

浙江大学



课程名称： 计算机网络与通信

报告题目： DNS

指导老师： 徐文渊

学 院： 电气工程学院

专业与班级： 自动化 1703

姓名与学号： 潘盛琪 3170105737

1. Run *nslookup* to obtain the IP address of a Web server in Asia.

For this question, I queried the webpage of Zhejiang university, which is in Asia

The IP address of www.zju.edu.cn is 10.203.6.101

```
Microsoft Windows [版本 10.0.18362.356]
(c) 2019 Microsoft Corporation。保留所有权利。

C:\Users\Rookie>nslookup www.zju.edu.cn
服务器:  dns1.zju.edu.cn
Address:  10.10.0.21

名称:     www.zju.edu.cn
Address:  10.203.6.101
```

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

I queried the webpage of Cambridge. There are five authoritative DNS servers for Cambridge as listed below:

- sns-pb.isc.org
- authdns0.csx.cam.ac.uk
- ns2.ic.ac.uk
- dns0.cl.cam.ac.uk
- dns0.eng.cam.ac.uk

```
C:\Users\Rookie>nslookup -type=NS cam.ac.uk.
服务器:  dns1.zju.edu.cn
Address:  10.10.0.21

非权威应答:
cam.ac.uk      nameserver = sns-pb.isc.org
cam.ac.uk      nameserver = authdns0.csx.cam.ac.uk
cam.ac.uk      nameserver = ns2.ic.ac.uk
cam.ac.uk      nameserver = dns0.cl.cam.ac.uk
cam.ac.uk      nameserver = dns0.eng.cam.ac.uk

ns2.ic.ac.uk   internet address = 155.198.142.82
dns0.eng.cam.ac.uk internet address = 129.169.8.8
sns-pb.isc.org internet address = 192.5.4.1
authdns0.csx.cam.ac.uk internet address = 131.111.8.37
ns2.ic.ac.uk   AAAA IPv6 address = 2001:630:12:600:1::82
dns0.cl.cam.ac.uk AAAA IPv6 address = 2001:630:212:200::d:a0
sns-pb.isc.org AAAA IPv6 address = 2001:500:2e::1
authdns0.csx.cam.ac.uk AAAA IPv6 address = 2001:630:212:8::d:a0
```

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

The IP address for the DNS server if queried for the Yahoo! mail server is 69.147.88.8

```
C:\Users\Rookie>nslookup cam.ac.uk mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
服务器: UnKnown
Address: 69.147.88.8

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** 请求 UnKnown 超时
```

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

There are four DNS query and response messages shown below.

As is shown in the following pictures, they are all sent over UDP

| | | | | | |
|------|-----------------|--------------|--------------|---------|---|
| 413 | 20:03:52.657699 | 10.110.33.41 | 10.10.0.21 | DNS | 72 Standard query 0x671d A www.ietf.org |
| 414 | 20:03:52.658394 | 10.10.0.21 | 10.110.33.41 | DNS | 239 Standard query response 0x671d A www.ietf.org CNAME www.ietf.org |
| 415 | 20:03:52.658677 | 10.110.33.41 | 10.10.0.21 | DNS | 72 Standard query 0xba55 AAAA www.ietf.org |
| 417 | 20:03:52.659744 | 10.10.0.21 | 10.110.33.41 | DNS | 554 Standard query response 0xba55 AAAA www.ietf.org CNAME www.ietf.org |
| 1312 | 20:03:56.254184 | 10.110.33.41 | 224.0.0.22 | IGMPv3 | 54 Membership Report / Join group 224.0.0.252 for any sources |
| 2206 | 20:03:57.754012 | 10.110.33.41 | 224.0.0.22 | IGMPv3 | 54 Membership Report / Join group 224.0.0.251 for any sources |
| 2633 | 20:03:58.656938 | 10.0.2.3 | 10.110.33.41 | PPP LCP | 60 Echo Request |
| 2634 | 20:03:58.657174 | 10.110.33.41 | 10.0.2.3 | PPP LCP | 62 Echo Reply |
| 2683 | 20:03:58.754112 | 10.110.33.41 | 224.0.0.22 | IGMPv3 | 54 Membership Report / Join group 239.255.255.250 for any sources |
| 4319 | 20:04:02.786824 | 10.0.2.3 | 10.110.33.41 | L2TP | 62 Control Message - Hello (tunnel id=4, session id=0) |

> Frame 413: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0

> Ethernet II, Src: Dell_f2:fd:99 (f4:8e:38:f2:fd:99), Dst: Hangzhou_00:95:03 (5c:dd:70:00:95:03)

> Internet Protocol Version 4, Src: 10.110.33.41, Dst: 10.10.0.21

> User Datagram Protocol, Src Port: 54374 (54374), Dst Port: domain (53)

> Domain Name System (query)

| | | | | | |
|------|-----------------|--------------|--------------|---------|---|
| 413 | 20:03:52.657699 | 10.110.33.41 | 10.10.0.21 | DNS | 72 Standard query 0x671d A www.ietf.org |
| 414 | 20:03:52.658394 | 10.10.0.21 | 10.110.33.41 | DNS | 239 Standard query response 0x671d A www.ietf.org CNAME www.ietf.org |
| 415 | 20:03:52.658677 | 10.110.33.41 | 10.10.0.21 | DNS | 72 Standard query 0xba55 AAAA www.ietf.org |
| 417 | 20:03:52.659744 | 10.10.0.21 | 10.110.33.41 | DNS | 554 Standard query response 0xba55 AAAA www.ietf.org CNAME www.ietf.org |
| 1312 | 20:03:56.254184 | 10.110.33.41 | 224.0.0.22 | IGMPv3 | 54 Membership Report / Join group 224.0.0.252 for any sources |
| 2206 | 20:03:57.754012 | 10.110.33.41 | 224.0.0.22 | IGMPv3 | 54 Membership Report / Join group 224.0.0.251 for any sources |
| 2633 | 20:03:58.656938 | 10.0.2.3 | 10.110.33.41 | PPP LCP | 60 Echo Request |
| 2634 | 20:03:58.657174 | 10.110.33.41 | 10.0.2.3 | PPP LCP | 62 Echo Reply |
| 2683 | 20:03:58.754112 | 10.110.33.41 | 224.0.0.22 | IGMPv3 | 54 Membership Report / Join group 239.255.255.250 for any sources |
| 4319 | 20:04:02.786824 | 10.0.2.3 | 10.110.33.41 | L2TP | 62 Control Message - Hello (tunnel id=4, session id=0) |

> Frame 414: 239 bytes on wire (1912 bits), 239 bytes captured (1912 bits) on interface 0

> Ethernet II, Src: Hangzhou_00:95:03 (5c:dd:70:00:95:03), Dst: Dell_f2:fd:99 (f4:8e:38:f2:fd:99)

> Internet Protocol Version 4, Src: 10.10.0.21, Dst: 10.110.33.41

> User Datagram Protocol, Src Port: domain (53), Dst Port: 54374 (54374)

