信息安全课程实验二

1. 实验目的

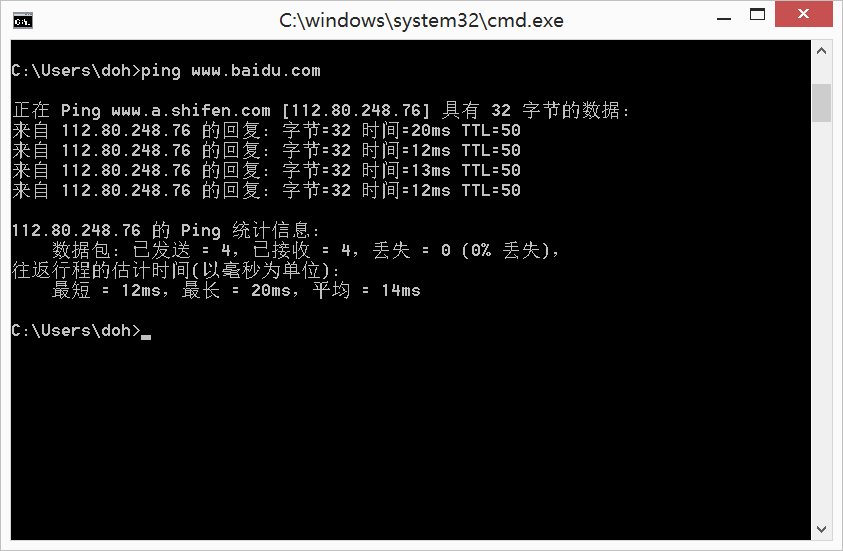
学习虚拟机安装，版本控制软件、抓包软件使用及初步具备协议分析能力；

1. 实验工具

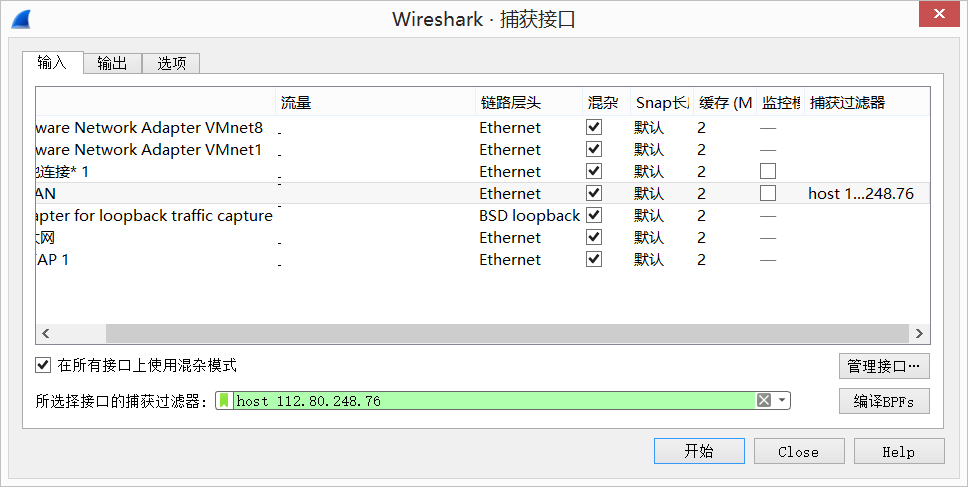
Centos6以上系统，GitHub，Tcpdump，Wireshark

1. 实验内容
2. 对ICMP协议的请求和应答包实施抓包，并采用标注方式进行协议分析，要对每个协议字段进行标注，并对Checksum值进行计算验证（需要写出验证计算过程）？

