

计算机网络DNS实验报告

PB19071535徐昊天

一.实验目的

- 深入了解域名系统 (DNS) 。
- 学习nslookup与ipconfig工具。
- 学习用wireshark追踪DNS。

二.实验环境与工具

- windows操作系统
- wireshark数据嗅探器
- Microsoft Edge浏览器

三.实验步骤

1.使用nslookup工具

nslookup工具允许主机查询任何指定的DNS服务器的DNS记录。 DNS服务器可以是根DNS服务器，顶级域DNS服务器，权威DNS服务器或中间DNS服务器。

需学习三个nslookup命令：

1.命令一

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

这个命令是说，请告诉我主机 www.mit.edu 的IP地址。此命令的响应提供两条信息：（1）提供响应的DNS服务器的名称和IP地址；（2）响应本身，即 www.mit.edu 的主机名和IP地址。

2.命令二

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

这个命令添加了选项"-type=NS"和域名"mit.edu"。这将使得nslookup将NS记录发送到默认的本地DNS服务器。

3.命令三

```
1 | nslookup www.aiit.or.kr bitsy.mit.edu
```

这个命令将查询请求发送到DNS服务器**bitsy.mit.edu**，而不是默认的DNS服务器（dns-prime.poly.edu）。

nslookup命令的一般语法如下：

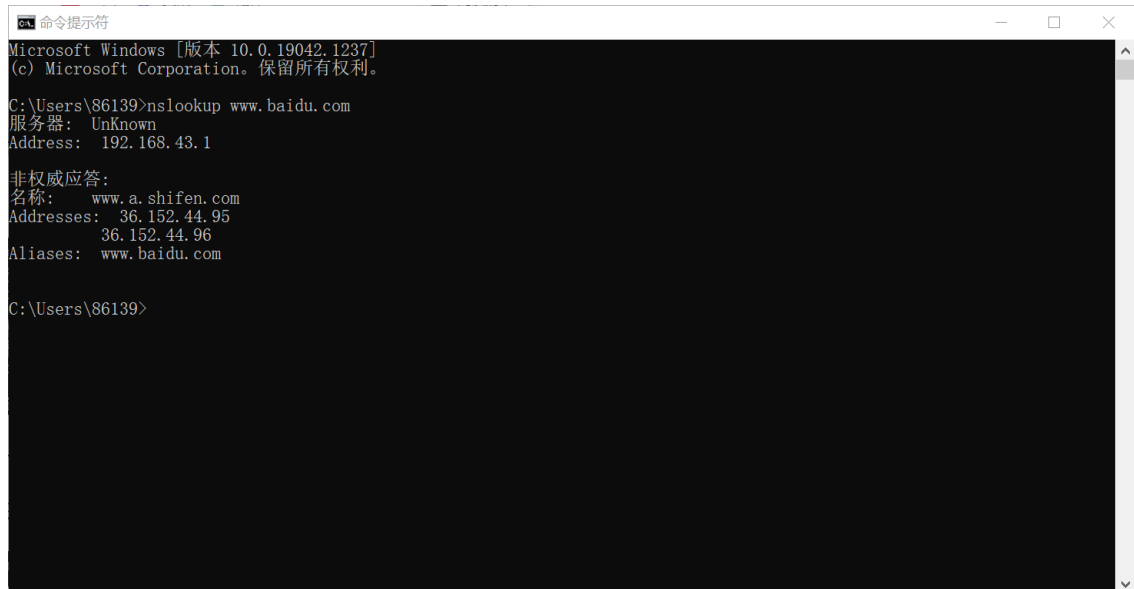
```
1 | nslookup -option1 -option2 host-to-find dns-server
```

nslookup可以不添加选项，或者添加一两个甚至更多选项。**dns-server**是可选的；如果这项没有提供，查询将发送到默认的本地DNS服务器。

执行以下操作：

1. 运行nslookup以获取一个亚洲的Web服务器的IP地址。该服务器的IP地址是什么？

答：利用nslookup获取www.baidu.comWeb服务器的IP地址如下图所示：



```
命令提示符
Microsoft Windows [版本 10.0.19042.1237]
(c) Microsoft Corporation。保留所有权利。

C:\Users\86139>nslookup www.baidu.com
服务器:  Unknown
Address:  192.168.43.1

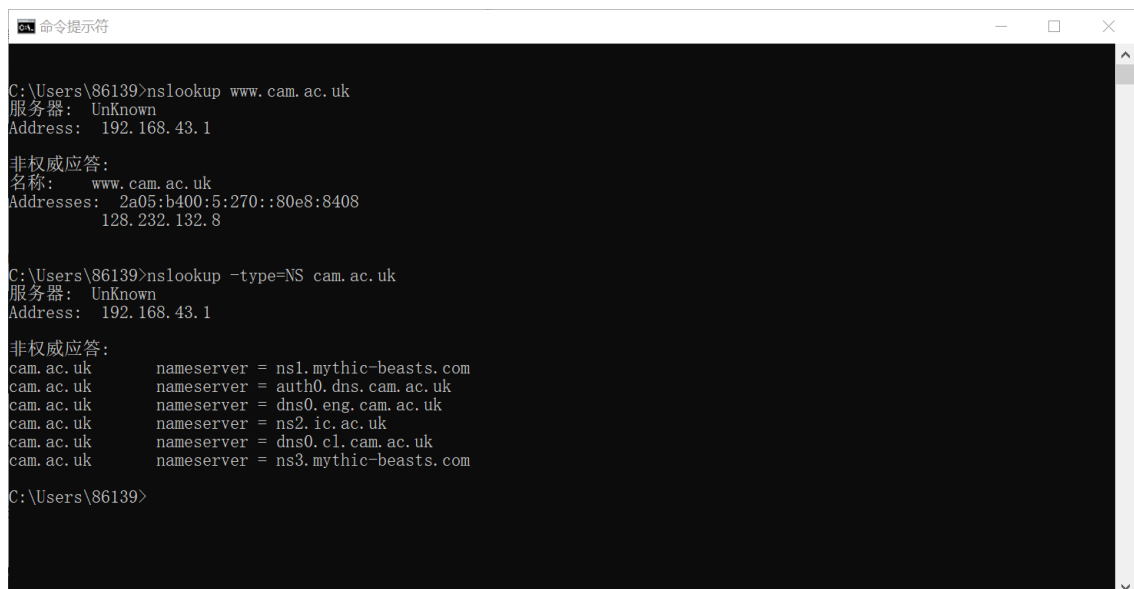
非权威应答:
名称:      www.a.shifen.com
Addresses:  36.152.44.95
            36.152.44.96
Aliases:    www.baidu.com

C:\Users\86139>
```

由图可知，该服务器的IP地址为36.152.44.95或36.152.44.96。

2. 运行nslookup来确定一个欧洲的大学的权威DNS服务器。

答：利用nslookup确定剑桥大学如下图所示：



```
命令提示符

C:\Users\86139>nslookup www.cam.ac.uk
服务器:  Unknown
Address:  192.168.43.1

非权威应答:
名称:      www.cam.ac.uk
Addresses:  2a05:b400:5:270::80e8:8408
            128.232.132.8

C:\Users\86139>nslookup -type=NS cam.ac.uk
服务器:  Unknown
Address:  192.168.43.1

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

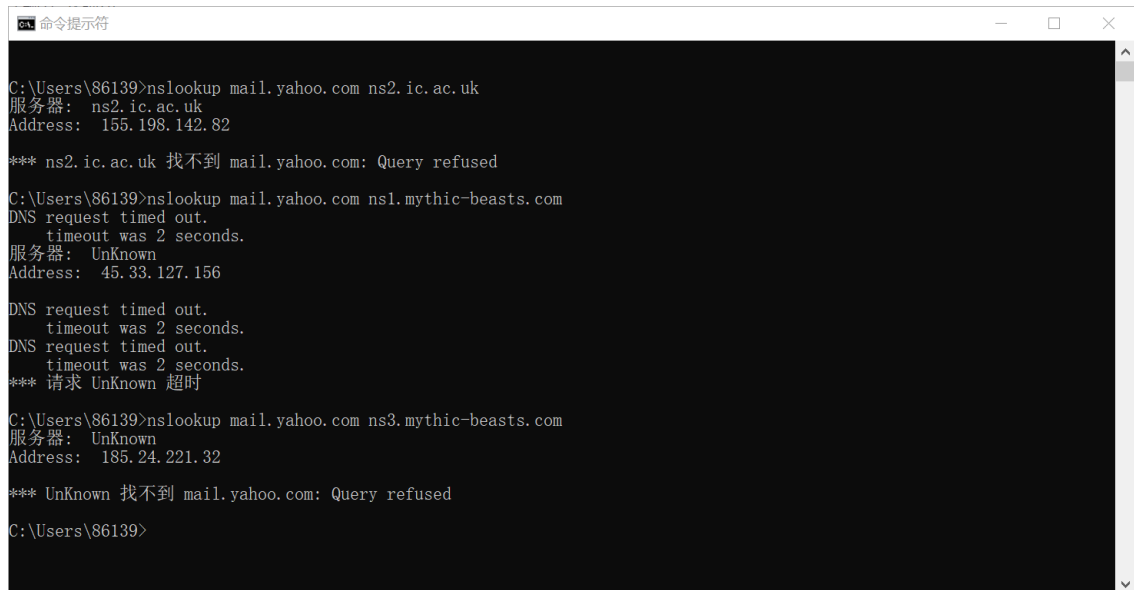
C:\Users\86139>
```

故剑桥大学权威DNS服务器如下：

- ns1.mythic-beasts.com
- auth0.dns.cam.ac.uk
- dns0.eng.cam.ac.uk
- ns2.ic.ac.uk
- dns0.cl.cam.ac.uk
- ns3.mythic-beasts.com

