户名就得找到黑客什么时候登录的，攻击点在哪里，那就用同样的方法，导出http处查看，发现有登录login请求，点击它便会自动跳转到那条流量，关闭导出框，对3747这条流量进行TCP追踪，这样便看到了用户名和密码，

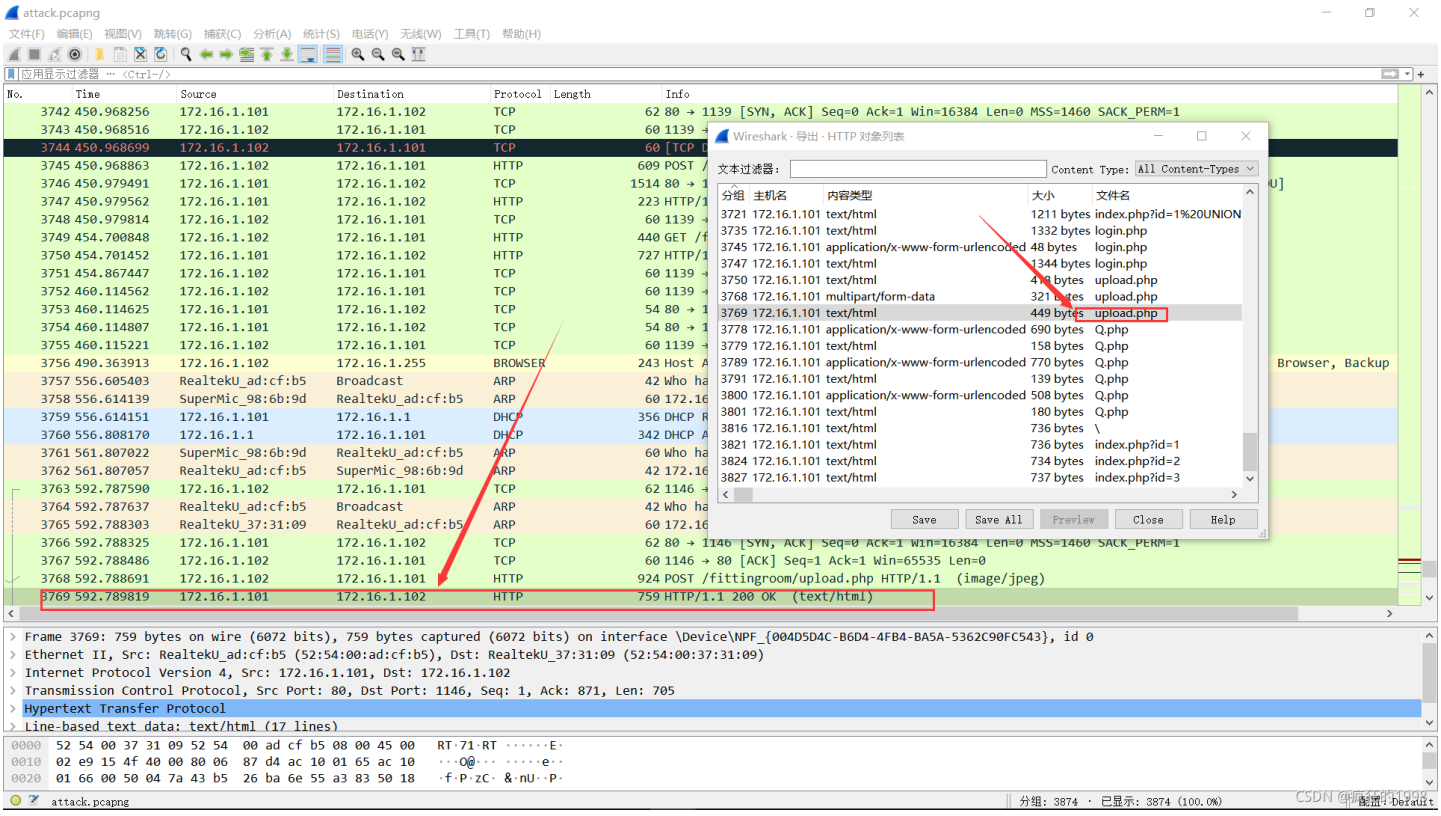
第三题flag便是 [Lancelot]

第四题flag便是 [12369874]

