

Project - 2 - Introduction to Computer Networks

© 李浩东 3190104890

© 徐浩然 3190104868

2021年4月16日

Project - 2 - Introduction to Computer Networks

nslookup

Run `nslookup` to obtain the IP address of a Web server in Asia

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

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

Is this your expected result?

How to obtain the “authoritative” answer to this query?

ipconfig & Tracing DNS with Wireshark

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

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

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?

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

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

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?

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

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

ZJU

MIT

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

ZJU

MIT

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

ZJU

MIT

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

ZJU

MIT

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

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

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

nslookup

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

- for `www.zju.edu.cn`
 - the Ip address is `10.203.6.122`
- for `www.tsinghua.edu.cn`
 - the IP address is `166.111.4.100`
- the command screenshots are below

```
C:\Users\87236>nslookup www.zju.edu.cn
```

```
服务器:  dns1.zju.edu.cn
```

```
Address:  10.10.0.21
```

```
名称:     www.zju.edu.cn
```

```
Address:  10.203.6.122
```

```
C:\Users\87236>nslookup -type=NS zju.edu.cn
```

```
服务器:  dns1.zju.edu.cn
```

```
Address:  10.10.0.21
```

```
zju.edu.cn      nameserver = dns1.zju.edu.cn
```

```
dns1.zju.edu.cn internet address = 10.10.0.38
```

```
C:\Users\87236>nslookup www.tsinghua.edu.cn
```

```
服务器:  dns1.zju.edu.cn
```

```
Address:  10.10.0.21
```

```
非权威应答:
```

```
名称:     www.tsinghua.edu.cn
```

```
Addresses: 2402:f000:1:404:166:111:4:100
```

```
166.111.4.100
```

```
C:\Users\87236>nslookup -type=NS tsinghua.edu.cn
```

```
服务器:  dns1.zju.edu.cn
```

```
Address:  10.10.0.21
```

```
非权威应答:
```

```
tsinghua.edu.cn nameserver = ns2.cuhk.edu.hk
```

```
tsinghua.edu.cn nameserver = dns.tsinghua.edu.cn
```

```
tsinghua.edu.cn nameserver = dns2.tsinghua.edu.cn
```

```
tsinghua.edu.cn nameserver = dns2.edu.cn
```

```
dns.tsinghua.edu.cn internet address = 166.111.8.30
```

```
dns2.edu.cn internet address = 202.112.0.13
```

```
dns2.tsinghua.edu.cn internet address = 166.111.8.31
```

```
ns2.cuhk.edu.hk AAAA IPV6 address = 2405:3000:3:6::15
```

```
dns2.edu.cn AAAA IPV6 address = 2001:da8:1:100::13
```

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

- for `www.imperial.ac.uk`
- we could find the Non-authoritative answers are

```
imperial.ac.uk  nameserver = ns0.ic.ac.uk
imperial.ac.uk  nameserver = auth0.dns.cam.ac.uk
imperial.ac.uk  nameserver = ns1.ic.ac.uk
imperial.ac.uk  nameserver = ns2.ic.ac.uk
```

- and the Authoritative answers are

```
ns0.ic.ac.uk    internet address = 155.198.142.80
ns1.ic.ac.uk    internet address = 155.198.142.81
ns2.ic.ac.uk    internet address = 155.198.142.82
auth0.dns.cam.ac.uk    internet address = 131.111.8.37
ns0.ic.ac.uk    AAAA IPv6 address = 2a0c:5bc0:4:1::80
ns1.ic.ac.uk    AAAA IPv6 address = 2a0c:5bc0:4:1::81
ns2.ic.ac.uk    AAAA IPv6 address = 2a0c:5bc0:4:1::82
auth0.dns.cam.ac.uk    AAAA IPv6 address = 2001:630:212:8::d:a0
```

