DNS

Domain Name System

DNS

Domain Name System

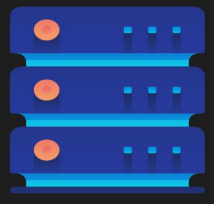
Why DNS

www.husseinnasser.com

- People can’t remember IPs
- A domain is a text points to an IP or a collection of IPs
- Additional layer of abstraction is good
- IP can change while the domain remain
- We can serve the closest IP to a client requesting the same domain
- Load balancing

DNS

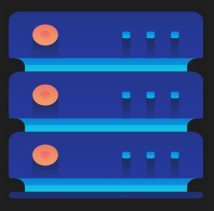
- A new addressing system means we need a mapping. Meet DNS
- If you have an IP and you need the MAC, we use ARP
- If you have the name and you need the IP, we use DNS
- Built on top of UDP
- Port 53
- Many records (MX, TXT, A, CNAME)



Google.com
(142.251.40.46)

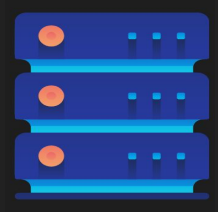
How DNS works

- DNS resolver - frontend and cache
- ROOT Server - Hosts IPs of TLDs
- Top level domain server - Hosts IPs of the ANS
- Authoritative Name server - Hosts the IP of the target server



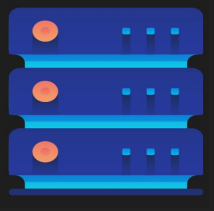
ANS

TLD



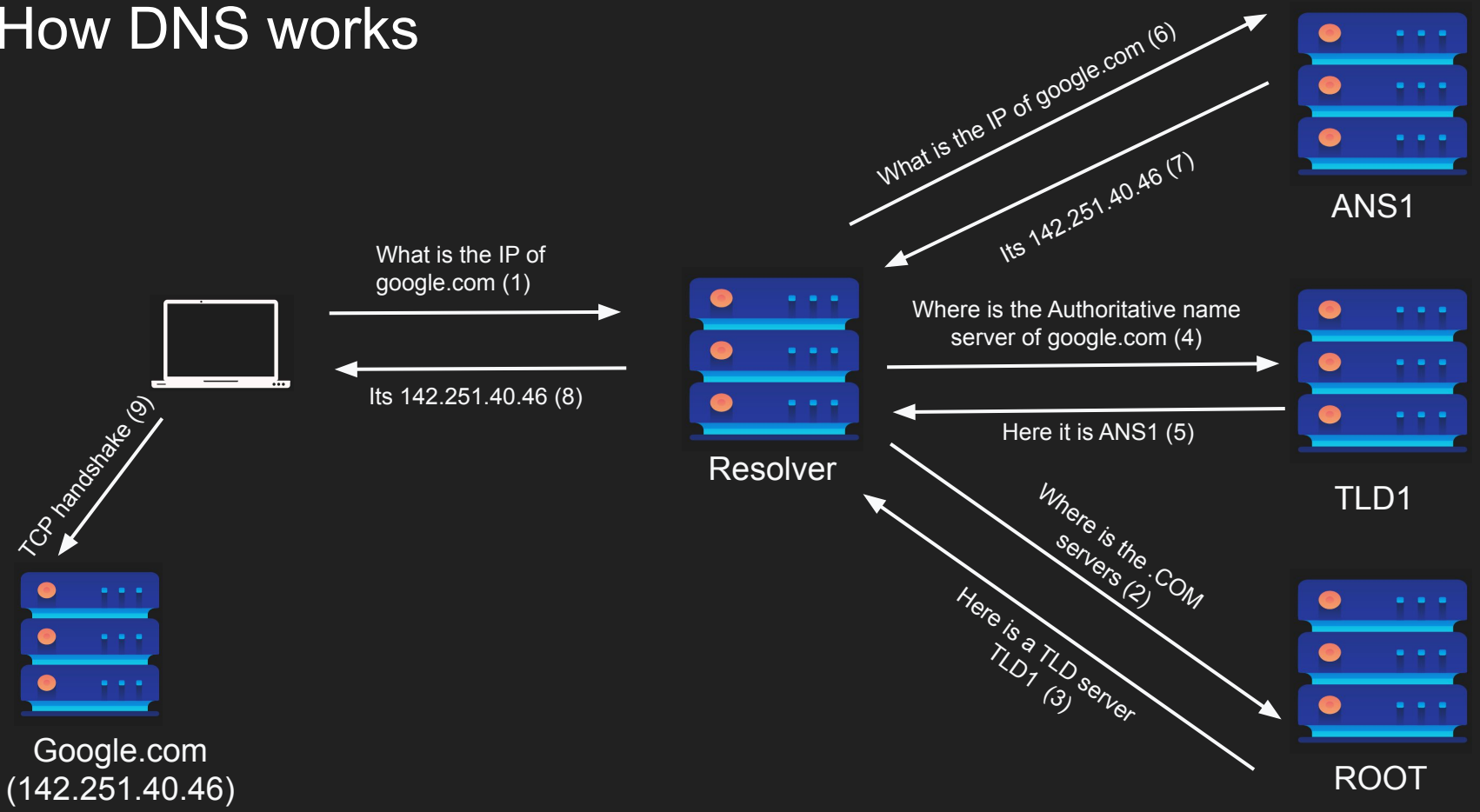
server

Resolver

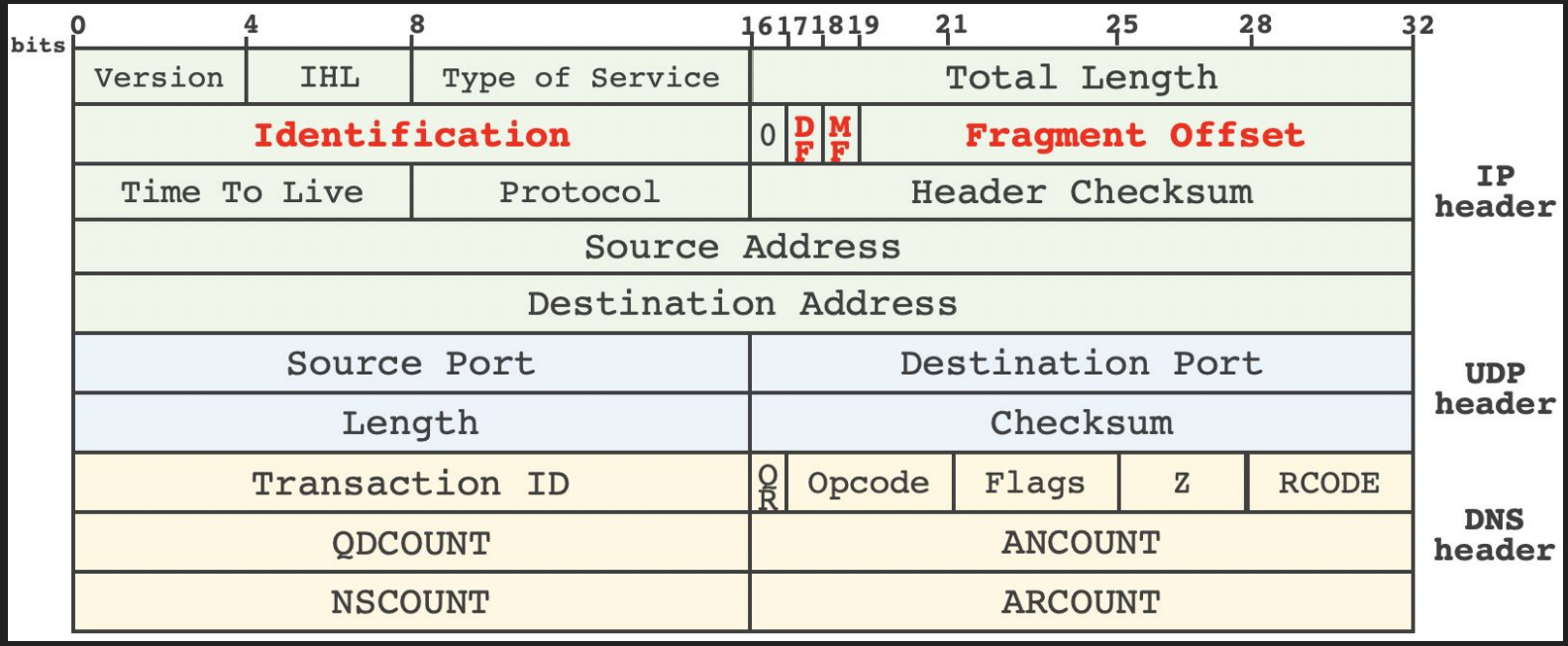


ROOT

How DNS works



DNS Packet



Source: https://www.usenix.org/system/files/sec20-zheng.pdf
RFC: https://datatracker.ietf.org/doc/html/rfc1035

Notes about DNS

- Why so many layers?
- DNS is not encrypted by default.
- Many attacks against DNS (DNS hijacking/DNS poisoning)
- DoT / DoH attempts to address this

Example

- Let us use nslookup to look up some DNS