



תקשרות

מטלה נ

Nathanael Benichou



WIRESHARK

DNS

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

```
nathben97@nathben97-VirtualBox: ~
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
tsinghua.edu.cn nameserver = ns2.cuhk.hk.
tsinghua.edu.cn nameserver = dns.tsinghua.edu.cn.
tsinghua.edu.cn nameserver = dns2.tsinghua.edu.cn.
tsinghua.edu.cn nameserver = dns2.edu.cn.

Authoritative answers can be found from:

nathben97@nathben97-VirtualBox: ~$ nslookup www.apple.co.jp
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
www.apple.co.jp canonical name = apple.co.jp.
Name:  apple.co.jp
Address: 17.172.224.38
Name:  apple.co.jp
Address: 17.142.160.9
Name:  apple.co.jp
Address: 17.178.96.9
```

Adresses :

- 17.172.224.38
- 17.142.160.9
- 17.178.96.9

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

```
nathben97@nathben97-VirtualBox: ~
www.apple.co.jp canonical name = apple.co.jp.
Name: apple.co.jp
Address: 17.172.224.38
Name: apple.co.jp
Address: 17.142.160.9
Name: apple.co.jp
Address: 17.178.96.9

nathben97@nathben97-VirtualBox:~$ c
c : commande introuvable
nathben97@nathben97-VirtualBox:~$ nslookup -type=NS univ-amu.fr
nslookup: '-type=NS' is not a legal IDNA2008 name (string contains a disallowed character), use +noidn
nathben97@nathben97-VirtualBox:~$ nslookup -type=NS univ-amu.fr
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
univ-amu.fr      nameserver = ns1.univmed.fr.
univ-amu.fr      nameserver = cnudns.cines.fr.

Authoritative answers can be found from:
```

Servers :

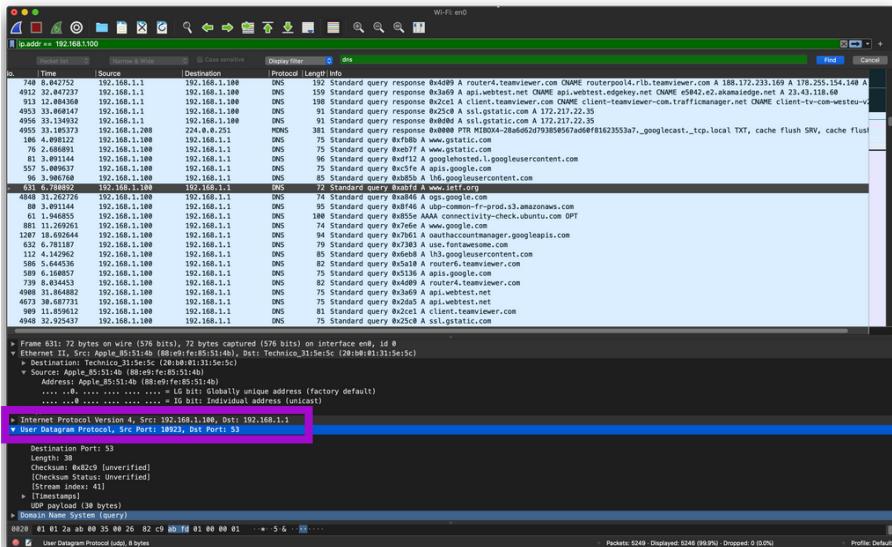
- ns1.univmed.fr
- cnudns.cines.fr

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?

```
nathben97@nathben97-VirtualBox:~$ nslookup univ-am.fr mail.yahoo.com  
;; connection timed out; no servers could be reached
```

```
nathben97@nathben97-VirtualBox:~$ █
```

Connection timed out no servers could be reached



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

UDP

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

- Source port :10923
- Destination port :53

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?