- note that there are multiple authoritative servers. and the response we got back was from cached record. in order to confirm the authoritative DNS server, we perform the same DNS query of one of the servers that can provide authoritative answers
 - the server is `ns0.ic.ac.uk`
 - the address of the server is `2a0c:5bc0:4:1::80`
- the command window is below

```
C:\Users\87236>nslookup www.imperial.ac.uk
```

```
服务器:  dns1.zju.edu.cn
```

```
Address:  10.10.0.21
```

```
非权威应答:
```

```
名称:     wrpwww.cc.gslb.ic.ac.uk
```

```
Addresses: 2001:630:12:600:1:2:0:172
```

```
146.179.40.148
```

```
Aliases:  www.imperial.ac.uk
```

```
C:\Users\87236>nslookup -type=NS imperial.ac.uk
```

```
服务器:  dns1.zju.edu.cn
```

```
Address:  10.10.0.21
```

```
非权威应答:
```

```
imperial.ac.uk  nameserver = ns0.ic.ac.uk
```

```
imperial.ac.uk  nameserver = auth0.dns.cam.ac.uk
```

```
imperial.ac.uk  nameserver = ns1.ic.ac.uk
```

```
imperial.ac.uk  nameserver = ns2.ic.ac.uk
```

```
ns0.ic.ac.uk    internet address = 155.198.142.80
```

```
ns1.ic.ac.uk    internet address = 155.198.142.81
```

```
ns2.ic.ac.uk    internet address = 155.198.142.82
```

```
auth0.dns.cam.ac.uk      internet address = 131.111.8.37
ns0.ic.ac.uk            AAAA IPV6 address = 2a0c:5bc0:4:1::80
ns1.ic.ac.uk            AAAA IPV6 address = 2a0c:5bc0:4:1::81
ns2.ic.ac.uk            AAAA IPV6 address = 2a0c:5bc0:4:1::82
auth0.dns.cam.ac.uk      AAAA IPV6 address = 2001:630:212:8::d:a0
```

```
C:\Users\87236>nslookup -type=NS imperial.ac.uk ns0.ic.ac.uk
服务器:  ns0.ic.ac.uk
Address:  2a0c:5bc0:4:1::80
```

```
imperial.ac.uk  nameserver = ns2.ic.ac.uk
imperial.ac.uk  nameserver = ns1.ic.ac.uk
imperial.ac.uk  nameserver = ns0.ic.ac.uk
imperial.ac.uk  nameserver = auth0.dns.cam.ac.uk
ns0.ic.ac.uk    AAAA IPV6 address = 2a0c:5bc0:4:1::80
ns1.ic.ac.uk    AAAA IPV6 address = 2a0c:5bc0:4:1::81
ns2.ic.ac.uk    AAAA IPV6 address = 2a0c:5bc0:4:1::82
auth0.dns.cam.ac.uk    AAAA IPV6 address = 2001:630:212:8::d:a0
ns0.ic.ac.uk    internet address = 155.198.142.80
ns1.ic.ac.uk    internet address = 155.198.142.81
ns2.ic.ac.uk    internet address = 155.198.142.82
auth0.dns.cam.ac.uk    internet address = 131.111.8.37
```

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

Is this your expected result?

we have tried all DNS servers in Question-2 but none of them queried for the mail servers for Yahoo! mail. the command window is below

```
C:\Users\87236>nslookup mail.yahoo.com ns0.ic.ac.uk
服务器:  ns0.ic.ac.uk
Address:  2a0c:5bc0:4:1::80
```

*** ns0.ic.ac.uk 找不到 mail.yahoo.com: Query refused

```
C:\Users\87236>nslookup mail.yahoo.com ns1.ic.ac.uk
服务器:  ns1.ic.ac.uk
Address:  2a0c:5bc0:4:1::81
```

*** ns1.ic.ac.uk 找不到 mail.yahoo.com: Query refused

```
C:\Users\87236>nslookup mail.yahoo.com ns2.ic.ac.uk
服务器:  ns2.ic.ac.uk
Address:  2a0c:5bc0:4:1::82
```

