DNS

Introduction

The Domain Name System (DNS) is a distributed database used to store various types of information required for the proper operation of the Internet.

In this lab you will use the nslookup utility to query DNS servers for various types of information and the Wireshark protocol analyzer to examine the requests and responses.

Procedure

Download the DNS wireshark labs from http://www-net.cs.umass.edu/wireshark-labs/.

You can use the lecture notes as reference material instead of the authors' text.

The Internet has changed significantly since the lab was written. Many authoritative DNS servers no longer act as recursive name servers and so they will not respond to queries for which they are not authoritative. Some recursive name servers only respond to queries originating from hosts within their organization.

Many of the DNS servers mentioned in the lab will no longer be available. You can use Google's DNS servers (8.8.8.8 or 8.8.4.4) instead.

UDP and TCP are transport layer protocols that operate "over" the IP protocol. The SYN packet is used to start a TCP connection. Both TCP and UDP packets include a "port" value in their headers that Wireshark can display. You should be able to do the lab without knowing how these protocols operate. We will study UDP and TCP later in this the course.

Pre-Lab

Download the lab from the link above and read it. If you have any questions, ask them in class or in the lab. You do not have to submit a pre-lab report for this lab.

Report

Prepare a report answering the 23 questions posed in the lab.

The best way to include Wireshark output for your report may be to display only the portions of the packet you need to show and save a packet range in plain text format with "as displayed" packet details.

You can view this file with the Notepad text editor and import it into your word processor in a format that preserves line breaks. Use small monospaced fonts to maintain formatting.