

****

信息学院软件工程系

《计算机网络》实验报告

**题　　目 实验三　基于PCAP库侦听并分析网络流量**

**班　　级 数字媒体技术2020级**

**姓　　名 庞天骏**

**学　　号 22920202202910**

**实验时间 2022年11月14日**

# 实验目的

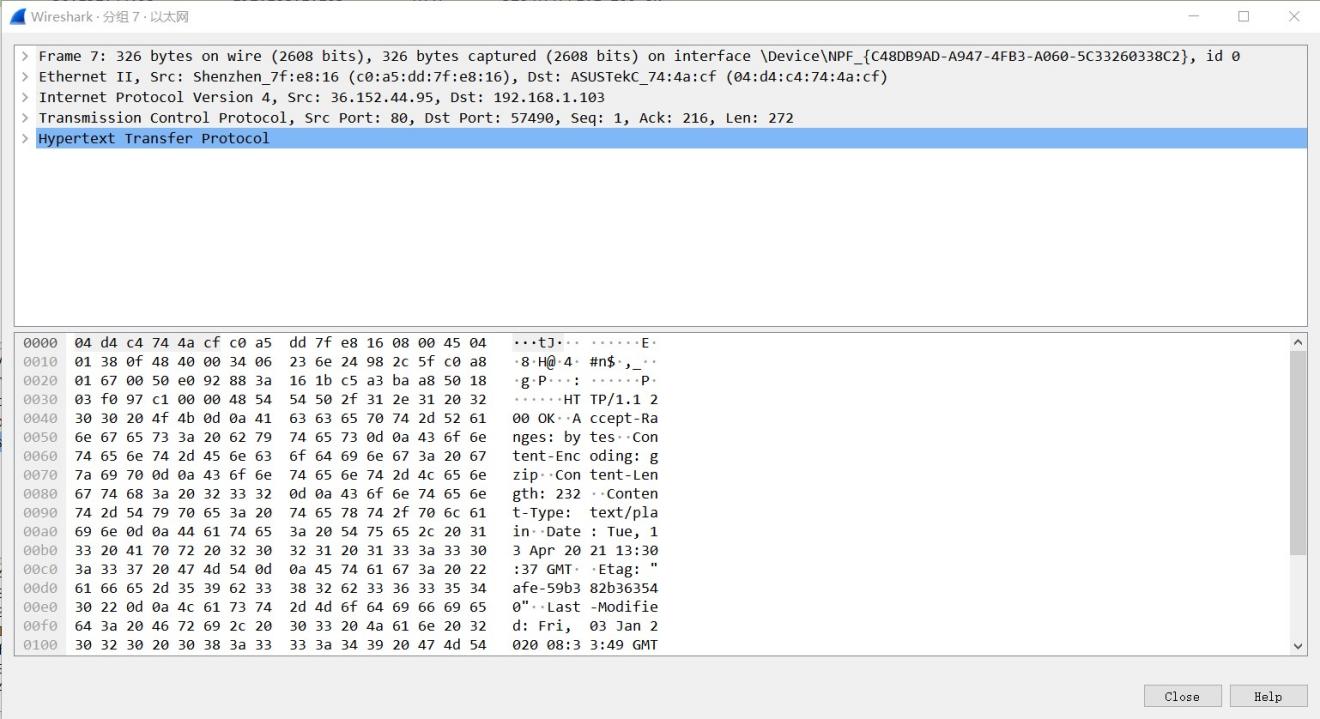
通过完成实验，理解数据链路层、网络层、传输层和应用层的基本原理。掌握用Wireshark观察网络流量并辅助网络侦听相关的编程；掌握用Libpcap或WinPcap库侦听并处理以太网帧和IP报文的方法；熟悉以太网帧、IP报文、TCP段和FTP命令的格式概念，掌握TCP协议的基本机制；熟悉帧头部或IP报文头部各字段的含义。熟悉TCP段和FTP数据协议的概念，熟悉段头部各字段和FTP控制命令的指令和数据的含义。

