Project - 2 - Introduction to Computer Networks

© 李浩东 3190104890
© 徐浩然 3190104868
2021年4月16日

Project - 2 - Introduction to Computer Networks
- nslookup
  - Run `nslookup` to obtain the IP address of a Web server in Asia
  - Run `nslookup` to determine the authoritative DNS servers for a university inEurope.
  - Run `nslookup` so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail.
    - Is this your expected result?
    - How to obtain the “authoritative” answer to this query?
- ipconfig & Tracing DNS with Wireshark
  - Locate the DNS query and response messages. Are they sent over UDP or TCP?
  - What is the destination port for the DNS query message? What is the source port of DNS response message?
  - 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?
  - Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
  - Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?
  - 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?
  - This web page contains images. Before retrieving each image, does your host issue new DNS queries?
  - What is the destination port for the DNS query message? What is the source port of DNS response message?
    - ZJU
    - MIT
  - To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
    - ZJU
    - MIT
  - Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
    - ZJU
    - MIT
  - Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?
    - ZJU
    - MIT
  - To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
  - Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
  - Examine the DNS response message. What MIT name servers does the response message provide? Does this response message also provide the IP addresses of all the MIT name servers?

nslookup

Run `nslookup` to obtain the IP address of a Web server in Asia

- for `www.zju.edu.cn`
  - the Ip address is `10.203.6.122`
- for `www.tsinghua.edu.cn`
  - the IP address is `166.111.4.100`
- the command screenshots are below

```
C:\Users\87236>nslookup www.zju.edu.cn
服务器:  dns1.zju.edu.cn
Address:  10.10.0.21

名称:    www.zju.edu.cn
Address:  10.203.6.122


C:\Users\87236>nslookup -type=NS zju.edu.cn
服务器:  dns1.zju.edu.cn
Address:  10.10.0.21

zju.edu.cn      nameserver = dns1.zju.edu.cn
dns1.zju.edu.cn internet address = 10.10.0.38


C:\Users\87236>nslookup www.tsinghua.edu.cn
服务器:  dns1.zju.edu.cn
Address:  10.10.0.21

非权威应答:
名称:    www.tsinghua.edu.cn
Addresses:  2402:f000:1:404:166:111:4:100
          166.111.4.100


C:\Users\87236>nslookup -type=NS tsinghua.edu.cn
服务器:  dns1.zju.edu.cn
Address:  10.10.0.21

非权威应答:
tsinghua.edu.cn nameserver = ns2.cuhk.edu.hk
tsinghua.edu.cn nameserver = dns.tsinghua.edu.cn
tsinghua.edu.cn nameserver = dns2.tsinghua.edu.cn
tsinghua.edu.cn nameserver = dns2.edu.cn

dns.tsinghua.edu.cn     internet address = 166.111.8.30
dns2.edu.cn     internet address = 202.112.0.13
dns2.tsinghua.edu.cn    internet address = 166.111.8.31
ns2.cuhk.edu.hk AAAA IPv6 address = 2405:3000:3:6::15
dns2.edu.cn     AAAA IPv6 address = 2001:da8:1:100::13
```

Run `nslookup` to determine the authoritative DNS servers for a university inEurope.

- for `www.imperial.ac.uk`
- we could find the Non-authoritative answers are

```
imperial.ac.uk  nameserver = ns0.ic.ac.uk
imperial.ac.uk  nameserver = auth0.dns.cam.ac.uk
imperial.ac.uk  nameserver = ns1.ic.ac.uk
imperial.ac.uk  nameserver = ns2.ic.ac.uk
```

- and the Authoritative answers are

```
ns0.ic.ac.uk    internet address = 155.198.142.80
ns1.ic.ac.uk    internet address = 155.198.142.81
ns2.ic.ac.uk    internet address = 155.198.142.82
auth0.dns.cam.ac.uk     internet address = 131.111.8.37
ns0.ic.ac.uk    AAAA IPv6 address = 2a0c:5bc0:4:1::80
ns1.ic.ac.uk    AAAA IPv6 address = 2a0c:5bc0:4:1::81
ns2.ic.ac.uk    AAAA IPv6 address = 2a0c:5bc0:4:1::82
auth0.dns.cam.ac.uk     AAAA IPv6 address = 2001:630:212:8::d:a0
```

- note that there are multiple authoritative servers. and the response we got back was from acached record. inorfder to confirm the authoritative `DNS` server, we perform the same `DNS` query ofone of the servers that can provide authoritative answers
  - the server is `ns0.ic.ac.uk`
  - the address of the server is `2a0c:5bc0:4:1::80`
- the command window is below

```
C:\Users\87236>nslookup www.imperial.ac.uk
服务器:  dns1.zju.edu.cn
Address:  10.10.0.21

非权威应答:
名称:    wrpwww.cc.gslb.ic.ac.uk
Addresses:  2001:630:12:600:1:2:0:172
          146.179.40.148
Aliases:  www.imperial.ac.uk


C:\Users\87236>nslookup -type=NS imperial.ac.uk
服务器:  dns1.zju.edu.cn
Address:  10.10.0.21

非权威应答:
imperial.ac.uk  nameserver = ns0.ic.ac.uk
imperial.ac.uk  nameserver = auth0.dns.cam.ac.uk
imperial.ac.uk  nameserver = ns1.ic.ac.uk
imperial.ac.uk  nameserver = ns2.ic.ac.uk

ns0.ic.ac.uk    internet address = 155.198.142.80
ns1.ic.ac.uk    internet address = 155.198.142.81
ns2.ic.ac.uk    internet address = 155.198.142.82
```

```
auth0.dns.cam.ac.uk     internet address = 131.111.8.37
ns0.ic.ac.uk    AAAA IPv6 address = 2a0c:5bc0:4:1::80
ns1.ic.ac.uk    AAAA IPv6 address = 2a0c:5bc0:4:1::81
ns2.ic.ac.uk    AAAA IPv6 address = 2a0c:5bc0:4:1::82
auth0.dns.cam.ac.uk     AAAA IPv6 address = 2001:630:212:8::d:a0


C:\Users\87236>nslookup -type=NS imperial.ac.uk ns0.ic.ac.uk
服务器:  ns0.ic.ac.uk
Address:  2a0c:5bc0:4:1::80

imperial.ac.uk  nameserver = ns2.ic.ac.uk
imperial.ac.uk  nameserver = ns1.ic.ac.uk
imperial.ac.uk  nameserver = ns0.ic.ac.uk
imperial.ac.uk  nameserver = auth0.dns.cam.ac.uk
ns0.ic.ac.uk    AAAA IPv6 address = 2a0c:5bc0:4:1::80
ns1.ic.ac.uk    AAAA IPv6 address = 2a0c:5bc0:4:1::81
ns2.ic.ac.uk    AAAA IPv6 address = 2a0c:5bc0:4:1::82
auth0.dns.cam.ac.uk     AAAA IPv6 address = 2001:630:212:8::d:a0
ns0.ic.ac.uk    internet address = 155.198.142.80
ns1.ic.ac.uk    internet address = 155.198.142.81
ns2.ic.ac.uk    internet address = 155.198.142.82
auth0.dns.cam.ac.uk     internet address = 131.111.8.37
```

Run `nslookup` so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail.

