实验六：UDP 与 TCP 协议分析

一、实验目的

1、理解 UDP 和 TCP 协议的基本原理；

2、理解 UDP 和 TCP 报文格式和各字段含义；

3、理解 TCP 协议的通信过程和状态变迁机制。

二、实验学时

2 学时

三、实验类型

验证型

四、实验需求

1、硬件

每人配备计算机 1 台。

2、软件

Windows 7 以上操作系统，安装 Wireshark 网络嗅探软件。

3、网络

实验室局域网支持，能够访问校园网。

4、工具

无。

五、实验理论

1、UDP 协议基本原理及其报文结构；

2、TCP 协议基本原理及其报文结构。

六、实验任务

1、完成 UDP 和 TCP 数据报文的采集；

2、完成 UDP 和 TCP 数据报文结构的分析；

3、完成 TCP 通信过程的报文分析。

七、实验内容及步骤

1、UDP 数据包分析

（1）获取数据报文

①打开 Wireshark，在【Filter】选项中输入报文过滤条件“udp”，选择【Start】，开始进行报文采集，如图 6-1 所示。

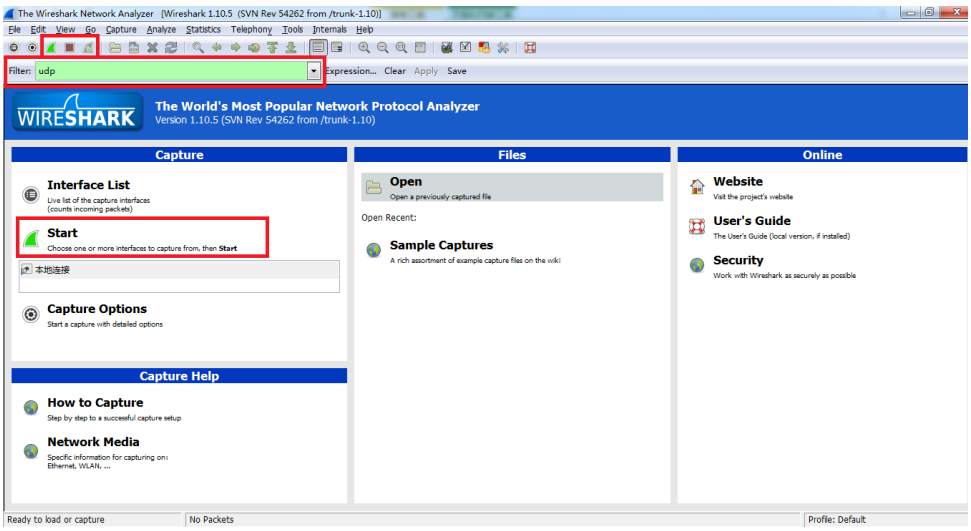

图 6-1 选择 UDP 协议

②在 Wireshark 的抓包窗体中，查看已获取的 UDP 数据报文，如图 6-2 所示。

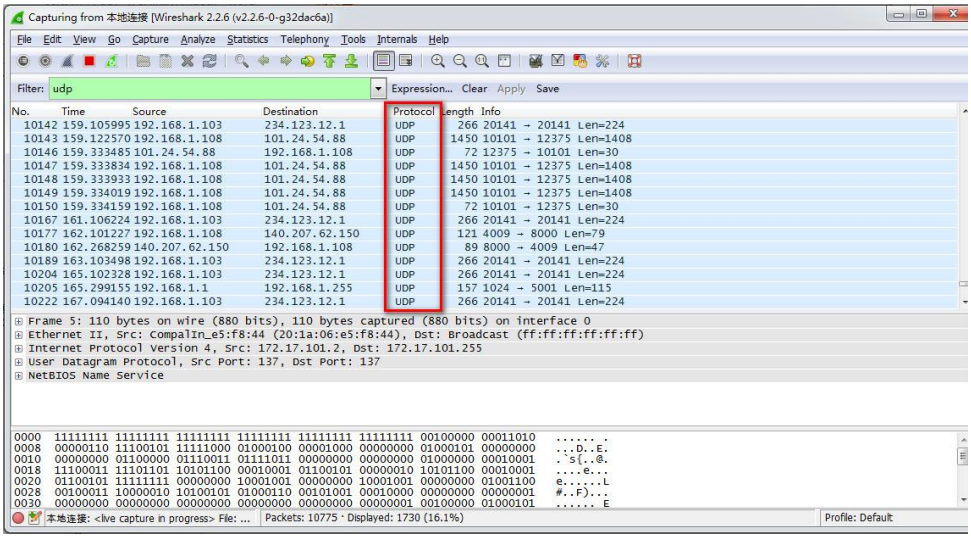

图 6-2 UDP 数据报文

（2）数据报文分析

从获取的 UDP 数据报文中任意选择其中一条数据报文，对该数据报文进行详细分析，并填写表 6-1。

表 6-1 UDP 协议报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Source Port		第 位		
2	Destination Port		第 位		
3	Length		第 位		
4	Checksum		第 位		

