

Southern University of Science and Technology

Computer Networking Lab Report

Name: 吴培霖 Student Number: 11711717

Major: None

Time: 2018/10/18

Introduction:

Assignment 5.1

- make an DNS query which will invoke the EDNS0
 - Screenshot on this command and its output
- capture the packages by Wireshark
 - What's the content of this query message
 - Find the name, type and class of this query.
 - How can you tell this DNS query is based on EDNS0
 - From this query message, can it handle DNSSEC security RRs or not
 - What's response content
 - Is there any answers, what's the ttl of each answer
 - Is there any authority RRs, what's the type of each RR
 - Is there any special additional RRs with OPT type, what does its 'Do bit' say: Does it accept DNSSEC security RRs or not

Assignment 5.2

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

– To query the type A value of www.163.com based on TCP and UDP stream respectively

- 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

– Screenshot on the TCP stream of query by TCP.

how many TCP packets are captured in this stream, Which port is used?

– Screenshot on the UDP stream of query by UDP.

how many UDP packets are captured in this stream, Which port is used?

– Is there any difference on DNS query and response message while using TCP and

UDP respectively

Produce:

Assignment 5.1:

– **Screenshot on this command and its output**

First, open the cmd.exe, input the order “dig @ns2.sustc.edu.cn www.baidu.com +dnssec”, then we can take a screenshot (fig.1)

– **What’s the content of this query message**

• **Find the name, type and class of this query.**

Open the Wireshark, set the filter: “dns.qry.name==“www.baidu.com””.

Select the query item, then we can get the result showed in fig.2 and fig.3.

Then, we can get the answer:

The server name: www.baidu.com **Type:** A; **Class:** In

• **How can you tell this DNS query is based on EDNS0**

From this query, we can see “**Additional RRs: 1**” , and the content of Additional records: (from fig.4)

<Root>: type OPT

 Name: <Root>

 Type: OPT (41)

 UDP payload size: 4096

 Higher bits in extended RCODE: 0x00

 EDNS0 version: 0

 Z: 0x8000

 Data length: 12

 Option: COOKIE

which is based on the format of EDNS0.

• **From this query message, can it handle DNSSEC security RRs or not**

Z: 0x8000

 1... .. = DO bit: Accepts DNSSEC security RRs

 .000 0000 0000 0000 = Reserved: 0x0000 (fig.4)

The value of it tells us that it can handle DNSSEC security RRs.

– **What ‘s response content**

• **Is there any answers, what’s the ttl of each answer**

See from the fig.5, we can find the 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: 541

Data length: 15

CNAME: www.a.shifen.com

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: 14

Data length: 4

Address: 14.215.177.38

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: 14

Data length: 4

Address: 14.215.177.38

There three answers, each answer's ttl is 541, 14, 14.

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

From the fig.6, we can learn one of authority RR:

Authoritative nameservers

shifen.com: type NS, class IN, ns dns.baidu.com

Name: shifen.com

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 139189

Data length: 6

Name Server: dns.baidu.com

shifen.com: type NS, class IN, ns ns2.baidu.com

Name: shifen.com

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 139189

Data length: 6

Name Server: ns2.baidu.com

shifen.com: type NS, class IN, ns ns3.baidu.com

Name: shifen.com

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 139189
Data length: 6
Name Server: ns3.baidu.com
shifen.com: type NS, class IN, ns ns4.baidu.com
Name: shifen.com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 139189
Data length: 6
Name Server: ns4.baidu.com

The type of each RR are: NS, NS, NS, NS, NS.

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

Yes, there is an RRs with OPT type.

1... .. = DO bit: Accepts DNSSEC security RRs

Its do bit say: Accepts DNSSEC security RRs.

It accept DNSSEC security RRs.

Assignment 5.2:

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

– To query the type A value of www.163.com based on TCP and UDP stream

Use python to run this code:

```
import dns.resolver
dns.resolver.query('www.163.com','A',tcp=True)
dns.resolver.query('www.163.com','A',tcp=False)
```

then, we can get result from Wireshark.

