Wireshark软件对多个报文进行合并的方法

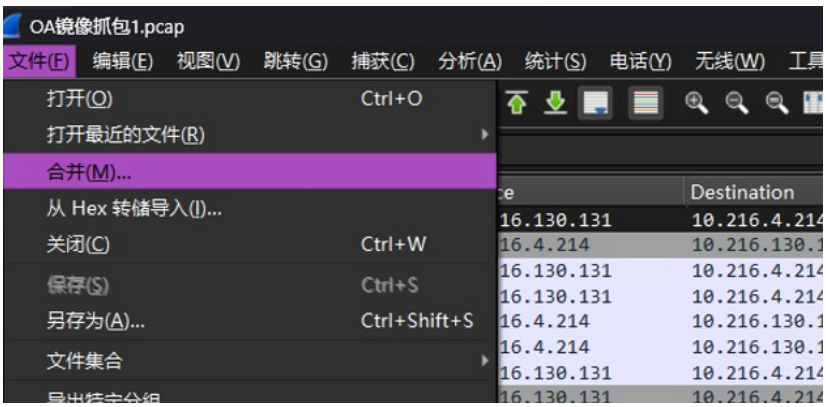
网络相关 网络相关 胡伟 2024-03-29 发表

问题描述

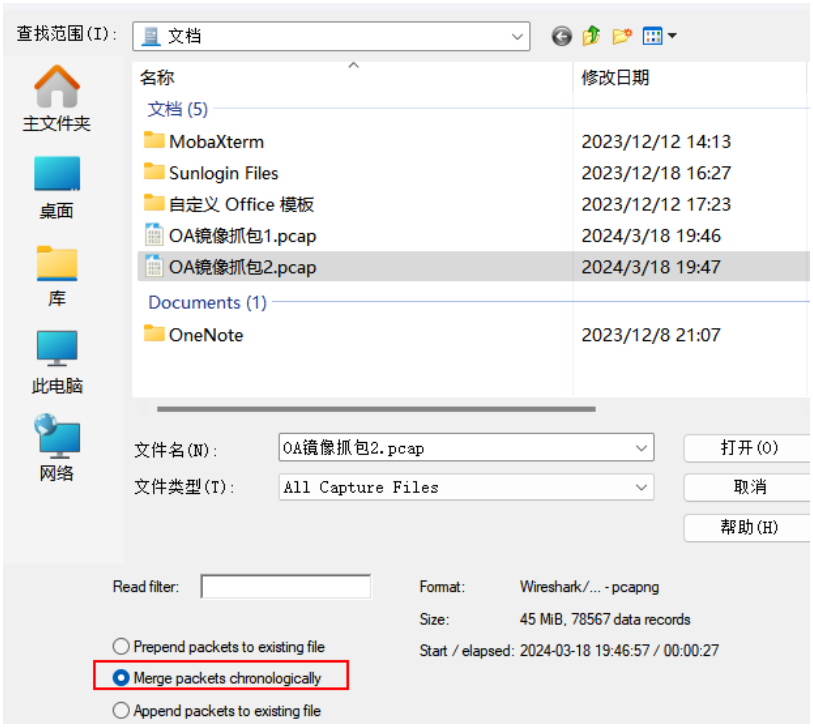
在分析抓包的时候通常需要对多个报文进行对比分析，比如报文经过设备的处理时延、往返时间、协议交互过程，此时如果将多个报文合并为一个报文后分析更为直接。

解决方法

1、在Wireshark软件已打开的第一个报文中，点击【文件】菜单栏【合并】选项。



2、在弹出的窗口中选择要合并的第二个报文，选择【Merge packets chronologically】后点击【打开】按钮即可进行报文自动合并。



> Prepend packets to existing file：将待打开pcap文件的报文插入到已打开pcap文件的前面
> Merge packets chronologically：将两个pcap文件的报文按照时间顺序进行合并
> Append packets to existing file：将待打开pcap文件的报文插入到已打开pcap文件的末尾