# 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 | **年级**：2023级 | **实验成绩**： |
| **实验名称**：UPD | **姓名**：陆尚辰 |  |
| **实验编号**：Labe5 | **学号**：10235101545 | **实验日期**：2024.12.20 |
| **指导教师**：刘献忠 | **组号**： | **实验时间**： |

**一、实验目的**

1. 学会通过Wireshark获取UDP消息

2. 掌握UDP数据包结构及各字段的含义

3. 了解UDP协议适用领域

**二、实验内容与实验步骤**

**1. 获取UDP消息**

(1)启动Wireshark，在菜单栏的捕获->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，将混杂模式设为关闭。

(2)点击开始，打开浏览器，在地址栏中输入网址浏览，例如 www.baidu.com或者在命令行中输入 “nslookup www.baidu.com” 查询DNS服务器；

如果没有DNS解析，在命令行中输入ipconfig/flushdns清空DNS缓存。

(3)停止捕获。

**2. 分析DNS-UDP包**

1. 选择一个数据帧，分析其UDP包头字段，并回答：

1）UDP数据包头中的Length字段指的是UDP有效载荷？还是UDP有效载荷加上UDP头的总长度？还是UDP有效载荷和UDP头以及低层协议的头部三者总长度？

2）UDP头中的校验和的长度是多少位？

3）整个UDP头的长度是多少字节？

**3. 分析其他类型UDP包**

win+R，输入cmd启动命令行，输入ipconfig获得计算机的ip地址，与数据包中的Source比较，回答：

1）在IP协议中哪个字段指明交给上一层的UDP传输进程？该字段值是多少？

