

问题描述

wireshake拆分大包、Ethernet文件解析成PPP格式、16进制debug转换为PCAP格式示例。

解决方法

wireshake拆分大包

示例：以10000行为单位拆分

`editcap.exe -c 10000 D:\Softwares\Wireshark\test.pcap E:\报文转换\test.pcap wireshake`

把Ethernet文件解析成PPP格式

在镜像抓串口的报文时，PC会将报文理解成以太帧导致报文无法正常解析，这个时候就需要还原为PPP帧。

示例：`editcap.exe -T ppp 20200724.pcap 20200724_1.pcap`

wireshake将16进制debug转换为PCAP格式

示例：`text2pcap.exe a.txt a.pcap`