Task 8 : Working with VPNs

Objective: Understand the role of VPNs in protecting privacy and secure communication.

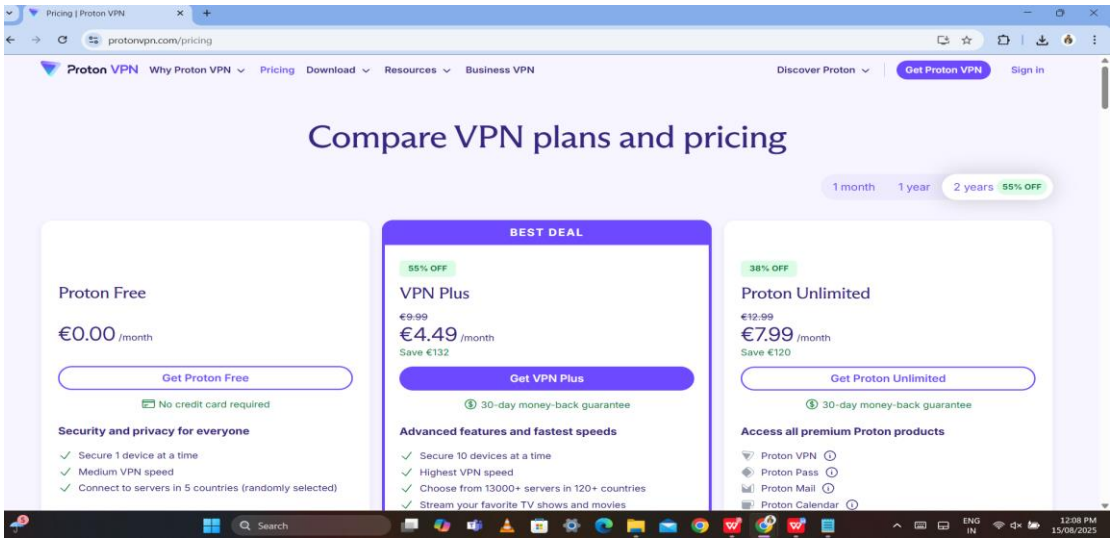
Tools Used:

1. VPN Client – ProtonVPN (Free tier) / Windscribe Free
2. IP Checker – whatismyipaddress.com
3. Operating System – Windows 10 (64-bit)
4. Web Browser – Google Chrome
5. Internet Speed Test (https://www.speedtest.net)

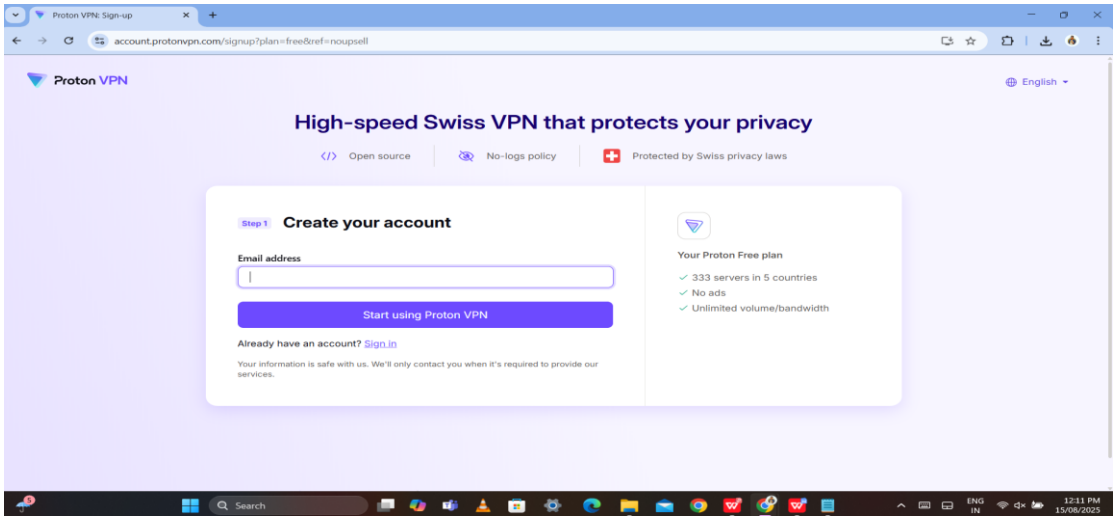
Steps Included :