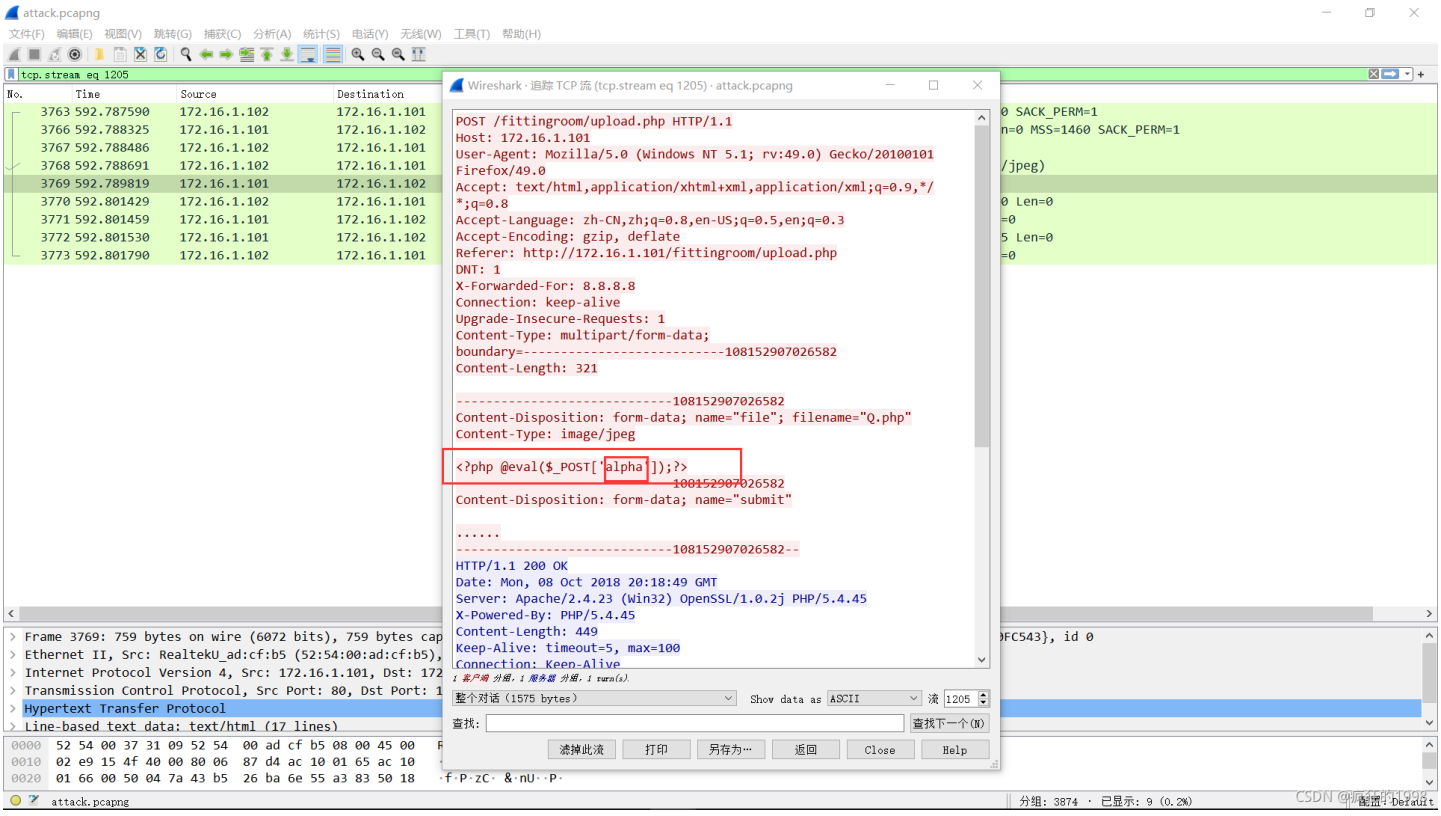




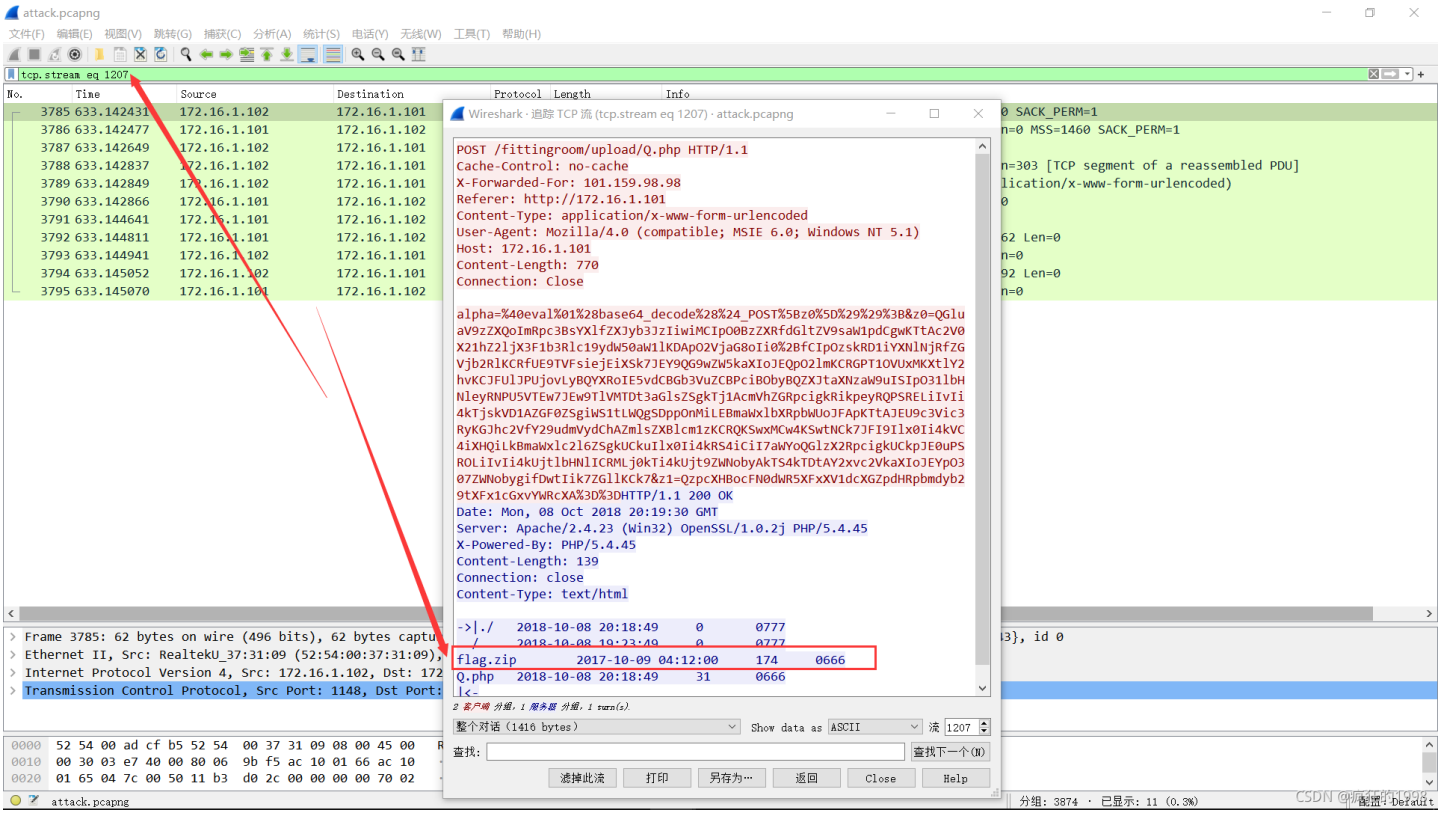
5、第五题要找木马密码，同样的思路，跟第3、4题思路一样，找导出http看木马可能会在upload上传点，果然可以看到有个upload.php



