华东师范大学数据科学与工程学院实验报告

课程名称：计算机网络与编程	**年级：**2021	**上机实践成绩：**
指导教师：张召	**姓名：温兆和**	**学号：**10205501432
上机实践名称：UDP 和 TCP 协议分析		**上机实践日期：**2022.05.20
上机实践编号：13	**组号：**001-432	**上机实践时间：**13：00

一、 实验目的

了解 UDP 协议的工作原理；

了解 TCP 协议的工作原理：

学习 TCP 建立连接三次握手的过程；

学习 TCP 断开连接四次挥手的过程。

二、 实验任务

使用 Wireshark 快速了解 UDP 协议；

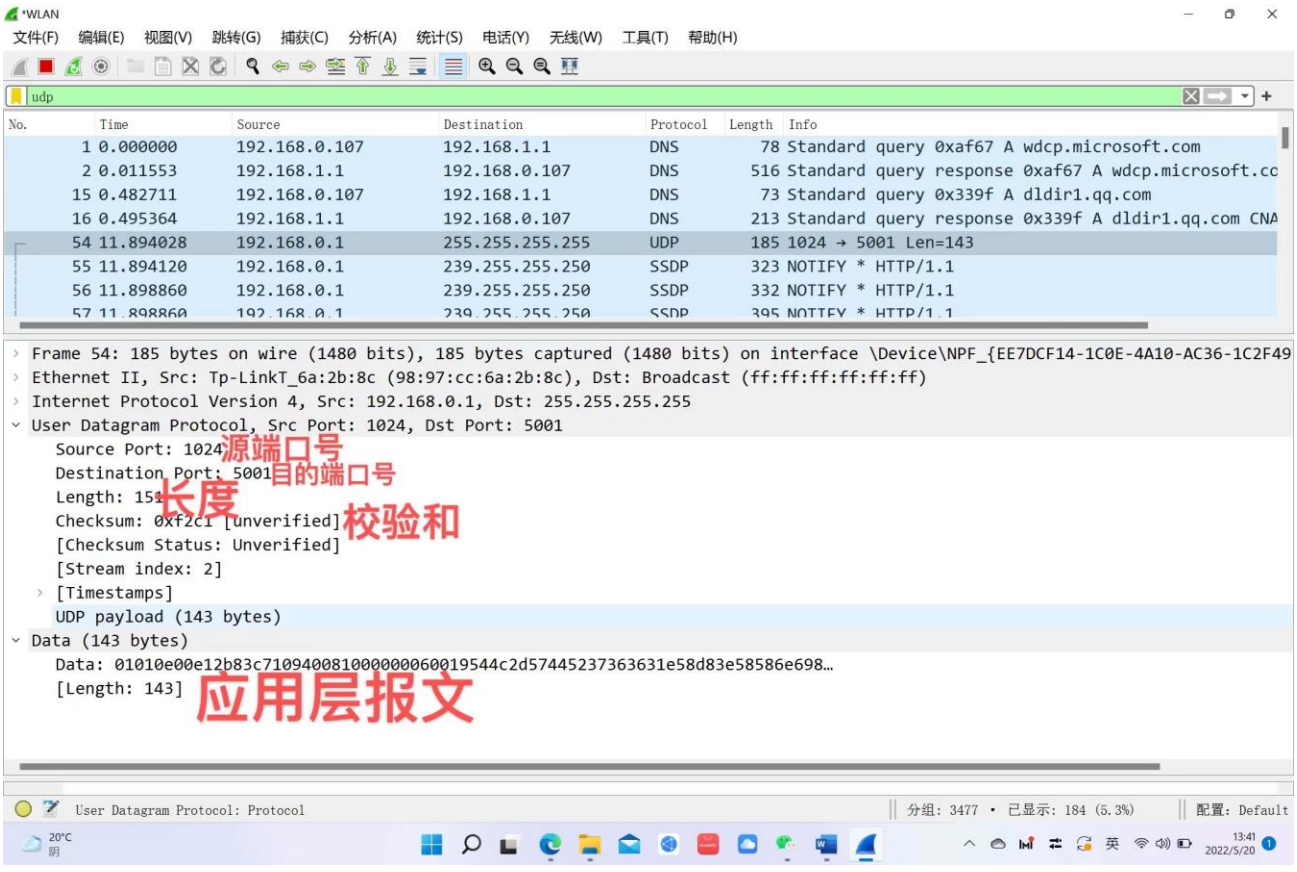
