

**桂 林 电 子 科 技 大 学**

计算机网络

实 验 报 告

实 验 名 称 实验四 TCP/UDP 协议分析

评语：

计算机与信息安全学院 学院

计算机科学与技术 专 业

**姓名 李嘉佳**

**学号 2000201916**

实 验 日 期 2022 年 11 月 17 日

成绩：

指导教师签名：

**一．实验目的**

1．

2．

3．

4．

5．

6．

加深理解 TCP 报文结构

领会 TCP 协议通信机制

通过跟踪 TCP 应用通信，能结合报文对整个通信过程进行分析 熟悉 UDP 协议报文结构

领会 UDP 协议通信机制

对比 TCP、UDP 协议主要特点

**二．实验环境**

1．

2．

3．

头歌基于 Linux 的虚拟机桌面系统

组网仿真工具 GNS3

浏览器 firefox

**三．相关原理或知识点**

1． TCP 首部格式

第 1 页 共 10 页

学生选课序号

实验项目序号

**4**

•

源端口( 16 位)：通信发送方使用的端口号

•

目标端口( 16 位)：通信接收方使用的端口号

•

序列号( 32 位)：用来确保数据可靠传输的唯一值

•

确认号( 32 位)：接收方在响应时发送的数值

•

数据偏移( 4 位)：标志数据包开始的位置，TCP 头部的长度

•

SYN：(同步)发起连接的数据包：同步 SYN=1 表示这是一个连接请求或连接接受报文。

•

ACK：(确认)确认收到的数据包：只有当 ACK=1 时，确认号字段才有效；当 ACK=0 时，

确认号无效。

•

RST：(重置)之前尝试的连接被关闭，(信号差，信号拥挤)：当 RST=1 时，表明 TCP 连

接中出现严重差错（如由于主机崩溃或其他原因），必须释放连接，然后再重新建立运

输连接。

•

FIN：(结束)连接成功，传输完毕之后，连接正在断开：用来释放一个连接，FIN=1 表明

此报文段的发送端的数据已发送完毕，并要求释放运输连接。

•

PSH：(推送)数据包直接发送给应用，而不是缓存起来：接收 TCP 收到 PSH=1 的报文

段，就尽快地交付接收应用进程，而不再等到整个缓存都填满了后再向上交付。

•

URG：(紧急)数据包中承载的内容应该立即由 TCP 协议栈立即进行处理：当 URG=1

时，表明紧急指针字段有效。它告诉系统此报文段中有紧急数据，应尽快传送(相当于高

优先级的数据)。

•

窗口大小( 16 位)：匹配缓存区的大小校验和( 16 位)：确认 TCP 数据段中的内容是否发

送了变化

•

紧急指针( 16 位)：明确显示数据之前的 16 进制序列号

2．

TCP 连接建立过程

TCP 连接建立过程，双方会产生三个报文，俗称三次握手。

1）. 第一次握手：

客户端将标志位 SYN 置为 1 ，随机产生一个值 SEQ = X，并将该数据包发送给服务

器，等待服务器确认；

2）. 第二次握手：

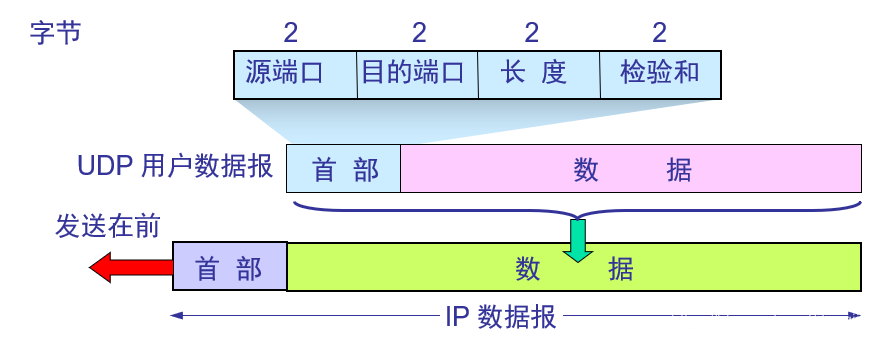
服务器收到数据包后由标志位 SYN = 1，知道客户端请求建立连接，服务器将标志位

