CS305 Lab5

Name: 胡玉斌
Student Id: 11712121

1. **Introduction**
   - DNS
     - DNS Message Structure
     - DNS Message head
     - RR in DNS
   - EDNS (aka. Extension mechanisms for DNS)
     - DNSSEC
   - DNS Resolver
2. **Procedure**
   - DNS is a distributed database.
   - Most machine has a local resolver which handles request of domain name and maintain a cache of query result
   - EDNS: a backward compatible mechanisms for allowing the DNS protocol to grow.
   - dig is a flexible tool for interrogating DNS name servers.
   - Domain Name System Security Extensions
   - a security mechanism designed to solve DNS spoofing and cache pollution.
   - By using cryptography, the DNS resolver can verify whether the reply it receives comes from the real server or is tampered with during transmission.
   - Most machine has a local resolver which handles request of domain name and maintain a cache of query result.
3. **Result & Analysis(including answer of question)**

lab5.1

make an DNS query which will invoke the EDNS0

> **Solution:**

```
eveneko@DESKTOP-MMVJRV3 /mnt/c/Users/Eveneko dig @ns1.sustech.edu.cn www.baidu.com +dnssec

; <<>> DiG 9.11.3-1ubuntu1.9-Ubuntu <<>> @ns1.sustech.edu.cn www.baidu.com +dnssec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 736
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.baidu.com.                 IN      A

;; ANSWER SECTION:
www.baidu.com.          145     IN      CNAME   www.a.shifen.com.
www.a.shifen.com.       315     IN      A       14.215.177.38
www.a.shifen.com.       315     IN      A       14.215.177.39

;; AUTHORITY SECTION:
a.shifen.com.           53      IN      NS      ns4.a.shifen.com.
a.shifen.com.           53      IN      NS      ns3.a.shifen.com.
a.shifen.com.           53      IN      NS      ns1.a.shifen.com.
a.shifen.com.           53      IN      NS      ns2.a.shifen.com.
a.shifen.com.           53      IN      NS      ns5.a.shifen.com.

;; ADDITIONAL SECTION:
ns1.a.shifen.com.       7       IN      A       61.135.165.224
ns5.a.shifen.com.       185     IN      A       180.76.76.95
ns3.a.shifen.com.       131     IN      A       112.80.255.253

;; Query time: 2 msec
;; SERVER: 172.18.1.92#53(172.18.1.92)
;; WHEN: Sun Oct 13 17:36:54 DST 2019
;; MSG SIZE  rcvd: 239
```

capture the packages using Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
109	4.382228	10.21.6.171	172.18.1.92	DNS	96	Standard query 0xfede A www.baidu.com OPT
110	4.385804	172.18.1.92	10.21.6.171	DNS	265	Standard query response 0xfede A www.baidu.com CNAME www.a.shifen.com A 14.215.

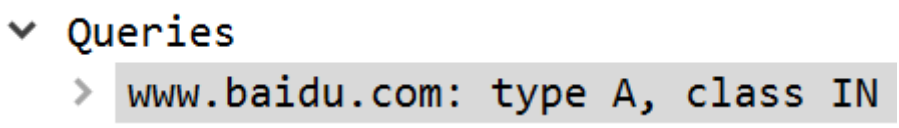
- what is the content of this query message
  - Find the name, type and class of this query

Solution:

name: www.baidu.com

type: A

class: IN



  - How can you tell this DNS query is based on EDNS0

Solution:

```
Additional records
  <Root>: type OPT
      Name: <Root>
      Type: OPT (41)
      UDP payload size: 4096
      Higher bits in extended RCODE: 0x00
      EDNS0 version: 0
    Z: 0x8000
        1... .... .... .... = DO bit: Accepts DNSSEC security RRs
        .000 0000 0000 0000 = Reserved: 0x0000
      Data length: 12
    Option: COOKIE
[Response In: 110]
```

- From this query massage , can it handle DNSSEC security RRs or not

Solution:

It can handle DNSSEC security

```
Domain Name System (query)
  Transaction ID: 0xfede
  Flags: 0x0120 Standard query
    0... .... .... .... = Response: Message is a query
    .000 0... .... .... = Opcode: Standard query (0)
    .... ..0. .... .... = Truncated: Message is not truncated
    .... ...1 .... .... = Recursion desired: Do query recursively
    .... .... .0.. .... = Z: reserved (0)
    .... .... ..1. .... = AD bit: Set
    .... .... ...0 .... = Non-authenticated data: Unacceptable
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 1
  Queries
    www.baidu.com: type A, class IN
      Name: www.baidu.com
      [Name Length: 13]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
  Additional records
    <Root>: type OPT
      Name: <Root>
      Type: OPT (41)
      UDP payload size: 4096
      Higher bits in extended RCODE: 0x00
      EDNS0 version: 0
    Z: 0x8000
      1... .... .... .... = DO bit: Accepts DNSSEC security RRs
      .000 0000 0000 0000 = Reserved: 0x0000
      Data length: 12
    Option: COOKIE
  [Response In: 110]
```

- what is the content of this response message
  - Is there any answers, what's the ttl of each answer

> **Solution:**
>
> There are 3 answers.
>
> ttl: 106, ttl: 276, ttl: 276.

```
Answers
    www.baidu.com: type CNAME, class IN, cname www.a.shifen.com
        Name: www.baidu.com
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 106
        Data length: 15
        CNAME: www.a.shifen.com
    www.a.shifen.com: type A, class IN, addr 14.215.177.39
        Name: www.a.shifen.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 276
        Data length: 4
        Address: 14.215.177.39
    www.a.shifen.com: type A, class IN, addr 14.215.177.38
        Name: www.a.shifen.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 276
        Data length: 4
        Address: 14.215.177.38
```

  - Is there any authority RRs, what's the type of each RR

> **Solution:**
>
> There are 5 authority RRs, the type of each RR is NS.

```
Authoritative nameservers
  a.shifen.com: type NS, class IN, ns ns1.a.shifen.com
      Name: a.shifen.com
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 14
      Data length: 6
      Name Server: ns1.a.shifen.com
  a.shifen.com: type NS, class IN, ns ns2.a.shifen.com
      Name: a.shifen.com
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 14
      Data length: 6
      Name Server: ns2.a.shifen.com
  a.shifen.com: type NS, class IN, ns ns5.a.shifen.com
      Name: a.shifen.com
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 14
      Data length: 6
      Name Server: ns5.a.shifen.com
  a.shifen.com: type NS, class IN, ns ns4.a.shifen.com
      Name: a.shifen.com
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 14
      Data length: 6
      Name Server: ns4.a.shifen.com
  a.shifen.com: type NS, class IN, ns ns3.a.shifen.com
      Name: a.shifen.com
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 14
      Data length: 6
      Name Server: ns3.a.shifen.com
```

- Is there any special additional RRs with OPT type, what does its 'Do bit' say: Does it accept DNSSEC security RRs or not

Solution:

There is a special additional RRs with OPT type. It accept DNSSEC security RRS.

```
Additional records
  ns5.a.shifen.com: type A, class IN, addr 180.76.76.95
      Name: ns5.a.shifen.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 146
      Data length: 4
      Address: 180.76.76.95
  ns3.a.shifen.com: type A, class IN, addr 112.80.255.253
      Name: ns3.a.shifen.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 92
      Data length: 4
      Address: 112.80.255.253
  <Root>: type OPT
      Name: <Root>
      Type: OPT (41)
      UDP payload size: 4096
      Higher bits in extended RCODE: 0x00
      EDNS0 version: 0
    Z: 0x8000
      1... .... .... .... = DO bit: Accepts DNSSEC security RRs
      .000 0000 0000 0000 = Reserved: 0x0000
      Data length: 0
  [Request In: 109]
  [Time: 0.003576000 seconds]
```

lab 5.2

Make the query by using query method of “dns resolver”(a python package)

- To query the type A value of www.sina.com.cn based on TCP and UDP stream respectively

Solution:

For TCP:

```
eveneko@DESKTOP-MMVJRV3 /mnt/c/Users/Eveneko python3
Python 3.6.8 (default, Aug 20 2019, 17:12:48)
[GCC 8.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import dns.resolver
>>> tcp_query = dns.resolver.query("www.sina.com.cn", rdtype=dns.rdatatype.A, tcp=True)
>>>
```

For UDP:

```
>>> udp_query = dns.resolver.query("www.sina.com.cn", rdtype=dns.rdatatype.A)
>>>
```

