# LAB ASSIGNMENT WEEK 1

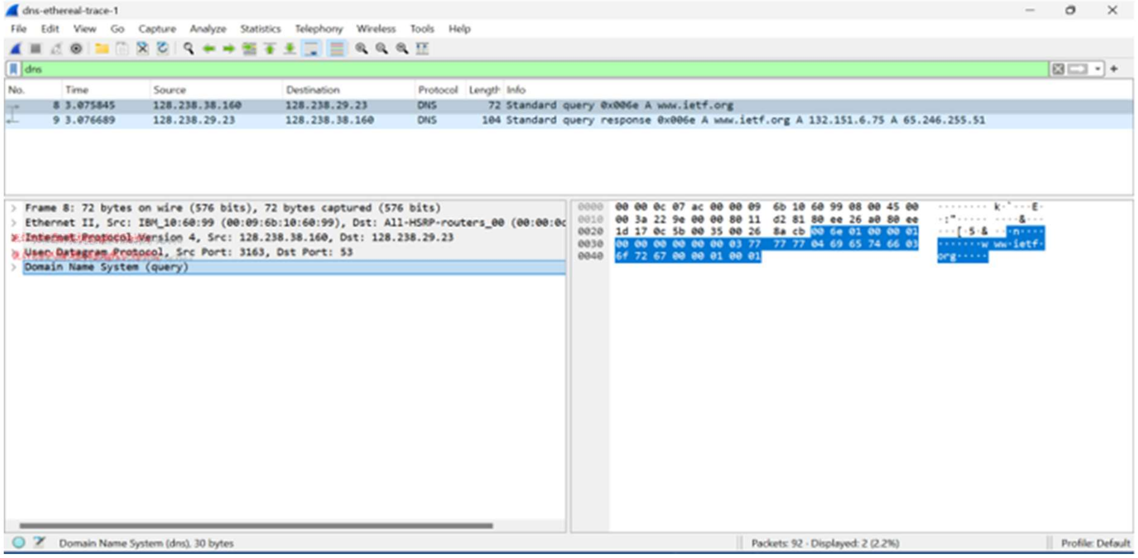
## Usirikayala Likhith – 20223295(D2)

**<u>Exercise # 1 Tracing DNS with Wireshark</u>**

**<u>dns-ethereal-trace-1 file:</u>**

1. Locate the DNS query and response messages. Are then sent over UDP or TCP?

A. They are sending over UDP


dns-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.   Time       Source           Destination      Protocol Length Info
    8 3.075845   128.238.38.160   128.238.29.23    DNS        72 Standard query 0x006e A www.ietf.org
    9 3.076689   128.238.29.23    128.238.38.160   DNS       104 Standard query response 0x006e A www.ietf.org A 132.151.6.75 A 65.246.255.51
```

```
> Frame 8: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.23
> User Datagram Protocol, Src Port: 3163, Dst Port: 53
> Domain Name System (query)
```

```
0000  00 00 0c 07 ac 00 00 09  6b 10 60 99 08 00 45 00   ········ k·`···E·
0010  00 3a 22 9e 00 00 80 11  d2 81 80 ee 26 a0 80 ee   ·:"····· ····&···
0020  1d 17 0c 5b 00 35 00 26  8a cb 00 6e 01 00 00 01   ···[·5·& ···n····
0030  00 00 00 00 00 00 03 77  77 77 04 69 65 74 66 03   ·······w ww·ietf·
0040  6f 72 67 00 00 01 00 01                            org·····
```

Domain Name System (dns), 30 bytes | Packets: 92 · Displayed: 2 (2.2%) | Profile: Default

2. What is the destination port for the DNS query message? What is the source port of DNS response message?

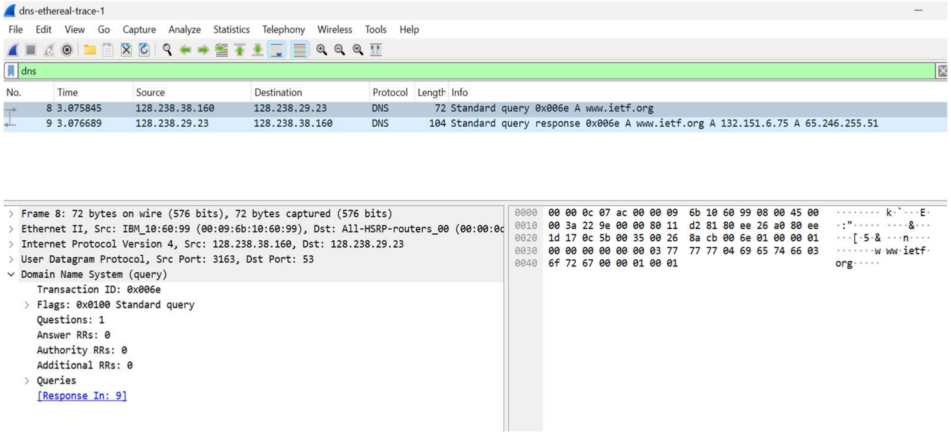
A. Destination port for the DNS query message is 53 and source port of DNS response message is 53

3. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

A. 128.238.29.23 is IP address is the DNS query message sent. The two IP addresses the same

4. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

A. It's a type A Standard Query and it doesn't contain any answers.


dns-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

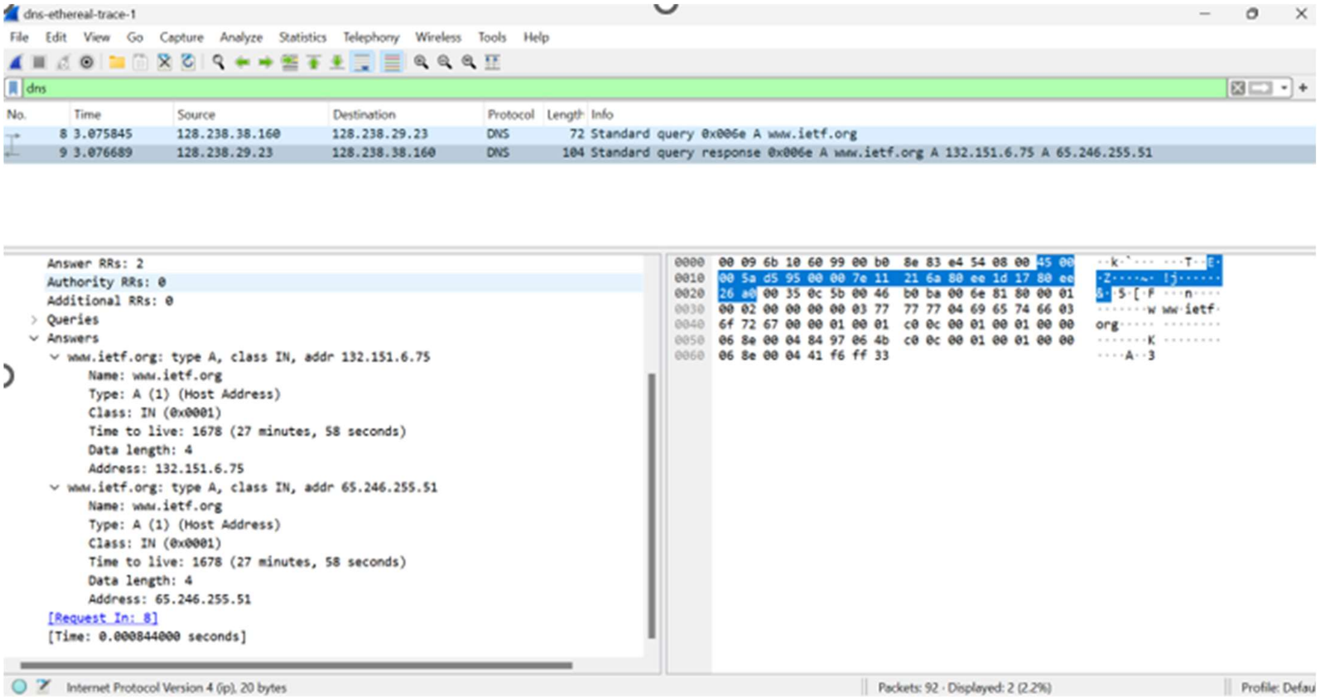
```
No.   Time       Source           Destination      Protocol Length Info
    8 3.075845   128.238.38.160   128.238.29.23    DNS        72 Standard query 0x006e A www.ietf.org
    9 3.076689   128.238.29.23    128.238.38.160   DNS       104 Standard query response 0x006e A www.ietf.org A 132.151.6.75 A 65.246.255.51
```