SYN 和 ACK 都置为 1 ，ACK = X + 1，随机产生一个值 SEQ = Y，并将该数据包发

送给客户端以确认连接请求；

3）. 第三次握手：

第 2 页 共 10 页



客户端收到确认后，检查 ACK 是否为 X + 1，ACK 是否为 1 ，如果正确则将标志位

ACK 置为 1 ，ACK = Y + 1，并将该数据包发送给服务器，服务器检查

ACK 是否为 1 ，

如果正确则连接建立成功。

3．

TCP 连接关闭过程

TCP 连接关闭过程，双方通常会产生四个报文，俗称四次握手。有时 TCP 连接关闭时，只

能得到三个报文，这是因为第二次、第三次握手合并到一个报文里了。

1）. 第一次握手：

主动关闭方发送一个 FIN ，用来关闭主动方到被动关闭方的数据传送，也就是主动关

闭方告诉被动关闭方：我已经不会再给你发数据了(当然，在 FIN 包之前发送出去的数

据，如果没有收到对应的 ACK 确认报文，主动关闭方依然会重发这些数据)，但此时

主动关闭方还可以接受数据。

2）. 第二次握手：

被动关闭方收到 FIN 包后，发送一个 ACK 给对方，确认序号为:收到报文序号 Seq +

收到报文所携带数据长度 len+ 1 。上一个报文可能“捎带”了主动关闭方发送的最后一

块数据,其长度用字段 len 来表示。

3）. 第三次握手：

被动关闭方发送一个 FIN ，用来关闭被动关闭方到主动关闭方的数据传送，也就是告

诉主动关闭方，我的数据也发送完了，不会再给你发数据了。

4）. 第四次握手：

主动关闭方收到 FIN 后，发送一个 ACK 给被动关闭方，确认序号为：收到报文的序

号 Seq + 收到报文所携带数据长度 len+ 1 ，至此，完成四次挥手。

4．

UDP 的首部格式

•

源端口： 源端口号，需要对方回信时选用，不需要时全部置 0 ；

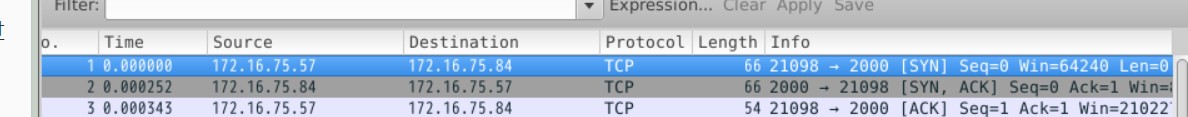
•

目的端口：目的端口号，在终点交付报文的时候需要用到；

•

长度：UDP 的数据报的长度（包括首部和数据）其最小值为 8（只有首部）。字段记录

第 3 页 共 10 页



了该 UDP 数据包的总长度（以字节为单位），包括 8 字节的 UDP 头和其后的数据部

分。最小值是 8（报文头的长度），最大值为 65535 字节；

•

校验和：检测 UDP 数据报在传输中是否有错，有错则丢弃。它的值是通过计算 UDP 数

据报及一个伪包头而得到的。校验和的计算方法与通用的一样，都是累加求和。

**四．实验任务**

1． 主机 A 上的某进程（这⾥称 A⽅）向主机 B 上的某进程（这⾥称 B⽅）请求建⽴TCP 连接，连 接建⽴后 A⽅向 B⽅发送⼀个⽂件，然后结束通信。A⽅的整个通信过程被 Wireshark 跟踪， 并记录在⽂件 send\_file\_by\_tcp.pcap 中。在报⽂列表窗⼝内，找到 TCP 建⽴连接时，所产

⽣的三个报⽂摘要，截图放到实验报告内。在实验报告内，结合具体的报⽂数据，分析三次 握⼿的过程。并且对数据包的相关信息进⾏计算；

2． ⽣成 UDP 报⽂，并使⽤Wireshark 抓取报⽂信息。在报⽂列表窗⼝中找到并选中刚刚⽣成的 UDP 报⽂，将报⽂摘要截图放到实验报告内，在报⽂解码窗⼝内，对当前报⽂报头信息进⾏ 截图（要求 UDP 头部展开），把它放到实验报告内，并分析各字段的含义。对⽐TCP、UDP 协

