Διαχείριση Δικτύων Βασισμένων στο Λογισμικό

2^{o} εργαστήριο: “HTTP-DNS”

HTTP lab

Q1-Q6: Please add one screenshot marking the answers to all questions below (e.g. circle the answers in the screenshot).

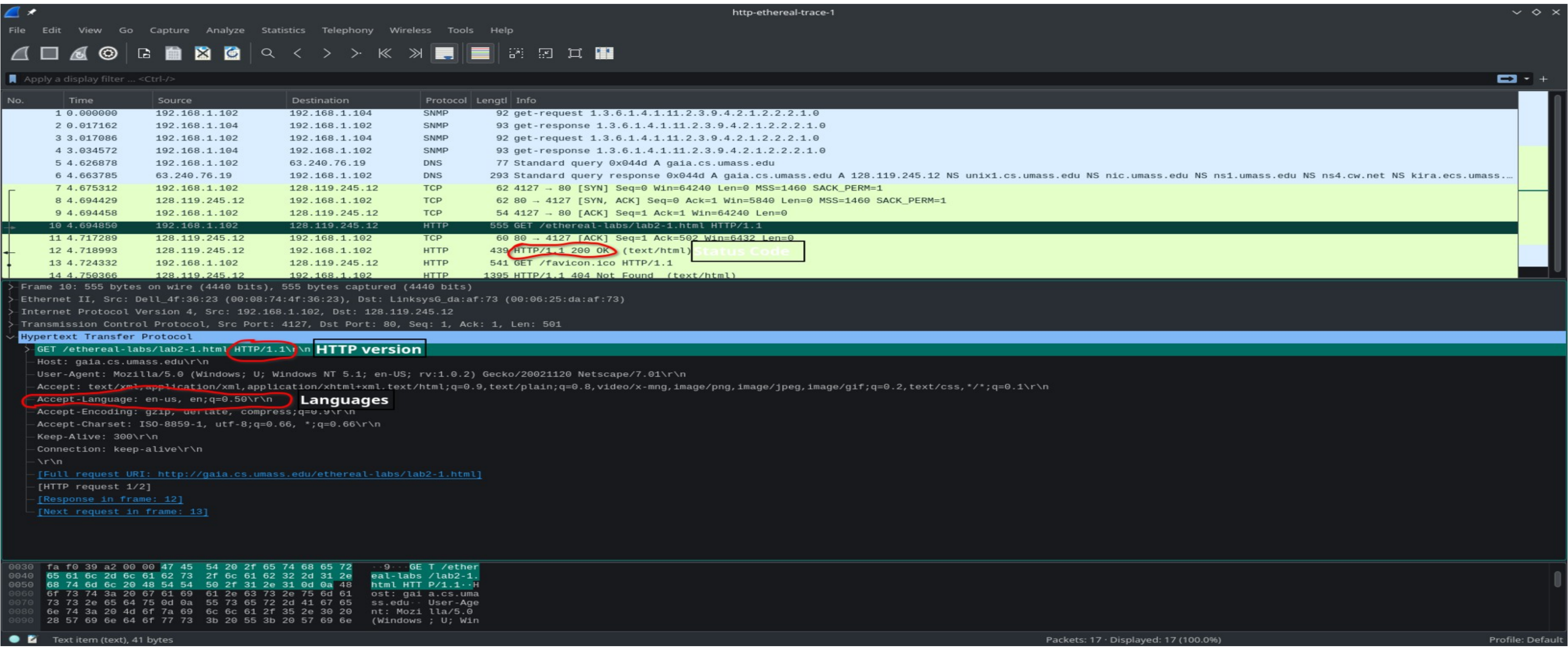
- Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
  Browser HTTP version 1.1. Server HTTP version 1.1

- What languages (if any) does your browser indicate that it can accept to the server?
  En-us, en

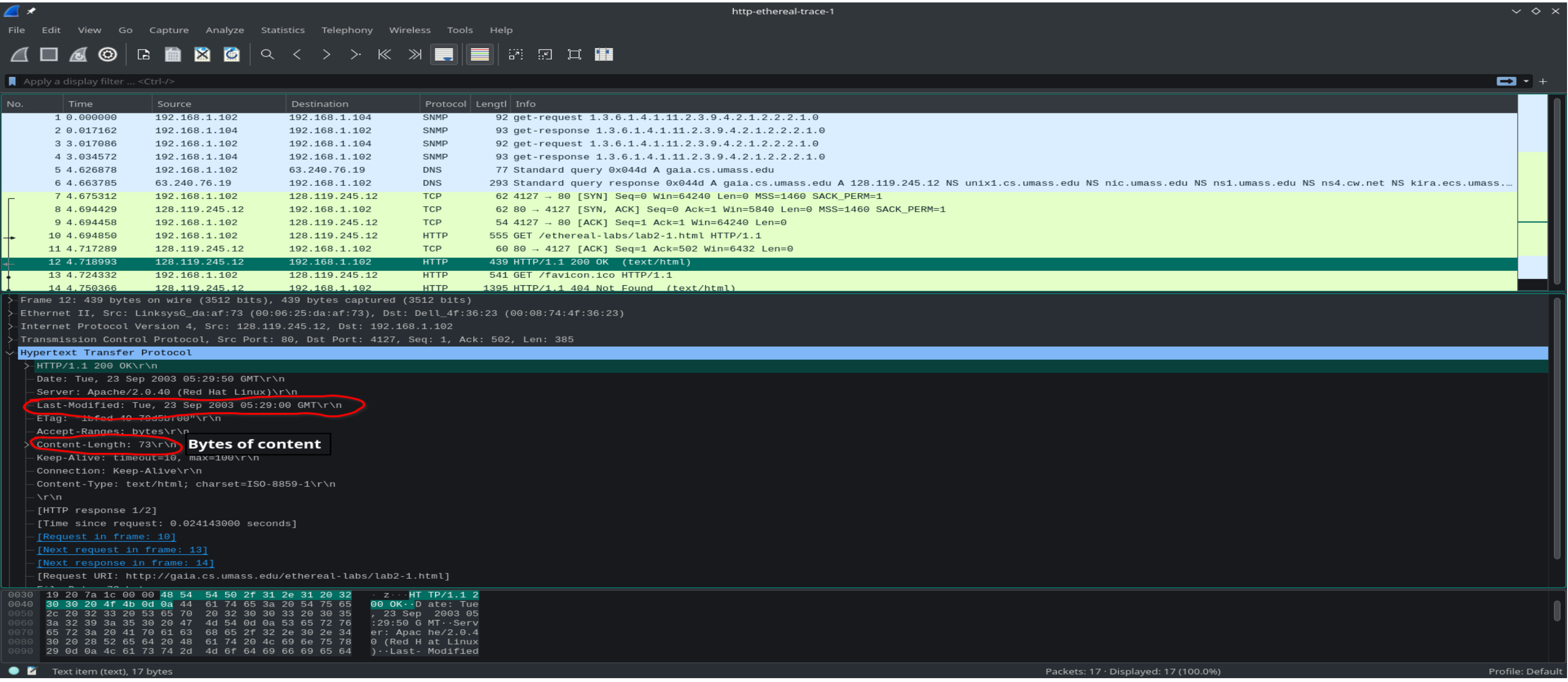
- What is the status code returned from the server to your browser?
  200 OK

