CS 315: Computer Networks Lab
Spring 2024-25, IIT Dharwad
Assignment-4
Wireshark Lab: DNS
January 27, 2025

Lab Instructions

- Login to the Ubuntu OS on your machine. The login credentials are as follows:
    - Username: user
    - Password: 123456
- Mark your attendance in the attendance sheet before leaving the lab.
- Handle the lab resources with utmost care.
- Please go through the following exercises in today's lab and **note to attach screenshots for all the answers**.
- It is recommended that you complete all the following exercises during the lab slot itself.
- If you face any difficulties, please feel free to seek help online or from your peers or TAs.
- After finishing all exercises, please carry your solutions with you (via email/pen drive) for future reference, and delete the files from the desktop.

Introduction

The Domain Name System (DNS) translates hostnames to IP addresses, fulfilling a critical role in the Internet infrastructure. In this lab, we'll take a closer look at the client side of DNS. The client's role in the DNS is relatively simple – a client sends a *query* to its local DNS server and receives a *response*.

In this assignment, you will explore the fundamental concepts of DNS resolution through practical tasks. The focus will be on understanding DNS functionality, query mechanisms, and analyzing network traffic to gain insights into how DNS operates. By performing these tasks, you will become familiar with using DNS tools and analyzing query behavior in different scenarios.

Part-1: Flushing DNS on Different Operating Systems

DNS caching improves resolution speed by storing recently resolved domain names. However, stale or incorrect DNS entries can cause issues, making it necessary to flush the DNS cache. In this section, you will:

1) Learn how DNS caching works and its role in resolving domain names.
2) Understand the steps to flush DNS caches on various operating systems, such as:

a) Windows: Using the `ipconfig /flushdns` command.
b) MacOS: Using `sudo dscacheutil -flushcache` and `sudo killall -HUP mDNSResponder`
c) Linux: Using `resolvectl flush-caches`

Try the above commands according to the OS you are using.

The goal is to clear cached DNS entries and observe how fresh resolutions are obtained when querying a domain.

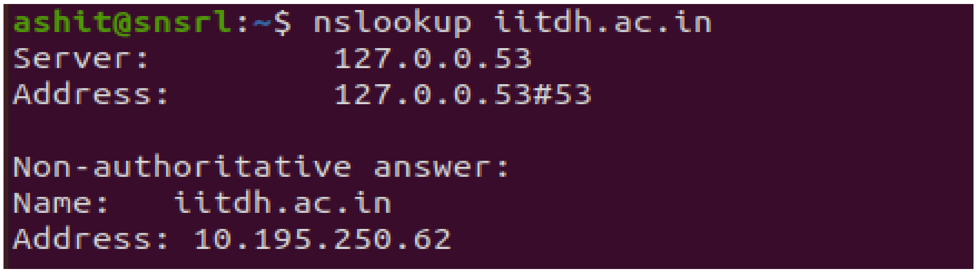
Part-2: Using nslookup for DNS Queries

The nslookup tool is widely used for querying DNS information. This part of the assignment focuses on exploring nslookup features and understanding its output. You will:

1) Use the `-type` option to specify DNS record types such as `A`, `MX`, `CNAME`, etc.
2) Resolve a domain name using nslookup and a specific nameserver. For example, resolving `drive.google.com` directly or using say nameserver `ns1.google.com`
3) Observe different fields that `nslookup` returns after resolving a domain name, and verify whether the IP address resolved for a domain name is the same as observed using other commands like `host`, `whois`, and `dig` (refer to slides).

By completing this section, you will understand how different nameservers respond and how record types influence DNS query results.

