华东师范大学软件工程学院实验报告

实验课程：计算机网络实践	**年级**：2023 级	**实验成绩**：
实验名称：UDP	**姓名**：顾翌炜	
实验编号：Lab-5	**学号**：10235101527	**实验日期**：2024/12/20
指导教师：王廷	**组号**：01	**实验时间**：2024/12/20

1 实验目的

1) 学习使用 Wireshark 抓取 UDP 数据包
2) 理解 UDP 数据包的结构
3) 熟悉 UDP 数据包中各个字段的含义
4) 掌握 UDP 协议的应用场景

2 实验内容与实验步骤

2.1 实验内容

1) 学会通过 Wireshark 获取 UDP 消息
2) 掌握 UDP 数据包结构
3) 掌握 UDP 数据包各字段的含义
4) 了解 UDP 协议适用领域

2.1.1 获取 UDP 消息

打开 Wireshark，在“捕获”菜单中选择“选项”，配置以太网接口，设置捕获过滤器为 udp，并关闭混杂模式。

点击“开始”按钮,使用浏览器访问一个网站,如 www.baidu.com,或在命令行中输入 nslookup www.baidu.com 查询 DNS 服务器。如果 DNS 解析失败，可以在命令行中输入 ipconfig /flushdns 清除 DNS 缓存。(使用 ipconfig /displaydns 可以在 Windows 系统中查看当前的 DNS 缓存)

完成捕获后，点击“停止”按钮。

2.1.2 分析 UDP 包

选择一个数据帧，分析其 UDP 包头字段。
回答以下问题:

1) What does the Length field include? The UDP payload, UDP payload and UDP header, or UDP payload, UDP header, and lower layer headers?

2) How long in bits is the UDP checksum?

3) How long in bytes is the entire UDP header?

打开命令行界面，输入 ipconfig 以获取计算机的 IP 地址，并将其与数据包中的 Source Port 进行比较。
回答以下问题：

1) Give the value of the IP Protocol field that identifies the upper layer protocol as UDP.

2) Examine the UDP messages and give the destination IP addresses that are used when your computer is neither the source IP address nor the destination IP address. (If you have only your computer as the source or destination IP address then you may use the supplied trace.)

3) What is the typical size of UDP messages in your trace?

2.1.3 问题讨论

We encourage you to keep exploring on your own, but there is not much more to UDP.

Instead, you might examine the traffic of UDP-based applications to look at packet sizes and loss rates. Voice-over-IP and its companion protocols like RTP (Real-Time Protocol) are good candidates.

Similarly, you might explore streaming and real-time applications to see which use UDP and which use TCP as a transport.

2.2 实验步骤

1) 启动 Wireshark，在“捕获”→“选项”中进行设置，选择已连接的以太网接口，将捕获过滤器设置为 udp，并关闭混杂模式，然后开始捕获。
2) 在命令行中输入 nslookup www.baidu.com 查询 DNS 服务器

```
1                    PS> nslookup www.baidu.com
```

3) 在 Wireshark 中停止捕获。
4) 对捕获到的 UDP 数据包进行分析，并回答相关问题。
5) 讨论问题

3 实验环境

- 操作系统：Windows 11 家庭中文版 23H2 22631.4460
- 网络适配器：Killer(R)Wi-Fi 6E AX1675i 160MHz Wireless Network Adapter(211NGW)
- Wireshark：Version 4.4.1
- wget：GNU Wget 1.21.4 built on mingw32