议，分析其主要特点，并记录到实验报告中。

**五．TCP 协议分析**

**1、TCP 连接建立过程分析**

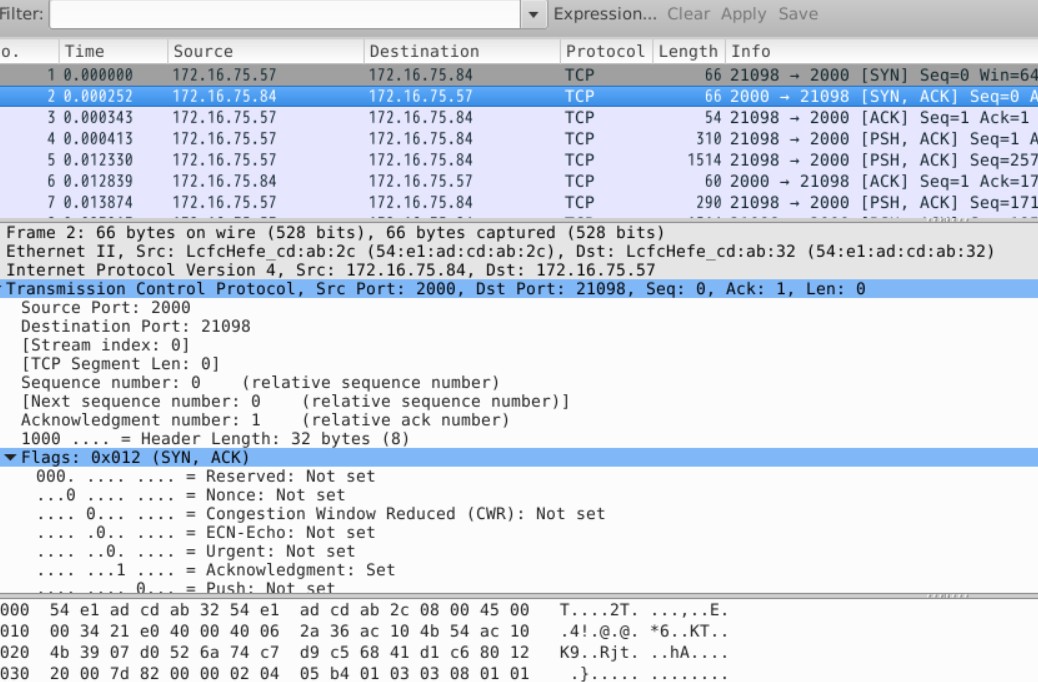
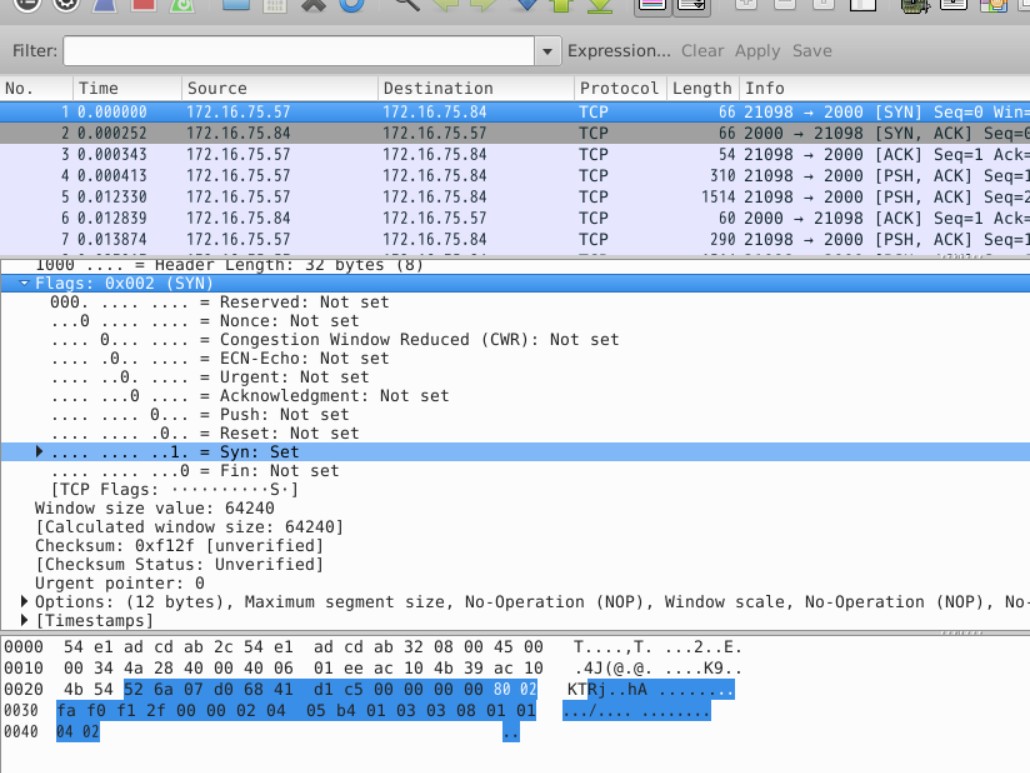
2、