3. 运行`nslookup`，使用问题2中一个已获得的DNS服务器，来查询Yahoo!邮箱的邮件服务器。它的IP地址是什么？

答：使用问题2中获得的DNS服务器查询Yahoo! 邮箱邮件服务器结果如下图所示：



```
命令提示符
C:\Users\86139>nslookup mail.yahoo.com ns2.ic.ac.uk
服务器: ns2.ic.ac.uk
Address: 155.198.142.82

*** ns2.ic.ac.uk 找不到 mail.yahoo.com: Query refused

C:\Users\86139>nslookup mail.yahoo.com ns1.mythic-beasts.com
DNS request timed out.
    timeout was 2 seconds.
服务器: UnKnown
Address: 45.33.127.156

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

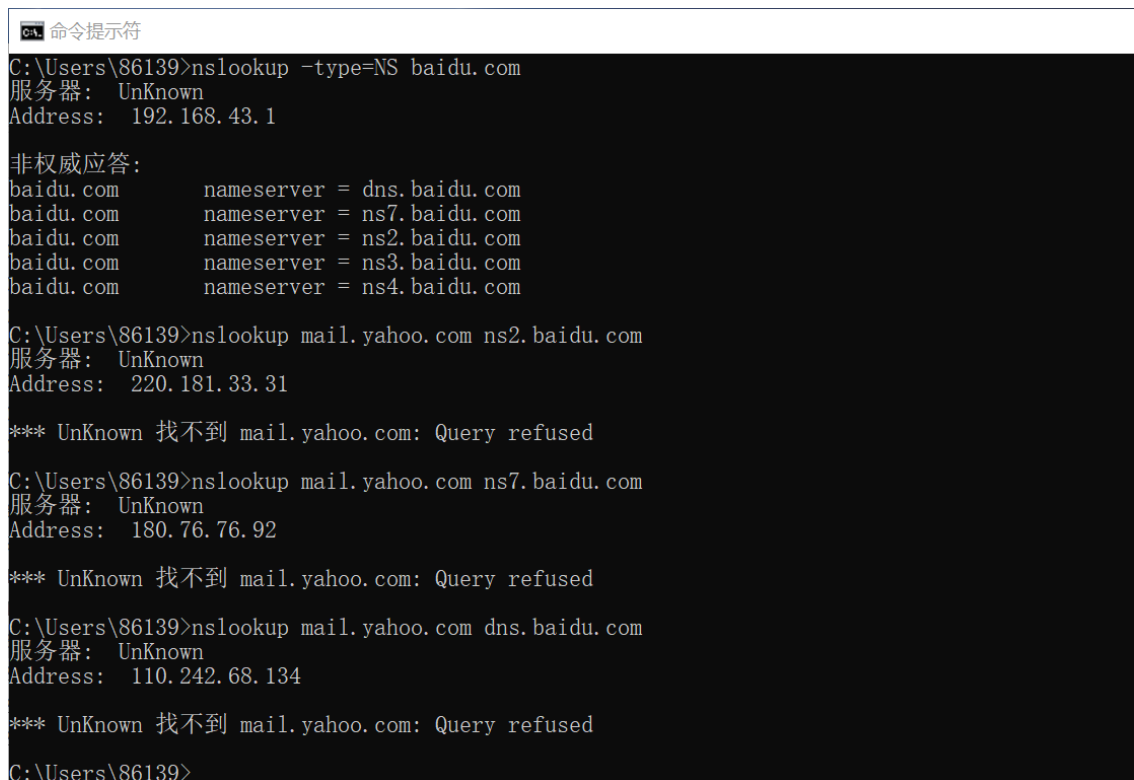
C:\Users\86139>nslookup mail.yahoo.com ns3.mythic-beasts.com
服务器: UnKnown
Address: 185.24.221.32

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

C:\Users\86139>
```

如上图所示，剑桥大学DNS服务器无法用来查询Yahoo!邮箱的邮件服务器。

使用**百度**的DNS服务器查询如下图所示：



```
命令提示符
C:\Users\86139>nslookup -type=NS baidu.com
服务器: UnKnown
Address: 192.168.43.1

非权威应答:
baidu.com      nameserver = dns.baidu.com
baidu.com      nameserver = ns7.baidu.com
baidu.com      nameserver = ns2.baidu.com
baidu.com      nameserver = ns3.baidu.com
baidu.com      nameserver = ns4.baidu.com

C:\Users\86139>nslookup mail.yahoo.com ns2.baidu.com
服务器: UnKnown
Address: 220.181.33.31

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

C:\Users\86139>nslookup mail.yahoo.com ns7.baidu.com
服务器: UnKnown
Address: 180.76.76.92

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

C:\Users\86139>nslookup mail.yahoo.com dns.baidu.com
服务器: UnKnown
Address: 110.242.68.134

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

C:\Users\86139>
```

如上图所示，依然无法查询成功。

直接用`nslookup`与`ping`查询IP地址如下图所示：

```
命令提示符
C:\Users\86139>nslookup mail.yahoo.com
服务器:  UnKnown
Address:  192.168.43.1

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

C:\Users\86139>ping mail.yahoo.com

正在 Ping edge.gycpi.b.yahoodns.net [69.147.88.7] 具有 32 字节的数据:
来自 69.147.88.7 的回复: 字节=32 时间=260ms TTL=48
来自 69.147.88.7 的回复: 字节=32 时间=236ms TTL=48
来自 69.147.88.7 的回复: 字节=32 时间=218ms TTL=48
来自 69.147.88.7 的回复: 字节=32 时间=255ms TTL=48

69.147.88.7 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 218ms, 最长 = 260ms, 平均 = 242ms

C:\Users\86139>
```

如上图所示，雅虎邮箱IP地址为69.147.88.7。

2.使用ipconfig工具

ipconfig对于调试网络问题非常实用，可用于显示当前的TCP/IP信息，包括地址，DNS服务器地址，适配器类型等。

可通过命令提示符使用：

1.命令一

```
1 | ipconfig /all
```

所有关于主机的信息都将显示于终端。

2.命令二

```
1 | ipconfig /displaydns
```

ipconfig可用于管理主机中存储的DNS信息，以上命令可用于查看缓存记录。

3.命令三

```
1 | ipconfig /flushdns
```

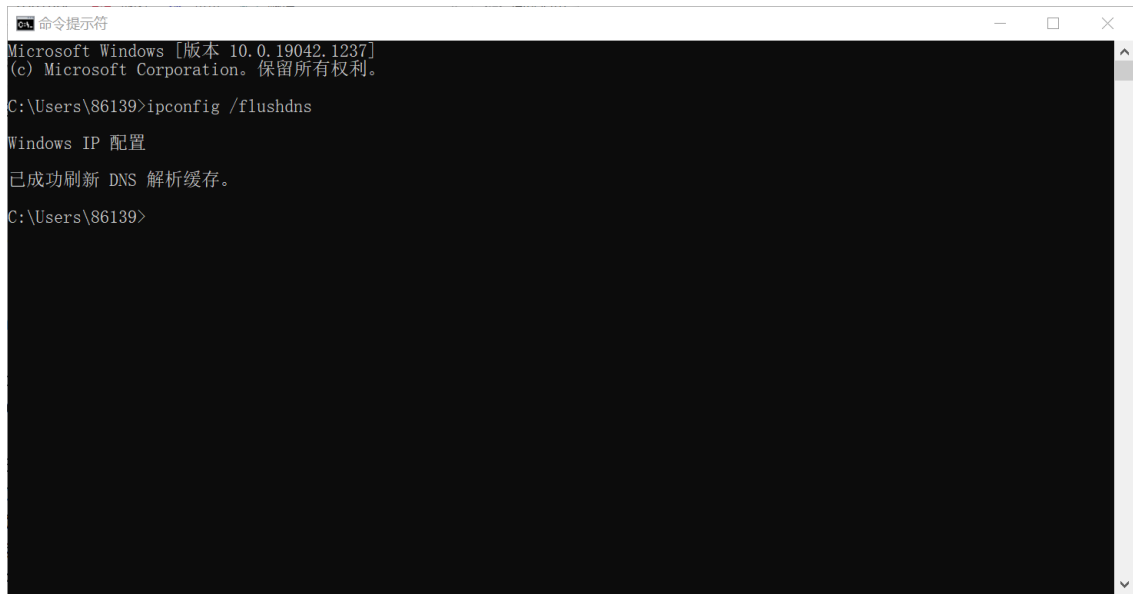
用于清除缓存。

3.使用Wireshark追踪DNS

捕获一些由常规上网活动生成的DNS数据包。

1. 使用ipconfig清空主机中的DNS缓存。

得到终端界面如下图：



```
命令提示符
Microsoft Windows [版本 10.0.19042.1237]
(c) Microsoft Corporation。保留所有权利。

C:\Users\86139>ipconfig /flushdns

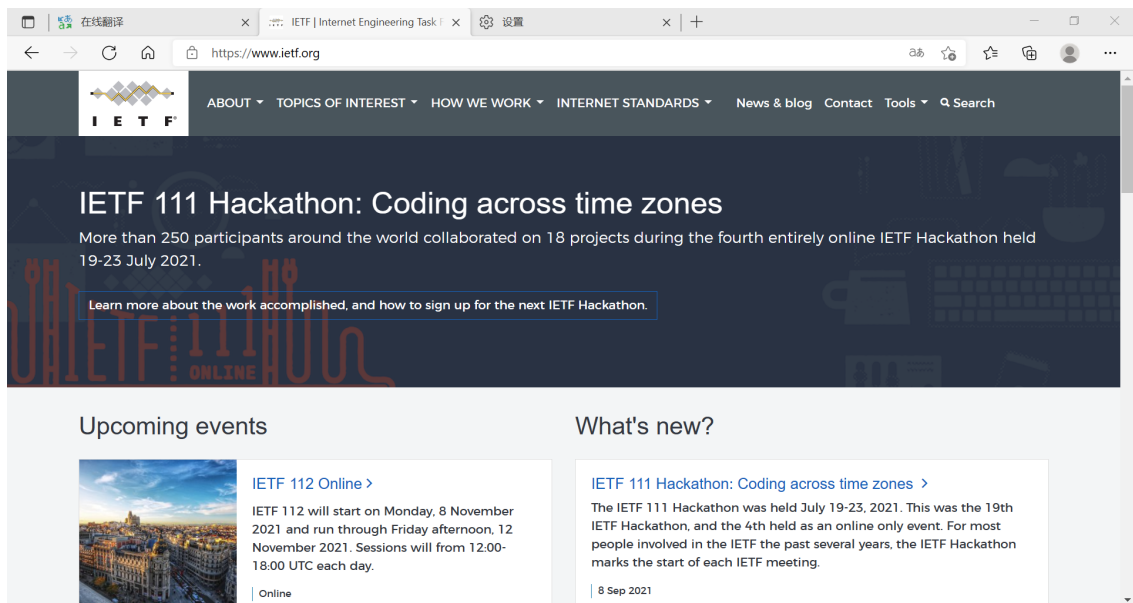
Windows IP 配置

已成功刷新 DNS 解析缓存。

C:\Users\86139>
```

