## 实验环境

服务器：Windows 7 ，IP地址：随机分配

辅助工具：Wireshark

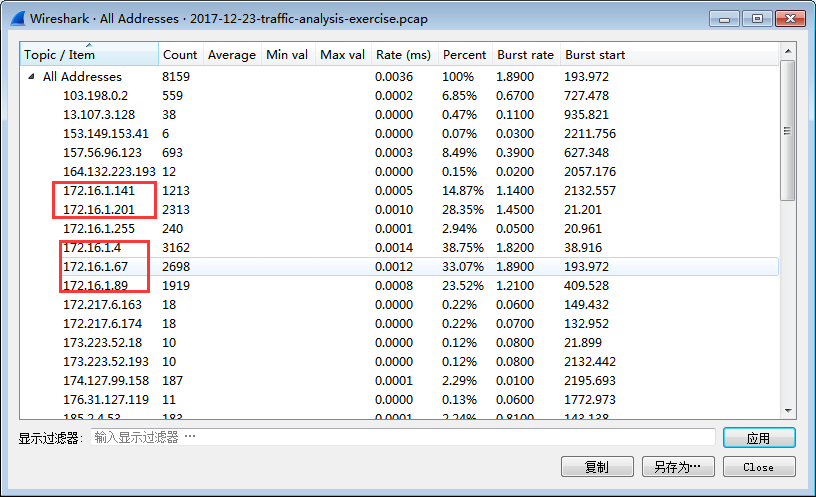
**注：**本课程所有访问互联网操作均不能在实验机内操作，旨在学习方法，可用自己电脑体验具体过程。

### 任务：检查pcap数据包查找出哪台主机感染了什么恶意软件。

       首先我们要确定局域网内几台主机

       Wireshark加载之后，点击上方菜单统计-->ipv4 statistics-->all address

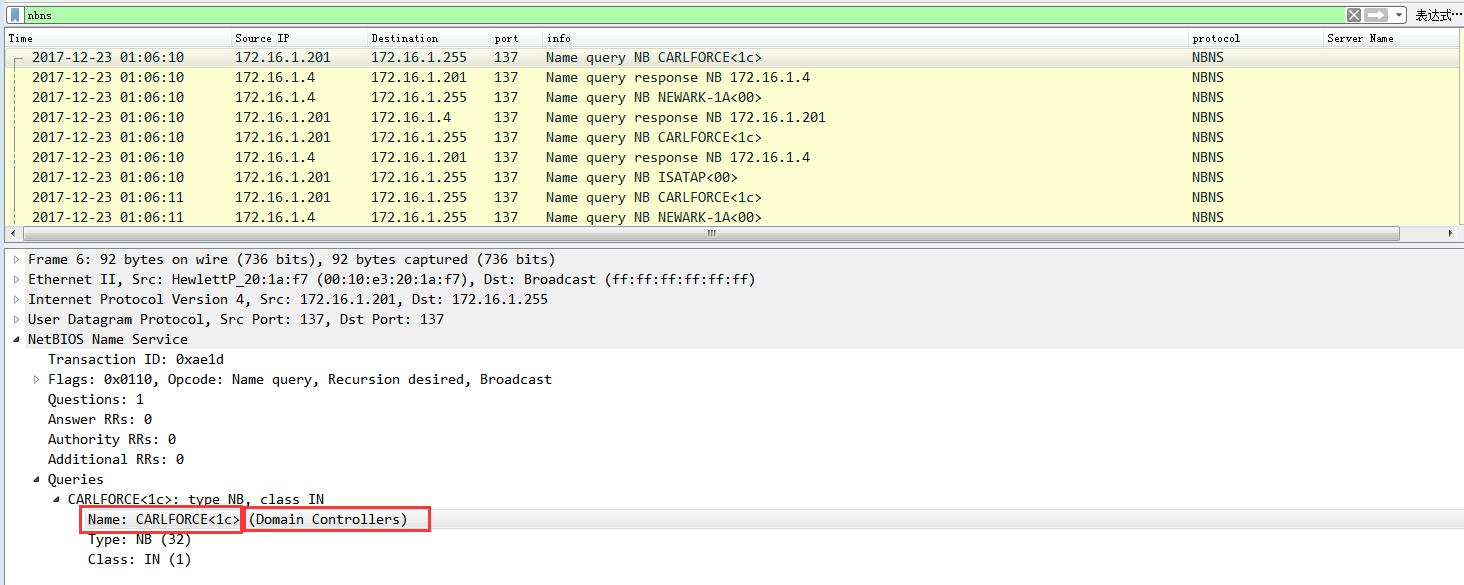
       从结果中可以看到共有5台主机



       接下来我们需要找到各个ip的主机名

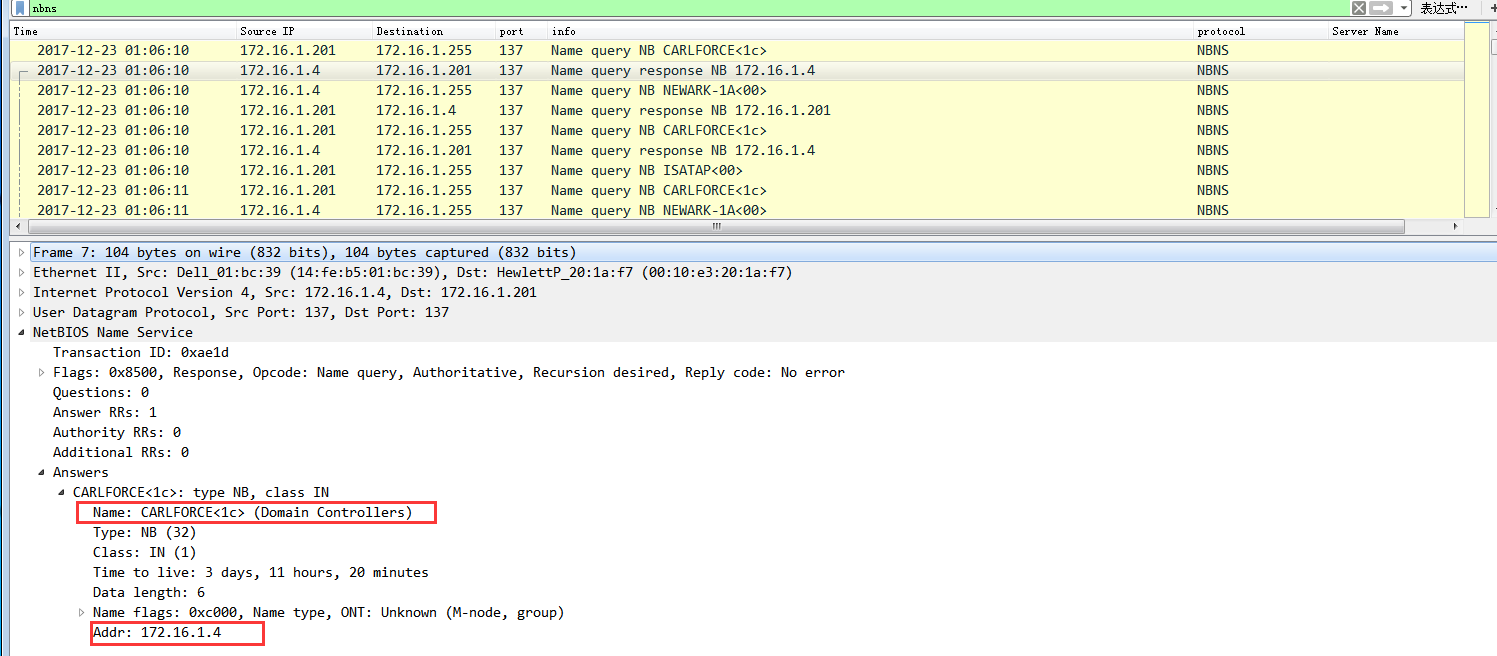
       我们前面的实验中知道可以通过nbns来找到主机名

       所以尝试使用nbns过滤



       第一条发现172.16.1.201发起了一个广播包，在红框中可以看到是域控，主机名为CARLFORECE

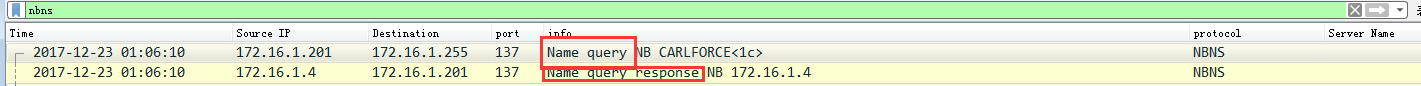
       继续看第二条



       发现不对劲的地方了吗？

       主机名还是CARLFORCE，这是怎么回事呢？

       我们仔细看这两条包的区别



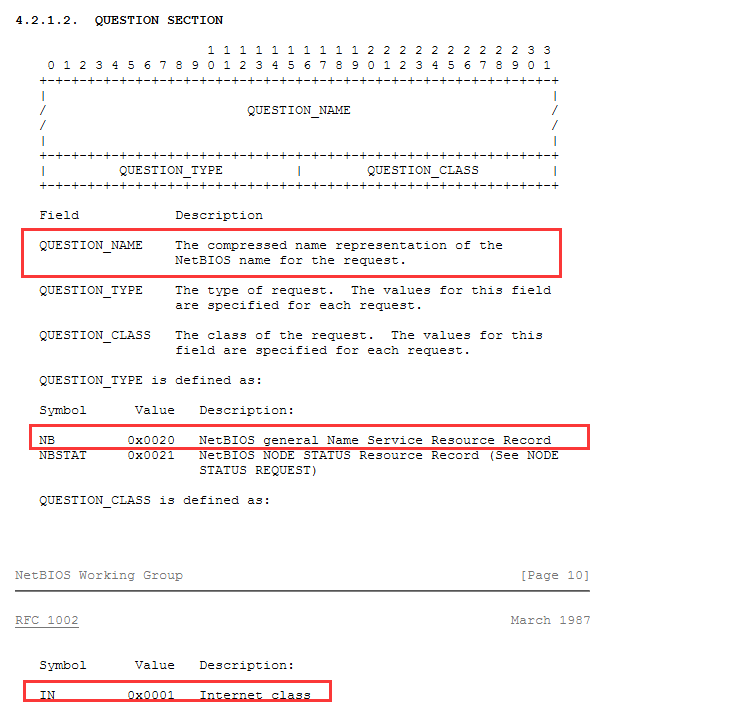
       172.6.1.201发起的是查询包，172.16.1.4发出的是响应包