- When was the HTML file that you are retrieving last modified at the server? Tuesday 23 September 2003 05:29:00 GMT

- How many bytes of content are being returned to your browser?
  73 bytes



```
No.  Time      Source          Destination     Protocol Lengtl Info
   1 0.000000  192.168.1.102   192.168.1.104   SNMP       92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
   2 0.017162  192.168.1.104   192.168.1.102   SNMP       93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
   3 3.017086  192.168.1.102   192.168.1.104   SNMP       92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
   4 3.034572  192.168.1.104   192.168.1.102   SNMP       93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
   5 4.626878  192.168.1.102   63.240.76.19    DNS        77 Standard query 0x044d A gaia.cs.umass.edu
   6 4.663785  63.240.76.19    192.168.1.102   DNS       293 Standard query response 0x044d A gaia.cs.umass.edu A 128.119.245.12 NS unix1.cs.umass.edu NS nic.umass.edu NS ns1.umass.edu NS ns4.cw.net NS kira.ecs.umass.…
   7 4.675312  192.168.1.102   128.119.245.12  TCP        62 4127 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
   8 4.694429  128.119.245.12  192.168.1.102   TCP        62 80 → 4127 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
   9 4.694458  192.168.1.102   128.119.245.12  TCP        54 4127 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
  10 4.694850  192.168.1.102   128.119.245.12  HTTP      555 GET /ethereal-labs/lab2-1.html HTTP/1.1
  11 4.717289  128.119.245.12  192.168.1.102   TCP        60 80 → 4127 [ACK] Seq=1 Ack=502 Win=6432 Len=0
  12 4.718993  128.119.245.12  192.168.1.102   HTTP      439 HTTP/1.1 200 OK  (text/html)
  13 4.724332  192.168.1.102   128.119.245.12  HTTP      541 GET /favicon.ico HTTP/1.1
  14 4.750366  128.119.245.12  192.168.1.102   HTTP     1395 HTTP/1.1 404 Not Found  (text/html)

> Frame 10: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 4127, Dst Port: 80, Seq: 1, Ack: 1, Len: 501
v Hypertext Transfer Protocol
  > GET /ethereal-labs/lab2-1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01\r\n
    Accept: text/xml,application/xml,application/xhtml+xml.text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1\r\n
    Accept-Language: en-us, en;q=0.50\r\n
    Accept-Encoding: gzip, deflate, compress;q=0.9\r\n
    Accept-Charset: ISO-8859-1, utf-8;q=0.66, *;q=0.66\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/ethereal-labs/lab2-1.html]
    [HTTP request 1/2]
    [Response in frame: 12]
    [Next request in frame: 13]

0030  fa f0 39 a2 00 00 47 45  54 20 2f 65 74 68 65 72   ··9···GE T /ether
0040  65 61 6c 2d 6c 61 62 73  2f 6c 61 62 32 2d 31 2e   eal-labs /lab2-1.
0050  68 74 6d 6c 20 48 54 54  50 2f 31 2e 31 0d 0a 48   html HTT P/1.1··H
0060  6f 73 74 3a 20 67 61 69  61 2e 63 73 2e 75 6d 61   ost: gai a.cs.uma
0070  73 73 2e 65 64 75 0d 0a  55 73 65 72 2d 41 67 65   ss.edu·· User-Age
0080  6e 74 3a 20 4d 6f 7a 69  6c 6c 61 2f 35 2e 30 20   nt: Mozi lla/5.0 
0090  28 57 69 6e 64 6f 77 73  3b 20 55 3b 20 57 69 6e   (Windows ; U; Win
```