```
> Frame 8: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.23
> User Datagram Protocol, Src Port: 3163, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x006e
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 9]
```

```
0000  00 00 0c 07 ac 00 00 09  6b 10 60 99 08 00 45 00   ········ k·`···E·
0010  00 3a 22 9e 00 00 80 11  d2 81 80 ee 26 a0 80 ee   ·:"····· ····&···
0020  1d 17 0c 5b 00 35 00 26  8a cb 00 6e 01 00 00 01   ···[·5·& ···n····
0030  00 00 00 00 00 00 03 77  77 77 04 69 65 74 66 03   ·······w ww·ietf·
0040  6f 72 67 00 00 01 00 01                            org·····
```

5. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

A. There were 2 answers containing information about the name of the host, the type of address, class, the TTL, the data length and the IP address.


dns-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
dns
```

```
No.   Time       Source          Destination     Protocol Length Info
    8 3.075845   128.238.38.160  128.238.29.23   DNS        72 Standard query 0x006e A www.ietf.org
    9 3.076689   128.238.29.23   128.238.38.160  DNS       104 Standard query response 0x006e A www.ietf.org A 132.151.6.75 A 65.246.255.51
```

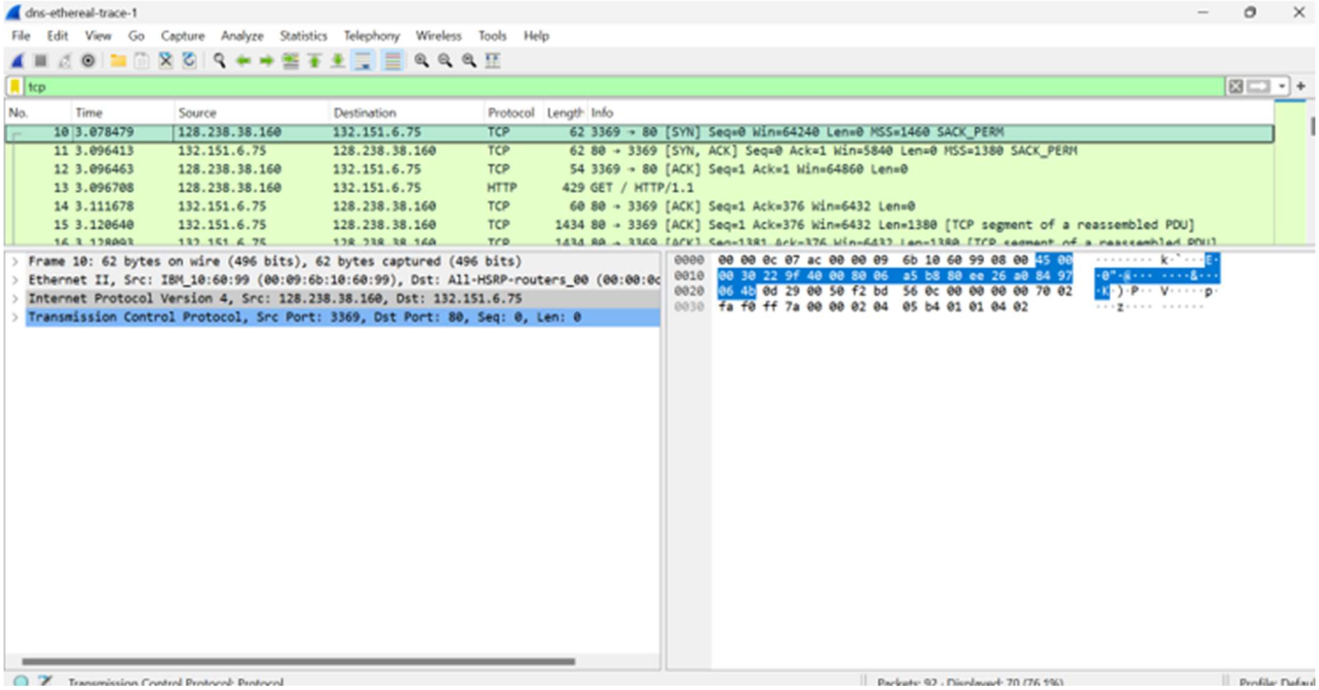
```
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    v www.ietf.org: type A, class IN, addr 132.151.6.75
        Name: www.ietf.org
        Type: A (1) (Host Address)
        Class: IN (0x0001)
        Time to live: 1678 (27 minutes, 58 seconds)
        Data length: 4
        Address: 132.151.6.75
    v www.ietf.org: type A, class IN, addr 65.246.255.51
        Name: www.ietf.org
        Type: A (1) (Host Address)
        Class: IN (0x0001)
        Time to live: 1678 (27 minutes, 58 seconds)
        Data length: 4
        Address: 65.246.255.51
    [Request In: 8]
    [Time: 0.000844000 seconds]
```

```
0000  00 09 6b 10 60 99 00 b0  8e 83 e4 54 08 00 45 00   ··k·`··· ···T··E·
0010  00 5a d5 95 00 00 7e 11  21 6a 80 ee 1d 17 80 ee   ·Z····~· !j······
0020  26 a0 00 35 0c 5b 00 46  b0 ba 00 6e 81 80 00 01   &··5·[·F ···n····
0030  00 02 00 00 00 00 03 77  77 77 04 69 65 74 66 03   ·······w ww·ietf·
0040  6f 72 67 00 00 01 00 01  c0 0c 00 01 00 01 00 00   org····· ········
0050  06 8e 00 04 84 97 06 4b  c0 0c 00 01 00 01 00 00   ·······K ········
0060  06 8e 00 04 41 f6 ff 33                            ····A··3
```

Internet Protocol Version 4 (ip), 20 bytes | Packets: 92 · Displayed: 2 (2.2%) | Profile: Defau

6. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

A. The first SYN packet was sent to 132.151.6.75 which corresponds to the first IP address provided in the DNS response message.


dns-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp
```

```
No.   Time       Source          Destination     Protocol Length Info
   10 3.078479   128.238.38.160  132.151.6.75    TCP        62 3369 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
   11 3.096413   132.151.6.75    128.238.38.160  TCP        62 80 → 3369 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM
   12 3.096463   128.238.38.160  132.151.6.75    TCP        54 3369 → 80 [ACK] Seq=1 Ack=1 Win=64860 Len=0
   13 3.096708   128.238.38.160  132.151.6.75    HTTP      429 GET / HTTP/1.1
   14 3.111678   132.151.6.75    128.238.38.160  TCP        60 80 → 3369 [ACK] Seq=1 Ack=376 Win=6432 Len=0
   15 3.120640   132.151.6.75    128.238.38.160  TCP      1434 80 → 3369 [ACK] Seq=1 Ack=376 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
   16 3.128093   132.151.6.75    128.238.38.160  TCP      1434 80 → 3369 [ACK] Seq=1381 Ack=376 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
```