# 实验环境

操作系统：Windows10

# 实验结果

1. 用侦听解析软件观察数据格式
2. 网络协议层次嵌套



·Frame：物理层的数据帧概况。

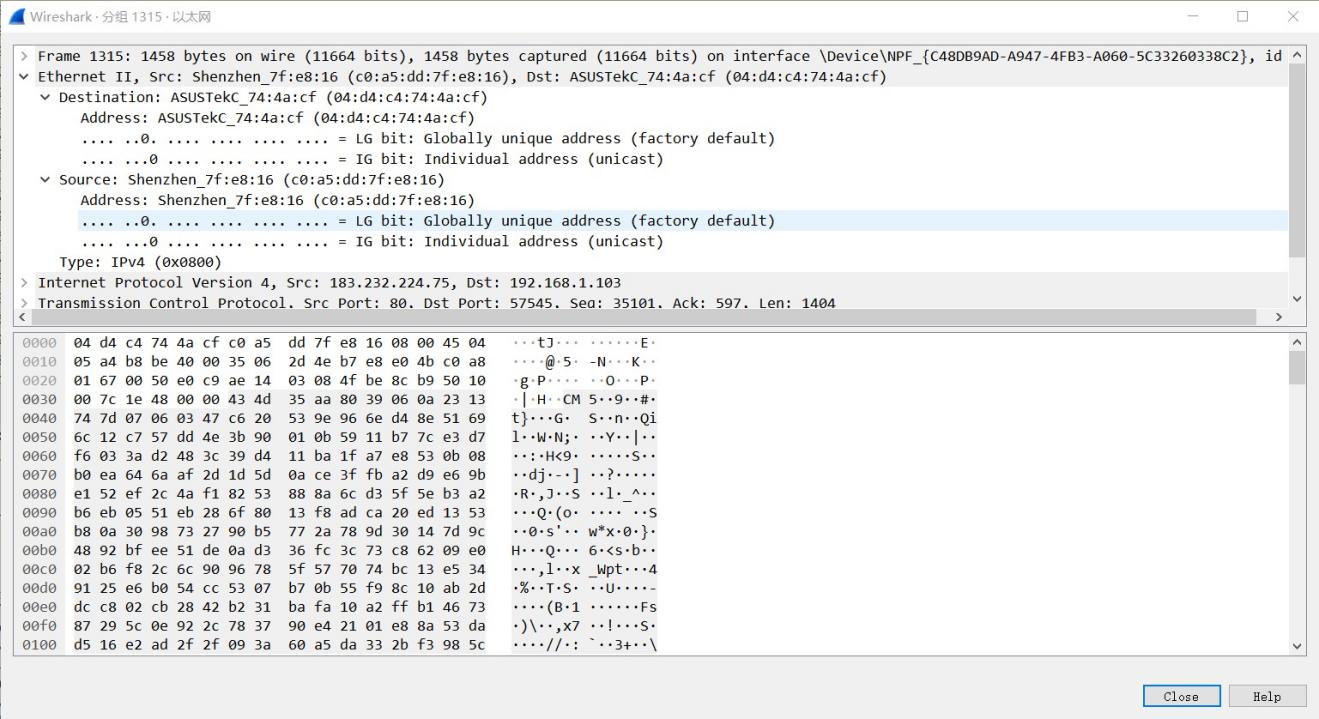
·Ethernet II：数据链路层以太网头部帧。

·Internet Protocol Version 4：互联网层IP报头的信息。

·Transmission Control Protocol：传输层的数据段头部信息，此处是TCP协议。

·Hypertext Transfer Protocol：应用层的信息，此处是HTTP协议。

1. 以太网帧格式

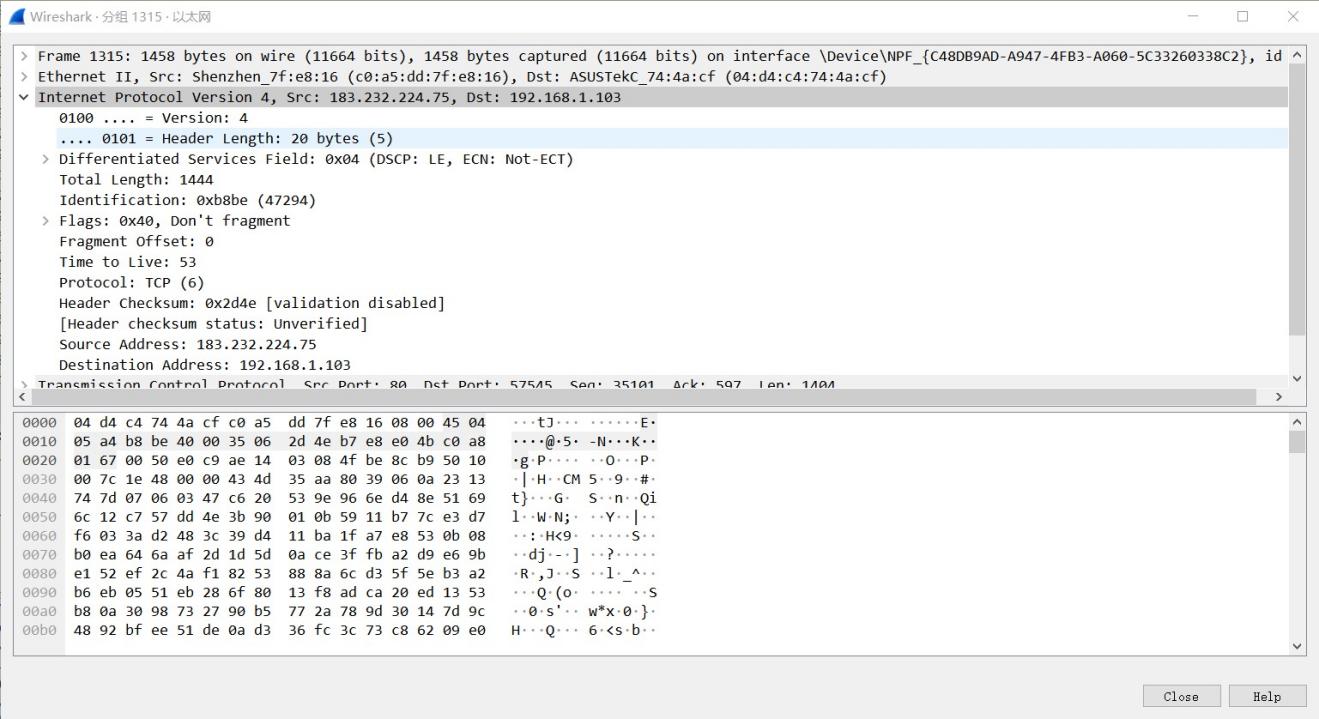


