

COMP 3203 Wireshark 5

Name: Nirmith Victor D'Almeida

Number: 101160124

1. Using Professor's downloaded packets

30	39.796777	192.168.1.1...	68.87.71.226	DNS	87	Standard query response 0x0002 NS mit.edu.hsd1.ma.comcast.net
31	39.823784	68.87.71.226	192.168.1.1...	DNS	167	Standard query response 0x0002 No such name NS mit.edu.hsd1.ma.comcast.net
32	39.825175	192.168.1.1...	68.87.71.226	DNS	82	Standard query 0x0003 NS mit.edu.ma.comcast.net

> Frame 30: 87 bytes on wire (696 bits), 87 bytes captured (696 bits)

> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)

> Internet Protocol Version 4, Src: 192.168.1.101, Dst: 68.87.71.226

> User Datagram Protocol, Src Port: 4377, Dst Port: 53

Source Port: 4377

Destination Port: 53

Length: 53

Checksum: 0xfa77 [unverified]

[Checksum Status: Unverified]

[Stream index: 5]

> [Timestamps]

UDP payload (45 bytes)

> Domain Name System (query)

There are 5 Fields: source Port, Destination Port, Length, Checksum and UDP Payload

If we include statuses index and timestamps there will be 8 fields.

2. Using the same packets as in q1

> User Datagram Protocol, Src Port: 4377, Dst Port: 53									
Source Port: 4377									
Destination Port: 53									
Length: 53									
Checksum: 0xfa77 [unverified]									
[Checksum Status: Unverified]									
[Stream index: 5]									
> [Timestamps]									
UDP payload (45 bytes)									
> Domain Name System (query)									

0020 47 e2 11 19 00 35 00 35 fa 77 00 02 01 00 00 01 G...5.5 .w.....

0030 00 00 00 00 00 00 03 6d 69 74 03 65 64 75 04 68m it-edu-h

0040 73 64 31 02 6d 61 07 63 6f 6d 63 61 73 74 03 6e sd1-ma-c omcast-n

0050 65 74 00 00 02 00 01 et.....

Details at: https://www.wireshark.org/docs/wsug_html_chunked/ChAdvChecksums.html (udp.checksum), 2 bytes

length of each UDP header fields is 2 bytes

3. Using the same packet for reference

we see that 8 bytes UDP (pic 1 related) is added with 45 bytes payload totaling 53 bytes (pic 2)

Wireshark packet capture analysis showing a DNS query packet. The packet list shows a User Datagram Protocol (UDP) packet of 8 bytes. The packet details pane shows the UDP payload (45 bytes) and the Domain Name System (query) section. The packet bytes pane shows the raw data of the packet.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
30	39.796777	192.168.1.1...	68.87.71.226	DNS	87	Standard query 0x0002 NS mit.edu.hsd1.ma.comcast.net
31	39.823784	68.87.71.226	192.168.1.1	DNS	167	Standard query response 0x0002 No such name NS mit.edu.hsd1.ma.comcast.net

Packet Details:

- Frame 30: 87 bytes on wire (696 bits), 87 bytes captured (696 bits)
- Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
- Internet Protocol Version 4, Src: 192.168.1.101, Dst: 68.87.71.226
- User Datagram Protocol, Src Port: 4377, Dst Port: 53
 - Source Port: 4377
 - Destination Port: 53
 - Length: 53
 - Checksum: 0xfa77 [unverified]
 - [Checksum Status: Unverified]
 - [Stream index: 5]

Packet Bytes:

```

0000 00 16 b6 f4 eb a8 00 08 74 4f 36 23 08 00 45 00 .....tO6#..E.
0010 00 49 3d 91 00 00 80 11 ae cc c0 a8 01 65 44 57 .I=.....eDW
0020 47 e2 11 19 00 35 00 35 fa 77 00 02 01 00 00 01 G...5.5.w.....
0030 00 00 00 00 00 00 03 6d 69 74 03 65 64 75 04 68 .....m it.edu.h
0040 73 64 31 02 6d 61 07 63 6f 6d 63 61 73 74 03 6e sd1.ma.c omcast.n
0050 65 74 00 00 02 00 01 et.....
  
```

Packet Details (User Datagram Protocol (udp), 8 bytes):

- Timestamps
- UDP payload (45 bytes)
- Domain Name System (query)

Packet Bytes (Domain Name System (dns), 45 bytes):

```

0000 00 16 b6 f4 eb a8 00 08 74 4f 36 23 08 00 45 00 .....tO6#..E.
0010 00 49 3d 91 00 00 80 11 ae cc c0 a8 01 65 44 57 .I=.....eDW
0020 47 e2 11 19 00 35 00 35 fa 77 00 02 01 00 00 01 G...5.5.w.....
0030 00 00 00 00 00 00 03 6d 69 74 03 65 64 75 04 68 .....m it.edu.h
0040 73 64 31 02 6d 61 07 63 6f 6d 63 61 73 74 03 6e sd1.ma.c omcast.n
0050 65 74 00 00 02 00 01 et.....
  
```

4. The largest possible source port number is $2^{16} - 1 = 65536 - 1 = 65535$
 Header bytes is 8 bytes (from q3 pic 1)
 Therefore maximum number of bytes is largest possible – header bytes
 = $65535 - 8 = 65527$ bytes

5. The largest possible source port number is $2^{16} - 1 = 65536 - 1 = 65535$

6. The Protocol number for the UDP for the packet number 30 is 17 and hexadecimal notation is 0×11

30	39.796777	192.168.1.1...	68.87.71.226	DNS	87 Standard query 0x0002 NS mit.edu.hsd1.ma.comcast.net
31	39.823784	68.87.71.226	192.168.1.1...	DNS	167 Standard query response 0x0002 No such name NS mit.edu.h

0100 = Version: 4
.... 0101	= Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00	(DSCP: CS0, ECN: Not-ECT)
Total Length: 73	
Identification: 0x3d91	(15761)
> Flags: 0x00	
...0 0000 0000 0000	= Fragment Offset: 0
Time to Live: 128	
Protocol: UDP (17)	
Header Checksum: 0xaecc	[validation disabled]
[Header checksum status: Unverified]	
Source Address: 192.168.1.101	
Destination Address: 68.87.71.226	
User Datagram Protocol, Src Port: 4377, Dst Port: 53	
Domain Name System (query)	

3000	00 16 b6 f4 eb a8 00 08	74 4f 36 23 08 00 45 00 t06#..E-
3010	00 49 3d 91 00 00 80 11	ae cc c0 a8 01 65 44 57	-I=.....eDW
3020	47 e2 11 19 00 35 00 35	fa 77 00 02 01 00 00 01	G....5-5 -w-.....
3030	00 00 00 00 00 00 03 6d	69 74 03 65 64 75 04 68m it-edu-h
3040	73 64 31 02 6d 61 07 63	6f 6d 63 61 73 74 03 6e	sd1-ma-c omcast-n
3050	65 74 00 00 02 00 01		et.....

7. UDP packet sent by host

30	39.796777	192.168.1.1...	68.87.71.226	DNS	87 Standard query 0x0002 NS mit.edu.hsd1.ma.comcast.net
31	39.823784	68.87.71.226	192.168.1.1	DNS	167 Standard query response 0x0002 No such name NS mit.edu

> Frame 30: 87 bytes on wire (696 bits), 87 bytes captured (696 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
> Internet Protocol Version 4, Src: 192.168.1.101, Dst: 68.87.71.226
> User Datagram Protocol, Src Port: 4377, Dst Port: 53
Source Port: 4377
Destination Port: 53
Length: 53
Checksum: 0xfa77 [unverified]
[Checksum Status: Unverified]
[Stream index: 5]
> [Timestamps]
[Time since first frame: 0.00000000 seconds]

UDP packet reply to host

31	39.823784	68.87.71.226	192.168.1.1...	DNS	167 Standard query response 0x0002 No such name NS mit.edu.hsd1.ma.comcast.net SOA dns1.inflow.pa.bo.comcast.net
32	39.825175	192.168.1.1...	68.87.71.226	DNS	82 Standard query 0x0003 NS mit.edu.ma.comcast.net
33	39.838373	68.87.71.226	192.168.1.1	DNS	82 Standard query response 0x0003 Server failure NS mit.edu.ma.comcast.net

> Frame 31: 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits)
> Ethernet II, Src: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
> Internet Protocol Version 4, Src: 68.87.71.226, Dst: 192.168.1.101
> User Datagram Protocol, Src Port: 53, Dst Port: 4377
Source Port: 53
Destination Port: 4377
Length: 133
Checksum: 0x04d3 [unverified]
[Checksum Status: Unverified]
[Stream index: 5]
> [Timestamps]
[Time since first frame: 0.027007000 seconds]
[Time since previous frame: 0.027007000 seconds]
UDP payload (125 bytes)
Domain Name System (response)

The relationship between the port numbers in the two above packets is that the source port sent by host is equal to destination port for the response and the Destination port sent by host is the source port for the reply back to the host.