http-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time        Source          Destination     Protocol Lengtl Info
   1 0.000000    192.168.1.102   192.168.1.104   SNMP       92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
   2 0.017162    192.168.1.104   192.168.1.102   SNMP       93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
   3 3.017086    192.168.1.102   192.168.1.104   SNMP       92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
   4 3.034572    192.168.1.104   192.168.1.102   SNMP       93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
   5 4.626878    192.168.1.102   63.240.76.19    DNS        77 Standard query 0x044d A gaia.cs.umass.edu
   6 4.663785    63.240.76.19    192.168.1.102   DNS       293 Standard query response 0x044d A gaia.cs.umass.edu A 128.119.245.12 NS unix1.cs.umass.edu NS nic.umass.edu NS ns1.umass.edu NS ns4.cw.net NS kira.ecs.umass.…
   7 4.675312    192.168.1.102   128.119.245.12  TCP        62 4127 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
   8 4.694429    128.119.245.12  192.168.1.102   TCP        62 80 → 4127 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
   9 4.694458    192.168.1.102   128.119.245.12  TCP        54 4127 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
  10 4.694850    192.168.1.102   128.119.245.12  HTTP      555 GET /ethereal-labs/lab2-1.html HTTP/1.1
  11 4.717289    128.119.245.12  192.168.1.102   TCP        60 80 → 4127 [ACK] Seq=1 Ack=502 Win=6432 Len=0
  12 4.718993    128.119.245.12  192.168.1.102   HTTP      439 HTTP/1.1 200 OK  (text/html)
  13 4.724332    192.168.1.102   128.119.245.12  HTTP      541 GET /favicon.ico HTTP/1.1
  14 4.750366    128.119.245.12  192.168.1.102   HTTP     1395 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 12: 439 bytes on wire (3512 bits), 439 bytes captured (3512 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
> Transmission Control Protocol, Src Port: 80, Dst Port: 4127, Seq: 1, Ack: 502, Len: 385
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Tue, 23 Sep 2003 05:29:50 GMT\r\n
    Server: Apache/2.0.40 (Red Hat Linux)\r\n
    Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT\r\n
    ETag: "1bfed-49-79d5bf00"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 73\r\n
    Keep-Alive: timeout=10, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=ISO-8859-1\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.024143000 seconds]
    [Request in frame: 10]
    [Next request in frame: 13]
    [Next response in frame: 14]
    [Request URI: http://gaia.cs.umass.edu/ethereal-labs/lab2-1.html]
```

Bytes of content

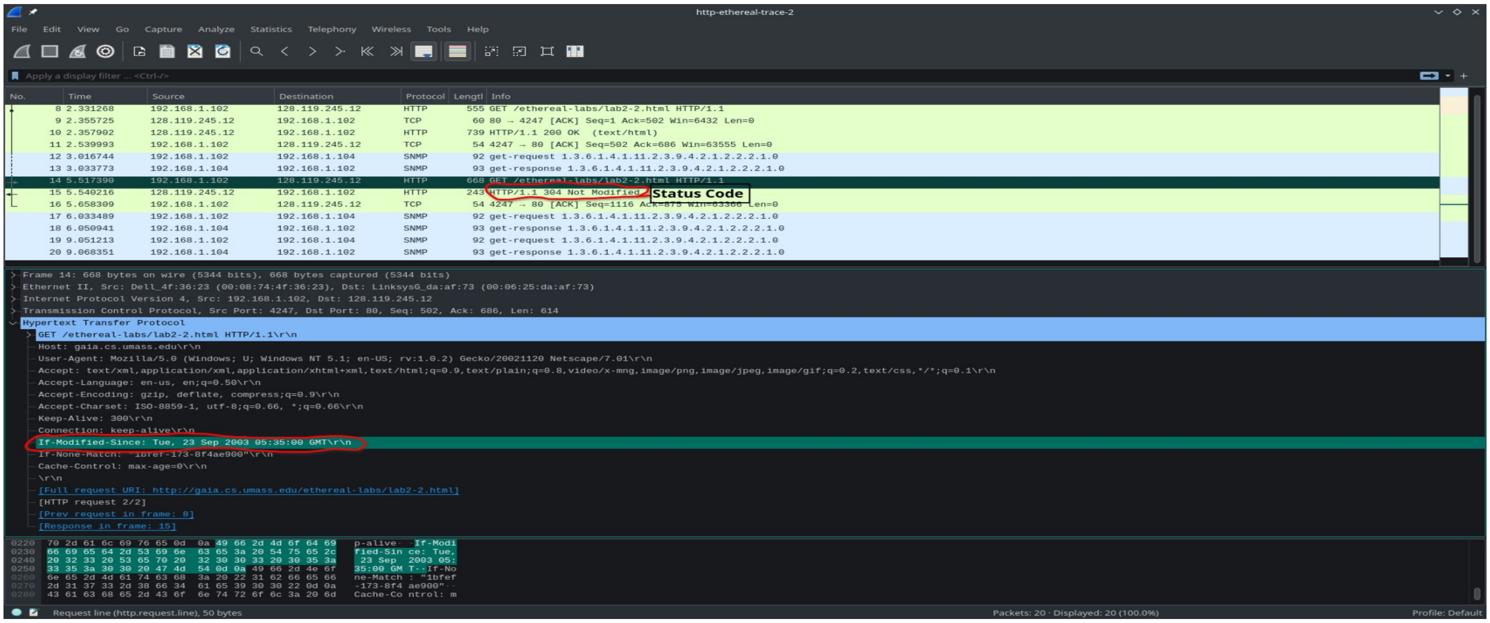
```
0030  19 20 7a 1c 00 00 48 54  54 50 2f 31 2e 31 20 32   · z···HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 54 75 65   00 OK··D ate: Tue
0050  2c 20 32 33 20 53 65 70  20 32 30 30 33 20 30 35   , 23 Sep  2003 05
0060  3a 32 39 3a 35 30 20 47  4d 54 0d 0a 53 65 72 76   :29:50 G MT··Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 30 2e 34   er: Apac he/2.0.4
0080  30 20 28 52 65 64 20 48  61 74 20 4c 69 6e 75 78   0 (Red H at Linux
0090  29 0d 0a 4c 61 73 74 2d  4d 6f 64 69 66 69 65 64   )··Last- Modified
```

Text item (text), 17 bytes
Packets: 17 · Displayed: 17 (100.0%)
Profile: Default

Q9-Q10: Please add a screenshot to justify answers to questions below:

- Inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IF-MODIFIED-SINCE:" header?
  If-Modified-Since: Tue, 23 Sep 2003 05:35:00 GMT

- What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.
  304 Not Modified. So the text of the file is NOT returned in the HTTP message.


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