使用 Wireshark 快速了解 TCP 协议。

三、 使用环境

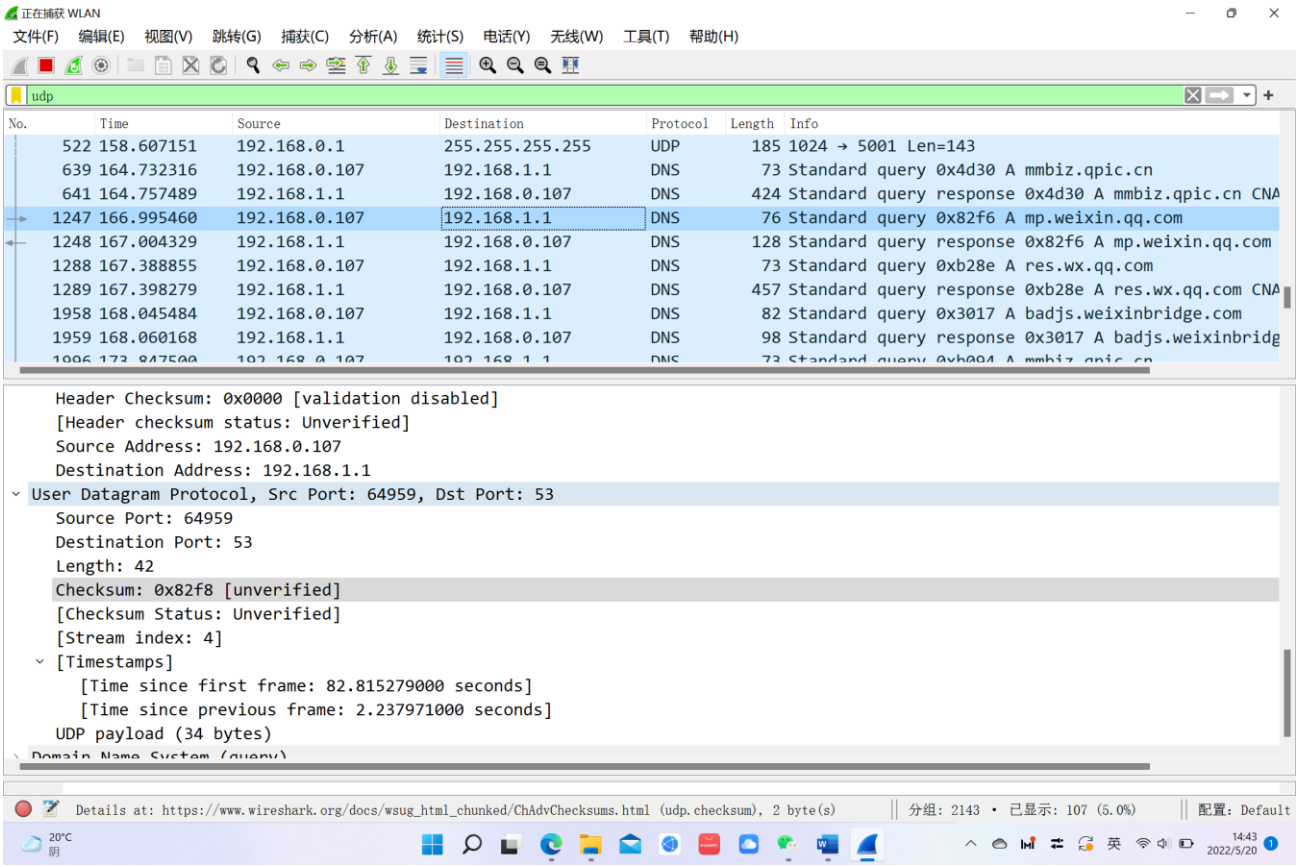
Wireshark

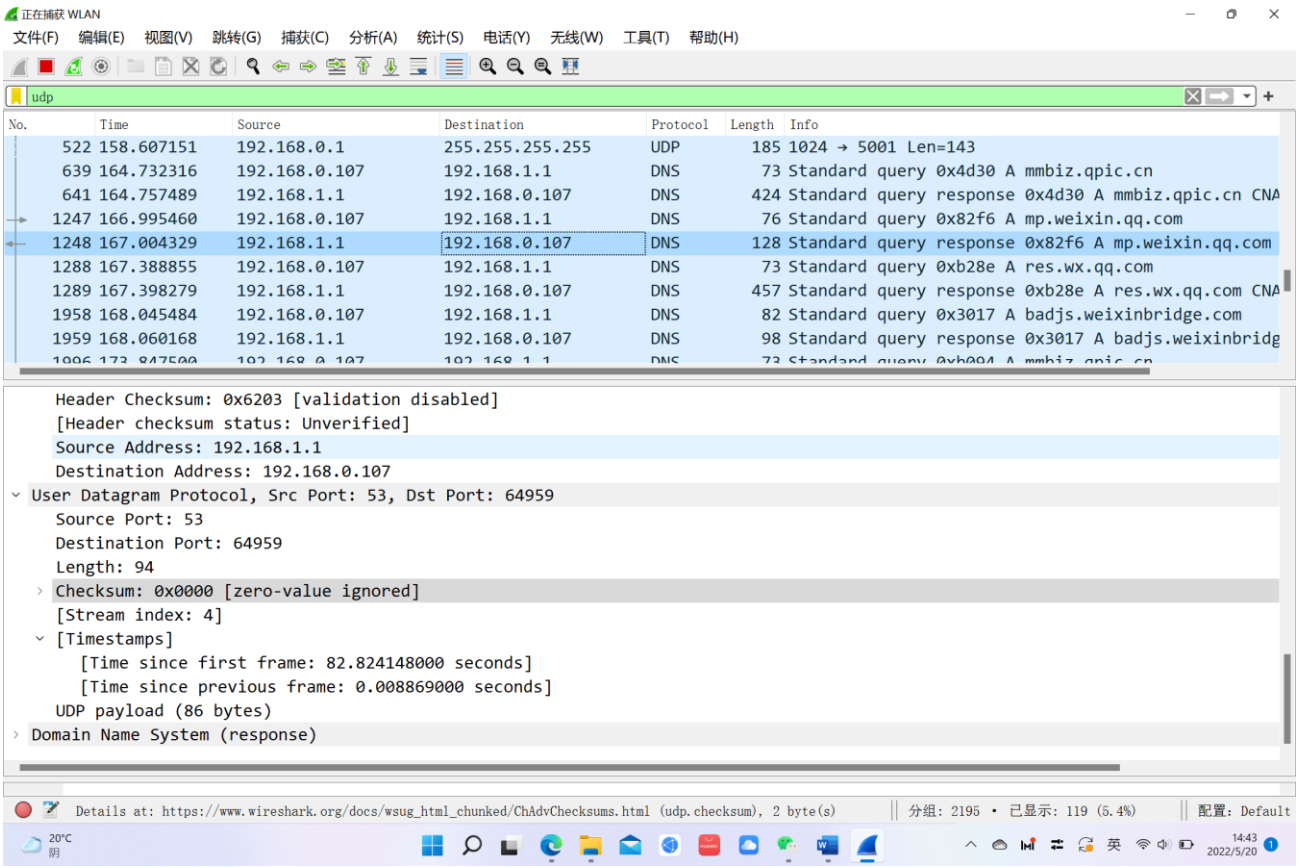
四、 实验过程

Task1. 从跟踪中选择一个 UDP 数据包。从此数据包中，识别并确定 UDP 首部字段，请为这些字段命名并将实验结果附在实验报告中。



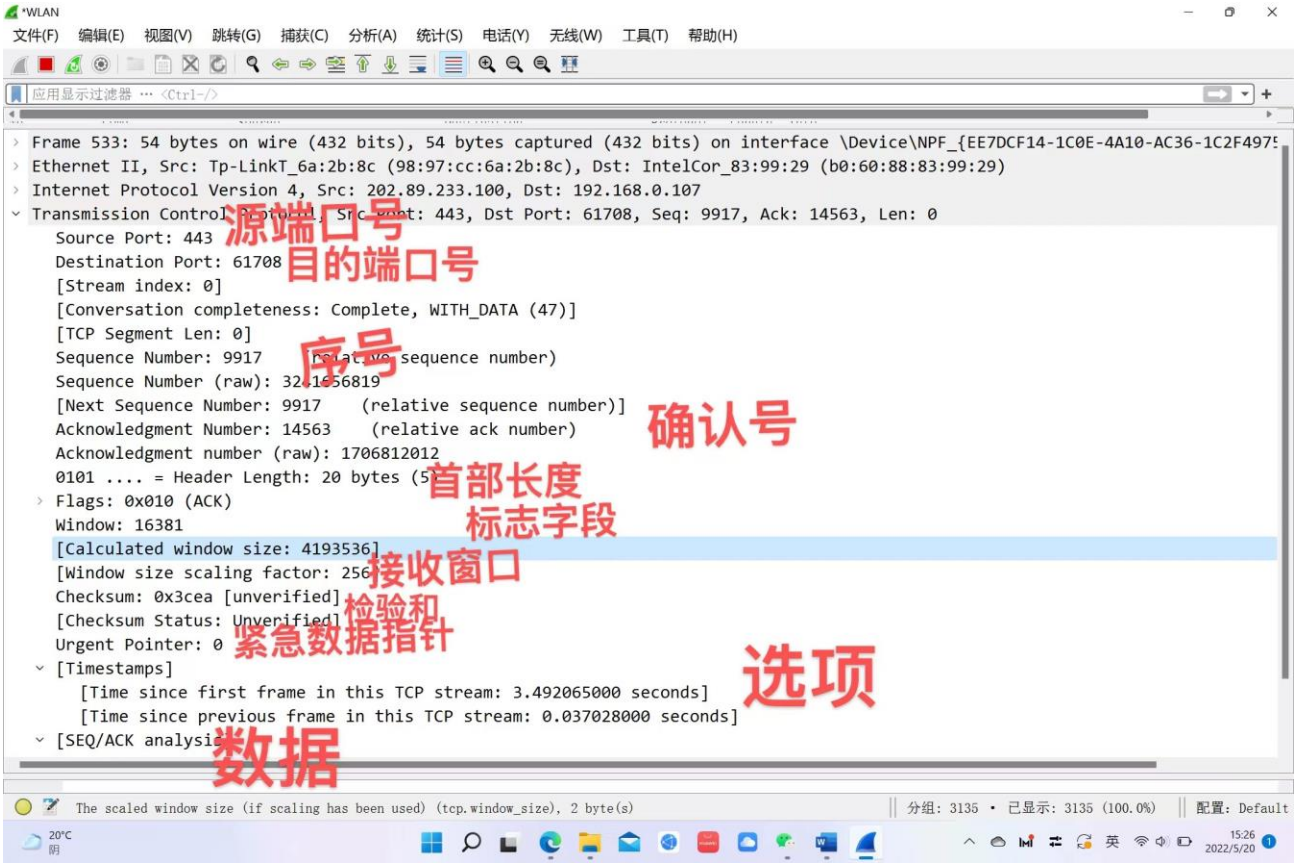
Task2. UDP 首部中的长度字段指的是什么，以及为什么需要这样设计？使用捕获的 UDP 数据包进行验证，请将实验结果附在实验报告中。
指的是数据字段长度加上首部字段长度，在上例中是 143+8=151。
这样设计是因为不同 UDP 网络包中数据字段长度不同，所以需要一个明确的长度。
Task3. UDP 有效负载中可包含的最大字节数是多少？请将实验结果附在实验报告中。
总长度：65536bit
首部字段：8bit
应用层报文中可容纳的最大长度：65536-8=65528bit
Task4. 观察发送 UDP 数据包后接收响应的 UDP 数据包，这是对发送的 UDP 数据包的回复，请描述两个数据包中端口号之间的联系。请将实验结果附在实验报告中。
上面抓到的 UDP 数据包并没有响应数据包，所以我们抓取一个 DNS 数据包并找到它的响应报文，观察源端口号和目的端口号之间的关系。DNS 使用 UDP。





