CTF misc之流量分析 password secret.log

原创

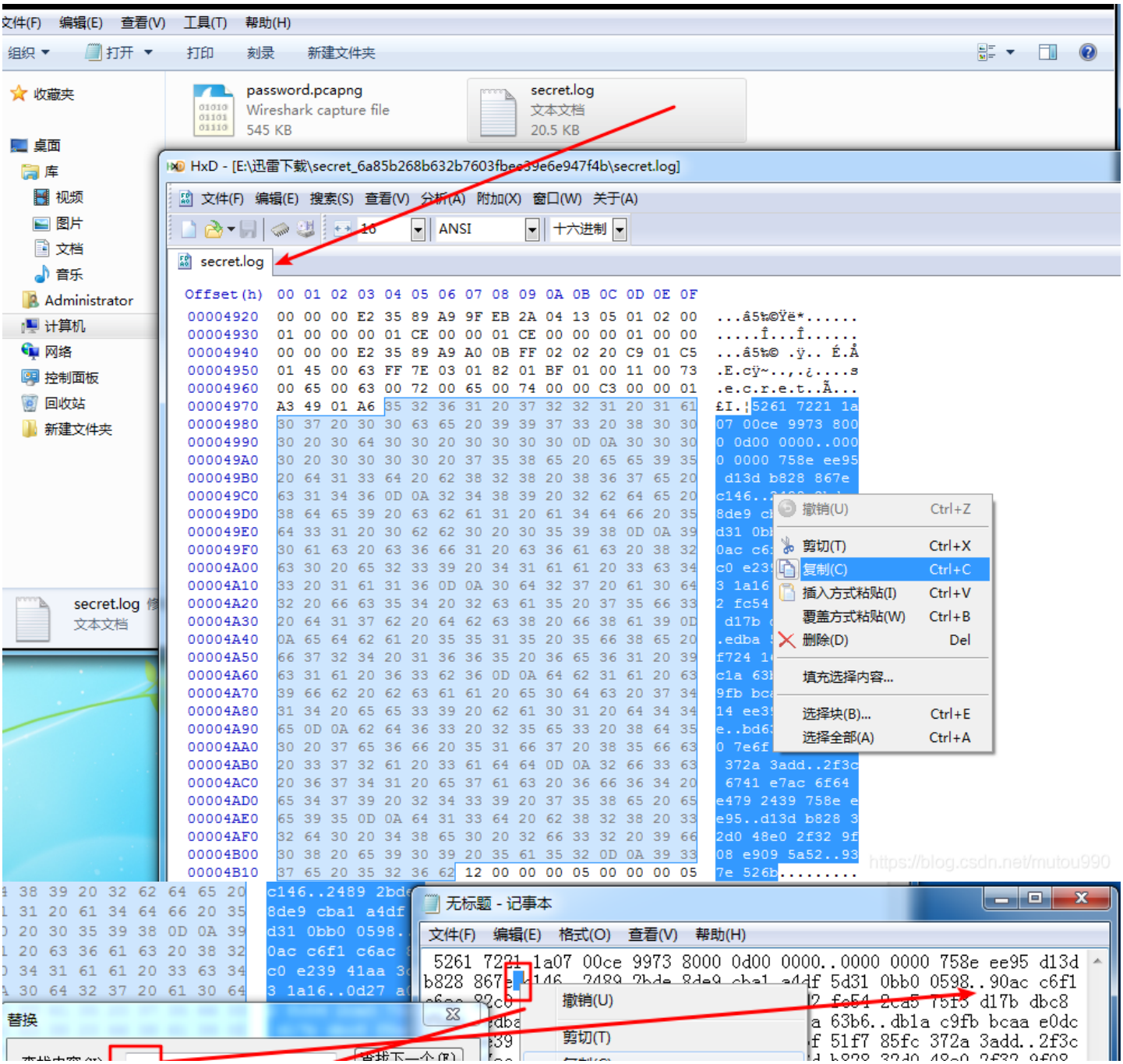
mutou990 于 2020-08-27 15:17:21 发布 869 收藏 2