1. VPN Setup & Testing

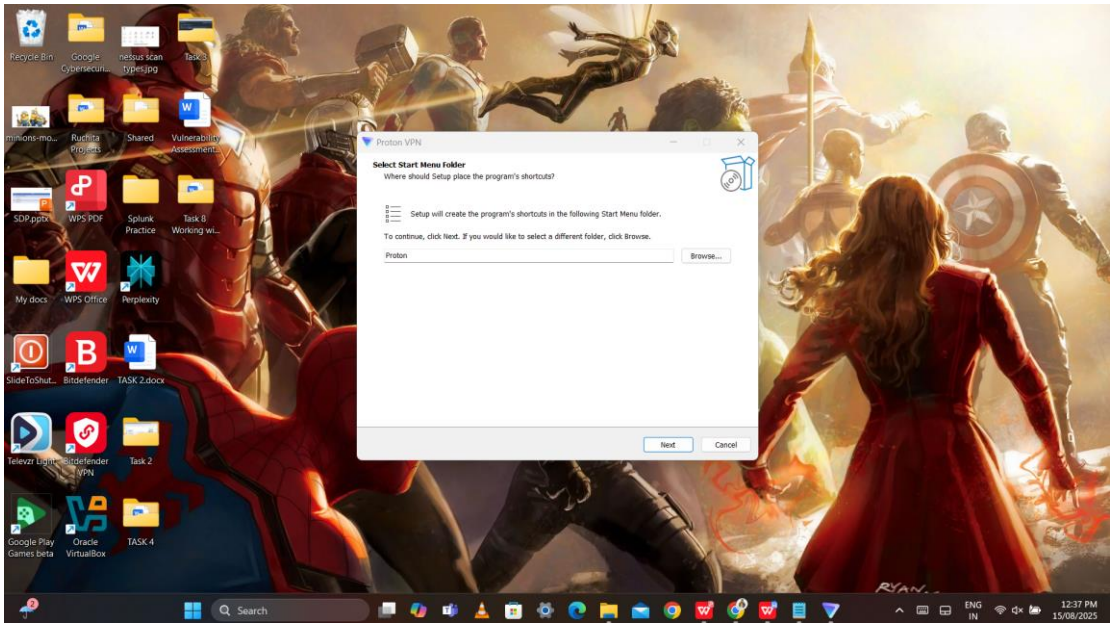
Created a free account on ProtonVPN



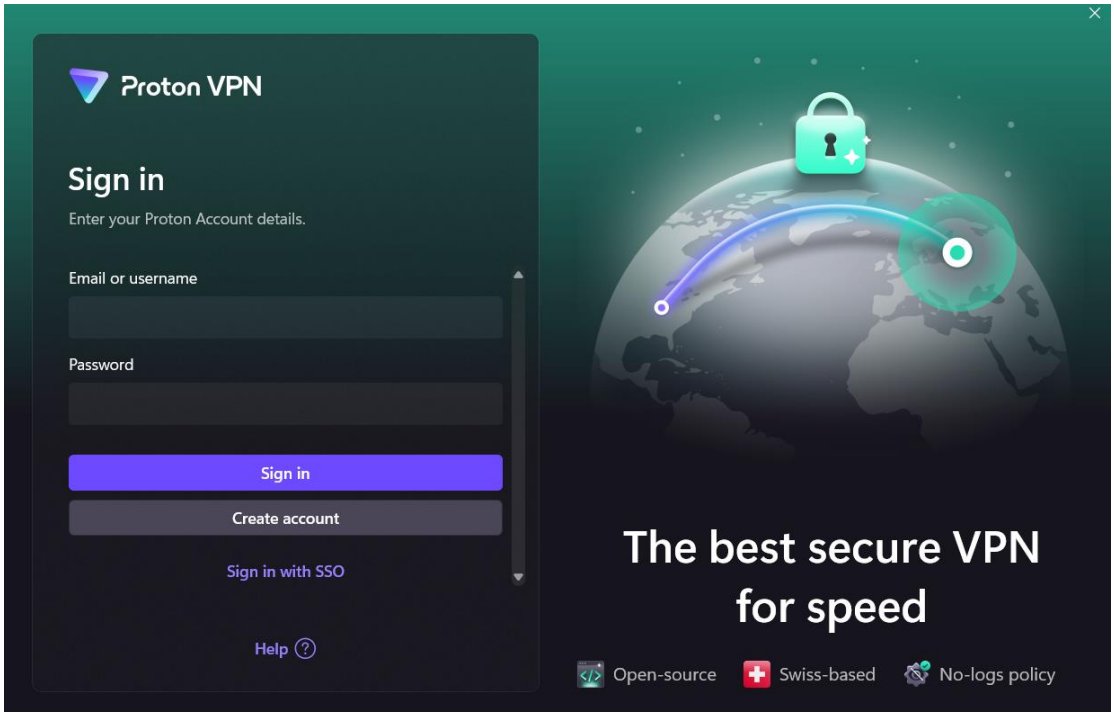
Creating account on Proton VPN