```
No.  Time        Source          Destination     Protocol Lengtl Info
   8 2.331268    192.168.1.102   128.119.245.12  HTTP      555 GET /ethereal-labs/lab2-2.html HTTP/1.1
   9 2.355725    128.119.245.12  192.168.1.102   TCP        60 80 → 4247 [ACK] Seq=1 Ack=502 Win=6432 Len=0
  10 2.357902    128.119.245.12  192.168.1.102   HTTP      739 HTTP/1.1 200 OK  (text/html)
  11 2.539993    192.168.1.102   128.119.245.12  TCP        54 4247 → 80 [ACK] Seq=502 Ack=686 Win=63555 Len=0
  12 3.016744    192.168.1.102   192.168.1.104   SNMP       92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
  13 3.033773    192.168.1.104   192.168.1.102   SNMP       93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
  14 5.517390    192.168.1.102   128.119.245.12  HTTP      668 GET /ethereal-labs/lab2-2.html HTTP/1.1
  15 5.540216    128.119.245.12  192.168.1.102   HTTP      243 HTTP/1.1 304 Not Modified
  16 5.658309    192.168.1.102   128.119.245.12  TCP        54 4247 → 80 [ACK] Seq=1116 Ack=875 Win=63366 Len=0
  17 6.033489    192.168.1.102   192.168.1.104   SNMP       92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
  18 6.050941    192.168.1.104   192.168.1.102   SNMP       93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
  19 9.051213    192.168.1.102   192.168.1.104   SNMP       92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
  20 9.068351    192.168.1.104   192.168.1.102   SNMP       93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
```

Status Code

```
> Frame 14: 668 bytes on wire (5344 bits), 668 bytes captured (5344 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 4247, Dst Port: 80, Seq: 502, Ack: 686, Len: 614
v Hypertext Transfer Protocol
  > GET /ethereal-labs/lab2-2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01\r\n
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1\r\n
    Accept-Language: en-us, en;q=0.50\r\n
    Accept-Encoding: gzip, deflate, compress;q=0.9\r\n
    Accept-Charset: ISO-8859-1, utf-8;q=0.66, *;q=0.66\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    If-Modified-Since: Tue, 23 Sep 2003 05:35:00 GMT\r\n
    If-None-Match: "1bfef-173-8f4ae900"\r\n
    Cache-Control: max-age=0\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/ethereal-labs/lab2-2.html]
    [HTTP request 2/2]
    [Prev request in frame: 8]
    [Response in frame: 15]
```

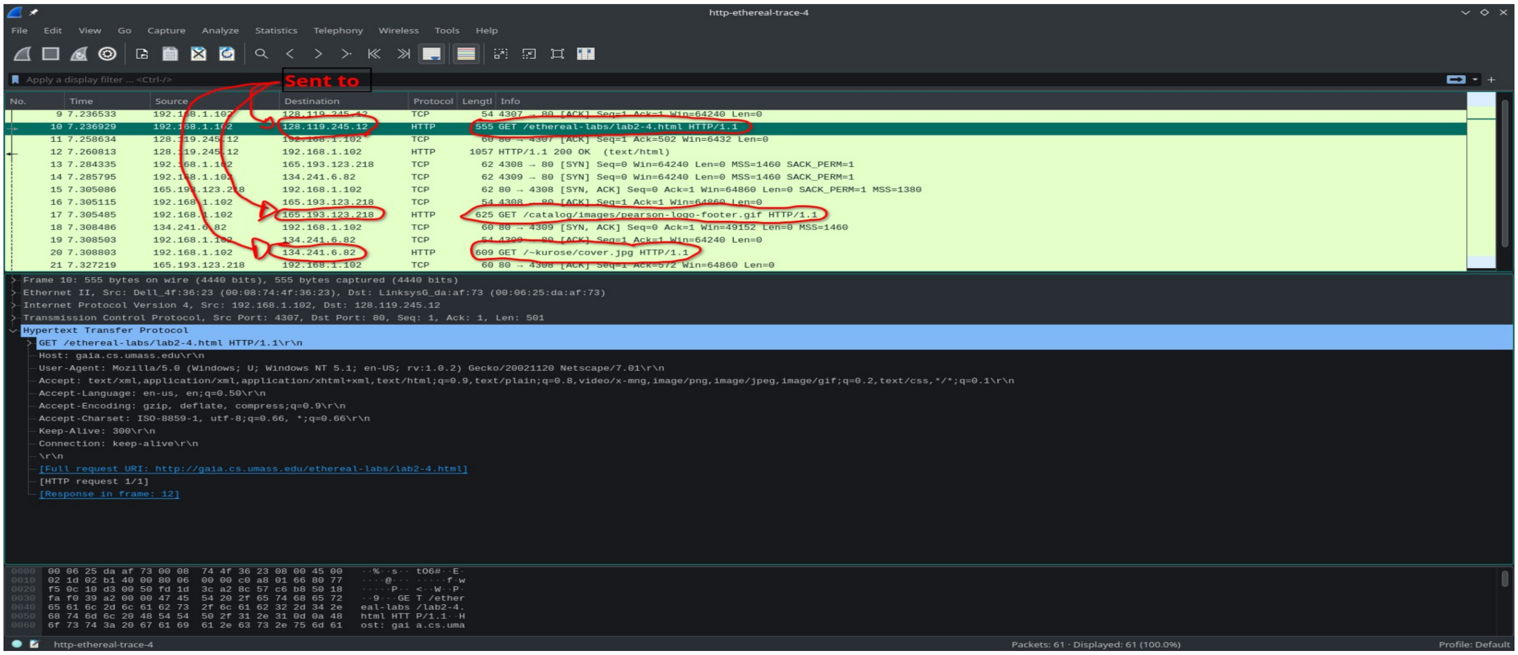
```
0220  70 2d 61 6c 69 76 65 0d  0a 49 66 2d 4d 6f 64 69   p-alive· ·If-Modi
0230  66 69 65 64 2d 53 69 6e  63 65 3a 20 54 75 65 2c   fied-Sin ce: Tue,
0240  20 32 33 20 53 65 70 20  32 30 30 33 20 30 35 3a    23 Sep  2003 05:
0250  33 35 3a 30 30 20 47 4d  54 0d 0a 49 66 2d 4e 6f   35:00 GM T··If-No
0260  6e 65 2d 4d 61 74 63 68  3a 20 22 31 62 66 65 66   ne-Match : "1bfef
0270  2d 31 37 33 2d 38 66 34  61 65 39 30 30 22 0d 0a   -173-8f4 ae900"··
0280  43 61 63 68 65 2d 43 6f  6e 74 72 6f 6c 3a 20 6d   Cache-Co ntrol: m
```

Request line (http.request.line), 50 bytes
Packets: 20 · Displayed: 20 (100.0%)
Profile: Default

Q15-Q16: Please briefly respond the questions:

- How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?
  It sent 3 HTTP GET. Each of these three GET messages were sent to different IP addresses. Packet line 10 sent to: 128.119.245.12, Packet line 17 sent to:165.193.123.218, Packet line 20 sent to: 134.241.6.82

- Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.
  They were downloaded in parallel. The two images are in packets line 17 and 20.



