UNIVERSITY OF PUERTO RICO
MAYAGÜEZ CAMPUS

COMPUTER SCIENCE AND ENGINEERING
DEPARTMENT

Computer Networks

CIIC – 4070

Project 1: DNS and Basic Tools

Raúl A. Ortiz Rivera ID: 802-18-7733

Professor: Kejie Lu

February 4, 2023

Table of Contents

List of Tables

List of figures

Section 1: Introduction

DNS is a tool that networking uses daily, but many people do not know how often it is used. The Domain Name System is accessed every time we perform a search on the internet and that is why this project will evaluate, analyze and study the fundamentals of this system. The terms, the organizations that handle the DNS, the standards, computer models, scale and others will be studied. It will start using the Wireshark tool to extract the packages from a website and be able to analyze it. The 5 layers will be analyzed and will show what are the protocols and entities of the place accessed. The project will contain the DNS procedures and Query answers. Also, will be explored different pages where you will know your public Ip, the owner of the server and the location of the server.

Section 2: Questions and DNS figure

1. The full term for DNS stands for Domain Name System.
2. The organization responsible for managing DNS standards is ICANN (Internet Corporation for Assigned Names and Numbers) in conjunction with the IETF (Internet Engineering Task Force).
3. The standards considered essential for the DNS are:

   RFC 1034: Concepts

   RFC 1035: Domain Names Implementation

   RFC 1122: Communication Layers

   RFC 1123: Application and Support

   RFC 1876: Location Information

   RFC 1995: Incremental Zone Transfer in DNS

   RFC 1996: Prompt Notification

RFC 2136: Dynamic Updates

RFC 2181: Clarifications to the DNS

RFC 2308: Negative Caching of DNS Queries

RFC 2535: Security Extensions

RFC 2782: DNS RR

RFC 2845: Secret Key Transaction Authentication for DNS

RFC 2915: Authority Pointer

RFC 2930: Secret Key Establishment

RFC 2931: DNS Request and Transaction Signatures

RFC 3110: RSA/SHA-1 SIGs and RSA KEYs

RFC 3445: Limiting the Scope of the KEY

RFC 3596: DNS Extensions to Support IP Version 6

RFC 3645: Generic Security Service Algorithm for Secret Key Transaction

4. The computing model of DNS is client-server. This model saves the names and IPs as in a phonebook to quickly access the webpages.
5. The basic process of a DNS is as follows:
    a. The user starts by searching for a page such as www.google.com and the query is sent to DNS resolver.
    b. Then the local DNS sends a query to the root name servers.
    c. The root server sends the address to the DNS resolver of the TLD (Top Level Domain) either .com .net .org.
    d. The TLD responds with the IP of the desired page.

    e. The IP is returned to DNS resolver and the browser can make a request for the page with the HTTP protocol.
    f. The server returns the rendered page.
6. The scale of DNS is trillions of public and private domains. There are 3 main types to resolve domain names. First those operated by major organizers such as ICANN. Then the TLD servers and finally the companies, government and agencies. The scalability is global.
7. The DNS structure is made up of the Root DNS server. Then following the pattern of a tree, they continue with each server (.com, .net, .edu, .org). At the end of the tree is the DNS server (amazon.com, netflix.com).
8. The short answer is yes. Some reasons are as follows:
    a. Some pages have several servers to handle traffic so you can receive several responses from different IP addresses.
    b. Location can be key to receiving different DNS responses.
    c. Use Round-Robin which makes it toggle Ip addresses to handle efficiency.
    d. Security to ensure that if a DNS request fails the page loads successfully.

