Jeremy Neal
CMSC 481 - Networking
Oct 03, 2014
Lab 3

1. nslookup www.aiit.or.kr

```
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
www.aiit.or.kr canonical name = aiit.or.kr.
Name:      aiit.or.kr
Address:   203.251.205.241
```

   The ip address is 203.251.205.241

2. nslookup -TYPE=NS ox.ac.uk

```
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
ox.ac.uk        nameserver = dns1.ox.ac.uk.
ox.ac.uk        nameserver = ns2.ja.net.
ox.ac.uk        nameserver = dns0.ox.ac.uk.
ox.ac.uk        nameserver = dns2.ox.ac.uk.

Authoritative answers can be found from:
ns2.ja.net      internet address = 193.63.105.17
ns2.ja.net      has AAAA address 2001:630:0:45::11
dns0.ox.ac.uk   internet address = 129.67.1.190
dns1.ox.ac.uk   internet address = 129.67.1.191
dns2.ox.ac.uk   internet address = 163.1.2.190
```

3. nslookup mail.yahoo.com dns1.ox.ac.uk

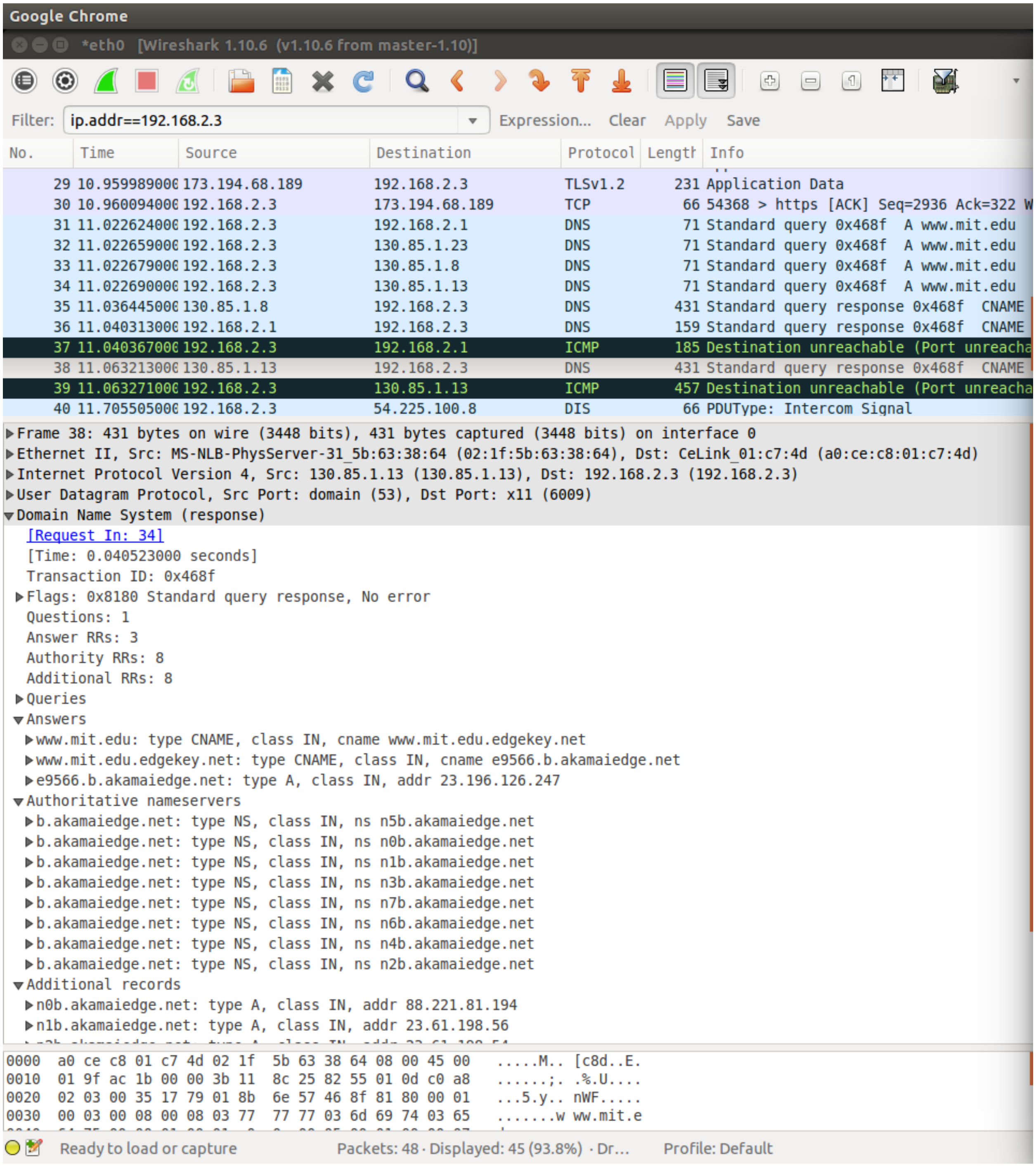
```
Server:         dns1.ox.ac.uk
Address:        129.67.1.191#53

** server can't find mail.yahoo.com: REFUSED
```

