

HOW DNS WORK

FROM ZERO TO HORE!

by Pujo Mulyono

INDOSYSADMIN

1. Root

Ini merupakan puncak hirarki yang berisi database valid Top level Domain

2. Top-Level Domain (TLD)

Ini ialah suatu kata yang posisinya itu berada paling kanan dari sebuah domain, atau paling belakang.
<https://id.tld-list.com/tlds-from-a-z>

3. Second-Level Domain

Ini dapat berisikan host serta domain lain, atau juga sering disebut dengan sebutan subdomain

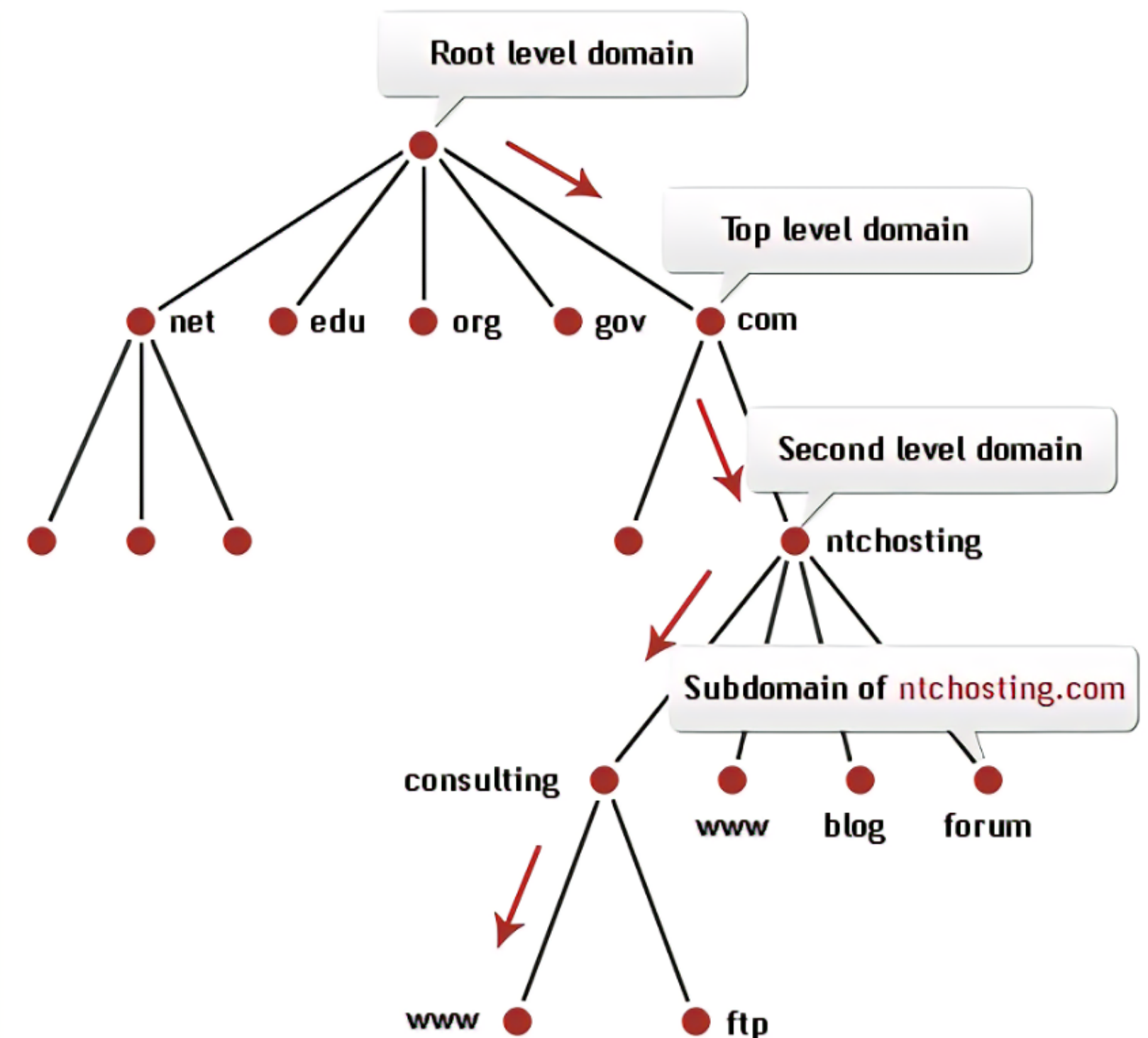
4. Third-Level Domain

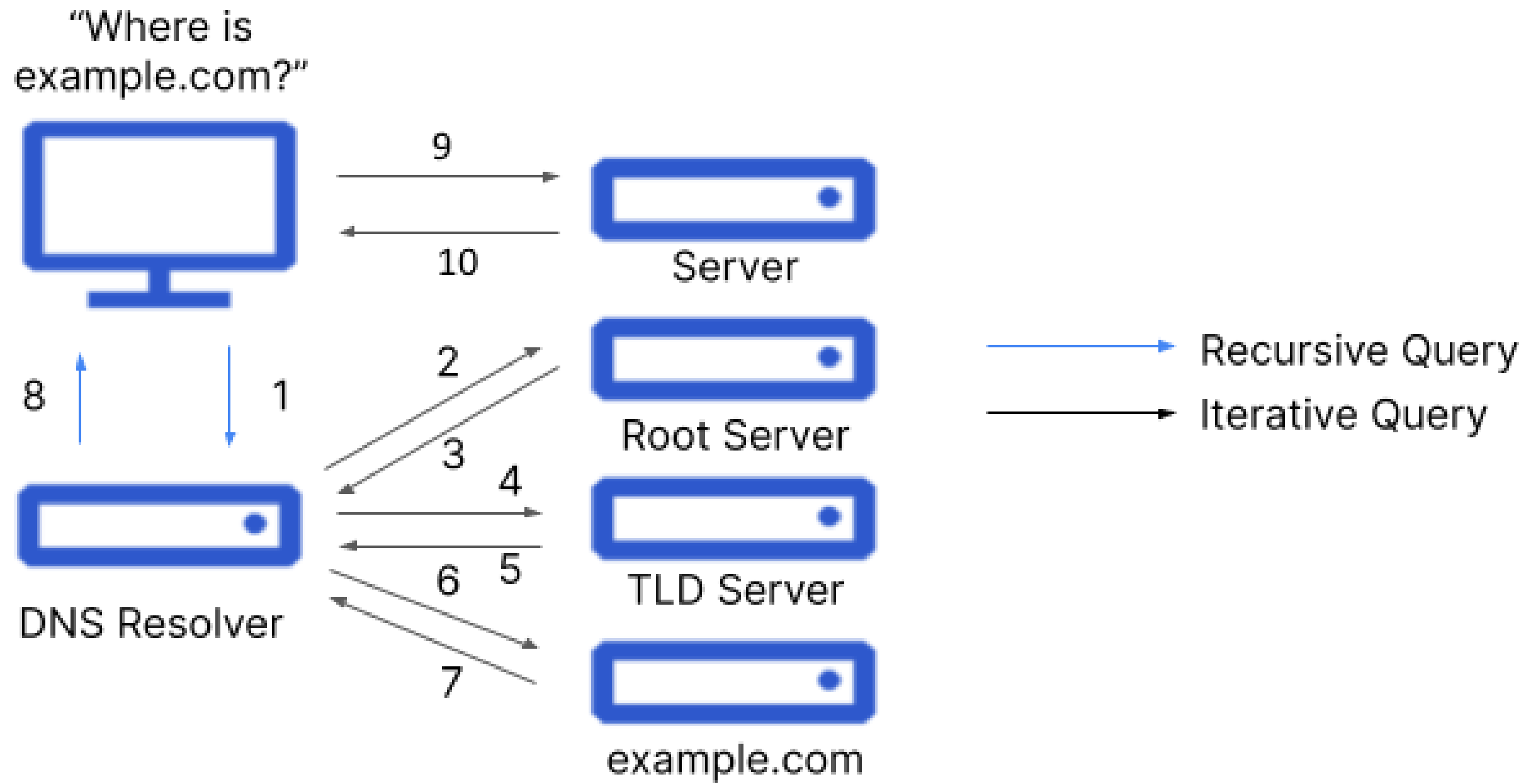
Ini merupakan kata yang letaknya di sebelah kiri second level domain serta dibatasi dengan titik.

5. Host Name

Kata yang terletak di paling depan disebuah domain

HIRARKI DNS





Cloud DNS as a
service

VS

Private DNS
Server

Registrar/Hosting
Cloudflare
AWS Route53
Azure DNS
Google Cloud DNS

BIND
Knot
PowerDNS
NSD
Unbound

- **SOA (Start of Authority)**, SOA mengacu pada Authority Name Server.
- **A (Address) Record**. A berguna sebagai penerjemah dengan mengubah nama domain menjadi IP Address v4.
- **CNAME**. CNAME merupakan jenis DNS yang melakukan redirect domain ke nama lain
- **PTR (Pointer)**. PTR atau Pointer digunakan untuk mengarahkan IP Address menjadi domain.
- **NS (Name Server)**. NS untuk mengarahkan suatu domain atau subdomain ke dns server lainnya
- **TXT (Text)**. TXT merupakan suatu catatan informasi teks untuk domain
- **MX (Mail Exchange)**. MX untuk mengarahkan ke mail server sebuah domain

DNS QUERY

Adalah suatu pertanyaan atas sebuah tipe dns record yang harus dijawab oleh DNS Server. Queries bisa muncul dari aplikasi yang dijalankan user atau dns client

