

山东大学 计算机科学与技术 学院

新兴网络技术与实践 课程实验报告

学号：202300130183	姓名：宋浩宇	班级：23 级智能班
实验题目：Wireshark DNS		
实验学时：2	实验日期：2025/3/19	
实验目的：了解 DNS		
<p>实验结果：</p> <p>1. Run nslookup to obtain the IP address of a Web server in Asia.What is the IP address of that server?</p> <div><pre>C:\Users\23676>nslookup sdu.edu.cn Server: UnKnown Address: 192.168.254.245 Name: sdu.edu.cn Addresses: 211.86.56.247 202.194.14.6 202.194.15.6 C:\Users\23676></pre></div> <p>从图中可以看出 www. sdu. edu. cn 的服务器 ip 地址对应了三个值，分别是 211. 86. 56. 247、202. 194. 14. 6、202. 194. 15. 6</p> <p>2. Run nslookup to determine the authoritative DNS servers for a university in Europe.</p>		

```
C:\Users\23676>nslookup -type=NS ox.ac.uk
Server: UnKnown
Address: 192.168.254.245

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

dns0.ox.ac.uk internet address = 129.67.1.190
dns1.ox.ac.uk internet address = 129.67.1.191
dns2.ox.ac.uk internet address = 163.1.2.190
auth5.dns.ox.ac.uk AAAA IPv6 address = 2a00:1098:0:80:1000::10
auth6.dns.ox.ac.uk internet address = 185.24.221.32

C:\Users\23676>|
```

可以看出牛津大学的权威 DNS 服务器有 auth5.dns.ox.ac.uk 、 dns1.ox.ac.uk 、 auth4.dns.ox.ac.uk 、 auth6.dns.ox.ac.uk 、 dns0.ox.ac.uk、 dns2.ox.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?

很不幸牛津大学的权威 DNS 不允许我们使用它来解析域名：

```
C:\Users\23676>nslookup mail.yahoo.com auth4.dns.ox.ac.uk
Server: UnKnown
Address: 45.33.127.156

*** UnKnown can't find mail.yahoo.com: Query refused
```

但是公共 DNS 解析的结果为：

```

C:\Users\23676>nslookup mail.yahoo.com 8.8.8.8
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:      edge.gycpi.b.yahoodns.net
Addresses: 2406:2000:a8:800::e6
           2406:2000:a8:800::e7
           180.222.116.12
           180.222.116.11
Aliases:   mail.yahoo.com

```

可以看出雅虎邮箱的 IP 地址为图中的四个，2406:2000:a8:800::e6、2406:2000:a8:800::e7、180.222.116.12、180.222.116.11

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

The image shows a Wireshark packet capture window titled "以太网". The packet list on the left shows two packets: packet 16449 (DNS Standard query) and packet 16451 (DNS Standard query response). The packet details pane for packet 16449 shows the following structure:

- Frame 16449: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{280B37C7-C9FA-43B8-8000-000000000000}
- Ethernet II, Src: ASUSTekCOMPU_c8:c8:3a (08:bf:b8:c8:c8:3a), Dst: JuniperNetwo_f6:12:a0 (28:a2:4b:f6:12:a0)
- Internet Protocol Version 4, Src: 192.168.254.198, Dst: 192.168.254.245
- User Datagram Protocol, Src Port: 68782, Dst Port: 53
- Domain Name System (query)

The packet bytes pane shows the raw data of the DNS query, including the query ID, flags, and the question section.

通过追踪流的方式，我们可以得知为我们服务的这个 DNS 是使用的 UDP 协议。

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

```

> Frame 16451: 506 bytes on wire (4048 bits), 506 bytes captured (4048 bits) on interface \Device\NPF_{28DB37C7-C9FA-4
> Ethernet II, Src: JuniperNetwo_f6:12:a0 (28:a2:4b:f6:12:a0), Dst: ASUSTekCOMPU_c0:c0:3a (08:bf:b8:c0:c0:3a)
> Internet Protocol Version 4, Src: 192.168.254.245, Dst: 101.76.244.190
> User Datagram Protocol, Src Port: 53, Dst Port: 60702
> Domain Name System (response)

```

从这里的信息可以看出，源端口号是 53，目的端口号是 60702

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?