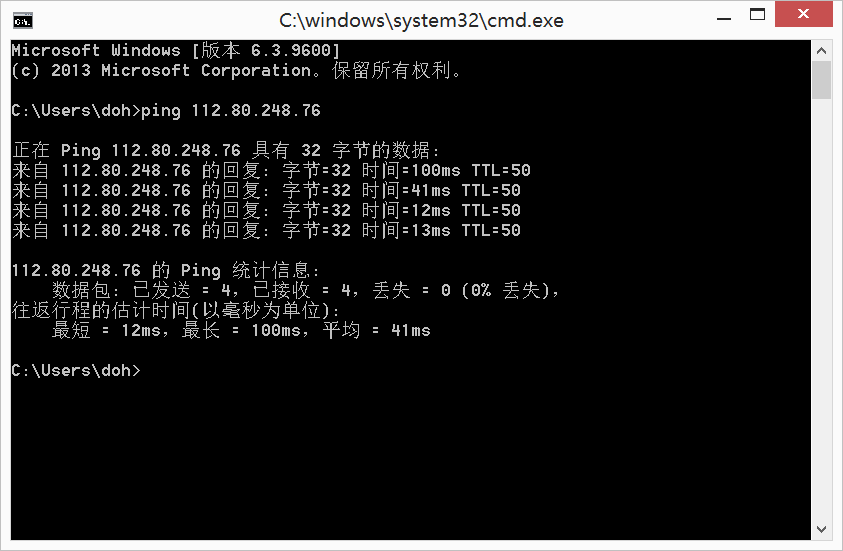
Ping百度网址得出百度ip地址为112.80.248.76：



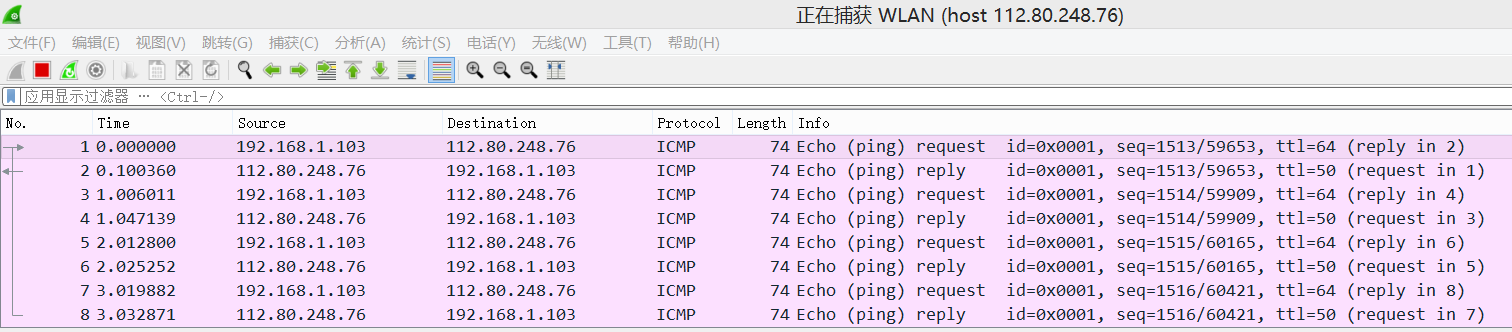
打开Wireshark，在捕获-选项中设置过滤器，过滤出地址为112.80.248.76的包：