DNS procedure and the network of DNS servers

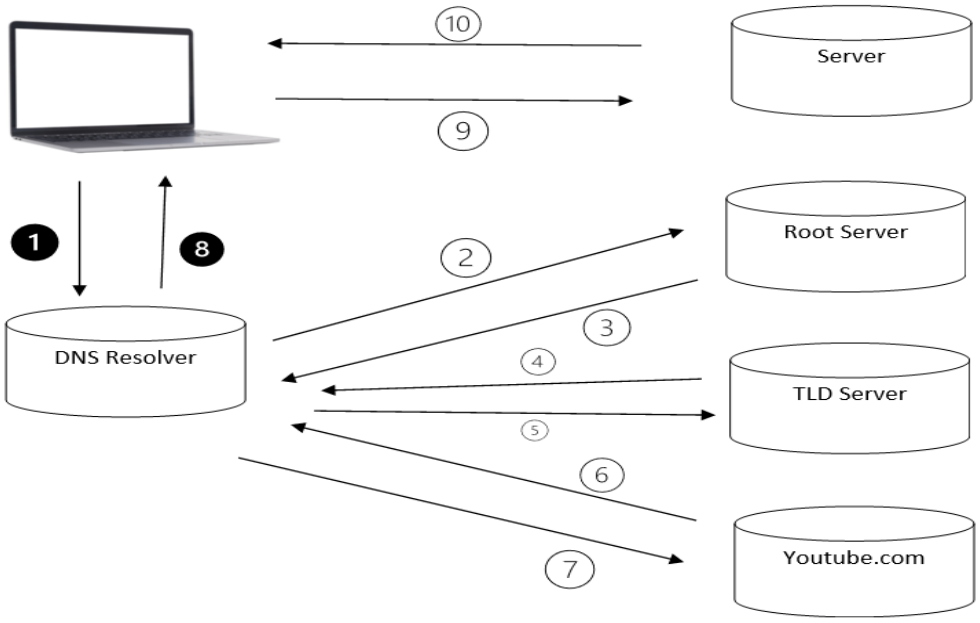

Fig1. DNS procedure

Section 3: Layered Model Analysis for DNS

Webpage for test: YouTube (www.youtube.com) Transaction ID: **0xceb2**

Based on the website I took YouTube (www.youtube.com) as an example, I determined which are the layers in each of the 5 models. Starting with the physical model and analyzing the web it can be said that the physical layer would be the connection between the computer and the internet. Let's use as an example a Wi-Fi network called "Free Wi-Fi" in a coffee shop. The user connects via Wi-Fi using the IEEE 802.11 protocol although another option would have been to connect via Ethernet cable. In the case of Wi-Fi, we were connected by waves that process the bits to be filtered by the higher layer protocols. Based on the above, the next layer is the Data Link. This layer is responsible for sending the source, handling the Media Access Control (MAC) address to process the data that is sent avoiding collisions using error detectors and flow

control. In the case of YouTube, the protocol it usually uses is Unrestricted Simplex Protocol since it sends the data in an address for the transmission of video content. The Simplex Stop-and-Wait Protocol and Simplex Protocol for a Noisy Channel are uncommon on YouTube as they are used to receive two communication channels, something more like a messaging app. If we focus on the next layer which is the MAC layer, the search for data collisions intensifies. In the example of using the Wi-Fi connection, the media access control uses a protocol called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). These protocols help in the case of YouTube that many users can stream videos at the same time. In the Network layer YouTube uses the IP protocol to direct and deliver the data to the server. It basically processes data packets over the internet. This prevents videos from loading efficiently and in case of a packet is damaged the Network layer asks for a replacement packet. Finally, the Transport Layer is used to transport the data from the server to the user's device. In the case of YouTube uses the Transmission Control Protocol or commonly known as TCP which is responsible for receiving and verifying the connection and dividing the videos into small fragments to process the information.

Layer	Protocol	Entity ID
Physical Layer	Wi-Fi (IEEE 802.11) or Ethernet I	Ip: 142.250.217.174
Data Link Layer	Unrestricted Simplex Protocol, Ethernet II	Src: ARRISGro_11:22:33 Dst: CloudNet_88:a8:45
Medium Access Control Layer	Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)	MAC address: 10:6f:d9:88:a8:45
Network Layer	IP Protocol (Ipv6)	Ip: 142.250.217.174
Transport Layer	Transmission Control Protocol (TCP)	Src port: 53 Dst port: 56471