       我们还是去看看RFC文档：[https://tools.ietf.org/html/rfc1002](https://tools.ietf.org/html/rfc1002" \t "http://www.hetianlab.com/pages/teacher/_blank)。

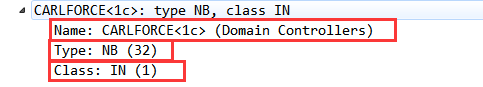
       仔细看看第一条可以看到目的ip为172.16.1.255,说明这是广播包，用于NBNS广播查找

IMG_260

       结合报文格式



       与我们第一条数据包有关的部分我已经用红框划重点了。结合数据包的实例

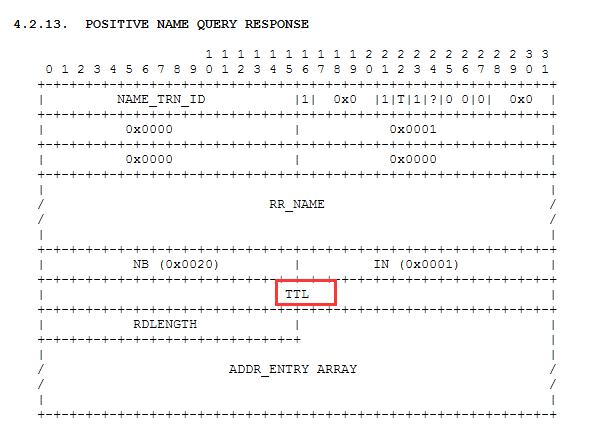


       可以知道172.16.1.201是在请求查询netbios名为CARLFORCE的机器

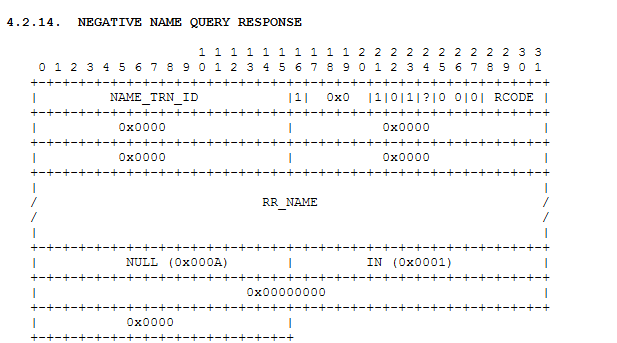
       Type为NB，表示类型是通用名称服务资源记录（注意，RFC中的0x0020就是10进制的32）

       Class为IN，表示类为Internet，一般都是默认的

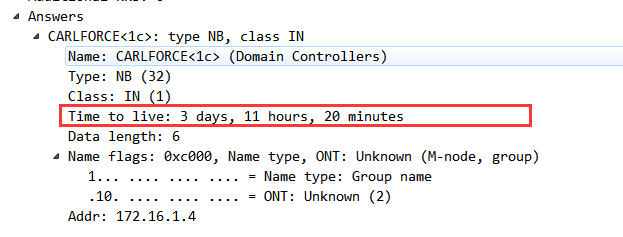
       然后分析第二条，第二条是对第一条的响应，我们在RFC文档中可以看到有两种响应，一种是主动的



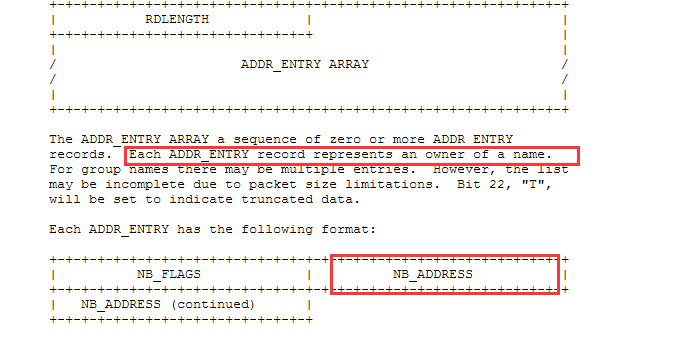
       一种是被动的



       结合第二条数据

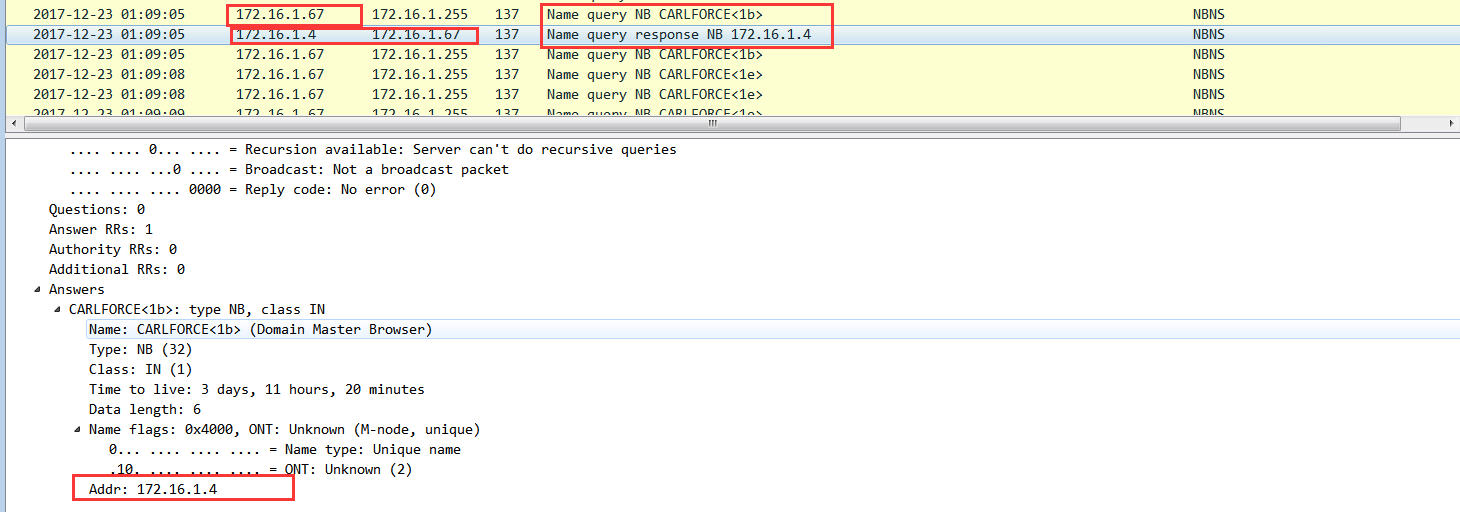


       可以判断出这是属于主动响应，既然是主动分析，我们要着重分析ADDR\_ENTRY ARRAY



       有圈出的话可以知道ADDR\_ENTRY记录反映了主机名的所有者信息，所有者的ip在NB\_ADDRESS中。结合数据包实例可以知道，172.16.1.4对应的主机名为CARLFORCE

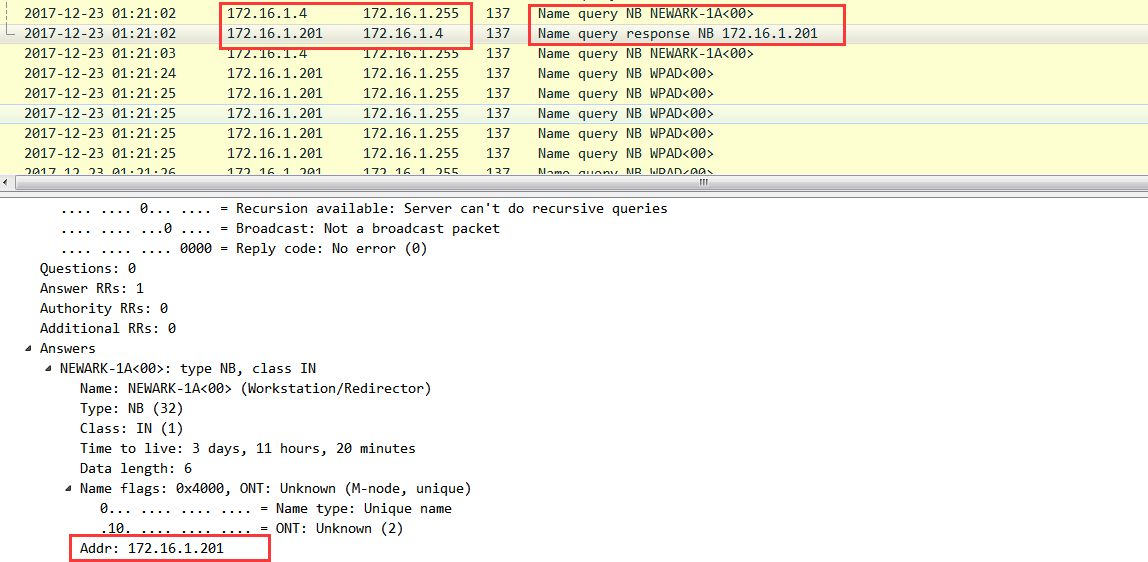
       或者我们从下面这两条数据也可以看出来



       172.16.1.67在查询CARLFORCE，然后172.16.1.4回应172.16.1.67，告诉172.16.1.67CARLFORCE对应着172.16.1.4

       可以说，找到一条不同的namequery response就能找到其他ip与name对应的信息

       我们继续往下找看看有没有



       上图中可以看到172.16.1.4查询NEWARK-1A的信息，然后172.16.1.201回复172.16.1.4，告诉它NEWARK-1A对应着172.16.1.201

