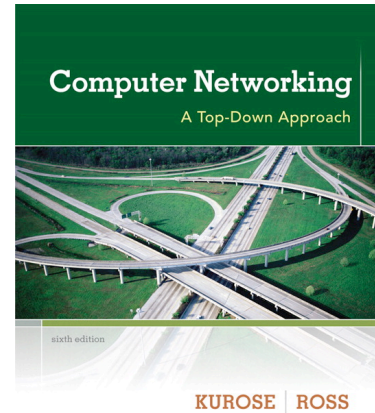# Wireshark Lab: Getting Started
SOLUTION

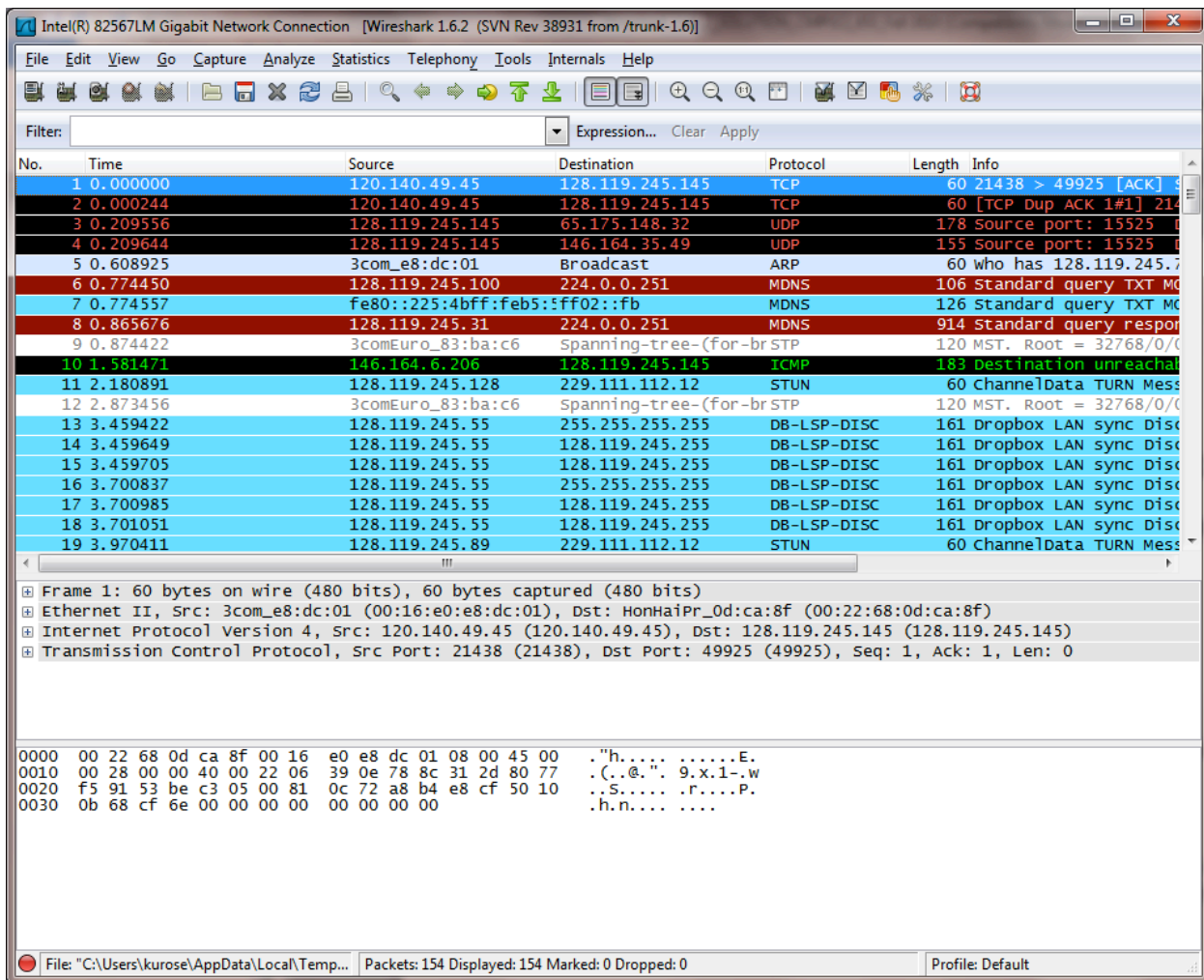Supplement to *Computer Networking: A Top-Down Approach, 6th ed.,* J.F. Kurose and K.W. Ross

Q1. List the 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

Answer: Some of the protocols listed in the screenshot below are UDP, TCP, ARP, ICMP, MDNS, and STUN. (Note you weren't asked to do a screenshot, but here is mine):

Intel(R) 82567LM Gigabit Network Connection   [Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)]

File   Edit   View   Go   Capture   Analyze   Statistics   Telephony   Tools   Internals   Help

Filter: [   ] ▼ Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	120.140.49.45	128.119.245.145	TCP	60	21438 > 49925 [ACK]
2	0.000244	120.140.49.45	128.119.245.145	TCP	60	[TCP Dup ACK 1#1] 214
3	0.209556	128.119.245.145	65.175.148.32	UDP	178	Source port: 15525
4	0.209644	128.119.245.145	146.164.35.49	UDP	155	Source port: 15525
5	0.608925	3com_e8:dc:01	Broadcast	ARP	60	who has 128.119.245.7
6	0.774450	128.119.245.100	224.0.0.251	MDNS	106	Standard query TXT MC
7	0.774557	fe80::225:4bff:feb5:5	ff02::fb	MDNS	126	Standard query TXT MC
8	0.865676	128.119.245.31	224.0.0.251	MDNS	914	Standard query respor
9	0.874422	3comEuro_83:ba:c6	Spanning-tree-(for-br	STP	120	MST. Root = 32768/0/(
10	1.581471	146.164.6.206	128.119.245.145	ICMP	183	Destination unreachal
11	2.180891	128.119.245.128	229.111.112.12	STUN	60	ChannelData TURN Mes!
12	2.873456	3comEuro_83:ba:c6	Spanning-tree-(for-br	STP	120	MST. Root = 32768/0/(
13	3.459422	128.119.245.55	255.255.255.255	DB-LSP-DISC	161	Dropbox LAN sync Disc
14	3.459649	128.119.245.55	128.119.245.255	DB-LSP-DISC	161	Dropbox LAN sync Disc
15	3.459705	128.119.245.55	128.119.245.255	DB-LSP-DISC	161	Dropbox LAN sync Disc
16	3.700837	128.119.245.55	255.255.255.255	DB-LSP-DISC	161	Dropbox LAN sync Disc
17	3.700985	128.119.245.55	128.119.245.255	DB-LSP-DISC	161	Dropbox LAN sync Disc
18	3.701051	128.119.245.55	128.119.245.255	DB-LSP-DISC	161	Dropbox LAN sync Disc
19	3.970411	128.119.245.89	229.111.112.12	STUN	60	ChannelData TURN Mes!

⊞ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
⊞ Ethernet II, Src: 3com_e8:dc:01 (00:16:e0:e8:dc:01), Dst: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f)
⊞ Internet Protocol Version 4, Src: 120.140.49.45 (120.140.49.45), Dst: 128.119.245.145 (128.119.245.145)
⊞ Transmission Control Protocol, Src Port: 21438 (21438), Dst Port: 49925 (49925), Seq: 1, Ack: 1, Len: 0

```
0000  00 22 68 0d ca 8f 00 16  e0 e8 dc 01 08 00 45 00   ."h.....  ......E.
0010  00 28 00 00 40 00 22 06  39 0e 78 8c 31 2d 80 77   .(..@.".  9.x.1-.w
0020  f5 91 53 be c3 05 00 81  0c 72 a8 b4 e8 cf 50 10   ..S.....  .r....P.
0030  0b 68 cf 6e 00 00 00 00  00 00 00 00               .h.n....  ....
```

⬤ File: "C:\Users\kurose\AppData\Local\Temp... | Packets: 154 Displayed: 154 Marked: 0 Dropped: 0 | Profile: Default