*** ns2.ic.ac.uk 找不到 mail.yahoo.com: Query refused

```
C:\Users\87236>nslookup mail.yahoo.com auth0.dns.cam.ac.uk
服务器:  auth0.dns.cam.ac.uk
Address:  2001:630:212:8::d:a0
```

*** auth0.dns.cam.ac.uk 找不到 mail.yahoo.com: Query refused

so we try `www.google.com`, `www.youtube.com` and `www.cam.ac.uk` instead

```
C:\Users\87236>nslookup www.google.com ns0.ic.ac.uk
服务器: ns0.ic.ac.uk
Address: 2a0c:5bc0:4:1::80
```

```
非权威应答:
名称: www.google.com
Addresses: 2001::6ca0:acd0
           31.13.67.41
```

```
C:\Users\87236>nslookup www.youtube.com ns0.ic.ac.uk
服务器: ns0.ic.ac.uk
Address: 2a0c:5bc0:4:1::80
```

```
非权威应答:
名称: www.youtube.com
Addresses: 2001::c085:4dbf
           179.60.193.9
```

```
C:\Users\87236>nslookup www.cam.ac.uk ns0.ic.ac.uk
服务器: ns0.ic.ac.uk
Address: 2a0c:5bc0:4:1::80
```

```
名称: www.cam.ac.uk
Addresses: 2a05:b400:5:270::80e8:8408
           128.232.132.8
```

but all queries above is Non-authoritative except `www.cam.ac.uk`

How to obtain the “authoritative” answer to this query?

just like we visit `www.cam.ac.uk`, only when the server find the IP address of `www.cam.ac.uk` in its IP list, will we see authoritative response. we take `www.cam.ac.uk` and `www.zju.edu.cn` for example, the command window is below

```
C:\Users\87236>nslookup www.cam.ac.uk
服务器: dns1.zju.edu.cn
Address: 10.10.0.21
```

```
非权威应答:
名称: www.cam.ac.uk
Addresses: 2a05:b400:5:270::80e8:8408
           128.232.132.8
```

```
C:\Users\87236>nslookup www.cam.ac.uk ns0.ic.ac.uk
服务器: ns0.ic.ac.uk
Address: 2a0c:5bc0:4:1::80
```

```
名称: www.cam.ac.uk
Addresses: 2a05:b400:5:270::80e8:8408
           128.232.132.8
```

ipconfig & Tracing DNS with Wireshark

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

- Query

The screenshot shows a Wireshark packet capture on the *WLAN interface. The filter is set to 'ip.addr == 10.186.34.53'. The packet list shows a DNS query (Standard query) from 10.186.34.53 to 10.10.0.21. The packet details pane shows the following information:

- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 58
- Identification: 0xc879 (51321)
- Flags: 0x00
 - 0... = Reserved bit: Not set
 - .0.. = Don't fragment: Not set
 - ..0. = More fragments: Not set
- Fragment Offset: 0
- Time to Live: 64
- Protocol: UDP (17)
- Header Checksum: 0x7b2c [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 10.186.34.53
- Destination Address: 10.10.0.21

- Response

The screenshot shows a Wireshark packet capture on the *WLAN interface. The filter is set to 'ip.addr == 10.186.34.53'. The packet list shows a DNS response (Standard query response) from 10.10.0.21 to 10.186.34.53. The packet details pane shows the following information:

- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 532
- Identification: 0x3f89 (16265)
- Flags: 0x00
 - 0... = Reserved bit: Not set
 - .0.. = Don't fragment: Not set
 - ..0. = More fragments: Not set
- Fragment Offset: 0
- Time to Live: 61
- Protocol: UDP (17)
- Header Checksum: 0x0543 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 10.10.0.21
- Destination Address: 10.186.34.53

- All use UDP

What is the destination port for the DNS query message?

What is the source port of DNS response message?

Wireshark packet capture showing DNS traffic. The packet list shows a query from 10.10.0.21 to 10.186.34.53 on port 53. The packet details show the query for ssl.gstatic.com. The packet bytes show the raw DNS query.

