

华东师范大学数据科学与工程学院上机实践报告

课程名称： 计算机网络与编程

年级： 2022

上机实践成绩：

指导教师： 张召

姓名： 李芳

学号： 10214602404

上机实践名称： UDP 协议分析

上机实践日期： 2024.05.10

上机实践编号： 11

组号：

上机实践时间：

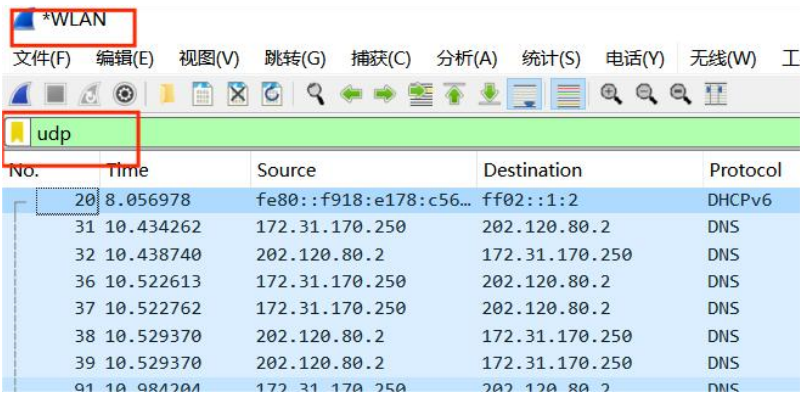
一、 题目要求及实现情况

task1: 从跟踪中选择一个 UDP 数据包。从此数据包中，识别并确定 UDP 首部字段，请为这些字段命名并将实验结果附在实验报告中。

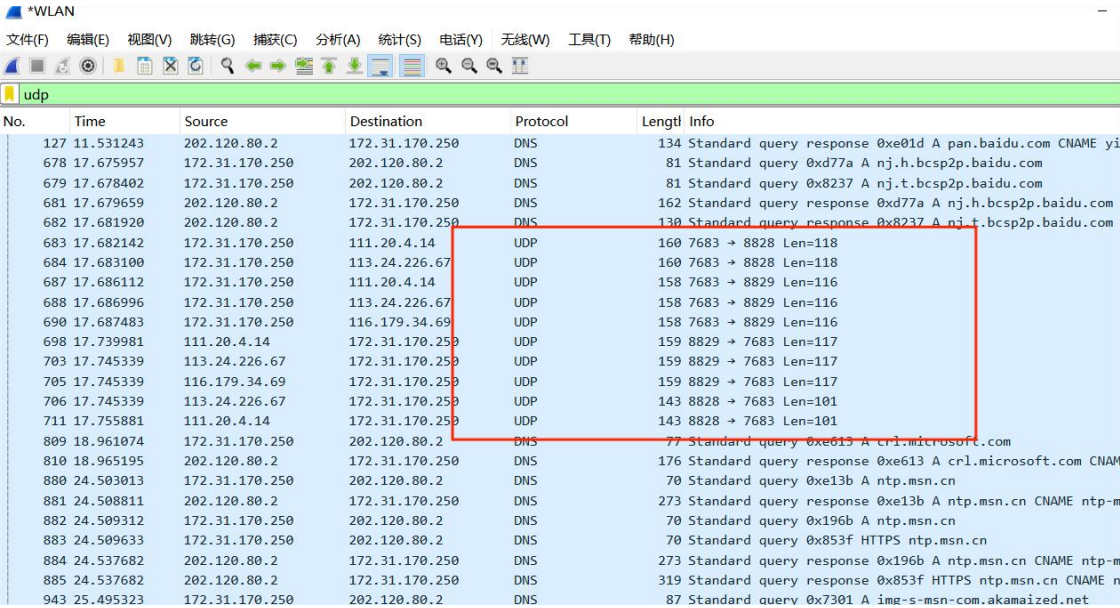
操作截图& 分析：

➤ 操作流程：

- 先打开 wireshark，选择 wlan 选项进行 udp 数据包捕获：



- 打开百度网盘客户端，进行用户登陆操作，就已经可以捕获到 UDP 数据包：



■ 选择其中一个 UDP 数据包，对其首部进行详细分析：

687	17.686112	172.31.170.250	111.20.4.14	UDP	158	7683 → 8829	Len=116
688	17.686996	172.31.170.250	113.24.226.67	UDP	158	7683 → 8829	Len=116
690	17.687483	172.31.170.250	116.179.34.69	UDP	158	7683 → 8829	Len=116
698	17.739981	111.20.4.14	172.31.170.250	UDP	159	8829 → 7683	Len=117
703	17.745339	113.24.226.67	172.31.170.250	UDP	159	8829 → 7683	Len=117
705	17.745339	116.179.34.69	172.31.170.250	UDP	159	8829 → 7683	Len=117
706	17.745339	113.24.226.67	172.31.170.250	UDP	143	8828 → 7683	Len=101
711	17.755881	111.20.4.14	172.31.170.250	UDP	143	8828 → 7683	Len=101

> Frame 698: 159 bytes on wire (1272 bits), 159 bytes captured (1272 bits) on interface  
 > Ethernet II, Src: NewH3CTechno\_7b:38:02 (54:c6:ff:7b:38:02), Dst: ChongqingFug\_83  
 > Internet Protocol Version 4, Src: 111.20.4.14, Dst: 172.31.170.250  
 v User Datagram Protocol, Src Port: 8829, Dst Port: 7683  
   Source Port: 8829  
   Destination Port: 7683  
   Length: 125  
   Checksum: 0x638e [unverified]  