```
> Frame 10: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 132.151.6.75
> Transmission Control Protocol, Src Port: 3369, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  00 00 0c 07 ac 00 00 09  6b 10 60 99 08 00 45 00   ········ k·`···E·
0010  00 30 22 9f 40 00 80 06  a5 b8 80 ee 26 a0 84 97   ·0"·@··· ····&···
0020  06 4b 0d 29 00 50 f2 bd  56 0c 00 00 00 00 70 02   ·K·)·P·· V·····p·
0030  fa f0 ff 7a 00 00 02 04  05 b4 01 01 04 02         ···z···· ······
```

Transmission Control Protocol: Protocol | Packets: 92 · Displayed: 70 (76.1%) | Profile: Defaul

7. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

A. No

## <u>dns-ethereal-trace-2 file:</u>

8. What is the destination port for the DNS query message? What is the source port of DNS response message?

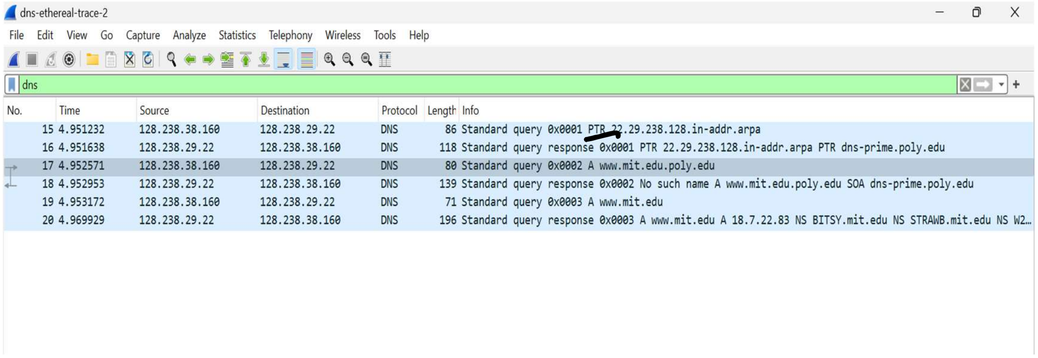
A. Destination port for the DNS query message is 53 and source port of DNS response message is 53

9. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

A. 128.238.29.22 is IP address is the DNS query message sent. The two IP addresses the same

10. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

A. The query is of type PTR and it doesn’t contain any answers

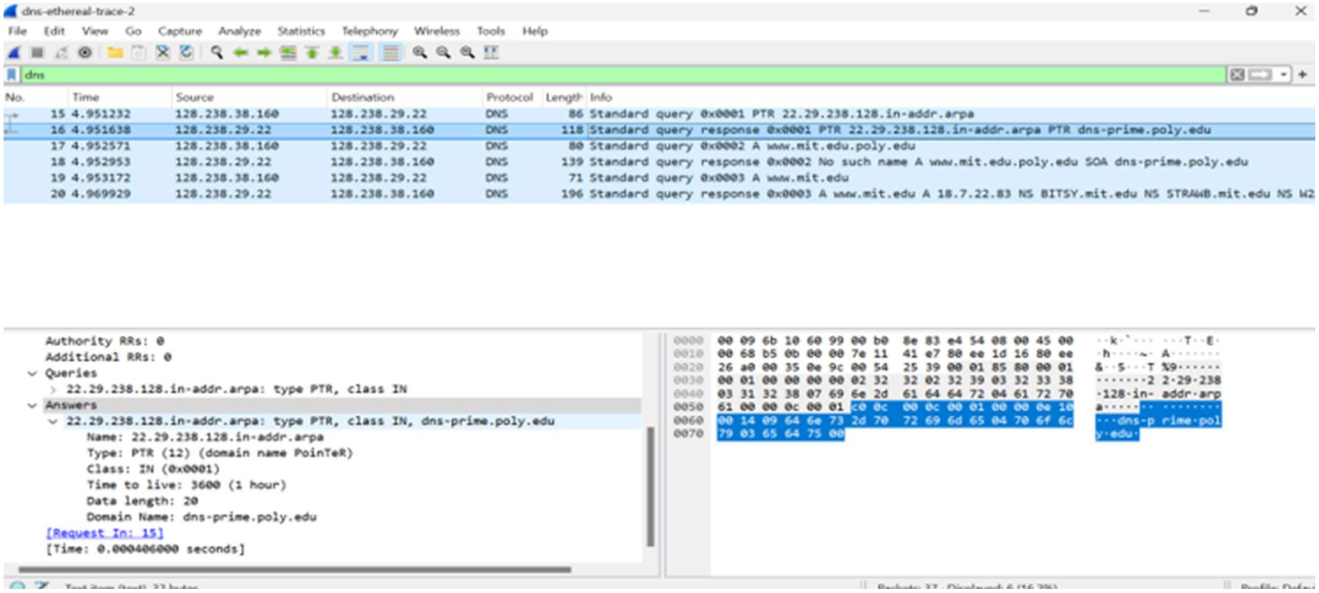

dns-ethereal-trace-2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

```
No.  Time       Source          Destination     Protocol Length Info
  15 4.951232   128.238.38.160  128.238.29.22   DNS        86 Standard query 0x0001 PTR 22.29.238.128.in-addr.arpa
  16 4.951638   128.238.29.22   128.238.38.160  DNS       118 Standard query response 0x0001 PTR 22.29.238.128.in-addr.arpa PTR dns-prime.poly.edu
  17 4.952571   128.238.38.160  128.238.29.22   DNS        80 Standard query 0x0002 A www.mit.edu.poly.edu
  18 4.952953   128.238.29.22   128.238.38.160  DNS       139 Standard query response 0x0002 No such name A www.mit.edu.poly.edu SOA dns-prime.poly.edu
  19 4.953172   128.238.38.160  128.238.29.22   DNS        71 Standard query 0x0003 A www.mit.edu
  20 4.969929   128.238.29.22   128.238.38.160  DNS       196 Standard query response 0x0003 A www.mit.edu A 18.7.22.83 NS BITSY.mit.edu NS STRAWB.mit.edu NS W2…
```

11. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

A. The response DNS message contains one answer containing the name of the host, the type of address, the class, the TTL, Data length and the Domain name.


dns-ethereal-trace-2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

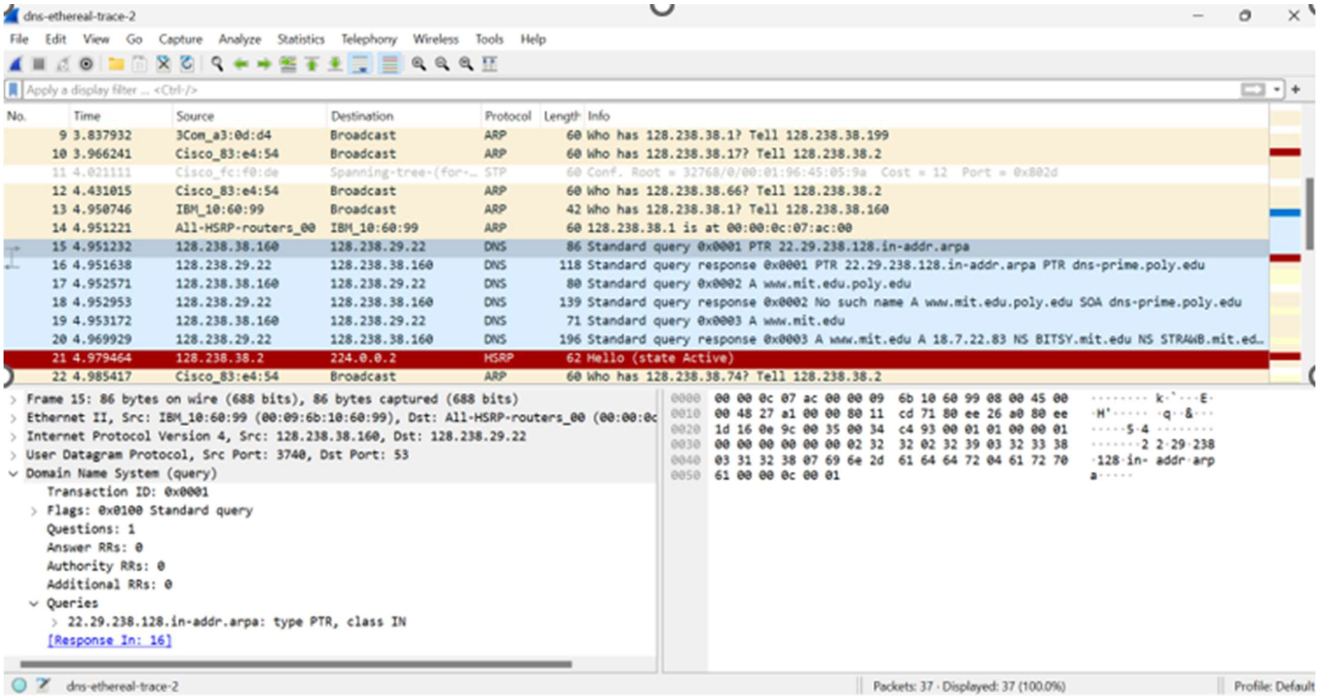
dns

