

DNS实验报告 胡延伸 PB22050983

nslookup

测试三个命令

首先得到MIT的官网：“<https://www.mit.edu.cn/>”的 IP 地址。

```
[> www.mit.edu
Server:      202.38.64.56
Address:     202.38.64.56#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: 23.66.41.93
```

再获取发送 jmu.edu.cn 的 DNS 主机名：

```
(base) huyanshen@huyanshens-MacBook-Air ~ % nslookup -type=NS mit.edu
Server:      202.38.64.56
Address:     202.38.64.56#53

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

最后通过 DNS 服务器 bitsy.mit.edu 看看解析MIT官网：

```
((base) huyanshen@huyanshens-MacBook-Air ~ % nslookup
[> www.aiit.or.kr bitsy.mit.edu
Server:      202.38.64.56
Address:     202.38.64.56#53

Non-authoritative answer:
Name:   www.aiit.or.kr
Address: 58.229.6.225
```

实验操作

1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?

```
[> www.ustc.edu.cn
Server:      202.38.64.56
Address:     202.38.64.56#53

Name:   www.ustc.edu.cn
Address: 202.38.64.246
```

如上图，中国科学技术大学的IP地址为:202.38.64.246

2. Run nslookup to determine the authoritative DNS servers for a university in Europe.

剑桥大学 <https://www.cam.ac.uk/>

```
(base) huyanshen@huyanshens-MacBook-Air ~ % nslookup -type=NS cam.ac.uk
Server:      202.38.64.56
Address:     202.38.64.56#53

Non-authoritative answer:
cam.ac.uk      nameserver = ns3.mythic-beasts.com.
cam.ac.uk      nameserver = auth0.dns.cam.ac.uk.
cam.ac.uk      nameserver = ns1.mythic-beasts.com.
cam.ac.uk      nameserver = ns2.ic.ac.uk.
cam.ac.uk      nameserver = dns0.eng.cam.ac.uk.
cam.ac.uk      nameserver = dns0.cl.cam.ac.uk.
```

3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

雅虎邮箱的域名为“mail.yahoo.com”，我选择服务器“ns3.mythic-beasts.com”来找。

```
(base) huyanshen@huyanshens-MacBook-Air ~ % nslookup
[> mail.yahoo.com ns3.mythic-beasts.com
Server:      202.38.64.56
Address:     202.38.64.56#53

Non-authoritative answer:
mail.yahoo.com canonical name = edge.gycpi.b.yahoodns.net.
Name:   edge.gycpi.b.yahoodns.net
Address: 69.147.88.7
Name:   edge.gycpi.b.yahoodns.net
Address: 69.147.88.8
```

它的 IP 地址为: 69.147.88.6(或7)

ipconfig(ifconfig)

基本使用

以下操作均在 MacOS14 中运行, 由于 MacOS 并不支持 ipconfig/ifconfig 的大部分命令, 所以采用一些替代方法.

列出主机的所有信息:

ifconfig:

```
(base) huyanshen@huyanshens-MacBook-Air ~ % ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
    inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
            inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
                nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=<> mtu 1280
anpii: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether 22:4a:89:20:2e:67
    media: none
    status: inactive
anpi0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether 22:4a:89:20:2e:66
    media: none
    status: inactive
```

使用 **log show --info --predicate 'process == "mDNSResponder"' --last 1h** 查看过去 1h 的 DNS 缓存记录

