**广州大学学生实验报告**

开课学院及实验室：计算机科学与工程实验室电子楼518室 2020年\*\*月\*\*日

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 学院 | 计算机科学与教育软件 | | 年级、专业、班 | \*\*\* | 姓名 | \*\*\* | 学号 | \*\*\* |
| 实验课程名称 | | 计算机网络实验 | | | | | 成绩 |  |
| 实验项目名称 | | 使用网络协议分析器捕捉和分析协议数据包 | | | | | 指导老师 | 綦科 |

**（1）实验目的**

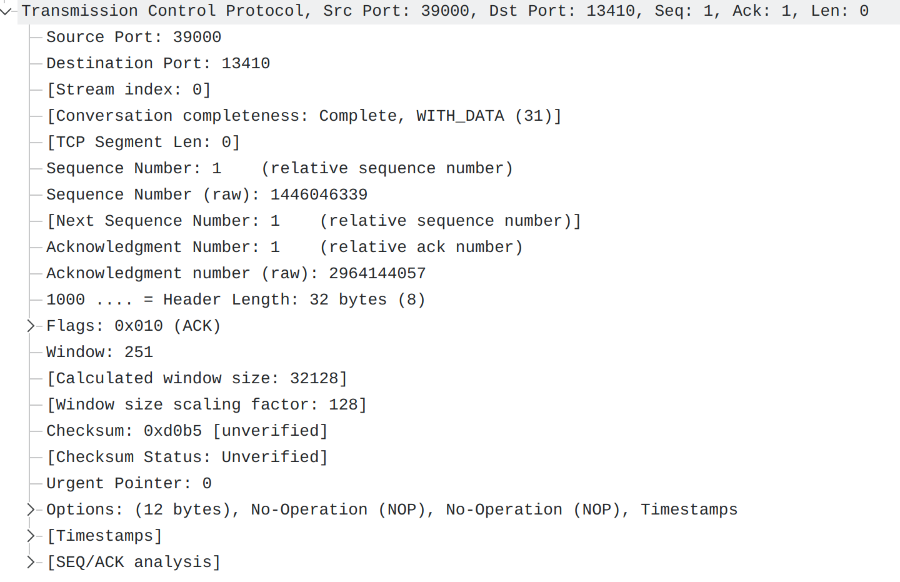
熟悉Wireshark的使用；验证各种协议数据包格式；学会捕捉并分析各种数据包。

**（2）实验环境**

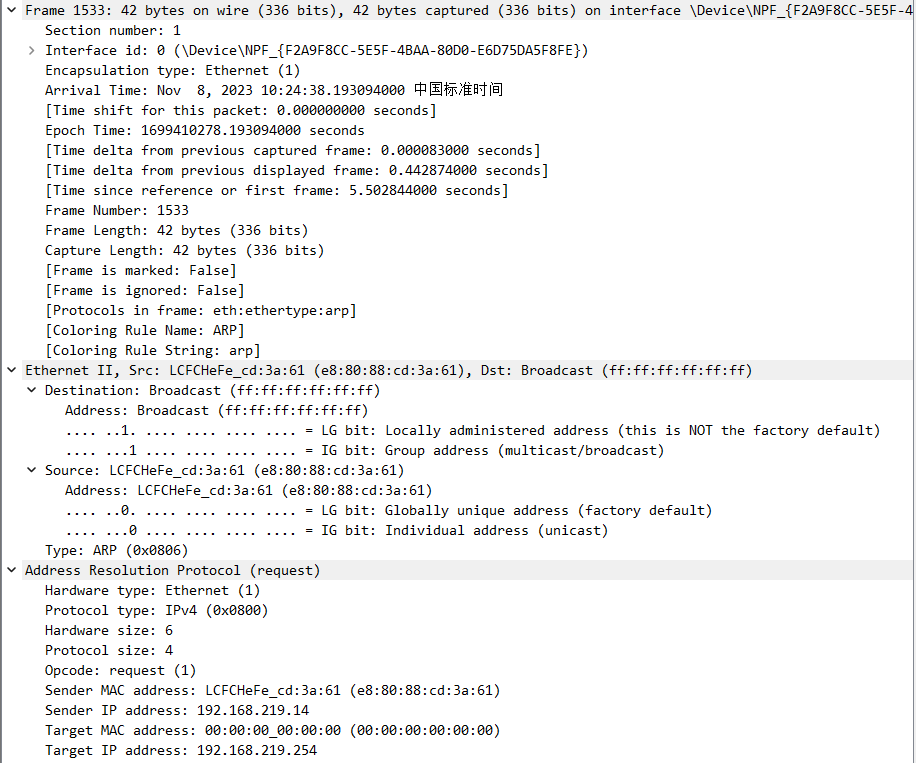
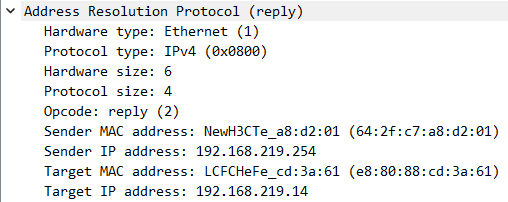
操作系统Windows 11 & Arch Linux、以太网；