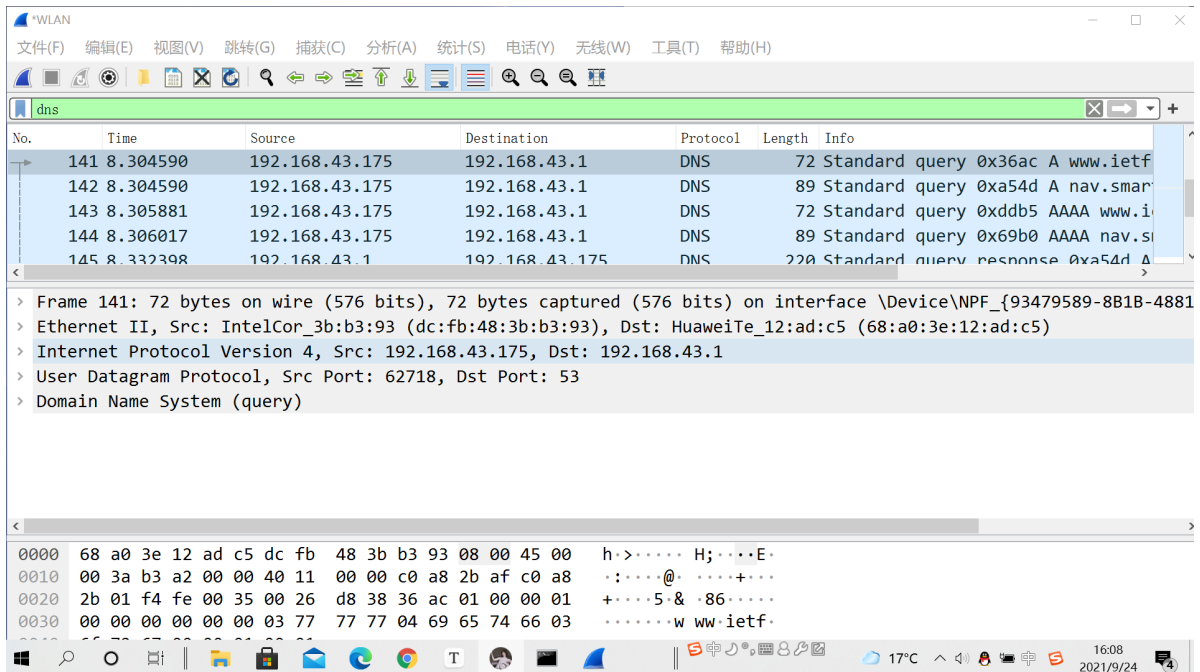
2. 打开浏览器并清空浏览器缓存。
3. 打开Wireshark，然后在过滤器中输入“**ip.addr==your_IP_address**”。
4. 在Wireshark中启动数据包捕获。
5. 使用浏览器访问网页：<http://www.ietf.org>。