       所以从nbns协议中我们知道：

       NEWARK-1A对应着172.16.1.201

       CARLFORCE对应的主机名为172.16.1.4

       那么其他主机呢？

       现在还剩下

       172.16.1.67

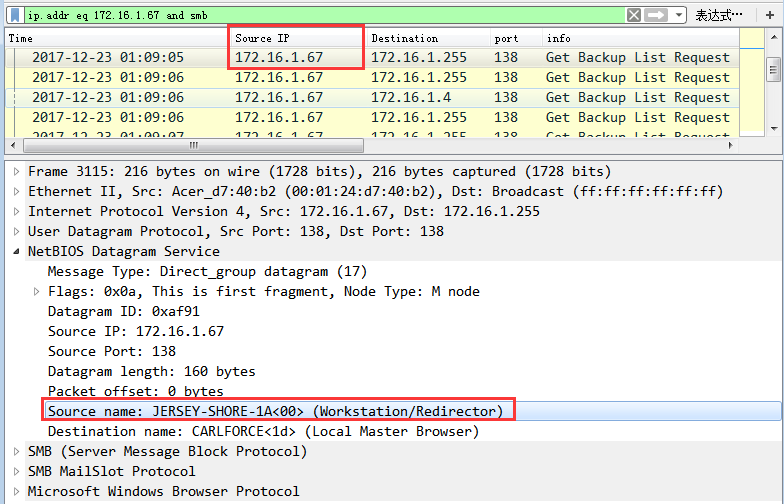
       172.16.1.89

       172.16.1.141

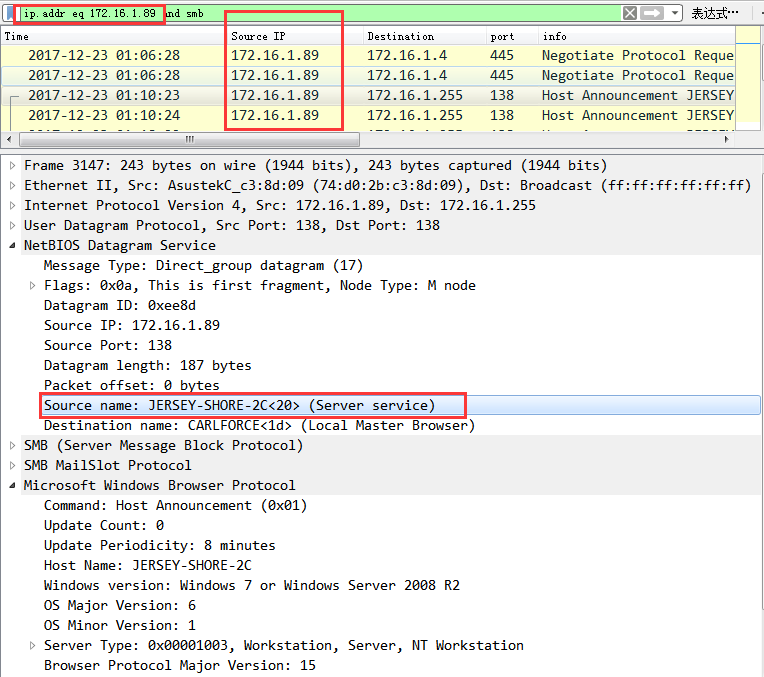
       我们知道SMB使用了NetBIOS的应用程序接口 （Application Program Interface，简称API），也是可以探测到主机名的。

