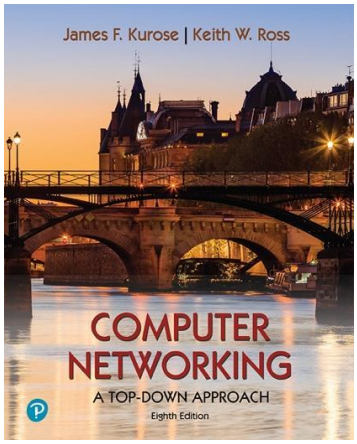
# Wireshark 实验室：

## 域名系统v8.1

补充*计算机网络：自上而下的方法，8th编辑*，JF 黑濑和 KW 罗斯

*“告诉我，我就忘记了。给我看，我就记住了。让我参与，我就能理解。”*中国谚语






---

如正文2.4节所述[1]域名系统 (DNS) 将主机名转换为 IP 地址，在互联网基础设施中发挥着关键作用。在本实验中，我们将仔细研究 DNS 的客户端。回想一下，客户端在 DNS 中的角色相对简单 – 客户端发送一个*询问*到其本地 DNS 服务器，并接收*回复*后退。正如教科书中的图 2.19 和 2.20 所示，当分层 DNS 服务器相互通信以递归或迭代地解析客户端的 DNS 查询时，许多事情都可以在“幕后”进行，而 DNS 客户端是看不到的。然而，从 DNS 客户端的角度来看，该协议非常简单 – 向本地 DNS 服务器制定查询并从该服务器接收响应。

在开始本实验之前，您可能需要阅读本文的第 2.4 节来回顾 DNS。特别是，您可能需要查看有关的材料**本地 DNS 服务器**,**DNS缓存**,**DNS 记录和消息**，以及**类型字段**在 DNS 记录中。

## 1. nslookup

让我们通过检查以下内容来开始对 DNS 的调查：查找命令，它将调用底层 DNS 服务来实现其功能。这查找
该命令在大多数 Microsoft、Apple IOS 和 Linux 操作系统中可用。跑步查找你只需输入查找DOS 窗口、Mac IOS 终端窗口或 Linux shell 中的命令行上的命令。

在其最基本的操作中，查找允许主机运行查找查询任何指定的 DNS 服务器的 DNS 记录。查询的 DNS 服务器可以是根 DNS 服务器、顶级域 (TLD) DNS 服务器、权威 DNS 服务器或中间 DNS 服务器（有关这些术语的定义，请参阅教科书）。例如，

---

[1]对图和章节的引用适用于 8th我们文本的版本，*计算机网络，自上而下方法，8H编辑，JF Kurose 和 KW Ross，Addison-Wesley/Pearson，2020*。我们这本书的网站是 http://gaia.cs.umass.edu/kurose_ross 您会在那里找到很多有趣的开放材料。

查找可用于检索将主机名（例如 www.nyu.edu）映射到其 IP 地址的“Type=A”DNS 记录。为了完成这个任务，查找向指定的 DNS 服务器（或所在主机的默认本地 DNS 服务器）发送 DNS 查询
查找如果没有指定特定的 DNS 服务器，则运行），从该 DNS 服务器接收 DNS 响应，并显示结果。

让我们来查找出去转转！我们先运行查找在位于马萨诸塞大学 (UMass) 校园 CS 系的 newworld.cs.umass.edu 主机上的 Linux 命令行上，本地名称服务器被命名为

primo.cs.umass.edu（IP 地址为 128.119.240.1）。咱们试试吧查找在其最简单的形式：

```
newworld.cs.umass.edu> nslookup www.nyu.edu
Server:         128.119.240.1
Address:        128.119.240.1#53

Non-authoritative answer:
www.nyu.edu     canonical name = WEB.GSLB.nyu.edu.
Name:   WEB.GSLB.nyu.edu
Address: 216.165.47.12
Name:   WEB.GSLB.nyu.edu
Address: 2607:f600:1002:6113::100
```

**图1：**基础的查找命令

在这个例子中查找命令有一个参数，即主机名 (www.nyu.edu)。换句话说，该命令的意思是“请向我发送主机 www.nyu.edu 的 IP 地址。” 如屏幕截图所示，该命令的响应提供了两条信息：(1) 提供答案的 DNS 服务器的名称和 IP 地址 - 在本例中为 UMass 的本地 DNS 服务器；(2) 答案本身，即 www.nyu.edu 的规范主机名和 IP 地址。您可能已经注意到，提供了两个名称/地址对www.nyu.edu 。第一个 (216.165.47.12) 是一个 IPv4 地址，采用看起来很熟悉的点分十进制表示法；第二个 (2607:f600:1002:6113::100) 是一个更长、更复杂的 IPv6 地址。我们将在第 4 章后面了解 IPv4 和 IPv6 以及它们的两种不同的寻址方案。现在，让我们只关注更舒适（和常见）的 IPv4 世界[2]。

