CYBER SECURITY INTERNSHIP

Task 8: VPN Setup and Testing Report

Submitted by: M.Vyshnavi

1. Introduction

Task Objectives

- Understand how VPNs protect privacy and secure communications
- Set up and test a free VPN client (ProtonVPN)
- Verify IP address changes and encryption functionality
- Compare browsing speeds with and without VPN
- Document VPN benefits and limitations

2. VPN Setup Process

2.1 VPN Selection: ProtonVPN Free Tier

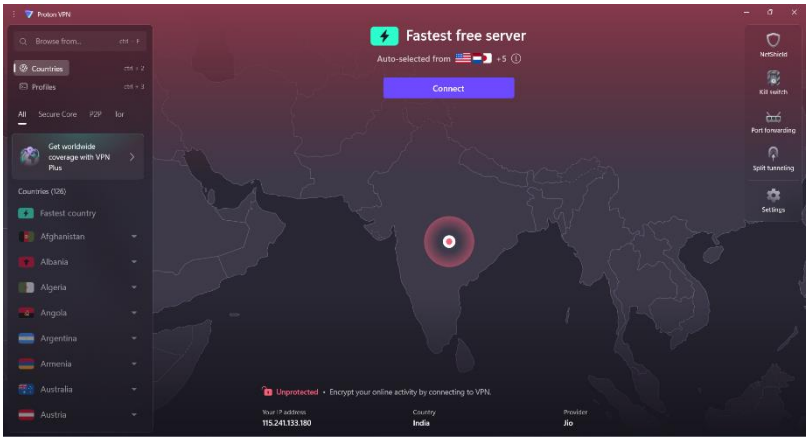
Why ProtonVPN?

- Unlimited bandwidth with no data caps
- Strong AES-256 encryption and WireGuard protocol
- No-logs policy with independent audits
- Based in privacy-friendly Switzerland
- No advertisements or data harvesting

2.2 Installation Steps

1. **Account Creation:** Visited protonvpn.com/free-vpn and created account with email and secure password
2. **Download:** Downloaded ProtonVPN Windows client from official website
3. **Installation:** Ran installer and completed setup wizard (took ~3 minutes)
4. **Login:** Signed into ProtonVPN application with account credentials

3. Testing and Results



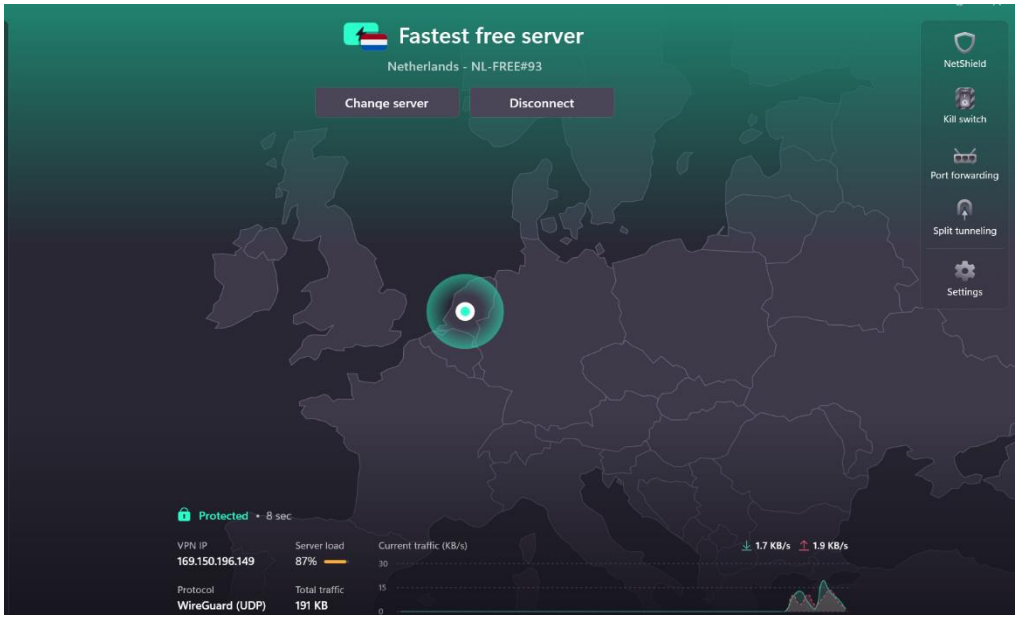
3.1 VPN Connection Test

Before Connection:

- IP Address: 115.241.133.180
- Country: India
- ISP: Jio
- Status: Unprotected

Connection Process:

- Clicked "Connect" button in ProtonVPN
- Automatically connected to fastest free server (Netherlands - NL-FREE#93)
- Connection established in 8 seconds



After Connection:

- VPN IP: 169.150.196.149
- Virtual Location: Netherlands (Amsterdam)
- Protocol: WireGuard (UDP)
- Status: Protected

3.2 IP Address Verification

Used whatismyipaddress.com to verify IP change:

Parameter	Without VPN	With VPN
IP Address	115.241.133.180	169.150.196.149
Country	India	Netherlands
City	-	Amsterdam
ISP	Jio	DataCamp Limited

Result: ✅ IP address successfully changed, confirming VPN is masking real location

3.3 Browsing Test

Browsed multiple websites (Google, YouTube, news sites) with VPN active:

- All websites loaded successfully
- HTTPS encryption maintained (padlock icons visible)
- Traffic routed through encrypted VPN tunnel
- No connection issues or DNS leaks

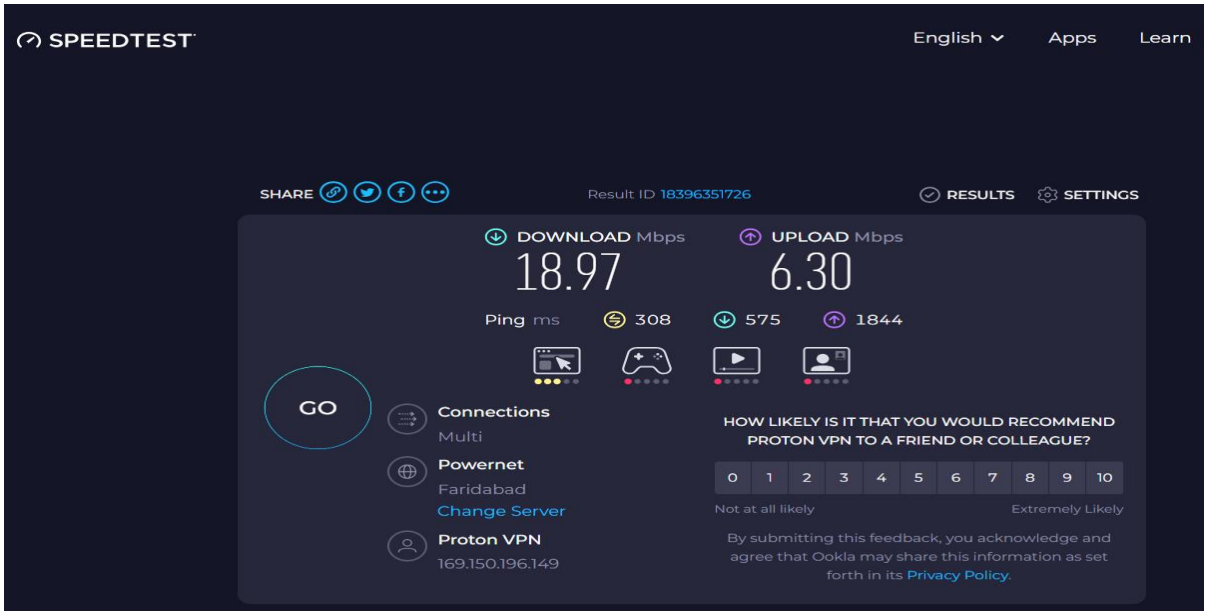
3.4 Speed Test Comparison

Without VPN:

- Download: 28.72 Mbps
- Upload: 24.25 Mbps
- Ping: 17 ms

With VPN (Netherlands server):

- Download: 18.97 Mbps
- Upload: 6.30 Mbps
- Ping: 308 ms



Analysis:

- Download speed decreased by 34% (encryption overhead + remote routing)
- Upload speed decreased by 74%
- Ping increased by 1712% due to distance to Netherlands server
- Speed reduction is expected and acceptable for privacy benefits

4. VPN Encryption and Privacy Features

4.1 Encryption Technology

AES-256 Encryption:

- Military-grade encryption standard
- Virtually unbreakable with current technology
- Transforms readable data into encrypted code
- Used by governments and financial institutions

WireGuard Protocol:

- Modern, fast VPN protocol
- Lightweight and efficient (better battery life)
- Strong cryptographic security
- Faster than older protocols like OpenVPN

4.2 How VPN Encryption Works

1. Device and VPN server negotiate encryption keys
2. All outgoing data encrypted before transmission
3. Encrypted data travels through secure tunnel to VPN server
4. VPN server decrypts and forwards to destination
5. Return traffic encrypted and sent back through tunnel
6. Device decrypts received data

4.3 Privacy Features

IP Masking: Hides real IP address, websites see VPN server IP instead

No-Logs Policy: ProtonVPN doesn't store browsing history or connection logs

DNS Leak Protection: All DNS queries routed through VPN tunnel, prevents ISP tracking

Kill Switch: Blocks internet if VPN drops to prevent IP leaks

NetShield: Blocks ads, trackers, and malware at DNS level

4.4 What VPNs Protect Against

- **ISP Surveillance:** ISP cannot monitor browsing history
- **Public WiFi Attacks:** Protects against hackers on public networks
- **Government Surveillance:** Makes mass monitoring difficult
- **Geo-Restrictions:** Bypasses location-based content blocking
- **Targeted Advertising:** Prevents tracking and profiling
- **Identity Theft:** Encrypted data prevents interception

5. Benefits of Using VPNs

5.1 Privacy Benefits

- Masks IP address from websites and advertisers
- Prevents ISP from monitoring browsing activity
- Reduces online tracking and behavioral profiling
- Protects against surveillance programs

5.2 Security Benefits

- Military-grade AES-256 encryption
- Protects data on public WiFi networks
- Prevents data interception and theft
- Secures online transactions and sensitive information

5.3 Access Benefits

- Bypass geo-restrictions for streaming and content
- Circumvent internet censorship
- Access home services while traveling abroad
- Avoid location-based price discrimination

5.4 Remote Work Benefits

- Secure connection for remote access to company resources
- Safe work environment on public networks
- Protects confidential business information
- Meets corporate security requirements

6. Limitations of VPNs

6.1 Performance Limitations

- **Reduced Speed:** 34% download speed decrease observed in testing
- **High Latency:** Ping increased from 17ms to 308ms (bad for gaming/video calls)
- **Server Congestion:** Free servers often overloaded
- **Battery Drain:** Encryption consumes more device power

6.2 Privacy Limitations

- **Not Complete Anonymity:** Browser fingerprinting and cookies still track users
- **Trust Required:** Must trust VPN provider honors no-logs policy
- **ISP Awareness:** ISP knows you're using VPN (but not what you're doing)
- **Login Tracking:** Logging into accounts reveals identity
- **No Malware Protection:** VPN doesn't protect against viruses or phishing

6.3 Technical Limitations

- **VPN Blocking:** Streaming services detect and block VPN traffic
- **Compatibility Issues:** Some devices/apps don't support VPNs
- **Connection Reliability:** VPN can drop unexpectedly
- **Setup Complexity:** Manual configuration can be challenging

6.4 Free VPN Limitations (ProtonVPN Free)

- Limited to 3 fastest server countries (Netherlands, Japan, USA)
- 45-90 second cooldown between server changes
- No streaming-optimized servers
- Single device connection only
- Lower priority during server congestion
- Missing advanced features (port forwarding, dedicated IP)

6.5 Legal Considerations

- VPNs banned/restricted in some countries (China, Russia, UAE)
- May violate terms of service for some platforms
- Doesn't make illegal activities legal
- Research local laws before use

7. Recommendations and Best Practices

When to Use VPN:

- ○ Public WiFi networks
- ○ Accessing sensitive information
- ○ International travel
- ○ Countries with censorship
- ○ Remote work
- ○ Privacy-concerned browsing

When VPN Not Necessary:

- ✕ Secure home network with HTTPS
- ✕ Local network activities
- ✕ When maximum speed needed

8. Conclusion

Task Completion

All objectives successfully achieved:

- ○ ProtonVPN account created and client installed
- ○ VPN connection established (Netherlands server)
- ○ IP address change verified (India → Netherlands)
- ○ Browsing functionality confirmed
- ○ Speed comparison completed (34% speed reduction)
- ○ Encryption and privacy features researched
- ○ Benefits and limitations documented