Destination Address：目的地址

Source Address：源地址

Type：类型

1. IP报文格式



Version：版本

Header Length：首部长度

Differentiated Services Field：区分服务

Total Length：总长度

Identification：标识

Flags：标志

Fragment Offset：片位移

Time to Live：生存时间

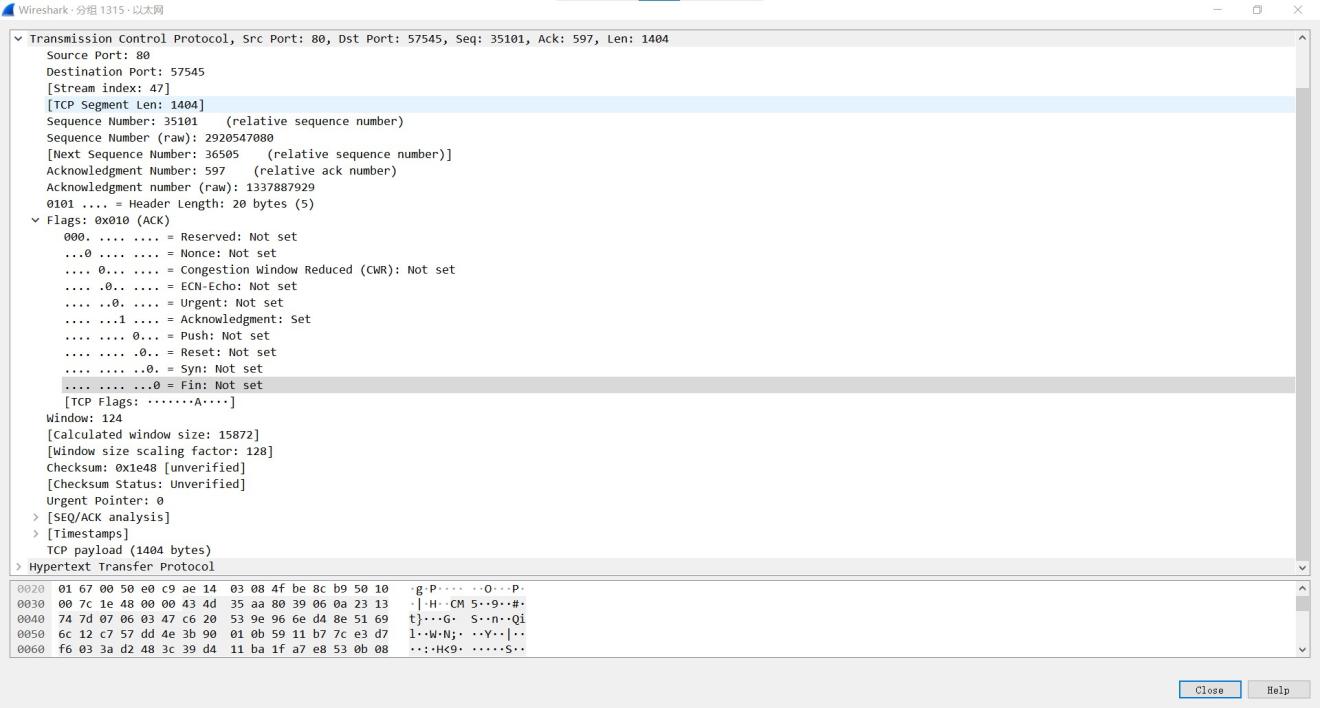
Protocol：协议

Header Checksum：首部校验和

Source Address：源地址

