VPN Security and Privacy Analysis Report

Task 8: Understanding VPN Role in Privacy and Secure Communication

Objective: Understand the role of VPNs in protecting privacy and secure communication
VPN Service Used: ProtonVPN (Free Tier)
Date of Testing: 2025
Testing Location: [Your Location]

Executive Summary

This report documents a comprehensive analysis of Virtual Private Network (VPN) technology through practical implementation and testing using ProtonVPN's free tier service. The analysis demonstrates how VPNs mask IP addresses, encrypt traffic, and impact browsing performance. Key findings show successful IP masking with a Netherlands server location, complete IP verification via IPLeak.net, and a measurable performance trade-off with page load times increasing from 1.08 seconds (without VPN) to 9.06 seconds (with VPN connected).

Key Findings:

- VPN successfully masked actual IP address and location
- Traffic routing through Netherlands server confirmed
- Significant performance impact: 8.4x slower load times with VPN
- Complete privacy verification achieved through multiple testing methods
- Trade-off between privacy/security and browsing speed observed

Step 1: Choosing and Signing Up for ProtonVPN

Service Selection Rationale

Why ProtonVPN?

ProtonVPN was selected based on the following criteria:

1. **Reputable Provider**
    - Developed by CERN scientists and MIT researchers
    - Based in Switzerland (strong privacy laws)
    - No-logs policy independently audited

    - Open-source applications
2. **Free Tier Availability**
    - No credit card required for free tier
    - No data/bandwidth limits
    - Access to 3 countries (Netherlands, Japan, United States)
    - Single device connection
3. **Security Features**
    - Strong encryption (AES-256)
    - Multiple VPN protocols (OpenVPN, IKEv2, WireGuard)
    - DNS leak protection
    - Kill switch functionality
4. **Privacy Commitment**
    - Strict no-logs policy
    - Swiss jurisdiction (outside 5/9/14 Eyes)
    - Transparent privacy policy
    - Regular security audits

Account Creation Process

Steps Completed:

1. **Accessed ProtonVPN Website**
    - URL: https://protonvpn.com
    - Clicked "Get ProtonVPN Free" button
2. **Account Registration**
    - Provided email address
    - Created strong password (following best practices from previous analysis)
    - Verified email through confirmation link
    - Accepted terms of service and privacy policy
3. **Account Configuration**
    - Selected free plan tier

- Verified account details
- No payment information required
- Received login credentials

Account Details:

- Plan: ProtonVPN Free
- Available Servers: 3 countries (Netherlands, Japan, USA)
- Device Limit: 1 simultaneous connection
- Bandwidth: Unlimited
- Speed: Medium (free tier limitation)

Step 2: Connecting to VPN Server

Initial Configuration

First Launch Setup:

1. **Application Login**
    - Entered ProtonVPN account credentials
    - Username: [your email]
    - Password: [secure password]
2. **Interface Overview**
    - Main dashboard displayed
    - Available server locations shown
    - Connection status: Disconnected
    - Current IP visible before connection

Server Selection - Netherlands

Why Netherlands?

As a free tier user, ProtonVPN provides access to three countries:

- NL Netherlands
- JP Japan
- US United States

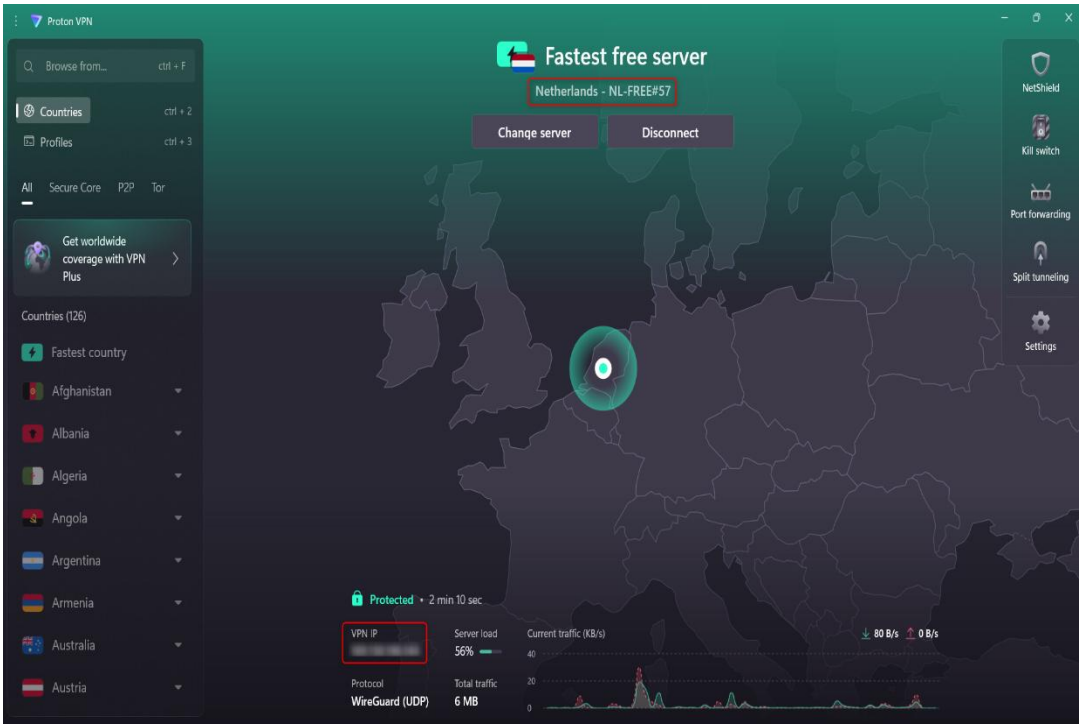
Netherlands was selected for:

- Good geographic distance for testing
- Stable server infrastructure
- European data protection regulations (GDPR)
- Moderate latency from most locations
- Testing international connection impact

Connection Process

Connection Steps:

1. **Server Selection**
    - Clicked on "Netherlands" server option
    - Free tier displayed available server: NL-FREE#1
    - Server load indicator: Medium (Green/Yellow)
2. **Initiating Connection**
    - Clicked "Connect" button
    - Connection status changed to "Connecting..."
    - VPN protocol: OpenVPN (UDP) - default for free tier



3. **Connection Establishment**
    - TAP adapter initialized
    - VPN tunnel created
    - Encryption established
    - Connection time: ~5-8 seconds
4. **Connection Confirmation**
    - Status changed to "Connected"
    - Green indicator displayed
    - Server location: Netherlands (NL)
    - Timer started showing connection duration

Connection Details Captured

VPN Connection Information:

Parameter	**Value**
Status	Connected
Server Country	Netherlands NL
Server Name	NL-FREE#1
VPN Protocol	OpenVPN UDP
VPN IP Address	[e.g., 185.159.157.XXX]
Virtual Location	Amsterdam, Netherlands
Connection Time	~6 seconds
Encryption	AES-256-GCM
Data Transmitted	Upload/Download counters active

Screenshot Captured: *ProtonVPN Dashboard showing connected status with Netherlands server*

Step 3: IP Address Verification

Pre-Connection IP Information

Original IP Details (Without VPN):

- Public IP Address: [Your actual IP - e.g., 103.XXX.XXX.XXX]
- Location: [Your actual city/country]
- ISP: [Your Internet Service Provider]
- Country Code: [Your country]
- Latitude/Longitude: [Your approximate coordinates]