2）有的数据包的source和destination ip地址都不是你计算机的ip地址，给出该数据包的destination IP地址。（如果有的话）

3）一般UDP消息的长度是多少？

**三、实验环境**

• 操作系统：Windows 11

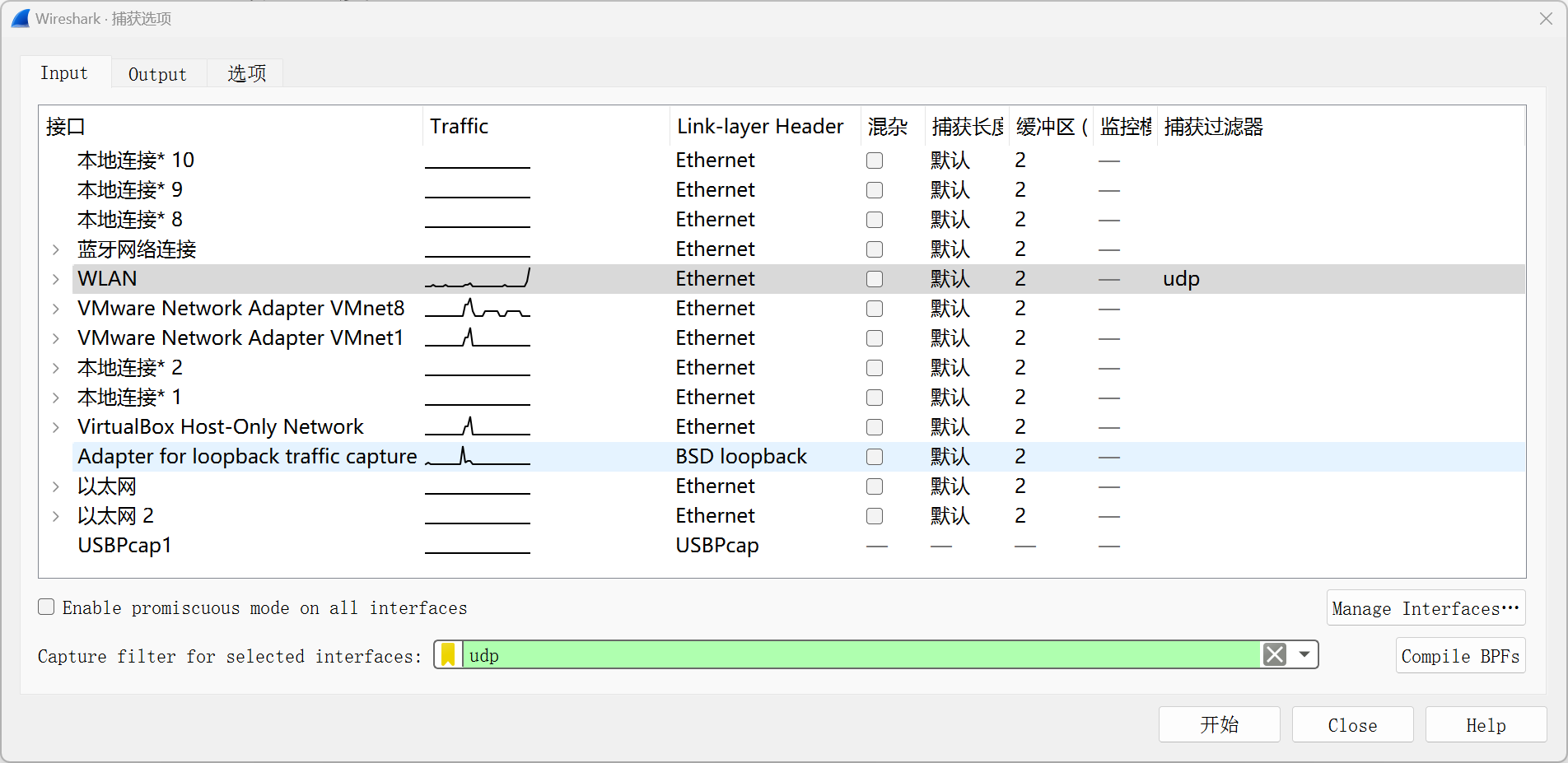
• Wireshark

• wget GNU Wget 1.21.4 built on mingw32

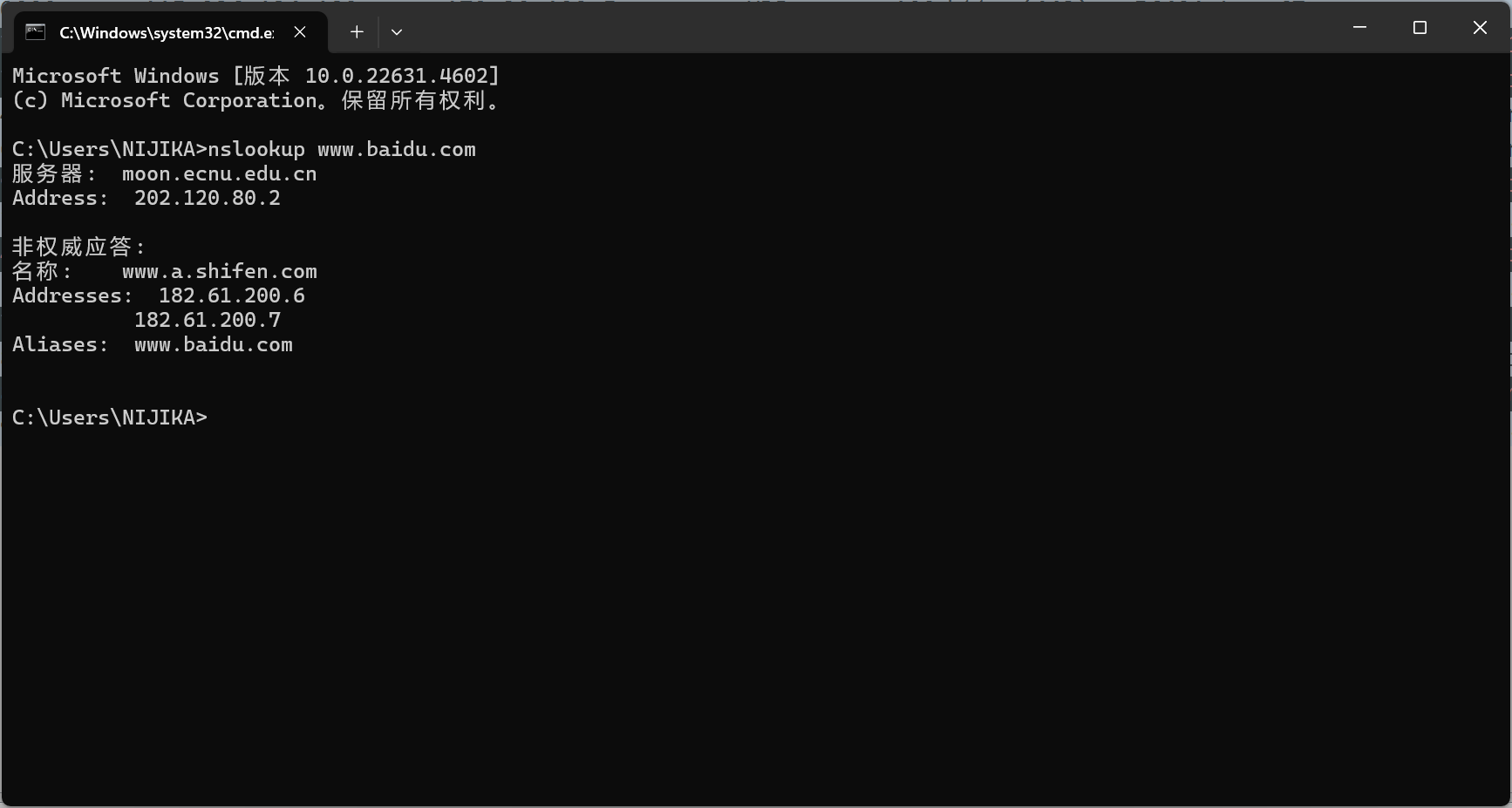
**四、实验过程与分析**

**1.获取UDP消息**

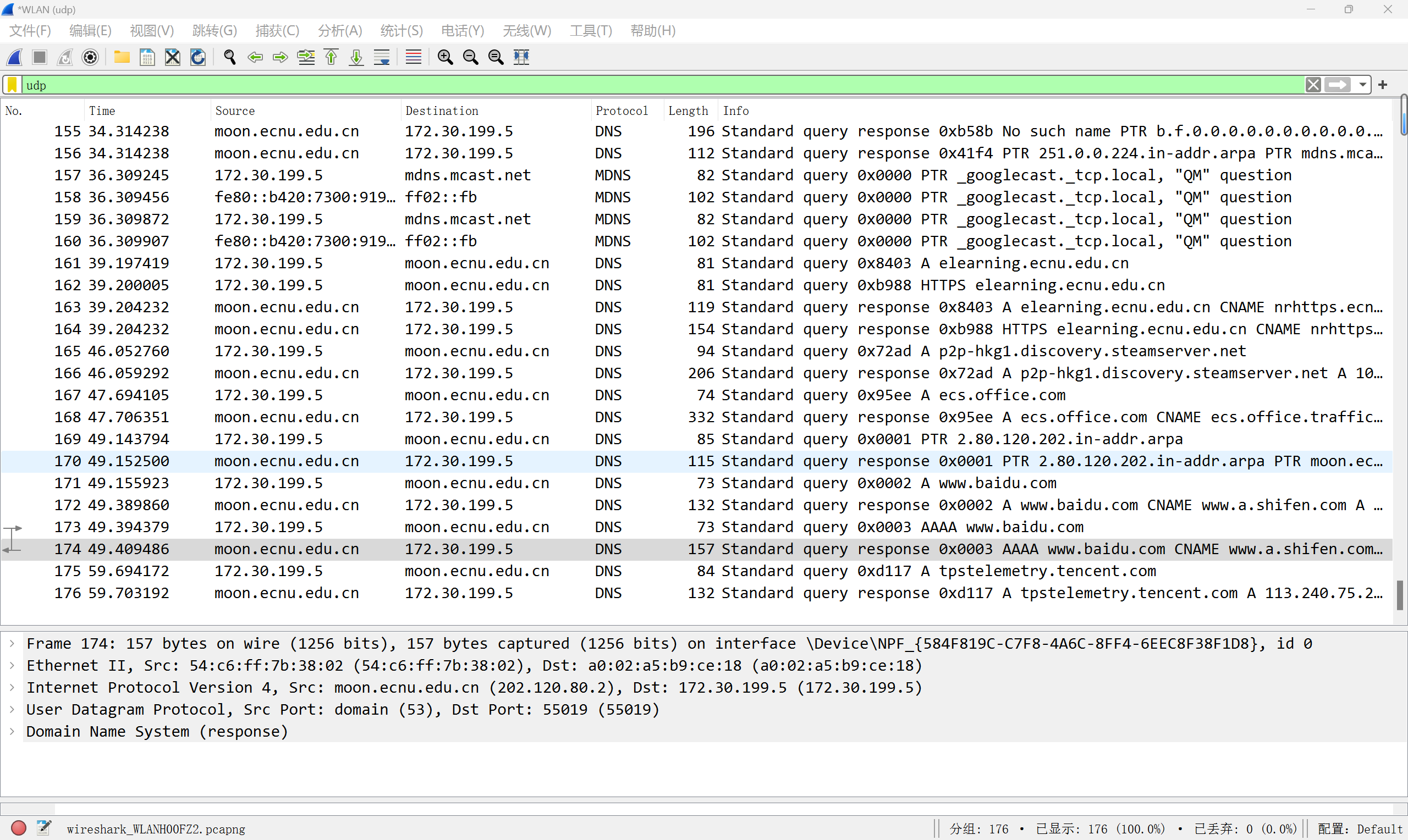
(1)启动Wireshark，在菜单栏的捕获->选项中进行设置，选择已连接的以太网，设置捕获过滤器为udp，将混杂模式设为关闭。