Is this your expected result?

we have tried all `DNS` servers in Question-2 but none of them queried for the mail servers for Yahoo! mail. the command window is below

```
C:\Users\87236>nslookup mail.yahoo.com ns0.ic.ac.uk
服务器:  ns0.ic.ac.uk
Address:  2a0c:5bc0:4:1::80

*** ns0.ic.ac.uk 找不到 mail.yahoo.com: Query refused

C:\Users\87236>nslookup mail.yahoo.com ns1.ic.ac.uk
服务器:  ns1.ic.ac.uk
Address:  2a0c:5bc0:4:1::81

*** ns1.ic.ac.uk 找不到 mail.yahoo.com: Query refused

C:\Users\87236>nslookup mail.yahoo.com ns2.ic.ac.uk
服务器:  ns2.ic.ac.uk
Address:  2a0c:5bc0:4:1::82

*** ns2.ic.ac.uk 找不到 mail.yahoo.com: Query refused

C:\Users\87236>nslookup mail.yahoo.com auth0.dns.cam.ac.uk
服务器:  auth0.dns.cam.ac.uk
Address:  2001:630:212:8::d:a0

*** auth0.dns.cam.ac.uk 找不到 mail.yahoo.com: Query refused
```

so we try `www.google.com`, `www.youtube.com` and `www.cam.ac.uk` instead

```
C:\Users\87236>nslookup www.google.com ns0.ic.ac.uk
服务器:  ns0.ic.ac.uk
Address:  2a0c:5bc0:4:1::80

非权威应答:
名称:    www.google.com
Addresses:  2001::6ca0:acd0
          31.13.67.41


C:\Users\87236>nslookup www.youtube.com ns0.ic.ac.uk
服务器:  ns0.ic.ac.uk
Address:  2a0c:5bc0:4:1::80

非权威应答:
名称:    www.youtube.com
Addresses:  2001::c085:4dbf
          179.60.193.9


C:\Users\87236>nslookup www.cam.ac.uk ns0.ic.ac.uk
服务器:  ns0.ic.ac.uk
Address:  2a0c:5bc0:4:1::80

名称:    www.cam.ac.uk
Addresses:  2a05:b400:5:270::80e8:8408
          128.232.132.8
```

but all queries above is Non-authoritative except `www.cam.ac.uk`

How to obtain the “authoritative” answer to this query?

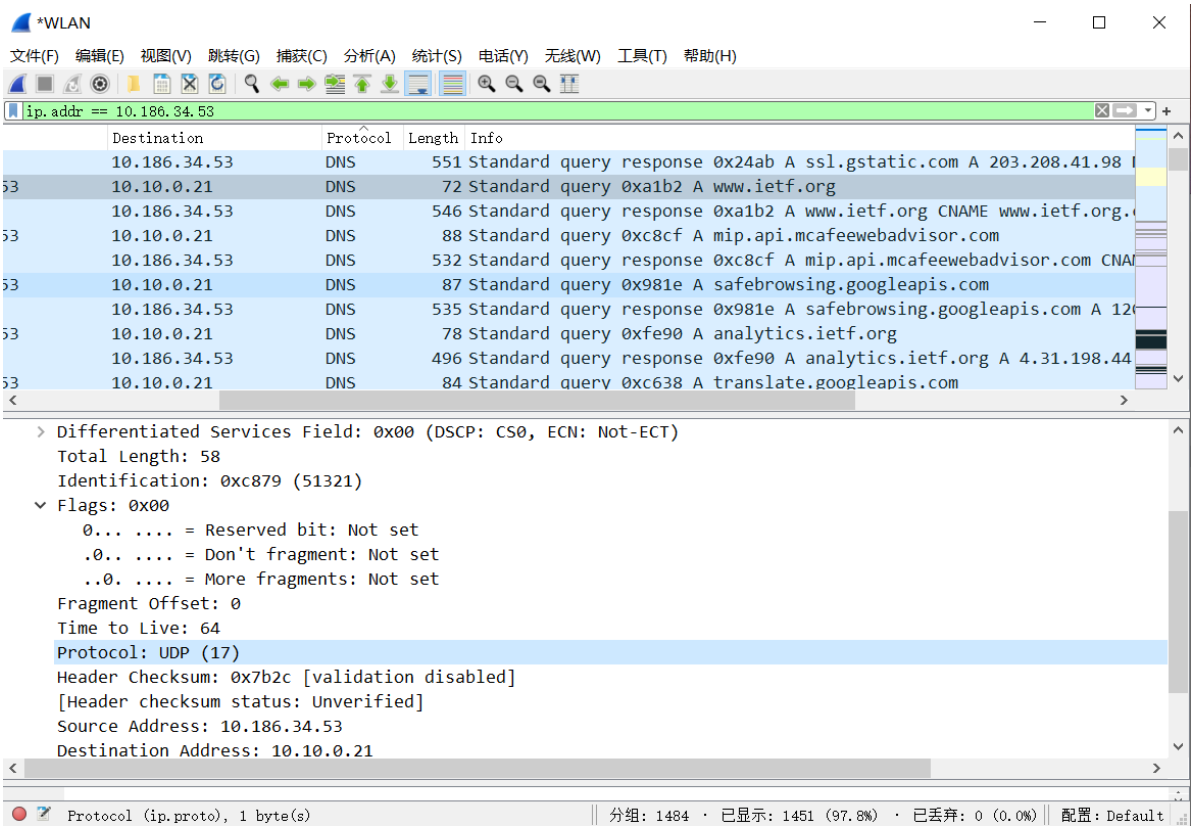
just like we visit `www.cam.ac.uk`, only when the server find the IP address of `www.cam.ac.uk` int its IP list, will we see authoritative response. we take `www.cam.ac.uk` and `www.zju.edu.cn` for example, the command window is below

```
C:\Users\87236>nslookup www.cam.ac.uk
服务器:  dns1.zju.edu.cn
Address:  10.10.0.21

非权威应答:
名称:    www.cam.ac.uk
Addresses:  2a05:b400:5:270::80e8:8408
          128.232.132.8


C:\Users\87236>nslookup www.cam.ac.uk ns0.ic.ac.uk
服务器:  ns0.ic.ac.uk
Address:  2a0c:5bc0:4:1::80

名称:    www.cam.ac.uk
Addresses:  2a05:b400:5:270::80e8:8408
          128.232.132.8
```

