Task 8: VPN Setup, Testing & Privacy Analysis – Detailed Report

Objective

To gain practical knowledge of VPN technology by installing, configuring, and testing a free VPN service, and evaluating its role in secure communication and online privacy protection.

Tools Used

- **ProtonVPN (Free Tier)**
- **Google Chrome**
- **whatismyipaddress.com** → for IP masking verification

Procedure (Step-by-Step Execution)

1. **VPN Provider Selection**
   Chose **ProtonVPN** due to its strong reputation, free plan, no data limits, and secure privacy policies.
2. **Account Creation**
   Signed up using a valid email address → activated free plan with basic features.
3. **Installation & Login**
   Downloaded the **Windows ProtonVPN client** and logged in to the dashboard with authenticated credentials.
4. **Connection Setup**
   - Auto-selected connection: **Fastest Free Server – Singapore**
   - VPN dashboard displayed status as **"Protected"**
   - New virtual IP assigned: **103.216.221.77**
   - **Encryption Protocol Used:** WireGuard (UDP)
5. **IP Verification (While Connected)**
   - Checked via **whatsmyipaddress.com**
   - Website clearly detected **VPN usage**
   - **Location changed to Singapore**
   - ISP masked as **Host Universal Pty Ltd (VPN Server)**
6. **Encrypted Browsing Check**
   - Visited multiple HTTPS websites
   - Observed **padlock icon** → confirming secure and encrypted traffic routing

7. **Disconnection & Comparison**
    - Disconnected from VPN using ProtonVPN client
    - IP returned to **152.57.229.174**
    - Location back to **India** (Jio network)
8. **Speed Performance Observation**
    - **With VPN:** Slight delay in webpage loading due to encrypted routing and distant server
    - **Without VPN:** Network speed normalized after disconnection

---

Observation Summary

Parameter	Without VPN	With VPN
Public IP	152.57.229.174	103.216.221.77
Location	India (Home ISP: Jio)	Singapore (VPN server)
Encryption	No VPN encryption	WireGuard + AES-256
Privacy Level	Real identity exposed	Identity masked
Speed	Normal	Slightly slower
Security Risk	Higher exposure	Highly protected

Technical Insights

- **WireGuard Protocol:**
  Faster, more secure, modern VPN tunneling protocol with minimal overhead.
- **AES-256 Encryption:**
  Military-grade encryption ensuring data confidentiality.
- **No-Logs Policy:**
  ProtonVPN does not track or store browsing data → increases anonymity.
- **Kill Switch Feature:**
  Prevents data leaks if VPN disconnects unexpectedly (enabled in premium/optional settings).
- **DNS Leak Protection:**
  Ensures DNS queries are also routed securely through VPN tunnels.

Benefits of Using VPN

✓ Protects user identity & hides actual location
✓ Secures data on public networks like cafes, airports
✓ Prevents ISP tracking and potential surveillance
✓ Bypasses geo-restrictions for certain services
✓ Protects against man-in-the-middle and sniffing attacks

Limitations Noted

⚠ Free servers have heavy load → slower connection
⚠ Limited geographic server options
⚠ Streaming and P2P features often restricted
⚠ VPN can be blocked by certain websites and networks
⚠ Trust still depends on VPN provider policy compliance

Conclusion

This practical exercise demonstrated that a VPN is an essential cybersecurity tool for improving online privacy and protecting sensitive information. By encrypting internet traffic and masking the real IP address, ProtonVPN effectively prevented third-party tracking and minimized exposure to potential network threats. Though free VPN services may introduce performance limitations such as reduced speed and limited server options, the security advantages outweigh these downsides for general browsing and privacy needs. Overall, VPNs provide a powerful layer of protection for secure and anonymous internet usage.