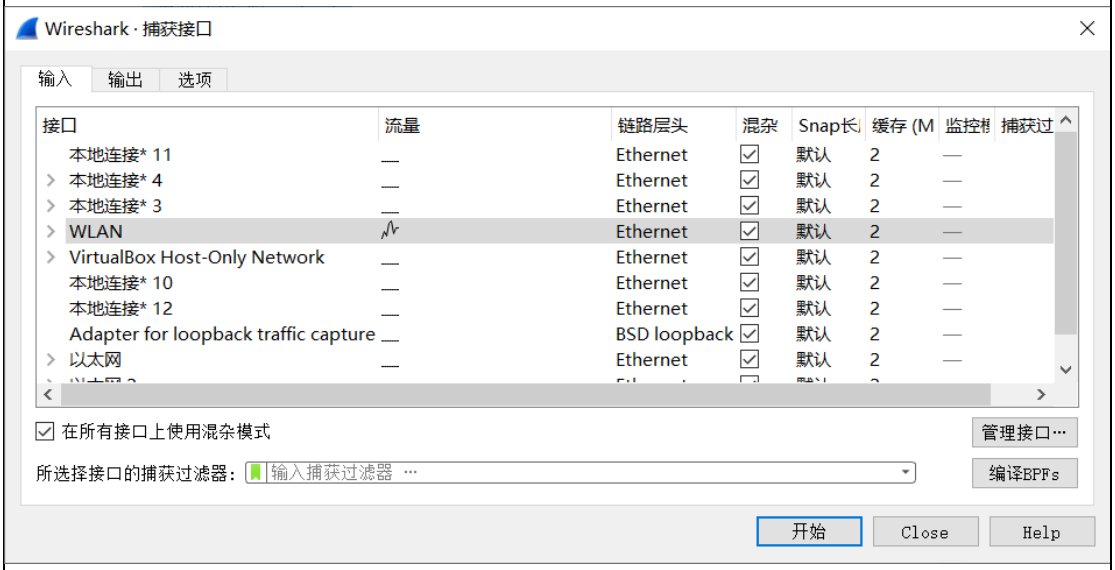
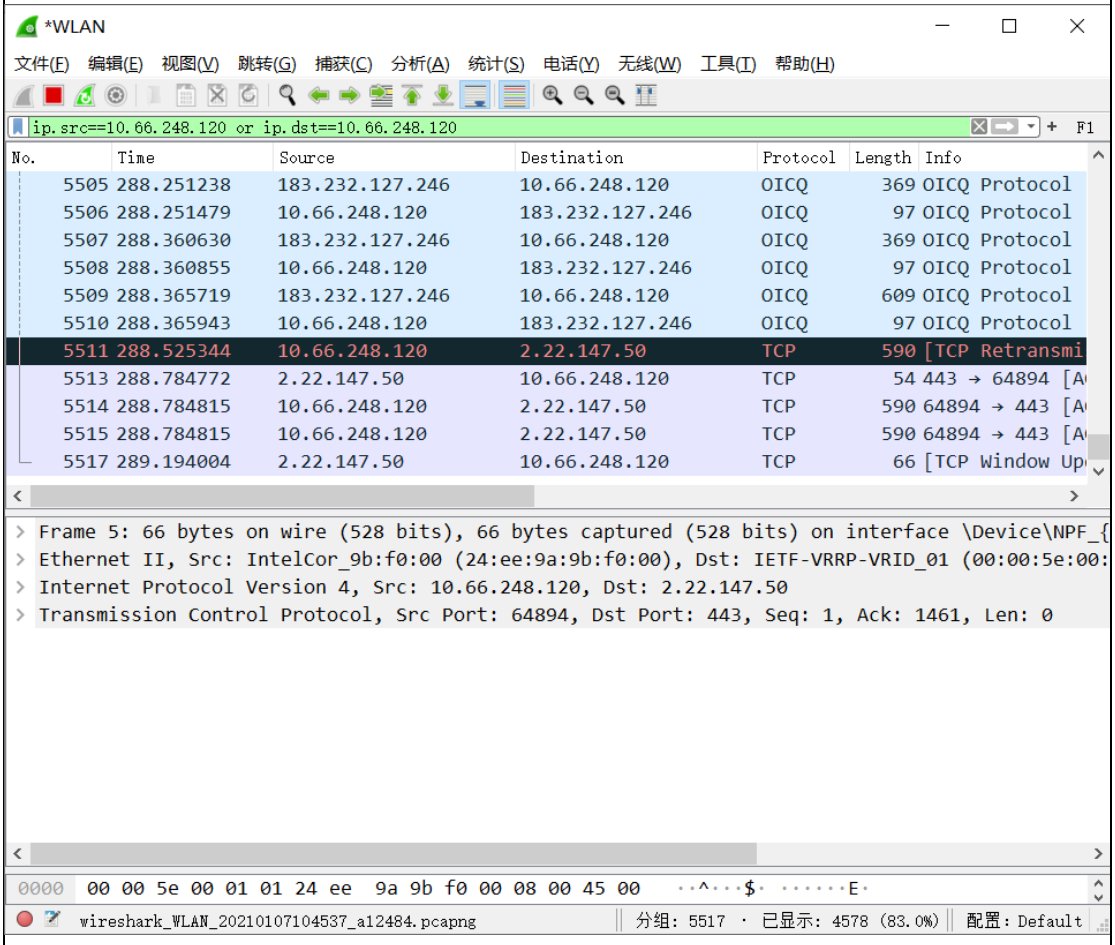
《计算机网络》实验报告

