

# 计算机学院 计算机网络 课程实验报告

实验题目：深入理解 DNS 域名系统		学号：202200400053
日期：2024-03-22	班级： 2 班	姓名： 王宇涵
Email：1941497679@qq.com		
<p>实验方法介绍：</p> <ol style="list-style-type: none"><li>通过访问一些网站或执行 DNS 查询操作：分析 DNS 查询和响应。</li><li>在 Wireshark 中观察捕获的数据包，可以利用 Wireshark 的过滤器功能来过滤出与 DNS 相关的数据包，这样可以更轻松的分析 DNS 查询和响应。</li></ol>		
<p>实验过程描述：</p> <p>一：nslookup</p> <p>输入 nslookup www.iitb.ac.in 和 nslookup -type=NS iitb.ac.in 观察结果</p> <pre>Microsoft Windows [版本 10.0.22621.3296] (c) Microsoft Corporation。保留所有权利。  C:\Users\Lenovo&gt;nslookup www.iitb.ac.in 服务器:  pdns.dnspod.cn Address:  119.29.29.29  非权威应答: 名称:      www.iitb.ac.in Address:   103.21.124.10  C:\Users\Lenovo&gt;nslookup -type=NS iitb.ac.in 服务器:  pdns.dnspod.cn Address:  119.29.29.29  非权威应答: iitb.ac.in      nameserver = dns3.iitb.ac.in iitb.ac.in      nameserver = dns1.iitb.ac.in iitb.ac.in      nameserver = dns2.iitb.ac.in</pre> <p>回答问题：</p> <ol style="list-style-type: none"><li>查找获取位于印度孟买的印度理工学院 Web 服务器的 IP 地址：www.iitb.ac.in 的 IP 地址是什么？</li></ol> <p>答：103.21.124.10</p>		

2. 为您提供答案的 DNS 服务器的 IP 地址是什么？

答: 119.29.29.29

3. 上述问题 1 中的命令来自权威服务器还是非权威服务器？

答: 非权威服务器

4. 使用查找命令来确定 iit.ac.in 域的权威名称服务器的名称。那名字是什么？（如果有多个权威服务器，则返回的第一个权威服务器的名称是什么？如果您必须找到该权威名称服务器的 IP 地址，您会怎么做？

```
C:\Users\Lenovo>nslookup dns3.iitb.ac.in
服务器:  pdns.dnspod.cn
Address:  119.29.29.29

非权威应答:
名称:     dns3.iitb.ac.in
Address:  103.21.127.129
```

答：名字为 dns3.iitb.ac.in. 若必须要找到 IP 地址则再进行一次查询即可：返回 IP103.21.127.129

## 二：DNS cache

1. 输入命令ipconfig /flushdns清除DNS缓存，打开 Web 浏览器并清除浏览器缓存。

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

Windows IP 配置

已成功刷新 DNS 解析缓存。
```

2. 打开Wireshark并输入ip.addr == 172.25.241.46进入显示过滤器，使用此过滤器，

Wireshark 将仅显示源自或发往您的主机的数据包。

```
本地链接 IPv6 地址: . . . . . : FE80::B2B7:577C:1BCC
IPv4 地址 . . . . . : 172.25.241.46
```

在 Wireshark 中启动数据包捕获。

使用浏览器访问网页：[http://gaia.cs.umass.edu/kurose\\_ross/](http://gaia.cs.umass.edu/kurose_ross/) 停止数据

3. 使用作者捕获的包进行实验

回答问题：

5. 找到解析名称 `gaia.cs.umass.edu` 的第一条 DNS 查询消息。包裹号码是多少？

在 DNS 查询消息的跟踪中？该查询消息是通过 UDP 还是 TCP 发送的？

