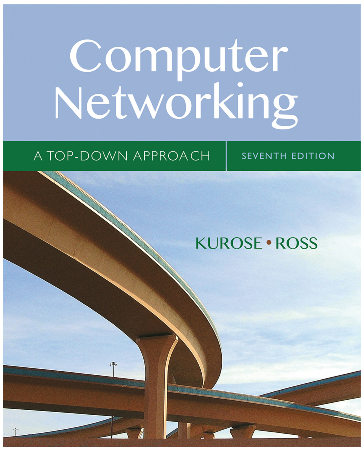
Wireshark Lab: DNS v7.0

Supplement to *Computer Networking: A Top-Down Approach, 7th ed.,* J.F. Kurose and K.W. Ross



"Tell me and I forget. Show me and I remember. Involve me and I understand." Chinese proverb

---

As described in Section 2.4 of the text[1], the Domain Name System (DNS) translates hostnames to IP addresses, fulfilling a critical role in the Internet infrastructure. In this lab, we'll take a closer look at the client side of DNS. Recall that the client's role in the DNS is relatively simple – a client sends a *query* to its local DNS server, and receives a *response* back. As shown in Figures 2.19 and 2.20 in the textbook, much can go on "under the covers," invisible to the DNS clients, as the hierarchical DNS servers communicate with each other to either recursively or iteratively resolve the client's DNS query. From the DNS client's standpoint, however, the protocol is quite simple – a query is formulated to the local DNS server and a response is received from that server.

如本文第 2.4 节所述，域名系统（DNS）将主机名转换为 IP 地址，从而在 Internet 基础结构中发挥关键作用。 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 - 客户端向其本地 DNS 服务器发送查询，然后收到响应。 如教科书中的图 2.19 和 2.20 所示，DNS 客户端看不到"隐藏起来"，因为分层 DNS 服务器相互通信以递归或迭代方式解析客户端的 DNS 查询。 但是，从 DNS 客户端的角度来看，协议非常简单 - 对本地 DNS 服务器进行查询，并从该服务器接收响应。

Before beginning this lab, you'll probably want to review DNS by reading Section 2.4 of the text. In particular, you may want to review the material on **local DNS servers**, **DNS caching**, **DNS records and messages**, and the **TYPE field** in the DNS record.

在开始本实验之前，您可能需要阅读书中的第 2.4 节来了解 DNS。另外，您可能需要查看关于**本地 DNS 服务器，DNS 缓存，DNS 记录和消息，以及 DNS 记录中的 TYPE 字段**的资料。

1. nslookup

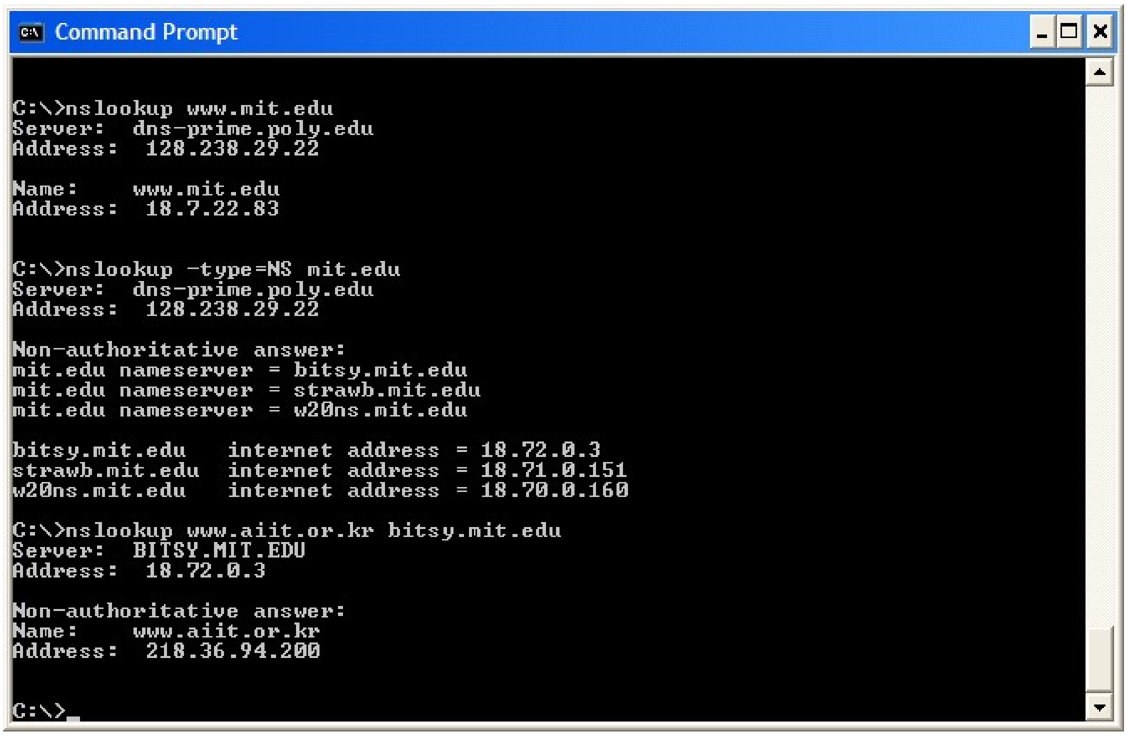
[1] References to figures and sections are for the 7th edition of our text, *Computer Networks, A Top-down Approach, 7th ed.,* J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2016.