> Domain Name System (response)

| | | | | | |
|------|-----------------|--------------|--------------|---------|--|
| 413 | 20:03:52.657699 | 10.110.33.41 | 10.10.0.21 | DNS | 72 Standard query 0x671d A www.ietf.org |
| 414 | 20:03:52.658394 | 10.10.0.21 | 10.110.33.41 | DNS | 239 Standard query response 0x671d A www.ietf.org |
| 415 | 20:03:52.658677 | 10.110.33.41 | 10.10.0.21 | DNS | 72 Standard query 0xba55 AAAA www.ietf.org |
| 417 | 20:03:52.659744 | 10.10.0.21 | 10.110.33.41 | DNS | 554 Standard query response 0xba55 AAAA www.ietf.org |
| 1312 | 20:03:56.254184 | 10.110.33.41 | 224.0.0.22 | IGMPv3 | 54 Membership Report / Join group 224.0.0.252 |
| 2206 | 20:03:57.754012 | 10.110.33.41 | 224.0.0.22 | IGMPv3 | 54 Membership Report / Join group 224.0.0.251 |
| 2633 | 20:03:58.656938 | 10.0.2.3 | 10.110.33.41 | PPP LCP | 60 Echo Request |
| 2634 | 20:03:58.657174 | 10.110.33.41 | 10.0.2.3 | PPP LCP | 62 Echo Reply |
| 2683 | 20:03:58.754112 | 10.110.33.41 | 224.0.0.22 | IGMPv3 | 54 Membership Report / Join group 239.255.255. |
| 4319 | 20:04:02.786824 | 10.0.2.3 | 10.110.33.41 | L2TP | 62 Control Message - Hello (tunnel id=4, sessi |

> Frame 415: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
 > Ethernet II, Src: Dell_f2:fd:99 (f4:8e:38:f2:fd:99), Dst: Hangzhou_00:95:03 (5c:dd:70:00:95:03)
 > Internet Protocol Version 4, Src: 10.110.33.41, Dst: 10.10.0.21
 > User Datagram Protocol, Src Port: 56509 (56509), Dst Port: domain (53)
 > Domain Name System (query)

| | | | | | |
|------|-----------------|--------------|--------------|---------|---|
| 413 | 20:03:52.657699 | 10.110.33.41 | 10.10.0.21 | DNS | 72 Standard query 0x671d A www.ietf.org |
| 414 | 20:03:52.658394 | 10.10.0.21 | 10.110.33.41 | DNS | 239 Standard query response 0x671d A www.ietf.org CNAME www.ietf.org |
| 415 | 20:03:52.658677 | 10.110.33.41 | 10.10.0.21 | DNS | 72 Standard query 0xba55 AAAA www.ietf.org |
| 417 | 20:03:52.659744 | 10.10.0.21 | 10.110.33.41 | DNS | 554 Standard query response 0xba55 AAAA www.ietf.org CNAME www.ietf.org |
| 1312 | 20:03:56.254184 | 10.110.33.41 | 224.0.0.22 | IGMPv3 | 54 Membership Report / Join group 224.0.0.252 for any sources |
| 2206 | 20:03:57.754012 | 10.110.33.41 | 224.0.0.22 | IGMPv3 | 54 Membership Report / Join group 224.0.0.251 for any sources |
| 2633 | 20:03:58.656938 | 10.0.2.3 | 10.110.33.41 | PPP LCP | 60 Echo Request |
| 2634 | 20:03:58.657174 | 10.110.33.41 | 10.0.2.3 | PPP LCP | 62 Echo Reply |
| 2683 | 20:03:58.754112 | 10.110.33.41 | 224.0.0.22 | IGMPv3 | 54 Membership Report / Join group 239.255.255.250 for any sources |
| 4319 | 20:04:02.786824 | 10.0.2.3 | 10.110.33.41 | L2TP | 62 Control Message - Hello (tunnel id=4, session id=0) |

> Frame 417: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface 0
 > Ethernet II, Src: Hangzhou_00:95:03 (5c:dd:70:00:95:03), Dst: Dell_f2:fd:99 (f4:8e:38:f2:fd:99)
 > Internet Protocol Version 4, Src: 10.10.0.21, Dst: 10.110.33.41
 > User Datagram Protocol, Src Port: domain (53), Dst Port: 56509 (56509)
 > Domain Name System (response)

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

As is shown in the following pictures, the destination port for the DNS query message and the source port of DNS response message are all 53. They are all the same, which is correspondence to the text book.

| | | | | | |
|------|-----------------|--------------|--------------|---------|--|
| 413 | 20:03:52.657699 | 10.110.33.41 | 10.10.0.21 | DNS | 72 Standard query 0x671d A www.ietf.org |
| 414 | 20:03:52.658394 | 10.10.0.21 | 10.110.33.41 | DNS | 239 Standard query response 0x671d A www.ietf.org |
| 415 | 20:03:52.658677 | 10.110.33.41 | 10.10.0.21 | DNS | 72 Standard query 0xba55 AAAA www.ietf.org |
| 417 | 20:03:52.659744 | 10.10.0.21 | 10.110.33.41 | DNS | 554 Standard query response 0xba55 AAAA www.ietf.org |
| 1312 | 20:03:56.254184 | 10.110.33.41 | 224.0.0.22 | IGMPv3 | 54 Membership Report / Join group 224.0.0.252 |
| 2206 | 20:03:57.754012 | 10.110.33.41 | 224.0.0.22 | IGMPv3 | 54 Membership Report / Join group 224.0.0.251 |
| 2683 | 20:03:58.754112 | 10.110.33.41 | 224.0.0.22 | IGMPv3 | 54 Membership Report / Join group 239.255.255. |
| 4319 | 20:04:02.786824 | 10.0.2.3 | 10.110.33.41 | L2TP | 62 Control Message - Hello (tunnel id=4, session id=0) |
| 4320 | 20:04:02.786948 | 10.110.33.41 | 10.0.2.3 | L2TP | 54 Control Message - ZLB (tunnel id=4, session id=0) |
| 2633 | 20:03:58.656938 | 10.0.2.3 | 10.110.33.41 | PPP LCP | 60 Echo Request |

> Frame 413: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
 > Ethernet II, Src: Dell_f2:fd:99 (f4:8e:38:f2:fd:99), Dst: Hangzhou_00:95:03 (5c:dd:70:00:95:03)
 > Internet Protocol Version 4, Src: 10.110.33.41, Dst: 10.10.0.21
 > User Datagram Protocol, Src Port: 54374 (54374), Dst Port: domain (53)
 Source Port: 54374 (54374)
 Destination Port: domain (53)
 Length: 38
 Checksum: 0x6bee [unverified]
 [Checksum Status: Unverified]
 [Stream index: 121]
 > [Timestamps]
 > Domain Name System (query)

