

实验报告

实验二 HTTP与DNS

Lab2 HTTP & DHS

PART 2

罗晏宸

PB17000297

2019.9.25

实验目的

2. 研究学习DNS协议

1. 实践学习DNS功能与工作原理
 2. 学习使用 `nslookup` 工具分析DNS工作过程
 3. 学习使用 `ipconfig` 工具调试网络
 4. 利用Wireshark捕获并过滤DNS分组并加以分析
-

实验内容

学习使用 `nslookup` 指令工具

1. 运行指令

```
1 | nslookup www.nju.edu.cn
```

以获取南京大学(www.nju.edu.cn)Web服务器的IP地址

C:\Users\瞳木水杉>nslookup www.nju.edu.cn
Server: mx.ustc.edu.cn
Address: 202.38.64.56

Non-authoritative answer:
Name: www.nju.edu.cn
Address: 202.119.32.7

2. 运行指令

```
1 | nslookup -type=NS ed.ac.edu.uk
```

以确定英国爱丁堡大学(ed.ac.edu.uk)的DNS服务器

```
C:\Users\瞳木水杉>nslookup -type=NS ed.ac.uk
Server: mx.ustc.edu.cn
Address: 202.38.64.56

In general, nslookup can be run with zero, one, two or more options. And as we have seen
Non-authoritative answer:
ed.ac.uk      nameserver = xlab-0.ed.ac.uk
ed.ac.uk      nameserver = dns0.inf.ed.ac.uk
ed.ac.uk      nameserver = lewis.ucs.ed.ac.uk
ed.ac.uk      nameserver = dns1.inf.ed.ac.uk
ed.ac.uk      nameserver = dns2.inf.ed.ac.uk
ed.ac.uk      nameserver = cancer.ucs.ed.ac.uk
```

3 运行指令

```
1 | nslookup mail.Yahoo.com ns.ustc.edu.cn
```

向中国科学技术大学DNS服务器(ns.ustc.edu.cn)请求解析Yahoo邮箱的服务器(mail.Yahoo.com)的IP地址

```
C:\Users\瞳木水杉>nslookup mail.Yahoo.com ns.ustc.edu.cn
Server: ns.ustc.edu.cn
Address: 2001:da8:d800::1

Non-authoritative answer:
Name: ds-any-ycpi-uno.aycpi.b.yahoodns.net
Addresses: 2001:4998:28:800::4001
            209.73.190.12
            209.73.190.11

Aliases: mail.Yahoo.com
          fd-geovcpi-uno.gvcpi.b.yahoodns.net
```

向爱丁堡大学的服务器请求会不被接受而超时

```
C:\Users\瞳木水杉>nslookup mail.Yahoo.com cancer.ucs.ed.ac.uk  
Server: cancer.ucs.ed.ac.uk  
Address: 129.215.200.7  
  
DNS request timed out. An overview of nslookup, it is time for you to test drive it  
you can probably write down the results):  
*** Request to cancer.ucs.ed.ac.uk timed-out
```

4. 由以上命令运行结果回答问题如下

1. 南京大学(www.nju.edu.cn)Web服务器的IP地址为 202.119.32.7

2. 英国爱丁堡大学的DNS服务器有 `xlab-0.ed.ac.uk`、
`dns0.inf.ed.ac.uk`、`lewis.ucs.ed.ac.uk`、
`dns1.inf.ed.ac.uk`、`dns2.inf.ed.ac.uk`、`cancer.ucs.ed.ac.uk`
3. 向中国科学技术大学DNS服务器(`ns.ustc.edu.cn`)请求解析Yahoo邮箱的
服务器(`mail.Yahoo.com`)得到其IP地址为 `209.73.190.12` 与
`209.73.190.11`