```
No.  Time       Source          Destination     Protocol Length Info
  15 4.951232   128.238.38.160  128.238.29.22   DNS        86 Standard query 0x0001 PTR 22.29.238.128.in-addr.arpa
  16 4.951638   128.238.29.22   128.238.38.160  DNS       118 Standard query response 0x0001 PTR 22.29.238.128.in-addr.arpa PTR dns-prime.poly.edu
  17 4.952571   128.238.38.160  128.238.29.22   DNS        80 Standard query 0x0002 A www.mit.edu.poly.edu
  18 4.952953   128.238.29.22   128.238.38.160  DNS       139 Standard query response 0x0002 No such name A www.mit.edu.poly.edu SOA dns-prime.poly.edu
  19 4.953172   128.238.38.160  128.238.29.22   DNS        71 Standard query 0x0003 A www.mit.edu
  20 4.969929   128.238.29.22   128.238.38.160  DNS       196 Standard query response 0x0003 A www.mit.edu A 18.7.22.83 NS BITSY.mit.edu NS STRAWB.mit.edu NS W2
```

```
    Authority RRs: 0
    Additional RRs: 0
  ∨ Queries
    > 22.29.238.128.in-addr.arpa: type PTR, class IN
  ∨ Answers
    ∨ 22.29.238.128.in-addr.arpa: type PTR, class IN, dns-prime.poly.edu
        Name: 22.29.238.128.in-addr.arpa
        Type: PTR (12) (domain name PointeR)
        Class: IN (0x0001)
        Time to live: 3600 (1 hour)
        Data length: 20
        Domain Name: dns-prime.poly.edu
    [Request In: 15]
    [Time: 0.000406000 seconds]
```

```
0000  00 09 6b 10 60 99 00 b0  8e 83 e4 54 08 00 45 00   ··k·`··· ···T··E·
0010  00 68 b5 0b 00 00 7e 11  41 e7 80 ee 1d 16 80 ee   ·h····~· A·······
0020  26 a0 00 35 0e 9c 00 54  25 39 00 01 85 80 00 01   &··5···T %9······
0030  00 01 00 00 00 00 02 32  32 02 32 39 03 32 33 38   ·······2 2·29·238
0040  03 31 32 38 07 69 6e 2d  61 64 64 72 04 61 72 70   ·128·in- addr·arp
0050  61 00 00 0c 00 01 c0 0c  00 0c 00 01 00 00 0e 10   a······· ········
0060  00 14 09 64 6e 73 2d 70  72 69 6d 65 04 70 6f 6c   ···dns-p rime·pol
0070  79 03 65 64 75 00                                  y·edu·
```

12. Provide a screenshot.

A. 

dns-ethereal-trace-2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time       Source              Destination          Protocol Length Info
    9 3.837932   3Com_a3:0d:d4       Broadcast            ARP       60 Who has 128.238.38.1? Tell 128.238.38.199
   10 3.966241   Cisco_83:e4:54      Broadcast            ARP       60 Who has 128.238.38.17? Tell 128.238.38.2
   11 4.021111   Cisco_fc:f0:de      Spanning-tree-(for-… STP       60 Conf. Root = 32768/0/00:01:96:45:05:9a  Cost = 12  Port = 0x802d
   12 4.431015   Cisco_83:e4:54      Broadcast            ARP       60 Who has 128.238.38.66? Tell 128.238.38.2
   13 4.950746   IBM_10:60:99        Broadcast            ARP       42 Who has 128.238.38.1? Tell 128.238.38.160
   14 4.951221   All-HSRP-routers_00 IBM_10:60:99         ARP       60 128.238.38.1 is at 00:00:0c:07:ac:00
   15 4.951232   128.238.38.160      128.238.29.22        DNS       86 Standard query 0x0001 PTR 22.29.238.128.in-addr.arpa
   16 4.951638   128.238.29.22       128.238.38.160       DNS      118 Standard query response 0x0001 PTR 22.29.238.128.in-addr.arpa PTR dns-prime.poly.edu
   17 4.952571   128.238.38.160      128.238.29.22        DNS       80 Standard query 0x0002 A www.mit.edu.poly.edu
   18 4.952953   128.238.29.22       128.238.38.160       DNS      139 Standard query response 0x0002 No such name A www.mit.edu.poly.edu SOA dns-prime.poly.edu
   19 4.953172   128.238.38.160      128.238.29.22        DNS       71 Standard query 0x0003 A www.mit.edu
   20 4.969929   128.238.29.22       128.238.38.160       DNS      196 Standard query response 0x0003 A www.mit.edu A 18.7.22.83 NS BITSY.mit.edu NS STRAWB.mit.ed…
   21 4.979464   128.238.38.2        224.0.0.2            HSRP      62 Hello (state Active)
   22 4.985417   Cisco_83:e4:54      Broadcast            ARP       60 Who has 128.238.38.74? Tell 128.238.38.2
```

```
> Frame 15: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.22
> User Datagram Protocol, Src Port: 3740, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0001
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > 22.29.238.128.in-addr.arpa: type PTR, class IN
    [Response In: 16]
```

```
0000  00 00 0c 07 ac 00 00 09  6b 10 60 99 08 00 45 00   ········ k·`···E·
0010  00 48 27 a1 00 00 80 11  cd 71 80 ee 26 a0 80 ee   ·H'····· ·q··&···
0020  1d 16 0e 9c 00 35 00 34  c4 93 00 01 01 00 00 01   ·····5·4 ········
0030  00 00 00 00 00 00 02 32  32 02 32 39 03 32 33 38   ·······2 2·29·238
0040  03 31 32 38 07 69 6e 2d  61 64 64 72 04 61 72 70   ·128·in- addr·arp
0050  61 00 00 0c 00 01                                  a·····
```