| | | | | | |
|------|-----------------|--------------|--------------|---------|---|
| 413 | 20:03:52.657699 | 10.110.33.41 | 10.10.0.21 | DNS | 72 Standard query 0x671d A www.ietf.org |
| 414 | 20:03:52.658394 | 10.10.0.21 | 10.110.33.41 | DNS | 239 Standard query response 0x671d A www.ietf.org CNAME www.ietf.org |
| 415 | 20:03:52.658677 | 10.110.33.41 | 10.10.0.21 | DNS | 72 Standard query 0xba55 AAAA www.ietf.org |
| 417 | 20:03:52.659744 | 10.10.0.21 | 10.110.33.41 | DNS | 554 Standard query response 0xba55 AAAA www.ietf.org CNAME www.ietf.org |
| 1312 | 20:03:56.254184 | 10.110.33.41 | 224.0.0.22 | IGMPv3 | 54 Membership Report / Join group 224.0.0.252 for any sources |
| 2206 | 20:03:57.754012 | 10.110.33.41 | 224.0.0.22 | IGMPv3 | 54 Membership Report / Join group 224.0.0.251 for any sources |
| 2683 | 20:03:58.754112 | 10.110.33.41 | 224.0.0.22 | IGMPv3 | 54 Membership Report / Join group 239.255.255.250 for any sources |
| 4319 | 20:04:02.786824 | 10.0.2.3 | 10.110.33.41 | L2TP | 62 Control Message - Hello (tunnel id=4, session id=0) |
| 4320 | 20:04:02.786948 | 10.110.33.41 | 10.0.2.3 | L2TP | 54 Control Message - ZLB (tunnel id=35536, session id=0) |
| 2633 | 20:03:58.656938 | 10.0.2.3 | 10.110.33.41 | PPP LCP | 60 Echo Request |

> Frame 414: 239 bytes on wire (1912 bits), 239 bytes captured (1912 bits) on interface 0

> Ethernet II, Src: Hangzhou_00:95:03 (5c:dd:70:00:95:03), Dst: Dell_f2:fd:99 (f4:8e:38:f2:fd:99)

> Internet Protocol Version 4, Src: 10.10.0.21, Dst: 10.110.33.41

> User Datagram Protocol, Src Port: domain (53), Dst Port: 54374 (54374)

> Source Port: domain (53)

Destination Port: 54374 (54374)

Length: 205

Checksum: 0x818a [unverified]

[Checksum Status: Unverified]

[Stream index: 121]

> [Timestamps]

> Domain Name System (response)

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?

The DNS query message is sent to 10.10.0.21 as is shown in the first picture.

Use *ipconfig /all* to find out the IP address of my local DNS server, which is shown in the second picture.

They are absolutely the same.

| | | | |
|--------------|--------------|-----|---|
| 10.110.33.41 | 10.10.0.21 | DNS | 72 Standard query 0x671d A www.ietf.org |
| 10.10.0.21 | 10.110.33.41 | DNS | 239 Standard query response 0x671d A www.ietf.org CNAME www.ietf.org.cdn.cloudflare |

```

C:\WINDOWS\system32\cmd.exe
物理地址. . . . . : 3A-BA-F8-01-3C-90
DHCP 已启用. . . . . : 是
自动配置已启用. . . . . : 是

以太网适配器 以太网:

   连接特定的 DNS 后缀 . . . . . :
   描述. . . . . : Realtek PCIe GBE Family Controller
   物理地址. . . . . : F4-39-09-81-99-C0
   DHCP 已启用. . . . . : 否
   自动配置已启用. . . . . : 是
   IPv6 地址. . . . . : 2001:da8:e000:79:84e3:f81e:c6d7:1408(首选)
   IPv6 地址. . . . . : 2001:da8:e000:1a05:84e3:f81e:c6d7:1408(首选)
   临时 IPv6 地址. . . . . : 2001:da8:e000:79:68a7:77ac:be71:1ed0(首选)
   临时 IPv6 地址. . . . . : 2001:da8:e000:1a05:68a7:77ac:be71:1ed0(首选)
   本地链接 IPv6 地址. . . . . : fe80::84e3:f81e:c6d7:1408%12(首选)
   IPv4 地址. . . . . : 10.110.33.93(首选)
   子网掩码. . . . . : 255.255.255.0
   默认网关. . . . . : fe80::5edd:70ff:fe00:9503%12
   . . . . . : 10.110.33.1
   DHCPv6 IAID. . . . . : 150223113
   DHCPv6 客户端 DUID. . . . . : 00-01-00-01-23-33-29-0F-F4-39-09-81-99-C0
   DNS 服务器. . . . . : 10.10.0.21
   TCP/IP 上的 NetBIOS. . . . . : 已启用

PPP 适配器 ZJUVPN:

   连接特定的 DNS 后缀 . . . . . :
   描述. . . . . : ZJUVPN
   物理地址. . . . . :

```

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

The DNS query message is shown below. It’s a Type A DNS query and no answers are contained.

```
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
v Queries
  v www.ietf.org: type A, class IN
    Name: www.ietf.org
    [Name Length: 12]
    [Label Count: 3]
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    [Response In: 414]
```

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

As is shown in the picture, one answer is provided in the DNS response message.

Name, Type, Class, Time to Live, Data Length and Address are contained in the response.

```
> Layer 2 Tunneling Protocol
> Point-to-Point Protocol
> Internet Protocol Version 4, Src: 10.10.0.21, Dst: 222.205.1.164
> User Datagram Protocol, Src Port: 53, Dst Port: 65330
v Domain Name System (response)
  Transaction ID: 0xe132
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 6
  Additional RRs: 0
  > Queries
  v Answers
    v ietf.org: type A, class IN, addr 4.31.198.44
      Name: ietf.org
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 10920
      Data length: 4
      Address: 4.31.198.44
  > Authoritative nameservers
  [Request In: 1500]
  [Time: 0.000923000 seconds]
```

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?

The destination IP address of the SYN packet is the same as the IP address provided in the DNS response message as is shown in the picture above and the picture below.

| | | | | | |
|------|-----------------|---------------|-------------|-----|--|
| 1503 | 22:59:21.768207 | 222.205.1.164 | 4.31.198.44 | TCP | 106 62117 → 80 [SYN] Seq=0 Win=65280 Len=0 MSS=1360 WS=256 SACK_PERM=1 |
| 1513 | 22:59:22.014224 | 222.205.1.164 | 4.31.198.44 | TCP | 106 62118 → 80 [SYN] Seq=0 Win=65280 Len=0 MSS=1360 WS=256 SACK_PERM=1 |

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

No, the images are all loaded from www.ietf.org, so no more DNS queries are necessary.

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------------|----------------|-----------------|----------|--------|--|
| 1500 | 22:59:21.763026 | 222.205.1.164 | 10.10.0.21 | DNS | 108 | Standard query 0xe132 A ietf.org |
| 1501 | 22:59:21.763949 | 10.10.0.21 | 222.205.1.164 | DNS | 279 | Standard query response 0xe132 A ietf.org A 4.31.198.44 NS ns1.mia.afiliias-nst.info NS ns1.hkg1.afiliias-nst.info |
| 1551 | 22:59:22.395340 | 222.205.1.164 | 10.10.0.21 | DNS | 112 | Standard query 0x8723 A www.ietf.org |
| 1552 | 22:59:22.398960 | 10.10.0.21 | 222.205.1.164 | DNS | 293 | Standard query response 0x8723 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.1.85 A 104.20.1.85 |
| 697 | 22:59:13.397349 | 222.205.1.164 | 123.151.176.26 | HTTP | 409 | POST /_cg1 HTTP/1.1 |
| 702 | 22:59:13.433695 | 123.151.176.26 | 222.205.1.164 | HTTP | 254 | HTTP/1.1 200 OK |
| 1300 | 22:59:19.546353 | 222.205.1.164 | 205.210.165.142 | HTTP | 1454 | GET /post.php?id=X51a007590674%1e16b80%42e0%bf%ce%8e17%fe%ad61b8%b218%a7%61%65%d9%54%57%79%41 |
| 1301 | 22:59:19.546371 | 222.205.1.164 | 205.210.165.142 | HTTP | 132 | Continuation |
| 1303 | 22:59:19.547204 | 222.205.1.164 | 205.210.165.142 | HTTP | 553 | Continuation[Malformed Packet] |
| 1304 | 22:59:19.547271 | 222.205.1.164 | 205.210.165.142 | HTTP | 1349 | Continuation |

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

The destination port for the DNS query message is 53.

