

实验目的

对DNS查询消息跟响应消息进行抓包

实验内容

熟悉nslookup

nslookup是一种网络管理 命令行工具,可在许多计算机操作系统中使用,用于查询域名系统(DNS)以获得域名或IP地址映射或其他DNS记录。名称“nslookup”表示“名称服务器查找”。(维基百科)

第一个命令：

表示查询某个域名的IP地址

```
nslookup www.szu.edu.cn
nslookup www.mit.edu.cn
```

```
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
copyright@copyright-Vostro-3559:~$ nslookup www.szu.edu.cn
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.szu.edu.cn
Address: 210.39.12.247
Name:   www.szu.edu.cn
Address: 2001:250:3c00:212::166

copyright@copyright-Vostro-3559:~$ nslookup www.mit.edu
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
www.mit.edu      canonical name = www.mit.edu.edgekey.net.
www.mit.edu.edgekey.net canonical name = e9566.dscb.akamaiedge.net.
Name:   e9566.dscb.akamaiedge.net
Address: 2.21.208.39
Name:   e9566.dscb.akamaiedge.net
Address: 2001:418:143c:189::255e
Name:   e9566.dscb.akamaiedge.net
Address: 2001:418:143c:19e::255e
```

- 黄色框
 - 本地DNS服务器名称: 127.0.0.53
 - 本地DNS服务器地址和端口号: 127.0.0.53#53
- 绿色框
 - 主机名: www.szu.edu.cn
 - IPV4地址: 210.39.12.247
 - IPV6地址: 2001:250:3c00:212::166

第二个命令：

DNS的资源记录格式：

❖资源记录(RR, resource records)

RR format: (name, value, type, ttl)

❖Type=A

- Name: 主机域名
- Value: IP地址

❖Type=NS

- Name: 域(edu.cn)
- Value: 该域权威域名解析服务的主机域名

❖Type=CNAME

- Name: 某一真实域名的别名
 - www.ibm.com –
servereast.backup2.ibm.com
- Value: 真实域名

❖Type=MX

- Value是与name相对应的邮件服务器

默认情况下不指定的话是 type=A (看前面的查询结果也可以推断出这个结论)。 type=NS 换句话说的意思就是 请给我发送mit.edu的权威DNS的主机名。

命令行输入：

```
nslookup -type=NS mit.edu
```

```
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
copyright@copyright-Vostro-3559:~$ nslookup -type=NS mit.edu
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
mit.edu nameserver = eur5.akam.net.
mit.edu nameserver = usw2.akam.net.
mit.edu nameserver = use5.akam.net.
mit.edu nameserver = use2.akam.net.
mit.edu nameserver = asia1.akam.net.
mit.edu nameserver = ns1-37.akam.net.
mit.edu nameserver = ns1-173.akam.net.
mit.edu nameserver = asia2.akam.net.

Authoritative answers can be found from:

copyright@copyright-Vostro-3559:~$
```

黄色框中表示 mit.edu 的权威域名服务器的主机名字。

第三个命令：

这次是利用 eur5.akam.net 这个上个命令查询到的DNS服务器主机告诉我们 www.aiit.or.kr 这个主机的IP地址,因为之前都是向本地的DNS服务器（比如我的是 127.0.0.53）查询某个主机的IP地址。

```
nslookup www.aiit.or.kr eur5.akam.net
```

```
copyright@copyright-Vostro-3559:~$ nslookup www.aiit.or.krbitsy.mit.edu
Server:      127.0.0.53
Address:     127.0.0.53#53

** server can't find www.aiit.or.krbitsy.mit.edu: NXDOMAIN

copyright@copyright-Vostro-3559:~$ nslookup www.aiit.or.kr bitsy.mit.edu
;; connection timed out; no servers could be reached
```

貌似查不到，可能是因为 qiang 的原因？

问题不大，让我们查查深大的

```
nslookup -type=NS szu.edu.cn
nslookup www.szu.edu.cn bay.szu.edu.cn
nslookup www.szu.edu.cn sea.szu.edu.cn
```

```
copyright@copyright-Vostro-3559:~$ nslookup -type=NS szu.edu.cn
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
szu.edu.cn   nameserver = bay.szu.edu.cn.
szu.edu.cn   nameserver = sea.szu.edu.cn.

Authoritative answers can be found from:
```

