厦門大學

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

1 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。

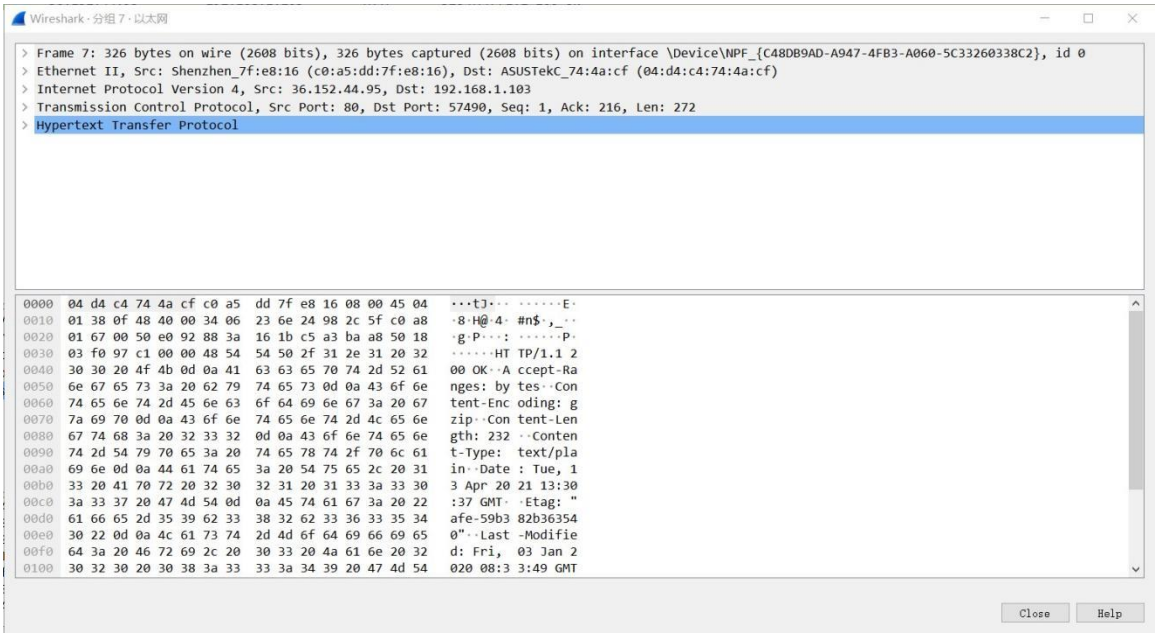
2 实验环境

操作系统：Windows10

3 实验结果

1. 用侦听解析软件观察数据格式

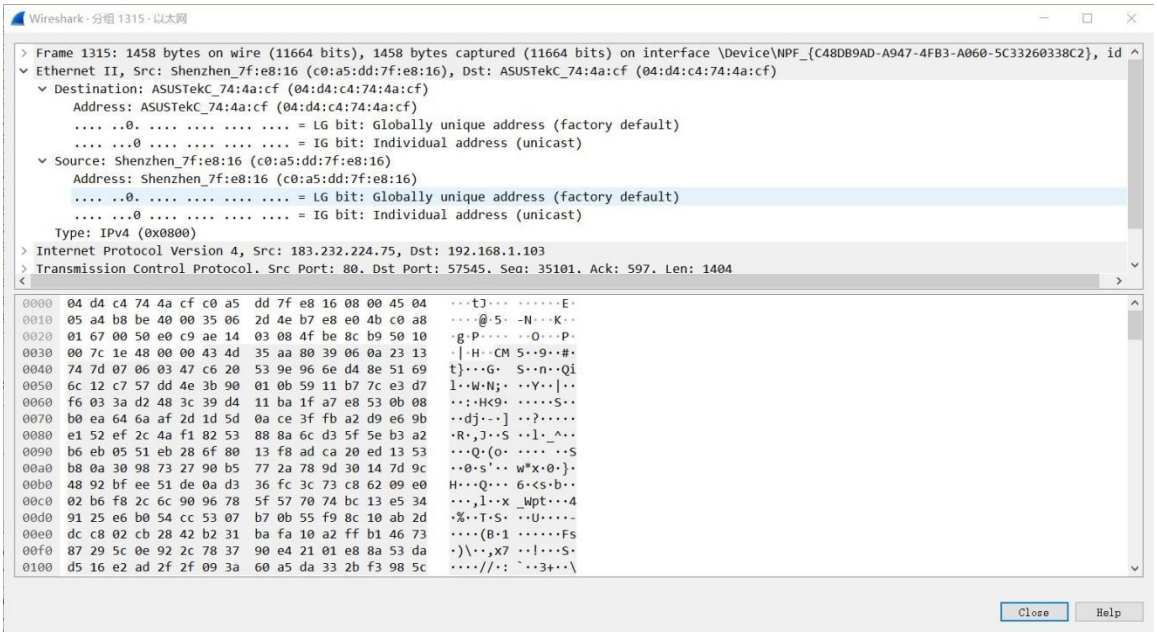
（1）网络协议层次嵌套



