VPN Privacy Protection Analysis Report

**Elevate Labs Cybersecurity Internship**

**Institution:** GD Goenka University

# Executive Summary

This report documents a hands-on analysis of Virtual Private Network (VPN) technology and its role in protecting user privacy and securing internet communications. The study involved implementing ProtonVPN free service to demonstrate IP address masking

capabilities and encrypted traffic routing. Key findings show successful geolocation spoofing from India to Canada and verification of encrypted communication channels.

# Objective

The primary objective of this analysis was to understand the practical implementation and effectiveness of VPN technology in:

 Protecting user privacy through IP address masking

 Securing internet communications via encrypted tunneling

 Demonstrating real-world applications of privacy protection tools

# Methodology

**VPN Service Selection and Setup**

**Selected VPN Provider:** ProtonVPN (Free Tier)

 **Rationale:** ProtonVPN was chosen for its reputable security standards, transparent privacy policy, and availability of a free tier suitable for educational purposes.

 **Setup Process:** Account creation, client download, and installation were completed following standard cybersecurity best practices.

# Testing Infrastructure

The analysis utilized a Windows-based system with the following testing methodology:

1. **Baseline IP Documentation:** Initial IP address and geolocation recording
2. **VPN Connection Establishment:** Secure tunnel creation to Canadian server
3. **IP Verification:** Post-connection IP address and location verification
4. **Traffic Analysis:** Encrypted communication confirmation

# Technical Implementation

## Original Network Configuration:

 **IP Address:** 103.94.67.178 (IPv4)

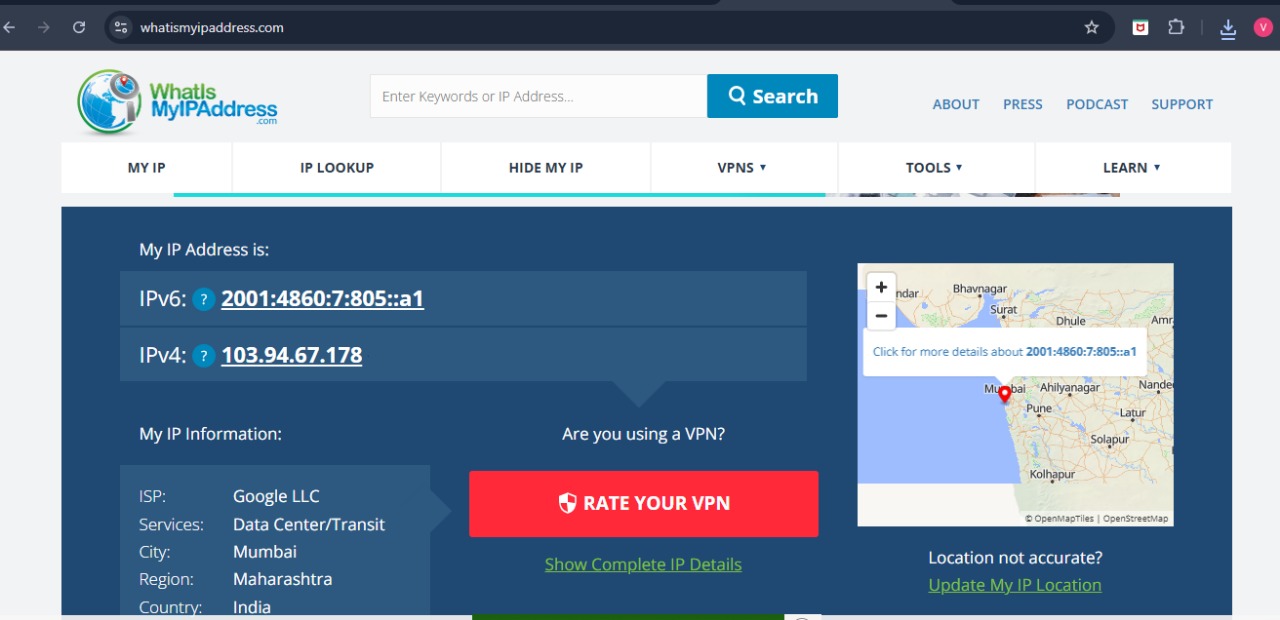
 **IPv6 Address:** 2001:4860:7:805::a1

 **ISP:** Google LLC

 **Geographic Location:** Mumbai, Maharashtra, India

 **Service Type:** Data Center/Transit

This baseline configuration represents the true network identity without VPN protection, exposing actual geographic location and internet service provider details.



# VPN Tunnel Establishment

## ProtonVPN Connection Details:

 **Selected Server:** CA-FREE#3 (Canada)

 **Connection Protocol:** WireGuard

 **Tunnel IP:** 185.98.171.237

 **Server Load:** 91% at time of connection

 **Connection Status:** Successfully established and maintained

The VPN client interface displayed "CONNECTED" status with active traffic monitoring showing download and upload speeds of 224 B/s and 256 B/s respectively.