Python:

```python
import dns.resolver

tcp_query = dns.resolver.query("www.sina.com.cn", rdtype=dns.rdatatype.A, tcp=True)
udp_query = dns.resolver.query("www.sina.com.cn", rdtype=dns.rdatatype.A)

print("TCP query:")
for i in tcp_query.response.answer:
    for j in i.items:
        print(j)

print("\nUDP query:")
for i in udp_query.response.answer:
    for j in i.items:
        print(j)
```

```
PS D:\CN\Homework> python -u "d:\CN\Homework\Lab5\query.py"
TCP query:
spool.grid.sinaedge.com.
222.76.214.26

UDP query:
spool.grid.sinaedge.com.
222.76.214.26
```

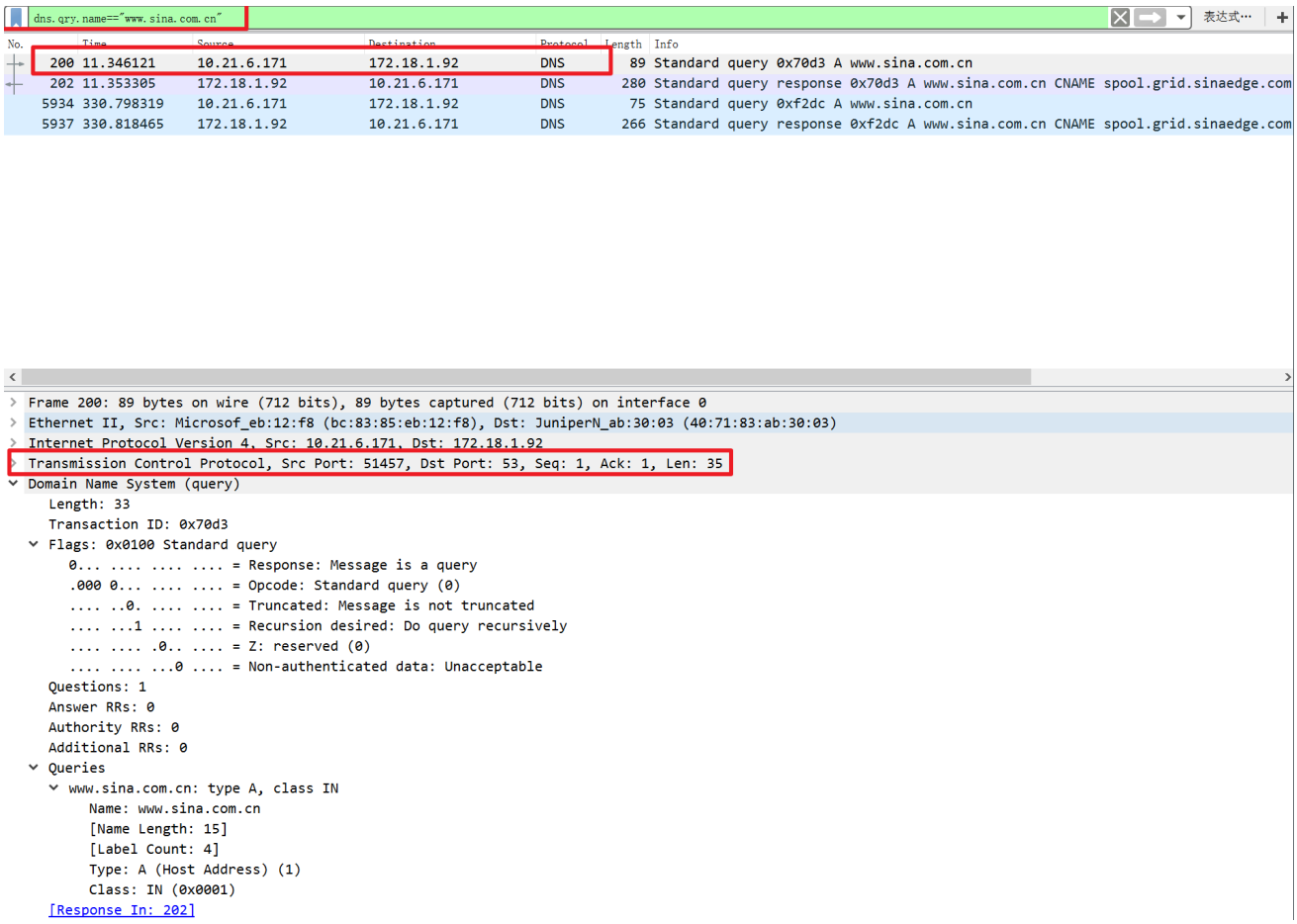
capture the related TCP stream and UDP stream using Wireshark

