🔍 In-Depth DNS Flow: "www.google.com" Request

Step-by-Step Breakdown

1. **User enters www.google.com in a browser**
    - The browser checks its internal DNS cache.
    - If not found, it proceeds to the next level.
2. **Operating System DNS Cache**
    - The OS (like Windows or Linux) maintains its own cache.
    - If a cached entry is found and still valid (TTL not expired), it's used.
    - If not, the OS sends a DNS query to the configured **DNS Resolver** (typically from ISP or a public DNS like 8.8.8.8).
3. **DNS Resolver (Recursive Resolver)**
    - Receives the query: "What is the IP of www.google.com?"
    - Checks its own cache.
    - If not found, begins the recursive resolution process by querying the DNS hierarchy:

🧭 Recursive Resolution Journey

4. **Query to Root DNS Server**
    - Resolver contacts a **Root Server** (there are 13 sets globally: A to M).
    - Root server doesn't know the IP but replies with the address of the responsible **TLD (Top-Level Domain) server**, e.g., .com.
5. **Query to TLD Server**
    - Resolver asks the .com TLD server: "What's the authoritative DNS for example.com?"
    - TLD replies with the IP of the **Authoritative Name Server** for example.com.
6. **Query to Authoritative Name Server**
    - Resolver asks: "What is the IP address of www.google.com?"
    - Authoritative server responds with the actual IP address (e.g., 93.184.216.34).
    - This may include A (IPv4) or AAAA (IPv6) records, along with TTL.

💾 Back to the Client

7. **Recursive Resolver stores the response**
    - Caches the IP and TTL.
    - Sends the IP back to the user's OS.
8. **OS stores it in cache and gives it to the browser**
9. **Browser initiates TCP/HTTPS connection**
    - Now the browser connects to 93.184.216.34 over port 443 (HTTPS) or port 80 (HTTP), and fetches the web page.