Destination Address：目的地址

1. TCP段格式



Source Port：源端口

Destination Port：目的端口

Sequence Number：序号

Acknowledgment Number：确认号

Header Length：首部长度

Reserved：保留

Urgent：URG紧急控制位

Acknowledgment：ACK确认控制位

Push：PSH推送控制位

Reset：RST复位控制位

Syn：SYN同步控制位

Fin：FIN终止控制位

Window：窗口

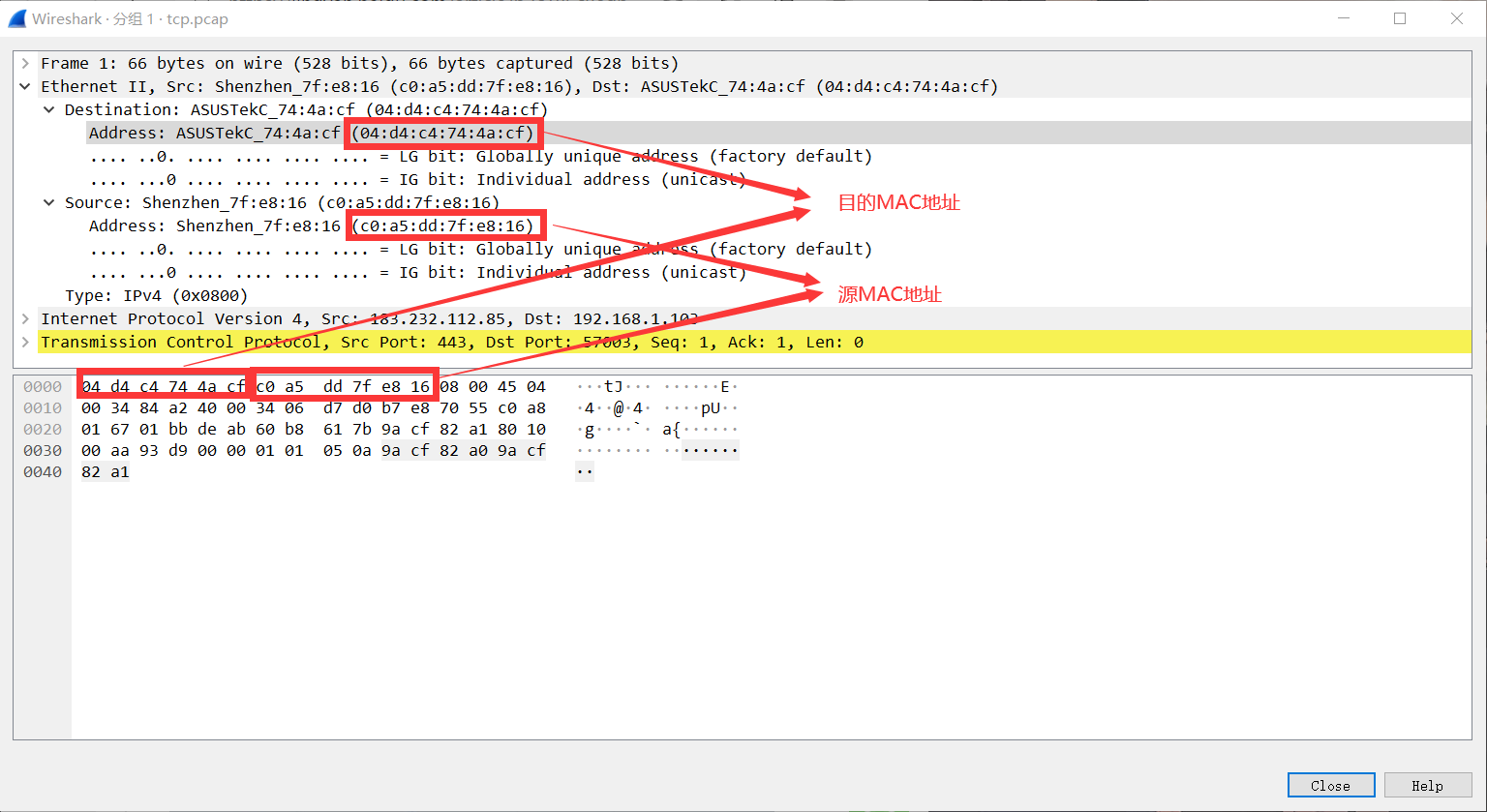
Checksum：校验和

Urgent Pointer：紧急指针