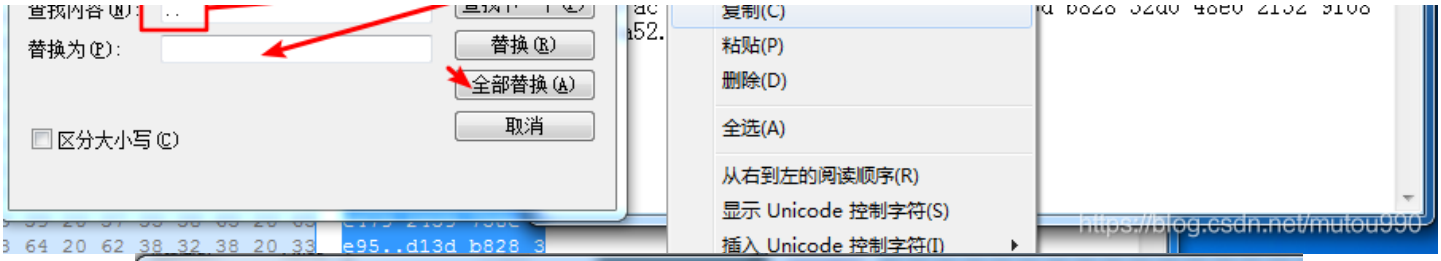
分类专栏： CTF 文章标签： 安全

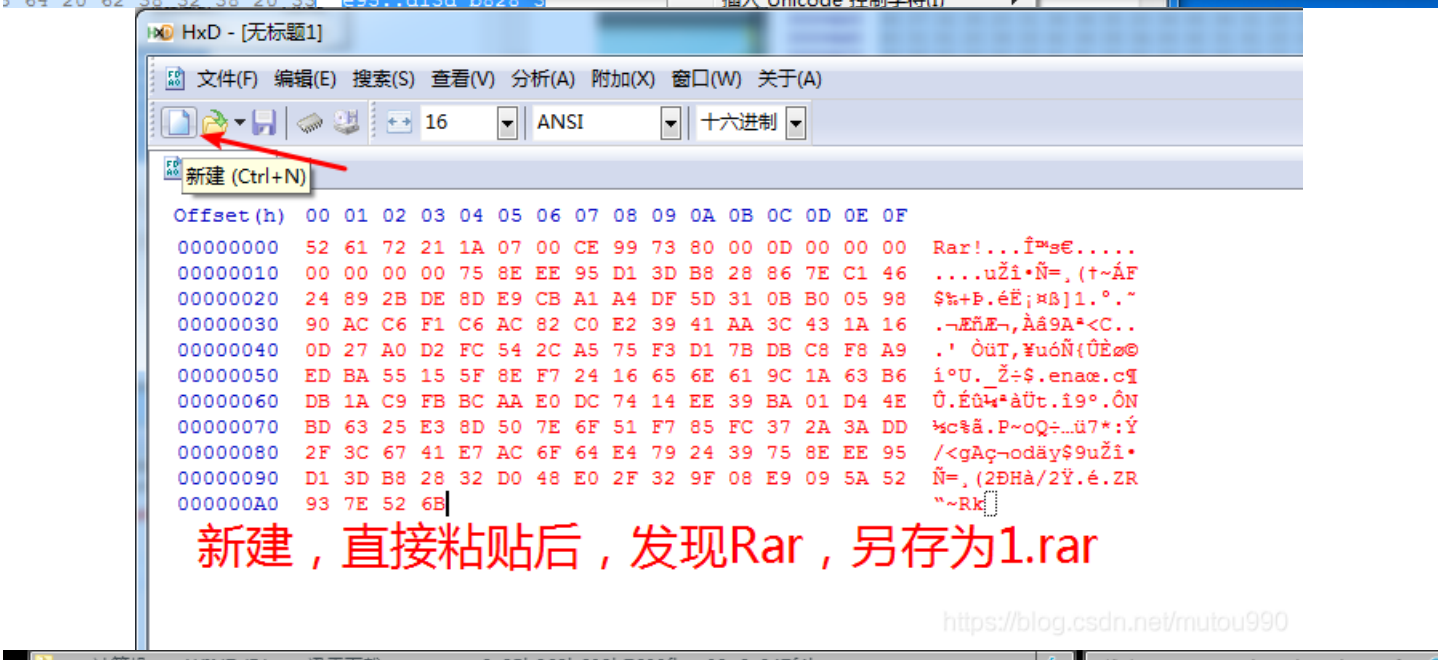
本文链接：https://blog.csdn.net/mutou990/article/details/108260680