– Screenshot on this two commands .

what’s the default transport lay protocol while invoke DNS query

Two commands are showed in fig.8.

The default transport lay protocol UDP.

– Screenshot on the TCP stream of query by TCP.

how many TCP packets are captured in this stream, Which port is used?

Two packets are captured in this stream.

The port used in the client is 53.

The port used in the server is 5627.

(see from the fig.9)

– Screenshot on the UDP stream of query by UDP.

how many UDP packets are captured in this stream, Which port is used?

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

The screenshot is showed by the fig10.

Two packets are capture in this stream.

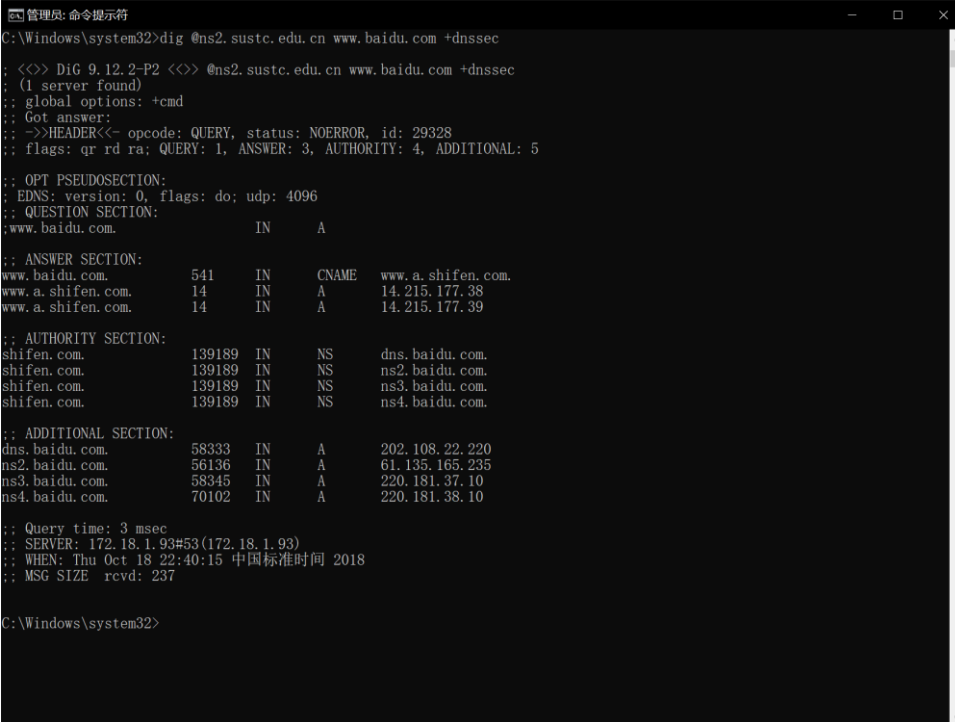
The port used in the server is 53.

The port used in the client is 63449.

There is no difference between the result of the query used by TCP and UDP, except the TCP query takes more time to get the response.

Result:

Assignment 5.1



```
管理员: 命令提示符
C:\Windows\system32>dig @ns2.sustc.edu.cn www.baidu.com +dnssec

<<>> DiG 9.12.2-P2 <<>> @ns2.sustc.edu.cn www.baidu.com +dnssec
(1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 29328
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 4, ADDITIONAL: 5

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

;; ANSWER SECTION:
www.baidu.com.        541     IN      CNAME   www.a.shifen.com.
www.a.shifen.com.     14      IN      A       14.215.177.38
www.a.shifen.com.     14      IN      A       14.215.177.39

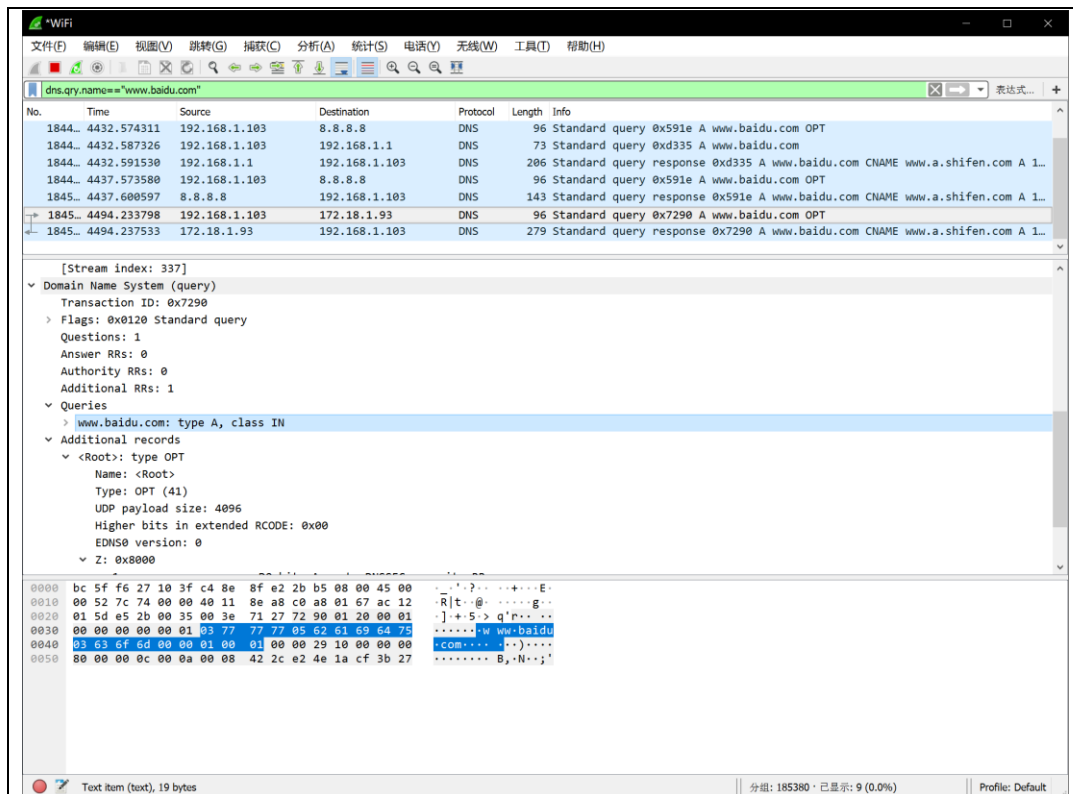
;; AUTHORITY SECTION:
shifen.com.           139189  IN      NS       dns.baidu.com.
shifen.com.           139189  IN      NS       ns2.baidu.com.
shifen.com.           139189  IN      NS       ns3.baidu.com.
shifen.com.           139189  IN      NS       ns4.baidu.com.

;; ADDITIONAL SECTION:
dns.baidu.com.        58333   IN      A       202.108.22.220
ns2.baidu.com.        56136   IN      A       61.135.165.235
ns3.baidu.com.        58345   IN      A       220.181.37.10
ns4.baidu.com.        70102   IN      A       220.181.38.10

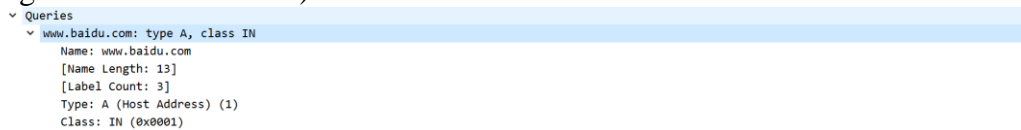
;; Query time: 3 msec
;; SERVER: 172.18.1.93#53(172.18.1.93)
;; WHEN: Thu Oct 18 22:40:15 中国标准时间 2018
;; MSG SIZE  rcvd: 237

C:\Windows\system32>
```

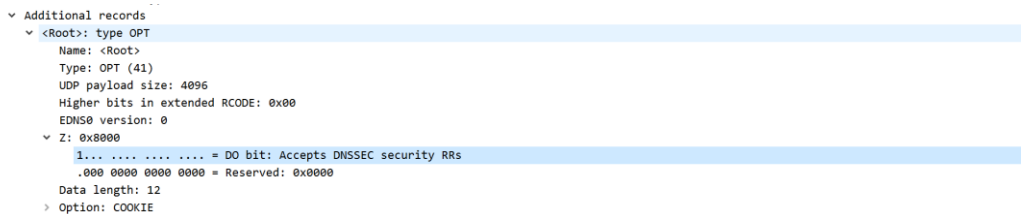
(fig.1 command and its output)



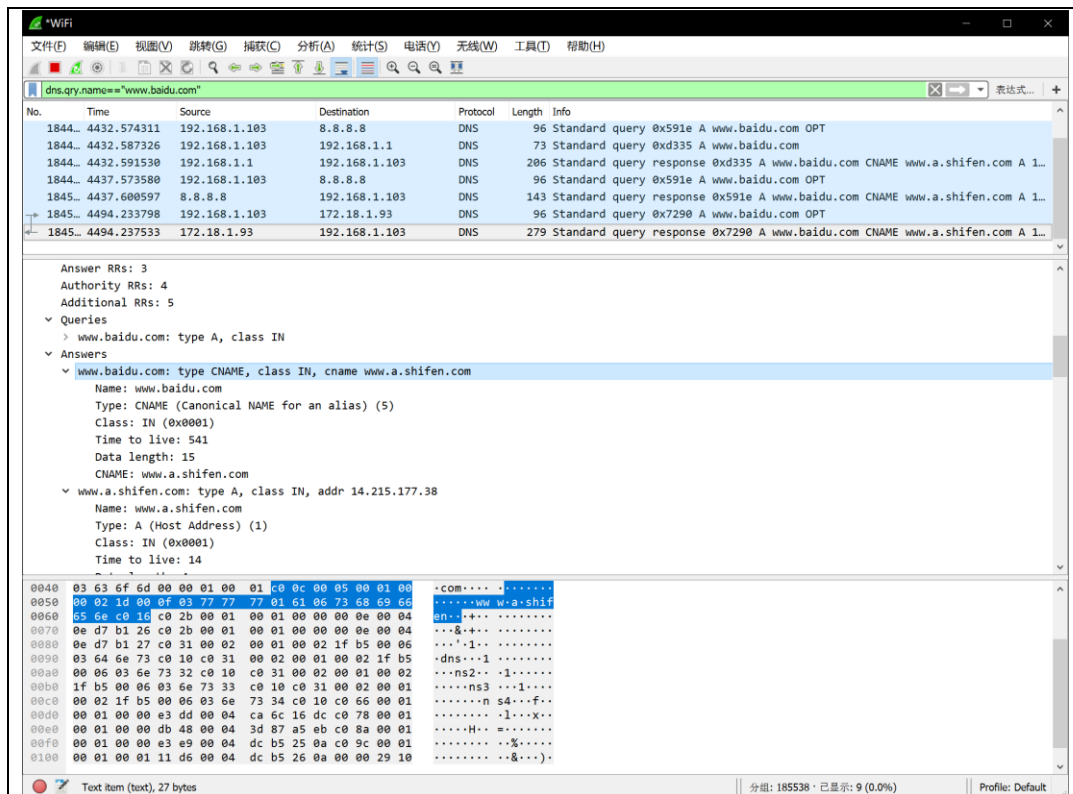
(fig.2 Wireshark's result)



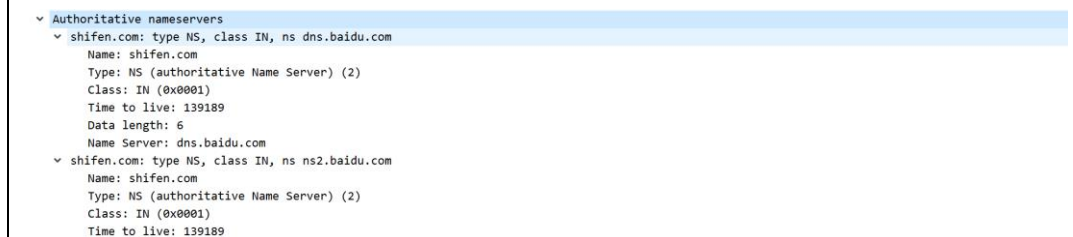
(fig.3 The content of query)



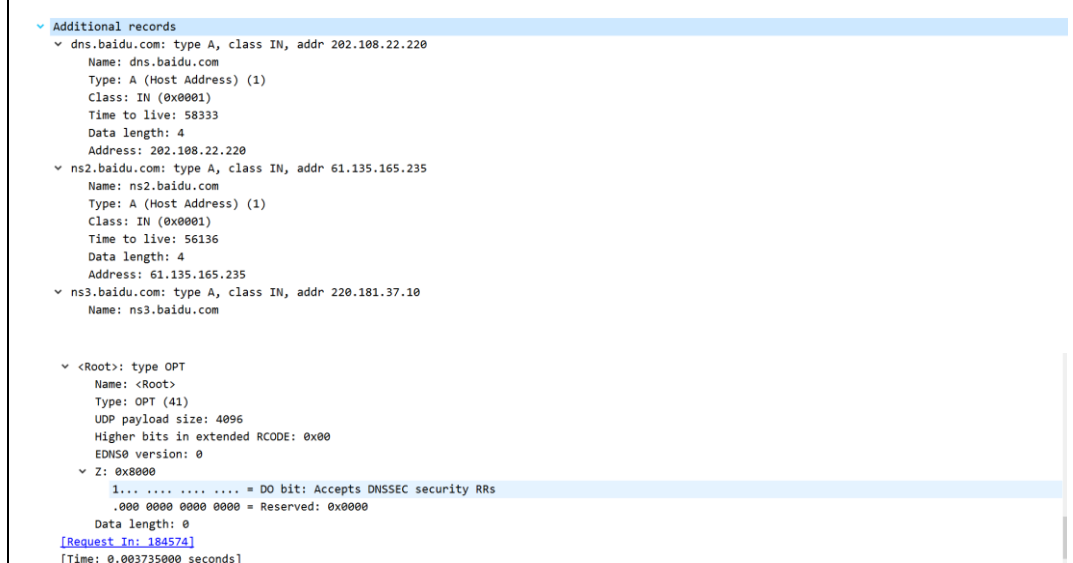
(fig.4 The content of additional records)



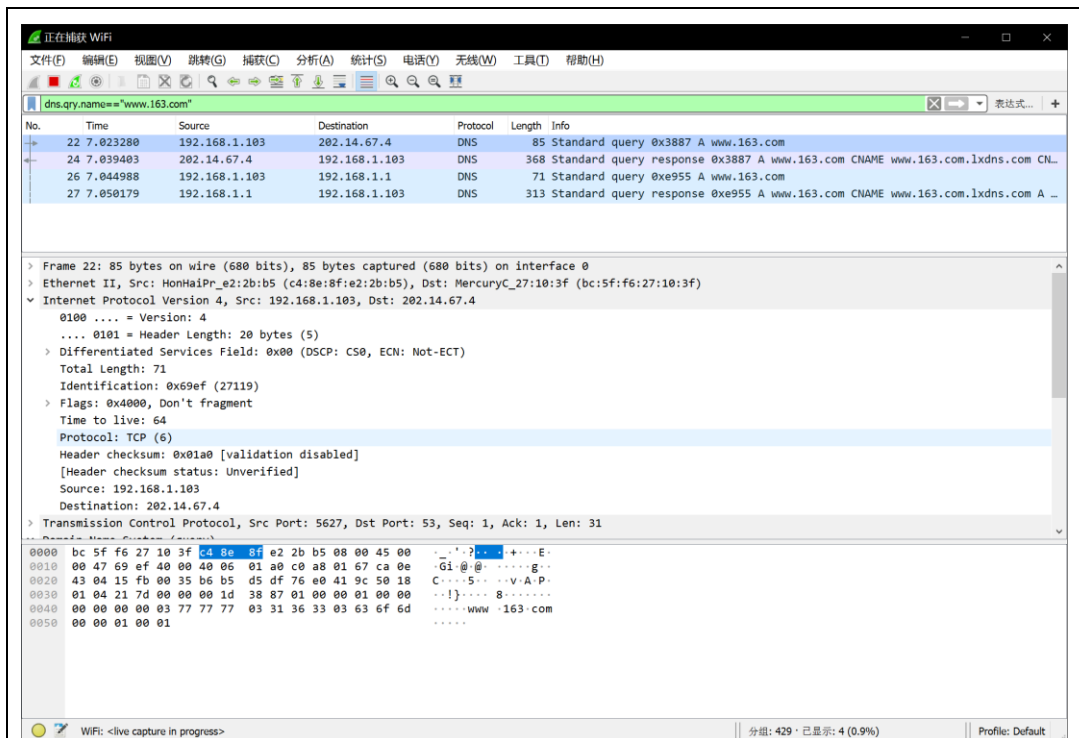
(fig.5 The answers of response)



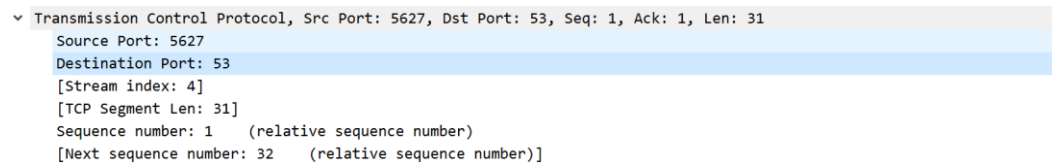
(fig.6 The authority RRs)



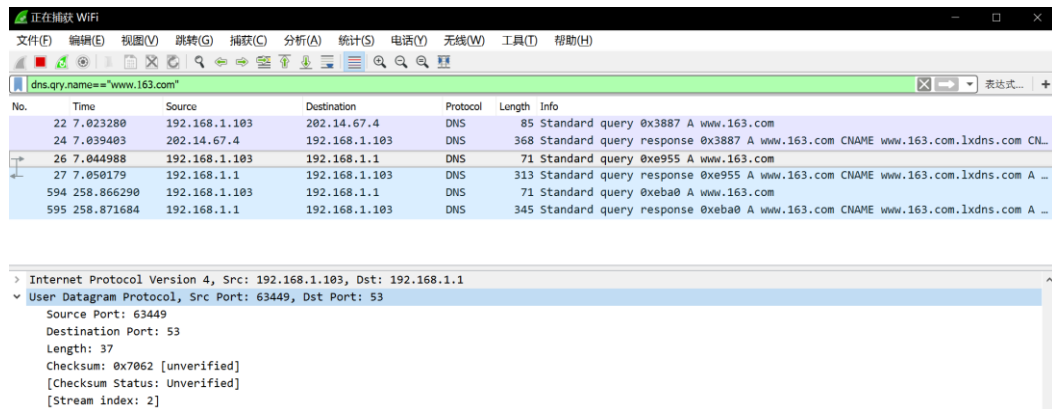
(fig.7 The additional records)



(fig.8 two commands captured by Wireshark)



(fig.9 The connection info about the TCP query)



(fig.10 The connection info about the UDP query)

Analysis(including answer of question):**Conclusion and Experience:**

From the assignments, we learn the structure of the dns query and response and the knowledge about EDNS and DNSSEC.

Tips: