**Report: Understanding the Role of VPNs in Privacy and Secure Communication**

**By : Rohita B**

# Overview

In this report, we evaluate the functionality and benefits of using a VPN through practical setup and connection using **ProtonVPN** (Free Tier). Additionally, we analyze the changes in IP address, encryption verification, and explore the advantages and limitations of VPN use in everyday scenarios.

# Table of Content

1. Introduction
2. VPN Client Setup
   * Choosing the VPN Provider
   * Account Creation
   * Installation
3. Connecting to a VPN Server
   * Server Selection
   * Connection Status
4. Verifying IP and Encryption  IP Address Check
   * Secure Browsing Test
5. Performance and Comparison
   * With VPN Enabled
   * Without VPN
6. Research on VPN Encryption and Privacy
   * Encryption Standards
   * Privacy Features
7. VPN Benefits and Limitations
8. Conclusion

# 1. Introduction

A Virtual Private Network (VPN) is a technology that creates a secure, encrypted connection over a less secure network, such as the Internet. VPNs are primarily used to protect online identity, encrypt web traffic, and bypass geographic restrictions.

# 2. VPN Client Setup

## 2.1 Choosing the VPN Provider

After researching various free VPN services, I selected **ProtonVPN** for the following reasons:

* Strong reputation for privacy and security
* Based in Switzerland (strict privacy laws)
* No data logging policy
* Available free tier with no data limit

## 2.2 Account Creation

* Visited the official website: [https://protonvpn.com](https://protonvpn.com/)
* Signed up using an email address to create a free-tier account
* Confirmed the email and logged into the ProtonVPN dashboard

## 2.3 Installation

* Downloaded ProtonVPN for Windows from the official site
* Installed the VPN client using default installation options
* Logged into the ProtonVPN client with the account credentials

# 3. Connecting to a VPN Server

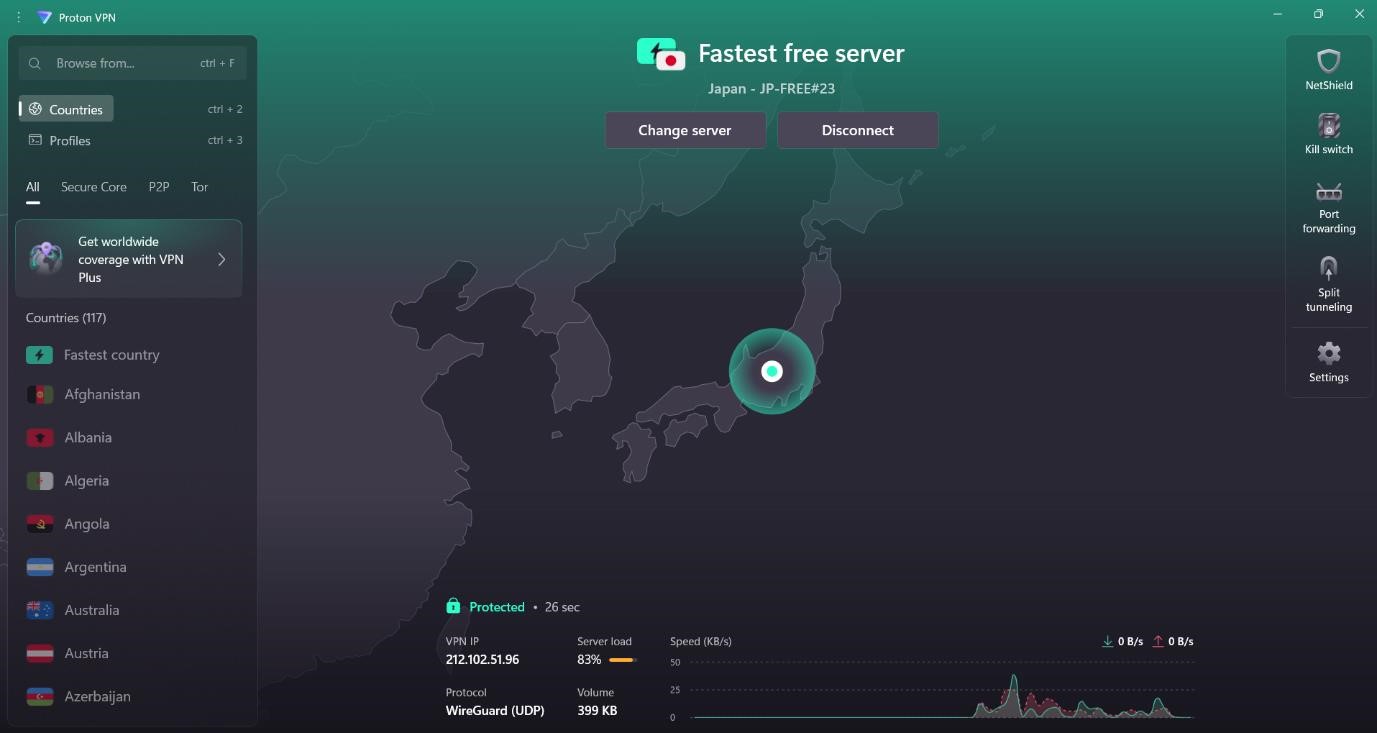
## 3.1 Server Selection

* Opened the ProtonVPN client and selected **“Quick Connect”**
* The app connected to a free server in **Netherlands** (based on best speed and availability)

