Southern University of Science and Technology

Computer Networking Lab Report

唐润哲 11710418

- ***Introduction：***

  #Lab5.1

  - make an DNS query which will invoke the EDNS0
    - Screenshot on this command and its output
  - capture the packages using Wireshark
    - what is 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 massage , can it handle DNSSEC security RRs or not
    - what is the content of this response message
      - ✓ 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

  #Lab5.2

- 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
- 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

- ***Procedure***

  #Lab5.1

  ① Open terminal to dig @ns2.sustech.edu.cn www.google.com

  ② Use wireshark to capture packages

  #Lab5.2

  ① Make the query by using query method of “dns resolver”

  ②capture the related TCP stream and UDP stream using Wireshark

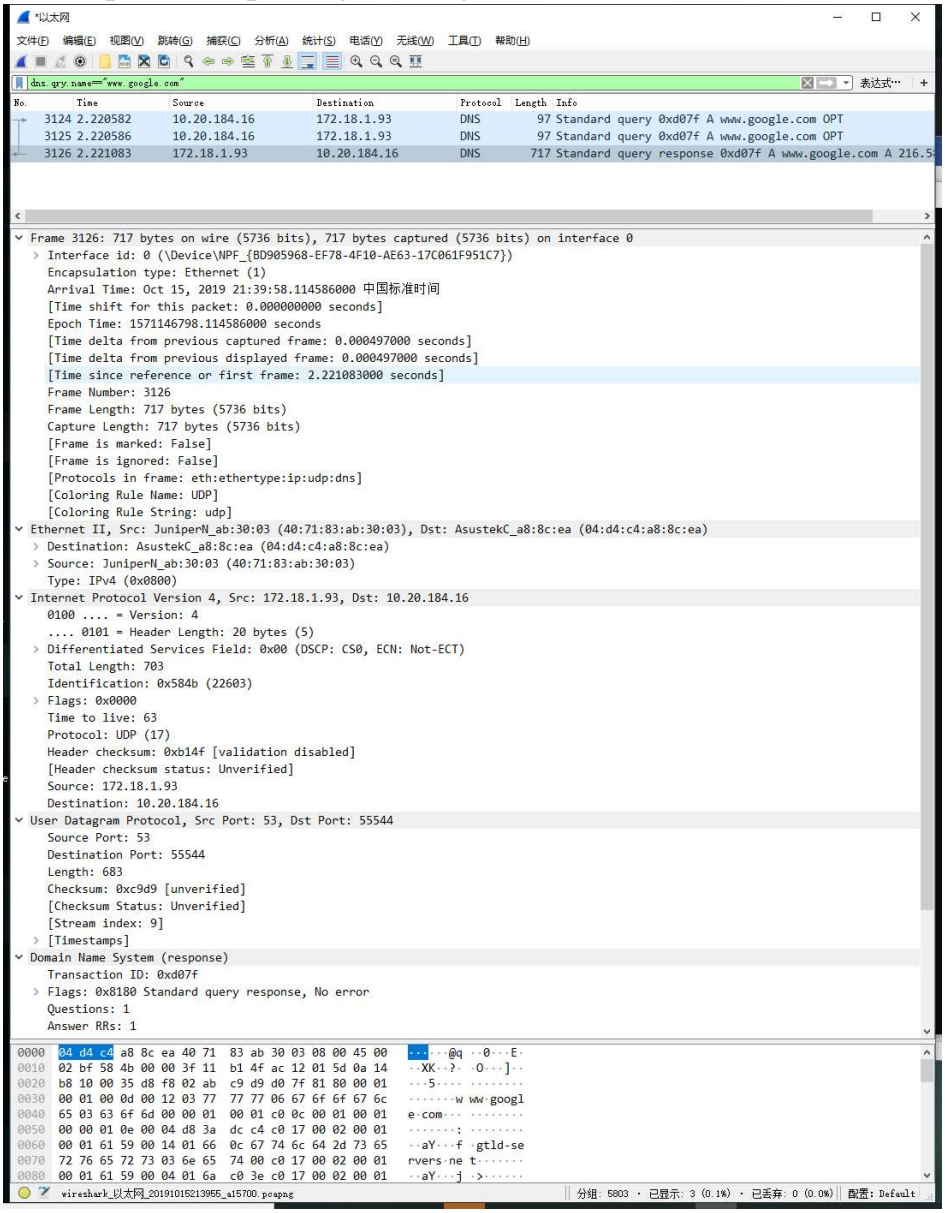
- ***Result：***

  #Lab5.1

  ➢ make an DNS query which will invoke the EDNS0

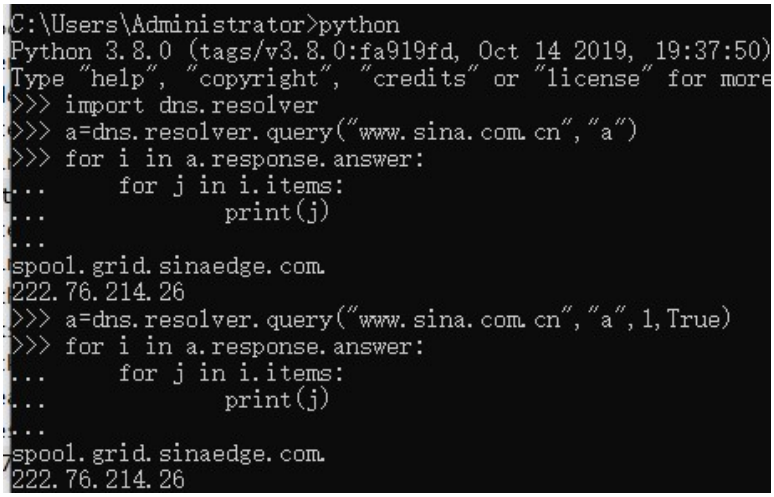
```
C:\Users\Administrator>dig @ns2.sustech.edu.cn www.google.com

; <<>> DiG 9.14.6 <<>> @ns2.sustech.edu.cn www.google.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31702
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 13, ADDITIONAL: 18

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

;; ANSWER SECTION:
www.google.com.         74      IN      A       216.58.220.196

;; AUTHORITY SECTION:
com.                    90637   IN      NS      f.gtld-servers.net.
com.                    90637   IN      NS      h.gtld-servers.net.
com.                    90637   IN      NS      e.gtld-servers.net.
com.                    90637   IN      NS      j.gtld-servers.net.
com.                    90637   IN      NS      i.gtld-servers.net.