In this lab, we’ll make extensive use of the *nslookup* tool, which is available in most Linux/Unix and Microsoft platforms today. To run *nslookup* in Linux/Unix, you just type the *nslookup* command on the command line. To run it in Windows, open the Command Prompt and run *nslookup* on the command line.

在本实验中，我们将广泛使用 nslookup 工具，该工具现在在大多数 Linux / Unix 和 Microsoft 平台上都可用。 要在 Linux / Unix 中运行 nslookup，只需在命令行上键入 nslookup 命令即可。 要在 Windows 中运行它，请打开命令提示符并在命令行上运行 nslookup。

In it is most basic operation, *nslookup* tool allows the host running the tool to query any specified DNS server for a DNS record. The queried DNS server can be a root DNS server, a top-level-domain DNS server, an authoritative DNS server, or an intermediate DNS server (see the textbook for definitions of these terms). To accomplish this task, *nslookup* sends a DNS query to the specified DNS server, receives a DNS reply from that same DNS server, and displays the result.

在最基本的操作中，nslookup 工具允许运行该工具的主机向任何指定的 DNS 服务器查询 DNS 记录。 查询的 DNS 服务器可以是根 DNS 服务器，顶级域 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）。 要完成此任务，nslookup 会将 DNS 查询发送到指定的 DNS 服务器，从同一 DNS 服务器接收 DNS 回复，并显示结果。



```
C:\>nslookup www.mit.edu
Server:  dns-prime.poly.edu
Address:  128.238.29.22

Name:    www.mit.edu
Address:  18.7.22.83


C:\>nslookup -type=NS mit.edu
Server:  dns-prime.poly.edu
Address:  128.238.29.22

Non-authoritative answer:
mit.edu nameserver = bitsy.mit.edu
mit.edu nameserver = strawb.mit.edu
mit.edu nameserver = w20ns.mit.edu

bitsy.mit.edu   internet address = 18.72.0.3
strawb.mit.edu  internet address = 18.71.0.151
w20ns.mit.edu   internet address = 18.70.0.160

C:\>nslookup www.aiit.or.kr bitsy.mit.edu
Server:  BITSY.MIT.EDU
Address:  18.72.0.3

Non-authoritative answer:
Name:    www.aiit.or.kr
Address:  218.36.94.200


C:\>_
```

The above screenshot shows the results of three independent *nslookup* commands (displayed in the Windows Command Prompt). In this example, the client host is located on the campus of Polytechnic University in Brooklyn, where the default local DNS server is dns-prime.poly.edu. When running *nslookup*, if no DNS server is specified, then *nslookup* sends the query to the default DNS server, which in this case is dns-prime.poly.edu. Consider the first command:

上面的屏幕截图显示了三个独立的 nslookup 命令的结果（显示在 Windows 命令提示符中）。 在此示例中，客户端主机位于布鲁克林的理工大学校园内，默认本地 DNS 服务器为 dns-prime.poly.edu。 运行 nslookup 时，如果未指定 DNS 服务器，则 nslookup 将查询发送到默认 DNS 服务器，在本例中为 dns-prime.poly.edu。 考虑第一个命令：

```
nslookup www.mit.edu
```

In words, this command is saying “please send me the IP address for the host www.mit.edu”. As shown in the screenshot, the response from this command provides two pieces of information: (1) the name and IP address of the DNS server that provides the answer; and (2) the answer itself, which is the host name and IP address of www.mit.edu. Although the response came from the local DNS server at Polytechnic University, it is quite possible that this local DNS server iteratively contacted several other DNS servers to get the answer, as described in Section 2.4 of the textbook.

