

华东师范大学数据科学与工程学院期末项目报告

课程名称：计算机网络与编程

年级：2022

上机实践成绩：

指导教师：张召

姓名：李芳

学号：10214602404

上机实践名称：week10_ DNS 报文分析

上机实践日期：2024.04.28

上机实践编号：10

组号：

上机实践时间：

一、题目要求及实现情况

- task1:** 运行 `nslookup` 来确定一个国外大学 (www.mit.edu) 的 IP 地址以及其权威 DNS 服务器，请在实验报告中附上操作截图并详细分析返回信息内容。

储备知识：

一、Nslookup

➤ 终端中：

- 使用 `nslookup /?` 命令查询 `nslookup` 命令的具体用法：

```
(base) PS C:\Users\HUAWEI> nslookup /?
用法：
nslookup [-opt ...]           # 使用默认服务器的交互模式
nslookup [-opt ...] - server  # 使用 "server" 的交互模式
nslookup [-opt ...] host      # 仅查找使用默认服务器的 "host"
nslookup [-opt ...] host server # 仅查找使用 "server" 的 "host"
```

➤ 交互模式：

- 只输入 `nslookup`，就可以进入交互模式，连续执行多条查询：

```
加载本地及系统配置文件用了 4910 毫秒。
(base) PS C:\Users\HUAWEI> nslookup
默认服务器:  UnKnown
Address:  172.17.0.2

> www.google.com
服务器:  UnKnown
Address:  172.17.0.2

非权威应答:
名称:      www.google.com
Addresses:  2a03:2880:f10c:83:face:b00c:0:25de
            162.125.18.133

> www.baidu.com
服务器:  UnKnown
Address:  172.17.0.2

非权威应答:
名称:      www.a.shifen.com
Addresses:  240e:e9:6002:15a:0:ff:b05c:1278
            240e:e9:6002:15c:0:ff:b015:146f
            180.101.50.242
            180.101.50.188
Aliases:   www.baidu.com

> |
```

- 设置超时和重试次数: nslookup -timeout=整数 -retry=整数 域名

```
(base) PS C:\Users\HUAWEI> nslookup -timeout=10 -retry=3 www.google.com
服务器:  UnKnown
Address:  172.17.0.2

非权威应答:
名称:     www.google.com
Addresses: 2a03:2880:f10c:83:face:b00c:0:25de
          162.220.12.226
```

- 指定端口: nslookup -port=端口号 域名

```
(base) PS C:\Users\HUAWEI> nslookup -port=54 www.google.com
服务器:  UnKnown
Address:  172.17.0.2

非权威应答:
名称:     www.google.com
Addresses: 2a03:2880:f10f:83:face:b00c:0:25de
          199.59.148.201
```

- 设置查询记录类型: nslookup -type=类型 域名

```
(base) PS C:\Users\HUAWEI> nslookup -type=MX www.google.com
服务器:  UnKnown
Address:  172.17.0.2

*** 没有 www.google.com 可以使用的 mail exchange (MX)记录
```

- 设置搜索域: 进入交互模式之后, 使用 set 命令: set domain=搜索域

```
(base) PS C:\Users\HUAWEI> nslookup
默认服务器:  UnKnown
Address:  172.17.0.2

> set domain=com
> google
服务器:  UnKnown
Address:  172.17.0.2

非权威应答:
名称:     google.com
Address:  46.82.174.69

> |
```

- 诊断模式: 使用 -debug 或 -d2 选项以启用诊断模式, 提供更多详细信息: nslookup -debug/-d2 域名

```
(base) PS C:\Users\HUAWEI> nslookup -debug www.google.com
-----
Got answer:
HEADER:
    opcode = QUERY, id = 1, rcode = NXDOMAIN
    header flags:  response, want recursion, recursion avail.
    questions = 1,  answers = 0,  authority records = 0,  additional = 0

QUESTIONS:
    2.0.17.172.in-addr.arpa, type = PTR, class = IN
-----
服务器:  UnKnown
Address:  172.17.0.2
-----
Got answer:
HEADER:
    opcode = QUERY, id = 2, rcode = NOERROR
    header flags:  response, want recursion, recursion avail.
    questions = 1,  answers = 1,  authority records = 0,  additional = 0

QUESTIONS:
    www.google.com, type = A, class = IN
ANSWERS:
-> www.google.com
    internet address = 108.160.166.42
    ttl = 29 (29 secs)
-----
非权威应答:
-----
Got answer:
HEADER:
    opcode = QUERY, id = 3, rcode = NOERROR
    header flags:  response, want recursion, recursion avail.
    questions = 1,  answers = 1,  authority records = 0,  additional = 0

QUESTIONS:
    www.google.com, type = AAAA, class = IN
ANSWERS:
-> www.google.com
-> www.google.com
    AAAA IPv6 address = 2a03:2880:f10d:183:face:b00c:0:25de
    ttl = 126 (2 mins 6 secs)
-----
名称:      www.google.com
Addresses:  2a03:2880:f10d:183:face:b00c:0:25de
            108.160.166.42
```