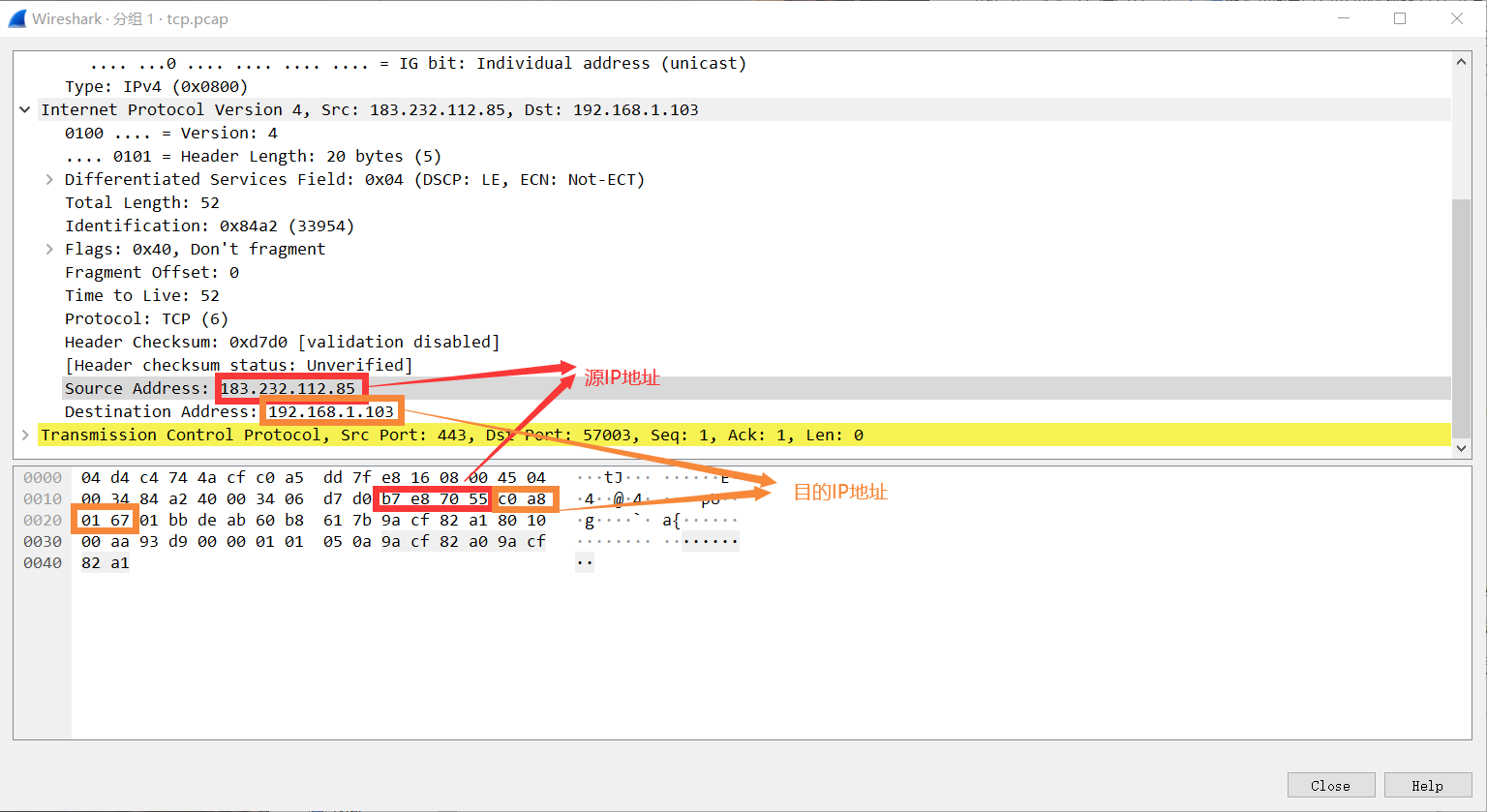
Timestamps：时间戳选项

TCP payload：TCP有效载荷

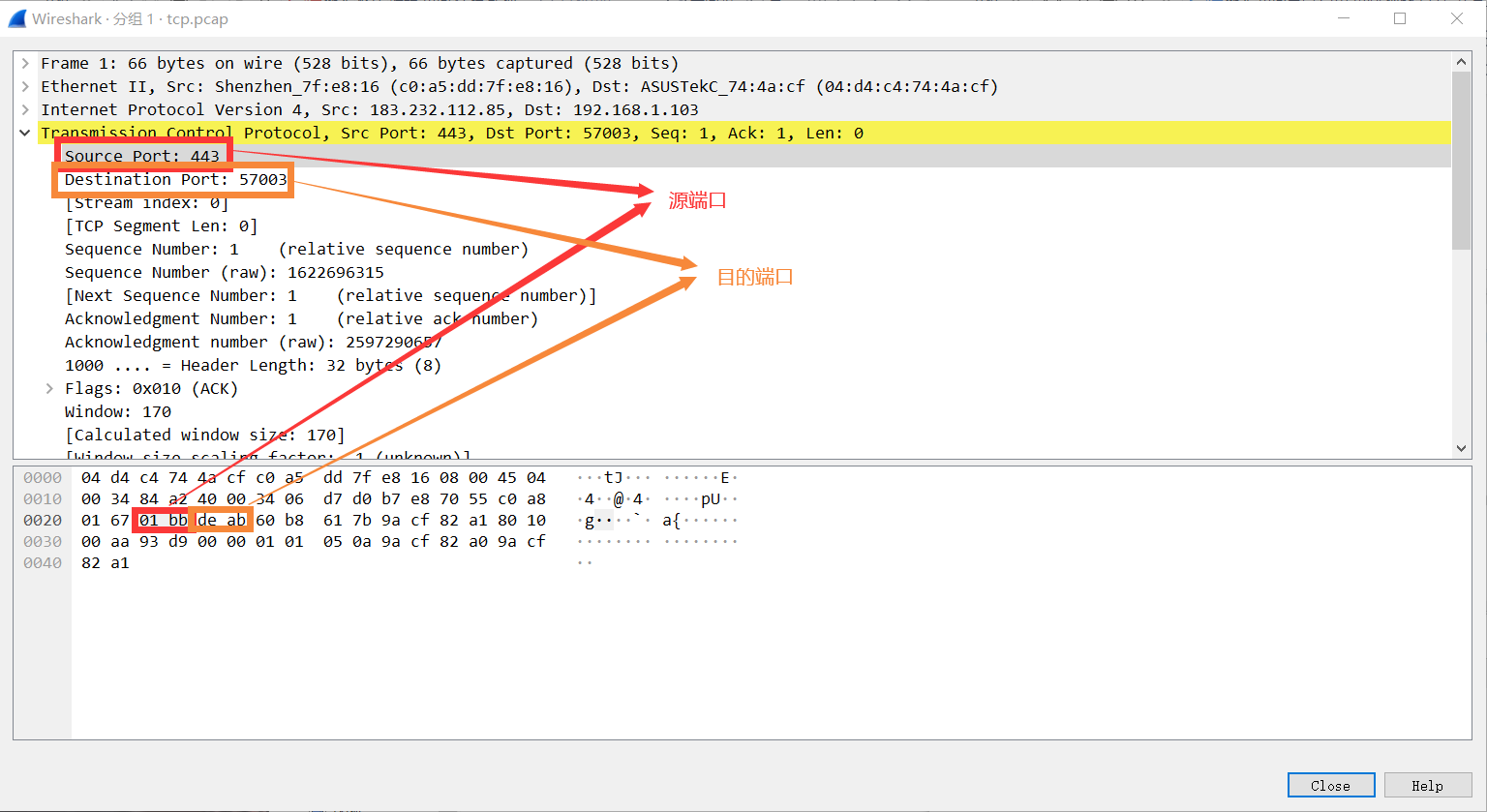
1. FTP协议命令和相应的格式
2. MAC地址



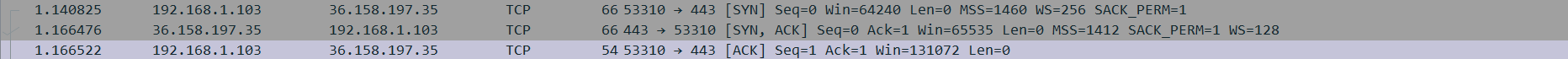
1. IP地址



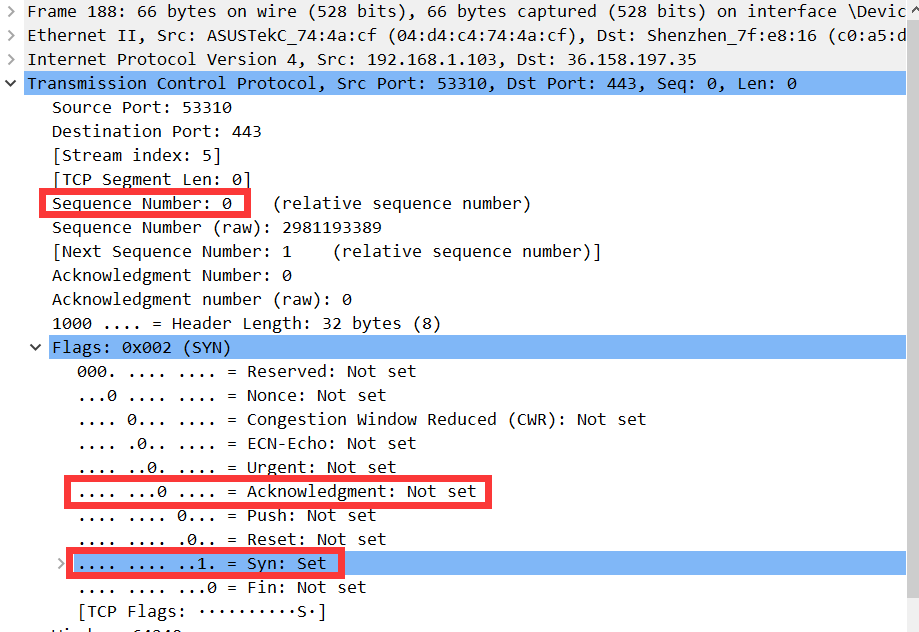
1. TCP端口



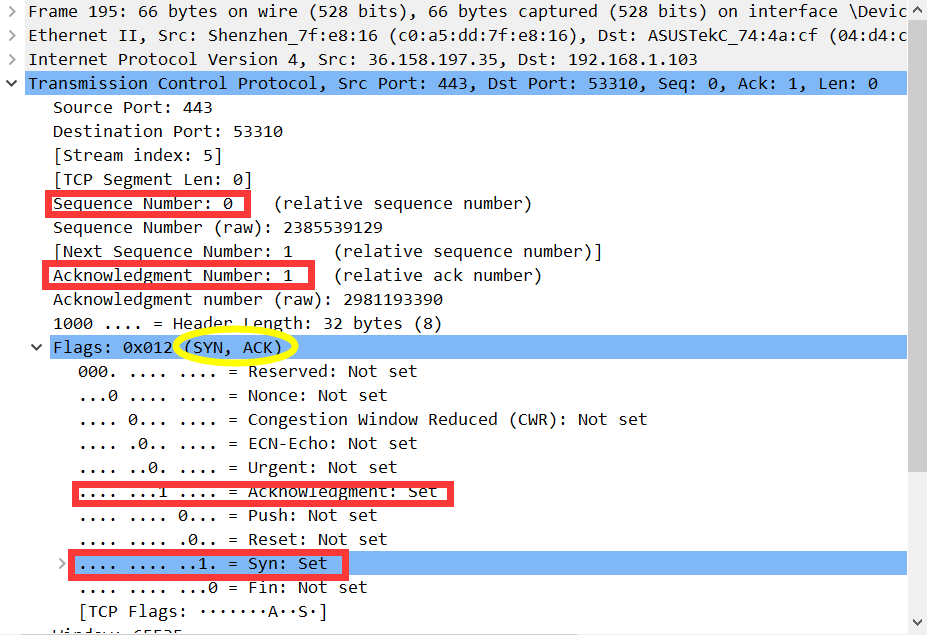
1. 用侦听解析软件观察TCP机制
2. TCP建立的三次握手连接



