

学号：	姓名：	班级：
实验题目： 实验三 DNS		
实验学时：2h	实验日期：2023. 03. 13	
实验目的： 查看本地 DNS 服务器、DNS 缓存、DNS 记录和消息以及 DNS 记录中的 TYPE 字段，使用 DNS 服务器查询其他服务器。		
硬件环境： Windows10 家庭版		
软件环境： Wireshark		
<p>实验步骤与内容：</p> <p>实验内容：</p> <p>实验一：</p> <ol style="list-style-type: none"> 1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server? 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? <p>实验二：</p> <ol style="list-style-type: none"> 4. Locate the DNS query and response messages. Are then sent over UDP or TCP? 5. What is the destination port for the DNS query message? What is the source port of DNS response message? 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? 7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”? 8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain? 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? 10. This web page contains images. Before retrieving each image, does your host issue new DNS queries? <p>实验三：</p> <ol style="list-style-type: none"> 11. What is the destination port for the DNS query message? What is the source port of DNS response message? 12. To what IP address is the DNS query message sent? Is this the IP address of your 		

default local DNS server?

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

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

15. Provide a screenshot

实验四：

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

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

19. Provide a screenshot.

实验五：

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?

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

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

23. Provide a screenshot.

实验步骤：

打开 Wireshark，然后根据实验指导书，完成相关的 DNS 查询，然后使用 Wireshark 进行抓包，并查看相关信息。

实验一：

1.



```
Microsoft Windows [版本 10.0.19044.2604]  
(c) Microsoft Corporation. 保留所有权利。  
  
C:\Users\sdu.wzl>nslookup www.sdu.edu.cn  
服务器: UnKnown  
Address: 192.168.254.245  
  
名称: www.sdu.edu.cn  
Addresses: 2001:da8:7000:7:202:194:7:118  
202.194.7.118
```

2.

```
C:\Users\sdu.wzl>nslookup -type=NS ox.ac.uk
服务器:  UnKnown
Address:  192.168.254.245
```

非权威应答:

```
ox.ac.uk          nameserver = auth4.dns.ox.ac.uk
ox.ac.uk          nameserver = dns0.ox.ac.uk
ox.ac.uk          nameserver = auth6.dns.ox.ac.uk
ox.ac.uk          nameserver = dns1.ox.ac.uk
ox.ac.uk          nameserver = dns2.ox.ac.uk
ox.ac.uk          nameserver = auth5.dns.ox.ac.uk
```

```
dns0.ox.ac.uk     internet address = 129.67.1.190
dns1.ox.ac.uk     internet address = 129.67.1.191
dns2.ox.ac.uk     internet address = 163.1.2.190
auth4.dns.ox.ac.uk internet address = 45.33.127.156
auth4.dns.ox.ac.uk AAAA IPv6 address = 2600:3c00:e000:19::1
auth5.dns.ox.ac.uk internet address = 93.93.128.67
auth5.dns.ox.ac.uk AAAA IPv6 address = 2a00:1098:0:80:1000::10
auth6.dns.ox.ac.uk internet address = 185.24.221.32
auth6.dns.ox.ac.uk AAAA IPv6 address = 2a02:2770:11:0:21a:4aff:febe:759b
```

3. 直接查询 Yahoo

```
C:\Users\sdu.wzl>nslookup mail.yahoo.com
服务器:  UnKnown
Address:  192.168.254.245
```

非权威应答:

```
名称:  edge.gycpi.b.yahoodns.net
Addresses:  2001:4998:64:800::6001
            2001:4998:64:800::6000
            69.147.80.15
            69.147.80.12
Aliases:  mail.yahoo.com
```

使用问题 2 的 DNS 服务器查询

```
C:\Users\sdu.wzl>nslookup mail.yahoo.com dns0.ox.ac.uk
服务器:  auth0.dns.ox.ac.uk
Address:  129.67.1.190

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

使用山大 DNS 服务器查询

```
C:\Users\sdu.wzl>nslookup mail.yahoo.com sdunetsv2.sdu.edu.cn
服务器: UnKnown
Address: 202.194.15.13