实验项目序号及名称	基本报文分析
实验成员及分工：张楷 组长： 张楷 组员： 张楷	
报告执笔人（签名）：张楷	实验完成时间：
实验目的： 1.理解 IP 层的作用以及 IP 地址的分类方法； 2.理解子网的划分和子网掩码的作用； 3.掌握 IP 数据包的组成和网络层基本功能；	
实验设备和环境：校园网；装有 Wireshark 的 PC	
实验过程及步骤：（给出相应的实验环境拓扑图和实验说明，可另附页） 一、 开始抓包；	

1. 使用 Wireshark 开始捕获数据包；



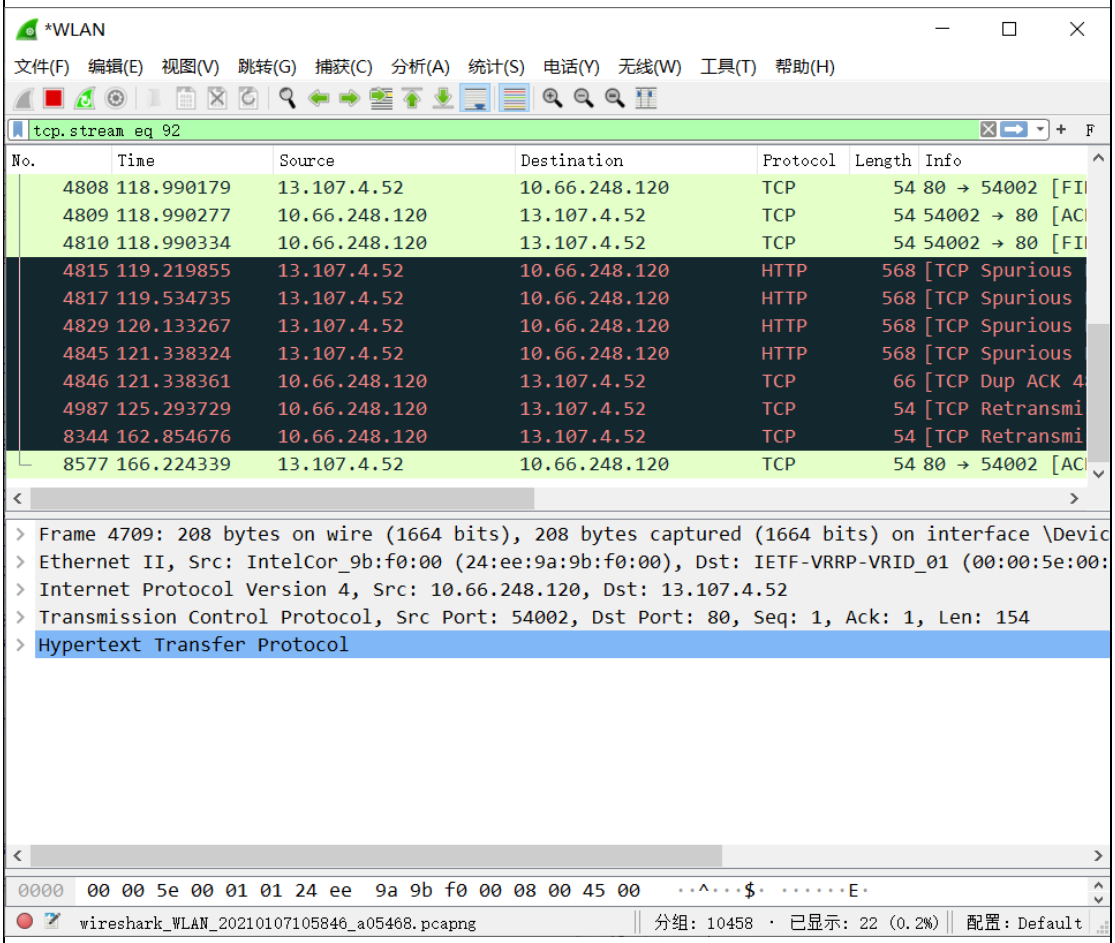
2. 过滤。通过 ip.src== 10.66.248.120 or ip.dst== 10.66.248.120 指令，查看源地址或目标地址为 10.66.248.120 的数据包；



