《计算机网络课程实验》
实验报告

姓名：	陈驰
学号：	2021303090
班级：	SC012101
日期：	2023/1/1

西北工业大学网络空间安全学院

2022 年 11 月

目录

实验一

一、实验题目和目的

实验题目：网络协议封包分析

实验时间：11 月 21 日

实验地点：翱翔学生中心 104 实验室

实验目的：掌握 Wireshark 软件的使用方法，并能够网络协议封包进行分析

二、实验具体内容与步骤

a)

1. 实验内容

分析 Ping 命令的执行过程

2. 实验步骤：

实验环境

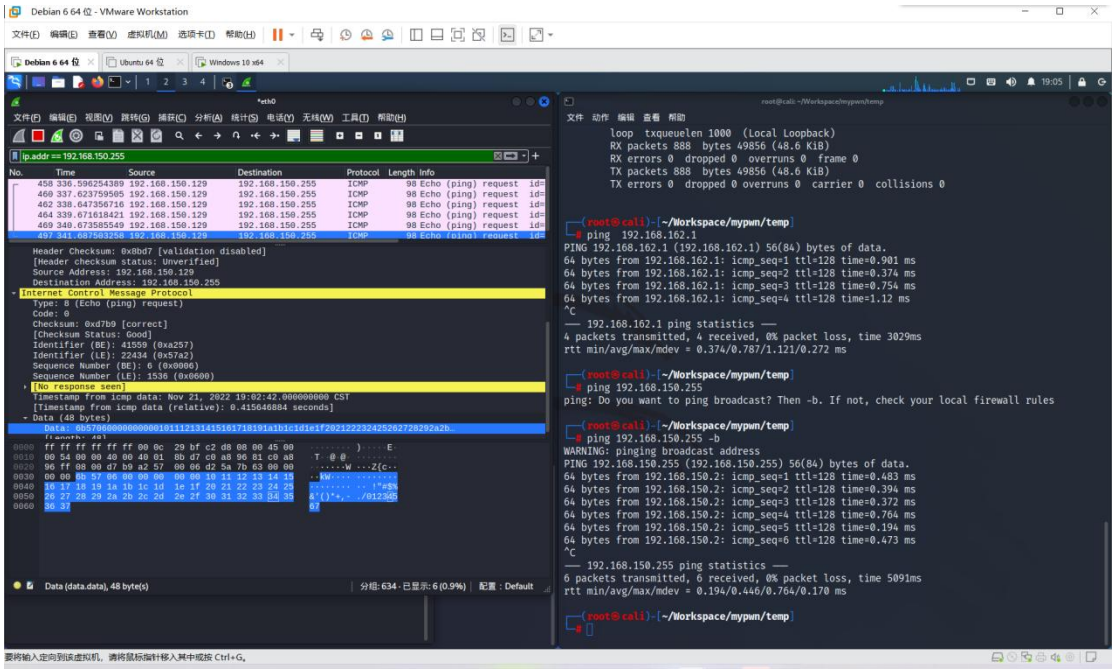
PC1　kali　　ip:192.168.150.129

PC2　win11　ip:192.168.162.1

默认网关 192.168.150.255

使用 PC1 向网关进行 ping，使用 wirshark 进行抓包

Ping 使用 ICMP 报文



IP　数据报首部信息如下

字段	报文信息	说明

版本	4	IP 使用版本号
首部长度	20	IP 头的长度
区分服务	0	优先级标志位和服务类型标志位，被路由器用来进行流量的优先排序
总长度	84	IP 头与数据包中数据的长度
标识	0	一个唯一的标识数字，用来识别一个数据包或者被分片数据包的次序
标志	0x40	用来标记一个数据包是否是一组分片数据包的一部分
片偏移	0	一个数据包是一个分片，这个域中的值就会被用来将数据包以正确的顺序重新组装
生存时间	64	用来定义数据包的生存周期，已经过路由器的跳数/秒数进行描述
协议	1	用来识别在数据包序列中上层协议数据包的类型
首部检验和	0x8db7	一个错误检测机制，用来确认 IP 头的内容没有被损坏或者篡改
源地址	192.168.150.129	发出数据包的主机的 IP 地址
目的地址	192.168.150.255	数据包目的地址 IP 地址

b)

