

计算机网络第三次实验实验报告

舒文炫

2021 年 9 月 30 日

目录

1	实验内容	2
2	实验过程	3
2.1	nslookup	3
2.1.1	过程截图	3
2.1.2	小节思考题	4
2.2	ipconfig	5
2.2.1	过程截图	5
2.3	Tracing DNS with Wireshark	7
2.3.1	第一部分	7
2.3.2	第二部分	10
2.3.3	第三部分	11
2.3.4	第四部分	14
3	实验总结	17

Chapter 1

实验内容

本次实验主要学习 DNS 有关内容，具体的方面如下：

- 使用 nslookup 工具，去查询一些 DNS 服务器的 DNS 记录
- 使用 ipconfig 命令，查看网络的一些设置
- 使用 wireshark 工具对 nslookup 命令执行过程进行抓包观察

下面我们逐一进行。

Chapter 2

实验过程

2.1 nslookup

这一小节学习 nslookup 命令的简单使用，以及其参数的含义。

2.1.1 过程截图

首先，我们打开命令行界面，输入 nslookup 回车，得到了本地服务器的 ip 地址和名称，截图如下：

```
C:\Users\SWX>nslookup
默认服务器: UnKnown
Address: 192.168.43.1
```

exit 退出进入的 nslookup 模式，然后我们输入命令 nslookup www.mit.edu，头两行是我本地的名称和 ip 地址，后面是所查询的 www.mit.edu 的主机的 ip 地址和名称，截图如下：

```
C:\Users\SWX>nslookup www.mit.edu
服务器: UnKnown
Address: 192.168.43.1

非权威应答:
名称: e9566.dscb.akamaiedge.net
Addresses: 2600:1406:e800:38a::255e
           2600:1406:e800:382::255e
           23.209.245.115
Aliases: www.MIT.edu
         www.mit.edu.edgekey.net
```

然后我们输入命令 nslookup -type=NS mit.edu。这里指定了查询的类型为 NS，也就是 mit.edu 域下的权威 DNS 服务器，返回的结果列出了很多条，前面的名字后面是 ip 地址，结果截图如下：

```
C:\Users\SWX>nslookup -type=NS mit.edu
服务器: UnKnown
Address: 192.168.43.1

非权威应答:
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = asia2.akam.net

ns1-173.akam.net      AAAA IPv6 address = 2600:1401:2::ad
use2.akam.net        internet address = 96.7.49.64
usw2.akam.net        internet address = 184.26.161.64
asia2.akam.net        internet address = 95.101.36.64
eur5.akam.net         internet address = 23.74.25.64
ns1-173.akam.net      internet address = 193.108.91.173
```

然后我们输入命令 nslookup www.aiit.or.kr bitsy.mit.edu，这条命令是说，我们将查询请求发送到 bitsy.mit.edu 服务器，而不是我们本地默认的服务器，让 bitsy.mit.edu 提供主机 www.aiit.or.kr 的地址，不过很可惜，这里超时了，前面的两行应该是 bitsy.mit.edu 服务器的地址，结果截图如下：

```

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

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** 请求 UnKnown 超时

```

2.1.2 小节思考题

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

这里我查询了 bilibili.com，这就是我们熟知的 b 站，的 ip 地址，截图如下

```

C:\Users\SWX>nslookup bilibili.com
服务器: UnKnown
Address: 192.168.43.1

非权威应答:
名称: bilibili.com
Addresses: 110.43.34.66
           119.3.238.64
           139.159.241.37
           119.3.70.188
           120.92.78.97
           120.92.174.135

```

这里返回了很多的 ip 地址，如 110.43.34.66，119.3.238.64，因为 b 站的用户量很大，只用一个服务器可能负担不够，从而设置了一个服务器群，所以会有这么多 ip 地址。

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

这里我查找了巴黎高师的权威 DNS 服务器，下面是返回结果的截图：

```

C:\Users\SWX>nslookup -type=NS ens.ps1.eu
服务器: UnKnown
Address: 192.168.43.1

非权威应答:
ens.ps1.eu      nameserver = panoramix.rap.prd.fr
ens.ps1.eu      nameserver = ns.ens.fr

panoramix.rap.prd.fr  internet address = 193.50.20.1
ns.ens.fr           internet address = 129.199.96.11
panoramix.rap.prd.fr  AAAA IPv6 address = 2001:660:2401:1102::53

```

这里返回了两个 panoramix.rap.prd.fr 和 ns.ens.fr 后面返回了这两个名称对应服务器的 ip 地址，其中 panoramix.rap.prd.fr 有两个，一个是 ip 地址，另一个是 ipv6 的地址。

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?