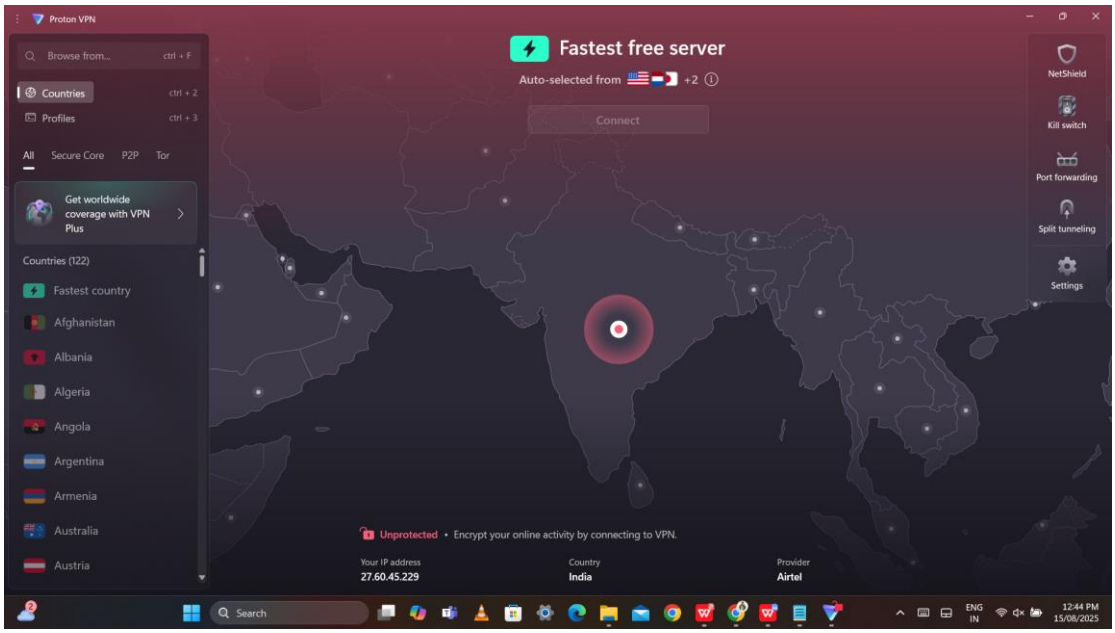
Installing Proton VPN on my computer



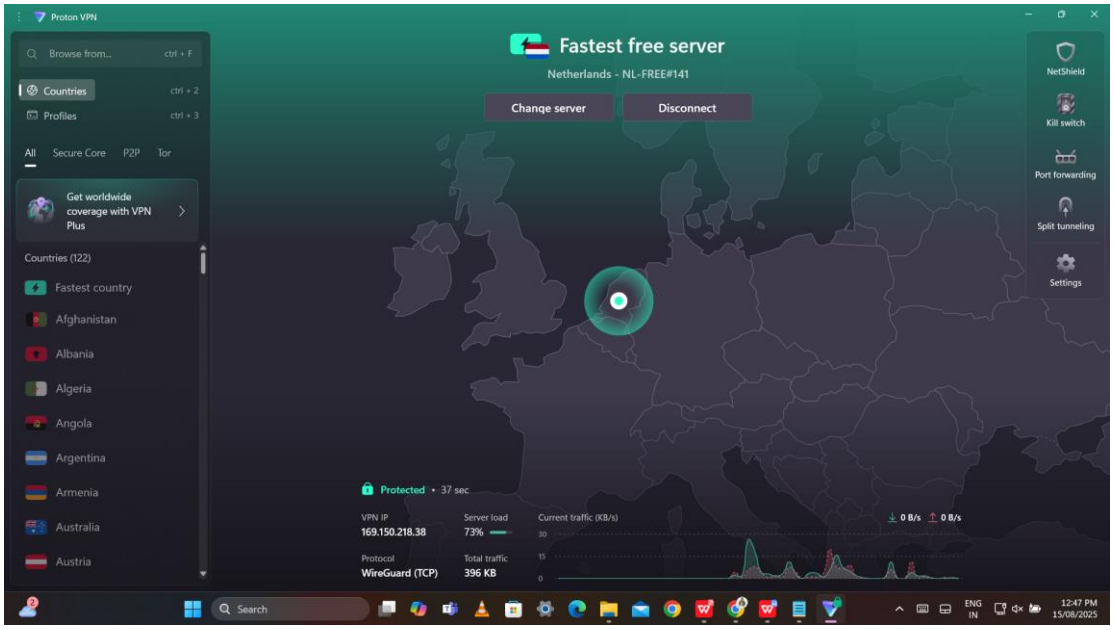
Signing In Proton VPN



Connecting to VPN Server



Connected to Netherlands Server

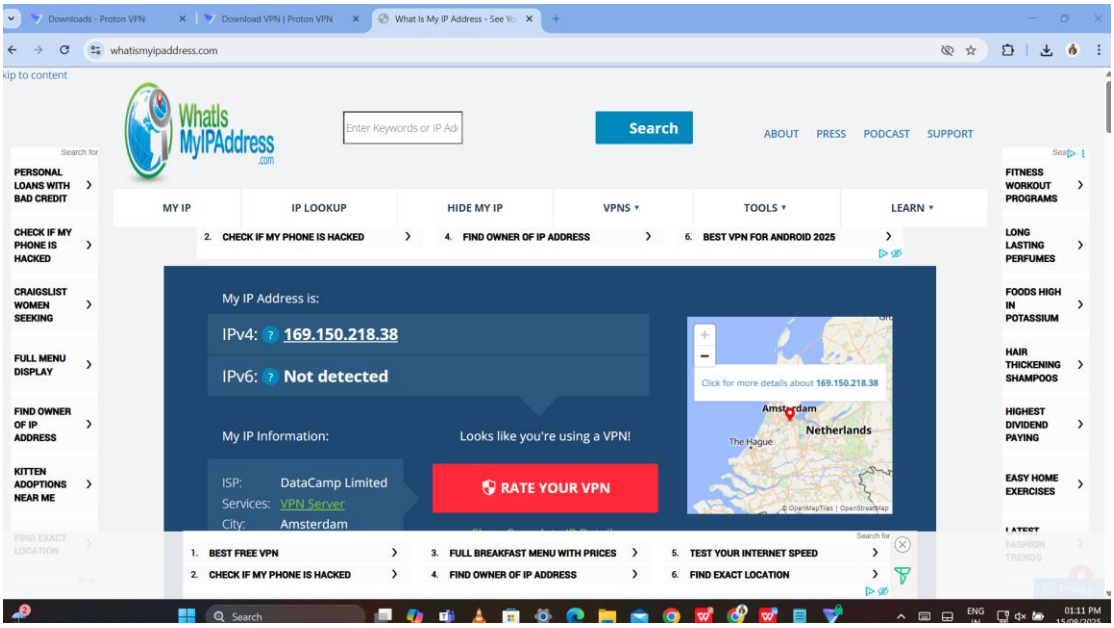


Verifying IP Change

Opened whatismyipaddress.com before and after VPN connection.