3、Figure 1.1

三次握手建立 TCP 连接

第 4

页 共 10 页



4、

5、Figure 1.2 第一次握手的报文

6、客户端发送的 TCP 报文中标志位 SYN 置 1，初始序号 seq=x（随机选择）。Client 进入 SYN\_SENT

状态，等待 Server 确认。

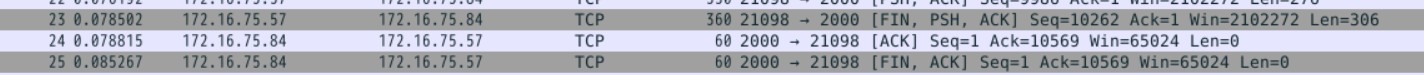
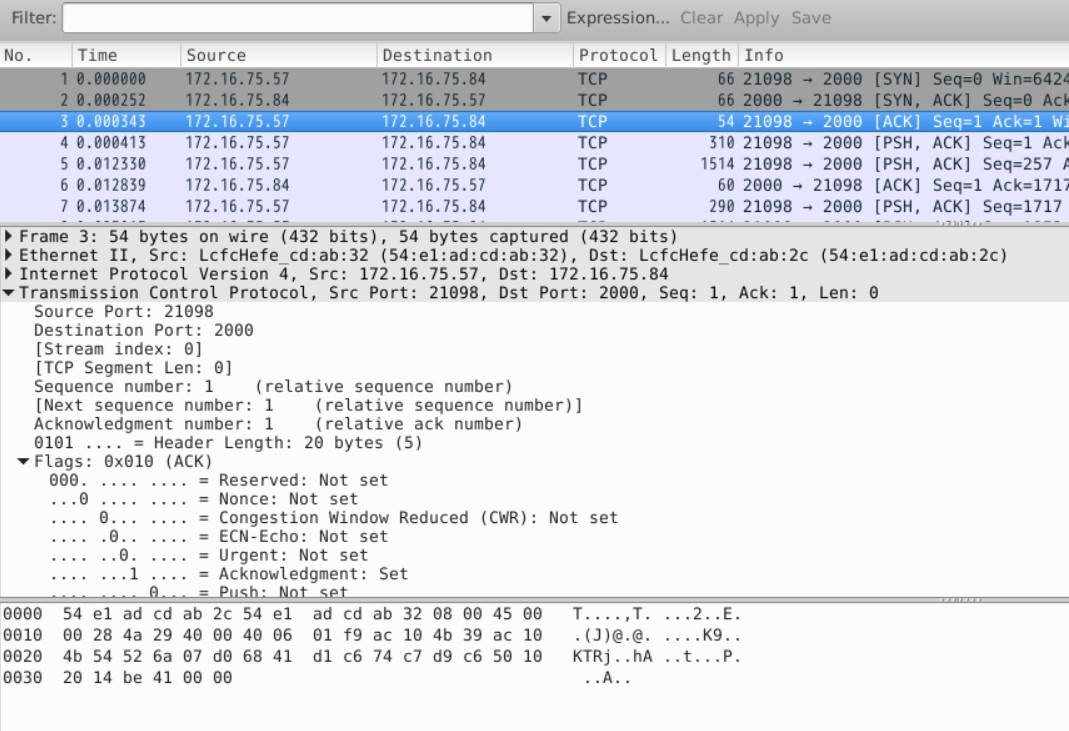
7、

8、Figure 1.3 第二次握手的报文

9、服务器收到数据包后，根据标志位 SYN=1 知道 Client 请求建立连接，Server 将标志位 SYN 和

ACK 都置为 1，ack=x+1，随机产生一个初始序号 seq=y，并将该数据包发送给 Client 以确认连接 请求，Server 进入 SYN\_RCVD 状态。