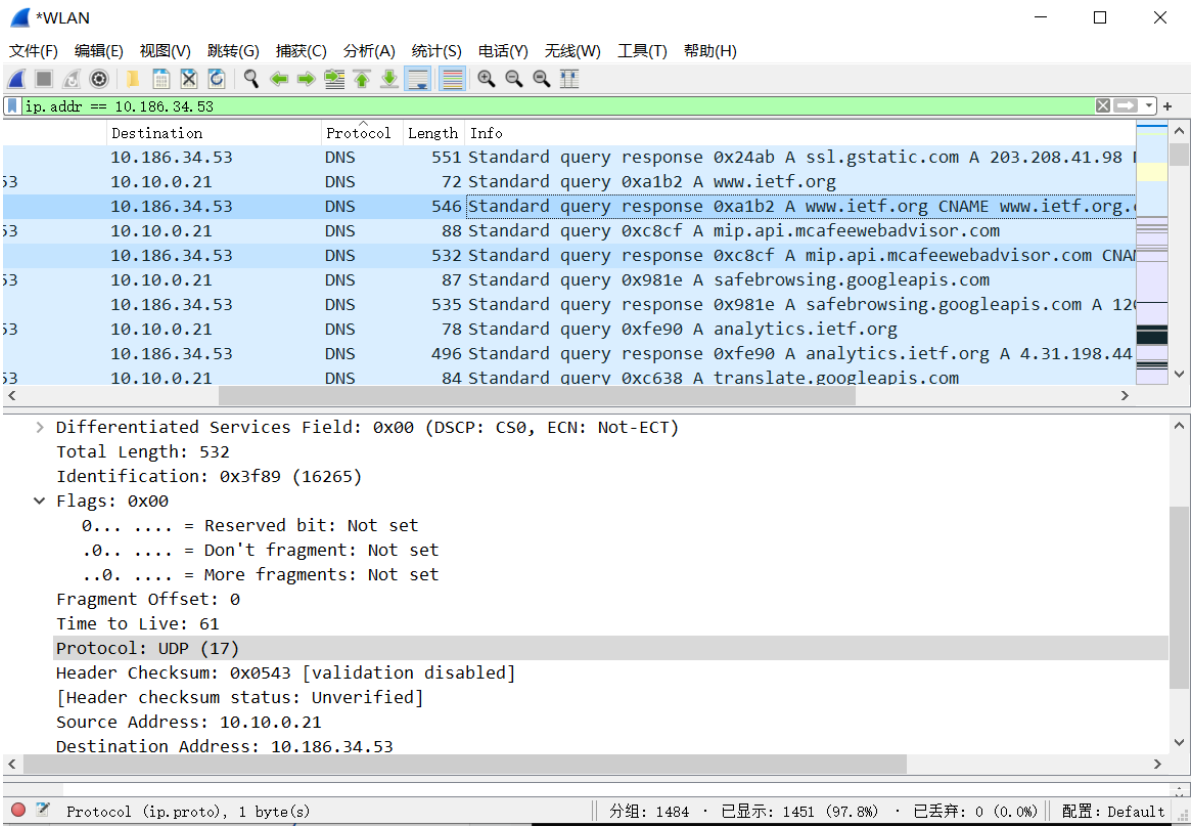
ipconfig & Tracing DNS with Wireshark

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

- Query

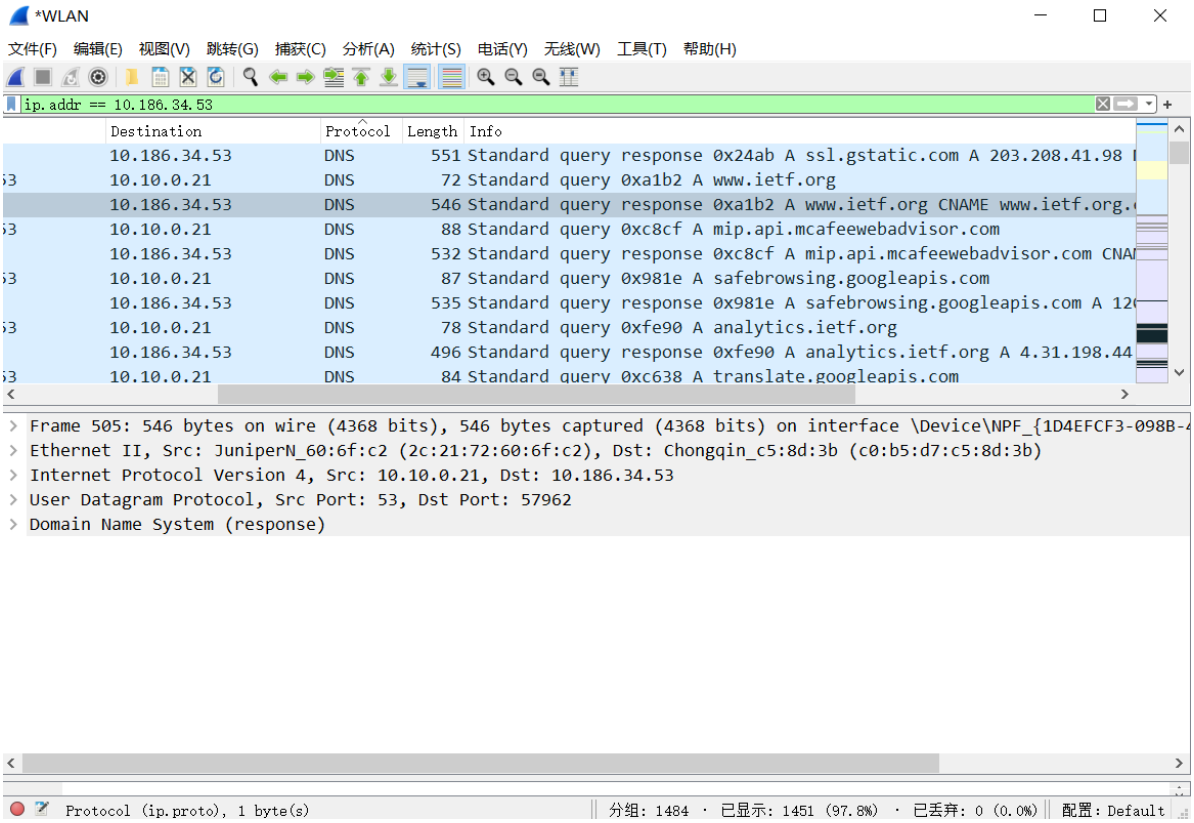


- Response



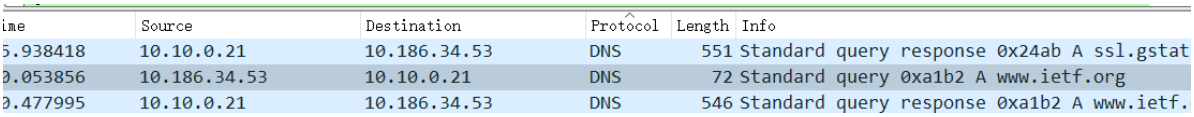
- All use UDP

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

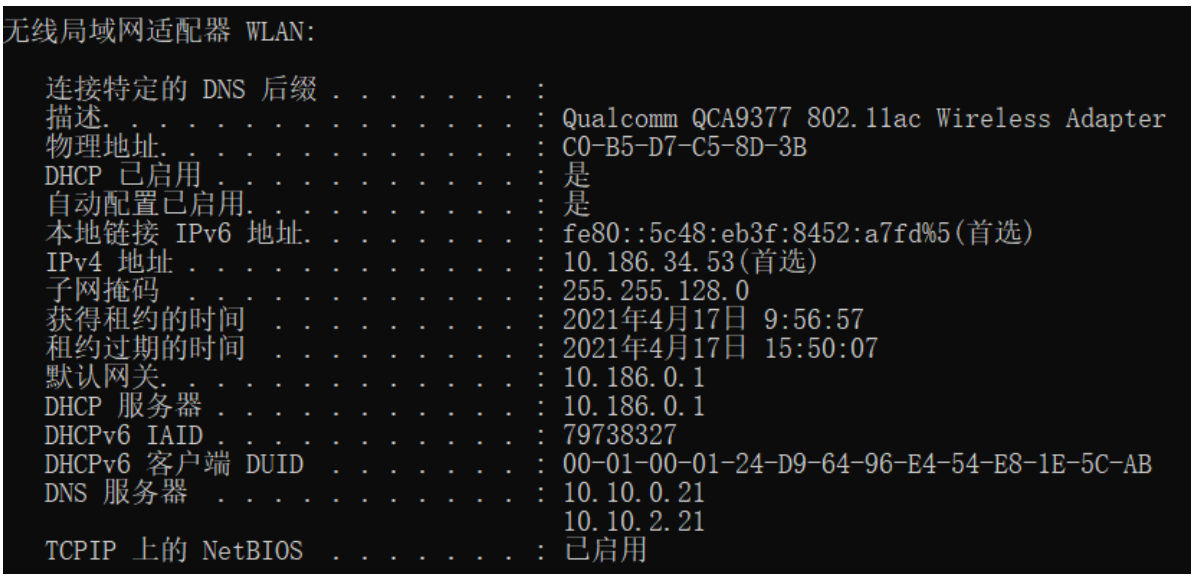