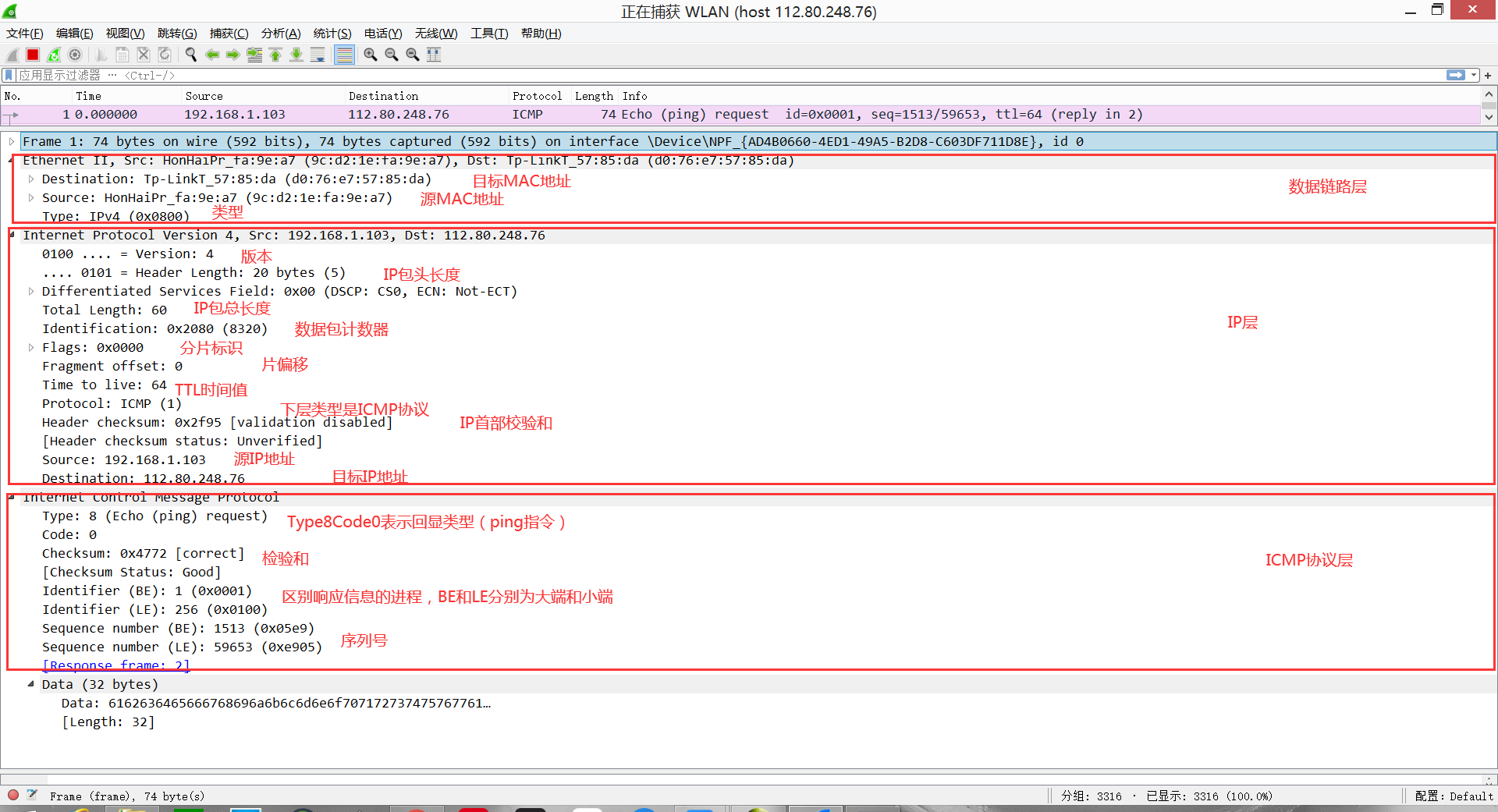
Ping 112.80.248.76:



在Wireshark中可以看到ICMP的包：



协议分析(请求包,应答包在ICMP协议层中多一个Response Time字段，即响应时间):



Checksun值计算:

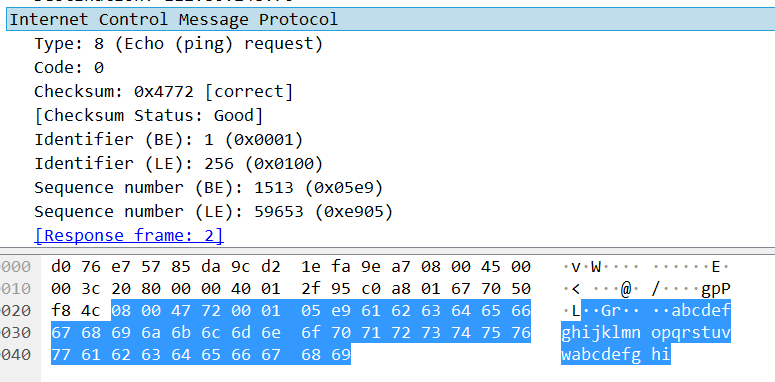


图1

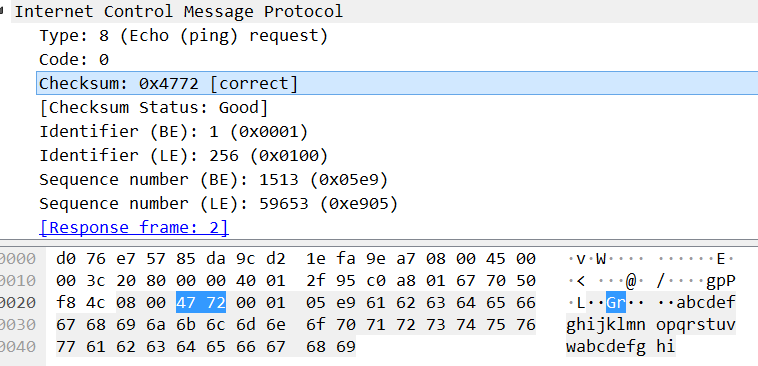
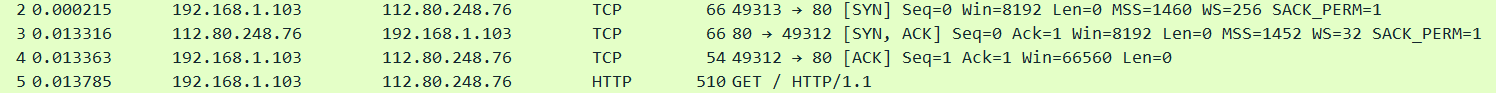


