# 实验报告:UDP

|  |  |  |
| --- | --- | --- |
| **实验课程**：计算机网络 | **年级**：2023 | **实验成绩**： |
| **实验名称**：UDP | **姓名**：张建夫 |  |
| **实验编号**：lab5 | **学号**：10235101477 | **实验日期**：2024/12/16 |
| **指导教师**：章玥 | **组号**： | **实验时间**：8:00~9:30 |

**一、实验目的**

1．使用wireshark进行抓取UDP数据包；

2．分析UDP数据包，掌握UDP数据包结构；

3．掌握UDP数据包字段含义；

4．了解UDP协议使用领域。

**二、实验内容与实验步骤**

（一）UDP抓包

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”，关闭混杂模式；

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；

3. 打开Wireshark， 停止捕获；

4. 查看Wireshark界面中抓取的UDP数据包。

（二）UDP实验结果分析

问题一：

通过查看UDP消息的详细信息，根据你看到的UDP消息绘制一个结构图，并回答以下问题：

1．UDP数据包头中的Length字段包括哪些部分？UDP有效载荷，还是UDP有效载荷加上UDP头部的总长度，还是UDP有效载荷和UDP头部以及低层协议的头部三者总长度？

2．UDP校验和为多少位？

3．整个UDP头部的长度为多少字节？

问题二:

为了了解UDP在实践中是如何进行传输的，观察数据包的IP头部并思考以下问题：

1．将上层协议标识为UDP的IP头部的协议字段值为多少？

2．查看源IP地址与目的IP地址都不是你的计算机的IP地址的数据包，并给出这些数据包的目的IP地址。

3．捕获到的UDP消息中，一般UDP消息的长度为多少？

（三）UDP问题与思考

在完成本实验后继续探索UDP协议：

1．探索基于UDP的应用程序的流量，查看数据包大小和丢失率。

2．探索流和实时应用程序，查看哪些使用UDP以及哪些使用TCP进行传输。

**三、实验环境**

调用dxdiag工具：

Operating System: Windows 11 家庭中文版 64-bit (10.0, Build 22621) (22621.ni\_release.220506-1250)

Language: Chinese (Simplified) (Regional Setting: Chinese (Simplified))

System Manufacturer: HP

System Model: HP Pavilion Aero Laptop 13-be2xxx

BIOS: F.13 (type: UEFI)

Processor: AMD Ryzen 5 7535U with Radeon Graphics (12 CPUs), ~2.9GHz

Memory: 16384MB RAM

Available OS Memory: 15574MB RAM

Page File: 27604MB used, 5685MB available

Windows Dir: C:\WINDOWS

DirectX Version: DirectX 12

DX Setup Parameters: Not found

User DPI Setting: 144 DPI (150 percent)

System DPI Setting: 192 DPI (200 percent)