4 实验结果与分析

4.1 获取 UDP 消息

打开 Wireshark，在菜单栏的捕获的选项中进行设置，选择已连接的以太网，设置捕获过滤器为 udp，关闭混杂模式。

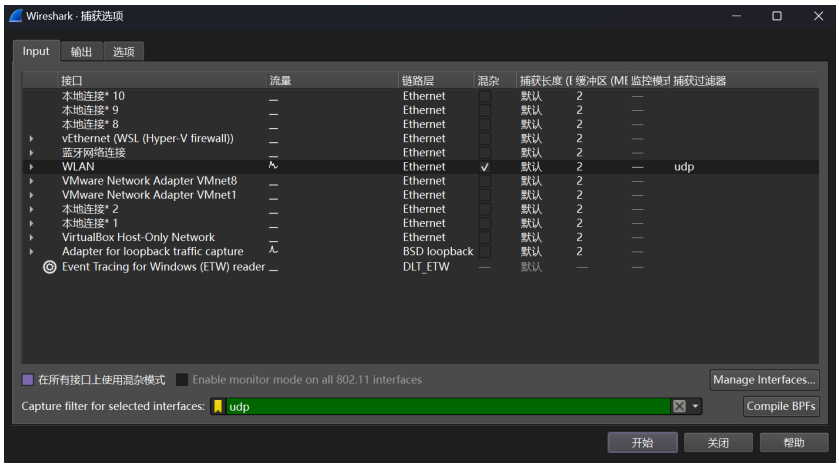

图 1: 设置捕获

开始捕获，在 cmd 中输入 nslookup www.baidu.com 查询 DNS 服务器

图 2: 查询 DNS 服务器

得到的捕获结果如下所示：

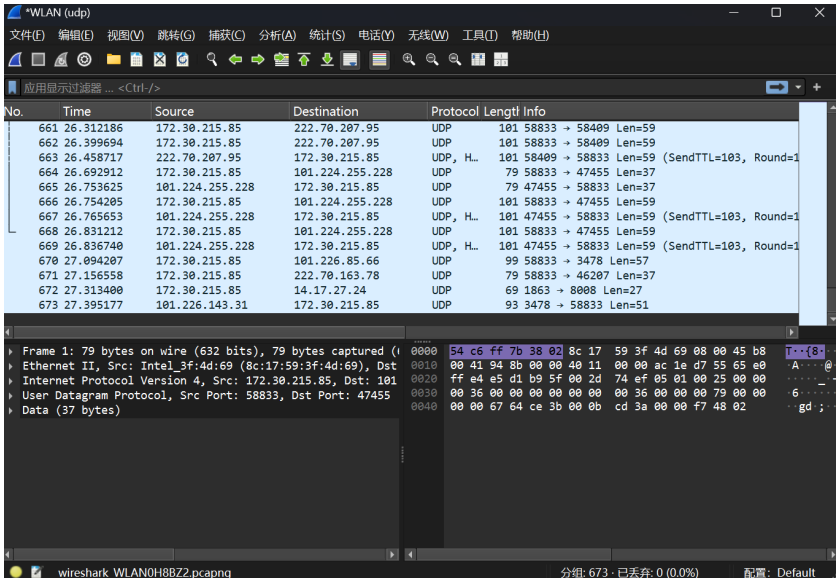

图 3: 捕获结果

由此，捕获 UDP 的部分就结束了。

4.2 分析 UDP 包

从捕获结果中选择一个数据帧，分析其 UDP 包头字段。

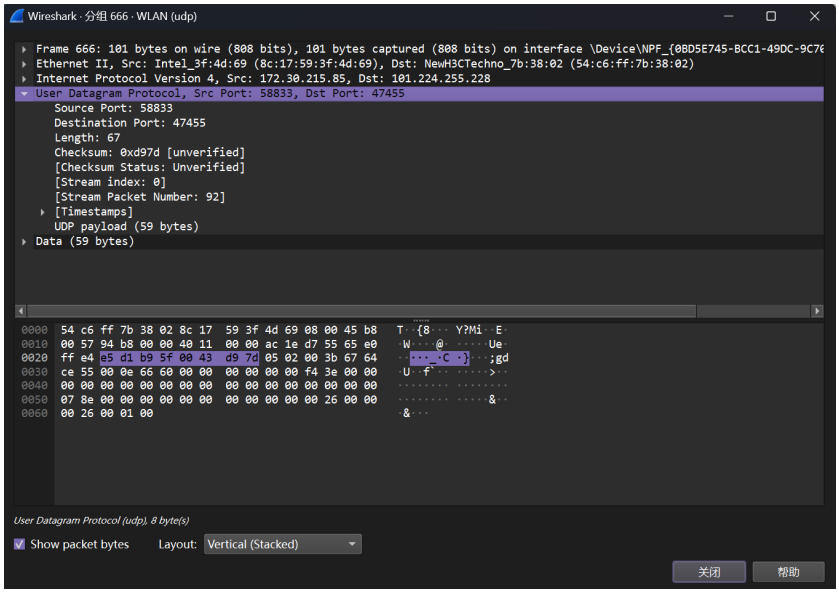

图 4: UDP 包

来看 UDP 包的每一个部分：

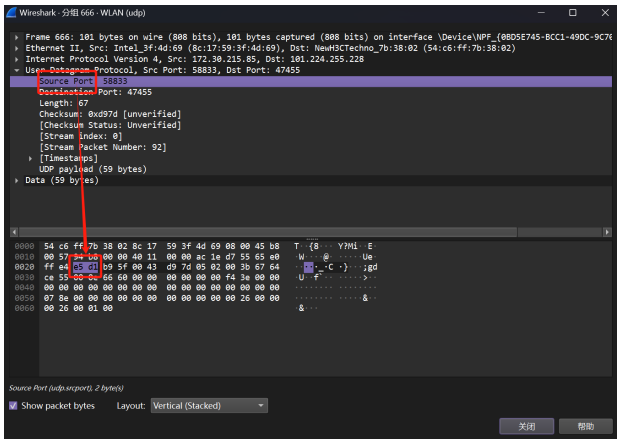

