VILNIUS UNIVERSITY
SIAULIAI ACADEMY

PROGRAMŲ SISTEMOS BACHELOR STUDY PROGRAMME

Software engineering

ANNA KUTOVA

Computer Networks
Laboratory work No.2
DNS

Šiauliai, 2025

Laboratory Work Report

Table of contents

1. nslookup

1. *Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?*

```
centr@Centrs-MacBook-Air ~ % nslookup imo.gov.qa
Server:         212.230.135.2
Address:        212.230.135.2#53

Non-authoritative answer:
Name:   imo.gov.qa
Address: 20.21.185.159
```

Answer: IP address is : 20.21.185.159

2. *Run nslookup to determine the authoritative DNS servers for a university in Europe.*

```
centr@Centrs-MacBook-Air ~ % nslookup -type=NS www.vu.lt
Server:         212.230.135.1
Address:        212.230.135.1#53

Non-authoritative answer:
www.vu.lt       canonical name = www11001.vu.lt.
www11001.vu.lt  canonical name = web9waf.vu.lt.

Authoritative answers can be found from:
vu.lt
        origin = ns.vu.lt
        mail addr = hostmaster.vu.lt
        serial = 2504241605
        refresh = 28800
        retry = 7200
        expire = 1209600
        minimum = 86400
```

Answer: The authoritative name server for vu.lt is ns.vu.lt

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?*

```
centr@Centrs-MacBook-Air ~ % nslookup -type=MX yahoo.com 212.230.135.1

Server:         212.230.135.1
Address:        212.230.135.1#53

Non-authoritative answer:
yahoo.com       mail exchanger = 1 mta6.am0.yahoodns.net.
yahoo.com       mail exchanger = 1 mta7.am0.yahoodns.net.
yahoo.com       mail exchanger = 1 mta5.am0.yahoodns.net.

Authoritative answers can be found from:
mta7.am0.yahoodns.net   internet address = 67.195.204.72
mta7.am0.yahoodns.net   internet address = 67.195.228.94
mta7.am0.yahoodns.net   internet address = 98.136.96.91
mta7.am0.yahoodns.net   internet address = 67.195.228.109
mta7.am0.yahoodns.net   internet address = 67.195.204.77
mta7.am0.yahoodns.net   internet address = 67.195.228.111
mta7.am0.yahoodns.net   internet address = 98.136.96.74
mta7.am0.yahoodns.net   internet address = 98.136.96.77
```

Answer: IP addresses for mta7.am0.yahoodns.net are:

- 67.195.204.72
- 67.195.228.94
- 98.136.96.91
- 67.195.228.109
- 67.195.204.77
- 67.195.228.111
- 98.136.96.74
- 98.136.96.77

3. Tracing DNS with Wireshark

As I was unable to run Wireshark on a live network connection, I have downloaded a packet trace file that was captured while following the steps on one of the authors' computers of the 'Wireshark Lab: DNS v8.0', as recommended in the lab work explanation.

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

```
No.     Time           Source                Destination           Protocol Length Info
      8 3.075845       128.238.38.160        128.238.29.23         DNS      72     Standard
query 0x006e A www.ietf.org
Frame 8: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
Ethernet II, Src: 00:09:6b:10:60:99, Dst: 00:00:0c:07:ac:00
Internet Protocol Version 4, Src: 128.238.38.160, Dst: 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]
    [Stream Packet Number: 1]
    [Timestamps]
    UDP payload (30 bytes)
Domain Name System (query)
No.     Time           Source                Destination           Protocol Length Info
      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
Frame 9: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)
Ethernet II, Src: 00:b0:8e:83:e4:54, Dst: 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
```

Answer: The DNS query and response messages are sent over UDP. This is confirmed by the protocol field in Wireshark, showing *User Datagram Protocol* for both packets.

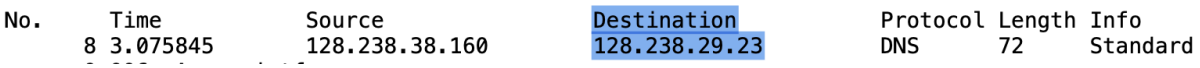
5. *What is the destination port for the DNS query message? What is the source port of DNS response message?*

```
No.     Time           Source                Destination           Protocol Length Info
      8 3.075845       128.238.38.160        128.238.29.23         DNS      72     Standard
query 0x006e A www.ietf.org
Frame 8: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
Ethernet II, Src: 00:09:6b:10:60:99, Dst: 00:00:0c:07:ac:00
Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.23
User Datagram Protocol, Src Port: 3163, Dst Port: 53
    Source Port: 3163
    Destination Port: 53
```

```
No.     Time           Source                Destination           Protocol Length Info
      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
Frame 9: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)
Ethernet II, Src: 00:b0:8e:83:e4:54, Dst: 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
    Source Port: 53
```

Answer: The destination port for the DNS query message - 53. The source port of the DNS response message - 53 as well (as it comes from the DNS server back to the client).

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?



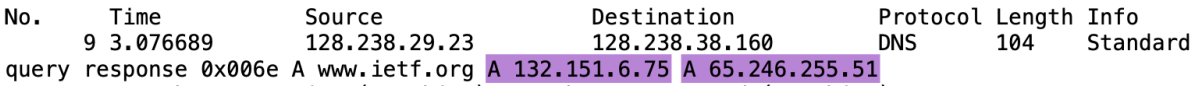
Answer:

a. The DNS query message is sent to IP address **128.238.29.23**
b. This IP address differs from my local DNS server address, since I am using the packet trace file from the lab authors' computer.

7. *Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?*

Answer: The "Type" of the DNS query is A (Address Record), it asks for the IP address of www.ietf.org.
The query message does not contain any answers - it only requests the information.

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



Answer: The DNS response message provides two answers:

1: www.ietf.org: type A, class IN, addr 132.151.6.75
2: www.ietf.org: type A, class IN, addr 65.246.255.51

These are the IP addresses corresponding to the domain www.ietf.org.

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?*

```
  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.
 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_
```

```
No.     Time           Source                Destination           Protocol Length Info
     10 3.078479       128.238.38.160        132.151.6.75          TCP      62     3369 → 80

No.     Time           Source                Destination           Protocol Length Info
      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
```

Answer: Yes, the destination IP address 132.151.6.75 of the SYN packet corresponds to the IP addresses provided in the DNS response message, which was the first answer "1: www.ietf.org: type A, class IN, addr 132.151.6.75".

10. *This web page contains images. Before retrieving each image, does your host issue new DNS queries?*

```
21 3.153293    128.238.38.160    132.151.6.75      TCP           54 3369 → 80 [ACK] Seq=376 Ack=5143 Win=63859 Len=0
22 3.161867    128.238.38.160    132.151.6.75      TCP           54 3369 → 80 [FIN, ACK] Seq=376 Ack=5143 Win=63859 Len=0
23 3.174716    132.151.6.75      128.238.38.160    TCP           60 80 → 3369 [ACK] Seq=5143 Ack=377 Win=6432 Len=0
24 3.178159    128.238.38.160    132.151.6.75      TCP           62 3370 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
25 3.179283    128.238.38.160    132.151.6.75      TCP           62 3371 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
26 3.191649    132.151.6.75      128.238.38.160    TCP           62 80 → 3370 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM
27 3.191726    128.238.38.160    132.151.6.75      TCP           54 3370 → 80 [ACK] Seq=1 Ack=1 Win=64860 Len=0
28 3.191998    128.238.38.160    132.151.6.75      HTTP         320 GET /images/ietflogo2e.gif HTTP/1.1
29 3.192665    132.151.6.75      128.238.38.160    TCP           62 80 → 3371 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM
30 3.192695    128.238.38.160    132.151.6.75      TCP           54 3371 → 80 [ACK] Seq=1 Ack=1 Win=64860 Len=0
31 3.192869    128.238.38.160    132.151.6.75      HTTP         314 GET /images/blue.gif HTTP/1.1
32 3.205736    132.151.6.75      128.238.38.160    TCP           60 80 → 3370 [ACK] Seq=1 Ack=267 Win=6432 Len=0
33 3.214651    132.151.6.75      128.238.38.160    TCP         1434 80 → 3370 [ACK] Seq=1 Ack=267 Win=6432 Len=1380 [TCP PDU reassembled in 36]
34 3.222185    132.151.6.75      128.238.38.160    TCP         1434 80 → 3370 [ACK] Seq=1381 Ack=267 Win=6432 Len=1380 [TCP PDU reassembled in 36]
35 3.222249    128.238.38.160    132.151.6.75      TCP           54 3370 → 80 [ACK] Seq=267 Ack=2761 Win=64860 Len=0
36 3.228451    132.151.6.75      128.238.38.160    HTTP        1212 HTTP/1.1 200 OK  (GIF89a)
37 3.228509    128.238.38.160    132.151.6.75      TCP           54 3370 → 80 [ACK] Seq=267 Ack=3920 Win=63702 Len=0
38 3.228523    132.151.6.75      128.238.38.160    TCP           60 80 → 3371 [ACK] Seq=1 Ack=261 Win=6432 Len=0
39 3.230578    132.151.6.75      128.238.38.160    HTTP         407 HTTP/1.1 200 OK  (GIF89a)
```

Answer: No, before retrieving each image, host wasn't issuing new queries. There were only 2 DNS queries at the start, in Frames 8 and 9.

11. *What is the destination port for the DNS query message? What is the source port of DNS response message?*

```
No.     Time           Source                Destination           Protocol Length Info
     15 4.951232       128.238.38.160        128.238.29.22         DNS      86     Standard
query 0x0001 PTR 22.29.238.128.in-addr.arpa
Frame 15: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 00:09:6b:10:60:99, Dst: 00:00:0c:07:ac:00
Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.22
User Datagram Protocol, Src Port: 3740, Dst Port: 53
    Source Port: 3740
    Destination Port: 53
```

Answer:

a. Destination port for the DNS query message - 53
b. Source port of DNS response message - 3740

12. *To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?*

```
No.     Time           Source                Destination           Protocol Length Info
     15 4.951232       128.238.38.160        128.238.29.22         DNS      86     Standard
query 0x0001 PTR 22.29.238.128.in-addr.arpa
```

Answer: the DNS query message is sent to 128.238.29.22, which is the configured local DNS server on the author's system.
(Note: this is not the same as the DNS server on my system.)

13. *Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?*

```
No.     Time           Source                Destination           Protocol Length Info
     15 4.951232       128.238.38.160        128.238.29.22         DNS      86     Standard
query 0x0001 PTR 22.29.238.128.in-addr.arpa

No.     Time           Source                Destination           Protocol Length Info
     17 4.952571       128.238.38.160        128.238.29.22         DNS      80     Standard
query 0x0002 A www.mit.edu.poly.edu

No.     Time           Source                Destination           Protocol Length Info
     19 4.953172       128.238.38.160        128.238.29.22         DNS      71     Standard
query 0x0003 A www.mit.edu
```

Answer:

a. - Frame 15: 22.29.238.128.in-addr.arpa: **type PTR**, class IN
- Frame 17: www.mit.edu.poly.edu: **type A**, class IN
- Frame 19: www.mit.edu: **type A**, class IN

```
Domain Name System (query)
    Transaction ID: 0x0001
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0

Domain Name System (query)
    Transaction ID: 0x0002
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0

Domain Name System (query)
    Transaction ID: 0x0003
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
```

b. None of the query messages contain any answers.

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

```
Transaction ID: 0x0001
Flags: 0x8580 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
Answers
    22.29.238.128.in-addr.arpa: type PTR, class IN, dns-prime.poly.edu
```

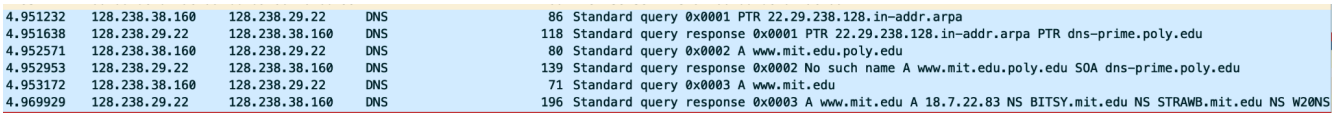
```
Transaction ID: 0x0002
Flags: 0x8583 Standard query response, No such name
Questions: 1
Answer RRs: 0
```

```
Transaction ID: 0x0003
Flags: 0x8580 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 3
Additional RRs: 3
Queries
Answers
    www.mit.edu: type A, class IN, addr 18.7.22.83
Authoritative nameservers
    mit.edu: type NS, class IN, ns BITSY.mit.edu
    mit.edu: type NS, class IN, ns STRAWB.mit.edu
    mit.edu: type NS, class IN, ns W20NS.mit.edu
Additional records
    BITSY.mit.edu: type A, class IN, addr 18.72.0.3
    STRAWB.mit.edu: type A, class IN, addr 18.71.0.151
    W20NS.mit.edu: type A, class IN, addr 18.70.0.160
```

Answer:

- **Packet 16** (response to PTR query): 1 answer : 22.29.238.128.in-addr.arpa: type PTR, class IN, dns-prime.poly.edu
- **Packet 18** (response to www.mit.edu.poly.edu): 0 answers : no such name
- **Packet 20** (response to www.mit.edu): 1 answer : www.mit.edu: type A, class IN, addr 18.7.22.83 (Also contains 3 authority records and 3 additional records).

15. *Provide a screenshot.*



```
4.951232   128.238.38.160   128.238.29.22    DNS    86  Standard query 0x0001 PTR 22.29.238.128.in-addr.arpa
4.951638   128.238.29.22    128.238.38.160   DNS   118  Standard query response 0x0001 PTR 22.29.238.128.in-addr.arpa PTR dns-prime.poly.edu
4.952571   128.238.38.160   128.238.29.22    DNS    80  Standard query 0x0002 A www.mit.edu.poly.edu
4.952953   128.238.29.22    128.238.38.160   DNS   139  Standard query response 0x0002 No such name A www.mit.edu.poly.edu SOA dns-prime.poly.edu
4.953172   128.238.38.160   128.238.29.22    DNS    71  Standard query 0x0003 A www.mit.edu
4.969929   128.238.29.22    128.238.38.160   DNS   196  Standard query response 0x0003 A www.mit.edu A 18.7.22.83 NS BITSY.mit.edu NS STRAWB.mit.edu NS W20NS
```

16. *To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?*

```
No.     Time           Source                Destination           Protocol Length Info
    488 30.916492      128.238.38.160        128.238.29.22         DNS      86     Standard
query 0x0001 PTR 22.29.238.128.in-addr.arpa
```

Answer:

a. the DNS query message sent to IP address **128.238.29.22**
b. Yes, this IP address should be the default local DNS server on the authors' computers.

17. *Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?*

```
Domain Name System (query)
    Transaction ID: 0x0003
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        mit.edu: type NS, class IN
    [Response In: 493]
```

Answer:

a. The type of the DNS query message is **NS** (Name Server)
b. No, the query message doesn't contain any answers: **Answer RRs: 0**

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 namesers?*

```
No.     Time           Source                Destination           Protocol Length Info
    493 30.918636      128.238.29.22         128.238.38.160        DNS      176    Standard
query response 0x0003 NS mit.edu NS bitsy.mit.edu NS strawb.mit.edu NS w20ns.mit.edu A
18.72.0.3 A 18.71.0.151 A 18.70.0.160

Answers
    mit.edu: type NS, class IN, ns bitsy.mit.edu
    mit.edu: type NS, class IN, ns strawb.mit.edu
    mit.edu: type NS, class IN, ns w20ns.mit.edu
Additional records
    bitsy.mit.edu: type A, class IN, addr 18.72.0.3
    strawb.mit.edu: type A, class IN, addr 18.71.0.151
    w20ns.mit.edu: type A, class IN, addr 18.70.0.160
[Request In: 492]
```

Answer:

a. In Frame 493, the response lists these MIT nameservers:
   - bitsy.mit.edu
   - strawb.mit.edu
   - w20ns.mit.edu

b. Yes, it also provides their IP addresses:
   - bitsy.mit.edu: 18.72.0.3
   - strawb.mit.edu: 18.71.0.151
   - w20ns.mit.edu: 18.70.0.160

19. *Provide a screenshot.*

```
488 30.916492  128.238.38.160  128.238.29.22   DNS   86 Standard query 0x0001 PTR 22.29.238.128.in-addr.arpa
489 30.916859  128.238.29.22   128.238.38.160  DNS  118 Standard query response 0x0001 PTR 22.29.238.128.in-addr.arpa PTR dns-prime.poly.edu
490 30.917700  128.238.38.160  128.238.29.22   DNS   76 Standard query 0x0002 NS mit.edu.poly.edu
491 30.918044  128.238.29.22   128.238.38.160  DNS  135 Standard query response 0x0002 No such name NS mit.edu.poly.edu SOA dns-prime.poly.edu
492 30.918275  128.238.38.160  128.238.29.22   DNS   67 Standard query 0x0003 NS mit.edu
493 30.918636  128.238.29.22   128.238.38.160  DNS  176 Standard query response 0x0003 NS mit.edu NS bitsy.mit.edu NS strawb.mit.edu NS w20ns.mit
```

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?*

No.	Time	Source	Destination	Protocol	Length	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

Answer:

a. the DNS query message sent to IP address **18.72.0.3**
b. No, the IP address 18.72.0.3 is not the IP address of my default local DNS server.
c. According to WHOIS, this IP belongs to Amazon Technologies Inc. and corresponds to a server in Amazon's global network, not to a local DNS resolver on my network.

