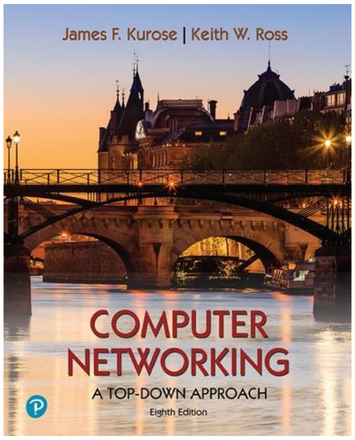
2151013087

Wireshark Lab: UDP v8.1

Supplement to *Computer Networking: A Top-Down Approach, 8th ed.*, J.F. Kurose and K.W. Ross

"Tell me and I forget. Show me and I remember. Involve me and I understand." Chinese proverb



In this lab, we'll take a quick look at the UDP transport protocol. As we saw in Chapter 3 of the text[1], UDP is a streamlined, no-frills protocol. You may want to re-read section 3.3 in the text before doing this lab. Because UDP is simple and sweet, we'll be able to cover it pretty quickly in this lab. So if you've another appointment to run off to in 30 minutes, no need to worry, as you should be able to finish this lab with ample time to spare.

At this stage, you should be a Wireshark expert. Thus, we are not going to spell out the steps as explicitly as in earlier labs. In particular, we are not going to provide example screenshots for all the steps.

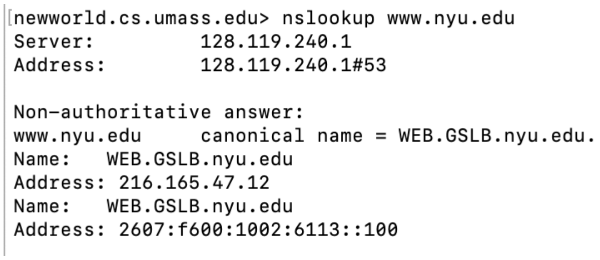
The Assignment

Start capturing packets in Wireshark and then do something that will cause your host to send and receive several UDP packets. It's also likely that just by doing nothing (except capturing packets via Wireshark) that some UDP packets sent by others will appear in your trace. In particular, the Domain Name System (DNS) protocol (see section 2.4 in the text; and the DNS Wireshark Lab) typically sends DNS query and response messages inside of UDP, so it's likely that you'll find some DNS messages (and therefore UDP packets) in your trace.

Specifically you can try out the `nslookup` command, which invokes the underlying DNS protocol, which in turn will send UDP segments from/to the host issuing the nslookup. `nslookup` is available in most Microsoft, Apple IOS, and Linux operating systems. To run `nslookup` you just type the `nslookup` command on the command line in a DOS window, Mac IOS terminal window, or Linux shell. Figure 1 is a screenshot of running `nslookup` on the Linux command line on the newworld.cs.umass.edu host

[1] References to figures and sections are for the 8th edition of our text, *Computer Networks, A Top-down Approach, 8th ed., J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2020.* Our website for this book is http://gaia.cs.umass.edu/kurose_ross You'll find lots of interesting open material there.

located in the CS Department at the University of Massachusetts (UMass) campus, to display the IP address of www.nyu.edu.



```
[newworld.cs.umass.edu> nslookup www.nyu.edu
Server:         128.119.240.1
Address:        128.119.240.1#53

Non-authoritative answer:
www.nyu.edu     canonical name = WEB.GSLB.nyu.edu.
Name:   WEB.GSLB.nyu.edu
Address: 216.165.47.12
Name:   WEB.GSLB.nyu.edu
Address: 2607:f600:1002:6113::100
```

Figure 1: the basic `nslookup` command

We don't need to go into any more details about `nslookup` or DNS, as we're just interested in getting a few UDP segments into Wireshark, and we promised this lab would be short!

After starting packet capture on Wireshark, run `nslookup` for a hostname that you haven't visited for a while. Then stop packet capture, set your Wireshark packet filter so that Wireshark only displays the UDP segments sent and received at your host. Pick the first UDP segment and expand the UDP fields in the details window. If you are unable to find UDP segments in your trace or are unable to run Wireshark on a live network connection, you can download a packet trace containing some UDP segments[2].

Answer the following questions[3]. If you're doing this lab as part of class, your teacher will provide details about how to hand in assignments, whether written or in an LMS.