这里我尝试了使用我第二题找到的两个 DNS 服务器，可是失败了，不知道为什么 qwq，下面是截图：

```
C:\Users\SWX>nslookup -type=MX login.yahoo.com ns.ens.fr
服务器: ns.ens.fr
Address: 129.199.96.11

*** ns.ens.fr 找不到 login.yahoo.com: Query refused
```

```
C:\Users\SWX>nslookup -type=MX login.yahoo.com panoramix.rap.prd.fr
服务器: panoramix.rap.prd.fr
Address: 2001:660:2401:1102::53

*** panoramix.rap.prd.fr 找不到 login.yahoo.com: Query refused
```

所以我就直接去用本地的 DNS 去访问了，这次成功了，下面是截图：

```
C:\Users\SWX>nslookup -type=MX login.yahoo.com
服务器: UnKnown
Address: 192.168.43.1

非权威应答:
login.yahoo.com canonical name = ds-ats.member.g02.yahoodns.net

g02.yahoodns.net
    primary name server = yf1.yahoo.com
    responsible mail addr = hostmaster.yahoo-inc.com
    serial = 1632486346
    refresh = 30 (30 secs)
    retry = 30 (30 secs)
    expire = 86400 (1 day)
    default TTL = 300 (5 mins)

C:\Users\SWX>nslookup ds-ats.member.g02.yahoodns.net
服务器: UnKnown
Address: 192.168.43.1

非权威应答:
名称: ds-ats.member.g02.yahoodns.net
Addresses: 2001:4998:c:900e::2000
           74.6.160.138
```

这里我先用 nslookup -type=MX login.yahoo.com 查到了 yahoo 邮件服务器的规范主机名，然后再查这个主机名对应的 ip，结果就是 yahoo 邮箱的 ip 地址为，74.6.160.138。

2.2 ipconfig

这一小节学习 ipconfig 命令的简单使用

2.2.1 过程截图

首先输入命令 ipconfig

all 这个命令查看 IP 的主机信息，DNS 信息，物理地址信息，DHCP 服务器信息等，截图如下，因为内容比较多，我只截出了比较重要的部分

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

Windows IP 配置

   主机名 . . . . . : DESKTOP-I3UFLAL
   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. . . . . : 98-28-A6-1C-59-55
   DHCP 已启用 . . . . . : 是
   自动配置已启用. . . . . : 是

无线局域网适配器 本地连接* 1:

   媒体状态 . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . :
   描述 . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   物理地址. . . . . : 32-D1-6B-97-9F-C5
   DHCP 已启用 . . . . . : 是
   自动配置已启用. . . . . : 是
```

```
无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . :
   描述 . . . . . : Qualcomm Atheros QCA9377 Wireless Network Adapter
   物理地址. . . . . : 30-D1-6B-97-9F-C5
   DHCP 已启用 . . . . . : 是
   自动配置已启用. . . . . : 是
   IPv6 地址 . . . . . : 240e:45a:407:40b9:5d6e:1d80:b232:21a6(首选)
   临时 IPv6 地址 . . . . . : 240e:45a:407:40b9:2d8b:8e4e:e3c9:38(首选)
   本地链接 IPv6 地址. . . . . : fe80::5d6e:1d80:b232:21a6%17(首选)
   IPv4 地址 . . . . . : 192.168.43.193(首选)
   子网掩码 . . . . . : 255.255.255.0
   获得租约的时间 . . . . . : 2021年9月24日 18:59:49
   租约过期的时间 . . . . . : 2021年9月24日 21:12:49
   默认网关 . . . . . : fe80::819:7aff:fe5a:984f%17
   . . . . . : 192.168.43.1
   DHCP 服务器 . . . . . : 192.168.43.1
   DHCPv6 IAID . . . . . : 238080363
   DHCPv6 客户端 DUID . . . . . : 00-01-00-01-26-52-B2-82-98-28-A6-1C-59-55
   DNS 服务器 . . . . . : 192.168.43.1
   . . . . . : 240e:45a:407:40b9:53
   TCP/IP 上的 NetBIOS . . . . . : 已启用
```

然后是命令 `ipconfig /displaydns`，这个命令可以列出主机上缓存的 DNS 记录。记录很多，只截出一部分，截图如下

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

Windows IP 配置

   mirror3.internetdownloadmanager.com
   -----
   记录名称 . . . . . : mirror3.internetdownloadmanager.com
   记录类型 . . . . . : 1
   生存时间 . . . . . : 5703
   数据长度 . . . . . : 4
   部分 . . . . . : 答案
   A (主机)记录 . . . . . : 174.127.113.77

   记录名称 . . . . . : ns1.tonec.com
   记录类型 . . . . . : 1
   生存时间 . . . . . : 5703
   数据长度 . . . . . : 4
   部分 . . . . . : 其他
   A (主机)记录 . . . . . : 159.69.68.58

   记录名称 . . . . . : ns2.tonec.com
   记录类型 . . . . . : 1
   生存时间 . . . . . : 5703
   数据长度 . . . . . : 4
   部分 . . . . . : 其他
   A (主机)记录 . . . . . : 185.80.220.22
```

