

计算机网络 DNS 实验报告

姓名：陈鹤影

学号：PB21061287

日期：2022.10.7

一、 实验目的：

1. 熟练掌握 nslookup 和 ipconfig 的使用方法
2. 体会不同的命令格式在域名解析过程中产生的区别
3. 利用 Wireshark 抓包深入观察域名解析客户端的具体过程

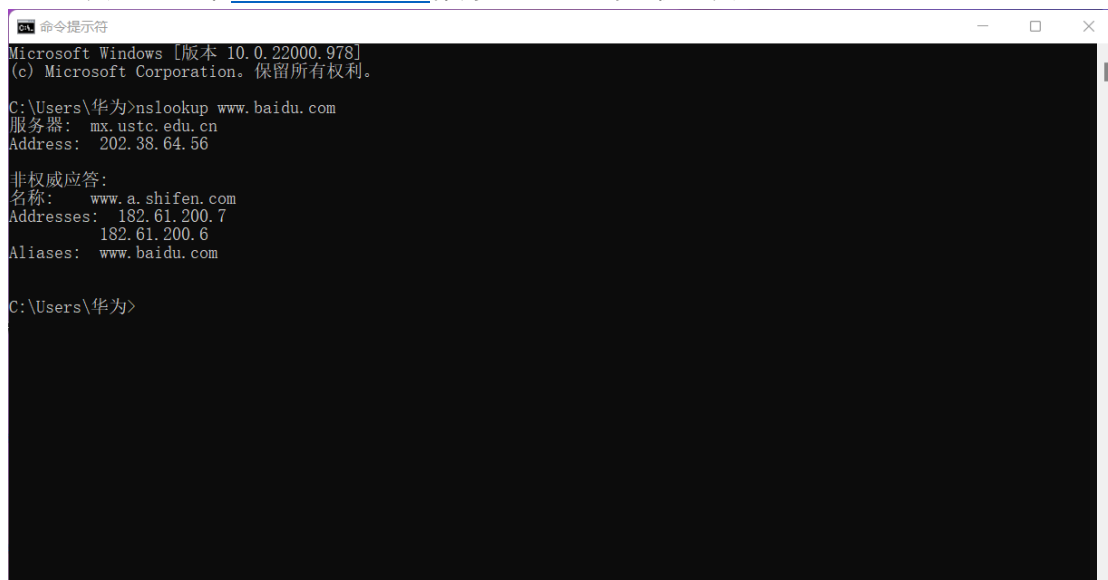
二、 实验流程及问题回答：

Part 1: nslookup

Q&A:

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

Ans: 实验中选择 www.baidu.com 作为需要查询的主机。实验结果如下：



```
命令提示符
Microsoft Windows [版本 10.0.22000.978]
(c) Microsoft Corporation. 保留所有权利。

C:\Users\华为>nslookup www.baidu.com
服务器: mx.ustc.edu.cn
Address: 202.38.64.56

非权威应答:
名称: www.a.shifen.com
Addresses: 182.61.200.7
          182.61.200.6
Aliases: www.baidu.com

C:\Users\华为>
```

(图 1-1 对 www.baidu.com 查询结果)

可见 www.baidu.com 对应的 IP 地址有两个，分别为 182.61.200.7 和 182.61.200.6。上述查询结果来自本地域名服务器 mx.ustc.edu.cn。此外，上述结果是一个非权威应答，即来自某 DNS 服务器的缓存。查询 IP 信息可知，182.61.200.7 和 182.61.200.6 对应主机均位于中国-北京-北京市-电信。

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

Ans: 实验中选择剑桥大学的域 cam.ac.uk 发起查询。为查询 cam.ac.uk 域对应的权威 DNS 服务器，将 nslookup 置为 -type=NS 模式，查询结果如下：

```
命令提示符
Microsoft Windows [版本 10.0.22000.978]
(c) Microsoft Corporation。保留所有权利。

C:\Users\华为>nslookup www.baidu.com
服务器: mx.ustc.edu.cn
Address: 202.38.64.56

非权威应答:
名称: www.a.shifen.com
Addresses: 182.61.200.7
          182.61.200.6
Aliases: www.baidu.com

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

非权威应答:
cam.ac.uk      nameserver = dns0.eng.cam.ac.uk
cam.ac.uk      nameserver = dns0.cl.cam.ac.uk
cam.ac.uk      nameserver = ns3.mythic-beasts.com
cam.ac.uk      nameserver = ns1.mythic-beasts.com
cam.ac.uk      nameserver = auth0.dns.cam.ac.uk
cam.ac.uk      nameserver = ns2.ic.ac.uk

C:\Users\华为>
```

(图 1-2 对 cam.ac.uk 查询结果)

对应有六个主机 dns0.eng.cam.ac.uk、dns0.cl.cam.ac.uk、ns3.mythic-beasts.com、ns1.mythic-beasts.com、auth0.dns.cam.ac.uk、ns2.ic.ac.uk。

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?

Ans: 这里向上述获得的第一个主机名 dns0.eng.cam.ac.uk 发起查询，查询 mail.yahoo.com 对应的 IP 地址，结果如下：

```
C:\Users\华为>nslookup mail.yahoo.com dns0.eng.cam.ac.uk
服务器: dns0.eng.cam.ac.uk
Address: 129.169.8.8

*** dns0.eng.cam.ac.uk 找不到 mail.yahoo.com: Query refused

C:\Users\华为>
```

(图 1-3 对 mail.yahoo.com 查询结果)

dns0.eng.cam.ac.uk 主机上没有相关信息，显示找不到。用本地服务器查询后得知：

```
C:\Users\华为>nslookup mail.yahoo.com
服务器: mx.ustc.edu.cn
Address: 202.38.64.56

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
```

(图 1-4 用本地服务器对 mail.yahoo.com 查询结果)

mail.yahoo.com 对应多台主机，相应的 IP 地址为 2001:4998:64:800::6001、2001:4998:64:800::6000、69.147.80.15、69.147.80.12。

Part 2: ipconfig

利用 ipconfig 查看主机当前 TCP/IP 全部信息，使用 ipconfig /all 命令。实验结果如下：

```

C:\Users\华为>ipconfig /all

Windows IP 配置

   主机名 . . . . . : LAPTOP-L02V65IS
   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

无线局域网适配器 本地连接* 3:

   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 #3
   物理地址. . . . . : E0-D4-E8-EF-93-5F
   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* 12:

   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 #4
   物理地址. . . . . : E2-D4-E8-EF-93-5E
   DHCP 已启用 . . . . . : 否
   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 . . . . . :
   描述. . . . . : VMware Virtual Ethernet Adapter for VMnet1 #2
   物理地址. . . . . : 00-50-56-C0-00-01
   DHCP 已启用 . . . . . : 否
   自动配置已启用. . . . . : 是
   本地连接 IPv6 地址. . . . . : fe80::e412:8a16:e1d0:6f79%16(首选)
   IPv4 地址 . . . . . : 192.168.133.1(首选)
   子网掩码 . . . . . : 255.255.255.0
   默认网关. . . . . :
   DHCPv6 IAID . . . . . : 134238294
   DHCPv6 客户端 DUID . . . . . : 00-01-00-01-29-E5-19-E0-E0-D4-E8-EF-93-5E
   TCP/IP 上的 NetBIOS . . . . . : 已启用

以太网适配器 以太网 3:

```

(图 1-5 用 ipconfig 命令查看当前全部 TCP/IP 信息)

利用 ipconfig 查看主机 DNS 缓存，使用 ipconfig /displaydns 命令。实验部分结果如下：

```

C:\Users\华为>ipconfig /displaydns

Windows IP 配置

tpstelemetry.tencent.com
-----
记录名称. . . . . : tpstelemetry.tencent.com
记录类型. . . . . : 1
生存时间. . . . . : 356
数据长度. . . . . : 4
部分. . . . . : 答案
A (主机)记录 . . . . . : 183.2.143.108

119.137.168.192.in-addr.arpa
-----
记录名称. . . . . : 119.137.168.192.in-addr.arpa.
记录类型. . . . . : 12
生存时间. . . . . : 92368
数据长度. . . . . : 8
部分. . . . . : 答案
PTR 记录 . . . . . : HUAWEI_Mate_40E-704591b1a.mshome.net

update.googleapis.com
-----
没有 AAAA 类型的记录

update.googleapis.com
-----
记录名称. . . . . : update.googleapis.com
记录类型. . . . . : 1
生存时间. . . . . : 18
数据长度. . . . . : 4
部分. . . . . : 答案
A (主机)记录 . . . . . : 203.208.41.98

edge.microsoft.com
-----