尽管响应来自麻省大学的本地 DNS 服务器（IP 地址为 128.119.240.1），但该本地 DNS 服务器很可能反复联系其他几个 DNS 服务器来获取答案，如教科书第 2.4 节中所述。

除了使用查找要查询 DNS“Type=A”记录，我们还可以使用
查找到查找查询“TYPE=NS”记录，该记录返回权威 DNS 服务器的主机名（及其 IP 地址），该服务器知道如何获取权威服务器域中主机的 IP 地址。

---

[2]对于 Mac OS，如果您只想在 IPv4 世界中工作：系统首选项 -> 网络。然后选择您的活动接口（例如，Wi-Fi）和高级->TCP/IP。然后选择“配置 IPv6”下拉菜单并将其设置为“仅限本地链接”或“关闭”。

```
newworld.cs.umass.edu> nslookup -type=NS nyu.edu
Server:         128.119.240.1
Address:        128.119.240.1#53

Non-authoritative answer:
nyu.edu nameserver = ns2.nyu.org.
nyu.edu nameserver = ns4.nyu.edu.
nyu.edu nameserver = ns1.nyu.net.

Authoritative answers can be found from:
ns2.nyu.org     internet address = 128.122.0.76
ns1.nyu.net     internet address = 128.122.0.8
ns4.nyu.edu     internet address = 216.165.87.102
ns4.nyu.edu     has AAAA address 2607:f600:2001:6100::135
```

**图2：**使用查找查找 nyu.edu 域的权威名称服务器

在图 2 的示例中，我们调用了查找带有选项“-type=NS”和域“nyu.edu”。这导致查找将类型 NS 记录的查询发送到默认本地 DNS 服务器。换句话说，该查询的意思是：“请将 nyu.edu 的权威 DNS 的主机名发送给我”。（当不使用--type选项时，*查找*使用默认值，即查询类型 A 记录。）上面的屏幕截图中显示的答案首先指示提供答案的 DNS 服务器（这是地址为 128.119.240.1 的默认本地 UMass DNS 服务器）以及三个 NYU DNS 名称服务器。这些服务器中的每一个实际上都是纽约大学校园主机的权威 DNS 服务器。然而，查找还表明答案是“非权威的”，这意味着该答案来自某个服务器的缓存，而不是来自权威的 NYU DNS 服务器。最后，答案还包括纽约大学权威 DNS 服务器的 IP 地址。（即使由生成的类型 NS 查询查找没有明确询问 IP 地址，本地 DNS 服务器“免费”返回这些地址，并且*查找*显示结果。）

查找除了“-type=NS”之外，您可能还想探索一些其他选项。这是一个网站，其中包含十个流行的屏幕截图查找用途：https://www.cloudns.net/blog/10-most-used-nslookup-commands/ 以下是 nslookup 的“手册页”：https://linux.die.net/man/1/nslookup 。

最后，我们有时可能有兴趣发现与给定 IP 地址关联的主机名称，即图 1 中所示查找的反向操作（其中主机名称已知/指定，并且返回主机的 IP 地址）。查找也可用于执行所谓的“反向 DNS 查找”。例如，在图 3 中，我们指定一个 IP 地址作为查找参数（本例中为 128.119.245.12）和查找返回具有该地址的主机名（本例中为 gaia.cs.umass.edu）

```
kurose@MacBook-Pro-6 ~ % nslookup 128.119.245.12
Server:         75.75.75.75
Address:        75.75.75.75#53

Non-authoritative answer:
12.245.119.128.in-addr.arpa     name = gaia.cs.umass.edu.

Authoritative answers can be found from:
```

**图3：**使用查找执行“反向 DNS 查找”

现在我们已经提供了概述ns查找，现在是您亲自试驾的时候了。执行以下操作（并写下结果[3]）。如果您将此实验作为课堂的一部分进行，您的老师将提供有关如何提交作业（无论是书面作业还是在学习管理系统中）的详细信息。如果您无法运行查找命令或正在使用 LMS 回答此问题，图 4 显示了执行该命令的屏幕截图查找问题 1 和 4 中的内容将帮助您回答以下问题。