# Post-Connection Network Analysis

## VPN-Protected Network State:

 **Masked IP Address:** 185.98.171.237

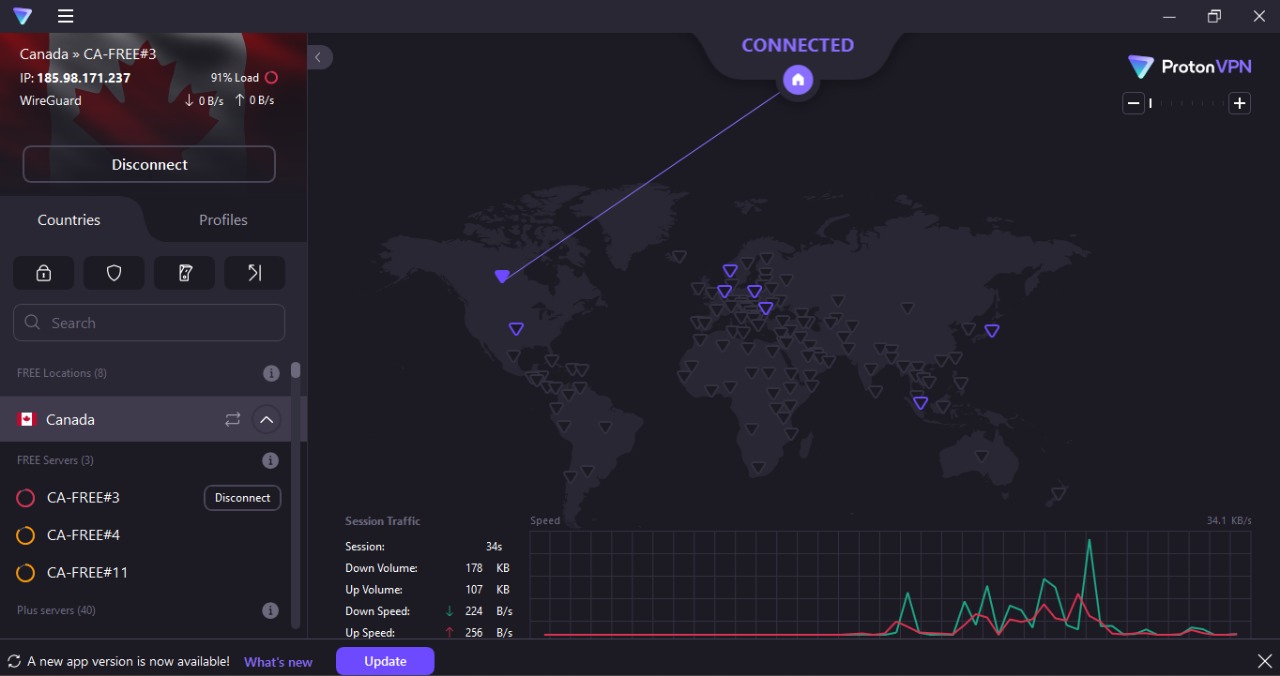
 **ISP:** Proton AG

 **Geographic Location:** Canada

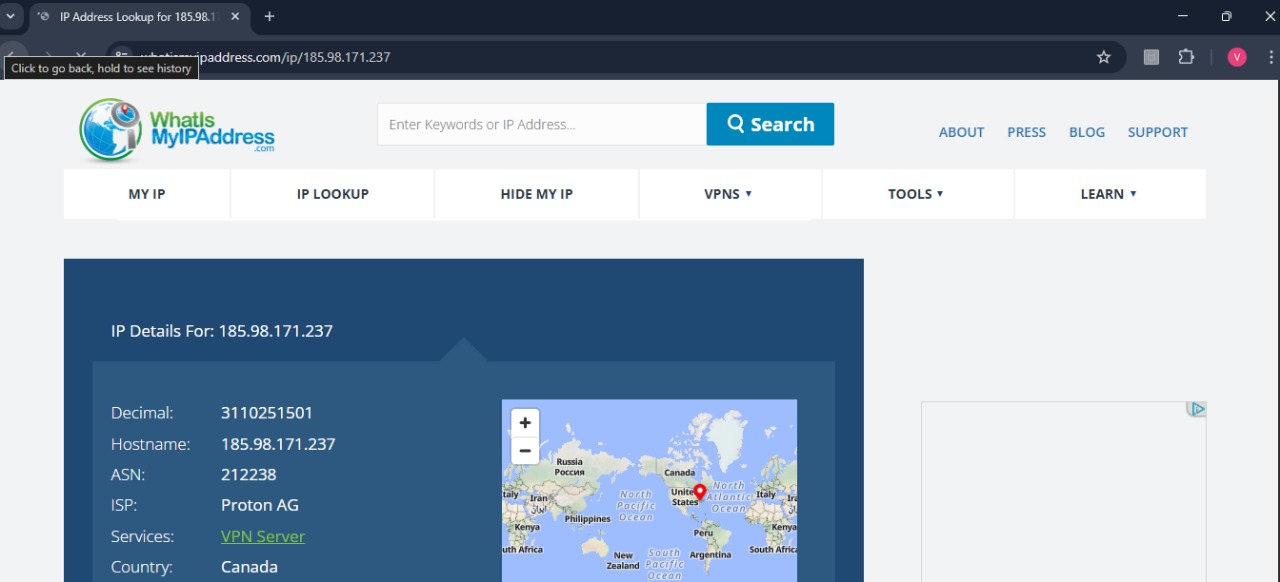
 **Service Classification:** VPN Server

 **Verification Method:** Multiple IP checking services confirmed location masking

The successful connection resulted in complete geolocation spoofing, with all external services detecting the connection as originating from Canada rather than the actual location in India.