## dns-ethereal-trace-3 file:

13. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

A. It was sent to 128.238.29.22 which is my default DNS server.

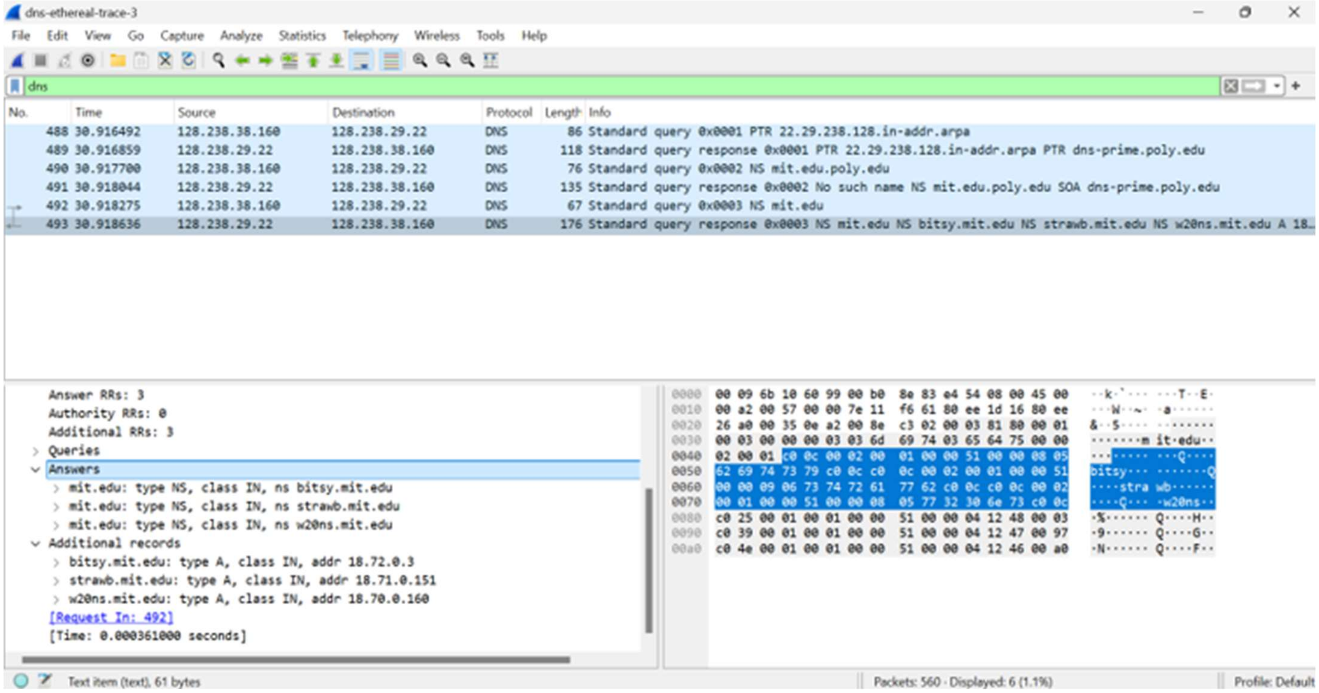
14. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

A. The query is of type NS and it doesn’t contain any answers.

15. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?

A. The nameservers are bitsy, strawb and w20ns. We can find their IP addresses if we expand the Additional records field in Wireshark as seen below.

16. Provide a screenshot.


dns-ethereal-trace-3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

```
No.   Time       Source          Destination     Protocol Length Info
  488 30.916492  128.238.38.160  128.238.29.22   DNS        86 Standard query 0x0001 PTR 22.29.238.128.in-addr.arpa
  489 30.916859  128.238.29.22   128.238.38.160  DNS       118 Standard query response 0x0001 PTR 22.29.238.128.in-addr.arpa PTR dns-prime.poly.edu
  490 30.917700  128.238.38.160  128.238.29.22   DNS        76 Standard query 0x0002 NS mit.edu.poly.edu
  491 30.918044  128.238.29.22   128.238.38.160  DNS       135 Standard query response 0x0002 No such name NS mit.edu.poly.edu SOA dns-prime.poly.edu
  492 30.918275  128.238.38.160  128.238.29.22   DNS        67 Standard query 0x0003 NS mit.edu
  493 30.918636  128.238.29.22   128.238.38.160  DNS       176 Standard query response 0x0003 NS mit.edu NS bitsy.mit.edu NS strawb.mit.edu NS w20ns.mit.edu A 18…
```

```
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 3
  > Queries
  v Answers
    > mit.edu: type NS, class IN, ns bitsy.mit.edu
    > mit.edu: type NS, class IN, ns strawb.mit.edu
    > mit.edu: type NS, class IN, ns w20ns.mit.edu
  v Additional records
    > bitsy.mit.edu: type A, class IN, addr 18.72.0.3
    > strawb.mit.edu: type A, class IN, addr 18.71.0.151
    > w20ns.mit.edu: type A, class IN, addr 18.70.0.160
    [Request In: 492]
    [Time: 0.000361000 seconds]
```

```
0000  00 09 6b 10 60 99 00 b0  8e 83 e4 54 08 00 45 00   ··k·`··· ···T··E·
0010  00 a2 00 57 00 00 7e 11  f6 61 80 ee 1d 16 80 ee   ···W··~· ·a······
0020  26 a0 00 35 0e a2 00 8e  c3 02 00 03 81 80 00 01   &··5···· ········
0030  00 03 00 00 00 03 03 6d  69 74 03 65 64 75 00 00   ·······m it·edu··
0040  02 00 01 c0 0c 00 02 00  01 00 00 51 00 00 08 05   ········ ···Q····
0050  62 69 74 73 79 c0 0c c0  0c 00 02 00 01 00 00 51   bitsy··· ·······Q
0060  00 00 09 06 73 74 72 61  77 62 c0 0c c0 0c 00 02   ····stra wb······
0070  00 01 00 00 51 00 00 08  05 77 32 30 6e 73 c0 0c   ····Q··· ·w20ns··
0080  c0 25 00 01 00 01 00 00  51 00 00 04 12 48 00 03   ·%······ Q····H··
0090  c0 39 00 01 00 01 00 00  51 00 00 04 12 47 00 97   ·9······ Q····G··
00a0  c0 4e 00 01 00 01 00 00  51 00 00 04 12 46 00 a0   ·N······ Q····F··
```

Text item (text), 61 bytes | Packets: 560 · Displayed: 6 (1.1%) | Profile: Default

