Task 8: VPN Setup and Privacy Analysis using ProtonVPN

Objective

The main goal of this task was to learn how a VPN helps in protecting our privacy and securing our internet connection. I used **ProtonVPN (Free Version)** to understand how it hides our IP address, encrypts data, and keeps browsing safe from tracking or hacking.

Step 1: Choosing a VPN Service

For this task, I decided to use **ProtonVPN** because it's one of the most trusted free VPNs available.
I chose it because:

- It's developed by the same team behind **ProtonMail**, which is known for privacy.
- It uses **strong AES-256 encryption** to protect data.
- It has a **no-log policy**, meaning it doesn't store our browsing history.
- The free version doesn't have any data limit, which is a big advantage.

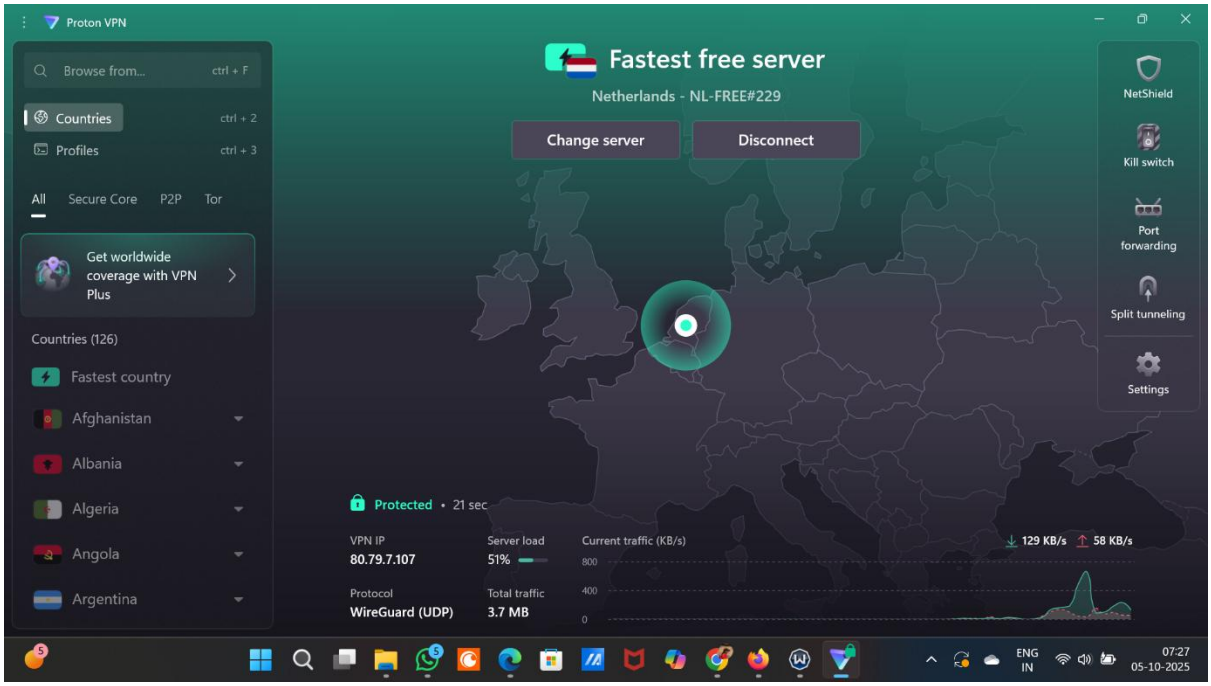
Step 2: Download and Installation

- I went to the official **ProtonVPN website** and signed up for a free account using my email.Then I downloaded the VPN client for Windows and installed it by following the setup instructions.
  After installation, I logged into the ProtonVPN app with my account credential.