```
19 6.003804 10.0.0.44 75.75.75.75 DNS 76 Standard query 0x609b A www.cs.umass.edu
Ethernet II, Src: Apple_08:00:27:1b:41:43, Dst: Maxlinear_00:50:11:80:00:00
Internet Protocol Version 4, Src: 10.0.0.44, Dst: 75.75.75.75
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 62
  Identification: 0xc2aa (49834)
  ▶ 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: UDP (17)
```

答: 包裹号码为19, 该消息是由UDP发送的

6. 现在找到对初始 DNS 查询的相应 DNS 响应。DNS 响应消息跟踪中的数据包编号是多少？该响应消息是通过 UDP 还是 TCP 接收的？

```
20 6.037987 75.75.75.75 10.0.0.44 DNS 92 Standard query response 0x609b A www.cs.umass.edu A 128.119.240.84
Ethernet II, Src: Maxlinear_00:50:11:80:00:00, Dst: Apple_08:00:27:1b:41:43
Internet Protocol Version 4, Src: 75.75.75.75, Dst: 10.0.0.44
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 78
  Identification: 0x0000 (0)
  ▶ 010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 58
  Protocol: UDP (17)
  Header Checksum: 0x9fdd [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 75.75.75.75
  Destination Address: 10.0.0.44
```

答: 编号为 20, 由 UDP 接受的

7. DNS 查询报文的目的端口是什么？DNS 响应报文的源端口是什么？

```
Destination Host End: 75.75.75.75
▶ User Datagram Protocol, Src Port: 57837, Dst Port: 53
```

答: 均为 53

8. DNS 查询报文发送到什么 IP 地址？

```
19 6.003804 10.0.0.44 75.75.75.75 DNS 76 Standard query 0x609b A www.cs.umass.edu
```

答: 75.75.75.75

9. 检查DNS 查询消息。此 DNS 消息包含多少个“问题”？它包含多少个答案？

```
Domain Name System (query)
  Transaction ID: 0x609b
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
```

答: 1 个问题, 0 个回答

10. 检查对初始查询消息的 DNS 响应消息。此 DNS 消息包含多少个“问题”？它包含多少个答案？