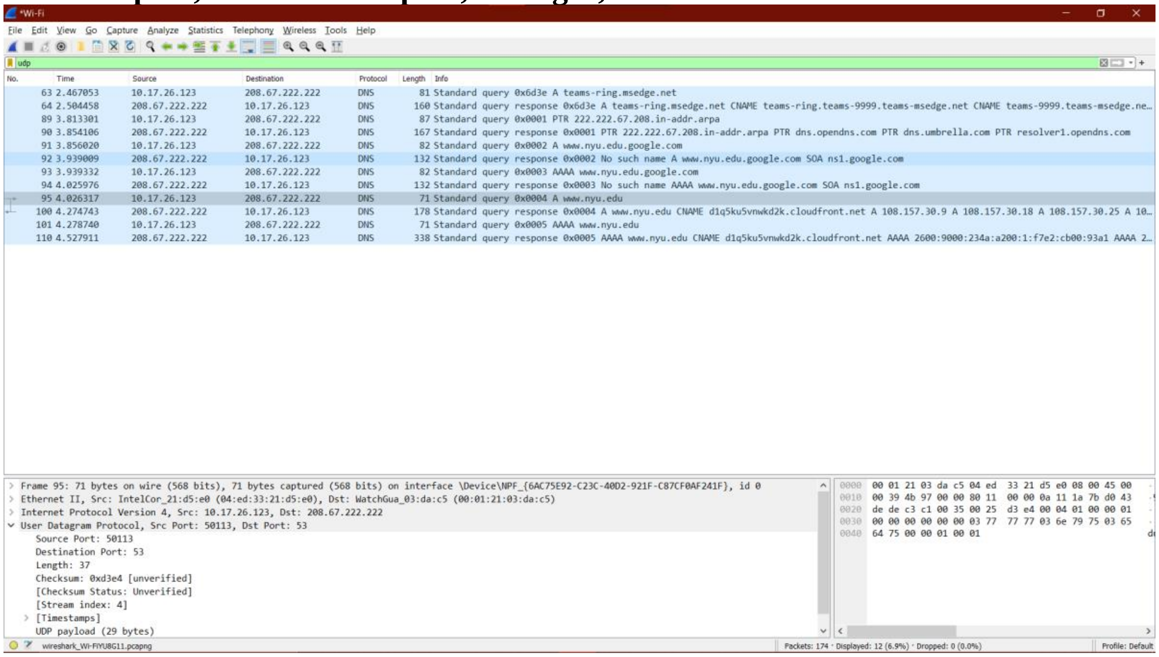
1. Select the first UDP segment in your trace. What is the packet number[4] of this segment in the trace file? What type of application-layer payload or protocol message is being carried in this UDP segment? Look at the details of this packet in Wireshark. How many fields there are in the UDP header? (You shouldn't look in the textbook! Answer these questions directly from what you observe in the packet trace.) What are the names of these fields?

[2] You can download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces-8.1.zip and extract the trace file dns-wireshark-trace1-1. This trace file can be used to answer this Wireshark lab without actually capturing packets on your own. This trace was made using Wireshark running on one of the author's computers, while performing the steps indicated in this Wireshark lab. Once you've downloaded a trace file, you can load it into Wireshark and view the trace using the *File* pull down menu, choosing *Open*, and then selecting the trace file name.

[3] For the author's class, when answering the following questions with hand-in assignments, students sometimes need to print out specific packets (see the introductory Wireshark lab for an explanation of how to do this) and indicate where in the packet they've found the information that answers a question. They do this by marking paper copies with a pen or annotating electronic copies with text in a colored font. There are also learning management system (LMS) modules for teachers that allow students to answer these questions online and have answers auto-graded for these Wireshark labs at http://gaia.cs.umass.edu/kurose_ross/lms.htm

[4] Remember that this "packet number" is assigned by Wireshark for listing purposes only; it is NOT a packet number contained in any real packet header.

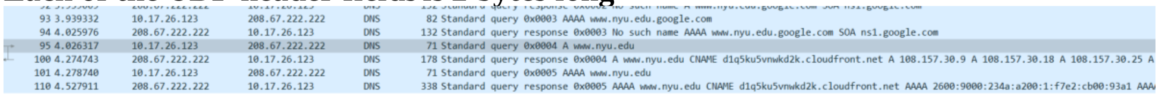
The packet number[5] of this segment in the trace file is 95
UDP header contains 4 fields:
1. source port; 2. destination port; 3. length; 4. Checksum