       所以我们可以使用剩余的ip加之smb进行过滤

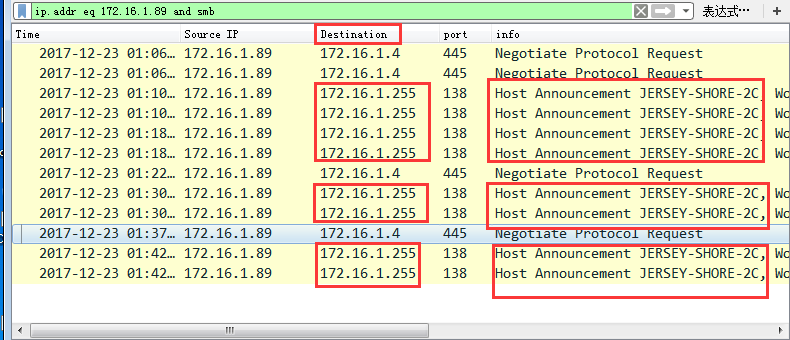
       ip.addr eq 172.16.1.67 and smb



       ip.addr eq 172.16.1.89 and smb

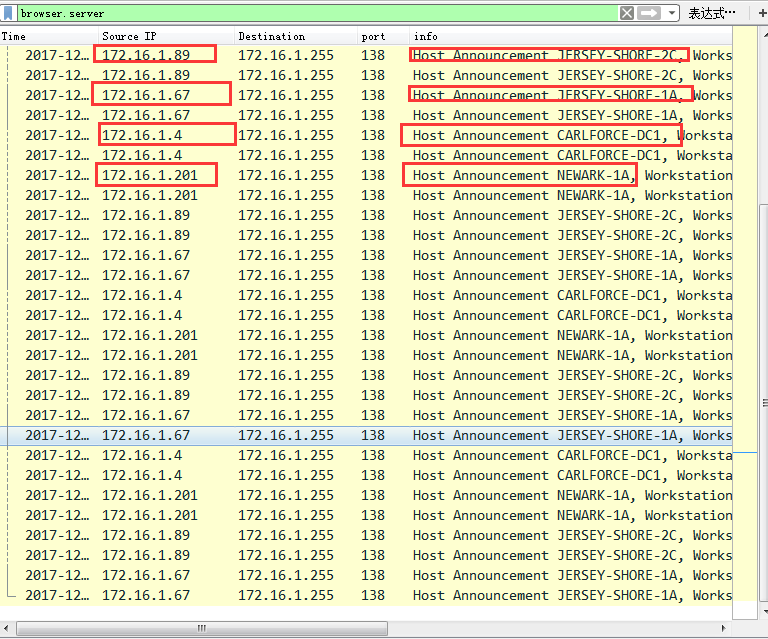


       我们仔细看看，可以发现凡是目的地址为172.16.1.255，即广播包，在info栏里会直接看到对应的主机名



       那么我们是不是可以直接过滤出广播包呢？

       使用browser.server的命令即可过滤

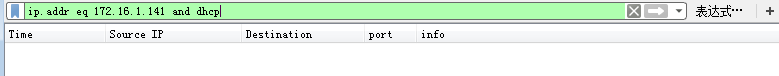


       这也是找主机名的一种简便的方法

       可是172.16.1.141的主机名呢？

       Nbns找不到，smb找不到，我们前面的实验中学过dhcp也可以找主机名我们试试dhcp

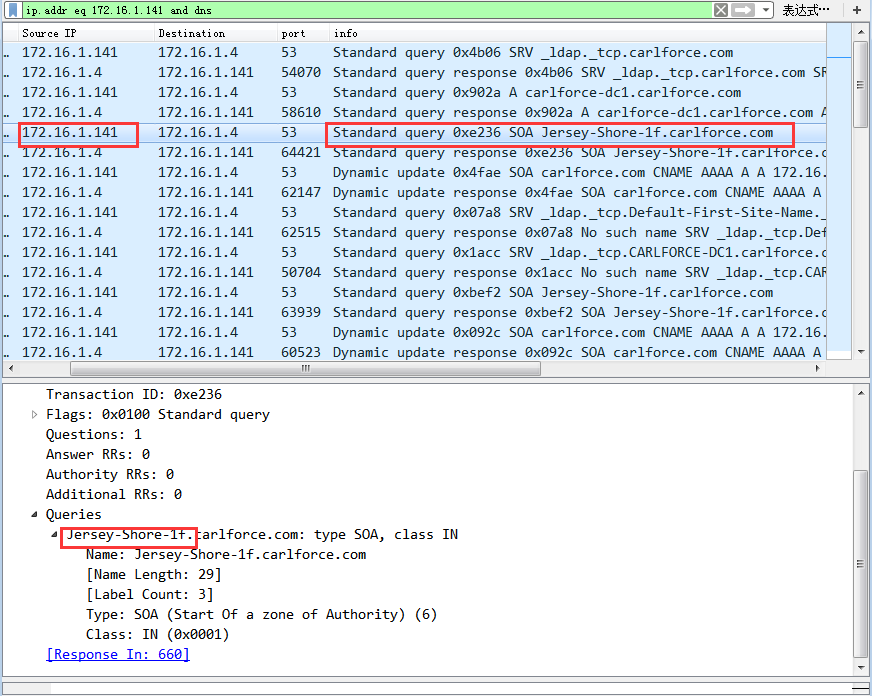
       ip.addr eq 172.16.1.141 and dhcp



       没有记录

       那试试dns呢？Dns也能得到主机名

       ip.addr eq 172.16.1.141 and dns



       可以看到172.16.1.141的主机名为Jersey-Shore-1f

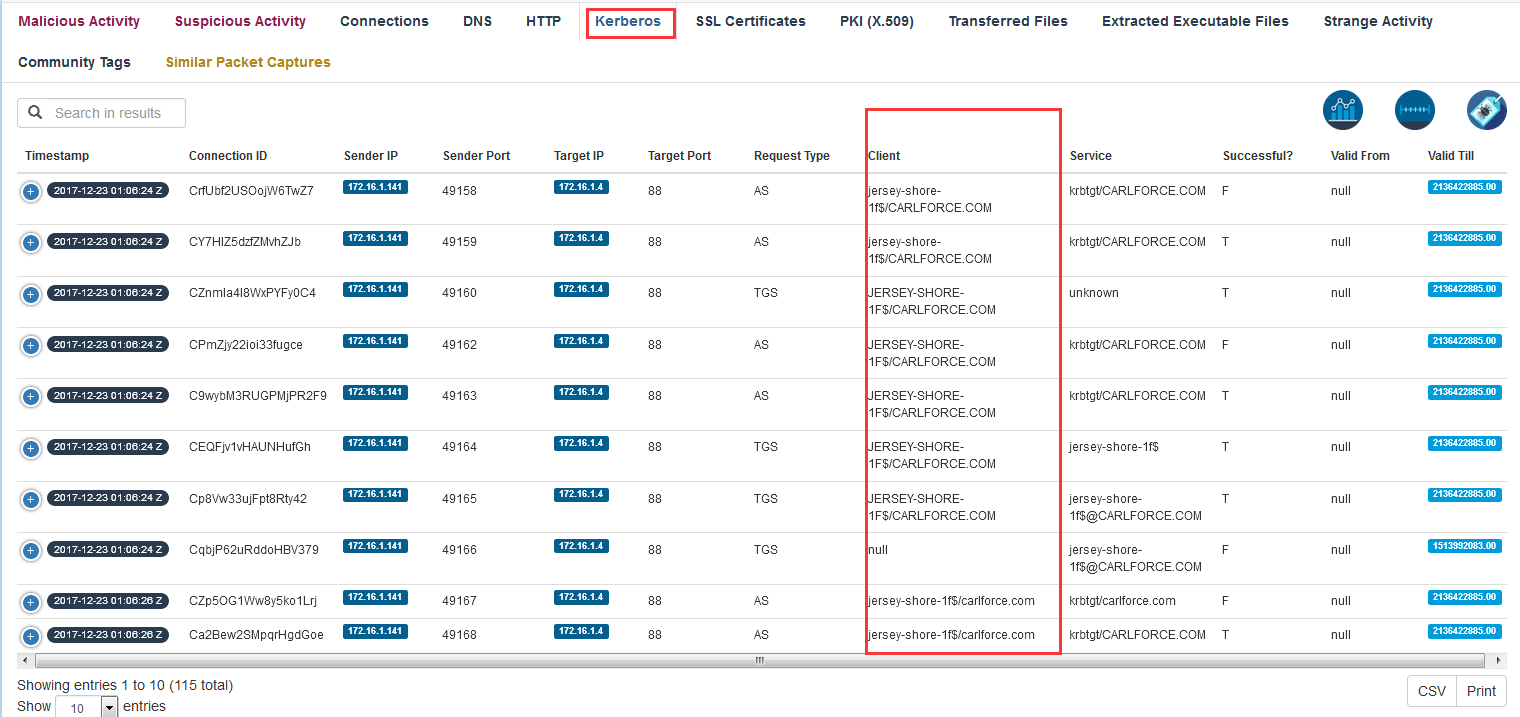
实验步骤二

       接下来我们需要找到各个ip对应的用户账户名

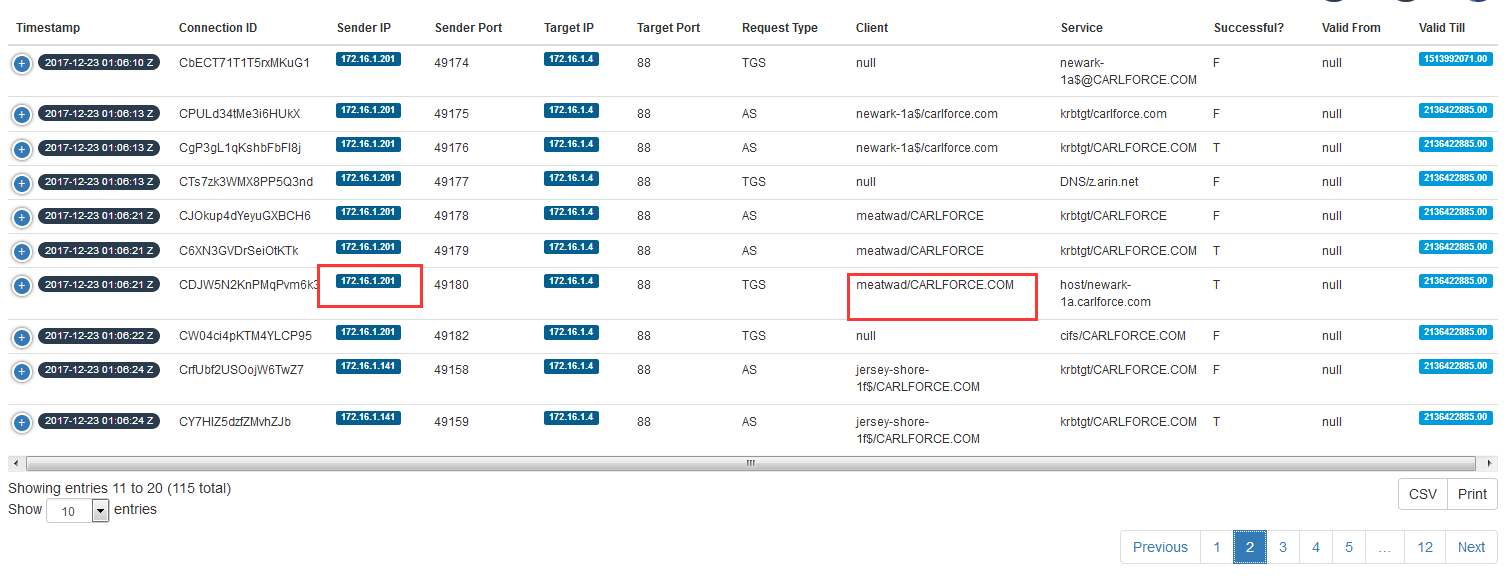
       这里我们使用[https://packettotal.com](https://packettotal.com/" \t "http://www.hetianlab.com/pages/teacher/_blank)，将数据包上传至此进行分析

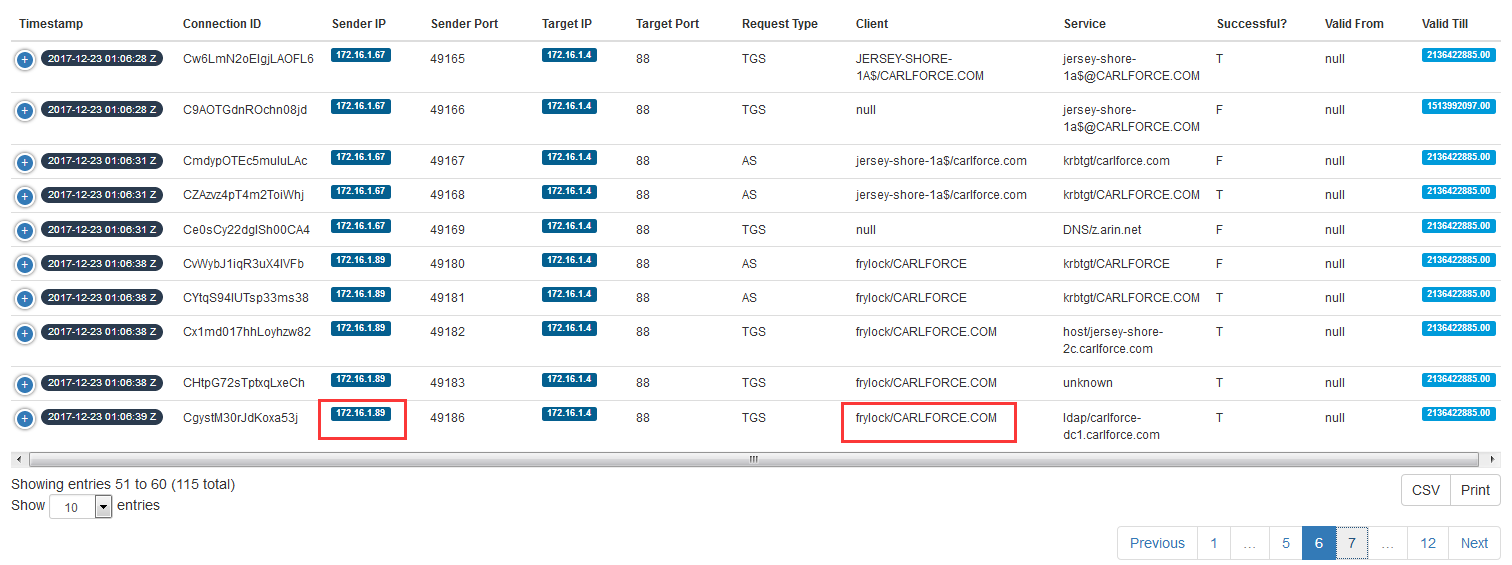


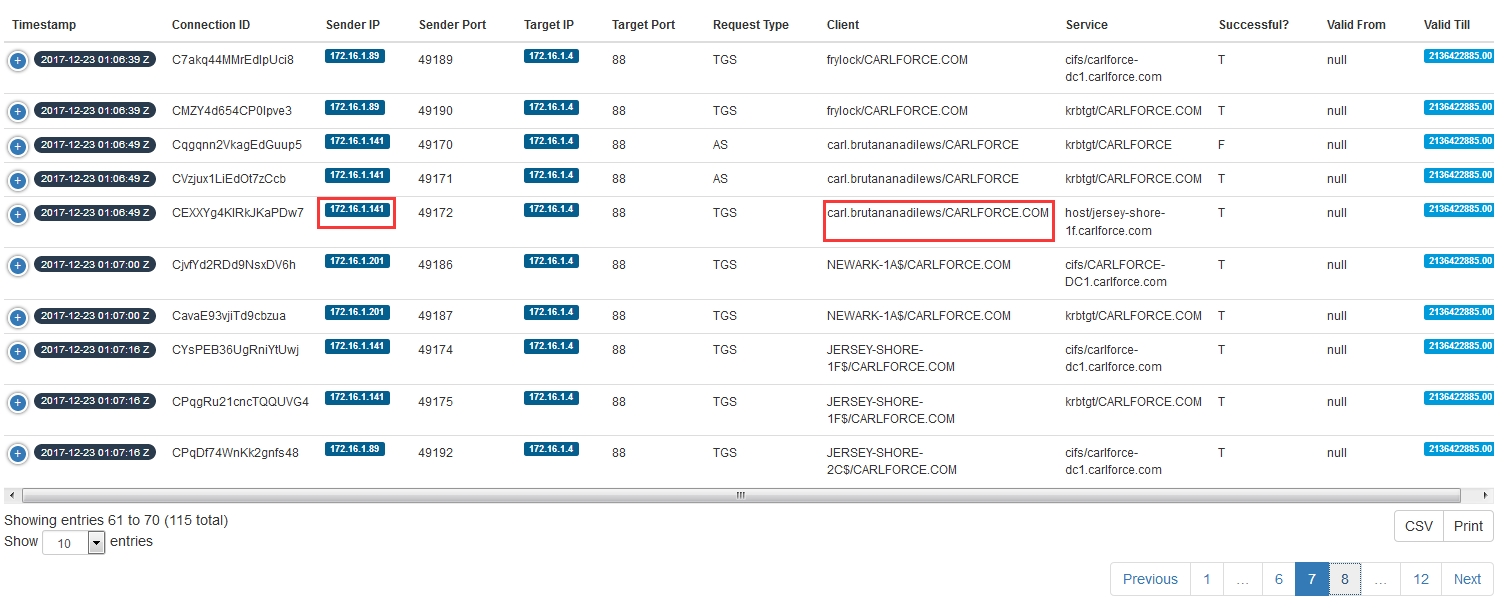
       分析完毕的界面如图所示，切换到kerberos选项卡，关注client这一栏

