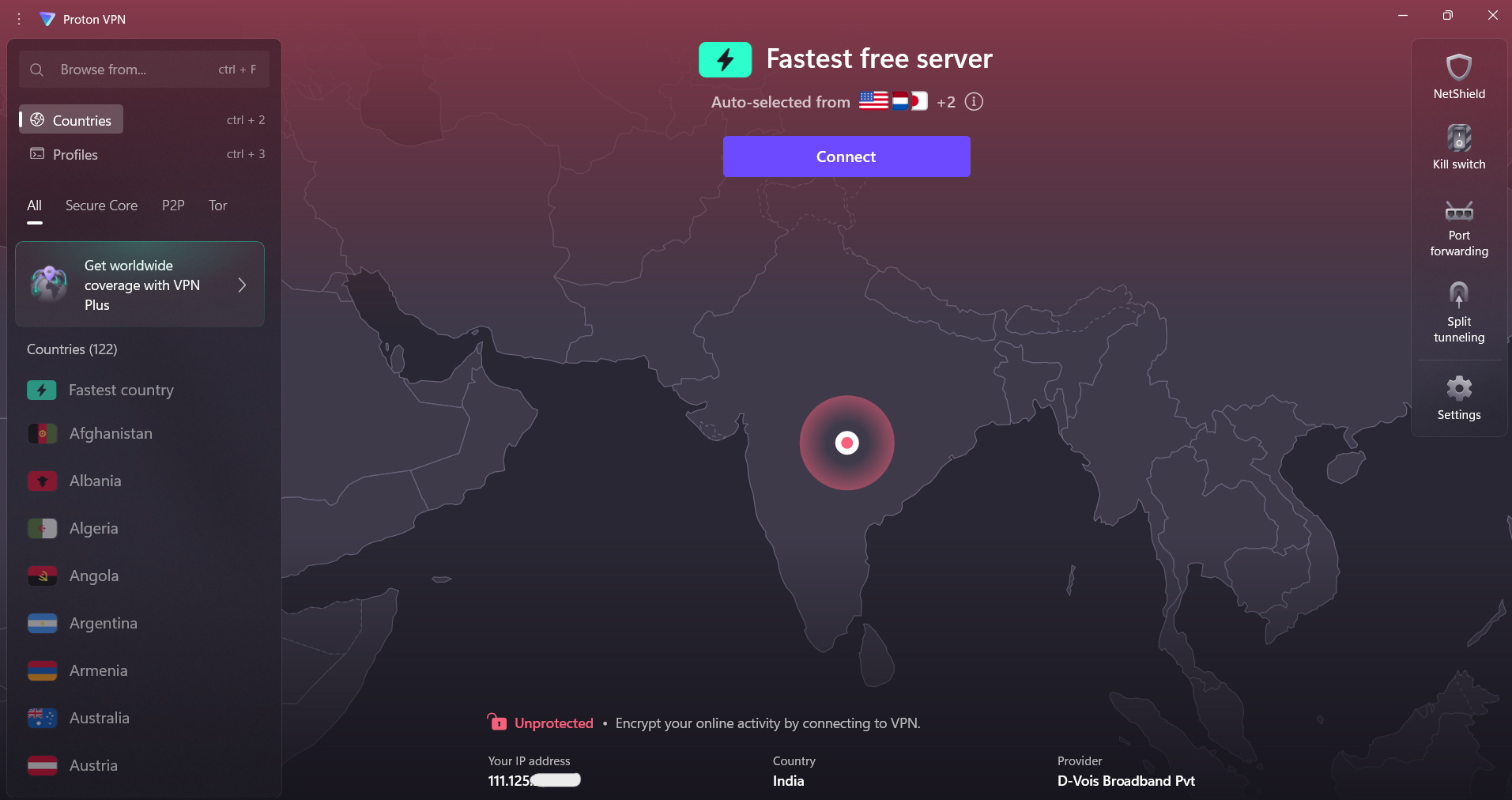
Working with VPNs: ProtonVPN

# Introduction

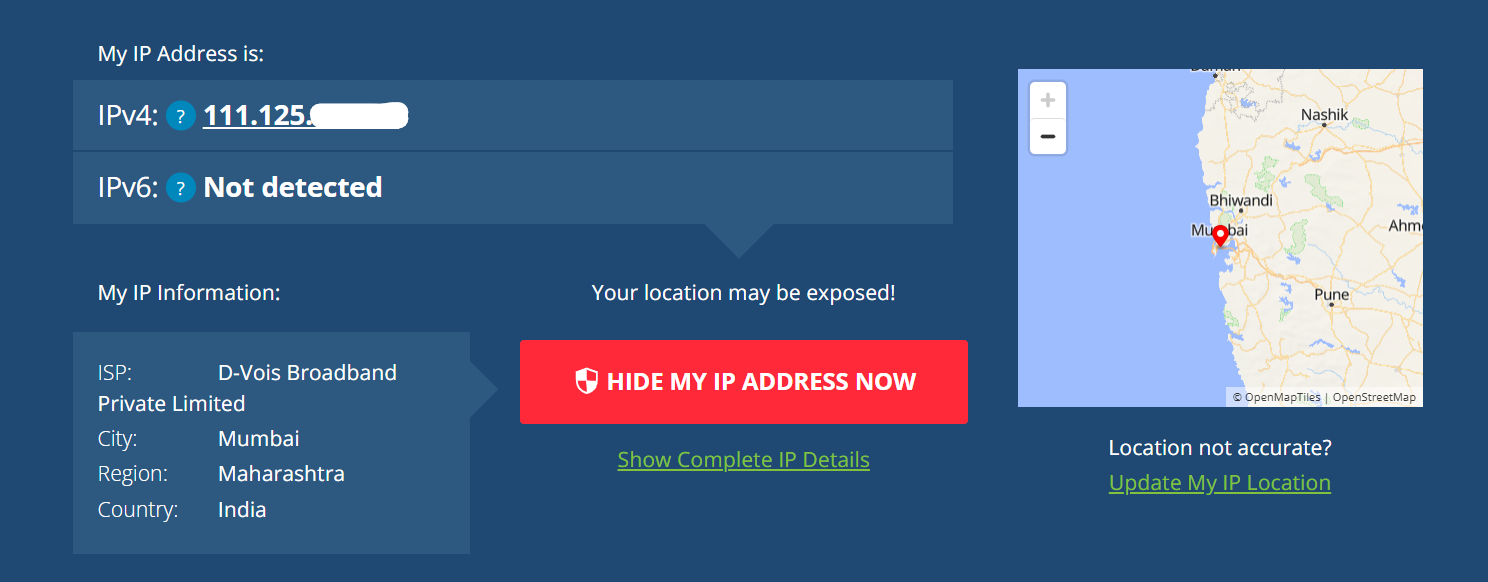
Virtual Private Networks (VPNs) have become essential tools for online privacy and security. They encrypt internet traffic, protect sensitive data from hackers, and mask users' IP addresses. This report demonstrates how a free VPN service (ProtonVPN) was set up, tested for effectiveness, and analyzed in terms of its security features, benefits, and limitations.

# VPN Setup and Testing

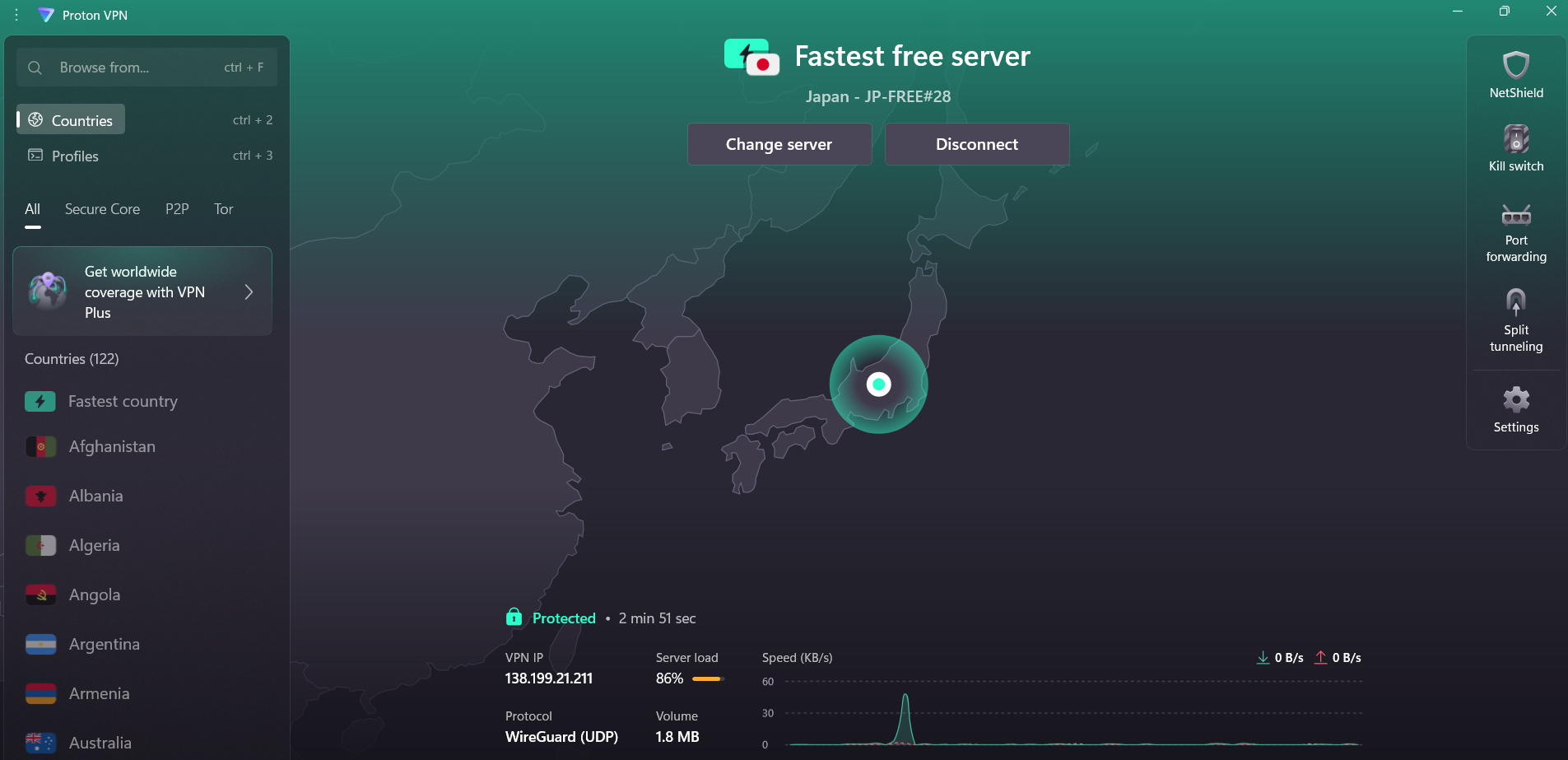
## 1. Signing into ProtonVPN Client

****The process begins with downloading and installing ProtonVPN’s free client. After installing the application, I logged in with my ProtonVPN account.

