Task 8 : Working with VPN's

VPN stands for **Virtual Private Network**. It is a service that creates a secure, encrypted connection between your device (computer, phone) and the internet.

Purpose of VPN:

1. **Privacy:** Hides your IP address and online activities from ISPs, hackers, or third parties.
2. **Security:** Encrypts your internet traffic so data can't be intercepted.
3. **Access Control:** Lets you access region-restricted websites or bypass censorship.
4. **Safe Public Wi-Fi:** Protects your data on unsecured networks.

How VPN Works (Simplified)?:

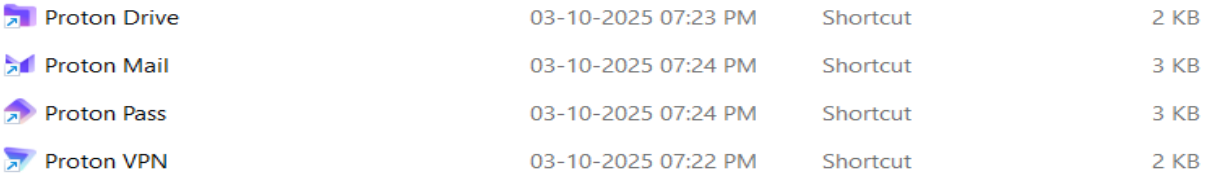
- Your device connects to a **VPN server**.
- All your internet traffic goes through this server.
- The server masks your real IP address and encrypts data.
- Websites see the VPN server's IP instead of yours.

Step A: Checking OS

- Open **Settings → System → About** or run winver in PowerShell

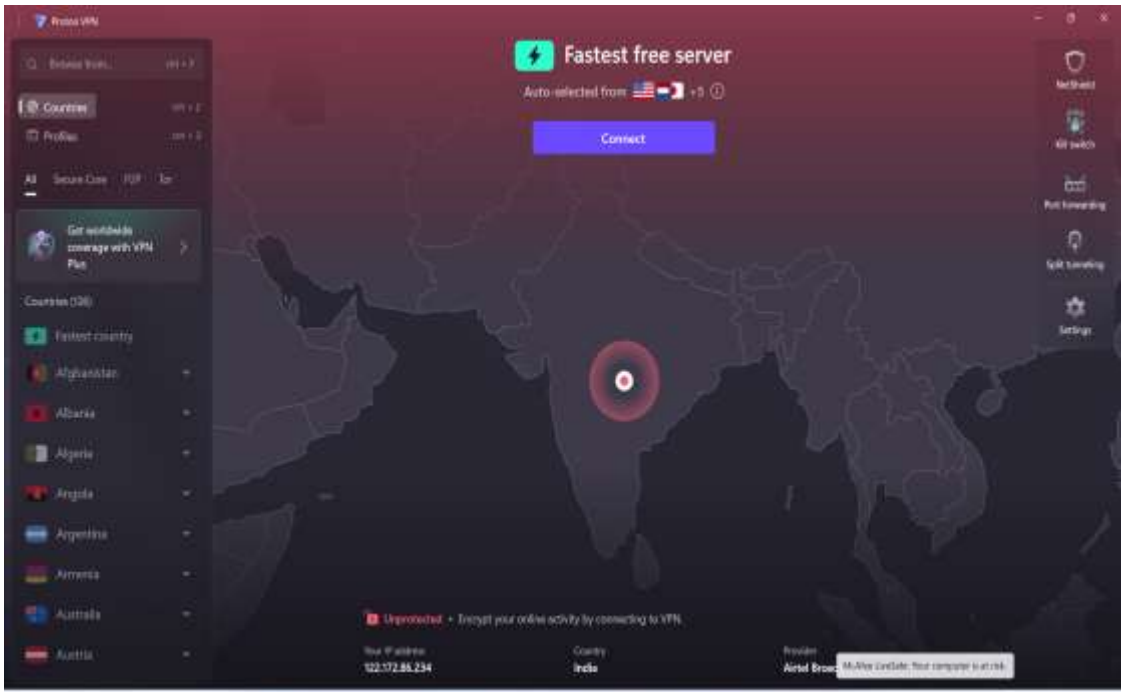
Step B: Install VPN

- Download VPN software (ProtonVPN, .).
- Run the installer and follow prompts.
- **Screenshot**: Installation completed page.