   [Checksum Status: Unverified]  
   [Stream index: 12]  
 v [Timestamps]  
   [Time since first frame: 0.053869000 seconds]  
   [Time since previous frame: 0.053869000 seconds]  
   UDP payload (117 bytes)  
 v Data (117 bytes)  
   Data [truncated]: 8478e450663d8d8000104007020000030000f500808d3d660c0000000000  
   [Length: 117]

0000 c0 b5 d7 83 a3 c5 54 c  
 0010 00 91 9a 17 40 00 22 1  
 0020 aa fa 22 7d 1e 03 00 7  
 0030 8d 80 00 10 40 07 02 0  
 0040 3d 66 0c 00 00 00 00 0  
 0050 df f1 80 94 8c 08 99 1  
 0060 f7 b6 2b 2b f8 5c e6 6  
 0070 71 80 b4 b4 f6 62 fa d  
 0080 b5 39 68 89 f8 d3 f2 d  
 0090 5a 9b 4a ed 5c b3 37 8

➤ UDP 数据包分析：



■ 根据上图结构分析选中数据包首部：

```

> Internet Protocol Version 4, Src: 111.20.4.14, Dst: 172.31.170.250
v User Datagram Protocol, Src Port: 8829, Dst Port: 7683
  Source Port: 8829
  Destination Port: 7683
  Length: 125
  Checksum: 0x638e [unverified]
  [Checksum Status: Unverified]
  [Stream index: 12]
> [Timestamps]
  UDP payload (117 bytes)
v Data (117 bytes)
  Data [truncated]: 8478e450663d8d8000104007020000030000f500808d3d6
  [Length: 117]
  
```

## ■ 数据包首部:

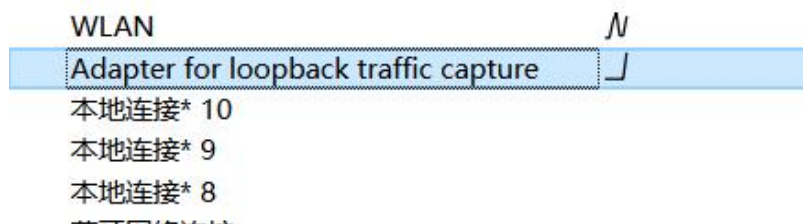
- ◆ Source Port (源端口): 8829 -> 源端口: 发送端的应用程序使用的端口号。
- ◆ Destination Port (目的端口): 7683 -> 目的端口: 接收端的应用程序期望接收数据的端口号。
- ◆ Length (长度): 125 -> 长度: UDP 数据报的长度, 包括首部和数据部分, 字节为单位。
- ◆ Checksum (校验和): 0x638e [未验证] -> 校验和: 检测 UDP 数据报在传输过程中是否发生了错误。此时为“未验证”, 表示校验和尚未被验证。

