Wireshark DNS lab quiz results for Ngoc Dao

Score for this attempt: **7** out of 7

Submitted 28 Mar at 14:42

This attempt took 46 minutes.

Page 1 of 8

Adapted from Version: 2.0 (c) 2007 J.F. Kurose, K.W. Ross. All Rights Reserved

As described in Section 2.5 of the textbook, 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 2.21 and 2.22 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.

Before beginning this lab, you'll probably want to review DNS by reading Section 2.5 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.

1. nslookup

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
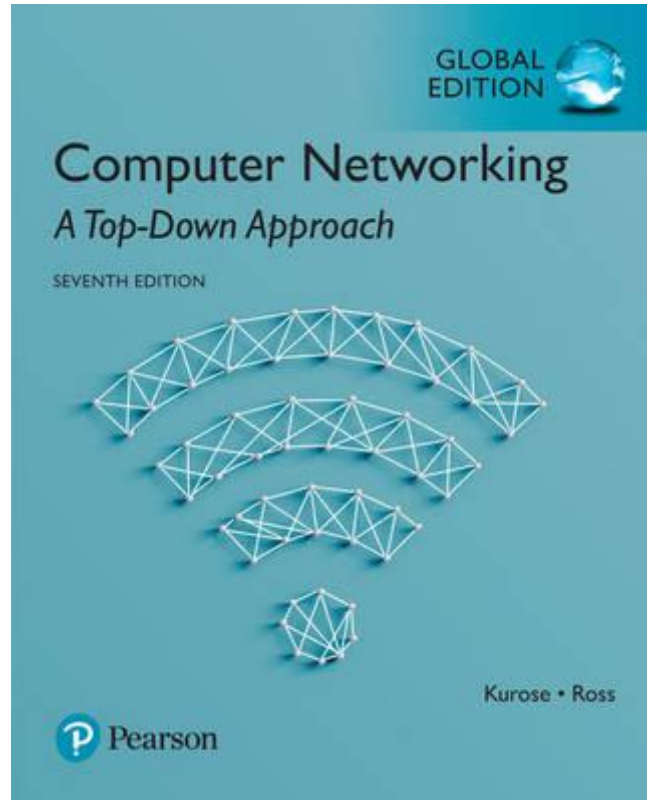
nslookup in Linux/Unix, you just type the `nslookup` command on the command line. To run it in Windows, open the Command Prompt and run `nslookup` on the command line.
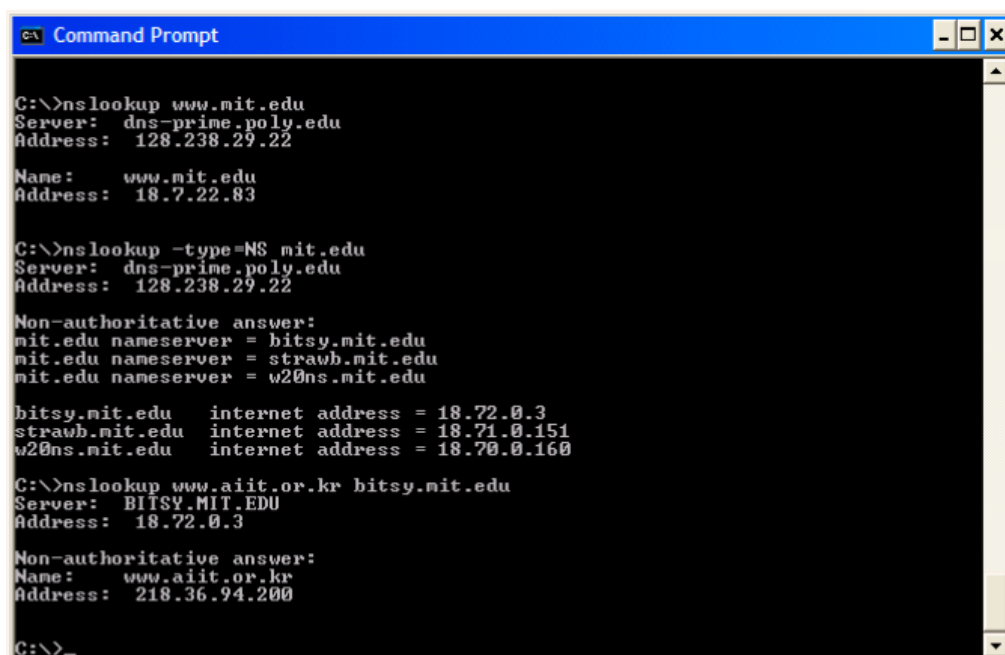
In it is most basic operation, `nslookup` tool allows the host running the tool to query any specified DNS server for a DNS record. The queried DNS server can be a root DNS server, a top-level-domain DNS server, an authoritative DNS server, or an intermediate DNS server (see the textbook for definitions 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.

dig

nslookup has largely been superseded by dig on Unix systems which provides more functionality and an easier to read response format. However nslookup is still supported (it was deprecated for a while but is now supported again) and is provided on all platforms. So we will use nslookup for compatibility, but have a look if you have the dig command (standard with Unix machines). You can use dig instead of nslookup for the questions in this lab and are encouraged to do so if you have it available.

`man dig` will give you the manual page.

Page 2 of 8

```
Command Prompt                                          _ □ ×

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:

```
nslookup www.mit.edu

dig 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 includes 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 2.5 of the textbook.

Try it yourself and discover your own local name server. Note the port number (marked by '#') that is

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 name servers. 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. Note this will only occur if these addresses are currently cached at your local name server. If you're working in the labs, they may be cached from another student's nslookups.)

Now finally consider the third command:

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

dig @bitsy.mit.edu
www.aiit.or.kr
```

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

being used. See if the IP address of www.mit.edu has changed since the above capture (in 2007).

Now consider the second command:

```
nslookup -type=NS mit.edu

dig mit.edu ns
```

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; see Section 2.5.3 in the text.)

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).

Times change and the name servers in this capture and the host www.aiit.or.kr no longer exists.

Run a -type=NS nslookup to find a current nameserver for the mit.edu domain.

You can find Korea Advanced Institute of Science and Technology at http://www.kaist.edu. Send a query for http://www.kaist.edu to one of the current mit.edu name servers.

If you try to run the above you will find that many namer servers will not perform such a query on your behalf (effectively a recursive query since the name server has to do the work for you). Think about the security issues we discussed in lecture and how this might help prevent the University computers from becoming part of a denial of service attack. If you're unsure, bring this up in your tutorial session.

Find out the current nameservers for kaist.edu. Try your query for

www.kaist.edu to one of these
nameservers. Does it work?

Page 3 of 8

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

```
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.

`dig` has an extensive range of options which you can see by looking at
`man dig`

Now that we have provided an overview of nslookup, it is time for you to
test drive it yourself. Do the following:

1. Run `nslookup` or `dig` to obtain the IP address of a Web server in
Asia.
2. Run `nslookup` or `dig` to determine the authoritative DNS servers
for a university in Europe.
3. Run `nslookup` or `dig` so that one of the DNS servers obtained in
Question 2 is queried for the mail servers for Yahoo! mail.

Page 4 of 8

`ipconfig` (for Windows) and `/sbin/ifconfig` (for Linux/Unix) are among the most useful little utilities in your host, especially for	`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

debugging network issues. Type `man ifconfig` to get an `ifconfig` manual page on Linux/Unix. Both do far more than we will see here and are particularly useful for checking if your network configuration is correct.

`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 want to see all this information about your host, simply enter:

`ipconfig /all`

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

On Unix machines look in the `/etc/resolv.conf` file to see your local DNS

`less /etc/resolv.conf`

DNS records it recently obtained. To see these cached records, after the prompt C:\> provide the following command:

`ipconfig /displaydns`

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

`ipconfig /flushdns`

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

On Unix/Linux unprivileged users can not flush the local DNS cache. Again consider the possibilities of DNS cache poisoning (sending incorrect information to the cache) and how this may impact on security.

```
Command Prompt                                                    _ □ ×
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:\>_
```

Question 1	1 / 1 pts

Page 5 of 8

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.

If you are on a windows host, do the following:

1. Use `ipconfig` to empty the DNS cache in your host.
2. 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.)
3. Open Wireshark and enter "dns && ip.addr == your_IP_address" into the filter, where you obtain your_IP_address (the IP address for the computer on which you are running Wireshark) with `ipconfig`. This filter removes all packets that neither originate nor are destined to your host or are not dns packets.
4. Start packet capture in Wireshark.
5. With your browser, visit the Web page: `http://www.ietf.org`
6. Stop packet capture.

If you are on a Linux/Unix machine and do not have privileges to clear your host cache (or don't know how to) you can download this **dns-tracefile (https://myuni.adelaide.edu.au/courses/85255/files/12505086/download?wrap=1)** ↓ **(https://myuni.adelaide.edu.au/courses/85255/files/12505086/download?download_frd=1)** that was captured while following the steps above. Or you could give it a try if you haven't been to www.ietf.org in a few days (it may not be cached). But if you don't see a DNS request, then download the tracefile.