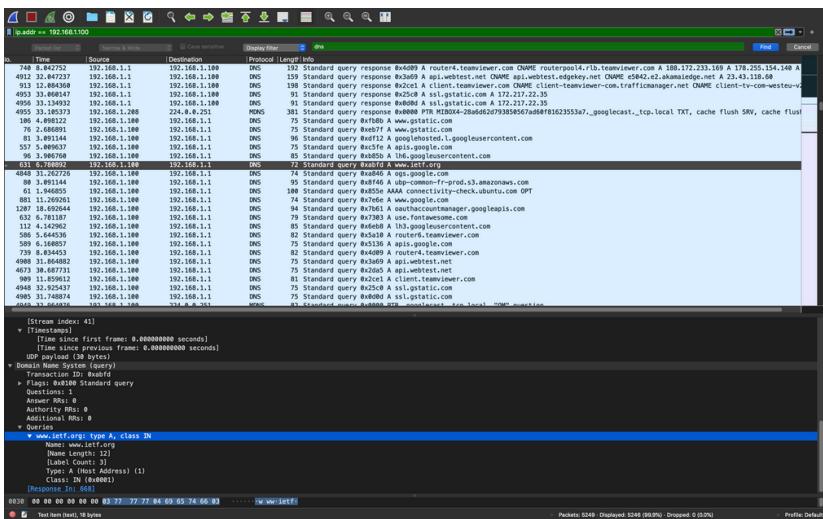
- Source :192.168.1.100
- Destination :192.168.1.1

```
status: inactive
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether 88:e9:fe:85:51:4b
    inet6 fe80::1ca9:cd24:91e4:6f82%en0 prefixlen 64 secured scopeid 0x6
        inet 192.168.1.100 netmask 0xffffffff broadcast 192.168.1.255
            nd6 options=201<PERFORMNUD,DAD>
            media: autoselect
            status: active
```

The MacOs (ipconfig /all) is "ifconfig" the inet show us that the destination feet with our DNS answer 192.168.100

7.Examine the DNS query message.

What “Type” of DNS query is it? Does the query message contain any “answers”?



Standard Query ;
Type of DNS Query : A;
no answer.

8. Examine the DNS response message.

How many “answers” are provided?

What do each of these answers contain?

The screenshot shows a Wireshark capture of a DNS response message. The packet list pane displays several DNS responses (labeled 'Answers') for various queries. The details pane shows the structure of one answer:

- Name: www.ietf.org
- Type: CNAME
- Class: IN
- TTL: 3600
- Data: ietf.org

The packet details and bytes panes show the raw DNS message structure, including the header and the multiple answers section.

Answers :

3 answers contains :

(name, type, class, time to live, data
,length ,adress)

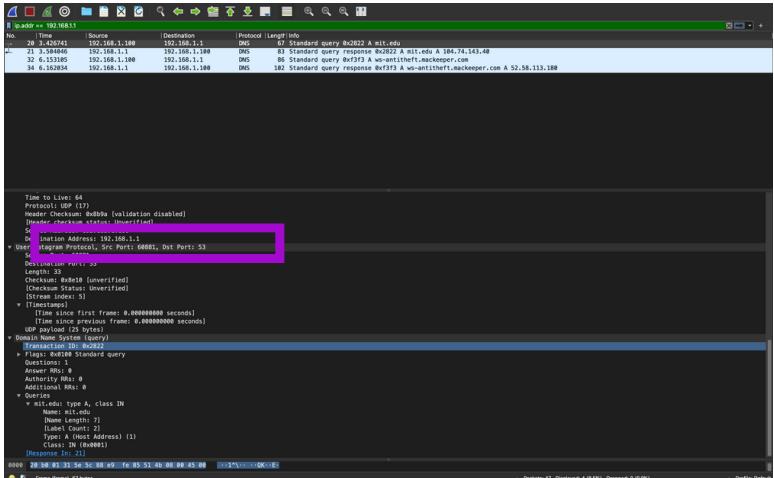
9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

Answer : adresse of provided by the DNS server of ietf.org is 104.16.44.99 as seen in the last screenshot

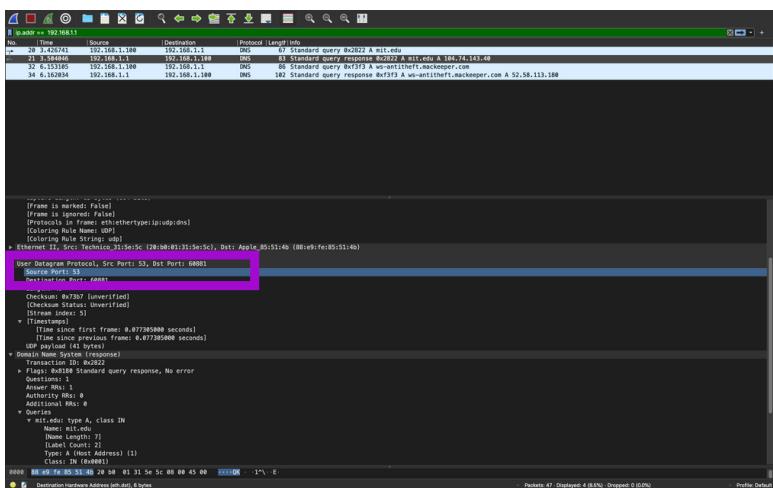
10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