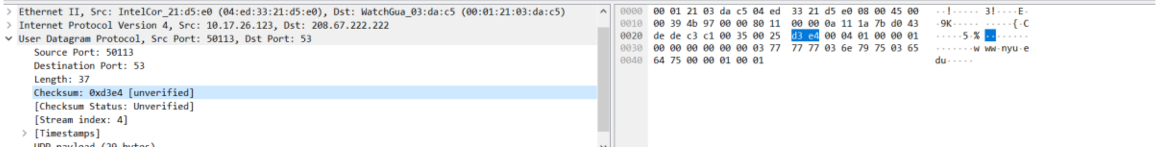
```
*Wi-Fi
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help
udp

No.     Time        Source          Destination     Protocol Length Info
     63 2.467053    10.17.26.123    208.67.222.222  DNS       81 Standard query 0x6d3e A teams-ring.msedge.net
     64 2.504458    208.67.222.222  10.17.26.123    DNS      160 Standard query response 0x6d3e A teams-ring.msedge.net CNAME teams-ring.teams-9999.teams-msedge.net CNAME teams-9999.teams-msedge.ne…
     89 3.813301    10.17.26.123    208.67.222.222  DNS       87 Standard query 0x0001 PTR 222.222.67.208.in-addr.arpa
     90 3.854106    208.67.222.222  10.17.26.123    DNS      167 Standard query response 0x0001 PTR 222.222.67.208.in-addr.arpa PTR dns.opendns.com PTR dns.umbrella.com PTR resolver1.opendns.com
     91 3.856020    10.17.26.123    208.67.222.222  DNS       82 Standard query 0x0002 A www.nyu.edu.google.com
     92 3.939009    208.67.222.222  10.17.26.123    DNS      132 Standard query response 0x0002 No such name A www.nyu.edu.google.com SOA ns1.google.com
     93 3.939332    10.17.26.123    208.67.222.222  DNS       82 Standard query 0x0003 AAAA www.nyu.edu.google.com
     94 4.025976    208.67.222.222  10.17.26.123    DNS      132 Standard query response 0x0003 No such name AAAA www.nyu.edu.google.com SOA ns1.google.com
     95 4.026317    10.17.26.123    208.67.222.222  DNS       71 Standard query 0x0004 A www.nyu.edu
    100 4.274743    208.67.222.222  10.17.26.123    DNS      178 Standard query response 0x0004 A www.nyu.edu CNAME d1q5ku5vnwkd2k.cloudfront.net A 108.157.30.9 A 108.157.30.18 A 108.157.30.25 A 10…
    101 4.278740    10.17.26.123    208.67.222.222  DNS       71 Standard query 0x0005 AAAA www.nyu.edu
    110 4.527911    208.67.222.222  10.17.26.123    DNS      338 Standard query response 0x0005 AAAA www.nyu.edu CNAME d1q5ku5vnwkd2k.cloudfront.net AAAA 2600:9000:234a:a200:1:f7e2:cb00:93a1 AAAA 2…

> Frame 95: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{6AC75E92-C23C-40D2-921F-C87CF0AF241F}, id 0
> Ethernet II, Src: IntelCor_21:d5:e0 (04:ed:33:21:d5:e0), Dst: WatchGua_03:da:c5 (00:01:21:03:da:c5)
> Internet Protocol Version 4, Src: 10.17.26.123, Dst: 208.67.222.222
v User Datagram Protocol, Src Port: 50113, Dst Port: 53
    Source Port: 50113
    Destination Port: 53
    Length: 37
    Checksum: 0xd3e4 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
  > [Timestamps]
    UDP payload (29 bytes)

0000  00 01 21 03 da c5 04 ed  33 21 d5 e0 08 00 45 00
0010  00 39 4b 97 00 00 80 11  00 00 0a 11 1a 7b d0 43
0020  de de c3 c1 00 35 00 25  d3 e4 00 04 01 00 00 01
0030  00 00 00 00 00 00 03 77  77 77 03 6e 79 75 03 65
0040  64 75 00 00 01 00 01

wireshark_Wi-FiYU8G11.pcapng        Packets: 174 · Displayed: 12 (6.9%) · Dropped: 0 (0.0%)        Profile: Default
```

2. By consulting the displayed information in Wireshark's packet content field for this packet (or by consulting the textbook), what is the length (in bytes) of each of the UDP header fields?

Each of the UDP header fields is 2 bytes long



```
     93 3.939332    10.17.26.123    208.67.222.222  DNS       82 Standard query 0x0003 AAAA www.nyu.edu.google.com
     94 4.025976    208.67.222.222  10.17.26.123    DNS      132 Standard query response 0x0003 No such name AAAA www.nyu.edu.google.com SOA ns1.google.com
     95 4.026317    10.17.26.123    208.67.222.222  DNS       71 Standard query 0x0004 A www.nyu.edu
    100 4.274743    208.67.222.222  10.17.26.123    DNS      178 Standard query response 0x0004 A www.nyu.edu CNAME d1q5ku5vnwkd2k.cloudfront.net A 108.157.30.9 A 108.157.30.18 A 108.157.30.25 A
    101 4.278740    10.17.26.123    208.67.222.222  DNS       71 Standard query 0x0005 AAAA www.nyu.edu
    110 4.527911    208.67.222.222  10.17.26.123    DNS      338 Standard query response 0x0005 AAAA www.nyu.edu CNAME d1q5ku5vnwkd2k.cloudfront.net AAAA 2600:9000:234a:a200:1:f7e2:cb00:93a1 AAA
```