查到两个DNS服务器主机的名字

```
copyright@copyright-Vostro-3559:~$ nslookup www.szu.edu.cn bay.szu.edu.cn
Server:      bay.szu.edu.cn
Address:     210.39.0.33#53

Name:   www.szu.edu.cn
Address: 210.39.12.247
Name:   www.szu.edu.cn
Address: 2001:250:3c00:212::166

copyright@copyright-Vostro-3559:~$ nslookup www.szu.edu.cn sea.szu.edu.cn
Server:      sea.szu.edu.cn
Address:     210.39.0.34#53

Name:   www.szu.edu.cn
Address: 210.39.12.247
Name:   www.szu.edu.cn
Address: 2001:250:3c00:212::166
```

红框里面可以看到我们查询 `www.szu.edu.cn` 这个主机的IP地址的时候，用的域名服务器分别是指定的 `bay.szu.edu.cn`，`sea.szu.edu.cn`。

回答问题：

1.运行nslookup以获取一个亚洲的Web服务器的IP地址。该服务器的IP地址是什么？

```
copyright@copyright-Vostro-3559:~$ nslookup www.google.hk.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   www.google.hk.com
Address: 202.81.238.12
```

查询的Web服务器是www.google.hk.com，IP地址是202.81.238.12

2.运行nslookup来确定一个欧洲的大学的权威DNS服务器。

```
copyright@copyright-Vostro-3559:~$ nslookup -type=NS ox.ac.uk
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
ox.ac.uk      nameserver = dns1.ox.ac.uk.
ox.ac.uk      nameserver = ns2.ja.net.
ox.ac.uk      nameserver = auth5.dns.ox.ac.uk.
ox.ac.uk      nameserver = auth4.dns.ox.ac.uk.
ox.ac.uk      nameserver = dns2.ox.ac.uk.
ox.ac.uk      nameserver = auth6.dns.ox.ac.uk.
ox.ac.uk      nameserver = dns0.ox.ac.uk.

Authoritative answers can be found from:
```

查询的是英国牛津大学的权威DNS服务器

3.运行nslookup,使用问题2中一个已获得的DNS服务器,来查询Yahoo!邮箱的邮件服务器。它的IP地址是什么?

```
copyright@copyright-Vostro-3559:~$ nslookup mail.yahoo.com dns1.ox.ac.uk
Server:      dns1.ox.ac.uk
Address:     129.67.1.191#53

** server can't find mail.yahoo.com: REFUSED
```

我输入的是nslookup mail.yahoo.com dns1.ox.ac.uk，但是查不到，不知道是什么原因，如果是直接查的话是可以查到雅虎的邮箱地址是87.248.114.11或者是87.248.114.11

```
copyright@copyright-Vostro-3559:~$ nslookup mail.yahoo.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
mail.yahoo.com canonical name = edge.gycpi.b.yahoodns.net.
Name:   edge.gycpi.b.yahoodns.net
Address: 87.248.114.12
Name:   edge.gycpi.b.yahoodns.net
Address: 87.248.114.11
Name:   edge.gycpi.b.yahoodns.net
Address: 2a00:1288:80:800::7001
Name:   edge.gycpi.b.yahoodns.net
Address: 2a00:1288:80:800::7000
```

