Q) What happens when we type google.com and press enter?

Ans:

1. **Initial typing**

   When we type the first letter 'G', the browser will either start looking for our history and pages that starts with letter 'G' in our recent visited history and start showing an autocomplete list.

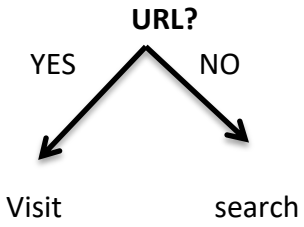
   OR

   Some browser will actually do a search to an index that is local through the locally searched index that is cached.

   OR

   Some browser might actually send the request to a server to the default search engine baked into the browser.

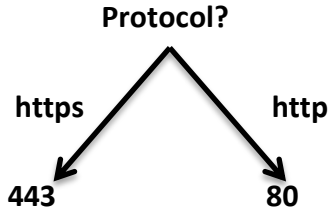
2. **URL phrase**



Browser will start parsing this thing and it asks a question "is this a URL or is this a search term?", if it's a search term it actually does a search.

If its URL it visits that page. It starts the process to visit the google.com page.

3. **Find protocol**



we determine which protocol and which port to connect to. It checks whether google.com is an https site or http site. If it is found in an hsts list then it uses the https protocol and the port will be 443.

4. **DNS lookup**

   TO find out the IP address we do a DNS look up .first we ask the operating system, because the domain could be cached, we find that its not . The OS then looks through the hosts file and see if there is a n hardcoded entry , there isnt ..

   Next the browser check if DoH is enabled DNS over HTTPS if yes then it communicate with the DNS provided (e.g cloud flair and ask for DNS) thats another TLS connection assume we are not using DoH The we establish an insecure UDP request to port 53 on the default DNS Configured on our router (could be 8.8.8.8 or 1.1.1.1) that in itself is a connection so we need to send the packet..

5. **TCP connection**

   We know the IP we know the port! we can now establish a connection, we also know that we should also do TLS since its HTTPS and our client is smart enough to do TLS 1.3 so we will first do 3 way handshake and establish a TCP connection between 10.0.0.2 port random 1234 and 4.1.2.3 port 443.

6. **TLS, ALPN, SNI**

   Assuming I'm using the latest browser so it supports TLS 1.3 and my server also supports TLS 1.3, next is Client Hello. Client generates a public and private key, merges public and private key in DH sends out public and merged keys which cannot be broken in a client hello. It also sends the supported cipher suits (supported for symmetric key algorithms) If TLS extensions are enabled such as ALPN & SNI the client also sends in the same request the host name google.com in the TLS client hello along with the fact that it actually supports HTTP2 (this might be different in Chrome since it uses HTTP/2 over UDP or QUIC)

7. **First Request GET**

   The client is now ready to send an actual HTTP data, so it builds header GET / since that is what we want to send, puts the hostname in the header and other stuff, checks if there are cookies and puts them, the whole thing is compressed and sent as a binary format. The data is then encrypted with the TLS symmetric key and sent..

8. The get request is then streamed into the HTTP/2 tcp connection and sent to the server.