- destination port for the DNS query message:53
- the source port of DNS response message:53

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?

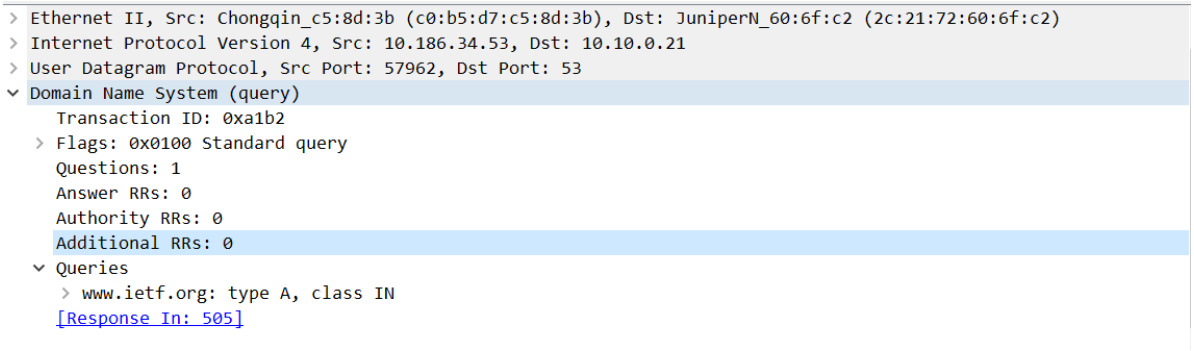


- IP address that the DNS query message sent:10.10.0.21



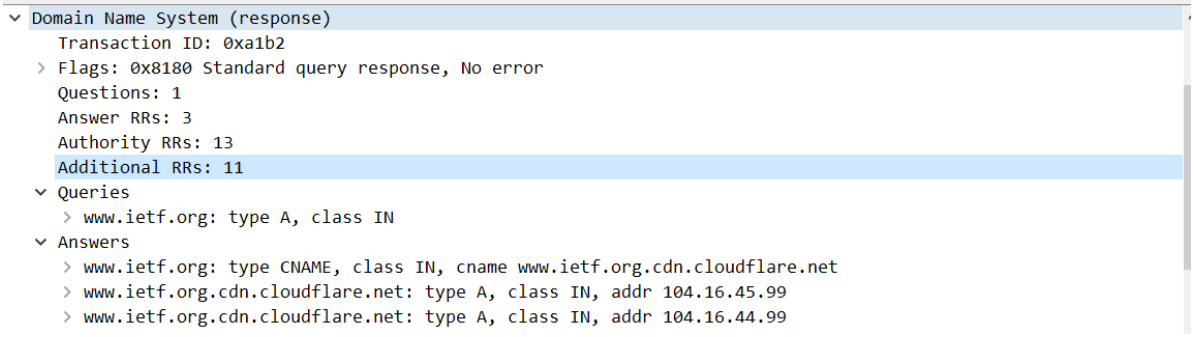
- The IP address of my local DNS server:10.10.0.21
- They are the same.