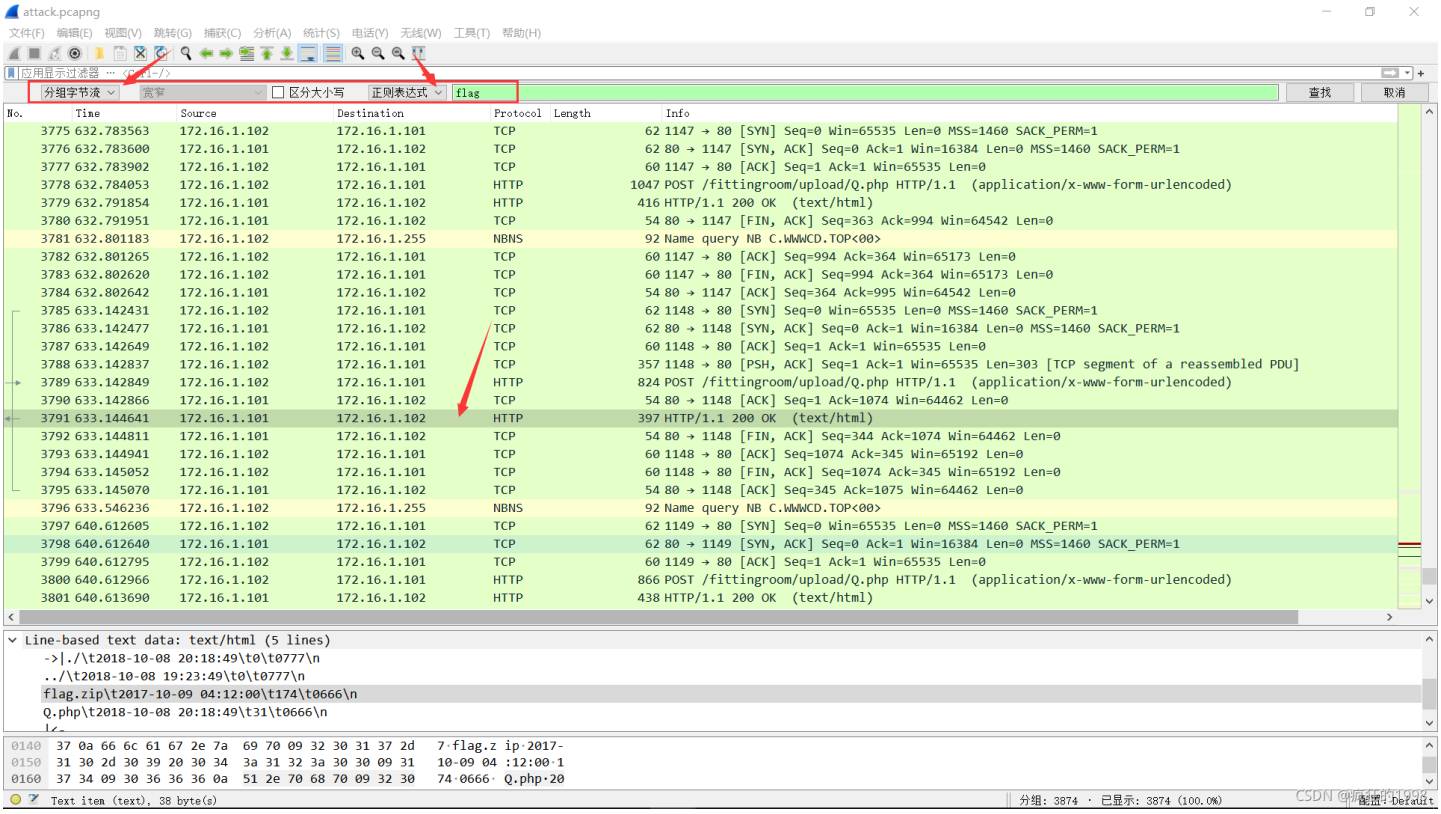
一样的道理，追踪TCP流得到木马密码，flag便是 [alpha]



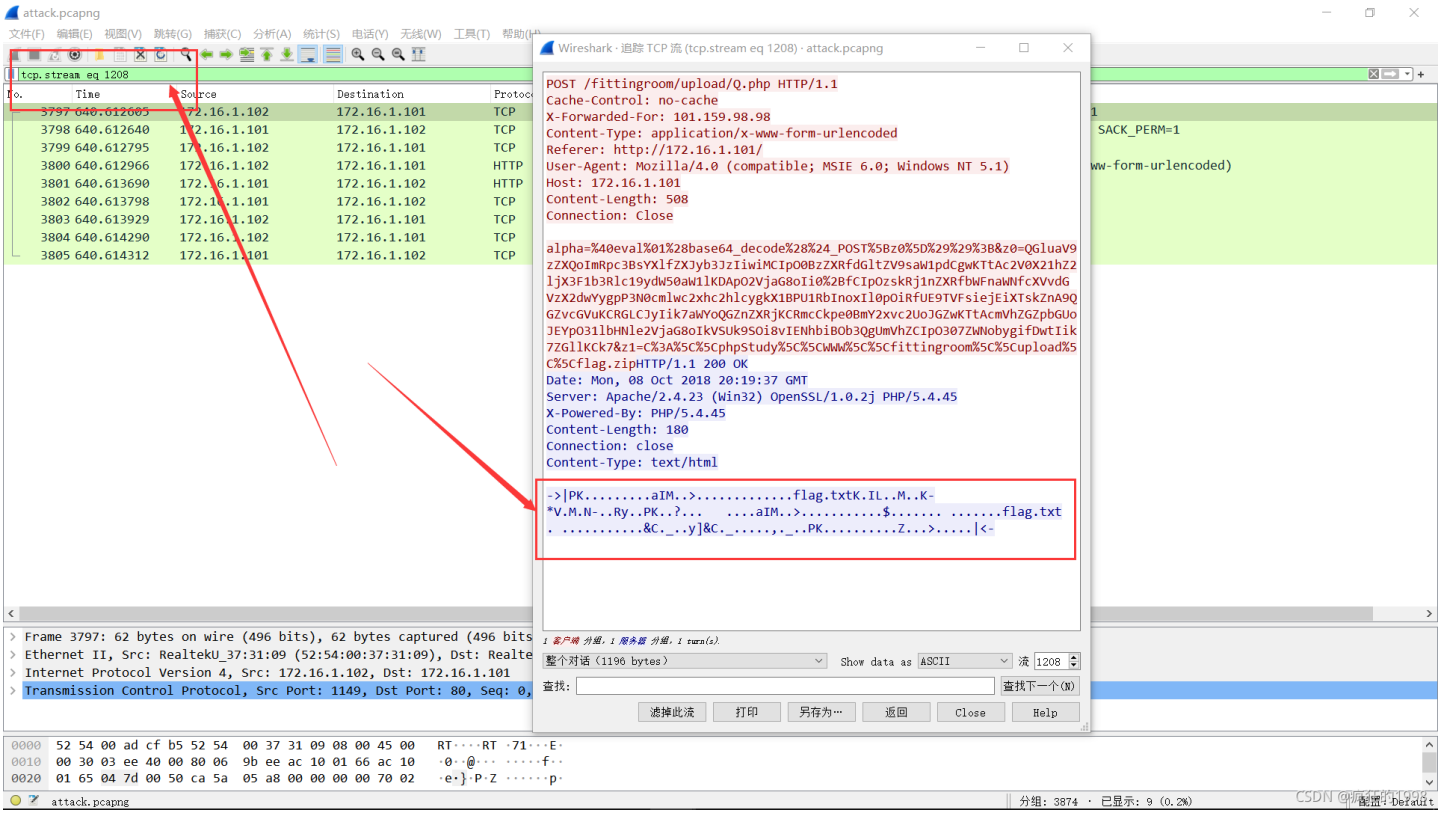
6、取出黑客下载的文件名字以及后缀，跟前面一样找攻击点，但是这次在导出并没有分析出有用的东西，这边我的方法有些另类，因为这种题肯定是按照流程出的，所以后面的flag必定在前面的基础之上的，所以我依旧追踪http看upload并对他进行TCP流追踪，然后关闭追踪选项，在上面过滤处tcp.stream eq 1205 往后进行过滤并且进行大致的TCP追踪（就只看第一条或后面几条流量），发现tcp.stream eq 1207有猫腻，看到flag.zip估计是答案了，便得到flag为[flag.zip]



（其实还有一种做法就是搜索flag,分组字节流搜flag刚好会显示那条流量也是跟上面追踪TCP得到的结果一样）

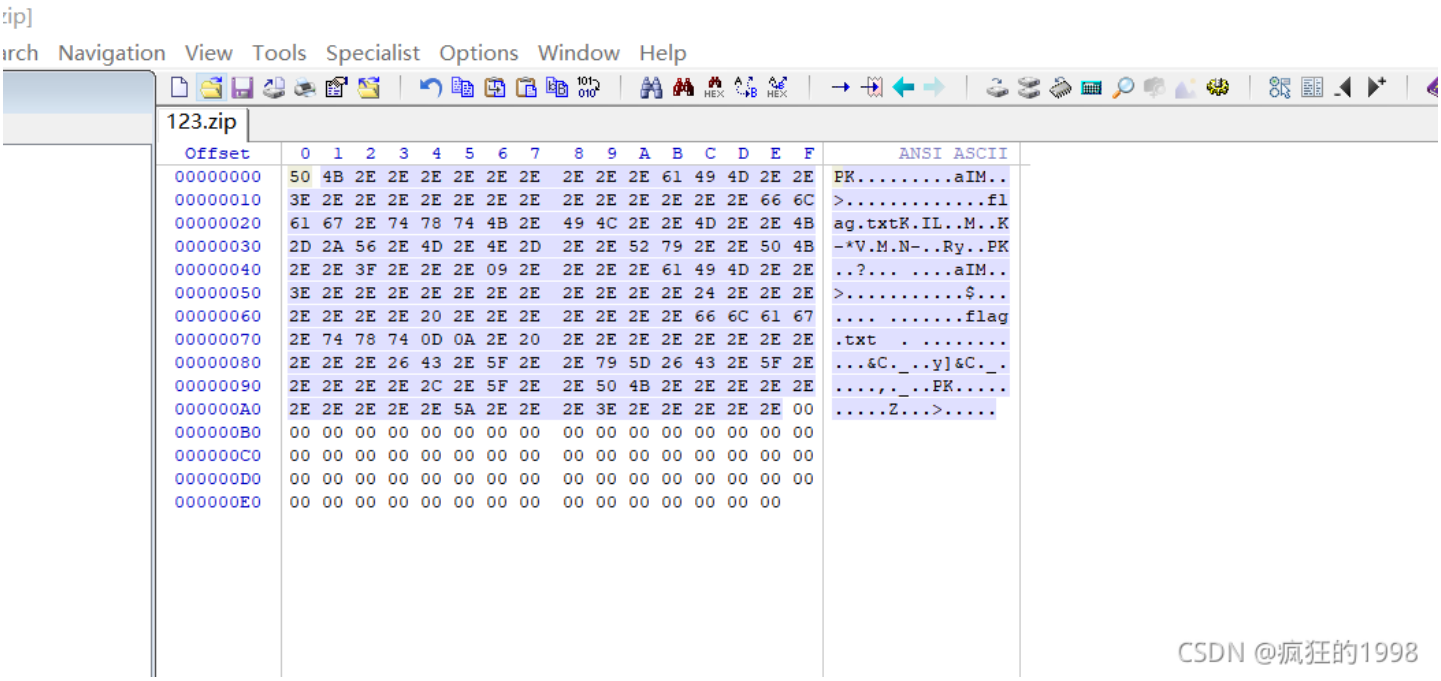


7、最后一题提取出黑客下载的文件（这边思路弯了），并将文件里面的内容为FLAG，这题有问题跟第6题思路一样，换过滤号，往后面分析 tcp.stream eq 1208 并且对第一条进行TCP流追踪，发现zip格式的ascii，将其提取放入hex保存

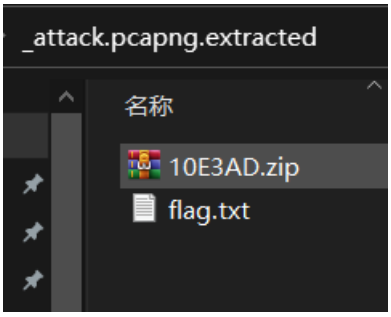


得到的ascii：

PK…aIM…>…flag.txtK.IL…M…K-*V.M.N-…Ry…PK…?.. …aIM…>…$… …flag.txt
. …&C.…*y]&C.…,._…PK…Z…>…



其实很明显zip开头是504B0304这显然有问题，压缩包恢复不了，直接凉凉，到这里发现是思路问题
将其放入kali中进行分离流量包，binwalk -e分离可得



其中打开第一个压缩包(存在伪加密，直接用360压缩打开）便是flag.txt一样的文件

flag{Manners maketh man}