No.	Time	Source	Destination	Protocol	Length	Info
16449	2025-03-19 16:51:10.121224	101.76.244.190	192.168.254.245	DNS	72 S	
16451	2025-03-19 16:51:10.121539	192.168.254.245	101.76.244.190	DNS	506 S	

从上图中可以看出 DNS query 信息被发送到了 192.168.254.245 这个 ip 地址，这与上文图中我们的本地 DNS 服务器地址是一致的。

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

```

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: 6
Additional RRs: 12
v Queries

```

这个 DNS query 的类型是 Standard query response, No error

Answers 为

Answers

✓ www.ietf.org: type A, class IN, addr 104.16.45.99

Name: www.ietf.org

Type: A (1) (Host Address)

Class: IN (0x0001)

Time to live: 56367 (15 hours, 39 minutes, 27 seconds)

Data length: 4

Address: 104.16.45.99

✓ www.ietf.org: type A, class IN, addr 104.16.44.99

Name: www.ietf.org

Type: A (1) (Host Address)

Class: IN (0x0001)

Time to live: 56367 (15 hours, 39 minutes, 27 seconds)

Data length: 4

Address: 104.16.44.99

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

如上图，一共两个回复，每个回复包括域名、类型、类别、time to live、数据长度、域名解析出的地址。

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?

No.

Time

Source

Destination

Protocol

Length

Info

121

1742375559.371761

101.76.244.190

192.168.254.245

TCP

56

8276 -> 53 [PSH, ACK] Seq=1 Ack=1 Win=5535 Len=0 [TCP PDU reassembled in 123]

122

1742375559.371761

101.76.244.190

192.168.254.245

TCP

56

8277 -> 53 [ACK] Seq=1 Ack=1 Win=5535 Len=0

123

1742375559.371802

101.76.244.190

192.168.254.245

DNS

84

Standard query 0x343b AAAA www.ietf.org

124

1742375559.371829

101.76.244.190

192.168.254.245

TCP

56

8277 -> 53 [PSH, ACK] Seq=1 Ack=1 Win=5535 Len=0 [TCP PDU reassembled in 125]

125

1742375559.371840

101.76.244.190

192.168.254.245

DNS

84

Standard query 0x0f08 A www.ietf.org

126

1742375559.371948

192.168.254.245

101.76.244.190

TCP

60

53 -> 8276 [ACK] Seq=1 Ack=3 Win=29200 Len=0

127

1742375559.371948

192.168.254.245

101.76.244.190

TCP

60

53 -> 8276 [ACK] Seq=1 Ack=3 Win=29200 Len=0

128

1742375559.372082

192.168.254.245

101.76.244.190

DNS

544

Standard query response 0x343b AAAA www.ietf.org AAAA 2606:4700::6810:c63 AAAA 2606:4700::6810:2663 NS c0.org.afiliast.info NS b0.org.afiliast.info

129

1742375559.372176

101.76.244.190

192.168.254.245

TCP

54

8276 -> 53 [FIN, ACK] Seq=3 Ack=491 Win=58045 Len=0

130

1742375559.372306

192.168.254.245

101.76.244.190

TCP

60

53 -> 8276 [FIN, ACK] Seq=3 Ack=491 Win=58045 Len=0

131

1742375559.372306

192.168.254.245

101.76.244.190

TCP

54

8276 -> 53 [ACK] Seq=3 Ack=492 Win=58045 Len=0

132

1742375559.372452

192.168.254.245

101.76.244.190

TCP

60

53 -> 8277 [ACK] Seq=1 Ack=3 Win=29200 Len=0

133

1742375559.372452

192.168.254.245

101.76.244.190

TCP

60

53 -> 8277 [ACK] Seq=1 Ack=3 Win=29200 Len=0

134

1742375559.372452

192.168.254.245

101.76.244.190

DNS

504

Standard query response 0x0f08 A www.ietf.org A 104.16.44.99 A 104.16.45.99 NS a0.org.afiliast.info NS a2.org.afiliast.info NS c0.org.afiliast.info