第 5 页 共 10 页



10、

11、Figure 1.4 第三次握手的报文

12、 Client 收到确认后，检查 ack 是否为 x+1，ACK 是否为 1，如果正确则将标志位 ACK 置为 1，

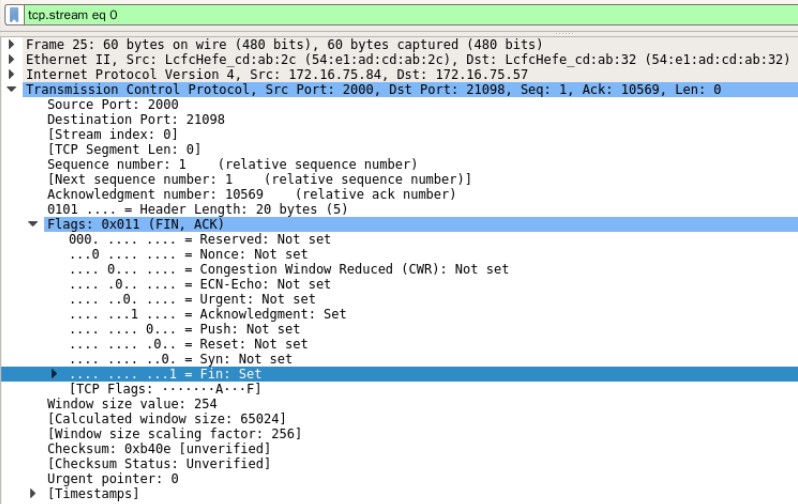
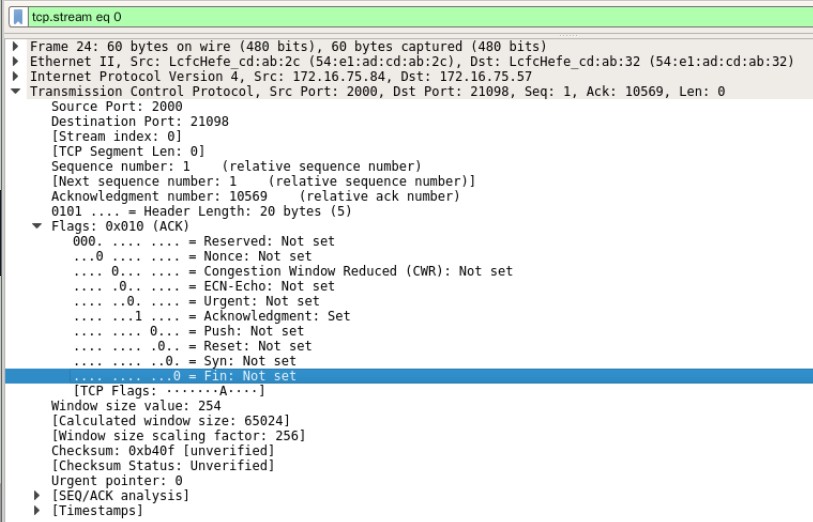
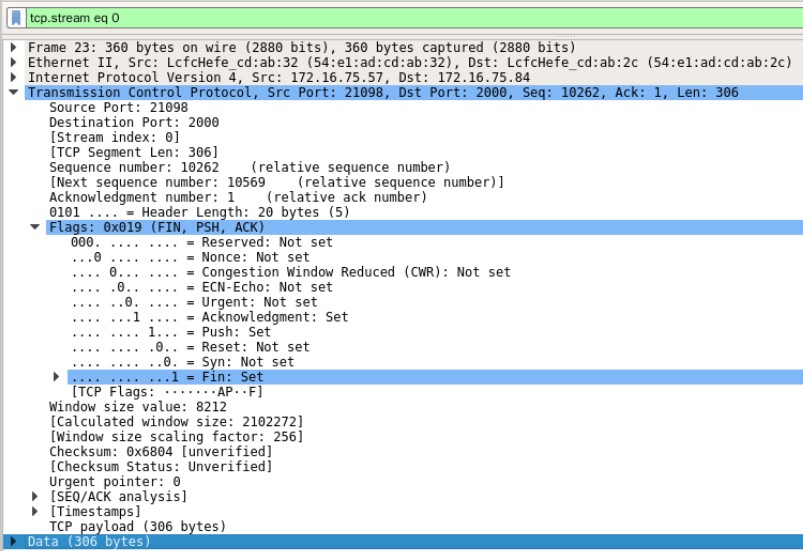
ack=y+1，并将该数据包发送给 Server。Server 检查 ack 是否为 y+1，ACK 是否为 1，如果正确则 连接建立成功，Client 和 Server 进入 ESTABLISHED 状态，完成三次握手，随后 Client 与 Server 之间可以开始传输数据了。