DWM DPI Scaling: UnKnown

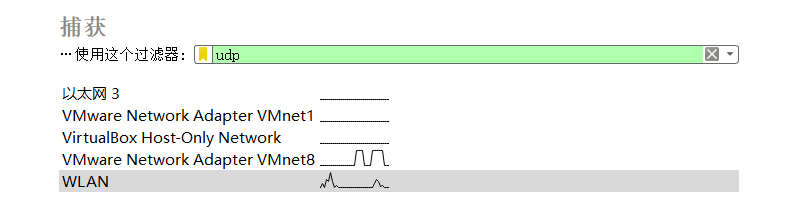
Miracast: Available, with HDCP

Microsoft Graphics Hybrid: Not Supported

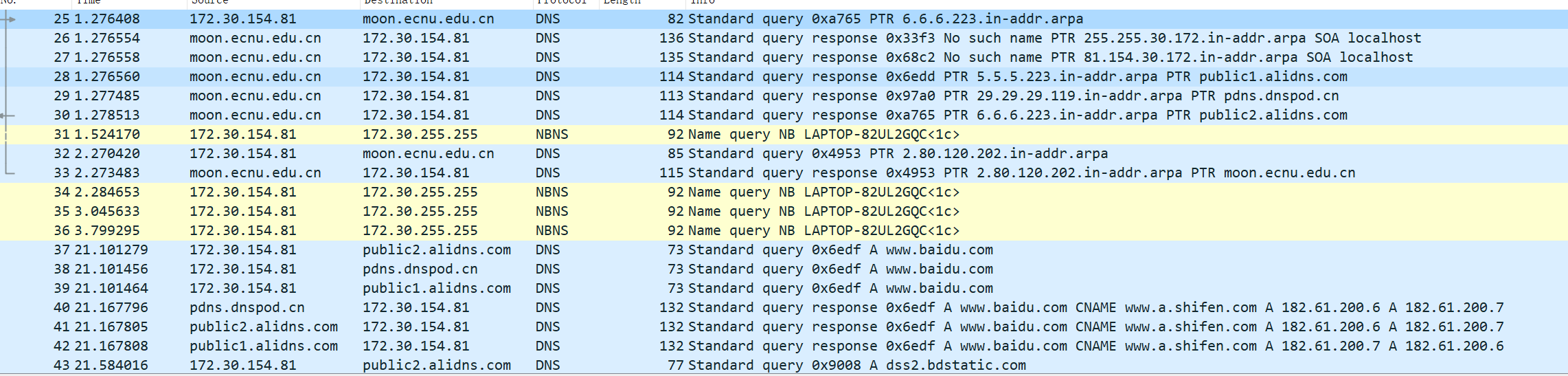
**四、实验过程与分析**

（一）

设置Wireshark：

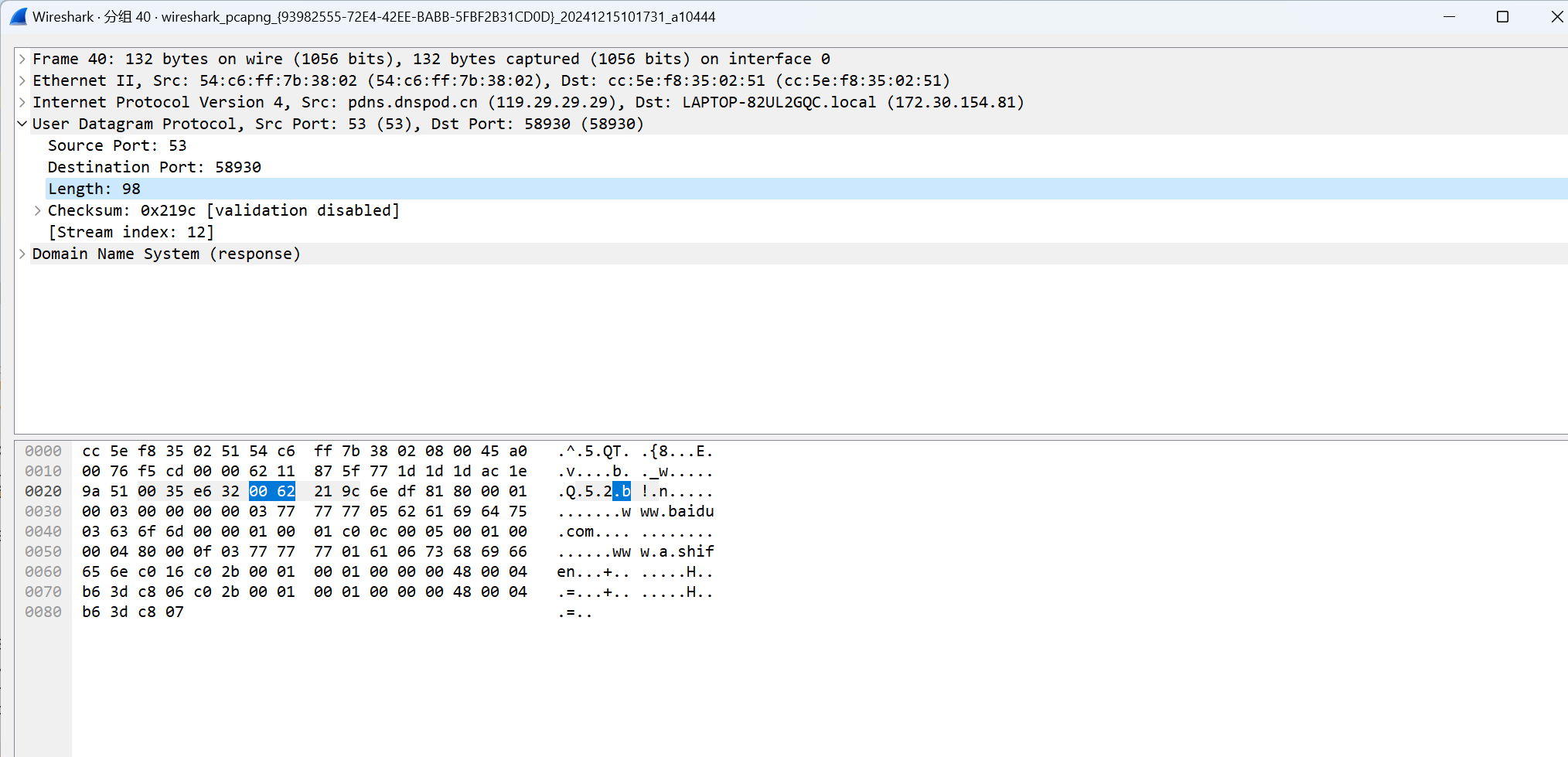


查看Wireshark捕获结果：



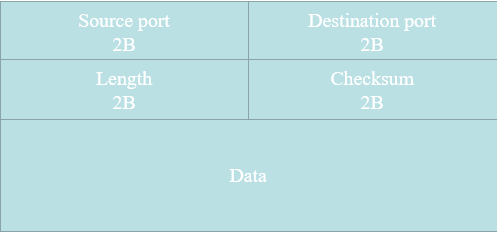
（二）

打开一个DNS数据包，查看其UDP头部：



问题一：

绘制UDP结构图：



1．UDP数据包头中的Length字段包括哪些部分？UDP有效载荷，还是UDP有效载荷加上UDP头部的总长度，还是UDP有效载荷和UDP头部以及低层协议的头部三者总长度？

由前面的UDP截图可知，UDP头部的Length字段为98，而98+20（ip头部长度）+14（以太网帧头部长度）=132（总长度），可以看出UDP包中Length包括UDP头部和UDP有效载荷的总长度。