```
(base) huyanshen@huyanshens-MacBook-Air ~ % log show --info --predicate 'process == "mDNSResponder"' --last 1h
Filtering the log data using "process == "mDNSResponder"""
Skipping debug messages, pass --debug to include.
Timestamp          Thread      Type       Activity      PID
    TTL
2024-10-09 23:42:33.326893+0800 0xa0d      Default      0x0          224
    0  mDNSResponder: [com.apple.mDNSResponder:Default] [R345636] DNSServiceCreateConnection START PID[38019](dnssd)
2024-10-09 23:42:33.327057+0800 0xa0d      Default      0x0          224
    0  mDNSResponder: [com.apple.mDNSResponder:mDNS] [R345637] DNSServiceResolve4000, -1, "<mask.hash: 'xVrNN+YCcPUyNDYRL+cGKQ==">'(7d204afc)) START PID[38019](dnssd)
2024-10-09 23:42:35.328039+0800 0xa0d      Default      0x0          224
    0  mDNSResponder: [com.apple.mDNSResponder:mDNS] [R345638] DNSServiceResolve4000, 0, "<mask.hash: 'LWyxA30j5P5HaL38kTDFfQ==">'(7980e4a4)) START PID[38019](dnssd)
```

清除缓存

利用命令 `sudo killall -HUP mDNSResponder` 即可。

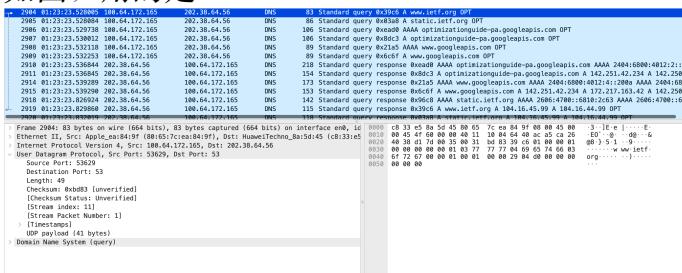
Tracing DNS with Wireshark

- 首先利用 `sudo killall -HUP mDNSResponder` 清除 DNS 缓存。
 - 清除浏览器缓存。
 - 利用 `networksetup -getinfo Wi-Fi` 得到我的 IP 地址: 100.64.172.165
 - 打开 Wireshark, 双击 WiFi:en0, 在顶部栏输入 filter 条件 `ip.addr==100.64.172.165`
 - 使用浏览器访问网页: <http://www.ietf.org>
 - 停止抓包。

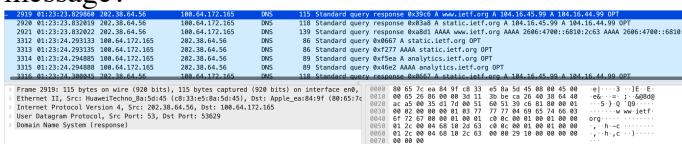
问题解答

4. Locate the DNS query and response messages. Are they sent over UDP or TCP?

如图，用的是 UDP：



5. What is the destination port for the DNS query message? What is the source port of DNS response message?

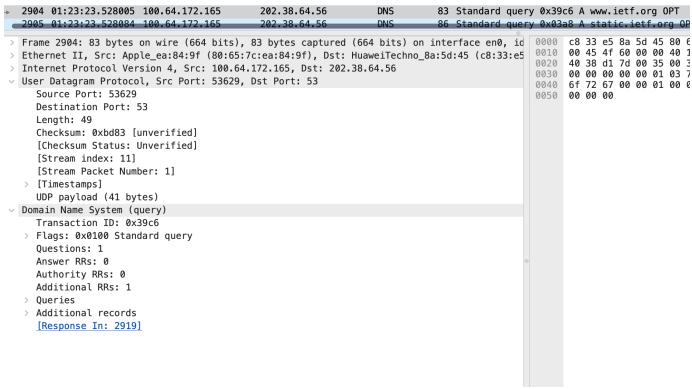


结合上图和上一题图，端口均为 53

6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

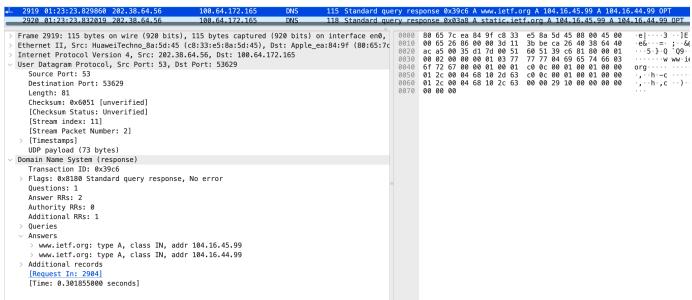
DNS查询消息发送到:202.38.64.46,而本地DNS服务器为202.38.64.56,显然两者一样。

7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?



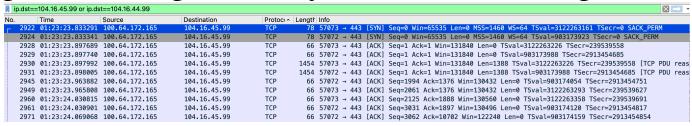
类型为A，没有任何 answers.

8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?



提供了 2 个 "answers"，是该域名的 2 个 IPV4 地址。

9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?



如上图所示，是对应的

10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?
没有，因为本机 DNS 已经被缓存了，不需要发起新的 DNS 查询。

nslookup 的 DNS 查询①

实验步骤

启动数据包捕获，再使用nslookup查询 www.mit.edu，最后停止.

问题解答

11. What is the destination port for the DNS query message? What is the source port of DNS response message?

