

华东师范大学数据科学与工程学院实验报告

课程名称：计算机网络与编程

年级：21 级

上机实践成绩：

指导教师：张召

姓名：杨茜雅

学号：10215501435

上机实践名称：Lab10

上机实践日期：2023. 5. 12

上机实践编号：10

组号：

上机实践时间：5. 12

一、实验目的

- 了解系统命令nslookup 的用法
- 学习 DNS 协议并掌握 DNS 的工作原理

二、实验任务

- nslookup 命令的简单使用
- 使用 Wireshark 分析 DNS 协议

三、使用环境

- nslookup
- Wireshark

四、实验过程

Task 1: 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。

尝试三个不同 nslookup 命令的结果：

1、nslookup www.mit.edu

```
C:\Users\86138>nslookup www.mit.edu
服务器: moon.ecnu.edu.cn
Address: 202.120.80.2 提供相应的dns服务器名称和ip地址

非权威应答: 主机名和ip地址
名称: e9566.dscb.akamaiedge.net
Addresses: 2600:1417:a000:689::255e
           2600:1417:a000:6b2::255e
           23.2.130.241

Aliases: www.mit.edu 所查询的别名
         www.mit.edu.edgekey.net
```

这个命令是说，请告诉我主机 www.mit.edu 的 IP 地址。如上图所示，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。虽然响应来自mit的本地 DNS 服务器，但本地 DNS 服务器很可能会迭代地联系其他几个 DNS 服务器来获得结果。

2、nslookup -type=NS mit.edu : 查询权威 DNS

```
C:\Users\86138>nslookup -type=NS mit.edu
服务器: moon.ecnu.edu.cn
Address: 202.120.80.2
提供响应的dns服务器

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

在这个例子中，我添加了选项 `-type=NS` 和一级域名 `mit.edu`。这将使得 `nslookup` 将NS（域名服务器记录，Name Server）记录发送到默认的本地 DNS 服务器。换句话说，“请给我发送 `mit.edu` 的权威 DNS 的主机名”（当不使用 `-type` 选项时，`nslookup` 使用默认值，即查询 A 类记录。）上图中，首先显示了提供响应的 DNS 服务器（这是默认本地 DNS 服务器）以及八个 `mit` 域名服务器。这些服务器中的每一个确实都是校园主机的权威 DNS 服务器。然而，`nslookup` 也表明该响应是非权威的，这意味着这个响应来自某个服务器的缓存，而不是来自权威mit DNS 服务器。

3、nslookup www.mit.edu asia1.akam.net

```
C:\Users\86138>nslookup www.mit.edu asia1.akam.net
服务器: UnKnown
Address: 95.100.175.64

名称: www.mit.edu
```

在这个例子中，我们希望将查询请求发送到 DNS 服务器 `asia1.akam.net`，而不是默认的本地DNS 服务器。因此，查询和响应事务直接发生在我们的主机和 `asia1.akam.net` 之间。在这个例子中，DNS 服务器 `asia1.akam.net`提供主机 www.mit.edu 的 IP 地址信息。

Task 2: 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。

使用DNS 服务器: moon.ecnu.edu.cn

输入指令: nslookup www.google.com moon.ecnu.edu.cn

```
C:\Users\86138>nslookup www.google.com moon.ecnu.edu.cn
服务器: moon.ecnu.edu.cn
Address: 202.120.80.2

非权威应答:
名称: www.google.com
Addresses: 2a03:2880:f11c:8083:face:b00c:0:25de
           208.43.170.231
```

task1选取的dns服务器
ip地址与task1相同
google服务器
返回www.google.com的ip地址

Task 3: 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。

先刷新 DNS 解析缓存

```
C:\Users\86138>ipconfig/flushdns

Windows IP 配置

已成功刷新 DNS 解析缓存。

C:\Users\86138>|
```

在浏览器中查询 www.weibo.com，在 Wireshark 中过滤器输入 dns，获取查询报文和响应报文：

No.	Time	Source	Destination	Protocol	Length	Info
60	6.024627	192.168.3.1	192.168.3.14	DNS	160	Standard query response 0x0894 AAAA china.bing123.com SOA ns1-04.azure-dns.com
157	11.201452	192.168.3.14	192.168.3.1	DNS	73	Standard query 0x25fe A www.weibo.com
158	11.207186	192.168.3.1	192.168.3.14	DNS	119	Standard query response 0x25fe A www.weibo.com CNAME weibo.com A 49.7.37.77 A 49.7.37.76
182	11.606779	192.168.3.14	192.168.3.1	DNS	74	Standard query 0x4a31 A ocsp.dccsp.cn
183	11.614242	192.168.3.1	192.168.3.14	DNS	245	Standard query response 0x4a31 A ocsp.dccsp.cn CNAME ocsp.dccsp.cn.w.kunlunar.com A 101.226.26.135 A
184	11.615429	192.168.3.14	192.168.3.1	DNS	89	Standard query 0x605e A ocsp.dccsp.cn.w.kunlunar.com
186	11.622707	192.168.3.1	192.168.3.14	DNS	217	Standard query response 0x605e A ocsp.dccsp.cn.w.kunlunar.com A 101.226.26.128 A 101.226.26.137 A 101.
189	11.623049	192.168.3.14	192.168.3.1	DNS	89	Standard query 0x0d90 AAAA ocsp.dccsp.cn.w.kunlunar.com
191	11.629035	192.168.3.1	192.168.3.14	DNS	152	Standard query response 0x0d90 AAAA ocsp.dccsp.cn.w.kunlunar.com SOA ns3.kunlunar.com
207	11.903416	192.168.3.14	192.168.3.1	DNS	78	Standard query 0xf88d A passport.weibo.com

DNS 只有两种报文：查询报文、响应报文，两者有着相同格式，如下：



注：
查询报文仅仅包含查询部分。响应报文包含查询部分、响应部分，也可能包含其他两部分。

查询报文：

