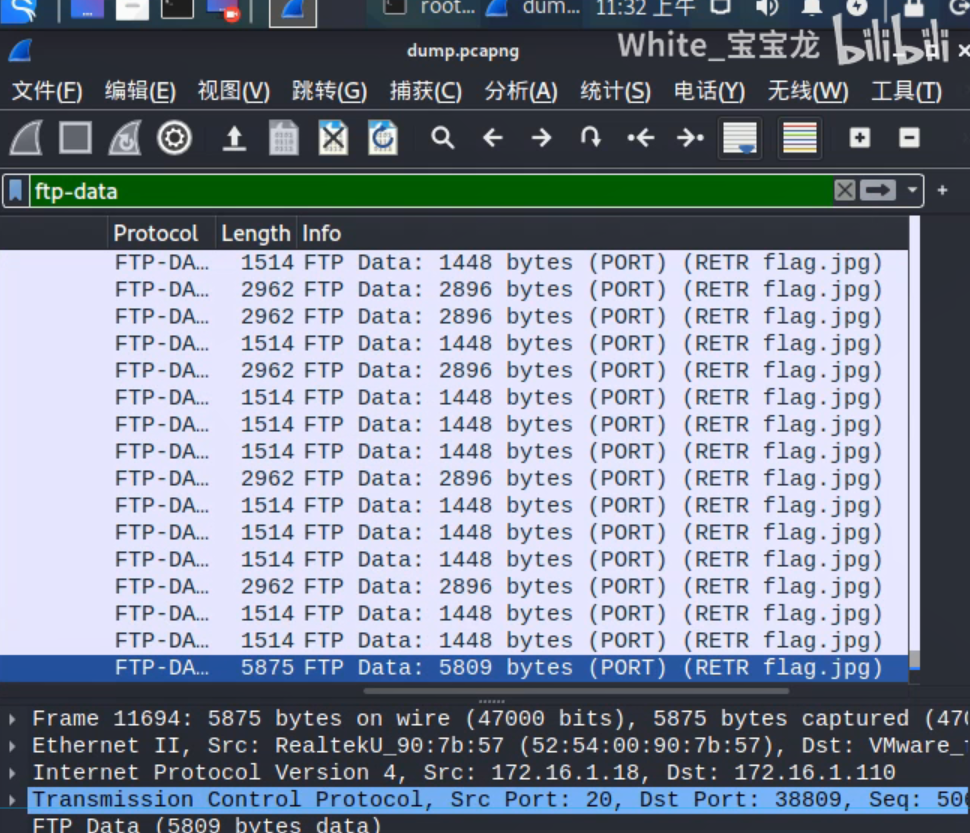
**数据包分析**

**找黑客IP**

过滤条件 http，主要看自己分析，比如黑客大量发包和目录扫描和渗透操作等等攻击，就可以分析出两个ip随便猜两下就出来了，并没有特别厉害的偷分过滤规则