图 5: Source Port

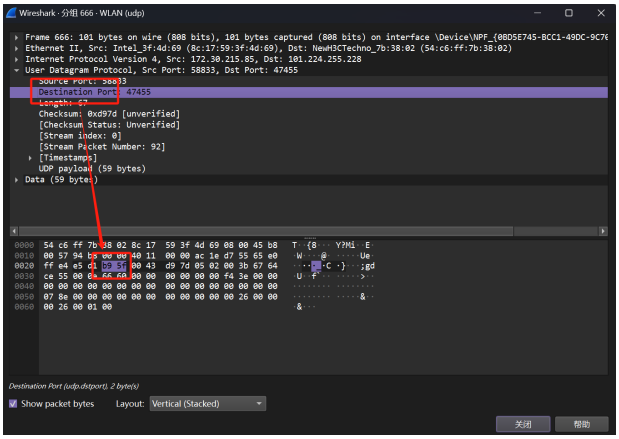

图 6: `Destination Port`

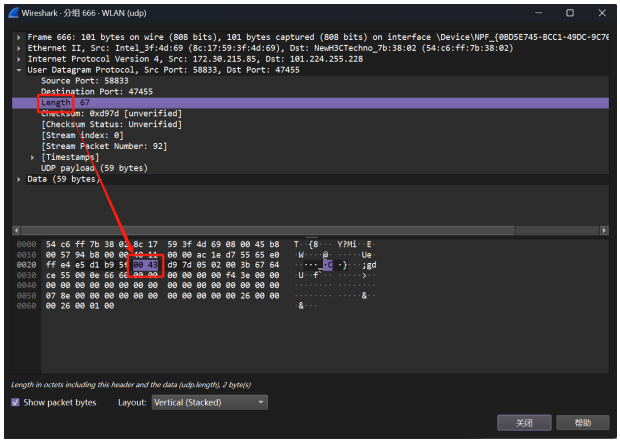

图 7: Length

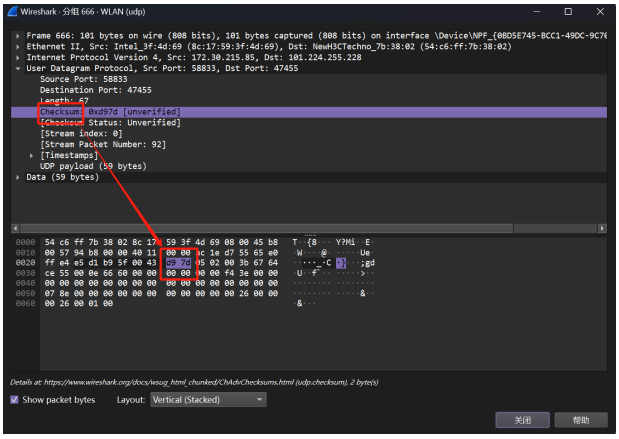

图 8: `Checksum`

由此可以画出 UDP 包的结构如下：

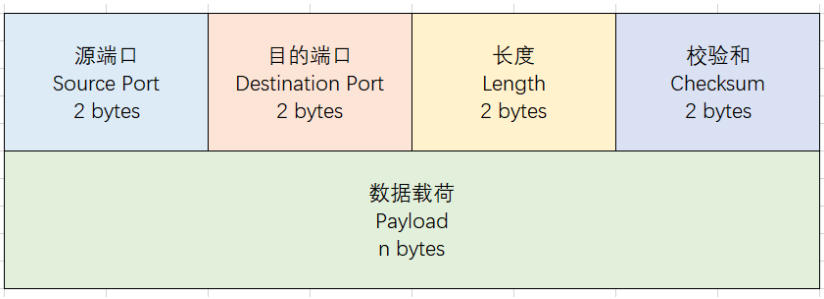

图 9: UDP 包的结构

4.3 回答问题

1) What does the Length field include? The UDP payload, UDP payload and UDP header, or UDP payload, UDP header, and lower layer headers?