最后是命令 `ipconfig /flushdns`，这个可以清空缓存，命令执行完后截图如下

```
C:\Users\SWX>ipconfig /flushdns

Windows IP 配置

已成功刷新 DNS 解析缓存。
```

这一小节没有思考题。

2.3 Tracing DNS with Wireshark

这一小节开始使用 wireshark 工具捕捉 DNS 包

2.3.1 第一部分

过程截图

这里我们先用 ipconfig /flushdns, 清空缓存, 打开浏览器, 清空浏览器缓存, 设置 wireshark 过滤器为 ip_addr=192.168.43.1 这个是我的 ip 地址。启动捕获, 浏览器输入网址 <http://www.ietf.org>, 然后停止捕获, 下面是 wireshark 包列表的截图

No.	Time	Source	Destination	Protocol	Length	Info
166	2021-09-24 20:36:26.596705	192.168.43.193	192.168.43.1	DNS	80	Standard query 0x0ae5 A beacons.gcp.gvt2.com
167	2021-09-24 20:36:26.596892	192.168.43.193	192.168.43.1	DNS	80	Standard query 0x5a86 AAAA beacons.gcp.gvt2.com
168	2021-09-24 20:36:26.623716	192.168.43.1	192.168.43.193	DNS	381	Standard query response 0x0ae5 A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com
170	2021-09-24 20:36:26.647848	192.168.43.1	192.168.43.193	DNS	167	Standard query response 0x5a86 AAAA beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com
212	2021-09-24 20:36:27.381111	192.168.43.193	192.168.43.1	DNS	72	Standard query 0x28b3 A www.ietf.org
213	2021-09-24 20:36:27.381594	192.168.43.193	192.168.43.1	DNS	72	Standard query 0xe7c3 AAAA www.ietf.org
214	2021-09-24 20:36:27.403096	192.168.43.1	192.168.43.193	DNS	399	Standard query response 0x28b3 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net
215	2021-09-24 20:36:27.403686	192.168.43.1	192.168.43.193	DNS	467	Standard query response 0xe7c3 AAAA www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net
443	2021-09-24 20:36:28.984248	192.168.43.193	192.168.43.1	DNS	78	Standard query 0x7c45 A analytics.ietf.org
447	2021-09-24 20:36:28.984458	192.168.43.193	192.168.43.1	DNS	78	Standard query 0x1c05 AAAA analytics.ietf.org
648	2021-09-24 20:36:29.293286	192.168.43.1	192.168.43.193	DNS	455	Standard query response 0x1c05 AAAA analytics.ietf.org AAAA 2001:1900:3001:11::1
664	2021-09-24 20:36:29.405917	192.168.43.1	192.168.43.193	DNS	399	Standard query response 0x7c45 A analytics.ietf.org A 4.31.198.45 NS ns1.ams1..
1416	2021-09-24 20:36:37.835254	192.168.43.193	192.168.43.1	DNS	78	Standard query 0x1e69 AAAA www.googleapis.com
1417	2021-09-24 20:36:37.861423	192.168.43.1	192.168.43.193	DNS	135	Standard query response 0x1e69 AAAA www.googleapis.com SOA ns1.google.com

我把需要的内容打印成了 pdf, 下面截出思考题需要的部分这是其中一个 query 报文:

```
No.      Time              Source            Destination      Protocol Length  Info
212 2021-09-24 20:36:27.381111 192.168.43.193 192.168.43.1    DNS           72      Standard query
0x28b3 A www.ietf.org
Frame 212: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface
\Device\NPF_{D7A10DBD-93D5-4F5B-95D5-A4C7F7828D05}, id 0
Ethernet II, Src: LiteonTe_97:9f:c5 (30:d1:6b:97:9f:c5), Dst: 0a:19:7a:5a:98:4f (0a:19:7a:5a:98:4f)
Internet Protocol Version 4, Src: 192.168.43.193, Dst: 192.168.43.1
User Datagram Protocol, Src Port: 57918, Dst Port: 53
Domain Name System (query)
  Transaction ID: 0x28b3
  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)
```

这是其中一个 response 报文:

No.	Time	Source	Destination	Protocol	Length	Info
214	2021-09-24 20:36:27.403096	192.168.43.1	192.168.43.193	DNS	399	Standard query response 0x28b3 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99 NS ns1.cloudflare.net NS ns2.cloudflare.net NS ns3.cloudflare.net NS ns4.cloudflare.net NS ns5.cloudflare.net AAAA 2400:cb00:2049:1::adf5:3b1f AAAA 2400:cb00:2049:1::c629:de83 AAAA 2400:cb00:2049:1::c629:de1f AAAA 2400:cb00:2049:1::c629:df1f A 173.245.59.31 A 198.41.222.131 A 198.41.222.31

```

Frame 214: 399 bytes on wire (3192 bits), 399 bytes captured (3192 bits) on interface
\Device\NPF_{D7A100BD-93D5-4F5B-95D5-A4C7F7828D05}, id 0
Ethernet II, Src: 0a:19:7a:5a:98:4f (0a:19:7a:5a:98:4f), Dst: LiteonTe_97:9f:c5 (30:d1:6b:97:9f:c5)
Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.193
User Datagram Protocol, Src Port: 53, Dst Port: 57918
Domain Name System (response)
  Transaction ID: 0x28b3
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Authority RRs: 5
  Additional RRs: 7
  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)
  Answers
    www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
      Name: www.ietf.org
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 900 (15 minutes)
      Data length: 33
      CNAME: www.ietf.org.cdn.cloudflare.net

    www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
      Name: www.ietf.org.cdn.cloudflare.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 900 (15 minutes)
      Data length: 4
      Address: 104.16.45.99
    www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
      Name: www.ietf.org.cdn.cloudflare.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 900 (15 minutes)

```

该部分思考题

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

查看我的截图里面 query 报文有一行 User Datagram Protocol, Src Port: 57918, Dst Port: 53, 表示其用 UDP 传输的, response 报文有一行 User Datagram Protocol, Src Port: 53, Dst Port: 57918, 表示其用 UDP 传输的。

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

第 4 题用到的那一行就提到了这个, query 报文的目标端口是 53, response 报文的源端口是 53(这是想告诉我这两个一样?)

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?

在我截出来的 query 报文那一部分有一行 Internet Protocol Version 4, Src: 192.168.43.193, Dst: 192.168.43.1, 即 query 报文送到的 ip 地址是 192.168.43.1, 在上一小节 ipconfig 里面, 我截出了我本地 DNS 服务器的 ip 地址, 也是 192.168.43.1 是相同的。

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

观察我的 DNS query 报文截图, 其类型是 A, (其实还有个 AAAA, 这个是 ipv6 的, 我没截出来) 这

个 query 报文里面没用看到有 answers 行。

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

观察我的 DNS response 报文截图，这里提供了三个 answers，具体内容如下：

```
Answers
www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
Name: www.ietf.org
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 900 (15 minutes)
Data length: 33
CNAME: www.ietf.org.cdn.cloudflare.net

www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
Name: www.ietf.org.cdn.cloudflare.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 900 (15 minutes)
Data length: 4
Address: 104.16.45.99

www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
Name: www.ietf.org.cdn.cloudflare.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 900 (15 minutes)
Data length: 4
Address: 104.16.44.99
```

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?

第一次并没有找到，这是后来又试了一次
这里过滤器加上 tcp，因为 syn 包在 tcp 里面

64	2021-09-30	21:30:08.871766	192.168.43.1	192.168.43.193	DNS	282 Standard query response 0x4b56 AAAA www.bing.com CNAME a-00
84	2021-09-30	21:30:09.549897	192.168.43.193	192.168.43.1	DNS	72 Standard query 0x1329 A www.ietf.org
85	2021-09-30	21:30:09.550468	192.168.43.193	192.168.43.1	DNS	72 Standard query 0x54fb AAAA www.ietf.org
86	2021-09-30	21:30:09.580292	192.168.43.1	192.168.43.193	DNS	483 Standard query response 0x54fb AAAA www.ietf.org CNAME www.
87	2021-09-30	21:30:09.580831	192.168.43.1	192.168.43.193	DNS	459 Standard query response 0x1329 A www.ietf.org CNAME www.iet
95	2021-09-30	21:30:09.766994	240e:45b:404:20e9:8d91:c8dd:1ae9:16e4	240e:45b:404:20e9:8d91:c8dd:1ae9:16e4	TCP	66 80 → 51552 [ACK] Seq=0 Ack=1 Win=131072 Len=0
102	2021-09-30	21:30:09.891332	192.168.43.193	104.16.44.99	TCP	66 61506 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK
105	2021-09-30	21:30:09.945612	2606:4700:6810:2d63	240e:45b:404:20e9:8d91:c8dd:1ae9:16e4	TCP	74 80 → 51552 [ACK] Seq=1 Ack=431 Win=67584 Len=0