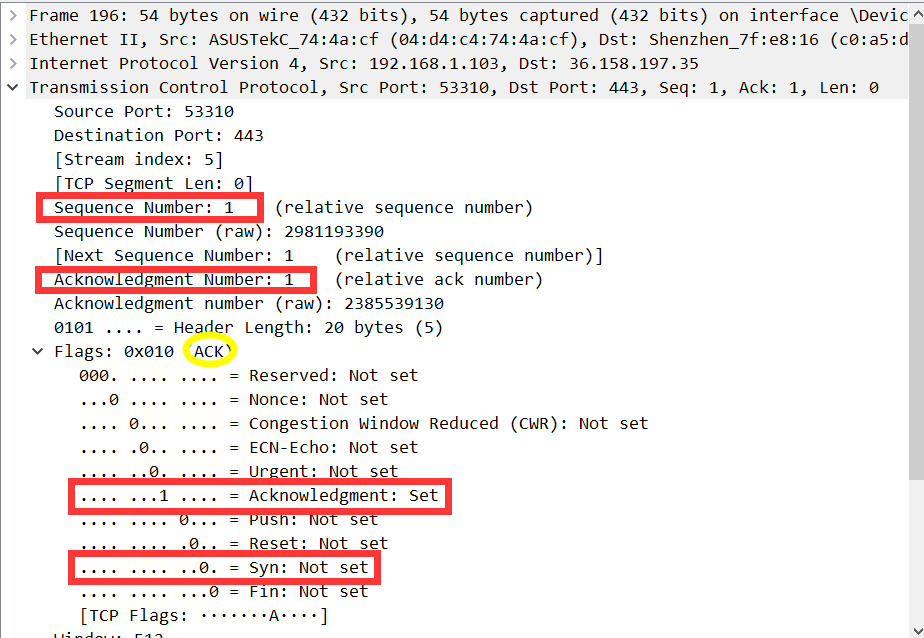
1. 第一个握手数据包：客户端发送一个TCP，标志位为SYN，序列号为0，代表客户端请求建立连接。



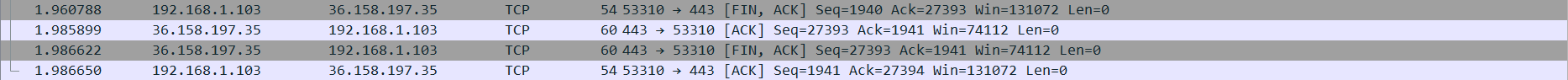
1. 第二个握手数据包：服务器接收到客户端的SYN报文，回复SYN+ACK报文。报文标志SYN，ACK，ACK number=接收到的Seq+1=1，自己的Seq=0。



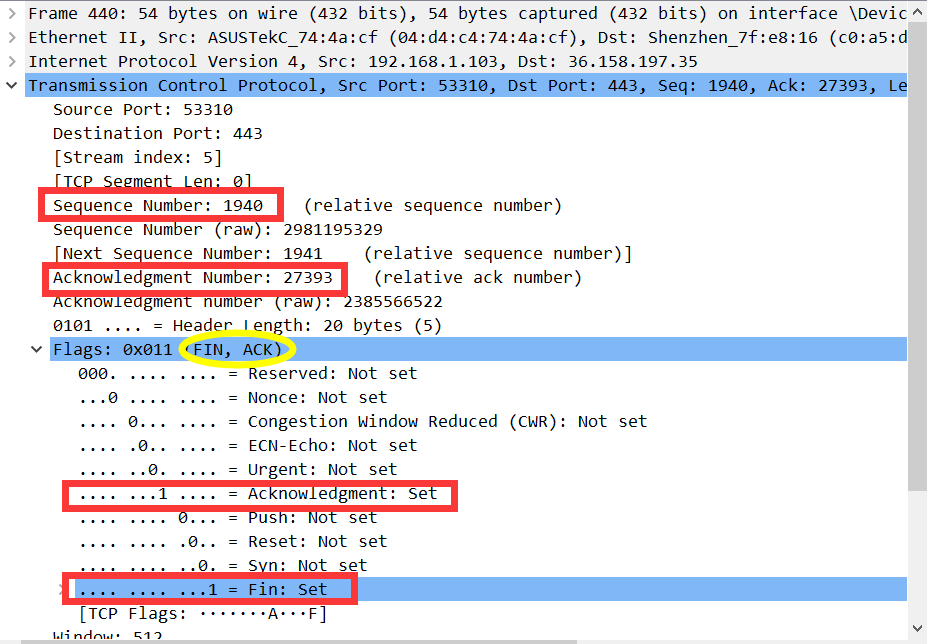
1. 第三个握手数据包：客户端接收到服务端的SYN+ACK报文后，回复ACK报文。报文标志ACK，Seq=1，ACK=接收到的Seq+1=1。