图2

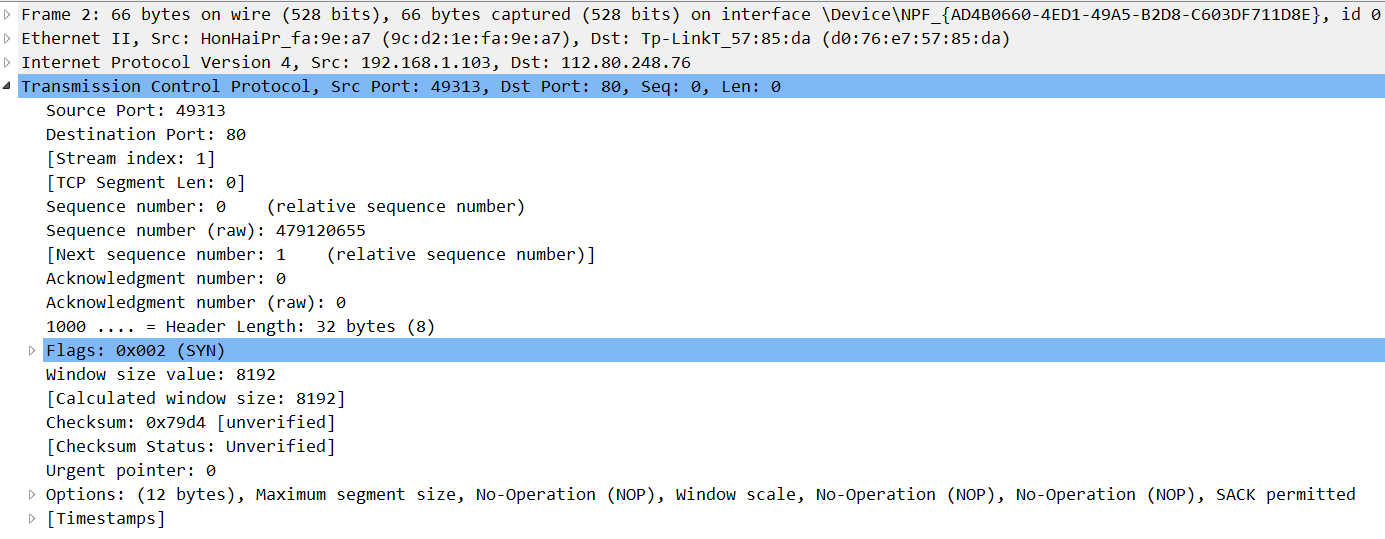
需计算Checksum值的字段为图1中所示字段，其中Checksum字段为图2所示。将图1中Checksum字段置为00 00，后按16bit为一组进行分组，末尾不足则补0，该字段则为0800+0000+0001+05e9……+6869=6B887，再将高16位与低16位相加，即6+B887=B88D，取反，得4772，验证正确。

1. 进行一次TCP协议的三次握手和四次挥手抓包实验，分析其中SYN，ACK，FIN等标志及 Sequence number，Acknowledgement number数值在握手连接中的变化情况。