(2)点击开始，在命令行中输入 “nslookup www.baidu.com” 查询DNS服务器；

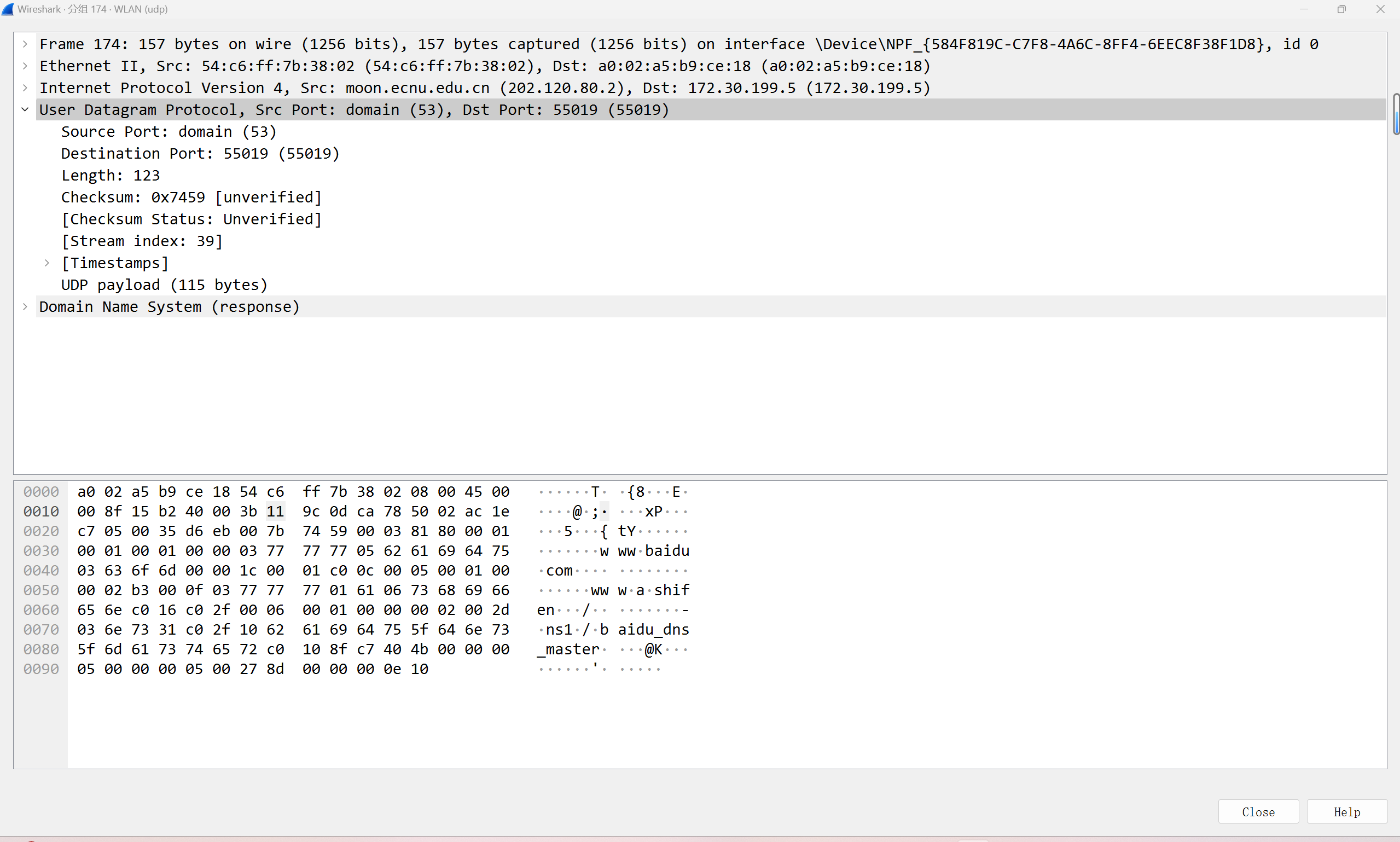


(3)停止捕获，得到如下结果：



**2. 分析DNS-UDP包**

（1）查看一个数据帧，分析其UDP包



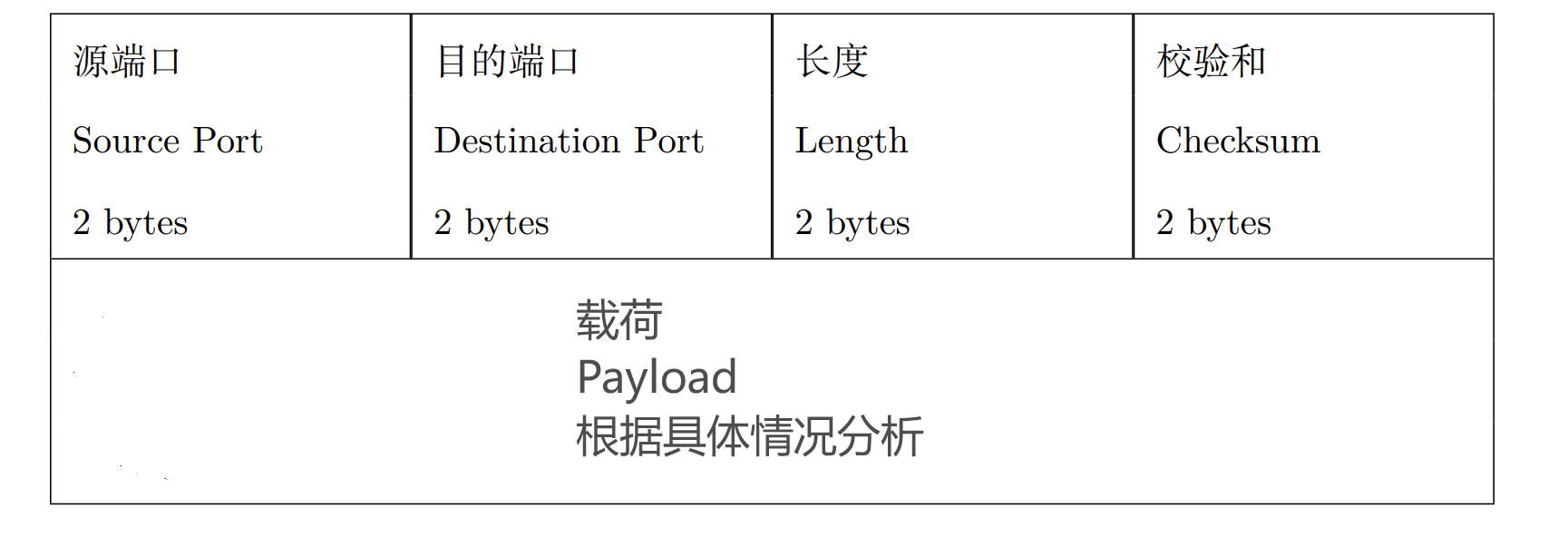