21. *Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?*

```
No.     Time           Source                Destination           Protocol Length 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
Frame 100: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)
Ethernet II, Src: 00:09:6b:10:60:99, Dst: 00:00:0c:07:ac:00
Internet Protocol Version 4, Src: 128.238.38.160, Dst: 18.72.0.3
User Datagram Protocol, Src Port: 3751, Dst Port: 53
Domain Name System (query)
    Transaction ID: 0x0001
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
```

```
No.     Time           Source                Destination           Protocol Length Info
    104 4.293517       128.238.38.160        18.72.0.3             DNS      74     Standard
query 0x0003 A www.aiit.or.kr
Frame 104: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: 00:09:6b:10:60:99, Dst: 00:00:0c:07:ac:00
Internet Protocol Version 4, Src: 128.238.38.160, Dst: 18.72.0.3
User Datagram Protocol, Src Port: 3753, Dst Port: 53
Domain Name System (query)
    Transaction ID: 0x0003
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
```

Answer:

a. Frame 100: Type - PTR; Answers - 0 (Answer RRs: 0)
b. Frame 104: Type - A; Answers - 0 (Answer RRs: 0)

22. *Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?*

```
No.     Time           Source                Destination           Protocol Length Info
    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 18.71.0.151

 Domain Name System (response)
     Transaction ID: 0x0001
     Flags: 0x8580 Standard query response, No error
     Questions: 1
     Answer RRs: 1
     Authority RRs: 3
     Additional RRs: 3
     Queries
         3.0.72.18.in-addr.arpa: type PTR, class IN
     Answers
         3.0.72.18.in-addr.arpa: type PTR, class IN, BITSY.MIT.EDU
     Authoritative nameservers
         18.in-addr.arpa: type NS, class IN, ns W20NS.MIT.EDU
         18.in-addr.arpa: type NS, class IN, ns BITSY.MIT.EDU
         18.in-addr.arpa: type NS, class IN, ns STRAWB.MIT.EDU
     Additional records
         W20NS.MIT.EDU: type A, class IN, addr 18.70.0.160
         BITSY.MIT.EDU: type A, class IN, addr 18.72.0.3
         STRAWB.MIT.EDU: type A, class IN, addr 18.71.0.151
```

```
Frame 103: 135 bytes on wire (1080 bits), 135 bytes captured (1080 bits)
Ethernet II, Src: 00:b0:8e:83:e4:54, Dst: 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: 3752
Domain Name System (response)
    Transaction ID: 0x0002
    Flags: 0x8583 Standard query response, No such name
    Questions: 1
    Answer RRs: 0
```

Answer:

a. Frame 101:Answers - 1 (Answer RRs: 1)
Content: 3.0.72.18.in-addr.arpa: type PTR, class IN, BITSY.MIT.EDU

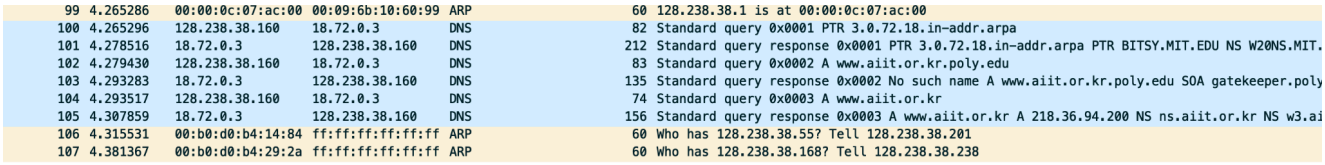
Additionally, it provides:

3 authoritative nameservers: nameservers
-W20NS.MIT.EDU
- BITSY.MIT.EDU
- STRAWB.MIT.EDU

Additional records: 3 A records with IP addresses for the nameservers

b. Frame 104:Answers - 0 (“No such name”)

23.*Provide a screenshot.*



99	4.265286	00:00:0c:07:ac:00	00:09:6b:10:60:99	ARP	60	128.238.38.1 is at 00:00:0c:07:ac:00
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.
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
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.ai
106	4.315531	00:b0:d0:b4:14:84	ff:ff:ff:ff:ff:ff	ARP	60	Who has 128.238.38.55? Tell 128.238.38.201
107	4.381367	00:b0:d0:b4:29:2a	ff:ff:ff:ff:ff:ff	ARP	60	Who has 128.238.38.168? Tell 128.238.38.238