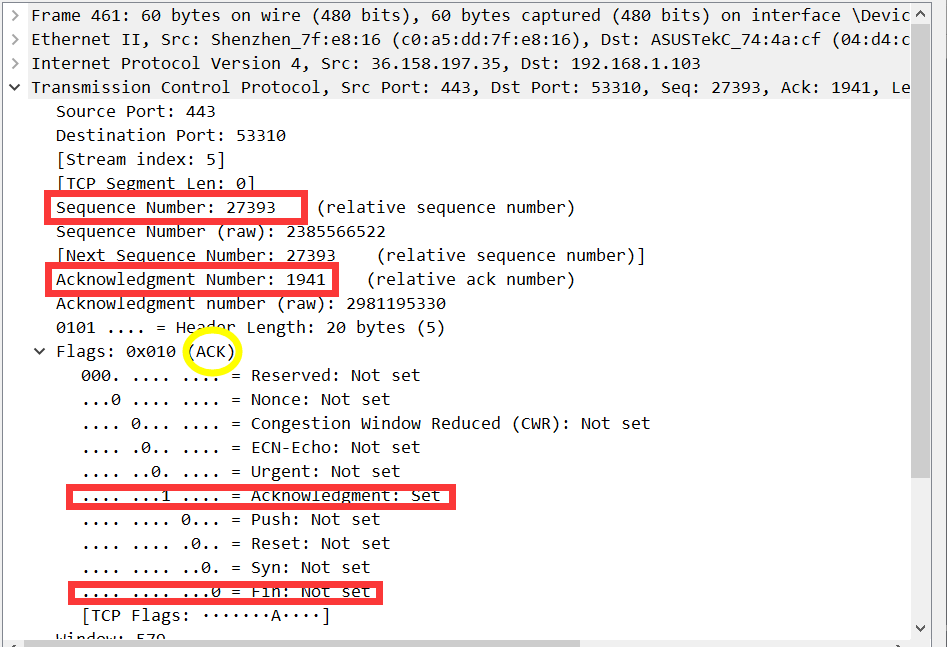
1. TCP撤除连接的四次挥手操作



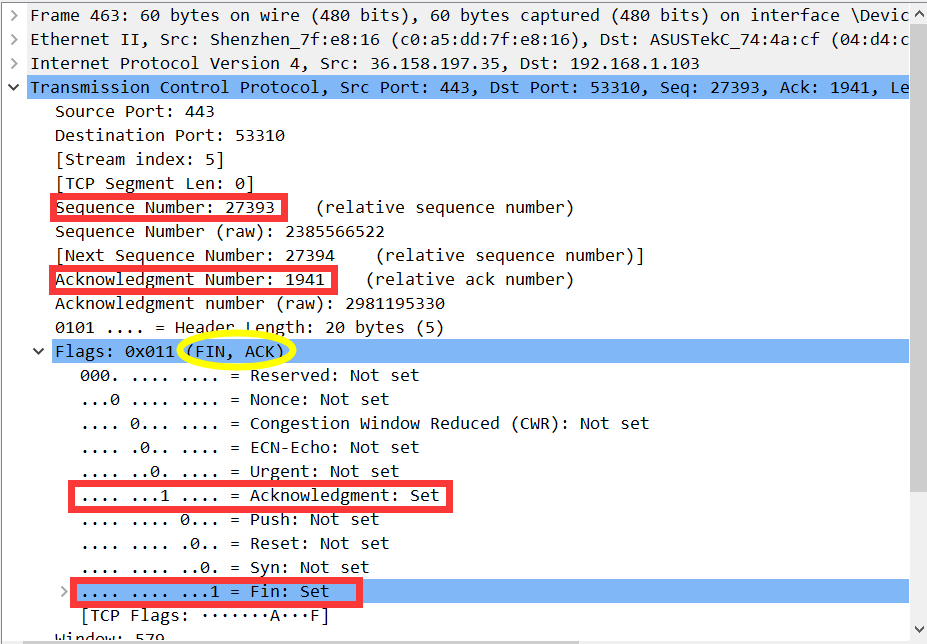
1. 第一次挥手：FIN+ACK。客户端发送一个FIN，用来关闭客户到服务器的数据传送。



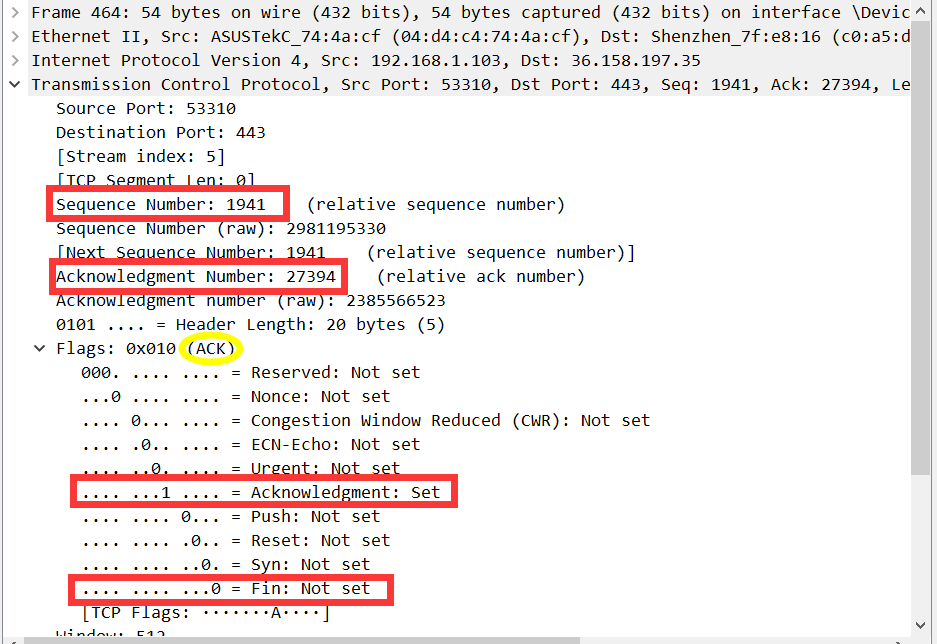
1. 第二次挥手：ACK。服务器收到这个FIN，它发回一个ACK，确认序号为收到的序号加1。