com.                    90637   IN      NS      d.gtld-servers.net.
com.                    90637   IN      NS      c.gtld-servers.net.
com.                    90637   IN      NS      m.gtld-servers.net.
com.                    90637   IN      NS      k.gtld-servers.net.
com.                    90637   IN      NS      a.gtld-servers.net.
com.                    90637   IN      NS      l.gtld-servers.net.
com.                    90637   IN      NS      b.gtld-servers.net.
com.                    90637   IN      NS      g.gtld-servers.net.

;; ADDITIONAL SECTION:
a.gtld-servers.net.     5006    IN      A       192.5.6.30
a.gtld-servers.net.     10792   IN      AAAA    2001:503:a83e::2:30
b.gtld-servers.net.     129949  IN      AAAA    2001:503:231d::2:30
c.gtld-servers.net.     5468    IN      A       192.26.92.30
c.gtld-servers.net.     34565   IN      AAAA    2001:503:83eb::30
d.gtld-servers.net.     30922   IN      A       192.31.80.30
d.gtld-servers.net.     33412   IN      AAAA    2001:500:856e::30
e.gtld-servers.net.     48775   IN      AAAA    2001:502:1ca1::30
h.gtld-servers.net.     38877   IN      A       192.54.112.30
h.gtld-servers.net.     17745   IN      AAAA    2001:502:8cc::30
i.gtld-servers.net.     6400    IN      A       192.43.172.30
i.gtld-servers.net.     8946    IN      AAAA    2001:503:39c1::30
j.gtld-servers.net.     35102   IN      A       192.48.79.30
j.gtld-servers.net.     29066   IN      AAAA    2001:502:7094::30
l.gtld-servers.net.     129627  IN      AAAA    2001:500:d937::30
m.gtld-servers.net.     9309    IN      A       192.55.83.30
m.gtld-servers.net.     16586   IN      AAAA    2001:501:b1f9::30

;; Query time: 0 msec
;; SERVER: 172.18.1.93#53(172.18.1.93)
;; WHEN: Tue Oct 15 21:36:58 中国标准时间 2019
;; MSG SIZE  rcvd: 675
```

