Διαχείριση Δικτύων Βασισμένων στο Λογισμικό
2ο εργαστήριο: "HTTP-DNS"

ΟΝΟΜΑΤΕΠΩΝΥΜΟ:	Μαυρόπουλος Νικόλας
Α.Μ.:	21865

HTTP lab

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

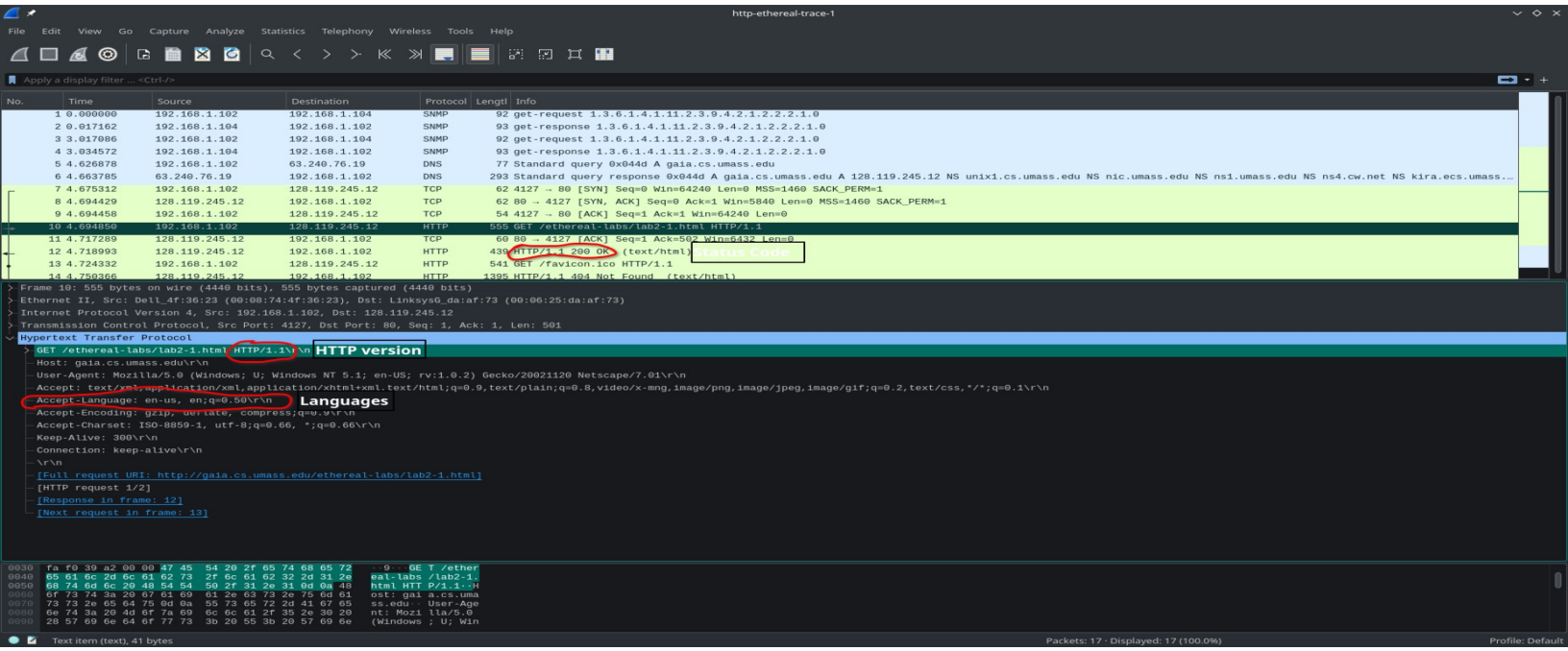
- Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
  Browser HTTP version 1.1. Server HTTP version 1.1