Q2. How long did it take from when the HTTP GET message was sent until the HTT OK reply was received? (By default, the value of the Time column in the packet listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)

Answer: As shown in the screen shot below (you didn't have to provide this), the GET was sent at 11.300694 and the reply was received at 11.301658. The delay was thus 0.000964 secs
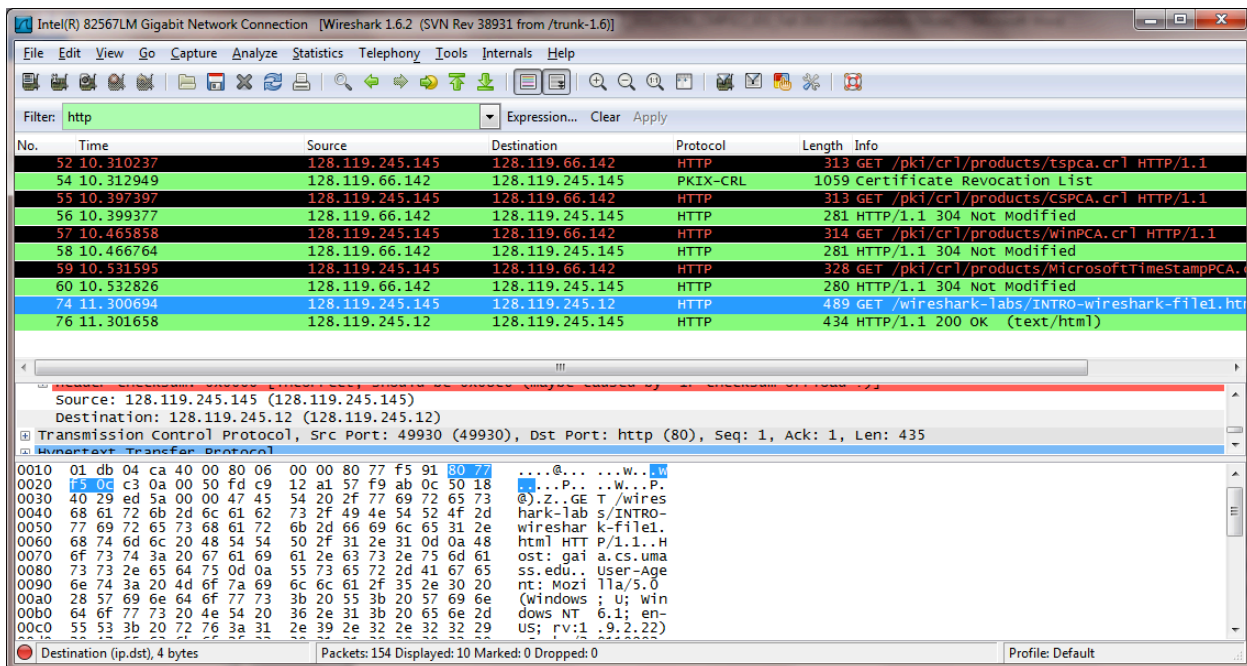
Q3. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.
cs.umass.edu)? What is the Internet address of your computer?

Answer: As shown in the screen shot below (you didn't have to provide this), the IP address of
gaia.cs.umass.edu is 128,119.245.145; the IP address of my laptop is 128.119.66.142

Q4. Print the HTTP GET and REPLY messages displayed in step 9 above. To do so, select Print
from the Wireshark File command menu, and select the"Selected Packet Only"
and "Print as displayed" radial buttons, and then click OK.
Answer: The print out of the two HTTP messages are below:

HTTP GET message:

```
No. Time Source Destination Protocol Length Info
74 11.300694 128.119.245.145 128.119.245.12 HTTP 489 GET /wireshark-labs/IN
Frame 74: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: DellComp_3b:8f:cd
(00:06:5b:3b:8f:cd)
Internet Protocol Version 4, Src: 128.119.245.145 (128.119.245.145), Dst:
128.119.245.12 (128.119.245.
Transmission Control Protocol, Src Port: 49930 (49930), Dst Port: http (80),
Seq: 1, Ack: 1, Len: 435
Hypertext Transfer Protocol
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.22)
Gecko/20110902 Firefox/3.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: en-us,en;q=0.5\r\n
Accept-Encoding: gzip,deflate\r\n
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
Keep-Alive: 115\r\n
```