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



- Type A.
- No answer.

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



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?

- 后续发送的TCP SYN数据包的目的IP地址和DNS响应消息中提供的源IP地址相对应。

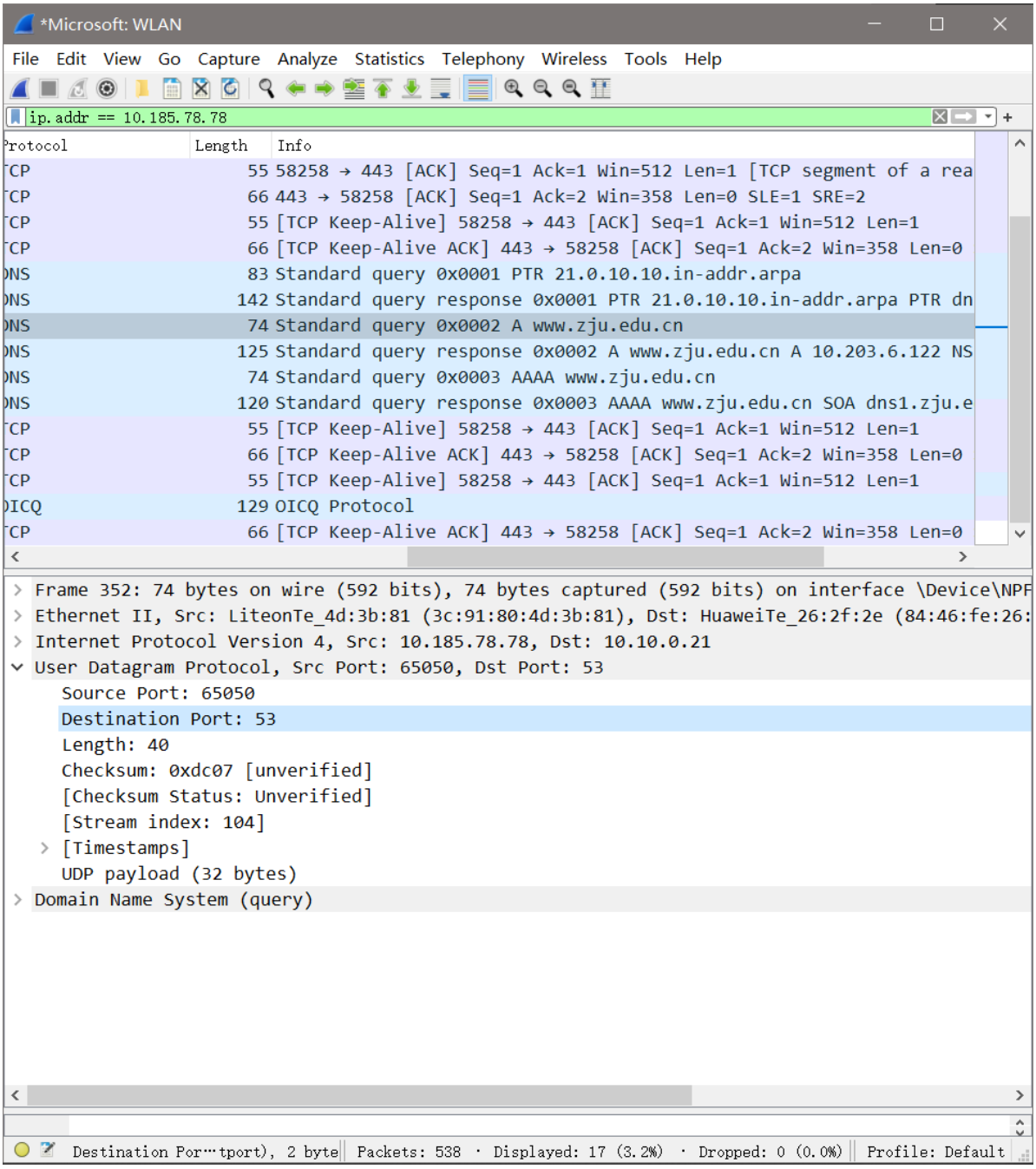
This web page contains images. Before retrieving each image, does your host issue new DNS queries?

