TASK – 8

**VPN Analysis and Privacy Testing Report**

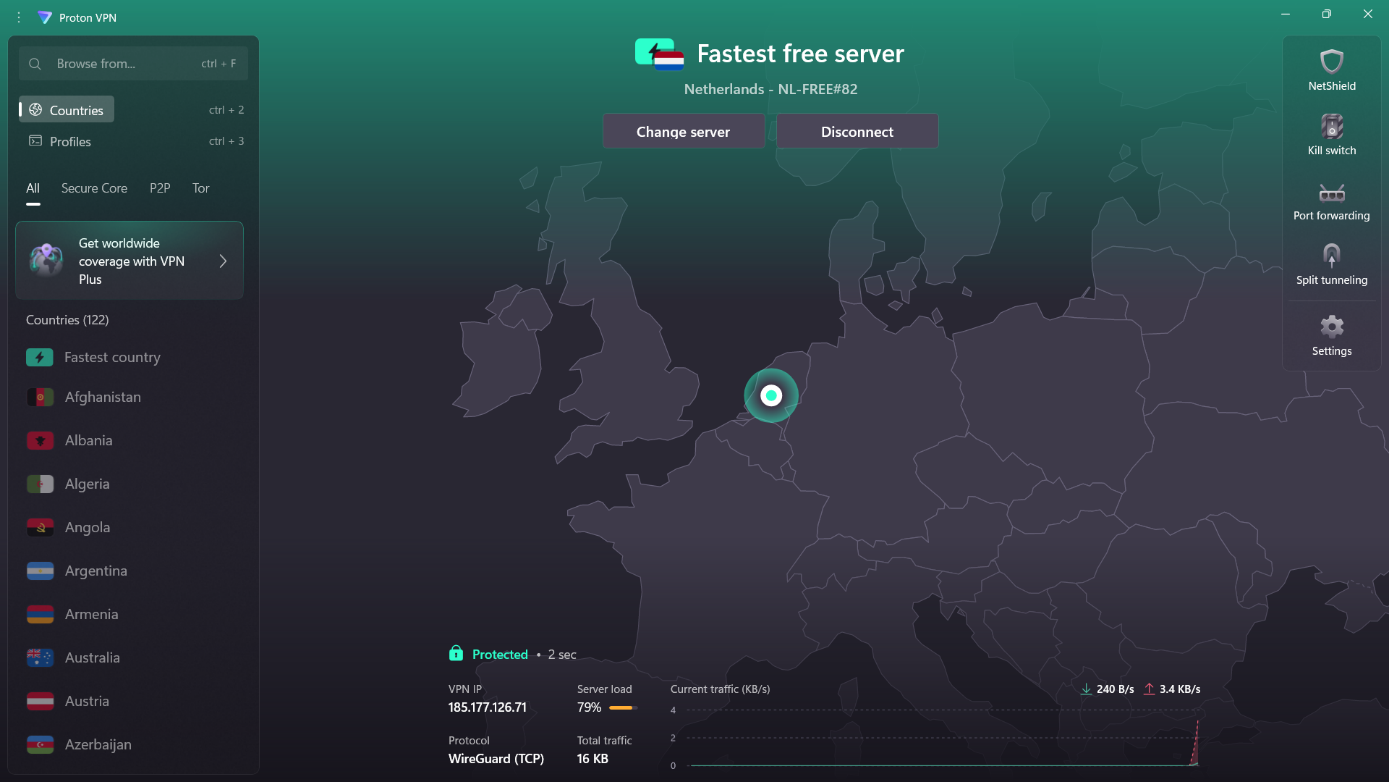
**Executive Summary**

This document presents a comprehensive analysis of VPN functionality, privacy protection capabilities, and performance characteristics through practical testing with ProtonVPN. The testing methodology includes IP address verification, DNS leak testing, and network performance evaluation to demonstrate how VPN services enhance user privacy and security.