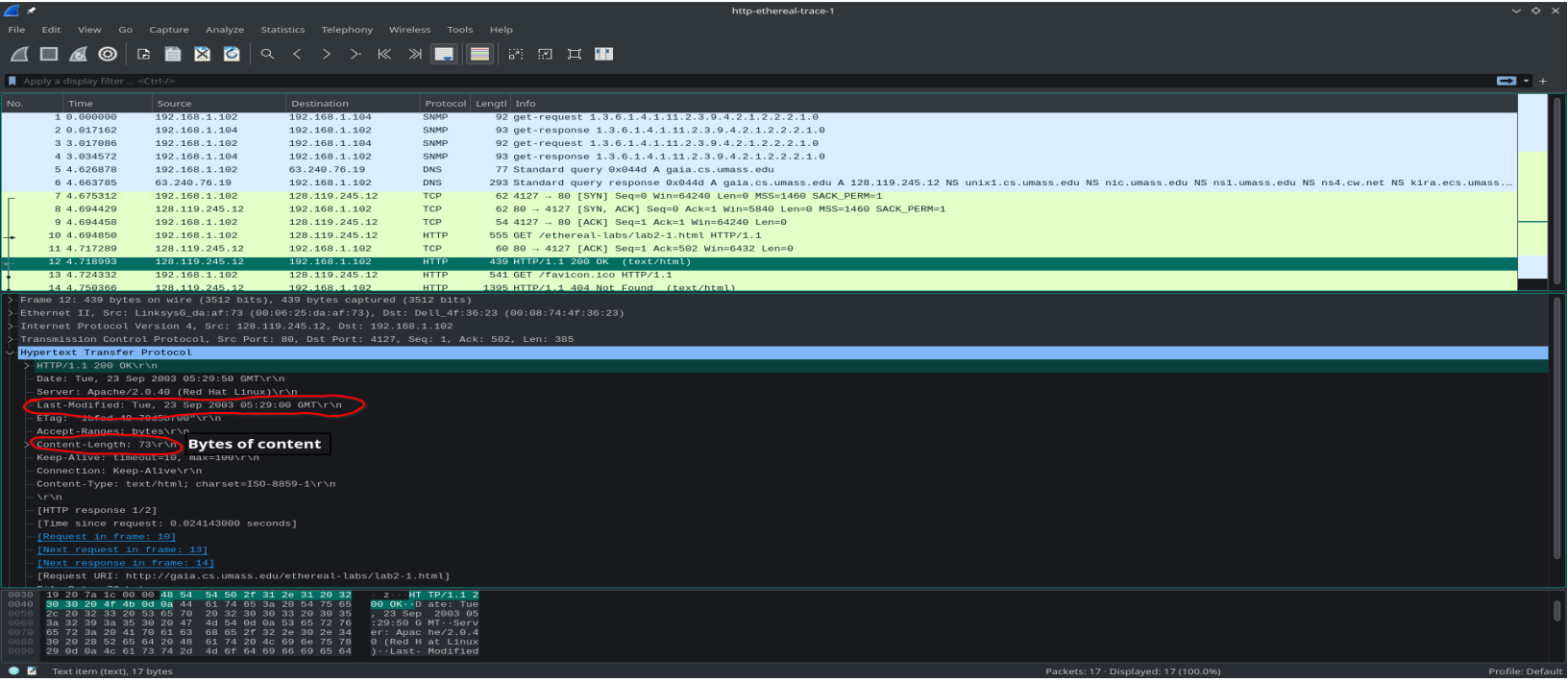
- What languages (if any) does your browser indicate that it can accept to the server?
  En-us, en

