# Working and Understanding VPN

## Objective:

To understand the working of VPNs and how they protect user privacy and secure communication.

## VPN Used:

ProtonVPN (Free Tier)

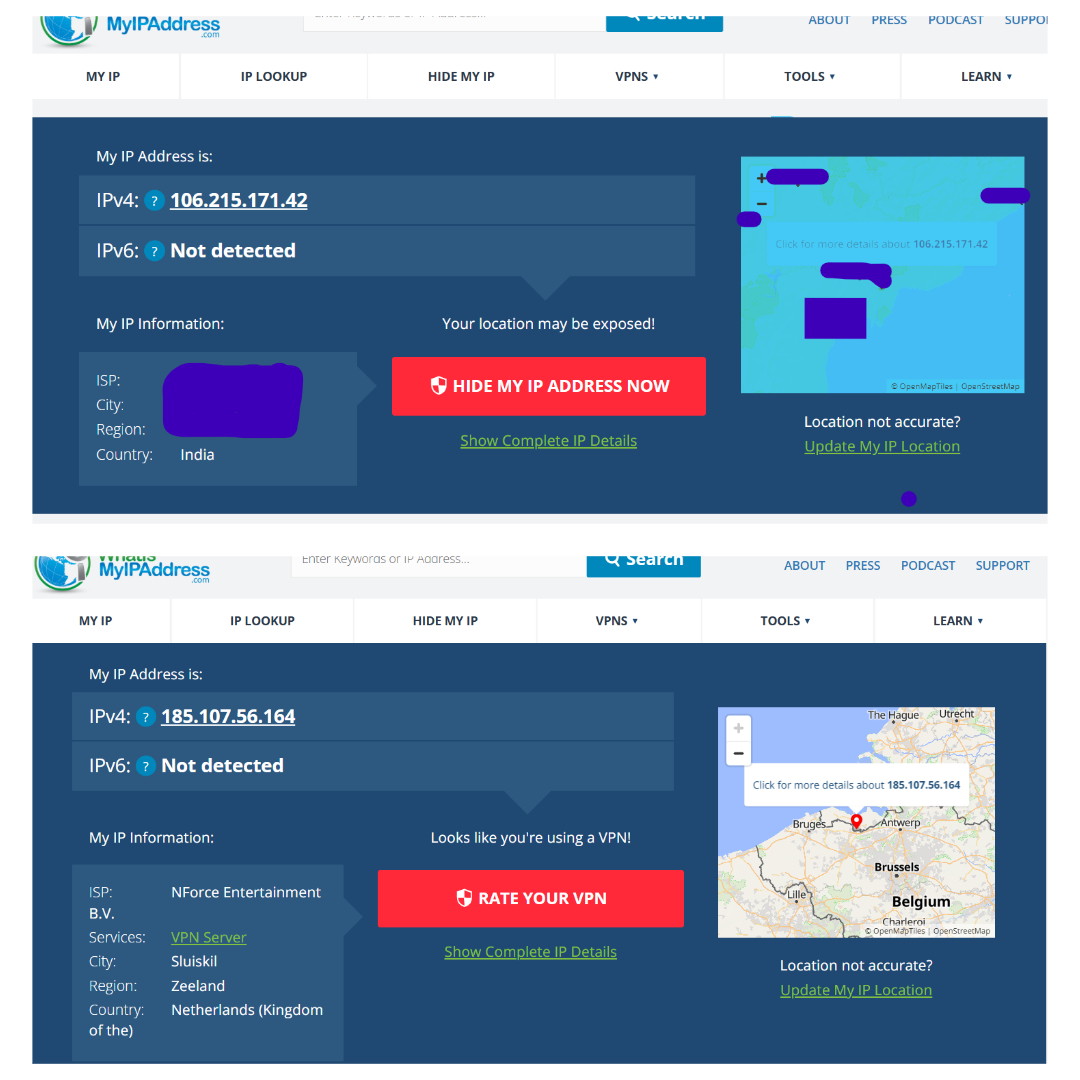
## Setup Process:

1. Signed up at “https://protonvpn.com”
2. Installed the VPN client on Windows.
3. Connected to a Netherlands-based VPN server.
4. Verified IP address before and after connection.

|  |  |  |
| --- | --- | --- |
| **State** | **IP Address** | **Location** |
| Before | 106.215.171.42 | India |
| After | 185.107.56.164 | Netherlands |

1. Confirmed traffic encryption (visited websites used HTTPS).
2. Browsing speed was slightly slower after VPN connection.
3. Disconnected VPN and noticed IP reverted to original.

Before VPN



After VPN

## VPN Encryption and Privacy Features:

VPNs (Virtual Private Networks) use a combination of encryption protocols and privacy techniques to ensure secure and anonymous internet usage. Some key features include:

* **Encryption Protocols:**  
  Most VPNs use advanced encryption standards like **AES-256**, which is considered military-grade encryption. Protocols such as **OpenVPN**, **WireGuard**, and **IKEv2/IPSec** ensure that data traveling through the VPN tunnel is encrypted and unreadable to outsiders.
* **No-Log Policy:**  
  A strict no-log policy means the VPN provider does **not store records** of your browsing activity, connection timestamps, or IP addresses—protecting your online privacy even from the VPN provider itself.
* **Kill Switch:**  
  A kill switch automatically disconnects your internet if the VPN connection drops, ensuring your IP address and data are never exposed.
* **DNS Leak Protection:**  
  This prevents DNS requests from bypassing the VPN tunnel, ensuring all web activity is securely routed through the VPN without revealing the sites you visit.
* **Multi-hop Servers:**  
  Some advanced VPNs route your connection through multiple servers in different countries, adding extra layers of encryption and anonymity.

## Benefits of using a VPN:

* **Privacy Protection:** Hides your IP address and encrypts data, keeping your online identity and activity private.
* **Secure Public Wi-Fi Use:** Shields sensitive information (like passwords and card details) when using untrusted networks.
* **Bypass Censorship and Geo-blocks:** Lets you access content restricted to certain regions, such as streaming services or news websites.
* **Avoid Tracking:** Prevents websites, advertisers, and ISPs from tracking your behavior and collecting personal data.

## Limitations of using a VPN:

* **Reduced Internet Speed:** Encryption and routing through remote servers may slow down your connection.
* **Limited Free Features:** Free VPNs often restrict bandwidth, speed, or the number of available servers.
* **Trust Issues:** You must trust the VPN provider not to misuse or log your data (especially if it's a free service).
* **Not a Full Security Solution:** VPNs don’t protect against malware, phishing, or unsafe websites on their own.

## Summary

This task involved using ProtonVPN to understand how VPNs secure internet traffic and protect user privacy. I connected to a server in the Netherlands, verified IP address changes, and observed the impact on browsing speed. I also explored VPN features like encryption, kill switch, and DNS leak protection.