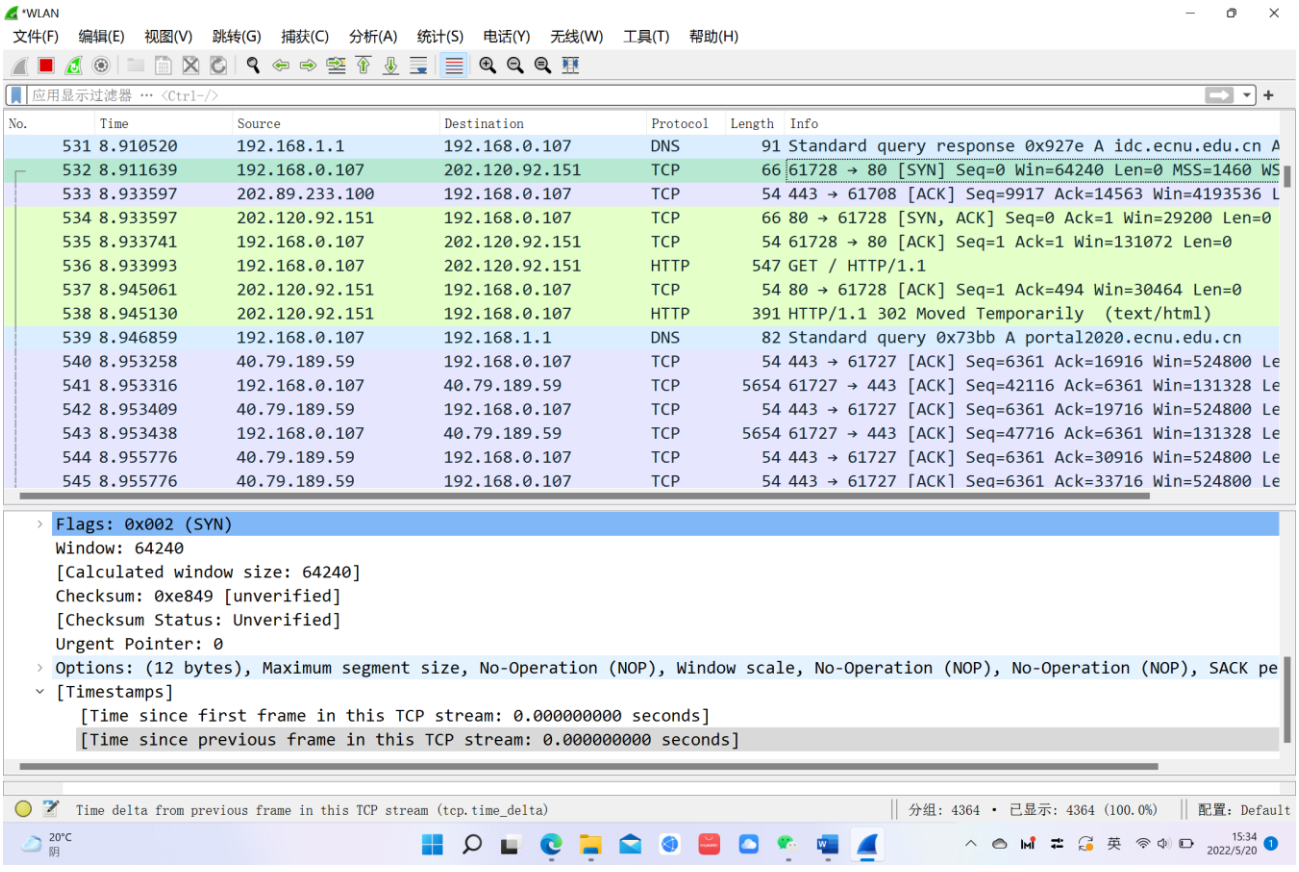
我们可以看到，在 UDP 协议中，响应数据包的目的端口号是原数据包的源端口号，源端口号是原数据包的目的端口号。

Task5. 利用 Wireshark 抓取一个 TCP 数据包，查看其具体数据结构和实际的数据（要求根据报文结构正确标识每个部分），请将实验结果附在实验报告中。