• 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。

（2）以太网帧格式

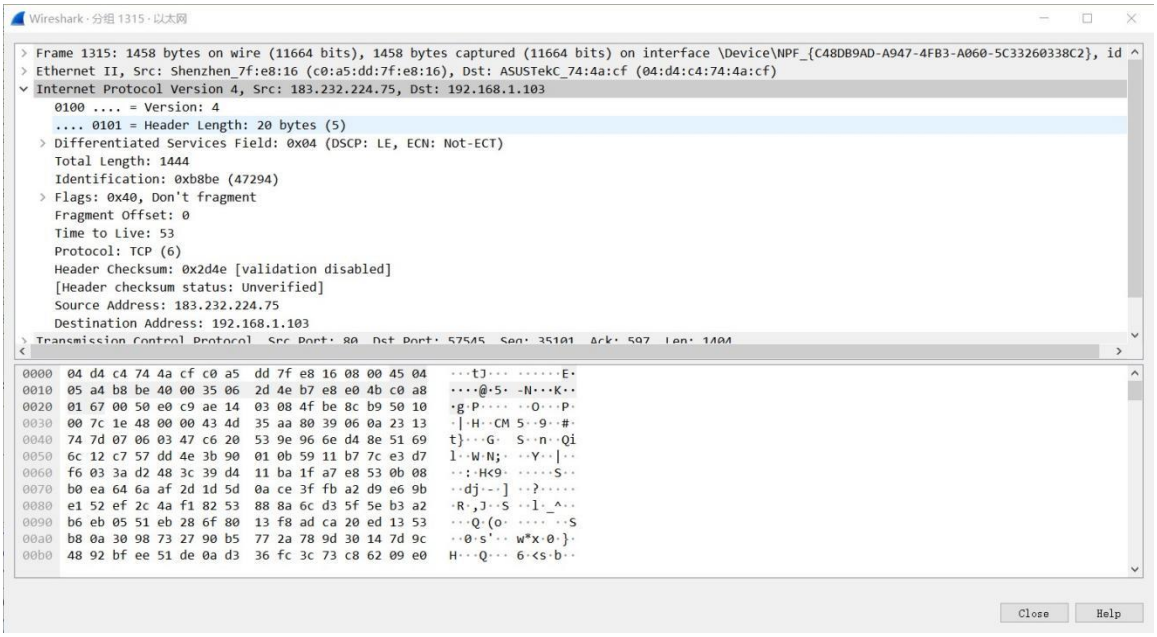


Destination Address：目的地址

Source Address：源地址

Type：类型

（3）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

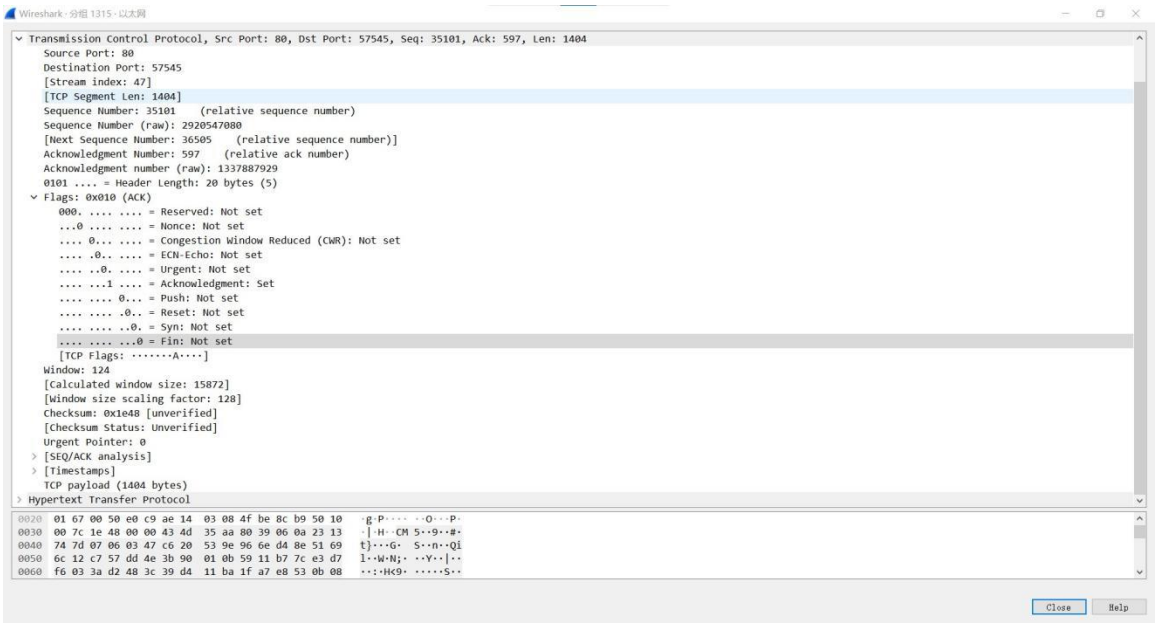
Protocol：协议

Header Checksum：首部校验和

