**Project 1 – DNS and Basic Tools**

**Project Overview**

* This project is a group project.
* Each group can have three to four students.
* In this project, you will need to learn DNS by yourself.
* In this project, you will need to use two software: Wireshark and OBS (see details below).
* Each group shall submit a project report in ecourse. Only one submission is required.
* Each group shall prepare an in-class demonstration.

**Required Steps**

1. Learn DNS and find answers for the following questions:
   1. What is the full term of DNS?
   2. Which organization or organizations specify the standards for DNS?
   3. What are the main standards for DNS?
   4. What is the computing model for DNS service?
   5. What is the basic procedure of DNS?
   6. What is the scale of the network for DNS servers?
   7. What is the structure of the network for DNS servers?
   8. In a DNS response, it is possible to have multiple answers. What are the reasons for multiple answers?
2. Analyze the layers for the basic DNS service based on the **five-layer model** introduced in class, and find answers for the following questions:
   1. What are the protocols in each layer?
   2. What are the IDs in each layer?
3. Wireshark exercise
   1. Download the latest version from site: https://www.wireshark.org/
   2. Install Wireshark in your PC
   3. Start capturing packets using Wireshark
   4. In a browser, visit a website (any website you want)
   5. Stop capturing packets
   6. Use filter to quickly find two DNS packets:
      1. Query for the website from your PC
      2. Answer from a DNS server
4. OBS exercise
   1. Download the latest version from site: https://obsproject.com/
   2. Install OBS in your PC
   3. Use OBS to record screen and your explanation for all steps in the Wireshark exercise
   4. Upload a video to YouTube using your upr account
      1. Set its access to private
      2. Share it to me: kejie.lu@upr.edu
5. Write a report (See the instruction below)
6. Prepare for an in-class demonstration (PC, necessary software, report, etc.)

**Content in the report**

* Cover page with the following information
  + Logo of UPRM
  + Title
  + Course
  + Names of team members with Student IDs
  + Name of Professor
  + Department
* Table of content
* Section 1: Introduction
  + Overview of the project
  + Contributions of each team member in a table
  + Outline of the rest of this report
* Section 2: Basics of DNS
  + Answers for all questions in Step 1
  + Use figures to illustrate
* Section 3: Layered Model Analysis for DNS
  + Based on the website you visited in the Wireshark exercise, answer questions in Step 2.
  + Used a table to summarize the protocol, ID, etc. for each layer
  + Used screenshots to:
    1. Show the website URL in the DNS packet
    2. Show the IP address you find from the DNS answer
* Section 4: More exercises about DNS and Wireshark
  + Visit the following websites in your browser and use Wireshark to capture the DNS answers
    1. www.uprm.edu
    2. www.upr.edu
    3. www.google.com
    4. www.amazon.com
    5. www.facebook.com
    6. www.netflix.com
    7. www.ets.org
  + **Every team member must visit at least two websites and capture packets**
  + For each website, find the first IP address in the DNS answer, then
    1. Find the physical location (e.g., 136.145.x.x is located in Puerto Rico) of the IP address
       1. There are many IP location tools
    2. Find the owner (e.g., 136.145.x.x is owned by UPR) of the IP address
  + Use a table to summarize the website, IP address, location of IP address, owner of the IP address, team member who visit this website, etc.
* Section 5: Conclusions
* References
  + Need **at least 10 references** for software used, standards, research papers, etc.