## 3.2 Connection Status

Upon successful connection, the client displayed:

* Connection time
* Server name and country
* New assigned IP address **Screenshot:**



# 4. Verifying IP and Encryption

**4.1 IP Address Check**

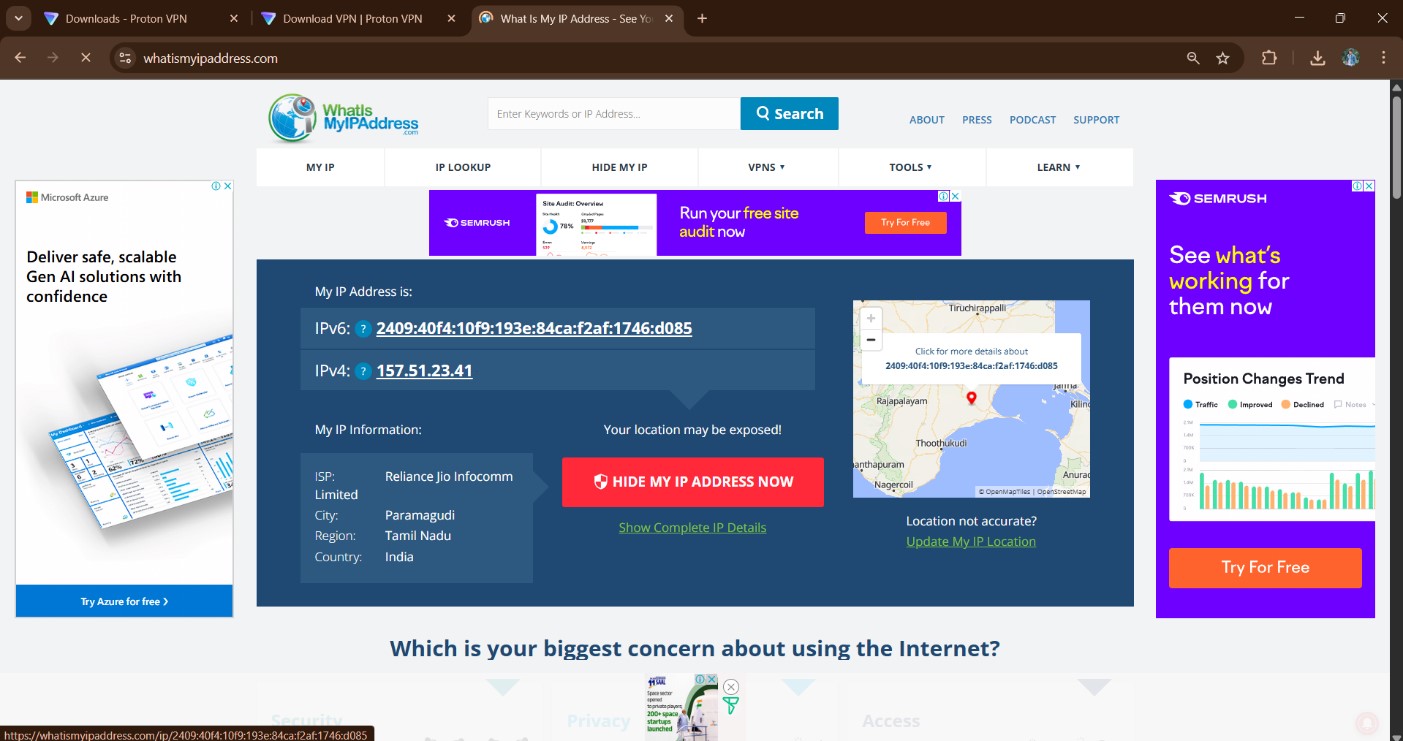
Used [https://whatismyipaddress.com](https://whatismyipaddress.com/) before and after enabling the VPN.

