

Διαχείριση Δικτύων Βασισμένων στο Λογισμικό

2^ο εργαστήριο: “HTTP-DNS”

ΟΝΟΜΑΤΕΠΩΝΥΜΟ:	Μαυρόπουλος Νικόλας
A.M.:	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

The screenshot shows a Wireshark packet capture of an HTTP transaction. The packet list on the left shows a GET request (No. 10) and a 200 OK response (No. 11). The packet details pane on the right shows the structure of the response. The 'HTTP version' is 1.1. The 'Accept-Language' header is 'en-us, en;q=0.50'. The response body is 'eal-labs/lab2-1.html'.

```
10.000000 192.168.1.102 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.1.0
2.0.017162 192.168.1.102 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.1.0
3.3.037086 192.168.1.102 192.168.1.104 SNMP 93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.1.0
4.3.034572 192.168.1.104 192.168.1.102 SNMP 77 Standard query 0x044d A gaia.cs.umass.edu
5.4.626878 192.168.1.102 63.240.76.19 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.edu
6.4.663785 63.240.76.19 192.168.1.102 DNS 62 4127 -- 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
7.4.675332 192.168.1.102 128.119.245.12 TCP 62 80 -- 4127 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
8.4.694429 128.119.245.12 192.168.1.102 TCP 54 4127 -- 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
9.4.694458 192.168.1.102 128.119.245.12 HTTP 555 GET /etheral-labs/lab2-1.html HTTP/1.1
10.4.694850 192.168.1.102 128.119.245.12 HTTP 60 80 -- 4127 [ACK] Seq=1 Ack=562 Win=6432 Len=0
11.4.717289 128.119.245.12 192.168.1.102 HTTP 439 HTTP/1.1 200 OK (text/html)
12.4.718993 128.119.245.12 192.168.1.102 HTTP 541 GET /favicon.ico HTTP/1.1
13.4.724332 192.168.1.102 128.119.245.12 HTTP 1395 HTTP/1.1 404 Not Found (text/html)
14.4.750366 128.119.245.12 192.168.1.102
```

Frame 10: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits) on Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Linksys_6a: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

Hypertext Transfer Protocol

GET /etheral-labs/lab2-1.html HTTP/1.1

Host: gaia.cs.umass.edu

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01

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

Accept-Language: en-us, en;q=0.50

Accept-Encoding: gzip, deflate, compress;q=0.5

Accept-Charset: ISO-8859-1, utf-8;q=0.66,*q=0.66

Keep-Alive: 300

Connection: keep-alive

[Full request URI: http://gaia.cs.umass.edu/etheral-labs/lab2-1.html]

[HTTP request 1/2]

[Response in frame 12]

[Next request in frame 13]

0030 fa f9 39 a2 00 00 00 47 45 54 20 2f 65 74 68 65 72 -- GET /etheral-labs/lab2-1.html HTTP/1.1