The source port of DNS response message is also 53.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------|-----------------|---------------|---------------|---------|---|
| | 1912 | 23:12:47.984007 | 222.205.1.164 | 10.10.0.21 | DNS | 123 Standard query 0x0001 PTR 21.0.10.10.in-addr.arpa |
| | 1913 | 23:12:47.984910 | 10.10.0.21 | 222.205.1.164 | DNS | 180 Standard query response 0x0001 PTR 21.0.10.10.in-addr.arpa PTR dns1.zju |
| | 1916 | 23:12:47.989086 | 222.205.1.164 | 10.10.0.21 | DNS | 111 Standard query 0x0002 A www.mit.edu |
| | 1917 | 23:12:47.992363 | 10.10.0.21 | 222.205.1.164 | DNS | 414 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey. |
| | 1918 | 23:12:47.994187 | 222.205.1.164 | 10.10.0.21 | DNS | 111 Standard query 0x0003 AAAA www.mit.edu |
| | 1932 | 23:12:48.095680 | 10.10.0.21 | 222.205.1.164 | DNS | 562 Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgek |
| | 194 | 23:12:29.521668 | 10.110.33.41 | 224.0.0.22 | IGMPv3 | 54 Membership Report / Join group 224.0.0.252 for any sources |
| | 408 | 23:12:30.521076 | 10.110.33.41 | 224.0.0.22 | IGMPv3 | 54 Membership Report / Join group 224.0.0.251 for any sources |
| | 599 | 23:12:32.021049 | 10.110.33.41 | 224.0.0.22 | IGMPv3 | 54 Membership Report / Join group 239.255.255.250 for any sources |
| | 1434 | 23:12:39.989551 | 10.0.2.3 | 10.110.33.41 | PPP LCP | 60 Echo Request |
| | 1435 | 23:12:39.989816 | 10.110.33.41 | 10.0.2.3 | PPP LCP | 62 Echo Reply |

```
> Frame 1916: 111 bytes on wire (888 bits), 111 bytes captured (888 bits) on interface 0
> Ethernet II, Src: Dell_f2:f2:99 (f4:8e:38:f2:fd:99), Dst: Hangzhou_00:95:03 (5c:dd:70:00:95:03)
> Internet Protocol Version 4, Src: 10.110.33.41, Dst: 10.0.2.3
> User Datagram Protocol, Src Port: 1701, Dst Port: 1701
> Layer 2 Tunneling Protocol
> Point-to-Point Protocol
> Internet Protocol Version 4, Src: 222.205.1.164, Dst: 10.10.0.21
√ User Datagram Protocol, Src Port: 54685, Dst Port: 53
    Source Port: 54685
    Destination Port: 53
    Length: 37
    Checksum: 0xc93 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 145]
    > [Timestamps]
> Domain Name System (query)
```


| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------------|---------------|---------------|----------|--------|--|
| 1912 | 23:12:47.984007 | 222.205.1.164 | 10.10.0.21 | DNS | 123 | Standard query 0x0001 PTR 21.0.10.10.in-addr.arpa |
| 1913 | 23:12:47.984910 | 10.10.0.21 | 222.205.1.164 | DNS | 180 | Standard query response 0x0001 PTR 21.0.10.10.in-addr. |
| 1916 | 23:12:47.989086 | 222.205.1.164 | 10.10.0.21 | DNS | 111 | Standard query 0x0002 A www.mit.edu |
| 1917 | 23:12:47.992363 | 10.10.0.21 | 222.205.1.164 | DNS | 414 | Standard query response 0x0002 A www.mit.edu CNAME www |
| 1918 | 23:12:47.994187 | 222.205.1.164 | 10.10.0.21 | DNS | 111 | Standard query 0x0003 AAAA www.mit.edu |
| 1932 | 23:12:48.095680 | 10.10.0.21 | 222.205.1.164 | DNS | 562 | Standard query response 0x0003 AAAA www.mit.edu CNAME |
| 194 | 23:12:29.521668 | 10.110.33.41 | 224.0.0.22 | IGMPv3 | 54 | Membership Report / Join group 224.0.0.252 for any sou |
| 408 | 23:12:30.521076 | 10.110.33.41 | 224.0.0.22 | IGMPv3 | 54 | Membership Report / Join group 224.0.0.251 for any sou |
| 599 | 23:12:32.021049 | 10.110.33.41 | 224.0.0.22 | IGMPv3 | 54 | Membership Report / Join group 239.255.255.250 for any |
| 1434 | 23:12:39.989551 | 10.0.2.3 | 10.110.33.41 | PPP LCP | 60 | Echo Request |
| 1435 | 23:12:39.989816 | 10.110.33.41 | 10.0.2.3 | PPP LCP | 62 | Echo Reply |

> Frame 1917: 414 bytes on wire (3312 bits), 414 bytes captured (3312 bits) on interface 0
 > Ethernet II, Src: Hangzhou_00:95:03 (5c:dd:70:00:95:03), Dst: Dell_f2:fd:99 (f4:8e:38:f2:fd:99)
 > Internet Protocol Version 4, Src: 10.0.2.3, Dst: 10.110.33.41
 > User Datagram Protocol, Src Port: 1701, Dst Port: 1701
 > Layer 2 Tunneling Protocol
 > Point-to-Point Protocol
 > Internet Protocol Version 4, Src: 10.10.0.21, Dst: 222.205.1.164
 > User Datagram Protocol, Src Port: 53, Dst Port: 54685
 > Source Port: 53
 > Destination Port: 54685
 > Length: 342
 > Checksum: 0xedf8 [unverified]
 > [Checksum Status: Unverified]
 > [Stream index: 145]
 > [Timestamps]
 > Domain Name System (response)

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

The DNS query message is sent to 10.10.0.21.

Use ipconfig /all to find out the IP address of my local DNS server, which is shown in the second picture. They are absolutely the same.

| | | | | | | |
|------|-----------------|---------------|---------------|-----|-----|---|
| 1916 | 23:12:47.989086 | 222.205.1.164 | 10.10.0.21 | DNS | 111 | Standard query 0x0002 A www.mit.edu |
| 1917 | 23:12:47.992363 | 10.10.0.21 | 222.205.1.164 | DNS | 414 | Standard query response 0x0002 A www.mit.edu CNAME www.mit. |
| 1918 | 23:12:47.994187 | 222.205.1.164 | 10.10.0.21 | DNS | 111 | Standard query 0x0003 AAAA www.mit.edu |
| 1932 | 23:12:48.095680 | 10.10.0.21 | 222.205.1.164 | DNS | 562 | Standard query response 0x0003 AAAA www.mit.edu CNAME www. |

```

C:\WINDOWS\system32\cmd.exe
物理地址. . . . . : 3A-BA-F8-01-3C-90
DHCP 已启用. . . . . : 是
自动配置已启用. . . . . : 是

以太网适配器 以太网:

   连接特定的 DNS 后缀 . . . . . :
   描述. . . . . : Realtek PCIe GBE Family Controller
   物理地址. . . . . : F4-39-09-81-99-C0
   DHCP 已启用. . . . . : 是
   自动配置已启用. . . . . : 是
   IPv6 地址. . . . . : 2001:da8:e000:79:84e3:f81e:c6d7:1408(首选)
   IPv6 地址. . . . . : 2001:da8:e000:1a05:84e3:f81e:c6d7:1408(首选)
   临时 IPv6 地址. . . . . : 2001:da8:e000:79:68a7:77ac:be71:1ed0(首选)
   临时 IPv6 地址. . . . . : 2001:da8:e000:1a05:68a7:77ac:be71:1ed0(首选)
   本地链接 IPv6 地址. . . . . : fe80::84e3:f81e:c6d7:1408%12(首选)
   IPv4 地址. . . . . : 10.110.33.93(首选)
   子网掩码. . . . . : 255.255.255.0
   默认网关. . . . . : fe80::5add:70ff:fe00:9503%12
                       10.110.33.1
   DHCPv6 IAID. . . . . : 150223113
   DHCPv6 客户端 DUID. . . . . : 00-01-00-01-23-33-29-0F-F4-39-09-81-99-C0
   DNS 服务器. . . . . : 10.10.0.21
   ICP/IP 上的 NetBIOS. . . . . : 已启用

PPP 适配器 ZJUVPN:
  
```


Yes. (see the screenshot)

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

The DNS query message is shown below. It’s a Type A DNS query and no answers are contained.

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------------|---------------|---------------|----------|--------|---|
| 1912 | 23:12:47.984007 | 222.205.1.164 | 10.10.0.21 | DNS | 123 | Standard query 0x0001 PTR 21.0.10.10.in-addr.arpa |
| 1913 | 23:12:47.984910 | 10.10.0.21 | 222.205.1.164 | DNS | 180 | Standard query response 0x0001 PTR 21.0.10.10.in-addr |
| 1916 | 23:12:47.989086 | 222.205.1.164 | 10.10.0.21 | DNS | 111 | Standard query 0x0002 A www.mit.edu |
| 1917 | 23:12:47.992363 | 10.10.0.21 | 222.205.1.164 | DNS | 414 | Standard query response 0x0002 A www.mit.edu CNAME ww |
| 1918 | 23:12:47.994187 | 222.205.1.164 | 10.10.0.21 | DNS | 111 | Standard query 0x0003 AAAA www.mit.edu |
| 1932 | 23:12:48.095680 | 10.10.0.21 | 222.205.1.164 | DNS | 562 | Standard query response 0x0003 AAAA www.mit.edu CNAME |
| 194 | 23:12:29.521668 | 10.110.33.41 | 224.0.0.22 | IGMPv3 | 54 | Membership Report / Join group 224.0.0.252 for any so |
| 408 | 23:12:30.521076 | 10.110.33.41 | 224.0.0.22 | IGMPv3 | 54 | Membership Report / Join group 224.0.0.251 for any so |
| 599 | 23:12:32.021049 | 10.110.33.41 | 224.0.0.22 | IGMPv3 | 54 | Membership Report / Join group 239.255.255.250 for an |
| 1434 | 23:12:39.989551 | 10.0.2.3 | 10.110.33.41 | PPP LCP | 60 | Echo Request |
| 1435 | 23:12:39.989816 | 10.110.33.41 | 10.0.2.3 | PPP LCP | 62 | Echo Reply |

> Frame 1916: 111 bytes on wire (888 bits), 111 bytes captured (888 bits) on interface 0

> Ethernet II, Src: Dell_f2:fd:99 (f4:8e:38:f2:fd:99), Dst: Hangzhou_00:95:03 (5c:dd:70:00:95:03)

> Internet Protocol Version 4, Src: 10.110.33.41, Dst: 10.0.2.3

> User Datagram Protocol, Src Port: 1701, Dst Port: 1701

> Layer 2 Tunneling Protocol

> Point-to-Point Protocol

> Internet Protocol Version 4, Src: 222.205.1.164, Dst: 10.10.0.21

> User Datagram Protocol, Src Port: 54685, Dst Port: 53

▼ Domain Name System (query)

Transaction ID: 0x0002

> 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 (Host Address) (1)

Class: IN (0x0001)

[Response In: 1917]

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

Three answers are provided.

Two of them contains type, class and cname.

Another one contains type, class, addr.

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------------|---------------|---------------|----------|--------|--|
| 1912 | 23:12:47.984007 | 222.205.1.164 | 10.10.0.21 | DNS | 123 | Standard query 0x0001 PTR 21.0.10.10.in-addr.arpa |
| 1913 | 23:12:47.984910 | 10.10.0.21 | 222.205.1.164 | DNS | 180 | Standard query response 0x0001 PTR 21.0.10.10.in-addr.arpa PTR dns1.zj |
| 1916 | 23:12:47.989086 | 222.205.1.164 | 10.10.0.21 | DNS | 111 | Standard query 0x0002 A www.mit.edu |
| 1917 | 23:12:47.992363 | 10.10.0.21 | 222.205.1.164 | DNS | 414 | Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey |
| 1918 | 23:12:47.994187 | 222.205.1.164 | 10.10.0.21 | DNS | 111 | Standard query 0x0003 AAAA www.mit.edu |
| 1932 | 23:12:48.095680 | 10.10.0.21 | 222.205.1.164 | DNS | 562 | Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edge |
| 194 | 23:12:29.521668 | 10.110.33.41 | 224.0.0.22 | IGMPv3 | 54 | Membership Report / Join group 224.0.0.252 for any sources |
| 408 | 23:12:30.521076 | 10.110.33.41 | 224.0.0.22 | IGMPv3 | 54 | Membership Report / Join group 224.0.0.251 for any sources |
| 599 | 23:12:32.021049 | 10.110.33.41 | 224.0.0.22 | IGMPv3 | 54 | Membership Report / Join group 239.255.255.250 for any sources |
| 1434 | 23:12:39.989551 | 10.0.2.3 | 10.110.33.41 | PPP LCP | 60 | Echo Request |
| 1435 | 23:12:39.989816 | 10.110.33.41 | 10.0.2.3 | PPP LCP | 62 | Echo Reply |

> Ethernet II, Src: Hangzhou_00:95:03 (Sc:dd:70:00:95:03), Dst: Dell_f2:fd:99 (f4:8e:38:f2:fd:99)
 > Internet Protocol Version 4, Src: 10.0.2.3, Dst: 10.110.33.41
 > User Datagram Protocol, Src Port: 1701, Dst Port: 1701
 > Layer 2 Tunneling Protocol
 > Point-to-Point Protocol
 > Internet Protocol Version 4, Src: 10.10.0.21, Dst: 222.205.1.164
 > User Datagram Protocol, Src Port: 53, Dst Port: 54685
 > Domain Name System (response)
 > Transaction ID: 0x0002
 > Flags: 0x8180 Standard query response, No error
 > Questions: 1
 > Answer RRs: 3
 > Authority RRs: 8
 > Additional RRs: 3
 > 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 23.63.9.86
 > Authoritative nameservers
 > Additional records
 > [Request In: 1916]
 [Time: 0.003277000 seconds]

15. Provide a screenshot.

Already shown after every question

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

The DNS query message is sent to 10.10.0.21.

Use ipconfig /all to find out the IP address of my local DNS server, which is shown in the second picture.

They are absolutely the same.

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------------|----------------|----------------|----------|--------|---|
| 1756 | 23:41:35.891489 | 222.205.1.164 | 10.10.0.21 | DNS | 123 | Standard query 0x0001 PTR 21.0.10.10.in-addr.arpa |
| 1757 | 23:41:35.892363 | 10.10.0.21 | 222.205.1.164 | DNS | 180 | Standard query response 0x0001 PTR 21.0.10.10.in-addr.arpa PTR dns1.zju.e |
| 1758 | 23:41:35.894133 | 222.205.1.164 | 10.10.0.21 | DNS | 107 | Standard query 0x0002 NS mit.edu |
| 1759 | 23:41:35.896137 | 10.10.0.21 | 222.205.1.164 | DNS | 380 | Standard query response 0x0002 NS mit.edu NS asia2.akam.net NS use2.akam. |
| 810 | 23:41:17.762669 | 222.205.1.164 | 123.151.176.26 | HTTP | 553 | POST /q.cgi HTTP/1.1 |
| 819 | 23:41:17.798148 | 123.151.176.26 | 222.205.1.164 | HTTP | 902 | HTTP/1.1 200 OK |
| 997 | 23:41:18.810844 | 222.205.1.164 | 123.151.176.26 | HTTP | 561 | POST /q.cgi HTTP/1.1 |
| 1007 | 23:41:18.843571 | 123.151.176.26 | 222.205.1.164 | HTTP | 302 | HTTP/1.1 200 OK |
| 1577 | 23:41:30.672717 | 10.203.1.89 | 222.205.1.164 | ICMP | 136 | Echo (ping) request id=0x29b4, seq=0/0, ttl=59 (no response found!) |
| 1594 | 23:41:31.172741 | 10.203.1.89 | 222.205.1.164 | ICMP | 136 | Echo (ping) request id=0x29b4, seq=1/256, ttl=59 (no response found!) |
| 1606 | 23:41:31.673284 | 10.203.1.89 | 222.205.1.164 | ICMP | 136 | Echo (ping) request id=0x29b4, seq=2/512, ttl=59 (no response found!) |

> Frame 1757: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface 0
 > Ethernet II, Src: Hangzhou_00:95:03 (Sc:dd:70:00:95:03), Dst: Dell_f2:fd:99 (f4:8e:38:f2:fd:99)
 > Internet Protocol Version 4, Src: 10.0.2.3, Dst: 10.110.33.41
 > User Datagram Protocol, Src Port: 1701, Dst Port: 1701
 > Layer 2 Tunneling Protocol
 > Point-to-Point Protocol
 > Internet Protocol Version 4, Src: 10.10.0.21, Dst: 222.205.1.164
 > User Datagram Protocol, Src Port: 53, Dst Port: 64110
 > Domain Name System (response)

```
C:\WINDOWS\system32\cmd.exe
物理地址. . . . . : 3A-BA-F8-01-3C-90
DHCP 已启用. . . . . : 是
自动配置已启用. . . . . : 是

以太网适配器 以太网:

连接特定的 DNS 后缀. . . . . :
描述. . . . . : Realtek PCIe GBE Family Controller
物理地址. . . . . : F4-39-09-81-99-C0
DHCP 已启用. . . . . : 否
自动配置已启用. . . . . : 是
IPv6 地址. . . . . : 2001:da8:e000:79:84e3:f81e:c6d7:1408(首选)
IPv6 地址. . . . . : 2001:da8:e000:1a05:84e3:f81e:c6d7:1408(首选)
临时 IPv6 地址. . . . . : 2001:da8:e000:79:68a7:77ac:be71:1ed0(首选)
临时 IPv6 地址. . . . . : 2001:da8:e000:1a05:68a7:77ac:be71:1ed0(首选)
本地链接 IPv6 地址. . . . . : fe80::84e3:f81e:c6d7:1408%12(首选)
IPv4 地址. . . . . : 10.110.33.93(首选)
子网掩码. . . . . : 255.255.255.0
默认网关. . . . . : fe80::5edd:70ff:fe00:9503%12
                  10.110.33.1
DHCPv6 IAID. . . . . : 150223113
DHCPv6 客户端 ID. . . . . : 00-01-00-01-23-33-29-0F-F4-39-09-81-99-C0
DNS 服务器. . . . . : 10.10.0.21
ICMP 上的 NetBIOS. . . . . : 已启用

PPP 适配器 ZJUVPN:
```

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

The DNS query message is shown below. It’s a Type NS DNS query and no answers are contained.

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------------|----------------|----------------|----------|--------|---|
| 1756 | 23:41:35.891489 | 222.205.1.164 | 10.10.0.21 | DNS | 123 | Standard query 0x0001 PTR 21.0.10.10.in-addr.arpa |
| 1757 | 23:41:35.892363 | 10.10.0.21 | 222.205.1.164 | DNS | 180 | Standard query response 0x0001 PTR 21.0.10.10.in-addr.arpa PTR dns1.zju.edu.cn NS dns1.zju.edu.cn A 10.1... |
| 1758 | 23:41:35.894133 | 222.205.1.164 | 10.10.0.21 | DNS | 107 | Standard query 0x0002 NS mit.edu |
| 1759 | 23:41:35.896137 | 10.10.0.21 | 222.205.1.164 | DNS | 380 | Standard query response 0x0002 NS mit.edu NS asia2.akam.net NS use2.akam.net NS use5.akam.net NS ns1-37... |
| 810 | 23:41:17.762669 | 222.205.1.164 | 123.151.176.26 | HTTP | 553 | POST /q.cgi HTTP/1.1 |
| 819 | 23:41:17.798148 | 123.151.176.26 | 222.205.1.164 | HTTP | 902 | HTTP/1.1 200 OK |
| 997 | 23:41:18.810844 | 222.205.1.164 | 123.151.176.26 | HTTP | 561 | POST /q.cgi HTTP/1.1 |
| 1007 | 23:41:18.843571 | 123.151.176.26 | 222.205.1.164 | HTTP | 302 | HTTP/1.1 200 OK |
| 1577 | 23:41:30.672717 | 10.203.1.89 | 222.205.1.164 | ICMP | 136 | Echo (ping) request id=0x29b4, seq=0/0, ttl=59 (no response found!) |
| 1594 | 23:41:31.172741 | 10.203.1.89 | 222.205.1.164 | ICMP | 136 | Echo (ping) request id=0x29b4, seq=1/256, ttl=59 (no response found!) |
| 1606 | 23:41:31.673284 | 10.203.1.89 | 222.205.1.164 | ICMP | 136 | Echo (ping) request id=0x29b4, seq=2/512, ttl=59 (no response found!) |

> Frame 1758: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface 0

> Ethernet II, Src: Dell f2:fd:99 (f4:8e:38:f2:fd:99), Dst: Hangzhou_00:95:03 (5c:dd:70:00:95:03)

> Internet Protocol Version 4, Src: 10.110.33.41, Dst: 10.0.2.3

> User Datagram Protocol, Src Port: 1701, Dst Port: 1701

> Layer 2 Tunneling Protocol

> Point-to-Point Protocol

> Internet Protocol Version 4, Src: 222.205.1.164, Dst: 10.10.0.21

> User Datagram Protocol, Src Port: 64111, Dst Port: 53

> Domain Name System (query)

Transaction ID: 0x0002

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

> mit.edu: type NS, class IN

Name: mit.edu

[Name Length: 7]

[Label Count: 2]

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

[Response In: 1759]

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

The following name servers are provided.

