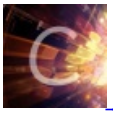
攻防世界-simple_transfer

原创

peng_xingang 于 2021-11-29 16:12:26 发布 2474 收藏
分类专栏： 攻防世界 杂项 文章标签： 安全 经验分享

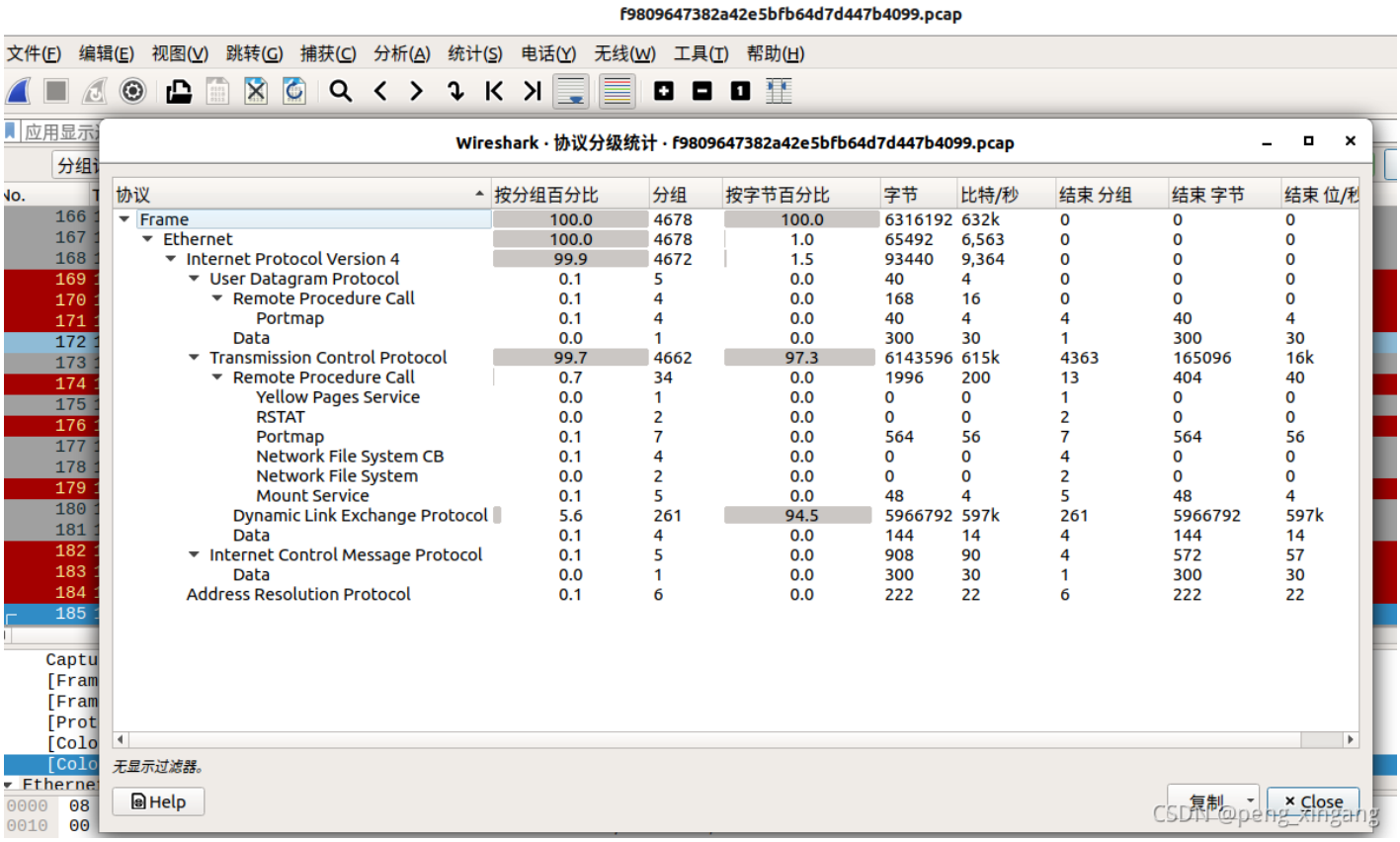


打开题目，下载附件，发现是一个pcap文件。