```

+ 617 01:49:58.600254 100.64.172.165 202.38.64.56 DNS 71 Standard query 0xe59c A www.mit.edu
- 768 01:49:58.797334 202.38.64.56 DNS 163 Standard query response 0xe59c A www.mit.edu
+ 617 01:49:59.008712 100.64.172.165 202.38.64.56 DNS 90 Standard query 0xe59f AAAA los.chat.op
Frame 617: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface en0, id 0x0000 c8 33 e5 8a 5d 45 81
> Ethernet II, Src: Apple_ea:84:9f (00:65:7c:ea:84:9f), Dst: HuaweiTechno_8a:5d:45 (c8:33:e5)
> Internet Protocol Version 4, Src: 100.64.172.165, Dst: 202.38.64.56
> User Datagram Protocol, Src Port: 53, Dst Port: 53
    Source Port: 62758
    Destination Port: 53
    Length: 37
    Checksum: 0xb6bb [unverified]
    [Checksum Status: Unverified]
    [Stream index: 5]
    [Stream Packet Number: 1]
    > [Timestamps]
    UDP payload (20 bytes)
    > Domain Name System (query)
        Transaction ID: 0xe59c
        Flags: 0x0100 Standard query
        Questions: 1
        Answer RRs: 0
        Authority RRs: 0
        Additional RRs: 0
        Queries
            [Response In: 768]

```

```

+ 768 01:49:58.797334 202.38.64.56 100.64.172.165 DNS 163 Standard query response 0xe59c A www.mit.edu CNAME
+ 617 01:49:59.008712 100.64.172.165 202.38.64.56 DNS 90 Standard query overwriting previous response
Frame 768: 163 bytes on wire (1304 bits), 163 bytes captured (1304 bits) on interface en0, id 0x0000 80 65 7c e8 91 c8 33 e5 8a 5
> Ethernet II, Src: HuaweiTechno_8a:5d:45 (c8:33:e5), Dst: Apple_ea:84:9f (00:65:7c)
> Internet Protocol Version 4, Src: 202.38.64.56, Dst: 100.64.172.165
> User Datagram Protocol, Src Port: 53, Dst Port: 62758
    Source Port: 53
    Destination Port: 62758
    Length: 129
    Checksum: 0x2b0e [unverified]
    [Checksum Status: Unverified]
    [Stream index: 5]
    [Stream Packet Number: 2]
    > [Timestamps]
    UDP payload (121 bytes)
    > Domain Name System (response)
        Transaction ID: 0xe59c
        Flags: 0x0100 Standard query response, No error
        Questions: 1
        Answer RRs: 3
        Authority RRs: 0
        Additional RRs: 0
        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 23.66.41.93
            [Request In: 617]
            [Time: 0.197880000 seconds]

```

如上面两幅图，均为53

12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

如上一题图，DNS 查询消息的目标 IP 地址是202.38.64.56，和我本地DNS服务器一致.

```

[(base) huyanshen@huyanshens-MacBook-Air ~ % nslookup www.mit.edu
Server:          202.38.64.56
Address:         202.38.64.56#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:          23.66.41.93

```

13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

```

+ 617 01:49:58.600254 100.64.172.165 202.38.64.56 DNS 71 Standard query 0xe59c A www.mit.edu
- 768 01:49:58.797334 202.38.64.56 DNS 163 Standard query response 0xe59c www.r
+ 617 01:49:59.008712 100.64.172.165 202.38.64.56 DNS 90 Standard query 0xe59f AAAA los.chat.op
Frame 617: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface en0, id 0x0000 c8 33 e5 8a 5d 45 81
> Ethernet II, Src: Apple_ea:84:9f (00:65:7c:ea:84:9f), Dst: HuaweiTechno_8a:5d:45 (c8:33:e5)
> Internet Protocol Version 4, Src: 100.64.172.165, Dst: 202.38.64.56
> User Datagram Protocol, Src Port: 53, Dst Port: 53
    Source Port: 62758
    Destination Port: 53
    Length: 37
    Checksum: 0xb6bb [unverified]
    [Checksum Status: Unverified]
    [Stream index: 5]
    [Stream Packet Number: 1]
    > [Timestamps]
    UDP payload (20 bytes)
    > Domain Name System (query)
        Transaction ID: 0xe59c
        Flags: 0x0100 Standard query
        Questions: 1
        Answer RRs: 0
        Authority RRs: 0
        Additional RRs: 0
        Queries
            > www.mit.edu: type A, class IN
                Name: www.mit.edu
                [Name length: 11]
                [Label Count: 3]
                Type: A (1) (Host Address)
                Class: IN (0x0001)
            [Response In: 768]

```

类型为A，表示查询 IP 地址，没有任何 "answers"。

14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