学习使用 `ipconfig` 指令工具

1. 运行指令

```
1 | ipconfig /all
```

以显示关于主机的所有信息

```
命令提示符  
C:\Users\瞳木水杉>ipconfig /all  
  
Windows IP Configuration  
  
Host Name . . . . . : YC  
Primary Dns Suffix . . . . . :  
Node Type . . . . . : Hybrid  
IP Routing Enabled. . . . . : No  
WINS Proxy Enabled. . . . . : No  
DNS Suffix Search List. . . . . : ustc.edu.cn  
  
Ethernet adapter Npcap Loopback Adapter:  
  
Connection-specific DNS Suffix . . . . . :  
Description . . . . . : Npcap Loopback Adapter  
Physical Address . . . . . : 02-00-4C-4F-4F-50  
DHCP Enabled. . . . . : Yes  
Autoconfiguration Enabled . . . . . : Yes  
Link-local IPv6 Address . . . . . : fe80::8d89:629:464:f9eb%13(Preferred)  
Autoconfiguration IPv4 Address. . . . . : 169.254.249.235(Preferred)  
Subnet Mask . . . . . : 255.255.0.0  
Default Gateway . . . . . :  
DHCPv6 IAID . . . . . : 889323596  
DHCPv6 Client DUID. . . . . : 00-01-00-01-22-24-0B-D9-3C-95-09-5D-2E-4B  
DNS Servers . . . . . : fec0:0:0:ffff::1%1  
fec0:0:0:ffff::2%1  
fec0:0:0:ffff::3%1  
NetBIOS over Tcpip. . . . . : Enabled  
  
Wireless LAN adapter 本地连接* 2:  
  
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . . . . . :  
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3  
Physical Address. . . . . : 3E-95-09-5D-2E-4B  
DHCP Enabled. . . . . : Yes  
Autoconfiguration Enabled . . . . . : Yes  
  
Wireless LAN adapter 本地连接* 4:  
  
Connection-specific DNS Suffix . . . . . :  
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #4  
Physical Address. . . . . : 4E-95-09-5D-2E-4B  
DHCP Enabled. . . . . : No  
Autoconfiguration Enabled . . . . . : Yes  
Link-local IPv6 Address . . . . . : fe80::9179:1975:75fa:c221%3(Preferred)  
IPv4 Address. . . . . : 192.168.137.1(Preferred)  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . :  
DHCPv6 IAID . . . . . : 55481609  
DHCPv6 Client DUID. . . . . : 00-01-00-01-22-24-0B-D9-3C-95-09-5D-2E-4B  
DNS Servers . . . . . : fec0:0:0:ffff::1%1  
fec0:0:0:ffff::2%1  
fec0:0:0:ffff::3%1  
NetBIOS over Tcpip. . . . . : Enabled  
  
Wireless LAN adapter WLAN:  
  
Connection-specific DNS Suffix . . . . . : ustc.edu.cn  
Description . . . . . . . . . : Qualcomm Atheros QCA61x4A Wireless Network  
Adapter  
Physical Address. . . . . . . . . : 3C-95-09-5D-2E-4B  
DHCP Enabled. . . . . . . . . : Yes  
Autoconfiguration Enabled . . . . . . . . : Yes  
IPv6 Address. . . . . . . . . : 2001:da8:d800:199:f488:426c:d370:8cae(Pref  
erred)  
Temporary IPv6 Address. . . . . . . . . : 2001:da8:d800:199:ad02:4462:4bd5:d9eb(Pref  
erred)  
Link-local IPv6 Address . . . . . . . . . : fe80::f488:426c:d370:8cae%17(Preferred)  
IPv4 Address. . . . . . . . . : 114.214.187.196(Preferred)  
Subnet Mask . . . . . . . . . : 255.255.240.0  
Lease Obtained. . . . . . . . . : 2019年9月25日 9:44:14
```

2. 运行指令

1 | ipconfig /display

以显示DNS缓存记录所有信息

3. 运行指令

```
1 | ipconfig /flushdns
```

以清除DNS缓存

```
C:\Users\瞳木水杉>ipconfig /flushdns
Provide the following command:
Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

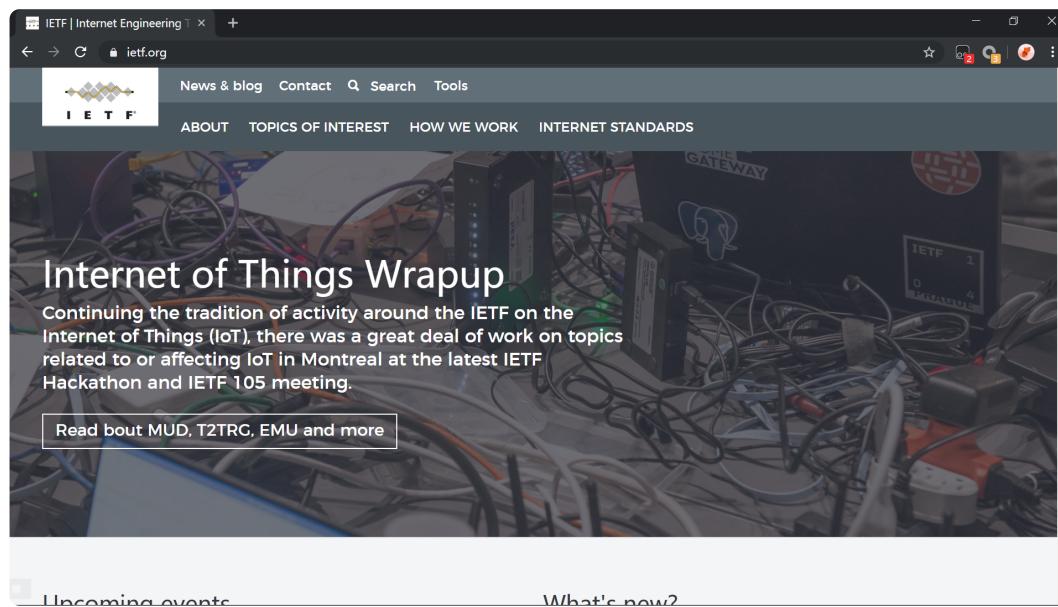
使用Wireshark捕获分析DNS报文

1. 清除网页缓存

2. 设置Wireshark过滤本机IP地址 192.168.1.103

3. 浏览给定网址

<http://www.ietf.org>



4. 捕获如下分组

1. DNS请求

```
1 Domain Name System (query)
2 Transaction ID: 0x8547
3 Flags: 0x0100 Standard query
4 0.... .... .... = Response: Message is a query
5 .000 0.... .... = Opcode: Standard query (0)
6 .... ..0. .... .... = Truncated: Message is not truncated
7 .... ...1 .... .... = Recursion desired: Do query
8 .... .... 0... .... = Z: reserved (0)
9 .... .... ....0 .... = Non-authenticated data: Unacceptable
```

```
10 | Questions: 1
11 | Answer RRs: 0
12 | Authority RRs: 0
13 | Additional RRs: 0
14 | Name: www.ietf.org
15 | Type: A (Host Address) (1)
16 | Class: IN (0x0001)
```

2. DNS响应

```
1 | Domain Name System (response)
2 | Transaction ID: 0x8547
3 | Flags: 0x8180 Standard query response, No error
4 | .... .... .... = Response: Message is a response
5 | .000 0.... .... = Opcode: Standard query (0)
6 | .... 0.. .... .... = Authoritative: Server is not an
7 | authority for domain
8 | .... ..0. .... .... = Truncated: Message is not truncated
9 | .... ...1 .... .... = Recursion desired: Do query
10 | recursively
11 | .... .... 1.... .... = Recursion available: Server can do
12 | recursive queries
13 | .... .... 0.. .... = Z: reserved (0)
14 | .... .... ...0. .... = Answer authenticated:
15 | Answer/authority portion was not authenticated by the
16 | server
17 | .... .... ...0 .... = Non-authenticated data: Unacceptable
18 | .... .... .... 0000 = Reply code: No error (0)
19 | Questions: 1
20 | Answer RRs: 3
21 | Authority RRs: 0
22 | Additional RRs: 0
23 | www.ietf.org: type A, class IN
24 | Name: www.ietf.org
25 | Type: A (Host Address) (1)
26 | Class: IN (0x0001)
27 | www.ietf.org: type CNAME, class IN, cname
28 | www.ietf.org.cdn.cloudflare.net
29 | www.ietf.org.cdn.cloudflare.net: type A, class IN, addr
30 | 104.20.0.85
31 | www.ietf.org.cdn.cloudflare.net: type A, class IN, addr
32 | 104.20.1.85
```

5. 阅读分组具体内容，对实验问题的回答如下

4. 通过UDP发送

5. DNS查询消息的目标端口和响应消息的源端口均为 53

6. DNS查询消息发送至IP地址 8.8.8.8，通过 ipconfig 查得本地的DNS
服务器地址 192.168.1.103#53 两者并不相同

7. 由内容 Type: A (Host Address) (1) 可知, 类别为 A; 由内容

Answer RRs: 0 可知, 查询消息不包含任何回答

8. 由内容 Answer RRs: 3 可知, 响应消息提供了3个回答, 分别包括了如下主机别名和主机地址的信息

```
1 | www.ietf.org: type CNAME, class IN, cname
  | www.ietf.org.cdn.cloudflare.net
2 | Name: www.ietf.org
3 | Type: CNAME (Canonical NAME for an alias) (5)
4 | Class: IN (0x0001)
5 | Time to live: 206
6 | Data length: 33
7 | CNAME: www.ietf.org.cdn.cloudflare.net
```

```
1 | www.ietf.org.cdn.cloudflare.net: type A, class IN, addr
  | 104.20.0.85
2 | Name: www.ietf.org.cdn.cloudflare.net
3 | Type: A (Host Address) (1)
4 | Class: IN (0x0001)
5 | Time to live: 206
6 | Data length: 4
7 | Address: 104.20.0.85
```

```
1 | www.ietf.org.cdn.cloudflare.net: type A, class IN, addr
  | 104.20.1.85
2 | Name: www.ietf.org.cdn.cloudflare.net
3 | Type: A (Host Address) (1)
4 | Class: IN (0x0001)
5 | Time to live: 206
6 | Data length: 4
7 | Address: 104.20.1.85
```

9. 有对应的TCP SYN分组存在

10. 主机没有发出新的DNS查询

6. 运行指令

```
1 | nslookup www.mit.edu
```

以获取麻省理工学院(www.mit.edu)Web服务器的IP地址

```
C:\Users\瞳木水杉>nslookup www.mit.edu
Server: ns1.mx.ustc.edu.cn
Address: 202.38.64.56

        Answer the following questions6:
DNS request timed out.
    timeout was 2 seconds, is the DNS query message sent? Is this the IP address of your
Non-authoritative answer:server? If not, what does the IP address correspond to?
Name:      e9566.dscb.akamaiedge.net. What "Type" of DNS query is it? Does the
Addresses: 2600:1417:8000:4be::255e"?
        2600:1417:8000:4a2::255e. How many "answers" are provided? What
        23.57.56.98. These answers contain?
Aliases:   www.mit.edu
          www.mit.edu.edgekey.net
```

7. 捕获如下分组

1. DNS请求

```
1 Domain Name System (query)
2 Transaction ID: 0x0006
3 Flags: 0x0100 Standard query
4 0.... .... .... = Response: Message is a query
5 .000 0.... .... = Opcode: Standard query (0)
6 .... .0. .... .... = Truncated: Message is not truncated
7 .... ..1 .... .... = Recursion desired: Do query
   recursively
8 .... .... 0.. .... = Z: reserved (0)
9 .... .... ..0 .... = Non-authenticated data: Unacceptable
10 Questions: 1
11 Answer RRs: 0
12 Authority RRs: 0
13 Additional RRs: 0
14 www.mit.edu: type A, class IN
15 Name: www.mit.edu
16 [Name Length: 11]
17 [Label Count: 3]
18 Type: A (Host Address) (1)
19 Class: IN (0x0001)
```

2. DNS响应

```
1 Domain Name System (response)
2 Transaction ID: 0x0006
3 Flags: 0x8180 Standard query response, No error
4 1.... .... .... = Response: Message is a response
5 .000 0.... .... = Opcode: Standard query (0)
6 .... .0. .... .... = Authoritative: Server is not an
   authority for domain
7 .... ..0. .... .... = Truncated: Message is not truncated
8 .... ..1 .... .... = Recursion desired: Do query
   recursively
9 .... .... 1.... .... = Recursion available: Server can do
   recursive queries
10 .... .... 0.. .... = Z: reserved (0)
11 .... .... ..0. .... = Answer authenticated:
   Answer/authority portion was not authenticated by the
   server
12 .... .... ..0 .... = Non-authenticated data: Unacceptable
13 .... .... .... 0000 = Reply code: No error (0)
14 Questions: 1
15 Answer RRs: 3
16 Authority RRs: 0
17 Additional RRs: 0
18 www.mit.edu: type A, class IN
19 Name: www.mit.edu
20 [Name Length: 11]
21 [Label Count: 3]
22 Type: A (Host Address) (1)
23 Class: IN (0x0001)
24 www.mit.edu: type CNAME, class IN, cname
   www.mit.edu.edgekey.net
25 www.mit.edu.edgekey.net: type CNAME, class IN, cname
   e9566.dsrb.akamaiedge.net
```

```
26 e9566.dscb.akamaiedge.net: type A, class IN, addr  
23.57.56.98
```

8. 阅读分组具体内容，对实验问题的回答如下

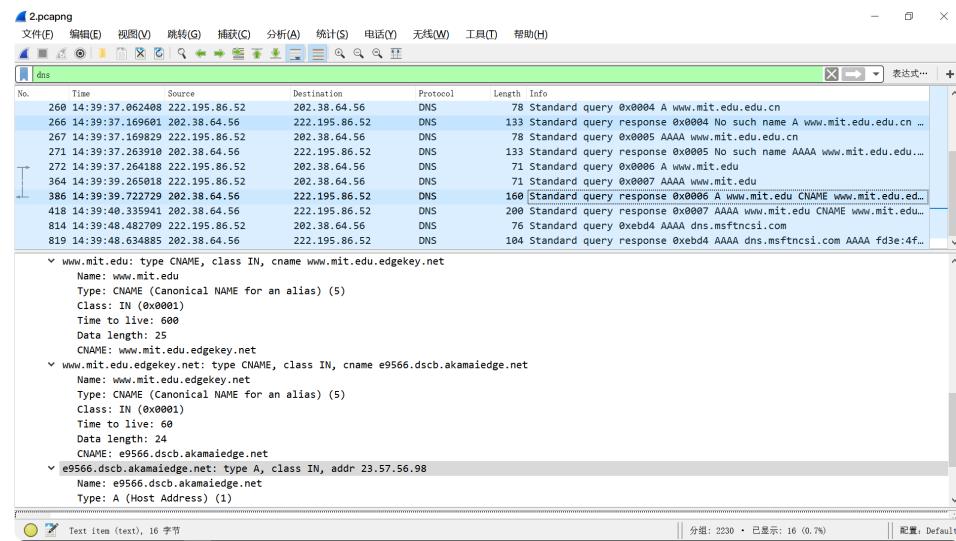
11. DNS查询消息的目标端口和响应消息的源端口均为 53
12. DNS请求送往 202.38.64.56，这是本地的DNS服务器
13. 由内容 Type: A (Host Address) (1) 可知，类别为 A；由内容 Answer RRs: 0 可知，查询消息不包含任何回答
14. 由内容 Answer RRs: 3 可知，响应消息提供了3个回答，分别包括了如下两个主机别名和主机IP地址的信息

```
1 www.mit.edu: type CNAME, class IN, cname  
www.mit.edu.edgekey.net  
2 Name: www.mit.edu  
3 Type: CNAME (Canonical NAME for an alias) (5)  
4 Class: IN (0x0001)  
5 Time to live: 600  
6 Data length: 25  
7 CNAME: www.mit.edu.edgekey.net
```

```
1 www.mit.edu.edgekey.net: type CNAME, class IN, cname  
e9566.dscb.akamaiedge.net  
2 Name: www.mit.edu.edgekey.net  
3 Type: CNAME (Canonical NAME for an alias) (5)  
4 Class: IN (0x0001)  
5 Time to live: 60  
6 Data length: 24  
7 CNAME: e9566.dscb.akamaiedge.net
```

```
1 e9566.dscb.akamaiedge.net: type A, class IN, addr  
23.57.56.98  
2 Name: e9566.dscb.akamaiedge.net  
3 Type: A (Host Address) (1)  
4 Class: IN (0x0001)  
5 Time to live: 20  
6 Data length: 4  
7 Address: 23.57.56.98
```

15. 屏幕截图如下



9. 运行指令

```
1 | nslookup -type=NS mit.edu
```

以确定麻省理工学院(mit.edu)的DNS服务器

```
C:\Users\瞳木水杉>nslookup -type=NS mit.edu
Non-authoritative answer:
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = use5.akam.net
```

10. 捕获如下分组

1. DNS请求

```
1 Domain Name System (query)
2 Transaction ID: 0x0004
3 0... .... .... = Response: Message is a query
4 .000 0... .... .... = Opcode: Standard query (0)
5 .... ..0. .... .... = Truncated: Message is not truncated
6 .... ...1 .... .... = Recursion desired: Do query
recursively
7 .... .... .0.. .... = Z: reserved (0)
8 .... .... ..0 .... = Non-authenticated data: Unacceptable
9 Questions: 1
10 Answer RRs: 0
11 Authority RRs: 0
12 Additional RRs: 0
13 mit.edu: type NS, class IN
14 Name: mit.edu
15 [Name Length: 7]
16 [Label Count: 2]
17 Type: NS (authoritative Name Server) (2)
18 Class: IN (0x0001)
```

2. DNS响应

```
1 Domain Name System (response)
2 Transaction ID: 0x0004
3 1... .... .... .... = Response: Message is a response
4 .000 0... .... .... = Opcode: Standard query (0)
5 .... 0.. .... .... = Authoritative: Server is not an
6 authority for domain
7 .... ..0. .... .... = Truncated: Message is not truncated
8 .... ...1 .... .... = Recursion desired: Do query
9 recursively
10 .... .... 1.... .... = Recursion available: Server can do
11 recursive queries
12 .... .... .0.. .... = Z: reserved (0)
13 .... .... ..0. .... = Answer authenticated:
14 Answer/authority portion was not authenticated by the
15 server
16 .... .... ....0 .... = Non-authenticated data: Unacceptable
17 .... .... .... 0000 = Reply code: No error (0)
18 Questions: 1
19 Answer RRs: 8
20 Authority RRs: 0
21 Additional RRs: 0
22 mit.edu: type NS, class IN
23 Name: mit.edu
24 [Name Length: 7]
25 [Label Count: 2]
26 Type: NS (authoritative Name Server) (2)
27 Class: IN (0x0001)
28 mit.edu: type NS, class IN, ns eur5.akam.net
29 mit.edu: type NS, class IN, ns ns1-37.akam.net
30 mit.edu: type NS, class IN, ns asia1.akam.net
31 mit.edu: type NS, class IN, ns usw2.akam.net
32 mit.edu: type NS, class IN, ns use2.akam.net
33 mit.edu: type NS, class IN, ns asia2.akam.net
34 mit.edu: type NS, class IN, ns ns1-173.akam.net
35 mit.edu: type NS, class IN, ns use5.akam.net
36 Name: mit.edu
37 Type: NS (authoritative Name Server) (2)
38 Class: IN (0x0001)
39 Time to live: 450
40 Data length: 7
41 Name Server: use5.akam.net
```

11. 阅读分组具体内容，对实验问题的回答如下

16. DNS请求送往 202.38.64.56，这是本地的DNS服务器

17. 由内容 Type: NS (authoritative Name Server) (2) 可知，类别为
NS；由内容 Answer RRs: 0 可知，查询消息不包含任何回答

18. 由内容 Answer RRs: 8 可知，响应消息提供了8个回答，分别包含了如
下内容

```
1 | mit.edu: type NS, class IN, ns eur5.akam.net
2 | Name: mit.edu
3 | Type: NS (authoritative Name Server) (2)
4 | Class: IN (0x0001)
5 | Time to live: 450
6 | Data length: 15
7 | Name Server: eur5.akam.net
```

```
1 | mit.edu: type NS, class IN, ns ns1-37.akam.net
2 | Name: mit.edu
3 | Type: NS (authoritative Name Server) (2)
4 | Class: IN (0x0001)
5 | Time to live: 450
6 | Data length: 9
7 | Name Server: ns1-37.akam.net
```

```
1 | mit.edu: type NS, class IN, ns asia1.akam.net
2 | Name: mit.edu
3 | Type: NS (authoritative Name Server) (2)
4 | Class: IN (0x0001)
5 | Time to live: 450
6 | Data length: 8
7 | Name Server: asia1.akam.net
```

```
1 | mit.edu: type NS, class IN, ns usw2.akam.net
2 | Name: mit.edu
3 | Type: NS (authoritative Name Server) (2)
4 | Class: IN (0x0001)
5 | Time to live: 450
6 | Data length: 7
7 | Name Server: usw2.akam.net
```

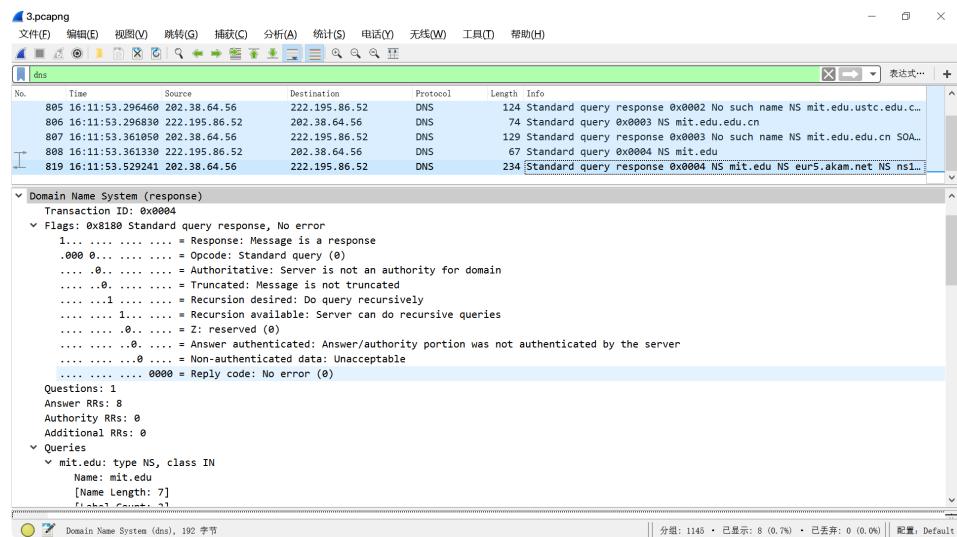
```
1 | mit.edu: type NS, class IN, ns use2.akam.net
2 | Name: mit.edu
3 | Type: NS (authoritative Name Server) (2)
4 | Class: IN (0x0001)
5 | Time to live: 450
6 | Data length: 7
7 | Name Server: use2.akam.net
```

```
1 | mit.edu: type NS, class IN, ns asia2.akam.net
2 | Name: mit.edu
3 | Type: NS (authoritative Name Server) (2)
4 | Class: IN (0x0001)
5 | Time to live: 450
6 | Data length: 8
7 | Name Server: asia2.akam.net
```

```
1 | mit.edu: type NS, class IN, ns ns1-173.akam.net
2 | Name: mit.edu
3 | Type: NS (authoritative Name Server) (2)
4 | Class: IN (0x0001)
5 | Time to live: 450
6 | Data length: 10
7 | Name Server: ns1-173.akam.net
```

```
1 | mit.edu: type NS, class IN, ns use5.akam.net
2 | Name: mit.edu
3 | Type: NS (authoritative Name Server) (2)
4 | Class: IN (0x0001)
5 | Time to live: 450
6 | Data length: 7
7 | Name Server: use5.akam.net
```

19. 屏幕截图如下



5. 运行指令

```
1 | nslookup www.aiit.or.kr ns.nju.edu.cn
```

向南京大学DNS服务器(ns.nju.edu.cn)请求解析韩国AIIT机构(www.aiit.or.kr)的IP地址



向麻省理工学院的请求会不被接受而超时

```
C:\Users\瞳木水杉>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server: Unknown
Address: 18.0.72.3

        nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
*** Request to Unknown timed-out
```

“

6. 捕获分组：参见第23题答案截图

7. 阅读分组具体内容，对实验问题的回答如下

20. 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

202.38.64.17，查询到**ns.nju.edu.cn**的IP地址：**202.119.32.12**，之后向这个IP地址发送查询消息

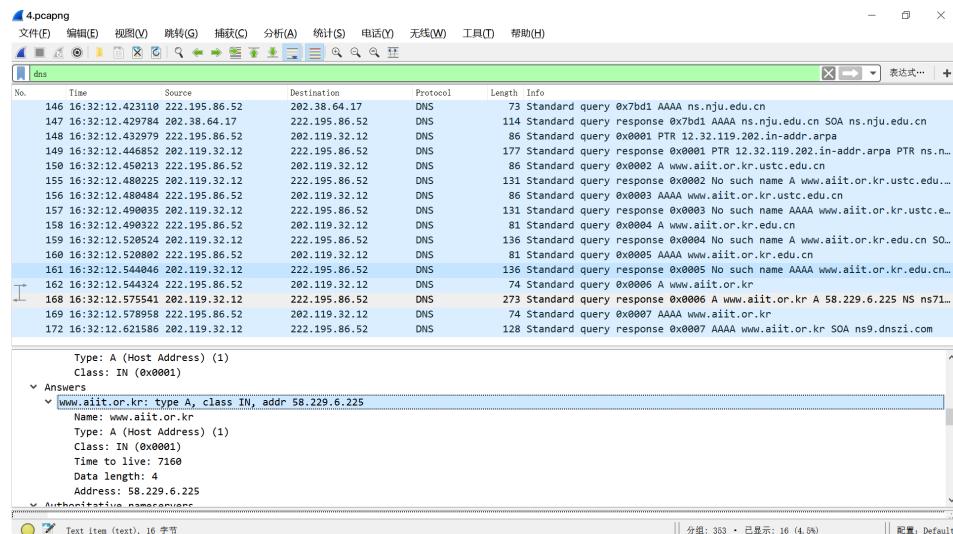
21. 由内容 **Type: A (Host Address) (1)** 和 **Type: AAAA (IPv6 Address)**

(28) 可知，类别为 **A** 或 **AAAA**；由内容 **Answer RRs: 0** 可知，查询消息不包含任何回答

22. 由内容 **Answer RRs: 1** 可知，响应消息提供了1个回答，包括了如下主机别名和主机地址的信息

```
1 | www.aiit.or.kr: type A, class IN, addr 58.229.6.225
2 | Name: www.aiit.or.kr
3 | Type: A (Host Address) (1)
4 | Class: IN (0x0001)
5 | Time to live: 7160
6 | Data length: 4
7 | Address: 58.229.6.225
```

23. 屏幕截图如下



实验总结

本次实验主要研究了DNS协议，通过学习nslookup与ipconfig等命令工具，结合Wireshark捕获并分析DNS请求响应的具体内容，深入理解了DNS功能的具体实现以及消息特征，为之后向下学习网络结构提供了知识背景和基础。

附

本报告中出现的捕获分组文件以及相关截图可见[GitHub@lyc0930](#)