135

1742375559.372566

101.76.244.190

192.168.254.245

TCP

54

8277 -> 53 [FIN, ACK] Seq=3 Ack=491 Win=58045 Len=0

136

1742375559.372781

192.168.254.245

101.76.244.190

TCP

60

53 -> 8277 [FIN, ACK] Seq=451 Ack=3 Win=29200 Len=0

137

1742375559.372912

101.76.244.190

192.168.254.245

TCP

54

8277 -> 53 [ACK] Seq=3 Ack=452 Win=58085 Len=0

138

1742375559.372912

101.76.244.190

104.16.45.99

UDP

794

63943 -> 443 [Len=752]

139

1742375559.379042

101.76.244.190

192.168.254.245

TCP

1494

8254 -> 443 [ACK] Seq=11620 Ack=2112 Win=255 Len=140 [TCP PDU reassembled in 141]

140

1742375559.379042

101.76.244.190

192.168.254.245

TCP

1494

8254 -> 443 [ACK] Seq=11606 Ack=20112 Win=255 Len=140 [TCP PDU reassembled in 141]

141

1742375559.379042

101.76.244.190

202.89.233.100

TLSv1.2

658

Application Data

142

1742375559.412819

202.89.233.100

101.76.244.190

TCP

60

443 -> 8254 [ACK] Seq=2012 Ack=13060 Win=16379 Len=0

143

1742375559.412819

202.89.233.100

101.76.244.190

TCP

60

443 -> 8254 [ACK] Seq=2012 Ack=15104 Win=16385 Len=0

>

Frame 145:

1242 bytes on wire (9936 bits), 1242 bytes captured (9936 bits) on interface Device\NPF_{280B3C7C-C9FA-F...}

Ethernet II

Src: JuniperNetwre06:12:12:a0 (28:b2:40:f6:12:a0),

Dest: ASUS-TCPVU-pc:c8:3a (08:f0:b8:c8:c8:3a)

Internet Protocol Version 4

Src: 104.16.45.99 (104.16.45.99),

Dest: 101.76.244.190 (101.76.244.190)

User Datagram Protocol

Src Port: 443,

Dst Port: 63943

Data (1200 bytes)

[Data ...]

0000

f1 0d 02 70 28 0a f7 c4 08 b6 c6 47 d1 65 d0 6e 69

0001

af 88 e2 30 92 af 77 85 84 c1 97 80 8e 87 00 00

0002

0c 43 e6 55 bb 46 59 fe 0a 07 37 39 ba 36 00 00

0003

00 00 00 00 c7 72 3e ad 07 ad 0c 31 85 17 72 e4

0004

67 06 47 62 35 2a 51 de 2a ee 00 50 e0 a9 5d

0005

54 c0 07 df c4 07 fa 01 06 06 e7 f1 57 00 99 9e

0006

fa 07 c3 25 f0 00 5d 1c 90 dd c7 17 45 74 00

0007

0a 8c 24 c4 f6 c6 70 90 00 66 75 5d d0 7a 00

0008

c1 f0 60 ef 51 0d 04 f2 b0 e1 e7 51 05 9a 8d

0009

00 00 31 ad 16 29 62 33 93 03 c7 35 c2 2b a9

0010

f7 07 02 ec c8 fa 09 ed 98 5d 60 16 70 18 01

0011

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0012

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0013

56 06 07 ca e7 e8 e0 d7 4c dc cf 6d 62 03 00

0014

0110 35 90 02 07 16 26 07 03 07 57 14 12 fa b1

0015

0b e

根据结果，TCP SYN 并没有发生在主机与 www.ietf.org 之间，而是在主机与本地 DNS 服务器之间。

10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

我们的主机在获取到图片之前，并没有在发出 DNS 事务。

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

```
> Internet Protocol Version 4, Src: 192.168.254.245, Dst: 101.76.244.190
> User Datagram Protocol, Src Port: 53, Dst Port: 63981
v Domain Name System (response)
  Transaction ID: 0x0003
```

