**云南大学软件学院**

**实 验 报 告**

课程： 计算机网络实践 任课教师： 李海

姓名： 陈俊宏 学号： 20211060245 专业： 人工智能 成绩：



**实验四、TCP 协议分析实验报告**

1．实验目的：

理解TCP报文首部格式和字段的作用，TCP连接的建立和释放过程，TCP数据传输过程中编号与确认的过程；分析UDP协议报文格式。

2．实验环境：

连网环境，可以是局域网，也可以是连入Internet的单机。

3．实验步骤：

(1)启动Wireshark协议分析软件，并开始抓包。

(2)启动某个基于TCP的应用程序，例如连接某个FTP站点，或通过浏览器访问某个网页。

(3)等出现浏览的网页后停止数据包的捕获。

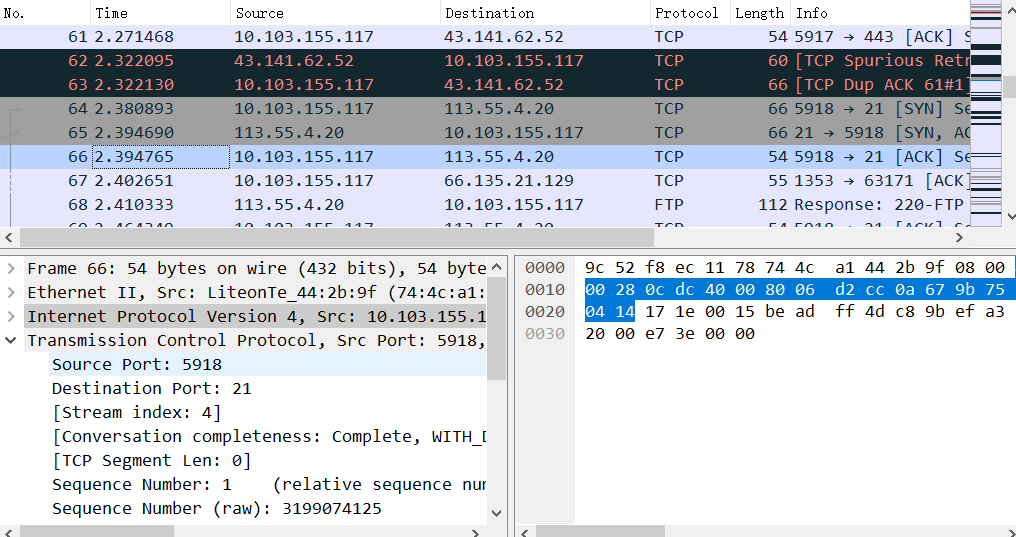
(4)出现协议分析界面，将filter 一栏填入tcp，则只显示TCP协议信息，通过此信息，可以看到TCP连接的三次握手过程和协商的初始的序列号，数据传输过程以及拆除连接的相应信息。

4．实验分析，回答下列问题

**（一） TCP协议分析**

**打开捕获文件**,通过捕获的数据包分析TCP建立连接的三次握手的过程，并将TCP建立连接过程中的三个报文填写下来。

|  |  |  |  |
| --- | --- | --- | --- |
| 字段名称 | 第一条报文 | 第二条报文 | 第三条报文 |
| 报文序号 | 64 | 65 | 66 |
| Sequence Number | 0 | 1 | 1 |
| Acknowedgement Numbber | 0 | 1 | 1 |
| ACK | 0 | 1 | 1 |
| SYN | 1 | 1 | 0 |



