ICSI 516 Homework 2 – Application Layer
20 points
Due date: Monday 2/27 at 11:59PM via Blackboard

1. [4 points] In this problem we will use two practical tools (**`whois`** database and **`nslookup`**) to learn some facts about the network of UAlbany.
    a. What is a **`whois`** database? Do some reading on the Internet to answer this question.
    b. Use the **`whois`** utility installed on **`itsunix`** to lookup UAlbany's domain **`albany.edu`**. What is the name of the registrar who manages our domain? How many authoritative DNS servers do we have? List their names. When was our domain registered? When is it going to expire?
    Note: you need to run **`whois albany.edu`** from command line after remote-login to **`itsunix`**.
    c. What does the **`nslookup`** Unix utility do? Do some reading on the Internet to answer this question. Note that there are many **`nslookup`** utilities (that generally provide the same functionality). Look for the Unix utility.
    d. Use **`nslookup`** from **`itsunix`** to find a web server that has multiple IP addresses. List the name of that server and a few of the addresses it maps to.
    Note: You will need to use the full path to the binary to run **`nslookup`** queries. The full path is **`/usr/sbin/nslookup`**
    e. Does the UAlbany web server have multiple IP addresses? What is(are) the IP address(es) of UAlbany's web server(s)?
    f. What is the IP address of **`itsunix`**?

2. [4 points] In this problem we are going to use an ordinary Web surfing activity captured by Wireshark to examine the operation of DNS. You will first need to install Wireshark on your computer and familiarize yourselves with it. Use the lecture slides from class and supplement materials from the textbook available here http://www.cs.albany.edu/~mariya/courses/csi516S17/papers/Wireshark_Intro.pdf.
    Now that you are familiar with Wireshark you can use it to examine the operation of DNS. Open Wireshark and load the provided packet capture file dns-wireshark-trace-1 (available on Blackboard and on this URL http://www.cs.albany.edu/~mariya/courses/csi516S17/hw/dns-wireshark-trace-1). Enter "ip.addr==128.238.38.160" into the filter field. This is the IP address on which the trace was captured. This filter will hide all the packets that neither originate nor are destined to the capturing host. The packet capture was generated by opening a web browser and then visiting the webpage http://www.ietf.org. Once the page was loaded, the packet capture was stopped.
    Answer the following questions.
    a. Locate the DNS query and the response message. Are they sent over UDP or TCP?
    b. What is the destination port of the DNS query message? What is the source port of the DNS response message?
    c. To what IP address is the DNS query message sent? Can you guess what kind of DNS server is this?
    d. Examine the DNS query message. What Type of DNS query is it?
    e. Examine the DNS response. How many answers does it contain? What are the

answers Type and address fields?

3. [2 points] For each below note whether it is an application, a protocol or both.

Web –
HTTP –
E-mail –
DNS –
BitTorrent –
IMAP –
SMTP –

4. [4 points] Consider distributing a file of size F=18Gbits to N clients. The file server has an upload speed of u_S=60Mbps and each peer has a download speed of d_i=9Mbps and an upload speed of u. For N=10, 100 and 1,000 and u=100kbps, 500kbps and 1Mbps prepare a chart giving the minimum distribution time for each of the combinations of N and u for both client-server and peer-to-peer architecture. Provide a brief discussion of your results.

5. [3 points] Consider the general operation of DNS. How can DNS be used for censorship? Comment on mechanisms to combat censorship Inspired by the work of ***[Duan+12]*** "*Hold On: Protecting against on-path DNS poisoning*".

6. [3 points] Consider the analysis of servents and resource distribution in Gnutella presented in ***[Damiani+02]***. What implications do these results have on P2P network design?