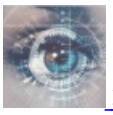
xctf攻防世界 MISC高手进阶区 Cephalopod

原创

l8947943 已于 2022-01-24 00:17:58 修改 10541 收藏

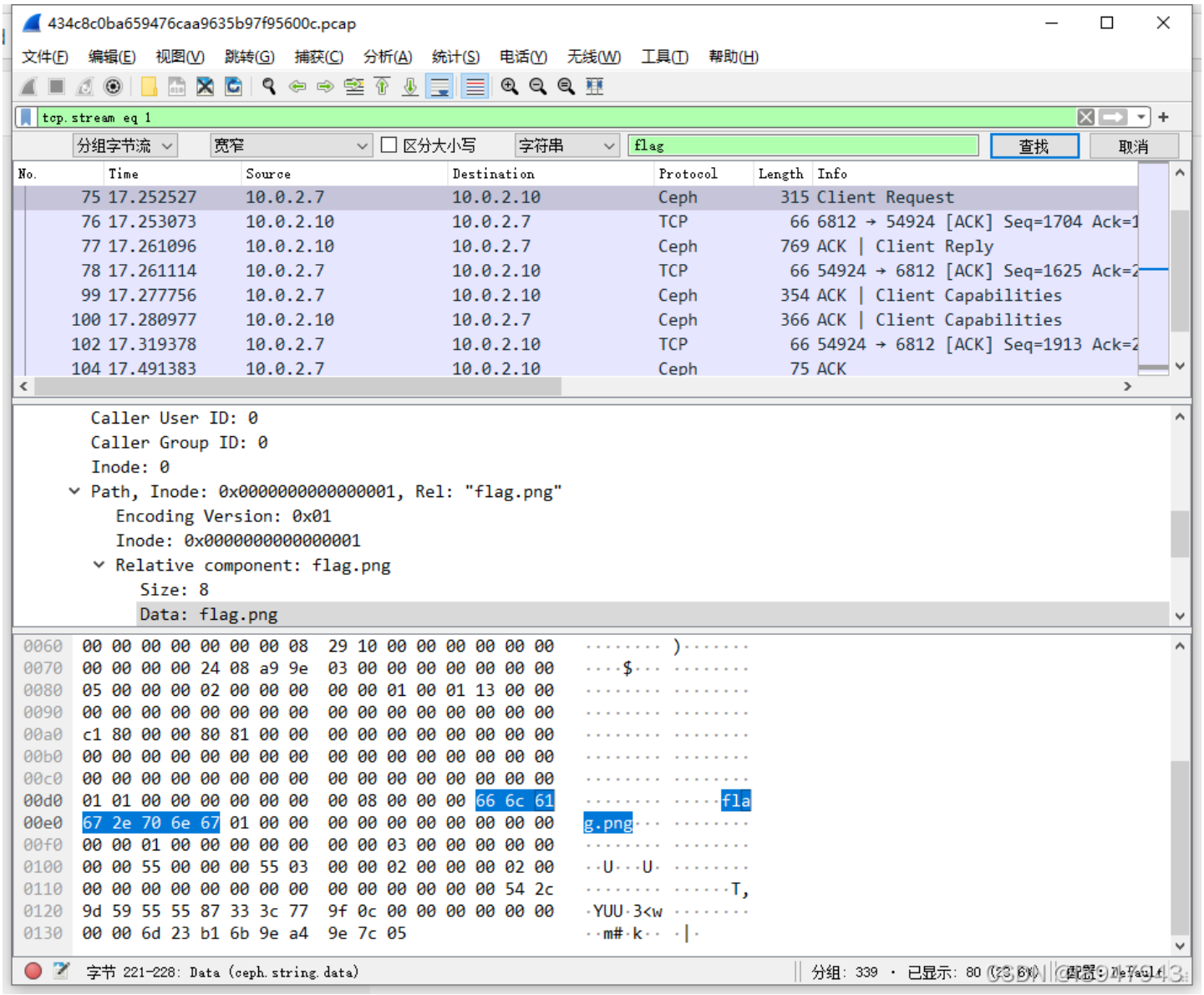
分类专栏： 攻防世界misc之路 文章标签： misc

于 2022-01-24 00:17:29 首次发布



1. 进入环境，下载附件

给的是一个pcap文件，果断塞入wireshark中，如图：



搜索到关键词

2. 问题分析

可以看到有一张png图片，那么判断流量包中可以提取该文件，尝试foremost并无法分离。

查看wp后，发现需要安装tcpxtract

```
sudo apt-get install tcpxtract
```

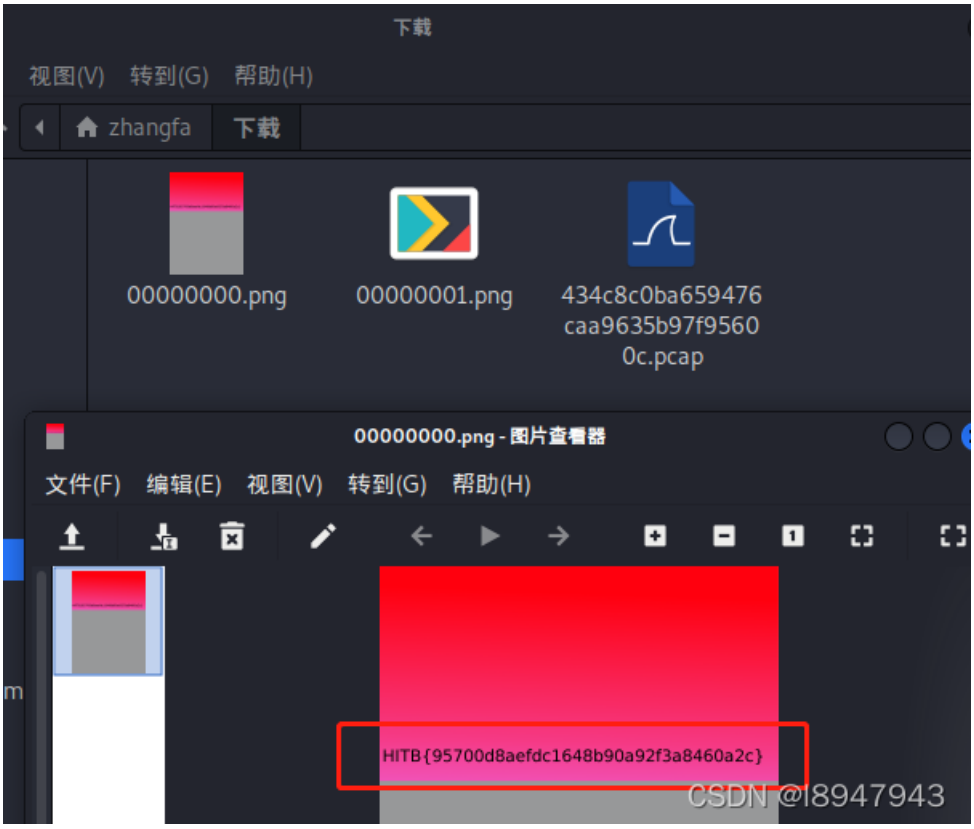
然后提取文件数据：

```
tcpxtract -f 434c8c0ba659476caa9635b97f95600c.pcap
```

```
┌──(zhangfa㉿kali)-[~/下载]
└─$ tcpxtract -f 434c8c0ba659476caa9635b97f95600c.pcap
Found file of type "png" in session [10.0.2.7:49818 → 10.0.2.10:36890], exporting
 to 00000000.png
Found file of type "png" in session [10.0.2.7:49818 → 10.0.2.10:36890], exporting
 to 00000001.png

┌──(zhangfa㉿kali)-[~/下载]
└─$
```

结果如图：



最终答案为：`HITB{95700d8aefdc1648b90a92f3a8460a2c}`