   在上面分析的 UDP 包中，Payload 长度为 59 字节，UDP 头长度为 8 字节，而 Length 字段的值为 67。因此可以得出 UDP 数据报头中的 Length 字段指的是 UDP 的 payload 长度加上 UDP 头的总长度。

2) How long in bits is the UDP checksum?

   UDP 头中的 checksum 的长度是 16 位。

3) How long in bytes is the entire UDP header?

   整个 UDP 头的长度是 8 字节。

打开命令行界面，输入 `ipconfig` 以获取计算机的 `IP` 地址，并将其与数据包中的 `Source Port` 进行比较。可以看到我的 ip 地址是：

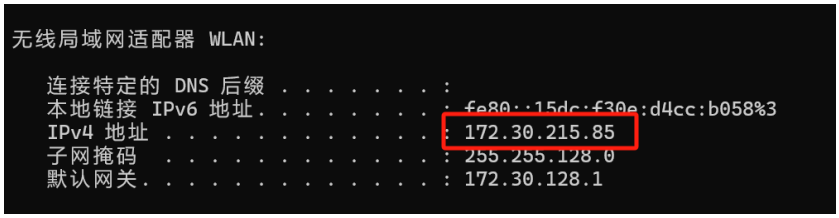

图 10: IP 地址

可以看到我的 ip 地址是 `172.30.215.85`，与数据报中的 Source Port = 58833 相同，与数据报中的 Destination Port = 47455 不同

回答以下问题：

1) Give the value of the IP Protocol field that identifies the upper layer protocol as UDP.

在 IP 协议中，Protocol 字段指出需要交给上一层的 UDP 传输进程，该字段值为 17。

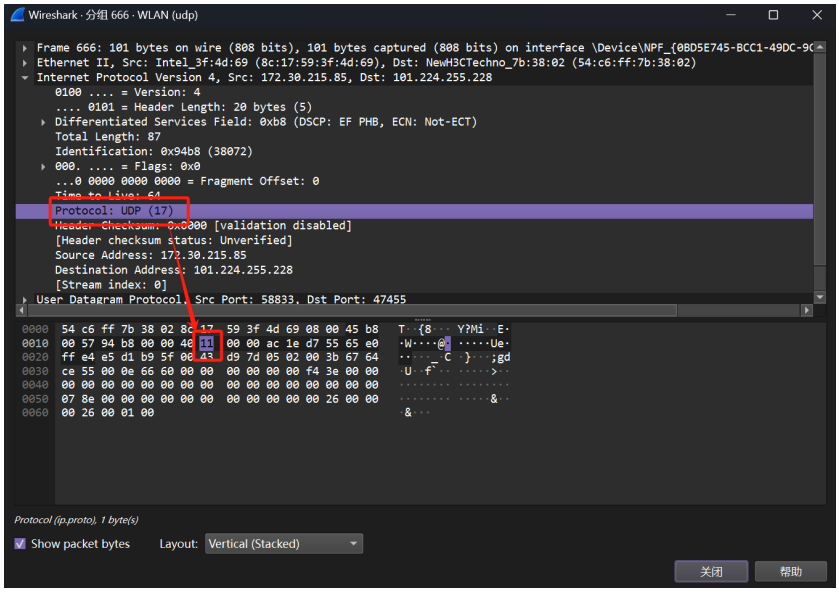

图 11: Protocol

2) Examine the UDP messages and give the destination IP addresses that are used when your computer is neither the source IP address nor the destination IP address. (If you have only your computer as the source or destination IP address then you may use the supplied trace.)