0040 65 61 6c 2d 6c 61 62 73 2f 6c 61 62 32 2d 31 2e eal-labs/lab2-1.html

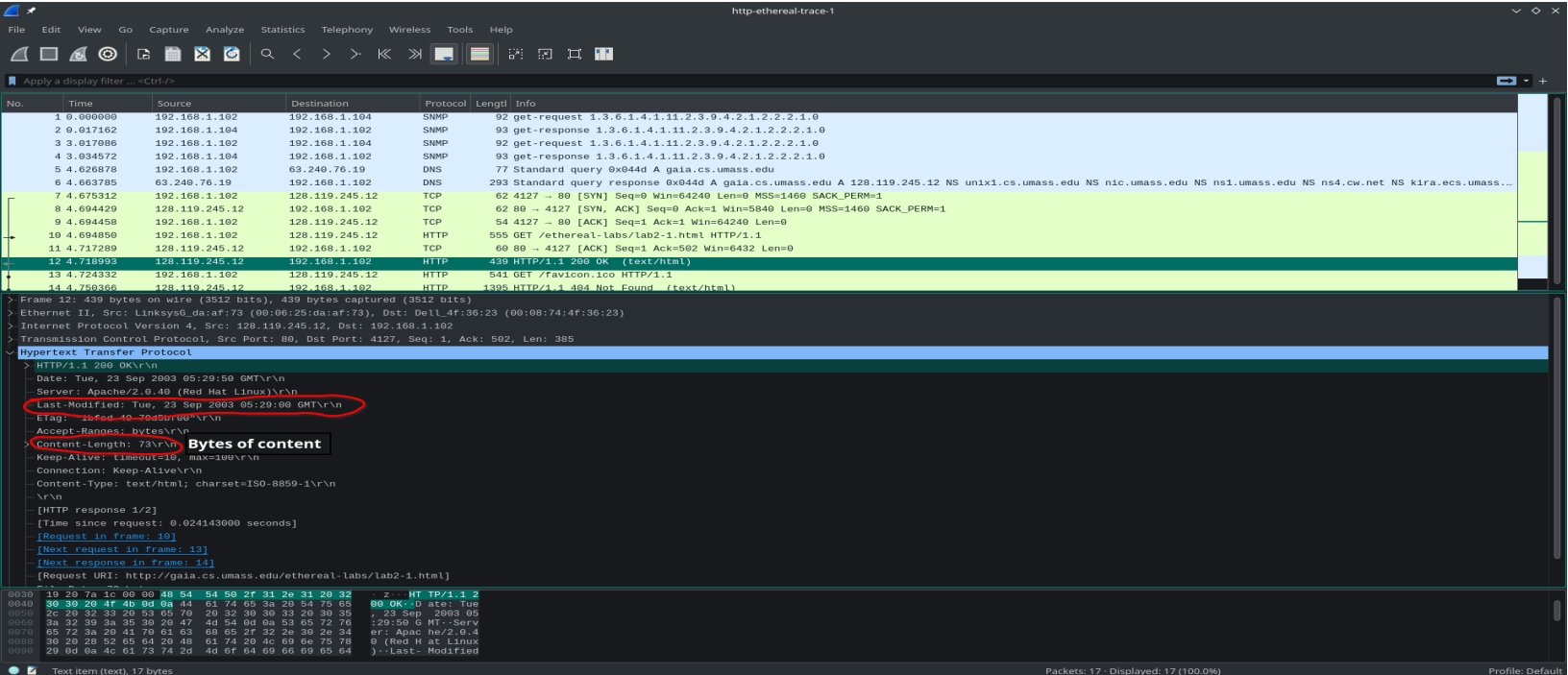
0050 68 74 68 6c 20 48 54 54 50 2f 31 2e 31 2e 31 2e 31 2e HTML HTTP/1.1

0060 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 ost: gaia.cs.umass.edu