Step C: Configure VPN

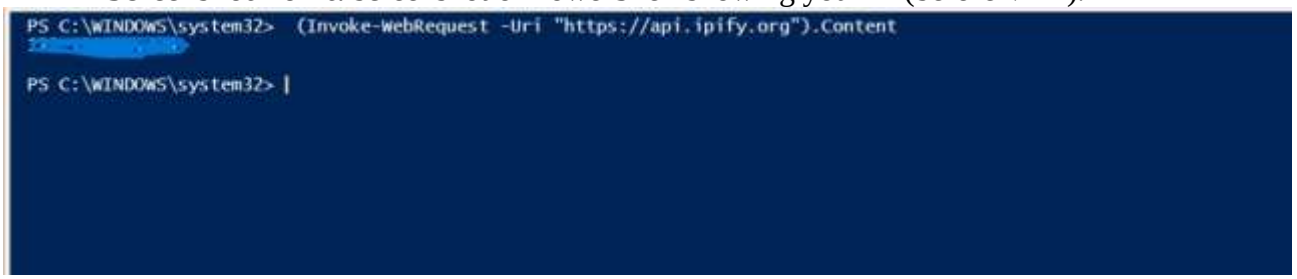
- Open VPN client.
- Sign in with credentials.
- Before connecting it is unprotected.
- **Screenshot**: VPN server selection page.


Fastest free server
Auto-selected from
Connect
Countries
Profiles
All
Secure Core
P2P
Tor
Countries (126)
Fastest country
Afghanistan
Albania
Algeria
Angola
Argentina
Armenia
Australia
Austria
Unprotected • Encrypt your online activity by connecting to VPN
122.172.86.234
India
Airtel Broa
NetShield
Kill switch
Port forwarding
Split tunneling
Settings

Action 1 – Check IP Before VPN

1. Open **PowerShell (Run as Administrator)**.
2. Run this command: (Invoke-WebRequest -Uri "https://api.ipify.org").Content
3. Note down the IP shown.

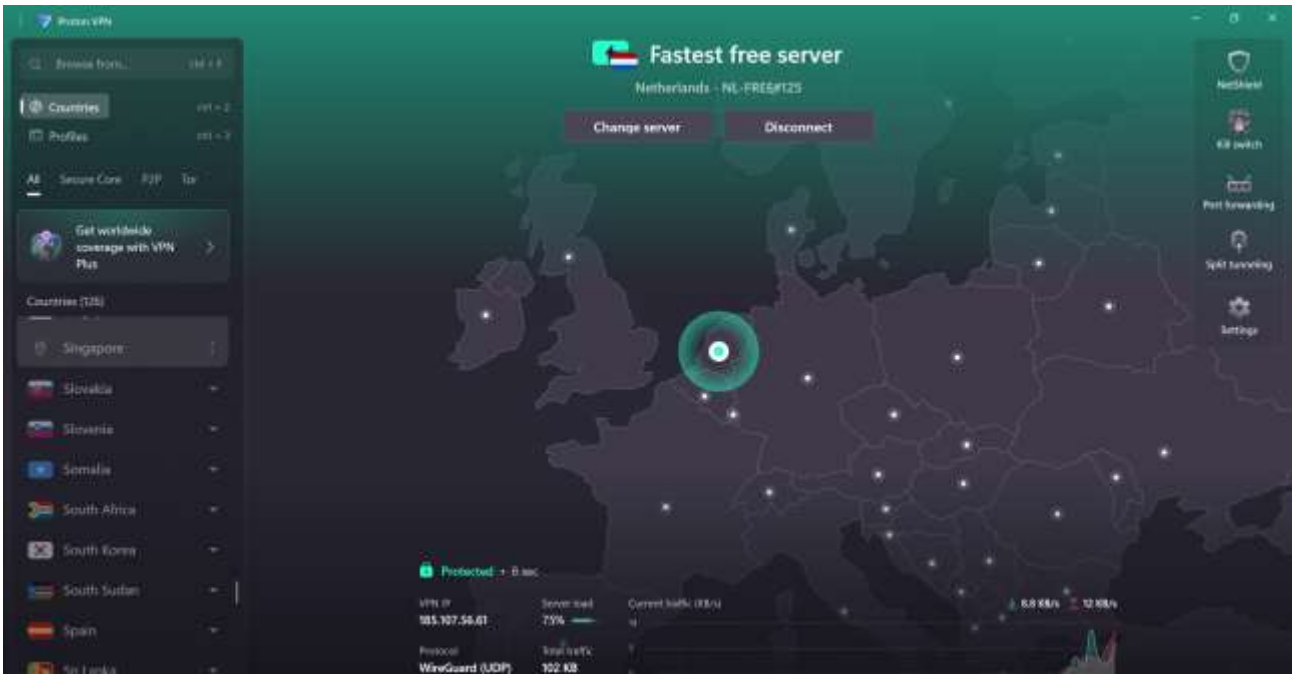
Screenshot Point: screenshot of PowerShell showing your IP (before VPN).