All the images coming from ietf.org so no need to use a new DNS queries

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

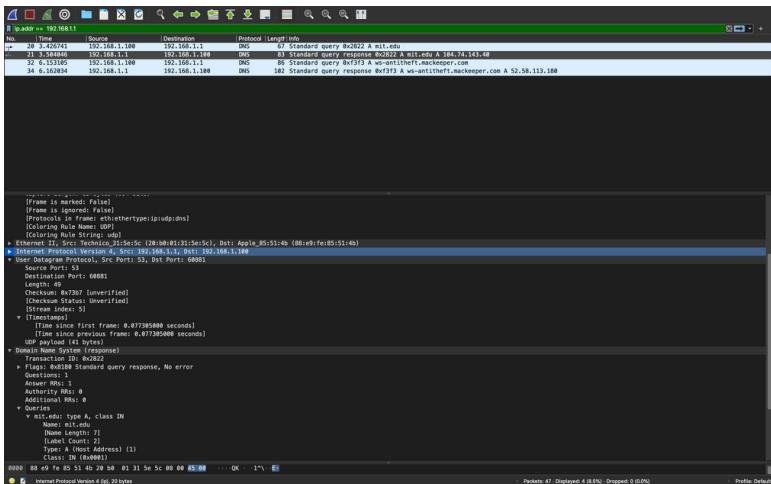


Request port 53



Answer port 53

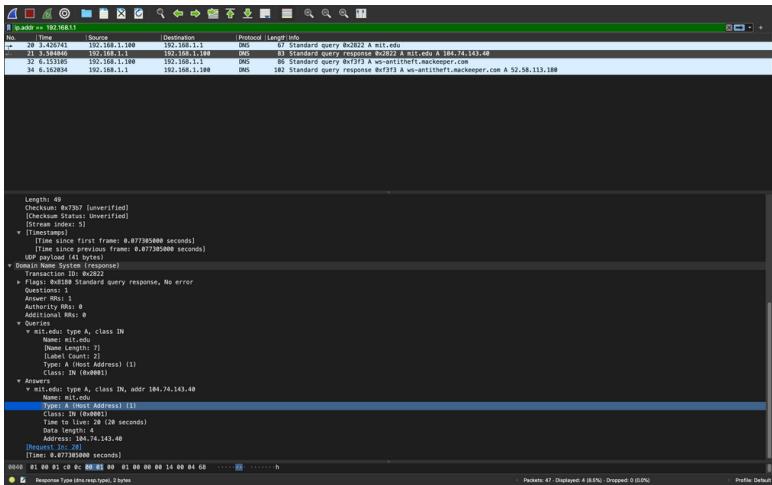
12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?



Destination is 192.168.1.100 its my Dns default ip as seen in the ifconfig screenshot

```
status: inactive
: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
options=400<CHANNEL_ID>
ether 88:e9:fe:85:51:4b
inet6 fe80::1ca9:c2d4:91e4:6f82%en0 prefixlen 64 secured scopeid 0x6
inet 192.168.1.100 netmask 0xffffffff broadcast 192.168.1.255
nd6 options=201<PERFORMNUD,DAD>
media: autoselect
status: active
```

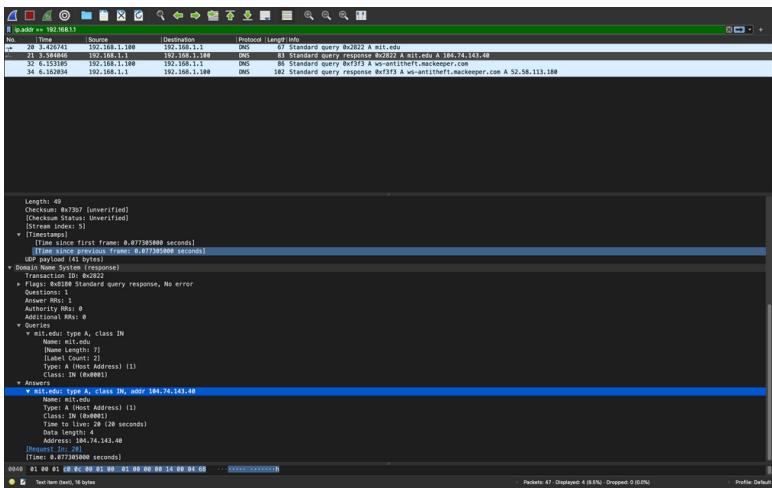
13. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?



