

Task -8

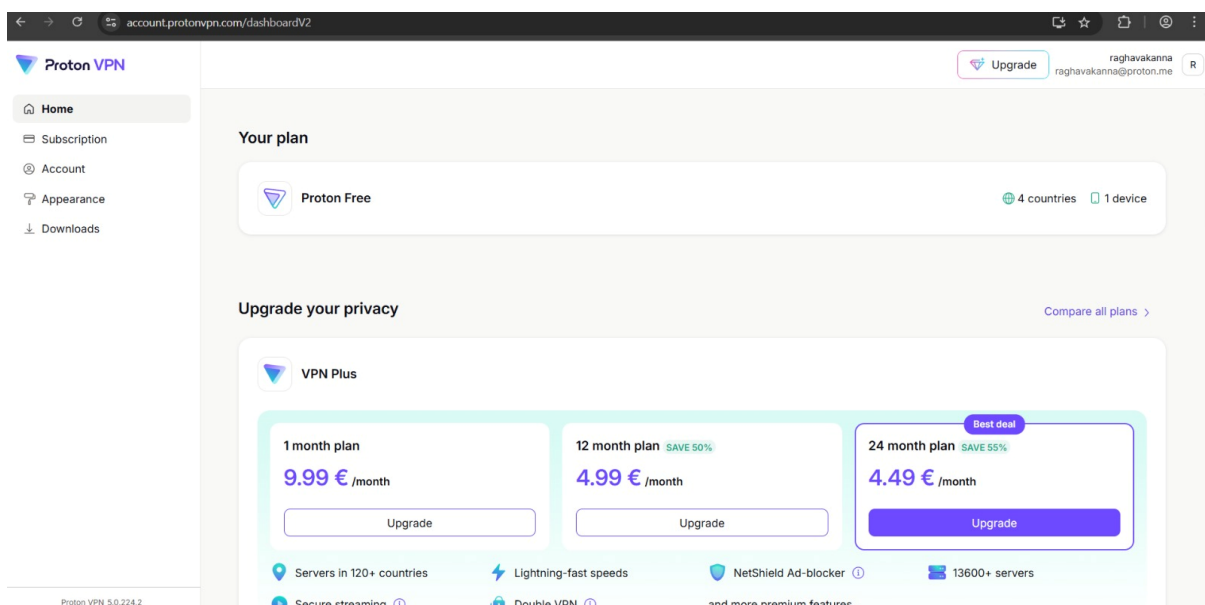
Working with VPNs (Virtual Private Network):

Virtual Private Network: A VPN (Virtual Private Network) is a tool that keeps your internet connection private and secure by sending your data through an encrypted tunnel to a VPN server. This hides your real IP address, making it look like you're browsing from a different location, and helps protect you from hackers, especially on public Wi-Fi. A VPN can also let you access websites or content blocked in your country. However, it doesn't make you completely anonymous or protect you from things like viruses or scams.

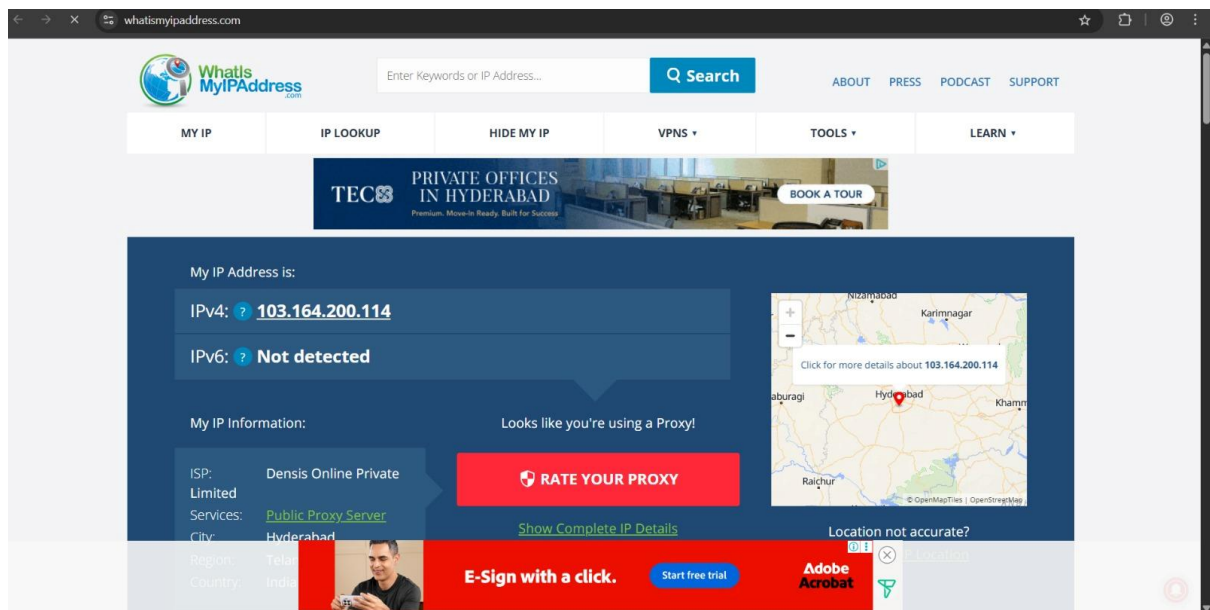
Proton VPN:

Proton VPN is a secure, privacy-focused VPN service created by the team behind Proton Mail (the well-known encrypted email provider). It offers strong encryption, a strict no-logs policy, and unique features like Secure Core (routing traffic through multiple servers for extra protection).

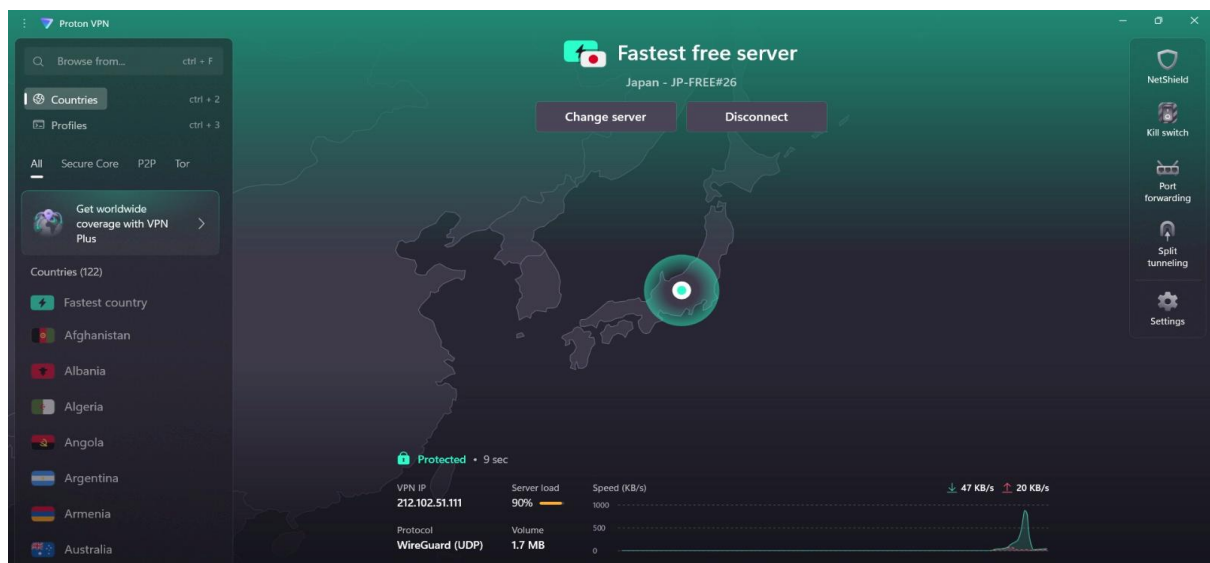
Sign up for a free Proton VPN account on their website, download and install the Proton VPN app for Windows, then log in and connect to a free server to start using the VPN.



The IP address of the system before connecting to the VPN is **103.164.200.114**

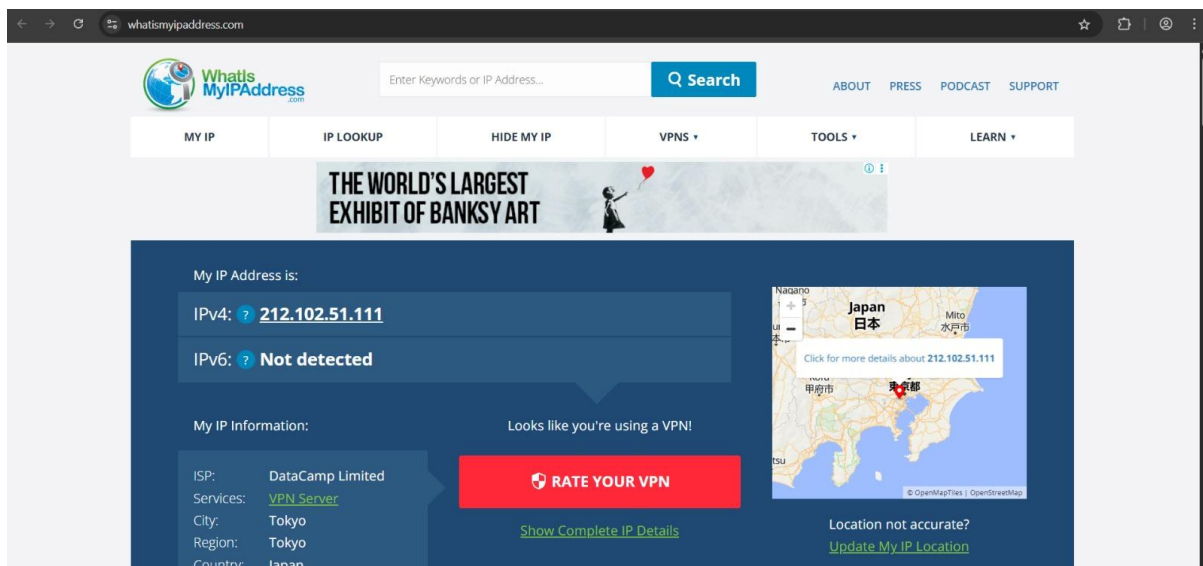


Connecting to the VPN



After connecting to the VPN, the IP address changes because the VPN encrypts your internet traffic and shows a masked IP address from the VPN server instead of your real one. This protects your privacy by hiding your actual location and identity online. The VPN acts like a secure proxy between your device and the websites or services you access, ensuring that your internet service provider (ISP) or anyone else on the network cannot see your browsing activity or original IP address. This helps prevent tracking, improves security on public Wi-Fi, and allows you to bypass geo-restrictions or censorship.