   The Yahoo mail servers are encrypted, so this is problematic.

4. Both the DNS requests and responses use UDP.
5. The destination port of the DNS requests is port 53. The source port of the DNS responses is also port 53.
6. The requests are sent to 130.85.1.23, a local DNS server. It is not the same IP given if you use `nslookup.`
7. The queries are standard queries, type A, and they contain no answers.
8. Each DNS response contains a single answer. The answers contain the IP address of the next link in the path to the destination.
9. Yes, the destination IP matches the one from the DNS response. It is caching this information locally so another DNS lookup won't be necessary.
10. Another DNS query is only needed if the IP is unknown. In this case, it does, as the images are located elsewhere.
11. The destination port of the query is 53, and the source port of the response is also 53.
12. 130.85.1.{8,13,23}. These are all local DNS servers. One is the default.
13. Type A queries with no answers.
14. Each response contains three answers. Each answer corresponds to a DNS server for the destination IP.

15.



Filter: ip.addr==192.168.2.3

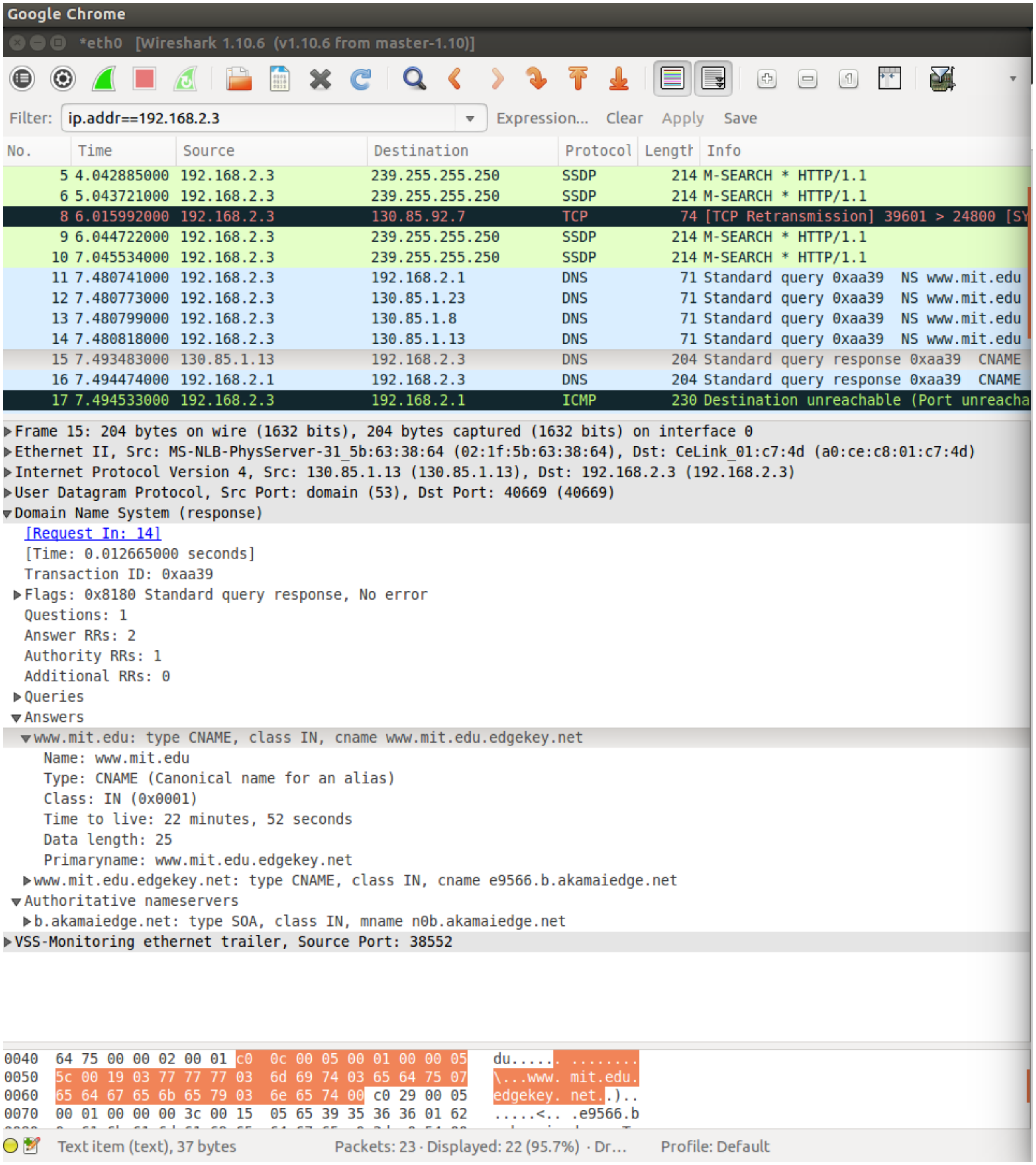
```
No.   Time         Source          Destination     Protocol Lengtl Info
   29 10.95998900С 173.194.68.189  192.168.2.3     TLSv1.2   231 Application Data
   30 10.96009400С 192.168.2.3     173.194.68.189  TCP        66 54368 > https [ACK] Seq=2936 Ack=322 W
   31 11.02262400С 192.168.2.3     192.168.2.1     DNS        71 Standard query 0x468f  A www.mit.edu
   32 11.02265900С 192.168.2.3     130.85.1.23     DNS        71 Standard query 0x468f  A www.mit.edu
   33 11.02267900С 192.168.2.3     130.85.1.8      DNS        71 Standard query 0x468f  A www.mit.edu
   34 11.02269000С 192.168.2.3     130.85.1.13     DNS        71 Standard query 0x468f  A www.mit.edu
   35 11.03644500С 130.85.1.8      192.168.2.3     DNS       431 Standard query response 0x468f  CNAME
   36 11.04031300С 192.168.2.1     192.168.2.3     DNS       159 Standard query response 0x468f  CNAME
