《计算机网络》实验指导

# 实验四：UDP 与 TCP 协议分析

## 一、实验目的

1、理解 UDP 和 TCP 报文首部格式和字段的作用；

2、理解 UDP 数据报的传输过程；

3、理解 TCP 连接的建立和释放过程，以及 TCP 数据报传输过程中编号与确认的过程；

4、掌握 WinPcap 和 Wireshark 软件的安装和使用方法，并能够使用 Wireshark 对 UDP 和 TCP 数据包进行抓取和分析。

## 二、实验学时

2 学时

## 三、实验类型

验证性

## 四、实验需求

**1、硬件**

每人配备计算机 1 台，计算机接入实验室局域网。

**2、软件**

Windows 7 操作系统。

**3、网络**

支持对互联网的访问。

**4、工具**

无

## 五、实验理论

1、UDP、TCP 协议；

2、网络嗅探工具的工作原理。

## 六、预备知识

1、UDP 和 TCP 报文结构；

> 要求：
> 请绘制出 UDP 和 TCP 的报文结构，并填写到实验报告册中。

2、WinPcap 和 Wireshark 软件的基本工作原理与使用方法；

3、请查阅资料，列举几种常见的网络分析工具，并填写表 4-1 网络分析工具对比分析一览表。

表 4-1 网络分析工具对比分析一览表

| 序号 | 软件名称 | 版本号 | 软件开发商 | 安装环境 |
|---|---|---|---|---|
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |
| 4 | | | | |
| 5 | | | | |
| … | | | | |

要求：

请查阅资料完成表 4-1 的具体内容，并将结果填写到实验报告册中。

## 七、实验任务

1、完成 WinPcap 和 Wireshark 软件的安装；

2、完成 UDP 和 TCP 报文的采集；

3、完成 UDP 和 TCP 报文结构的分析；

4、完成 UDP 和 TCP 通信过程的分析。

## 八、实验内容及步骤

### 1、WinPcap 和 Wireshark 的安装与使用

（1）获得软件

WinPcap 是针对 Windows 32 位平台上的抓包和网络分析的一个架构，是 Windows 平台下免费、公共的网络访问系统。它包括一个核心态的包过滤器，一个底层的动态链接库（packet.dll）和一个高层的不依赖于系统的库（wpcap.dll）。

Wireshark 是一个网络数据包分析软件。该软件的功能是截取网络数据包，并尽可能显示出最为详细的网络数据包数据。开发者可以使用 Wireshark 来为新的通信协议除错，普通用户可以使用 Wireshark 来学习网络协议的相关知识。