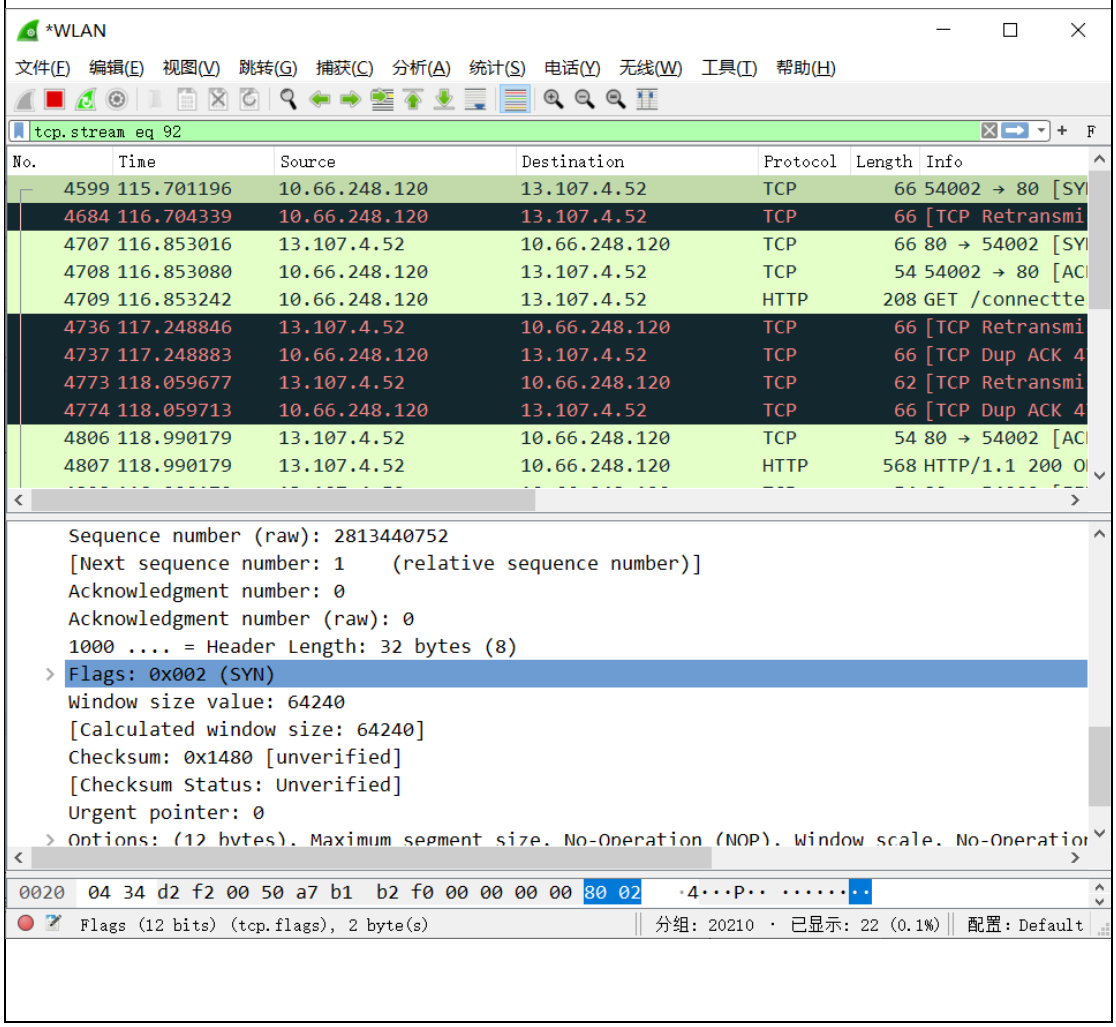
二、 TCP 三次握手；

1. 访问一个网址，并用 http 指令过滤；