   37 11.04036700С 192.168.2.3     192.168.2.1     ICMP      185 Destination unreachable (Port unreacha
   38 11.06321300С 130.85.1.13     192.168.2.3     DNS       431 Standard query response 0x468f  CNAME
   39 11.06327100С 192.168.2.3     130.85.1.13     ICMP      457 Destination unreachable (Port unreacha
   40 11.70550500С 192.168.2.3     54.225.100.8    DIS        66 PDUType: Intercom Signal
```

```
▶Frame 38: 431 bytes on wire (3448 bits), 431 bytes captured (3448 bits) on interface 0
▶Ethernet II, Src: MS-NLB-PhysServer-31_5b:63:38:64 (02:1f:5b:63:38:64), Dst: CeLink_01:c7:4d (a0:ce:c8:01:c7:4d)
▶Internet Protocol Version 4, Src: 130.85.1.13 (130.85.1.13), Dst: 192.168.2.3 (192.168.2.3)
▶User Datagram Protocol, Src Port: domain (53), Dst Port: x11 (6009)
▼Domain Name System (response)
  [Request In: 34]
  [Time: 0.040523000 seconds]
  Transaction ID: 0x468f
 ▶Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Authority RRs: 8
  Additional RRs: 8
 ▶Queries
 ▼Answers
  ▶www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
  ▶www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.b.akamaiedge.net
  ▶e9566.b.akamaiedge.net: type A, class IN, addr 23.196.126.247
 ▼Authoritative nameservers
  ▶b.akamaiedge.net: type NS, class IN, ns n5b.akamaiedge.net
  ▶b.akamaiedge.net: type NS, class IN, ns n0b.akamaiedge.net
  ▶b.akamaiedge.net: type NS, class IN, ns n1b.akamaiedge.net
  ▶b.akamaiedge.net: type NS, class IN, ns n3b.akamaiedge.net
  ▶b.akamaiedge.net: type NS, class IN, ns n7b.akamaiedge.net
  ▶b.akamaiedge.net: type NS, class IN, ns n6b.akamaiedge.net
  ▶b.akamaiedge.net: type NS, class IN, ns n4b.akamaiedge.net
  ▶b.akamaiedge.net: type NS, class IN, ns n2b.akamaiedge.net
 ▼Additional records
  ▶n0b.akamaiedge.net: type A, class IN, addr 88.221.81.194
  ▶n1b.akamaiedge.net: type A, class IN, addr 23.61.198.56
```

```
0000  a0 ce c8 01 c7 4d 02 1f  5b 63 38 64 08 00 45 00   .....M.. [c8d..E.
0010  01 9f ac 1b 00 00 3b 11  8c 25 82 55 01 0d c0 a8   ......;. .%.U....
0020  02 03 00 35 17 79 01 8b  6e 57 46 8f 81 80 00 01   ...5.y.. nWF.....
0030  00 03 00 08 00 08 03 77  77 77 03 6d 69 74 03 65   .......w ww.mit.e
```