按实验A设置过滤器，打开百度官网，可以看到以下包：

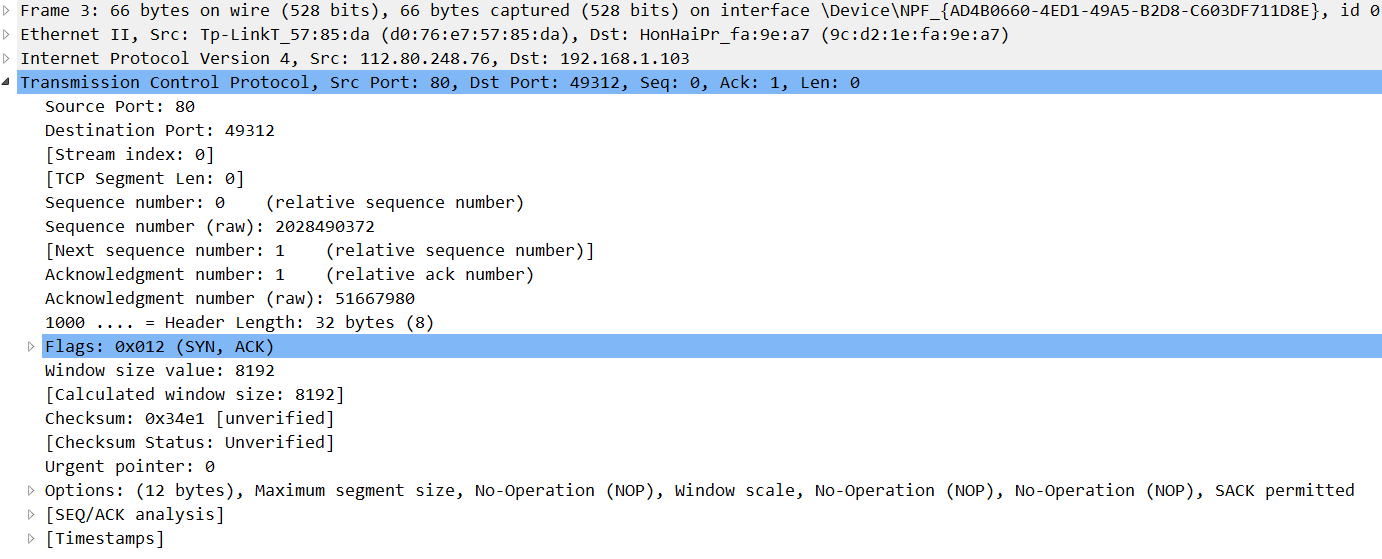


第一次握手：



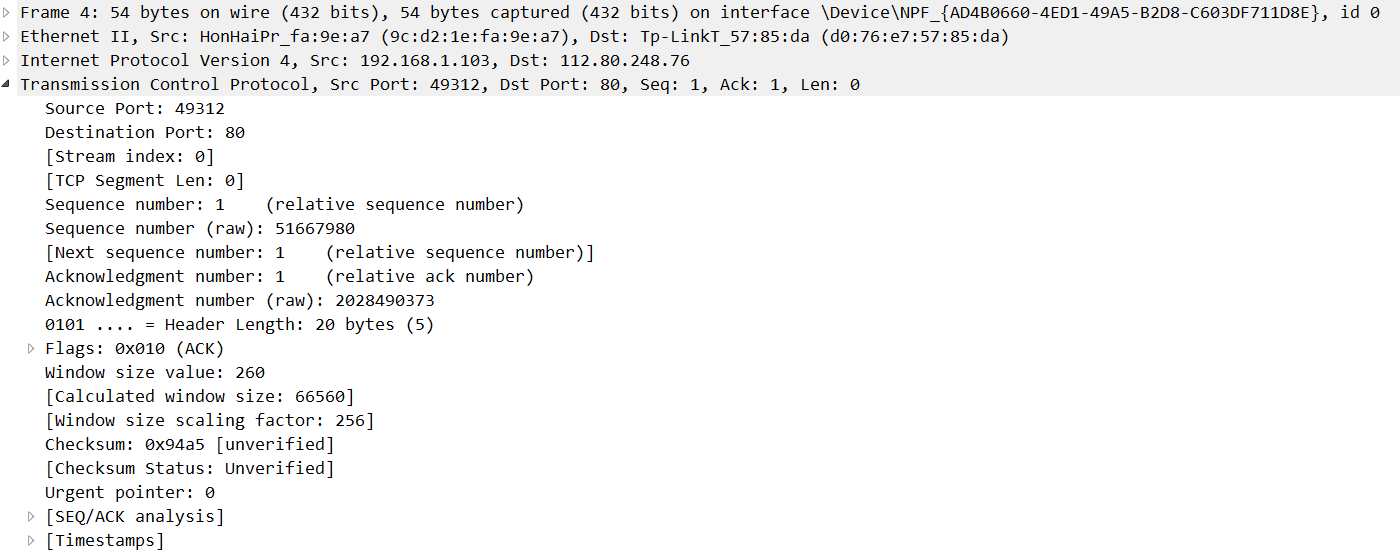
标识为SYN,seq=0，Ack=0;