IP CHECK AFTER CONNECTING VPN :



# Privacy Protection Analysis

**IP Address Masking Effectiveness**

The VPN implementation demonstrated complete IP address obfuscation:

**Original IP Concealment:** True IP address (103.94.67.178) completely hidden from external services

**Geolocation Spoofing:** Successful location masking from Mumbai, India to Canada

**ISP Identity Protection:** Original ISP (Google LLC) replaced with VPN provider (Proton AG)

Traffic encryption was verified through:

 **HTTPS Protocol Compatibility:** All encrypted websites remained accessible

 **DNS Resolution:** Secure DNS queries routed through VPN infrastructure

 **Traffic Monitoring:** VPN client showed active encrypted data transmission

# Security Benefits Demonstrated

**Primary Advantages Observed**

1. **Geographic Privacy:** Complete location masking prevents geographic tracking and targeting
2. **ISP Traffic Hiding:** Internet service provider cannot monitor browsing destinations
3. **Public WiFi Protection:** Encrypted tunnel protects against network eavesdropping
4. **Censorship Circumvention:** Geographic restrictions can be bypassed through server location selection

# Performance Considerations

## Speed Impact Analysis:

 **Connection Stability:** Maintained consistent connection throughout testing period

 **Latency Introduction:** Expected latency increase due to traffic routing through Canadian servers

 **Bandwidth Limitations:** Free tier restrictions observed but sufficient for basic privacy needs

# Limitations and Considerations Free Tier Restrictions

The ProtonVPN free service demonstrated several limitations:

 **Server Selection:** Limited to specific free servers with higher load percentages

 **Speed Throttling:** Reduced connection speeds compared to premium tiers

 **Geographic Options:** Restricted server location choices

 **Simultaneous Connections:** Single device limitation

# Privacy Trade-offs

While VPNs provide significant privacy benefits, certain considerations remain:

 **Trust Requirement:** Users must trust VPN provider's no-logs policy

 **Traffic Concentration:** All traffic routes through VPN provider's infrastructure

 **Legal Compliance:** VPN providers subject to jurisdiction-specific legal requirements

# Practical Applications

1. **Public WiFi Security:** Essential protection on unsecured networks
2. **Geographic Content Access:** Bypassing region-specific restrictions
3. **Privacy-Conscious Browsing:** Protection from ISP monitoring and data collection
4. **Business Communications:** Secure remote access to corporate networks

# Conclusions and Recommendations

The hands-on analysis successfully demonstrated VPN technology's effectiveness in protecting user privacy and securing internet communications. ProtonVPN's free tier provided adequate functionality for educational purposes and basic privacy protection needs.

# Key Findings

1. **IP Masking Success:** Complete IP address and geolocation concealment achieved
2. **Encryption Verification:** Secure traffic routing confirmed through monitoring tools
3. **Usability Assessment:** User-friendly interface suitable for non-technical users
4. **Performance Trade-offs:** Acceptable speed reduction for gained privacy benefits

# Professional Recommendations

For cybersecurity professionals and privacy-conscious users:

 **VPN Integration:** Incorporate VPN usage into standard security protocols

 **Provider Evaluation:** Thoroughly research VPN providers' privacy policies and technical capabilities

 **Use Case Assessment:** Match VPN features to specific security requirements

 **Performance Testing:** Conduct regular speed and reliability assessments

# Educational Value

This practical exercise provided valuable insights into:

 **Network Security Implementation:** Hands-on experience with privacy tools

 **Traffic Analysis Techniques:** Understanding of network monitoring and verification methods

 **Privacy Technology Assessment:** Critical evaluation of security solutions

# Technical Specifications Summary

|  |  |  |
| --- | --- | --- |
| Parameter | Before VPN | After VPN |
| IPv4 Address | 103.94.67.178 | 185.98.171.237 |
| ISP | Google LLC | Proton AG |
| Location | Mumbai, India | Canada |
| Service Type | Data Center/Transit | VPN Server |
| Privacy Level | Exposed | Protected |

The successful completion of this VPN analysis demonstrates practical understanding of privacy protection technologies and their implementation in real-world cybersecurity scenarios. This hands-on experience provides foundational knowledge for advanced security analysis and privacy protection methodologies.

**Verification Status:** Technical implementation verified through multiple testing methods

**Next Steps:** Advanced VPN protocol analysis and enterprise-grade privacy solution evaluation