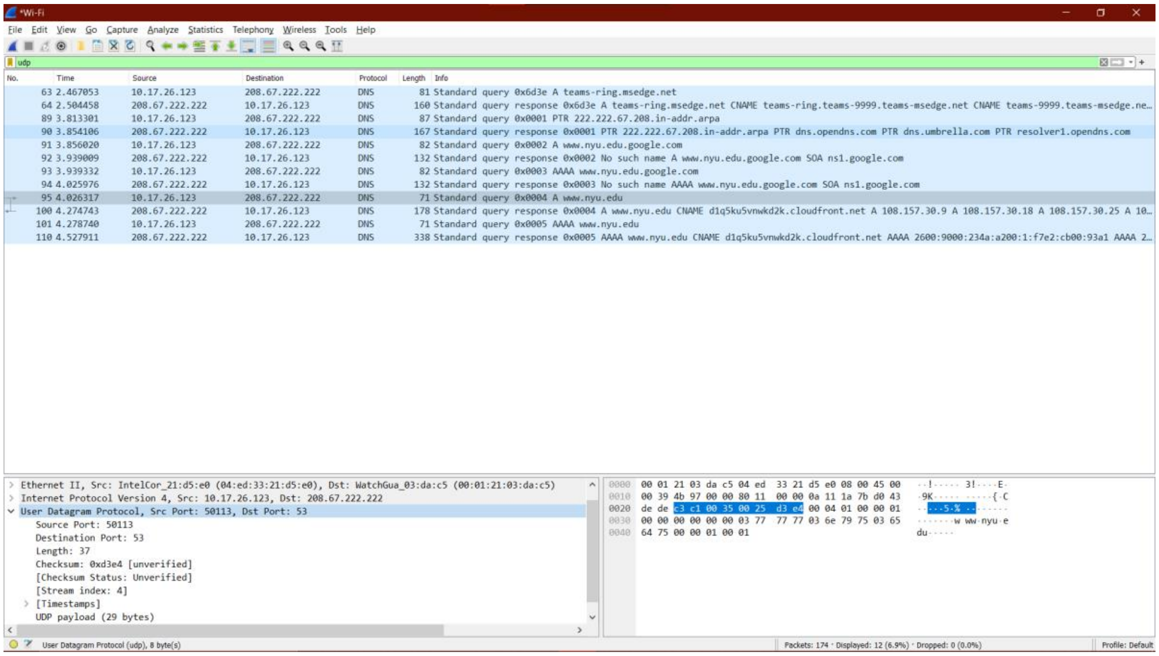


```
> Ethernet II, Src: IntelCor_21:d5:e0 (04:ed:33:21:d5:e0), Dst: WatchGua_03:da:c5 (00:01:21:03:da:c5)
> Internet Protocol Version 4, Src: 10.17.26.123, Dst: 208.67.222.222
v User Datagram Protocol, Src Port: 50113, Dst Port: 53
    Source Port: 50113
    Destination Port: 53
    Length: 37
    Checksum: 0xd3e4 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
  > [Timestamps]

0000  00 01 21 03 da c5 04 ed  33 21 d5 e0 08 00 45 00   ··!····· 3!····E·
0010  00 39 4b 97 00 00 80 11  00 00 0a 11 1a 7b d0 43   ·9K····· ·····{·C
0020  de de c3 c1 00 35 00 25  d3 e4 00 04 01 00 00 01   ·····5·% ········
0030  00 00 00 00 00 00 03 77  77 77 03 6e 79 75 03 65   ·······w ww·nyu·e
0040  64 75 00 00 01 00 01                               du·····
```

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.

The value in the length field, in the example below it is 37, is the sum of the 8 header bytes and the remaining data bytes encapsulated in the packet.
The length of UDP payload for selected packet is 29 bytes. 37 bytes - 8 bytes = 29 bytes.

[5] Remember that this "packet number" is assigned by Wireshark for listing purposes only; it is NOT a packet number contained in any real packet header.