```

(图 1-6 用 ipconfig 命令查看主机 DNS 缓存信息)

利用 ipconfig 清除主机 DNS 缓存，使用 ipconfig /flushdns 命令。

Part 3: Tracing DNS with Wireshark

Step 1: 使用 ipconfig 命令清除主机 DNS 缓存
结果如下:

```
C:\Users\华为>ipconfig /flushdns

Windows IP 配置

已成功刷新 DNS 解析缓存。

C:\Users\华为>
```

(图 1-7 用 ipconfig 命令清除主机 DNS 缓存信息)

Step 2: 清除浏览器缓存

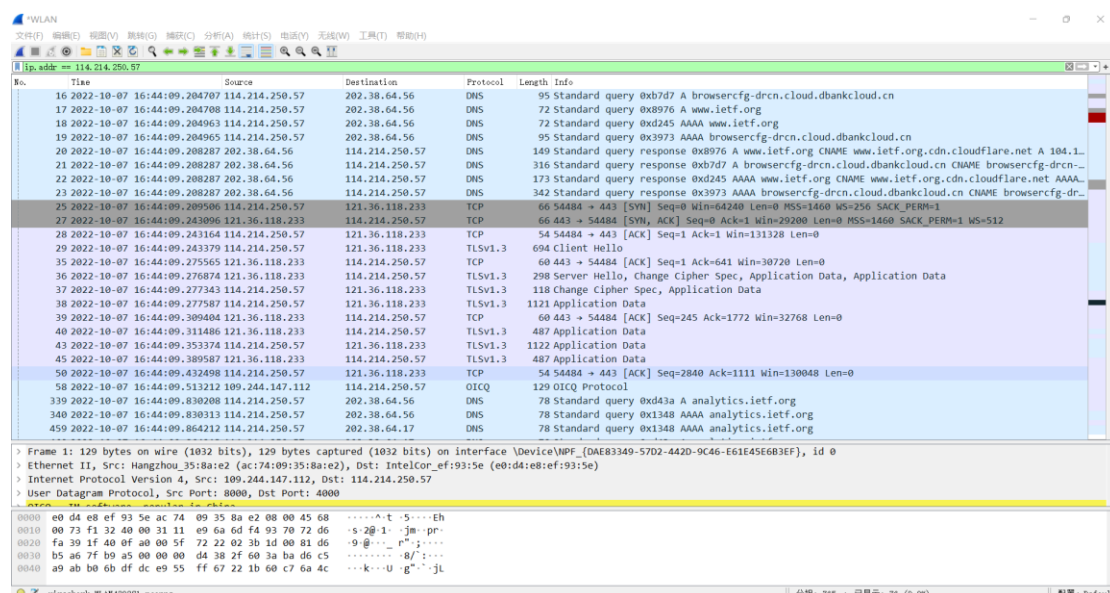
Step 3: 启动 Wireshark 选择地址过滤

由 ipconfig /all 可知, 主机 IPv4 地址为 114.214.250.57。

Step 4: 启动 Wireshark 抓包, 在浏览器端访问 Web 网页: <http://www.ietf.org>

Step 5: 停止抓包

实验结果如下:

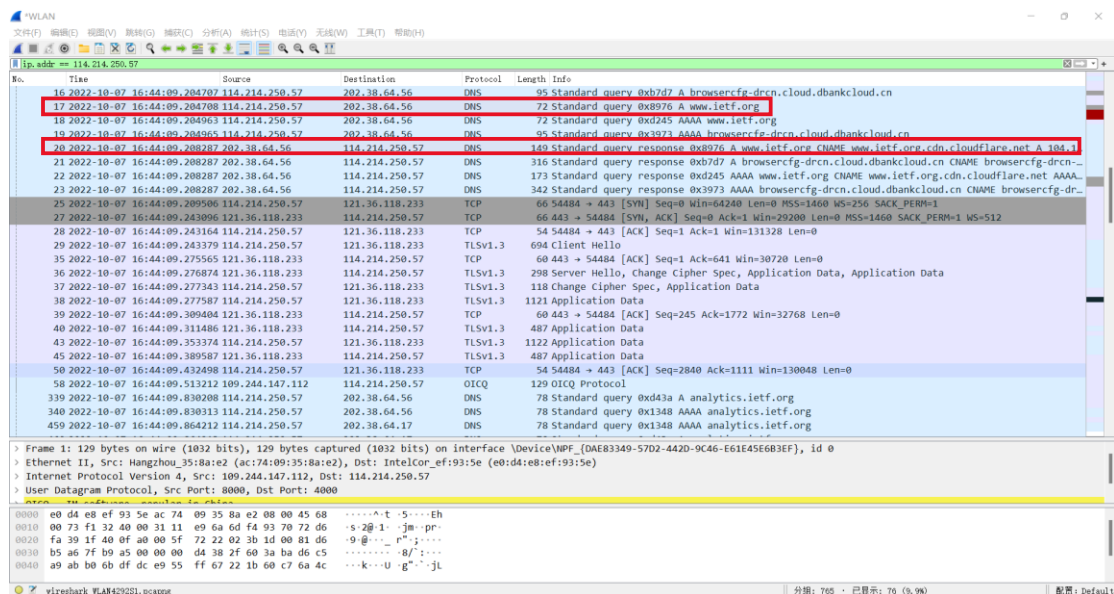


(图 1-8 Wireshark 抓包结果)

Q&A:

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

Ans: DNS 请求和相应报文位置如下:

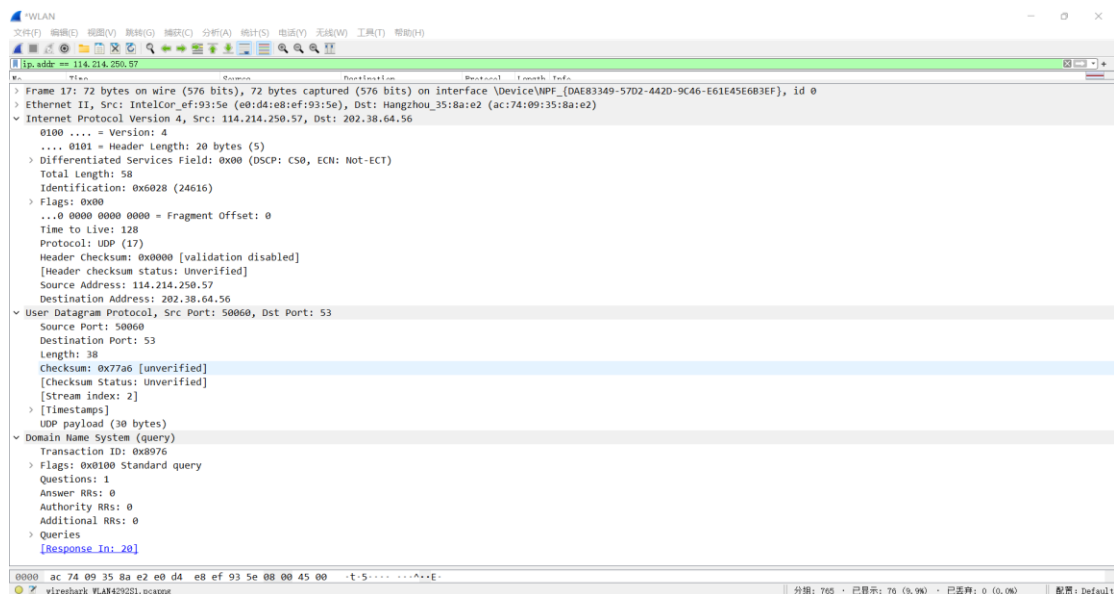


(图 1-9 请求响应报文位置)