No.	Time	Source	Destination	Protocol	Length	Info
53	0.000000	10.10.0.21	10.186.34.53	DNS	72	Standard query 0xa1b2 A www.ietf.org
54	0.000000	10.186.34.53	10.10.0.21	DNS	546	Standard query response 0xa1b2 A www.ietf.org CNAME www.ietf.org

Frame 505: 546 bytes on wire (4368 bits), 546 bytes captured (4368 bits) on interface \Device\NPF_{1D4EFCF3-098B-4...}

Ethernet II, Src: JuniperN_60:6f:c2 (2c:21:72:60:6f:c2), Dst: Chongqin_c5:8d:3b (c0:b5:d7:c5:8d:3b)

Internet Protocol Version 4, Src: 10.10.0.21, Dst: 10.186.34.53

User Datagram Protocol, Src Port: 53, Dst Port: 57962

Domain Name System (response)

- destination port for the DNS query message:53
- the source port of DNS response message:53

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?

Time	Source	Destination	Protocol	Length	Info
5.938418	10.10.0.21	10.186.34.53	DNS	551	Standard query response 0x24ab A ssl.gstatic.com
0.053856	10.186.34.53	10.10.0.21	DNS	72	Standard query 0xa1b2 A www.ietf.org
0.477995	10.10.0.21	10.186.34.53	DNS	546	Standard query response 0xa1b2 A www.ietf.org

- IP address that the DNS query message sent:10.10.0.21

```

无线局域网适配器 WLAN:

    连接特定的 DNS 后缀 . . . . . : 
    描述. . . . . : Qualcomm QCA9377 802.11ac Wireless Adapter
    物理地址. . . . . : C0-B5-D7-C5-8D-3B
    DHCP 已启用 . . . . . : 是
    自动配置已启用. . . . . : 是
    本地链接 IPv6 地址. . . . . : fe80::5c48:eb3f:8452:a7fd%5(首选)
    IPv4 地址 . . . . . : 10.186.34.53(首选)
    子网掩码 . . . . . : 255.255.128.0
    获得租约的时间 . . . . . : 2021年4月17日 9:56:57
    租约过期的时间 . . . . . : 2021年4月17日 15:50:07
    默认网关. . . . . : 10.186.0.1
    DHCP 服务器 . . . . . : 10.186.0.1
    DHCPv6 IAID . . . . . : 79738327
    DHCPv6 客户端 DUID . . . . . : 00-01-00-01-24-D9-64-96-E4-54-E8-1E-5C-AB
    DNS 服务器 . . . . . : 10.10.0.21
    . . . . . : 10.10.2.21
    TCP/IP 上的 NetBIOS . . . . . : 已启用
  
```

- The IP address of my local DNS server:10.10.0.21
- They are the same.

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

```
> Ethernet II, Src: Chongqin_c5:8d:3b (c0:b5:d7:c5:8d:3b), Dst: JuniperN_60:6f:c2 (2c:21:72:60:6f:c2)
> Internet Protocol Version 4, Src: 10.186.34.53, Dst: 10.10.0.21
> User Datagram Protocol, Src Port: 57962, Dst Port: 53
√ Domain Name System (query)
  Transaction ID: 0xa1b2
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  √ Queries
    > www.ietf.org: type A, class IN
    [Response In: 505]
```

- Type A.
- No answer.

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

```
√ Domain Name System (response)
  Transaction ID: 0xa1b2
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Authority RRs: 13
  Additional RRs: 11
  √ Queries
    > www.ietf.org: type A, class IN
  √ Answers
    > www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
    > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
    > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
```

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?

- 后续发送的TCP SYN数据包的目的IP地址和DNS响应消息中提供的源IP地址相对应。

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

- 没有，只有部分重新发送新的DNS查询。

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

- Query

The image shows a Wireshark packet capture window titled '*Microsoft: WLAN'. The filter bar at the top is set to 'ip.addr == 10.185.78.78'. The packet list on the left shows several TCP and DNS packets. The selected packet is packet 74, a DNS Standard query for 'www.zju.edu.cn'. The packet details pane on the right shows the following structure:

- Frame 352: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF...
- Ethernet II, Src: LiteonTe_4d:3b:81 (3c:91:80:4d:3b:81), Dst: HuaweiTe_26:2f:2e (84:46:fe:26:2f:2e)
- Internet Protocol Version 4, Src: 10.185.78.78, Dst: 10.10.0.21
- User Datagram Protocol, Src Port: 65050, Dst Port: 53
 - Source Port: 65050
 - Destination Port: 53
 - Length: 40
 - Checksum: 0xdc07 [unverified]
 - [Checksum Status: Unverified]
 - [Stream index: 104]
 - [Timestamps]
 - UDP payload (32 bytes)
- Domain Name System (query)

The status bar at the bottom indicates: Destination Port: 53, 2 byte | Packets: 538 · Displayed: 17 (3.2%) · Dropped: 0 (0.0%) | Profile: Default

- Response

*Microsoft: WLAN

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 10.185.78.78

Protocol	Length	Info
TCP	55	58258 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP segment of a reassembled
TCP	66	443 → 58258 [ACK] Seq=1 Ack=2 Win=358 Len=0 SLE=1 SRE=2
TCP	55	[TCP Keep-Alive] 58258 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1
TCP	66	[TCP Keep-Alive ACK] 443 → 58258 [ACK] Seq=1 Ack=2 Win=358 Len=0
DNS	83	Standard query 0x0001 PTR 21.0.10.10.in-addr.arpa
DNS	142	Standard query response 0x0001 PTR 21.0.10.10.in-addr.arpa PTR dn
DNS	74	Standard query 0x0002 A www.zju.edu.cn
DNS	125	Standard query response 0x0002 A www.zju.edu.cn A 10.203.6.122 NS
DNS	74	Standard query 0x0003 AAAA www.zju.edu.cn
DNS	120	Standard query response 0x0003 AAAA www.zju.edu.cn SOA dns1.zju.e
TCP	55	[TCP Keep-Alive] 58258 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1
TCP	66	[TCP Keep-Alive ACK] 443 → 58258 [ACK] Seq=1 Ack=2 Win=358 Len=0
TCP	55	[TCP Keep-Alive] 58258 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1
OICQ	129	OICQ Protocol
TCP	66	[TCP Keep-Alive ACK] 443 → 58258 [ACK] Seq=1 Ack=2 Win=358 Len=0

> Frame 353: 125 bytes on wire (1000 bits), 125 bytes captured (1000 bits) on interface \Device
 > Ethernet II, Src: HuaweiTe_26:2f:2e (84:46:fe:26:2f:2e), Dst: LiteonTe_4d:3b:81 (3c:91:80:4d:
 > Internet Protocol Version 4, Src: 10.10.0.21, Dst: 10.185.78.78
 ✓ User Datagram Protocol, Src Port: 53, Dst Port: 65050
 Source Port: 53
 Destination Port: 65050
 Length: 91
 Checksum: 0x97f5 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 104]
 > [Timestamps]
 UDP payload (83 bytes)
 > Domain Name System (response)

Source Port (udp...cport), 2 byte | Packets: 538 · Displayed: 17 (3.2%) · Dropped: 0 (0.0%) | Profile: Default

- All is 53

MIT

- Query

*WLAN

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(T) 帮助(H)

ip.addr == 10.186.34.53

Source	Destination	Protocol	Length	Info
0.204.17.18	10.186.34.53	OICQ	129	OICQ Protocol
0.204.17.18	10.186.34.53	OICQ	129	OICQ Protocol
0.204.17.18	10.186.34.53	OICQ	129	OICQ Protocol
10.0.21	10.186.34.53	DNS	144	Standard query response 0x0003 AAAA www.mit.edu CNAME www
186.34.53	10.10.0.21	DNS	71	Standard query 0x0003 AAAA www.mit.edu
10.0.21	10.186.34.53	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mi
186.34.53	10.10.0.21	DNS	71	Standard query 0x0002 A www.mit.edu
10.0.21	10.186.34.53	DNS	170	Standard query response 0x0001 PTR 21.0.10.10.in-addr.arpa
186.34.53	10.10.0.21	DNS	83	Standard query 0x0001 PTR 21.0.10.10.in-addr.arpa
10.0.21	10.186.34.53	DNS	542	Standard query response 0x4ba5 A az700632.vo.msecnd.net

