

# CS305B Lab6 Report

11812418 樊青远 Fan Qingyuan

## 6.1 DNS Query with EDNS

```
dig @119.29.29.29 mirrors.ustc.edu.cn +subnet=116.7.234.0/24 +edns=0
```

```
; <>> DiG 9.10.6 <>> @119.29.29.29 mirrors.ustc.edu.cn +subnet=116.7.234.0/24
+edns=0
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24696
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; CLIENT-SUBNET: 116.7.234.0/24/24
;; QUESTION SECTION:
;mirrors.ustc.edu.cn. IN A

;; ANSWER SECTION:
mirrors.ustc.edu.cn. 600 IN A 202.141.160.110

;; Query time: 310 msec
;; SERVER: 119.29.29.29#53(119.29.29.29)
;; WHEN: Thu Apr 01 18:52:32 CST 2021
;; MSG SIZE rcvd: 75
```

```

cyf@LAPTOP-TMBP81 ~ ~/Documents/GitHub/ccse-mirrors/ccse-mirrors-web master ? dig @
119.29.29.29 mirrors.ustc.edu.cn +subnet=116.7.234.0/24 +edns=0

; <>> DiG 9.10.6 <>> @119.29.29.29 mirrors.ustc.edu.cn +subnet=116.7.234.0/24 +edns=0
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24696
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

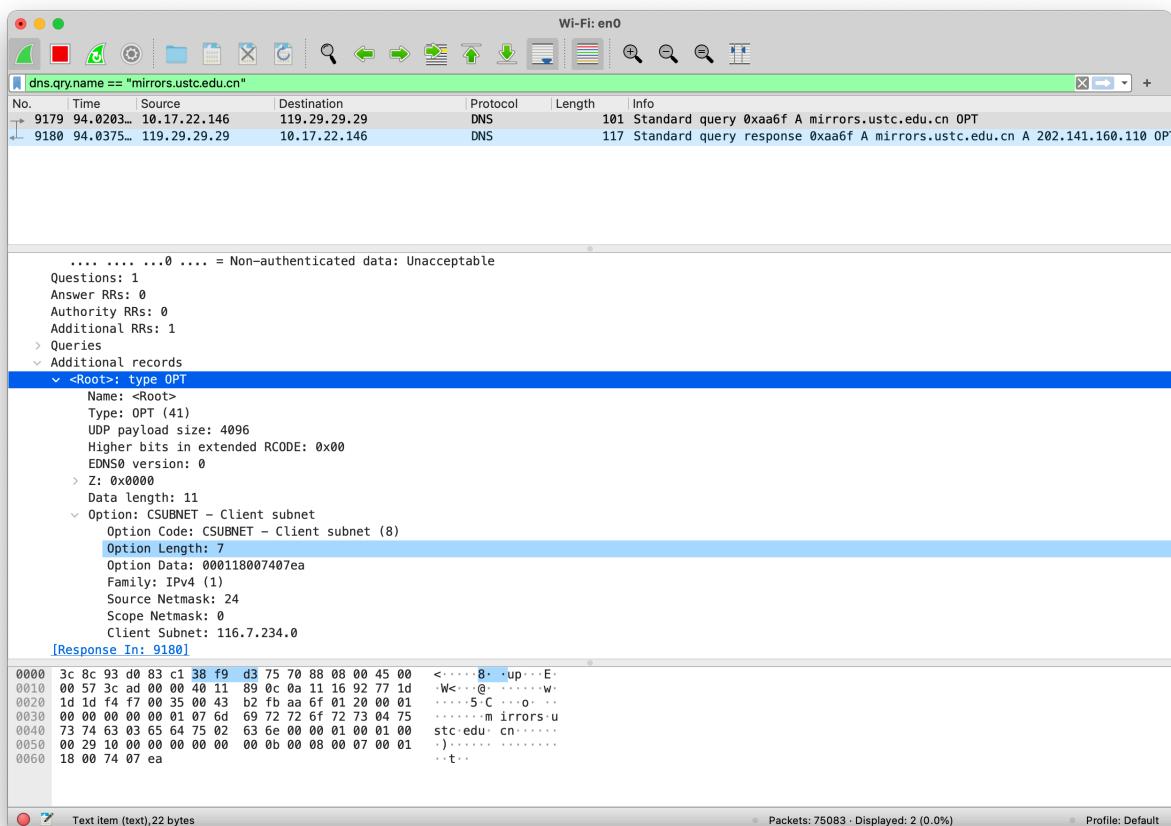
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; CLIENT-SUBNET: 116.7.234.0/24/24
;; QUESTION SECTION:
;mirrors.ustc.edu.cn.           IN      A

;; ANSWER SECTION:
mirrors.ustc.edu.cn.    600     IN      A      202.141.160.110

;; Query time: 310 msec
;; SERVER: 119.29.29.29#53(119.29.29.29)
;; WHEN: Thu Apr 01 18:52:32 CST 2021
;; MSG SIZE rcvd: 75