Source Port: 源端口 domain（53） 占2B

Destination Port: 目标端口 55019 占2B

Length : 长度 123 占2B

Checksum: 校验和 0x7459 占2B

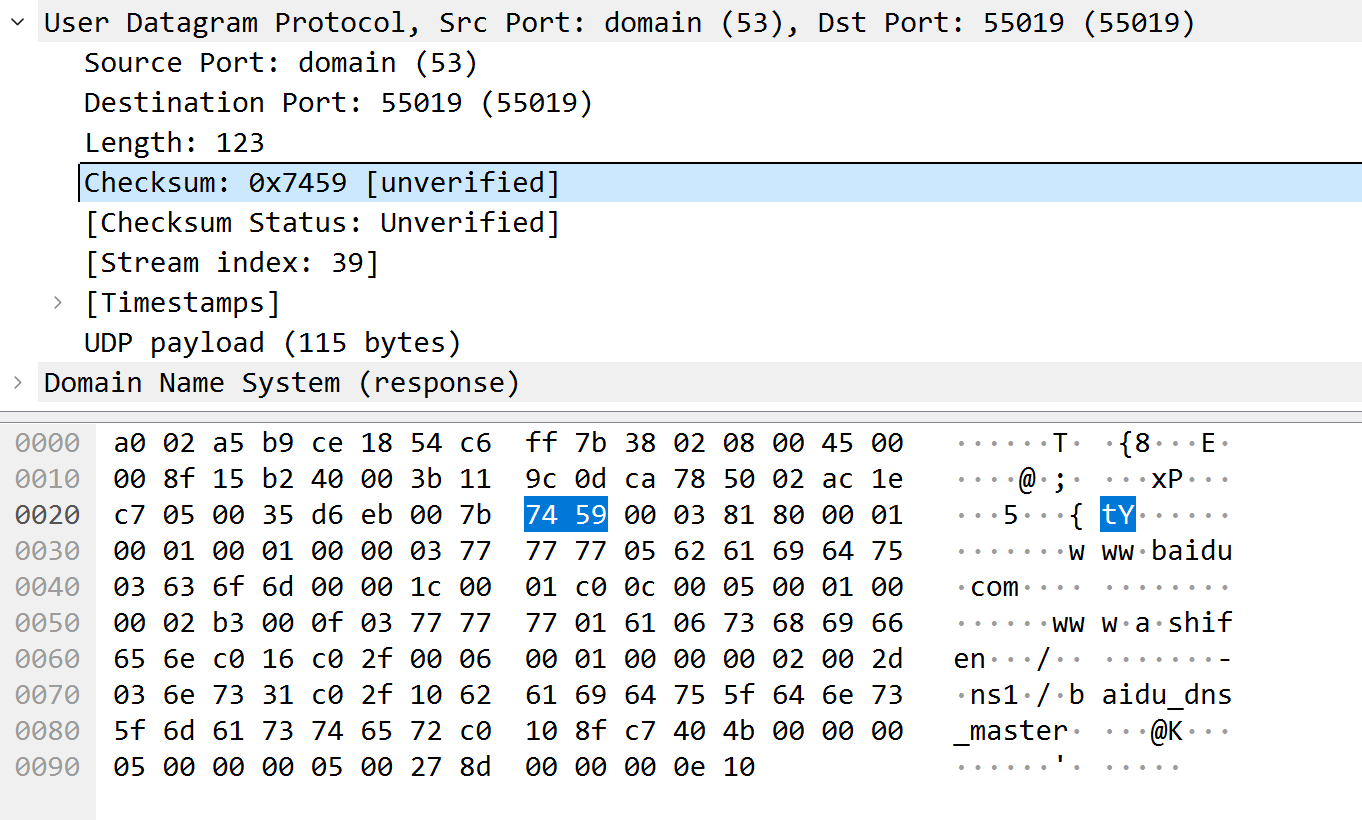
由此可以画出UPD的结构