WinPcap 的官方地址：http://www.winpcap.org

Wireshark 的官方地址：http://www.wireshark.org

上述两个软件，也可以通过课程网站（http://ke.51xueweb.cn/Network.html）获得。

（2）安装 Wireshark

直接运行 Wireshark 软件包，即可安装该软件。在安装过程中，将默认安装 WinPcap，按照软件安装的提示，完成软件安装。

（3）启动 Wireshark，进行数据包抓取

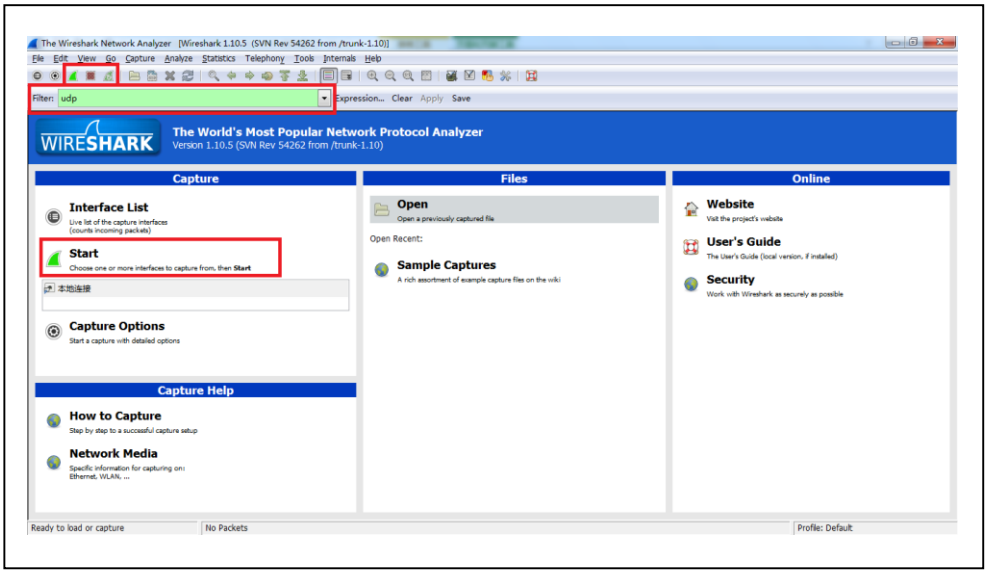
WinPcap 是一个框架软件，因此用户不需要对该软件进行操作。

若开始进行网络通信分析，可通过启动 Wireshark 进行。

## 2、UDP 数据包分析

（1）创建 UDP 协议的抓包任务

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，选择左上角红色按钮停止报文采集。如图 4-1 所示。




（2）对数据包进行分析

在 Wireshark 的抓包窗体中，可以发现整个软件分为三个区域，如图 4-2 所示。上部分为抓取的数据包，中间部分为数据详细分析，下部分为数据包的内容。

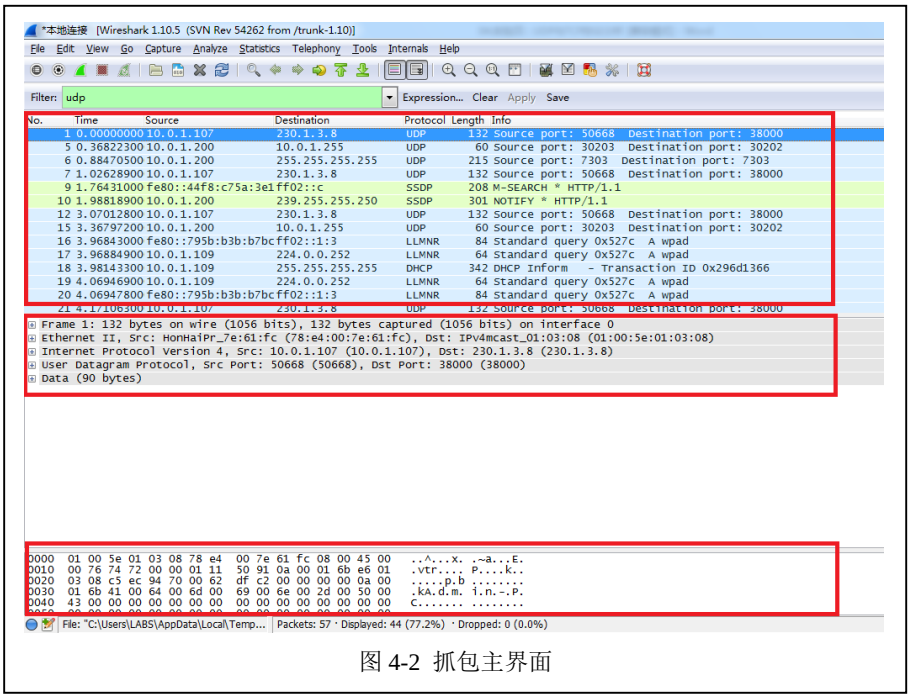



图 4-2 抓包主界面

（3）在上部分区域中选择其中的一条内容，对该数据包进行详细的分析。并填写表 4-2。

**表 4-2 UDP 协议分析**

| 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： | | | | |
| | | | | | |

**要求：**

请按照上述要求进行抓包和数据包分析，完成表 4-2 的填写，并将分析结果填写到实验报告册中。

### 3、TCP 数据包分析

（1）创建 TCP 协议的抓包任务

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，选择左上角红色按钮停止报文采集。如图 4-3 所示。

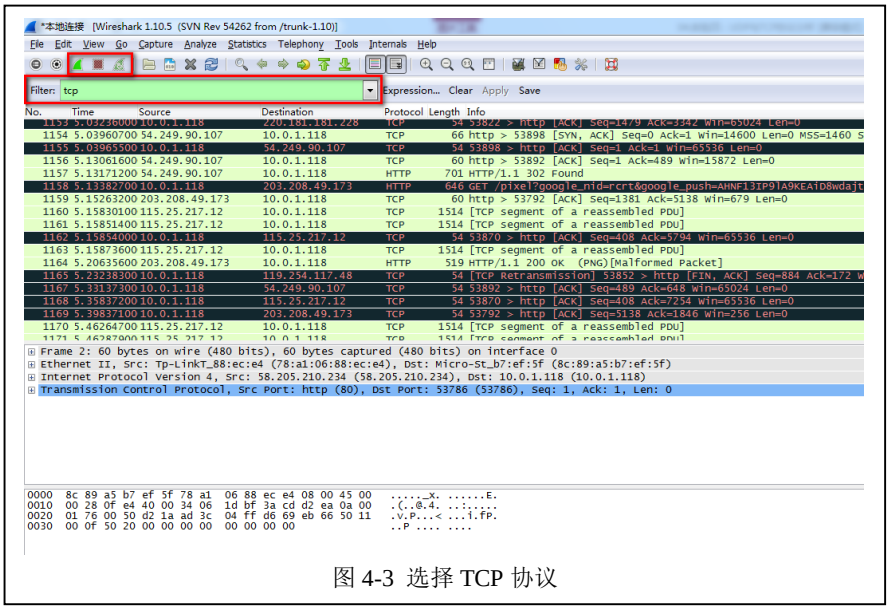



图 4-3 选择 TCP 协议

（2）对数据包进行分析

在 Wireshark 的抓包窗体中，选择一条数据进行详细分析，并填写表 4-3。

**表 4-3 TCP 协议分析**

| 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： | | | | |
| | | | | | |

要求：
请按照上述要求进行抓包和数据包分析，完成表 4-3 的填写，并将结果填写到实验报告册中。

## 九、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？

要求：