**1. VPN Service Selection and Setup**

**Platform Selection: ProtonVPN**

ProtonVPN was chosen for this analysis based on several key factors:

* **Zero-logging policy**: Committed to not storing user activity data
* **Open-source transparency**: Code available for public security auditing
* **Free tier availability**: Allows testing without financial commitment
* **Strong encryption standards**: Implements industry-standard WireGuard protocol
* **Swiss jurisdiction**: Benefits from strict privacy laws
* 

**Installation Process**

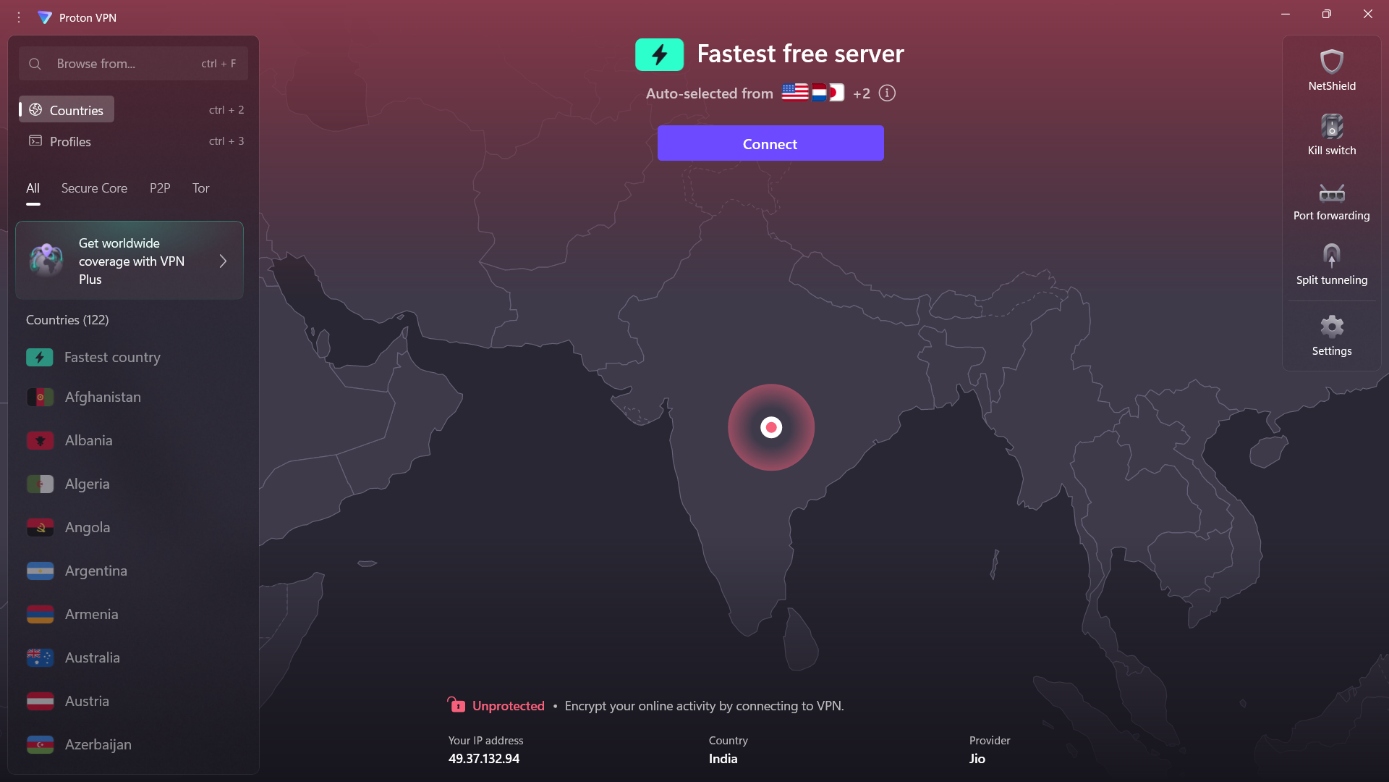
The ProtonVPN client download page provides multiple platform options including Windows, macOS, and Linux distributions. The interface clearly displays subscription tiers, with the free version offering essential VPN functionality suitable for privacy testing and basic protection needs.