说这个命令是说，请告诉我主机 www.mit.edu 的 IP 地址。如屏幕截图所示，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。虽然响应来自理工大学的本地 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，如书中第 2.4 节所述。

Now consider the second command:

现在来看第二个命令：

```
nslookup –type=NS mit.edu
```

In this example, we have provided the option “-type=NS” and the domain “mit.edu”. This causes *nslookup* to send a query for a type-NS record to the default local DNS server. In words, the query is saying, “please send me the host names of the authoritative DNS for mit.edu”. (When the –type option is not used, *nslookup* uses the default, which is to query for type A records.) The answer, displayed in the above screenshot, first indicates the DNS server that is providing the answer (which is the default local DNS server) along with three MIT nameservers. Each of these servers is indeed an authoritative DNS server for the hosts on the MIT campus. However, *nslookup* also indicates that the answer is “non-authoritative,” meaning that this answer came from the cache of some server rather than from an authoritative MIT DNS server. Finally, the answer also includes the IP addresses of the authoritative DNS servers at MIT. (Even though the type-NS query generated by *nslookup* did not explicitly ask for the IP addresses, the local DNS server returned these “for free” and *nslookup* displays the result.)

在这个例子中，我们添加了选项"-type=NS"和域名"mit.edu"。这将使得 *nslookup* 将 NS 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。）上述屏幕截图中，首先显示了提供响应的 DNS 服务器（这是默认本地 DNS 服务器）以及三个 MIT 域名服务器。这些服务器中的每一个确实都是麻省理工学院校园主机的权威 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。最后，响应结果还显示了麻省理工学院权威 DNS 服务器的 IP 地址。 （即使 *nslookup* 生成的 NS 类型查询没有明确要求 IP 地址，本地 DNS 服务器依然”免费“返回了这些信息，然后被 *nslookup* 显示出来。）

Now finally consider the third command:

最后来看第三个命令：

```
nslookup www.aiit.or.kr bitsy.mit.edu
```

In this example, we indicate that we want to the query sent to the DNS server bitsy.mit.edu rather than to the default DNS server (dns-prime.poly.edu). Thus, the query and reply transaction takes place directly between our querying host and bitsy.mit.edu. In this example, the DNS server bitsy.mit.edu provides the IP address of the host www.aiit.or.kr, which is a web server at the Advanced Institute of Information Technology (in Korea).

在这个例子中，我们希望将查询请求发送到 DNS 服务器 bitsy.mit.edu ，而不是默认的 DNS 服务器（dns-prime.poly.edu）。因此，查询和响应事务直接发生在我们的主机和 bitsy.mit.edu 之间。在这个例子中，DNS 服务器 bitsy.mit.edu 提供主机 www.aiit.or.kr 的 IP 地址，它是高级信息技术研究所（韩国）的 Web 服务器。

Now that we have gone through a few illustrative examples, you are perhaps wondering about the general syntax of *nslookup* commands. The syntax is:

现在我们已经完成了一些示例性示例，您可能想知道 nslookup 命令的一般语法。语法是：

```
nslookup –option1 –option2 host-to-find dns-server
```

In general, *nslookup* can be run with zero, one, two or more options. And as we have seen in the above examples, the dns-server is optional as well; if it is not supplied, the query is sent to the default local DNS server.

一般来说，*nslookup* 可以不添加选项，或者添加一两个甚至更多选项。正如我们在上面的示例中看到的，dns-server 也是可选的；如果这项没有提供，查询将发送到默认的本地 DNS 服务器。

Now that we have provided an overview of *nslookup*, it is time for you to test drive it yourself. Do the following (and write down the results):