**13、TCP 关闭连接过程分析**

14、

*15***、**Figure 2.0 TCP 释放连接

第 6 页 共 10 页



16、

17、Figure2.1 第一次握手的报文

18、Client 发送一个 FIN，用来关闭 Client 到 Server 的数据传送，Client 进入 FIN\_WAIT\_1 状态。

19、

20、Figure 2.2 第二次握手的报文

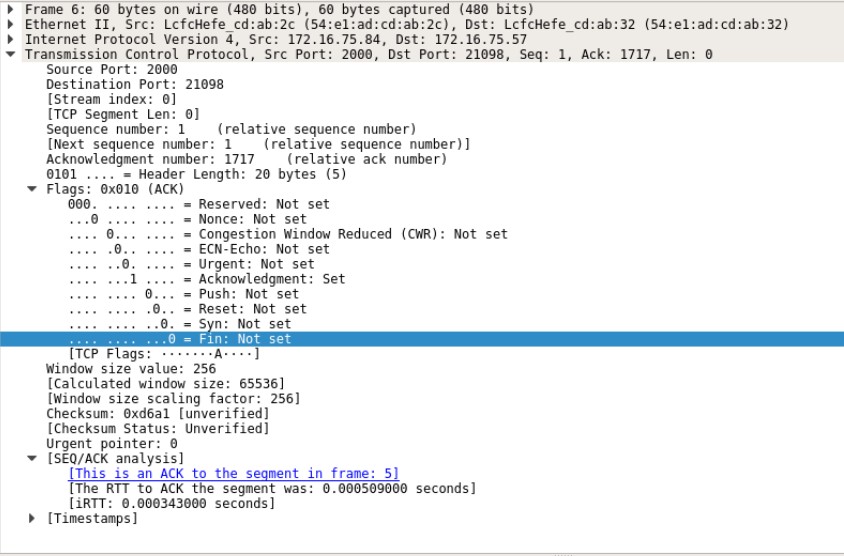
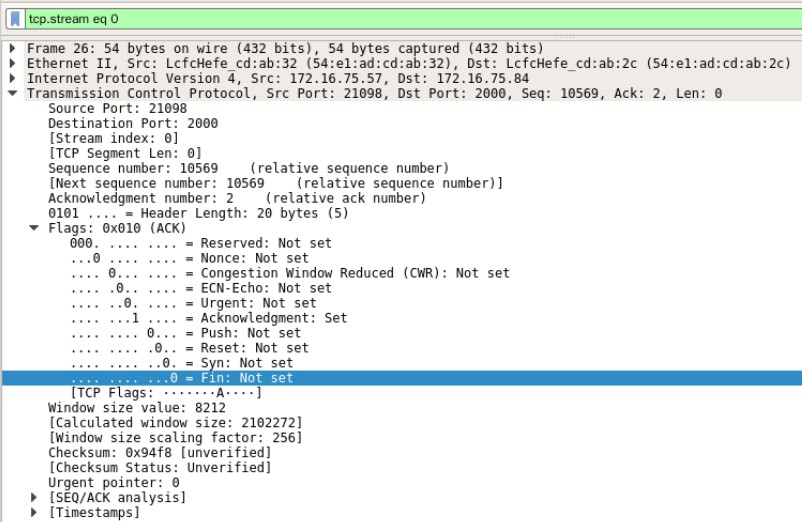
21、Server 收到 FIN 后，发送一个 ACK 给 Client，确认序号为 u + 1（与 SYN 相同，一个 FIN 占