在 DNS 包后面一点我找到了需要的 TCP SYN 包，就是我第二张截图，包的编号是 102

```
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
Authoritative nameservers
> cloudflare.net: type NS, class IN, ns ns3.cloudflare.net
> cloudflare.net: type NS, class IN, ns ns2.cloudflare.net
> cloudflare.net: type NS, class IN, ns ns4.cloudflare.net
> cloudflare.net: type NS, class IN, ns ns1.cloudflare.net
> cloudflare.net: type NS, class IN, ns ns5.cloudflare.net
Additional records
> ns1.cloudflare.net: type AAAA, class IN, addr 2400:cb00:2049:1::adf5:3b1f
> ns2.cloudflare.net: type AAAA, class IN, addr 2400:cb00:2049:1::c629:de83
> ns3.cloudflare.net: type AAAA, class IN, addr 2400:cb00:2049:1::c629:de1f
> ns4.cloudflare.net: type AAAA, class IN, addr 2400:cb00:2049:1::c629:df83
> ns5.cloudflare.net: type AAAA, class IN, addr 2400:cb00:2049:1::c629:df1f
> ns1.cloudflare.net: type A, class IN, addr 173.245.59.31
> ns2.cloudflare.net: type A, class IN, addr 198.41.222.131
> ns3.cloudflare.net: type A, class IN, addr 198.41.222.31
> ns4.cloudflare.net: type A, class IN, addr 198.41.223.131
> ns5.cloudflare.net: type A, class IN, addr 198.41.223.31
```

这是前面 DNS response 的 answer 截图，里面有很多个 ip 地址，我们发现其中的 101.16.44.99 就是这个 TCP SYN 包的目标 ip 地址，即这里是相对应的。

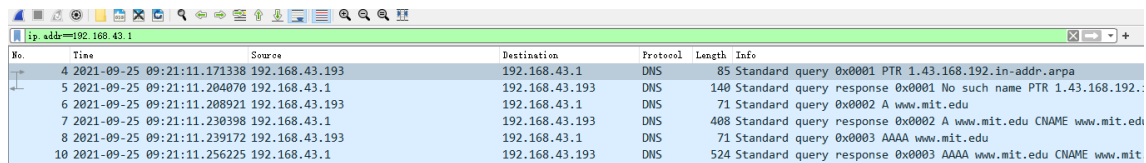
10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

并没有，从我抓到的包来看，并没有单独请求图片的 DNS query 。

2.3.2 第二部分

过程截图

这一部分我们使用 nslookup 命令，并用 wireshark 捕获观察这个命令执行时发生了什么首先我们打开捕获，然后输入 nslookup www.mit.edu，然后停止捕获，截图如下，这里我们重点关注最后两行。



No.	Time	Source	Destination	Protocol	Length	Info
4	2021-09-25 09:21:11.171338	192.168.43.193	192.168.43.1	DNS	85	Standard query 0x0001 PTR 1.43.168.192.in-addr.arpa
5	2021-09-25 09:21:11.204070	192.168.43.1	192.168.43.193	DNS	140	Standard query response 0x0001 No such name PTR 1.43.168.192.
6	2021-09-25 09:21:11.208921	192.168.43.193	192.168.43.1	DNS	71	Standard query 0x0002 A www.mit.edu
7	2021-09-25 09:21:11.230398	192.168.43.1	192.168.43.193	DNS	408	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu
8	2021-09-25 09:21:11.239172	192.168.43.193	192.168.43.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
10	2021-09-25 09:21:11.256225	192.168.43.1	192.168.43.193	DNS	524	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.

我把具体内容打印到了 pdf 中，截图如下：这是 query 报文

```
Vo.      Time      Source      Destination  Protocol Length Info
6 2021-09-25 09:21:11.208921 192.168.43.193 192.168.43.1 DNS 71 Standard query
3x0002 A www.mit.edu
Frame 6: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface
\Device\NPF_{D7A10DBD-93D5-4F5B-95D5-A4C7F7828D05}, id 0
Ethernet II, Src: LiteonTe_97:9f:c5 (30:d1:6b:97:9f:c5), Dst: 9a:01:f5:96:c9:7e (9a:01:f5:96:c9:7e)
Internet Protocol Version 4, Src: 192.168.43.193, Dst: 192.168.43.1
User Datagram Protocol, Src Port: 56963, 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
Queries
www.mit.edu: type A, class IN
Name: www.mit.edu
[Name Length: 11]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 7]
```

