

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:22级	上机实践成绩:
指导教师:张召	姓名:郭夏辉	学号:10211900416
上机实践名称:DNS报文分析	上机实践日期:2023年5月12日	上机实践编号:No.10
组号:1-416	上机实践时间:2023年5月12日	

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、实验过程

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。

```
C:\Users\tom>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: 2600:140e:6:ab3::255e
           2600:140e:6:a83::255e
           23.10.222.138
Aliases:   www.mit.edu
           www.mit.edu.edgekey.net
```

在终端中输入 `nslookup www.mit.edu` 可以看到如上结果，其中包括DNS服务器的信息和DNS响应的内容。

DNS服务器的信息：

权威DNS服务器：`moon.ecnu.edu.cn`

权威DNS服务器的IP地址：`202.120.80.2`

DNS响应的内容：

`www.mit.edu`的主机名称：`e9566.dscb.akamaiedge.net`

它的地址：`2600:140e:6:ab3::255e`

`2600:140e:6:a83::255e`

`23.10.222.138`

他的别名：`www.mit.edu`

`www.mit.edu.edgekey.net`

这个响应内容看起来是十分精简的，但是在获得来自mit的本地DNS服务器的响应内容的过程中，应该迭代了很多轮、经历了许多其他DNS服务器才得到这个结果。

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。

根据task1，我们可以看到我的本地DNS服务器是 `moon.ecnu.edu.cn`

```
C:\Users\tom>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:f10f:83:face:b00c:0:25de
           162.125.18.133
```

由此我们可以看到www.google.com的地址是2a03:2880:f10f:83:face:b00c:0:25de(一个ipv6地址)和162.125.18.133,当然google的ip地址肯定不止这两个, DNS这么响应, 推测其中可能涉及到了拥塞控制等调节因素。

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。

首先我要来刷新一下DNS的缓存

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

Windows IP 配置

已成功刷新 DNS 解析缓存。
```

然后我在浏览器中访问github.com,接着就在wireshark中抓取相关的报文:

No.	Time	Source	Destination	Protocol	Length	Info
2174	48.675353	172.30.204.59	202.120.80.2	DNS	70	Standard query 0x6fe2 A github.com
2175	48.678218	202.120.80.2	172.30.204.59	DNS	86	Standard query response 0x6fe2 A github.com A 20.205.243.166
2484	45.295239	172.30.204.59	202.120.80.2	DNS	91	Standard query 0xab00 A settings-win.data.microsoft.com
2485	45.298396	202.120.80.2	172.30.204.59	DNS	222	Standard query response 0xab00 A settings-win.data.microsoft.com CNAME atm-sett

DNS只有两种报文: 查询报文、响应报文, 两者有着相同格式, 如下所示:



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。

各部分的一般属性如下所述:

Transaction ID (事务 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。

Flags (标志)

Questions(问题计数)

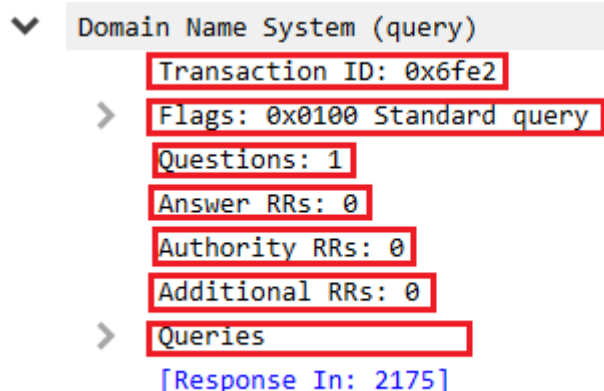
Answer RRs(回答资源记录数)

Authority RRs(权威名称能服务器计数)

Additional RRs(附加资源记录数)

Queries (查询问题区域)

查询报文



查询报文其实并不用特别地去说明了, 上面我所说的一般属性基本全覆盖了, 只用对照着查询就能了解相关的含义。

响应报文

```
▼ Domain Name System (response)
  Transaction ID: 0x6fe2
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  > Queries
  > Answers
  \[Request In: 2174\]
  [Time: 0.002865000 seconds]
```

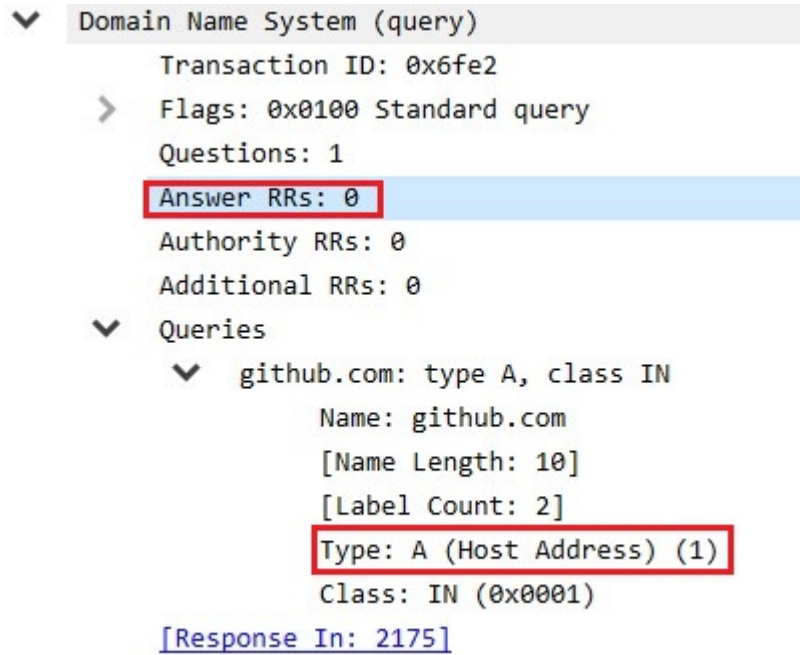
对比发现，虽然响应报文和请求报文差不多，就是一般的属性都有，但是在最后多了一条Answers资源部，这个是用来存放响应的内容的，让好奇的我来点开这个看一下吧：

```
▼ Answers
  ▼ github.com: type A, class IN, addr 20.205.243.166
    Name: github.com
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 11613 (3 hours, 13 minutes, 33 seconds)
    Data length: 4
    Address: 20.205.243.166
```

task4

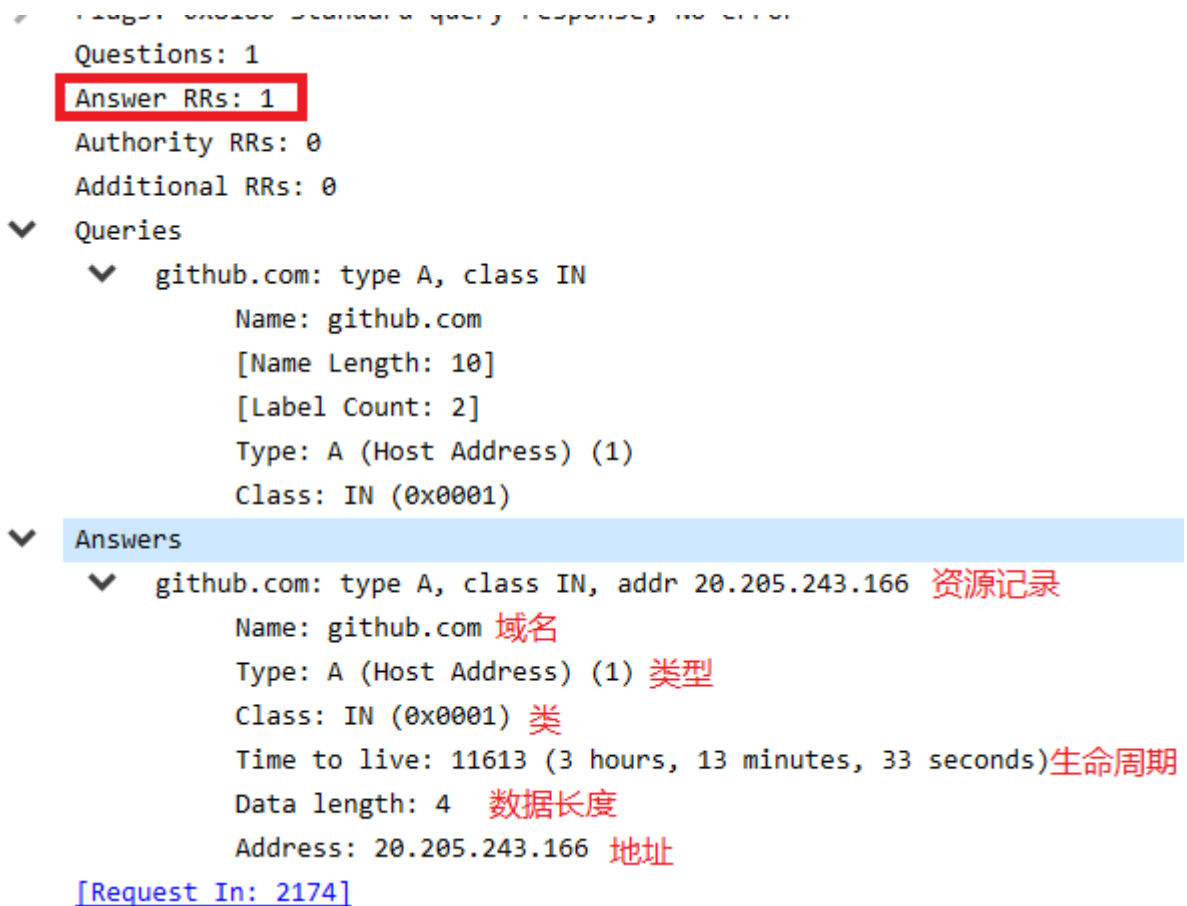
基于task3中得到的查询和响应报文进行分析，试问这里的查询是什么“Type”的，查询消息是否包含任何“answers”？试问这里的响应消息提供了多少个“answers”，这些“answers”具体包含什么？请将实验结果附在实验报告中。

先来看一下响应报文：



可以看到Type是A类型的，而查询消息并不包含任何answers。

然后再来看响应报文：



这里只有一条answer,然后具体的字段之解释我已在图中标明了。

四、总结

整体来说，这是一次简单的实验。凭借wireshark和nslookup这两个有利的工具，我对DNS的理解更进一步，希望未来能更加娴熟地掌握DNS技术，在计算机网络的世界中顺利畅游。