0070 73 12 2e 65 64 75 0d 6a 55 73 65 72 2d 31 2f 67 65 User-Agent

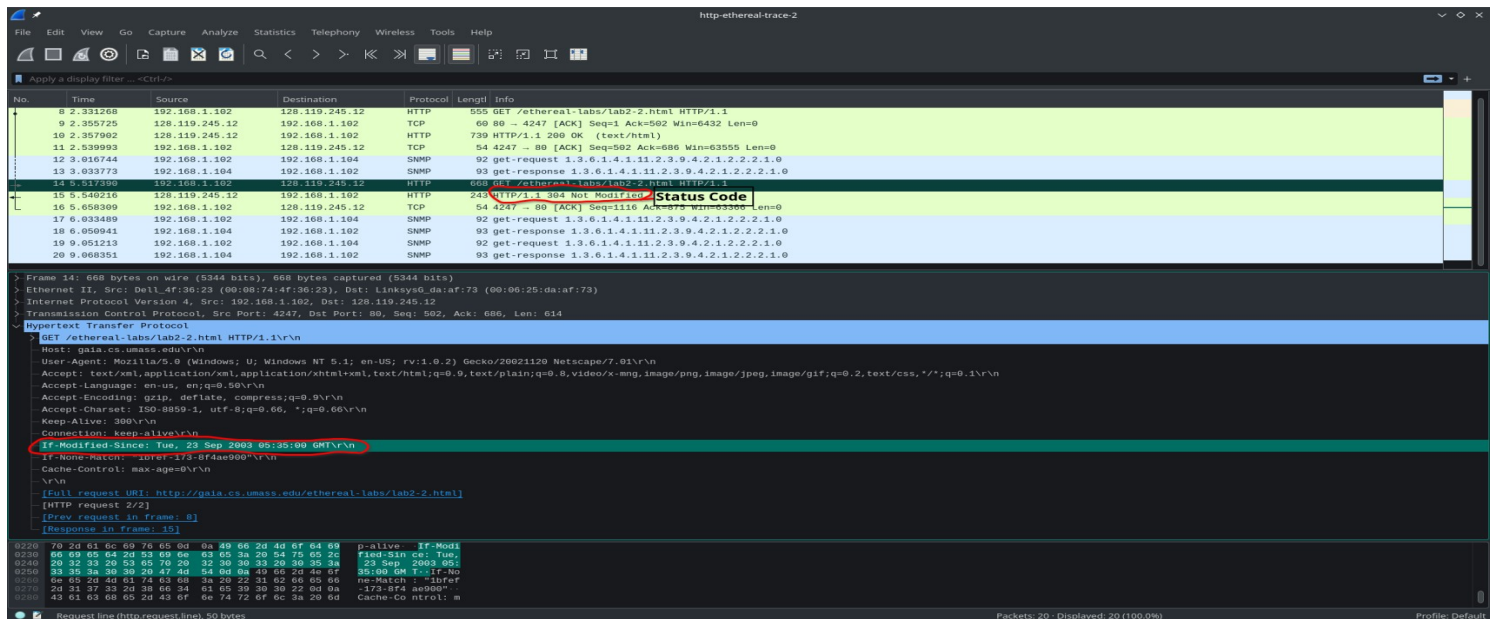
0080 6e 74 3a 20 4d 6f 7a 09 6c 6c 61 2f 35 2e 30 20 nt: Mozilla/5.0

