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

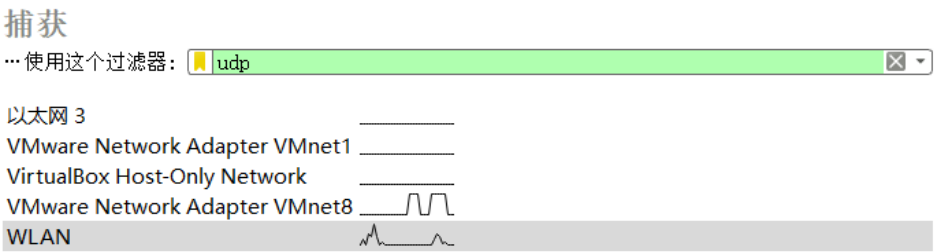
调用 dxdiag 工具：

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

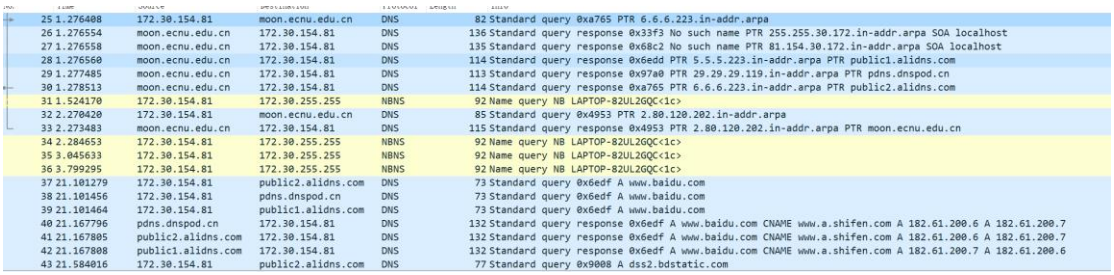
四、实验过程与分析

（一）

设置 Wireshark：



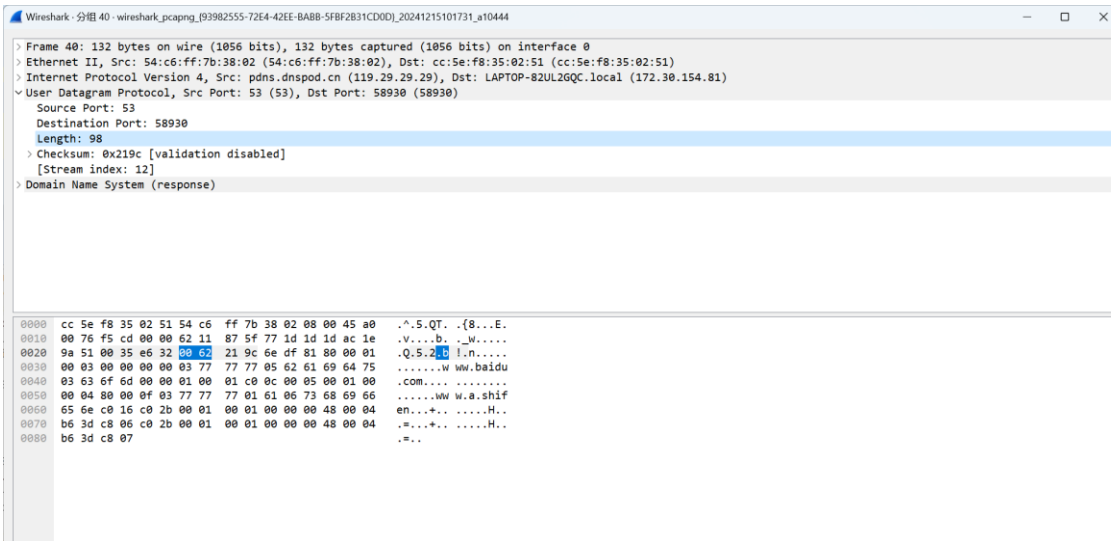
查看 Wireshark 捕获结果：



25	1.276408	172.30.154.81	moon.ecnu.edu.cn	DNS	82	Standard query 0xa765 PTR 6.6.6.223.in-addr.arpa
26	1.276554	moon.ecnu.edu.cn	172.30.154.81	DNS	136	Standard query response 0x33f3 No such name PTR 255.255.30.172.in-addr.arpa SOA localhost
27	1.276558	moon.ecnu.edu.cn	172.30.154.81	DNS	135	Standard query response 0x68c2 No such name PTR 81.154.30.172.in-addr.arpa SOA localhost
28	1.276560	moon.ecnu.edu.cn	172.30.154.81	DNS	114	Standard query response 0x6edd PTR 5.5.5.223.in-addr.arpa PTR public1.alidns.com
29	1.277485	moon.ecnu.edu.cn	172.30.154.81	DNS	113	Standard query response 0x97a0 PTR 29.29.29.119.in-addr.arpa PTR pdns.dnspod.cn
30	1.278513	moon.ecnu.edu.cn	172.30.154.81	DNS	114	Standard query response 0xa765 PTR 6.6.6.223.in-addr.arpa PTR public2.alidns.com
31	1.524170	172.30.154.81	172.30.255.255	NBNS	92	Name query NB LAPTOP-82UL2GQC<1c>
32	2.270420	172.30.154.81	moon.ecnu.edu.cn	DNS	85	Standard query 0x4953 PTR 2.80.120.202.in-addr.arpa