Connection: keep-alive\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

HTTP REPLY message:

```
No. Time Source Destination Protocol Length Info
76 11.301658 128.119.245.12 128.119.245.145 HTTP 434 HTTP/1.1 200 OK (text
Frame 76: 434 bytes on wire (3472 bits), 434 bytes captured (3472 bits)
Ethernet II, Src: DellComp_3b:8f:cd (00:06:5b:3b:8f:cd), Dst: HonHaiPr_0d:ca:8f
(00:22:68:0d:ca:8f)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst:
128.119.245.145 (128.119.245.1
Transmission Control Protocol, Src Port: http (80), Dst Port: 49930 (49930),
Seq: 1, Ack: 436, Len: 38
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Mon, 26 Sep 2011 19:52:01 GMT\r\n
Server: Apache/2.2.3 (CentOS)\r\n
Last-Modified: Mon, 26 Sep 2011 19:51:01 GMT\r\n
ETag: "8734b-51-7a797340"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 81\r\n
Keep-Alive: timeout=10, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
Line-based text data: text/html
```

Wireshark Lab: DNS
SOLUTION

Supplement to *Computer Networking: A Top-Down Approach, 6th ed.,* J.F. Kurose and K.W. Ross
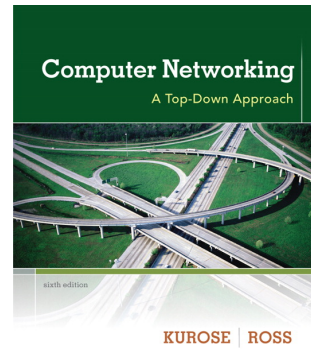
1. Run *nslookup* to obtain the IP address of a Web server in Asia. What is its IP address? ***ANSWER:*** *I performed nslookup for www.rediff.com. Its IP address is 208.184.138.70*

Screenshot taken for question 1

2. Run *nslookup* to determine the authoritative DNS servers for a university in Europe. What is its IP address. ***ANSWER****: I performed nslookup for a European University in Ioannina Greece. Its IP address is 128.238.29.22*

Screenshot taken for question 2

3. Run *nslookup* so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address? ***ANSWER:*** *the IP address of the mail server(s) is 18.72.0.3.*
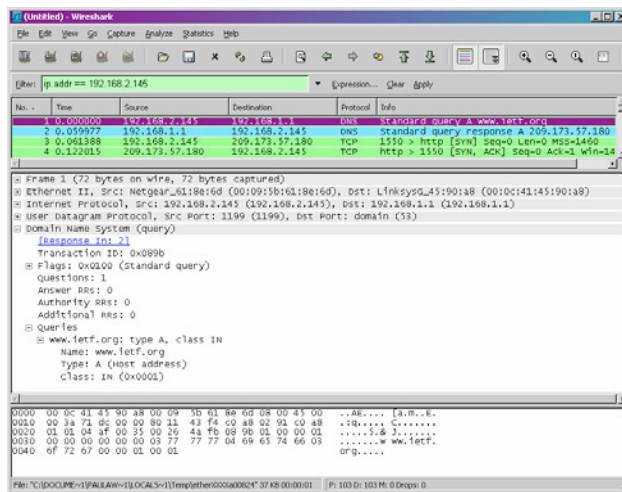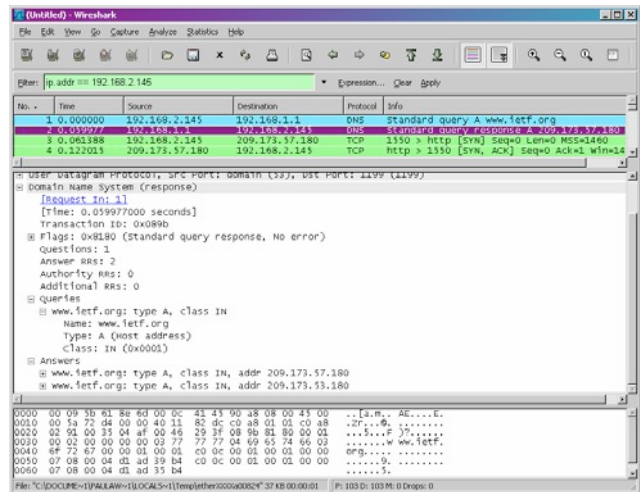
Screenshot taken for question 3

