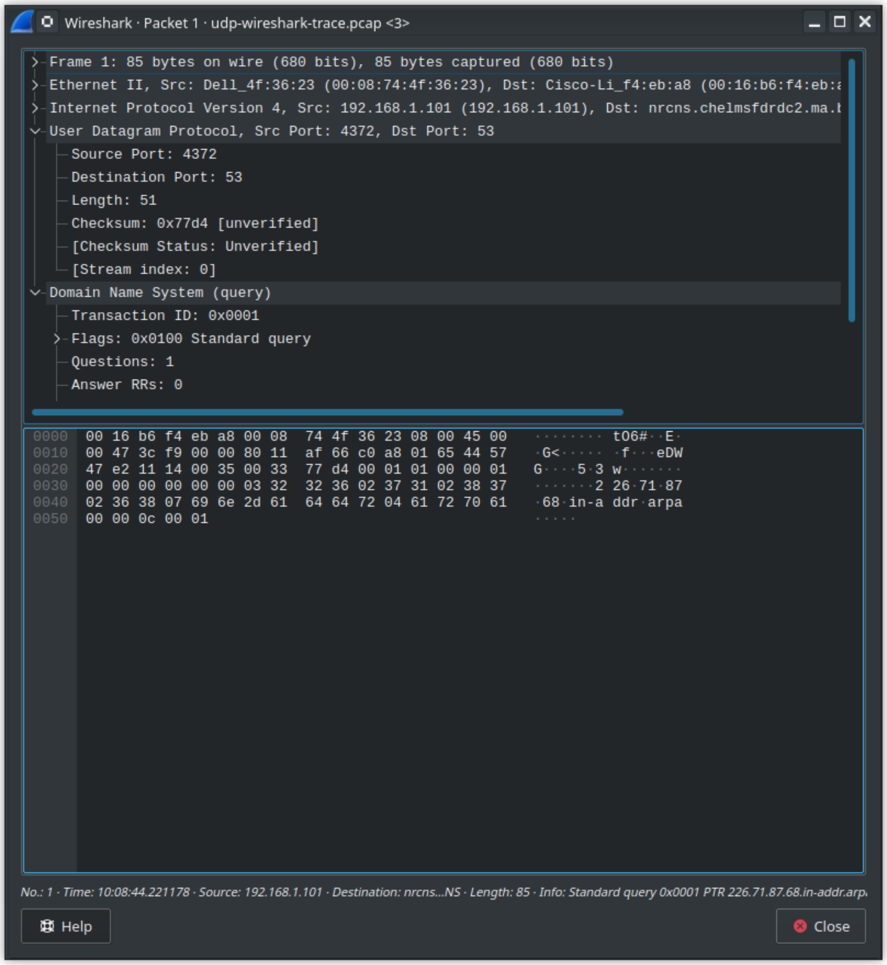
Mark Lam
2 October 2019
Computer Networking

Wireshark Lab 2

1. There are four fields in the UDP header: source port, destination port, length, and checksum.
2. Each header field is 2 bytes.
3. The Length field is the length of headers, 8 bytes, and the data bytes. This packet is has 43 bytes of data.
4. The maximum number of bytes that can be used with UDP is 2^16 – the headers, 65527 bytes.
5. The largest possible source pot is 65535
6. The protocol number is 17 or 0x11.
7. The two packets use the same two ports but in different fields. The first packet has src port of 4372 and dst port 53 and the second packet had src port 53 and dst port 4372

1.

