

四川大學

《计算机网络》实验报告（7）



Wireshark Lab: DNS

专 业 软件工程

姓 名 郭 政

学 号 2023141461076

指导老师 程艳红

成绩分数

二零二五年五月二十七日

Wireshark Lab: DNS

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

nslookup www.baidu.com

IP 地址是：110.242.69.21; 110.242.70.57

```
C:\Users\13929>nslookup www.baidu.com
服务器:  UnKnown
Address:  192.168.43.1

非权威应答:
名称:     www.a.shifen.com
Addresses: 110.242.69.21
          110.242.70.57
Aliases:  www.baidu.com
```

2. Run nslookup to determine the authoritative DNS servers for a university in Europe. What is its IP address.

nslookup -type=NS ox.ac.uk

IP 地址是：192.168.43.1

```
C:\Users\13929>nslookup -type=NS ox.ac.uk
服务器:  UnKnown
Address:  192.168.43.1

非权威应答:
ox.ac.uk      nameserver = dns2.ox.ac.uk
ox.ac.uk      nameserver = auth6.dns.ox.ac.uk
ox.ac.uk      nameserver = auth5.dns.ox.ac.uk
ox.ac.uk      nameserver = auth4.dns.ox.ac.uk
ox.ac.uk      nameserver = dns0.ox.ac.uk
ox.ac.uk      nameserver = dns1.ox.ac.uk
```

3. 用 DNS 服务器查询 Yahoo! Mail 的邮件服务器

```
C:\Users\13929>nslookup -type=MX yahoo.com 8.8.8.8
服务器:  dns.google
Address:  8.8.8.8

非权威应答:
yahoo.com     MX preference = 1, mail exchanger = mta6.am0.yahoodns.net
yahoo.com     MX preference = 1, mail exchanger = mta7.am0.yahoodns.net
yahoo.com     MX preference = 1, mail exchanger = mta5.am0.yahoodns.net
```

4. DNS 查询/响应是用 UDP 还是 TCP?

用的是 UDP 协议

5. DNS 查询消息的目的端口和响应消息的源端口?

DNS 查询消息的目的端口：53

DNS 响应消息的源端口：也是 53

No.	Time	Source	Destination	Protocol	Length	Info
92	2.425624	10.176.153.54	211.67.48.8	DNS	72	Standard query 0x6749 A www.ietf.org
132	3.436414	10.176.153.54	211.67.48.8	DNS	72	Standard query 0x6749 A www.ietf.org
133	3.446498	211.67.48.8	10.176.153.54	DNS	120	Standard query response 0x6749 A www.ietf.o...
134	3.449464	10.176.153.54	172.67.33.249	TCP	66	9475→80 [SYN] Seq=0 Win=64240 Len=0 MSS=146...
135	3.450001	10.176.153.54	172.67.33.249	TCP	66	9476→80 [SYN] Seq=0 Win=64240 Len=0 MSS=146...
137	3.484470	10.176.153.54	172.67.33.249	TCP	66	9477→80 [SYN] Seq=0 Win=64240 Len=0 MSS=146...

> Frame 92: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
> Ethernet II, Src: HonHaiPr_96:2a:8d (48:e2:44:96:2a:8d), Dst: FujianSt_6b:28:f1 (14:14:4b:6b:28:f1)
> Internet Protocol Version 4, Src: 10.176.153.54, Dst: 211.67.48.8
> User Datagram Protocol, Src Port: 60703, Dst Port: 53
> Domain Name System (query)

```
C:\Users\13929>ipconfig -all
```

Windows IP 配置

```
主机名 . . . . . : LAPTOP-196TL048
主 DNS 后缀 . . . . . :
节点类型 . . . . . : 混合
IP 路由已启用 . . . . . : 否
WINS 代理已启用 . . . . . : 否
```

以太网适配器 以太网：

```
媒体状态 . . . . . : 媒体已断开连接
连接特定的 DNS 后缀 . . . . . :
描述 . . . . . : Realtek PCIe GbE Family Controller
物理地址 . . . . . : BC-EC-A0-07-3F-21
DHCP 已启用 . . . . . : 是
自动配置已启用 . . . . . : 是
```

```
C:\Users\13929>ipconfig /displaydns
```

Windows IP 配置

osfsr.lenovomm.com

```
记录名称 . . . . . : osfsr.lenovomm.com
记录类型 . . . . . : 5
生存时间 . . . . . : 7614
数据长度 . . . . . : 8
部分 . . . . . : 答案
CNAME 记录 . . . . . : fsr.cn.lenovomm.com
```

osfsr.lenovomm.com

没有 AAAA 类型的记录

```
记录名称 . . . . . : osfsr.lenovomm.com
记录类型 . . . . . : 5
生存时间 . . . . . : 8185
数据长度 . . . . . : 8
部分 . . . . . : 答案
CNAME 记录 . . . . . : fsr.cn.lenovomm.com
```