## **dns-ethereal-trace-4 file:**

17. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

A. The query is sent to 18.72.0.3 which corresponds to bitsy.mit.edu.

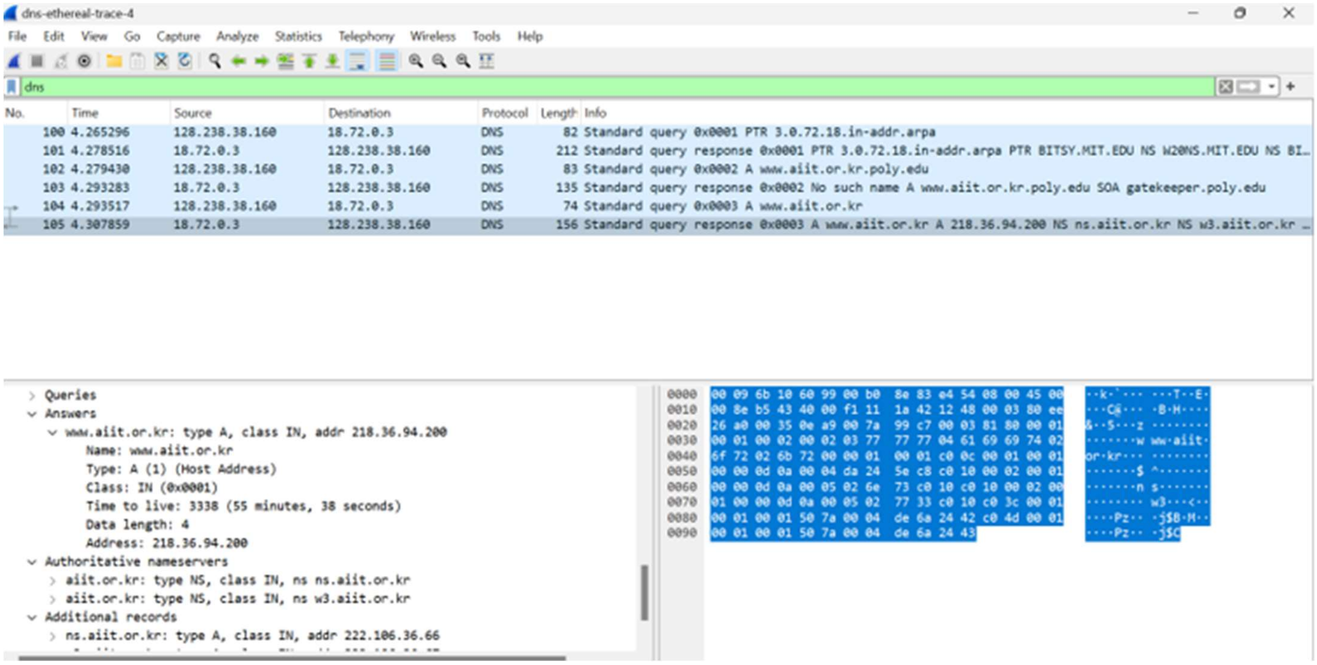
18. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

A. It’s a standard type A query that doesn’t contain any answers.

19. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

A. One answer is provided in the DNS response message. It contains the following:
Name, type, class, data length, address.

20. Provide a screenshot.



dns-ethereal-trace-4
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.   Time      Source          Destination     Protocol Length Info
  100 4.265296  128.238.38.160  18.72.0.3       DNS       82 Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
  101 4.278516  18.72.0.3       128.238.38.160  DNS      212 Standard query response 0x0001 PTR 3.0.72.18.in-addr.arpa PTR BITSY.MIT.EDU NS W20NS.MIT.EDU NS BI…
  102 4.279430  128.238.38.160  18.72.0.3       DNS       83 Standard query 0x0002 A www.aiit.or.kr.poly.edu
  103 4.293283  18.72.0.3       128.238.38.160  DNS      135 Standard query response 0x0002 No such name A www.aiit.or.kr.poly.edu SOA gatekeeper.poly.edu
  104 4.293517  128.238.38.160  18.72.0.3       DNS       74 Standard query 0x0003 A www.aiit.or.kr
  105 4.307859  18.72.0.3       128.238.38.160  DNS      156 Standard query response 0x0003 A www.aiit.or.kr A 218.36.94.200 NS ns.aiit.or.kr NS w3.aiit.or.kr …
```

```
> Queries
v Answers
  v www.aiit.or.kr: type A, class IN, addr 218.36.94.200
      Name: www.aiit.or.kr
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 3338 (55 minutes, 38 seconds)
      Data length: 4
      Address: 218.36.94.200
v Authoritative nameservers
  > aiit.or.kr: type NS, class IN, ns ns.aiit.or.kr
  > aiit.or.kr: type NS, class IN, ns w3.aiit.or.kr
v Additional records
  > ns.aiit.or.kr: type A, class IN, addr 222.106.36.66
```

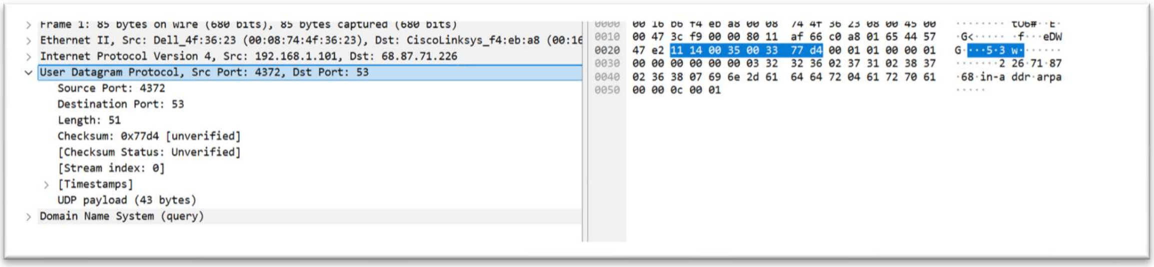
```
0000  00 09 6b 10 60 99 00 b0  8e 83 e4 54 08 00 45 00   ··k·`··· ···T··E·
0010  00 8e b5 43 40 00 f1 11  1a 42 12 48 00 03 80 ee   ···C@··· ·B·H····
0020  26 a0 00 35 0e a9 00 7a  99 c7 00 03 81 80 00 01   &··5···z ········
0030  00 01 00 02 00 02 03 77  77 77 04 61 69 69 74 02   ·······w ww·aiit·
0040  6f 72 02 6b 72 00 00 01  00 01 c0 0c 00 01 00 01   or·kr··· ········
0050  00 00 0d 0a 00 04 da 24  5e c8 c0 10 00 02 00 01   ·······$ ^·······
0060  00 00 0d 0a 00 05 02 6e  73 c0 10 c0 10 00 02 00   ·······n s·······
0070  01 00 00 0d 0a 00 05 02  77 33 c0 10 c0 3c 00 01   ········ w3···<··
0080  00 01 00 01 50 7a 00 04  de 6a 24 42 c0 4d 00 01   ····Pz·· ·j$B·M··
0090  00 01 00 01 50 7a 00 04  de 6a 24 43              ····Pz·· ·j$C
```

## Exercise # 2 Tracing UDP with Wireshark

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.

A. UDP header contains 4 fields:

1.source port; 2. destination port; 3. length; 4. Checksum



```
> 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: CiscoLinksys_f4:eb:a8 (00:16
> Internet Protocol Version 4, Src: 192.168.1.101, Dst: 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]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (43 bytes)
> Domain Name System (query)
```