- 没有，只有部分重新发送新的DNS查询。

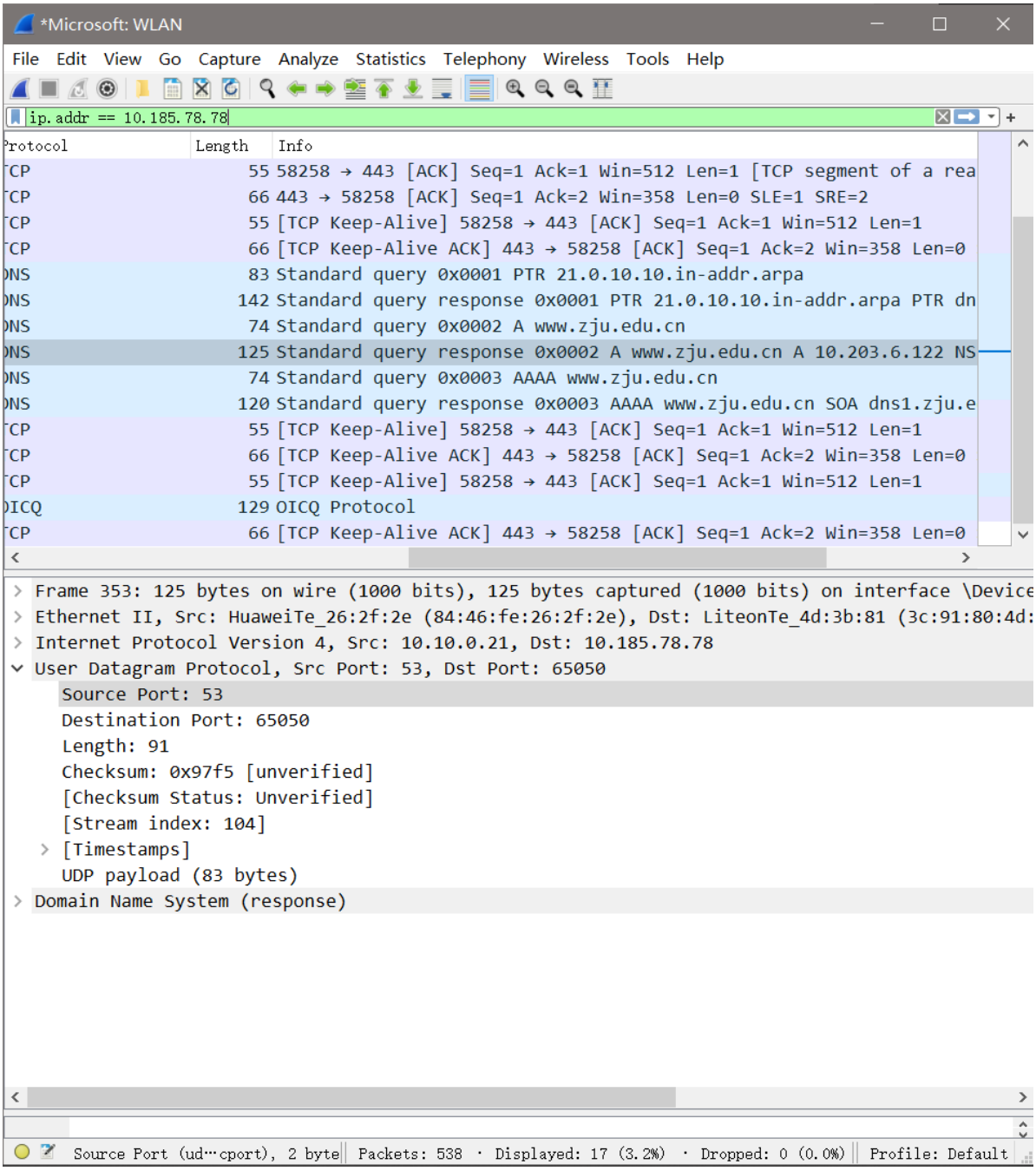
What is the destination port for the DNS query message? What is the source port of DNS response message?