Source Address：源地址

Destination Address：目的地址

（4）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

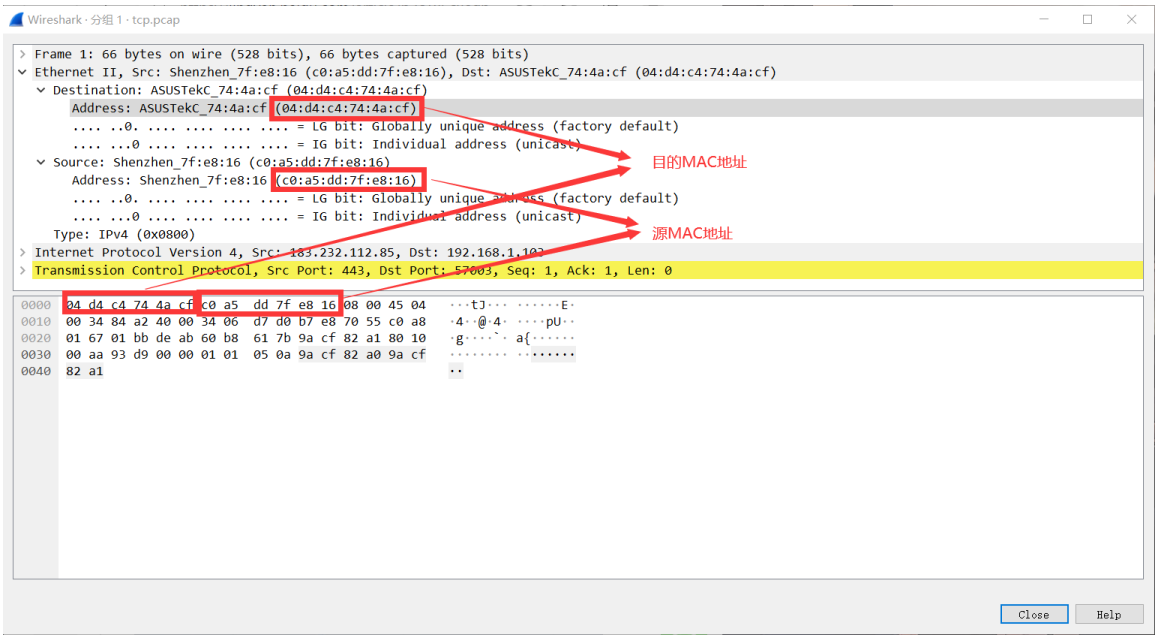
Urgent Pointer：紧急指针

Timestamps：时间戳选项

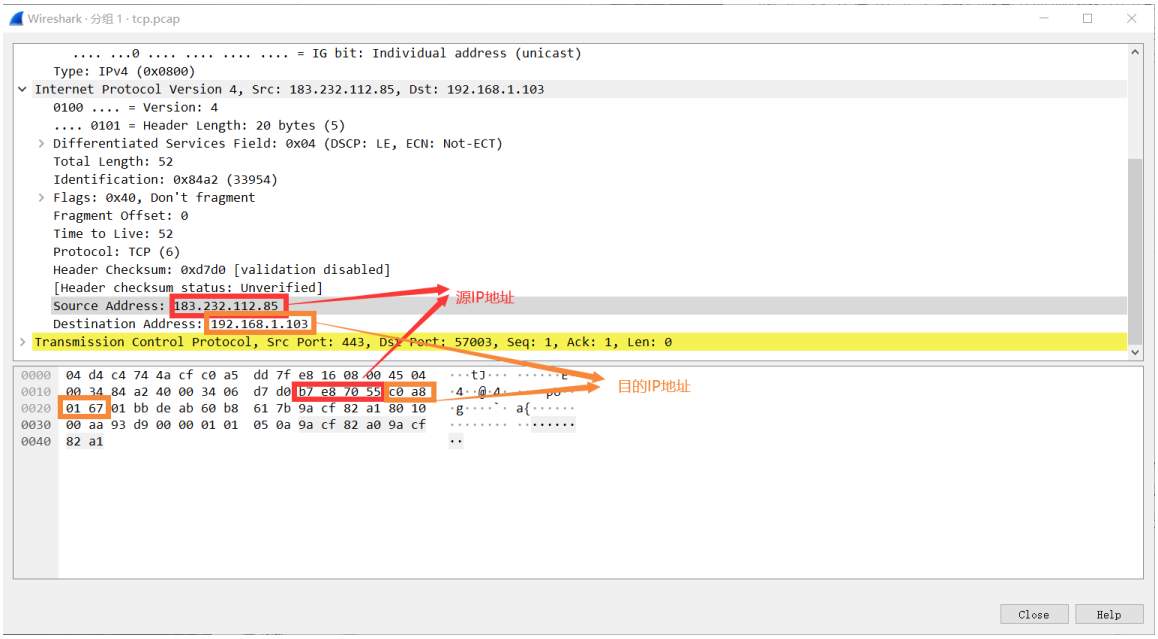
TCP payload：TCP 有效载荷

（5）FTP 协议命令和相应的格式

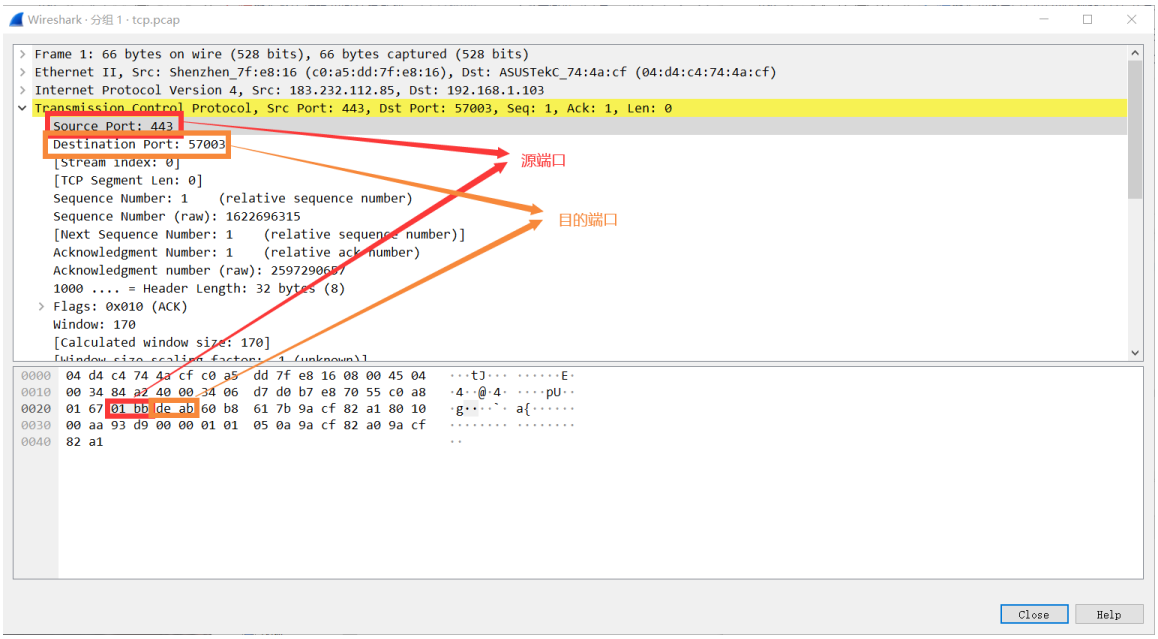