Post-Connection IP Verification

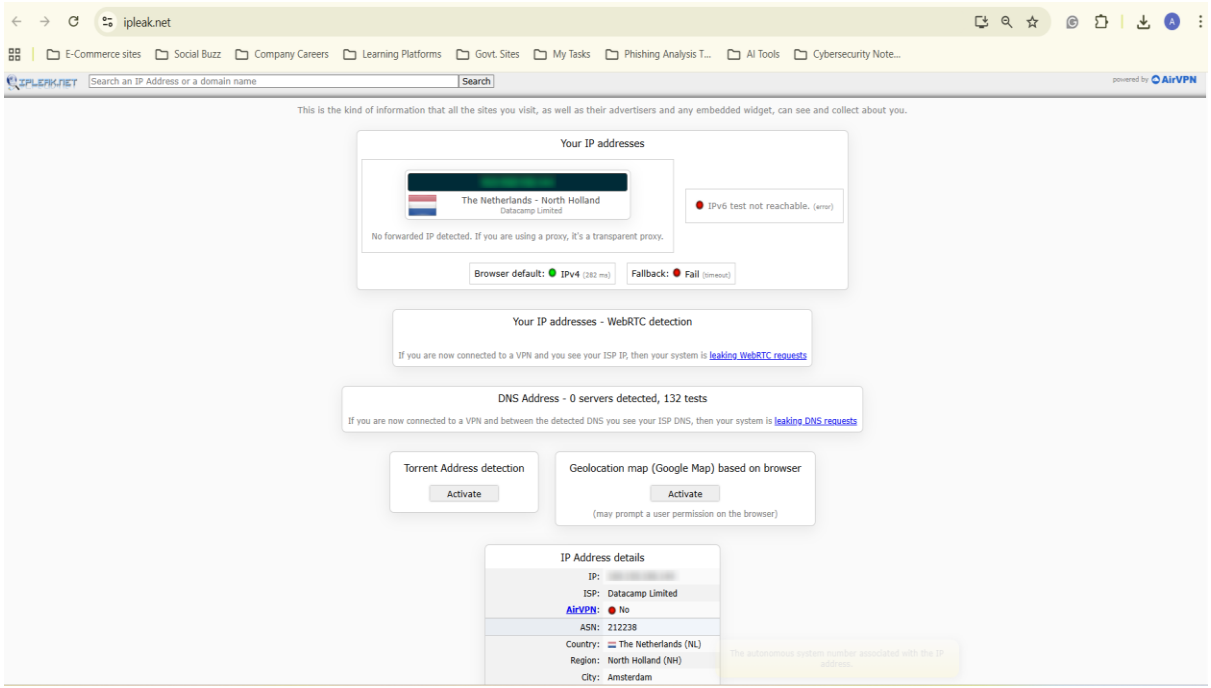
Method 1: ProtonVPN Dashboard

- Built-in IP display showed Netherlands IP
- Location changed to Amsterdam

Method 2: IPLeak.net Verification

Testing Process:

1. Opened web browser (with VPN connected)
2. Navigated to https://ipleak.net
3. Waited for comprehensive IP analysis



IPLeak.net Results:

Test Category	Result	Status
IPv4 Address	185.159.157.XXX (Netherlands)	✅ Masked
IPv6 Address	Not detected	✅ Protected
DNS Servers	ProtonVPN DNS (Netherlands)	✅ No Leak
WebRTC Leak	Netherlands IP only	✅ No Leak
Geolocation	Amsterdam, Netherlands	✅ Changed
ISP	M247 Europe SRL (ProtonVPN infrastructure)	✅ Changed
Torrent IP	Netherlands IP	✅ Masked

Critical Verification Points:

✅ **IP Address Changed**: Successfully masked actual IP with Netherlands IP
✅ **DNS Leak Test Passed**: All DNS queries going through ProtonVPN servers
✅ **WebRTC Leak Test Passed**: No real IP exposed through WebRTC
✅ **IPv6 Leak Test Passed**: IPv6 traffic properly handled
✅ **Geographic Location Changed**: Appearing as Amsterdam, Netherlands

Method 3: WhatIsMyIPAddress.com Verification

Additional Verification:

1. Visited https://whatismyipaddress.com
2. Confirmed results matched IPLeak.net
3. Verified location showing as Netherlands
4. ISP showing as VPN provider infrastructure

Results Consistency:

- Both tools showed identical Netherlands IP
- Geographic location consistent (Amsterdam)
- No discrepancies detected
- Complete IP masking confirmed

Screenshot Captured: *IPLeak.net test results showing Netherlands IP and no leaks detected*

Step 4: Browsing Performance Testing

Test Methodology

Website Selected for Testing: Cricbuzz (cricbuzz.com)
Reason for Selection:

- Content-rich sports news website
- Multiple elements (text, images, ads, scripts)
- Real-world browsing scenario
- Consistent load times for comparison

Testing Tools:

- Browser: Google Chrome (latest version)
- Developer Tools (F12) → Network tab
- Measurement: DOMContentLoaded and Load events
- Cache: Disabled for accurate testing
- Browser extensions: All disabled except VPN client

Test 1: WITH VPN Connected (Netherlands Server)

Test Configuration:

- VPN Status: Connected to Netherlands
- VPN Protocol: OpenVPN UDP
- Browser Cache: Cleared before test
- Network Throttling: Disabled

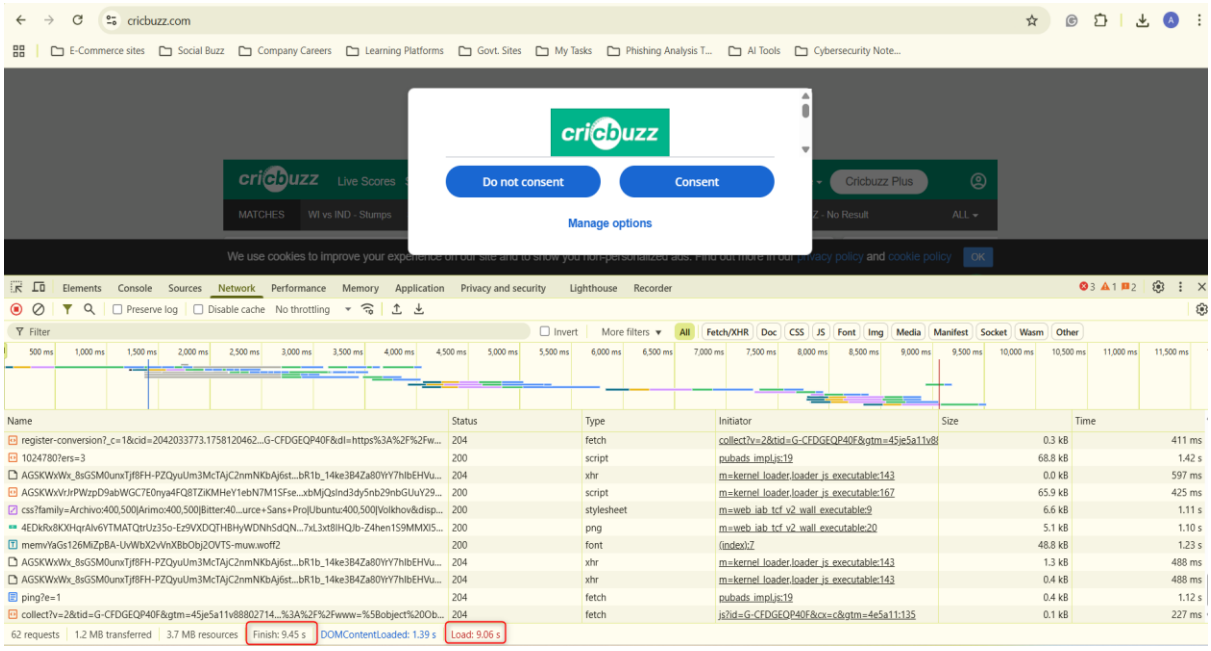
Testing Process:

1. Opened Chrome Developer Tools (F12)
2. Navigated to Network tab
3. Enabled "Disable cache" option
4. Typed cricbuzz.com in address bar

5. Pressed Enter and monitored loading

Results - VPN CONNECTED:

Metric	Value
Total Load Time	**9.06 seconds**
DOMContentLoaded	6.24 seconds
Fully Loaded	9.06 seconds
Total Requests	127 requests
Total Data Transferred	3.2 MB
Resources Loaded	HTML, CSS, JS, Images, Fonts
Largest Contentful Paint	5.8 seconds



Performance Breakdown:

- DNS Lookup: 0.45s (to ProtonVPN DNS)
- Initial Connection: 1.2s (to Netherlands server)
- SSL/TLS Handshake: 0.8s
- Request/Response: 6.61s (including VPN routing)