- Screenshot on this two commands. what's the default transport lay protocol while invoke DNS query

Solution:

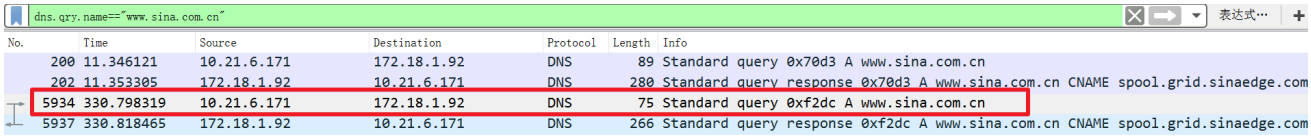
For TCP:

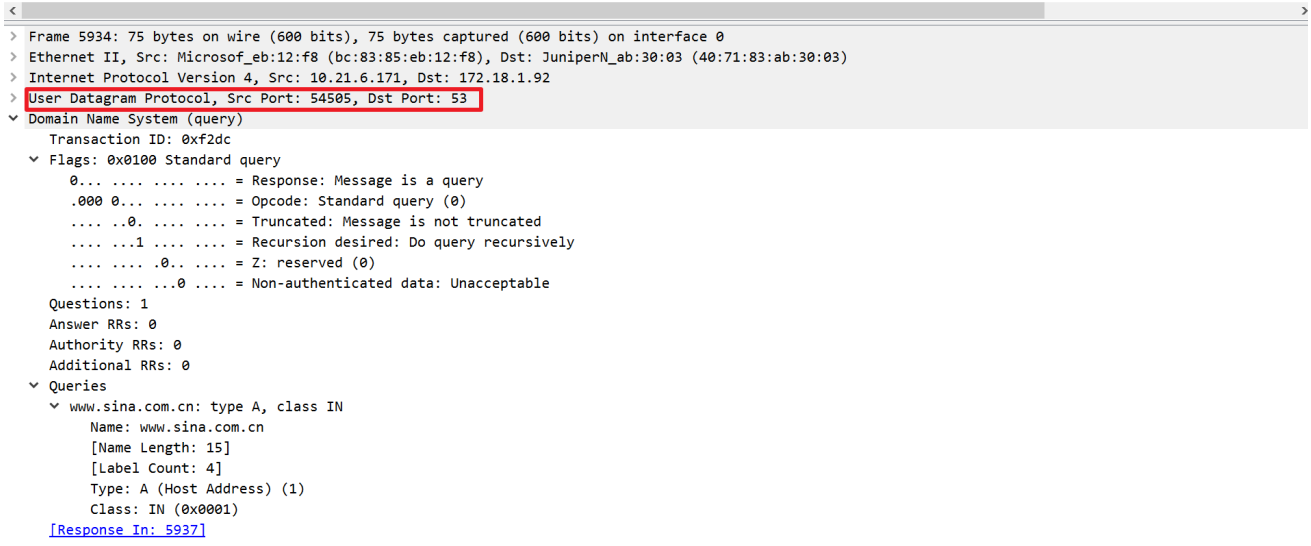
```
eveneko@DESKTOP-MMVJRV3 /mnt/c/Users/Eveneko python3
Python 3.6.8 (default, Aug 20 2019, 17:12:48)
[GCC 8.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import dns.resolver
>>> tcp_query = dns.resolver.query("www.sina.com.cn", rdtype=dns.rdatatype.A, tcp=True)
>>>
```

