山东大学 计算机 学院

计算机网络 课程实验报告

学号：202400130240	姓名： 贾宗翰	班级： 24.6
实验题目： Wireshark Lab:UDP v8.1		
实验学时：2h	实验日期： 2025.9.22	
实验目的： 通过 wireshark 抓包并分析 UDP 内容		
硬件环境： 联想拯救者		
软件环境： Wireshark，edge 浏览器		

实验步骤与内容：

1. 开启 wireshark，并使用 nslookup 查找：

```
C:\Users\jiazonghan>nslookup www.nyu.edu
服务器:  UnKnown
Address:  192.168.254.245

非权威应答:
名称:    d1q5ku5vnwkd2k.cloudfront.net
Addresses:  2600:9000:221a:2800:1:f7e2:cb00:93a1
          2600:9000:221a:fc00:1:f7e2:cb00:93a1
          2600:9000:221a:1a00:1:f7e2:cb00:93a1
          2600:9000:221a:d400:1:f7e2:cb00:93a1
          2600:9000:221a:4a00:1:f7e2:cb00:93a1
          2600:9000:221a:2c00:1:f7e2:cb00:93a1
          2600:9000:221a:b000:1:f7e2:cb00:93a1
          2600:9000:221a:dc00:1:f7e2:cb00:93a1
          18.65.185.51
          18.65.185.118
          18.65.185.7
          18.65.185.68
Aliases:  www.nyu.edu
```

抓包结果：

232	9.696917	192.168.254.245	101.76.243.171	DNS	123	Standard query response 0x0001 No such name PTR 245.254
233	9.698053	101.76.243.171	192.168.254.245	DNS	71	Standard query 0x0002 A www.nyu.edu
234	9.698285	192.168.254.245	101.76.243.171	DNS	178	Standard query response 0x0002 A www.nyu.edu CNAME d1q5
235	9.700088	101.76.243.171	192.168.254.245	DNS	71	Standard query 0x0003 AAAA www.nyu.edu
236	9.704904	192.168.254.245	101.76.243.171	DNS	338	Standard query response 0x0003 AAAA www.nyu.edu CNAME d

结论分析与体会：

```
> Frame 233: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{8D0CDAB8-A5C2-4E9C-
> Ethernet II, Src: LCFCElectron_cb:90:63 (c4:c6:e6:cb:90:63), Dst: JuniperNetwo_f6:12:a0 (28:a2:4b:f6:12:a0)
> Internet Protocol Version 4, Src: 101.76.243.171, Dst: 192.168.254.245
v User Datagram Protocol, Src Port: 56621, Dst Port: 53
    Source Port: 56621
    Destination Port: 53
    Length: 37
    Checksum: 0x18cd [unverified]
    [Checksum Status: Unverified]
    [Stream index: 9]
    [Stream Packet Number: 1]
  > [Timestamps]
    UDP payload (29 bytes)
v Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 234]
```

1.

数据包编号是 233，携带的是 DNS，有四个字段：Source port,Destination port,Length,Checksum;

2.每一个字段长度都是 2 字节，一共是 2*4=8 字节。

```
0000  28 a2 4b f6 12 a0 c4
0010  00 39 23 f9 00 00 80
0020  fe f5 dd 2d 00 35 00
0030  00 00 00 00 00 00 03
0040  64 75 00 00 01 00 01
```

3.Length 字节是 37，观察：

```
> Internet Protocol Version 4, Src:
v User Datagram Protocol, Src Port:
    Source Port: 56621
    Destination Port: 53
    Length: 37
```

得知 37 = 29+8(payload+header)

4.由 2 分析 length 占 2 字节，16 比特，总就是 2^16,除去 header 所以 payload 最长可以是（2^16-8）= 65528 bytes。

5.端口占 2 字节，所以最大表示的数字就是 2^(2*8)-1 = 2^16 - 1 = 65535

6.见下图 protocol：

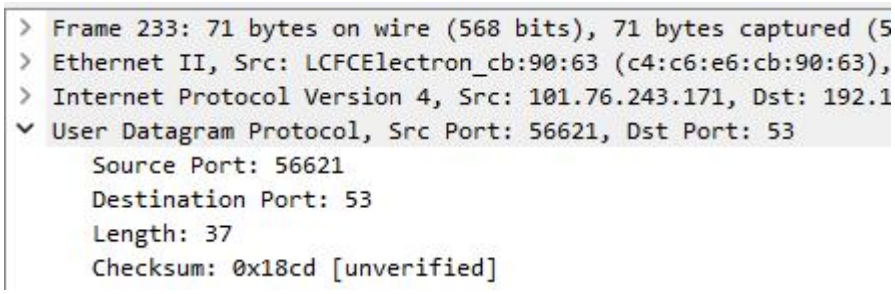
```
    [Coloring Rule String: udp]
v Ethernet II, Src: LCFCElectron_cb:90:63 (c4:c6:e6:cb:90:63), Dst: JuniperNetwo_f6:12:a0 (28:a2:4b:f6:12:a0)
  > Destination: JuniperNetwo_f6:12:a0 (28:a2:4b:f6:12:a0)
  > Source: LCFCElectron_cb:90:63 (c4:c6:e6:cb:90:63)
    Type: IPv4 (0x0800)
    [Stream index: 0]
v Internet Protocol Version 4, Src: 101.76.243.171, Dst: 192.168.254.245
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 57
    Identification: 0x23f9 (9209)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
```

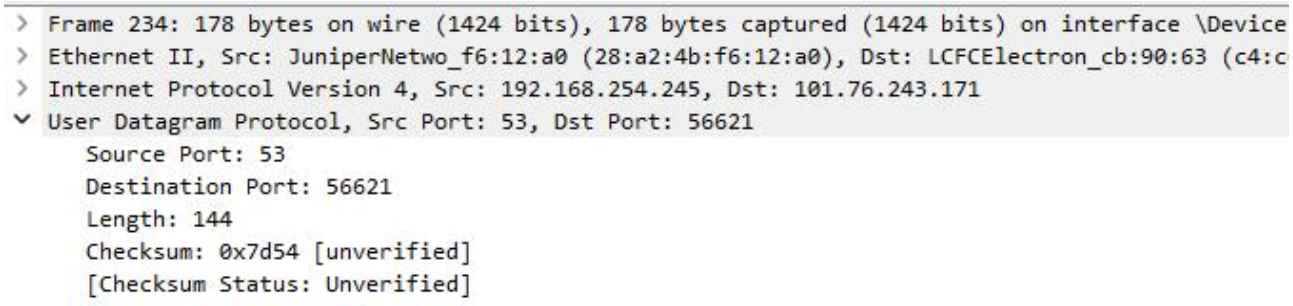
```
0000  28 a2 4b f6 12 a0 c4 c6  e6 cb
0010  00 39 23 f9 00 00 80 11  00 00
0020  fe f5 dd 2d 00 35 00 25  18 cd
0030  00 00 00 00 00 00 03 77  77 77
0040  64 75 00 00 01 00 01
```

分析结果是 0x11 = 17.

7. 观察 233 与 234：

```
  233 9.698053    101.76.243.171    192.168.254.245    DNS     71 Standard query 0x0002 A www.nyu.edu
  234 9.698285    192.168.254.245   101.76.243.171     DNS    178 Standard query response 0x0002 A www.nyu.edu
```





发现 DNS 查询的源端口号（56621）和目的端口号（53）分别与 DNS 查询响应的目的端口号（53）和源端口号相对应（56621）

通过此次实验，我对于 UDP 有了更深刻的理解。