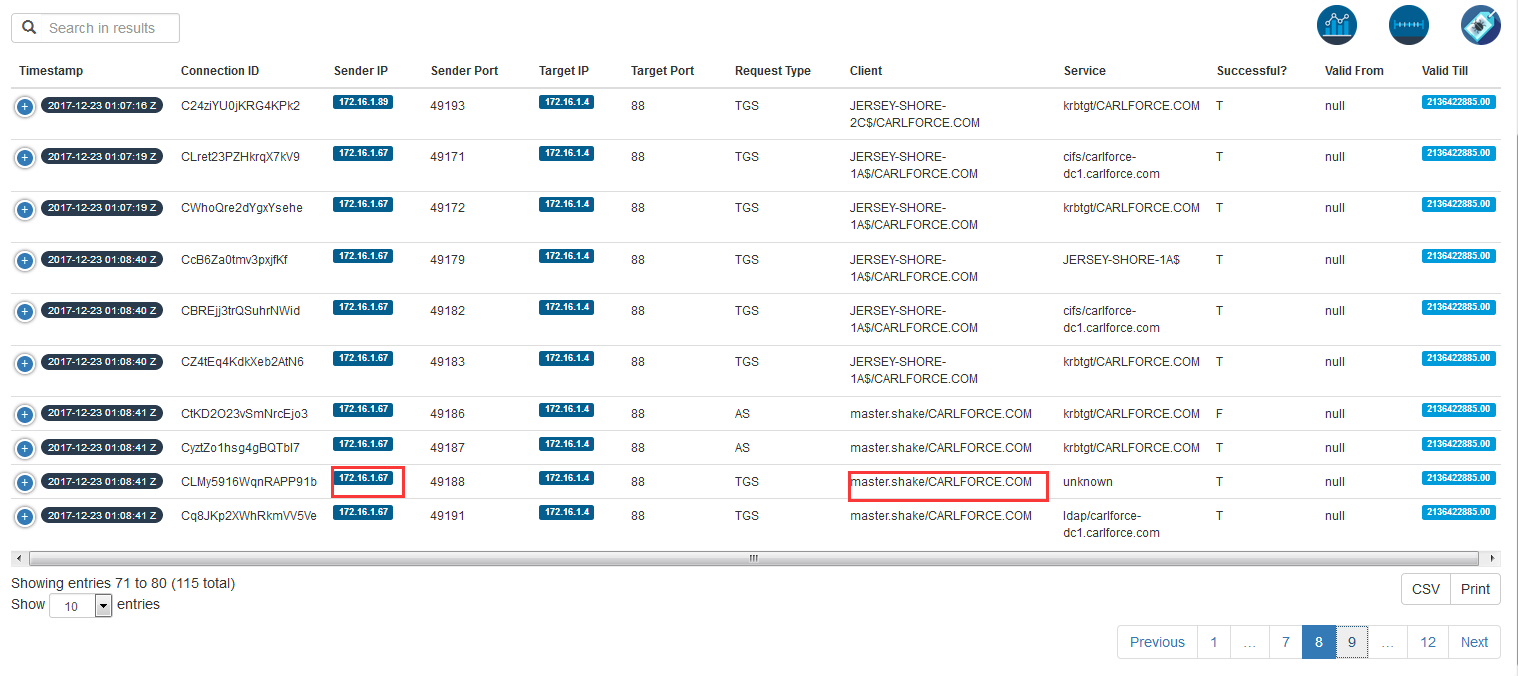


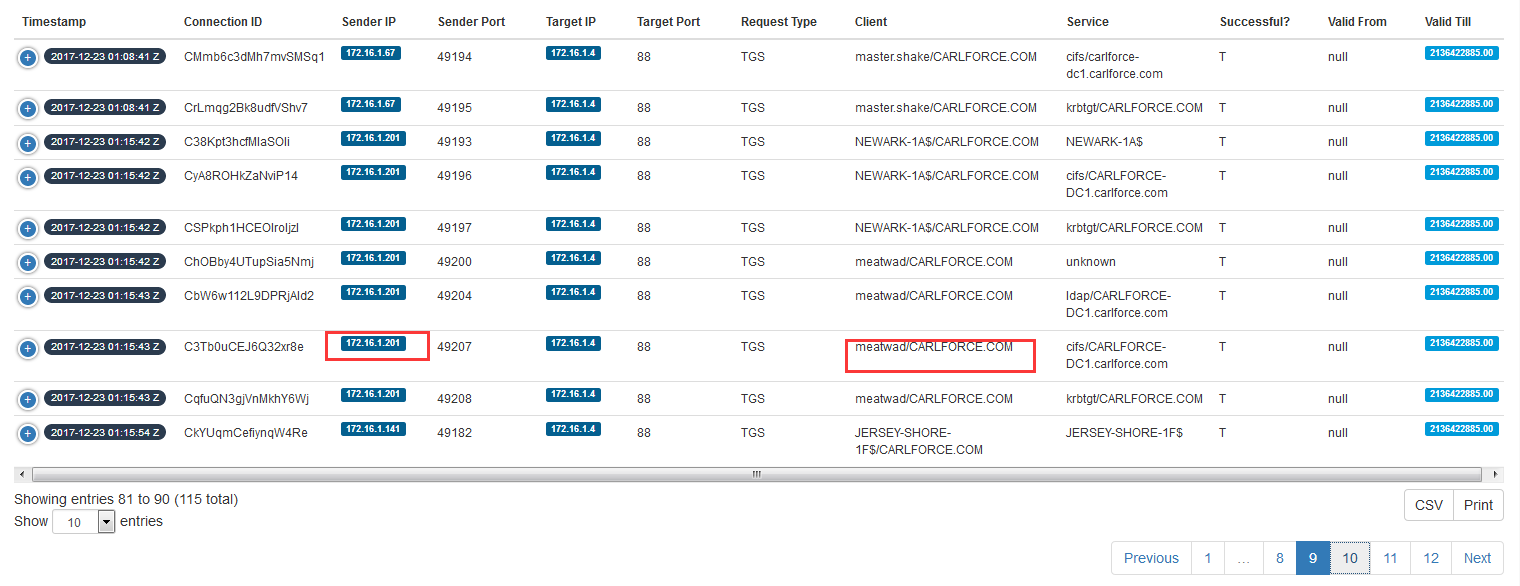
       找到的信息如下所示











       由上整理我们现在得到的信息：

       Ip:172.16.1.67

       主机名：jersey-shore-1a

       用户名：master.shake

       Ip:172.16.1.89

       主机名：jersey-shore-2d

       用户名：frylock

       Ip:172.16.1.141

       主机名：jersey-shore-1f

       用户名：carl.brutananandilews

       Ip:172.16.1.201

       主机名：newark-1a

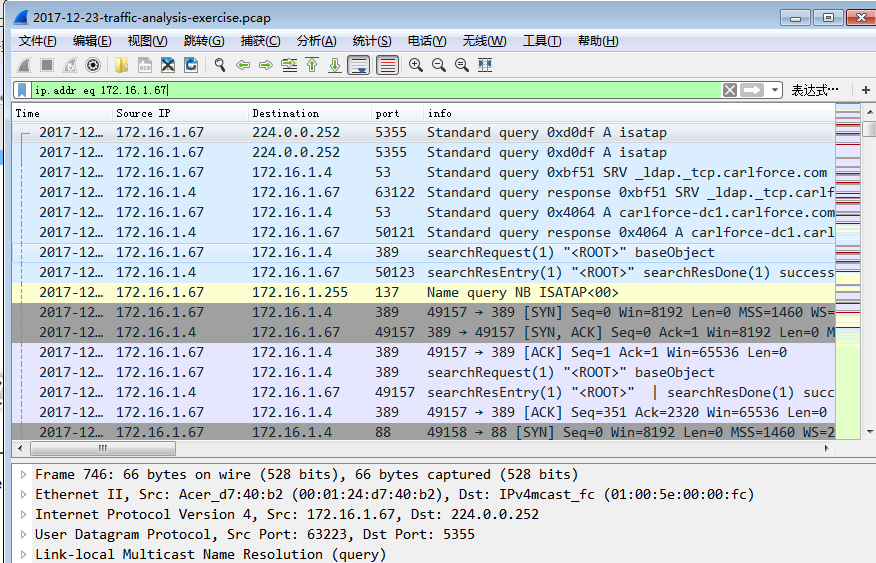
       用户名：meatwad

实验步骤三

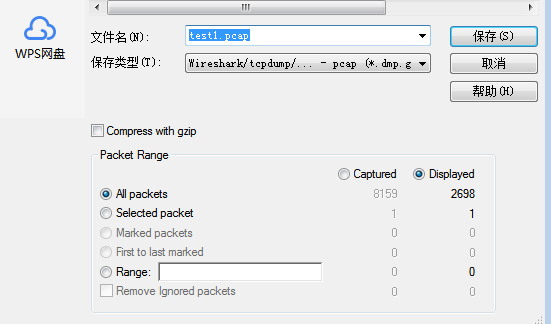
       接下来我们看看各个主机都发生了什么。

       先看看172.16.1.67

       首先ip.addr eq 172.16.1.67过滤出来

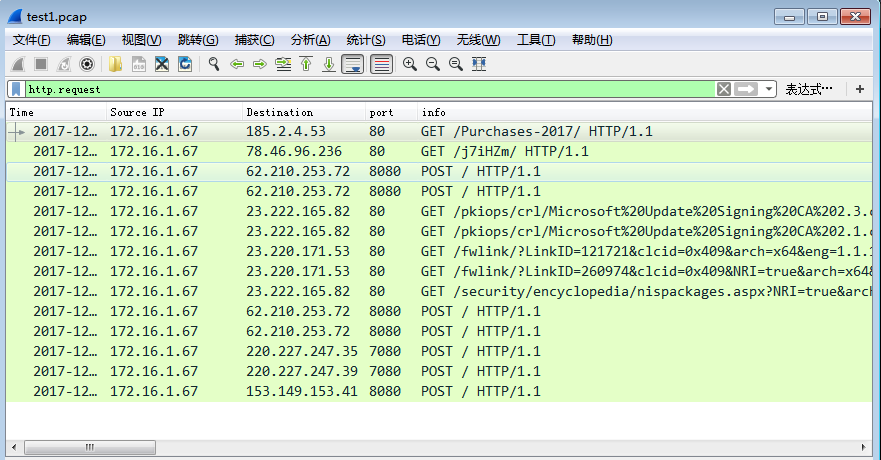


       左上方菜单栏  文件-》导出特定分组



       点击保存即可，然后打开

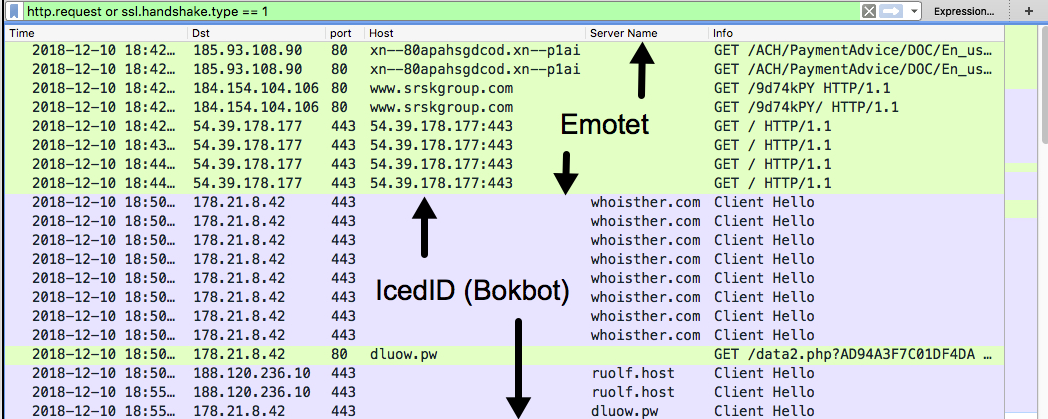
       有前几次的分析经验，我们这次首先使用http.request来进行过滤