```
> Frame 157: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{90CB2279-4FDD-49D7-8293-23DC640088EA}, id 0
> Ethernet II, Src: IntelCor_9a:dc:a6 (10:3d:1c:9a:dc:a6), Dst: HuaweiDe_19:e7:f4 (a0:de:0f:19:e7:f4)
> Internet Protocol Version 4, Src: 192.168.3.14, Dst: 192.168.3.1
> User Datagram Protocol, Src Port: 61116, Dst Port: 53
  < Domain Name System (query)
    Transaction ID: 0x25fe
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
      > www.weibo.com: type A, class IN
      [Response In: 158]
```

头部：

Transaction ID: DNS 报文的ID 标识，对于请求报文和其对应的应答报文，该字段的值是相同的ID 课题区。通过这个分DNS 应答报文是对哪个请求进行相应的，这里是0x25fe。

Flags:标志（query 查询，query response 响应），此处为 0x0100 Standard query

Questions:问题计数，此处为 1

Answer RRS:回答资源记录数，此处为 0

Authority RRS:权威名称能服务器计数，此处为 0

Additional RRs:附加资源记录数，此处为 0

因查询报文仅包含查询部分，所以**查询部分**：

Queries: 查询问题区域，此处为 www.weibo.com: type A, class IN

响应报文：

```
> User Datagram Protocol, Src Port: 53, Dst Port: 61116
  < Domain Name System (response)
    Transaction ID: 0x25fe
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
    Queries
      > www.weibo.com: type A, class IN
    Answers
      > www.weibo.com: type CNAME, class IN, cname weibo.com
      > weibo.com: type A, class IN, addr 49.7.37.77
      > weibo.com: type A, class IN, addr 49.7.37.76
    [Request In: 157]
    [Time: 0.005734000 seconds]
```


DNS 响应报文的头部、查询问题区域结构基本和响应报文一致。并且一些查询主机的主名字、查询类型等信息也需要保持一致。比如上图的Transaction ID、Flags、Questions、Authority RRs、Additional RRs、Queries，但是此处Answer RRs（应答记录数）的数量变为三个，并且比起查询报文，响应报文多了一个Answers（资源记录部分）。

Task 4: 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。

查询消息不包含任何 answers，查询是‘Type A’，响应提供了三个‘answers’。

```

    v Domain Name System (query)
      Transaction ID: 0x25fe
      > Flags: 0x0100 Standard query
      Questions: 1
      Answer RRs: 0
      Authority RRs: 0
      Additional RRs: 0
      v Queries
        > www.weibo.com: type A, class IN
        [Response In: 158]

    > User Datagram Protocol, Src Port: 53, Dst Port: 61116
    v Domain Name System (response)
      Transaction ID: 0x25fe
      > Flags: 0x8180 Standard query response, No error
      Questions: 1
      Answer RRs: 3
      Authority RRs: 0
      Additional RRs: 0
      v Queries
        > www.weibo.com: type A, class IN
      v Answers
        > www.weibo.com: type CNAME, class IN, cname weibo.com
        > weibo.com: type A, class IN, addr 49.7.37.77
        > weibo.com: type A, class IN, addr 49.7.37.76
      [request in: 157]
      [Time: 0.005734000 seconds]

    v Answers
      v www.weibo.com: type CNAME, class IN, cname weibo.com
        Name: www.weibo.com 域名字段
        Type: CNAME (Canonical NAME for an alias) (5) 类型字段，这里是CNAME
        Class: IN (0x0001) 类字段
        Time to live: 600 (10 minutes) 生存时间
        Data length: 2 数据长度
        CNAME: weibo.com 资源数据，这里是CNAME的信息
      v weibo.com: type A, class IN, addr 49.7.37.77
        Name: weibo.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 600 (10 minutes)
        Data length: 4
        Address: 49.7.37.77
      v weibo.com: type A, class IN, addr 49.7.37.76
        Name: weibo.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 600 (10 minutes)
        Data length: 4
        Address: 49.7.37.76
      [Request In: 157]
      [Time: 0.005734000 seconds]
  
```

五、总结

通过本次实验，我学习了系统命令`nslookup` 的简单使用，学会了三个不同`nslookup`命令的不同结果。理解了DNS 协议并掌握DNS的工作原理，能够实验使用Wireshark 抓取查询和响应报文并分析字段。