

实验三

Wireshark Lab: DNS

阅读实验文档并进行操作。

1. nslookup

阅读文档，熟悉nslookup的各个操作，并以此完成1，2，3题

1. 用nslookup访问科大的web，IP地址为202.38.64.246

```
C:\Users\P>nslookup www.ustc.edu.cn
服务器:  mx.ustc.edu.cn
Address:  202.38.64.56

名称:     www.ustc.edu.cn
Addresses: 2001:da8:d800:642::246
          202.38.64.246

C:\Users\P>
```

2. 用nslookup确定一个欧洲大学的权威服务器

```
C:\Users\P>nslookup -type=NS ox.ac.uk
服务器:  mx.ustc.edu.cn
Address:  202.38.64.56

非权威应答:
ox.ac.uk      nameserver = auth5.dns.ox.ac.uk
ox.ac.uk      nameserver = dns2.ox.ac.uk
ox.ac.uk      nameserver = dns1.ox.ac.uk
ox.ac.uk      nameserver = auth4.dns.ox.ac.uk
ox.ac.uk      nameserver = ns2.ja.net
ox.ac.uk      nameserver = auth6.dns.ox.ac.uk
ox.ac.uk      nameserver = dns0.ox.ac.uk
```

3. 利用2的一个DNS服务器查询Yahoo邮箱的邮件服务器，尝试了一下上面的DNS都不行，似乎是被墙了，但是尝试使用科大的DNS成功查询

```
C:\Users\P>nslookup mail.yahoo.com auth5.dns.ox.ac.uk
服务器: ns2.mythic-beasts.com
Address: 93.93.128.67

*** ns2.mythic-beasts.com 找不到 mail.yahoo.com: Query refused

C:\Users\P>nslookup mail.yahoo.com dns0.ox.ac.uk
DNS request timed out.
    timeout was 2 seconds.
服务器: UnKnown
Address: 129.67.1.190

*** UnKnown 找不到 mail.yahoo.com: Query refused

C:\Users\P>
```

```
C:\Users\P>nslookup mail.yahoo.com ns.ustc.edu.cn
服务器: ns.ustc.edu.cn
Address: 202.38.64.1

非权威应答:
名称: edge.gycpi.b.yahoodns.net
Addresses: 2001:4998:18:800::4003
           2001:4998:18:800::4002
           69.147.88.7
           69.147.88.8
Aliases: mail.yahoo.com

C:\Users\P>_
```

2. ipconfig

阅读实验文档，熟悉ipconfig

```
C:\Users\P>ipconfig/all

Windows IP 配置

   主机名 . . . . . : DESKTOP-CX
   主 DNS 后缀 . . . . . :
   节点类型 . . . . . : 混合
   IP 路由已启用 . . . . . : 否
   WINS 代理已启用 . . . . . : 否
   DNS 后缀搜索列表 . . . . . : ustc.edu.cn

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 . . . . . : ustc.edu.cn
   描述. . . . . : Realtek PCIe FE Family Controller
   物理地址. . . . . : E4-54-E8-00-9B-5D
   DHCP 已启用 . . . . . : 是
   自动配置已启用. . . . . : 是

以太网适配器 以太网 2:

   连接特定的 DNS 后缀 . . . . . : ustc.edu.cn
   描述. . . . . : ASIX AX88179 USB 3.0 to Gigabit Ethernet Adapter
   物理地址. . . . . : F8-E4-3B-4B-E9-B8
   DHCP 已启用 . . . . . : 是
   自动配置已启用. . . . . : 是
   IPv6 地址 . . . . . : 2001:da8:d800:523:25a6:ff11:7b52:98a1(首选)
   临时 IPv6 地址. . . . . : 2001:da8:d800:523:60fa:a356:6e08:7361(首选)
   本地链接 IPv6 地址. . . . . : fe80::25a6:ff11:7b52:98a1%3(首选)
   IPv4 地址 . . . . . : 114.214.232.254(首选)
   子网掩码 . . . . . : 255.255.252.0
   获得租约的时间 . . . . . : 2021年9月24日 11:54:50
   租约过期的时间 . . . . . : 2021年9月24日 17:25:58
   默认网关 . . . . . : 114.214.235.254
   DHCP 服务器 . . . . . : 202.38.64.17
   DHCPv6 IAID . . . . . : 905503803
   DHCPv6 客户端 DUID . . . . . : 00-01-00-01-28-C7-2C-42-E4-54-E8-00-9B-5D
   DNS 服务器 . . . . . : 202.38.64.56
                           202.38.64.17
   TCPIP 上的 NetBIOS . . . . . : 已启用
```