```
No.  Time       Source            Destination       Protocol Lengtl Info
   9 7.236533   192.168.1.102     128.119.245.12    TCP        54 4307 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
  10 7.236929   192.168.1.102     128.119.245.12    HTTP      555 GET /ethereal-labs/lab2-4.html HTTP/1.1
  11 7.258634   128.119.245.12    192.168.1.102     TCP        60 80 → 4307 [ACK] Seq=1 Ack=502 Win=6432 Len=0
  12 7.260813   128.119.245.12    192.168.1.102     HTTP     1057 HTTP/1.1 200 OK  (text/html)
  13 7.284335   192.168.1.102     165.193.123.218   TCP        62 4308 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
  14 7.285795   192.168.1.102     134.241.6.82      TCP        62 4309 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
  15 7.305086   165.193.123.218   192.168.1.102     TCP        62 80 → 4308 [SYN, ACK] Seq=0 Ack=1 Win=64860 Len=0 SACK_PERM=1 MSS=1380
  16 7.305115   192.168.1.102     165.193.123.218   TCP        54 4308 → 80 [ACK] Seq=1 Ack=1 Win=64860 Len=0
  17 7.305485   192.168.1.102     165.193.123.218   HTTP      625 GET /catalog/images/pearson-logo-footer.gif HTTP/1.1
  18 7.308486   134.241.6.82      192.168.1.102     TCP        60 80 → 4309 [SYN, ACK] Seq=0 Ack=1 Win=49152 Len=0 MSS=1460
  19 7.308503   192.168.1.102     134.241.6.82      TCP        54 4309 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
  20 7.308803   192.168.1.102     134.241.6.82      HTTP      609 GET /~kurose/cover.jpg HTTP/1.1
  21 7.327219   165.193.123.218   192.168.1.102     TCP        60 80 → 4308 [ACK] Seq=1 Ack=572 Win=64860 Len=0
```

```
> Frame 10: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 4307, Dst Port: 80, Seq: 1, Ack: 1, Len: 501
v Hypertext Transfer Protocol
  > GET /ethereal-labs/lab2-4.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01\r\n
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1\r\n
    Accept-Language: en-us, en;q=0.50\r\n
    Accept-Encoding: gzip, deflate, compress;q=0.9\r\n
    Accept-Charset: ISO-8859-1, utf-8;q=0.66, *;q=0.66\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/ethereal-labs/lab2-4.html]
    [HTTP request 1/1]
    [Response in frame: 12]
```