```
    768 01:49:59.0802715 100.64.172.165 DNS 163 Standard query response 0x59c A www.mit.edu CNAME www.mit.edu
  904 01:49:59.0802734 100.64.172.165 DNS 98 Standard query response 0x3cf AAAA [ios.chat.openai.com] OPT
  905 01:49:59.0802751 100.64.172.165 DNS 98 Standard query response 0x312 A [ios.chat.openai.com] OPT

> Frame 768: 160 bytes on wire (1304 bits), 163 bytes captured (1304 bits) on interface en0,
  Ethernet II, Src: HomeTechno_Ba:5d:45 (08:33:e5:ba:5d:45), Dst: Apple_ea:84:9f (00:80:00:00:00:00)
  Internet Protocol Version 4, Src: 202.38.64.56, Dst: 100.64.172.165
  User Datagram Protocol, Src Port: 53, Dst Port: 62758
  > [http://www.mit.edu] [response]
    Transaction ID: 0x859c
  > Flags: 0x0080 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Additional RRs: 0
  Queries
    > www.mit.edu type A, class IN
      Name: www.mit.edu
      [Name Length: 11]
      Label Count: 3
      Type: A (1) [Host Address]
      Class: IN (0x8001)

  > 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.dsrb.akamaiedge.net
    e9566.dsrb.akamaiedge.net: type A, class IN, addr 23.66.41.93
  [Request In: 61774]
  [Time: 0.139708000 seconds]
```

如上图，一共有 3 个 answers，分别包含正式名称 CNAME，以及 IPV4 地址。

15. Provide a screenshot.

nslookup 的 DNS 查询②

实验步骤

和上一步骤类似，只是把命令换成：

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

16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

```

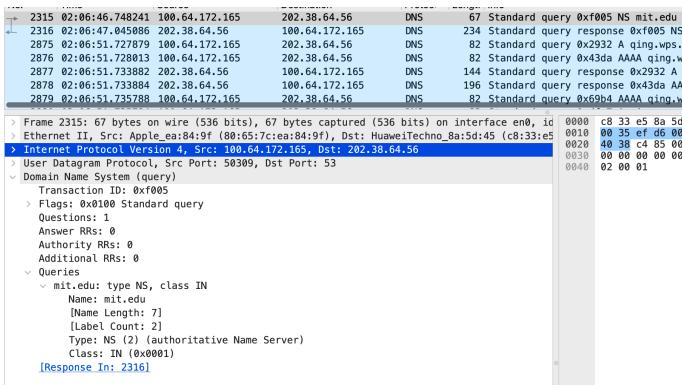
2315 02:06:46.748241 100.64.172.165 202.38.64.56 DNS 67 Standard query 0x0f05 NS mit.edu
2316 02:06:45.045086 202.38.64.56 100.64.172.165 DNS 234 Standard query response 0x0f05 NS mit.edu
2875 02:06:51.7272879 100.64.172.165 202.38.64.56 DNS 82 Standard query 0x2932 A qing.wps.cn OF
2876 02:06:51.7272813 100.64.172.165 202.38.64.56 DNS 82 Standard query 0x43da AAAA qing.wps.cn
2877 02:06:51.733882 202.38.64.56 100.64.172.165 DNS 144 Standard query response 0x2932 A qing.
2878 02:06:51.733884 202.38.64.56 100.64.172.165 DNS 196 Standard query response 0x43da AAAA q
2879 02:06:51.357588 100.64.172.165 202.38.64.56 DNS 82 Standard query 0x69fa AAAA qing.wps.cn

