# xctf攻防世界 CRYPTO高手进阶区 工控安全取证

原创

l8947943 于 2022-02-24 18:58:11 发布 133 收藏

分类专栏： 攻防世界crypto之路 文章标签： 安全 web安全 网络





## 0x01. 进入环境，下载附件

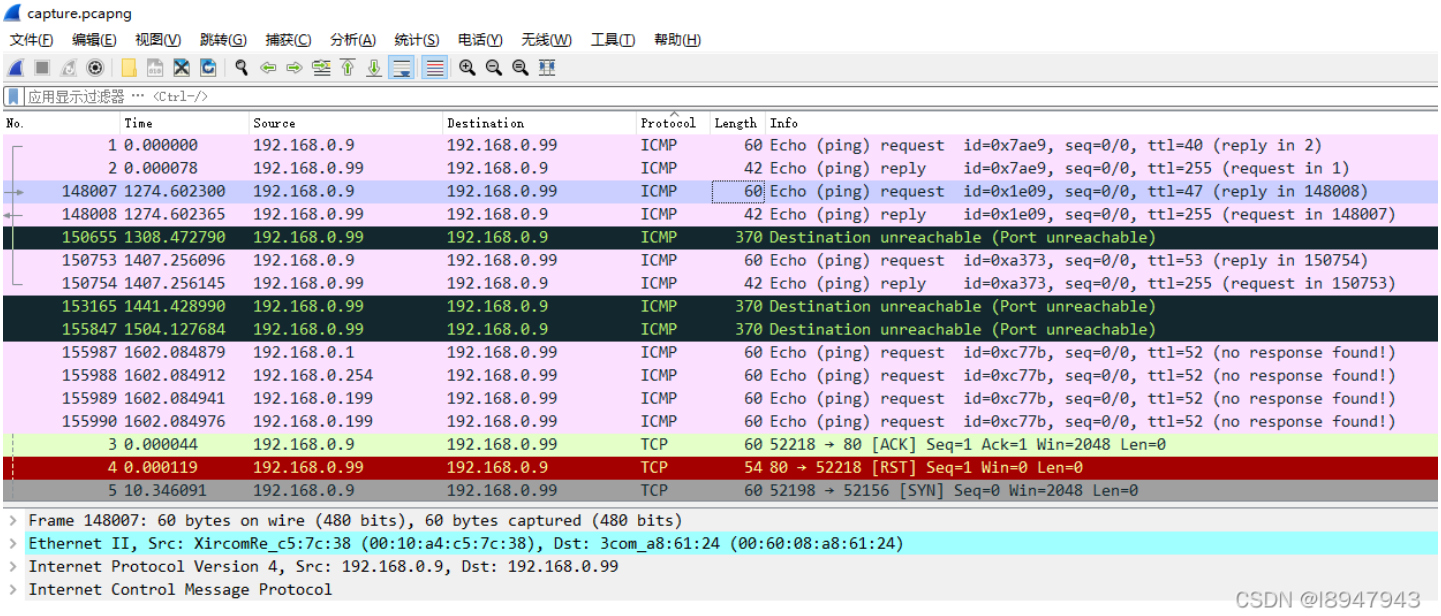
题目给的是一个日志文件，放入kali中查看文件类型：

```
file capture.log
```

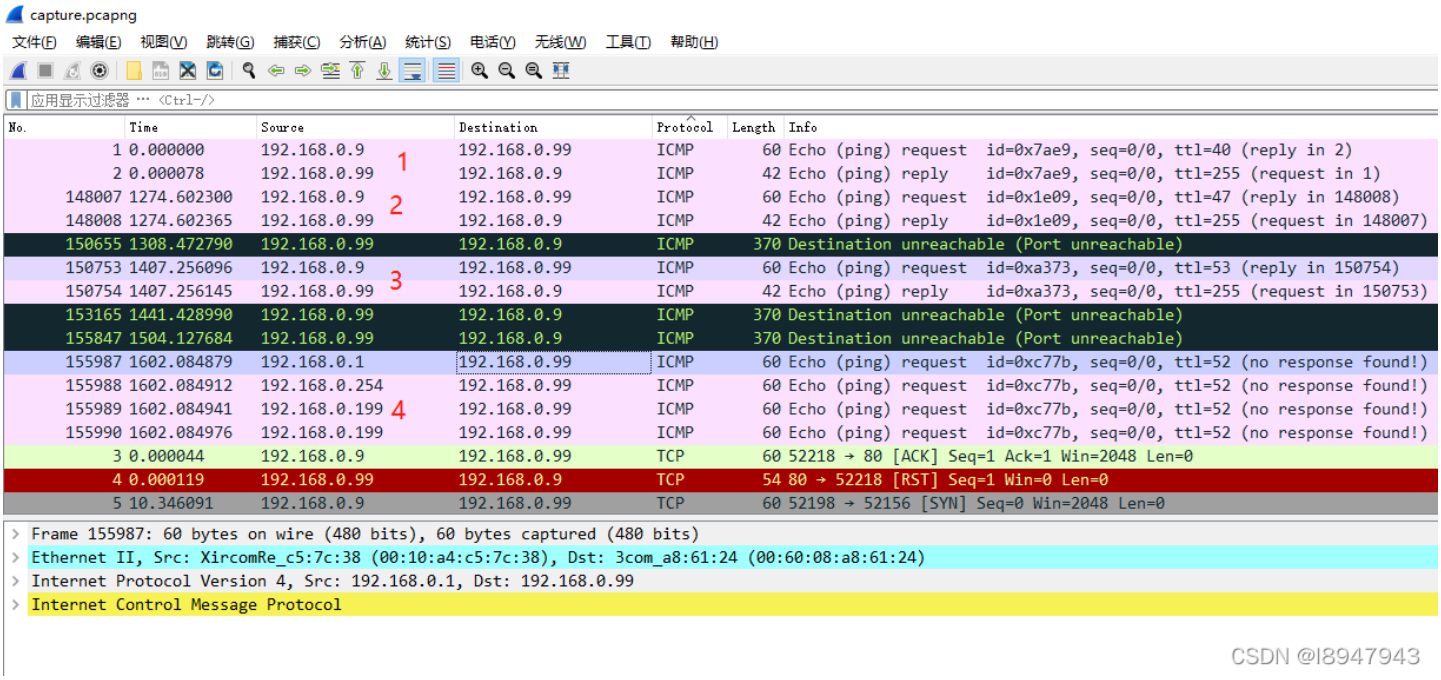
可以看到，该文件是一个pcapng流量包文件，如图：


## 0x02. 问题分析

将文件的后缀修改为pcapng，用wireshark打开，发现是一堆tcp链接和少量的ICMP链接。题目提示是对端口进行多次扫描，扫描端口一般是利用ICMP回显请求，那么我们对icmp进行排序，如图：




我们可以看到，题目让找到第四次的扫描编号，如图，对流量进行分析




ICMP请求第一组编号有发出也有回显正常的信息，我们认为该次扫描为一次正常的扫描；第二组和第三组同理！！！

第四组为什么是155989？第四次我们可以推测在155987到155990之间。

但在一个c类地址网段中，一般地址为1-254可用，第四个字节全0和全1都是不可用，一般首位地址和末尾地址用于特殊设备使用，因此推测第四次扫描编号为155989。

最终答案为：`flag{155989}`