- Asia2.akam.net
- Use2.akam.net

- Use5.akam.net
- Ns1-37.akam.net
- Ns1-173.akam.net
- Usw2.akam.net
- Asia1.akm.net
- Eur5.akm.net

The IP address of the MIT name servers are also provided in the additional records.

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------------|----------------|----------------|----------|--------|--|
| 1756 | 23:41:35.891489 | 222.205.1.164 | 10.10.0.21 | DNS | 123 | Standard query 0x0001 PTR 21.0.10.10.in-addr.arpa |
| 1757 | 23:41:35.892363 | 10.10.0.21 | 222.205.1.164 | DNS | 180 | Standard query response 0x0001 PTR 21.0.10.10.in-addr.arpa PTR dns1.zju.edu.cn NS dns1.zju.edu.cn |
| 1758 | 23:41:35.894133 | 222.205.1.164 | 10.10.0.21 | DNS | 107 | Standard query 0x0002 NS mit.edu |
| 1759 | 23:41:35.896137 | 10.10.0.21 | 222.205.1.164 | DNS | 380 | Standard query response 0x0002 NS mit.edu NS asia2.akam.net NS use2.akam.net NS use5.akam.net NS ns1-37.akam.net NS ns1-173.akam.net NS usw2.akam.net NS asia1.akam.net NS eur5.akam.net |
| 810 | 23:41:17.762669 | 222.205.1.164 | 123.151.176.26 | HTTP | 553 | POST /q.cgi HTTP/1.1 |
| 819 | 23:41:17.798148 | 123.151.176.26 | 222.205.1.164 | HTTP | 902 | HTTP/1.1 200 OK |
| 997 | 23:41:18.810844 | 222.205.1.164 | 123.151.176.26 | HTTP | 561 | POST /q.cgi HTTP/1.1 |
| 1007 | 23:41:18.843571 | 123.151.176.26 | 222.205.1.164 | HTTP | 302 | HTTP/1.1 200 OK |
| 1577 | 23:41:30.672717 | 10.203.1.89 | 222.205.1.164 | ICMP | 136 | Echo (ping) request id=0x29b4, seq=0/0, ttl=59 (no response found!) |
| 1594 | 23:41:31.172741 | 10.203.1.89 | 222.205.1.164 | ICMP | 136 | Echo (ping) request id=0x29b4, seq=1/256, ttl=59 (no response found!) |
| 1606 | 23:41:31.673284 | 10.203.1.89 | 222.205.1.164 | ICMP | 136 | Echo (ping) request id=0x29b4, seq=2/512, ttl=59 (no response found!) |


```

Name: mit.edu
[Name Length: 7]
[Label Count: 2]
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
  Answers
    > mit.edu: type NS, class IN, ns asia2.akam.net
    > mit.edu: type NS, class IN, ns use2.akam.net
    > mit.edu: type NS, class IN, ns use5.akam.net
    > mit.edu: type NS, class IN, ns ns1-37.akam.net
    > mit.edu: type NS, class IN, ns ns1-173.akam.net
    > mit.edu: type NS, class IN, ns usw2.akam.net
    > mit.edu: type NS, class IN, ns asia1.akam.net
    > mit.edu: type NS, class IN, ns eur5.akam.net
  Additional records
    > eur5.akam.net: type A, class IN, addr 23.74.25.64
    > use2.akam.net: type A, class IN, addr 96.7.49.64
    > use5.akam.net: type A, class IN, addr 2.16.40.64
    > asia2.akam.net: type A, class IN, addr 95.101.36.64
    > ns1-37.akam.net: type A, class IN, addr 193.108.91.37
    > use5.akam.net: type AAAA, class IN, addr 2600:1403:a::40
[Request In: 1758]
[Time: 0.002004000 seconds]
  
```

19. Provide a screenshot.

Already shown after every question

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?

The DNS query message is sent to 10.10.0.21.

Use ipconfig /all to find out the IP address of my local DNS server, which is shown in the second picture.

They are absolutely the same.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------------|---------------|---------------|----------|--------|---|
| 91 | 00:01:05.999016 | 222.205.1.164 | 10.10.0.21 | DNS | 123 | Standard query 0x0001 PTR 21.0.10.10.in-addr.arpa |
| 92 | 00:01:05.999859 | 10.10.0.21 | 222.205.1.164 | DNS | 180 | Standard query response 0x0001 PTR 21.0.10.10.in-addr.arpa PTR dns1.zju.edu.cn NS dns1.zju.edu.cn |
| 93 | 00:01:06.003065 | 222.205.1.164 | 10.10.0.21 | DNS | 110 | Standard query 0x0002 A www.sc.edu |
| 95 | 00:01:06.026527 | 10.10.0.21 | 222.205.1.164 | DNS | 347 | Standard query response 0x0002 A www.sc.edu CNAME sc.edu A 65.122.170.137 NS ns0.dnsmadeeasy.com |
| 96 | 00:01:06.028259 | 222.205.1.164 | 10.10.0.21 | DNS | 110 | Standard query 0x0003 AAAA www.sc.edu |
| 97 | 00:01:06.029084 | 10.10.0.21 | 222.205.1.164 | DNS | 181 | Standard query response 0x0003 AAAA www.sc.edu CNAME sc.edu SOA ns0.dnsmadeeasy.com |
| 141 | 00:01:07.524035 | 10.24.31.37 | 222.205.1.164 | TCP | 100 | 52320 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1 |
| 210 | 00:01:09.730031 | 10.0.2.3 | 10.110.33.41 | PPP LCP | 60 | Echo Request |
| 211 | 00:01:09.730287 | 10.110.33.41 | 10.0.2.3 | PPP LCP | 62 | Echo Reply |

```
C:\WINDOWS\system32\cmd.exe
物理地址. . . . . : 3A-BA-F8-01-3C-90
DHCP 已启用. . . . . : 是
自动配置已启用. . . . . : 是

以太网适配器 以太网:

连接特定的 DNS 后缀. . . . . :
描述. . . . . : Realtek PCIe GBE Family Controller
物理地址. . . . . : F4-39-09-81-99-C0
DHCP 已启用. . . . . : 否
自动配置已启用. . . . . : 是
IPv6 地址. . . . . : 2001:da8:e000:79:84e3:f81e:c6d7:1408(首选)
IPv6 地址. . . . . : 2001:da8:e000:1a05:84e3:f81e:c6d7:1408(首选)
临时 IPv6 地址. . . . . : 2001:da8:e000:79:68a7:77ac:be71:1ed0(首选)
临时 IPv6 地址. . . . . : 2001:da8:e000:1a05:68a7:77ac:be71:1ed0(首选)
本地链接 IPv6 地址. . . . . : fe80::84e3:f81e:c6d7:1408%12(首选)
IPv4 地址. . . . . : 10.110.33.93(首选)
子网掩码. . . . . : 255.255.255.0
默认网关. . . . . : fe80::5edd:70ff:fe00:9503%12
                  10.110.33.1
DHCPv6 IAID. . . . . : 150223113
DHCPv6 客户端 DUID. . . . . : 00-01-00-01-23-33-29-0F-F4-39-09-81-99-C0
DNS 服务器. . . . . : 10.10.0.21
ICMP 上的 NetBIOS. . . . . : 已启用

PPP 适配器 ZJUVPN:
```