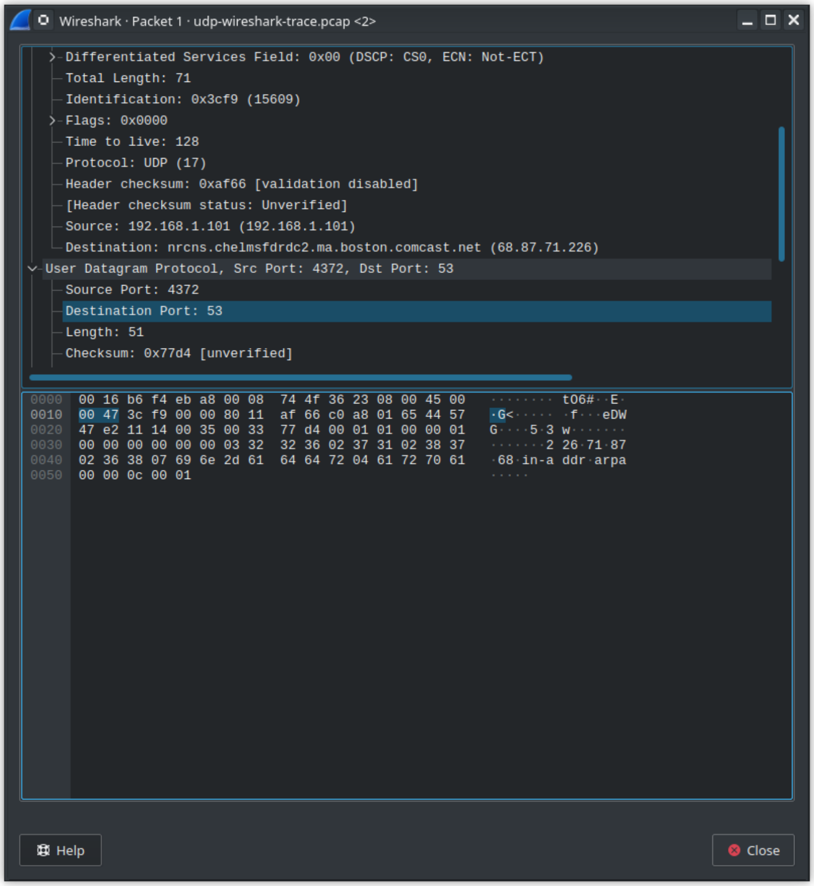


```
> Frame 1: 85 bytes on wire (680 bits), 85 bytes captured (680 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a
> Internet Protocol Version 4, Src: 192.168.1.101 (192.168.1.101), Dst: nrcns.chelmsfdrdc2.ma.b
v User Datagram Protocol, Src Port: 4372, Dst Port: 53
    Source Port: 4372
    Destination Port: 53
    Length: 51
    Checksum: 0x77d4 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
v Domain Name System (query)
    Transaction ID: 0x0001
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0

0000  00 16 b6 f4 eb a8 00 08  74 4f 36 23 08 00 45 00   ········ tO6#··E·
0010  00 47 3c f9 00 00 80 11  af 66 c0 a8 01 65 44 57   ·G<····· ·f···eDW
0020  47 e2 11 14 00 35 00 33  77 d4 00 01 01 00 00 01   G····5·3 w·······
0030  00 00 00 00 00 00 03 32  32 36 02 37 31 02 38 37   ·······2 26·71·87
0040  02 36 38 07 69 6e 2d 61  64 64 72 04 61 72 70 61   ·68·in-a ddr·arpa
0050  00 00 0c 00 01                                     ·····
```

No.: 1 · Time: 10:08:44.221178 · Source: 192.168.1.101 · Destination: nrcns...NS · Length: 85 · Info: Standard query 0x0001 PTR 226.71.87.68.in-addr.arp

6.