- 查询所有记录：检查域名的所有 DNS 信息：nslookup -type=ANY 域名

```
(base) PS C:\Users\HUAWEI> nslookup -type=ANY www.google.com
服务器:  UnKnown
Address:  172.17.0.2

非权威应答:
www.google.com  internet address = 128.242.245.212
```

操作截图&分析:

- 操作流程:

- 先打开终端，在 powershell 中使用 nslookup 命令，确定 www.mit.edu 的 IP 地址:

```
(base) PS C:\Users\HUAWEI> nslookup www.mit.edu
服务器: moon.ecnu.edu.cn
Address: 202.120.80.2

非权威应答:
名称: e9566.dscb.akamaiedge.net
Addresses: 2402:4f00:4001:19c::255e
           2402:4f00:4001:1a6::255e
           223.119.214.63
Aliases: www.mit.edu
```

- 再使用 nslookup 命令, 查询 www.mit.edu 的权威 DNS 服务器:

```
(base) PS C:\Users\HUAWEI> nslookup -type=NS mit.edu
服务器: moon.ecnu.edu.cn
Address: 202.120.80.2

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

➤ 分析返回信息内容:

- 第一个查询:

```
(base) PS C:\Users\HUAWEI> nslookup www.mit.edu
服务器: moon.ecnu.edu.cn
Address: 202.120.80.2

非权威应答:
名称: e9566.dscb.akamaiedge.net
Addresses: 2402:4f00:4001:19c::255e
           2402:4f00:4001:1a6::255e
           223.119.214.63
Aliases: www.mit.edu
```

指定用于执行DNS查询的DNS服务器名称
上面执行DNS查询的moon.ecnu.edu.cn的IP地址
表明返回的DNS信息并非来自权威DNS服务器, 而是来自缓存或其他来源
被查询主机名
被查询主机名对应的IP地址列表
主机名的别名

- ◆ 在这个例子中, 返回的 DNS 信息可能来自本地 DNS 服务器或者中间 DNS 缓存。
- ◆ 返回的被查询主机对应 IP 地址列表中包含了三个地址:
 - 两个 IPv6 地址: 2402:4f00:4001:19c::255e 和 2402:4f00:4001:1a6::255e";
 - 一个 IPv4 地址: 223.119.214.63

- ◆ `www.mit.edu` 是 `"e9566.dscb.akamaiedge.net"` 的别名，说明原始的主机名被重定向到了 Akamai 的 CDN 服务。

■ 第二个查询：

```
(base) PS C:\Users\HUAWEI> nslookup -type=NS mit.edu
服务器: moon.ecnu.edu.cn
Address: 202.120.80.2

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

- ◆ 在这个例子中，虽然返回了 `mit.edu` 域名的权威 DNS 服务器列表，但是仍然会显示“非权威应答”的原因可能是因为：这个查询结果不是直接从 MIT.edu 的权威 DNS 服务器获取的。
- ◆ `mit.edu nameserver`：这些是 MIT.edu 域名的权威 DNS 服务器的名称。MIT.edu 使用 Akamai 的 DNS 服务器作为其权威 DNS 服务器。这些服务器分布在不同的地区，这种分布式的设置有助于提高域名解析的性能和可靠性。

- **task2:** 运行 `nslookup`，使用 task1 中一个已获得的 DNS 服务器，来查询 Google 服务器 (www.google.com) 的 IP 地址（可直接查询），请在实验报告中附上操作截图并详细分析返回信息内容。

操作截图&分析：

➤ 操作流程：

- 选取 task1 获取的第一个 DNS 服务器，进行后续操作：

```
(base) PS C:\Users\HUAWEI> nslookup -type=NS mit.edu
服务器: moon.ecnu.edu.cn
Address: 202.120.80.2

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

- 使用 `nslookup` 语法：`nslookup -option1 -option2 host-to-find dns-server` 查询 google 服务器的 IP 地址：

```
(base) PS C:\Users\HUAWEI> nslookup www.google.com asia2.akam.net
服务器:  UnKnown
Address:  95.101.36.64

非权威应答:
名称:     www.google.com
Addresses: 2001::453f:be1a
          199.59.149.207
```

➤ 分析返回信息内容:

```
(base) PS C:\Users\HUAWEI> nslookup www.google.com asia2.akam.net
服务器:  UnKnown
Address:  95.101.36.64
非权威应答:
名称:     www.google.com
Addresses: 2001::453f:be1a
          199.59.149.207
```

进行DNS查询的中间服务器的名称和IP地址

查询返回的目标主机名还有其IP地址

- 使用指定 DNS 服务器 asia2.akam.net 查询 www.google.com。
- 发起 DNS 查询的本地计算机或网络设备的信息部分: 显示 Unknown 表示计算机没有直接与 "asia2.akam.net" 通信, 而是通过一个中间服务器来进行 DNS 查询, 无法确定中间服务器的名称, 但有其 IP 地址。
- 虽然结果显示为非权威应答, 但是查询的 IP 地址 (IPv6: 2001::453f:be1a 和 IPv4: 199.59.149.207) 是可信的, 因为它们来自 google 服务器, 是由权威 DNS 服务器提供的。

- **task3:** 根据 Wireshark 抓取的报文信息 (例, 下图所示示例), 分别分析 DNS 查询报文和响应报文的组成结构, 参考上面的报文格式指出报文的每个部分 (如, 头部区域等), 请将实验结果附在实验报告中。

储备知识:

- DNS 分为查询请求和查询响应, 请求和响应的报文结构基本相同, 如下:

事务ID (Transaction ID)	标志 (Flags)
问题计数 (Questions)	回答资源记录数 (Answer RRs)
权威名称服务器计数 (Authority RRs)	附加资源记录数 (Additional RRs)
查询问题区域 (Queries)	
回答问题区域 (Answers)	
权威名称服务器区域 (Authoritative nameservers)	
附加信息区域 (Additional records)	

首部

➤ 首部:

- 事物 ID: DNS 报文的 ID 表示, 对于请求报文和其对应的应答报文, 该字段的值是相同的。通过它可以区分 DNS 应答报文是对哪个请求进行响应的。
- 标志: DNS 报文中的标志字段。
 - ◆ QR (Response) : 查询请求/响应的标志信息。查询请求时, 值为 0; 响应时, 值为 1。
 - ◆ Opcode: 操作码。其中, 0 表示标准查询; 1 表示反向查询; 2 表示服务器状态请求。
 - ◆ AA (Authoritative) : 授权应答, 该字段在响应报文中有效。值为 1 时, 表示名称服务器是权威服务器; 值为 0 时, 表示不是权威服务器。
 - ◆ TC (Truncated) : 表示是否被截断。值为 1 时, 表示响应已超过 512 字节并已被截断, 只返回前 512 个字节。
 - ◆ RD (Recursion Desired) : 期望递归。该字段能在一个查询中设置, 并在响应中返回。该标志告诉名称服务器必须处理这个查询, 这种方式被称为一个递归查询。如果该位为 0, 且被请求的名称服务器没有一个授权回答, 它将返回一个能解答该查询的其他名称服务器列表。这种方式被称为迭代查询。
 - ◆ RA (Recursion Available) : 可用递归。该字段只出现在响应报文中。当值为 1 时, 表示服务器支持递归查询。
 - ◆ Z: 保留字段, 在所有的请求和应答报文中, 它的值必须为 0。
 - ◆ rcode (Reply code) : 返回码字段, 表示响应的差错状态。当值为 0 时, 表示没有错误; 当值为 1 时, 表示报文格式错误 (Format error), 服务器不能理解请求的报文; 当值为 2 时, 表示域名服务器失败 (Server failure), 因为服务器的原因导致没办法处理这个请求; 当值为 3 时, 表示名字错误 (Name Error), 只有对授权域名解析服务器有意义, 指出解析的域名不存在; 当值为 4 时, 表示查询类型不支持 (Not Implemented), 即域名服务器不支持查询类型; 当值为 5 时, 表示拒绝 (Refused), 一般是服务器由于设置的策略拒绝给出应答, 如服务器不希望对某些请求者给出应答。
- 问题计数: DNS 查询请求的数目。
- 回答资源记录数: DNS 响应的数目。

- 权威名称服务器计数：权威名称服务器的数目。
 - 附加资源记录数：额外的记录数目（权威名称服务器对应 IP 地址的数目）。
- Queries 查询问题部分：
- 显示 DNS 查询请求的问题，通常只有一个问题
 - 该部分包含正在进行的查询信息，包含查询名（被查询主机名字）、查询类型、查询类
 - 字段含义
 - ◆ 查询名：是可变长字段。查询名称由标签序列构成，每个标签前有一个八位位组指出该标签的长度。因为每个域名以空标签结束，因此每个域名的最后一个八位位组的值为 0。一般为要查询的域名，有时也会是 IP 地址，用于反向查询。
 - ◆ 查询类型：两个八位位组代码，长度 16 位，指定 DNS 查询请求的资源类型。通常查询类型为 A 类型，表示由域名获取对应的 IP 地址。
 - ◆ 查询类：两个八位位组代码，指定查询的地址类型。例如：对于 Internet，符号表示为 IN，查询类字段值为 1。
- 回答问题部分、权威名称服务器部分和附加信息部分：
