# 抓到一只苍蝇 writeup

转载

剑西楼 于 2016-11-30 16:57:55 发布 2090 收藏
文章标签： IDF

题目在 http://ctf.idf.cn/index.php?g=game&m=article&a=index&id=57

下载到的文件是misc_fly.pcapng，使用wireshark打开，能看到一堆tcp、http和dns协议混合的数据包，在上面的框里面输入http，让它只显示http协议的数据包。

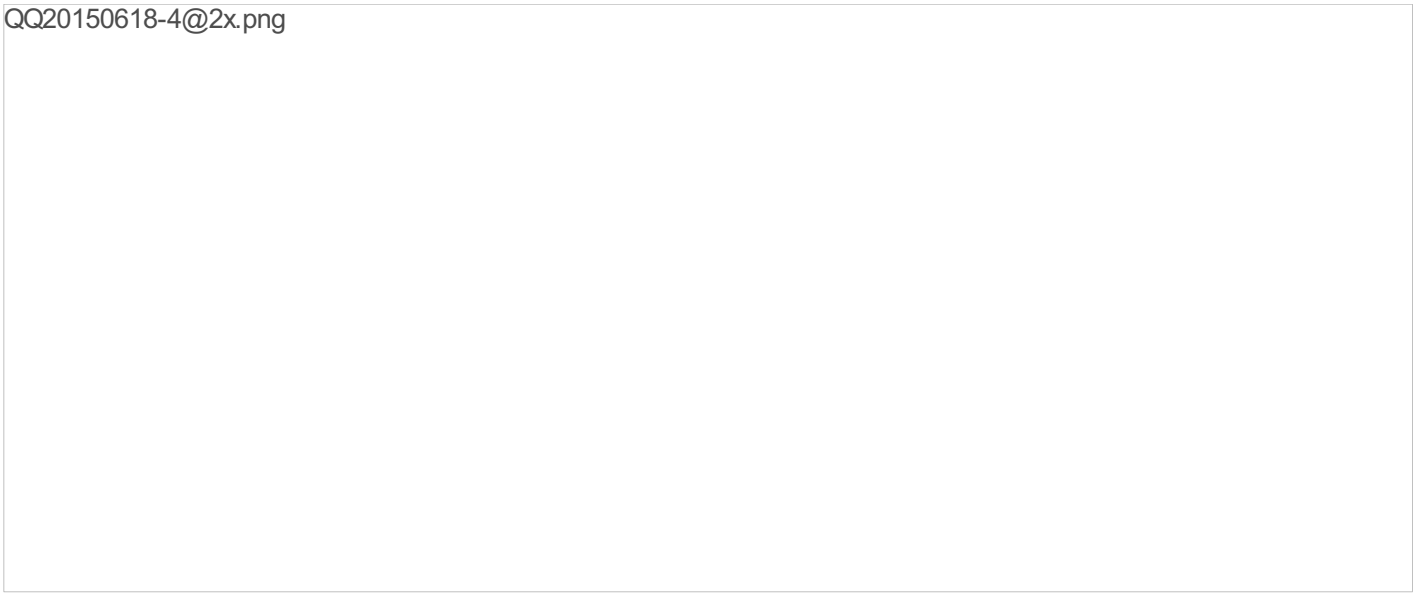
QQ20150618-1@2x.png

逐个展开大致的看了下，是在qq邮箱里面发送邮件。其中有一个上传文件行为，分为5个HTTP请求。

```
{
    "path": "fly.rar",
    "appid": "",
    "size": 525701,
    "md5": "e023afa4f6579db5becda8fe7861c2d3",
    "sha": "ecccba7aea1d482684374b22e2e7abad2ba86749",
    "sha3": ""
}
```

QQ20150618-2@2x.png

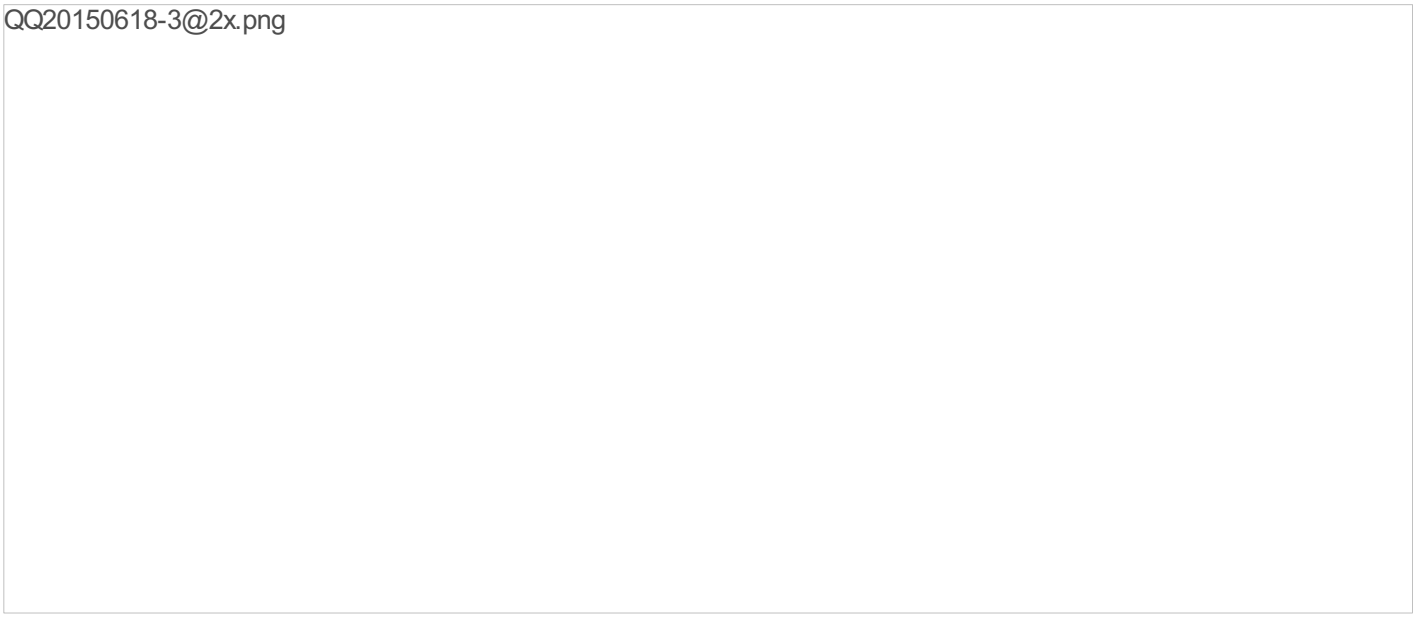
接下来提取文件 在每个请求的media type上点右键export




发现提取出来的文件比实际的要大呢

```
-rw-r--r-- 1 root root 131436  6月 18 15:47 1
-rw-r--r-- 1 root root 131436  6月 18 15:47 2
-rw-r--r-- 1 root root 131436  6月 18 15:48 3
-rw-r--r-- 1 root root 131436  6月 18 15:48 4
-rw-r--r-- 1 root root   1777  6月 18 15:48 5
```

怀疑是文件头部添加了东西，对比一下每个文件，确实在大约0x4d0的位置以上都是一样的。后来搜索得知这是文件分块的头部，存储有分块大小等信息。



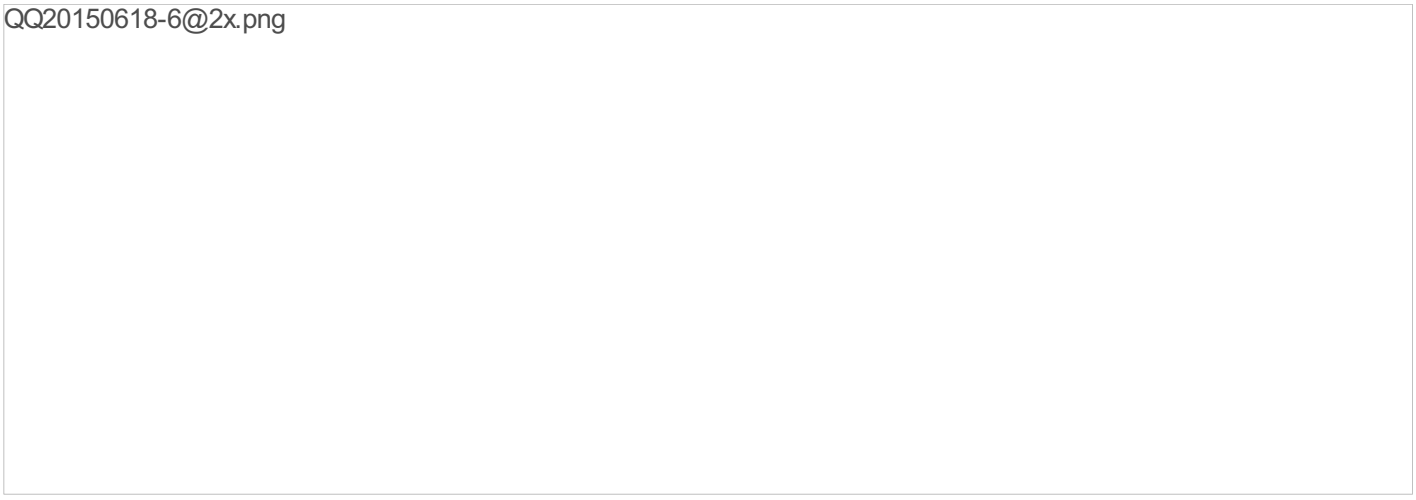

提取出来的文件总大小是527521，而上面提示的文件大小是525701，(527521 - 525701) / 5.0 = 364就是每个文件被添加的头部的大小，手动的去掉就可以了。

可以使用命令 `dd if=输入文件名 bs=1 skip=364 of=输出文件名` 然后cat，或者用Python seek一下就好了。

最终得到一个rar文件。

其实提取文件还有简单的方法就是使用foremost，`foremost -i -e misc_fly.pcapng`，然后output/rar/xxx.rar就有了。但是文件大小是对的，md5却是错的。再研究一下。。。。

文件在mac和linux打开都提示输入密码，在windows下使用360压缩提示文件损坏，怀疑文件被修改过。使用Bless打开文件，看到第17个字节处rar加密标志位是84，可能是伪加密，将它修改为80以后，保存并正常解压得到一个exe。




继续开windows虚拟机，

运行这个exe得到一屏幕的苍蝇，也倒符合了这个题目的意思。。。

回到linux，使用binwalk分析可以看到文件末尾包含一个图片，有点异常，提取出来看看。还是用`dd if=flag.txt bs=1skip=991232 of=1.png`

```
             0xEDCC2         Zlib compressed data, best compression, uncompressed size >= 14460
      47       0xEF3EB         PC bitmap, Windows 3.x format, 49 x 23 x 8
      96       0xF1BF4         XML document, version: "1.0"
      32       0xF2000         PNG image, 280 x 280, 1-bit colormap, non-interlaced
```

得到一个二维码，扫一下就能获取到flag了。结果是`flag{m1Sc_oxO2_Fly}`