学生实验实习报告册

学年学期：2018-2019 学年 □春☑秋学期

课程名称：计算机网络

学生学院：软件工程学院

专业班级：13001603班

学生学号：2016214052

学生姓名：姜文泽

联系电话：17783101834

重庆邮电大学教务处制

实验三：TCP 协议分析

一、实验目的

1. 熟悉 TCP 协议的基本原理；

2. 学会使用 Wireshark 分析 TCP 协议。

二、实验内容

通过 Wireshark 抓包工具分析 TCP/IP 的三次握手。

三、实验环境

操作系统：Windows 10 专业版 1803

工具软件：Wireshark 2.6.4

浏览器软件：Google Chrome

网络环境：

无线局域网适配器 WLAN:

连接特定的 DNS 后缀 . . . . . : lan

本地链接 IPv6 地址. . . . . : fe80::3079:5439:d245:e240%9

IPv4 地址 . . . . . : 192.168.199.175

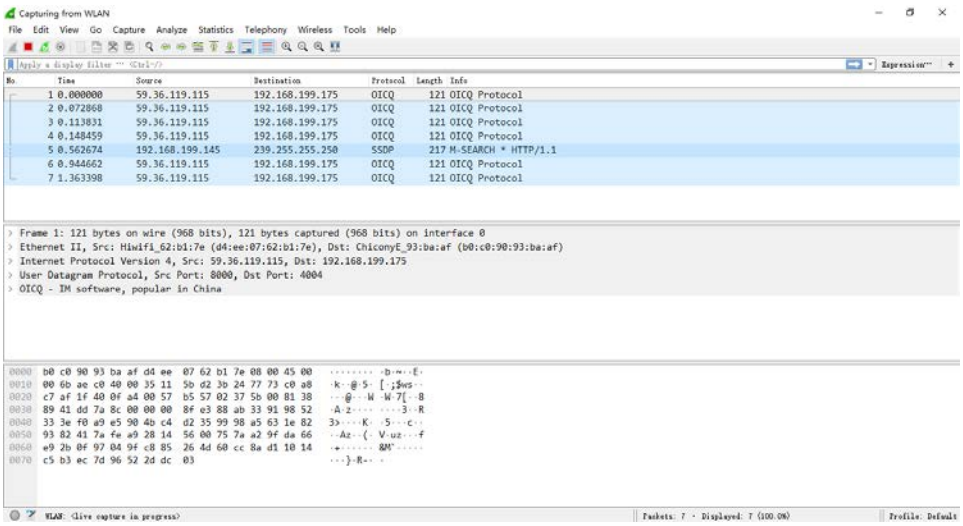
子网掩码 . . . . . : 255.255.255.0

默认网关. . . . . : 192.168.199.1

四、实验步骤

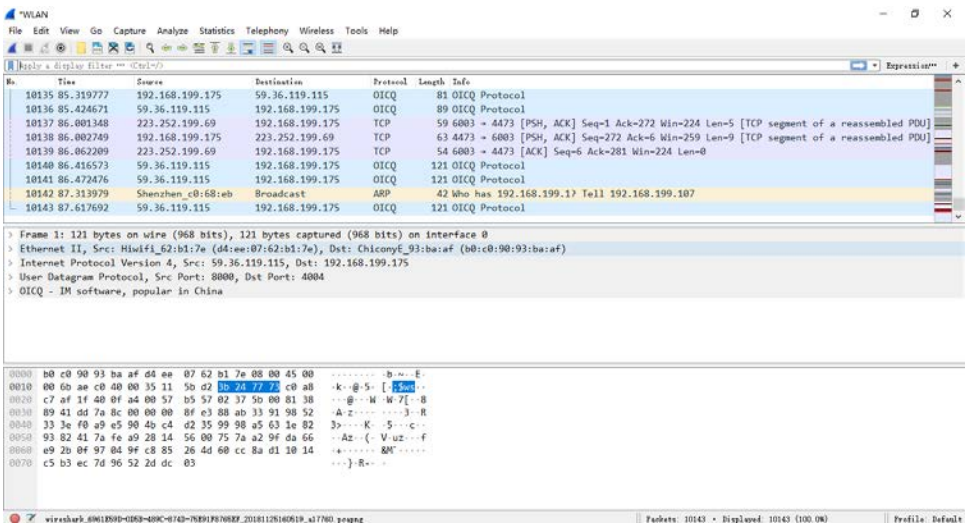
1. 捕获大量的由本地主机到远程服务器的 TCP 分组

（1） 启动 Wireshark，开始进行；



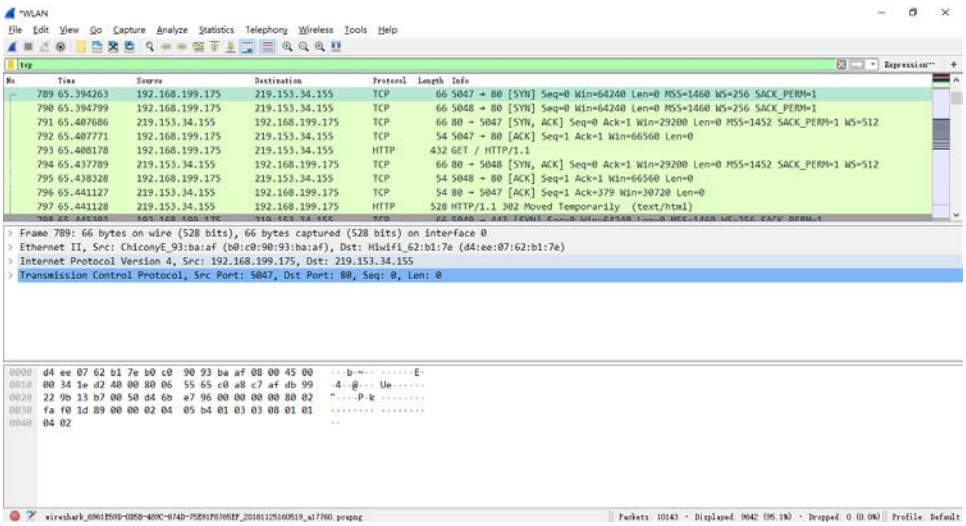
（2） 启动 Chrome 浏览器，打开 https://www.sina.com.cn/网页；

（3） 停止分组捕获。



2. 浏览追踪信息

（1） 在显示筛选规则编辑框中输入“tcp”，可以看到在本地主机和服务器之间传输的一系列 tcp 和 HTTP 消息，可以看到包含 SYN Segment 的三次握手。也可以看到有主机向服务器发送的一个 HTTP GET 消息和一系列的“http continuation”报文。



