计算机网络 DNS实验

PB20000180 刘良宇

1. nslookup

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

```
liu@liu-Laptop ~> nslookup ustc.edu.cn
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   ustc.edu.cn
Address: 202.38.64.246
Name:   ustc.edu.cn
Address: 2001:da8:d800:642::248
```

   - IPv4: `202.38.64.246`
   - IPv6: `2001:da8:d800:642::248`

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

```
liu@liu-Laptop ~> nslookup -type=NS cam.ac.uk
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
cam.ac.uk       nameserver = ns3.mythic-beasts.com.
cam.ac.uk       nameserver = auth0.dns.cam.ac.uk.
cam.ac.uk       nameserver = ns1.mythic-beasts.com.
cam.ac.uk       nameserver = ns2.ic.ac.uk.
cam.ac.uk       nameserver = dns0.eng.cam.ac.uk.
cam.ac.uk       nameserver = dns0.cl.cam.ac.uk.

Authoritative answers can be found from:
ns3.mythic-beasts.com   internet address = 185.24.221.32
dns0.cl.cam.ac.uk       internet address = 128.232.0.19
ns1.mythic-beasts.com   internet address = 45.33.127.156
ns2.ic.ac.uk    internet address = 155.198.142.82
dns0.eng.cam.ac.uk      internet address = 129.169.8.8
auth0.dns.cam.ac.uk     internet address = 131.111.8.37
ns3.mythic-beasts.com   has AAAA address 2a02:2770:11:0:21a:4aff:febe:759b
dns0.cl.cam.ac.uk       has AAAA address 2a05:b400:110::d:a0
dns0.cl.cam.ac.uk       has AAAA address 2001:630:212:200::d:a0
ns1.mythic-beasts.com   has AAAA address 2600:3c00:e000:19::1
ns2.ic.ac.uk    has AAAA address 2a0c:5bc0:4:1::82
auth0.dns.cam.ac.uk     has AAAA address 2001:630:212:8::d:a0
```

Authoritative DNS servers can be found in the last block.

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?

```
liu@liu-Laptop ~> nslookup -type=MX mail.yahoo.com 8.8.8.8
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
mail.yahoo.com  canonical name = edge.gycpi.b.yahoodns.net.
```

In fact there is a `CNAME` record for `mail.yahoo.com`

So actual IP:

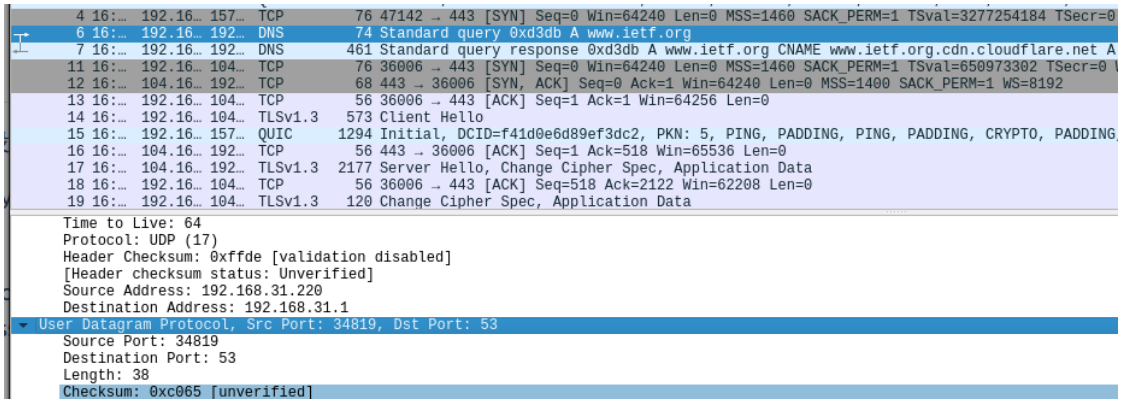
```
liu@liu-Laptop ~> nslookup edge.gycpi.b.yahoodns.net 8.8.8.8
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   edge.gycpi.b.yahoodns.net
Address: 106.10.236.37
Name:   edge.gycpi.b.yahoodns.net
Address: 119.161.10.11
Name:   edge.gycpi.b.yahoodns.net
Address: 106.10.236.40
Name:   edge.gycpi.b.yahoodns.net
Address: 119.161.10.12
Name:   edge.gycpi.b.yahoodns.net
Address: 2406:2000:98:800::e6
Name:   edge.gycpi.b.yahoodns.net
Address: 2406:2000:e4:1604::1000
Name:   edge.gycpi.b.yahoodns.net
Address: 2406:2000:98:800::e5
Name:   edge.gycpi.b.yahoodns.net
Address: 2406:2000:e4:1604::1001
```