## ■ 剩余部分:

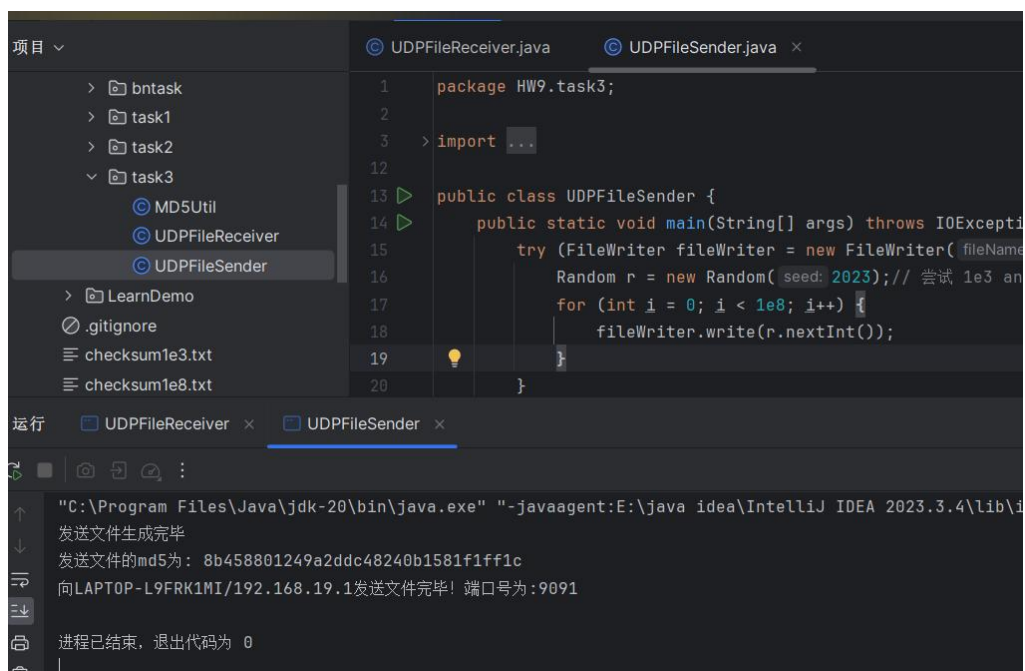
- ◆ Timestamps (时间戳) -> 提供关于数据报发送的时间信息。
- ◆ UDP Payload (UDP 数据部分) -> 包含应用层传输的实际数据, 长度为 117 字节。

*UDPjava 代码实验流程:*

- 启动 wireshark 捕获 Adapter for loopback traffic capture 选项, 并筛选 UDP 数据包:



- 运行 UDP 的 Socket 实验的 Task3 代码, 发送 1e8 长度的数据





正在捕获 Adapter for loopback traffic capture

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

udp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.19.1	192.168.19.1	ICMP	28	Destination unreachable
3	2.060381	192.168.19.1	192.168.19.1	UDP	2032	60932 → 9091 Len=2000
4	2.060694	192.168.19.1	192.168.19.1	UDP	2032	60932 → 9091 Len=2000
5	2.060763	192.168.19.1	192.168.19.1	UDP	2032	60932 → 9091 Len=2000
6	2.060835	192.168.19.1	192.168.19.1	UDP	2032	60932 → 9091 Len=2000
7	2.060885	192.168.19.1	192.168.19.1	UDP	2032	60932 → 9091 Len=2000
8	2.060932	192.168.19.1	192.168.19.1	UDP	2032	60932 → 9091 Len=2000
9	2.060978	192.168.19.1	192.168.19.1	UDP	2032	60932 → 9091 Len=2000
10	2.061023	192.168.19.1	192.168.19.1	UDP	2032	60932 → 9091 Len=2000
11	2.061073	192.168.19.1	192.168.19.1	UDP	2032	60932 → 9091 Len=2000
12	2.061125	192.168.19.1	192.168.19.1	UDP	2032	60932 → 9091 Len=2000