（6）MAC 地址



（7）IP 地址

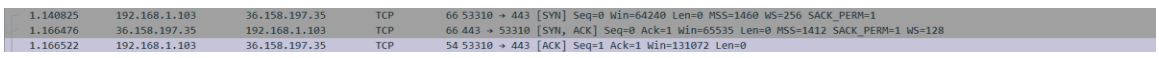


（8）TCP 端口

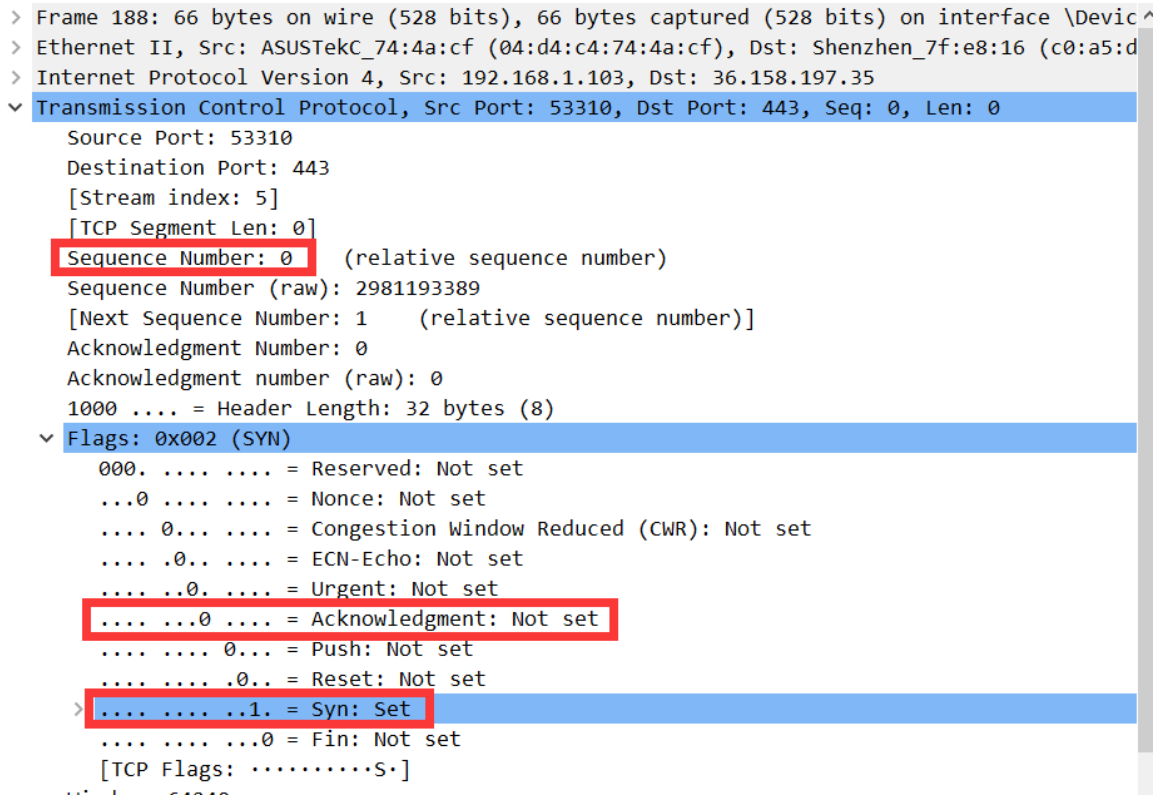


2. 用侦听解析软件观察 TCP 机制

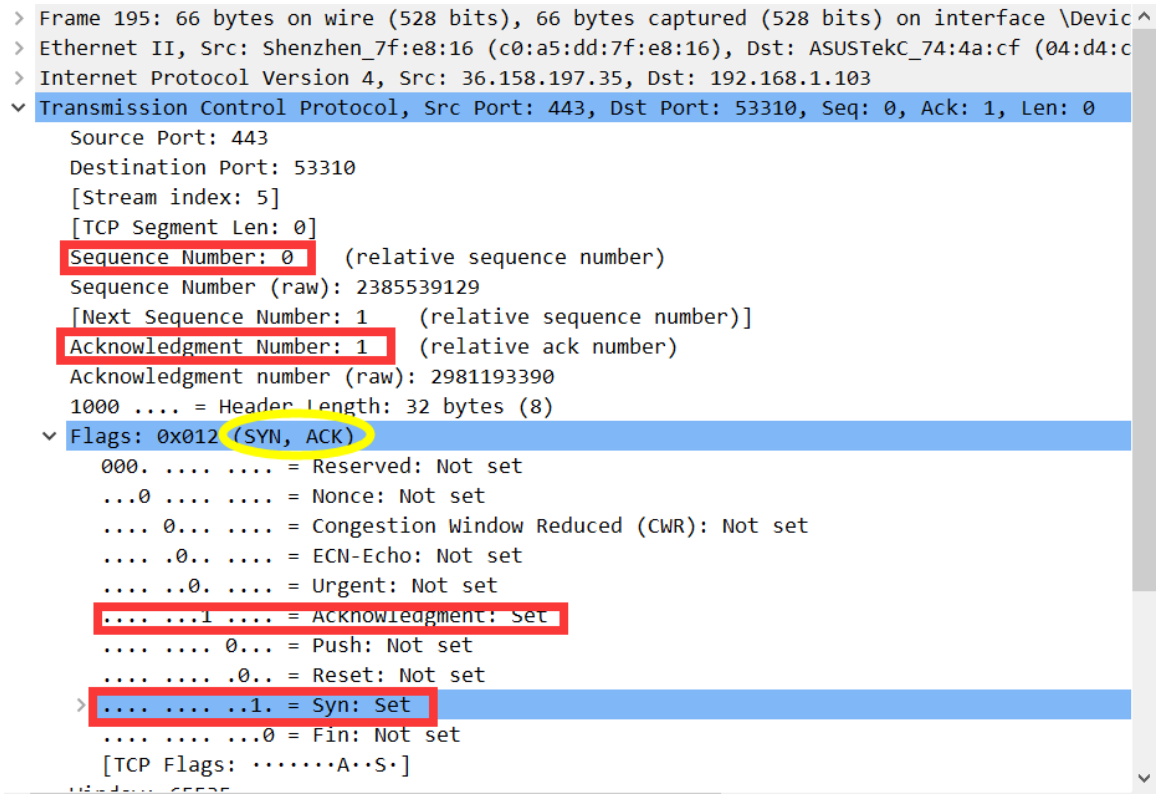
（1）TCP 建立的三次握手连接



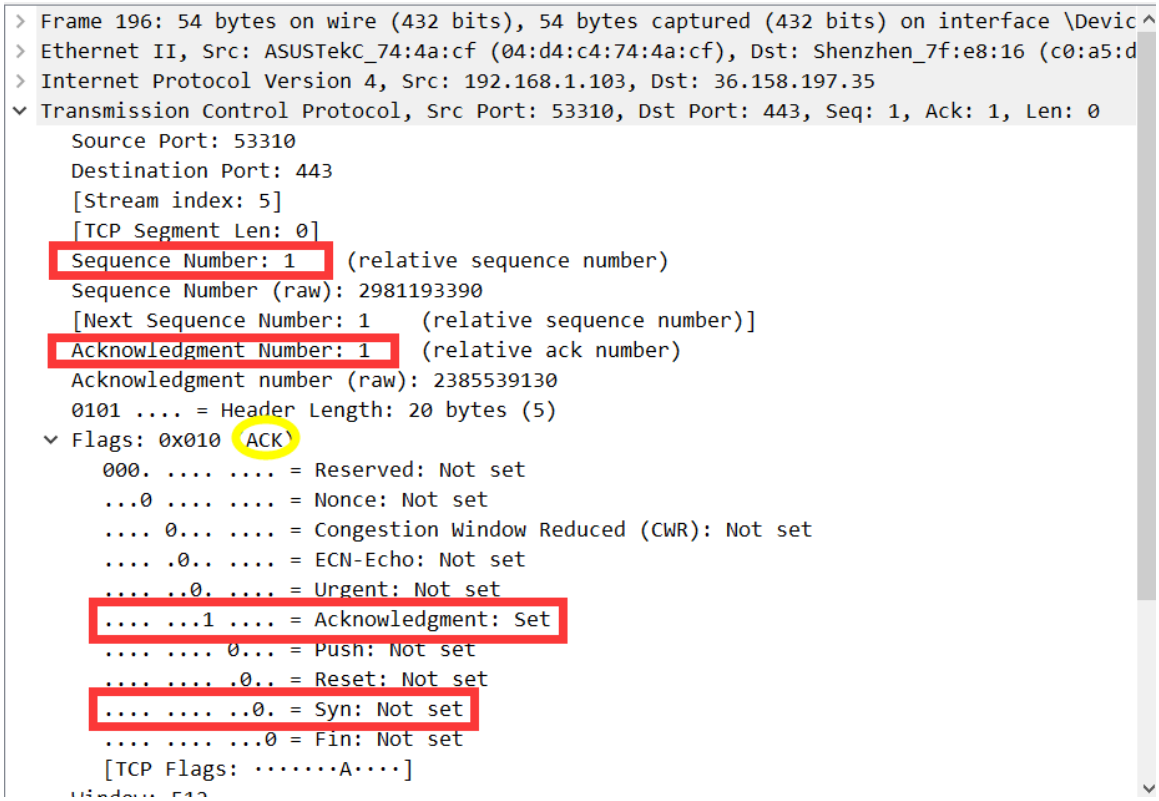
（i）第一个握手数据包：客户端发送一个 TCP，标志位为 SYN，序列号为 0，代表客户端请求建立连接。