这是 response 报文

```
No.      Time      Source      Destination  Protocol Length Info
7 2021-09-25 09:21:11.230398 192.168.43.1 192.168.43.193 DNS 408 Standard query
response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.2.133.29 NS
n6dscb.akamaiedge.net NS n7dscb.akamaiedge.net NS n5dscb.akamaiedge.net NS n2dscb.akamaiedge.net NS
n4dscb.akamaiedge.net NS n0dscb.akamaiedge.net NS n1dscb.akamaiedge.net NS n3dscb.akamaiedge.net A
104.109.129.148 A 88.221.81.192 A 23.33.94.102 A 104.109.129.109 A 104.109.129.183
Frame 7: 408 bytes on wire (3264 bits), 408 bytes captured (3264 bits) on interface
\Device\NPF_{D7A10DBD-93D5-4F5B-95D5-A4C7F7828D05}, id 0
Ethernet II, Src: 9a:01:f5:96:c9:7e (9a:01:f5:96:c9:7e), Dst: LiteonTe_97:9f:c5 (30:d1:6b:97:9f:c5)
Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.193
User Datagram Protocol, Src Port: 53, Dst Port: 56963
Domain Name System (response)
Transaction ID: 0x0002
Flags: 0x8100 Standard query response, No error
Questions: 1
Answer RRs: 3
Authority RRs: 8
Additional RRs: 5
Queries
www.mit.edu: type A, class IN
Name: www.mit.edu
[Name Length: 11]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
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: 969 (16 minutes, 9 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: 900 (15 minutes)
Data length: 24
CNAME: e9566.dscb.akamaiedge.net
```

该部分思考题

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

从 query 报文中找出这一行 User Datagram Protocol, Src Port: 56963, Dst Port: 53, 表示其目标端口是 53, 从 response 报文中找出这一行 User Datagram Protocol, Src Port: 53, Dst Port: 56963, 表示其源端口是 53.

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

从 query 报文中找到这一行 Internet Protocol Version 4, Src: 192.168.43.193, Dst: 192.168.43.1, 表示 query 报文送到 192.168.43.1. 这恰好是我本地 DNS 服务器的 ip 地址。

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

观察我的 query 报文截图, 其类型为 A, 这里面找不到 answers 行。

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

观察我的 response 报文截图, 里面有三条 answers, 我将具体内容截图如下:

```
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: 969 (16 minutes, 9 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: 900 (15 minutes)
  Data length: 24
  CNAME: e9566.dscb.akamaiedge.net
e9566.dscb.akamaiedge.net: type A, class IN, addr 23.2.133.29
  Name: e9566.dscb.akamaiedge.net
  Type: A (Host Address) (1)
  Class: IN (0x0001)
  Time to live: 900 (15 minutes)
  Data length: 4
  Address: 23.2.133.29
```

15. Provide a screenshot.

该提供的截图都提供了 qwq。

2.3.3 第三部分

过程截图

这一部分运行 nslookup -type=NS mit.edu 命令, 使用 wireshark 抓包看发生了什么, 抓包结果如下:

46	2021-09-25 09:26:54.275673	192.168.43.193	192.168.43.1	DNS	85 Standard query 0x0001 PTR 1.43.168.192.in-addr.arpa
47	2021-09-25 09:26:54.279080	192.168.43.1	192.168.43.193	DNS	85 Standard query response 0x0001 No such name PTR 1.43.168.192.
48	2021-09-25 09:26:54.280835	192.168.43.193	192.168.43.1	DNS	67 Standard query 0x0002 NS mit.edu
50	2021-09-25 09:26:54.313565	192.168.43.1	192.168.43.193	DNS	390 Standard query response 0x0002 NS mit.edu NS ns1-37.akam.net

具体内容打印到了 pdf 中，我截出如下：这是 query 报文

```
No.      Time      Source      Destination  Protocol Length Info
  48 2021-09-25 09:26:54.280835 192.168.43.193 192.168.43.1  DNS      67      Standard query
0x0002 NS mit.edu
Frame 48: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface
\Device\NPF_{D7A10DBD-93D5-4F5B-95D5-A4C7F7828D05}, id 0
Ethernet II, Src: LiteonTe_97:9f:c5 (30:d1:6b:97:9f:c5), Dst: 9a:01:f5:96:c9:7e (9a:01:f5:96:c9:7e)
Internet Protocol Version 4, Src: 192.168.43.193, Dst: 192.168.43.1
User Datagram Protocol, Src Port: 49885, 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
  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)
  [Response In: 50]
```

这是 response 报文

```
No.      Time      Source      Destination  Protocol Length Info
  50 2021-09-25 09:26:54.313565 192.168.43.1 192.168.43.193  DNS      390      Standard query
response 0x0002 NS mit.edu NS ns1-37.akam.net NS usw2.akam.net NS ns1-173.akam.net NS use5.akam.net NS
asia2.akam.net NS use2.akam.net NS eur5.akam.net NS asia1.akam.net A 95.101.36.64 A 193.108.91.173 A
95.100.175.64 A 2.16.40.64 A 96.7.49.64 A 23.74.25.64 AAAA 2600:1401:2::ad AAAA 2600:1403:a::40
Frame 50: 390 bytes on wire (3120 bits), 390 bytes captured (3120 bits) on interface
\Device\NPF_{D7A10DBD-93D5-4F5B-95D5-A4C7F7828D05}, id 0
Ethernet II, Src: 9a:01:f5:96:c9:7e (9a:01:f5:96:c9:7e), Dst: LiteonTe_97:9f:c5 (30:d1:6b:97:9f:c5)
Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.193
User Datagram Protocol, Src Port: 53, Dst Port: 49885
Domain Name System (response)
  Transaction ID: 0x0002
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 8
  Authority RRs: 0
  Additional RRs: 8
  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 ns1-37.akam.net
      Name: MIT.edu
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 1124 (18 minutes, 44 seconds)
      Data length: 17
      Name Server: ns1-37.akam.net
    MIT.edu: type NS, class IN, ns usw2.akam.net
      Name: MIT.edu
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 1124 (18 minutes, 44 seconds)
      Data length: 7
      Name Server: usw2.akam.net
```

```

Name Server: usw2.akam.net
MIT.edu: type NS, class IN, ns ns1-173.akam.net
Name: MIT.edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 1124 (18 minutes, 44 seconds)
Data length: 10
Name Server: ns1-173.akam.net
MIT.edu: type NS, class IN, ns use5.akam.net
Name: MIT.edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 1124 (18 minutes, 44 seconds)
Data length: 7
Name Server: use5.akam.net
MIT.edu: type NS, class IN, ns asia2.akam.net
Name: MIT.edu
Type: NS (authoritative Name Server) (2)

```

```

Class: IN (0x0001)
Time to live: 1124 (18 minutes, 44 seconds)
Data length: 8
Name Server: asia2.akam.net
MIT.edu: type NS, class IN, ns use2.akam.net
Name: MIT.edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 1124 (18 minutes, 44 seconds)
Data length: 7
Name Server: use2.akam.net
MIT.edu: type NS, class IN, ns eur5.akam.net
Name: MIT.edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 1124 (18 minutes, 44 seconds)
Data length: 7
Name Server: eur5.akam.net

```

```

MIT.edu: type NS, class IN, ns asia1.akam.net
Name: MIT.edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 1124 (18 minutes, 44 seconds)
Data length: 8
Name Server: asia1.akam.net
Additional records
asia2.akam.net: type A, class IN, addr 95.101.36.64
Name: asia2.akam.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 136286 (1 day, 13 hours, 51 minutes, 26 seconds)
Data length: 4
Address: 95.101.36.64
ns1-173.akam.net: type A, class IN, addr 193.108.91.173
Name: ns1-173.akam.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 133764 (1 day, 13 hours, 9 minutes, 24 seconds)
Data length: 4
Address: 193.108.91.173
asia1.akam.net: type A, class IN, addr 95.100.175.64
Name: asia1.akam.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 123766 (1 day, 10 hours, 22 minutes, 46 seconds)
Data length: 4
Address: 95.100.175.64
use5.akam.net: type A, class IN, addr 2.16.40.64
Name: use5.akam.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 130457 (1 day, 12 hours, 14 minutes, 17 seconds)
Data length: 4
Address: 2.16.40.64

```



```

Address: 2.10.40.04
use2.akam.net: type A, class IN, addr 96.7.49.64
  Name: use2.akam.net
  Type: A (Host Address) (1)
  Class: IN (0x0001)
  Time to live: 39970 (11 hours, 6 minutes, 10 seconds)
  Data length: 4
  Address: 96.7.49.64
eur5.akam.net: type A, class IN, addr 23.74.25.64
  Name: eur5.akam.net
  Type: A (Host Address) (1)
  Class: IN (0x0001)
  Time to live: 172714 (1 day, 23 hours, 58 minutes, 34 seconds)
  Data length: 4
  Address: 23.74.25.64
ns1-173.akam.net: type AAAA, class IN, addr 2600:1401:2::ad
  Name: ns1-173.akam.net
  Type: AAAA (IPv6 Address) (28)
  Class: IN (0x0001)
  Time to live: 133764 (1 day, 13 hours, 9 minutes, 24 seconds)
  Data length: 16
  AAAA Address: 2600:1401:2::ad
use5.akam.net: type AAAA, class IN, addr 2600:1403:a::40
  Name: use5.akam.net
  Type: AAAA (IPv6 Address) (28)
  Class: IN (0x0001)
  Time to live: 134963 (1 day, 13 hours, 29 minutes, 23 seconds)
  Data length: 16
  AAAA Address: 2600:1403:a::40

```

该部分思考题

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

query 报文里面有一行 Internet Protocol Version 4, Src: 192.168.43.193, Dst: 192.168.43.1, 表示这个 query 报文送到 192.168.43.1 这是我本地 DNS 服务器的默认 ip 地址

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

观察 DNS query 报文，有一行 mit.edu: type NS, class IN，表示其 type 为 NS，里面没有 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?

观察响应报文,其提供了 ns1-37.akam.net,usw2.akam.net,ns1-173.akam.net,use5.akam.net,asia2.akam.net use2.akam.net, eur5.akam.net, asia1.akam.net 这几个，也提供了 ip 地址，就在 Additional records 里面。

19. Provide a screenshot.

该提供的都提供了 qaq

2.3.4 第四部分

过程截图

这一部分，运行 nslookup www.aiit.or.kr bitsy.mit.edu，使用 wireshark 抓包观察，这里需要把 ip 地址为 bitsy.mit.edu 的过滤出来，截图如下

No.	Time	Source	Destination	Protocol	Length	Info
13	2021-09-26 19:12:34.666087	192.168.43.193	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
41	2021-09-26 19:12:36.679592	192.168.43.193	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
46	2021-09-26 19:12:38.685797	192.168.43.193	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
51	2021-09-26 19:12:40.702643	192.168.43.193	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
59	2021-09-26 19:12:42.716492	192.168.43.193	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr

这里实际上访问超时了，好像出的结果不对劲 orz, 试了几个其他的服务器也不行，不知道为什么，网上查找了一些方法也没有解决

这是其中一个 query 报文：

```
> Frame 41: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{D7A10D8D-93D5-4F58-95D5-A4C7F7828D05}, id 0
> Ethernet II, Src: LiteonTe_97:9f:c5 (30:d1:6b:97:9f:c5), Dst: ea:b7:4f:07:4d:c4 (ea:b7:4f:07:4d:c4)
> Internet Protocol Version 4, Src: 192.168.43.193, Dst: 18.0.72.3
> User Datagram Protocol, Src Port: 51127, 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
  Queries
    > www.aiit.or.kr: type A, class IN
```

这里超时未响应所以没有 response 报文，所以我直接用本地的 DNS 了，下面我们得到了一个响应报文

```
> Frame 5: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{D7A10D8D-93D5-4F58-95D5-A4C7F7828D05}, id 0
> Ethernet II, Src: ea:b7:4f:07:4d:c4 (ea:b7:4f:07:4d:c4), Dst: LiteonTe_97:9f:c5 (30:d1:6b:97:9f:c5)
> Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.193
> User Datagram Protocol, Src Port: 53, Dst Port: 59689
> Domain Name System (response)
  Transaction ID: 0x0002
  Flags: 0x8100 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  Queries
    > www.aiit.or.kr: type A, class IN
  Answers
    > www.aiit.or.kr: type A, class IN, addr 58.229.6.225
      Name: www.aiit.or.kr
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 3527 (58 minutes, 47 seconds)
      Data length: 4
      Address: 58.229.6.225
      [Request In: 4]
      [Time: 0.003914000 seconds]
```

该部分思考题

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?

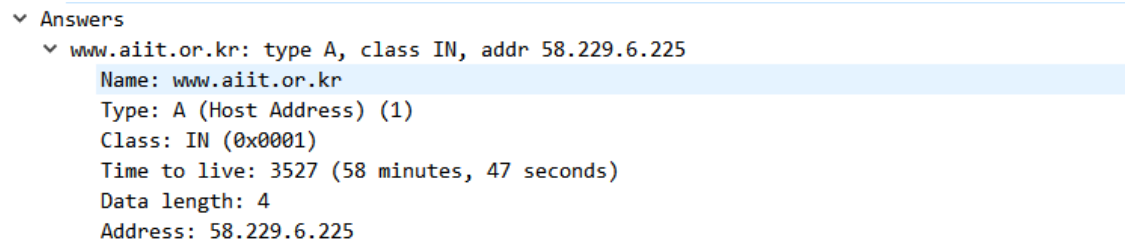
观察 query 报文截图，有一行 Internet Protocol Version 4, Src: 192.168.43.193, Dst: 18.0.72.3，可知这个 DNS query 送往 18.0.72.3，我本地默认的 DNS 服务器为 192.168.43.1，这两个不一样，这个 ip 地址是 bitsy.mit.edu 的

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

观察 query 报文截图，有一行 www.aiit.or.kr: type A, class IN，表示它的 type 是 A，在报文里面没有 answers

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

根据 response 报文，这里只有一个 answers, 包含内容截图如下



```
Answers
  www.aiit.or.kr: type A, class IN, addr 58.229.6.225
    Name: www.aiit.or.kr
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 3527 (58 minutes, 47 seconds)
    Data length: 4
    Address: 58.229.6.225
```

有名称，类型，类，生存时间，数据长度，ip 地址。

23. Provide a screenshot.

截图都在上面

Chapter 3

实验总结

本次实验，我学习了有关 DNS 的各种命令，以及 DNS 报文的格式，学会了使用 nslookup 查询域名的各种信息，ipconfig 查看各种网络的设置，收获很多。