Answer the following questions

What is the destination port for the DNS query message for www.ietf.org?

enter a number

Correct!

53

The port reserved for DNS is port 53. Ports reserved for a specific application are known as "well-known ports". Some other examples of "well-known ports" you have seen so far are port 80 for HTTP and port 25 for SMTP.

You can find the list of "well-known ports" at the Internet Assigned Number Authority (IANA) http://www.iana.org/assignments/port-numbers

orrect Answers   53 (with margin: 0)

Question 2   1 / 1 pts

What 'Type' of DNS query is generated when you download the **www.ietf.org** ⤷ **(http://www.ietf.org/)** web site?"

○ MX

Correct!

◉ A

The web browser needs the authoritative (A) record mapping the hostname www.ietf.org to its IP address.

○ CNAME

○ NS

Question 3   1 / 1 pts

How many 'answers' are provided in the DNS response to the DNS query for www.ietf.org?

Enter a number.

Correct!

> 3

> It is possible to return more than one if a single host has more than one address. In the capture file both a CNAME (alias) as well as two address mappings are returned as answers.

orrect Answers   3 (with margin: 0)

Question 4   1 / 1 pts

Which of the following are contained in the DNS response?

Select all that appear in the DNS response.

Correct!

☑ authoritative nameservers for the domain

> The original query, the authoritative name servers (if not cached) and the IP address of the host being resolved are all returned in the response.

☐ date/time

Correct!

☑ IP address of host being looked up (resolved)

> The original query, the authoritative name servers (if not cached) and the IP address of the host being resolved are all returned in the response.

Correct!

☑ the original query

> The original query, the authoritative name servers (if not cached) and the IP address of the host being resolved are all returned in the response.

Question 5   1 / 1 pts

A DNS query is made for each image in the web page.
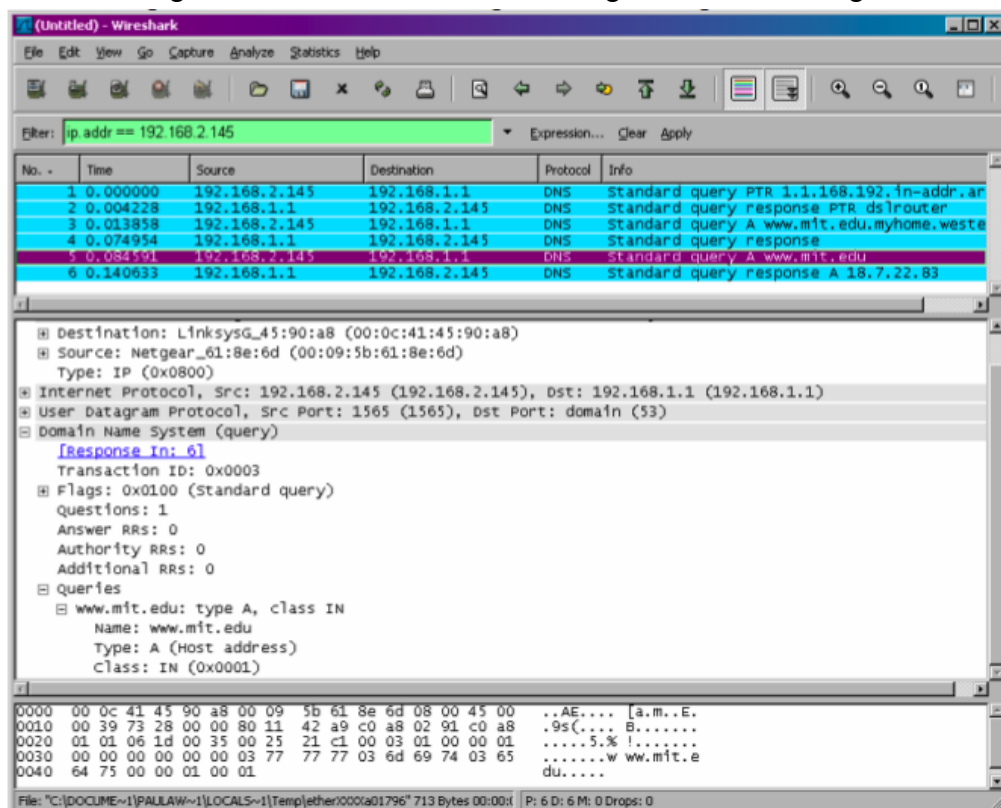
   ○ True

Correct!

