实验步骤

由于DNS协议是运行在UDP之上的,故可用nslookup进行查询网站来抓包

- 1.清除浏览器等的缓存
- 2.打开Wireshark, 开始捕获
- 3.进入命令窗口,输入nslookup www.mit.edu

```
Microsoft Windows [版本 10.0.19042.1237]
(c) Microsoft Corporation。保留所有权利。

C:\Users\Eiffel>nslookup www.mit.edu
服务器: UnKnown
Address: fe80::819:e2aa:2497:5256

非权威应答:
名称: e9566.dscb.akamaiedge.net
Addresses: 2600:140e:6:a83::255e
2600:140e:6:ab3::255e
23.7.172.76

Aliases: www.mit.edu
www.mit.edu.edgekey.net
```

4.停止捕获

题目

1. Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. (You shouldn't look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields.

4个:源端口号、目的端口号、长度、检验和

```
Vuser Datagram Protocol, Src Port: 4012, Dst Por
Source Port: 4012
Destination Port: 8000
Length: 55
Checksum: 0x76c2 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
> [Timestamps]
UDP payload (47 bytes)
Data (47 bytes)
```

2. By consulting the displayed information in Wireshark's packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.

```
Source Port: 4012
  Destination Port: 8000
  Length: 55
  Checksum: 0x76c2 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
> [Timestamps]
  UDP payload (47 bytes)
Data (47 bytes)
000
    b6 85 e1 05 57 64 74 4c a1 da 20 a1
    00 4b 63 d5 00 00 40 11 f0 88 ac 14
10
    fa 72 <mark>0f ac</mark> 1f 40 00 37 76 c2 02 3a
)20
    87 91 f8 3d 6d 02 00 00
                              00 01 01 01
)30
)40
    94 23 65 3e 70 c2 13 5e
                              5a 51 96 fe
    81 0c b7 99 e1 fd eb bf
                              03
)50
  / User Datagram Protocol, Src Port:
      Source Port: 4012
      Destination Port: 8000
      Length: 55
      Checksum: 0x76c2 [unverified]
      [Checksum Status: Unverified]
      [Stream index: 0]
    > [Timestamps]
      UDP payload (47 bytes)
   Data (47 bytes)
        b6 85 e1 05 57 64 74 4c
  0006
                                  a1 d
  010
        00 4b 63 d5 00 00 40 11
                                  f0 8
  3020 fa 72 0f ac 1f 40 00 37
                                  76 c
  3030 87 91 f8 3d 6d 02 00 00
                                  00 0
```

USER Datagram Protocol, Src Port: 4012,

```
/ Internet Protocol version 4, Sit. 1/2.20
 Vuser Datagram Protocol, Src Port: 4012, I
      Source Port: 4012
      Destination Port: 8000
      Length: 55
      Checksum: 0x76c2 [unverified]
      [Checksum Status: Unverified]
      [Stream index: 0]
    > [Timestamps]
      UDP payload (47 bytes)
 Data (47 bytes)
  0000 b6 85 e1 05 57 64 74 4c a1 da 20 a1
  0010 00 4b 63 d5 00 00 40 11 f0 88 ac 14
  0020 fa 72 0f ac 1f 40 00 37 76 c2 02 3a
  0030 87 91 f8 3d 6d 02 00 00 00 01 01 01
  0040 94 23 65 3e 70 c2 13 5e 5a 51 96 f0
  0050 81 0c b7 99 e1 fd eb bf 03
> Frame 7: 89 bytes on wire (712 bits), 89 byt
> Ethernet II, Src: LiteonTe da:20:a1 (74:4c:a
> Internet Protocol Version 4, Src: 172.20.10.
V User Datagram Protocol, Src Port: 4012, Dst
    Source Port: 4012
    Destination Port: 8000
    Length: 55
    Checksum: 0x76c2 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (47 bytes)
Data (47 bytes)
      b6 85 e1 05 57 64 74 4c a1 da 20 a1 08
0000
      00 4b 63 d5 00 00 40 11 f0 88 ac 14 0a
0010
0020 fa 72 0f ac 1f 40 00 37
                               76 c2 02 3a 21
0030 87 91 f8 3d 6d 02 00 00 00 01 01 01 00
0040 94 23 65 3e 70 c2 13 5e 5a 51 96 f0 55
0050 81 0c b7 99 e1 fd eb bf 03
```

3. The value in the Length field is the length of what? (You can consult the text for this answer). Verify your claim with your captured UDP packet.

UDP报文段中的字节数。从下图可知,Length中的值为数据的字节数加8,其中,8为UDP报文首部的字节数,故可知Length为UDP报文段的字节数。

```
V User Datagram Protocol, Src Port: 401
    Source Port: 4012
    Destination Port: 8000
    Length: 55
    Checksum: 0x76c2 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (47 bytes)
 Data (47 bytes)
 > Internet Protocol Version 4, Src: 1
 V User Datagram Protocol, Src Port: 8
     Source Port: 8000
     Destination Port: 4012
     Length: 863
     Checksum: 0x6b94 [unverified]
     [Checksum Status: Unverified]
     [Stream index: 0]
   > [Timestamps]
     UDP payload (855 bytes)
  Data (855 bytes)
 v user patagram protocol, Src port: 
     Source Port: 4012
     Destination Port: 8000
    Length: 143
     Checksum: 0xb6eb [unverified]
     [Checksum Status: Unverified]
     [Stream index: 0]
   > [Timestamps]
     UDP payload (135 bytes)
  Data (135 bytes)
```

4. What is the maximum number of bytes that can be included in a UDP payload? (Hint: the answer to this question can be determined by your answer to 2. above)

UDP报文的首部有2 byte 用于记录报文的长度,2 byte = 16 bit, 2^{16} -1=65535,除去首部的8 byte,则应用数据所占的字节数为 65535 - 8 = 65527。

5. What is the largest possible source port number? (Hint: see the hint in 4.) 源端口号为 2 byte,即16 bit, 2^{16} -1 = 65535,故最大端口号为65535。

6. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation. To answer this question, you'll need to look into the Protocol field of the IP datagram containing this UDP segment (see Figure 4.13 in the text, and the discussion of IP header fields).

十六进制: 0x11

十进制: 17

IOTAL Length: 163

Identification: 0x63dc (25564)

> Flags: 0x00

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 64

Protocol: UDP (17)

Header Checksum: 0xf029 [validation disable

[Header checksum status: Unverified]

Source Address: 172.20.10.5

7. Examine a pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet. (Hint: for a second packet to be sent in response to a first packet, the sender of the first packet should be the destination of the second packet). Describe the relationship between the port numbers in the two packets.

第一个UDP报文的源端口(源端口号为4012)是第二个UDP报文的目的端口,而第一个UDP报文的目的端口(目的端口号为8000)则是第二个UDP报文的源端口。

2 COST TO TO 02:20:02:02:04:20 II1:104:520:II4	1/2.20.10.3	OTCA	DID OTCK I LOCOCOT	
4 2021-10-10 09:36:05.651145 172.20.10.5	117.184.250.114	OICQ	89 OICQ Protocol	
5 2021-10-10 09:36:05.651289 172.20.10.5	117.184.250.114	OICQ	81 OICO Protocol	
7 2021-10-10 09:36:05.671563 172.20.10.5	117.184.250.114	UDP	89 4012 → 8000 Len=47	
8 2021-10-10 09:36:05.752662 117.184.250.114	172.20.10.5	OICQ	873 OICQ Protocol	
9 2021-10-10 09:36:05.752804 117.184.250.114	172.20.10.5	OICQ	913 OICO Protocol	
10 2021-10-10 09:36:05.752804 117.184.250.114	172.20.10.5	UDP	897 <mark>8000 → 4012 Len=855 -</mark>	
11 2021-10-10 09:36:05.753559 172.20.10.5	117.184.250.114	OICQ	89 OICQ Protocol	
12 2021-10-10 09:36:05.753675 172.20.10.5	117.184.250.114	OICQ	81 OICQ Protocol	