1）UDP数据包头中的Length字段指的是UDP有效载荷？还是UDP有效载荷加上UDP头的总长度？还是UDP有效载荷和UDP头以及低层协议的头部三者总长度？

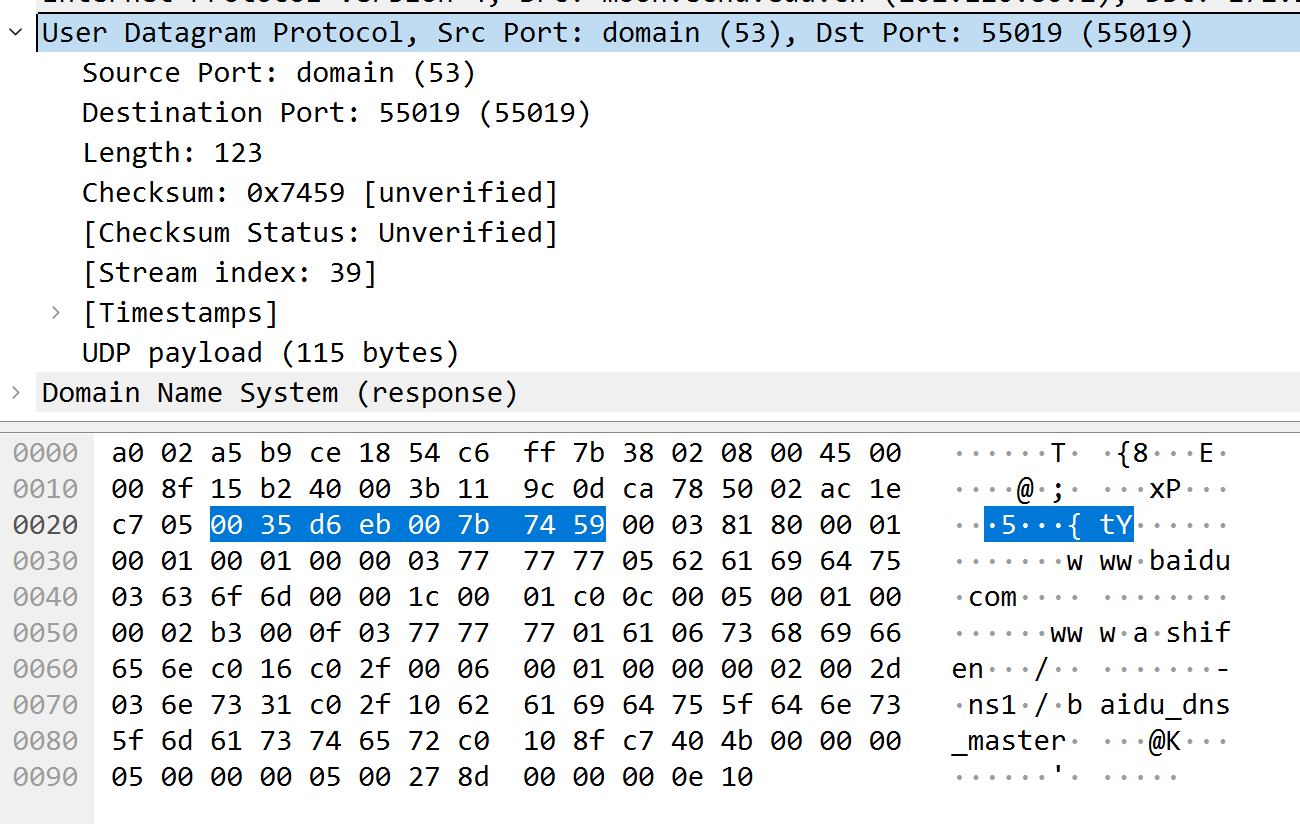
在上面的数据包中，Length字段的长度为123字节，而payload为115字节，UPD头的总长度为8个字节，由此可以看出，Length字段指的是UDP有效载荷加上UDP头的总长度。