```
Domain Name System (response)
  Transaction ID: 0x609b
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  Queries
```

答 : 1 个问题, 1 个回答

11. 基本文件的网页 [http://gaia.cs.umass.edu/kurose\\_ross/](http://gaia.cs.umass.edu/kurose_ross/) 引用图像对象 [http://gaia.cs.umass.edu/kurose\\_ross/header\\_graphic\\_book\\_8E\\_2.jpg](http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E_2.jpg)，与基本网页一样，位于 [gaia.cs.umass.edu](http://gaia.cs.umass.edu)。

基本文件 [http://gaia.cs.umass.edu/kurose\\_ross/](http://gaia.cs.umass.edu/kurose_ross/) 的初始 HTTP GET 请求的跟踪中的数据包编号是多少？为了解析 [gaia.cs.umass.edu](http://gaia.cs.umass.edu) 以便将此初始 HTTP 请求发送到 [gaia.cs.umass.edu](http://gaia.cs.umass.edu) IP 地址而进行的 DNS 查询跟踪中的数据包编号是多少？收到的 DNS 响应跟踪中的数据包编号是多少？

图像对象 [http://gaia.cs.umass.edu/kurose\\_ross/header\\_graphic\\_book\\_8E2.jpg](http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E2.jpg) 的 HTTP GET 请求跟踪中的数据包编号是多少？为了解析 [gaia.cs.umass.edu](http://gaia.cs.umass.edu) 以便将第二个 HTTP 请求发送到 [gaia.cs.umass.edu](http://gaia.cs.umass.edu) IP 地址, DNS 查询中的数据包编号是多少？讨论 DNS 缓存如何影响最后一个问题的答案。

No.	Time	Source	Destination	Protocol	Length	Info
22	3.367054	10.0.0.44	128.119.245.12	HTTP	831	GET /kurose_ross/ HTTP/1.1
28	3.395005	128.119.245.12	10.0.0.44	HTTP	857	HTTP/1.1 200 OK (text/html)
205	3.570142	10.0.0.44	128.119.245.12	HTTP	817	GET /kurose_ross/header_graphic_book_8E_2.jpg HTTP/1.1
516	3.670350	128.119.245.12	10.0.0.44	HTTP	454	HTTP/1.1 200 OK (JPEG/JFIF image)

15	3.325064	10.0.0.44	75.75.75.75	DNS	77 Standard query 0x3c29 A gaia.cs.umass.edu
17	3.348972	75.75.75.75	10.0.0.44	DNS	93 Standard query response 0x3c29 A gaia.cs.umass.edu A 128.119.245.12
205	3.570142	10.0.0.44	128.119.245.12	HTTP	817 GET /kurose_ross/header_graphic_book_8E_2.jpg HTTP/1.1
516	3.670350	128.119.245.12	10.0.0.44	HTTP	454 HTTP/1.1 200 OK (JPEG JFIF image)

  

15	3.325064	10.0.0.44	75.75.75.75	DNS	77 Standard query 0x3c29 A gaia.cs.umass.edu
17	3.348972	75.75.75.75	10.0.0.44	DNS	93 Standard query response 0x3c29 A gaia.cs.umass.edu A 128.119.245.12
30	3.427392	10.0.0.44	75.75.75.75	DNS	83 Standard query 0xeda4 A maxcdn.bootstrapcdn.com
31	3.428514	10.0.0.44	75.75.75.75	DNS	79 Standard query 0x0a79 A ajax.googleapis.com
35	3.445049	75.75.75.75	10.0.0.44	DNS	135 Standard query response 0xeda4 A maxcdn.bootstrapcdn.com CNAME cds.jsz9t3p6.hwcdn.net A 209.197.3.15
36	3.448996	75.75.75.75	10.0.0.44	DNS	95 Standard query response 0x0a79 A ajax.googleapis.com A 172.217.12.202
521	3.678228	10.0.0.44	75.75.75.75	DNS	75 Standard query 0xdcfa A www.pearson.com
522	3.678393	10.0.0.44	75.75.75.75	DNS	79 Standard query 0xb436 A www.vitalsource.com
523	3.678598	10.0.0.44	75.75.75.75	DNS	72 Standard query 0xd3a3 A redshelf.com
525	3.695928	75.75.75.75	10.0.0.44	DNS	169 Standard query response 0xdcfa A www.pearson.com CNAME wildcard.pearson.com.edgekey.net CNAME e290.x.akamaiedge.net A 23.34.92.227
527	3.698647	10.0.0.44	75.75.75.75	DNS	74 Standard query 0xe1a9 A www.amazon.com
528	3.703716	75.75.75.75	10.0.0.44	DNS	159 Standard query response 0xb436 A www.vitalsource.com A 104.17.67.241 A 104.17.65.241 A 104.17.68.241 A 104.17.69.241 A 104.17.66.241
529	3.704968	75.75.75.75	10.0.0.44	DNS	88 Standard query response 0xd3a3 A redshelf.com A 34.196.10.62
530	3.718156	75.75.75.75	10.0.0.44	DNS	169 Standard query response 0xe1a9 A www.amazon.com CNAME tp.47cf2c8c9-frontier.amazon.com CNAME d3ag4hukkh62yn.cloudfront.net A 65.8.192.9
541	6.801907	10.0.0.44	75.75.75.75	DNS	96 Standard query 0x6cf4 A ss-prod-ue1-notif-63.aws.adobess.com
542	6.818616	75.75.75.75	10.0.0.44	DNS	144 Standard query response 0x6cf4 A ss-prod-ue1-notif-63.aws.adobess.com A 52.205.134.231 A 52.20.111.22 A 3.213.114.154

答：HTTP GET 请求的数据包编号为 22，解析的 DNS 查询数据包编号为 15，收到的 DNS 响应跟踪的数据包编号为 17。

图像对象的 HTTP GET 请求的数据包编号为 205，未发现再次解析的 DNS 查询数据包编号。

原因解释：当主机需要调用 DNS 服务时，该主机首先会检查所需的 DNS 记录是否驻留在该主机的 DNS 缓存中；如果找到该记录，主机甚至不会费心联系本地 DNS 服务器，而是使用此缓存的 DNS 记录，因此再次进行 HTTP GET 请求无需解析域名。

### 三：Play With nslookup

#### 12. DNS查询报文的目的端口是什么？DNS响应报文的源端口是什么？