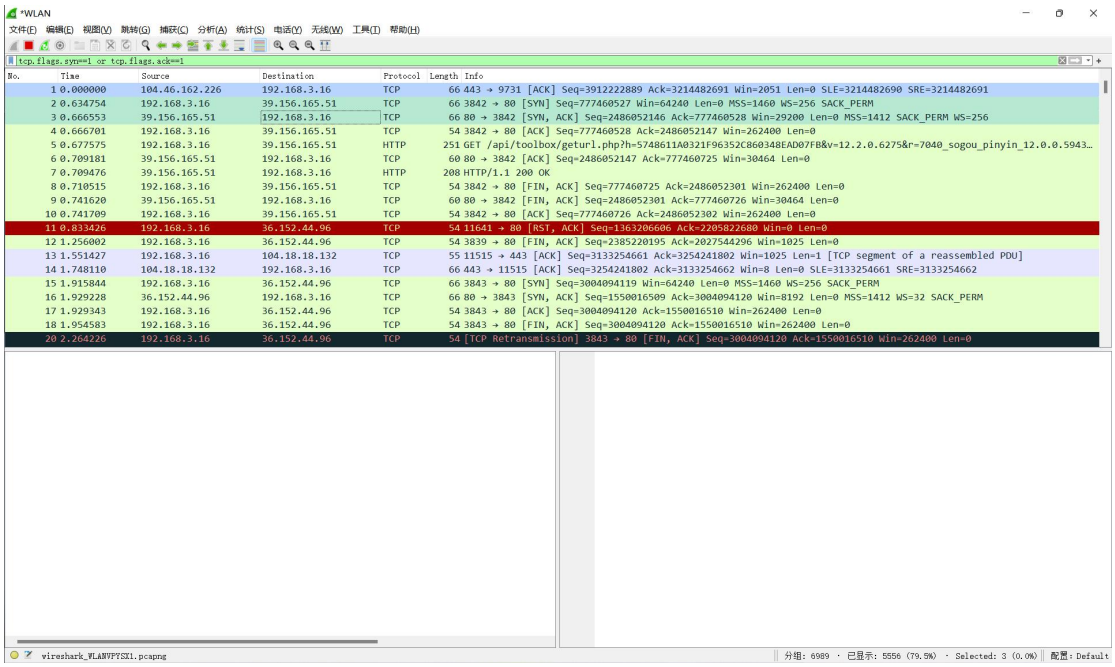
1.实验内容

分析 TCP 三次握手过程

2.实验步骤：

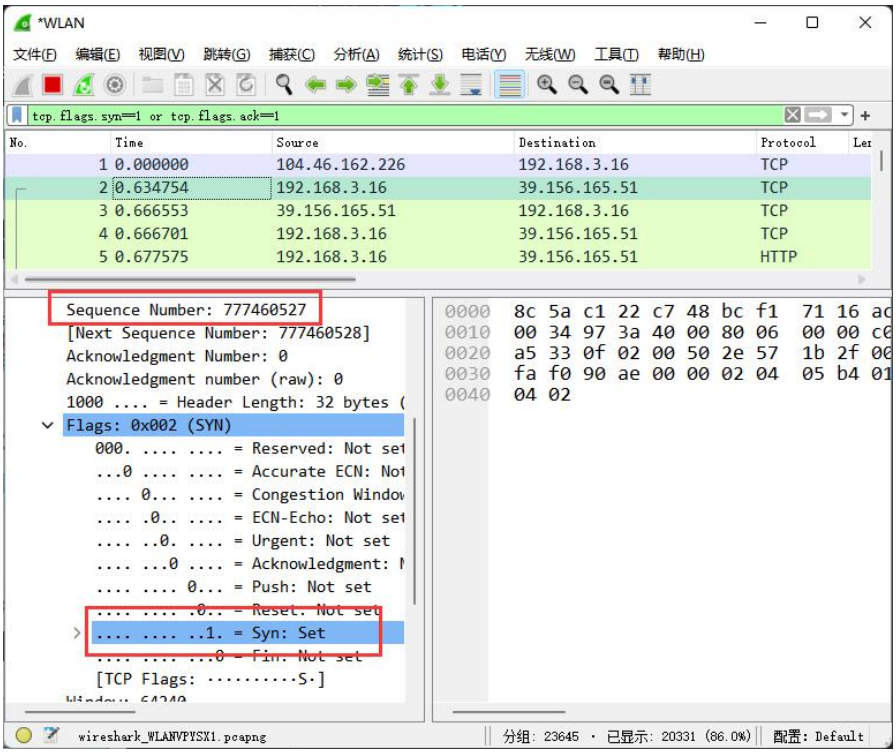
打开 Wireshark，选择网络接口捕获流量

在过滤器中输 tcp.flags.syn==1 过滤出所有 SYN 包，使用 tcp.flags.ack==1 过滤出 ACK 包，可以看到 TCP 三次握手的过程——客户端发送的 SYN 包，然后服务器回复 SYN-ACK 包，最后客户端回复 ACK 包。且可以看到在三次 TCP 后出现 HTTP 报文，说明 http 是有 TCP 协议建立连接的。