       我们看到这种数据有没有似曾相识的感觉？

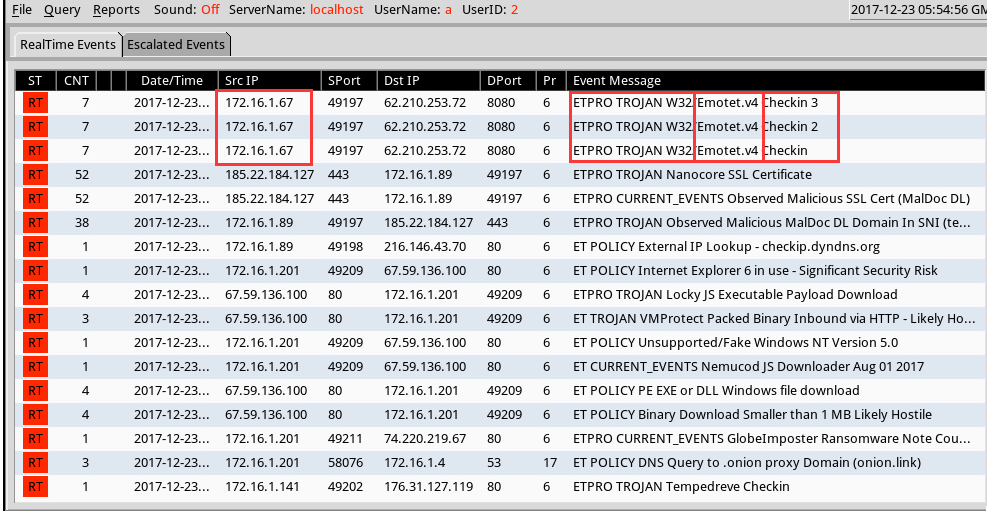
       我们在“恶意流量分析训练二”中碰到过这种流量，如下所示（在附件中已经给出）

       http.request or ssl.handshake.type == 1



       可以看到我们的流量也有连续发起两次相同GET请求的特征，所以我们猜测可能是感染了Emotet

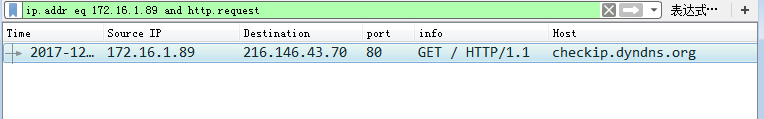
       或者我们从给出的告警日志中也可以看出来



       再来看看172.16.1.89

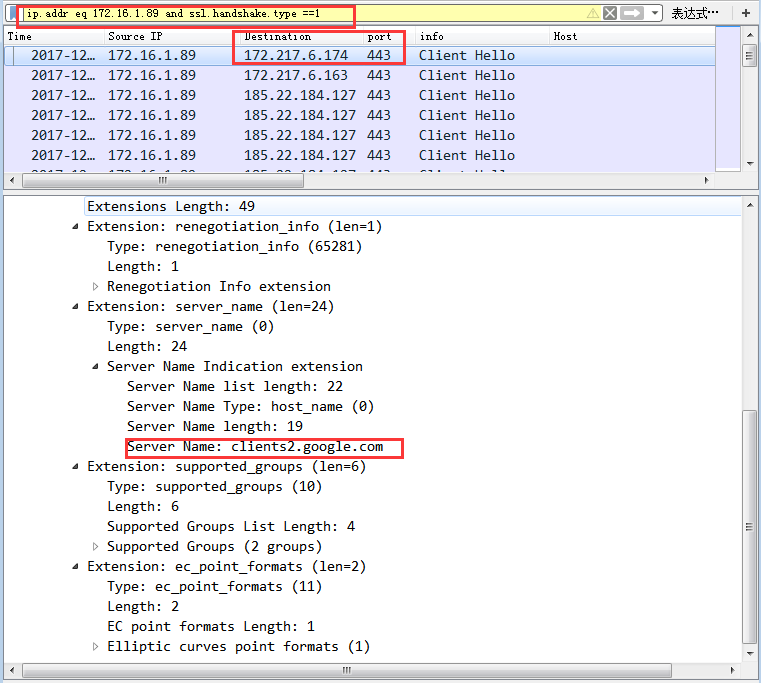
       在给出的数据包中过滤如下

       ip.addr eq 172.16.1.89 and http.request

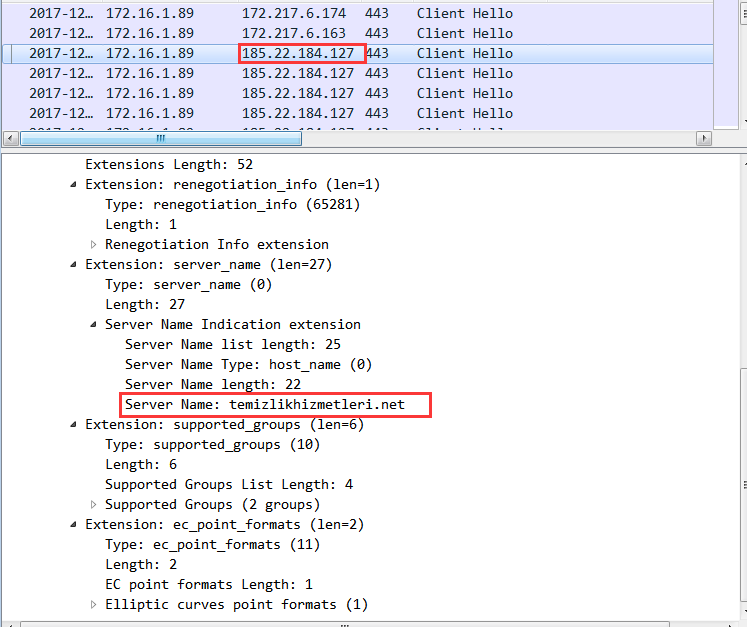


       可以看到只有一条数据，用处不大，没有http，那么我们看看有没有https的流量

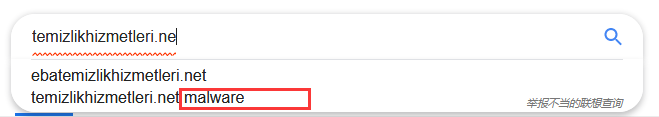
       ip.addr eq 172.16.1.89 and ssl.handshake.type ==1



       上图可以看到目的ip有三个，172.217.6.174是google的，172.217.6.163自然也是google的，我们看看第三个



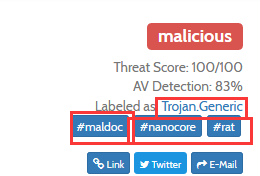
       这个域名没见过，搜索引擎查一下，我们还没输完就已经自动联想出了这可能是恶意软件