第二次握手：



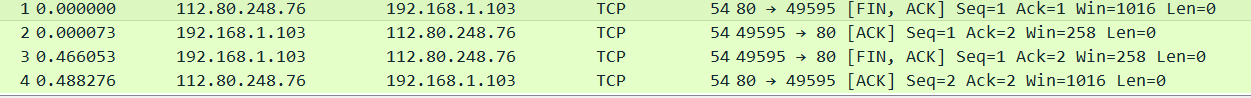
标志为SYN,ACK，seq=0,Ack=第一次握手的seq+1=1；

第三次握手：

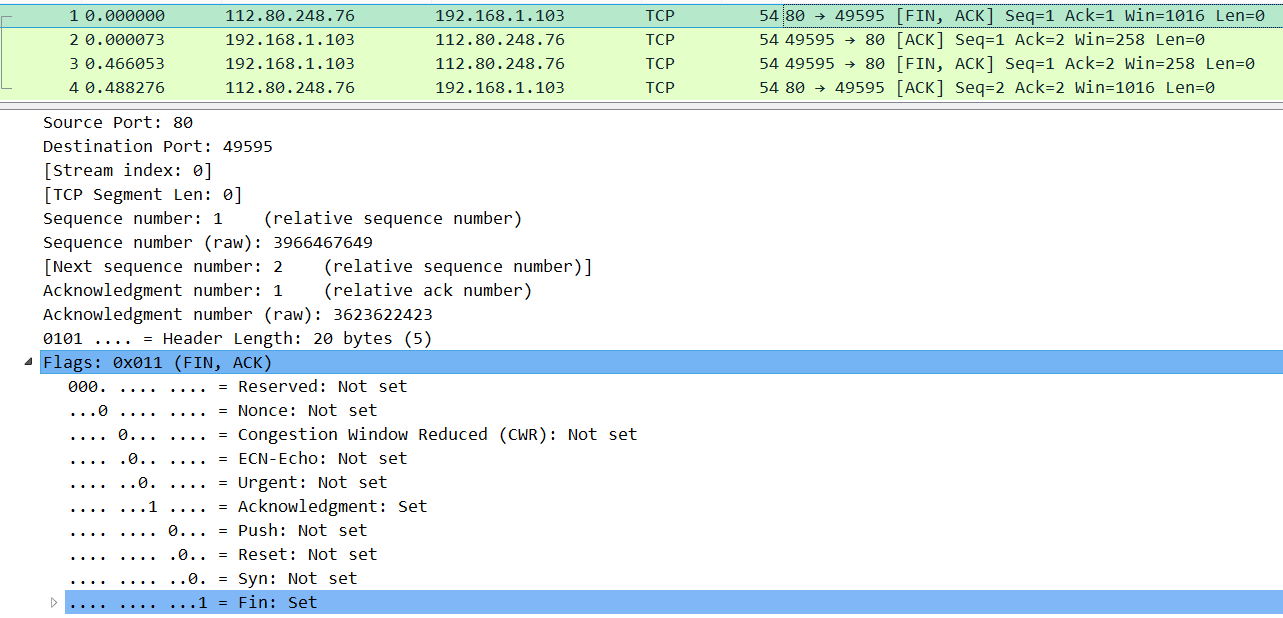


标志为ACK，seq=第一次握手的seq+1=1，Ack=第二次握手的seq+1=1；

四次挥手：

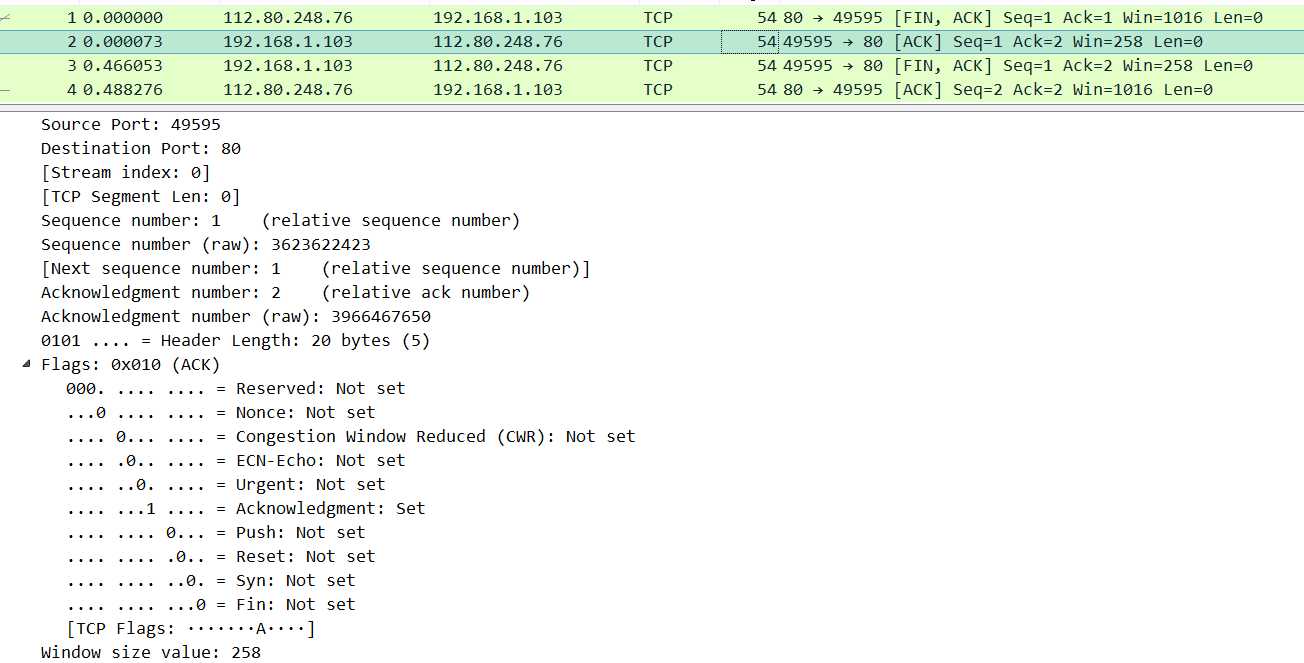