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp

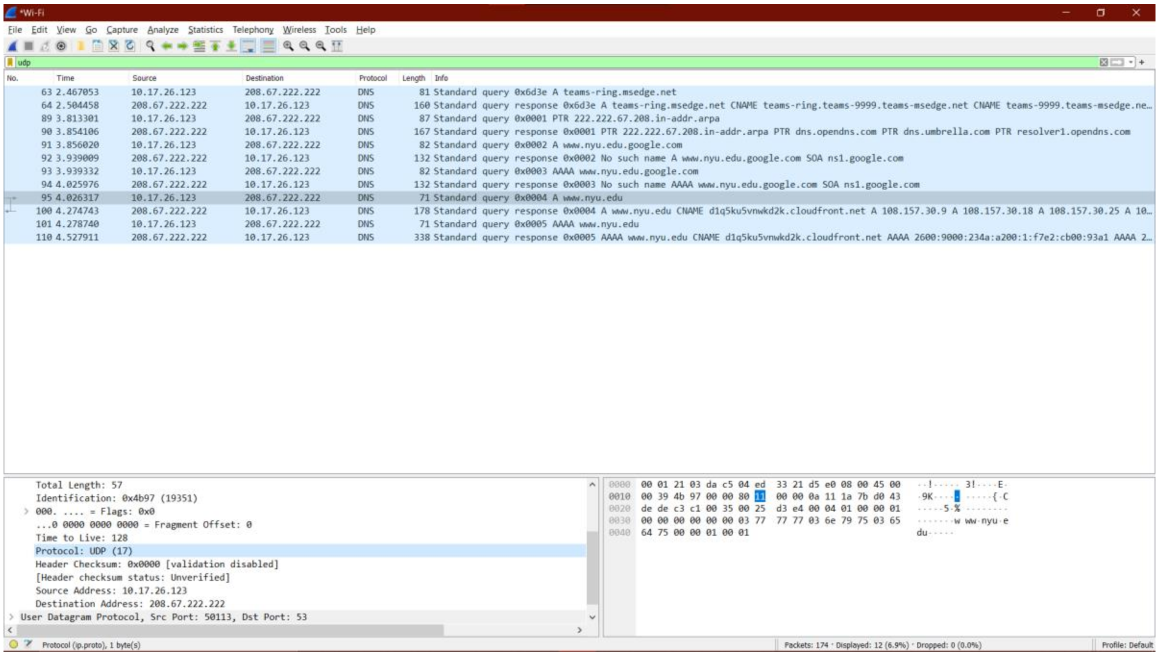
No.	Time	Source	Destination	Protocol	Length	Info
63	2.467053	10.17.26.123	208.67.222.222	DNS	81	Standard query 0x6d3e A teams-ring.msedge.net
64	2.504458	208.67.222.222	10.17.26.123	DNS	160	Standard query response 0x6d3e A teams-ring.msedge.net CNAME teams-ring.teams-9999.teams-msedge.net CNAME teams-9999.teams-msedge.ne…
89	3.813301	10.17.26.123	208.67.222.222	DNS	87	Standard query 0x0001 PTR 222.222.67.208.in-addr.arpa
90	3.854106	208.67.222.222	10.17.26.123	DNS	167	Standard query response 0x0001 PTR 222.222.67.208.in-addr.arpa PTR dns.opendns.com PTR dns.umbrella.com PTR resolver1.opendns.com
91	3.856020	10.17.26.123	208.67.222.222	DNS	82	Standard query 0x0002 A www.nyu.edu.google.com
92	3.939009	208.67.222.222	10.17.26.123	DNS	132	Standard query response 0x0002 No such name A www.nyu.edu.google.com SOA ns1.google.com
93	3.939332	10.17.26.123	208.67.222.222	DNS	82	Standard query 0x0003 AAAA www.nyu.edu.google.com
94	4.025976	208.67.222.222	10.17.26.123	DNS	132	Standard query response 0x0003 No such name AAAA www.nyu.edu.google.com SOA ns1.google.com
95	4.026317	10.17.26.123	208.67.222.222	DNS	71	Standard query 0x0004 A www.nyu.edu
100	4.274743	208.67.222.222	10.17.26.123	DNS	178	Standard query response 0x0004 A www.nyu.edu CNAME d1q5ku5vnwkd2k.cloudfront.net A 108.157.30.9 A 108.157.30.18 A 108.157.30.25 A 10…
101	4.278740	10.17.26.123	208.67.222.222	DNS	71	Standard query 0x0005 AAAA www.nyu.edu
110	4.527911	208.67.222.222	10.17.26.123	DNS	338	Standard query response 0x0005 AAAA www.nyu.edu CNAME d1q5ku5vnwkd2k.cloudfront.net AAAA 2600:9000:234a:a200:1:f7e2:cb00:93a1 AAAA 2…

```
> Ethernet II, Src: IntelCor_21:d5:e0 (04:ed:33:21:d5:e0), Dst: WatchGua_03:da:c5 (00:01:21:03:da:c5)
> Internet Protocol Version 4, Src: 10.17.26.123, Dst: 208.67.222.222
v User Datagram Protocol, Src Port: 50113, Dst Port: 53
    Source Port: 50113
    Destination Port: 53
    Length: 37
    Checksum: 0xd3e4 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
  > [Timestamps]
    UDP payload (29 bytes)
```

```
0000  00 01 21 03 da c5 04 ed  33 21 d5 e0 08 00 45 00   ··!·····3!····E·
0010  00 39 4b 97 00 00 80 11  00 00 0a 11 1a 7b d0 43   ·9K··········{·C
0020  de de c3 c1 00 35 00 25  d3 e4 00 04 01 00 00 01   ·····5·%········
0030  00 00 00 00 00 00 03 77  77 77 03 6e 79 75 03 65   ·······www·nyu·e
0040  64 75 00 00 01 00 01                               du·····
```

User Datagram Protocol (udp), 8 byte(s) | Packets: 174 · Displayed: 12 (6.9%) · Dropped: 0 (0.0%) | Profile: Default

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)
   The maximum number of bytes that can be in the payload is (2^16- 1) the bytes already being used by the header field (8). Therefore the maximum payload is 65535-8= 65527 bytes.
5. What is the largest possible source port number? (Hint: see the hint in 4.)
   The largest possible source port number is (2^16 – 1) = 65535
6. What is the protocol number for UDP? Give your answer in 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).
   The IP protocol number for UDP is 0x11 hex, which is 17 in decimal value.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp

```
No.   Time      Source          Destination     Protocol Length Info
   63 2.467053  10.17.26.123    208.67.222.222  DNS        81 Standard query 0x6d3e A teams-ring.msedge.net
   64 2.504458  208.67.222.222  10.17.26.123    DNS       160 Standard query response 0x6d3e A teams-ring.msedge.net CNAME teams-ring.teams-9999.teams-msedge.net CNAME teams-9999.teams-msedge.ne…
   89 3.813301  10.17.26.123    208.67.222.222  DNS        87 Standard query 0x0001 PTR 222.222.67.208.in-addr.arpa
   90 3.854106  208.67.222.222  10.17.26.123    DNS       167 Standard query response 0x0001 PTR 222.222.67.208.in-addr.arpa PTR dns.opendns.com PTR dns.umbrella.com PTR resolver1.opendns.com
   91 3.856020  10.17.26.123    208.67.222.222  DNS        82 Standard query 0x0002 A www.nyu.edu.google.com
   92 3.939009  208.67.222.222  10.17.26.123    DNS       132 Standard query response 0x0002 No such name A www.nyu.edu.google.com SOA ns1.google.com
   93 3.939332  10.17.26.123    208.67.222.222  DNS        82 Standard query 0x0003 AAAA www.nyu.edu.google.com
   94 4.025976  208.67.222.222  10.17.26.123    DNS       132 Standard query response 0x0003 No such name AAAA www.nyu.edu.google.com SOA ns1.google.com
   95 4.026317  10.17.26.123    208.67.222.222  DNS        71 Standard query 0x0004 A www.nyu.edu
  100 4.274743  208.67.222.222  10.17.26.123    DNS       178 Standard query response 0x0004 A www.nyu.edu CNAME d1q5ku5vnwkd2k.cloudfront.net A 108.157.30.9 A 108.157.30.18 A 108.157.30.25 A 10…
  101 4.278740  10.17.26.123    208.67.222.222  DNS        71 Standard query 0x0005 AAAA www.nyu.edu
  110 4.527911  208.67.222.222  10.17.26.123    DNS       338 Standard query response 0x0005 AAAA www.nyu.edu CNAME d1q5ku5vnwkd2k.cloudfront.net AAAA 2600:9000:234a:a200:1:f7e2:cb00:93a1 AAAA 2…
```

```
    Total Length: 57
    Identification: 0x4b97 (19351)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.17.26.123
    Destination Address: 208.67.222.222
> User Datagram Protocol, Src Port: 50113, Dst Port: 53
```

