Task 8: VPN Setup and Privacy Report

Cybersecurity Lab Report

KANDI TEJASREE
ELEVATE LABS

Task 8:

VPN Setup and Privacy Report

Index:

1.Choose a reputable free VPN service and sign up.
2.Download and install the VPN client.
3.Connect to a VPN server (choose closest or any location).
4.Verify your IP address has changed (use whatismyipaddress.com).
5.Browse a website to confirm traffic is encrypted.
6.Disconnect VPN and compare browsing speed and IP.
7.Research VPN encryption and privacy features.
8.Write a summary on VPN benefits and limitations

Objective:

Understand the role of VPNs in protecting privacy and secure communication.

Tools Used:

- Any VPN

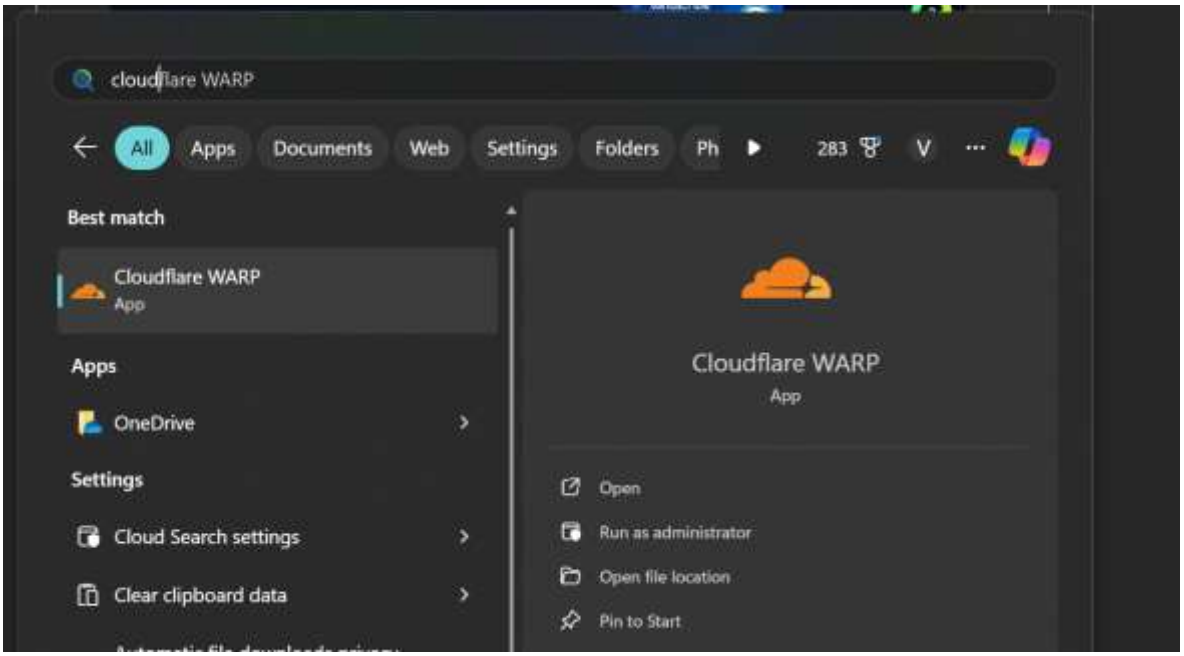
Steps Performed:

1. Sign Up:

- Go to https://windscribe.com
- Create a free account.

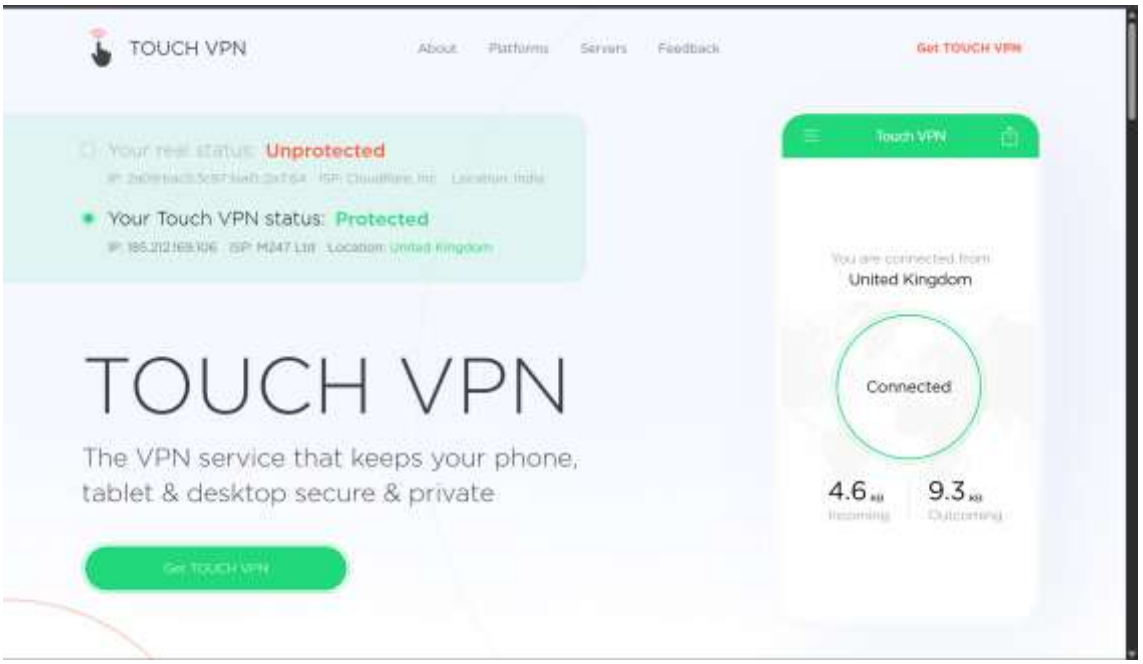
2. Download & Install:

- Download ProtonVPN for your OS (Windows/Linux/macOS/Android).
- Install and log in.



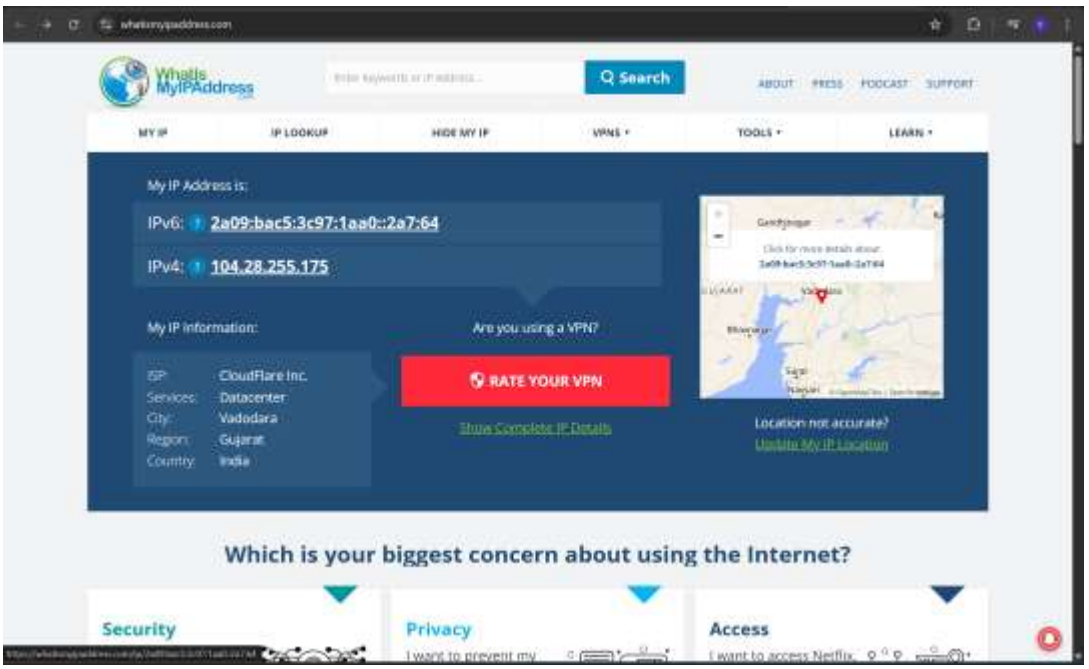
3. Connect to VPN Server:

- Open the client.
- Choose the Nearest Location (e.g., India/Netherlands/US).
- Click Connect.



4. Verify IP Address Change:

- Visit https://whatismyipaddress.com
- Confirm that your IP has changed to the VPN server's IP.



5. **Testing Encrypted Traffic:**

- Browse websites like Google or YouTube.
- Data now travels through an encrypted tunnel.

Once connected to a VPN server, you can confirm that your internet traffic is encrypted by visiting secure websites such as Google or Wikipedia. Make sure the URL begins with "https://" and that a padlock icon appears in the browser's address bar, indicating SSL/TLS encryption is active. To further verify that your data is being securely routed through the VPN, you can use tools like ipleak.net or dnsleaktest.com to check for IP and DNS leaks. If the VPN is working correctly, your real IP address and DNS servers should be hidden, and only the VPN server's information will be visible. This confirms that your internet traffic is encrypted and anonymized, protecting your data from being monitored or intercepted—especially useful when connected to public Wi-Fi. Even if a malicious actor attempts to capture your traffic, all they would see is encrypted data, thanks to the secure tunnel created between your device and the VPN server.

6. **Disconnect VPN:**

- Turn off VPN and check:
  - IP reverts to your real IP.
  - Browsing speed returns to normal.

Conclusion:

We successfully set up a free VPN (e.g., ProtonVPN or Windscribe), verified encrypted communication, and confirmed that the public IP address was masked. VPNs play a crucial role in:

- Protecting online identity and location
- Encrypting data on public networks
- Preventing ISP and third-party tracking

Key Learning:
VPNs are essential tools for secure and private browsing, especially on public or untrusted networks. However, they should be used in combination with good cybersecurity practices, as VPNs alone do not protect against malware or phishing.