Table 1. Protocols and Entity ID of Different Layers

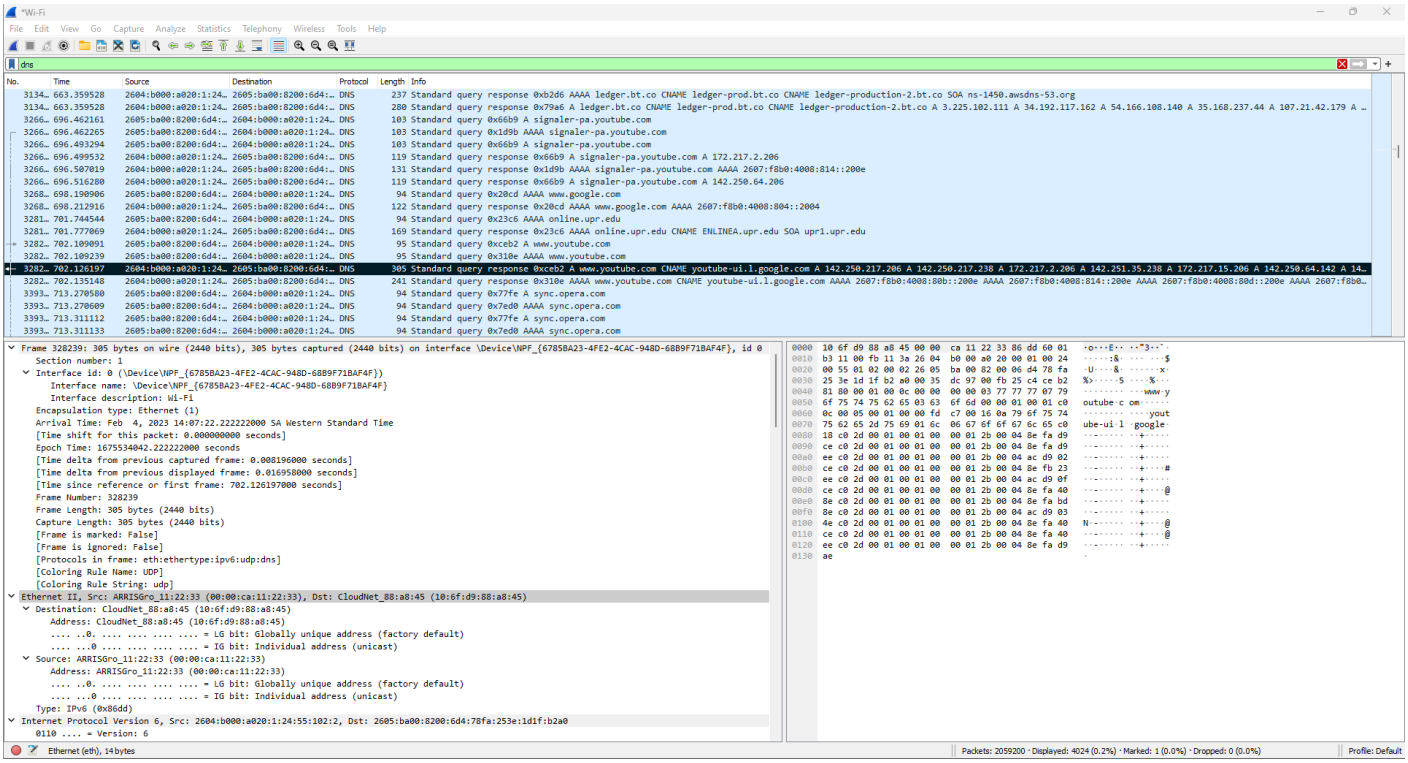

Fig 2.1. Image with URL in DNS Packet.

