**VPN Setup and Privacy Demonstration**

**Objective**

To understand and demonstrate how VPNs enable privacy and secure communication by hiding the real IP address, encrypting traffic, and altering the perceived geographic location. IP\_After\_VPN.png

**Tools Used**

* **VPN Client:** ProtonVPN (Free Tier)
* **IP Verification Website:** whatismyipaddress.com.

**Steps Performed**

**1. Checked IP Address before Connecting to VPN**

* Accessed whatismyipaddress.com to view the original IP.
* **Result:**
  + IP Address: 1.39.\*\*.\*\*5
  + Location: Solapur, Maharashtra, India
  + ISP: Vodafone Essar. (IP\_Before\_VPN.png)

**2. Downloaded and Installed ProtonVPN**

* Created a free account on ProtonVPN.
* Downloaded and installed the ProtonVPN client from the official site.
* Logged in with newly created credentials.

**3. Connected to VPN Server**

* Selected the fastest free server (Norway).VPN\_Connected.jpg
* Connection established; client status showed "Protected" with a new VPN IP.

**4. Checked IP Address After Connecting to VPN**

* Again visited whatismyipaddress.com to verify IP change.
* **Result:**
  + IP Address: 205.147.17.31
  + Location: Switzerland (Geneve) [ISP: Proton AG]
  + Website flagged VPN usage. (IP\_After\_VPN.png)

**5. Verified Encrypted Browsing**

* Browsed normal sites with VPN enabled; traffic was encrypted as indicated in the ProtonVPN dashboard .(VPN\_Connected.png)

**6. Disconnected VPN and Compared Speed/IP**

* Disconnected VPN.
* Speed comparison observed: some reduction in speed while connected due to routing traffic through a remote server (qualitative observation).

**VPN Encryption and Privacy Features**

* ProtonVPN uses modern encryption (WireGuard UDP in your case) to protect data in transit.VPN\_Connected.jpg
* Hides real IP, masking location and making it difficult to track browsing habits.
* Provides a "Kill Switch" to prevent real IP leaks in case of disconnection.
* Offers split tunneling and server selection for targeted access.

**Summary: Benefits and Limitations of VPNs**

**Benefits**

* **Privacy Protection:** Hides real IP address and location.
* **Encryption:** Data is securely encrypted to prevent eavesdropping.
* **Bypass Restrictions:** Allows sidestepping geographic content blocks.
* **Public Network Security:** Protects against threats on open Wi-Fi.

**Limitations**

* **Speed Reduction:** Can slow down Internet speeds due to encryption overhead and traffic routing.
* **Service Restrictions:** Some websites/services may block known VPN IPs.
* **Free Tiers Have Limits:** Free versions of VPNs have limited server locations, speed, and bandwidth.
* **Potential Trust Risks:** Trust in VPN provider is required as all data passes through their servers. (IP\_After\_VPN.png)

**Evidence**

* Screenshot of IP before VPN: shows original location and ISP.IP\_Before\_VPN.jpg
* Screenshot of VPN connection: shows successful connection to Norway server, new IP, encrypted state.VPN\_Connected.jpg
* Screenshot of IP after VPN: shows VPN IP and changed location detected.IP\_After\_VPN.jpg