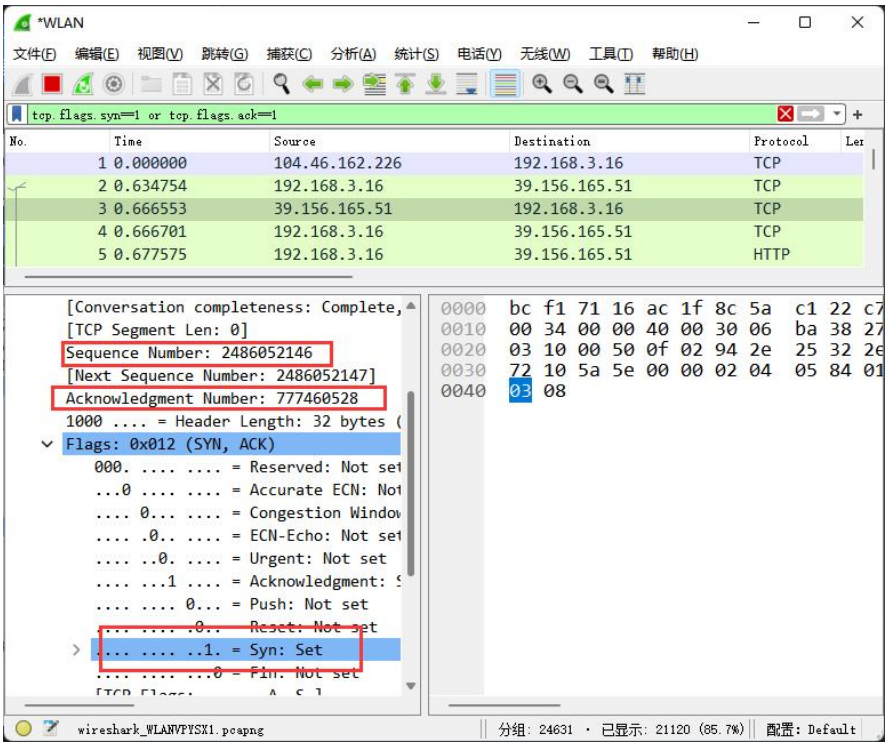


专门观察这三次包，

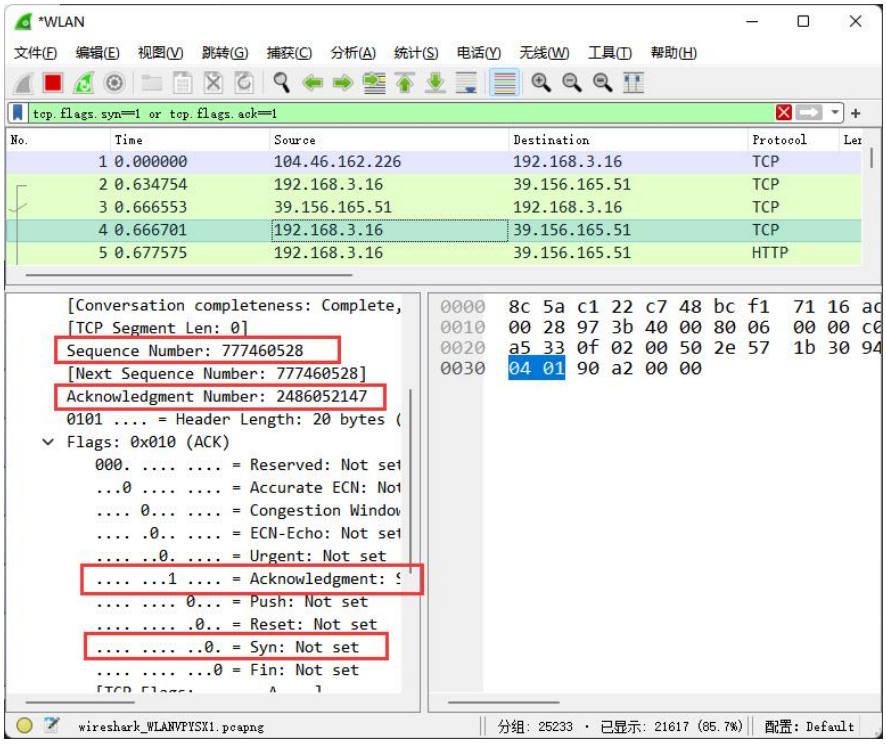
第一次握手，客户端向服务器发送连接请求包，标志位 SYN 为 1，Sequence number 为 777460527



第二次握手： 服务器收到客户端发过来报文，由 SYN=1 知道客户端要求建立联机。向客户端发送一个 SYN 和 ACK 都置为 1 的 TCP 报文，设置初始序号为 2486052146，将确认序号(Acknowledgement Number)设置为客户的序列号加 1，



第三次握手： 客户端收到服务器发来的包后检查确认序号(Acknowledgement Number)是否正确，即第一次发送的序号加 1。以及标志位 ACK 是否为 1。若正确，客户端再次发送确认包，ACK 标志位为 1，SYN 标志位为 0。Acknowledgement Number 加一变为 2486052147，Sequence number 加一变为 777460528。服务器收到后确认序号值与 ACK=1 连接建立成功。



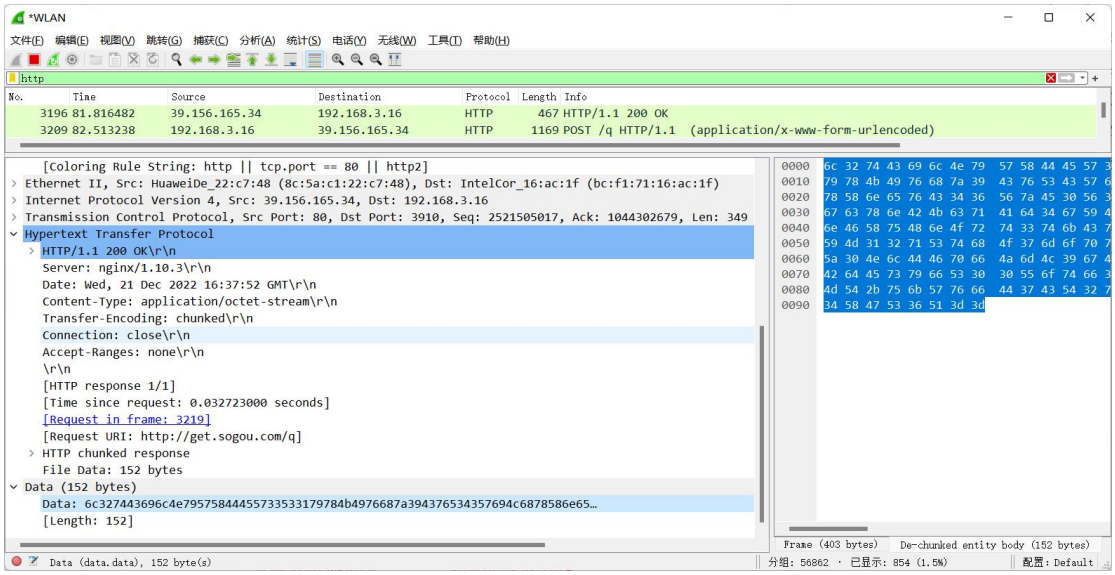
c)

1. 实验内容

分析 http 报文长度

2. 实验步骤：

选择一个 http 数据包，查看 fileData 字段查看长度，说明传输 152 字节的数据



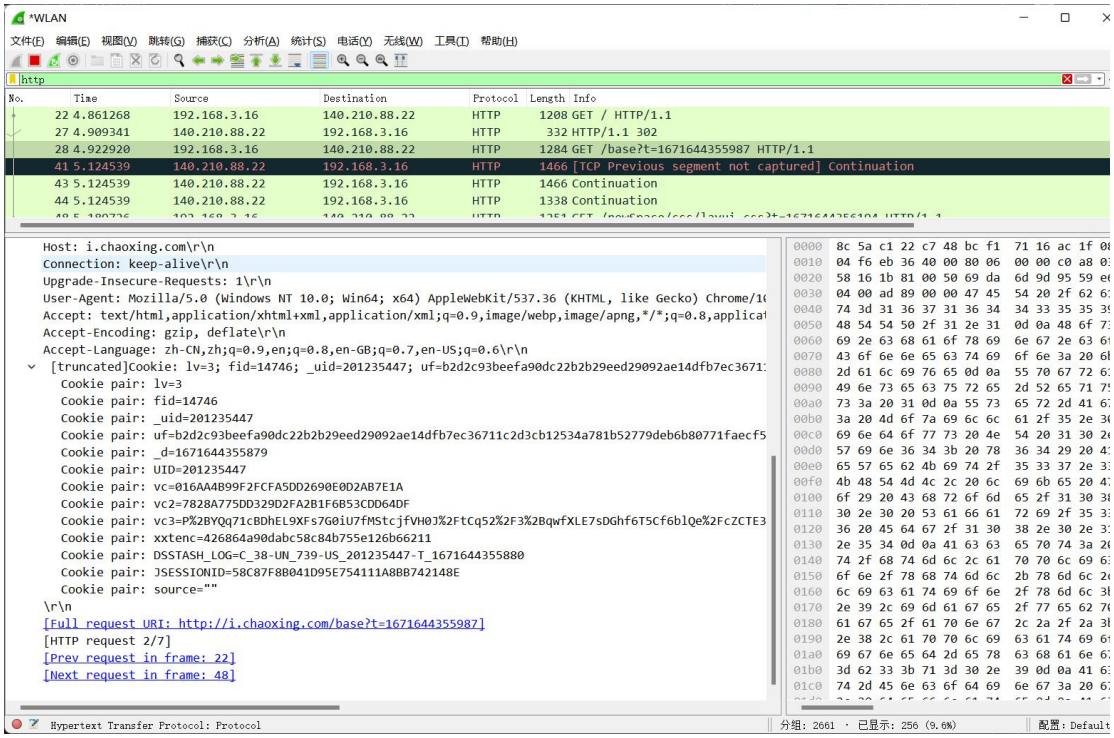
d)

1. 实验内容

找出 HTTP 中的口令字段

2. 实验步骤：

打开超星进行登录同时抓包



可以看到有我在学习通中的 uid，以及 cookie。

三、体会和收获

在本次学习中我掌握了 Wireshark 的使用方法，通过使用 Wireshark，可以快速查看网络中传输的各种协议封包，并对封包进行过滤和分类，以便更好地理解网络中发生的事情，帮助了解学习网络知识。

学会使用 Wireshark 并能够对网络协议封包进行分析，对我的网络管理工作将大有裨益。这项技能不仅能帮助我更好地理解网络中发生的事情，还能帮助我快速定位网络故障并进行修复。