2．UDP校验和为多少位？

截图中的UDP头部的checksum为0x219c，因此校验和为2B，16位。

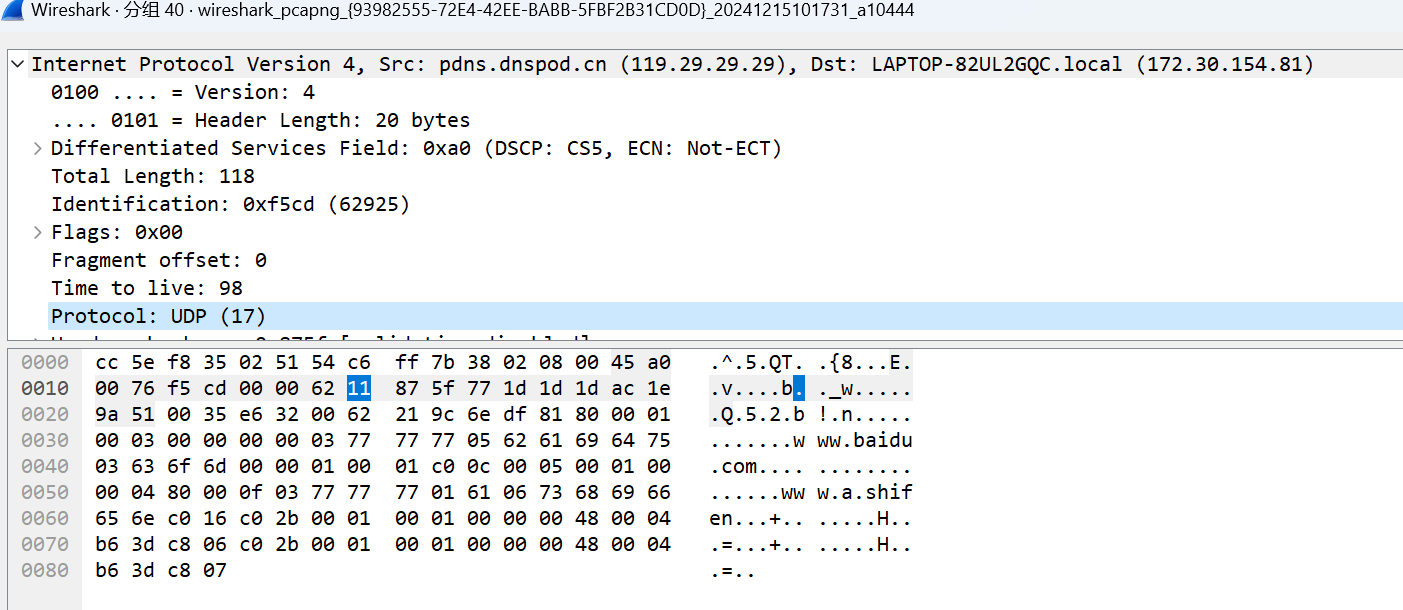
3．整个UDP头部的长度为多少字节？

整个头部长度为2（源端口）+2（目的端口）+2（UDP及其荷载的总长度）+2（checksum）=8字节。

问题二：

1．将上层协议标识为UDP的IP头部的协议字段值为多少？

观察IP头部：

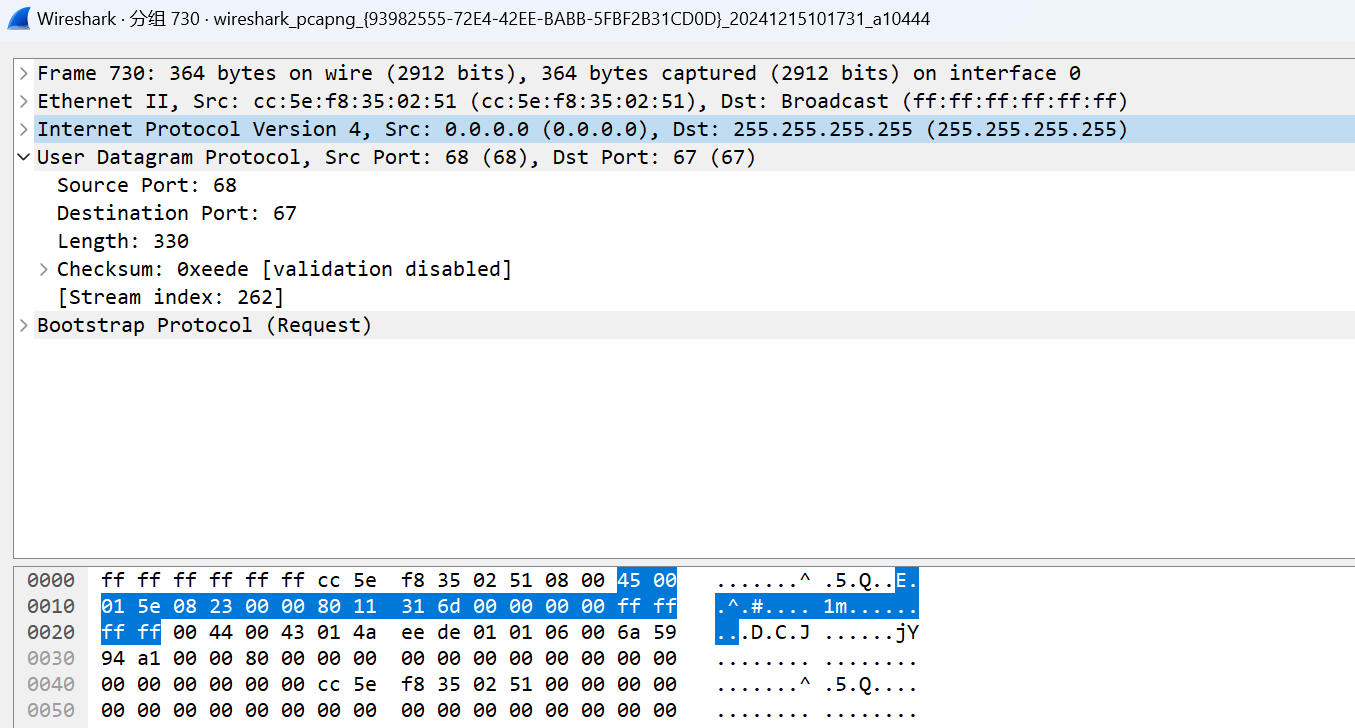


可以看到，将上层协议标识为UDP的字段值为17(0x11)