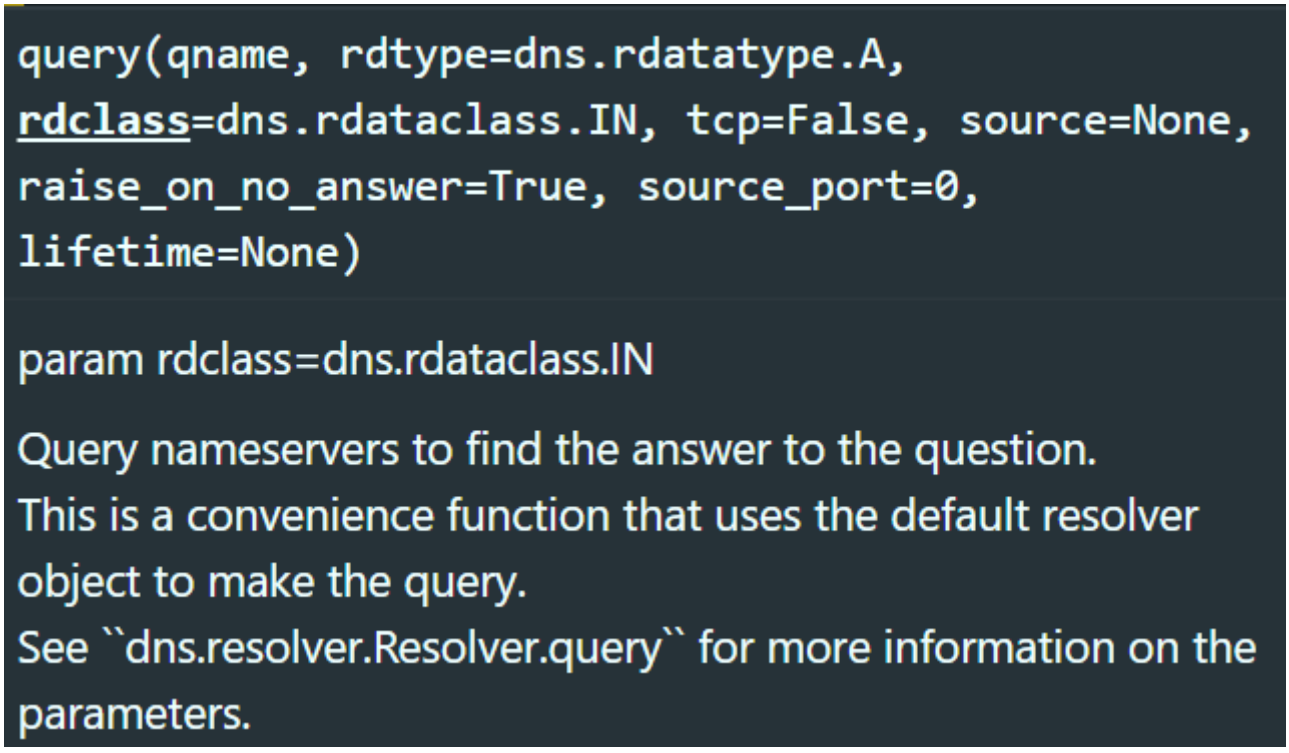


For UDP:

```
>>> udp_query = dns.resolver.query("www.sina.com.cn", rdtype=dns.rdatatype.A)
>>>
```







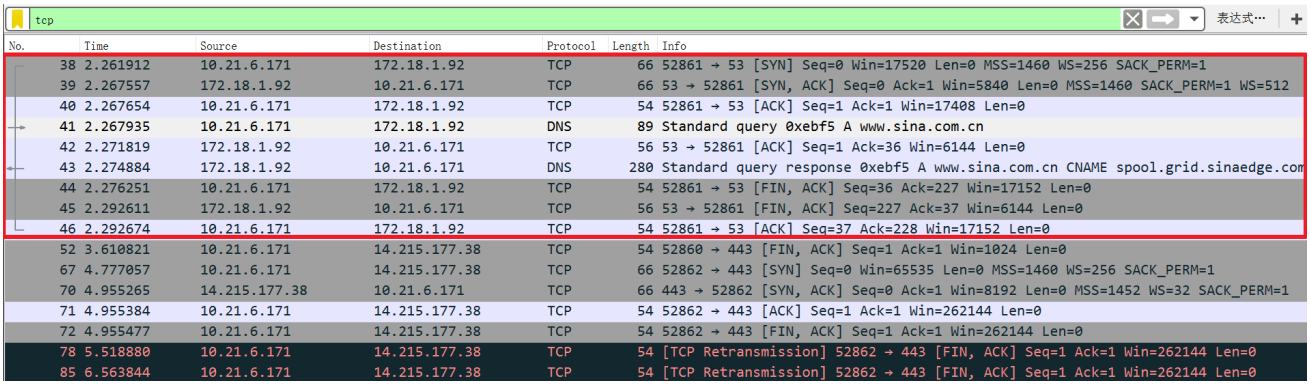
The default transport lay protocol while invoke DNS query is UDP.

- Screenshot on the TCP stream of query by TCP. how many TCP packets are captured in this stream, Which port is used?

Solution:

There are 9 TCP packets are captured in this stream.