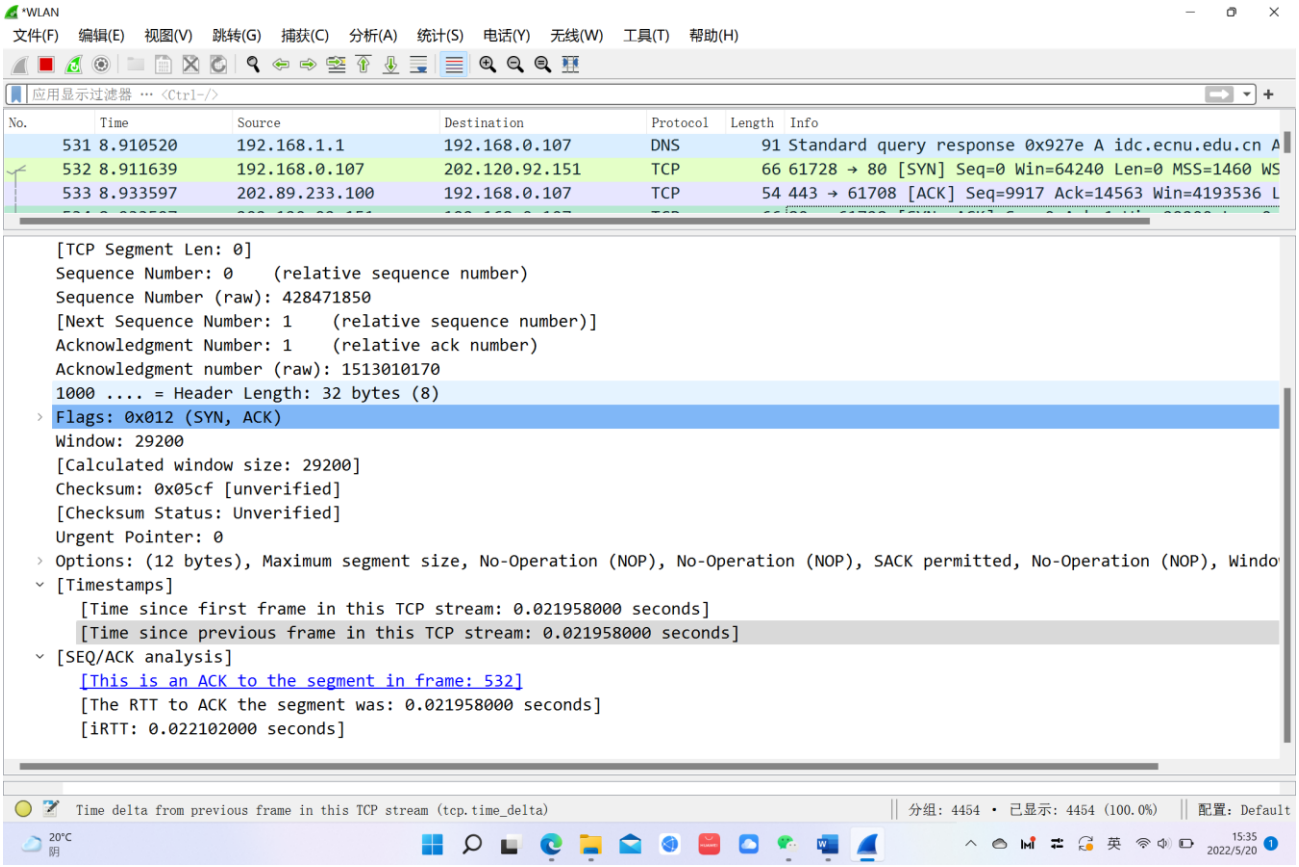


Task6. 根据 TCP 三次握手的交互图以及 TCP 报文段结构图逐步分析三次握手过程，请将实验结果附在实验报告中。

