Exploring Domain Name Services

The UNIX system command nslookup can be used to look up information in the domain name services. You can find out about how to use this command using the UNIX man command. It also has some brief built-in help that you can get by typing `?` on a line by itself. Here is a sample interaction:

```
nslookup
Default Server:  venkman.ics.mq.edu.au
Address:  137.111.216.56

> pompeii.ics.mq.edu.au
Server:  venkman.ics.mq.edu.au
Address:  137.111.216.56

Name:    pompeii.ics.mq.edu.au
Address:  137.111.235.16

>
```

You will obtain a lot more information if you first use the command `> set querytype=ANY` to tell nslookup to return all types of information about the requested host. Using nslookup, find out what you can about the following domain names:

- pompeii.ics.mq.edu.au
- venkman.ics.mq.edu.au
- www.ics.mq.edu.au
- ics.mq.edu.au
- mq.edu.au
- edu.au
- au
- edu
- whitehouse.gov

From what you’ve found out, what host handles e-mails sent to mq.edu.au, ics.mq.edu.au? What is the name server for ics.mq.edu.au domain? for mq.edu.au?

Monitoring TCP application protocols

`Relay.c` is the course code for a TCP relay server. You start this server and specify what port it is to sit on, and also a remote host and port number on that host. When a client connects to the relay server, the relay server connects to the remote host and the remote port. It then acts as a middle-man passing on whatever it receives from the client to the remote server, and whatever it receives from the remote server to the client.

Everything that is passed back and forth is also printed out to your terminal via stderr.

You can use this relay server to observe various protocols in action. For example:
1. Start to relay server so that it connects to a telnet server and itself serves port 2000.

   relay 2000 pompeii.mq.edu.au 23

   The telnet well-known port is 23, as found in /etc/services.

   Now connect to the relay server from telnet using

   telnet pompeii 2000

   The relay server passes your interaction to the remote telnet server and the output of the telnet server back to the telnet client. It is not easy to see what is travelling in what direction because the telnet protocol is not line oriented. You will notice some strange characters being transmitted. Remember that \377 (octal) is 255 i.e. IAC.

2. Start the relay server so that it connects to a web server and itself serves port 2000.

   relay 2000 www.comp.mq.edu.au 80

   Now connect to the relay server from a web browser and interact with the www.comp.mq.edu.au web server. Everything that is transferred appears in the window where you started the relay server.

   By this means, you can observe how information is sent to fill in a form, and all the other types of interaction supported by web browsers.

3. Start the relay server so that it connects to an ftp server (port 21). Now you can monitor the control channel transactions for an ftp session (but not the data transactions) that you start explicitly by

   ftp pompeii 2000

   **Note:** you **cannot** use relay.c to monitor your interactions with the SFTP server in assignment 1.