### Watch the Todays Lecture again - Done

## Research about How API Works?

An API (Application Programming Interface) is a set of rules and protocols that allows different software applications to communicate and interact with each other. It acts like a "middleman" or translator between a client (such as a mobile app or web browser) and a server, enabling requests for specific data or services and responses back to the client in a standardized way.

How does it work?

A client sends a request to the API, usually specifying an endpoint URL and an HTTP method like GET (to retrieve data), POST (to submit data), PUT (to update data), or DELETE (to remove data).

The API processes the request, communicates with the server or service behind it, and then sends back a response with the requested data or confirmation of an action.

This interaction follows a request-response cycle, ensuring secure, structured communication without the client having to know the internal workings of the server.

A common analogy is a restaurant: the client is the customer, the API is the waiter taking orders, and the server is the kitchen preparing what is requested.

Example: User Authentication with Google Account Login. An app or website allows users to log in using their Google account instead of creating a new username and password.

## what happen when you type google.com in browser and how you see the google page and every time you time gogole.com in the browser then always same process happen?

When you type "google.com" in your browser and press enter, a series of steps happen so that you can see the Google homepage. This process is repeated every time you type the same URL, involving these main stages:

DNS Resolution: Your browser asks a Domain Name System (DNS) server to translate "google.com" into an IP address (the actual address of Google's servers).

TCP/TLS Connection: Using the IP address, your browser establishes a connection with Google's server using the Internet protocols TCP and sets up a secure encrypted link via TLS (the modern version of SSL) to protect your data.

HTTP Request: Your browser sends an HTTP(S) request to the Google server asking for the homepage.

Server Response: Google's server processes your request and sends back the HTML, CSS, JavaScript, and other files that make up the Google homepage.

Parsing and Rendering: Your browser parses these files, builds internal data structures like the DOM (Document Object Model) and CSSOM, and then renders the webpage you see on the screen.

This entire workflow from typing the URL to seeing the page happens quickly and is repeated each time because web content can update, and connections are typically temporary. However, the browser caches some resources and DNS lookups for efficiency, so parts of this process may be faster on subsequent visits.

This cycle ensures you get the most current version of the webpage securely and efficiently every time you visit.

## How many Protocols are there for API/Network?

Here are key categories and examples:

**Transport and Internet Protocols:**

Transmission Control Protocol (TCP)

User Datagram Protocol (UDP)

Internet Protocol (IP)

**Application Layer Protocols for Web and Services:**

Hypertext Transfer Protocol (HTTP/HTTPS)

Simple Mail Transfer Protocol (SMTP)

File Transfer Protocol (FTP)

Domain Name System (DNS)

Simple Network Management Protocol (SNMP)

**Authentication and Session Management Protocols:**

OAuth (used for API authentication)

Kerberos

RADIUS

**Routing and Network Management Protocols:**

Border Gateway Protocol (BGP)

Open Shortest Path First (OSPF)

Dynamic Host Configuration Protocol (DHCP)

**Other Protocols for Real-Time, Security, and Specialized Uses:**

Internet Control Message Protocol (ICMP)

Secure Shell (SSH)

Session Initiation Protocol (SIP) for VoIP

Network Time Protocol (NTP)

## what is the full form of API?

Application Programming Interface

## what is the max length of the URL?

There is no strictly defined length for a URL

## How or when the IP address update of our mobile or laptop device (optional extra point)

The IP address of your mobile or laptop device updates in several common situations:

Dynamic IP Assignment by Network: Most devices get their IP address dynamically assigned by the network's DHCP server (e.g., your home router, cellular provider). The IP address can change when you:

Connect to a different Wi-Fi network or mobile network.

Reboot or reset your router or modem, which could request a new IP from your ISP.

Reconnect or renew your device's network connection, prompting the DHCP server to assign a possibly new IP address.

Network Changes: When your device switches from one network to another (e.g., from home Wi-Fi to mobile data or another Wi-Fi hotspot), it receives a new IP address appropriate for that network.

Scheduled or Event-Triggered Renewals: Many ISPs assign IP addresses dynamically and can change them periodically or due to network management policies. Your device may receive a new IP when its lease expires, and it requests a renewal.

Manual or VPN Changes: You can manually change your local IP address on your device or use a VPN to mask/change your public IP address to one from the VPN server’s pool.

This process means your IP address is not fixed but updates dynamically as you connect, disconnect, or change networks, or as network equipment resets.