

lab3 Wireshark_DNS

- 学号：1813075
 - 姓名：刘茵
-

1.nslookup

问题：

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

答：

```
服务器： baidu.com
Addresses:  39.156.69.79
           220.181.38.148

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

服务器的IP地址为 39.156.69.79和 220.181.38.148

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

[注]：2.3电脑链接失败，且网上没有找到对应的解决办法。

2.ipconfig

No questions

3.Tracing DNS with Wireshark

问题：

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

dns

No.	Time	Source	Destination	Protocol	Length	In
45	2020-11-14 16:50:03.508568	10.134.253.81	222.30.45.41	DNS	72	St
46	2020-11-14 16:50:03.509410	10.134.253.81	222.30.45.41	DNS	72	St
47	2020-11-14 16:50:03.524491	222.30.45.41	10.134.253.81	DNS	173	St
48	2020-11-14 16:50:03.543985	10.134.253.81	202.113.16.41	DNS	72	St

Frame 45: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{2358D703-B4C5-4DF2-A2AE-DCAA3D49EDA3}

- Interface id: 0 (\Device\NPF_{2358D703-B4C5-4DF2-A2AE-DCAA3D49EDA3})
- Encapsulation type: Ethernet (1)
- Arrival Time: Nov 14, 2020 16:50:03.508568000 中国标准时间
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1605343803.508568000 seconds
- [Time delta from previous captured frame: 0.658951000 seconds]
- [Time delta from previous displayed frame: 0.000000000 seconds]
- [Time since reference or first frame: 4.929084000 seconds]
- Frame Number: 45
- Frame Length: 72 bytes (576 bits)
- Capture Length: 72 bytes (576 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: eth:ethertype:ip:udp:dns]
- [Coloring Rule Name: UDP]
- [Coloring Rule String: udp]

答：是UDP

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

No.	Time	Source	Destination	Protocol
45	2020-11-14 16:50:03.508568	10.134.253.81	222.30.45.41	DNS
46	2020-11-14 16:50:03.509410	10.134.253.81	222.30.45.41	DNS
47	2020-11-14 16:50:03.524491	222.30.45.41	10.134.253.81	DNS
48	2020-11-14 16:50:03.543985	10.134.253.81	202.113.16.41	DNS

Frame 46: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{2358D703-B4C5-4DF2-A2AE-DCAA3D49EDA3}

- Ethernet II, Src: IntelCor_0a:57:17 (38:de:ad:0a:57:17), Dst: IETF-VRRP-VRID_0e (00:00:5e:00:01:0e)
- Internet Protocol Version 4, Src: 10.134.253.81, Dst: 222.30.45.41
- User Datagram Protocol, Src Port: 64008, Dst Port: 53
- Domain Name System (query)

No.	Time	Source	Destination	Protocol
45	2020-11-14 16:50:03.508568	10.134.253.81	222.30.45.41	DNS
46	2020-11-14 16:50:03.509410	10.134.253.81	222.30.45.41	DNS
47	2020-11-14 16:50:03.524491	222.30.45.41	10.134.253.81	DNS
48	2020-11-14 16:50:03.543985	10.134.253.81	202.113.16.41	DNS

Frame 47: 173 bytes on wire (1384 bits), 173 bytes captured (1384 bits) on interface \Device\NPF_{2358D703-B4C5-4DF2-A2AE-DCAA3D49EDA3}

- Ethernet II, Src: IETF-VRRP-VRID_0e (00:00:5e:00:01:0e), Dst: IntelCor_0a:57:17 (38:de:ad:0a:57:17)
- Internet Protocol Version 4, Src: 222.30.45.41, Dst: 10.134.253.81
- User Datagram Protocol, Src Port: 53, Dst Port: 64008
- Domain Name System (response)

No.	Time	Source	Destination	Protocol
45	2020-11-14 16:50:03.508568	10.134.253.81	222.30.45.41	DNS
46	2020-11-14 16:50:03.509410	10.134.253.81	222.30.45.41	DNS
47	2020-11-14 16:50:03.524491	222.30.45.41	10.134.253.81	DNS
48	2020-11-14 16:50:03.543985	10.134.253.81	202.113.16.41	DNS

Frame 46: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{2358D703-B4C5-4DF2-A2AE-DCAA3D49EDA3}

- Ethernet II, Src: IntelCor_0a:57:17 (38:de:ad:0a:57:17), Dst: IETF-VRRP-VRID_0e (00:00:5e:00:01:0e)
- Internet Protocol Version 4, Src: 10.134.253.81, Dst: 222.30.45.41
- User Datagram Protocol, Src Port: 64008, Dst Port: 53
- Domain Name System (query)

45	2020-11-14 16:50:03.508568	10.134.253.81	222.30.45.41	DNS
46	2020-11-14 16:50:03.509410	10.134.253.81	222.30.45.41	DNS
47	2020-11-14 16:50:03.524491	222.30.45.41	10.134.253.81	DNS
48	2020-11-14 16:50:03.543985	10.134.253.81	202.113.16.41	DNS
49	2020-11-14 16:50:03.551115	10.134.253.81	222.30.45.41	DNS


```

> Frame 47: 173 bytes on wire (1384 bits), 173 bytes captured (1384 bits) on interface \Dev:
> Ethernet II, Src: IETF-VRRP-VRID_0e (00:00:5e:00:01:0e), Dst: IntelCor_0a:57:17 (38:de:ad:
> Internet Protocol Version 4, Src: 222.30.45.41, Dst: 10.134.253.81
> User Datagram Protocol, Src Port: 53, Dst Port: 64008
> Domain Name System (response)

```

答：端口号都是53

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

```

无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . : 
   描述. . . . . : Intel(R) Dual Band Wireless-AC 8265
   物理地址. . . . . : 38-DE-AD-0A-57-17
   DHCP 已启用 . . . . . : 是
   自动配置已启用. . . . . : 是
   IPv6 地址. . . . . : 2001:250:401:6544:d4ac:b2fa:7dcf:c405(首选)
   临时 IPv6 地址. . . . . : 2001:250:401:6544:d8d2:9637:1f9c:6d54(首选)
   本地链接 IPv6 地址. . . . . : fe80::d4ac:b2fa:7dcf:c405%5(首选)
   IPv4 地址. . . . . : 10.134.253.81(首选)
   子网掩码 . . . . . : 255.255.192.0
   获得租约的时间 . . . . . : 2020年11月14日 13:35:42
   租约过期的时间 . . . . . : 2020年11月14日 22:35:43
   默认网关. . . . . : fe80::865b:12ff:fe5e:360f%5
                       10.134.192.1
   DHCP 服务器 . . . . . : 10.134.192.1
   DHCPv6 IAID . . . . . : 37281453
   DHCPv6 客户端 DUID . . . . . : 00-01-00-01-22-F7-38-02-38-DE-AD-0A-57-17
   DNS 服务器 . . . . . : 222.30.45.41
                       202.113.16.41
   TCP/IP 上的 NetBIOS . . . . . : 已启用

```

答：Destination IP与本地DNS IP相同，都是222.30.45.41

7. 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: 0xa907
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  < Queries
    < 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: 91]

```

答：type is A , no answers.

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

```

Domain Name System (response)
  Transaction ID: 0xa907
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Authority RRs: 0
  Additional RRs: 0
  > Queries
  > 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 104.16.44.99
    > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99

```

答：包含了三个answers。

第一个type为CNAME，指明了www.ietf.org的另一个域名
www.ietf.org.cdn.cloudflare.net，是由国外 CDN 厂商 Cloudflare 提供的规范 CNAME 的 CDN 加速 (type=cname) 地址

第二个和第三个type为A，class为in，ipv4是104.16.44.99/104.16.45.99

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?

答：是对应的

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

答：并没有，因为本机 DNS 已经被缓存了，因此不需要发起新的 DNS 查询。

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

232.53	202.113.16.41	DNS	71 Standard query 0x0002 A www.mit.edu
13.16.41	10.22.232.53	DNS	160 Standard query response 0x0002 A www.mit.edu
232.53	202.113.16.41	DNS	71 Standard query 0x0003 AAAA www.mit.edu
2.16.41	10.22.232.53	DNS	160 Standard query response 0x0003 AAAA www.mit.edu

```

> Frame 868: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{235...}
> Ethernet II, Src: IntelCor_0a:57:17 (38:de:ad:0a:57:17), Dst: HuaweiTe_ea:ac:03 (30:d1:7e:ea:ac:03)
> Internet Protocol Version 4, Src: 10.22.232.53, Dst: 202.113.16.41
> User Datagram Protocol, Src Port: 55371, Dst Port: 53
> Domain Name System (query)

```

13.16.41	10.22.232.53	DNS	160 Standard query response 0x0002 A www.mit.edu
232.53	202.113.16.41	DNS	71 Standard query 0x0003 AAAA www.mit.edu
2.16.41	10.22.232.53	DNS	160 Standard query response 0x0003 AAAA www.mit.edu

```

> Frame 910: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface \Device\NPF_{235...}
> Ethernet II, Src: HuaweiTe_ea:ac:03 (30:d1:7e:ea:ac:03), Dst: IntelCor_0a:57:17 (38:de:ad:0a:57:17)
> Internet Protocol Version 4, Src: 202.113.16.41, Dst: 10.22.232.53
> User Datagram Protocol, Src Port: 53, Dst Port: 55371
> Domain Name System (response)

```

答：端口号都为53。

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

答：202.113.16.41，是本地默认DNS服务器的IP。

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

答：Type:A no "answers".

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

```

Domain Name System (response)
Transaction ID: 0x0002
> Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 0
> Queries
✓ Answers
  > www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
  > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
  > e9566.dscb.akamaiedge.net: type A, class IN, addr 23.57.254.82
[Request In: 868]

```

答：提供了三个answer，包括两个规范主机地址（type=cname），一个规范主机地址指向 IPV4(type=a)

15. Provide a screenshot

```

.53      202.113.16.41      DNS      71 Standard query 0x0002 A www.mit.edu
5.41     10.22.232.53      DNS      160 Standard query response 0x0002 A www.mit.edu CNAME
.53      202.113.16.41      DNS      71 Standard query 0x0003 AAAA www.mit.edu
5.41     10.22.232.53      DNS      200 Standard query response 0x0003 AAAA www.mit.edu
401:e02b:1a5... 2600:1408:5c00:29d::2... DNS      88 Standard query 0x0004 A nslookup
401:e02b:1a5... 2600:1408:5c00:29d::2... DNS      88 Standard query 0x0005 AAAA nslookup
.53      202.113.16.41      DNS      82 Standard query 0x29ca AAAA internal-api.feishu.c
5.41     10.22.232.53      DNS      181 Standard query response 0x29ca AAAA internal-api

<----->
> Internet Protocol Version 4, Src: 202.113.16.41, Dst: 10.22.232.53
> User Datagram Protocol, Src Port: 53, Dst Port: 55371
✓ Domain Name System (response)
  Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Authority RRs: 0
  Additional RRs: 0
  > Queries
  ✓ Answers
    > www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
    > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
    > e9566.dscb.akamaiedge.net: type A, class IN, addr 23.57.254.82

```

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

答：<使用给定数据包不确定>，但按照报文格式应该是作者的本地默认DNS服务器的IP地址

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

答：Type NS 表示查询**权威 DNS 服务器** 查询消息不包含任何“answers”

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

答：响应消息没提供 MIT 的域名的 IP 地址。

```

Domain Name System (response)
Transaction ID: 0x0003
> Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 3
> Queries
✓ Answers
  > mit.edu: type NS, class IN, ns bitsy.mit.edu
  > mit.edu: type NS, class IN, ns strawb.mit.edu
  > mit.edu: type NS, class IN, ns w20ns.mit.edu
  > Additional records

```

19. Provide a screenshot.

	Source	Destination	Protocol	Length	Info
5.848640	128.238.38.160	128.238.29.22	DNS	86	Standard query 0x0001 PTR 22.29.23
5.849007	128.238.29.22	128.238.38.160	DNS	118	Standard query response 0x0001 PTR
5.849848	128.238.38.160	128.238.29.22	DNS	76	Standard query 0x0002 NS mit.edu.p
5.850192	128.238.29.22	128.238.38.160	DNS	135	Standard query response 0x0002 No
5.850423	128.238.38.160	128.238.29.22	DNS	67	Standard query 0x0003 NS mit.edu
5.850784	128.238.29.22	128.238.38.160	DNS	176	Standard query response 0x0003 NS

<

> Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54), Dst: IBM_10:60:99 (00:09:6b:10:60:99)

> Internet Protocol Version 4, Src: 128.238.29.22, Dst: 128.238.38.160

> User Datagram Protocol, Src Port: 53, Dst Port: 3746

Domain Name System (response)

Transaction ID: 0x0003

> Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 3

Authority RRs: 0

Additional RRs: 3

> Queries

Answers

> mit.edu: type NS, class IN, ns bitsy.mit.edu

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?

> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 18.72.0.3

答：不是

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

答：Type 为“A”，表示查询 IP 地址，没有任何 “answers”。

Domain Name System (query)
Transaction ID: 0x0004
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0

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

Answers
> www.aiit.or.kr: type A, class IN, addr 218.36.94.200

答：提供了一个“answers”，为该域名的ip地址。

23. Provide a screens

1	128.238.38.160	18.72.0.3	DNS	82	Standard query 0x0001 PTR 3.0.72.1
1	18.72.0.3	128.238.38.160	DNS	212	Standard query response 0x0001 PTR
5	128.238.38.160	18.72.0.3	DNS	83	Standard query 0x0002 A www.aiit.c
8	18.72.0.3	128.238.38.160	DNS	135	Standard query response 0x0002 No
2	128.238.38.160	18.72.0.3	DNS	74	Standard query 0x0003 A www.aiit.c
4	18.72.0.3	128.238.38.160	DNS	156	Standard query response 0x0003 A w

Frame 104: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-MSRP-routers_00 (00:00:0c:07:ac:00)
Internet Protocol Version 4, Src: 128.238.38.160, Dst: 18.72.0.3
User Datagram Protocol, Src Port: 3753, Dst Port: 53
Domain Name System (query)

