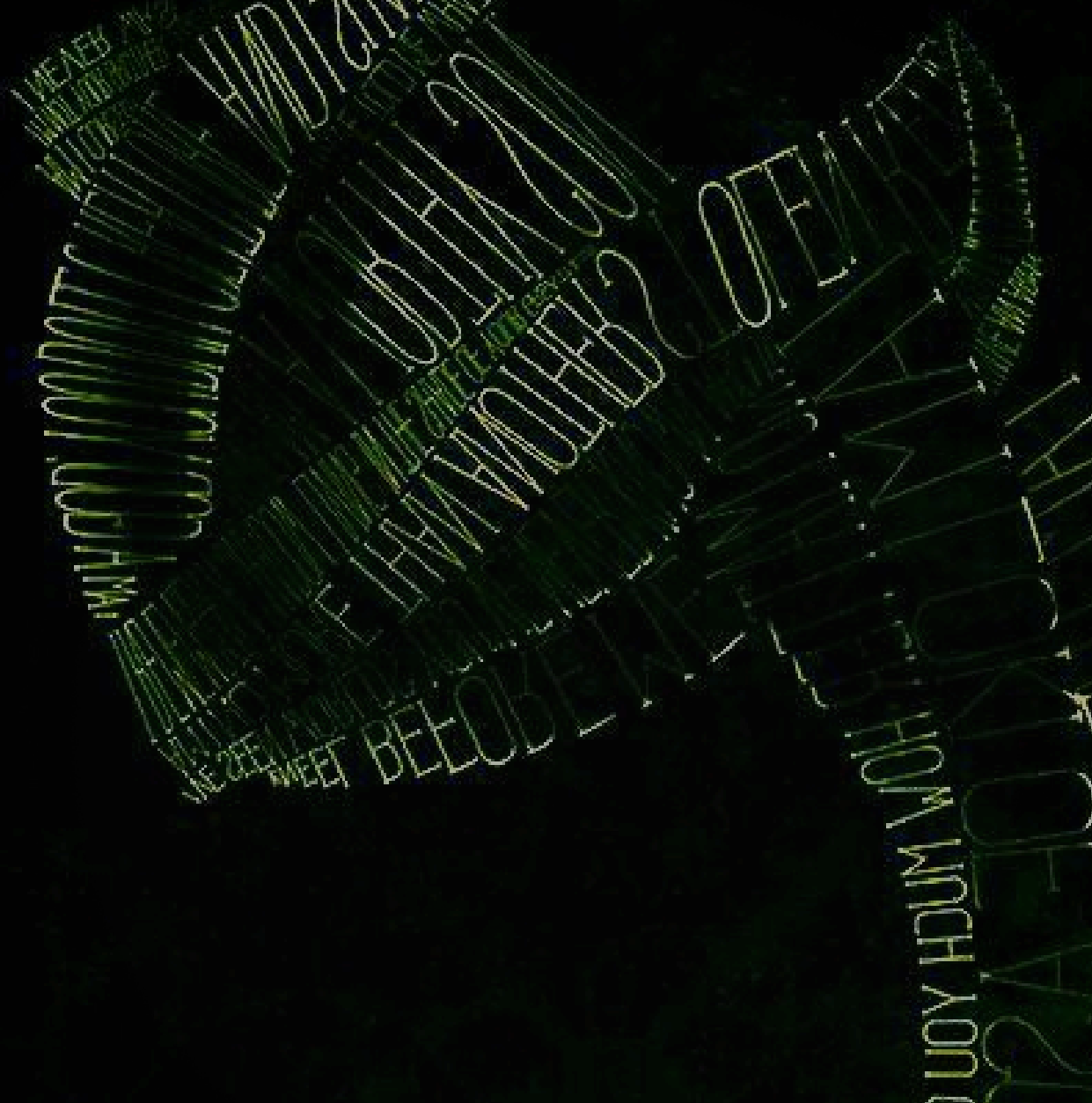
Sheryians
Coding School

Live Cohort

Day - 4

Understanding HTTP & HTTPS



Understanding HTTP & HTTPS

1. What is HTTP and Its Different Versions

HTTP (HyperText Transfer Protocol) is the foundation of communication between a client (browser) and a server.
It defines **how requests are made** by the client and **how responses are returned** by the server.