非权威应答:
名称: edge.gycpi.b.yahoodns.net
Addresses: 2001:4998:64:800::6000
           2001:4998:64:800::6001
           69.147.80.12
           69.147.80.15
Aliases: mail.yahoo.com
```

实验二:

4. 使用的是 UDP。

273	2023-03-13	14:04:32.532653	172.25.162.148	192.168.254.245	DNS	95 Standard query 0x88b4 A content-signature-2.cdn.mozilla.net
274	2023-03-13	14:04:32.533934	192.168.254.245	172.25.162.148	DNS	249 Standard query response 0x88b4 A content-signature-2.cdn.mozilla.net
275	2023-03-13	14:04:32.535125	172.25.162.148	192.168.254.245	DNS	117 Standard query 0xbe1c A prod.content-signature-chains.prod.mozilla.net
277	2023-03-13	14:04:32.536907	192.168.254.245	172.25.162.148	DNS	430 Standard query response 0xbe1c A prod.content-signature-chains.prod.mozilla.net
284	2023-03-13	14:04:32.685592	172.25.162.148	192.168.254.245	DNS	84 Standard query 0xa465 A detectportal.firefox.com
286	2023-03-13	14:04:32.708550	172.25.162.148	192.168.254.245	DNS	80 Standard query 0x1a59 A home.firefoxchina.cn
297	2023-03-13	14:04:32.712343	192.168.254.245	172.25.162.148	DNS	221 Standard query response 0x1a59 A home.firefoxchina.cn CNAME
298	2023-03-13	14:04:32.714268	172.25.162.148	192.168.254.245	DNS	111 Standard query 0x311f A home.firefoxchina.cn.wwebpic.com.cn
299	2023-03-13	14:04:32.716982	172.25.162.148	192.168.254.245	DNS	84 Standard query 0xa465 A detectportal.firefox.com

> Frame 273: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface \Device\NPF	0000	28 a2 4b f6 12 a0 14 5a fc 1f d7 61 08 00 45 00
> Ethernet II, Src: LiteonTe_1f:d7:61 (14:5a:fc:1f:d7:61), Dst: JuniperN_f6:12:a0 (28:a2:4b:f6:12:a0)	0010	00 51 6e 76 00 00 80 11 bd d9 ac 19 a2 94 c0 a8
> Internet Protocol Version 4, Src: 172.25.162.148, Dst: 192.168.254.245	0020	fe f5 f6 24 00 35 00 3d d2 ba 88 b4 01 00 00 01
> User Datagram Protocol, Src Port: 63012, Dst Port: 53	0030	00 00 00 00 00 00 13 63 6f 6e 74 65 6e 74 2d 73
Source Port: 63012	0040	69 67 6e 61 74 75 72 65 2d 32 03 63 64 6e 07 6d
Destination Port: 53	0050	6f 7a 69 6c 6c 61 03 6e 65 74 00 00 01 00 01
Length: 61		
Checksum: 0xd2ba [unverified]		
[Checksum Status: Unverified]		
[Stream index: 6]		
> [Timestamps]		
UDP payload (53 bytes)		
> Domain Name System (query)		

5. 查询消息的目标端口和响应消息的源端口都是 53。

6. 发送到 192.168.254.245，与本机的 DNS 服务器的 IP 地址是相同的。

7. DNS 查询的类型是 A 类型，不包含答案。

8. 提供答案的数量不固定，其中答案中包含了主机的 IP 地址、主机的名称等。

9. 通过查询发现，SYN 数据包的目标 IP 地址是与 DNS 响应消息提供的 IP 地址对应的。

10. 不会每次都发出新的 DNS 查询，因为本机的 DNS 会被缓存，因此不需要发起新的 DNS 查询。

实验三:

11. 查询消息的目标端口和响应消息的源端口都是 53。

12. 发送到 IP 地址为 192.168.254.245，是本机的 DNS 服务器的 IP 地址。

13. DNS 查询的类型是 A 类型，不包含答案。

14. 三个答案，其中包含了 IP 地址，主机名，规范主机名等信息。

15.

137	2023-03-13	14:24:55.827930	192.168.254.245	192.168.254.245	DNS	71	Standard	query	0x0002	A	www.mit.edu	
138	2023-03-13	14:24:55.837839	192.168.254.245	172.25.162.148	DNS	160	Standard	query response	0x0002	A	www.mit.edu	CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net
139	2023-03-13	14:24:55.838911	172.25.162.148	192.168.254.245	DNS	71	Standard	query	0x0003	AAAA	www.mit.edu	
140	2023-03-13	14:24:55.847078	192.168.254.245	172.25.162.148	DNS	200	Standard	query response	0x0003	AAAA	www.mit.edu	CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net

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: 980 (16 minutes, 20 seconds)

