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:
    a. What is the full term of DNS?
        i. Domain Name System
    b. Which organization or organizations specify the standards for DNS?
        i. Internet Engineering Task Force (IETF)
    c. What are the main standards for DNS
        i. Standards
        ii. The Domain Name System is defined by Request for Comments (RFC) documents published by the Internet Engineering Task Force (Internet standards). The following is a list of RFCs that define the DNS protocol.
        iii.
        iv. RFC 1034, Domain Names - Concepts and Facilities
        v. RFC 1035, Domain Names - Implementation and Specification
        vi. RFC 1123, Requirements for Internet Hosts—Application and Support
        vii. RFC 1995, Incremental Zone Transfer in DNS
        viii. RFC 1996, A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)
        ix. RFC 2136, Dynamic Updates in the domain name system (DNS UPDATE)
        x. RFC 2181, Clarifications to the DNS Specification
        xi. RFC 2308, Negative Caching of DNS Queries (DNS NCACHE)
        xii. RFC 2672, Non-Terminal DNS Name Redirection
        xiii. RFC 2845, Secret Key Transaction Authentication for DNS (TSIG)
        xiv. RFC 3225, Indicating Resolver Support of DNSSEC
        xv. RFC 3226, DNSSEC and IPv6 A6 aware server/resolver message size requirements
        xvi. RFC 3596, DNS Extensions to Support IP Version 6
        xvii. RFC 3597, Handling of Unknown DNS Resource Record (RR) Types
        xviii. RFC 4343, Domain Name System (DNS) Case Insensitivity Clarification
        xix. RFC 4592, The Role of Wildcards in the Domain Name System
        xx. RFC 4635, HMAC SHA TSIG Algorithm Identifiers
        xxi. RFC 5001, DNS Name Server Identifier (NSID) Option
        xxii. RFC 5011, Automated Updates of DNS Security (DNSSEC) Trust Anchors

xxiii. RFC 5452, Measures for Making DNS More Resilient against Forged Answers
xxiv. RFC 5890, Internationalized Domain Names for Applications (IDNA):Definitions and Document Framework
xxv. RFC 5891, Internationalized Domain Names in Applications (IDNA): Protocol
xxvi. RFC 5892, The Unicode Code Points and Internationalized Domain Names for Applications (IDNA)
xxvii. RFC 5893, Right-to-Left Scripts for Internationalized Domain Names for Applications (IDNA)
xxviii. RFC 6891, Extension Mechanisms for DNS (EDNS0)
xxix. RFC 7766, DNS Transport over TCP - Implementation Requirements
xxx. Proposed security standards
xxxi. RFC 4033, DNS Security Introduction and Requirements
xxxii. RFC 4034, Resource Records for the DNS Security Extensions
xxxiii. RFC 4035, Protocol Modifications for the DNS Security Extensions
xxxiv. RFC 4509, Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records
xxxv. RFC 4470, Minimally Covering NSEC Records and DNSSEC On-line Signing
xxxvi. RFC 5155, DNS Security (DNSSEC) Hashed Authenticated Denial of Existence
xxxvii. RFC 5702, Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC
xxxviii. RFC 5910, Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)
xxxix. RFC 5933, Use of GOST Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSEC
xl. RFC 7830, The EDNS(0) Padding Option
xli. RFC 7858, Specification for DNS over Transport Layer Security (TLS)
xlii. RFC 8310, Usage Profiles for DNS over TLS and DNS over DTLS
xliii. RFC 8484, DNS Queries over HTTPS (DoH)

d. What is the computing model for DNS service?
    i. a hierarchical and decentralized naming system for computers,
e. What is the basic procedure of DNS?
    i. Iterative query procedure
f. What is the scale of the network for DNS servers?
    i. WAN ??? idk lol
g. What is the structure of the network for DNS servers?
    i. Consists of a tree data structure
h. In a DNS response, it is possible to have multiple answers. What are the reasons for multiple answers? Yes, one typical example is if you have multiple webservers, each with a different IP address, that should serve traffic for a given domain

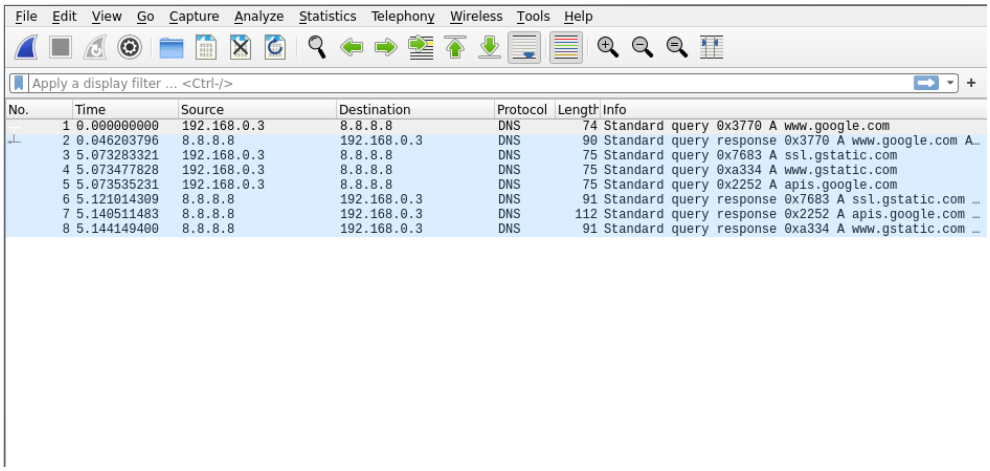
2) Analyze the layers for the basic DNS service based on the **five-layer model** introduced in class, and find answers for the following questions:
    a. What are the protocols in each layer?

Layer Number	Layer Name	Protocol
5	Application Layer	HTTP ,SMTP, etc.
4	Transport Layer	TCP, UDP
3	Network Layer	IP
2	Data Link Layer	Ethernet, Wifi
1	Physical Layer	10 Base T, 802.11

    b. What are the IDs in each layer?

Layer ID	Layer Name
5	Application Layer
4	Transport Layer
3	Network Layer
2	Data Link Layer
1	Physical Layer

3) Wireshark exercise
    a. Download the latest version from site: https://www.wireshark.org/
    b. Install Wireshark in your PC
    c. Start capturing packets using Wireshark
    d. In a browser, visit a website (any website you want)
    e. Stop capturing packets
    f. Use filter to quickly find two DNS packets:
        i. Query for the website from your PC
        ii. Answer from a DNS server



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.0.3	8.8.8.8	DNS	74	Standard query 0x3770 A www.google.com
2	0.046203796	8.8.8.8	192.168.0.3	DNS	90	Standard query response 0x3770 A www.google.com A…
3	5.073283321	192.168.0.3	8.8.8.8	DNS	75	Standard query 0x7683 A ssl.gstatic.com
4	5.073477828	192.168.0.3	8.8.8.8	DNS	75	Standard query 0xa334 A www.gstatic.com
5	5.073535231	192.168.0.3	8.8.8.8	DNS	75	Standard query 0x2252 A apis.google.com
6	5.121014309	8.8.8.8	192.168.0.3	DNS	91	Standard query response 0x7683 A ssl.gstatic.com …
7	5.140511483	8.8.8.8	192.168.0.3	DNS	112	Standard query response 0x2252 A apis.google.com …
8	5.144149400	8.8.8.8	192.168.0.3	DNS	91	Standard query response 0xa334 A www.gstatic.com …

4) OBS exercise
    a. Download the latest version from site: https://obsproject.com/
    b. Install OBS in your PC
    c. Use OBS to record screen and your explanation for all steps in the Wireshark exercise
    d. Upload a video to YouTube using your upr account
        i. Set its access to private
        ii. 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.