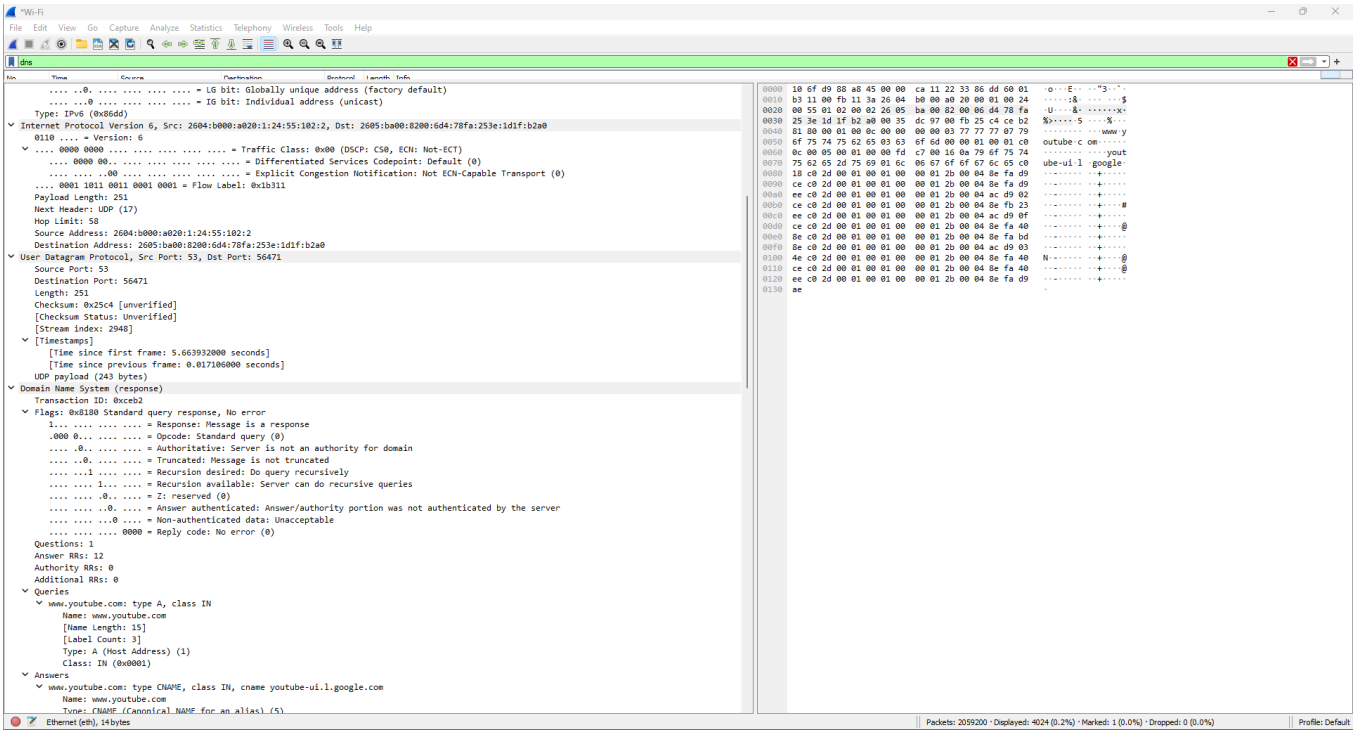

Fig 2.2. IP protocol, Queries

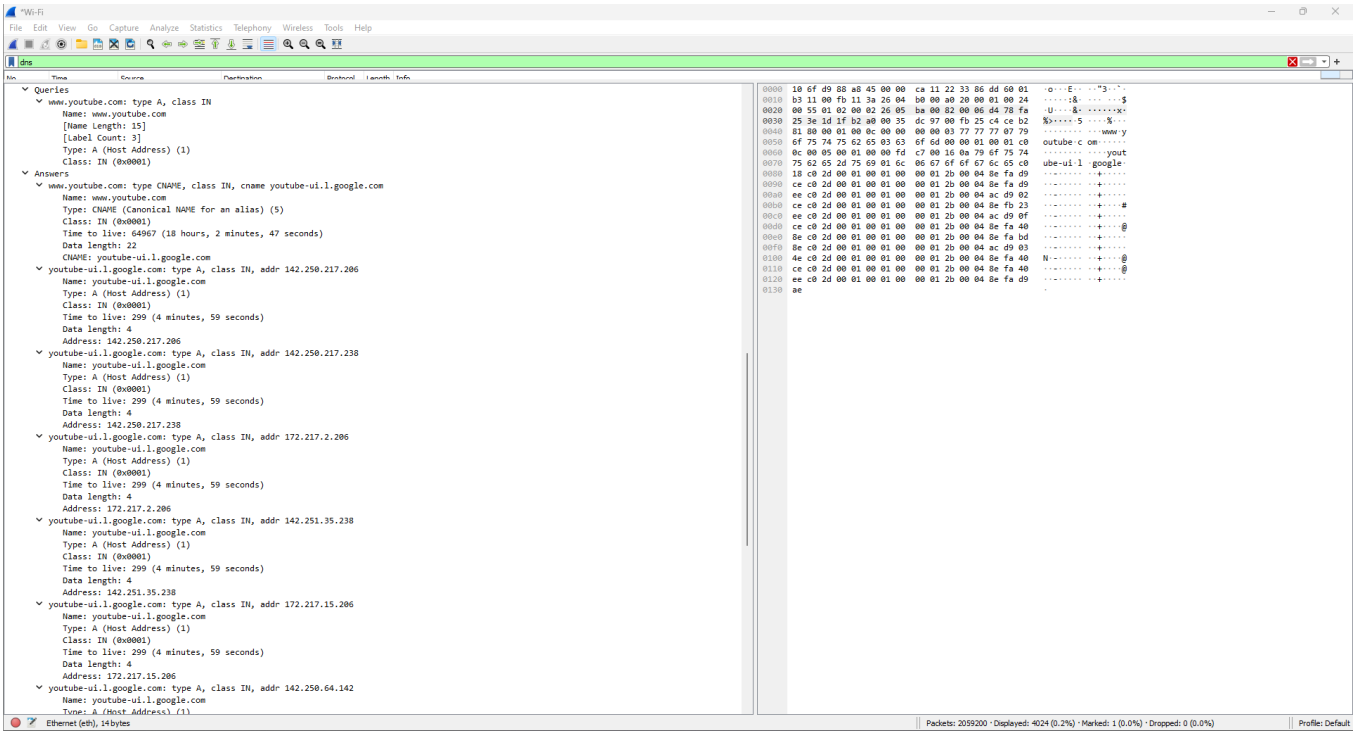

Fig 2.3. Image with queries answer and URL's

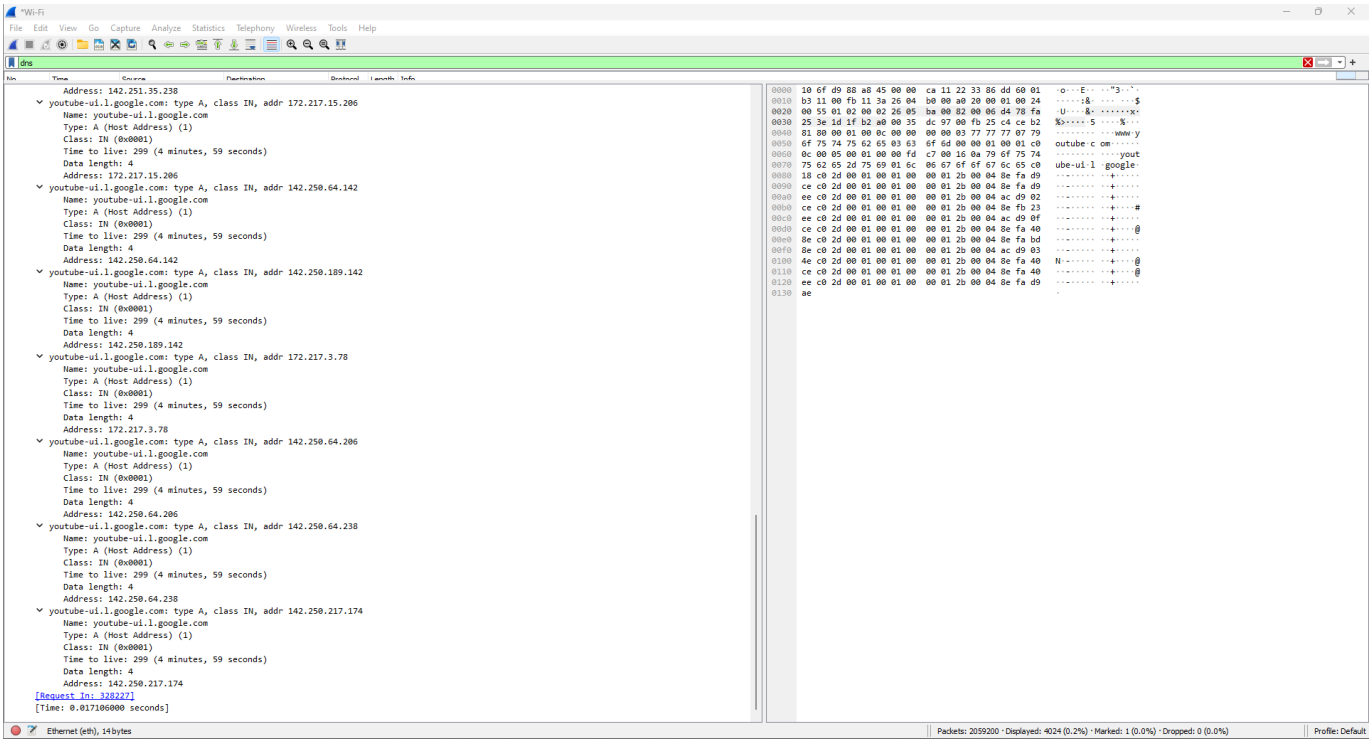

Fig 2.4. Last answer with the IP used

Section 4: Wireshark Exercise

Website	IP Address	Location of IP	Owner of IP
www.uprm.edu	136.145.30.45	Puerto Rico	University of Puerto Rico
www.upr.edu	136.145.11.14	Puerto Rico	University of Puerto Rico
www.google.com	142.250.64.132	USA	Google Inc.
www.amazon.com	52.46.154.73	USA	Amazon.com Inc.
www.facebook.com	157.240.213.35	USA	Facebook Inc.
www.netflix.com	3.230.129.93	USA	Amazon.com
www.etsi.org	146.75.125.224	USA	Fastly Inc.