- capture the packages using Wireshark



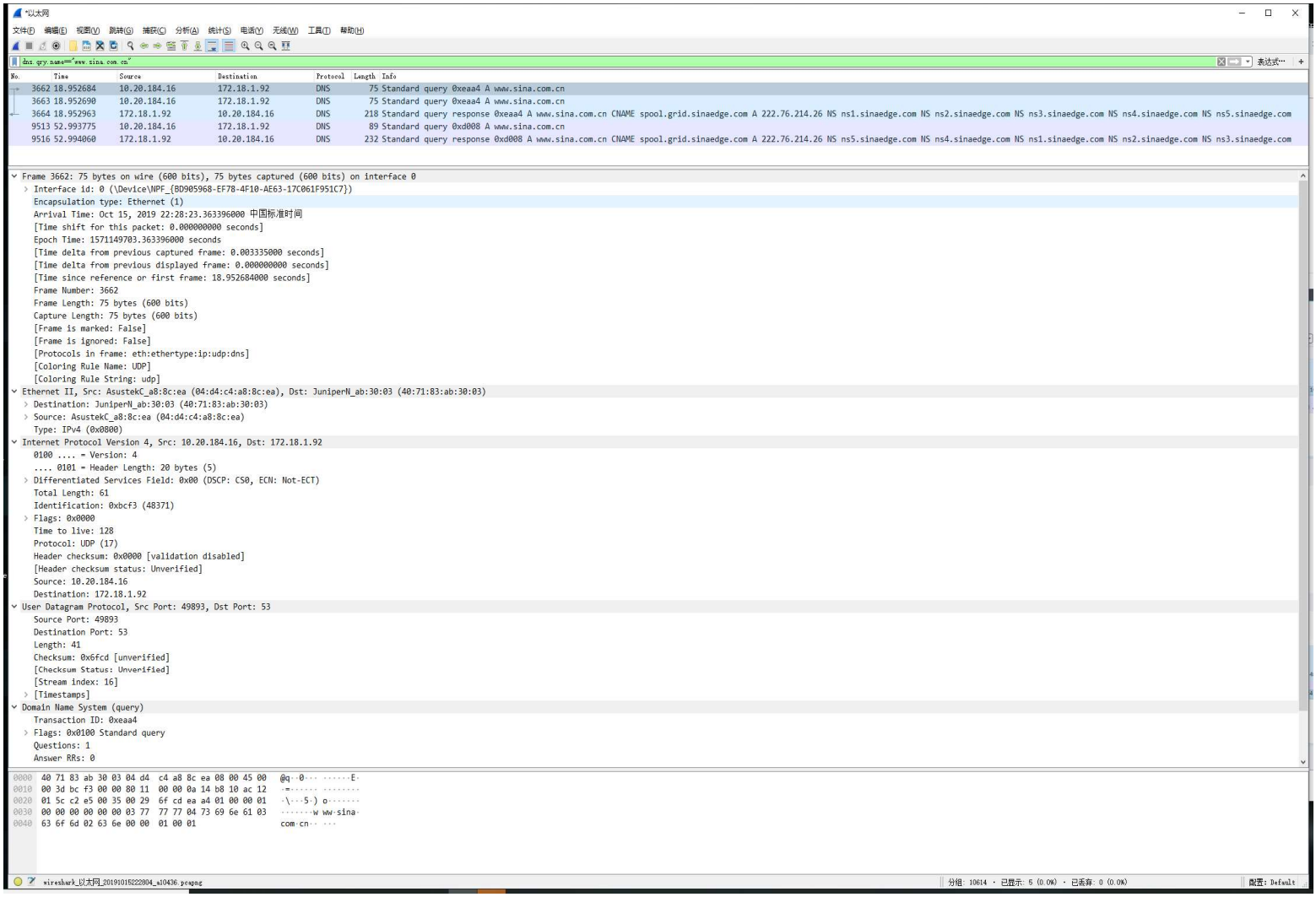
#Lab5.2

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



```
C:\Users\Administrator>python
Python 3.8.0 (tags/v3.8.0:fa919fd, Oct 14 2019, 19:37:50)
Type "help", "copyright", "credits" or "license" for more
>>> import dns.resolver
>>> a=dns.resolver.query("www.sina.com.cn","a")
>>> for i in a.response.answer:
...     for j in i.items:
...             print(j)
...
spool.grid.sinaedge.com.
222.76.214.26
>>> a=dns.resolver.query("www.sina.com.cn","a",1,True)
>>> for i in a.response.answer:
...     for j in i.items:
...             print(j)
...
spool.grid.sinaedge.com.
222.76.214.26
```

- capture the related TCP stream and UDP stream using Wireshark



- ***Conclusion and Experience：***
  #Lab5.1
  - *make an DNS query which will invoke the EDNS0*
    Answer: The screenshot is shown above.
  - *capture the packages using Wireshark*
    - *what is the content of this query message*
      - ✓ *Find the name, type and class of this query*
        Answer:
        1. *Name: www.google.com*
        2. *Type: A(Type: AAAA for IPv6 Address)*
        3. *Class: In*

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

  Answer: <Root>:type OPT can be found in the Additional records

```
Additional records
  > a.gtld-servers.net: type A, class IN, addr 192.5.6.30
  > a.gtld-servers.net: type AAAA, class IN, addr 2001:503:a83e::2:30
  > b.gtld-servers.net: type AAAA, class IN, addr 2001:503:231d::2:30
  > c.gtld-servers.net: type A, class IN, addr 192.26.92.30
  > c.gtld-servers.net: type AAAA, class IN, addr 2001:503:83eb::30
  > d.gtld-servers.net: type A, class IN, addr 192.31.80.30
  > d.gtld-servers.net: type AAAA, class IN, addr 2001:500:856e::30
  > e.gtld-servers.net: type AAAA, class IN, addr 2001:502:1ca1::30
  > h.gtld-servers.net: type A, class IN, addr 192.54.112.30
  > h.gtld-servers.net: type AAAA, class IN, addr 2001:502:8cc::30
  > i.gtld-servers.net: type A, class IN, addr 192.43.172.30
  > i.gtld-servers.net: type AAAA, class IN, addr 2001:503:39c1::30
  > j.gtld-servers.net: type A, class IN, addr 192.48.79.30
  > j.gtld-servers.net: type AAAA, class IN, addr 2001:502:7094::30
  > l.gtld-servers.net: type AAAA, class IN, addr 2001:500:d937::30
  > m.gtld-servers.net: type A, class IN, addr 192.55.83.30
  > m.gtld-servers.net: type AAAA, class IN, addr 2001:501:b1f9::30
  > <Root>: type OPT
```

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

  Answer: It can not handle DNSSEC security RRs

```
<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: 0
```

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

    Answer: The ttl of each answer is 270

```
Answers
  www.google.com: type A, class IN, addr 216.58.220.196
    Name: www.google.com
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 270
    Data length: 4
    Address: 216.58.220.196
```

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

Answer: There are several authority RRs, and their types are NS(authoritative Name Server)

```
Authoritative nameservers
  com: type NS, class IN, ns f.gtld-servers.net
      Name: com
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 90457
      Data length: 20
      Name Server: f.gtld-servers.net
  com: type NS, class IN, ns j.gtld-servers.net
  com: type NS, class IN, ns m.gtld-servers.net
  com: type NS, class IN, ns k.gtld-servers.net
  com: type NS, class IN, ns g.gtld-servers.net
  com: type NS, class IN, ns d.gtld-servers.net
```

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

  Answer: There is one special additional RRs with OPT type ,and it does not accept DNSSEC security RRs

```
<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: 0
```

#Lab5.2

- 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

    Answer: The screenshot above is the result.

    UDP stream: dns.resolver.query("www.sina.com.cn","a")

    TCP stream:dns.resolver.query("www. sina.com.cn ","a",1,"True")

- capture the related TCP stream and UDP stream using Wireshark
  - Screenshot on this two commands .
    Answer: The screenshot above is the result.
    what's the default transport lay protocol while invoke DNS query
    Answer: The default transport lay protocol is UDP.

  - Screenshot on the TCP stream of query by TCP.
    Answer: The screenshots are shown below(red lines)

9513	52.993775	10.20.184.16	172.18.1.92	DNS	89	Standard query 0xd008 A www.sina.com.cn
3664	18.952963	172.18.1.92	10.20.184.16	DNS	218	Standard query response 0xeaa4 A www.sina.
9516	52.994060	172.18.1.92	10.20.184.16	DNS	232	Standard query response 0xd008 A www.sina.

```
> Frame 9516: 232 bytes on wire (1856 bits), 232 bytes captured (1856 bits) on interface 0
> Ethernet II, Src: JuniperN_ab:30:03 (40:71:83:ab:30:03), Dst: AsustekC_a8:8c:ea (04:d4:c4:a8:8c:ea)
> Internet Protocol Version 4, Src: 172.18.1.92, Dst: 10.20.184.16
> Transmission Control Protocol, Src Port: 53, Dst Port: 13708, Seq: 1, Ack: 36, Len: 178
> Domain Name System (response)
```

how many TCP packets are captured in this stream, Which port is used?
Answer: 2 TCP packets are captured.
The port used by DNS Server is 53.

  - Screenshot on the UDP stream of query by UDP.
    Answer: The screenshots are shown below(blue lines)

3662	18.952684	10.20.184.16	172.18.1.92	DNS	75	Standard query 0xeaa4 A www.sina.com.cn
3663	18.952690	10.20.184.16	172.18.1.92	DNS	75	Standard query 0xeaa4 A www.sina.com.cn
9513	52.993775	10.20.184.16	172.18.1.92	DNS	89	Standard query 0xd008 A www.sina.com.cn
3664	18.952963	172.18.1.92	10.20.184.16	DNS	218	Standard query response 0xeaa4 A www.sina

```
> Frame 3664: 218 bytes on wire (1744 bits), 218 bytes captured (1744 bits) on interface 0
> Ethernet II, Src: JuniperN_ab:30:03 (40:71:83:ab:30:03), Dst: AsustekC_a8:8c:ea (04:d4:c4:a8:8c:ea)
> Internet Protocol Version 4, Src: 172.18.1.92, Dst: 10.20.184.16
> User Datagram Protocol, Src Port: 53, Dst Port: 49893
> Domain Name System (response)
```

how many UDP packets are captured in this stream, Which port is used?
Answer: 2 UCP packets are captured.
The port used by DNS Server is 53.
(Attention: As shown in the screenshot below, an error happened so a dns query retransmission is acted,so in the screenshot above,there are 3 UDP packets.

```
v Domain Name System (query)
  v Transaction ID: 0xeaa4
    > [Expert Info (Warning/Protocol): DNS query retransmission. Original request in frame 3662]
```

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

  Answer: From screenshots below, we can know that when we use TCP, we will get packets' length ,which can not be transferred by UDP.

  - Query:

    - ✓ UDP:

No.	Time	Source	Destination	Protocol	Length	Info
3662	18.952684	10.20.184.16	172.18.1.92	DNS	75	Standard query 0xeaa4 A www.sina.com.cn
3663	18.952690	10.20.184.16	172.18.1.92	DNS	75	Standard query 0xeaa4 A www.sina.com.cn
9513	52.993775	10.20.184.16	172.18.1.92	DNS	89	Standard query 0xd008 A www.sina.com.cn
3664	18.952963	172.18.1.92	10.20.184.16	DNS	218	Standard query response 0xeaa4 A www.sin
9516	52.994060	172.18.1.92	10.20.184.16	DNS	232	Standard query response 0xd008 A www.sin

```
> Frame 3662: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 0
> Ethernet II, Src: AsustekC_a8:8c:ea (04:d4:c4:a8:8c:ea), Dst: JuniperN_ab:30:03 (40:71:83:ab:30:03)
> Internet Protocol Version 4, Src: 10.20.184.16, Dst: 172.18.1.92
> User Datagram Protocol, Src Port: 49893, Dst Port: 53
> Domain Name System (query)
```