> Frame 3: 2032 bytes on wire (16256 bits), 2032 bytes captured (16256 bits) on 0

> Null/Loopback

> Internet Protocol Version 4, Src: 192.168.19.1, Dst: 192.168.19.1

▼ User Datagram Protocol, Src Port: 60932, Dst Port: 9091

Source Port: 60932

Destination Port: 9091

Length: 2008

Checksum: 0xd4e1 [unverified]

[Checksum Status: Unverified]

[Stream index: 1]

> [Timestamps]

UDP payload (2000 bytes)

> Data (2000 bytes)

0020 e5 92 b6 3f ef bf 9b e1  
0030 eb 8d a1 e7 80 aa e1 b0  
0040 8a aa e5 82 a8 e2 b5 83  
0050 b4 82 ee a5 b6 ee b0 bc  
0060 89 e3 99 9d e3 a4 af e6  
0070 e4 a3 b7 e3 9f a7 e3 9c  
0080 92 b7 e9 bf 87 ec ad b7  
0090 bc 8a e8 b5 b2 e6 97 8e  
00a0 83 eb a3 97 ee a7 9c ef  
00b0 e4 b5 94 e4 a4 ba e8 af  
00c0 af a2 e3 9c b5 e1 ac 9d  
00d0 b8 ea b0 bd e9 b4 bf e1  
00e0 ec 9f a1 e6 a1 a6 ed 88  
00f0 b3 95 ea 98 95 e1 90 ab  
0100 84 e6 aa 82 e4 af b9 ea  
0110 ee 81 b4 ea 98 9c e9 bc  
0120 e6 ab ae e8 b4 90 ed 8e  
0130 a1 8e df b4 e5 ba b6 e7

**task2:** UDP首部中的长度字段指的是什么，以及为什么需要这样设计？使用捕获的 UDP 数据包进行验证，请将实验结果附在实验报告中。

回答：

➤ UDP 首部中的长度字段：

- 指的是 UDP 数据报文的长度
- 组成：UDP 首部长度（8 字节） + 数据部分长度。
- 长度：在首部中，该字段为 2 字节，取值范围是 0--65535。
- 作用：让接收方能够正确地识别 UDP 数据报文的边界，正确从接收缓冲区中读取数据。

➤ 设计意义：接收方通过数据报文的长度，正确解析数据报文，并从网络中把数据提取出来。这简化协议实现，同时提高协议的灵活性（长度可以根据实际需要而变化，而不受固定长度的限制）

验证分析：

➤ 捕获 UDP 数据包：

下面是用来证明的，捕获的 UDP 数据包。

26882	73.699603	172.31.170.250	116.179.34.69	UDP
26886	73.743044	116.179.34.69	172.31.170.250	UDP
27130	76.005992	172.31.170.250	202.120.80.2	DNS
27131	76.011383	172.31.170.250	202.120.80.2	DNS
27132	76.030629	202.120.80.2	172.31.170.250	DNS
27133	76.030685	202.120.80.2	172.31.170.250	DNS
27137	76.033676	172.31.170.250	202.120.80.2	DNS

>	Frame 26882: 163 bytes on wire (1304 bits), 163 bytes captured (1304 bits) on	00:00:00:00:00:00
>	Ethernet II, Src: ChongqingFug_83:a3:c5 (c0:b5:d7:83:a3:c5), Dst: NewH3CTech	00:00:00:00:00:00
>	Internet Protocol Version 4, Src: 172.31.170.250, Dst: 116.179.34.69	00:00:00:00:00:00
>	User Datagram Protocol, Src Port: 7683, Dst Port: 8829	00:00:00:00:00:00
>	Source Port: 7683	00:00:00:00:00:00
>	Destination Port: 8829	00:00:00:00:00:00
>	Length: 129	00:00:00:00:00:00
>	Checksum: 0x5ad1 [unverified]	00:00:00:00:00:00
>	[Checksum Status: Unverified]	00:00:00:00:00:00
>	[Stream index: 14]	00:00:00:00:00:00
>	[Timestamps]	00:00:00:00:00:00
>	UDP payload (121 bytes)	00:00:00:00:00:00
>	Data (121 bytes)	00:00:00:00:00:00

详细分析可以知道，Length 标明数据包长度为 120 字节，除去首部固定的 8 个字节，剩下就是 Data 数据部分的 121 字节。

**task3: UDP 有效负载中可包含的最大字节数是多少？请将实验结果附在实验报告中。**

- IPv4 下，UDP 有效负载的最大字节数为  $1500 - 20$  (IP 首部)  $- 8$  (UDP 首部) = 1472 字节
- IPv6 下，UDP 有效负载的最大字节数为  $1280 - 40$  (IP 首部)  $- 8$  (UDP 首部) = 1232 字节
- **UDP 有效负载 (Payload)**：UDP 数据报文中的实际数据部分，不包括 UDP 首部 (8 字节) 和 IP 首部 (通常为 20 字节)。

**task4: 观察发送 UDP 数据包后接收响应的 UDP 数据包，这是对发送的 UDP 数据包的回复，请描述两个数据包中端口号之间的关系。(提示：对于响应 UDP 目的地应该为发送 UDP 包的地址。) 请将实验结果附在实验报告中。**

- 发送 UDP 数据包：

21970	45.732233	116.179.34.69	172.31.170.250	UDP	163 8829 → 7683 Len=121
26882	73.699603	172.31.170.250	116.179.34.69	UDP	163 7683 → 8829 Len=121
26886	73.743044	116.179.34.69	172.31.170.250	UDP	163 8829 → 7683 Len=121
27130	76.005992	172.31.170.250	202.120.80.2	DNS	77 Standard query 0x5bef...
27131	76.011383	172.31.170.250	202.120.80.2	DNS	83 Standard query 0xa10e...
27132	76.030629	202.120.80.2	172.31.170.250	DNS	153 Standard query respon...
27133	76.030685	202.120.80.2	172.31.170.250	DNS	286 Standard query respon...
27137	76.033676	172.31.170.250	202.120.80.2	DNS	72 Standard query 0xeaf3...
27138	76.036330	202.120.80.2	172.31.170.250	DNS	214 Standard query respon...
27141	76.063526	172.31.170.250	202.120.80.2	DNS	82 Standard query 0xfd79...
27224	76.093282	202.120.80.2	172.31.170.250	DNS	210 Standard query respon...

> Frame 26882: 163 bytes on wire (1304 bits), 163 bytes captured (1304 bits) on interface 0

> Ethernet II, Src: ChongqingFug\_83:a3:c5 (c0:b5:d7:83:a3:c5), Dst: NewH3CTech\_7b:38:02 (54:c6:ff:7b:38:02)

> Internet Protocol Version 4, Src: 172.31.170.250, Dst: 116.179.34.69

> User Datagram Protocol, Src Port: 7683, Dst Port: 8829

Source Port: 7683

Destination Port: 8829

Length: 129

Checksum: 0x5ad1 [unverified]

[Checksum Status: Unverified]

[Stream index: 14]

> [Timestamps]

UDP payload (121 bytes)

> Data (121 bytes)

0000 54 c6 ff 7b 38 02 c0 b5  
0010 00 95 2c 7f 00 00 80 11  
0020 22 45 1e 03 22 7d 00 81  
0030 8d b8 00 10 40 06 02 00  
0040 3d 66 26 00 00 00 00 00  
0050 ca 67 5f 2f 2c 0e 02 05  
0060 e2 20 f4 90 58 70 7d 44  
0070 64 16 6b 0f 56 64 61 c5  
0080 5a 26 5d bc 44 76 55 d4  
0090 f8 40 01 00 b8 00 91 06  
00a0 9f 1d 7e