得到界面如下图：



6. 停止数据包捕获。

抓包结束后，wireshark界面如下图所示：

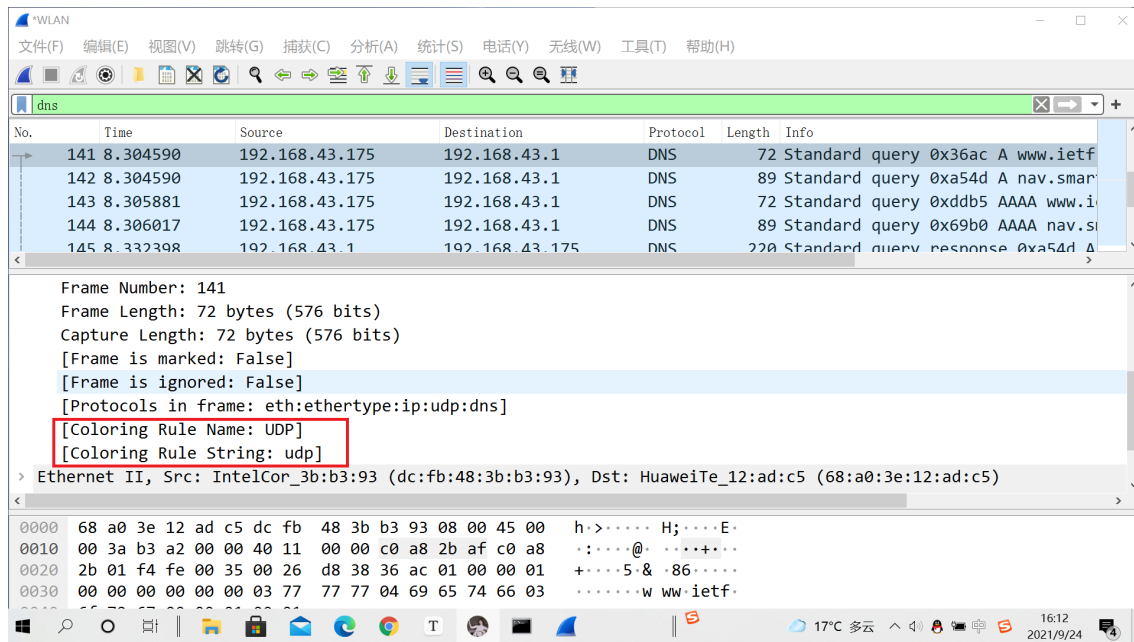


回答如下问题：

4. 找到DNS查询和响应报文。它们是否通过UDP或TCP发送？

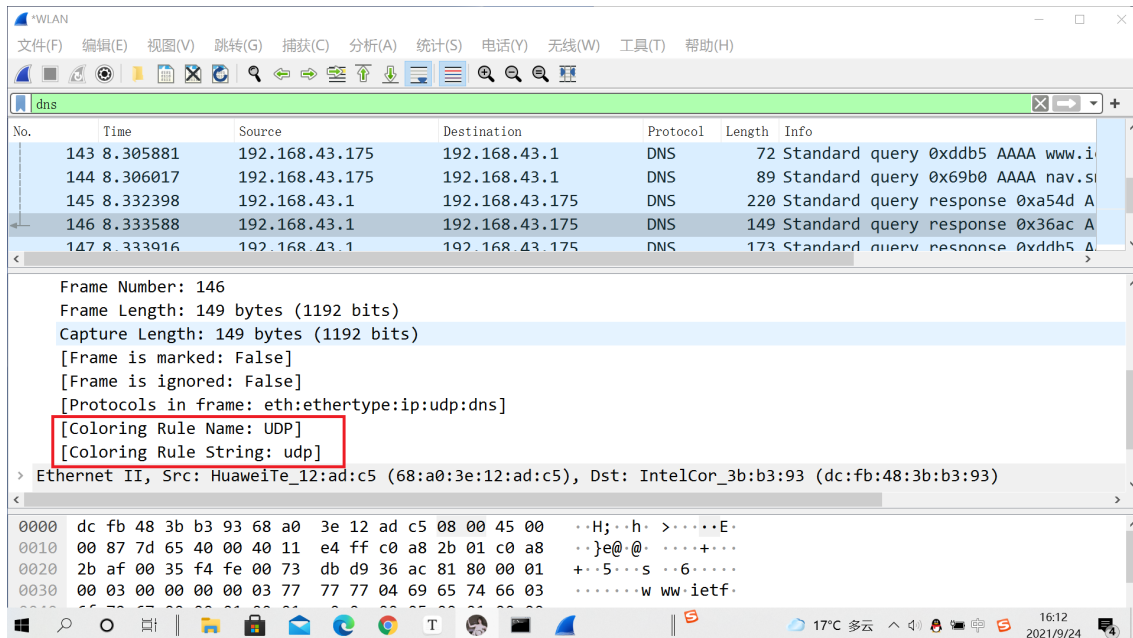
答：

①DNS查询报文信息如下图所示：



根据红色框中信息可知，查询报文由UDP发送。

②DNS响应报文信息如下图所示：

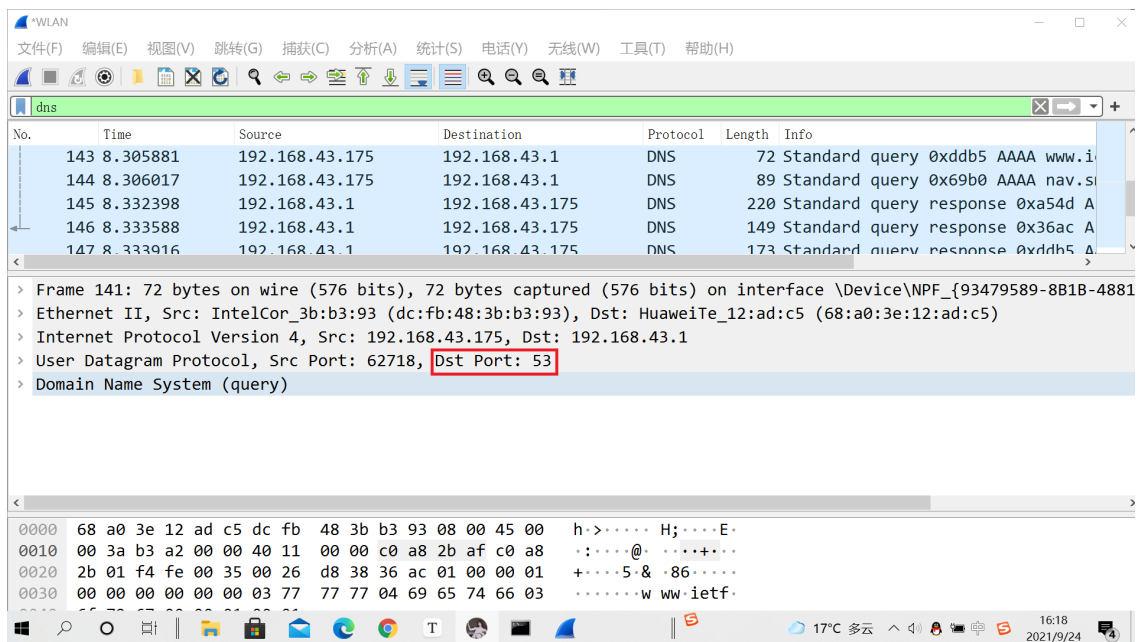


根据红色框中信息可知，响应报文由UDP发送。

5. DNS查询报文的目标端口是什么？DNS响应报文的源端口是什么？

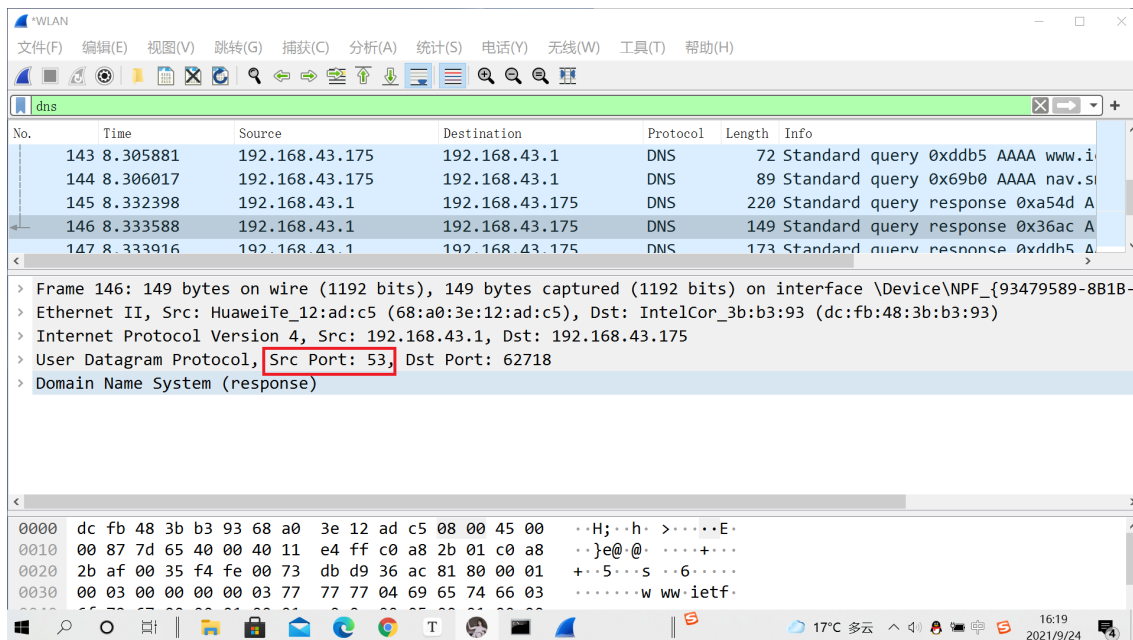
答：

①DNS查询报文信息如下图所示：



根据红色框中信息可知，查询报文的目标端口为53。

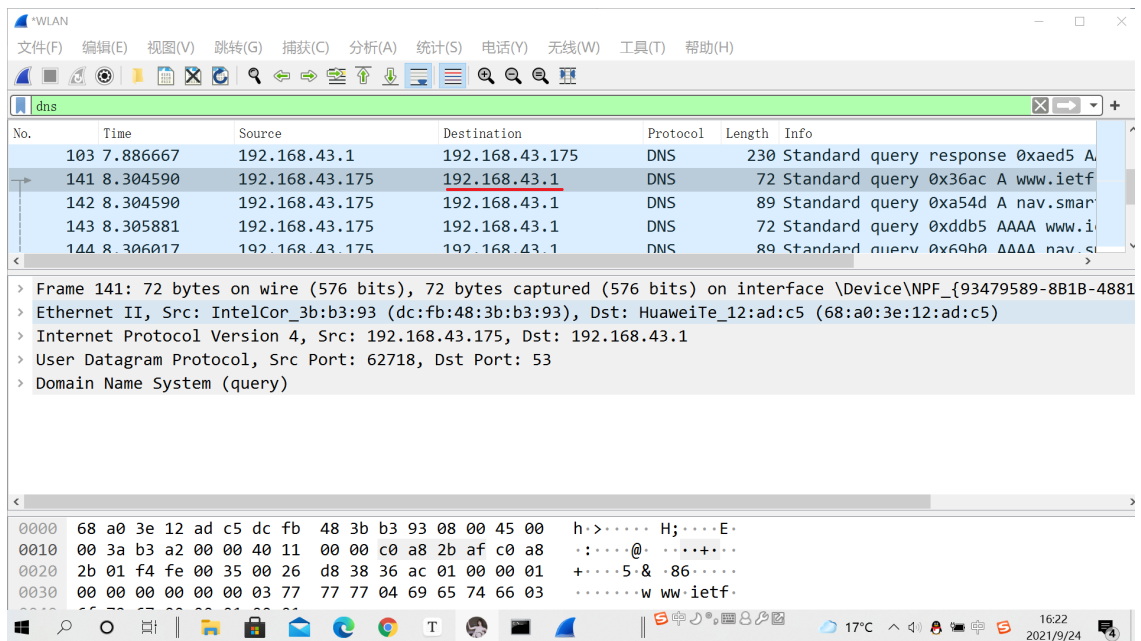
②DNS响应报文信息如下图所示：



根据红色框中信息可知，响应报文的源端口为53。

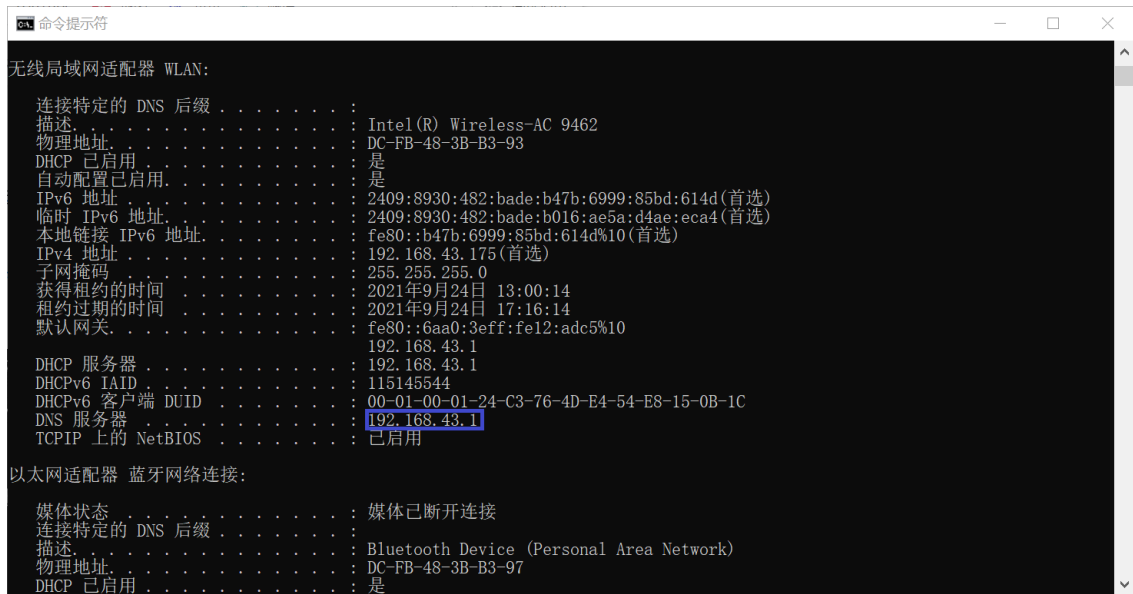
6. DNS查询报文发送到哪个IP地址？使用ipconfig来确定本地DNS服务器的IP地址。这两个IP地址是否相同？