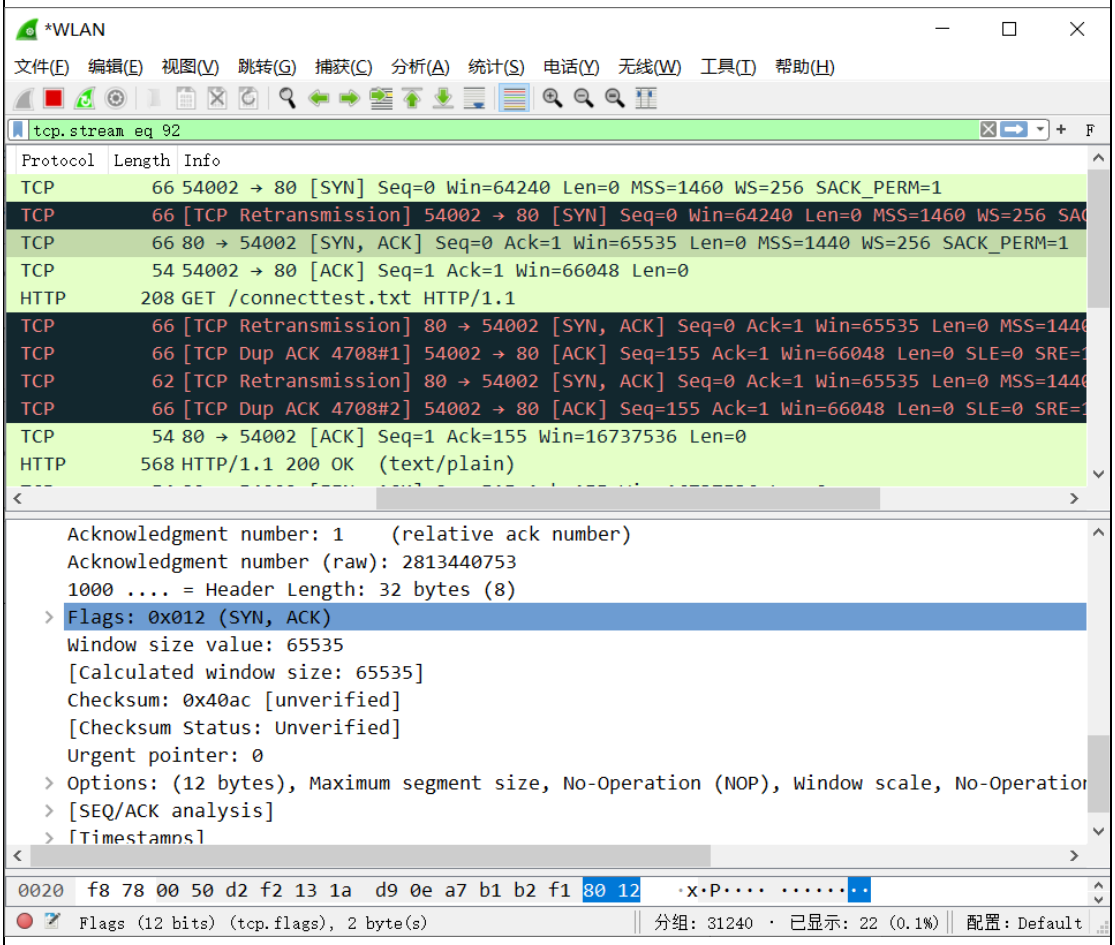
2. 寻找到 Info 为 GET/connecttext.txt HTTP/1.1,并追随 TCP 流；