6. DNS 查询消息发往的 IP 是否与本地 DNS 相同？

DNS 查询消息发送到的 IP 地址是 211.67.48.8。

使用 ipconfig 得到的本地 DNS 服务器地址也是 211.67.48.8，两者一致

7. 查询消息的类型是什么？是否包含 answers？

消息类型为 A；没有包含任何 answer

132	3.436414	10.176.153.54	211.67.48.8	DNS	72 Standard query 0x6749 A www.ietf.org
133	3.446498	211.67.48.8	10.176.153.54	DNS	120 Standard query response 0x6749 A www.ietf.o...
134	3.449464	10.176.153.54	172.67.33.249	TCP	66 9475→80 [SYN] Seq=0 Win=64240 Len=0 MSS=146...
135	3.450001	10.176.153.54	172.67.33.249	TCP	66 9476→80 [SYN] Seq=0 Win=64240 Len=0 MSS=146...
137	3.484470	10.176.153.54	172.67.33.249	TCP	66 9477→80 [SYN] Seq=0 Win=64240 Len=0 MSS=146...

Transaction ID: 0x6749	
> Flags: 0x0100 Standard query	
Questions: 1	
Answer RRs: 0	
Authority RRs: 0	
Additional RRs: 0	
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)	

8. 响应消息中有多少 answers? 都包含了什么内容?

No.	Time	Source	Destination	Protocol	Length	Info
92	2.425624	10.176.153.54	211.67.48.8	DNS	72	Standard query 0x6749 A www.ietf.org
132	3.436414	10.176.153.54	211.67.48.8	DNS	72	Standard query 0x6749 A www.ietf.org
133	3.446498	211.67.48.8	10.176.153.54	DNS	120	Standard query response 0x6749 A www.ietf.o...
134	3.449464	10.176.153.54	172.67.33.249	TCP	66	9475→80 [SYN] Seq=0 Win=64240 Len=0 MSS=146...
135	3.450001	10.176.153.54	172.67.33.249	TCP	66	9476→80 [SYN] Seq=0 Win=64240 Len=0 MSS=146...
137	3.484470	10.176.153.54	172.67.33.249	TCP	66	9477→80 [SYN] Seq=0 Win=64240 Len=0 MSS=146...

[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)

Answers

- www.ietf.org: type A, class IN, addr 172.67.33.249
Name: www.ietf.org
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 54
Data length: 4
Address: 172.67.33.249
- www.ietf.org: type A, class IN, addr 104.20.110.6
- www.ietf.org: type A, class IN, addr 104.20.111.6

0000 00 03 00 00 00 00 03 77 77 77 04 69 65 74 66 03w ww.ietf.
0040 6f 72 67 00 00 01 00 01 c0 0c 00 01 00 01 00 00 org.....
0050 00 36 00 04 ac 43 21 f9 c0 0c 00 01 00 01 00 00 .6...Cl.
0060 00 36 00 04 68 14 6e 06 c0 0c 00 01 00 01 00 00 .6...h.n.

有 3 个答案包含以下信息:

主机名称、地址类型、类、TTL、数据长度和 IP 地址等信息

9. TCP SYN 包的目的 IP 是否在 DNS 响应中?

TCP SYN 包的目的 IP 不在 DNS 响应中

10. 网页中包含图片时, 是否为每张图片重新发起 DNS 查询?

若图片域名已缓存, 则不触发新的查询, 若不在缓存中则发起查询

11. DNS 查询的目的端口和响应的源端口?

文件(E) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(I) 帮助(H)						
ip.addr == 10.176.153.54						
No.	Time	Source	Destination	Protocol	Length	Info
102	1.107831	13.107.4.52	10.176.153.54	TCP	60	80→10537 [ACK] Seq=516 Ack=113 Win=525056 L...
116	1.238793	10.176.153.54	211.67.48.8	DNS	84	Standard query 0x0001 PTR 8.48.67.211.in-ad...
117	1.243189	211.67.48.8	10.176.153.54	DNS	177	Standard query response 0x0001 PTR 8.48.67.2...
118	1.246213	10.176.153.54	211.67.48.8	DNS	71	Standard query 0x0002 A www.mit.edu
119	1.250499	211.67.48.8	10.176.153.54	DNS	87	Standard query response 0x0002 A www.mit.ed...
120	1.253662	10.176.153.54	211.67.48.8	DNS	71	Standard query 0x0003 AAAA www.mit.edu
126	1.400553	211.67.48.8	10.176.153.54	DNS	524	Standard query response 0x0003 AAAA www.mit...

