【CTF MISC】隐写术wireshark找出图片-“强网杯”网络安全挑战赛writeup

转载

weixin_30782331 于 2016-12-11 00:49:00 发布 1001 收藏
原文链接：http://www.cnblogs.com/17bdw/p/6158828.html

这场CTF中有一道题是分析pcap包的。。

13.大黑阔：
从给的pcap包里把图片提取出来，是一张中国地图。
题目提示是黑阔在聊天，从数据里可以找出几段话。

思路：主要考察wireshark的过滤规则与熟悉度。

如果熟悉发送数据包的格式截取特定的字符串 "[{"，就能找出聊天记录了，也可以通过以下两个步骤找出关键的图片。

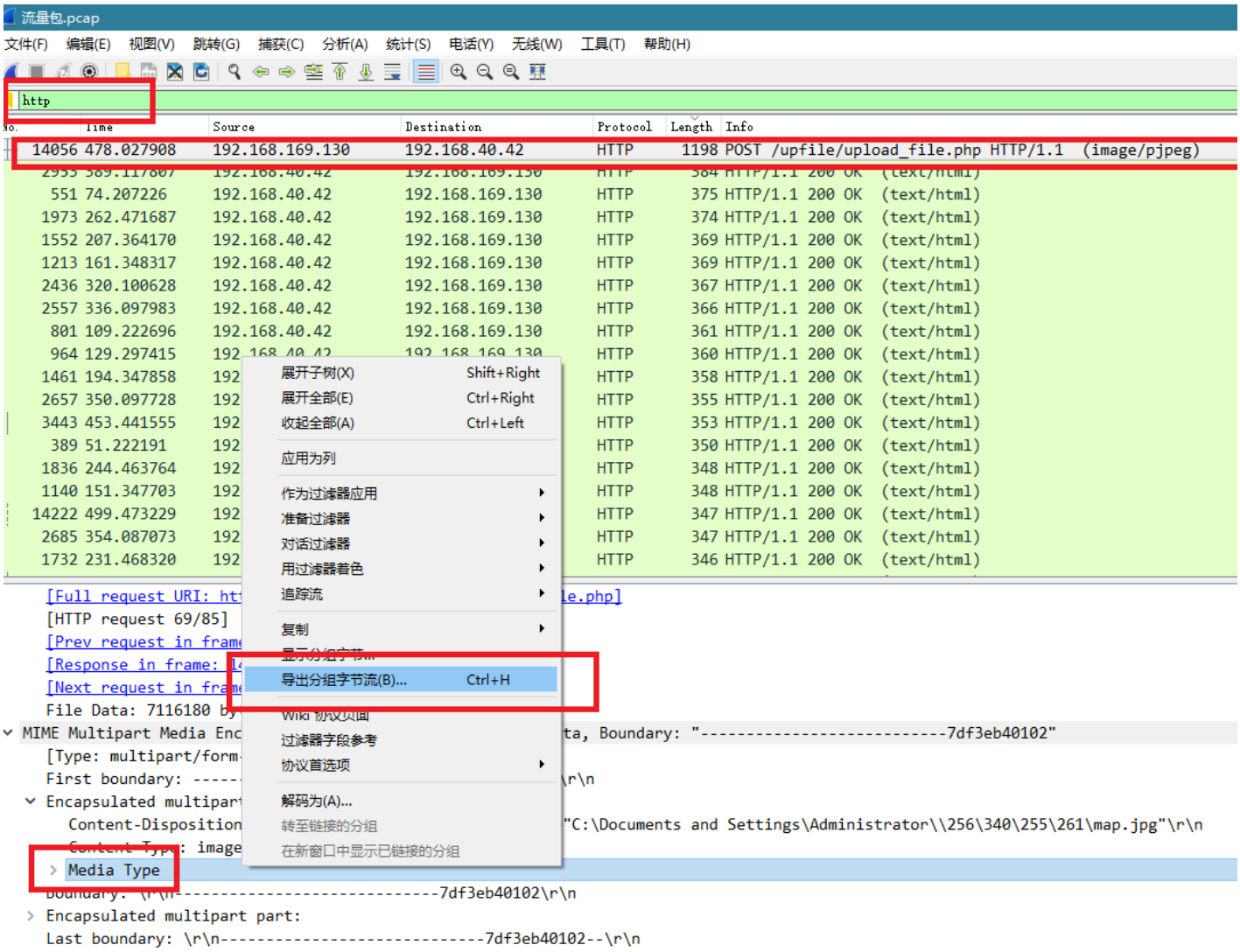
1、通过http过滤语句过滤出聊天内容

```
((http) && !(frame.len == 78)) && !(frame.len == 312)
```

2、将数据包中的图片提取出来。

```
HTTP数据  -  查看POST数据包  -  Media Type  -  导出分组字节流
```

就可以将图片直接导出来了,如果用Winhex要从FFD8，FFD9头尾进行截取，则比较麻烦。



转载于:https://www.cnblogs.com/17bdw/p/6158828.html