**查看ftp下载**

**了什么就用ftp-data**

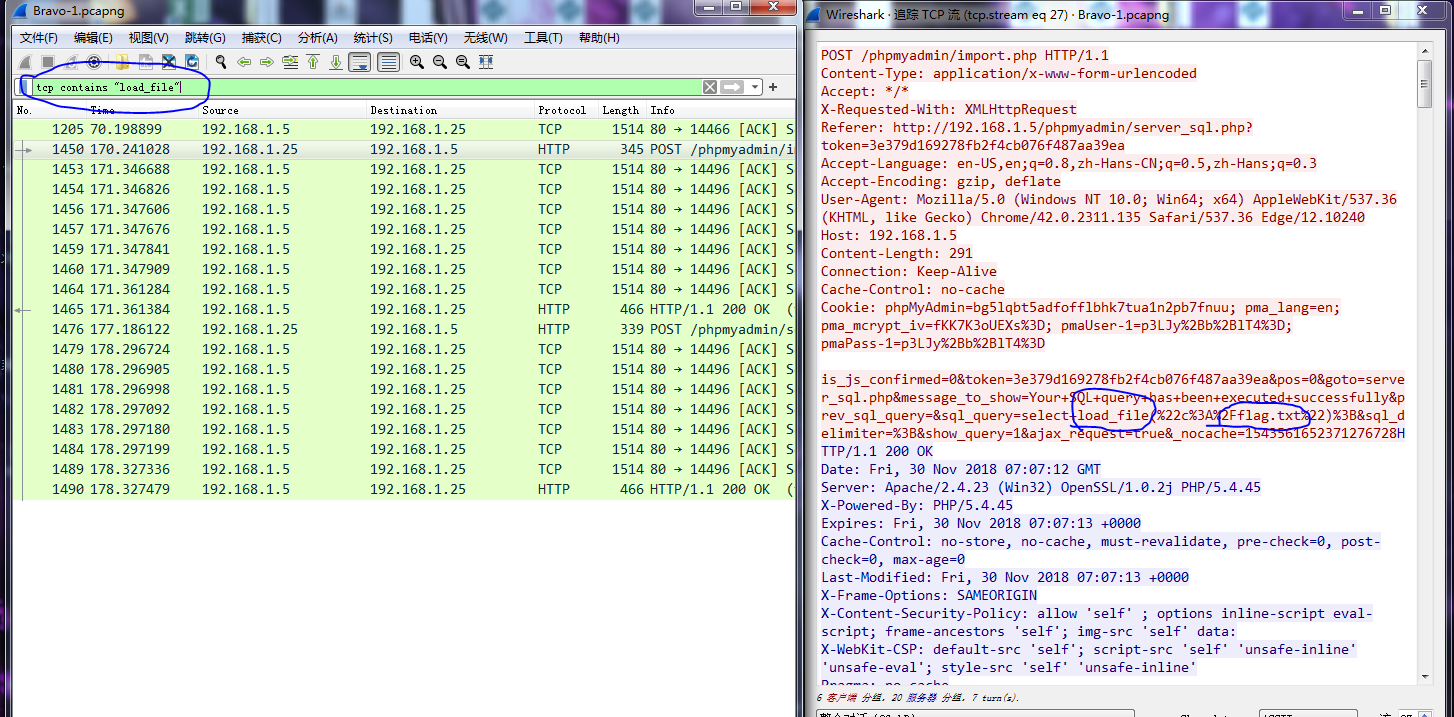


**找黑客从php中读取的文件**

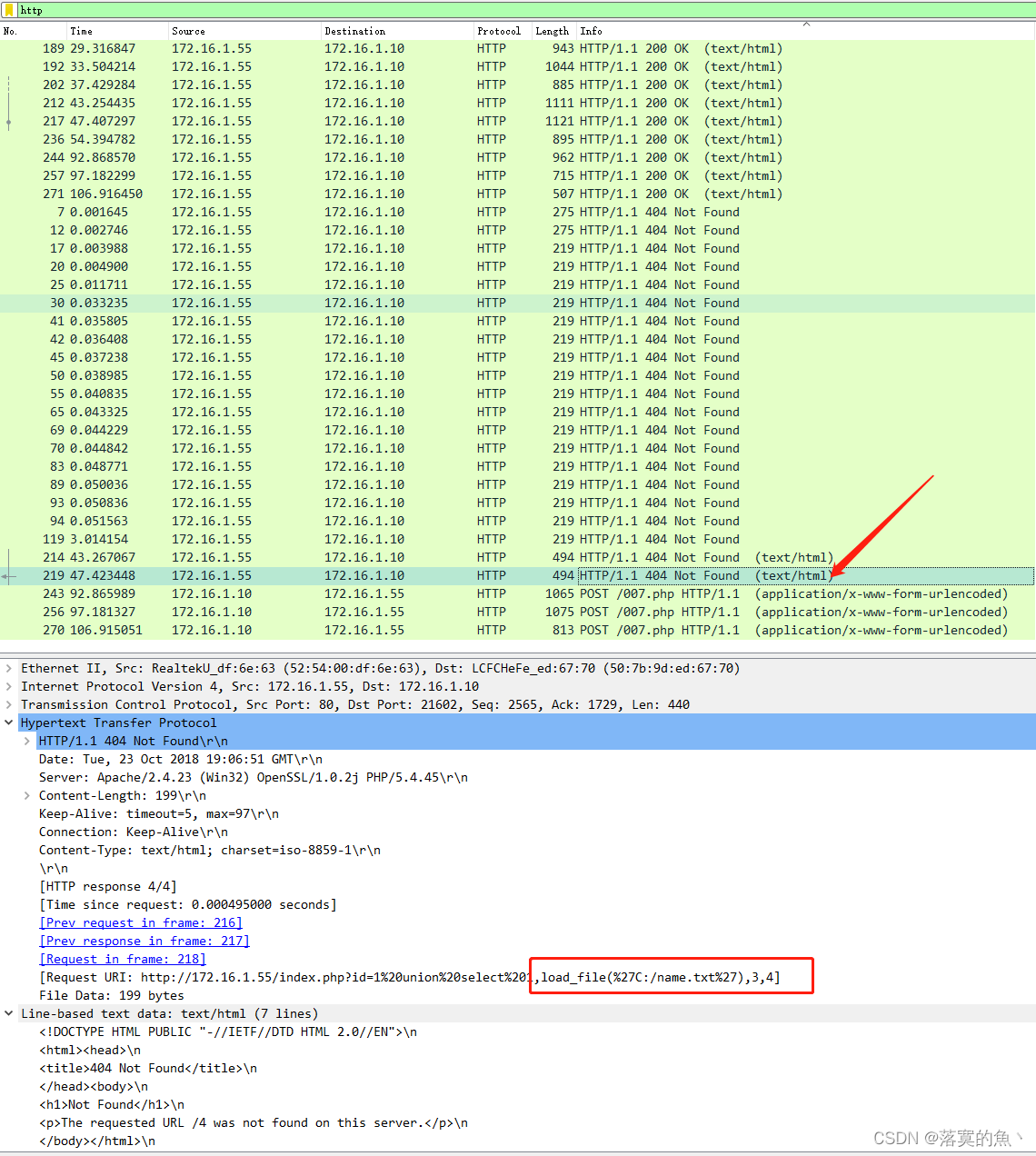
3.继续查看数据包文件分析出恶意用户读取服务器的文件名是什么，并将该文件名作为FLAG（形式：[robots.txt]）提交；

从php数据库使用php语言读取文件一般是load\_file函数所以我们直接搜查关键字

tcp contains "load\_file"

