CSE 3300 - Homework 2

Nicholas Lambourne - ndl17004 - 2749404

Question 1

Total time elapsed from click to object receipt:

$$= 2 \cdot RTT_0 + RTT_1 + RTT_2 + \ldots RTT_n$$

Question 2

a) 1 HTML File + 8 other small objects = 9 total files, over non-persistent:

$$= 9 \cdot 2 \cdot RTT_0 + RTT_1 + RTT_2 + \ldots RTT_n$$
$$= 18 \cdot RTT_0 + RTT_1 + RTT_2 + \ldots RTT_n$$

b) 1 HTML + 8 other small objects = 9 total files, over non-persistent with 5 parallel connections. But HTML has to be retrieved first, so 2RTT (for HTML) + 2*2RTT (two lots of parallel connections for the objects).

$$= 2 \cdot RTT_0 + 2 \cdot 2 \cdot RTT_0 + RTT_1 + RTT_2 + \ldots RTT_n$$
$$= 6 \cdot RTT_0 + RTT_1 + RTT_2 + \ldots RTT_n$$

c) 1 HTML + 8 other small objects = 9 objects over persistent HTTP. 2RTT to set up the connection. 2RTT to set up the persistent connection, 1RTT for HTML + 1RTT for all referenced objects.

$$= 2 \cdot RTT_0 + RTT_0 + RTT_0 + RTT_1 + RTT_2 + \ldots + RTT_n$$
$$= 4 \cdot RTT_0 + RTT_1 + RTT_2 + \ldots RTT_n$$

Question 3

a)

1. a.root-servers.net
2. e.root-servers.net
3. a.edu-servers.net
4. msb-cache.net.uconn.edu

b)

google.com:

1. a.root-servers.net
2. l.root-servers.net
3. b.gtld-servers.net
4. ns2.google.com

yahoo.com:

1. a.root-servers.net
2. c.root-servers.net
3. l.gtld-servers.net
4. ns3.yahoo.com

amazon.com:

1. a.root-servers.net
2. g.root-servers.net
3. b.gtld-servers.net
4. ns3.p31.dynect.net

Question 4

MAIL FROM: is the return address, for contact purposes.

FROM: is the sender, or author of the message.

It is useful to think of the analogy with regular mail, where the return address (or sender) provided on the reverse of the envelope's exterior (MAIL FROM) may differ from the actual author of the letter inside the envelope (FROM).

Question 5

Number of two-second chunks:

$$\frac{10 \cdot 60}{2} = 300$$

Multiplied by number of quality levels:

$$300 \cdot 6 = 1800$$

Therefore there are 1800 URLs required for one ten minute video provided at six quality levels.

HTTP Wireshark Lab

1. The Basic HTTP GET/response interaction.

   1) My Browser is using HTTP version 1.1. The server is also using HTTP version 1.1.

   2) Accept-Language: en-GB, en-US (i.e. British and American English).

   3) My IP: 67.221.82.156; gaia.cs.umass.edu: 128.119.245.12.

   4) Status code returned: 200 (OK).

   5) Last-Modified: Mon, 26 Feb 2018 06:59:01 GMT.

   6) 552 bytes

   7) Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3
2. The HTTP Conditional GET/response interaction:

   8) The first HTTP/GET request does not have an IF-MODIFIED-SINCE line.

   9) The server did return the contents in a field called 'Line-based text data: text/html'. The size of the response is also larger than the cached version (796 vs 306 bytes).