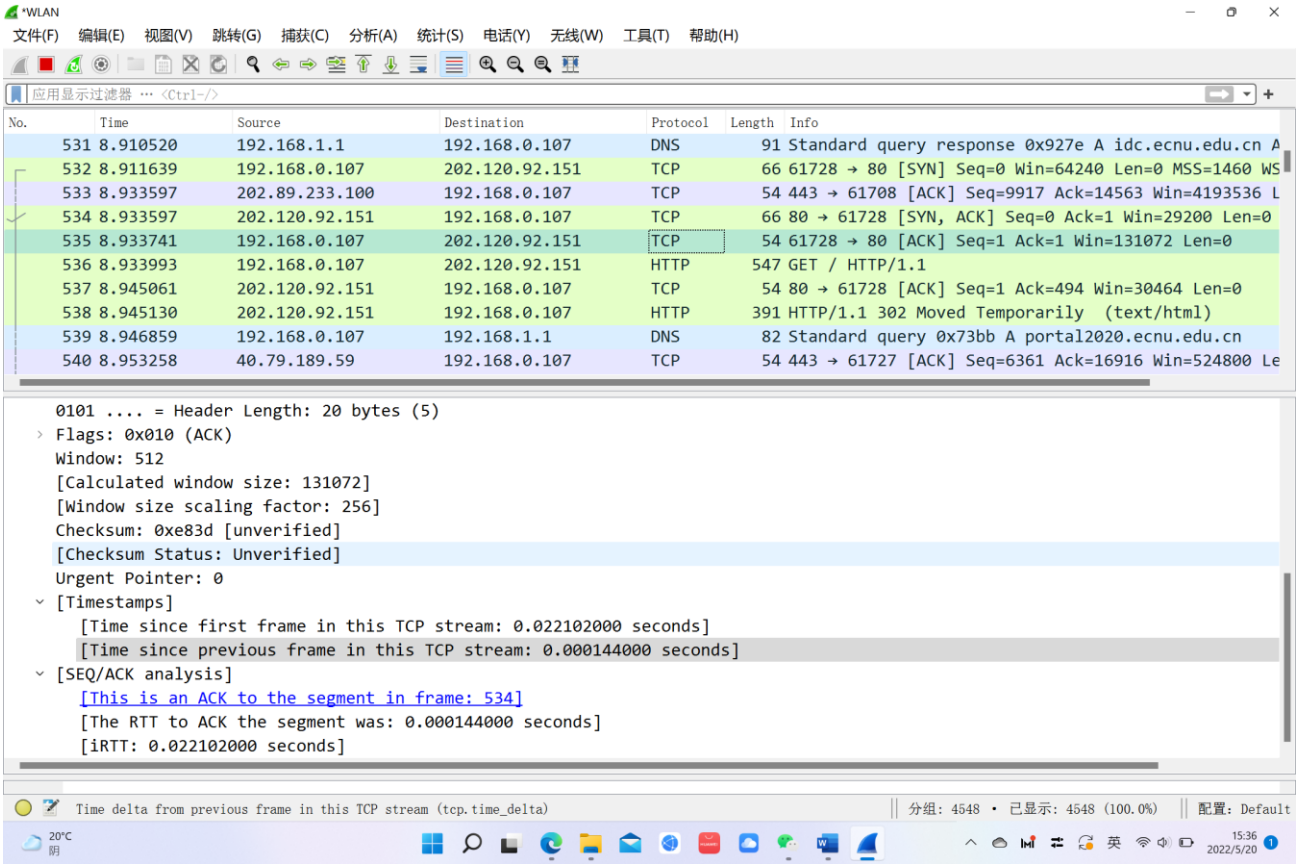
第一次握手：客户端发送 SYN 报文



第二次握手：服务端发送 SYN 和 ACK 报文



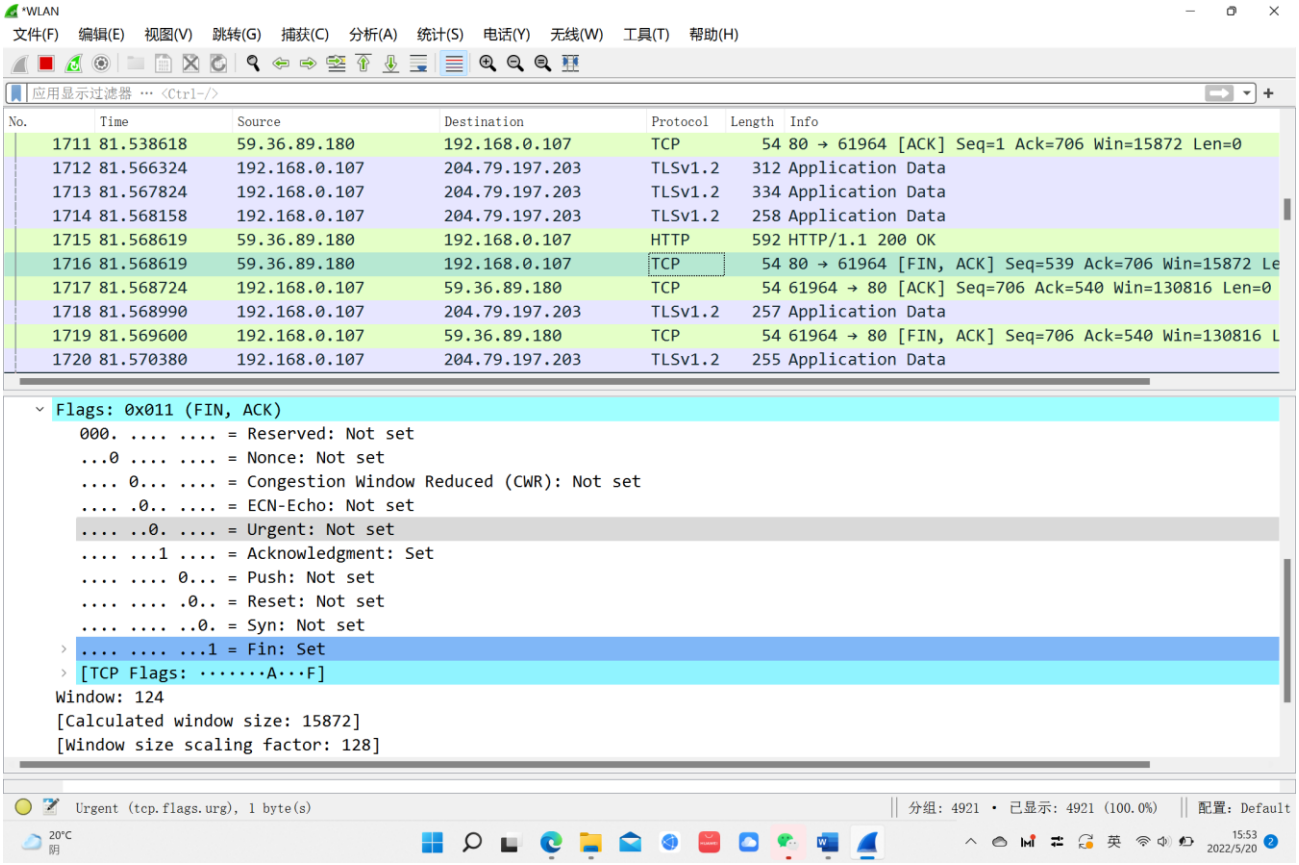