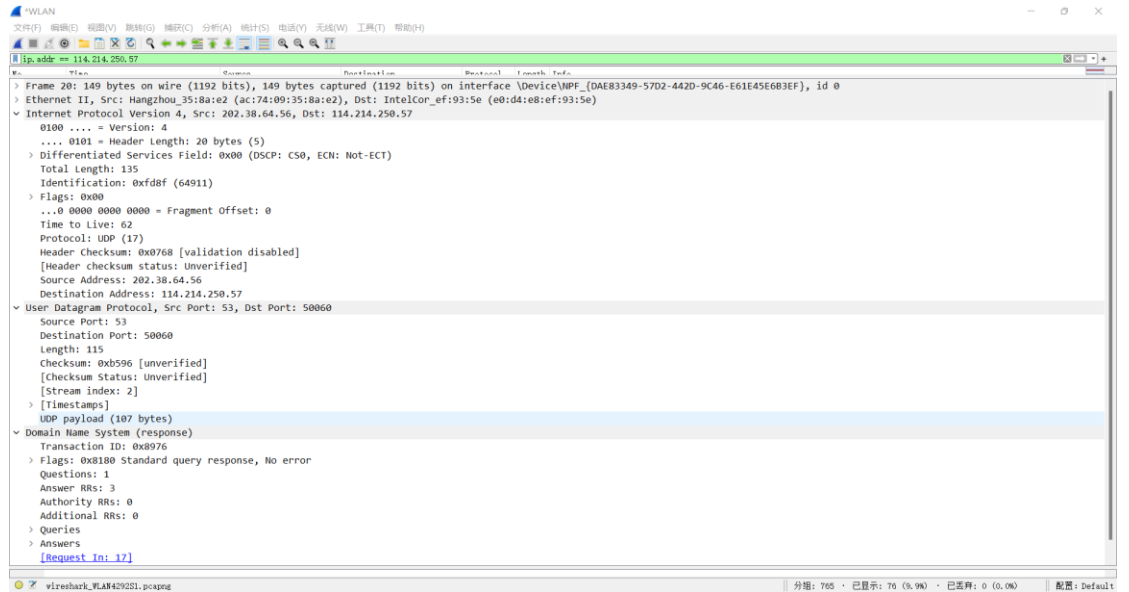
他们均使用 UDP 协议。



报文具体内容如下：



(图 1-10 请求报文内容)



(图 1-11 响应报文内容)

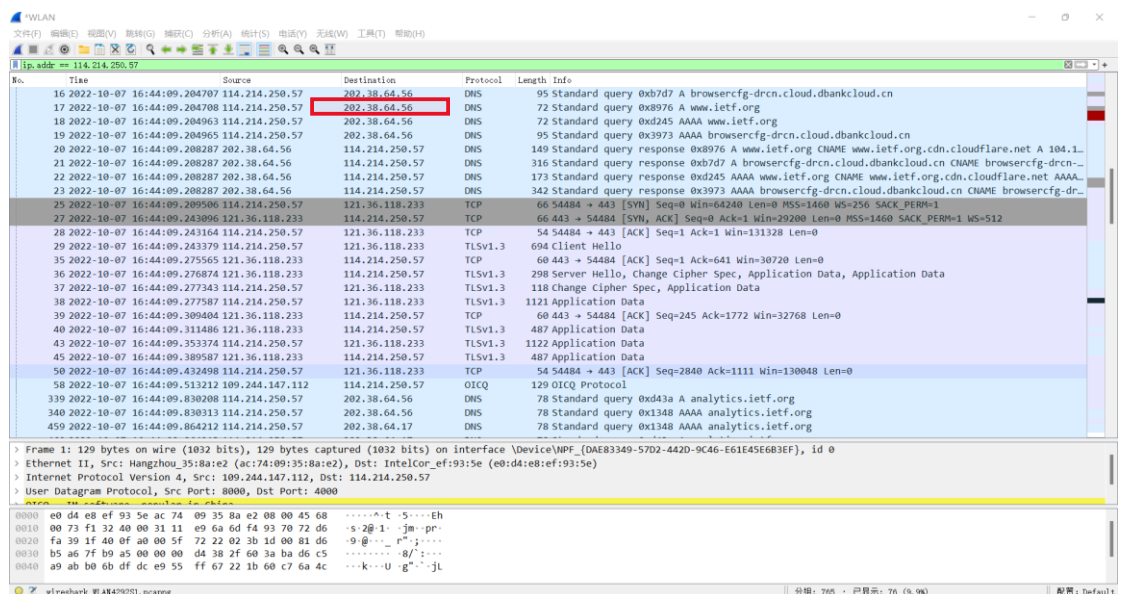
5) What is the destination port for the DNS query message? What is the source port of DNS response message?

Ans: 请求报文的目的端口为: 53; 响应报文的源端口为: 53.



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?

Ans: 请求报文的目的 IP 地址 202.38.64.56。



用 ipconfig 查询到本地 DNS 服务器的 IP 地址为 202.38.64.56。两者一致。

```
命令提示符
以太网适配器 以太网 3:
    连接特定的 DNS 后缀 . . . . . :
    描述 . . . . . : VMware Virtual Ethernet Adapter for VMnet8 #2
    物理地址 . . . . . : 00-50-56-C0-00-08
    DHCP 已启用 . . . . . : 否
    自动配置已启用 . . . . . : 是
    本地链接 IPv6 地址 . . . . . : fe80::fc8c:7756:4b93:adf17(首选)
    IPv4 地址 . . . . . : 192.168.118.1(首选)
    子网掩码 . . . . . : 255.255.255.0
    默认网关 . . . . . : 285233238
    DHCPv6 客户端 DUID . . . . . : 00-01-00-01-29-B5-19-B0-E0-D4-E8-EF-93-5E
    TCP/IP 上的 NetBIOS . . . . . : 已启用

无线网络适配器 WLAN:
    连接特定的 DNS 后缀 . . . . . : ustc.edu.cn
    描述 . . . . . : Intel(R) Wi-Fi 6 AX200 160MHz
    物理地址 . . . . . : E0-D4-E8-EF-93-5E
    DHCP 已启用 . . . . . : 是
    自动配置已启用 . . . . . : 是
    IPv6 地址 . . . . . : 2001:da8:d800:186:3991:a910:28d2:e19c(首选)
    临时 IPv6 地址 . . . . . : 2001:da8:d800:186:9106:b75:d21e:6c4(首选)
    本地链接 IPv6 地址 . . . . . : fe80::3991:a910:28d2:e19c%20(首选)
    IPv4 地址 . . . . . : 114.214.250.57(首选)
    子网掩码 . . . . . : 255.255.240.0
    获得租约的时间 . . . . . : 2022年10月7日 16:07:13
    租约过期的时间 . . . . . : 2022年10月7日 18:07:22
    默认网关 . . . . . : fe80::aef4:92ff:fe35:8ae2%20
    114.214.240.1
    DHCP 服务器 . . . . . : 202.38.64.17
    DHCPv6 IAD . . . . . : 163729512
    DHCPv6 客户端 DUID . . . . . : 00-01-00-01-29-B5-19-B0-E0-D4-E8-EF-93-5E
    DNS 服务器 . . . . . : 202.38.64.56
    202.38.64.17
    TCP/IP 上的 NetBIOS . . . . . : 已启用

以太网适配器 蓝牙网络连接:
    媒体状态 . . . . . : 媒体已断开连接
    连接特定的 DNS 后缀 . . . . . :
    描述 . . . . . : Bluetooth Device (Personal Area Network)
    物理地址 . . . . . : E0-D4-E8-EF-93-62
    DHCP 已启用 . . . . . : 否
    自动配置已启用 . . . . . : 是

C:\Users\华为>
```

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

Ans: 请求报文的类型为 A 类型，报文中没有包含任何“answers”。

```
> Frame 17: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{DAE83349-5702-442D-9C46-E61E45E6B3EF}, id 0
> Ethernet II, Src: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
> Internet Protocol Version 4, Src: 114.214.250.57, Dst: 202.38.64.56
> User Datagram Protocol, Src Port: 50060, Dst Port: 53
> Domain Name System (query)
  Transaction ID: 0x8976
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    [Response In: 20]
```

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

Ans: 一共有 3 条 answers；第一条 answer 包括 www.ietf.org 对应的标准名 (type = CNAME)，后两条包含对应主机的 IPv4 地址(type = A)。

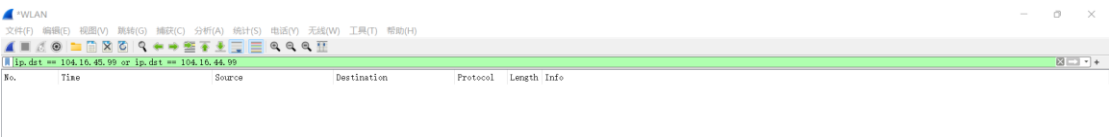
```
Wireshark · 分型 20 · WLAN
> Frame 20: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{DAE83349-5702-442D-9C46-E61E45E6B3EF}, id 0
> Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e)
> Internet Protocol Version 4, Src: 202.38.64.56, Dst: 114.214.250.57
> User Datagram Protocol, Src Port: 53, Dst Port: 50060
> Domain Name System (response)
  Transaction ID: 0x8976
  Flags: 0x8100 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Authority RRs: 0
  Additional RRs: 0
  Queries
    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 104.16.45.99
      > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
    [Request In: 17]
    [Time: 0.003579000 seconds]

0000  e0 d4 e8 ef 93 5e ac 74 09 35 8a e2 08 00 45 00  .....^t -5----E-
0010  00 87 fd 8f 00 00 3e 11 07 68 ca 26 40 38 72 d6  .....> -h-&8r-
0020  fa 39 00 35 c3 8c 00 73 b5 96 89 76 81 80 00 01  .....9-5---s -v---
0030  00 03 00 00 00 00 03 77 77 77 04 69 65 74 66 03  .....ww-ietf-
0040  6f 72 67 00 00 01 00 01 c0 0c 00 05 00 01 00 00  .....org-----
0050  01 7d 00 21 03 77 77 77 04 69 65 74 66 03 6f 72  .....}!-www-ietf-or
0060  6f 03 63 64 6e 0a 63 6c 6f 75 64 66 6c 61 72 65  .....g-cdn-cl oudflare
0070  03 6e 65 74 00 c0 2a 00 01 00 01 00 00 0b 00  .....net-.*-----
0080  04 68 10 2d 63 c0 2a 00 01 00 01 00 00 0b 00  .....h--c*-----
0090  04 68 10 2c 63  .....h-,c-----
```