（1）TCP建立连接时的三个报文，其报文首部与其他TCP报文有什么不同？

答：

TCP建立连接时的三个报文分别是SYN、SYN-ACK和ACK。它们的报文首部与其他TCP报文有以下不同：

1、SYN报文首部：SYN标志位被设置为1，ACK标志位被设置为0，序列号用于初始化TCP发送端的序列号，而确认号被忽略。

2、SYN-ACK报文首部：SYN和ACK标志位都被设置为1，序列号用于初始化TCP接收端的序列号，而确认号用于确认TCP发送端对接收到的SYN报文的接收。

3、ACK报文首部：ACK标志位被设置为1，序列号被设置为接收到的SYN-ACK报文的确认号，而确认号被设置为接收到的SYN-ACK报文的序列号加1。

（2）报文首部的OPTION字段的作用是什么？值为多少？

答：

TCP报文首部中的OPTION字段用于传递TCP选项，它的作用是提供一些可选的功能或者对TCP协议进行扩展。

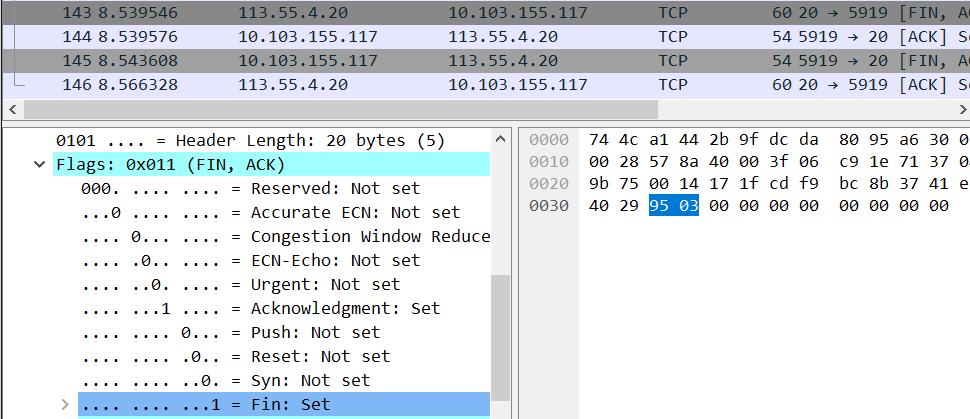
（3）分析TCP数据传输阶段的前8个报文，将报文信息填入到表中

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 报文序号 | 报文种类（发送/确认） | 序号字段 | 确认号字段 | 数据长度 | 被确认报文序号 |
| 66 | 发送 | 0 | 0 | 34字节 | 66 |
| 67 | 确认 | 1 | 1 | 34字节 | 67 |
| 68 | 确认 | 74 | 258 | 34字节 | 68 |
| 71 | 确认 | 1 | 1 | 40字节 | 71 |
| 72 | 确认 | 305 | 1 | 40字节 | 72 |
| 73 | 确认 | 1 | 306 | 34字节 | 73 |
| 74 | 确认 | 74 | 282 | 34字节 | 74 |
| 75 | 确认 | 1 | 306 | 34字节 | 75 |

数据传送阶段第一个报文的序号字段值是否等于连接建立时第三个报文的序号？

答：不等于。

(4)捕获一个拆除TCP连接的数据包,附上捕获截图,主要要包含拆除连接的数据包部分,分析TCP释放连接的过程，选择TCP释放连接过程当中的四个报文，将报文信息填在下表。



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名称 | 第一条报文 | 第二条报文 | 第三条报文 | 第四条报文 |
| 报文序号 | 163 | 164 | 165 | 166 |
| Sequence Number | 80 | 296 | 296 | 81 |
| Acknowedgement Numbber | 296 | 81 | 81 | 297 |
| ACK | 1 | 1 | 1 | 1 |
| FIN | 1 | 0 | 1 | 0 |

提示：打开捕获器—>打开DOS窗口—>输入：ftp 113.55.4.20 回车；—>在显示窗口中输入帐号：lihai\_std ,密码：std 回车；——>进入显示窗口输入dir; ——>输入quit——>停止捕获。如下图所示：