从这里的信息可以看出，源端口号是 53，目的端口号是 63981

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

No.	Time	Source	Destination	Protocol	Length	Info
933	1742376962.115025	101.76.244.190	192.168.254.245	DNS	88	Standard query 0x0001 PTR 245.254.168.192.in-addr.arpa
934	1742376962.115642	192.168.254.245	101.76.244.190	DNS	123	Standard query response 0x0001 No such name PTR 245.254.168.192.in-addr.arpa SOA 168.192.192.in-addr.arpa 1
935	1742376962.116943	101.76.244.190	192.168.254.245	DNS	71	Standard query 0x0002 A www.mit.edu
936	1742376962.127862	192.168.254.245	101.76.244.190	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscloud.net
937	1742376962.130299	101.76.244.190	192.168.254.245	DNS	71	Standard query 0x0003 AAAA www.mit.edu
950	1742376962.323019	192.168.254.245	101.76.244.190	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscloud.net
1054	1742376964.203571	101.76.244.190	192.168.254.245	DNS	80	Standard query 0xd005 AAAA otheve.beacon.qq.com
1055	1742376964.203677	101.76.244.190	192.168.254.245	DNS	80	Standard query 0x09a2 A otheve.beacon.qq.com
1056	1742376964.203746	101.76.244.190	192.168.254.245	DNS	80	Standard query 0x5520 HTTPS otheve.beacon.qq.com
1059	1742376964.203934	192.168.254.245	101.76.244.190	DNS	184	Standard query response 0xd005 AAAA otheve.beacon.qq.com CNAME ins-u4xprfqu.ias.tencent-cloud.com
1060	1742376964.203934	192.168.254.245	101.76.244.190	DNS	160	Standard query response 0x09a2 A otheve.beacon.qq.com CNAME ins-u4xprfqu.ias.tencent-cloud.com
1064	1742376964.204192	192.168.254.245	101.76.244.190	DNS	128	Standard query response 0x5520 HTTPS otheve.beacon.qq.com CNAME ins-u4xprfqu.ias.tencent-cloud.com

如图，这个 192.168.254.245 和我们本地的 DNS 服务器的 IP 是一致的。

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

```

> User Datagram Protocol, Src Port: 53, Dst Port: 63981
√ Domain Name System (response)
  Transaction ID: 0x0003
  √ 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: 4
  Authority RRs: 0
  Additional RRs: 0
  √ Queries
    √ www.mit.edu: type AAAA, class IN
      Name: www.mit.edu
      [Name Length: 11]
      [Label Count: 3]

```

这个 DNS query 的类型是 Standard query response, No error

Answers 为

```

√ Answers
  √ www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
    Name: www.mit.edu
    Type: CNAME (5) (Canonical NAME for an alias)
    Class: IN (0x0001)
    Time to live: 1166 (19 minutes, 26 seconds)
    Data length: 25
    CNAME: www.mit.edu.edgekey.net
  √ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
    Name: www.mit.edu.edgekey.net
    Type: CNAME (5) (Canonical NAME for an alias)
    Class: IN (0x0001)
    Time to live: 60 (1 minute)
    Data length: 24
    CNAME: e9566.dscb.akamaiedge.net
  √ e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2600:1417:8400:286::255e
    Name: e9566.dscb.akamaiedge.net
    Type: AAAA (28) (IP6 Address)
    Class: IN (0x0001)
    Time to live: 60 (1 minute)
    Data length: 16
    AAAA Address: 2600:1417:8400:286::255e
  √ e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2600:1417:8400:28a::255e
    Name: e9566.dscb.akamaiedge.net
    Type: AAAA (28) (IP6 Address)
    Class: IN (0x0001)
    Time to live: 60 (1 minute)
    Data length: 16
    AAAA Address: 2600:1417:8400:28a::255e
  [Request In: 937]
  [Time: 0.192720000 seconds]

```

14. Examine the DNS response message. How many “answers” are

provided? What do each of these answers contain?