**（3）实验内容、过程和分析**

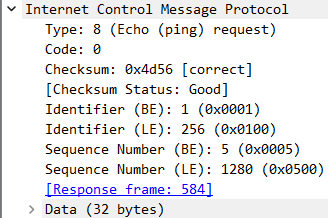
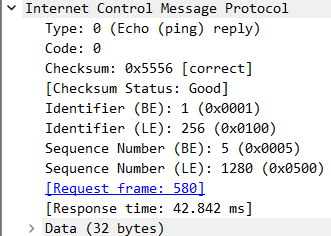
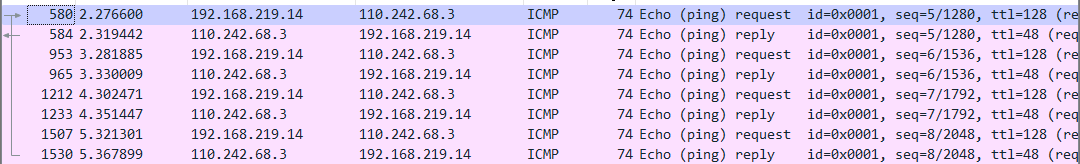
1. 安装Wireshark软件
2. 捕捉数据包，验证数据帧、IP数据报、TCP数据段的报文格式。



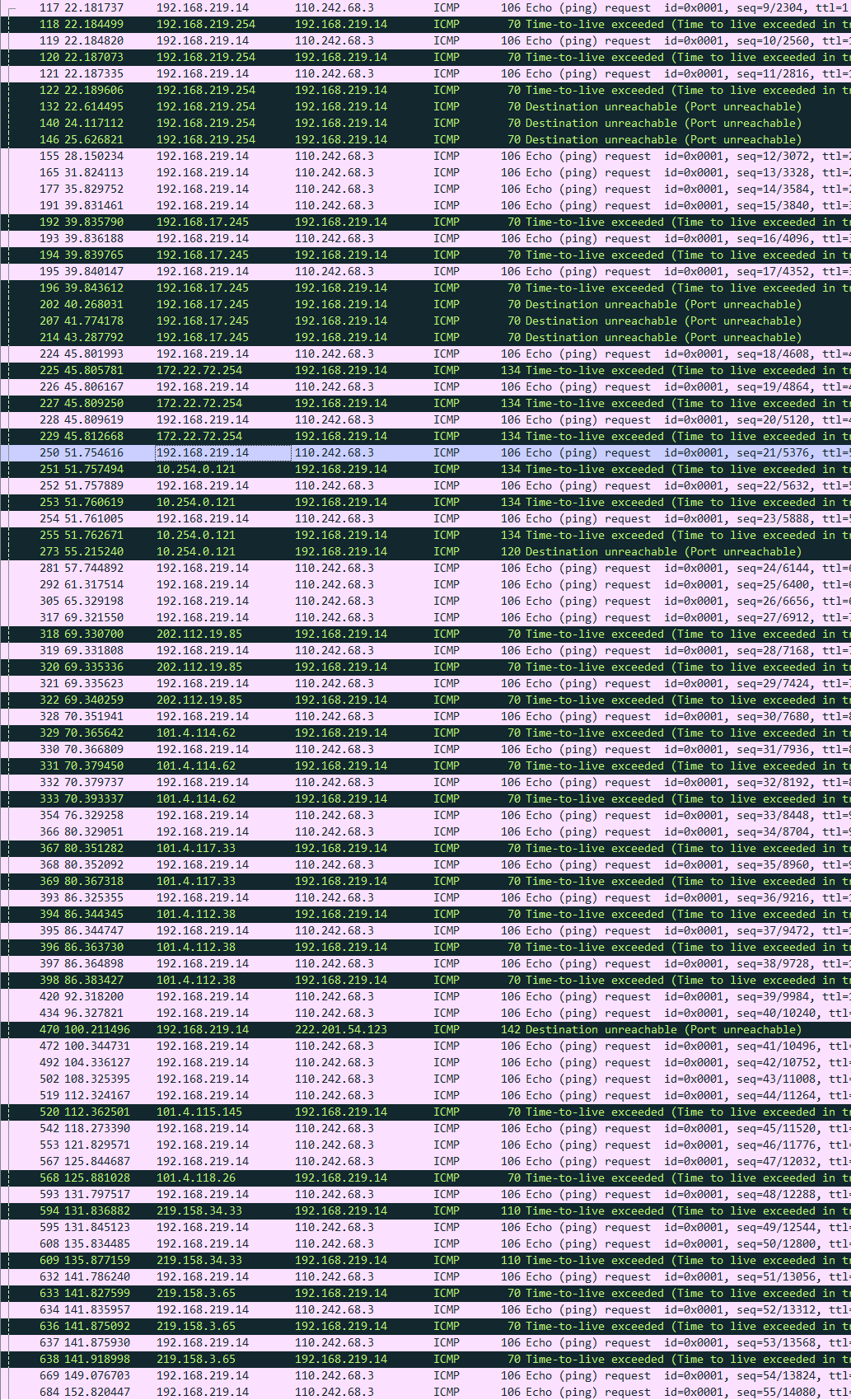
1. 捕捉并分析ARP报文。