熟悉ifconfig

之前[博客](#)有写过就不多说了

清除dns缓存

ubuntu

在网上看到有很多说法，所以我选择这位[博主](#)的说法试了一下

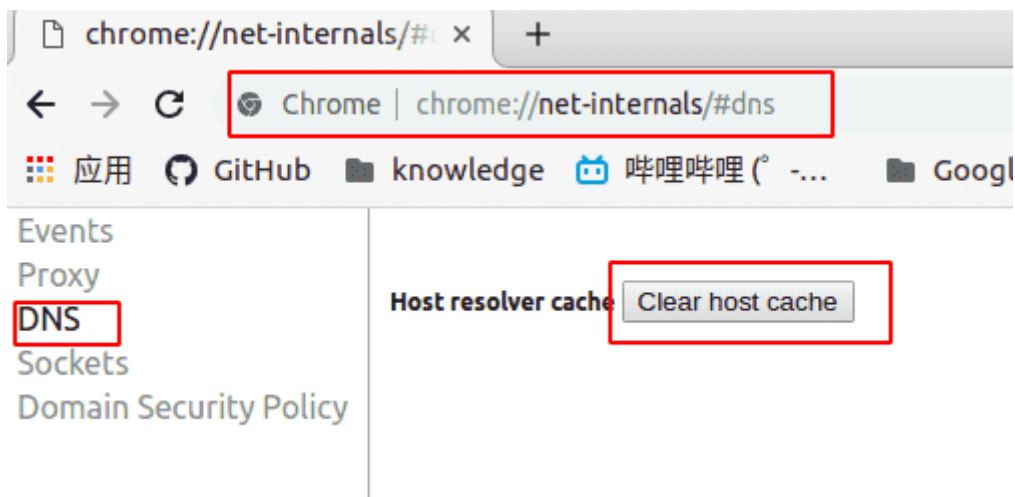
DNS缓存可以加快网站IP的解析速度，所以大多数系统都支持DNS缓存。DNS的缓存时间是24小时，也就是每隔24小时DNS缓存将被自动清除。如果某些网站更新了DNS信息，而本机又没到自动清除的时间，这时，我们就要手动清除DNS缓存，最简单的方法如下。

```
$sudo /etc/init.d/dns-clean start
```

```
active
copyright@copyright-Vostro-3559:~$ sudo /etc/init.d/dns-clean start
Running 0dns-down to make sure resolv.conf is ok...done.
copyright@copyright-Vostro-3559:~$
```

浏览器

- 1、打开Google Chrome浏览器，输入chrome://net-internals/#dns打开页面。
- 2、点击右边的Clear host cache按钮就可以删除谷歌Chrome浏览器DNS缓存了



wireshark追踪DNS

追踪DNS

如上所述先清除主机跟浏览器的缓存后，打开浏览器，查询自己的IP地址，（当前我的IP地址是192.168.1.103），然后打开Wiresharks，在过滤设置那里输入`id.addr==192.168.1.103`，然后开始捕获，在浏览器输入深大的主页 `www.szu.edu.cn`。

No.	Time	Source	Destination	Protocol	Length	Info
1	2020-04-28 22:27:01.307329900	Tp-LinkT_b2:a6:cc	Broadcast	ARP	42	Who has 192.168.1.147? T
2	2020-04-28 22:27:01.309852889	Tp-LinkT_b2:a6:cc	Broadcast	ARP	42	Who has 192.168.1.147? T
3	2020-04-28 22:27:01.310841536	Tp-LinkT_b2:a6:cc	Broadcast	ARP	42	Who has 192.168.1.147? T
4	2020-04-28 22:27:01.311732118	Tp-LinkT_b2:a6:cc	Broadcast	ARP	42	Who has 192.168.1.147? T
5	2020-04-28 22:27:01.312700187	Tp-LinkT_b2:a6:cc	Broadcast	ARP	42	Who has 192.168.1.147? T
6	2020-04-28 22:27:01.313624850	Tp-LinkT_b2:a6:cc	Broadcast	ARP	42	Who has 192.168.1.147? T
7	2020-04-28 22:27:03.457648790	192.168.1.104	224.0.0.251	MDNS	247	Standard query response

回答问题：

4.找到DNS查询和响应消息，它们是否通过UDP或TCP发送？

No.	Time	Source	Destination	Protocol	Length	Info
345	2020-04-28 22:39:17.768566623	192.168.1.103	202.96.128.166	DNS	74	Standard query 0x080b A www.szu.edu
346	2020-04-28 22:39:17.786497481	202.96.128.166	192.168.1.103	DNS	198	Standard query response 0x080b A ww

Frame 346: 198 bytes on wire (1584 bits), 198 bytes captured (1584 bits) on interface 0
Ethernet II, Src: Tp-LinkT_b2:a6:cc (28:2c:b2:b2:a6:cc), Dst: IntelCor_11:2c:59 (9c:da:3e:11:2c:59)
Internet Protocol Version 4, Src: 202.96.128.166, Dst: 192.168.1.103
User Datagram Protocol, Src Port: 53, Dst Port: 41976
Domain Name System (response)

在过滤器输入`dns and ip.addr==192.168.1.103`，可以看到DNS是通过UDP发送的。

5.DNS查询消息的目标端口是什么？DNS响应消息的源端口是什么？

ip.addr==192.168.1.103						
No.	Time	Source	Destination	Protocol	Length	Info
3	2020-04-28 23:05:09.932449095	192.168.1.103	202.96.128.166	DNS	71	Standard
4	2020-04-28 23:05:09.955845675	202.96.128.166	192.168.1.103	DNS	484	Standard
5	2020-04-28 23:05:09.959252185	192.168.1.103	202.96.128.166	DNS	85	Standard
6	2020-04-28 23:05:09.978729570	202.96.128.166	192.168.1.103	DNS	465	Standard