如上图，一共五个回复，每个回复包括域名、类型、类别、time to live、数据长度、域名别名、域名解析出的地址。

15. Provide a screenshot.

截图均在上文文中。

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

996	1742377414.013889	101.76.244.190	192.168.254.245	DNS	67	Standard query 0x0002 NS mit.edu
997	1742377414.066890	192.168.254.245	101.76.244.190	DNS	446	Standard query response 0x0002 NS mit.edu

发送到了 192.168.254.245，和本地 DNS 是一致的。

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

```
Transaction ID: 0x0002
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: 8
Authority RRs: 0
Additional RRs: 11
Queries:
```

这个 DNS query 的类型是 Standard query response, No error

Answers 为

✓ Answers

- ✓ mit.edu: type NS, class IN, ns ns1-173.akam.net
Name: mit.edu
Type: NS (2) (authoritative Name Server)
Class: IN (0x0001)
Time to live: 1800 (30 minutes)
Data length: 18
Name Server: ns1-173.akam.net
- ✓ mit.edu: type NS, class IN, ns usw2.akam.net
Name: mit.edu
Type: NS (2) (authoritative Name Server)
Class: IN (0x0001)
Time to live: 1800 (30 minutes)
Data length: 7
Name Server: usw2.akam.net
- ✓ mit.edu: type NS, class IN, ns ns1-37.akam.net
Name: mit.edu
Type: NS (2) (authoritative Name Server)
Class: IN (0x0001)
Time to live: 1800 (30 minutes)
Data length: 9
Name Server: ns1-37.akam.net
- ✓ mit.edu: type NS, class IN, ns use5.akam.net
Name: mit.edu
Type: NS (2) (authoritative Name Server)
Class: IN (0x0001)
Time to live: 1800 (30 minutes)
Data length: 7
Name Server: use5.akam.net
- ✓ mit.edu: type NS, class IN, ns asia1.akam.net
Name: mit.edu
Type: NS (2) (authoritative Name Server)
Class: IN (0x0001)
Time to live: 1800 (30 minutes)
Data length: 8
Name Server: asia1.akam.net
- ✓ mit.edu: type NS, class IN, ns eur5.akam.net
Name: mit.edu
Type: NS (2) (authoritative Name Server)
Class: IN (0x0001)
Time to live: 1800 (30 minutes)
Data length: 7
Name Server: eur5.akam.net

```
✓ mit.edu: type NS, class IN, ns asia2.akam.net
  Name: mit.edu
  Type: NS (2) (authoritative Name Server)
  Class: IN (0x0001)
  Time to live: 1800 (30 minutes)
  Data length: 8
  Name Server: asia2.akam.net
✓ mit.edu: type NS, class IN, ns use2.akam.net
  Name: mit.edu
  Type: NS (2) (authoritative Name Server)
  Class: IN (0x0001)
  Time to live: 1800 (30 minutes)
  Data length: 7
  Name Server: use2.akam.net
```

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 nameservers?

由上图可知，提供了 ns1-173.akam.net、usw2.akam.net、ns1-37.akam.net、use5.akam.net、asia1.akam.net、eur5.akam.net、asia2.akam.net、use2.akam.net 这些 nameservers，且同时也在下文提供了这些 nameservers 的地址

NAME SERVER: use2.akam.net

✓ Additional records

✓ eur5.akam.net: type A, class IN, addr 23.74.25.64

Name: eur5.akam.net

Type: A (1) (Host Address)

Class: IN (0x0001)

Time to live: 33721 (9 hours, 22 minutes, 1 second)

Data length: 4

Address: 23.74.25.64

✓ use2.akam.net: type A, class IN, addr 96.7.49.64

Name: use2.akam.net

Type: A (1) (Host Address)

Class: IN (0x0001)

Time to live: 33718 (9 hours, 21 minutes, 58 seconds)

Data length: 4

Address: 96.7.49.64

✓ use5.akam.net: type A, class IN, addr 2.16.40.64

Name: use5.akam.net

Type: A (1) (Host Address)

Class: IN (0x0001)

Time to live: 34550 (9 hours, 35 minutes, 50 seconds)

Data length: 4

Address: 2.16.40.64

✓ use5.akam.net: type AAAA, class IN, addr 2600:1403:a::40

✓ use5.akam.net: type AAAA, class IN, addr 2600:1403:a::40

Name: use5.akam.net

Type: AAAA (28) (IP6 Address)

Class: IN (0x0001)

Time to live: 34550 (9 hours, 35 minutes, 50 seconds)

Data length: 16

AAAA Address: 2600:1403:a::40

✓ usw2.akam.net: type A, class IN, addr 184.26.161.64

Name: usw2.akam.net

Type: A (1) (Host Address)

Class: IN (0x0001)