话不多说，放到wireshark里面追踪流量。

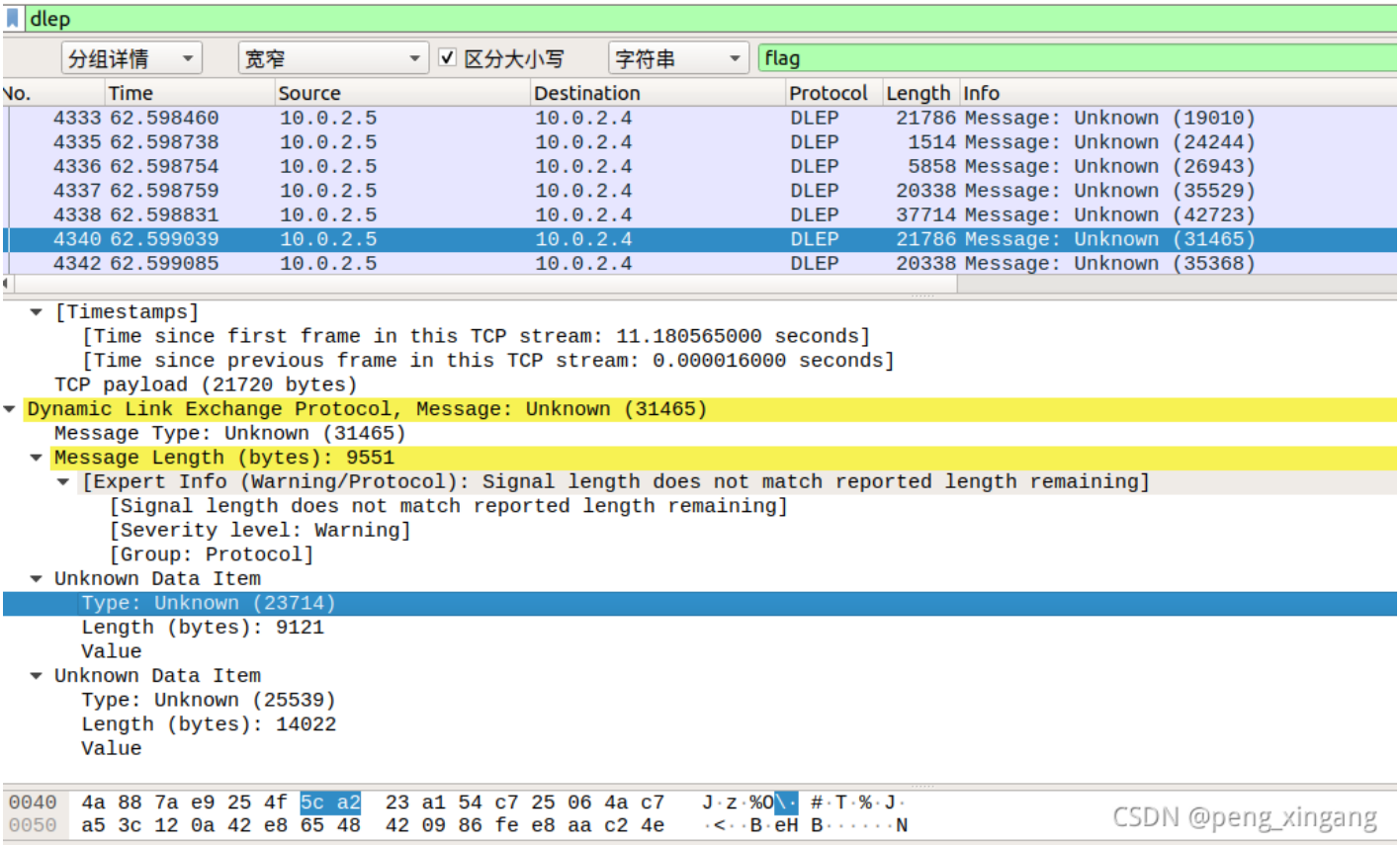
搜索flag，发现前面很多很多的TCP协议，但是追踪进去没啥东西。

这里选择统计->协议分级，看哪些协议的数据占比多。



找到一个占比94%的协议DLEP，那么就直接选中这个协议，右键作为过滤器应用直接开始搜索。

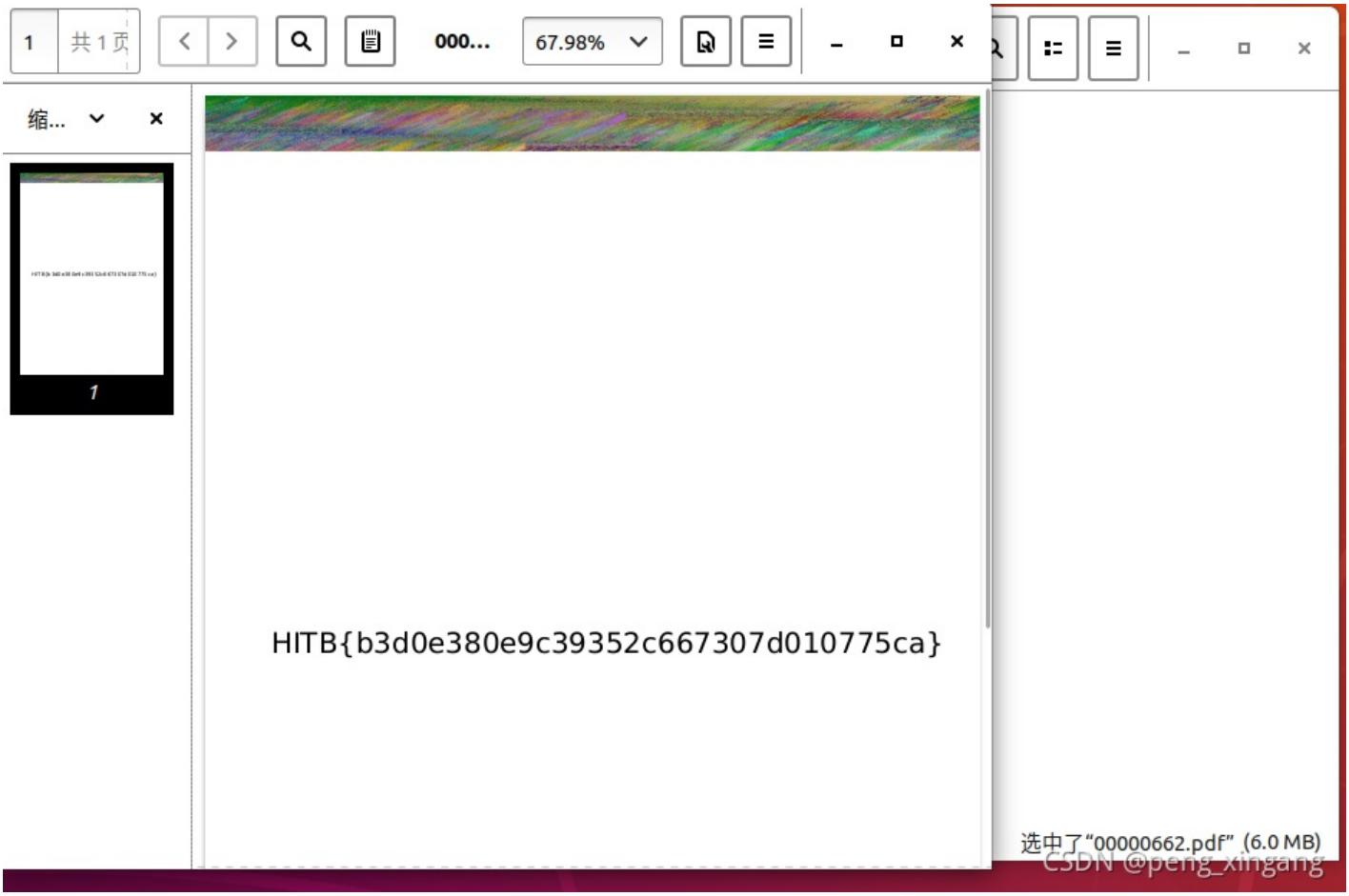
搜索出来，但是提示unknown message！



没有啥信息没关系，这么大个的unknown message摆在面前，尝试一下分解。

```
foremost -t all -i f9809647382a42e5bfb64d7d447b4099.pcap
```

发现输出一个pdf，打开就是flag。



```
HITB{b3d0e380e9c39352c667307d010775ca}
```

尝试提交，成功！