用一个序号），Server 进入 CLOSE\_WAIT 状态。

22、

23、Figure 2.3 第三次握手的报文

第 7 页 共 10 页



24、Server 发送一个 FIN，用来关闭 Server 到 Client 的数据传送，Server 进入 LAST\_ACK 状态。

25、

26、Figure 2.4 第四次握手的报文

27、Client 收到 FIN 后，Client 进入 TIME\_WAIT 状态(主动关闭方才会进入该状态），接着发送一

个 ACK 给 Server，确认序号为 w + 1，Server 进入 CLOSED 状态，完成四次挥手。

**28、6 号报文分析**

29、

30、Figure 3.1 6 号报文

31、源端⼝为 2000，⽬的端⼝为 21098。报⽂序号为 1，确认序号为 1717。窗⼝⼤⼩为 65536。从

SEQ/ACK analysis 中我们可以得到 6 号报⽂对五号报⽂进⾏了确认。

**32、A 方 TCP 报文序列号分析**

**1．**

第 8 页 共 10 页

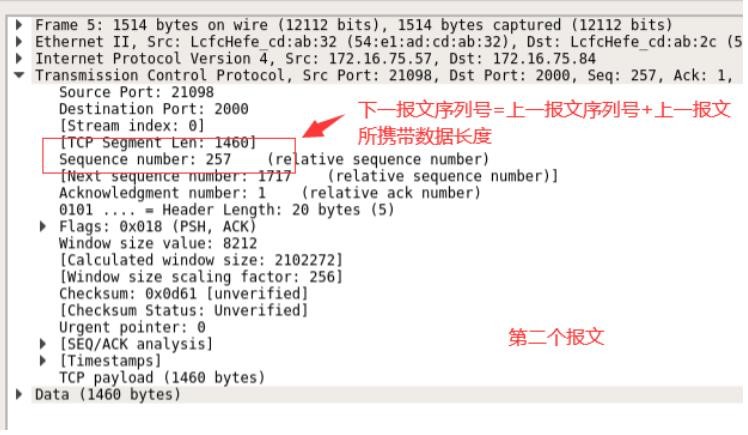
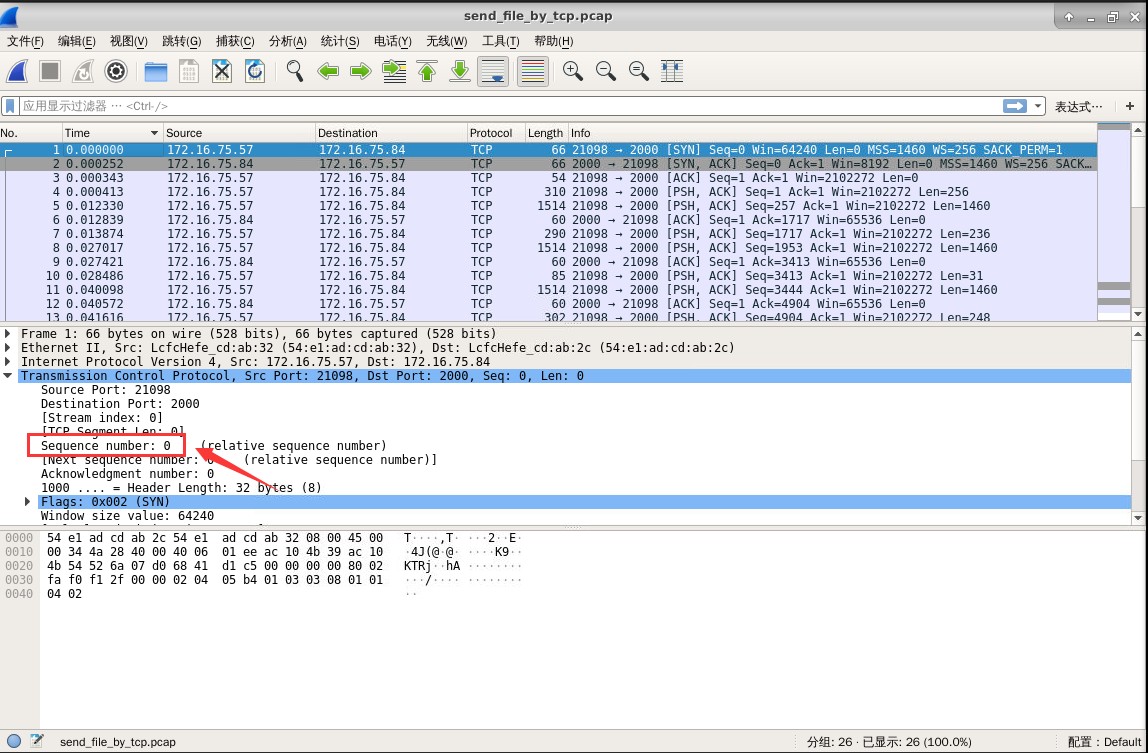


Figure 4.1 第一个报文

A 方第 1 个报文的序列号是 0

Figure 4.2 第二个报文

后一个报文的序列号=前一个报文的序列号+前一个报文的 len 长度，A 方所传文件的长度

为 9986 个字节

**33、计算**

1．

双⽅通信所⽤的时间：0.085306s

2．

所有帧的⻓度之和：将所有帧的 Length 相加：结果为 11497 字节

3．

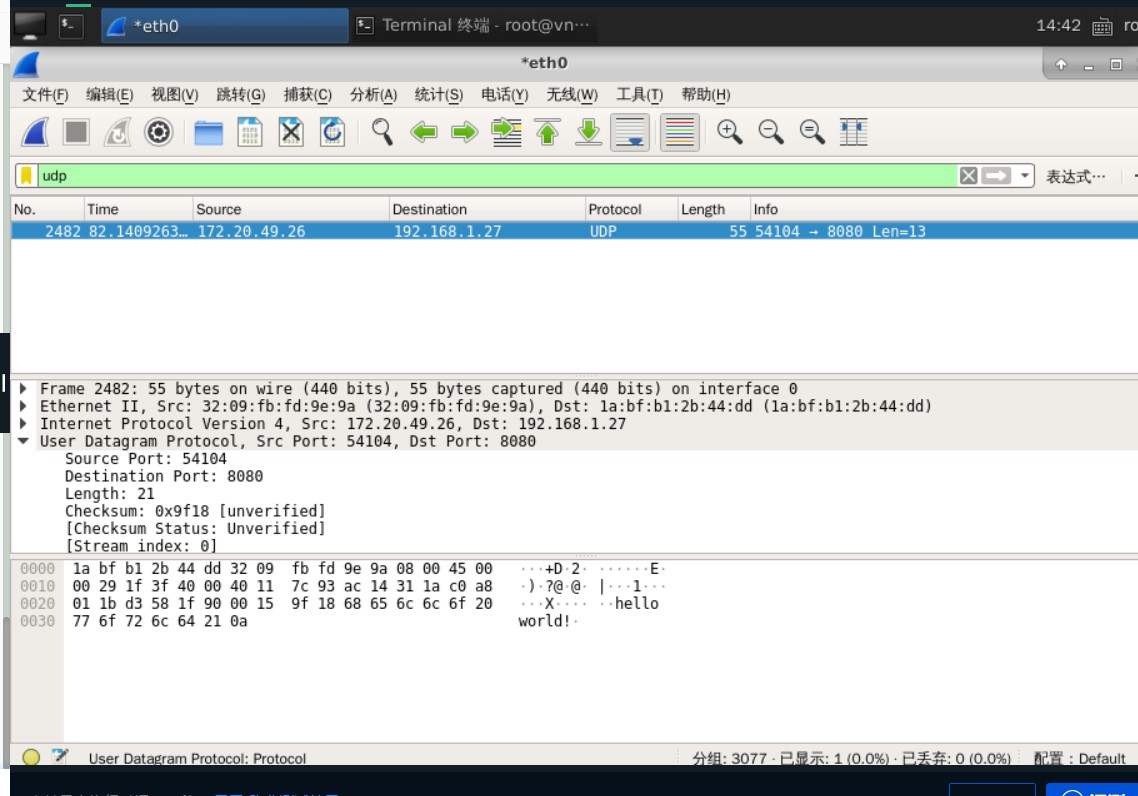
通信吞吐率：吞吐量计算公式为：帧长度除以通所用时间，得到 1.078Mbps

第 9 页 共 10 页

**七．实验总结**

<实验过程中遇到的问题及解决方法；实验过程体会；现存在的疑惑或问题>

1. 通过此次实验，我加深理解 TCP 报文结构的理解，并且能对TCP 协议通信机制有一定的认识。
2. 其次我还学会了通过跟踪 TCP 应用通信，能结合报文对整个通信过程进行分析，熟悉 UDP 协议报文结构的同时也领会 UDP 协议通信机制的独特之处。
3. 在学习的最后，我通过对比 TCP、UDP 协议主要特点，对TCP和UDP协议有了不一样的理解。



**六．UDP 协议分析**

**1、UDP 报文分析**

Figure 1.1 UDP 报文

使用 UDP 协议、源端口为：54104、服务器端口：8080、长度：21、校验和：0x9f18、校验

状态：Unverified、流序号：0

**2、分析 TCP、UDP 协议主要特点**

填写下表：

第 10 页 共 10 页

**序号**

**特性**

**TCP 协议的特点**

**UDP 协议的特点**

**1**

连接

面向连接

面向无连接

**2**

可靠性

高可靠

较可靠

**3**

实时性

一般

较好

**4**

网络开销

较大

较小

**5**

数据负载边界

面向字节流，以整个待传输的 数据为边界，保证数据正确性

基于数据报，以每段报文为边界，不保 证传输的数据顺序