答：DNS查询报文信息如下图所示：



如红色横线部分所示，DNS查询消息发送到的IP地址为192.168.43.1

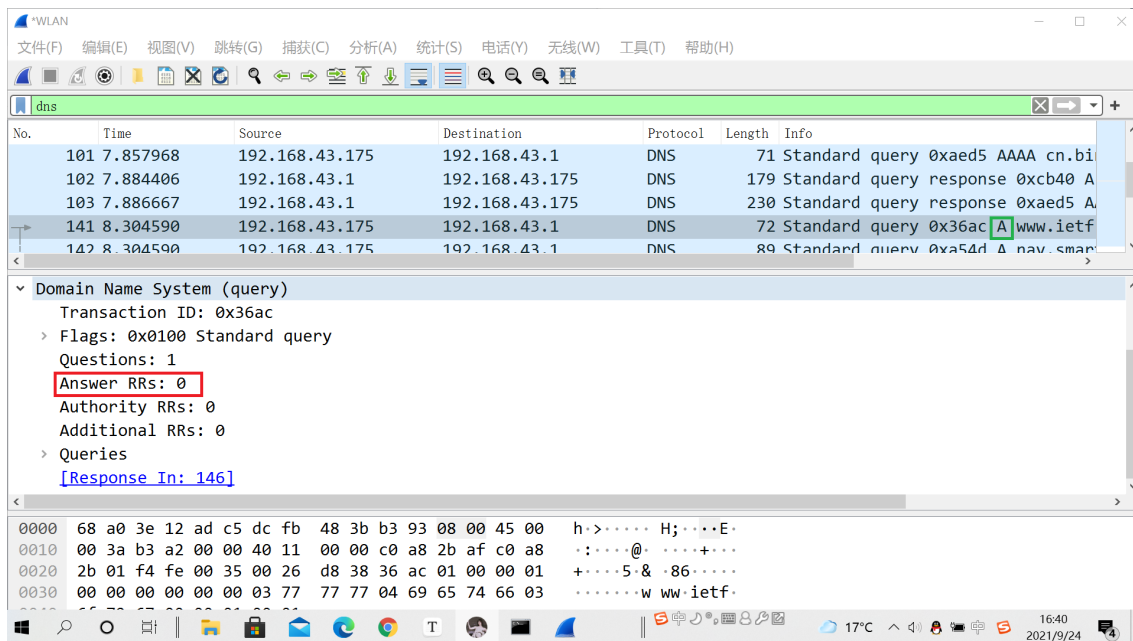
在命令中输入ipconfig /all得到下图：



由蓝色框中读取出本地DNS服务器的IP地址为：192.168.43.1，两者相同。

7. 检查DNS查询报文。DNS查询是什么"Type"的？查询报文是否包含任何"answers"？

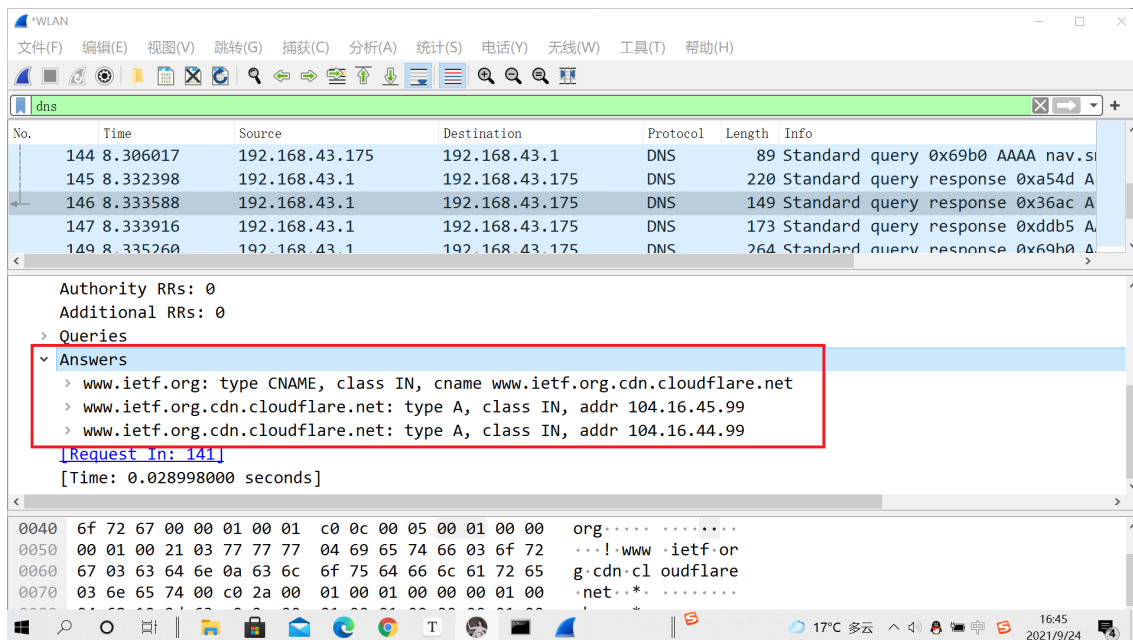
答：DNS查询报文如下图所示：



由上图绿色框中信息可知，Type为“A”；由红色框中信息可知，查询报文中不含任何“answers”。

8. 检查DNS响应报文。提供了多少个"answers"？这些答案具体包含什么？

答：DNS响应报文如下图所示：



由上图红色框中所示，响应报文提供了三个“answers”。

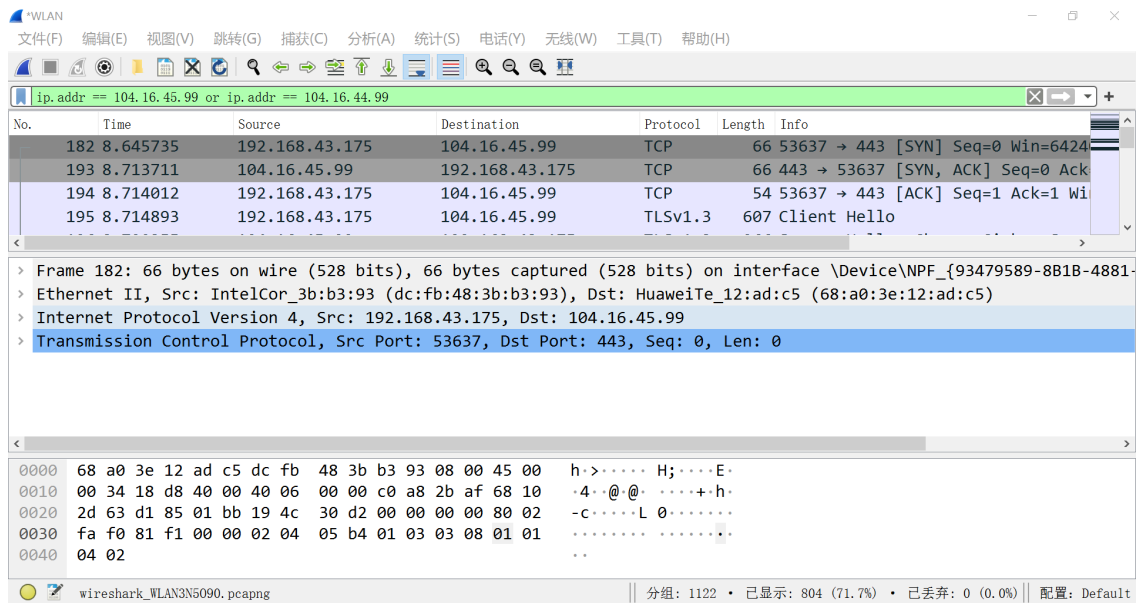
三个answer包含的信息分别如下图所示：

- v 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: 1 (1 second)
 Data length: 33
 CNAME: www.ietf.org.cdn.cloudflare.net
- v 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: 1 (1 second)
 Data length: 4
 Address: 104.16.45.99
- v 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: 1 (1 second)
 Data length: 4
 Address: 104.16.44.99

具体包含了“Name”、“Type”、“Class”、“Time to live”、“Data length”、“Address”等内容。

9. 考虑从您主机发送的后续TCP SYN数据包。SYN数据包的目的IP地址是否与DNS响应消息中提供的任何IP地址相对应？

答：根据IP地址筛选数据包如下图所示：



由图中182号数据包可知，SYN数据包的目的IP地址与DNS响应消息中提供的IP地址相对应。

10. 这个网页包含一些图片。在获取每个图片前，您的主机是否都发出了新的DNS查询？

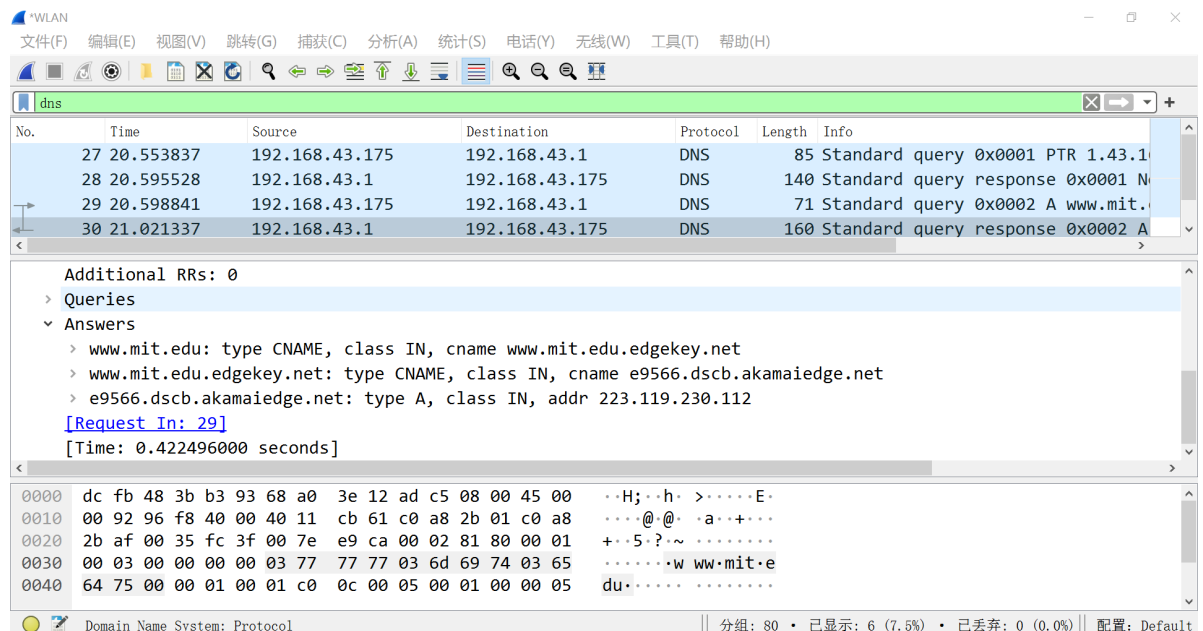
答：否。本机 DNS 已经被缓存了，因此不需要发起新的 DNS 查询。

使用nslookup进行抓包

第一部分

1. 启动数据包捕获。
2. 使用nslookup查询www.mit.edu。
3. 停止数据包捕获。

抓包结束后wireshark界面如下图所示：

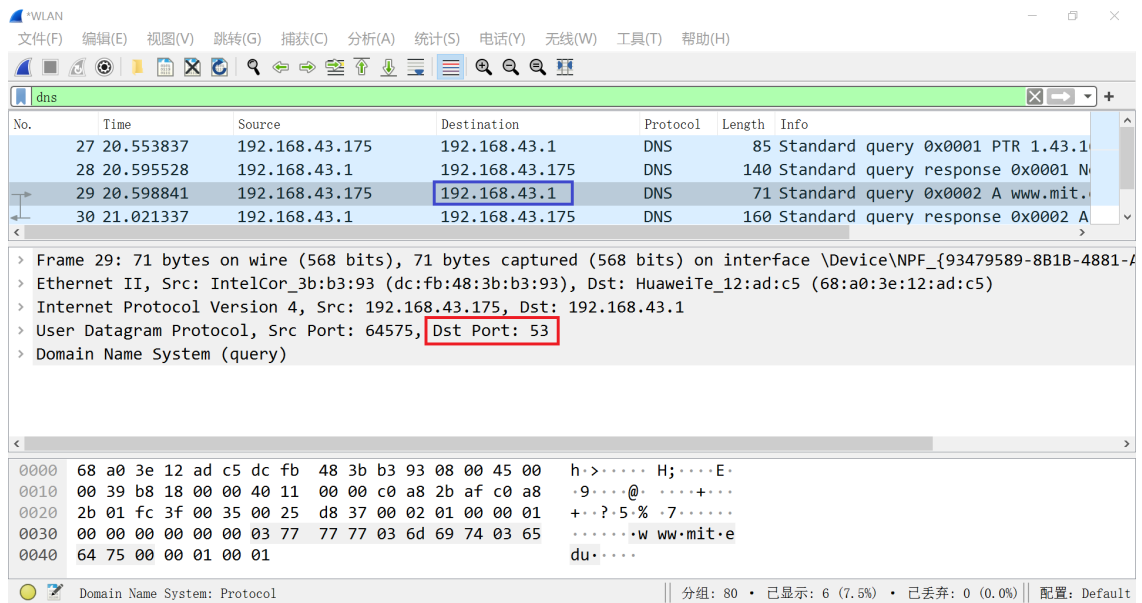


回答如下问题：

11. DNS查询报文的目标端口是什么？ DNS响应报文的源端口是什么？

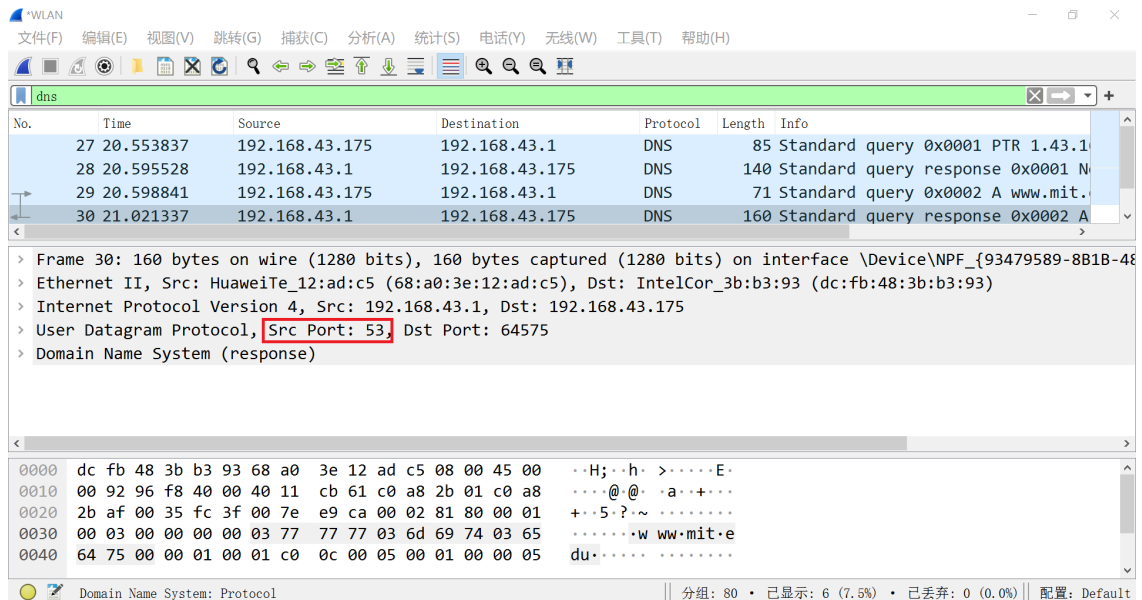
答：

①DNS查询报文的信息如下图所示：



根据上图中红色框中信息可知，DNS查询报文的目标端口为53。

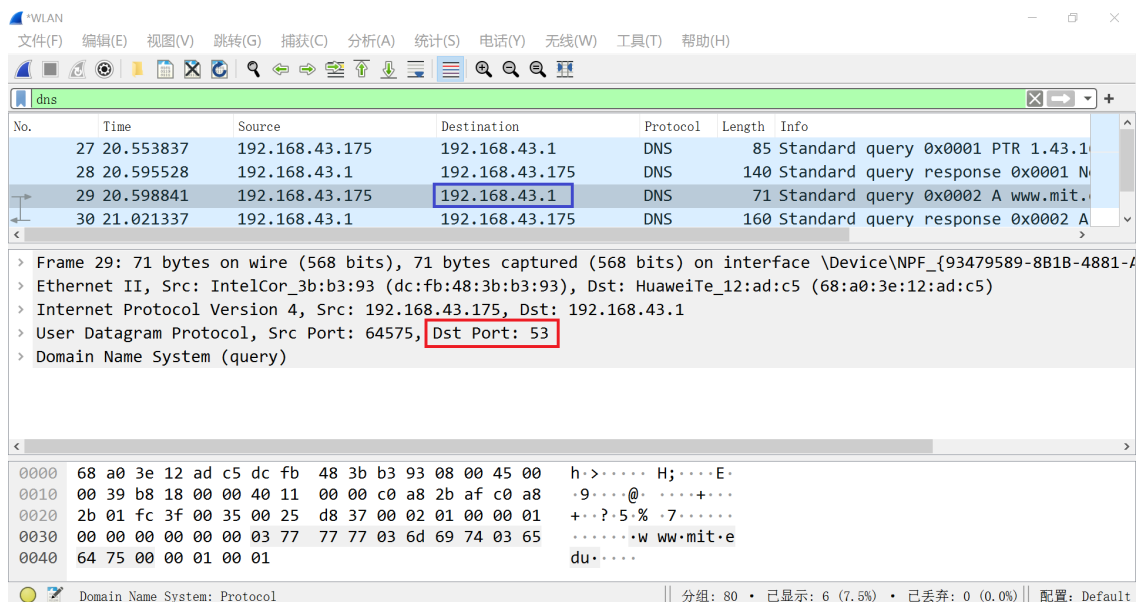
②DNS响应报文的信息如下图所示：



根据上图中红色框中信息可知，DNS响应报文的源端口为53。

12. DNS查询报文的目标IP地址是什么？这是你的默认本地DNS服务器的IP地址吗？

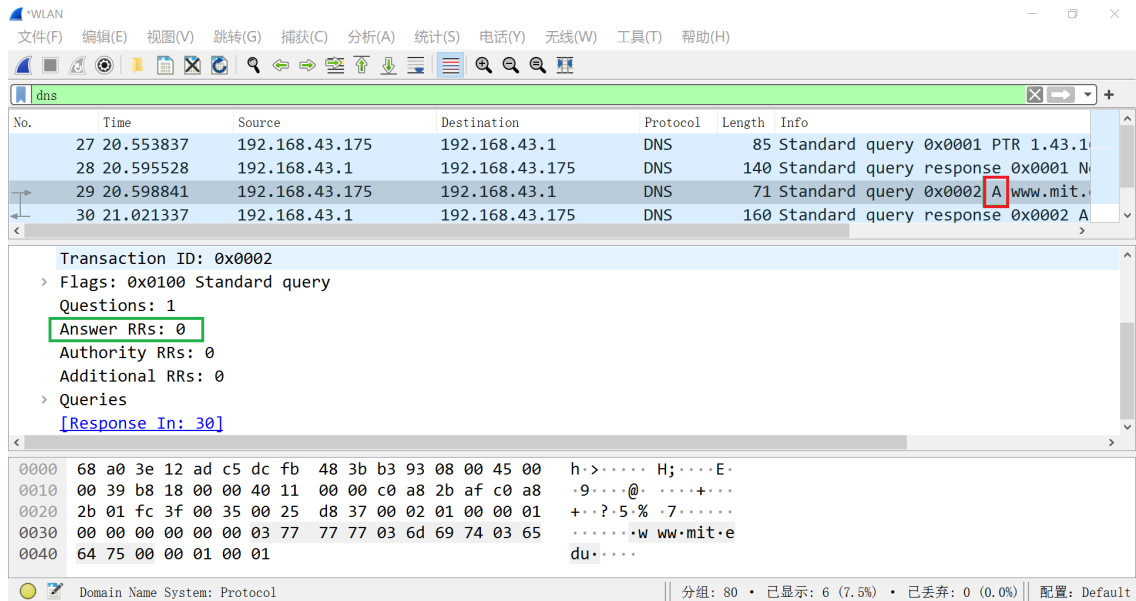
答：DNS查询报文信息如下图所示：



如上图蓝色框中所示，DNS查询报文的目标IP地址是192.168.43.1，根据第6题可知这是我的默认本地DNS服务器的IP地址。

13. 检查DNS查询报文。DNS查询是什么"Type"的？查询消息是否包含任何"answers"？

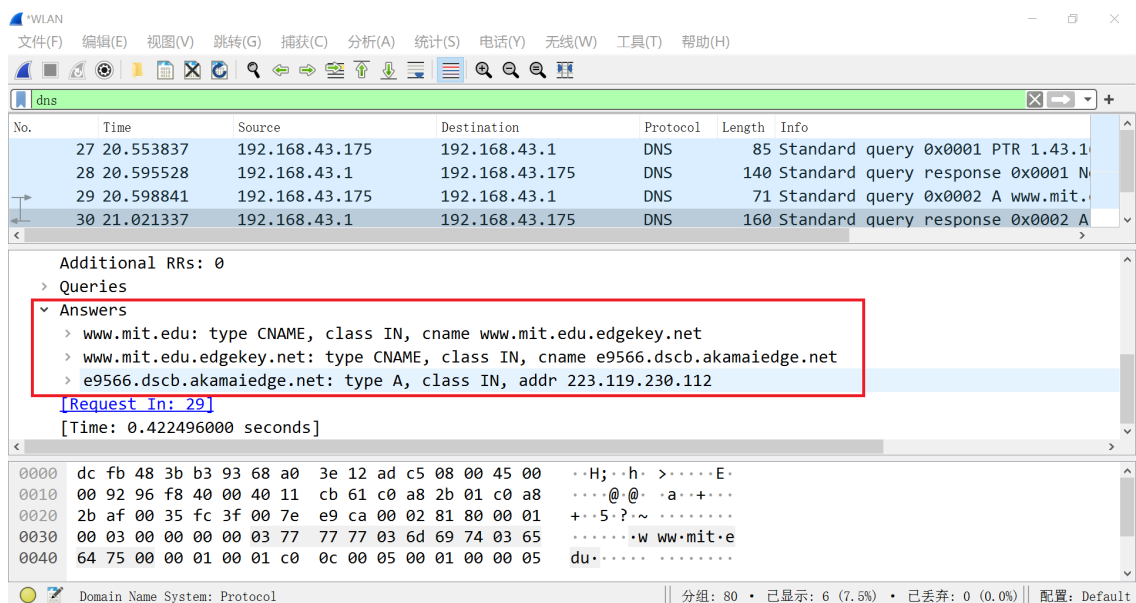
答：DNS查询报文的信息如下图所示：



如上图红色框中所示，DNS查询的"Type"是"A"；根据绿色框中所示，查询消息中未包含任何"answers"。

14. 检查DNS响应报文。提供了多少个"answers"？这些答案包含什么？

答：DNS响应报文的信息如下图所示：



根据上图红色框中，可知响应报文提供了3个"answers"。

三个answer包含的信息分别如下图所示：

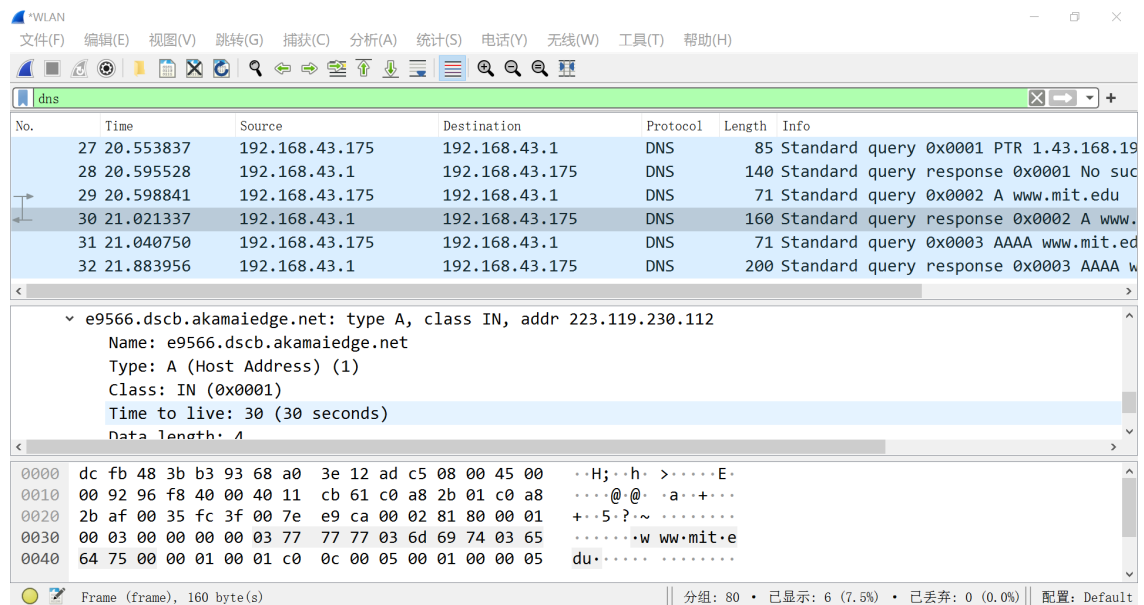
- www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
Name: www.mit.edu
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 1469 (24 minutes, 29 seconds)
Data length: 25
CNAME: www.mit.edu.edgekey.net

- 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 223.119.230.112
Name: e9566.dscb.akamaiedge.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 30 (30 seconds)
Data length: 4
Address: 223.119.230.112

具体包含了“Name”、“Type”、“Class”、“Time to live”、“Data length”、“Address”等内容。

15. 提供屏幕截图。

答：屏幕截图如下：



第二部分

1. 启动数据包捕获。
2. 输入命令 **nslookup -type=NS mit.edu**。
3. 停止数据包捕获。

抓包结束后wireshark界面如下图所示：

No.	Time	Source	Destination	Protocol	Length	Info
54	2.876746	192.168.43.1	192.168.43.175	DNS	107	Standard query response 0xae4b A
57	2.887218	192.168.43.1	192.168.43.175	DNS	107	Standard query response 0xae4b A
169	3.670349	192.168.43.175	192.168.43.1	DNS	85	Standard query 0x0001 PTR 1.43.1
171	3.688972	192.168.43.1	192.168.43.175	DNS	120	Standard query response 0x0001 N
173	3.695188	192.168.43.175	192.168.43.1	DNS	67	Standard query 0x0002 NS mit.edu
181	3.759620	192.168.43.1	192.168.43.175	DNS	234	Standard query response 0x0002 N

> Frame 39: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface \Device\NPF_{93479589-8B1B-4881-A...
 > Ethernet II, Src: IntelCor_3b:b3:93 (dc:fb:48:3b:b3:93), Dst: HuaweiTe_12:ad:c5 (68:a0:3e:12:ad:c5)
 > Internet Protocol Version 4, Src: 192.168.43.175, Dst: 192.168.43.1
 > User Datagram Protocol, Src Port: 50551, Dst Port: 53
 > Domain Name System (query)

0000 68 a0 3e 12 ad c5 dc fb 48 3b b3 93 08 00 45 00 h>.....H;....E.
 0010 00 41 57 ef 00 00 40 11 00 00 c0 a8 2b af c0 a8 .AW...@.+..
 0020 2b 01 c5 77 00 35 00 2d d8 3f 17 ed 01 00 00 01 +..w.5.- .?.....

Domain Name System: Protocol | 分组: 209 • 已显示: 11 (5.3%) • 已丢弃: 0 (0.0%) | 配置: Default

回答下列问题：

16. DNS查询报文发送到的IP地址是什么？这是您的默认本地DNS服务器的IP地址吗？

答：DNS查询报文的信息如下图所示：

No.	Time	Source	Destination	Protocol	Length	Info
54	2.876746	192.168.43.1	192.168.43.175	DNS	107	Standard query response 0xae4b A
57	2.887218	192.168.43.1	192.168.43.175	DNS	107	Standard query response 0xae4b A
169	3.670349	192.168.43.175	192.168.43.1	DNS	85	Standard query 0x0001 PTR 1.43.1
171	3.688972	192.168.43.1	192.168.43.175	DNS	120	Standard query response 0x0001 N
173	3.695188	192.168.43.175	192.168.43.1	DNS	67	Standard query 0x0002 NS mit.edu
181	3.759620	192.168.43.1	192.168.43.175	DNS	234	Standard query response 0x0002 N

> Frame 39: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface \Device\NPF_{93479589-8B1B-4881-A...
 > Ethernet II, Src: IntelCor_3b:b3:93 (dc:fb:48:3b:b3:93), Dst: HuaweiTe_12:ad:c5 (68:a0:3e:12:ad:c5)
 > Internet Protocol Version 4, Src: 192.168.43.175, Dst: 192.168.43.1
 > User Datagram Protocol, Src Port: 50551, Dst Port: 53
 > Domain Name System (query)

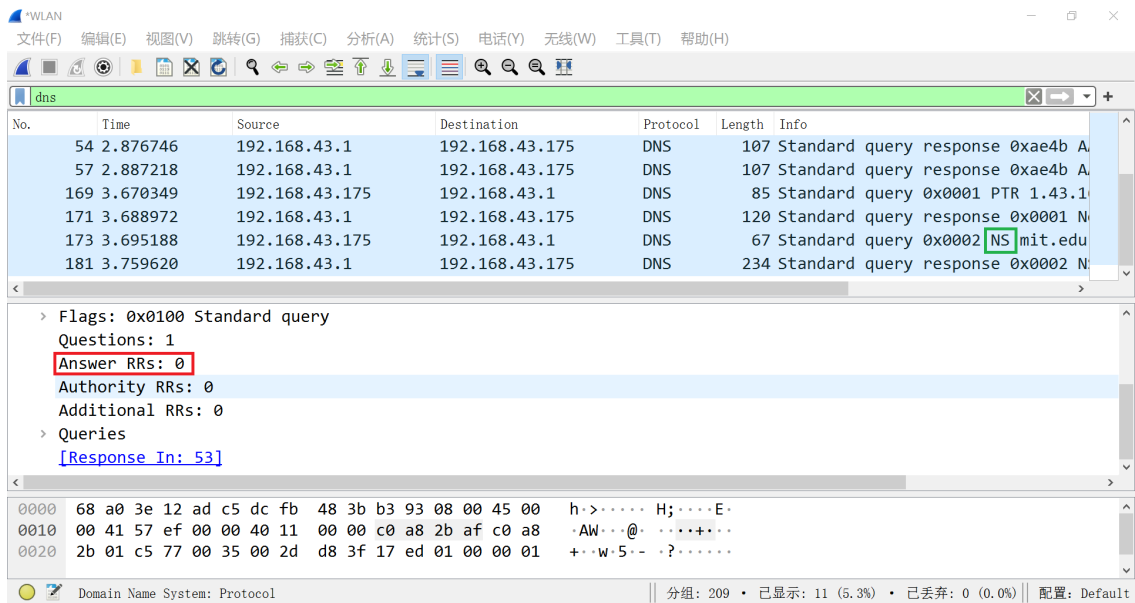
0000 68 a0 3e 12 ad c5 dc fb 48 3b b3 93 08 00 45 00 h>.....H;....E.
 0010 00 41 57 ef 00 00 40 11 00 00 c0 a8 2b af c0 a8 .AW...@.+..
 0020 2b 01 c5 77 00 35 00 2d d8 3f 17 ed 01 00 00 01 +..w.5.- .?.....

Domain Name System: Protocol | 分组: 209 • 已显示: 11 (5.3%) • 已丢弃: 0 (0.0%) | 配置: Default

根据上图红色框中信息可知，DNS查询报文发送的IP地址是192.168.43.1，这是我的默认本地DNS服务器的IP地址。

17. 检查DNS查询报文。DNS查询是什么"Type"的？查询报文是否包含任何"answers"？

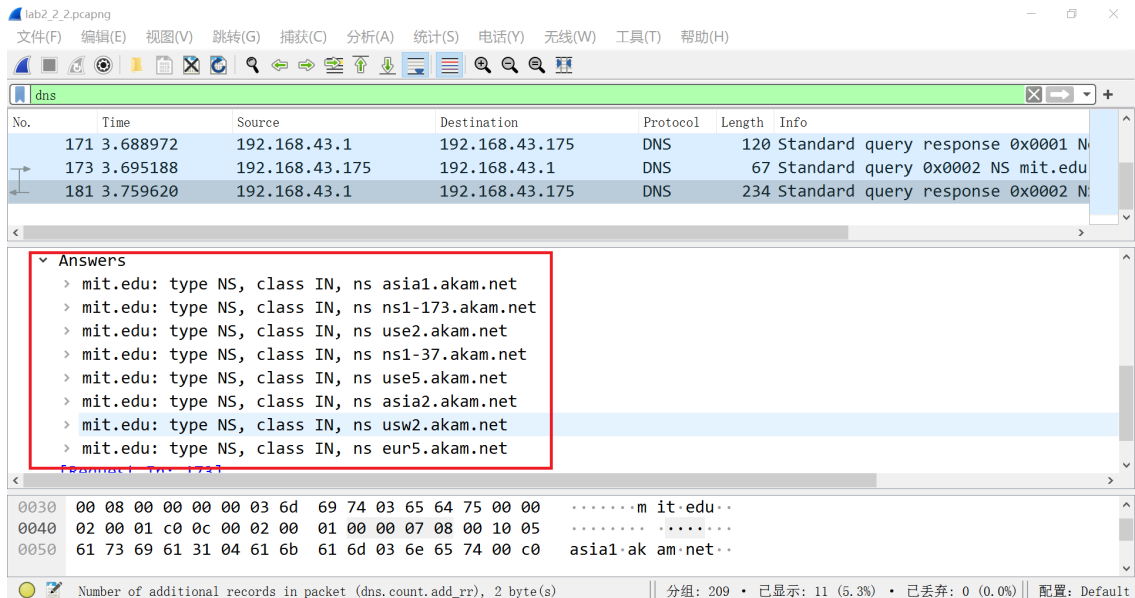
答：DNS查询报文信息如下图所示：



根据绿色框中信息可知DNS查询的“Type”是“NS”；查询报文不含任何“answers”。

18. 检查DNS响应报文。响应报文提供的MIT域名服务器是什么？此响应报文还提供了MIT域名服务器的IP地址吗？

答：DNS响应报文信息如下图所示：



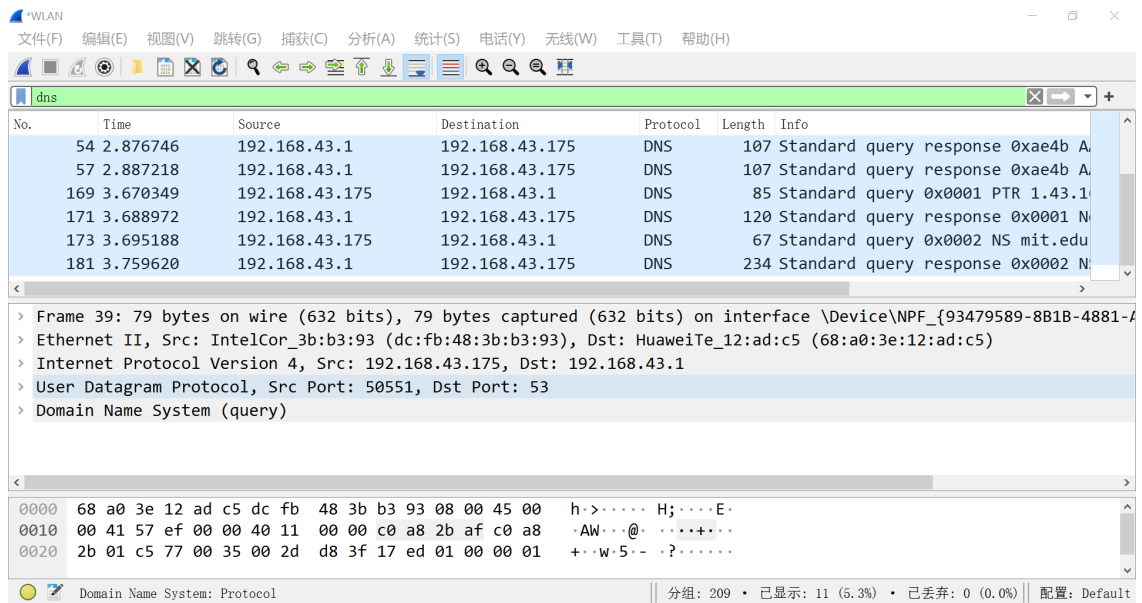
根据红色框中信息可知，响应报文提供了以下八个域名服务器：

- o asia1.akam.net
- o ns1-173.akam.net
- o use2.akam.net
- o ns1-37.akam.net
- o use5.akam.net
- o asia2.akam.net
- o usw2.akam.net
- o eur5.akam.net

此响应报文未提供MIT域名服务器的IP地址。

19. 提供屏幕截图。

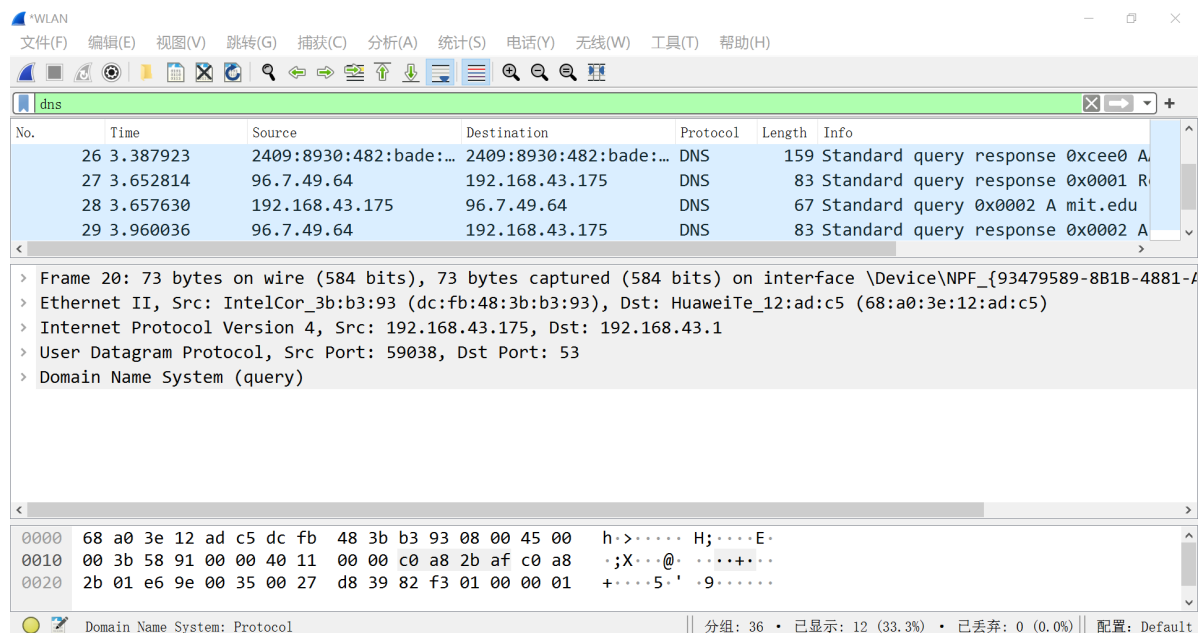
答：屏幕截图如下：



第三部分

1. 启动数据包捕获。
2. 输入命令 **nslookup mit.edu use2.akam.net**。
3. 停止数据包捕获。

抓包结束后wireshark界面如下图所示：



回答下列问题：

20. DNS查询报文发送到的IP地址是什么？这是您的默认本地DNS服务器的IP地址吗？如果不是，这个IP地址是什么？

答：DNS查询报文的信息如下图所示：

No.	Time	Source	Destination	Protocol	Length	Info
26	3.387923	2409:8930:482:bade:...	2409:8930:482:bade:...	DNS	159	Standard query response 0xcee0 A
27	3.652814	96.7.49.64	192.168.43.175	DNS	83	Standard query response 0x0001 R
28	3.657630	192.168.43.175	96.7.49.64	DNS	67	Standard query 0x0002 A mit.edu
29	3.960036	96.7.49.64	192.168.43.175	DNS	83	Standard query response 0x0002 A

> Frame 20: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{93479589-8B1B-4881-A...}
 > Ethernet II, Src: IntelCor_3b:b3:93 (dc:fb:48:3b:b3:93), Dst: HuaweiTe_12:ad:c5 (68:a0:3e:12:ad:c5)
 > Internet Protocol Version 4, Src: 192.168.43.175, Dst: 192.168.43.1
 > User Datagram Protocol, Src Port: 59038, Dst Port: 53
 > Domain Name System (query)

0000 68 a0 3e 12 ad c5 dc fb 48 3b b3 93 08 00 45 00 h>.....H;....E.
 0010 00 3b 58 91 00 00 40 11 00 00 c0 a8 2b af c0 a8 .;X...@.+...
 0020 2b 01 e6 9e 00 35 00 27 d8 39 82 f3 01 00 00 01 +....5-' .9.....

Domain Name System: Protocol | 分组: 36 • 已显示: 12 (33.3%) • 已丢弃: 0 (0.0%) | 配置: Default

根据红色框中内容，DNS查询报文发送到的IP地址为96.7.49.64；

这不是我的默认本地DNS服务器的IP地址，是use2.akam.net的域名服务器地址。

21. 检查DNS查询报文。DNS查询是什么"Type"的？查询消息是否包含任何"answers"？

答：DNS查询报文的信息如下图所示：

No.	Time	Source	Destination	Protocol	Length	Info
26	3.387923	2409:8930:482:bade:...	2409:8930:482:bade:...	DNS	159	Standard query response 0xcee0 A
27	3.652814	96.7.49.64	192.168.43.175	DNS	83	Standard query response 0x0001 R
28	3.657630	192.168.43.175	96.7.49.64	DNS	67	Standard query 0x0002 A mit.edu
29	3.960036	96.7.49.64	192.168.43.175	DNS	83	Standard query response 0x0002 A

> User Datagram Protocol, Src Port: 56020, 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
 [Response In: 20]

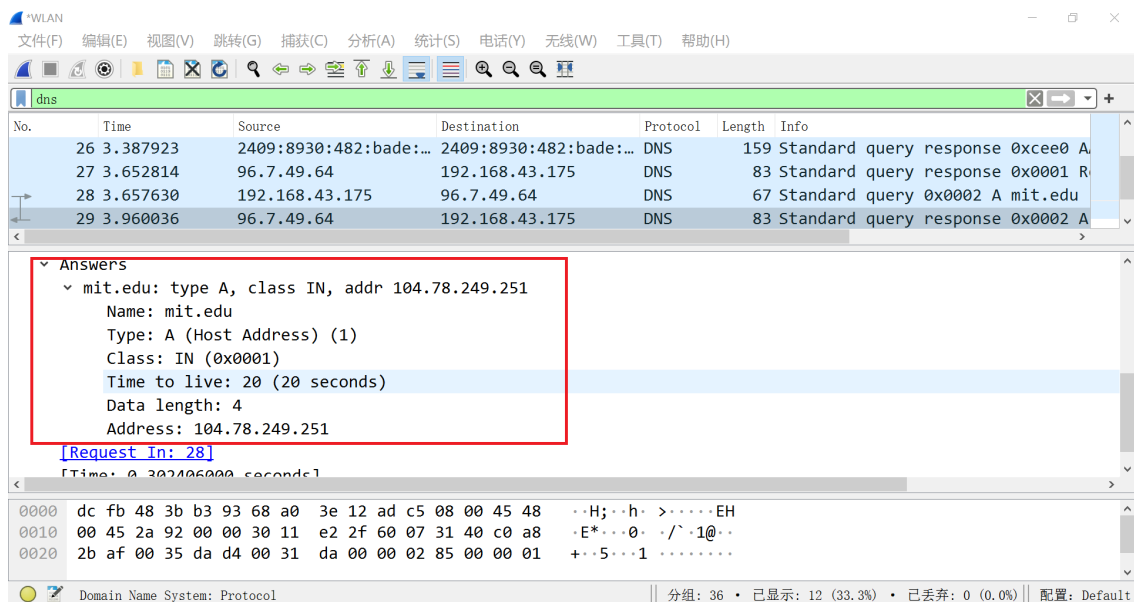
0000 68 a0 3e 12 ad c5 dc fb 48 3b b3 93 08 00 45 00 h>.....H;....E.
 0010 00 35 98 3c 00 00 40 11 00 00 c0 a8 2b af 60 07 .5<...@.+...
 0020 31 40 da d4 00 35 00 21 7d d1 00 02 01 00 00 01 1@...5-! }.....

Domain Name System: Protocol | 分组: 36 • 已显示: 12 (33.3%) • 已丢弃: 0 (0.0%) | 配置: Default

根据绿色框中内容，DNS查询的"Type"是"A"；查询消息不包含任何"answers"。

22. 检查DNS响应报文。提供了多少个"answers"？这些答案包含什么？

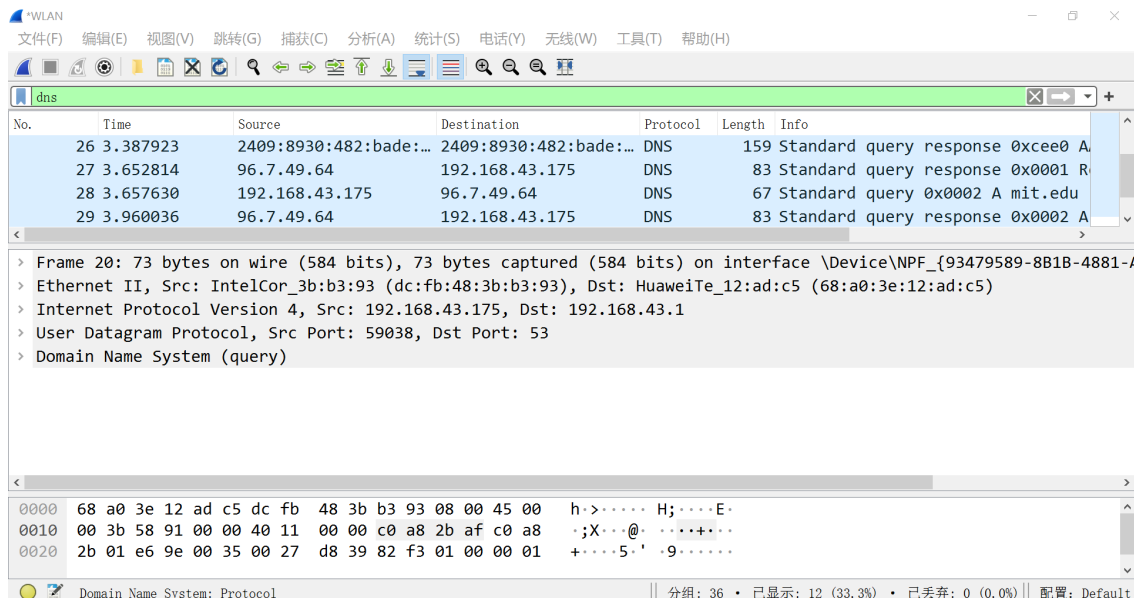
答：DNS响应报文的信息如下图所示：



根据红色框中内容，DNS响应报文提供了一个answer，具体包含了“Name”、“Type”、“Class”、“Time to live”、“Data length”、“Address”等内容。

23. 提供屏幕截图。

答：屏幕截图如下：



四.实验感想与收获

1. 本次实验深入了解了域名系统（DNS），了解了DNS服务器的工作原理。
2. 学习了使用nslookup，ipconfig等工具，从而掌握了对DNS的观察与处理。
3. 加深了对wireshark的了解，学习了读取数据包的更多方面的信息。