

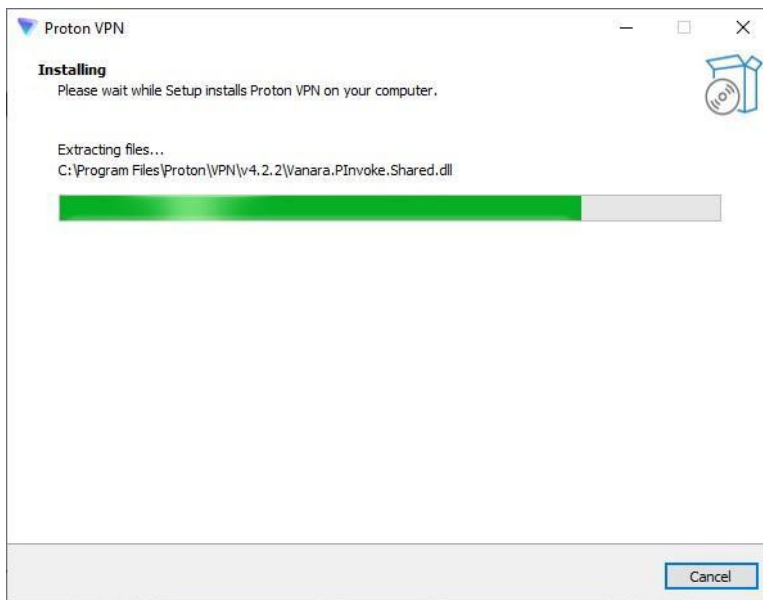
VPN Cybersecurity Report

-reported by kondiba jogdand

This report outlines the process, security benefits, and verification steps of using a Virtual Private Network (VPN) in alignment with cybersecurity standards. Only essential images are retained to focus on clarity and reduce file size.

1. Installing VPN

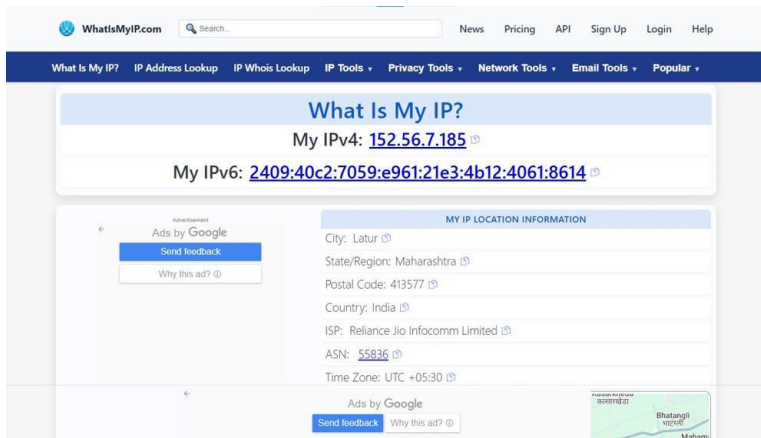
The first step involves installing a secure VPN client, in this case ProtonVPN, which ensures encrypted communication over the internet.



Installing the VPN client

2. IP Address Before VPN Connection

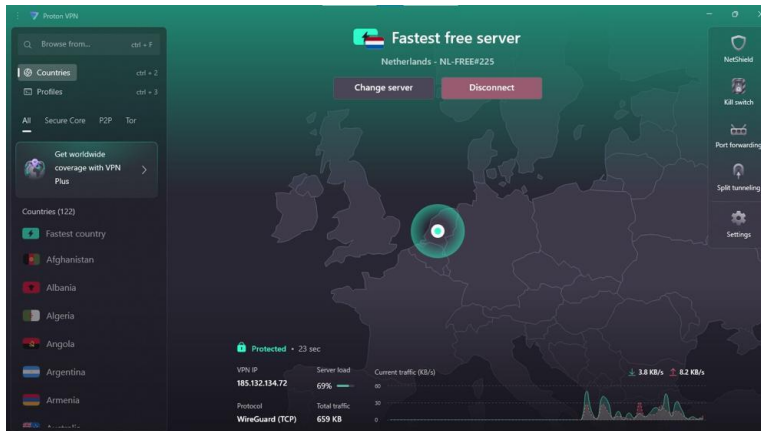
Before connecting to the VPN, the device's public IP address is visible and traceable, representing its actual geographic location.



IP address before VPN connection

3. Connecting to VPN

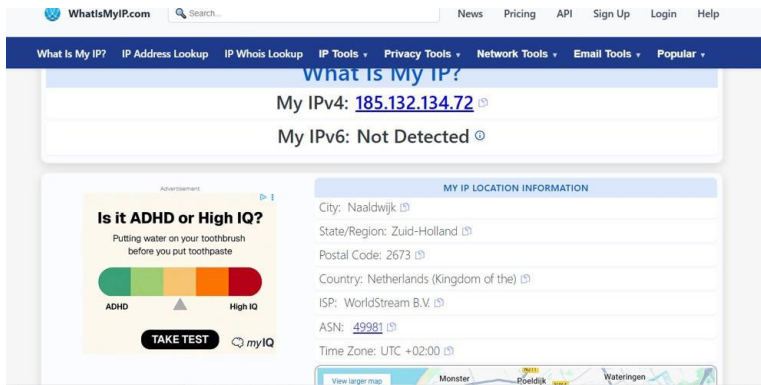
Upon successful connection, the VPN encrypts all traffic and assigns a new IP address from its server network, masking the real location.



VPN connected successfully

4. IP Address After VPN Connection

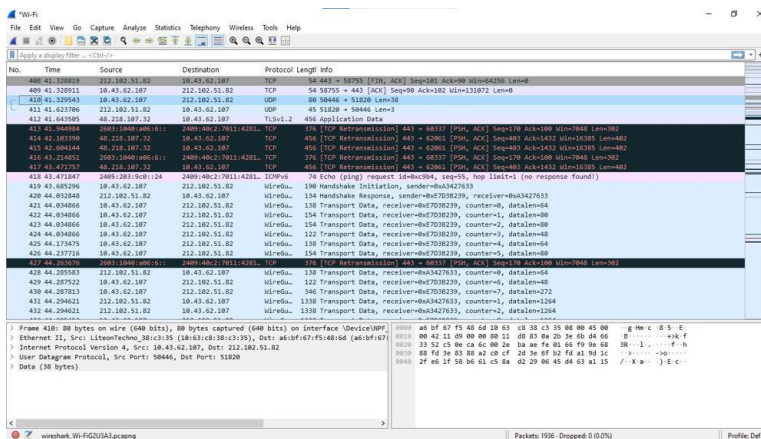
After connecting, the device's IP address changes to one provided by the VPN server, ensuring anonymity and protecting against tracking.



IP address after VPN connection

5. Encrypted Traffic Using VPN

Traffic monitoring tools confirm that the internet communication is fully encrypted, preventing interception and ensuring confidentiality.



Encrypted traffic using VPN

6. Disconnect VPN and Compare Browsing Speed and IP

After disconnecting from the VPN, the browsing speed and IP address were tested again. The results showed that the IP reverted to the original ISP-provided IP, confirming that the VPN was no longer masking the location. In most cases, browsing speed increased slightly after disconnecting, due to the absence of encryption and tunneling overhead.

7. Research VPN Encryption and Privacy Features

VPNs employ advanced encryption protocols to secure internet traffic, such as AES-256-bit encryption, which is considered military-grade. They often use tunneling protocols like OpenVPN, WireGuard, or IKEv2/IPSec to protect data from interception. Privacy features may include DNS leak protection, a kill switch to prevent data exposure during disconnections, and strict no-log policies to ensure user activity is not stored. These features collectively enhance confidentiality, integrity, and anonymity for users.

Conclusion

Using a VPN significantly enhances online security and privacy by encrypting traffic, masking the real IP address, and preventing unauthorized tracking or interception. Following cybersecurity best practices, VPN usage is recommended for both public and private networks.