1. 捕捉ping过程中的ICMP报文，分析结果各参数的意义。



1. 捕捉tracert过程中的ICMP报文，分析跟踪的路由器IP是哪个接口的。



1. 捕捉并分析TCP三次握手建立连接的过程。



（7） 捕捉整个FTP工作工程的协议包

对协议包进行分析说明，依据不同阶段的协议分析，画出FTP工作过程的示意图

a.. 地址解析ARP协议执行过程

b. FTP控制连接建立过程

c . FTP 用户登录身份验证过程

d. FTP 数据连接建立过程

e. FTP数据传输过程

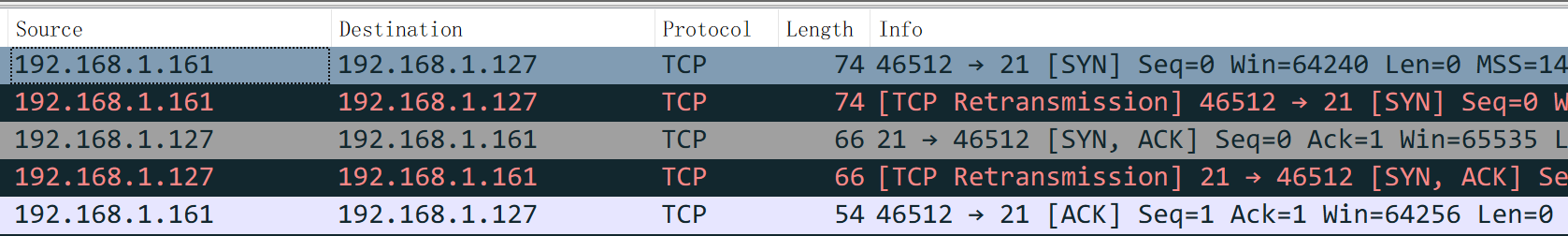
f. FTP连接释放过程（包括数据连接和控制连接）

主机上使用Filezilla Server建立FTP站点

使用Ubuntu虚拟机，从Windows 10主机用Wireshark抓包，指定以下规则捕捉桥接到LAN的Ubuntu虚拟机。



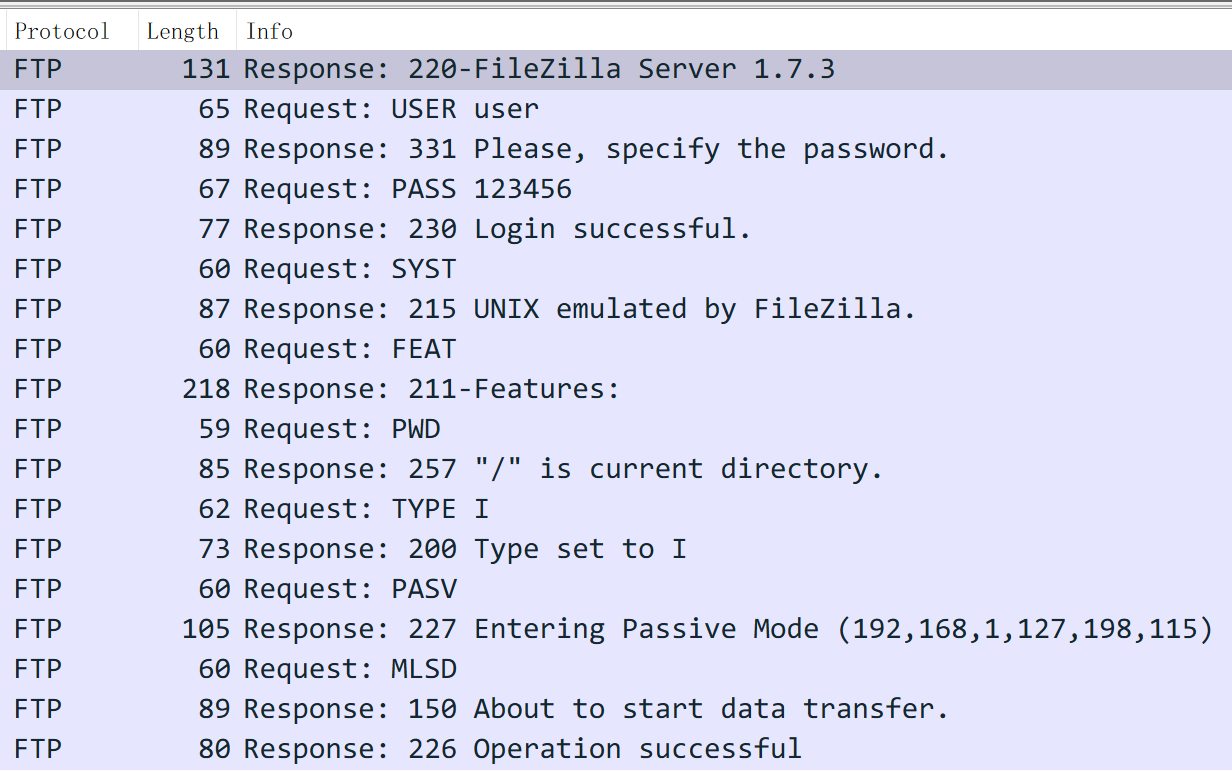
在虚拟机上使用Filezilla连接到主机建立的FTP站点，发现TCP握手，此时控制连接建立。