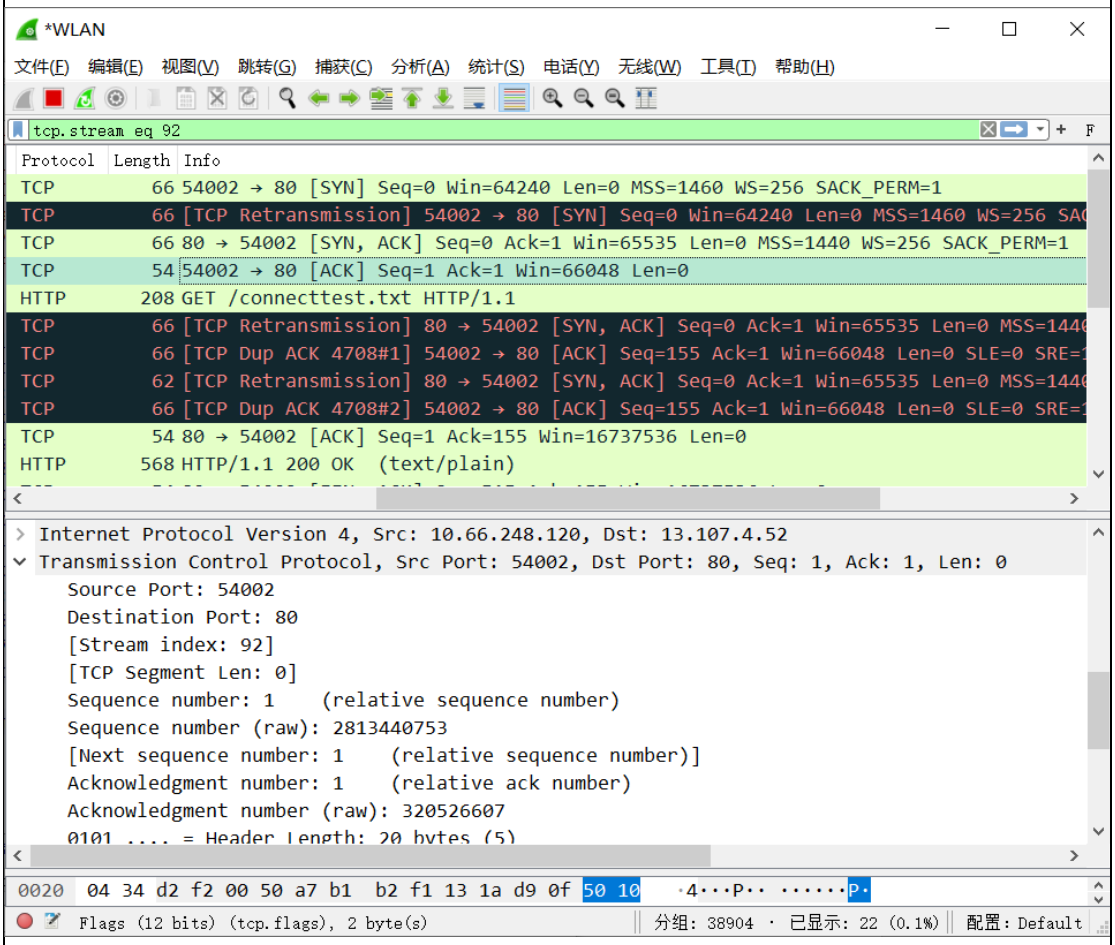
3. 第一次握手。标志位为 SYN，序列号为 0，代表客户端请求建立链接



4. 第二次握手。标志位为 SYN,ACK,将 Acknowledgment number 置为 1，即用户发送的 ISN+1（0+1）；



5. 第三次握手。可见客户端再次发送确认包 号字段+1,放在确定字段中发送给对方 就这样通过了 TCP 三次握手 客户端再次发送确认包(ACK) SYN 标志位为 0,ACK 标志位为 1.并且把服务器发来 放在确定字段中发送给对方.并且在数据段放写 ISN 的+1。



三、 IP 报文解析

捕获到的 IP 报文如下:

Internet Protocol Version 4, Src: 10.66.248.120, Dst: 13.107.4.52

0100 .... = Version: 4 //版本号为 4

.... 0101 = Header Length: 20 bytes (5) //首部长度为 20B

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0000 00.. = Differentiated Services Codepoint: Default (0)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 52 //总长度为 52B

Identification: 0xbf6a (49002) //标识符

Flags: 0x4000, Don't fragment //标志

0... .... = Reserved bit: Not set

.1.. .... = Don't fragment: Set
..0. .... = More fragments: Not set
Fragment offset: 0 //片偏移
Time to live: 64 //存活时间
Protocol: TCP (6) //协议
Header checksum: 0x0000 [validation disabled] 首部校验和
[Header checksum status: Unverified]
Source: 10.66.248.120 源地址
Destination: 13.107.4.52 目标地址

实验总结：（遇到问题、解决办法、收获和体会，可另附页）

大概明白了 IP 协议的报头