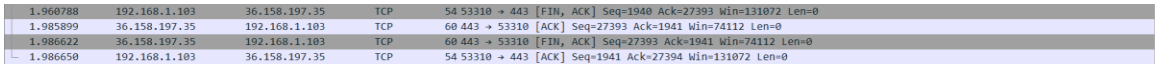
（ii）第二个握手数据包：服务器接收到客户端的 SYN 报文，回复 SYN+ACK 报文。报文标志 SYN，ACK，ACK number=接收到的 Seq+1=1，自己的 Seq=0。



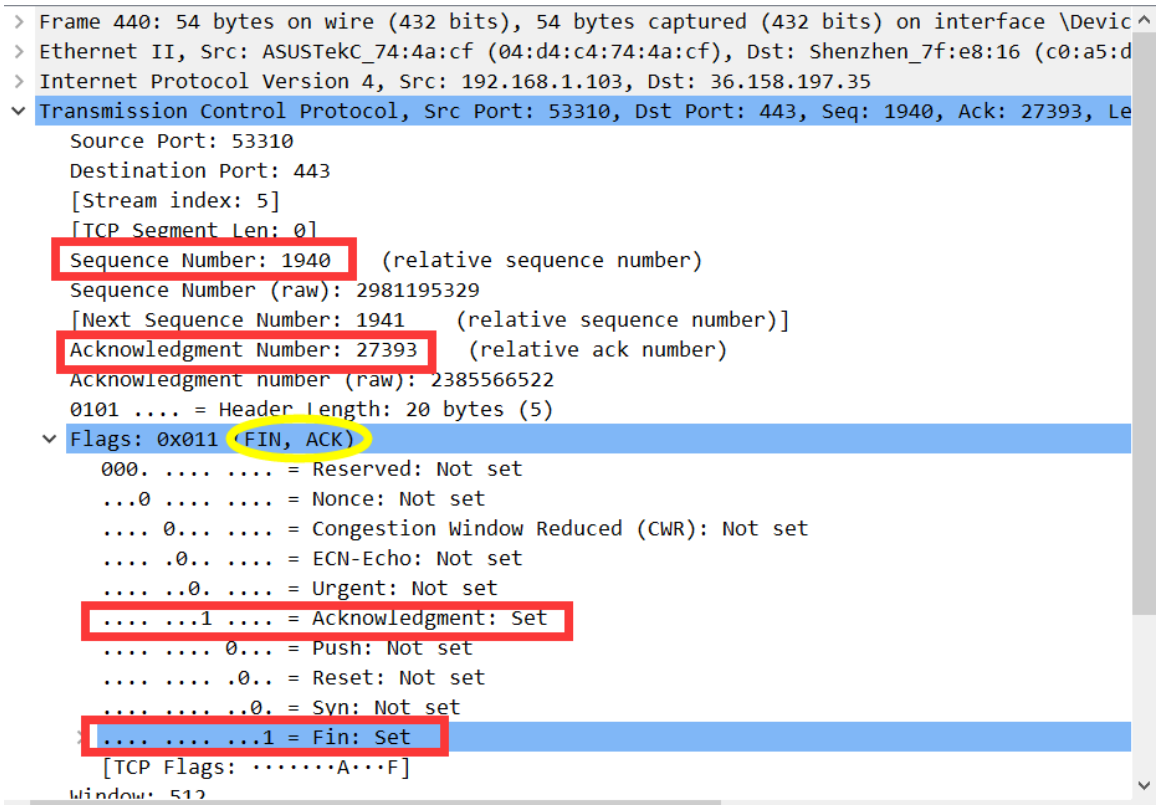
（iii）第三个握手数据包：客户端接收到服务端的 SYN+ACK 报文后，回复 ACK 报文。报文标志 ACK，Seq=1，ACK=接收到的 Seq+1=1。