PART 3a

Screenshot for DNS query　　　　　　Screenshot for DNS response

4. Locate the DNS query and response messages. Are then sent over UDP or TCP? *ANSWER: They are sent over UDP*

5. What is the destination port for the DNS query message? What is the source port of DNS response message? *ANSWER: The destination port for the DNS query is 53 and the source port of the DNS response is 53.*
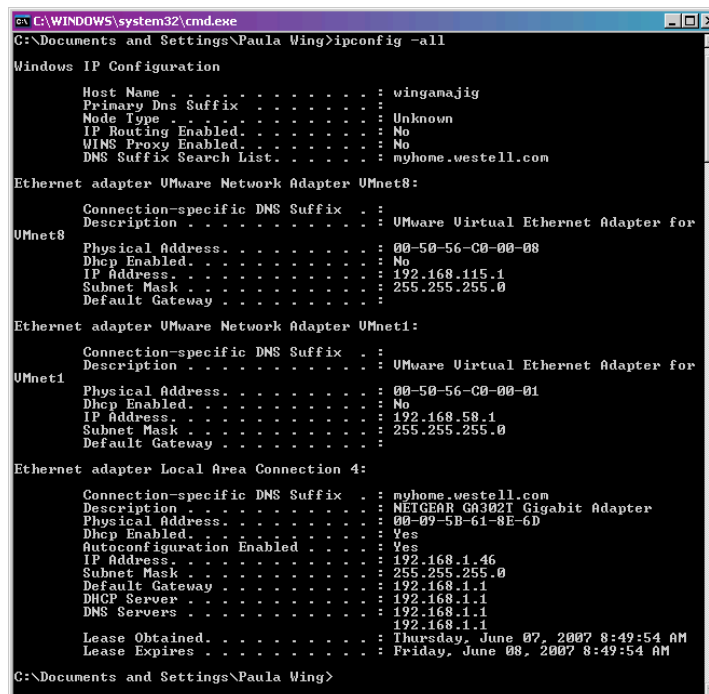
Screenshot for ipconfig –all

6. 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? *ANSWER: It's sent to 192.168.1.1, which is the IP address of one of my local DNS servers.*

7. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"? ***ANSWER:*** *It's a type A Standard Query and it doesn't contain any answers.*

8. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain? ***ANSWER:*** *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.*

```
Answers
www.ietf.org: type A, class IN, addr 209.173.57.180
   Name:
   www.ietf.org
   Type: A (Host
   address) Class:
   IN (0x0001)
   Time to live: 30 minutes
   Data length: 4
   Addr: 209.173.57.180
www.ietf.org: type A, class IN, addr 209.173.53.180
   Name:
   www.ietf.org
   Type: A (Host
   address) Class:
   IN (0x0001)
   Time to live: 30 minutes
   Data length: 4
   Addr: 209.173.53.180
```

9. 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? ***ANSWER:*** *The first SYN packet was sent to 209.173.57.180 which corresponds to the first IP address provided in the DNS response message.*
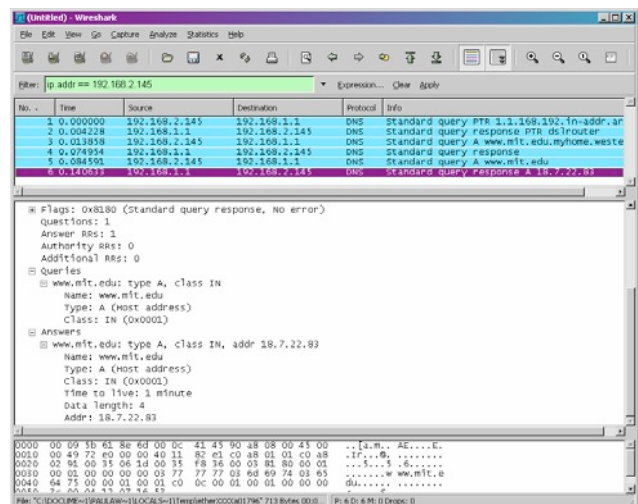
10. This web page contains images. Before retrieving each image, does your host issue new DNS queries? ***ANSWER:*** *No*