5	抓取数据包的详细内容：

2、TCP 数据包分析

（1）获取数据报文

①打开 Wireshark，在【Filter】选项中输入报文过滤条件“tcp”，选择【Start】，开始进行报文采集，如图 6-3 所示。

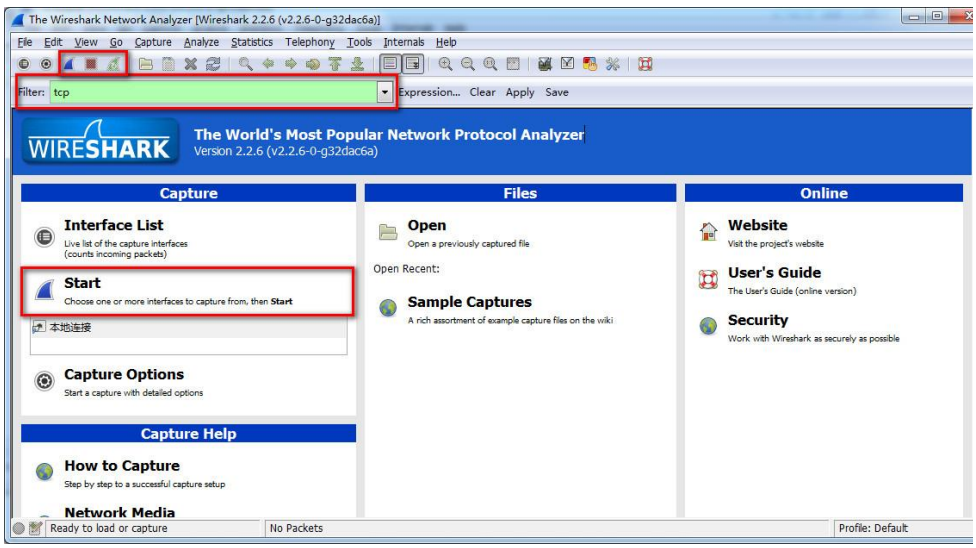

图 6-3 选择 TCP 协议

②在 Wireshark 的抓包窗体中，查看已获取的 TCP 数据报文，如图 6-4 所示。

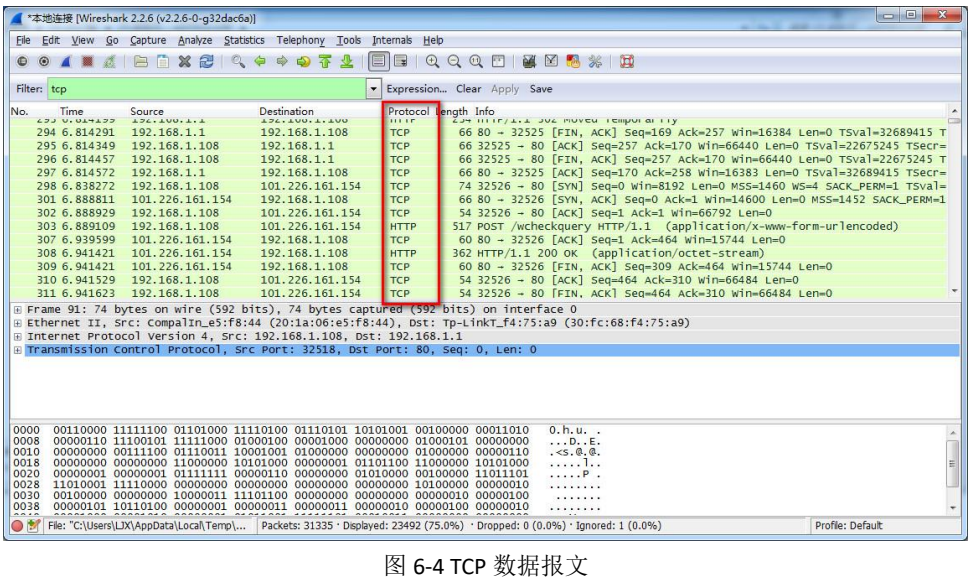

图 6-4 TCP 数据报文

（2）数据报文分析

从获取的 TCP 数据报文中任意选择其中一条数据报文，对该数据报文进行详细分析，并填写表 6-2。

表 6-2 TCP 协议报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Source Port		第　位		
2	Destination Port		第　位		
3	Sequence Number		第　位		
4	Acknowledgement Number		第　位		
5	Header Length		第　位		
6	Reserved		第　位		
7	Flags		第　位		
8	Window Size		第　位		
9	Checksum		第　位		
10	Urgent Pointer		第　位		
11	抓取数据包的详细内容：				