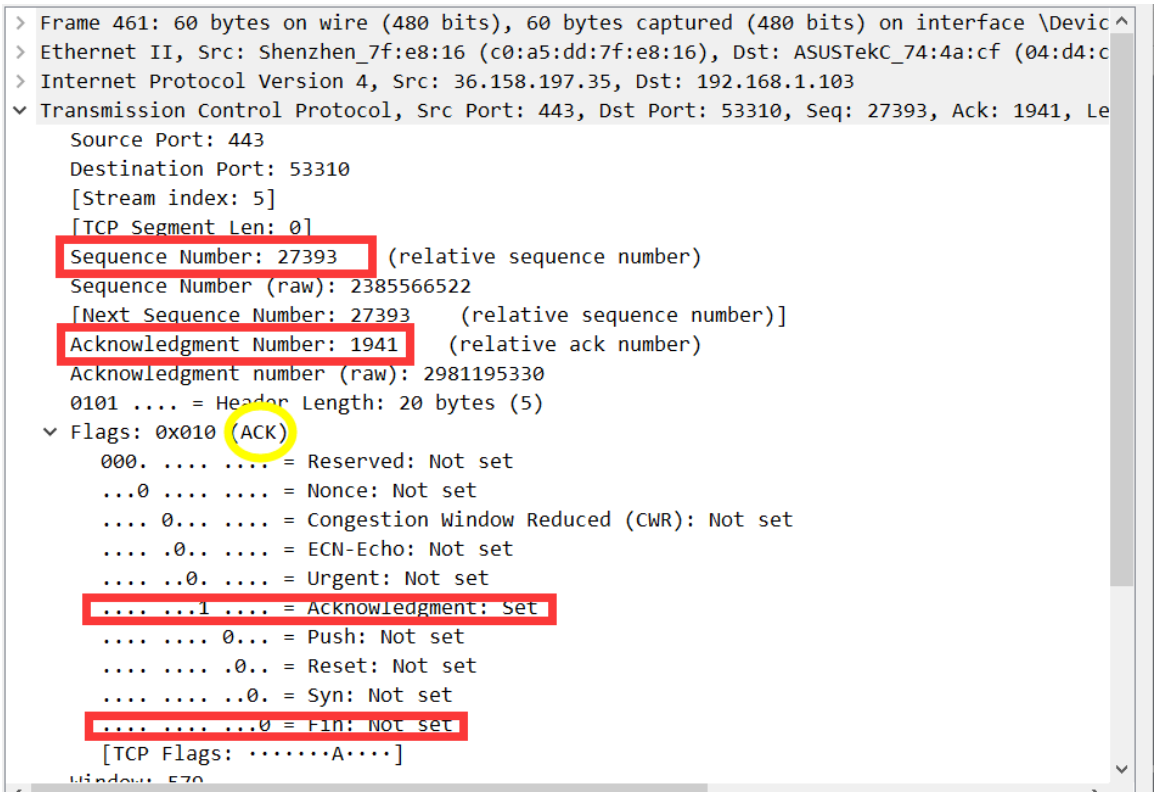
（2）TCP 撤除连接的四次挥手操作



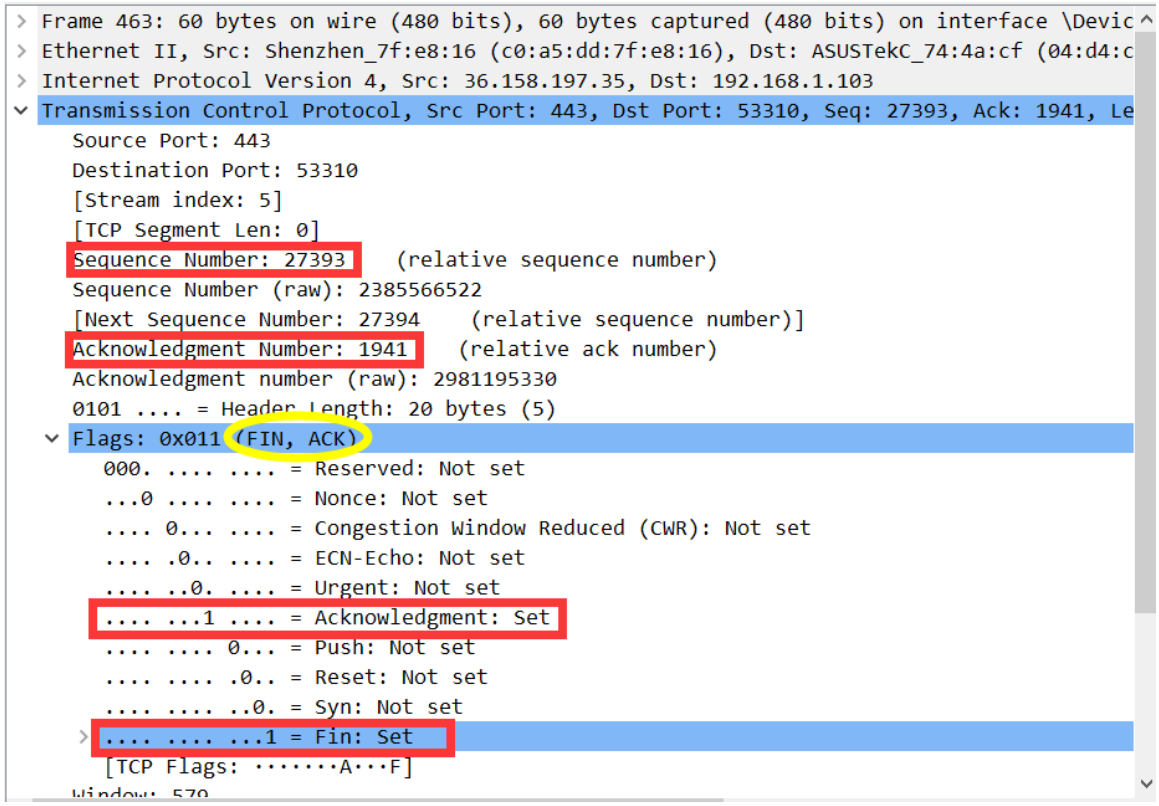
（i）第一次挥手：FIN+ACK。客户端发送一个 FIN，用来关闭客户到服务器的数据传送。