No answer /DNS type :A

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

15.ScreenShot

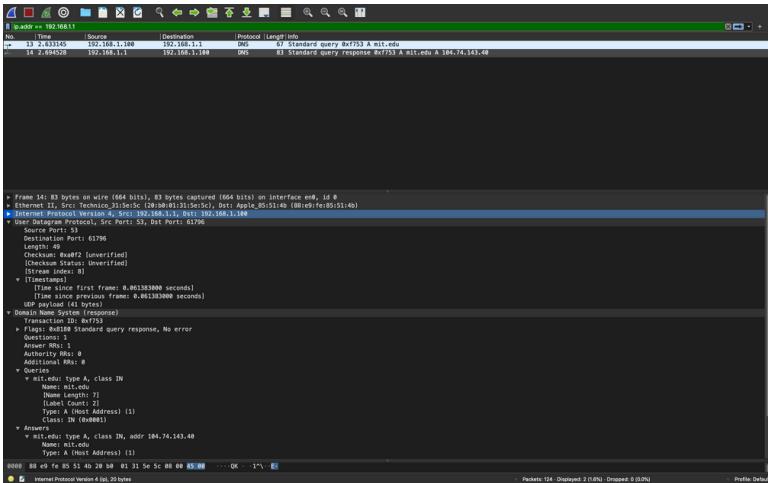


Answers :

1 answers contains :

(name, type, class, time to live, data ,length ,adress)

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



Destination is 192.168.1.100 its my Dns default ip as seen in the ifconfig screenshot

```
status: inactive
: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
  options=400<CHANNEL_IO>
  ether 88:e9:fe:85:51:4b
  inet6 fe80::1ca9:cd24:91e4:6f82%en0 prefixlen 64 secured scopeid 0x6
    inet 192.168.1.100 netmask 0xffffffff broadcast 192.168.1.255
      nd6 options=201<PERFORMNUD,DAD>
      media: autoselect
      status: active
```

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

The screenshot shows a network traffic capture in Wireshark. The top status bar indicates the interface is 'ip.addr == 192.168.1.1'. The packet list shows two DNS frames:

- Frame 13: A DNS query from 192.168.1.100 to 192.168.1.1 (mit.edu) with Transaction ID 0x7f53, type Standard query, and class IN.
- Frame 14: A DNS response from 192.168.1.100 to 192.168.1.100 (mit.edu) with Transaction ID 0x7f53, type Standard query response, and class IN.

The details and bytes panes for frame 14 are expanded, showing the DNS message structure. The DNS header includes fields like QDCount (1), AnCount (0), and ARCount (0). The single answer resource record (RR) has a name of 'mit.edu' (length 7), a type of 'A (Host Address)' (1), and a class of 'IN' (4). The data length is 20 bytes, and the TTL is 20 seconds. The hex and ASCII panes show the raw bytes of the DNS message, starting with 0000 88 e9 fe 85 51 4b 29 b6 81 31 5e 5c 80 80 85 80 ... OK .. 1% ..