    - ✓ TCP:

No.	Time	Source	Destination	Protocol	Length	Info
3662	18.952684	10.20.184.16	172.18.1.92	DNS	75	Standard query 0xeaa4 A www.sina.com.cn
3663	18.952690	10.20.184.16	172.18.1.92	DNS	75	Standard query 0xeaa4 A www.sina.com.cn
9513	52.993775	10.20.184.16	172.18.1.92	DNS	89	Standard query 0xd008 A www.sina.com.cn
3664	18.952963	172.18.1.92	10.20.184.16	DNS	218	Standard query response 0xeaa4 A www.sina
9516	52.994060	172.18.1.92	10.20.184.16	DNS	232	Standard query response 0xd008 A www.sina

```
> Frame 9513: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface 0
> Ethernet II, Src: AsustekC_a8:8c:ea (04:d4:c4:a8:8c:ea), Dst: JuniperN_ab:30:03 (40:71:83:ab:30:03)
> Internet Protocol Version 4, Src: 10.20.184.16, Dst: 172.18.1.92
> Transmission Control Protocol, Src Port: 13708, Dst Port: 53, Seq: 1, Ack: 1, Len: 35
> Domain Name System (query)
```

  - Response:

    - ✓ UDP:

No.	Time	Source	Destination	Protocol	Length	Info
3662	18.952684	10.20.184.16	172.18.1.92	DNS	75	Standard query 0xeaa4 A www.sina.com.cn
3663	18.952690	10.20.184.16	172.18.1.92	DNS	75	Standard query 0xeaa4 A www.sina.com.cn
9513	52.993775	10.20.184.16	172.18.1.92	DNS	89	Standard query 0xd008 A www.sina.com.cn
3664	18.952963	172.18.1.92	10.20.184.16	DNS	218	Standard query response 0xeaa4 A www.sin
9516	52.994060	172.18.1.92	10.20.184.16	DNS	232	Standard query response 0xd008 A www.sin

```
> Frame 3664: 218 bytes on wire (1744 bits), 218 bytes captured (1744 bits) on interface 0
> Ethernet II, Src: JuniperN_ab:30:03 (40:71:83:ab:30:03), Dst: AsustekC_a8:8c:ea (04:d4:c4:a8:8c:ea)
> Internet Protocol Version 4, Src: 172.18.1.92, Dst: 10.20.184.16
> User Datagram Protocol, Src Port: 53, Dst Port: 49893
> Domain Name System (response)
```

    - ✓ TCP:

No.	Time	Source	Destination	Protocol	Length	Info
3662	18.952684	10.20.184.16	172.18.1.92	DNS	75	Standard query 0xeaa4 A www.sina.com.cn
3663	18.952690	10.20.184.16	172.18.1.92	DNS	75	Standard query 0xeaa4 A www.sina.com.cn
9513	52.993775	10.20.184.16	172.18.1.92	DNS	89	Standard query 0xd008 A www.sina.com.cn
3664	18.952963	172.18.1.92	10.20.184.16	DNS	218	Standard query response 0xeaa4 A www.sina
9516	52.994060	172.18.1.92	10.20.184.16	DNS	232	Standard query response 0xd008 A www.sina

```
> Frame 9516: 232 bytes on wire (1856 bits), 232 bytes captured (1856 bits) on interface 0
> Ethernet II, Src: JuniperN_ab:30:03 (40:71:83:ab:30:03), Dst: AsustekC_a8:8c:ea (04:d4:c4:a8:8c:ea)
> Internet Protocol Version 4, Src: 172.18.1.92, Dst: 10.20.184.16
> Transmission Control Protocol, Src Port: 53, Dst Port: 13708, Seq: 1, Ack: 36, Len: 178
> Domain Name System (response)
```