第一次挥手：



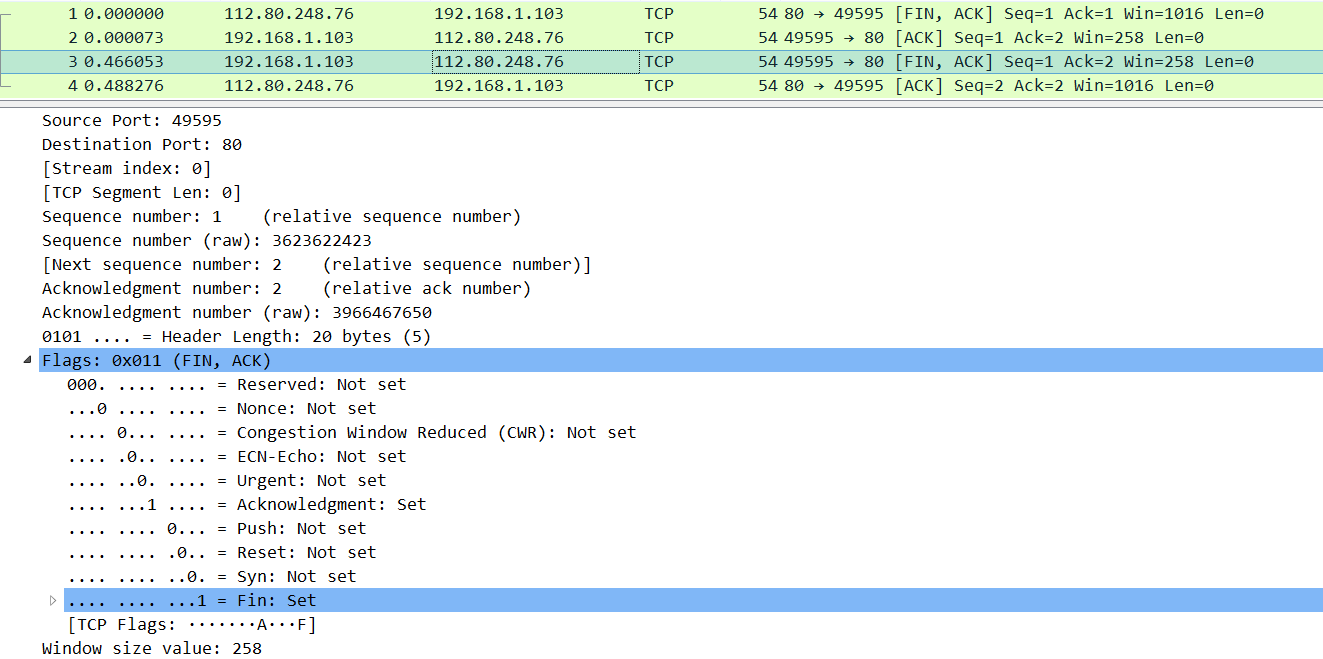
标志为FIN,ACK，seq=1，Ack=1；

第二次挥手：



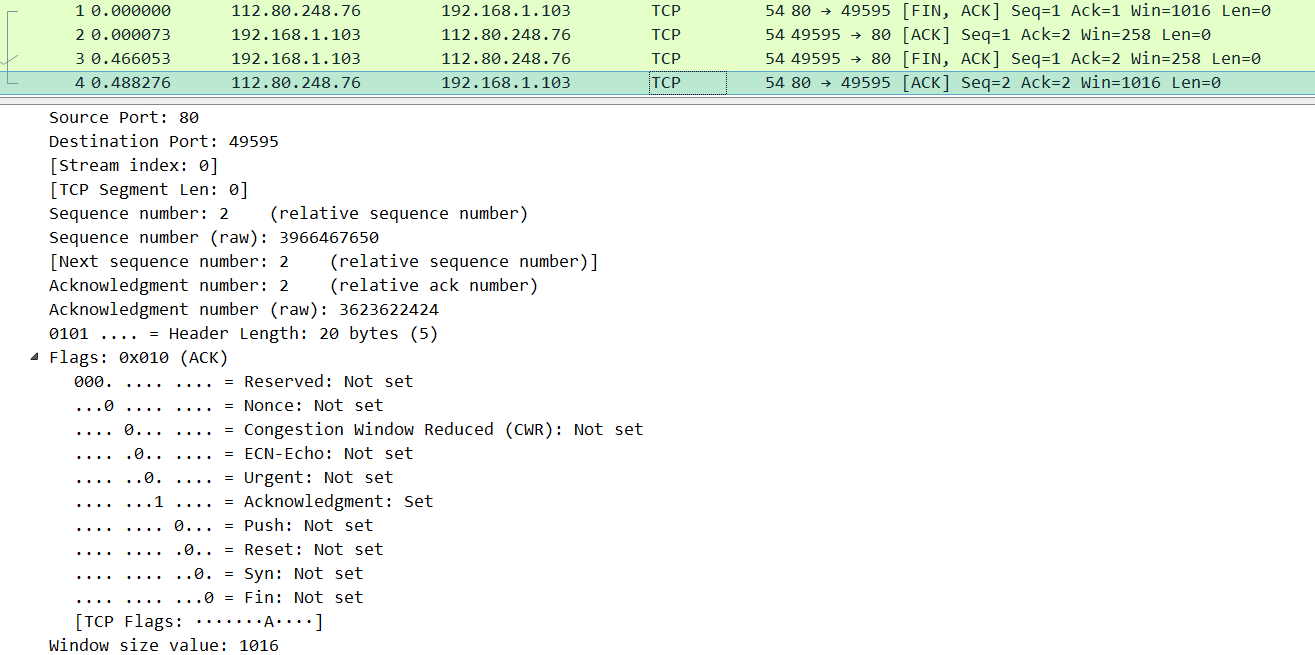
标志为ACK，seq=1，Ack=第一次挥手seq+1=2；

第三次挥手：



标志为FIN,ACK，seq=1，Ack=第二次握手的Ack=2；

第四次挥手：



标志为ACK，seq=第三次挥手的Ack=2，Ack=第三次挥手的seq+1=2；

1. 通过抓包以截图和文字形式分析以下问题：TCP 第一次握手的 SYN 丢包了，会发生了什么？TCP 第二次握手的 SYN、ACK 丢包了，会发生什么？TCP 第三次握手的 ACK 包丢了，会发生什么？
2. SYN包以递增的时间间隔重传；
3. 客户端以递增时间间隔重传SNY包，服务器端以递增时间间隔重传SYN+ACK包；
4. 服务器端以递增的时间间隔重传SYN+ACK包，客户端开始发送数据。