- 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

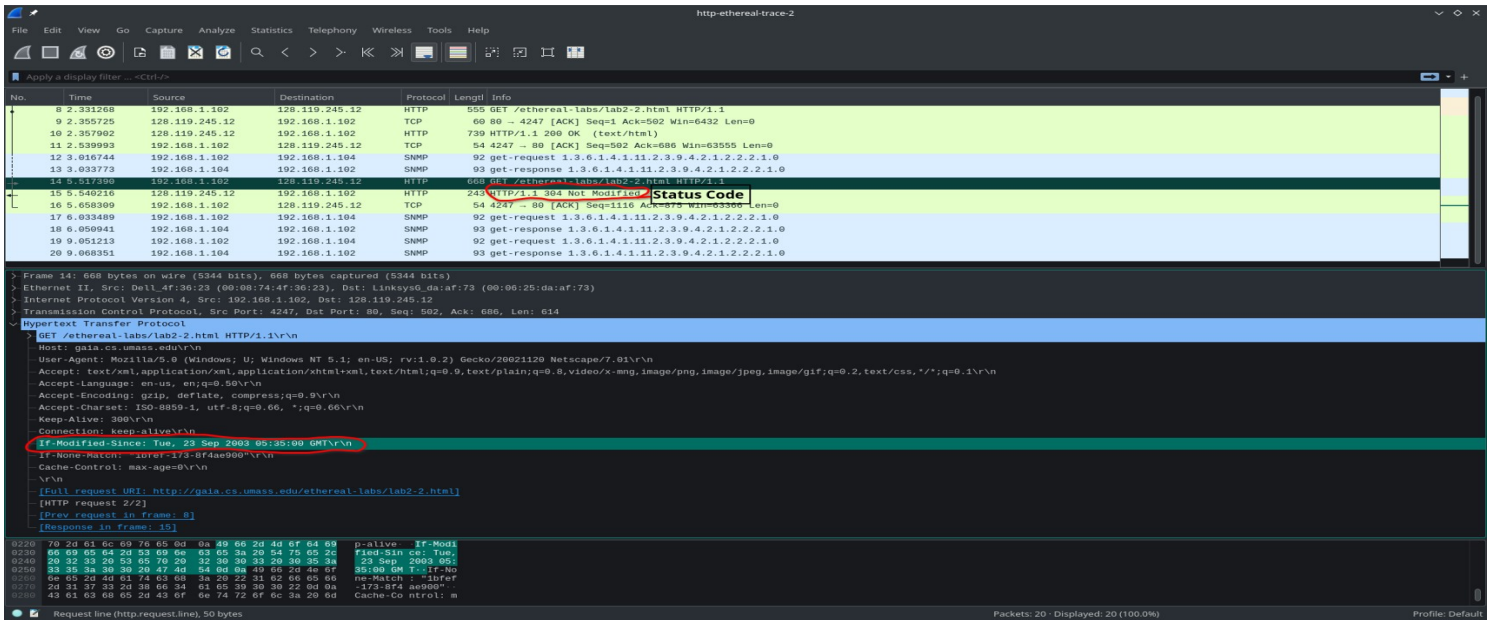




Q9-Q10: Please add a screenshot to justify answers to questions below:

- 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

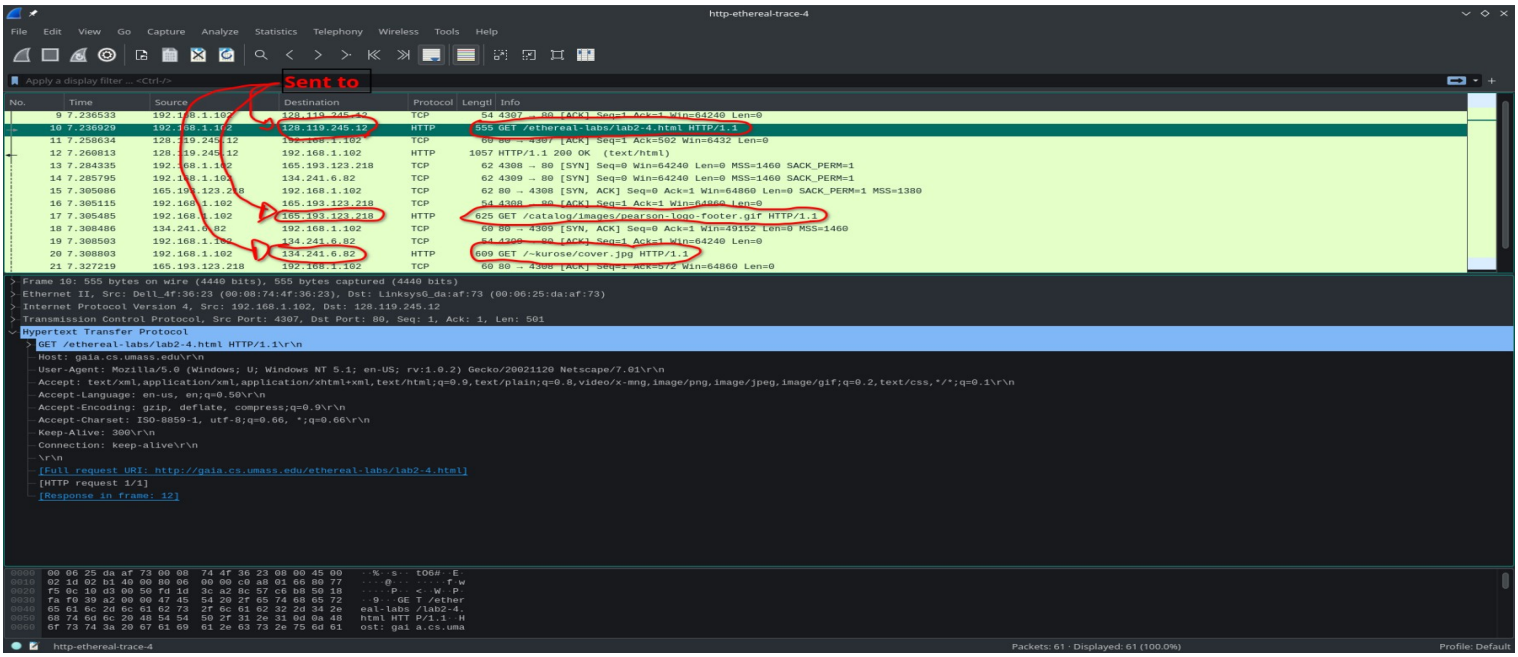
- What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.
  304 Not Modified. So the text of the file is NOT returned in the HTTP message.