Verified that IP address and location changed to match VPN server's region.

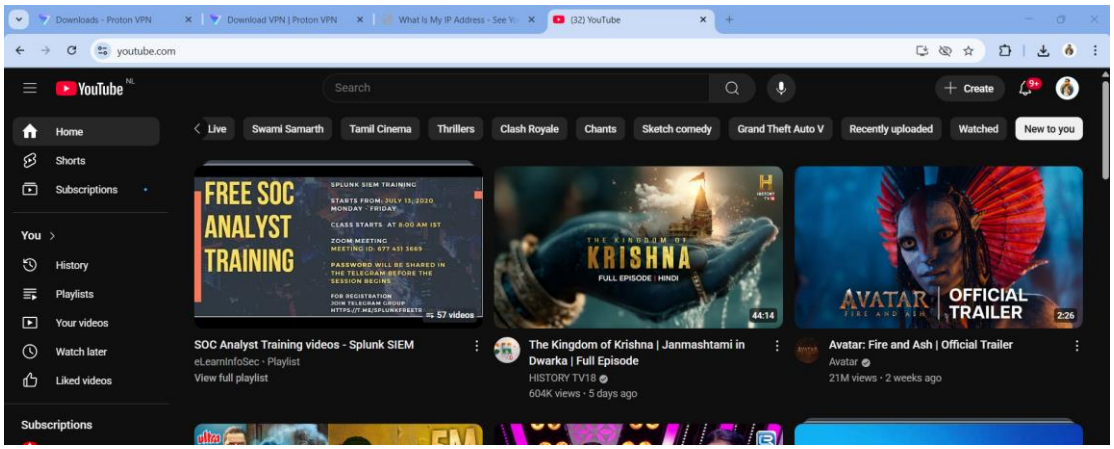
IP gets changed when connected to VPN.