Step 3: Connecting to a VPN Server

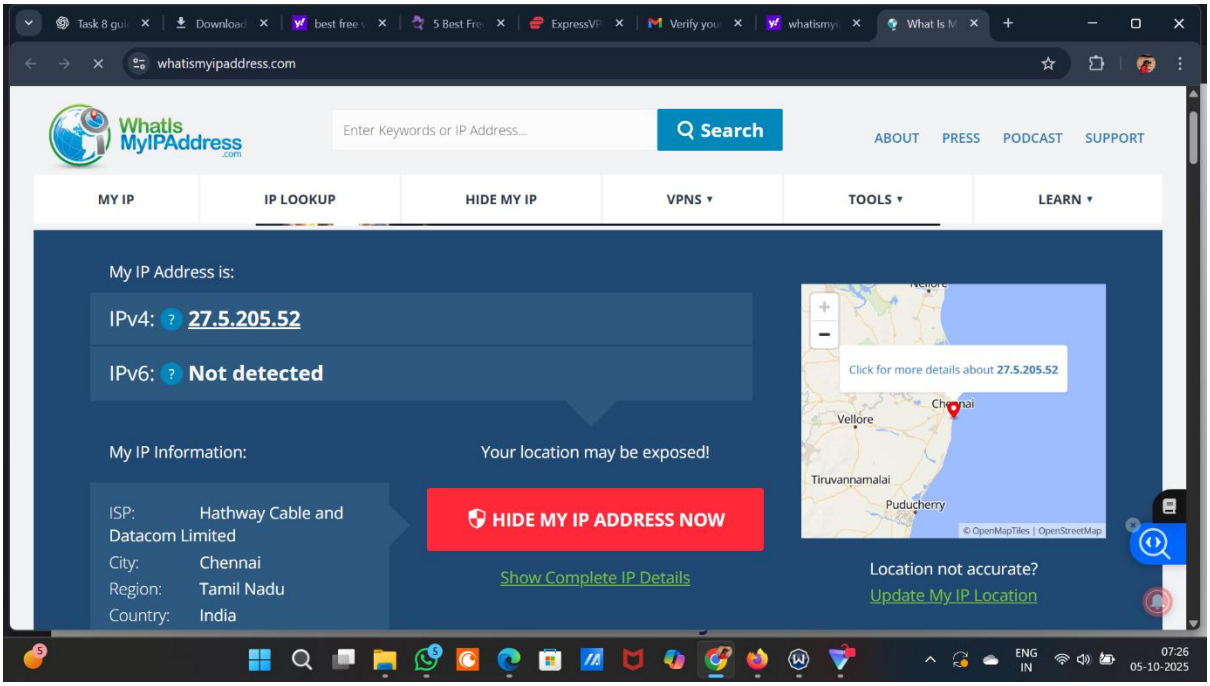
- Once logged in, I clicked on the **"Quick Connect"** button.
  The VPN automatically connected me to the nearest available server for better speed and performance.
  After connecting, the app showed a new IP address and the country I was connected to, which confirmed that the VPN was working.

Here I added a screenshot showing the VPN connected successfully

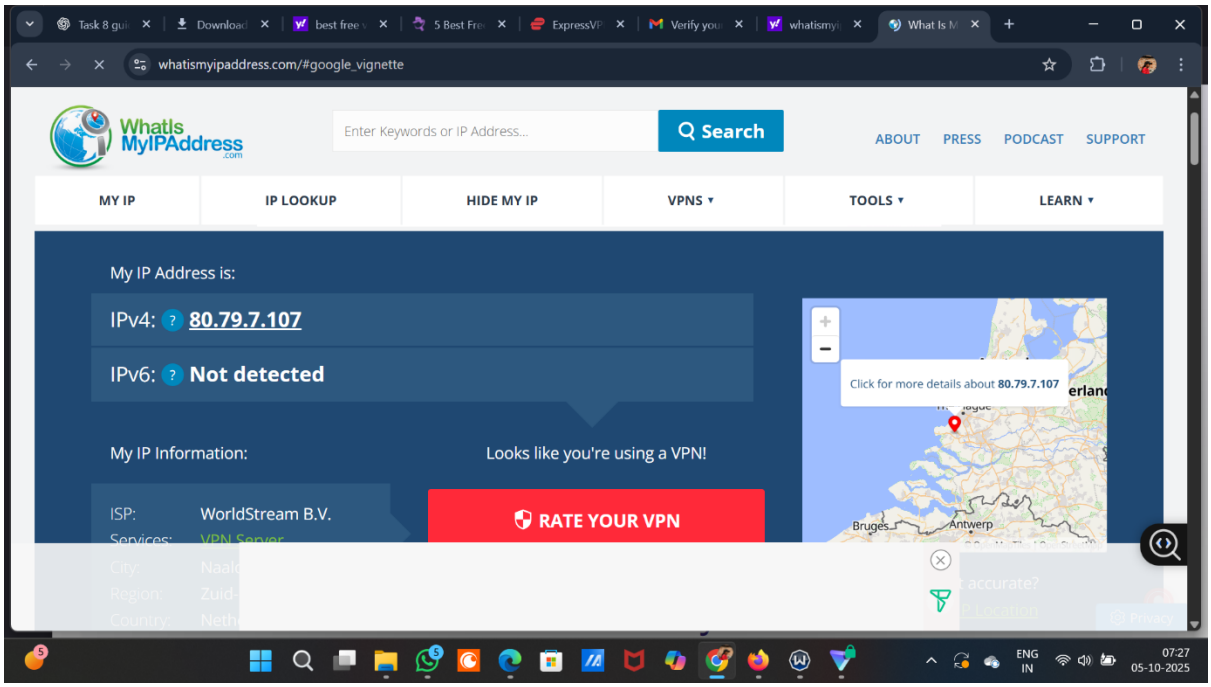


Step 4: Checking My IP Address

- Before connecting to the VPN, I visited **whatismyipaddress.com** to note down my original IP and location.



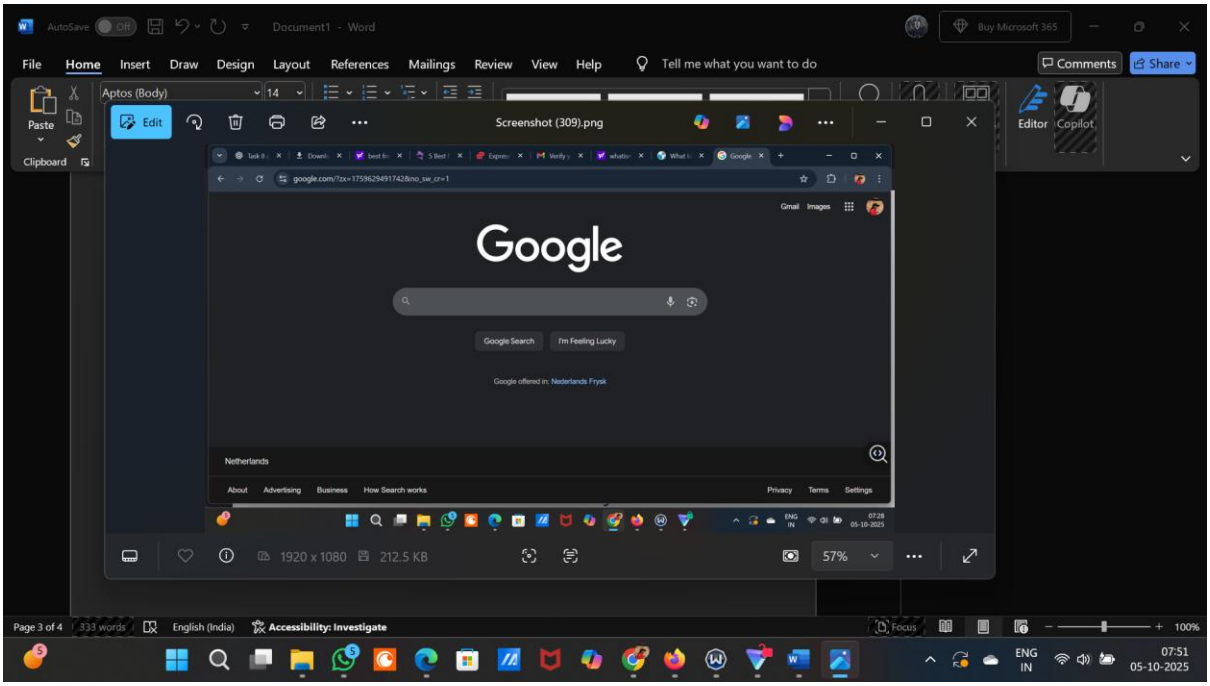
- After connecting to ProtonVPN, I refreshed the page, and my IP address and location had changed.



- This confirmed that all my traffic was now going through a secure ProtonVPN server.

Step 5: Testing Encrypted Browsing

- To check if everything was working fine, I opened websites like Google
- All sites loaded normally without any issue.
- This showed that my internet connection was encrypted and running safely through the VPN.



Step 6: Disconnecting and Comparing

After that, I disconnected the VPN and checked my IP again — it changed back to my real one.
I also noticed a small difference in browsing speed:

- With VPN: Slightly slower (because data is encrypted and sent through another server).
- Without VPN: Normal speed.
  This small speed drop is normal for most VPNs.

Step 7: Learning About VPN Security

While researching more about ProtonVPN, I learned some interesting technical details:

- It uses **AES-256-bit encryption**, one of the strongest in the world.
- It supports **OpenVPN** and **WireGuard protocols** for secure connections.
- It has a **Kill Switch** feature, which stops traffic if the VPN suddenly disconnects.
- It also prevents **DNS leaks**, meaning my real IP remains hidden at all times.

Step 8: VPN Benefits and Limitations

Benefits:

- Hides my real IP and location.
- Encrypts my browsing data for privacy.
- Keeps me safe when using public Wi-Fi.
- Helps access blocked or restricted websites.
- Prevents online tracking by websites or ISPs.

Limitations:

- Slightly reduces internet speed.
- Limited free servers in the free plan.
- Not 100% anonymous (the VPN company still manages the servers).
- Some websites or streaming services may block VPN access.

Outcome

- After completing this task, I understood how a VPN actually works in real time.
- I learned how to set it up, verify IP changes, and test encrypted browsing.
- Using ProtonVPN gave me hands-on experience with privacy tools and how they protect data online.
- Overall, this task helped me understand how VPNs enhance privacy and why encryption is so important in cybersecurity.