现在我们提供了总览了 *nslookup*，现在是你自己驾驭它的时候了。执行以下操作（并记下结果）：

1. Run *nslookup* to obtain the IP address of a Web server in Asia. What is the IP address of that server?

   运行 *nslookup* 以获取一个亚洲的 Web 服务器的 IP 地址。该服务器的 IP 地址是什么？

2. Run *nslookup* to determine the authoritative DNS servers for a university in Europe.

   运行 *nslookup* 来确定一个欧洲的大学的权威 DNS 服务器。

3. Run *nslookup* so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

   运行 *nslookup*，使用问题 2 中一个已获得的 DNS 服务器，来查询 Yahoo! 邮箱的邮件服务器。它的 IP 地址是什么？

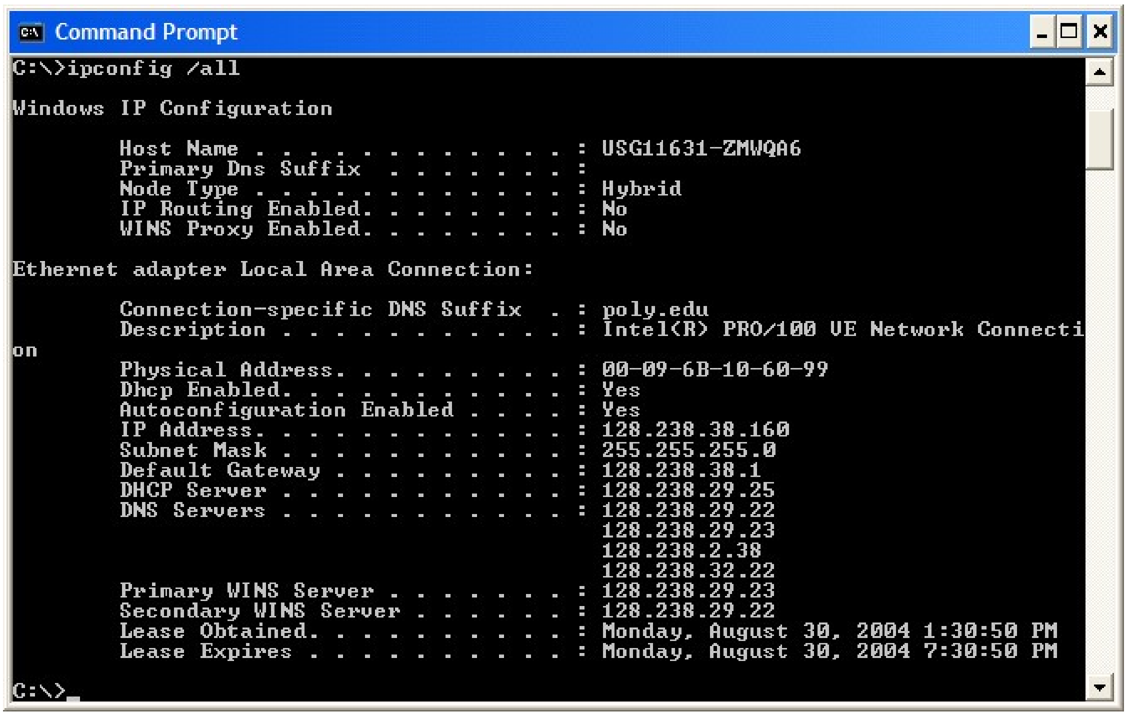
2. ipconfig

ipconfig (for Windows) and *ifconfig* (for Linux/Unix) are among the most useful little utilities in your host, especially for debugging network issues. Here we'll only describe *ipconfig*, although the Linux/Unix *ifconfig* is very similar. *ipconfig* can be used to show your current TCP/IP information, including your address, DNS server addresses, adapter type and so on. For example, if you all this information about your host simply by entering *ipconfig*（对于 Windows）和 *ifconfig*（对于 Linux / Unix）是主机中最实用的程序，尤其是用于调试网络问题时。这里我们只讨论 *ipconfig*，尽管 Linux / Unix 的 *ifconfig* 与其非常相似。 *ipconfig* 可用于显示您当前的 TCP/IP 信息，包括您的地址，DNS 服务器地址，适配器类型等。例如，您只需进入命令提示符，输入

```
ipconfig \all
```

into the Command Prompt, as shown in the following screenshot.