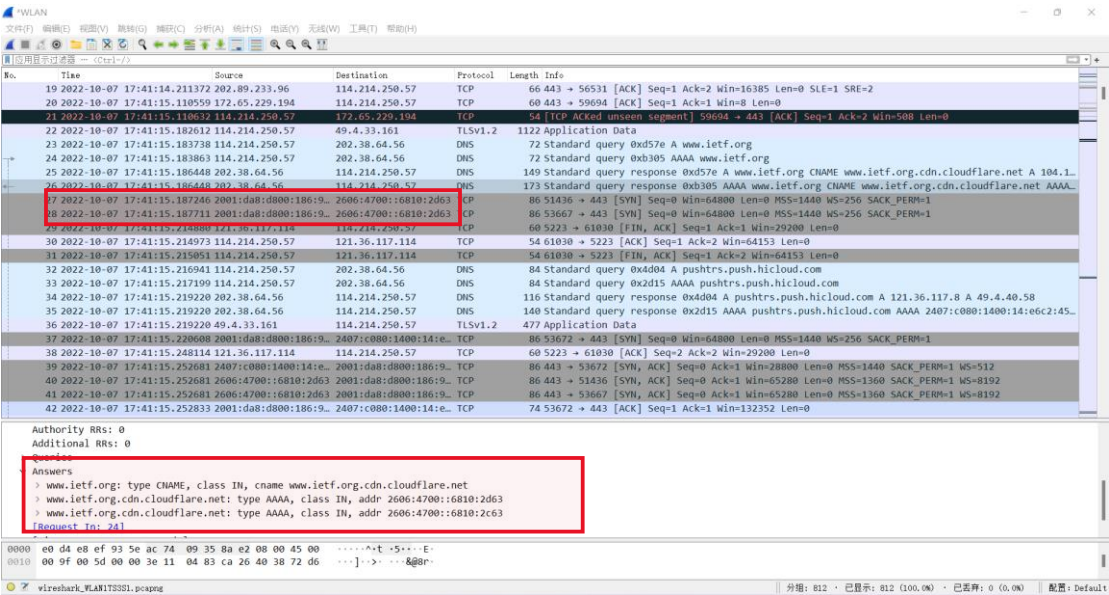
9) Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP

addresses provided in the DNS response message?

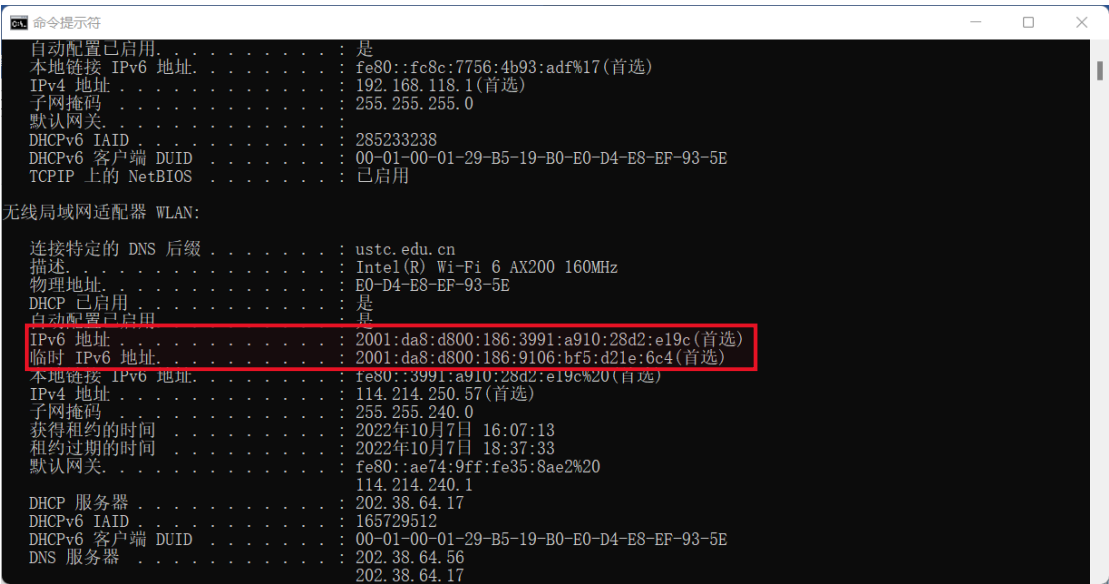
Ans: 并未找到对应上述 IPv4 地址的 TCP SYN packet。



但观察后发现可以找到对应 AAAA 响应返回的 IPv6 地址的 TCP SYN packet:

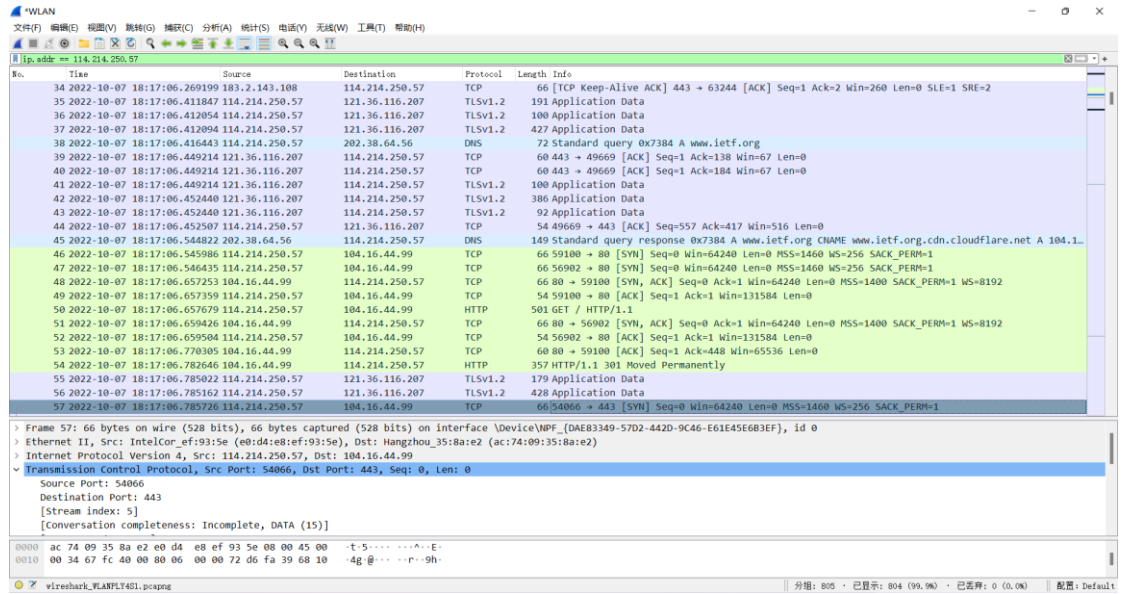


且源地址与主机 IPv6 地址一致:



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

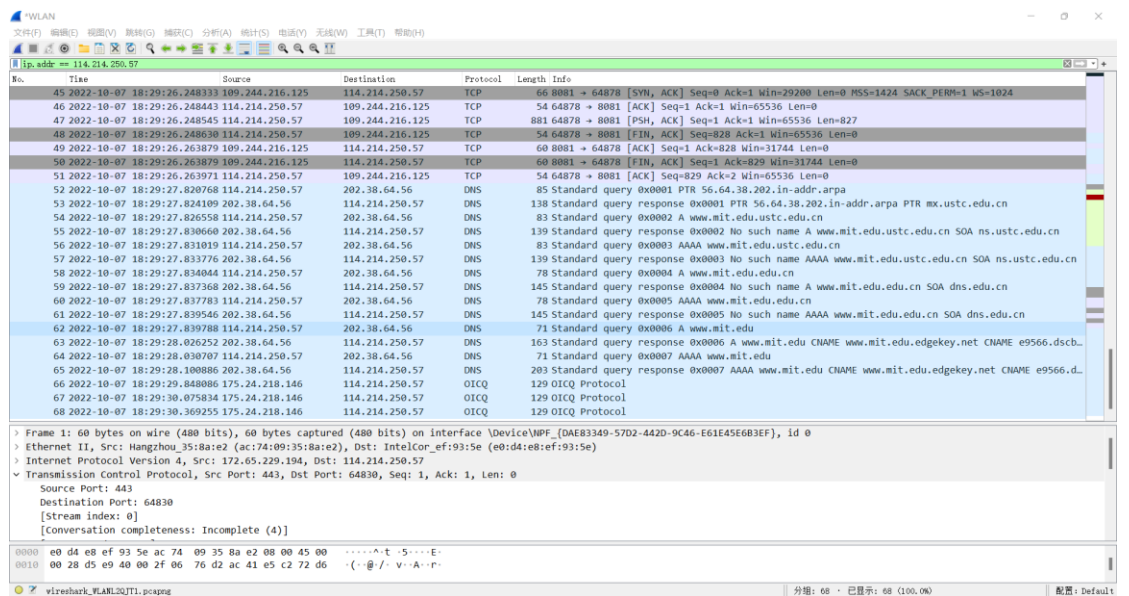
Ans: 为避免 IPv6 对实验的影响, 后续实验关闭 IPv6 重新进行。实验结果如下:



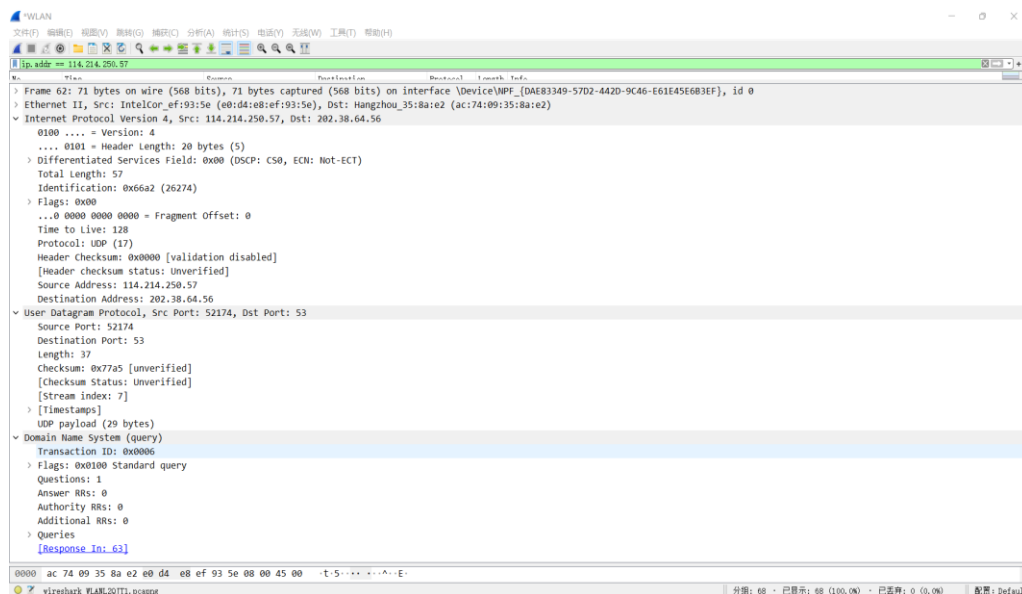
在后续检索过程中并未发送新的 DNS 请求，原因可能是本地 DNS 缓存了对应的 IP 地址。

Step 6: 利用 nslookup 查询 www.mit.edu 的 IP 地址，并抓包

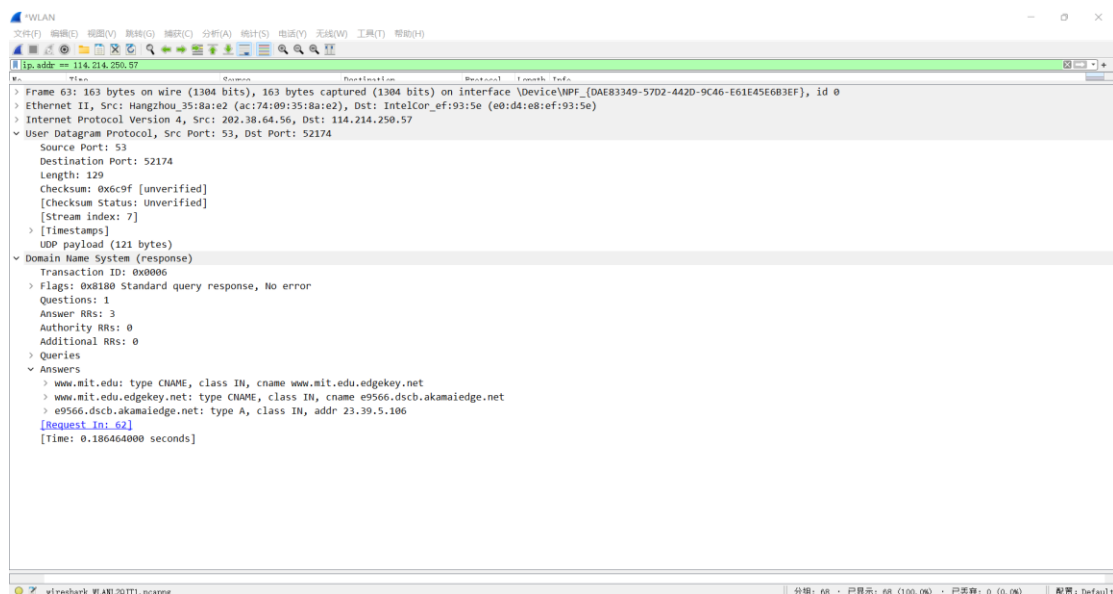
实验结果如下：



(图 1-12 对 nslookup 抓包结果)



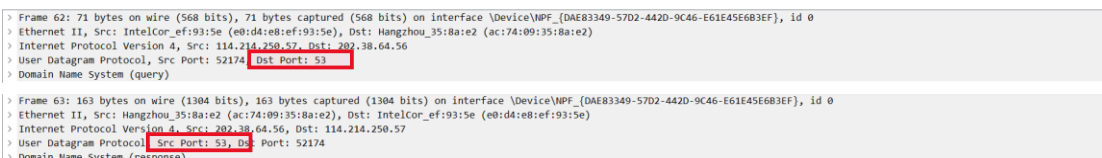
(图 1-13 请求报文内容)



(图 1-14 响应报文内容)

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

Ans: DNS 请求报文的目的端口为: 53; DNS 响应报文的源端口为: 53。



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

Ans: DNS 请求报文的目的地址为: 202.38.64.56。默认本地 DNS 服务器的地址为: 202.38.64.56。二者一致。

```
> Frame 62: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
> Ethernet II, Src: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e), Dst: Hangzhou_35:8a:e2 (ac:174:09:35:8a:e2)
> Internet Protocol Version 4, Src: 114.214.250.57, Dst: 202.38.64.56
> User Datagram Protocol, Src Port: 52174, Dst Port: 53
> Domain Name System (query)
```

```
C:\Users\华为>nslookup
默认服务器: mx.ustc.edu.cn
Address: 202.38.64.56
```

13) Examine the DNS query message. What “Type” of DNS query is it?

Does the query message contain any “answers”?

Ans: DNS 请求报文的类型为 A 类型。它不含有任何“answers”。

Wireshark packet capture showing a DNS query. The packet list shows a DNS query from 114.214.250.57 to 202.38.64.56. The packet details show a standard query for www.mit.edu. The packet bytes show the raw DNS query structure.

Wireshark packet capture showing a DNS response. The packet list shows a DNS response from 202.38.64.56 to 114.214.250.57. The packet details show a standard query response with three answers: two CNAME records and one A record. The packet bytes show the raw DNS response structure.