```
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                                     ·····
```

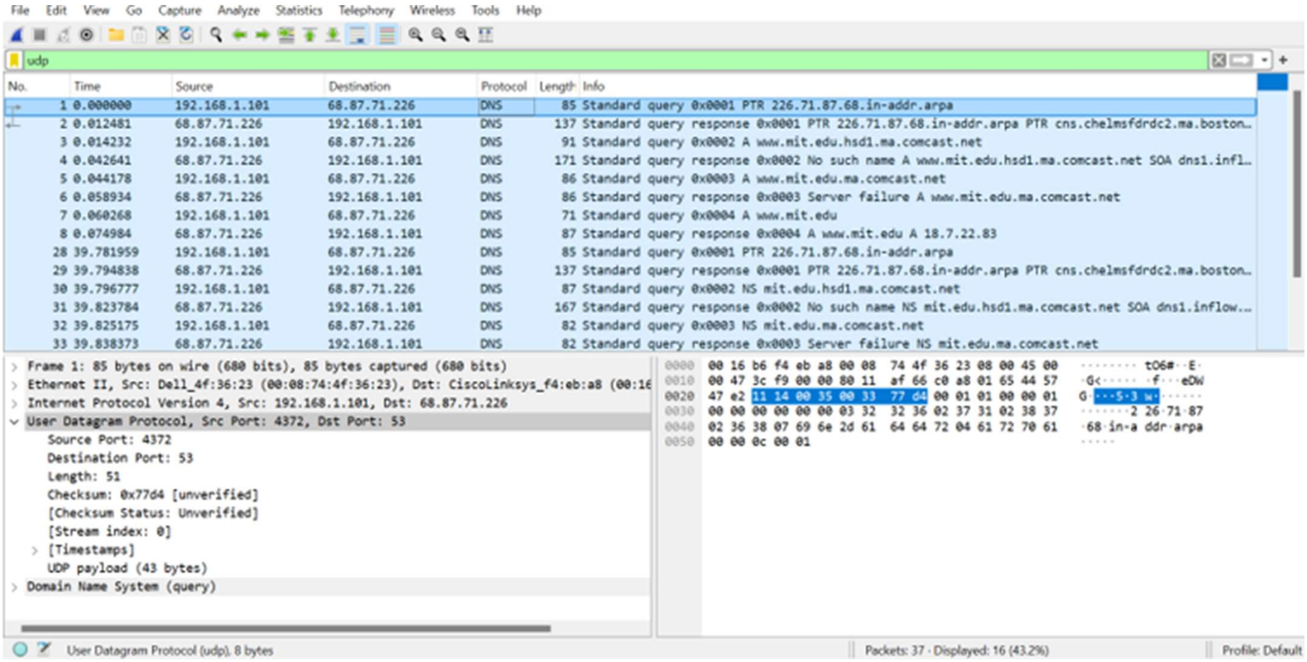
2. By consulting the displayed information in Wireshark's packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.

A. The UDP header has a fixed length of 8 bytes. Each of these 4 header fields is 2 bytes long.

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.

A. The length field specifies the number of bytes in the UDP segment (header plus data). An explicit length value is needed since the size of the data field may differ from one UDP segment to the next.

The length of UDP payload for selected packet is 43 bytes. 51 bytes - 8 bytes = 43 bytes.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp

```
No.  Time       Source          Destination     Protocol Length Info
   1 0.000000   192.168.1.101   68.87.71.226    DNS       85 Standard query 0x0001 PTR 226.71.87.68.in-addr.arpa
   2 0.012481   68.87.71.226    192.168.1.101   DNS      137 Standard query response 0x0001 PTR 226.71.87.68.in-addr.arpa PTR cns.chelmsfdrdc2.ma.boston…
   3 0.014232   192.168.1.101   68.87.71.226    DNS       91 Standard query 0x0002 A www.mit.edu.hsd1.ma.comcast.net
   4 0.042641   68.87.71.226    192.168.1.101   DNS      171 Standard query response 0x0002 No such name A www.mit.edu.hsd1.ma.comcast.net SOA dns1.infl…
   5 0.044178   192.168.1.101   68.87.71.226    DNS       86 Standard query 0x0003 A www.mit.edu.ma.comcast.net
   6 0.058934   68.87.71.226    192.168.1.101   DNS       86 Standard query response 0x0003 Server failure A www.mit.edu.ma.comcast.net
   7 0.060268   192.168.1.101   68.87.71.226    DNS       71 Standard query 0x0004 A www.mit.edu
   8 0.074984   68.87.71.226    192.168.1.101   DNS       87 Standard query response 0x0004 A www.mit.edu A 18.7.22.83
  28 39.781959  192.168.1.101   68.87.71.226    DNS       85 Standard query 0x0001 PTR 226.71.87.68.in-addr.arpa
  29 39.794838  68.87.71.226    192.168.1.101   DNS      137 Standard query response 0x0001 PTR 226.71.87.68.in-addr.arpa PTR cns.chelmsfdrdc2.ma.boston…
  30 39.796777  192.168.1.101   68.87.71.226    DNS       87 Standard query 0x0002 NS mit.edu.hsd1.ma.comcast.net
  31 39.823784  68.87.71.226    192.168.1.101   DNS      167 Standard query response 0x0002 No such name NS mit.edu.hsd1.ma.comcast.net SOA dns1.inflow…
  32 39.825175  192.168.1.101   68.87.71.226    DNS       82 Standard query 0x0003 NS mit.edu.ma.comcast.net
  33 39.838373  68.87.71.226    192.168.1.101   DNS       82 Standard query response 0x0003 Server failure NS mit.edu.ma.comcast.net
```

```
> 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: CiscoLinksys_f4:eb:a8 (00:16
> Internet Protocol Version 4, Src: 192.168.1.101, Dst: 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]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (43 bytes)
> Domain Name System (query)
```

```
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····5·3w·······
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                                     ·····
```

```
User Datagram Protocol (udp), 8 bytes      Packets: 37 · Displayed: 16 (43.2%)      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)

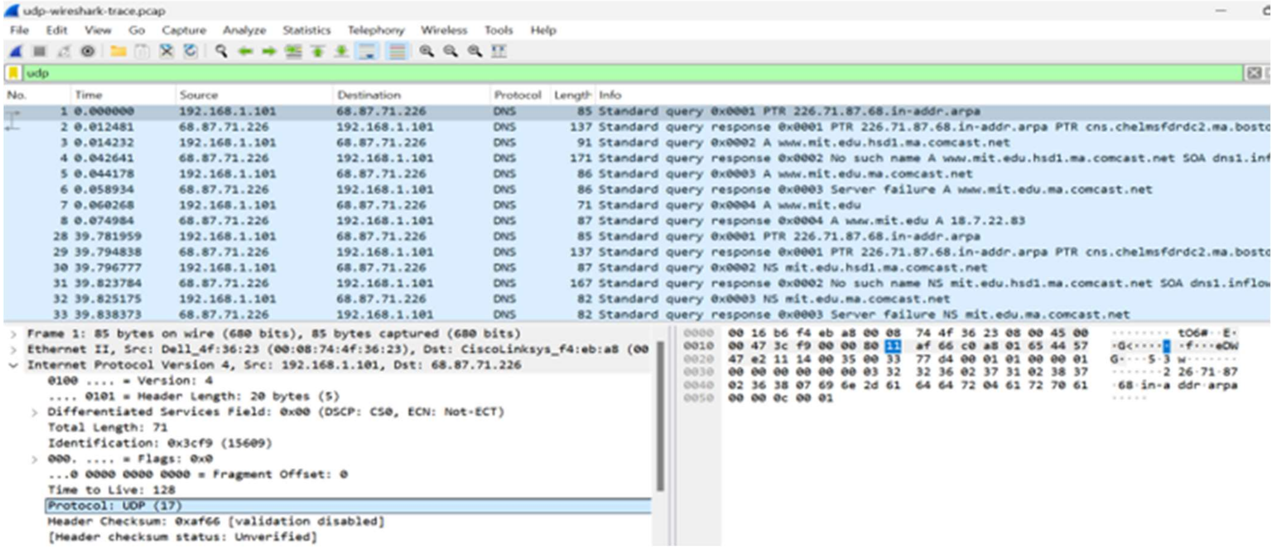
A. The maximum number of bytes that can be included in a UDP payload is (2^16 – 1) bytes plus the header bytes. This gives 65535 bytes – 8 bytes = 65527 bytes.