   10) If-Modified-Since: Tue, 27 Feb 2018 06:22:02 GMT

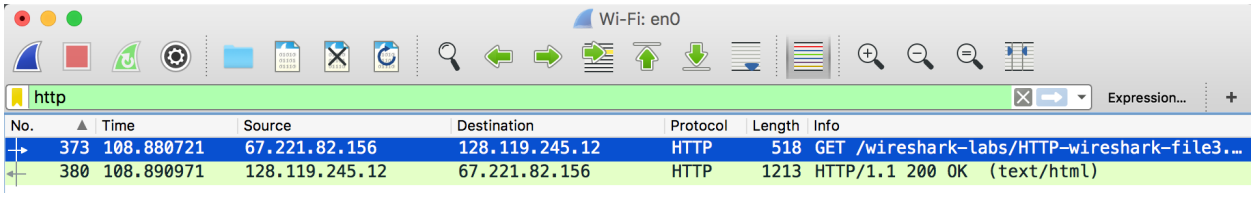
   11) HTTP Response Code: 304 (Not Modified). The server did not explicitly return the contents of the text file as the field described above was not included and the response was significantly smaller than the previous response (see 9, above).
3. Retrieving Long Documents

   12) My browser sent one single GET request message. The first HTTP packet in the trace (#373) contains the GET message for the Bill of Rights.

   13) The response code and phrase were sent back in the second HTTP packet in the trace (#380).

   14) The status code return was 200 (phrase: OK).

   15) Four TCP packets were required to transmit the response and the text of the bill of rights.

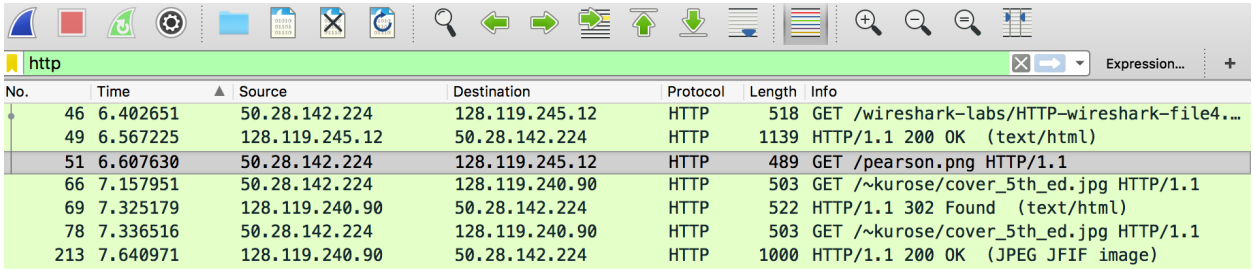


4. HTML Documents with Embedded Objects

   16) My browser sent four GET requests to:

   - 128.119.245.12 (original HTML page)
   - 128.119.245.12 (pearson.png)
   - 128.119.240.90 (cover_5th_ed.jpg)
   - 128.119.240.90 (cover_5th_ed.jpg - after 302 redirect)

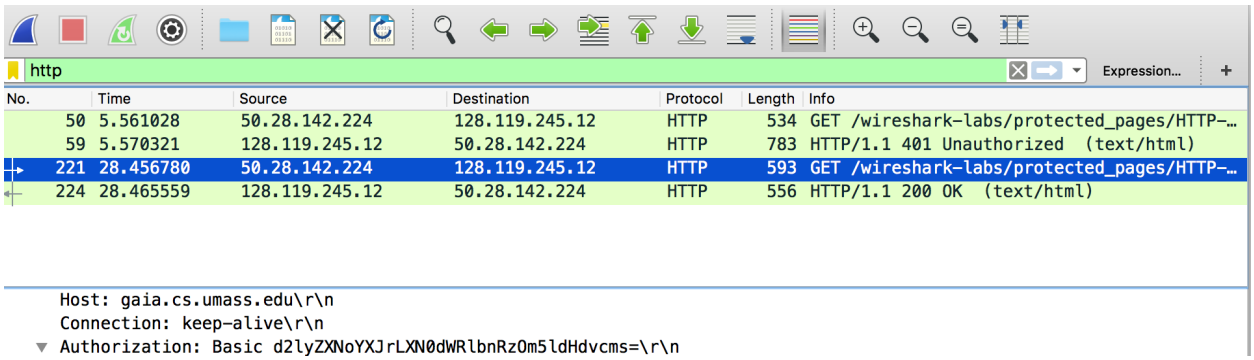
17) The two requests were sent in parallel as both requests were sent before either of the responses had been received. There was one complicating factor in that the textbook cover image had been moved and required a 302 redirect to be found (necessitating another GET request).



5. HTTP Authentication

18) The initial response from the server was 401 (Unauthorized).

19) Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms (Credentials: wireshark-students:network)



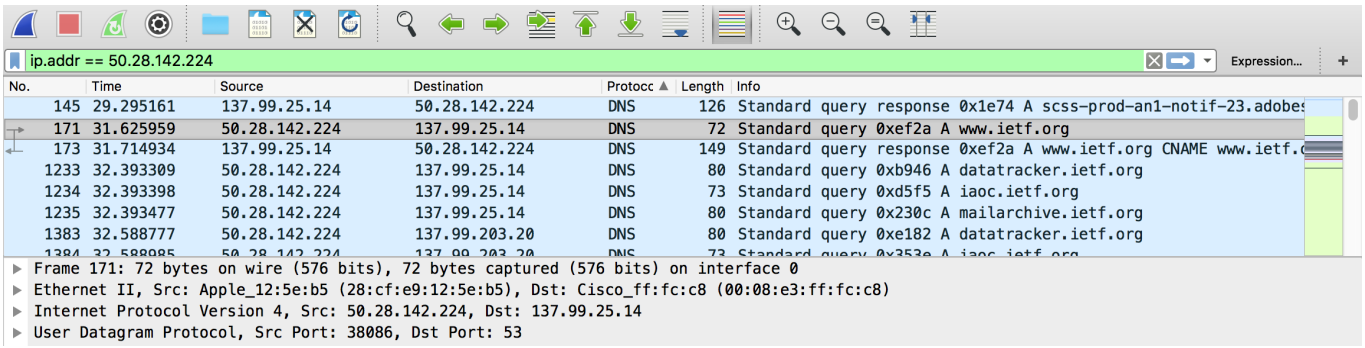
DNS Wireshark Lab

1) wwww.boj.or.jp : 104.97.120.139

2) www.ed.ac.uk : Nameserver = dns0.ed.ac.uk

3) nslookup mail.yahoo.com dns0.ed.ac.uk - > 87.248.114.11 (fd-geoycpi-uno.gycpi.b.yahoodns.net)

4) The DNS requests were sent using UDP, as can be seen at the bottom of the image below.



5) The DNS query destination port is 53. The source response port is also 53. Port 53 is the default port for DNS.

6) The DNS query destination IP address is 137.99.25.14, which is the same as the IP address of the default local DNS server.

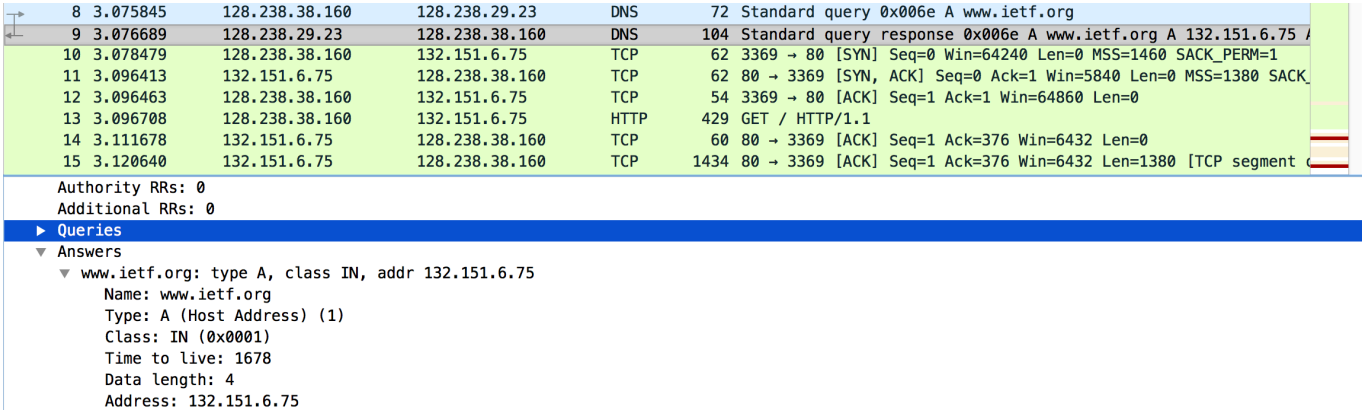
7) The type of DNS query is "A, class IN". It contains zero answers.

```
▼ Domain Name System (query)
    [Response In: 173]
    Transaction ID: 0xef2a
  ▼ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▶ www.ietf.org: type A, class IN
```

8) Three answers were provided, containing the information in the answers below (the first contained a CNAME, the second and third containing A Records):

```
▼ Answers
  ▼ www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
      Name: www.ietf.org
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 1800
      Data length: 33
      CNAME: www.ietf.org.cdn.cloudflare.net
  ▼ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
      Name: www.ietf.org.cdn.cloudflare.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300
      Data length: 4
      Address: 104.20.1.85
  ▼ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
      Name: www.ietf.org.cdn.cloudflare.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300
      Data length: 4
      Address: 104.20.0.85
```

9) The destination IP address of the TCP SYN packet corresponds to the first A record provided by the DNS response (see below):

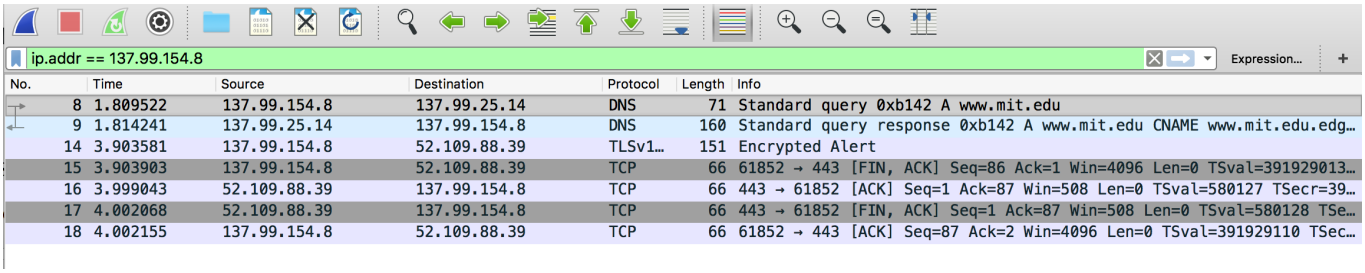


```
    8 3.075845    128.238.38.160  128.238.29.23   DNS      72 Standard query 0x006e A www.ietf.org
    9 3.076689    128.238.29.23   128.238.38.160  DNS     104 Standard query response 0x006e A www.ietf.org A 132.151.6.75 A
   10 3.078479    128.238.38.160  132.151.6.75    TCP      62 3369 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
   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_
   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
    Authority RRs: 0
    Additional RRs: 0
  ▶ Queries
  ▼ Answers
    ▼ www.ietf.org: type A, class IN, addr 132.151.6.75
        Name: www.ietf.org
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 1678
        Data length: 4
        Address: 132.151.6.75
```

10) There are no more DNS queries in the trace, hence my host must not be doing a new DNS query before retrieving each image.

11) The destination port of the DNS query and the source port of the DNS response were both 53.

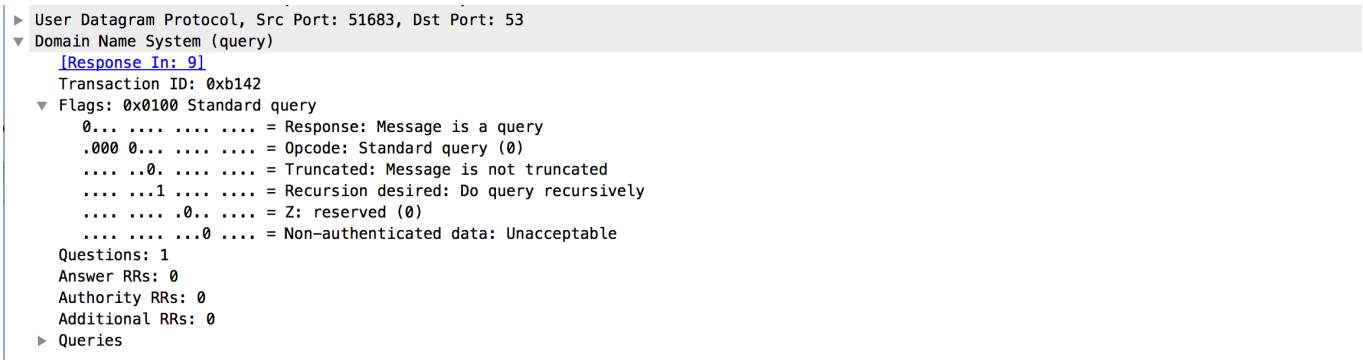
12) The DNS request was sent to 137.99.25.14, which appears to be the local UConn DNS server.



ip.addr == 137.99.154.8

No.	Time	Source	Destination	Protocol	Length	Info
8	1.809522	137.99.154.8	137.99.25.14	DNS	71	Standard query 0xb142 A www.mit.edu
9	1.814241	137.99.25.14	137.99.154.8	DNS	160	Standard query response 0xb142 A www.mit.edu CNAME www.mit.edu.edg…
14	3.903581	137.99.154.8	52.109.88.39	TLSv1…	151	Encrypted Alert
15	3.903903	137.99.154.8	52.109.88.39	TCP	66	61852 → 443 [FIN, ACK] Seq=86 Ack=1 Win=4096 Len=0 TSval=391929013…
16	3.999043	52.109.88.39	137.99.154.8	TCP	66	443 → 61852 [ACK] Seq=1 Ack=87 Win=508 Len=0 TSval=580127 TSecr=39…
17	4.002068	52.109.88.39	137.99.154.8	TCP	66	443 → 61852 [FIN, ACK] Seq=1 Ack=87 Win=508 Len=0 TSval=580128 TSe…
18	4.002155	137.99.154.8	52.109.88.39	TCP	66	61852 → 443 [ACK] Seq=87 Ack=2 Win=4096 Len=0 TSval=391929110 TSec…

13) The type of DNS message is a "A, class IN". It does not contain any answers.



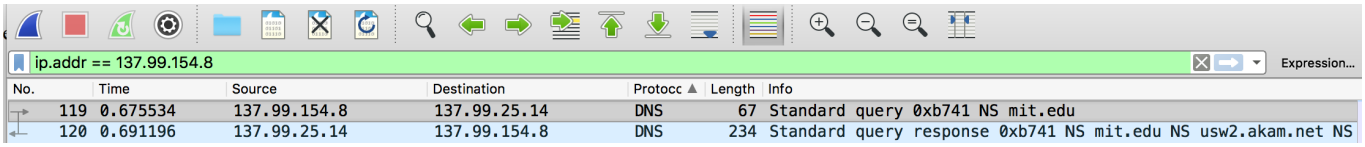
```
▶ User Datagram Protocol, Src Port: 51683, Dst Port: 53
▼ Domain Name System (query)
    [Response In: 9]
    Transaction ID: 0xb142
  ▼ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▶ Queries
```

14) Three answers were provided (see below), two CNAME records and one A record.

```
    9 1.814241      137.99.25.14          137.99.154.8          DNS       160 Standard query response 0xb142 A www.mit.edu CNAME www.mit.edu
   14 3.903581      137.99.154.8          52.109.88.39          TLSv1…    151 Encrypted Alert
   15 3.903903      137.99.154.8          52.109.88.39          TCP        66 61852 → 443 [FIN, ACK] Seq=86 Ack=1 Win=4096 Len=0 TSval=39191
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) (5)
      Class: IN (0x0001)
      Time to live: 1041
      Data length: 25
      CNAME: www.mit.edu.edgekey.net
  ▼ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
      Name: www.mit.edu.edgekey.net
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 26
      Data length: 24
      CNAME: e9566.dscb.akamaiedge.net
  ▼ e9566.dscb.akamaiedge.net: type A, class IN, addr 23.14.144.128
      Name: e9566.dscb.akamaiedge.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 6
      Data length: 4
      Address: 23.14.144.128
```

15) See response to questions 12 and 14 (above).

16) The DNS query message is sent to 137.99.25.14, the default local nameserver.



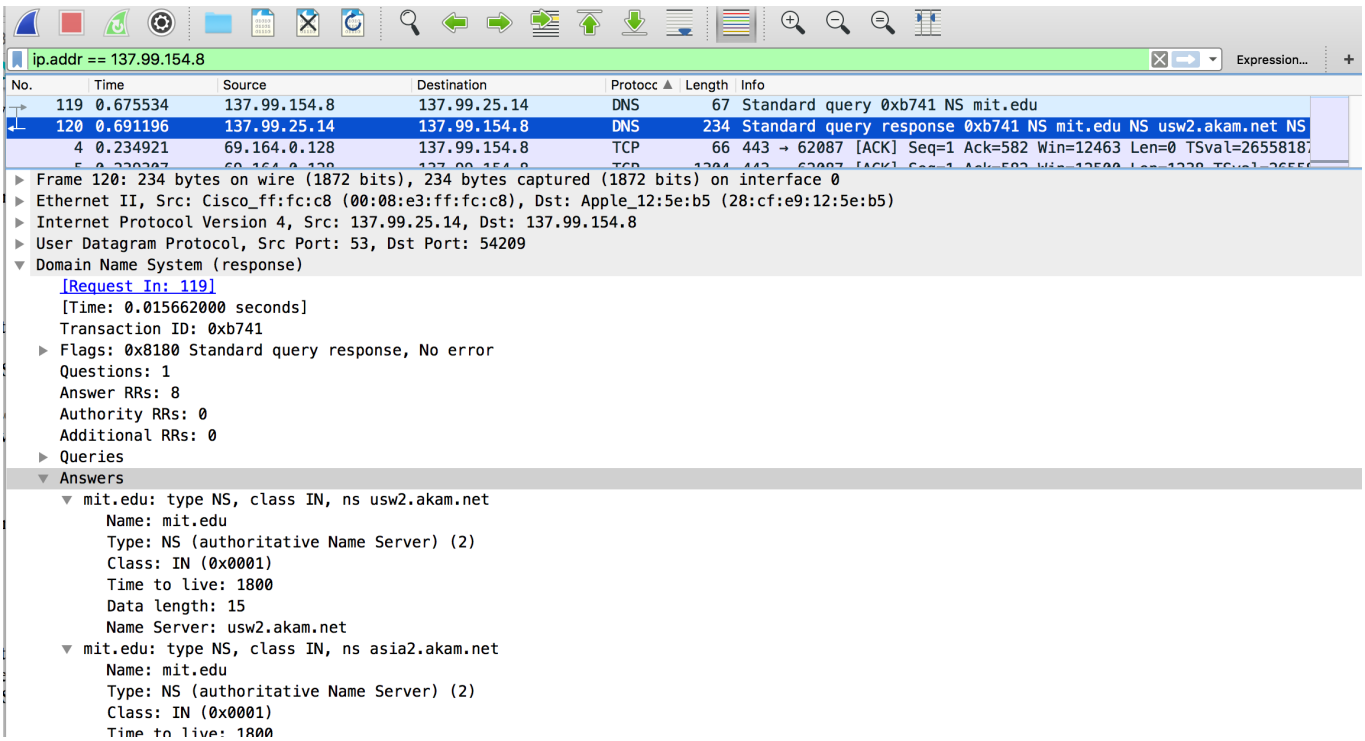
17) The type of DNS query is "A, class IN". It contains no answers:

```
▼ Domain Name System (query)
    [Response In: 120]
    Transaction ID: 0xb741
  ▶ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▶ Queries
```

18) The MIT nameservers provided by the response are detailed below. The IP addresses of these servers were not included.

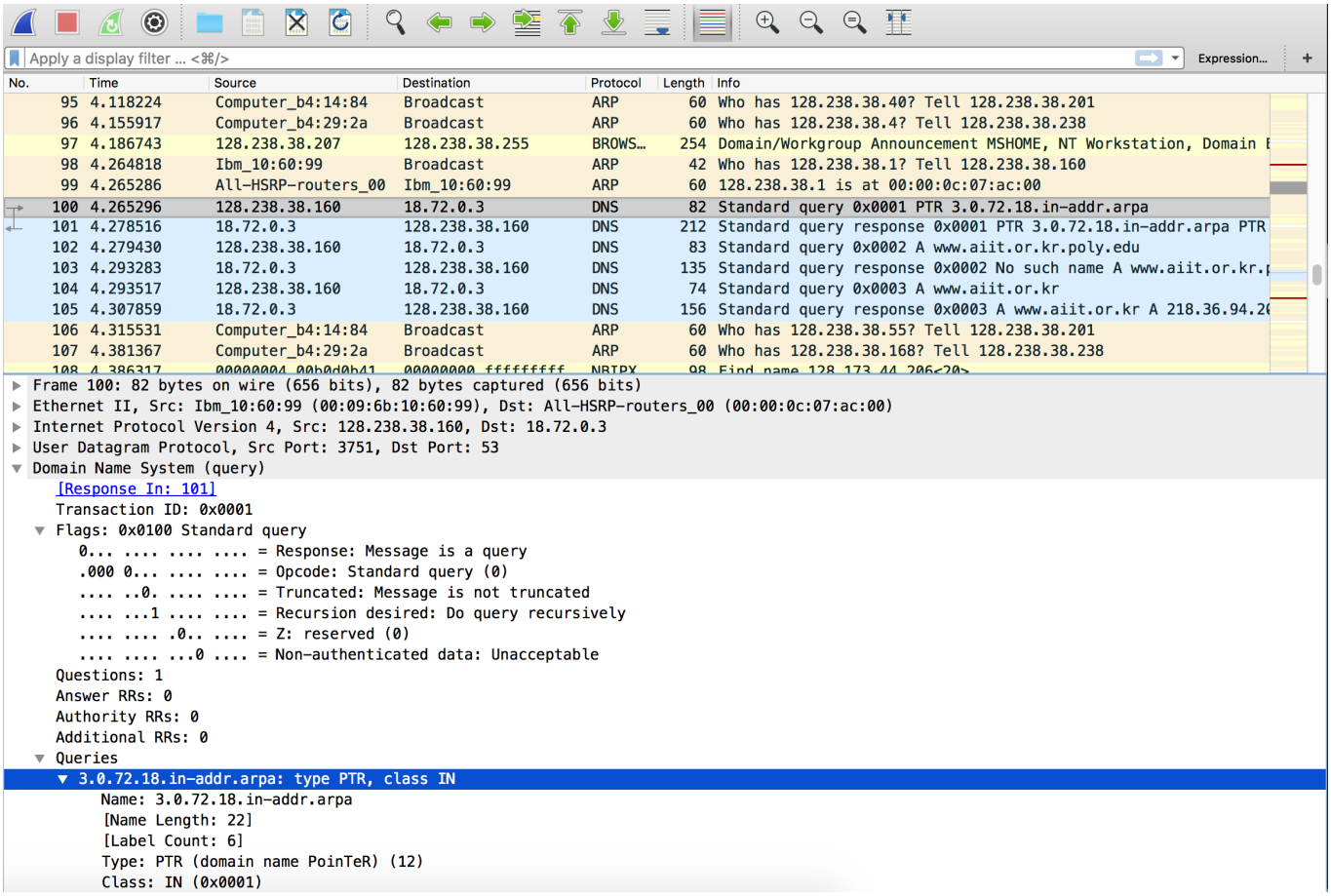
```
▼ Answers
  ▼ mit.edu: type NS, class IN, ns usw2.akam.net
      Name: mit.edu
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 1800
      Data length: 15
      Name Server: usw2.akam.net
  ▼ mit.edu: type NS, class IN, ns asia2.akam.net
      Name: mit.edu
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 1800
      Data length: 8
      Name Server: asia2.akam.net
  ▼ mit.edu: type NS, class IN, ns use5.akam.net
      Name: mit.edu
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 1800
      Data length: 7
      Name Server: use5.akam.net
  ▼ mit.edu: type NS, class IN, ns ns1-173.akam.net
      Name: mit.edu
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 1800
      Data length: 10
      Name Server: ns1-173.akam.net
  ▼ mit.edu: type NS, class IN, ns eur5.akam.net
      Name: mit.edu
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 1800
      Data length: 7
      Name Server: eur5.akam.net
  ▼ mit.edu: type NS, class IN, ns use2.akam.net
      Name: mit.edu
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 1800
      Data length: 7
      Name Server: use2.akam.net
  ▼ mit.edu: type NS, class IN, ns ns1-37.akam.net
      Name: mit.edu
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 1800
      Data length: 9
      Name Server: ns1-37.akam.net
  ▼ mit.edu: type NS, class IN, ns asia1.akam.net
      Name: mit.edu
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 1800
      Data length: 8
      Name Server: asia1.akam.net
```

19) See screenshot below.

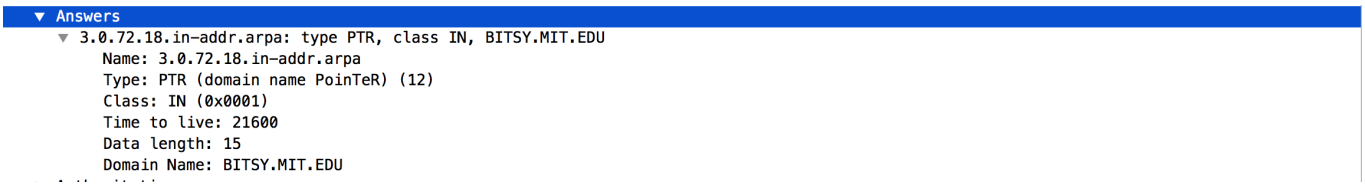


20) [Note: Had to use provided trace as the specified endpoint was down] The original DNS query is sent to 18.72.0.3, the default local DNS server.

21) The type of message is "PTR, class IN". It contains no answers.



22) There was one "Answer RR" provided, which contained the following:



The response also contained three authoritative nameservers and three additional records:

- Authoritative nameservers
  - 18.in-addr.arpa: type NS, class IN, ns W20NS.MIT.EDU
    - Name: 18.in-addr.arpa
    - Type: NS (authoritative Name Server) (2)
    - Class: IN (0x0001)
    - Time to live: 21600
    - Data length: 8
    - Name Server: W20NS.MIT.EDU
  - 18.in-addr.arpa: type NS, class IN, ns BITSY.MIT.EDU
    - Name: 18.in-addr.arpa
    - Type: NS (authoritative Name Server) (2)
    - Class: IN (0x0001)
    - Time to live: 21600
    - Data length: 2
    - Name Server: BITSY.MIT.EDU
  - 18.in-addr.arpa: type NS, class IN, ns STRAWB.MIT.EDU
    - Name: 18.in-addr.arpa
    - Type: NS (authoritative Name Server) (2)
    - Class: IN (0x0001)
    - Time to live: 21600
    - Data length: 9
    - Name Server: STRAWB.MIT.EDU
- Additional records
  - W20NS.MIT.EDU: type A, class IN, addr 18.70.0.160
    - Name: W20NS.MIT.EDU
    - Type: A (Host Address) (1)
    - Class: IN (0x0001)
    - Time to live: 21600
    - Data length: 4
    - Address: 18.70.0.160
  - BITSY.MIT.EDU: type A, class IN, addr 18.72.0.3
    - Name: BITSY.MIT.EDU
    - Type: A (Host Address) (1)
    - Class: IN (0x0001)
    - Time to live: 21600
    - Data length: 4
    - Address: 18.72.0.3
  - STRAWB.MIT.EDU: type A, class IN, addr 18.71.0.151