ZJU

- Query



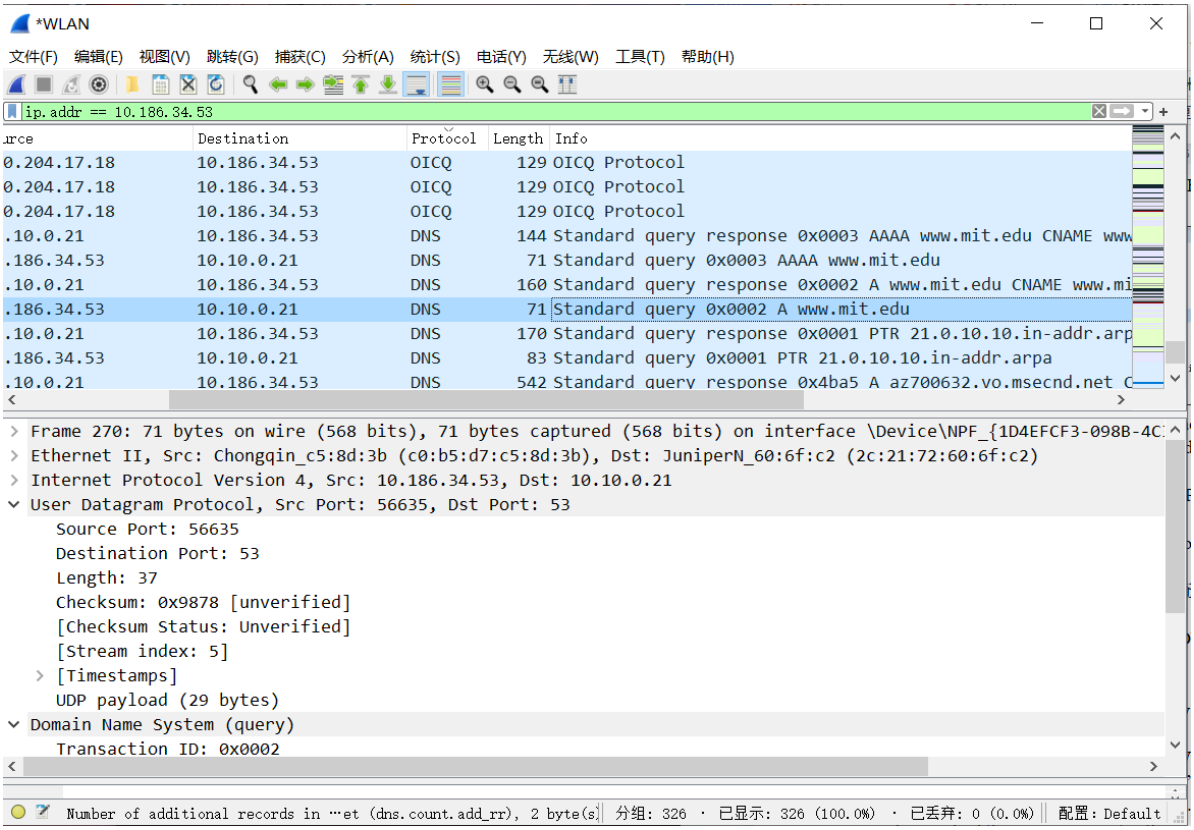
- Response



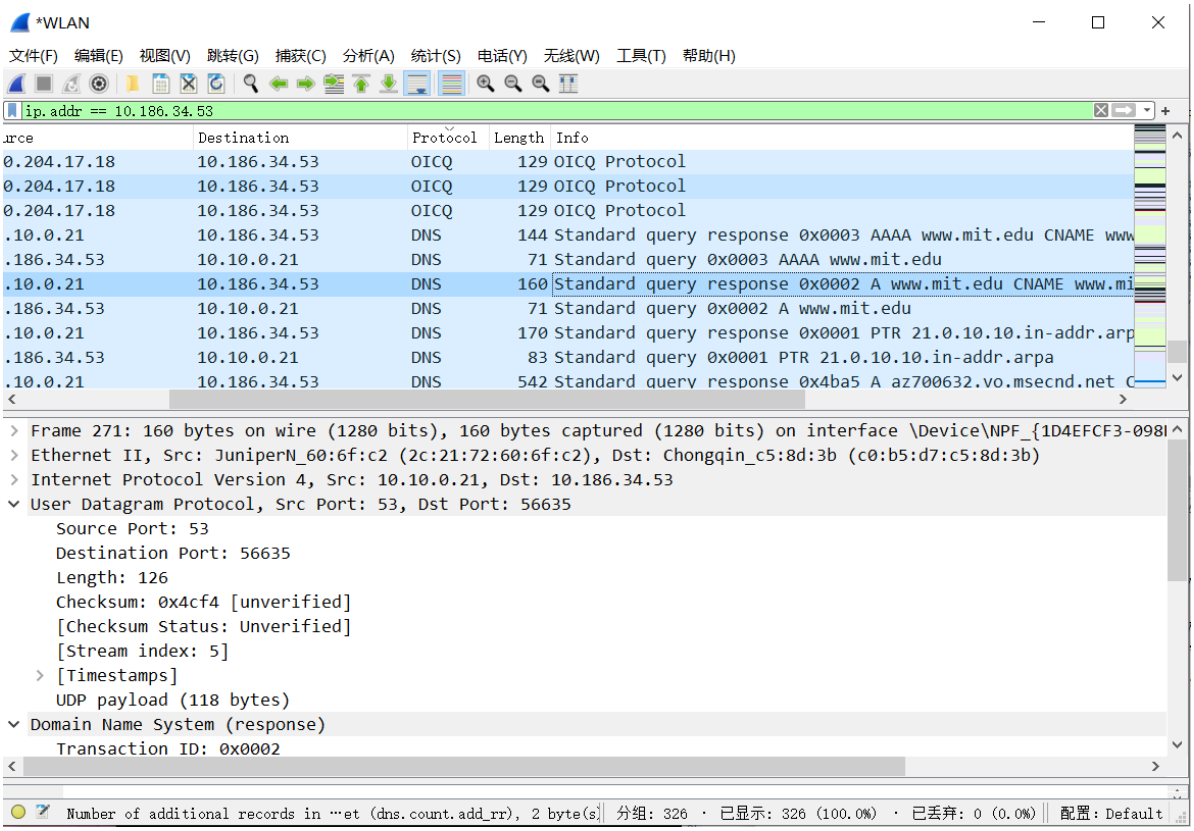
- All is 53

MIT

- Query



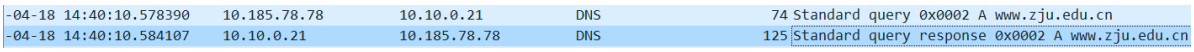
- Response



- All is 53

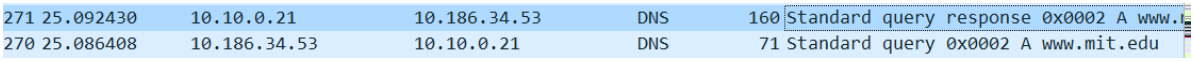
To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

ZJU



- 目标IP地址：10.10.0.21
- 与本地DNS服务器一致

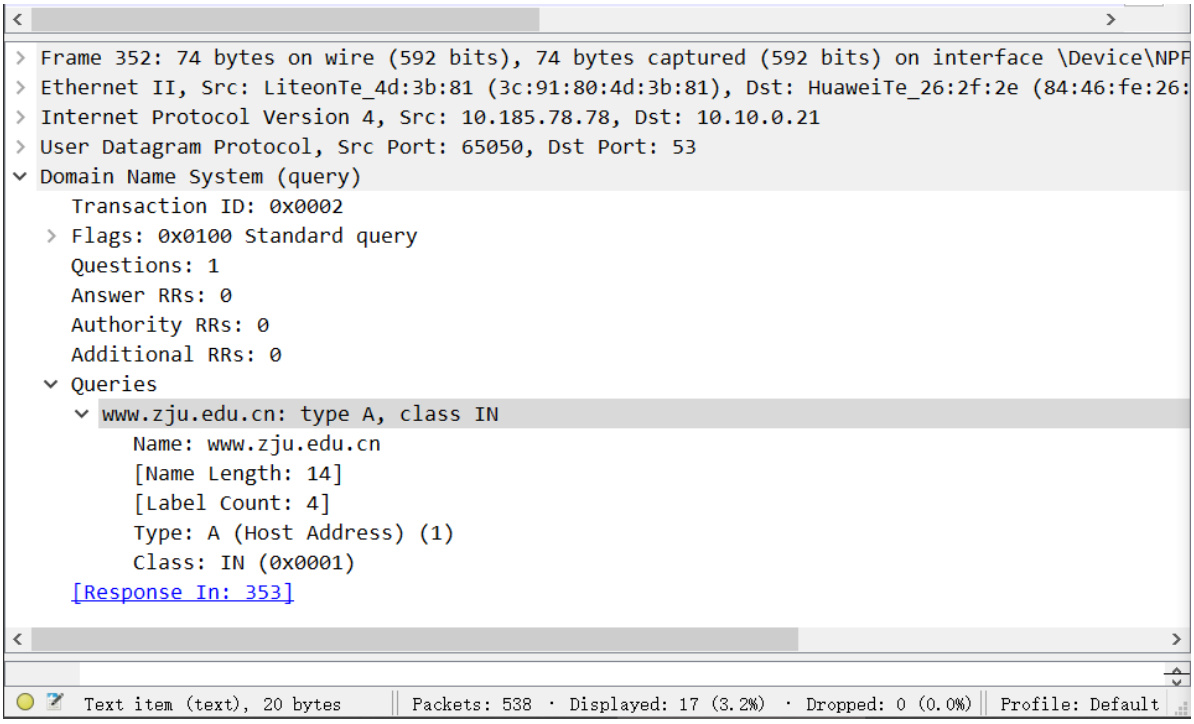
MIT



- 目标IP地址：10.10.0.21
- 与本地DNS服务器一致

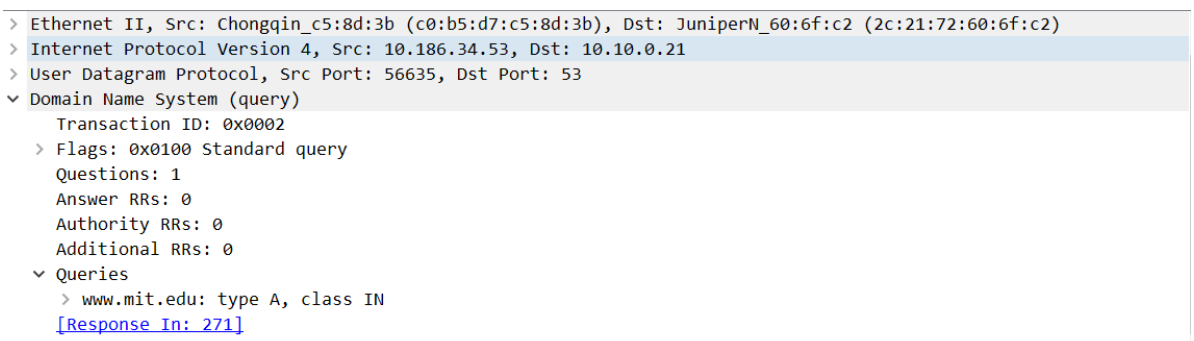
Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