```

## Capture by wireshark



```

Type: A (Host Address) (1)
Class: IN (0x0001)

Answers
  mirrors.ustc.edu.cn: type A, class IN, addr 202.141.160.110
    Name: mirrors.ustc.edu.cn
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 154 (2 minutes, 34 seconds)
    Data length: 4
    Address: 202.141.160.110

Additional records
  <Root>: type OPT
    Name: <Root>
    Type: OPT (41)
    UDP payload size: 4096
    Higher bits in extended RCODE: 0x00
    EDNS0 version: 0
      Z: 0x0000
        0... .... .... = DO bit: Cannot handle DNSSEC security RRs
        .000 0000 0000 0000 = Reserved: 0x0000
        Data length: 11
      0000 38 f9 d3 75 70 88 20 76 93 44 b6 fb 08 00 45 00 8...up...v...D...E...
      0010 00 67 1f f1 00 00 29 11 a1 89 77 1d 1d 1d c0 a8 g....)....w.....
      0020 7b 29 00 35 c6 b7 00 53 5d 74 e9 42 81 80 00 01 {).5...S ]t.B...
      0030 00 01 00 00 01 07 6d 69 72 72 6f 72 73 04 75 .....m mirrors.u
      0040 73 74 63 03 65 64 75 02 63 6e 00 00 01 00 01 c0 stc.edu.cn.....
      0050 0c 00 01 00 01 00 00 00 9a 00 04 ca 8d a0 6e 00 .....n.
      0060 00 29 10 00 00 00 00 00 00 0b 00 08 00 07 00 01 ).....
      0070 18 18 74 07 ea .....t...

```

## Query Content

Server name: 119.29.29.29

Length: 101

How can you tell this DNS query is based on EDNS0: We could find the `EDNS0 version` entity in wireshark log.