（2） 根据操作回答“实验报告内容”中的 1-2 题。

3. TCP 基础

根据操作回答“实验报告内容”中的 3-5 题；

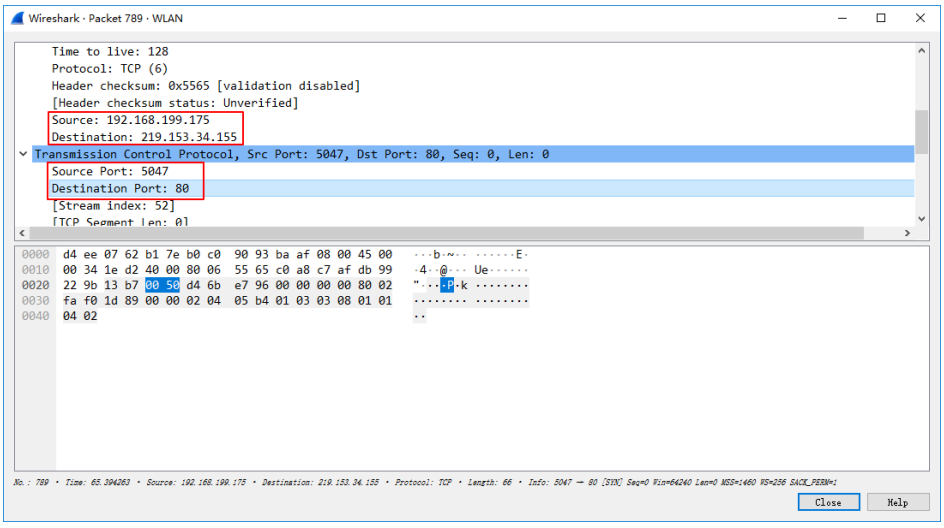
4. TCP 拥塞控制

（1） 在 Wireshark 已捕获分组列表子窗口中选择一个 TCP 报文段；

（2） 选择菜单：Statistics->TCP Stream Graph->Time Sequence Graph (Stevens)。

5. 实验结果

（1） 向 www.sina.com.cn 服务器传送文件的客户端主机的 IP 地址和 TCP 端口号分别是多少？请截图并回答。

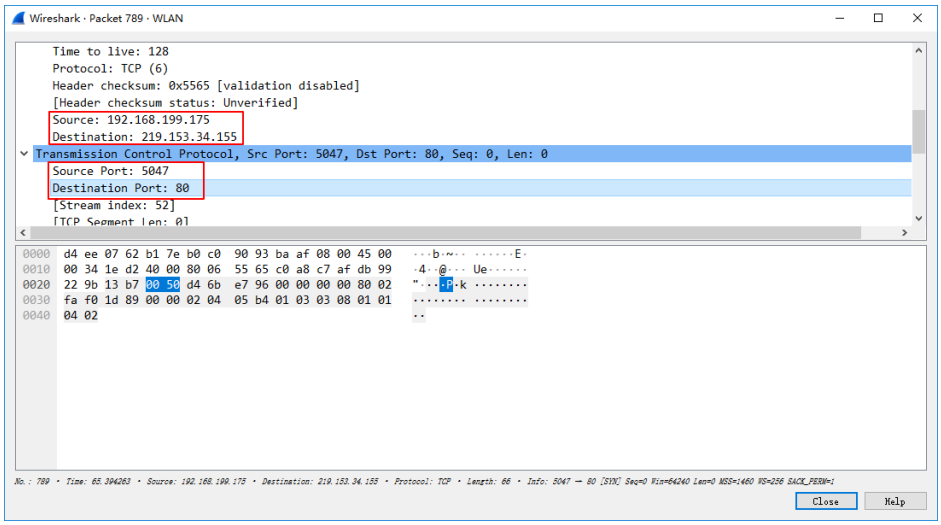


主机：192.168.199.175

端口号：5047

（2） www.sina.com.cn 服务器的 IP 地址是多少？对这一连接，它用来发送和接收

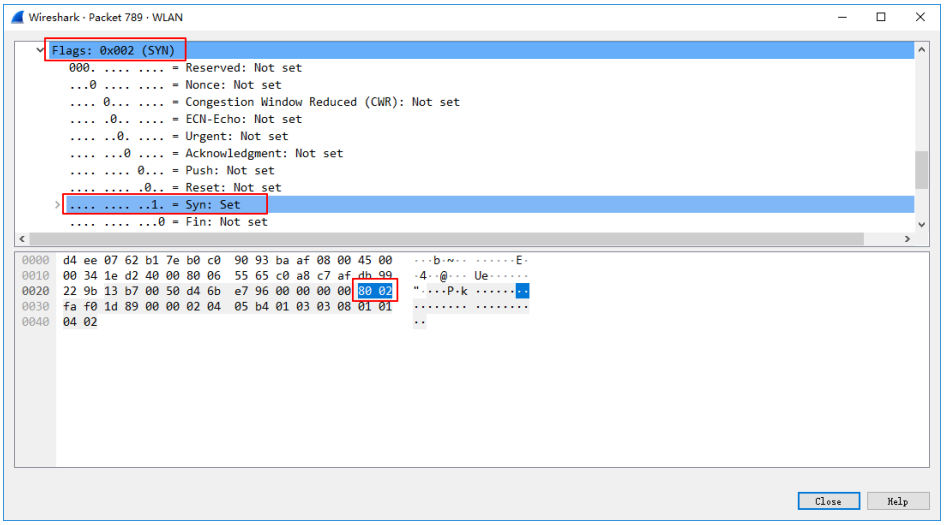
TCP 报文的端口号是多少？请截图并回答。



IP 地址：219.153.34.155

端口号：80

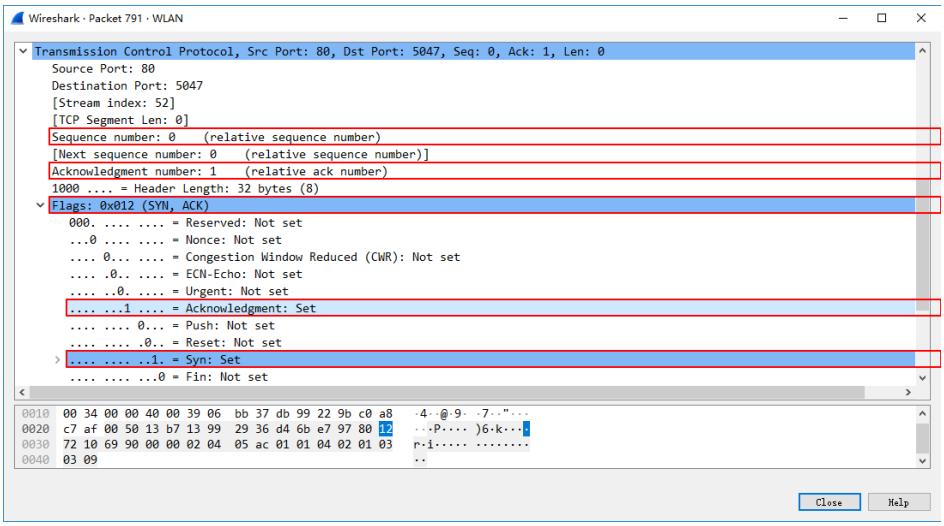
（3） 客户服务器之间用于初始化 TCP 连接的 TCP SYN 报文段的序号（sequence number)是多少？在该报文段中,是用什么来标示该报文段是SYN报文段的？



该报文段序号为 0；

在该报文段中，含有一个 Flags 标志，该标志总共可以设置 10 个标志，当该报文段为 SYN 时，该标志的第 2 位（设该二进制的最小位为第 1 位）置 1，对应 16 进制的值为 0x002；

（4） 服务器向客户端发送的 SYNACK 报文段序号是多少？该报文段中，Acknowledgement 字段的值是多少？www.sina.com.cn 服务器是如何决定此值的？在该报文段中，是用什么来标识该报文段是 SYN ACK 报文段的？



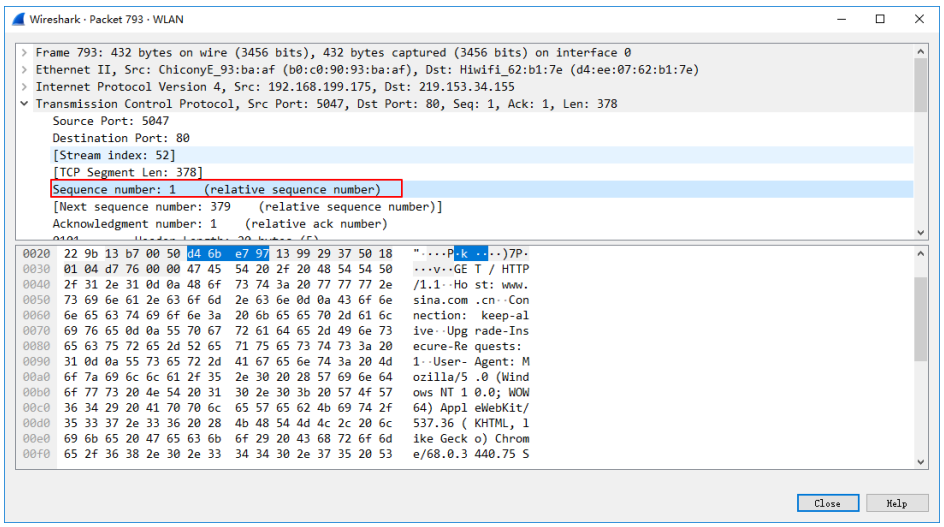
该报文段序号为 0；

Acknowledgement 字段的值为 1；

ACK 的值由服务器接收到的 SYN 的值+1 得到；

在该报文段中，含有一个 Flags 标志，该标志总共可以设置 10 个标志，当该报文段为 SYN ACK 报文段时，该标志的第 2 位和第 5 位（设该二进制的最小位为第 1 位）置 1，对应 16 进制的值为 0x012；

（5） 包含 HTTP GET 消息的 TCP 报文段的序号是多少？



序号为 1。

五、实验结论

收获 1. Wireshark 捕获的数据过多时可以使用过滤规则 ip.src == IP_ADDRESS or ip.dst = IP_ADDRESS 来筛选数据。如本题，可以先使用 ping 命令获取 www.sina.com.cn 的 IP 地址，然后使用过滤规则过滤即可，即使用语句 ip.src ==

219.153.34.155 or ip.dst = 219.153.34.155

收获 2. TCP 三次握手图解：