由于要监控FTP连接，Wireshark过滤规则改为如下。



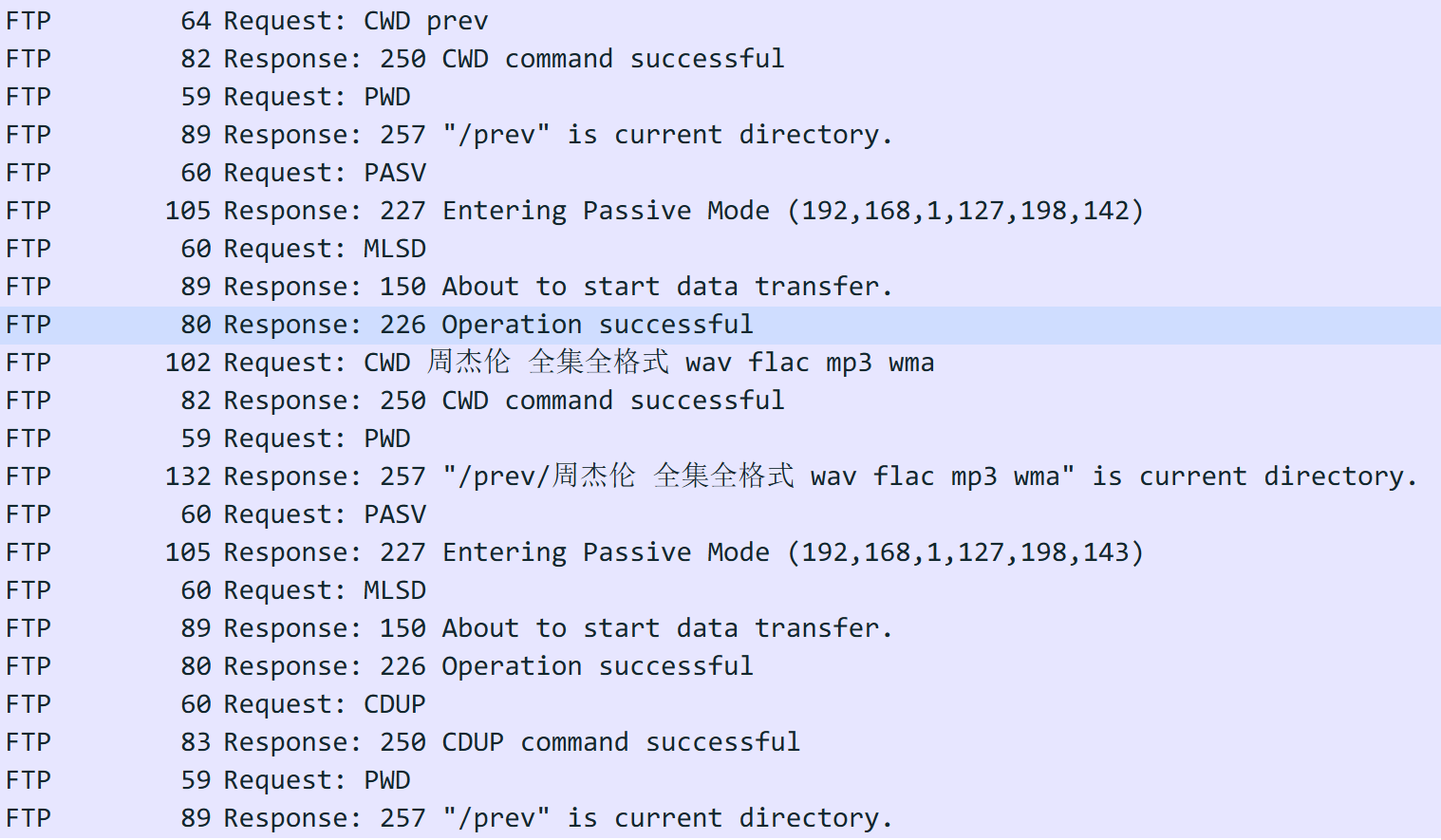
过滤可得FTP身份验证记录。



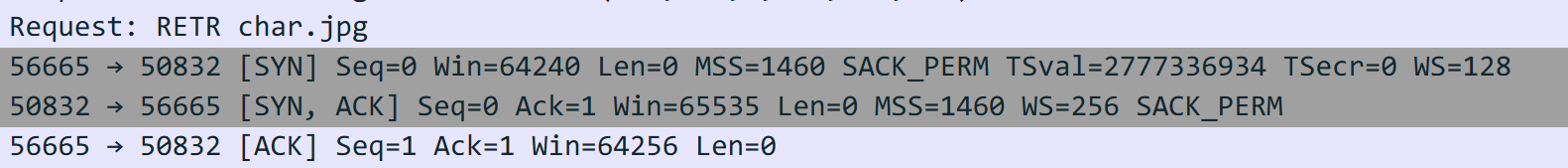
此时服务器也可见操作记录。



Filezilla中稍作浏览，可见操作。

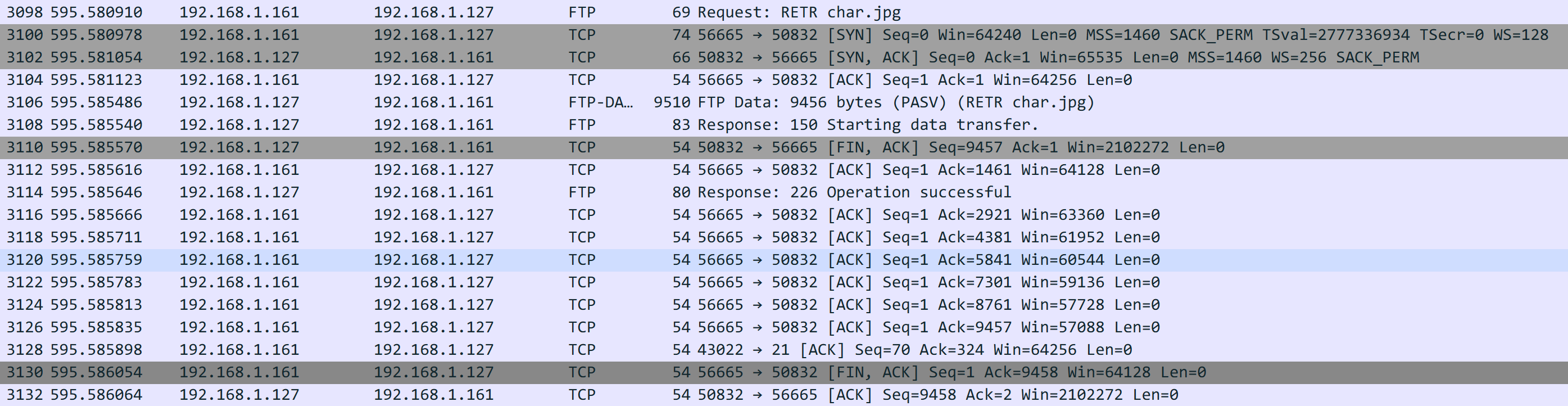


客户端侧开始下载文件，可以见到连接建立。

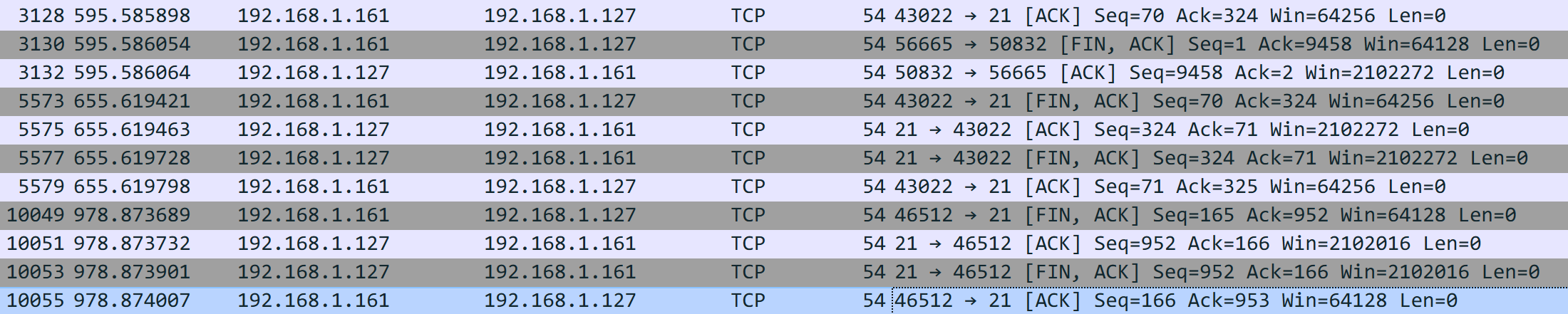


为了更好的分析连接情况，Wireshark筛选改为：(ip.src == 192.168.1.161 || ip.dst == 192.168.1.161) && (ip.src == 192.168.1.127 || ip.dst == 192.168.1.127) && !(tcp.analysis.retransmission or tcp.analysis.fast\_retransmission or tcp.analysis.duplicate\_ack)