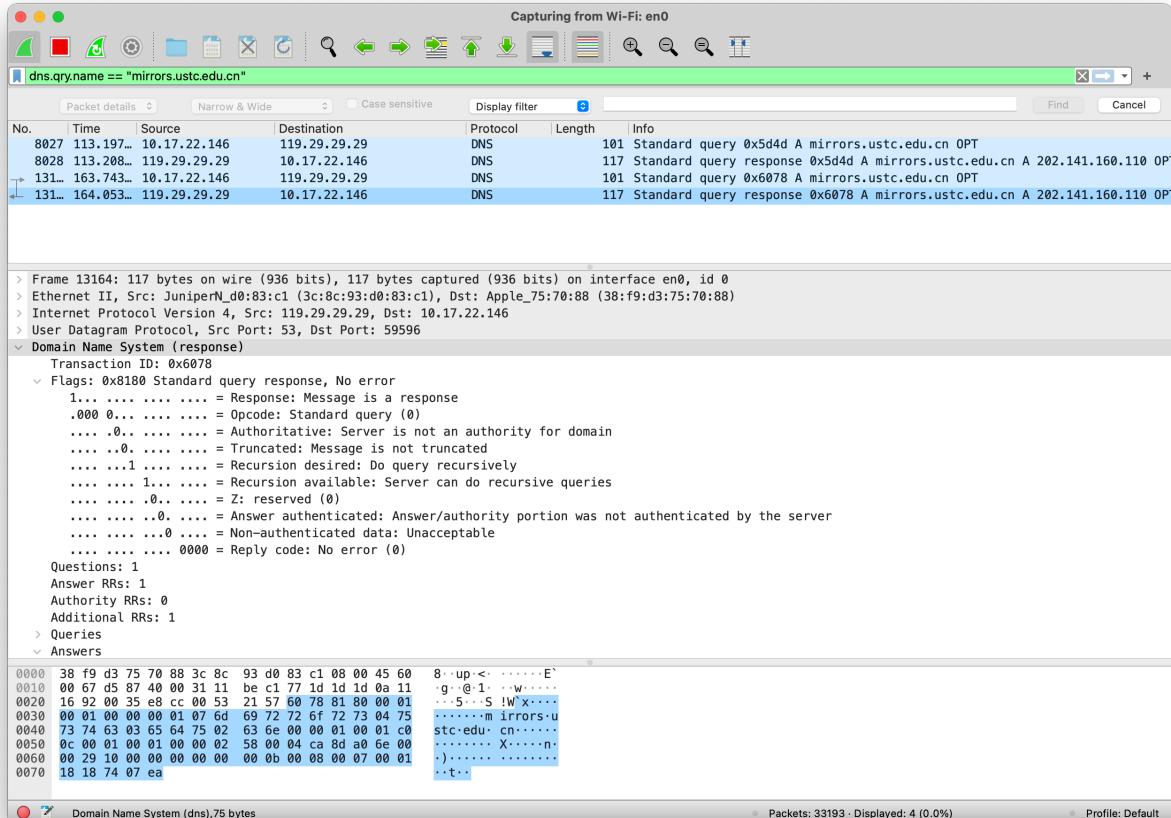
```

  ↴ queries
  ↵ Additional records
    <Root>: type OPT
      Name: <Root>
      Type: OPT (41)
      UDP payload size: 4096
      Higher bits in extended RCODE: 0x00
      EDNS0 version: 0
        Z: 0x0000
          0... .... .... = DO bit: Cannot handle DNSSEC security RRs
          .000 0000 0000 0000 = Reserved: 0x0000
          Data length: 11
        Option: CSUBNET - Client subnet
          Option Code: CSUBNET - Client subnet (8)
          Option Length: 7
          Option Data: 000118007407ea
          Family: IPv4 (1)
          Source Netmask: 24
          Scope Netmask: 0
          Client Subnet: 116.7.234.0
[Response In: 13164]

```

# What's response content

Info:



TTL: 600 seconds

Answers

- mirrors.ustc.edu.cn: type A, class IN, addr 202.141.160.110
  - Name: mirrors.ustc.edu.cn
  - Type: A (Host Address) (1)
  - Class: IN (0x0001)

Time to live: 600 (10 minutes)

Data length: 4

Address: 202.141.160.110

Additional records

Authority RRs: No

Addition RRs: Yes

```
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
```

```

DNSSEC: 2021-11-10T11:11:11Z
  Additional records
    <Root>: type OPT
      Name: <Root>
      Type: OPT (41)
      UDP payload size: 4096
      Higher bits in extended RCODE: 0x00
      EDNS0 version: 0
    Z: 0x0000
      0... .... .... .... = DO bit: Cannot handle DNSSEC security RRs
      .000 0000 0000 0000 = Reserved: 0x0000
      Data length: 11
    Option: CSUBNET - Client subnet
      Option Code: CSUBNET - Client subnet (8)
      Option Length: 7
      Option Data: 000118187407ea
      Family: IPv4 (1)
      Source Netmask: 24
      Scope Netmask: 24
      Client Subnet: 116.7.234.0
[Request In: 13148]
[Time: 0.310554000 seconds]

```

There still have some bits reserved in use. It only contains zero.

```

  EDNS0 version: 0
  Z: 0x0000
    0... .... .... .... = DO bit: Cannot handle DNSSEC security RRs
    .000 0000 0000 0000 = Reserved: 0x0000
    Data length: 11
  Option: CSUBNET - Client subnet

```

## 6.2 Python DNS query

**Make the query of python dns resolver to query A type by using UDP and TCP:**

**Find the difference between two commands, what's the default transport layer protocol while invoke DNS query**

The command to query with tcp needs to add the parameter `tcp=True`

UDP is the default portal while invoke DNS query.

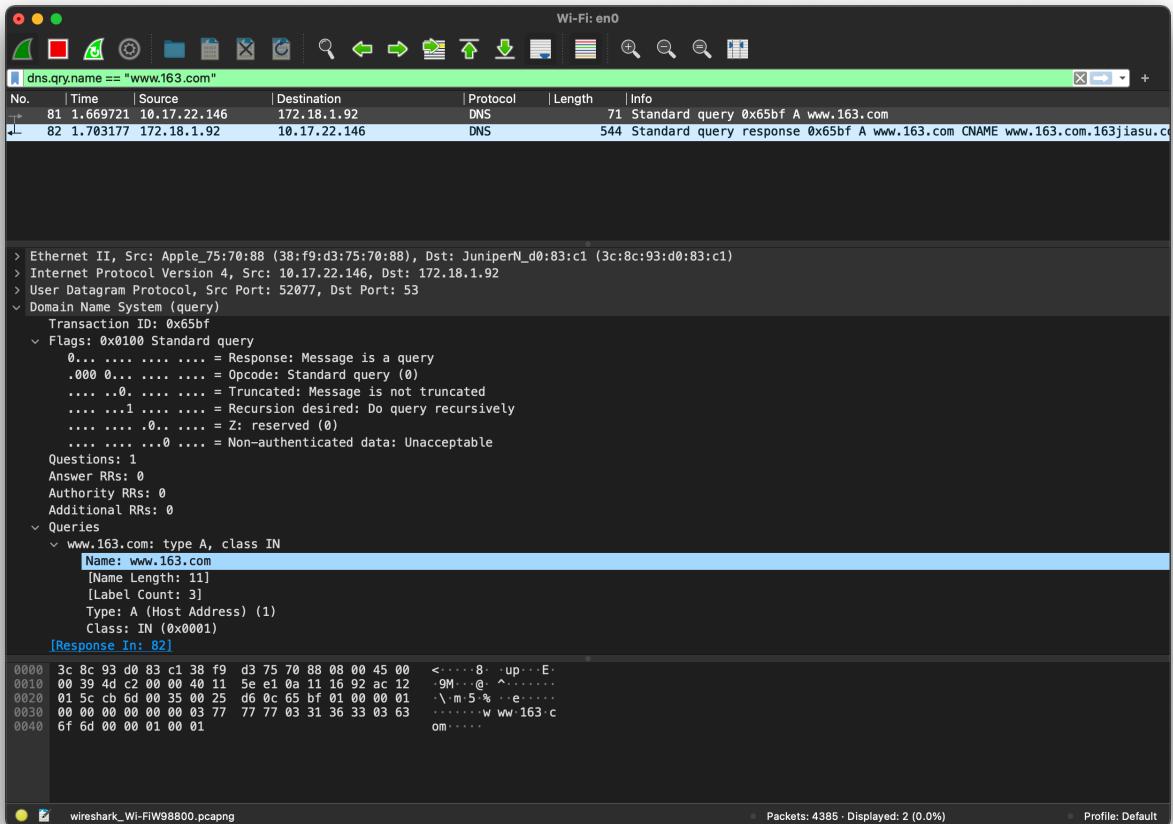
### UDP

```

import dns
import dns.resolver

result = dns.resolver.query('www.163.com', 'A')
for ipval in result:
    print('IP', ipval.to_text())