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.



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

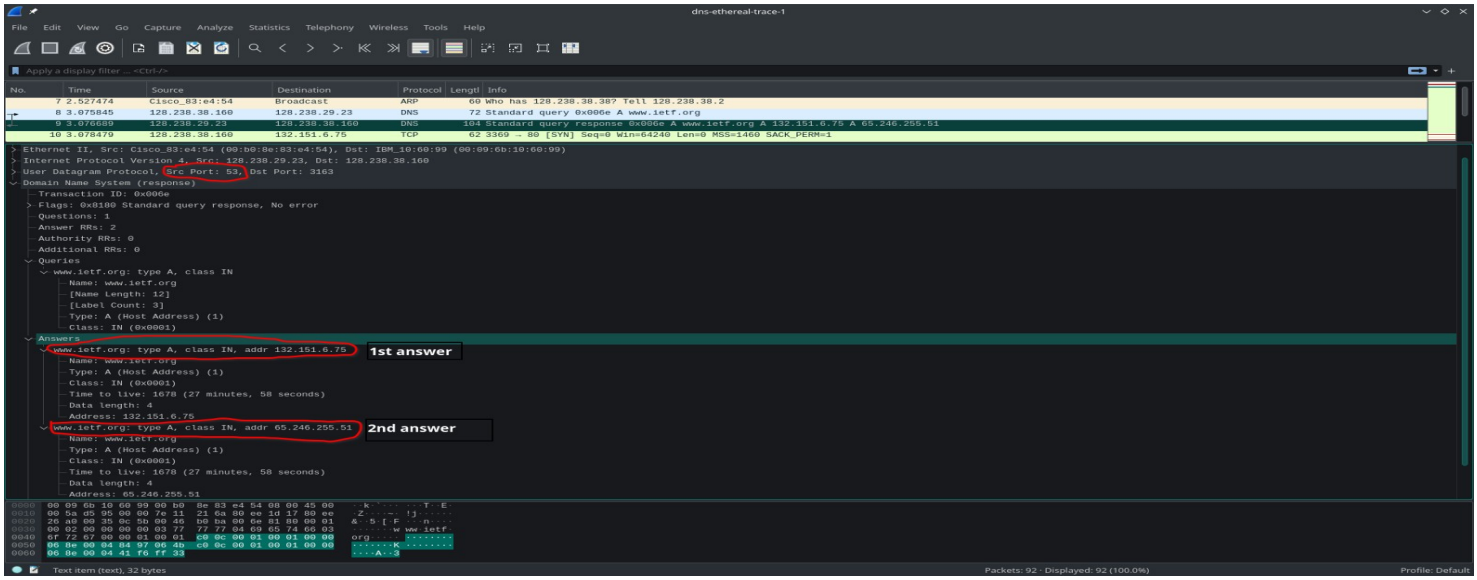
- To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?
  128.238.29.23