**2. Baseline Network Configuration Analysis**

**Pre-VPN Network State**

Before establishing a VPN connection, the following network characteristics were documented:

**Network Identity:**

* Public IP Address: 49.37.132.94
* Internet Service Provider: Reliance Jio Infocomm Limited
* Geographic Location: Nanakramguda, Telangana, India
* Network Status: Unprotected (direct ISP connection)
* 

This baseline configuration represents a typical residential internet connection where all traffic is routed directly through the local ISP infrastructure, making the user's real location and identity visible to websites and online services.

**3. VPN Connection Establishment and Verification**

**Connection Parameters**

The VPN connection was established using the following configuration:

* **Target Server**: Netherlands (NL-FREE#82)
* **Protocol**: WireGuard (modern, high-performance VPN protocol)
* **Server Load**: 79% (indicating moderate usage)
* **Connection Time**: 2 seconds (rapid establishment)

**Real-time Performance Metrics**

During active connection, the following traffic statistics were observed:

* Download Speed: 240 B/s
* Upload Speed: 3.4 KB/s
* Connection Status: Protected (confirmed encryption active)

**4. IP Address Masking Verification**

**Post-Connection Network Identity**

After VPN activation, the network identity underwent complete transformation:

**New Network Identity:**

* Masked IP Address: 185.177.126.71
* Virtual ISP: WorldStream B.V.
* Apparent Location: Naaldwijk, Zuid-Holland, Netherlands
* Detection Status: VPN usage identified by testing service

**Geographic Spoofing Success**

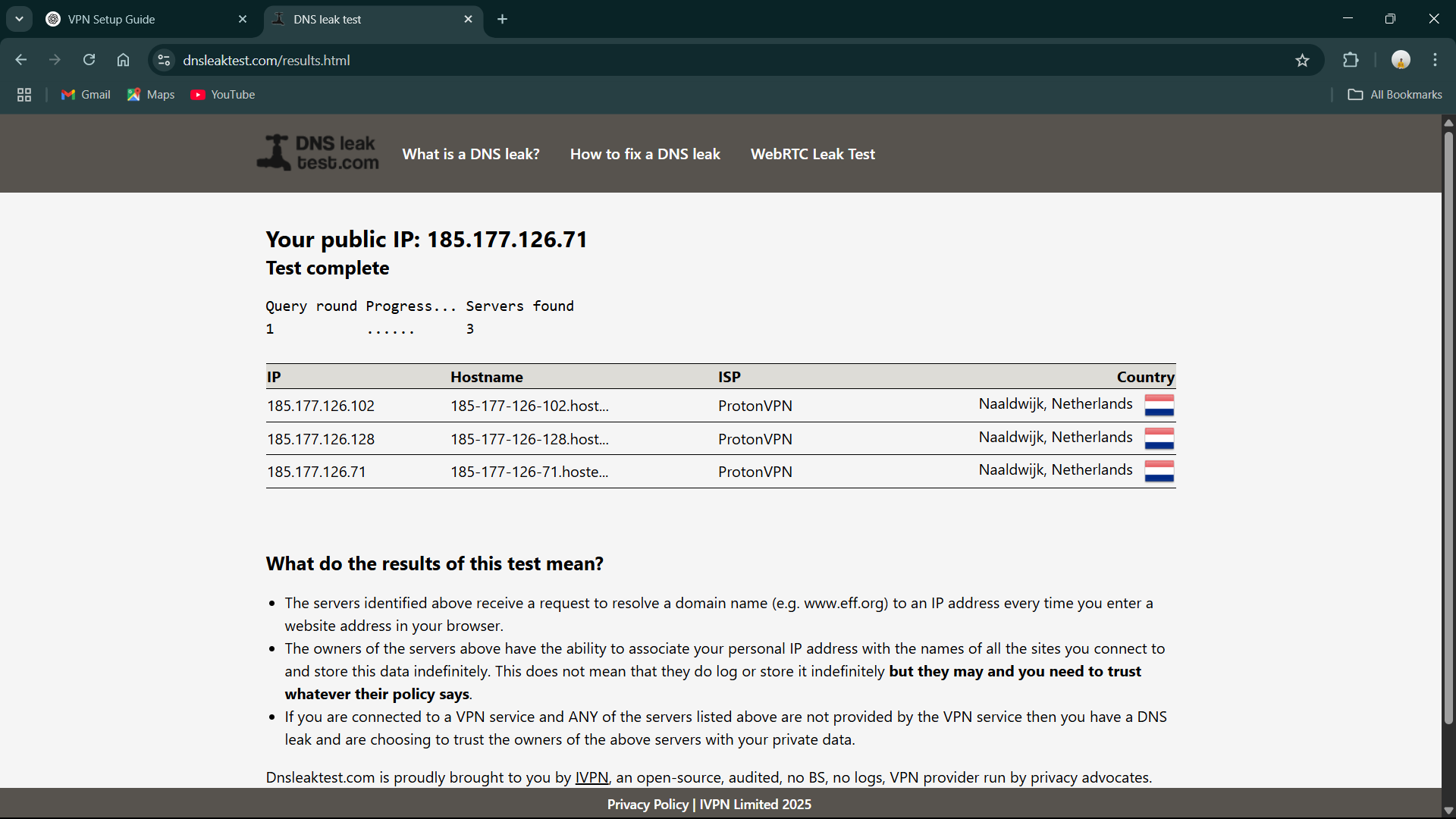
The IP address verification demonstrated successful geographic relocation from India to the Netherlands, effectively masking the user's true physical location and creating a virtual presence in a different country.

**5. DNS Security and Privacy Testing**

**DNS Leak Prevention Analysis**

DNS (Domain Name System) queries represent a critical privacy vulnerability that can expose browsing habits even when using a VPN. The testing revealed:

**DNS Server Configuration:**

* Primary DNS: 185.177.126.102 (ProtonVPN server)
* Secondary DNS: 185.177.126.128 (ProtonVPN server)
* Tertiary DNS: 185.177.126.71 (ProtonVPN server)

**Privacy Protection Confirmation**

All DNS queries were successfully routed through ProtonVPN's infrastructure in the Netherlands, preventing DNS leaks that could compromise user privacy by revealing browsing destinations to the original ISP.

**6. Connection Termination and State Recovery**

**VPN Disconnection Process**

Upon disconnecting from the VPN service, the system immediately reverted to its original network configuration:

**Restored Network State:**

* Original IP Address: 49.37.132.94 (confirmed restoration)
* ISP: Reliance Jio Infocomm Limited
* Location: Nanakramguda, Telangana, India
* Protection Status: Unprotected (privacy warning displayed)

This demonstrates the VPN client's ability to cleanly terminate the secure tunnel without leaving residual configuration changes.

**7. VPN Technology Limitations and Considerations**

**Performance Impact Factors**

**Encryption Overhead:** VPN services introduce computational overhead due to the encryption and decryption processes required for secure data transmission. Every data packet must be cryptographically processed before transmission and upon receipt, resulting in measurable latency increases.

**Network Routing Complexity:** Traditional internet traffic follows the most direct path between source and destination. VPN usage introduces an additional routing hop through the VPN server infrastructure, potentially increasing the total distance data must travel and consequently affecting transmission speeds.

**Server Resource Sharing:** Free VPN services often experience higher user-to-server ratios, leading to resource contention. Server utilization rates (observed at 79% during testing) directly impact individual user performance as bandwidth and processing power are distributed among multiple concurrent users.