Frame 2315: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface en0, id 0000 c8 33 e5 8a 5d 45 8
Ethernet II, Src: Apple-ea:84:9f (08:65:c7:ea:84:9f), Dst: WebTechno_8a:5d:45 (c8:33:e5)
Internet Protocol Version 4, Src: 100.64.172.165, Dst: 202.38.64.56
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 53
    Identification: 0xfe6d (61398)
    > 0000 0000 0000 0000 = Flags: 0x0
    > 0000 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0xf69d [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 100.64.172.165
    Destination Address: 202.38.64.56
    [Stream index: 11]

```

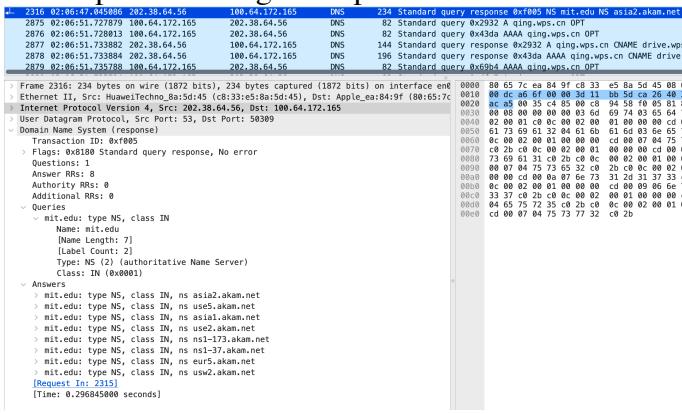
如上图，和上一实验一样地址为202.38.64.56，与我的本地DNS服务器地址一样。

17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?



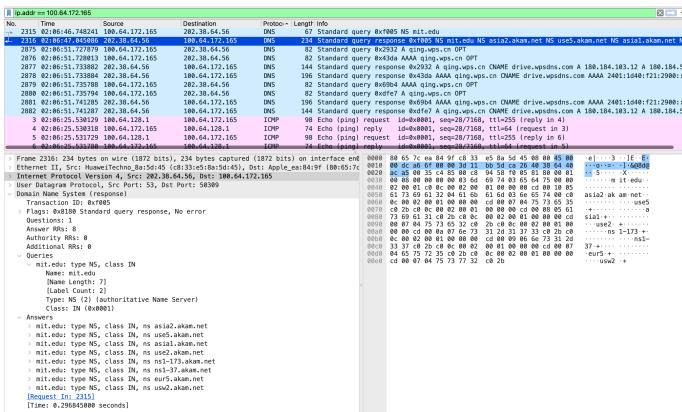
如上图，类型为 NS 表示查询权威 DNS 服务器，没有任何 "answers".

18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?



服务器如上图 Answers 中所示，响应消息没提供 MIT 的域名的 IP 地址。

19. Provide a screenshot.



nslookup 的 DNS 查询③

实验步骤

和前两个实验类似，只不过把命令替换成如下：

`nslookup www.aiit.or.kr bitsy.mit.edu`

得到 nslookup 结果为：

```
[base) huyanshen@huyanshens-MacBook-Air ~ % nslookup  
[> www.aiit.or.kr bitsy.mit.edu  
Server: 202.38.64.56  
Address: 202.38.64.56#53  
  
Non-authoritative answer:  
Name: www.aiit.or.kr  
Address: 58.229.6.225
```

20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

```
987 02:17:42.248471 100.64.172.165 202.38.64.56 DNS 74 Standard query 0x62a6 A www.aiit.or.kr  
988 02:17:42.254966 202.38.64.56 100.64.172.165 DNS 90 Standard query response 0x62a6 A www.aiit.or.kr  
93 02:17:36.092971 100.64.128.1 100.64.172.165 ICMP 98 Echo (ping) request id=0x0001, seq=28/7168,  
94 02:17:36.092974 100.64.128.1 100.64.172.165 ICMP 98 Echo (ping) request id=0x0001, seq=28/7168,  
95 02:17:36.093148 100.64.128.1 100.64.172.165 ICMP 74 Echo (ping) reply id=0x0001, seq=28/7168,  
96 02:17:36.093245 100.64.172.165 100.64.128.1 ICMP 74 Echo (ping) reply id=0x0001, seq=28/7168,  
97 02:17:36.096851 100.64.128.1 100.64.172.165 ICMP 98 Echo (ping) request id=0x0001, seq=28/7168,  
98 02:17:36.096851 100.64.128.1 100.64.172.165 ICMP 98 Echo (ping) request id=0x0001, seq=28/7168  
Frame 987: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface en0, id 0000 c8 33 e5 8a 5d 45 80 11  
Ethernet II, Src: Apple_ea:84:9f (00:65:7c:ea:84:9f), Dst: HuaweiTechne_8a:5d:45 (c8:33:e5  
Internet Protocol Version 4, Src: 100.64.172.165, Dst: 202.38.64.56  
User Datagram Protocol, Src Port: 58520, Dst Port: 53  
Domain Name System (query)  
Transaction ID: 0x62a6  
Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries  
www.aiit.or.kr type A, class IN  
Name: www.aiit.or.kr  
[Name Length: 14]  
[Label Count: 4]  
Type: A (1) (Host Address)  
Class: IN (0x0001)  
[Response In: 9881]
```

其地址为202.38.64.56，显然也和我的本地DNS地址一致。

21. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