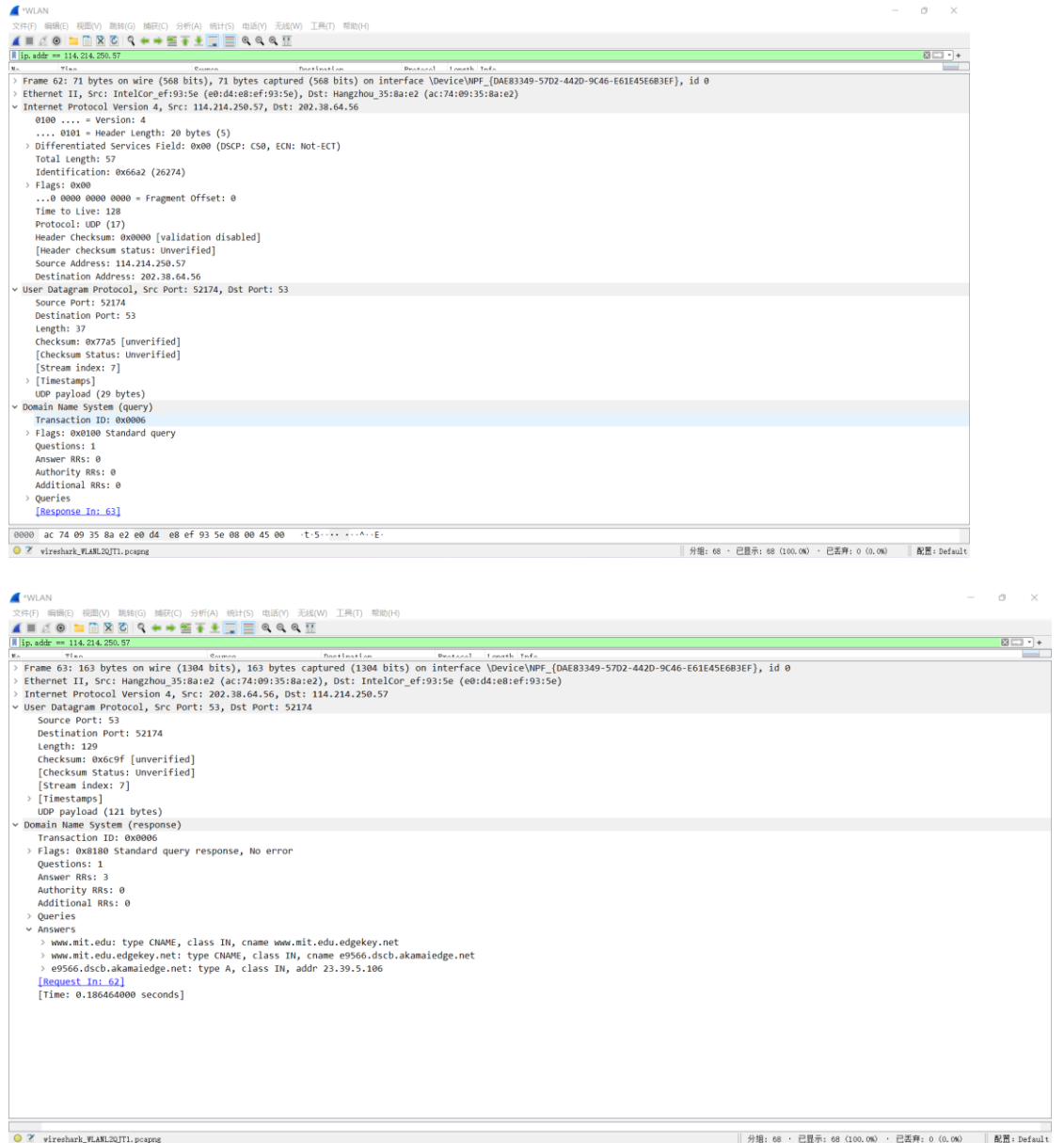
14) Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Ans: DNS 响应报文含有三条“answers”。前两条包含对应域名的标准名 (type = CNAME)，最后一条包含标准名对应的 IP 地址 (type = A)。

```
> Domain Name System (response)
  Transaction ID: 0x0006
  > Flags: 0x1800 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Authority RRs: 0
  Additional RRs: 0
  > 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 23.39.5.106
    [Request In: 62]
    [Time: 0.186464000 seconds]
```

15) Provide a screenshot.

Ans: 如下:



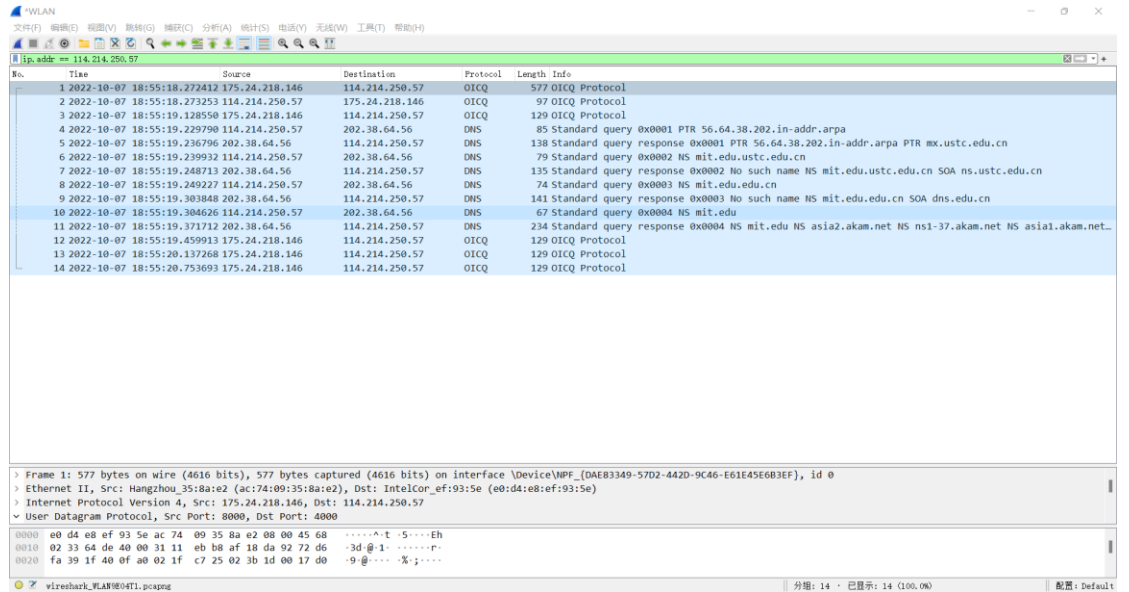
Step 6: 使用 `nslookup -type=NS mit.edu` 命令，并抓包
实验结果如下：

```
C:\Users\华为>nslookup -type=NS mit.edu
服务器: mx.ustc.edu.cn
Address: 202.38.64.56

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

C:\Users\华为>
```

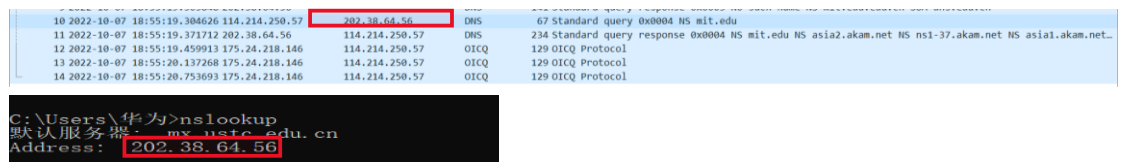
(图 1-15 实验结果)



(图 1-16 实验抓包结果)

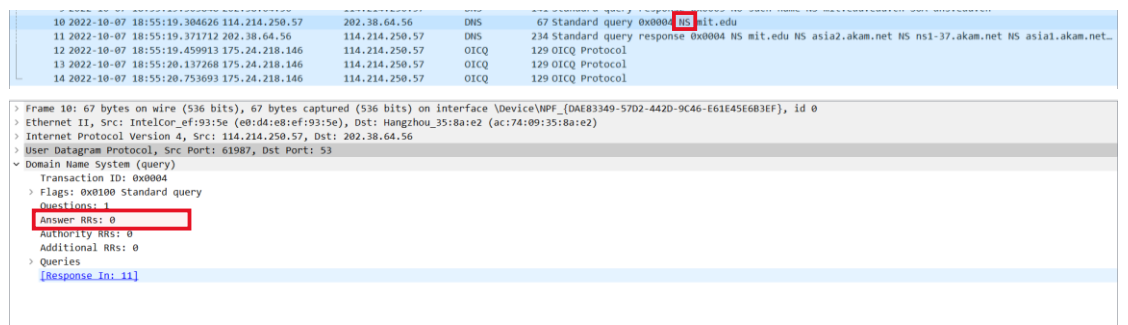
- 16) To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Ans: DNS 请求报文的地址为: 202.38.64.56。默认本地 DNS 服务器的地址为: 202.38.64.56。二者一致。



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

Ans: DNS 请求报文的类型为 NS 类型。它不含有任何“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?