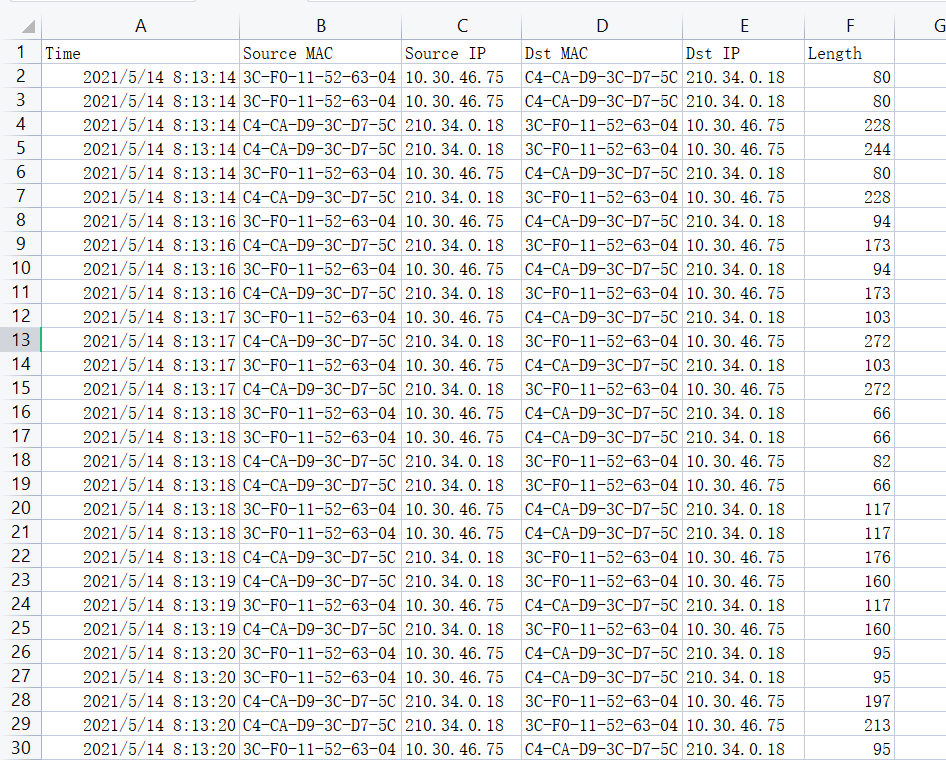
1. 第三次挥手：FIN+ACK。服务器关闭与客户端的连接，发送一个FIN给客户端。

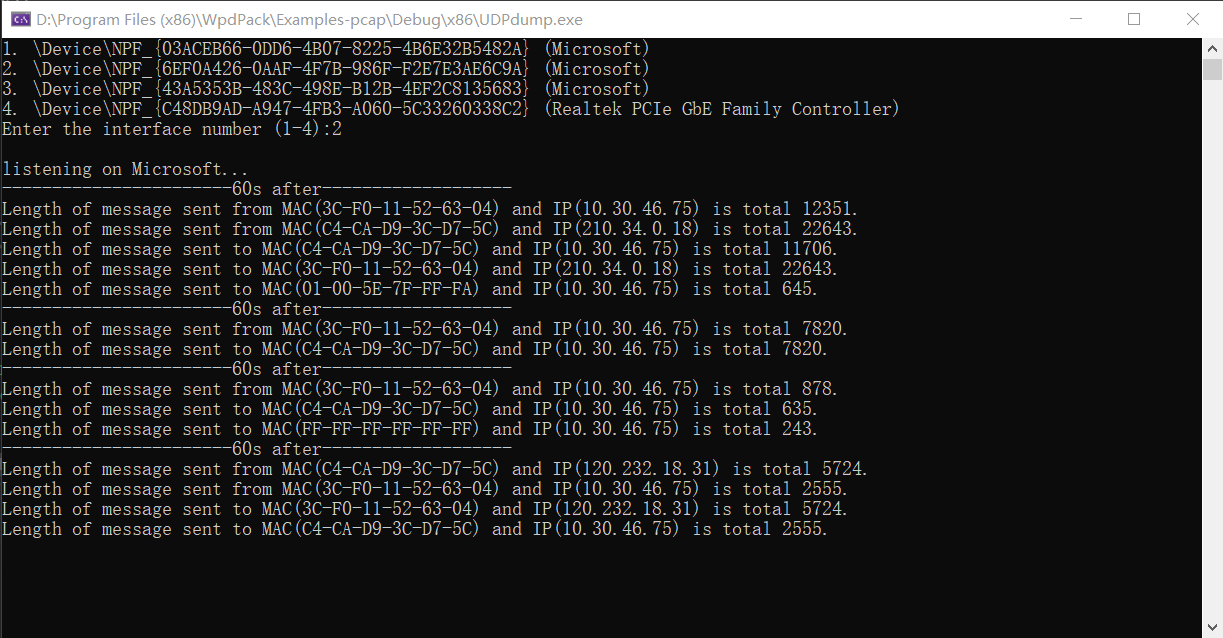


1. 第四次挥手：ACK。客户端发回ACK报文确认，并将确认序号设置为收到序号加1。

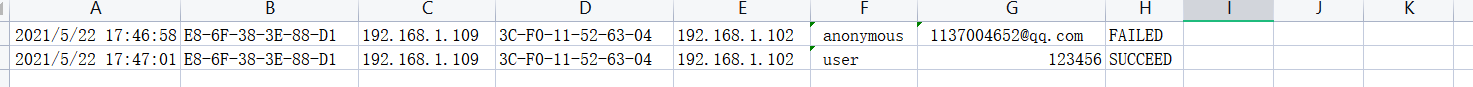


1. 用Libpcap或WinPcap库侦听网络数据





1. 解析侦听到的网络数据



# 实验代码

本次实验的代码已上传于以下代码仓库：

https://github.com/0maple-syrup0/EX3.git

# 实验总结

通过此次实验，理解了数据链路层、网络层、传输层和应用层的基本原理。掌握了用Wireshark观察网络流量并辅助网络侦听相关的编程；熟悉了以太网帧、IP报文、TCP段和FTP命令的格式概念，掌握了TCP协议的基本机制；熟悉了帧头部或IP报文头部各字段的含义。熟悉了TCP段和FTP数据协议的概念，熟悉了段头部各字段和FTP控制命令的指令和数据的含义。