第三次握手：客户端发送 ACK 报文



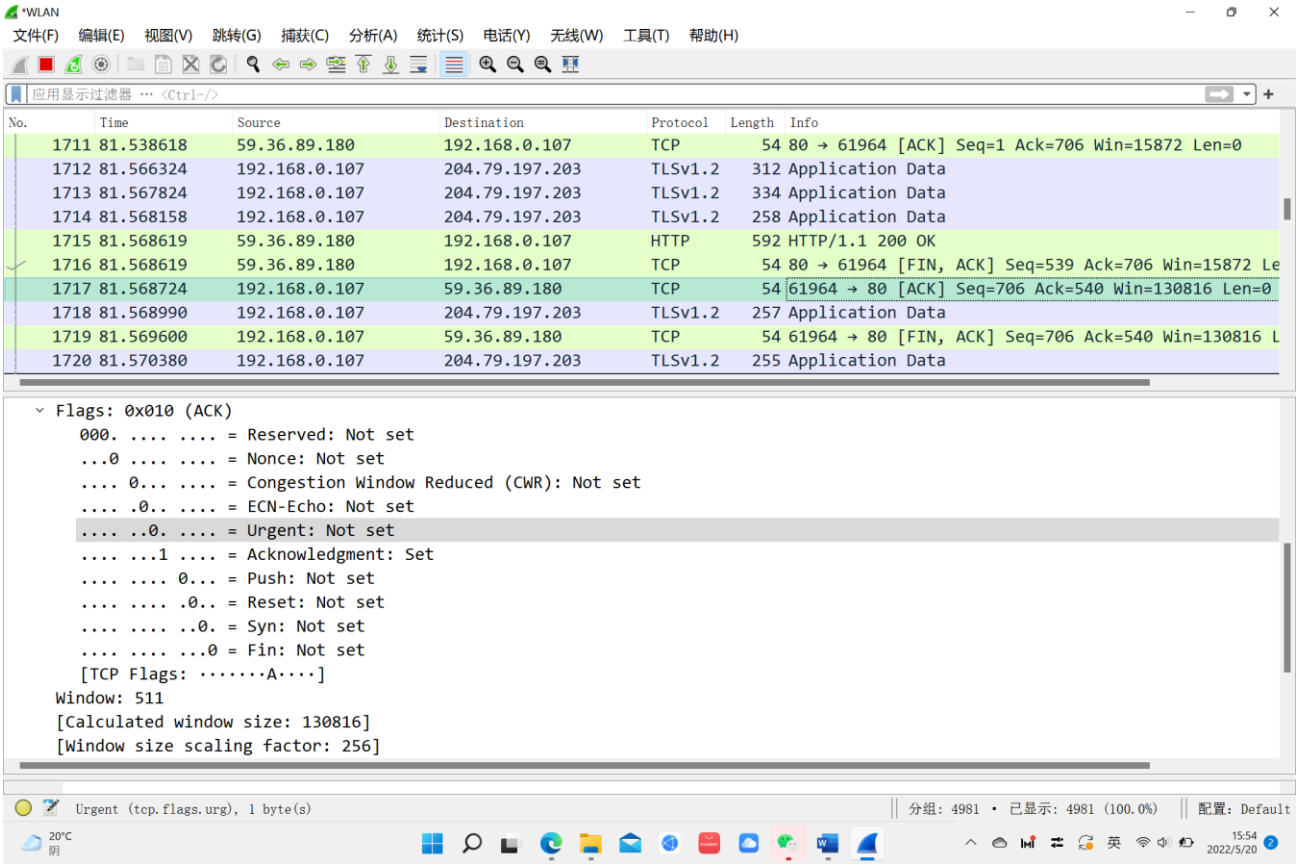
Task7. 根据 TCP 四次挥手的交互图以及 TCP 报文段结构图逐步分析四次挥手过程，请