ZJU



- Type A
- No answer

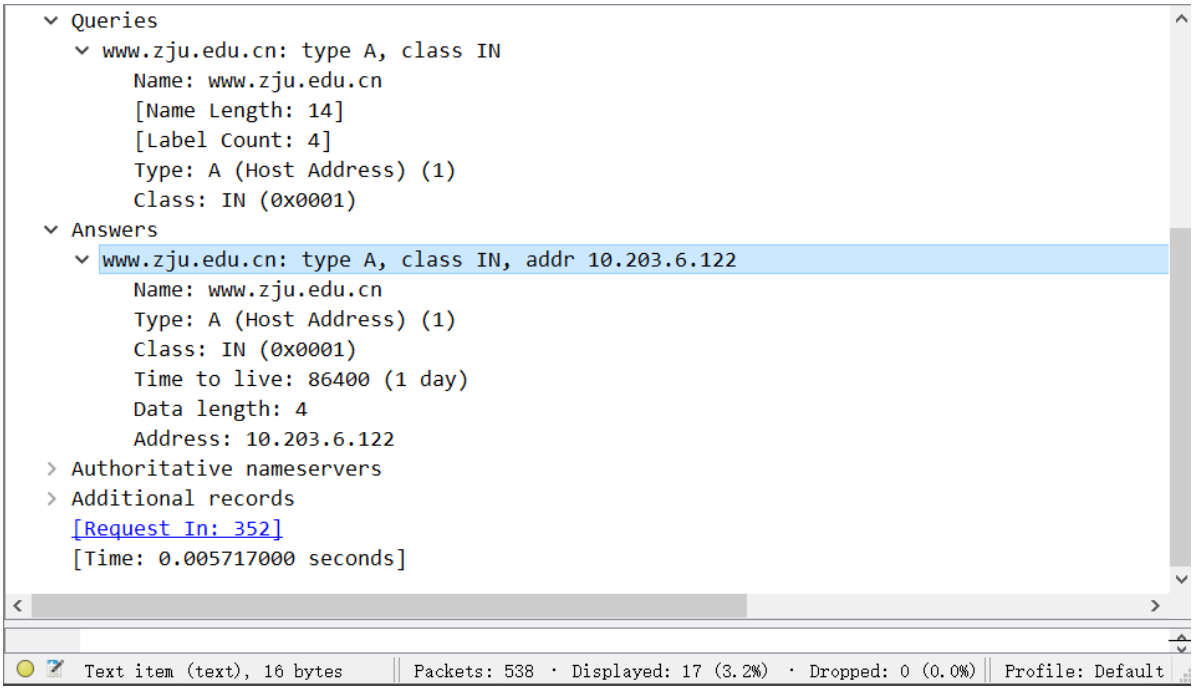
MIT



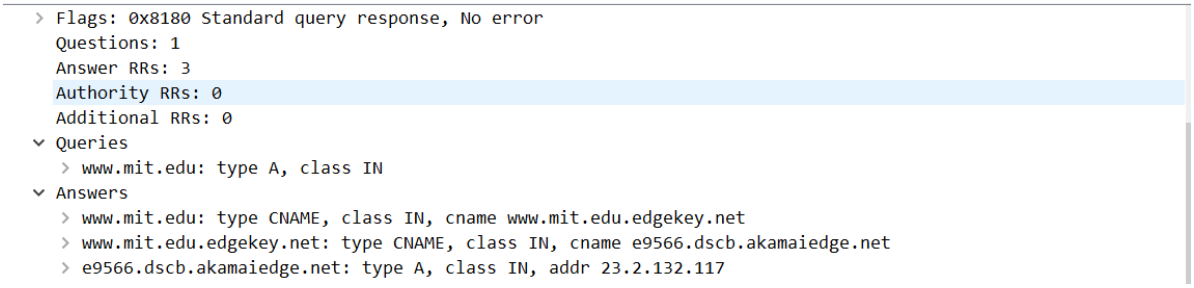
- Type A
- No answer

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

ZJU



MIT



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

Source	Destination	Protocol	Length	Info
10.186.34.53	10.10.0.21	DNS	83	Standard query 0x0001 PTR 21.0.10.10.in-addr.arpa
10.10.0.21	10.186.34.53	DNS	142	Standard query response 0x0001 PTR 21.0.10.10.in-addr.
10.186.34.53	10.10.0.21	DNS	67	Standard query 0x0002 NS mit.edu
10.10.0.21	10.186.34.53	DNS	234	Standard query response 0x0002 NS mit.edu NS asia2.aka

- 目标IP地址：10.10.0.21
- 是本地DNS服务器地址

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: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > mit.edu: type NS, class IN
    [Response In: 19]
```

- Type NS
- No answer

Examine the DNS response message. What MIT name servers does the response message provide? Does this response message also provide the IP addresses of all the MIT name servers?

```
v Queries
  > mit.edu: type NS, class IN
v Answers
  > mit.edu: type NS, class IN, ns asia2.akam.net
  > mit.edu: type NS, class IN, ns use2.akam.net
  > mit.edu: type NS, class IN, ns usw2.akam.net
  > mit.edu: type NS, class IN, ns ns1-173.akam.net
  > mit.edu: type NS, class IN, ns eur5.akam.net
  > mit.edu: type NS, class IN, ns asia1.akam.net
  > mit.edu: type NS, class IN, ns use5.akam.net
  > mit.edu: type NS, class IN, ns ns1-37.akam.net
  [Request In: 18]
  [Time: 0.046111000 seconds]
```