```



**How many UDP packets are captured in this stream, What is the port number used?**

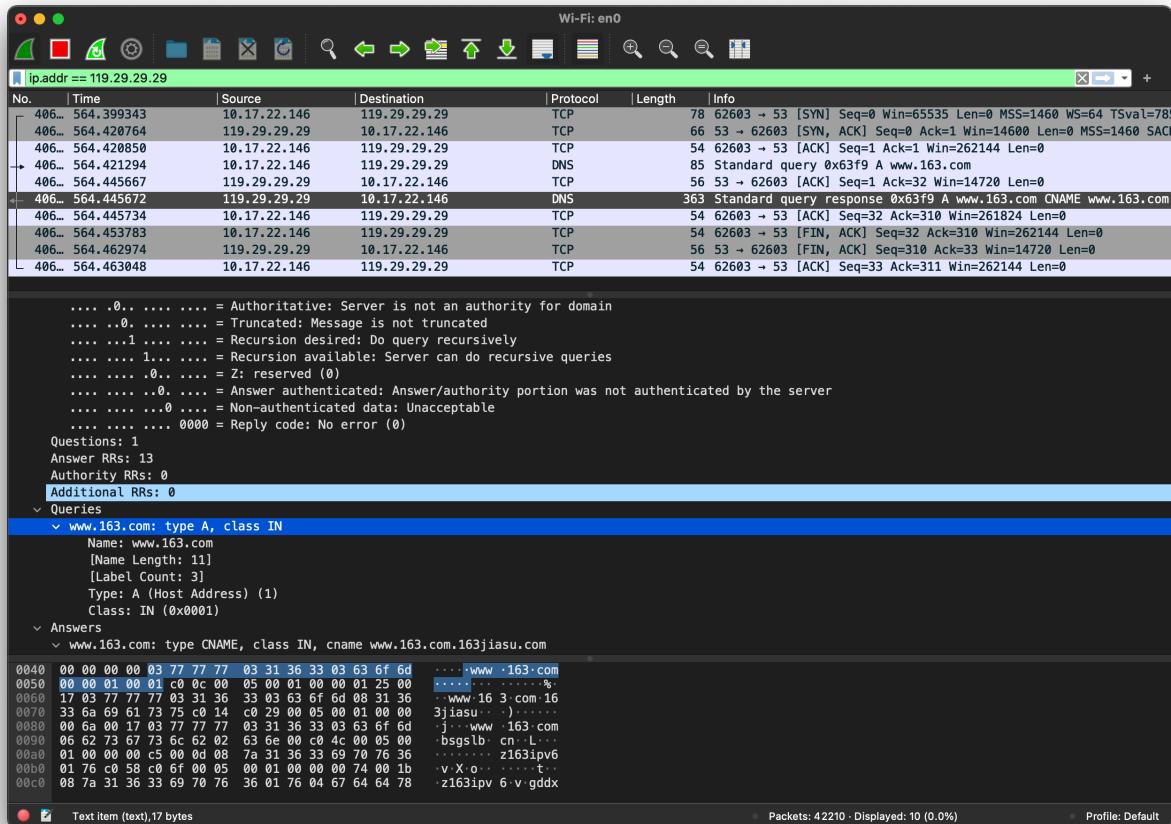
2 packets with port 53.

**TCP**

```
import dns.resolver

my_resolver = dns.resolver.Resolver()
my_resolver.nameservers = [ '119.29.29.29' ]

result = my_resolver.query('www.163.com', 'A', tcp=True)
for ipval in result:
    print('IP', ipval.to_text())
```



## How many TCP packets are captured in this stream, What is the port number used?

10 Packets with port 53.

## Is there any difference on query and response of DNS between using TCP and using UDP?

Unlike UDP, to initiate the TCP DNS query, the client needs handshake with the server first.

The contents of the DNS query response are same.