   ◉ False

> Only one DNS query is needed. The images are all on the same
> server, so the IP address is cached after the first lookup.

Page 6 of 8

Now let's play with `nslookup` or `dig`.

1. Start packet capture.
2. Do an `nslookup` or `dig` on `www.mit.edu`
3. Stop packet capture.

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

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 for www.mit.edu and response
messages.

Answer the following questions

Question 6   1 / 1 pts

What is contained in the response to the DNS query generated by the
command nslookup -type=NS **mit.edu** ⤷ **(http://www.mit.edu/)**

Correct!

⦿ The authoritative name servers for the mit.edu domain

> The request specifies the type NS (name servers) and this is what
> is returned.

○ The aliases for the mit.edu domain

○ The mail server for the mit.edu domain

○ The IP address of www.mit.edu

Page 8 of 8

| In lecture we looked at an *iterative DNS query*. In these queries, if the local dns does not have the full or part of the answer in its cache, it iteratively asks name servers how to find the information. Let's assume we are looking for www.ietf.org and the local name server does not have this host's IP address cached, does not have | Another alternative is for the local name server to ask the root name server and then have the root name server ask the TLD server and have the TLD server ask the authoritative server. So each server that is asked, recursively passes on the query to the next level closer to the authoritative DNS server. Then the answer is |

ietf.org's name server and does not have the top level domain (TLD) .org name server cached. If it had one of these cached it could ask the cached server directly.

The local name server starts by querying the root name server, which will tell it where to find the top level domain (TLD) server, for the domain. In our example the root name server will tell the local name server the name server (and IP address) for .org

The local name server then asks the .org name server, which will reply with the name server for ietf.org

Finally the local name server asks the name server for ietf.org (the authoritative name server), which responds with the IP address of the host www.ietf.org.

This can be seen in the figure below from the text.
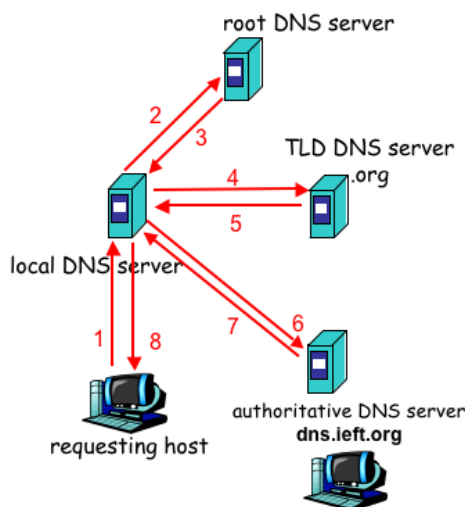
recursively passed back up the chain until it reaches the local DNS server. This *recursive query* can be seen in the picture from the textbook below.
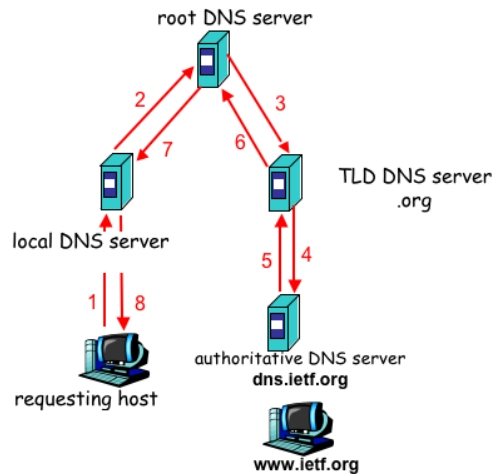
In reality both recursive and iterative queries can be used within a single request. The local DNS is performing a recursive query for the local host, as it forwards the query to another server and forwards the reply to the local host.

Consider carefully both types of queries in terms of load and vulnerability to attacks (denial of service, cache poisoning) for each server involved.

Then answer the following question.

Question 7

1 / 1 pts

Consider carefully both types of queries in terms of load and vulnerability to attacks (denial of service, cache poisoning) for each server involved.

Which type of query is more likely to be allowed by a *root name server*?

Correct!

◉ iterative query

> As well as tying up resources for longer while awaiting query responses, providing recursive queries can also make the server susceptible to several security attacks.
>
> See www.cert.org/archive/pdf/dns.pdf

○ recursive query

Quiz score: **7** out of 7