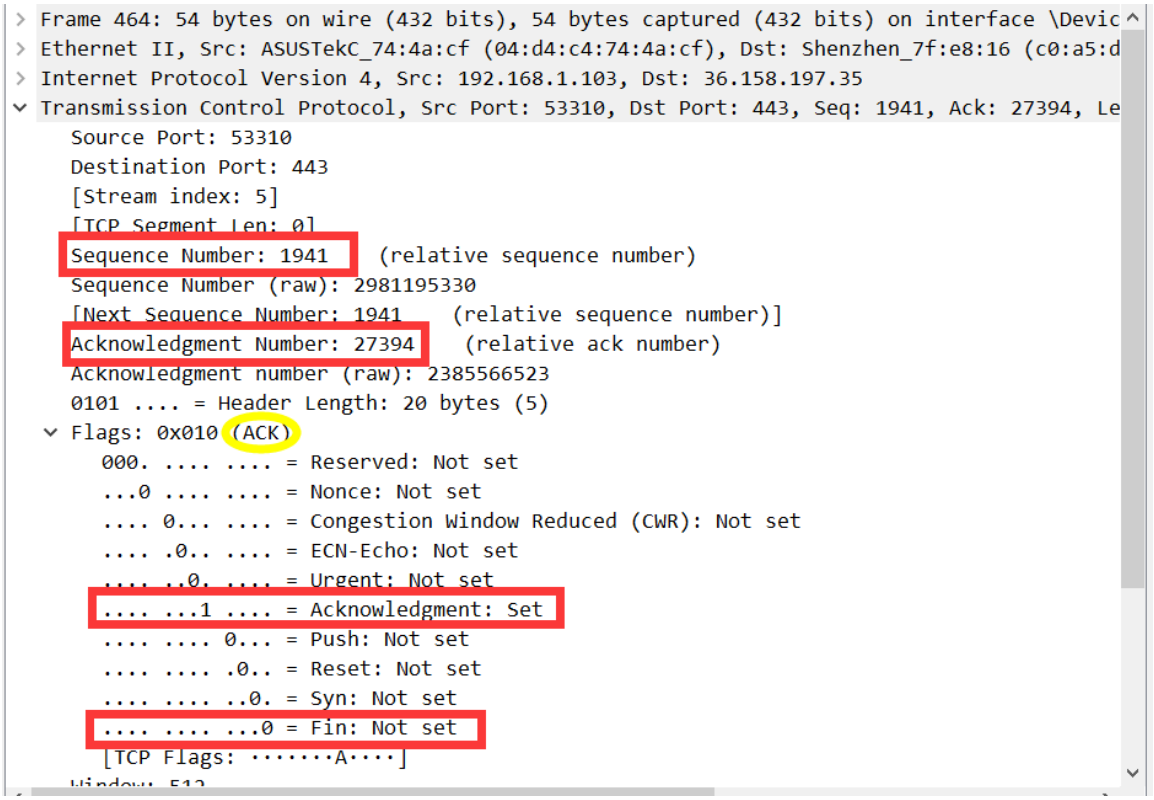
（ii）第二次挥手：ACK。服务器收到这个 FIN，它发回一个 ACK，确认序号为收到的序号加 1。