```
0000  00 06 25 da af 73 00 08  74 4f 36 23 08 00 45 00   ··%··s·· tO6#··E·
0010  02 1d 02 b1 40 00 80 06  00 00 c0 a8 01 66 80 77   ····@··· ·····f·w
0020  f5 0c 10 d3 00 50 fd 1d  3c a2 8c 57 c6 b8 50 18   ·····P·· <··W··P·
0030  fa f0 39 a2 00 00 47 45  54 20 2f 65 74 68 65 72   ··9···GE T /ether
0040  65 61 6c 2d 6c 61 62 73  2f 6c 61 62 32 2d 34 2e   eal-labs /lab2-4.
0050  68 74 6d 6c 20 48 54 54  50 2f 31 2e 31 0d 0a 48   html HTT P/1.1··H
0060  6f 73 74 3a 20 67 61 69  61 2e 63 73 2e 75 6d 61   ost: gai a.cs.uma
```

DNS lab

Q4-Q9: Please respond to the following questions and add respective screenshot(s):

- Locate the DNS query and response messages. Are they sent over UDP or TCP?
  UDP

- What is the destination port for the DNS query message? What is the source port of DNS response message?
  Destination post is 53
  Source port is 53

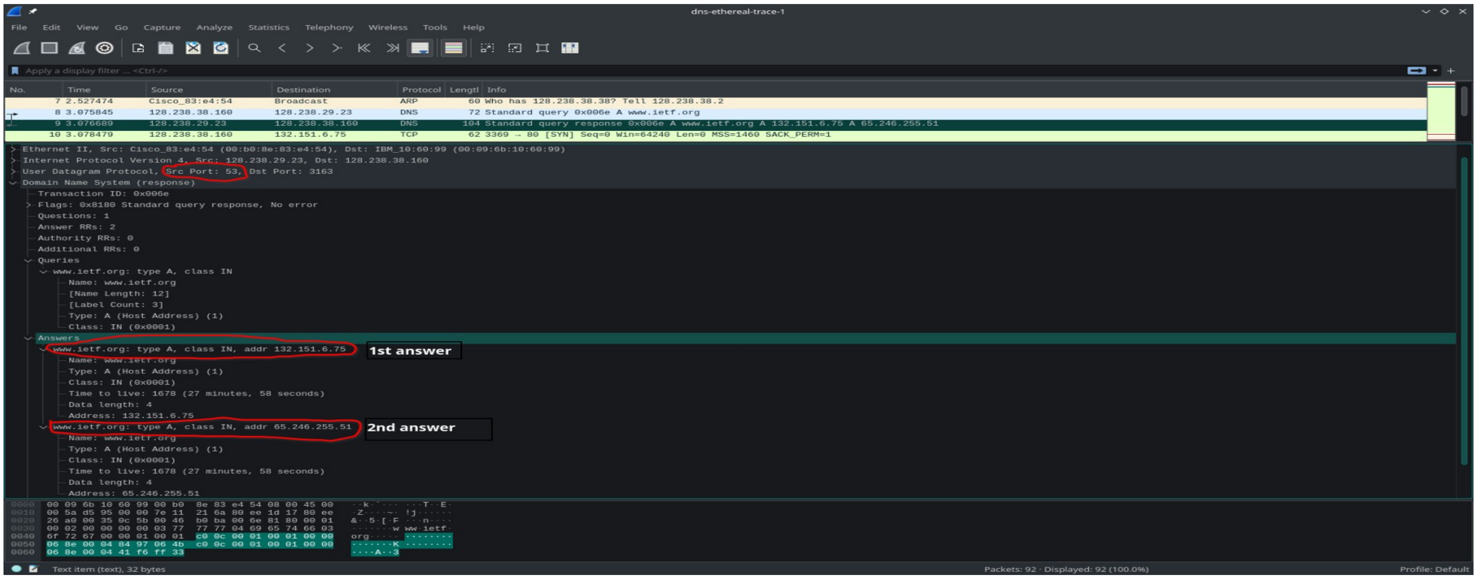
- To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?
  128.238.29.23

- Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
  Type A. It doesn’t contain any answers.

- Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?
  2 answers provided. They each contain name of host, type of address, class, the TTL, data length and the IP address.

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

- This web page contains images. Before retrieving each image, does your host issue new DNS queries?
  No



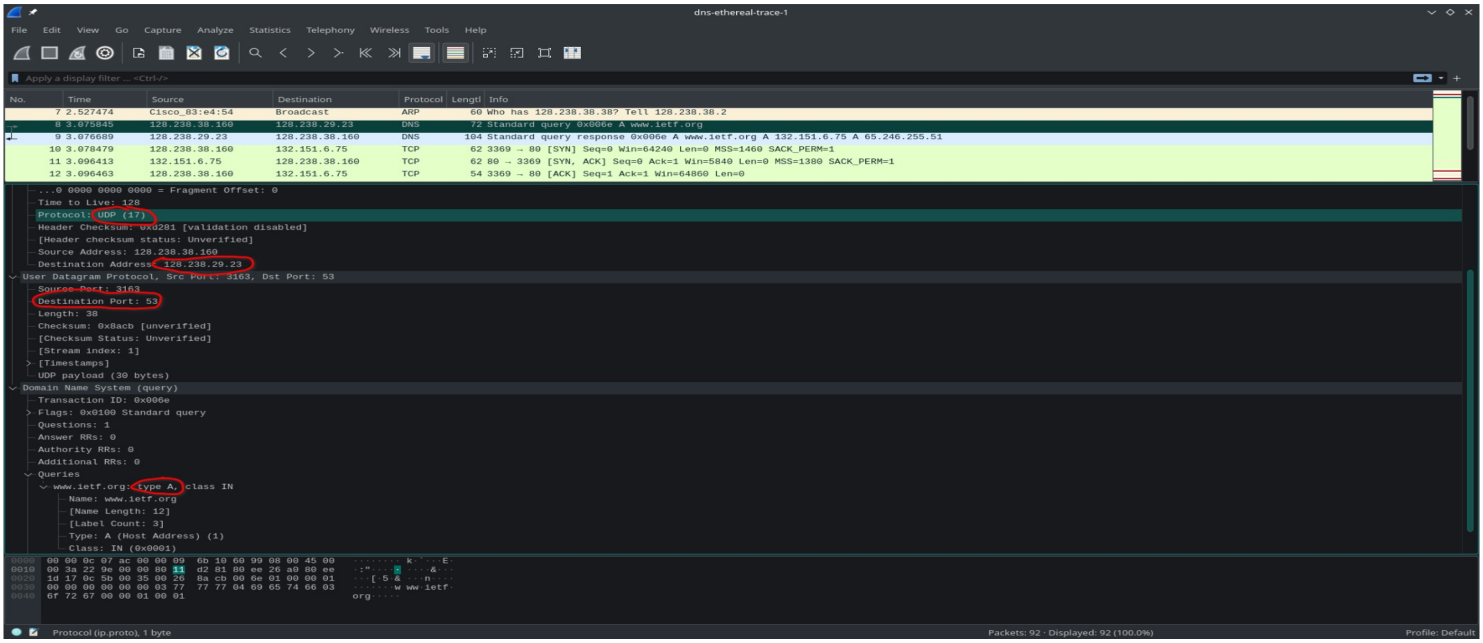
```
No.  Time      Source          Destination     Protocol Lengtl Info
   7 2.527474  Cisco_83:e4:54  Broadcast       ARP       60 Who has 128.238.38.38? Tell 128.238.38.2
   8 3.075845  128.238.38.160  128.238.29.23   DNS       72 Standard query 0x006e A www.ietf.org
   9 3.076689  128.238.29.23   128.238.38.160  DNS      104 Standard query response 0x006e A www.ietf.org A 132.151.6.75 A 65.246.255.51
  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
```