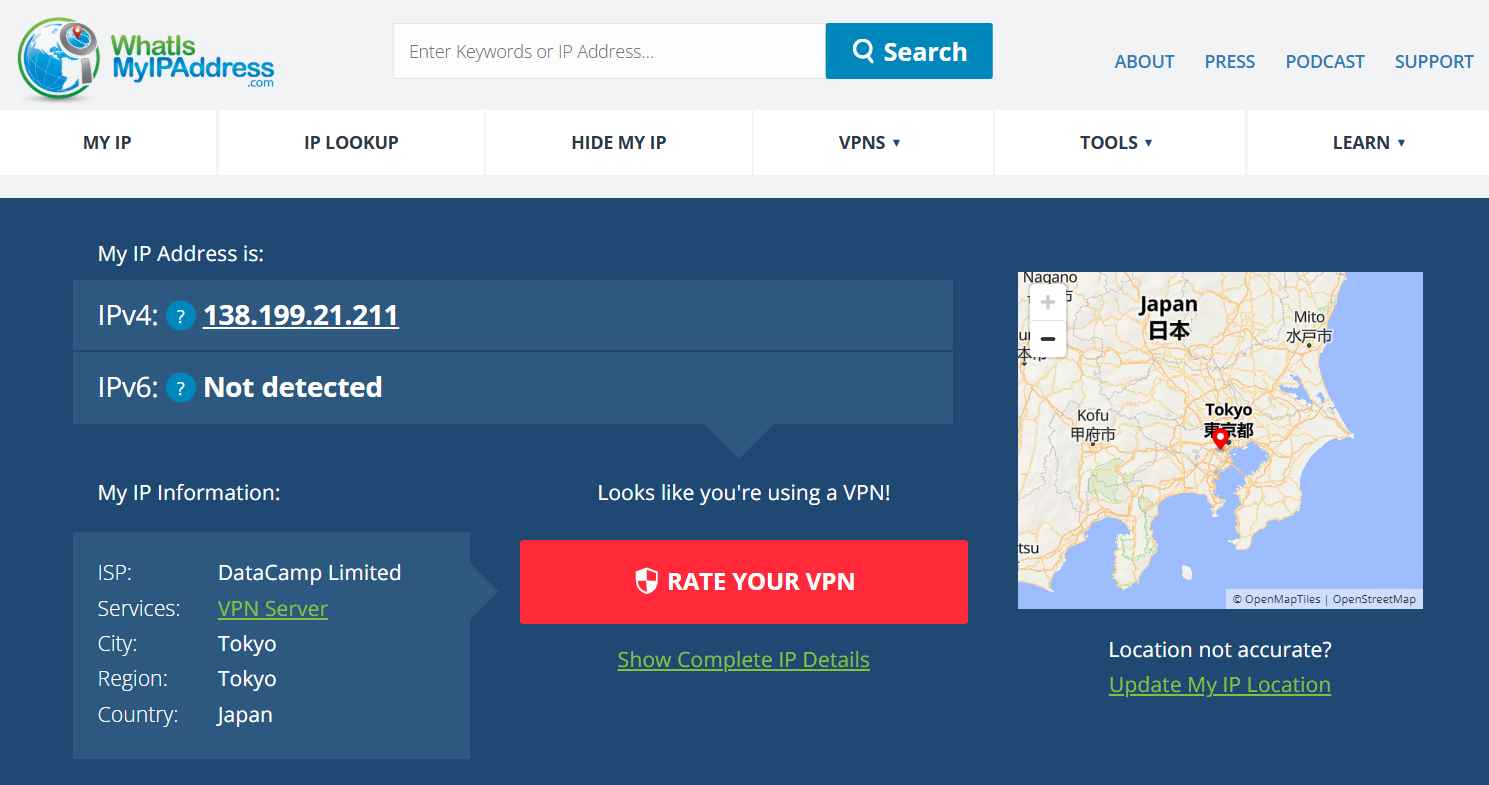
## 2. Checking Original IP Address

****Before connecting to the VPN, I checked my original IP address and location by visiting <https://whatismyipaddress.com>. The result showed my real IP address and approximate location.

## 3. Connecting to the VPN

I connected to a US-based server using ProtonVPN. The application displayed a connection status after a successful connection.

## 4. Verifying Changed IP Address

****After connecting to ProtonVPN, I refreshed <https://whatismyipaddress.com> to verify that my IP address had changed. It showed a new location corresponding to the VPN server.

## 5. Browsing a Website to Confirm Traffic is Encrypted

I visited several websites <https://www.wikipedia.org> to confirm that my internet traffic was being routed through the VPN and encrypted. The page loaded successfully without issues, confirming the VPN was working.

## 6. Disconnecting the VPN

After verifying that the VPN was functioning correctly, I disconnected from ProtonVPN to observe the changes. The application displayed a **“Disconnected”** status.

# VPN Encryption and Privacy Features

ProtonVPN uses robust encryption protocols like OpenVPN and WireGuard, which ensure that internet traffic is securely encrypted using AES-256 encryption. These protocols protect data, especially on public Wi-Fi, by ensuring that any data transferred cannot be easily intercepted by third parties.

# Summary: Benefits and Limitations

**Benefits:**  
Enhanced Privacy: VPNs encrypt data, ensuring online activities remain private.  
Security: Protects sensitive information, especially when using public Wi-Fi.  
Bypass Geo-Restrictions: VPNs allow access to websites or streaming services unavailable in certain regions.

**Limitations:**  
Speed Impact: VPN connections can sometimes slow down internet speeds, especially with free tiers.  
Server Limitations: Free versions often restrict access to a limited number of servers, leading to less flexibility.  
Trust Factor: Users must trust their VPN provider not to log or misuse data.

# Conclusion

Using ProtonVPN, I successfully masked my real IP address and encrypted my internet traffic. While the free tier offers essential features, there are some trade-offs regarding speed and server options. Nonetheless, VPNs remain an essential tool for enhancing privacy and security online. This experiment clearly demonstrated the core functionalities of a VPN in protecting internet traffic and masking user identity.