Frame 3: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0	
Ethernet II, Src: IntelCor_11:2c:59 (9c:da:3e:11:2c:59), Dst: Tp-LinkT_b2:a6:cc (28:2c:b2:b2:a6:cc)	
Internet Protocol Version 4, Src: 192.168.1.103, Dst: 202.96.128.166	
User Datagram Protocol, Src Port: 54075, Dst Port: 53	
Source Port: 54075	
Destination Port: 53	
Length: 37	
Checksum: 0xbc23 [unverified]	
[Checksum Status: Unverified]	
[Stream index: 1]	
Domain Name System (query)	
Transaction ID: 0x104e	
Flags: 0x0100 Standard query	
Questions: 1	
Answer RRs: 0	
Authority RRs: 0	
Additional RRs: 0	
Queries	
[Response In: 4]	

dns and ip.addr==192.168.1.103						
No.	Time	Source	Destination	Protocol	Length	Info
345	2020-04-28 22:39:17.768566623	192.168.1.103	202.96.128.166	DNS	74	Standard query 0x080b A www.szu.edu
346	2020-04-28 22:39:17.786497481	202.96.128.166	192.168.1.103	DNS	198	Standard query response 0x080b A w
3881	2020-04-28 22:39:46.354061702	192.168.1.103	202.96.128.166	DNS	89	Standard query 0xdab2 A connectivi
3885	2020-04-28 22:39:46.374730753	202.96.128.166	192.168.1.103	DNS	233	Standard query response 0xdab2 A cc

Frame 346: 198 bytes on wire (1584 bits), 198 bytes captured (1584 bits) on interface 0	
Ethernet II, Src: Tp-LinkT_b2:a6:cc (28:2c:b2:b2:a6:cc), Dst: IntelCor_11:2c:59 (9c:da:3e:11:2c:59)	
Internet Protocol Version 4, Src: 202.96.128.166, Dst: 192.168.1.103	
User Datagram Protocol, Src Port: 53, Dst Port: 41976	
Source Port: 53	
Destination Port: 41976	
Length: 164	
Checksum: 0xbc2 [unverified]	
[Checksum Status: Unverified]	
[Stream index: 3]	
Domain Name System (response)	

查询消息是query,目标端口是53
响应消息是response,源端口是53

6.DNS查询消息发送到哪个IP地址?使用ipconfig来确定本地DNS服务器的IP地址。这两个IP地址是否相同？

dns and ip.addr==192.168.1.103						
No.	Time	Source	Destination	Protocol	Length	Info
345	2020-04-28 22:39:17.768566623	192.168.1.103	202.96.128.166	DNS	74	Standard query 0x080b A www.s
346	2020-04-28 22:39:17.786497481	202.96.128.166	192.168.1.103	DNS	198	Standard query response 0x080
3881	2020-04-28 22:39:46.354061702	192.168.1.103	202.96.128.166	DNS	89	Standard query 0xdab2 A conne
3885	2020-04-28 22:39:46.374730753	202.96.128.166	192.168.1.103	DNS	233	Standard query response 0xdab
4453	2020-04-28 22:43:05.044184443	192.168.1.103	202.96.128.166	DNS	79	Standard query 0xa5a6 A accou
4454	2020-04-28 22:43:05.044330775	192.168.1.103	202.96.128.166	DNS	79	Standard query 0xc5c4 AAAA ac
4460	2020-04-28 22:43:05.103615749	202.96.128.166	192.168.1.103	DNS	287	Standard query response 0xa5a
4461	2020-04-28 22:43:05.103652058	202.96.128.166	192.168.1.103	DNS	129	Standard query response 0xc5c
4468	2020-04-28 22:43:06.241697839	192.168.1.103	202.96.128.166	DNS	76	Standard query 0xbfd4 daisv


```
copyright@copyright-Vostro-3559:~$ cat /etc/resolv.conf
# This file is managed by man:systemd-resolved(8). Do not edit.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs must not access this file directly, but only through the
# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,
# replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.
nameserver 127.0.0.53
options edns0
copyright@copyright-Vostro-3559:~$
```

