**Task 8: Identify and Remove Suspicious Browser Extensions**

**(VPN Setup and Privacy Protection Report)**

**Objective**

To understand the role of VPNs in protecting privacy and enabling secure communication by setting up and testing a free VPN service.

**Tools Used**

* **VPN Service**: ProtonVPN (Free Tier)
* **Verification Website**: whatismyipaddress.com
* **Browser**: Google Chrome

**Procedure**

**Step 1: Choose a Reputable VPN Service**  
I selected **ProtonVPN Free Tier** due to its good reputation, no data limits, and strong encryption.

**Step 2: Download and Install the VPN Client**

* Created a free ProtonVPN account on the official website.
* Downloaded the ProtonVPN client for Windows.
* Installed and launched the application.

**Step 3: Connect to a VPN Server**

* Logged into ProtonVPN with my account credentials.
* Selected the **Fastest Server** option for best speed.
* Connected successfully (Green "Connected" status shown).

**Step 4: Verify IP Address Change**

* Visited **whatismyipaddress.com** before connecting — saw my real location and IP.
* After connecting to the VPN, refreshed the page — IP and location changed to match the VPN server location.

**Step 5: Confirm Traffic Encryption**

* Browsed websites — confirmed padlock icon in browser for secure HTTPS connection.
* Verified encryption via Cloudflare’s encryption check page.

**Step 6: Disconnect and Compare**

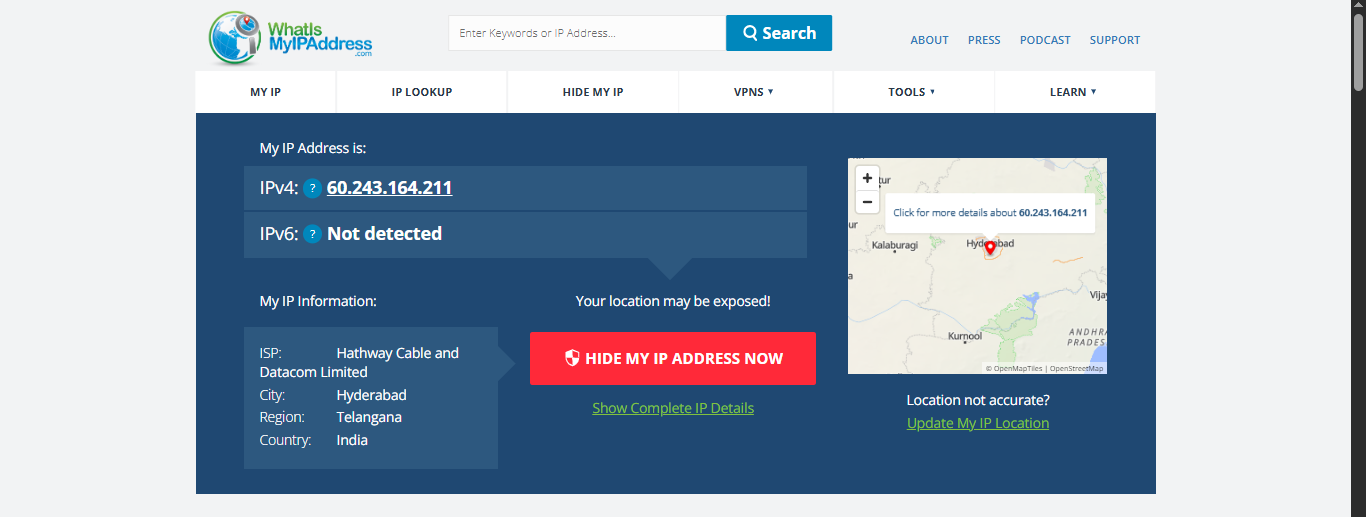
* Disconnected from ProtonVPN.
* Checked IP again — returned to original IP and location.
* Browsing speed improved slightly after disconnecting.

**Step 7: Research VPN Encryption and Privacy**

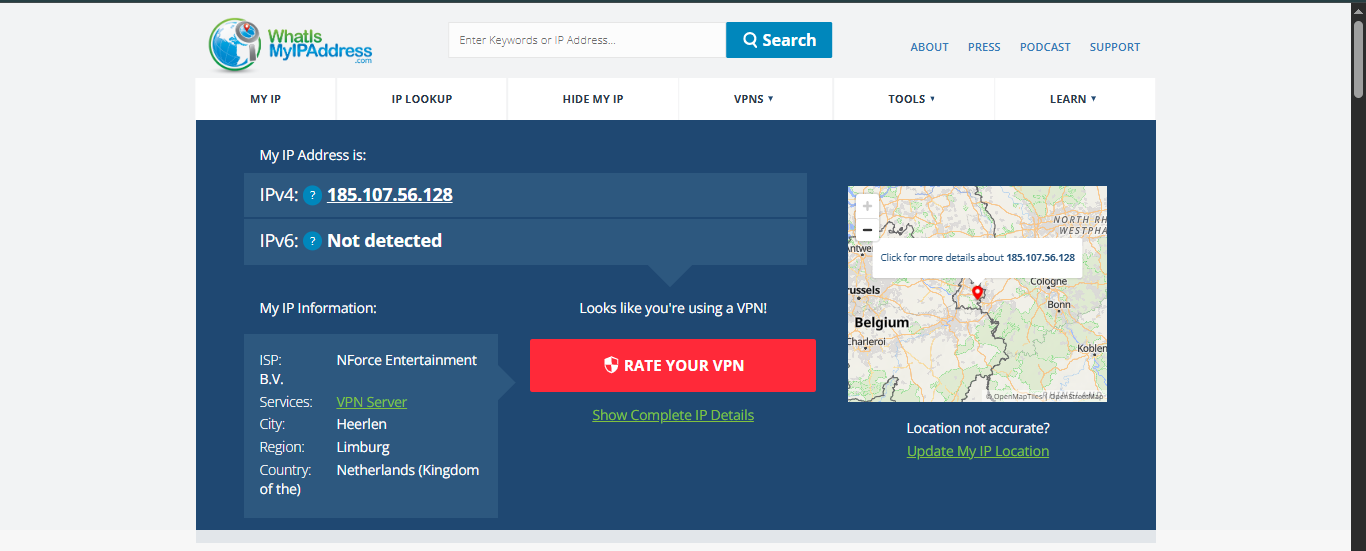
* ProtonVPN uses **AES-256** encryption and **OpenVPN / WireGuard** protocols.
* Has a **strict no-logs policy** to protect user privacy.

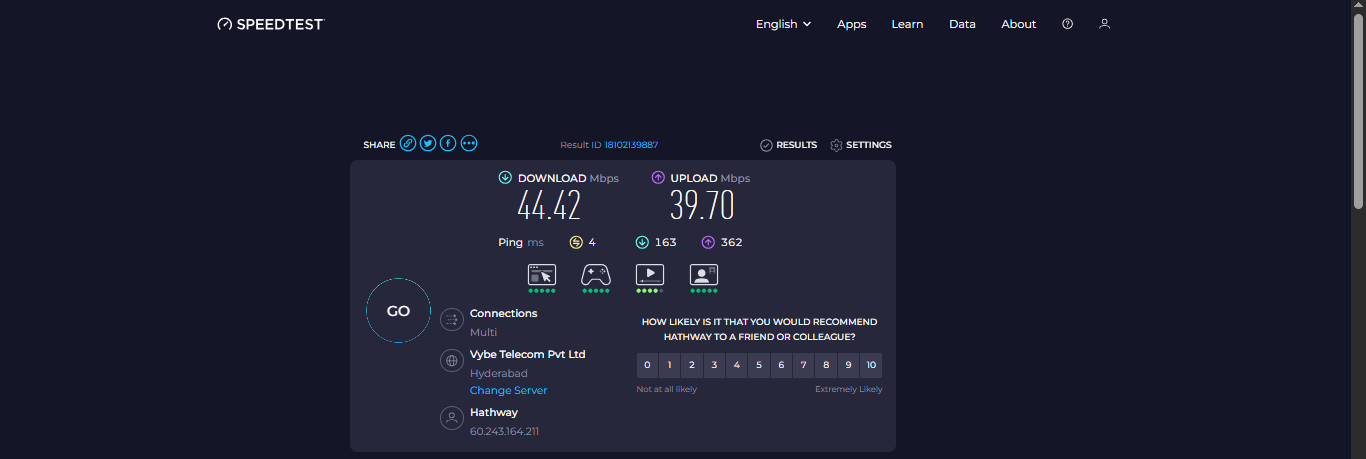
**Connection Status Screenshot:**

**Before Connection:**

****

**After Connecting to a VPN:**

****

**Speed Test Before Connecting to VPN:  
**

**Speed Test After Connecting to VPN:**