0090 28 57 69 6e 64 6f 77 73 3b 20 55 3b 20 57 69 6e (Windows; U; Win



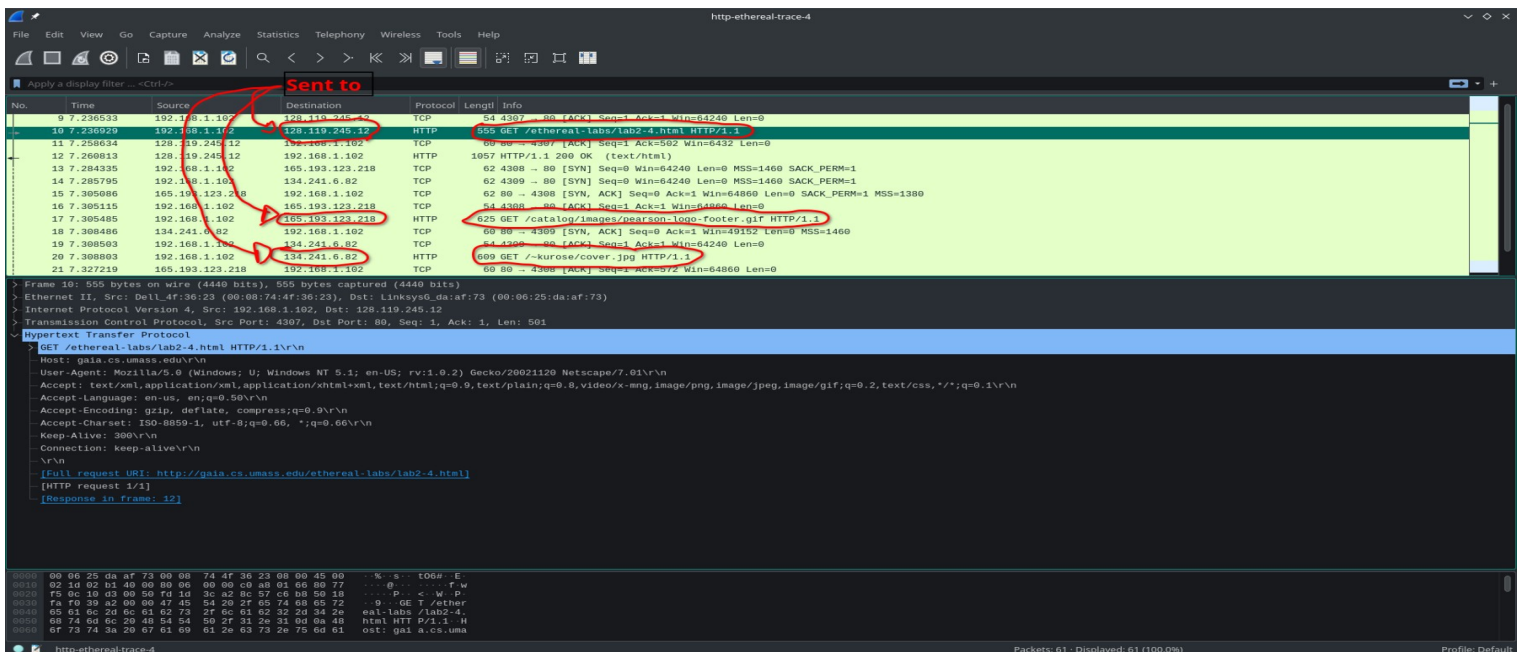
Q9-Q10: Please add a screenshot to justify answers to questions below:

- 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.

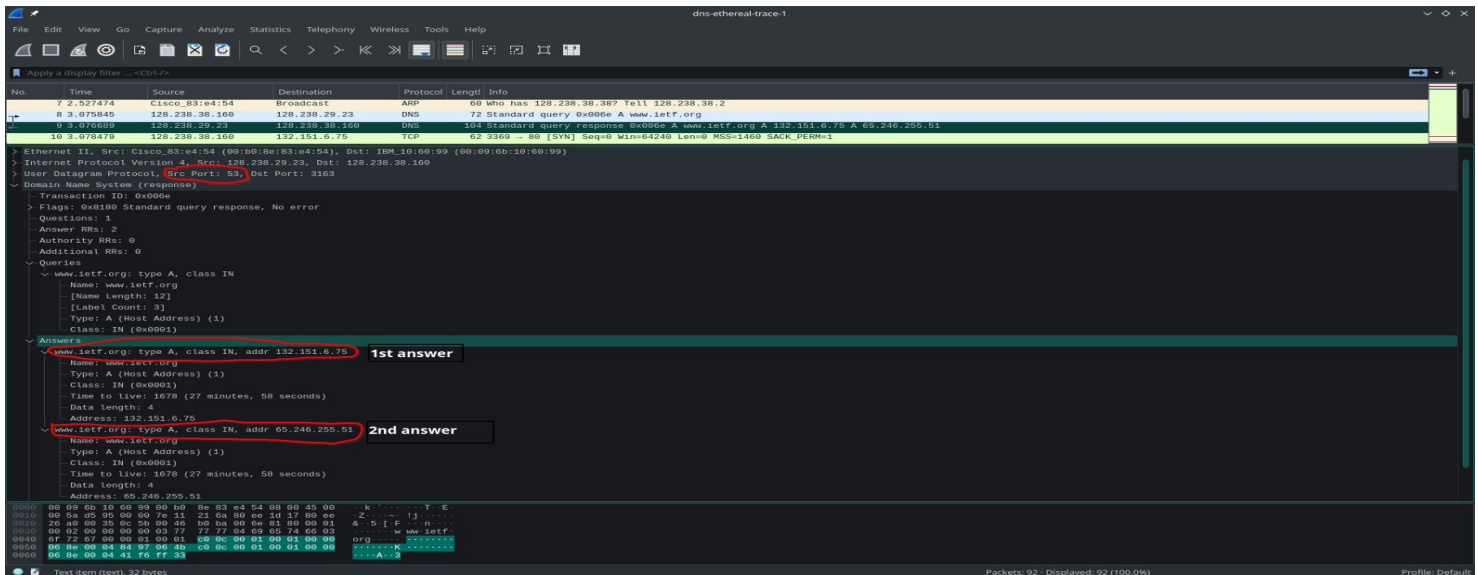


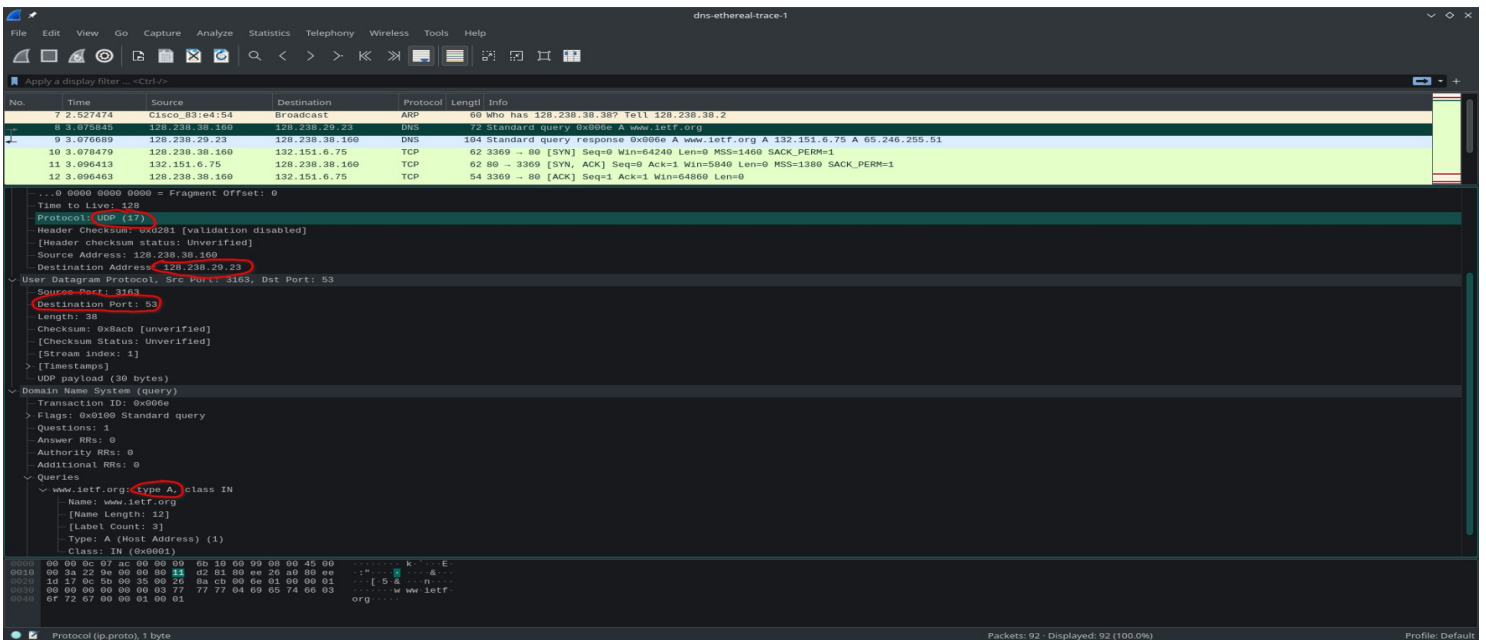
DNS lab

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 port 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

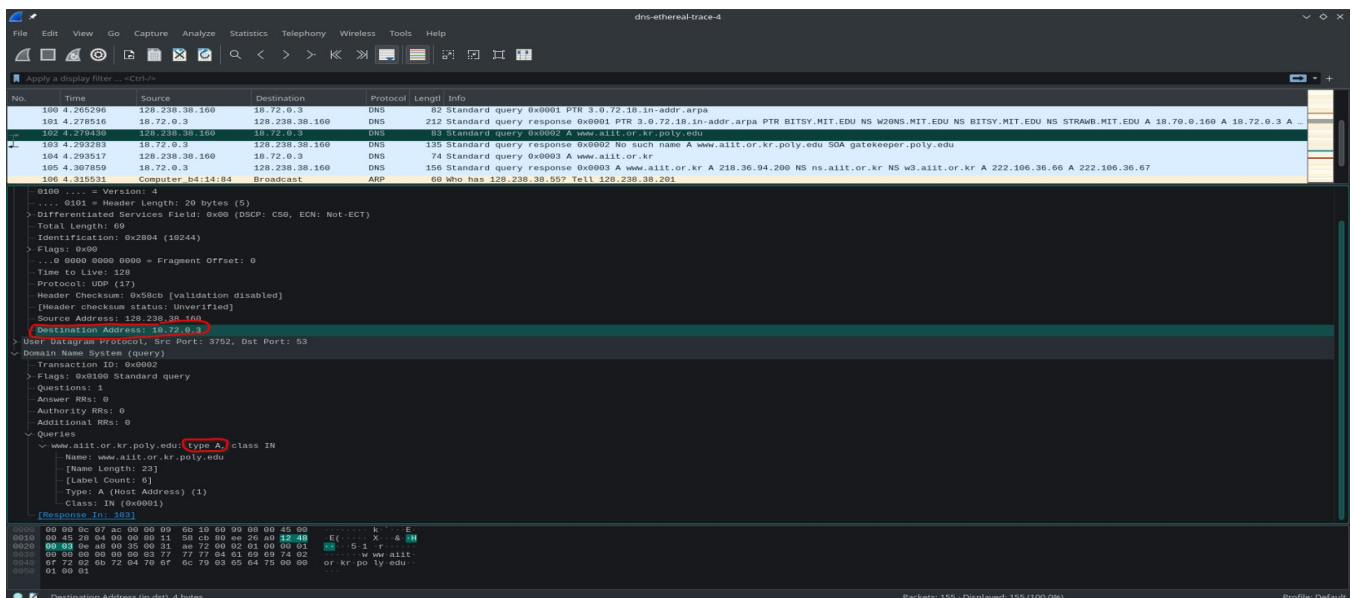
- Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
Type A. It doesn’t contain any answers.
- Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?
2 answers provided. They each contain name 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-F>

No.	Time	Source	Destination	Protocol	Length	Info
100	4.265290	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 W2ONS.MIT.EDU NS BITSY.MIT.EDU NS STRAWB.MIT.EDU A 18.70.0.100 A 18.72.0.3 A ...
102	4.279430	128.238.38.160	18.72.0.3	DNS	83	Standard query 0x0002 A www.a11t.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.a11t.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.a11t.or.kr
105	4.307859	18.72.0.3	128.238.38.160	DNS	156	Standard query response 0x0003 A www.a11t.or.kr A 218.36.94.200 NS ns.a11t.or.kr NS w3.a11t.or.kr A 222.106.36.60 A 222.106.36.67

100-4.315531 Computer(128.238.38.160) Broadcast 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) on 0

> Ethernet II, Src: Cisco_83:e4:54 (00:08:0e: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.a11t.or.kr: type A, class IN

Name: www.a11t.or.kr

[Name Length: 14]

[Label Count: 4]

Type: A (Host Address) (1)

Class: IN (0x0001)

Answers

www.a11t.or.kr: type A, class IN, addr 218.36.94.200

Name: www.a11t.or.kr

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 3238 (55 minutes, 38 seconds)

Data length: 4

Address: 218.36.94.200

Authoritative nameservers

Additional records

[Request in: 104]

0000 00 01 00 02 00 02 03 77 77 77 04 61 69 69 74 02 www.a11t-
0040 6f 72 02 6b 72 09 09 01 00 01 c9 0c 00 01 00 01 or.kr
0080 00 00 00 00 00 04 06 24 5e c8 c9 10 00 02 00 01 \$A
00c0 00 00 0a 0a 00 05 02 6a 73 c0 10 c0 10 00 02 00 n s
0070 01 00 00 0a 0a 00 05 02 77 33 c0 10 c0 3c 00 01 w3
00b0 00 01 00 01 50 7a 00 04 de 6a 24 42 c3 4d 00 01 ... Pz ... JSB H
00f0 00 01 00 01 50 7a 00 04 de 6a 24 43 ... Pz ... JSB H

Text item (text), 16 bytes

Packets: 155 · Displayed: 155 (100.0%)

Profile: Default