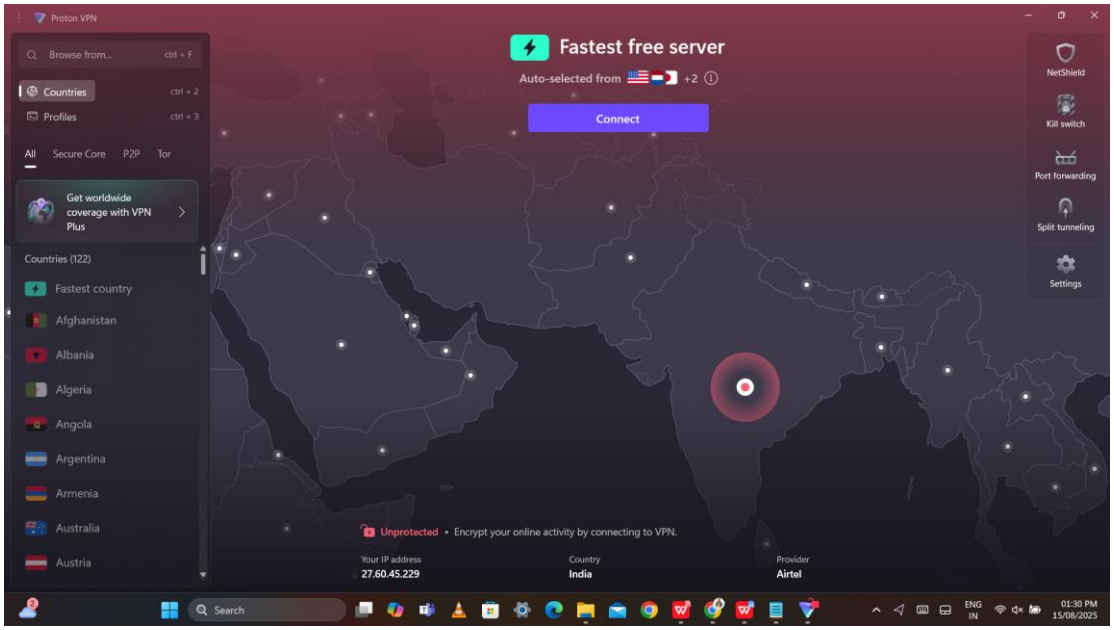
Testing Encrypted Browsing

Accessed websites YouTube to confirm that traffic was routed through the VPN.

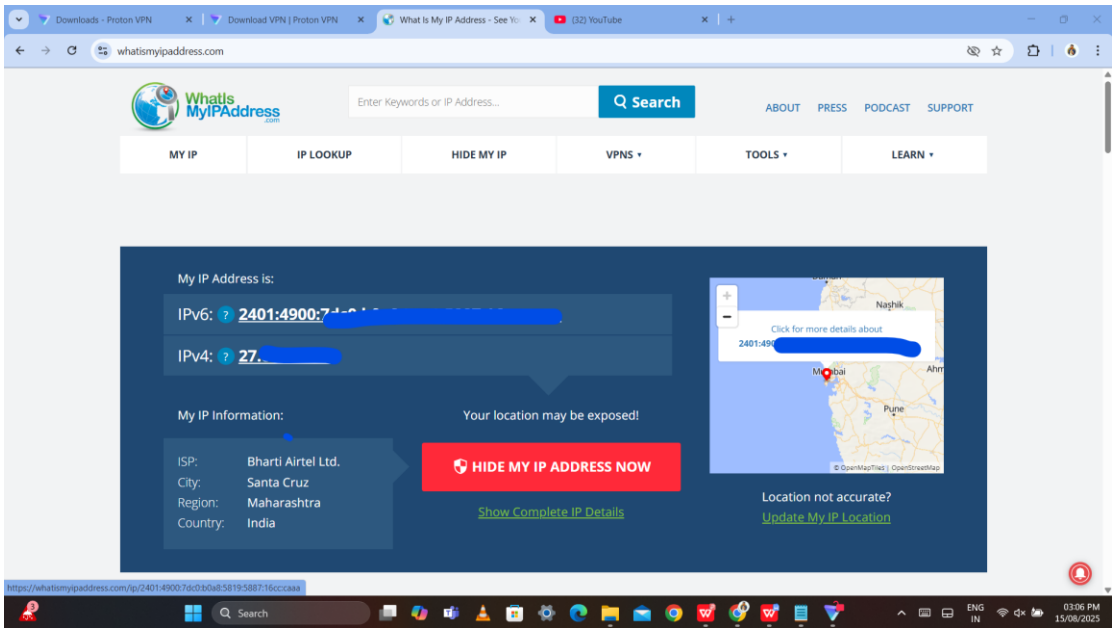
(Its routed through netherlands VPN server.)



Disconnected VPN and compared browsing speed, IP address, and location.