将实验结果附在实验报告中。

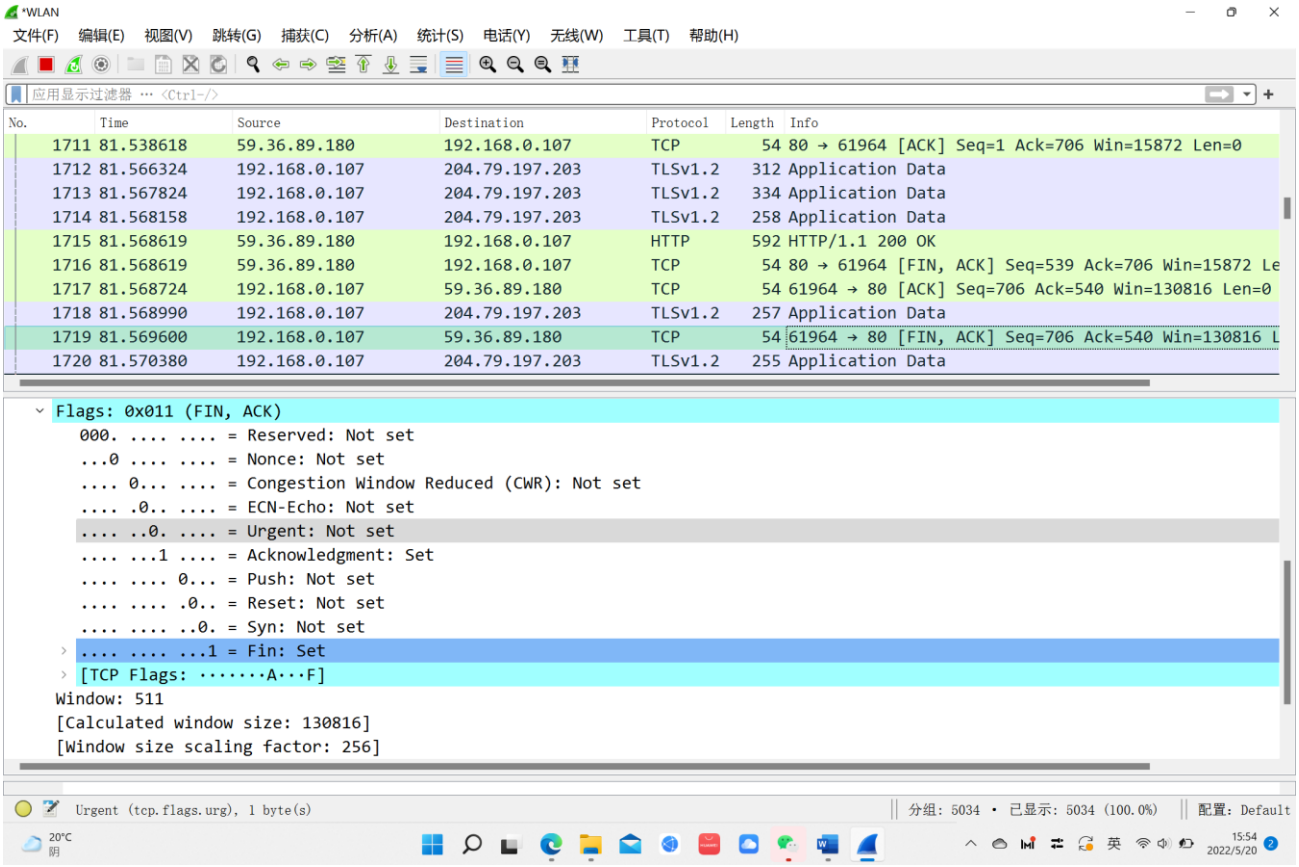
第一次挥手：主动关闭方发送 FIN



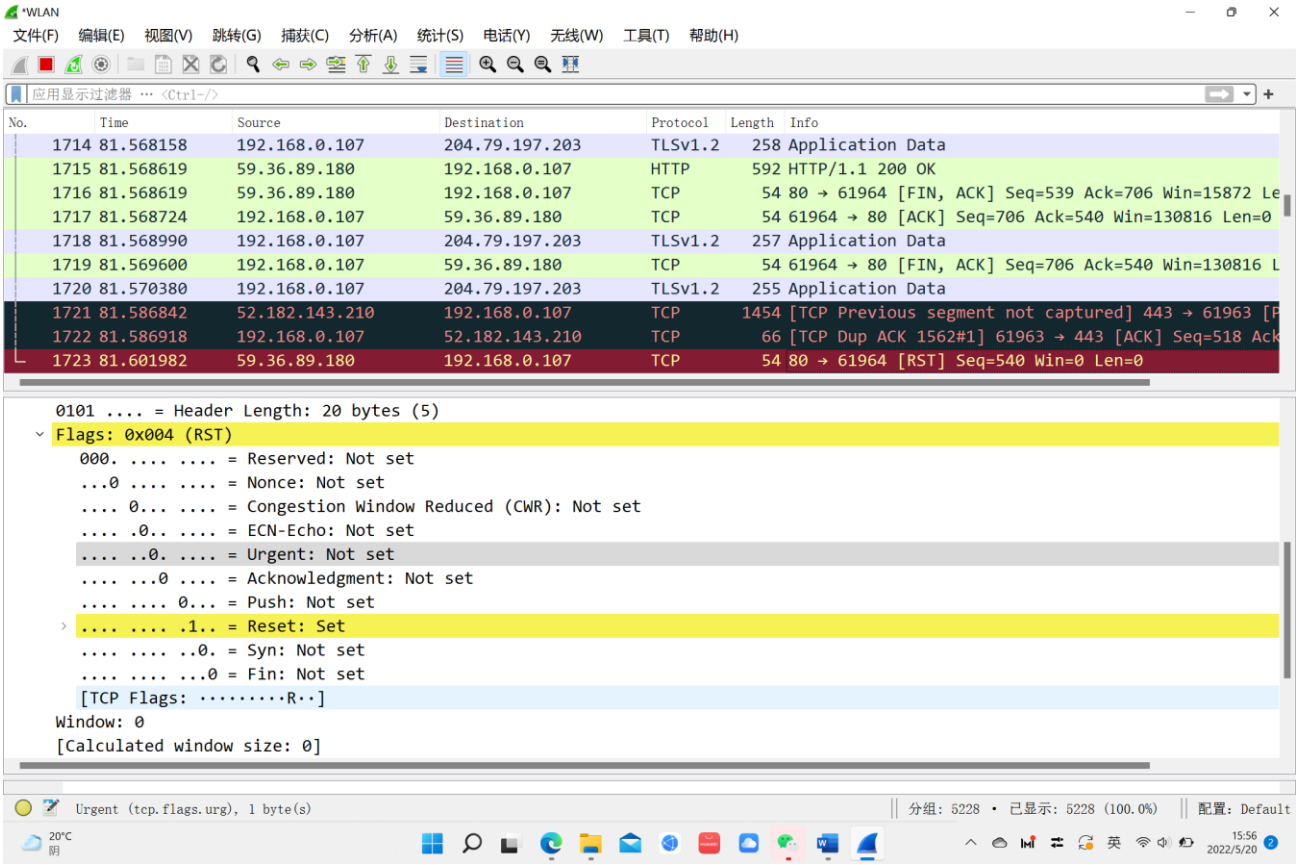
第二次挥手：被动关闭方发送 ACK



第三次挥手：被动关闭方发送 FIN



第四次挥手：主动关闭方发送 ACK，连接断开



五、**总结**

在本周的实验中，我们使用 Wireshark 快速了解了 TCP 和 UDP 协议，为以后的学习打好了基础。