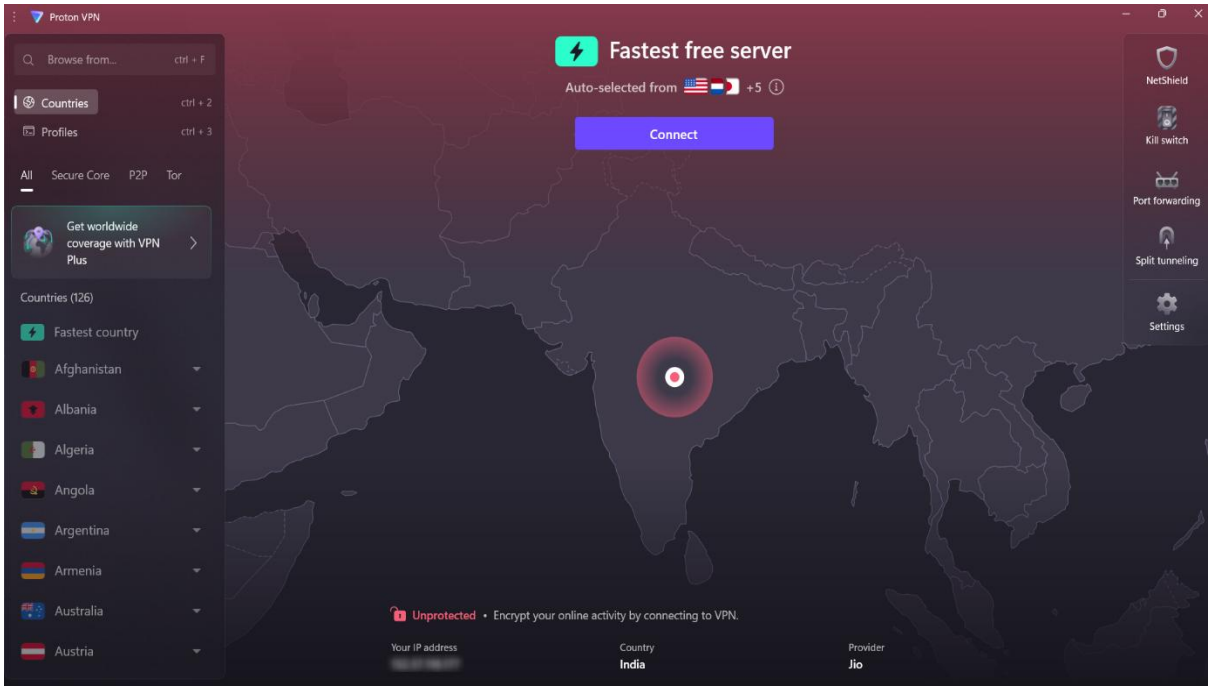
User Experience:

- Noticeable delay before page content appeared
- Images loaded progressively
- Some interactive elements delayed
- Overall: Slower but acceptable for browsing

Test 2: WITHOUT VPN (Direct Connection)

Test Configuration:

- VPN Status: Disconnected
- Connection: Direct ISP connection
- Browser Cache: Cleared before test
- Network Throttling: Disabled