33	2.273483	moon.ecnu.edu.cn	172.30.154.81	DNS	115	Standard query response 0x4953 PTR 2.80.120.202.in-addr.arpa PTR moon.ecnu.edu.cn
34	2.284653	172.30.154.81	172.30.255.255	NBNS	92	Name query NB LAPTOP-82UL2GQC<1c>
35	3.045633	172.30.154.81	172.30.255.255	NBNS	92	Name query NB LAPTOP-82UL2GQC<1c>
36	3.799295	172.30.154.81	172.30.255.255	NBNS	92	Name query NB LAPTOP-82UL2GQC<1c>
37	21.101279	172.30.154.81	public2.alidns.com	DNS	73	Standard query 0x6edf A www.baidu.com
38	21.101456	172.30.154.81	pdns.dnspod.cn	DNS	73	Standard query 0x6edf A www.baidu.com
39	21.101464	172.30.154.81	public1.alidns.com	DNS	73	Standard query 0x6edf A www.baidu.com
40	21.167796	pdns.dnspod.cn	172.30.154.81	DNS	132	Standard query response 0x6edf A www.baidu.com CNAME www.a.shifen.com A 182.61.200.6 A 182.61.200.7
41	21.167805	public2.alidns.com	172.30.154.81	DNS	132	Standard query response 0x6edf A www.baidu.com CNAME www.a.shifen.com A 182.61.200.6 A 182.61.200.7
42	21.167808	public1.alidns.com	172.30.154.81	DNS	132	Standard query response 0x6edf A www.baidu.com CNAME www.a.shifen.com A 182.61.200.7 A 182.61.200.6
43	21.584016	172.30.154.81	public2.alidns.com	DNS	77	Standard query 0x9008 A dss2.bdstatic.com