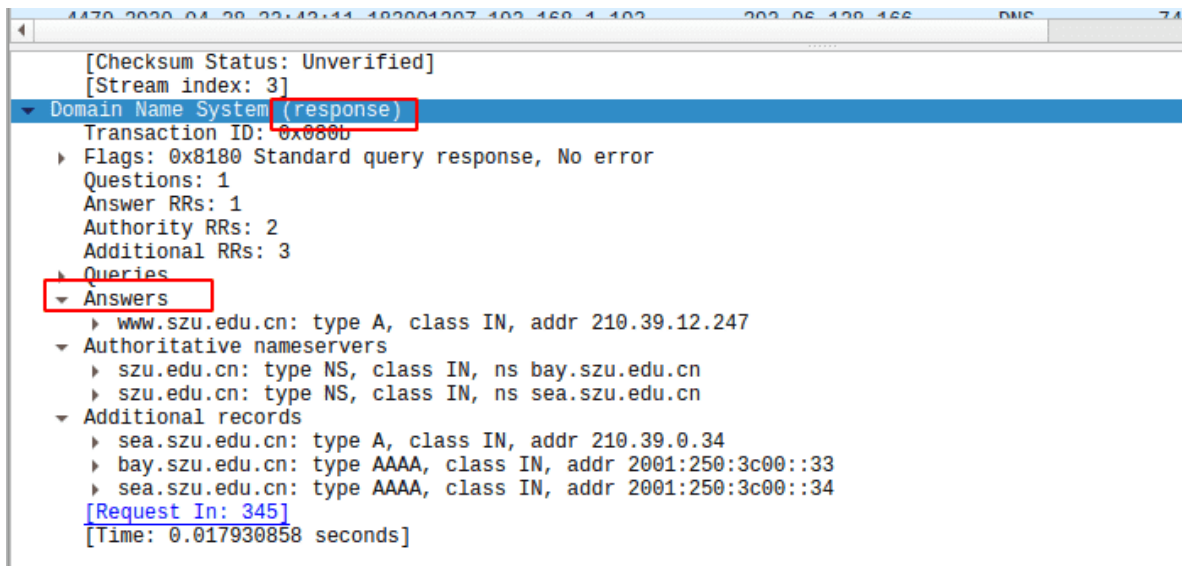
DNS发送查询消息发送到202.96.128.166这个IP地址，本地DNS服务器地址是127.0.0.53。这两个IP地址不相同。

7.检查DNS查询消息。DNS查询是什么 Type 的？查询消息是否包含任何 answers？

```
[Stream index: 3]
Domain Name System (query)
Transaction ID: 0x080b
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    www.szu.edu.cn: type A, class IN
      Name: www.szu.edu.cn
      [Name Length: 14]
      [Label Count: 4]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
[Response In: 346]
```

