VPN Privacy & Secure Communication — Lab Report

Student: rithubaran

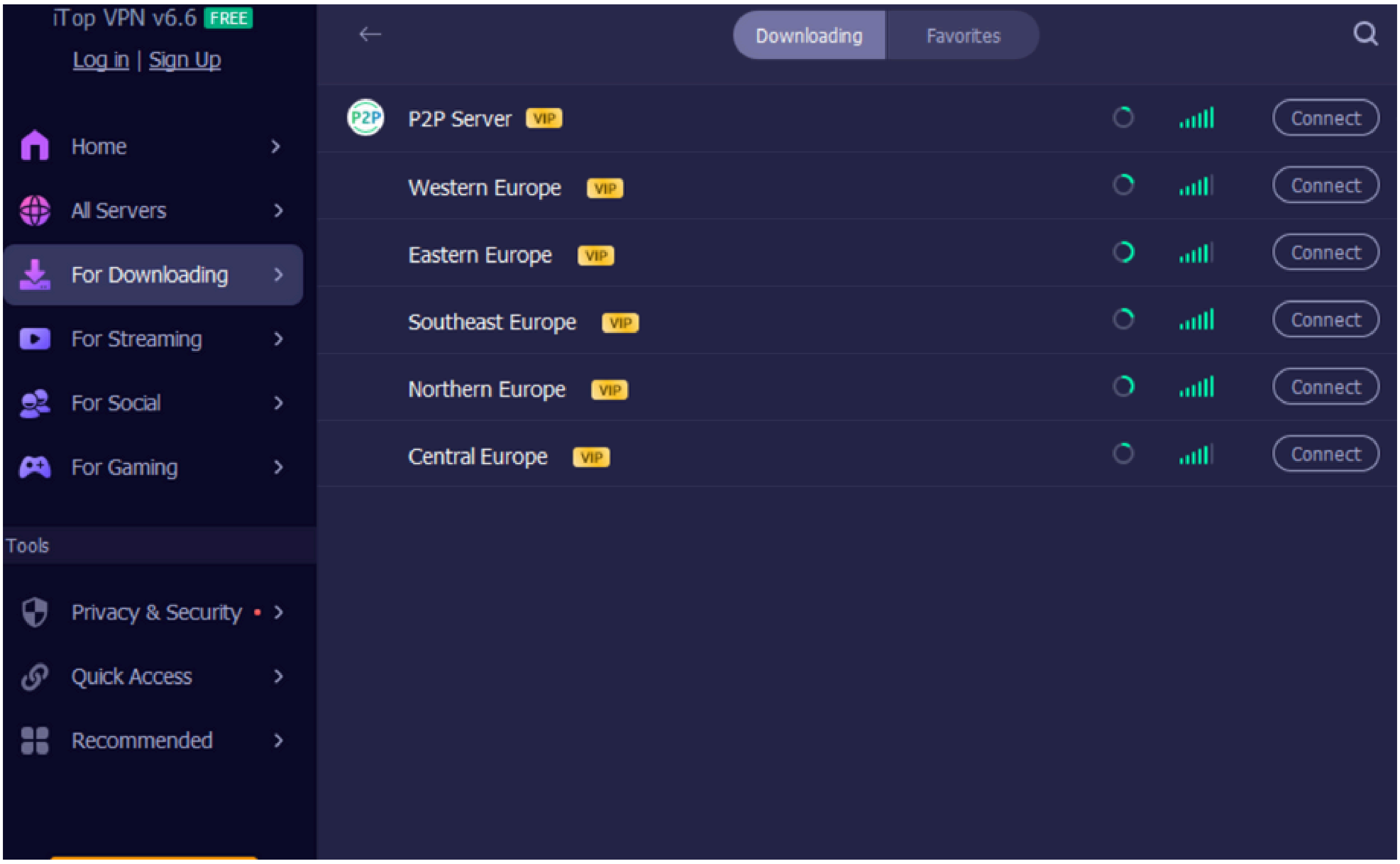
Date:15/8/24

Objective: Understand how VPNs protect privacy and enable secure communication by setting up a free VPN, verifying the connection, and comparing browsing with/without the VPN.

Tools

- **Device/OS: (Windows/macOS/Linux/Android/iOS)**
- **VPN service: ProtonVPN (Free) or Windscribe (Free)**
- **Browser: (Chrome/Firefox/Edge/Safari)**
- **Test sites: whatismyipaddress.com, ipleak.net (optional), fast.com (optional speed)**

A. Choose & Sign Up (Free Tier)

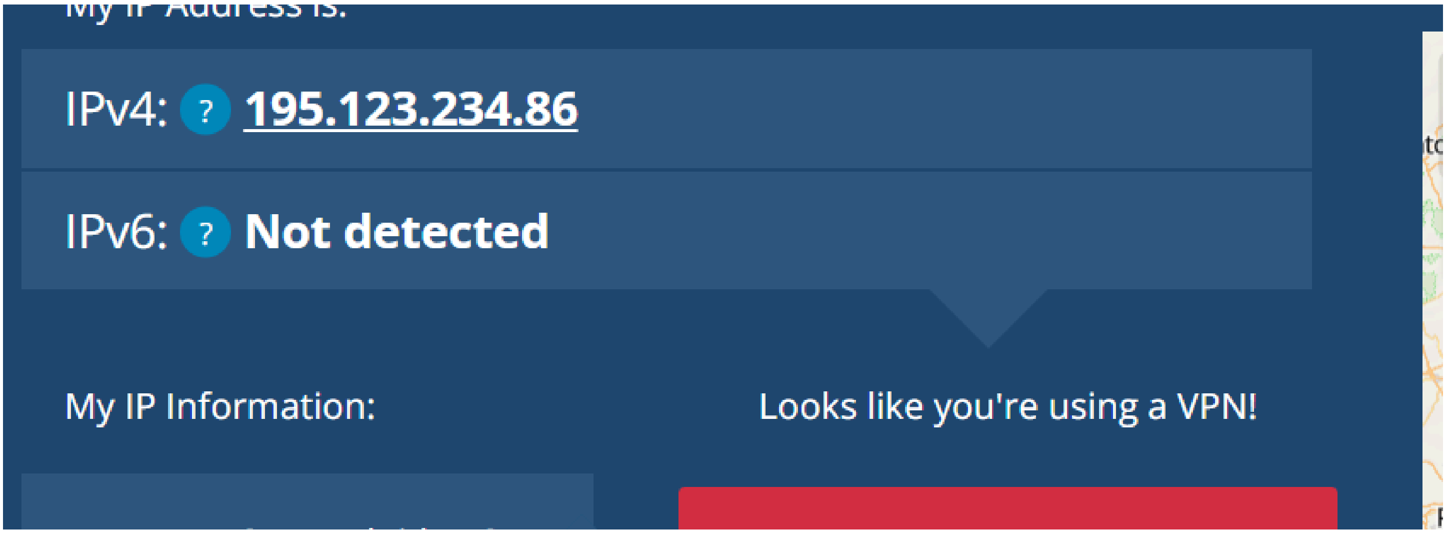


B. Install & Connect

Windows/macOS (ProtonVPN GUI)

1. Launch ProtonVPN → Log in.
2. In the map/list, pick a Free server (usually marked "FREE").
3. Click Connect. Wait for status: Connected.
4. Optional: Enable Kill Switch and Auto-connect in Settings.

C. Verify the Tunnel



My IP Address is:

IPv4: ? 195.123.234.86

IPv6: ? Not detected

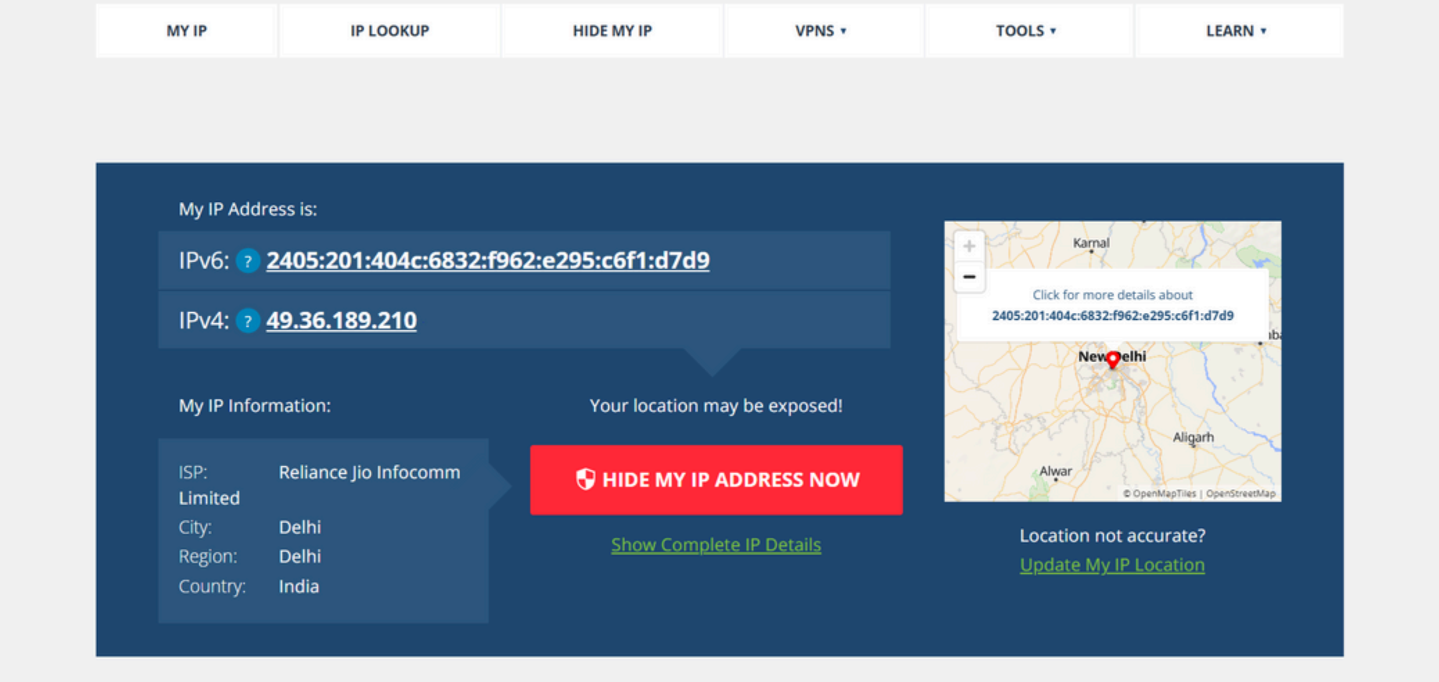
My IP Information:

Looks like you're using a VPN!

E. Connection Status Screenshot (Deliverable)

F. Observations

1) IP & Location — Before india



My IP Address is:

IPv6: ? 2405:201:404c:6832:f962:e295:c6f1:d7d9

IPv4: ? 49.36.189.210

My IP Information:

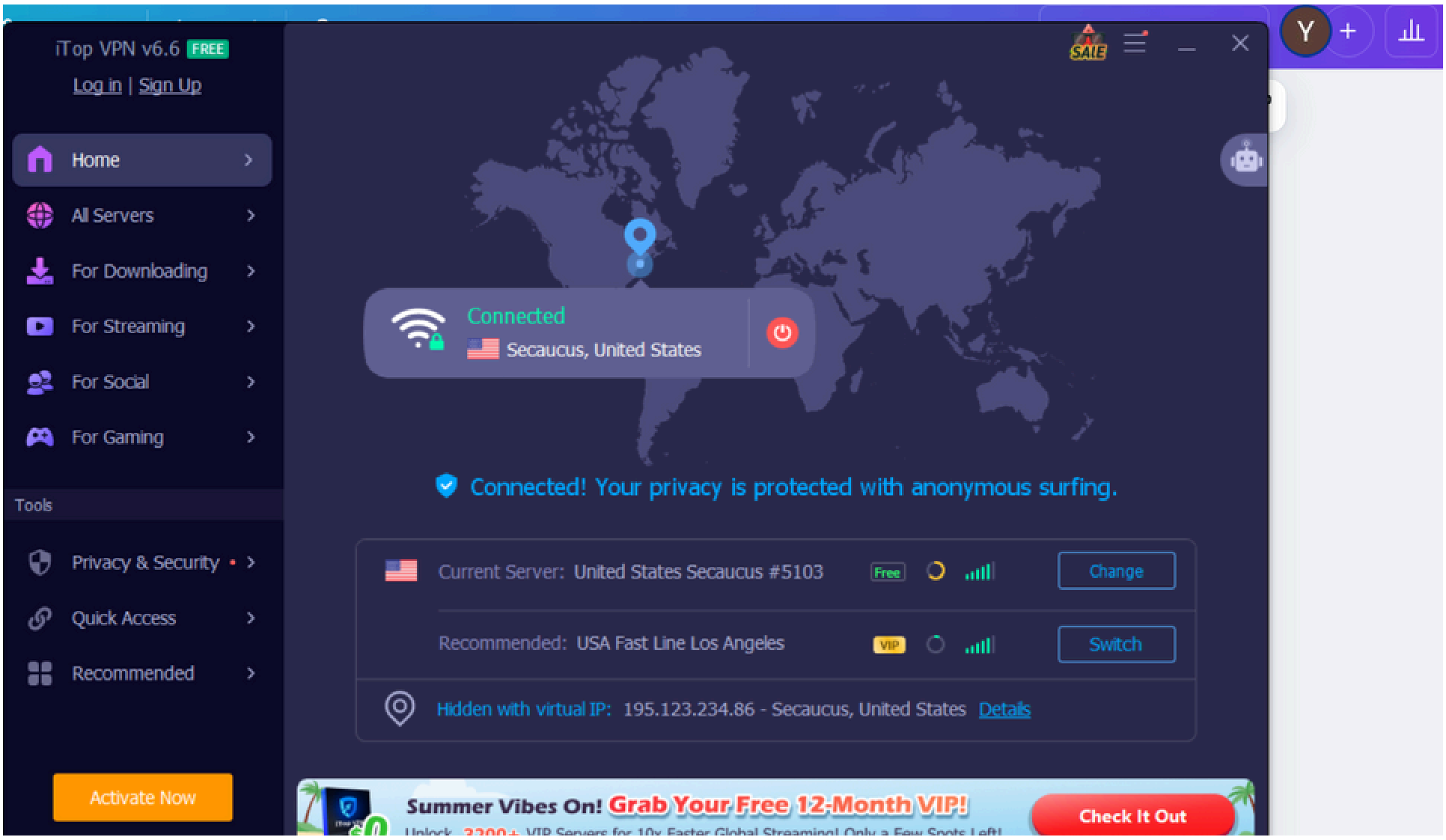
ISP: Reliance Jio Infocomm Limited
City: Delhi
Region: Delhi
Country: India

Your location may be exposed!

HIDE MY IP ADDRESS NOW
Show Complete IP Details
Karnal
Click for more details about
2405:201:404c:6832:f962:e295:c6f1:d7d9
New Delhi
Aligarh
Alwar
© OpenMapTiles | OpenStreetMap

Location not accurate?
Update My IP Location

after usa



Connected
Secaucus, United States

Connected! Your privacy is protected with anonymous surfing.

Current Server: United States Secaucus #5103 Free

Recommended: USA Fast Line Los Angeles VIP

Hidden with virtual IP: 195.123.234.86 - Secaucus, United States

Summer Vibes On! Grab Your Free 12-Month VIP!
Unlock 3200+ VIP Servers for 10x Faster Global Streaming! Only a Few Spots Left!

3) Any site/app issues while on VPN?

G. How VPNs Protect Privacy (Brief Research Notes)

- **Encrypted tunnel: Your device ⇔ VPN server traffic is encrypted (typically AES-256 or ChaCha20 with modern protocols like OpenVPN or WireGuard). This prevents local** eavesdropping on public Wi-Fi and hides URLs/content from local network operators.

- IP masking: Websites see the VPN server’s IP, not your home/phone IP. This reduces IP-based tracking and shields your real IP from the sites you visit.
- ISP/Network visibility: ISPs can see you’re connected to a VPN (server IP/port, data volume) but not the specific sites you visit (hostnames/content) when the tunnel is active.
- Kill switch: Automatically blocks traffic if the VPN drops to prevent leaks.
- DNS protection: Good VPNs route DNS queries inside the tunnel to avoid ISP DNS leaks.
- Split tunneling (optional): Choose which apps/sites go through the VPN vs direct Internet.

H. Benefits vs. Limitations

Benefits

- Protects against snooping on public Wi-Fi.
- Masks your IP from websites and apps, reducing surface for targeted attacks/abuse.
- Can bypass local network blocks/censorship (depending on provider and region).
- Centralized DNS handling can reduce DNS leaks.

Limitations & Caveats

- Not total anonymity: The VPN provider can technically see your traffic metadata; trust and no-logs policies matter.
- Jurisdiction & policy: Provider location and laws affect data handling and disclosure duties.
- Speed & stability: Free servers can be crowded; expect slower speeds and occasional disconnects.
- Service blocking: Some sites block known VPN IPs; captchas may increase.
- Device leaks: WebRTC/DNS/IPv6 leaks can reveal your IP if not mitigated.
- Account logins: Logging into personal accounts (Google, banking) still identifies you to those services.
- Malware/phishing: VPNs don’t replace antivirus, safe browsing, or OS updates.
- Illegal/geolocation-restricted use: Respect laws and terms of service wherever you are.