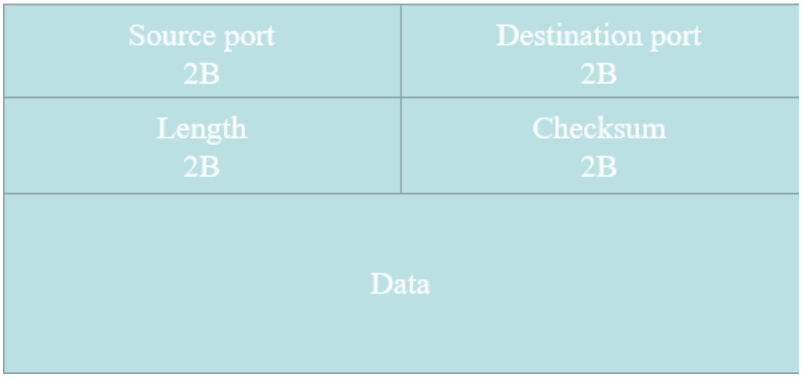
（二）

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。

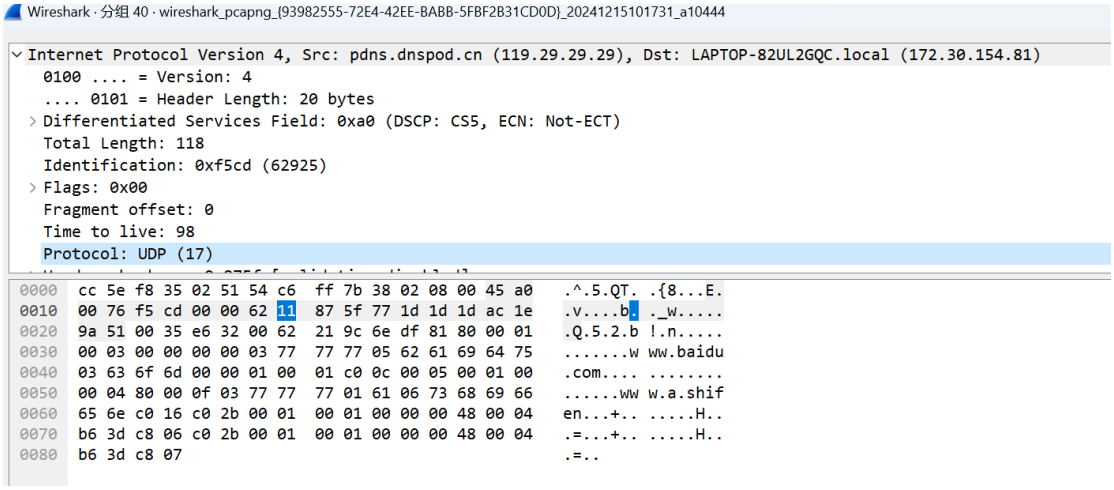
3．整个 UDP 头部的长度为多少字节？

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？

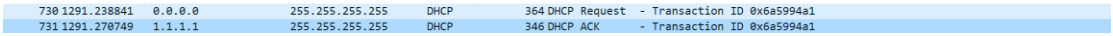
观察 IP 头部：

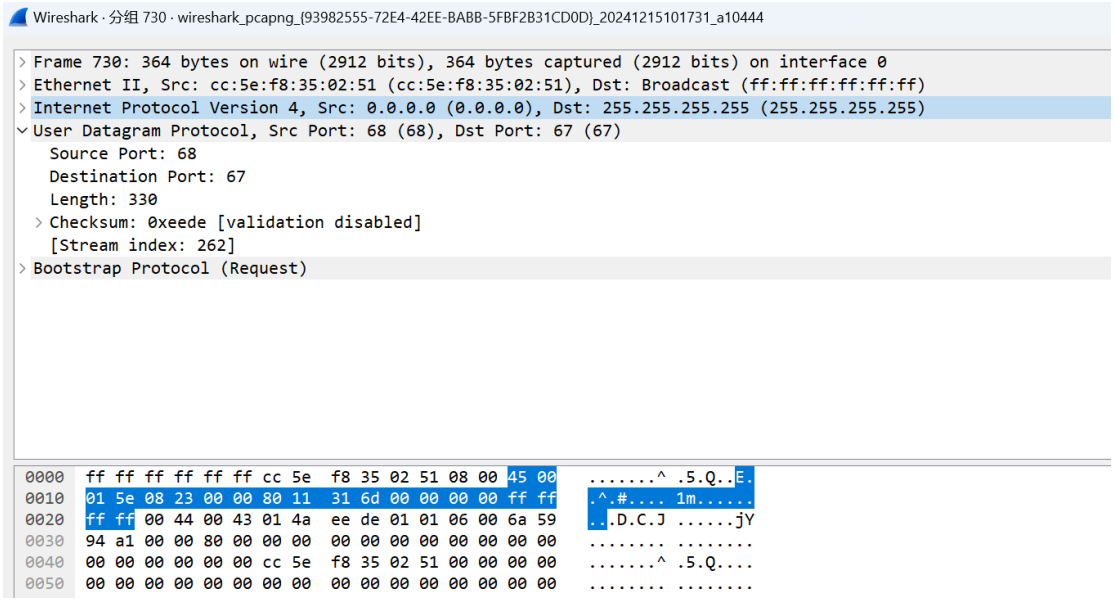


可以看到，将上层协议标识为 UDP 的字段值为 17(0x11)

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

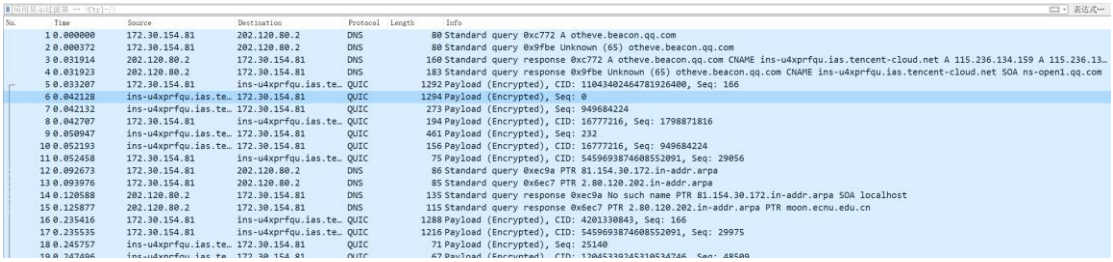
3. 捕获到的 UDP 消息中，一般 UDP 消息的长度为多少？

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