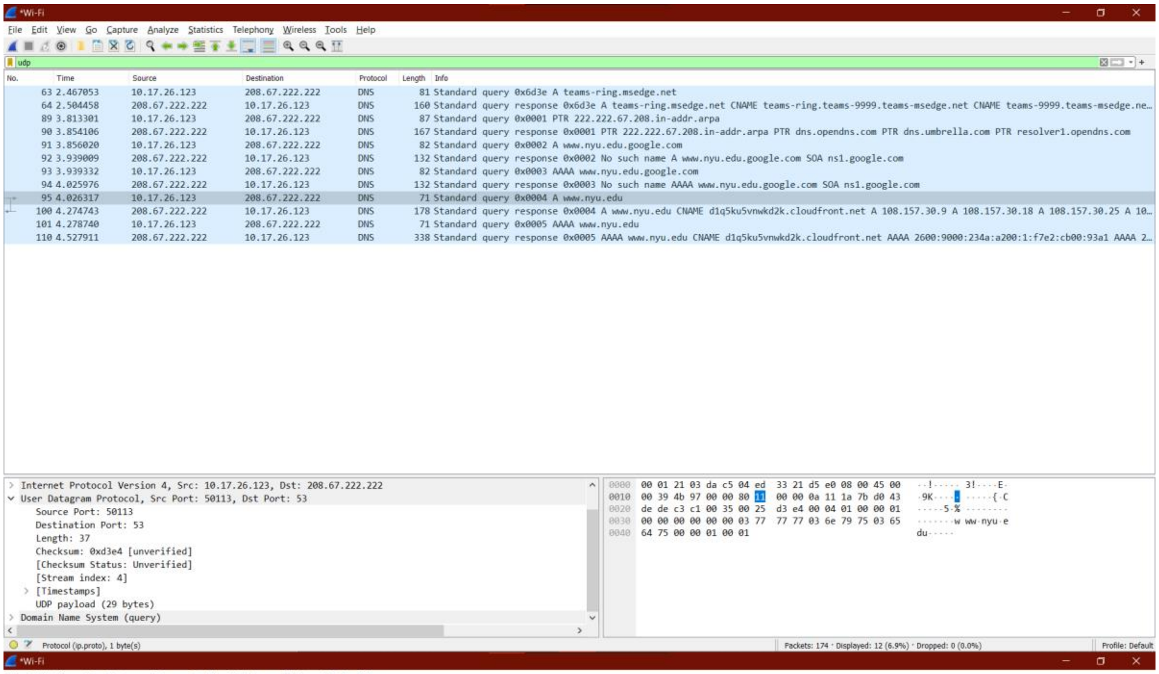
```
0000  00 01 21 03 da c5 04 ed  33 21 d5 e0 08 00 45 00   ··!····· 3!····E·
0010  00 39 4b 97 00 00 80 11  00 00 0a 11 1a 7b d0 43   ·9K····· ·····{·C
0020  de de c3 c1 00 35 00 25  d3 e4 00 04 01 00 00 01   ·····5·% ········
0030  00 00 00 00 00 00 03 77  77 77 03 6e 79 75 03 65   ·······w ww·nyu·e
0040  64 75 00 00 01 00 01                               du·····
```

```
Protocol (ip.proto), 1 byte(s)        Packets: 174 · Displayed: 12 (6.9%) · Dropped: 0 (0.0%)        Profile: Default
```

7. Examine the 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). What is the packet number[6] of the first of these two UDP segments in the trace file? What is the packet number[7] of the second of these two UDP segments in the trace file? Describe the relationship between the port numbers in the two packets.
   The source port of the UDP packet sent by the host is the same as the destination port of the reply packet, and conversely the destination port of the UDP packet sent by the host is the same as the source port of the reply packet.

[6] Remember that this "packet number" is assigned by Wireshark for listing purposes only; it is NOT a packet number contained in any real packet header.

[7] Remember that this "packet number" is assigned by Wireshark for listing purposes only; it is NOT a packet number contained in any real packet header.