IP address is changed to **212.102.51.111**

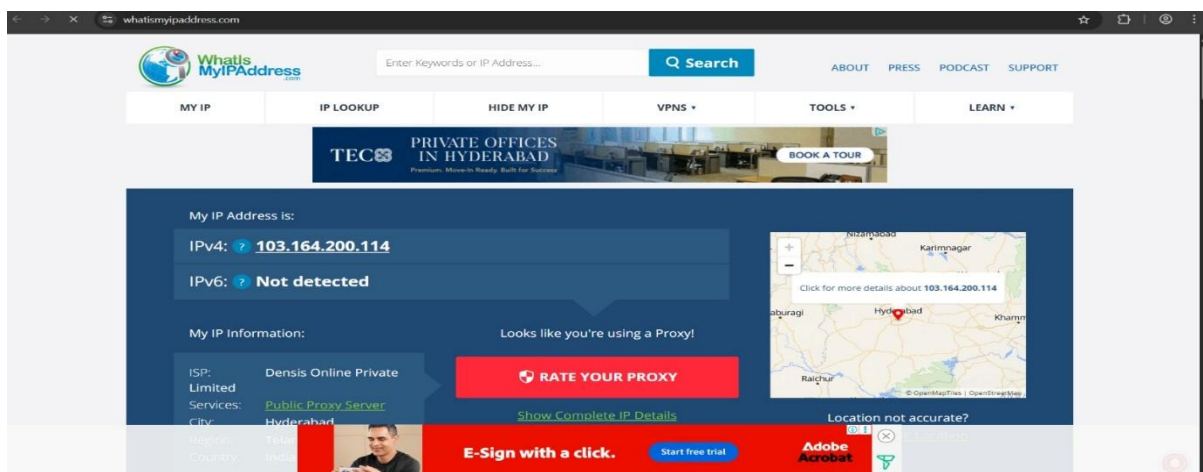


The screenshot shows the WhatIsMyIPAddress.com website. The main content area displays the user's IP address as 212.102.51.111 (IPv4) and 'Not detected' (IPv6). Below this, it states 'Looks like you're using a VPN!' and provides information about the ISP: DataCamp Limited, Services: VPN Server, City: Tokyo, Region: Tokyo, and Country: Japan. A red button labeled 'RATE YOUR VPN' is visible. To the right, a map shows the location in Japan. The website also features a search bar, navigation links (ABOUT, PRESS, PODCAST, SUPPORT), and a banner for 'THE WORLD'S LARGEST EXHIBIT OF BANKSY ART'.

After connecting to the VPN, the internet speed may also decrease because your data has to travel through the VPN server, and the encryption process adds overhead, which can cause slower speeds compared to a direct connection.

If you **disconnect the VPN**, your internet connection stops routing through the VPN server, and your IP address **reverts back to your original, real IP assigned by your internet service provider (ISP)**. This means websites and online services will again see your true location and IP address.

At the same time, your **internet speed usually returns to normal**, because your traffic is no longer being encrypted and routed through a potentially distant VPN server — so there's less overhead and latency compared to when the VPN was connected.



The screenshot shows the WhatIsMyIPAddress.com website. The main content area displays the user's IP address as 103.164.200.114 (IPv4) and 'Not detected' (IPv6). Below this, it states 'Looks like you're using a Proxy!' and provides information about the ISP: Densis Online Private Limited, Services: Public Proxy Server, City: Hyderabad, Region: Hyderabad, and Country: India. A red button labeled 'RATE YOUR PROXY' is visible. To the right, a map shows the location in Hyderabad. The website also features a search bar, navigation links (ABOUT, PRESS, PODCAST, SUPPORT), and a banner for 'PRIVATE OFFICES IN HYDERABAD'.

VPN Encryption and Privacy Features:

Encryption — VPNs use strong encryption protocols like AES-256 to protect your data by scrambling it so no one (like hackers or ISPs) can read your traffic.

Secure Protocols — Modern VPNs support protocols like OpenVPN, WireGuard, and IKEv2/IPSec, which balance strong security with good speed.

IP Address Masking — VPNs hide your real IP address and replace it with the VPN server's IP, making your online activity harder to trace back to you.

No-Logs Policies — Good VPNs promise not to keep records of your browsing activity or connection history, protecting your privacy even if someone demands their logs.

DNS Leak Protection — VPNs can prevent your device from accidentally sending DNS requests outside the VPN tunnel, which could reveal what websites you're visiting.

Kill Switch — If the VPN disconnects unexpectedly, a kill switch blocks all internet traffic until the VPN reconnects, ensuring your real IP and data are never exposed.

Split Tunneling (optional) — Lets you choose which apps or sites use the VPN and which connect directly, giving you flexibility over what traffic is encrypted.

VPN Benefits:

- **Privacy Protection** — Hides your real IP address and location, helping keep your identity private online.
- **Data Encryption** — Secures your internet traffic, protecting sensitive information from hackers, especially on public Wi-Fi.
- **Bypass Restrictions** — Lets you access geo-blocked content and websites censored in certain countries.
- **Prevent Tracking** — Reduces tracking by ISPs, advertisers, or third parties monitoring your internet activity.
- **Safer Remote Work** — Allows secure connections to company networks from anywhere.

VPN Limitations:

- **Speed Reduction** — Encryption and routing through VPN servers can slow down your internet speed.
 - **Trust Required** — You must trust your VPN provider not to log or misuse your data.
 - **Not Complete Anonymity** — VPNs hide your IP but don't make you fully anonymous; websites may still track you via cookies or browser fingerprinting.
 - **May Not Defeat All Blocks** — Some services detect and block VPN traffic (e.g., some streaming platforms or government firewalls).
 - **Doesn't Protect Against Malware** — A VPN won't stop viruses or phishing attacks on its own; you still need good security practices.
-