Computer Networks, Spring 2026

Instructor: Shashi Prabh

Lab 5: DNS Deep-Dive

In this lab, you will explore the Domain Name System (DNS) using command-line diagnostic tools and packet analysis. *This lab is to be done individually.*

1 Basic DNS Queries

Use `nslookup` and `dig` to perform basic name resolution.

1. Use `nslookup` to find the IP address of `ahduni.edu.in`.
2. Use `dig ahduni.edu.in` and identify the following sections in the output:
   - HEADER (specifically the FLAGS - is the response authoritative?)
   - QUESTION SECTION
   - ANSWER SECTION
   - AUTHORITY SECTION
3. What is the TTL (Time To Live) of the record you just received?

2 DNS Record Types

DNS supports multiple record types for different purposes.

1. Use `dig` to find the Mail Exchange (`MX`) records for `google.com`.
2. Use `dig` to find the Name Server (`NS`) records for `ahduni.edu.in`.
3. Use `dig` to find the IPv6 address (`AAAA` record) for `facebook.com`.

3 The Resolution Process: Tracing DNS

The `+trace` switch in `dig` allows you to see the iterative resolution process.

1. Run `dig ahduni.edu.in +trace`.
2. Identify the Root Servers contacted initially.
3. Identify the TLD (`.in`) servers contacted next.
4. Identify the authoritative servers for `ahduni.edu.in`.
5. How many iterations did it take to reach the final answer?

4 Reverse DNS Lookup

Find the hostname associated with a given IP address.

1. Perform a reverse lookup for `8.8.8.8` using `dig -x 8.8.8.8`. What is the result?

5 Reflection

1. Find out what is DNS spoofing.
2. If you were designing DNS today, what would you do differently?

6 Evaluation

☐ Can interpret the flags in a DNS header. TA: _____

☐ Understands the difference between recursive and iterative resolution. TA: _____

☐ Successfully traced a resolution to the root servers. TA: _____