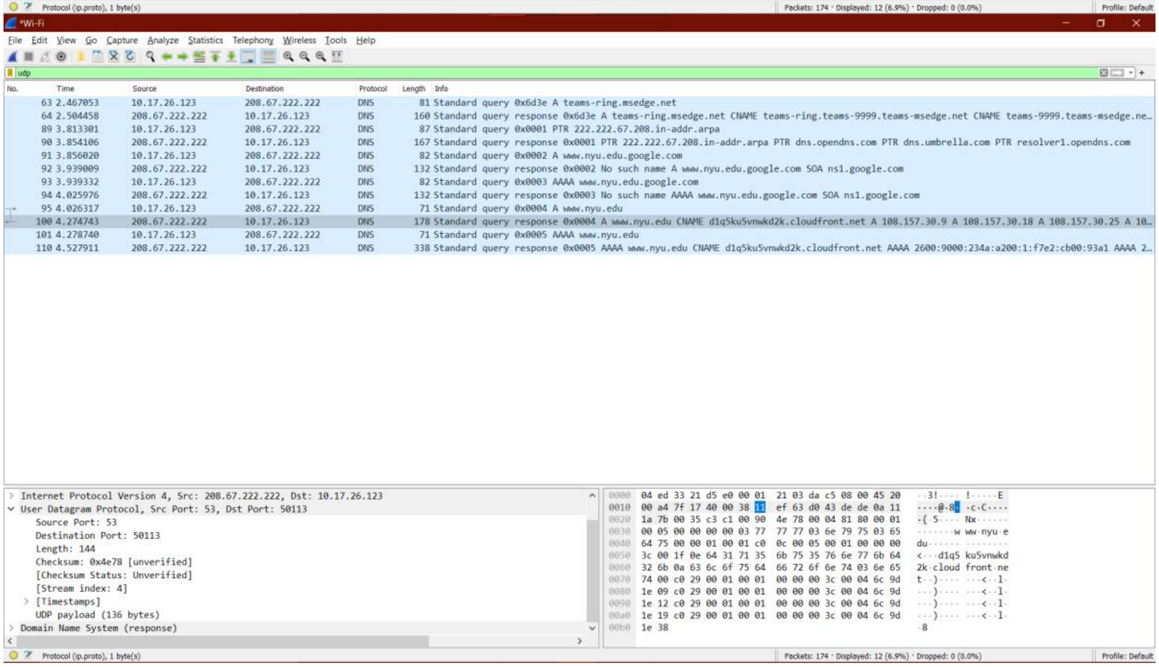
*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp

```
No.   Time       Source          Destination     Protocol Length Info
   63 2.467053   10.17.26.123    208.67.222.222  DNS       81 Standard query 0x6d3e A teams-ring.msedge.net
   64 2.504458   208.67.222.222  10.17.26.123    DNS      160 Standard query response 0x6d3e A teams-ring.msedge.net CNAME teams-ring.teams-9999.teams-msedge.net CNAME teams-9999.teams-msedge.ne…
   89 3.813301   10.17.26.123    208.67.222.222  DNS       87 Standard query 0x0001 PTR 222.222.67.208.in-addr.arpa
   90 3.854106   208.67.222.222  10.17.26.123    DNS      167 Standard query response 0x0001 PTR 222.222.67.208.in-addr.arpa PTR dns.opendns.com PTR dns.umbrella.com PTR resolver1.opendns.com
   91 3.856020   10.17.26.123    208.67.222.222  DNS       82 Standard query 0x0002 A www.nyu.edu.google.com
   92 3.939009   208.67.222.222  10.17.26.123    DNS      132 Standard query response 0x0002 No such name A www.nyu.edu.google.com SOA ns1.google.com
   93 3.939332   10.17.26.123    208.67.222.222  DNS       82 Standard query 0x0003 AAAA www.nyu.edu.google.com
   94 4.025976   208.67.222.222  10.17.26.123    DNS      132 Standard query response 0x0003 No such name AAAA www.nyu.edu.google.com SOA ns1.google.com
   95 4.026317   10.17.26.123    208.67.222.222  DNS       71 Standard query 0x0004 A www.nyu.edu
  100 4.274743   208.67.222.222  10.17.26.123    DNS      178 Standard query response 0x0004 A www.nyu.edu CNAME d1q5ku5vnwkd2k.cloudfront.net A 108.157.30.9 A 108.157.30.18 A 108.157.30.25 A 10…
  101 4.278740   10.17.26.123    208.67.222.222  DNS       71 Standard query 0x0005 AAAA www.nyu.edu
  110 4.527911   208.67.222.222  10.17.26.123    DNS      338 Standard query response 0x0005 AAAA www.nyu.edu CNAME d1q5ku5vnwkd2k.cloudfront.net AAAA 2600:9000:234a:a200:1:f7e2:cb00:93a1 AAAA 2…
```

```
> Internet Protocol Version 4, Src: 10.17.26.123, Dst: 208.67.222.222
v User Datagram Protocol, Src Port: 50113, Dst Port: 53
    Source Port: 50113
    Destination Port: 53
    Length: 37
    Checksum: 0xd3e4 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
  > [Timestamps]
    UDP payload (29 bytes)
> Domain Name System (query)
```

```
0000  00 01 21 03 da c5 04 ed  33 21 d5 e0 08 00 45 00   ··!····· 3!····E·
0010  00 39 4b 97 00 00 80 11  00 00 0a 11 1a 7b d0 43   ·9K····· ·····{·C
0020  de de c3 c1 00 35 00 25  d3 e4 00 04 01 00 00 01   ·····5·% ········
0030  00 00 00 00 00 00 03 77  77 77 03 6e 79 75 03 65   ·······w ww·nyu·e
0040  64 75 00 00 01 00 01                               du·····
```