Action 2 – Connect to VPN

1. Open ProtonVPN (or whichever VPN you installed).
2. Log in and connect to a **Free Server** (e.g., US, Germany, Singapore).
3. As of mine connected to Singapore and the IP address is also protected.
4. And if we can also change the server and also disconnect the present sever connection.

Screenshot Point: screenshot of VPN app after VPN connection.



Action 3 – Check IP After VPN

1. While VPN is connected, go back to **PowerShell**.
2. Run the same command again:

   (Invoke-WebRequest -Uri "https://api.ipify.org").Content
3. Compare the result with the “Before VPN” IP.

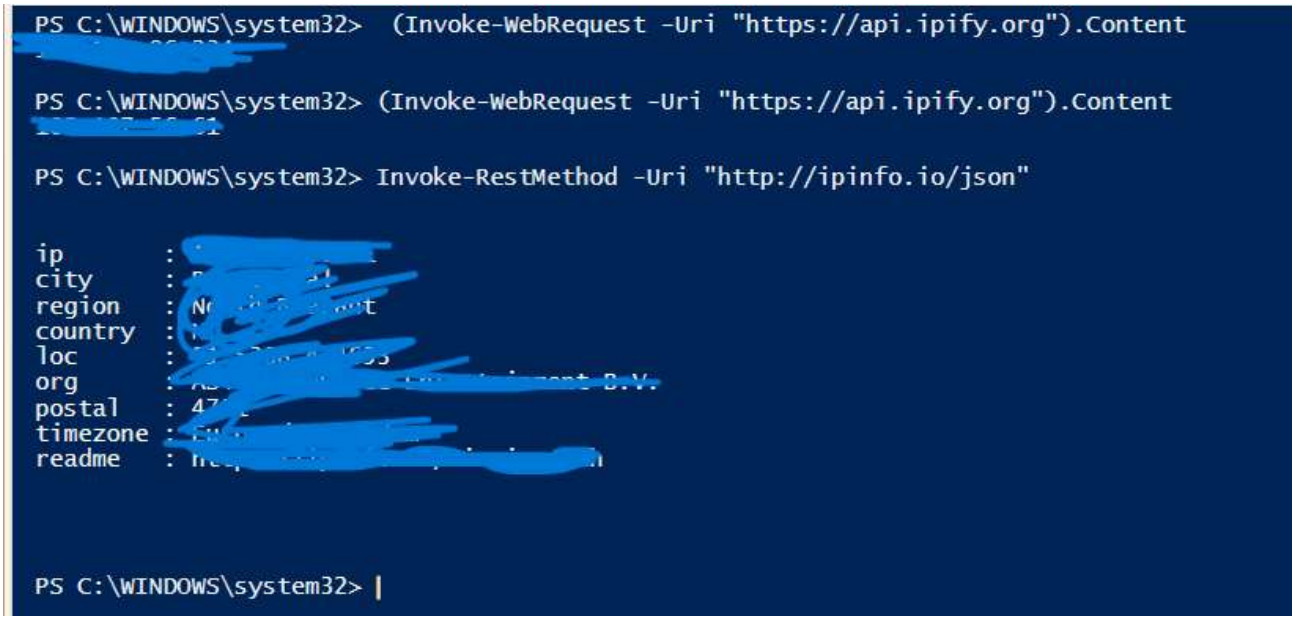
   IP should be **different** (belonging to the VPN server location).
4. For location information of my IP

   Run the command :

   Invoke-RestMethod -Uri "http://ipinfo.io/json"

   It shows details like IP, City, Country, ISP

   Screenshot Point: screenshot of new IP after VPN connection and location information.



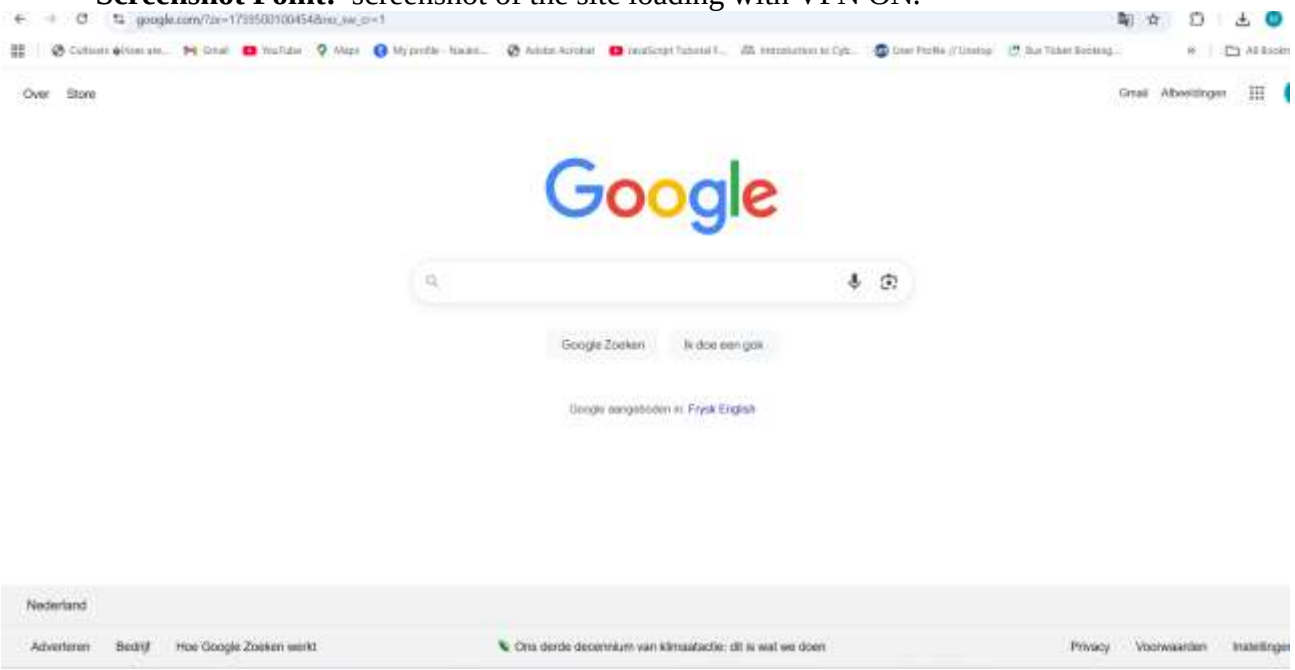
Step D: Browse Securely

Action 1 – Open a Website

1. While VPN is ON, open your browser.
2. Visit a website :https://www.google.com

- **Website loads normally (encrypted traffic).**

Screenshot Point: screenshot of the site loading with VPN ON.



Action 2 – Compare Speed

1. Disconnect VPN → reload the same website.
2. Notice that the site loads slightly faster without VPN.

- **With VPN: Works, but may be a bit slower.**
- **Without VPN: Faster (no encryption overhead).**