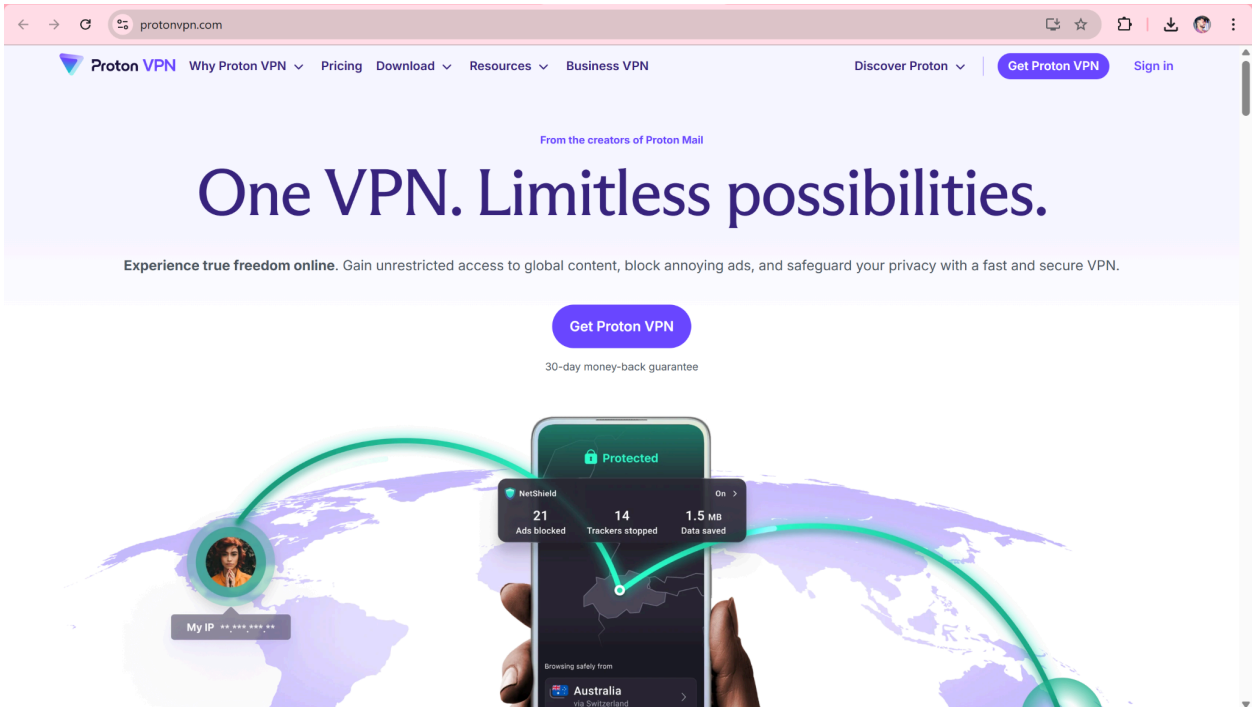
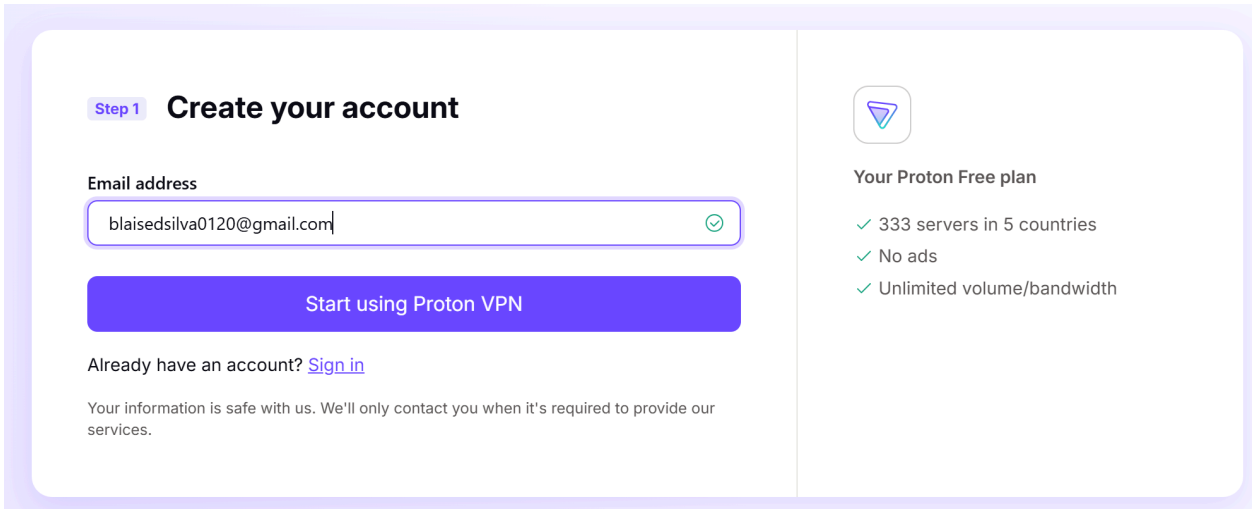
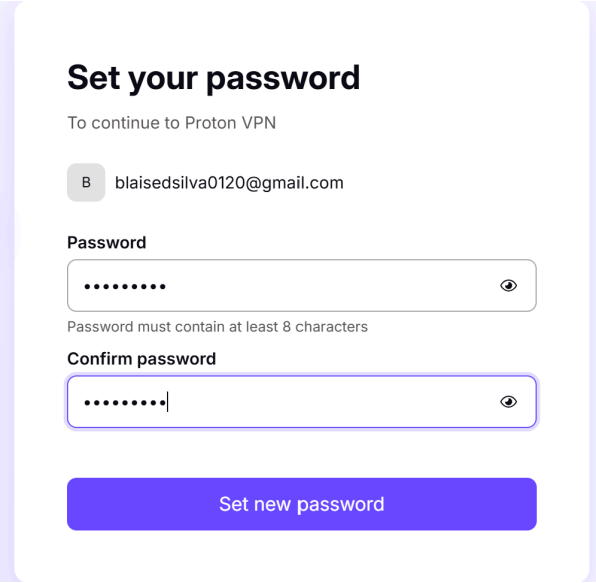
Task 8 : Working with VPNs