所有关于您的主机信息都类似如下面的屏幕截图所显示。



```
C:\>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : USG11631-ZMWQA6
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : poly.edu
        Description . . . . . . . . . . . : Intel(R) PRO/100 VE Network Connecti
on
        Physical Address. . . . . . . . . : 00-09-6B-10-60-99
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 128.238.38.160
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 128.238.38.1
        DHCP Server . . . . . . . . . . . : 128.238.29.25
        DNS Servers . . . . . . . . . . . : 128.238.29.22
                                            128.238.29.23
                                            128.238.2.38
                                            128.238.32.22
        Primary WINS Server . . . . . . . : 128.238.29.23
        Secondary WINS Server . . . . . . : 128.238.29.22
        Lease Obtained. . . . . . . . . . : Monday, August 30, 2004 1:30:50 PM
        Lease Expires . . . . . . . . . . : Monday, August 30, 2004 7:30:50 PM

C:\>_
```

ipconfig is also very useful for managing the DNS information stored in your host. In Section 2.5 we learned that a host can cache DNS records it recently obtained. To see these cached records, after the prompt C:\> provide the following command:

朗读 ipconfig 对于管理存储在主机中的 DNS 信息也非常有用。在 2.5 节中，我们了解到主机可以缓存最近获得的 DNS 记录。要查看这些缓存的记录，请在提示符 C：\>之后提供以下命令：

```
ipconfig /displaydns
```

Each entry shows the remaining Time to Live (TTL) in seconds. To clear the cache, enter

每个条目显示剩余的生存时间（TTL）（秒）。要清除缓存，请输入

```
ipconfig /flushdns
```

Flushing the DNS cache clears all entries and reloads the entries from the hosts file.

清除了所有条目并从 hosts 文件重新加载条目。

3. Tracing DNS with Wireshark

Now that we are familiar with *nslookup* and *ipconfig*, we're ready to get down to some serious business. Let's first capture the DNS packets that are generated by ordinary Web-surfing activity.

- Use *ipconfig* to empty the DNS cache in your host.
- Open your browser and empty your browser cache. (With Internet Explorer, go to Tools menu and select Internet Options; then in the General tab select Delete Files.)
- Open Wireshark and enter "ip.addr == your_IP_address" into the filter, where you obtain your_IP_address with ipconfig. This filter removes all packets that neither originate nor are destined to your host.
- Start packet capture in Wireshark.
- With your browser, visit the Web page: http://www.ietf.org
- Stop packet capture.

- 使用 *ipconfig* 清空主机中的 DNS 缓存。
- 打开浏览器并清空浏览器缓存。（若使用 Internet Explorer，转到**工具**菜单并选择 **Internet 选项**；然后在**常规**选项卡中选择删除文件。）
- 打开 Wireshark，然后在过滤器中输入"ip.addr==your_IP_address"，您可以先使用 *ipconfig* 获取你的 IP 地址。此过滤器将删除既从你主机不发出也不发往你主机的所有数据包。
- 在 Wireshark 中启动数据包捕获。
- 使用浏览器访问网页：http://www.ietf.org
- 停止数据包捕获。

If you are unable to run Wireshark on a live network connection, you can download a packet trace file that was captured while following the steps above on one of the author's computers[2]. Answer the following questions. Whenever possible, when answering a question below, you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout[3] to explain your answer. To print a packet, use *File->Print*, choose *Selected packet only*, choose *Packet summary line,* and select the minimum amount of packet detail that you need to answer the question.

如果您无法在实时网络连接上运行 Wireshark，则可以下载在作者计算机之一上执行上述步骤时捕获的数据包跟踪文件。 回答下列问题。 只要有可能，在回答下面的问题时，您应该在跟踪中提交用于回答问题的数据包的打印输出。 注释打印输出以解释您的答案。 要打印数据包，请使用文件 - >打印，选择仅选定数据包，选择数据包摘要行，然后选择回答问题所需的最小数据包详细信息量。

4. Locate the DNS query and response messages. Are then sent over UDP or TCP?
5. What is the destination port for the DNS query message? What is the source port of DNS response message?
6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?
7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?
9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?
10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

4. 找到 DNS 查询和响应消息。它们是否通过 UDP 或 TCP 发送？

[2] Download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zipand extract the file dns-ethereal-trace-1. The traces in this zip file were collected by Wireshark running on one of the author’s computers, while performing the steps indicated in the Wireshark lab. Once you have downloaded the trace, you can load it into Wireshark and view the trace using the *File* pull down menu, choosing *Open*, and then selecting the dns-ethereal-trace-1 trace file.