可以看到文件传输的ACK和最后释放数据连接的过程。



客户端侧断开连接，可以看到控制连接的释放过程。



服务器也提示session终止。

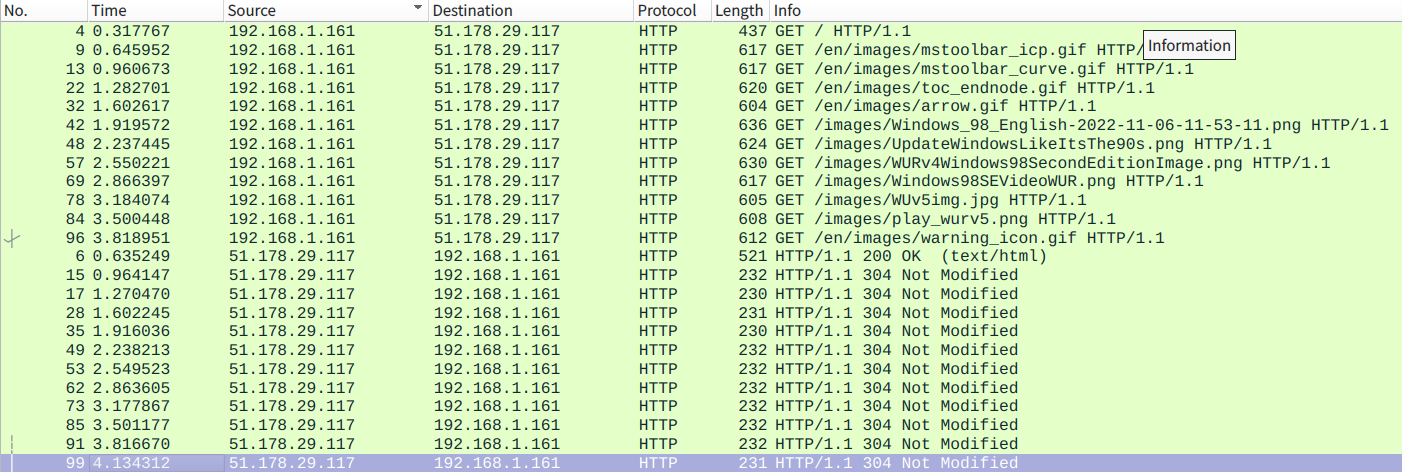


1. 捕捉及研究WWW应用的协议报文，回答以下问题：

a. .当访问某个主页时，从应用层到网络层，用到了哪些协议？

用到了HTTP（S）协议、TCP/IP协议

b. 对于用户请求的百度主页（[www.baidu.com](http://www.baidu.com)），客户端将接收到几个应答报文？具体是哪几个？假设从本地主机到该页面的往返时间是RTT，那么从请求该主页开始到浏览器上出现完整页面，一共经过多长时间？



因为百度强制HTTPS，只能捕捉到TLS包，所以这里使用支持明文HTTP的Windows Update Restored网站进行实验。

可以看到这里浏览器对/发起了请求（获取首页），发送了一系列请求获取资源（由于是刷新操作，所以浏览器已经知道HTML内容）。

收到了很多（12个）报文，具体是/地址的HTML内容和媒体资源。一共经过了大约4秒的时间。

c. 两个存放在同一个服务器中的截然不同的Web页（例如， http://www.gzhu.edu.cn/index.jsp，和http://www.gzhu.edu.cn/cn/research/index.jsp可以在同一个持久的连接上发送吗？

d. 假定一个超链接从一个万维网文档链接到另一个万维网文档，由于万维网文档上出现了差错而使超链接指向一个无效的计算机名，这时浏览器将向用户报告什么？

HTTP 404错误

e. 当点击一个万维网文档时，若该文档除了有文本外，还有一个本地.gif图像和两个远地.gif图像，那么需要建立几次TCP连接和有几个UDP过程？

1.若使用HTTP/1.0，需要建立0次UDP连接，4次TCP连接

2.若使用HTTP/1.1，需要建立0次UDP连接，1次TCP连接