(DNS servers in step2 are all unusable, so I pick up `8.8.8.8`)

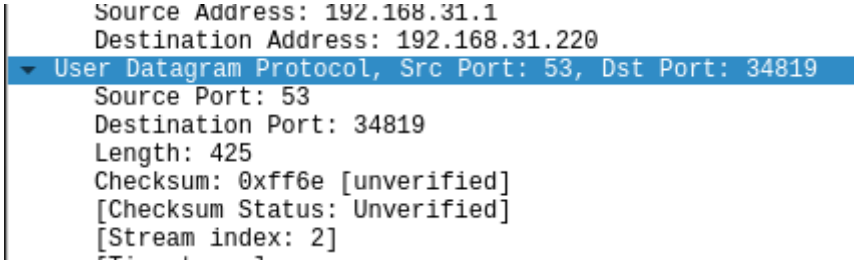
3. Tracing DNS with Wireshark

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



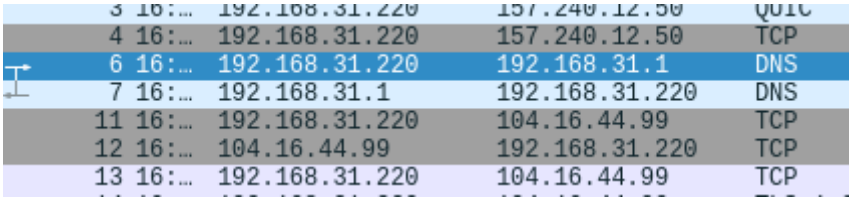
- query: No.6
- response: No.7
- UDP. See below `User Datagram Protocol`

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

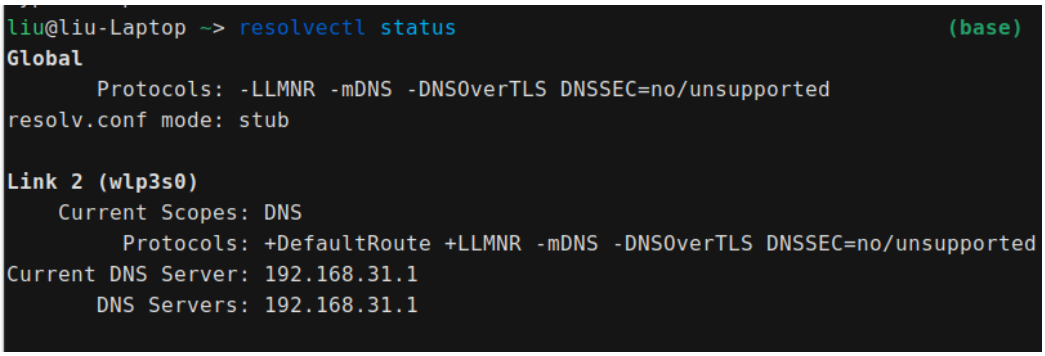


Both 53. See picture in question 4 and above

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?



`192.168.31.1`



`192.168.31.1`

The same. It is actually provided by the router.

7. 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: 0xd3db
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ www.ietf.org: type A, class IN
        Name: www.ietf.org
        [Name Length: 12]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

- Type A
- No

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

```
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
▾ Answers
  ▸ www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
  ▸ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
  ▸ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
▸ Authoritative nameservers
▸ Additional records
```

- 3 answers in total
- CNAME for `www.ietf.org`
- 2 A record for `www.ietf.org.cdn.cloudflare.net` ,

  pointing to different IPv4 addresses

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?

```
     4 16:… 192.168.31.220   157.240.12.50   TCP     76 47142 → 443 [SYN]
     6 16:… 192.168.31.220   192.168.31.1    DNS     74 Standard query 0x
     7 16:… 192.168.31.1     192.168.31.220  DNS    461 Standard query re
    11 16:… 192.168.31.220   104.16.44.99    TCP     76 36006 → 443 [SYN]
    12 16:… 104.16.44.99     192.168.31.220  TCP     68 443 → 36006 [SYN,
    13 16:… 192.168.31.220   104.16.44.99    TCP     56 36006 → 443 [ACK]
```