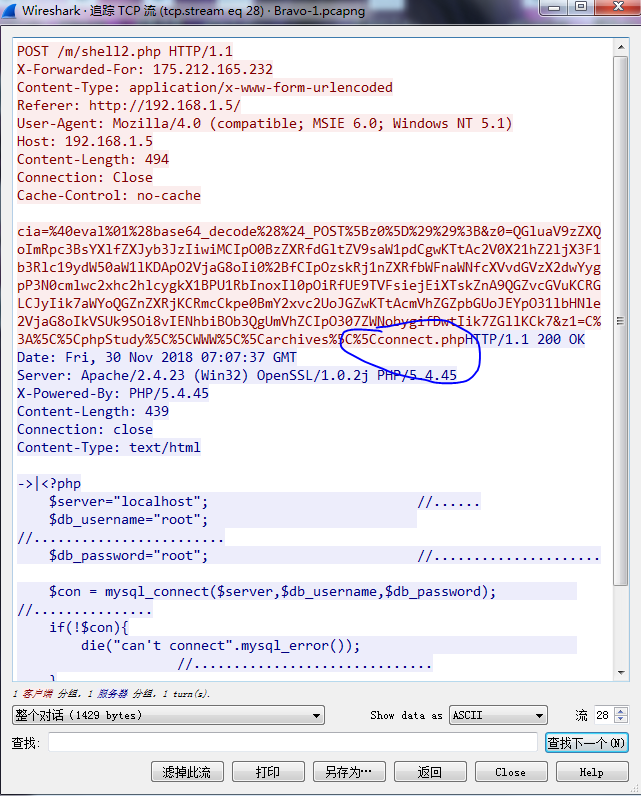


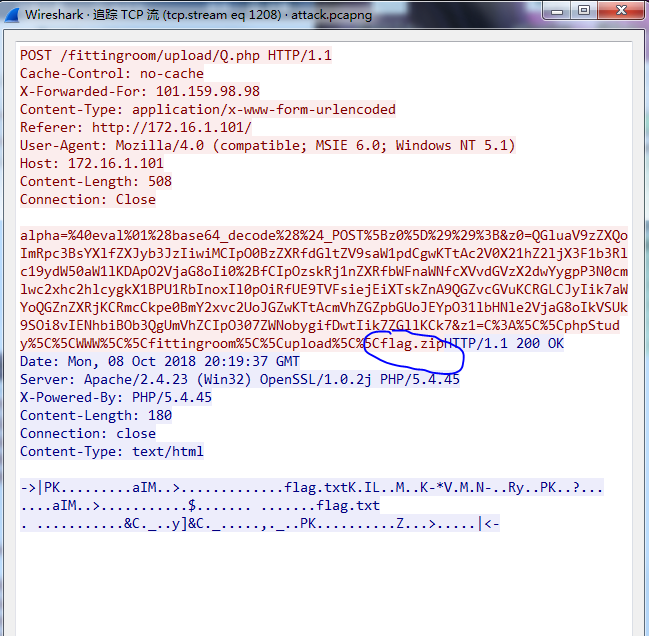
例2



7.继续查看数据包文件将恶意用户下载的文件里面的内容作为Flag值（形式：[文件内容]）提交。

（一般是跟在一句话木马的密码后面）



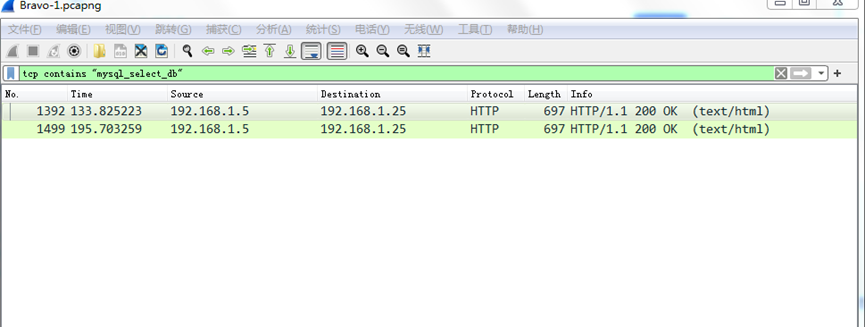


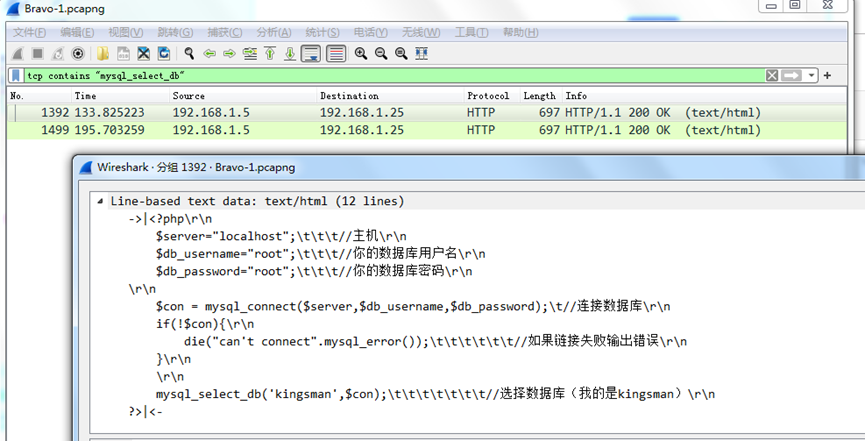
**找连接的数据库名**

7.继续查看数据包文件Bravo-1.pcapng将Web服务器连接的数据库名作为Flag值提交。

php中的mysqli\_select\_db() 函数用于更改连接的默认数据库

Tcp contains “mysql\_elect\_db”