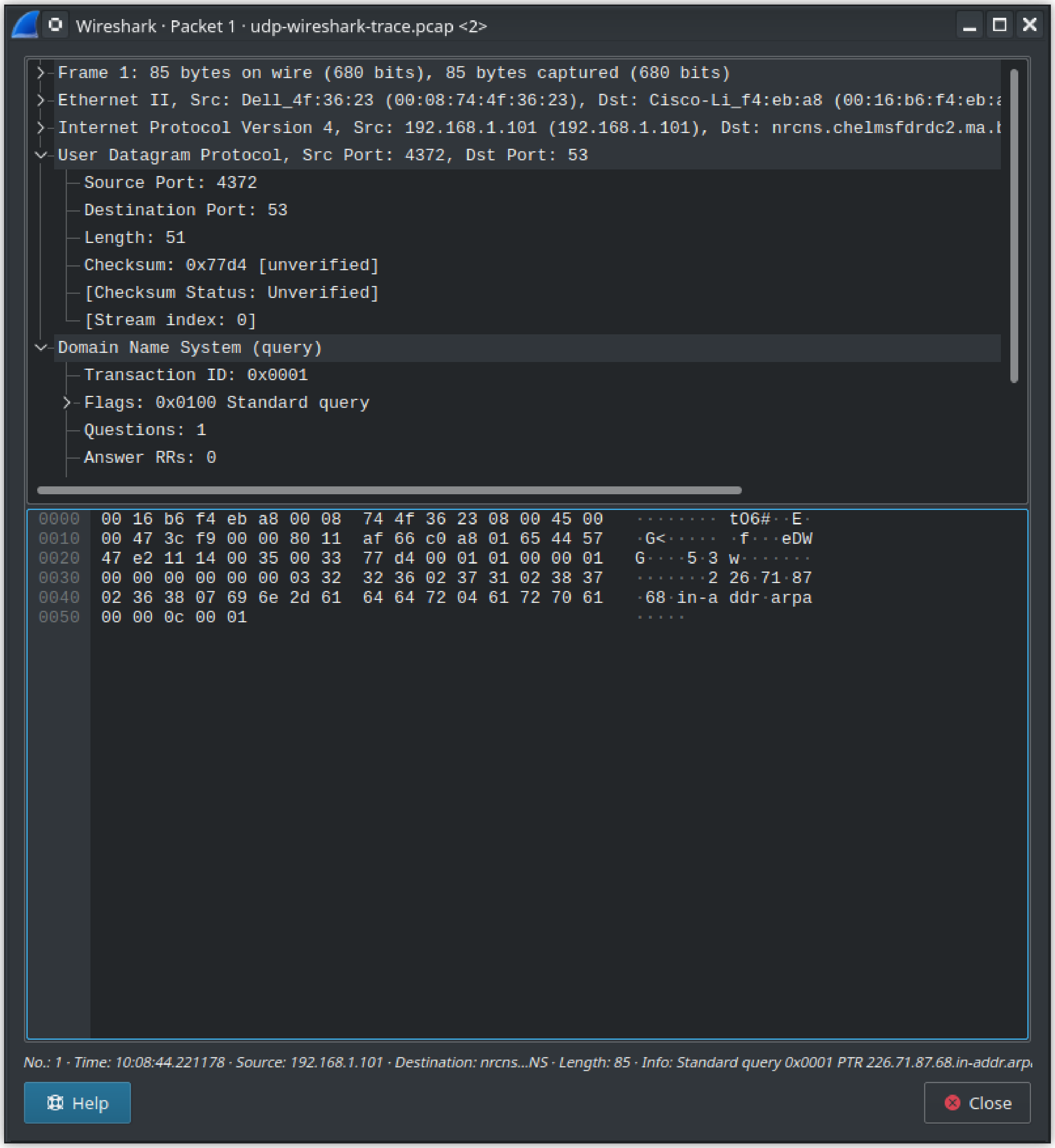


Wireshark · Packet 1 · udp-wireshark-trace.pcap <2>

```
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 71
    Identification: 0x3cf9 (15609)
  > Flags: 0x0000
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0xaf66 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.101 (192.168.1.101)
    Destination: nrcns.chelmsfdrdc2.ma.boston.comcast.net (68.87.71.226)
v User Datagram Protocol, Src Port: 4372, Dst Port: 53
    Source Port: 4372
    Destination Port: 53
    Length: 51
    Checksum: 0x77d4 [unverified]
```

```
0000  00 16 b6 f4 eb a8 00 08  74 4f 36 23 08 00 45 00   ········ tO6#··E·
0010  00 47 3c f9 00 00 80 11  af 66 c0 a8 01 65 44 57   ·G<····· ·f···eDW
0020  47 e2 11 14 00 35 00 33  77 d4 00 01 01 00 00 01   G····5·3 w·······
0030  00 00 00 00 00 00 03 32  32 36 02 37 31 02 38 37   ·······2 26·71·87
0040  02 36 38 07 69 6e 2d 61  64 64 72 04 61 72 70 61   ·68·in-a ddr·arpa
0050  00 00 0c 00 01                                     ·····
```

7.