➤ 响应 UDP 数据包：

21970	45.732233	116.179.34.69	172.31.170.250	UDP	163 8829 → 7683 Len=121
26882	73.699603	172.31.170.250	116.179.34.69	UDP	163 7683 → 8829 Len=121
26886	73.743044	116.179.34.69	172.31.170.250	UDP	163 8829 → 7683 Len=121
27130	76.005992	172.31.170.250	202.120.80.2	DNS	77 Standard query 0x5bef...
27131	76.011383	172.31.170.250	202.120.80.2	DNS	83 Standard query 0xa10e...
27132	76.030629	202.120.80.2	172.31.170.250	DNS	153 Standard query respon...
27133	76.030685	202.120.80.2	172.31.170.250	DNS	286 Standard query respon...
27137	76.033676	172.31.170.250	202.120.80.2	DNS	72 Standard query 0xeaf3...
27138	76.036330	202.120.80.2	172.31.170.250	DNS	214 Standard query respon...
27141	76.063526	172.31.170.250	202.120.80.2	DNS	82 Standard query 0xfd79...
27224	76.093282	202.120.80.2	172.31.170.250	DNS	210 Standard query respon...

> Frame 26886: 163 bytes on wire (1304 bits), 163 bytes captured (1304 bits) on interface 0

> Ethernet II, Src: NewH3CTech\_7b:38:02 (54:c6:ff:7b:38:02), Dst: ChongqingFug\_83:a3:c5 (c0:b5:d7:83:a3:c5)

> Internet Protocol Version 4, Src: 116.179.34.69, Dst: 172.31.170.250

> User Datagram Protocol, Src Port: 8829, Dst Port: 7683

Source Port: 8829

Destination Port: 7683

Length: 129

Checksum: 0x8d4b [unverified]

[Checksum Status: Unverified]

[Stream index: 14]

> [Timestamps]

UDP payload (121 bytes)

> Data (121 bytes)

0000 c0 b5 d7 83 a3 c5 54 c6  
0010 00 95 86 d0 40 00 23 11  
0020 aa fa 22 7d 1e 03 00 81  
0030 8d b8 00 10 40 07 02 00  
0040 3d 66 26 00 00 00 00 00  
0050 b4 36 31 32 9f de c3 a4  
0060 9c 71 9a 8d eb a0 bc e9  
0070 1a 47 05 12 e5 b4 a0 64  
0080 24 77 33 8f 6e 14 4b 5c  
0090 3a 77 a8 20 ce ad 44 38  
00a0 b5 cd 29

➤ 数据包中端口号之间的关系：

通过观察上面两图中发送 UDP 数据包后接收响应的 UDP 数据包，两个数据包的端口号**对应相反**。发送方的源端口号作为响应方的目标端口号，发送方的目标端口号作为响应方的源端口号。

## 二、总结

这次上机实验主要就是使用 Wireshark 来捕获 UDP 数据包，去深入了解 UDP 协议的工作原理，包括 UDP 协议的首部字段、长度字段、有效负载最大字节数以及发送和接收 UDP 数据包之间的关系。

在实验过程中，我完成了四个实验任务：

Task 1:我从跟踪中选择一个 UDP 数据包, 识别、确定了 UDP 首部字段(包括源端口号、目的端口号、长度字段和校验和字段)。这些字段很重要: 源端口号和目的端口号用于标识通信的源和目的地, 长度字段表示整个 UDP 数据包的长度, 校验和字段用于检测数据包是否损坏或丢失。

Task 2: 我对 UDP 首部长度字段进行了分析, 知道了 UDP 首部中的长度字段指的是整个 UDP 数据包的长度(包括首部和有效负载部分)。这种设计有助于接收端正确解析 UDP 数据报文, 并提取出有效载荷部分进行处理。

Task 3: 我又根据 pdf 提供的百度百科的有效负载定义, 去探究 UDP 的有效负载。其中可包含的最大字节数取决于网络配置、MTU 大小以及捕获设备的能力等因素。通常情况下, UDP 数据包的大小不能超过网络链路的 MTU 大小。我们进行了实验验证, 并得出了 UDP 有效负载的最大字节数。

Task 4:我观察了发送 UDP 数据包后接收到的响应 UDP 数据包。响应 UDP 数据包的目的地应为发送 UDP 包的地址, 并且端口号之间对应相反。

通过这次实验, 我加深了对 UDP 协议工作原理的理解, 对于我进一步理解课本上有关网络通信和网络协议的知识有重要意义。