5. What is the largest possible source port number? (Hint: see the hint in 4.)

A. The largest possible source port number is (2^16 – 1) = 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).

A. The IP protocol number for UDP is 0x11 hex, which is 17 in decimal value.


udp-wireshark-trace.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp

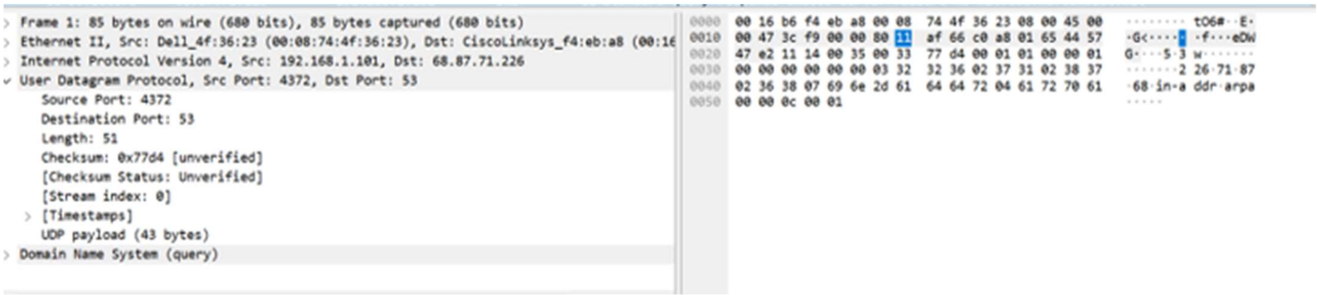
```
No.  Time       Source          Destination     Protocol Length Info
   1 0.000000   192.168.1.101   68.87.71.226    DNS       85 Standard query 0x0001 PTR 226.71.87.68.in-addr.arpa
   2 0.012481   68.87.71.226    192.168.1.101   DNS      137 Standard query response 0x0001 PTR 226.71.87.68.in-addr.arpa PTR cns.chelmsfdrdc2.ma.bosto
   3 0.014232   192.168.1.101   68.87.71.226    DNS       91 Standard query 0x0002 A www.mit.edu.hsd1.ma.comcast.net
   4 0.042641   68.87.71.226    192.168.1.101   DNS      171 Standard query response 0x0002 No such name A www.mit.edu.hsd1.ma.comcast.net SOA dns1.inf
   5 0.044178   192.168.1.101   68.87.71.226    DNS       86 Standard query 0x0003 A www.mit.edu.ma.comcast.net
   6 0.058934   68.87.71.226    192.168.1.101   DNS       86 Standard query response 0x0003 Server failure A www.mit.edu.ma.comcast.net
   7 0.060268   192.168.1.101   68.87.71.226    DNS       71 Standard query 0x0004 A www.mit.edu
   8 0.074984   68.87.71.226    192.168.1.101   DNS       87 Standard query response 0x0004 A www.mit.edu A 18.7.22.83
  28 39.781959  192.168.1.101   68.87.71.226    DNS       85 Standard query 0x0001 PTR 226.71.87.68.in-addr.arpa
  29 39.794838  68.87.71.226    192.168.1.101   DNS      137 Standard query response 0x0001 PTR 226.71.87.68.in-addr.arpa PTR cns.chelmsfdrdc2.ma.bosto
  30 39.796777  192.168.1.101   68.87.71.226    DNS       87 Standard query 0x0002 NS mit.edu.hsd1.ma.comcast.net
  31 39.823784  68.87.71.226    192.168.1.101   DNS      167 Standard query response 0x0002 No such name NS mit.edu.hsd1.ma.comcast.net SOA dns1.inflow
  32 39.825175  192.168.1.101   68.87.71.226    DNS       82 Standard query 0x0003 NS mit.edu.ma.comcast.net
  33 39.838373  68.87.71.226    192.168.1.101   DNS       82 Standard query response 0x0003 Server failure NS mit.edu.ma.comcast.net
```

```
> 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: CiscoLinksys_f4:eb:a8 (00
v Internet Protocol Version 4, Src: 192.168.1.101, Dst: 68.87.71.226
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 71
    Identification: 0x3cf9 (15609)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0xaf66 [validation disabled]
    [Header checksum status: 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····5·3w·······
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                                     ·····
```

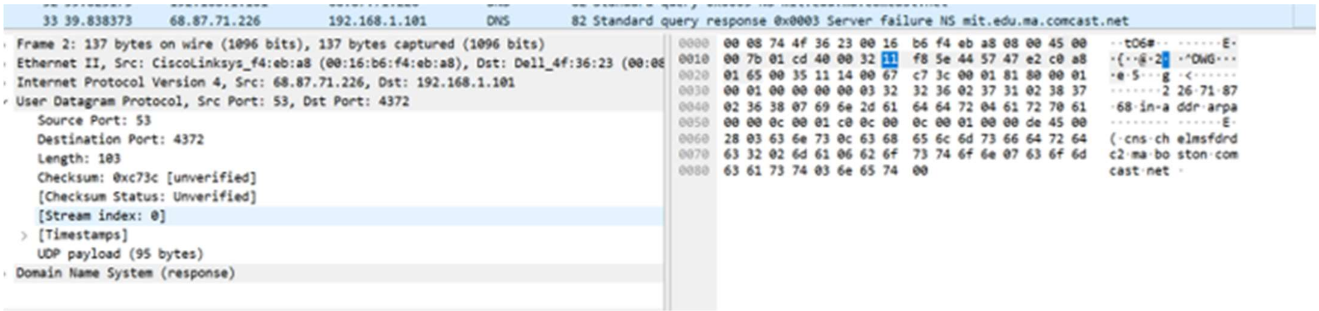
7. Examine a pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet. (Hint: for a second packet to be sent in response to a first packet, the sender of the first packet should be the destination of the second packet). Describe the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

A. 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.



```
> 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: CiscoLinksys_f4:eb:a8 (00:16
> Internet Protocol Version 4, Src: 192.168.1.101, Dst: 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]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (43 bytes)
> Domain Name System (query)
```

```
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                                     ·····
```



```
   33 39.838373   68.87.71.226    192.168.1.101    DNS    82 Standard query response 0x0003 Server failure NS mit.edu.ma.comcast.net
```

```
> Frame 2: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits)
> Ethernet II, Src: CiscoLinksys_f4:eb:a8 (00:16:b6:f4:eb:a8), Dst: Dell_4f:36:23 (00:08
> Internet Protocol Version 4, Src: 68.87.71.226, Dst: 192.168.1.101
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]
  > [Timestamps]
    UDP payload (95 bytes)
> Domain Name System (response)
```

```
0000  00 08 74 4f 36 23 00 16  b6 f4 eb a8 08 00 45 00   ··tO6#·· ······E·
0010  00 7b 01 cd 40 00 32 11  f8 5e 44 57 47 e2 c0 a8   ·{··@·2· ·^DWG···
0020  01 65 00 35 11 14 00 67  c7 3c 00 01 81 80 00 01   ·e·5···g ·<······
0030  00 01 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 c0 0c 00  0c 00 01 00 00 de 45 00   ········ ······E·
0060  28 03 63 6e 73 0c 63 68  65 6c 6d 73 66 64 72 64   (·cns·ch elmsfdrd
0070  63 32 02 6d 61 06 62 6f  73 74 6f 6e 07 63 6f 6d   c2·ma·bo ston·com
0080  63 61 73 74 03 6e 65 74  00                        cast·net ·
```