- 共享相同格式，就是可变数目的资源记录，其中记录的数目在首部相应计数字段中规定。只有应答报文才提供资源记录。
 - 字段含义
 - ◆ Name：可变长字段，指该资源记录匹配的域名。它实际上就是查询报文问题部分查询名称的副本，但由于在域名重复出现的地方 DNS 使用压缩，这个字段就是到查询报文问题部分中的相应域名的指针偏移。
 - ◆ Type：两个八位位组代码，长度 16 位，指定资源记录的类型，说明 RDATA 字段中数据意义。该字段与问题部分的查询类型字段相同。
 - ◆ Class：两个八位位组，指定 RDATA 字段中数据的类，与问题部分的查询类字段相同。
 - ◆ TTL：生成时间，32 位无正负号整数，指定资源记录可以被缓存时间，单位是秒。值为 0 表示资源记录仅能用于正在进行的业务，不能被缓存。

- ◆ Data length: 资源数据长度，无符号 16 位整数，指定 RDATA 字段长度，以八位位组为字节。
- ◆ 资源数据：可变长字段，是资源记录的具体内容。其格式取决于资源记录的 TYPE 和 CLASS 字段。资源数据格式种类包含如下：
 - 数字：八位位组表示数，例如，IPv4 地址是 4 个八位组整数，而 IPv6 地址是一个 16 个八位组整数。
 - 域名：可用标签序列来表示。每一个标签前面有 1 个字节长度字段，它定义标签中的字段数。长度字段的两个高位永远是 0，标签的长度不能超过 63 字节。
 - 偏移指针：域名可以用偏移指针来替换。偏移指针是 2 字节字段，它的两个高位置为 1
 - 字符串：用 1 字节的长度字段后面跟着长度字段数。长度字段并不像域名长度字段那样受限。字符串可以多达 256 个字符。

操作流程截图：

- 清除 dns 缓存和浏览器缓存后，打开 wireshark 开始捕获：



- 第一种方法，使用浏览器：

- 浏览器输入 <https://www.baidu.com/index.html> 网址：



- 使用 wireshark 进行抓包筛选, ip.addr == 172.17.0.2 and dns:

No.	Time	Source	Destination	Protocol	Length	Info
1278	35.357377	172.17.1.240	172.17.0.2	DNS	73	Standard query 0x5a20 A sp0.baidu.com
1279	35.357524	172.17.1.240	172.17.0.2	DNS	73	Standard query 0xa588 HTTPS sp0.baidu.com
1283	35.358202	172.17.0.2	172.17.1.240	DNS	183	Standard query response 0x9082 HTTPS pss.bdstatic.com CNAME ...
1284	35.360056	172.17.0.2	172.17.1.240	DNS	132	Standard query response 0x72e2 HTTPS sp2.baidu.com CNAME www...
1285	35.361124	172.17.0.2	172.17.1.240	DNS	132	Standard query response 0x45a4 HTTPS sp1.baidu.com CNAME www...
1323	35.374767	172.17.0.2	172.17.1.240	DNS	132	Standard query response 0x5a20 A sp0.baidu.com CNAME www.a.s...
1339	35.378187	172.17.0.2	172.17.1.240	DNS	132	Standard query response 0xa588 HTTPS sp0.baidu.com CNAME www...
1411	35.418774	172.17.1.240	172.17.0.2	DNS	82	Standard query 0x2e90 A hectorstatic.baidu.com
1412	35.419029	172.17.1.240	172.17.0.2	DNS	82	Standard query 0xe0ad HTTPS hectorstatic.baidu.com
1415	35.422105	172.17.0.2	172.17.1.240	DNS	208	Standard query response 0x2e90 A hectorstatic.baidu.com CNAM...
1428	35.433280	172.17.0.2	172.17.1.240	DNS	256	Standard query response 0xe0ad HTTPS hectorstatic.baidu.com ...
2256	36.832572	172.17.1.240	172.17.0.2	DNS	76	Standard query 0x32f0 A hector.baidu.com
2257	36.832922	172.17.1.240	172.17.0.2	DNS	76	Standard query 0x4946 HTTPS hector.baidu.com
2260	36.835858	172.17.0.2	172.17.1.240	DNS	92	Standard query response 0x32f0 A hector.baidu.com A 39.156.6...