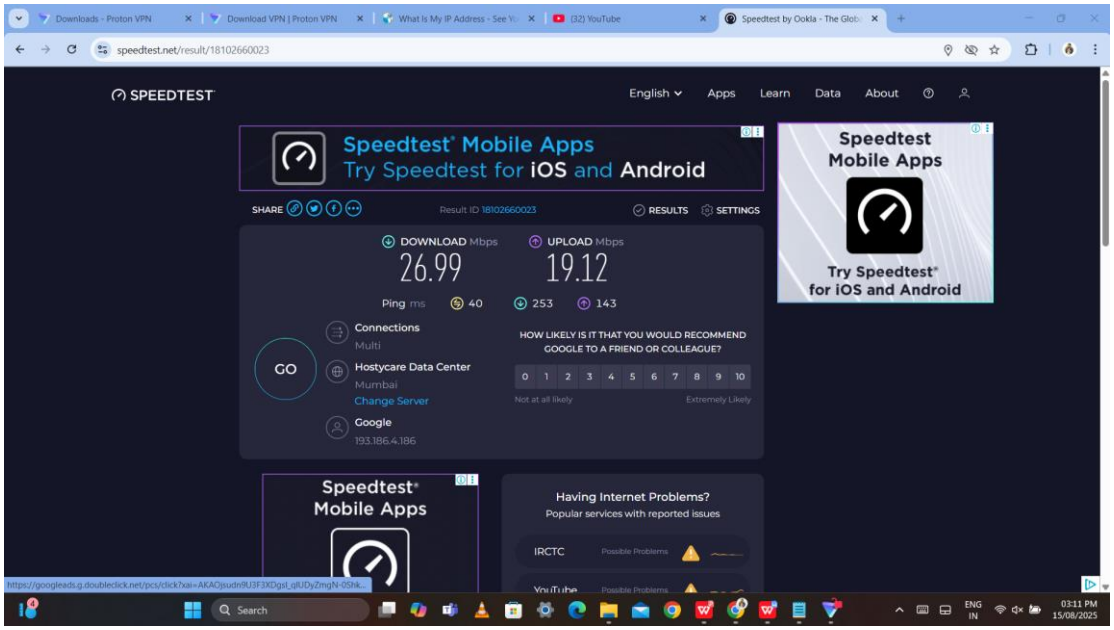


IP address after disconnecting VPN Server

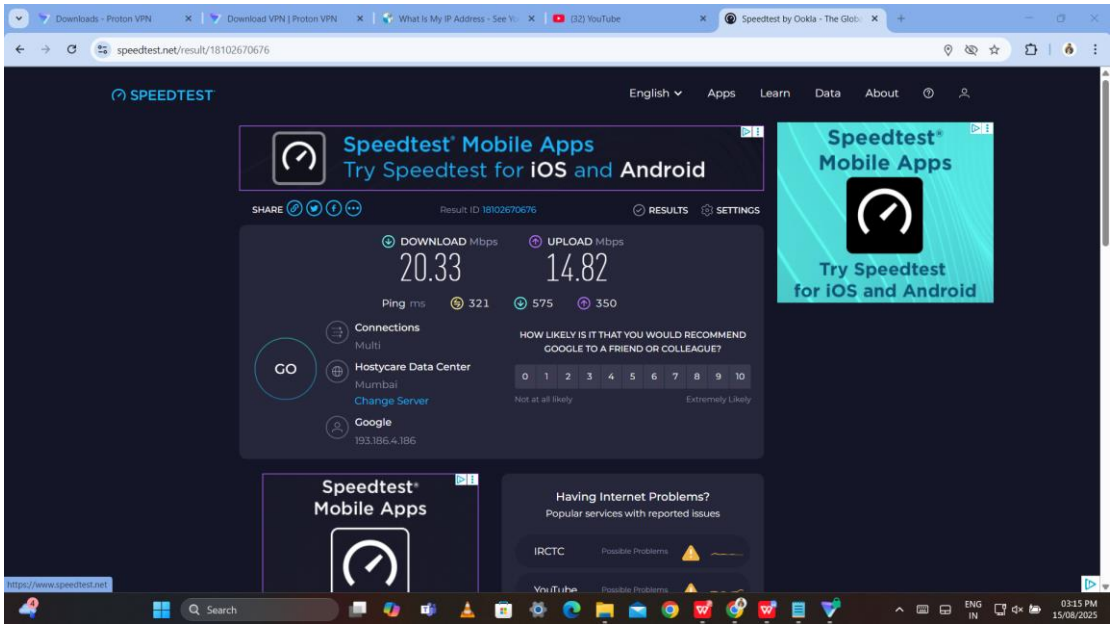


Internet Speed after disconnecting VPN Server vs Connecting VPN server

1. Without VPN server



2. With VPN server



Getting low speed if we connected to VPN server.

Research on VPN Encryption & Privacy

Learned that ProtonVPN uses AES-256 encryption, OpenVPN, and WireGuard protocols to secure traffic.

ProtonVPN is a security-focused VPN service developed by the same team behind ProtonMail in Switzerland, a country known for strong privacy laws. It emphasizes both encryption strength and user privacy.

Encryption Standard

- AES-256-bit encryption

- Considered military-grade encryption.

- Resistant to brute-force attacks with current technology.

- 256-bit key length means 2^{256} possible combinations, which is computationally unbreakable.

Tunneling Protocols

- OpenVPN (TCP & UDP) – An open-source, highly secure protocol that balances speed and security.

- IKEv2/IPSec – Often used for mobile devices due to fast reconnections during network changes.

- WireGuard (in beta) – Lightweight, faster protocol with modern cryptography.

Key Privacy Features

- Perfect Forward Secrecy (PFS)

- Ensures that even if an encryption key is compromised in the future, past session data cannot be decrypted.

- Uses ephemeral session keys that change regularly.

- Secure Core Servers

- Routes traffic through multiple servers in privacy-friendly countries before exiting to the internet.

- Example: Your connection might first go through Iceland, then Switzerland, before reaching the target site.

- No-Logs Policy

- ProtonVPN does not log browsing activity, IP addresses, or session data.

- Independent audits have verified its privacy claims.

- DNS Leak Protection

- All DNS requests are routed through the encrypted tunnel, preventing exposure to ISPs.

- Kill Switch & Always-On VPN

- Automatically blocks internet traffic if VPN connection drops, preventing accidental IP leaks.

Summary on VPN benefits and limitations

Benefits of Using a VPN

1. Enhanced Privacy – Masks your real IP address and location, making it harder for websites, ISPs, or hackers to track you.
2. Data Encryption – Uses strong encryption (e.g., AES-256) to secure your internet traffic from eavesdropping, especially on public Wi-Fi.
3. Bypass Geo-Restrictions – Allows access to websites, streaming services, and content blocked in your region.
4. Protection on Public Networks – Prevents Man-in-the-Middle (MITM) attacks when using unsecured hotspots.
5. Avoid ISP Throttling – Hides your online activity so ISPs cannot slow down certain types of traffic (e.g., streaming).

Limitations of Using a VPN

1. Reduced Speed – Encryption and routing through distant servers can cause slower internet performance.
2. Not Complete Anonymity – VPN providers can still log connection data unless they follow a strict no-logs policy.
3. Service Blocking – Some websites and streaming platforms actively block known VPN IP addresses.
4. Legal & Policy Restrictions – VPN usage is restricted or illegal in certain countries.
5. Limited Features in Free Plans – Lower speeds, fewer server locations, and data caps compared to premium versions.

Limitations in Free Version

- Limited to 3 countries: Netherlands, Japan, and the United States.

- Lower speed compared to paid tiers due to server congestion.

- No P2P or Secure Core servers on the free plan.

Real-World Usage Notes

- Encryption overhead may slightly reduce browsing speed.

- While it hides IP address and encrypts traffic, it cannot prevent tracking via cookies, fingerprinting, or logged-in accounts.

- Works well for bypassing censorship and accessing restricted content in some regions.