Table 2. Website, IP address, Location and Owner of IP Wireshark exercise

Conclusion

The main objective of this project was to familiarize oneself with the DNS. In addition to developing the skills studied in class applying the 5 layers of networking. It began by acquiring basic and theoretical knowledge. Then the analysis of the layers was applied using a web page. Their security protocols and IDs were obtained. After this, several example pages were explored and OBS was used to demonstrate knowledge of the Wireshark tool. In the end, a base was obtained in terms of DNS, protocols, IP, and how the packets travel between servers to give us an efficient and secure load when browsing.

References

C. to W. projects, “Communication Networks/DNS,” *Wikibooks, open books for an open world*, 25-Oct-2021. [Online]. Available: https://en.wikibooks.org/wiki/Communication_Networks/DNS#:~:text=It%20is%20a%20tree-like,have%20any%20number%20of%20branches. [Accessed: 04-Feb-2023].

“DNSSEC – what is it and why is it important?,” *ICANN*. [Online]. Available: https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en#:~:text=The%20DNS%20Security%20Extensions%20(%20DNSSEC,in%20DNS%20was%20a%20problem. [Accessed: 04-Feb-2023].

“Download,” *Wireshark · Go Deep*. [Online]. Available: https://www.wireshark.org/. [Accessed: 04-Feb-2023].

“The F5 intelligent DNS scale reference architecture,” *弘协网络*. [Online]. Available: https://www.f5.com.cn/services/resources/white-papers/the-f5-intelligent-dns-scale-reference-architecture#:~:text=Generally%2C%20organizations%20have%20a%20set,around%20200%2C000%20queries%20per%20second. [Accessed: 04-Feb-2023].

“How to clear your browser cache, cookies, and history,” *Grand Valley State University - Knowledge Base*, 15-Aug-2022. [Online]. Available: https://services.gvsu.edu/TDClient/60/Portal/KB/ArticleDet?ID=520#Desktop-Opera. [Accessed: 04-Feb-2023].

“MAC address and OUI LOOKUPFOR 10:6f:D9:88:a8:45if(typeof ez_ad_units != 'undefined'){ez_ad_units.push([[300,250],'aruljohn_com-box-3','ezslot_5',106,'0','0'])};__ez_fad_position('div-GPT-ad-aruljohn_com-box-3-0');” *Aruls*. [Online]. Available: https://aruljohn.com/mac/106FD988A845. [Accessed: 04-Feb-2023].

“OBS Studio,” *OBS*. [Online]. Available: https://obsproject.com/. [Accessed: 04-Feb-2023].

P. Hoffman, A. Sullivan, and K. Fujiwara, “DNS terminology,” *RFC Editor*, 01-Jan-1970. [Online]. Available: https://www.rfc-editor.org/rfc/rfc8499.html. [Accessed: 04-Feb-2023].

R. Ortiz Rivera, “Project 1 - CIIC4070 090 Raul Ortiz Rivera DNS Server,” *YouTube*, 04-Feb-2023. [Online]. Available: https://youtu.be/DlI3JEHajRU. [Accessed: 04-Feb-2023].

Stevewhims, “DNS standards documents - win32 apps,” *Win32 apps | Microsoft Learn*. [Online]. Available: https://learn.microsoft.com/en-us/windows/win32/dns/dns-standards-documents. [Accessed: 04-Feb-2023].

“University of Puerto Rico Login - online.upr.edu.” [Online]. Available: https://online.upr.edu/course/view.php?id=275245. [Accessed: 05-Feb-2023].

“What is DNS? | how DNS works | cloudflare.” [Online]. Available: https://www.cloudflare.com/learning/dns/what-is-dns/. [Accessed: 05-Feb-2023].

"What is DNS? – introduction to DNS - AWS." [Online]. Available: https://aws.amazon.com/route53/what-is-dns/. [Accessed: 05-Feb-2023].

"What is my IP location? (geolocation)," *IP Address Lookup | Geolocation*. [Online]. Available: https://www.iplocation.net/. [Accessed: 04-Feb-2023].

"Your IP address (ipv4)," *Shows Your IPv4 & IPv6, OS, Browser, Organisation, Country on Interactive Map. Live Hosting Information on where any website is hosted on the internet and other information about IP address owners. Online Blacklist your IP Check (Real-time DB). Web Bots 2023 List*. [Online]. Available: https://myip.ms/. [Accessed: 04-Feb-2023].