Ready to load or capture   Packets: 48 · Displayed: 45 (93.8%) · Dr...   Profile: Default

16. The queries were sent to the same three DNS servers. Again, one of these is the default.
17. The queries are now Type NS. Queries do not contain answers.
18. The responses contain the nameserver `www.mit.edu.edgekey.net` and `e9566.b.akamaiedge.net`, but no IP addresses for either name server.

19. 

Filter: ip.addr==192.168.2.3

```
No.  Time         Source        Destination      Protocol Length Info
   5 4.042885000  192.168.2.3   239.255.255.250  SSDP     214 M-SEARCH * HTTP/1.1
   6 5.043721000  192.168.2.3   239.255.255.250  SSDP     214 M-SEARCH * HTTP/1.1
   8 6.015992000  192.168.2.3   130.85.92.7      TCP       74 [TCP Retransmission] 39601 > 24800 [SY
   9 6.044722000  192.168.2.3   239.255.255.250  SSDP     214 M-SEARCH * HTTP/1.1
  10 7.045534000  192.168.2.3   239.255.255.250  SSDP     214 M-SEARCH * HTTP/1.1
  11 7.480741000  192.168.2.3   192.168.2.1      DNS       71 Standard query 0xaa39  NS www.mit.edu
  12 7.480773000  192.168.2.3   130.85.1.23      DNS       71 Standard query 0xaa39  NS www.mit.edu
  13 7.480799000  192.168.2.3   130.85.1.8       DNS       71 Standard query 0xaa39  NS www.mit.edu
  14 7.480818000  192.168.2.3   130.85.1.13      DNS       71 Standard query 0xaa39  NS www.mit.edu
  15 7.493483000  130.85.1.13   192.168.2.3      DNS      204 Standard query response 0xaa39  CNAME
  16 7.494474000  192.168.2.1   192.168.2.3      DNS      204 Standard query response 0xaa39  CNAME
  17 7.494533000  192.168.2.3   192.168.2.1      ICMP     230 Destination unreachable (Port unreacha
```

```
▶Frame 15: 204 bytes on wire (1632 bits), 204 bytes captured (1632 bits) on interface 0
▶Ethernet II, Src: MS-NLB-PhysServer-31_5b:63:38:64 (02:1f:5b:63:38:64), Dst: CeLink_01:c7:4d (a0:ce:c8:01:c7:4d)
▶Internet Protocol Version 4, Src: 130.85.1.13 (130.85.1.13), Dst: 192.168.2.3 (192.168.2.3)
▶User Datagram Protocol, Src Port: domain (53), Dst Port: 40669 (40669)
▼Domain Name System (response)
   [Request In: 14]
   [Time: 0.012665000 seconds]
   Transaction ID: 0xaa39
  ▶Flags: 0x8180 Standard query response, No error
   Questions: 1
   Answer RRs: 2
   Authority RRs: 1
   Additional RRs: 0
  ▶Queries
  ▼Answers
   ▼www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
      Name: www.mit.edu
      Type: CNAME (Canonical name for an alias)
      Class: IN (0x0001)
      Time to live: 22 minutes, 52 seconds
      Data length: 25
      Primaryname: www.mit.edu.edgekey.net
   ▶www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.b.akamaiedge.net
  ▼Authoritative nameservers
   ▶b.akamaiedge.net: type SOA, class IN, mname n0b.akamaiedge.net
▶VSS-Monitoring ethernet trailer, Source Port: 38552
```

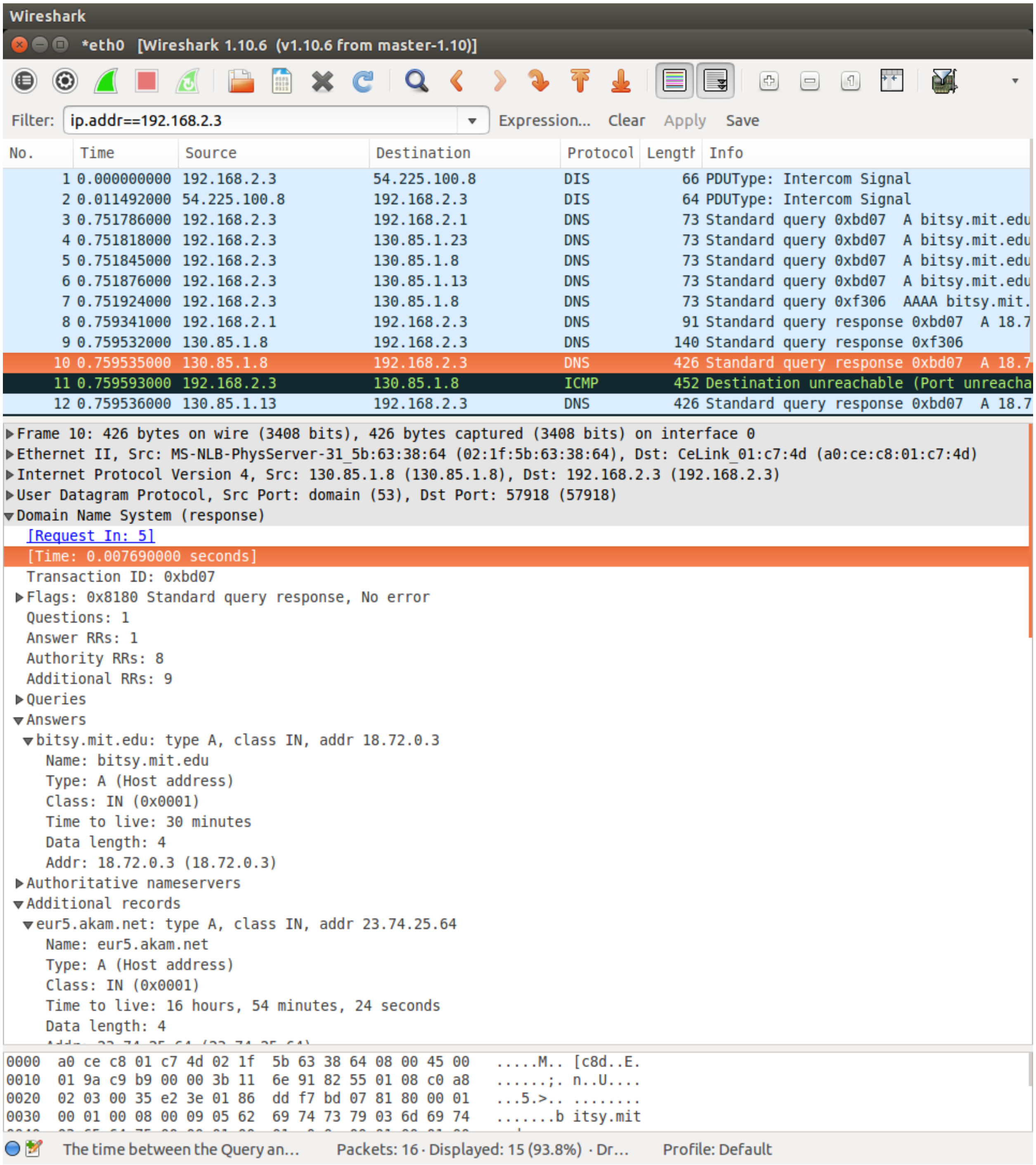
```
0040  64 75 00 00 02 00 01 c0  0c 00 05 00 01 00 00 05   du...... ........
0050  5c 00 19 03 77 77 77 03  6d 69 74 03 65 64 75 07   \...www. mit.edu.
0060  65 64 67 65 6b 65 79 03  6e 65 74 00 c0 29 00 05   edgekey. net..)..
0070  00 01 00 00 00 3c 00 15  05 65 39 35 36 36 01 62   .....<.. .e9566.b
```

Text item (text), 37 bytes   Packets: 23 · Displayed: 22 (95.7%) · Dr...   Profile: Default

20. The queries are sent to the same DNS servers again. These are the local DNS servers.

21. These are type A queries, since -TYPE=NS was not declared. The queries contain no answers.

22. Each response contains a single answer, containing the name of the DNS server (bitsy.mit.edu) and its IP address (18.72.0.3).