Yes. `104.16.44.99`

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

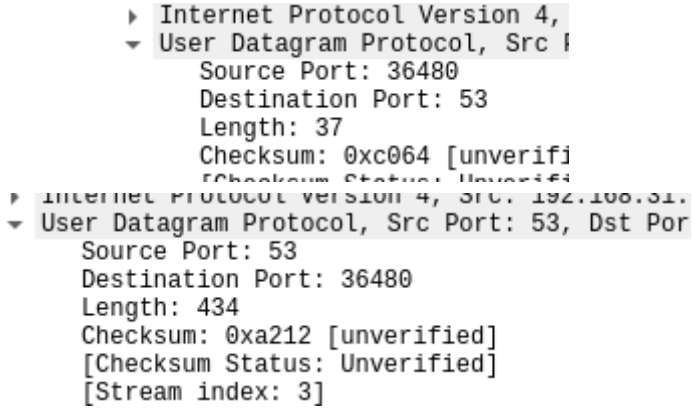
No. Because the DNS query result has been cached.

```
▾ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
    Name: www.ietf.org.cdn.cloudflare.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 900 (15 minutes)
    Data length: 4
    Address: 104.16.45.99
▾ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
    Name: www.ietf.org.cdn.cloudflare.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 900 (15 minutes)
    Data length: 4
    Address: 104.16.44.99
```

TTL is set to 15 minutes

www.mit.edu

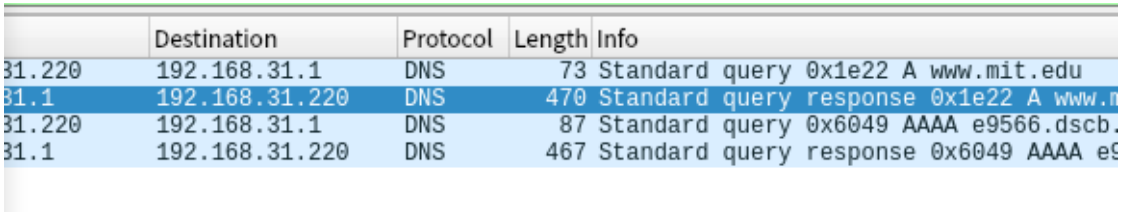
11. What is the destination port for the DNS query message? What is the source port of DNS response message?



Both are 53

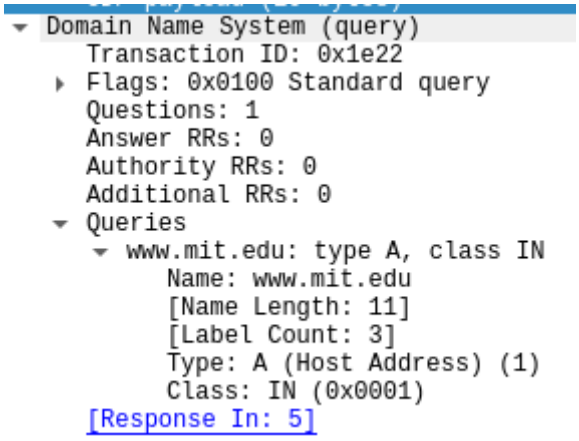
12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

（这里实验指导书应该是过时了，现在这两条都是 DNS 查询记录）



- 192.168.31.1
- Yes

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



- Type A
- No

```
▾ Domain Name System (query)
    Transaction ID: 0x6049
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ e9566.dscb.akamaiedge.net: type AAAA
        Name: e9566.dscb.akamaiedge.net
        [Name Length: 25]
        [Label Count: 4]
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
```

- Type AAAA
- No

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

```
▾ Answers
  ▸ www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
  ▸ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
  ▸ e9566.dscb.akamaiedge.net: type A, class IN, addr 104.71.147.10
```

- 3 answers
- 2 CNAME, eventually points to `e9566.dscb.akamaiedge.net`
- one A record (IP addr) for `e9566.dscb.akamaiedge.net`

```
Additional RRs: 0
▾ Queries
  ▾ e9566.dscb.akamaiedge.net: type AAAA, class IN
      Name: e9566.dscb.akamaiedge.net
      [Name Length: 25]
      [Label Count: 4]
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
▾ Answers
  ▸ e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2600:1406:3400:78f::255e
  ▸ e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2600:1406:3400:795::255e
▸ Authoritative nameservers
```