查询消息的Type是A，不包含answer。

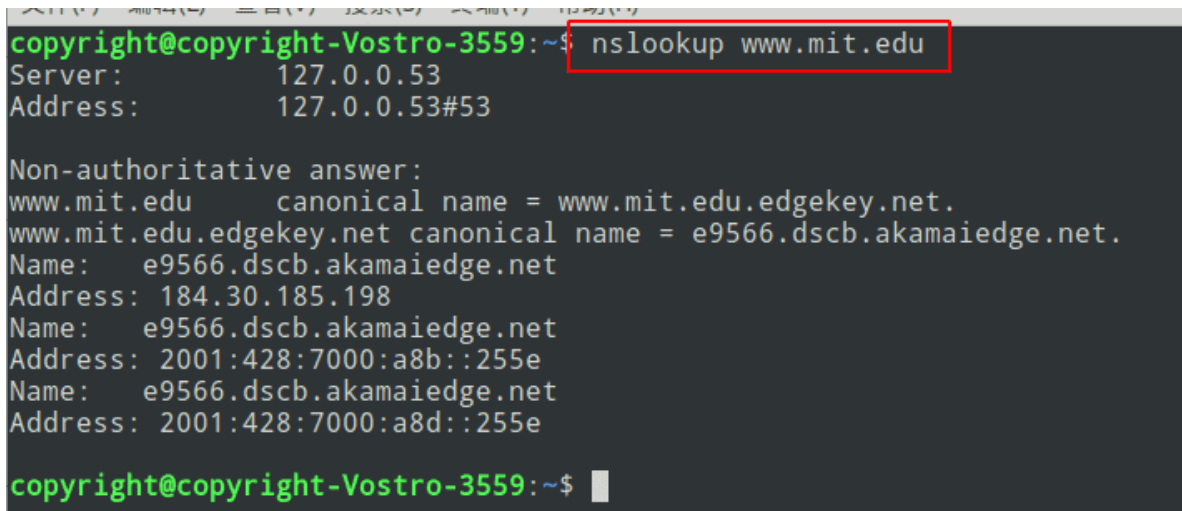
8.检查DNS响应消息，提供了多少个 answers？这些答案具体包含什么？



提供一个answer，内容是 www.szu.edu.cn: type A, class IN, addr 210.39.12.24

nslookup

重新捕获，使用nslookup在终端查询 www.mit.edu 的地址，查询完成后立即停止捕获。



回答问题：

9.DNS查询消息的目标端口是什么?DNS响应消息的源端口是什么?

No.	Time	Source	Destination	Protocol	Length	Info
3	2020-04-28 23:05:09.932449095	192.168.1.103	202.96.128.166	DNS	71	Standard qu
4	2020-04-28 23:05:09.955845675	202.96.128.166	192.168.1.103	DNS	484	Standard qu
5	2020-04-28 23:05:09.959252185	192.168.1.103	202.96.128.166	DNS	85	Standard qu
6	2020-04-28 23:05:09.978729570	202.96.128.166	192.168.1.103	DNS	465	Standard qu

▶ Frame 4: 484 bytes on wire (3872 bits), 484 bytes captured (3872 bits) on interface 0
 ▶ Ethernet II, Src: Tp-LinkT_b2:a6:cc (28:2c:b2:b2:a6:cc), Dst: IntelCor_11:2c:59 (9c:da:3e:11:2c:59)
 ▶ Internet Protocol Version 4, Src: 202.96.128.166, Dst: 192.168.1.103
 ▶ User Datagram Protocol, Src Port: 53, Dst Port: 54075
 Source Port: 53
 Destination Port: 54075
 Length: 450
 Checksum: 0x94a5 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 1]
 ▶ Domain Name System (response)
 Transaction ID: 0x104e
 Flags: 0x8180 Standard query response, No error
 Questions: 1
 Answer RRs: 3
 Authority RRs: 8
 Additional RRs: 9

查询消息的目标端口号是53，响应消息的源端口号是53。

10.DNS查询消息的目标IP地址是什么?这是你的默认本地DNS服务器的IP地址吗?

ip.addr==192.168.1.103

No.	Time	Source	Destination	Protocol	Length	Info
3	2020-04-28 23:05:09.932449095	192.168.1.103	202.96.128.166	DNS	71	Standard
4	2020-04-28 23:05:09.955845675	202.96.128.166	192.168.1.103	DNS	484	Standard
5	2020-04-28 23:05:09.959252185	192.168.1.103	202.96.128.166	DNS	85	Standard
6	2020-04-28 23:05:09.978729570	202.96.128.166	192.168.1.103	DNS	465	Standard

▶ Frame 3: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
 ▶ Ethernet II, Src: IntelCor_11:2c:59 (9c:da:3e:11:2c:59), Dst: Tp-LinkT_b2:a6:cc (28:2c:b2:b2:a6:cc)
 ▶ Internet Protocol Version 4, Src: 192.168.1.103, Dst: 202.96.128.166
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 57
 Identification: 0x20c1 (8385)
 Flags: 0x4000, Don't fragment
 Time to live: 64
 Protocol: UDP (17)
 Header checksum: 0x0cdd [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.1.103
 Destination: 202.96.128.166
 ▶ User Datagram Protocol, Src Port: 54075, Dst Port: 53
 ▶ Domain Name System (query)

DNS查询消息的目标地址是202.96.28.166，不是本地的IP地址。

11.检查DNS查询消息。DNS查询是什么 Type 的?查询消息是否包含任何 answers ?

Type A，不提供任何answer。

12.检查DNS响应消息。提供了多少个 answers ?这些答案包含什么?

```
▶ User Datagram Protocol, Src Port: 53, Dst Port: 54075
▼ Domain Name System (response)
  Transaction ID: 0x104e
  ▶ Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Authority RRs: 8
  Additional RRs: 9
  ▶ Queries
  ▼ 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 184.30.185.198
    Authority RRs: 8
```

提供了3个answer, 答案包括

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 184.30.185.198

参考资料

在做实验的过程中, 查到了一些资料, 算是补充自己知识面的不足

- [链接1](#)
- [链接2](#)
- [链接3](#)