> Frame 270: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{1D4EFCF3-098B-4C...}

> Ethernet II, Src: Chongqin_c5:8d:3b (c0:b5:d7:c5:8d:3b), Dst: JuniperN_60:6f:c2 (2c:21:72:60:6f:c2)

> Internet Protocol Version 4, Src: 10.186.34.53, Dst: 10.10.0.21

▼ User Datagram Protocol, Src Port: 56635, Dst Port: 53

Source Port: 56635

Destination Port: 53

Length: 37

Checksum: 0x9878 [unverified]

[Checksum Status: Unverified]

[Stream index: 5]

> [Timestamps]

UDP payload (29 bytes)

▼ Domain Name System (query)

Transaction ID: 0x0002

Number of additional records in ...et (dns.count.add_rr), 2 byte(s) | 分组: 326 · 已显示: 326 (100.0%) · 已丢弃: 0 (0.0%) | 配置: Default

• Response

*WLAN

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(T) 帮助(H)

ip.addr == 10.186.34.53

Source	Destination	Protocol	Length	Info
0.204.17.18	10.186.34.53	OICQ	129	OICQ Protocol
0.204.17.18	10.186.34.53	OICQ	129	OICQ Protocol
0.204.17.18	10.186.34.53	OICQ	129	OICQ Protocol
10.0.21	10.186.34.53	DNS	144	Standard query response 0x0003 AAAA www.mit.edu CNAME www
186.34.53	10.10.0.21	DNS	71	Standard query 0x0003 AAAA www.mit.edu
10.0.21	10.186.34.53	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mi
186.34.53	10.10.0.21	DNS	71	Standard query 0x0002 A www.mit.edu
10.0.21	10.186.34.53	DNS	170	Standard query response 0x0001 PTR 21.0.10.10.in-addr.arpa
186.34.53	10.10.0.21	DNS	83	Standard query 0x0001 PTR 21.0.10.10.in-addr.arpa
10.0.21	10.186.34.53	DNS	542	Standard query response 0x4ba5 A az700632.vo.msecnd.net

> Frame 271: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface \Device\NPF_{1D4EFCF3-098B-4C...}

> Ethernet II, Src: JuniperN_60:6f:c2 (2c:21:72:60:6f:c2), Dst: Chongqin_c5:8d:3b (c0:b5:d7:c5:8d:3b)

> Internet Protocol Version 4, Src: 10.10.0.21, Dst: 10.186.34.53

▼ User Datagram Protocol, Src Port: 53, Dst Port: 56635

Source Port: 53

Destination Port: 56635

Length: 126

Checksum: 0x4cf4 [unverified]

[Checksum Status: Unverified]

[Stream index: 5]

> [Timestamps]

UDP payload (118 bytes)

▼ Domain Name System (response)

Transaction ID: 0x0002

Number of additional records in ...et (dns.count.add_rr), 2 byte(s) | 分组: 326 · 已显示: 326 (100.0%) · 已丢弃: 0 (0.0%) | 配置: Default

• All is 53

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

ZJU

-04-18 14:40:10.578390	10.185.78.78	10.10.0.21	DNS	74 Standard query 0x0002 A www.zju.edu.cn
-04-18 14:40:10.584107	10.10.0.21	10.185.78.78	DNS	125 Standard query response 0x0002 A www.zju.edu.cn