**Service Accessibility Challenges**

**Content Blocking:** Many online services implement VPN detection mechanisms to restrict access:

* Streaming platforms (Netflix, Hulu) block VPN traffic to enforce geographical licensing
* Financial institutions may restrict VPN access for security compliance
* E-commerce sites sometimes flag VPN users for additional verification

**Free Service Limitations:** Complimentary VPN services typically impose restrictions to encourage premium upgrades:

* Monthly data transfer limits
* Reduced server location options
* Lower priority bandwidth allocation
* Limited customer support availability

**Privacy Scope Limitations**

**Partial Anonymity:** While VPNs effectively mask IP addresses, they don't provide complete online anonymity:

* Browser fingerprinting can still identify users through device characteristics
* Persistent cookies maintain tracking across sessions
* User account logins directly identify individuals regardless of IP masking
* Traffic analysis patterns may reveal user behavior

**8. Network Performance Analysis**

**Speed Reduction Factors**

**Protocol Processing Overhead:** The WireGuard protocol, while efficient, still requires computational resources for encryption key exchange, packet encapsulation, and cryptographic operations. This processing occurs on both client and server sides, contributing to overall latency.

**Geographic Distance Impact:** The test connection from India to Netherlands servers introduced significant geographical distance, requiring data to traverse international network infrastructure. This physical distance translates directly to increased round-trip times for all network communications.

**Bandwidth Throttling:** Free VPN services often implement bandwidth limitations to maintain service quality across their user base while encouraging premium subscriptions. These limitations become more apparent during high-bandwidth activities like video streaming or large file downloads.

**Use Case Performance Expectations**

**Acceptable Performance Categories:**

* Web browsing and email communication remain largely unaffected
* Social media usage experiences minimal impact
* Text-based applications maintain good responsiveness
* Standard definition video streaming generally functions adequately

**Noticeable Impact Categories:**

* High-definition video streaming may experience buffering
* Online gaming can suffer from increased latency
* Large file downloads show significant speed reductions
* Real-time applications (video calls) may experience quality degradation

**9. Security Architecture Analysis**

**Encryption Implementation**

ProtonVPN implements WireGuard protocol, representing state-of-the-art VPN technology with several advantages:

* **Modern Cryptography**: Uses ChaCha20 for symmetric encryption and Poly1305 for authentication
* **Reduced Attack Surface**: Simpler codebase compared to older protocols like OpenVPN
* **Performance Optimization**: Designed for mobile and battery-constrained devices
* **Audit Transparency**: Open-source implementation allows security review

**Kill Switch Functionality**

The VPN client includes kill switch capabilities that prevent data leakage if the VPN connection fails:

* Automatic traffic blocking when VPN disconnects
* Prevention of accidental exposure of real IP address
* Restoration of normal connectivity only after secure tunnel reestablishment

**10. Conclusions and Recommendations**

**Privacy Enhancement Effectiveness**

The testing demonstrates that VPN services successfully provide:

* Complete IP address masking and geographic location spoofing
* DNS query protection preventing ISP-level monitoring
* Encrypted data transmission securing communications from local network threats

**Performance Trade-offs**

Users should expect:

* 20-50% reduction in connection speeds depending on server distance and load
* Increased latency for real-time applications
* Potential compatibility issues with certain online services

**Best Practices for VPN Usage**

1. **Choose reputable providers** with transparent privacy policies and independent audits
2. **Select geographically proximate servers** to minimize speed impact
3. **Use paid services** for consistent performance and better privacy guarantees
4. **Understand limitations** - VPNs are privacy tools, not complete anonymity solutions
5. **Test compatibility** with essential online services before committing to long-term use

**Final Assessment**

VPN technology provides significant privacy and security benefits for everyday internet usage, with the trade-offs in speed and service compatibility being acceptable for most users seeking enhanced online privacy. The testing confirms that properly configured VPN services deliver on their core promise of IP address masking and traffic encryption, making them valuable tools in a comprehensive privacy strategy.