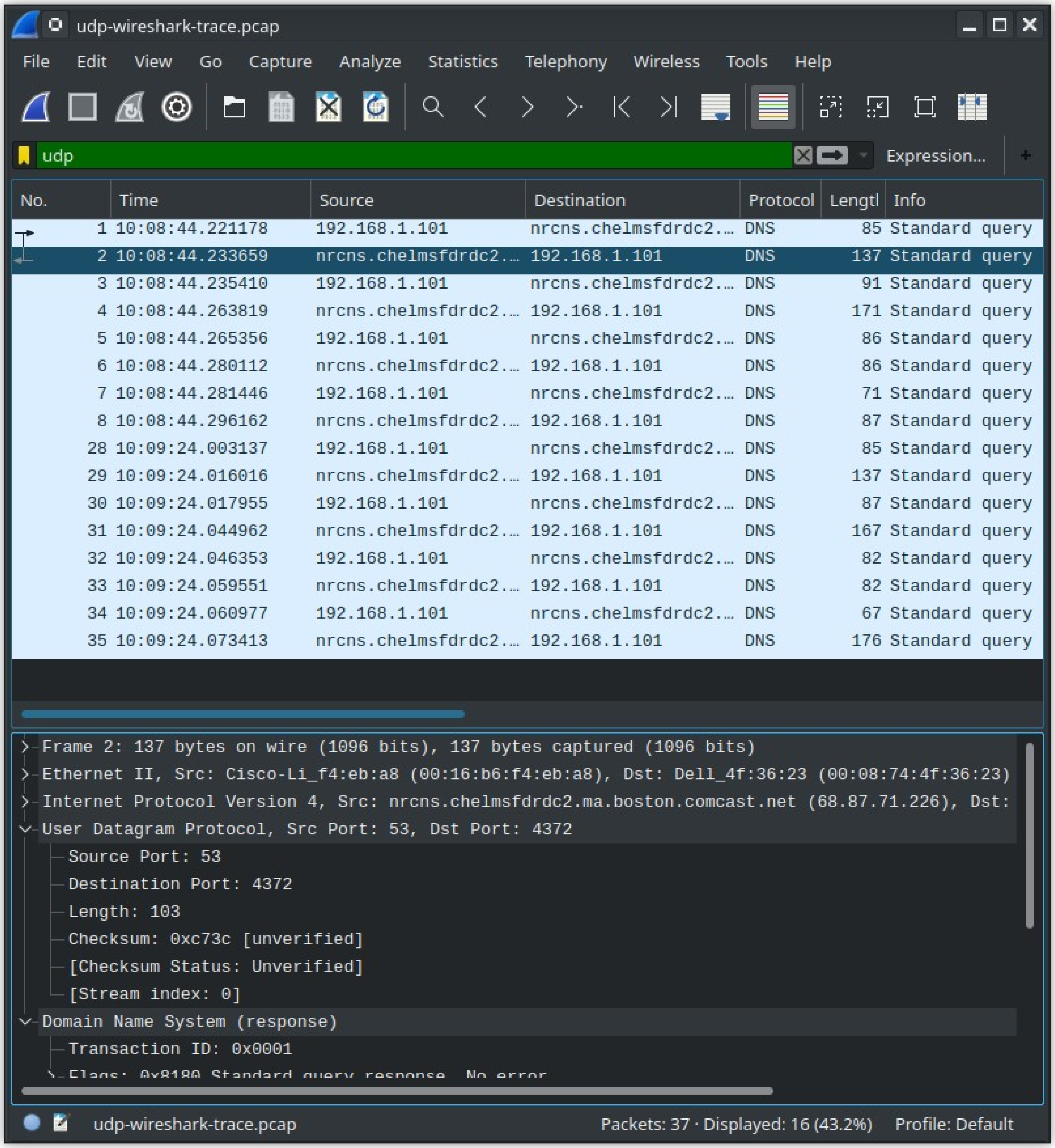


Wireshark · Packet 1 · udp-wireshark-trace.pcap <2>

```
> Frame 1: 85 bytes on wire (680 bits), 85 bytes captured (680 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:a
> Internet Protocol Version 4, Src: 192.168.1.101 (192.168.1.101), Dst: nrcns.chelmsfdrdc2.ma.b
v User Datagram Protocol, Src Port: 4372, Dst Port: 53
    Source Port: 4372
    Destination Port: 53
    Length: 51
    Checksum: 0x77d4 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
v Domain Name System (query)
    Transaction ID: 0x0001
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
```

```
0000  00 16 b6 f4 eb a8 00 08  74 4f 36 23 08 00 45 00   ········ tO6#··E·
0010  00 47 3c f9 00 00 80 11  af 66 c0 a8 01 65 44 57   ·G<····· ·f···eDW
0020  47 e2 11 14 00 35 00 33  77 d4 00 01 01 00 00 01   G····5·3 w·······
0030  00 00 00 00 00 00 03 32  32 36 02 37 31 02 38 37   ·······2 26·71·87
0040  02 36 38 07 69 6e 2d 61  64 64 72 04 61 72 70 61   ·68·in-a ddr·arpa
0050  00 00 0c 00 01                                      ·····
```

No.: 1 · Time: 10:08:44.221178 · Source: 192.168.1.101 · Destination: nrcns...NS · Length: 85 · Info: Standard query 0x0001 PTR 226.71.87.68.in-addr.arp



```
udp
```

```
No.   Time             Source              Destination         Protocol Lengtl Info
    1 10:08:44.221178  192.168.1.101       nrcns.chelmsfdrdc2.… DNS          85 Standard query
    2 10:08:44.233659  nrcns.chelmsfdrdc2.… 192.168.1.101      DNS         137 Standard query
    3 10:08:44.235410  192.168.1.101       nrcns.chelmsfdrdc2.… DNS          91 Standard query
    4 10:08:44.263819  nrcns.chelmsfdrdc2.… 192.168.1.101      DNS         171 Standard query