3、TCP 通信过程数据包分析

（1）TCP 建立连接报文分析

①获取建立连接报文。

a、打开 Wireshark，在【Filter】选项中输入报文过滤条件“tcp and ip.addr==192.168.1.103(本地主机 IP 地址)，选择【Start】，开始进行报文采集；

b、通过浏览器访问学校官网（http://www.hactcm.edu.cn），网站访问后，点击左上角红色按钮停止报文采集，如图 6-5 所示。

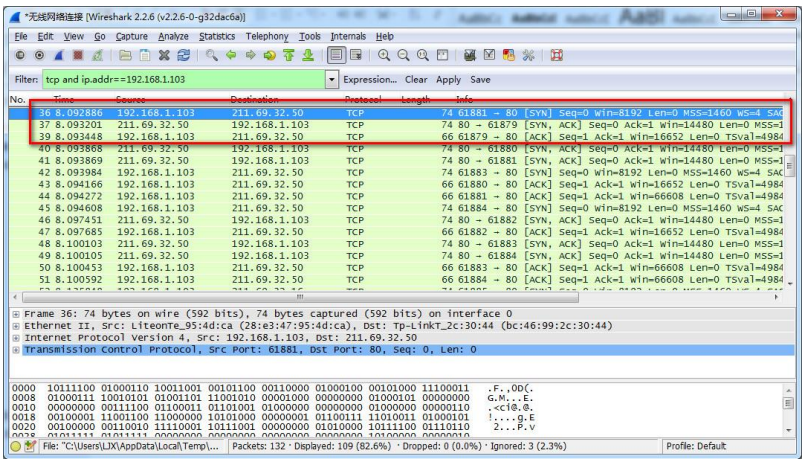

图 6-5 TCP 建立连接报文

②建立连接报文分析。

对抓取到的 TCP 报文进行分析，找到建立连接的三次握手机制所对应的报文，进行详细内容分析，并根据数据报文内容填写表 6-3。

表 6-3 TCP 建立连接报文分析

序号	字段名称	第一次	第二次	第三次	字段表示的信息
		字段值	字段值	字段值	
1	Source Port				
2	Destination Port				
3	Sequence Number				
4	Acknowledgement Number				
5	Header Length				
6	Reserved				
7	Flags				
8	Window Size				
9	Checksum				
10	Urgent Pointer				
11	抓取数据包的详细内容：				