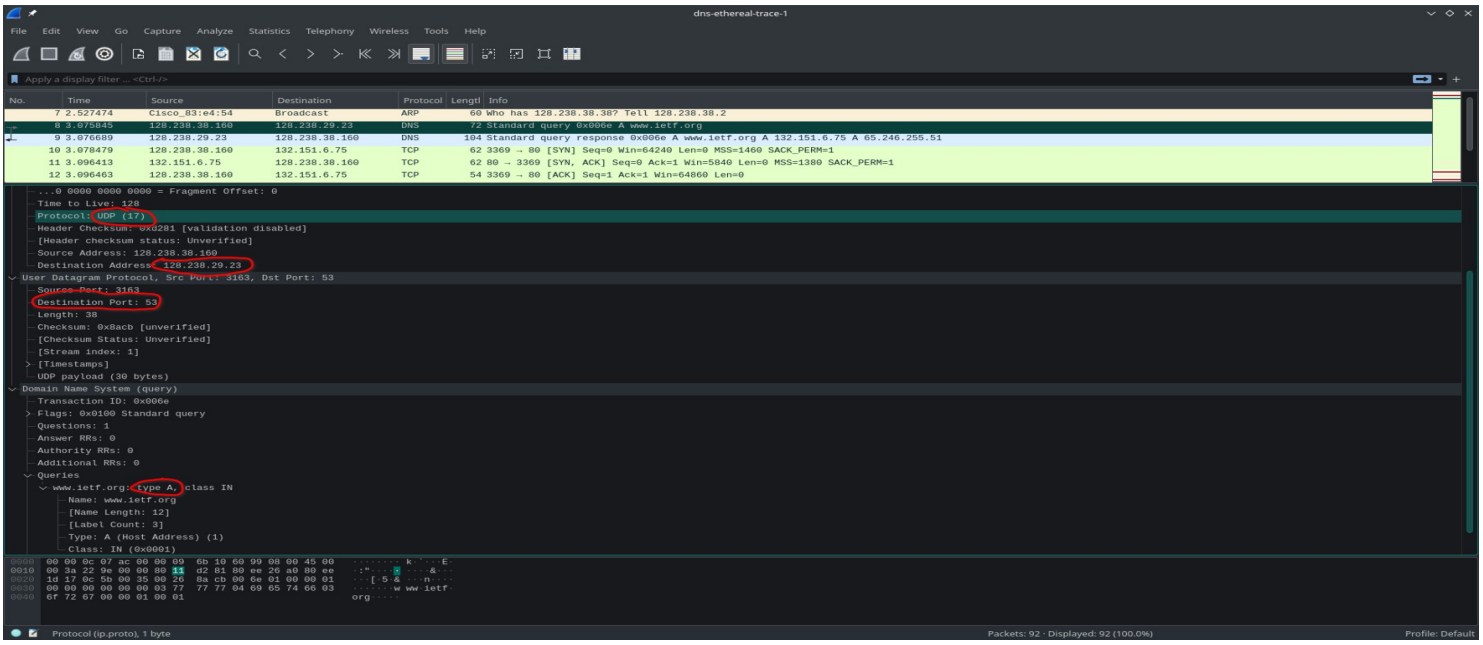
- Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
  Type A. It doesn’t contain any answers.