```
> Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54), Dst: IBM_10:60:99 (00:09:6b:10:60:99)
> Internet Protocol Version 4, Src: 128.238.29.23, Dst: 128.238.38.160
> User Datagram Protocol, Src Port: 53, Dst Port: 3163
v Domain Name System (response)
    Transaction ID: 0x006e
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.ietf.org: type A, class IN
        Name: www.ietf.org
        [Name Length: 12]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  v Answers
    v 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 (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 (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 1678 (27 minutes, 58 seconds)
        Data length: 4
        Address: 65.246.255.51
```

1st answer

2nd answer

```
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
```


dns-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

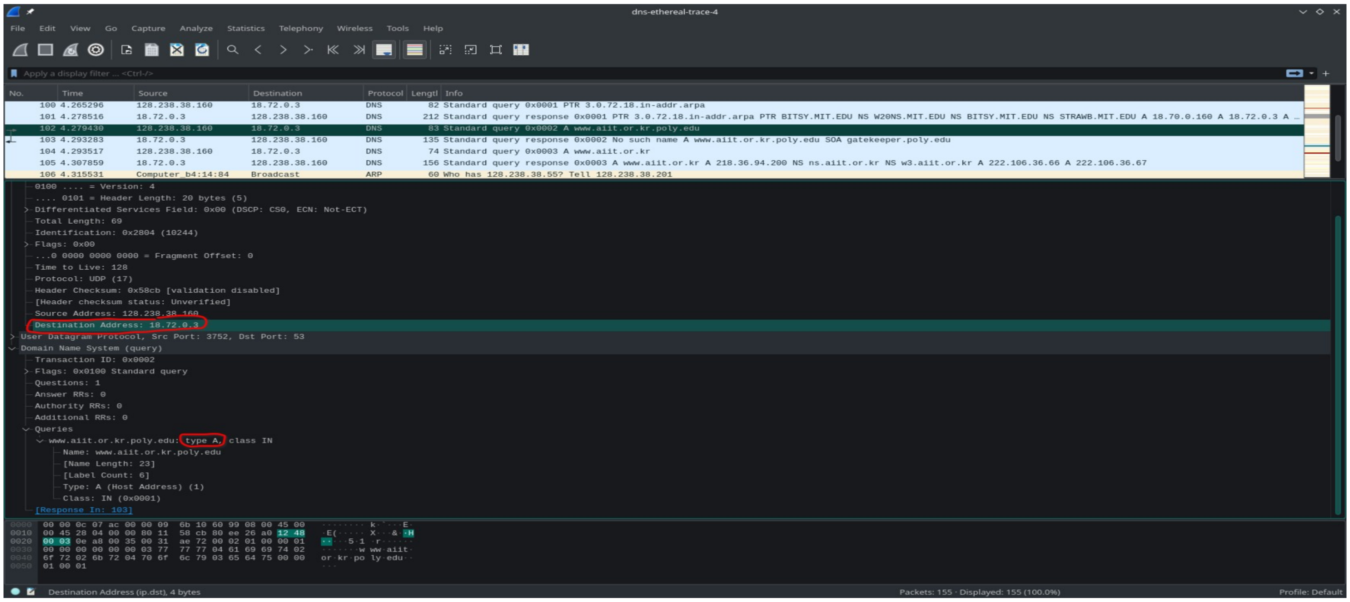
```
No.  Time        Source           Destination      Protocol Lengtl Info
   7 2.527474    Cisco_83:e4:54   Broadcast        ARP       60 Who has 128.238.38.38? Tell 128.238.38.2
   8 3.075845    128.238.38.160   128.238.29.23    DNS       72 Standard query 0x006e A www.ietf.org
   9 3.076689    128.238.29.23    128.238.38.160   DNS      104 Standard query response 0x006e A www.ietf.org A 132.151.6.75 A 65.246.255.51
  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_PERM=1
  12 3.096463    128.238.38.160   132.151.6.75     TCP       54 3369 → 80 [ACK] Seq=1 Ack=1 Win=64860 Len=0

    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0xd281 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.238.38.160
    Destination Address: 128.238.29.23
User Datagram Protocol, Src Port: 3163, Dst Port: 53
    Source Port: 3163
    Destination Port: 53
    Length: 38
    Checksum: 0x8acb [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
    UDP payload (30 bytes)
Domain Name System (query)
    Transaction ID: 0x006e
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
      www.ietf.org: type A, class IN
          Name: www.ietf.org
          [Name Length: 12]
          [Label Count: 3]
          Type: A (Host Address) (1)
          Class: IN (0x0001)