请回答上述 2 个问题，并将答案填写到实验报告册中。

## 十、课外自主实验

**1、通过抓包分析 TCP 建立连接和断开连接的过程**

（1）设计一个抓包实验，对 TCP 建立连接和断开连接过程中的数据包进行记录；

（2）通过数据分析，说明 TCP 建立连接和断开连接的过程。

要求：
1、请按照（1）的要求完成该实验的设计，并将具体实验步骤填写到实验报告册中。

2、请按照（2）的要求完成实验结果分析，用实验结果说明 TCP 建立连接和断开连接的过程，并将分析结果填写到实验报告册中。

**2、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？

要求：

1、请查阅相关资料，回答（1）(3）2 个问题，并将答案填写到实验报告册中。

2、请按照（2）的要求设计实验，通过数据包抓取的方式进行分析，以说明两种信息传输所使用的传输协议。并将具体的实验设计、实验步骤以及实验结果分析填写到实验报告册中。

**3、网络分析工具：tcpdump**

（1）了解 tcpdump 的详细信息；

（2）学习在 Linux & Unix 系统下 tcpdump 工具的具体使用方法；

（3）通过 tcpdump 工具完成本实验中的实验内容。

## 十一、实验扩展资源

**1、图书**

（1）网络协议分析与实现 胡维华 高等教育出版社

（2）网络协议教程 陈明 清华大学出版社

（3）TCP/IP 详解 Gary.Wrigh W.Richard Stevens 机械工业出版社

（4）TCP/IP 协议深入分析 徐宇杰 清华大学出版社

**2、文章**

（1）UDP 协议与 TCP 协议的对比分析与可靠性改进 赵飞 叶震 《计算机技术与发展》2006 年 09 期

（2）容迟网络中的 TCP 性能分析 雷仕英 王磊 侯维娜 《2009 年全国无线电应用与管理学术会议论文集》 2009 年

（3）CDP-基于 UDP 的 TCP 协议实现 赵丽玲 《电脑知识与技术（学术交流）》 2007 年 03 期

（4）基于 UDP 协议的视频图像传输的研究与实现 王军 吕海宝 许国梁 《现代计算机（专业版）》 2002 年 09 期

**3、互联网资源**

（1）协议分析网：http://www.cnpaf.net/Class/ProtocolAll/

（2）网易公开课：

http://c.open.163.com/coursera/courseIntro.htm?cid=105&tabNoJmp=1#/courseIntro

（3）Wireshark 官方文档：http://www.wireshark.org/docs/

（4）科来网络分析系统：http://www.colasoft.com.cn/products/capsa.php

**4、电子资源下载**

课程网站：ke.51xueweb.cn/Network.html