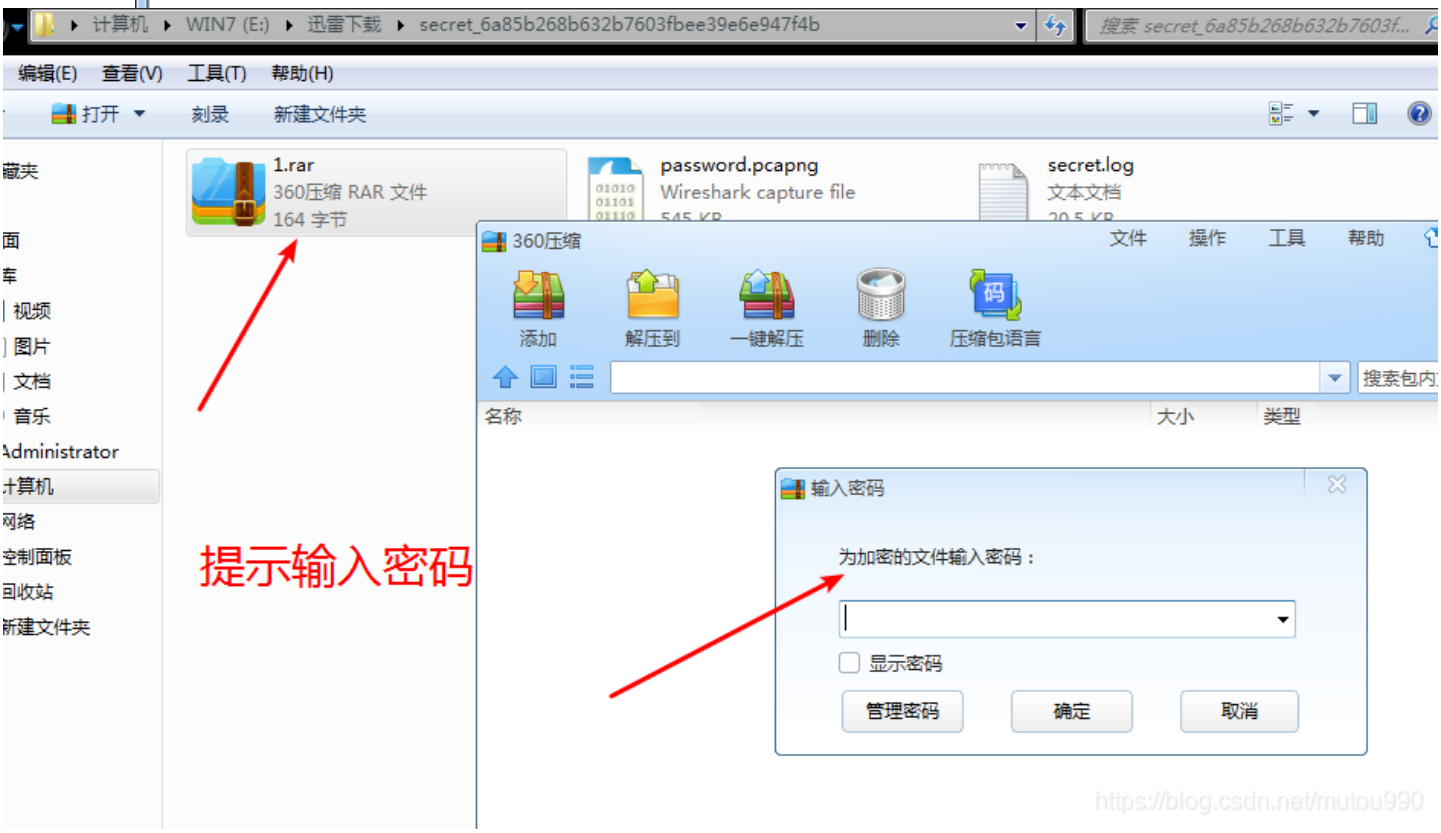
参考：【迎圣诞，拿大奖】+流量分析+Writeup分享

171221 杂项-i春秋【迎圣诞】（可恶的黑客、流量分析）





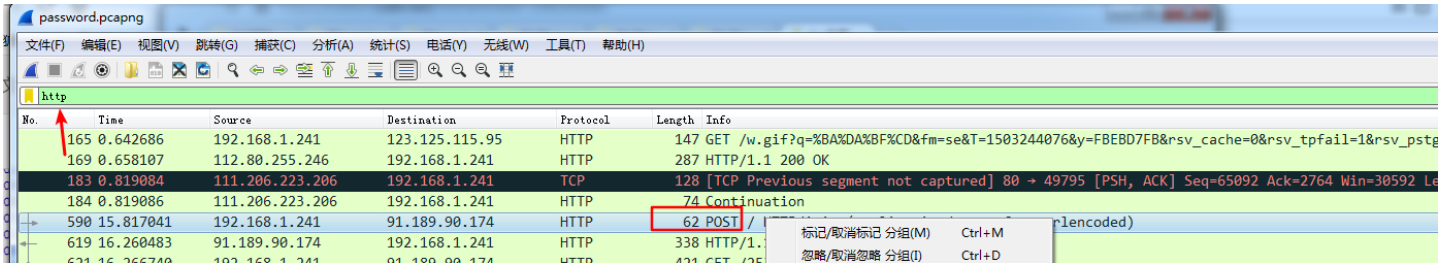


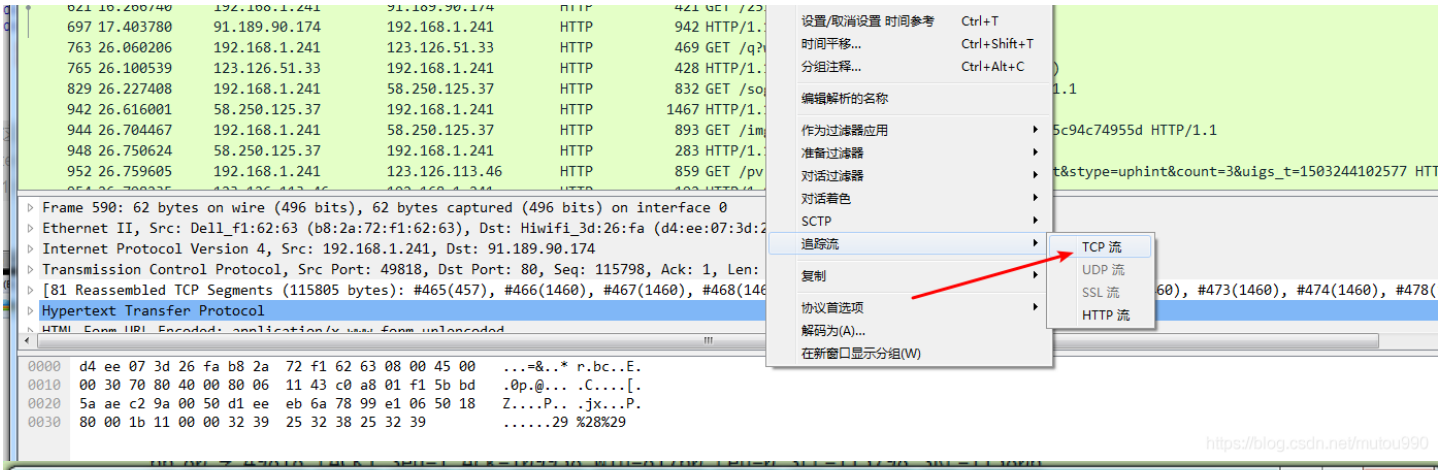


手里还有一个pcapng数据包没看，拿来分析

导出为HTTP对象发现大部分都是baidu和sougo的干扰流量

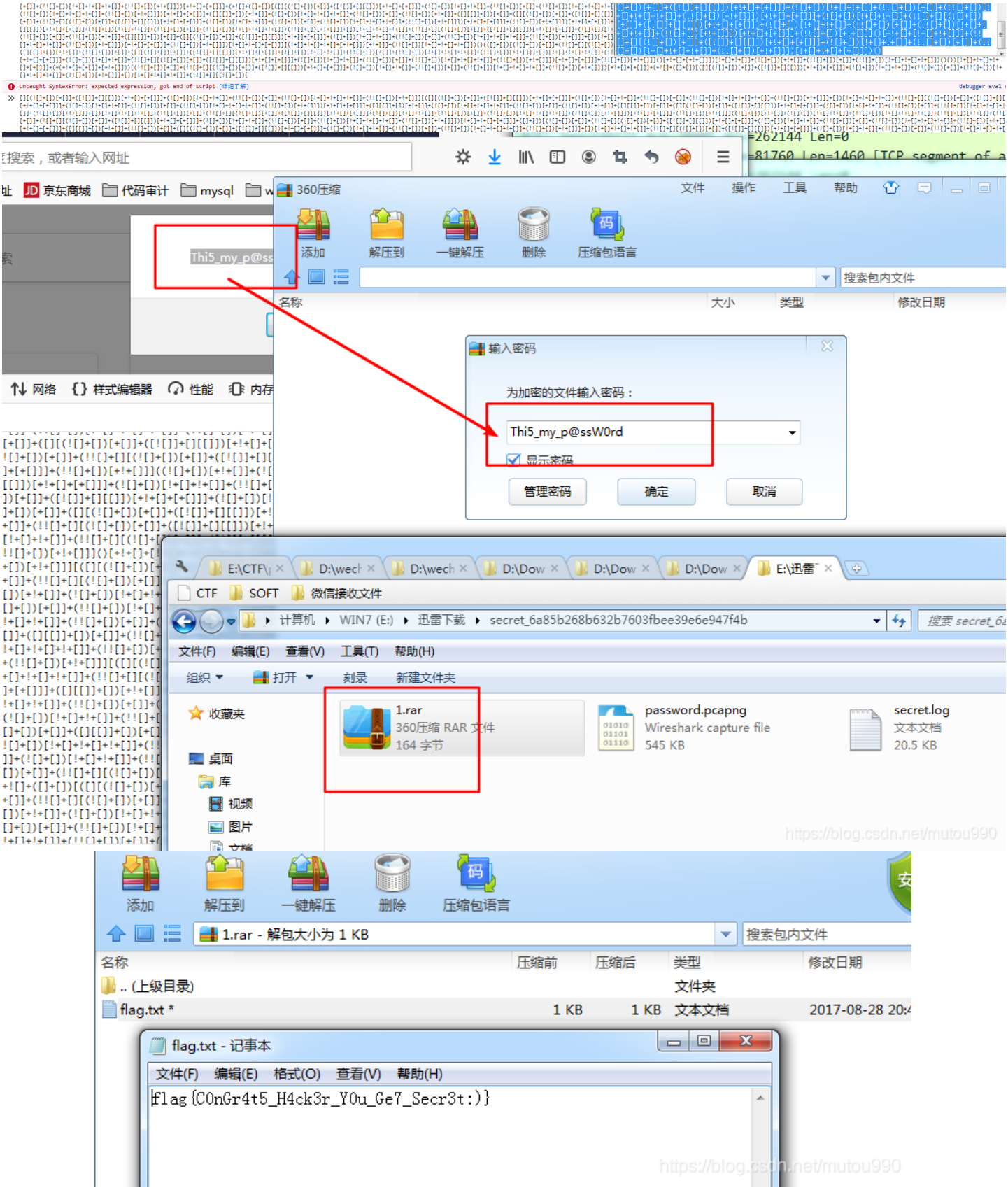
除此以外有两个paste.ubuntu.com的，点开分析发现post参数中有jsfuck，放到控制台里运行就弹出了密码




设置/取消设置 时间参考 Ctrl+T
时间平移... Ctrl+Shift+T
分组注释... Ctrl+Alt+C
编辑解析的名称
作为过滤器应用
准备过滤器
对话过滤器
对话着色
SCTP
追踪流
复制
协议首选项
解码为(A)...
在新窗口显示分组(W)
TCP 流
UDP 流
SSL 流
HTTP 流
Frame 590: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