2．查看源IP地址与目的IP地址都不是你的计算机的IP地址的数据包，并给出这些数据包的目的IP地址。

对于没有本机ip地址的数据包，我捕到了如下包：





这些包的目的ip地址都为255.255.255.255

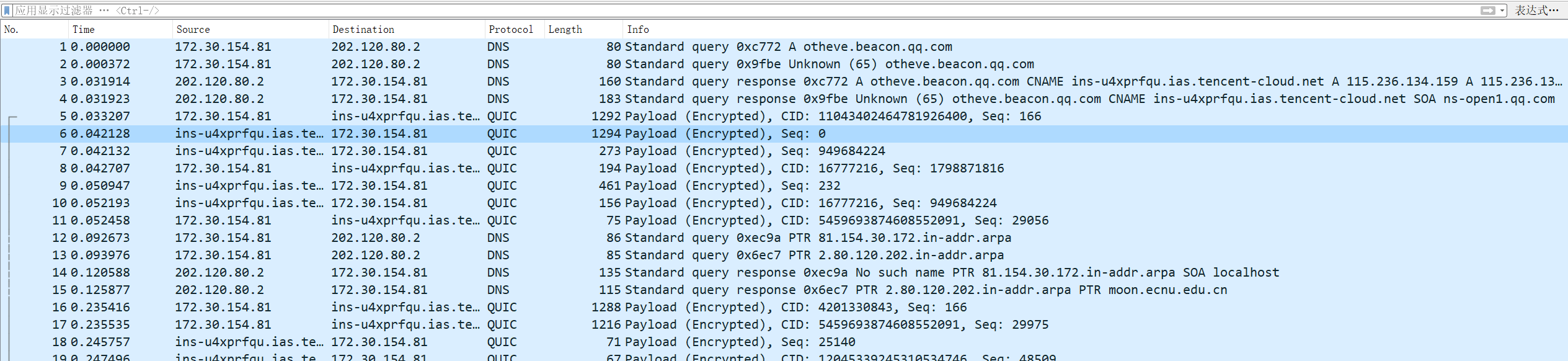
3．捕获到的UDP消息中，一般UDP消息的长度为多少？

根据统计抓到的数据包，常见的UDP消息的长度在80-120。 结合所学知识可知，最大传输单元1MTU为1500字节，减去ip协议头部20字节和UDP头部8字 节，得到1472字节，为UDP载荷的最大值。

(三)

1．探索基于UDP的应用程序的流量，查看数据包大小和丢失率。

从网络上了解到QQ以UDP为主,而微信以TCP为主，所以尝试捕获QQ的数据包:



这里面捕获的数据包的上层协议与网上所说的qq的oicq协议并不一致，qq反而使用了quic的加密数据包来传输数据，数据包的大小也从两位数到四位数不等，也就是说，数据包的大小从最小到最大都有，而丢包率上网查了诸多方法也没有找到能正确获取丢包率的方法，因此暂无丢包率计算。

2．探索流和实时应用程序，查看哪些使用UDP以及哪些使用TCP进行传输。

现实工作环境下常见的UDP应用主要有P2P下载、视频会议、在线视频、VOIP语音、在线游戏等.

TCP一般用于文件传输（FTP HTTP 对数据准确性要求高，速度可以相对慢），发送或接收邮件（POP IMAP SMTP 对数据准确性要求高，非紧急应用），远程登录（TELNET SSH 对数据准确性有一定要求，有连接的概念）等等；UDP一般用于即时通信（QQ聊天 对数据准确性和丢包要求比较低，但速度必须快），在线视频（RTSP 速度一定要快，保证视频连续，但是偶尔花了一个图像帧，人们还是能接受的），网络语音电话（VoIP 语音数据包一般比较小，需要高速发送，偶尔断音或串音也没有问题）等等。

**五、实验结果总结**

本次实验加深了我对udp数据包的理解，也对一些应用程序使用的udp包有了一个初步的认识，且加深了对数据流和数据包区别的理解，并了解了一些解码译码相关的知识。

**六、附录**