DNS RESPONSE

Adalah suatu jawaban dari DNS Server atas query type yang diminta , diantaranya yang utama adalah

- **NOERROR**, merupakan jawaban dengan data/record atau tanpa data (NODATA)
- **NXDOMAIN**, merupakan jawaban bahwa record tidak ada
- **REFUSED**, merupakan jawaban bahwa permintaan ditolak, karena konfigurasi tidak mengizinkan
- **SERVFAIL**, server tidak menjawab, atau gagal dijawab, biasanya karena 3 sebab; gangguan jaringan, proteksi firewall, atau server memang tidak running

- 1. Standard DNS Service** (not encrypted)
 - **UDP port 53** untuk common query dan notify
 - **TCP port 53** untuk fail-over dan zone transfer
- 2. DNS over TLS / DoT** (encrypted)
 - **TCP port 853** untuk common query
- 3. DNS over HTTPS / DoH** (encrypted)
 - **TCP port 443** untuk common query
- 4. DNS over QUIC / DoQ**
 - **TCP/UDP port 443 ?**

Domain Name System

Domain Name System, atau DNS, berfungsi mentranslasi nama domain yang mudah dibaca manusia menjadi IP address yang bisa dikenali oleh mesin, atau sebaliknya.

Analogi

Analogi yang sesuai , DNS adalah semacam buku alamat, atau address book



Terdapat beberapa software yang bisa digunakan untuk melakukan query type DNS record, diantaranya dua software yang sering dipakai adalah:

- **NSLOOKUP**, umumnya tersedia di OS Windows
- **DIG**, umumnya tersedia di OS Linux, tetapi juga bisa diinstall di OS Windows.

Jika dibandingkan dengan nslookup, dig memiliki kelebihan karena data yang ditampilkan lebih detail, termasuk response time dari DNS Server dalam menjawab sebuah query