# State IP Address Location

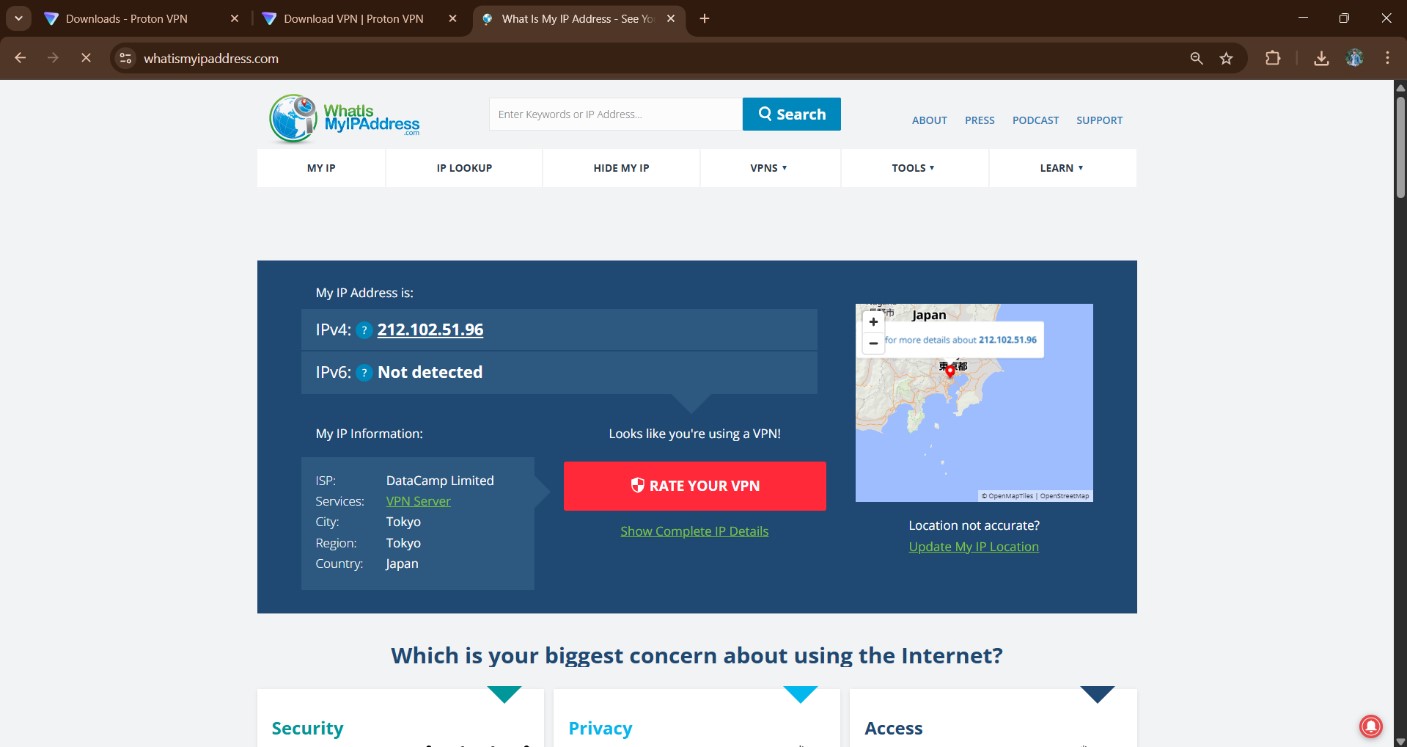
Before VPN India (actual location)

After VPN Netherlands (VPN server)

# Before



# After



This confirmed that my real IP address was successfully masked.

## 4.2 Secure Browsing Test

* Visited several secure websites (e.g., [https://wikipedia.org)](https://wikipedia.org/)
* Verified the presence of the 🔒 **lock symbol** in the browser address bar, confirming HTTPS encryption
* ProtonVPN also encrypts all traffic, including DNS queries, ensuring complete tunnel security

# 5. Performance and Comparison

**5.1 With VPN Enabled:**

* Browsing speed was slightly slower, especially while loading media-rich websites
* Increased latency due to traffic being routed through a foreign server

**5.2 Without VPN:**

* Normal browsing speed restored
* Original IP and ISP were exposed

This comparison highlights the trade-off between **speed** and **privacy** when using VPNs.

# 6. Research on VPN Encryption and Privacy

## 6.1 Encryption Standards

ProtonVPN uses:

* **AES-256 encryption**: Military-grade encryption for securing data
* **4096-bit RSA keys**: For secure key exchanges
* **Perfect Forward Secrecy (PFS)**: Ensures session keys cannot be compromised

## 6.2 Privacy Features

* **No logs policy:** ProtonVPN does not track or store user activity
* **DNS leak protection:** Prevents DNS queries from revealing your IP
* **Kill Switch (Paid Tier):** Disconnects internet if VPN connection drops to prevent data leaks

# 7. VPN Benefits and Limitations

**Benefits:**

1. **Privacy Protection:** Hides your real IP and location from websites, ISPs, and trackers.
2. **Encrypted Communication:** Secures data transmission over insecure networks, like public Wi-Fi.
3. **Geo-unblocking:** Allows access to restricted content and websites not available in your region.
4. **Bypass Censorship:** Useful in countries with restricted internet access.

**Limitations:**

1. **Reduced Speed:** Encryption and rerouting cause a slight reduction in internet speed.
2. **Limited Features on Free Plans:** Some VPNs limit servers, speeds, or data on free accounts.
3. **No Malware Protection:** VPNs don’t inherently protect against viruses or phishing.
4. **Trust in VPN Provider:** Privacy depends on the provider’s policies; some may log user data.

# 8. Conclusion

This exercise demonstrated the practical benefits of using a VPN to protect online privacy and secure communication. By encrypting traffic and masking IP addresses, VPNs act as a strong line of defense against tracking, censorship, and cyber threats. However, users must choose a **trustworthy provider**, understand the **trade-offs in performance**, and remember that a VPN is just one layer of a broader cybersecurity strategy.