（2）TCP 释放连接报文分析

①获取释放连接报文。关闭浏览器后，由于长时间未进行连接，将进行释放该 TCP 连接操作，可通过 Wireshark 网络分析工具，获取释放 TCP 连接的数据报文如图 6-6 所示。

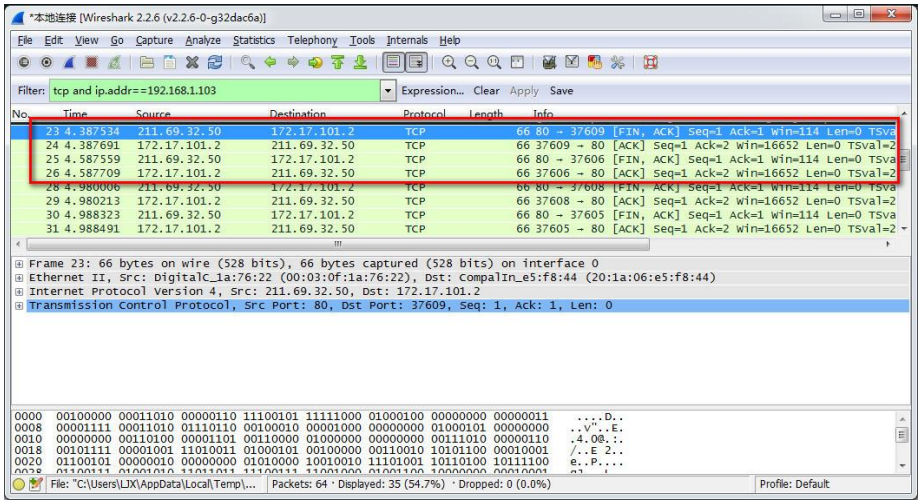

图 6-7 TCP 释放连接报文

②释放连接报文分析。

对抓取到的 TCP 报文进行分析，找到释放连接所对应的数据报文，进行详细内容分析，并根据数据报文内容填写表 6-4。

表 6-4 释放连接报文分析

序号	字段名称	第一次	第二次	第三次	第四次	字段表示的信息
		字段值	字段值	字段值	字段值	
1	Source Port					
2	Destination Port					
3	Sequence Number					
4	Acknowledgement Number					
5	Header Length					
6	Reserved					
7	Flags					
8	Window Size					
9	Checksum					
10	Urgent Pointer					
11	抓取数据包的详细内容：					

（3）对比分析

根据 TCP 建立连接和释放连接的报文结构，比较两个过程数据报结构的 6 个关键差别，并填写表 6-5。

表 6-5 TCP 通信过程报文对比分析

序号	字段名称	请求连接报文		释放连接报文	
		字段值	字段表示信息	字段值	字段表示的信息
1					
2					
3					
4					
5					
6					
7	对比描述详细内容：				

八、实验分析

1、UDP 报文和 TCP 报文结构有何区别？

（1）UDP 报文和 TCP 报文结构上有什么不同？

（2）UDP 协议和 TCP 协议的不同之处是什么？

2、如何找到欲分析的数据报文？

（1）网络抓包时如何找到指定协议的数据报文？

（2）网络抓包时如何找到指定来源和目的地址的数据报文？

（3）网络抓包时如何找到指定套接字的数据报文？

（4）如何从众多的 TCP 数据报文中找到建立连接和释放连接的数据报文？

3、聊天工具使用的传输协议

（1）使用 TCP 传输协议的聊天工具有哪些，使用 UDP 传输协议的聊天工具有哪些？

（2）QQ 软件发送消息和发送文件使用的传输协议是否一样？分别是什么？

（3）软件开发者在开发软件时如何选取软件使用的传输协议？