1. 跑步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。www.iitb.ac.in 的 IP 地址是什么

2. 为您提供答案的 DNS 服务器的 IP 地址是什么
   查找上面问题1中的命令?
3. 是否回答了您的问题查找上述问题1中的命令来自权威服务器还是非权威服务器?
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

   nslookup）？如果您必须找到该权威名称服务器的 IP 地址，您会怎么做?

```
kurose@MacBook-Pro-6 ~ % nslookup www.iitb.ac.in
Server:         75.75.75.75
Address:        75.75.75.75#53

Non-authoritative answer:
Name:   www.iitb.ac.in
Address: 103.21.124.10

kurose@MacBook-Pro-6 ~ % nslookup -type=NS iitb.ac.in
Server:         75.75.75.75
Address:        75.75.75.75#53

Non-authoritative answer:
iitb.ac.in      nameserver = dns1.iitb.ac.in.
iitb.ac.in      nameserver = dns2.iitb.ac.in.
iitb.ac.in      nameserver = dns3.iitb.ac.in.
```

**图4：**使用查找查找 www.iitb.ac.in 的 IP 地址和名称
iitb.ac.in 域的权威名称服务器

## 2.您计算机上的 DNS 缓存

从我们教科书中对迭代和递归 DNS 查询解析的描述（图 2.19 和 2.20）来看，您可能会认为必须联系本地 DNS 服务器*每一个*

---

[3]在笔者的课堂上，学生在通过交作业回答以下问题时，
有时需要打印出特定的数据包（有关如何执行此操作的说明，请参阅介绍性 Wireshark 实验室）并指出他们在数据包中的何处找到了回答问题的信息。他们通过用笔标记纸质副本或用彩色字体的文本注释电子副本来做到这一点。还有供教师使用的学习管理系统 (LMS) 模块，允许学生在线回答这些问题，并为这些 Wireshark 实验室自动评分答案

http://gaia.cs.umass.edu/kurose_ross/lms.htm

应用程序需要将主机名转换为 IP 地址的时间。但实际情况并非总是如此！

大多数主机（例如，您的个人计算机）都保留一个*缓存*最近检索到的 DNS 记录（有时称为 DNS*解析器缓存*），就像许多 Web 浏览器保留最近通过 HTTP 检索到的对象的缓存一样。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。解析器缓存中的 DNS 记录最终将超时并从解析器缓存中删除，就像本地 DNS 服务器中缓存的记录（参见图 2.19、2.20）将超时一样。

您还可以明确清除 DNS 缓存中的记录。这样做并没有什么坏处，只是意味着您的计算机下次需要使用 DNS 名称解析服务时需要调用分布式 DNS 服务，因为它将在缓存中找不到任何记录。在 Mac 计算机上，您可以在终端窗口中输入以下命令来清除 DNS 解析器缓存：

sudo Killall -HUP mDNSResponder
在 Windows 计算机上，您可以在命令提示符下输入以下命令：
ipconfig /flushdns
在 Linux 计算机上输入：
sudo systemd-resolve --flush-caches

## 3. 使用 Wireshark 跟踪 DNS

现在我们已经熟悉了查找清除 DNS 解析器缓存后，我们就可以开始处理一些重要的事情了。让我们首先捕获普通网上冲浪活动生成的 DNS 消息。

- 如上所述，清除主机中的 DNS 缓存。打开 Web 浏览
- 器并清除浏览器缓存。
- 打开Wireshark并输入ip.addr == <你的IP地址>进入显示过滤器，其中<你的IP地址>是您计算机的 IPv4 地址[4]。使用此过滤器，Wireshark 将仅显示源自或发往您的主机的数据包。

- 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/ 停止数据
- 包捕获。

[4]如果您不确定如何查找计算机的 IP 地址，可以在网络上搜索适用于您的操作系统的文章。
Windows 10 信息是这里 ; Mac 信息是这里 ; Linux 信息是这里

如果您无法在实时网络连接上运行 Wireshark，您可以下载在作者的一台计算机上执行上述步骤时捕获的数据包跟踪文件[5]。回答下列问题。

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[6]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？

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？

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？

8. DNS查询报文发送到什么IP地址？
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”答案？
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”答案？