**（二）UDP协议分析**

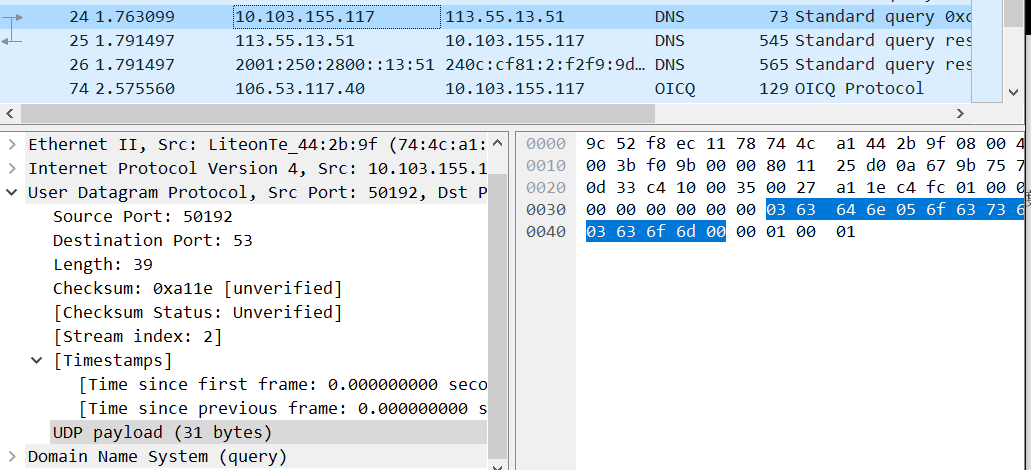
（1）请说明你是如何获得UDP的捕获文件，并附上捕获的截图。

答：(1)清空浏览器历史记录及缓存。

(2)启动Wireshark协议分析软件，并开始抓包。

(3)启动某个基于UDP的应用程序：通过浏览器访问某个网页。

(4)等出现浏览的网页后停止数据包的捕获。

(5)出现协议分析界面，将filter 一栏填入udp，则只显示UDP协议信息。

（2）通过捕获的数据包分析UDP的报文结构，将UDP协议树中各名字字段，字段长度，字段信息填入下表。

|  |  |  |  |
| --- | --- | --- | --- |
| 字段名 | 字段长度 | 字段值 | 字段表达信息 |
| Source Port | 2 Bytes | 50192 | 用来传输数据包的端口 |
| Destination Port | 2 Bytes | 53 | 数据报将要被传输到的端口 |
| Length | 2 Bytes | 39 | 数据报的字节长度 |
| Checksum | 2 Bytes | 0xa11e | 用来确保UDP首部和数据到达时的完整性 |
| UDP payload | 31 Bytes | c4 fc 01 00 00 01 00 00 00 00 00 00 03 63 64 6e 05 6f 63 73 6a 73 03 63 6f 6d 00 00 01 00 01 | 被UDP封装进去的数据，包含应用层协议头部和用户发出的数据 |

（3）通过和第一部分TCP的结果比较，UDP报文和TCP报文结构有何区别？

答：

UDP报文由源端口号、目的端口号、长度、检验和、应用数据报文五个部分组成。而TCP报文结构除此之外还有(1)32比特的序号字段（2）32比特的确认号字段 (3)16比特的接收窗口字段，用于流量控制（4）4比特的首部长度字段（5）可选与变长字段，用于发送方与接收方协商最大报文段长度（6）比特的标志字段，用于对已被成功接收报文段的确认。

（4）通过实验（一）和实验（二），总结TCP协议和UDP协议的不同之处。

答：

TCP协议是可靠的传输协议，具有流控制和拥塞控制，能够防止数据的丢失，还有确认重发机制保证数据的到达，应用于不允许数据丢失但对带宽无严格要求的服务。

UDP协议是不可靠的传输协议，无流控制和拥塞控制，是尽力服务机制，可最大程度的利用带宽，传输速率较快，应用于对带宽有严格要求但可以容忍数据丢失的服务。

**（三）总结实验过程中出现的问题,及解决方法。**

答：

1、在进行TCP报文的填写时，不确定哪些报文属于数据传输阶段，后来通过观察DOS窗口中的相同字节和字段描述，发现Request: LIST后的八个报文便是数据传输阶段的报文。

2、在进行TCP报文的填写时，不确定四次握手的开始在哪里，后来通过观察DOS窗口中的响应字段和字段描述，发现Response: 221 Goodbye!之后的四个报文便是四次握手的报文。

3、在进行UDP报文的填写时，UDP的报文结构不太熟悉，实验出现了困难，后来通过重新捕获和熟悉UDP报文结构，完成了实验。