- 目标IP地址: 10.10.0.21
- 与本地DNS服务器一致

MIT

271 25.092430	10.10.0.21	10.186.34.53	DNS	160 Standard query response 0x0002 A www.m
270 25.086408	10.186.34.53	10.10.0.21	DNS	71 Standard query 0x0002 A www.mit.edu

- 目标IP地址: 10.10.0.21
- 与本地DNS服务器一致

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

ZJU

The image shows a Wireshark packet capture of a DNS query. The packet list on the left shows a packet of 74 bytes on wire (592 bits) captured on interface \Device\NPF. The packet details pane shows the following structure:

- Frame 352: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF
- Ethernet II, Src: LiteonTe_4d:3b:81 (3c:91:80:4d:3b:81), Dst: HuaweiTe_26:2f:2e (84:46:fe:26:2f:2e)
- Internet Protocol Version 4, Src: 10.185.78.78, Dst: 10.10.0.21
- User Datagram Protocol, Src Port: 65050, 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.zju.edu.cn: type A, class IN
 - Name: www.zju.edu.cn
 - [Name Length: 14]
 - [Label Count: 4]
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)

The packet bytes pane at the bottom shows a text item (text), 20 bytes.

- Type A
- No answer

MIT

The image shows a Wireshark packet capture of a DNS query. The packet list on the left shows a packet of 71 bytes on wire (568 bits) captured on interface \Device\NPF. The packet details pane shows the following structure:

- Ethernet II, Src: Chongqin_c5:8d:3b (c0:b5:d7:c5:8d:3b), Dst: JuniperN_60:6f:c2 (2c:21:72:60:6f:c2)
- Internet Protocol Version 4, Src: 10.186.34.53, Dst: 10.10.0.21
- User Datagram Protocol, Src Port: 56635, 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: 14]
 - [Label Count: 4]
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)

The packet bytes pane at the bottom shows a text item (text), 20 bytes.

- Type A
- No answer

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

ZJU

```

    Queries
    - www.zju.edu.cn: type A, class IN
      Name: www.zju.edu.cn
      [Name Length: 14]
      [Label Count: 4]
      Type: A (Host Address) (1)
      Class: IN (0x0001)

    Answers
    - www.zju.edu.cn: type A, class IN, addr 10.203.6.122
      Name: www.zju.edu.cn
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 86400 (1 day)
      Data length: 4
      Address: 10.203.6.122

    > Authoritative nameservers
    > Additional records
    [Request In: 352]
    [Time: 0.005717000 seconds]
  
```

Text item (text), 16 bytes | Packets: 538 · Displayed: 17 (3.2%) · Dropped: 0 (0.0%) | Profile: Default

MIT

```

    > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0

    Queries
    - www.mit.edu: type A, class IN

    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 23.2.132.117
  
```

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

Source	Destination	Protocol	Length	Info
10.186.34.53	10.10.0.21	DNS	83	Standard query 0x0001 PTR 21.0.10.10.in-addr.arpa
10.10.0.21	10.186.34.53	DNS	142	Standard query response 0x0001 PTR 21.0.10.10.in-addr.
10.186.34.53	10.10.0.21	DNS	67	Standard query 0x0002 NS mit.edu
10.10.0.21	10.186.34.53	DNS	234	Standard query response 0x0002 NS mit.edu NS asia2.aka

- 目标IP地址: 10.10.0.21
- 是本地DNS服务器地址

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

```
✓ 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
    \[Response In: 19\]
```

- Type NS
- No answer

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

```
✓ Queries
  > mit.edu: type NS, class IN
  ✓ 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 usw2.akam.net
    > mit.edu: type NS, class IN, ns ns1-173.akam.net
    > mit.edu: type NS, class IN, ns eur5.akam.net
    > mit.edu: type NS, class IN, ns asia1.akam.net
    > mit.edu: type NS, class IN, ns use5.akam.net
    > mit.edu: type NS, class IN, ns ns1-37.akam.net
    \[Request In: 18\]
    [Time: 0.046111000 seconds]
```