11. 基础文件的网页 http://gaia.cs.umass.edu/kurose_ross/ 引用了图像对象

    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 上。基本文件的初始 HTTP GET 请求的跟踪中的数据包编号是多少
    http://gaia.cs.umass.edu/kurose_ross/? 为了解析 gaia.cs.umass.edu 以便将此初始 HTTP 请求发送到 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？图像对象的 HTTP GET 请求跟踪中的数据包编号是多少

    http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E2.jpg? 为解析 gaia.cs.umass.edu 以便将第二个 HTTP 请求发送到 gaia.cs.umass.edu IP 地址而进行的 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。

现在我们来玩一下恩斯洛库*p*[7]。

- 开始抓包。
- 做一个查找在 www.cs.umass.edu
- 停止数据包捕获。

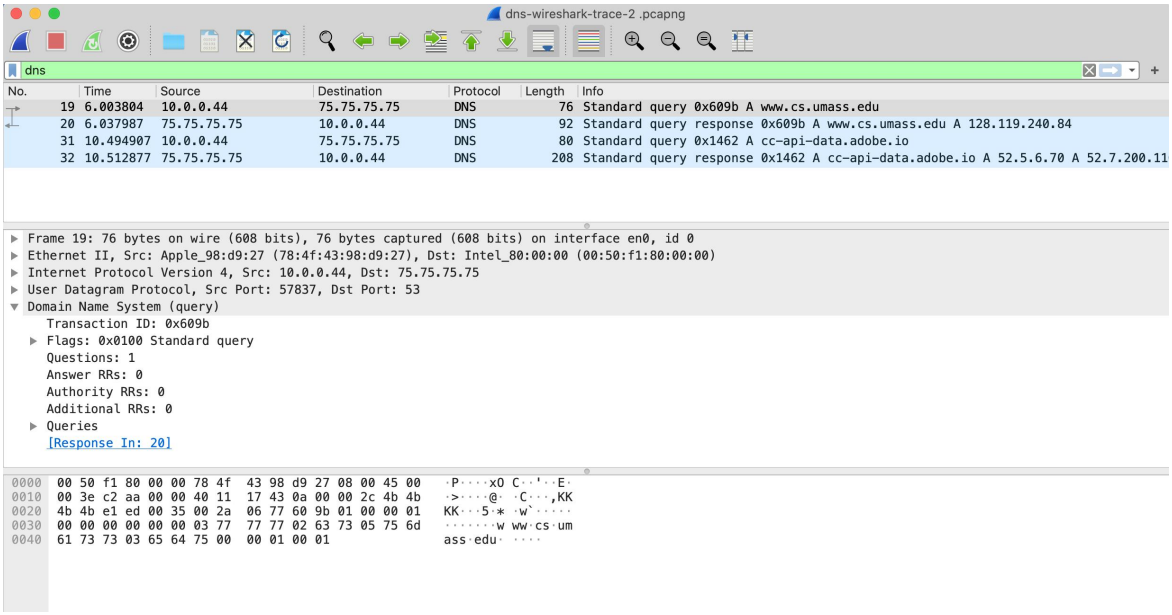
---

[5]您可以下载 zip 文件http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces-8.1.zip 和提取跟踪文件 dns-wireshark-trace1-1。这些跟踪文件可用于回答这些 Wireshark 实验室问题，而无需您自己实际捕获数据包。每个跟踪都是使用在作者的一台计算机上运行的 Wireshark 进行的，同时执行 Wireshark 实验室中指示的步骤。下载跟踪文件后，您可以将其加载到 Wireshark 中并使用以下命令查看跟踪：*文件*下拉菜单，选择*打开*，然后选择跟踪文件名。

[6]请记住，此“数据包编号”由 Wireshark 分配，仅用于列出目的；它不是一个任何真实数据包标头中包含的数据包编号。

[7]如果您无法运行 Wireshark 并捕获跟踪文件，或者正在使用 LMS，请使用跟踪文件 dns-上面脚注中痕迹 zip 文件中的wireshark-trace-2 回答了下面的问题 12-16。

您应该在 Wireshark 窗口中看到类似于以下内容的跟踪。我们来看第一个A类查询（下图中的19号数据包，在报文中用“A”表示）*信息*该数据包的列。




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？

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？

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”？
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”？

最后，让我们使用查找要发出返回 NS 类型 DNS 记录的命令，请输入以下命令：

nslookup –type=NS umass.edu 然后回
答以下问题[8]:

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？

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”？
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

[8]如果您无法运行 Wireshark 并捕获跟踪文件，或者正在使用 LMS，请使用跟踪文件*dnswireshark-trace-3*在上面脚注中的踪迹 zip 文件中回答下面的问题 17-19。

记录被返回？这些附加资源记录中包含哪些附加信息？