```

▶ Internet Protocol Version 4, Src: 10.0.0.44, Dst: 75.75.75.75
▶ User Datagram Protocol, Src Port: 57837, Dst Port: 53
Domain Name System (query)
Internet Protocol Version 4, Src: 75.75.75.75, Dst: 10.0.0.44
User Datagram Protocol, Src Port: 53, Dst Port: 57837

```

答：查询目的端口为 53，响应源端口为 53

#### 13. DNS查询报文发送到什么IP地址？这是您默认本地 DNS 服务器的 IP 地址吗？

答：发送到 75.75.75.75，这应该是作者抓包时本地 DNS 服务器的 IP 地址

#### 14. 检查 DNS 查询消息。DNS 查询是什么“类型”？查询消息中是否包含任何“答案”？

```

Queries
▶ www.cs.umass.edu: type A, class IN
Answer RRs: 0

```

答：类型：A 不包含任何答案

#### 15.检查对查询消息的 DNS 响应消息。此 DNS 响应消息包含多少个“问题”？有多少个“答案”？

```

Questions: 1
Answer RRs: 1

```

答：1个问题，1个答案

#### 四：打开命令行输入命令 `nslookup - type=NS umass.edu`并抓包

```
13 3.425869 10.0.0.44 75.75.75.75 DNS 69 Standard query 0x6683 NS umass.edu
```

16. DNS 查询报文发送到什么 IP 地址？这是您默认本地 DNS 服务器的 IP 地址吗？

答：发送到 75.75.75.75，应该是本地 DNS 的 IP 地址。

17. 检查 DNS 查询消息。该查询有多少个问题？查询消息中是否包含任何“答案”？

```
Domain Name System (query)
Transaction ID: 0x6683
  Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
```

答：1 个问题, 0 个回答

18. 检查 DNS 响应消息。回应有多少个答案？答案中包含哪些信息？多少额外资源记录被返回？

这些附加资源记录中包含哪些附加信息？

```
Domain Name System (response)
Transaction ID: 0x6683
  Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 3
  Queries
    ▶ umass.edu: type NS, class IN
  Answers
    ▶ umass.edu: type NS, class IN, ns ns1.umass.edu
    ▶ umass.edu: type NS, class IN, ns ns3.umass.edu
    ▶ umass.edu: type NS, class IN, ns ns2.umass.edu
  Additional records
    ▶ ns2.umass.edu: type A, class IN, addr 128.119.10.28
    ▶ ns1.umass.edu: type A, class IN, addr 128.119.10.27
    ▶ ns3.umass.edu: type A, class IN, addr 128.103.38.68
[Request In: 13]
[Time: 0.024632000 seconds]
```

答：回应中有 3 个答案，答案中包含了该域的权威 DNS 服务器的主机名。

3 个额外资源记录被返回，包含这些权威 DNS 服务器的 IP 地址

#### 结论分析：

本次实验我通过执行命令行, WireShark 抓包等操作, 观察 DNS 数据包数据, 从而了解 DNS 的结构层次, DNS 缓存等, 更加深刻地掌握了 DNS 的多方面相关知识, 收获良多。

## 结论：

1. 可以通过命令行进行 nslookup 域名查询操作.
2. 通过分析捕获的数据包，确定 DNS 查询的类型，例如 A 记录、MX 记录、CNAME 记录、NX 记录等.
3. DNS 缓存可以减少对 DNS 服务器的查询次数，提高域名解析的速度.
4. 可以通过分析 DNS 数据包的结构来了解 DNS 协议的工作原理，包括 DNS 报头、问题部分、回答部分、授权部分和附加部分等.