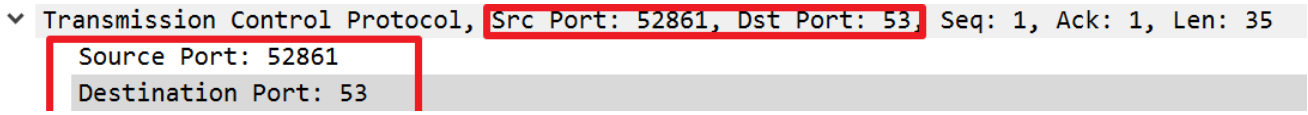
(DNS is over the TCP)



No.	Time	Source	Destination	Protocol	Length	Info
38	2.261912	10.21.6.171	172.18.1.92	TCP	66	52861 → 53 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM=1
39	2.267557	172.18.1.92	10.21.6.171	TCP	66	53 → 52861 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=512
40	2.267654	10.21.6.171	172.18.1.92	TCP	54	52861 → 53 [ACK] Seq=1 Ack=1 Win=17408 Len=0
41	2.267935	10.21.6.171	172.18.1.92	DNS	89	Standard query 0xebf5 A www.sina.com.cn
42	2.271819	172.18.1.92	10.21.6.171	TCP	56	53 → 52861 [ACK] Seq=1 Ack=36 Win=6144 Len=0
43	2.274884	172.18.1.92	10.21.6.171	DNS	280	Standard query response 0xebf5 A www.sina.com.cn CNAME spool.grid.sinaedge.com
44	2.276251	10.21.6.171	172.18.1.92	TCP	54	52861 → 53 [FIN, ACK] Seq=36 Ack=227 Win=17152 Len=0
45	2.292611	172.18.1.92	10.21.6.171	TCP	56	53 → 52861 [FIN, ACK] Seq=227 Ack=37 Win=6144 Len=0
46	2.292674	10.21.6.171	172.18.1.92	TCP	54	52861 → 53 [ACK] Seq=37 Ack=228 Win=17152 Len=0
52	3.610821	10.21.6.171	14.215.177.38	TCP	54	52860 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1024 Len=0
67	4.777057	10.21.6.171	14.215.177.38	TCP	66	52862 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
70	4.955265	14.215.177.38	10.21.6.171	TCP	66	443 → 52862 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1452 WS=32 SACK_PERM=1
71	4.955384	10.21.6.171	14.215.177.38	TCP	54	52862 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
72	4.955477	10.21.6.171	14.215.177.38	TCP	54	52862 → 443 [FIN, ACK] Seq=1 Ack=1 Win=262144 Len=0
78	5.518880	10.21.6.171	14.215.177.38	TCP	54	[TCP Retransmission] 52862 → 443 [FIN, ACK] Seq=1 Ack=1 Win=262144 Len=0
85	6.563844	10.21.6.171	14.215.177.38	TCP	54	[TCP Retransmission] 52862 → 443 [FIN, ACK] Seq=1 Ack=1 Win=262144 Len=0

Source Port: 52861

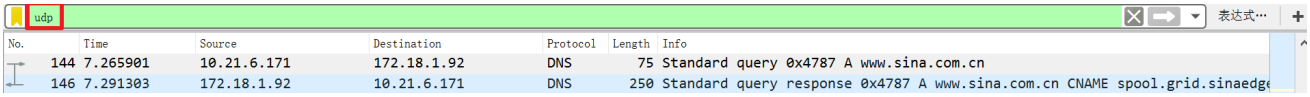
Destination Port: 53



- Screenshot on the UDP stream of query by UDP. how many UDP packets are captured in this stream, Which port is used?

Solution:

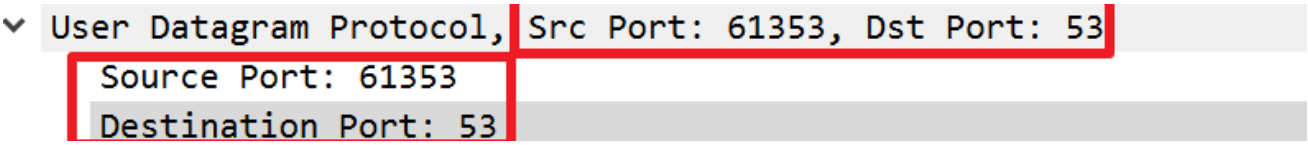
There are 2 UDP packets are captured in this stream



No.	Time	Source	Destination	Protocol	Length	Info
144	7.265901	10.21.6.171	172.18.1.92	DNS	75	Standard query 0x4787 A www.sina.com.cn
146	7.291303	172.18.1.92	10.21.6.171	DNS	250	Standard query response 0x4787 A www.sina.com.cn CNAME spool.grid.sinaedge