Protocol (ip.proto), 1 byte(s)
Packets: 174 · Displayed: 12 (6.9%) · Dropped: 0 (0.0%)
Profile: Default



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp

```
No.   Time       Source          Destination     Protocol Length Info
   63 2.467053   10.17.26.123    208.67.222.222  DNS       81 Standard query 0x6d3e A teams-ring.msedge.net
   64 2.504458   208.67.222.222  10.17.26.123    DNS      160 Standard query response 0x6d3e A teams-ring.msedge.net CNAME teams-ring.teams-9999.teams-msedge.net CNAME teams-9999.teams-msedge.ne…
   89 3.813301   10.17.26.123    208.67.222.222  DNS       87 Standard query 0x0001 PTR 222.222.67.208.in-addr.arpa
   90 3.854106   208.67.222.222  10.17.26.123    DNS      167 Standard query response 0x0001 PTR 222.222.67.208.in-addr.arpa PTR dns.opendns.com PTR dns.umbrella.com PTR resolver1.opendns.com
   91 3.856020   10.17.26.123    208.67.222.222  DNS       82 Standard query 0x0002 A www.nyu.edu.google.com
   92 3.939009   208.67.222.222  10.17.26.123    DNS      132 Standard query response 0x0002 No such name A www.nyu.edu.google.com SOA ns1.google.com
   93 3.939332   10.17.26.123    208.67.222.222  DNS       82 Standard query 0x0003 AAAA www.nyu.edu.google.com
   94 4.025976   208.67.222.222  10.17.26.123    DNS      132 Standard query response 0x0003 No such name AAAA www.nyu.edu.google.com SOA ns1.google.com
   95 4.026317   10.17.26.123    208.67.222.222  DNS       71 Standard query 0x0004 A www.nyu.edu
  100 4.274743   208.67.222.222  10.17.26.123    DNS      178 Standard query response 0x0004 A www.nyu.edu CNAME d1q5ku5vnwkd2k.cloudfront.net A 108.157.30.9 A 108.157.30.18 A 108.157.30.25 A 10…
  101 4.278740   10.17.26.123    208.67.222.222  DNS       71 Standard query 0x0005 AAAA www.nyu.edu
  110 4.527911   208.67.222.222  10.17.26.123    DNS      338 Standard query response 0x0005 AAAA www.nyu.edu CNAME d1q5ku5vnwkd2k.cloudfront.net AAAA 2600:9000:234a:a200:1:f7e2:cb00:93a1 AAAA 2…
```

```
> Internet Protocol Version 4, Src: 208.67.222.222, Dst: 10.17.26.123
v User Datagram Protocol, Src Port: 53, Dst Port: 50113
    Source Port: 53
    Destination Port: 50113
    Length: 144
    Checksum: 0x4e78 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
  > [Timestamps]
    UDP payload (136 bytes)
> Domain Name System (response)
```

```
0000  04 ed 33 21 d5 e0 00 01  21 03 da c5 08 00 45 20   ··3!···· !·····E
0010  00 a4 7f 17 40 00 38 11  ef 63 d0 43 de de 0a 11   ····@·8· ·c·C····
0020  1a 7b 00 35 c3 c1 00 90  4e 78 00 04 81 80 00 01   ·{·5···· Nx······
0030  00 05 00 00 00 00 03 77  77 77 03 6e 79 75 03 65   ·······w ww·nyu·e
0040  64 75 00 00 01 00 01 c0  0c 00 05 00 01 00 00 00   du······ ········
0050  3c 00 1f 0e 64 31 71 35  6b 75 35 76 6e 77 6b 64   <···d1q5 ku5vnwkd
0060  32 6b 0a 63 6c 6f 75 64  66 72 6f 6e 74 03 6e 65   2k·cloud front·ne
0070  74 00 c0 29 00 01 00 01  00 00 00 3c 00 04 6c 9d   t··)···· ···<··l·
0080  1e 09 c0 29 00 01 00 01  00 00 00 3c 00 04 6c 9d   ···)···· ···<··l·
0090  1e 12 c0 29 00 01 00 01  00 00 00 3c 00 04 6c 9d   ···)···· ···<··l·
00a0  1e 19 c0 29 00 01 00 01  00 00 00 3c 00 04 6c 9d   ···)···· ···<··l·
00b0  1e 38                                              ·8
```

Protocol (ip.proto), 1 byte(s)
Packets: 174 · Displayed: 12 (6.9%) · Dropped: 0 (0.0%)
Profile: Default

That’s it! As a streamlined, no-frills protocol , UDP deserves a streamlined, no-frills Wireshark Lab ☺.