What happens when you type google.com in your browser and press enter ?

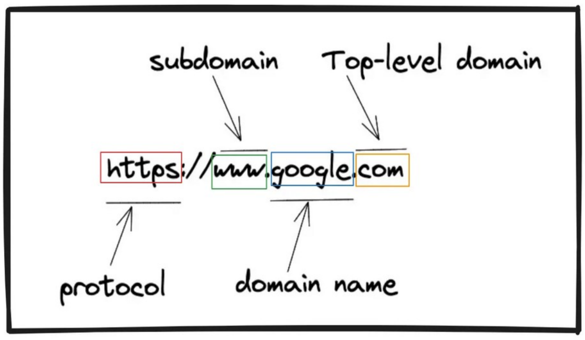
Before we start, it is important to know what a client-server model is. In-order for us to communicate with “Google”, we need our computer with a browser from our side, and Google server to respond to our request. we also need some kind of responder from the google and we call it server. **Server** is nothing more than a computer. So, in this case, our computer is a client, and the google ‘computer’ is a server.

Overview:-

1. DNS resolution
2. TCP 3-way handshake
3. HTTP request-response
4. Browser rendering the server response

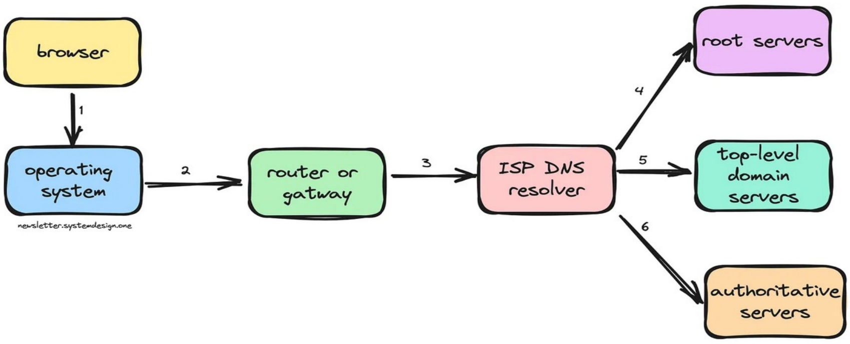
1. What is Domain Name Resolution

Domain Name System (**DNS**) is a database that stores mapping from a domain name (google.com) to its IP address (142.250.185.78).



Parts of the URL(Unified Resource Locator)

- Protocol: Informs web server on which protocol to use like HTTPS or FTP
- Subdomain: A service offered by a website like Google Search or Maps
- Domain: Name of the website
- Top-level domain: the organization entity



How DNS gets resolved:-

- ✔ The browser checks its local cache for the DNS entry
- ✔ The browser checks whether the operating system cache contains the DNS entry. It does that by executing a system call
- ✔ The browser makes a DNS request to the home router or gateway server to check its local cache

- ✔ The router forwards the DNS request to the internet service provider (**ISP**) to check its DNS cache
- ✔ DNS resolver queries the root servers
- ✔ DNS resolver queries the top-level domain servers like .com or .org
- ✔ DNS resolver queries Authoritative name servers like google.com

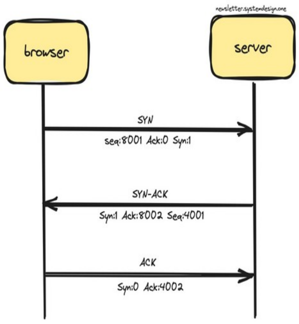
Each component in the DNS resolution caches the result when a DNS query gets resolved. Also DNS entry is assigned a time-to-live (**TTL**) expiry limit.

2. What Is a Three-Way Handshake in TCP?

The browser uses Hypertext Transfer Protocol (**HTTP**) to transfer data.

While Transmission Control Protocol (**TCP**) is a low-level protocol. It belongs to the transport layer or layer 4 in the OSI model. It allows the detection of errors and the retransmission of corrupted data packets.

how a browser opens a TCP connection to the server:



i. The browser sends a SYN request with a random sequence number

ii. The servers respond with SYN-ACK. The acknowledgment number is created by incrementing the received sequence number by 1. Also the server sends a random sequence number.

iii. The browser sends ACK. The acknowledgment number is created by incrementing the received sequence number by 1.

3. HTTP Request Response

a. How to Upgrade From HTTP to HTTPS?

HTTP doesn’t encrypt the data. So anybody can eavesdrop on the data packets. While HTTPS encrypts the data to prevent man-in-the-middle attacks. HTTP upgrade request uses *asymmetric* encryption. While communication that occurs after an HTTPS upgrade uses *symmetric* encryption.

Asymmetric encryption uses a key pair: public and private keys. While symmetric encryption uses a single private key to encrypt and decrypt the messages.

b. HTTP Request Response

The browser makes a GET request to view the Google webpage. While a POST request is used to search a keyword via the search engine.

An HTTP request consists of different entities:

- Uniform Resource Locator (**URL**)
- HTTP headers
- HTTP body (optional)

This is how the server handles an HTTP request:

1. The server forwards the HTTP request to the request handlers. The request handler is a piece of code defined in any programming language like Python, Node.js, or Java
2. The request handler checks the HTTP request headers (content-type, content-encoding, cookies, etc)
3. The request handler validates the HTTP request body
4. The request handler generates a response in the content type (JSON or XML) requested by the client

4. How Browser Renders Server Response

The browser usually makes different HTTP requests to get the data to render a website. The types of files needed are CSS, JavaScript, and Images.

The browser then render the HTML with the received data.