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·····

Protocol (ip.proto), 1 byte          Packets: 92 · Displayed: 92 (100.0%)          Profile: Default
```

Q19-Q21: Please respond to the following questions and add respective screenshot(s):

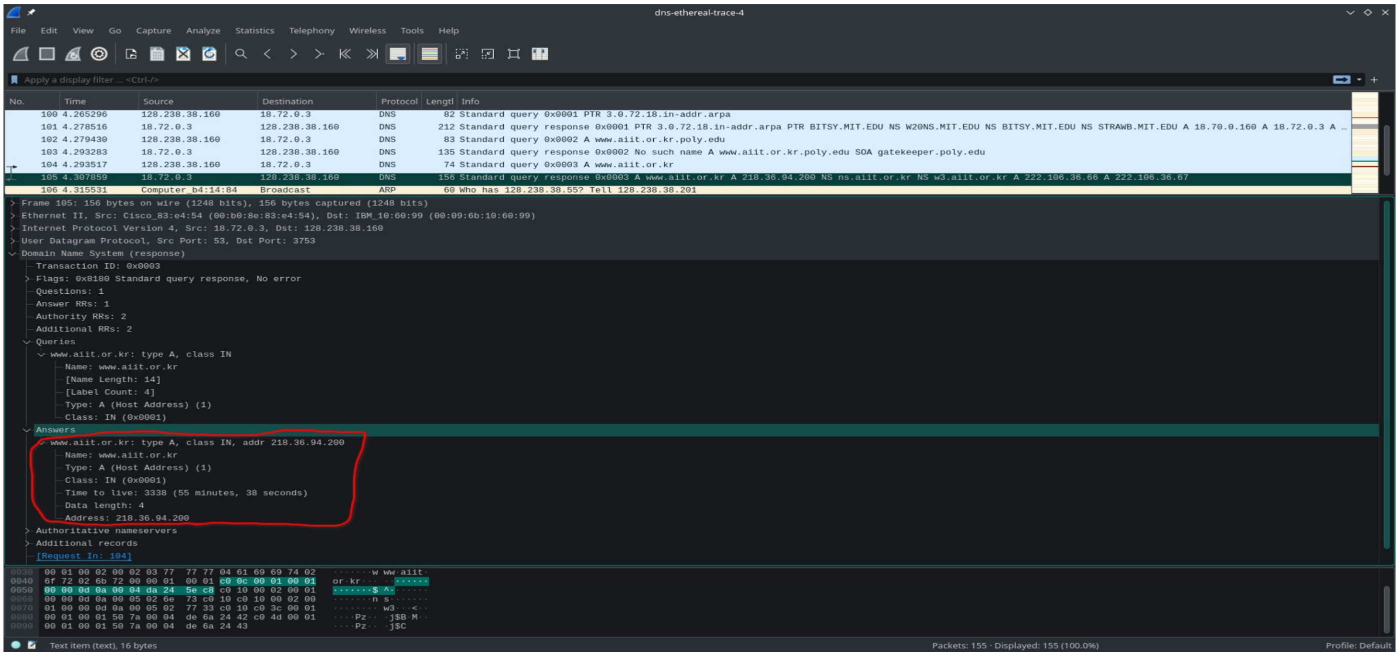
- To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?
  18.72.0.3

- Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
  Type A, doesn't contain any answers

- Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?
  1 answer provided. It contains name of host, type of address, class, the TTL, data length and IP address.


dns-ethereal-trace-4
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time        Source             Destination      Protocol Lengtl 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 BITSY.MIT.EDU NS STRAWB.MIT.EDU A 18.70.0.160 A 18.72.0.3 A …
 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 A 222.106.36.66 A 222.106.36.67
 106 4.315531    Computer_b4:14:84  Broadcast        ARP       60 Who has 128.238.38.55? Tell 128.238.38.201

    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 69
    Identification: 0x2804 (10244)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x58cb [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.238.38.160
    Destination Address: 18.72.0.3
> User Datagram Protocol, Src Port: 3752, Dst Port: 53
Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
      www.aiit.or.kr.poly.edu: type A, class IN
          Name: www.aiit.or.kr.poly.edu
          [Name Length: 23]
          [Label Count: 6]
          Type: A (Host Address) (1)
          Class: IN (0x0001)
    [Response In: 103]

0000  00 00 0c 07 ac 00 00 09  6b 10 60 99 08 00 45 00   ········k·`···E·
0010  00 45 28 04 00 00 80 11  58 cb 80 ee 26 a0 12 48   ·E(·····X···&··H
0020  00 03 0e a8 00 35 00 31  ae 72 00 02 01 00 00 01   ·····5·1 ·r······
0030  00 00 00 00 00 00 03 77  77 77 04 61 69 69 74 02   ·······w ww·aiit·
0040  6f 72 02 6b 72 04 70 6f  6c 79 03 65 64 75 00 00   or·kr·po ly·edu··
0050  01 00 01                                           ···

Destination Address (ip.dst), 4 bytes          Packets: 155 · Displayed: 155 (100.0%)          Profile: Default
```



```
No.  Time       Source             Destination      Protocol  Lengtl  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 BITSY.MIT.EDU NS STRAWB.MIT.EDU A 18.70.0.160 A 18.72.0.3 A …
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 A 222.106.36.66 A 222.106.36.67
106 4.315531   Computer_b4:14:84   Broadcast        ARP        60 Who has 128.238.38.55? Tell 128.238.38.201
```

```
> Frame 105: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits)
> Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54), Dst: IBM_10:60:99 (00:09:6b:10:60:99)
> Internet Protocol Version 4, Src: 18.72.0.3, Dst: 128.238.38.160
> User Datagram Protocol, Src Port: 53, Dst Port: 3753
v Domain Name System (response)
    Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 2
    Additional RRs: 2
  v Queries
    v www.aiit.or.kr: type A, class IN
        Name: www.aiit.or.kr
        [Name Length: 14]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  v Answers
    v www.aiit.or.kr: type A, class IN, addr 218.36.94.200
        Name: www.aiit.or.kr
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 3338 (55 minutes, 38 seconds)
        Data length: 4
        Address: 218.36.94.200
  > Authoritative nameservers
  > Additional records
    [Request In: 104]
```

```
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
```

Text item (text), 16 bytes   Packets: 155 · Displayed: 155 (100.0%)   Profile: Default