Wireshark抓包软件抓取大流量报文（>200MB）的方法

网络相关 网络相关 胡伟 2024-03-29 发表

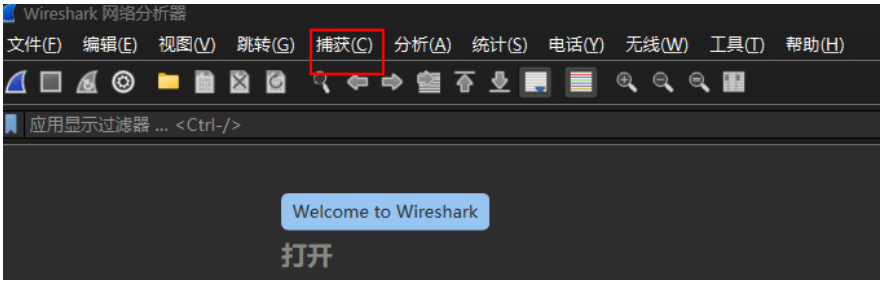
问题描述

在分析网络流量的过程中，通常使用流镜像或端口镜像的方式将业务流镜像到笔记本，同时打开Wireshark抓包软件进行实时分析，但是当镜像的流量过大或抓包时间过长时，容易导致Wireshark软件卡死，报文分析无法正常完成。

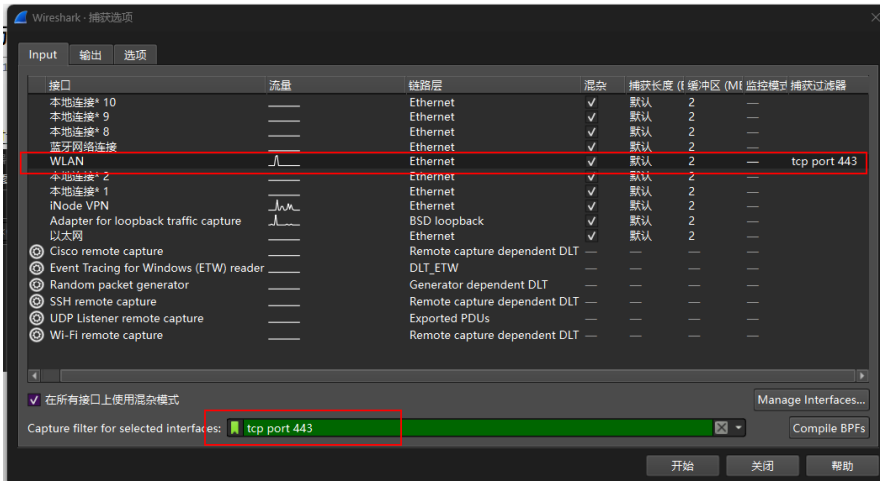
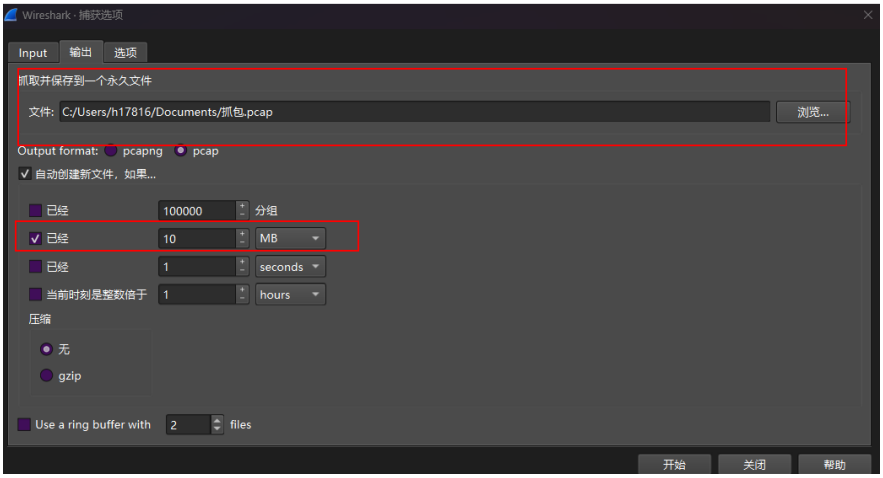
解决方法

Wireshark需要对抓取的报文进行分段保存，即抓取的报文到达某个阈值时自动保存，并自动重新抓取剩余的报文。

1、打开Wireshake软件，点击【捕获】菜单。



2、在弹出的【捕获窗口】选项中，在【Input】页面中，选择对应的接口，这里我以WLAN接口举例。同时可对报文进行过滤，只抓取需要的业务流量，这里我以https流量举例（tcp port 443）。



3、在输出页面中，选择对应的文件保存目录。同时确定自动创建新文件的方式，建议200MB生成一个抓包文件。