Ans: DNS 响应报文提供了 mit.edu 对应的权威域名服务器 (8 个), 但并未提供相应的 IP 地址。

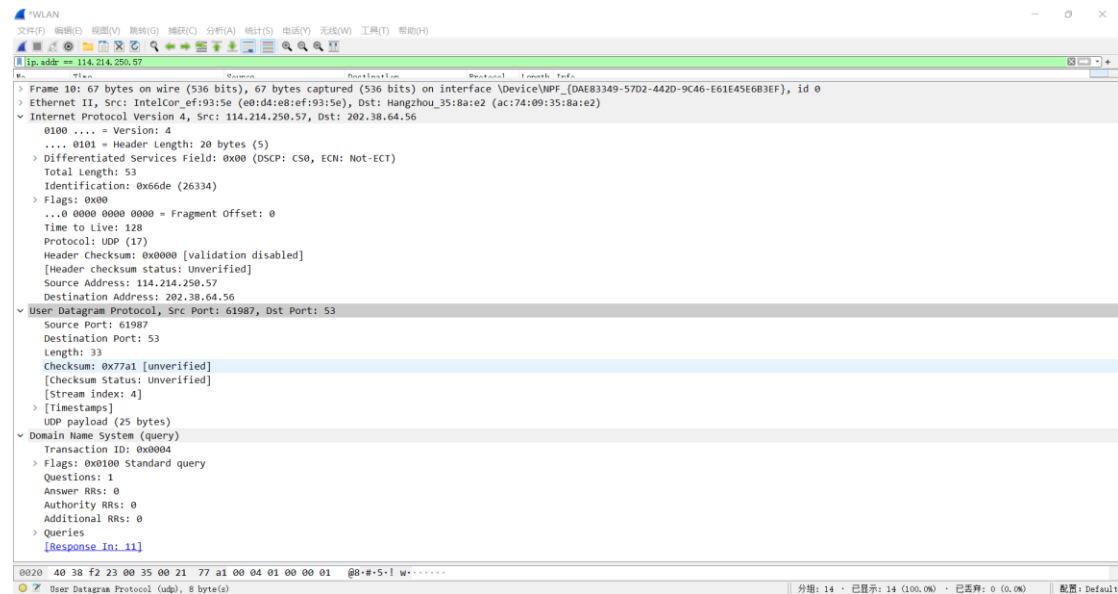
```

> Frame 11: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
> Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e)
> Internet Protocol Version 4, Src: 202.38.64.56, Dst: 114.214.250.57
> User Datagram Protocol, Src Port: 53, Dst Port: 61987
> Domain Name System (response)
  Transaction ID: 0x0004
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 8
  Authority RRs: 0
  Additional RRs: 0
  Queries
  Answers
    > mit.edu: type NS, class IN, ns asia2.akam.net
    > 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 ns1-173.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 eur5.akam.net
    > mit.edu: type NS, class IN, ns usa2.akam.net
  [Request In: 10]
  [Time: 0.067086000 seconds]

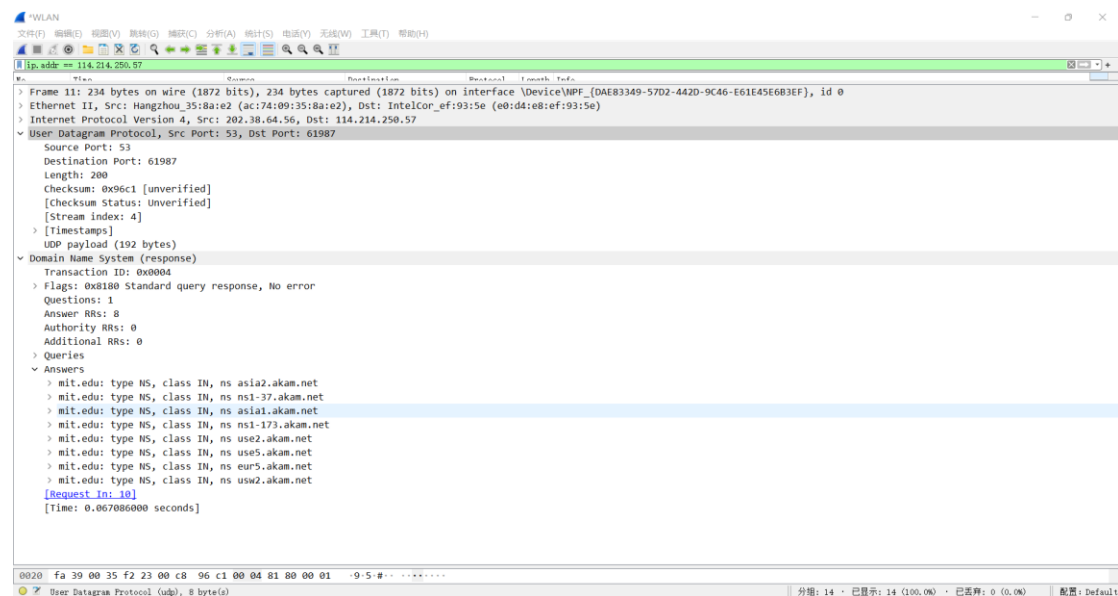
```

19) Provide a screenshot.

Ans: 如下图:



(图 1-17 DNS 请求报文内容)



(图 1-18 DNS 响应报文内容)

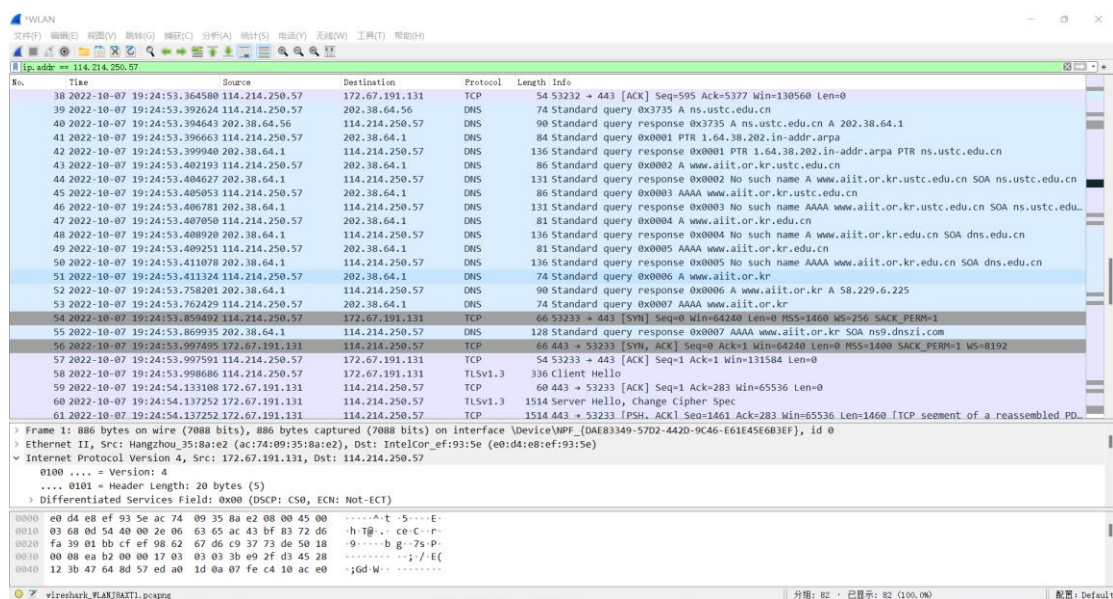
Step 7: 使用 nslookup www.aiit.or.kr bitsy.mit.edu 命令，并抓包
实验结果如下:


```
C:\Users\华为>
C:\Users\华为>nslookup www.ait.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
```

(图 1-19 实验结果)

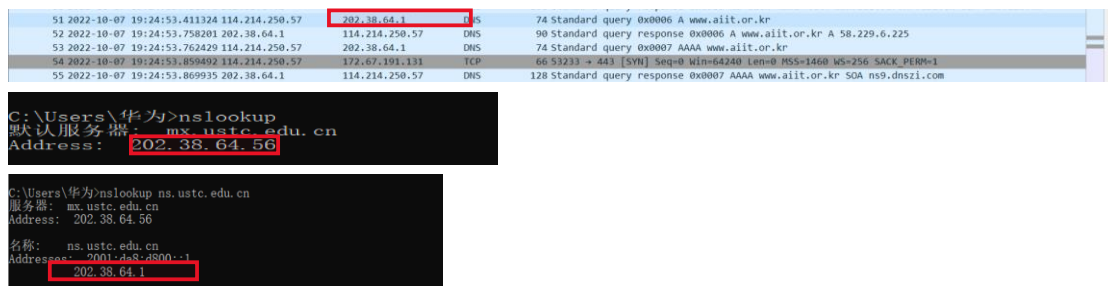
由于请求超时，故将 bitsy.mit.edu 换成 ns.ustc.edu.cn,实验结果如下：



(图 1-20 实验抓包结果)

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?

Ans: DNS 请求报文的目的地址为：202.38.64.1。默认本地 DNS 服务器的地址为：202.38.64.56。二者不一致。此 IP 地址与所选用的查询 DNS 服务器 ns.ustc.edu.cn 相对应。



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

Ans: DNS 请求报文的类型为 A 类型。它不含有任何“answers”。

51	2022-10-07 19:24:53.411324	114.214.250.57	202.38.64.1	DNS	74 Standard query 0x0006 A www.aiit
52	2022-10-07 19:24:53.758201	202.38.64.1	114.214.250.57	DNS	90 Standard query response 0x0006 A www.aiit.or.kr A 58.229.6.225
53	2022-10-07 19:24:53.762429	114.214.250.57	202.38.64.1	DNS	74 Standard query 0x0007 AAAA www.aiit.or.kr
54	2022-10-07 19:24:53.859492	114.214.250.57	172.67.191.131	TCP	66 53233 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
55	2022-10-07 19:24:53.869935	202.38.64.1	114.214.250.57	DNS	128 Standard query response 0x0007 AAAA www.aiit.or.kr SOA ns9.dnszi.com

```

> Frame 51: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
> Ethernet II, Src: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
> Internet Protocol Version 4, Src: 114.214.250.57, Dst: 202.38.64.1
> User Datagram Protocol, Src Port: 54287, Dst Port: 53
  > Domain Name System (query)
    Transaction ID: 0x0006
    > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    > Queries
      [Response In: 52]

```

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

Ans: DNS 响应报文提供了 1 个 answer，它包含了 www.aiit.or.kr 对应的 IP 地址（A 类型）。

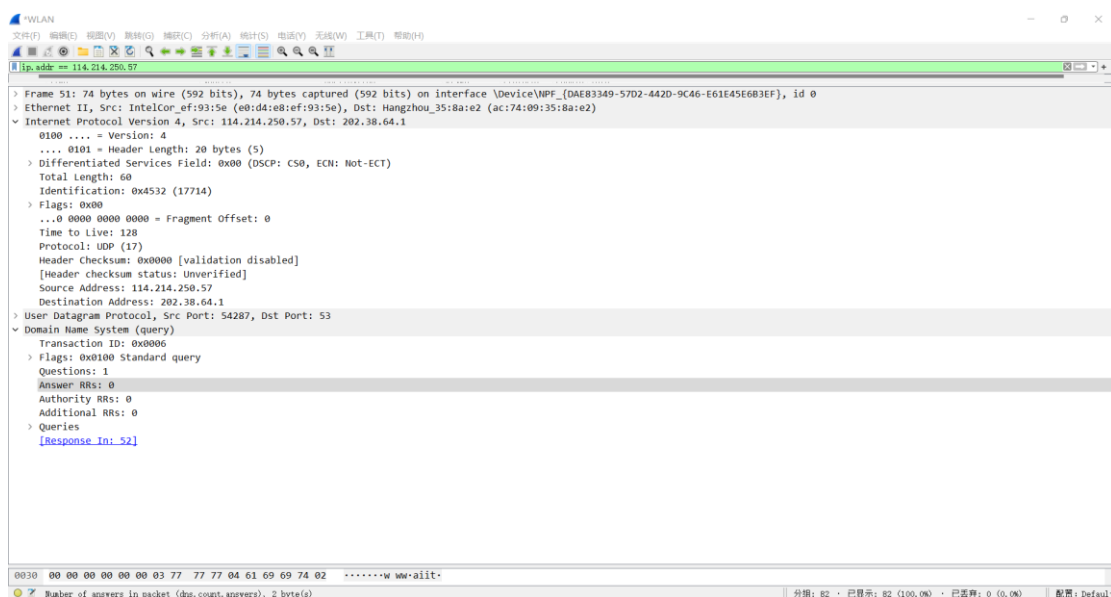
```

> Frame 52: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
> Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e)
> Internet Protocol Version 4, Src: 202.38.64.1, Dst: 114.214.250.57
> User Datagram Protocol, Src Port: 53, Dst Port: 54287
  > Domain Name System (response)
    Transaction ID: 0x0006
    > 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, addr 58.229.6.225
        [Request In: 51]
        [Time: 0.346877000 seconds]

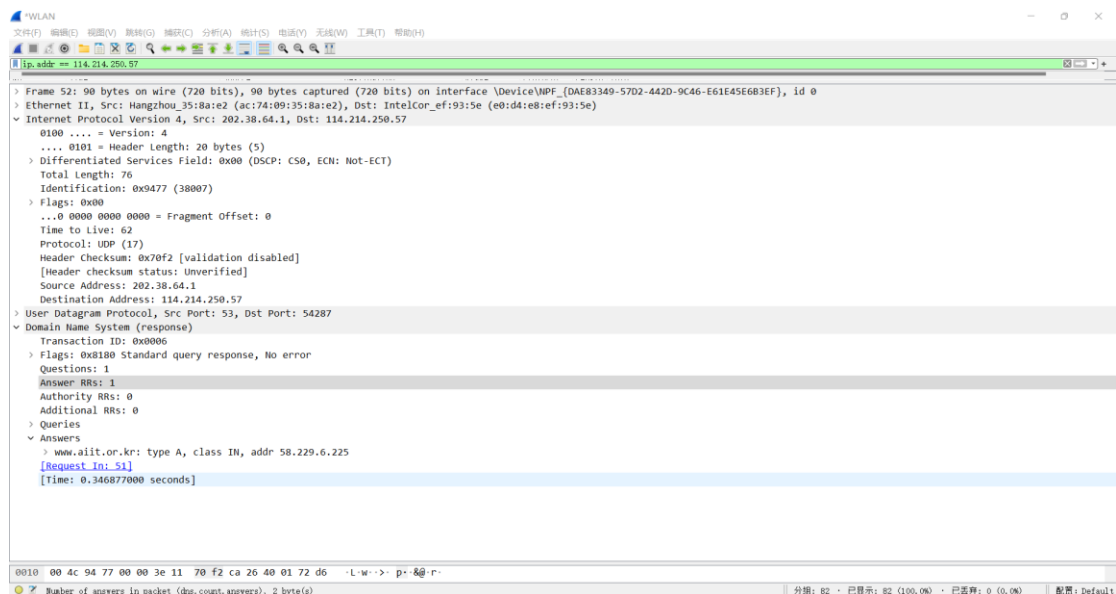
```

23. Provide a screenshot.

Ans: 如下图：



（图 1-21 DNS 请求报文内容）



(图 1-22 DNS 响应报文内容)

三、 补充内容：

DNS 客户端解析超时：

1) 在 NIC 上配置 1 个 DNS 服务器时

从 (开始开始的时间)	Action
0	客户端查询 DNS 服务器
1	如果在 1 秒后未收到响应，客户端将再次查询 DNS 服务器
2	如果在 1 秒后未收到响应，客户端将再次查询 DNS 服务器
4	如果在 2 秒后未收到响应，客户端将再次查询 DNS 服务器
8	如果在 4 秒后未收到响应，客户端将再次查询 DNS 服务器
10	如果在 2 秒后未收到响应，客户端将停止查询

2) 在 NIC 上配置 2 个 DNS 服务器时

从 (开始开始的时间)	Action
0	客户端查询列表的第一个 DNS 服务器
1	如果在 1 秒后未收到响应，客户端将查询列表的第二个 DNS 服务器
2	如果在 1 秒后未收到响应，客户端将再次查询列表的第二个 DNS 服务器
4	如果在 2 秒后未收到响应，客户端将同时查询列表中的所有服务器
8	如果在 4 秒后未收到响应，客户端将同时查询列表中的所有服务器
10	如果在 2 秒后未收到响应，客户端将停止查询

3) 在 NIC 上配置 3 个 DNS 服务器时

从 (开始开始的时间)	Action
0	客户端查询列表的第一个 DNS 服务器
1	如果在 1 秒后未收到响应，客户端将查询列表的第二个 DNS 服务器
2	如果在 1 秒后未收到响应，客户端将查询列表的第三个 DNS 服务器
4	如果在 2 秒后未收到响应，客户端将同时查询列表中的所有服务器
8	如果在 4 秒后未收到响应，客户端将再次同时查询列表中的所有服务器
10	如果在 2 秒后未收到响应，客户端将停止查询