23. 

Filter: ip.addr==192.168.2.3

```
No.  Time         Source         Destination    Protocol Length Info
   1 0.000000000  192.168.2.3    54.225.100.8   DIS        66 PDUType: Intercom Signal
   2 0.011492000  54.225.100.8   192.168.2.3    DIS        64 PDUType: Intercom Signal
   3 0.751786000  192.168.2.3    192.168.2.1    DNS        73 Standard query 0xbd07  A bitsy.mit.edu
   4 0.751818000  192.168.2.3    130.85.1.23    DNS        73 Standard query 0xbd07  A bitsy.mit.edu
   5 0.751845000  192.168.2.3    130.85.1.8     DNS        73 Standard query 0xbd07  A bitsy.mit.edu
   6 0.751876000  192.168.2.3    130.85.1.13    DNS        73 Standard query 0xbd07  A bitsy.mit.edu
   7 0.751924000  192.168.2.3    130.85.1.8     DNS        73 Standard query 0xf306  AAAA bitsy.mit.
   8 0.759341000  192.168.2.1    192.168.2.3    DNS        91 Standard query response 0xbd07  A 18.7
   9 0.759532000  130.85.1.8     192.168.2.3    DNS       140 Standard query response 0xf306
  10 0.759535000  130.85.1.8     192.168.2.3    DNS       426 Standard query response 0xbd07  A 18.7
  11 0.759593000  192.168.2.3    130.85.1.8     ICMP      452 Destination unreachable (Port unreacha
  12 0.759536000  130.85.1.13    192.168.2.3    DNS       426 Standard query response 0xbd07  A 18.7
```

```
▶Frame 10: 426 bytes on wire (3408 bits), 426 bytes captured (3408 bits) on interface 0
▶Ethernet II, Src: MS-NLB-PhysServer-31_5b:63:38:64 (02:1f:5b:63:38:64), Dst: CeLink_01:c7:4d (a0:ce:c8:01:c7:4d)
▶Internet Protocol Version 4, Src: 130.85.1.8 (130.85.1.8), Dst: 192.168.2.3 (192.168.2.3)
▶User Datagram Protocol, Src Port: domain (53), Dst Port: 57918 (57918)
▼Domain Name System (response)
  [Request In: 5]
  [Time: 0.007690000 seconds]
  Transaction ID: 0xbd07
 ▶Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 8
  Additional RRs: 9
 ▶Queries
 ▼Answers
  ▼bitsy.mit.edu: type A, class IN, addr 18.72.0.3
     Name: bitsy.mit.edu
     Type: A (Host address)
     Class: IN (0x0001)
     Time to live: 30 minutes
     Data length: 4
     Addr: 18.72.0.3 (18.72.0.3)
 ▶Authoritative nameservers
 ▼Additional records
  ▼eur5.akam.net: type A, class IN, addr 23.74.25.64
     Name: eur5.akam.net
     Type: A (Host address)
     Class: IN (0x0001)
     Time to live: 16 hours, 54 minutes, 24 seconds
     Data length: 4
     Addr: 23.74.25.64 (23.74.25.64)
```

```
0000  a0 ce c8 01 c7 4d 02 1f  5b 63 38 64 08 00 45 00   .....M.. [c8d..E.
0010  01 9a c9 b9 00 00 3b 11  6e 91 82 55 01 08 c0 a8   ......;. n..U....
0020  02 03 00 35 e2 3e 01 86  dd f7 bd 07 81 80 00 01   ...5.>.. ........
0030  00 01 00 08 00 09 05 62  69 74 73 79 03 6d 69 74   .......b itsy.mit
```

The time between the Query an...   Packets: 16 · Displayed: 15 (93.8%) · Dr...   Profile: Default