🔷 Different Versions of HTTP

- **HTTP/1.0 (1996)**:
  - Every request opens a new connection.
  - Slower and inefficient because connections closed after each response.
- H**TTP/1.1 (1997):**
  - Introduced **persistent connections (keep-alive).**
  - Multiple requests could share the same connection.
  - Became the most **widely used** version for years.
- **HTTP/2 (2015):**
  - Much faster; supports **multiplexing** (many requests in one connection).
  - Uses **binary protocol** (instead of plain text), reducing delay.
  - Greatly improved performance.
- **HTTP/3 (2020s):**
  - Built on **QUIC protocol** (runs on UDP).
  - Even faster and more reliable for modern apps like **video streaming, gaming, and real-time communication.**

Understanding HTTP & HTTPS

2. HTTP Status Codes for Responses

Whenever a server responds, it sends back a **status code** to indicate the result of the request.

- 1**xx – Informational**: Request received, still processing.
- **2xx – Success:** Request completed successfully.
  - 200 OK: Standard success message.
- **3xx – Redirection:** Further action needed.
  - 301 Moved Permanently, 302 Found.
- **4xx – Client Errors**: Problem with the client's request.
  - **400 Bad Request, 401 Unauthorized, 404 Not Found.**
- **5xx – Server Errors:** Issue with the server itself.
  - 500 Internal Server Error, 503 Service Unavailable.

🔷 Example :

If you type a wrong link, you'll often see **404 Not Found.**

3. What is HTTPS and Why It's Better than HTTP

HTTPS (HyperText Transfer Protocol Secure) is the secure version of HTTP.

- It uses **encryption** to protect communication between browser and server.
- Prevents hackers from **reading** or **modifying** your data.
- Always used in sensitive activities like **banking**, **payments**, and **login forms**.

Understanding HTTP & HTTPS

4. How HTTPS Provides a Secure Connection

HTTPS uses **SSL/TLS encryption** to secure communication.

- Data is converted into unreadable form before sending.
- Only the **intended server** and **browser** can decrypt it.
- Protects against:
  - **Eavesdropping** (hackers listening to traffic).
  - **Data tampering.**
  - **Identity theft.**

5. What is SSL/TLS Encryption

- **SSL (Secure Sockets Layer)** and **TLS (Transport Layer Security)** are security protocols.
- TLS is the **modern** and **more secure** version of SSL.

They ensure three key things:

1. **Encryption** → Outsiders can't read your data.
2. **Authentication** → Confirms the website is genuine.
3. **Integrity** → Data isn't modified during transfer.

6. What are Proxy and Reverse Proxy

🔷 Proxy Server

- Works between **client and internet**.
- Hides the client's identity.
- Uses:
  - Privacy (hide IP address).
  - Access blocked content.
  - Content filtering in schools/offices.

🔷 Reverse Proxy

- Sits in **front of servers** and handles client requests on their behalf.
- Clients don't know the actual server details.
- Uses:
  - **Load balancing** (distributing traffic).
  - **Security** (protecting actual servers).
  - **Caching** (faster performance).

7. How VPN Works and Helps Accessing Restricted Content

A **VPN (Virtual Private Network)** creates a secure "tunnel" between your device and the internet.

- Encrypts all data → ISP or government cannot monitor browsing activity.
- Hides your real location by showing a **different IP** address.
- Useful for:
  - Accessing restricted websites/apps.
  - Ensuring privacy on **public Wi-Fi**.
  - Securing sensitive business or personal communication.

🔷 Example :

Using a VPN can make it appear like you're browsing from the US, even if you're in India.