下载 zip 文件 http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip 并解压缩文件 dns-ethereal-trace-1。 此 zip 文件中的跟踪是由作者计算机上运行的 Wireshark 收集的，同时执行 Wireshark 实验室中指示的步骤。 下载跟踪后，可以将其加载到 Wireshark 并使用 File 下拉菜单查看跟踪，选择 Open，然后选择 dns-ethereal-trace-1 跟踪文件。

[3] What do we mean by “annotate”? If you hand in a paper copy, please highlight where in the printout you’ve found the answer and add some text (preferably with a colored pen) noting what you found in what you ‘ve highlight. If you hand in an electronic copy, it would be great if you could also highlight and annotate.

“注释”是什么意思？ 如果您提交纸质副本，请突出显示您在打印输出中找到答案的位置并添加一些文本（最好使用彩色笔），注意您在突出显示的内容中找到的内容。 如果您提交电子副本，如果您还可以突出显示和注释，那将会非常棒。

5. DNS 查询消息的目标端口是什么？ DNS 响应消息的源端口是什么？
6. DNS 查询消息发送到哪个 IP 地址？使用 ipconfig 来确定本地 DNS 服务器的 IP 地址。这两个 IP 地址是否相同？
7. 检查 DNS 查询消息。DNS 查询是什么"Type"的？查询消息是否包含任何"answers"？
8. 检查 DNS 响应消息。提供了多少个"answers"？这些答案具体包含什么？
9. 考虑从您主机发送的后续 TCP SYN 数据包。 SYN 数据包的目的 IP 地址是否与 DNS 响应消息中提供的任何 IP 地址相对应？
10. 这个网页包含一些图片。在获取每个图片前，您的主机是否都发出了新的 DNS 查询？

Now let’s play with *nslookup*[4].

现在让我们玩玩 *nslookup*

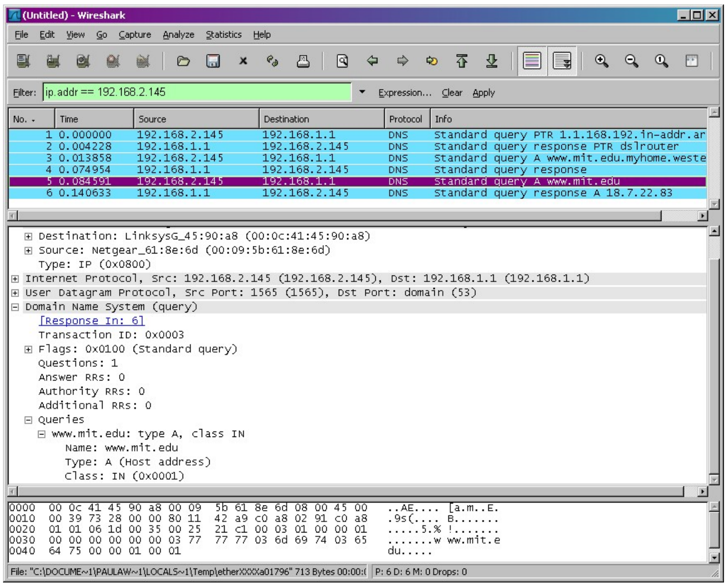
- Start packet capture.
- Do an *nslookup* on www.mit.edu
- Stop packet capture.

- 启动数据包捕获。
- 使用 nslookup 查询 www.mit.edu
- 停止数据包捕获。

You should get a trace that looks something like the following:

[4] If you are unable to run Wireshark and capture a trace file, use the trace file dns-ethereal-trace-2 in the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip
如果您无法运行 Wireshark 并捕获跟踪文件，请使用 zip 文件中的跟踪文件 dns-ethereal-trace-2 http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip

你应该得到类似下图所示的捕获结果：


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply

Filter: ip.addr == 192.168.2.145

```
No. -  Time      Source         Destination    Protocol Info
     1 0.000000  192.168.2.145  192.168.1.1    DNS      Standard query PTR 1.1.168.192.in-addr.ar
     2 0.004228  192.168.1.1    192.168.2.145  DNS      Standard query response PTR dslrouter
     3 0.013858  192.168.2.145  192.168.1.1    DNS      Standard query A www.mit.edu.myhome.weste
     4 0.074954  192.168.1.1    192.168.2.145  DNS      Standard query response
     5 0.084591  192.168.2.145  192.168.1.1    DNS      Standard query A www.mit.edu
     6 0.140633  192.168.1.1    192.168.2.145  DNS      Standard query response A 18.7.22.83
```

```
  ⊞ Destination: LinksysG_45:90:a8 (00:0c:41:45:90:a8)
  ⊞ Source: Netgear_61:8e:6d (00:09:5b:61:8e:6d)
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 192.168.2.145 (192.168.2.145), Dst: 192.168.1.1 (192.168.1.1)
⊞ User Datagram Protocol, Src Port: 1565 (1565), Dst Port: domain (53)
⊟ Domain Name System (query)
    [Response In: 6]
    Transaction ID: 0x0003
  ⊞ Flags: 0x0100 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ www.mit.edu: type A, class IN
        Name: www.mit.edu
        Type: A (Host address)
        Class: IN (0x0001)
```

```
0000   00 0c 41 45 90 a8 00 09  5b 61 8e 6d 08 00 45 00   ..AE.... [a.m..E.
0010   00 39 73 28 00 00 80 11  42 a9 c0 a8 02 91 c0 a8   .9s(.... B.......
0020   01 01 06 1d 00 35 00 25  21 c1 00 03 01 00 00 01   .....5.% !.......
0030   00 00 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   .......w ww.mit.e
0040   64 75 00 00 01 00 01                               du.....
```

File: "C:\DOCUME~1\PAULAW~1\LOCALS~1\Temp\etherXXXXa01796" 713 Bytes 00:00:(P: 6 D: 6 M: 0 Drops: 0

We see from the above screenshot that *nslookup* actually sent three DNS queries and received three DNS responses. For the purpose of this assignment, in answering the following questions, ignore the first two sets of queries/responses, as they are specific to *nslookup* and are not normally generated by standard Internet applications. You should instead focus on the last query and response messages.

我们从上面的屏幕截图看到，*nslookup* 实际上发送了三个 DNS 查询，并收到了三个 DNS 响应。只考虑本次实验相关结果，在回答以下问题时，请忽略前两组查询/响应，因为 *nslookup* 的一些特殊性，这些查询通常不是由标准网络应用程序生成的。您应该专注于最后一个查询和响应消息。

11. What is the destination port for the DNS query message? What is the source port of DNS response message?
12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?
15. Provide a screenshot.

11. DNS 查询消息的目标端口是什么？ DNS 响应消息的源端口是什么？
12. DNS 查询消息的目标 IP 地址是什么？这是你的默认本地 DNS 服务器的 IP 地址吗？
13. 检查 DNS 查询消息。DNS 查询是什么"Type"的？查询消息是否包含任何"answers"？
14. 检查 DNS 响应消息。提供了多少个"answers"？这些答案包含什么？
15. 提供屏幕截图。

Now repeat the previous experiment, but instead issue the command:

现在重复上一个实验，但换成以下命令：

```
nslookup –type=NS mit.edu
```

Answer the following questions[5] :

16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?
19. Provide a screenshot.

回答下列问题：

16. DNS 查询消息发送到的 IP 地址是什么？这是您的默认本地 DNS 服务器的 IP 地址吗？
17. 检查 DNS 查询消息。DNS 查询是什么"Type"的？查询消息是否包含任何"answers"？
18. 检查 DNS 响应消息。响应消息提供的 MIT 域名服务器是什么？此响应消息还提供了 MIT 域名服务器的 IP 地址吗？
19. 提供屏幕截图。

[5] If you are unable to run Wireshark and capture a trace file, use the trace file dns-ethereal-trace-3 in the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip
如果您无法运行 Wireshark 并捕获跟踪文件，请使用 zip 文件中的跟踪文件 dns-ethereal-trace-3 http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip

Now repeat the previous experiment, but instead issue the command:

现在重复上一个实验，但换成以下命令：

```
nslookup www.aiit.or.kr bitsy.mit.edu
```

Answer the following questions[6]:

20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?
21. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
22. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?
23. Provide a screenshot.

回答下列问题：

20. DNS 查询消息发送到的 IP 地址是什么？这是您的默认本地 DNS 服务器的 IP 地址吗？如果不是，这个 IP 地址是什么？
21. 检查 DNS 查询消息。DNS 查询是什么"Type"的？查询消息是否包含任何"answers"？
22. 检查 DNS 响应消息。提供了多少个"answers"？这些答案包含什么？
23. 提供屏幕截图。

[6] If you are unable to run Wireshark and capture a trace file, use the trace file dns-ethereal-trace-4 in the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip
如果您无法运行 Wireshark 并捕获跟踪文件，请使用 zip 文件中的跟踪文件 dns-ethereal-trace-4 http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip