xctf攻防世界 MISC高手进阶区 simple_transfer

原创

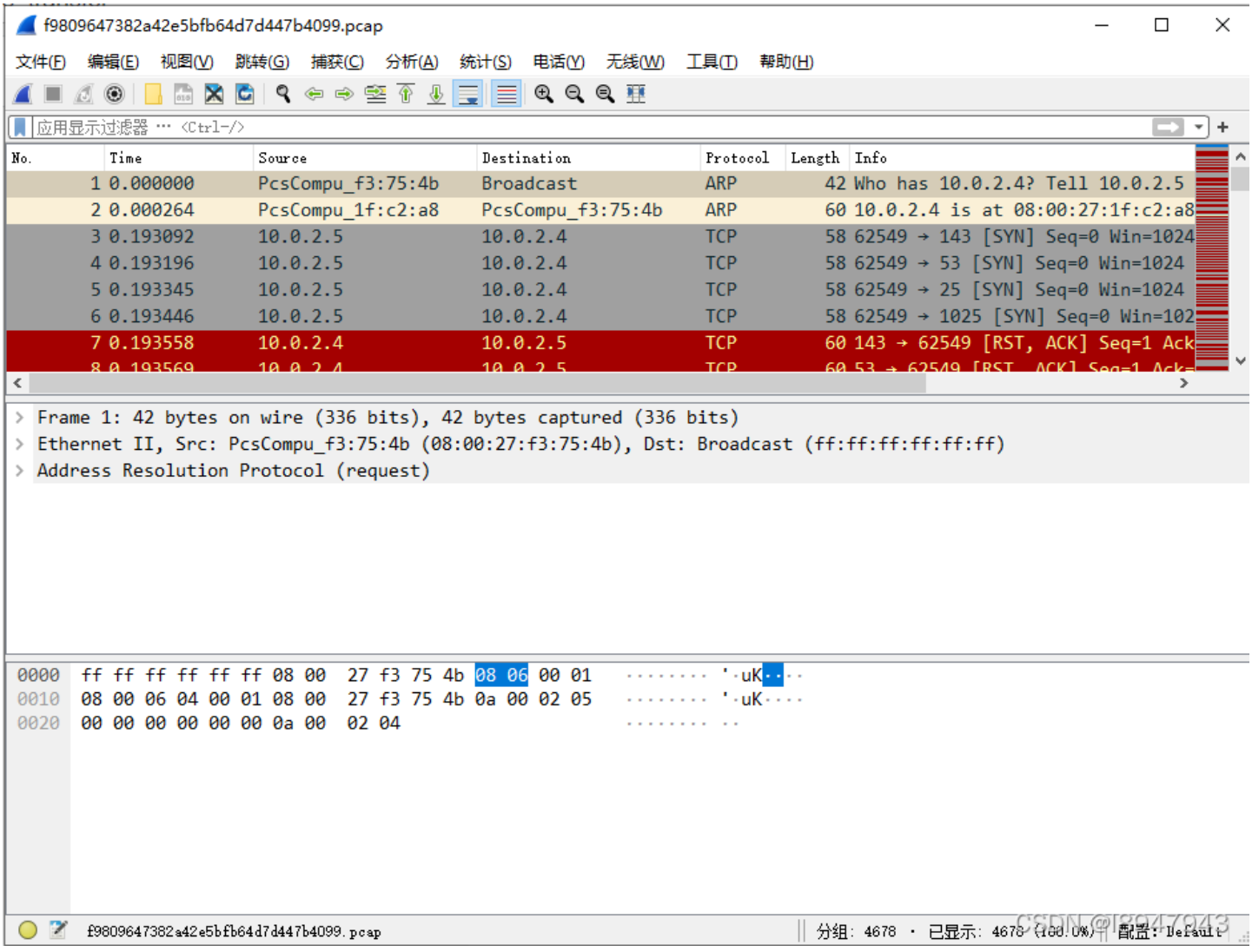
l8947943 于 2022-01-12 19:16:57 发布 150 收藏