3. Tracing DNS with Wireshark

按照操作清除缓存，打开Wireshark进行捕获，捕获后的结果有点多，干扰较大，回答问题。

No.	Time	Source	Destination	Protocol	Length	Info
4.	39	16:51:44.993606	114.214.232.254	DNS	72	Standard query 0xa873 A www.ietf.org
	40	16:51:45.020858	114.214.232.254	DNS	72	Standard query 0xa873 A www.ietf.org
	51	16:51:45.476089	202.38.64.17	DNS	149	Standard query response 0xa873 A www.ietf.org CNAME www.ietf.org..
	54	16:51:45.485071	114.214.232.254	DNS	89	Standard query 0x7751 A nav.smartscreen.microsoft.com
	55	16:51:45.485264	114.214.232.254	DNS	89	Standard query 0x6291 AAAA nav.smartscreen.microsoft.com
	56	16:51:45.486208	202.38.64.56	DNS	223	Standard query response 0x7751 A nav.smartscreen.microsoft.com C..
	57	16:51:45.486267	202.38.64.56	DNS	283	Standard query response 0x6291 AAAA nav.smartscreen.microsoft.co..
	90	16:51:45.822078	114.214.232.254	DNS	90	Standard query 0x6345 A smartscreen-prod.microsoft.com

```
Frame Number: 39
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]
Ethernet II, Src: ASIXElec 4b:e9:b8 (f8:e4:3b:4b:e9:b8), Dst: Hanzhou 91:72:e2 (5c:dd:70:91:72:e2)
```

根据捕获内容，是使用UDP发送

5.	>	User Datagram Protocol, Src Port: 49152, Dst Port: 53
		Internet Protocol Version 4, Src: 202.38.64.56, Dst: 114.214.232.254
		User Datagram Protocol, Src Port: 53, Dst Port: 49152

都是53端口

6. 查询消息发送到202.38.64.56

```
DHCPv6 客户端 DUID . . . . . : 00-01-00-01-28-C7-2C-42-E4-54-E8-00-9B-5D
DNS 服务器 . . . . . : 202.38.64.56
                           202.38.64.17
TCPIP 上的 NetBIOS . . . . . : 已启用
```

正是本地DNS服务器地址

7. type是A, Answer RRs: 0, 查询消息不包含任何answer

8.

✓ Query 153

✓ 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

[Request In: 39]

回复3条，回复是类型，主机别名，以及两个ip地址

9.

No.	Time	Source	Destination	Protocol	Length	Info
52	16:51:45.476940	114.214.232.254	104.16.44.99	TCP	66	14627 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
53	16:51:45.477615	114.214.232.254	104.16.44.99	TCP	66	8993 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
59	16:51:45.517498	114.214.232.254	104.16.44.99	TCP	66	1850 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
72	16:51:45.645952	114.214.232.254	104.16.44.99	TCP	54	14627 → 80 [ACK] Seq=1 Ack=1 Win=263168 Len=0
74	16:51:45.646120	114.214.232.254	104.16.44.99	TCP	54	8993 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
75	16:51:45.646604	114.214.232.254	104.16.44.99	HTTP	530	GET / HTTP/1.1
77	16:51:45.685970	114.214.232.254	104.16.44.99	TCP	54	1850 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
96	16:51:45.832266	114.214.232.254	104.16.44.99	TCP	66	13150 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

> Frame 52: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{1536386D-6982-4F84-9A37-9CF9F936F7CD}, id 0

是对应的

10. 并没有，本地的DNS已经缓存了，不需要再查询了

使用nslookup，查询www.mit.edu，回答问题

11.

13	17:27:45.696870	114.214.232.254	202.38.64.56	DNS	85	Standard query 0x0001 PTR 56.64.38.202.in-addr.arpa
14	17:27:45.697646	202.38.64.56	114.214.232.254	DNS	138	Standard query response 0x0001 PTR 56.64.38.202.in-addr.arpa
15	17:27:45.701331	114.214.232.254	202.38.64.56	DNS	71	Standard query 0x0002 A www.mit.edu
16	17:27:45.702251	202.38.64.56	114.214.232.254	DNS	163	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu
17	17:27:45.705745	114.214.232.254	202.38.64.56	DNS	71	Standard query 0x0003 AAAA www.mit.edu
18	17:27:45.706788	202.38.64.56	114.214.232.254	DNS	203	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu

> Frame 15: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{1536386D-6982-4F84-9A37-9CF9F936F7CD}, id 0
> Ethernet II, Src: ASIXElec_4b:e9:b8 (f8:e4:3b:4b:e9:b8), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)
> Internet Protocol Version 4, Src: 114.214.232.254, Dst: 202.38.64.56
> User Datagram Protocol, Src Port: 50486, Dst Port: 53
> Domain Name System (query)
Transaction ID: 0x0002
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0

14	17:27:45.697646	202.38.64.56	114.214.232.254	DNS	138	Standard query response 0x0001 PTR 56.64.38.202.in-addr.arpa
15	17:27:45.701331	114.214.232.254	202.38.64.56	DNS	71	Standard query 0x0002 A www.mit.edu
16	17:27:45.702251	202.38.64.56	114.214.232.254	DNS	163	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu
17	17:27:45.705745	114.214.232.254	202.38.64.56	DNS	71	Standard query 0x0003 AAAA www.mit.edu
18	17:27:45.706788	202.38.64.56	114.214.232.254	DNS	203	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu

> Frame 16: 163 bytes on wire (1304 bits), 163 bytes captured (1304 bits) on interface \Device\NPF_{1536386D-6982-4F84-9A37-9CF9F936F7CD}, id 0
> Ethernet II, Src: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2), Dst: ASIXElec_4b:e9:b8 (f8:e4:3b:4b:e9:b8)
> Internet Protocol Version 4, Src: 202.38.64.56, Dst: 114.214.232.254
> User Datagram Protocol, Src Port: 53, Dst Port: 50486
> Domain Name System (response)
Transaction ID: 0x0002
> Flags: 0x8180 Standard query response, No error
Questions: 1

都是53端口

12.

14	17:27:45.697646	202.38.64.56	114.214.232.254	DNS	138	Standard query response 0x0001 PTR 56.64.38.202.in-addr.arpa PTR mx1
15	17:27:45.701331	114.214.232.254	202.38.64.56	DNS	71	Standard query 0x0002 A www.mit.edu
16	17:27:45.702251	202.38.64.56	114.214.232.254	DNS	163	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey
17	17:27:45.705745	114.214.232.254	202.38.64.56	DNS	71	Standard query 0x0003 AAAA www.mit.edu
18	17:27:45.706788	202.38.64.56	114.214.232.254	DNS	203	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey

Time to Live: 128
Protocol: UDP (17)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 114.214.232.254
Destination Address: 202.38.64.56
> User Datagram Protocol, Src Port: 50486, Dst Port: 53

IP地址202.38.64.56，是本地DNS地址

13. type为A，查询信息没有任何answer

14. > 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 104.106.56.136

[Request In: 15]

[Time: 0.000000000 seconds]

3个回复，包含两个主机别名和一个IP地址

15.

Time	Source	Destination	Protocol	Length	Info
13	17:27:45.696870	114.214.232.254	202.38.64.56	DNS	85 Standard query 0x0001 PTR 56.64.38.202.in-addr.arpa
14	17:27:45.697646	202.38.64.56	114.214.232.254	DNS	138 Standard query response 0x0001 PTR 56.64.38.202.in-addr.arpa PTR mx.us...
15	17:27:45.701331	114.214.232.254	202.38.64.56	DNS	71 Standard query 0x0002 A www.mit.edu
16	17:27:45.702251	202.38.64.56	114.214.232.254	DNS	163 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey...
17	17:27:45.705745	114.214.232.254	202.38.64.56	DNS	71 Standard query 0x0003 AAAA www.mit.edu
18	17:27:45.706788	202.38.64.56	114.214.232.254	DNS	203 Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey...

Destination Address: 202.38.64.56	
> User Datagram Protocol, Src Port: 50486, 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	

0000	5c dd 70 91 72 e2 f8 e4 3b 4b e9 b8 08 00 45 00	\p r . . . ; K . . . E .
0010	00 39 cc cf 00 00 00 11 00 00 72 d6 e8 fe ca 26	. 9 ; p &
0020	40 38 c5 36 00 00 00 05 66 6a 0a 07 01 00 00 01	@ R . 6 . 5 . % f i

更改指令重复实验，回答问题

16. IP地址202.38.64.56，是本地服务器DNS地址
17. type是NS，Answer RRs: 0，没有任何answer
18. 域名服务器

Answers	
>	mit.edu: type NS, class IN, ns ns1-37.akam.net
>	mit.edu: type NS, class IN, ns asia1.akam.net
>	mit.edu: type NS, class IN, ns eur5.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 use2.akam.net
>	mit.edu: type NS, class IN, ns use5.akam.net
>	mit.edu: type NS, class IN, ns ns1-173.akam.net
[Request In: 76]	

0010	00 dc 23 cc 00 00 3e 11 f2 11 ca 26 40 38 72 d6	. . # . . . > . . . & @ 8 r .
------	---	-------------------------------

没有提供IP地址

19.

75	17:39:05.125969	202.38.64.56	114.214.232.254	DNS	138 Standard query response 0x0001 PTR 56.64.38.202.in-addr.arpa PTR mx.us...
76	17:39:05.127027	114.214.232.254	202.38.64.56	DNS	67 Standard query 0x0002 NS mit.edu
78	17:39:05.193089	202.38.64.56	114.214.232.254	DNS	234 Standard query response 0x0002 NS mit.edu NS ns1-37.akam.net NS asia1...

Destination Address: 114.214.232.254	
> User Datagram Protocol, Src Port: 53, Dst Port: 60473	
Domain Name System (response)	
Transaction ID: 0x0002	
> Flags: 0x8180 Standard query response, No error	
Questions: 1	
Answer RRs: 8	
Authority RRs: 0	
Additional RRs: 0	
> Queries	

0030	00 00 00 00 00 00 03 6d 69 74 03 65 64 75 00 00 m i t . e d u .
0040	02 00 01 c0 0c 00 02 00 01 00 00 01 63 00 11 06 c .
0050	6e 73 31 2d 33 37 04 61 6b 61 6d 03 6e 65 74 00	n s 1 - 3 7 - a k a m . n e t .
0060	c0 0c 00 02 00 01 00 00 01 63 00 08 05 61 73 69 c . n s i a 1 .

更改指令后重复操作，回答问题

20. 地址是18.0.72.3，不是本地默认DNS服务器地址，这是mit的bitsy.mit.edu的IP地址
21. type是A，Answer RRs: 0，没有回复
22. DNS查询失败，从23的截图中看出wireshark中并没有回复，所以answer应该是0

```

S C:\Users\P>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
- t 服务器: UnKnown
Address: 18.0.72.3

u DNS request timed out.
    timeout was 2 seconds.
e DNS request timed out.
    timeout was 2 seconds.
JS DNS request timed out.
JS    timeout was 2 seconds.
co DNS request timed out.
    timeout was 2 seconds.
JS*** 请求 UnKnown 超时
JS

```

23.

16	17:54:24.664518	202.38.64.56	114.214.232.254	DNS	138 Standard query response 0xc/r9 AAAA bitsy.mit.edu SOA use2.
19	17:54:24.666689	114.214.232.254	18.0.72.3	DNS	82 Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
49	17:54:26.678450	114.214.232.254	18.0.72.3	DNS	74 Standard query 0x0002 A www.aiit.or.kr
71	17:54:28.690001	114.214.232.254	18.0.72.3	DNS	74 Standard query 0x0003 AAAA www.aiit.or.kr
114	17:54:30.707738	114.214.232.254	18.0.72.3	DNS	74 Standard query 0x0004 A www.aiit.or.kr
484	17:54:32.719810	114.214.232.254	18.0.72.3	DNS	74 Standard query 0x0005 AAAA www.aiit.or.kr

Destination Address: 18.0.72.3	
> User Datagram Protocol, Src Port: 65150, Dst Port: 53	
v Domain Name System (query)	
Transaction ID: 0x0002	
> Flags: 0x0100 Standard query	
Questions: 1	
Answer RRs: 0	
Authority RRs: 0	
Additional RRs: 0	
> Queries	

0000	5c dd 70 91 72 e2 f8 e4 3b 4b e9 b8 08 00 45 00	\-p-r-;K-;E-
0010	00 3c 74 53 00 00 00 11 00 00 72 d6 e8 fe 12 00	-<S- -p-
0020	48 03 fe 7e 00 35 00 28 b6 11 00 02 01 00 00 01	H-~5:(- - - -
0030	00 00 00 00 00 00 03 77 77 77 04 61 69 69 74 02WW-aiit-
0040	6f 72 02 6b 72 00 00 01 00 01	or-kr- - -