2264	36.844749	172.17.0.2	172.17.1.240	DNS	76	Standard query response 0x4946 HTTPS hector.baidu.com
2274	36.853800	172.17.1.240	172.17.0.2	DNS	78	Standard query 0xfb09 A edge.microsoft.com
2275	36.854075	172.17.1.240	172.17.0.2	DNS	78	Standard query 0x8e35 HTTPS edge.microsoft.com
2280	36.858060	172.17.0.2	172.17.1.240	DNS	181	Standard query response 0xfb09 A edge.microsoft.com CNAME ed...
2287	36.869498	172.17.0.2	172.17.1.240	DNS	181	Standard query response 0x8e35 HTTPS edge.microsoft.com CNAM...
2420	37.073116	172.17.1.240	172.17.0.2	DNS	96	Standard query 0xd3f7 A functional.events.data.microsoft.com
2421	37.073368	172.17.1.240	172.17.0.2	DNS	96	Standard query 0xa3ae HTTPS functional.events.data.microsoft...
2440	37.087090	172.17.0.2	172.17.1.240	DNS	207	Standard query response 0xa3ae HTTPS functional.events.data...
2442	37.089401	172.17.0.2	172.17.1.240	DNS	223	Standard query response 0xd3f7 A functional.events.data.micr...
2628	37.353828	172.17.1.240	172.17.0.2	DNS	78	Standard query 0xb18f A passport.baidu.com
2629	37.354096	172.17.1.240	172.17.0.2	DNS	78	Standard query 0x4ae6 HTTPS passport.baidu.com
2637	37.365352	172.17.0.2	172.17.1.240	DNS	110	Standard query response 0x4ae6 HTTPS passport.baidu.com CNAM...
2638	37.366481	172.17.0.2	172.17.1.240	DNS	158	Standard query response 0xb18f A passport.baidu.com CNAME pa...
2801	37.750400	172.17.1.240	172.17.0.2	DNS	78	Standard query 0xe1a3 A edge.microsoft.com
2882	37.750665	172.17.1.240	172.17.0.2	DNS	78	Standard query 0x97b3 HTTPS edge.microsoft.com
2886	37.753272	172.17.0.2	172.17.1.240	DNS	181	Standard query response 0xe1a3 A edge.microsoft.com CNAME ed...
2895	37.764982	172.17.0.2	172.17.1.240	DNS	181	Standard query response 0x97b3 HTTPS edge.microsoft.com CNAM...

> Frame 2628: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{4EACE2AD-512}	0000	b8 69 f4 c5 1b a4 c0 b5 d7 83 a3
> Ethernet II, Src: ChongqingFug_83:a3:c5 (c0:b5:d7:83:a3:c5), Dst: Routerboardc_c5:1b:a4 (b8:69:f4:c5:1b:a4)	0010	00 40 23 74 00 00 00 11 bd 24 ac
> Internet Protocol Version 4, Src: 172.17.1.240, Dst: 172.17.0.2	0020	00 02 fb 56 00 35 00 2c 25 5e b1
> User Datagram Protocol, Src Port: 64342, Dst Port: 53	0030	00 00 00 00 00 00 08 70 61 73 73
> Domain Name System (query)	0040	62 61 69 64 75 03 63 6f 6d 00 00

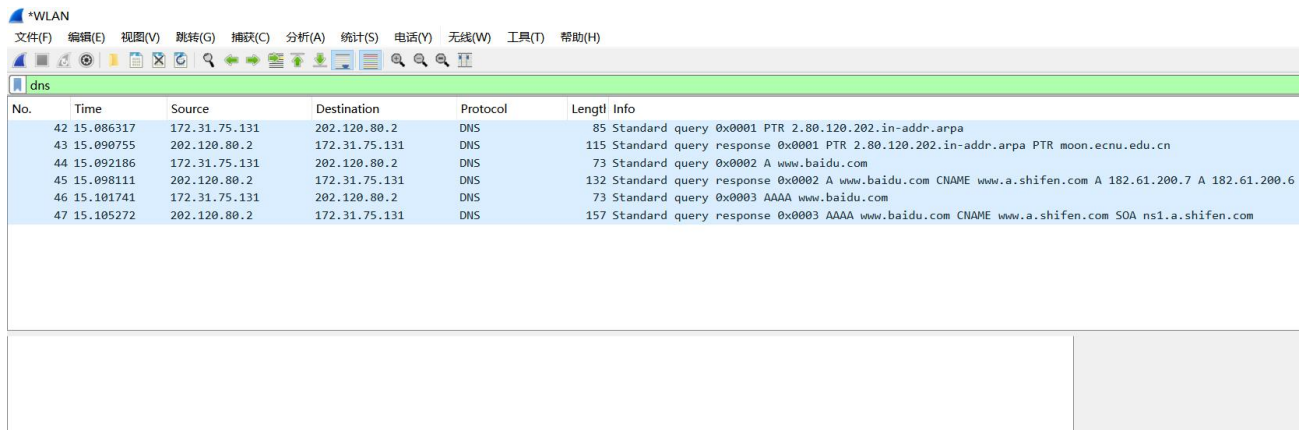
- 第二种方法, 使用命令行:

- 先在终端命令行中输入 nslookup www.baidu.com 命令:

```
(base) PS C:\Users\HUAWEI> nslookup www.baidu.com
服务器: moon.ecnu.edu.cn
Address: 202.120.80.2

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

- 使用 wireshark 同步抓包, 并筛选 DNS 协议:

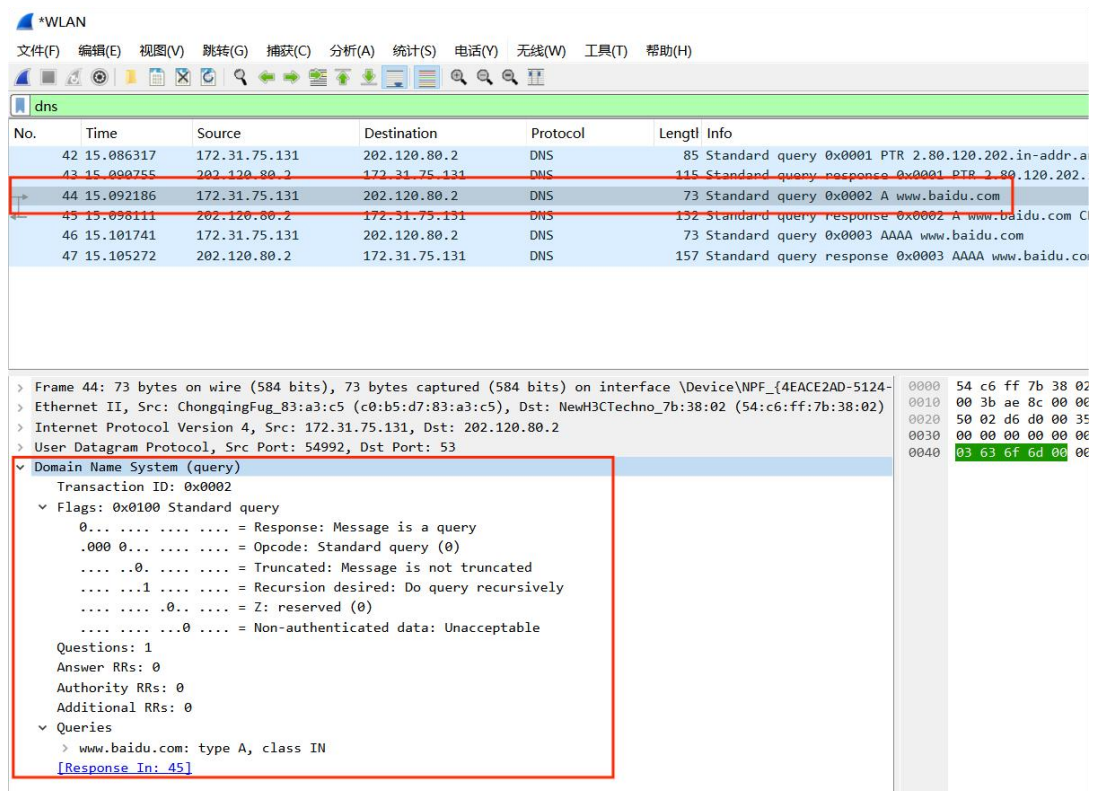


No.	Time	Source	Destination	Protocol	Length	Info
42	15.086317	172.31.75.131	202.120.80.2	DNS	85	Standard query 0x0001 PTR 2.80.120.202.in-addr.arpa
43	15.090755	202.120.80.2	172.31.75.131	DNS	115	Standard query response 0x0001 PTR 2.80.120.202.in-addr.arpa PTR moon.ecnu.edu.cn
44	15.092186	172.31.75.131	202.120.80.2	DNS	73	Standard query 0x0002 A www.baidu.com
45	15.098111	202.120.80.2	172.31.75.131	DNS	132	Standard query response 0x0002 A www.baidu.com CNAME www.a.shifen.com A 182.61.200.7 A 182.61.200.6
46	15.101741	172.31.75.131	202.120.80.2	DNS	73	Standard query 0x0003 AAAA www.baidu.com
47	15.105272	202.120.80.2	172.31.75.131	DNS	157	Standard query response 0x0003 AAAA www.baidu.com CNAME www.a.shifen.com SOA ns1.a.shifen.com

报文组成结构分析:

➤ 查询报文:

- 选取第二种抓取方法中的 standard query 0x0002 A www.baidu.com, 这项标准 DNS 查询报文:



Frame 44: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{4EACE2AD-5124-...}

Ethernet II, Src: ChongqingFug_83:a3:c5 (c0:b5:d7:83:a3:c5), Dst: NewH3CTechno_7b:38:02 (54:c6:ff:7b:38:02)

Internet Protocol Version 4, Src: 172.31.75.131, Dst: 202.120.80.2

User Datagram Protocol, Src Port: 54992, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x0002

Flags: 0x0100 Standard query

0... .. = Response: Message is a query

.000 0... .. = Opcode: Standard query (0)

... ..0... .. = Truncated: Message is not truncated

... ..1... .. = Recursion desired: Do query recursively

... ..0... .. = Z: reserved (0)

... ..0... .. = Non-authenticated data: Unacceptable

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

> www.baidu.com: type A, class IN

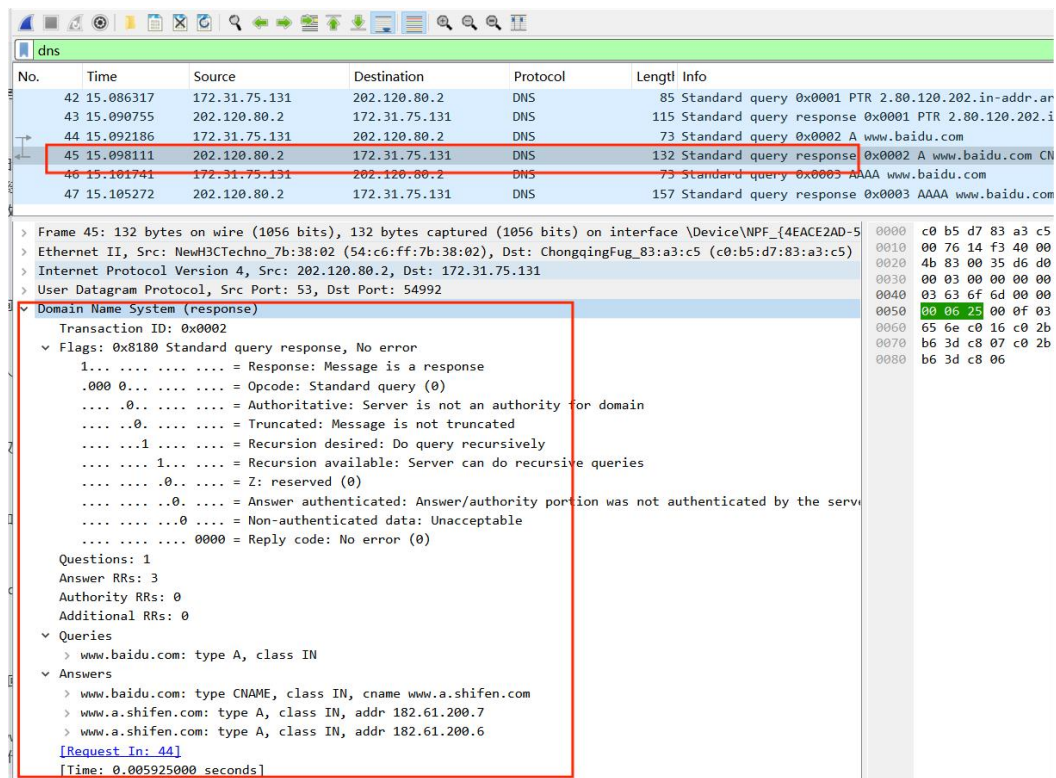
[Response In: 45]