1.Choose a reputable free VPN service and sign up.

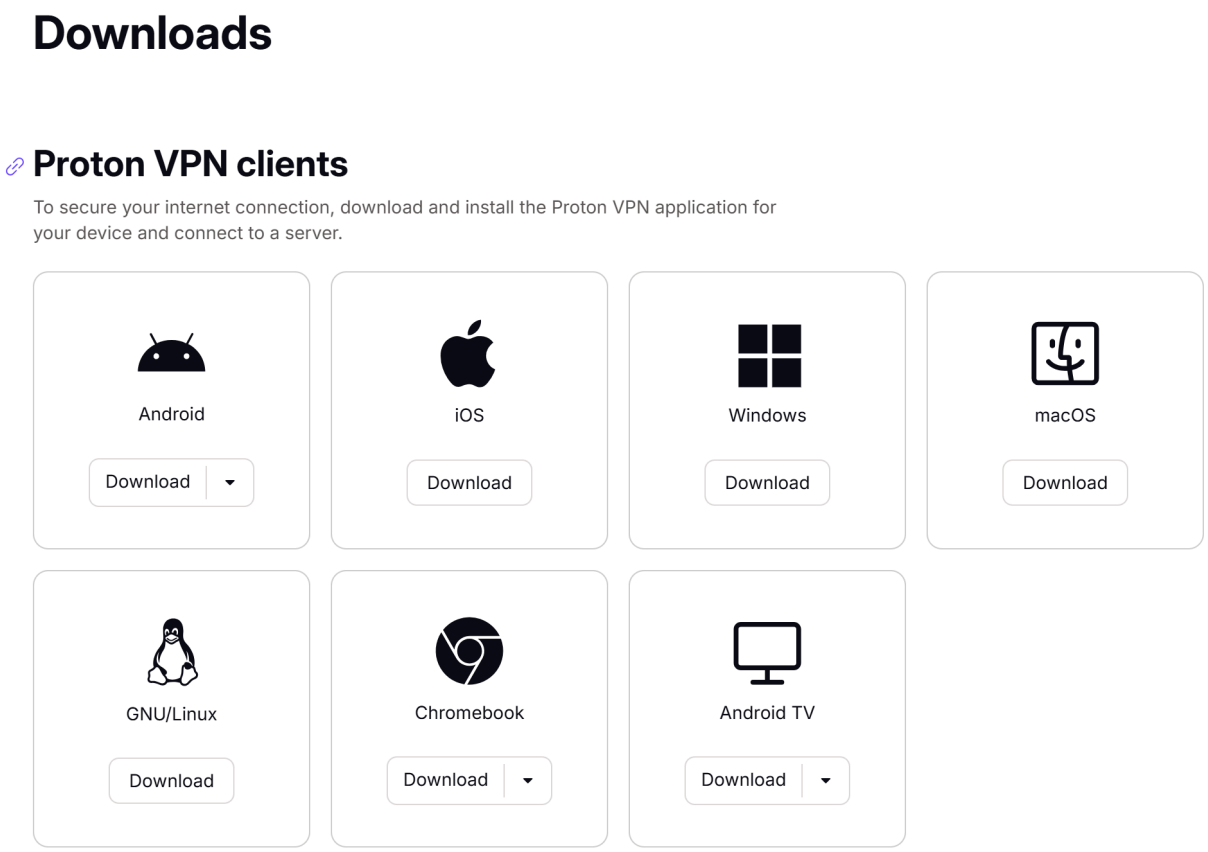


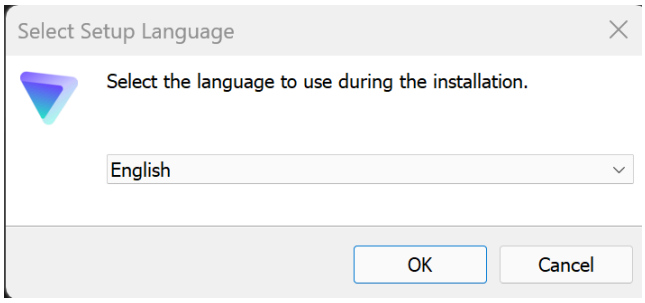


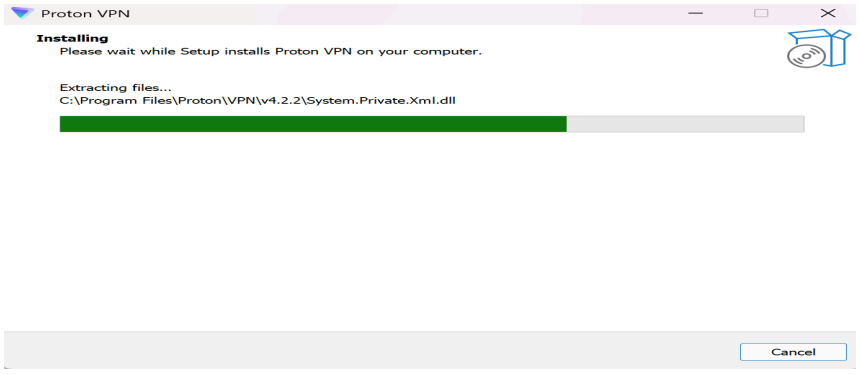


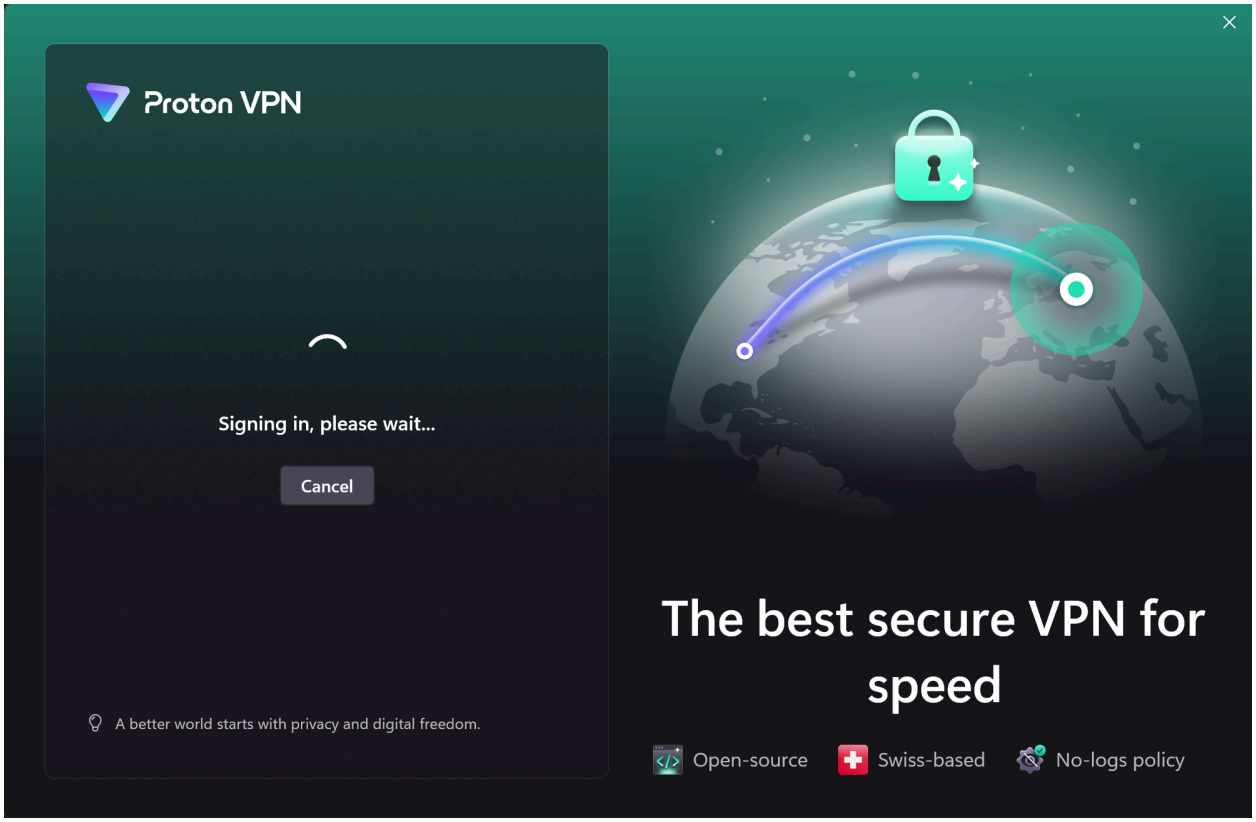
I selected ProtonVPN as my free VPN service due to its reliability and unlimited data on the free tier. I visited the official ProtonVPN website, created a free account using my email, and completed the verification process. After logging in, I confirmed that my account was active under the free plan.

2.Download and install the VPN client.



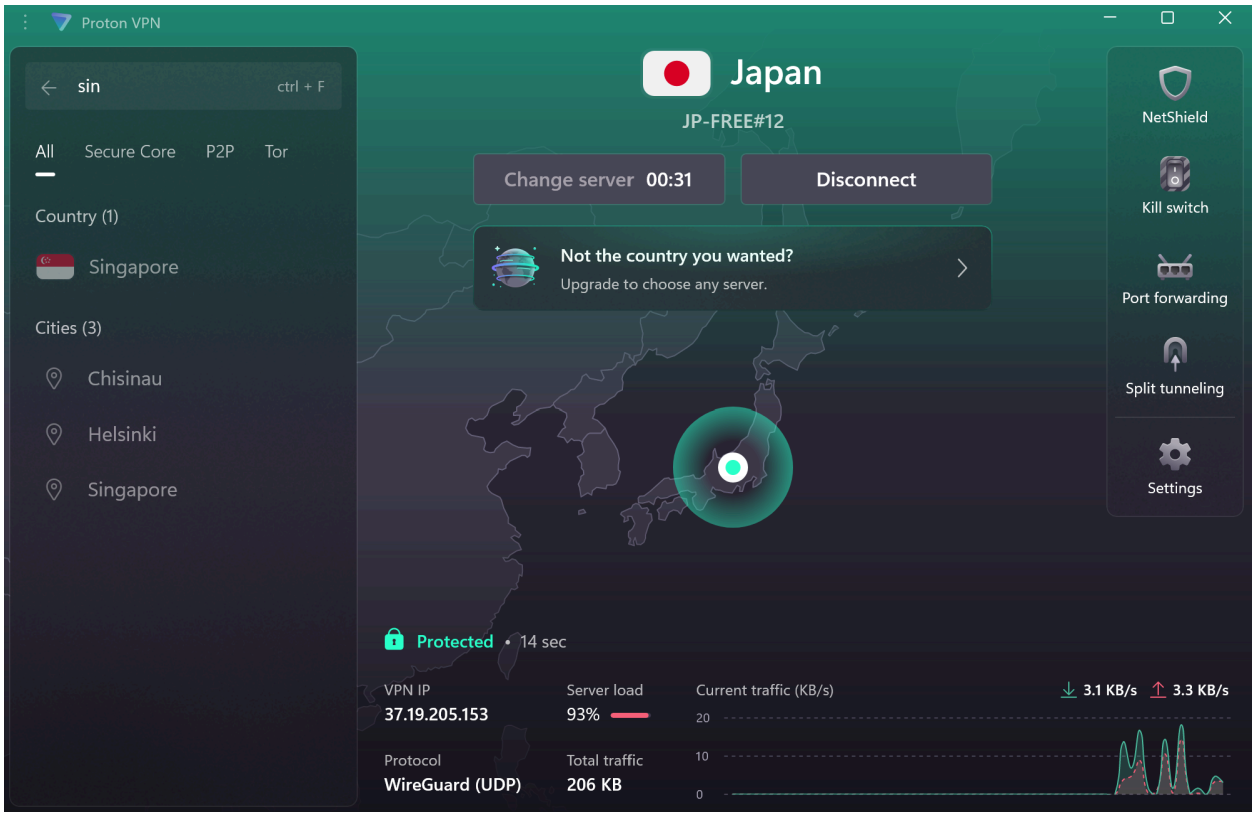






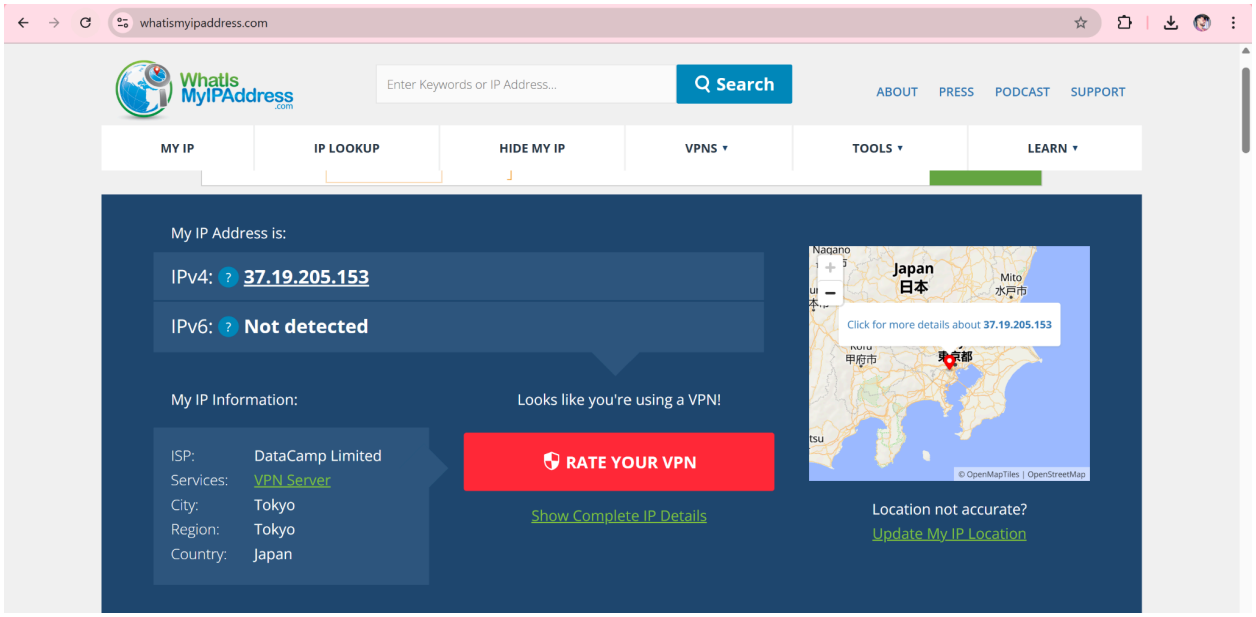
I downloaded the Windows (x64) version of ProtonVPN from the official website. After the download was complete, I ran the installer and