CS 309
Assignment 9

1. Using tcpdump answer the following questions?

   (a) What types of packets arrive or leave my system in a 5 second period. Not every packet, just what types. Which of these can you not identify?

   (b) What happens on the network if I ping another system?

   (c) Suppose you have reason to believe that someone is trying to exploit your web server. Give a tcpdump command to help test this theory.

2. Using Ethereal, capture 10 seconds of udp traffic. Try some of the nice features of Ethereal, such as filtering post capture with the display filters and sorting the order. For example, you might capture some TCP traffic and try to solve problem 3 above with Ethereal.

   In the interest of your learning to do this on your own, the documentation for Ethereal is at http://www.ethereal.com/docs and it is quite complete.

3. Use traceroute to check out the route to a couple of places, like google.com. Also, check out stanford.edu. This is interesting because of the difference in response times. Why?