Answer: Type A query, and no answer

```

nathanaelbenichou — bash — 80x22
Q Rechercher
Address: 104.74.143.40

MacBook-Pro-de-Nathanael:~ nathanaelbenichou$ nslookup mit.edu
Server:      192.168.1.1
Address:      192.168.1.1#53

Non-authoritative answer:
Name:  mit.edu
Address: 104.74.143.40

MacBook-Pro-de-Nathanael:~ nathanaelbenichou$ nslookup mit.edu
Server:      192.168.1.1
Address:      192.168.1.1#53

Non-authoritative answer:
Name:  mit.edu
Address: 104.74.143.40

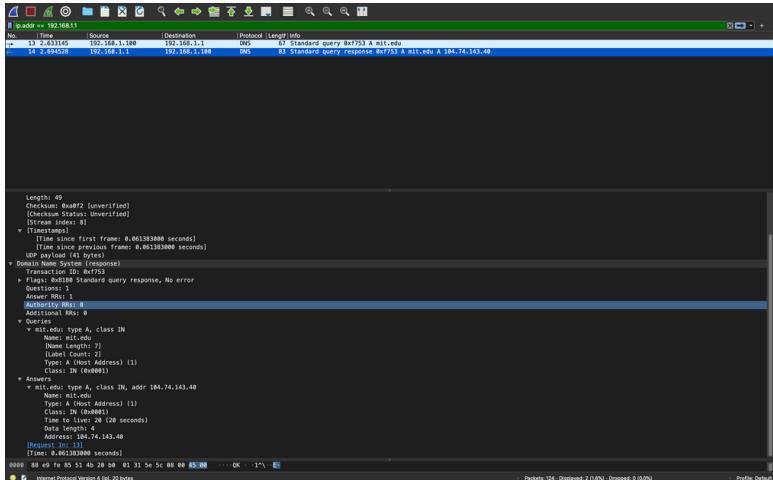
MacBook-Pro-de-Nathanael:~ nathanaelbenichou$ nslookup -type=NS mit.edu
;; connection timed out; no servers could be reached

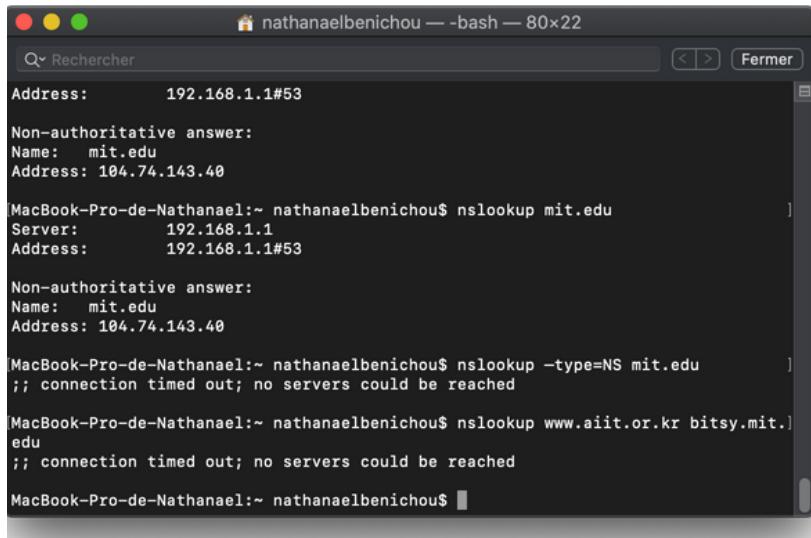
MacBook-Pro-de-Nathanael:~ nathanaelbenichou$ █

```

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?

19. Provide a screenshot.





nathanaelbenichou — bash — 80x22

Q Rechercher Fermer

```
Address: 192.168.1.1#53
Non-authoritative answer:
Name: mit.edu
Address: 104.74.143.40

MacBook-Pro-de-Nathanael:~ nathanaelbenichou$ nslookup mit.edu
Server: 192.168.1.1
Address: 192.168.1.1#53

Non-authoritative answer:
Name: mit.edu
Address: 104.74.143.40

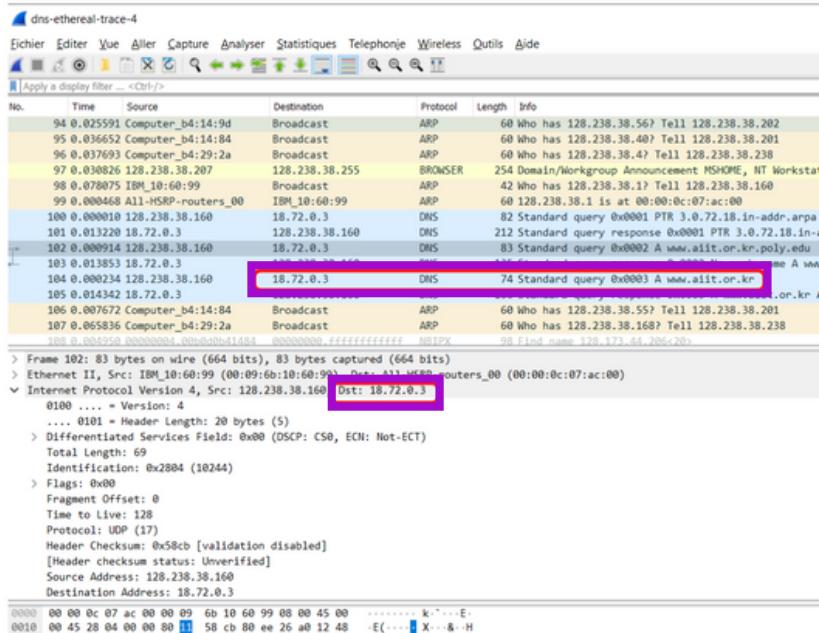
MacBook-Pro-de-Nathanael:~ nathanaelbenichou$ nslookup -type=NS mit.edu
;; connection timed out; no servers could be reached

MacBook-Pro-de-Nathanael:~ nathanaelbenichou$ nslookup www.aiit.or.kr bitsy.mit.edu
;; connection timed out; no servers could be reached

MacBook-Pro-de-Nathanael:~ nathanaelbenichou$
```