```
987 02:17:42.248471 100.64.172.165 202.38.64.56 DNS 74 Standard query 0x62a6 A www.aiit.or.kr  
988 02:17:42.254966 202.38.64.56 100.64.172.165 DNS 90 Standard query response 0x62a6 A www.aiit.or.kr  
93 02:17:36.092971 100.64.128.1 100.64.172.165 ICMP 98 Echo (ping) request id=0x0001, seq=28/  
94 02:17:36.092974 100.64.128.1 100.64.172.165 ICMP 98 Echo (ping) request id=0x0001, seq=28/  
95 02:17:36.093148 100.64.172.165 100.64.128.1 ICMP 74 Echo (ping) reply id=0x0001, seq=28/  
96 02:17:36.093245 100.64.172.165 100.64.128.1 ICMP 74 Echo (ping) reply id=0x0001, seq=28/  
97 02:17:36.096851 100.64.128.1 100.64.172.165 ICMP 98 Echo (ping) request id=0x0001, seq=28/  
98 02:17:36.096851 100.64.128.1 100.64.172.165 ICMP 98 Echo (ping) request id=0x0001, seq=28/  
Frame 987: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface en0, id 0000 c8 33 e5 8a 5d 45 80 11  
Ethernet II, Src: Apple_ea:84:9f (00:65:7c:ea:84:9f), Dst: HuaweiTechne_8a:5d:45 (c8:33:e5  
Internet Protocol Version 4, Src: 100.64.172.165, Dst: 202.38.64.56  
User Datagram Protocol, Src Port: 58520, Dst Port: 53  
Domain Name System (query)  
Transaction ID: 0x62a6  
Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries  
www.aiit.or.kr type A, class IN  
Name: www.aiit.or.kr  
[Name Length: 14]  
[Label Count: 4]  
Type: A (1) (Host Address)  
Class: IN (0x0001)  
[Response In: 9881]
```

类型为A，没有Answers

22. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

```
988 02:17:42.254966 202.38.64.56 100.64.172.165 DNS 98 Standard query response 0x62a6 A www.aiit.or.kr A 58.229.6.225  
93 02:17:36.092971 100.64.128.1 100.64.172.165 ICMP 98 Echo (ping) request id=0x0001, seq=28/7168, ttl=25 (request 1)  
94 02:17:36.092974 100.64.128.1 100.64.172.165 ICMP 98 Echo (ping) request id=0x0001, seq=28/7168, ttl=25 (request 1)  
95 02:17:36.093148 100.64.172.165 100.64.128.1 ICMP 74 Echo (ping) reply id=0x0001, seq=28/7168, ttl=64 (request 1)  
96 02:17:36.093245 100.64.172.165 100.64.128.1 ICMP 74 Echo (ping) reply id=0x0001, seq=28/7168, ttl=64 (request 1)  
97 02:17:36.096851 100.64.128.1 100.64.172.165 ICMP 98 Echo (ping) request id=0x0001, seq=28/7168, ttl=25 (no error)  
98 02:17:36.096851 100.64.128.1 100.64.172.165 ICMP 98 Echo (ping) request id=0x0001, seq=28/7168, ttl=25 (no error)  
Frame 988: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface en0, id 0000 80 55 7c ea 84 9f c8 33 e5 8a 5d 45 80 11  
Ethernet II, Src: HuaweiTechne_8a:5d:45 (c8:33:e5:8a:5d:45), Dst: Apple_ea:84:9f (00:65:7c:ea:84:9f)  
Internet Protocol Version 4, Src: 202.38.64.56, Dst: 100.64.172.165  
User Datagram Protocol, Src Port: 58520, Dst Port: 53  
Domain Name System (response)  
Transaction ID: 0x62a6  
Flags: 0x8100 Standard query response, No error  
Questions: 1  
Answer RRs: 1  
Authority RRs: 0  
Additional RRs: 0  
Queries  
www.aiit.or.kr type A, class IN  
Name: www.aiit.or.kr  
[Name Length: 14]  
[Label Count: 4]  
Type: A (1) (Host Address)  
Class: IN (0x0001)  
Answers  
www.aiit.or.kr type A, class IN, addr 58.229.6.225  
[Request In: 9871]  
[Time: 0.000495800 seconds]
```

一共有1个answer，包含该域名的IPV4地址

23. Provide a screenshot.