分类专栏： 攻防世界misc之路 文章标签： misc foremost

本文链接：https://blog.csdn.net/l8947943/article/details/122460189

1. 进入环境，下载附件

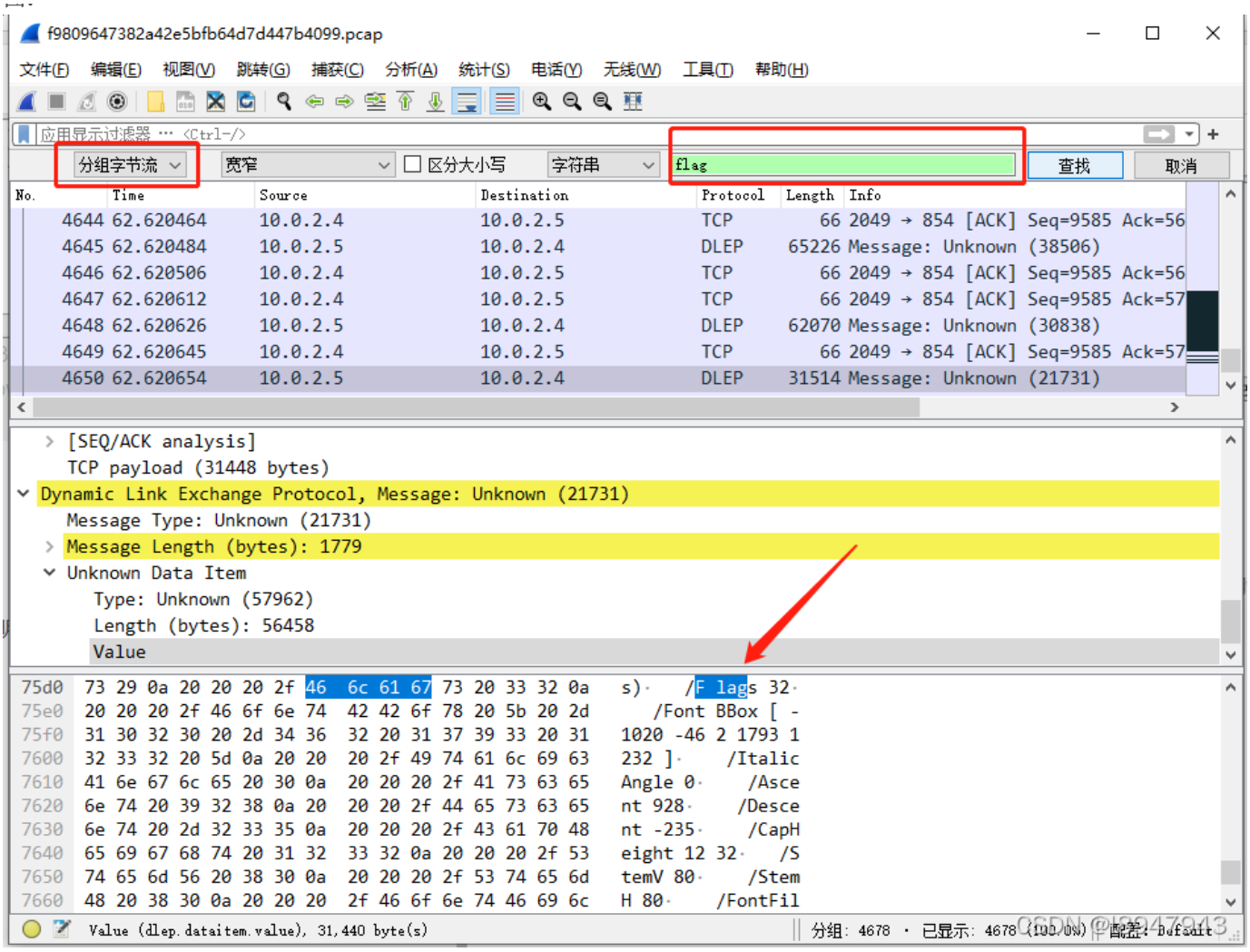
内容是个pcap文件，果断用wireshark打开



2. 问题分析

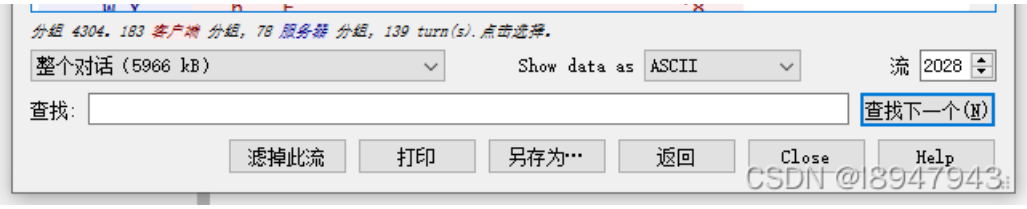