- 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



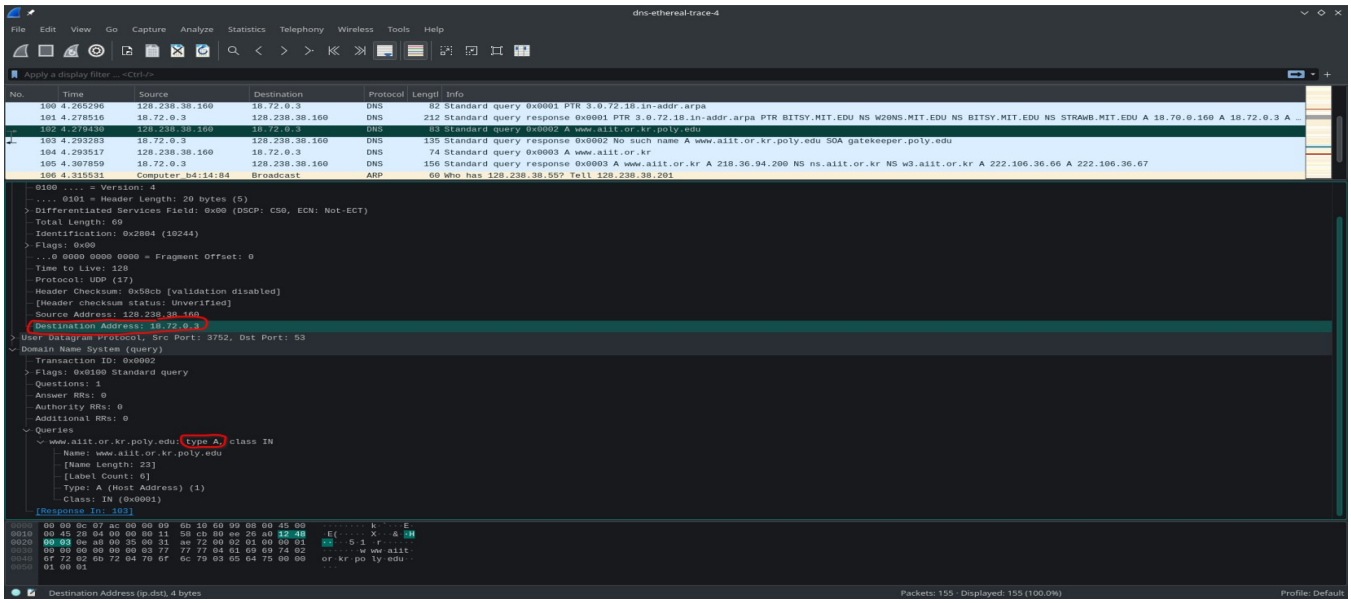


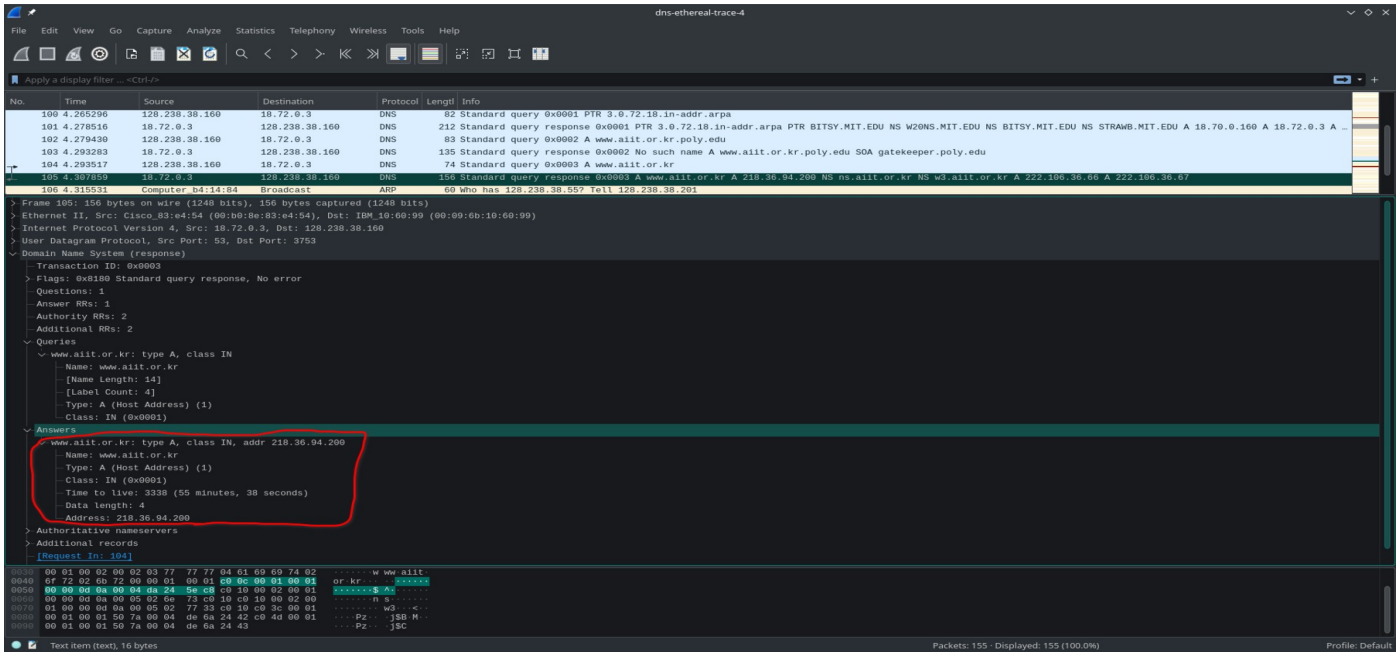
Q19-Q21: Please respond to the following questions and add respective screenshot(s):

- 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
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
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
Queries
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)
Answers
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 04 61 69 69 74 02
0040 6f 72 02 6b 72 00 00 01 00 01 c0 0c 00 01 00 01
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
0070 01 00 00 0d 0a 00 05 02 77 33 c0 10 c0 3c 00 01
0080 00 01 00 01 50 7a 00 04 de 6a 24 42 c0 4d 00 01
0090 00 01 00 01 50 7a 00 04 de 6a 24 43
Text item (text), 16 bytes
Packets: 155 · Displayed: 155 (100.0%)
Profile: Default