**Steps Followed**

1. **Service Selection and Registration**  
   Chose **ProtonVPN** due to its strong privacy policy and availability of a free tier. Created an account on their official website.
2. **Installation**  
   Downloaded the ProtonVPN client from <https://protonvpn.com> and completed the installation on the system.
3. **Connecting to a Server**  
   Logged into the VPN client and connected to the nearest available server. The connection status was confirmed as “Connected.”
4. **IP Address Verification**  
   Visited <https://whatismyipaddress.com> to confirm the IP address had changed. The new IP reflected the location of the connected VPN server.
5. **Browsing Test with VPN Enabled**  
   Opened multiple websites using HTTPS and ensured the connections were encrypted. Browsing was smooth, and the identity was protected.
6. **VPN Disconnection and Comparison**  
   Disconnected the VPN and reloaded the IP-check site. The original IP from the local ISP reappeared, confirming the VPN was effectively masking my location.
7. **Privacy and Encryption Research**
   * ProtonVPN uses **AES-256-bit encryption**, a military-grade standard.
   * **DNS Leak Protection** was enabled to prevent exposure of DNS queries.
   * Operates under a **strict no-logs policy**, ensuring user activity is not stored.
8. **Summary of Observations**

**Benefits**:

* + Masks real IP address to protect identity.
  + Encrypts internet traffic to prevent eavesdropping.
  + Useful for bypassing censorship and accessing restricted content.

**Limitations**:

* + The free version has limited speed and server access.
  + Not effective against malware or unsafe websites unless paired with antivirus.
  + Some services may detect and block VPN usage.