       直接看搜索结果第一条

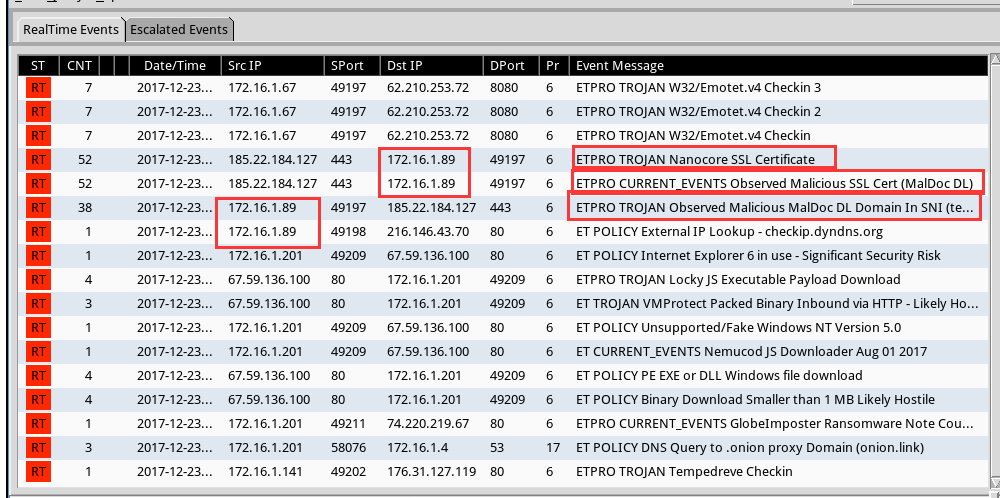


       网站中可以看到



       是恶意word文件，属于某种远控的攻击

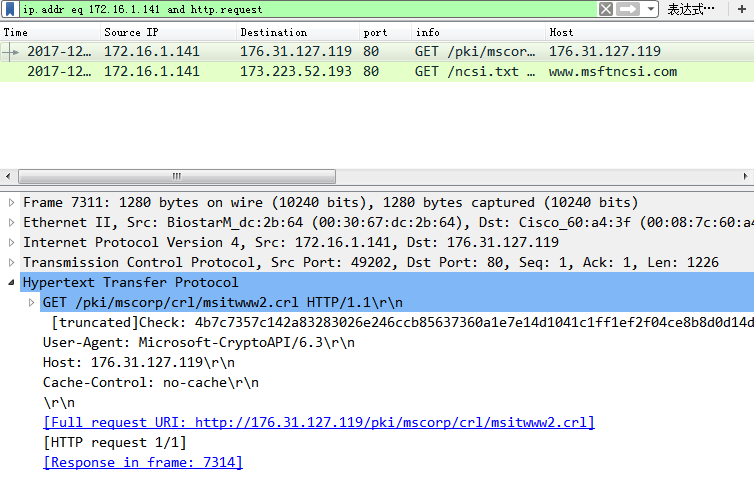
       这与我们在附件给出的告警日志中是相同的



       所以是NanoCoreRAT malware

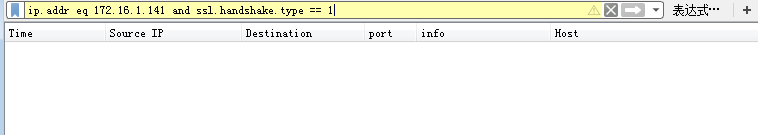
       接下来看看172.16.1.141

       使用ip.addr eq 172.16.1.141 and http.request过滤，先看http



       再看https

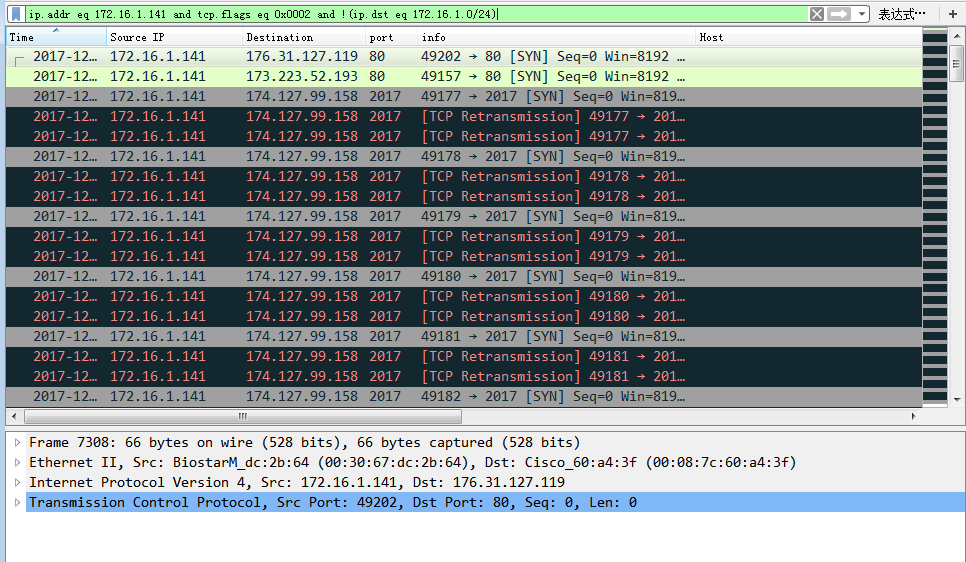
       ip.addr eq 172.16.1.141 and ssl.handshake.type == 1



       都没有帮助

       我们看看其他tcp连接吧，熟悉tcp的三次握手的流程都知道，第一步是发送syn，syn的flag是0x0002，同时因为我们要找的流量其目的地址不应该是同个局域网内的，这又是一个过滤条件，所以结合分析过滤条件为：

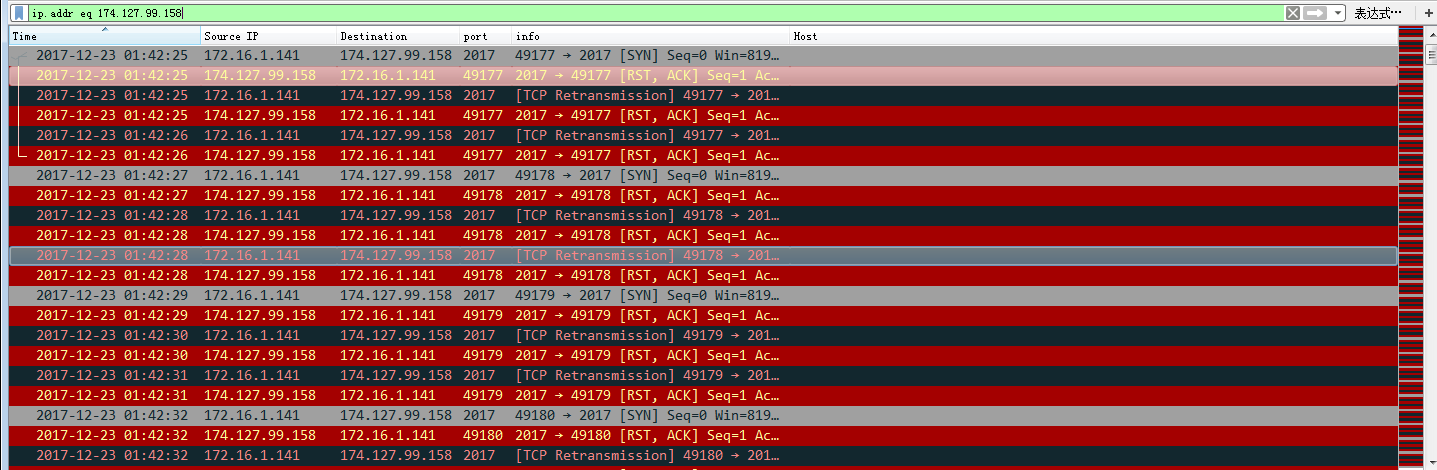
       ip.addr eq 172.16.1.141 and tcp.flags eq 0x0002 and !(ip.dst eq 172.16.1.0/24)



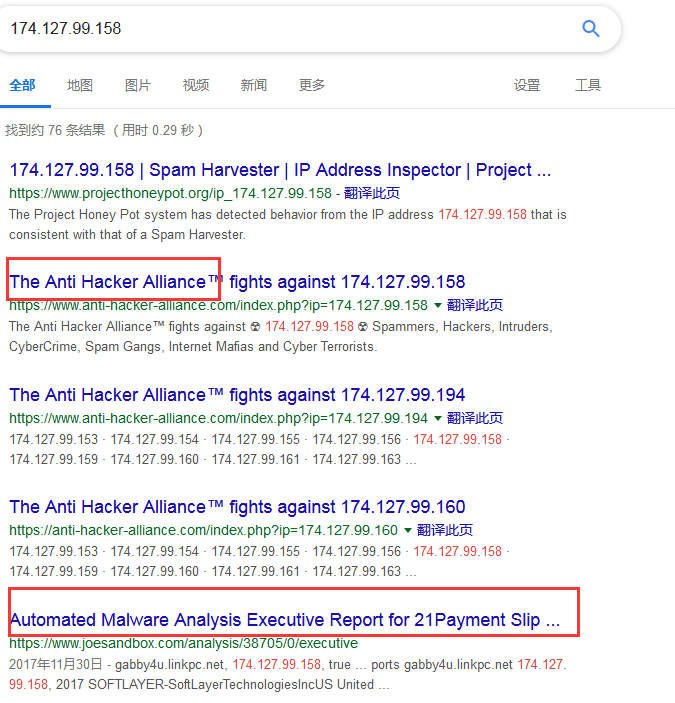
       我们发现2017端口很可疑，这端口很明显不是随机的，我们看看目的ip为174.127.99.158

       我们使用这个ip进行过滤

       ip.addr eq 174.127.99.158

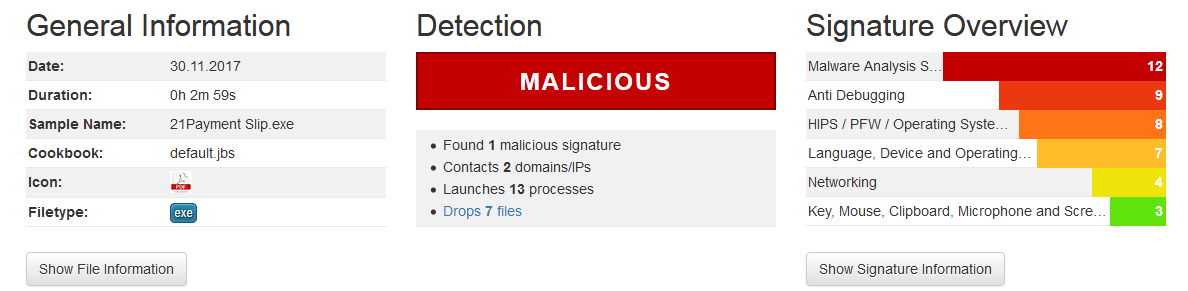


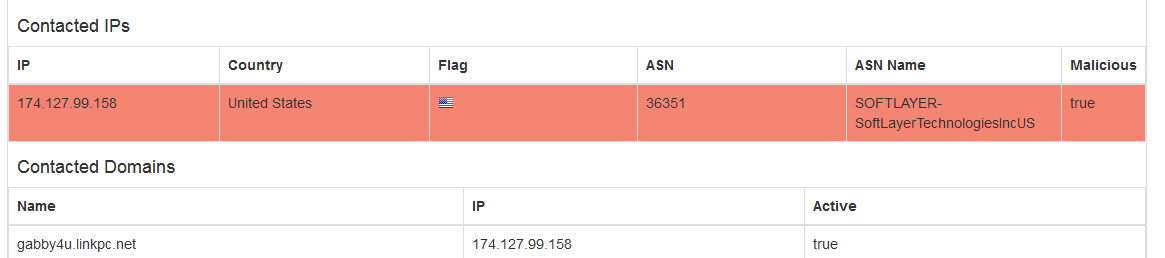
       发现只有syn和rst包，却没有正常该有的syn ack，说明这里流量是有问题的，我们用搜索引擎查查这个ip