> Frame 126: 524 bytes on wire (4192 bits), 524 bytes captured (4192 bits) on interface 0
> Ethernet II, Src: FujianSt_6b:28:f1 (14:14:4b:6b:28:f1), Dst: HonHaiPr_96:2a:8d (48:e2:44:96:2a:8d)
> Internet Protocol Version 4, Src: 211.67.48.8, Dst: 10.176.153.54
> User Datagram Protocol, Src Port: 53, Dst Port: 63084
> Domain Name System (response)
[Request In: 120]
[Time: 0.146891000 seconds]
Transaction ID: 0x0003
> Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 4
Authority RRs: 8
Additional RRs: 9

0000 00 04 00 00 00 09 03 77 77 77 03 6d 69 74 03 65w ww.mit.e
0040 64 75 00 00 1c 00 01 c0 0c 00 05 00 01 00 00 04 du.....
0050 0b 00 19 03 77 77 77 03 6d 69 74 03 65 64 75 07www. mit.edu.
0060 65 64 67 65 6b 65 79 03 6e 65 74 00 c0 29 00 05 edgekey. net...)

DNS 查询的目标端口是 53, DNS 响应的源端口也是 53

12. 查询发送到哪个 IP? 是否是默认本地 DNS?

它被发送到 211.67.48.8, 这是默认的本地 DNS 服务器

13. 查询类型? 是否有 answers?

查询类型是 AAAA 类型, 该查询消息不包含 answer

14. 响应中有多少 answers? 都包含什么?

3 个 answer, 该答案包括: 主机名、地址类型、地址类别, 以及 IP 地址

No.	Time	Source	Destination	Protocol	Length	Info
117	1.243189	211.67.48.8	10.176.153.54	DNS	177	Standard query response 0x0001 PTR 8.48.67...
118	1.246213	10.176.153.54	211.67.48.8	DNS	71	Standard query 0x0002 A www.mit.edu
119	1.250499	211.67.48.8	10.176.153.54	DNS	87	Standard query response 0x0002 A www.mit.ed...
120	1.253662	10.176.153.54	211.67.48.8	DNS	71	Standard query 0x0003 AAAA www.mit.edu
126	1.400553	211.67.48.8	10.176.153.54	DNS	524	Standard query response 0x0003 AAAA www.mit...
197	2.423956	10.176.153.54	47.96.231.89	UDP	42	58447→8200 Len=0
204	2.464064	10.176.153.54	47.96.231.89	UDP	42	58447→8200 Len=0

Transaction ID: 0x0003

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

- www.mit.edu: type AAAA, class IN

Name: www.mit.edu

[Name Length: 11]

[Label Count: 3]

Type: AAAA (IPv6 Address) (28)

Class: IN (0x0001)

0000 14 14 4b 6b 28 f1 48 e2 44 96 2a 8d 08 00 45 00 ..Kk(.H. D.*...E.

0010 00 39 cb 87 00 00 80 11 c7 fa 0a b0 99 36 d3 43 .9.....6.C

0020 30 08 f6 6c 00 35 00 25 f4 21 00 03 01 00 00 01 0..l.5.% !.....

0030 00 00 00 00 00 00 03 77 77 77 03 6d 69 74 03 65w ww.mit.e

0040 64 75 00 00 1c 00 01 du.....

15. 提供截图

No.	Time	Source	Destination	Protocol	Length	Info
117	1.243189	211.67.48.8	10.176.153.54	DNS	177	Standard query response 0x0001 PTR 8.48.67...
118	1.246213	10.176.153.54	211.67.48.8	DNS	71	Standard query 0x0002 A www.mit.edu
119	1.250499	211.67.48.8	10.176.153.54	DNS	87	Standard query response 0x0002 A www.mit.ed...
120	1.253662	10.176.153.54	211.67.48.8	DNS	71	Standard query 0x0003 AAAA www.mit.edu
126	1.400553	211.67.48.8	10.176.153.54	DNS	524	Standard query response 0x0003 AAAA www.mit...
197	2.423956	10.176.153.54	47.96.231.89	UDP	42	58447→8200 Len=0
204	2.464064	10.176.153.54	47.96.231.89	UDP	42	58447→8200 Len=0

Answers

- www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net

Name: www.mit.edu

Type: CNAME (Canonical NAME for an alias) (5)

Class: IN (0x0001)

Time to live: 1035

Data length: 25

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 AAAA, class IN, addr 2600:1417:8000:c8d::255e
- e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2600:1417:8000:cae::255e

Authoritative nameservers

Additional records

0030 00 04 00 08 00 09 03 77 77 77 03 6d 69 74 03 65w ww.mit.e

0040 64 75 00 00 1c 00 01 c0 0c 00 05 00 01 00 00 04 du.....

0050 0b 00 19 03 77 77 77 03 6d 69 74 03 65 64 75 07www. mit.edu.

0060 65 64 67 65 6b 65 79 03 6e 65 74 00 c0 29 00 05 edgekey. net...)

0070 00 01 00 00 00 3c 00 18 05 65 39 35 36 36 04 64<...e9566.d

16. 查询消息发往哪个 IP? 是默认 DNS 吗?

是默认 DNS

17. 查询类型? 是否有 answers?

查询类型是 NS 类型, 不包含任何 answer

18. 响应中提供了哪些 MIT 名称服务器? 是否提供了其 IP?

提供了大概 10 个, 具体结果如下图

19. 提供截图

11	2018-08-06 20:08:...	10.21.2.185	239.255.255.2...	SSDP	216	M-SEARCH * HTTP/1.1
12	2018-08-06 20:08:...	10.21.2.48	10.21.2.185	SSDP	535	HTTP/1.1 200 OK
17	2018-08-06 20:08:...	10.21.2.185	239.255.255.2...	SSDP	216	M-SEARCH * HTTP/1.1
20	2018-08-06 20:08:...	10.21.2.48	10.21.2.185	SSDP	535	HTTP/1.1 200 OK
25	2018-08-06 20:08:...	10.21.2.185	10.21.30.100	DNS	67	Standard query 0x6a57 NS mit.edu
26	2018-08-06 20:08:...	10.21.30.100	10.21.2.185	DNS	430	Standard query response 0x6a57 NS mit.edu NS eur5.akam.
27	2018-08-06 20:08:...	10.21.2.185	239.255.255.2...	SSDP	216	M-SEARCH * HTTP/1.1
28	2018-08-06 20:08:...	10.21.2.48	10.21.2.185	SSDP	535	HTTP/1.1 200 OK
33	2018-08-06 20:08:...	10.21.2.185	239.255.255.2...	SSDP	216	M-SEARCH * HTTP/1.1
34	2018-08-06 20:08:...	10.21.2.48	10.21.2.185	SSDP	535	HTTP/1.1 200 OK

```

▶ Ethernet II, Src: HuaweiTe_b4:29:e1 (34:b3:54:b4:29:e1), Dst: Apple_ce:46:2d (ac:bc:32:ce:46:2d)
▶ Internet Protocol Version 4, Src: 10.21.30.100, Dst: 10.21.2.185
▶ User Datagram Protocol, Src Port: 53, Dst Port: 49594
▼ Domain Name System (response)
  Transaction ID: 0x6a57
  ▶ Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 8
  Authority RRs: 0
  Additional RRs: 10
  ▼ 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)
  ▼ Answers
    ▶ mit.edu: type NS, class IN, ns eur5.akam.net
    ▶ mit.edu: type NS, class IN, ns ns1-173.akam.net
    ▶ mit.edu: type NS, class IN, ns asia2.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 use5.akam.net
    ▶ mit.edu: type NS, class IN, ns ns1-37.akam.net
    ▶ mit.edu: type NS, class IN, ns use2.akam.net
  ▼ Additional records
    ▶ eur5.akam.net: type A, class IN, addr 23.74.25.64
    ▶ ns1-173.akam.net: type A, class IN, addr 193.108.91.173
    ▶ ns1-173.akam.net: type AAAA, class IN, addr 2600:1401:2::ad
    ▶ usw2.akam.net: type A, class IN, addr 184.26.161.64
    ▶ asia1.akam.net: type A, class IN, addr 95.100.175.64
    ▶ use5.akam.net: type A, class IN, addr 2.16.40.64
    ▶ use5.akam.net: type AAAA, class IN, addr 2600:1403:a::40

```

20. 查询消息发往哪个 IP? 是否是默认 DNS? 若不是, 对应什么?

No.	Time	Source	Destination	Protocol	Length	Info
48	1.424289	10.176.153.54	211.67.48.8	DNS	73	Standard query 0x83b0 A bitsy.mit.edu
53	1.453822	10.176.153.54	211.67.48.8	DNS	73	Standard query 0x83b0 A bitsy.mit.edu
54	1.459599	211.67.48.8	10.176.153.54	DNS	89	Standard query response 0x83b0 A bitsy.mit...
55	1.462642	10.176.153.54	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr...
78	2.173767	10.176.153.54	47.96.231.89	UDP	42	58447→8200 Len=0
120	3.477643	10.176.153.54	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
139	4.039722	10.176.153.54	39.97.4.86	TLSv1.2	273	Application Data

DNS 第一次查询消息发送的 IP 地址是默认的本地域名服务器, 查询到 bitsy.mit.edu 的 IP 地址: 18.72.0.3, 之后向这个 IP 地址发送查询消息, 但失败了, 因为 MIT 的这个 DNS 服务器已停用

21. 查询类型? 是否有 answers?

查询类型是 A 类型, 该查询消息不包含任何答案

22. 响应中有多少 answers? 都包含了什么?

没有 answer

No.	Time	Source	Destination	Protocol	Length	Info
19	2018-08-06 20:31:...	10.21.2.185	10.21.30.100	DNS	73	Standard query 0x7f9a A bitsy.mit.edu
20	2018-08-06 20:31:...	10.21.30.100	10.21.2.185	DNS	89	Standard query response 0x7f9a A bitsy.mit.edu
21	2018-08-06 20:31:...	10.21.2.185	18.72.0.3	DNS	74	Standard query 0x5fc5 A www.aiit.or.kr
46	2018-08-06 20:31:...	10.21.2.185	18.72.0.3	DNS	74	Standard query 0x5fc5 A www.aiit.or.kr
76	2018-08-06 20:31:...	10.21.2.185	18.72.0.3	DNS	74	Standard query 0x5fc5 A www.aiit.or.kr
10...	2018-08-06 20:34:...	10.21.2.185	10.21.30.100	DNS	98	Standard query 0x548f PTR lb._dns-sd._udp.0.2.
10...	2018-08-06 20:34:...	10.21.30.100	10.21.2.185	DNS	175	Standard query response 0x548f No such name PT

```

▶ Frame 76: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▶ Ethernet II, Src: Apple_ce:46:2d (ac:bc:32:ce:46:2d), Dst: HuaweiTe_b4:29:e1 (34:b3:54:b4:29:e1)
▶ Internet Protocol Version 4, Src: 10.21.2.185, Dst: 18.72.0.3
▶ User Datagram Protocol, Src Port: 64657, Dst Port: 53
▼ Domain Name System (query)
  Transaction ID: 0x5fc5
  ▶ Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▶ www.aiit.or.kr: type A, class IN
      Name: www.aiit.or.kr
      [Name Length: 14]
      [Label Count: 4]
      Type: A (Host Address) (1)
      Class: IN (0x0001)

```

23. 提供截图

The screenshot shows a Wireshark packet capture window titled '*WLAN'. The filter bar at the top is set to 'ip.addr == 10.176.153.54'. The packet list on the left shows several packets, with packet 54 selected. The packet details pane on the right shows the structure of the selected packet, which is a DNS Standard query response. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
48	1.424289	10.176.153.54	211.67.48.8	DNS	73	Standard query 0x83b0 A bitsy.mit.edu
53	1.453822	10.176.153.54	211.67.48.8	DNS	73	Standard query 0x83b0 A bitsy.mit.edu
54	1.459599	211.67.48.8	10.176.153.54	DNS	89	Standard query response 0x83b0 A bitsy.mit...
55	1.462642	10.176.153.54	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr...
78	2.173767	10.176.153.54	47.96.231.89	UDP	42	58447→8200 Len=0
120	3.477643	10.176.153.54	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
139	4.039722	10.176.153.54	39.97.4.86	TLSv1.2	273	Application Data

Packet 54 details:

- Name: bitsy.mit.edu
- [Name Length: 13]
- [Label Count: 3]
- Type: A (Host Address) (1)
- Class: IN (0x0001)
- Answers
 - bitsy.mit.edu: type A, class IN, addr 18.0.72.3
 - Name: bitsy.mit.edu
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)
 - Time to live: 54
 - Data length: 4
 - Address: 18.0.72.3

Packet 54 bytes:

```
0010  00 4b 00 00 40 00 3b 11 98 70 d3 43 30 08 0a b0 .K..@.;. .p.C0...
0020  99 36 00 35 fc e9 00 37 50 d6 83 b0 81 80 00 01 .6.5...7 P.....
0030  00 01 00 00 00 00 05 62 69 74 73 79 03 6d 69 74 .....b itsy.mit
0040  03 65 64 75 00 00 01 00 01 c0 0c 00 01 00 01 00 .edu.... ....
0050  00 00 36 00 04 12 00 48 03 ..6...H .
```