Enterprise Digital Infrastructure – Assignment #2 – April 2023

Domain Name System

1. **Active experiments**

   Perform the following experiments using different Name Servers and compare the results of the queries as well as the time taken by the queries. Specify the Local Name Servers used in the experiments. Commands for performing DNS queries: **`dig`**, **`host`**, **`nslookup`**, **`whois`**, **`jwhois`**.

   - Query the DNS to obtain the IP addresses of **`achille.unipv.it`** and of another hostname in the TLD domain **`it`**; are the answers authoritative? Why?
   - Query the DNS to obtain the name(s) of the mail servers associated with the domain **`universitadipavia.it`** and **`harvard.edu`**. How many servers provide this service? Is there anything specific associated with these RRs?
   - Query the DNS to obtain the IP address of a Web server located outside Europe; is the answer authoritative? Why? How many RRs did you obtain? What is their type? Does the domain sign any RR type using **`DNSSEC`**?
   - Query the DNS to obtain the IP addresses of the Name Servers of a company located outside Europe; how many queries did you execute? What type(s) of queries? How many Name Servers are associated with the company? Do they belong to the same domain? Can you identify the primary Name Server? Why? Who registered the domain? When will it expire?
   - Query one of the Name Servers identified in the previous experiment to obtain the IP address of the Name Servers of the domains **`unipv.it`** and **`cloudflare.com`**. How many IP addresses did you get? Why?

2. **Performance experiments**

   Test the behavior and performance of different Name Servers using diagnostic tools, such as **`dnsperf`**, **`dnsping`**, **`dnstraceroute`**, **`dnseval`**, **`reseval`**.

   - Measure the performance of a Name Server when processing multiple queries. Did you notice any variability? Any expected/unexpected behavior? Does the performance depend on the transport protocol (i.e., UDP, TCP) or on usage of encrypted transmissions (i.e., DoT, DoH)? Does the performance vary when DNSSEC is enabled?
   - Measure the performance of different Name Servers when processing the same set of queries. Does the performance vary with the Name Server? Does it depend on the type of query or on the geographic location of the Name Server?
   - Check the path followed by your queries using different Name Servers; does the performance depend on the number of hops? Did you notice any expected/unexpected behavior?