    5 10:08:44.265356  192.168.1.101       nrcns.chelmsfdrdc2.… DNS          86 Standard query
    6 10:08:44.280112  nrcns.chelmsfdrdc2.… 192.168.1.101      DNS          86 Standard query
    7 10:08:44.281446  192.168.1.101       nrcns.chelmsfdrdc2.… DNS          71 Standard query
    8 10:08:44.296162  nrcns.chelmsfdrdc2.… 192.168.1.101      DNS          87 Standard query
   28 10:09:24.003137  192.168.1.101       nrcns.chelmsfdrdc2.… DNS          85 Standard query
   29 10:09:24.016016  nrcns.chelmsfdrdc2.… 192.168.1.101      DNS         137 Standard query
   30 10:09:24.017955  192.168.1.101       nrcns.chelmsfdrdc2.… DNS          87 Standard query
   31 10:09:24.044962  nrcns.chelmsfdrdc2.… 192.168.1.101      DNS         167 Standard query
   32 10:09:24.046353  192.168.1.101       nrcns.chelmsfdrdc2.… DNS          82 Standard query
   33 10:09:24.059551  nrcns.chelmsfdrdc2.… 192.168.1.101      DNS          82 Standard query
   34 10:09:24.060977  192.168.1.101       nrcns.chelmsfdrdc2.… DNS          67 Standard query
   35 10:09:24.073413  nrcns.chelmsfdrdc2.… 192.168.1.101      DNS         176 Standard query
```

```
> Frame 2: 137 bytes on wire (1096 bits), 137 bytes captured (1096 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: nrcns.chelmsfdrdc2.ma.boston.comcast.net (68.87.71.226), Dst:
v User Datagram Protocol, Src Port: 53, Dst Port: 4372
    Source Port: 53
    Destination Port: 4372
    Length: 103
    Checksum: 0xc73c [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
v Domain Name System (response)
    Transaction ID: 0x0001
  > Flags: 0x8180 Standard query response, No error
```

```
udp-wireshark-trace.pcap                Packets: 37 · Displayed: 16 (43.2%)    Profile: Default
```