- 2 answers
- Both are AAAA records for `e9566.dscb.akamaiedge.net` representing IPv6 addresses

15. Provide a screenshot.

    See above

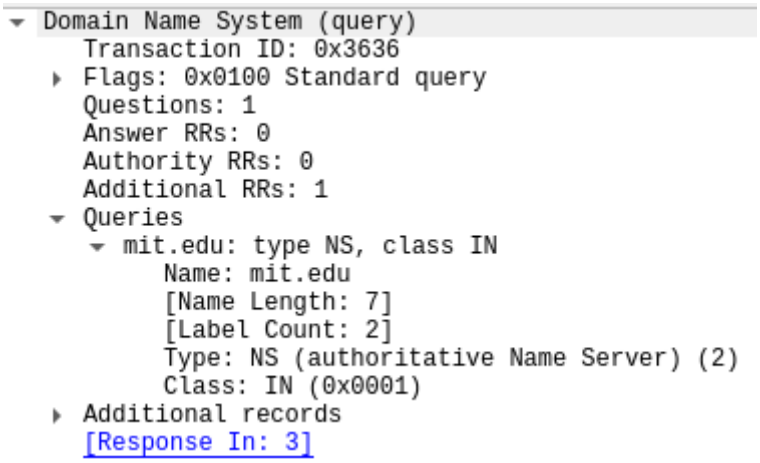
mit.edu

（...怎么还有，这实验太无聊了）

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

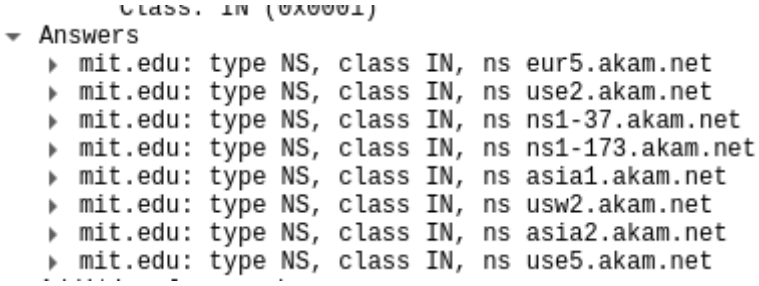
    Same as above.

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

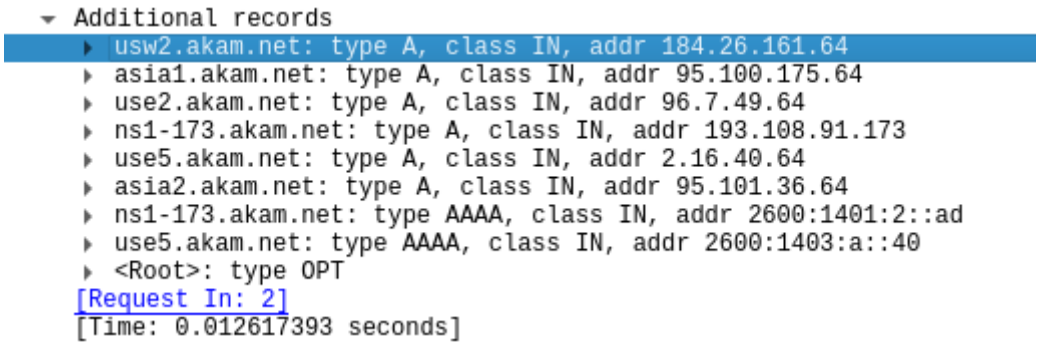


- Type NS
- No

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 nameservers?



- Well, a lot.
- Yes.



19. Provide a screenshot.

    See above

www.aiit.or.kr

（.....令人感叹）

因为超时所以换成默认 DNS server

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?

    Yes. 因为给的不能用

21. 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: 0x829e
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ 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)
    [Response In: 5]
```

- Type A
- No

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

```
▸ Queries
▾ Answers
  ▸ www.aiit.or.kr: type A, class IN, addr 58.229.6.225
[Request In: 4]
[Time: 0.006451623 seconds]
```

- One
- IP addr for the site

23. Provide a screenshot.

    See above