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

It’s a Type A DNS query and no answers are contained.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------------|------------------------|---------------|----------|--------|--|
| 308 | 23:29:00.629645 | Hangzhou_00:95:03 | Broadcast | ARP | 64 | Who has 10.110.32.118? Tell 10.110.32.1 |
| 309 | 23:29:00.630820 | Hangzhou_00:95:03 | Broadcast | ARP | 64 | Who has 10.110.33.238? Tell 10.110.33.1 |
| 310 | 23:29:00.631483 | Hangzhou_00:95:03 | Broadcast | ARP | 64 | Who has 10.111.6.198? Tell 10.111.6.1 |
| 80 | 23:28:56.805182 | fe80::e409:9f4b:4f6... | ff02::1:2 | DHCPv6 | 144 | Solicit XID: 0x5bbc27 CID: 0001000122e601eaa45e60e |
| 107 | 23:28:57.125234 | fe80::7c34:f697:a0f... | ff02::1:2 | DHCPv6 | 157 | Solicit XID: 0xace487 CID: 0001000122c25a1a34f39a1 |
| 210 | 23:28:58.906812 | 222.205.6.238 | 10.10.0.21 | DNS | 123 | Standard query 0x0001 PTR 21.0.10.10.in-addr.arpa |
| 211 | 23:28:58.907594 | 10.10.0.21 | 222.205.6.238 | DNS | 180 | Standard query response 0x0001 PTR 21.0.10.10.in-addr.arpa |
| 212 | 23:28:58.910283 | 222.205.6.238 | 10.10.0.21 | DNS | 110 | Standard query 0x0002 A www.sc.edu |
| 213 | 23:28:58.912306 | 10.10.0.21 | 222.205.6.238 | DNS | 391 | Standard query response 0x0002 A www.sc.edu CNAME |
| 215 | 23:28:58.915117 | 222.205.6.238 | 10.10.0.21 | DNS | 110 | Standard query 0x0003 AAAA www.sc.edu |
| 216 | 23:28:58.916153 | 10.10.0.21 | 222.205.6.238 | DNS | 181 | Standard query response 0x0003 AAAA www.sc.edu CNAME |

> Frame 212: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0

> Ethernet II, Src: Dell_f2:fd:99 (f4:8e:38:f2:fd:99), Dst: Hangzhou_00:95:03 (5c:dd:70:00:95:03)

> Internet Protocol Version 4, Src: 10.110.33.41, Dst: 10.0.2.3

> User Datagram Protocol, Src Port: 1701, Dst Port: 1701

> Layer 2 Tunneling Protocol

> Point-to-Point Protocol

> Internet Protocol Version 4, Src: 222.205.6.238, Dst: 10.10.0.21

> User Datagram Protocol, Src Port: 61968, Dst Port: 53

> Domain Name System (query)

Transaction ID: 0x0002

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

> Queries

> www.sc.edu: type A, class IN

Name: www.sc.edu

[Name Length: 10]

[Label Count: 3]

Type: A (Host Address) (1)

Class: IN (0x0001)

[Response In: 213]

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

Two answers are provided.

One answer contains Name, Type, Class, Time to Live, Data Length and Address and the other contains Name, Type, Class, Time to Live, Data Length and CNAME

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------------|---------------------------------|---------------|----------|--------|---|
| 308 | 23:29:00.629645 | Hangzhou.00:95:03 | Broadcast | ARP | 64 | who has 10.110.32.118? Tell 10.110.32.1 |
| 309 | 23:29:00.630820 | Hangzhou.00:95:03 | Broadcast | ARP | 64 | who has 10.110.33.238? Tell 10.110.33.1 |
| 310 | 23:29:00.631483 | Hangzhou.00:95:03 | Broadcast | ARP | 64 | who has 10.111.6.198? Tell 10.111.6.1 |
| 80 | 23:28:56.805182 | fe80::e409:9fab:4ff6::ff02:1:12 | ff02::1:2 | DHCPv6 | 144 | Solicit XID: 0x5bbc27 CID: 0001000122e601eaa45e60e30f95 |
| 107 | 23:28:57.125234 | fe80::7c34:f697:a0f::ff02:1:12 | ff02::1:2 | DHCPv6 | 157 | Solicit XID: 0xace487 CID: 0001000122c25a1a34f39a1f581a |
| 210 | 23:28:58.906812 | 222.205.6.238 | 10.10.0.21 | DNS | 123 | Standard query 0x0001 PTR 21.0.10.10.in-addr.arpa |
| 211 | 23:28:58.907594 | 10.10.0.21 | 222.205.6.238 | DNS | 180 | Standard query response 0x0001 PTR 21.0.10.10.in-addr.arpa PTR dns1.zju.edu.cn NS dns1.zju.edu.cn A 10.1... |
| 212 | 23:28:58.910283 | 222.205.6.238 | 10.10.0.21 | DNS | 110 | Standard query 0x0002 A www.sc.edu |
| 213 | 23:28:58.912306 | 10.10.0.21 | 222.205.6.238 | DNS | 391 | Standard query response 0x0002 A www.sc.edu CNAME sc.edu A 65.122.170.137 NS ns2.dnsmadeeasy.com NS ns3... |
| 215 | 23:28:58.915117 | 222.205.6.238 | 10.10.0.21 | DNS | 110 | Standard query 0x0003 AAAA www.sc.edu |
| 216 | 23:28:58.916153 | 10.10.0.21 | 222.205.6.238 | DNS | 181 | Standard query response 0x0003 AAAA www.sc.edu CNAME sc.edu SOA ns0.dnsmadeeasy.com |

Answer RRs: 2
Authority RRs: 5
Additional RRs: 7

> Queries
v Answers
v www.sc.edu: type CNAME, class IN, cname sc.edu
Name: www.sc.edu
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 10609
Data length: 2
CNAME: sc.edu
v sc.edu: Type A, Class IN, addr 65.122.170.137
Name: sc.edu
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 271
Data length: 4
Address: 65.122.170.137
> Authoritative name servers
> Additional records
[Request ID: 212]
[Time: 0.002023000 seconds]

23. Provide a screenshot.

Already shown after every question