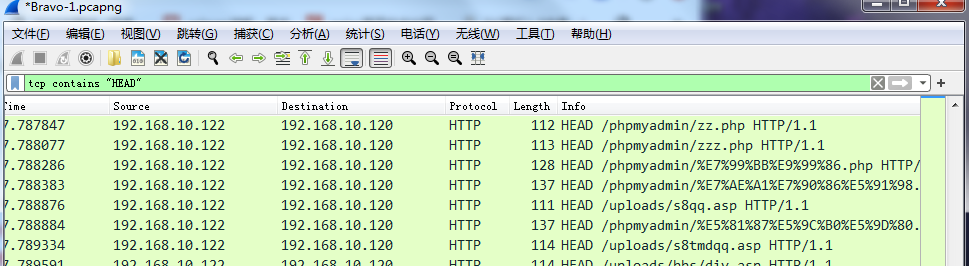




Flag: kingsman

**分析目录扫描**

1.分析Server8桌面下的Bravo-1.pcapng数据包文件，通过分析数据包Bravo-1.pcapng找出恶意用户目录扫描的第2个目录名，并将该目录名作为Flag值提交;



分析扫描流量可以看到，扫目录的请求头一般为HEAD，所以

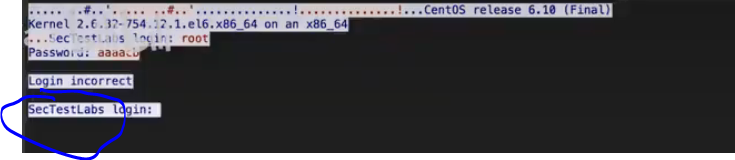
tcp contains “HEAD”

flag{/uploads}

**找靶机的主机名字**

**telnet找到登录的主机名字**

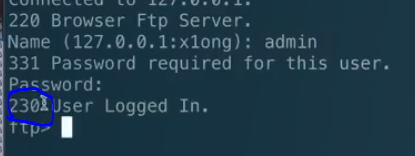
**telnet登录时候会回显**



ftp找到黑客登录的账号密码（root,toor）(ftp登录成功都会返回230状态)

过滤规则

ftp|telnet|http contains "230" 或 ftp contains "success"



黑客执行命令LIST，一般是dir，ls

**找一句话木马**

分析A.pcapng数据包，找到黑客的一句话木马的密码，将该密码作为flag提交：

在显示过滤器中输入:ip.addr==192.168.10.12and http contains “@eval”

或有可能是 ip.addr==192.168.10.12and http contains “$\_GET”

Flag{oo}

**找补丁号**

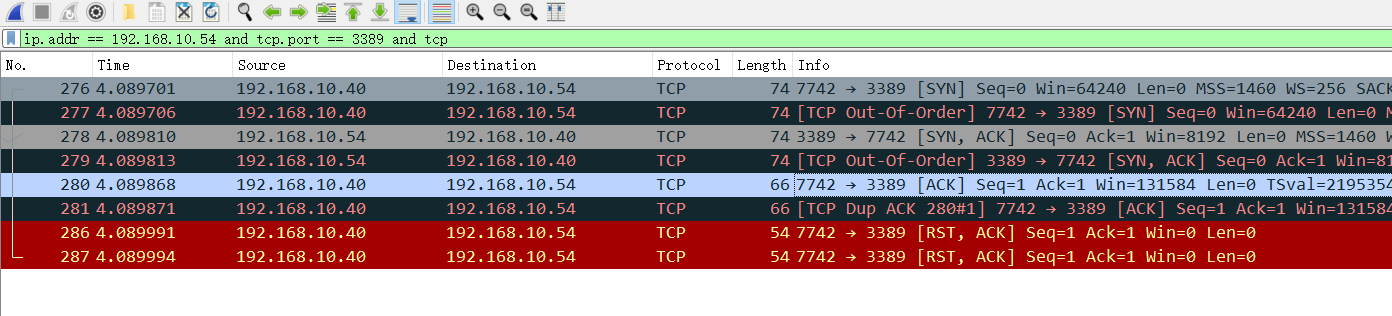
通过分析数据包，找到服务器安装的第一个修补程序

http contains “KB”

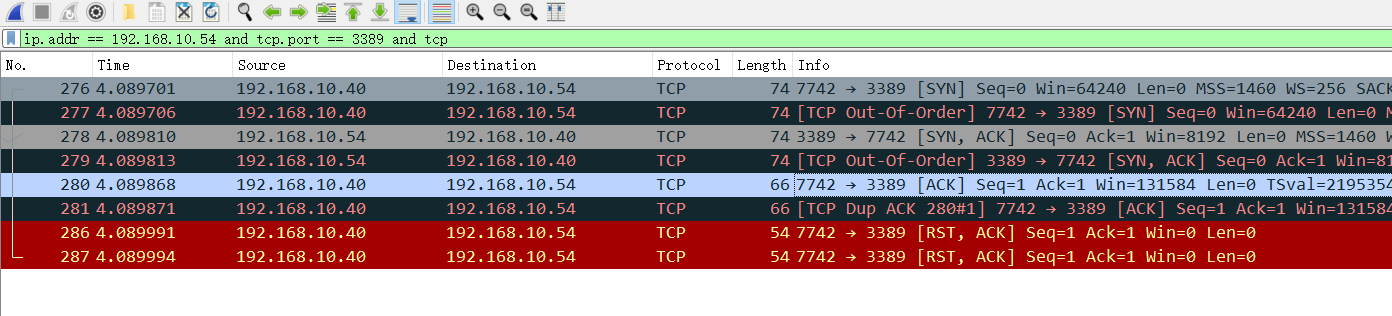
找到黑客扫描的IP地址网段，从上一题可以得到黑客的IP地址为192.168.10.12.看一下arp协议的数据

如下图若端口是打开的，返回了SYN,ACK则表明端口开放，然后扫描主机箱目标机发送ACK/RST包断开连接。

**判断某个端口是否开放验证（黑客nmap扫开的端口）**



如果端口是关闭的，则会直接返回RST/ACK报文断开连接，说明端口是关闭的。



该种方法进行扫描会留下扫描纪录，而且速度较慢

先找靶机IP

ip.src==靶机ip 一般到最下面它会有个总结 开启颜色放便一些

ip.src==攻击机ip and tcp.flags.reset==0

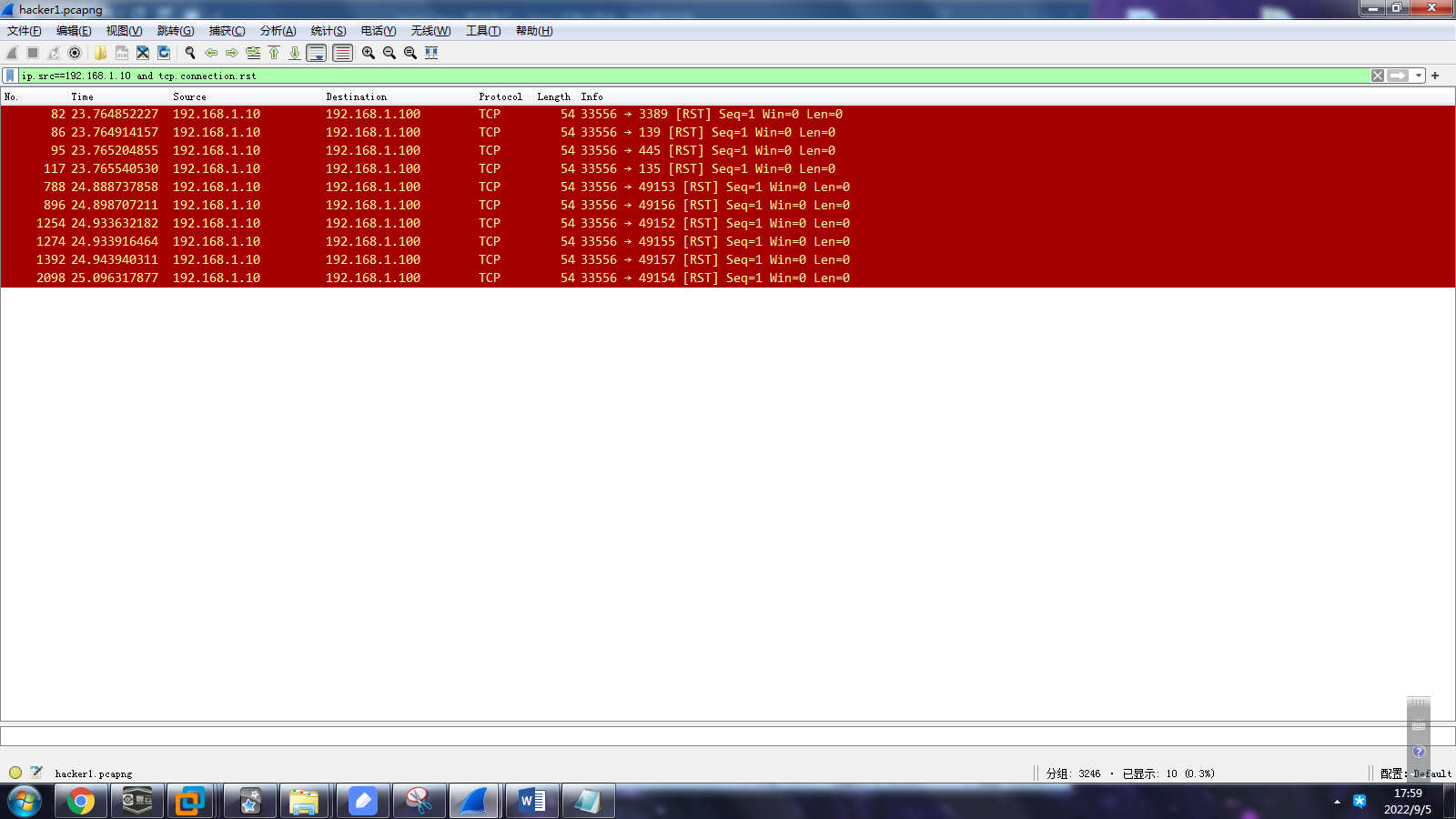
可以用下面这个命令测试如果开了端口就会返回【 SYN,ACK】

ip.addr==172.16.123.115 and tcp.port == 88

**找黑客IP扫描到开发的端口**

还有这种方法可以查看开放端口虽然是红的

ip.src==黑客ip and tcp.connection.rst



**考三次握手的过滤规则**

使用Wireshark查看并分析PYsystem20191桌面下的capturepcap数据包文件，通过设置过滤规则，要求只显示三次握手协议过程中的RST包以及实施攻击的源IP地址，将该过滤规则作为Flag值（存在两个过滤规则时，使用and连接，提交的答案中不包含空格，例d如tcp.ack and ip.dst == 1716.1.1

则Flag为tcp.ackandip.dst==172.16.1.1）提交；

过滤参数是：tcp.connection.rst and ip.src==172.16.123.112

flag:tcp.connection.rstandip.src==172.16.123.112

过滤为POST

http.request.method == POST

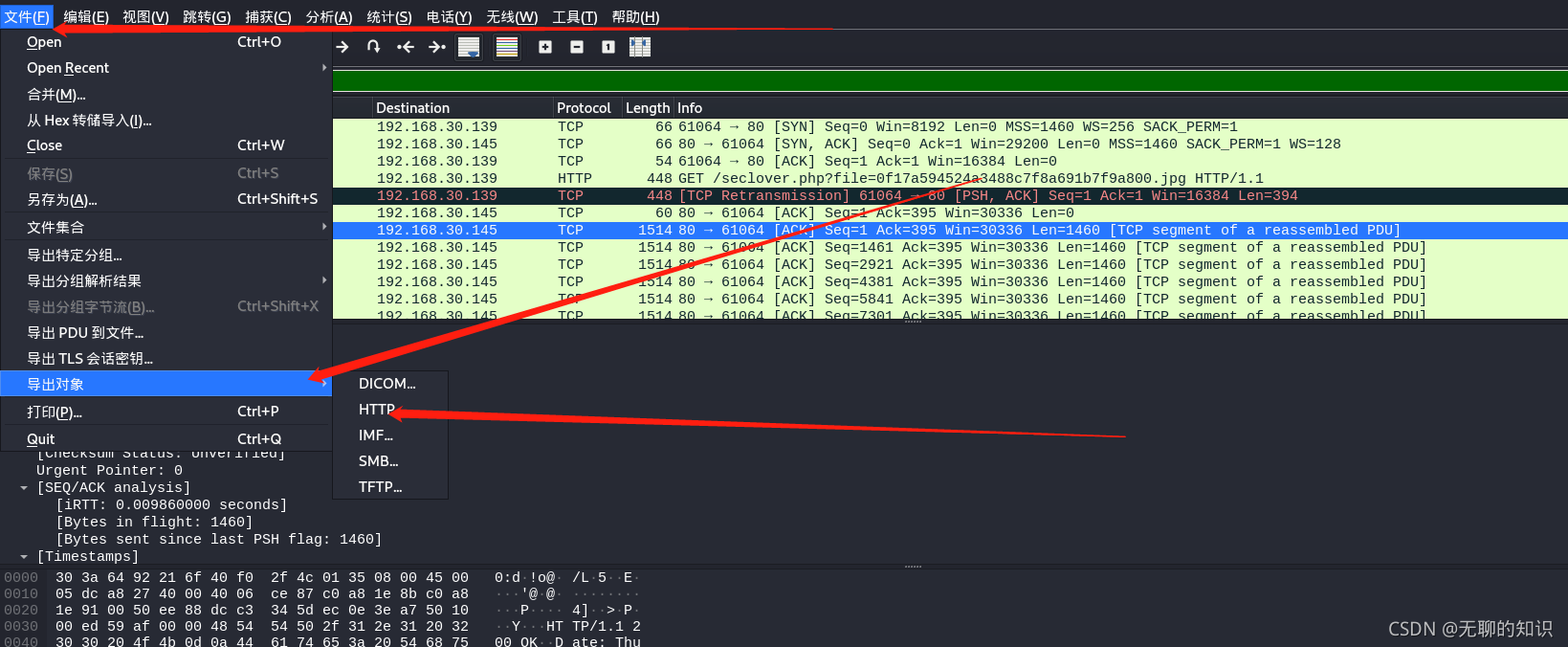
**tcpxtract 命令从pcap提取照片**

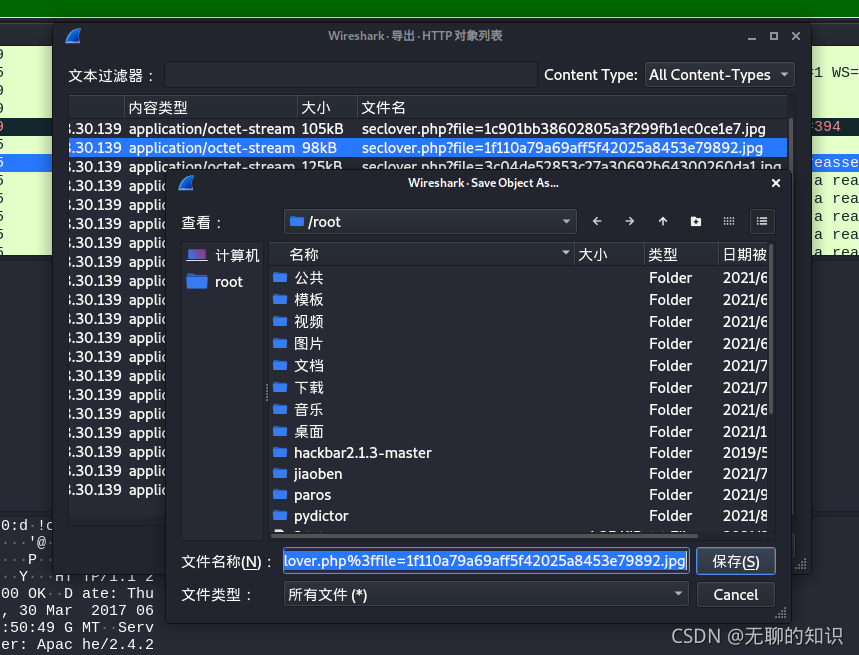
tcpxtract -f 434c8c0ba659476caa9635b97f95600c.pcap

**当tcpxtract或foremost提照片有问题就用这个办法**

打开菜单栏中的导出文件

选择导出的位置





最近需要解析HTTPS流量，所以对[wireshark](https://so.csdn.net/so/search?q=wireshark&spm=1001.2101.3001.7020)的HTTPS解密进行了实测。

使用wireshark解密https的方法

方法一：

1、在wireshark的首选项中的protocols的tls选项里添加服务器[私钥](https://so.csdn.net/so/search?q=%E7%A7%81%E9%92%A5&spm=1001.2101.3001.7020)文件。p12文件需要填写密码。