Ethernet II, Src: Dell_f1:62:63 (b8:2a:72:f1:62:63), Dst: Hiwifi_3d:26:fa (d4:ee:07:3d:2
Internet Protocol Version 4, Src: 192.168.1.241, Dst: 91.189.90.174
Transmission Control Protocol, Src Port: 49818, Dst Port: 80, Seq: 115798, Ack: 1, Len:
[81 Reassembled TCP Segments (115805 bytes): #465(457), #466(1460), #467(1460), #468(146
Hypertext Transfer Protocol
0000 d4 ee 07 3d 26 fa b8 2a 72 f1 62 63 08 00 45 00 ...=&..* r.bc..E.
0010 00 30 70 80 40 00 80 06 11 43 c0 a8 01 f1 5b bd .0p.@... .C....[.
0020 5a ae c2 9a 00 50 d1 ee eb 6a 78 99 e1 06 50 18 Z....P.. .jx...P.
0030 80 00 1b 11 00 00 32 39 25 32 38 25 32 39 ......29 %28%29


Wireshark · 追踪 TCP 流 (tcp.stream eq 27) · password
这样的乱码要删掉，否则解密
1f40
不出来
Entire conversation (156 kB)
显示和保存数据为 ASCII
流 27
查找:
查找下一个(N)
滤掉此流
打印
Save as...
返回
Close
Help


Thi5_my_p@ssW0rd
确定
粘贴到一个
空白文件，
去掉乱码，全选复制后，粘贴
到火狐浏览器F12 console
平台，回车，提示结果



心得：一是要注意seceret.log里面的那一部分十六进制才是rar文件，我一直把整个seceret.log另存为为rar，所以一直报压缩包损坏错误，没法往下进行；

二是，对于十六进制那部分代码，里面有乱码...，要记得替换掉；后来的jsfuck里面也要乱码也要去掉，当时没去掉，一直解密不出来；还有之前做的一道流量分析，里面有段base64代码，这段代码最后两位是%3D，要记得把%3d换成=,再去base64解密，否则也解出来的也不正确。

输入发现还是提示不对，发现把flag的l变成1了,矫正一下即可。