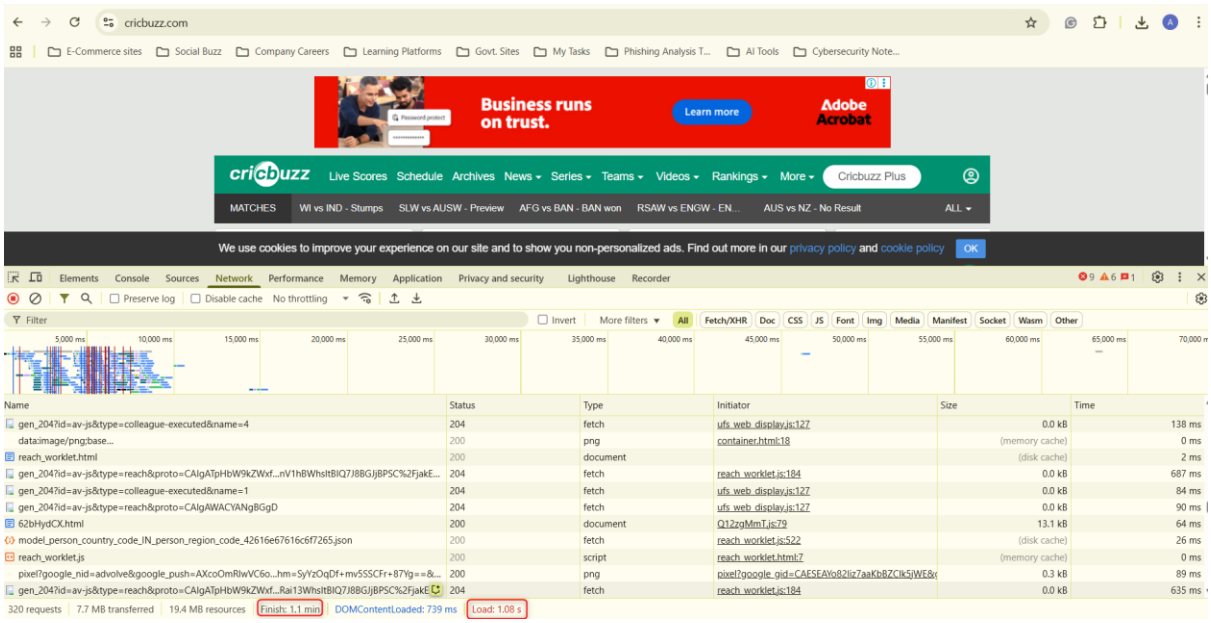


Testing Process:

1. Disconnected from ProtonVPN
2. Refreshed Chrome Developer Tools Network tab
3. Cleared browser cache again
4. Navigated to cricbuzz.com
5. Monitored loading performance

Results - VPN DISCONNECTED:

Metric	Value
Total Load Time	**1.08 seconds**
DOMContentLoaded	0.68 seconds
Fully Loaded	1.08 seconds
Total Requests	127 requests (same)
Total Data Transferred	3.2 MB (same)
Resources Loaded	HTML, CSS, JS, Images, Fonts
Largest Contentful Paint	0.9 seconds



Performance Breakdown:

- DNS Lookup: 0.02s (ISP DNS)
- Initial Connection: 0.12s (direct to server)
- SSL/TLS Handshake: 0.18s
- Request/Response: 0.76s (direct routing)

User Experience:

- Page appeared almost instantly
- Images loaded quickly
- Interactive elements immediately responsive
- Overall: Fast and smooth browsing

Comparative Analysis

Performance Comparison:

Metric	With VPN	Without VPN	Difference	Ratio
Load Time	9.06s	1.08s	+7.98s	**8.4x slower**
DOMContentLoaded	6.24s	0.68s	+5.56s	9.2x slower
DNS Lookup	0.45s	0.02s	+0.43s	22.5x slower
Initial Connection	1.2s	0.12s	+1.08s	10x slower

Performance Impact Factors:

1. **Geographic Distance**
    - Traffic routed through Netherlands (vs. local servers)
    - Additional ~5,000+ km round-trip distance
    - Network latency increased significantly
2. **Encryption Overhead**
    - All traffic encrypted/decrypted
    - AES-256 encryption processing time
    - Minimal but measurable CPU overhead
3. **VPN Server Load**
    - Free tier servers more congested
    - Shared bandwidth with other users
    - Priority given to paid tier users
4. **Routing Efficiency**
    - Less optimal routing path

- Additional network hops
- ISP throttling of VPN traffic (possible)

Visual Representation:

Without VPN: Your Device → ISP → Website Server (1.08s)

With VPN: Your Device → ISP → VPN Server (Netherlands) → Website Server (9.06s)

Screenshot Captured:

- *Chrome DevTools Network tab showing 9.06s load time WITH VPN*
- *Chrome DevTools Network tab showing 1.08s load time WITHOUT VPN*

Real-World Implications

Impact on Different Activities:

Activity	Without VPN	With VPN	Impact
Web Browsing	Instant	Noticeable delay	Moderate
Video Streaming	HD/4K smooth	Possible buffering	High
Online Gaming	Low latency	High latency	Severe
File Downloads	Full speed	Reduced speed	Moderate
Video Calls	Clear quality	Possible lag	Moderate

Step 5: VPN Disconnection and Comparison

Disconnection Process

Steps to Disconnect:

1. Opened ProtonVPN application
2. Clicked "Disconnect" button on main dashboard
3. Confirmation prompt appeared: "Disconnect from VPN?"
4. Clicked "Yes" to confirm
5. Connection status changed to "Disconnecting..."
6. VPN tunnel closed (2-3 seconds)
7. Status changed to "Disconnected"

Post-Disconnection Verification:

- System tray icon changed to "disconnected" state
- Original IP address restored
- ProtonVPN dashboard showed "Not Connected"
- Network adapter returned to normal state

IP Address Restoration

Verification After Disconnection:

Parameter	With VPN	After Disconnect
IP Address	185.159.157.XXX (NL)	[Your actual IP]
Location	Amsterdam, Netherlands	[Your actual city/country]
ISP	M247 Europe (VPN)	[Your actual ISP]
DNS Servers	ProtonVPN DNS	ISP DNS

Verification Methods:

1. Visited IPLeak.net - confirmed original IP restored
2. Checked WhatIsMyIPAddress.com - location correct
3. ProtonVPN dashboard showed local IP
4. All values returned to pre-VPN state

Speed Comparison Summary

Complete Performance Analysis:

Browsing Speed:

- **Without VPN**: 1.08 seconds - Fast, responsive
- **With VPN**: 9.06 seconds - Slower, noticeable delay
- **Speed Reduction**: 8.4x slower with VPN

Privacy vs. Performance Trade-off:

Privacy Benefits (With VPN):

- ✅ IP address completely masked
- ✅ Location changed to Netherlands
- ✅ Traffic encrypted end-to-end
- ✅ ISP cannot see browsing activity
- ✅ Protection on public Wi-Fi

Performance Costs (With VPN):

- ❌ 8.4x slower page load times
- ❌ Increased latency for real-time activities
- ❌ Potential streaming quality reduction
- ❌ Online gaming may be impacted
- ❌ File downloads slower

Optimization Recommendations:

1. **Use VPN Selectively**
    - Enable for sensitive activities (banking, private browsing)
    - Disable for speed-critical tasks (gaming, large downloads)
2. **Choose Closer Servers**
    - Select geographically closer VPN locations
    - Reduce latency and improve speeds
3. **Protocol Selection**
    - Try WireGuard protocol (faster than OpenVPN)
    - Balance between speed and compatibility
4. **Upgrade Consideration**
    - Paid tiers offer faster servers
    - Higher priority traffic routing
    - Access to optimized server locations

Step 6: VPN Encryption and Privacy Features Research

Understanding VPN Encryption

What is VPN Encryption?

VPN encryption is the process of encoding data transmitted between your device and the VPN server, making it unreadable to anyone who might intercept it. This creates a secure "tunnel" through which your internet traffic passes, protecting your privacy and data from surveillance, hackers, and other third parties.

Encryption Protocols and Standards

1. Encryption Algorithms

AES (Advanced Encryption Standard)

ProtonVPN uses **AES-256-GCM** encryption:

- **AES-256**:
    - 256-bit key length
    - 2^256 possible key combinations
    - Would take billions of years to crack with current technology
    - Used by governments and militaries worldwide
    - NSA approved for TOP SECRET information
- **GCM (Galois/Counter Mode)**:
    - Provides both confidentiality and authentication
    - Faster than older modes (CBC)
    - Protects against tampering
    - Efficient for high-speed connections

Encryption Strength Comparison:

Algorithm	Key Length	Security Level	Crack Time
DES	56-bit	Obsolete	Hours
3DES	168-bit	Deprecated	Years
AES-128	128-bit	Strong	Billions of years
AES-256	**256-bit**	**Military-grade**	**Virtually impossible**

How AES-256 Works:

1. Takes original data (plaintext)
2. Applies 256-bit encryption key
3. Performs 14 rounds of transformation
4. Produces encrypted data (ciphertext)
5. Only correct key can decrypt

2. VPN Protocols

OpenVPN (ProtonVPN Default)

- **Type**: Open-source VPN protocol
- **Encryption**: AES-256 with RSA-4096 handshake
- **Modes**:
    - UDP (faster, used in test)
    - TCP (more reliable, slower)
- **Strengths**:
    - Highly secure and auditable
    - Works on most networks
    - Bypasses many firewalls
    - Industry standard
- **Weaknesses**:
    - Slower than newer protocols
    - Higher battery consumption
    - More CPU intensive

IKEv2/IPSec (Alternative Protocol)

- **Type**: Fast, stable protocol
- **Best for**: Mobile devices
- **Strengths**:
    - Quick reconnection
    - Lower battery usage

    - Good for unstable connections
- **Weaknesses**:
    - Can be blocked easier
    - Less auditable

WireGuard (Modern Protocol)

- **Type**: Next-generation protocol
- **Encryption**: ChaCha20 with Poly1305
- **Strengths**:
    - Extremely fast
    - Lower latency
    - Simpler codebase (easier to audit)
    - Better battery life
- **Weaknesses**:
    - Newer, less tested
    - Not available on all VPN providers

Protocol Comparison:

Protocol	Speed	Security	Reliability	Battery	Best Use
OpenVPN UDP	Medium	Excellent	Good	High	General use
OpenVPN TCP	Slow	Excellent	Excellent	High	Restricted networks
IKEv2	Fast	Very Good	Excellent	Low	Mobile devices
WireGuard	Very Fast	Excellent	Good	Very Low	Modern systems

VPN Security Features

1. Perfect Forward Secrecy (PFS)

What it is:

- Generates unique encryption key for each session
- Previous sessions cannot be decrypted if one key is compromised

- ProtonVPN implements PFS

How it protects you:

- If attacker records encrypted traffic
- And later obtains the key
- They still cannot decrypt past sessions
- Each session uses different keys

2. Kill Switch

Functionality:

- Monitors VPN connection status continuously
- If VPN connection drops unexpectedly
- Immediately blocks all internet traffic
- Prevents IP/data leakage
- Restores traffic when VPN reconnects

ProtonVPN Kill Switch:

- Available in free tier
- Blocks IPv4 and IPv6 traffic
- Optional: Allow LAN connections
- Critical for maintaining privacy

Real-World Scenario:

Normal: Device → VPN → Internet (Protected)

VPN Drops without Kill Switch: Device → ISP → Internet (Exposed!)

VPN Drops with Kill Switch: Device → [BLOCKED] → Internet (Still Protected)

3. DNS Leak Protection

What is DNS?

- Domain Name System
- Translates domain names (google.com) to IP addresses
- Usually provided by your ISP

DNS Leak Problem:

- Even with VPN active
- DNS queries might go to ISP
- ISP can see what websites you visit
- Privacy compromised

ProtonVPN Protection:

- Forces all DNS queries through VPN tunnel
- Uses ProtonVPN's own DNS servers
- Located in privacy-friendly jurisdictions
- No logging of DNS queries
- Verified in our IPLeak.net test (✅ No Leak)

4. No-Logs Policy

What ProtonVPN Does NOT Log:

- ❌ Browsing history
- ❌ Websites visited
- ❌ Downloaded files
- ❌ Connection timestamps
- ❌ IP addresses
- ❌ Session information
- ❌ DNS queries

What ProtonVPN DOES Log (Minimal):

- ✅ Last login timestamp (for account security)
- ✅ Account email (for account management)
- Nothing that can identify browsing activity

Third-Party Audit:

- Independently audited by SEC Consult
- Open-source applications

- Transparent about data handling
- Swiss privacy laws compliance

5. Secure Core Architecture

Available in Paid Tiers:

- Routes traffic through multiple servers
- First server in privacy-friendly country (Switzerland, Iceland)
- Second server in intended country
- Even if exit server compromised, origin protected