（iii）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。

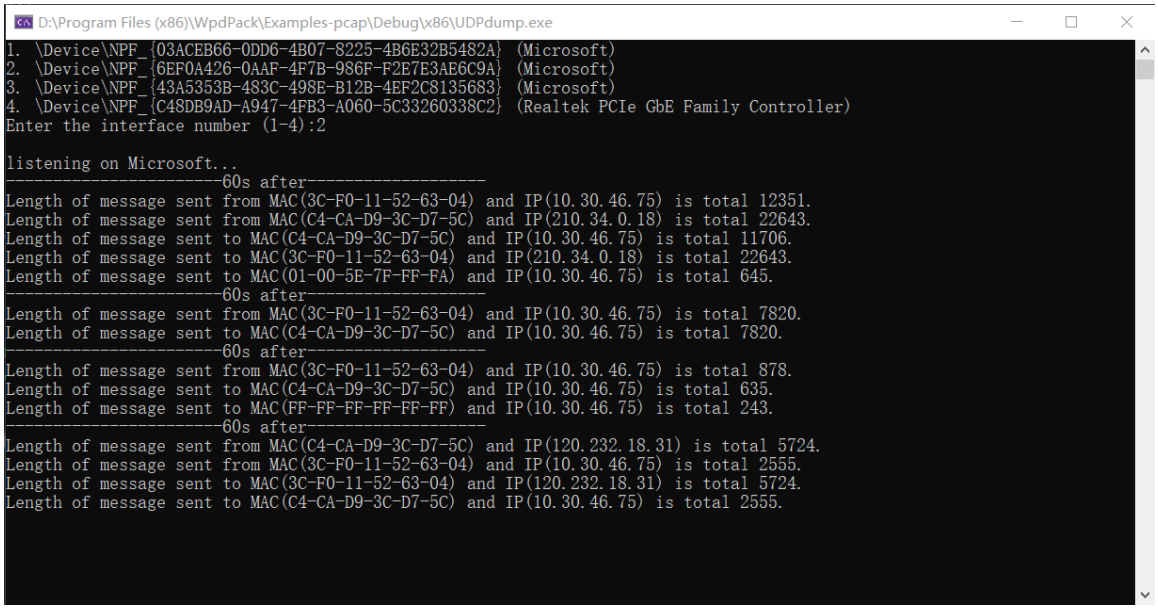


（iv）第四次挥手：ACK。客户端发回 ACK 报文确认，并将确认序号设置为收到序号加 1。



（3）用 Libpcap 或 WinPcap 库侦听网络数据

	A	B	C	D	E	F	G
1	Time	Source MAC	Source IP	Dst MAC	Dst IP	Length	
2	2021/5/14 8:13:14	3C-F0-11-52-63-04	10.30.46.75	C4-CA-D9-3C-D7-5C	210.34.0.18	80	
3	2021/5/14 8:13:14	3C-F0-11-52-63-04	10.30.46.75	C4-CA-D9-3C-D7-5C	210.34.0.18	80	
4	2021/5/14 8:13:14	C4-CA-D9-3C-D7-5C	210.34.0.18	3C-F0-11-52-63-04	10.30.46.75	228	
5	2021/5/14 8:13:14	C4-CA-D9-3C-D7-5C	210.34.0.18	3C-F0-11-52-63-04	10.30.46.75	244	
6	2021/5/14 8:13:14	3C-F0-11-52-63-04	10.30.46.75	C4-CA-D9-3C-D7-5C	210.34.0.18	80	
7	2021/5/14 8:13:14	C4-CA-D9-3C-D7-5C	210.34.0.18	3C-F0-11-52-63-04	10.30.46.75	228	
8	2021/5/14 8:13:16	3C-F0-11-52-63-04	10.30.46.75	C4-CA-D9-3C-D7-5C	210.34.0.18	94	
9	2021/5/14 8:13:16	C4-CA-D9-3C-D7-5C	210.34.0.18	3C-F0-11-52-63-04	10.30.46.75	173	
10	2021/5/14 8:13:16	3C-F0-11-52-63-04	10.30.46.75	C4-CA-D9-3C-D7-5C	210.34.0.18	94	
11	2021/5/14 8:13:16	C4-CA-D9-3C-D7-5C	210.34.0.18	3C-F0-11-52-63-04	10.30.46.75	173	
12	2021/5/14 8:13:17	3C-F0-11-52-63-04	10.30.46.75	C4-CA-D9-3C-D7-5C	210.34.0.18	103	
13	2021/5/14 8:13:17	C4-CA-D9-3C-D7-5C	210.34.0.18	3C-F0-11-52-63-04	10.30.46.75	272	
14	2021/5/14 8:13:17	3C-F0-11-52-63-04	10.30.46.75	C4-CA-D9-3C-D7-5C	210.34.0.18	103	
15	2021/5/14 8:13:17	C4-CA-D9-3C-D7-5C	210.34.0.18	3C-F0-11-52-63-04	10.30.46.75	272	
16	2021/5/14 8:13:18	3C-F0-11-52-63-04	10.30.46.75	C4-CA-D9-3C-D7-5C	210.34.0.18	66	
17	2021/5/14 8:13:18	3C-F0-11-52-63-04	10.30.46.75	C4-CA-D9-3C-D7-5C	210.34.0.18	66	
18	2021/5/14 8:13:18	C4-CA-D9-3C-D7-5C	210.34.0.18	3C-F0-11-52-63-04	10.30.46.75	82	
19	2021/5/14 8:13:18	C4-CA-D9-3C-D7-5C	210.34.0.18	3C-F0-11-52-63-04	10.30.46.75	66	
20	2021/5/14 8:13:18	3C-F0-11-52-63-04	10.30.46.75	C4-CA-D9-3C-D7-5C	210.34.0.18	117	
21	2021/5/14 8:13:18	3C-F0-11-52-63-04	10.30.46.75	C4-CA-D9-3C-D7-5C	210.34.0.18	117	
22	2021/5/14 8:13:18	C4-CA-D9-3C-D7-5C	210.34.0.18	3C-F0-11-52-63-04	10.30.46.75	176	
23	2021/5/14 8:13:19	C4-CA-D9-3C-D7-5C	210.34.0.18	3C-F0-11-52-63-04	10.30.46.75	160	
24	2021/5/14 8:13:19	3C-F0-11-52-63-04	10.30.46.75	C4-CA-D9-3C-D7-5C	210.34.0.18	117	
25	2021/5/14 8:13:19	C4-CA-D9-3C-D7-5C	210.34.0.18	3C-F0-11-52-63-04	10.30.46.75	160	
26	2021/5/14 8:13:20	3C-F0-11-52-63-04	10.30.46.75	C4-CA-D9-3C-D7-5C	210.34.0.18	95	
27	2021/5/14 8:13:20	3C-F0-11-52-63-04	10.30.46.75	C4-CA-D9-3C-D7-5C	210.34.0.18	95	
28	2021/5/14 8:13:20	C4-CA-D9-3C-D7-5C	210.34.0.18	3C-F0-11-52-63-04	10.30.46.75	197	
29	2021/5/14 8:13:20	C4-CA-D9-3C-D7-5C	210.34.0.18	3C-F0-11-52-63-04	10.30.46.75	213	
30	2021/5/14 8:13:20	3C-F0-11-52-63-04	10.30.46.75	C4-CA-D9-3C-D7-5C	210.34.0.18	95	



（4）解析侦听到的网络数据

	A	B	C	D	E	F	G	H	I	J	K
1	2021/5/22 17:46:58	E8-6F-38-3E-88-D1	192.168.1.109	3C-F0-11-52-63-04	192.168.1.102	anonymous	1137004652@qq.com	FAILED			
2	2021/5/22 17:47:01	E8-6F-38-3E-88-D1	192.168.1.109	3C-F0-11-52-63-04	192.168.1.102	user	123456	SUCCEED			

4 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

5 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。