Source Port: 61353

Destination Port: 53



- Is there any difference on DNS query and response message while using TCP and UDP respectively

Solution:

TCP query:

```
> Transmission Control Protocol, Src Port: 53611, Dst Port: 53, Seq: 1, Ack: 1, Len: 35
v Domain Name System (query)
    Length: 33
    Transaction ID: 0x58fb
  v Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.sina.com.cn: type A, class IN
        Name: www.sina.com.cn
        [Name Length: 15]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 83]
```

UDP query:

```
> User Datagram Protocol, Src Port: 49945, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x595f
  v Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.sina.com.cn: type A, class IN
        Name: www.sina.com.cn
        [Name Length: 15]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 96]
```

TCP response:

```
> Transmission Control Protocol, Src Port: 53, Dst Port: 53611, Seq: 1, Ack: 36, Len: 210
v Domain Name System (response)
    Length: 208
    Transaction ID: 0x58fb
  v Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 2
    Authority RRs: 5
    Additional RRs: 2
  v Queries
    v www.sina.com.cn: type A, class IN
        Name: www.sina.com.cn
        [Name Length: 15]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  v Answers
    v www.sina.com.cn: type CNAME, class IN, cname spool.grid.sinaedge.com
        Name: www.sina.com.cn
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 14
        Data length: 25
        CNAME: spool.grid.sinaedge.com
    v spool.grid.sinaedge.com: type A, class IN, addr 222.76.214.26
        Name: spool.grid.sinaedge.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 141
        Data length: 4
        Address: 222.76.214.26
  v Authoritative nameservers
    v sinaedge.com: type NS, class IN, ns ns3.sinaedge.com
        Name: sinaedge.com
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 2765
        Data length: 6
        Name Server: ns3.sinaedge.com
```

```
  sinaedge.com: type NS, class IN, ns ns5.sinaedge.com
    Name: sinaedge.com
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 2765
    Data length: 6
    Name Server: ns5.sinaedge.com
  sinaedge.com: type NS, class IN, ns ns4.sinaedge.com
    Name: sinaedge.com
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 2765
    Data length: 6
    Name Server: ns4.sinaedge.com
  sinaedge.com: type NS, class IN, ns ns1.sinaedge.com
    Name: sinaedge.com
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 2765
    Data length: 6
    Name Server: ns1.sinaedge.com
  sinaedge.com: type NS, class IN, ns ns2.sinaedge.com
    Name: sinaedge.com
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 2765
    Data length: 6
    Name Server: ns2.sinaedge.com
Additional records
  ns2.sinaedge.com: type A, class IN, addr 58.63.238.144
    Name: ns2.sinaedge.com
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 22
    Data length: 4
    Address: 58.63.238.144
  ns1.sinaedge.com: type A, class IN, addr 123.126.42.246
    Name: ns1.sinaedge.com
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 88
    Data length: 4
    Address: 123.126.42.246
[Request In: 81]
[Time: 0.003481000 seconds]
```

UDP response:

```
> User Datagram Protocol, Src Port: 53, Dst Port: 49945
v Domain Name System (response)
    Transaction ID: 0x595f
  v Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 2
    Authority RRs: 5
    Additional RRs: 2
  v Queries
    v www.sina.com.cn: type A, class IN
        Name: www.sina.com.cn
        [Name Length: 15]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  v Answers
    v www.sina.com.cn: type CNAME, class IN, cname spool.grid.sinaedge.com
        Name: www.sina.com.cn
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 13
        Data length: 25
        CNAME: spool.grid.sinaedge.com
    v spool.grid.sinaedge.com: type A, class IN, addr 222.76.214.26
        Name: spool.grid.sinaedge.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 140
        Data length: 4
        Address: 222.76.214.26
  v Authoritative nameservers
    v sinaedge.com: type NS, class IN, ns ns2.sinaedge.com
        Name: sinaedge.com
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 2764
        Data length: 6
        Name Server: ns2.sinaedge.com
```

```
  sinaedge.com: type NS, class IN, ns ns5.sinaedge.com
    Name: sinaedge.com
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 2764
    Data length: 6
    Name Server: ns5.sinaedge.com
  sinaedge.com: type NS, class IN, ns ns4.sinaedge.com
    Name: sinaedge.com
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 2764
    Data length: 6
    Name Server: ns4.sinaedge.com
  sinaedge.com: type NS, class IN, ns ns3.sinaedge.com
    Name: sinaedge.com
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 2764
    Data length: 6
    Name Server: ns3.sinaedge.com
  sinaedge.com: type NS, class IN, ns ns1.sinaedge.com
    Name: sinaedge.com
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 2764
    Data length: 6
    Name Server: ns1.sinaedge.com
Additional records
  ns2.sinaedge.com: type A, class IN, addr 58.63.238.144
    Name: ns2.sinaedge.com
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 21
    Data length: 4
    Address: 58.63.238.144
  ns1.sinaedge.com: type A, class IN, addr 123.126.42.246
    Name: ns1.sinaedge.com
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 87
    Data length: 4
    Address: 123.126.42.246
  [Request In: 93]
  [Time: 0.002851000 seconds]
```

> TCP and UDP have the same DNS query and response message except that TCP's query and response have a attribute "Length", but UDP donot have.

lab5.3 Implement a local resolver

ip and port

```
# Local
serverName = '127.0.0.1'
serverPort = 12000

# Public DNS server
pubName = '114.114.114.114'
pubPort = 53
```

The complete code is enclosed in the package.

4. **Conclusion and Experience：**
   - 标识ID(id)： 请求客户端设置的16位标示，服务器给出应答的时候会带相同的标示字段回来，这样请求客户端就可以区分不同的请求应答了。
   - 标志(flags)：QR 1个比特位用来区分是请求（0）还是应答（1）。OPCODE 4个比特位用来设置查询的种类，应答的时候会带相同值，可用的值如下：
     - 0 标准查询 (QUERY)
     - 1 反向查询 (IQUERY)
     - 2 服务器状态查询 (STATUS)
     - 3-15 保留值，暂时未使用
   - AA 授权应答(Authoritative Answer) - 这个比特位在应答的时候才有意义，指出给出应答的服务器是查询域名的授权解析服务器。注意因为别名的存在，应答可能存在多个主域名，这个AA位对应请求名，或者应答中的第一个主域名。
   - TC 截断(TrunCation) - 用来指出报文比允许的长度还要长，导致被截断。
   - RD 期望递归(Recursion Desired) - 这个比特位被请求设置，应答的时候使用的相同的值返回。如果设置了RD，就建议域名服务器进行递归解析，递归查询的支持是可选的。
   - RA 支持递归(Recursion Available) - 这个比特位在应答中设置或取消，用来代表服务器是否支持递归查询。
   - Z 保留值，暂时未使用。在所有的请求和应答报文中必须置为0。
   - 问题数QDCOUNT 无符号16位整数表示报文请求段中的问题记录数。
   - 资源记录数ANCOUNT 无符号16位整数表示报文回答段中的回答记录数。
   - 授权资源记录数NSCOUNT 无符号16位整数表示报文授权段中的授权记录数。
   - 额外资源记录数ARCOUNT 无符号16位整数表示报文附加段中的附加记录数。
   - Query
     - 查询名QNAME 要查找的名字，是一个或多个标识符的序列。每个标识符以首字节的计数值来说明随后标识符的字节长度，每个名字以最后字节为0结束，长度为0的标识符是根标识符。单个标识符最大长度为63字节。

        - 查询类型QTYPE 每个问题有一个查询类型。2个字节表示查询类型，取值可以为任何可用的类型值，以及通配码来表示所有的资源记录。
    - Answer
        - 域名NAME 资源记录包含的域名
        - 类型TYPE 2个字节表示资源记录的类型，指出RDATA数据的含义
        - 类CLASS 2个字节表示RDATA的类
        - 生存时间TTL 4字节无符号整数表示资源记录可以缓存的时间。0代表只能被传输，但是不能被缓存。
        - 资源数据长度URDLENGT 2个字节无符号整数表示RDATA的长度
        - 资源数据RDATA 不定长字符串来表示记录，格式根TYPE和CLASS有关。比如，TYPE是A，CLASS 是 IN，那么RDATA就是一个4个字节的ARPA网络地址。
    - 每次请求的ID是不一样的，在cache中判断是否存在的时候不能比较ID，应该比较QName，QType，QClass等。
    - 一个query的多个answer的TTL取最小的
    - 用wireshark的时候，尽量关掉别的应用，防止其他应用干扰。
    - 可以使用断网测试判断DNS server的cache时候正常运行。