使用wireshark找到flag

题目提示，`文件里有flag，找到它。` 那么说明数据流中包含flag，我们使用wireshark中的分组字节流查找flag关键字，如图：



追踪流

上下滑动，翻一翻发现了端倪，如图：



说明文件中有隐藏pdf，因此自然想到了文件分离

foremost文件分离

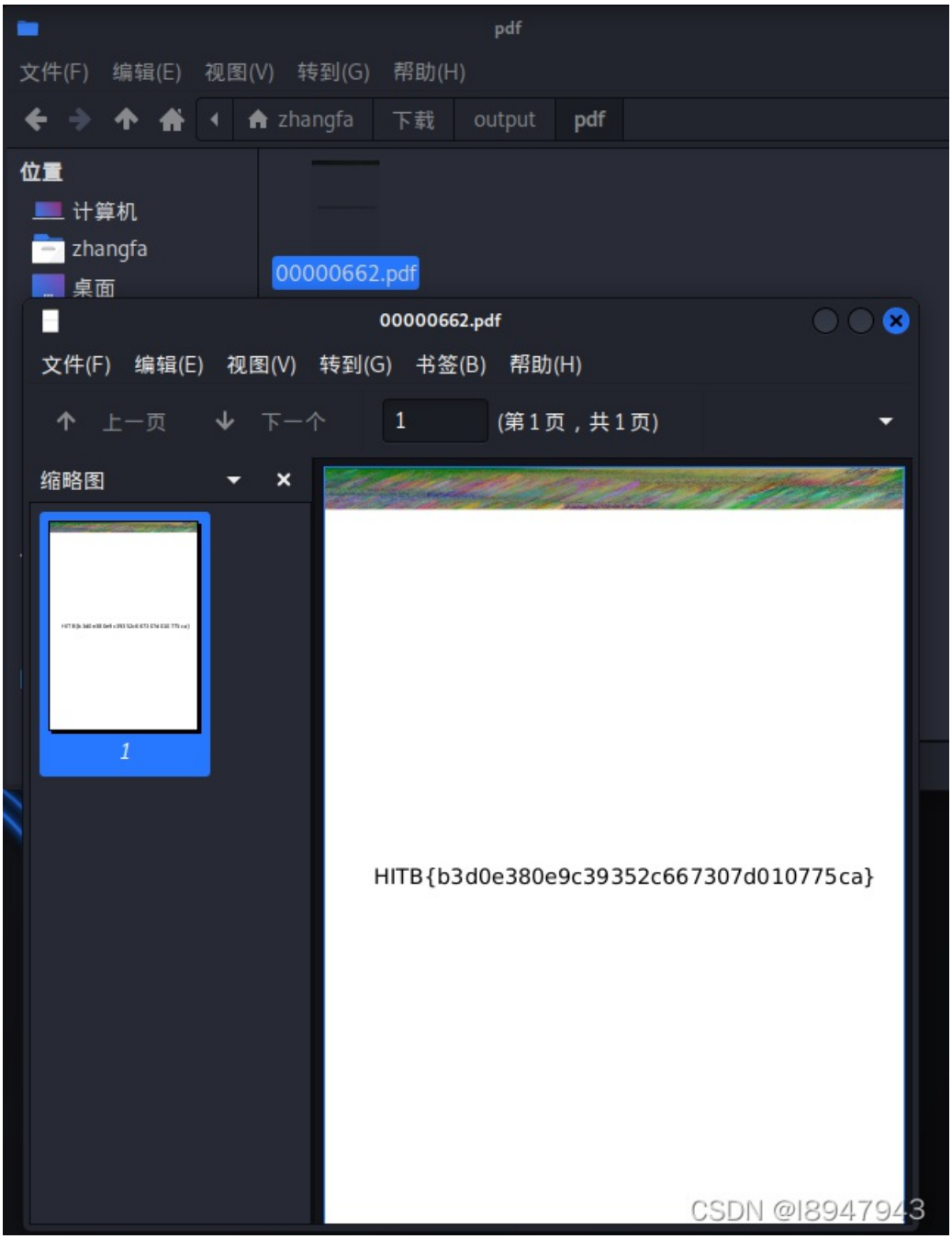
先安装foremost

```
$ apt-get install foremost
```