Part 2.1: Use `nslookup` command on two domains (`iitdh.ac.in`, and `google.com`) separately (as shown in the below figure), and answer the following questions.



```
ashit@snsrl:~$ nslookup iitdh.ac.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   iitdh.ac.in
Address: 10.195.250.62
```

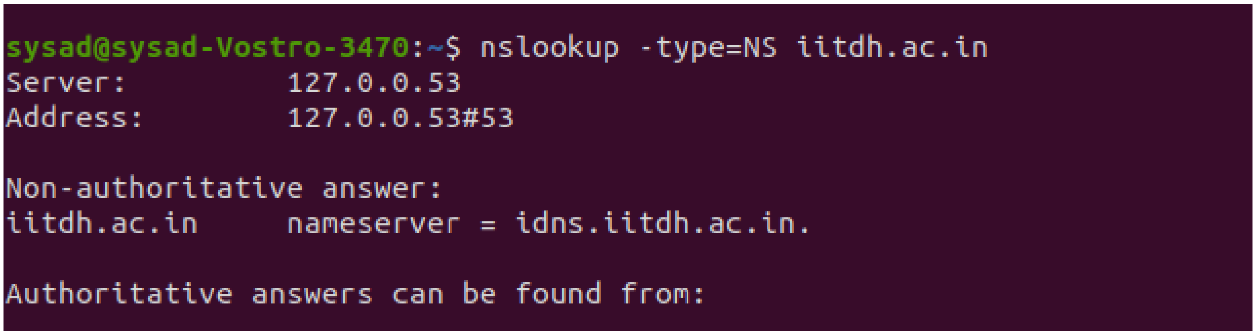
Q.1. **[1 mark]** What is the IP address of the requested domain?

Q.2. **[1 mark]** What is the IP address of the DNS resolver?

Q.3. **[1 mark]** Which port number is used to resolve the domain?

Q.4. **[3 marks]** Verify the IP address obtained using the DNS for the requested domain using the `host`, `whois`, and `dig` commands (refer slides for the commands).

Part 2.2: Use `nslookup` command on two domains (`iitdh.ac.in`, and `google.com`) separately (as shown in the below figure), and answer the following questions.



```
sysad@sysad-Vostro-3470:~$ nslookup -type=NS iitdh.ac.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
iitdh.ac.in     nameserver = idns.iitdh.ac.in.

Authoritative answers can be found from:
```

Q.1. **[4 marks]** List the nameservers you are observing for the above-requested domain names.

Part 2.3: Use `nslookup -type=[RECORD] google.com`

Where, `RECORD` can be `A`, `NS`, and `MX`

Answer the following questions based on the above command:

Q.1. **[3 marks]** Mention the significance of each of the record types.

Q.2. **[3 marks]** List the IP addresses in the "Non-authoritative answer" for all the above record types.

Part 2.4: Use `nslookup` to resolve `drive.google.com` using all the nameservers of `google.com` and answer the following questions.

Q.1. **[4 marks]** What are the IPV4 and IPV6 addresses of `drive.google.com` from all the nameservers of `google.com`?

Q.2. **[4 marks]** List the IP addresses of all `NS` of `google.com`.

Part 2.5: Use the following commands to answer the following questions.

CMD1: `nslookup drive.google.com`

CMD2: `nslookup drive.google.com ns1.google.com`

Q.1. **[1 mark]** What is the difference you observe on the terminal for these two commands?

Q.2. **[1 mark]** Why does CMD2 not show the "Non-authoritative answer" line in its output?

Part-3: Capturing and Analyzing DNS Queries with Wireshark

Analyzing DNS traffic provides a deeper understanding of how queries and responses are structured. In this part, you will:

1) Use nslookup to query a domain and simultaneously capture the DNS traffic using Wireshark.
2) Observe the packet exchange between your system and the DNS resolver, noting:
    a) The query format.
    b) The DNS request and response fields.
    c) Any additional information in the response (e.g., additional or authoritative records).

Answer the following questions

1. Start Wireshark
2. Flush DNS cache in terminal
3. Use nslookup on machinelearningmastery.com domain
4. Stop the Wireshark and use dns in the display filter.

Q.1. **[6 marks]** How many IP addresses are available in the terminal for machinelearningmastery.com? Do you observe the same in DNS response packet in Wireshark?

Q.2. **[2 marks]** What are the different types of DNS records you observe in Wireshark?

Q.3. **[3 marks]** List out the IP addresses of client (your system), DNS resolver, and the domain you have requested.

Q.4. **[3 marks]** What are the source and destination port numbers the DNS request made? What is the significance of the destination port and also which transport layer protocol is used to make the request?

Submission Details

- Write your answers in a single doc/tex file, and submit its PDF named after your IIT Dharwad roll number, which contains all answers.
- Attach the screenshots for all the answers.