TCP 协议分析

一、实验目的

掌握 TCP 协议，包括 TCP 报文段格式、序号和确认号、连接建立、流量控制及拥塞控制，使用 WireShark 对 TCP 协议的性能进行分析（吞吐量和往返时间 RTT）

二、实验环境

操作系统 Windows，WireShark、浏览器

注意事项：

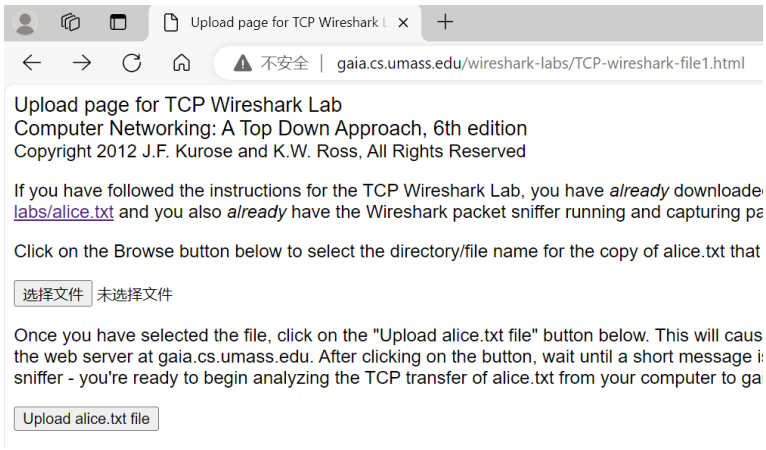
1）不能运行 VPN

2） 浏览器没有默认使用 HTTP3.0/QUIC 协议进行通信

三、 实验步骤

1 捕获由本地主机到远程服务器的 TCP 分组；

- 打开浏览器，输入“http://gaia.cs.umass.edu/wireshark-labs/alice.txt”，得到 *alice.txt*，将该文件保存到本地。
- 打开 http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html ，如下图所示。



选择 alice.txt 文件，不要点击“Upload”按钮

- 启动 WireShark，开始抓包。
- 在浏览器中，点击“Upload”按钮，将文件上传到 gaia.cs.umass.edu 服务器，等待上传成功

- 停止抓包。

2 WiresShark 查看抓包信息

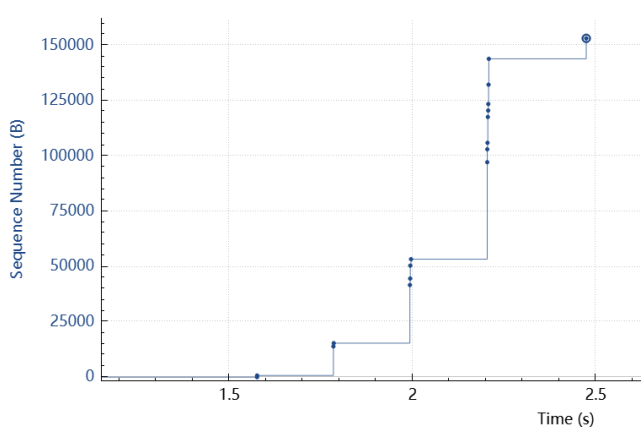
- 在显示筛选规则框中输入“tcp”，可以看到在本地主机和服务器之间传输的 TCP 和 HTTP 消息，包含三次握手、HTTP POST、HTTP Continuation 报文（取决于 WireShark 的版本）以及 TCP ACK。
- 根据操作回答“四、实验任务”中的 1-2 题。

3 TCP 基础

根据操作回答“四、实验任务”中的 3-9 题。

4 TCP 拥塞控制

- 在 WireShark 已捕获分组窗口中选择一个 TCP 报文段。点击菜单： 统计 ->TCP 流图-> 时间序列



每个点代表一个已发送的 TCP 段，绘制出该段的序列号与发送时间的关系。注意，相互堆叠的一组点代表发送方连续发送的一系列数据包

- 根据操作回答“四、实验报告内容”中的第 10 题

四、 实验任务

回答以下问题，附实验步骤和截图：

1. 向 gaia.cs.umass.edu 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？（附本主机的 IP 地址，MAC 地址截图/IPconfig）
2. gaia.cs.umass.edu 服务器的 IP 地址是多少？此次连接，服务器发送和接收 TCP 报文的端口号是多少？

3. 通过对 TCP 包的分析，给出建立 TCP 连接的三次握手过程，标志位（SYN、ACK）设置、序号和确认号分别是多少？（注意：给出“raw” sequence number，以及“raw” Acknowledgement number）
4. 包含 HTTP POST 命令头的 TCP 报文段的序号是多少？ 该 TCP 段的有效载荷（数据）部分中包含多少字节的数据？
5. 如果将包含 HTTP POST 消息的 TCP 报文段看作是 TCP 连接上的第一个报文段：回答以下问题
   a) 该报文段何时发送？响应的 ACK 是何时接收的？
   b) 该报文段的 RTT 是多少？
   c) 第二个报文段的发送时间和 ACK 接收时间分别是多少？RTT 是多少？
   d) 估算往返时间 EstimatedRTT（假设在计算第二个段的 ACK 后的 EstimatedRTT 时，初始值 EstimatedRTT 等于第一个段的测量 RTT，采用教材上的公式计算，且 α=0.125）
6. 前 4 个承载数据的 TCP 段，每个段的长度（首部加上数据）是多少？
7. 在发送前 4 个承载数据 TCP 段的过程中，服务器向客户端发送的窗口最小值是多少？分析该窗口值的作用；
8. 分析 trace file（菜单**统计 → TCP 流图 →时间序列**）发送过程中是否有重传的报文段？判断的依据是什么？
9. TCP 连接的吞吐率(bytes transferred per unit time，单位时间传输的字节数)是多少？给出计算过程。
10. 浏览由客户端向服务器发送的报文段序号和时间对应关系图。能否辨别出 TCP 慢启动阶段的起止，以及在何处转入避免拥塞阶段？ 根据实际得到的数据，分析窗口变化情况，以及与理论上的 TCP 拥塞控制算法有何不同。