2）UDP头中的校验和的长度是多少位？



可以看出校验和占两个字节，16位

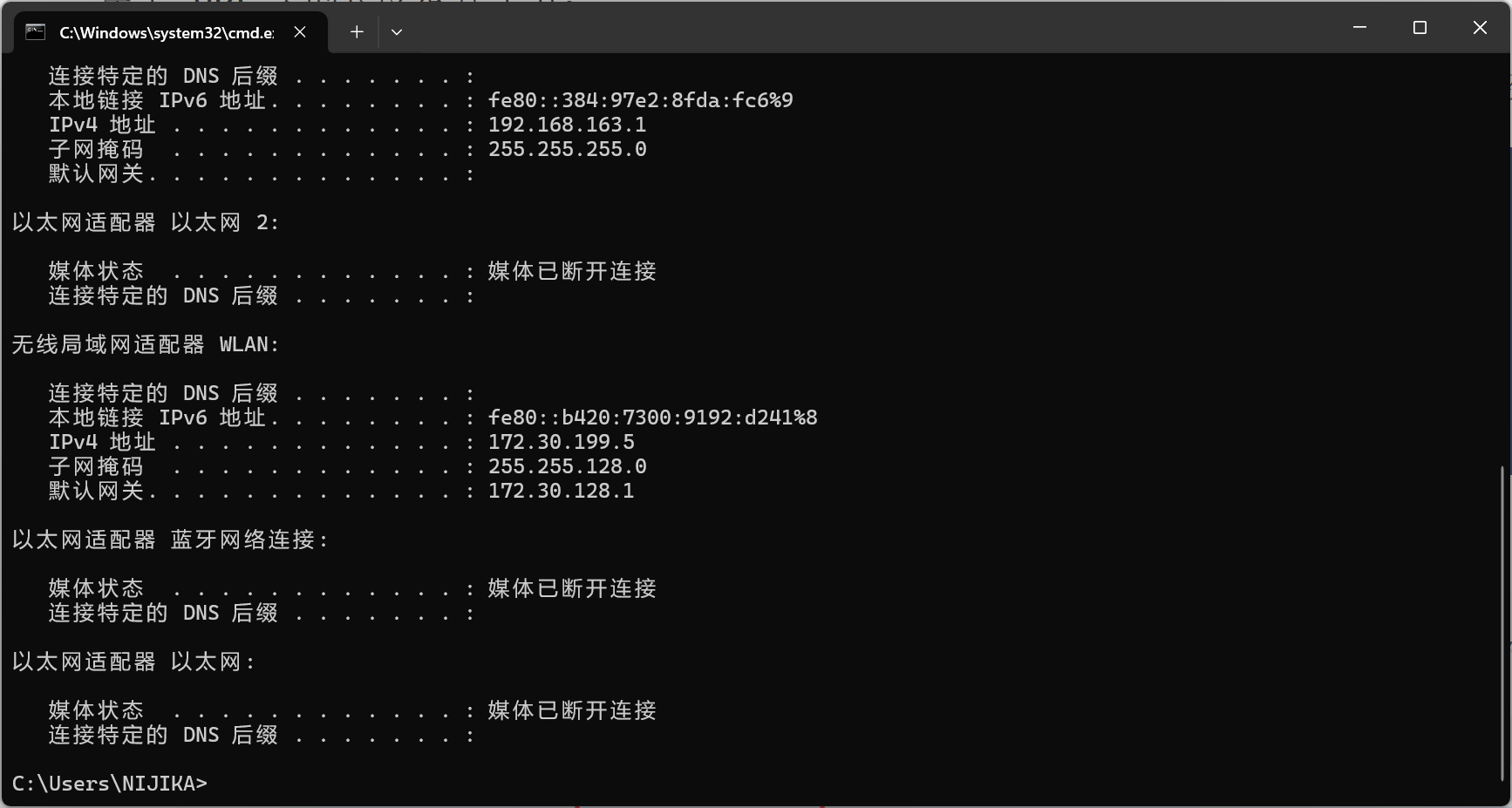
3）整个UDP头的长度是多少字节？



可以看出，UDP头的长度为8个字节

**3. 分析其他类型的UDP包**

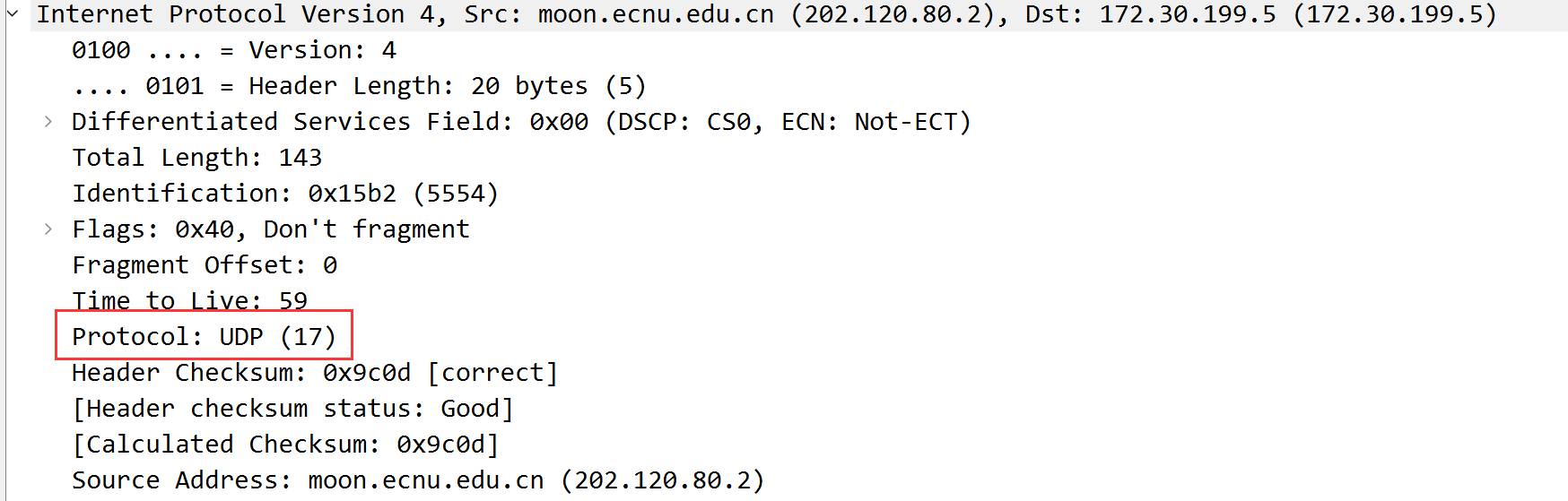
win+R，输入cmd启动命令行，输入ipconfig获得计算机的ip地址



与数据包中的Source比较，IP 地址为 172.30.199.5，而数据包中的 Source Port 为55019，二者并不相同。

问题：

1）在IP协议中哪个字段指明交给上一层的UDP传输进程？该字段值是多少？



Protocal字段指明交给上一层的为UDP传输进程，字段的值为17

2）有的数据包的source和destination ip地址都不是你计算机的ip地址，给出该数据包的destination IP地址。（如果有的话）



为ff02::fb

3）一般UDP消息的长度是多少？

UDP 数据报长度最小为8字节（仅包含UDP头部），理论上最大长度是 65535 字节（包括 UDP 头部和数据部分），但由于以太网一帧的最大载荷为 1500 字节，IP报头为20字节，也就是说UDP消息总长度不能超过1480字节。

**五、实验结果总结**

通过本次实验，我学会了通过 Wireshark 获取 UDP 消息，了解了 UDP 数据包各字段的含义和UDP 数据包结构，更深刻地了解了“端到端”的传输，对不同的UDP包有了新的认识，也看到了 UDP 协议适用领域。

**思考题：**

1. 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 useTCP as a transport.

你可以检测基于用户数据报协议的应用程序的流量，查看数据包大小和丢失率。网络语音电话（VoIP）及其配套协议，比如实时传输协议（RTP），都是很好的检测对象。同样，你也可以研究流媒体和实时应用程序，看看哪些使用用户数据报协议（UDP），哪些使用传输控制协议（TCP）作为传输协议。

**六、附录**

无