

## 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：2020 级

上机实践成绩：

指导教师：张召

姓名：张熙翔

学号：10205501427

上机实践名称：DNS 报文分析

上机实践日期：2022/5/3

### 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

**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。

windows 平台下打开 cmd 命令行输入指令：`nslookup www.mit.edu`

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。

```
C:\Users\admin>nslookup www.mit.edu
Microsoft Windows [版本 10.0.19044.1645]
(c) Microsoft Corporation。保留所有权利。

C:\Users\admin>nslookup www.mit.edu
服务器: ns-nh2.online.sh.cn
Address: 180.168.255.118

非权威应答:
名称: e9566.dsccb.akamaiedge.net
Addresses: 2600:140b:400:2a8::255e
           2600:140b:400:2a1::255e
           23.201.253.95
Aliases: www.mit.edu
          www.mit.edu.edgekey.net

C:\Users\admin>
```

**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。

使用 DNS 服务器: ns-nh2.online.sh.cn

输入指令: nslookup www.google.com ns-nh2.online.sh.cn

```
C:\Users\admin>nslookup www.google.com ns-nh2.online.sh.cn
服务器: ns-nh2.online.sh.cn
Address: 180.168.255.118

非权威应答:
名称: www.google.com
Addresses: 2001::c73b:95ef
104.16.251.55
```