- 这个 DNS 查询报文请求解析主机 www.baidu.com 的 IPv4 地址, 并希望递归服务器返回递归查询结果。组成结构分析:

■ 首部:

- ◆ Transaction ID: 0x0002 -> 事务 ID, 用于标识该查询的唯一 ID。
- ◆ Flags: 0x0100 -> 标志位, 表示该消息是一个标准查询消息。

- Response: 消息是一个查询。
 - Opcode: 标准查询。
 - Truncated: 消息未被截断。
 - Recursion desired: 表示递归查询，即希望服务器在本地缓存无法解析时进行递归查询。
 - Non-authenticated data: 表示不接受非认证数据。
- ◆ Questions: 1 -> 查询问题数，表示该报文中包含一个查询。
 - ◆ Answer RRs: 0 -> 回答资源记录数，表示该报文中没有回答的资源记录。
 - ◆ Authority RRs: 0 -> 授权资源记录数，表示该报文中没有授权的资源记录。
 - ◆ Additional RRs: 0 -> 附加资源记录数，表示该报文中没有附加的资源记录。
- 查询问题区域： (Queries:)
 - ◆ www.baidu.com: 查询主机为 www.baidu.com 的 A 记录，即查询百度网站的 IPv4 地址。
- 后三个区域没有
- 响应报文：
- 选取刚分析的查询报文的对应响应报文



The image shows a Wireshark packet capture of a DNS response. The packet list at the top shows several DNS packets. Packet 45 is selected, which is a 'Standard query response' from 202.120.80.2 to 172.31.75.131. The packet details pane shows the following information:

- Transaction ID: 0x0002
- Flags: 0x8180 Standard query response, No error
 - 1... .. = Response: Message is a response
 - .000 0... .. = Opcode: Standard query (0)
 -0... .. = Authoritative: Server is not an authority for domain
 -0... .. = Truncated: Message is not truncated
 -1... .. = Recursion desired: Do query recursively
 -1... .. = Recursion available: Server can do recursive queries
 -0... .. = Z: reserved (0)
 -0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server
 -0... .. = Non-authenticated data: Unacceptable
 -0000 = Reply code: No error (0)
- Questions: 1
 - Answer RRs: 3
 - Authority RRs: 0
 - Additional RRs: 0
- Queries
 - > www.baidu.com: type A, class IN
- Answers
 - > www.baidu.com: type CNAME, class IN, cname www.a.shifen.com
 - > www.a.shifen.com: type A, class IN, addr 182.61.200.7
 - > www.a.shifen.com: type A, class IN, addr 182.61.200.6

The packet bytes pane shows the raw data of the response, including the domain name system response section.

- 这个 DNS 响应报文是对查询主机 `www.baidu.com` 的 IPv4 地址的响应，包含了 3 个回答的资源记录，并且回应代码表示没有错误。组成结构分析：
- 首部：
 - ◆ Transaction ID: 0x0002 -> 事务 ID，与相应的查询报文中的事务 ID 相同，用于标识响应和查询的对应关系。
 - ◆ Flags: 0x8180 -> 标志位，表示该消息是一个标准查询响应消息。
 - Response: 消息是一个响应。
 - Opcode: 标准查询。
 - Authoritative: 服务器不是该域的权威服务器。
 - Truncated: 消息未被截断。
 - Recursion desired: 发送方希望递归查询。
 - Recursion available: 服务器能够进行递归查询。
 - Answer authenticated: 答案/权威部分未经服务器验证。
 - Non-authenticated data: 不接受非认证数据。
 - Reply code: 响应代码为无错误。
 - ◆ Questions: 1 -> 查询问题数，表示该报文中包含一个查询。
 - ◆ Answer RRs: 3 -> 回答资源记录数，表示该报文中包含三个回答的资源记录。
 - ◆ Authority RRs: 0 -> 授权资源记录数，表示该报文中没有授权的资源记录。
 - ◆ Additional RRs: 0 -> 附加资源记录数，表示该报文中没有附加的资源记录。
- 查询问题区域：(Queries:)
 - ◆ `www.baidu.com`: 查询主机为 `www.baidu.com` 的 A 记录，即查询百度网站的 IPv4 地址。
- 回答问题区域：(Answers:)
 - ◆ 包含了 3 个回答的资源记录：
 - 第一个回答是关于 `www.baidu.com` 的 CNAME 记录，指向 `www.a.shifen.com`。

- 第二个回答是关于 www.a.shifen.com 的 A 记录，指向 182.61.200.7。
- 第三个回答是关于 www.a.shifen.com 的另一个 A 记录，指向 182.61.200.6。