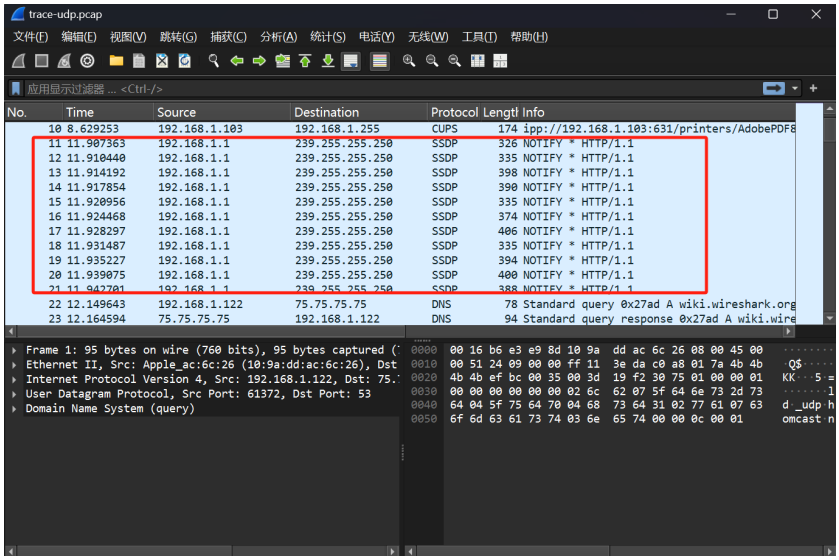

图 12: 数据包

可以看到，这些数据包的 destination IP 地址为 239.255.255.250

3) What is the typical size of UDP messages in your trace?

由于 UDP 报头中的 Length 字段为 2 字节，因此最大长度可达到 $2^{16}-1$ 字节，即 65535 字节。然而，考虑到以太网帧的最大载荷为 1500 字节，而 IP 报头为 20 字节，这意味着 UDP 消息的总长度不应超过 1480 字节。

4.4 问题讨论

We encourage you to keep exploring on your own, but there is not much more to UDP. Instead, you might examine the traffic of UDP-based applications to look at packet sizes and loss rates. Voice-over-IP and its companion protocols like RTP (Real-Time Protocol) are good candidates.

此处以 QQ 为例，QQ 采用的是 OICQ 协议，这是基于 UDP 的，因此可以捕获 QQ 的数据包来分析

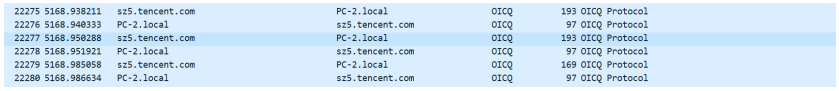

图 13: OICQ 数据包

选择一个 OICQ 数据包。

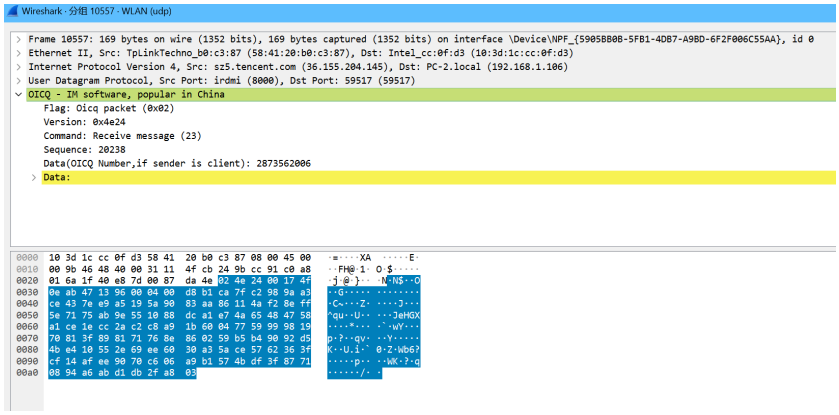

图 14: 打开 OICQ

可以看到，OICQ 数据包的长度为 647 字节。

Similarly, you might explore streaming and real-time applications to see which use UDP and which use TCP as a transport.

由于文件传输需要确保数据的完整性，因此通常采用 TCP 协议。相比之下，流媒体传输和实时通信可以使用 UDP 协议，因为这些应用对数据的实时性要求更高，偶尔的数据包丢失不会对其产生显著影响。

5 实验结果总结

通过本次实验，我学会了使用 `Wireshark` 捕获 `UDP` 消息，掌握了 `UDP` 数据包的结构，理解了各字段的含义，了解了 `UDP` 协议的应用场景。

6 附录

无