**Task 8: Working and Understanding VPN**

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

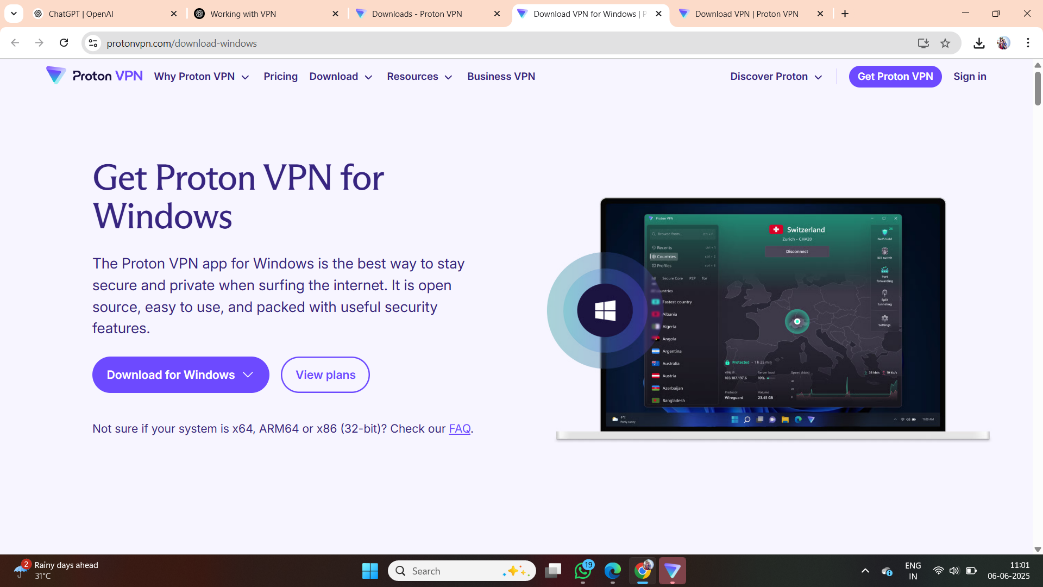
**Tools:** Free VPN client (ProtonVPN free tier, Windscribe free)

**Deliverables**: Report describing VPN setup steps and connection status screenshot.

**Step 1: Choose a Reputable Free VPN Service and Sign Up**

🔹 **What to Do:**

* Visit a trusted VPN provider website:
  + [ProtonVPN Free Tier](https://protonvpn.com/free-vpn)
  + [Windscribe Free VPN](https://windscribe.com/)



🔹 **Why:**

* Trusted services offer secure encryption, good speed, and a no-logs policy—important for privacy.

🔹 **Action:**

* Click **Sign Up**, enter your email, and confirm registration via the email link.

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

🔹 **What to Do:**

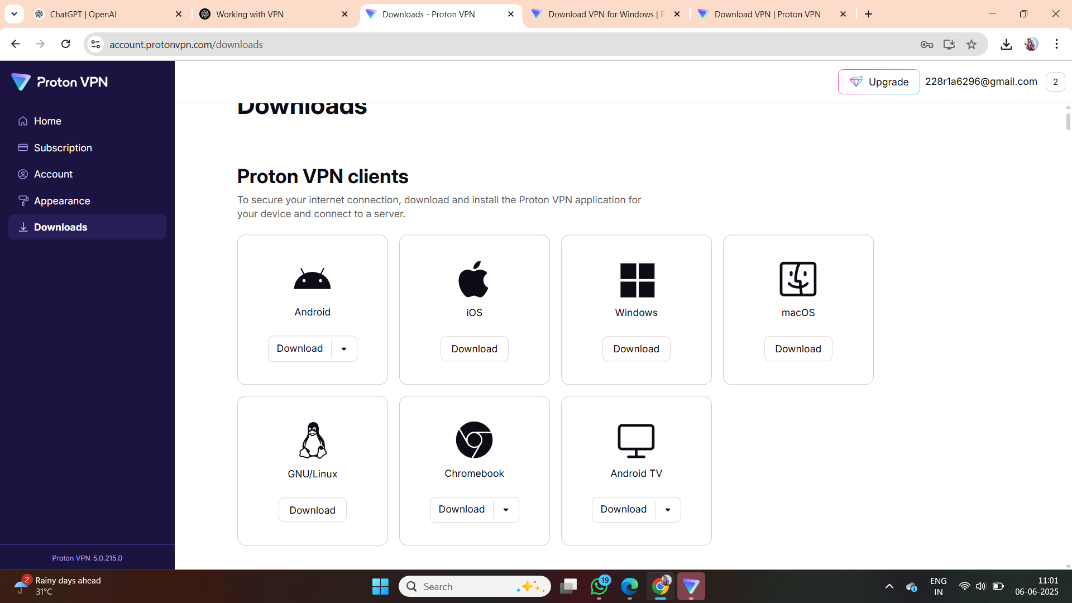
* After signing up, download the VPN app for your device (Windows, macOS, Linux, Android, or iOS).

🔹 **Why:**

* The VPN client is the software that lets you easily connect to VPN servers.

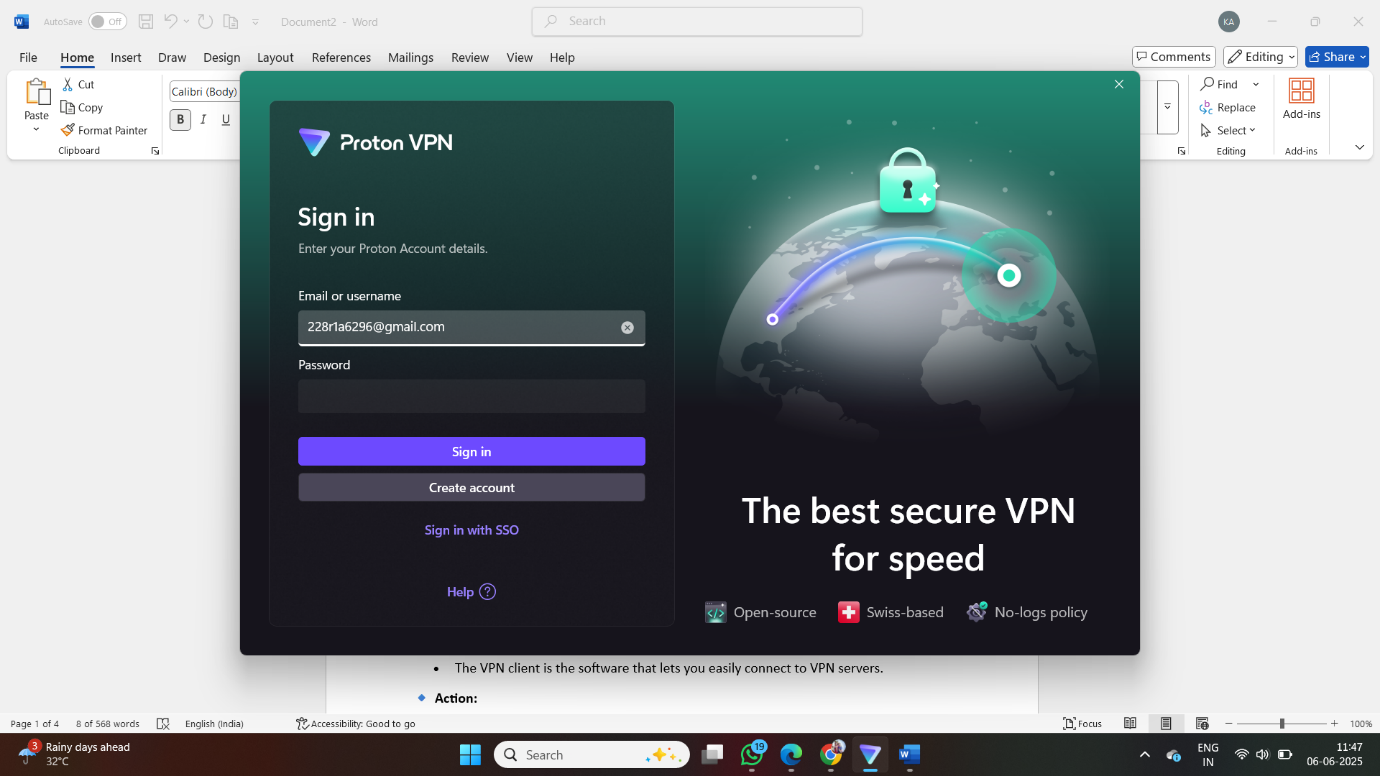
🔹 **Action:**

* Open the installer and follow on-screen instructions to install the VPN client.



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

🔹 **What to Do:**

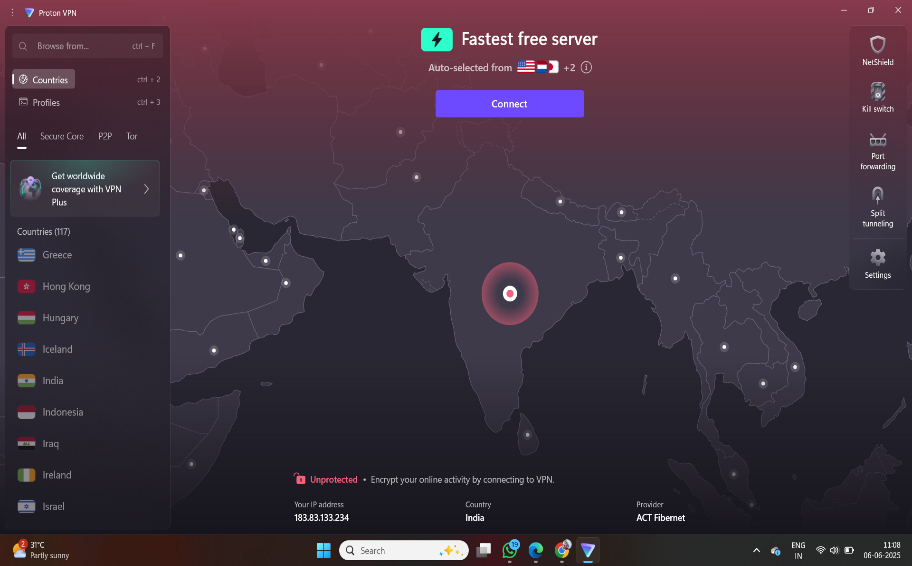
* Launch the VPN app and log in using the credentials you created earlier.
* 

🔹 **Why:**

* You need to connect to a remote VPN server to start encrypting your traffic.

🔹 **Action:**

* Choose a server location (e.g., India, US, or the closest available).
* Click **Connect**. Once connected, the app will show “Connected” or a green shield icon.



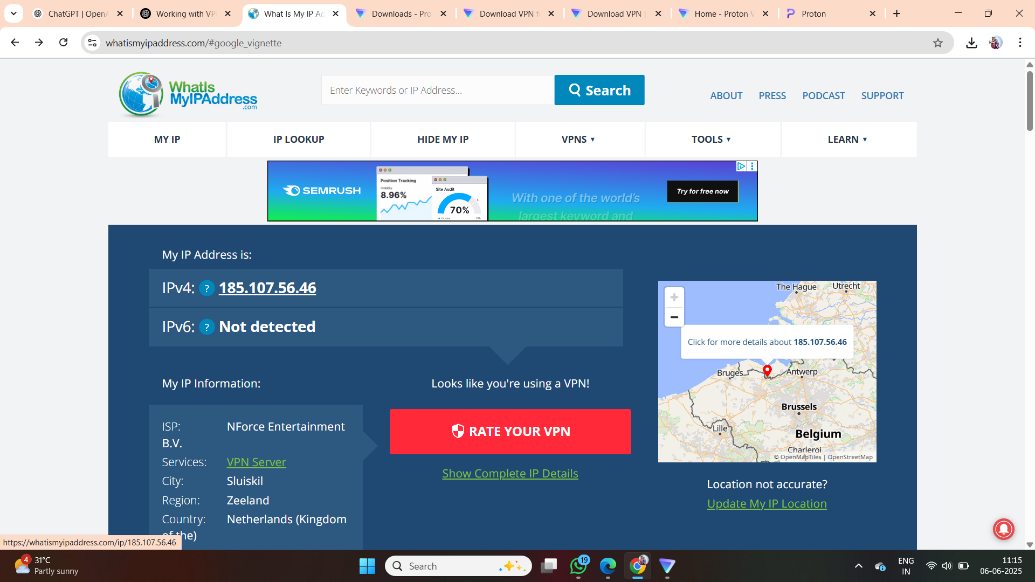
**Step 4: Verify Your IP Address Has Changed**

🔹 **What to Do:**

* Open your browser and go to [https://whatismyipaddress.com](https://whatismyipaddress.com/).

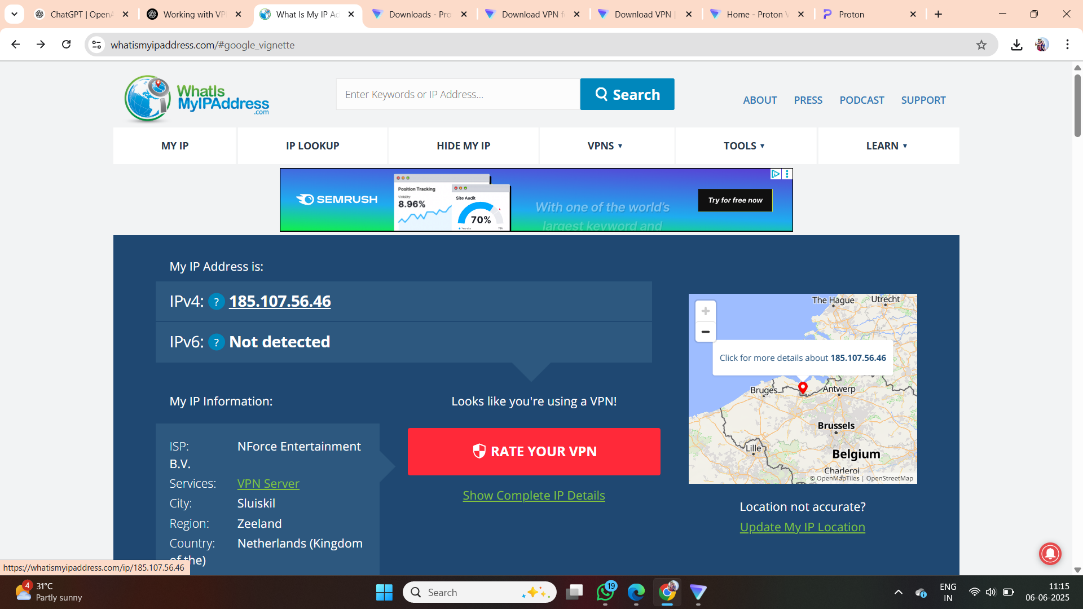
🔹 **Why:**

* This site shows your public IP address and location.
* Checking this before and after connecting proves the VPN is working.



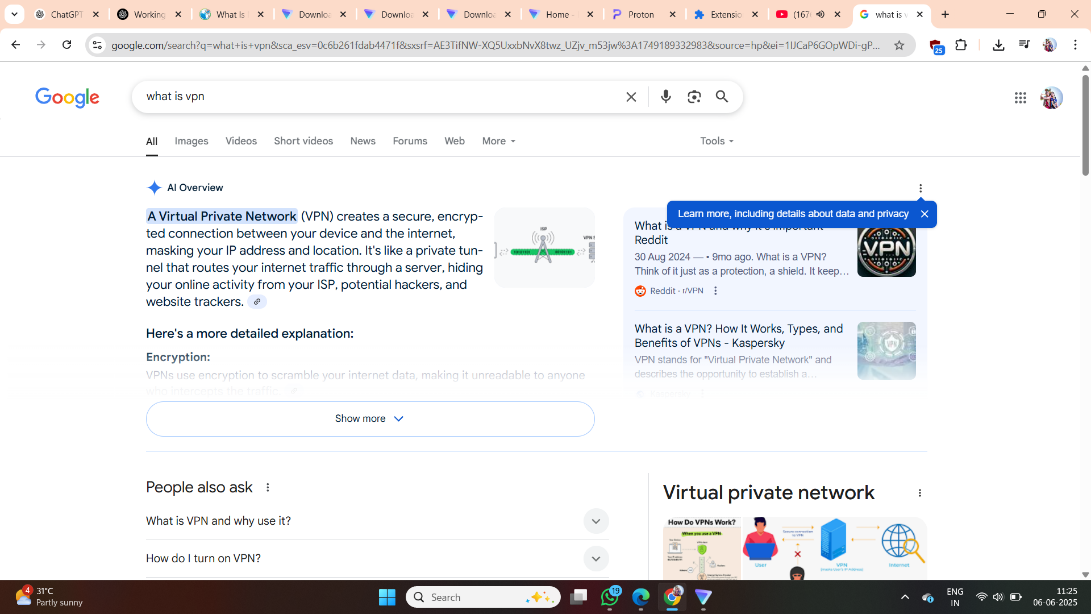
🔹 **Action:**

* Note down your IP before connecting.
* After connecting, refresh the page—your IP and location should now match the VPN server.



**Step 5: Browse a Website to Confirm Traffic Is Encrypted**

🔹 **What to Do:**

* While still connected to the VPN, open websites like:
  + Google.com
  + YouTube.com
  + Your bank or government site
* 

🔹 **Why:**

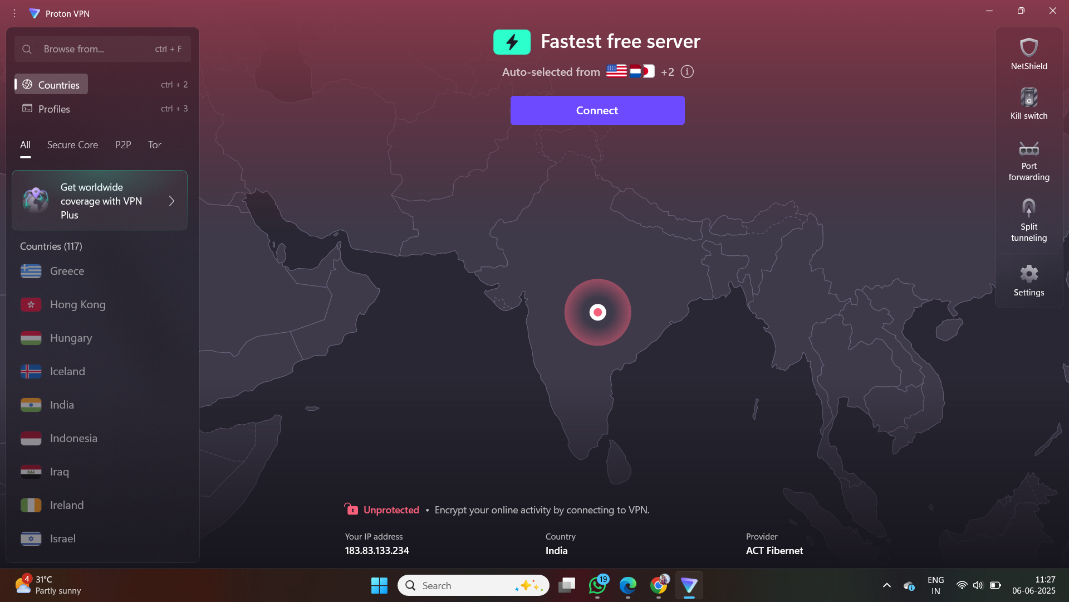
* To confirm that you can access websites as normal and the traffic is routed through the VPN tunnel.

🔹 **Action:**

* If websites load without issues, your connection is encrypted and secure.

**Step 6: Disconnect VPN and Compare Browsing Speed and IP**

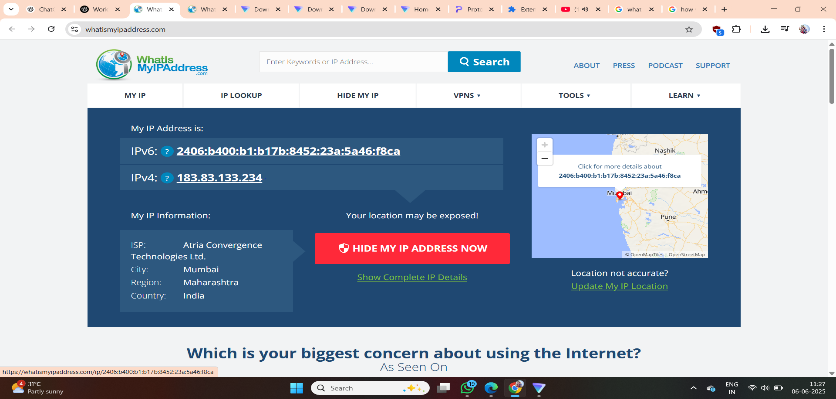
🔹 **What to Do:**

* In the VPN app, click **Disconnect**.
* 

🔹 **Why:**

* To see how VPN affects browsing performance and to confirm that your real IP is restored.

🔹 **Action:**

* Go back to [https://whatismyipaddress.com](https://whatismyipaddress.com/) and check your real IP.
* Try loading a few sites again to compare speed before and after VPN.
* 

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

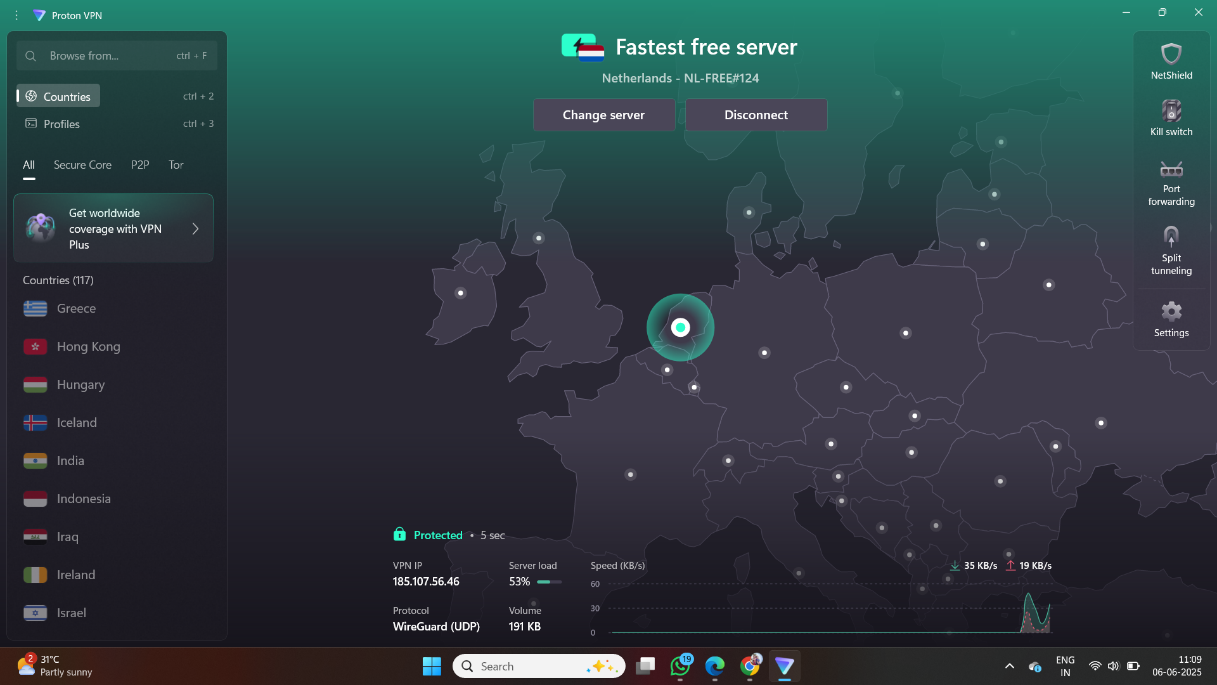
🔹 **What to Do:**

* Google search or read articles about:
  + VPN encryption protocols (OpenVPN, WireGuard, IKEv2)
  + VPN features like kill switch, no-log policy, DNS leak protection
  + Article:- https://levelblue.com/blogs/security-essentials/the-ultimate-guide-to-vpn-encryption-protocols-and-ciphers

🔹 **Why:**

* To understand what makes a VPN secure or not. Knowing this helps you choose better VPNs.

🔹 **Action:**

* Note down 2–3 key features from the VPN you used and what encryption protocol it supports.
* 

**Step 8: Write a Summary on VPN Benefits and Limitations**

**✅ VPN Benefits:**

* Online Privacy Protection
* VPN hides your real IP address, making it difficult for websites, advertisers, and governments to track your online activity.
* Encrypted Internet Traffic
* All data sent and received is encrypted, which secures your connection on public Wi-Fi or untrusted networks.
* Bypass Geo-Restrictions
* Allows access to blocked or region-restricted content (e.g., websites, streaming platforms like Netflix or YouTube in other countries).
* Secure Remote Access
* Useful for remote workers to safely connect to office networks or resources over the internet.
* Avoid ISP Tracking and Throttling
* ISPs can’t monitor or slow down your traffic when you're using a VPN.

**⚠️ VPN Limitations:**

* Reduced Internet Speed
* Encryption and routing traffic through remote servers can slow down browsing and download speeds.
* Free VPN Risks
* Free VPNs often have data limits, limited server locations, and may log your activity or show ads.
* Not a Complete Security Solution
* VPNs do not protect against phishing, malware, or unsafe websites—antivirus and safe browsing habits are still needed.
* Legal and Policy Risks
* In some countries, using a VPN is restricted or illegal. Also, some websites block known VPN IP addresses.
* Trust in VPN Provider
* You must trust the VPN service to follow its no-log policy and not misuse your data.

**Conclusion: Working and Understanding VPN**

I gained practical experience in setting up and using a Virtual Private Network (VPN). By installing a trusted free VPN client (such as ProtonVPN or Windscribe), I successfully connected to a remote server, verified my IP address had changed, and confirmed that my internet traffic was encrypted.

This task helped me understand how VPNs enhance online privacy, secure communication, and protect users on public or untrusted networks. I also learned about encryption protocols like OpenVPN and WireGuard, and the importance of choosing a VPN provider with a strict no-logs policy.

While VPNs offer strong privacy benefits, they also have limitations such as slower internet speeds, limited free features, and the need to trust the VPN provider. Despite these, VPNs remain a crucial tool in today’s digital world for safer and more private browsing.

Overall, this task improved my technical knowledge and practical skills in using privacy tools effectively.