■ 后两个区域没有

- **task4:** 基于 task3 中得到的查询和响应报文进行分析，试问这里的查询是什么“Type”的，查询消息是否包含任何“answers”？试问这里的响应消息提供了多少个“answers”，这些“answers”具体包含什么？请将实验结果附在实验报告中。

报文分析：

➤ 查询报文：

44	15.092186	172.31.75.131	202.120.80.2	DNS	73 Standard query 0x0002 A
45	15.098111	202.120.80.2	172.31.75.131	DNS	132 Standard query response
46	15.101741	172.31.75.131	202.120.80.2	DNS	73 Standard query 0x0003 A
47	15.105272	202.120.80.2	172.31.75.131	DNS	157 Standard query response


```

> Frame 44: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{4EACE2AD-5124-4000-8000-000000000000}
> Ethernet II, Src: ChongqingFug_83:a3:c5 (c0:b5:d7:83:a3:c5), Dst: NewH3CTechno_7b:38:02 (54:c6:ff:7b:38:02)
> Internet Protocol Version 4, Src: 172.31.75.131, Dst: 202.120.80.2
> User Datagram Protocol, Src Port: 54992, Dst Port: 53
> Domain Name System (query)
  Transaction ID: 0x0002
  Flags: 0x0100 Standard query
    0... .. = Response: Message is a query
    .000 0... .. = Opcode: Standard query (0)
    ....0... .. = Truncated: Message is not truncated
    ....1... .. = Recursion desired: Do query recursively
    ....0... .. = Z: reserved (0)
    ....0... .. = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  Queries
    > www.baidu.com: type A, class IN
    [Response In: 45]
  
```

➤ 响应报文：

45	15.098111	202.120.80.2	172.31.75.131	DNS	132 Standard query response
46	15.101741	172.31.75.131	202.120.80.2	DNS	73 Standard query 0x0003 A
47	15.105272	202.120.80.2	172.31.75.131	DNS	157 Standard query response


```

> Frame 45: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits) on interface \Device\NPF_{4EACE2AD-5124-4000-8000-000000000000}
> Ethernet II, Src: NewH3CTechno_7b:38:02 (54:c6:ff:7b:38:02), Dst: ChongqingFug_83:a3:c5 (c0:b5:d7:83:a3:c5)
> Internet Protocol Version 4, Src: 202.120.80.2, Dst: 172.31.75.131
> User Datagram Protocol, Src Port: 53, Dst Port: 54992
> Domain Name System (response)
  Transaction ID: 0x0002
  Flags: 0x8180 Standard query response, No error
    1... .. = Response: Message is a response
    .000 0... .. = Opcode: Standard query (0)
    ....0... .. = Authoritative: Server is not an authority for domain
    ....0... .. = Truncated: Message is not truncated
    ....1... .. = Recursion desired: Do query recursively
    ....1... .. = Recursion available: Server can do recursive queries
    ....0... .. = Z: reserved (0)
    ....0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server
    ....0... .. = Non-authenticated data: Unacceptable
    ....0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  Queries
    > www.baidu.com: type A, class IN
  Answers
    > www.baidu.com: type CNAME, class IN, cname www.a.shifen.com
    > www.a.shifen.com: type A, class IN, addr 182.61.200.7
    > www.a.shifen.com: type A, class IN, addr 182.61.200.6
    [Request In: 44]
    [Time: 0.005925000 seconds]
  
```

- 查询 Type:
 - 查询类型为“A”，表示查询主机的 IPv4 的地址
- 查询消息是否包含任何 answers:
 - 否
- 响应消息提供 answers 个数:
 - 三个
- answers 结构:
 - 名称 Name+类型 Type+类 Class+具体值 Data
- answers 具体包含内容:
 - 一：关于 www.baidu.com 的 CNAME 记录，指向 www.a.shifen.com。
 - 二：关于 www.a.shifen.com 的 A 记录，指向 182.61.200.7。
 - 三：关于 www.a.shifen.com 的另一个 A 记录，指向 182.61.200.6。

二、总结

本次实验通过 nslookup 命令和 Wireshark 工具深入了解了 DNS 协议及其工作原理。通过分析 DNS 报文，我了解了其结构和各部分的含义。同时，实验中学会了使用 nslookup 查询域名的 IP 地址，并了解了如何指定特定的 DNS 服务器进行查询。通过 Wireshark 抓取的报文信息，我对 DNS 查询和响应的过程有了更深入的理解。

Task1: nslookup 查询 www.mit.edu

Task2: 使用已获得的 DNS 服务器查询 Google 服务器

这两个实验任务帮我很好的了解和掌握了命令行命令 nslookup 的使用。

Task3: Wireshark 抓取的 DNS 报文分析

Task4: 基于查询和响应报文的分析

这两个实验任务帮我更好的分析和掌握了 DNS 查询和响应报文组成结构和每部分包含的具体信息：

查询报文结构：包括头部区域、问题区域；响应报文结构：包括头部区域、回答区域、授权区域、附加区域。

总之，本次实验帮助我更好地理解 DNS 协议，并学会了使用相关工具进行 DNS 查询和分析。这将对我今后的网络管理和故障排查工作有所帮助。