Data length: 25

CNAME: www.mit.edu.edgekey.net

www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net

Name: www.mit.edu.edgekey.net

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

Class: IN (0x0001)

Time to live: 60 (1 minute)

Data length: 24

CNAME: e9566.dscb.akamaiedge.net

e9566.dscb.akamaiedge.net: type A, class IN, addr 23.2.130.241

Name: e9566.dscb.akamaiedge.net

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 60 (1 minute)

Data length: 4

Address: 23.2.130.241

[Request In: 137]

[Time: 0.009909000 seconds]

0000 14 5a fc 1f d7 61 28 a2 4b f6 12 a0 08 00 45 00 -Z...a(- K...-E-

0010 00 92 1f dd 00 00 3e 11 4e 32 c0 a8 fe 15 ac 19> N2.....

0020 a2 94 00 35 fb 84 00 7e c9 13 00 02 81 80 00 01 ...5... 0.....

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

0040 64 75 00 00 01 00 01 c0 0c 00 05 00 01 00 00 03 du.....

0050 d4 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 64e9566=d

0080 73 63 62 0a 61 6b 61 6d 61 69 65 64 67 65 c0 3d scb-akam aiedge=

0090 c0 4e 00 01 00 01 00 00 00 3c 00 04 17 02 82 f1 -H.....<.....

实验四：

16. 发送到 IP 地址为 192. 168. 254. 245，是本机的 DNS 服务器的 IP 地址。

17. 类型是 NS，不包含答案。

18. 并没有提供 IP 地址。

Answers	
>	mit.edu: type NS, class IN, ns asia1.akam.net
>	mit.edu: type NS, class IN, ns ns1-37.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 use5.akam.net
>	mit.edu: type NS, class IN, ns eur5.akam.net
>	mit.edu: type NS, class IN, ns use2.akam.net
>	mit.edu: type NS, class IN, ns ns1-173.akam.net

19.

227	2023-03-13	14:32:38.075362	192.168.254.245	172.25.162.148	DNS	446	Standard	query	0x0002	NS	mit.edu	NS asia1.akam.net NS ns1-37.akam.net NS asia2
259	2023-03-13	14:32:38.947435	172.25.162.148	192.168.254.245	DNS	72	Standard	query	0xa83c	A	www.bing.com	
260	2023-03-13	14:32:38.983867	172.25.162.148	192.168.254.245	DNS	72	Standard	query	0xa83c	A	www.bing.com	
261	2023-03-13	14:32:38.993360	192.168.254.245	172.25.162.148	DNS	226	Standard	query response	0xa83c	A	www.bing.com	CNAME www-www.bing.com.trafficmanager.net

[Checksum Status: Unverified]

[Stream index: 6]

[Timestamps]

UDP payload (404 bytes)

Domain Name System (response)

Transaction ID: 0x0002

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 8

Authority RRs: 0

Additional RRs: 11

Queries

Answers

> mit.edu: type NS, class IN, ns asia1.akam.net

> mit.edu: type NS, class IN, ns ns1-37.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 use5.akam.net

> mit.edu: type NS, class IN, ns eur5.akam.net

> mit.edu: type NS, class IN, ns use2.akam.net

> mit.edu: type NS, class IN, ns ns1-173.akam.net

0010 01 b0 92 2a 00 00 3e 11 da c6 c0 a8 fe f5 ac 19 ...*->>.....

0020 a2 94 00 35 e4 f8 01 9c 4f 09 00 02 81 80 00 01 ...5... 0.....

0030 00 08 00 00 00 0b 03 6d 69 74 03 65 64 75 00 00m it-edu-

0040 02 00 01 c0 0c 00 02 00 01 00 00 03 d4 00 10 05>.....

0050 61 73 69 61 31 04 61 6b 61 6d 03 6e 65 74 00 c0 asia1-ak am-net-

0060 0c 00 02 00 01 00 00 03 d4 00 09 06 6e 73 31 2dns1-

0070 33 37 c0 2b c0 0c 00 02 00 01 00 00 03 d4 00 08 37+.....

0080 05 61 73 69 61 32 c0 2b c0 0c 00 02 00 01 00 00asia2+.....

0090 03 d4 00 07 04 75 73 77 32 c0 2b c0 0c 00 02 00usw 2+.....

00a0 01 00 00 03 d4 00 07 04 75 73 65 35 c0 2b c0 0cuse5+.....

00b0 00 02 00 01 00 00 03 d4 00 07 04 65 75 72 35 c0eur5+.....

00c0 2b c0 0c 00 02 00 01 00 00 03 d4 00 07 04 75 73+.....

00d0 65 32 c0 2b c0 0c 00 02 00 01 00 00 03 d4 00 0a e2+.....

00e0 07 6e 73 31 2d 31 37 33 c0 2b c0 90 00 01 00 01ns1-173 -+.....

00f0 00 00 fa cb 00 04 17 4a 19 40 c0 a3 00 01 00 01J.....

0100 00 00 da 63 00 04 60 07 31 40 c0 7d 00 01 00 01lg.....

0110 00 00 ff dd 00 04 02 10 28 40 c0 7d 00 1c 00 01(g.....

0120 00 00 ff dd 00 10 26 00 14 03 00 0a 00 00 00 00&.....

0130 00 00 00 00 00 40 c0 6a 00 01 00 01 00 01 22 e7@j.....

0140 00 04 b8 1a a1 40 c0 25 00 01 00 01 00 00 69 c0@%.....

0150 00 04 5f 64 af 40 c0 56 00 01 00 01 00 00 6d b5d@v.....

0160 00 04 5f 65 24 40 c0 41 00 01 00 01 00 01 3a e3e\$@A.....

0170 00 04 c1 6c 5b 25 c0 41 00 1c 00 01 00 01 3a e3[}%A.....

实验五：

20. 发送到 18. 0. 72. 3，并不是本地 DNS 服务器的 IP 地址。

21. 查询类型是 A 类型，不包含答案。

110	2023-03-20	10:50:19.808063	192.168.254.245	172.25.147.201	DNS	155	Standard query response 0xbd86 HTTPS hm.
202	2023-03-20	10:50:41.393967	172.25.147.201	192.168.254.245	DNS	73	Standard query 0xbbe4 A bitsy.mit.edu
203	2023-03-20	10:50:41.428273	172.25.147.201	192.168.254.245	DNS	73	Standard query 0xbbe4 A bitsy.mit.edu
204	2023-03-20	10:50:41.429544	192.168.254.245	172.25.147.201	DNS	468	Standard query response 0xbbe4 A bitsy.m
205	2023-03-20	10:50:41.432013	172.25.147.201	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-a
206	2023-03-20	10:50:41.441251	192.168.254.245	172.25.147.201	DNS	384	Standard query response 0xbbe4 A bitsy.m
217	2023-03-20	10:50:43.444146	172.25.147.201	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
222	2023-03-20	10:50:45.459802	172.25.147.201	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.k
244	2023-03-20	10:50:47.467963	172.25.147.201	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
247	2023-03-20	10:50:49.475015	172.25.147.201	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.k

Frame 217: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF{...}						0000	28 a2 4b f6 12 a0 14 5a fc 1
Ethernet II, Src: LiteonTe_1f:d7:61 (14:5a:fc:1f:d7:61), Dst: JuniperM_f6:12:a0 (28:a2:4b:f6:12:a0)						0010	00 3c 6a bd 00 00 80 11 36 0
Internet Protocol Version 4, Src: 172.25.147.201, Dst: 18.0.72.3						0020	48 03 dd 95 00 35 00 28 46 4
User Datagram Protocol, Src Port: 56725, Dst Port: 53						0030	00 00 00 00 00 00 03 77 77 7
Domain Name System (query)						0040	6f 72 02 6b 72 00 00 01 00 0
Transaction ID: 0x0002							
Flags: 0x0100 Standard query							
Questions: 1							
Answer RRs: 0							
Authority RRs: 0							
Additional RRs: 0							
Queries							

22. 提供 1 个 answer，包含主机的 IP 地址等等。

23.

110	2023-03-20	10:50:19.808063	192.168.254.245	172.25.147.201	DNS	155	Standard query response 0xbd86 HTTPS hm.baidu.com CNAME hm.e.shifen.com SOA ns1.e.shifen.com
202	2023-03-20	10:50:41.393967	172.25.147.201	192.168.254.245	DNS	73	Standard query 0xbbe4 A bitsy.mit.edu
203	2023-03-20	10:50:41.428273	172.25.147.201	192.168.254.245	DNS	73	Standard query 0xbbe4 A bitsy.mit.edu
204	2023-03-20	10:50:41.429544	192.168.254.245	172.25.147.201	DNS	468	Standard query response 0xbbe4 A bitsy.mit.edu A 18.0.72.3 NS ns1-173.akam.net NS use5.akam.n.
205	2023-03-20	10:50:41.432013	172.25.147.201	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
206	2023-03-20	10:50:41.441251	192.168.254.245	172.25.147.201	DNS	384	Standard query response 0xbbe4 A bitsy.mit.edu A 18.0.72.3 NS eur5.akam.net NS asia2.akam.net.
217	2023-03-20	10:50:43.444146	172.25.147.201	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
222	2023-03-20	10:50:45.459802	172.25.147.201	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
244	2023-03-20	10:50:47.467963	172.25.147.201	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
247	2023-03-20	10:50:49.475015	172.25.147.201	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr

Frame 206: 384 bytes on wire (3072 bits), 384 bytes captured (3072 bits) on interface \Device\NPF{...}						0000	14 5a fc 1f d7 61 28 a2 4b f6 12 a0 08 00 45 00	+Z---a(- K-----E-
Ethernet II, Src: JuniperM_f6:12:a0 (28:a2:4b:f6:12:a0), Dst: LiteonTe_1f:d7:61 (14:5a:fc:1f:d7:61)						0010	01 72 ae c5 00 00 3e 11 cd 34 c0 a8 fe f5 ac 19	+P-----> -4-----
Internet Protocol Version 4, Src: 192.168.254.245, Dst: 172.25.147.201						0020	93 c9 00 35 dd 93 01 5e ff 87 bb e4 81 80 00 01	...5---A -----
User Datagram Protocol, Src Port: 53, Dst Port: 56723						0030	00 01 00 08 00 08 05 62 69 74 73 79 03 6d 69 74	-----b itsy-mit
Domain Name System (response)						0040	03 65 64 75 00 00 01 00 01 c0 0c 00 01 00 01 00	edu-----
Transaction ID: 0xbbe4						0050	00 00 3c 00 04 12 00 48 03 c0 12 00 02 00 01 00	---<-----H -----
Flags: 0x8180 Standard query response, No error						0060	01 72 38 00 0f 04 65 75 72 35 04 61 6b 61 6d 03	+r8---eu r5-akam-
Questions: 1						0070	6e 65 74 00 c0 12 00 02 00 01 00 01 72 38 00 08	net-----r8---
Answer RRs: 1						0080	05 61 73 69 61 32 c0 40 c0 12 00 02 00 01 00 01	asia2@-----
Authority RRs: 8						0090	72 38 00 08 05 61 73 69 61 31 c0 40 c0 12 00 02	r8---asl al@---
Additional RRs: 8						00a0	00 01 00 01 72 38 00 07 04 75 73 77 32 c0 40 c0	---r8---use2@---
Queries						00b0	12 00 02 00 01 00 01 72 38 00 07 04 75 73 65 32	-----P 8---use2
Answers						00c0	c0 40 c0 12 00 02 00 01 00 01 72 38 00 0a 07 6e	@-----r8---n
bitsy.mit.edu: type A, class IN, addr 18.0.72.3						00d0	73 31 2d 31 37 33 c0 40 c0 12 00 02 00 01 00 01	s1-173@-----
Name: bitsy.mit.edu						00e0	72 38 00 09 06 6e 73 31 2d 33 37 c0 40 c0 12 00	r8---ns1 -37@---
Type: A (Host Address) (1)						00f0	02 00 01 00 01 72 38 00 07 04 75 73 65 35 c0 40	---r8---use5@---
Class: IN (0x0001)						0100	c0 3b 00 01 00 01 00 00 e2 9b 00 04 17 4a 19 40	;------>@---
Time to live: 60 (1 minute)						0110	c0 91 00 01 00 01 00 00 e1 91 00 04 60 07 31 40	;------>@---
Data length: 4						0120	c0 cf 00 01 00 01 00 01 8c b4 00 04 02 10 28 40	-----@-----
Address: 18.0.72.3						0130	c0 7e 00 01 00 01 00 00 a1 e7 00 04 b8 1a a1 40	-----@-----
Authoritative nameservers						0140	c0 6a 00 01 00 01 00 01 4f 45 00 04 5f 64 af 40	+j;-----0E--_d@---
Additional records						0150	c0 56 00 01 00 01 00 00 8d 0a 00 04 5f 65 24 40	+V;-----es@---
[Retransmitted response, original response in: 204]						0160	c0 ba 00 01 00 01 00 01 3c f4 00 04 c1 6c 5b 25	-----<---l[%
[Retransmission: True]						0170	c0 a4 00 01 00 01 00 00 05 d2 00 04 c1 6c 5b ad	-----<---l[.

结论分析与体会：

通过具体地执行 DNS 的相关命令，增加了对 DNS 相关知识的认识，同时查看了 DNS 记录和报文的相关内容。当使用一些国外的 DNS 服务器无法进行查询时，我们可以使用山大本地的 DNS 服务器。