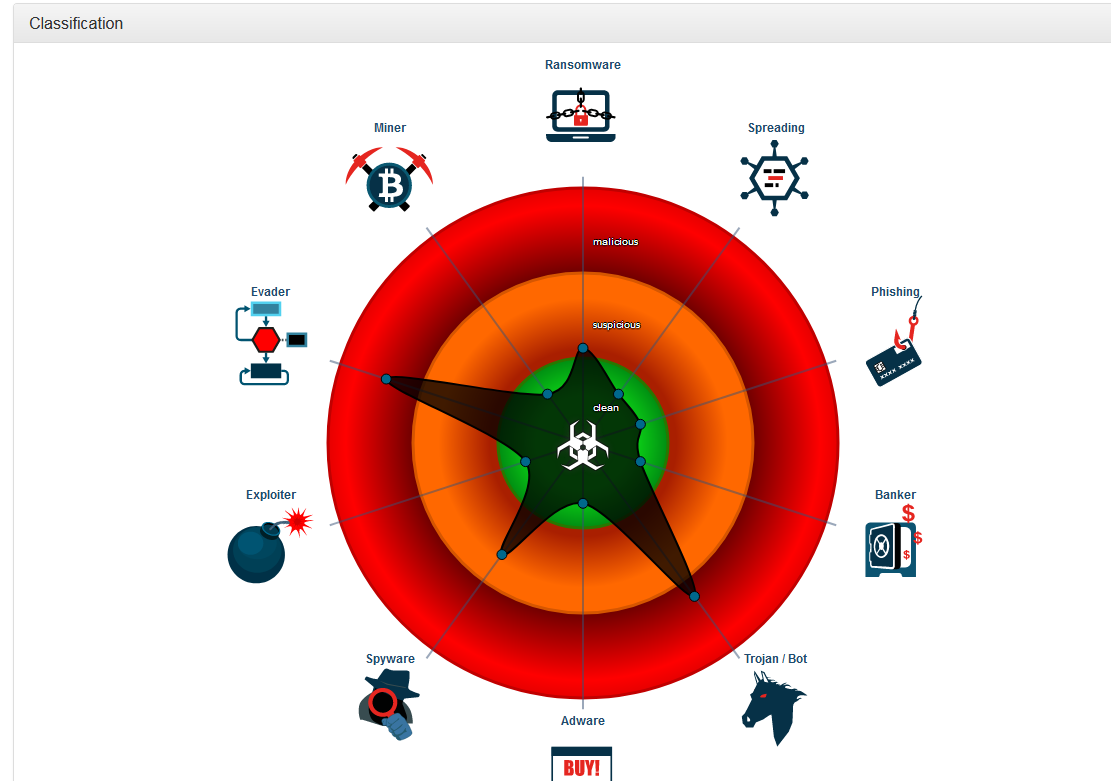


       从结果中可以看出这个ip是上了安全厂商的黑名单了

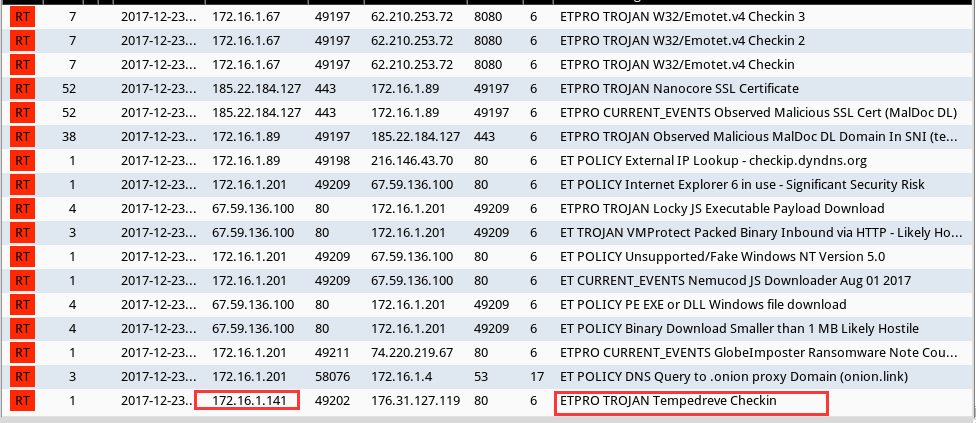
       在此处可以看到分析详情[https://www.joesandbox.com/analysis/38705/0/executive](https://www.joesandbox.com/analysis/38705/0/executive" \t "http://www.hetianlab.com/pages/teacher/_blank)，部分截图如下







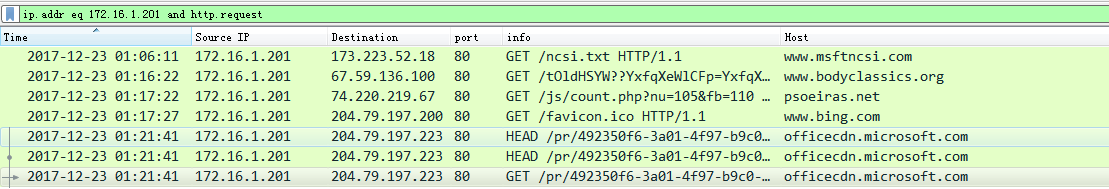
       报告中根据其行为将其判断木马，接下来结合告警日志看看



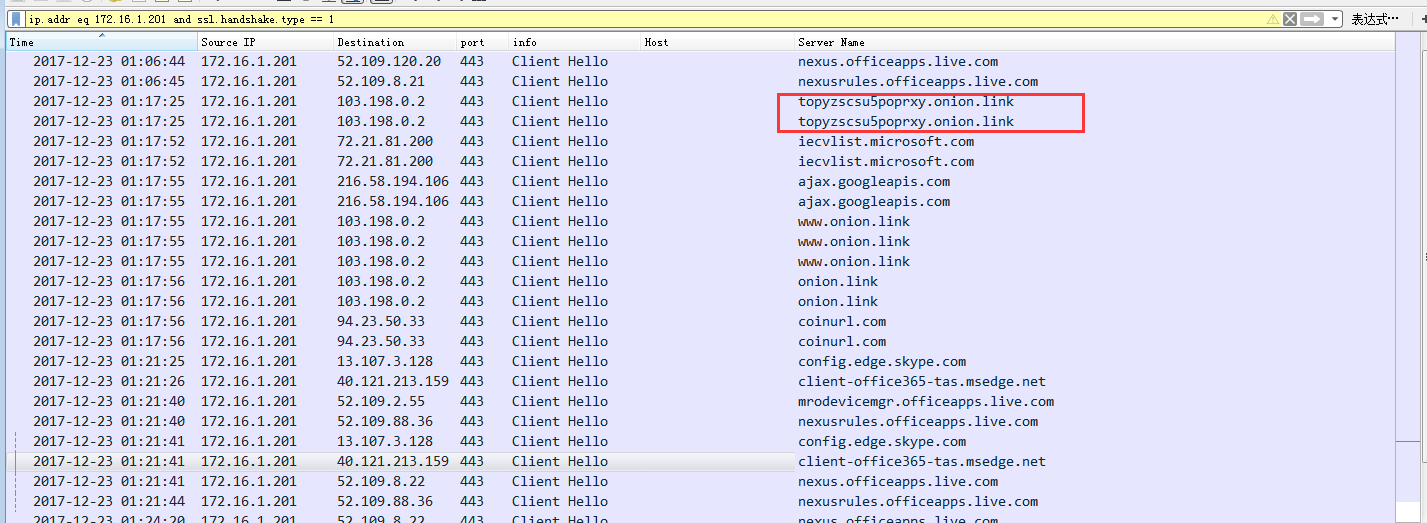
       可以看到是Tempedreve malware，恶意文件名可能为21Payment Slip.exe

       接下来分析172.16.1.201

       ip.addr eq 172.16.1.201 and http.request

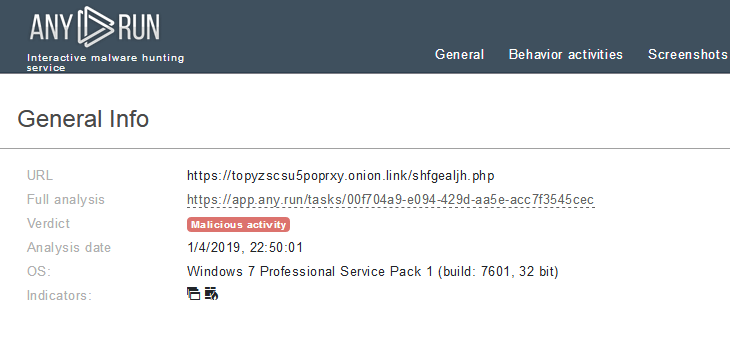


       ip.addr eq 172.16.1.201 and ssl.handshake.type == 1

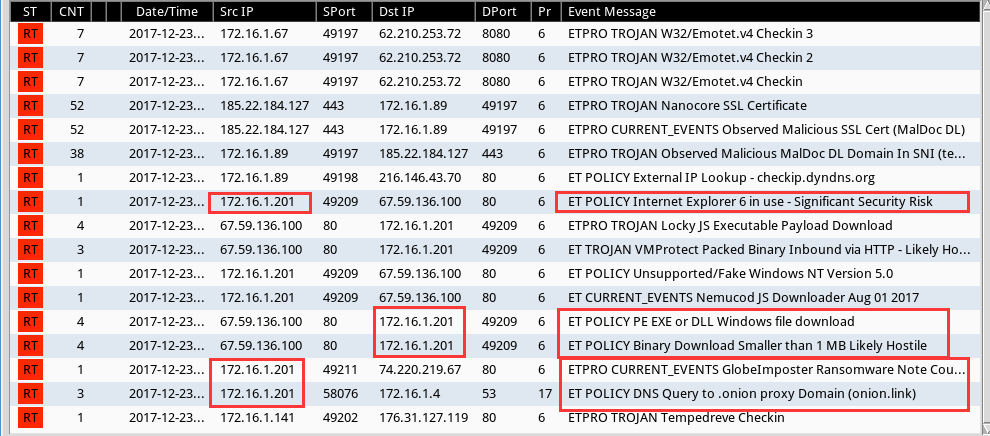


       相比而言https中有onion，我们知道这跟洋葱路由有关，此处的流量比较可疑

       把这个域名在搜索引擎中查询，可以看到在线沙箱网站分析出这是恶意链接



       在附件的告警日志中也可以看出来



       所以分析出来为GLobelmposter Ransomware.

IOC

综上所述，答案如下：

1）IP:172.16.1.67

       主机名：jersey-shore-1a

       用户名：master.shake

       感染了Emoter malware

2）IP:172.16.1.89

       主机名：jersey-shore-2d

       用户名：carl.brutamamamdolews

       感染了NanoCoreRAT malware

3）IP:172.16.1.141

       主机名：jersey-shore-1f

       用户名：carl.brutananandilews

       感染了Tempedrevemalware,恶意文件可能是21PaymentSlip.exe

4）Ip:172.16.1.201

       主机名：newark-1a

       用户名：meatwad

       感染了Globelposter malware

实验报告要求

参考实验原理与相关介绍，完成实验任务，并对实验结果进行分析，完成思考题目，总结实验的心得体会，并提出实验的改进意见。

配套学习资源

本系列所涉及流量均来自[https://www.malware-traffic-analysis.net/](https://www.malware-traffic-analysis.net/" \t "http://www.hetianlab.com/pages/teacher/_blank)