followed the setup wizard to finish the installation. Once installed, I launched the ProtonVPN application, which opened successfully and was ready for login.

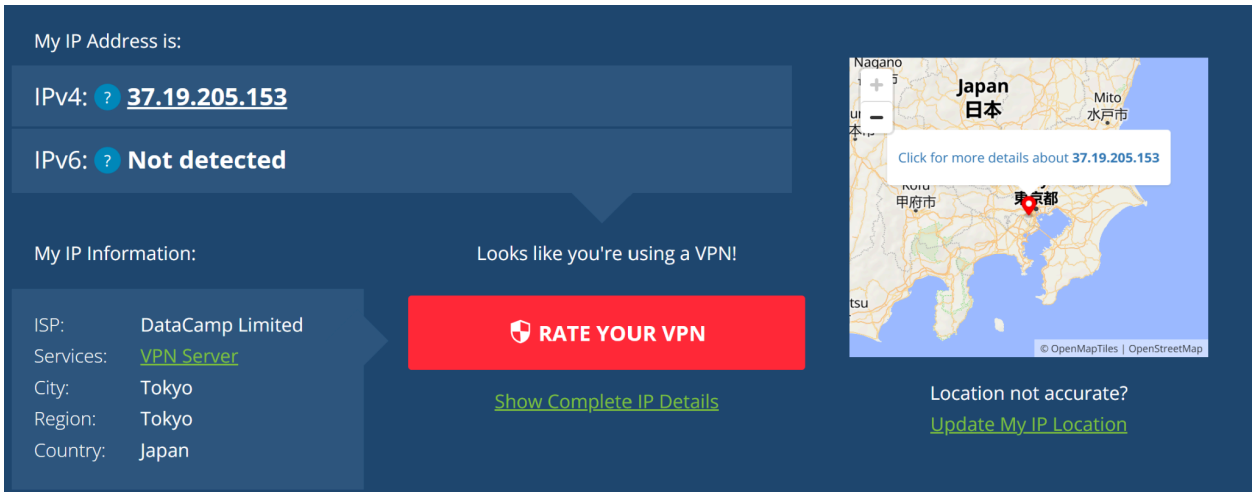
3.Connect to a VPN server (choose closest or any location).



I opened the ProtonVPN application and logged in with my account. From the available free servers, I selected a server in Japan and clicked the connect button. Within a few seconds, the status changed to “Connected” and my IP address was updated to reflect the new location.

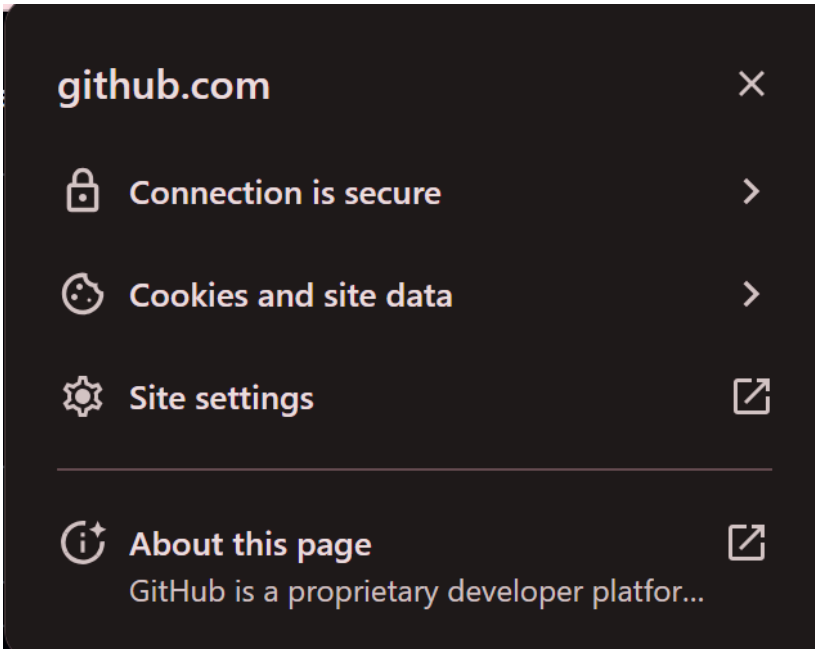
4.Verify your IP address has changed (use whatismyipaddress.com).





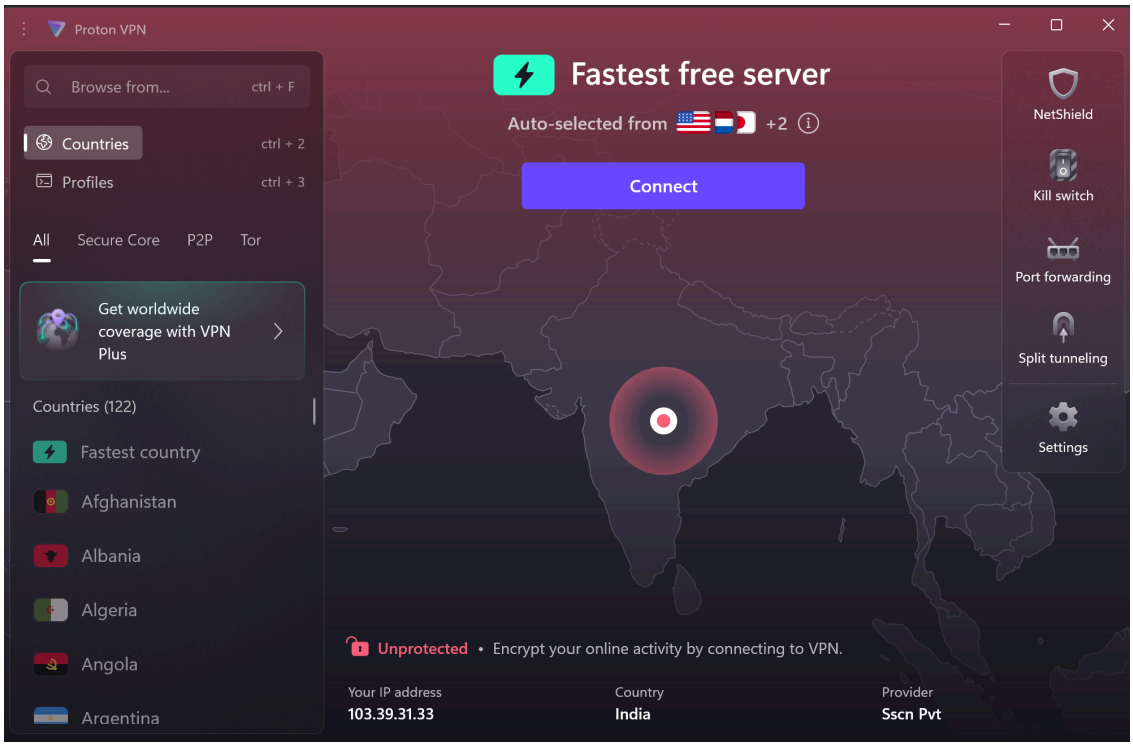
With the VPN connected, I visited whatismyipaddress.com to check my current IP details. The website displayed a new IP address and location matching the VPN server I had connected to in Japan, confirming that my real IP address was successfully masked.

5.Browse a website to confirm traffic is encrypted.

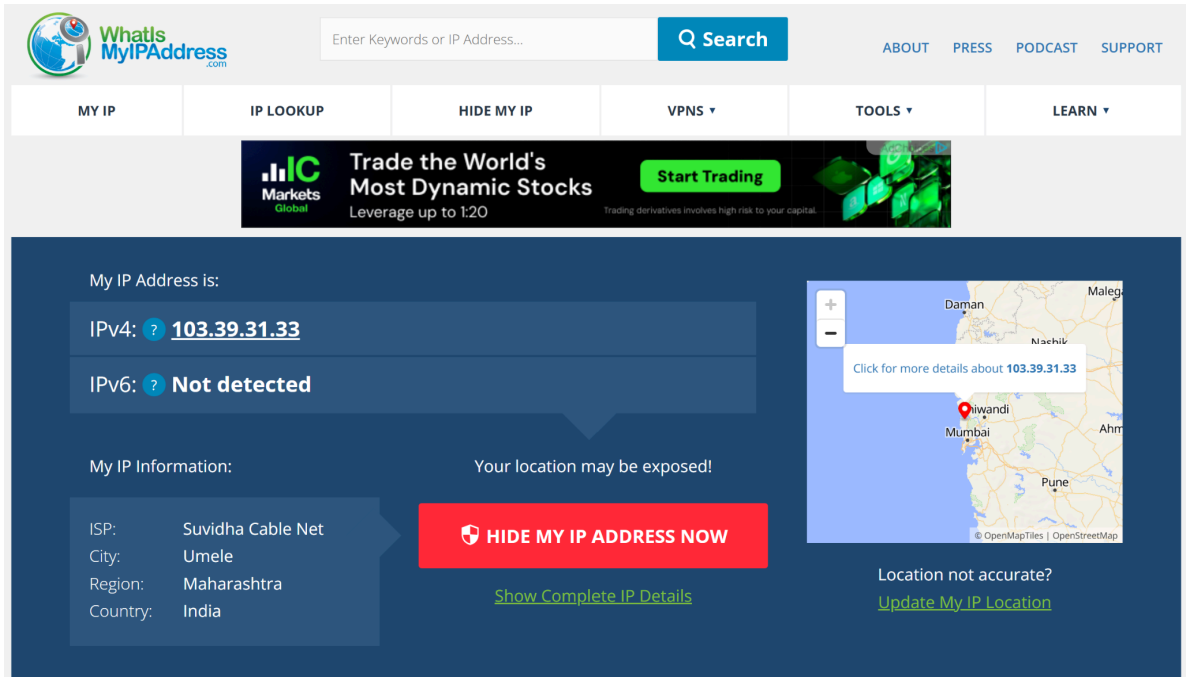


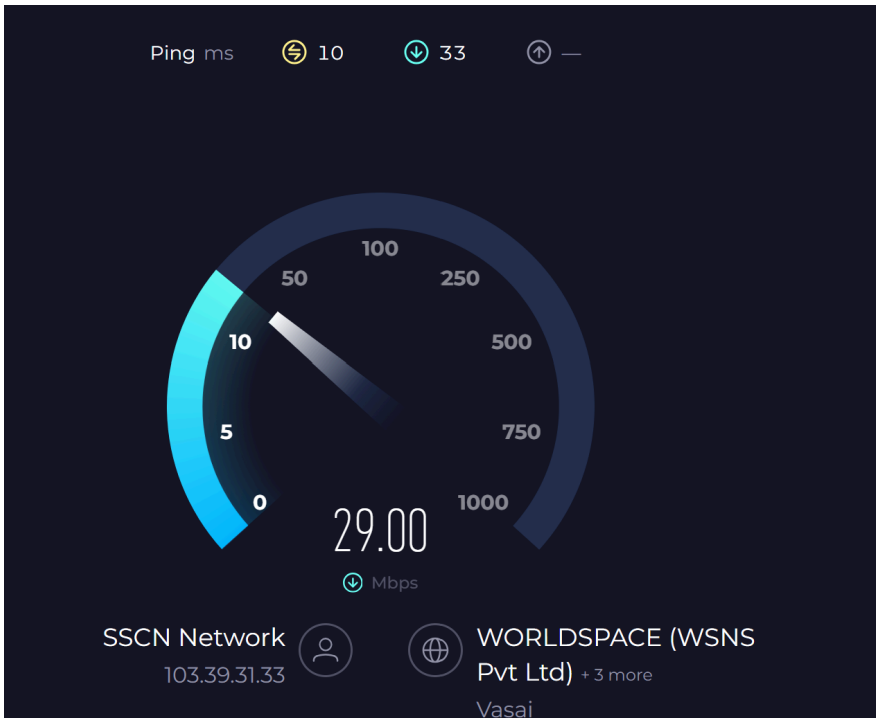
While connected to the VPN, I visited GitHub's website using my browser. The site information panel indicated that the connection was secure and encrypted with HTTPS. This confirmed that my browsing traffic was protected, with the VPN adding an extra layer of encryption.

6.Disconnect VPN and compare browsing speed and IP.



So the status shows not connected





After completing the browsing tests with VPN enabled, I disconnected from ProtonVPN. I then revisited *whatismyipaddress.com* to verify that my IP address reverted to my original ISP-assigned address, confirming the VPN tunnel was closed. Additionally, I conducted a speed test on *speedtest.net*, which showed a download speed of **29 Mbps** with significantly lower latency compared to the VPN-connected session. This comparison illustrated the typical improvement in speed after disconnecting from a VPN, as well as the return to my real network identity.

7.Research VPN encryption and privacy features.

I explored VPN encryption and privacy features using *security.org* and *linfordco.com*. VPN encryption protects data by converting it into ciphertext using strong algorithms like AES-256, ensuring that even if intercepted, the data is unreadable. It relies on secure tunneling protocols such as OpenVPN, IKEv2, and WireGuard to transmit information safely. I learned that VPNs also mask the real IP address, replacing it with one from the VPN server to hide the user's location and activity. Privacy features such as kill switches prevent data leaks if the VPN connection drops, and DNS leak protection ensures all DNS queries stay encrypted. This combination of encryption and privacy measures keeps online activity safe from hackers, ISPs, and surveillance, while maintaining anonymity and security.

I explored VPN encryption and privacy features using **security.org** and **linfordco.com**. VPN encryption works by converting data into ciphertext using strong algorithms like **AES-256**, which ensures that even if the data is intercepted, it cannot be read by unauthorized parties. VPNs rely on secure tunneling protocols such as **OpenVPN, IKEv2, and WireGuard**, which create a protected channel for transmitting information over the internet. One key feature I learned is that VPNs mask the user's real IP address by replacing it with the IP of the VPN server, effectively hiding the user's location and online activities from websites, ISPs, and potential attackers.

Additionally, VPNs offer multiple privacy-enhancing features. **Kill switches** prevent sensitive data from being exposed if the VPN connection unexpectedly drops, while **DNS leak protection** ensures that all DNS queries are securely routed through the VPN, preventing accidental exposure of browsing activity. Some VPNs also provide **split tunneling**, allowing users to route specific traffic through the VPN while keeping other traffic on the normal network. Together, these encryption methods and privacy features provide a comprehensive approach to online security, safeguarding sensitive information, maintaining anonymity, and protecting users from hackers, tracking, and surveillance. Exploring these features helped me understand how VPNs are not just tools for bypassing geo-restrictions, but essential tools for secure, private, and trustworthy internet usage.

Links : https://www.security.org/vpn/encryption/
https://linfordco.com/blog/vpn-encryption/

8.Write a summary on VPN benefits and limitations.

Benefits:

- VPNs keep your data safe by encrypting it, so hackers or others can’t read it.
- They hide your real IP address, helping to protect your privacy and location.
- You can access websites or content that might be blocked in your country.
- Features like kill switch and DNS leak protection add extra safety.

Limitations:

- VPNs can sometimes make your internet slower because your data goes through the VPN server.
- Free VPNs may not be very secure or can log your data.
- Not all websites or services work with VPNs.
- If the VPN fails and there’s no kill switch, your data could leak.