Time to live: 35050 (9 hours, 44 minutes, 10 seconds)

Data length: 4

Address: 184.26.161.64

✓ asia1.akam.net: type A, class IN, addr 95.100.175.64

Name: asia1.akam.net

Type: A (1) (Host Address)

Class: IN (0x0001)

Time to live: 33724 (9 hours, 22 minutes, 4 seconds)

Data length: 4

Address: 95.100.175.64

✓ asia2.akam.net: type A, class IN, addr 95.101.36.64

```

    Name: asia2.akam.net
    Type: A (1) (Host Address)
    Class: IN (0x0001)
    Time to live: 52827 (14 hours, 40 minutes, 27 seconds)
    Data length: 4
    Address: 95.101.36.64
  ✓ ns1-37.akam.net: type A, class IN, addr 193.108.91.37
    Name: ns1-37.akam.net
    Type: A (1) (Host Address)
    Class: IN (0x0001)
    Time to live: 35050 (9 hours, 44 minutes, 10 seconds)
    Data length: 4
    Address: 193.108.91.37
  ✓ ns1-37.akam.net: type AAAA, class IN, addr 2600:1401:2::25
    Name: ns1-37.akam.net
    Type: AAAA (28) (IP6 Address)
    Class: IN (0x0001)
    Time to live: 35050 (9 hours, 44 minutes, 10 seconds)
    Data length: 16
    AAAA Address: 2600:1401:2::25

  ✓ ns1-37.akam.net: type AAAA, class IN, addr 2600:1401:2::25
    Name: ns1-37.akam.net
    Type: AAAA (28) (IP6 Address)
    Class: IN (0x0001)
    Time to live: 35050 (9 hours, 44 minutes, 10 seconds)
    Data length: 16
    AAAA Address: 2600:1401:2::25

  ✓ ns1-173.akam.net: type A, class IN, addr 193.108.91.173
    Name: ns1-173.akam.net
    Type: A (1) (Host Address)
    Class: IN (0x0001)
    Time to live: 35050 (9 hours, 44 minutes, 10 seconds)
    Data length: 4
    Address: 193.108.91.173
  ✓ ns1-173.akam.net: type AAAA, class IN, addr 2600:1401:2::ad
    Name: ns1-173.akam.net
    Type: AAAA (28) (IP6 Address)
    Class: IN (0x0001)
    Time to live: 35050 (9 hours, 44 minutes, 10 seconds)
    Data length: 16
    AAAA Address: 2600:1401:2::ad
\[Request In: 996\]
[Time: 0.053001000 seconds]

```

19. Provide a screenshot.

截图均在上文文中。

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?

1	2007-07-23	22:08:44.221178	192.168.1.101	68.87.71.226	DNS	85	Standard query 0x0001 PTR 226.71.87.68.in-addr.arpa
2	2007-07-23	22:08:44.233659	68.87.71.226	192.168.1.101	DNS	137	Standard query response 0x0001 PTR 226.71.87.68.in-addr.arpa PTR cns.chelmsfordc2.ma.boston.comcast.net
3	2007-07-23	22:08:44.235410	192.168.1.101	68.87.71.226	DNS	91	Standard query 0x0002 A www.mit.edu.hsd1.ma.comcast.net
4	2007-07-23	22:08:44.263819	68.87.71.226	192.168.1.101	DNS	171	Standard query response 0x0002 No such name A www.mit.edu.hsd1.ma.comcast.net SOA dns1.inflow.pa.bo.comcast.net
5	2007-07-23	22:08:44.265356	192.168.1.101	68.87.71.226	DNS	86	Standard query 0x0003 A www.mit.edu.ma.comcast.net
6	2007-07-23	22:08:44.280112	68.87.71.226	192.168.1.101	DNS	86	Standard query response 0x0003 Server failure A www.mit.edu.ma.comcast.net
7	2007-07-23	22:08:44.281446	192.168.1.101	68.87.71.226	DNS	71	Standard query 0x0004 A www.mit.edu
8	2007-07-23	22:08:44.296363	68.87.71.226	192.168.1.101	DNS	87	Standard query response 0x0004 A www.mit.edu A 18.7.22.83
28	2007-07-23	22:09:24.003137	192.168.1.101	68.87.71.226	DNS	85	Standard query 0x0001 PTR 226.71.87.68.in-addr.arpa
29	2007-07-23	22:09:24.016016	68.87.71.226	192.168.1.101	DNS	137	Standard query response 0x0001 PTR 226.71.87.68.in-addr.arpa PTR cns.chelmsfordc2.ma.boston.comcast.net
30	2007-07-23	22:09:24.017955	192.168.1.101	68.87.71.226	DNS	87	Standard query 0x0002 NS mit.edu.hsd1.ma.comcast.net
31	2007-07-23	22:09:24.044962	68.87.71.226	192.168.1.101	DNS	167	Standard query response 0x0002 No such name NS mit.edu.hsd1.ma.comcast.net SOA dns1.inflow.pa.bo.comcast.net
32	2007-07-23	22:09:24.046353	192.168.1.101	68.87.71.226	DNS	82	Standard query 0x0003 NS mit.edu.ma.comcast.net
33	2007-07-23	22:09:24.059551	68.87.71.226	192.168.1.101	DNS	82	Standard query response 0x0003 Server failure NS mit.edu.ma.comcast.net
34	2007-07-23	22:09:24.060977	192.168.1.101	68.87.71.226	DNS	67	Standard query 0x0004 NS mit.edu
35	2007-07-23	22:09:24.073413	68.87.71.226	192.168.1.101	DNS	176	Standard query response 0x0004 NS mit.edu NS W2BNS.mit.edu NS BITSY.mit.edu NS STRAWB.mit.edu A 18.72.0.3 A 18.71.0.151 A 18.70.0.160