PART 3b
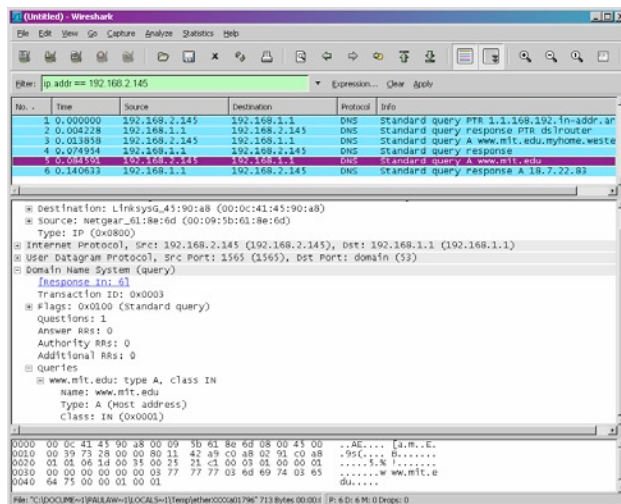
Screenshot for DNS query

Screenshot for DNS response

11. What is the destination port for the DNS query message? What is the source port of DNS response message? *ANSWER: The destination port of the DNS query is 53 and the source port of the DNS response is 53.*

12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? *ANSWER: It's sent to 192.168.1.1 which as we can see from the ipconfig –all screenshot, is the default local DNS server.*

13. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"? *ANSWER: The query is of type A and it doesn't contain any answers.*

14. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain? *ANSWER: The response DNS message contains one answer containing the name of the host, the type of address, the class, and the IP address.*

```
Answers
    www.mit.edu: type A, class IN, addr 18.7.22.83
        Name: www.mit.edu
        Type: A (Host
        address) Class:
        IN (0x0001)
        Time to live: 1 minute
        Data length: 4
        Addr: 18.7.22.83
```

15. Provide a screenshot.

PART 3c


```
dns-ethereal-trace-3 - Wireshark

File  Edit  View  Go  Capture  Analyze  Statistics  Help

Filter: ip.addr == 128.238.38.160              Expression...  Clear  Apply

No. ·   Time        Source           Destination      Protocol  Info
    488 30.916492   128.238.38.160   128.238.29.22    DNS       Standard query PTR 22.29.238.128.in-addr.
    489 30.916859   128.238.29.22    128.238.38.160   DNS       Standard query response PTR dns-prime.pol
    490 30.917700   128.238.38.160   128.238.29.22    DNS       Standard query NS mit.edu.poly.edu
    491 30.918044   128.238.29.22    128.238.38.160   DNS       Standard query response, No such name
    492 30.918275   128.238.38.160   128.238.29.22    DNS       Standard query NS mit.edu
    493 30.918636   128.238.29.22    128.238.38.160   DNS       Standard query response NS bitsy.mit.edu

       Authority RRs: 0
       Additional RRs: 3
     ⊟ Queries
       ⊟ mit.edu: type NS, class IN
            Name: mit.edu
            Type: NS (Authoritative name server)
            Class: IN (0x0001)
     ⊟ Answers
       ⊟ mit.edu: type NS, class IN, ns bitsy.mit.edu
            Name: mit.edu
            Type: NS (Authoritative name server)
            Class: IN (0x0001)
            Time to live: 5 hours, 45 minutes, 36 seconds
            Data length: 8
            Name server: bitsy.mit.edu
       ⊟ mit.edu: type NS, class IN, ns strawb.mit.edu
            Name: mit.edu
            Type: NS (Authoritative name server)
            Class: IN (0x0001)

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

File: "C:\Documents and Settings\Paula Wing\My Documents\Wireshark\traces - ethere...  P: 560 D: 6 M: 0
```

Screenshot for DNS response

16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? **ANSWER:** *It was sent to 128.238.29.22 which is my default DNS server.*

17. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"? **ANSWER:** *It's a type NS DNS query that doesn't contain any answers.*
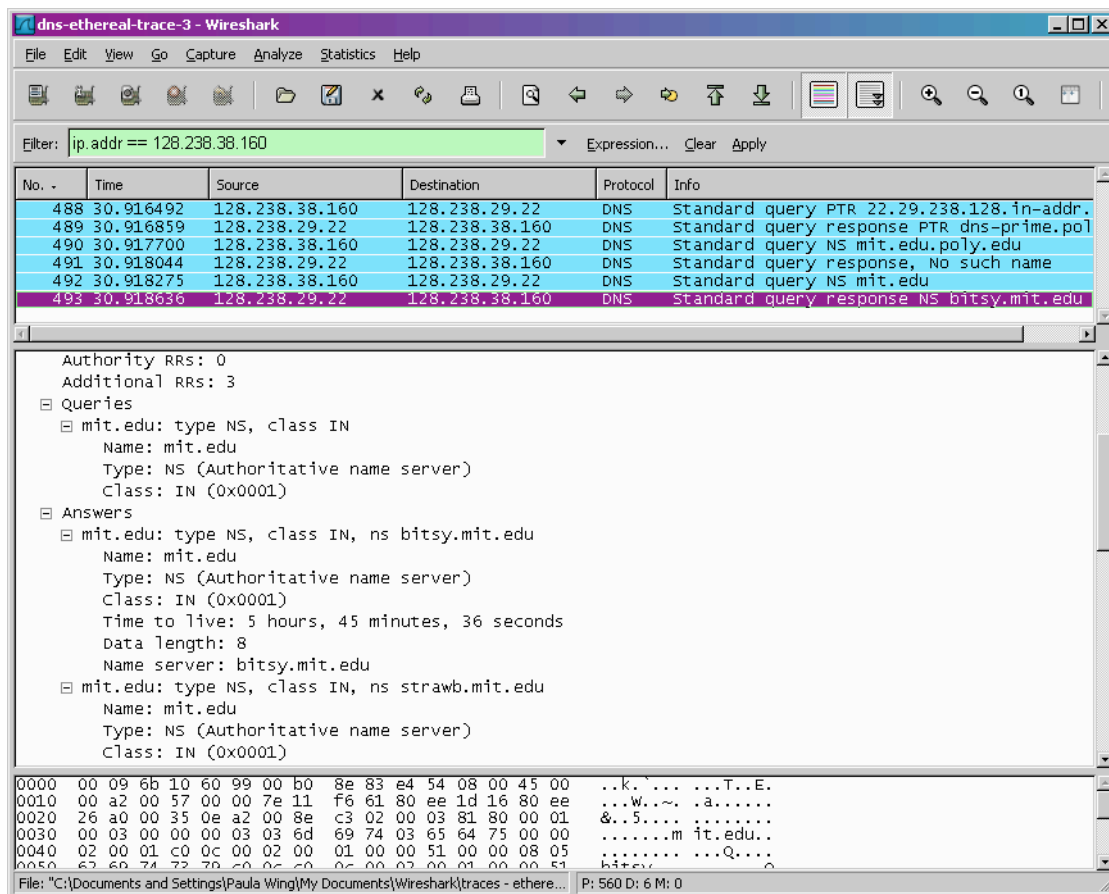
18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT nameservers? **ANSWER:** *The nameservers are bitsy, strawb and w20ns. We can find their IP addresses if we expand the Additional records field in Wireshark as seen below.*
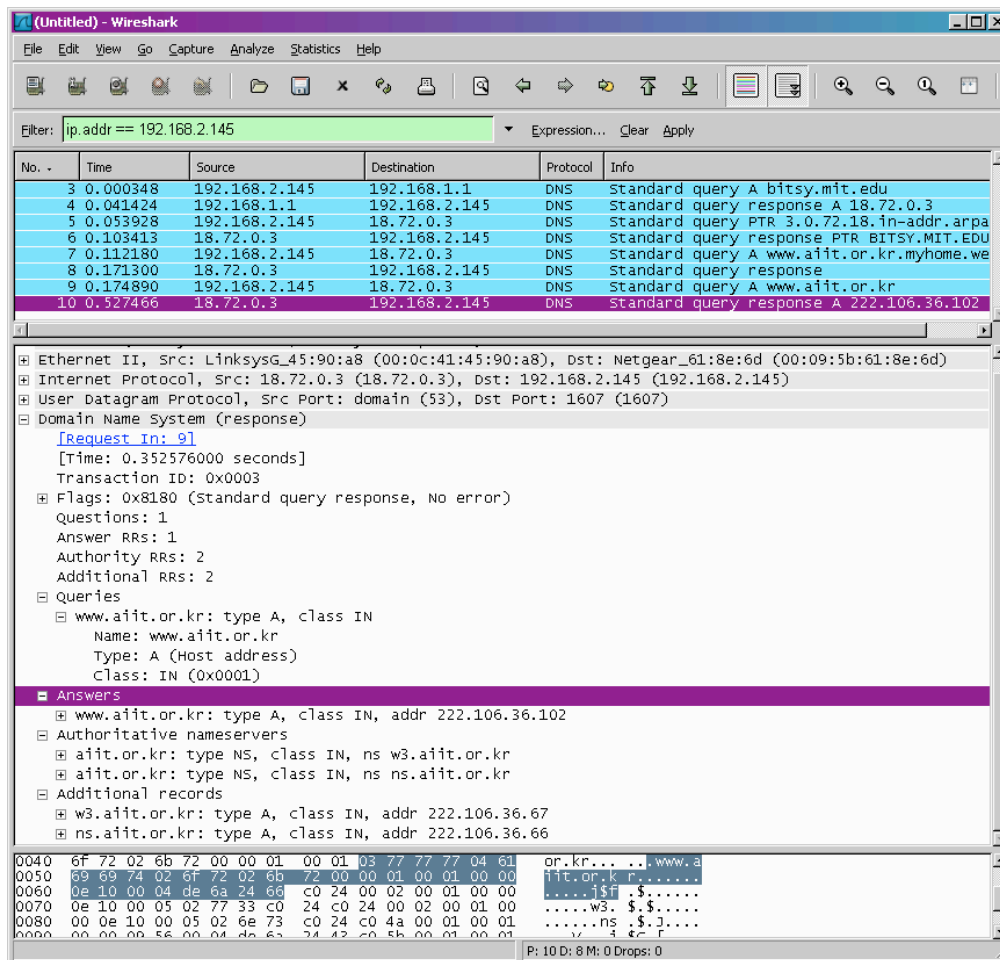
```
Answers
      mit.edu: type NS, class inet, ns bitsy.mit.edu
      mit.edu: type NS, class inet, ns strawb.mit.edu
      mit.edu: type NS, class inet, ns w20ns.mit.edu
   Additional records
      bitsy.mit.edu: type A, class inet, addr 18.72.0.3
      strawb.mit.edu: type A, class inet, addr 18.71.0.151
      w20ns.mit.edu: type A, class inet, addr 18.70.0.160
```

19. Provide a screenshot.

PART 3d

Screenshot for DNS response

20. 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? *ANSWER: The query is sent to 18.72.0.3 which corresponds to bitsy.mit.edu.*

21. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"? *ANSWER It's a standard type A query that doesn't contain any answers.*

22. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain? *ANSWER: One answer is provided in the DNS response message. It contains the following:*

```
Answers
      www.aiit.or.kr: type A, class inet, addr 222.106.36.102
         Name: www.aiit.or.kr
         Type: Host address
         Class: inet
         Time to live: 1 hour
         Data length: 4
         Addr: 222.106.36.102
```

23. Provide a screenshot.