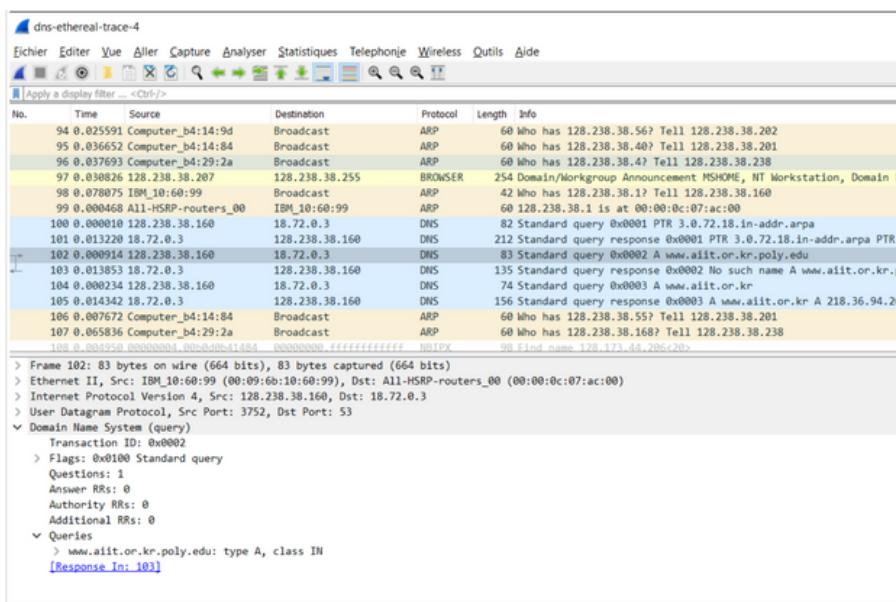
Doesn't work so i used the given pdf in
this case

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: DNS send to 18.72.0.3
the IP address of the wait response sender.

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



Answer: Type of DNS : A
Standard query
no answer

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

23. Provide a Screenshot:

The screenshot shows a Wireshark capture titled "dns-ethereal-trace-4". The packet list pane displays several network frames. Frame 103 is highlighted in yellow and shows a DNS query from host 18.72.0.3 to port 53, asking for the A record of www.alit.or.kr. The DNS response (Frame 135) is also highlighted in yellow, indicating a standard query response with transaction ID 0x0002, flags 0x08583, and a "No such name" error code. The details and bytes panes show the DNS message structure, including the question and answer sections.

```
> Frame 103: 135 bytes on wire (1080 bits), 135 bytes captured (1080 bits)
> Ethernet II, Src: Cisco_83:e4:54 (00:0b: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: 3752
    Transaction ID: 0x0002
    Flags: 0x08583 Standard query response, No such name
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 0
    Queries
        > www.alit.or.kr.poly.edu: type A, class IN
    Authoritative nameservers
        [Request In: 102]
        [Time: 0.013853000 seconds]
0000  00 09 6b 10 60 99 00 b0  8e 83 e4 54 08 00 45 00  ..k....T.E...
0010  00 79 b5 42 40 00 f1 11  1a 58 12 48 00 03 88 ee  .v.BB...X.H....
```

Answer: Type of DNS : A
Standard query
no answer