发到 68.87.71.226 了，这和本地的 DNS 服务器是不一样的。他应该对应了 bitsy.mit.edu 的地址

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

```
> Frame 35: 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits)
> Ethernet II, Src: CiscoLinksys_f4:eb:a8 (00:16:b6:f4:eb:a8), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
> Internet Protocol Version 4, Src: 68.87.71.226, Dst: 192.168.1.101
> User Datagram Protocol, Src Port: 53, Dst Port: 4379
> Domain Name System (response)
  Transaction ID: 0x0004
  > Flags: 0x8180 Standard query response, No error
    1... .. = Response: Message is a response
    .000 0... .. = Opcode: Standard query (0)
    .... .. = Authoritative: Server is not an authority for domain
    .... .. = 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: 3
  Authority RRs: 0
  Additional RRs: 3
  > Queries
    > mit.edu: type NS, class IN
      Name: mit.edu
      [Name Length: 7]
```

这个 DNS query 的类型是 Standard query response, No error
Answers 为


```

  v Answers
  v mit.edu: type NS, class IN, ns W20NS.mit.edu
    Name: mit.edu
    Type: NS (2) (authoritative Name Server)
    Class: IN (0x0001)
    Time to live: 21493 (5 hours, 58 minutes, 13 seconds)
    Data length: 8
    Name Server: W20NS.mit.edu
  v mit.edu: type NS, class IN, ns BITSY.mit.edu
    Name: mit.edu
    Type: NS (2) (authoritative Name Server)
    Class: IN (0x0001)
    Time to live: 21493 (5 hours, 58 minutes, 13 seconds)
    Data length: 8
    Name Server: BITSY.mit.edu
  v mit.edu: type NS, class IN, ns STRAWB.mit.edu
    Name: mit.edu
    Type: NS (2) (authoritative Name Server)
    Class: IN (0x0001)
    Time to live: 21493 (5 hours, 58 minutes, 13 seconds)
    Data length: 9
    Name Server: STRAWB.mit.edu
  .....

```

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

如上图，一共有 3 个 answers，每个回复包括域名、类型、类别、time to live、数据长度、Name Server.

23. Provide a screenshot.

截图均在上文文中。

问题及收获：

DNS 是互联网的核心基础设施之一，它的主要功能是将人类可读的域名转换为计算机可识别的 IP 地址。DNS 的存在使得互联网用户能够更方便、更高效地访问网络资源，而无需记住复杂的数字 IP 地址。并且也可以提供灵活性和可管理性，能够实现负载均衡、故障转移，增强了安全性和隐私保护，促进了全球互联网的互联互通。