**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。

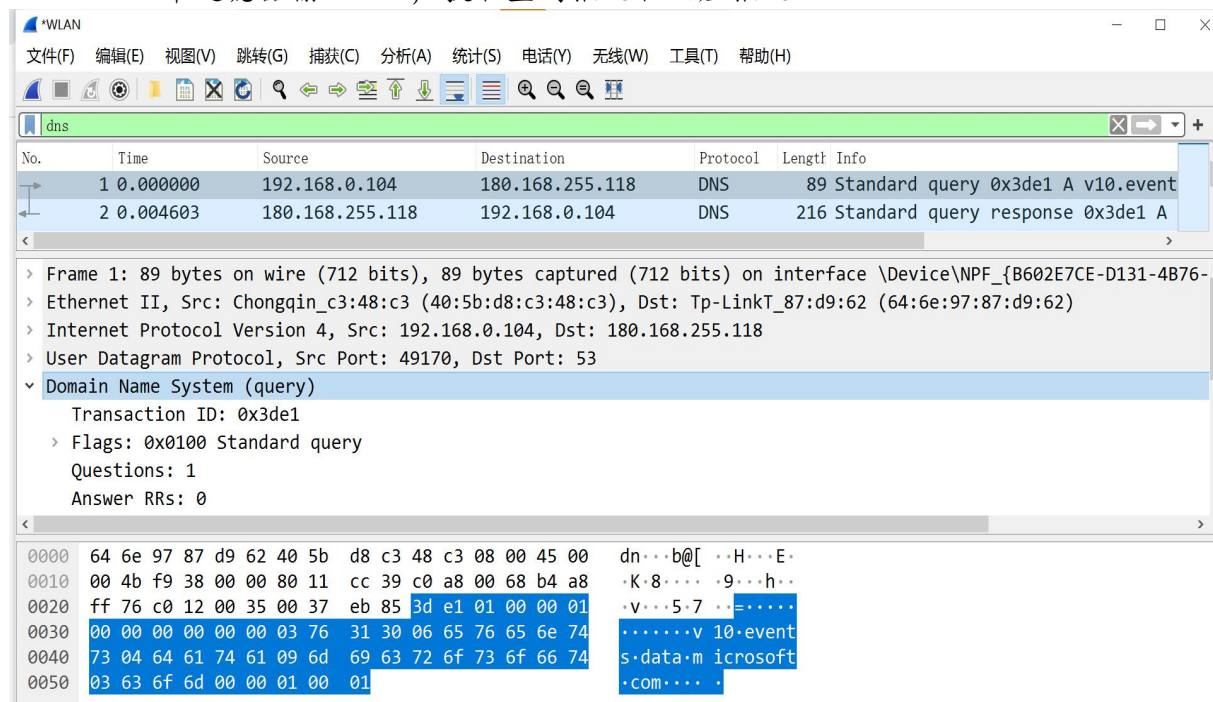
刷新 DNS 解析缓存

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

Windows IP 配置

已成功刷新 DNS 解析缓存。
```

Wireshark 中过滤器输入 dns, 获取查询报文和响应报文:



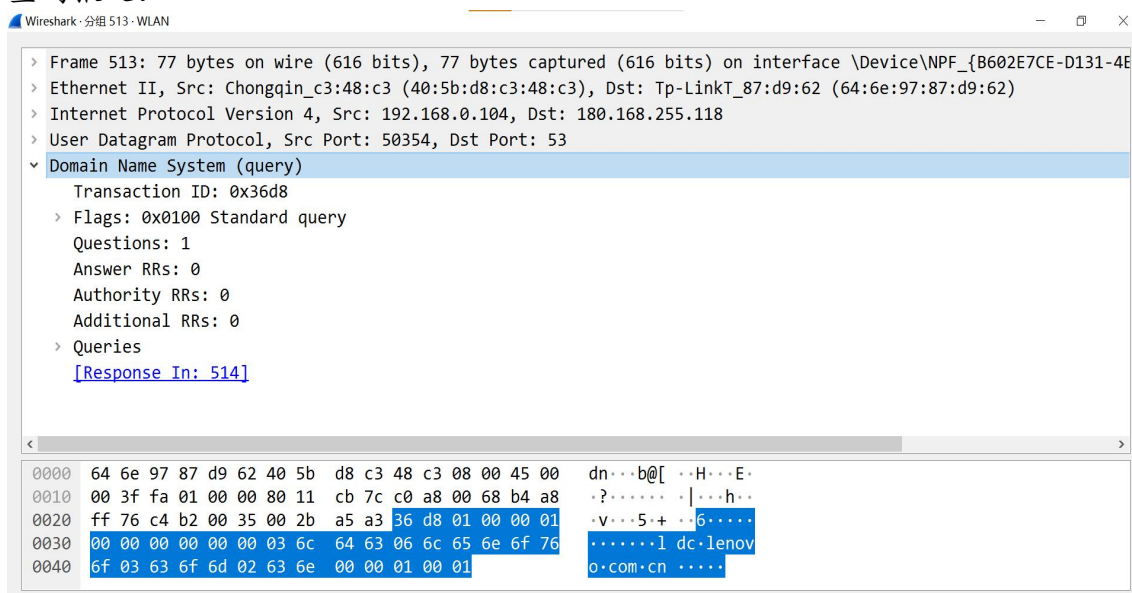
DNS 查询报文和响应报文有相同的格式：



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：



其中各部分如下表所示：

头部	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。
头部	Flags (标志)
头部	Questions(问题计数)
头部	Answer RRs(回答资源记录数)
头部	Authority RRs(权威名称能服务器计数)
头部	Additional RRs(附加资源记录数)
问题部分	Queries (查询问题区域)

响应报文：

Wireshark packet capture showing a DNS response. The packet list shows four packets, with packet 514 selected. The packet details pane shows the structure of the DNS response, including the transaction ID, flags, and the number of questions and answers. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
513	12.290703	192.168.0.104	180.168.255.118	DNS	77	Standard query 0x36d8 A ldc.lenovo.co
514	12.295847	180.168.255.118	192.168.0.104	DNS	229	Standard query response 0x36d8 A ldc.
698	19.708371	192.168.0.104	180.168.255.118	DNS	79	Standard query 0x8b47 A honeycomb.wps
699	19.715040	180.168.255.118	192.168.0.104	DNS	443	Standard query response 0x8b47 A hone

Frame 514: 229 bytes on wire (1832 bits), 229 bytes captured (1832 bits) on interface \Device\NPF\_{B602E7CE-D131-...}

Ethernet II, Src: Tp-LinkT\_87:d9:62 (64:6e:97:87:d9:62), Dst: Chongqin\_c3:48:c3 (40:5b:d8:c3:48:c3)

Internet Protocol Version 4, Src: 180.168.255.118, Dst: 192.168.0.104

User Datagram Protocol, Src Port: 53, Dst Port: 50354

Domain Name System (response)

Transaction ID: 0x36d8

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 7

0020 00 68 00 35 c4 b2 00 c3 6d 54 36 d8 81 80 00 01 .h.5... mT5....

0030 00 07 00 00 00 00 03 6c 64 63 06 6c 65 6e 6f 76 .....l dc.lenov

0040 6f 03 63 6f 6d 02 63 6e 00 00 01 00 01 c0 0c 00 o.com.cn .....l

0050 05 00 01 00 00 09 0b 00 0d 03 6c 64 63 06 6d 62 .....ldc.mb

0060 67 63 64 6e c0 10 c0 2f 00 05 00 01 00 00 75 63 gcdn.../ .....uc

0070 00 1e 03 6c 64 63 06 6c 65 6e 6f 76 6f 03 63 6f ...ldc.l enovo.co

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名字、查询类型等信息也需要保持一致。但是比起查询报文，响应报文多了一个资源记录部分。

Wireshark packet capture showing a DNS response with annotations. The packet details pane shows the structure of the DNS response, including the transaction ID, flags, and the number of questions and answers. The packet bytes pane shows the raw data of the packet.

Frame 514: 229 bytes on wire (1832 bits), 229 bytes captured (1832 bits) on interface

Ethernet II, Src: Tp-LinkT\_87:d9:62 (64:6e:97:87:d9:62), Dst: Chongqin\_c3:48:c3 (40:5b:d8:c3:48:c3)

Internet Protocol Version 4, Src: 180.168.255.118, Dst: 192.168.0.104

User Datagram Protocol, Src Port: 53, Dst Port: 50354

Domain Name System (response)

Transaction ID: 0x36d8 ID标识

Flags: 0x8180 Standard query response, No error 标志

Questions: 1 查询记录数

Answer RRs: 7 应答记录数

Authority RRs: 0 授权记录数

Additional RRs: 0 附加记录数

Queries 查询部分

Answers 响应部分 (资源记录)

ldc.lenovo.com.cn: type CNAME, class IN, cname ldc.mbgcdn.lenovo.com.cn

ldc.mbgcdn.lenovo.com.cn: type CNAME, class IN, cname ldc.lenovo.com.cn.trpcdn.net

0040 6f 03 63 6f 6d 02 63 6e 00 00 01 00 01 c0 0c 00 o.com.cn .....l

0050 05 00 01 00 00 09 0b 00 0d 03 6c 64 63 06 6d 62 .....ldc.mb

0060 67 63 64 6e c0 10 c0 2f 00 05 00 01 00 00 75 63 gcdn.../ .....uc

0070 00 1e 03 6c 64 63 06 6c 65 6e 6f 76 6f 03 63 6f ...ldc.l enovo.co

0080 6d 02 63 6e 06 74 72 70 63 64 6e 03 6e 65 74 00 m.cn.trp cdn.net.



**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。

查询 Type，查询消息不包含任何“answer”：

513	12.290703	192.168.0.104	180.168.255.118	DNS
514	12.295847	180.168.255.118	192.168.0.104	DNS

Domain Name System (query)

Transaction ID: 0x36d8

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

ldc.lenovo.com.cn: type A, class IN

Name: ldc.lenovo.com.cn

[Name Length: 17]

响应消息提供了 7 个“answers”：

Wireshark · 分组 514 · WLAN

Questions: 1

Answer RRs: 7

Authority RRs: 0

Additional RRs: 0

Queries

Answers

ldc.lenovo.com.cn: type CNAME, class IN, cname ldc.mbgcdn.lenovo.com.cn

ldc.mbgcdn.lenovo.com.cn: type CNAME, class IN, cname ldc.lenovo.com.cn.trpcdn.net

ldc.lenovo.com.cn.trpcdn.net: type CNAME, class IN, cname uz95.v.trpcdn.net

uz95.v.trpcdn.net: type A, class IN, addr 180.127.236.58

uz95.v.trpcdn.net: type A, class IN, addr 180.127.236.62

uz95.v.trpcdn.net: type A, class IN, addr 180.127.236.61

uz95.v.trpcdn.net: type A, class IN, addr 180.127.236.57

[Request In: 513]

[Time: 0.005144000 seconds]

“answers” 具体包含：

Answers

资源记录部分

ldc.lenovo.com.cn: type CNAME, class IN, cname ldc.mbgcdn.lenovo.com.cn

Name: ldc.lenovo.com.cn 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: 2315 (38 minutes, 35 seconds) 生存时间

Data length: 13 数据长度

CNAME: ldc.mbgcdn.lenovo.com.cn 资源数据, 这里是 CNAME 的信息

ldc.mbgcdn.lenovo.com.cn: type CNAME, class IN, cname ldc.lenovo.com.cn.trpcdn.net

## 五、总结

通过本次实验，学习了系统命令 `nslookup` 的简单使用，理解了 DNS 协议并掌握 DNS 的工作原理，能够实验使用 **Wireshark** 分析 DNS 协议。