我们使用foremost去分离文件，命令：

```
$ foremost f9809647382a42e5bfb64d7d447b4099.pcap
```

得到的结果如图：



最终flag为：`HITB{b3d0e380e9c39352c667307d010775ca}`

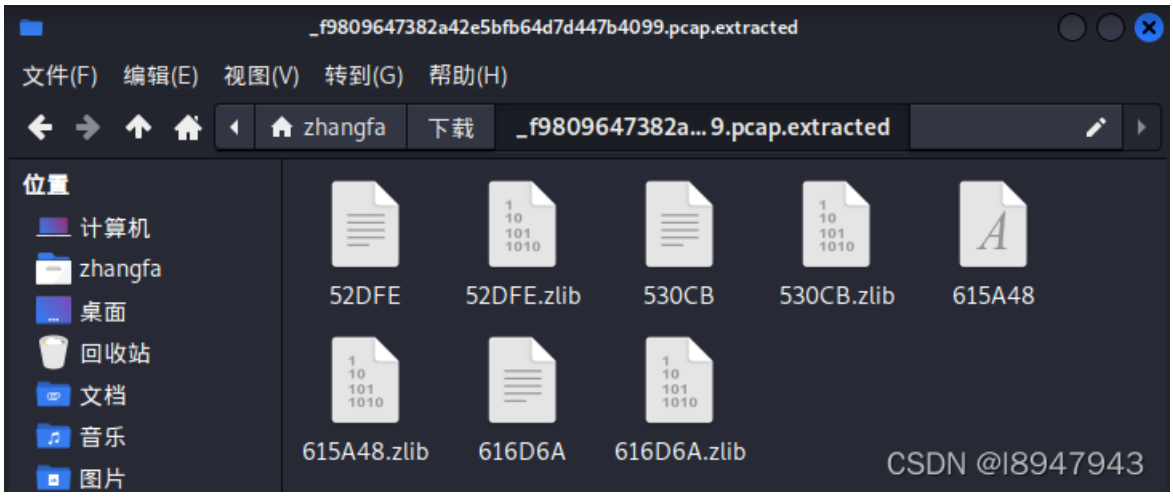
4. **kali工具之binwalk**

使用binwalk，但是不知道为什么只能检测出有pdf文件包含，分离不出来文件就很迷，如图：

```
┌──(zhangfa㉿kali)-[~/下载]
└─$ binwalk -e f9809647382a42e5bfb64d7d447b4099.pcap

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Libpcap capture file, little-endian, version 2.4, E
thernet, snaplen: 262144
339380        0x52DB4         PDF document, version: "1.5"
339454        0x52DFE         Zlib compressed data, default compression
340171        0x530CB         Zlib compressed data, default compression
6380104       0x615A48        Zlib compressed data, default compression
6385002       0x616D6A        Zlib compressed data, default compression
```


结果如图：



一堆莫名其妙的zlib文件和无后缀的文件，估计binwalk使用不对，蹲个好心人拯救一下我~~~

3. 总结

今天题不难，感觉有点累，刷不动了，附个美图欣赏欣赏吧！